



PX-1000/2000 シリーズ

ユーザ ガイド
リリース 2.3

Copyright © 2012 Raritan, Inc.

DPX2-1000-0D-v2.3-J

2012 年 3 月

255-80-6105-00

安全基準

警告: このガイドのすべてのセクションを読んで理解してから、本製品を設置または運用してください。

警告: 本製品は、電圧が製品のネームプレートに示されている範囲内にある AC 電源に接続してください。ネームプレートの電圧を超えた状態で本製品を動作させると、感電、火災、死傷につながるおそれがあります。

警告: 本製品は、国や地域の電気工事規定に従って適切な定格のヒューズまたはサーキットブレーカーで電流が制限されている AC 電源に接続してください。適切な電流制限をかけずに本製品を動作させると、感電、火災、死傷につながるおそれがあります。

警告: 本製品は、保安用接地に接続してください。製品のプラグと壁のアウトレット（コンセント）の間に「グラウンド リフト アダプタ」は使用しないでください。保安用接地に接続していない場合、感電、火災、死傷につながるおそれがあります。

警告: 本製品には、ユーザによる保守が可能な部品はありません。本製品を開いたり、改造や分解をしたりしないでください。あらゆる保守サービスは、資格を持った担当者が行う必要があります。本製品の保守サービスを行う前に、電源を切断してください。この警告に従わなかった場合、感電、死傷につながるおそれがあります。

警告: 本製品は、湿気の少ない場所で使用してください。本製品を湿気の多い場所で使用した場合、感電、死傷につながるおそれがあります。

警告: 本製品のアウトレット（コンセント）ランプ、アウトレット（コンセント）リレー スイッチ、およびその他のアウトレット（コンセント）電源オン/オフ インジケータを利用して、アウトレット（コンセント）に電力が供給されているかどうかを判断しないようにしてください。本製品に接続されているデバイスの修理や保守サービスを行う前に、そのデバイスの電源プラグを抜いてください。デバイスの電源プラグを抜かずに保守サービスを行うと、感電、火災、死傷につながるおそれがあります。

警告: 本製品は、UL/IEC 60950-1 に相当する定格の IT 機器に電力を供給する場合にのみ使用してください。この定格を満たしていないデバイスに電力を供給しようとすると、感電、火災、死傷につながるおそれがあります。

警告: アウトレット（コンセント）リレーを含む Raritan 製品は、モーターやコンプレッサのような大量の誘導負荷に電力を供給する目的では使用しないでください。大量の誘導負荷に電力を供給しようとすると、リレーが損傷するおそれがあります。

警告: 本製品は、重篤な患者向けの医療機器、火災報知器、煙感知器などに電力を供給する目的では使用しないでください。本製品を使用してそのような機器に電力を供給すると、死傷につながるおそれがあります。

警告: 本製品が、電源コードやプラグの取り付けが必要なモデルである場合、そうした取り付け作業はすべて電気工事士が行い、製品のネームプレートに記載されている定格および国や地域の電気工事規定に基づいて、適切な定格のコードやプラグを使用する必要があります。無資格の電気技術者が取り付けを行った場合や、適切な定格のコードやプラグを使用しなかった場合は、感電、火災、死傷につながるおそれがあります。

警告: 本製品には、カリフォルニア州において発癌、出生異常、または生殖障害の原因として知られている化学物質が含まれています。

安全の指針

1. 本製品の設置は、電力に関する知識や経験を備えた担当者のみが行うべきものです。
2. 本製品の設置や場所の移動を行う前に、電源から電源コードが抜かれていることを確認してください。
3. 本製品は、電子設備ラック内で使用されるように設計されています。本製品の金属ケースには、電源コードの接地線が電氣的に結合されています。ケースのねじ式接地点は、本製品とラックの保安用接地の追加手段として使用できます。
4. 本製品に電力を供給する分岐回路アウトレット（コンセント）を調べてください。アウトレット（コンセント）の送電線、ニュートラル ピン、および保安用接地ピンが正しく結線されており、電圧と相が正しいことを確認してください。また、分岐回路アウトレット（コンセント）が適切な定格のヒューズまたはサーキット ブレーカで保護されていることを確認してください。
5. 製品が、オン/オフを切り替えられるアウトレット（コンセント）を備えたモデルである場合は、アウトレット（コンセント）をオフにしても電力が存在することがあります。

この文書には、著作権で保護されている固有の情報が含まれています。無断で転載することは禁じられています。この文書のどの部分も Raritan, Inc. より事前に書面による承諾を得ることなく複写、複製、他の言語へ翻訳することを禁じます。

© Copyright 2012 Raritan, Inc. このドキュメントに記載されているすべてのサードパーティ製のソフトウェアおよびハードウェアは、それぞれの所有者の登録商標または商標であり、それぞれの所有者に帰属します。

FCC 情報

この装置は試験済みであり、FCC 規則の Part 15 に規定された Class A デジタル装置の制限に準拠していることが証明されています。これらの制限は、商業環境に設置した場合に有害な干渉を防止するために規定されています。この装置は、無線周波数を生成、利用、および放射する可能性があり、指示に従って設置および使用しなかった場合、無線通信に対して有害な干渉を引き起こす可能性があります。この装置を居住環境で使用した場合、有害な干渉を引き起こす可能性があります。

VCCI 情報 (日本)

この装置は、情報処理装置等電波障害自主規制協議会 (V C C I) の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan 社は、事故、自然災害、本来の用途とは異なる使用、不正使用、Raritan 社以外による製品の変更、その他 Raritan 社が関与しない範囲での使用や、通常の使用条件以外での使用による製品の故障について、一切の責任を負いません。



目次

安全基準	ii
安全の指針	iv
対象モデル	xv
『Dominion PX ユーザ ガイド』における最新情報	xvi
はじめに	1
製品モデル	1
製品の機能	1
パッケージの内容	3
ゼロ U 製品	4
1U 製品	4
2U 製品	4
PDU のラックマウント	5
ラック マウント安全基準	5
サーキット ブレーカの向きの制限	6
L-ブラケットを使用したゼロ U モデルの装着	7
ボタン マウントを使用したゼロ U モデルの装着	9
かぎつめ足ブラケットを使用したゼロ U モデルの装着	11
背面の 2 つのボタンを使用したゼロ U モデルの装着	12
L-ブラケットとボタンを使用したゼロ U モデルの装着	14
1U モデルまたは 2U モデルの装着	15
設置と設定	18
設置前の確認点	18
製品およびコンポーネントのパッケージの開梱	18
設置場所の準備	19
装置の設定ワークシートの記入	19
分岐回路の定格の確認	19

インレットへのケーブル リテンション クリップの取り付け (任意).....	20
電源への PDU の接続.....	21
Dominion PX の設定	21
コンピュータへの Dominion PX の接続	22
USB-to-Serial ドライバのインストール	23
ネットワークへの Dominion PX の接続	25
初期ネットワーク設定.....	26
USB による PDU のカスケード接続.....	33
アウトレット (コンセント) へのケーブル リテンション クリップの取り付け (任意).....	36
環境センサーの接続 (オプション)	37
接点閉鎖センサーについて	39
空気差圧センサーの接続方法.....	42
資産管理センサーの接続 (オプション).....	42
資産センサーの結合	43
Dominion PX への資産センサーの接続	45
ブレード拡張ストリップの接続	47
AMS-M2-Z 資産センサーの接続 (オプション).....	50
Logicool Web カメラの接続 (オプション)	52
GSM モデムの接続 (オプション).....	52
Schroff LHX ヒート エクスチェンジャの接続 (オプション).....	53

PDU の使用 54

パネルのコンポーネント	54
電源コード	54
アウトレット (コンセント).....	54
接続ポート	55
LED 表示.....	58
リセット (RESET) ボタン	62
サーキット ブレーカ.....	63
ボタンタイプのサーキット ブレーカのリセット	63
ハンドルタイプのサーキット ブレーカのリセット	64
ヒューズ.....	65
ゼロ U モデルでのヒューズの交換.....	65
1U モデルでのヒューズの交換.....	66
ブザー	68

Web インタフェースの使用 69

サポートされている Web ブラウザ	70
Web インタフェースへのログイン	70
ログイン	70
パスワードの変更	72

ログアウト	72
Web インタフェースの概要	73
メニュー	74
Dominion PX Explorer ペイン	75
[Setup (設定)] ボタン	78
ステータス バー	78
[Add Page (ページの追加)] アイコン	80
[logout (ログアウト)] ボタン	80
データ ペイン	81
詳細情報	81
ダッシュボードの表示	87
警告対象のセンサー	88
デバイス管理	88
PDU 情報の表示	89
PDU の名前付け	90
ネットワーク設定の変更	91
ネットワーク サービス設定の変更	97
日付と時刻の設定	104
拡張ポートの設定	107
シリアル ポートの設定	108
デバイスの高度の指定	109
データ ロギングの設定	110
SMTP の設定	111
EnergyWise の設定	112
Dominion PX デバイスの再起動	113
[User Management (ユーザ管理)]	113
ユーザ プロファイルの作成	114
ユーザ プロファイルの変更	118
ユーザ プロファイルの削除	118
ユーザ リスト表示の変更	119
役割の設定	119
役割の作成	120
役割の変更	121
役割の削除	122
役割リスト表示の変更	123
アクセス セキュリティ コントロール	123
HTTPS 暗号化を強制的に使用	123
ファイアウォールの設定	124
ユーザ ログイン制御の設定	130
役割ベースのアクセス制御ルールの設定	134
SSL 証明書の設定	139
証明書署名リクエスト	140
自己署名された証明書の作成	142
既存のキーと証明書ファイルのインストール	144
キー ファイルと証明書ファイルのダウンロード	145

LDAP 認証の設定	146
LDAP 情報の収集	146
LDAP サーバ設定の追加	147
LDAP アクセス順序の並べ替え	150
LDAP サーバ接続のテスト	150
LDAP サーバ設定の編集	151
LDAP サーバ設定の削除	151
LDAP 認証の無効化	152
LDAP とローカル認証サービスの有効化	152
アウトレット (コンセント) 管理	153
アウトレット (コンセント) の名前付け	153
関連するサーキット ブレーカの確認	154
アウトレット (コンセント) 切り替え	155
コンセントのデフォルト状態の設定	158
電源再投入時の電源オフ時間の変更	160
初期化遅延の設定	162
突入電流防止遅延の設定	163
アウトレット (コンセント) の電源オン順序の設定	164
アウトレット (コンセント) 固有の電源オン遅延の設定	165
非臨界アウトレット (コンセント) と負荷遮断モードの設定	166
インレットとサーキット ブレーカの管理	169
インレットの名前付け	170
サーキット ブレーカの名前付け	170
インレットの監視	171
サーキット ブレーカの監視	172
電力しきい値の設定	173
インレットのしきい値の設定	173
サーキット ブレーカのしきい値の設定	175
サーキット ブレーカのしきい値の一括設定	176
アサート停止ヒステリシスとは	177
アサート タイムアウトとは	178
イベント ルールの設定	179
イベント ルールのコンポーネント	179
イベント ルールの作成	179
イベント ルールのサンプル	210
無限ループに関する注意	214
イベント ルールの変更	216
アクションの変更	217
イベント ルールまたはアクションの削除	217
トリガされないルールについての注意事項	218
イベント ログिंगの管理	218
ローカル イベント ログの表示	218
イベント エントリの消去	219
接続中のユーザの表示	220
サーバ アクセシビリティの監視	221
ping 監視対象の IT デバイスの追加	221

ping 監視設定の編集	222
ping 監視設定の削除	222
サーバ監視状態の確認	223
[Environmental Sensors (環境センサー)]	224
環境センサーの識別	224
環境センサーの管理	225
環境センサーの設定	227
センサー データの表示	230
環境センサーを管理対象から除外	234
資産管理	234
資産センサーの設定	235
資産センサーの LED 色の設定	236
特定のラック ユニットの設定	237
ブレード拡張ストリップの展開	238
資産センサー情報の表示	239
一括設定による設定のコピー	240
Dominion PX 設定の保存	241
Dominion PX の設定のコピー	242
測定単位の変更	242
Web カメラの画像またはビデオの管理	244
Web カメラの設定	244
画像またはビデオのプロパティの調整	245
Web カメラの画像またはビデオの表示	246
スナップショット ストレージ	249
ネットワーク診断	250
ホストへの ping	251
ネットワーク ルートの追跡	251
TCP 接続の一覧表示	252
通信ログの表示	252
診断情報のダウンロード	253
Schroff LHX ヒート エクスチェンジャの管理	254
LHX のサポートの有効化	254
LHX デバイスの設定	255
LHX デバイスの監視	257
LHX デバイスの制御	260
ファームウェアのアップグレード	261
Dominion PX ファームウェアの更新	261
ファームウェア更新履歴の表示	263
全面的な障害復旧	264
資産センサーのファームウェアの更新	264
ヘルプの使用	264
ソフトウェア パッケージの情報の取得	265
オンライン ヘルプの参照	265

SNMP の使用 267

SNMP の有効化	267
暗号化された SNMP v3 のユーザの設定	268
SNMP トラップの設定	269
SNMP の GET と SET	270
Dominion PX MIB	270
しきい値の有効化についての注意事項	273

コマンド ライン インタフェースの使用 274

インタフェースについて	274
CLI へのログイン	275
ハイパーターミナルの使用	275
SSH または Telnet の使用	276
さまざまな CLI モードとプロンプト	277
シリアル接続の終了	277
ヘルプ コマンド	277
情報の表示	278
ネットワーク設定	278
IP 設定	279
LAN インタフェース設定	279
ネットワーク モード	279
ワイヤレス設定	280
ネットワーク サービス設定	280
PDU 設定	281
アウトレット (コンセント) の情報	281
インレット情報	282
サーキット ブレーカ情報	283
日付と時刻の設定	284
環境センサー情報	284
インレット センサーしきい値情報	285
インレットの極センサーしきい値情報	286
サーキット ブレーカ センサーしきい値情報	287
環境センサーしきい値情報	288
セキュリティ設定	289
既存のユーザ プロファイル	289
既存の役割	290
負荷遮断設定	291
シリアル ポート設定	291
EnergyWise 設定	291
資産センサー設定	292
資産センサーのラック ユニット設定	293
ブレード拡張ストリップの設定	294

信頼性データ	294
信頼性エラー ログ	295
コマンド履歴	295
履歴バッファの長さ	295
例	295
Dominion PX デバイスとネットワークの設定	297
設定モードへの移行	297
PDU 設定コマンド	298
ネットワーク設定コマンド	308
時刻設定コマンド	334
セキュリティ設定コマンド	337
アウトレット (コンセント) 設定コマンド	359
インレット設定コマンド	361
サーキット ブレーカ設定コマンド	362
環境センサー設定コマンド	363
センサーしきい値設定コマンド	367
ユーザ設定コマンド	393
役割設定コマンド	405
EnergyWise 設定コマンド	410
資産管理コマンド	412
シリアル ポート設定コマンド	420
履歴バッファの長さの設定	421
マルチコマンド構文	422
設定モードの終了	423
負荷遮断設定コマンド	423
負荷遮断の有効化または無効化	424
電源制御操作	425
アウトレット (コンセント) の電源オン	425
アウトレット (コンセント) の電源オフ	427
アウトレット (コンセント) の電源の再投入	428
ユーザのブロック解除	429
Dominion PX のリセット	430
PDU の再起動	430
工場出荷時設定へのリセット	430
ネットワークのトラブルシューティング	431
診断モードへの移行	431
診断コマンド	431
診断モードの終了	434

コマンドで利用できるパラメータの確認	435
前のコマンドの取得	435
コマンドの自動補完	435
CLI のログアウト	436
仕様	437
電源測定精度	437
最高動作周囲温度	437
シリアル RS-232 ポートのピン配列	437
センサー RJ-12 ポートのピン配列	438
装置の設定ワークシート	439
工場出荷時設定へのリセット	443
リセット (RESET) ボタンの使用	443
CLI コマンドの使用	444
LDAP 設定の例	446
手順 A. ユーザ アカウントとグループの決定	446
手順 B. AD サーバでのユーザ グループの設定	447
手順 C. Dominion PX デバイスでの LDAP 認証の設定	448
手順 D. Dominion PX デバイスでのユーザ グループの設定	451
統合	455
Power IQ の設定	455
Power IQ の管理への PDU の追加	455
Dominion KX II 設定	457
ラック PDU (電源タップ) ターゲットの設定	457
RF Code エネルギー監視ソリューション	463
Dominion PX の追加情報	464
MAC アドレス	464
アウトレット (コンセント) とコードのロック	464
SecureLock™ アウトレット (コンセント) およびコード	465
ボタンタイプのロック アウトレット (コンセント)	467

目次

高度補正率	467
BTU 計算のデータ	468
CLI コマンドの適用可能性	468
Show コマンド	468
設定コマンド	470
その他のコマンド	471
Web インタフェースでのデータの切り捨て	472

索引	473

対象モデル

このユーザ ガイドは、PX-1000 シリーズおよび PX-2000 シリーズのモデルで、モデル名が PX2-1nnn または PX2-2nnn という形式のモデルを対象としています。n は数値です。

注: PX2-3nnn、PX2-4nnn、および PX2-5nnn シリーズについては、PX2-3000/4000/5000 シリーズのユーザ ガイドまたはオンライン ヘルプを参照してください。

『Dominion PX ユーザ ガイド』における最新情報

『Dominion PX ユーザ ガイド』では、装置やユーザ マニュアルの拡張および変更に基づいて、次のセクションが変更されたり、情報が追加されたりしました。

USB-to-Serial ドライバのインストール 『23p. 』

ブレード拡張ストリップの接続 『47p. 』

AMS-M2-Z 資産センサーの接続 (オプション) 『50p. 』

Schroff LHX ヒート エクスチェンジャの接続 (オプション) 『53p. 』

ヒューズ 『65p. 』

Modbus 設定の変更 『102p. 』

サービス アドバタイズメントの有効化 『103p. 』

拡張ポートの設定 『107p. 』

シリアル ポートの設定 『108p. 』

ファイアウォールの設定 『124p. 』

役割ベースのアクセス制御ルールの設定 『134p. 』

サーキット ブレーカのしきい値の一括設定 『176p. 』

イベント ルールの設定 『179p. 』

特定のラック ユニットの設定 『237p. 』

ブレード拡張ストリップの展開 『238p. 』

Web カメラの画像またはビデオの管理 『244p. 』

Schroff LHX ヒート エクスチェンジャの管理 『254p. 』

情報の表示 『278p. 』

PDU 設定コマンド 『298p. 』

時刻設定コマンド 『334p. 』

セキュリティ設定コマンド 『337p. 』

資産管理コマンド 『412p. 』

シリアル ポート設定コマンド 『420p. 』

Dominion KX II 設定 『457p. 』

Dominion PX の追加情報 『464p. 』

Web インタフェースでのデータの切り捨て 『472p. 』

このバージョンの *Dominion PX* に適用される変更の詳細については、リリース ノートを参照してください。

Dominion PX は、インテリジェント PDU (電源タップ) です。リモート サーバおよびその他のネットワーク デバイスのリブートや、データ センターの電源の監視を実行できます。

Raritan Dominion PX は、サーバ ルームのラックに設置されているようなコンピュータや通信機器などの IT 機器に電力を供給することを目的とした製品です。

Raritan 社は、さまざまなタイプの PDU を提供しています。たとえば、アウトレット (コンセント) 切り替え対応製品や非対応製品などがあります。アウトレット (コンセント) 切り替え機能があると、システム障害またはシステムのフリーズが発生した場合にシステムをリモートで回復できるので、手動での対応および現地への保守要員の派遣が不要になり、ダウンタイムと平均修復時間の短縮と生産性の向上につながります。

この章の内容

製品モデル	1
製品の機能	1
パッケージの内容	3

製品モデル

Dominion PX には、何種類かのストック モデルがあります。Raritan 社は、受注生産のカスタム モデルも提供しており、注文後に入手できます。

入手可能なモデルのリストについては、Raritan Web サイトの **製品セレクト** ページ『<http://www.raritan.com/resources/px-product-selector>/参照』を参照するか、最寄りのリセラーにお問い合わせください。

製品の機能

Dominion PX には、さまざまなサイズと機能のモデルがあります。通常、Dominion PX には以下の機能が備わっています。

- 切り替え機能があるユニットで、各アウトレット (コンセント) に接続されているデバイスの電源をオン/オフおよび再投入する機能
- インレット レベルで次の項目を監視する機能:
 - ラインあたりの RMS 電流 (A)
 - ライン ペアあたりの RMS 電圧 (V)
 - 有効電力 (W)
 - 皮相電力 (VA)
 - 力率

- 電力量 (Wh)
 - 不平衡負荷 (%)
- サークット ブレーカ レベルで次の項目を監視する機能:
 - ステータス (閉/開)
 - 消費電流 (A)
 - 残留電流 (A)
- 外部温度および湿度などの環境要素を監視する機能
- 環境センサーに対するユーザ指定の場所の属性
- 電流過負荷を知らせるための警報音の鳴るアラーム (ブザー)
- 設定可能なアラームのしきい値およびヒステリシス
- しきい値の設定可能なアサート タイムアウト
- 接続された資産センサーを使用して、ラック上の IT デバイスの場所をリモートで追跡できる機能
- 接続されている UPS がバッテリー駆動モードに移行したときに、「非臨界」アウトレット (コンセント) をオフにし、「臨界」アウトレット (コンセント) をオンのままにする機能 (この機能は、PX-2000 シリーズではサポートされていますが、PX-1000 シリーズではサポートされていません)
- SNMP v1、v2、v3 のサポート
- SNMP プロトコルを使用してトラップを送信する機能
- すべてのセンサー測定値のデータ ログを保存し、SNMP 経由で取得できる機能

注: Raritan の Power IQ またはその他の外部システムで、Dominion PX から、保存されたデータ (サンプル) を取得できます。

- SNMP を使用して、電力しきい値レベルなどの値を設定する機能
- 1 つのデバイスの設定を保存して、それを他の Dominion PX デバイスに展開する機能
- LED 表示の向きの調整のサポート
- SSH および Telnet サービスのサポート
- SSH の場合、パスワード認証と公開キー認証の両方をサポート
- IPv4 ネットワークと IPv6 ネットワークの両方のサポート
- Baytech BSNMP のサポート
- ゼロ構成サービス アドバタイズメントのサポート
- Raritan が提供するワイヤレス USB LAN アダプタを使用したワイヤレス接続
- 接続された Logicool® QuickCam® Pro 9000 Web カメラによってデータ センターの環境を視覚的に監視する機能
- 指定した受信者に電子メールで送信される Web カメラ画像のサポート
- 指定した受信者に特定のイベントのカスタマイズ SMS メッセージを送信するための Cinterion® MC52i GSM モデムのサポート
- 接続された Schroff® LHX-20 または LHX-40 ヒート エクスチェンジャの監視機能
- Cisco EnergyWise のサポート
- RF Code エネルギー監視システムのサポート
- 接続されている装置を過負荷や短絡から保護するために、定格が 20A を超える製品に搭載されている分岐回路ブレーカまたはヒューズを使用したローカル過電流保護 (OCP)
- 特定のモデルでのアウトレット (コンセント) タイプの組み合わせ (たとえば、C13 アウトレット (コンセント) と C19 アウトレット (コンセント))
- 特定のモデルでのアウトレット (コンセント) 電圧 (120 ボルトと 208 ボルト) の組み合わせ
- 特定のモデルでの高電流デバイス (ブレード サーバなど) のサポート
- ホストに対する ping の実行や TCP 接続の一覧表示など、ネットワークを診断する機能
- ファームウェア アップグレードで致命的なエラーが発生した場合の全面的な障害復旧
- ユーザ証明書に応じて、温度を摂氏または華氏、高さをメートルまたはフィート、圧力をパスカルまたは psi で表示する機能

パッケージの内容

ここからは、製品パッケージに付属する装置およびその他の構成要素について説明します。

ゼロ U 製品

- Dominion PX デバイス
- ゼロ U のねじ、ブラケット、ボタン
- 両端が DB9 コネクタのヌル モデム ケーブル (Raritan 部品番号: 254-01-0006-00) (オプション)
- インレットのケーブル リテンション クリップ (一部のモデルのみ)
- アウトレット (コンセント) のケーブル リテンション クリップ (一部のモデルのみ)

1U 製品

- Dominion PX デバイス
- 1U のブラケット パックとねじ
- 両端が DB9 コネクタのヌル モデム ケーブル (Raritan 部品番号: 254-01-0006-00) (オプション)
- インレットのケーブル リテンション クリップ (一部のモデルのみ)

2U 製品

- Dominion PX デバイス
- 2U のブラケット パックとねじ
- 両端が DB9 コネクタのヌル モデム ケーブル (Raritan 部品番号: 254-01-0006-00) (オプション)
- インレットのケーブル リテンション クリップ (一部のモデルのみ)

Ch 2

PDU のラックマウント

この章では、Dominion PX デバイスをラックにマウントする方法を説明します。ゼロ U PX-1000 シリーズの PDU を装着するには、Raritan 社製の 2 つのボタンまたは L ブラケットを使用できます。

この章の内容

ラック マウント安全基準	5
サーキット ブレーカの向きの制限	6
L-ブラケットを使用したゼロ U モデルの装着	7
ボタン マウントを使用したゼロ U モデルの装着	9
かぎつめ足ブラケットを使用したゼロ U モデルの装着	11
背面の 2 つのボタンを使用したゼロ U モデルの装着	12
L-ブラケットとボタンを使用したゼロ U モデルの装着	14
1U モデルまたは 2U モデルの装着	15

ラック マウント安全基準

Raritan の製品をラック マウントする必要がある場合は、以下の点に注意してください。

- 閉め切ったラック環境内の温度は室温より高くなる場合があります。分電盤 (PDU) に指定された最高動作温度を超えないようにしてください。ユーザ ガイドの「仕様『437p.』」を参照してください。
- ラック内に十分な空気の流れがあることを確認してください。
- 装置をラックに装着する際は、機械的荷重が均一になるように注意してください。
- 装置を電源に接続する際は、回路に過剰な電流が流れないように注意してください。
- すべての装置を正しく接地してください。特に、分岐回路に接続する場合など、電源への接続には注目してください。

サーキット ブレーカの向きの制限

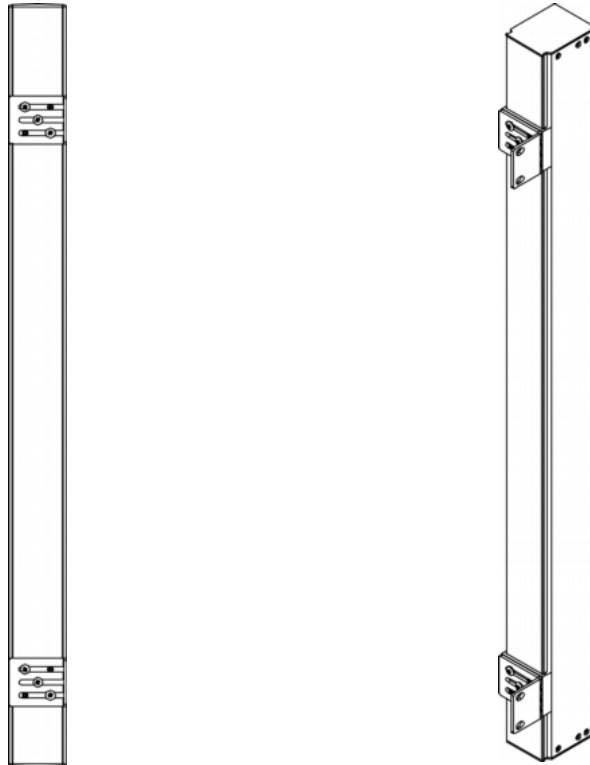
通常、PDU はどの向きでも装着できます。ただし、サーキット ブレーカ付きの PDU を装着する場合は、次のルールに従う必要があります。

- サーキット ブレーカを下向きにすることはできません。たとえば、サーキット ブレーカ付きのゼロ U PDU を天井に水平に装着しないでください。
- ボートや飛行機などの環境でラックが衝撃を受ける場合は、PDU を上下を逆にして装着することはできません。上下を逆にして装着すると、衝撃応力によりトリップ点が 10% 下がります。

注: 通常の状態では電源コードが下向きの場合、上下を逆にすると電源コードが上向きになります。

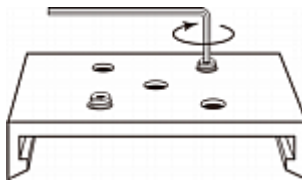
L-ブラケットを使用したゼロ U モデルの装着

PDU にサーキット ブレーカが実装されている場合は、マウントする前に「**サーキット ブレーカの向きの制限**『6p.』」をお読みください。



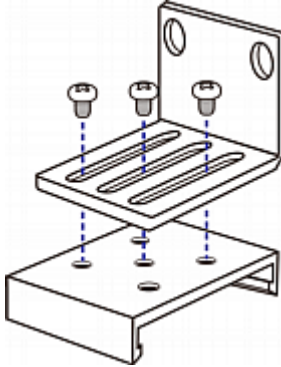
▶ **L-ブラケットを使用してゼロ U モデルを装着するには、次の手順に従います。**

1. Dominion PX デバイスの背面にベースプレートを合わせます。
2. ベースプレートを所定の位置に固定します。付属の L 型六角レンチを使用して、ベースプレートが軽く固定されるまで六角穴付きねじを緩めます。



3. ベースプレートの 5 つのねじ穴と L-ブラケットのスロットが合うように、L-ブラケットとベースプレートの位置を合わせます。ラック マウント側のブラケットは、Dominion PX デバイスの左側または右側に面している必要があります。

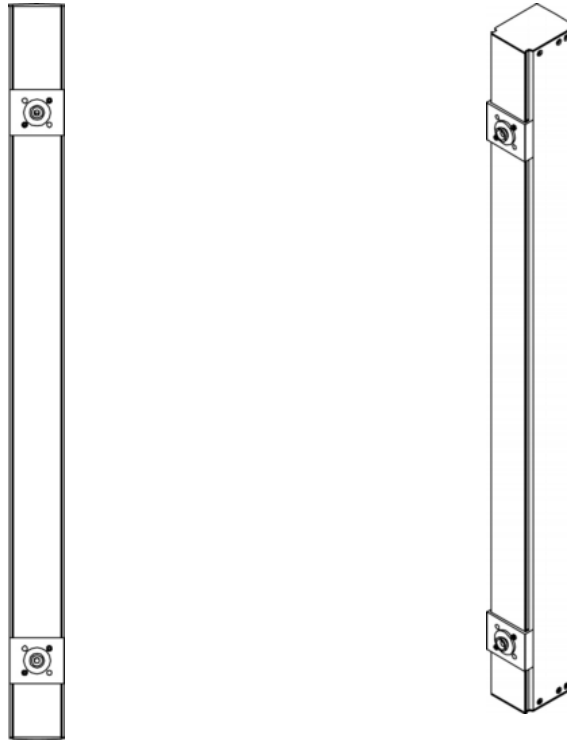
4. ブラケットを少なくとも 3 つのネジ（各スロットに 1 つ）で適切な位置に固定します。必要に応じて残りのネジも使用します。



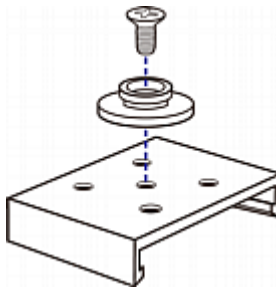
5. ラックのねじを使用して、Dominion PX デバイスを L-ブラケットを通してラックに固定します。

ボタン マウントを使用したゼロ U モデルの装着

PDU にサーキット ブレーカが実装されている場合は、マウントする前に「**サーキット ブレーカの向きの制限**『6p.』」をお読みください。



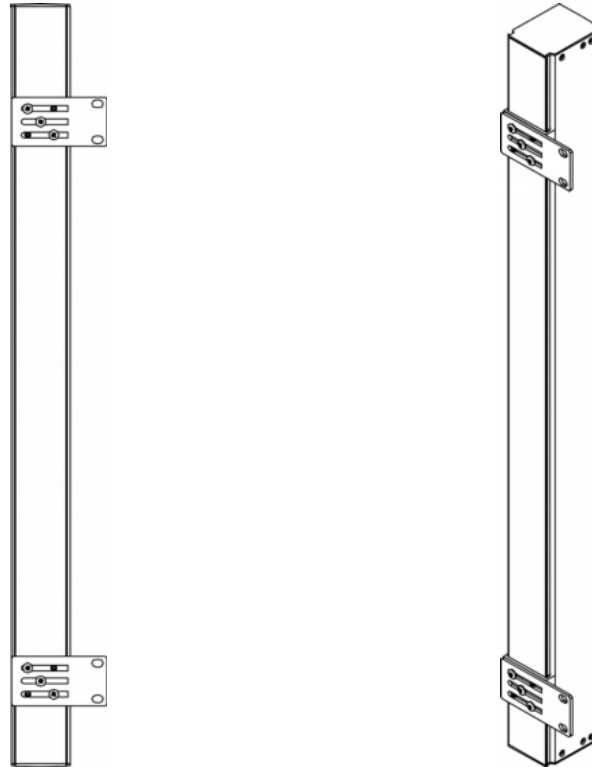
- ▶ ボタン マウントを使用してゼロ U モデルを装着するには、次の手順に従います。
- 1. Dominion PX デバイスの背面にベースプレートを合わせます。安定させるために、ボタンの間隔を 60cm 以上にしてください。
- 2. ベースプレートに Dominion PX デバイスを軽く留めます。付属の L 型六角レンチを使用して、ベースプレートが軽く固定されるまで六角穴付きねじを緩めます。
- 3. 各マウント ボタンを各ベースプレートの中央でねじ留めします。ボタンの推奨トルクは 1.96 N・m (20 kgf・cm) です。



4. 大きいマウント ボタンをキャビネットのマウント穴に合わせ、一方を固定し、もう一方を調整します。
5. マウント ボタンがその位置で固定されるまで、六角穴付きねじを緩めます。
6. 両方のボタンは、マウント穴に同時にはまるようにします。
7. Dominion PX デバイスを前に押し、マウント穴にマウント ボタンを押し込み、デバイスが約 1.6 cm 下がるようにします。これにより、Dominion PX デバイスが所定の位置に固定され、設置が完了します。

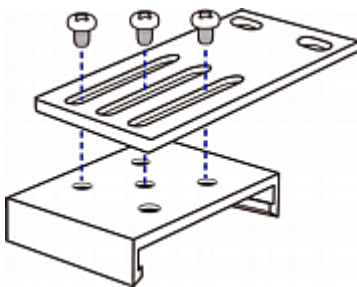
かぎつめ足ブラケットを使用したゼロ U モデルの装着

PDU にサーキット ブレーカが実装されている場合は、マウントする前に「**サーキット ブレーカの向きの制限**『6p.』」をお読みください。



▶ **かぎつめ足ブラケットを使用してゼロ U モデルを装着するには、次の手順に従います。**

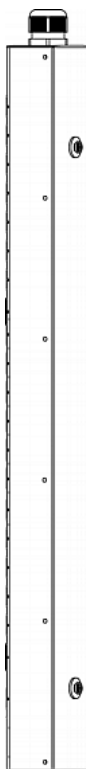
1. Dominion PX デバイスの背面にベースプレートを合わせます。
2. ベースプレートを所定の位置に固定します。付属の L 型六角レンチを使用して、ベースプレートが軽く固定されるまで六角穴付きねじを緩めます。
3. ベースプレートの 5 つのねじ穴とかぎつめ足ブラケットのスロットが合うように、かぎつめ足ブラケットとベースプレートの位置を合わせます。ラック マウント側のブラケットは、Dominion PX デバイスの左側または右側に面している必要があります。
4. ブラケットを少なくとも 3 つのネジ (各スロットに 1 つ) で適切な位置に固定します。必要に応じて残りのネジも使用します。



5. ラックのねじを使用して、Dominion PX デバイスをかぎつめ足ブラケットを通してラックに固定します。

背面の 2 つのボタンを使用したゼロ U モデルの装着

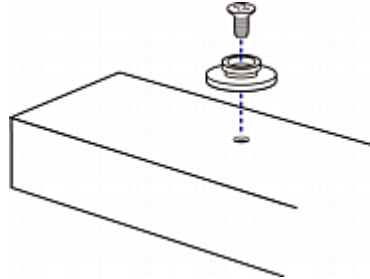
次に、2 つのボタンだけを使用して PDU を装着する方法について説明します。PDU にサーキット ブレーカが実装されている場合は、マウントする前に「サーキット ブレーカの向きの制限『6p.』」をお読みください。



- ▶ 2 つのボタンを使用してゼロ U モデルを装着するには、次の手順に従います。

1. PDU の背面パネルを前に向けます。

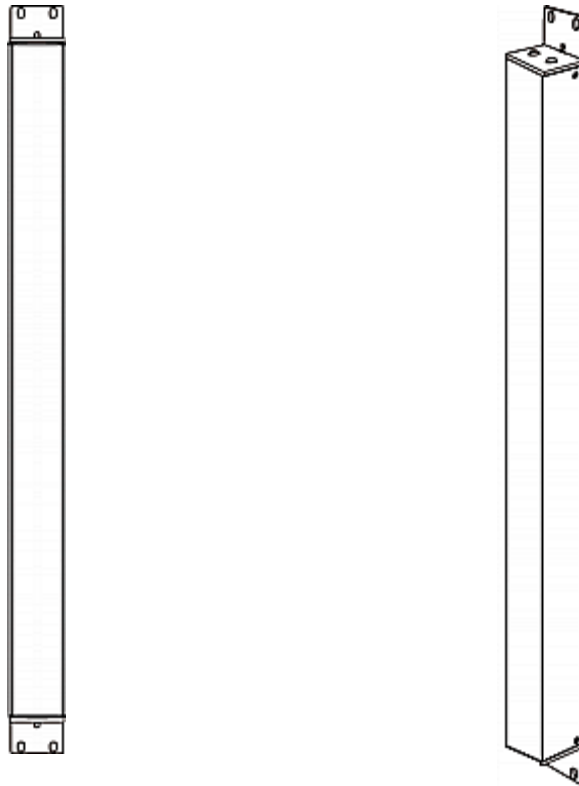
2. 背面パネルの 2 つのねじ穴を探します。1 つは一番下付近にあり、もう 1 つは一番上付近 (ケーブル グランドの側) にあります。
3. 一番下付近のねじ穴にボタンをねじ留めします。ボタンの推奨トルクは $1.96 \text{ N}\cdot\text{m}$ ($20 \text{ kgf}\cdot\text{cm}$) です。



4. 一番上付近のねじ穴にボタンをねじ留めします。ボタンの推奨トルクは $1.96 \text{ N}\cdot\text{m}$ ($20 \text{ kgf}\cdot\text{cm}$) です。
5. 2 つのボタンがラックまたはキャビネットのマウント穴に同時にはまることを確認します。
6. Dominion PX デバイスを前に押し、マウント穴にマウント ボタンを押し込み、デバイスがわずかに下がるようにします。これにより、Dominion PX デバイスが所定の位置に固定され、設置が完了します。

L-ブラケットとボタンを使用したゼロ U モデルの装着

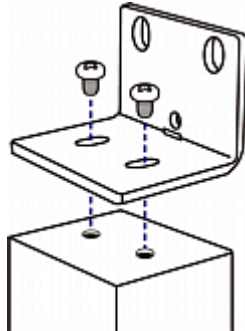
このセクションでは、L-ブラケットと 2 つのボタンを使用して PDU を装着する方法について説明します。PDU にサーキット ブレーカが実装されている場合は、マウントする前に「**サーキット ブレーカの向き**の制限『6p. 』」をお読みください。



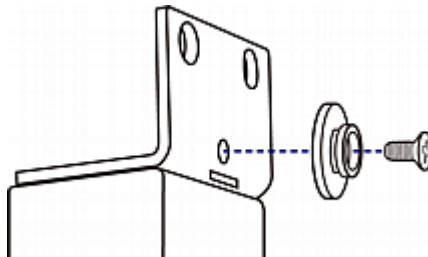
▶ **L-ブラケットと 2 つのボタンを使用してゼロ U モデルを装着するには、次の手順に従います。**

1. L-ブラケットの中央の 2 つの穴と Dominion PX デバイスの 2 つのねじ穴を合わせます。

2. L-ブラケットをデバイスにねじ留めし、ブラケットがしっかり固定されていることを確認します。



3. 手順 1 と 2 を繰り返して、もう 1 つの L-ブラケットをデバイスの下部にねじ留めします。
4. 両方の L-ブラケットをデバイスに取り付けたら、次のいずれかの方法でデバイスをラックに装着できます。
 - ラックねじを使用して、各 L-ブラケットの端付近にある 2 つの同じ穴を通してデバイスをラックに固定します。
 - 各 L-ブラケットの背面中央にマウント ボタンをねじ留めし、両方のボタンをラックのマウント穴にはめ込んで、デバイスを装着します。 ボタンの推奨トルクは 1.96 N・m (20 kgfcm) です。



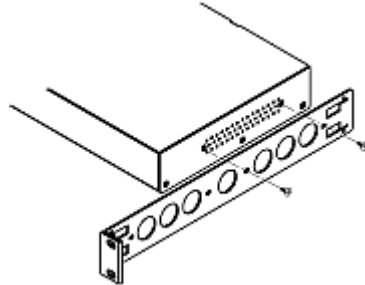
1U モデルまたは 2U モデルの装着

適切なブラケットと工具を使用して、1U または 2U の Dominion PX デバイスをラックまたはキャビネットに固定します。PDU にサーキット ブレーカが実装されている場合は、マウントする前に「**サーキット ブレーカの向きの制限**『6p.』」をお読みください。

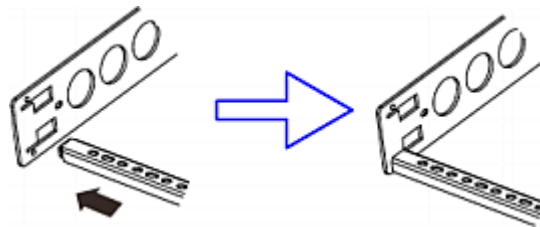
▶ Dominion PX デバイスを装着するには、次の手順に従います。

1. ラック マウント ブラケットを Dominion PX デバイスの側面に取り付けます。
 - a. ラック マウント ブラケットの 2 つの楕円形の穴と Dominion PX デバイスの側面にある 2 つのねじ穴を合わせます。
 - b. ラック マウント ブラケットを Raritan が提供する 2 つのねじで固定します。

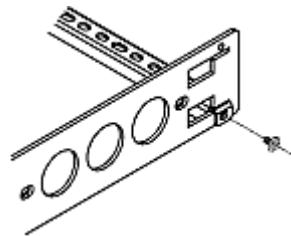
注: ラック マウント ブラケットの楕円形の穴の適切な場所は、モデルのねじ穴によって異なる場合があります。



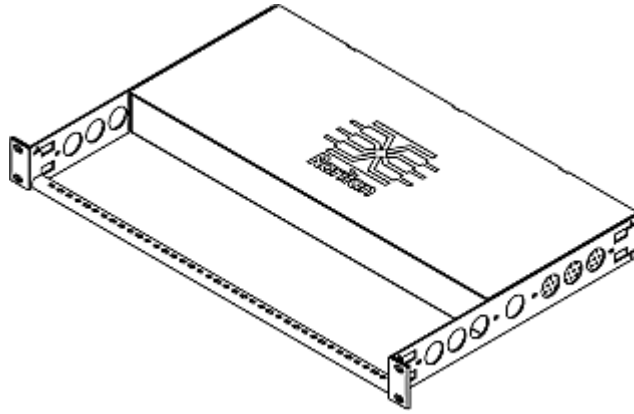
2. 手順 1 を繰り返して、もう一方のラック マウント ブラケットを Dominion PX のもう一方の側面に固定します。
3. ケーブル サポート バーの一方の端をラック マウント ブラケットの L 型の穴に挿入し、バーの端にある穴を L 型の穴の横にあるねじ穴に合わせます。



4. ケーブル サポート バーを Raritan が提供するキャップねじで固定します。



5. 手順 3 ~ 4 を繰り返して、ケーブル サポート バーのもう一方の端をもう一方のラック マウント ブラケットに固定します。



手持ちのねじ、ボルト、ケージ ナットなどでラック マウント ブラケットの耳をラックの前面のレールに固定して、ラックに Dominion PX デバイスを装着します。

Ch 3

設置と設定

この章では、Dominion PX デバイスを設置し、ネットワーク接続を設定する方法について説明します。

この章の内容

設置前の確認点	18
インレットへのケーブル リテンション クリップの取り付け (任意) ...	20
電源への PDU の接続	21
Dominion PX の設定	21
USB による PDU のカスケード接続	33
アウトレット (コンセント) へのケーブル リテンション クリップの取り付け (任意).....	36
環境センサーの接続 (オプション)	37
資産管理センサーの接続 (オプション).....	42
Logicool Web カメラの接続 (オプション).....	52
GSM モデムの接続 (オプション).....	52
Schroff LHX ヒート エクスチェンジャの接続 (オプション).....	53

設置前の確認点

設置する前に、以下の作業を実施してください。

- 製品およびコンポーネントのパッケージを開梱する
- 設置場所を準備する
- 装置の設定ワークシートに記入する
- 分岐回路の定格を確認する

製品およびコンポーネントのパッケージの開梱

1. 梱包箱から Dominion PX デバイスおよびその他の装置を取り出します。梱包されているすべての装置の一覧については、「**パッケージの内容**『3p. 』」を参照してください。
2. 装置のシリアル番号を箱の外側にある梱包明細に記載されている番号と比較し、一致していることを確認します。
3. 装置を慎重に点検します。破損または不足している装置がある場合は、Raritan テクニカル サポート部門に連絡してください。
4. Dominion PX デバイスのすべてのサーキット ブレーカがオンになっていることを確認します。オンになっていない場合は、該当するサーキット ブレーカをオンにします。

ヒューズのある PDU の場合、すべてのヒューズが正しく挿入され、配置されていることを確認します。ヒューズ カバーがある場合は、カバーが閉じていることを確認します。

注: すべての *Dominion PX* デバイスが、過電流保護機構を備えているわけではありません。

設置場所の準備

1. 設置場所が清潔で、適切な温度と湿度の範囲であることを確認します。

注: 使用するモデルの最高動作温度については、必要に応じて *Raritan* テクニカル サポートにお問い合わせください。「**最高動作周囲温度** 『437p. 』」を参照してください。

2. *Dominion PX* デバイスの周囲にケーブルとアウトレット（コンセント）の接続のための十分なスペースを確保します。
3. このユーザ ガイドの冒頭に記載されている「**安全の指針** 『ivp. 』」を確認してください。

装置の設定ワークシートの記入

装置の設定ワークシートは、このガイドに用意されています。「**装置の設定ワークシート** 『439p. 』」を参照してください。このワークシートを使用して、PDU に接続する各 IT デバイスのモデル、シリアル番号、および用途を記録します。

デバイスを追加または削除するたびに、ワークシートを更新します。

分岐回路の定格の確認

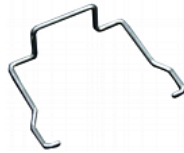
このセクションでは、PDU に電力を供給する分岐回路の定格について説明します。

- 分岐回路の定格は、国や地域の電気工事規定に従う必要があります。
- 北米の場合、分岐回路の定格は、PDU の定格より最大 125% 大きくなる可能性があります。ただし、国や地域の電気工事規定で禁じられている場合は除きます。
 - 入力電流の定格が 16A の PDU の場合は 20A
 - 入力電流の定格が 24A の PDU の場合は 30A
 - 入力電流の定格が 32A の PDU の場合は 40A
 - 入力電流の定格が 35A の PDU の場合は 50A
 - 入力電流の定格が 40A の PDU の場合は 50A
 - 入力電流の定格が 45A の PDU の場合は 60A
- 北米では、外部の過電流プロテクタは UL/CSA (または同等の認定規格) によって認定されている必要があります。その他の国または地域では、過電流プロテクタが国や地域の電気工事規定に準拠していることを確認してください。

インレットへのケーブル リテンション クリップの取り付け (任意)

ケーブル リテンション クリップを使用するように Dominion PX デバイスが設計されている場合は、クリップを取り付けてから電源コードを接続します。ケーブル リテンション クリップは、接続された電源コードの緩みや垂れ下がりを防ぎます。

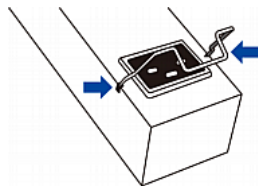
地震活動が活発な地域、または衝撃や振動が予想される環境では、ケーブル リテンション クリップの使用を強くお勧めします。



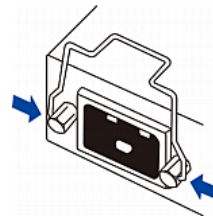
▶ ケーブル リテンション クリップをインレットに取り付けて使用するには、次の手順に従います。

1. インレット付近の 2 つの小さい穴を探します。
2. この小さい穴にクリップの両端を差し込んでケーブル リテンション クリップを取り付けます。

ゼロ U モデル

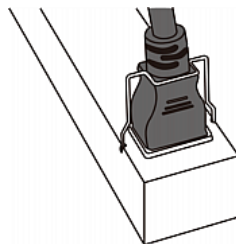


1U/2U モデル

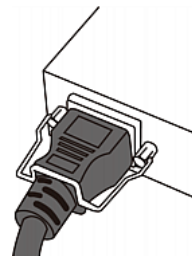


3. 電源コードをインレットに接続し、電源コードがしっかり固定されるように電源コードに向かってクリップを押します。

ゼロ U モデル



1U/2U モデル



電源への PDU の接続

1. Dominion PX デバイスのすべてのサーキット ブレーカがオンになっていることを確認します。オンになっていない場合は、該当するサーキット ブレーカをオンにします。

ヒューズのある PDU の場合、すべてのヒューズが正しく挿入され、配置されていることを確認します。ヒューズ カバーがある場合は、カバーが閉じていることを確認します。

注: すべての Dominion PX デバイスが、過電流保護機構を備えているわけではありません。

2. 各 Dominion PX デバイスを適切な定格の分岐回路に接続します。適切な入力定格または定格の範囲については、Dominion PX デバイ스에 貼られているラベルまたはネームプレートを参照してください。

注: Dominion PX デバイスの電源がオンになると、しばらくの間はパワーオン セルフテストとソフトウェアのロードが実行されます。このとき、アウトレット (コンセント) の LED がさまざまな色に切り替わります。

注: アウトレット (コンセント) の LED は、アウトレット (コンセント) 切り替え対応 PDU でのみ利用できます。

3. ソフトウェアのロードが完了すると、アウトレット (コンセント) の LED が一定の色になり、LED 表示が点灯します。

Dominion PX の設定

Dominion PX デバイスの初期設定には 2 つの方法があります。

- Dominion PX デバイスを設定するには、シリアル接続または USB 接続で Dominion PX デバイスとコンピュータを接続します。

コンピュータには、ハイパーターミナルまたは PuTTY などの通信プログラムが必要です。

シリアル接続の場合、両端が DB9 コネクタのヌル モデム ケーブルが必要です (Raritan 部品番号: 254-01-0006-00)。

- Dominion PX デバイスを、DHCP がサポートされている TCP/IP ネットワークに接続します。

DHCP によって割り当てられた IP アドレスは、Dominion PX の MAC アドレスを介して取得できます。サポートについては、LAN 管理者にお問い合わせください。「**MAC アドレス**『464p.』」を参照してください。

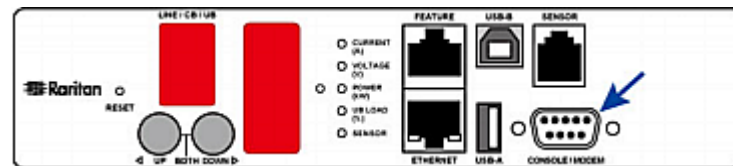
有線ネットワーク接続にはカテゴリ 5e/6 UTP ケーブルが必要です。

コンピュータへの Dominion PX の接続

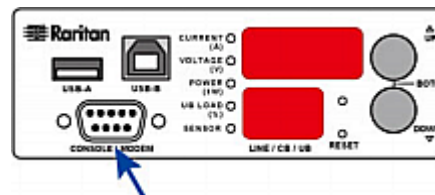
コンピュータを使用して Dominion PX を設定するには、RS-232 シリアル インタフェースで Dominion PX をコンピュータに接続する必要があります。

次の図は、さまざまなタイプの PDU 上にあるシリアル ポートの場所を示しています。

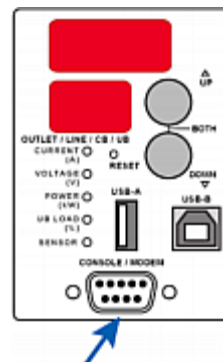
ゼロ U モデル:



1U モデル:



2U モデル:



コンピュータにシリアル ポートがない場合は、初期設定のために通常の USB ケーブルを使用して Dominion PX をコンピュータに接続します。Dominion PX デバイスは、USB-to-serial ドライバが Windows® オペレーティング システムに適切にインストールされた後、USB-to-serial コンバータをエミュレートできます。

注: すべての serial-to-USB コンバータが Dominion PX デバイスで正しく動作するとは限らないので、このセクションではこれらのコンバータの使用についての説明は省きます。

初期設定のため、以下のいずれかの手順に従って Dominion PX をコンピュータに接続します。

▶ **シリアル接続を確立するには、次の手順に従います。**

1. ノル モデム ケーブルの片側を Dominion PX の CONSOLE / MODEM というラベルの RS-232 ポートに接続します。
2. ノル モデム ケーブルの反対側をコンピュータのシリアル ポート (COM) に接続します。

▶ **USB 接続を確立するには、次の手順に従います。**

1. 通常の USB ケーブルの一方の端を Dominion PX の USB-B ポートに接続します。
2. USB ケーブルの反対側をコンピュータの USB-A ポートに接続します。

注: シリアル接続を使用してコマンド ライン インタフェースにログインする場合は、設定を完了した後もケーブルを接続したままにします。

USB-to-Serial ドライバのインストール

Dominion PX は、USB 接続で USB-to-serial コンバータをエミュレートできます。Microsoft® Windows® オペレーティング システムには、“Dominion Serial Console” という名前の USB-to-serial ドライバが必要です。Raritan Web サイトの以下の URL から *dominion-serial.zip* ドライバ ファイルをダウンロードします。これには、*dominion-serial.inf* ファイルと *dominion-serial-setup.exe* ファイルが含まれています。

<http://www.raritan.com/support/dominion-px/2.2.0/dominion-px2-series-usb-serial-driver>

▶ **Windows® Vista および 7 でドライバをインストールするには、次の手順に従います。**

1. Dominion PX の USB ケーブルをコンピュータから外します。
2. *dominion-serial-setup.exe* を実行します。Dominion Serial Console Driver Setup Wizard (Dominion Serial Console ドライバ セットアップ ウィザード) が表示されます。
3. [Install (インストール)] をクリックして、ドライバをインストールします。
4. インストールが完了したら、[Finish (完了)] をクリックします。
5. Dominion PX の USB ケーブルをコンピュータに接続します。ドライバが自動的にインストールされます。

▶ **Windows® XP でドライバをインストールするには、次の手順に従います。**

1. Dominion PX の USB ケーブルをコンピュータから外します。

2. C:\Windows\ServicePackFiles\i386 に「usbser.sys」があるかどうかを確認します。ない場合は、Windows インストール CD ディスクから USB-to-serial ドライバの保存先と同じディレクトリにコピーします。
 - SP3 が含まれている CD ディスクでは、I386\SP3.CAB からコピーします。
 - SP 2 が含まれている CD ディスクでは、I386\SP2.CAB からコピーします。
 - SP が含まれている CD ディスクでは、I386\DRIVER.CAB からコピーします。
3. Dominion PX の USB ケーブルをコンピュータに接続します。
4. コンピュータで新しいデバイスが検出され、「新しハードウェアの検出ウィザード」ダイアログ ボックスが表示されます。このダイアログ ボックスが表示されない場合は、[コントロール パネル] > [システム] > [ハードウェア] > [デバイス マネージャ] をクリックし、[Dominion Serial Console] を右クリックし、[ドライバの更新] を選択します。
5. [一覧または特定の場所からインストールする] を選択し、ドライバの保存場所を指定します
6. 「usbser.sys」 ファイルを要求するメッセージが表示されたら、ファイルの場所を指定します。
7. インストールは完了です。

▶ **Linux の場合:**

追加のドライバは不要ですが、tty デバイスの名前を入力する必要があります。これは、Dominion PX をコンピュータに接続した後、「dmesg」を実行した結果に含まれています。通常、tty デバイスは「/dev/ttyACM#」または「/dev/ttyUSB#」です。# は整数です。

たとえば、kermit ターミナル プログラムを使用し、tty デバイスが「/dev/ttyACM0」の場合は、次のコマンドを実行します。

```
> set line /dev/ttyACM0  
> connect
```


ネットワークへの Dominion PX の接続

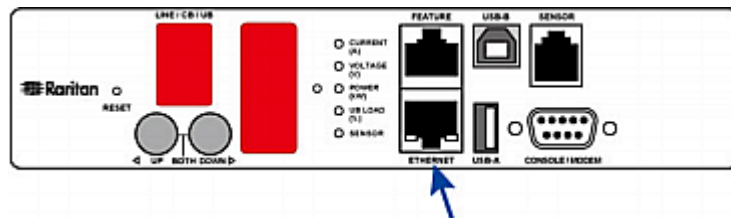
Web インタフェースを使用して Dominion PX を管理するには、Dominion PX をローカル エリア ネットワーク (LAN) に接続する必要があります。Dominion PX は、有線ネットワークまたはワイヤレス ネットワークに接続できます。

注: PDU にワイヤレス ネットワーク機能が実装されていない場合、または PDU が USB カスケード構成のマスタ デバイスとして使用される場合は、有線接続を確立します。

▶ 有線接続を確立するには、次の手順に従います。

1. 標準のカテゴリ 5e/6 UTP ケーブルを Dominion PX の Ethernet ポートに接続します。
2. ケーブルのもう一方の端を LAN に接続します。

ゼロ U モデルの ETHERNET ポートの場所については、次の図を参照してください。



1U/2U モデルの場合、Ethernet ポートは一部のモデルを除き通常は背面にあります。次の図は背面のポートを示しています。



2U モデルの場合、Ethernet ポートは前面にあります。次の図は 2U モデルのポートを示しています。

▶ ワイヤレス接続を確立するには、次の手順に従います。

次のいずれかを実行してください。

- 802.11n ワイヤレス USB LAN アダプタを Dominion PX 上の USB-A ポートに接続します。
- USB ドッキング ステーションを Dominion PX 上の USB-A ポートに接続し、802.11n ワイヤレス USB LAN アダプタをドッキング ステーション上の適切な USB ポートに接続します。

サポートされているワイヤレス LAN 設定

ワイヤレス接続を選択する場合は、ワイヤレス USB LAN アダプタとワイヤレス ネットワーク設定の両方が次の要件を満たしていることを確認します。

- ネットワーク タイプ: 802.11n
- プロトコル: WPA2 (RSN)
- キー管理: WPA-PSK
- 暗号化: CCMP (AES)

重要: 現在は **Raritan** が提供するワイヤレス **USB LAN** アダプタのみがサポートされています。この情報については、**Raritan** テクニカル サポートにお問い合わせください。

初期ネットワーク設定

Dominion PX デバイスをネットワークに接続した後は、IP アドレスおよびその他のネットワーク情報を指定する必要があります。

このセクションでは、シリアル接続または USB 接続を介した初期設定について説明します。

注: LAN を介して *Dominion PX* を設定する場合は、「Web インタフェースの使用 [69p.]」で Web インタフェースの使用方法を参照してください。

▶ **Dominion PX** デバイスを設定するには、次の手順に従います。

1. Dominion PX に接続したコンピュータで、ハイパーターミナルまたは PuTTY などの通信プログラムを開きます。
2. 適切な COM ポートを選択し、ポートが次のように設定されていることを確認します。
 - ビット/秒 = 115200 (115.2Kbps)
 - データ ビット = 8
 - ストップ ビット = 1
 - パリティ = なし
 - フロー制御 = なし

ヒント: USB 接続の場合、どの COM ポートが *Dominion PX* に割り当てられているかを調べるには、[コントロールパネル] > [システム] > [ハードウェア] > [デバイス マネージャ] を選択し、[ポート] グループの下で「*Dominion Serial Console*」を探します。

3. Enter キーを押します。

4. Dominion PX にログインするよう求めるプロンプトが表示されます。ユーザ名とパスワードは、いずれも大文字と小文字が区別されることに注意してください。
 - a. [Username (ユーザ名)] プロンプトで、「admin」と入力し、Enter キーを押します。
 - b. [Password (パスワード)] プロンプトで、「raritan」と入力し、Enter キーを押します。
5. Dominion PX に初めてログインする場合は、パスワードを変更するよう求められます。画面に表示される指示に従って、新しいパスワードを入力します。
6. 正常にログインすると、# プロンプトが表示されます。
7. 「config」と入力して、Enter キーを押します。
8. ネットワークを設定するには、適切なコマンドを入力し、Enter キーを押します。すべてのコマンドで大文字と小文字が区別されます。
 - a. ネットワーク モードを設定するには、次のコマンドを入力します。
`network mode <mode>`
 <mode> は、有線接続（デフォルト）の場合は *wired*、ワイヤレス接続の場合は *wireless* です。
 - b. 有線接続モードの場合、LAN インタフェース設定を指定できます。ほとんどの場合、デフォルトの設定である「auto」で正常に機能します。必要のない限り変更しないでください。

設定対象	使用するコマンド
LAN interface speed (LAN インタフェース速度)	<code>network interface LANInterfaceSpeed <option></code> <option> は、 <i>auto</i> 、 <i>10Mbps</i> 、または <i>100Mbps</i> です。
LAN interface duplex mode (LAN インタフェースデュプレックスモード)	<code>network interface LANInterfaceDuplexMode <mode></code> <mode> は、 <i>half</i> 、 <i>full</i> 、または <i>auto</i> です。

ヒント: 複数のコマンドを組み合わせることで複数のパラメータを一度に設定できます。たとえば、次のように設定します。

```
network interface LANInterfaceSpeed <option>
LANInterfaceDuplexMode <mode>
```

- c. ワイヤレス ネットワーク モードの場合、Service Set Identifier (SSID) パラメータを設定する必要があります。

設定対象	使用するコマンド
SSID	network wireless SSID <ssid> <ssid> は、SSID 文字列です。

必要な場合は、次の表に示す他のワイヤレス パラメータを設定します。

設定対象	使用するコマンド
BSSID	network wireless BSSID <bssid> <bssid> は、AP MAC アドレスです。
認証方法	network wireless authMethod <method> <method> は、事前共有キーの場合は <i>psk</i> 、拡張認証プロトコルの場合は <i>eap</i> です。
PSK (PSK)	network wireless PSK <psk> <psk> は、PSK 文字列です。
EAP 外部認証	network wireless eapOuterAuthentication <outer_auth> <outer_auth> は <i>PEAP</i> です。
EAP 内部認証	network wireless eapInnerAuthentication <inner_auth> <inner_auth> は <i>MSCHAPv2</i> です。
EAP ID	network wireless eapIdentity <identity> <identity> は EAP 認証のユーザ名です。

設定対象	使用するコマンド
EAP パスワード	network wireless eapPassword EAP 認証のパスワードを入力するプロンプトが表示されたら、パスワードを入力します。
EAP CA 証明書	network wireless eapCACertificate CA 証明書を入力するプロンプトが表示されたら、テキスト エディタで証明書を開き、その内容を通信プログラムにコピー アンド ペーストします。

注: CA 証明書からコピーする内容に、“BEGIN CERTIFICATE”が含まれる最初の行と“END CERTIFICATE”が含まれる最後の行を含めないでください。

- d. 有効にする IP プロトコルと DNS サーバから返された使用する IP アドレスを決定するには、次のパラメータを設定します。

設定対象	使用するコマンド
IP プロトコル	network ip proto <protocol> <protocol> は、IPv4 を有効にする場合は <i>v4Only</i> 、IPv6 を有効にする場合は <i>v6Only</i> 、IPv4 プロトコルと IPv6 プロトコルの両方を有効にする場合は <i>both</i> です。
DNS サーバから返された IP アドレス	network ip dnsResolverPreference <resolver> <resolver> は、IPv4 アドレスの場合は <i>preferV4</i> 、IPv6 アドレスの場合は <i>preferV6</i> です。

- e. 前の手順で IPv4 プロトコルを有効にした場合は、IPv4 ネットワーク パラメータを設定します。

設定対象	使用するコマンド
IP 設定方法	<pre>network ipv4 ipConfigurationMode <mode></pre> <mode> には、自動設定（デフォルト）の場合は <i>dhcp</i>、固定 IP アドレスを指定する場合は <i>static</i> を指定します。

- IPv4 DHCP 設定の場合は、次のパラメータを設定します。

設定対象	使用するコマンド
優先ホスト名 (オプション)	<pre>network ipv4 preferredHostName <name></pre> <name> は、優先ホスト名です。

ヒント: DHCP によって割り当てられた IPv4 DNS サーバを手動で指定したサーバで上書きするには、次のコマンドを入力します。

```
network ipv4 overrideDNS <option>
```

<option> は、*enable* または *disable* です。DNS サーバを手動で指定するための IPv4 コマンドについては、次の表を参照してください。

- 固定 IPv4 設定の場合は、次のパラメータを設定します。

設定対象	使用するコマンド
固定 IPv4 アドレス	<pre>network ipv4 ipAddress <ip address></pre> <ip address> は、割り当てる IP アドレスです。
サブネット マスク	<pre>network ipv4 subnetMask <netmask></pre> <netmask> は、サブネット マスクです。
ゲートウェイ	<pre>network ipv4 gateway <ip address></pre> <ip address> は、ゲートウェイの IP アドレスです。

設定対象	使用するコマンド
プライマリ DNS サーバ	<pre>network ipv4 primaryDNSServer <ip address></pre> <ip address> は、プライマリ DNS サーバの IP アドレスです。
セカンダリ DNS サーバ (オプション)	<pre>network ipv4 secondaryDNSServer <ip address></pre> <ip address> は、セカンダリ DNS サーバの IP アドレスです。

- f. 前の手順で IPv6 を有効にした場合は、IPv6 ネットワーク パラメータを設定します。

設定対象	使用するコマンド
IP 設定方法	<pre>network ipv6 ipConfigurationMode <mode></pre> <mode> には、自動設定 (デフォルト) の場合は <i>automatic</i>、固定 IP アドレスを指定する場合は <i>static</i> を指定します。

ヒント: DHCP によって割り当てられた IPv6 DNS サーバを手動で指定したサーバで上書きするには、次のコマンドを入力します。

```
network ipv6 overrideDNS <option>
```

<option> は、*enable* または *disable* です。DNS サーバを手動で指定するための IPv6 コマンドについては、次の表を参照してください。

- 固定 IPv6 設定の場合は、次のパラメータを設定する必要があります。IP アドレスは、IPv6 の形式に従っている必要があります。

設定対象	使用するコマンド
固定 IPv6 アドレス	network ipv6 ipAddress <ip address> <ip address> は、割り当てる IP アドレスです。
ゲートウェイ	network ipv6 gateway <ip address> <ip address> は、ゲートウェイの IP アドレスです。
プライマリ DNS サーバ	network ipv6 primaryDNSServer <ip address> <ip address> は、プライマリ DNS サーバの IP アドレスです。
セカンダリ DNS サーバ (オプション)	network ipv6 secondaryDNSServer <ip address> <ip address> は、セカンダリ DNS サーバの IP アドレスです。

9. 変更を保存するかどうかにかかわらず、設定モードを終了するには、次のいずれかのコマンドを入力し、Enter キーを押します。

コマンド	説明
apply	設定変更をすべて保存して、設定モードを終了します。
cancel	設定変更をすべて中止して、設定モードを終了します。

プロンプトが表示され、設定モードが終了したことがわかります。

10. すべて正しく設定されているかどうかを確認するには、次のコマンドを 1 つずつ入力します。現在のネットワーク設定が表示されます。

コマンド	説明
show network	ネットワーク パラメータが表示されます。

コマンド	説明
show network ip all	すべての IP 設定パラメータが表示されます。
show network wireless details	すべてのワイヤレス パラメータが表示されます (このコマンドは、ワイヤレス モードを有効にした場合にのみ実行します)。

ヒント: 「show network wireless」と入力すると、ワイヤレス設定の簡易表示版が表示されます。

11. すべて正しい場合は、「exit」と入力して Dominion PX からログアウトします。正しくない設定がある場合は、手順 7 ～ 10 を繰り返してネットワーク設定を変更します。

設定された IP アドレスが有効になるまでには、数秒かかる場合があります。

USB による PDU のカスケード接続

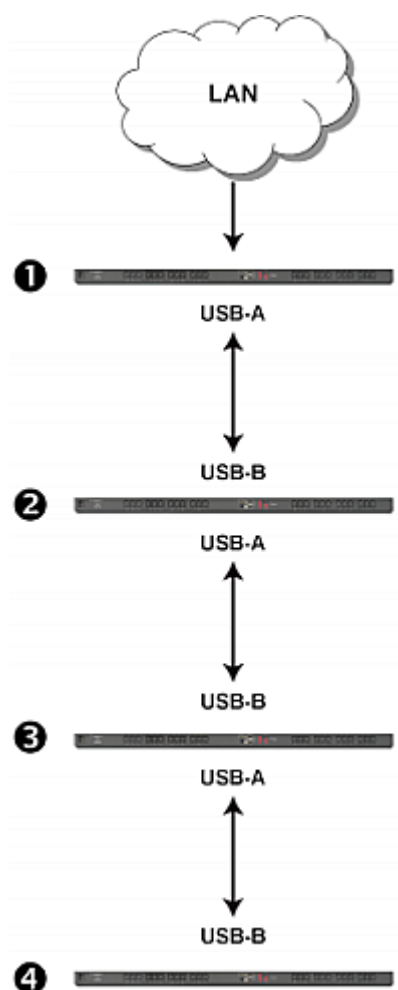
同一または異なるモデルの Dominion PX を最大 4 台まで、USB インタフェースを介してカスケード接続できます。1 台目のデバイスがマスタデバイスで、それに接続されるすべてのデバイスはスレーブ デバイスです。マスタ デバイスは、LAN とスレーブ デバイス間で IP パケットを転送するネットワーク ブリッジとして機能することで、その有線ネットワークをスレーブ デバイスと共有します。スレーブ デバイスには、Web、SNMP、SSH、または Telnet インタフェースを介してアクセスできます。USB カスケード構成は有線ネットワークのみに対応しているので、ご注意ください。

- マスタ デバイスは、「有線」Ethernet 接続に対応しています。
- スレーブ デバイスは有線 Ethernet 接続には対応していません。
スレーブ デバイスがネットワーク ケーブルで LAN に接続されている場合、その有線 Ethernet インタフェースは自動的に無効になります。
- デイジーチェーン内のデバイスで無線接続に対応するものではありません。

重要: モデル名が **PX2** で始まる **Dominion PX** デバイスのみ、**USB** カスケード接続機能をサポートしています。

▶ **Dominion PX デバイスをカスケード接続するには、次の手順に従います。**

1. Dominion PX デバイスのファームウェア バージョンが以下の要件を満たしていることを確認します。満たしていない場合は、そのデバイスをアップグレードします。「*Dominion PX ファームウェアの更新*『261p. 』」を参照してください。
 - Dominion PX: バージョン 2.3 以降
2. マスタ デバイスとして使用するデバイスを決定します。
 - マスタ デバイスは、標準 Category 5e/6 UTP ケーブルで LAN に接続する必要があります。
3. USB ケーブルでマスタ デバイスの USB-A ポートを別の Dominion PX デバイスの USB-B ポートに接続します。
 - マスタ デバイスに接続されるデバイスが、1 台目のスレーブ デバイスになります。
4. USB ケーブルで 1 台目のスレーブ デバイスの USB-A ポートを別の Dominion PX デバイスの USB-B ポートに接続します。
 - 1 台目のスレーブ デバイスに接続されるデバイスが、2 台目のスレーブ デバイスになります。
5. USB ケーブルで 2 台目のスレーブ デバイスの USB-A ポートを別の Dominion PX デバイスの USB-B ポートに接続します。
 - 2 台目のスレーブ デバイスに接続されるデバイスが、3 台目のスレーブ デバイスになります。



番号	デバイスの役割
①	マスタ デバイス
②	1 台目のスレーブ デバイス
③	2 台目のスレーブ デバイス
④	3 台目のスレーブ デバイス

注: マスタ デバイスでは、ネットワーク モードは「Wired (有線)」と表示されます。スレーブ デバイスでは、ネットワーク モードは「Wired(USB) (有線 (USB))」と表示されます。これは、USB カスケード接続で LAN に接続されていることを示します。「PDU 情報の表示 『89p. 』」を参照してください。

アウトレット (コンセント) へのケーブル リテンション クリップの取り付け (任意)

ケーブル リテンション クリップを使用するように Dominion PX デバイスが設計されている場合は、クリップを取り付けてから電源コードを接続します。ケーブル リテンション クリップは、接続された電源コードの緩みや垂れ下がりを防ぎます。

地震活動が活発な地域、または衝撃や振動が予想される環境では、ケーブル リテンション クリップの使用を強くお勧めします。

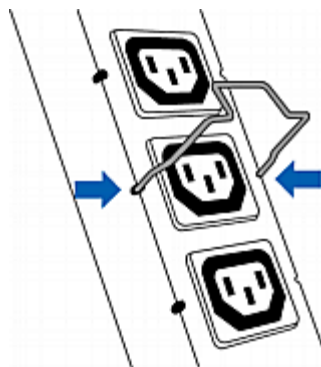
IT 機器で、C13 または C19 アウトレット (コンセント) に接続されて使用される電源コードにはさまざまなものがあります。これらに対応するため、オプションのクリップにもさまざまなサイズがあります。異なるサイズのクリップを含むケーブル リテンション キットは、リセラーに注文できます。(保守サービスのための) 取り付けまたは取り外しの操作がスムーズに運ぶように、電源コードにぴったりフィットするクリップを使用してください。



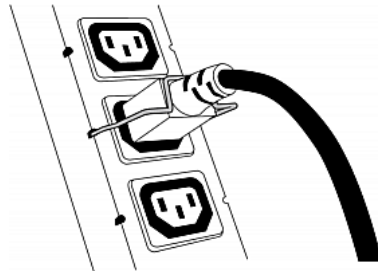
注: PSE 認定済みの日本向け PDU の NEMA ソケットにはロック機能が組み込まれているので、ケーブル リテンション クリップは不要です。

▶ **ケーブル リテンション クリップをアウトレット (コンセント) に取り付けて使用するには、次の手順に従います。**

1. アウトレット (コンセント) 付近の 2 つの小さい穴を探します。
2. この小さい穴にクリップの両端を差し込んでケーブル リテンション クリップを取り付けます。



3. 電源コードをアウトレット（コンセント）に接続し、電源コードがしっかり固定されるように電源コードに向かってクリップを押します。クリップは、逆「U」字のようにプラグを支える中央部分が床の方に下向きになっている必要があります。これにより、クリップが重力によって所定の位置に保たれます。



4. 同じ手順を繰り返して、クリップと電源コードを他のアウトレット（コンセント）に取り付けます。

ヒント: Raritan では、電源コードを所定の位置に固定するための仕組みを他にも用意しています。「アウトレット（コンセント）とコードのロック『464p.』」を参照してください。

環境センサーの接続 (オプション)

Dominion PX の周囲の環境要因の検出を有効にするには、1 つ以上の Raritan 環境センサーを Dominion PX デバイスに接続します。

製品のセンサー ポートに接続したすべてのセンサー ケーブルの最大距離は 30 メートル/100 フィート以内にする必要があります。ご質問がある場合は Raritan テクニカル サポートにお問い合わせください。

Raritan 製センサー ハブを使用すれば、Dominion PX に最大 16 台の環境センサーを接続できます。

Raritan 環境センサーには、通常、複数のセンサーが含まれています。たとえば、DPX-T2H2 と DPX-T3H1 は 4 個のセンサーとしてカウントされます。

警告: 正しく動作させるために、複数の環境センサーを接続または切断する際には、15 ～ 30 秒待ってから次の操作を行ってください。

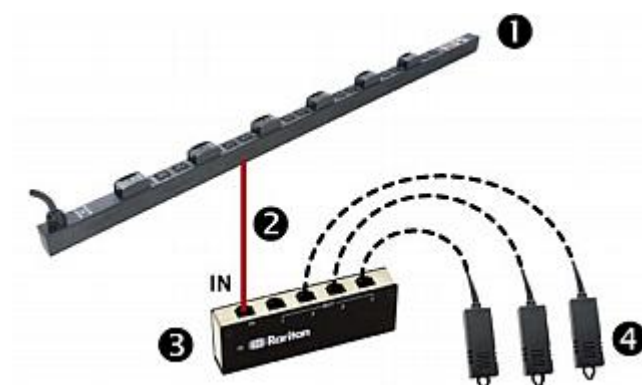
- ▶ **1 つまたは複数の環境センサーを直接接続するには、次の手順に従います。**
- 環境センサーのコネクタを Dominion PX デバイスの Sensor ポートに接続します。

注: 購入したモデルによって、Sensor ポートの合計数は異なります。

▶ オプションの PX センサー ハブを介して環境センサーを接続するには、次の手順に従います。

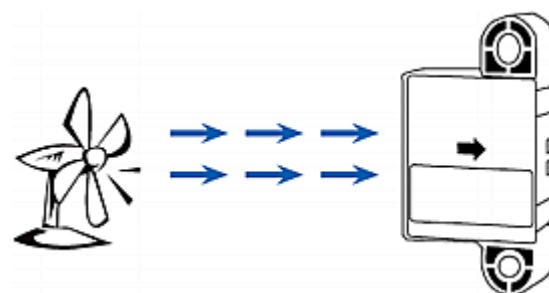
1. Raritan センサー ハブを Dominion PX デバイスに接続します。
 - a. Raritan が提供する電話ケーブル (4 芯、6 ピン、RJ-12) の片側をハブの入力ポート (ポート 1) に接続します。
 - b. もう一方の端を Dominion PX の SENSOR ポートに差し込みます。
2. Raritan 環境センサーをハブの 4 つの出力ポートのいずれかに接続します。

Raritan センサー ハブはカスケード接続できないので、Dominion PX デバイスの各 Sensor ポートに接続できるセンサー ハブは 1 台までです。次の図は、センサー ハブが接続された構成を示しています。



①	Dominion PX デバイス:
②	Raritan が提供する電話ケーブル
③	Raritan PX センサー ハブ
④	Raritan 環境センサー

3. Raritan エアフロー センサーが接続されている場合は、そのセンサーの矢印が示す正しい方向で、送風元 (ファンなど) に向いていることを確認します。



接点閉鎖センサーについて

Raritan の接点閉鎖センサー (DPX-CC2-TR) は、接続済みの検出装置/スイッチの開閉状態を検出できます。

この機能を正しく機能させるには、少なくとも 1 台のディスクリート (オン/オフ) 検出装置/スイッチを統合している必要があります。DPX-CC2-TR に接続できるディスクリート検出装置/スイッチのタイプには、以下を目的としたものがあります。

- 扉開閉検出
- 扉施錠検出
- 床面の水の検出
- 煙検出
- 振動検出

Raritan 製のディスクリート検出装置/スイッチはありません。これらはサードパーティ製プローブなので、Raritan の DPX-CC2-TR で適切に動作するかをテストして確認する必要があります。

重要: サードパーティ製の検出装置/スイッチの統合とテストはお客様単独の責任で行ってください。Raritan は、お客様がご用意して設置したサードパーティ製検出装置/スイッチの不適切な終了または障害 (付随的または派生的) の結果についての責任を負うことはできません。設置および設定手順の後の障害に対しては、誤ったアラームが通知されるか、アラームがまったく通知されない可能性があります。Raritan は、すべてのサードパーティ製検出装置/スイッチが **DPX-CC2-TR** で正しく機能することを表明または主張するものではありません。

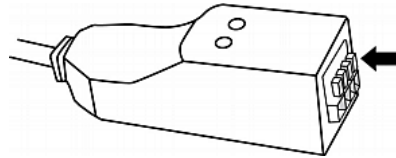
DPX-CC2-TR へのサードパーティ製検出装置/スイッチの接続

DPX-CC2-TR ユニットには、2 つのサードパーティ製検出装置/スイッチを接続するための 2 つのチャンネルが用意されています。DPX-CC2-TR の本体には、4 つのバネ荷重終端点があります。右側の 2 つは一方のチャンネル (LED 番号で示されている) に関連付けられ、左側の 2 つはもう一方のチャンネルに関連付けられています。これらの終端点にサードパーティ製検出装置/スイッチを接続する必要があります。

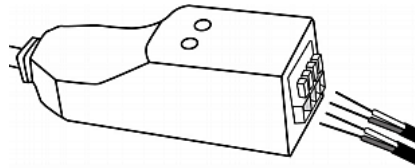
▶ サードパーティ製検出装置/スイッチを接続するには、次の手順に従います。

1. 2 つのサードパーティ製検出装置/スイッチの各線の端から約 12mm のところで絶縁を取り除きます。
2. DPX-CC2-TR 本体の終端点の上にある小さい四角形のボタンを押したままにします。

注: 各ボタンは、対応する各終端点のバネを制御します。



3. 各終端点に両方のサードパーティ製検出装置/スイッチの各線を完全に挿入します。
 - 検出装置/スイッチの両方の線を左側の 2 つの終端点に接続します。
 - 別の検出装置/スイッチの両方の線を右側の 2 つの終端点に接続します。



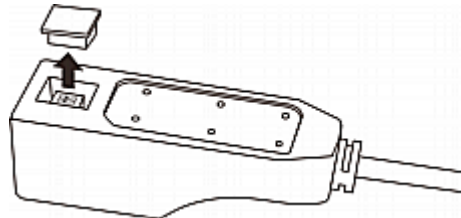
4. 線を正しく挿入したら、小さい四角形のボタンを放します。
5. これらの線がしっかり固定されていることを確認します。

接点閉鎖センサーの設定

DPX-CC2-TR を使用して接点閉鎖状態、水、煙、または振動を検出するには、まず、DPX-CC2-TR 本体の LED の状態を制御するディップスイッチを調整して正常状態を決定する必要があります。ディップスイッチは、チャンネルに関連付けられています。

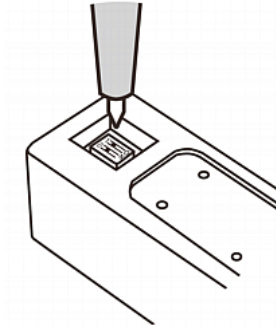
▶ ディップスイッチの設定を調整するには、次の手順に従います。

1. DPX-CC2-TR に接続された検出装置/スイッチを、特定の環境条件を検出する場所に配置します。
2. DPX-CC2-TR 本体のディップスイッチのカバーを取ります。



3. チャンネル 1 の正常状態を設定するには、1 というラベルのディップスイッチを探します。
4. 尖ったペン先などを使用して、スライドスイッチを「NO」(Normally Open (ノーマル オープン)) または「NC」(Normally Closed (ノーマル クローズ)) のラベルの側に移動します。

- Normally Open (ノーマル オープン): 接続されている検出装置/スイッチの開状態が正常と見なされます。
- Normally Closed (ノーマル クローズ): 接続されている検出装置/スイッチの閉状態が正常と見なされます。デフォルトではこの設定です。



5. チャンネル 2 の正常状態を設定するには、手順 4 を繰り返して他のディップ スイッチの設定を調整します。
6. ディップ スイッチのカバーを戻します。

注: ディップ スイッチは適切に設定する必要があります。不適切な場合は、センサーの LED が正常状態で誤って点灯する可能性があります。

接点閉鎖センサーの LED

DPX-CC2-TR には、接続された検出装置/スイッチの状態を表示するための LED があります。

LED は、関連付けられている検出装置/スイッチが「異常」状態（正常状態の逆）になったときに点灯します。正常状態の設定方法については、「**接点閉鎖センサーの設定**『40p.』」を参照してください。

点灯している LED の意味は、正常状態の設定に応じて異なります。

- 正常状態が閉に設定されている場合:

LED	センサーの状態
点灯していない	閉
点灯している	開

- 正常状態が開に設定されている場合:

LED	センサーの状態
点灯していない	開
点灯している	閉

LED	センサーの状態
点灯している	閉

空気差圧センサーの接続方法

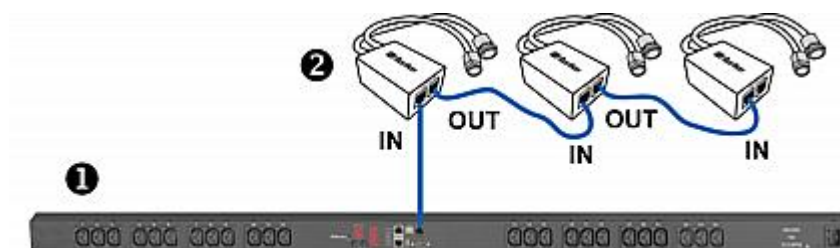
空気差圧データが必要な場合は、Raritan 空気差圧センサーを Dominion PX デバイスに接続しておくことができます。

このセンサーを使用すると、内部に搭載されている温度センサーで、センサー周辺の温度も検出できます。

▶ 空気差圧センサーを接続するには、次の手順に従います。

1. Raritan が提供する電話ケーブルの片側を Dominion PX デバイスの Sensor ポートに接続します。
2. この電話ケーブルのもう一方の端を空気差圧センサーの入力ポートに接続します。

①	Dominion PX デバイス:
②	Raritan 空気差圧センサー



資産管理センサーの接続 (オプション)

ラック内の最大 64 台の IT デバイスに電子タグを付けてから資産管理センサー (資産センサー) を Dominion PX に接続すると、それらの IT デバイスの場所をリモートで追跡できます。

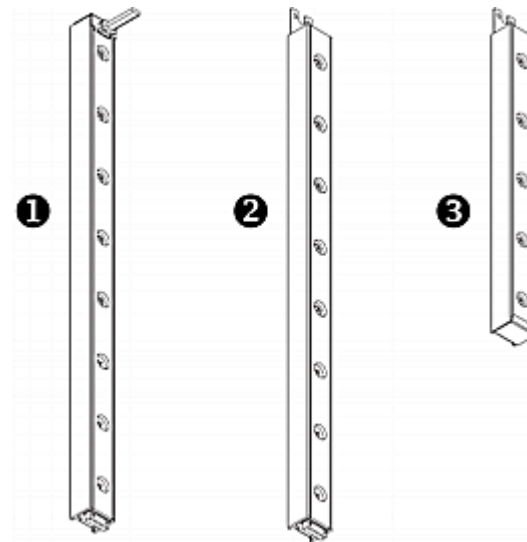
この資産管理機能を使用するには、次のものがが必要です。

- Raritan 資産センサー: 資産センサーは、タグと位置の情報を Dominion PX に転送します。
- Raritan 資産タグ: 資産タグは、接続されている IT デバイスに電子タグを付けます。

資産センサーの結合

資産センサーの各タグ ポートは、ラック ユニットに対応し、特定のラック（またはキャビネット）上の IT デバイスを探すのに使用できます。ラックごとに、資産センサー（1 つのマスタ資産センサーと複数のスレーブ資産センサーで構成される）を最長 64U まで接続できます。マスタ資産センサーとスレーブ資産センサーの違いは、前者には RJ-45 コネクタがあり、後者にはない点です。

次の図は、いくつかの資産センサーを示します。Raritan 社製の資産センサーには、これ以外のタイプもあります。



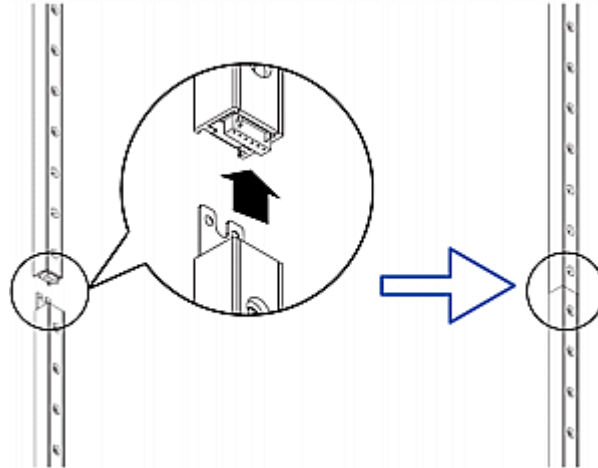
番号	項目
①	8 つのタグ ポートを搭載した 8U マスタ資産センサー
②	8 つのタグ ポートを搭載した 8U スレーブ資産センサー
③	5 つのタグ ポートを搭載した 5U 「エンド」スレーブ資産センサー

注: 通常のスレーブ資産センサーには DIN コネクタが両端に 1 つずつありますが、それとは異なり、エンド スレーブ資産センサーには一方の端にだけ DIN コネクタが 1 つあります。エンド資産センサーは、資産センサー アセンブリの端に装着されます。

▶ 資産センサーを組み立てるには、次の手順に従います。

1. マスタ資産センサーを 8U スレーブ資産センサーに接続します。

- スレーブ資産センサーの白いオス DIN コネクタをマスタ資産センサーの白いメス DIN コネクタに接続します。
- オス DIN コネクタの横にある U 型のシート メタルがマスタ資産センサーの背面スロットに挿入されていることを確認します。U 型のシート メタルをねじで締めて接続を補強します。



2. 手順 1 と同じ方法で、別の 8U スレーブ資産センサーをマスタ資産センサーに接続されている資産センサーに接続します。
3. 上記の手順を繰り返して、他のスレーブ資産センサーを接続します。資産センサー アセンブリの長さは、最長 64U です。
 - 最後の資産センサーは、ラックの実際の高さに応じて 8U または 5U にすることができます。
 - 最後の資産センサーには「エンド」資産センサーを使用することを強くお勧めします。
4. 各タグ ポートをラック ユニットに横に並べて、IT 機器の横にあるラックに資産センサー アセンブリを縦に接続します。資産センサーは、背面に磁気タップが付いているため、磁力でラックに装着されます。

注: 資産センサーにはチルト センサーが搭載されているので、上下を逆にして装着することもできます。

Dominion PX への資産センサーの接続

IT デバイスの追跡には、資産センサーと資産タグの両方が必要です。資産タグは、IT デバイスに貼付され、各 IT デバイスの ID 番号を示します。一方、資産センサーは、ID 番号と位置情報を、接続された Dominion PX デバイスに転送します。

次の図は、資産タグを示します。



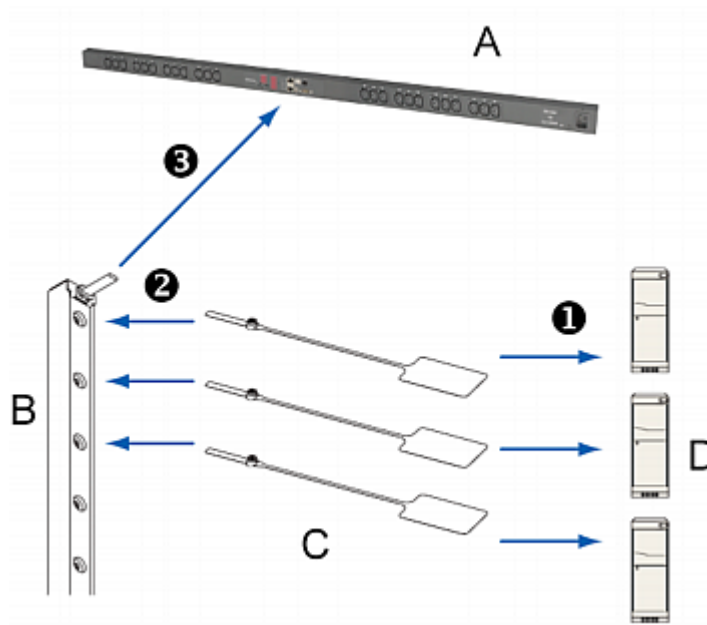
文字	項目
A	資産タグのいずれかの端にあるバーコード (ID 番号)。
B	タグ コネクタ
C	テープ付きの接着部分

注: 各資産タグのバーコードは一意で、Dominion PX Web インタフェースに表示されるので、簡単に識別できます。

► 資産センサーを **Dominion PX** デバイスに接続するには、次の手順に従います。

1. 資産タグの接着部分がある側をタグのテープを使用して各 IT デバイスに貼付します。
2. 各資産タグのもう一方の側にあるコネクタを資産センサーの対応するタグ ポートに接続します。
3. 次の手順に従って、ラックの資産センサー アセンブリを Dominion PX デバイスに接続します。
 - a. カテゴリ 5e/6 ケーブルの一方の端をマスタ資産センサー上の RJ-45 コネクタに接続します。
 - b. ケーブルの一方の端を Dominion PX デバイスの FEATURE ポートに接続します。

Dominion PX デバイスは、カテゴリ 5e/6 ケーブルを使用して電力を資産センサー アセンブリに供給します。資産センサーのファームウェアが Dominion PX デバイスによってアップグレードされている場合は、電源をオンにしたときに資産センサー アセンブリのすべての LED がさまざまな色で点滅を繰り返すことがあります。電源オンまたはファームウェアのアップグレードプロセスが完了すると、LED が点灯したままになります。タグポートの LED の色は、資産タグが接続されているかどうかによって異なります。



文字	項目
A	Dominion PX デバイス:
B	資産センサー
C	資産タグ
D	サーバなどの IT デバイス

注: Dominion PX では、接続されている資産センサーのラック ユニットの台数を検出できません。この情報を手動で設定する必要があります。
資産センサーの設定 『235p.』を参照してください。

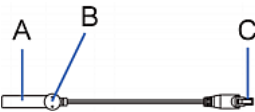
ブレード拡張ストリップの接続

1 つのシャーシに収められたブレード サーバの場合は、ブレード拡張ストリップを使用して個別のブレード サーバを追跡できます。

Raritan 社製のブレード拡張ストリップは、Raritan 資産センサーと同じように機能しますが、通常の資産センサーまたは AMS-M2-Z 上のタグポートに接続するためのタグ コネクタ ケーブルが必要です。ブレード拡張ストリップには、購入されたモデルに応じて 4 ～ 16 個のタグポートがあります。

図は、タグ コネクタ ケーブルと、タグポートが 16 個あるブレード拡張ストリップを示しています。

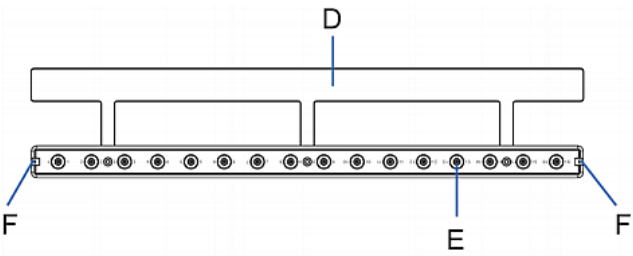
タグ コネクタ ケーブル



項目	説明
A	タグ コネクタ ケーブルのバーコード (ID 番号)
B	タグ コネクタ
C	ブレード拡張ストリップを接続するためのケーブル コネクタ

注: タグ コネクタ ケーブルには、接続された各ブレード拡張ストリップを識別するための固有のバーコードがあり、Dominion PX の Web インタフェースに表示されます。

ブレード拡張ストリップ



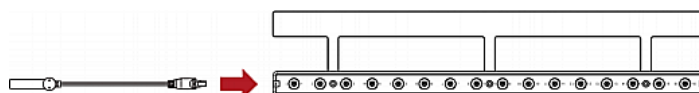
項目	説明
D	接着テープ付きのマイラー部分
E	タグ ポート

項目	説明
F	タグ コネクタ ケーブル接続用のケーブル ソケット

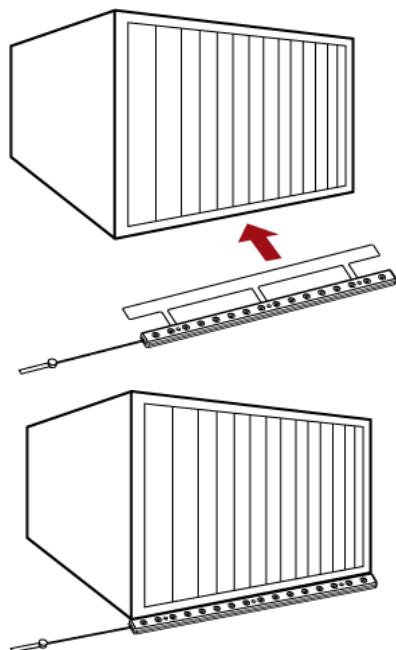
注: ブレード拡張ストリップの各タグ ポートには番号のラベルが付いており、これが *Dominion PX* の Web インタフェースでスロット番号として表示されます。

▶ ブレード拡張ストリップを取り付けるには、次の手順に従います。

1. タグ コネクタ ケーブルをブレード拡張ストリップに接続します。
 - ケーブルのコネクタをブレード拡張ストリップのいずれかの端のソケットに差し込みます。

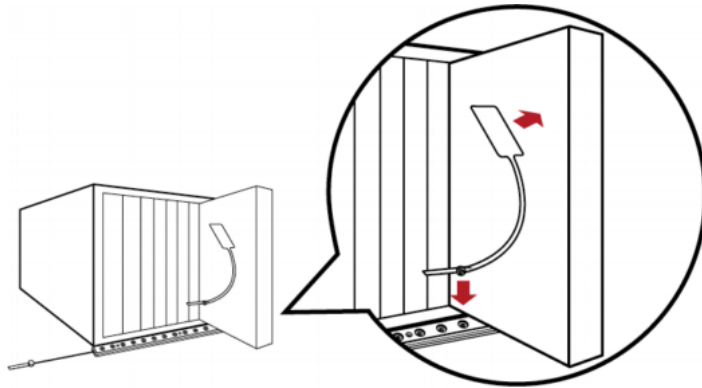


2. ブレード拡張ストリップをブレード シャーシの下に入れて、マイラー部分が完全にシャーシの下に隠れるようにし、ブレード拡張ストリップが簡単に落ちないことを確認します。必要な場合はマイラー部分の裏の接着テープを使用してストリップの位置を固定できます。

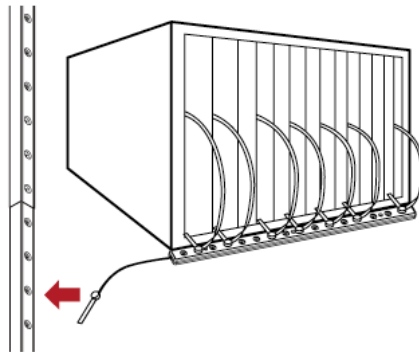


3. 資産タグの一方の端をブレード サーバに接続し、もう一方の端をブレード拡張ストリップに接続します。
 - a. 資産タグの接着部分をタグのテープでブレード サーバの片側に貼付します。

- b. 資産タグのタグ コネクタをブレード拡張ストリップのタグ ポートに差し込みます。



4. 上記の手順を繰り返して、シャーシ内のすべてのブレード サーバを資産タグを使ってブレード拡張ストリップに接続します。
5. ブレード拡張ストリップのタグ コネクタを資産センサー アセンブリまたはラックの AMS-M2-Z 資産センサーの最も近いタグ ポートに接続します。



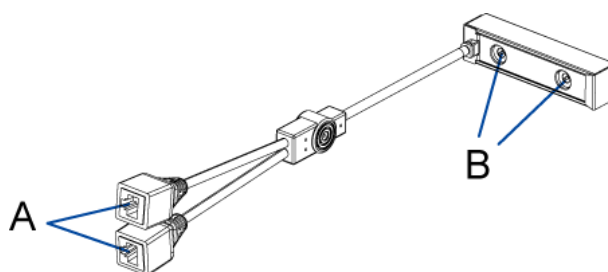
注: ブレード拡張ストリップのタグ コネクタを一時的に取り外す必要がある場合は、1 秒以上経ってから接続し直してください。早すぎると、*Dominion PX* で検出されないことがあります。

AMS-M2-Z 資産センサーの接続 (オプション)

AMS-M2-Z は、特殊なタイプの資産センサーで、通常のマスタ資産センサーと同じように機能しますが、以下の点で異なります。

- RJ-45 コネクタが 2 つあります。
- 複数の AMS-M2-Z 資産センサーをデイジーチェーン接続できます。
- 各 AMS-M2-Z で利用できるタグ ポートは 2 つだけなので、接続できる資産タグは 2 つだけです。

この製品は、キャビネット内の SAN ボックスなど大量のデバイスを追跡する際に特に便利です。

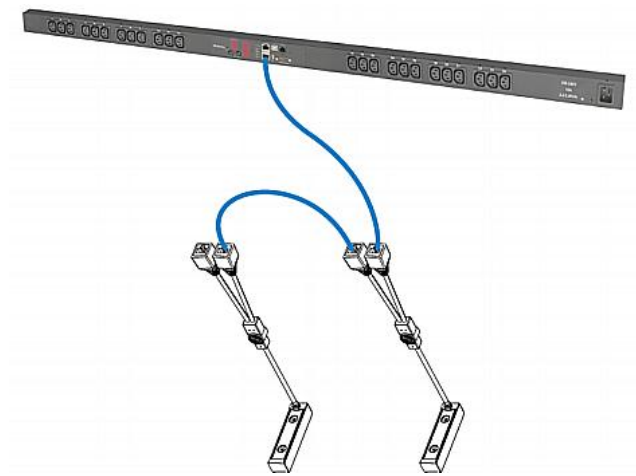


項目	説明
A	RJ-45 コネクタ
B	タグ ポート

▶ **AMS-M2-Z 資産センサーを Dominion PX するには、次の手順に従います。**

- カテゴリ 5e/6 ケーブルを使用して AMS-M2-Z を Dominion PX に接続します。
 - ケーブルの一方の端を、AMS-M2-Z の「Input (入力)」というラベルが付いた RJ-45 ポートに接続します。
 - ケーブルのもう一方の端を Dominion PX の FEATURE ポートに接続します。
- 資産タグを IT デバイスに貼付し、タグ コネクタを AMS-M2-Z のタグ ポートに差し込んで、この資産タグを AMS-M2-Z に接続します。詳細については、「*Dominion PX への資産センサーの接続* 『45p.』」を参照してください。
- 必要な場合は、複数の AMS-M2-Z をデイジーチェーン接続して、2 台以上の IT デバイスをこの Dominion PX で追跡します。
 - カテゴリ 5e/6 ケーブルの長さが制限内であることを確認します。ケーブル長の制限については、「*AMS-M2-Z デイジーチェーンの制限* 『51p.』」を参照してください。

- b. カテゴリ 5e/6 ケーブルの一方の端を、Dominion PX が接続されている AMS-M2-Z の「Output (出力)」というラベルが付いた RJ-45 コネクタに接続します。
- c. ケーブルのもう一方の端を、AMS-M2-Z の「Input (入力)」というラベルが付いた RJ-45 ポートに接続します。
- d. ここまでの手順を繰り返して、追加の AMS-M2-Z をデイジーチェーン接続します。チェーンでサポートされる AMS-M2-Z 資産センサーの最大数については、「**AMS-M2-Z デイジーチェーンの制限**『51p.』」を参照してください。
- e. すべての接続ケーブルの重量を支えるのに役立つケーブル タイを使用することを強くお勧めします。



4. 手順 2 を繰り返して、資産タグを介して IT デバイスをチェーン内の他の AMS-M2-Z に接続します。

AMS-M2-Z デイジーチェーンの制限

AMS-M2-Z アセット センサーをデイジーチェーン接続する場合にはいくつかの制限があります。制限は、最初の AMS-M2-Z に接続される Raritan モデルによって異なります。

モデル	デイジーチェーンの制限
モデル名が PX2 で始まるすべての PDU	- AMS-M2-Z を 2 台までデイジーチェーン接続可能。 - チェーン内の各 AMS-M2-Z 間のケーブルの最大長は 2 メートル。
EMX2-111	- AMS-M2-Z を 2 台までデイジーチェーン接続可能。 - チェーン内の各 AMS-M2-Z 間のケーブルの最大長は 2 メートル。

モデル	デイジーチェーンの制限
EMX2-888	- AMS-M2-Z を 6 台までデイジーチェーン接続可能。 - チェーン内の各 AMS-M2-Z 間のケーブルの最大長は 3 メートル。

Logicool Web カメラの接続 (オプション)

Dominion PX は、Logicool® QuickCam® Pro 9000 Web カメラの接続をサポートして、カメラの周囲のエリアのビデオまたはスナップショットを表示できるようにしています。Dominion PX では 1 台の Web カメラをサポートしています。Web カメラを接続すると、どこからでも Web インタフェースを通じて Dominion PX の近くの環境条件を視覚的に監視できます。

QuickCam Web カメラの詳細については、それに付属しているユーザー マニュアルを参照してください。

► Web カメラを接続するには、次の手順に従います。

1. Web カメラを Dominion PX デバイスの USB-A ポートに接続します。Dominion PX は Web カメラを自動的に検出します。
2. Web カメラを適切に配置します。

Web カメラでキャプチャした静止画像またはビデオは、すぐに Dominion PX Web インタフェースに表示されます。「**Web カメラの画像またはビデオの表示** 『246p.』」を参照してください。

GSM モデムの接続 (オプション)

SMS イベント メッセージを送信するには、Cinterion® MC52i/MC55iGSM モデムを Dominion PX に接続する必要があります。SMS イベント メッセージの詳細については、「**アクションの作成** 『180p.』」を参照してください。

注: Dominion PX は SMS メッセージを受信できません。

► GSM モデムを接続するには、次の手順に従います。

1. GSM モデムを Dominion PX の DB9 シリアル ポートに接続します。
2. 必要に応じて GSM モデムを設定します。GSM モデムの設定については、サポートされている GSM モデムのヘルプを参照してください。

Schroff LHX ヒート エクスチェンジャの接続 (オプション)

Dominion PX デバイスを使用して Schroff® LHX-20 または LHX-40 ヒート エクスチェンジャをリモートで監視および管理するには、ヒート エクスチェンジャと Dominion PX デバイスの接続を確立する必要があります。モデル名が PX2 で始まる PDU のみ、LHX ヒート エクスチェンジャをサポートしています。

LHX ヒート エクスチェンジャの詳細については、製品に付属のユーザマニュアルを参照してください。

PDU と LHX ヒート エクスチェンジャの接続を確立するには、Schroff が提供する RJ-45 RS-232 アダプタ ケーブルが必要です。

▶ **LHX ヒート エクスチェンジャを接続するには、次の手順に従います。**

1. アダプタ ケーブルの RS-232 DB9 側を Schroff LHX ヒート エクスチェンジャの RS-232 ポートに接続します。
2. ケーブルの RJ-45 側を Dominion PX デバイスの「FEATURE」というラベルのあるポートに接続します。

LHX ヒート エクスチェンジャのサポートを有効にする方法については、「*Schroff LHX ヒート エクスチェンジャの管理*」『254p.』を参照してください。

この章では、Dominion PX デバイスを使用する方法について説明します。また、PDU の LED とポートについて、および LED 表示パネルの使用方法について説明します。さらに、サーキット ブレーカ（過電流プロテクタ）の動作およびブザーが鳴るタイミングについても説明します。

この章の内容

パネルのコンポーネント	54
サーキット ブレーカ	63
ヒューズ	65
ブザー	68

パネルのコンポーネント

Dominion PX には、ゼロ U、1U、および 2U の各サイズがあります。すべてのタイプのモデルの外部パネルに、次のコンポーネントが備わっています。

- 電源コード
- アウトレット（コンセント）
- 接続ポート
- LED 表示
- リセット（RESET）ボタン

電源コード

ほとんどの Raritan PDU は、電源コードが取り付けられており、いつでも適切なアウトレット（コンセント）に接続して受電できる状態になっています。そのようなデバイスをユーザが配線し直すことはできません。

各 Dominion PX デバイスを適切な定格の分岐回路に接続します。適切な入力定格または定格の範囲については、Dominion PX デバイスに貼られているラベルまたはネームプレートを参照してください。

Dominion PX デバイスに電源スイッチはありません。PDU の電源の再投入を行うには、電源コードを分岐回路から抜いて 10 秒待った後、もう一度電源コードを接続します。

アウトレット（コンセント）

アウトレット（コンセント）の合計数は、モデルによって異なります。

PX-1000 シリーズ

これらの PDU は、アウトレット（コンセント）切り替え対応モデルではないため、すべてのアウトレット（コンセント）は常時オンの状態です。
アウトレット（コンセント）の LED は使用できません。

PX-2000 シリーズ

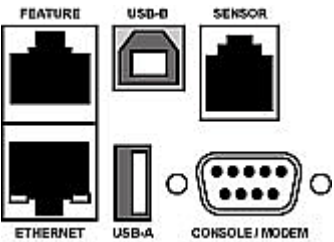
これらのモデルは、アウトレット（コンセント）切り替え対応 PDU です。
小さい LED が各アウトレット（コンセント）の隣にあり、リレー ボードの状態を示します。

LED の状態	アウトレット (コンセント) のステータス	意味
点灯していない	電源オフ	アウトレット（コンセント）が電源に接続されていないか、または制御回路の電源が壊れています。
赤	オン、ライブ	ライブ電源。アウトレット（コンセント）の電源がオンで、電力を供給できます。
	オン、非ライブ	アウトレット（コンセント）の電源はオンですが、サーキット ブレーカが作動しているので電力を供給できません。

接続ポート

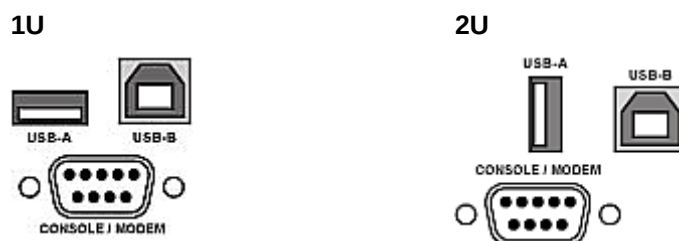
購入したモデルによって、使用可能なポートの合計数は異なります。

- ほとんどのゼロ U モデルでは、次に示すようにフロント パネルにポートが 6 つあります。



- ほとんどの 1U および 2U モデルでは、フロント パネルと背面パネルにそれぞれ 7 つのポートがあります。

- フロント パネルのポート:



- 背面パネルのポート:



ゼロ U モデル、1U モデル、および 2U モデルのポートの違いは、ゼロ U モデルにはセンサー ポートが 1 つだけであるのに対し、1U モデルと 2U モデルには 2 つある点です。

次の表に、各ポートの機能の説明を示します。

ポート	用途...
USB-B	コンピュータと Dominion PX デバイスとの USB 接続の確立。 このポートは、Dominion PX デバイスの障害復旧に使用できます。手順については Raritan テクニカル サポートにお問い合わせください。
USB-A	USB デバイスの接続。 これは、USB 2.0 の仕様に従った「ホスト」ポートで、電源が供給されています。
FEATURE	Power CIM を使用した、一部の Raritan アクセス製品 (Dominion KX II など) への接続、または Schroff 提供の RJ-45 RS-232 ケーブルを使用した Schroff® LHX-20 または LHX-40 デバイスへの接続、または ラック上の IT デバイスの場所を追跡できる Raritan 資産管理センサーへの接続。「 資産管理センサーの接続 (オプション) 」『42p.』を参照してください。

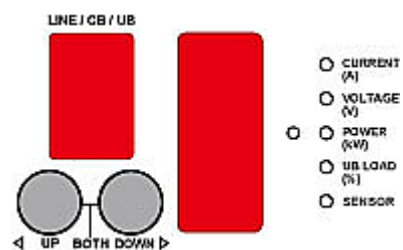
ポート	用途...
	警告: これは RS-232 ポートではないため、RS-232 デバイスを接続しないでください。接続すると、デバイスが破損する可能性があります。
CONSOLE/ MODEM	コンピュータと Dominion PX デバイスとのシリアル接続の確立。 これは、標準の DTE RS-232 ポートです。両端に 2 つの DB9 コネクタを持つヌル モデム ケーブルを使用して、Dominion PX デバイスをコンピュータに接続できます。
SENSOR	Raritan の環境センサーへの接続。 ゼロ U 製品で複数の環境センサーを接続する場合は、センサー ハブが必要です。
ETHERNET	Dominion PX デバイスの社内ネットワークへの接続。 標準のカテゴリ 5e/6 UTP ケーブルをこのポートに接続し、もう一方の端をネットワークに接続します。この接続は、Web インタフェースを使用して Dominion PX デバイスの管理またはアクセスをリモートで行うために必要です。 ポートの横に 2 つの小さな LED があります。 ■ 緑色は、物理リンクとそのアクティビティを示します。 ■ 黄色は、10/100 BaseT の通信速度を示します。 USB カスケード接続構成の場合、マスタ Dominion PX には有線接続が必須です。詳細については、「USB を経由した PDU のカスケード接続『33p. の“USB による PDU のカスケード接続”参照』」を参照してください。 注: Dominion PX デバイスがワイヤレス ネットワークに接続されている場合、このポートへの接続は不要です。

LED 表示

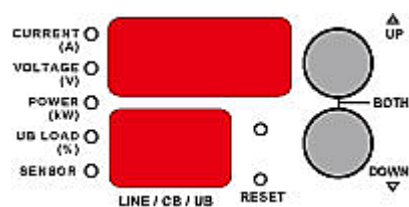
LED 表示は、アウトレット（コンセント）と同じ側にあります。

次の図は、さまざまなタイプの PDU 上の LED 表示を示しています。
LED 表示は、購入した PDU によって少し異なる場合があります。

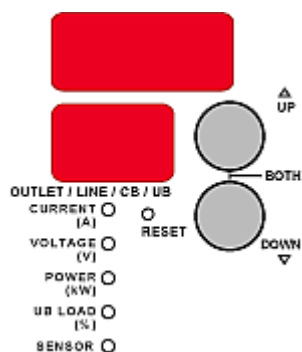
ゼロ U モデル:



1U モデル:



2U モデル:



LED 表示は、以下で構成されます。

- 3 桁表示パネル
- 2 桁表示パネル
- 上 (UP) ボタンと下 (DOWN) ボタン
- 測定単位の 5 つの LED

ゼロ U モデルでは、組み込みのチルト センサーによってそれ自体の向きが検出され、LED 表示の英数字を読みやすい向きに自動的に変更できます。LED 表示の文字の向きをロックするには、コマンド ライン インタフェースを使用して表示方向を設定できます。「**LED 表示の向きの変更**」『308p.』を参照してください。

注: Dominion PX デバイスの電源がオンになると、しばらくの間はパワーオン セルフテストとソフトウェアのロードが実行されます。ソフトウェアのロードが完了すると、LED 表示が点灯します。

3 桁表示パネル

3 桁表示パネルには、選択したコンポーネントの測定値が表示されます。以下のような値が表示されます。

- インレットの有効電力または不平衡負荷
- 選択したサーキット ブレーカの電流
- 選択したラインの電流、電圧、または有効電力

注: L1 電圧は L1-L2 または L1-N 電圧に該当し、L2 電圧は L2-L3 または L2-N 電圧に、また L3 電圧は L3-L1 または L3-N 電圧に該当します。

- 文字列「FuP」(ファームウェア アップグレードの実行中を示す)
- 文字列「CbE」(選択したサーキット ブレーカが作動したことを示す)

測定単位の LED

LED 表示に 5 つの小さい LED インジケータがあります。4 つの測定単位 LED と 1 つのセンサー LED です。

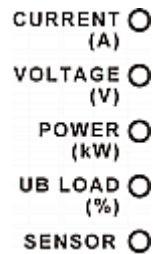
測定単位は、3 桁表示パネルに表示される測定値に応じて異なります。次の測定単位が使用されます。

- 電流の場合は、アンペア (A)
- 電圧の場合は、ボルト (V)
- 有効電力のキロワット (kW)
- 不平衡負荷の割合 (%)

いずれかの測定単位 LED が点灯し、3 桁表示パネルに現在表示されている値の単位が示されます。

センサー LED は、Dominion PX で環境センサーの物理接続が検出された場合にのみ点灯します。

5 つの LED は次の図のようになりますが、購入したモデルによって少し異なる場合があります。



2 桁表示パネル

2 桁表示パネルには、現在選択されているアウトレット (コンセント)、ラインまたはサーキット ブレーカの番号が表示されます。以下のような値が表示されます。

- 2 桁の数字: これは、選択したアウトレット (コンセント) を示します。たとえば、03 はアウトレット (コンセント) 3 を示します。
- Cx: これは、選択したサーキット ブレーカを示します。x はサーキット ブレーカ番号です。たとえば、C1 はサーキット ブレーカ 1 を表します。
- Lx: これは、単一インレット PDU の選択したラインを示します。x はライン番号です。たとえば、L2 はライン 2 を表します。

注: 単相モデルの場合、L1 電流はユニット電流を表します。

- AP: これは、選択したインレットの有効電力を示します。
- UL: これは、選択したインレットまたはアウトレット（コンセント）の不平衡負荷を表し、3 相 PDU でのみ利用できます。

一部の Dominion PX モデルでは、ファームウェアのアップグレード中に、2 桁表示パネルに bx と表示されることがあります。これは、x 番目のリレーまたはメーター ボードが更新中であることを示すものです。

自動モード

そのままにしておくと、LED 表示には、Dominion PX で取得可能なラインの測定値とサーキット ブレーカの測定値が 10 秒周期で繰り返し表示されます。これが自動モードです。

手動モード

上 (UP) ボタンまたは下 (DOWN) ボタンを押すと手動モードになり、特定のラインまたはサーキット ブレーカを選択してその測定値を表示できるようになります。

▶ LED 表示を操作するには、次の手順に従います。

- 2 桁表示パネルで目的のラインまたはサーキット ブレーカ番号が選択されるまで、上 (UP) ボタンまたは下 (DOWN) ボタンを押します。または、いずれかのボタンを押して、AP と表示されるインレットの有効電力を選択することもできます。
 - ▲ (UP) ボタンを押すと、番号が 1 だけ大きくなります。
 - ▼ (DOWN) ボタンを押すと、番号が 1 だけ小さくなります。
- 選択したコンポーネントの現在値は、3 桁表示パネルに表示されます。同時に CURRENT(A) LED が点灯します。「**測定単位の LED**」『60p. 』を参照してください。
- ラインを選択した場合は、上 (UP) ボタンと下 (DOWN) ボタンを同時に押すと、電圧、有効電力、電流の各測定値の表示を切り替えることができます。
 - 電圧が表示されると、VOLTAGE(V) LED が点灯します。約 5 秒間表示された後、現在の測定値が再表示されます。
 - 有効電力が表示されると、POWER(kW) LED が点灯します。約 5 秒間表示された後、現在の測定値が再表示されます。
- インレット (AP) を選択した場合は、有効電力の測定値が表示されます。
 - 有効電力が表示されると、POWER(kW) LED が点灯します。

注: LED 表示は、最後にボタンが押されてから 20 秒経過すると、自動モードに戻ります。

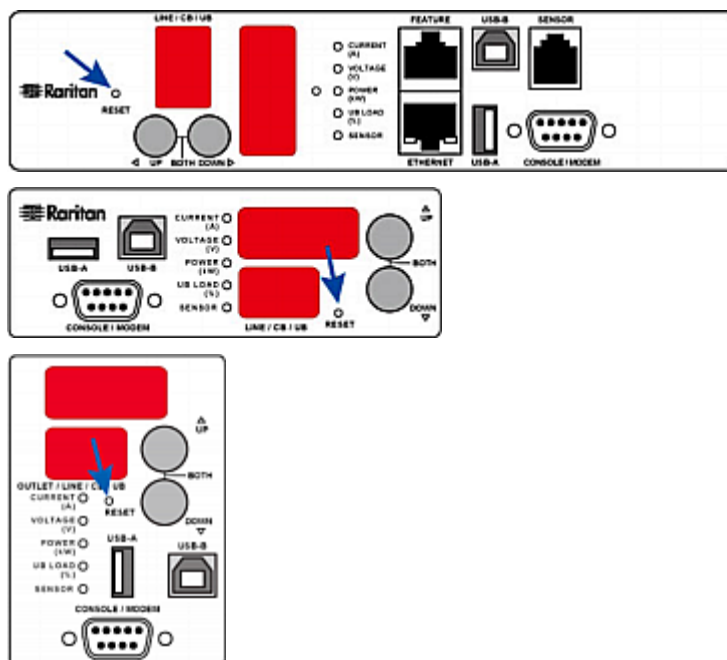
リセット (RESET) ボタン

リセット (RESET) ボタンは、2 桁表示パネルの横の小さな穴の中にあります。

シリアル接続されている場合に、このボタンを使用すると、Dominion PX デバイスを工場出荷時のデフォルト設定にリセットできます。「**工場出荷時設定へのリセット**『443p.』」を参照してください。

シリアル接続されていない場合は、このリセット (RESET) ボタンを押すと、アウトレット (コンセント) への電源供給が停止することなく Dominion PX デバイスのソフトウェアが再起動されます。この操作により、LED 表示の電源の再投入が行われるため、LED 表示が空白になり、その後正常に戻ります。

次の図は、0U、1U、および 2U モデルのリセット (RESET) ボタンの場所を示しています。



サーキット ブレーカ

定格が 20A (北米) または 16A (北米以外) を超える Dominion PX モデルには、分岐回路ブレーカが搭載されています。こうしたサーキット ブレーカは、サーキット ブレーカを流れる電流が定格を超えると、自動的に作動 (電源を切断) します。

サーキット ブレーカが電源をオフにすると、LED 表示は次のようになります。

- 3 桁表示パネルに、サーキット ブレーカ エラーを意味する「CbE」が表示されます。

サーキット ブレーカが作動すると、そのブレーカに接続されているすべてのアウトレット (コンセント) への電流が遮断されます。そのため、遮断されたアウトレット (コンセント) が再び正常に動作するように、手動でサーキット ブレーカをリセットする必要があります。

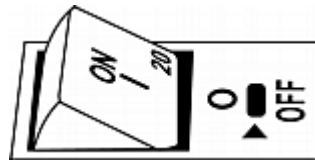
購入したモデルによって、サーキット ブレーカには、ボタン リセットまたはハンドル リセット機構が採用されている場合があります。

ボタンタイプのサーキット ブレーカのリセット

ご使用のボタンタイプのサーキット ブレーカが、このセクションに記載されている図とは若干異なる場合がありますが、リセット手順は同じです。

- ▶ ボタンタイプのサーキット ブレーカをリセットするには、次の手順に従います。

1. ブレーカが作動していることを示す、オン ボタンが上がっているブレーカを探します。



2. Dominion PX デバイスおよび接続された装置を調べ、過負荷または短絡の原因を解消します。この手順を実行しなければ、次の手順に進めません。
3. オン ボタンを完全に下がるまで押し込みます。

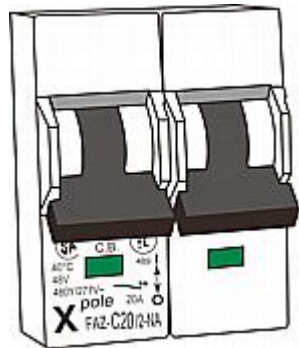


ハンドルタイプのサーキット ブレーカのリセット

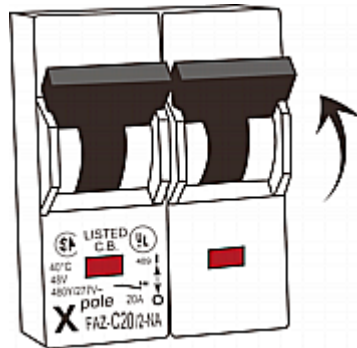
ご使用のハンドルタイプのサーキット ブレーカが、このセクションに記載されている図とは若干異なる場合がありますが、リセット手順は同じです。

▶ ハンドルタイプのサーキット ブレーカをリセットするには、次の手順に従います。

1. 蝶番付きカバーをブレーカの上に持ち上げます。
2. 操作ハンドルの下にある長方形または三角形の色表示が、ブレーカの作動を示す緑色になっているかどうかを確認します。



3. Dominion PX デバイスおよび接続された装置を調べ、過負荷または短絡の原因を解消します。この手順を実行しなければ、次の手順に進めません。
4. 操作ハンドルを引き上げて、長方形または三角形の色表示を赤色にします。



ヒューズ

一部の Dominion PX デバイスには、サーキット ブレーカの代わりにヒューズが搭載されています。過負荷が検出されると、ヒューズが溶断して、関連付けられているアウトレット（コンセント）を保護します。

PDU でヒューズが使用されている場合は、ヒューズが溶断したり正常に機能しなくなったときに新しいものと交換する必要があります。新しいヒューズの定格は元のものと同じにする必要があります。



不適切な定格のヒューズを使用すると、PDU や接続している装置の破損、感電、火災、死傷につながります。

ヒューズの交換方法は、PDU の設計によって異なります。

ゼロ U モデルでのヒューズの交換

このセクションは、「交換可能な」ヒューズがあるゼロ U PDU にのみ適用されます。

▶ ゼロ U モデルでヒューズを交換するには、次の手順に従います。

1. ヒューズの蝶番付きカバーを持ち上げます。



2. 新しいヒューズの定格とヒューズ ホルダのカバーに示されている定格を照合します。



3. ヒューズ ホルダのカバーを押します。ヒューズが見えます。



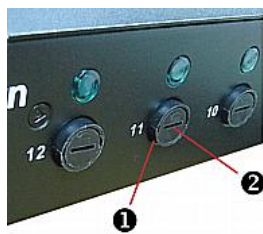
4. ホルダからヒューズを取り出します。



5. ホルダに新しいヒューズを入れます。ヒューズの向きはどちらでもかまいません。
6. 先ほどと逆の順序でヒューズ ホルダと蝶番付カバーを閉じます。

1U モデルでのヒューズの交換

1U モデルでは、ヒューズは、PDU のヒューズ キャリアに収まるヒューズ ノブ内に装着されます。



番号	説明
①	ヒューズ キャリア
②	ヒューズを装着するヒューズ ノブ

▶ **1 U PDU でヒューズを交換するには、次の手順に従います。**

1. 電源から PDU の電源コードを外します。
2. マイナスねじ回しを使用して PDU のヒューズ キャリアから目的のヒューズを外します。
 - a. ヒューズ ノブをスロットが 45 度傾くまで反時計回りに回します。



- b. このノブをヒューズ キャリアから外します。
3. ノブから古いヒューズを取り外し、新しいヒューズのどちらかの端をノブに挿入します。新しいヒューズの定格が元のものと同じであることを確認します。



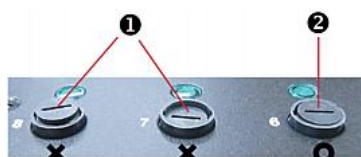
番号	説明
①	ヒューズ ノブ
②	ヒューズ

4. ノブと新しいヒューズを、マイナスねじ回しを使用してヒューズ キャリアに装着します。
 - a. ノブをヒューズ キャリアに挿入するときは、ノブのスロットを 45 度傾けます。



- b. ノブをヒューズ キャリアにそっと押し込んで、スロットが水平になるまで時計回りに回します。

5. ノブとヒューズ キャリアの高さが揃っていることを確認します。ノブの頭がヒューズ キャリアより高いか低い場合は、装着し直します。



番号	説明
①	不適切な装着
②	適切な装着

6. PDU の電源コードを電源に接続し、対応するヒューズの LED が点灯していることを確認します。これは、LED が適切に機能していることを示します。

ブザー

Dominion PX は、重大な状況になると警報音が鳴るブザーを備えています。

- ブザーは、サーキット ブレーカが作動して 3 秒以内に鳴動します。
- ブザーは、すべてのサーキット ブレーカがリセットされるとすぐに停止します。

Ch 5

Web インタフェースの使用

この章では、Web インタフェースを使用して Dominion PX を管理する方法について説明します。

この章の内容

サポートされている Web ブラウザ	70
Web インタフェースへのログイン	70
ログアウト	72
Web インタフェースの概要	73
ダッシュボードの表示	87
デバイス管理	88
[User Management (ユーザ管理)]	113
役割の設定	119
アクセス セキュリティ コントロール	123
SSL 証明書の設定	139
LDAP 認証の設定	146
アウトレット (コンセント) 管理	153
インレットとサーキット ブレーカの管理	169
電力しきい値の設定	173
イベント ルールの設定	179
イベント ロギングの管理	218
接続中のユーザの表示	220
サーバ アクセシビリティの監視	221
[Environmental Sensors (環境センサー)]	224
資産管理	234
一括設定による設定のコピー	240
測定単位の変更	242
Web カメラの画像またはビデオの管理	244
ネットワーク診断	250
通信ログの表示	252
診断情報のダウンロード	253
Schroff LHX ヒート エクスチェンジャの管理	254
ファームウェアのアップグレード	261
ヘルプの使用	264

サポートされている Web ブラウザ

次の Web ブラウザを使用して Dominion PX Web インタフェースにアクセスできます。

- Internet Explorer® 8 および 9
- Firefox® 3.x および 4+
- Safari® 5.x (MacOS Lion)
- Google® Chrome® 12+

Web インタフェースへのログイン

Web インタフェースにログインするには、ユーザ名とパスワードを入力する必要があります。初めて Dominion PX にログインするときは、デフォルトのユーザ名 (admin) とパスワード (raritan) を使用します。セキュリティ上の理由により、その後にパスワードを変更するように求められます。

例外: 『初期ネットワーク設定 『26p.』』で、admin アカウントのパスワードをすでに変更した場合は、新しいパスワードを使用して Web インタフェースにログインすると、パスワードの変更を求められることはありません。

正常にログインすると、他のユーザのユーザ プロファイルを作成できるようになります。このプロファイルで各ユーザのログイン名とパスワードを定義します。「ユーザ プロファイルの作成 『114p.』」を参照してください。

ログイン

Web インタフェースでは、最大 16 ユーザが同時にログインできます。正しく動作するように、Web ブラウザで JavaScript を有効にする必要があります。

► **Web インタフェースにログインするには、次の手順に従います。**

1. Microsoft Internet Explorer または Mozilla Firefox などのブラウザを開き、次の URL を入力します。

`http(s)://<ip address>`

ここで、<ip address> は、Dominion PX デバイスの IP アドレスです。

2. セキュリティ警告メッセージが表示される場合は、[OK] または [Yes (はい)] をクリックします。[Login (ログイン)] ページが表示されます。

Login

User Name:

Password:

3. [User Name (ユーザ名)] フィールドにユーザ名を入力し、[Password (パスワード)] フィールドにパスワードを入力します。

注: ユーザ名とパスワードのいずれも、大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。ユーザ名やパスワードを間違えて入力した場合、入力内容や表示されたエラー メッセージを消去するには、[Clear (クリア)] をクリックします。

4. [Login (ログイン)] をクリックするか、Enter キーを押します。[Dominion PX] ページが表示されます。

注: ハードウェア構成によっては、[Dominion PX] ページに表示される要素が、次の図とは若干異なる場合があります。

Raritan. Dominion PX

User Management | Device Settings | Maintenance

Dashboard

Inlet

RMS Current: 0.2 A / 16.0 A

RMS Voltage: 111 V

Active Power: 15 W

Apparent Power: 26 VA

Power Factor: 0.58

Active Energy: 134448 Wh

Alerted Sensors

Sensor	Reading	State

Overcurrent Protectors (2)

#	Name (Label)	Current Drawn	Current Remaining	Status
1	Overcurrent Protector C1	0.00 A	20.00 A	closed
2	Overcurrent Protector C2	0.00 A	20.00 A	closed

External Sensors (4 managed, 0 unmanaged)

Name	Reading	State
Humidity 1	55 %	normal
Humidity 2	55 %	normal
Temperature 1	25.5 °C	normal
Temperature 2	25.6 °C	normal

my PX (192.168.04.90) | Administrator (admin) | Last Login: 3/1/12 4:14 AM | 3/1/12 4:16 AM

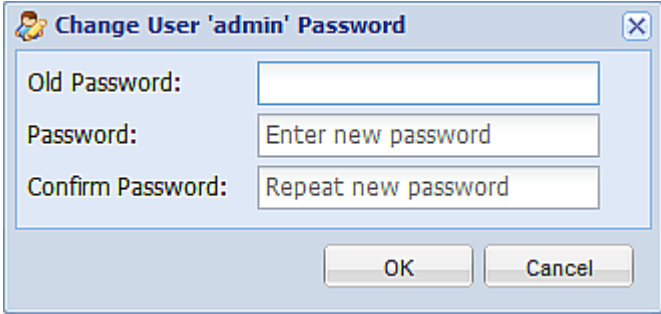
パスワードの変更

通常のユーザは、自身のパスワードの変更権限があれば、自身のパスワードを変更できます。「**役割の設定**『119p.』」を参照してください。

管理者 (admin) である場合は、初めて Dominion PX にログインすると、Dominion PX Web インタフェースにより自動的にパスワードの変更が求められます。管理者権限を持っている場合は、他のユーザのパスワードも変更できます。「**ユーザ プロファイルの変更**『118p.』」を参照してください。

▶ **パスワードを変更するには、以下の手順に従います。**

1. [User Management (ユーザ管理)] > [Change Password (パスワードの変更)] を選択します。[Change User Password (ユーザ パスワードの変更)] ダイアログ ボックスが表示されます。



2. [Old Password (古いパスワード)] フィールドに現在のパスワードを入力します。
3. [Password (パスワード)] フィールドと [Confirm Password (パスワードの確認)] フィールドに新しいパスワードを入力します。パスワードとして設定できる文字数は 4 ～ 32 文字です。パスワードの大文字と小文字は区別されます。
4. [OK] をクリックして変更を保存します。

ヒント: 管理者権限を持っている場合は、他のユーザのパスワードを変更できます。「**ユーザ プロファイルの変更**『118p.』」を参照してください。

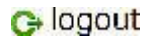
ログアウト

Dominion PX での作業が完了したら、他のユーザが Web インタフェースにアクセスできないように、ログアウトする必要があります。

▶ **Web インタフェースからログアウトするには、次の手順に従います。**

1. 次のいずれかを実行します。

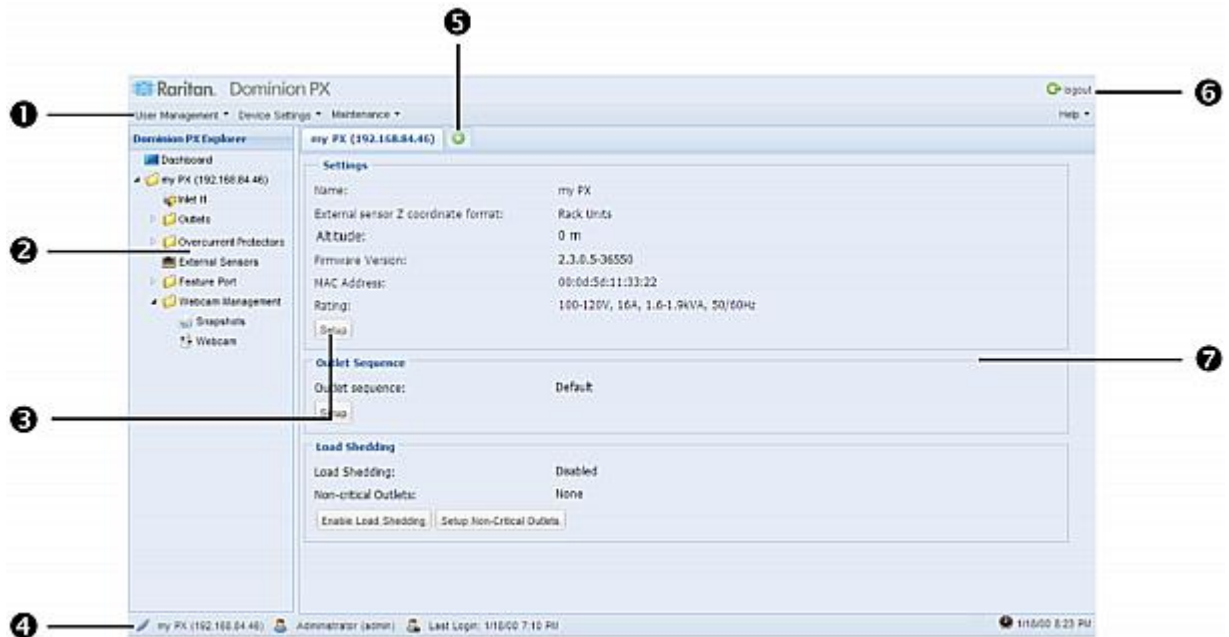
- Web インタフェースの右上隅の [logout (ログアウト)] をクリックします。



- ブラウザの右上隅の [Close (閉じる)] ボタン (X) をクリックして、Web ブラウザを閉じます。
 - [File (ファイル)] > [Close (閉じる)] または [File (ファイル)] > [Exit (終了)] を選択して、Web ブラウザを閉じます。コマンドは、使用するブラウザのバージョンによって異なります。
 - 更新コマンドを選択するか、Web ブラウザの更新ボタンをクリックします。
2. 前の手順で選択した内容に応じて、ログイン ページが表示されるか、ブラウザが閉じられます。

Web インタフェースの概要

Web インタフェースでは、どのページでも 2 つのペイン、メニュー バー、ステータス バー、[Add Page (ページの追加)] アイコン、および [logout (ログアウト)] ボタンが表示されます。



番号	Web インタフェース要素
①	メニュー
②	Domain PX Explorer ペイン

番号	Web インタフェース要素
③	[Setup (設定)] ボタン*
④	ステータス バー
⑤	[Add Page (ページの追加)] アイコン
⑥	[logout (ログアウト)] ボタン
⑦	データ ペイン

* [Setup (設定)] ボタンは、一部のページ (ダッシュボード ページなど) では使用できません。

これらの Web インタフェース要素の詳細については、この後のセクションを参照してください。

メニュー

メニュー バーは、ページの上部にあります。メニューをクリックすると、ドロップダウン リストから目的のメニュー項目を選択できます。

4 つのメニューで、さまざまなタスクの管理または情報の表示を行うことができます。

- **[User Management (ユーザ管理)]** には、ユーザ プロファイル、権限 (役割)、およびパスワードを管理するためのメニュー項目が用意されています。
- **[Device Settings (デバイスの設定)]** では、デバイスに関する設定 (デバイス名、ネットワーク設定、セキュリティ設定、システム時刻など) を行うことができます。
- **[Maintenance (メンテナンス)]** には、Dominion PX の保守に役立つツール (イベント ログ、ハードウェア情報、ファームウェア アップグレードなど) が用意されています。
- **[Help (ヘルプ)]** では、Dominion PX に組み込まれているファームウェアおよびすべてのオープン ソース パッケージに関する情報が表示されます。さらに、このメニューからユーザ ガイドにアクセスできます。

Dominion PX Explorer ペイン

左側の階層ツリーには、アクセスしている Dominion PX デバイス、およびこの PDU に組み込まれているか接続されているすべての物理コンポーネント（インレット、アウトレット（コンセント）、環境センサーなど）が表示されます。さらに、PDU の概要情報を表示するための [Dashboard (ダッシュボード)] という名前のアイコンを使用できます。

ツリーは、3 階層レベルの構成になっています。

第 1 レベル	第 2 レベル	第 3 レベル
ダッシュボード	なし	なし
PDU フォルダ*	インレット I1	なし
	アウトレット（コンセント）	1 ～ n**
	過電流プロテクタ フォルダ	C1 から Cn へ**
	外部センサー フォルダ	接続されている環境センサーのリスト
	Feature Port (拡張ポート) フォルダ	設定に応じて、次のいずれかが表示されます。 - なし - Asset Strip (資産ストリップ) - Power CIM - LHX-20 - LHX-40
	Webcam Management (Web カメラ管理)	- Snapshots (スナップショット) - Webcam (Web カメラ)

* PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「*Naming the PDU (PDU のネーミング)*」『90p. の「PDU の名前付け」参照先』を参照してください。

** n は、該当するコンポーネントの最後の番号を表します。

注: Web カメラ アイコンは、Logicool® QuickCam® Pro 9000 Web カメラが Dominion PX に接続されている場合にのみ表示されます。「*Logicool Web カメラの接続 (オプション)*」『52p. 』を参照してください。

▶ ツリー内を移動するには、次の手順に従います。

1. フォルダを展開するには、「ツリーの展開」『76p. 』を参照してください。
2. ツリー項目のデータを表示するには、該当する項目をクリックします。「*[Add Page (ページの追加)] アイコン*」『80p. 』を参照してください。

ツリーの展開

Dominion PX デバイスに実装されているコンポーネントや、接続されているコンポーネントを表すアイコンは、デフォルトでは展開されています。非表示になっている場合は、ツリーを手動で展開すると、すべてのコンポーネント アイコンを表示できます。

▶ ツリーを展開するには、次の手順に従います。

1. デフォルトでは、PDU フォルダは展開されています。

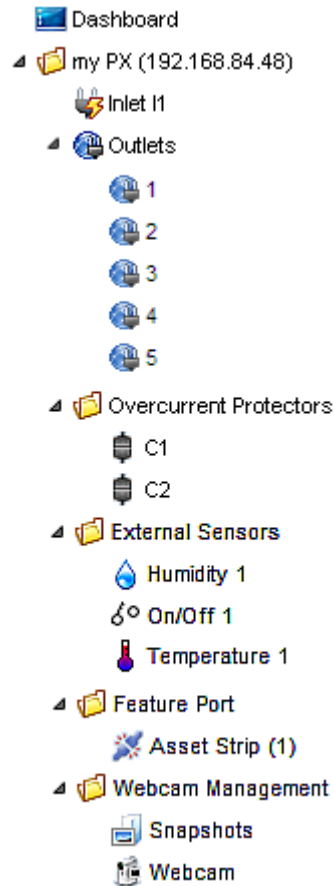
注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「*Naming the PDU (PDU のネーミング)*」『90p. の「PDU の名前付け」参照先』を参照してください。

PDU フォルダが展開されていない場合は、フォルダ アイコンの前の白色の矢印 ▴ をクリックするか、フォルダをダブルクリックします。矢印が黒色の斜め矢印 ▲ に変わり、コンポーネントまたはコンポーネント グループのアイコンが、PDU フォルダの下に表示されます。

2. 第 2 レベルのコンポーネント グループを展開するには、フォルダ アイコンの前の白色の矢印 ▴ をクリックするか、フォルダをダブルクリックします。

矢印が黒色の斜め矢印 ▲ に変わり、個々のコンポーネントを表すアイコンが、グループ フォルダの下に表示されます。

他のコンポーネント グループを展開するには、そのグループについても手順 2 を実行します。展開されたツリーは、次の図のようになります。



ツリーの縮小

ツリー構造全体または特定のコンポーネント グループを折りたたんで、全部または一部のツリー項目を非表示にすることができます。

▶ ツリー全体を折りたたむには、次の手順に従います。

- PDU フォルダ アイコンの前にある黒色の斜め矢印 ▲ をクリックするか、そのフォルダをダブルクリックします。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、『Naming the PDU (PDU のネーミング) 90p. の PDU の名前付け “参照先”』を参照してください。

矢印が白色の矢印 ▸ になり、PDU フォルダの下すべての項目が非表示になります。

▶ 一部のツリー項目を非表示にするには、次の手順に従います。

1. 折りたたむコンポーネント グループ フォルダの前にある黒色の斜め矢印 ▲ をクリックするか、そのフォルダをダブルクリックします。矢印が白色の矢印 ▸ になり、フォルダの下すべての項目が非表示になります。
2. 他のコンポーネント グループを折りたたむには、そのグループについても手順 1 を実行します。

ペインの調整

ペインの幅を変更して、領域を広くしたり、狭くしたりすることができます。

▶ ペインの幅を調整するには、次の手順に従います。

1. マウス ポインタを Dominion PX Explorer ペインの右側の境界に移動します。
2. マウス ポインタが双方向の矢印になったら、境界を横方向にドラッグすることで、ペインを拡大または縮小できます。

[Setup (設定)] ボタン

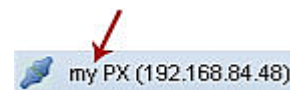
[Setup (設定)] ボタンは、ほとんどのツリー項目で使用できます。このボタンを使用すると、選択したツリー項目の設定を変更するための設定ダイアログ ボックスが表示されます。

ステータス バー

ステータス バーには、左から右に 5 種類の情報が表示されます。

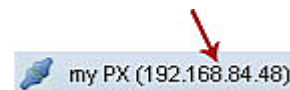
- デバイス名:

これは、Dominion PX デバイスに割り当てられている名前です。デフォルトでは、「my PX」です。「*PDU の名前付け*『90p.』」を参照してください。



- IP アドレス:

括弧で囲まれた番号は、Dominion PX デバイスに割り当てられている IP アドレスです。「*初期ネットワーク設定*『26p.』」または「*ネットワーク設定の変更*『93p.』」を参照してください。



ヒント: ステータス バーにデバイス名と IP アドレスが表示される場合は、*Dominion PX* デバイスに接続されていることを表しています。接続されていない場合は、代わりに「 disconnected」が表示されます。

- ログイン名:

この名前は、Web インタフェースへのログインに使用したユーザ名です。

 Administrator (admin)

- 前回のログイン時刻:

これは、このログイン名を使用して前回この *Dominion PX* デバイスにログインしたときの日時を示します。

 Last Login: 3/24/11 9:46 PM

前回のログイン時刻にマウス ポインタを置くと、アクセス クライアントや IP アドレスなど、前回のログインに関する詳細情報が表示されます。

シリアル接続経由のログインでは、〈local〉が IP アドレスの代わりに表示されます。

さまざまなタイプのアクセス クライアントがあります。

- Web GUI: *Dominion PX* Web インタフェースを指します。
- CLI: コマンド ライン インタフェース (CLI) を指します。
「CLI」に続く括弧内の情報は、このユーザが CLI に接続した方法を示します。
 - *Serial* (シリアル): ローカル接続 (シリアルまたは USB) を示します。
 - *SSH*: SSH 接続を示します。
 - *Telnet*: Telnet 接続を示します。

- システムの日付と時刻:

現在の日付、年、および時刻は、バーの右側に表示されます。システムの日付と時刻にマウス ポインタを置くと、タイム ゾーンの情報も表示されます。

 3/24/11 10:18 PM

Dominion PX デバイスとグラフィカル ユーザ インタフェース (GUI) との間で通信エラーが発生した場合は、バーの右側にフラグ アイコン () が表示されることがあります。アイコンが表示されている場合は、そのアイコンをクリックすると、通信ログが表示されます。「[通信ログの表示『252p.』](#)」を参照してください。

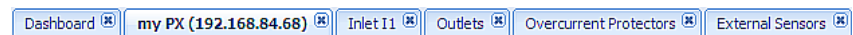
[Add Page (ページの追加)] アイコン

データ ペインの上部にある [Add Page (ページの追加)] アイコン  を使用すると、開いているページを上書きすることなく複数のツリー項目のデータ ページを開くことができます。

▶ 新しいデータ ページを開くには、次の手順に従います。

1. [Add Page (ページの追加)] アイコン  をクリックします。新しいタブが開かれ、空白のデータ ページが表示されます。
2. データ ページを開くツリー項目をクリックします。選択したツリー項目のデータが空白のページに表示されます。
3. 他のデータ ページを開くには、手順 1 ～ 2 を繰り返します。開かれたページを表すすべてのタブが、ページの上部に表示されます。

次の図に、マルチタブの例を示します。



4. 複数のページを開いた場合は、次の操作を実行できます。
 - 開いているデータ ページのいずれかに切り替えるには、対応するタブをクリックします。
タブが多すぎてすべてを表示できない場合は、ペインの左右の境界に 2 つの矢印 ( と ) が表示されます。どちらかの矢印をクリックすると、すべてのタブに移動できます。
 - データ ページを閉じるには、対応するタブの [Close (閉じる)] ボタン () をクリックします。

[logout (ログアウト)] ボタン

Web インタフェースからログアウトするには、[logout (ログアウト)] ボタンをクリックします。

 logout

データ ペイン

右側のペインには、選択したツリー項目のデータ ページが表示されます。データ ページには、項目の現在の状態、設定、および [Setup (設定)] ボタン (使用可能な場合) が表示されます。

ペインの上のすべてのタブは、開かれたデータ ページを表しています。強調表示されたタブは、現在の選択されています。

ペインの幅を変更して、領域を広くしたり、狭くしたりすることができます。

▶ ペインの幅を調整するには、次の手順に従います。

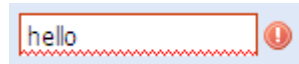
1. マウス ポインタを右側のペインの左側の境界に移動します。
2. マウス ポインタが双方向の矢印になったら、境界を横方向にドラッグすることで、ペインを拡大または縮小できます。

詳細情報

このセクションでは、その他の役立つ Web インタフェース要素または操作について説明します。

警告アイコン

特定のフィールドに入力した値が無効な場合は、右側に赤色の警告アイコンが表示され、問題のフィールドが、この図に示すように赤色の枠で囲まれます。



このようになった場合は、警告アイコンにマウス ポインタを置いて理由を表示し、入力した値を適宜変更します。

測定値の黄色表示または赤色表示

数値センサーの測定値が上限または下限のしきい値を超えると、ユーザーに警告するために、行全体の背景色が黄色または赤色になります。

ディスクリート（オン/オフ）センサーの場合は、センサーが異常状態になったときに、行の背景色が変わります。

サーキット ブレーカが作動すると、サーキット ブレーカの行も赤色で表示されます。

各色の意味については、次の表を参照してください。

色	状態
白	次のいずれかの場合に背景が白になります。 - 数値センサーの場合は、有効なしきい値がありません。 - 数値センサーでしきい値が有効になっていない場合、センサーの測定値は警告しきい値の下限と上限の間になります。 - ディスクリート（オン/オフ）センサーの場合、センサー状態が正常です。 - センサーの測定値または状態は「使用不可能」です。
黄色	測定値が、警告しきい値の下限を下回っているか、警告しきい値の上限を上回っています。
赤	赤色の意味は、センサー タイプによって異なります。 - 数値センサーの場合、この色は、臨界しきい値の下限を下回っているか、臨界しきい値の上限を上回っていることを示します。 - ディスクリート（オン/オフ）センサーの場合、この色はセンサーが「alarmed (アラーム)」状態であることを示します。 - サーキット ブレーカ作動センサーの場合は、サーキット ブレーカが作動したことを表します。

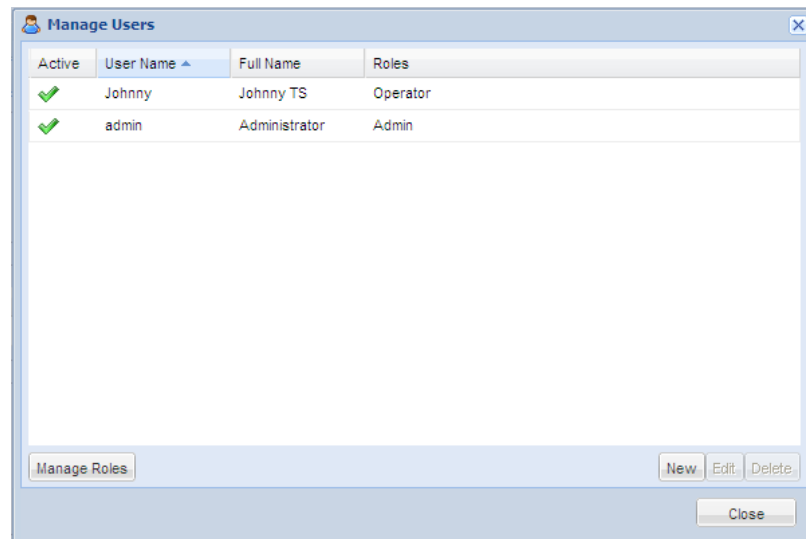
警告の正確な意味を理解するには、[State (状態)] (または [Status (ステータス)]) 列に表示される情報をお読みください。

- below lower critical (下位臨界未満): 数値センサーの測定値が、下位臨界しきい値を下回っています。
- below lower warning (下位警告未満): 数値センサーの測定値が、下位警告しきい値を下回っています。
- above upper critical (上位臨界以上): 数値センサーの測定値が、上位臨界しきい値に達しているか、上位臨界しきい値を下回っています。
- above upper warning (上位警告以上): 数値センサーの測定値が、上位警告しきい値に達しているか、上位警告しきい値を下回っています。
- alarmed (アラーム): ディスクリート センサーが正常状態ではありません。
- Open (開): サーキット ブレーカが作動しました。

しきい値については、「**電力しきい値の設定**『173p.』」を参照してください。

リストの表示の変更

以下に示す [Manage Users (ユーザの管理)] ダイアログ ボックスのような一部のダイアログ ボックスおよびデータ ページには、リストまたは表が含まれています。データを効率よく表示するために、リストの表示列の数または並べ替え順序を変更できます。ダイアログ ボックスまたはデータ ページを終了する場合、列または並べ替えの変更は保存されないことに注意してください。次回、ダイアログ ボックスまたはページを再び開くと、リストはデフォルトの表示に戻っています。



注: すべてのダイアログ ボックスで、並べ替えの変更や列の変更の機能がサポートされているわけではありません。

列の変更

リストまたは表の一部の列を非表示にしたり、特定の列の幅を調整したりすることができます。

▶ 表示列を変更するには、次の手順に従います。

1. 列見出しにマウス ポインタを置きます。この列見出しの右側に黒色の三角形  が表示されます。
2. 黒色の三角形をクリックすると、ドロップダウン メニューが表示されます。
3. [Columns (列)] をポイントします。すべての列を表示するサブメニューが表示されます。
4. 選択解除または選択する列をクリックします。
 - 列を非表示にするには、その列のチェックボックスをオフにします。
 - 列を表示するには、その列のチェックボックスをオンにします。

▶ 列の幅を変更するには、次の手順に従います。

1. 目的の列の右側の境界にマウス ポインタを置きます。
2. マウス ポインタが双方向の矢印になったら、境界を横方向にドラッグすることで、列を拡大または縮小できます。

並べ替えの変更

デフォルトでは、リストや表は、最初の列をキーにして昇順に並べられますが、リストの並び順を逆にしたり、別の列をキーにして並べ替えたりすることができます。

▶ 次のいずれかを実行して、リストを並べ替えます。

- リストの並べ替えのキーとする列見出しをクリックします。
 - a. 1 回クリックすると、リストは昇順に並べ替えられます。青色の三角形が上向き ▲ に表示され、昇順であることを確認できます。
 - b. 2 回クリックすると、リストは降順に並べ替えられます。青色の三角形が下向き ▼ に表示され、降順であることがわかります。
- 列メニューから並べ替えコマンドを選択します。
 - a. リストの並べ替えのキーとする列見出しにマウス ポインタを置きます。この列見出しの右側に黒色の三角形  が表示されます。
 - b. 黒色の三角形をクリックすると、ドロップダウン メニューが表示されます。
 - c. [Sort Ascending (昇順に並べ替え)] または [Sort Descending (降順に並べ替え)] を選択します。

新たに選択した列見出しに、上向きまたは下向きの三角形が表示されます。

ダイアログ ボックスのサイズ変更

ほとんどのダイアログ ボックスはサイズを変更できませんが、[Event Log (イベント ログ)] ダイアログ ボックスなどのいくつかのダイアログ ボックスは、詳細情報が一度に表示されるように、サイズを変更できます。

▶ ダイアログ ボックスのサイズを変更するには、次の手順に従います。

1. ダイアログ ボックスの任意の境界にマウス ポインタを置きます。
2. マウス ポインタが双方向の矢印になったら、境界を縦方向または横方向にドラッグすると、ダイアログ ボックスを拡大または縮小できます。

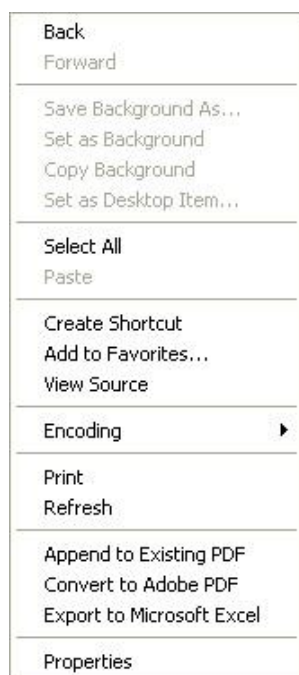
ブラウザで定義されたショートカット メニュー

Dominion PX の Web インタフェースで右クリックすると、Web ブラウザに組み込まれているショートカット メニューが表示される場合があります。

ショートカット メニューの機能は、ブラウザによって定義されています。たとえば、Internet Explorer® (IE) のショートカット メニューの「前に戻る」コマンドは、IE ブラウザの「戻る」ボタンと同じように機能します。どちらの機能を使用しても、前のページに戻ります。

各ショートカット メニューのコマンドまたは項目については、Web ブラウザに付属するオンライン ヘルプまたはマニュアルを参照してください。

次に示すのは、IE ブラウザのショートカット メニューの図です。使用可能なメニュー コマンドまたはメニュー項目は、Web ブラウザのバージョンによって若干異なる場合があります。



ダッシュボードの表示

Web インタフェースにログインすると、デフォルトではダッシュボード ページが表示されます。このページには、Dominion PX デバイスのステータスの概要が表示されます。

このページは、インレット、サーキット ブレーカなどのコンポーネントタイプに準じた各種セクションに分かれています。

注: センサーの表示値の行が色付きで表示されている場合は、センサーの表示値がすでにいずれかのしきい値を超えているか、サーキット ブレーカーがトリップしています。詳細については、『**The Yellow- or Red-Highlighted Reading (表示値の黄色表示または赤色表示)**』82p. の「**測定値の黄色表示または赤色表示**」を参照してください。

階層ツリーで他のアイコンをクリックすると、ダッシュボード ページが切り替わります。ダッシュボード ページに戻るには、[Dashboard (ダッシュボード)] アイコンをクリックします。

ダッシュボード ページが開かれると、以下の操作によって、特定のデータを表示または非表示にすることができます。

▶ **セクションを折りたたむには、次の手順に従います。**

1. 折りたたむセクションを探します。
2. セクション タイトルの前の上向き矢印  をクリックします。セクションに固有のデータが非表示になります。

▶ **折りたたんだセクションを展開するには、次の手順に従います。**

1. 展開するセクションを探します。
2. セクション タイトルの前の下向き矢印  をクリックします。セクションに固有のデータが表示されます。

警告対象のセンサー

ダッシュボード ページには、内部センサーまたは外部センサーによって検出された臨界状態または重大な状況のみを表示するセクションがあり、何らかのアクションを実行するようにユーザに警告できるようになっています。このセクションには、[Alerted Sensors (警告対象のセンサー)] というラベルが付いています。

[Alerted Sensors (警告対象のセンサー)] セクションには、以下のいずれかまたはすべてがリストされます。

- しきい値が有効な場合に上位または下位のしきい値を超えたセンサー
- 作動したサーキット ブレーカ
- アラーム状態になったディスクリット (オン/オフ) センサー

Alerted Sensors		
Sensor	Reading	State
Inlet H L1-L2 RMS Voltage	427 V	above upper warning
Temperature 1	20.7 °C	below lower warning
Temperature 2	20.2 °C	below lower warning
On/Off 1		alarmed

このセクションの背景色については、「**測定値の黄色表示または赤色表示**『82p.』」を参照してください。

デバイス管理

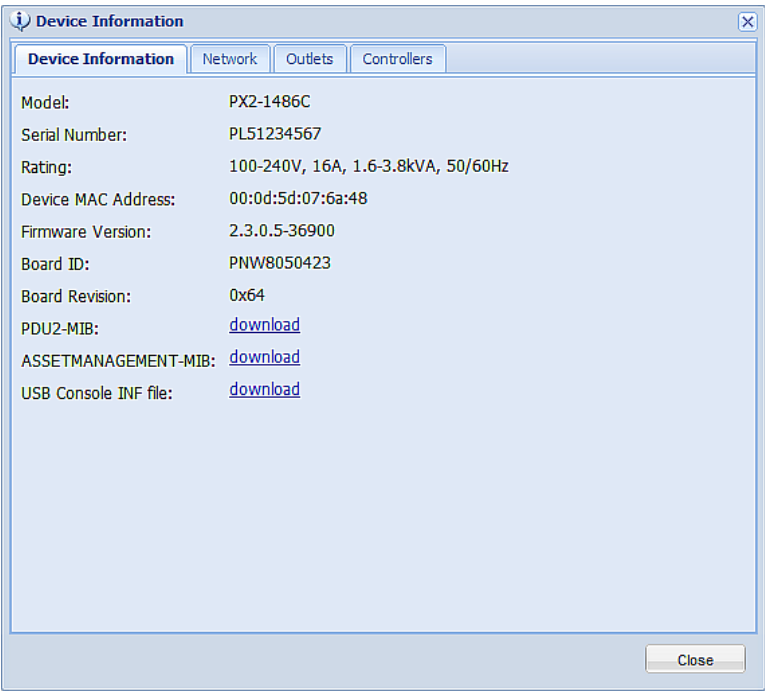
Web インタフェースを使用すると、基本的なハードウェア情報やソフトウェア情報の取得、Dominion PX への新しいデバイス名の指定、システムの日付と時刻の設定、および初期設定プロセス中に入力したネットワーク設定の変更を行うことができます。

PDU 情報の表示

使用している Dominion PX デバイスに固有の情報（インレットまたはアウトレット（コンセント）のタイプなど）を表示するには、[Device Information（デバイス情報）] ダイアログ ボックスを表示します。

▶ PDU 固有の情報を表示するには、次の手順に従います。

- 1. [Maintenance（メンテナンス）] > [Device Information（デバイス情報）] を選択します。[Device Information（デバイス情報）] ダイアログ ボックスが表示されます。



- 2. 表示する情報が含まれているタブをクリックします。使用可能なタブの数は、購入したモデルによって異なります。

タブ	データ
Device Information（デバイス情報）	一般的な PDU 情報（モデル名、シリアル番号、ファームウェア バージョン、ハードウェア リビジョンなど）。
[Network（ネットワーク）]	PDU 固有のネットワーク情報（現在のネットワーク モード、IPv4 アドレス、IPv6 アドレスなど）。 このタブには、PDU が USB カスケード構成の一部であるかどうか也表示されます。 「USB による PDU のカスケード接続」

タブ	データ
	『33p. 』を参照してください。
アウトレット (コンセント)	各アウトレット (コンセント) のタイプ、動作電圧、および定格電流。
Inlets (インレット)	各インレットのプラグ タイプ、定格電圧、定格電流。
Overcurrent Protectors (過電流プロテクタ)	各サーキット ブレーカのタイプ、定格電流、および保護されるアウトレット (コンセント)。
Controllers (コントローラ)	各インレットまたはアウトレット (コンセント) のコントローラのシリアル番号、ファームウェア バージョン、およびハードウェア バージョン。
Asset Strips (資産ストリップ)	資産センサーの ID、ブート バージョン、アプリケーション バージョン、およびプロトコル バージョン。

注: アウトレット (コンセント) の動作電圧は、インレットの定格電圧から導出されます。この計算の結果は、最も近い整数値 (ボルト) に丸められます。たとえば、最小電圧の計算が $380/\sqrt{3}=219.39$ の場合、Web インタフェースでは 219 V と表示されます。

- 必要に応じてダイアログ ボックスを拡大します。
- リストの並べ替え、または表示列の変更を行うことができます。
- [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

ヒント: ファームウェア バージョンは、*Dominion PX Explorer* ペインで PDU フォルダをクリックして表示することもできます。

PDU の名前付け

Dominion PX のデフォルトの名前は、*my PX* ですが、一意なデバイス名にすることができます。

▶ デバイス名を変更するには、次の手順に従います。

- PDU フォルダをクリックします。

注: PDU フォルダは、デフォルトでは「*my PX*」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、『*Naming the PDU (PDU のネーミング)* 90p. の「PDU の名前付け」参照先』を参照してください。

2. [設定] セクションの [Setup (セットアップ)] をクリックします。[Pdu Setup (PDU のセットアップ)] ダイアログ ボックスが開きます。
3. [Device Name (デバイス名)] フィールドに新しい名前を入力します。
4. [OK] をクリックして変更を保存します。

ネットワーク設定の変更

Web インタフェースを介して変更できるネットワーク設定には、有線設定、ワイヤレス設定、IPv4 設定、IPv6 設定が含まれています。

ネットワーク インタフェース設定の変更

Dominion PX がサポートするネットワーク インタフェースには、有線およびワイヤレスという 2 つのタイプがあります。ネットワーク インタフェース設定は、適用されるネットワーク モードに従って行う必要があります。「**ネットワークへの Dominion PX の接続『25p.』**」を参照してください。

有線ネットワーク設定

LAN インタフェースの速度とデュプレックス モードは、設置および設定プロセス中に設定されます。「**初期ネットワーク設定『26p.』**」を参照してください。

デフォルトでは、LAN の速度およびデュプレックス モードは [Auto (自動)] (自動) に設定されており、ほぼすべての環境でこのままで機能します。特殊な要件がある場合は、この設定を変更できます。

▶ ネットワーク インタフェース設定を変更するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Network (ネットワーク)] を選択します。[Network Configuration (ネットワーク設定)] ダイアログ ボックスが表示されます。
2. [Interface Settings (インタフェース設定)] タブが選択されています。選択されていない場合は、[Interface Settings (インタフェース設定)] タブをクリックします。
3. [Network Interface (ネットワーク インタフェース)] フィールドのドロップダウン矢印をクリックし、リストから [Wired (有線)] を選択します。
4. LAN 速度を変更するには、[Speed (速度)] フィールドのドロップダウン矢印をクリックし、リストからオプションを選択します。
 - Auto (自動): 自動ネゴシエーションによって最適な LAN 速度が自動的に決定されます。
 - 10 Mbit/s (100 メガビット/秒): LAN の速度は、常時 10Mbps です。
 - 100 Mbit/s (100 メガビット/秒): LAN の速度は、常時 100Mbps です。

5. デュプレックス モードを変更するには、[Duplex (デュプレックス)] フィールドのドロップダウン矢印をクリックし、リストからオプションを選択します。
 - Auto (自動): Dominion PX では、自動ネゴシエーションによって最適な送信モードが自動的に選択されます。
 - Full (全二重): データは、全二重で送信されます。
 - Half (半二重): データは、Dominion PX デバイスに対して半二重で送信されます。
6. [OK] をクリックして変更を保存します。

ヒント: LAN の状態 (速度、デュプレックス モードなど) は、[Current State (現在の状態)] フィールドで確認できます。

ワイヤレス ネットワーク設定

ワイヤレス SSID、PSK、および BSSID パラメータは、設置および設定プロセス中に設定されます。「**初期ネットワーク設定『26p.』**」を参照してください。Web インタフェースで変更できます。

▶ ワイヤレス インタフェース設定を変更するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Network (ネットワーク)] を選択します。[Network Configuration (ネットワーク設定)] ダイアログ ボックスが表示されます。
2. [Interface Settings (インタフェース設定)] タブが選択されています。選択されていない場合は、[Interface Settings (インタフェース設定)] タブをクリックします。
3. [Network Interface (ネットワーク インタフェース)] フィールドのドロップダウン矢印をクリックし、リストから [Wireless (ワイヤレス)] を選択します。
4. [Hardware State (ハードウェア状態)] フィールドをオンにして、Dominion PX デバイスでワイヤレス USB LAN アダプタが検出されたことを確認します。検出されない場合は、USB LAN アダプタがしっかり接続されているかどうか、またはサポートされているかどうかを確認します。「**ネットワークへの Dominion PX の接続『25p. の "ネットワークへの Dominion PX の接続" 参照』**」を参照してください。
5. [SSID (SSID)] フィールドにワイヤレス アクセス ポイント (AP) の名前を入力します。
6. BSSID を使用できる場合は、[Force AP BSSID (強制的に AP BSSID を使用)] チェックボックスをオンにし、[BSSID (BSSID)] フィールドに MAC アドレスを入力します。

注: BSSID は、ワイヤレス ネットワークのアクセス ポイントの MAC アドレスを参照します。

7. [Authentication (認証)] フィールドのドロップダウン矢印をクリックし、リストから適切なオプションを選択します。

オプション	説明
No Authentication (認証なし)	このオプションは、認証データが必要ないときに選択します。
PSK (PSK)	このオプションを選択する場合は事前共有キーが必要です。 ▪ [Pre-Shared Key (事前共有キー)] フィールドに PSK 文字列を入力します。
EAP – PEAP (EAP – PEAP)	PEAP は Protected Extensible Authentication Protocol の略です。 次の認証データが必要です。 ▪ 内部認証: Microsoft Challenge Authentication Protocol Version 2 (MSCHAPv2) のみがサポートされ、MSCHAPv2 をサポートするデータベースへの認証が可能です。 ▪ ID: EAP 認証のユーザ名を入力します。 ▪ パスワード: EAP 認証のパスワードを入力します。 ▪ CA 証明書: EAP 認証にサードパーティの CA 証明書が必要です。[Browse (参照)] をクリックして有効な証明書ファイルを選択します。 – 選択した証明書ファイルの内容を表示するには、[Show (表示)] をクリックします。 – 選択した証明書ファイルが無効な場合は、[Remove (削除)] をクリックします。次に、新しいファイルを選択します。

1. [OK] をクリックして変更を保存します。

ネットワーク設定の変更

Dominion PX は、設置および設定プロセス中に、ネットワーク接続も設定されます。「***Dominion PX の設定***『21p.』」を参照してください。必要に応じて、Web インタフェースを使用してネットワーク設定を変更できます。

インターネット プロトコルの選択

Dominion PX デバイスは、2 つのタイプのインターネット プロトコル (IPv4 と IPv6) をサポートしています。どちらか一方または両方のインターネット プロトコルを有効にすることができます。目的のインターネット プロトコルを有効にすることで、その有効にしたインターネット プロトコルに準拠することになるプロトコルには、次のようなものがあります。

- LDAP
- NTP
- SMTP
- SSH
- Telnet
- FTP
- SSL
- SNMP
- SysLog

▶ 適切なインターネット プロトコルを選択するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Network (ネットワーク)] を選択します。[Network Configuration (ネットワーク設定)] ダイアログ ボックスが表示されます。
2. [IP Protocol (IP プロトコル)] タブをクリックします。
3. 有効にするインターネット プロトコルのチェックボックスを 1 つ オンにします。
 - [IPv4 only (IPv4 のみ)]: すべてのインタフェースに対して IPv4 のみを有効にします。デフォルトではこの設定です。
 - [IPv6 only (IPv6 のみ)]: すべてのインタフェースに対して IPv6 のみを有効にします。
 - [IPv4 and IPv6 (IPv4 と IPv6)]: すべてのインタフェースに対して IPv4 と IPv6 の両方を有効にします。
4. 前の手順で [IPv4 and IPv6 (IPv4 と IPv6)] チェックボックスをオンにした場合は、DNS リゾルバから IPv4 アドレスと IPv6 アドレスの両方が返されたときに使用する IP アドレスを決定する必要があります。
 - [IPv4 Address (IPv4 アドレス)]: DNS サーバから返された IPv4 アドレスを使用します。
 - [IPv6 Address (IPv6 アドレス)]: DNS サーバから返された IPv6 アドレスを使用します。
5. [OK] をクリックして変更を保存します。

IPv4 設定の変更

IPv4 ネットワーク設定を変更する前に、IPv4 プロトコルを有効にする必要があります。「インターネット プロトコルの選択 『94p. 』」を参照してください。

▶ IPv4 の設定を変更するには、次の手順に従います。

- 1. [Device Settings (デバイス設定)] > [Network (ネットワーク)] を選択します。[Network Configuration (ネットワーク設定)] ダイアログ ボックスが表示されます。
- 2. [IPv4 Settings (IPv4 設定)] タブをクリックします。
- 3. [IP Auto Configuration (IP 自動設定)] フィールドのドロップダウン矢印をクリックし、リストから目的のオプションを選択します。

オプション 説明	
DHCP	Dominion PX を自動設定するには、[DHCP] を選択します。DHCP を選択した場合、優先 DHCP ホスト名を入力できます。ただし、この設定はオプションです。[Preferred Hostname (優先ホスト名)] フィールドにホスト名を入力します。 ホスト名には、次のような条件が適用されます。 ▪ 英数字やハイフンで構成されます。 ▪ 先頭および末尾をハイフンにすることはできません。 ▪ 63 文字を超えることはできません。 ▪ 句読点、空白文字などの記号は使用できません。 必要に応じて、[Specify DNS server manually (DNS サーバを手動で指定する)] チェックボックスをオンにします。次に、[Primary DNS Server (プライマリ DNS サーバ)] フィールドにプライマリ DNS サーバのアドレスを入力します。セカンダリ DNS サーバと DNS サフィックスはオプションです。
Static (固定)	手動で IP アドレスを割り当てるには、[Static (固定)] を選択し、対応するフィールドに次の情報を入力します。 ▪ IP アドレス ▪ ネットマスク ▪ ゲートウェイ ▪ プライマリ DNS サーバ ▪ セカンダリ DNS サーバ (オプション) ▪ DNS サフィックス (オプション)

- 4. [OK] をクリックして変更を保存します。

注: *Dominion PX* では、最大 3 台の DNS サーバがサポートされています。2 台の IPv4 DNS サーバと 2 台の IPv6 DNS サーバを利用できる場合は、*Dominion PX* でプライマリ IPv4 DNS サーバとプライマリ IPv6 DNS サーバのみが使用されます。

IPv6 設定の変更

IPv6 ネットワーク設定を変更する前に、IPv6 プロトコルを有効にする必要があります。「インターネット プロトコルの選択」『94p.』を参照してください。

▶ IPv6 の設定を変更するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Network (ネットワーク)] を選択します。[Network Configuration (ネットワーク設定)] ダイアログ ボックスが表示されます。
2. [IPv6 Settings (IPv6 設定)] タブをクリックします。
3. [IP Auto Configuration (IP 自動設定)] フィールドのドロップダウン矢印をクリックし、リストから目的のオプションを選択します。

オプション	説明
Automatic (自動)	<i>Dominion PX</i> を自動設定するには、[Automatic (自動)] を選択します。 このオプションを選択した場合、優先ホスト名を入力できます。ただし、この設定はオプションです。[Preferred Hostname (優先ホスト名)] フィールドにホスト名を入力します。 ホスト名には、次のような条件が適用されます。 ▪ 英数字やハイフンで構成されます。 ▪ 先頭および末尾をハイフンにすることはできません。 ▪ 63 文字を超えることはできません。 ▪ 句読点、空白文字などの記号は使用できません。 必要に応じて、[Specify DNS server manually (DNS サーバを手動で指定する)] チェックボックスをオンにします。次に、[Primary DNS Server (プライマリ DNS サーバ)] フィールドにプライマリ DNS サーバのアドレスを入力します。セカンダリ DNS サーバと DNS サフィックスはオプションです。
Static (固定)	手動で IP アドレスを割り当てるには、[Static (固定)] を選択し、対応するフィールドに次の情報を入力します。 ▪ IP アドレス

オプション	説明
	■ ゲートウェイ ■ プライマリ DNS サーバ ■ セカンダリ DNS サーバ (オプション) ■ DNS サフィックス (オプション)

4. [OK] をクリックして変更を保存します。

注: *Dominion PX* では、最大 3 台の DNS サーバがサポートされています。2 台の IPv4 DNS サーバと 2 台の IPv6 DNS サーバを利用できる場合は、*Dominion PX* でプライマリ IPv4 DNS サーバとプライマリ IPv6 DNS サーバのみが使用されます。

DNS サーバの役割

インターネット通信は、IP アドレスに基づいて実行されるため、ドメイン名 (ホスト名) を対応する IP アドレスにマッピングするための適切な DNS サーバ設定が必要です。この設定がなければ、*Dominion PX* から指定したホストに接続できません。

このため、LDAP 認証には DNS サーバの設定が重要です。DNS が適切に設定されていると、*Dominion PX* で LDAP サーバの名前を IP アドレスに解決して接続を確立できます。SSL 暗号化が有効になっている場合は、LDAP サーバの指定に使用できるのは完全修飾ドメイン名のみであるため、DNS サーバの設定が重要です。

LDAP 認証の詳細については、「**LDAP 認証の設定**『146p.』」を参照してください。

ネットワーク サービス設定の変更

Dominion PX がサポートするネットワーク通信サービスには、HTTPS、HTTP、Telnet、および SSH があります。

HTTPS および HTTP では、Web インタフェースにアクセスすることができ、Telnet および SSH では、**コマンド ライン インタフェース**『274p. の「**コマンド ライン インタフェースの使用**」参照』にアクセスできます。

デフォルトでは、SSH が有効で Telnet は無効になっています。また、サポートされているサービス用のすべての TCP ポートは、標準ポートに設定されています。デフォルトの設定は、必要に応じて変更できます。

注: *Telnet* アクセスは、公開通信であり、安全ではないため、デフォルトでは無効になっています。

さらに、*Dominion PX* では SNMP プロトコルもサポートされています。

HTTP(S) 設定の変更

HTTPS では、SSL (Secure Sockets Layer) テクノロジを使用して Dominion PX デバイスに対するすべての送受信トラフィックが暗号化されるため、HTTPS は HTTP より安全なプロトコルです。

デフォルトでは、Dominion PX デバイスに HTTP 経由でアクセスすると、自動的に HTTPS にリダイレクトされます。「**HTTPS 暗号化を強制的に使用**『123p.』」を参照してください。

▶ **HTTP または HTTPS ポート設定を変更するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Network Services (ネットワークサービス)] > [HTTP] を選択します。[HTTP Settings (HTTP 設定)] ダイアログ ボックスが表示されます。
2. HTTP または HTTPS 用に別のポートを使用するには、対応するフィールドに新しいポート番号を入力します。有効な範囲は 1 ～ 65535 です。

警告: 複数のネットワーク サービスで同じ TCP ポートを共有することはできません。

3. [OK] をクリックして変更を保存します。

SSH 設定の変更

コマンド ライン インタフェースへの SSH アクセスを有効または無効にすることや、SSH サービス用のデフォルトの TCP ポートを変更することができます。さらに、ログインするときに、パスワードを使用するか、SSH 接続を介して公開キーを使用するかを決定できます。

▶ **SSH サービス設定を変更するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Network Services (ネットワークサービス)] > [SSH] を選択します。[SSH Settings (SSH 設定)] ダイアログ ボックスが表示されます。
2. 別のポートを使用するには、フィールドに新しいポート番号を入力します。有効な範囲は 1 ～ 65535 です。
3. SSH アプリケーションを有効にするには、[Enable SSH (SSH を有効にする)] チェックボックスをオンにします。アプリケーションを無効にするには、このチェックボックスをオフにします。
4. 異なる認証方法を選択するには、いずれかのチェックボックスをオンにします。
 - [Allow password authentication only (パスワード認証のみを許可する)]: パスワードベースのログインのみを有効にします。

- [Allow public key authentication only (公開キー認証のみを許可する)]: 公開キーベースのログインのみを有効にします。
 - [Allow password and public key authentication (パスワード認証と公開キー認証を許可する)]: パスワードベースと公開キーベースの両方のログインを有効にします。デフォルトではこの設定です。
5. [OK] をクリックして変更を保存します。

公開キーベースの認証が選択されている場合、SSH 接続を介してログインするには、各ユーザ プロファイルの有効な SSH 公開キーを入力する必要があります。「**ユーザ プロファイルの作成**『114p.』」を参照してください。

Telnet 設定の変更

コマンド ライン インタフェースへの Telnet アクセスを有効または無効にすることや、Telnet サービス用のデフォルトの TCP ポートを変更することができます。

▶ Telnet サービス設定を変更するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Network Services (ネットワーク サービス)] > [Telnet] を選択します。[Telnet Settings (Telnet 設定)] ダイアログ ボックスが表示されます。
2. 別のポートを使用するには、フィールドに新しいポート番号を入力します。有効な範囲は 1 ～ 65535 です。
3. Telnet アプリケーションを有効にするには、[Enable Telnet Access (Telnet アクセスを有効にする)] チェックボックスをオンにします。アプリケーションを無効にするには、このチェックボックスをオフにします。
4. [OK] をクリックして変更を保存します。

SNMP の設定

SNMP マネージャと Dominion PX デバイスの間の SNMP 通信を有効または無効にすることができます。SNMP 通信を有効にすると、マネージャで各アウトレット（コンセント）の電力ステータスを取得して制御することができます。

さらに、組み込みの「System SNMP Trap Rule (システム SNMP トラップルール)」が有効になっている場合にまだトラップの送信先が設定されていない場合は、SNMP の送信先を設定する必要があります。「**イベントルールの設定**『179p.』」を参照してください。

▶ SNMP 通信を設定するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Network Services (ネットワークサービス)] > [SNMP] を選択します。[SNMP Settings (SNMP 設定)] ダイアログ ボックスが表示されます。

2. [SNMP v1 / v2c (SNMP v1 / v2c)] フィールドで [enable (有効にする)] チェックボックスをオンにして、SNMP v1 または v2c プロトコルを使用した SNMP マネージャとの通信を可能にします。
 - SNMP 読み取り専用コミュニティ スtring を [Read Community String (コミュニティ スtring の読み取り)] フィールドに入力します。通常、String は「public」です。
 - 読み取り/書き込みコミュニティ スtring を [Write Community String (コミュニティ スtring の書き込み)] フィールドに入力します。通常、String は「private」です。
3. [SNMP v3 (SNMP v3)] フィールドで [enable (有効にする)] チェックボックスをオンにして、SNMP v3 プロトコルを使用した SNMP マネージャとの通信を可能にします。

ヒント: SNMP v3 プロトコルを使用した、ユーザによる *Dominion PX* へのアクセスを許可または拒否できます。『暗号化された SNMP v3 のユーザの設定』『268p.』を参照してください。

4. SNMP MIB-II の sysContact 値を [sysContact] フィールドに入力します。
5. SNMP MIB-II の sysName 値を [sysName] フィールドに入力します。
6. SNMP MIB-II の sysLocation 値を [sysLocation] フィールドに入力します。
7. [OK] をクリックして変更を保存します。

重要: SNMP マネージャで、使用する *Dominion PX* の SNMP MIB をダウンロードする必要があります。このダイアログ ボックスで [Download MIB (MIB のダウンロード)] をクリックして、目的の MIB ファイルをダウンロードします。詳細については、「*SNMP MIB* のダウンロード」『270p.』を参照してください。

▶ **SNMP トラップの送信先を設定するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Network Services (ネットワーク サービス)] > [SNMP] を選択します。[SNMP Settings (SNMP 設定)] ダイアログ ボックスが表示されます。
2. [Trap (トラップ)] タブをクリックします。
3. [System Snmp Trap Event Rule (システム SNMP トラップ イベント ルール)] フィールドの [Enabled (有効)] チェックボックスをオンにします。
4. 次の操作を行って SNMP トラップの送信先を指定します。
 - a. [Host *x* (ホスト *x*)] フィールドに SNMP トラップの送信先を 3 つまで指定できます。*x* は 1 ~ 3 の数値です。
 - b. [Port *x* (ポート *x*)] フィールドに各送信先のポート番号を指定します。*x* は 1 ~ 3 の数値です。
 - c. [Community *x* (コミュニティ *x*)] フィールドに各送信先のコミュニティ スtring を指定します。*x* は 1 ~ 3 の数値です。
5. [OK] をクリックして変更を保存します。

ヒント: SNMP トラップの送信先の設定は、[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスでも設定できます。『アクションの変更』『217p.』を参照してください。

Modbus 設定の変更

Dominion PX への Modbus アクセスまたは Modbus 読み取り専用モードを有効または無効にすることや、Modbus サービス用のデフォルトの TCP ポートを変更することができます。

► **Modbus サービス設定を変更するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Network Services (ネットワークサービス)] > [Modbus] を選択します。[Modbus Settings (Modbus 設定)] ダイアログ ボックスが表示されます。
2. 別のポートを使用するには、フィールドに新しいポート番号を入力します。有効な範囲は 1 ~ 65535 です。
3. Modbus アクセスを有効にするには、[Enable Modbus/TCP Access (Modbus/TCP アクセスを有効にする)] チェックボックスをオンにします。アプリケーションを無効にするには、このチェックボックスをオフにします。
4. Modbus 読み取り専用モードを有効にするには、[Enable read-only mode (読み取り専用モードを有効にする)] チェックボックスをオンにします。アプリケーションを無効にするには、このチェックボックスをオフにします。
5. [OK] をクリックして変更を保存します。

サービス アドバタイズメントの有効化

Dominion PX は、IP ネットワークを使用して到達できるすべての有効なサービスをアドバタイズします。この機能は、DNS-SD (ドメイン ネーム システム - サービス ディスカバリ) および mDNS (マルチキャスト DNS) を使用します。アドバタイズされたサービスは、DNS-SD および mDNS を実装したクライアントによって検出されます。

アドバタイズされるサービスには、以下が含まれます。

- HTTP
- HTTPS
- Telnet
- SSH
- Modbus
- json-rpc
- SNMP

デフォルトでは、この機能は有効になっています。

▶ サービス アドバタイズメントを有効にするには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Network Services (ネットワーク サービス)] を選択し、[Service Advertisement (サービス アドバタイズメント)] チェックボックスをオンにします。
2. 確認メッセージで [Yes (はい)] をクリックして、ゼロ構成アドバタイズメントに切り替えます。機能が有効になり、メニューの [Service Advertisement (サービス アドバタイズメント)] チェックボックスがオンになります。

▶ サービス アドバタイズメントを無効にするには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Network Services (ネットワーク サービス)] を選択し、[Service Advertisement (サービス アドバタイズメント)] チェックボックスをオフにします。
2. 確認メッセージで [Yes (はい)] をクリックして、ゼロ構成アドバタイズメントをオフにします。機能が無効になり、メニューの [Service Advertisement (サービス アドバタイズメント)] チェックボックスがオフになります。

日付と時刻の設定

Dominion PX デバイスの内部時計は手動で設定するか、ネットワーク タイム プロトコル (NTP) サーバにリンクし、サーバに Dominion PX の日付と時刻の設定を実行させます。

▶ 日付と時刻を設定するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Date/Time (日付/時刻)] を選択します。[Configure Date/Time Settings (日付/時刻の設定)] ダイアログボックスが表示されます。
2. [Time Zone (タイム ゾーン)] フィールドのドロップダウン矢印をクリックし、リストからタイム ゾーンを選択します。
3. タイム ゾーンで夏時間が実施されている場合は、[Automatic Daylight Saving Time Adjustment (自動夏時間調整)] チェックボックスがオンになっていることを確認します。

選択したタイム ゾーンに夏時間ルールを適用できない場合は、チェックボックスが設定できなくなっています。

4. 次のいずれかの方法で、日付と時刻を設定します。
 - 日付と時刻をカスタマイズするには、[User Specified Time (ユーザーによる指定時刻)] ラジオ ボタンを選択し、該当するフィールドに日付と時刻を入力します。yyyy-mm-dd 形式で日付を指定し、hh:mm:ss 形式で時刻を指定します。
 - 日付を設定するには、[Date (日付)] フィールドの既存の数値を削除して新しい数値を入力するか、カレンダー アイコン  をクリックして日付を選択します。
 - 時刻には 24 時間形式を使用し、1:00pm の場合は「13」、2:00pm の場合は「14」、その他同様に入力します。時刻を入力するには、時、分、秒の各フィールドの既存の数値を削除して新しい数値を入力するか、矢印  をクリックして各数値を調整します。
 - NTP サーバで日時を設定するには、[Synchronize with NTP Server (NTP サーバと同期)] ラジオ ボタンを選択します。NTP サーバの割り当て方法には、次の 2 種類があります。

- DHCP によって割り当てられた NTP サーバを使用するには、[Always use the servers below and ignore DHCP-provided servers (常に以下のサーバのみを使用し、DHCP が提供するサーバを無視する)] チェックボックスをオフにします。この方法は、IPv4 または IPv6 DHCP が有効である場合のみ便利です。
- 手動で指定された NTP サーバを使用するには、[Always use the servers below and ignore DHCP-provided servers (常に以下のサーバのみを使用し、DHCP が提供するサーバを無視する)] チェックボックスをオンにし、[First Time Server (1 つ目のタイム サーバ)] フィールドでプライマリ NTP サーバを指定します。セカンダリ NTP サーバはオプションです。

注: IPv4 または IPv6 DHCP を介して Dominion PX デバイスの IP アドレスが割り当てられている場合は、NTP サーバを自動的に検出できます。NTP サーバのアドレスが検出されると、[First Time Server (1 つ目のタイム サーバ)] フィールドおよび [Second Time Server (2 つ目のタイム サーバ)] フィールドに入力したデータが上書きされます。

5. [OK] をクリックして変更を保存します。

重要: Raritan の Power IQ を使用して Dominion PX を管理する場合は、同じ日付/時刻または NTP 設定を持つするように Power IQ と Dominion PX を設定する必要があります。

カレンダーの使用法

[Date (日付)] フィールドの横のカレンダー アイコン  は、年月日を手早く変更できる便利なツールです。



▶ カレンダーによる日付の選択

1. カレンダーに表示されている年を変更するには、次のいずれかの操作を実行します。
 - Ctrl+上矢印または Ctrl+下矢印を押して年を切り替えます。
 - 年の近くの ▼ をクリックして、年と月のリストを表示します。設定する年を右側のリストから選択し、[OK] をクリックします。設定する年がリストに表示されない場合は、◀ または ▶ をクリックしてその他の年を表示します。



2. カレンダーに表示されている月を変更するには、次のいずれかの操作を実行します。
 - Ctrl+右矢印または Ctrl+左矢印を押して月を切り替えます。
 - カレンダー上部の ◀ または ▶ をクリックして月を切り替えます。
 - 年の近くの ▼ をクリックして、年と月のリストを表示します。設定する月を左側のリストから選択し、[OK] をクリックします。
3. 日を選択するには、カレンダーの日をクリックします。
 - 今日を選択する場合は、[Today (今日)] をクリックします。

注: カレンダーでは、今日の日付には赤色の枠が付いています。

拡張ポートの設定

Dominion PX デバイスでは、FEATURE ポートに次のいずれかのデバイスを接続できます。

- Raritan 資産管理センサー (資産センサー)。「**資産管理センサーの接続 (オプション)**」『42p.』」を参照してください。
- PDU 使用のための Raritan コンピュータ インタフェース モジュール (CIM)。「**Dominion KX II 設定**」『457p.』」を参照してください。
- Schroff® LHX-20 または LHX-40 ヒート エクスチェンジャ。「**Schroff LHX ヒート エクスチェンジャの接続 (オプション)**」『53p.』」を参照してください。

デフォルトでは、FEATURE ポートは、接続されているデバイスを自動的に検出して表示できます。ただし、Schroff® LHX-20 または LHX-40 デバイスだけは例外で、これらを Dominion PX で検出または表示するには、事前に LHX サポートを有効にしておく必要があります。「**Schroff LHX ヒート エクスチェンジャの管理**」『254p.』」を参照してください。

必要なデバイスだけが Dominion PX Web インタフェースに表示されるように、FEATURE ポートに適用されるモードを変更できます。

FEATURE ポートを設定するには、次の手順に従います。

1. [Feature Port (拡張ポート)] フォルダをクリックします。[Feature Port (拡張ポート)] ページが右側のペインに表示されます。
2. [Feature Port (拡張ポート)] ページで、ポート番号 1 のデバイスを選択し、[Setup (設定)] をクリックします。[Feature Port Setup (拡張ポートの設定)] ダイアログ ボックスが表示されます。
3. [Detected Mode (検出モード)] フィールドで、目的のモードを選択します。
 - Auto (自動): Dominion PX は、FEATURE ポートに接続されているデバイスを自動的に検出して表示します。これはデフォルトです。
 - [Disabled (無効)]: FEATURE ポートが無効になり、接続されているデバイスの検出および表示は行われません。
 - [Pinned (固定)]: Dominion PX は、接続されているデバイスや選択されたデバイスが検出されるかどうかにかかわらず、選択されたデバイス タイプを常に表示します。利用可能なデバイス タイプを次に示します。

デバイス タイプ 説明

資産ストリップ	Raritan 資産センサー。

デバイス タイプ	説明
Power CIM	Raritan Power CIM、D2CIM-PWR。この CIM は、Dominion PX を Raritan デジタル KVM スイッチである Dominion KX II に接続するために使用されます。
LHX-20	Schroff® LHX-20 ヒート エクスチェンジャ。このデバイス タイプは、LHX サポートを有効にした後にのみ使用可能です。
LHX-40	Schroff® LHX-40 ヒート エクスチェンジャ。このデバイス タイプは、LHX サポートを有効にした後にのみ使用可能です。

4. [OK] をクリックして変更を保存します。

シリアル ポートの設定

Dominion PX デバイスの「CONSOLE / MODEM」というラベルが付いたシリアル ポートのボーレート (bps) を変更できます。デフォルトのボーレートは 115200 bps です。Dominion PX を別の Raritan 製品とシリアル インタフェースで統合した場合のみ、ボーレートの調整が必要になることがあります。シリアル ポートを介して Raritan 製品と接続する前にボーレートを変更してください。先に接続すると、通信の問題が発生します。

注: シリアル ポート設定は、Dominion PX を Raritan の Dominion LX KVM スイッチとともに使用する場合に特に役立ちます。Dominion LX では、シリアル インタフェースを介した通信では 19200 bps のみをサポートしています。

▶ シリアル ポートのボーレート設定を変更するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Serial Port Settings (シリアル ポート設定)] を選択します。[Serial Port Configuration (シリアル ポート設定)] ダイアログ ボックスが表示されます。
2. [Baud Rate (ボーレート)] フィールドのドロップダウン矢印をクリックし、リストから目的のボーレートを選択します。

デバイスの高度の指定

Raritan 空気差圧センサーが接続されている場合、Dominion PX デバイスの海拔高度を指定する必要があります。これは、デバイスの高度が高度補正率に関連付けられているためです。「**高度補正率**『467p.』」を参照してください。

デフォルトの高度測定単位はメートルです。ユーザ証明書に応じて、測定単位をメートルとフィートの間で切り替えることができます。「**測定単位の変更**『242p.』」を参照してください。

▶ **Dominion PX デバイスの高度を指定するには、次の手順に従います。**

1. PDU フォルダをクリックします。

注：PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「**Naming the PDU (PDU のネーミング)**『90p. の PDU の名前付け参照先』」を参照してください。

2. [設定] セクションの [Setup (セットアップ)] をクリックします。[Pdu Setup (PDU のセットアップ)] ダイアログ ボックスが開きます。
3. [Altitude (高度)] フィールドに整数値を入力します。表示される測定単位によって有効な数値の範囲が異なります。
 - メートル (m) の場合、値の範囲は 0 ～ 3000 です。
 - フィート (ft) の場合、値の範囲は 0 ～ 9842 です。
4. [OK] をクリックして変更を保存します。

データ ロギングの設定

Dominion PX では、メモリ バッファにセンサーあたり 120 個の測定値を保存できます。このメモリ バッファは、データ ログと呼ばれます。データ ログ内のセンサー測定値は、SNMP を使用して取得できます。

[Measurements Per Log Entry (ログ エントリごとの測定値)] フィールドを使用して、測定値をデータ ログに書き込む頻度を設定できます。〈ProductName〉の内部センサーは 1 秒ごとに測定されるため、たとえば値 60 を指定すると、測定値は 1 秒に 1 回データ ログに書き込まれます。センサーあたり 120 個の測定値を保存できるため、値 60 を指定した場合、直近の 2 時間の測定値をログに保存できます。その後はログ内の最も古い測定値が上書きされます。

測定値がログに書き込まれるたびに、センサーごとに 3 つの値 (平均値、最小値、および最大値) が書き込まれます。たとえば、測定値が毎分書き込まれる場合、その前の 60 秒間に発生したすべての測定の平均値が最小測定値および最大測定値とともにログに書き込まれます。

このユーザ ガイドで説明している Raritan PDU モデルでは、アウトレット (コンセント) レベルの測定データは使用できません。

注: この機能を使用するには、Dominion PX の SNMP エージェントを有効にする必要があります。詳細については、『SNMP の有効化』[『267p.』](#)を参照してください。さらに、NTP タイム サーバを使用すると、測定値に正確なタイム スタンプが適用されます。

データ ロギングの有効化

デフォルトでは、データ ロギングは無効になっています。「Administrator (管理者)」または「Change Data Logging Settings (データ ロギング設定の変更)」の権限のあるユーザだけが、この機能を有効または無効にすることができます。「[役割の設定](#)」[『119p.』](#)を参照してください。

▶ データ ロギング機能を設定するには、次の手順に従います。

1. [Device Settings (デバイスの設定)] > [Data Logging (データ ロギング)] を選択します。[Data Logging Options (データ ロギング オプション)] ダイアログ ボックスが表示されます。
2. データ ロギング機能を有効にするには、[Enable Data Logging (データ ロギングを有効にする)] フィールドの [enable (有効にする)] チェックボックスをオンにします。
3. [Measurements Per Log Entry (ログ エントリごとの測定値)] フィールドに数値を入力します。有効な範囲は 1 ～ 600 です。デフォルトは 60 です。

4. すべてのセンサーのロギングが有効になっていることを確認します。有効になっていない場合は、[Enable All in Page (ページのすべてを有効にする)] をクリックしてすべてのセンサーを選択します。
5. [OK] をクリックして変更を保存します。

重要: 手順 4 で **Dominion PX** の個々のセンサーのロギングを有効または無効にすることができますが、それはお勧めしません。この機能は今後削除される可能性があります。

SMTP の設定

Dominion PX の設定により、特定の管理者に電子メールで警告またはイベント メッセージを送信することができます。そのためには、Dominion PX の SMTP 設定を指定して、SMTP サーバと送信者の電子メール アドレスを入力する必要があります。

注: 電子メール通知を送信するためのイベント ルールの作成方法については、「イベント ルールの設定 [179p.]」を参照してください。

▶ SMTP サーバを設定するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [SMTP Server (SMTP サーバ)] を選択します。[SMTP Server Settings (SMTP サーバ設定)] ダイアログ ボックスが表示されます。
2. [Server Name (サーバ名)] フィールドにメール サーバの名前または IP アドレスを入力します。
3. [Port (ポート)] フィールドに SMTP サーバのポート番号を入力します。デフォルトは 25 です。
4. Sender Email Address (送信者の電子メール アドレス) フィールドに、送信者の電子メール アドレスを入力します。
5. [Number of Sending Retries (送信の再試行回数)] フィールドに電子メール送信の再試行回数を入力します。デフォルトの再試行回数は 2 回です。
6. [Time Interval Between Sending Retries (in minutes) (送信の再試行間隔 (分))] フィールドに電子メール送信の再試行間隔を入力します。この時間の単位は分です。デフォルトは 2 分です。
7. SMTP サーバでパスワード認証が要求される場合は、次の操作を実行します。
 - a. [Server Requires Authentication (サーバで認証が要求される)] チェックボックスをオンにします。
 - b. [User Name (ユーザ名)] フィールドにユーザ名を入力します。
 - c. [Password (パスワード)] フィールドにパスワードを入力します。
8. SMTP の設定を行った後は、その設定で正常に動作するかどうかを確認するため、テストを実行します。次の手順を実行します。

- a. [Recipient Email Addresses (受信者の電子メール アドレス)] フィールドに受信者の電子メール アドレスを入力します。複数の電子メール アドレスを区切る場合は、カンマを使用します。
 - b. [Send Test Email (テスト電子メールの送信)] をクリックします。
9. [OK] をクリックして変更を保存します。
 10. 受信者が電子メールを正常に受信するかどうかを確認します。

EnergyWise の設定

Cisco® EnergyWise エネルギー管理アーキテクチャが実装されている場合、Dominion PX デバイスが Cisco EnergyWise ドメインに含まれるように、このデバイスに実装されている Cisco EnergyWise エンドポイントを有効にすることができます。

Dominion PX に実装されている Cisco EnergyWise 機能は、デフォルトでは無効になっています。

► **Cisco EnergyWise を設定するには、次の手順に従います。**

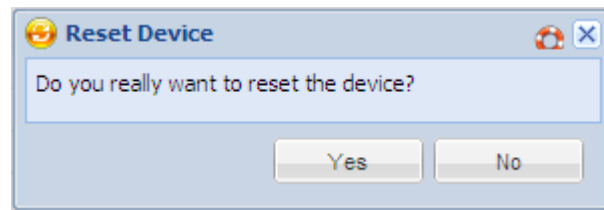
1. [Device Settings (デバイスの設定)] > [EnergyWise (EnergyWise)] を選択します。[EnergyWise Configuration (EnergyWise 設定)] ダイアログボックスが表示されます。
2. [Enable EnergyWise (EnergyWise を有効にする)] フィールドで、[enable (有効)] チェックボックスをオンにして、Cisco EnergyWise 機能を有効にします。
3. [Domain name (ドメイン名)] フィールドに、Dominion PX が属している Cisco EnergyWise ドメインの名前を入力します。ドメイン名は、最大 127 文字の ASCII の表示可能文字で構成されます。
 - 空白文字とアスタリスクは使用できません。
4. [Domain password (ドメイン パスワード)] フィールドに、Cisco EnergyWise ドメインに入るための認証パスワード (シークレット) を入力します。パスワードは、最大 127 文字の ASCII の表示可能文字で構成されます。
 - 空白文字とアスタリスクは使用できません。
5. [Port (ポート)] フィールドに、Cisco EnergyWise ドメインで通信するための User Datagram Protocol (UDP) ポート番号を入力します。ポート番号の範囲は 1 ~ 65535 です。デフォルトは 43440 です。
6. [Polling interval (ポーリング間隔)] フィールドに、Cisco EnergyWise ドメインで Dominion PX を照会する頻度を指定します。ポーリング間隔の範囲は 30 ~ 600 秒です。デフォルトは 180 秒です。
7. [OK] をクリックして変更を保存します。

Dominion PX デバイスの再起動

Web インタフェースを介して Dominion PX デバイスをリモートから再起動できます。

▶ デバイスをリブートするには、次の手順に従います。

1. [Maintenance (メンテナンス)] > [Unit Reset (本体のリセット)] を選択します。[Reset Device (デバイスのリセット)] ダイアログ ボックスが表示されます。



2. [Yes (はい)] をクリックして、Dominion PX を再起動します。
3. 操作の残り時間を示すカウントダウン タイマーとともに、メッセージが表示されます。完了までに約 1 分かかります。
4. リセットが完了すると、[Login (ログイン)] ページが表示されます。これで、Dominion PX デバイ스에 로그인할 수 있습니다。

注: リセットが完了してもログイン ページにリダイレクトされない場合は、メッセージ内の下線付きの文字列「*this link (このリンク)*」をクリックしてください。

[User Management (ユーザ管理)]

Dominion PX には、1 つのユーザ プロファイル (**admin**) が組み込まれており、そのプロファイルが初回のログインおよび設定に使用されます。このプロファイルでは、システムとアウトレット (コンセント) に対するすべての権限が与えられているので、システム管理者用に予約しておく必要があります。管理者を削除することはできません。また、その権限 (SNMP v3 権限を除く) をユーザが設定することはできません。

すべてのユーザにユーザ プロファイルを設定する必要があります。プロファイルには、ログイン名とパスワードを指定し、ユーザに関する追加 (任意) 情報を登録します。どのユーザ プロファイルにも、ユーザのシステム権限とアウトレット (コンセント) の権限を決定するために少なくとも 1 つの役割が必要です。「**役割の設定** 『119p.』」を参照してください。

ヒント: デフォルトでは、複数のユーザが同じログイン名で同時にログインできます。

ユーザ プロファイルの作成

新規ユーザを作成すると、Dominion PX への新しいログインが追加されます。

▶ ユーザ プロファイルを作成するには、以下の手順に従います。

1. [User Management (ユーザ管理)] > [Users (ユーザ)] を選択します。
[Manage Users (ユーザの管理)] ダイアログ ボックスが表示されます。
2. [New (新規)] をクリックします。[Create New User (ユーザの新規作成)] ダイアログ ボックスが表示されます。
3. ユーザに関する情報を、対応するフィールドに入力します。[User Name (ユーザ名)]、[Password (パスワード)]、[Confirm Password (パスワードの確認)] の各フィールドは、入力が必要であることを注意してください。

フィールド	入力内容
User Name (ユーザ名)	ユーザが Dominion PX にログインするために入力する名前。 ■ 名前として設定できる文字数は 4 ～ 32 文字です。 ■ パスワードの大文字と小文字は区別されます。 ■ 空白文字は使用できません。
Full Name (フル ネーム)	ユーザの姓名。
Password (パスワード)、 Confirm Password (パスワードの確認)	ユーザがログインするために入力するパスワード。始めに [Password (パスワード)] フィールドに入力し、[Confirm Password (パスワードの確認)] フィールドにもう一度入力します。 ■ パスワードとして設定できる文字数は 4 ～ 32 文字です。 ■ パスワードの大文字と小文字は区別されます。 ■ 空白文字を使用できます。
Telephone Number (電話番号)	ユーザに連絡するための電話番号です。
eMail Address (電子メール アドレス)	ユーザに連絡するための電子メール アドレス。 ■ 電子メール アドレスとして設定できる文字数は最大 32 文字です。

フィールド	入力内容
	パスワードの大文字と小文字は区別されます。

4. [Enabled (有効)] チェックボックスをオンにします。オンにしなかった場合、ユーザは Dominion PX デバイスにログインできません。
5. このチェックボックスをオンにした後、ユーザが初めてログインしたときにユーザにパスワードの変更を求める場合は、[Force password change on next login (次回ログイン時にパスワードを変更させる)] チェックボックスをオンにします。
6. [SNMPv3] タブをクリックし、SNMPv3 のアクセス権限を設定します。デフォルトでは、権限は無効になっています。
 - a. このユーザの SNMPv3 アクセスを許可するには、[Enable SNMPv3 access (SNMPv3 アクセスを有効にする)] チェックボックスをオンにします。SNMPv3 のアクセスを許可しない場合は、このチェックボックスはオフのままにしておきます。

注: SNMPv3 アクセスを有効にするには、SNMPv3 プロトコルを有効にする必要があります。『SNMP の設定 100p.』を参照してください。

- b. SNMPv3 アクセス権限を有効にした場合は、SNMPv3 パラメータを設定します。

フィールド	説明
Security Level (セキュリティ レベル)	ドロップダウン矢印をクリックし、優先セキュリティ レベルをリストから選択します。 - NoAuthNoPriv: 認証なし、プライバシーなし。 - AuthNoPriv: 認証あり、プライバシーなし。 - AuthPriv: 認証あり、プライバシーあり。デフォルトではこの設定です。
Use Password as Authentication Pass Phrase (パスワードを認証パス フレーズとして使用)	このチェックボックスは、AuthNoPriv または AuthPriv が選択されている場合にのみ設定できます。 このチェックボックスをオンにした場合、認証パス フレーズは、ユーザのパスワードと同じになります。別の認証パス フレーズを指定するには、このチェックボックスをオフにします。
Authentication Pass Phrase (認証パス フレーズ)	[Use Password as Authentication Pass Phrase (パスワードを認証パス フレーズとして使用)] チェックボックスがオフになっている場合は、このフィ

フィールド	説明
	ールドに認証パス フレーズを入力します。 パス フレーズには、8 ～ 32 文字の ASCII の表示可能文字を使用する必要があります。
Confirm Authentication Pass Phrase (認証パスフレーズの確認)	確認のために同じ認証パス フレーズを再度入力します。
Use Authentication Pass Phrase as Privacy Pass Phrase (認証パス フレーズをプライバシー パス フレーズとして使用)	このチェックボックスは、AuthPriv が選択されている場合にのみ設定できます。 このチェックボックスをオンにした場合、プライバシー パス フレーズは、認証パス フレーズと同じになります。別のプライバシー パス フレーズを指定するには、このチェックボックスをオフにします。
Privacy Pass Phrase (プライバシー パス フレーズ)	[Use Authentication Pass Phrase as Privacy Pass Phrase (認証パス フレーズをプライバシー パス フレーズとして使用)] チェックボックスがオフになっている場合は、このフィールドにプライバシー パス フレーズを入力します。 パス フレーズには、8 ～ 32 文字の ASCII の表示可能文字を使用する必要があります。
Confirm Privacy Pass Phrase (プライバシー パス フレーズの確認)	確認のために同じプライバシー パス フレーズを再度入力します。
Authentication Protocol (認証プロトコル)	ドロップダウン矢印をクリックし、リストから目的の認証プロトコルを選択します。次の 2 つのプロトコルを利用できます。 - MD5 - SHA-1 (デフォルト)
Privacy Protocol (プライバシー プロトコル)	ドロップダウン矢印をクリックし、リストから目的のプライバシー プロトコルを選択します。次の 2 つのプロトコルを利用できます。 - DES (デフォルト) - AES-128

- SSH サービスの公開キー認証が有効である場合は、[SSH] をクリックして公開キーを入力します。「SSH 設定の変更『98p.』」を参照してください。

- a. SSH 公開キーをテキスト エディタで開きます。
 - b. テキスト エディタのすべての内容をコピーし、[SSH] タブの [Public Key (公開キー)] フィールドに貼り付けます。
8. [Roles (役割)] タブをクリックし、ユーザの権限を決定します。
 9. 対応するチェックボックスをオンにして、1 つ以上の役割を選択します。
 - 管理者の役割には、すべての権限が与えられています。
 - オペレータの役割には、頻繁に使用する機能に対する限られた権限が与えられています。権限の範囲については、「**役割の設定** 『119p.』」を参照してください。この役割は、デフォルトで選択されています。
 - 役割がニーズに合わない場合は、次のようにすることができます。
 - **既存の役割の権限を変更:** 役割の権限を変更するには、役割をダブルクリックするか、役割を選択して [Edit Role (役割の編集)] をクリックします。「**役割の変更** 『121p.』」を参照してください。
 - **[Manage Roles (役割の管理)] ボタンをクリックして新しい役割を作成:** 「**役割の作成** 『120p.』」を参照してください。

注: 複数の役割を選択すると、ユーザには、すべての役割の権限がまとめて設定されます。

10. この新しいユーザの Web インタフェースに表示される測定単位を変更するには、[Preferences (個人設定)] タブをクリックし、次のいずれかを実行します。
 - [Temperature Unit (温度単位)] フィールドで、温度の測定単位として [°C] (摂氏) または [°F] (華氏) を選択します。
 - [Length Unit (長さ単位)] フィールドで、長さまたは高さの測定単位として [Meter (メートル)] または [Feet (フィート)] を選択します。
 - [Pressure Unit (圧力単位)] フィールドで、圧力の測定単位として [Pascal (パスカル)] または [psi (psi)] を選択します。
- 1 パスカルは、1 平方メートルあたりの 1 ニュートンに相当します。
Psi は、1 平方インチあたりのポンドを表します。

注: 測定単位変更は、Web インタフェースとコマンド ライン インタフェースにのみ適用されます。

11. [OK] をクリックして変更を保存します。

ユーザ プロファイルの変更

ユーザ名以外のあらゆるユーザ プロファイルの情報を変更できます。

▶ ユーザ プロファイルを変更するには、以下の手順に従います。

1. [User Management (ユーザ管理)] > [Users (ユーザ)] を選択します。
[Manage Users (ユーザの管理)] ダイアログ ボックスが表示されます。
2. ユーザをクリックして選択します。
3. [Edit (編集)] をクリックするか、ユーザをダブルクリックします。
[Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスが表示されます。XXX にはユーザ名が表示されます。
4. 必要なすべての変更を行います。
パスワードを変更するには、[Password (パスワード)] フィールドと
[Confirm Password (パスワードの確認)] フィールドに新しいパスワード
を入力します。パスワードのフィールドを空白のままにすると、パ
スワードは変更されません。
5. SNMPv3 のアクセス権限を変更するには、[SNMPv3] タブをクリック
し、必要な変更を加えます。詳細については、「**ユーザ プロファイ
ルの作成** 『114p. 』」の手順 6 を参照してください。
6. 権限を変更するには、[Roles (役割)] タブをクリックし、次のいづれ
かを実行します。
 - 任意の役割のチェックボックスをオンまたはオフにします。
 - 役割の権限を変更するには、役割をダブルクリックするか、役割
を選択して [Edit Role (役割の編集)] をクリックします。「**役割
の変更** 『121p. 』」を参照してください。
7. 温度、長さ、または圧力の測定単位を変更するには、[Preferences (個
人設定)] タブをクリックし、ドロップダウン リストから別のオプシ
ョンを選択します。

注: 測定単位変更は、Web インタフェースとコマンド ライン イン
タフェースにのみ適用されます。

8. [OK] をクリックして変更を保存します。

ユーザ プロファイルの削除

必要に応じて古いユーザ プロファイルや冗長なユーザ プロファイルを
削除します。

▶ ユーザ プロファイルを削除するには、次の手順に従います。

1. [User Management (ユーザ管理)] > [Users (ユーザ)] を選択します。
[Manage Users (ユーザの管理)] ダイアログ ボックスが表示されます。

2. 削除するユーザをクリックして選択します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
3. [Delete (削除)] をクリックします。
4. 操作の確認を求めるメッセージが表示されます。[Yes (はい)] をクリックして、削除を確認します。

ユーザ リスト表示の変更

データを効率よく表示するために、リストの表示列の数または並べ替え順序を変更できます。「[リストの表示の変更『83p.』](#)」を参照してください。

役割の設定

役割では、ユーザが実行したり利用したりすることのできる操作や機能が定義されます。どのユーザにも、少なくとも 1 つの役割を割り当てる必要があります。

Dominion PX には、あらかじめ**管理者 (Admin)** および**オペレータ (Operator)** という 2 つの役割が組み込まれています。

- 管理者の役割には、すべての権限が与えられています。この役割は、変更することも削除することもできません。
- オペレータの役割には、頻繁に使用する機能に対する限られた権限が与えられています。この役割は、変更または削除することができます。デフォルトでは、オペレータの役割には、次の権限があります。
 - イベント設定の表示
 - ローカル イベント ログの表示
 - イベント設定の変更
 - PDU、インレット、アウトレット (コンセント)、および過電流プロテクタの設定の変更
 - 自身のパスワードの変更
 - アウトレット (コンセント) の切り替え (すべてのアウトレット (コンセント))

注: PX-1000 シリーズは、アウトレット (コンセント) 切り替え対応ではないため、[Switch Outlet (アウトレット (コンセント) の切り替え)] の権限は使用できません。

オペレータの役割は、新たに作成したユーザ プロファイルにデフォルトで割り当てられます。「[ユーザ プロファイルの作成『114p.』](#)」を参照してください。

役割の作成

権限の組み合わせが新規に必要な場合は、新しい役割を作成します。

▶ **役割を作成するには、次の手順に従います。**

1. [User Management (ユーザ管理)] > [Roles (役割)] を選択します。
[Manage Roles (役割の管理)] ダイアログ ボックスが表示されます。

ヒント: [Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスの [Manage Roles (役割の管理)] ボタンをクリックして、[Manage Roles (役割の管理)] ダイアログ ボックスにアクセスすることもできます。

2. [New (新規)] をクリックします。[Create New Role (役割の新規作成)] ダイアログ ボックスが表示されます。
3. [Role Name (役割名)] フィールドに役割の名前を入力します。
4. [Description (説明)] フィールドに役割の説明を入力します。
5. [Privileges (権限)] タブをクリックし、1 つ以上の権限を割り当てます。
 - a. [Add (追加)] をクリックします。[Add Privileges to new Role (新しい役割への権限の追加)] ダイアログ ボックスが表示されます。
 - b. [Privileges (権限)] リストから必要な権限を選択します。
 - c. 選択した権限に引数設定がある場合は、右側に [Arguments (引数)] リストが表示されます。次に、1 つまたは複数の引数を選択します。

たとえば、[Switch Outlet (アウトレット (コンセント) の切り替え)] の権限が選択されている場合は、この役割で制御できるアウトレット (コンセント) がどれかを判断できるように、[Arguments (引数)] リストにすべてのアウトレット (コンセント) が表示されます。目的のアウトレット (コンセント) のチェックボックスをオンにするか、すべてのアウトレット (コンセント) を選択する場合は [all (すべて)] のラベルが付いたチェックボックスをオンにします。
 - d. [Add (追加)] をクリックし、選択した権限 (および、存在する場合は引数) を追加します。
 - e. 必要な権限をすべて追加するまで、手順 a ~ d を繰り返します。
6. [OK] をクリックして変更を保存します。

これで、ユーザに新しい役割を割り当てることができます。「**ユーザ プロファイルの作成**『114p.』」または「**ユーザ プロファイルの変更**『118p.』」を参照してください。

役割の変更

名前を除く、既存の役割の設定を変更できます。

▶ 役割を変更するには、次の手順に従います。

1. [User Management (ユーザ管理)] > [Roles (役割)] を選択します。
[Manage Roles (役割の管理)] ダイアログ ボックスが表示されます。

ヒント: [Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスの [Manage Roles (役割の管理)] ボタンをクリックして、[Manage Roles (役割の管理)] ダイアログ ボックスにアクセスすることもできます。

2. 変更する役割をクリックして選択します。
3. [Edit (編集)] をクリックするか、役割をダブルクリックします。[Edit Role 'XXX' (役割 'XXX' の編集)] ダイアログ ボックスが表示されます。XXX は役割の名前です。

ヒント: [Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスの [Edit Role (役割の編集)] ボタンをクリックして、[Edit Role 'XXX' (役割 'XXX' の編集)] ダイアログ ボックスにアクセスすることもできます。

4. 必要に応じて、[Description (説明)] フィールドに表示されている文字列を変更します。
5. 権限を変更するには、[Privileges (権限)] タブをクリックします。

注: 管理者の役割の権限は変更できません。

6. 権限を削除するには、次の操作を実行します。
 - a. 削除する権限をクリックして選択します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
 - b. [Delete (削除)] をクリックします。
7. 権限を追加するには、次の操作を実行します。
 - a. [Add (追加)] をクリックします。[Add Privileges to Role 'XXX' (役割 'XXX' への権限の追加)] ダイアログ ボックスが表示されます。XXX は役割の名前です。
 - b. [Privileges (権限)] リストから必要な権限を選択します。
 - c. 選択した権限に引数設定がある場合は、右側に [Arguments (引数)] リストが表示されます。次に、1 つまたは複数の引数を選択します。

たとえば、[Switch Outlet (アウトレット (コンセント) の切り替え)] の権限が選択されている場合は、この役割で制御できるアウトレット (コンセント) がどれかを判断できるように、[Arguments (引数)] リストにすべてのアウトレット (コンセント) が表示されます。目的のアウトレット (コンセント) のチェックボックスをオンにするか、すべてのアウトレット (コンセント) を選択する場合は [all (すべて)] のラベルが付いたチェックボックスをオンにします。

- d. [Add (追加)] をクリックし、選択した権限 (および、存在する場合は引数) を追加します。
- e. 必要な権限をすべて追加するまで、手順 a ~ d を繰り返します。
8. 特定の権限の引数を変更するには、次の操作を実行します。
 - a. 権限をクリックして選択します。
 - b. [Edit (編集)] をクリックします。[Edit arguments of privilege 'XXX' (権限 'XXX' の引数の編集)] ダイアログ ボックスが表示されます。XXX は権限の名前です。

注: 選択した権限に引数がない場合、[Edit (編集)] ボタンは無効になります。

- c. 目的の引数を選択します。複数の選択も可能です。
- d. [OK] をクリックします。
9. [OK] をクリックして変更を保存します。

役割の削除

管理者の役割以外の役割は、削除できます。

▶ 役割を削除するには、次の手順に従います。

1. [User Management (ユーザ管理)] > [Roles (役割)] を選択します。
[Manage Roles (役割の管理)] ダイアログ ボックスが表示されます。

ヒント: [Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスの [Manage Roles (役割の管理)] ボタンをクリックして、[Manage Roles (役割の管理)] ダイアログ ボックスにアクセスすることもできます。

2. 削除する役割をクリックして選択します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
3. [Delete (削除)] をクリックします。
4. 操作の確認を求めるメッセージが表示されます。[Yes (はい)] をクリックして、削除を確認します。

役割リスト表示の変更

データを効率よく表示するために、リストの表示列の数または並べ替え順序を変更できます。「[リストの表示の変更](#)『83p.』」を参照してください。

アクセス セキュリティ コントロール

Dominion PX には、アクセスを制御するためのツールがあります。HTTPS 暗号化を必須にし、内部のファイアウォールを有効にし、ファイアウォールのルールを作成し、ログインの制約を作成できます。

ヒント: 証明書を作成してインストールしたり、アクセスを制御するために外部の認証サーバを設定したりすることもできます。「[SSL 証明書の設定](#)『139p.』」および「[LDAP 認証の設定](#)『146p.』」を参照してください。

HTTPS 暗号化を強制的に使用

HTTPS では、SSL (Secure Sockets Layer) テクノLOGYを使用して Dominion PX デバイスに対するすべての送受信トラフィックが暗号化されるため、HTTPS は HTTP より安全なプロトコルです。

HTTPS プロトコル経由でのみユーザが Dominion PX Web インタフェースにアクセスできるよう設定できます。デフォルトでは、このプロトコルが有効になっています。

▶ Web インタフェースへのアクセスに HTTPS が使用されるようにするには、次の手順に従います。

1. [Device Settings (デバイスの設定)] > [Security (セキュリティ)] > [Force HTTPS for Web Access (Web アクセスには強制的に HTTPS を使用)] を選択します。
2. 操作の確認を求めるメッセージが表示されます。[Yes (はい)] をクリックすると、HTTPS サービスが強制的に使用されるようになります。
3. [Device Settings (デバイスの設定)] > [Security (セキュリティ)] を選択し、次の図に示すように [Force HTTPS for Web Access (Web アクセスには強制的に HTTPS を使用)] チェックボックスがオンになっていることを確認します。

☒ Force HTTPS for Web Access

チェックボックスがオンになっていない場合は、ここまでの手順を再度実行します。

HTTPS プロトコルを有効にすると、HTTP を使用したアクセスはすべて自動的に HTTPS にリダイレクトされます。

ファイアウォールの設定

Dominion PX にはファイアウォールがあり、それを設定すると、特定の IP アドレスまたは IP アドレスの範囲からの Dominion PX デバイスへのアクセスを防止できます。デフォルトでは、ファイアウォールは無効になっています。

▶ **ファイアウォールを設定するには、次の手順に従います。**

1. ファイアウォールを有効にします。「**ファイアウォールの有効化**『124p.』」を参照してください。
2. デフォルトのポリシーを設定します。「**デフォルト ポリシーの変更**『125p.』」を参照してください。
3. アクセスを許可するアドレスと拒否するアドレスを指定するファイアウォールのルールを作成します。「**ファイアウォールのルールの作成**『126p.』」を参照してください。

ファイアウォールのルールへの変更は即座に有効になります。権限のないすべての IP アクティビティは即座に停止します。

注: デフォルトでファイアウォールを無効にしておく目的は、ユーザが誤って自分自身をデバイスにアクセスできないように設定してしまうことを防止するためです。

ファイアウォールの有効化

ファイアウォールのルールが存在していても、ファイアウォールが有効になっていないと効果はありません。

▶ **Dominion PX のファイアウォールを有効にするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [IP Access Control (IP アクセス コントロール)] を選択します。
[Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスが表示されます。
2. IPv4 ファイアウォールを有効にするには、[IPv4] タブをクリックし、[Enable IPv4 Access Control (IPv4 アクセス コントロールを有効にする)] チェックボックスをオンにします。
3. IPv6 ファイアウォールを有効にするには、[IPv6] タブをクリックし、[Enable IPv6 Access Control (IPv6 アクセス コントロールを有効にする)] チェックボックスをオンにします。
4. [OK] をクリックして変更を保存します。

デフォルト ポリシーの変更

ファイアウォールを有効にした後のデフォルトのポリシーでは、すべての IP アドレスからのトラフィックが受け入れられます。つまり、指定したルールによって拒否された IP アドレスだけが Dominion PX にアクセスできなくなることです。

デフォルトのポリシーを [Drop (破棄)] または [Reject (拒否)] に変更すると、指定したルールで許可されている IP アドレスを除いて、すべての IP アドレスからのトラフィックが破棄されます。

▶ デフォルト ポリシーを変更するには、以下の手順に従います。

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [IP Access Control (IP アクセス コントロール)] を選択します。
[Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスが表示されます。
2. IPv4 アドレスのデフォルト ポリシーを決定するには、次の手順に従います。
 - a. 必要な場合 [IPv4] タブをクリックします。
 - b. [Enable IPv4 Access Control (IPv4 アクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
 - c. デフォルト ポリシーは、[Default Policy (デフォルト ポリシー)] フィールドに表示されます。デフォルト ポリシーを変更するには、ドロップダウン リストから別のポリシーを選択します。
 - [Accept (許可)]: すべての IPv4 アドレスからのトラフィックを受け入れます。
 - [Drop (破棄)]: エラー通知を送信元ホストに送信せずにすべての IPv4 アドレスからのトラフィックを破棄します。
 - [Reject (拒否)]: すべての IPv4 アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージを送信元ホストに送信されます。
3. IPv6 アドレスのデフォルト ポリシーを決定するには、次の手順に従います。
 - a. [IPv6] タブをクリックします。
 - b. [Enable IPv6 Access Control (IPv6 アクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
 - c. デフォルト ポリシーは、[Default Policy (デフォルト ポリシー)] フィールドに表示されます。デフォルト ポリシーを変更するには、ドロップダウン リストから別のポリシーを選択します。

- [Accept (許可)]: すべての IPv6 アドレスからのトラフィックを受け入れます。
 - [Drop (破棄)]: エラー通知を送信元ホストに送信せずにすべての IPv6 アドレスからのトラフィックを破棄します。
 - [Reject (拒否)]: すべての IPv6 アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージを送信元ホストに送信されます。
4. [OK] をクリックして変更を保存します。新しいデフォルト ポリシーが適用されます。

ファイアウォールのルール作成

ファイアウォールのルールによって、Dominion PX にトラフィックを送信するホストの IP アドレスに基づいて、トラフィックを受け入れるかどうかが決まります。ファイアウォールのルールを作成する場合は、以下の原則を考慮します。

- **ルールの順序は重要です。**

トラフィックが Dominion PX デバイスに到達すると、ルールが番号順に実行されます。IP アドレスに一致する最初のルールが見つかった時点で、トラフィックを受け入れるかどうかが決まります。IP アドレスに一致する後続のルールは、Dominion PX では無視されます。

- **サブネット マスクが必要な場合があります。**

IP アドレスを入力するときに、アドレスとサブネット マスクの両方を指定する必要がある場合と、その必要がない場合があります。デフォルトのサブネット マスクは /32 (つまり、255.255.255.255) です。サブネット マスクを指定する必要があるのは、デフォルトと異なる場合のみです。たとえば、次の形式を使用して Class C ネットワークの単一のアドレスを指定します。

x.x.x.x/24

ここで、/24 は 255.255.255.0 のサブネット マスクです。

サブネット全体またはアドレスの範囲を指定する場合は、それに応じてサブネット マスクを変更します。

注: 有効な IP アドレスの範囲は、0.0.0.0 ~ 255.255.255.255 です。入力した IP アドレスが、この範囲内であることを確認してください。

▶ **ファイアウォールのルールを作成するには、以下の手順に従います。**

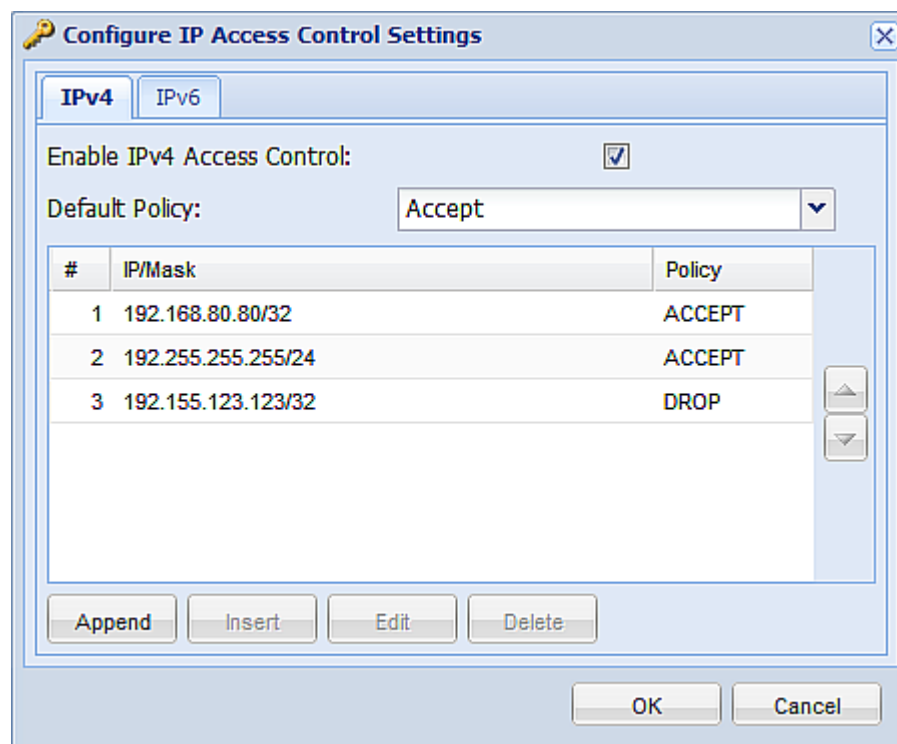
1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [IP Access Control (IP アクセス コントロール)] を選択します。
[Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスが表示されます。

- 2. ファイアウォール ルールを作成するには [IPv4] タブ、IPv6 ファイアウォール ルールを作成するには [IPv6] タブをクリックします。
- 3. [IPv4] タブの [Enable IPv4 Access Control (IPv4 アクセス コントロールを有効にする)] チェックボックス、または[IPv6] タブの [Enable IPv6 Access Control (IPv6 アクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
- 4. 各自のルールを作成します。さまざまな操作については、表を参照してください。

アクション	手順
ルール リストの最後にルールを追加する	▪ [Append (追加)] をクリックします。[Append new Rule (新しいルールの追加)] ダイアログ ボックスが表示されます。 ▪ [IP/Mask (IP/マスク)] フィールドに IP アドレスとサブネット マスクを入力します。 ▪ [Policy (ポリシー)] フィールドのドロップダウン リストで、[Accept (許可)]、[Drop (破棄)]、または [Reject (拒否)] を選択します。 ▪ [Accept (許可)]: 指定された IP アドレスからのトラフィックを受け入れます。 ▪ [Drop (破棄)]: エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。 ▪ [Reject (拒否)]: 指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージを送信元ホストに送信されます。 ▪ [OK] をクリックして変更を保存します。 システムが自動的にルールに番号を付けます。

アクション	手順
2 つの既存ルールの中にルールを挿入する	■ 上に新しいルールを挿入するルールを選択します。たとえば、ルール番号 3 と 4 の間にルールを挿入する場合は、4 を選択します。 ■ [Insert (挿入)] をクリックします。[Insert new Rule (新しいルールの挿入)] ダイアログ ボックスが表示されます。 ■ [IP/Mask (IP/マスク)] フィールドに IP アドレスとサブネット マスクを入力します。 ■ [Policy (ポリシー)] フィールドのドロップダウン リストで、[Accept (許可)]、[Drop (破棄)]、または [Reject (拒否)] を選択します。 ■ [Accept (許可)]: 指定された IP アドレスからのトラフィックを受け入れます。 ■ [Drop (破棄)]: エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。 ■ [Reject (拒否)]: 指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージを送信元ホストに送信されます。 ■ [OK] をクリックして変更を保存します。 ルールが挿入され、後続のルールには自動的に番号が振り直されます。

5. 完了すると、ルールが [Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスに表示されます。



6. [OK] をクリックして変更を保存します。 ルールが適用されます。

ファイアウォールのルールの編集

既存のファイアウォール ルールで IP アドレス範囲やポリシーの更新が必要な場合は、ルールを適宜変更します。

▶ ファイアウォール ルールを変更するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [IP Access Control (IP アクセス コントロール)] を選択します。
[Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスが表示されます。
2. IPv4 ファイアウォール ルールを変更するには、[IPv4] タブをクリックします。IPv6 ファイアウォール ルールを変更するには、[IPv6] タブをクリックします。
3. [IPv4] タブの [Enable IPv4 Access Control (IPv4 アクセス コントロールを有効にする)] チェックボックス、または[IPv6] タブの [Enable IPv6 Access Control (IPv6 アクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
4. ルール リストで変更するルールを選択します。
5. [Edit (編集)] をクリックするか、ルールをダブルクリックします。
[Edit Rule (ルールの編集)] ダイアログ ボックスが表示されます。
6. 表示される内容に変更を加えます。
7. [OK] をクリックして変更を保存します。
8. [OK] をクリックして [Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスを終了します。そうしなければ、変更は失われます。

ファイアウォールのルールの並べ替え

ルールの順序によって、同じ IP アドレスに一致するルールのうちのどれが実行されるかが決まります。

▶ ファイアウォールのルールを並べ替えるには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [IP Access Control (IP アクセス コントロール)] を選択します。
[Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスが表示されます。
2. IPv4 ファイアウォール ルールを並べ替えるには、[IPv4] タブをクリックします。IPv6 ファイアウォール ルールを並べ替えるには、[IPv6] タブをクリックします。

3. [IPv4] タブの [Enable IPv4 Access Control (IPv4 アクセス コントロールを有効にする)] チェックボックス、または[IPv6] タブの [Enable IPv6 Access Control (IPv6 アクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
4. 特定のルールをクリックして選択します。
5.  または  をクリックし、選択したルールを上下に動かして目的の場所に移動します。
6. [OK] をクリックして変更を保存します。

ファイアウォールのルールの削除

ファイアウォールのルールが古くなった場合や、不要になった場合は、ルール リストから削除します。

▶ グループ ベースのアクセス制御ルールを削除するには

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [IP Access Control (IP アクセス コントロール)] を選択します。
[Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスが表示されます。
2. IPv4 ファイアウォール ルールを削除するには、[IPv4] タブをクリックします。IPv6 ファイアウォール ルールを削除するには、[IPv6] タブをクリックします。
3. [IPv4] タブの [Enable IPv4 Access Control (IPv4 アクセス コントロールを有効にする)] チェックボックス、または[IPv6] タブの [Enable IPv6 Access Control (IPv6 アクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
4. 削除するルールを選択します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
5. [Delete (削除)] をクリックします。
6. 操作の確認を求めるメッセージが表示されます。[Yes (はい)] をクリックし、選択したルールをルール リストから削除します。
7. [OK] をクリックして変更を保存します。

ユーザ ログイン制御の設定

ログイン制御を設定して、ハッカーによる Dominion PX および接続されるデバイスへのアクセスを、より困難なものにすることができます。ログインの失敗が指定回数に達したユーザをロック アウトしたり、同じユーザ名を使用して同時にログインするユーザ数を制限したり、ユーザに強力なパスワードを作成させたりすることができます。

ユーザ ブロックの有効化

ユーザ ブロックにより、Dominion PX へのログインを試みて認証に失敗した回数が一定の数に達したユーザのログインをブロックするように指定できます。

この機能は、外部の AA サーバによる認証ではなく、ローカル認証にのみ適用されます。

注: ユーザ ブロック イベントが発生した場合、シリアル接続経由で "unblock" CLI コマンドを使用して、そのユーザのブロックを手動で解除できます。『ユーザのブロック解除』[『429p.』](#)を参照してください。

▶ ユーザ ブロックを有効化するには、以下の手順に従います。

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Login Settings (ログイン設定)] を選択します。[Login Settings (ログイン設定)] ダイアログ ボックスが表示されます。
2. [User Blocking (ユーザ ブロック)] セクションを探します。
3. ユーザ ブロック機能を有効にするには、[Block user on login failure (ログイン失敗時にユーザをブロック)] チェックボックスをオンにします。
4. [Maximum number of failed logins (ログインに失敗できる回数)] フィールドに数値を入力します。これは、ユーザ ログインが Dominion PX へのアクセスをブロックされるまでに許容される、ユーザのログインの最大失敗回数です。
5. ログインをブロックする時間を指定するには、[Block timeout (ブロック タイムアウト)] フィールドでドロップダウン リストから目的の時間の長さを選択します。次に、使用可能なオプションについて説明します。
 - [Infinite (無限)]: このオプションは、ログインのブロックに時間制限を設定しません。
 - X min: このタイプのオプションは、時間制限を X 分に設定します。X は数値です。
 - X h: このタイプのオプションは、時間制限を X 時間に設定します。X は数値です。
 - 1 d: このオプションは、時間制限を 1 日に設定します。

ヒント: 目的の時間オプションが表示されていない場合は、このフィールドに目的の時間を手動で入力できます。たとえば、「4 min」と入力すると、時間を 4 分間に設定できます。

6. [OK] をクリックして変更を保存します。

ログイン制限の有効化

ログイン制限により、同時に複数のユーザが同じログイン名を使用できるかどうか、およびアイドル状態のユーザが強制的にログアウトされるまでの時間が決まります。

▶ **ログイン制限を有効にするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Login Settings (ログイン設定)] を選択します。[Login Settings (ログイン設定)] ダイアログ ボックスが表示されます。
2. [Login Limitations (ログイン制限)] セクションを探します。
3. 複数のユーザが同時に同じログイン情報を使用しないようにするには、[Prevent concurrent login with same username (同じユーザ名を使用した同時ログインの防止)] チェックボックスをオンにします。
4. アイドル状態のユーザが Dominion PX によって強制的にログアウトされるまでの時間を調整するには、[Idle Timeout Period (アイドル タイムアウト時間)] フィールドで時間オプションを選択します。デフォルトは 10 分です。
 - X min: このタイプのオプションは、時間制限を X 分に設定します。X は数値です。
 - X h: このタイプのオプションは、時間制限を X 時間に設定します。X は数値です。
 - 1 d: このオプションは、時間制限を 1 日に設定します。

ヒント: 目的の時間オプションが表示されていない場合は、このフィールドに目的の時間を手動で入力できます。たとえば、「4 min」と入力すると、時間を 4 分間に設定できます。

5. [OK] をクリックして変更を保存します。

ヒント: 可能な場合は、アイドル タイムアウトを 20 分以内にします。これによって、接続中のアイドル セッション数と Dominion PX に送信される同時コマンド数が削減されます。

強力なパスワードの有効化

強力なパスワードを使用すると、侵入者がユーザ パスワードを破って Dominion PX デバイスへアクセスすることは、より困難になります。デフォルトでは、強力なパスワードには、最低 8 文字以上の長さで、大文字と小文字、数字、および特殊文字 (@ や & など) を含める必要があります。

▶ ユーザに強力なパスワードを作成させるには、次の手順に従います。

1. +[Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Password Policy (パスワード ポリシー)] を選択します。[Password Policy (パスワード ポリシー)] ダイアログ ボックスが表示されます。
2. [Strong Passwords (強力なパスワード)] チェックボックスをオンにして、強力なパスワード機能をアクティブにします。デフォルトの設定を以下に示します。

最小長	= 8 文字
最大長	= 32 文字
1 文字以上の小文字	= 必要
1 文字以上の大文字	= 必要
1 文字以上の数字	= 必要
1 文字以上の特殊文字	= 必要
履歴内の制限パスワードの数	= 5

注: Dominion PX が受け付けるパスワードの長さは最長 32 文字です。

3. デフォルトの設定に、必要な変更を行います。
4. [OK] をクリックして変更を保存します。

パスワード エージングの有効化

パスワード エージングでは、ユーザにパスワードの定期的な変更を要求するかどうかを指定します。デフォルトの間隔は 60 日です。

▶ ユーザにパスワードを定期的に変更させるには、次の手順に従います。

1. +[Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Password Policy (パスワード ポリシー)] を選択します。[Password Policy (パスワード ポリシー)] ダイアログ ボックスが表示されます。
2. [Password Aging (パスワード エージング)] チェックボックスをオンにして、パスワード エージング機能を有効にします。

3. ユーザにパスワードの変更を要求する頻度を指定するには、[Password Aging Interval (パスワード エージング間隔)] フィールドで日数を選択します。ユーザは、指定した日数が経過するたびにパスワードの変更を要求されます。

ヒント: 目的の時間オプションが表示されていない場合は、このフィールドに目的の時間を手動で入力できます。たとえば、「9 d」と入力すると、パスワード エージング時間を 9 日間に設定できます。

4. [OK] をクリックして変更を保存します。

役割ベースのアクセス制御ルールの設定

役割ベースのアクセス制御ルールは、特定の役割を共有するメンバーに適用されることを除いて、ファイアウォールのルールと同じです。これによって、IP アドレスに基づいて、特定の役割にシステムの権限を与えることができます。

▶ **役割ベースのアクセス制御ルールを設定するには、次の手順に従います。**

1. 機能を有効にします。「**機能の有効化** 『134p.』」を参照してください。
2. デフォルトのポリシーを設定します。「**デフォルト ポリシーの変更** 『135p.』」を参照してください。
3. アドレスが特定の役割に関連付けられている場合に、アクセスを許可するアドレスと拒否するアドレスを指定するルールを作成します。「**役割ベースのアクセス制御ルールの作成** 『136p.』」を参照してください。

変更内容は現在ログインしているユーザには影響を与えません。ユーザの次のログイン時に有効になります。

機能の有効化

関連するルールを有効にする前に、このアクセス制御機能を有効にする必要があります。

▶ **役割ベースのアクセス制御ルールを有効にするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Role Based Access Control (役割ベースのアクセス制御)] を選択します。
[Configure Role Based Access Control Settings (役割ベースのアクセス制御の設定)] ダイアログ ボックスが表示されます。
2. IPv4 ファイアウォールを有効にするには、[IPv4] タブをクリックし、[Enable Role Based Access Control for IPv4 (IPv4 の役割ベースのアクセス コントロールを有効にする)] チェックボックスをオンにします。

3. IPv6 ファイアウォールを有効にするには、[IPv6] タブをクリックし、[Enable Role Based Access Control for IPv6 (IPv6 の役割ベースのアクセス コントロールを有効にする)] チェックボックスをオンにします。
4. [OK] をクリックして変更を保存します。

デフォルト ポリシーの変更

デフォルト ポリシーは、ユーザに適用されている役割にかかわらず、すべての IP アドレスからのすべてのトラフィックを受け入れます。

▶ デフォルト ポリシーを変更するには、以下の手順に従います。

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Role Based Access Control (役割ベースのアクセス制御)] を選択します。
[Configure Role Based Access Control Settings (役割ベースのアクセス制御の設定)] ダイアログ ボックスが表示されます。
2. IPv4 アドレスのデフォルト ポリシーを決定するには、次の手順に従います。
 - a. 必要な場合 [IPv4] タブをクリックします。
 - b. [Enable Role Based Access Control for IPv4 (IPv4 の役割ベースのアクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
 - c. [Default Policy (デフォルト ポリシー)] ドロップダウン リストから目的のアクションを選択します。
 - [Allow (許可)]: ユーザの役割にかかわらず、すべての IPv4 アドレスからのトラフィックを受け入れます。
 - [Deny (拒否)]: ユーザの役割にかかわらず、すべての IPv4 アドレスからのトラフィックを破棄します。
3. IPv6 アドレスのデフォルト ポリシーを決定するには、次の手順に従います。
 - a. [IPv6] タブをクリックします。
 - b. [Enable Role Based Access Control for IPv6 (IPv6 の役割ベースのアクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
 - c. [Default Policy (デフォルト ポリシー)] ドロップダウン リストから目的のアクションを選択します。
 - [Allow (許可)]: ユーザの役割にかかわらず、すべての IPv6 アドレスからのトラフィックを受け入れます。
 - [Deny (拒否)]: ユーザの役割にかかわらず、すべての IPv6 アドレスからのトラフィックを破棄します。
4. [OK] をクリックして変更を保存します。

役割ベースのアクセス制御ルールを作成

ユーザの役割と IP アドレスをベースに、役割ベースのアクセス制御ルールはトラフィックを受け入れるか、または破棄します。ルールは番号順に実行されるため、ファイアウォール ルールと同様にルールの順番が重要です。

▶ **役割ベースのアクセス制御ルールを作成するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Role Based Access Control (役割ベースのアクセス制御)] を選択します。
[Configure Role Based Access Control Settings (役割ベースのアクセス制御の設定)] ダイアログ ボックスが表示されます。
2. ファイアウォール ルールを作成するには [IPv4] タブ、IPv6 ファイアウォール ルールを作成するには [IPv6] タブをクリックします。
3. [IPv4] タブの [Enable Role Based Access Control for IPv4 (IPv4 の役割ベースのアクセス コントロールを有効にする)] チェックボックス、または [IPv6] タブの [Enable Role Based Access Control for IPv6 (IPv6 の役割ベースのアクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
4. 各自のルールを作成します。

アクション	作業内容
ルール リストの最後にルールを追加する	▪ [Append (追加)] をクリックします。[Append new Rule (新しいルールの追加)] ダイアログ ボックスが表示されます。 ▪ [Starting IP Address (開始 IP アドレス)] フィールドに開始 IP アドレスを入力します。 ▪ [Ending IP Address (終了 IP アドレス)] フィールドに終了 IP アドレスを入力します。 ▪ [Role (役割)] フィールドのドロップ ダウン リストで役割を選択します。このルールは、この役割のメンバーのみに適用されます。 ▪ [Policy (ポリシー)] フィールドのドロップダウン リストで、[Allow (許可)] または [Deny (拒否)] を選択します。 ▪ [Allow (許可)]: ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを受け入れます。 ▪ [Deny (拒否)]: ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを破棄します。

アクション	作業内容
	▪ [OK] をクリックして変更を保存します。 システムが自動的にルールに番号を付けます。
2 つの既存ルールの中にルールを挿入する	▪ 上に新しいルールを挿入するルールを選択します。たとえば、ルール番号 3 と 4 の間にルールを挿入する場合は、4 を選択します。 ▪ [Insert (挿入)] をクリックします。[Insert new Rule (新しいルールの挿入)] ダイアログ ボックスが表示されます。 ▪ [Starting IP Address (開始 IP アドレス)] フィールドに開始 IP アドレスを入力します。 ▪ [Ending IP Address (終了 IP アドレス)] フィールドに終了 IP アドレスを入力します。 ▪ [Role (役割)] フィールドのドロップ ダウン リストで役割を選択します。このルールは、この役割のメンバーのみに適用されます。 ▪ [Policy (ポリシー)] フィールドのドロップダウン リストで、[Allow (許可)] または [Deny (拒否)] を選択します。 ▪ [Allow (許可)]: ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを受け入れます。 ▪ [Deny (拒否)]: ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを破棄します。 ▪ [OK] をクリックして変更を保存します。 ルールが挿入され、後続のルールには自動的に番号が振り直されます。

5. [OK] をクリックして変更を保存します。

役割ベースのアクセス制御ルールの編集

これらの役割がニーズに合わない場合は、既存のルールを変更できます。

▶ 役割ベースのアクセス制御ルールを変更するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Role Based Access Control (役割ベースのアクセス制御)] を選択します。
[Configure Role Based Access Control Settings (役割ベースのアクセス制御の設定)] ダイアログ ボックスが表示されます。

2. IPv4 ファイアウォール ルールを変更するには、[IPv4] タブをクリックします。IPv6 ファイアウォール ルールを変更するには、[IPv6] タブをクリックします。
3. [IPv4] タブの [Enable Role Based Access Control for IPv4 (IPv4 の役割ベースのアクセス コントロールを有効にする)] チェックボックス、または[IPv6] タブの [Enable Role Based Access Control for IPv6 (IPv6 の役割ベースのアクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
4. ルール リストで変更するルールを選択します。
5. [Edit (編集)] をクリックするか、ルールをダブルクリックします。
[Edit Rule (ルールの編集)] ダイアログ ボックスが表示されます。
6. 表示される内容に変更を加えます。
7. [OK] をクリックして変更を保存します。

役割ベースのアクセス制御ルールの並べ替え

ファイアウォールのルールと同様に、役割ベースのアクセス制御ルールの順序によって、同じ IP アドレスに一致するルールのうちのどれが実行されるかが決まります。

▶ 役割ベースのアクセス制御ルートを並べ替えるには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Role Based Access Control (役割ベースのアクセス制御)] を選択します。
[Configure Role Based Access Control Settings (役割ベースのアクセス制御の設定)] ダイアログ ボックスが表示されます。
2. IPv4 ファイアウォール ルールを並べ替えるには、[IPv4] タブをクリックします。IPv6 ファイアウォール ルールを並べ替えるには、[IPv6] タブをクリックします。
3. [IPv4] タブの [Enable Role Based Access Control for IPv4 (IPv4 の役割ベースのアクセス コントロールを有効にする)] チェックボックス、または[IPv6] タブの [Enable Role Based Access Control for IPv6 (IPv6 の役割ベースのアクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
4. 特定のルールをクリックして選択します。
5.  または  をクリックし、選択したルールを上下に動かして目的の場所に移動します。
6. [OK] をクリックして変更を保存します。

役割ベースのアクセス制御ルールの削除

アクセス制御ルールが不要になった場合、または古くなった場合は、それを削除します。

▶ **役割ベースのアクセス制御ルールを削除するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Role Based Access Control (役割ベースのアクセス制御)] を選択します。
[Configure Role Based Access Control Settings (役割ベースのアクセス制御の設定)] ダイアログ ボックスが表示されます。
2. IPv4 ファイアウォール ルールを削除するには、[IPv4] タブをクリックします。IPv6 ファイアウォール ルールを削除するには、[IPv6] タブをクリックします。
3. [IPv4] タブの [Enable Role Based Access Control for IPv4 (IPv4 の役割ベースのアクセス コントロールを有効にする)] チェックボックス、または [IPv6] タブの [Enable Role Based Access Control for IPv6 (IPv6 の役割ベースのアクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
4. ルール リストで削除するルールを選択します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
5. [Delete (削除)] をクリックします。
6. 操作の確認を求めるメッセージが表示されます。[Yes (はい)] をクリックして、削除を確認します。
7. [OK] をクリックして変更を保存します。

SSL 証明書の設定

X.509 デジタル証明書があると、SSL で接続されている双方が、互いの身元を確認することができます。

Dominion PX の証明書を取得するには、証明書署名リクエスト (CSR) を作成し、それを証明機関 (CA) に送信します。CSR に含まれる情報が CA で処理されると、直ちに SSL 証明書が発行されるので、これを Dominion PX にインストールする必要があります。

注: ユーザが *Dominion PX* に接続するときに必ず *SSL* が使用されるようにする手順については、[『HTTPS 暗号化を強制的に使用』](#) (123p.) を参照してください。

CSR は、次のいずれかの場合に不要です。

- 自己署名された証明書を Dominion PX デバイス上に生成することにした場合。
- 適切かつ有効な証明書とキー ファイルを入手できている場合。

証明書署名リクエスト

Dominion PX の適切な証明書とキー ファイルを入手できない場合は、Dominion PX デバイスの CSR と秘密キーを作成し、CSR を CA に送信して証明書に署名してもらう方法などがあります。

証明書署名リクエストの作成

次の手順に従って、Dominion PX デバイスの CSR を作成します。

▶ CSR を作成するには、次の手順に従います。

1. [Device Settings (デバイスの設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 証明書)] を選択します。[Manage SSL Certificate (SSL 証明書の管理)] ダイアログ ボックスが表示されます。
2. [New SSL Certificate (新しい SSL 証明書)] タブをクリックします。
3. 必要な情報を入力します。
 - [Subject (サブジェクト)] セクションでは、次の情報が対象となります。

フィールド	入力情報
Country (ISO code) (国名 (ISO コード))	会社の所在地の国名。標準の ISO 国コードを使用します。ISO コードのリストについては、 <i>ISO Web サイト</i> 『 http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm 参照』を参照してください。
State or Province (都道府県)	会社の所在地の都道府県の正式名称。
Locality (所在地)	会社の所在地の都市。
Organization (組織)	会社の登録名。
Organizational Unit (組織ユニット)	部署の名称。
Common Name (コマンド名)	Dominion PX デバイスの完全修飾ドメイン名 (FQDN)。
Email Address (電子メール アドレス)	あなた、またはあなた以外の管理ユーザの連絡先電子メール アドレス。

注:[Organization (組織)], [Organizational Unit (組織ユニット)], [Email Address (電子メール アドレス)] の各フィールドを除いて、[Subject (サブジェクト)] セクションのすべてのフィールドは必須です。必須フィールドに値を入力せずに CSR を生成した場合は、サードパーティの証明書を取得できません。

- [Key Creation Parameters (キーの作成パラメータ)] セクションでは、次の情報が対象となります。

フィールド	実行する操作
キーの長さ	このフィールドのドロップダウン リストからキーの長さ (ビット) を選択します。キーを長くすると、セキュリティは向上しますが、Dominion PX デバイスの応答は遅くなります。
Self Sign (自己署名)	CA によって署名された証明書を要求する場合は、このチェックボックスがオンになっていないことを確認します。
Challenge (チャレンジ)	パスワードを入力します。証明書または CSR を保護するためのパスワード。この情報はオプションであり、値には 4 ～ 64 文字の文字列を設定できます。 パスワードでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。
Confirm Challenge (チャレンジの確認)	確認のためにもう一度同じパスワードを入力します。

4. [Create New SSL Key (SSL キーの新規作成)] をクリックし、CSR と秘密キーを作成します。この処理には数分かかる場合があります。
5. 新たに作成した CSR をコンピュータにダウンロードするには、[Download Certificate Signing Request (証明書署名リクエストのダウンロード)] をクリックします。
 - a. ファイルを開くか保存するかを確認するメッセージが表示されます。[Save (保存)] をクリックして、コンピュータにファイルを保存します。
 - b. コンピュータにファイルが保存されたら、そのファイルを直ちに CA に送信し、デジタル証明書を取得します。
 - c. 必要に応じて、[Delete Certificate Signing Request (証明書署名リクエストの削除)] をクリックし、Dominion PX デバイスから CSR ファイルを完全に削除します。
6. 新たに作成された秘密キーをコンピュータに保存するには、[Download Key (キーのダウンロード)] をクリックします。ファイルを開くか保存するかを確認するメッセージが表示されます。[Save (保存)] をクリックして、コンピュータにファイルを保存します。
7. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

CA の署名済み証明書のインストール

送信した CSR に従って CA から署名入りの証明書が提供されたら、その証明書を Dominion PX デバイスにインストールする必要があります。

▶ **証明書をインストールするには、次の手順に従います。**

1. [Device Settings (デバイスの設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 証明書)] を選択します。[Manage SSL Certificate (SSL 証明書の管理)] ダイアログ ボックスが表示されます。
2. [New SSL Certificate (新しい SSL 証明書)] タブをクリックします。
3. [Certificate File (証明書ファイル)] フィールドで、[Browse (参照)] をクリックし、CA から得られた証明書ファイルを選択します。
4. [Upload (アップロード)] をクリックします。証明書が Dominion PX デバイスにインストールされます。

ヒント: 証明書が正常にインストールされたかどうかを確認するには、後で [Active SSL Certificate (アクティブな SSL 証明書)] タブをクリックします。

5. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

自己署名された証明書の作成

Dominion PX デバイスの適切な証明書とキー ファイルを入手できない場合は、CA に CSR を送信する方法以外に、自己署名された証明書を生成する方法もあります。

▶ **自己署名された証明書を作成してインストールするには、次の手順に従います。**

1. [Device Settings (デバイスの設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 証明書)] を選択します。[Manage SSL Certificate (SSL 証明書の管理)] ダイアログ ボックスが表示されます。
2. [New SSL Certificate (新しい SSL 証明書)] タブをクリックします。
3. 必要な情報を入力します。

フィールド	入力情報
Country (ISO code) (国名 (ISO コード))	会社の所在地の国名。標準の ISO 国コードを使用します。ISO コードのリストについては、 <i>ISO Web サイト</i> 『 http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm 参照』を参照してください。
State or Province (都道府県)	会社の所在地の都道府県の正式名称。

フィールド	入力情報
Locality (所在地)	会社の所在地の都市。
Organization (組織)	会社の登録名。
Organizational Unit (組織ユニット)	部署の名前。
Common Name (コマンド名)	Dominion PX デバイスの完全修飾ドメイン名 (FQDN)。
Email Address (電子メール アドレス)	あなた、またはあなた以外の管理ユーザの連絡先電子メール アドレス。
キーの長さ	このフィールドのドロップダウン リストからキーの長さ (ビット) を選択します。キーを長くすると、セキュリティは向上しますが、Dominion PX デバイスの応答は遅くなります。
Self Sign (自己署名)	このチェックボックスがオンになっていることを確認します。これにより、自己署名された証明書を作成していることがわかります。
Validity in days (有効日数)	このフィールドは、[Self Sign (自己署名)] チェックボックスがオンになると表示されます。このフィールドには、自己署名された証明書の有効日数を入力します。

注: [Organization (組織)], [Organizational Unit (組織ユニット)], [Email Address (電子メール アドレス)] の各フィールドを除いて、[Subject (サブジェクト)] セクションのすべてのフィールドは必須です。

自己署名された証明書にはパスワードは必要ないため、[Self Sign (自己署名)] チェックボックスをオンにすると、[Challenge (チャレンジ)] フィールドと [Confirm Challenge (チャレンジの確認)] フィールドは表示されなくなります。

4. [Create New SSL Key (SSL キーの新規作成)] をクリックし、自己署名された証明書と秘密キーの両方を作成します。この処理には数分かかる場合があります。
5. また、次のいずれかの操作を実行することもできます。
 - [Install Key and Certificate (キーと証明書のインストール)] をクリックし、自己署名された証明書と秘密キーを直ちにインストールします。確認メッセージやセキュリティ メッセージが表示されたら、[Yes (はい)] をクリックして続行します。

ヒント: 証明書が正常にインストールされたかどうかを確認するには、後で [Active SSL Certificate (アクティブな SSL 証明書)] タブをクリックします。

- 自己署名された証明書または秘密キーをダウンロードするには、[Download Certificate (証明書のダウンロード)] または [Download Key (キーのダウンロード)] をクリックします。ファイルを開くか保存するかを確認するメッセージが表示されます。[Save (保存)] をクリックして、コンピュータにファイルを保存します。
 - 自己署名された証明書と秘密キーを Dominion PX デバイスから完全に削除するには、[Delete Key and Certificate (キーと証明書の削除)] をクリックします。
6. 手順 5 で自己署名された証明書をインストールした場合は、インストールが完了すると、Dominion PX デバイスがリセットされ、ログイン ページが再び表示されます。

既存のキーと証明書ファイルのインストール

SSL 証明書と秘密キー ファイルをすでに入手している場合は、CSR や自己署名された証明書を作成せずに、証明書とキー ファイルを直接インストールできます。

▶ **既存のキーと証明書ファイルをインストールするには、次の手順に従います。**

1. [Device Settings (デバイスの設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 証明書)] を選択します。[Manage SSL Certificate (SSL 証明書の管理)] ダイアログ ボックスが表示されます。
2. [New SSL Certificate (新しい SSL 証明書)] タブをクリックします。
3. [Upload Key and Certificate (キーと証明書のアップロード)] チェックボックスをオンにします。[Key File (キー ファイル)] と [Certificate File (証明書ファイル)] のフィールドが表示されます。
4. [Key File (キー ファイル)] フィールドで、[Browse (参照)] をクリックして、秘密キー ファイルを選択します。
5. [Certificate File (証明書ファイル)] フィールドで、[Browse (参照)] をクリックして、証明書ファイルを選択します。
6. [Upload (アップロード)] をクリックします。選択したファイルが Dominion PX デバイ스에インストールされます。

ヒント: 証明書が正常にインストールされたかどうかを確認するには、後で [Active SSL Certificate (アクティブな SSL 証明書)] タブをクリックします。

7. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

キー ファイルと証明書ファイルのダウンロード

Dominion PX デバイスに現在インストールされているキー ファイルと証明書ファイルは、バックアップやその他の操作を行うためにダウンロードしておくことができます。たとえば、各ファイルを Dominion PX の代替デバイスにインストールしたり、ブラウザに証明書を追加したりすることができます。

► **Dominion PX デバイスから証明書ファイルとキー ファイルをダウンロードするには、次の手順に従います。**

1. [Device Settings (デバイスの設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 証明書)] を選択します。[Manage SSL Certificate (SSL 証明書の管理)] ダイアログ ボックスが表示されます。
2. [Active SSL Certificate (アクティブな SSL 証明書)] タブが表示されます。このタブが表示されない場合は、タブをクリックします。
3. [Download Key (キーのダウンロード)] をクリックし、Dominion PX デバイスにインストールされている秘密キー ファイルをダウンロードします。ファイルを開くか保存するかを確認するメッセージが表示されます。[Save (保存)] をクリックして、コンピュータにファイルを保存します。
4. [Download Certificate (証明書のダウンロード)] をクリックし、Dominion PX デバイスにインストールされている証明書ファイルをダウンロードします。ファイルを開くか保存するかを確認するメッセージが表示されます。[Save (保存)] をクリックして、コンピュータにファイルを保存します。
5. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

LDAP 認証の設定

セキュリティのために、Dominion PX へのログインを試みるユーザは認証される必要があります。Dominion PX は、次のいずれかの認証機構を使用したアクセスをサポートします。

- Dominion PX デバイス上のユーザ プロファイルのローカル データベース
- LDAP (Lightweight Directory Access Protocol)

Dominion PX のデフォルトの設定では、ローカル認証を使用できるように設定されています。この方法を使用する場合は、承認された各ユーザのユーザ プロファイルを作成するだけです。外部の LDAP サーバを使用する場合は、次のようにする必要があります。

- Dominion PX に LDAP サーバに関する情報を設定します。
- 外部で認証されたユーザのユーザ プロファイルを作成します。
Dominion PX デバイス上のユーザ プロファイルによって、ユーザに割り当てられる役割が決定され、それによってユーザの権限が決まるからです。

LDAP 認証を使用できるように設定した場合は、LDAP サーバ上にすべての Dominion PX ユーザのアカウントが必要です。ローカル認証のみのユーザは、Dominion PX にアクセスできません。ただし、管理者は常に Dominion PX にアクセスできるため、これには含まれません。

LDAP 情報の収集

Dominion PX で LDAP 認証の設定を行うには、LDAP サーバおよびディレクトリ設定に関する知識が必要です。この設定について十分な知識をお持ちでない場合は、LDAP 管理者に問い合わせてください。

LDAP 認証を設定するには、以下のことを確認する必要があります。

- LDAP サーバの IP アドレスまたはホスト名
- セキュア LDAP プロトコル (SSL over LDAP) が使用されているかどうか
 - セキュア LDAP が使用されている場合は、CA 証明書ファイルについて LDAP 管理者に問い合わせてください。
- LDAP サーバが使用するネットワーク ポート
- LDAP サーバのタイプ (通常は、次のいずれか)
 - *[OpenLDAP]*
 - OpenLDAP サーバを使用する場合、バインド識別名 (DN) とパスワードについては、LDAP 管理者に確認してください。
 - *Microsoft Active Directory® (AD)*

- Microsoft Active Directory サーバを使用する場合は、Active Directory ドメインの名前を AD 管理者に確認してください。
- バインド識別名 (DN) とパスワード (匿名バインドが使用されない場合)
- サーバのベース DN (ユーザの検索に使用)
- ログイン名の属性 (または AuthorizationString)
- ユーザ エントリのオブジェクト クラス
- ユーザ検索サブフィルタ (または BaseSearch)

LDAP サーバ設定の追加

外部の LDAP/LDAPS サーバ認証をアクティブにして使用するには、LDAP 認証を有効にし、LDAP/LDAPS サーバについて収集した情報を入力します。

注: LDAPS サーバとは、SSL で保護された LDAP サーバのことです。

▶ LDAP/LDAPS サーバ設定を追加するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)] を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。
2. [LDAP] ラジオ ボタンを選択し、リモート LDAP/LDAPS サーバ認証をアクティブにします。
3. [New (新規)] をクリックし、認証用の LDAP/LDAPS サーバを追加します。[Create new LDAP Server Configuration (LDAP サーバ設定の新規作成)] ダイアログ ボックスが表示されます。
4. [IP Address / Hostname (IP アドレス / ホスト名)] - LDAP/LDAPS 認証サーバの IP アドレスまたはホスト名を入力します。

重要: SSL 暗号化が有効になっていなくても、このフィールドにドメイン名または IP アドレスを入力できますが、SSL 暗号化が有効になっている場合は、完全修飾ドメイン名を入力する必要があります。

5. 外部 LDAP サーバの種類。使用可能な以下のオプションから選択します。
 - [OpenLDAP]
 - [Microsoft Active Directory]。Active Directory は、Windows 環境で使用できる、Microsoft によって実装された LDAP/LDAPS ディレクトリ サービスです。
6. LDAP over SSL - SSL を使用する場合は、このチェックボックスをオンにします。SSL (Secure Sockets Layer) は、Dominion PX が LDAP/LDAPS サーバと安全に通信できるようにする暗号化プロトコルです。
7. [Port (ポート)] - デフォルト ポートは 389 です。標準の LDAP TCP ポートを使用するか、別のポートを指定します。

8. [SSL Port (SSL ポート)] – デフォルトは 636 です。デフォルトのポートを使用するか、別のポートを指定します。[LDAP over SSL] チェックボックスがオンになっている場合に、このフィールドが有効になります。
9. [Use only trusted LDAP Server Certificates (信頼する LDAP サーバ証明書のみを使用する)] – 信頼する LDAP サーバ証明書ファイル、つまり、CA によって署名された証明書ファイルを使用する場合に、このチェックボックスをオンにします。オンにしていない場合は、自己署名された証明書ファイルを始めとする、すべての LDAP/LDAPS サーバ証明書を使用できます。証明書ファイルはこのオプションを有効にした後に必要になります。
10. [Server Certificate (サーバ証明書)] – LDAP/LDAPS サーバの CA 証明書ファイルを取得する場合は、認証サーバ管理者に問い合わせてください。[Browse (参照)] ボタンを使用して、証明書ファイルに移動します。このファイルは、[Use only trusted LDAP Server Certificates (信頼する LDAP サーバ証明書のみを使用する)] チェックボックスをオンにした場合に必要です。

ヒント: [Use only trusted LDAP Server Certificates (信頼する LDAP サーバ証明書のみを使用する)] チェックボックスをオンにする前に、まず今後使用する CA 証明書ファイルをアップロードしておく必要があります。その後、証明書ファイルの使用がなくなったときにこのチェックボックスをオンにします。

11. [Anonymous Bind (匿名バインド)] – OpenLDAP の場合、このチェックボックスを使用して、匿名バインドを有効または無効にします。
 - 匿名バインドを使用するには、このチェックボックスをオンにします。
 - 外部の LDAP/LDAPS サーバにバインドするためにバインド DN とパスワードが必要な場合は、このチェックボックスをオフにします。
12. [Use Bind Credentials (バインド証明書を使用)] – Microsoft Active Directory の場合、このチェックボックスを使用して、匿名バインドを有効または無効にします。
 - 匿名バインドを使用するには、このチェックボックスをオフにします。デフォルトではオフになっています。
 - 外部の LDAP/LDAPS サーバにバインドするためにバインド DN とパスワードが必要な場合は、このチェックボックスをオンにします。
13. [Bind DN (バインド DN)] – 定義済みの検索ベースにおいて LDAP ディレクトリの検索を許可されているユーザの DN を指定します。この情報は、[Use Bind Credential (バインド証明書を使用)] チェックボックスをオンにした場合にのみ必要です。

14. [Bind Password (バインド パスワード)] と [Confirm Bind Password (バインド パスワードの確認)] – 最初に [Bind Password (バインド パスワード)] フィールドに、次に [Confirm Bind Password (バインド パスワードの確認)] フィールドにバインド パスワードを入力します。この情報は、[Use Bind Credential (バインド証明書を使用)] チェックボックスをオンにした場合にのみ必要です。
15. [Base DN for Search (検索用のベース DN)] – LDAP/LDAPS にバインドする名前 (最長 31 文字) と、指定したベース DN の検索をデータベースのどこから開始するかを入力します。ベース検索の値は、たとえば「cn=Users,dc=raritan,dc=com」のようになります。これらのフィールドに入力する適切な値については、認証サーバ管理者に確認してください。
16. 以下の情報を対応するフィールドに入力します。LDAP は、ユーザ名およびパスワードを検証するために、この情報を必要とします。
 - ログイン名の属性 (AuthorizationString と呼ばれます)
 - ユーザ エントリのオブジェクト クラス
 - ユーザ検索サブフィルタ (BaseSearch と呼ばれます)

注: Dominion PX により、ログイン名の属性とユーザ エントリのオブジェクト クラスにデフォルト値が設定されます。この値は必要な場合を除き変更しないでください。

17. [Active Directory Domain (Active Directory ドメイン)] – Active Directory ドメインの名前を入力します。たとえば, testradius.com などです。具体的なドメイン名については、Active Directory 管理者に確認してください。
18. LDAP/LDAPS が正しく設定されているかどうかを確認するには、[Test Connection (テスト接続)] をクリックし、Dominion PX から LDAP/LDAPS サーバに正常に接続できるかどうかを確認します。

ヒント: この操作は、[Authentication Settings (認証設定)] ダイアログボックスの [Test Connection (テスト接続)] ボタンを使用して実行することもできます。

19. [OK] をクリックして変更を保存します。新しい LDAP サーバが [Authentication Settings (認証設定)] ダイアログ ボックスに表示されます。
20. さらに LDAP/LDAPS サーバを追加するには、手順 3 ～ 19 を繰り返します。
21. [OK] をクリックして変更を保存します。これで、LDAP 認証の準備が整いました。

注: *Dominion PX* クロックと *LDAP* サーバ クロックが同期されていない場合は、証明書が期限切れと見なされ、ユーザは *LDAP* を使用した認証ができません。適切な同期を維持するために、管理者は、*Dominion PX* と *LDAP* サーバが同じ *NTP* サーバを使用するように設定する必要があります。

AD 設定に関する詳細情報

Microsoft Active Directory を使用する *LDAP* 設定の詳細については、「*LDAP 設定の例*『446p.』」を参照してください。

LDAP アクセス順序の並べ替え

LDAP リストの順序によって、リモート *LDAP/LDAPS* サーバのアクセス優先順位が決まります。*Dominion PX* では、認証するために最初にリストの最上位の *LDAP/LDAPS* サーバへのアクセスが試行されます。最初のサーバへのアクセスが失敗すると、その次のサーバへのアクセスが試行され、以下同様に試行されます。この動作は、*Dominion PX* デバイスがリストのいずれかの *LDAP/LDAPS* サーバに正常に接続されるまで続きます。

注: いずれかの *LDAP/LDAPS* サーバに正常に接続されると、ユーザ認証結果にかかわらず、リストの残りの *LDAP/LDAPS* サーバへのアクセスは終了となります。

▶ **LDAP サーバ アクセス リストを並べ替えるには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)] を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。
2. 優先順位を変更する *LDAP/LDAPS* サーバを選択します。
3. 選択したサーバがリスト内の目的の位置に移動するまで [Move up (上に移動)] または [Move down (下に移動)] をクリックします。
4. [OK] をクリックして変更を保存します。

LDAP サーバ接続のテスト

LDAP/LDAPS サーバへの接続をテストすると、サーバ アクセシビリティまたは認証設定の妥当性を確認できます。

▶ **LDAP/LDAPS サーバへの接続をテストするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)] を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。

2. テストする LDAP/LDAPS サーバを選択します。
3. [Test Connection (テスト接続)] をクリックして、接続テストを開始します。

LDAP サーバ設定の編集

LDAP/LDAPS サーバの設定（ポート番号、バインド DN、パスワードなど）が変更された場合は、Dominion PX デバイスの LDAP/LDAPS 設定を適宜変更する必要があります。変更しないままでは、認証が失敗します。

▶ **LDAP 認証設定を変更するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)] を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。
2. 編集する LDAP/LDAPS サーバを選択します。
3. [Edit (編集)] をクリックします。[Edit LDAP Server Configuration (LDAP サーバ設定の編集)] ダイアログ ボックスが表示されます。
4. 表示される内容に必要な変更を加えます。
5. [OK] をクリックして変更を保存します。

LDAP サーバ設定の削除

特定の LDAP/LDAPS サーバが使用可能でない場合や、リモート認証に使用されていない場合は、そのサーバの認証設定を削除できます。

▶ **1 つまたは複数の LDAP/LDAPS サーバを削除するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)] を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。
2. 削除する LDAP/LDAPS サーバを選択します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
3. [Delete (削除)] をクリックします。
4. 操作の確認を求めるメッセージが表示されます。[Yes (はい)] をクリックして、削除を確認します。
5. [OK] をクリックして変更を保存します。

LDAP 認証の無効化

リモート認証サービスが無効になっている場合は、Dominion PX デバイスに保存されているローカル データベースを使用してユーザが認証されます。

▶ **LDAP 認証サービスを無効にするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)] を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。
2. [Local Authentication (ローカル認証)] ラジオ ボタンを選択します。
3. [OK] をクリックして変更を保存します。

LDAP とローカル認証サービスの有効化

外部の認証を利用できないときにも、認証機能を常に正常に機能させるために、ローカル認証サービスとリモート認証サービスの両方を有効にすることができます。

両方の認証サービスが有効になっている場合、Dominion PX の認証では次のルールが適用されます。

- アクセス リストのいずれかの LDAP/LDAPS サーバにアクセスできる場合は、接続された LDAP/LDAPS サーバに対してのみ認証が行われます。
- LDAP/LDAPS サーバへの接続がすべて失敗する場合は、ローカル データベースに対する認証が許可されます。

▶ **両方の認証サービスを有効にするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)] を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。
2. [LDAP] ラジオ ボタンが選択されていることを確認します。
3. [Use Local Authentication if Remote Authentication service is not available (リモート認証サービスを利用できない場合にローカル認証を使用する)] チェックボックスをオンにします。
4. [OK] をクリックして変更を保存します。

アウトレット (コンセント) 管理

Dominion PX では、Web インタフェースを介して、各アウトレット (コンセント) の名前をリモートでカスタマイズしたり、各アウトレット (コンセント) に関連付けられているサーキット ブレーカをリモートで確認したりできます。

PX-2000 シリーズでは、各アウトレット (コンセント) をリモートでオンまたはオフにすることもできます。

アウトレット (コンセント) の名前付け

アウトレット (コンセント) に接続された装置を識別するために、各アウトレット (コンセント) に最大 32 文字の一意の名前を付けることができます。カスタマイズされた名前の後に括弧で囲まれたラベルが付きます。

注: このコンテキストでは、ラベルは、アウトレット (コンセント) 番号 (1、2、3 など) に該当します。

▶ **アウトレット (コンセント) に名前を付けるには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*」『76p. の「ツリーの展開」参照』を参照してください。
2. Dominion PX Explorer ペインで [Outlets (アウトレット (コンセント))] をクリックすると、右側のペインにアウトレット (コンセント) のページが表示されます。
3. 右側のペインで目的のアウトレット (コンセント) をクリックします。

ヒント: PX-2000 シリーズでは、Dominion PX Explorer ペインで目的のアウトレット (コンセント) をクリックできます。

4. [Settings (設定)] セクションで [Setup (設定)] をクリックします。選択したアウトレット (コンセント) の設定ダイアログ ボックスが表示されます。
5. 名前を [Outlet Name (アウトレット (コンセント) 名)] フィールドに入力します。
6. [OK] をクリックして変更を保存します。

関連するサーキット ブレーカの確認

各アウトレット (コンセント) が PDU のどのサーキット ブレーカによって保護されているかは、[Outlets (アウトレット (コンセント))] ページで確認できます。

ヒント: 同じ情報は、[Maintenance (メンテナンス)] > [Device Information (デバイス情報)] を選択して、確認することもできます。『PDU 情報の表示』『89p.』を参照してください。

▶ すべてのアウトレット (コンセント) の関連するサーキット ブレーカを確認するには、次の手順に従います。

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*」『76p. の「ツリーの展開」参照』を参照してください。
2. Dominion PX Explorer ペインで [Outlets (アウトレット (コンセント))] をクリックすると、右側のペインにアウトレット (コンセント) のページが表示されます。

サーキット ブレーカが関連付けられているすべてのアウトレット (コンセント) は、[Overcurrent Protector (過電流プロテクタ)] 列に表示されます。



Outlets		
#	Name (Label)	Overcurrent Protector
1	Outlet 1	Overcurrent Protector C1
2	Outlet 2	Overcurrent Protector C1
3	Outlet 3	Overcurrent Protector C1
4	Outlet 4	Overcurrent Protector C1
5	Outlet 5	Overcurrent Protector C2
6	Outlet 6	Overcurrent Protector C2
7	Outlet 7	Overcurrent Protector C2
8	Outlet 8	Overcurrent Protector C2

アウトレット (コンセント) 切り替え

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

Web インタフェースで 1 回クリックするだけで、1 つ以上のアウトレット (コンセント) の電力ステータスを変更できます。電源の状態を変更するには、PDU にアウトレット (コンセント) 切り替え機能が搭載されている必要があります。また、ユーザが *Switch Outlet* (アウトレット (コンセント) の切り替え) 権限を持っている必要があります。

注: *Dominion PX* デバイスでアウトレット (コンセント) 切り替えがサポートされていない場合は、ユーザの権限にかかわらず電源のオン/オフを切り替えられるアウトレット (コンセント) はありません。

複数またはすべてのアウトレット (コンセント) の切り替え

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

電源の状態は、各アウトレット (コンセント) のそのときの状態に関係なく変更できます。つまり、対象のアウトレット (コンセント) が、すでに選択された状態になっていたとしても、アウトレット (コンセント) の電源のオン、オフ、または再投入ができます。

アウトレット (コンセント) の電源再投入によって、アウトレット (コンセント) がオフにされてからオンに戻されます。

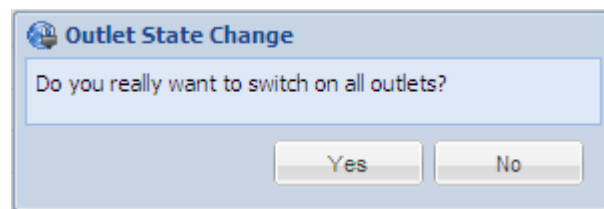
▶ 複数またはすべてのアウトレット (コンセント) の電源をオン、オフ、または再投入するには、次の手順に従います。

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*」『76p. の「ツリーの展開」参照』を参照してください。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「*Naming the PDU (PDU のネーミング)*」『90p. の「PDU の名前付け」参照先』を参照してください。

2. Outlets (アウトレット (コンセント)) フォルダをクリックすると、右側のペインに [Outlets (アウトレット (コンセント))] ページが表示されます。
3. 電源の状態を変更するアウトレット (コンセント) を選択し、そのチェックボックスがすべてオンになっていることを確認します。

- すべてのアウトレット (コンセント) を選択するには、見出し行の上部のチェックボックスをオンにします。
 - 複数のアウトレット (コンセント) を選択するには、目的の各アウトレット (コンセント) のチェックボックスを 1 つずつオンにします。
 - 1 つのアウトレット (コンセント) を選択するには、そのアウトレット (コンセント) のチェックボックスをオンにします。
4. [On (オン)], [Off (オフ)], または [Cycle (再投入)] をクリックします。
 5. 操作の確認のためのダイアログ ボックスが表示されます。 [Yes (はい)] をクリックすると、すべてのアウトレット (コンセント) の電源をオン、オフ、または再投入できます。



1 つのアウトレット (コンセント) の切り替え

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にも適用されます。

どのアウトレット (コンセント) も、その現在の状態に関係なく電源オン、オフ、または再投入できます。

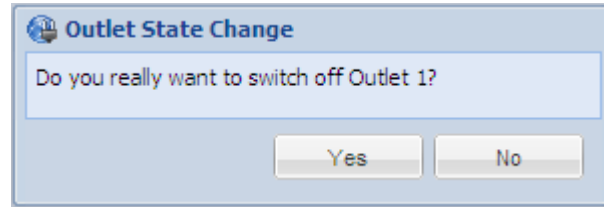
アウトレット (コンセント) の電源再投入によって、アウトレット (コンセント) がオフにされてからオンに戻されます。

アウトレット (コンセント) の電源をオン、オフ、または再投入するには、さまざまな方法があります。

▶ 特定のアウトレット (コンセント) アイコンを選択した状態でアウトレット (コンセント) を制御するには、次の手順に従います。

1. Outlets (アウトレット (コンセント)) フォルダが展開されていない場合は、フォルダを展開して、すべてのアウトレット (コンセント) を表示します。「ツリーの展開『76p.』」を参照してください。
2. PX Explorer ペインで目的のアウトレット (コンセント) をクリックして、右側のペインの [Control (制御)] セクションを見つけます。
3. [On (オン)], [Off (オフ)], または [Cycle (再投入)] をクリックします。

4. 操作の確認のためのダイアログ ボックスが表示されます。[Yes (はい)] をクリックすると、アウトレット (コンセント) のオンまたはオフが切り替わるか、電源が再投入されます。



- ▶ **Outlets (アウトレット (コンセント)) フォルダ アイコンを選択した状態でアウトレット (コンセント) を制御するには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*」『76p. の「ツリーの展開」参照 』」を参照してください。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「*Naming the PDU (PDU のネーミング)*」『90p. の「PDU の名前付け」参照先 』」を参照してください。

2. Outlets (アウトレット (コンセント)) フォルダをクリックすると、右側のペインに [Outlets (アウトレット (コンセント))] ページが表示されます。
3. 右側のペインで目的のアウトレット (コンセント) をクリックすると、対応するチェックボックスがオンになります。
4. [On (オン)]、[Off (オフ)]、または [Cycle (再投入)] をクリックします。
5. 操作の確認のためのダイアログ ボックスが表示されます。[Yes (はい)] をクリックすると、アウトレット (コンセント) のオンまたはオフが切り替わるか、電源が再投入されます。

コンセントのデフォルト状態の設定

このセクションは、アウトレット（コンセント）切り替え対応 PDU にも適用されます。

デフォルトのアウトレット（コンセント）の状態は、Dominion PX デバイスの電源がオンになった後のアウトレット（コンセント）の電源の初期状態によって決まります。すべてのアウトレット（コンセント）、または特定のアウトレット（コンセント）のデフォルト状態を設定できます。個々のアウトレット（コンセント）に設定した値は、常にすべてのアウトレット（コンセント）に対して設定された値を上書きすることに注意してください。

PDU から電源を取り外す場合は、電源を 10 分以上オフにしておく必要があります。そうしなければ、PDU の電源を再びオンにした後、アウトレット（コンセント）のデフォルト状態の設定が正しく機能しない場合があります。

PDU 定義のデフォルト状態の設定

このセクションは、アウトレット（コンセント）切り替え対応 PDU にも適用されます。

この手順では、PDU 定義のアウトレット（コンセント）状態を設定します。これによって、Dominion PX デバイスの電源がオンになった後のすべてのアウトレット（コンセント）の初期電源状態が決まります。

ヒント: 特定のアウトレット（コンセント）に異なる状態を設定する方法については、「アウトレット（コンセント）固有のデフォルト状態の設定 [159p.]」を参照してください。

▶ **すべてのアウトレット（コンセント）のデフォルト状態を設定するには、次の手順に従います。**

1. PDU フォルダをクリックします。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「Naming the PDU (PDU のネーミング) [90p. の PDU の名前付け参照先]」を参照してください。

2. [設定] セクションの [Setup (セットアップ)] をクリックします。[Pdu Setup (PDU のセットアップ)] ダイアログ ボックスが開きます。
3. [Outlet state on device startup (デバイス起動時のアウトレット（コンセント）の状態)] フィールドのドロップダウン矢印をクリックし、リストからオプションを選択します。

- [on(オン)]: Dominion PX デバイスの電源がオンになったときに、すべてのアウトレット (コンセント) の電源をオンにします。
 - [off(オフ)]: Dominion PX デバイスの電源がオンになったときに、すべてのアウトレット (コンセント) の電源をオフにします。
 - [last known (前回の状態)]: すべてのアウトレット (コンセント) を、Dominion PX デバイスの電源がオフになる前の電源の状態に戻します。
4. [OK] をクリックして変更を保存します。

アウトレット (コンセント) 固有のデフォルト状態の設定

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

デフォルトでは、各アウトレット (コンセント) の電源状態は、PDU 定義の設定に従います。特定のアウトレット (コンセント) のデフォルト状態を [PDU defined (PDU 定義)] 以外の値に設定すると、そのアウトレット (コンセント) では、PDU 定義の設定が上書きされます。

▶ 特定のアウトレット (コンセント) の電源のデフォルト状態を設定するには、次の手順に従います。

1. Outlets (アウトレット (コンセント)) フォルダが展開されていない場合は、フォルダを展開して、すべてのアウトレット (コンセント) を表示します。「ツリーの展開 [76p.]」を参照してください。
2. Dominion PX Explorer ペインで目的のアウトレット (コンセント) をクリックします。そのアウトレット (コンセント) に固有のページが右側のペインに表示されます。
3. [Settings (設定)] セクションで [Setup (設定)] をクリックします。選択したアウトレット (コンセント) の設定ダイアログ ボックスが表示されます。

ヒント: Outlets (アウトレット (コンセント)) フォルダが選択されている場合は、[Outlets (アウトレット (コンセント))] ページでアウトレット (コンセント) を強調表示して、[Setup (設定)] をクリックする方法でも、同じダイアログ ボックスを表示できます。

4. [State on device startup (デバイス起動時の状態)] フィールドのドロップダウン矢印をクリックし、リストからオプションを選択します。
 - [on(オン)]: Dominion PX デバイスの電源がオンになったときに、このアウトレット (コンセント) の電源をオンにします。
 - [off(オフ)]: Dominion PX デバイスの電源がオンになったときに、このアウトレット (コンセント) の電源をオフにします。
 - [last known (前回の状態)]: このアウトレット (コンセント) を、Dominion PX デバイスの電源がオフになる前の電源の状態に戻します。

- [PDU defined (PDU 定義)]: アウトレット (コンセント) のデフォルトの電源の状態は、PDU 定義の状態によって決まります。
「**PDU 定義のデフォルト状態の設定** 『158p. 』」を参照してください。

ヒント: [PDU defined (PDU 定義)] オプションの後に続くカッコ内の情報は、現在の PDU 定義の選択内容を示しています。

5. [OK] をクリックして変更を保存します。

電源再投入時の電源オフ時間の変更

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

アウトレット (コンセント) の電源再投入によって、アウトレット (コンセント) がオフにされてからオンに戻されます。電源の再投入で電源をオフにされたアウトレット (コンセント) が再びオンにされるまでの時間の長さを調整できます。

電源再投入時の電源オフ時間は、すべてのアウトレット (コンセント) に対して、または個別のアウトレット (コンセント) に対して設定できます。個々のアウトレット (コンセント) に設定した値は、常にすべてのアウトレット (コンセント) に対して設定された値を上書きすることに注意してください。

PDU 定義の電源再投入時の電源オフ時間の変更

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

「PDU 定義」の電源オフ時間によって、すべてのアウトレット (コンセント) の電源が、電源再投入時にオフにされてから再びオンになるまでの時間が決まります。デフォルトの PDU 定義の電源オフ時間は、10 秒 (10 s) です。

注: 特定のアウトレット (コンセント) に異なる電源オフ時間を設定する方法については、「**アウトレット (コンセント) 固有の電源再投入時の電源オフ時間の変更** 『161p. 』」を参照してください。

- ▶ **すべてのアウトレット (コンセント) の電源オフ時間を設定するには、次の手順に従います。**

1. PDU フォルダをクリックします。

注：PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、『Naming the PDU (PDU のネーミング)』90p. の「PDU の名前付け」参照先』を参照してください。

2. [設定] セクションの [Setup (セットアップ)] をクリックします。[Pdu Setup (PDU のセットアップ)] ダイアログ ボックスが開きます。
3. [Power off period during power cycle (電源再投入時の電源オフ時間)] フィールドのドロップダウン矢印をクリックし、リストからオプションを選択します。有効な範囲は 0 秒～ 1 時間です。
リストの時間の単位について次に説明します。
 - s: 秒
 - min: 分
 - h: 時

目的の時刻がリストにない場合は、値を入力することもできます。たとえば、15 秒の遅延が必要な場合は、「15 s」と入力します。

4. [OK] をクリックして変更を保存します。

ヒント：多数のアウトレット (コンセント) が存在する場合は、すべてのアウトレット (コンセント) が再度使用可能になるまで長時間待たなくとも済むように、値を短い数値に設定します。

アウトレット (コンセント) 固有の電源再投入時の電源オフ時間の変更

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

電源再投入時、各アウトレット (コンセント) のデフォルトの電源オフ時間は、PDU 定義の設定に従います。特定のアウトレット (コンセント) の電源オフ時間を調整して、電源がオンになるまでの電源オフ時間をさまざまに設定できます。

特定のアウトレット (コンセント) の電源オフ時間を [PDU defined (PDU 定義)] 以外の値に設定すると、そのアウトレット (コンセント) では、PDU 定義の設定が上書きされます。

▶ 特定のアウトレット (コンセント) の電源オフ時間を設定するには、次の手順に従います。

1. Outlets (アウトレット (コンセント)) フォルダが展開されていない場合は、フォルダを展開して、すべてのアウトレット (コンセント) を表示します。「ツリーの展開」76p.』を参照してください。
2. Dominion PX Explorer ペインで目的のアウトレット (コンセント) をクリックします。そのアウトレット (コンセント) に固有のページが右側のペインに表示されます。

3. [Settings (設定)] セクションで [Setup (設定)] をクリックします。選択したアウトレット (コンセント) の設定ダイアログ ボックスが表示されます。

ヒント: Outlets (アウトレット (コンセント)) フォルダが選択されている場合は、[Outlets (アウトレット (コンセント))] ページでアウトレット (コンセント) を強調表示して、[Setup (設定)] をクリックする方法でも、同じダイアログ ボックスを表示できます。

4. [Power off period during power cycle (電源再投入時の電源オフ時間)] フィールドのドロップダウン矢印をクリックし、リストからオプションを選択します。有効な範囲は 0 秒～ 1 時間です。

リストの時間の単位について次に説明します。

- s: 秒
- min: 分
- h: 時
- アウトレット (コンセント) の電源オフ時間を PDU 定義の設定と同じにするには、[PDU defined (PDU 定義)] オプションを選択します。「**PDU 定義の電源再投入時の電源オフ時間の変更『160p.』**」を参照してください。

ヒント: [PDU defined (PDU 定義)] オプションの後に続くかっこ内の情報は、現在の PDU 定義の選択内容を示しています。

目的の時刻がリストにない場合は、値を入力することもできます。たとえば、15 秒の遅延が必要な場合は、「15 s」と入力します。

5. [OK] をクリックして変更を保存します。

初期化遅延の設定

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

アウトレット (コンセント) の初期化遅延では、電源再投入時、または一時的な電源切れなどから回復するときに、Dominion PX デバイスが、すべてのアウトレット (コンセント) への電力供給を開始する前に待機する時間を決定します。これは、リストアップ後すぐの電力が安定しない可能性がある場合、または UPS バッテリーが充電中の可能性がある場合に便利です。

- ▶ **すべてのアウトレット (コンセント) の初期化遅延を設定するには、次の手順に従います。**

1. PDU フォルダをクリックします。

注：PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、『Naming the PDU (PDU のネーミング)』90p. の「PDU の名前付け参照先」を参照してください。

2. [設定] セクションの [Setup (セットアップ)] をクリックします。[Pdu Setup (PDU のセットアップ)] ダイアログ ボックスが開きます。
3. [Outlet state on device startup (デバイス起動時のアウトレット (コンセント) の初期化遅延)] フィールドのドロップダウン矢印をクリックし、リストからオプションを選択します。有効な範囲は 1 秒～ 1 時間です。
リストの時間の単位について次に説明します。
 - s: 秒
 - min: 分
 - h: 時
4. [OK] をクリックして変更を保存します。

ヒント：多数のアウトレット (コンセント) が存在する場合は、すべてのアウトレット (コンセント) が再度使用可能になるまで長時間待たなくても済むように、値を短い数値に設定します。

突入電流防止遅延の設定

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

電気機器の電源をオンにすると、最初に突入電流と呼ばれる大量の電流が引き込まれることがあります。突入電流は、通常 20 ～ 40 ミリ秒間続きます。突入電流防止遅延機能は、多くのデバイスの電源が同時にオンになって一度に大量の突入電流が発生することにより、サーキット ブレーカが作動するのを防止します。たとえば、突入電流防止遅延を 100 ミリ秒に設定し、2 つ以上のアウトレット (コンセント) を同時にオンにすると、PDU はアウトレット (コンセント) を順番にオンにしますが、それぞれ 100 ミリ秒遅らせます。

▶ 突入電流防止遅延時間を設定するには、次の手順に従います。

1. PDU フォルダをクリックします。

注：PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、『Naming the PDU (PDU のネーミング)』90p. の「PDU の名前付け参照先」を参照してください。

2. [設定] セクションの [Setup (セットアップ)] をクリックします。[Pdu Setup (PDU のセットアップ)] ダイアログ ボックスが開きます。

3. [Inrush Guard Delay (突入電流防止遅延)] フィールドのドロップダウン矢印をクリックし、リストからオプションを選択します。有効な範囲は 100 ミリ秒～ 100 秒です。
リストの時間の単位について次に説明します。
 - ms: ミリ秒
 - s: 秒
4. [OK] をクリックして変更を保存します。

アウトレット (コンセント) の電源オン順序の設定

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

デフォルトでは、Dominion PX デバイスのすべてのアウトレット (コンセント) の電源をオンまたは再投入する場合、アウトレット (コンセント) は、アウトレット (コンセント) 1 から高位番号のアウトレット (コンセント) の昇順で、順次電源がオンにされます。アウトレット (コンセント) の電源がオンになる順序は、変更できます。これは、接続されている IT 機器の電源をオンにするときに特定の順序に従う必要がある場合に便利です。

▶ **アウトレット (コンセント) の電源オン順序を設定するには、以下の手順に従います。**

1. 次のいずれかを実行して、[Outlet Sequence Setup(アウトレット (コンセント) の順序の設定)] ダイアログ ボックスを表示します。
 - Outlets (アウトレット (コンセント)) フォルダをクリックすると、右側のペインに [Outlets (アウトレット (コンセント))] ページが表示されます。[Sequence Setup (順序の設定)] をクリックします。
 - PDU フォルダをクリックし、[Outlet Sequence (アウトレット (コンセント) の順序)] セクションで [Setup (設定)] ボタンをクリックします。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、『Naming the PDU (PDU のネーミング)』90p. の「PDU の名前付け参照先」を参照してください。

[Outlet Sequence Setup (アウトレット (コンセント) の順序の設定)] ダイアログ ボックスが表示され、現在の電源オン順序がリストのアウトレット (コンセント) 順序で示されます。

2. アウトレット (コンセント) の優先順位を変更するには、一覧から選択して次のボタンのいずれかをクリックします。

- : アウトレット (コンセント) が一覧の一番上に移動し、電源が供給される最初のアウトレット (コンセント) になります。
 - : アウトレット (コンセント) が一覧内の 1 つ上に移動します。
 - : アウトレット (コンセント) が一覧内の 1 つ下に移動します。
 - : アウトレット (コンセント) が一覧の一番下に移動し、電源が供給される最後のアウトレット (コンセント) になります。
 - : リストをデフォルトの電源オン順序 (昇順) に戻します。
3. リストの並べ替え、または表示列の変更を行うことができます。 リストを並べ替えると、アウトレット (コンセント) の電源オン順序が変わります。
 4. [OK] をクリックして変更を保存します。

次回 PDU の電源を再投入すると、リストの新しい順序に基づいてすべてのアウトレット (コンセント) の電源がオンになります。

アウトレット (コンセント) 固有の電源オン遅延の設定

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

PDU ですべてのアウトレット (コンセント) がオンになったときに連続してオンになる 2 つのアウトレット (コンセント) 間で電源オン遅延を発生させることができます。

たとえば、電源オン順序がアウトレット (コンセント) 1 ~ アウトレット (コンセント) 12 の場合、PDU でアウトレット (コンセント) 3 をオンにしてからアウトレット (コンセント) 4 をオンにするまで 5 秒間待機するには、アウトレット (コンセント) 3 に対して 5 秒間の遅延を割り当てます。

▶ アウトレット (コンセント) 固有の電源オン遅延を設定するには、次の手順に従います。

1. 次のいずれかを実行して、[Outlet Sequence Setup(アウトレット (コンセント) の順序の設定)] ダイアログ ボックスを表示します。
 - Outlets (アウトレット (コンセント)) フォルダをクリックすると、右側のペインに [Outlets (アウトレット (コンセント))] ページが表示されます。[Sequence Setup (順序の設定)] をクリックします。
 - PDU フォルダをクリックし、[Outlet Sequence (アウトレット (コンセント) の順序)] セクションで [Setup (設定)] ボタンをクリックします。

2. オンにした後で遅延を発生させるアウトレット (コンセント) の [Delay (遅延)] 列をクリックし、既存の値を削除して新しい数値を秒単位で入力します。数値は 10 進数です。
 - 遅延を無効にするには、数値 0 (ゼロ) を入力するだけです。
3. 上記の手順を繰り返して、他のアウトレット (コンセント) の遅延設定を変更します。
4. [OK] をクリックして変更を保存します。

非臨界アウトレット (コンセント) と負荷遮断モードの設定

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

PDU スイッチに電力を供給する UPS がバッテリー バックアップ動作に切り替わったら、非臨界アウトレット (コンセント) をオフにして UPS のバッテリー寿命を延ばすことが望ましい場合があります。この機能は、負荷遮断と呼ばれます。

負荷遮断を有効にするには、Web インタフェース、SNMP、CLI を使用するか、接点閉鎖センサーによってトリガします。

負荷遮断を有効にするときにオフになるアウトレット (コンセント) は、非臨界アウトレット (コンセント) と呼ばれます。負荷遮断の影響を受けないアウトレット (コンセント) は、臨界アウトレット (コンセント) と呼ばれます。負荷遮断が無効である場合、PDU はすべての非臨界アウトレット (コンセント) を再びオンにします。デフォルトでは、すべてのアウトレット (コンセント) は、他の方法で設定するまで臨界として設定されます。

すべてのアウトレット (コンセント) のマーク付け

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

すべての臨界および非臨界アウトレット (コンセント) を一度に設定できます。

- ▶ **すべてのアウトレット (コンセント) に一度にマークを付けるには、次の手順に従います。**

1. PDU フォルダをクリックします。

注 : PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、『Naming the PDU (PDU のネーミング) 』90p. の「PDU の名前付け参照先」を参照してください。

2. [Load Shedding (負荷遮断)] セクションで [Setup Non-Critical Outlets (非臨界アウトレット (コンセンメント) の設定)] をクリックします。
[Non-critical Outlet Setup (非臨界アウトレット (コンセンメント) の設定)] ダイアログ ボックスが表示されます。

ヒント: このダイアログ ボックスは、Outlets (アウトレット (コンセンメント)) フォルダを選択するときに、[Outlets (アウトレット (コンセンメント))] ページで [Non-critical Outlet Setup (非臨界アウトレット (コンセンメント) の設定)] ボタンをクリックして開くこともできます。

3. アウトレット (コンセンメント) に「非臨界」のマークを付けるには、[Critical outlets (臨界アウトレット (コンセンメント))] ペインでリストからアウトレット (コンセンメント) を選択し、 をクリックして [Non-critical outlets (非臨界アウトレット (コンセンメント))] ペインに移動します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
4. アウトレット (コンセンメント) に「臨界」のマークを付けるには、[Non-critical outlets (非臨界アウトレット (コンセンメント))] ペインでリストからアウトレット (コンセンメント) を選択し、 をクリックして [Critical outlets (臨界アウトレット (コンセンメント))] ペインに移動します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
5. [OK] をクリックして変更を保存します。

アウトレット (コンセンメント) のマーク付け

このセクションは、アウトレット (コンセンメント) 切り替え対応 PDU にのみ適用されます。

設定ダイアログ ボックスで特定のアウトレット (コンセンメント) に臨界または非臨界のマークを付けることもできます。

▶ アウトレット (コンセンメント) にマークを付けるには、次の手順に従います。

1. Outlets (アウトレット (コンセンメント)) フォルダが展開されていない場合は、フォルダを展開して、すべてのアウトレット (コンセンメント) を表示します。「ツリーの展開」『76p.』を参照してください。
2. Dominion PX Explorer ペインで目的のアウトレット (コンセンメント) をクリックします。そのアウトレット (コンセンメント) に固有のページが右側のペインに表示されます。
3. [Settings (設定)] セクションで [Setup (設定)] をクリックします。選択したアウトレット (コンセンメント) の設定ダイアログ ボックスが表示されます。

ヒント: *Outlets (アウトレット (コンセント))* フォルダが選択されている場合は、*[Outlets (アウトレット (コンセント))]* ページでアウトレット (コンセント) を強調表示して、*[Setup (設定)]* をクリックする方法でも、同じダイアログ ボックスを表示できます。

4. [Non Critical (非臨界)] フィールドで、ドロップダウン リストからオプションを選択します。
 - [True (True)]: このオプションは、アウトレット (コンセント) に非臨界のマークを付けます。
 - [False (False)]: このオプションは、アウトレット (コンセント) に臨界のマークを付けます。
5. [OK] をクリックして変更を保存します。

負荷遮断モードの有効化または無効化

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

負荷遮断モードに入ると、Dominion PX はすべての非臨界アウトレット (コンセント) をオフにします。

負荷遮断モードを終了すると、Dominion PX は、負荷遮断モードに入る前にオンになっていたすべての非臨界アウトレット (コンセント) をオンにします。

このモードは、[PDU] ページまたは [Outlets (アウトレット (コンセント))] ページから有効または無効にすることができます。

► [PDU] ページから負荷遮断モードに入る、または負荷遮断モードを終了するには、次の手順に従います。

1. PDU フォルダをクリックします。

注: PDU フォルダは、デフォルトでは「*my PX*」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、『*Naming the PDU (PDU のネーミング)* 90p. の「PDU の名前付け参照先」を参照してください。

2. [Load Shedding (負荷遮断)] セクションで、[Enable Load Shedding (負荷遮断を有効にする)] をクリックして負荷遮断モードに入るか、[Disable Load Shedding (負荷遮断を無効にする)] をクリックして負荷遮断モードを無効にします。
3. この操作を確認するように求められます。

4. 前の手順でモードを有効にするように選択した場合は、[Yes (はい)] をクリックしてすべての非臨界アウトレット (コンセント) をオフにします。モードを無効にするように選択した場合は、[Yes (はい)] をクリックして、負荷遮断モードの前にすでにオンになっていたすべての非臨界アウトレット (コンセント) をオンにします。

▶ **[Outlets (アウトレット (コンセント))] ページから負荷遮断モードに入る、または負荷遮断モードを終了するには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*」『76p. の「ツリーの展開」参照』を参照してください。
2. Outlets (アウトレット (コンセント)) フォルダをクリックすると、右側のペインに [Outlets (アウトレット (コンセント))] ページが表示されます。
3. 負荷遮断モードに入るには、[Load Shedding (負荷遮断)] チェックボックスをオンにします。負荷遮断モードを終了するには、[Load Shedding (負荷遮断)] チェックボックスをオフにします。
4. この操作を確認するように求められます。
5. 前の手順でモードを有効にするように選択した場合は、[Yes (はい)] をクリックしてすべての非臨界アウトレット (コンセント) をオフにします。モードを無効にするように選択した場合は、[Yes (はい)] をクリックして、負荷遮断モードの前にすでにオンになっていたすべての非臨界アウトレット (コンセント) をオンにします。

注: 負荷遮断モードの間は、[Outlets (アウトレット (コンセント))] ページのすべての非臨界アウトレット (コンセント) にこのアイコン  が表示され、それらのアウトレット (コンセント) をオンにすることはできません。

インレットとサーキット ブレーカの管理

各インレットやサーキット ブレーカに名前を付けたり、それらの状態を監視したりすることができます。

インレットの名前付け

目的に合わせてインレットの名前をカスタマイズできます。カスタマイズされた名前の後に括弧で囲まれたラベルが付きます。

注: このコンテキストでは、ラベルは、インレット番号 (I1 など) に該当します。

▶ **インレットに名前を付けるには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*」『76p. の「ツリーの展開」参照』」を参照してください。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「*Naming the PDU (PDU のネーミング)*」『90p. の「PDU の名前付け」参照先』」を参照してください。

2. Dominion PX Explorer ペインで [Inlet I1 (インレット I1)] をクリックすると、右側のペインにインレット I1 のページが表示されます。
3. [Setup (設定)] をクリックします。[Inlet I1 Setup (インレット 1 の設定)] ダイアログ ボックスが表示されます。
4. 新しい名前を [Name (名前)] フィールドに入力します。
5. [OK] をクリックして変更を保存します。

サーキット ブレーカの名前付け

各サーキット ブレーカに名前を付けると、ブレーカの識別が簡単になります。

カスタマイズされた名前の後に括弧で囲まれたラベルが付きます。

注: このコンテキストでは、ラベルは、サーキット ブレーカ番号 (C1 など) に該当します。

▶ **サーキット ブレーカに名前を付けるには、次の手順に従います。**

1. 過電流プロテクタ フォルダを展開し、Dominion PX Explorer ペインですべてのサーキット ブレーカを表示します。「*ツリーの展開*」『76p. 』」を参照してください。
2. Dominion PX Explorer ペインで目的のサーキット ブレーカをクリックすると、右側のペインにこのサーキット ブレーカのページが表示されます。
3. [Setup (設定)] をクリックします。[Overcurrent Protector Setup (過電流プロテクタの設定)] ダイアログ ボックスが表示されます。

ヒント: このダイアログ ボックスは、Dominion PX Explorer ペインの [Overcurrent Protectors (過電流プロテクタ)] フォルダが選択されている場合に [Overcurrent Protectors (過電流プロテクタ)] ページの [Setup (設定)] ページをクリックする方法でも表示できます。

4. 新しい名前を [Name (名前)] フィールドに入力します。
5. [OK] をクリックして変更を保存します。

インレットの監視

インレットの詳細情報を表示できます。表示できる内容には、以下のものがあります。

- ラベル (番号)
- カスタマイズされた名前
- インレット センサー測定値:
 - ラインあたりの RMS 電流 (A)
 - ライン ペアあたりの RMS 電圧 (V)
 - 有効電力 (W)
 - 皮相電力 (VA)
 - 力率
 - 電力量 (Wh)
 - 不平衡負荷 (%)

注: センサーの測定値が色付きで表示される場合は、測定値がしきい値のいずれかをすでに超えていることを表します。『測定値の黄色表示または赤色表示』『82p.』を参照してください。

インレット情報へのアクセス方法には、次の 2 種類があります。

▶ **インレットの状態の概要を取得するには、次の手順に従います。**

1. Dominion PX Explorer ペインで [ダッシュボード] アイコンをクリックすると、右側のペインに [ダッシュボード] ページが表示されます。
2. ダッシュボード ページでインレットのセクションを探します。

▶ **インレットの詳細を表示するには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、『*Expanding the Tree (ツリーの展開)*』『76p. の“ツリーの展開”参照』を参照してください。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、『*Naming the PDU (PDU のネーミング)*』『90p. の PDU の名前付け”参照先』を参照してください。

2. Dominion PX Explorer ペインで [Inlet I1 (インレット I1)] をクリックすると、右側のペインにインレット I1 のページが表示されます。

サーキット ブレーカの監視

Dominion PX デバイスの各サーキット ブレーカは、アウトレット (コンセント) のバンクに電力を供給し、1 本または 2 本のラインから電力を引き出します。

サーキット ブレーカの詳細情報を表示できます。表示できる内容には、以下のものがあります。

- ラベル (番号)
- 名前
- ステータス (閉/開)
- サーキット ブレーカに関連付けられているライン
- センサー測定値:
 - 消費電流 (A)
 - 残留電流 (A)

注: センサーの表示値の行が色付きで表示されている場合は、センサーの表示値がすでにいずれかのしきい値を超えているか、サーキット ブレーカーがトリップしています。詳細については、『**The Yellow- or Red-Highlighted Reading (表示値の黄色表示または赤色表示)**』82p. の **測定値の黄色表示または赤色表示 “参照”**」を参照してください。

すべてのサーキット ブレーカの概要を一度に表示することや、個々のサーキット ブレーカの状態を表示することができます。

- ▶ **すべてのサーキット ブレーカの状態を表示するには、次の手順に従います。**

ダッシュボード ページまたは過電流プロテクタ ページで、すべてのサーキット ブレーカの状態を一度に確認できます。

- **ダッシュボード ページの使用:**
 - a. Dominion PX Explorer ペインで [ダッシュボード] アイコンをクリックすると、右側のペインに [ダッシュボード] ページが表示されます。
 - b. ダッシュボード ページで過電流プロテクタのセクションを見つけます。
- **過電流プロテクタ ページの使用:**
 - a. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、『**Expanding the Tree (ツリーの展開)**』76p. の **“ツリーの展開” 参照**』」を参照してください。

- b. Dominion PX Explorer ペインで [Overcurrent Protectors (過電流プロテクタ)] をクリックすると、右側のペインに過電流プロテクタ ページが表示されます。

▶ **サーキット ブレーカの詳細を表示するには、次の手順に従います。**

1. 過電流プロテクタ フォルダを展開し、Dominion PX Explorer ペインですべてのサーキット ブレーカを表示します。「ツリーの展開『76p. 』」を参照してください。
2. Dominion PX Explorer ペインで目的のサーキット ブレーカをクリックすると、右側のペインにこのサーキット ブレーカのページが表示されます。

電力しきい値の設定

しきい値を設定して有効にすると、コンポーネントの電力がしきい値を超えた状態になったときに警告通知が生成されます。

センサーごとに下位臨界、下位警告、上位警告、上位臨界という 4 つのしきい値があります。

- 上位警告と下位警告のしきい値は、センサー測定値が臨界しきい値手前の警告範囲に入るかどうかの境界となる値です。
- 上位臨界と下位臨界のしきい値は、センサー測定値が臨界レベルに入るかどうかの境界となる値です。

大量の警告イベントが生成されないように、各しきい値のアサート停止ヒステリシスが有効になっています。デフォルトのヒステリシス値は、必要に応じて変更できます。アサート停止ヒステリシスの詳細については、「アサート停止ヒステリシスとは『177p. 』」を参照してください。

注: しきい値を設定したら、必ずイベント ルールを設定してください。「イベント ルールの設定『179p. 』」を参照してください。

インレットのしきい値の設定

インレットの電流や電圧がしきい値を超えたときに警告が生成されるように、インレットのしきい値を設定できます。

▶ **インレットのしきい値を設定するには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*『76p. の“ツリーの展開”参照 』」を参照してください。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「*Naming the PDU (PDU のネーミング)*『90p. のPDU の名前付け”参照先 』」を参照してください。

2. Dominion PX Explorer ペインで [Inlet I1 (インレット I1)] をクリックすると、右側のペインにインレット I1 のページが表示されます。
3. [Setup (設定)] をクリックします。[Inlet I1 Setup (インレット 1 の設定)] ダイアログ ボックスが表示されます。
4. しきい値設定表で、しきい値を設定するセンサーをクリックします。
5. [Edit (編集)] をクリックします。選択したセンサーのしきい値設定ダイアログ ボックスが表示されます。

ヒント: しきい値設定表で目的のセンサーをダブルクリックして、このダイアログ ボックスを表示することもできます。

6. [Lower Critical (下位臨界)], [Lower Warning (下位警告)], [Upper Warning (上位警告)], および [Upper Critical (上位臨界)] のしきい値をそれぞれ設定します。
 - しきい値を有効にするには、対応するチェックボックスをオンにします。しきい値を無効にするには、[enabled (有効)] チェックボックスをオフにします。
 - しきい値を有効にしてから、付随するテキスト ボックスに適切な数値を入力します。
7. すべてのしきい値のアサート停止ヒステリシスを有効にするには、[Deassertion Hysteresis (アサート停止ヒステリシス)] フィールドにゼロ以外の数値を入力します。「**アサート停止ヒステリシスとは『177p.』**」を参照してください。
8. すべてのしきい値のアサート タイムアウトを有効にするには、[Assertion Timeout (samples) (アサート タイムアウト (サンプル))] フィールドにゼロ以外の数値を入力します。「**アサート タイムアウトとは『178p.』**」を参照してください。
9. しきい値設定ダイアログ ボックスで [OK] をクリックして、変更を維持します。
10. 他のセンサーのしきい値を設定するには、手順 4 ~ 9 を繰り返します。
11. [OK] をクリックして変更を保存します。

重要: 最終手順を実行しなければ、しきい値の変更は保存されません。

サーキット ブレーカのしきい値の設定

サーキット ブレーカのしきい値を設定すると、サーキット ブレーカの電流がしきい値を超えたときに PDU で警告が生成されます。

▶ サーキット ブレーカのしきい値を設定するには、次の手順に従います。

1. 過電流プロテクタ フォルダを展開し、Dominion PX Explorer ペインですべてのサーキット ブレーカを表示します。「ツリーの展開『76p.』」を参照してください。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「Naming the PDU (PDU のネーミング)『90p. の PDU の名前付け参照先』」を参照してください。

2. Dominion PX Explorer ペインで目的のサーキット ブレーカをクリックすると、右側のペインにこのサーキット ブレーカのページが表示されます。
3. [Setup (設定)] をクリックします。[Overcurrent Protector Setup (過電流プロテクタの設定)] ダイアログ ボックスが表示されます。
4. しきい値設定表で、しきい値を設定するセンサーをクリックします。
5. [Edit (編集)] をクリックします。選択したセンサーのしきい値設定ダイアログ ボックスが表示されます。

ヒント: しきい値設定表で目的のセンサーをダブルクリックして、このダイアログ ボックスを表示することもできます。

6. [Lower Critical (下位臨界)], [Lower Warning (下位警告)], [Upper Warning (上位警告)], および [Upper Critical (上位臨界)] のしきい値をそれぞれ設定します。
 - しきい値を有効にするには、対応するチェックボックスをオンにします。しきい値を無効にするには、[enabled (有効)] チェックボックスをオフにします。
 - しきい値を有効にしてから、付随するテキスト ボックスに適切な数値を入力します。
7. すべてのしきい値のアサート停止ヒステリシスを有効にするには、[Deassertion Hysteresis (アサート停止ヒステリシス)] フィールドにゼロ以外の数値を入力します。「アサート停止ヒステリシスとは『177p.』」を参照してください。
8. すべてのしきい値のアサート タイムアウトを有効にするには、[Assertion Timeout (samples) (アサート タイムアウト (サンプル))] フィールドにゼロ以外の数値を入力します。「アサート タイムアウトとは『178p.』」を参照してください。
9. [OK] をクリックして変更を保存します。

サーキット ブレーカのしきい値の一括設定

Dominion PX では、複数のサーキット ブレーカの電力しきい値を一度に設定できるので、多数のサーキット ブレーカのしきい値を設定する場合に作業時間を短縮できます。

注: 個別のサーキット ブレーカの電力しきい値を設定するには、次の手順、または「サーキット ブレーカのしきい値の設定」『175p.』」セクションの説明に従います。

▶ 複数のサーキット ブレーカのしきい値、アサート停止ヒステリシス、およびアサート タイムアウトを設定するには、次の手順に従います。

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*」『76p. の「ツリーの展開」参照』」を参照してください。

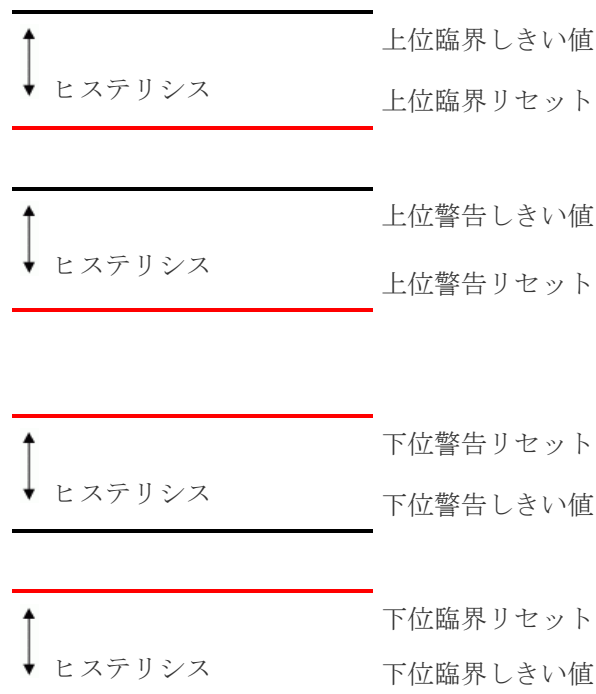
注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「*Naming the PDU (PDU のネーミング)*」『90p. の「PDU の名前付け」参照先』」を参照してください。

2. [Overcurrent Protectors (過電流プロテクタ)] フォルダをクリックします。[Overcurrent Protectors (過電流プロテクタ)] ページが表示されます。
3. [Bulk Setup (一括設定)] をクリックします。[Overcurrent Protector Threshold Bulk Setup (過電流プロテクタのしきい値の一括設定)] ダイアログ ボックスが表示され、すべてのサーキット ブレーカのリストが表示されます。
4. 目的のサーキット ブレーカを、それに対応するチェックボックスをオンにして選択します。
 - すべてのサーキット ブレーカを選択するには、見出し行の [Sensor (センサー)] というラベルが付いたチェックボックスをオンにします。これで、すべてのチェックボックスがオンになります。
 - 一部のサーキット ブレーカを選択するには、それに対応するチェックボックスをオンにして、それらのサーキット ブレーカのチェックボックスを選択します。
 - サーキット ブレーカの選択を解除するには、そのチェックボックスを再度クリックします。
5. [Edit Thresholds (しきい値の編集)] をクリックします。しきい値の一括設定のダイアログ ボックスが表示されます。

6. [Lower Critical (下位臨界)], [Lower Warning (下位警告)], [Upper Warning (上位警告)], および [Upper Critical (上位臨界)] のしきい値をそれぞれ設定します。
 - しきい値を有効にするには、対応するチェックボックスをオンにします。しきい値を無効にするには、[enabled (有効)] チェックボックスをオフにします。
 - しきい値を有効にしてから、付随するテキスト ボックスに適切な数値を入力します。
7. すべてのしきい値のアサート停止ヒステリシスを有効にするには、[Deassertion Hysteresis (アサート停止ヒステリシス)] フィールドにゼロ以外の数値を入力します。「**アサート停止ヒステリシスとは『177p.』**」を参照してください。
8. すべてのしきい値のアサート タイムアウトを有効にするには、[Assertion Timeout (samples) (アサート タイムアウト (サンプル))] フィールドにゼロ以外の数値を入力します。「**アサート タイムアウトとは『178p.』**」を参照してください。
9. [OK] をクリックして変更を保存します。

アサート停止ヒステリシスとは

ヒステリシス設定によって、しきい値の条件をいつリセットするかが決定されます。この図は、ヒステリシス値としきい値の関連を示しています。



ヒステリシスの値は、リセットしきい値を定義します。上位しきい値の場合は、測定値がこのリセットしきい値より下になると、アサート停止イベントが生成されます。下位しきい値の場合は、測定値がこのリセットしきい値より高くなると、アサート停止イベントが生成されます。

例: ヒステリシスが役立つ場合

この例では、どのような場合にアサート停止ヒステリシスが役立つかを説明します。

インレットの電流の臨界しきい値が 19 アンペア (A) に設定されています。引き出し電流が 20A に上昇すると、電流臨界警告がトリガされます。その後、電流が 18.1A と 20A の間で変動し続けます。

ヒステリシスを 1A に設定しても、引き続きインレットの電流が臨界を超えていることが示されます。ヒステリシスなしの場合 (つまり、ヒステリシスをゼロに設定した場合) は、電流が 18.9A に低下するたびに条件のアサートが停止され、電流が 19A 以上になるたびに条件が再度アサートされます。この場合、電流が変動すると、SNMP トラップが何度も繰り返されたり、繰り返し送信される SMTP 警告通知で電子メール アカウントがいっぱいになる可能性があります。

例: ヒステリシスを無効にする場合

これは、インレットのヒステリシスを無効にする場合の例です。ヒステリシスは、その値をゼロに設定すると無効になります。

インレットの電流の上位警告しきい値が、15A に設定されています。通常、インレットには 14.6A の電流が引き込まれます。需要が急増すると電流は 16A に達するため、警告がトリガされます。その後、電流が通常の 14.6A に落ち着きます。

ヒステリシスを無効にした場合は、電流が 14.9A まで低下すると、条件のアサートが停止されます。ヒステリシスをゼロ以外に設定した場合は、電流が 14.0A まで低下しない限り、インレットは警告しきい値を上回っていると見なされます。電流が通常の状態に戻っても、条件のアサートは停止されません。

アサート タイムアウトとは

アサート タイムアウトが有効な場合、Dominion PX デバイスは、特定のしきい値を超えるサンプルが連続して生成され、その数が指定した数に達した場合のみ、警告または臨界状態をアサートします。これによって、測定値がいずれかの上位しきい値を超えるか下位しきい値を下回った直後に正常に戻った場合に、多数のしきい値アラートが生成されるのを防ぐことができます。

イベント ルールの設定

この製品のインテリジェント機能の利点は、状況の変化の通知や変化への対応が行えることです。このイベント通知または応答が「イベント ルール」です。

Dominion PX には、あらかじめ 2 つのイベント ルールが組み込まれており、それらは削除できません。

- [System Event Log Rule (システム イベント ログ ルール)]: このルールにより、Dominion PX に対して発生するあらゆるイベントが内部ログに記録されます。デフォルトでは、このルールは有効になっています。
- [System SNMP Trap Rule (システム SNMP トラップ ルール)]: このルールにより、Dominion PX に対するイベントが発生したときに、指定した IP アドレスまたはホストに SNMP トラップが送信されます。デフォルトでは、このルールは無効になっています。

これらの 2 つでニーズが満たされない場合は、別のイベントに対応する追加のルールを作成できます。

注: Internet Explorer® 8 (IE8) では、コンパイルされた JAVA スクリプトを使用しません。IE8 を使用してイベント ルールを作成または変更すると、CPU パフォーマンスが低下し、接続タイムアウト メッセージが表示される場合があります。その場合は、[Ignore (無視)] をクリックして続行します。

イベント ルールのコンポーネント

イベント ルールは、特定の状況における Dominion PX の機能を定義するものであり、次の 2 つの部分から成ります。

- [Event (イベント)]: これは、Dominion PX またはその一部が特定の条件を満たす状態のことです。たとえば、インレットの電圧が警告しきい値を超える状態などです。
- [Action (アクション)]: これは、イベントに対する対応です。たとえば、システム管理者にイベントが通知され、イベントがログに記録されます。

イベント ルールの作成

新しいイベント ルールのセットを順を追って作成する最適な方法は、次のとおりです。

- 1 つまたは複数のイベントに対応するためのアクションを作成します。
- これらのイベントが発生したときにどのようなアクションを実行するのかを決めるルールを作成します。

アクションの作成

Dominion PX には、次の 2 つのアクションが組み込まれています。

- [System Event Log Action (システム イベント ログ アクション)]: このアクションでは、選択したイベントが発生すると、そのイベントが内部ログに記録されます。
- [System SNMP Trap Action (システム SNMP トラップ アクション)]: このアクションでは、選択したイベントが発生した後に 1 つ以上の IP アドレスに SNMP トラップが送信されます。

注: デフォルトでは、[System SNMP Trap Action (システム SNMP トラップ アクション)] に IP アドレスが指定されていないため、このアクションをイベント ルールに適用する前に IP アドレスを指定する必要があります。

これらの組み込みのアクションは、削除できません。これらのアクションではニーズが満たされない場合は、新しいアクションを作成します。

▶ 新しいアクションを作成するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. [Actions (アクション)] タブをクリックします。
3. [New Action (新規アクション)] をクリックします。
4. [Action name (アクション名)] フィールドに、アクションの新しい名前を入力します。デフォルトの名前は、[New Action <number> (新規アクション <番号>)] です。<number> は連番です。
5. [Action (アクション)] フィールドのドロップダウン矢印をクリックし、リストから目的のアクションを選択します。

オプション	説明
Execute an action group (アクション グループの実行)	このオプションでは、「複数の」既存のアクションをグループ化できるので、イベント発生時に、選択していたアクションの組み合わせを実行できます。
Log event message (ログ イベント メッセージ)	このオプションでは、選択したイベントが内部ログに記録されます。

オプション	説明
Send Snapshots via SMTP (SMTP でのスナップショットの送信)	このオプションでは、接続した Logicool® QuickCam® Pro 9000 Web カメラがある場合に、それによってキャプチャされたスナップショットを電子メールで送信する方法で、選択したイベントを 1 人以上の人に通知します。 ▪ [Recipients email addresses (受信者の電子メール アドレス)] フィールドに受信者の電子メール アドレスを指定します。複数の電子メール アドレスを区切る場合は、カンマを使用します。 ▪ [SMTP Server Settings (SMTP サーバ設定)] ダイアログ ボックスで指定した SMTP サーバを使用するには、[Use Default SMTP Server (デフォルトの SMTP サーバを使用する)] チェックボックスをオンにします。別の SMTP サーバを使用するには、[Use Custom SMTP Settings (カスタム SMTP 設定を使用する)] チェックボックスをオンにします。SMTP サーバがまだ設定されていない場合は、[Configure (設定)] をクリックします。各フィールドについては、「SMTP の設定『111p. 』」を参照してください。 ▪ [Webcam (Web カメラ)] フィールドで、送信するスナップショットを撮影する Web カメラを選択します。 ▪ [Number of Snapshots (スナップショット数)] フィールドで、イベントが発生したときにキャプチャされる画像の合計数を指定します。 ▪ [Snapshots/Mail (スナップショット/メール)] フィールドで、電子メールで一度に送信する画像の最大数を指定します。 ▪ [Time before first Snapshot (s): (スナップショットの撮影開始までの時間:)] フィールドで、イベントが発生してから最初のスナップショットがキャプチャされるまでの時間を指定します。 ▪ [Time between Snapshots (s): (スナップショットの撮影間隔:)] フィールドで、個々のスナップショットのキャプチャ アクションの間隔を指定します。

オプション	説明
Send SMTP message (SMTP メッセージの送信)	このオプションでは、選択したイベントが 1 人以上の人に電子メールで通知されます。 ▪ [Recipients email addresses (受信者の電子メール アドレス)] フィールドに受信者の電子メール アドレスを指定します。複数の電子メール アドレスを区切る場合は、カンマを使用します。 ▪ [SMTP Server Settings (SMTP サーバ設定)] ダイアログ ボックスで指定した SMTP サーバを使用するには、[Use Default SMTP Server (デフォルトの SMTP サーバを使用する)] チェックボックスをオンにします。別の SMTP サーバを使用するには、[Use Custom SMTP Settings (カスタム SMTP 設定を使用する)] チェックボックスをオンにします。SMTP サーバがまだ設定されていない場合は、[Configure (設定)] をクリックします。各フィールドについては、「SMTP の設定『111p. 』」を参照してください。
Send SNMP trap (SNMP トラップの送信)	このオプションでは、SNMP トラップが 1 つ以上の SNMP マネージャに送信されます。 ▪ [Host <i>x</i> (ホスト <i>x</i>)] フィールドに SNMP トラップの送信先を 3 つまで指定できます。<i>x</i> は 1 ～ 3 の数値です。 ▪ [Port <i>x</i> (ポート <i>x</i>)] フィールドに各送信先のポート番号を指定します。<i>x</i> は 1 ～ 3 の数値です。 ▪ [Community <i>x</i> (コミュニティ <i>x</i>)] フィールドに各送信先のコミュニティ スtring を指定します。<i>x</i> は 1 ～ 3 の数値です。
Syslog message (Syslog メッセージ)	このオプションでは、イベント メッセージが、指定した syslog サーバに自動的に転送されます。 ▪ [Syslog server (Syslog サーバ)] フィールドに、syslog の送信先 IP アドレスを指定します。 ▪ [Port (ポート)] フィールドに、適切なポート番号を指定します。

オプション	説明
Send SMS message (SMS メッセージの送信)	このオプションは、指定した携帯電話に英語のテキスト メッセージを送信します。 - この機能を実行するには、Dominion PX に Cinterion® GSM MC52i または MC55i モデムを接続する必要があります。 [Recipient Phone Number(受信者の電話番号)] フィールドに電話番号を入力します。 <i>注: Dominion PX では SMS メッセージを受信できません。</i>
Record Snapshots to Webcam Storage (スナップショットを Web カメラ ストレージに記録)	このオプションでは、イベント発生時に特定の Web カメラのスナップショット撮影を開始または停止できます。 [Webcam (Web カメラ)] フィールドで、イベント発生時にスナップショットを撮影する Web カメラを選択します。 [Action (アクション)] フィールドで、選択した Web カメラによるスナップショット撮影を開始する場合は [Start recording (記録開始)] を、また中止する場合は [Stop recording (記録中止)] を選択します。 [Start recording (記録開始)] オプションが選択されている場合は、次の 3 つのフィールドを入力する必要があります。 [Number of Snapshots (スナップショット数)] フィールドで、イベントが発生したときにキャプチャされる画像の合計数を指定します。 [Time before first Snapshot (s): (スナップショットの撮影開始までの時間:)] フィールドで、イベントが発生してから最初のスナップショットがキャプチャされるまでの時間を指定します。 [Time between Snapshots (s): (スナップショットの撮影間隔:)] フィールドで、個々のスナップショットのキャプチャ アクションの間隔を指定します。

オプション	説明
[Change load shedding state (負荷遮断状態の変更)]	このオプションは、イベントが発生したときに負荷遮断モードを有効または無効にします。 ▪ [Operation (動作)] フィールドで、[Enable load shedding (負荷遮断を有効にする)] を選択して負荷遮断モードを有効にするか、[Disable load shedding (負荷遮断を無効にする)] を選択して負荷遮断モードを無効にします。
[Switch outlet (アウトレット (コンセント) の切り替え)]:	このオプションでは、特定のアウトレット (コンセント) の電源のオン/オフまたは電源の再投入が行われます。 ▪ [Operation (動作)] フィールドで、選択したアウトレット (コンセント) の動作を選択します。 [Turn Outlet On (アウトレット (コンセント) のオン)]: 選択したアウトレット (コンセント) の電源をオンにします。 [Turn Outlet Off (アウトレット (コンセント) のオフ)]: 選択したアウトレット (コンセント) の電源をオフにします。 [Cycle Outlet (アウトレット (コンセント) の電源の再投入)]: 選択したアウトレット (コンセント) の電源を再投入します。 ▪ 指定したアクションを適用するアウトレット (コンセント) を選択するには、それを [Available Outlets (使用可能なアウトレット (コンセント))] リストで選択し、 をクリックします。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。 ▪ [Switched Outlets (切り替えられるアウトレット (コンセント))] リストからアウトレット (コンセント) を削除するには、そのリストでアウトレット (コンセント) を選択し、 をクリックします。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。

注: [Change load shedding state (負荷遮断状態の変更)] オプションと [Switch outlet (アウトレット (コンセント) の切り替え)] オプションは、アウトレット (コンセント) 切り替え対応の PDU でのみ使用できます。

1. [Save (保存)] をクリックして新しいアクションを保存します。

注: [Save (保存)] をクリックしないで現在の設定ページを閉じると、メッセージが表示されます。変更を保存する場合は [Yes (はい)] を、変更を中止する場合は [Discard (破棄)] を、現在の設定ページに戻る場合は [Cancel (キャンセル)] をクリックします。

2. さらにアクションを作成するには、手順 3 ~ 7 を繰り返します。
3. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

アクション グループの作成

最大 32 個のアクションを実行するアクション グループを作成できます。このようなアクション グループを作成しておく、必要なすべてのアクションを個々のイベント ルールに 1 つずつ選択しなくても、特定のアクション セットをルールに簡単に割り当てることができます。

▶ アクション グループを作成するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. [Actions (アクション)] タブをクリックします。
3. [New Action (新規アクション)] をクリックします。
4. [Action name (アクション名)] フィールドに、アクションの新しい名前を入力します。デフォルトの名前は、[New Action <number> (新規アクション <番号>)] です。<number> は連番です。
5. [Action (アクション)] フィールドのドロップダウン矢印をクリックし、リストから目的のアクションを選択します。アクション グループを作成するには、[Execute an action group (アクション グループの実行)] を選択します。
6. アクションにアクション グループの一部としてのマークを付けるには、[Available Actions (使用可能なアクション)] ペインでリストからアクションを選択し、 をクリックして [Used Actions (使用するアクション)] ペインに移動します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。32 個までのアクションをグループ化できます。

7. アクションをアクション グループから削除するには、[Used Actions (使用するアクション)] ペインでリストからアクションを選択し、 をクリックして [Available Actions (使用可能なアクション)] ペインに移動します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
8. [Save (保存)] をクリックして新しいアクションを保存します。

注: [Save (保存)] をクリックしないで現在の設定ページを閉じると、メッセージが表示されます。変更を保存する場合は [Yes (はい)] を、変更を中止する場合は [Discard (破棄)] を、現在の設定ページに戻る場合は [Cancel (キャンセル)] をクリックします。

9. さらにアクション グループを作成するには、手順 3 ~ 8 を繰り返します。

カスタムの電子メール メッセージの作成

イベント発生時に電子メールを送信するように設定している場合は、電子メールに含めるメッセージをカスタマイズできます。

メッセージは、自由書式のテキストと Dominion PX プレースホルダを組み合わせて構成します。プレースホルダで表された情報は、Dominion PX から抽出され、メッセージに挿入されます。

たとえば、

```
[USERNAME] logged into the device on [TIMESTAMP]
([USERNAME] が [TIMESTAMP] にデバイスにログインしました)
```

これは次のように変換されます。

```
JQPublic logged into the device on 2012-January-30 21:00
(JQPublic が 2012-January-30 21:00 にデバイスにログインしました)
```

使用可能な変数のリストと定義については、「**電子メール メッセージのプレースホルダ**『187p. 』」を参照してください。

▶ カスタム メッセージを作成するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。
2. [Actions (アクション)] タブをクリックします。
3. 左側のペインから、以前作成した [Send SMTP message (SMTP メッセージの送信)] アクションを選択するか、新しいアクションを作成します。「**アクションの作成**『180p. 』」を参照してください。
4. ダイアログ ボックスの [Action Settings (アクション設定)] セクションの [Actions (アクション)] ドロップダウン リストから [Send SMTP message (SMTP メッセージの送信)] を選択します。

5. [Use Custom Log Message (カスタム ログ メッセージを使用)] チェックボックスをオンにします。
6. 表示されているテキスト フィールドにカスタム情報を入力してメッセージを作成します。必要な場合は、プレースホルダをメッセージの一部として使用できます。

注: [Information (情報)] アイコン  をクリックすると、プレースホルダとその定義のリストを含む [Event Context Information (イベント コンテキスト情報)] ダイアログ ボックスが表示されます。次に、目的のプレースホルダを選択し、それをダブルクリックするか、[Paste into message (メッセージに貼り付け)] ボタンをクリックして、カスタマイズしたメッセージにそれを挿入します。

7. [Save (保存)] をクリックします。

電子メール メッセージのプレースホルダ

カスタムのイベント電子メール メッセージで使用できるプレースホルダを以下に示します。

注: [Information (情報)] アイコン  をクリックすると、プレースホルダとその定義のリストを含む [Event Context Information (イベント コンテキスト情報)] ダイアログ ボックスが表示されます。

プレースホルダ	定義
[TIMESTAMP]	イベント発生時のタイムスタンプ
[TARGETUSER]	アクションがトリガされる対象のユーザ
[USERIP]	ユーザの接続元の IP アドレス
[ASSERTION]	あるイベント条件に入った (1) か、それから脱した (0) ことを示すブール フラグ
[EXTSENSORNAME]	外部センサーの名称
[EXTSENSORSLOT]	外部センサー スロットの ID
[IFNAME]	人間が判読できるネットワーク インタフェース名
[INLET]	電源インレット ラベル
[INLETPOLE]	インレット電力線の識別子
[INLETSENSOR]	インレット センサー名
[LEDCOLOR]	RGB LED 色
[LEDMODE]	LED が示すモード

プレースホルダ	定義
[LEDOPMODE]	LED の動作モード
[LHXFANID]	LHX に接続されているファンの ID
[LHXPOWERSUPPLYID]	LHX 電源の ID
[LHXSENSORID]	LHX センサー プローブの ID
[STATE]	人間が判読できる、資産ストリップの状態
[VALUE]	パラメータの新しい値
[VERSION]	デバイスがアップグレードされるファームウェア バージョン
[OCP]	過電流プロテクタ ラベル
[OCPSENSOR]	過電流プロテクタ センサー名
[OLDVERSION]	デバイスのアップグレード前のファームウェア バージョン
[OUTLET]	アウトレット (コンセント) ラベル
[OUTLETPOLE]	アウトレット (コンセント) 電力線の識別子
[OUTLETSensor]	アウトレット (コンセント) センサー名
[PARAMETER]	設定パラメータの名前
[POLESENSOR]	特定の電力線のセンサー名
[PORTID]	イベントでトリガされるデバイスが接続されている外部ポートのラベル。
[PORTTYPE]	イベントでトリガされるデバイスが接続されている外部ポートのタイプ (「feature (拡張)」または「auxiliary (補助)」)。
[RACKUNIT]	アクションが適用されるラック ユニットの (垂直) 位置
[TARGETROLE]	アクションが適用されたユーザ管理役割の名前
[SERVER]	サーバの名前または IP アドレス
[RACKSLOT]	アクションが適用されるスロットの (水平) 位置
[STRIPID]	資産ストリップの数値 ID

プレースホルダ	定義
[STRIPNAME]	資産ストリップの名前
[TAGID]	資産タグ ID
[USERNAME]	アクションをトリガしたユーザ
[RECIPIENTS]	SMTP メッセージが送信された受信者のリスト
[LDAPERRORDESC]	発生した LDAP エラー

デフォルト ログ メッセージ

以下は、Dominion PX イベントが発生したとき (TRUE)、または場合によっては発生しなかったとき (FALSE) にトリガされ、指定した受信者に送信されるデフォルト ログ メッセージです。指定したイベントが発生したときに送信される電子メール メッセージの設定については、「**アクションの作成**」『180p. 』を参照してください。

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
[Device (デバイス)] > [System started (システムの開始)]	System started. (システムが開始されました。)	
[Device (デバイス)] > [System reset (システム リセット)]	System reset performed by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がシステムのリセットを実行しました。)	
[Device (デバイス)] > [Firmware validation failed (ファームウェアの確認失敗)]	Firmware validation failed by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が行ったファームウェアの確認が失敗しました。)	
[Device (デバイス)] > [Firmware update started (ファームウェアの更新開始)]	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がバージョン '[OLDVERSION]' からバージョン '[VERSION]' へのファームウェアのアップグレードを開始しました。)	
[Device (デバイス)] > [Firmware	Firmware upgraded successfully from	

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
update completed (ファームウェアの更新完了)	version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が行ったバージョン '[OLDVERSION]' からバージョン '[VERSION]' へのファームウェアのアップグレードが正常に終了しました。)	
[Device (デバイス)] > [Firmware update failed (ファームウェアの更新失敗)]	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が行ったバージョン '[OLDVERSION]' からバージョン '[VERSION]' へのファームウェアのアップグレードが失敗しました。)	
[Device (デバイス)] > [Device identification changed (デバイス ID の変更)]	Config parameter '[PARAMETER]' changed to '[VALUE]' by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が構成パラメータ '[PARAMETER]' を '[VALUE]' に変更しました。)	
[Device (デバイス)] > [Event log cleared (イベント ログのクリア)]	Event log cleared by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がイベント ログをクリアしました。)	
[Device (デバイス)] > [Bulk configuration saved (一括設定の保存)]	Bulk configuration saved from host '[USERIP]'. (ホスト '[USERIP]' から一括設定が保存されました。)	
[Device (デバイス)] > [Bulk configuration copied (一括設定のコピー)]	Bulk configuration copied from host '[USERIP]'. (ホスト '[USERIP]' から一括設定がコピーされました。)	
[Device (デバイス)] > [Network interface link state is up (ネットワーク インタフェースのリンク状態がアップ)]	The [IFNAME] network interface link is now up. ([IFNAME] ネットワーク インタフェース リンクがアップ状態になりました。)	The [IFNAME] network interface link is now down. ([IFNAME] ネットワーク インタフェース リンクがダウン状態になりました。)

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
[Device (デバイス)] > [Sending SMTP message failed (SMTP メッセージの送信の失敗)]	Sending SMTP message to '[RECIPIENTS]' using server '[SERVER]' failed. (サーバ '[SERVER]' を使用した '[RECIPIENTS]' への SMTP メッセージの送信が失敗しました。)	
[Device (デバイス)] > [An LDAP error occurred (LDAP エラーの発生)]	An LDAP error occurred: [LDAPERRORDESC]. (LDAP エラーが発生しました: [LDAPERRORDESC]。)	
[Device (デバイス)] > [USB slave connected (USB スレーブの接続)]	USB slave connected. (USB スレーブが接続されました。)	USB slave disconnected. (USB スレーブが切断されました。)
[Device (デバイス)] > [Features (機能)] > [Schroff LHX Support (Schroff LHX サポート)]	Schroff LHX support enabled. (Schroff LHX サポートが有効になりました。)	Schroff LHX support disabled. (Schroff LHX サポートが無効になりました。)
[User Administration (ユーザ管理)] > [User added (ユーザの追加)]	User '[TARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がユーザ '[TARGETUSER]' を追加しました。)	
[User Administration (ユーザ管理)] > [User modified (ユーザの変更)]	User '[TARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がユーザ '[TARGETUSER]' を変更しました。)	
[User Administration (ユーザ管理)] > [User deleted (ユーザの削除)]	User '[TARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がユーザ '[TARGETUSER]' を削除しました。)	
[User Administration (ユーザ管理)] > Password changed (パスワードの変更)]	Password of user '[TARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がユーザ '[TARGETUSER]' のパスワードを変更しました。)	
[User Administration (ユーザ管理)] > Password settings changed (パスワード設定の変更)]	Password settings changed by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ	

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
	'[USERNAME]' がパスワード設定を変更しました。)	
[User Administration (ユーザ管理)] > [Role added (役割の追加)]	Role '[TARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が役割 '[TARGETROLE]' を追加しました。)	
[User Administration (ユーザ管理)] > [Role modified (役割の変更)]	Role '[TARGETROLE]' modified by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が役割 '[TARGETROLE]' を変更しました。)	
[User Administration (ユーザ管理)] > [Role deleted (役割の削除)]	Role '[TARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が役割 '[TARGETROLE]' を削除しました。)	
[User Activity (ユーザ アクティビティ)] > * > [User logged in (ユーザ ログイン)]	User '[USERNAME]' from host '[USERIP]' logged in. (ホスト '[USERIP]' からユーザ '[USERNAME]' がログインしました。)	User '[USERNAME]' from host '[USERIP]' logged out. (ホスト '[USERIP]' からユーザ '[USERNAME]' がログアウトしました。)
[User Activity (ユーザ アクティビティ)] > * > [Authentication failure (認証失敗)]	Authentication failed for user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からのユーザ '[USERNAME]' の認証が失敗しました。)	
[User Activity (ユーザ アクティビティ)] > * > [User blocked (ユーザ ブロック)]	User '[USERNAME]' from host '[USERIP]' was blocked. (ホスト '[USERIP]' からユーザ '[USERNAME]' がブロックされました。)	
[User Activity (ユーザ アクティビティ)] > * > [Session timeout (セッション タイムアウト)]	Session of user '[USERNAME]' from host '[USERIP]' timed out. (ホスト '[USERIP]' からのユーザ '[USERNAME]' のセッションがタイムアウトしました。)	
[PDU] > [Load Shedding (負荷遮断)] > [Enabled (有効)]	PX placed in Load Shedding Mode by user '[USERNAME]' from host	PX removed from Load Shedding Mode by user '[USERNAME]' from

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
	'[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が PX を負荷遮断モードにしました。)	host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が PX を負荷遮断モードから解除しました。)
[Inlet (インレット)] > * > [Sensor (センサー)] > * > [Unavailable (使用不可能)]	Sensor '[INLETSensor]' on inlet '[INLET]' unavailable. (インレット '[INLET]' のセンサー '[INLETSensor]' は使用不可能です。)	Sensor '[INLETSensor]' on inlet '[INLET]' available. (インレット '[INLET]' のセンサー '[INLETSensor]' は使用可能です。)
[Inlet (インレット)] > * > [Sensor (センサー)] > * > [Above upper critical threshold (上位臨界しきい値より上)]	Sensor '[INLETSensor]' on inlet '[INLET]' asserted 'above upper critical'. (インレット '[INLET]' のセンサー '[INLETSensor]' が '上位臨界以上' をアサートしました。)	Sensor '[INLETSensor]' on inlet '[INLET]' deasserted 'above upper critical'. (インレット '[INLET]' のセンサー '[INLETSensor]' の '上位臨界以上' のアサートが停止されました。)
[Inlet (インレット)] > * > [Sensor (センサー)] > * > [Above upper warning threshold (上位警告しきい値より上)]	Sensor '[INLETSensor]' on inlet '[INLET]' asserted 'above upper warning'. (インレット '[INLET]' のセンサー '[INLETSensor]' が '上位警告以上' をアサートしました。)	Sensor '[INLETSensor]' on inlet '[INLET]' deasserted 'above upper warning'. (インレット '[INLET]' のセンサー '[INLETSensor]' の '上位警告以上' のアサートが停止されました。)
[Inlet (インレット)] > * > [Sensor (センサー)] > * > [Below lower warning threshold (下位警告しきい値より下)]	Sensor '[INLETSensor]' on inlet '[INLET]' asserted 'below lower warning'. (インレット '[INLET]' のセンサー '[INLETSensor]' が '下位警告未満' をアサートしました。)	Sensor '[INLETSensor]' on inlet '[INLET]' deasserted 'below lower warning'. (インレット '[INLET]' のセンサー '[INLETSensor]' の '下位警告未満' のアサートが停止されました。)
[Inlet (インレット)] > * > [Sensor (センサー)] > * > [Below lower critical threshold (下位臨界しきい値より下)]	Sensor '[INLETSensor]' on inlet '[INLET]' asserted 'below lower critical'. (インレット '[INLET]' のセンサー '[INLETSensor]' が '下位臨界未満' をアサートしました。)	Sensor '[INLETSensor]' on inlet '[INLET]' deasserted 'below lower critical'. (インレット '[INLET]' のセンサー '[INLETSensor]' の '下位臨界未満' のアサートが停止されました。)
[Inlet (インレット)] > * > [Pole (ポール)] > * > [Sensor (センサー)] > * > [Unavailable (使用不可能)]	Sensor '[POLESensor]' on pole '[INLETPole]' of inlet '[INLET]' unavailable. (インレット '[INLET]' のポール '[INLETPole]' のセンサー '[POLESensor]' は使用不可能です。)	Sensor '[POLESensor]' on pole '[INLETPole]' of inlet '[INLET]' available. (インレット '[INLET]' のポール '[INLETPole]' のセンサー '[POLESensor]' は使用可能です。)

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
[Inlet (インレット)] > * > [Pole (ポール)] > * > [Sensor (センサー)] > * > [Above upper critical threshold (上位臨界しきい値より上)]	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'above upper critical'. (インレット '[INLET]' のポール '[INLETPOLE]' のセンサー '[POLESENSOR]' が '上位臨界以上' をアサートしました。)	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'above upper critical'. (インレット '[INLET]' のポール '[INLETPOLE]' のセンサー '[POLESENSOR]' の '上位臨界以上' のアサートが停止されました。)
[Inlet (インレット)] > * > [Pole (ポール)] > * > [Sensor (センサー)] > * > [Above upper warning threshold (上位警告しきい値より上)]	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'above upper warning'. (インレット '[INLET]' のポール '[INLETPOLE]' のセンサー '[POLESENSOR]' が '上位警告以上' をアサートしました。)	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'above upper warning'. (インレット '[INLET]' のポール '[INLETPOLE]' のセンサー '[POLESENSOR]' の '上位警告以上' のアサートが停止されました。)
[Inlet (インレット)] > * > [Pole (ポール)] > * > [Sensor (センサー)] > * > [Below lower warning threshold (下位警告しきい値より下)]	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'below lower warning'. (インレット '[INLET]' のポール '[INLETPOLE]' のセンサー '[POLESENSOR]' が '下位警告未満' をアサートしました。)	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'below lower warning'. (インレット '[INLET]' のポール '[INLETPOLE]' のセンサー '[POLESENSOR]' の '下位警告未満' のアサートが停止されました。)
[Inlet (インレット)] > * > [Pole (ポール)] > * > [Sensor (センサー)] > * > [Below lower critical threshold (下位臨界しきい値より下)]	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'below lower critical'. (インレット '[INLET]' のポール '[INLETPOLE]' のセンサー '[POLESENSOR]' が '下位臨界未満' をアサートしました。)	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'below lower critical'. (インレット '[INLET]' のポール '[INLETPOLE]' のセンサー '[POLESENSOR]' の '下位臨界未満' のアサートが停止されました。)
[Outlet (アウトレット (コンセント))] > * > [Power control (電源制御)] > [Powered on (電源オン)]	Outlet '[OUTLET]' has been powered on by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がアウトレット (コンセント) '[OUTLET]' の電源をオンにしました。)	

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
[Outlet (アウトレット (コンセント))] > * > [Power control (電源制御)] > [Powered off (電源オフ)]	Outlet '[OUTLET]' has been powered off by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がアウトレット (コンセント) '[OUTLET]' の電源をオフにしました。)	
[Outlet (アウトレット (コンセント))] > * > [Power control (電源制御)] > [Powered cycled (電源再投入)]	Outlet '[OUTLET]' power cycle initiated by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がアウトレット (コンセント) '[OUTLET]' の電源再投入を開始しました。)	
[Outlet (アウトレット (コンセント))] > * > [Sensor (センサー)] > * > [Unavailable (使用不可能)]	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' unavailable. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' は使用不可能です。)	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' available. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' は使用可能です。)
[Outlet (アウトレット (コンセント))] > * > [Sensor (センサー)] > * > [Above upper critical threshold (上位臨界しきい値より上)]	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'above upper critical'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' が '上位臨界以上' をアサートしました。)	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'above upper critical'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' の '上位臨界以上' のアサートが停止されました。)
[Outlet (アウトレット (コンセント))] > * > [Sensor (センサー)] > * > [Above upper warning threshold (上位警告しきい値より上)]	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'above upper warning'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' が '上位警告以上' をアサートしました。)	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'above upper warning'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' の '上位警告以上' のアサートが停止されました。)
[Outlet (アウトレット (コンセント))] > * > [Sensor (センサー)] > * > [Below lower warning threshold (下位警告しきい値より下)]	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'below lower warning'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' が '下位警告未満' をアサートしました。)	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'below lower warning'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' の '下位警告未満' のアサートが停止されました。)

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
[Outlet (アウトレット (コンセン ト))] > * > [Sensor (センサー)] > * > [Below lower critical threshold (下位臨界しきい値より 下)]	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'below lower critical'. (アウトレット (コンセン ト) '[OUTLET]' のセンサー '[OUTLETSENSOR]' が '下位臨界未満' 'をアサートしました。)	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'below lower critical'. (アウトレッ ト (コンセン ト) '[OUTLET]' のセ ンサー '[OUTLETSENSOR]' の ' 下位臨界未満' のアサートが停止 されました。)
[Outlet (アウトレット (コンセン ト))] > * > [Sensor (センサー)] > * > [On (オン)]	Outlet '[OUTLET]' state changed to on. (アウトレット (コンセン ト) '[OUTLET]' の状態がオンに変更され ました。)	Outlet '[OUTLET]' state changed to off. (アウトレット (コンセン ト) '[OUTLET]' の状態がオフに変更 されました。)
[Outlet (アウトレット (コンセン ト))] > * > [Pole (ポール)] > * > [Sensor (センサー)] > [Unavailable (使用不可能)]	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' unavailable. (アウトレット (コンセン ト) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' は使用不可能です。)	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' available. (アウトレッ ト (コンセン ト) '[OUTLET]' のポ ール '[OUTLETPOLE]' のセンサ ー '[POLESENSOR]' は使用可能 です。)
[Outlet (アウトレット (コンセン ト))] > * > [Pole (ポール)] > * > [Sensor (センサー)] > * > [Above upper critical threshold (上位臨界しきい値より上)]	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'above upper critical'. (アウト レット (コンセン ト) '[OUTLET]' のポ ール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' が '上位臨界以上' をアサートしました。)	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'above upper critical'. (アウトレット (コ ンセン ト) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' の '上位臨界以 上' のアサートが停止されまし た。)
[Outlet (アウトレット (コンセン ト))] > * > [Pole (ポール)] > * > [Sensor (センサー)] > * > [Above upper warning threshold (上位警告しきい値より上)]	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'above upper warning'. (アウト レット (コンセン ト) '[OUTLET]' のポ ール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' が '上位警告以上' をアサートしました。)	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'above upper warning'. (アウトレット (コ ンセン ト) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' の '上位警告以 上' のアサートが停止されまし た。)
[Outlet (アウトレット (コンセン ト))] > * > [Pole (ポール)] > * > [Sensor (センサー)] > [Below	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'below lower warning'. (アウト	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'below

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
lower warning threshold (下位警告しきい値より下)]	レット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' が '下位警告未満' をアサートしました。)	lower warning'. (アウトレット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' の '下位警告未満' のアサートが停止されました。)
[Outlet (アウトレット (コンセント))] > * > [Pole (ポール)] > * > [Sensor (センサー)] > [Below lower critical threshold (下位臨界しきい値より下)]	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'below lower critical'. (アウトレット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' が '下位臨界未満' をアサートしました。)	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'below lower critical'. (アウトレット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' の '下位臨界未満' のアサートが停止されました。)
[Overcurrent Protector (過電流プロテクタ)] > * > [Sensor (センサー)] > * > [Unavailable (使用不可能)]	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' unavailable. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' は使用不可能です。)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' available. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' は使用可能です。)
[Overcurrent Protector (過電流プロテクタ)] > * > [Sensor (センサー)] > * > [Above upper critical threshold (上位臨界しきい値より上)]	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper critical'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' が '上位臨界以上' をアサートしました。)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper critical'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' の '上位臨界以上' のアサートが停止されました。)
[Overcurrent Protector (過電流プロテクタ)] > * > [Sensor (センサー)] > * > [Above upper warning threshold (上位警告しきい値より上)]	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper warning'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' が '上位警告以上' をアサートしました。)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper warning'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' の '上位警告以上' のアサートが停止されました。)
[Overcurrent Protector (過電流プロテクタ)] > * > [Sensor (センサー)] > * > [Below lower warning threshold (下位警告しきい値より下)]	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'below lower warning'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' が '下位警告未満' をアサートしました。)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'below lower warning'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' の '下位警告未満' のアサートが停止され

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
		ました。)
[Overcurrent Protector (過電流プロテクタ)] > * > [Sensor (センサー)] > * > [Below lower critical threshold (下位臨界しきい値より下)]	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'below lower critical'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' が '下位臨界未満' をアサートしました。)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'below lower critical'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' の '下位臨界未満' のアサートが停止されました。)
[Overcurrent Protector (過電流プロテクタ)] > * > [Sensor (センサー)] > * > [Open (開)]	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is open. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' が開いています。)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is closed. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' が閉じています。)
[External Sensor Slot (外部センサー スロット)] > * > [Numeric Sensor (数値センサー)] > [Unavailable (使用不可能)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' は使用不可能です。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' は使用可能です。)
[External Sensor Slot (外部センサー スロット)] > * > [Numeric Sensor (数値センサー)] > [Above upper critical threshold (上位臨界しきい値より上)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper critical'. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' が '上位臨界以上' をアサートしました。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper critical'. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' の '上位臨界以上' のアサートが停止されました。)
[External Sensor Slot (外部センサー スロット)] > * > [Numeric Sensor (数値センサー)] > [Above upper warning threshold (上位警告しきい値より上)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper warning'. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' が '上位警告以上' をアサートしました。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper warning'. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' の '上位警告以上' のアサートが停止されました。)
[External Sensor Slot (外部センサー スロット)] > * > [Numeric Sensor (数値センサー)] > [Below	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning'. (スロット	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
lower warning threshold (下位警告しきい値より下)]	'[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' が '下位警告未満' をアサートしました。)	'below lower warning'. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' の '下位警告未満' のアサートが停止されました。)
[External Sensor Slot (外部センサー スロット)] > * > [Numeric Sensor (数値センサー)] > [Below lower critical threshold (下位臨界しきい値より下)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower critical'. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' が '下位臨界未満' をアサートしました。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower critical'. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' の '下位臨界未満' のアサートが停止されました。)
[External Sensor Slot (外部センサー スロット)] > * > [State Sensor (状態センサー)] > [Unavailable (使用不可能)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' は使用不可能です。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' は使用可能です。)
[External Sensor Slot (外部センサー スロット)] > * > [State Sensor (状態センサー)] > [Closed (閉)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is closed. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' が閉じています。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is open. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' が開いています。)
[External Sensor Slot (外部センサー スロット)] > * > [State Sensor (状態センサー)] > [On (オン)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is on. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' がオンになっています。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is off. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' がオフになっています。)
[External Sensor Slot (外部センサー スロット)] > * > [State Sensor (状態センサー)] > [Alarmed (アラーム)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is alarmed. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' がアラーム状態です。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is no longer alarmed. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' のアラーム状態が解除されました。)

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
[Server Monitoring (サーバ監視)] > * > [Monitored (監視)]	Server '[SERVER]' is now being monitored. (サーバ '[SERVER]' が監視対象になりました。)	Server '[SERVER]' is no longer being monitored. (サーバ '[SERVER]' が監視対象外になりました。)
[Server Monitoring (サーバ監視)] > * > [Unreachable (到達不能)]	Server '[SERVER]' is unreachable. (サーバ '[SERVER]' に到達できません。)	Server '[SERVER]' is reachable. (サーバ '[SERVER]' に到達できます。)
[EnergyWise] > [Enabled (有効)]	User '[USERNAME]' from host '[USERIP]' enabled EnergyWise. (ホスト '[USERIP]' からユーザ '[USERNAME]' が EnergyWise を有効にしました。)	User '[USERNAME]' from host '[USERIP]' disabled EnergyWise. (ホスト '[USERIP]' からユーザ '[USERNAME]' が EnergyWise を無効にしました。)
[Asset Management (資産管理)] > [State (状態)]	State of asset strip [STRIPID] ('[STRIPNAME]') changed to '[STATE]'. (資産ストリップ [STRIPID] ('[STRIPNAME]') の状態が '[STATE]' になりました。)	
[Asset Management (資産管理)] > [Rack Unit (ラック ユニット)] > * > [Tag Connected (タグの接続)]	Asset tag with ID '[TAGID]' connected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]'). (ID '[TAGID]' の資産タグが、資産ストリップ [STRIPID] ('[STRIPNAME]') のラック ユニット [RACKUNIT]、スロット [RACKSLOT] に接続されました。)	Asset tag with ID '[TAGID]' disconnected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]'). (ID '[TAGID]' の資産タグが、資産ストリップ [STRIPID] ('[STRIPNAME]') のラック ユニット [RACKUNIT]、スロット [RACKSLOT] から切断されました。)
[Asset Management (資産管理)] > [Rack Unit (ラック ユニット)] > * > [Blade Extension Connected (ブレード拡張の接続)]	Blade extension with ID '[TAGID]' connected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]'). (ID '[TAGID]' のブレード拡張が、資産ストリップ [STRIPID] ('[STRIPNAME]') のラック ユニット [RACKUNIT] に接続されました。)	Blade extension with ID '[TAGID]' disconnected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]'). (ID '[TAGID]' のブレード拡張が、資産ストリップ [STRIPID] ('[STRIPNAME]') のラック ユニット [RACKUNIT] から切断されました。)
[Asset Management (資産管理)] > [Firmware Update (ファームウェア)]	Firmware update for asset strip [STRIPID] ('[STRIPNAME]'):status changed to '[STATE]'. (資産ストリップ	

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
アの更新]]	[STRIPID] ('[STRIPNAME]') のファームウェアの更新: ステータスが '[STATE]' に変更されました。)	
[Asset Management (資産管理)] > [Device Config Changed (デバイス設定の変更)]	Config parameter '[PARAMETER]' of asset strip [STRIPID] ('[STRIPNAME]') changed to '[VALUE]' by user '[USERNAME]'. (資産ストリップ [STRIPID] ('[STRIPNAME]') の設定パラメータ '[PARAMETER]' がユーザ '[USERNAME]' によって '[VALUE]' に変更されました。)	
[Asset Management (資産管理)] > [Rack Unit Config Changed (ラック ユニット設定の変更)]	Config of rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]') changed by user '[USERNAME]' to: LED Operation Mode '[LEDOPMODE]', LED Color '[LEDCOLOR]', LED Mode '[LEDMODE]' (資産ストリップ [STRIPID] ('[STRIPNAME]') のラック ユニット [RACKUNIT] の設定がユーザ '[USERNAME]' によって変更されました: LED 動作モード '[LEDOPMODE]', LED 色 '[LEDCOLOR]', LED モード '[LEDMODE]')	
[Asset Management (資産管理)] > [Blade Extension Overflow (ブレード拡張のオーバーフロー)]	Blade extension overflow occurred on strip [STRIPID] ('[STRIPNAME]'). (ブレード拡張のオーバーフローがストリップ [STRIPID] ('[STRIPNAME]') で発生しました。)	Blade extension overflow cleared for strip [STRIPID] ('[STRIPNAME]'). (ブレード拡張のオーバーフローがストリップ [STRIPID] ('[STRIPNAME]') でクリアされました。)
[Asset Management (資産管理)] > [Composite Asset Strip Composition Changed (複合資産ストリップ構成の変更)]	Composition changed on composite asset strip [STRIPID] ('[STRIPNAME]'). (複合資産ストリップ [STRIPID] ('[STRIPNAME]') 構成が変更されました。)	
[RF Code Tag (RF Code タグ)] > [Connected (接続)]	RF Code tag has been connected. (RF Code タグが接続されました。)	RF Code tag has been disconnected. (RF Code タグが切断されました。)
[LHX] > [Connected (接続)]	LHX has been connected to [PORTTYPE] port [PORTID]. (LHX が	LHX has been disconnected from [PORTTYPE] port [PORTID]. (LHX

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
	[PORTTYPE] ポート [PORTID] に接続されました。)	が [PORTTYPE] ポート [PORTID] から切断されました。)
[LHX] > [Operational State (操作状態)]	LHX connected to [PORTTYPE] port [PORTID] has been switched on. ([PORTTYPE] ポート [PORTID] に接続された LHX がオンになりました。)	LHX connected to [PORTTYPE] port [PORTID] has been switched off. ([PORTTYPE] ポート [PORTID] に接続された LHX がオフになりました。)
[LHX] > [Sensor (センサー)] > [Unavailable (使用不可能)]	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' unavailable. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' は使用不可能です。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' available. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' は使用可能です。)
[LHX] > [Sensor (センサー)] > [Above upper critical threshold (上位臨界しきい値より上)]	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper critical'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' が '上位臨界以上' をアサートしました。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper critical'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' の '上位臨界以上' のアサートが停止されました。)
[LHX] > [Sensor (センサー)] > [Above upper warning threshold (上位警告しきい値より上)]	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper warning'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' が '上位警告以上' をアサートしました。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper warning'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' の '上位警告以上' のアサートが停止されました。)
[LHX] > [Sensor (センサー)] > [Below lower warning threshold (下位警告しきい値より下)]	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower warning'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' が '下位警告未満' をアサートしました。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower warning'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' の '下位警告未満' のアサートが停止されました。)
[LHX] > [Sensor (センサー)] > [Below lower critical threshold (下	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]'

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
位臨界しきい値より下]]	'below lower critical'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' が '下位臨界未満' をアサートしました。)	deasserted 'below lower critical'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' の '下位臨界未満' のアサートが停止されました。)
[LHX] > [Emergency Cooling (緊急冷却)]	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was activated. (LHX の [PORTTYPE] ポート '[PORTID]' の緊急冷却が有効になりました。)	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was deactivated. (LHX の [PORTTYPE] ポート '[PORTID]' の緊急冷却が無効になりました。)
[LHX] > [Maximum cooling request (最大冷却要求)]	Maximum cooling was requested for LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' の最大冷却が要求されました。)	Maximum cooling is not any more requested for LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' の最大冷却の要求が解除されました。)
[LHX] > [Parameter Data Loss (パラメータ データの損失)]	Data loss in parameter memory was detected on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' でパラメータ メモリ内のデータが失われたことが検出されました。)	
[LHX] > [ST-Bus Communication Error (ST-バス通信エラー)]	An ST-Bus communication error was detected on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' で ST-バス通信エラーが検出されました。)	
[LHX] > [Collective fault (集合異常)]	A collective fault occurred on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' で集合異常が発生しました。)	
[LHX] > [Door Contact (扉接触)]	The door of LHX at [PORTTYPE] port '[PORTID]' was opened. (LHX の [PORTTYPE] ポート '[PORTID]' の扉が開かれました。)	The door of LHX at [PORTTYPE] port '[PORTID]' was closed. (LHX の [PORTTYPE] ポート '[PORTID]' の扉が閉じられました。)
[LHX] > [Sensor Failure (センサー障害)]	A sensor failure (broken or short circuit) occurred on LHX at [PORTTYPE] port	

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
	'[PORTID]' at sensor '[LHXSENSORID]'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' で、センサー障害 (破損または短絡) が発生しました。)	
[LHX] > [Fan Failure (ファン障害)]	A fan motor failure occurred on LHX at [PORTTYPE] port '[PORTID]' at fan '[LHXFANID]'. (LHX の [PORTTYPE] ポート '[PORTID]' の ファン '[LHXFANID]' でファン モーターの障害が発生しました。)	
[LHX] > [Power Supply Failure (電源障害)]	A power supply failure occurred on LHX at [PORTTYPE] port '[PORTID]' at power supply '[LHXPOWERSUPPLYID]'. (LHX の [PORTTYPE] ポート '[PORTID]' の 電源 '[LHXPOWERSUPPLYID]' で電源障害が発生しました。)	
[LHX] > [Threshold Air Inlet (吸気口のしきい値)]	The air inlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed. (LHX の [PORTTYPE] ポート '[PORTID]' の吸気口の温度しきい値を超えました。)	The air inlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds. (LHX の [PORTTYPE] ポート '[PORTID]' の吸気口の温度はしきい値の範囲内になりました。)
[LHX] > [Threshold Air Outlet (排気口のしきい値)]	The air outlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed. (LHX の [PORTTYPE] ポート '[PORTID]' の排気口の温度しきい値を超えました。)	The air outlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds. (LHX の [PORTTYPE] ポート '[PORTID]' の排気口の温度はしきい値の範囲内になりました。)
[LHX] > [Threshold Water Inlet (吸水口のしきい値)]	The water inlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed. (LHX の [PORTTYPE] ポート '[PORTID]' の吸水口の温度しきい値を超えました。)	The water inlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds. (LHX の [PORTTYPE] ポート '[PORTID]' の吸水口の温度はしきい値の範囲内になりました。)
[LHX] > [Threshold Water Outlet (排水口のしきい値)]	The water outlet temperature threshold on LHX at [PORTTYPE] port	The water outlet temperature on LHX at [PORTTYPE] port

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
	'[PORTID]' was crossed. (LHX の [PORTTYPE] ポート '[PORTID]' の排水口の温度しきい値を超えました。)	'[PORTID]' is within thresholds. (LHX の [PORTTYPE] ポート '[PORTID]' の排水口の温度はしきい値の範囲内になりました。)
[LHX] > [Threshold Humidity (湿度のしきい値)]	The humidity threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed. (LHX の [PORTTYPE] ポート '[PORTID]' の湿度しきい値を超えました。)	The humidity on LHX at [PORTTYPE] port '[PORTID]' is within thresholds. (LHX の [PORTTYPE] ポート '[PORTID]' の湿度はしきい値の範囲内になりました。)
[LHX] > [External Water Cooling Failure (外部の水冷障害)]	An external water cooling failure occurred on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' で外部の水冷障害が発生しました。)	
[LHX] > [Water Leak (漏水)]	Water leakage was detected on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' で漏水が検出されました。)	

*注: 'トリガ' イベントに対する設定はありません ([ASSERTION] を参照してください)。

ルールの作成

必要なアクションが使用可能になると、特定のイベントに対応するための実行アクションを決定するイベント ルールを作成できます。

Dominion PX にはデフォルトで [System Event Log Rule (システム イベント ログ ルール)] と [System SNMP Trap Rule (システム SNMP トラップ ルール)] という 2 つのイベント ルールが組み込まれています。組み込みのルールではニーズが満たされない場合は、新しいルールを作成します。

▶ イベント ルールを作成するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. [Rules (ルール)] タブで、[New Rule (新規ルール)] をクリックします。
3. [Rule name (ルール名)] フィールドに、ルールを識別する新しい名前を入力します。デフォルトの名前は、[New Rule <number> (新規ルール <番号>)] です。<number> は連番です。

4. このイベント ルールを有効にするには、[Enabled (有効)] チェックボックスをオンにします。
5. [Event (イベント)] をクリックし、アクションをトリガするイベントを選択します。すべてのタイプのイベントを表示するプルダウン メニューが表示されます。
 - プルダウン メニューから目的のイベント タイプを選択します。サブメニューが表示される場合は、目的のイベントを選択するまで選択を続けます。

注: オプション [Any sub-event (任意のサブイベント)] は同じサブメニューに表示されるすべてのイベント/項目を指し、[Any slot (任意のスロット)] はすべてのスロット、[Any server (任意のサーバ)] はすべてのサーバ、[Any user (任意のユーザ)] はすべてのユーザを指します。

6. 前の手順で選択したイベントに応じて、3 つのラジオ ボタンが含まれる [Trigger condition (トリガ条件)] フィールドが表示される場合と表示されない場合があります。

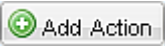
イベントのタイプ	ラジオ ボタン
数値センサーのしきい値超過イベント、または資産タグの接続や切断	利用可能なラジオ ボタンは、[Asserted (アサート)]、[Deasserted (アサート停止)]、および [Both (両方)] です。 ■ [Asserted (アサート)]: イベントが発生したときにのみ、Dominion PX でアクションが実行されます。つまり、記述したイベントの FALSE から TRUE への遷移の状態を表しています。 ■ [Deasserted (アサート停止)]: イベント条件が解消されたときにのみ、Dominion PX でアクションが実行されます。つまり、記述したイベントの TRUE から FALSE への遷移の状態を表しています。 ■ [Both (両方)]: イベントが発生したとき (アサート)、およびイベント条件が解消されたとき (アサート停止) に、Dominion PX でアクションが実行されます。

イベントのタイプ	ラジオ ボタン
ディスクリート (オン/オフ) センサーの状態変化	利用可能なラジオ ボタンは、[Alarmed (アラーム)]、[No longer alarmed (アラーム停止)]、および [Both (両方)] です。 ▪ [Alarmed (アラーム)]: 選択したセンサーがアラーム状態、つまり異常状態になったときにのみ、Dominion PX でアクションが実行されます。 ▪ [No longer alarmed (アラーム停止)]: 選択したセンサーが正常に戻ったときにのみ、Dominion PX でアクションが実行されます。 ▪ [Both (両方)]: 選択したセンサーがアラーム状態になるか、アラーム状態でなくなったときに、Dominion PX でアクションが実行されます。
センサーの可用性	利用可能なラジオ ボタンは、[Unavailable (使用不可能)]、[Available (使用可能)]、および [Both (両方)] です。 ▪ [Unavailable (使用不可能)]: 選択したセンサーが検出されないとき、および使用不可能になったときにのみ、Dominion PX でアクションが実行されます。 ▪ [Available (使用可能)]: 選択したセンサーが検出されたとき、および使用可能になったときにのみ、Dominion PX でアクションが実行されます。 ▪ [Both (両方)]: 選択したセンサーが使用不可能または使用可能になったときに、Dominion PX でアクションが実行されます。
ネットワーク インタフェースのリンク状態	利用可能なラジオ ボタンは、[Link state is up (リンク状態がアップ)]、[Link state is down (リンク状態がダウン)]、および [Both (両方)] です。 ▪ [Link state is up (リンク状態がアップ)]: ネットワーク リンク状態がダウンからアップに変わったときにのみ、Dominion PX でアクションが実行されます。 ▪ [Link state is down (リンク状態がダウン)]: ネットワーク リンク状態がアップからダウンに変わったときにのみ、Dominion PX でアクションが実行されます。 ▪ [Both (両方)]: ネットワーク リンク状態が変わるたびに、Dominion PX でアクションが実行されます。

イベントのタイプ	ラジオ ボタン
機能が有効または無効	利用可能なラジオ ボタンは、[Enabled (有効)]、[Disabled (無効)]、および [Both (両方)] です。 ▪ [Enabled (有効)]: 選択した機能が有効になったときにのみ、Dominion PX でアクションが実行されます。 ▪ [Disabled (無効)]: 選択した機能が無効になったときにのみ、Dominion PX でアクションが実行されます。 ▪ [Both (両方)]: 選択した機能が有効または無効になったときに、Dominion PX でアクションが実行されます。
ユーザのログインまたはログアウト	利用可能なラジオ ボタンは、[Logged in (ログイン)]、[Logged out (ログアウト)]、および [Both (両方)] です。 ▪ [Logged in (ログイン)]: 選択したユーザがログインしたときにのみ、Dominion PX でアクションが実行されます。 ▪ [Logged out (ログアウト)]: 選択したユーザがログアウトしたときにのみ、Dominion PX でアクションが実行されます。 ▪ [Both (両方)]: 選択したユーザがログインおよびログアウトしたときに、Dominion PX でアクションが実行されます。
サーバ監視イベント	利用可能なラジオ ボタンは、[Monitoring started (監視開始)]、[Monitoring stopped (監視停止)]、および [Both (両方)] です。 ▪ [Monitoring started (監視開始)]: 指定したサーバの監視が開始されたときにのみ、Dominion PX でアクションが実行されます。 ▪ [Monitoring stopped (監視停止)]: 指定したサーバの監視が停止されたときにのみ、Dominion PX でアクションが実行されます。 ▪ [Both (両方)]: 指定したサーバの監視が開始または停止されたときに、Dominion PX でアクションが実行されます。

イベントのタイプ	ラジオ ボタン
サーバへの到達可能性	利用可能なラジオ ボタンは、[Unreachable (到達不能)]、[Reachable (到達可能)]、および [Both (両方)] です。 ▪ [Unreachable (到達不能)]: 指定したサーバにアクセス不能になったときにのみ、Dominion PX でアクションが実行されます。 ▪ [Reachable (到達可能)]: 指定したサーバにアクセス可能になったときにのみ、Dominion PX でアクションが実行されます。 ▪ [Both (両方)]: 指定したサーバにアクセス不能またはアクセス可能になったときに、Dominion PX でアクションが実行されます。
RF Code tag connection or disconnection (RF Code タグの接続または切断)	利用可能なラジオ ボタンは、[Connected (接続)]、[Disconnected (切断)]、および [Both (両方)] です。 ▪ [Connected (接続)]: RF Code タグが物理的に接続されたときにのみ、Dominion PX でアクションが実行されます。 ▪ [Disconnected (切断)]: RF Code タグが物理的に切断されたときにのみ、Dominion PX でアクションが実行されます。 ▪ [Both (両方)]: RF Code タグが物理的に接続されたとき、および切断されたときに、Dominion PX でアクションが実行されます。
Outlet power state change (アウトレット (コンセント) の電源状態の変化)	利用可能なラジオ ボタンは、[On (オン)]、[Off (オフ)]、および [Both (両方)] です。 ▪ [On (オン)]: 選択したアウトレット (コンセント) がオンになったときにのみ、Dominion PX でアクションが実行されます。 ▪ [Off (オフ)]: 選択したアウトレット (コンセント) がオフになったときにのみ、Dominion PX でアクションが実行されます。 ▪ [Both (両方)]: 選択したアウトレット (コンセント) がオンまたはオフになったときに、Dominion PX でアクションが実行されます。

注: アウトレット (コンセント) の電源状態変更イベントは、アウトレット (コンセント) 切り替え対応 PDU でのみ使用できます。

1. [Actions (アクション)] フィールドのドロップダウン矢印をクリックして、必要なアクションをリストから選択し、[Add Action (アクションの追加)] ボタン  をクリックしてアクションを追加します。

追加したアクションは、[Actions (アクション)] フィールドの右にあるリスト ボックスに表示されます。

2. さらにアクションを追加するには、手順 7 を繰り返します。
3. 追加したアクションを削除するには、リスト ボックスから選択して [Remove selected Action (選択したアクションの削除)] ボタン  をクリックします。

4. [Save (保存)] をクリックして新しいイベント ルールを保存します。

注: [Save (保存)] をクリックしないで現在の設定ページを閉じると、メッセージが表示されます。変更を保存する場合は [Yes (はい)] を、変更を中止する場合は [Discard (破棄)] を、現在の設定ページに戻る場合は [Cancel (キャンセル)] をクリックします。

5. さらにイベント ルールを作成するには、手順 2 ~ 10 を繰り返します。
6. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

イベント ルールのサンプル

PDU レベルのイベント ルールのサンプル

この例では、ファームウェア アップグレード エラーが発生したときに、そのエラーが Dominion PX の内部ログに記録されるようにします。イベント ルールのサンプルは、次のようになります。

- [Event (イベント)]: [Events (イベント)] > [Device (デバイス)] > [Firmware update failed (ファームウェアの更新エラー)]
- [Trigger condition (トリガ条件)]: [asserted (アサート)]
- [Actions (アクション)]: [System Event Log Action (システム イベント ログ アクション)]

▶ 上記のイベント ルールを作成するには、次の手順に従います。

1. PDU レベルのイベントを指定するため、[Events (イベント)] > [Device (デバイス)] を選択します。
2. サブメニューの [Firmware update failed (ファームウェアの更新エラー)] を選択します。これは、ファームウェア アップグレード エラーに関するイベントに Dominion PX が対応するように指定するためです。

3. ファームウェアの更新エラー イベントが内部ログに記録されるように、[System Event Log Action (システム イベント ログ アクション)] を選択します。
4. 選択したイベントが発生したときにのみそのイベントが記録されるように、[asserted (アサート)] ラジオ ボタンを選択します。

アウトレット (コンセント) レベルのイベント ルールのサンプル

この例では、アウトレット (コンセント) 3 の任意のセンサー測定値がしきい値のいずれかを超えたとき、およびその測定値が正常に戻ったときに、Dominion PX から SNMP マネージャに SNMP トラップが送信されるようにします。このためには、イベント ルールを次のように設定します。

- [Event (イベント)]: [Events (イベント)] > [Outlet (アウトレット (コンセント))] > [Outlet 3 (アウトレット (コンセント) 3)] > [Sensor (センサー)] > [Any sub-event (任意のサブイベント)]
- [Trigger condition (トリガ条件)]: [both (両方)]
- [Actions (アクション)]: [System SNMP Trap Action (システム SNMP トラップ アクション)]

▶ 上記のイベント ルールを作成するには、次の手順に従います。

1. アウトレット (コンセント) レベルのイベントを指定するため、[Events (イベント)] > [Outlet (アウトレット (コンセント))] を選択します。
2. サブメニューから、対象のアウトレット (コンセント) である [Outlet 3 (アウトレット (コンセント) 3)] を選択します。
3. センサー測定値を参照するため、[Sensor (センサー)] を選択します。
4. アウトレット (コンセント) のあらゆるタイプのセンサーおよびしきい値 (電流、電圧、上位臨界しきい値、上位警告しきい値、下位臨界しきい値、下位警告しきい値など) に関連するすべてのイベントを指定するため、[Any sub-event (任意のサブイベント)] を選択します。
5. 指定したイベントに対応する SNMP トラップを送信するため、[System SNMP Trap Action (システム SNMP トラップ アクション)] を選択します。
6. [both (両方)] ラジオ ボタンを選択し、アウトレット (コンセント) 3 の任意のセンサー測定値が警告状態または臨界状態になったとき、およびセンサー測定値が正常に戻ったときに、SNMP トラップが送信されるようにします。

たとえば、アウトレット (コンセント) 3 の電圧が上位警告範囲に入ると、SNMP トラップが送信され、この電圧が上位警告しきい値を下回ると、もう一度 SNMP トラップが送信されます。

インレット レベルのイベント ルールのサンプル

この例では、インレット I1 の任意のセンサー測定値がしきい値のいずれかを超えたとき、およびその測定値が正常に戻ったときに、Dominion PX から SNMP マネージャに SNMP トラップが送信されるようにします。このイベント ルールの設定は、次のようになります。

- [Event (イベント)]: [Events (イベント)] > [Inlet (インレット)] > [Inlet I1 (インレット I1)] > [Sensor (センサー)] > [Any sub-event (任意のサブイベント)]
- [Trigger condition (トリガ条件)]: [both (両方)]
- [Actions (アクション)]: [System SNMP Trap Action (システム SNMP トラップ アクション)]

▶ 上記のイベント ルールを作成するには、次の手順に従います。

1. インレット レベルでイベントを指定するため、[Events (イベント)] > [Inlet (インレット)] を選択します。
2. サブメニューから、対象のインレットである [Inlet I1 (インレット I1)] を選択します。
3. センサー測定値を参照するため、[Sensor (センサー)] を選択します。
4. インレットのあらゆるタイプのセンサーおよびしきい値（電流、電圧、上位臨界しきい値、上位警告しきい値、下位臨界しきい値、下位警告しきい値など）に関連するすべてのイベントを指定するため、[Any sub-event (任意のサブイベント)] を選択します。
5. 指定したイベントに対応する SNMP トラップを送信するため、[System SNMP Trap Action (システム SNMP トラップ アクション)] を選択します。
6. [both (両方)] ラジオ ボタンを選択し、インレット I1 の任意のセンサー測定値が警告状態または臨界状態になったとき、およびセンサー測定値が正常に戻ったときに、SNMP トラップが送信されるようにします。

たとえば、インレット I1 の電圧が上位警告範囲に入ると、SNMP トラップが送信され、この電圧が上位警告しきい値を下回ると、もう一度 SNMP トラップが送信されます。

環境センサー レベルのイベント ルールのサンプル

このセクションは、アウトレット（コンセント）切り替え対応 PDU にのみ適用されます。

この例では、接点閉鎖センサーがアラーム状態になったときに Dominion PX で負荷遮断機能を有効にします。このサンプル イベント ルールでは、ルールを作成する前に、新しいアクションを作成する必要があります。

▶ 手順 1: 負荷遮断モードを有効にする新規アクションの作成

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. [Actions (アクション)] タブをクリックします。
3. [New Action (新規アクション)] をクリックします。
4. [Action name (アクション名)] フィールドに、このアクションを識別する名前を入力します。この例では、「Enable Load Shedding (負荷遮断モードを有効化)」と入力します。
5. [Action (アクション)] フィールドで、[Change load shedding state (負荷遮断状態の変更)] を選択します。
6. [Operation (動作)] フィールドで、[Enable load shedding (負荷遮断を有効にする)] を選択します。
7. [Save (保存)] をクリックしてこのアクションを保存します。

負荷遮断モードを有効にする新規アクションが作成できたら、次に接点閉鎖センサーがアラーム状態になったときに負荷遮断モードをトリガできるイベント ルールを作成できます。このイベント ルールのサンプルは、次のようになります。

- [Event (イベント)]: [Events (イベント)] > [External Sensor Slot (外部センサー スロット)] > [Slot 1 (スロット 1)] > [State Sensor (状態センサー)] > [Alarmed (アラーム)]
- [Trigger condition (トリガ条件)]: [Alarmed (アラーム)]
- [Actions (アクション)]: [Enable Load Shedding (負荷遮断モードを有効化)]

▶ 手順 2: 「接点閉鎖で負荷遮断をトリガ」イベント ルールの作成

1. [Rules (ルール)] タブをクリックします。
2. [New Rule (新規ルール)] をクリックします。
3. [Rule name (ルール名)] フィールドに、このイベント ルールを識別するための名前を入力します。この例では、「Contact Closure Triggered Load Shedding (接点閉鎖で負荷遮断をトリガ)」と入力します。
4. [Enabled (有効)] チェックボックスをオンにします。オフの場合は、新しいイベント ルールは実行されません。

- 5. [Events (イベント)] > [External Sensor Slot (外部センサー スロット)] を選択して、環境センサーに関連するイベントの指定中であることを示します。
- 6. 目的の接点閉鎖センサーの ID 番号を選択します。この例では、目的の接点閉鎖センサーの ID 番号を 1 とするので、サブメニューの [Slot 1 (スロット 1)] を選択します。
- 7. 接点閉鎖センサーは、状態の変化を通じて環境が変わったことを示す ディスクリット センサーなので、[State Sensor (状態センサー)] を選択します。
- 8. 選択した接点閉鎖センサーが「alarmed (アラーム)」状態に関連付けられている状態に変わったときにアクション [Enable Loading Shedding (負荷遮断モードを有効化)] を実行させるので、サブメニューの [Alarmed (アラーム)] を選択します。
- 9. Dominion PX がイベントに対応するのは接点閉鎖センサーがアラーム状態に入った場合に限るので、[Trigger condition (トリガ条件)] フィールドで [Alarmed (アラーム)] ラジオ ボタンを選択します。

無限ループに関する注意

イベント ルールを作成する場合は、無限ループを作らないようにする必要があります。

無限ループとは、特定のイベントに対するアクションまたは複数のアクションのうちの 1 つが、同一または類似のイベントをトリガし、それによってアクションが再度イベントをトリガする結果となって、PDU が常にビジーとなっている状況を指します。

例 1

この例では、イベント ルールが PDU による SMTP メッセージの連続送信を引き起こします。

選択したイベント	含まれるアクション
[Device (デバイス)] > [Sending SMTP message failed (SMTP メッセージの送信の失敗)]	Send SMTP message (SMTP メッセージの送信)

例 2

この例のイベント ルールは、[Device (デバイス)] メニューのリスト内の選択したイベントの 1 つが発生したときに、PDU による SMTP メッセージの連続送信を引き起こします。[Device (デバイス)] メニューの下の〈Any sub-event〉(任意のサブイベント) には、「Sending SMTP message failed (SMTP メッセージの送信の失敗)」が含まれることに注意してください。

選択したイベント	含まれるアクション
[Device (デバイス)] > [Any sub-event (任意のサブイベント)]	Send SMTP message (SMTP メッセージの送信)

例 3

この例は、アウトレット (コンセント) 状態の変化に関する 2 つのイベント ルールが組み合わせられて、PDU によるアウトレット (コンセント) 1 および 2 の連続的な電源再投入を引き起こす状況を示しています。

選択したイベント	含まれるアクション
[Outlet (アウトレット (コンセント))] > [Outlet 1 (アウトレット (コンセント) 1)] > [Sensor (センサー)] > [State (状態)] > [On/Off (オン/オフ)]	[Cycle Outlet 2 (アウトレット (コンセント) 2) の電源の再投入] ([Switch Outlets (アウトレット (コンセント) の切り替え)] --> [Cycle Outlet (アウトレット (コンセント) の電源の再投入)] --> [Outlet 2 (アウトレット (コンセント) 2)])
[Outlet (アウトレット (コンセント))] > [Outlet 2 (アウトレット (コンセント) 2)] > [Sensor (センサー)] > [State (状態)] > [On/Off (オン/オフ)]	[Cycle Outlet 1 (アウトレット (コンセント) 1) の電源の再投入] ([Switch Outlets (アウトレット (コンセント) の切り替え)] --> [Cycle Outlet (アウトレット (コンセント) の電源の再投入)] --> [Outlet 1 (アウトレット (コンセント) 1)])

イベント ルールの変更

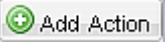
イベント ルールのイベント、アクション、トリガ条件、および、存在する場合はその他の設定も変更できます。

例外: [System Event Log Rule (システム イベント ログ ルール)] や [System SNMP Trap Rule (システム SNMP トラップ ルール)] を始めとする、組み込みのイベント ルールで選択されているイベントおよびアクションは、変更できません。

▶ イベント ルールを変更するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. [Rules (ルール)] タブの左側のペインで、変更するイベント ルールを選択します。
3. イベント ルールを無効にするには、[Enabled (有効)] チェックボックスをオフにします。
4. イベントを変更するには、[Event (イベント)] フィールドで目的のタブをクリックし、プルダウン メニューまたはサブメニューから別の項目を選択します。

たとえば、「admin」ユーザのユーザ アクティビティ イベント ルールで、[admin (admin)] タブをクリックして、すべてのユーザ名を表示するプルダウン サブメニューが表示されたら、別のユーザ名またはすべてのユーザ名 ([Any user (任意のユーザ)]) を選択します。

5. ラジオ ボタンが使用できる場合は、現在選択されていないラジオ ボタンを選択して、ルールのトリガ条件を変更できます。
6. アクションを変更するには、[Actions (アクション)] フィールドで次のいずれかの操作を実行します。
 - 新しいアクションを追加するには、ドロップダウン矢印をクリックし、リストからアクションを選択して、[Add Action (アクションの追加)] ボタン  をクリックします。
 - 追加したアクションを削除するには、リスト ボックスから選択して [Remove selected Action (選択したアクションの削除)] ボタン  をクリックします。
7. [Save (保存)] をクリックして変更を保存します。

注: [Save (保存)] をクリックしないで現在の設定ページを閉じると、メッセージが表示されます。変更を保存する場合は [Yes (はい)] を、変更を中止する場合は [Discard (破棄)] を、現在の設定ページに戻る場合は [Cancel (キャンセル)] をクリックします。

8. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

アクションの変更

既存のアクションを変更すると、それに従って、そのアクションが関与するすべてのイベント ルールの動作が変更されます。

例外: 組み込みのアクション [System Event Log Action (システム イベント ログ アクション)] は、ユーザが設定することはできません。

▶ **アクションを変更するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. [Actions (アクション)] タブをクリックします。
3. 変更するアクションを左側のリストから選択します。
4. 表示される内容に必要な変更を加えます。
5. [Save (保存)] をクリックして変更を保存します。

注: [Save (保存)] をクリックしないで現在の設定ページを閉じると、メッセージが表示されます。変更を保存する場合は [Yes (はい)] を、変更を中止する場合は [Discard (破棄)] を、現在の設定ページに戻る場合は [Cancel (キャンセル)] をクリックします。

6. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

イベント ルールまたはアクションの削除

イベント ルールまたはアクションが古くなった場合は、それを削除します。

注: 組み込みのイベント ルールおよびアクションは削除できません。

▶ **イベント ルールまたはアクションを削除するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. イベント ルールを削除するには、次の手順に従います。
 - a. [Rules (ルール)] タブが選択されていることを確認します。選択されていない場合は、[Rules (ルール)] タブをクリックします。
 - b. 目的のルールを左側のリストから選択し、[Delete Rule (ルールの削除)] をクリックします。

- c. 操作の確認を求めるメッセージが表示されます。[Yes (はい)] をクリックして、削除を確認します。
3. アクションを削除するには、次の手順に従います。
 - a. [Actions (アクション)] タブをクリックします。
 - b. 目的のアクションを左側のリストから選択し、[Delete Action (アクションの削除)] をクリックします。
 - c. 操作の確認を求めるメッセージが表示されます。[Yes (はい)] をクリックして、削除を確認します。
4. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

トリガされないルールについての注意事項

場合によっては、測定値がしきい値を超えると、Dominion PX で警告が生成されます。その後、測定値がしきい値内の値に戻っても、Dominion PX でアサート停止イベントの警告メッセージは生成されません。このような状況は、Dominion PX で使用されるヒステリシス追跡機能が原因で生じることがあります。「アサート停止ヒステリシスとは『177p.』」を参照してください。

イベント ログिंगの管理

Dominion PX のデフォルトの設定では、特定のシステム イベントの情報が収集され、ローカル (内部) のイベント ログに保存されます。

ローカル イベント ログの表示

ローカル イベント ログでは、Dominion PX デバイスで発生した最大 2,000 個の履歴イベントを表示できます。

ログのエントリが 2,000 件に達した場合は、最も古いエントリが新しいエントリで上書きされます。

▶ **ローカル ログを表示するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [View Event Log (イベント ログの表示)] を選択します。[Event Log (イベント ログ)] ダイアログ ボックスが表示されます。

ローカル ログの各イベント エントリは、以下で構成されます。

- イベントの日付と時刻
- イベントのタイプ
- イベントの説明
- イベントの ID 番号

2. このダイアログ ボックスには、デフォルトでは最後のページが表示されます。次の作業を行うことができます。
 - 別のページを表示するには、次のいずれかの操作を行います。
 -  または  をクリックすると、最初または最後のページに移動します。
 -  または  をクリックすると、前または次のページに移動します。
 - [Page (ページ)] テキスト ボックスに番号を入力して Enter キーを押すと、指定したページに移動します。
 - リストからログ エントリを選択して [Show Details (詳細の表示)] をクリックするか、ログ エントリをダブルクリックすると、詳細情報が表示されます。
-
- 注: ダイアログ ボックスが狭すぎる場合は、[Show Details (詳細の表示)] ボタンではなく、アイコン  が表示されます。その場合は、 をクリックして [Show Details (詳細の表示)] を選択すると、詳細が表示されます。
-
-  をクリックして最新のイベントを表示します。
 3. 必要に応じてダイアログ ボックスを拡大します。
 4. リストの並べ替え、または表示列の変更を行うことができます。
 5. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

イベント エントリの消去

既存のイベント履歴を保持する必要がない場合は、すべてのイベント履歴をローカル ログから削除できます。

▶ すべてのイベント エントリを削除するには、次の手順に従います。

1. [Maintenance (メンテナンス)] > [View Event Log (イベント ログの表示)] を選択します。[Event Log (イベント ログ)] ダイアログ ボックスが表示されます。
2. [Clear Event Log (イベント ログのクリア)] をクリックします。
3. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

接続中のユーザの表示

Dominion PX デバイスに接続されているユーザとそのステータスを確認できます。管理者権限がある場合は、Dominion PX デバイスへのユーザの接続を終了できます。

▶ **接続中のユーザを表示するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [Connected Users (接続中のユーザ)] を選択します。[Connected Users (接続中のユーザ)] ダイアログ ボックスが表示され、接続中のユーザと次の情報のリストが表示されます。

列	説明
User Name (ユーザ名)	接続中の各ユーザによって使用されるログイン名。
IP Address (IP アドレス)	各ユーザのホストの IP アドレス。 シリアル接続経由のログインでは、〈local〉が IP アドレスの代わりに表示されます。
Client Type (クライアント タイプ)	ユーザが Dominion PX に接続するために使用しているインタフェース。 ▪ Web GUI: Dominion PX Web インタフェースを指します。 ▪ CLI: コマンド ライン インタフェース (CLI) を指します。 「CLI」に続く括弧内の情報は、このユーザが CLI に接続した方法を示します。 - <i>Serial</i> (シリアル): ローカル接続 (シリアルまたは USB) を示します。 - <i>SSH</i>: SSH 接続を示します。 - <i>Telnet</i>: Telnet 接続を示します。
Idle Time (アイドル時間)	ユーザがアイドル状態にいる時間。 単位「min」は分を表します。

1. ユーザを切断するには、対応する [Disconnect (切断)] ボタンをクリックします。
 - a. 操作の確認を求めるダイアログ ボックスが表示されます。
 - b. [Yes (はい)] をクリックしてユーザを切断するか、[No (いいえ)] をクリックして操作を中止します。[Yes (はい)] をクリックすると、接続中のユーザは強制的にログアウトされます。
2. 必要に応じて、リストの並べ替え順序を変更できます。「**並べ替えの変更**」『84p.』を参照してください。

- 3. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

サーバ アクセシビリティの監視

Dominion PX デバイスで継続的に ping を実行して、特定の IT デバイスが動作しているかどうかを監視できます。IT デバイスが ping コマンドに正常に応答した場合、その IT デバイスはまだ動作中であり、リモートでアクセスできます。

ping 監視対象の IT デバイスの追加

DB サーバやリモート認証サーバなどの IT 機器のアクセシビリティを Dominion PX で監視できます。

- ▶ **ping 監視対象の IT 機器を追加するには、次の手順に従います。**
 - 1. [Device Settings (デバイス設定)] > [Server Reachability (サーバへの到達可能性)] を選択します。[Server Reachability (サーバへの到達可能性)] ダイアログ ボックスが表示されます。
 - 2. [New (新規)] をクリックします。[Add New Server (新しいサーバの追加)] ダイアログ ボックスが表示されます。
 - 3. デフォルトでは、[Enable Ping Monitoring for this Server (このサーバの ping 監視を有効にする)] チェックボックスがオンになっています。オフになっている場合は、オンにして ping 監視機能を有効にします。
 - 4. 必要な情報を入力します。

フィールド	説明
IP Address/Hostname (IP アドレス/ホスト名)	アクセシビリティを監視する IT 機器の IP アドレスまたはホスト名。
Number of Successful Pings to Enable Feature (機能を有効にするために必要な ping の成功数)	この機能を有効にするために必要な、成功した ping の数。有効な範囲は 0 ～ 200 です。
Wait Time (in seconds) after Successful Ping (ping 成功後の待機時間 (秒))	前の ping の応答を正常に受信した場合に、次の ping を送信するまで待機する時間。有効な範囲は 5 ～ 600 (秒) です。
Wait Time (in seconds) after Unsuccessful Ping (ping 失敗後の待機時間 (秒))	前の ping の応答がなかった場合に、次の ping を送信するまで待機する時間。有効な範囲は 3 ～ 600 (秒) です。

フィールド	説明
Number of Consecutive Unsuccessful Pings for Failure (失敗時の連続した ping 失敗数)	IT 装置が応答不能と判断されるまでの応答のない連続した ping の数。有効な範囲は 1 ～ 100 です。
Wait Time (in seconds) before Resuming Pinging (ping 再開までの待機時間 (秒))	IT 装置が応答不能と判断された後、ping を再開するまで待機する時間。有効な範囲は 1 ～ 1200 (秒) です。

5. [OK] をクリックして変更を保存します。
6. 他の IT デバイスを追加するには、手順 2 ～ 5 を繰り返します。
7. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

ping 監視設定の編集

IT デバイスの ping 監視設定は、変更が必要なときにいつでも編集できます。

▶ IT デバイスの ping 監視設定を変更するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Server Reachability (サーバへの到達可能性)] を選択します。[Server Reachability (サーバへの到達可能性)] ダイアログ ボックスが表示されます。
2. 設定を変更する IT デバイスをクリックして選択します。
3. [Edit (編集)] をクリックするか、IT デバイスをダブルクリックします。[Edit Server 'XXX' (サーバ 'XXX' の編集)] ダイアログ ボックスが表示されます。XXX は IT デバイスの IP アドレスまたはホスト名です。
4. 表示される内容に変更を加えます。
5. [OK] をクリックして変更を保存します。

ping 監視設定の削除

IT デバイスのアクセシビリティを監視する必要がない場合は、IT デバイスを削除するだけです。

▶ IT デバイスの ping 監視設定を削除するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Server Reachability (サーバへの到達可能性)] を選択します。[Server Reachability (サーバへの到達可能性)] ダイアログ ボックスが表示されます。

2. ping 監視設定を削除する IT デバイスをクリックして選択します。
複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
3. [Delete (削除)] をクリックします。
4. 操作の確認を求めるメッセージが表示されます。[Yes (はい)] をクリックして、削除を確認します。
5. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

サーバ監視状態の確認

サーバ監視の結果は、監視する Dominion PX デバイスのサーバを指定した後、[Server Reachability (サーバへの到達可能性)] ダイアログ ボックスに表示されます。

▶ サーバ監視の状態と結果を確認するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Server Reachability (サーバへの到達可能性)] を選択します。[Server Reachability (サーバへの到達可能性)] ダイアログ ボックスが表示されます。
2. [Ping Enabled (ping 有効)] というラベルの付いた列は、対応するサーバの監視が有効かどうかを示します。
 - : このアイコンは、対応するサーバの監視が有効であることを示します。
 - : このアイコンは、対応するサーバの監視が無効であることを示します。
3. [Status (状態)] というラベルの付いた列は、各監視対象サーバのアクセシビリティを示します。

状態	説明
Reachable (到達可能)	サーバにアクセスできます。
Unreachable (到達不能)	サーバにアクセスできません。
Waiting for reliable connection (信頼できる接続を待機中)	Dominion PX デバイスとサーバ間の接続はまだ確立されていません。

4. 必要に応じて、リストの並べ替え順序を変更できます。「**並べ替えの変更**『84p.』」を参照してください。
5. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

[Environmental Sensors (環境センサー)]

Dominion PX では、環境センサーが配置されている場所の温度や湿度などの環境条件を監視できます。

▶ **環境センサーを追加するには、次の手順に従います。**

1. 環境センサーを Dominion PX デバイスに物理的に接続します。「**環境センサーの接続 (オプション)**」『37p.』を参照してください。
2. Dominion PX Web インタフェースにログインします。接続したセンサーは、Dominion PX で検出され、Web インタフェースに表示されます。
3. 各センサーは、センサーのシリアル番号で識別します。「**環境センサーの識別**」『224p.』を参照してください。
4. 検出されたセンサーは、Dominion PX で自動的に管理されます。検出されたセンサーが管理されているかどうかを確認します。管理されていない場合は、そのセンサーを管理対象にします。「**環境センサーの管理**」『225p.』を参照してください。
5. センサーを設定します。「**環境センサーの設定**」『227p.』を参照してください。この手順は、次のとおりです。
 - a. センサーに名前を付けます。
 - b. 接続したセンサーが Raritan 製接点閉鎖センサーの場合、適切なセンサー タイプを指定します。
 - c. ラックまたはルーム内のセンサーの物理的な場所を指定します。
 - d. 数値センサーの場合、センサーのしきい値、ヒステリシス、およびアサート タイムアウトを設定します。

注: 数値センサーでは、環境条件や内部条件が数値で示され、ディスプレイ (オン/オフ) センサーでは、状態が英字で示されます。しきい値設定があるのは数値センサーだけです。

環境センサーの識別

環境センサーのケーブルにはシリアル番号のタグが付いています。



各センサーのシリアル番号は、Dominion PX によって各センサーが検出された後に Web インタフェースに表示されます。

▶ **検出された各環境センサーを識別するには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*」『76p. の「ツリーの展開」参照』を参照してください。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「*Naming the PDU (PDU のネーミング)*」『90p. の「PDU の名前付け」参照先』を参照してください。

2. Dominion PX Explorer ペインで [External Sensors (外部センサー)] をクリックすると、右側のペインに [External Sensors (外部センサー)] ページが表示されます。

External Sensors						
#	Serial Number	Type	Channel	Name	Reading	State
1	PRC0190292	Contact (On/Off)	1	On/Off 1		normal
2	PRC0190292	Contact (On/Off)	2	On/Off 2		normal
3	AEI7A00022	Temperature		Temperature 1	25.6 °C	normal
4	AEI7A00022	Humidity		Humidity 1	59 %	normal

3. タグのシリアル番号を、センサーの一覧に表示されている番号と突き合わせます。

環境センサーの管理

環境センサーが管理対象になると、Dominion PX によって環境センサーの表示値や状態が取得され、状態遷移が記録されます。

Dominion PX では最大 16 台の環境センサーを管理できます。

環境センサーが 16 台未満の場合、検出されたすべての環境センサーが Dominion PX によって自動的に管理対象になります。管理対象になっていないセンサーを手動で管理することもできます。

▶ **環境センサーを手動で管理するには、以下の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*」『76p. の「ツリーの展開」参照』を参照してください。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「*Naming the PDU (PDU のネーミング)*」『90p. の「PDU の名前付け」参照先』を参照してください。

2. Dominion PX Explorer ペインで [External Sensors (外部センサー)] をクリックすると、右側のペインに [External Sensors (外部センサー)] ページが表示されます。
3. [External Sensors (外部センサー)] ページで管理するセンサーをクリックします。

注: 検出されたすべてのセンサーを識別するには、「**環境センサーの識別**」『224p.』を参照してください。

4. [Manage (管理)] をクリックします。[Manage sensor <serial number> (<sensor type>) (センサーの管理 <シリアル番号> (<センサー タイプ>))] ダイアログ ボックスが表示されます。<serial number> にはセンサーのシリアル番号、<sensor type> にはセンサーのタイプが表示されます。

注: 接点閉鎖センサーの場合は、<sensor type> の後にチャンネル番号が追加されます。

5. センサーの管理方法には、次の 2 種類があります。
 - Dominion PX で番号を割り当てる方法でこのセンサーを管理するには、[Automatically assign a sensor number (センサー番号の自動割り当て)] を選択します。この方法では、管理対象センサーは解放されません。
 - 自分で番号を割り当てる方法でこのセンサーを管理するには、[Manually select a sensor number (センサー番号の手動選択)] を選択します。次に、ドロップダウン矢印を使用して番号を選択します。

選択した番号がすでにセンサーに割り当てられていた場合、そのセンサーは、この ID 番号が失われ 6 日後、解放されます。

ヒント: 各 ID 番号に続く括弧内の情報は、番号がすでにセンサーに割り当てられているかどうかを示します。すでに割り当てられている場合は、そのセンサーのシリアル番号が表示されます。それ以外の場合は、「unused (未使用)」と表示されます。

6. [OK] をクリックします。Dominion PX による追跡が開始され、管理対象センサーの測定値や状態が表示されます。
7. 他のセンサーも管理するには、手順 3 ～ 6 を繰り返します。

注: 管理対象のセンサー数が最大に達した場合は、管理対象のいずれかのセンサーを削除するか置き換えない限り、それ以上のセンサーを管理することはできません。センサーを削除するには、「**環境センサーを管理対象から除外**」『234p.』を参照してください。

環境センサーの設定

管理対象のセンサーを容易に識別できるようにデフォルトの名前を変更したり、センサーの場所を X、Y、Z 座標で記述したりすることができます。

▶ 環境センサーを設定するには、次の手順に従います。

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*」『76p. の「ツリーの展開」参照』を参照してください。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「*Naming the PDU (PDU のネーミング)*」『90p. の「PDU の名前付け」参照先』を参照してください。

2. Dominion PX Explorer ペインで [External Sensors (外部センサー)] をクリックすると、右側のペインに [External Sensors (外部センサー)] ページが表示されます。
3. 設定するセンサーを選択します。
4. [Setup (設定)] をクリックします。[Setup of external sensor <serial number> (<sensor type>) (外部センサーの設定 <シリアル番号> (<センサー タイプ>))] ダイアログ ボックスが表示されます。<serial number> にはこのセンサーのシリアル番号、<sensor type> にはセンサーのタイプが表示されます。

ヒント: この設定ダイアログ ボックスは、ツリーで目的の環境センサーのアイコンを選択し、右側のペインに表示されたそのセンサーのページで [Setup (設定)] ページをクリックする方法でも表示できます。

5. 選択した環境センサーがサードパーティ検出装置/スイッチに接続された Raritan 接点閉鎖センサーである場合、[Binary Sensor Subtype (バイナリ センサー サブタイプ)] フィールドで適切なセンサー タイプを選択します。
 - [Contact (接点)]: 検出装置/スイッチは、扉施錠状態または扉開閉状態を検出するように設計されています。
 - [Smoke Detection (煙検出)]: 検出装置/スイッチは、煙を検出するように設計されています。
 - [Water Detection (水検出)]: 検出装置/スイッチは、床面の水を検出するように設計されています。
 - [Vibration (振動)]: 検出装置/スイッチは、床の振動を検出するように設計されています。
6. 新しい名前を [Name (名前)] フィールドに入力します。

7. X、Y、Z 座標に英数字の値を割り当ててセンサーの場所を記述します。「**センサーの場所の記述**『229p.』」を参照してください。

注：Z 位置フィールドのかっこ内に「Rack Units (ラック ユニット)」というテキストが表示されている場合、Z 座標形式が [Rack Units (ラック ユニット)] に設定されているので、整数値を入力する必要があります。

8. 選択した環境センサーが数値センサーである場合、そのしきい値設定がダイアログ ボックスに表示されます。[Edit (編集)] をクリックするか、[Threshold Configuration (しきい値設定)] をダブルクリックして、しきい値、アサート停止ヒステリシス、およびアサート タイムアウトの設定を調整します。
 - しきい値を有効にするには、対応するチェックボックスをオンにします。しきい値を無効にするには、[enabled (有効)] チェックボックスをオフにします。
 - しきい値を有効にしてから、付随するテキスト ボックスに適切な数値を入力します。
 - すべてのしきい値のアサート停止ヒステリシスを有効にするには、[Deassertion Hysteresis (アサート停止ヒステリシス)] フィールドにゼロ以外の数値を入力します。「**アサート停止ヒステリシスとは**『177p.』」を参照してください。
 - すべてのしきい値のアサート タイムアウトを有効にするには、[Assertion Timeout (samples) (アサート タイムアウト (サンプル))] フィールドにゼロ以外の数値を入力します。「**アサート タイムアウトとは**『178p.』」を参照してください。

注：[Upper Critical (上位臨界)] 値と [Lower Critical (下位臨界)] 値は、Dominion PX で、動作環境が臨界状態であり、かつ許容可能なしきい値の範囲外であると見なされる点です。

9. [OK] をクリックして変更を保存します。
10. さらに環境センサーを設定するには、手順 3 ～ 9 を繰り返します。

Z 座標形式の設定

ラック ユニットの番号またはわかりやすいテキストを使用して、環境センサーの垂直位置 (Z 座標) を記述できます。

▶ Z 座標形式を決定するには、次の手順に従います。

1. PDU フォルダをクリックします。

注：PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「**Naming the PDU (PDU のネーミング)**『90p. の PDU の名前付け参照先』」を参照してください。

2. [設定] セクションの [Setup (セットアップ)] をクリックします。[Pdu Setup (PDU のセットアップ)] ダイアログ ボックスが開きます。
3. [External sensors Z coordinate format (外部センサーの Z 座標形式)] フィールドのドロップダウン矢印をクリックし、リストからオプションを選択します。
 - [Rack Units (ラック ユニット)]: Z 座標の高さが、標準のラック ユニットで表されます。これを選択すると、ラック ユニットの数値を入力して、環境センサーの Z 座標を表すことができます。
 - [Free-Form (自由形式)]: Z 座標の指定に、任意の英数字を使用できます。
4. [OK] をクリックして変更を保存します。

センサーの場所の記述

X、Y、Z の座標を使用して、各センサーの物理的な場所を示します。このような場所の値を使用することで、IT 機器周辺の一定の場所における環境条件の記録を追跡できます。X、Y、Z の値は、追加属性として扱われるもので、特定の単位に限定されてはいません。必要に応じて、定量的でない値を使用することもできます。たとえば、

X = 茶色のキャビネットの並び

Y = 3 番目のラック

Z = キャビネットの最上段

X、Y、Z の座標には、次のような値を使用することができます。

- X と Y: 英数字の組み合わせ。座標値として設定できる文字数は 0 ～ 32 文字です。
- Z 座標の形式を [Rack Units (ラック ユニット)] に設定した場合、Z に設定できる数値の範囲は 0 ～ 60 です。
- Z 座標の形式を [Free-Form (自由形式)] に設定した場合、Z に設定できる英数字の文字数は 0 ～ 32 文字です。

ヒント: これらの座標の値を SNMP 経由で設定および取得するには、*Dominion PX* の MIB を参照してください。コマンド ライン インタフェースを利用してこれらの値の設定や取得を行うには、「**コマンド ライン インタフェースの使用** [274p.]」を参照してください。

センサー データの表示

環境センサーが正常に接続され、管理対象になると、環境センサーの測定値が Web インタフェースに表示されます。

ダッシュボード ページには、管理対象の環境センサーの情報のみが表示されますが、外部センサー ページには、管理対象のセンサーと管理対象から除外されたセンサーの両方の情報が表示されます。

センサーの表示値の行が色付きで表示されている場合は、センサーの表示値がすでにいずれかのしきい値を超えているか、サーキット ブレーカーがトリップしています。詳細については、「*The Yellow- or Red-Highlighted Reading (表示値の黄色表示または赤色表示)*」『82p. の「測定値の黄色表示または赤色表示」参照』を参照してください。

▶ 管理対象の環境センサーのみを表示するには、次の手順に従います。

1. Dominion PX Explorer ペインで [ダッシュボード] アイコンをクリックすると、右側のペインに [ダッシュボード] ページが表示されます。
2. ダッシュボード ページで外部センサーのセクションを探します。このセクションには、以下の情報が表示されます。
 - 管理対象のセンサーの合計数
 - 管理対象から除外されているセンサーの合計数
 - 以下を始めとする、管理対象の各センサーの情報
 - 名前
 - 測定値
 - 状態

▶ 管理対象のセンサーと管理対象から除外されたセンサーの両方の情報を表示するには、次の手順に従います。

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*」『76p. の「ツリーの展開」参照』を参照してください。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「*Naming the PDU (PDU のネーミング)*」『90p. の「PDU の名前付け」参照先』を参照してください。

2. Dominion PX Explorer ペインで [External Sensors (外部センサー)] をクリックすると、右側のペインに [External Sensors (外部センサー)] ページが表示されます。

以下を始めとする、接続された各センサーの詳細情報が表示されます。

- ラベル (番号)

- シリアル番号
- センサー タイプ
- 名前
- 測定値
- 状態
- チャンネル (接点閉鎖センサーの場合のみ)

センサーの測定精度

Raritan の環境センサーの工場出荷時の仕様は、次のとおりです。環境センサーの調整は必要ありません。

- Temperature (温度): +/-2%
- 湿度: +/-5%
- 空気差圧: +/-1.5%
- 空気圧: +/-6.5%

管理対象センサーの状態

環境センサーは、管理対象となった後に状態を表示します。

センサーの状態は、センサーのタイプ (数値またはディスクリート) によって異なります。たとえば、接点閉鎖センサーはディスクリート センサーなので、unavailable (使用不可能)、alarmed (アラーム)、normal (正常) の 3 つの状態でのみ切り替わります。

注: 数値センサーでは、環境条件や内部条件が数値で示され、ディスクリート (オン/オフ) センサーでは、状態が英字で示されます。

センサーの状態	対象
unavailable (使用不可能)	すべてのセンサー
alarmed (アラーム)	ディスクリート センサー
normal (正常)	すべてのセンサー
below lower critical (下位臨界未満)	数値センサー
below lower warning (下位警告未満)	数値センサー
above upper warning (上位警告以上)	数値センサー
above upper critical (上位臨界以上)	数値センサー

「使用不可能」状態

unavailable (使用不可能) 状態は、センサーの接続が失われたことを意味します。

Dominion PX は秒単位の定期的な間隔で管理対象のすべてのセンサーに対して ping を実行します。特定のセンサーがスキャンで 3 回連続検出されなかった場合、そのセンサーの状態として「*unavailable* (使用不可能)」が表示されます。

接点閉鎖センサーのプロセッサとの通信が失われた場合、同じセンサーモジュールに接続されていたすべての検出装置 (つまりすべてのスイッチ) にも「*unavailable* (使用不可能)」状態が表示されます。

注: センサーが使用不可能と見なされても、既存のセンサー設定は変更されません。たとえば、そのセンサーに割り当てられている ID 番号はそれに関連付けられたままになります。

Dominion PX では、使用不可能のセンサーに対して ping の実行が続けられ、スキャンでそのセンサーを 2 回連続で検出できたら、*unavailable* (使用不可能) 状態が変更されます。

「normal (正常)」状態

この状態は、センサーが正常状態であることを示します。

接点閉鎖センサーの場合、この状態は、ユーザが設定した正常状態です。

- 正常状態が Normally Closed (ノーマル クローズ) に設定されている場合、*normal* (正常) 状態は接点閉鎖スイッチが閉じていることを意味します。
- 正常状態が Normally Open (ノーマル オープン) に設定されている場合、*normal* (正常) 状態は接点閉鎖スイッチが開いていることを意味します。

注: 正常状態の設定については、「**接点閉鎖センサーの設定** [40p.]」を参照してください。

数値センサーの場合、この状態は、センサー測定値が次に示す許容可能な範囲内であることを意味します。

下位警告しきい値 $\leq$ 測定値 $<$ 上位警告しきい値

注: 記号 $\leq$ は「より小さい」 ($<$) または「等しい」 ($=$) を意味します。

「alarmed (アラーム)」状態

この状態は、ディスクリート（オン/オフ）センサーが「異常」状態であることを意味します。

接点閉鎖センサーの場合、この状態の意味は、センサーの正常状態の設定によって異なります。

- 正常状態が Normally Closed（ノーマル クローズ）に設定されている場合、アラーム 状態は接点閉鎖スイッチが開いていることを意味します。
- 正常状態が Normally Open（ノーマル オープン）に設定されている場合、アラーム 状態は接点閉鎖スイッチが閉じていることを意味します。

注: 正常状態の設定については、**「接点閉鎖センサーの設定」** [40p.] を参照してください。

ヒント: 接点閉鎖センサーの LED は、アラーム状態になった後に点灯します。センサー モジュールに、2 つのスイッチの接続用にチャンネルが 2 つある場合は、2 つの LED を使用できます。LED のチャンネル番号で、どちらの接点閉鎖スイッチが「異常」状態になっているのかを確認します。

「below lower critical (下位臨界未満)」状態

この状態は、数値センサーの測定値が、次に示す下位臨界しきい値を下回っていることを意味します。

測定値 < 下位臨界しきい値

「below lower warning (下位警告未満)」状態

この状態は、数値センサーの測定値が、次に示す下位警告しきい値を下回っていることを意味します。

下位臨界しきい値 <= 測定値 < 下位警告しきい値

注: 記号 <= は「より小さい」 (<) または「等しい」 (=) を意味します。

「above upper warning (上位警告以上)」状態

この状態は、数値センサーの測定値が、次に示す上位警告しきい値を上回っていることを意味します。

上位警告しきい値 <= 測定値 < 上位臨界しきい値

注: 記号 <= は「より小さい」 (<) または「等しい」 (=) を意味します。

「above upper critical (上位臨界以上)」状態

この状態は、数値センサーの測定値が、次に示す上位臨界しきい値を上回っていることを意味します。

上位臨界しきい値 <= 測定値

注: 記号 <= は「より小さい」 (<) または「等しい」 (=) を意味します。

環境センサーを管理対象から除外

特定の環境要因を監視する必要がない場合は、対応する環境センサーを管理対象から除外するか解放して、Dominion PX デバイスでのセンサーの測定値や状態の取得を停止できます。

▶ 管理対象のセンサーを解放するには、次の手順に従います。

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*」『76p. の“ツリーの展開”参照』」を参照してください。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「*Naming the PDU (PDU のネーミング)*」『90p. の“PDU の名前付け”参照先』」を参照してください。

2. Dominion PX Explorer ペインで [External Sensors (外部センサー)] をクリックすると、右側のペインに [External Sensors (外部センサー)] ページが表示されます。
3. [External Sensors (外部センサー)] ページで管理対象から除外するセンサーをクリックします。
4. [Release (除外)] をクリックします。

センサーが管理対象から除外されると、そのセンサーに割り当てられていた ID 番号が解放され、新たに検出されたセンサーに自動的に割り当てることができます。

資産管理

資産管理設定は、資産センサーが Dominion PX デバイスに物理的に接続されている場合にのみ設定します。

注: 資産管理システムを設定するには、「*資産管理センサーの接続 (オプション)*」『42p. 』」を参照してください。

資産センサーの設定

Dominion PX では、接続されている資産センサーでサポートされるラック ユニット (タグ ポート) の台数を検出できないため、この情報を手動で入力する必要があります。

さらに、Web インタフェースで、資産センサーに名前を付けるか、またはすべてのラック ユニットのナンバリング方法を決定できます。

▶ **資産センサー (資産ストリップ) を設定するには、次の手順に従います。**

1. Feature Port (拡張ポート) フォルダが展開されていない場合は展開して、その下のデバイスを表示します。「ツリーの展開 [76p.]」を参照してください。
2. 左側のペインで資産センサーをクリックします。その資産センサーのページが右側のペインに表示されます。

注: 資産センサーにはデフォルトで「Asset Strip 1 (資産センサー 1)」という名前が付けられます。この名前は、カスタマイズすると変更されます。

ヒント: 同じ資産センサーのページは、左側のペインで [Feature Port (拡張ポート)] をクリックし、右側のペインで資産センサーをダブルクリックして開くこともできます。

3. [Setup (設定)] をクリックします。資産センサーの設定ダイアログ ボックスが表示されます。

ヒント: 同じダイアログ ボックスは、左側のペインで [Asset Management (資産管理)] をクリックし、[Asset Strip Setup (資産ストリップの設定)] をクリックするか、右側のペインで資産センサーをダブルクリックして開くこともできます。

4. 資産センサーの名前を変更するには、[Name (名前)] フィールドに新しい名前を入力します。
5. 選択した資産センサーのラック ユニットの合計台数を [Number of Rack Units (ラック ユニット数)] フィールドに入力します。このフィールドのデフォルト設定は 48 です。
6. [Numbering Mode (ナンバリング モード)] でオプションを選択して、資産センサーのすべてのラック ユニットの番号を振る方法を指定します。
 - [Top-Down (最上位から最下位へ)]: ラック ユニットには、最下位のラック ユニットから最上位のラック ユニットへ昇順に番号が振られます。

- [Bottom-Up (最下位から最上位へ)]: ラック ユニットには、最下位のラック ユニットから最上位のラック ユニットへ降順に番号が振られます。
- 7. [Numbering Offset (ナンバリング オフセット)] フィールドで、開始番号を選択します。たとえば、3 を選択すると、最初のラック ユニットに 3、2 番目のユニットに 4、3 番目のユニットに 5 のように最後まで番号が振られます。
- 8. [Orientation (向き)] フィールドで、資産センサーをラックに装着する方法を指定します。資産センサーの RJ-45 コネクタに最も近いラック ユニットは、Web インタフェースでインデックス番号 1 のマークが付けられます。

チルト センサーが組み込まれている最新バージョンの資産センサーでは、向きの設定を手動で行う必要はありません。Dominion PX デバイスは、資産センサーの向きを検出し、自動的に設定できます。

 - [Top Connector (上部コネクタ)]: 資産センサーを上部にある RJ-45 コネクタで装着することを示します。
- 9. [Bottom Connector (下部コネクタ)]: 資産センサーを下部にある RJ-45 コネクタで装着することを示します。[OK] をクリックして変更を保存します。

資産センサーの LED 色の設定

資産センサーの各 LED は、その色の変化によって、接続されている資産タグの有無を示します。次の手順に従って、接続されている資産センサーのすべての LED の色設定を指定または変更できます。

この機能には、管理権限を持つユーザのみがアクセスできます。

▶ **すべての LED の色を設定するには、次の手順に従います。**

1. まだ資産センサーを Dominion PX に接続していない場合は接続します。「*Dominion PX への資産センサーの接続*」『45p.』を参照してください。
2. ナビゲーション ツリーで [Feature Ports (拡張ポート)] フォルダをクリックして展開します。
3. 目的の資産センサーをクリックします。その資産センサー固有のページが右側のペインに表示され、資産センサーの設定とすべてのラックユニット (タグ ポート) の情報が表示されます。

注: ダッシュボード ページに表示されている資産センサーをダブルクリックする方法でもこのダイアログ ボックスを表示できます。

4. 資産センサーのページで [Setup (設定)] をクリックします。その資産センサーの設定ダイアログ ボックスが表示されます。

5. タグが接続されていることを示す LED 色を変更するには、カラーパレットで色をクリックするか、[Color with connected Tag (タグが接続されている場合の色)] フィールドで色の 16 進 RGB 値を入力します。
6. タグが接続されていないことを示す LED 色を変更するには、カラーパレットで色をクリックするか、[Color without connected Tag (タグが接続されていない場合の色)] フィールドで色の 16 進 RGB 値を入力します。
7. [OK] をクリックして変更を保存します。

ヒント: 特定の LED の色設定を他の LED と違う設定にするには、**特定のラック ユニットの設定** 『237p. 』を参照してください。

特定のラック ユニットの設定

Dominion PX の Web インタフェースでは、ラック ユニットは、資産センサーのタグ ポートを意味します。特定のラック ユニットに名前を付けることができます。また、その LED が同じ資産センサー上の他の LED とは異なる動作をするように、LED 色の設定を変更できます。

▶ 特定のラック ユニットを設定するには、次の手順に従います。

1. Feature Port (拡張ポート) フォルダが展開されていない場合は展開して、その下のデバイスを表示します。「**ツリーの展開** 『76p. 』」を参照してください。
2. 左側のペインで資産センサーをクリックします。その資産センサーのページが右側のペインに表示されます。

注: 資産センサーにはデフォルトで「Asset Strip 1 (資産センサー 1)」という名前が付けられます。この名前は、カスタマイズすると変更されます。

ヒント: 同じ資産センサーのページは、左側のペインで [Feature Port (拡張ポート)] をクリックし、右側のペインで資産センサーをダブルクリックして開くこともできます。

3. LED 設定を変更するラック ユニットを選択します。
4. [Configure Rack Unit (ラック ユニットの設定)] をクリックするか、選択したラック ユニットをダブルクリックします。選択したラック ユニットの設定ダイアログ ボックスが表示されます。
5. [Name (名前)] フィールドに、このラック ユニットを識別するための名前を入力します。
6. ラック ユニットの LED モードとして [Auto (自動)] または [Manual Override (手動上書き)] を選択します。

- [Auto (自動)] (タグに基づく): デフォルトではこの設定です。このオプションを選択すると、LED はグローバルな LED 色設定に従います。
- [Manual Override (手動上書き)]: この LED の動作を区別します。このオプションを選択した後で、選択したラック ユニットの LED モードや LED 色を選択する必要があります。
 - [LED Mode (LED モード)]: LED を点灯させるには [On (オン)] を、消灯させるには [Off (オフ)] を、ゆっくりと点滅させるには [Slow blinking (ゆっくり点滅)] を、速く点滅させるには [Fast blinking (速く点滅)] を選択します。
 - [LED Color (LED 色)]: [LED Mode (LED モード)] フィールドで [On (オン)]、[Slow blinking (ゆっくり点滅)]、または [Fast blinking (速く点滅)] を選択した場合は、カラー パレットで色をクリックするか、付随するテキスト ボックスに色の 16 進 RGB 値を入力して、LED 色を選択します。

7. [OK] をクリックして変更を保存します。

ブレード拡張ストリップの展開

資産センサーと同様に、ブレード拡張ストリップには複数のタグ ポートがあります。それを特定の資産センサーに接続すると、その資産センサーのページにフォルダとして表示されます。

注: ブレード拡張ストリップのタグ コネクタを一時的に取り外す必要がある場合は、1 秒以上経ってから接続し直してください。早すぎると、Dominion PX で検出されないことがあります。

▶ ブレード拡張ストリップ フォルダを展開するには、次の手順に従います。

1. 左側のペインで目的の資産センサーをクリックします。選択した資産センサーのページが右側のペインに表示されます。
2. ブレード拡張ストリップが接続されているラック ユニット (タグ ポート) を探します。

Rack Units					
	Rack Unit	Index	Slot	Name	Asset / ID
	1	1			
▷ 	2	2			00000007CACB
	3	3			
	4	4			

- ラック ユニットのダブルクリックするか、フォルダ アイコンの前の白い矢印 ▽ をクリックします。矢印が黒色の斜め矢印 ▲ に変わり、すべてのタグ ポートがフォルダの下に表示されます。

	Rack Unit	Index	Slot	Name	Asset / ID
	1	1			
▲ 	2	2			00000007CACB
			1		
			2		
			3		
			4		
			5		
			6		
			7		
			8		
			9		
			10		
			11		
			12		
			13		
			14		
			15		
			16		
	3	3			
	4	4			

- ▶ ブレード拡張ストリップを折りたたむには、次の手順に従います。
 - ブレード拡張ストリップ フォルダをダブルクリックするか、フォルダ アイコンの前の黒色の斜めの矢印 ▲ をクリックします。フォルダの下すべてのタグ ポートが非表示になります。

資産センサー情報の表示

接続されている資産センサーのハードウェアとソフトウェアの情報は、Web インタフェースに表示できます。

- ▶ 資産センサー情報を表示するには、次の手順に従います。
 - まだ資産センサーを Dominion PX に接続していない場合は接続します。「*Dominion PX への資産センサーの接続*」『45p.』を参照してください。
 - ナビゲーション ツリーで [Feature Ports (拡張ポート)] フォルダをクリックして展開します。
 - 目的の資産センサーをクリックします。その資産センサー固有のページが右側のペインに表示され、資産センサーの設定とすべてのラックユニット (タグ ポート) の情報が表示されます。

注: ダッシュボード ページに表示されている資産センサーをダブルクリックする方法でもこのダイアログ ボックスを表示できます。

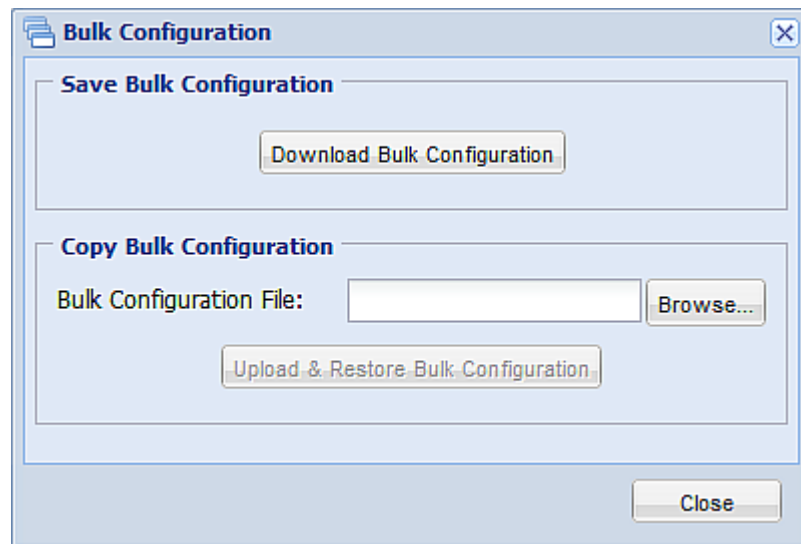
4. 資産センサー データが表示される [Extended Device Info (拡張デバイス情報)] タブをクリックします。
5. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

一括設定による設定のコピー

一括設定機能を使用すると、Dominion PX デバイスの設定を PC に保存できます。この設定ファイルを使用して、次の操作を実行できます。

- 設定を同じモデルおよびファームウェア バージョンの他の Dominion PX デバイスにコピーします。
- 同じ Dominion PX デバイスの設定を前の設定に戻します。

Dominion PX 設定を保存およびコピーするには、管理者の権限が必要です。



Dominion PX 設定の保存

ソース デバイスとは、設定ファイルの作成に使用された、設定済みの Dominion PX デバイスのことです。この設定ファイルに記述されている設定を、他の Dominion PX デバイスでも使用することができます。こうした設定には、ユーザおよび役割の設定、しきい値、イベント ルール、セキュリティ設定などがあります。

このファイルには、以下の項目を始めとする、デバイス固有の情報は保存されません。

- デバイス名
- システム名、システムの連絡先、システムの場所
- ネットワーク設定 (IP アドレス、ゲートウェイ、ネットマスクなど)
- デバイス ログ
- アウトレット (コンセント) 名
- アウトレット (コンセント) のステータス
- 環境センサーの名称
- 環境センサーの状態および値
- SSL 証明書

日付と時刻の設定は設定ファイルに保存されるため、ソース デバイスと異なるタイム ゾーンの Dominion PX デバイスに設定ファイルを配布する場合は、注意する必要があります。

▶ 設定ファイルを保存するには、以下の手順に従います。

1. [Maintenance (メンテナンス)] > [Bulk Configuration (一括設定)] を選択します。[Bulk Configuration (一括設定)] ダイアログ ボックスが表示されます。
2. [Download Bulk Configuration (一括設定のダウンロード)] をクリックします。
3. Web ブラウザで、設定ファイルを開くか保存するかを確認するメッセージが表示されたら、[Save (保存)] をクリックします。適切な場所を選択し、設定ファイルを PC に保存します。

設定ファイルは XML 形式で保存され、その内容は AES-128 暗号化アルゴリズムを使用して暗号化されます。

Dominion PX の設定のコピー

ターゲット デバイスとは、他の Dominion PX デバイスの設定ファイルをロードする Dominion PX デバイスのことです。

Dominion PX の設定をターゲット デバイスにコピーすると、その Dominion PX デバイスの設定が、Dominion PX ソース デバイスの設定に合わせて調整されます。Dominion PX の設定を正しくコピーするには、以下の条件を満たす必要があります。

- 管理者ユーザである必要があります。または、管理者の役割がユーザに割り当てられます。
- ターゲットの Dominion PX デバイスは、ソースの Dominion PX デバイスとモデル タイプが同じである必要があります。
- ターゲットの Dominion PX デバイスでは、ソースの Dominion PX デバイスと同じバージョンのファームウェアが実行されている必要があります。

▶ **Dominion PX の設定をコピーするには、次の手順に従います。**

1. ターゲット デバイスの Web インタフェースにログインします。
2. ターゲット デバイスのファームウェアのバージョンがソース デバイスのファームウェアと一致しない場合は、ターゲットのファームウェアを更新します。「**ファームウェアのアップグレード**『261p.』」を参照してください。
3. [Maintenance (メンテナンス)] > [Bulk Configuration (一括設定)] を選択します。[Bulk Configuration (一括設定)] ダイアログ ボックスが表示されます。
4. [Copy Bulk Configuration (一括設定のコピー)] セクションで、[Browse (参照)] をクリックし、PC に保存されている設定ファイルを選択します。
5. [Upload & Restore Bulk Configuration (一括設定のアップロードとリストア)] をクリックして、ファイルをコピーします。
6. 操作の確認を求めるメッセージが表示されます。[Yes (はい)] をクリックして、操作を確認します。
7. Dominion PX デバイスがリセットされ、ログイン ページが再度表示されることで、設定のコピーが完了したことがわかるまで待ちます。

測定単位の変更

デフォルトでは、Dominion PX の Web インタフェースに表示されるすべてのデータに次の測定単位が適用されます。

- 温度: 摂氏 (°C)
- 長さまたは高さ: メートル (m)

- 空気圧: パスカル (pa)

Dominion PX の Web インタフェースでは、ユーザ ログイン名に基づいてさまざまな測定単位を表示できます。つまり、個人設定に従って、ユーザごとに異なる測定単位を表示できます。各測定単位の他の単位は次のとおりです。

- 温度: 華氏 (°F)
- 長さまたは高さ: フィート (ft)
- 空気圧: psi

ユーザ プロファイルを作成するときに、目的の測定単位を指定します。「**ユーザ プロファイルの作成**『114p.』」を参照してください。測定単位設定を変更するには、管理者権限が必要です。

▶ **優先測定単位を設定するには、次の手順に従います。**

1. [User Management (ユーザ管理)] > [Users (ユーザ)] を選択します。
[Manage Users (ユーザの管理)] ダイアログ ボックスが表示されます。
2. ユーザをクリックして選択します。
3. [Edit (編集)] をクリックするか、ユーザをダブルクリックします。
[Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスが表示されます。XXX にはユーザ名が表示されます。
4. [Preferences (個人設定)] タブをクリックします。
5. 温度単位を変更するには、[Temperature Unit (温度単位)] フィールドで目的のオプションを選択します。
 - °C: 温度を摂氏で表示します。
 - °F: 温度を華氏で表示します。
6. 長さまたは高さの単位を変更するには、[Length Unit (長さ単位)] フィールドで目的のオプションを選択します。
 - [Meter (メートル)]: 長さまたは高さをメートルで表示します。
 - [Feet (フィート)]: 長さまたは高さをフィートで表示します。
7. 圧力単位を変更するには、[Pressure Unit (圧力単位)] フィールドで目的のオプションを選択します。
 - [Pascal (パスカル)]: 圧力をパスカル (Pa) で表示します。1 パスカルは、1 平方メートルあたりの 1 ニュートンに相当します。
 - [psi]: 圧力を psi で表示します。Psi は、1 平方インチあたりのポンドを表します。
8. [OK] をクリックして変更を保存します。

Web カメラの画像またはビデオの管理

Logicool® QuickCam® Pro 9000 Web カメラを Dominion PX デバイスに接続している場合は、Dominion PX の近く的环境を視覚的に監視できます。

「**Logicool Web カメラの接続 (オプション)** 『52p.』」を参照してください。

ツリーで Web カメラが選択されると、その Web カメラによってキャプチャされたスナップショットまたはビデオが Dominion PX Web インタフェースの右側のペインに表示されます。また、[Live Preview (ライブ プレビュー)] アイコン  をクリックすると、スナップショットおよびビデオを個別のブラウザ ウィンドウに表示できます。

Web インタフェースで、Web カメラで撮影したスナップショットを手動で保存できます。「**スナップショットの保存** 『249p.』」を参照してください。

Web カメラによってキャプチャされたビデオへのリンクは、電子メールまたはインスタント メッセージで送信できます。「**電子メールまたはインスタント メッセージでのスナップショットまたはビデオの送信** 『247p.』」を参照してください。

Web カメラによるスナップショットを含む電子メールをトリガするイベントを作成できます。「**アクションの作成** 『180p.』」を参照してください。

Web カメラの設定

Web カメラを設定するには、まず Dominion PX に接続する必要があります。「**Logicool Web カメラの接続 (オプション)** 『52p.』」を参照してください。

► Web カメラを設定するには、次の手順に従います。

1. ナビゲーション ツリーで、[Webcam Management (Web カメラ管理)] フォルダをクリックします。[Webcam Management (Web カメラ管理)] ページが表示されます。
2. 設定する Web カメラをクリックし、ページの左下の [Setup (設定)] をクリックします。[Webcam Setup (Web カメラの設定)] ページが表示されます。
3. Web カメラの名前を入力します。設定できる文字数は最大 64 文字です。
4. Web カメラの解像度を選択します。
5. Web カメラ モードを選択します。これは、Web カメラ設定後に必要に応じて変更できます。

- a. [Video (ビデオ)] – Web カメラはビデオ モードです。[Framerate (frames per second) (フレームレート (フレーム/秒))] の速度を設定します。
 - b. [Snapshot (スナップショット)] – Web カメラでキャプチャした画像を表示します。秒単位で測定される [Time Between Image(s) (画像の間隔)] の速度を設定します
6. [OK] をクリックします。これで、ナビゲーション ツリーで Web カメラをクリックしたときに Dominion PX で Web カメラの画像またはビデオを利用できるようになります。

► **Web カメラの設定を編集するには、次の手順に従います。**

1. ナビゲーション ツリーで、[Webcam Management (Web カメラ管理)] フォルダをクリックします。[Webcam Management (Web カメラ管理)] ページが表示されます。
2. 編集する Web カメラをダブルクリックします。新しいタブで Web カメラの画像またはビデオが開かれます。
3. [Setup (設定)] をクリックします。
4. 必要に応じて情報を編集します。解像度に対する変更は、既存の保存済みの画像には適用されません。適用対象は、解像度の変更後に撮影された画像およびビデオだけです。
5. [OK] をクリックします。

画像またはビデオのプロパティの調整

画像またはビデオのプロパティ (輝度、コントラスト、彩度、ゲインの設定などのプロパティ) がニーズを満たしていない場合は、それらを [Webcam Setup (Web カメラの設定)] ダイアログ ボックスで調整します。

► **画像またはビデオのプロパティを調整するには、次の手順に従います。**

1. [Webcam Management (Web カメラ管理)] ページまたはナビゲーション ツリーで Web カメラをクリックします。「**Web カメラの設定**」『**244p.**』を参照してください。
2. [Setup (設定)] をクリックします。[Webcam Setup (Web カメラの設定)] ダイアログ ボックスが表示されます。
3. [Controls (制御)] タブをクリックします。
4. 目的のプロパティをそれに対応するスライド バーで調整します。
5. [OK] をクリックして変更を保存します。

Web カメラの画像またはビデオの表示

Logicool® QuickCam® Pro 9000 Web カメラを Dominion PX デバイスに接続している場合は、Dominion PX の近くの環境を視覚的に監視できます。

「**Logicool Web カメラの接続 (オプション) 『52p.』**」を参照してください。

Dominion PX では、Web カメラでキャプチャした静止画像とライブ ビデオを切り替えることができます。

▶ スナップショットまたはビデオを表示するには、次の手順に従います。

1. 左側のペインで Web カメラをクリックします。

注: Web カメラ アイコンは、Logicool® QuickCam® Pro 9000 Web カメラが Dominion PX に接続されている場合にのみ表示されます。

「**Logicool Web カメラの接続 (オプション) 『52p.』**」を参照してください。

2. デフォルトで、Dominion PX はスナップショット モードになります。スナップショットが表示されるまで 1 分程度待ちます。スナップショット モードの場合は、画像の左上隅にスナップショット モード アイコン  が表示されます。Web カメラの場所は、画像の下 [Location (位置)] ペインに表示されます。

- 画像の解像度を変更するには、[Setup (設定)] をクリックします。[Resolution (解像度)] ドロップダウン リストからユーザ グループを選択します。解像度を変更すると、画像は、最新のスナップショットで更新されます。
- 画像のスナップショットを撮影するには、[Store Snapshot to Webcam Storage (スナップショットを Web カメラ ストレージに保存)] アイコン  をクリックします。「**スナップショットの保存 『249p.』**」を参照してください。

現在のモードがビデオの場合に、スナップショット モードに戻るには、次の手順に従います。

- a. [Setup (設定)] をクリックします。
 - b. [Webcam Mode (Web カメラ モード)] フィールドで、[Snapshot (スナップショット)] を選択します。
3. ビデオ モードに切り替えるには、次の手順に従います。
 - a. [Setup (設定)] をクリックします。
 - b. [Webcam Mode (Web カメラ モード)] フィールドで、[Video (ビデオ)] を選択します。

ビデオ モードの場合は、画像の左上隅にビデオ モード アイコン  が表示されます。

- ビデオの解像度を変更するには、[Setup (設定)] をクリックし、[Resolution (解像度)] ドロップダウンリストから別の解像度を選択します。

電子メールまたはインスタント メッセージでのスナップショットまたはビデオの送信

2 人までの受信者に、Dominion PX に接続されている Web カメラへのリンクを電子メールまたはインスタント メッセージで送信できます。受信したユーザは、リンクをクリックして、スナップショットまたはビデオを表示できます。

注: 電子メールまたはインスタントメッセージのリンクを介してアクセスするなどのリモート ライブ プレビュー セッションの場合、一度に合計 3 つまでの同時ライブ プレビュー セッションがサポートされています。Dominion PX インタフェースの発信者からのセッションが 1 つと、リモート セッションが 2 つまでです。

注: このトピックでは、メッセージの送信者をユーザ A、受信者をユーザ B とします。

受信者は、次のいずれかである限り、リンクを介してスナップショットまたはビデオ画像にアクセスできます。

- ユーザ A の Dominion PX インタフェースでスナップショットまたはビデオがライブ プレビュー モードで開かれており、ユーザ A がインタフェースからログアウトしておらず、セッションがタイムアウトしていない。
または

- スナップショットまたはビデオがユーザ A の Dominion PX インタフェースのセカンダリ [Live Preview (ライブ プレビュー)] ウィンドウで開かれている。ユーザ A のインタフェースでセカンダリ [Live Preview (ライブ プレビュー)] ウィンドウが開かれている限り、ユーザ A が Dominion PX インタフェースからログアウトしたりセッションがタイムアウトしたりした後でも、リンクを利用できます。

ベスト プラクティス

ベスト プラクティスとして、ユーザ A は、Dominion PX インタフェースでのセカンダリ [Live Preview (ライブ プレビュー)] ウィンドウでスナップショットまたはビデオを開き、少なくともユーザ B がリンク経由でそのスナップショットまたはビデオを開くまで、[Live Preview (ライブ プレビュー)] ウィンドウを開いたままにしておく必要があります。

ユーザ B がリンク経由でスナップショットまたはビデオを開いたら、ユーザ A の Dominion PX インタフェースのセカンダリ [Live Preview (ライブ プレビュー)] モード ウィンドウを閉じることができます。

ユーザ B は、リンクを開いたことをユーザ A に手動で通知できます。または、ユーザ A 側で、[Maintenance (メンテナンス)] > [Connected Users (接続中のユーザ)] を選択して、ユーザ B が現在アプリケーションに接続しているかどうかを確認することもできます。

▶ 電子メールまたはインスタント メッセージでスナップショットまたはビデオのリンクを送信するには、次の手順に従います。

1. ナビゲーション ツリーで、電子メールでリンクを配布するスナップショットまたはビデオをキャプチャしている Web カメラをクリックします。スナップショットまたはビデオが右側のペインにライブ プレビュー モードで表示されます。
2. スナップショットまたはビデオの上にある [Live Preview (ライブ プレビュー)] アイコン  をクリックします。スナップショットまたはビデオがセカンダリ [Live Preview (ライブ プレビュー)] ウィンドウで開かれます。
3. [Live Preview (ライブ プレビュー)] ウィンドウから URL をコピーし、電子メールまたはインスタント メッセージ アプリケーションに貼り付けます。少なくとも受信者がスナップショットまたはビデオをリンク経由で開くまで、[Live Preview (ライブ プレビュー)] ウィンドウは開いたままにしておきます。

スナップショット ストレージ

Dominion PX では、選択したスナップショットの履歴を保存できるようになっています。保存されるすべてのスナップショットは、Dominion PX にファイル名、ファイル サイズ、保存日時が表示された JPEG 形式のファイルとして保存されます。

警告: 保存されたスナップショットは Dominion PX をリセットすると失われるので、リセットを実行する前にスナップショットの履歴をクリアしてもよいかを確認してください。

スナップショットの保存

表示中の Web カメラのスナップショットを保存する場合は、手動で Dominion PX に保存できます。

警告: 保存されたスナップショットは Dominion PX をリセットすると失われるので、リセットを実行する前にスナップショットの履歴をクリアしてもよいかを確認してください。

▶ 現在のスナップショットを保存するには、次の手順に従います。

1. ツリーの Web カメラ アイコンをクリックするか、[Webcam Management (Web カメラ管理)] ページにリストされている Web カメラをダブルクリックして、[Webcam (Web カメラ)] ページを開きます。

2. スナップショットの上の [Save (保存)] アイコン  をクリックします。表示中のスナップショットがすぐに JPEG 形式のファイルに保存され、[Snapshots (スナップショット)] アイコンに格納されます。

注: 現在のモードがビデオ モードの場合は、[Save (保存)] アイコンは使用できません。『Web カメラの画像またはビデオの表示 246p. 』を参照してください。

3. ツリーの [Snapshots (スナップショット)] アイコンをクリックして、選択したスナップショットが保存され、[Snapshots (スナップショット)] ページに表示されることを確認します。

スナップショット履歴の管理

保存したすべてのスナップショットは、[Snapshots (スナップショット)] ページにリストされ、表示されます。

[Snapshots (スナップショット)] ページは、[Storage (ストレージ)]、[Snapshot (スナップショット)]、[Details (詳細)] の 3 つのペインに分かれています。[Storage (ストレージ)] ペインの上部には、ストレージの概要情報として、スナップショットの合計数 ([Used (使用済み)]) とストレージに格納できるスナップショットの最大数 ([Size (サイズ)]) が表示されます。

▶ スナップショット履歴を管理するには、次の手順に従います。

1. 任意のスナップショットを表示するには、[Storage (ストレージ)] ペインのリストでそれをクリックします。選択したスナップショット画像が、[Snapshot (スナップショット)] ペインに表示されます。
2. [Storage (ストレージ)] リストの並べ替え順序または表示列を変更するには、「**リストの表示の変更** 『83p. 』」を参照してください。
3. 1 つまたは複数のスナップショットをストレージから削除するには、それらに対応するチェックボックスをオンにして選択し、[Remove (削除)] アイコン  をクリックします。
 - リスト内のすべてのスナップショットを選択または選択解除するには、見出し行のチェックボックスをオンまたはオフにします。

ネットワーク診断

Dominion PX は、ネットワークの潜在的な問題を診断するための次のツールを Web インタフェース上に用意しています。

- Ping
- ルートの追跡
- TCP 接続の一覧表示

ヒント: これらのネットワーク診断ツールは、CLI でも使用できます。
「**ネットワークのトラブルシューティング** 『431p. 』」を参照してください。

ホストへの ping

Ping ツールは、ネットワークまたはインターネットを介してホストにアクセスできるかどうかを確認するのに役立ちます。

▶ **ホストに対して ping を実行するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [Network Diagnostics (ネットワーク診断)] > [Ping (Ping)] を選択します。[Ping Network Host (ネットワークホストへの ping)] ダイアログ ボックスが表示されます。
2. [Host Name (ホスト名)] フィールドに、確認するホストの名前または IP アドレスを入力します。
3. [Number of Requests (要求数)] フィールドで、最大 10 の数値を入力するか、どちらかの矢印をクリックして値を調整します。この数値によって、ホストへの ping のために送信されるパケットの数が決まります。
4. [Run Ping (ping の実行)] をクリックして、ホストへの ping を開始します。ダイアログ ボックスが表示され、ping の結果が表示されます。
5. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

ネットワーク ルートの追跡

ルートの追跡では、2 つのホストまたはシステム間のネットワークを介したルートを確認できます。

▶ **ホストのルートを追跡するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [Network Diagnostics (ネットワーク診断)] > [Trace Route (ルートの追跡)] を選択します。[Trace Route to Host (ホストへのルートの追跡)] ダイアログ ボックスが表示されます。
2. [Host Name (ホスト名)] フィールドに、ルートを確認するホストの IP アドレスまたは名前を入力します。
3. [Run (実行)] をクリックします。ダイアログ ボックスが表示され、ルート追跡の結果が表示されます。
4. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

TCP 接続の一覧表示

[List TCP Connections (TCP 接続の一覧表示)] を使用して、TCP 接続のリストを表示できます。

▶ **ホストのルートを追跡するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [Network Diagnostics (ネットワーク診断)] > [List TCP Connections (TCP 接続の一覧表示)] を選択します。
[TCP connections (TCP 接続)] ダイアログ ボックスが表示されます。
2. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

通信ログの表示

Dominion PX では、Dominion PX デバイスとグラフィカル ユーザ インタフェース (GUI) との間で行われたすべての通信を検査できます。通常、この情報が役に立つのはテクニカル サポート エンジニアのみであるため、表示する必要はありません。

この機能には、管理権限を持つユーザのみがアクセスできます。

▶ **通信ログを表示するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [View Communication Log (通信ログの表示)] を選択します。[Communication Log (通信ログ)] ダイアログ ボックスが表示されます。
2. このダイアログ ボックスには、デフォルトでは最後のページが表示されます。次の作業を行うことができます。
 - 別のページを表示するには、次のいずれかの操作を行います。
 - ◀ または ▶ をクリックすると、最初または最後のページに移動します。
 - ◀ または ▶ をクリックすると、前または次のページに移動します。
 - [Page (ページ)] テキスト ボックスに番号を入力して Enter キーを押すと、指定したページに移動します。
 - リストからログ エントリを選択して [Show Details (詳細の表示)] をクリックするか、ログ エントリをダブルクリックすると、詳細情報が表示されます。

注: ダイアログ ボックスが狭すぎる場合は、[Show Details (詳細の表示)] ボタンではなく、アイコン ▶▶ が表示されます。その場合は、▶▶ をクリックして [Show Details (詳細の表示)] を選択すると、詳細が表示されます。

3. 通信ログを即座に更新するには、 をクリックします。

4. 通信ログをコンピュータに保存するには、 をクリックします。
5. 必要に応じてダイアログ ボックスを拡大します。
6. リストの並べ替え、または表示列の変更を行うことができます。
7. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

診断情報のダウンロード

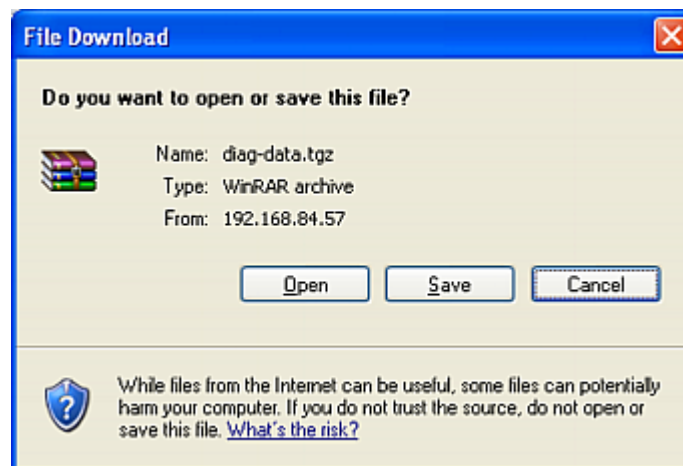
重要: この機能は、**Raritan** フィールド エンジニアが使用するための機能です。**Raritan** テクニカル サポートから指示された場合に限り、ユーザも使用できます。

診断ファイルを Dominion PX デバイスからクライアント マシンにダウンロードできます。このファイルは .tgz ファイルに圧縮され、解析のために Raritan テクニカル サポートに送信する必要があります。

この機能には、管理権限を持つユーザのみがアクセスできます。

▶ 診断ファイルを取得するには、次の手順に従います。

1. [Maintenance (メンテナンス)] > [Download Diagnostic Information (診断情報のダウンロード)] を選択します。[File Download (ファイルのダウンロード)] ダイアログ ボックスが表示されます。



2. [Save (保存)] をクリックします。[Save As (名前を付けて保存)] ダイアログ ボックスが表示されます。
3. 目的のディレクトリに移動し、[Save (保存)] をクリックします。
4. Raritan テクニカル サポートに指示された場合、このファイルを電子メールで送信します。

Schroff LHX ヒート エクスチェンジャの管理

Dominion PX では、Schroff® LHX-20 または LHX-40 ヒート エクスチェンジャが Dominion PX に接続されている場合に、その監視および管理ができます。

▶ **Dominion PX を使用して 1 台の LHX ヒート エクスチェンジャを監視するには、次の手順に従います。**

1. LHX-20 または LHX-40 ヒート エクスチェンジャを Dominion PX デバイスにまだ接続していない場合は、これらを物理的に接続します。
「*Schroff LHX ヒート エクスチェンジャの接続 (オプション) 『53p. 』*」を参照してください。
2. Dominion PX で LHX ヒート エクスチェンジャのサポートを有効にします。「*LHX のサポートの有効化 『254p. 』*」を参照してください。
3. 接続されたヒート エクスチェンジャを設定します。「*LHX デバイスの設定 『255p. 』*」を参照してください。
4. これで、接続された LHX ヒート エクスチェンジャを Dominion PX を介してリモートで監視および制御できるようになりました。
 - ヒート エクスチェンジャを監視するには、「*LHX デバイスの監視 『257p. 』*」を参照してください。
 - ヒート エクスチェンジャを制御するには、「*LHX デバイスの制御 『260p. 』*」を参照してください。

LHX のサポートの有効化

Dominion PX では、LHX ヒート エクスチェンジャのサポートがデフォルトでは無効になっているので、接続された LHX ヒート エクスチェンジャをリモートで監視または制御するには、LHX サポートを有効にする必要があります。

LHX サポートを有効または無効にするには、Dominion PX デバイスを再起動して変更を有効にする必要があります。

▶ **LHX サポートを有効または無効にするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Features (機能)] を選択し、[Schroff LHX Support (Schroff LHX サポート)] チェックボックスをオンまたはオフにします。
2. [Yes (はい)] をクリックして確認します。
3. Dominion PX が再起動されることを通知するメッセージが表示されます。[Continue (続行)] をクリックしてデバイスをリブートします。

4. カウントダウン タイマー ダイアログ ボックスが表示されます。
 Dominion PX のリブートが完了するまで待つと、ログイン ページにリダイレクトされます。数十秒経ってもログイン ページにリダイレクトされない場合は、ダイアログ ボックス内の「this link (このリンク)」をクリックしてください。

LHX デバイスの設定

Dominion PX の LHX サポートが有効になると、接続されている LHX デバイスが自動的に検出され、[Feature Port (拡張ポート)] フォルダの下に表示されます。ただし、拡張ポートが自動モード以外に設定されている場合を除きます。この場合は、拡張ポートのモードを変更して、Web インタフェースに LHX デバイスが正しく表示されるようにします。「**拡張ポートの設定**『107p.』」を参照してください。

これ以外にも、Dominion PX では、温度またはファンの速度のしきい値を設定して警告が通知されるようにしたり、LHX デバイスの名前をわかりやすくカスタマイズしたりできます。

LHX デバイスの正しい表示

Dominion PX で Web インタフェースに正しい LHX モデルを表示させる方法は 2 つあります。

- [Auto detection (自動検出)]: 拡張ポートのモードを [Auto (自動)] に設定して、デバイス タイプを自動検出させます。
- [Manual assignment (手動割り当て)]: Dominion PX に物理的に接続している LHX モデルに応じて、拡張ポートのモードを [LHX-20] または [LHX-40] に設定します。

拡張ポートのモードの変更方法については、「**拡張ポートの設定**『107p.』」を参照してください。

正しい LHX デバイス タイプの検出または割り当てが終わると、

[Feature Port (拡張ポート)] フォルダの下に [LHX] アイコン  が表示されます。

デバイスの状態が変わると、そのアイコンの画像も変わります。詳細については、「**デバイスの状態とアイコンの変化**『260p.』」を参照してください。

LHX デバイスの名前付け

Dominion PX Web インタフェースで LHX ヒート エクスチェンジャを識別しやすくするには、名前を割り当てます。カスタマイズした LHX ヒート エクスチェンジャの名前の後に、括弧で囲まれた拡張ポート番号が続きます。

▶ ヒート エクスチェンジャに名前を付けるには、次の手順に従います。

1. Feature Port (拡張ポート) フォルダが展開されていない場合は展開して、その下のデバイスを表示します。「ツリーの展開『76p.』」を参照してください。
2. Dominion PX Explorer ペインで LHX ヒート エクスチェンジャをクリックします。そのデバイスに固有のページが右側のペインに表示されます。
3. [Settings (設定)] セクションで [Setup (設定)] をクリックします。設定ダイアログ ボックスが表示されます。
4. [Name (名前)] フィールドにヒート エクスチェンジャの名前を入力します。
5. [OK] をクリックして変更を保存します。

温度およびファンのしきい値の設定

LHX ヒート エクスチェンジャには、気温、水温、およびファンの速度を検出するためのさまざまなセンサーが搭載されています。いずれかのセンサーの測定値が臨界状態に近づいた場合に Dominion PX が警告を通知するように、これらのセンサーのしきい値を設定できます。これらの設定は、ヒート エクスチェンジャが接続されている Dominion PX ポートに保存され、そのヒート エクスチェンジャが別のポートに移動されると失われます。

▶ センサーのしきい値を設定するには、次の手順に従います。

1. まだ LHX ヒート エクスチェンジャを Dominion PX に接続していない場合は接続します。
2. Feature Port (拡張ポート) フォルダが展開されていない場合は展開して、その下のデバイスを表示します。「ツリーの展開『76p.』」を参照してください。
3. Dominion PX Explorer ペインで LHX ヒート エクスチェンジャをクリックします。そのデバイスに固有のページが右側のペインに表示されます。

4. [Sensors (センサー)] の表で目的のセンサーを選択し、[Setup Thresholds (設定しきい値)] をクリックするか、単にそのセンサーをダブルクリックします。選択したセンサーの設定ダイアログ ボックスが表示されます。
5. しきい値およびアサート停止ヒステリシスの設定を調整します。
[Upper Critical (上位臨界)] 値と [Lower Critical (下位臨界)] 値は、Dominion PX で、動作環境が臨界状態であり、かつ許容可能なしきい値の範囲外であると見なされる点です。
 - しきい値を有効にするには、対応するチェックボックスをオンにします。しきい値を無効にするには、[enabled (有効)] チェックボックスをオフにします。
 - しきい値を有効にしてから、付随するテキスト ボックスに適切な数値を入力します。
 - すべてのしきい値のアサート停止ヒステリシスを有効にするには、[Deassertion Hysteresis (アサート停止ヒステリシス)] フィールドにゼロ以外の数値を入力します。「アサート停止ヒステリシスとは『177p. 』」を参照してください。
6. [OK] をクリックして変更を保存します。

LHX デバイスの監視

Dominion PX Web インタフェースでは、接続した LHX ヒート エクスチェンジャと LHX 組み込みセンサーのステータスを監視できます。

概要の表示

ダッシュボード ページと [Feature Port (拡張ポート)] ページの両方に、接続した LHX ヒート エクスチェンジャの概要 (ヒート エクスチェンジャの名前とステータス、および LHX デバイスが検出されたものか機能ポートに手動で割り当てられたものか) が表示されます。

概要内で LHX ヒート エクスチェンジャが赤色で表示されている場合は、そのヒート エクスチェンジャで LHX センサーの障害が発生していることを示します。障害があるセンサーを特定するには、[State (状態)] 列を表示します。

▶ ダッシュボード ページに LHX の概要を表示するには、次の手順に従います。

1. Dominion PX Explorer ペインで [Dashboard (ダッシュボード)] アイコンをクリックします。ダッシュボード ページが右側のペインに表示されます。
2. [LHX Heat Exchanger (LHX ヒート エクスチェンジャ)] セクションを探します。

▶ **[Feature Port (拡張ポート)] ページに LHX の概要を表示するには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。詳細については、「*Expanding the Tree (ツリーの展開)*」『76p. の「ツリーの展開」参照』」を参照してください。

注: PDU フォルダは、デフォルトでは「my PX」という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。詳細については、「*Naming the PDU (PDU のネーミング)*」『90p. の「PDU の名前付け」参照先』」を参照してください。

2. [Feature Port (拡張ポート)] フォルダをクリックします。[Feature Port (拡張ポート)] ページが右側のペインに表示され、接続されている LHX デバイス情報が表示されます。

詳細の表示

LHX ヒート エクスチェンジャのページには、以下を含む詳細情報が表示されます。

- デバイスの情報および設定
- 排気口の温度
- すべての LHX 組み込みセンサーの測定値および状態
- 累積稼働時間
- 障害のある LHX センサーまたは緊急冷却の有効化などのエラー

▶ **特定の LHX ヒート エクスチェンジャの詳細を表示するには、次の手順に従います。**

1. Feature Port (拡張ポート) フォルダが展開されていない場合は展開して、その下のデバイスを表示します。「*ツリーの展開*」『76p. 』」を参照してください。
2. 左側のペインで [LHX] アイコンをクリックします。[LHX] ページが右側のペインに表示されます。

ヒント: 同じ [LHX] ページは、左側のペインで [Feature Port (拡張ポート)] をクリックし、右側のペインで LHX をダブルクリックして開くこともできます。

いずれかの LHX センサーの測定値が臨界または警告しきい値以上になっている場合は、そのセンサーの測定値の行が赤色または黄色で表示されます。「*測定値の黄色表示または赤色表示*」『82p. 』」を参照してください。

アラート状態および LHX イベント ログ

LHX ヒート エクスチェンジャが Dominion PX デバイスに物理的に接続されている場合は、そのデバイスのページに [Alert States (アラート状態)] というラベルのセクションが表示されます。[Alert States (アラート状態)] セクションには、現在障害が発生している LHX センサーを特定する情報が表示されます。

ヒント: ダッシュボード ページと [Feature Port (拡張ポート)] ページでも、障害が発生しているセンサーが示されます。『LHX デバイスの監視 』257p. 』を参照してください。

[Alert States (アラート状態)] セクションには、[Show Event Log (イベントログの表示)] というラベルのボタンがあります。Dominion PX に関連付けられているイベントを表示するには、このボタンをクリックします。

稼働時間

稼働時間は、LHX ヒート エクスチェンジャが最初に Dominion PX デバイスに接続され、電源がオンになってからの累積時間です。

Dominion PX の Web インタフェースには、ヒート エクスチェンジャとそのファンの両方の稼働時間が表示されます。稼働時間の情報は、各ヒート エクスチェンジャのページの [Statistics (統計)] セクションに表示されます。

Statistics	
Operating Hours (Varistar LHX):	41 d 16 h
Operating Hours (Fan M1):	0 h
Operating Hours (Fan M2):	4 d 4 h
Operating Hours (Fan M3):	8 d 8 h
Operating Hours (Fan M4):	12 d 12 h
Operating Hours (Fan M5):	16 d 16 h
Operating Hours (Fan M6):	20 d 20 h
Operating Hours (Fan M7):	25 d

以下は、稼働時間で使用される時間単位です。

- h: 時
- d: 日

たとえば、「3d 5h」は合計稼働時間が 3 日と 5 時間であることを示します。

デバイスの状態とアイコンの変化

Dominion PX Web インタフェースでは、接続されている LHX ヒート エクスチェンジャのさまざまなステータスに合わせてアイコンが変更されます。

アイコン	デバイスのステータス
	ヒート エクスチェンジャの電源がオンで正常に動作しています。
	ヒート エクスチェンジャの電源がオフです。
	ヒート エクスチェンジャの電源はオンですが、いずれかの LHX センサーの障害により臨界状態になっています。
	少なくとも 1 つの LHX センサーの測定値が上位警告しきい値を上回っているか、下位警告しきい値を下回っています。
	FEATURE ポートで LHX デバイスが検出されていません。

臨界状態の原因を特定するには、以下のいずれかを表示します。

- ダッシュボード ページの [LHX Heat Exchanger (LHX ヒート エクスチェンジャ)] セクション。
- [Feature Port (拡張ポート)] ページ。

詳細については、「**概要の表示** 『257p. 』」を参照してください。

LHX デバイスの制御

Dominion PX では、接続されているヒート エクスチェンジャの電源をリモートでオン/オフできます。

▶ LHX ヒート エクスチェンジャを制御するには、次の手順に従います。

1. Feature Port (拡張ポート) フォルダが展開されていない場合は展開して、その下のデバイスを表示します。「**ツリーの展開** 『76p. 』」を参照してください。
2. Dominion PX Explorer ペインで LHX ヒート エクスチェンジャをクリックします。そのデバイスに固有のページが右側のペインに表示されます。
3. [Information (情報)] セクションを探します。
 - LHX ヒート エクスチェンジャの電源をオフにするには、[Switch Off (スイッチ オフ)] をクリックします。

- LHX ヒート エクスチェンジャの電源をオンにするには、[Switch On (スイッチ オン)] をクリックします。
- 4. 前の手順で [Switch Off (スイッチ オフ)] をクリックした場合、操作の確認を求めるダイアログ ボックスが表示されます。[Yes (はい)] をクリックして電源をオフにするか、[No (いいえ)] をクリックして操作を中止します。

電源をオンまたはオフにした後、Web インタフェースに表示されているヒート エクスチェンジャのアイコンが変更されます。「**デバイスの状態とアイコンの変化** 『260p. 』」を参照してください。

ファームウェアのアップグレード

Dominion PX デバイスをアップグレードすることで、最新の拡張、改善、および機能のメリットが得られます。

Dominion PX のファームウェア ファイルは、Raritan Web サイトの「**Firmware and Documentation (ファームウェアとドキュメント)**」『<http://www.raritan.com/support/firmware-and-documentation>/参照 』」セクションで入手できます。

Dominion PX ファームウェアの更新

Dominion PX デバイスのファームウェアを更新するには、システム管理者であるか、ファームウェアの更新権限を持つユーザ プロファイルでログインする必要があります。

ご使用のモデルに該当する場合は、Raritan の Web サイトから最新のファームウェア ファイルをダウンロードし、リリース ノートを読んでアップグレードを開始できます。アップグレードについてご質問またはご不明な点がある場合は、アップグレードを実行する前に Raritan テクニカル サポートにお問い合わせください。

警告: ワイヤレス接続を使用してファームウェアのアップグレードを行わないでください。

▶ ファームウェアを更新するには、次の手順に従います。

1. [Maintenance (メンテナンス)] > [Update Firmware (ファームウェアの更新)] を選択します。[Firmware Update (ファームウェアの更新)] ダイアログ ボックスが表示されます。
2. [Firmware File (ファームウェア ファイル)] フィールドで、[Browse (参照)] をクリックして、適切なファームウェア ファイルを選択します。
3. [Upload (アップロード)] をクリックします。アップロードの状態を示す進行状況バーが表示されます。

4. アップロードが完了すると、既存のファームウェアとアップロードされたファームウェアの両方のバージョン情報が表示され、続行すると更新処理を中止できなくなります。
5. アップロードされたファームウェアの証明書を表示するには、[View Certificate (証明書の表示)] をクリックします。これはオプションです。
6. 更新を続行するには、[Update Firmware (ファームウェアの更新)] をクリックします。更新処理には数分かかる場合があります。

警告: 更新中は *Dominion PX* の電源をオフにしないでください。

ファームウェアの更新中は、次のようになります。

- Web インタフェースで、更新の状況を示す進行状況バーが表示されます。
 - *Dominion PX* デバイスの 3 桁 LED 表示に「FUP」と表示されます。
 - ユーザは、*Dominion PX* に正常にログインできません。
 - Web インタフェースで、ログインしているすべてのユーザに *Dominion PX* のタイムアウト メッセージが表示され、ステータス バーに「切断」状態が示されます。
 - ユーザ管理の操作が行われている場合は、強制的に中断されます。
7. 更新が完了すると、更新が正常に終了したことを示すメッセージが表示されます。
 8. *Dominion PX* デバイスはリセットされ、ログイン ページが再び表示されます。これで、ログインして操作を再開できます。

注 1: ファームウェアの更新が完了すると、他のログイン ユーザもログアウトされます。

注 2: *Dominion PX* とともに **SNMP** マネージャを使用している場合は、ファームウェアを更新した後に *Dominion PX* の **MIB** をダウンロードし直す必要があります。これにより、使用している最新のリリースに対応した適切な **MIB** が **SNMP** マネージャで使用されるようになります。「**SNMP** の使用 『267p. 』」を参照してください。

ファームウェアのアップグレード時間についての注意事項

PDU ファームウェアのアップグレード時間は、外部および内部の各種要因によって、ユニットごとに異なります。

外部要因には、ネットワークのスループット、ファームウェアのファイル サイズ、ファームウェアを保存場所から取得する際の速度など、さまざまな要素があります。内部要因には、マイクロコントローラ上のファームウェアをアップグレードする必要性、およびアップグレードを必要とするマイクロコントローラの数（アウトレット（コンセント）の数に依存します）などがあります。マイクロコントローラは、必要な場合にのみアップグレードされます。そのため、ファームウェアのアップグレード時間は、約 3 分（マイクロコントローラの更新なし）～ 7 分（48 のアウトレット（コンセント）のマイクロコントローラをすべて更新）になります。PDU のファームウェアのアップグレード時間を見積もる場合は、上記の要因を考慮してください。

この注意事項に記載されている時間は、Web インタフェースベースのアップグレードに関するものです。他の管理システム（Raritan の Power IQ など）によってアップグレードする場合は、PDU では管理できない時間が加わる可能性があります。この注意事項では、他の管理システムを使用したアップグレードについては説明しません。

ファームウェア更新履歴の表示

ファームウェア アップグレード履歴（使用可能な場合）は、Dominion PX デバイスに永続的に保存されます。

この履歴は、ファームウェア アップグレード イベントが発生した日時、ファームウェア アップグレード イベントに関連付けられている前のバージョンと新しいバージョン、およびアップグレード結果を示します。

▶ ファームウェア更新履歴を表示するには、次の手順に従います。

1. [Maintenance（メンテナンス）] > [View Firmware Update History（ファームウェア更新履歴の表示）] を選択します。[Firmware Update History（ファームウェア更新履歴）] ダイアログ ボックスが表示され、次の情報が表示されます。
 - ファームウェア アップグレード イベントの日付と時刻
 - 前のファームウェアのバージョン
 - 更新ファームウェアのバージョン
 - ファームウェア アップグレードの結果
2. データを効率よく表示するために、リストの表示列の数または並べ替え順序を変更できます。「**リストの表示の変更**『83p.』」を参照してください。

3. ファームウェア アップグレード イベントの詳細を表示するには、イベントを選択して [Details (詳細)] をクリックするか、イベントをダブルクリックします。[Firmware Update Details (ファームウェア更新の詳細)] ダイアログ ボックスが表示され、選択したイベントの詳細情報が表示されます。
4. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

全面的な障害復旧

ファームウェアのアップグレードに失敗し、それによって Dominion PX デバイスが停止した場合は、専用のユーティリティを使用することで復旧させることができます。デバイスを Raritan に返送する必要はありません。

Windows XP/Vista/7 および Linux で動作する復旧用のユーティリティについては、Raritan テクニカル サポートにお問い合わせください。なお、復旧手順の実行には Dominion PX の適切なファームウェア ファイルが必要です。

資産センサーのファームウェアの更新

資産センサーを Dominion PX デバイ스에接続すると、それ自体のファームウェア バージョンが Dominion PX ファームウェアに保存されている資産センサーのファームウェア バージョンと自動的に照合されます。2 つのバージョンが異なる場合は、資産センサーによって Dominion PX デバイスからの新しいファームウェアのダウンロードが自動的に開始され、それ自体のファームウェアがアップグレードされます。

ファームウェアのアップグレード中に、次のイベントが発生します。

- 資産センサーが点灯し、点滅している LED の色が赤から緑色に変わります。
- ファームウェア アップグレード プロセスが Dominion PX の Web インタフェースに示されます。
- ファームウェア アップグレード イベントを示す SNMP トラップが送信されます。

ヘルプの使用

[Help (ヘルプ)] メニューからは、以下にアクセスできます。

- 現在のファームウェアおよびソフトウェア パッケージの情報
- Dominion PX ユーザ ガイド (オンライン ヘルプ) へのリンク

ソフトウェア パッケージの情報の取得

現在のファームウェアのバージョン、および Dominion PX デバイスに組み込まれているすべてのオープン ソース パッケージの情報を Web インタフェースを介して確認できます。

▶ 組み込みのソフトウェア パッケージの情報を取得するには、次の手順に従います。

1. [Help (ヘルプ)] > [About Dominion PX (バージョン情報)] を選択します。[About Dominion PX (バージョン情報)] ダイアログ ボックスが、オープン ソース パッケージの一覧とともに表示されます。
2. このダイアログ ボックス内のリンクをクリックすると、関連情報にアクセスしたり、ソフトウェア パッケージをダウンロードしたりすることができます。

オンライン ヘルプの参照

Dominion PX ユーザ ガイドは、オンライン ヘルプの形式で用意されており、インターネット経由で利用することもできます。

オンライン ヘルプを使用するには、ブラウザでアクティブ コンテンツを有効にする必要があります。Internet Explorer 7 を使用している場合、スクリプトレットを有効にする必要があります。これらの機能を有効にする方法については、ブラウザのヘルプを参照してください。

▶ Dominion PX オンライン ヘルプを使用するには、次の手順に従います。

1. [Help (ヘルプ)] > [User Guide (ユーザ ガイド)] を選択します。オンライン ヘルプは、デフォルトの Web ブラウザに表示されます。
2. トピックの内容を表示するには、左側のペインでトピックをクリックします。その内容が右側のペインに表示されます。
3. 別のトピックを選択するには、次のいずれかの操作を実行します。
 - 次のトピックを表示するには、ツールバーの [Next (次へ)] アイコン  をクリックします。
 - 前のトピックを表示するには、[Previous (前へ)] アイコン  をクリックします。
 - 最初のトピックを表示するには、[Home (ホーム)] アイコン  をクリックします。
4. サブトピックを含むトピックを展開するか折りたたむには、次の手順を実行します。
 - トピックを展開するには、トピックの前の白色の矢印  をクリックするか、トピックをダブルクリックします。矢印が黒色の斜め矢印  に変わり、トピックの下にサブトピックが表示されます。

- トピックを折りたたむには、トピックの前の黒色の斜め矢印 ▲ をクリックするか、展開されているトピックをダブルクリックします。矢印が白色の矢印 ▾ になり、そのトピックの下すべてのサブトピックが非表示になります。
5. 特定の情報を検索するには、[Search (検索)] テキスト ボックスにキーワードまたは文字列を入力し、Enter キーを押すか、[Search (検索)] アイコン  をクリックして検索を開始します。
 - 必要な場合は、[Match partial words (部分一致を含む)] チェックボックスをオンにして、[Search (検索)] テキスト ボックスに入力した単語の一部が一致する情報も含めます。

検索結果は、左側のペインに表示されます。

6. 左側のペインにトピックのリストを表示するには、下部の [Contents (目次)] タブをクリックします。
7. [Index (索引)] ページを表示するには、[Index (索引)] タブをクリックします。
8. 選択中のトピックへの URL リンクをだれかに電子メールで送信するには、ツールバーの [Email this page (このページを電子メール)] アイコン  をクリックします。
9. ユーザ ガイドに関するコメントまたは提案を Raritan に電子メールで送信するには、[Send feedback (フィードバックを送信)] アイコン  をクリックします。
10. 選択中のトピックを印刷するには、[Print this page (このページを印刷)] アイコン  をクリックします。

ここでは SNMP について説明し、SNMP マネージャとともに使用できるよう Dominion PX を設定するために役立つ情報を提供します。Dominion PX を設定することで、SNMP マネージャにトラップを送信できるだけでなく、ステータスの取得および基本設定を行うための GET コマンドと SET コマンドを受け取ることができます。

この章の内容

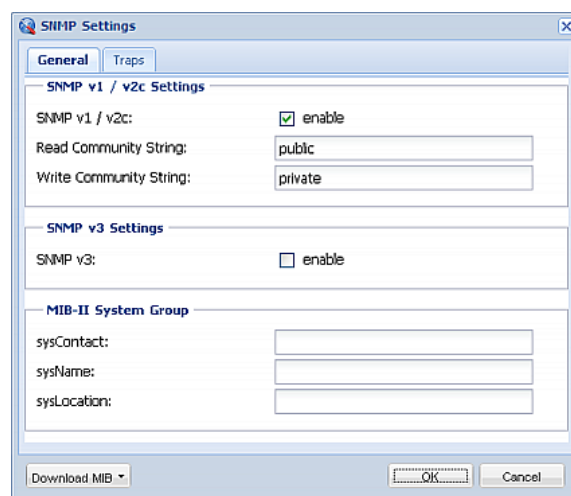
SNMP の有効化	267
暗号化された SNMP v3 のユーザの設定	268
SNMP トラップの設定	269
SNMP の GET と SET	270

SNMP の有効化

SNMP マネージャと通信するには、まず Dominion PX デバイスで SNMP エージェントを有効にする必要があります。

▶ SNMP を有効にするには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Network Services (ネットワークサービス)] > [SNMP] を選択します。[SNMP Settings (SNMP 設定)] ダイアログ ボックスが表示されます。



2. [SNMP v1 / v2c (SNMP v1 / v2c)] フィールドで [enable (有効にする)] チェックボックスをオンにして、SNMP v1 または v2c プロトコルを使用した SNMP マネージャとの通信を可能にします。

- SNMP 読み取り専用コミュニティ スtring を [Read Community String (コミュニティ String の読み取り)] フィールドに入力します。通常、String は「public」です。
 - 読み取り/書き込みコミュニティ String を [Write Community String (コミュニティ String の書き込み)] フィールドに入力します。通常、String は「private」です。
3. [SNMP v3 (SNMP v3)] フィールドで [enable (有効にする)] チェックボックスをオンにして、SNMP v3 プロトコルを使用した SNMP マネージャとの通信を可能にします。

ヒント: SNMP v3 プロトコルを使用した、ユーザによる *Dominion PX* へのアクセスを許可または拒否できます。「暗号化された SNMP v3 のユーザの設定」『268p. 』を参照してください。

4. SNMP MIB-II の sysContact 値を [sysContact] フィールドに入力します。
5. SNMP MIB-II の sysName 値を [sysName] フィールドに入力します。
6. SNMP MIB-II の sysLocation 値を [sysLocation] フィールドに入力します。
7. [OK] をクリックして変更を保存します。

重要: SNMP マネージャで、使用する *Dominion PX* の SNMP MIB をダウンロードする必要があります。このダイアログ ボックスで [Download MIB (MIB のダウンロード)] をクリックして、目的の MIB ファイルをダウンロードします。詳細については、「*SNMP MIB* のダウンロード」『270p. 』を参照してください。

暗号化された SNMP v3 のユーザの設定

SNMP v3 プロトコルを使用すると、暗号化された通信が可能になります。この機能を利用するには、ユーザに認証パス フレーズおよびプライバシー パス フレーズが必要です。これらのパス フレーズは、ユーザと *Dominion PX* の間の共有シークレットの役割を果たします。

▶ **SNMP v3 暗号化通信を使用できるようにユーザの設定を行うには、次の手順に従います。**

1. [User Management (ユーザ管理)] > [Users (ユーザ)] を選択します。
[Manage Users (ユーザの管理)] ダイアログ ボックスが表示されます。
2. ユーザをクリックして選択します。
3. [Edit (編集)] をクリックするか、ユーザをダブルクリックします。
[Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスが表示されます。XXX にはユーザ名が表示されます。

4. SNMPv3 のアクセス権限を変更するには、[SNMPv3] タブをクリックし、必要な変更を加えます。詳細については、「**ユーザ プロファイルの作成** 『114p.』」の手順 6 を参照してください。
5. [OK] をクリックして変更を保存します。これで、暗号化された SNMP v3 通信が設定されました。

SNMP トラップの設定

Dominion PX では、発生するイベントの内部ログが自動的に保持されます。「**イベント ルールの設定** 『179p.』」を参照してください。これらのイベントは、サード パーティのマネージャに SNMP トラップを送信するためにも使用できます。

▶ **SNMP トラップを送信するように Dominion PX を設定するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. [Rules (ルール)] タブで、[System SNMP Trap Rule (システム SNMP トラップ ルール)] を選択します。
3. このイベント ルールを有効にするには、[Enabled (有効)] チェックボックスをオンにします。
4. [Save (保存)] をクリックして変更を保存します。
5. SNMP トラップ アクションを設定していない場合は、[Actions (アクション)] タブをクリックします。
6. [System SNMP Trap Action (システム SNMP トラップ アクション)] を選択して、トラップの送信先を設定します。
7. [Host 1 (ホスト 1)] フィールドに IP アドレスを入力します。これは SNMP システム エージェントによりトラップが送信されるアドレスです。
8. [Port 1 (ポート 1)] フィールドに通信ポート番号を入力します。
9. SNMP コミュニティ名を [Community (コミュニティ)] フィールドに入力します。コミュニティとは、Dominion PX とすべての SNMP 管理ステーションを表すグループのことです。
10. SNMP トラップの送信先を複数指定するには、追加する送信先について手順 8 ～ 10 を実行します。送信先は 3 つまで指定できます。
11. [Save (保存)] をクリックして変更を保存します。
12. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

注: 新しい *Dominion PX* リリースに更新する場合は、SNMP マネージャで使用される MIB を更新する必要があります。これにより、使用しているリリースに適した MIB が SNMP マネージャで使用されるようになります。『SNMP MIB のダウンロード』『270p.』を参照してください。

SNMP の GET と SET

Dominion PX では、トラップを送信できるほか、サードパーティの SNMP マネージャから SNMP の GET 要求と SET 要求を受信できます。

- GET 要求は、Dominion PX に関する情報（システムの場所や、特定のアウトレット（コンセント）の電流など）の取得に使用されます。
- SET 要求は、情報のサブセット（SNMP システム名など）の設定に使用されます。

注: SNMP システム名は、*Dominion PX* のデバイス名です。SNMP システム名を変更すると、Web インタフェースで表示されるデバイス名も変更されます。

Dominion PX では、SNMP の SET 要求を使用した IPv6 関連のパラメータの設定はサポートされません。

これらの要求に対して有効なオブジェクトは、SNMP MIB-II システム グループと Dominion PX のカスタム MIB で見つかったオブジェクトに限られます。

Dominion PX MIB

SNMP MIB ファイルは、SNMP マネージャで Dominion PX デバイスを使用するために必要です。SNMP MIB ファイルには、SNMP 機能が記述されています。

SNMP MIB のダウンロード

Dominion PX の SNMP MIB ファイルは、Web インタフェースから容易にダウンロードできます。SNMP MIB ファイルのダウンロード方法には、次の 2 種類があります。

- ▶ **[SNMP Settings (SNMP 設定)] ダイアログ ボックスからファイルをダウンロードするには、次の手順に従います。**
1. [Device Settings (デバイス設定)] > [Network Services (ネットワーク サービス)] > [SNMP] を選択します。[SNMP Settings (SNMP 設定)] ダイアログ ボックスが表示されます。
 2. [Download MIB (MIB のダウンロード)] をクリックします。MIB ファイルのサブメニューが表示されます。
 3. ダウンロードする目的の MIB ファイルを選択します。

- PDU2-MIB: Dominion PX の電源管理用の SNMP MIB ファイル。
 - ASSETMANAGEMENT-MIB: 資産管理用の SNMP MIB ファイル。
4. [Save (保存)] をクリックして、コンピュータにファイルを保存します。

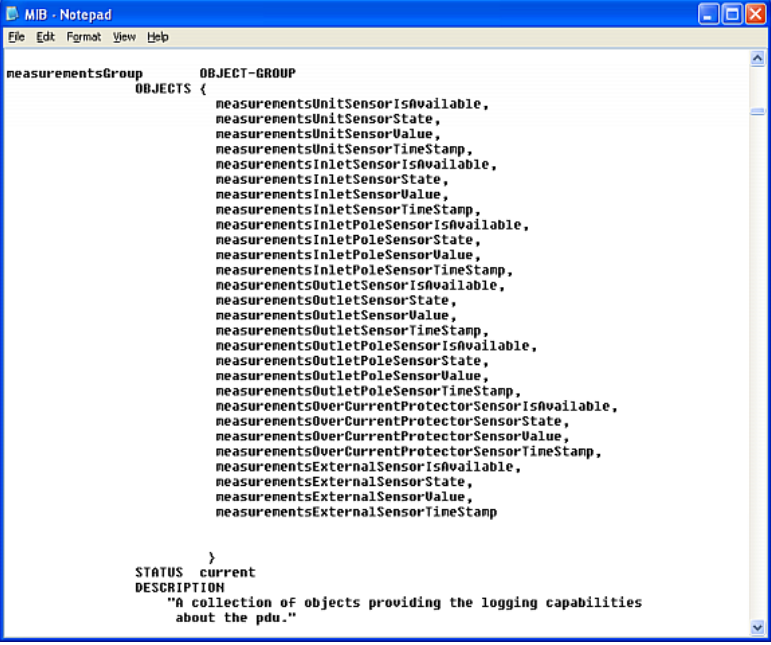
▶ **[Device Information (デバイス情報)] ダイアログ ボックスからファイルをダウンロードするには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [Device Information (デバイス情報)] を選択します。[Device Information (デバイス情報)] ダイアログ ボックスが表示されます。
2. [PDU2-MIB] または [ASSETMANAGEMENT-MIB] リンクをクリックして、目的の SNMP MIB ファイルをダウンロードします。
 - PDU2-MIB: Dominion PX の電源管理用の SNMP MIB ファイル。
 - ASSETMANAGEMENT-MIB: 資産管理用の SNMP MIB ファイル。「USB Console INF file (USB コンソール INF ファイル)」リンクからは、USB-to-serial ドライバをダウンロードできます。これは、設定のために PDU を USB ケーブルでコンピュータと接続している場合にのみ必要です。詳細については、「*USB-to-Serial ドライバのインストール* 『23p. 』」を参照してください。
3. [Save (保存)] をクリックして、コンピュータにファイルを保存します。

レイアウト

MIB を開くと、Dominion PX システムをユニット レベルと個々のアウトレット（コンセント）レベルで記述するカスタム オブジェクトが明らかになります。

標準的には、これらのオブジェクトはまずファイルの先頭に現れて、親グループの下に一覧表示されます。次に、オブジェクトは再度別個に現れて、詳細が定義および記述されます。



```

measurementsGroup      OBJECT-GROUP
                        OBJECTS {
                            measurementsUnitSensorIsAvailable,
                            measurementsUnitSensorState,
                            measurementsUnitSensorValue,
                            measurementsUnitSensorTimeStamp,
                            measurementsInletSensorIsAvailable,
                            measurementsInletSensorState,
                            measurementsInletSensorValue,
                            measurementsInletSensorTimeStamp,
                            measurementsInletPoleSensorIsAvailable,
                            measurementsInletPoleSensorState,
                            measurementsInletPoleSensorValue,
                            measurementsInletPoleSensorTimeStamp,
                            measurementsOutletSensorIsAvailable,
                            measurementsOutletSensorState,
                            measurementsOutletSensorValue,
                            measurementsOutletSensorTimeStamp,
                            measurementsOutletPoleSensorIsAvailable,
                            measurementsOutletPoleSensorState,
                            measurementsOutletPoleSensorValue,
                            measurementsOutletPoleSensorTimeStamp,
                            measurementsOverCurrentProtectorSensorIsAvailable,
                            measurementsOverCurrentProtectorSensorState,
                            measurementsOverCurrentProtectorSensorValue,
                            measurementsOverCurrentProtectorSensorTimeStamp,
                            measurementsExternalSensorIsAvailable,
                            measurementsExternalSensorState,
                            measurementsExternalSensorValue,
                            measurementsExternalSensorTimeStamp
                        }
                        STATUS current
                        DESCRIPTION
                            "A collection of objects providing the logging capabilities
                            about the pdu."

```

たとえば、measurementsGroup グループには、Dominion PX 全体のセンサー測定値のオブジェクトが含まれています。このグループの下に表示されるオブジェクトの 1 つである measurementsUnitSensorValue は、MIB の後半で「The sensor value (センサー値)」として記述されます。また、configGroup グループに含まれている pduRatedCurrent には、PDU の定格電流が記述されます。

SNMP の SET としきい値

一部のオブジェクトは、SNMP の set コマンドを使用して SNMP マネージャから設定できます。設定可能なオブジェクトには、MIB での MAX-ACCESS レベルの「読み書き」権限があります。

これらのオブジェクトには、しきい値オブジェクトが用意されており、特定のパラメータがしきい値を超えると、Dominion PX で警告の生成および SNMP トラップの送信が行われます。しきい値のしくみについては、「**電力しきい値の設定**『173p.』」を参照してください。

注: SNMP SET コマンドによってしきい値を設定する場合は、上位臨界しきい値が上位警告しきい値よりも大きいことを確認してください。

しきい値の有効化についての注意事項

SNMP 経由で以前に無効にしたしきい値を有効にする場合は、実際に有効にする前に、有効にするすべてのしきい値に必ず正しい値を設定してください。正しい値が設定されていない場合、エラー メッセージが表示されることがあります。

このセクションでは、コマンド ライン インタフェース (CLI) を使用して Dominion PX デバイスを管理する方法について説明します。

この章の内容

インタフェースについて	274
CLI へのログイン	275
ヘルプ コマンド	277
情報の表示	278
Dominion PX デバイスとネットワークの設定	297
負荷遮断設定コマンド	423
電源制御操作	425
ユーザのブロック解除	429
Dominion PX のリセット	430
ネットワークのトラブルシューティング	431
コマンドで使用できるパラメータの確認	435
前のコマンドの取得	435
コマンドの自動補完	435
CLI のログアウト	436

インタフェースについて

Dominion PX にはコマンド ライン インタフェースがあり、それを使用して、データ センターの管理者が基本的な管理タスクを実行できます。このインタフェースを使用すると、次の作業を実行できます。

- Dominion PX デバイスをリセットします。
- Dominion PX およびネットワーク情報 (デバイス名、ファームウェアのバージョン、IP アドレスなど) を表示する。
- Dominion PX およびネットワーク設定の設定を行う。
- ネットワークの問題のトラブルシューティングを行う。

このインタフェースには、ハイパーターミナルなどのターミナル エミュレーション プログラム、または PuTTY などの Telnet / SSH クライアントを使用して、シリアル接続でアクセスします。

注: Telenet アクセスは、公開通信であり、安全ではないため、デフォルトでは無効になっています。Telnet を有効にするには、「**ネットワーク サービス設定の変更** [97p.]」を参照してください。

CLI へのログイン

ローカル接続でハイパーターミナルを使用したログイン方法は、SSH や Telnet の場合とは少し異なります。

ハイパーターミナルの使用

コマンド ライン インタフェースにローカルにアクセスするための任意の端末エミュレーション プログラムを使用できます。

このセクションでは、Windows Vista より前の Windows オペレーティング システムに用意されているハイパーターミナルについて説明します。

▶ ハイパーターミナルでログインするには、次の手順に従います。

1. ローカル接続経由でコンピュータを Dominion PX デバイスに接続します。
2. コンピュータでハイパーターミナルを起動し、コンソール ウィンドウを開きます。最初のウィンドウには何も表示されません。

COM ポートが次の設定を使用していることを確認します。

- ビット/秒 = 115200 (115.2Kbps)
- データ ビット = 8
- ストップ ビット = 1
- パリティ = なし
- フロー制御 = なし

ヒント: USB 接続の場合、どの COM ポートが Dominion PX に割り当てられているかを調べるには、[コントロールパネル] > [システム] > [ハードウェア] > [デバイス マネージャ] を選択し、[ポート] グループの下で「Dominion Serial Console」を探します。

3. Enter キーを押します。[Username (ユーザ名)] プロンプトが表示されます。

Username: _

4. 名前を入力し、Enter キーを押します。名前では大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。次に、パスワードを入力するためのプロンプトが表示されます。

Username: admin
Password: _

5. パスワードを入力し、Enter キーを押します。パスワードでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

パスワードを正しく入力すると、# または > というシステム プロンプトが表示されます。詳細については、「**さまざまな CLI モードとプロンプト** 『277p. 』」を参照してください。

ヒント: 日時などの「**前回のログイン**」情報は、*Dominion PX Web* インタフェースまたは *CLI* へのログインに同じユーザ プロファイルを使用した場合にも表示されます。

- これでコマンド ライン インタフェースにログインして、*Dominion PX* デバイスの管理を開始できます。

SSH または Telnet の使用

SSH または Telnet クライアント (PuTTY など) を使用して、コマンド ライン インタフェースにリモートからログインできます。

注: *PuTTY* は、インターネットからダウンロード可能な無料のプログラムです。詳細な設定方法は、*PuTTY* のマニュアルを参照してください。

▶ **SSH または Telnet を使用してログインするには、次の手順に従います。**

- SSH または Telnet が有効になっていることを確認します。「**ネットワーク サービス設定の変更** 『97p. 』」を参照してください。
- SSH または Telnet クライアントを起動し、コンソール ウィンドウを開きます。ログイン プロンプトが表示されます。

```
login as: █
```

- 名前を入力し、Enter キーを押します。名前では大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

注: SSH クライアントを使用する場合、名前は 25 文字以下にする必要があります。そうでない場合、ログインは失敗します。

次に、パスワードを入力するためのプロンプトが表示されます。

```
login as: admin
admin@192.168.84.88's password: █
```

- パスワードを入力し、Enter キーを押します。パスワードでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。
- パスワードを正しく入力すると、# または > というシステム プロンプトが表示されます。詳細については、「**さまざまな CLI モードとプロンプト** 『277p. 』」を参照してください。

ヒント: 日時などの「前回のログイン」情報は、*Dominion PX Web* インタフェースまたは *CLI* へのログインに同じユーザ プロファイルを使用した場合にも表示されます。

- これでコマンド ライン インタフェースにログインして、*Dominion PX* デバイスの管理を開始できます。

さまざまな CLI モードとプロンプト

CLI のシステム プロンプトは、使用するログイン名やモードによって異なります。

- ユーザ モード: 通常ユーザとしてログインし、*Dominion PX* デバイスを設定するためのすべての権限が付与されていない場合は、`>` プロンプトが表示されます。
- 管理者モード: 管理者としてログインし、*Dominion PX* デバイスを設定するためのすべての権限が付与されている場合は、`#` プロンプトが表示されます。
- 設定モード: 設定モードには、管理者モードから移行できます。このモードでは、プロンプトが `config:#` になり、*Dominion PX* デバイスおよびネットワークの設定を変更できます。「[設定モードへの移行『297p.』](#)」を参照してください。
- 診断モード: 診断モードには、管理者モードから移行できます。このモードでは、プロンプトが `diag:>` になり、ネットワークトラブルシューティング コマンド (ping コマンドなど) を実行できます。「[診断モードへの移行『431p.』](#)」を参照してください。

シリアル接続の終了

シリアル接続を使用した *Dominion PX* デバイスへのアクセスを終了するには、ウィンドウまたは端末エミュレーション プログラムを閉じます。

複数の *Dominion PX* デバイスへのアクセスやアップグレードを行う場合は、シリアル接続ウィンドウを閉じる前に、シリアル ケーブルがあるデバイスから別のデバイスに移行しないようにしてください。

ヘルプ コマンド

ヘルプ コマンドでは、メインの CLI コマンドの一覧が表示されます。このコマンドは、コマンドに慣れていない場合に役立ちます。

- ▶ ヘルプ コマンドの構文は、次のとおりです。

```
# help
```

コマンドを入力した後に Enter キーを押すと、メインのコマンドの一覧が表示されます。

ヒント: 特定の CLI コマンドに使用可能なパラメータを確認するには、コマンドの末尾に疑問符 (?) を加えて実行します。「コマンドで使用できるパラメータの確認」『435p. 』を参照してください。

情報の表示

show コマンドを使用すると、IP アドレス、ネットワーク モード、ファームウェアのバージョン、サーキット ブレーカの状態、インレットの定格など、Dominion PX デバイスまたはその一部の、現在の設定や状態を表示できます。

一部の「show」コマンドには、パラメータ「details」を指定する形式と指定しない形式の 2 種類があります。この違いは、show コマンドにパラメータ「details」を指定しない場合には簡潔な情報が表示され、指定した場合には詳細な情報が表示されることです。

「show」コマンドを入力した後に、Enter キーを押して実行します。

注: ログイン名によっては、# プロンプトではなく > プロンプトが表示されることがあります。

ネットワーク設定

次のコマンドでは、すべてのネットワーク設定 (IP アドレス、ネットワーク モード、MAC アドレスなど) が表示されます。

```
# show network
```

IP 設定

次のコマンドでは、IP 関連の設定 (IPv4 および IPv6 設定、アドレス、ゲートウェイ、サブネット マスクなど) のみが表示されます。

```
# show network ip <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *all*、*v4*、または *v6*。

オプション	説明
all	IPv4 設定と IPv6 設定の両方が表示されます。 <i>ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。</i>
v4	IPv4 設定のみが表示されます。
v6	IPv6 設定のみが表示されます。

LAN インタフェース設定

次のコマンドでは、LAN インタフェース情報 (LAN インタフェース速度、デュプレックス モード、現在の LAN インタフェース ステータスなど) のみが表示されます。

```
# show network interface
```

ネットワーク モード

次のコマンドでは、現在のネットワーク モードが有線であるかワイヤレスであるかが表示されます。

```
# show network mode
```

ワイヤレス設定

次のコマンドでは、Dominion PX デバイスのワイヤレス設定（SSID パラメータなど）のみが表示されます。

```
# show network wireless
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
# show network wireless details
```

ネットワーク サービス設定

次のコマンドでは、ネットワーク サービス設定（Telnet 設定、HTTP サービス、HTTPS サービス、および SSH サービス用の TCP ポート、SNMP 設定など）のみが表示されます。

```
# show network services <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *all*、*http*、*https*、*telnet*、*ssh*、*snmp*、および *zeroconfig*。

オプション	説明
all	すべてのネットワーク サービス（HTTP、HTTPS、Telnet、SSH、SNMP など）の設定が表示されます。 <i>ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。</i>
http	HTTP サービスの TCP ポートのみが表示されます。
https	HTTPS サービスの TCP ポートのみが表示されます。
telnet	Telnet サービスの設定のみが表示されます。
ssh	SSH サービスの設定のみが表示されます。
snmp	SNMP の設定のみが表示されます。
zeroconfig	ゼロ構成アドバタイズメントの設定のみが表示されます。

オプション	説明
modbus	Modbus サービスの設定のみが表示されます。

PDU 設定

次のコマンドでは、PDU 設定（デバイス名、ファームウェアのバージョン、モデル タイプなど）が表示されます。

```
# show pdu
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
# show pdu details
```

アウトレット (コンセント) の情報

次のコマンド構文では、アウトレット (コンセント) 情報が表示されます。

```
# show outlets <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
# show outlets <n> details
```

変数:

- <n> は、次のいずれかのオプションです。all または番号。

オプション	説明
all	すべてのアウトレット (コンセント) の情報を表示します。 <i>ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。</i>
特定のアウトレット (コンセント) 番号	指定したアウトレット (コンセント) の情報のみを表示します。

表示情報:

- パラメータ「details」を指定しない場合は、アウトレット（コンセント）名のみが表示されます。PX-2000 シリーズの場合、アウトレット（コンセント）状態も表示されます。
- パラメータ「details」を指定した場合は、アウトレット（コンセント）名のほかに、アウトレット（コンセント）の定格などの、アウトレット（コンセント）の情報が表示されます。

インレット情報

次のコマンド構文では、インレットの情報が表示されます。

```
#          show inlets <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#          show inlets <n> details
```

変数:

- <n> は、次のいずれかのオプションです。all または番号。

オプション	説明
all	すべてのインレットの情報を表示します。 <i>ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。</i>
特定のインレット番号	指定したインレットの情報のみを表示します。 PDU に複数のインレットがある場合にのみ、インレット番号を指定する必要があります。

表示情報:

- パラメータ「details」を指定しない場合は、インレットの RMS の電流値とインレット名のみが表示されます。
- パラメータ「details」を指定した場合は、RMS 電流値のほかに、インレットの RMS 電流、電圧、有効電力などの、インレットの詳細情報が表示されます。

サーキット ブレーカ情報

このコマンドは、過電流保護機構が実装されている PDU でのみ使用できます。

次のコマンド構文では、サーキット ブレーカの情報が表示されます。

```
# show ocp <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
# show ocp <n> details
```

変数:

- <n> は、次のいずれかのオプションです。all または番号。

オプション	説明
all	すべてのサーキット ブレーカの情報を表示します。 ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。
特定のサーキット ブレーカ番号	指定したサーキット ブレーカの情報のみを表示します。

表示情報:

- パラメータ「details」を指定しない場合は、サーキット ブレーカの状態と名前のみが表示されます。
- パラメータ「details」を指定した場合は、状態のほかに、定格や RMS 電流値などの、サーキット ブレーカの詳細情報が表示されます。

日付と時刻の設定

次のコマンドでは、Dominion PX デバイスの現在の日付と時刻の設定が表示されます。

```
# show time
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
# show time details
```

環境センサー情報

次のコマンド構文では、環境センサーの情報が表示されます。

```
# show externalsensors <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
# show externalsensors <n> details
```

変数:

- <n> は、次のいずれかのオプションです。 *all* または番号。

オプション	説明
all	すべての環境センサーの情報を表示します。 ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。
特定の環境センサー番号*	指定した環境センサーの情報のみを表示します。

* 環境センサー番号とは、センサーに割り当てられる ID 番号のことです。この番号は、Dominion PX の Web インタフェースの [External Sensors (外部センサー)] ページにあります。

表示情報:

- パラメータ「details」を指定しない場合は、センサー ID、センサー タイプ、および測定値のみが表示されます。

注: ディスクリット (オン/オフ) センサーでは、測定値の代わりにセンサー状態が表示されます。

- パラメータ「details」を指定した場合は、ID 番号とセンサー測定値のほかに、シリアル番号や X、Y、Z 座標のような、詳細情報が表示されます。

インレット センサーしきい値情報

次のコマンド構文では、特定のインレット センサーのしきい値関連の情報が表示されます。

```
# show sensor inlet <n> <sensor type>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
# show sensor inlet <n> <sensor type> details
```

変数:

- <n> は、センサーを照会するインレットの番号です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

表示情報:

- パラメータ「details」を指定しない場合は、指定されたインレット センサーの測定値、状態、しきい値、アサート停止ヒステリシス、およびアサート遅延設定のみが表示されます。
- パラメータ「details」を指定すると、精度や範囲など、センサーの詳細情報が表示されます。
- 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

インレットの極センサーしきい値情報

このコマンドは、インライン モニタ (PX2-3000 シリーズ) を除く 3 相 PDU でのみ使用できます。

次のコマンド構文では、特定のインレットの極センサーのしきい値関連の情報が表示されます。

```
# show sensor inletpole <n> <p> <sensor type>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
# show sensor inletpole <n> <p> <sensor type> details
```

変数:

- <n> は、極センサーを照会するインレットの番号です。
- <p> は、センサーを照会するインレットの極のラベルです。

極	ラベル <p>	電流センサー	電圧センサー
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー

センサー タイプ	説明
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー

表示情報:

- パラメータ「details」を指定しない場合は、指定されたインレットの極センサーの測定値、状態、しきい値、アサート停止ヒステリシス、およびアサート タイムアウト設定のみが表示されます。
- パラメータ「details」を指定すると、精度や範囲など、センサーの詳細情報が表示されます。
- 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

サーキット ブレーカ センサーしきい値情報

このコマンドは、過電流保護機構が実装されている PDU でのみ使用できます。

次のコマンド構文では、特定のサーキット ブレーカ センサーのしきい値関連の情報が表示されます。

```
# show sensor ocp <n> <sensor type>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
# show sensor ocp <n> <sensor type> details
```

変数:

- <n> は、センサーを照会するサーキット ブレーカの番号です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー

表示情報:

- パラメータ「details」を指定しない場合は、指定されたサーキット ブレーカ センサーの測定値、状態、しきい値、およびアサート停止ヒステリシス設定が表示されます。
- パラメータ「details」を指定すると、精度や範囲など、センサーの詳細情報が表示されます。
- 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

環境センサーしきい値情報

次のコマンド構文では、指定した環境センサーのしきい値関連の情報が表示されます。

```
# show sensor externalsensor <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
# show sensor externalsensor <n> details
```

変数:

- <n> は、環境センサー番号です。 環境センサー番号とは、センサーに割り当てられる ID 番号のことです。この番号は、Dominion PX の Web インタフェースの [External Sensors (外部センサー)] ページにあります。

表示情報:

- パラメータ「details」を指定しない場合は、指定された環境センサーの測定値、しきい値、アサート停止ヒステリシス、およびアサート タイムアウト設定のみが表示されます。
- パラメータ「details」を指定すると、精度や範囲など、センサーの詳細情報が表示されます。

注: ディスクリット (オン/オフ) センサーの場合、しきい値関連のデータと精度関連のデータは使用できません。

セキュリティ設定

次のコマンドでは、Dominion PX のセキュリティ設定が表示されます。

```
# show security
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
# show security details
```

表示情報:

- パラメータ「details」を指定しない場合は、IP アクセス制御、役割ベースのアクセス制御、パスワード ポリシー、HTTPS 暗号化などの情報が表示されます。
- パラメータ「details」を指定すると、ユーザ ブロック時間やユーザ アイドル タイムアウトなどのセキュリティ詳細情報が表示されます。

既存のユーザ プロファイル

次のコマンドでは、1 つまたはすべての既存のユーザ プロファイルのデータが表示されます。

```
# show user <user_name>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
# show user <user_name> details
```

変数:

- <user_name> は、プロフィールを照会するユーザの名前です。変数は、*all* またはユーザ名のいずれかです。

オプション	説明
all	既存のすべてのユーザ プロファイルが表示されます。
	ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。

オプション	説明
特定のユーザ名	指定されたユーザのプロファイルのみが表示されます。

表示情報:

- パラメータ「details」を指定しない場合は、4 つのユーザ情報（ユーザ名、「有効」状態、SNMP v3 アクセス権限、および役割）のみが表示されます。
- パラメータ「details」を指定すると、電話番号、電子メール アドレス、優先温度単位などのユーザ詳細情報が表示されます。

既存の役割

次のコマンドでは、1 つまたはすべての既存の役割のデータが表示されます。

```
# show roles <role_name>
```

変数:

- <role_name> は、権限を照会する役割の名前です。変数は、次のいずれかのオプションです。

オプション	説明
all	既存のすべての役割が表示されます。 <i>ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。</i>
特定の役割の名前	指定された役割のデータのみが表示されます。

表示情報:

- 役割の説明、権限など、役割の設定が表示されます。

負荷遮断設定

このセクションは、アウトレット（コンセント）切り替え対応 PDU にのみ適用されます。

次のコマンドでは、負荷遮断設定が表示されます。

```
# show loadshedding
```

表示情報:

- 負荷遮断状態は、非臨界アウトレット（コンセント）とともに表示されます。

注: 負荷遮断モードは、臨界および非臨界アウトレット（コンセント）に関連付けられます。CLI で臨界および非臨界アウトレット（コンセント）を指定するには、『**非臨界アウトレット（コンセント）の指定**』[『304p.』](#)を参照してください。

シリアル ポート設定

次のコマンドでは、Dominion PX デバイスの「CONSOLE / MODEM」というラベルが付いたシリアル ポートのボーレートの設定が表示されます。

```
# show serial
```

EnergyWise 設定

次のコマンドでは、Dominion PX の現在の Cisco® EnergyWise 設定が表示されます。

```
# show energywise
```

資産センサー設定

このコマンドでは、資産センサー設定（ラック ユニット（タグ ポート）の合計数、資産センサーの状態、ナンバリング モード、向き、使用可能なタグ、および LED 色の設定など）が表示されます。

```
#          show assetStrip <n>
```

変数:

- <n> は、次のいずれかのオプションです。all または番号。

オプション	説明
all	すべての資産センサー情報が表示されます。 <i>ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。</i>
特定の資産センサー番号	指定した FEATURE ポート番号に接続された資産センサーの設定を表示します。 FEATURE ポートが 1 つだけの Dominion PX デバイスの場合、有効な番号は常に 1 になります。

次のコマンド構文では、接続されている資産センサーのすべてのラックユニットの LED 色を設定して、資産タグが接続されていないことを示すことができます。

```
config:#    assetStrip <n> LEDColorForDisconnectedTags <color>
```

変数:

- <color> は、HTML 形式の色の 16 進 RGB 値です。<color> 変数の範囲は、#000000 ～ #FFFFFF です。

資産センサーのラック ユニット設定

Raritan 資産センサーの場合、ラック ユニットはタグ ポートを意味します。次のコマンドでは、資産センサーの特定のラック ユニットまたはすべてのラック ユニットの設定（ラック ユニットの LED 色、LED モードなど）が表示されます。

```
# show rackUnit <n> <rack_unit>
```

変数:

- <n> は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの Dominion PX デバイスの場合、番号は常に 1 になります。
- <rack_unit> は、*all* または特定のラック ユニットのインデックス番号のいずれかです。

オプション	説明
all	指定した資産センサーのすべてのラック ユニットの設定が表示されます。 ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。
特定の数値	指定した資産センサーの指定したラック ユニットの設定が表示されます。 インデックス番号を使用してラック ユニットを指定します。各ラック ユニットのインデックス番号は、Web インタフェースの [Asset Strip (資産ストリップ)] ページに表示されます。

ブレード拡張ストリップの設定

このコマンドでは、ブレード拡張ストリップの情報（タグ ポートの合計数、および可能な場合は接続されているタグの ID (バーコード) 番号を含む）が表示されます。

```
#          show bladeSlot <n> <rack_unit> <blade_slot>
```

変数:

- <n> は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの Dominion PX デバイスの場合、番号は常に 1 になります。
- <rack_unit> は、選択した資産センサーの目的のラック ユニット（タグ ポート）のインデックス番号です。各ラック ユニットのインデックス番号は、Web インタフェースの [Asset Strip (資産ストリップ)] ページに表示されます。
- <blade_slot> は、次のいずれかのオプションです。all、またはブレード拡張ストリップの特定のタグ ポートの番号。

オプション	説明
all	特定のラック ユニットの接続されている、指定したブレード拡張ストリップのすべてのタグ ポートの情報を表示します。 ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。
特定の数値	特定のラック ユニットの接続されているブレード拡張ストリップの指定したタグ ポートの情報を表示します。 ブレード拡張ストリップの各タグ ポートの番号は、[Asset Strip (資産ストリップ)] ページに表示されます。

信頼性データ

次のコマンドでは、信頼性データが表示されます。

```
#          show reliability data
```

信頼性エラー ログ

次のコマンドでは、信頼性エラー ログが表示されます。

```
# show reliability errorlog <n>
```

変数:

- <n> は、次のいずれかのオプションです。0(ゼロ) またはその他の整数。

オプション	説明
0	信頼性エラー ログのすべてのエントリが表示されます。 ヒント: このオプション「0」を追加せずにコマンドを入力しても、すべてのデータを取得できます。
特定の整数	信頼性エラー ログの指定した数の最後のエントリが表示されます。

コマンド履歴

次のコマンド構文では、現在の接続セッションのコマンド履歴が表示されます。

```
# show history
```

表示情報:

- 現在のセッションでこれまでに入力されたコマンドのリストが表示されます。

履歴バッファの長さ

次のコマンド構文では、history コマンドを格納するための履歴バッファの長さが表示されます。

```
# show history bufferlength
```

表示情報:

- 現在の履歴バッファの長さが表示されます。

例

このセクションでは、show コマンドの例を示します。

例 1 - 基本的なセキュリティ情報

次の図は、*show security* コマンドの出力を示しています。

```
# show security
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled

Prevent concurrent user login: No

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

例 2 - 詳細なセキュリティ情報

show security details コマンドを入力すると、詳細な情報が表示されます。

```
# show security details
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled
Aging interval: 60 days

Prevent concurrent user login: No
Maximum number of failed logins: 3
User block time: 10 minutes

User idle timeout: 10 minutes

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

例 3 - 基本的な PDU 情報

次の図は、*show pdu* コマンドの出力を示しています。

```
# show pdu
PDU 'my PX'
Model: PX2-5260R
Firmware version: 2.2.0.1-26020
#
```


例 4 - 詳細な PDU 情報

`show pdu details` コマンドを入力すると、詳細な情報が表示されます。

```
# show pdu details
PDU 'my PX'
Model: PX2-5260R
Firmware version: 2.2.0.1-26020
Serial number: PEG1234567

Default outlet state on startup: Last known state
Power cycle delay: 10 seconds

Outlet power sequence: default
Outlet sequence delays: 1-12: 0 s
Inrush guard delay: 200 ms

Voltage rating: 200-240V
Current rating: 16A
Frequency rating: 50/60Hz
Power rating: 3.2-3.8kVA

Sensor data retrieval: Enabled
Measurements per log entry: 60

External sensor Z coordinate format: Rack units
Device altitude: 0 m
#
```

Dominion PX デバイスとネットワークの設定

CLI を使用して Dominion PX デバイスまたはネットワークを設定するには、管理者としてログインする必要があります。

設定モードへの移行

設定コマンドは設定モードでのみ機能するため、設定モードに移行する必要があります。

▶ **設定モードに移行するには、次の手順に従います。**

1. 管理者モードになっていて、# プロンプトが表示されていることを確認します。

注: ユーザ モードから設定モードに移行すると、設定を変更するための権限が制限されることがあります。「さまざまな CLI モードとプロンプト」『277p.』を参照してください。

2. 「config」と入力して、Enter キーを押します。 config:# プロンプトが表示され、設定モードになっていることがわかります。

config:# _

3. これで、設定コマンドを入力して Enter キーを押すと、設定を変更できます。

重要: 新しい設定を適用するには、「**apply**」コマンドを発行してから、端末エミュレーション プログラムを閉じる必要があります。プログラムを閉じて、設定の変更は保存されません。「設定モードの終了『423p. 』」を参照してください。

PDU 設定コマンド

PDU 設定コマンドは、*pdu* で始まります。PDU 設定コマンドを使用すると、Dominion PX デバイス全体に適用される設定を変更できます。

コマンドでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

PDU 名の変更

次のコマンド構文では、Dominion PX デバイスの名前を変更します。

```
config:# pdu name "<name>"
```

変数:

- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。<name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

例

次のコマンドでは、PDU に「my px12」という名前が割り当てられます。

```
config:# pdu name "my px12"
```

アウトレット (コンセント) の電源オン順序の設定

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

次のコマンドの構文では、PDU の電源がオンになったときのアウトレット (コンセント) の電源オン順序を設定できます。

```
config:# pdu outletSequence <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *default*、またはアウトレット (コンセント) の番号のカンマ区切りのリストです。

オプション	説明
default	Dominion PX デバイスの電源がオンになったときに、すべてのアウトレット (コンセント) は、昇順に (アウトレット (コンセント) 1 から最後のアウトレット (コンセント)) スイッチがオンになります。
アウトレット (コンセント) 番号のカンマ区切りのリスト	すべてのアウトレット (コンセント) はカンマ区切りリストで指定した順にスイッチがオンになります。 リストには、PDU のすべてのアウトレット (コンセント) を含める必要があります。

例

次のコマンドでは、10 個のアウトレット (コンセント) を備えた PDU で、PDU の電源がオンになった後、最初に 8 番目から 6 番目のアウトレット (コンセント) が電源オンになり、その後、残りのアウトレット (コンセント) が昇順にオンになります。

```
config:# pdu outletSequence 8-6,1-5,9,10
```

アウトレット (コンセント) の電源オンのシーケンス遅延の設定

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

次のコマンド構文では、すべてのアウトレット (コンセント) を順にオンにする場合のアウトレット (コンセント) の遅延 (秒単位) を設定できます。

```
config:# pdu outletSequenceDelay <outlet1>:<delay1>;<outlet2>:<delay2>;<outlet3>:<delay3>;...
```

アウトレット (コンセント) 番号とその遅延設定の間を、コロンで区切ります。アウトレット (コンセント) とその遅延の各組み合わせの間を、セミコロンで区切ります。

変数:

- <outlet1>、<outlet2>、<outlet3> などは、個々のアウトレット (コンセント) 番号またはアウトレット (コンセント) の範囲です。
- <delay1>、<delay2>、<delay3> などは、遅延時間 (秒単位) です。

例

次のコマンドでは、アウトレット (コンセント) 1 の遅延を 2.5 秒、アウトレット (コンセント) 2 の遅延を 3 秒、アウトレット (コンセント) 3 ~ 5 の遅延を 10 秒に指定します。

```
config:# pdu outletSequenceDelay 1:2.5;2:3;3-5:10
```

アウトレット (コンセント) の PDU 定義のデフォルト状態の設定

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

次のコマンド構文では、PDU の電源がオンになった後のすべてのアウトレット (コンセント) の初期電源状態を指定できます。

```
config:# pdu outletStateOnDeviceStartup <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *off*、*on*、または *lastKnownState*。

オプション	説明
off	Dominion PX デバイスの電源がオンになったときに、すべてのアウトレット (コンセント) の電源をオフにします。
on	Dominion PX デバイスの電源がオンになったときに、すべてのアウトレット (コンセント) の電源をオンにします。
lastKnownState	PDU の電源が再びオンになったときに、すべてのアウトレット (コンセント) を、Dominion PX デバイスの電源がオフになる前のステータスに戻します。

例

次のコマンドでは、PDU を再び電源オンにした後に、すべてのアウトレット (コンセント) が PDU の電源がオフになる前の電源状態に戻ります。

```
config:# pdu outletStateOnDeviceStartup lastKnownState
```

PDU 定義の電源再投入時の電源オフ時間の設定

このセクションは、アウトレット（コンセント）切り替え対応 PDU にのみ適用されます。

次のコマンド構文では、すべてのアウトレット（コンセント）に対して、電源再投入操作の電源オフ時間を設定できます。

```
config:# pdu cyclingPowerOffPeriod <timing>
```

変数:

- <timing> は、再投入時の電源オフ時間の秒数で、0 ～ 3600 の整数です。

例

次のコマンドでは、電源再投入操作の電源オフ時間を 5 秒に設定できます。

```
config:# pdu cyclingPowerOffPeriod 5
```

突入電流防止遅延時間の設定

このセクションは、アウトレット（コンセント）切り替え対応 PDU にのみ適用されます。

次のコマンド構文では、突入電流防止遅延を設定できます。

```
config:# pdu inrushGuardDelay <timing>
```

変数:

- <timing> は、100 ～ 100000 ミリ秒の遅延時間です。

例

次のコマンドでは、突入電流防止遅延を 1000 ミリ秒に設定します。

```
config:# pdu inrushGuardDelay 1000
```

アウトレット (コンセント) 初期化遅延の設定

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

次のコマンド構文では、デバイス起動時のアウトレット (コンセント) 初期化遅延の時間を決定できます。アウトレット (コンセント) 初期化遅延については、「**初期化遅延の設定**『162p.』」を参照してください。

```
config:# pdu outletInitializationDelayOnDeviceStartup <timing>
```

変数:

- <timing> は、1 ～ 3600 秒の遅延時間です。

例

次のコマンドでは、アウトレット (コンセント) 初期化遅延の時間が 5 秒に設定されます。

```
config:# pdu outletInitializationDelayOnDeviceStartup 5
```

非臨界アウトレット (コンセント) の指定

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

次のコマンド構文では、臨界アウトレット (コンセント) と非臨界アウトレット (コンセント) を指定できます。これは負荷遮断モードに関連付けられます。「**非臨界アウトレット (コンセント) と負荷遮断モードの設定**『166p. 』」を参照してください。

```
config:# pdu nonCriticalOutlets <outlets1>:false;<outlets2>:true
```

アウトレット (コンセント) 番号とその設定の間を、コロンで区切ります。「false」と「true」の各組み合わせの間を、セミコロンで区切ります。

変数:

- <outlets1> は、非臨界アウトレット (コンセント) として設定する 1 つ以上のアウトレット (コンセント) 番号です。カンマを使用してアウトレット (コンセント) 番号を区切ります。
- <outlets2> は、臨界アウトレット (コンセント) として設定する 1 つ以上のアウトレット (コンセント) 番号です。カンマを使用してアウトレット (コンセント) 番号を区切ります。

例

次のコマンドでは、12 アウトレット (コンセント) PDU のアウトレット (コンセント) 1、2、3、7、および 9 を臨界アウトレット (コンセント) として設定し、4、5、6、8、10、11、および 12 を非臨界アウトレット (コンセント) として設定します。

```
config:# pdu nonCriticalOutlets 1-3,7,9:false;4-6,8,10-12:true
```


データ ログイングの有効化または無効化

次のコマンド構文では、データ ログイング機能の有効/無効を切り替えることができます。

```
config:# pdu dataRetrieval <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *enable* または *disable*。

オプション	説明
enable	データ ログイング機能を有効にします。
disable	データ ログイング機能を無効にします。

詳細については、「**データ ログイングの設定**『110p.』」を参照してください。

例

次のコマンドでは、データ ログイング機能が有効になります。

```
config:# pdu dataRetrieval enable
```

エン트리ごとのデータ ログイング測定数の設定

次のコマンド構文では、ログ エントリーごとに蓄積される測定値の数を指定できます。

```
config:# pdu measurementsPerLogEntry <number>
```

変数:

- <number> は、1 ～ 600 の範囲の整数です。デフォルトは、ログ エントリーごとに 60 サンプルです。

詳細については、「**データ ログイングの設定**『110p.』」を参照してください。

例

次のコマンドでは、センサーについてログ エントリごとに 66 の測定値を蓄積します。この場合、測定周期は 66 秒になります。

```
config:# pdu measurementsPerLogEntry 66
```

デバイスの高度の指定

次のコマンド構文では、Dominion PX デバイスの海拔高度（メートル単位）を指定します。Raritan 空気差圧センサーが接続されている場合、Dominion PX デバイスの海拔高度を指定する必要があります。これは、デバイスの高度が高度補正率に関連付けられているためです。「**高度補正率**」『467p. 』を参照してください。

```
config:# pdu deviceAltitude <altitude>
```

変数:

- <altitude> は、1 ～ 3000 メートルの整数です。

例

次のコマンドでは、Dominion PX デバイスを海拔高度 1500 メートルの場所に配置することを指定します。

```
config:# pdu deviceAltitude 1500
```

環境センサーの Z 座標形式の設定

次のコマンド構文では、ラック ユニットによる環境センサーの高さ (Z 座標) の指定を有効または無効にすることができます。

```
config:# pdu externalSensorsZCoordinateFormat <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *rackUnits* または *freeForm*。

オプション	説明
rackUnits	Z 座標の高さが、標準のラック ユニットで表されます。これを選択すると、ラック ユニットの数値を入力して、環境センサーの Z 座標を表すことができます。
freeForm	Z 座標の指定に、任意の英数字を使用できます。

注: Z 座標の形式を決定した後、Z 座標の値を設定できます。『Z 座標の設定 366p. 』を参照してください。

例

次のコマンドでは、環境センサーの Z 座標を指定するためにラック ユニットを使用するように指定します。

```
config:# pdu externalSensorsZCoordinateFormat rackUnits
```

LED 表示の向きの変更

次のコマンド構文では、ゼロ UPDU の LED 表示の値の向きを決定できます。

```
config:# pdu displayOrientation <orientation>
```

変数:

- <orientation> は、次のいずれかのオプションです。*automatic*、*flipped*、または *normal*。

オプション	説明
automatic	LED 表示の値の向きは、組み込みのチルト センサーで検出された PDU の向きによって決まります。
flipped	LED 表示の値は、PDU の向きに関係なく常に上下逆に表示されます。
normal (正常)	LED 表示の値は、PDU の向きに関係なく常に標準の向きで表示されます。

このコマンドは、ゼロ UPDU 以外には適用できません。

例

次のコマンドでは、ゼロ UPDU で LED 表示の値の向きを逆にできます。

```
config:# pdu displayOrientation flipped
```

ネットワーク設定コマンド

CLI を使用して、さまざまなネットワーク設定 (IP アドレス、送信速度、デュプレックス モードなど) を変更できます。

ネットワーク モードの設定

Dominion PX デバイスに有線ネットワーク機構とワイヤレス ネットワーク機構の両方が実装されている場合は、詳細なネットワーク パラメータを設定する前に、有効にするネットワーク接続の機構を指定する必要があります。

次のコマンド構文では、有線ネットワーク モードまたはワイヤレス ネットワーク モードを有効にします。

```
config:# network mode <mode>
```

変数:

- <mode> は、次のいずれかのモードです。 *wired* または *wireless*

モード	説明
wired	有線ネットワーク モードを有効にします。
wireless	ワイヤレス ネットワーク モードを有効にします。

注: ワイヤレス ネットワーク モードを有効にし、*Dominion PX* によってワイヤレス USB LAN アダプタが検出されないか、接続されているワイヤレス USB LAN アダプタがサポートされていない場合は、「Supported Wireless device not found (サポートされているワイヤレス デバイスが見つかりません)」というメッセージが表示されます。

例

次のコマンドでは、有線ネットワーク モードが有効になります。

```
config:# network mode wired
```

IP プロトコルの設定

デフォルトでは、IPv4 プロトコルのみが有効になっています。Dominion PX デバイスに対して、IPv4 および IPv6 プロトコルの両方、または IPv6 プロトコルのみを有効にすることができます。

IP プロトコル設定コマンドは、*network ip* で始まります。

IPv4 または IPv6 の有効化

次のコマンド構文では、Dominion PX に対して有効にする IP プロトコルを指定できます。

```
config:#    network ip proto <protocol>
```

変数:

- <protocol> は、*v4Only*、*v6Only*、または *both* のいずれかです。

モード	説明
v4Only	すべてのインタフェースに対して IPv4 のみを有効にします。デフォルトではこの設定です。
v6Only	すべてのインタフェースに対して IPv6 のみを有効にします。
[both (両方)]	すべてのインタフェースに対して IPv4 と IPv6 の両方を有効にします。

例

次のコマンドでは、IPv4 プロトコルと IPv6 プロトコルの両方を有効にします。

```
config:#    network ip protocol both
```

IPv4 アドレスまたは IPv6 アドレスの選択

次のコマンド構文では、DNS サーバから IPv4 アドレスと IPv6 アドレスの両方が返された場合に使用する IP アドレスを指定できます。この設定は、Dominion PX に対して IPv4 プロトコルと IPv6 プロトコルの両方を有効にした場合にのみ設定する必要があります。

```
config:#    network ip dnsResolverPreference <resolver>
```

変数:

- <resolver> は、*preferV4* または *preferV6* のいずれかです。

オプション	説明
preferV4	DNS サーバから返された IPv4 アドレスを使用します。

オプション	説明
preferV6	DNS サーバから返された IPv6 アドレスを使用します。

例

次のコマンドでは、DNS サーバから返された IPv4 アドレスのみを使用するように指定します。

```
config:# network ip dnsResolverPreference preferV4
```

ワイヤレス パラメータの設定

ワイヤレス ネットワーキング モードを有効にした後、Service Set Identifier (SSID)、認証方法、事前共有キー (PSK)、および Basic Service Set Identifier (BSSID) などのワイヤレス パラメータを設定する必要があります。

ワイヤレス設定コマンドは、*network wireless* で始まります。

注: 現在のネットワーク モードがワイヤレスでない場合、SSID、PSK、および BSSID の値は、ネットワーク モードが「ワイヤレス」に変更されるまで適用されません。さらに、アクティブなネットワーク インタフェースがワイヤレスでないことを示すメッセージが表示されます。

コマンドでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

SSID の設定

次のコマンド構文では、SSID 文字列を指定できます。

```
config:# network wireless SSID <ssid>
```

変数:

- <ssid> は、ワイヤレス アクセス ポイントの名前で、構成は次のとおりです。
 - 最大 32 文字の ASCII 文字
 - スペースなし
 - ASCII コード 0x20 ~ 0x7E

例

次のコマンドでは、「myssid」を SSID として割り当てます。

```
config:# network wireless SSID myssid
```

認証方法の設定

次のコマンド構文では、ワイヤレス認証方法を PSK または Extensible Authentication Protocol (EAP) に設定します。

```
config:# network wireless authMethod <method>
```

変数:

- <method> は、PSK または EAP のいずれかの認証方法です。

方法	説明
PSK (PSK)	ワイヤレス認証方法が PSK に設定されます。
EAP	ワイヤレス認証方法が EAP に設定されます。

例

次のコマンドでは、ワイヤレス認証方法を PSK に設定します。

```
config:# network wireless authMethod PSK
```

PSK の設定

事前共有キー (PSK) 認証方法を選択した場合は、次のコマンド構文を使用して、PSK パスフレーズを割り当てる必要があります。

```
config:# network wireless PSK <psk>
```

変数:

- <psk> は、パスフレーズの文字列で、構成は次のとおりです。
 - 最大 32 文字の ASCII 文字
 - スペースなし
 - ASCII コード 0x20 ~ 0x7E

例

次のコマンドでは、「encrypt-key」を PSK として割り当てます。

```
config:#    network wireless PSK encrypt-key
```

EAP パラメータの設定

ワイヤレス認証方法を EAP に設定した場合は、外部認証、内部認証、EAP ID、パスワード、CA 証明書などの EAP 認証パラメータを設定する必要があります。

外部認証の設定

次のコマンド構文では、EAP の外部認証プロトコルを指定できます。

```
config:#    network wireless eapOuterAuthentication <outer_auth>
```

変数:

- Dominion PX では外部認証として Protected Extensible Authentication Protocol (PEAP) のみがサポートされるため、<outer_auth> の値は *PEAP* です。

例

次のコマンドでは、EAP 認証の外部認証プロトコルとして Protected Extensible Authentication Protocol (PEAP) を指定します。

```
config:#    network wireless eapOuterAuthentication PEAP
```

内部認証の設定

次のコマンド構文では、EAP の内部認証プロトコルを指定できます。

```
config:#    network wireless eapInnerAuthentication <inner_auth>
```

変数:

- Dominion PX では内部認証として Microsoft Challenge Authentication Protocol Version 2 (MSCHAPv2) のみがサポートされるため、<inner_auth> の値は *MSCHAPv2* です。

例

次のコマンドでは、EAP 認証の内部認証プロトコルとして MSCHAPv2 を指定します。

```
config:#    network wireless eapInnerAuthentication MSCHAPv2
```

EAP ID の設定

次のコマンド構文では、EAP ID を指定できます。

```
config:#    network wireless eapIdentity <identity>
```

変数:

- <identity> は EAP 認証のユーザ名です。

例

次のコマンドでは、EAP ID が「eap_user01」に設定されます。

```
config:#    network wireless eapIdentity eap_user01
```

EAP パスワードの設定

次のコマンド構文では、EAP パスワードを指定できます。

```
config:#    network wireless eapPassword
```

変数:

- <password> は EAP 認証のパスワードです。

例

次のコマンドでは、EAP パスワードが「user01_password」に設定されます。

```
config:#    network wireless eapPassword user01_password
```

EAP CA 証明書を入力

EAP 認証のためにサードパーティの CA 証明書を入力する必要があります。

▶ 証明書を入力するには、以下の手順に従います。

- 次に示す CA 証明書のコマンドを入力し、Enter キーを押します。

```
config:# network wireless eapCACertificate
```
- CA 証明書の内容を入力するように求められます。次の操作を実行して内容を入力します。
 - テキスト エディタで CA 証明書を開きます。
 - 証明書の「--- BEGIN CERTIFICATE ---」行と「--- END CERTIFICATE ---」行の間の内容をコピーします。
 - 証明書の内容を端末に貼り付けます。
 - Enter キーを押します。

ヒント: 既存の CA 証明書を削除するには、証明書の内容の入力を求められたときに、何も入力したり貼り付けたりせずに Enter を押します。

- 証明書が有効な場合は、コマンド プロンプト「config:#」が再度表示されます。有効でない場合は、証明書が無効であることを示すメッセージが表示されます。

例

このセクションでは、CA 証明書の例のみを示します。実際の CA 証明書の内容は、この例で表示されている内容とは異なります。

▶ 証明書を入力するには、以下の手順に従います。

- 設定モードになっていることを確認します。「**設定モードへの移行**『297p.』」を参照してください。
- 次のコマンドを入力し、Enter キーを押します。

```
config:# network wireless eapCACertificate
```
- CA 証明書の内容を入力するように求められます。
- テキスト エディタで CA 証明書を開きます。次のような証明書の内容が表示されます。

```

--- BEGIN CERTIFICATE ---
MIICjTCCAfIgAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwrGJBALrAwYydgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwLYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTA1VTMTYwNAYDVQQK
Ey1OYXRpb25hbCBXBZjvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVROBAQH/BA0wC4AJODMyOTcwODEwMBGGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVROKBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXD/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---

```

- 次に示すように、「BEGIN CERTIFICATE」を含む最初の行と「END CERTIFICATE」を含む最後の行以外の内容を選択し、コピーします。

```

MIICjTCCAfIgAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwrGJBALrAwYydgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwLYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTA1VTMTYwNAYDVQQK
QKEy1OYXRpb25hbCBXBZjvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVROBAQH/BA0wC4AJODMyOTcwODEwMBGGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVROKBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH
21X82tZXD/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO

```

- 内容を端末に貼り付けます。
- Enter キーを押します。
- 入力した証明書が有効であることを示す次のコマンド プロンプトが表示されるかどうかを確認します。

```
config:#
```

BSSID の設定

次のコマンド構文では、BSSID を指定できます。

```
config:#    network wireless BSSID <bssid>
```

変数:

- <bssid> は、ワイヤレス アクセス ポイントの MAC アドレスです。

例

次のコマンドでは、BSSID を 00:14:6C:7E:43:81 に設定します。

```
config:#    network wireless BSSID 00:14:6C:7E:43:81
```

IPv4 パラメータの設定

IPv4 設定コマンドは、*network ipv4* で始まります。

コマンドでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

IPv4 設定モードの設定

次のコマンド構文では、IP 設定モードを決定できます。

```
config:#    network ipv4 ipConfigurationMode <mode>
```

変数:

- <mode> は、次のいずれかのモードです。 *dhcp* または *static*。

モード	説明
dhcp	IPv4 設定モードが DHCP に設定されます。
static	IPv4 設定モードが固定 IP アドレスに設定されます。

例

次のコマンドでは、固定 IP 設定モードが有効になります。

```
config:#    network ipv4 ipConfigurationMode static
```

優先ホスト名の設定

IPv4 設定モードとして DHCP を選択すると、優先ホスト名を指定できます。ただし、これはオプションです。コマンド構文は、次のとおりです。

```
config:#    network ipv4 preferredHostName <name>
```

変数:

- <name> は、次の条件を満たすホスト名です。
 - 英数字やハイフンで構成されます。
 - 先頭および末尾をハイフンにすることはできません。
 - 63 文字を超えることはできません。
 - 句読点、空白文字などの記号は使用できません。

例

次のコマンドでは、優先ホスト名が「my-host」に設定されます。

```
config:#    network ipv4 preferredHostName my-host
```

IPv4 アドレスの設定

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、Dominion PX デバイスに永続的な IP アドレスを割り当てることができます。

```
config:#    network ipv4 ipAddress <ip address>
```

変数:

- <ip address> は、Dominion PX デバイスに割り当てる IP アドレスです。値の範囲は、0.0.0.0 ~ 255.255.255.255 です。

例

次のコマンドでは、Dominion PX デバイスに固定 IPv4 アドレス「192.168.84.222」が割り当てられます。

```
config:#    network ipv4 ipAddress 192.168.84.222
```

IPv4 サブネット マスクの設定

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、サブネット マスクを定義できます。

```
config:#    network ipv4 subnetMask <netmask>
```

変数:

- <netmask> は、サブネット マスク アドレスです。 値の範囲は、0.0.0.0 ~ 255.255.255.255 です。

例

次のコマンドでは、サブネット マスクが 192.168.84.0 に設定されます。

```
config:#    network ipv4 subnetMask 192.168.84.0
```

IPv4 ゲートウェイの設定

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、ゲートウェイを指定できます。

```
config:#    network ipv4 gateway <ip address>
```

変数:

- <ip address> は、ゲートウェイの IP アドレスです。 値の範囲は、0.0.0.0 ~ 255.255.255.255 です。

例

次のコマンドでは、IPv4 ゲートウェイが 255.255.255.0 に設定されます。

```
config:#    network ipv4 gateway 255.255.255.0
```

IPv4 プライマリ DNS サーバの設定

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、プライマリ DNS サーバを指定できます。

```
config:#    network ipv4 primaryDNSServer <ip address>
```

変数:

- <ip address> は、プライマリ DNS サーバの IP アドレスです。 値の範囲は、0.0.0.0 ～ 255.255.255.255 です。

例

次のコマンドでは、プライマリ DNS サーバが 192.168.84.30 に設定されます。

```
config:#    network ipv4 primaryDNSServer 192.168.84.30
```

IPv4 セカンダリ DNS サーバの設定

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、セカンダリ DNS サーバを指定できます。

```
config:#    network ipv4 secondaryDNSServer <ip address>
```

変数:

- <ip address> は、セカンダリ DNS サーバの IP アドレスです。 値の範囲は、0.0.0.0 ～ 255.255.255.255 です。

注: *Dominion PX* では、最大 3 台の DNS サーバがサポートされています。2 台の IPv4 DNS サーバと 2 台の IPv6 DNS サーバを利用できる場合は、*Dominion PX* でプライマリ IPv4 DNS サーバとプライマリ IPv6 DNS サーバのみが使用されます。

例

次のコマンドでは、セカンダリ DNS サーバが 192.168.84.33 に設定されます。

```
config:#    network ipv4 secondaryDNSServer 192.168.84.33
```


IPv4 DHCP によって割り当てられた DNS サーバの上書き

プライマリ/セカンダリ DNS サーバを指定した場合は、次のコマンドを使用して、DHCP によって割り当てられた DNS サーバを指定した DNS サーバで上書きできます。

```
config:# network ipv4 overrideDNS <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *enable* または *disable*。

オプション	説明
enable	DHCP によって割り当てられた DNS サーバを、自分で割り当てるプライマリ/セカンダリ DNS サーバで上書きします。
disable	DHCP によって割り当てられた DNS サーバの使用を再開します。

例

次のコマンドでは、DHCP によって割り当てられた DNS サーバを、指定した DNS サーバで上書きできます。

```
config:# network ipv4 overrideDNS enable
```

IPv6 パラメータの設定

IPv6 設定コマンドは、*network ipv6* で始まります。

コマンドでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

IPv6 設定モードの設定

次のコマンド構文では、IP 設定モードを決定できます。

```
config:# network ipv6 ipConfigurationMode <mode>
```

変数:

- <mode> は、次のいずれかのモードです。 *automatic* または *static*。

モード	説明
automatic	IPv6 設定モードが自動的に設定されます。

モード	説明
static	IPv6 設定モードが固定 IP アドレスに設定されます。

例

次のコマンドでは、IP 設定モードが固定 IP アドレス モードに設定されます。

```
config:# network ipv6 ipConfigurationMode static
```

IPv6 アドレスの設定

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、Dominion PX デバイスに永続的な IP アドレスを割り当てることができます。

```
config:# network ipv6 ipAddress <ip address>
```

変数:

- <ip address> は、Dominion PX デバイスに割り当てる IP アドレスです。この値では、IPv6 アドレスの形式を使用します。

例

次のコマンドでは、Dominion PX デバイスに固定 IPv6 アドレス「3210:4179:0:8:0:800:200C:417A」が割り当てられます。

```
config:# network ipv6 ipAddress 3210:4179:0:8:0:800:200C:417A
```

IPv6 ゲートウェイの設定

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、ゲートウェイを指定できます。

```
config:# network ipv6 gateway <ip address>
```

変数:

- <ip address> は、ゲートウェイの IP アドレスです。この値では、IPv6 アドレスの形式を使用します。

例

次のコマンドでは、ゲートウェイが 500:0:330:0:4:9:3:2 に設定されます。

```
config:#    network ipv6 gateway 500:0:330:0:4:9:3:2
```

IPv6 プライマリ DNS サーバの設定

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、プライマリ DNS サーバを指定できます。DNS サーバを手動で指定する前に、自動的に割り当てられた DNS サーバの上書きを有効にする必要があります。「*IPv6 DHCP によって割り当てられた DNS サーバの上書き*『324p. 』」を参照してください。

```
config:#    network ipv6 primaryDNSServer <ip address>
```

変数:

- <ip address> は、プライマリ DNS サーバの IP アドレスです。この値では、IPv6 アドレスの形式を使用します。

例

次のコマンドでは、プライマリ DNS サーバが 2103:288:8201:1::14 に設定されます。

```
config:#    network ipv6 primaryDNSServer 2103:288:8201:1::14
```

IPv6 セカンダリ DNS サーバの設定

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、セカンダリ DNS サーバを指定できます。DNS サーバを手動で指定する前に、自動的に割り当てられた DNS サーバの上書きを有効にする必要があります。「*IPv6 DHCP によって割り当てられた DNS サーバの上書き*」を参照してください。

```
config:# network ipv6 secondaryDNSServer <ip address>
```

変数:

- <ip address> は、セカンダリ DNS サーバの IP アドレスです。この値では、IPv6 アドレスの形式を使用します。

注: *Dominion PX* では、最大 3 台の DNS サーバがサポートされています。2 台の IPv4 DNS サーバと 2 台の IPv6 DNS サーバを利用できる場合は、*Dominion PX* でプライマリ IPv4 DNS サーバとプライマリ IPv6 DNS サーバのみが使用されます。

例

次のコマンドでは、セカンダリ DNS サーバが 2103:288:8201:1::700 に設定されます。

```
config:# network ipv6 secondaryDNSServer 2103:288:8201:1::700
```

IPv6 DHCP によって割り当てられた DNS サーバの上書き

プライマリ/セカンダリ DNS サーバを指定した場合は、次のコマンドを使用して、DHCP によって割り当てられた DNS サーバを指定した DNS サーバで上書きできます。

```
config:# network ipv6 overrideDNS <option>
```

変数:

- <option> は、次のいずれかのオプションです。enable または disable。

オプション	説明
enable	DHCP によって割り当てられた DNS サーバを、自分で割り当てるプライマリ/セカンダリ DNS サーバで上書きします。
disable	DHCP によって割り当てられた DNS サーバの使用を再開します。

例

次のコマンドでは、DHCP によって割り当てられた DNS サーバを、指定した DNS サーバで上書きできます。

```
config:#    network ipv6 overrideDNS enable
```

LAN インタフェース パラメータの設定

LAN インタフェース設定コマンドは、*network interface* で始まります。コマンドでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

LAN インタフェース速度の変更

次のコマンド構文では、LAN インタフェース速度を指定できます。

```
config:#    network interface LANInterfaceSpeed <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *auto*、*10Mbps*、および *100Mbps*。

オプション	説明
auto	自動ネゴシエーションによって最適な LAN 速度が自動的に決定されます。
10Mbps	LAN の速度は、常時 10Mbps です。
100Mbps	LAN の速度は、常時 100Mbps です。

例

次のコマンドでは、自動ネゴシエーションによって Dominion PX で最適な LAN インタフェース速度が決定されます。

```
config:#    network interface LANInterfaceSpeed auto
```

LAN デュプレックス モードの変更

次のコマンド構文では、LAN インタフェースのデュプレックス モードを指定できます。

```
config:#    network interface LANInterfaceDuplexMode <mode>
```

変数:

- <mode> は、次のいずれかのモードです。 *auto*、*half*、または *full*。

オプション	説明
auto	Dominion PX では、自動ネゴシエーションによって最適な送信モードが自動的に選択されます。
half	半二重: データは、Dominion PX デバイスに対して半二重で送信されます。
full	全二重: データは、全二重で送信されます。

例

次のコマンドでは、自動ネゴシエーションによって Dominion PX で最適な送信モードが決定されます。

```
config:#    network interface LANInterfaceDuplexMode auto
```

ネットワーク サービス パラメータの設定

ネットワーク サービス コマンドは、*network services* で始まります。

HTTP ポートの変更

次のコマンド構文では、HTTP ポートを変更できます。

```
config:#    network services http <n>
```

変数:

- <n> は、1 ～ 65535 の TCP ポート番号です。デフォルトの HTTP ポートは 80 です。

例

次のコマンドでは、HTTP ポートが 81 に設定されます。

```
config:# network services http 81
```

HTTPS ポートの変更

次のコマンド構文では、HTTPS ポートを変更できます。

```
config:# network services https <n>
```

変数:

- <n> は、1 ～ 65535 の TCP ポート番号です。デフォルトの HTTPS ポートは 443 です。

例

次のコマンドでは、HTTPS ポートが 333 に設定されます。

```
config:# network services https 333
```

Telnet 設定の変更

CLI コマンドを使用して、Telnet サービスを有効または無効にしたり、その TCP ポートを変更したりできます。

Telnet コマンドは、*network services telnet* で始まります。

Telnet の有効化または無効化

次のコマンド構文では、Telnet サービスの有効/無効を切り替えることができます。

```
config:# network services telnet enabled <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *true* または *false*。

オプション	説明
true	Telnet サービスが有効になります。
false	Telnet サービスが無効になります。

例

次のコマンドでは、Telnet サービスが有効になります。

```
config:# network services telnet enabled true
```

Telnet ポートの変更

次のコマンド構文では、Telnet ポートを変更できます。

```
config:# network services telnet port <n>
```

変数:

- <n> は、1 ～ 65535 の TCP ポート番号です。デフォルトの Telnet ポートは 23 です。

例

次のコマンドでは、Telnet の TCP ポートが 44 に設定されます。

```
config:# network services telnet port 44
```

SSH 設定の変更

CLI コマンドを使用して、SSH サービスを有効または無効にしたり、その TCP ポートを変更したりできます。

SSH コマンドは、*network services ssh* で始まります。

SSH の有効化または無効化

次のコマンド構文では、SSH サービスの有効/無効を切り替えることができます。

```
config:# network services ssh enabled <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *true* または *false*。

オプション	説明
true	SSH サービスが有効になります。
false	SSH サービスが無効になります。

例

次のコマンドでは、SSH サービスが有効になります。

```
config:# network services ssh enabled true
```

SSH ポートの変更

次のコマンド構文では、SSH ポートを変更できます。

```
config:# network services ssh port <n>
```

変数:

- <n> は、1 ～ 65535 の TCP ポート番号です。デフォルトの SSH ポートは 22 です。

例

次のコマンドでは、SSH の TCP ポートが 555 に設定されます。

```
config:# network services ssh port 555
```

SNMP の設定

CLI コマンドを使用して、SNMP v1/v2c または v3 エージェントの有効/無効を切り替えたり、読み取り/書き込みコミュニティ スtringを設定したり、sysContact などの MIB-II パラメータを設定したりできます。

SNMP コマンドは、*network services snmp* で始まります。

SNMP v1/v2c の有効化または無効化

次のコマンド構文では、SNMP v1/v2c プロトコルの有効/無効を切り替えることができます。

```
config:# network services snmp v1/v2c <option>
```

変数:

- <option> は、次のいずれかのオプションです。enable または disable。

オプション	説明
enable	SNMP v1/v2c プロトコルが有効になります。
disable	SNMP v1/v2c プロトコルが無効になります。

例

次のコマンドでは、SNMP v1/v2c プロトコルが有効になります。

```
config:# network services snmp v1/v2c enable
```

SNMP v3 の有効化または無効化

次のコマンド構文では、SNMP v3 プロトコルの有効/無効を切り替えることができます。

```
config:# network services snmp v3 <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *enable* または *disable*。

オプション	説明
enable	SNMP v3 プロトコルが有効になります。
disable	SNMP v3 プロトコルが無効になります。

例

次のコマンドでは、SNMP v3 プロトコルが有効になります。

```
config:# network services snmp v3 enable
```

SNMP の読み取りコミュニティの設定

次のコマンド構文では、SNMP 読み取り専用コミュニティ スtring を設定できます。

```
config:# network services snmp readCommunity <string>
```

変数:

- <string> は、4 ～ 64 文字の ASCII の表示可能文字で構成される文字列です。
- 文字列にスペースを含めることはできません。

例

次のコマンド構文では、SNMP 読み取り専用コミュニティ スtringが「public」に設定されます。

```
config:# network services snmp readCommunity public
```

SNMP の書き込みコミュニティの設定

次のコマンド構文では、SNMP 読み取り/書き込みコミュニティ スtringを設定できます。

```
config:# network services snmp writeCommunity <string>
```

変数:

- <string> は、4 ～ 64 文字の ASCII の表示可能文字で構成される文字列です。
- 文字列にスペースを含めることはできません。

例

次のコマンドでは、SNMP 読み取り/書き込みコミュニティ スtringが「private」に設定されます。

```
config:# network services snmp writeCommunity private
```

sysContact 値の設定

次のコマンド構文では、SNMP sysContact MIB-II 値を設定できます。

```
config:# network services snmp sysContact <value>
```

変数:

- <value> は、0 ～ 255 文字の英数字で構成される文字列です。

例

次のコマンドでは、SNMP MIB-II sysContact が「John_Krause」に設定されます。

```
config:# network services snmp sysContact John_Krause
```

sysName 値の設定

次のコマンド構文では、SNMP sysName MIB-II 値を設定できます。

```
config:#    network services snmp sysName <value>
```

変数:

- <value> は、0 ～ 255 文字の英数字で構成される文字列です。

例

次のコマンドでは、SNMP MIB-II sysName が「Win7_system」に設定されます。

```
config:#    network services snmp sysName Win7_system
```

sysLocation 値の設定

次のコマンド構文では、SNMP sysLocation MIB-II 値を設定できます。

```
config:#    network services snmp sysLocation <value>
```

変数:

- <value> は、0 ～ 255 文字の英数字で構成される文字列です。

例

次のコマンドでは、SNMP MIB-II sysLocation が「New_TAIPEI」に設定されます。

```
config:#    network services snmp sysLocation New_TAIPEI
```

Modbus 設定の変更

Modbus エージェントの有効化または無効化、読み取り専用機能の設定、TCP ポートの変更ができます。

Modbus コマンドは、*network services modbus* で始まります。

Modbus の有効化または無効化

次のコマンド構文では、Modbus プロトコルの有効/無効を切り替えることができます。

```
config:#    network services modbus enabled <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *true* または *false*。

オプション	説明
true	Modbus エージェントが有効になります。
false	Modbus エージェントが無効になります。

例

次のコマンドでは、Modbus プロトコルが有効になります。

```
config:#    network services modbus enabled true
```

読み取り専用モードの有効化または無効化

次のコマンド構文では、Modbus エージェントの読み取り専用モードを有効または無効にできます。

```
config:#    network services modbus read-only <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *true* または *false*。

オプション	説明
true	読み取り専用モードを有効にします。
false	読み取り専用モードを無効にします。

例

次のコマンドでは、Modbus エージェントの読み取り専用モードを無効にします。

```
config:#    network services modbus read-only false
```

Modbus ポートの変更

次のコマンド構文では、Modbus ポートを変更できます。

```
config:#    network services modbus port <n>
```

変数:

- <n> は、1 ~ 65535 の TCP ポート番号です。デフォルトの Modbus ポートは 502 です。

例

次のコマンドでは、Modbus ポートを変更できます。

```
config:#    network services modbus port 600
```

サービス アドバタイズメントの有効化または無効化

次のコマンド構文では、ネットワーク サービスのアドバタイズメントまたは自動検出を有効にするゼロ構成プロトコルを有効または無効にします。詳細については、「**サービス アドバタイズメントの有効化**『103p. 』」を参照してください。

```
config:#    network services zeroconfig enabled <option>
```

変数:

- <option> は、次のいずれかのオプションです。true または false。

オプション	説明
true	ゼロ構成プロトコルが有効になります。
false	ゼロ構成プロトコルが無効になります。

例

次のコマンドでは、ゼロ構成プロトコルが有効になります。

```
config:#    network services zeroconfig enabled true
```

時刻設定コマンド

時刻設定コマンドは、time で始まります。

時刻の設定方法の決定

次のコマンド構文では、システムの日時の設定方法を指定できます。

```
config:#    time method <method>
```

変数:

- <method> は、次のいずれかの時刻設定オプションです。 *manual* または *ntp*。

モード	説明
manual	日付と時刻の設定がカスタマイズされます。
ntp	日付と時刻の設定は、指定した NTP サーバと同期されます。

例

次のコマンドでは、NTP サーバを使用して日付と時刻を設定します。

```
config:#    time method ntp
```

NTP パラメータの設定

NTP パラメータの設定に使用される時刻設定コマンドは、*time ntp* で始まります。

プライマリ NTP サーバの指定

次のコマンド構文では、NTP サーバとの同期を有効にしている場合のプライマリ タイム サーバを指定できます。

```
config:#    time ntp firstServer <first_server>
```

変数:

- <first_server> は、プライマリ NTP サーバの IP アドレスまたはホスト名です。

例

次のコマンドでは、プライマリ タイム サーバが 192.168.80.66 に設定されます。

```
config:#    time ntp firstServer 192.168.80.66
```

セカンダリ NTP サーバの指定

次のコマンド構文では、NTP サーバとの同期を有効にしている場合のセカンダリ タイム サーバを指定できます。

```
config:#    time ntp secondServer <second_server>
```

変数:

- <second_server> は、セカンダリ NTP サーバの IP アドレスまたはホスト名です。

例

次のコマンドでは、セカンダリ タイム サーバが 192.168.80.78 に設定されます。

```
config:#    time ntp secondServer 192.168.80.78
```

DHCP によって割り当てられた NTP サーバの上書き

次のコマンド構文では、カスタマイズされた NTP サーバ設定で DHCP によって指定された NTP サーバを上書きするかどうかを指定できます。

```
config:#    time ntp overrideDHCPProvidedServer <option>
```

変数:

- <option> は、次のいずれかのオプションです。true または false。

モード	説明
true	カスタマイズされた NTP サーバ設定で、DHCP によって指定された NTP サーバを上書きします。
false	カスタマイズされた NTP サーバ設定で、DHCP によって指定された NTP サーバを上書きしません。

例

次のコマンドでは、DHCP によって指定された NTP サーバを、プライマリおよびセカンダリ NTP サーバなどのカスタマイズされた NTP サーバで上書きできます。

```
config:#    time ntp overrideDHCPProvidedServer true
```

セキュリティ設定コマンド

セキュリティ設定コマンドは、*security* で始まります。

ファイアウォール制御

CLI を使用してファイアウォール制御機能を管理できます。ファイアウォール制御を使用すると、特定の IP アドレスまたは IP アドレスの範囲からの Dominion PX へのアクセスを許可または拒否するルールを設定できます。

- IPv4 ファイアウォール設定コマンドは、*security ipAccessControl ipv4* で始まります。
- IPv6 ファイアウォール設定コマンドは、*security ipAccessControl ipv6* で始まります。

ファイアウォール制御パラメータの変更

ファイアウォール制御パラメータを変更するための各種コマンドがあります。

- IPv4 コマンド

- ▶ **IPv4** ファイアウォール制御機能を有効または無効にするには、次のコマンド構文を使用します。

```
config:# security ipAccessControl ipv4 enabled <option>
```

- ▶ デフォルトの **IPv4** ファイアウォール制御ポリシーを指定するには、次のコマンド構文を使用します。

```
config:# security ipAccessControl ipv4 defaultPolicy <policy>
```

- IPv6 コマンド

- ▶ **IPv6** ファイアウォール制御機能を有効または無効にするには、次のコマンド構文を使用します。

```
config:# security ipAccessControl ipv6 enabled <option>
```

- ▶ デフォルトの **IPv6** ファイアウォール制御ポリシーを指定するには、次のコマンド構文を使用します。

```
config:# security ipAccessControl ipv6 defaultPolicy <policy>
```

変数:

- <option> は、次のいずれかのオプションです。 *true* または *false*。

オプション	説明
true	IP アクセス コントロール機能を有効にします。
false	IP アクセス コントロール機能を無効にします。

- <policy> は、*accept*、*drop*、または *reject* のいずれかです。

オプション	説明
accept	すべての IP アドレスからのトラフィックを受け入れます。

オプション	説明
drop	エラー通知を送信元ホストに送信せずにすべての IP アドレスからのトラフィックを破棄します。
reject	すべての IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージを送信元ホストに送信されます。

ヒント: 両方のコマンドを組み合わせ、すべてのファイアウォール制御パラメータを一度に変更できます。「マルチコマンド構文 『422p. 』」を参照してください。

例

次のコマンドでは、IPv4 アクセス制御機能の 2 つのパラメータを設定します。

```
config:# security ipAccessControl ipv4 enabled true defaultPolicy accept
```

結果:

- IPv4 アクセス制御機能が有効になります。
- デフォルト ポリシーは「accept」に設定されます。

ファイアウォールのルール管理

CLI コマンドを使用してファイアウォール ルールを追加、削除、または変更できます。

- IPv4 ファイアウォール制御ルール コマンドは、*security ipAccessControl ipv4 rule* で始まります。
- IPv6 ファイアウォール制御ルール コマンドは、*security ipAccessControl ipv6 rule* で始まります。

ファイアウォール ルールの追加

新しいファイアウォール ルールをリストのどこに追加するかによって、ルールを追加するコマンド構文は異なります。

- IPv4 コマンド
 - ▶ 新しい IPv4 ルールをルール リストの一番下に追加するには、次のコマンド構文を使用します。

```
config:# security ipAccessControl ipv4 rule add <ip_mask> <policy>
```

- ▶ 新しい IPv4 ルールを特定のルールの上または下に挿入して追加するには、次のコマンド構文を使用します。

```
config:# security ipAccessControl ipv4 rule add <ip_mask> <policy> <insert>
<rule_number>
```

-- または --

```
config:# security ipAccessControl ipv4 rule add <insert> <rule_number> <ip_mask>
<policy>
```

- IPv6 コマンド

- ▶ 新しい IPv6 ルールをルール リストの一番下に追加するには、次のコマンド構文を使用します。

```
config:# security ipAccessControl ipv6 rule add <ip_mask> <policy>
```

- ▶ 新しい IPv6 ルールを特定のルールの上または下に挿入して追加するには、次のコマンド構文を使用します。

```
config:# security ipAccessControl ipv6 rule add <ip_mask> <policy> <insert> <rule_number>
```

-- または --

```
config:# security ipAccessControl ipv6 rule add <insert> <rule_number> <ip_mask> <policy>
```

変数:

- <ip_mask> は、IP アドレスとサブネット マスク値の組み合わせです。各組み合わせの間を、スラッシュで区切ります。たとえば、IPv4 の組み合わせは、次のようになります: 192.168.94.222/24.
- <policy> は、accept、drop、または reject のいずれかです。

ポリシー	説明
accept	指定された IP アドレスからのトラフィックを受け入れます。
drop	エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。

ポリシー	説明
reject	指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。

- <insert> は、*insertAbove* または *insertBelow* のいずれかです。

オプション	説明
insertAbove	指定されたルール番号の上に新しいルール番号を挿入します。次のようにします。 新しいルール番号 = 指定されたルール番号
insertBelow	指定されたルール番号の下に新しいルール番号を挿入します。次のようにします。 新しいルール番号 = 指定されたルール番号 + 1

- <rule_number> は、新しいルールを上または下に挿入する既存のルールの番号です。

例

次のコマンドでは、新しい IPv4 アクセス制御ルールが追加され、リストにおけるそのルールの位置が指定されます。

```
config:# security ipAccessControl ipv4 rule add 192.168.84.123/24 accept
insertAbove 5
```

結果:

- IPv4 アドレス 192.168.84.123 からのすべてのパケットを許可する新しい IPv4 ファイアウォール制御ルールが追加されます。
- 新しく追加したルールは、5 番目のルールの上に挿入されます。つまり、新しいルールが 5 番目のルールになり、元の 5 番目のルールが 6 番目のルールになります。

ファイアウォール ルールの変更

既存のルールのどの内容を変更するかによって、コマンド構文が異なります。

- IPv4 コマンド

- ▶ **IPv4 ルールの IP アドレスやサブネット マスクを変更するコマンド構文は、次のとおりです。**

```
config:# security ipAccessControl ipv4 rule modify <rule_number> ipMask <ip_mask>
```

- ▶ IPv4 ルールのポリシーを変更するコマンド構文は、次のとおりです。
 - 。

```
config:# security ipAccessControl ipv4 rule modify <rule_number> policy <policy>
```

- ▶ 既存の IPv4 ルールの内容をすべて変更するコマンド構文は、次のとおりです。

```
config:# security ipAccessControl ipv4 rule modify <rule_number> ipMask <ip_mask>  
policy <policy>
```

- IPv6 コマンド

- ▶ IPv6 ルールの IP アドレスやサブネット マスクを変更するコマンド構文は、次のとおりです。

```
config:# security ipAccessControl ipv6 rule modify <rule_number> ipMask <ip_mask>
```

- ▶ IPv6 ルールのポリシーを変更するコマンド構文は、次のとおりです。
 - 。

```
config:# security ipAccessControl ipv6 rule modify <rule_number> policy <policy>
```

- ▶ 既存の IPv6 ルールの内容をすべて変更するコマンド構文は、次のとおりです。

```
config:# security ipAccessControl ipv6 rule modify <rule_number> ipMask <ip_mask>
policy <policy>
```

変数:

- <rule_number> は、変更する既存のルールの番号です。
- <ip_mask> は、IP アドレスとサブネット マスク値の組み合わせです。各組み合わせの間を、スラッシュで区切ります。たとえば、IPv4 の組み合わせは、次のようになります: *192.168.94.222/24*。
- <policy> は、*accept*、*drop*、または *reject* のいずれかです。

オプション	説明
accept	指定された IP アドレスからのトラフィックを受け入れます。
drop	エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。
reject	指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージを送信元ホストに送信されます。

例

次のコマンドでは、5 番目の IPv4 ルールの内容がすべて変更されます。

```
config:# security ipAccessControl ipv4 rule modify 5 ipMask 192.168.84.123/24
policy accept
```

結果:

- IPv4 アドレスは 192.168.84.123 に変更され、サブネット マスクは 255.255.255.0 に変更されます。
- ポリシーは「accept」になります。

ファイアウォール ルールの削除

次のコマンドは、特定の IPv4 または IPv6 ルールをリストから削除します。

- IPv4 コマンド

```
config:# security ipAccessControl ipv4 rule delete <rule_number>
```

- IPv6 コマンド

```
config:# security ipAccessControl ipv6 rule delete <rule_number>
```

変数:

- <rule_number> は、削除する既存のルール番号です。

例

次のコマンドでは、IPv6 アクセス制御リストから 5 番目のルールが削除されます。

```
config:# security ipAccessControl ipv6 rule delete 5
```

HTTPS アクセス

次のコマンドでは、Dominion PX Web インタフェースへの HTTPS アクセスを強制するかどうかを指定できます。強制する場合、すべての HTTP アクセスは自動的に HTTPS に送信されます。

```
config:# security enforceHttpsForWebAccess <option>
```

変数:

- <option> は、次のいずれかのオプションです。enable または disable。

オプション	説明
enable	Web インタフェースへの HTTPS アクセスを有効にします。
disable	Web インタフェースへの HTTPS アクセスを無効にします。

例

次のコマンドでは、HTTPS アクセス機能が無効になります。

```
config:# security enforceHttpsForWebAccess disable
```


ログイン制限

ログイン制限機能では、ログイン関連の制限（パスワード エージング、同じユーザ名を使用した同時ログイン、ログアウトを強制するまでのアイドル時間など）を制御します。

ログイン制限コマンドは、*security loginLimits* で始まります。

複数のコマンドを組み合わせ、ログイン制限パラメータを一度に変更できます。「**マルチコマンド構文**『422p. 』」を参照してください。

シングル ログイン制限

次のコマンド構文では、シングル ログイン機能を有効または無効にして、同じログイン名を同時に使用した複数のログインを許可するかどうかを制御できます。

```
config:# security loginLimits singleLogin <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *enable* または *disable*。

オプション	説明
enable	シングル ログイン機能を有効にします。
disable	シングル ログイン機能を無効にします。

例

次のコマンドでは、シングル ログイン機能を無効にして、複数のユーザが同じユーザ名を同時に使用してログインできるようにします。

```
config:# security loginLimits singleLogin disable
```

パスワード エージング

次のコマンド構文では、パスワード エージング機能を有効または無効にして、パスワードの定期的な変更を要求するかどうかを制御できます。

```
config:# security loginLimits passwordAging <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *enable* または *disable*。

オプション	説明
enable	パスワード エージング機能を有効にします。
disable	パスワード エージング機能を無効にします。

例

次のコマンドでは、パスワード エージング機能が有効になります。

```
config:# security loginLimits passwordAging enable
```

パスワード エージング間隔

次のコマンド構文では、パスワードを変更する頻度を指定できます。

```
config:# security loginLimits passwordAgingInterval <value>
```

変数:

- <value> は、パスワード エージング間隔に設定する数値（日数）です。間隔の範囲は 7 ～ 365 日です。

例

次のコマンドでは、パスワード エージング間隔が 90 日に設定されます。

```
config:# security loginLimits passwordAgingInterval 90
```

アイドル タイムアウト

次のコマンド構文では、アイドル状態のユーザが Dominion PX Web インタフェースから強制的にログアウトされるまでの時間を指定できます。

```
config:# security loginLimits idleTimeout <value>
```

変数:

- <value> は、アイドル タイムアウトに設定する数値 (分) です。タイムアウトの範囲は 1 ~ 1440 分 (24 時間) です。

例

次のコマンドでは、アイドル タイムアウトが 10 分に設定されます。

```
config:# security loginLimits idleTimeout 10
```

ユーザ ブロック

さまざまなユーザ ブロック パラメータを変更するための各種コマンドがあります。これらのコマンドは、security userBlocking で始まります。

- ▶ ユーザをブロックするまでのログイン失敗の最大数を指定するには、次のコマンド構文を使用します。

```
config:# security userBlocking maximumNumberOfFailedLogins <value1>
```

- ▶ ユーザのログインをブロックする時間を指定するには、次のコマンド構文を使用します。

```
config:# security userBlocking blockTime <value2>
```

変数:

- <value1> は、3 ~ 10 の整数、またはログイン失敗の最大数に制限を設定せずにユーザ ブロック機能を無効にする *unlimited* です。
- <value2> は数値 (分) です。

ヒント: 複数のコマンドを組み合わせ、ユーザ ブロック パラメータを一度に変更できます。「マルチコマンド構文 [422p.]」を参照してください。

例

次のコマンドでは、2 つのユーザ ブロック パラメータが設定されます。

```
config:# security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

結果:

- ログイン失敗の最大数が 5 に設定されます。
- ユーザ ブロック時間は 30 分に設定されます。

強力なパスワード

強力なパスワード コマンドでは、ログインに強力なパスワードを要求するかどうか、および強力なパスワードの最低文字数を指定できます。

強力なパスワード コマンドは、`security strongPasswords` で始まります。

複数の強力なパスワード コマンドを組み合わせ、さまざまなパラメータを一度に変更できます。「[マルチコマンド構文『422p.』](#)」を参照してください。

強力なパスワードの有効化または無効化

次のコマンド構文では、強力なパスワード機能の有効/無効を切り替えることができます。

```
config:# security strongPasswords enabled <option>
```

変数:

- <option> は、次のいずれかのオプションです。 `true` または `false`。

オプション	説明
true	強力なパスワード機能を有効にします。
false	強力なパスワード機能を無効にします。

例

次のコマンド構文では、強力なパスワード機能が有効になります。

```
config:# security strongPasswords enabled true
```

パスワードの最小長

次のコマンド構文では、パスワードの最小長を指定できます。

```
config:# security strongPasswords minLength <value>
```

変数:

- <value> 値は、8 ～ 32 の整数です。

例

次のコマンド構文では、パスワードの最小長が 8 文字に指定されます。

```
config:# security strongPasswords minLength 8
```

パスワードの最大長

次のコマンド構文では、パスワードの最大長を指定できます。

```
config:# security strongPasswords maxLength <value>
```

変数:

- <value> 値は、16 ～ 64 の整数です。

例

次のコマンド構文では、パスワードの最大長が 20 文字に指定されます。

```
config:# security strongPasswords maxLength 20
```

小文字の要件

次のコマンド構文では、強力なパスワードに少なくとも 1 つの小文字を含めるかどうかを指定できます。

```
config:# security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *enable* または *disable*。

オプション	説明
enable	1 文字以上の小文字が必要です。
disable	小文字は必要ありません。

例

次のコマンド構文では、パスワードに少なくとも 1 つの小文字が必要であることが指定されます。

```
config:# security strongPasswords enforceAtLeastOneLowerCaseCharacter enable
```

大文字の要件

次のコマンド構文では、強力なパスワードに少なくとも 1 つの大文字を含めるかどうかを指定できます。

```
config:# security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *enable* または *disable*。

オプション	説明
enable	1 文字以上の大文字が必要です。
disable	大文字は必要ありません。

例

次のコマンドでは、パスワードに少なくとも 1 つの大文字が必要であることが指定されます。

```
config:# security strongPasswords enforceAtLeastOneUpperCaseCharacter enable
```

数字の要件

次のコマンド構文では、強力なパスワードに少なくとも 1 つの数字を含めるかどうかを指定できます。

```
config:# security strongPasswords enforceAtLeastOneNumericCharacter <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *enable* または *disable*。

オプション	説明
enable	1 文字以上の数字が必要です。

オプション	説明
disable	数字は必要ありません。

例

次のコマンドでは、パスワードに少なくとも 1 つの数字が必要であることが指定されます。

```
config:# security strongPasswords enforceAtLeastOneNumericCharacter enable
```

特殊文字の要件

次のコマンド構文では、強力なパスワードに少なくとも 1 つの特殊文字を含めるかどうかを指定できます。

```
config:# security strongPasswords enforceAtLeastOneSpecialCharacter <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *enable* または *disable*。

オプション	説明
enable	1 文字以上の特殊文字が必要です。
disable	特殊文字は必要ありません。

例

次のコマンドでは、パスワードに少なくとも 1 つの特殊文字が必要であることが指定されます。

```
config:# security strongPasswords enforceAtLeastOneSpecialCharacter enable
```

パスワード履歴の最大数

次のコマンド構文では、パスワードを変更するときに繰り返すことのできない過去のパスワードの数を指定できます。

```
config:# security strongPasswords passwordHistoryDepth <value>
```

変数:

- <value> 値は、1 ～ 12 の整数です。

例

次のコマンドでは、パスワードを変更するときに再利用できない過去のパスワードの数が 7 に設定されます。

```
config:# security strongPasswords passwordHistoryDepth 7
```

役割ベースのアクセス制御

IP アドレスに基づくファイアウォール アクセス制御に加えて、IP アドレスとユーザの役割に基づく他のアクセス制御ルールを設定できます。

- IPv4 の役割ベースのアクセス制御コマンドは、*security roleBasedAccessControl ipv4* で始まります。
- IPv6 の役割ベースのアクセス制御コマンドは、*security roleBasedAccessControl ipv6* で始まります。

役割ベースのアクセス制御パラメータの変更

役割ベースのアクセス制御パラメータを変更するための各種コマンドがあります。

- IPv4 コマンド
 - ▶ **IPv4 の役割ベースのアクセス制御機能を有効または無効にするには、次のコマンド構文を使用します。**

```
config:# security roleBasedAccessControl ipv4 enabled <option>
```

- ▶ **IPv4 役割ベースのアクセス制御ポリシーを指定するには、次のコマンド構文を使用します。**


```
config:# security roleBasedAccessControl ipv4 defaultPolicy <policy>
```

- IPv6 コマンド

- ▶ **IPv6** の役割ベースのアクセス制御機能を有効または無効にするには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv6 enabled <option>
```

- ▶ **IPv6** 役割ベースのアクセス制御ポリシーを指定するには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv6 defaultPolicy <policy>
```

変数:

- <option> は、次のいずれかのオプションです。 *true* または *false*。

オプション	説明
true	役割ベースのアクセス制御機能を有効にします。
false	役割ベースのアクセス制御機能を無効にします。

- <policy> は、*allow* または *deny* のいずれかです。

ポリシー	説明
allow	ユーザの役割にかかわらず、すべての IP アドレスからのトラフィックを受け入れます。
deny	ユーザの役割にかかわらず、すべての IP アドレスからのトラフィックを破棄します。

ヒント: 両方のコマンドを組み合わせて、すべての役割ベースのアクセス制御パラメータを一度に変更できます。『マルチコマンド構文』[422p.] を参照してください。

例

次のコマンドでは、役割ベースの IPv4 アクセス制御機能の 2 つのパラメータを設定します。

```
config:# security roleBasedAccessControl ipv4 enabled true defaultPolicy allow
```

結果:

- 役割ベースの IPv4 アクセス制御機能が有効になります。
- デフォルト ポリシーは「allow」に設定されます。

役割ベースのアクセス制御ルールの管理

役割ベースのアクセス制御ルールを追加、削除、または変更できます。

- ルールを管理するための IPv4 の役割ベースのアクセス制御コマンドは、*security roleBasedAccessControl ipv4 rule* で始まります。
- ルールを管理するための IPv6 の役割ベースのアクセス制御コマンドは、*security roleBasedAccessControl ipv6 rule* で始まります。

役割ベースのアクセス制御ルールの追加

新しいルールをリストのどこに追加するかによって、ルールを追加するコマンド構文は異なります。

- IPv4 コマンド

- ▶ 新しい IPv4 ルールをルール リストの一番下に追加するには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role> <policy>
```

- ▶ 新しい IPv4 ルールを特定のルールの上または下に挿入して追加するには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role> <policy>  
<insert> <rule_number>
```

- IPv6 コマンド

- ▶ 新しい IPv6 ルールをルール リストの一番下に追加するには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role> <policy>
```

- ▶ 新しい IPv6 ルールを特定のルールの上または下に挿入して追加するには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role> <policy>
<insert> <rule_number>
```

変数:

- <start_ip> は、開始 IP アドレスです。
- <end_ip> は、終了 IP アドレスです。
- <role> は、アクセス制御ルールを作成する役割です。
- <policy> は、*allow* または *deny* のいずれかです。

ポリシー	説明
allow	ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを受け入れます。
deny	ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを破棄します。

- <insert> は、*insertAbove* または *insertBelow* のいずれかです。

オプション	説明
insertAbove	指定されたルール番号の上に新しいルール番号を挿入します。次のようにします。 新しいルール番号 = 指定されたルール番号
insertBelow	指定されたルール番号の下に新しいルール番号を挿入します。次のようにします。 新しいルール番号 = 指定されたルール番号 + 1

- <rule_number> は、新しいルールを上または下に挿入する既存のルールの番号です。

例

次のコマンドでは、新しい IPv4 役割ベースのアクセス制御ルールが作成され、リストにおけるそのルールの位置が指定されます。

```
config:# security roleBasedAccessControl ipv4 rule add 192.168.78.50 192.168.90.100 admin deny insertAbove 3
```

結果:

- ユーザが役割「admin」のメンバーである場合に 192.168.78.50 と 192.168.90.100 の間にある IPv4 アドレスからのすべてのパケットを破棄する新しい IPv4 の役割ベースのアクセス制御ルールが追加されます。
- 新しく追加した IPv4 ルールは、3 番目のルールの上に挿入されます。つまり、新しいルールが 3 番目のルールになり、元の 3 番目のルールが 4 番目のルールになります。

役割ベースのアクセス制御ルールの変更

既存のルールのどの内容を変更するかによって、コマンド構文が異なります。

- IPv4 コマンド

▶ ルールの IPv4 アドレス範囲を変更するには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number> startIpAddress <start_ip> endIpAddress <end_ip>
```

▶ IPv4 ルールの役割を変更するには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number> role <role>
```

▶ IPv4 ルールのポリシーを変更するには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number> policy <policy>
```

▶ 既存の IPv4 ルールの内容をすべて変更するには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number>
startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

- IPv6 コマンド

- ▶ ルールの IPv6 アドレス範囲を変更するには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number>
startIpAddress <start_ip> endIpAddress <end_ip>
```

- ▶ IPv6 ルールの役割を変更するには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number> role <role>
```

- ▶ IPv6 ルールのポリシーを変更するには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number> policy
<policy>
```

- ▶ 既存の IPv6 ルールの内容をすべて変更するには、次のコマンド構文を使用します。

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number>
startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

変数:

- <rule_number> は、変更する既存のルールの番号です。
- <start_ip> は、開始 IP アドレスです。
- <end_ip> は、終了 IP アドレスです。
- <role> は、いずれかの既存の役割です。
- <policy> は、allow または deny のいずれかです。

ポリシー	説明
allow	ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを受け入れます。

ポリシー	説明
deny	ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを破棄します。

例

次のコマンドでは、8 番目の IPv4 ルールの内容がすべて変更されます。

```
config:# security roleBasedAccessControl ipv4 rule modify 8
startIpAddress 192.168.8.8 endIpAddress 192.168.90.90 role operator
policy allow
```

結果:

- 開始 IPv4 アドレスは 192.168.8.8 に変更され、終了 IPv4 アドレスは 192.168.90.90 に変更されます。
- 役割は、「operator」に変更されます。
- ポリシーは「allow」になります。

役割ベースのアクセス制御ルールの削除

次のコマンドでは、特定のルールをリストから削除できます。

- IPv4 コマンド

```
config:# security roleBasedAccessControl ipv4 rule delete <rule_number>
```

- IPv6 コマンド

```
config:# security roleBasedAccessControl ipv6 rule delete <rule_number>
```

変数:

- <rule_number> は、削除する既存のルールの番号です。

例

次のコマンドでは、7 番目の IPv6 ルールが削除されます。

```
config:# security roleBasedAccessControl ipv6 rule delete 7
```

アウトレット (コンセント) 設定コマンド

アウトレット (コンセント) 設定コマンドは、*outlet* で始まります。それらのコマンドで、個々のアウトレット (コンセント) の設定ができます。

アウトレット (コンセント) 名の変更

このコマンド構文では、アウトレット (コンセント) に名前を付けられます。

```
config:#    outlet <n> name "<name>"
```

変数:

- <n> は、設定するアウトレット (コンセント) の番号です。
- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。 <name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

例

次のコマンドでは、アウトレット (コンセント) 8 に「Win XP」という名前が割り当てられます。

```
config:#    outlet 8 name "Win XP"
```

アウトレット (コンセント) のデフォルト状態の変更

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

次のコマンド構文では、PDU の電源がオンになった後のアウトレット (コンセント) の初期電源状態を指定できます。

```
config:#    outlet <n> stateOnDeviceStartup <option>
```

変数:

- <n> は、設定するアウトレット (コンセント) の番号です。
- <option> は、次のいずれかのオプションです。 *off*、*on*、*lastKnownState*、および *pduDefined*。

オプション	説明
off	Dominion PX デバイスの電源がオンになったときに、アウトレット (コンセント) の電源をオフにします。
on	Dominion PX デバイスの電源がオンになったときに、アウトレット (コンセント) の電源をオンにします。
lastKnownState	PDU の電源がオンになったときに、アウトレット (コンセント) を、Dominion PX デバイスの電源がオフになる前のステータスに戻します。
pduDefined	アウトレット (コンセント) のデフォルト状態を、PDU 定義の設定に従って決定します。

注: アウトレット (コンセント) のデフォルト状態を *pduDefined* 以外のオプションに設定すると、そのアウトレット (コンセント) では、PDU 定義のデフォルト設定が上書きされます。「**アウトレット (コンセント) の PDU 定義のデフォルト状態の設定** [301p.]」を参照してください。

例

次のコマンドでは、PDU を再び電源オンにした後に、アウトレット (コンセント) 8 が PDU の電源がオフになる前の電源状態に戻ります。

```
config:#    outlet 8 stateOnDeviceStartup lastKnownState
```


アウトレット (コンセント) の電源再投入時の電源オフ時間の設定

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

次のコマンド構文では、特定のアウトレット (コンセント) に対して、電源再投入操作の電源オフ時間を設定できます。

```
config:#    outlet <n> cyclingPowerOffPeriod <timing>
```

変数:

- <n> は、設定するアウトレット (コンセント) の番号です。
- <timing> は、再投入時の電源オフ時間の秒数で、0 ～ 3600 の整数です。

注: この設定では、特定のアウトレット (コンセント) の PDU 定義の電源再投入時の電源オフ時間が上書きされます。『PDU 定義の電源再投入時の電源オフ時間の設定 』302p. 』を参照してください。

例

次のコマンドでは、電源再投入操作を実行したときのアウトレット (コンセント) 8 の電源オフ時間を 3 秒に設定できます。

```
config:#    outlet 8 cyclingPowerOffPeriod 3
```

インレット設定コマンド

インレット設定コマンドは、*inlet* で始まります。インレット設定コマンドを使用して、インレットの設定ができます。

インレット名の変更

このコマンド構文では、インレットに名前を付けられます。

```
config:#    inlet <n> name "<name>"
```

変数:

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。この値は、1 ～ 50 の整数です。
- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。<name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

例

次のコマンドでは、inlet 1 に名前「AC source」が割り当てられます。Dominion PX デバイスに複数のインレットが含まれている場合、次のコマンドでは、最初のインレットに名前が付けられます。

```
config:#    inlet 1 name "AC source"
```

サーキット ブレーカ設定コマンド

サーキット ブレーカ設定コマンドは、*ocp* で始まります。このコマンドでは、個々のサーキット ブレーカが設定されます。

サーキット ブレーカ名の変更

次のコマンド構文では、サーキット ブレーカの名前を変更できます。

```
config:#    ocp <n> name "<name>"
```

変数:

- <n> は、設定するサーキット ブレーカの番号です。この値は、1 ～ 50 の整数です。
- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。<name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

例

次のコマンドでは、サーキット ブレーカ 3 に「Email servers CB」という名前が割り当てられます。

```
config:# ocp 3 name "Email servers CB"
```

環境センサー設定コマンド

環境センサー設定コマンドは、*externalsensor* で始まります。個々の環境センサーの名前と場所のパラメータを設定できます。

センサー名の変更

このコマンド構文では、環境センサーに名前が付けられます。

```
config:# externalsensor <n> name "<name>"
```

変数:

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Dominion PX の Web インタフェースに表示されます。値は、1 ～ 16 の整数です。
- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。<name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

例

次のコマンドでは、ID 番号 4 の環境センサーに「Cabinet humidity」という名前が割り当てられます。

```
config:# externalsensor 4 name "Cabinet humidity"
```

センサー タイプの指定

Raritan の接点閉鎖センサー (DPX-CC2-TR) では、さまざまなサードパーティ製検出装置/スイッチの接続がサポートされています。正しく動作させるために、接続済みの検出装置/スイッチのタイプを指定する必要があります。センサー タイプを指定する必要がある場合は、次のコマンド構文を使用します。

```
config:#    externalsensor <n> sensorSubType <type>
```

変数:

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Dominion PX の Web インタフェースに表示されます。値は、1 ～ 16 の整数です。
- <type> は、*contact*、*smokeDetection*、*waterDetection*、または *vibration* のいずれかのタイプです。

タイプ	説明
contact	接続されている検出装置/スイッチは、扉施錠状態または扉開閉状態の検出用です。
smokeDetection	接続されている検出装置/スイッチは、煙の検出用です。
waterDetection	接続されている検出装置/スイッチは、水の検出用です。
vibration	接続されている検出装置/スイッチは、振動の検出用です。

例

次に、Dominion PX Web インタフェースに ID 番号が 2 と表示される Raritan の接点閉鎖センサー (DPX-CC2-TR) に煙検出装置を接続する例を示します。

```
config:#    externalsensor 2 sensorSubType smokeDetection
```

X 座標の設定

次のコマンド構文では、環境センサーの X 座標を指定できます。

```
config:#    externalsensor <n> xlabel "<coordinate>"
```

変数:

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Dominion PX の Web インタフェースに表示されます。値は、1 ～ 16 の整数です。
- <coordinate> は、最大 24 文字の ASCII の表示可能文字で構成される文字列であり、引用符で囲む必要があります。

例

次のコマンドでは、ID 番号 4 の環境センサーの X 座標に値「The 2nd cabinet」が設定されます。

```
config:#    externalsensor 4 xlabel "The 2nd cabinet"
```

Y 座標の設定

次のコマンド構文では、環境センサーの Y 座標を指定できます。

```
config:#    externalsensor <n> ylabel "<coordinate>"
```

変数:

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Dominion PX の Web インタフェースに表示されます。値は、1 ～ 16 の整数です。
- <coordinate> は、最大 24 文字の ASCII の表示可能文字で構成される文字列であり、引用符で囲む必要があります。

例

次のコマンドでは、ID 番号 4 の環境センサーの Y 座標に値「The 4th row」が設定されます。

```
config:#    externalsensor 4 ylabel "The 4th row"
```

Z 座標の設定

次のコマンド構文では、環境センサーの Z 座標を指定できます。

```
config:#          externalsensor <n> zlabel "<coordinate>"
```

変数:

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Dominion PX の Web インタフェースに表示されます。値は、1 ～ 16 の整数です。
- 設定した Z 座標の形式に応じて、<coordinate> 変数には 2 つのタイプの値があります。

タイプ	説明
自由形式	<coordinate> は、最大 24 文字の ASCII の表示可能文字で構成される文字列であり、引用符で囲む必要があります。
ラック ユニ ット	<coordinate> は、ラック ユニット内の整数値です。

注: Z 座標は、ラック ユニットを使用して指定できます。『環境センサーの Z 座標形式の設定』[\[307p.\]](#)」を参照してください。

例

Z 座標の形式が *freeForm* に設定されると、次のコマンドでは、ID 番号 4 の環境センサーの Z 座標に値「The 5th rack」が設定されます。

```
config:#          externalsensor 4 zlabel "The 5th rack"
```

センサーの説明の変更

次のコマンド構文では、特定の環境センサーの説明を指定できます。

```
config:#    externalsensor <n> description "<description>"
```

変数:

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Dominion PX の Web インタフェースに表示されます。値は、1 ～ 16 の整数です。
- <description> は、最大 64 文字の ASCII の表示可能文字で構成される文字列であり、引用符で囲む必要があります。

例

次のコマンドでは、ID 番号 4 の環境センサーに「humidity detection」という説明が付けられます。

```
config:#    externalsensor 4 description "humidity detection"
```

センサーしきい値設定コマンド

センサー設定コマンドは、*sensor* で始まります。このコマンドを使用すると、次の項目に関連付けられているセンサーのしきい値、ヒステリシス値、およびアサート タイムアウトを設定できます。

- Inlets (インレット)
- インレットの極 (3 相 PDU のみ)
- サーキット ブレーカ
- 環境センサー

しきい値が有効になっているかどうかを問わず、いつでもしきい値に新しい値を割り当てることができます。

インレット センサー用のコマンド

インレットのセンサー設定コマンドは、*sensor inlet* で始まります。

インレットの上位臨界しきい値の設定

次のコマンド構文では、インレットの上位臨界しきいを設定できます。

```
config:#    sensor inlet <n> <sensor type> upperCritical <option>
```

変数:

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

注:要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定したインレット センサーの上位臨界しきい値を有効にします。
disable	指定したインレット センサーの上位臨界しきい値を無効にします。
数値	指定したインレット センサーの上位臨界しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、インレット 1 の RMS 電流の上位臨界しきい値が有効になります。

```
config:#    sensor inlet 1 current upperCritical enable
```

インレットの上位警告しきい値の設定

次のコマンド構文では、インレットの上位警告しきい値を設定できます。

```
config:#    sensor inlet <n> <sensor type> upperWarning <option>
```

変数:

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

注:要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定したインレット センサーの上位警告しきい値を有効にします。
disable	指定したインレット センサーの上位警告しきい値を無効にします。
数値	指定したインレット センサーの上位警告しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、インレット 1 の RMS 電流の上位警告しきい値が 12A に設定されます。上位警告しきい値がまだ有効になっていない場合は、このしきい値も有効になります。

```
config:#    sensor inlet 1 current upperWarning 12
```

インレットの下位臨界しきい値の設定

次のコマンド構文では、インレットの下位臨界しきい値を設定できます。

```
config:#    sensor inlet <n> <sensor type> lowerCritical <option>
```

変数:

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

注: 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定したインレット センサーの下位臨界しきい値を有効にします。
disable	指定したインレット センサーの下位臨界しきい値を無効にします。

オプション	説明
数値	指定したインレット センサーの下位臨界しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、インレット 1 の RMS 電流の下位臨界しきい値が無効になります。

```
config:#    sensor inlet 1 current lowerCritical disable
```

インレットの下位警告しきい値の設定

次のコマンド構文では、インレットの下位警告しきい値を設定できます。

```
config:#    sensor inlet <n> <sensor type> lowerWarning <option>
```

変数:

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

注:要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定したインレット センサーの下位警告しきい値を有効にします。
disable	指定したインレット センサーの下位警告しきい値を無効にします。
数値	指定したインレット センサーの下位警告しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、インレット 1 の RMS 電流の下位警告しきい値が 20A に設定されます。下位警告しきい値がまだ有効になっていない場合は、このしきい値も有効になります。

```
config:#    sensor inlet 1 current lowerWarning 20
```

インレットのアサート停止ヒステリシスの設定

次のコマンド構文では、インレットのアサート停止ヒステリシス値を設定できます。

```
config:#    sensor inlet <n> <sensor type> hysteresis <value>
```

変数:

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー

センサー タイプ	説明
unbalancedCurrent	不平衡負荷センサー

注:要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <value> は、指定したインレット センサーのヒステリシスに割り当てられる数値です。アサート停止ヒステリシスの機能については、「アサート停止ヒステリシスとは『177p.』」を参照してください。

例

次のコマンドでは、インレット 1 の RMS 電流のアサート停止ヒステリシスが 0.2A に設定されます。つまり、しきい値超過イベントのアサートが停止されるまで、電流が上位しきい値より少なくとも 0.2A 低下するか、下位しきい値より少なくとも 0.2A 上昇する必要があります。

```
config:#    sensor inlet 1 current hysteresis 0.2
```

インレットのアサート タイムアウトの設定

次のコマンド構文では、インレットのアサート タイムアウト値を設定できます。

```
config:#    sensor inlet <n> <sensor type> assertionTimeout <value>
```

変数:

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

注: 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <value> は、指定したインレット センサーのアサート タイムアウトに割り当てられるサンプルの数です。「アサート タイムアウトとは『178p. 』」を参照してください。

例

次のコマンドでは、インレット 1 の RMS 電流のアサート タイムアウト値が 4 サンプルに設定されます。つまり、しきい値超過イベントがアサートされるまでに、少なくとも 4 つの連続したサンプルが特定の電流しきい値を超える必要があります。

```
config:#    sensor inlet 1 current assertionTimeout 4
```

インレットの極センサー用のコマンド

インレットの極のセンサー設定コマンドは、*sensor inletpole* で始まります。このタイプのコマンドは、3 相 PDU でのみ使用できます。

インレットの極の上位臨界しきい値の設定

次のコマンド構文では、インレットの極の上位臨界しきい値を設定できます。

```
config:#    sensor inletpole <n> <p> <sensor type> upperCritical <option>
```

変数:

- <n> は、極センサーを設定するインレットの番号です。
- <p> は、設定するインレットの極のラベルです。

極	ラベル <p>	電流センサー	電圧センサー
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー

センサー タイプ	説明
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

注: 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定したインレットの極センサーの上位臨界しきい値を有効にします。
disable	指定したインレットの極センサーの上位臨界しきい値を無効にします。
数値	指定したインレットの極センサーの上位臨界しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、インレット 1 の極 3 (L3-L1) の電圧に対する上位臨界しきい値が無効になります。

```
config:#    sensor inletpole 1 L3 voltage upperCritical disable
```

インレットの極の上位警告しきい値の設定

次のコマンド構文では、インレットの極の上位警告しきい値を設定できます。

```
config:#    sensor inletpole <n> <p> <sensor type> upperWarning <option>
```

変数:

- <n> は、極センサーを設定するインレットの番号です。
- <p> は、設定するインレットの極のラベルです。

極	ラベル <p>	電流センサー	電圧センサー
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

注:要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定したインレットの極センサーの上位警告しきい値を有効にします。
disable	指定したインレットの極センサーの上位警告しきい値を無効にします。
数値	指定したインレットの極センサーの上位警告しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、インレット 1 の極 2 (L2-L3) の電圧に対する上位警告しきい値に 180V が設定されます。上位警告しきい値がまだ有効になっていない場合は、このしきい値も有効になります。

```
config:#    sensor inletpole 1 L2 voltage upperWarning 180
```

インレットの極の下位臨界しきい値の設定

次のコマンド構文では、インレットの極の下位臨界しきい値を設定できます。

```
config:#    sensor inletpole <n> <p> <sensor type> lowerCritical <option>
```

変数:

- <n> は、極センサーを設定するインレットの番号です。
- <p> は、設定するインレットの極のラベルです。

極	ラベル <p>	電流センサー	電圧センサー
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

注: 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定したインレットの極センサーの下位臨界しきい値を有効にします。
disable	指定したインレットの極センサーの下位臨界しきい値を無効にします。
数値	指定したインレットの極センサーの下位臨界しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、インレット 1 の極 2 (L2-L3) の電圧に対する下位臨界しきい値が有効になります。

```
config:#    sensor inletpole 1 L2 voltage lowerCritical enable
```

インレットの極の下位警告しきい値の設定

次のコマンド構文では、インレットの極の下位警告しきい値を設定できます。

```
config:#    sensor inletpole <n> <p> <sensor type> lowerWarning <option>
```

変数:

- <n> は、極センサーを設定するインレットの番号です。
- <p> は、設定するインレットの極のラベルです。

極	ラベル <p>	電流センサー	電圧センサー
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー

センサー タイプ	説明
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

注:要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定したインレットの極センサーの下位警告しきい値を有効にします。
disable	指定したインレットの極センサーの下位警告しきい値を無効にします。
数値	指定したインレットの極センサーの下位警告しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、インレット 1 の極 3 (L3-L1) の電圧に対する下位警告しきい値が 190V に設定されます。下位警告しきい値がまだ有効になっていない場合は、このしきい値も有効になります。

```
config:#    sensor inletpole 1 L3 voltage lowerWarning 190
```

インレットの極のアサート停止ヒステリシスの設定

次のコマンド構文では、インレットの極のアサート停止ヒステリシス値を設定できます。

```
config:#    sensor inletpole <n> <p> <sensor type> hysteresis <value>
```

変数:

- <n> は、極センサーを設定するインレットの番号です。
- <p> は、設定するインレットの極のラベルです。

極	ラベル <p>	電流センサー	電圧センサー
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

注:要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <value> は、指定したインレットの極センサーのヒステリシスに割り当てられる数値です。アサート停止ヒステリシスの機能については、「アサート停止ヒステリシスとは『177p.』」を参照してください。

例

次のコマンドでは、インレット 1 の極 2 (L2) の電流に対するアサート停止ヒステリシスが 0.2A に設定されます。つまり、しきい値超過イベントのアサートが停止されるまで、電流が上位しきい値より少なくとも 0.2A 低下するか、下位しきい値より少なくとも 0.2A 上昇する必要があります。

```
config:#    sensor inletpole 1 L2 current hysteresis 0.2
```

インレットの極のアサート タイムアウトの設定

次のコマンド構文では、インレットの極のアサート タイムアウト値を設定できます。

```
config:#    sensor inletpole <n> <p> <sensor type> assertionTimeout <value>
```

変数:

- <n> は、極センサーを設定するインレットの番号です。
- <p> は、設定するインレットの極のラベルです。

極	ラベル <p>	電流センサー	電圧センサー
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

注: 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <value> は、指定したインレットの極センサーのアサート タイムアウトに割り当てられるサンプルの数です。「アサート タイムアウトとは『178p. 』」を参照してください。

例

次のコマンドでは、インレット 1 の極 2 (L2) の電流に対するアサート タイムアウト値が 4 サンプルに設定されます。つまり、しきい値超過イベントがアサートされるまでに、少なくとも 4 つの連続したサンプルが特定の電流しきい値を超える必要があります。

```
config:#    sensor inletpole 1 L2 current assertionTimeout 4
```

サーキット ブレーカ センサー用のコマンド

サーキット ブレーカのセンサー設定コマンドは、*sensor ocp* で始まります。

サーキット ブレーカの上位臨界しきい値の設定

次のコマンド構文では、サーキット ブレーカの上位臨界しきい値を設定できます。

```
config:#    sensor ocp <n> <sensor type> upperCritical <option>
```

変数:

- <n> は、設定するサーキット ブレーカの番号です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー

注:要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定したサーキット ブレーカ センサーの上位臨界しきい値を有効にします。

オプション	説明
disable	指定したサーキット ブレーカ センサーの上位臨界しきい値を無効にします。
数値	指定したサーキット ブレーカ センサーの上位臨界しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、3 番目のサーキット ブレーカの上位臨界しきい値が 16A に設定されます。上位臨界しきい値がまだ有効になっていない場合は、このしきい値も有効になります。

```
config:#    sensor ocp 3 current upperCritical 16
```

サーキット ブレーカの上位警告しきい値の設定

次のコマンド構文では、サーキット ブレーカの上位警告しきい値を設定できます。

```
config:#    sensor ocp <n> <sensor type> upperWarning <option>
```

変数:

- <n> は、設定するサーキット ブレーカの番号です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー

注:要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定したサーキット ブレーカ センサーの上位警告しきい値を有効にします。
disable	指定したサーキット ブレーカ センサーの上位警告しきい値を無効にします。

オプション	説明
数値	指定したサーキット ブレーカ センサーの上位警告しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、3 番目のサーキット ブレーカの上位警告しきい値が有効になります。

```
config:#    sensor ocp 3 current upperWarning enable
```

サーキット ブレーカの下位臨界しきい値の設定

次のコマンド構文では、サーキット ブレーカの下位臨界しきい値を設定できます。

```
config:#    sensor ocp <n> <sensor type> lowerCritical <option>
```

変数:

- <n> は、設定するサーキット ブレーカの番号です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー

注:要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定したサーキット ブレーカ センサーの下位臨界しきい値を有効にします。
disable	指定したサーキット ブレーカ センサーの下位臨界しきい値を無効にします。
数値	指定したサーキット ブレーカ センサーの下位臨界しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、3 番目のサーキット ブレーカの下位臨界しきい値が 5A に設定されます。下位臨界しきい値がまだ有効になっていない場合は、このしきい値も有効になります。

```
config:#    sensor ocp 3 current lowerCritical 5
```

サーキット ブレーカの下位警告しきい値の設定

次のコマンド構文では、サーキット ブレーカの下位警告しきい値を設定できます。

```
config:#    sensor ocp <n> <sensor type> lowerWarning <option>
```

変数:

- <n> は、設定するサーキット ブレーカの番号です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー

注:要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定したサーキット ブレーカ センサーの下位警告しきい値を有効にします。
disable	指定したサーキット ブレーカ センサーの下位警告しきい値を無効にします。
数値	指定したサーキット ブレーカ センサーの下位警告しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、3 番目のサーキット ブレーカの下位警告しきい値が有効になります。

```
config:#    sensor ocp 3 current lowerWarning enable
```

サーキット ブレーカのアサート停止ヒステリシスの設定

次のコマンド構文では、サーキット ブレーカのアサート停止ヒステリシス値を設定できます。

```
config:#    sensor ocp <n> <sensor type> hysteresis <value>
```

変数:

- <n> は、設定するサーキット ブレーカの番号です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー

注:要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <value> は、指定したサーキット ブレーカ センサーのヒステリシスに割り当てられる数値です。アサート停止ヒステリシスの機能については、「**アサート停止ヒステリシスとは『177p.』**」を参照してください。

例

次のコマンドでは、3 番目のサーキット ブレーカの RMS 電流のアサート停止ヒステリシスが 0.2A に設定されます。つまり、しきい値超過イベントのアサートが停止されるまで、電流が上位しきい値より少なくとも 0.2A 低下するか、下位しきい値より少なくとも 0.2A 上昇する必要があります。

```
config:#    sensor ocp 3 current hysteresis 0.2
```

サーキット ブレーカのアサート タイムアウトの設定

次のコマンド構文では、サーキット ブレーカのアサート タイムアウト値を設定できます。

```
config:#    sensor ocp <n> <sensor type> assertionTimeout <value>
```

変数:

- <n> は、設定するサーキット ブレーカの番号です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー

注:要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <value> は、指定したサーキット ブレーカ センサーのアサート タイムアウトに割り当てられるサンプルの数です。「**アサート タイムアウトとは**『178p.』」を参照してください。

例

次のコマンドでは、3 番目のサーキット ブレーカの RMS 電流のアサート タイムアウト値が 4 サンプルに設定されます。つまり、しきい値超過イベントがアサートされるまでに、少なくとも 4 つの連続したサンプルが特定の電流しきい値を超える必要があります。

```
config:#    sensor ocp 3 current assertionTimeout 4
```

環境センサー用のコマンド

環境センサーのセンサーしきい値設定コマンドは、*sensor externalsensor* で始まります。

センサーの上位臨界しきい値の設定

次のコマンド構文では、数値環境センサーの上位臨界しきい値を設定できます。

```
config:#    sensor externalsensor <n> <sensor type> upperCritical <option>
```

変数:

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Dominion PX の Web インタフェースに表示されます。値は、1 ～ 16 の整数です。
- <sensor type> は、次のセンサー タイプのいずれかです。 *temperature, humidity, airPressure or air Flow*.

注: 指定したセンサー タイプが、指定した環境センサーのタイプと一致していない場合は、エラー メッセージ「*Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)* (指定したセンサー タイプ XXX がセンサーのタイプ (<sensortype>) と一致しません)」が表示されます。ここで、XXX は指定したセンサー タイプであり、<sensortype> は正しいセンサー タイプです。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定した環境センサーの上位臨界しきい値を有効にします。
disable	指定した環境センサーの上位臨界しきい値を無効にします。
数値	指定した環境センサーの上位臨界しきい値に値を設定し、このしきい値を同時に有効にします。

例

次のコマンドでは、ID 番号 2 の “temperature” (温度) の環境センサーの上位臨界しきい値が摂氏 40 度に設定されます。上位臨界しきい値がまだ有効になっていない場合は、このしきい値も有効になります。

```
config:#    sensor externalsensor 2 temperature upperCritical 40
```

センサーの上位警告しきい値の設定

次のコマンド構文では、数値環境センサーの上位警告しきい値を設定できます。

```
config:# sensor externalsensor <n> <sensor type> upperWarning <option>
```

変数:

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Dominion PX の Web インタフェースに表示されます。値は、1 ～ 16 の整数です。
- <sensor type> は、次のセンサー タイプのいずれかです。 *temperature*, *humidity*, *airPressure* or *air Flow*.

注: 指定したセンサー タイプが、指定した環境センサーのタイプと一致していない場合は、エラー メッセージ「*Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)* (指定したセンサー タイプ XXX がセンサーのタイプ (<sensortype>) と一致しません)」が表示されます。ここで、XXX は指定したセンサー タイプであり、<sensortype> は正しいセンサー タイプです。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定した環境センサーの上位警告しきい値を有効にします。
disable	指定した環境センサーの上位警告しきい値を無効にします。
数値	指定した環境センサーの上位警告しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、ID 番号 4 の "temperature" (温度) の環境センサーの上位警告しきい値が有効になります。

```
config:# sensor externalsensor 4 temperature upperWarning enable
```

センサーの下位臨界しきい値の設定

次のコマンド構文では、数値環境センサーの下位臨界しきい値を設定できます。

```
config:#    sensor externalsensor <n> <sensor type> lowerCritical <option>
```

変数:

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Dominion PX の Web インタフェースに表示されます。値は、1 ～ 16 の整数です。
- <sensor type> は、次のセンサー タイプのいずれかです。 *temperature, humidity, airPressure or air Flow*.

注: 指定したセンサー タイプが、指定した環境センサーのタイプと一致していない場合は、エラー メッセージ「*Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)* (指定したセンサー タイプ XXX がセンサーのタイプ (<sensortype>) と一致しません)」が表示されます。ここで、XXX は指定したセンサー タイプであり、<sensortype> は正しいセンサー タイプです。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定した環境センサーの下位臨界しきい値を有効にします。
disable	指定した環境センサーの下位臨界しきい値を無効にします。
数値	指定した環境センサーの下位臨界しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、ID 番号 1 の “humidity” (湿度) の環境センサーの下位臨界しきい値が 1 ～ 15% に設定されます。下位臨界しきい値がまだ有効になっていない場合は、このしきい値も有効になります。

```
config:#    sensor externalsensor 1 humidity lowerCritical 15
```

センサーの下位警告しきい値の設定

次のコマンド構文では、数値環境センサーの下位警告しきい値を設定できます。

```
config:# sensor externalsensor <n> <sensor type> lowerWarning <option>
```

変数:

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Dominion PX の Web インタフェースに表示されます。値は、1 ～ 16 の整数です。
- <sensor type> は、次のセンサー タイプのいずれかです。 *temperature*, *humidity*, *airPressure* or *air Flow*.

注: 指定したセンサー タイプが、指定した環境センサーのタイプと一致していない場合は、エラー メッセージ「*Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)* (指定したセンサー タイプ XXX がセンサーのタイプ (<sensortype>) と一致しません)」が表示されます。ここで、XXX は指定したセンサー タイプであり、<sensortype> は正しいセンサー タイプです。

- <option> は、次のいずれかのオプションです。 *enable*、*disable*、または数値。

オプション	説明
enable	指定した環境センサーの下位警告しきい値を有効にします。
disable	指定した環境センサーの下位警告しきい値を無効にします。
数値	指定した環境センサーの下位警告しきい値に値を設定し、同時にこのしきい値を有効にします。

例

次のコマンドでは、ID 番号 3 の “humidity” (湿度) の環境センサーの下位警告しきい値が無効になります。

```
config:# sensor externalsensor 3 humidity lowerWarning disable
```

センサーのアサート停止ヒステリシスの設定

次のコマンド構文では、数値環境センサーのアサート停止ヒステリシス値を設定できます。

```
config:#    sensor externalsensor <n> <sensor type> hysteresis <value>
```

変数:

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Dominion PX の Web インタフェースに表示されます。値は、1 ～ 16 の整数です。
- <sensor type> は、次のセンサー タイプのいずれかです。temperature, humidity, airPressure or air Flow.

注: 指定したセンサー タイプが、指定した環境センサーのタイプと一致していない場合は、エラー メッセージ「Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (指定したセンサー タイプ XXX がセンサーのタイプ (<sensortype>) と一致しません)」が表示されます。ここで、XXX は指定したセンサー タイプであり、<sensortype> は正しいセンサー タイプです。

- <value> は、指定した環境センサーのヒステリシスに割り当てられる数値です。アサート停止ヒステリシスの機能については、「**アサート停止ヒステリシスとは**『177p. 』」を参照してください。

例

次のコマンドでは、ID 番号 4 の “temperature” (温度) の環境センサーのアサート停止ヒステリシスが摂氏 2 度に設定されます。つまり、しきい値超過イベントのアサートが停止されるまで、温度が上位しきい値より少なくとも 2 度 (摂氏) 低下するか、下位しきい値より少なくとも 2 度 (摂氏) 上昇する必要があります。

```
config:#    sensor externalsensor 4 temperature hysteresis 2
```

センサーのアサート タイムアウトの設定

次のコマンド構文では、数値環境センサーのアサート タイムアウト値を設定できます。


```
config:# sensor externalsensor <n> <sensor type> assertionTimeout <value>
```

変数:

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Dominion PX の Web インタフェースに表示されます。値は、1 ～ 16 の整数です。
- <sensor type> は、次のセンサー タイプのいずれかです。temperature, humidity, airPressure or air Flow.

注: 指定したセンサー タイプが、指定した環境センサーのタイプと一致していない場合は、エラー メッセージ「Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (指定したセンサー タイプ XXX がセンサーのタイプ (<sensortype>) と一致しません)」が表示されます。ここで、XXX は指定したセンサー タイプであり、<sensortype> は正しいセンサー タイプです。

- <value> は、指定した環境センサーのアサート タイムアウトに割り当てられるサンプルの数です。「アサート タイムアウトとは『178p. 』」を参照してください。

例

次のコマンドでは、ID 番号 3 の “temperature” (温度) の環境センサーのアサート タイムアウトが 4 サンプルに設定されます。つまり、しきい値超過イベントがアサートされるまでに、少なくとも 4 つの連続したサンプルが特定の電流しきい値を超える必要があります。

```
config:# sensor externalsensor 3 temperature assertionTimeout 4
```

ユーザ設定コマンド

ほとんどのユーザ設定コマンドは、パスワード変更コマンドを除き user で始まります。

ユーザ プロファイルの作成

次のコマンド構文では、新しいユーザ プロファイルを作成できます。

```
config:# user create <name> <option> <roles>
```

ユーザ作成コマンドの実行後、新たに作成したユーザにパスワードを割り当てるように求められます。次のようにします。

1. パスワードを入力し、Enter キーを押します。
2. 確認のために同じパスワードを再入力し、Enter キーを押します。

変数:

- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。 <name> 変数にスペースを含めることはできません。
- <option> は、次のいずれかのオプションです。 *enable* または *disable*。

オプション	説明
enable	新たに作成したユーザ プロファイルを有効にします。
disable	新たに作成したユーザ プロファイルを無効にします。

- <roles> は、指定したユーザ プロファイルに割り当てられている役割、またはカンマ区切りの役割のリストです。

例

次のコマンドでは、新しいユーザ プロファイルが作成され、新しいユーザに 2 つのパラメータが設定されます。

```
config:# user create May enable admin
```

結果:

- 新しいユーザ プロファイル「May」が作成されます。
- 新しいユーザ プロファイルが有効になります。
- **admin** 役割が新しいユーザ プロファイルに割り当てられます。

ユーザ プロファイルの変更

ユーザ プロファイルには、さまざまなパラメータが含まれています。それらは変更できます。

ヒント: すべてのコマンドを組み合わせ、特定のユーザ プロファイルのパラメータを一度に変更できます。「マルチコマンド構文『422p.』」を参照してください。

ユーザのパスワードの変更

次のコマンド構文では、管理者権限がある場合に既存のユーザのパスワードを変更できます。

```
config:# user modify <name> password
```

上記のコマンドの実行後、新しいパスワードを入力するように求められます。次のようにします。

1. 新しいパスワードを入力し、Enter キーを押します。
2. 確認のために新しいパスワードを再入力し、Enter キーを押します。

変数:

- <name> は、設定を変更するユーザの名前です。

例

次の手順では、ユーザ「May」のパスワードの変更方法を示します。

1. 設定モードになっていることを確認します。「設定モードへの移行『297p.』」を参照してください。
2. 次のコマンドを入力して、ユーザ プロファイル「May」のパスワードを変更します。

```
config:# user modify May password
```

3. プロンプトが表示されたら新しいパスワードを入力し、Enter キーを押します。
4. 同じ新しいパスワードを入力し、Enter キーを押します。
5. パスワードの変更が正常に実行されると、config:# プロンプトが表示されます。

ユーザの個人データの変更

ユーザのフル ネーム、電話番号、電子メール アドレスなどのユーザの個人データを変更できます。

- ▶ ユーザのフル ネームを変更するには、次のコマンド構文を使用します。

```
config:#    user modify <name> fullName "<full_name>"
```

- ▶ ユーザの電話番号を変更するには、次のコマンド構文を使用します。

```
config:#    user modify <name> telephoneNumber "<phone_number>"
```

- ▶ ユーザの電子メール アドレスを変更するには、次のコマンド構文を使用します。

```
config:#    user modify <name> emailAddress <email_address>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <full_name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。<full_name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。
- <phone_number> は、指定したユーザに連絡するための電話番号です。<phone_name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。
- <email_address> は、指定したユーザの電子メール アドレスです。

ヒント: すべてのコマンドを組み合わせ、特定のユーザ プロファイルのパラメータを一度に変更できます。「マルチコマンド構文 [422p.]」を参照してください。

例

次のコマンドでは、ユーザ プロファイル「May」の 2 つのパラメータが変更されます。

```
config:# user modify May fullName "May Turner" telephoneNumber 123-4567
```

結果:

- May のフル ネームは「May Turner」と指定されます。
- May の電話番号は 123-4567 に設定されます。

ユーザ プロファイルの有効化または無効化

次のコマンド構文では、ユーザ プロファイルの有効/無効を切り替えることができます。ユーザは、そのユーザ プロファイルが有効になっている場合にのみ Dominion PX デバイスにログインできます。

```
config:# user modify <name> enabled <option>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option> は、次のいずれかのオプションです。 *true* または *false*。

オプション	説明
true	指定したユーザ プロファイルを有効にします。
false	指定したユーザ プロファイルを無効にします。

例

次のコマンドでは、ユーザ プロファイル「May」が有効になります。

```
config:# user modify May enabled true
```

パスワード変更の強制

次のコマンド構文では、ユーザが指定したユーザ プロファイルに次回ログインするときにパスワード変更を強制するかどうかを指定できます。

```
config:# user modify <name> forcePasswordChangeOnNextLogin <option>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option> は、次のいずれかのオプションです。 *true* または *false*。

オプション	説明
true	ユーザの次のログイン時にパスワード変更が強制されます。
false	ユーザの次のログイン時にパスワード変更が強制されません。

例

次のコマンドでは、May の次のログイン時にパスワード変更が強制されます。

```
config:# user modify May forcePasswordChangeOnNextLogin true
```

SNMPv3 設定の変更

特定のユーザ プロファイルの SNMPv3 パラメータを変更するための各種コマンドがあります。次のコマンドをすべて組み合わせて、SNMPv3 パラメータを一度に変更できます。「マルチコマンド構文『422p.』」を参照してください。

- ▶ 指定したユーザについて **Dominion PX** への **SNMP v3** アクセスを有効または無効にするには、次の手順に従います。

```
config:# user modify <name> snmpV3Access <option1>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option1> は、*enable* または *disable*。

オプション	説明
enable	指定したユーザの SNMP v3 アクセス権限を有効にします。
disable	指定したユーザの SNMP v3 アクセス権限を無効にします。

- ▶ セキュリティ レベルを指定するには、次の手順に従います。

```
config:# user modify <name> securityLevel <option2>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option2> は、*noAuthNoPriv*、*authNoPriv*、または *authPriv* のいずれかです。

オプション	説明
noAuthNoPriv	認証なし、プライバシーなし。
authNoPriv	認証あり、プライバシーなし。
authPriv	認証あり、プライバシーあり。

- ▶ 認証パスフレーズをパスワードと同じにするかどうかを指定するには、次の手順に従います。

```
config:# user modify <name> userPasswordAsAuthenticationPassPhrase <option3>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option3> は、*true* または *false*。

オプション	説明
true	認証パスフレーズはパスワードと同じです。
false	認証パスフレーズはパスワードとは異なります。

- ▶ 認証パスフレーズを指定するには、次の手順に従います。

```
config:# user modify <name> authenticationPassPhrase <authentication_passphrase>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <authentication_passphrase> は、認証パスフレーズとして使用される文字列で、最大 32 文字の ASCII の表示可能文字で構成されます。

- ▶ プライバシー パスフレーズを認証パスフレーズと同じにするかどうかを指定するには、次の手順に従います。

```
config:# user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option4> は、*true* または *false*。

オプション	説明
true	プライバシー パスフレーズは認証パスフレーズと同じです。
false	プライバシー パスフレーズは認証パスフレーズとは異なります。

- ▶ プライバシー パスフレーズを指定するには、次の手順に従います。


```
config:# user modify <name> privacyPassPhrase <privacy_passphrase>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <privacy_passphrase> は、プライバシー パスフレーズとして使用される文字列で、最大 32 文字の ASCII の表示可能文字で構成されます。

▶ 認証プロトコルを指定するには、次の手順に従います。

```
config:# user modify <name> authenticationProtocol <option5>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option5> は、MD5 または SHA-1 のいずれかです。

オプション	説明
MD5	MD5 認証プロトコルが適用されます。
SHA-1	SHA-1 認証プロトコルが適用されます。

▶ プライバシー プロトコルを指定するには、次の手順に従います。

```
config:# user modify <name> privacyProtocol <option6>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option6> は、DES または AES-128 のいずれかです。

オプション	説明
DES	DES プライバシー プロトコルが適用されます。
AES-128	AES-128 プライバシー プロトコルが適用されます。

例

次のコマンドでは、ユーザ「May」の 3 つの SNMPv3 パラメータが設定されます。

```
config:# user modify May snmpV3Access enable securityLevel authNoPriv  
userPasswordAsAuthenticationPassPhrase true
```

結果:

- ユーザの SNMPv3 アクセス権限が有効になります。
- SNMPv3 セキュリティ レベルは、認証のみ、プライバシーなしです。
- 認証パスワードはユーザのパスワードと同じです。

役割の変更

次のコマンド構文では、特定のユーザの役割を変更できます。

```
config:# user modify <name> roles <roles>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <roles> は、指定したユーザ プロファイルに割り当てられている役割、またはカンマ区切りの役割のリストです。

例

次のコマンドでは、ユーザ「May」に 2 つの役割が割り当てられます。

```
config:# user modify May roles admin,tester
```

結果:

- ユーザ「May」に、「admin」と「tester」のすべての権限がまとめて設定されます。

測定単位の変更

特定のユーザ プロファイルの温度、長さ、および圧力に表示される測定単位を変更できます。さまざまな測定単位コマンドを組み合わせ、すべての測定単位を一度に設定できます。すべてのコマンドを組み合わせるには、「**マルチコマンド構文『422p.』**」を参照してください。

注: 測定単位変更は、Web インタフェースとコマンド ライン インタフェースにのみ適用されます。

► **優先温度単位を設定するには、次の手順に従います。**

```
config:# user modify <name> preferredTemperatureUnit <option1>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option1> は、*C* または *F* のいずれかです。

オプション	説明
C	温度を摂氏で表示します。
F	温度を華氏で表示します。

► **優先長さ単位を設定するには、次の手順に従います。**

```
config:# user modify <name> preferredLengthUnit <option2>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option2> は、*meter* または *feet* のいずれかです。

オプション	説明
meter	長さまたは高さをメートルで表示します。
feet	長さまたは高さをフィートで表示します。

▶ **優先圧力単位を設定するには、次の手順に従います。**

```
config:# user modify <name> preferredPressureUnit <option3>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option3> は、*pascal* または *psi* のいずれかです。

オプション	説明
pascal	圧力をパスカル (Pa) で表示します。
psi	圧力を psi で表示します。

例

次のコマンドでは、ユーザ「May」のすべての測定単位が設定されます。

```
config:# user modify May preferredTemperatureUnit F preferredLengthUnit feet
preferredPressureUnit psi
```

結果:

- 優先温度単位が華氏に設定されます。
- 優先長さ単位がフィートに設定されます。
- 優先圧力単位が psi に設定されます。

ユーザ プロファイルの削除

次のコマンド構文では、既存のユーザ プロファイルを削除できます。

```
config:# user delete <name>
```

例

次のコマンドでは、ユーザ プロファイル「May」が削除されます。

```
config:# user delete May
```

自身のパスワードの変更

どのユーザも、自身のパスワードの変更権限があれば、次のコマンド構文で自身のパスワードを変更できます。このコマンドは `user` で始まりません。

```
config:# password
```

このコマンドの実行後、現在のパスワードと新しいパスワードの両方をそれぞれ入力するように求められます。

重要: パスワードの変更に成功すると、コマンド「**apply**」を入力しても、変更を保存しなくても、新しいパスワードがすぐに有効になります。

例

次の手順では、自身のパスワードを変更します。

1. 設定モードになっていることを確認します。「**設定モードへの移行**」『297p. 』を参照してください。
2. 次のコマンドを入力し、Enter キーを押します。

```
config:# password
```

3. 次のプロンプトが表示されたら、既存のパスワードを入力し、Enter キーを押します。

```
Current password:
```

4. 次のプロンプトが表示されたら、新しいパスワードを入力し、Enter キーを押します。

```
Enter new password:
```

5. 次のプロンプトが表示されたら、確認のために新しいパスワードを再入力し、Enter キーを押します。

```
Re-type new password:
```

役割設定コマンド

役割設定コマンドは、`role` で始まります。

役割の作成

次のコマンド構文では、役割に割り当てる各権限をセミコロンで区切ったリストを指定して、新しい役割を作成できます。

```
config:#    role create "<name>" <privilege1>;<privilege2>;<privilege3>...
```

特定の権限に引数を指定する場合は、その権限の後にコロンと引数を続けます。

```
config:#    role create "<name>" <privilege1>:<argument1>,<argument2>...;
<privilege2>:<argument1>,<argument2>...;
<privilege3>:<argument1>,<argument2>...;
...
```

変数:

- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。
- <privilege1>、<privilege2>、<privilege3> などは、役割に割り当てられている権限の名前です。各権限の間を、セミコロンで区切ります。「**すべての権限**『406p. 』」を参照してください。
- <argument1>、<argument2> などは、特定の権限に設定される引数です。権限とその引数の間を、コロンで区切ります。

すべての権限

次の表にすべての権限を示します。使用可能な権限は、購入したモデルによって異なります。たとえば、アウトレット（コンセント）切り替え機能のない PDU には、「switchOutlet」権限はありません。

権限	説明
adminPrivilege	管理者権限
changeAssetStripConfiguration	資産ストリップ設定の変更
changeAuthSettings	認証設定の変更
changeDataTimeSettings	日付/時刻設定の変更
changeEventSetup	イベント設定の変更
changeExternalSensorsConfiguration	外部センサー設定の変更
changeLhxConfiguration	LHX 設定の変更
changeNetworkSettings	ネットワーク設定の変更
changePassword	自身のパスワードの変更

権限	説明
changePduConfiguration	PDU、インレット、アウトレット (コンセント)、および過電流プロテクタの設定の変更
changeSecuritySettings	セキュリティ設定の変更
changeSnmpSettings	SNMP 設定の変更
changeUserSettings	ローカル ユーザ管理の変更
changeWebcamSettings	Web カメラ 設定の変更
clearLog	ローカル イベント ログのクリア
firmwareUpdate	ファームウェアの更新
performReset	リセット (ウォーム スタート)
switchOutlet*	アウトレット (コンセント) の切り替え
viewEventSetup	イベント設定の表示
viewLog	ローカル イベント ログの表示
viewSecuritySettings	セキュリティ設定の表示
viewSnmpSettings	SNMP 設定の表示
viewUserSettings	ローカル ユーザ管理の表示
viewWebcamSettings	Web カメラのスナップショットと設定の表示

* 「switchOutlet」権限には、コロンで区切られた引数が必要です。引数は次のとおりです。

- すべてのアウトレット (コンセント)、つまり
switchOutlet:all
- アウトレット (コンセント) 番号。たとえば、
switchOutlet:1
switchOutlet:2
switchOutlet:3
- アウトレット (コンセント) のカンマ区切りのリスト。たとえば、
switchOutlet:1,3,5,7,8,9

例

次のコマンドでは、新しい役割が作成され、役割に権限が割り当てられます。

```
config:#    role create tester firmwareUpdate;viewEventSetup
```

結果:

- 新しい役割「tester」が作成されます。
- 役割に 2 つの権限、firmwareUpdate (ファームウェアの更新) と viewEventSetup (イベント設定の表示) が割り当てられます。

役割の変更

既存の役割のさまざまなパラメータ (権限など) を変更できます。

▶ 役割の説明を変更するには、次の手順に従います。

```
config:#    role modify <name> description <description>
```

変数:

- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。
- <description> は、英数字で構成される説明です。<description> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

▶ 特定の役割に権限を追加するには、次の手順に従います。

```
config:#    role modify <name> addPrivileges  
            <privilege1>;<privilege2>;<privilege3>...
```

特定の権限に引数を指定する場合は、その権限の後にコロンと引数を追加します。


```
config:#    role modify <name> addPrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

変数:

- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。
- <privilege1>、<privilege2>、<privilege3> などは、役割に割り当てられている権限の名前です。各権限の間を、セミコロンで区切ります。「**すべての権限**『406p.』」を参照してください。
- <argument1>、<argument2> などは、特定の権限に設定される引数です。権限とその引数の間を、コロンで区切ります。

▶ **役割から特定の権限を削除するには、次の手順に従います。**

```
config:#    role modify <name> removePrivileges
            <privilege1>;<privilege2>;<privilege3>...
```

特定の権限に引数を指定する場合は、その権限の後にコロンと引数を追加します。

```
config:#    role modify <name> removePrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

注: 役割から権限を削除する場合は、指定した権限と引数 (ある場合) が、役割に割り当てられている権限と引数に正確に一致している必要があります。一致しない場合、指定した利用できない権限の削除に失敗します。

変数:

- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。
- <privilege1>、<privilege2>、<privilege3> などは、役割に割り当てられている権限の名前です。各権限の間を、セミコロンで区切ります。「**すべての権限**『406p.』」を参照してください。
- <argument1>、<argument2> などは、特定の権限に設定される引数です。権限とその引数の間を、コロンで区切ります。

例

次のコマンドでは、役割「tester」の権限が変更されます。

```
config:#    role modify tester addPrivileges changeAuthSettings removePrivileges  
            firmwareUpgrade
```

結果:

- 「changeAuthSettings」(認証設定の変更) 権限が役割に追加されます。
- 「firmwareUpgrade」(ファームウェアのアップグレード) 権限が役割から削除されます。

役割の削除

次のコマンド構文では、既存の役割を削除できます。

```
config:#    role delete <name>
```

例

次のコマンドでは、既存の役割が削除されます。

```
config:#    role delete tester
```

EnergyWise 設定コマンド

EnergyWise 設定コマンドは、*energywise* で始まります。

EnergyWise の有効化または無効化

次のコマンド構文では、Dominion PX デバイスに実装されている Cisco® EnergyWise エンドポイントを有効にするかどうかを指定できます。

```
config:#    energywise enabled <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *true* または *false*。

オプション	説明
true	Cisco EnergyWise 機能が有効になります。
false	Cisco EnergyWise 機能が無効になります。

例

次のコマンドでは、Cisco® EnergyWise 機能が有効になります。

```
config:# energywise enabled true
```

EnergyWise ドメインの指定

次のコマンド構文では、Dominion PX デバイスが属する Cisco® EnergyWise ドメインを指定できます。

```
config:# energywise domain <name>
```

変数:

- <name> は、ASCII の表示可能文字で構成される文字列で、最大 127 文字です。 空白文字とアスタリスクは使用できません。

例

次のコマンドでは、Dominion PX デバイスが属する Cisco® EnergyWise ドメインが「helloDomain」に設定されます。

```
config:# energywise domain helloDomain
```

EnergyWise のシークレットの指定

次のコマンド構文では、Cisco® EnergyWise ドメインに入るためのパスワード（シークレット）を指定できます。

```
config:# energywise secret <password>
```

変数:

- <password> は、ASCII の表示可能文字で構成される文字列で、最大 127 文字です。 空白文字とアスタリスクは使用できません。

例

次のコマンドでは、Cisco® EnergyWise ドメインのシークレット（パスワード）として「password5233」が指定されます。

```
config:# energywise secret password5233
```

UDP ポートの変更

次のコマンド構文では、Cisco® EnergyWise ドメイン内で通信するための UDP ポートを指定できます。

```
config:# energywise port <port>
```

変数:

- <port> は、1 ～ 65535 の範囲の UDP ポート番号です。

例

次のコマンドでは、Cisco® EnergyWise の UDP ポートとして 10288 が指定されます。

```
config:# energywise port 10288
```

ポーリング間隔の設定

次のコマンド構文では、Cisco® EnergyWise ドメインが Dominion PX デバイスを照会するポーリング間隔を指定できます。

```
config:# energywise polling <timing>
```

変数:

- <timing> は、整数値 (秒) です。範囲は 30 ～ 600 秒です。

例

次のコマンドでは、Dominion PX デバイスを照会するポーリング間隔が 300 秒に設定されます。

```
config:# energywise polling 300
```

資産管理コマンド

CLI コマンドを使用して、接続されている資産センサー (ある場合) の設定または資産センサーの LED の設定を変更できます。

資産センサー管理

資産センサー管理設定コマンドは、assetStrip で始まります。

資産センサーの名前付け

次のコマンド構文では、Dominion PX デバイスに接続されている資産センサーの名前が指定または変更されます。

```
config:#    assetStrip <n> name "<name>"
```

変数:

- <n> は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの Dominion PX デバイスの場合、番号は常に 1 になります。
- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。 <name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

例

次のコマンド構文では、Dominion PX デバイスに接続されている資産センサーの名前が指定または変更されます。

```
config:#    assetStrip 1 name "Red Rack"
```

ラック ユニットの数の指定

次のコマンド構文では、Dominion PX デバイスに接続されている資産センサーのラック ユニットの合計数を指定できます。

```
config:#    assetStrip <n> numberOfRackUnits <number>
```

注: Raritan 資産センサーの場合、ラック ユニットはタグ ポートを意味します。

変数:

- <n> は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの Dominion PX デバイスの場合、番号は常に 1 になります。
- <number> は、接続されている資産センサーで利用できるラック ユニットの合計数です。この値の範囲は、8 ～ 64 です。

例

次のコマンドでは、資産センサーのラック ユニットの合計数が 48 に指定されます。

```
config:#    assetStrip 1 numberOfRackUnits 48
```

ラック ユニットのナンバリング モードの指定

次のコマンド構文では、Dominion PX デバイスに接続されている資産センサーのラック ユニットのナンバリング モードを指定できます。ナンバリング モードは、ラック ユニットの番号を変更します。

```
config:#    assetStrip <n> rackUnitNumberingMode <mode>
```

変数:

- <n> は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの Dominion PX デバイスの場合、番号は常に 1 になります。
- <mode> は、*topDown* または *bottomUp* のいずれかのナンバリング モードです。

モード	説明
topDown	ラック ユニットには、最下位のラック ユニットから最上位のラック ユニットへ昇順に番号が振られます。
bottomUp	ラック ユニットには、最下位のラック ユニットから最上位のラック ユニットへ降順に番号が振られます。

例

次のコマンドでは、資産センサー 1 のラック ユニットに、資産センサーの RJ-45 コネクタに最も近い方から遠い方へ昇順に番号が振られます。したがって、RJ-45 コネクタに最も近いラック ユニットに番号 1 が振られます。

```
config:#    assetStrip 1 rackUnitNumberingMode topDown
```

ラック ユニットのナンバリング オフセットの指定

次のコマンド構文では、Dominion PX デバイスに接続されている資産センサーのラック ユニットの開始番号を指定できます。

```
config:#    assetStrip <n> rackUnitNumberingOffset <number>
```

変数:

- <n> は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの Dominion PX デバイスの場合、番号は常に 1 になります。
- <number> は、接続されている資産センサーで、番号が振られるラック ユニットの開始番号です。この値は整数です。

例

次のコマンドでは、資産センサー 1 のラック ユニットの開始番号が 5 に指定されます。つまり、資産センサー 1 の最初のラック ユニットから最後のラック ユニットまで 5、6、7 のように番号が振られます。

```
config:#    assetStrip 1 rackUnitNumberingOffset 5
```

資産センサーの向きの指定

次のコマンド構文では、Dominion PX デバイスに接続されている資産センサーの向きを指定できます。通常は、資産センサーにチルト センサーが組み込まれていないために Dominion PX で資産センサーの向きを検出できない場合を除いて、このコマンドを実行する必要はありません。

```
config:#    assetStrip <n> assetStripOrientation <orientation>
```

変数:

- <n> は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの Dominion PX デバイスの場合、番号は常に 1 になります。
- <orientation> は、*topConnector* または *bottomConnector* のいずれかのオプションです。

向き	説明
topConnector	資産センサーを上部にある RJ-45 コネクタで装着することを示します。
bottomConnector	資産センサーを下部にある RJ-45 コネクタで装着することを示します。

例

次のコマンドでは、資産センサー 1 の RJ-45 コネクタが上部になる向きにすることが指定されます。

```
config:#    assetStrip 1 assetStripOrientation topConnector
```

タグが接続されている場合の LED 色の設定

次のコマンド構文では、資産センサー #1 のすべてのラック ユニットの LED 色を設定して、資産タグが接続されていることを示すことができます。

```
config:#    assetStrip <n> LEDColorForConnectedTags <color>
```

変数:

- <color> は、HTML 形式の色の 16 進 RGB 値です。<color> 変数の範囲は、#000000 ～ #FFFFFF です。

例

次のコマンドでは、資産センサー #1 のすべてのラック ユニットの LED 色が赤（つまり FF0000）に設定され、資産タグが接続されていることが示されます。

```
config:#    assetStrip 1 LEDColorForConnectedTags #FF0000
```

タグが接続されていない場合の LED 色の設定

次のコマンド構文では、接続されている資産センサーのすべてのラック ユニットの LED 色を設定して、資産タグが接続されていないことを示すことができます。

```
config:#    assetStrip <n> LEDColorForDisconnectedTags <color>
```

変数:

- <color> は、HTML 形式の色の 16 進 RGB 値です。<color> 変数の範囲は、#000000 ～ #FFFFFF です。

例

次のコマンド構文では、資産センサー #1 のすべてのラック ユニットの LED 色が黒（つまり 000000）に設定され、資産タグが接続されていないことが示されます。

```
config:#    assetStrip 1 LEDColorForDisconnectedTags #000000
```

注: 色を黒に設定すると、LED はオフのままになります。

ラック ユニットの設定

Raritan 資産センサーの場合、ラック ユニットはタグ ポートを意味します。ラック ユニットの設定コマンドは、`rackUnit` で始まります。

ラック ユニットの名前付け

次のコマンド構文では、指定した資産センサーの指定したラック ユニットの名前の割り当てまたは変更ができます。

```
config:#    rackUnit <n> <rack_unit> name "<name>"
```

変数:

- `<n>` は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの Dominion PX デバイスの場合、番号は常に 1 になります。
- `<rack_unit>` は目的のラック ユニットのインデックス番号です。各ラック ユニットのインデックス番号は、Web インタフェースの [Asset Strip (資産ストリップ)] ページに表示されます。
- `<name>` は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。`<name>` 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

例

次のコマンドでは、資産センサー 1 のインデックス番号 25 のラック ユニットに、「Linux server (Linux サーバ)」という名前を割り当てます。

```
config:#    rackUnit 1 25 name "Linux server"
```

LED 動作モードの設定

次のコマンド構文では、指定した資産センサーの特定のラック ユニットがグローバルな LED 色設定に従うかどうかを指定できます。

```
config:#    rackUnit <n> <rack_unit> LEDOperationMode <mode>
```

変数:

- <n> は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの Dominion PX デバイスの場合、番号は常に 1 になります。
- <rack_unit> は目的のラック ユニットのインデックス番号です。各ラック ユニットのインデックス番号は、Web インタフェースの [Asset Strip (資産ストリップ)] ページに表示されます。
- <mode> は、*automatic* または *manual* のいずれかの LED モードです。

モード	説明
automatic	指定したラック ユニットの LED は、グローバルな LED 色設定に従います。「 タグが接続されている場合の LED 色の設定『416p.』 」および「 タグが接続されていない場合の LED 色の設定『416p.』 」を参照してください。 デフォルトではこの設定です。
manual	指定したラック ユニットに異なる LED 色や LED モードを選択できます。 このオプションを選択した場合は、「 ラック ユニットの LED 色の設定『419p.』 」および「 ラック ユニットの LED モードの設定『420p.』 」を参照して異なる LED 設定を行ってください。

例

次のコマンドでは、資産センサー 1 のインデックス番号が 25 のラック ユニットに異なる LED 色や LED モードを設定できるようになります。

```
config:#    rackUnit 1 25 LEDOperationMode manual
```

ラック ユニットの LED 色の設定

次のコマンド構文では、指定した資産センサーの特定のラック ユニットの LED 色を設定できます。このラック ユニットの LED 動作モードが「manual」に設定されている場合にのみラック ユニットの LED 色を設定する必要があります。

```
config:#    rackUnit <n> <rack_unit> LEDColor <color>
```

変数:

- <n> は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの Dominion PX デバイスの場合、番号は常に 1 になります。
- <rack_unit> は目的のラック ユニットのインデックス番号です。各ラック ユニットのインデックス番号は、Web インタフェースの [Asset Strip (資産ストリップ)] ページに表示されます。
- <color> は、HTML 形式の色の 16 進 RGB 値です。<color> 変数の範囲は、#000000 ～ #FFFFFF です。

注: ラック ユニットの LED 色設定によって、グローバルな LED 色設定が上書きされます。「タグが接続されている場合の LED 色の設定『416p. 』」および「タグが接続されていない場合の LED 色の設定『416p. 』」を参照してください。

例

次のコマンドでは、資産センサー 1 のインデックス番号が 25 のラック ユニットの LED 色がピンク (つまり FF00FF) に設定されます。

```
config:#    rackUnit 1 25 LEDColor #FF00FF
```

ラック ユニットの LED モードの設定

次のコマンド構文では、指定した資産センサーの特定のラック ユニットの LED モードを設定できます。このラック ユニットの LED 動作モードが「manual」に設定されている場合にのみラック ユニットの LED モードを設定する必要があります。

```
config:#    rackUnit <n> <rack_unit> LEDMode <mode>
```

変数:

- <n> は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの Dominion PX デバイスの場合、番号は常に 1 になります。
- <rack_unit> は目的のラック ユニットのインデックス番号です。各ラック ユニットのインデックス番号は、Web インタフェースの [Asset Strip (資産ストリップ)] ページに表示されます。
- <mode> は、*on*、*off*、*blinkSlow*、または *blinkFast* のいずれかの LED モードです。

モード	説明
on	このモードでは、LED は常に点灯したままです。
off	このモードでは、LED は常に消灯したままです。
blinkSlow	このモードでは、LED はゆっくり点滅します。
blinkFast	このモードでは、LED は速く点滅します。

例

次のコマンドでは、資産センサー 1 のインデックス番号 25 のラック ユニットの LED が速く点滅します。

```
config:#    rackUnit 1 25 LEDMode blinkFast
```

シリアル ポート設定コマンド

シリアル ポート設定コマンドは、*serial* で始まります。

シリアル ポートのボー レートの設定

次のコマンド構文では、Dominion PX デバイスの「CONSOLE / MODEM」というラベルが付いたシリアル ポートのボーレート (bps) を設定できます。ローカル接続経由でボー レートを変更した場合にこの設定を有効にするには、CLI からログアウトする必要があります。

```
config:#    serial baudRate <baud_rate>
```

変数:

- <baud_rate> は、次のいずれかのボー レート オプションです。1200、2400、4800、9600、19200、38400、57600、115200。

注: シリアル ポート設定は、Dominion PX を Raritan の Dominion LX KVM スイッチとともに使用する場合に特に役立ちます。Dominion LX では、シリアル インタフェースを介した通信では 19200 bps のみをサポートしています。

例

次のコマンドでは、Dominion PX デバイスのシリアル ポートのボー レートを 9600 bps に設定します。

```
config:#    serial baudRate 9600
```

履歴バッファの長さの設定

次のコマンド構文では、履歴バッファの長さを変更できます。デフォルトの長さは 25 です。

```
config:#    history length <n>
```

変数:

- <n> は、1 ～ 250 メートルの整数です。
- コマンドの使用時に <n> 変数を空白のままにすると、履歴バッファはデフォルトで 25 に設定されます。

マルチコマンド構文

さまざまな設定コマンドを 1 つのコマンドにまとめて一度に実行することで、設定時間を短縮することができます。

マルチコマンド構文は、次のようになります。

<設定 1> <値 1> <設定 2> <値 2> <設定 3> <値 3> ...

例 1 - IP、サブネット マスク、ゲートウェイの各パラメータの組み合わせ

次のマルチコマンド構文では、ネットワーク接続のための IPv4 アドレス、サブネット マスク、およびゲートウェイを同時に設定できます。

```
config:# network ipv4 ipAddress 192.168.84.225 subnetMask 255.255.255.0
gateway 192.168.84.0
```

結果:

- IP アドレスが 192.168.84.225 に設定されます。
- サブネット マスクが 255.255.255.0 に設定されます。
- ゲートウェイが 192.168.84.0 に設定されます。

例 2 - 上位臨界設定と上位警告設定の組み合わせ

次のマルチコマンド構文では、3 番目のサーキット ブレーカの RMS 電流の上位臨界しきい値と上位警告しきい値を同時に設定できます。

```
config:# sensor ocp 3 current upperCritical disable upperWarning 20
```

結果:

- 3 番目のサーキット ブレーカの RMS 電流の上位臨界しきい値が無効になります。
- 3 番目のサーキット ブレーカの RMS 電流の上位警告しきい値が 20A に設定され、同時に有効になります。

例 3 - SSID パラメータと PSK パラメータの組み合わせ

次のマルチコマンド構文では、ワイヤレス機能の SSID パラメータと PSK パラメータの両方が同時に設定されます。

```
config:#    network wireless SSID myssid PSK encryp_key
```

結果:

- SSID 値は myssid に設定されます。
- PSK 値は encryp_key に設定されます。

設定モードの終了

「apply」および「cancel」のいずれのコマンドでも、設定モードを終了できます。ただし、「apply」では、設定モードで加えたすべての変更が保存されますが、「cancel」ではすべての変更が破棄されるという点が異なります。

► 設定モードを終了するには、次のいずれかのコマンドを使用します

```
config:#    apply
-- または --
config:#    cancel
```

Enter キーを押すと # プロンプトが表示され、管理者モードになったことがわかります。

負荷遮断設定コマンド

このセクションは、アウトレット（コンセント）切り替え対応 PDU にのみ適用されます。

負荷遮断設定コマンドは、*loadshedding* で始まります。

他の CLI 設定コマンドとは異なり、負荷遮断設定コマンドは設定モードではなく **管理者モード** で実行されます。「**さまざまな CLI モードとプロンプト**」『277p.』を参照してください。

負荷遮断の有効化または無効化

このセクションは、アウトレット（コンセント）切り替え対応 PDU にのみ適用されます。

次のコマンド構文では、負荷遮断機能を有効にするかどうかを指定できます。

```
#          loadshedding <option>
```

上記のコマンドの実行後、操作の確認を求められます。y を押して操作を確認するか、n を押して操作を中止します。

確認手順をスキップするには、コマンドの最後に「/y」パラメータを追加します。これにより、操作は直ちに実行されます。

```
#          loadshedding <option> /y
```

変数:

- <option> は、次のいずれかのオプションです。*enable* または *disable*。

オプション	説明
enable	負荷遮断機能が有効になります。
disable	負荷遮断機能が無効になります。

例

次のコマンドでは、負荷遮断機能が有効になります。

```
config:#    loadshedding enable
```


電源制御操作

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

Dominion PX デバイスのアウトレット (コンセント) では、CLI を通じて電源オン、オフ、または再投入できます。

この操作は、*管理者モード*で実行する必要があります。「**さまざまな CLI モードとプロンプト** 『277p. 』」を参照してください。

アウトレット (コンセント) の電源オン

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

次のコマンド構文で、1 つ以上のアウトレット (コンセント) の電源をオンにできます。

```
# power outlets <numbers> on
```

操作を迅速化するには、コマンドの最後に、操作確認を行うパラメータ「/y」を追加します。

```
# power outlets <numbers> on /y
```

変数:

- <numbers> は、次のいずれかのオプションです。all は、アウトレット (コンセント) の番号、リスト、または範囲です。

オプション	説明
all	すべてのアウトレット (コンセント) をオンにします。
特定のアウトレット (コンセント) 番号	指定したアウトレット (コンセント) をオンにします。
アウトレット (コンセント) のカンマ区切りのリスト	順不同または連続した複数のアウトレット (コンセント) をオンにします。 たとえば、7 つのアウトレット (コンセント) (2、4、9、11、12、13、および 15) を指定するには、「outlets 2,4,9,11-13,15」と入力します。

オプション	説明
間に半角ダッシュがあるアウトレット (コンセント) の範囲	連続する複数のアウトレット (コンセント) をオンにします。 たとえば、6 つの連続したアウトレット (コンセント) (3、4、5、6、7、8) を指定するには、「outlets 3-8」と入力します。

「/y」を指定せずにコマンドを入力した場合は、操作の確認を求めるメッセージが表示されます。その場合は、次のいずれかを入力します。

- 「y」と入力して、操作を確認します。または
- 「n」と入力して、操作を中止します。

例

次のコマンドでは、すべてのアウトレット (コンセント) の電源をオンにします。

```
# power outlets all on
```

アウトレット (コンセント) の電源オフ

このセクションは、アウトレット (コンセント) 切り替え対応 PDU にのみ適用されます。

次のコマンド構文で、1 つ以上のアウトレット (コンセント) の電源をオフにできます。

```
#          power outlets <numbers> off
```

操作を迅速化するには、コマンドの最後に、操作確認を行うパラメータ「/y」を追加します。

```
#          power outlets <numbers> off /y
```

変数:

- <numbers> は、次のいずれかのオプションです。all は、アウトレット (コンセント) の番号、リスト、または範囲です。

オプション	説明
all	すべてのアウトレット (コンセント) をオフにします。
特定のアウトレット (コンセント) 番号	指定したアウトレット (コンセント) をオフにします。
アウトレット (コンセント) のカンマ区切りのリスト	順不同または連続した複数のアウトレット (コンセント) をオフにします。 たとえば、7 つのアウトレット (コンセント) (2、4、9、11、12、13、および 15) を指定するには、「outlets 2,4,9,11-13,15」と入力します。
間に半角ダッシュがあるアウトレット (コンセント) の範囲	連続する複数のアウトレット (コンセント) をオフにします。 たとえば、6 つの連続したアウトレット (コンセント) (3、4、5、6、7、8) を指定するには、「outlets 3-8」と入力します。

「/y」を指定せずにコマンドを入力した場合は、操作の確認を求めるメッセージが表示されます。その場合は、次のいずれかを入力します。

- 「y」と入力して、操作を確認します。または
- 「n」と入力して、操作を中止します。

例

次のコマンドでは、アウトレット（コンセント）6 の電源をオフにします。

```
# power outlets 6 off
```

アウトレット（コンセント）の電源の再投入

このセクションは、アウトレット（コンセント）切り替え対応 PDU にのみ適用されます。

次のコマンド構文で、1 つ以上のアウトレット（コンセント）の電源を再投入できます。

```
# power outlets <numbers> cycle
```

操作を迅速化するには、コマンドの最後に、操作確認を行うパラメータ「/y」を追加します。

```
# power outlets <numbers> cycle /y
```

変数:

- <numbers> は、次のいずれかのオプションです。all は、アウトレット（コンセント）の番号、リスト、または範囲です。

オプション	説明
all	すべてのアウトレット（コンセント）の電源を再投入します。
特定のアウトレット（コンセント）番号	指定したアウトレット（コンセント）の電源を再投入します。
アウトレット（コンセント）のカンマ区切りのリスト	順不同または連続した複数のアウトレット（コンセント）の電源を再投入します。 たとえば、7 つのアウトレット（コンセント）(2、4、9、11、12、13、および 15) を指定するには、「outlets 2,4,9,11-13,15」と入力します。

オプション	説明
間に半角ダッシュがあるアウトレット（コンセント）の範囲	連続した複数のアウトレット（コンセント）の電源を再投入します。 たとえば、6 つの連続したアウトレット（コンセント）(3,4,5,6,7,8) を指定するには、「outlets 3-8」と入力します。

「/y」を指定せずにコマンドを入力した場合は、操作の確認を求めるメッセージが表示されます。その場合は、次のいずれかを入力します。

- 「y」と入力して、操作を確認します。または
- 「n」と入力して、操作を中止します。

例

次のコマンドでは、アウトレット（コンセント）2、6、7、8、10、13、14、15、16 の電源を再投入できます。

```
# power outlets 2,6-8,10,13-16 cycle
```

ユーザのブロック解除

ユーザが Dominion PX へのアクセスをブロックされている場合は、そのブロックをローカル コンソールで解除できます。

▶ ユーザのブロックを解除するには、次の手順に従います。

1. ローカル接続でターミナル プログラムを使用して、CLI インタフェースにログインします。「ハイパーターミナルの使用『275p.』」を参照してください。
2. [Username (ユーザ名)] プロンプトが表示されたら、「unblock」と入力し、Enter キーを押します。

Username: unblock

3. [Username to unblock (ブロックを解除するユーザ名)] プロンプトが表示されたら、ブロックを解除するユーザのログイン名を入力し、Enter キーを押します。

Username to unblock:

4. 指定したユーザのブロックが正常に解除されたことを示すメッセージが表示されます。

Dominion PX のリセット

CLI コマンドを使用して、Dominion PX デバイスを工場出荷時のデフォルトの設定にリセットしたり、単純に再起動したりすることができます。

PDU の再起動

このコマンドでは、Dominion PX デバイスが再起動されます。工場出荷時のデフォルトの設定にはリセットされません。

▶ **Dominion PX デバイスを再起動するには、次の手順に従います。**

1. 管理者モードになっていて、# プロンプトが表示されていることを確認します。
2. 次のいずれかのコマンドを入力して、Dominion PX デバイスを再起動します。

```
#      reset unit
      -- または --
#      reset unit /y
```

3. 手順 2 で「/y」を指定せずにコマンドを入力した場合は、操作の確認を求めるメッセージが表示されます。「y」と入力して、リセットを確認します。
4. リセットの完了を示す [Username (ユーザ名)] プロンプトが表示されるまで待ちます。

工場出荷時設定へのリセット

このコマンドでは、Dominion PX デバイスのすべての設定が工場出荷時のデフォルトの設定に戻されます。

▶ **Dominion PX の設定をリセットするには、次のいずれかのコマンドを使用します。**

```
#      reset factorydefaults
      -- または --
#      reset factorydefaults /y
```

詳細については、「*CLI コマンドの使用*」『444p.』を参照してください。

ネットワークのトラブルシューティング

Dominion PX には、ネットワークに関する問題のトラブルシューティングを行うための *nslookup*、*netstat*、*ping*、および *traceroute* という 4 つの診断コマンドが用意されています。診断コマンドは、対応する Linux コマンドとして機能し、実行すると、対応する Linux の出力が得られます。

診断モードへの移行

診断コマンドは、診断モードでのみ機能します。

▶ **診断モードに移行するには、次の手順に従います。**

1. 管理者モードになっていて、# プロンプトが表示されていることを確認します。
2. 「diag」と入力して、Enter キーを押します。diag> プロンプトが表示され、診断モードに移行したことがわかります。
3. これで、トラブルシューティング用の診断コマンドを入力できます。

診断コマンド

診断コマンドの構文は、コマンドによって異なります。

DNS サーバの照会

次のコマンド構文では、ネットワーク ホストのインターネット ドメイン ネーム サーバ (DNS) 情報を照会できます。

```
diag> nslookup <host>
```

変数:

- <host> は、DNS 情報を照会するホストの名前または IP アドレスです。

例

次のコマンドでは、ホスト 192.168.84.222 に関する DNS 情報を確認できます。

```
diag> nslookup 192.168.84.222
```

ネットワーク接続の表示

次のコマンド構文では、ネットワーク接続やポートの状態が表示されます。

```
diag> netstat <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *ports* または *connections*。

オプション	説明
ports	TCP/UDP ポートを表示します。
connections	ネットワーク接続を表示します。

例

次のコマンドでは、Dominion PX デバイスへのサーバ接続が表示されます。

```
diag> netstat connections
```


ネットワーク接続のテスト

次のコマンド構文では、ICMP ECHO_REQUEST メッセージがネットワーク ホストに送信され、ネットワーク接続を確認できます。このコマンドの出力でホストが正常に応答していると示された場合は、ネットワーク接続に問題がないか、または、ホストがシャットダウンされているか、ネットワークに接続されていません。

```
diag> ping <host>
```

変数:

- <host> は、ネットワーク接続を確認するホスト名または IP アドレスです。

オプション:

- ping コマンドでは、以下の追加オプションの一部または全部を指定できます。

オプション	説明
count <number1>	送信されるメッセージの数を指定します。 <number1> は、整数値です。
size <number2>	パケット サイズを指定します。<number2> は、バイト数を表す整数値です。
timeout <number3>	タイムアウトまでの待機時間を指定します。 <number3> は、秒数を表す整数値です。

すべてのオプションを指定した場合のコマンド構文は、次のようになります。

```
diag> ping <host> count <number1> size <number2> timeout <number3>
```

例

次のコマンド構文では、ICMP ECHO_REQUEST メッセージを 5 回ホストに送信することによって、ホスト 192.168.84.222 のネットワーク接続を確認できます。

```
diag> ping 192.168.84.222 count 5
```

ルートの追跡

次のコマンド構文では、Dominion PX デバイスとネットワーク ホストの間のネットワーク ルートを追跡できます。

```
diag>          traceroute <host>
```

変数:

- <host> は、追跡するホストの名前または IP アドレスです。

例

次のコマンドでは、ホスト 192.168.84.222 の既存のネットワーク ルーティング情報が表示されます。

```
diag>          traceroute 192.168.84.222
```

診断モードの終了

▶ 診断モードを終了するには、次のコマンドを使用します。

```
diag>          exit
```

Enter キーを押すと # プロンプトが表示され、管理者モードになったことがわかります。

コマンドで使用できるパラメータの確認

特定のタイプの CLI コマンドで使用できるコマンドまたはパラメータがわからない場合は、該当するコマンドの末尾に空白文字と疑問符を追加すると、使用可能なコマンドが表示されます。使用可能なパラメータとその説明の一覧が表示されます。

以下に、確認するコマンドの例をいくつか示します。

- ▶ 「show」コマンドの使用可能なパラメータを確認する構文は、次のとおりです。

```
# show ?
```

- ▶ 使用可能なネットワーク設定パラメータを確認する構文は、次のとおりです。

```
config:# network ?
```

- ▶ 使用可能な役割設定パラメータを確認する構文は、次のとおりです。

```
config:# role ?
```

前のコマンドの取得

同じ接続セッション内で以前に入力したコマンドを取得するには、目的のコマンドが表示されるまで、キーボードの上矢印キー (↑) を押します。

コマンドの自動補完

CLI コマンドは、常に複数語で構成されています。一部の一意な CLI コマンド (reset コマンドなど) は、コマンドを一語ずつすべて入力しなくても、Tab キーまたは Ctrl+i キーを押すことで簡単に入力できます。

- ▶ 一意なコマンドを自動補完で入力するには、次の手順に従います。
1. コマンドの最初の数文字または数語を入力します。たとえば、「reset factorydefaults」コマンドの最初の語、つまり「reset」を入力します。
 2. 完全なコマンドが表示されるまで、Tab キーまたは Ctrl+i キーを押します。たとえば、reset コマンドの 1 語しか入力しなくても、Tab キーまたは Ctrl+i キーを押すと、コマンドの残りが表示されます。

CLI のログアウト

CLI を使用する作業を終了した後は、必ず CLI からログアウトし、他の人が CLI にアクセスできないようにしてください。

▶ **CLI からログアウトするには、次の手順に従います。**

1. 管理者モードになっていて、# プロンプトが表示されていることを確認します。
2. 「exit」と入力して、Enter キーを押します。

この章の内容

電源測定精度.....	437
最高動作周囲温度.....	437
シリアル RS-232 ポートのピン配列.....	437
センサー RJ-12 ポートのピン配列.....	438

電源測定精度

次の測定精度は、モデル名が PX2 または PXE で始まるすべての Raritan PDU に適用されます。

	電源測定精度	測定精度の範囲
RMS 電圧 (V)	1%	
RMS 電流 (A)	1%+/-0.1A	0.1A ～定格電流
有効電力 (ワット)	1%	20W ～定格電力
皮相電力 (VA)	1%	20VA ～定格電力
電力量 (ワット時)	1%	

最高動作周囲温度

Dominion PX の最高動作周囲温度 (TMA) は、モデルや認定規格 (CE または UL) によって異なり、摂氏 50 ～ 60 度です。モデルのこの情報については、必要に応じて Raritan テクニカル サポートにお問い合わせください。

仕様	測定
最高動作温度	摂氏 50 ～ 60 度

シリアル RS-232 ポートのピン配列

RS-232 ピン/信号の定義			
ピン番号	信号	方向	説明
1	DCD	入力	データ
2	RxD	入力	受信データ（入力データ）
3	TxD	出力	転送データ
4	DTR	出力	データ ターミナル準備完了
5	GND	—	シグナル グラウンド
6	DSR	入力	データ セット準備完了
7	RTS	出力	送信する要求
8	CTS	入力	送信するクリア
9	RI	入力	鳴動インジケータ

センサー RJ-12 ポートのピン配列

RJ-12 ピン/信号の定義			
ピン番号	信号	方向	説明
1	+12V	—	電源 (500mA、ヒューズ保護)
2	GND	—	シグナル グラウンド
3	—	—	—
4	—	—	—
5	GND	—	シグナル グラウンド
6	単線		拡張ポートに使用

Dominion PX シリーズ モデル _____

Dominion PX シリーズ シリアル番号 _____

アウトレット (コンセント) 1	アウトレット (コンセント) 2	アウトレット (コンセント) 3
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況
アウトレット (コンセント) 4	アウトレット (コンセント) 5	アウトレット (コンセント) 6
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況

Ap B: 装置の設定ワークシート

アウトレット (コンセント) 7	アウトレット (コンセント) 8	アウトレット (コンセント) 9
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況
アウトレット (コンセント) 10	アウトレット (コンセント) 11	アウトレット (コンセント) 12
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況
アウトレット (コンセント) 13	アウトレット (コンセント) 14	アウトレット (コンセント) 15
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況

アウトレット（コンセント） 16	アウトレット（コンセント） 17	アウトレット（コンセント） 18
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況
アウトレット（コンセント） 19	アウトレット（コンセント） 20	アウトレット（コンセント） 21
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況

Ap B: 装置の設定ワークシート

アウトレット (コンセント) 22	アウトレット (コンセント) 23	アウトレット (コンセント) 24
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況

アダプタのタイプ

ケーブルのタイプ

ソフトウェア プログラム名

セキュリティ上の理由により、Dominion PX デバイスを工場出荷時のデフォルト設定にリセットする操作は、ローカルのコンソールからのみ行うことができます。

重要: Dominion PX を工場出荷時の設定にリセットする場合は注意が必要です。リセットすると、既存の情報やカスタマイズした設定 (ユーザ プロファイル、しきい値など) が消去されます。電力量データおよびファームウェア アップグレードの履歴のみが引き続き保持されます。

リセット (RESET) ボタンまたはコマンド ライン インタフェース (CLI) を使用して、Dominion PX をリセットできます。

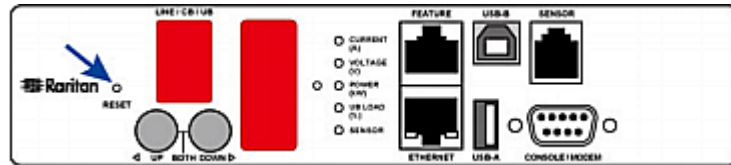
この章の内容

リセット (RESET) ボタンの使用	443
CLI コマンドの使用	444

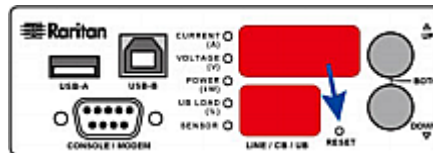
リセット (RESET) ボタンの使用

- ▶ **リセット (RESET) ボタン**を使用して工場出荷時のデフォルトの設定にリセットするには、次の手順に従います。
- 1. コンピュータを Dominion PX デバイスに接続します。「**コンピュータへの Dominion PX の接続**『22p.』」を参照してください。
- 2. ハイパーターミナル、Kermit、PuTTY などのターミナル エミュレーション プログラムを起動して、Dominion PX のウィンドウを開きます。シリアル ポートの設定については、「**初期ネットワーク設定**『26p.』」の手順 2 を参照してください。
- 3. キーボードの Esc キーを数回すばやく押し続けながら、Dominion PX デバイスのリセット (RESET) ボタンを押して放します。約 1 秒後にプロンプト (=) が表示されます。
- 4. 「defaults」と入力して、Dominion PX を工場出荷時のデフォルトの設定にリセットします。
- 5. リセットの完了を示す [Username (ユーザ名)] プロンプトが表示されるまで待ちます。

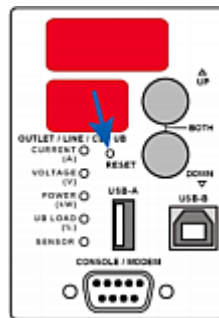
次の図は、ゼロ U モデルのリセット (RESET) ボタンの場所を示しています。



次の図は、1U モデルのリセット (RESET) ボタンの場所を示しています。



次の図は、2U モデルのリセット (RESET) ボタンの場所を示しています。



注: ハイパーターミナルは、Windows Vista より前の Windows オペレーティング システムで使用できます。Windows Vista 以降のバージョンでは、PuTTY を使用できます。このツールは、インターネットからダウンロードできる無償のプログラムです。詳細な設定方法は、PuTTY のマニュアルを参照してください。

CLI コマンドの使用

コマンド ライン インタフェース (CLI) には、Dominion PX を工場出荷時のデフォルト設定に戻すためのリセット コマンドが用意されています。CLI については、「**コマンド ライン インタフェースの使用**『274p.』」を参照してください。

- ▶ **CLI コマンドを使用して工場出荷時のデフォルト設定にリセットするには、次の手順に従います。**
- 1. コンピュータを Dominion PX デバイスに接続します。「**コンピュータへの Dominion PX の接続**『22p.』」を参照してください。

2. ハイパーターミナル、Kermit、PuTTY などのターミナル エミュレーション プログラムを起動して、Dominion PX のウィンドウを開きます。シリアル ポートの設定については、「**初期ネットワーク設定『26p.』**」の手順 2 を参照してください。
3. ユーザ名「admin」とそのパスワードを入力して、CLI にログインします。「**初期ネットワーク設定『26p.』**」の手順 4 を参照してください。
4. # システム プロンプトが表示されたら、次のいずれかのコマンドを入力して、Enter キーを押します。

```
#      reset factorydefaults
```

-- または --

```
#      reset factorydefaults /y
```
5. 手順 4 で「/y」を指定せずにコマンドを入力した場合は、操作の確認を求めるメッセージが表示されます。「y」と入力して、リセットを確認します。
6. リセットの完了を示す [Username (ユーザ名)] プロンプトが表示されるまで待ちます。

このセクションでは、LDAP の例を挙げて、Microsoft Active Directory® (AD) を使用した設定手順について解説します。LDAP 認証を設定するには、大まかに次の 4 つの手順が必要です。

- a. Dominion PX のためのユーザ アカウントおよびグループを決定する。
- b. AD サーバ上に Dominion PX のユーザ グループを作成する。
- c. Dominion PX デバイス上で LDAP 認証を設定する。
- d. Dominion PX デバイス上で役割を設定する。

この章の内容

手順 A. ユーザ アカウントとグループの決定	446
手順 B. AD サーバでのユーザ グループの設定	447
手順 C. Dominion PX デバイスでの LDAP 認証の設定	448
手順 D. Dominion PX デバイスでのユーザ グループの設定	451

手順 A. ユーザ アカウントとグループの決定

Dominion PX へのアクセスを認証するユーザ アカウントとグループを決定します。この例では、異なる権限を持つ 2 つのユーザ グループを作成します。それぞれのグループは、AD サーバ上で使用可能な 2 つのユーザ アカウントで構成されます。

ユーザ グループ	ユーザ アカウント (メンバー)
PX_User	usera
	pxuser2
PX_Admin	userb
	pxuser

グループ権限:

- PX_User グループには、システムの権限もアウトレット (コンセント) の権限も付与しません。
- PX_Admin グループには、システムとアウトレット (コンセント) に対するすべての権限を付与します。

手順 B. AD サーバでのユーザ グループの設定

AD サーバ上で Dominion PX のグループを作成した後、これらのグループの適切なユーザ メンバーを作成する必要があります。

この例における前提は、次のとおりです。

- Dominion PX のグループの名前は、*PX_Admin* および *PX_User* である。
- ユーザ アカウント *pxuser*、*pxuser2*、*usera*、および *userb* が AD サーバに存在している。

▶ AD サーバ上でユーザ グループを設定するには、次の手順に従います。

1. AD サーバ上で新しいグループ (*PX_Admin* と *PX_User*) を作成します。

注: 詳細な手順については、Microsoft AD に付属するマニュアルまたはオンライン ヘルプを参照してください。

2. *PX_User* グループに *pxuser2* アカウントと *usera* アカウントを追加します。
3. *PX_Admin* グループに *pxuser* アカウントと *userb* アカウントを追加します。
4. 各グループが正しいユーザ構成になっているかどうかを確認します。



手順 C. Dominion PX デバイスでの LDAP 認証の設定

外部認証を使用するには、Dominion PX デバイス上で LDAP 認証を有効にして適切に設定する必要があります。

この例における前提は、次のとおりです。

- DNS サーバが正しく設定されている。「**ネットワーク設定の変更**」『93p.』および「**DNS サーバの役割**」『97p.』を参照してください。
- AD サーバのドメイン名が `techadssl.com` であり、その IP アドレスが `192.168.56.3` である。
- AD プロトコルが SSL を介して暗号化されていない。
- AD サーバでデフォルトの TCP ポート `389` が使用されている。
- 匿名バインドが使用されている。

▶ LDAP 認証を設定するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)] を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。
2. [LDAP] ラジオ ボタンを選択し、リモート LDAP/LDAPS サーバ認証をアクティブにします。
3. [New (新規)] をクリックし、認証用の LDAP/LDAPS サーバを追加します。[Create new LDAP Server Configuration (LDAP サーバ設定の新規作成)] ダイアログ ボックスが表示されます。
4. Dominion PX に AD サーバに関する情報を設定します。
 - [IP Address / Hostname (IP アドレス / ホスト名)] – ドメイン名「`techadssl.com`」または IP アドレス「`192.168.56.3`」を入力します。

重要: SSL 暗号化が有効になっていなくても、このフィールドにドメイン名または IP アドレスを入力できますが、SSL 暗号化が有効になっている場合は、完全修飾ドメイン名を入力する必要があります。

- [Use settings from LDAP server (LDAP サーバからの設定を使用する)] – このチェックボックスは、オフのままにします。
- [Type of LDAP Server (LDAP サーバのタイプ)] – ドロップダウン リストから [Microsoft Active Directory] を選択します。
- LDAP over SSL – この例では SSL 暗号化が適用されないなので、このチェックボックスはオフにしておきます。
- [Port (ポート)] – このフィールドに `389` が設定されていることを確認します。

- [SSL Port (SSL ポート)] と [Server Certificate (サーバ証明書)] – SSL 暗号化が有効になっていないので、この 2 つのフィールドはスキップします。
- [Use Bind Credentials (バインド証明書を使用)] – 匿名バインドが使用されるため、このチェックボックスをオンにしないでください。
- [Bind DN (バインド DN)]、[Bind Password (バインド パスワード)]、[Confirm Bind Password (バインド パスワードの確認)] – 匿名バインドが使用されるため、3 つのフィールドはスキップします。
- [Base DN for Search (検索用のベース DN)] – AD サーバ上での検索の開始点として「dc=techadssl,dc=com」を入力します。
- [Login Name Attribute (ログイン名の属性)] – LDAP サーバが Microsoft Active Directory であるため、このフィールドが sAMAccountName に設定されていることを確認します。
- [User Entry Object Class (ユーザ エントリのオブジェクト クラス)] – LDAP サーバが Microsoft Active Directory であるため、このフィールドが user に設定されていることを確認します。
- [User Search Subfilter (ユーザ検索サブフィルタ)] – このフィールドはオプションです。サブフィルタ情報は、大規模なディレクトリ構造においてオブジェクトを絞り込む場合にも役立ちます。この例では、このフィールドは空白のままにします。

- [Active Directory Domain (Active Directory ドメイン)] – 「techadssl.com」と入力します。

Create new LDAP Server Configuration

IP Address / Hostname: 192.168.56.3

☐ Use settings from LDAP Server

Select LDAP Server

Type of LDAP Server: Microsoft Active Directory

☐ LDAP over SSL

Port: 389

SSL Port: 636

☐ Use only trusted LDAP Server Certificates

Server Certificate: not set Show... Remove...

select new certificate... Browse...

☐ Anonymous Bind

☐ Use Bind Credentials

Bind DN:

Bind Password:

Confirm Bind Password:

Base DN for Search: dc=techadssl,dc=com

Login Name Attribute: sAMAccountName

User Entry Object Class: user

User Search Subfilter:

Active Directory Domain: techadssl.com

Test Connection

OK Cancel

注: LDAP 設定の詳細については、『LDAP 認証の設定 146p.』を参照してください。

5. [OK] をクリックして変更を保存します。LDAP サーバが保存されます。
6. [OK] をクリックして変更を保存します。LDAP 認証がアクティブになります。

注: *Dominion PX* クロックと *LDAP* サーバ クロックが同期されていない場合は、証明書が期限切れと見なされ、ユーザは *LDAP* を使用した認証ができません。適切な同期を維持するために、管理者は、*Dominion PX* と *LDAP* サーバが同じ *NTP* サーバを使用するように設定する必要があります。

手順 D. *Dominion PX* デバイスでのユーザ グループの設定

Dominion PX デバイスでの役割によって、システムおよびアウトレット (コンセント) の権限が決まります。AD サーバ上で作成した、*Dominion PX* のユーザ グループと同じ名前の役割を作成する必要があります。名前が同じでない場合、承認が失敗します。そのため、ここでは PDU 上に *PX_User* および *PX_Admin* という名前の役割を作成します。

この例における前提は、次のとおりです。

- *PX_User* の役割を割り当てられたユーザは、*Dominion PX* の設定も、アウトレット (コンセント) へのアクセスもできない。
- *PX_Admin* の役割を割り当てられたユーザは、管理者の権限を持ち、*Dominion PX* の設定も、アウトレット (コンセント) へのアクセスもできる。

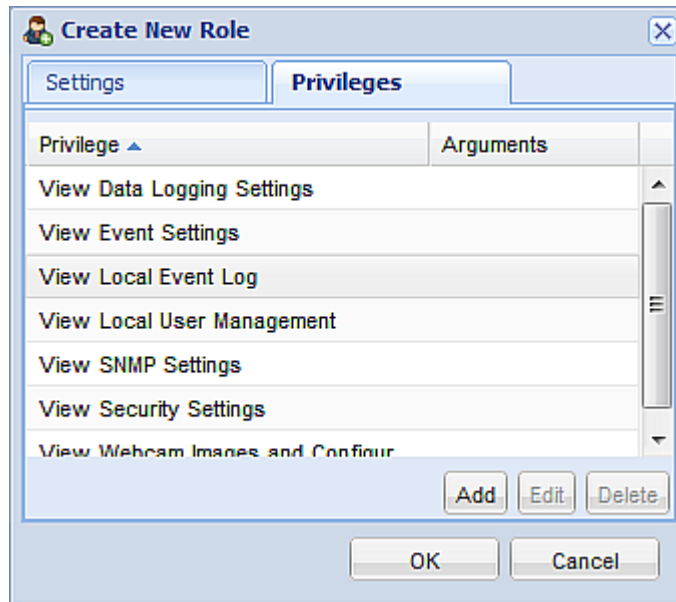
▶ *PX_User* という役割を作成し、適切な権限を設定するには、次の手順に従います。

1. [User Management (ユーザ管理)] > [Roles (役割)] を選択します。
[Manage Roles (役割の管理)] ダイアログ ボックスが表示されます。

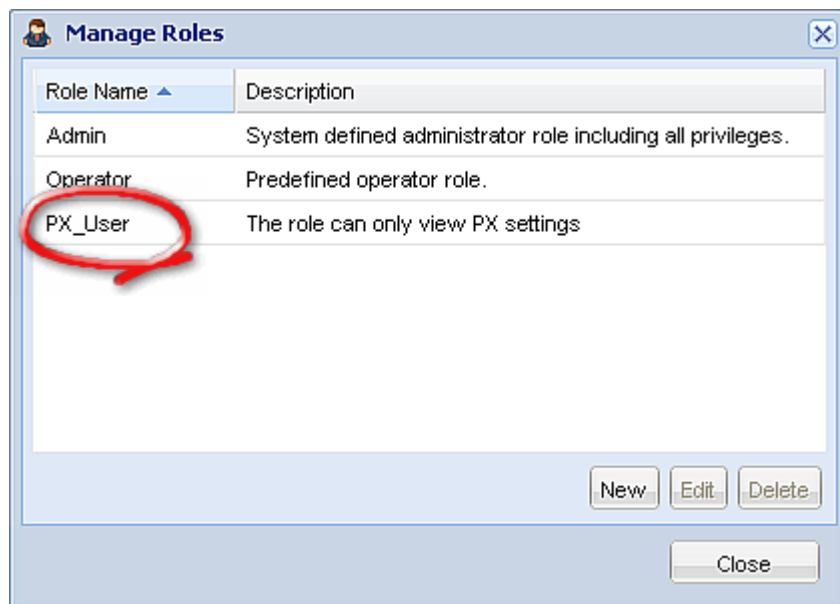
ヒント: [Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスの [Manage Roles (役割の管理)] ボタンをクリックして、[Manage Roles (役割の管理)] ダイアログ ボックスにアクセスすることもできます。

2. [New (新規)] をクリックします。[Create New Role (役割の新規作成)] ダイアログ ボックスが表示されます。
3. [Role Name (役割名)] フィールドに「*PX_User*」と入力します。
4. [Description (説明)] フィールドに役割 *PX_User* の説明を入力します。
この例では、役割の説明として「The role can only view PX settings (この役割では *PX* 設定の参照のみが可能)」と入力します。
5. [Privileges (権限)] タブをクリックし、すべての [View XXX permissions (XXX の表示権限)] を選択します (XXX は設定の名前です)。
[View XXX permissions (XXX 権限の表示)] を選択すると、ユーザは XXX の設定を表示できますが、設定または変更はできません。
 - a. [Add (追加)] をクリックします。[Add Privileges to new Role (新しい役割への権限の追加)] ダイアログ ボックスが表示されます。

- b. [Privileges (権限)] のリストから「View (表示)」という語で始まる権限 ([View Event Settings (イベント設定の表示)] など) を選択します。
- c. [Add (追加)] をクリックします。
- d. 手順 a ～ c を繰り返して、「View (表示)」で始まる権限をすべて追加します。



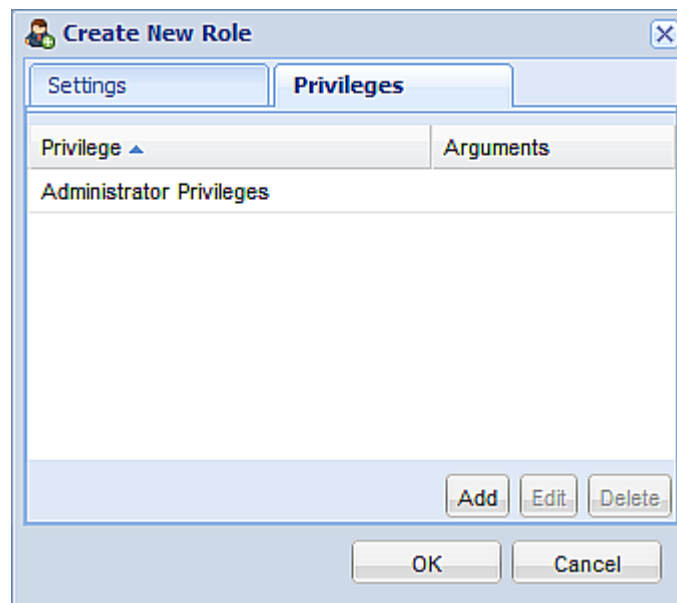
6. [OK] をクリックして変更を保存します。役割 PX_User が作成されます。



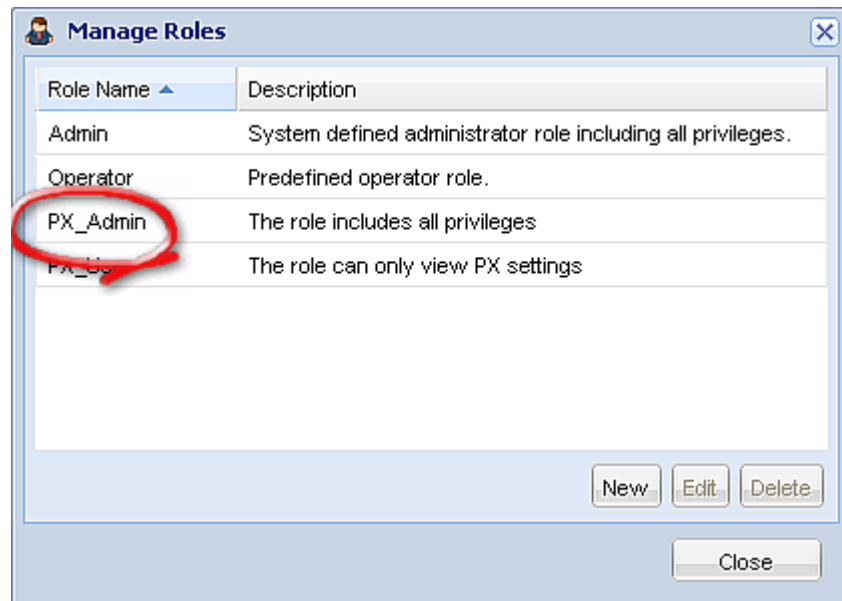
7. 役割 PX_Admin を作成するために、[Manage Roles (役割の管理)] ダイアログ ボックスを開いたままにします。

▶ **PX_Admin という役割を作成し、すべての権限を付与するには、次の手順に従います。**

1. [New (新規)] をクリックします。[Create New Role (役割の新規作成)] ダイアログ ボックスが表示されます。
2. [Role Name (役割名)] フィールドに「PX_Admin」と入力します。
3. [Description (説明)] フィールドに役割 PX_Admin の説明を入力します。この例では、役割の説明として「The role includes all privileges (この役割はすべての権限を持つ)」と入力します。
4. [Privileges (権限)] タブをクリックして、管理者権限を選択します。管理者権限により、ユーザは、Dominion PX のすべての設定について設定または変更ができます。
 - a. [Add (追加)] をクリックします。[Add Privileges to new Role (新しい役割への権限の追加)] ダイアログ ボックスが表示されます。
 - b. [Privileges (権限)] の一覧から [Administrator Privileges (管理者権限)] という名前の権限を選択します。
 - c. [Add (追加)] をクリックします。



5. [OK] をクリックして変更を保存します。役割 PX_Admin が作成されます。



6. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

Dominion PX デバイスは、特定の Raritan 製品または Raritan 以外の製品と連動してさまざまな電源ソリューションを提供できます。

この章の内容

Power IQ の設定	455
Dominion KX II 設定	457
RF Code エネルギー監視ソリューション	463

Power IQ の設定

Raritan の Power IQ は、サーバ ルームまたはデータ センターに設置されているさまざまな PDU からデータを収集し、管理するソフトウェアアプリケーションです。このソフトウェアを使用して次の操作を実行できます。

- 複数の PDU の一括設定
- さまざまな PDU のアウトレット (コンセント) の名前付け
- アウトレット (コンセント) 切り替え対応 PDU のアウトレット (コンセント) のオン/オフの切り替え

Power IQ の詳細については、次のいずれかを参照してください。

- 『Power IQ User Guide』: Raritan Web サイトの「*Firmware and Documentation* (ファームウェアとドキュメント)」
『<http://www.raritan.com/support/firmware-and-documentation/参照>』セクションで入手できます。
- Power IQ オンライン ヘルプ: 「*Product Online Help* (製品オンラインヘルプ)」
『<http://www.raritan.com/support/online-help/参照>』セクションから参照できます。

Power IQ の管理への PDU の追加

Power IQ を設定した後、Dominion PX またはその他の PDU を管理対象として追加します。こうすることで、Power IQ はこれらの PDU のデータを収集できるようになります。

情報を含む CSV ファイルをアップロードして PDU を Power IQ に追加することもできます。『Power IQ ユーザ ガイド』の「CSV ファイルで PDU を一括追加する」を参照してください。

この手順に従って、Power IQ に Raritan EMX を追加します。

▶ Power IQ の管理に PDU を追加するには、次の手順に従います。

1. [PDU's (PDU)] タブで、[Add (追加)] をクリックします。

2. PDU の IP アドレスを入力します。
3. PDU がディジーチェーン設定またはコンソール サーバ設定に組み込まれている場合、チェーンにおける PDU の位置番号またはシリアル ポート番号を [Proxy Index (プロキシ インデックス)] フィールドに入力します。

注: この種の設定に PDU がない場合、[Proxy Index (プロキシ インデックス)] フィールドは空白のままにします。

4. 資産タグ番号または他の資産管理コードを [外部キー] フィールドに入力します。これはオプションです。
5. データを [カスタム フィールド 1] と [カスタム フィールド 2] に入力します。これはオプションです。Power IQ では、これらのフィールドを識別するためにラベルが変更されている場合があります。
6. PDU が Dominion PX の場合、[Dominion PX Credentials (Dominion PX 資格情報)] セクションに PDU に対する有効なユーザ名とパスワードを入力します。[Password Confirm (パスワードの確認)] フィールドにパスワードを再度入力します。
7. SNMP バージョンを選択します。
 - SNMP バージョン 1/2c の PDU では、少なくともこの PDU に対する読み込み権限を持っている SNMP コミュニティ文字列を入力します。これによって、PDU のデータのポーリングが有効になります。PDU への読み込みと書き込みの両方の権限を持っている SNMP コミュニティ文字列を入力すると、電源制御、アウトレット (コンセント) 名の変更、およびバッファ データの取得が有効になります。
 - SNMP バージョン 3 の PDU では、ユーザ名を入力し、[Authorization Level (認証レベル)] を選択します。認証レベルは、次のとおりです。
 - noAuthNoPriv - 認証パスキーなし、エンコード パスキーなし
 - authNoPriv - 認証パスキーあり、エンコード パスキーなし
 - authPriv - 認証パスキーあり、エンコード パスキーあり
 - a. 選択した認証レベルによっては、認証とプライバシーに対するその他の資格情報を入力する必要があります。
 - b. Authorization Protocol (認証プロトコル): [MD5] または [SHA] を選択します。
 - c. PDU の認証パスキーを入力し、[Authorization Passkey Confirm (認証パスキーの確認)] フィールドにパスキーを再度入力します。
 - d. Privacy Protocol (プライバシー プロトコル): [DES] または [AES] を選択します。
 - e. PDU のプライバシー パスキーを入力し、[Privacy Passkey Confirm (プライバシー パスキーの確認)] フィールドにパスキーを再度入力します。

注: Power IQ に追加されているすべての PDU に対して SNMP エージェントを有効にする必要があります。

8. [Validate and wait for discovery to complete before proceeding (検索が完了した後で処理を続ける)] を選択し、資格情報を検査し、この PDU を追加する際の検出プロセスのステータスを表示します。**これはオプションです。**『Power IQ ユーザ ガイド』の「PDU 資格情報の検査」を参照してください。
9. [Add (追加)] をクリックします。

注: PDU 検索は、PDU モデル タイプが決定されると終了します。連絡先または場所の値などの SNMP フィールドは、このデバイスが初めて検出されるまで不明です。

追加された PDU は、PDU リストに表示されます。Power IQ でセンサー データに対する PDU のポーリングが開始されます。Power IQ で PDU のポーリング間隔を設定できます。『Power IQ ユーザ ガイド』の「ポーリング間隔を設定する」を参照してください。

Dominion KX II 設定

PX2 シリーズの PDU を Raritan の Dominion KX II デバイス (デジタル KVM スイッチ) に接続して、電源制御機能をもう 1 つ提供できます。

この統合には、次のファームウェア バージョンが必要です。

- Dominion KX II -- 2.4 以降
- PX2 シリーズ -- 2.2 以降

Dominion KX II との統合には、D2CIM-PWR およびストレート CAT5 ケーブルが必要です。

Dominion KX II の詳細については、次のいずれかを参照してください。

- 『Dominion KX II ユーザ ガイド』: Raritan Web サイトの「**Firmware and Documentation (ファームウェアとドキュメント)**」
『<http://www.raritan.com/support/firmware-and-documentation/>参照』」セクションで入手できます。
- Dominion KX II オンライン ヘルプ: 「**Product Online Help (製品オンライン ヘルプ)**」『<http://www.raritan.com/support/online-help/>参照』」セクションから参照できます。

ラック PDU (電源タップ) ターゲットの設定

KX II では、ラック PDU (電源タップ) を KX II ポートに接続できます。KX II のラック PDU の設定は、KX II の [Port Configuration (ポート設定)] ページから行います。

ラック PDU の接続

ラック PDU は、D2CIM-PWR CIM を使用して KX II に接続します。

▶ **ラック PDU を接続するには、次の手順に従います。**

1. D2CIM-PWR のオス RJ-45 をラック PDU の「FEATURE」というラベルのメス RJ-45 コネクタに接続します。
2. D2CIM-PWR のメス RJ-45 コネクタを、Cat5 ストレート ケーブルで KX II の利用可能なメス システム ポート コネクタのいずれかに接続します。
3. AC 電源コードをターゲット サーバと利用可能なラック PDU アウトレット (コンセント) に接続します。
4. ラック PDU を AC 電源に接続します。
5. デバイスの電源をオンにします。



KX II または LX でのラック PDU の名前付け (電源タップの [Port (ポート)] ページ)

注: PX ラック PDU (電源タップ) の名前は、PX、KX II、および LX で指定できます。

Raritan リモート ラック PDU が KX II または LX に接続されると、それが [Port Configuration (ポート設定)] ページに表示されます。そのページにある電源ポート名をクリックしてアクセスします。[Type (タイプ)] および [Name (名前)] フィールドはあらかじめ指定されています。

注: (CIM) タイプは変更できません。

ラック PDU の各アウトレット (コンセント) に関する次の情報が表示されます。コンセントの [Number (番号)]、[Name (名前)]、[Port Association (ポートの関連付け)]。

このページを使用して、ラック PDU とそのアウトレット (コンセント) に名前を付けます。名前には最大 32 文字の英数字が使用でき、特殊文字を含めることができます。

注: ラック PDU がターゲット サーバ (ポート) と関連付けられると、アウトレット (コンセント) 名はターゲット サーバ名に置き換えられます。アウトレット (コンセント) に別の名前を割り当てている場合も同様です。

► **ラック PDU とアウトレット (コンセント) に名前を付けるには、次の手順に従います。**

注: CommandCenter Secure Gateway では、スペースを含むラック PDU 名を認識できません。

1. ラック PDU の名前を入力します (必要な場合)。
2. 必要に応じて、([アウトレット (コンセント)]) [Name (名前)] を変更します。(アウトレット (コンセント) 名は「outlet #」です。)

3. [OK] をクリックします。

Home > Device Settings > Port Configuration > Port

Port 17

Type:
PowerStrip

Name:

Outlets

Number	Name	Port Association
1	Dominion-Port1(1)	Dominion- Port7
2	Outlet 2	
3	Outlet 3	
4	Outlet 4	
5	Outlet 5	
6	Outlet 6	
7	Outlet 7	
8	Outlet 8	

KX II および LX でのアウトレット (コンセント) とターゲット サーバの関連付け

[Port Configuration (ポート設定)] ページでポートをクリックすると、[Port (ポート)] ページが開きます。このページで電源の関連付けを行えます。ポートの名前を入力しやすい名前に変更し、D2CIM-VUSB CIM を使用している場合はターゲット サーバの設定を更新します。(CIM) [Type (タイプ)] および (ポート) [Name (名前)] フィールドはあらかじめ指定されています。CIM タイプは変更できないことに注意してください。

サーバには最大で 4 つの電源プラグを接続でき、それぞれに別のラック PDU (電源タップ) を関連付けられます。このページでそれらの関連付けを定義して、[Port Access (ポート アクセス)] ページからサーバの電源オン、オフ、再投入を行えます。

この機能を使用するには、以下が必要です。

- Raritan リモート ラック PDU
- Power CIM (D2CIM-PWR)

▶ 電源の関連付けを行う (ラック PDU コンセントを KVM ターゲット サーバに関連付ける) には、以下の手順に従います。

注: ラック PDU がターゲット サーバ (ポート) に関連付けられると、アウトレット (コンセント) 名はターゲット サーバ名に置き換えられます (アウトレット (コンセント) に別の名前を割り当てている場合も同様です)。

1. [Power Strip Name (電源タップ名)] ドロップダウン リストからラック PDU を選択します。
2. そのラック PDU に対して、[Outlet Name (アウトレット (コンセント) 名)] ドロップダウン リストからアウトレット (コンセント) を選択します。
3. 該当するすべての電源の関連付けで、手順 1 および 2 を繰り返します。
4. [OK] をクリックします。確認メッセージが表示されます。

▶ ポート名を変更するには、次の手順に従います。

1. [Name (名前)] フィールドにわかりやすい名前を入力します。候補としてはターゲット サーバ名が挙げられます。名前には最大 32 文字の英数字が使用でき、特殊文字を含めることができます。
2. [OK] をクリックします。

電源の関連付けの削除

ターゲット サーバまたはラック PDU をデバイスから取り外す場合は、まずすべての電源の関連付けを削除する必要があります。ターゲットがラック PDU に関連付けられたままでターゲットをデバイスから取り外した場合、電源の関連付けは残ります。この場合、電源の関連付けを適切に削除するために [Device Settings (デバイス設定)] で切断されたターゲット サーバの [Port Configuration (ポート設定)] にアクセスすることはできません。

▶ **ラック PDU の関連付けを削除するには、次の手順に従います。**

1. [Power Strip Name (電源タップ名)] ドロップダウン リストから適切なラック PDU を選択します。
2. そのラック PDU に対して、[Outlet Name (アウトレット (コンセント) 名)] ドロップダウン リストから適切なアウトレット (コンセント) を選択します。
3. [Outlet Name (アウトレット (コンセント) 名)] ドロップダウンリストから [None (なし)] を選択します。
4. [OK] をクリックします。そのラック PDU/アウトレット (コンセント) の関連付けが削除され、確認メッセージが表示されます。

▶ **ラック PDU がターゲットから削除されている場合にラック PDU の関連付けを削除するには、以下の手順に従います。**

1. [Device Settings (デバイス設定)] > [Port Configuration (ポート設定)] をクリックし、アクティブなターゲットをクリックします。
2. アクティブなターゲットを切断された電源ポートに関連付けます。これで、切断されたターゲットの電源の関連付けが破棄されます。

最後に、アクティブなターゲットを、正しい電源ポートに関連付けます。

RF Code エネルギー監視ソリューション

RF Code のアクティブ型 RFID ハードウェアおよび管理ソフトウェアと Raritan の Dominion PX を組み合わせることにより、電力利用のイメージを把握できるワイヤフリー エネルギー監視ソリューションが提供されます。

この組み合わせソリューションに IP アドレスの設定や関連付けを追加する必要はありません。必要なのは、RF Code R170 PDU センサー タグを Dominion PX デバイスの Sensor ポートに接続することだけです。

RF Code R170 PDU センサー タグにより、Raritan Dominion PX によって生成された電力データが収集され、RF Code Sensor Manager ソフトウェアに送信されます。このソフトウェアは、電力データを管理するだけでなく、収集されたデータに基づいて電力利用に関する計算も行います。

RF Code Sensor Manager では、次の機能を使用して電力データを管理できます。

- ライブ テーブル ビュー
- マップ ビュー
- 対話型のグラフ作成とレポート作成
- スケジュールされたグラフ作成とレポート作成
- 警告としきい値

この章の内容

MAC アドレス	464
アウトレット (コンセント) とコードのロック	464
高度補正率	467
BTU 計算のデータ	468
CLI コマンドの適用可能性	468
Web インタフェースでのデータの切り捨て	472

MAC アドレス

Dominion PX デバイスには、LED 表示の近くに、PDU のシリアル番号および MAC アドレスが記載されたラベルが貼付されています。



必要な場合は、一般的なネットワーク ツールを使用することで、MAC アドレスから PDU の IP アドレスを検出できます。サポートについては、LAN 管理者にお問い合わせください。

アウトレット (コンセント) とコードのロック

ケーブル リテンション クリップ以外にも、Raritan は IT 機器の電源コードを Raritan PDU にしっかり接続するための方法を用意しています。

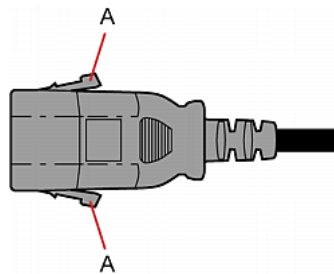
- SecureLock™ アウトレット (コンセント) およびコード
- ボタンタイプのロック アウトレット (コンセント)

すべての Raritan PDU が上記のロック アウトレット (コンセント) を備えているわけではありません。

SecureLock™ アウトレット (コンセント) およびコード

SecureLock™ は、Raritan が設計した革新的な機構で、Raritan PDU に接続された C14 または C20 プラグがしっかり固定されます。この方法は、次の 2 つのコンポーネントを必要とします。

- SecureLock™ アウトレット (コンセント) を備えた Raritan PDU。アウトレット (コンセント) の両側にラッチ スロットが内蔵されています。
- SecureLock™ コード。プラグの両側にロック ラッチが付いた電源コードです。次の図にこのプラグを示します。



項目	説明
A	SecureLock™ コードのプラグのラッチ

SecureLock™ 機構を備えているのは特定の PDU のみです。使用している PDU がこの設計ではない場合は、SecureLock™ コードを使用しないでください。

ヒント: SecureLock™ アウトレット (コンセント) では、標準の電源コードを使用した電力供給が可能ですが、SecureLock™ 機構の効果はありません。

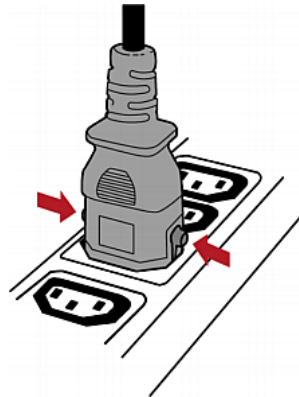
▶ SecureLock™ 機構を使用して電源コードをロックするには、次の手順に従います。

1. 購入した SecureLock™ コードがニーズに合っていることを確認します。
 - コードのメス ソケットが IT 機器の電源ソケットのタイプ (C14 または C20) と合っている。
 - コードのオス プラグが PDU のアウトレット (コンセント) のタイプ (C13 または C19) と合っている。
2. IT 機器と PDU を SecureLock™ コードで接続します。
 - コードのメス ソケット側を、使用する IT 機器の電源ソケットに接続します。

- コードのオス プラグを、PDU の適切な SecureLock™ アウトレット (コンセント) に接続します。アウトレット (コンセント) にプラグを挿して、プラグのラッチがアウトレット (コンセント) のラッチ スロットにはまるカチッという音がするまで押し込みます。

▶ **PDU から SecureLock™ 電源コードを取り外すには、次の手順に従います。**

1. 次の図に示すように、コードのプラグの 2 つのラッチを押したままにします。



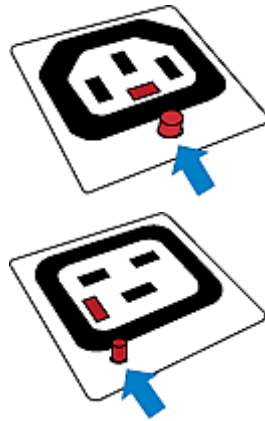
2. そのままコードを抜きます。

ボタンタイプのロック アウトレット (コンセント)

ボタンタイプのロック アウトレット (コンセント) には、ボタンがあります。このようなアウトレット (コンセント) は、特殊な電源コードがなくてもロックできます。標準の電源コードをロック アウトレット (コンセント) に挿すだけで、アウトレット (コンセント) によりコードが自動的にロックされます。

▶ **ロック アウトレット (コンセント) から電源コードを取り外すには、次の手順に従います。**

1. アウトレット (コンセント) の小さいボタンを押したままにします。ボタンの位置は、アウトレット (コンセント) のタイプに応じて異なります。



2. そのまま電源コードを抜きます。

高度補正率

Raritan 空気差圧センサーがデバイスに接続されている場合、そのデバイスに対して入力した高度は、高度補正率として使用できます。つまり、空気差圧センサーの測定値には、正しい測定値を取得するために補正率が掛けられます。

次の表に、さまざまな高度と補正率の関係を示します。

高度 (メートル)	高度 (フィート)	補正率
0	0	0.95
250	820	0.98
425	1394	1.00
500	1640	1.01
740	2428	1.04

高度 (メートル)	高度 (フィート)	補正率
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

BTU 計算のデータ

Dominion PX デバイスで発生する熱量は、購入したモデルによって異なります。熱量 (BTU/hr) を計算するには、BTU 計算式でモデル タイプに従って次の電力データを使用します。

モデル名	最大電力 (ワット)
PX2-1nnn シリーズ	5
PX2-2nnn シリーズ	20
PX2-3nnn シリーズ	24
PX2-4nnn シリーズ	24
PX2-5nnn シリーズ	24

モデル名に含まれる文字「n」は、数字を表します。

CLI コマンドの適用可能性

Dominion PX PDU ではモデルごとに機能が異なるので、すべての CLI コマンドがすべての PDU に適用されるわけではありません。たとえば、PX-1000 シリーズには、アウトレット (コンセント) 切り替え機能が搭載されていないので、アウトレット (コンセント) 切り替えコマンドは適用できません。

この付録の表は、さまざまな Dominion PX 製品ラインに対するコマンドの適用可能性を示しています。以下はすべての表で共通です。

- PX-1000 は、PX2-1000 ～ PX2-1999 の範囲の PDU を示します。
- PX-2000 は、PX2-2000 ～ PX2-2999 の範囲の PDU を示します。

Show コマンド

次の表は、show コマンドの適用可能性を示しています。

- Y: 適用可能
- N: 適用不可

CLI コマンド	PX-1000	PX-2000
show assetStrip <n>	Y	Y
show assetStripManagement	Y	Y
show energywise	Y	Y
show externalsensors <n> (details)	Y	Y
show history	Y	Y
show history bufferlength	Y	Y
show inlets <n> (details)	Y	Y
show loadshedding	N	Y
show network	Y	Y
show network mode	Y	Y
show network services <option>	Y	Y
show network wireless (details)	Y	Y
show ocp <n> (details)	Y	Y
show outlets <n> (details)	Y	Y
show pdu (details)	Y (1)	Y
show reliability data	Y	Y
show reliability errorlog <n>	Y	Y
show roles <role_name>	Y	Y
show security (details)	Y	Y
show sensor externalsensor <n> (details)	Y	Y
show sensor inlet <n> <sensor type> (details)	Y	Y
show sensor inletpole <n> <p> <sensor type> (details)	Y	Y
show sensor ocp <n> <sensor type> (details)	Y	Y
show serial	Y	Y
show time (details)	Y	Y
show user <user_name> (details)	Y	Y
show network wireless (details)	Y	Y

注:

- PX-1000 シリーズでは、show pdu (details) コマンドの実行後、次の PDU 情報を利用できません。
 - 起動時のアウトレット（コンセント）のデフォルト状態
 - アウトレット（コンセント）の電源の順序
 - アウトレット（コンセント）の電源のシーケンス遅延

設定コマンド

次の表は、設定コマンドの適用可能性を示しています。

- Y: 適用可能
- N: 適用不可

CLI コマンド	PX-1000	PX-2000
すべての network コマンド	Y	Y
すべての network services コマンド	Y	Y
すべての security コマンド	Y	Y
すべての inlet コマンド	Y	Y
すべての ocp コマンド	Y	Y
すべての externalsensor コマンド	Y	Y
すべての sensor inlet コマンド	Y	Y
すべての sensor inletpole コマンド	Y	Y
すべての sensor ocp コマンド	Y	Y
すべての sensor externalsensor コマンド	Y	Y
すべての serial コマンド	Y	Y
すべての time コマンド	Y	Y
すべての user コマンド	Y	Y
すべての role コマンド	Y	Y
すべての energywise コマンド	Y	Y
すべての assetStrip コマンド	Y	Y
すべての loadshedding コマンド	N	Y
history length <n>	Y	Y
network mode <mode>	Y	Y

CLI コマンド	PX-1000	PX-2000
outlet <n> cyclingPowerOffPeriod <timing>	N	Y
outlet <n> name "<name>"	Y	Y
outlet <n> stateOnDeviceStartup <option>	N	Y
pdu cyclingPowerOffPeriod <timing>	Y	Y
pdu dataRetrieval <option>	Y	Y
pdu deviceAltitude <altitude>	Y	Y
pdu displayOrientation <orientation>	Y (1)	Y (1)
pdu externalSensorsZCoordinateFormat <option>	Y	Y
pdu inrushGuardDelay <timing>	N	Y
pdu measurementsPerLogEntry <number>	Y	Y
pdu name "<name>"	Y	Y
pdu nonCriticalOutlets <outlets1>:false;<outlets2>:true	N	Y
pdu outletInitializationDelayOnDeviceStartup <timing>	N	Y
pdu outletSequence <option>	N	Y
pdu outletSequenceDelay <outlet1>:<delay1>;<outlet2>:<delay2>;<outlet3>:<delay3>;...	N	Y
pdu outletStateOnDeviceStartup <option>	N	Y

注:

1. pdu displayOrientation <orientation> コマンドは、ゼロ U モデルにのみ適用されます。

その他のコマンド

次の表は、show コマンドおよび設定コマンド以外の CLI コマンドの適用可能性を示しています。

- Y: 適用可能
- N: 適用不可

CLI コマンド	PX-1000	PX-2000
すべての power outlets コマンド	N	Y

CLI コマンド	PX-1000	PX-2000
すべての reset pdu コマンド	Y	Y
nslookup <host>	Y	Y
netstat <option>	Y	Y
ping <host>	Y	Y
tracert <host>	Y	Y

Web インタフェースでのデータの切り捨て

Dominion PX Web インタフェースの一部のフィールドでは、最大 256 文字のデータを入力できます。以下の要因の一部または全部によって、入力されたデータが長くなりすぎた場合、データが切り捨てられる可能性があります。

- 画面解像度
- フォント サイズ
- フォント タイプ
- さまざまな文字のサイズ

現在の Web ブラウザ テクノロジでは、フィールド内のデータが長くなっても改行したり折り返したりすることができません。

この問題には、次のような解決法があります。

- 画面解像度を上げる
- フォントのサイズを小さくする
- CLI や SNMP などの他のインタフェースを使用してこれらのフィールドのデータを表示する

索引

[

[Add Page (ページの追加)] アイコン - 76, 80
[Environmental Sensors (環境センサー)] - 224
[logout (ログアウト)] ボタン - 80
[Setup (設定)] ボタン - 78
[User Management (ユーザ管理)] - 113

「

「above upper critical (上位臨界以上)」状態 - 233
「above upper warning (上位警告以上)」状態 - 233
「alarmed (アラーム)」状態 - 233
「below lower critical (下位臨界未満)」状態 - 233
「below lower warning (下位警告未満)」状態 - 233
「normal (正常)」状態 - 232
「使用不可能」状態 - 232

『

『Dominion PX ユーザ ガイド』における最新情報 - xvi

1

1 つのアウトレット (コンセント) の切り替え - 156
1U モデルでのヒューズの交換 - 66
1U モデルまたは 2U モデルの装着 - 15
1U 製品 - 4

2

2 桁表示パネル - 60
2U 製品 - 4

3

3 桁表示パネル - 59

A

AD 設定に関する詳細情報 - 150
AMS-M2-Z デイジーチェーンの制限 - 50, 51

AMS-M2-Z 資産センサーの接続 (オプション)
- xvi, 50

B

BSSID の設定 - 317
BTU 計算のデータ - 468

C

CA の署名済み証明書のインストール - 142
CLI コマンドの使用 - 430, 444
CLI コマンドの適用可能性 - 468
CLI のログアウト - 436
CLI へのログイン - 275

D

DHCP によって割り当てられた NTP サーバ
の上書き - 336
DNS サーバの照会 - 431
DNS サーバの役割 - 97, 448
Dominion KX II 設定 - xvi, 107, 457
Dominion PX Explorer ペイン - 75
Dominion PX MIB - 270
Dominion PX デバイスとネットワークの設定
- 297
Dominion PX デバイスの再起動 - 113
Dominion PX のリセット - 430
Dominion PX の設定 - 21, 93
Dominion PX の設定のコピー - 242
Dominion PX の追加情報 - xvi, 464
Dominion PX ファームウェアの更新 - 34,
261
Dominion PX への資産センサーの接続 - 45,
50, 236, 239
Dominion PX 設定の保存 - 241
DPX-CC2-TR へのサードパーティ製検出装置
/スイッチの接続 - 39

E

EAP CA 証明書の入力 - 315
EAP ID の設定 - 314
EAP パスワードの設定 - 314
EAP パラメータの設定 - 313
EnergyWise ドメインの指定 - 411

EnergyWise のシークレットの指定 - 411
 EnergyWise の設定 - 112
 EnergyWise の有効化または無効化 - 410
 EnergyWise 設定 - 291
 EnergyWise 設定コマンド - 410

G

GSM モデムの接続 (オプション) - 52

H

HTTP ポートの変更 - 326
 HTTP(S) 設定の変更 - 98
 HTTPS アクセス - 344
 HTTPS ポートの変更 - 327
 HTTPS 暗号化を強制的に使用 - 98, 123, 139

I

IP プロトコルの設定 - 309
 IP 設定 - 279
 IPv4 DHCP によって割り当てられた DNS サーバの上書き - 321
 IPv4 アドレスの設定 - 318
 IPv4 アドレスまたは IPv6 アドレスの選択 - 310
 IPv4 ゲートウェイの設定 - 319
 IPv4 サブネット マスクの設定 - 319
 IPv4 セカンダリ DNS サーバの設定 - 320
 IPv4 パラメータの設定 - 317
 IPv4 プライマリ DNS サーバの設定 - 320
 IPv4 または IPv6 の有効化 - 310
 IPv4 設定の変更 - 95
 IPv4 設定モードの設定 - 317
 IPv6 DHCP によって割り当てられた DNS サーバの上書き - 323, 324
 IPv6 アドレスの設定 - 322
 IPv6 ゲートウェイの設定 - 322
 IPv6 セカンダリ DNS サーバの設定 - 324
 IPv6 パラメータの設定 - 321
 IPv6 プライマリ DNS サーバの設定 - 323
 IPv6 設定の変更 - 96
 IPv6 設定モードの設定 - 321

K

KX II および LX でのアウトレット (コンセント) とターゲット サーバの関連付け - 461

KX II または LX でのラック PDU の名前付け (電源タップの [Port (ポート)] ページ) - 459

L

LAN インタフェース パラメータの設定 - 325
 LAN インタフェース設定 - 279
 LAN インタフェース速度の変更 - 325
 LAN デュプレックス モードの変更 - 326
 LDAP アクセス順序の並べ替え - 150
 LDAP サーバ接続のテスト - 150
 LDAP サーバ設定の削除 - 151
 LDAP サーバ設定の追加 - 147
 LDAP サーバ設定の編集 - 151
 LDAP とローカル認証サービスの有効化 - 152
 LDAP 情報の収集 - 146
 LDAP 設定の例 - 150, 446
 LDAP 認証の設定 - 97, 123, 146, 450
 LDAP 認証の無効化 - 152
 LED 動作モードの設定 - 418
 LED 表示 - 58
 LED 表示の向きの変更 - 59, 308
 LHX デバイスの監視 - 254, 257, 259
 LHX デバイスの制御 - 254, 260
 LHX デバイスの正しい表示 - 255
 LHX デバイスの設定 - 254, 255
 LHX デバイスの名前付け - 256
 LHX のサポートの有効化 - 254
 Logicool Web カメラの接続 (オプション) - 52, 76, 244, 246
 L-ブラケットとボタンを使用したゼロ U モデルの装着 - 14
 L-ブラケットを使用したゼロ U モデルの装着 - 7

M

MAC アドレス - 21, 464
 Modbus の有効化または無効化 - 333
 Modbus ポートの変更 - 334
 Modbus 設定の変更 - xvi, 102, 332

N

NTP パラメータの設定 - 335

P

PDU のラックマウント - 5
 PDU の再起動 - 430
 PDU の使用 - 54
 PDU の名前付け - 76, 77, 78, 90, 109, 155, 157, 158, 161, 163, 164, 166, 168, 170, 171, 173, 175, 176, 225, 227, 228, 230, 234, 258
 PDU レベルのイベント ルールのサンプル - 210
 PDU 情報の表示 - 35, 89, 154
 PDU 設定 - 281
 PDU 設定コマンド - xvi, 298
 PDU 定義のデフォルト状態の設定 - 158, 160
 PDU 定義の電源再投入時の電源オフ時間の設定 - 302, 361
 PDU 定義の電源再投入時の電源オフ時間の変更 - 160, 162
 PDU 名の変更 - 298
 ping 監視設定の削除 - 222
 ping 監視設定の編集 - 222
 ping 監視対象の IT デバイスの追加 - 221
 Power IQ の管理への PDU の追加 - 455
 Power IQ の設定 - 455
 PSK の設定 - 312
 PX-1000 シリーズ - 55
 PX-2000 シリーズ - 55

R

RF Code エネルギー監視ソリューション - 463

S

Schroff LHX ヒート エクスチェンジャの管理 - xvi, 53, 107, 254
 Schroff LHX ヒート エクスチェンジャの接続 (オプション) - xvi, 53, 107, 254
 SecureLock™ アウトレット (コンセント) およびコード - 465
 Show コマンド - 468
 SMTP の設定 - 111, 181, 182
 SNMP MIB のダウンロード - 101, 268, 270
 SNMP v1/v2c の有効化または無効化 - 329
 SNMP v3 の有効化または無効化 - 330
 SNMP トラップの設定 - 269
 SNMP の GET と SET - 270

SNMP の SET としきい値 - 273
 SNMP の使用 - 262, 267
 SNMP の書き込みコミュニティの設定 - 331
 SNMP の設定 - 100, 115, 329
 SNMP の読み取りコミュニティの設定 - 330
 SNMP の有効化 - 110, 267
 SNMPv3 設定の変更 - 398
 SSH の有効化または無効化 - 328
 SSH ポートの変更 - 329
 SSH または Telnet の使用 - 276
 SSH 設定の変更 - 98, 116, 328
 SSID の設定 - 311
 SSL 証明書の設定 - 123, 139
 sysContact 値の設定 - 331
 sysLocation 値の設定 - 332
 sysName 値の設定 - 332

T

TCP 接続の一覧表示 - 252
 Telnet の有効化または無効化 - 327
 Telnet ポートの変更 - 328
 Telnet 設定の変更 - 99, 327

U

UDP ポートの変更 - 412
 USB による PDU のカスケード接続 - 33, 57, 89
 USB-to-Serial ドライバのインストール - xvi, 23, 271

W

Web インタフェースでのデータの切り捨て - xvi, 472
 Web インタフェースの概要 - 73
 Web インタフェースの使用 - 26, 69
 Web インタフェースへのログイン - 70
 Web カメラの画像またはビデオの管理 - xvi, 244
 Web カメラの画像またはビデオの表示 - 52, 246, 249
 Web カメラの設定 - 244, 245

X

X 座標の設定 - 365

Y

Y 座標の設定 - 365

Z

Z 座標の設定 - 307, 366

Z 座標形式の設定 - 228

あ

アイドル タイムアウト - 347

アウトレット (コンセント) - 54

アウトレット (コンセント) とコードのロック
- 37, 464

アウトレット (コンセント) の PDU 定義の
デフォルト状態の設定 - 301, 360

アウトレット (コンセント) のデフォルト状態
の変更 - 360

アウトレット (コンセント) のマーク付け -
167

アウトレット (コンセント) の情報 - 281

アウトレット (コンセント) の電源オフ - 427

アウトレット (コンセント) の電源オン - 425

アウトレット (コンセント) の電源オンのシー
ケンス遅延の設定 - 300

アウトレット (コンセント) の電源オン順序の
設定 - 164, 299

アウトレット (コンセント) の電源の再投入 -
428

アウトレット (コンセント) の電源再投入時の
電源オフ時間の設定 - 361

アウトレット (コンセント) の名前付け - 153

アウトレット (コンセント) へのケーブル リ
テンション クリップの取り付け (任意) - 36

アウトレット (コンセント) レベルのイベント
ルールのサンプル - 211

アウトレット (コンセント) 管理 - 153

アウトレット (コンセント) 固有のデフォルト
状態の設定 - 158, 159

アウトレット (コンセント) 固有の電源オン遅
延の設定 - 165

アウトレット (コンセント) 固有の電源再投入
時の電源オフ時間の変更 - 160, 161

アウトレット (コンセント) 初期化遅延の設定
- 303

アウトレット (コンセント) 切り替え - 155

アウトレット (コンセント) 設定コマンド -
359

アウトレット (コンセント) 名の変更 - 359

アクション グループの作成 - 185

アクションの作成 - 52, 180, 186, 189, 244

アクションの変更 - 101, 217

アクセス セキュリティ コントロール - 123

アサート タイムアウトとは - 174, 175, 177,
178, 228, 374, 382, 387, 393

アサート停止ヒステリシスとは - 173, 174,
175, 177, 218, 228, 257, 373, 380, 386, 392

アラート状態および LHX イベント ログ -
259

イベント エントリの消去 - 219

イベント ルールのコンポーネント - 179

イベント ルールのサンプル - 210

イベント ルールの作成 - 179

イベント ルールの設定 - xvi, 100, 111, 173,
179, 269

イベント ルールの変更 - 216

イベント ルールまたはアクションの削除 -
217

イベント ログिंगの管理 - 218

インターネット プロトコルの選択 - 94, 95,
96

インタフェースについて - 274

インレット センサーしきい値情報 - 285

インレット センサー用のコマンド - 367

インレット レベルのイベント ルールのサン
プル - 212

インレットとサーキット ブレーカの管理 -
169

インレットのアサート タイムアウトの設定 -
373

インレットのアサート停止ヒステリシスの設
定 - 372

インレットのしきい値の設定 - 173

インレットの下位警告しきい値の設定 - 371

インレットの下位臨界しきい値の設定 - 370

インレットの監視 - 171

インレットの極センサーしきい値情報 - 286

インレットの極センサー用のコマンド - 374

インレットの極のアサート タイムアウトの設
定 - 381

インレットの極のアサート停止ヒステリシス
の設定 - 379

インレットの極の下位警告しきい値の設定 - 378
 インレットの極の下位臨界しきい値の設定 - 377
 インレットの極の上位警告しきい値の設定 - 375
 インレットの極の上位臨界しきい値の設定 - 374
 インレットの上位警告しきい値の設定 - 369
 インレットの上位臨界しきい値の設定 - 368
 インレットの名前付け - 170
 インレットへのケーブル リテンション クリップの取り付け (任意) - 20
 インレット情報 - 282
 インレット設定コマンド - 361
 インレット名の変更 - 362
 エントリごとのデータ ロギング測定数の設定 - 305
 オンライン ヘルプの参照 - 265

か

かぎつめ足ブラケットを使用したゼロ U モデルの装着 - 11
 カスタムの電子メール メッセージの作成 - 186
 カレンダーの使用法 - 105
 キー ファイルと証明書ファイルのダウンロード - 145
 コマンド ライン インタフェースの使用 - 97, 229, 274, 444
 コマンドで利用できるパラメータの確認 - 278, 435
 コマンドの自動補完 - 435
 コマンド履歴 - 295
 コンセントのデフォルト状態の設定 - 158
 コンピュータへの Dominion PX の接続 - 22, 443, 444

さ

サーキット ブレーカ - 63
 サーキット ブレーカ センサーしきい値情報 - 287
 サーキット ブレーカ センサー用のコマンド - 382
 サーキット ブレーカのアサート タイムアウトの設定 - 387

サーキット ブレーカのアサート停止ヒステリシスの設定 - 386
 サーキット ブレーカのしきい値の一括設定 - xvi, 176
 サーキット ブレーカのしきい値の設定 - 175, 176
 サーキット ブレーカの下位警告しきい値の設定 - 385
 サーキット ブレーカの下位臨界しきい値の設定 - 384
 サーキット ブレーカの監視 - 172
 サーキット ブレーカの向きの制限 - 6, 7, 9, 11, 12, 14, 15
 サーキット ブレーカの上位警告しきい値の設定 - 383
 サーキット ブレーカの上位臨界しきい値の設定 - 382
 サーキット ブレーカの名前付け - 170
 サーキット ブレーカ情報 - 283
 サーキット ブレーカ設定コマンド - 362
 サーキット ブレーカ名の変更 - 362
 サーバ アクセシビリティの監視 - 221
 サーバ監視状態の確認 - 223
 サービス アドバタイズメントの有効化 - xvi, 103, 334
 サービス アドバタイズメントの有効化または無効化 - 334
 サポートされている Web ブラウザ - 70
 サポートされているワイヤレス LAN 設定 - 26
 さまざまな CLI モードとプロンプト - 276, 277, 297, 423, 425
 しきい値の有効化についての注意事項 - 273
 シリアル RS-232 ポートのピン配列 - 437
 シリアル ポートのボー レートの設定 - 421
 シリアル ポートの設定 - xvi, 108
 シリアル ポート設定 - 291
 シリアル ポート設定コマンド - xvi, 420
 シリアル接続の終了 - 277
 シングル ログイン制限 - 345
 ステータス バー - 78
 スナップショット ストレージ - 249
 スナップショットの保存 - 244, 246, 249
 スナップショット履歴の管理 - 250
 すべてのアウトレット (コンセント) のマーク付け - 166

すべての権限 - 406, 409
 セカンダリ NTP サーバの指定 - 336
 セキュリティ設定 - 289
 セキュリティ設定コマンド - xvi, 337
 ゼロ U モデルでのヒューズの交換 - 65
 ゼロ U 製品 - 4
 センサー RJ-12 ポートのピン配列 - 438
 センサー タイプの指定 - 364
 センサー データの表示 - 230
 センサーしきい値設定コマンド - 367
 センサーのアサート タイムアウトの設定 - 392
 センサーのアサート停止ヒステリシスの設定 - 391
 センサーの下位警告しきい値の設定 - 390
 センサーの下位臨界しきい値の設定 - 389
 センサーの上位警告しきい値の設定 - 388
 センサーの上位臨界しきい値の設定 - 387
 センサーの場所の記述 - 228, 229
 センサーの説明の変更 - 367
 センサーの測定精度 - 231
 センサー名の変更 - 363
 その他のコマンド - 471
 ソフトウェア パッケージの情報の取得 - 265

た

ダイアログ ボックスのサイズ変更 - 85
 タグが接続されていない場合の LED 色の設定 - 416, 418, 419
 タグが接続されている場合の LED 色の設定 - 416, 418, 419
 ダッシュボードの表示 - 87
 ツリーの縮小 - 77
 ツリーの展開 - 76, 153, 154, 155, 156, 157, 159, 161, 167, 169, 170, 171, 172, 173, 175, 176, 225, 227, 230, 234, 235, 237, 256, 258, 260
 データ ペイン - 81
 データ ロギングの設定 - 110, 305
 データ ロギングの有効化 - 110
 データ ロギングの有効化または無効化 - 305
 デバイスの高度の指定 - 109, 306
 デバイスの状態とアイコンの変化 - 255, 260, 261
 デバイス管理 - 88

デフォルト ポリシーの変更 - 124, 125, 134, 135
 デフォルト ログ メッセージ - 189
 トリガされないルールについての注意事項 - 218

な

ネットワーク インタフェース設定の変更 - 91
 ネットワーク サービス パラメータの設定 - 326
 ネットワーク サービス設定 - 280
 ネットワーク サービス設定の変更 - 97, 274, 276
 ネットワーク モード - 279
 ネットワーク モードの設定 - 309
 ネットワーク ルートの追跡 - 251
 ネットワークのトラブルシューティング - 250, 431
 ネットワークへの Dominion PX の接続 - 25, 91, 92
 ネットワーク診断 - 250
 ネットワーク接続のテスト - 433
 ネットワーク接続の表示 - 432
 ネットワーク設定 - 278
 ネットワーク設定コマンド - 308
 ネットワーク設定の変更 - 78, 91, 93, 448

は

ハイパーターミナルの使用 - 275, 429
 はじめに - 1
 パスワード エージング - 346
 パスワード エージングの有効化 - 133
 パスワード エージング間隔 - 346
 パスワードの最小長 - 349
 パスワードの最大長 - 349
 パスワードの変更 - 72
 パスワード変更の強制 - 397
 パスワード履歴の最大数 - 352
 パッケージの内容 - 3, 18
 パネルのコンポーネント - 54
 ハンドルタイプのサーキット ブレーカのリセット - 64
 ヒューズ - xvi, 65
 ファームウェアのアップグレード - 242, 261

ファームウェアのアップグレード時間についての注意事項 - 263
 ファームウェア更新履歴の表示 - 263
 ファイアウォール ルールの削除 - 343
 ファイアウォール ルールの追加 - 339
 ファイアウォール ルールの変更 - 341
 ファイアウォールのルールの管理 - 339
 ファイアウォールのルールの作成 - 124, 126
 ファイアウォールのルールの削除 - 130
 ファイアウォールのルールの並べ替え - 129
 ファイアウォールのルールの編集 - 129
 ファイアウォールの設定 - xvi, 124
 ファイアウォールの有効化 - 124
 ファイアウォール制御 - 337
 ファイアウォール制御パラメータの変更 - 338
 ブザー - 68
 プライマリ NTP サーバの指定 - 335
 ブラウザで定義されたショートカット メニュー - 86
 ブレード拡張ストリップの接続 - xvi, 47
 ブレード拡張ストリップの設定 - 294
 ブレード拡張ストリップの展開 - xvi, 238
 ペインの調整 - 78
 ヘルプ コマンド - 277
 ヘルプの使用 - 264
 ポーリング間隔の設定 - 412
 ホストへの ping - 251
 ボタン マウントを使用したゼロ U モデルの装着 - 9
 ボタンタイプのサーキット ブレーカのリセット - 63
 ボタンタイプのロック アウトレット (コンセント) - 467

ま

マルチコマンド構文 - 339, 345, 347, 348, 353, 395, 396, 398, 403, 422
 メニュー - 74

や

ユーザ ブロック - 347
 ユーザ ブロックの有効化 - 131
 ユーザ プロファイルの作成 - 70, 99, 114, 118, 119, 120, 243, 269, 394
 ユーザ プロファイルの削除 - 118, 404

ユーザ プロファイルの変更 - 72, 118, 120, 395
 ユーザ プロファイルの有効化または無効化 - 397
 ユーザ リスト表示の変更 - 119
 ユーザ ログイン制御の設定 - 130
 ユーザのパスワードの変更 - 395
 ユーザのブロック解除 - 131, 429
 ユーザの個人データの変更 - 396
 ユーザ設定コマンド - 393

ら

ラック PDU (電源タップ) ターゲットの設定 - 457
 ラック PDU の接続 - 458
 ラック マウント安全基準 - 5
 ラック ユニットの LED モードの設定 - 418, 420
 ラック ユニットの LED 色の設定 - 418, 419
 ラック ユニットのナンバリング オフセットの指定 - 415
 ラック ユニットのナンバリング モードの指定 - 414
 ラック ユニットの数の指定 - 413
 ラック ユニットの設定 - 417
 ラック ユニットの名前付け - 417
 リストの表示の変更 - 83, 119, 123, 250, 263
 リセット (RESET) ボタン - 62
 リセット (RESET) ボタンの使用 - 443
 ルートの追跡 - 434
 ルールの作成 - 205
 レイアウト - 272
 ローカル イベント ログの表示 - 218
 ログアウト - 72
 ログイン - 70
 ログイン制限 - 345
 ログイン制限の有効化 - 132

わ

ワイヤレス ネットワーク設定 - 92
 ワイヤレス パラメータの設定 - 311
 ワイヤレス設定 - 280

漢字

安全の指針 - iv, 19
 安全基準 - ii

- 暗号化された SNMP v3 のユーザの設定 - 101, 268
- 一括設定による設定のコピー - 240
- 温度およびファンのしきい値の設定 - 256
- 稼働時間 - 259
- 画像またはビデオのプロパティの調整 - 245
- 外部認証の設定 - 313
- 概要の表示 - 257, 260
- 拡張ポートの設定 - xvi, 107, 255
- 環境センサー レベルのイベント ルールのサンプル - 213
- 環境センサーしきい値情報 - 288
- 環境センサーの Z 座標形式の設定 - 307, 366
- 環境センサーの管理 - 224, 225
- 環境センサーの識別 - 224, 226
- 環境センサーの接続 (オプション) - 37, 224
- 環境センサーの設定 - 224, 227
- 環境センサーを管理対象から除外 - 226, 234
- 環境センサー情報 - 284
- 環境センサー設定コマンド - 363
- 環境センサー用のコマンド - 387
- 管理対象センサーの状態 - 231
- 関連するサーキット ブレーカの確認 - 154
- 既存のキーと証明書ファイルのインストール - 144
- 既存のユーザ プロファイル - 289
- 既存の役割 - 290
- 機能の有効化 - 134
- 強力なパスワード - 348
- 強力なパスワードの有効化 - 133
- 強力なパスワードの有効化または無効化 - 348
- 空気差圧センサーの接続方法 - 42
- 警告アイコン - 81
- 警告対象のセンサー - 88
- 工場出荷時設定へのリセット - 62, 430, 443
- 高度補正率 - 109, 306, 467
- 最高動作周囲温度 - 19, 437
- 仕様 - 5, 437
- 資産センサーの LED 色の設定 - 236
- 資産センサーのファームウェアの更新 - 264
- 資産センサーのラック ユニット設定 - 293
- 資産センサーの結合 - 43
- 資産センサーの向きの指定 - 415
- 資産センサーの設定 - 46, 235
- 資産センサーの名前付け - 413
- 資産センサー管理 - 413
- 資産センサー情報の表示 - 239
- 資産センサー設定 - 292
- 資産管理 - 234
- 資産管理コマンド - xvi, 412
- 資産管理センサーの接続 (オプション) - 42, 56, 107, 234
- 時刻の設定方法の決定 - 335
- 時刻設定コマンド - xvi, 334
- 自己署名された証明書の作成 - 142
- 自身のパスワードの変更 - 405
- 自動モード - 61
- 手順 A. ユーザ アカウントとグループの決定 - 446
- 手順 B. AD サーバでのユーザ グループの設定 - 447
- 手順 C. Dominion PX デバイスでの LDAP 認証の設定 - 448
- 手順 D. Dominion PX デバイスでのユーザ グループの設定 - 451
- 手動モード - 61
- 初期ネットワーク設定 - 26, 70, 78, 91, 92, 443, 445
- 初期化遅延の設定 - 162, 303
- 小文字の要件 - 349
- 証明書署名リクエスト - 140
- 証明書署名リクエストの作成 - 140
- 詳細の表示 - 258
- 詳細情報 - 81
- 情報の表示 - xvi, 278
- 信頼性エラー ログ - 295
- 信頼性データ - 294
- 診断コマンド - 431
- 診断モードの終了 - 434
- 診断モードへの移行 - 277, 431
- 診断情報のダウンロード - 253
- 数字の要件 - 350
- 製品およびコンポーネントのパッケージの開梱 - 18
- 製品の機能 - 1
- 製品モデル - 1
- 接続ポート - 55
- 接続中のユーザの表示 - 220
- 接点閉鎖センサーについて - 39

- 接点閉鎖センサーの LED - 41
- 接点閉鎖センサーの設定 - 40, 41, 232, 233
- 設置と設定 - 18
- 設置場所の準備 - 19
- 設置前の確認点 - 18
- 設定コマンド - 470
- 設定モードの終了 - 298, 423
- 設定モードへの移行 - 277, 297, 315, 395, 405
- 前のコマンドの取得 - 435
- 全面的な障害復旧 - 264
- 装置の設定ワークシート - 19, 439
- 装置の設定ワークシートの記入 - 19
- 測定単位の LED - 60, 61
- 測定単位の変更 - 109, 242, 403
- 測定値の黄色表示または赤色表示 - 82, 87, 88, 171, 172, 230, 258
- 対象モデル - xv
- 大文字の要件 - 350
- 通信ログの表示 - 79, 252
- 電源コード - 54
- 電源への PDU の接続 - 21
- 電源再投入時の電源オフ時間の変更 - 160
- 電源制御操作 - 425
- 電源測定精度 - 437
- 電子メール メッセージのプレースホルダ - 186, 187
- 電子メールまたはインスタント メッセージでのスナップショットまたはビデオの送信 - 244, 247
- 電力しきい値の設定 - 83, 173, 273
- 統合 - 455
- 特殊文字の要件 - 351
- 特定のラック ユニットの設定 - xvi, 237
- 読み取り専用モードの有効化または無効化 - 333
- 突入電流防止遅延の設定 - 163
- 突入電流防止遅延時間の設定 - 302
- 内部認証の設定 - 313
- 日付と時刻の設定 - 104, 284
- 認証方法の設定 - 312
- 背面の 2 つのボタンを使用したゼロ U モデルの装着 - 12
- 非臨界アウトレット (コンセント) と負荷遮断モードの設定 - 166, 304
- 非臨界アウトレット (コンセント) の指定 - 291, 304
- 負荷遮断の有効化または無効化 - 424
- 負荷遮断モードの有効化または無効化 - 168
- 負荷遮断設定 - 291
- 負荷遮断設定コマンド - 423
- 複数またはすべてのアウトレット (コンセント) の切り替え - 155
- 分岐回路の定格の確認 - 19
- 並べ替えの変更 - 84, 220, 223
- 無限ループに関する注意 - 214
- 役割の作成 - 117, 120, 405
- 役割の削除 - 122, 410
- 役割の設定 - 72, 110, 113, 117, 119
- 役割の変更 - 117, 118, 121, 402, 408
- 役割ベースのアクセス制御 - 352
- 役割ベースのアクセス制御パラメータの変更 - 352
- 役割ベースのアクセス制御ルールの管理 - 354
- 役割ベースのアクセス制御ルールの作成 - 134, 136
- 役割ベースのアクセス制御ルールの削除 - 139, 358
- 役割ベースのアクセス制御ルールの設定 - xvi, 134
- 役割ベースのアクセス制御ルールの追加 - 354
- 役割ベースのアクセス制御ルールの並べ替え - 138
- 役割ベースのアクセス制御ルールの変更 - 356
- 役割ベースのアクセス制御ルールの編集 - 137
- 役割リスト表示の変更 - 123
- 役割設定コマンド - 405
- 優先ホスト名の設定 - 318
- 有線ネットワーク設定 - 91
- 履歴バッファの長さ - 295
- 履歴バッファの長さの設定 - 421

索引

- 例 - 295, 298, 299, 300, 301, 302, 303, 304,
305, 306, 307, 308, 309, 310, 311, 312, 313,
314, 315, 317, 318, 319, 320, 321, 322, 323,
324, 325, 326, 327, 328, 329, 330, 331, 332,
333, 334, 335, 336, 337, 339, 341, 343, 344,
345, 346, 347, 348, 349, 350, 351, 352, 353,
355, 358, 359, 360, 361, 362, 363, 364, 365,
366, 367, 369, 370, 371, 372, 373, 374, 375,
377, 378, 379, 381, 382, 383, 384, 385, 386,
387, 388, 389, 390, 391, 392, 393, 394, 395,
396, 397, 398, 401, 402, 404, 405, 408, 409,
410, 411, 412, 413, 414, 415, 416, 417, 418,
419, 420, 421, 424, 426, 428, 429, 431, 432,
433, 434
- ヒステリシスが役立つ場合 - 178
- ヒステリシスを無効にする場合 - 178
- 例 1 - 214
- 例 1 - IP、サブネット マスク、ゲートウェイ
の各パラメータの組み合わせ - 422
- 例 1 - 基本的なセキュリティ情報 - 296
- 例 2 - 215
- 例 2 - 詳細なセキュリティ情報 - 296
- 例 2 - 上位臨界設定と上位警告設定の組み合
わせ - 422
- 例 3 - 215
- 例 3 - SSID パラメータと PSK パラメータ
の組み合わせ - 423
- 例 3 - 基本的な PDU 情報 - 296
- 例 4 - 詳細な PDU 情報 - 297
- 列の変更 - 84



▶ 米国/カナダ/ラテン アメリカ

月曜日～金曜日
午前 8 時～午後 8 時 (米国東海岸時間)
電話 :800-724-8090 または 732-764-8886
CommandCenter NOC に関するお問い合わせ :6 を押してから 1 を押してください。
CommandCenter Secure Gateway に関するお問い合わせ :6 を押してから 2 を押してください。
Fax :732-764-8887
CommandCenter NOC に関する電子メール :tech-ccnoc@raritan.com
その他のすべての製品に関する電子メール :tech@raritan.com

▶ 中国

北京

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-10-88091890

上海

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-21-5425-2499

広州

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-20-8755-5561

▶ インド

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+91-124-410-7881

▶ 日本

月曜日～金曜日
午前 9 時 30 分～午後 5 時 30 分
電話 : 03-5795-3170
電子メール :support.japan@raritan.com

▶ ヨーロッパ

ヨーロッパ

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 :+31-10-2844040
電子メール :tech.europe@raritan.com

英国

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT)
電話 :+44(0)20-7090-1390

フランス

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 :+33-1-47-56-20-39

ドイツ

月曜日～金曜日
午前 8 時 30 分～午後 5 時 30 分 (GMT+1 CET)
電話 :+49-20-17-47-98-0
電子メール :rg-support@raritan.com

▶ メルボルン (オーストラリア)

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+61-3-9866-6887

▶ 台湾

月曜日～金曜日
午前 9 時～午後 6 時 (標準時 : GMT -5、夏時間 : GMT -4)
電話 :+886-2-8919-1333
電子メール :support.apac@raritan.com