



Copyright © 2011 Raritan, Inc. CCA-0N-v5.1-J February 2011 255-80-5140-00-0N このドキュメントには著作権によって保護されている所有者情報が含まれています。無断で転載することは、禁じられており、このドキュメントのどの部分も Raritan, Inc. (Raritan 社) 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はできません。

© Copyright 2011 Raritan, Inc.、CommandCenter®、Dominion®、Paragon®、Raritan 社のロゴは 、Raritan, Inc. の商標または登録商標です。無断で転載することは、禁じられています。Java® は Sun Microsystems, Inc. の登録商標、Internet Explorer® は Microsoft Corporation の登録商標です。 また、Netscape® および Netscape Navigator® は Netscape Communication Corporation の登録商 標です。その他すべての商標または登録商標は、その所有会社に帰属します。

FCC 情報

この装置は FCC 規則のパート 15 による Class A デジタル装置の制限に準拠することが試験により証明されています。これらの制限は、商業上の設置における有害な干渉を防止するために設けられています。この装置は、無線周波数を生成、利用、放射する可能性があるので、指示に従った設置および使用をしないと、無線通信への干渉を招く恐れがあります。この装置を居住環境で操作すると、干渉を招く場合があります。

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(VCCI)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。

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、通常の運用条件以外での使用による製品の故障については 、Raritan 社は一切責任を負いかねます。



『CC-SG 管理者ガイド』中の新規機能

xvii

はじめに	1
	1
用語/略語	2
クライアントのブラウザ要件	4

CC-SG へのアクセス

CC-SG Admin Client を介したブラウザ ベースのアクセス	5
JRE 非互换性	6
シック クライアント アクセス	6
シック クライアントのインストール	7
シック クライアントの使用	8
CC-SG Admin Client	9

使用を始める際に

ライセンス設定 - はじめに - 新規顧客および既存の顧客	.12
ライセンス設定 - 基本的なライセンス情報	.13
使用可能なライセンス	.13
物理アプライアンスのホスト ID の検索およびデータベース内のノード数の確認	.15
ライセンス設定 - 新規顧客 - 物理アプライアンス	.16
ライセンス設定 - クラスタ - 新規顧客	.18
ライセンス設定 - ライセンス サーバを使用する仮想アプライアンス	.19
仮想アプライアンスのインストール要件	.19
インストール ファイルをダウンロードする	.20
Linux または Windows サーバにライセンス サーバ ソフトウェアをインストールす	3 20
ライセンスを取得する	.22
ライセンス ファイルをライセンス サーバにコピーする	.24
ライセンス サーバを起動する	.24
CommandCenter Secure Gateway を VMware ESX Server 4.0 にインストールする	.25
診断コンソールにログインし CC-SG IP アドレスを設定する	.26
CC-SG にログインする	.26
ライセンスをインストールしてチェックアウトする	.27
ライセンス サーバ通信	.27
ライセンス サーバ管理用のコマンド ライン ユーティリティ	.29
VMware ツールをインストールまたはアップグレードする	.31



仮想アプライアンスおよびストレージ サーバのバックアップとスナップショットを	設
定する	31
リモート ストレージ サーバを使用する仮想アプライアンス	31
ライセンス設定 - ライセンスのインストール前の限られた動作	32
ライセンス設定 - 既存の顧客	33
ライセンス設定 - 再ホスト	33
ライセンスの追加	34
IP アドレスの確認	34
CC-SG サーバ時間の設定	35
互換表の確認	36
アプリケーション バージョンの確認とアップグレード	36

ガイド付き設定を使用した CC-SG の設定

ガイド付き設定を使用する前に	38
ガイド付き設定の関連	39
カテゴリとエレメントの作成	39
デバイス設定	39
デバイスの検出と追加	40
グループの作成	41
デバイス グループおよびノード グループの追加	42
ユーザ管理	44
ユーザとユーザ グループの追加	44

関連、カテゴリ、エレメント

関連について	47
関連の用語	
関連 - カテゴリとエレメントの定義	
関連の作成方法	
カテゴリとエレメントの追加、編集、削除	
カテゴリの追加	
カテゴリの削除	
エレメントの追加	49
CSV ファイルのインポートによるカテゴリとエレメントの追加	50
カテゴリとエレメントの CSV ファイルの要件	50
カテゴリとエレメントの CSV ファイルの例	51
カテゴリとエレメントのインポート	51
カテゴリとエレメントのエクスポート	52

デバイス、デバイス グループ、ポート

デバイスの表示54	ł
[デバイス] タブ54	ł



47

53

デバイスとポートのアイコン	54
ポート並び替えオプション	55
[デバイス プロファイル] 画面	57
トポロジー表示	
[デバイス] タブの右クリック オプション	
デバイスの検索	
検索用ワイルドカード	
ワイルドカードの例	59
デバイスの検出	59
デバイスの追加	60
KVM またはシリアル デバイスの追加	61
電源タップ デバイスの追加	63
Dominion PX デバイスの追加	63
デバイスの編集	64
KX2 デバイス用の HTTP ポートおよび HTTPS ポートの変更	64
電源タップ デバイスまたは Dominion PX デバイスの編集	
デバイス プロファイルへの注意の追加	65
デバイス プロファイルへの場所と連絡先の追加	
デバイスの削除	
ポートの設定	
シリアル ポートの設定	
KVM ポートの設定	
ポートの設定により作成されるノード	
ポートの編集	
ポートの削除	
KX2 に接続されたブレード シャーシ デバイスの設定	
ブレード シャーシの概要	
ブレード シャーシ デバイスの追加	
ブレード シャーシ デバイスの編集	75
ブレード シャーシ デバイスの削除	76
別のポートへのブレード シャーシ デバイスの移動	76
ブレード サーバ ポートの標准 $KX2$ ポートへのリストア	70
デバイスの関連、提氏、お上び連絡先の一括コピー	77
アメーバの固定 物所 初なび 足縮九の 沿って	78
KX2 に接続する K //M スイッチの追加	79
KX2 に接続するアナログ KVM スイッチ デバイスのポートの設定	70
デバイス グループ マネージャ	
デバイス グループの概要	
デバイス ブループの沪加	
アハイへ アループの距離	
アハイへ アループの測除	00 88
$\gamma \gamma $	00
ジゾ ノ ノ 1 ルツ1 ノ 小「 下によるノ ハ1 ヘツ 2 加	00 7 و
アハイへの OSV ファイルの安住	07
デバイスの しい ファイルの四	ອາ ດາ
ノ ハイ へのイン ホート デバイフのエクフポート	ອ∠ ດາ
ノ ハイ ヘのエフ ヘルード	



v

vi

目次

デバイスのアップグレード	93
デバイス設定のバックアップ	94
デバイス設定のリストア	95
デバイス設定のリストア (KX、KSX、KX101、SX、IP-Reach)	95
ネットワーク設定以外のすべての設定データの KX2、KSX2、または KX2-101 デバ	イ
スへのリストア	96
デバイス設定またはユーザとユーザ グループのデータのみの KX2、KSX2、KX2-10	1
デバイスへのリストア	96
すべての設定データの KX2、KSX2、または KX2-101 デバイスへのリストア	97
デバイス バックアップ ファイルの保存、アップロード、削除	97
デバイス設定のコピー	99
デバイスの再起動	100
デバイスの ping	100
CC-SG のデバイス管理の一時停止	100
デバイスの管理の再開	101
スケジュールされたタスクを使用したデバイス管理の一時停止と再開	101
デバイス パワー マネージャ	102
デバイスの管理ページの起動	103
ユーザの切断	103
Paragon II システム デバイスへの専用アクセス	104
Paragon II システム コントローラ (P2-SC)	104
IP-Reach と UST-IP 管理	104

管理対象電源タップ

CC-SG 内の別のデバイスによって管理される電源タップの設定
KX、KX2、KX2-101、KSX2、P2SC に接続された電源タップの設定108
KX、KX2、KX2-101、KSX2、または P2SC デバイスに接続された電源タップ デバイ
スの追加108
KX、KX2、KX2-101、KSX2、または P2SC の電源タップの別のポートへの移動108
KX、KX2、KX2-101、KSX2、または P2SC デバイスに接続された電源タップの削除109
SX 3.0 および KSX に接続された電源タップの設定109
SX 3.0 デバイスまたは KSX デバイスに接続された電源タップの追加109
SX 3.0 デバイスまたは KSX デバイスに接続された電源タップの削除110
電源タップのデバイスまたはポートの関連の変更 (SX 3.0、KSX)
SX 3.1 に接続された電源タップの設定111
SX 3.1 デバイスに接続された電源タップの追加111
SX 3.1 の電源タップの別のポートへの移動112
SX 3.1 デバイスに接続された電源タップの削除112
電源タップのコンセントの設定113

ノード、ノード グループ、インタフェース

ノードとインタフェースの概要	
ノードについて	



105

ノードの名前......115 インタフェースについて......116 ノードの表示116 ノードとインタフェースのアイコン.....119 サービス アカウント......119 サービス アカウントの概要......119 サービス アカウントの追加、編集、削除.....120 サービス アカウントのパスワードの変更.....121 サービス アカウントをインタフェースに割り当て122 ノードの追加、編集、および削除......123 ポートの設定により作成されるノード124 ノードの編集......124 ノードの削除......124 ノード プロファイルへの場所と連絡先の追加......125 ノード プロファイルへの注意の追加......125 CC-SG での仮想インフラストラクチャの設定.....126 仮想インフラストラクチャの用語.....126 仮想ノードの概要......127 仮想ホストと仮想マシンを持つ制御システムの追加......127 仮想マシンを持つ仮想ホストの追加......130 制御システム、仮想ホスト、仮想マシンの編集......133 制御システムおよび仮想ホストの削除135 仮想マシン ノードの削除......135 仮想インフラストラクチャの削除.....135 vSphere 4 ユーザは新しいプラグインをインストールする必要がある136 仮想インフラストラクチャと CC-SG の同期.....137 仮想インフラストラクチャの同期......137 仮想ホスト ノードのリブートまたは強制リブート.....138 [Virtual Topology] (仮想トポロジー) 表示へのアクセス138 Access Client の Firefox ユーザは JNLP ファイルのダウンロードが必要......139 ノードへの ping の実行......139 インタフェースの追加、編集、削除.....140 インタフェースの追加......140 インタフェースの編集......151 インタフェースの削除......152 インタフェースをブックマークに設定.....152 ノードへのダイレクト ポート アクセスの設定......153 ノードの関連、場所、および連絡先の一括コピー154 チャットの使用......155 CSV ファイルのインポートによるノードの追加......156 ノードの CSV ファイルの要件.....157



目次

ノードの CSV ファイルの例	168
ノードのインポート	168
ノードのエクスポート	169
CSV ファイルのインポートを利用した IP アドレスの編集	169
ノード グループの追加、編集、削除	170
ノード グループの概要	170
ノード グループの追加	171
ノード グループの編集	174
ノード グループの削除	175

ユーザとユーザ グループ

[ユーザ] タブ	
デフォルトのユーザ グループ	
CC スーパーユーザ グループ	
システム管理者グループ	
CC ユーザ グループ	
ユーザ グループの追加、編集、削除	
ユーザ グループの追加	
ユーザ グループの編集	
ユーザ グループの削除	
ユーザあたりの KVM セッション数の制限	
ユーザ グループのアクセス監査の設定	
ユーザの追加、編集、削除	
ユーザの追加	
ユーザの編集	
ユーザの削除	
ユーザのグループへの割り当て	
ユーザをグループから削除	
CSV ファイルのインポートによるユーザの追加	
ユーザの CSV ファイルの要件	
ユーザの CSV ファイルの例	
ユーザのインポート	
ユーザのエクスポート	
ユーザ プロファイル	
パスワードの変更	
名前の変更	194
デフォルトの検索設定の変更	194
CC-SG デフォルト フォント サイズの変更	194
電子メール アドレスの変更	194
CC-SG スーパー ユーザのユーザ名の変更	



ポリシーの追加	. 198
ポリシーの編集	. 199
ポリシーの削除	.200
仮想メディアのサポート	.201
ユーザ グループへのポリシーの割り当て	.201

デバイスおよびノードのカスタム表示

リモート認証

認証と承認 (AA) の概要	210
認証の流れ	211
ユーザ アカウント	211
LDAP と AD の識別名	211
AD の識別名の指定	212
LDAP の識別名の指定	212
AD のユーザ名の指定	212
ベース DN の指定	212
認証および承認のモジュール指定	212
外部 AA サーバの順序の確立	213
AD および CC-SG の概要	213
CC-SG への AD モジュールの追加	213
AD の一般設定	214
AD の詳細設定	215
AD のグループ設定	217
AD の信頼設定	218
AD モジュールの編集	218
AD ユーザ グループのインポート	219
AD と CC-SG の同期	221
すべてのユーザ グループの AD との同期	
全 AD モジュールの同期	



ix

210

197

Х

目次

すべての AD モジュールの日次同期の有効化または無効化	
AD の日次同期の時刻の変更	
AD グループの名前の変更および移動	
LDAP と CC-SG について	
CC-SG への LDAP (Netscape) モジュールの追加	
LDAP の一般設定	
LDAP の詳細設定	
Sun One LDAP (iPlanet)の設定	
OpenLDAP (eDirectory)の設定	
IBM LDAP の設定	
TACACS+ と CC-SG について	
TACACS+ モジュールの追加	
TACACS+ の一般設定	
RADIUS と CC-SG について	230
RADIUS モジュールの追加	230
RADIUS の一般設定	230
RADIUS による 2 ファクタ認証	

レポート

レポートの使用		
レポート デー	タのソート	
レポートの列幅	の変更	
レポートの詳細	1の表示	
複数ページ レン	ポート間の移動	
レポートの印刷	[]	
ファイルへのレ	イポートの保存	
CC-SG からの	レポートのデータの消去	
レポート フィ	ルタの非表示または表示	



監査証跡レポート	234
エラー ログ レポート	235
アクセス レポート	236
可用性レポート	237
アクティブ ユーザ レポート	237
ロックアウト ユーザ レポート	238
全ユーザ データ レポート	238
ユーザ グループ データ レポート	239
デバイス資産レポート	239
デバイス グループ データ レポート	239
ポートの照会レポート	240
ノード資産レポート	241
アクティブ ノード レポート	
ノード作成レポート	
ノード グループ データ レポート	243
AD ユーザ グループ レポート	243
スケジュールされたレポート	244
デバイス ファームウェアのアップグレード レポート	245

システム メンテナンス

メンテナンス モード	246
予定タスクとメンテナンス モード	247
メンテナンス モードの起動	247
メンテナンス モードの終了	247
CC-SG のバックアップ	248
完全バックアップと標準バックアップの違いは何ですか。	250
バックアップ ファイルの保存および削除	250
バックアップ ファイルの保存	250
バックアップ ファイルの削除	251
CC-SG のリストア	251
CC-SG のリセット	253
CC-SG の再起動	255
CC-SG のアップグレード	
ブラウザ キャッシュのクリア	258
Java キャッシュのクリア	
クラスタのアップグレード	259
プライマリ ノードのアップグレード エラー	
CC-SG データベースのマイグレーション	
マイグレーションの要件	
CC-SG データベースのマイグレーション	



目次

CC-SG	のシャットダウン	262
CC-SG	のシャットダウン後の再起動	262
CC-SG	の電源切断	263
CC-SG	セッションの終了	263
С	C-SG のログアウト	263
С	C-SG の終了	264

高度な管理

今日のメッヤージの設定	265
ノードにアクセスするためのアプリケーションの設定	266
ノードにアクセスするためのアプリケーションについて	266
アプリケーション バージョンの確認とアップグレード	266
アップグレード後に古いバージョンのアプリケーションが聞く	268
アプリケーションの追加	268
アプリケーションの測除	268
/ / / / / ジョンの別示 AKC を使用するため前提条件	269
デフォルトのアプリケーションの設定	269
デフォルトのアプリケーションについて	269
デフォルト アプリケーションの割り当ての表示	
インタフェースまたはポートのタイプのデフォルト アプリケーションの設定	
デバイス ファームウェアの管理	
ファームウェアのアップロード	
ファームウェアの削除	
CC-SG ネットワークの設定	
ネットワーク設定について	
CC-SG LAN ポートについて	
IP フェイルオーバ モードとは	
IP 分離モードとは	
CC-SG で推奨される DHCP 設定	
ログ アクティビティの設定	
CC-SG の内部ログの消去	
CC-SG サーバ時間および時刻の設定	
接続モード: ダイレクトおよびプロキシ	
接続モードについて	
すべてのクライアント接続にダイレクト モードを設定	
すべてのクライアント接続にプロキシ モードを設定	
ダイレクト モードとプロキシ モードの組み合わせを設定	
デバイス設定	
AKC ダウンロード サーバ証明書の検証の有効化	
カスタム JRE 設定の定義	
SNMP の設定	
MIB ファイル	
CC-SG クラスタの設定	
CC-SG クラスタの要件	



CC-SG クラスタへのアクセス	
クラスタの作成	
クラスタの設定	
プライマリ ノードとセカンダリ ノードのステータスの切り替え	
クラスタの復元	
クラスタの削除	291
クラスタのアップグレード	291
クラスタ ライセンス	292
隣接システムの設定	
隣接システムとは	293
隣接システムの作成	293
隣接システムの編集	
隣接システムの更新	
隣接システムの削除	
セキュリティ マネージャ	
リモート認証	
AES 暗号化	
ブラウザ接続プロトコルの設定: HTTP または HTTPS/SSL	
CC-SG への SSH アクセスに使用するポート番号の設定	
ログイン設定	
休止タイマーの設定	
ポータル	
証明書	
アクセス制御リスト	
通知マネージャ	
外部 SMTP サーハの設定	
タ人ク マネージャ	
ダムノのダイノ	
建続したタイノの人7 ンユール	
タイクの电ナメール通知	
人生シュールされたレホート	د ا د
タイクの快楽わよい衣小	د ا د
ダスクのスケンユール	دا د
$1 / 1 \land 1 / - \Delta J \perp 1 0 / 9 / 9 / 9 / - 下の \land 1 / 2 \perp - h$	
入/ シュールしたシステの変更	
リハノのハノノエール友丈	310
カウタハノと頬成したタハノのハナシュール	319
$CC-SG \land O SSH Z Z Z Z$	310
SSH コマンドのヘルプの表示	320
SSH コマンドレパラメーター	321
コマンドのトント	323
- 、、 - ッピン シリアル対応デバイスへの SSH 接続の作成	
SSH を使用してシリアル アウト オブ バンド インタフィース経由で /	ードに接続 325
SSH 接続の数了	1 103女前に.020



シリアル管理ポート	
端末エミュレーション プログラム	
CC-SG シリアル ナンバーの検出	
Web サービス API	
CC-NOC	

診断コンソール

診断コンソールへのアクセス	
VGA/キーボード/マウス ポートからの診断コンソールへのアクセス	
SSH を介した診断コンソールへのアクセス332	
Status Console	
Status Console について333	
Status Console へのアクセス333	
Status Console 情報	
Administrator Console	
Administrator Console について340	
Administrator Console へのアクセス	
Administrator Console のナビゲート342	
診断コンソール設定の編集	
ネットワーク インタフェース設定の編集 (ネットワーク インタフェース)344	
IP アドレスの ping345	
Traceroute の使用347	
静的ルートの編集	
診断コンソールでのログ ファイルの表示350	
診断コンソールを使用した CC-SG の再起動354	
診断コンソールを使用した CC-SG のリブート	
診断コンソールからの CC-SG システムの電源オフ	
診断コンソールを使用した CC スーパー ユーザのパスワードのリセット	
CC-SG 工場出荷時設定へのリセット	
診断コンソールのパスワード設定	
診断コンソール アカウント設定	
リモート システム監視の設定	
履歴データ傾向分析レポートの表示	
RAID ステータスとディスク使用率の表示	
ディスクまたは RAID テストの実行367	
ディスク テストのスケジュール	
RAID ディスクの修復または再作成371	
診断コンソールでのトップ ディスプレイの表示	
NTP ステータスの表示	
システム スナップショットの取得375	
診断コンソールのビデオ解像度の変更	



Power IQ の統合

V1 および E1 の仕様

V1	モデル	386
	V1 一般什様	386
	V1 環境要件	386
E1	モデル	387
	E1 一般仕様	387
	E1 環境要件	387

CC-SG およびネットワーク設定

CC-SG ネットワークに必要なオープン ポート:要旨	
CC-SG 通信チャンネル	
CC-SG と Raritan デバイス	
CC-SG クラスタリング	
インフラストラクチャ サービスへのアクセス	
PC クライアントから CC SG	
PC クライアントとノード	
CC-SG と IPMI、iLO/RILOE、DRAC、RSA のクライアント	
CC-SG & SNMP	
CC-SG 内部ポート	
NAT 対応ファイアウォール経由の CC-SG アクセス	
ノードへの RDP アクセス	
ノードへの VNC アクセス	
ノードへの SSH アクセス	
リモート システム監視ポート	



377

386

ユーザ グループ権限

SNMP トラップ

CSV ファイルのインポート 411 インポートに関する監査証跡エントリ......413

CSV ファイルの問題のトラブルシューティング414 トラブルシューティング

診断ユーティリティ

CC-SG ディスク監視.......419

2 ファクタ認証

2	ファクタ認証のサポート環境	.422
2	ファクタ認証の設定条件	.422
2	ファクタ認証の既知の問題	. 423

FAQ

認証に関する FAQ.......426 セキュリティに関する FAQ.......427 アカウントに関する FAQ429 パフォーマンスに関する FAQ......429 承認に関する FAQ431 使い心地に関する FAQ......431 ライセンス設定に関する FAQ......433

ショートカット キー



422

424

434

408

415

417

『CC-SG 管理者ガイド』中の新規機能[#]

ユーザ情報	
ノード情報	
Location Information (ロケーション情報)	
連絡先情報	
サービス アカウント	
デバイス情報	
ポート情報	
関連	437
答理	437
日生	

診断コンソール起動メッセージ

索引

装置やマニュアルに対する強化および変更に応じて、CommandCenter Secure Gateway 管理者ガイドに対して、次のセクションが変更されて いるか、次の情報が追加されました。

- *ライセンスの追加* 『**34**p. 』
- スケジュールされたタスクを使用したデバイス管理の一時停止と再 開 『101p. 』
- IBM IMM モジュール接続の詳細 『147p. 』
- ユーザ グループへのポリシーの割り当て 『**201**p. 』
- クラスタのアップグレード 『**259**p. 』
- プライマリ ノードのアップグレード エラー 『**260**p. 』
- **CC-SG** データベースのマイグレーション **[260**p.]
- マイグレーションの要件 **『261**p. 』
- **CC-SG** データベースのマイグレーション 『261p. 』
- クラスタ ライセンス 『**292**p. 』
- *ライセンス設定に関する FAQ* 『433p. 』

このバージョンの CommandCenter Secure Gateway に適用される変更 についての詳細は、リリース ノートを参照してください。



441

Ch1 はじめに

『CommandCenter Secure Gateway (CC-SG) 管理者ガイド』は、 CC-SG を管理および維持する方法について説明します。

このマニュアルは、一般的に使用可能なすべての権限を持つ管理者を読 者として想定しています。

管理者以外のユーザは、Raritan の『**CommandCenter Secure Gateway** ユーザ ガイド』を参照してください。

この章の内容

必要条件	1
用語/略語	2
クライアントのブラウザ要件	4

必要条件

本書の手順に従って CC-SG を設定する前に	、CC-SG により管理され
る Raritan デバイスを設置するための包括的	な手順について、Raritan
の『CommandCenter Secure Gateway Dep	loyment Guide』を参照し
てください。	



用語/略語

このマニュアルで使用する用語と略語には、次のようなものがあります

Access Client – CC-SG により管理されるノードにアクセスする必要が ある標準アクセス ユーザ向けの HTML ベースのクライアントです。 Access Client では、管理機能は使用できません。

Admin Client - 標準アクセス ユーザと管理者向けの CC-SG 用 Java ベースのクライアントです。これは、管理を行うことができる唯一のクライアントです。

関連 - カテゴリ、カテゴリのエレメント、ポート/デバイス相互間の関係です。たとえば、「Location」カテゴリをデバイスに関連付ける場合は、関連を作成してから、CC-SG にデバイスとポートを追加します。

カテゴリ - 値またはエレメントのセットを含む変数です。たとえば、「 New York City」、「Philadelphia」、または「Data Center 1」などのエ レメントを含む Location がカテゴリです。CC-SG にデバイスやポー トを追加する場合は、この情報を追加対象に関連付けます。最初に関連 を正しく設定した方が、後からデバイスやポートを関連に追加するより も簡単です。カテゴリのその他の例に、「Windows」、「Unix」、また は「Linux」などのエレメントを含む「OS Type」があります。

CIM (コンピュータ インタフェース モジュール) - ターゲット サーバと Raritan デバイスの接続に使用されるハードウェアです。Dominion KX101 を除く各ターゲットは、CIM を必要とします。Dominion KX101 はターゲットの 1 つに直接取り付けられるので、CIM を必要としませ ん。ターゲット サーバは電源をオンにして、CIM に接続します。CIM を Raritan デバイスに接続してから、デバイスを追加して CC-SG のポ ートを設定します。そうしないと、空白の CIM 名が CC-SG ポート名 を上書きします。CIM に接続したら、サーバをリブートする必要があり ます。

デバイス グループ - ユーザがアクセスできるデバイスの定義されたグ ループです。ポリシーを作成してグループ内のデバイスへのアクセスを 制御する際に、デバイス グループは使用されます。

デバイス - CC-SG で管理する Dominion KX、Dominion KX II、 Dominion SX、Dominion KSX、IP-Reach、Paragon II System Controller 、USTIP 搭載 Paragon II UMT832 などの Raritan 製品です。これらの デバイスは、接続されているターゲット サーバとシステム、つまり「ノ ード」を制御します。Raritan のサポート Web サイトにある CC-SG の互換表を参照して、サポートされるデバイスのリストを確認してくだ さい。

エレメント - カテゴリの値です。たとえば、「New York City」エレメントは「Location」カテゴリに属し、「Windows」エレメントは「OS Type」カテゴリに属します。



ゴースト ポート - ゴースト ポートは、Paragon デバイスを管理する 際に、CIM またはターゲット サーバがシステムから削除されるか、(手 動またはうっかり) 電源がオフになる場合に生じます。Raritan の『 Paragon II ユーザ マニュアル』を参照してください。

ホスト名 - DNS サーバのサポートが有効である場合に使用できます。 「*ネットワーク設定について* **[271**p. **]**」を参照してください。

ホスト名とその完全修飾ドメイン名 (FQDN = ホスト名 + サフィック ス) は、257 文字以下にします。「.」(ピリオド) で区切られている限り 、いくつでもコンポーネントを含むことができます。

各コンポーネントは最大 63 文字で、最初の文字はアルファベットにす る必要があります。残りの文字には、英数字または「-」(ハイフンまたは マイナス記号)を使用できます。

コンポーネントの最後の文字には、「-」を使用できません。

システムに入力される文字の大文字や小文字は区別されますが、FQDN では使用時にこれを区別しません。

iLO/RILOE および iLO2/RILOE2 - CC-SG で管理可能な Hewlett Packard 社の Integrated Lights Out/Remote Insight Lights Out サーバで す。iLO/RILOE デバイスのターゲットの電源は、直接投入/切断、およ び再投入されます。iLO/RILOE デバイスは、CC-SG では検出できない ので、ノードとして手動で追加する必要があります。このマニュアルで は、「iLO/RILOE」という語には iLO/RILOE と iLO2/RILOE2 の両方が 含まれます。

インバンド アクセス - TCP/IP ネットワーク経由で、ネットワークのタ ーゲットを修正またはトラブルシューティングします。KVM デバイス およびシリアル デバイスは、インバンド アプリケーションである RemoteDesktop Viewer、SSH Client、RSA Client、VNC Viewer を使っ てアクセスできます。

IPMI (Intelligent Platform Management Interface) サーバ – CC-SG で 制御できるサーバです。IPMI は自動検出されますが、手動で追加する こともできます。

アウト オブ バンド アクセス - Raritan Remote Console (RRC)、 Raritan Console (RC)、Multi-Platform Client (MPC)、仮想 KVM クライ アント (VKC)、Active KVM Client (AKC) などのアプリケーションを使 って、ネットワーク上の KVM や管理対象シリアル ノードを修正また はトラブルシューティングします。

ポリシー - CC-SG ネットワーク内のユーザ グループのアクセス権を定 義します。ポリシーはユーザ グループに適用され、アクセスの日と時 刻など、制御レベルを決定するいくつかの制御パラメータが含まれてい ます。

ノード - サーバ、デスクトップ PC、他のネットワーク機器など、 CC-SG ユーザがアクセスできるターゲット システムです。



インタフェース - Dominion KX2 接続などのアウト オブ バンド ソリ ューションを通じてか、VNC サーバなどのインバンド ソリューション を通じてノードにアクセスするためのさまざまな手段です。

ノード グループ - ユーザがアクセスできるノードの定義されたグルー プです。ノード グループは、ポリシーを作成してグループ内のノード へのアクセスを制御する際に使用されます。

ポート - Raritan デバイスとノード間の接続ポイントてす。ポートは Raritan デバイスにのみ存在し、そのデバイスからノードへの経路を特 定します。

SASL (Simple Authentication and Security Layer) - 認証サポートを接続 ベースのプロトコルに追加する方法です。

SSH - PuTTY や OpenSSH などのクライアントは CC-SG にコマンド ライン インタフェースを提供します。CC-SG コマンドのサブセットの みが SSH から提供され、デバイスと CC-SG 自体を管理します。

ユーザ グループ - 同じレベルのアクセスと権限を共有するユーザのグ ループです。

クライアントのブラウザ要件

サポートされるブラウザの全リストについては、Raritan のサポート Web サイトで互換表を参照してください。



Ch 2 CC-SG へのアクセス

CC-SG には、次のいくつかの方法でアクセスできます。

- ブラウザ: CC-SG は、数多くの Web ブラウザをサポートします(サポートされるブラウザの全リストについては、Raritan のサポー ト Web サイトで互換表を参照してください)。
- シック クライアント: ご使用のクライアント コンピュータに Java Web Start シック クライアントをインストールできます。シック クライアントはブラウザベースのクライアントと同様に機能します。
- SSH: シリアル ポートに接続されたリモート デバイスには SSH を使用してアクセスできます。
- 診断コンソール:緊急の修復や診断のみを行います。CC-SG の設定 と操作を行うブラウザベースの GUI に代わるものではありません。 「診断コンソール 『332p. 』」を参照してください。

注: 複数のユーザが CC-SG にアクセスしながらブラウザ、シック ク ライアント、および SSH を使用して同時に接続できます。

この章の内容

CC-SG Admin Client	を介したブラウザ ベースのアクセス5
シック クライアント	アクセス6
CC-SG Admin Client.	9

CC-SG Admin Client を介したブラウザ ベースのアクセス

CC-SG Admin Client は、ユーザの許可に応じて管理タスクとアクセス タスクの両方に **GUI** を提供する、Java ベースのクライアントです。

 サポートされているインターネット ブラウザを使用して、CC-SG の URL に続けて「/admin」を入力し、http(s)://IP アドレス/admin(たとえば http://10.0.3.30/admin 『https://10.0.3.30/admin参照』 または https://10.0.3.30/admin) を入力します。

[JRE Incompatibility Warning] (JRE 非互換性警告) ウィンドウが表 示された場合、クライアント コンピュータに適した JRE バージョ ンを選択し、インストールします。JRE がインストールされたら、 この手順をもう一度試行してください。「JRE 非互換性 『6p. 』」 を参照してください。

あるいは新しい JRE バージョンをインストールしないで続行する ことができます。



- 2. 制限付きサービス同意書が表示されたら、その内容を読み、[制限付 きサービス同意書を理解の上、同意します] チェックボックスを選 択します。
- [ユーザ名] と [パスワード] を入力し、[ログイン] をクリックします。
- 4. ログインが成功すると、CC-SG Admin Client が開きます。

JRE 非互換性

必要最小限のバージョンの JRE がクライアント コンピュータにインス トールされていない場合に、CC-SG Admin クライアントへのアクセス を試みると、警告メッセージが表示されます。CC-SG がクライアント コンピュータに必要な JRE ファイルを見つけられないと、[JRE Incompatibility Warning] (JRE 非互換性警告) ウィンドウが開きます。

[JRE Incompatibility Warning] (JRE 非互換性警告) ウィンドウが表示された場合、クライアント コンピュータに適した JRE バージョンを選択 してインストールするか、新しい JRE バージョンをインストールしな いで続行することができます。

JRE がインストールされたら、CC-SG をもう一度起動する必要があり ます。

管理者は、推奨される最小限度の JRE バージョンおよび [JRE Incompatibility Warning] (JRE 非互換性警告) ウィンドウに表示される メッセージを設定できます。「カスタム JRE 設定の定義 『284p. 』」 を参照してください。

シック クライアント アクセス

CC-SG シック クライアントを使用すると、Web ブラウザを介してア プレットを実行する代わりに Java Web Start アプリケーションを起動 して CC-SG に接続できます。シック クライアントの方がブラウザよ り高速である可能性があります。 シック クライアントの実行には、バ ージョン 1.6.0.10 以上の Java が必要です。



シック クライアントのインストール

CC-SG からシック クライアントをダウンロードするには、以下の 手順に従います。

注: JRE バージョン 1.6.0_20 を使用している場合は、Java コントロー ル パネルで [インターネットー時ファイル] タブの [コンピュータにー 時ファイルを保持します] チェックボックスがオンになっていることを 確認してください。このように設定していない場合は、シック クライ アントが起動できず、"Unable to launch application(アプリケーションを 起動できません)" というメッセージが表示されます。

- Web ブラウザを起動して、URL「 http(s)://<IP_address>/install」と入力します。
 <IP_address> は、CC-SG の IP アドレスです。
 - セキュリティ警告メッセージが表示されたら、[開始] をクリッ クしてダウンロードを続行します。
- 2. ダウンロードが完了したら、CC-SG の IP アドレスを指定できる 新しいウィンドウが開きます。
- [接続先 IP] フィールドにアクセスする CC-SG ユニットの IP アドレスを入力します。接続後、このアドレスは [接続先 IP] ドロップダウン リストから使用できるようになります。IP アドレスは、ご使用のデスクトップに保存されているプロパティ ファイルに格納されます。
- CC-SG がセキュアなブラウザ接続に設定されている場合は、[セキ ュア ソケット レイヤ (SSL)] チェックボックスをオンにする必要 があります。CC-SG がセキュアなブラウザ接続用に設定されてい ない場合は、[セキュア ソケット レイヤ (SSL)] チェックボックス を選択解除する必要があります。この設定は正しくなければなりま せん。正しくない場合、シック クライアントは CC-SG に接続で きません。
 - CC-SG の設定を確認するには、以下の手順に従います。[管理] >[セキュリティ] を選択します。[暗号化] タブで、[ブラウザ接 続プロトコル] オプションを参照します。[HTTPS/SSL] オプシ ョンが選択されている場合は、シック クライアントの IP アド レス指定ウィンドウの [セキュア ソケット レイヤ (SSL)] チェ ックボックスをオンにする必要があります。[HTTP] オプション が選択されている場合は、[シック クライアントの IP アドレス 指定] ウィンドウの [セキュア ソケット レイヤ (SSL)] チェッ クボックスを選択解除します。
- 5. [開始] をクリックします。



- マシン上のサポートされていない Java Runtime Environment バ ージョンを使用すると、警告メッセージが表示されます。プロ ンプトの表示に従って、サポートされている Java バージョン をダウンロードするか、現在インストールされているバージョ ンで続行します。
- 6. ログイン画面が表示されます。
- 7. 制限付きサービス同意書が有効になっている場合は、この同意書の テキストを読んでから、[制限付きサービス同意書を理解の上、同意 します] チェックボックスをオンにします。
- 8. ユーザ名とパスワードを対応するフィールドに入力し、[ログイン] をクリックして続行します。

シック クライアントの使用

シック クライアントの実行には、バージョン 1.6.0.10 以上の Java が 必要です。

シック クライアントがインストールされたら、ご使用のクライアント コンピュータで 2 通りの方法でこのシック クライアントにアクセスで きます。

- ▶ シック クライアントにアクセスするには、以下の手順に従います。
- Java コントロール パネルの Java Application Cache Viewer から シック クライアントを起動します。
- Java コントロール パネルの Java Application Cache Viewer を使用して、デスクトップにシック クライアント用のショートカット アイコンをインストールします。



CC-SG Admin Client

🕮 Raritan。 Comm	andCenter [®] Secure Gateway	******
Secure Gateway Users Devices	Nodes Assogiations Reports Access Administration System Maintenance View Window	Help
🛍 😂 🚚 😫 🕹 🚲 👪	🍠 🖉 🚍 🖓 💭 🏖 🌺 🧶 💿 🗸 💿 🗸 🚱 Server time: 16:46 (GMT-05:00)
Nodes Users Devices	Message of the Day Welcome to CommandCenter Secure Gateway!	×
Grand AccessUSTIPLocal Grand AccessUSTIPLocal		
▼ Search For Node		Close

ログインが成功すると、CC-SG Admin Client が表示されます。



- [ノード] タブ:[ノード] タブをクリックすると、ツリー表示に既知の全ターゲット ノードが表示されます。ノード プロファイルを表示するにはノードをクリックします。インタフェースは親ノードの下に分類されています。+ と の記号をクリックすると、ツリーを広げたり折りたたんだりすることができます。インタフェースを右クリックして、[接続] を選択し、そのインタフェースに接続します。ノードはノード名 (アルファベット順)、またはノード ステータス (利用可能、使用中、利用不可)でソートできます。ツリー表示を右クリックし、[ノード並べ替えオプション]を選択し、[ノード名でソート] または [ノード ステータスでソート] を選択します。
- [ユーザ] タブ: [ユーザ] タブをクリックすると、ツリー表示に登録 済みのすべてのユーザとグループが表示されます。+ と - の記号を クリックすると、ツリーを広げたり折りたたんだりすることができ ます。
- [デバイス] タブ: [デバイス] タブをクリックすると、ツリー表示に 既知の全 Raritan デバイスが表示されます。デバイス タイプごと にアイコンが異なります。ポートは、親デバイスの下でグループ化 されています。+ と - の記号をクリックすると、ツリーを広げたり 折りたたんだりすることができます。ポートをクリックしてポート プロファイルを表示します。ポートを右クリックして、[接続] を選 択し、そのポートに接続します。ポートは、ポート名 (アルファベ ット順)、ポート ステータス (利用可能、使用中、利用不可)、また はポート番号 (番号順)を基準にして並べ替えることができます。 ツリー表示を右クリックし、[ポート並び替えオプション] を選択し 、[ノード名でソート] または [ノード ステータスでソート] を選択 します。
- クィック コマンド ツールバー: このツールバーは、よく使うコマンドを実行するためのショートカット ボタンの役割を果たします。
- 操作および設定メニュー バー: このメニューには、CC-SG の操作 および設定のためのコマンドが含まれています。このようなコマン ドの一部は、[ノード]、[ユーザ]、および [デバイス] の各選択タブ でアイコンを右クリックしてアクセスすることもできます。表示さ れるメニューおよびメニュー項目は、ユーザ アクセス権限によりま す。
- サーバ時間:設定マネージャで CC-SG に設定された現在の時刻と タイム ゾーン。この時間は、タスク マネージャでタスクをスケジ ュールするときに使用されます。「タスク マネージャ 『311p. 』」 を参照してください。この時間はクライアント PC で使用されてい る時間と異なる場合があります。



Ch3 使用を始める際に

CC-SG で設定および作業を開始するには、有効なライセンスがインス トールされている必要があります。次に、最初のログイン時に、IP ア ドレスを確認し、CC-SG サーバ時間を設定し、インストールされてい るファームウェアおよびアプリケーションのバージョンをチェックしま す。ファームウェアとアプリケーションのアップグレードが必要になる 場合があります。

初期設定を完了したら、ガイド付き設定に進みます。「ガイド付き設定 を使用した CC-SG の設定 『38p. 』」を参照してください。

この章の内容

ライセンス設定 - はじめに - 新規顧客および既存の顧客	.12
ライセンス設定 - 基本的なライセンス情報	.13
ライセンス設定 - 新規顧客 - 物理アプライアンス	.16
ライセンス設定 - ライセンス サーバを使用する仮想アプライアンス	.19
ライセンス設定 - ライセンスのインストール前の限られた動作	.32
ライセンス設定 - 既存の顧客	.33
ライセンス設定 - 再ホスト	.33
ライセンスの追加	.34
IP アドレスの確認	.34
CC-SG サーバ時間の設定	.35
互換表の確認	.36
アプリケーション バージョンの確認とアップグレード	.36



ライセンス設定 - はじめに - 新規顧客および既存の顧客

CC-SG 5.0 では、新しいライセンス設定技術が導入されています。 CC-SG 5.0 を使い始めるには、有効なライセンスがインストールされて いる必要があります。ライセンスがインストールされるまでは、CC-SG の限られた機能しか使用できません。「*ライセンス設定 - ライセンスの インストール前の限られた動作* **32**₀. **」** を参照してください。

ライセンスの設定を開始するには、以下の手順に従います。

物理アプライアンスを持つ CC-SG の新規顧客である場合は、「*ライセンス設定 - 新規顧客 - 物理アプライアンス* 『16p. 』」を参照してください。

仮想アプライアンスを持つ CC-SG の新規顧客である場合は、「*ライセンス設定 - 新規顧客 - ライセンス サーバを使用する仮想アプライアン* ス『19p. の"*ライセンス設定 - ライセンス サーバを使用する仮想アプ ライアンス*"参照 』」を参照してください。

CC-SG 5.0 にアップグレードする既存の顧客である場合は、「*ライセン* ス設定 - 既存の顧客 『33p. 』」を参照してください。



ライセンス設定 - 基本的なライセンス情報

ライセンスは、CC-SG で設定されたノード数に基づきます。

物理または仮想アプライアンスを購入すると、特定のノード数の使用ラ イセンスが付与されます。この "基本ライセンス" により、CC-SG 機能 が使用可能になり、指定された数までのノードのライセンスが付与され ます。それ以上のノードが必要な場合は、追加ノード用のアドオン ラ イセンスも購入します。WS-API 機能を使用する場合は、WS-API アク セス用のアドオン ライセンスも購入する必要があります。

物理アプライアンスのライセンス ファイルは、特定の CC-SG ユニットのホスト ID に関連付けられています。

仮想アプライアンスのライセンス ファイルは、特定のライセンス サー バのホスト ID に関連付けられています。

したがって、ライセンス ファイルを他のユニットやサーバで使用する ことはできません。

- 物理アプライアンスの新規顧客の場合は、Raritan ライセンス ページ Web サイトからライセンス ファイルをダウンロードします。「 ライセンス設定 - 新規顧客 - 物理アプライアンス 『16p. 』」を参照してください。
- 5.0 以前の既存の顧客である場合、ライセンス ファイルをダウンロードする必要はありません。5.0 以前の CC-SG ユニットを 5.0 以降にアップグレードすると、ライセンスは新しい形式に変換されます。新しい基本ライセンスおよび適切なアドオン ライセンスが作成され、現在の設定に適応するように必要に応じて自動的にインストールおよびチェックアウトが行われます。「ライセンス設定 既存の顧客 『33p.』」を参照してください。
- 仮想アプライアンスの顧客である場合は、ライセンス サーバを配備 する必要があります。「ライセンス設定 - ライセンス サーバを使用 する仮想アプライアンス 『19p. 』」を参照してください。

使用可能なライセンス

CC-SG 製品	説明	初めてライセンスを作成する場合に必要な情 報
CC-E1-128	CC-SG E1 アプライアンス、 128 ノード ライセンスが付与され ています	CC-SG ユニットのホスト ID
CC-E1-256	CC-SG E1 アプライアンス、 256 ノード ライセンスが付与され ています	CC-SG ユニットのホスト ID



Ch 3: 使用を始める際に

CC-SG 製品	説明	初めてライセンスを作成する場合に必要な情 報
CC-E1-512	CC-SG E1 アプライアンス、 512 ノード ライセンスが付与され ています	CC-SG ユニットのホスト ID
CC-V1-128	CC-SG V1 アプライアンス、 128 ノード ライセンスが付与され ています	CC-SG ユニットのホスト ID
CC-V1-256	CC-SG V1 アプライアンス、 256 ノード ライセンスが付与され ています	CC-SG ユニットのホスト ID
CCSG128-VA	CC-SG 仮想アプライアンス、 128 ノード ライセンスが付与され ています	 Windows または Linux のライセンス サーバのホスト ID Windows または Linux のライセンス サーバのホスト名または IP アドレス
CC-2XE1-512	クラスタ キット: 2 CC-SG E1 アプ ライアンス、512 ノード ライセン スが付与されています	クラスタ内の各 CC-SG ユニットのホスト ID
CC-2XE1-1024	クラスタ キット: 2 CC-SG E1 アプ ライアンス、1024 ノード ライセ ンスが付与されています	クラスタ内の各 CC-SG ユニットのホスト ID
CC-2XV1-256	クラスタ キット: 2 CC-SG V1 アプ ライアンス、256 ノード ライセン スが付与されています	クラスタ内の各 CC-SG ユニットのホスト ID
アドオン ライセンス	追加ノードおよび付加価値サービス (WS-API など) のライセンス。	CC-SG ユニットのホスト ID



物理アプライアンスのホスト ID の検索およびデータベース内のノード 数の確認

[ライセンス マネージャ] ページには、データベース内の現在ライセン スされているノード数を始めとする、ライセンスに関する情報が表示さ れます。物理アプライアンスのホスト ID は、[License Management(ラ イセンス管理)] ページから取得できます。Raritan ライセンス ポータル でライセンス ファイルを作成する場合は、<製品名> のホスト ID を入 力する必要があります。新しいライセンス ファイルの取得方法につい ての詳細は、「*ライセンス設定 - 新規顧客 - 物理アプライアンス*『16p. 』」を参照してください。

仮想アプライアンスを持っている場合は、ライセンス サーバのホスト ID の取得について、「*ライセンスを取得する* 『22p. 』」を参照してく ださい。

- ホスト ID を表示してデータベース内のノード数を確認するには、
 以下の手順に従います。
- 1. [管理] > [License Management(ライセンス管理)] を選択します。
- ログインしている <製品名> ユニットのホスト ID は、[License Management(ライセンス管理)] ページに表示されます。ホスト ID をコピーして貼り付けることができます。 仮想 CC-SG の場合、 ホスト ID は、ライセンス サーバをインストールした後、[License Summary(ライセンスの概要)] セクションに表示されます。[ライセ ンス マネージャ] ページは、物理アプライアンスと仮想アプライア ンスで少し異なります。
- このページでデータベース内のノード数を確認します。ライセンス 制限までさらに追加できるノード数を特定できます。

License Manager			
The License M CommandCen the CC-SG ap	anager allows you to add and re ter Secure Gateway. Ensure tha pliance, for Additional Nodes/Int	move licenses, check out and check in features requi t you have added and checked out the necessary bas erfaces, and services.	red for operation of se and add-on licenses for
-License Summarri	CC-SG Host ID: 7EC869EC-	2BB3-9395-F32C-5AB05986BB95	
NOT SERVED	CCSG-57-238,raritan.com	7EC869EC-2BB3-9395-F32C-5AB05986BB95	Operational
433 of 384 Licen	sed Nodes Currently in Database	3	



ライセンス設定 - 新規顧客 - 物理アプライアンス

CC-SG 5.0 物理アプライアンスを購入した新規顧客の場合は、次の手順 に従って、有効なライセンスをインストールして有効にします。

▶ 手順 1: ライセンスの取得:

 購入時に指定されたライセンス管理者は、送信元電子メール アドレスが licensing@raritan.com で、件名が "Thank You for Registering(ご登録ありがとうございます)" という Raritan Licensing Portal(Raritan ライセンス ポータル) からの電子メールを 受信します。

Reriton.				
Thank You for Registering				
7/15/2010 0035000000ZeXEa				
Customer Name Customer Address				
Dear Customer				
Raritan welcomes you to our firm as a new customer. We know that you will satisfied with our award winning products and services.				
Online account access is now available to register the software product(s) y purchased. Your registration will generate a license key to activate your soft provide you with access to a web portal where you can review the history of have purchased and their associated license keys.				
Please follow this link to confirm your company and contact information for t that will have access to license keys for your Raritan software. <u>http://www.raritan.com/CreateAccount?ContactID=0035000000ZeXEa</u> Your e-mail address will be used as your username to access the License k				
Should you have any questions or need assistance, please contact Raritan Service @ (800) 724-8090 prompt "5" then "1" or your Sales Representative.				
and a second				
 電子メール内のリンクをクリックして、Raritan ソフトウェア ライセンス キー ログイン ページ 				

- 電子メール内のリンクをクリックして、Raritan の Web サイトの ソフトウェア ライセンス キー ログイン ページに移動します。ユ ーザ アカウントおよびログインを作成します。ユーザ名は自分の電 子メール アドレスです。ライセンス アカウント情報ページが開き ます。間もなくライセンス ファイルが使用可能になります。
- 送信元電子メール アドレスが licensing@raritan.com で、件名が "Your Raritan Commandcenter SG Software License Key is Available(Raritan Commandcenter SG ソフトウェア ライセンス キ ーが使用可能です)" という Raritan Licensing Portal(Raritan ライセ ンス ポータル) からのもう 1 通の電子メールを確認してください



Ch 3: 使用を始める際に



- 電子メール内のリンクをクリックして、Raritan の Web サイトの ソフトウェア ライセンス キー ログイン ページに移動し、作成さ れたユーザ アカウントでログインします。
- [Product License(製品ライセンス)] タブをクリックします。購入したライセンスが一覧表示されます。ライセンスが1つしか表示されない場合や、複数表示される場合があります。「使用可能なライセンス『13p.』」を参照してください。
- 各ライセンスを取得するには、リスト内の項目の横にある [作成 (Create)] をクリックし、<製品名> のホスト ID を入力します。 [License Management(ライセンス管理)] ページからホスト ID をコ ピーして貼り付けることができます。 「ホスト ID の検索およびデ ータベース内のノード数の確認 『15p. の"物理アプライアンスのホ スト ID の検索およびデータベース内のノード数の確認"参照 』」を 参照してください。
- 7. [Create License(ライセンスの作成)]をクリックします。入力した詳細情報がポップアップに表示されます。ホスト ID が正しいことを 確認します。

- 8. [OK] をクリックします。ライセンス ファイルが作成されます。
- 9. [Download Now(今すぐダウンロード)] をクリックし、ライセンス ファイルを保存します。

▶ 手順 2: ライセンスのインストール:

- 1. [管理] > [License Management(ライセンス管理)] を選択します。
- 2. [Add License(ライセンスの追加)] をクリックします。



- 3. ライセンス契約を読み、テキスト領域の下までスクロールして、[I Agree(同意する)] チェックボックスをオンにします。
- 手順 3: 有効にするライセンスのチェックアウト: 機能を有効にするには、ライセンスをチェックアウトする必要があります。
- リストからライセンスを選択し、[Check Out(チェックアウト)] をク リックします。有効にするライセンスをすべてチェックアウトしま す。

ライセンス設定 - クラスタ - 新規顧客

クラスタ キット ライセンスを使用することで、2 つの CC-SG 物理ユ ニットが、ライセンスを共有するクラスタとして作動します。システム では、クラスタが作成されアクティブに動作し、プライマリ クラスタ ノードでライセンスがインストールされチェックアウトされるまでは、 動作が限定されます。クラスタ内の CC-SG ユニットは、各ユニットの 個別のメンテナンスを考慮して、一時的にスタンドアロン ユニットと して運用できます。ただし、2 つの CC-SG ユニットは、引き続きすべ てが機能するようにもう一度クラスタに追加する必要があります。クラ スタリングは、仮想アプライアンスではサポートされていません。

注: スタンドアロン猶予期間が満了すると、クラスタに追加されるまで CC-SG の動作は制限されます。「ライセンス設定 - ライセンスのイン ストール前の限られた動作 『32p. 』」を参照してください。

Raritan ライセンス ポータルでクラスタ ライセンス ファイルを作成す る場合は、各 CC-SG ユニットのホスト ID を入力する必要があります 。ホスト ID は、各 CC-SG ユニットの [管理] > [License Management(ライセンス管理)] ページで探してください。

クラスタ キット ライセンスで CC-SG クラスタを導入するには、 以下の手順に従います。

CC-SG クラスタについての詳細は、「**CC-SG** クラスタの設定 **『287**p. **』**」を参照してください。

- 1. クラスタ化する両方の CC-SG ユニットを配備します。配備につい ての詳細は、『CC-SG Quick Setup Guide(CC-SG クイック セット アップ ガイド)』を参照してください。
- 各 CC-SG ユニットのホスト ID を検索します。「ホスト ID の検 索およびデータベース内のノード数の確認 『15p. の"物理アプライ アンスのホスト ID の検索およびデータベース内のノード数の確認" 参照 』」を参照してください。
- 3. クラスタ キット ライセンス ファイルを取得します。「*ライセンス* 設定 - 新規顧客 - 物理アプライアンス 『16p. 』」を参照してくだ さい。


- 4. クラスタを作成します。「**クラスタの作成『288**p.**』**」を参照して ください。
- クラスタ内のプライマリ ノードにライセンス ファイルをインスト ールします。このファイルは、クラスタが作成されるとセカンダリ ノードにコピーされます。ライセンス ファイルのインストール方法 についての詳細は、「*ライセンス設定 - 新規顧客 - 物理アプライア* ンス『16p.』」を参照してください。
- 有効にするライセンスをチェックアウトします。必ずクラスタ キット ライセンスをチェックアウトしてください。「ライセンス設定 新規顧客 物理アプライアンス 『16p.』」を参照してください。

ライセンス設定 - ライセンス サーバを使用する仮想アプライアンス

CC-SG 仮想アプライアンスでは、ライセンスをホストするすべてのラ イセンス サーバをインストールする必要があります。Raritan では、ラ イセンス サーバ ソフトウェアおよびツール、ベンダ デーモンを提供 します。これを物理サーバにインストールします。「*仮想アプライアン スのインストール要件* 『**19**p. 』」を参照してください。

CC-SG 5.0 仮想アプライアンスを購入して間もない新規顧客の場合は、 次の手順に従って、ライセンス サーバをインストールし、有効なライ センスが有効になっていることを確認します。

仮想アプライアンスのインストール要件

- CommandCenter Secure Gateway 仮想アプライアンス版を配備する ESX 4.0
 - 空き領域 40GB 以上のデータストアが必要
 - 利用可能なメモリ 2GB が必要
 - 仮想 NIC 2 つ
 - 共有ストレージを持つ高可用クラスタを推奨
- vSphere Client 4.0 を実行するクライアント コンピュータ
- Flexera[™] FlexNet Publisher[®] ライセンス サーバおよびサポートされ ている OS をホストする Windows または Linux の物理サーバ

Flexera の Imgrd ユーティリティは以下でサポートされています。

- Windows Server 2008、Windows Server 2003、Windows XP Professional with SP3、Windows Vista (Ultimate)、Windows 7 (Ultimate) の Windows 32-bit (x86)
- Red Hat Enterprise Linux 4.0 および 5.0 上の Linux 32-bit Linux Standard Base (LSB) 3.0 認定 x86



以下のファイル

(http://www.raritan.com/support/commandcenter-secure-gateway から入手可能)。詳細は、「インストール ファイルをダウンロードする 『**20**p. 』」を参照してください。

- CommandCenter Secure Gateway 仮想アプライアンス版 .OVF ファイル
- Raritan ベンダ デーモン ファイル
- Flexera FlexNet Publisher ライセンス サーバ

インストール ファイルをダウンロードする

全インストール ファイルのセットは、

http://www.raritan.com/support/CommandCenter-Secure-Gateway/ から 入手できます。

このリンクでファイルにアクセスするには、Raritan ライセンス ポータ ルにログインする必要があります。「*ライセンスを取得する* **『22**p. **』** 」を参照してください。

サイズの問題で .OVF ファイルのダウンロードを希望しない顧客には、 .OVF ファイルを製品 DVD でお送りします。DVD には Flexera ファ イルまたはベンダ デーモン ファイルは含まれていないので、これらは Web サイトからダウンロードする必要があります。

インストール ファイルは 2 つの .ZIP ファイルに収められています。 ファイル名の <release number> の部分には、実際の CC-SG リリース 番号が入ります。

vccsg_rel_<release number>_ovf.ZIP ファイルには以下が含まれています。

• 仮想アプライアンス版の配備に使用される .OVF ファイル

flexserver-11.8-raritan.ZIP ファイルには以下が含まれています。

- Linux および Windows 用の Raritan ベンダ デーモン ファイル
- Linux および Windows 用 Flexera[™] FlexNet Publisher[®] ライセンス サーバ ツールキット

Linux または Windows サーバにライセンス サーバ ソフトウェアを インストールする

CommandCenter Secure Gateway 仮想アプライアンス版を使用するに は、Flexera[™] FlexNet Publisher[®] ライセンス サーバ ソフトウェアを物 理サーバにインストールしておく必要があります。サポートされている サーバについては、「要件」を参照してください。

Linux のサーバ

1. Linux のサーバにログインします。



- 2. システムに flex というユーザを追加します。
- 3. flex としてログインし、端末を開きます。
- ダウンロードした flexserverv11.8-linux.tar.gz ファイルを home/flex にコピーします。コンテンツを同じ場所に解凍します。
- 次のコマンドを入力します。 tar -xvzf flexserverv11.8.tar.gz ファイルのパッケージが解凍されます。以下のディレクトリが作成 されます。
 - flexserverv11.8
 - flexserverv11.8 の下に i86_lsb が作成されます。
- 6. 5-1-0-raritan-daemon/raritan-linux32-1.1.zip ファイルを home/flex に解凍します。
- 7. 次のコマンドを使用して、Raritan ベンダ デーモン ファイルを移 動します。

```
cp raritan /home/flex/flexserverv11.8/i86 lsb/
```

- 8. 次のコマンドを入力します。 chmod +x raritan
- redhat-lsb パッケージをインストールしていることを確認してくだ さい。これをインストールするには、root として yum install redhat-lsb を実行します。

Windows のサーバ

- flexserverv11.8-win.zip ファイルを Windows のサーバの C:\ に解 凍します。これによって、flexnet-win というフォルダが作成されま す。
- 2. raritan-win32-1.0.zip を C:\flexnet-win\i86_n3\ に解凍します。



ライセンスを取得する

 購入時に指定されたライセンス管理者は、送信元電子メール アドレ スが licensing@raritan.com で、件名が "Thank You for Registering(ご登録ありがとうございます)" という Raritan Licensing Portal(Raritan ライセンス ポータル) からの電子メールを 受信します。



- 電子メール内のリンクをクリックして、Raritan の Web サイトの ソフトウェア ライセンス キー ログイン ページに移動します。ユ ーザ アカウントおよびログインを作成します。ユーザ名は自分の電 子メール アドレスです。ライセンス アカウント情報ページが開き ます。間もなくライセンス ファイルが使用可能になります。
- 送信元電子メール アドレスが licensing@raritan.com で、件名が "Your Raritan Commandcenter SG Software License Key is Available(Raritan Commandcenter SG ソフトウェア ライセンス キ ーが使用可能です)" という Raritan Licensing Portal(Raritan ライセ ンス ポータル) からのもう 1 通の電子メールを確認してください



Ch 3: 使用を始める際に



- 電子メール内のリンクをクリックして、Raritan の Web サイトの ソフトウェア ライセンス キー ログイン ページに移動し、作成さ れたユーザ アカウントでログインします。
- 5. [Product License(製品ライセンス)] タブをクリックします。購入し たライセンスが一覧表示されます。ライセンスが 1 つしか表示され ない場合や、複数表示される場合があります。
- 各ライセンスを取得するには、リスト内の項目の横にある [作成 (Create)] をクリックします。複数のライセンスがある場合は、最初 に基本ライセンスを作成します。
- 初めてライセンスを作成する場合は、[New License Server Deployment(新しいライセンス サーバ配備)] を選択します。複数の ライセンス サーバで複数の CC-SG を配備している場合は、[Add to an Existing License Server Deployment(既存のライセンス サーバ 配備に追加)] を選択し、このライセンスを追加するライセンス サー バを選択します。
- [Deployment Mode and Path(配備モードおよびパス)] には [Single(単一)] を選択します。[Vendor Daemon Path(ベンダー デーモン パ ス)] は空白のままにし、[次へ] をクリックします。
- 9. [ホスト名] または [Host IP(ホストの IP)] を選択し、ライセンス サ ーバのホスト名または IP アドレスを入力します。
- ライセンス サーバのホスト ID を入力します。不明な場合は次の手順に従って取得します。ホスト ID は、 A005B983-8DFE-D511-A510-00112FCB87F6 のように、文字と 数字からなる長い文字列です。
 - ライセンス サーバのホスト ID を取得するには、ライセンス サ ーバでディレクトリから dmidecode プログラムを実行します



- Linux: su root; dmidecode -s system-uuid
- Windows: cdを使用して /flexnet-win/i86_n3 ディレクトリに 移動し、dmidecode -s system-uuid を実行します。
- CC-SG がライセンス サーバとの通信に使用する TCP ポート番号を入力します。デフォルトのポートは 27000 です。 ライセンス サーバでファイアウォールが有効になっている 場合は、入力するポート番号が開いていることを確認します。
- [Create License(ライセンスの作成)]をクリックします。入力した詳細情報がポップアップに表示されます。ホスト ID が正しいことを確認します。

警告: ホスト ID が正しいことを確認してください。不正なホスト
 ID で作成されたライセンスは、有効ではないので、Raritan のテク
 ニカル サポートに修正してもらう必要があります。

- 12. [OK] をクリックします。ライセンス ファイルが作成されます。
- **13.** [Download Now(今すぐダウンロード)] をクリックし、ライセンス ファイルを保存します。

ライセンス ファイルをライセンス サーバにコピーする

ライセンス ファイルはライセンス サーバに追加する必要があります。 複数のライセンス ファイルがある場合は、テキスト エディタを使用し て各ファイルのすべての内容をコピーして 1 つのファイルに貼り付け 、それをライセンス サーバに保存します。ファイルに .LIC 拡張子を付 けて保存していることを確認してください。

Linux のサーバ

 ライセンス ファイルを /home/flex/flexserverv11.8/i86_lsb/ にコピ ーします。

Windows のサーバ

• ライセンス ファイルを c:\flexnet-win\i86_n3\ にコピーします。

ライセンス サーバを起動する

Linux のサーバ

1. cd /home/flex/flexserverv11.8/i86 lsb/



 1mgrd を実行してサーバを起動します。サンプル コマンド内の "license-file.lic" は .LIC ファイルのファイル名です。複数のライセ ンス ファイルがある場合は、コマンドで各ファイル名を ★ で区切 って指定する必要があります。 コロンで区切ります。次の例を参照 してください。 /lmgrd -c ./license-file.lic

/lmgrd -c ./license-file1.lic:license-file2.lic

Windows のサーバ

- 1. Windows cmd.exe シェルを起動します。
- 次のコマンドを入力してディレクトリを変更します。 cd c:\flexnet-win\i86_n3\
- Imgrd を実行してサーバを起動します。サンプル コマンド内の "license-file.lic" は .LIC ファイルのファイル名です。複数のライセンス ファイルがある場合は、コマンドで各ファイル名を ★ で区切って指定する必要があります。セミコロンで区切ります。次の例を参照してください。

lmgrd -z -c license-file.lic
lmgrd -z -c license-file1.lic;license-file2.lic

CommandCenter Secure Gateway を VMware ESX Server 4.0 にイ ンストールする

- 1. vSphere 4.0 を使用してクライアント コンピュータから ESX 4.0 に接続します。
- 仮想マシンの作成、開始、停止許可を持つユーザとしてログインします。
- [File(ファイル)] > [Deploy OVF Template(OVF テンプレートの配備)] を選択します。
- [Deploy From File(ファイルから配備)] を選択し、[参照] をクリック してファイルを解凍したディレクトリに移動します。.OVF ファイ ルを選択します。[次へ] をクリックします。
- 5. 作成される仮想マシンの詳細が表示されます。仮想マシンのデフォ ルト名は変更可能です。[次へ]をクリックします。
- 6. インベントリの場所を選択します。[次へ]をクリックします。
- CommandCenter Secure Gateway の配備先にするホストを選択します。フェイルオーバ保護のため、高可用クラスタを構成するホストを選択することをお勧めします。[次へ]をクリックします。
- 8. クラスタを選択した場合は、特定のホストを選択します。[次へ] を クリックします。
- すべてのファイルを保存するデータストアを選択します。データストアに 40GB の空き領域があることを確認します。[次へ] をクリックします。



- 10. CC-SG が配備されるネットワークを選択します。[次へ] をクリッ クします。
- 11. サマリーを表示し、[終了] をクリックします。仮想マシンが作成さ れる間、数分待ちます。
- 12. 仮想マシンの電源をオンにします。
- **13.** [コンソール] タブを開き、CC-SG の診断コンソールにアクセスします。

診断コンソールにログインし CC-SG IP アドレスを設定する

- 1. admin/raritan としてログインします。ユーザ名とパスワードは大文 字と小文字を区別します。
- 2. 続いてローカル コンソールのパスワードの変更を求めるプロンプト が表示されます。
 - a. デフォルトのパスワード (raritan) を再度入力します。
 - b. 新しいパスワードを入力し、確認します。新しいパスワードは 、文字と数字を組み合わせた 8 文字以上の強力なパスワードに する必要があります。
- 3. [Welcome] 画面が表示されたら CTRL+X を押します。
- 4. [Operation] > [Network Interfaces] > [Network Interface Config] を選 択します。Administrator Console が表示されます。
- 5. [Configuration] フィールドから、[DHCP] または [Static] を選択し ます。[Static] を選択した場合、静的 IP アドレスを入力します。必 要に応じて、DNS サーバ、ネットマスク、ゲートウェイ アドレス を指定します。
- 6. [Save] を選択します。CC-SG が再起動するまで数分間待ちます。

CC-SG のデフォルト設定

IP アドレス: 192.168.0.192 サブネット マスク: 255.255.255.0 ユーザ名/パスワード: admin/raritan

CC-SG にログインする

 サポートされているブラウザを起動し、CC-SG の URL 「https://<IP アドレス>/admin」と入力します。

たとえば、「https://192.168.0.192/admin」のように入力します。

注: ブラウザ接続のデフォルトの設定は、HTTPS/SSL 暗号化です

2. セキュリティ警告ウィンドウが表示されたら、接続を受け入れます



- サポートされていない Java Runtime Environment バージョンを使用すると、警告が表示されます。プロンプトの表示に従って、正しいバージョンをダウンロードするか、続行します。ログイン ウィンドウが表示されます。
- デフォルトのユーザ名 (admin) とパスワード (raritan) を入力し、 [Login] をクリックします。
 CC-SG Admin Client が表示されます。

ライセンスをインストールしてチェックアウトする

- 1. [管理] > [License Management(ライセンス管理)] を選択します。
- 2. [Add License(ライセンスの追加)] をクリックします。
- 3. ライセンス契約を読み、テキスト領域の下までスクロールして、[I Agree(同意する)] チェックボックスをオンにします。
- 4. [参照] をクリックし、仮想アプライアンスの基本ライセンス ファイ ルを選択します。
- 5. [開く] をクリックします。CC-SG がライセンス サーバと接続され 、ライセンスされている機能のリストが取得されます。機能がリス トに表示されます。
- 6. CCSG128-VA の基本ライセンスを選択し、[Check-Out(チェックア ウト)] をクリックして有効にします。
- 7. アドオン ライセンスを有効にするには、各ライセンスを選択し、 [Check-Out(チェックアウト)] をクリックします。

ライセンスについての詳細は、『CC-SG 管理者ガイド』を参照してくだ さい。 ライセンス サーバの管理の詳細は、Flexera[™] FlexNet Publisher[®] マニュアルを参照してください。『FlexNet Publisher License Administration Guide for FlexNet Publisher Licensing Toolkit 11.8』は、 www.flexera.com の [Support(サポート)] > [Documentation Center(ドキ ュメンテーション センター)] からダウンロードできます。

ライセンス サーバ通信

CC-SG 仮想アプライアンスとライセンス サーバ間の接続を維持する必要があります。**CC-SG** は、この接続を使用して、ライセンス サーバの 稼働を確認したり、使用可能なライセンス ファイルを特定したります 。また、ライセンスのチェックインおよびチェックアウト時にも使用さ れます。



ライセンスにアクセスする

チェックアウトされるすべてのライセンスは、常にライセンス サーバ で利用可能になっている必要があります。ライセンス ファイルがライ センス サーバから移動または削除されている場合、CC-SG がライセン ス サーバをポーリングするときにライセンスを確認できなくなります 。チェックアウトされているライセンスがライセンス サーバで見つか らない場合は、CC-SG はアクセスを停止します。

アクセスの切断を回避するには、ライセンス サーバからライセンスを 移動または削除する前に、常にライセンスをチェックインするようにし ます。

ライセンス サーバの障害

CC-SG がライセンス サーバと接続できない場合、ライセンスは、7 日間の猶予期間中、引き続き有効になります。ライセンス サーバとの接続が回復していない場合は、**CC-SG** にログインするたびに、最終アク セス可能日を通知するメッセージが表示されます。

ライセンス サーバとの接続が回復しないまま 7 日間の猶予期間が経過 した場合は、チェックアウトしたライセンスはチェックインされます。 CC-SG はアクセスを停止します。その後は、CC-SG でアクセスできる オプションが限定されます。「*ライセンス設定 - ライセンスのインスト* ール前の限られた動作 『32p. 』」を参照してください。

ライセンス サーバが再稼働した場合は、各ライセンスを再度チェック アウトして通常の操作を再開する必要があります。「*ライセンスをイン ストールしてチェックアウトする* **[27**p. **]**」を参照してください。

障害後にライセンス サーバを再起動する

ライセンス サーバが障害発生後に処理を再開した場合、またはライセンス ファイルを移動、追加、または削除した場合は、ライセンス サーバを再起動する必要があります。

ライセンス サーバを再起動すると、CC-SG を最新情報と確実に同期させることができます。

注: Windows のライセンス サーバは障害後に自動的に同期されます。 Linux のライセンス サーバは、2 時間のタイムアウト後に同期されます が、再起動すれば障害後すぐに同期されます。

▶ ライセンス サーバを再起動するには、以下の手順に従います。

コマンド 1mdown を実行してライセンス サーバを正常にシャットダウ ンします。



ライセンス サーバ管理用のコマンド ライン ユーティリティ

ライセンス サーバ ソフトウェアをインストールすると、以下のユーティリティがインストールされます。それぞれをコマンド ラインから実行してライセンス サーバを管理できます。

サンプルでは、カッコ内の項目に以下の値を使用します。

<機能名> は、Admin Client の [管理] > [ライセンス マネージャ] ページの [Feature(機能)] 列内の値です。たとえば、"CCSG128-VA" は、仮想アプライアンスの基本ライセンスの機能名です。

<ライセンス ファイル名> は、インストールされているライセンス フ ァイルがライセンス サーバに保存されたときのファイル名です。

ライセンス サーバの管理の詳細は、Flexera[™] FlexNet Publisher[®] マニュ アルを参照してください。『FlexNet Publisher License Administration Guide for FlexNet Publisher Licensing Toolkit 11.8』は、www.flexera.com の [Support(サポート)] > [Documentation Center(ドキュメンテーション センター)] からダウンロードできます。

コマンド	説明
Imborrow	ユーザが機能をチェックアウトし、一定 期間それを借用できるようにします。た だし、ネットワークからは切断されます 。
Imdiag	機能をチェックアウトできないときに、 ユーザが問題を診断できるようにします 。機能のチェックアウトを試み、その成 否を示します。 1mdiag -c <ライセンス ファイル名> < 機能名> -n
Imdown	選択したライセンス デーモンを正常にシ ャットダウンします。 Raritan ベンダ デーモンをシャットダウ ンするには、1mdown -vendor raritan を使用します。
Imhostid	ユーザが現在のプラットフォームのホス ト ID を取得できるようにします。 -uuid と、-hostdomain または -internet 引数を含めます。
Iminstall	読み取り可能なテキスト形式と 10 進数 形式との間でライセンスの変換を可能に します。



Ch 3: 使用を始める際に

Imnewlog	既存のレポート ログ情報を新しいファイ ルに移動し、元のログ ファイル名で新し いレポートを開始します。
Impath	現在のライセンス パス設定に追加、設定 の上書き、または取得を行います。
Imremove	指定した機能の 1 人のユーザ ライセン スを削除します。 ライセンス サーバ マネージャで、 Imremove を許可なく実行できないよう に設定できます。
Imreread	lmreread - vendor raritan は、 Raritan ベンダ デーモンでライセンスお よびオプション ファイルを再度読み取る 場合に使用されます。
Imswitchr	既存のレポート ログを閉じ、新しいレポ ート ログを新しいファイル名で開始しま す。 レポート ログ ファイルがない場合に新 しいファイルを開始するためにも使用で きます。
Imswitch	ベンダ デーモンの既存のデバッグ ログ を終了し、新しいファイル名でそのベン ダ デーモンの新しいデバッグ ログを開 始します。 ベンダ デーモンが書き込んだデバッグ ログ ファイルがない場合に新しいファイ ルを開始するためにも使用できます。
Imstat	 ライセンス サーバから受信するライセン ス ファイル ステータス、機能の可用性 、および使用情報を取得して表示します 。 lmstat -c <ライセンス ファイル名> -f <機能名>
Imver	Imgrd、Imadmin、Imdown、ベンダ デー モンなどの FLEXnet Publisher ライブラ リまたはバイナリ ファイルのバージョン をレポートします。



VMware ツールをインストールまたはアップグレードする

VMware は、VMware ツールをすべての仮想マシン配備にインストール することを推奨しています。いったん VMware ツールを CommandCenter Secure Gateway 仮想アプライアンスにインストール しておけば、VMware が新リリースを公開したときに、このプロセスに 従ってツールをアップグレードできます。

仮想 CC-SG OVF パッケージには、デフォルトでインストールされる VMware ツール バージョンが含まれています。

- VMware ツールをインストールまたはアップグレードするには、以下の手順に従います。
- 1. vSphere クライアントにログインし、CC-SG 仮想アプライアンス をホストしている ESX ホストに接続します。
- 2. 仮想マシンを選択し、[コンソール] タブをクリックします診断コン ソールが表示されます。
- 仮想マシンを右クリックし、[Guest(ゲスト)] > [Install/Upgrade VMware Tools(VMware のインストール/アップグレード)] を選択し ます。これによって、ファイルが仮想マシンにマウントされるので 、CC-SG によるインストールが可能なります。
- 4. ブラウザを開き、Admin Client にログインします。
- 5. [システム メンテナンス] > [Install / Upgrade VMware Tools(VMware のインストール/アップグレード)] を選択します。インストールが完 了すると、成功メッセージが表示されます。

仮想アプライアンスおよびストレージ サーバのバックアップとスナッ プショットを設定する

CC-SG 仮想アプライアンスを配備したら、VMware[®] を通じて仮想アプ ライアンスのバックアップを設定し、それによって使用されるストレー ジ サーバのバックアップを設定します。

また、VMware でスナップショットを有効にすることも必要です。

これらの機能の詳細は、VMware のマニュアル

(http://www.vmware.com/jp/support/pubs/vs_pubs.html) を参照してくだ さい。

リモート ストレージ サーバを使用する仮想アプライアンス

CC-SG 仮想アプライアンスでファイル ストレージにリモート サーバ を使用している場合にそのストレージにアクセスできなくなると、スト レージ サーバが完全に起動されるまで CC-SG へのアクセスが中断さ れることがあります。場合によっては、Problems Retrieving Configuration Data(設定データ取得エラー) メッセージが表示されます



ライセンス設定 - ライセンスのインストール前の限られた動作

適切なライセンスをインストールしてチェックアウトするまで、CC-SG の動作は制限されます。次のメニュー項目だけが有効になります。

 診断コンソール:必要な情報およびログを取得するために、ネット ワーク インタフェースを設定します。

注: VGA/キーボード/マウス ポート (該当する場合)、シリアル ポート (該当する場合)、または SSH を介して Administrator Console と Status Console の両方のインタフェースにアクセスできます。 Status Console インタフェースは、有効にすると Web インタフェースからも利用できます。

- パスワードの変更
- Secure Gateway: [今日のメッセージ]、[印刷]、[画面印刷]、[ログア ウト]、および [終了] が表示されます。
- [管理]>[クラスタ設定]: クラスタを設定し、クラスタ ノードに役割 を割り当てます。クラスタベースのライセンスで動作するためには、クラスタの構築が前提条件となります。クラスタは、物理アプラ イアンスでのみ利用できます。
- [管理]>[ライセンス マネージャ]: ライセンス ファイルのアップロ ードや削除、およびライセンスのチェックアウト/チェックインを許 可します。
- システム メンテナンス:次のメニュー項目が有効になります。
 - リストア:完全にリセットした場合や、誤ってライセンスを削除 した場合に備えて、CC-SGのライセンスの復元を許可します。
 - メンテナンス モード:必要に応じてメンテナンス モードを切り 替え、クラスタを作成したりアップグレードを実行します。
 - 再起動
 - アップグレード
 - シャットダウン
- 表示
- ヘルプ:オンライン ヘルプ ドキュメントを表示します。



ライセンス設定 - 既存の顧客

既存の CC-SG 物理アプライアンスの顧客が CC-SG ユニットを 5.0 以降にアップグレードする場合は、アップグレード時に設定したノード 数で引き続き CC-SG を使用できるようになるライセンス ファイルが 作成され、インストールされます。

既存のすべての顧客は、まず 5.0 にアップグレードしてから 5.0 より 上のリリースにアップグレードする必要があります。

このトピックの手順に従って、5.0 へのアップグレード後にライセンス ファイルが整っていることを確認してください。

▶ 手順 1:5.0 へのアップグレード:

「CC-SG のアップグレード 『256p. 』」を参照してください。

- ▶ 手順 2: ライセンス ファイルの表示:
- Admin Client で、[管理] > [License Management(ライセンス管理)] を選択します。[ライセンス マネージャ] ページが開きます。
 - [License Summary(ライセンスの概要)] セクションに、ライセン スに関する概略の情報が表示されます。ライセンス ファイルに 関連付けられている CC-SG ホスト ID を表示できます。
 - 使用中のノード数および許可されたノード数が、ページの中央 に表示されます。

注: 許可されたノード数が最初にライセンスを購入したときの数よ り少ないことが判明した場合は、Raritan の正規販売店にお問い合 わせください。

ライセンス設定 - 再ホスト

物理アプライアンス ライセンスは、ある特定の CC-SG ユニットに関 連付けられます。仮想アプライアンス ライセンスは、ある特定のライ センス サーバに関連付けられます。

これらのアイテムが変わった場合、ライセンス ファイルが間違ったホ スト ID に割り当てられている場合、または何らかの原因でライセンス ファイルと CC-SG システムが一致していない場合は、正しいホスト ID で新しいライセンス ファイルを取得する必要があります。

 別のホスト ID で新しいライセンス ファイルを取得するには、以下 の手順に従います。

ラリタン社のテクニカル サポートにご連絡ください。「**Technical** Support Contacts(テクニカル サポートの問い合わせ先) 『2p. 』」を 参照してください。



ライセンスの追加

新しいアドオン ライセンスを購入する場合、または既存のライセンスの置換が必要な場合は、CC-SG にライセンスを追加できます。

ライセンスを置換する場合は、最初に基本ライセンスを追加します。以前の基本ライセンスに関連付けられているアドオン ライセンスは、ス タンドアロンまたはクラスタなどタイプが異なるかホスト ID が異なる などの理由で新しい基本ライセンスで有効でない場合には自動的に削除 されます。

ライセンス置換のルールの詳細は、「*ライセンス設定に関する FAQ* 『 433p. 』」を参照してください。

▶ ライセンスを追加するには、以下の手順に従います。

- 1. [管理] > [License Management(ライセンス管理)] を選択します。
- 2. [Add License(ライセンスの追加)] をクリックします。
- 3. ライセンス契約を読み、テキスト領域の下までスクロールして、[I Agree(同意する)] チェックボックスをオンにします。
- 4. [参照] をクリックし、ライセンス ファイルを選択します。
- [開く] をクリックします。
 注: ライセンス サーバを使用している場合、CC-SG はライセンス サーバにアクセスしてサーバで見つかった全機能のリストを表示し ます。
- 6. 有効にする機能を選択して、[Check Out(チェックアウト)] をクリッ クします。

IP アドレスの確認

- 1. [管理]>[設定] を選択します。
- 2. [ネットワーク設定] タブをクリックします。
- 3. ネットワーク設定が正しいことを確認し、必要に応じて変更を加え ます。「*ネットワーク設定について* 『271p. 』」を参照してくださ い。オプション。
- 4. [設定の更新] をクリックして変更を適用します。
- 5. [すぐに再起動] をクリックし、設定を確認して CC-SG を再起動し ます。



CC-SG サーバ時間の設定

CC-SG では、デバイス管理機能の信頼性のため、常に正確な日付と時刻を表示する必要があります。

重要:時刻/日付設定は、タスク マネージャでタスクをスケジュールする 際に使用されます。「タスク マネージャ 『311p. 』」を参照してくだ さい。クライアント PC の時刻設定は CC-SG の時刻設定と異なってい ても構いません。

時刻と日付を設定できるのは、CC スーパーユーザおよび同等の権限を 持つユーザだけです。

クラスタ設定ではタイム ゾーンの変更は無効になっています。

- ▶ **CC-SG** サーバ時間および時刻を設定するには、以下の手順に従います。
- 1. [管理]>[設定] を選択します。
- 2. [時刻/日付] タブをクリックします。
 - a. 日付と時刻を手動で設定するには、以下の手順に従います。
 - 日付 ドロップダウン矢印をクリックして月を選択し、上下の 矢印を使用して年を選択してから、カレンダー領域で日をクリ ックします。
 - 時刻 上下矢印を使って時、分、秒を設定し、次に [タイム ゾ ーン] ドロップダウン矢印をクリックして CC-SG が動作する タイム ゾーンを選択します。
 - a. 日付と時刻を NTP 経由で設定するには、以下の手順に従います。ウィンドウ下部の [ネットワーク時間プロトコルを有効にする] チェックボックスを選択し、プライマリ NTP サーバとセカンダリ NTP サーバの IP アドレスを対応するフィールドに入力します。

注: Network Time Protocol (NTP) は、接続されたコンピュータの日 付と時刻のデータを参照用 NTP サーバに同期させるためのプロト コルです。CC-SG を NTP で設定すると、そのクロックの時刻を 適切な NTP 参照サーバに同期させ、正確で一貫した時刻を維持す ることができます。

- 3. [設定の更新] をクリックして日付と時刻の変更を CC-SG に適用し ます。
- 4. [更新] をクリックして、新しいサーバ時刻を [現在の時刻] フィール ドに再ロードします。

[システム メンテナンス]>[再起動] を選択して CC-SG を再起動しま す。



互換表の確認

互換表には、CC-SG の現在のバージョンと互換性のある、Raritan のフ アームウェア バージョンおよびアプリケーションのソフトウェア バー ジョンの一覧が表示されます。CC-SG は、デバイスを追加したり、デ バイス ファームウェアをアップグレードしたり、あるいは使用するア プリケーションを選択したりするごとに、このデータと照合してチェッ クします。ファームウェアやソフトウェアのバージョンに互換性がない 場合は、さらに手順を進める前に CC-SG が警告メッセージを表示しま す。CC-SG の各バージョンは、Raritan デバイスのリリースの時点での 最新ファームウェア バージョンおよびそれ以前のバージョンしかサポ ートしません。互換表は、Raritan のサポート Web サイトで参照でき ます。

- 互換表を確認するには、以下の手順に従います。
- [管理]>[互換表] を選択します。

アプリケーション バージョンの確認とアップグレード

Raritan Console (RC) や Raritan Remote Client (RRC) などの CC-SG アプリケーションを確認およびアップグレードします。

- アプリケーション バージョンを確認するには、以下の手順に従います。
- 1. [管理] > [アプリケーション] を選択します。
- リストからアプリケーション名を選択します。[バージョン] フィー ルドの番号を確認してください。一部のアプリケーションは、バー ジョン番号が自動的に表示されません。
- アプリケーションをアップグレードするには、以下の手順に従います。

アプリケーションのバージョンが最新でない場合は、アプリケーション をアップグレードする必要があります。アプリケーション アップグレ ード ファイルは、Raritan の Web サイトからダウンロードできます。 サポートされるアプリケーションのバージョンをまとめたリストが必要 な場合は、Raritan のサポート Web サイトで互換表を参照してください。

アプリケーションをアップグレードする前に、メンテナンス モードで 起動することをお勧めします。「メンテナンス モードの起動 『247p. 』 」を参照してください。

1. クライアント PC にアプリケーション ファイルを保存します。



- [アプリケーション名] ドロップダウン矢印をクリックし、アップグレードする必要があるアプリケーションをリストから選択します。アプリケーションが表示されない場合は、まず追加する必要があります。「アプリケーションの追加 『268p. 』」を参照してください。
- 3. [参照] をクリックして、表示されるダイアログでアプリケーション アップグレード ファイルを見つけて選択し、[開く] をクリックしま す。
- 4. [アプリケーション マネージャ] 画面の [新しいアプリケーション ファイル] フィールドにアプリケーション名が表示されます。
- [アップロード] をクリックします。進捗ウィンドウに新しいアプリ ケーションをアップロード中であることが示されます。完了すると 、別のウィンドウが表示され、新しいアプリケーションが CC-SG データベースに追加されて、使用可能なことが示されます。
- [バージョン] フィールドが自動的に更新されない場合は、[バージョン] フィールドに新しいバージョン番号を入力します。一部のアプリケーションについては、[バージョン] フィールドが自動的に更新されます。
- 7. [更新] をクリックします。

注: アップグレード時にログインしていたユーザは、いったん CC-SG からログアウトしてから、再度ログインし、新しいバージョンのアプリ ケーションが起動されるようにする必要があります。「アップグレード 後に古いバージョンのアプリケーションが開く 『268p. 』」も参照して ください。



Ch 4

ガイド付き設定を使用した **CC-SG** の 設定

ガイド付き設定は、ネットワーク設定の完了後、最初の CC-SG 設定タ スクを完了するための簡単な手段を提供するものです。ガイド付き設定 インタフェースでは、関連の定義、デバイスの検出と CC-SG への追加 、デバイス グループおよびノード グループの作成、ユーザ グループ の作成、ユーザ グループへのポリシーおよび権限の割り当て、ユーザ の追加を行う手順が案内されます。ガイド付き設定を完了した後は、い つでも構成を個別に編集できます。

ガイド付き設定は、以下の4つのタスクに分類されます。

- 関連 装置を整理するためのカテゴリおよびエレメントを定義します。「ガイド付き設定の関連 『39p. 』」を参照してください。
- デバイス設定 ネットワーク内のデバイスを検出し、それを CC-SG に追加します。デバイス ポートを構成します。「デバイス 設定 『39p. 』」を参照してください。
- グループの作成 CC-SG が管理するデバイスおよびノードをグル ープに分類し、各グループについてフル アクセス ポリシーを作成 します。「グループの作成 『41p. 』」を参照してください。
- ユーザ管理 ユーザとユーザ グループを CC-SG に追加し、
 CC-SG 内でデバイスおよびノードへのユーザ アクセスを管理する ポリシーおよび権限を選択します。「ユーザ管理 『44p. 』」を参照 してください。

名前の長さに関する CC-SG のルールについての詳細は、「*命名規則*『 **435**p. 』」を参照してください。

この章の内容

ガイド付き設定を使用する前に	.38
ガイド付き設定の関連	.39
デバイス設定	.39
グループの作成	.41
ユーザ管理	.44

ガイド付き設定を使用する前に

CC-SG の構成手順を進める前に、システム構成を完了する必要があります。

 IP アドレスの割り当てを含めて、Dominion シリーズおよび IP-Reach アプライアンス (シリアルおよび KVM の両デバイス)を 構成およびインストールします。



ガイド付き設定の関連

カテゴリとエレメントの作成

- ガイド付き設定でカテゴリとエレメントを作成するには、以下の手順に従います。
- [ガイド付き設定] ウィンドウで、[関連] をクリックし、左のパネルの [カテゴリの作成] をクリックして [カテゴリの作成] パネルを開 きます。
- 2. [カテゴリ名] フィールドで、装置を整理するカテゴリの名前を入力 します (例: 「Location」など)。
- [適用対象] フィールドで、デバイスまたはノード、あるいはその両 方でカテゴリを使用可能にするかどうかを示します。[適用対象] ド ロップダウン メニューをクリックし、リストから値を選択します。
- [エレメント] テーブルで、カテゴリ内のエレメントの名前を入力し ます (例: 「Raritan US」など)。

 - エレメントを削除するには、その行を選択してから、[選択した 行をテーブルから削除] アイコン
 をクリックします。
- 5. カテゴリ内のすべてのエレメントを [エレメント] テーブルに追加す るまで上記の手順を繰り返します。
- 別のカテゴリを作成するには、[適用] をクリックしてこのカテゴリ を保存した後、このセクションの手順を繰り返してカテゴリを追加 します。(任意)
- カテゴリとエレメントの作成が終わったら、[OK] をクリックします。 [関連の概要] パネルには、作成したカテゴリとエレメントのリストが表示されます。
- 8. [続行] をクリックし、次のタスクであるデバイス設定を開始します。次のセクションの手順に従います。

デバイス設定

ガイド付き設定の 2 番目のタスクは、デバイス設定です。デバイス設 定により、ネットワーク内のデバイスを検索および検出し、検出された デバイスを CC-SG に追加できます。デバイスを追加する場合、デバイ スに関連付けるカテゴリごとに 1 つのエレメントを選択できます。

重要: **CC-SG** 設定時に、デバイスに他のユーザがログオンしていないこ とを確認してください。



デバイスの検出と追加

関連タスクが終わった後、[続行] をクリックすると、[デバイス検出] パ ネルが開きます。また、[デバイス設定] をクリックし、左のパネルの [ガイド付きタスク] ツリー表示で [デバイス検出] をクリックしても、[デバイス検出] パネルを開くことができます。

- ガイド付き設定でデバイスを検出し、追加するには、以下の手順に 従います。
- 1. [開始アドレス] フィールドと [終了アドレス] フィールドに、デバイ スの IP アドレスを検索する範囲を入力します。
- 2. デバイスを検索する際のサブネット マスクを [マスク] フィールド に入力します。
- [デバイス タイプ] リストで、指定した範囲で検索するデバイスのタ イプを選択します。複数のデバイス タイプを選択する場合は、Ctrl キーを押しながらデバイス タイプをクリックします。
- CC-SG と同じサブネットにあるデバイスを検索する場合は、[ブロ ードキャスト検出] チェックボックスを選択します。すべてのサブ ネット上のデバイスを検出するには、[ブロードキャスト検出]の選 択を解除します。
- 5. [検出] をクリックします。
- 6. CC-SG により指定のアドレス範囲で指定のタイプのデバイスが検 出された場合、[デバイス検出] パネルの下部にあるテーブルにデバ イスが表示されます。パネルの上部の黒い矢印をクリックすると上 部のセクションが隠れ、パネルの下部のセクションで検出結果の表 示が拡張されます。
- 検出されたデバイスのテーブルで、CC-SG に追加するデバイスを 選択し、[追加] をクリックします。[デバイスの追加] パネルが開き ます。[デバイスの追加] パネルは、追加するデバイスのタイプによ って若干異なります。
- 8. [デバイス名] と [説明] は、対応するフィールドに新しい情報を入力 することにより変更できます。
- 9. 必要に応じて、CC-SG へのデバイスの追加準備時に割り当てた IP アドレスが [デバイスの IP またはホスト名] フィールドに表示され ていることを確認するか、正しいアドレスをフィールドに入力しま す。
- 10. [TCP ポート番号] フィールドは、デバイス タイプに基づいて自動 的に入力されます。
- 11. CC-SG へのデバイスの追加準備時に作成したユーザ名とパスワー ドを対応するフィールドに入力します。



- 12. [ハートビート タイムアウト (秒)] フィールドに、デバイスと CC-SG との間でのタイムアウトまでの時間を秒単位で入力します
- Dominion SX デバイスまたは Dominion KXII バージョン 2.2 以降 のデバイスを追加する場合、デバイスにローカル アクセスを許可す るには、[デバイスの直接アクセスを許可] チェックボックスをオン にします。デバイスへのローカル アクセスを許可しない場合は、[ローカル アクセス] で [許可] チェックボックスをオフにします。
- 電源タップ デバイスを手動で追加する場合は、[ポート数] ドロップ ダウン矢印をクリックし、電源タップにあるコンセントの数を選択 します。
- 15. IPMI サーバを追加する場合は、可用性の確認に使用される間隔を [間隔] フィールド、IPMI サーバの設定内容に一致する必要がある認 証メソッドを [認証メソッド] フィールドに入力します。
- 16. デバイス上で使用可能なすべてのポートを設定する場合は、[すべてのポートの設定] チェックボックスを選択します。デバイス上のすべてのポートが CC-SG に追加され、各ポートに対応するノードが作成されます。
- 17. パネル下部の [デバイスの関連] セクションで、デバイスに割り当て る各カテゴリに対応するエレメント列のドロップダウン矢印をクリ ックし、デバイスに関連付けるエレメントをリストから選択します

注: 同じカテゴリの複数のエレメントが割り当てられているノード またはデバイスは、カテゴリおよびエレメントに基づいて、カスタ ム表示に複数回表示されます。

- 18. エレメントをデバイス、およびそのデバイスに接続するノードに適 用する場合は、[ノードに適用] チェックボックスを選択します。
- 19. 別のデバイスを追加する場合は、[適用] をクリックしてこのデバイ スを保存し、この手順を繰り返します。オプション。
- 20. デバイスの追加が終わったら、[OK] をクリックします。[デバイスの概要] パネルに、追加したデバイスのリストが表示されます。
- 21. [続行] をクリックし、次のタスクであるグループの作成を開始しま す。次のセクションの手順に従います。

グループの作成

ガイド付き設定の 3 番目のタスクは、グループの作成です。グループ の作成では、デバイス グループおよびノード グループを定義し、各グ ループに含まれるデバイスまたはノードのセットを指定できます。管理 者は、各デバイスまたはノードを個別に管理するのではなく、同様のデ バイスおよびノードのグループを管理することで、時間を節約できます



デバイス グループおよびノード グループの追加

- ガイド付き設定でデバイス グループおよびノード グループを追加 するには、以下の手順に従います。
- [デバイス グループ:新規] パネルを、デバイス設定タスクが終わった後、[続行] をクリックして開きます。また、[グループの作成] を クリックし、左のパネルの [ガイド付きタスク] ツリー表示で [デバ イス グループの追加] をクリックする方法で、[デバイス グループ: 新規] クリックします。
- 2. [グループ名] フィールドで、作成するデバイス グループの名前を入 力します。
- グループにデバイスを追加するには、[デバイスの選択] と [デバイスの説明] の 2 つの方法があります。[デバイスの選択] タブでは、使用可能なデバイスのリストから、グループに割り当てるデバイスを選択できます。[デバイスの説明] タブでは、デバイスについて記述するルールを指定できます。このルールに従うパラメータを持つデバイスがグループに追加されます。
 - デバイスの選択
 - a. [デバイス グループ:新規] パネルの [デバイスの選択] タブを クリックします。
 - b. [利用可能] リストで、グループに追加するデバイスを選択し、[追加] をクリックしてデバイスを [選択中] リストに移動します
 。[選択中] リストのデバイスがグループに追加されます。
 - c. グループからデバイスを削除するには、[選択中] リストでデバ イス名を選択し、[削除] をクリックします。
 - d. [利用可能] リストまたは [選択中] リストのいずれでもデバイス を検索できます。リストの下にあるフィールドに検索語を入力 し、[実行] をクリックします。
 - デバイスの説明
 - a. [デバイス グループ:新規] パネルの [デバイスの説明] タブを クリックします。[デバイスの説明] タブで、グループに割り当 てるデバイスを説明するルールのテーブルを作成します。
 - b. [新しい行をテーブルに追加] アイコン
 をクリックして行を
 テーブルに追加します。
 - c. 各列で作成したセルをダブルクリックしてドロップダウン メニ ューを開きます。各リストから使用するルール コンポーネント を選択します。



- このデバイス グループに対して、グループ内のすべてのノードおよびデバイスへの制御許可付きアクセスを常に許可するポリシーを作成する場合は、[グループにフル アクセス ポリシーを作成] チェックボックスを選択します。
- 5. 別のデバイス グループを追加するには、[適用] をクリックしてこの グループを保存し、以下の手順を繰り返します。オプション。
- デバイス グループの追加が終わったら、[OK] をクリックします。[ノード グループ:新規] パネルが開きます。また、[グループの作成] をクリックし、左のパネルの [ガイド付きタスク] ツリー表示で [ノ ード グループの追加] をクリックする方法でも、[ノード グループ: 新規] クリックします。
- 7. 作成するノード グループの名前を [グループ名] フィールドに入力 します。
- グループにノードを追加する方法には、[ノードの選択] と [ノードの説明]の2種類があります。[ノードの選択] セクションでは、使用可能なノードのリストから、グループに割り当てるノードを選択できます。[ノードの説明] タブでは、ノードについて記述するルールを指定できます。このルールに従うパラメータを持つノードがグループに追加されます。
 - ノードの選択
 - a. [ノード グループ: 新規] パネルの [ノードの選択] タブをクリ ックします。
 - b. [利用可能] リストで、グループに追加するノードを選択し、[追加] をクリックしてノードを [選択中] リストに移動します。[選択中] リストのノードがグループに追加されます。
 - c. グループからノードを削除するには、[選択中] リストでノード 名を選択し、[削除] をクリックします。
 - d. [利用可能] または [選択中] リストのいずれでも、ノードを検索 できます。リストの下にあるフィールドに検索語を入力し、[実 行] をクリックします。
 - ノードの説明
 - a. [ノード グループ:新規] パネルの [ノードの説明] タブをクリ ックします。[ノードの説明] タブで、グループに割り当てるノ ードを記述するルールのテーブルを作成します。
 - b. [新しい行をテーブルに追加] アイコン
 をクリックして行を
 テーブルに追加します。
 - c. 各列で作成したセルをダブルクリックしてドロップダウンメニューを開きます。各リストから使用するルール コンポーネントを選択します。「アクセス制御のポリシー 『197p. 』」を参照してください。



Ch 4: ガイド付き設定を使用した CC-SG の設定

- このノード グループに対して、グループ内のすべてのノードへの制 御許可付きアクセスを常に許可するポリシーを作成する場合は、[グ ループにフル アクセス ポリシーを作成] チェックボックスを選択 します。
- 10. 別のノード グループを追加するには、[適用] をクリックしてこのグ ループを保存し、上記の手順を繰り返します。オプション。
- 11. ノード グループの追加が終わったら、[OK] をクリックします。[グ ループの概要] パネルには、追加したグループのリストが表示され ます。
- 12. [続行] をクリックし、次のタスクであるユーザ管理を開始します。 次のセクションの手順に従います。

ユーザ管理

ガイド付き設定の 4 番目のタスクは、ユーザ管理です。ユーザ管理で は、ユーザ グループのアクセスおよび作業を管理する権限とポリシー を選択できます。権限では、CC-SG 内でユーザ グループのメンバが実 行できる作業を指定します。ポリシーでは、ユーザ グループのメンバ が表示および変更できるデバイスおよびノードを指定します。ポリシー は、カテゴリとエレメントに基づきます。ユーザ グループを作成した 場合、個別のユーザを定義してユーザ グループに追加できます。

ユーザとユーザ グループの追加

グループの作成タスクが終わった後、[続行] をクリックすると、[ユーザ グループの追加] パネルが開きます。また、[ユーザ管理] をクリックし 、左のパネルの [ガイド付きタスク] ツリー表示で [ユーザ グループの 追加] をクリックして [ユーザ グループの追加] パネルを開くこともで きます。

- ガイド付き設定でユーザ グループおよびユーザを追加するには、以下の手順に従います。
- [ユーザ グループ名] フィールドで、作成するユーザ グループの名 前を入力します。ユーザ グループ名には、最大 64 文字を含めるこ とができます。
- 2. [説明] フィールドに、ユーザ グループの説明を入力します。
- このユーザ グループのユーザごとに、この機能が有効になっている デバイスへのアクセス時の最大 KVM セッション数を設定するには 、[Limit Number of KVM Sessions per Device (デバイスあたりの KVM セッション数を制限する)] チェックボックスをオンにし、 [Max KVM Sessions (1-8) (最大 KVM セッション (1 ~ 8))] フィー ルドで許可するセッション数を選択します。オプション。詳細は、 「ユーザあたりの KVM セッション数の制限 『182p. 』」を参照し てください。



- [権限] タブをクリックし、権限に対応するチェックボックスを選択 するか、またはユーザ グループに割り当てる CC-SG 作業のタイ プに対応するチェックボックスを選択します。
- [ノード アクセス] セクションでは、ユーザ グループにインバンド ノード、アウト オブ バンド ノード、およびパワー管理機能へのア クセスを許可するかどうかを指定できます。グループに割り当てる アクセス タイプに対応するチェックボックスを選択します。
- 6. [ポリシー] タブをクリックします。
- [すべてのポリシー] リストで、ユーザ グループに割り当てるポリシ ーを選択し、[追加] をクリックしてそのポリシーを [選択されたポ リシー] リストに移動します。[選択されたポリシー] リスト内のポ リシーがユーザ グループに割り当てられます。この手順を繰り返し て、ユーザ グループにポリシーを追加します。
- ユーザ グループからポリシーを削除するには、[選択されたポリシー] リストでポリシー名を選択し、[削除] をクリックします。
- リモートに認証されたユーザを Active Directory モジュールに関連 付ける場合は、AD が設定された [Active Directory の関連付け] タ ブが表示されている状態で、[Active Directory の関連付け] タブをク リックします。ユーザ グループに関連付ける各 Active Directory モ ジュールに対応するチェックボックスを選択します。
- 10. 別のユーザ グループを追加するには、[適用] をクリックしてこのグ ループを保存し、上記の手順を繰り返します。オプション。
- ユーザ グループの追加が終わったら、[OK] をクリックします。[ユ ーザの追加] パネルが開きます。また、[ユーザ管理] をクリックし 、左のパネルの [ガイド付きタスク] ツリー表示で [ユーザの追加] をクリックしても、[ユーザの追加] パネルを開くことができます。
- 12. [ユーザ名] フィールドで、追加するユーザが CC-SG にログインす るために使用する名前を入力します。
- **13.** ユーザが CC-SG にログインできる場合は、[ログイン有効] チェッ クボックスを選択します。
- TACACS+、RADIUS、LDAP、AD など、外部サーバによりユーザ を認証する必要がある場合のみ、[リモート認証] チェックボックス を選択します。リモート認証を使用する場合は、パスワードは必要 ありません。[リモート認証] をオンにした場合、[新しいパスワード] フィールドおよび [パスワード再入力] フィールドは無効になります。
- **15.** [新しいパスワード] と [パスワード再入力] フィールドに、ユーザが CC-SG へのログインに使用するパスワードを入力します。
- [次のログインでパスワードの変更を強制]をオンにすると、このユ ーザは次回ログインしたときに、割り当てられたパスワードの変更 を強制されます。



Ch 4: ガイド付き設定を使用した CC-SG の設定

- **17.** ユーザにパスワードを変更することを強制する頻度を指定する場合 は、[パスワードの定期的な変更を強制] チェックボックスを選択し ます。
- 18. [有効期間 (日数)] フィールドに、変更を強制されるまでにユーザが 同じパスワードを使用できる日数を入力します。
- 19. [電子メール アドレス] フィールドに、ユーザの電子メール アドレ スを入力します。
- 20. [ユーザ グループ] ドロップダウン矢印をクリックし、ユーザを割り 当てるユーザ グループをリストから選択します。
- 21. 別のユーザを追加する場合は、[適用] をクリックしてこのユーザを 保存した後、このセクションの手順を繰り返してユーザを追加しま す。
- 22. ユーザの追加が終わったら、[OK] をクリックします。[User Summary] (ユーザの概要) パネルには、追加したユーザ グループと ユーザのリストが表示されます。オプション。



Ch 5 関連、カテゴリ、エレメント

この章の内容

関連について	
カテゴリとエレメントの追加、網	編集、削除48
CSV ファイルのインポートによ	よるカテゴリとエレメントの追加50

関連について

CC-SG が管理する装置を整理するために役立つ関連を設定できます。 各関連には最上位の組織グループであるカテゴリと、それに関連するエ レメント (カテゴリのサブセット) が含まれます。たとえば、America、 Asia Pacific、Europe のデータ センターにあるターゲット サーバを管 理する Raritan デバイスを使用しているとします。この装置を場所ごと に整理する関連を設定できます。次に、CC-SG インタフェースで選択 したカテゴリ (Location)、および関連エレメント (America、Asia Pacific、および Europe) に応じて、Raritan デバイスとノードを表示す るために CC-SG をカスタマイズできます。CC-SG をカスタマイズし て、お好みに合わせてサーバを整理し、表示できます。

関連の用語

- 関連 カテゴリ、カテゴリのエレメント、およびノード/デバイスの 間の相互関係です。
- カテゴリ エレメントと呼ばれる値セットを含む変数です。たとえば、「America」や「Asia Pacific」などのエレメントを含む Locationがカテゴリです。カテゴリのその他の例に、「Windows」、「Unix」、または「Linux」などのエレメントを含む「OS Type」があります。
- エレメント カテゴリの値です。たとえば、「America」エレメントは「Location」カテゴリに属します。

関連 - カテゴリとエレメントの定義

Raritan デバイスとノードは、カテゴリおよびエレメントごとに整理されます。各カテゴリ/エレメントのペアは、デバイス、ノードまたはその両方に割り当てられます。

カテゴリは、同様のエレメントのグループです。

カテゴリ	エレメント
OS Type	Unix、Windows、Linux



カテゴリ	エレメント
Department	Sales、IT、Engineering

ポリシーはまた、サーバへのユーザ アクセスを制御するためにカテゴ リとエレメントを使用します。たとえば、America 内のサーバへのユー ザ アクセスを制御するポリシーを作成するために、カテゴリ/エレメン トのペア Location/America を使用できます。「*アクセス制御のポリシー* 『197p. 』」を参照してください。

CSV ファイルのインポートによって、カテゴリの複数のエレメントを ノードまたはデバイスに割り当てることができます。

デバイスとノードを CC-SG に追加しながら、これらを事前に定義した カテゴリやエレメントにリンクさせます。ノードおよびデバイス グル ープを作成してそれをポリシーに割り当てる場合、カテゴリとエレメン トを使用して、各グループに属するノードおよびデバイスを定義します

関連の作成方法

関連、ガイド付き設定、および関連マネージャを作成するには、2 つの 方法があります。

- ガイド付き設定により、多くの設定タスクを自動インタフェースに 組み合わせることができます。最初の CC-SG 構成では、ガイド付 き設定を使用することをお勧めします。ガイド付き設定を完了した 後は、いつでも構成を個別に編集できます。「ガイド付き設定を使用 した CC-SG の設定 『38p.』」を参照してください。
- 関連マネージャでは、関連の操作のみを行うことができます。設定 タスクが自動化されることはありません。関連マネージャを使用す ると、ガイド付き設定の使用後に関連を編集することもできます。 「カテゴリとエレメントの追加、編集、削除 『48p. 』」を参照して ください。

カテゴリとエレメントの追加、編集、削除

関連マネージャを使用すると、カテゴリとエレメントを追加、編集、または削除できます。

注: デフォルトで、CC-SG では、デフォルト カテゴリ名 "System Type" および "US States and territories" は英語のままになります。

カテゴリの追加

- カテゴリを追加するには、以下の手順に従います。
- 1. [関連] > [関連] を選択します。



- 2. [追加] をクリックします。[カテゴリの追加] ウィンドウが開きます。
- 3. カテゴリ名を [カテゴリ名] フィールドに入力します。名前の長さに 関する CC-SG のルールについての詳細は、「命名規則 『435p. 』 」を参照してください。
- 4. エレメントのデータ タイプを選択します。
 - 値がテキストとして読み取れる場合は [文字列] を選択します。
 - 値が数値の場合は [整数] を選択します。
- 5. [適用対象] フィールドで、このカテゴリの適用対象として [デバイス]、[ノード]、または [デバイスとノード] を選択します。
- 6. [OK] をクリックして新しいカテゴリを作成します。[カテゴリ名] フィールドに新しいカテゴリ名が表示されます。

カテゴリの削除

カテゴリを削除すると、カテゴリ内に作成されたエレメントがすべて削除されます。画面を更新するかユーザがいったんログアウトしてから再 ログインすると、削除されたカテゴリはノード ツリーまたはデバイス ツリーに表示されなくなります。

- カテゴリを削除するには、以下の手順に従います。
- 1. [関連] > [関連] を選択します。
- 2. [カテゴリ名] ドロップダウン矢印をクリックし、削除するカテゴリ を選択します。
- 3. 画面の [カテゴリ] パネルで [削除] をクリックし、カテゴリを削除 します。[カテゴリの削除] ウィンドウが開きます。
- 4. [はい]をクリックし、カテゴリを削除します。

エレメントの追加

- エレメントを追加するには、以下の手順に従います。
- 1. [関連] > [関連] を選択します。
- 2. [カテゴリ名] ドロップダウン矢印をクリックし、新しいエレメント が追加されるカテゴリを選択します。
- 3. [Add a new row] (新しい行の追加) アイコンをクリックします。
- 空白の行に新しいエレメント名を入力します。名前の長さに関する CC-SG のルールについての詳細は、「命名規則 『435p. 』」を参 照してください。エレメント名では大文字と小文字が区別されます。
- 5. [OK] をクリックして変更を保存します。



CSV ファイルのインポートによるカテゴリとエレメントの追加

値が含まれている CSV ファイルをインポートすることによって、カテ ゴリとエレメントを CC-SG に追加できます。カテゴリとエレメントを インポートおよびエクスポートするには、ユーザ セキュリティ管理権 限および CC の設定と制御権限が必要です。

カテゴリとエレメントの CSV ファイルの要件

カテゴリとエレメントの CSV ファイルでは、カテゴリ、その関連エレ メント、タイプ、および適用対象 (デバイス、ノード、または両方) が 定義されています。

- すべての CATEGORY レコードと CATEGORYELEMENT レコー ドは関連しています。CATEGORY レコードには、1 つ以上の CATEGORYELEMENT レコードが必要です。
- CATEGORYELEMENT レコードには、対応する CATEGORY レコ ードは必要ありませんが、その CATEGORY がすでに CC-SG に 存在する場合に限ります。たとえば、既存のカテゴリにエレメント を追加する場合は、その新しいエレメントが属するカテゴリを再定 義するために行を追加する必要はありません。
- 有効な CSV ファイルの作成に必要なすべてのタグとパラメータが 含まれているコメントを参照するには、CC-SG からファイルをエ クスポートします。「カテゴリとエレメントのエクスポート『52p. 』 」を参照してください。
- すべての CSV ファイルの追加要件を満たします。「CSV ファイル の共通要件 『412p. 』」を参照してください。

列 1	列 2	列 3	列 4	列 5
ADD	CATEGORY	カテゴリ名	タイプ	適用
			値:	値:
			 Integer 	■ ノード
			 String 	■ デバイス
			デフォルトは	 Both
			String です。	デフォルトは
				Both です。

CSV ファイルにカテゴリを追加する場合

CSV ファイルにエレメントを追加する場合



列 1	列 2	列 3	列 4
ADD	CATEGORYELEMENT	カテゴリ名	エレメント名

カテゴリとエレメントの CSV ファイルの例

ADD, CATEGORY, OS, String, Node

ADD, CATEGORYELEMENT, OS, UNIX

ADD, CATEGORYELEMENT, OS, WINDOWS

ADD, CATEGORYELEMENT, OS, LINUX

ADD, CATEGORY, Location, String, Device

ADD, CATEGORYELEMENT, Location, Aisle 1

ADD, CATEGORYELEMENT, Location, Aisle 2

ADD, CATEGORYELEMENT, Location, Aisle 3

カテゴリとエレメントのインポート

CSV ファイルを作成したら、エラーがないかどうかを確認してからイ ンポートします。

重複するレコードはスキップされ、追加されません。

▶ CSV ファイルをインポートするには、以下の手順に従います。

- 1. [管理]>[インポート]>[カテゴリのインポート]を選択します。
- [参照] をクリックし、インポートする CSV ファイルを選択します。
 [開く] をクリックします。
- 3. [確認] をクリックします。[分析レポート] 領域にファイルの内容が 表示されます。
 - ファイルが有効でない場合は、エラー メッセージが表示されます。[OK] をクリックし、ページの [問題] 領域でファイルに関する問題の説明を参照します。[ファイルに保存] をクリックして問題リストを保存します。CSV ファイルを修正し、再度検証します。「CSV ファイルの問題のトラブルシューティング 『414p. 』」を参照してください。
- 4. [インポート] をクリックします。
- 5. [アクション] 領域でインポート結果を確認します。正常にインポートされたアイテムは、緑色のテキストで表示されます。インポートに失敗したアイテムは、赤いテキストで表示されます。重複するアイテムがすでに存在するか、またはすでにインポートされているためにインポートに失敗したアイテムも赤いテキストで表示されます



6. インポート結果の詳細を参照するには、監査証跡レポートを確認し ます。「インポートに関する監査証跡エントリ 『413p. 』」を参照 してください。

カテゴリとエレメントのエクスポート

エクスポート ファイルの一番上には、ファイル内の各アイテムを説明 するコメントが含まれています。コメントは、インポートするファイル を作成するための指示として使用できます。

- カテゴリとエレメントをエクスポートするには、以下の手順に従い ます。
- 1. [管理]>[エクスポート]>[カテゴリのエクスポート]を選択します。
- 2. [ファイルにエクスポート] をクリックします。
- 3. ファイルの名前を入力し、保存する場所を選択します。
- 4. [保存] をクリックします。

ファイルを初めて Excel で保存するときに、[名前を付けて保存] を 選択し、ファイルの種類として [CSV] を選択する必要があります。 それ以降は、ファイルは CSV として保存されます。

ファイルの種類を正しく設定しないと、ファイルは破損し、インポートに使用できません。



Ch 6 デバイス、デバイス グループ、ポート

他の Raritan デバイスに接続された Raritan 電源タップ デバイスを CC-SG に追加する場合、「*管理対象電源タップ*『105p. 』」を参照し てください。

注: iLO/RILOE デバイス、IPMI デバイス、Dell DRAC デバイス、IBM RSA デバイス、またはその他の Raritan 以外のデバイスを設定する場 合は、[ノードの追加] メニューを使用し、これらの項目をインタフェー スとして追加します。「ノード、ノード グループ、インタフェース 『 114p. 』」を参照してください。

この章の内容

デバイスの表示	54
デバイスの検索	
デバイスの検出	
デバイスの追加	60
デバイスの編集	64
KX2 デバイス用の HTTP ポートおよび HTTPS ポートの変更.	64
電源タップ デバイスまたは Dominion PX デバイスの編集	65
デバイス プロファイルへの注意の追加	65
デバイス プロファイルへの場所と連絡先の追加	66
デバイスの削除	66
ポートの設定	67
ポートの編集	69
ポートの削除	70
KX2 に接続されたブレード シャーシ デバイスの設定	70
ブレード サーバ ポートの標準 KX2 ポートへのリストア	77
デバイスの関連、場所、および連絡先の一括コピー	77
KX2 2.3 以降に接続するアナログ KVM スイッチの設定	78
デバイス グループ マネージャ	81
CSV ファイルのインポートによるデバイスの追加	
デバイスのアップグレード	93
デバイス設定のバックアップ	94
デバイス設定のリストア	
デバイス設定のコピー	
デバイスの再起動	100
デバイスの ping	100
CC-SG のデバイス管理の一時停止	100
デバイスの管理の再開	101
スケジュールされたタスクを使用したデバイス管理の一時停止と	再開101
デバイス パワー マネージャ	102



Ch 6: デバイス、デバイス グループ、ポート

デバイスの管理ページの起動	103
ユーザの切断	
Paragon II システム デバイスへの専用アクセス	

デバイスの表示

[デバイス] タブ

[デバイス] タブをクリックすると、CC-SG の管理下にあるすべてのデ バイスが表示されます。



各デバイスの構成済みポートは、それが属するデバイスの下にネストさ れます。リスト内で構成済みのポートを持つデバイスは、+ 記号が表示 されます。+ または - をクリックすると、ポートのリストが拡張するか 、または隠れます。

デバイスとポートのアイコン

デバイス ツリーでは、区別しやすいように KVM、シリアル、電源のデ バイスとポートを別々のアイコンで表します。デバイス ツリーのアイ コンにマウス ポインタを合わせると、デバイスまたはポートに関する 情報のツール ヒントが表示されます。

アイコン	意味
	デバイスが利用可能


Ch 6: デバイス、デバイス グループ、ポート

アイコン	意味
9	KVM ポートが利用できない状態、また は接続されていない状態
5	KVM ポートが非アクティブ
==	シリアル ポートが利用可能
	シリアル ポートが利用不可能
	ゴースト ポート (ゴースト モードの 詳細は、Raritan の『Paragon II ユーザ マニュアル』を参照してください。
4	デバイスが停止した状態
æ	デバイスが利用不可能
(i)	電源タップ
©	コンセント ポート
₩.	ブレード シャーシが利用可能
-	ブレード シャーシが利用不可能
l.	ブレード サーバが利用可能
l.	ブレード サーバが利用不可能

ポート並び替えオプション

[デバイス] タブで、設定済みポートは親デバイスの下に分類されていま す。ポートの並べ替え順序は変更できます。ステータスによって並べ替 えたポートは、接続ステータス グループ内ではアルファベット順に配 列されます。デバイスも同様に並べられます。

- [デバイス] タブでポートを並べ替えるには、以下の手順に従います。
- 1. [デバイス]>[ポート並び替えオプション]を選択します。



名前のアルファベット順か、可用性ステータスを基準にするか、またはポート番号順にデバイス内のポートを整列するには、[ポート名でソート]、[ポート ステータスでソート]、または [ポート番号でソート]を選択します。

注: KVM スイッチが統合されていないブレード サーバの場合 (HP BladeSystem サーバなど)、その親デバイスは、KX2 デバイスではなく 、CC-SG が作成する仮想ブレード シャーシです。これらのサーバは、 仮想ブレード シャーシ デバイス内でのみ並べ替えられます。これらの ブレード サーバ ポートを標準 KX2 ポートにリストアしない限り、他 の KX2 ポートと一緒に並べ替えられて表示されることはありません。 「ブレード サーバ ポートの標準 KX2 ポートへのリストア 『77 p. 』 」を参照してください。



[デバイス プロファイル] 画面

[デバイス] タブでデバイスを選択すると、[デバイス プロファイル] 画 面が開き、選択したデバイスに関する情報が表示されます。

デバイスが使用不可の場合、[デバイス プロファイル] 画面の情報は読 み取り専用です。使用不可のデバイスは、削除できます。「デバイスの 削除 『66p. 』」を参照してください。

[デバイス プロファイル] 画面には、デバイスに関する情報を含むタブ があります。

🕨 [関連] タブ

[関連] タブには、ノードに割り当てられたすべてのカテゴリとエレメン トが含まれます。関連を変更するには、選択を変更します。「*関連、カ テゴリ、エレメント* **『47**p. 』」を参照してください。

▶ [場所 & 連絡先] タブ

[場所 & 連絡先] タブには、デバイスに対して作業を行っている際に必要になる場合があるデバイスの場所と連絡先に関する情報 (電話番号など) が含まれます。フィールド内の情報は、新しい情報を入力して変更できます。「デバイス プロファイルへの場所と連絡先の追加 『66p. 』」を参照してください。

🕨 [メモ] タブ:

[メモ] タブには、デバイスに関するメモを他のユーザが参照できるよう に残しておくためのツールがあります。タブ内のすべてのメモには、メ モを追加した時点の日付、ユーザのユーザ名と IP アドレスが表示され ます。

デバイス、ポート、ノードの管理権限がある場合は、[クリア] をクリッ クすると、ノード プロファイルからすべてのメモをクリアすることが できます。

「*デバイス プロファイルへのメモの追加* 『**65**p. の"*デバイス プロファ イルへの注意の追加*"参照 』」を参照してください

🕨 [ブレード] タブ

IBM BladeCenter などのブレード シャーシ ノードには、[ブレード] タ ブが含まれます。[ブレード] タブには、ブレード シャーシに常駐する ブレード サーバについての情報が表示されます。

ブレード情報の表示に加えて、このタブでは、未設定ブレード サーバ を設定できます。このためには、サーバに対応するチェックボックスを 選択します。



「*ブレード シャーシ デバイスのスロットの設定* 『**73**p. 』」を参照し てください。

トポロジー表示

トポロジー表示では、設定内のすべての接続アプライアンスの構造上の 設定が表示されます。

トポロジー表示は、閉じるまで、デバイス選択時に通常表示されるデバイス プロファイル画面に代わって表示されます。

- ▶ トポロジー表示を開くには、以下の手順に従います。
- 1. [デバイス] タブをクリックし、トポロジーが表示されるデバイスを 選択します。
- 2. [デバイス]>[デバイス マネージャ]>[トポロジー表示] を選択しま す。選択したデバイスの [トポロジー表示] が表示されます。
 - + または をクリックすることで、表示を広げたり、折りたたんだりします。

[デバイス] タブの右クリック オプション

[デバイス] タブでデバイスまたはポートを右クリックすると、選択した デバイスまたはポートで使用可能なコマンドのメニューを表示できます。

デバイスの検索

[デバイス] タブでは、ツリー内のデバイスを検索できます。検索では、 結果としてデバイスのみが返されます。ポート名は含まれません。検索 方法は、[プロファイル] で設定できます。「デフォルトの検索設定の変 更『194p. 』」を参照してください。

- デバイスを検索するには、以下の手順に従います。
- [デバイス] タブの下部にある [デバイスの検索] フィールドに検索文 字列を入力し、Enter キーを押します。
- 検索文字列では、ワイルドカードがサポートされます。「検索用ワイ ルドカード 『58p. 』」を参照してください。

検索用ワイルドカード

ワイルドカード	説明
?	任意の文字を示す。
[-]	範囲内の文字を示す。



Ch 6: デバイス、デバイス グループ、ポート

ワイルドカード

か1 文字以上の文字を示す。

ワイルドカードの例

例	説明
KX?	「KX1」や「KXZ」はヒットしま すが、「KX1Z」はヒットしません 。
KX*	「KX1」、「KX」、「KX1Z」がヒ ットします。
KX[0-9][0-9]T	「KX95T」、「KX66T」はヒット しますが、「KXZ」と「KX5PT」 はヒットしません。

デバイスの検出

[デバイス検出] により、ネットワーク上のすべてのデバイスの検索が開始します。検出したデバイスがまだ管理されていない場合は、そのデバイスを CC-SG に追加できます。

説明

デバイスを検出するには、以下の手順に従います。

- 1. [デバイス]>[デバイス検出]を選択します。
- [開始アドレス] フィールドと [終了アドレス] フィールドに、デバイ スを検出する IP アドレスの範囲を入力します。[終了アドレス] に は、[開始アドレス] より大きい値を設定します。この範囲に適用す るマスクを指定します。マスクを指定しない場合、255.255.255.255 というブロードキャスト アドレスが送信され、ローカルのネットワ ーク全体にブロードキャストされます。サブネット間のデバイスを 検出するには、マスクを指定する必要があります。
- 3. CC-SG と同じサブネットにあるデバイスを検索する場合は、[ブロ ードキャスト検出] をオンにします。さまざまなサブネット上のデ バイスを検出するには、[ブロードキャスト検出]の選択を解除しま す。
- 特定の種類のデバイスを検索するには、デバイスの種類のリストで 対象となるデバイスを選択します。デフォルトでは、すべてのデバ イス タイプが選択されます。Ctrl キーとマウスクリックを使って、 1 つかそれ以上のデバイス タイプを選択します。
- 5. パワー制御機能を提供するターゲットを検索する場合は、[IPMI エ ージェントを含める] チェックボックスを選択します。



- 6. [検出] をクリックして検索を開始します。検出中に検出処理を中止 するには、[停止] をクリックできます。検出されたデバイスがリス トに表示されます。
- 検出された 1 つ以上のデバイスを CC-SG に追加するには、リストからデバイスを選択し、[追加] をクリックします。[デバイスの追加] 画面が開き、入力済みのデータの一部が表示されます。
 追加するデバイスを複数選択した場合、画面下部にある [前へ] および [スキップ] をクリックして、追加するデバイスについて、[デバイスの追加] 画面を表示できます。
- 8. [デバイスの追加] ページは、デバイス タイプによって異なります。 CC-SG が検出した各デバイス タイプの追加手順を参照してください。
 - KVM またはシリアル デバイスについては、「KVM またはシリアル デバイスの追加 『61p. 』を参照してください。
 - 電源タップについては、「電源タップ デバイスの追加 『63p. 』 」を参照してください。
 - IP ネットワーク上の Dominion PX 電源タップについては、「 Dominion PX デバイスの追加 『63p. 』」を参照してください
- [適用] をクリックすると検出されたデバイスが追加され、引き続き 次のデバイスを追加できます。[OK] をクリックすると、現在のデバ イスを追加し、デバイスの追加処理が終了します。

デバイスの追加

ポートの構成、またはポートに接続されたノードにアクセス可能なイン タフェースの追加を行うには、デバイスを CC-SG に追加する必要があ ります。[デバイスの追加] 画面を使用し、プロパティがわかっていて CC-SG に提供できるデバイスを追加します。追加するデバイスを検索 するには、[デバイス検出] オプションを使用します。「デバイス検出『 59p. の"デバイスの検出"参照』」を参照してください。

他の Raritan デバイスに接続された Raritan 電源タップ デバイスを CC-SG に追加する場合、「*管理対象電源タップ* 『105p. 』」を参照し てください。

- ▶ CC-SG にデバイスを追加するには、以下の手順に従います。
- 1. [デバイス]>[デバイス マネージャ]>[デバイスの追加] を選択します。
- [デバイス タイプ] ドロップダウン矢印をクリックし、追加するデバ イスのタイプをリストから選択します。デバイス タイプによって、 [デバイスの追加] ページの表示内容が若干異なります。



- KVM またはシリアル デバイスの追加手順については、「KVM また はシリアル デバイスの追加 『61p. 』」を参照してください。
- 電源タップデバイスの追加手順については、「電源タップデバイスの追加 『63p. 』」を参照してください。
- Dominion PX デバイスの追加手順については、「Dominion PX デバ イスの追加 『63p. 』」を参照してください。

KVM またはシリアル デバイスの追加

ー部の KVM およびシリアル デバイスでは 256 ビット AES 暗号化を サポートします。CC-SG でも、リリース 4.1 からこの暗号化をサポー トしています。デバイスの暗号化モードがデフォルトの「自動ネゴシエ ーション」に設定されている場合、デバイスは、CC-SG とのネゴシエー ションによって、CC-SG で機能する適切な暗号化レベルを選択します

- デバイス名を [デバイス名] フィールドに入力します。名前の長さに 関する CC-SG のルールについての詳細は、「命名規則 『435p. 』 」を参照してください。
- デバイスの IP アドレスまたはホスト名を [デバイス IP またはホ スト名] フィールドに入力します。ホスト名のルールについては、 「*用語/略語* 『2p. 』」を参照してください。
- デバイスとの通信に使用する TCP 通信ポートの番号を [Discovery Port(検出ポート)] フィールドに入力します。最大 5 桁の数値 (1 ~ 65535) を入力できます。大半の Raritan デバイスのデフォルト ポート番号は 5000 です。
- このデバイスへのログインに使用する名前を [ユーザー名] フィール ドに入力します。ユーザは、管理機能にアクセスできる必要があり ます。
- このデバイスにアクセスするためのパスワードを [パスワード] フィ ールドに入力します。ユーザは、管理機能にアクセスできる必要が あります。
- 新しいデバイスと CC-SG との間でのタイムアウトまでの時間を、[ハートビート タイムアウト (秒)] フィールドに秒単位で入力します。
- Dominion SX デバイスまたは Dominion KX2 バージョン 2.2 以降 のデバイスを追加する場合、[デバイスの直接アクセスを許可] チェ ックボックスを使用すると、デバイスが CC-SG の管理下にある場 合でも、デバイスからターゲットへの直接アクセスを可能にするこ とができます。
- 8. このデバイスの短い説明を [説明] フィールドに入力します。オプション。
- このデバイスのすべてのポートを [デバイス] タブに自動的に追加し、 (ノード] タブでこのデバイスの各ポートのノードを作成する場合は、[すべてのポートの設定] チェックボックスを選択します。



- 対応するノードおよびポートは、一致する名前により設定されます。
- 各ポートに対して新しいノードが作成され、さらにそのノードのアウトオブバンドインタフェースが作成されます(ブレードシャーシノードおよび汎用のアナログKVMスイッチノードは除きます)。
- ブレード シャーシまたは汎用のアナログ KVM スイッチの IP アドレスまたはホスト名が KX2 で入力されているかどうかに 応じて、KX2 ポートに接続されたブレード シャーシ アプライ アンスまたは汎用のアナログ KVM スイッチのノードが作成さ れる場合とされない場合があります。『KX II ユーザ ガイド』を 参照してください。Web ブラウザ インタフェースは、デフォ ルトで CC-SG のブレード シャーシ ノードに割り当てられま す。
- KX2 ポートに直接接続されるブレード サーバ用のブレード ポ ート グループが KX 2 で適切に設定されている場合は、それら のブレード サーバの [デバイス] タブに仮想ブレード シャーシ デバイスが作成されます。『KX II ユーザ ガイド』を参照してく ださい。
- 10. このデバイスとそれに接続するノードの説明および整理方法を修正 するために、カテゴリとエレメントのリストを設定できます。「*関連* 、カテゴリ、エレメント 『47p. 』」を参照してください。
- 11. リストに表示されている [カテゴリ] ごとに、[エレメント] ドロップ ダウン メニューをクリックし、デバイスに適用するエレメントをリ ストから選択します。不要な [カテゴリ] については、それぞれの [エレメント] フィールドで空白の項目を選択します。

デバイスに加えて関連ノードにもエレメントを割り当てる場合 、[ノードに適用] チェックボックスを選択します。

- 使用する [カテゴリ] または [エレメント] 値が表示されない場合は、
 (関連] メニューから追加できます。「*関連、カテゴリ、エレメント* 『47p. 』」を参照してください。
- このデバイスの設定が完了して、[適用] をクリックすると、このデバイスが追加され、新しいブランクの [デバイスの追加] 画面が開きます。この画面で引き続きデバイスを追加することができます。
 [OK] をクリックすると、このデバイスが追加されますが、新たに [デバイスの追加] 画面は表示されません。
- デバイスのファームウェア バージョンに CC-SG との互換性がな い場合、メッセージが表示されます。[はい] をクリックし、CC-SG にデバイスを追加します。デバイスのファームウェアは、CC-SG への追加後にアップグレードできます。「デバイスのアップグレード 『93p.』」を参照してください。



電源タップ デバイスの追加

電源タップ デバイスを CC-SG に追加するプロセスは、電源タップが 物理的に接続されている Raritan デバイスによって異なります。「*管理* **対象電源タップ**『105p. 』」を参照してください。

別の Raritan デバイスに接続されていない Dominion PX を追加する場 合は、「*Dominion PX デバイスの追加* **『63**p. **』**」を参照してください 。

Dominion PX デバイスの追加

Dominion PX は、ご使用の IP ネットワークのみに接続される電源タッ プです。Dominion PX デバイスは、別の Raritan デバイスによって管 理されません。別の Raritan デバイスによって管理される電源タップを 追加する場合、手順が異なります。「*管理対象電源タップ*『105p.』」 を参照してください。

- [デバイス名] フィールドにデバイス名を入力します。名前の長さに 関する CC-SG のルールについての詳細は、「命名規則 『435p. 』 」を参照してください。
- [IP アドレス/ホスト名] フィールドにデバイスの IP アドレスまた はホスト名を入力します。ホスト名のルールについては、「用語/略 語『2p.』」を参照してください。
- このデバイスへのログインに使用する名前を [ユーザー名] フィール ドに入力します。ユーザは、管理機能にアクセスできる必要があり ます。
- このデバイスにアクセスするためのパスワードを [パスワード] フィ ールドに入力します。ユーザは、管理機能にアクセスできる必要が あります。

警告: ユーザ名またはパスワードが変更された場合、CC-SG は Dominion PX デバイスと接続できなくなります。PX でのパスワー ドを変更する場合は、CC-SG で PX デバイスのパスワードを変更 する必要があります。「デバイスの編集 『64p. 』」を参照してくだ さい。

- 5. このデバイスの短い説明を [説明] フィールドに入力します。オプション。
- 6. [すべてのアウトレットを設定] チェックボックスを選択すると、こ の Dominion PX のすべてのコンセントが自動的に [デバイス] タブ に追加されます。
- [カテゴリ] および [エレメント] のリストは、このノードをわかりや すく整理するために設定することができます。
 - リストされたカテゴリごとに、デバイスに適用するエレメント をリストから選択します。不要な [カテゴリ] については、それ ぞれの [エレメント] フィールドで空白の項目を選択します。



- 使用する [カテゴリ] または [エレメント] 値が表示されない場合は、その他の値を追加できます。「*関連、カテゴリ、エレメン* ト 『47p. 』」を参照してください。
- このデバイスの設定が完了して、[適用] をクリックすると、このデバイスが追加され、新しいブランクの [デバイスの追加] 画面が開きます。この画面で引き続きデバイスを追加することができます。
 [OK] をクリックすると、このデバイスが追加されますが、新たに [デバイスの追加] 画面は表示されません。

デバイスの編集

デバイスを編集して、その名前とプロパティを変更できます。これには PX デバイスのユーザ名とパスワードの変更も含まれます。

- ▶ デバイスを編集するには、以下の手順に従います。
- 1. [デバイス] タブをクリックし、編集するデバイスを選択します。
- 2. [デバイス プロファイル] ページで、 必要に応じてパラメータを変 更します。
- 3. [OK] をクリックして変更を保存します。

KX2 デバイス用の HTTP ポートおよび HTTPS ポートの変更

KX2 デバイス (バージョン 2.3 以降) 用の HTTP ポートおよび HTTPS ポートを変更するには、デバイス プロファイルを編集します。 KX2 デバイスに新しいポート番号が反映されます。

新しいポートは、CC-SG と KX2 デバイス間の通信、または AKC や VKC のようなクライアント アプリケーションと KX2 デバイスとの直 接通信に使用されます。新しいポート番号は、ユーザのクライアント コンピュータと CC-SG 間の通信には使用されません。

KX2 デバイス用の HTTP ポートおよび HTTPS ポートを変更する には、以下の手順に従います。

注: KX2 バージョン 2.3 以降だけに適用されます。

- 1. [デバイス] タブをクリックし、編集するデバイスを選択します。
- 2. [デバイス プロファイル] ページで、 HTTP ポートおよび HTTPS ポートの新しい値を入力します。
- 3. [OK] をクリックします。



電源タップ デバイスまたは Dominion PX デバイスの編集

管理対象電源タップ デバイスまたは Dominion PX デバイスを編集する と、その名前およびプロパティを変更し、コンセント設定ステータスを 表示できます。

- ▶ 電源タップ デバイスを編集するには、以下の手順に従います。
- 1. [デバイス] タブをクリックし、編集する電源タップ デバイスを選択 します。
- この画面で、該当するフィールドに新しいデバイスのプロパティを 入力します。必要に応じて、デバイスに関連するカテゴリとエレメ ントを編集します。
- 3. [アウトレット] タブをクリックして、この電源タップのすべてのコ ンセントを表示します。
- 4. コンセントがノードに関連付けられている場合、[ノード]のハイパ ーリンクをクリックするとノード プロファイルが開きます。
- コンセントがノードに関連付けられている場合、コンセントを選択して [パワー制御] をクリックすると、関連するノードの [パワー制御] 画面が開きます。
- 6. コンセントを削除するには、コンセント名の横のチェックボックス を選択解除します。
- 7. コンセントを設定するには、コンセント名の横のチェックボックス をオンにします。
- 8. [OK] をクリックして変更を保存します。デバイスが変更されるとメ ッセージが表示されます。

デバイス プロファイルへの注意の追加

[Notes](注意)タブを使用すると、他のユーザの参照用にデバイスに関する注意を追加できます。タブ内のすべてのメモには、メモを追加した時点の日付、ユーザのユーザ名と IP アドレスが表示されます。

デバイス、ポート、ノードの管理権限がある場合は、[Notes](注意)タブに表示されるすべての注意をクリアすることができます。

- デバイス プロファイルに注意を追加するには、以下の手順に従います。
- [デバイス] タブでデバイスを選択します。[デバイス プロファイル] ページが開きます。
- 2. [Notes] (注意) タブをクリックします。
- 3. 注意を [New Notes] (新しい注意) フィールドに入力します。
- 4. [追加] をクリックします。注意が [Notes] (注意) リストに表示され ます。



- すべての注意をクリアするには、以下の手順に従います。
- 1. [Notes] (注意) タブをクリックします。
- 2. [Clear Notes] (注意のクリア) をクリックします。
- 3. [はい] をクリックして確認します。すべての注意が [Notes] (注意) タブから削除されます。

デバイス プロファイルへの場所と連絡先の追加

デバイスの場所に関する詳細およびデバイスを管理または使用する人物 の連絡先情報を入力します。

- デバイス プロファイルに場所および連絡先を追加するには、以下の 手順に従います。
- [デバイス] タブでデバイスを選択します。[デバイス プロファイル] ページが開きます。
- 2. [Location & Contacts] (場所&連絡先) タブをクリックします。
- 3. 場所情報を入力します。
 - Department:最大 64 文字です。
 - Site:最大 64 文字です。
 - Location:最大 128 文字です。
- 4. 連絡先情報を入力します。
 - 主連絡先名と二次連絡先名:最大 64 文字です。
 - 電話番号と携帯電話番号:最大 32 文字です。
- 5. [OK] をクリックして変更を保存します。

デバイスの削除

デバイスを削除して CC-SG 管理からデバイスを除外できます。

重要:デバイスを削除すると、そのデバイスに対して構成されたすべての ポートが削除されます。そのポートに関連するすべてのインタフェース がノードから削除されます。該当ノードに他のインタフェースが存在し ない場合、ノードも **CC-SG** から削除されます。

- ▶ デバイスを削除するには、以下の手順に従います。
- 1. [デバイス] タブをクリックし、削除するデバイスを選択します。
- 2. [デバイス]>[デバイス マネージャ]>[デバイスの削除] を選択します。
- 3. [OK] をクリックして、デバイスを削除します。デバイスが削除され るとメッセージが表示されます。



ポートの設定

デバイスの追加時に [すべてのポートの設定] を選択してデバイスのす べてのポートを自動追加しなかった場合は、[ポートの設定] 画面を使用 してデバイス上のポートを個別またはまとめて CC-SG に追加します。 ポートを設定すると、ポートごとに CC-SG でノードが作成され、デフ ォルトのインタフェースも作成されます。「ポートの設定により作成さ れるノード『68p. 』」を参照してください。

シリアル ポートの設定

- シリアル ポートを設定するには、以下の手順に従います。
- 1. [デバイス] タブをクリックし、シリアル デバイスを選択します。
- [デバイス]>[ポート マネージャ]>[ポートの設定] を選択します。
 列のヘッダをクリックすると、ポートがその属性によって昇順に並べ替えられます。ヘッダを再度クリックすると、ポートが降順に並び替わります。
- 3. 設定するシリアル ポートに対応する [設定] ボタンをクリックしま す。
- 【ポート名】フィールドに名前を入力します。使いやすくするため、 ポートにはポートに接続するターゲットにちなんだ名前を付けます 。名前の長さに関する CC-SG のルールについての詳細は、「命名 規則 『435p. 』」を参照してください。
- このポートからのアウト オブ バンド インタフェースで新しいノー ドを作成するために、ノード名を [ノード名] フィールドに入力しま す。使いやすくするため、ノードにはポートに接続するターゲット にちなんだ名前を付けます。つまり、[ポート名] フィールドと [ノ ード名] フィールドに同じ名前を入力します。
- [アクセス アプリケーション] ドロップダウン メニューをクリック し、このポートへの接続時に使用するアプリケーションをリストか ら選択します。ブラウザに基づいて正しいアプリケーションを CC-SG で自動的に選択できるようにするには、[自動検出] を選択 します。
- 7. [OK] をクリックして、ポートを追加します。

KVM ポートの設定

- ▶ KVM ポートを設定するには、以下の手順に従います。
- 1. [デバイス] タブをクリックし、KVM デバイスを選択します。
- 2. [デバイス]>[ポート マネージャ]>[ポートの設定] を選択します。



- 列のヘッダをクリックすると、ポートがその属性によって昇順に並べ替えられます。ヘッダを再度クリックすると、ポートが降順に並び替わります。
- 3. 設定する KVM ポートに対応する [設定] ボタンをクリックします。
- ポート名を [ポート名] フィールドに入力します。使いやすくするため、ポートにはポートに接続するターゲットにちなんだ名前を付けます。名前の長さに関する CC-SG のルールについての詳細は、「 命名規則 『435p. 』」を参照してください。
- このポートからのアウト オブ バンド インタフェースで新しいノー ドを作成するために、ノード名を [ノード名] フィールドに入力しま す。使いやすくするため、ノードにはポートに接続するターゲット にちなんだ名前を付けます。つまり、[ポート名] フィールドと [ノ ード名] フィールドに同じ名前を入力します。
- [アクセス アプリケーション] ドロップダウン メニューをクリック し、このポートへの接続時に使用するアプリケーションをリストか ら選択します。ブラウザに基づいて正しいアプリケーションを CC-SG で自動的に選択できるようにするには、[自動検出] を選択 します。
- 7. [OK] をクリックして、ポートを追加します。

ポートの設定により作成されるノード

デバイスのポートを設定すると、ポートごとにノードが自動的に作成さ れます。インタフェースもノードごとに作成されます。

ノードが自動的に作成されると、関連付けられたポートと同じ名前が付けられます。このノード名がすでに存在する場合は、ノード名に拡張部分が追加されます。たとえば、Channel1(1)などです。拡張部分は、数字をカッコで囲んだものです。この拡張部分は、ノード名の文字数には含まれません。ノード名を編集した場合、新しい名前は最大文字数によって制限されます。「命名規則『435p.』」を参照してください。



ポートの編集

ポートを編集すると、ポート名、アクセス アプリケーション、シリア ル ポート設定など、さまざまなパラメーターを変更できます。変更可 能な設定は、ポート タイプおよびデバイス タイプによって異なります

注: [管理の起動] を使用して KX2 の Web インタフェースを使用する ことで、Dominion KX2 のポート設定を編集することもできます。

KVM を編集するか、シリアル ポート名またはアクセス アプリケ ーションを編集するには、以下の手順に従います。

一部のポートは 1 つのアクセス アプリケーションしかサポートしない ので、アクセス アプリケーション設定は変更できません。

- 1. [デバイス] タブをクリックし、編集するポートを選択します。
- 2. 必要に応じて、ポートの新しい名前を [ポート名] フィールドに入力 します。
- [アクセス アプリケーション] ドロップダウン メニューをクリック し、このポートへの接続時に使用するアプリケーションをリストか ら選択します。ブラウザに基づいて正しいアプリケーションを CC-SG で自動的に選択できるようにするには、[自動検出] を選択 します。
- 4. [OK] をクリックして変更を保存します。
- KSX2 または KSX シリアル ポートの設定 (ボーレート、フロー制御、パリティ/データ ビットなど)を変更するには、以下の手順に従います。
- 1. [デバイス] タブをクリックして、編集するシリアル ポートを選択す るか、単に編集するポートを含むデバイスを選択します。
- 2. [デバイス]>[デバイス マネージャ]>[管理の起動] を選択します。 デバイスの管理ページが開きます。
- 3. [ポート設定] をクリックします。
- 4. 編集するシリアル ポートをクリックします。
- 5. ポート設定を編集します。
- [OK] をクリックして変更を保存します。管理ページを閉じて、 CC-SG に戻ります。



- SX シリアル ポート設定 (ボーレート、フロー制御、パリティ/デー タ ビットなど) を変更するには、以下の手順に従います。
- [デバイス] タブをクリックし、編集するポートを選択します。[ポート プロファイル]ページが開きます。
- 2. ポート設定を編集します。
- 3. [OK] をクリックして変更を保存します。

ポートの削除

ポートを削除し、デバイスからポート エントリを削除します。ポート が使用不可の場合、[ポート プロファイル] 画面の情報は読み取り専用 です。使用不可のポートは、削除できます。

重要: ノードに関連するポートを削除すると、そのポートにより提供され る関連アウト オブ バンド KVM またはシリアル インタフェースがノ ードから削除されます。ノードに他のインタフェースが存在しなければ、 ノードも CC-SG から削除されます。

- ポートを削除するには、以下の手順に従います。
- 1. [デバイス] タブをクリックし、削除するポートを持つデバイスを選 択します。
- 2. [デバイス]>[ポート マネージャ]>[ポートの削除] を選択します。
- 3. 選択するポートのチェックボックスを選択します。
- 4. [OK] をクリックして、選択したポートを削除します。ポートが削除 されるとメッセージが表示されます。

KX2 に接続されたブレード シャーシ デバイスの設定

ブレード シャーシの概要

ブレード シャーシ デバイスには、2 つのタイプがあります。1 つは KVM スイッチが統合されたタイプで、これは IP 対応の KVM スイッ チとして機能できます。もう 1 つはこのスイッチが統合されていない タイプです。



KVM スイッチが統合されたブレード シャーシ

KVM スイッチが統合されたブレード シャーシ (Dell PowerEdge および IBM BladeCenter シリーズなど) は、CIM を介して KX2 に接続されます。そのシャーシでは、1 つだけの CIM を使用してすべてのブレード サーバにアクセスするので、ユーザが 1 つのブレード サーバにアクセスしている場合、他のユーザが使用できるパスは残っていません。

CC-SG ですべての KX2 ポートを設定する場合は、KX2 デバイスに接続されているブレード シャーシを設定します。「ブレード シャーシ デバイスの追加『71p.』」を参照してください。このタイプのブレード シャーシ内のブレード サーバはまだ設定されていないので、後でブレード サーバを設定する必要があります。「ブレード シャーシ デバイスの スロットの設定 『73p.』」を参照してください。

KVM スイッチが統合されていないブレード シャーシ

KVM スイッチが統合されていないブレード シャーシの場合 (HP BladeSystem シリーズなど)、各ブレード サーバが CIM を介してそれ ぞれ KX2 に接続できます。シャーシ内のブレード サーバごとにアクセ ス用の CIM があるので、あるユーザが 1 つのブレード サーバにアク セスしている場合でも、他のユーザは他のブレード サーバにアクセス できます。

CC-SG ですべての KX2 ポートを設定する場合は、KX2 デバイスに接 続されているブレード サーバを設定します。KX2 デバイスでこれらの ブレード サーバのブレード ポート グループが適切に構成されている 場合は、CC-SG によって、これらのブレード サーバのコンテナとして 、KX2 ポート レベルで仮想ブレード シャーシが作成されます。「ブレ ード シャーシ デバイスの追加 『71p.』」を参照してください。それ 以外の場合、これらのブレード サーバは、CC-SG の [デバイス] タブ に標準 KX2 ポートとして表示されます。

ブレード シャーシ デバイスの追加

ブレード シャーシ デバイスを追加する手順は、ブレード シャーシの タイプによって異なります。

ブレード シャーシ デバイスは、[デバイス] タブに常に 2 つの名前で 表示されます。カッコが付いていない名前は KX2 デバイスから取得さ れたもので、カッコ内の名前は CC-SG に保存されているシャーシ名で す。

KVM スイッチが統合されているブレード シャーシ デバイスを追加するには、以下の手順に従います。

1. KX2 でブレード シャーシを適切に設定します。『KX II ユーザ ガイ ド』を参照してください。



- CC-SG で KX2 デバイスを適切に設定します。「KVM またはシリ アル デバイスの追加 『61p. 』」を参照してください。
- 3. CC-SG は、ブレード シャーシ デバイスを検出し、1 つまたは 2 つのタブにブレード シャーシ アイコンを追加します。
 - [デバイス] タブでは、ブレード シャーシ デバイスが、接続されている KX2 デバイスの下に表示されます。
 - [ノード] タブでは、ブレード シャーシの IP アドレスまたはホ スト名を KX2 デバイスで入力した場合は、ブレード シャーシ が、それに追加された Web ブラウザ インタフェースを持つノ ードとして表示されます。

注: このタイプのブレード シャーシの場合、後でブレード サーバを設 定する必要があります。「ブレード シャーシ デバイスのスロットの設 定 『**73**p. 』」を参照してください。

- KVM スイッチが統合されていないブレード シャーシ デバイスを 追加するには、以下の手順に従います。
- KX2 でブレード サーバのブレード ポート グループを適切に設定 します。『KX II ユーザ ガイド』を参照してください。
- 2. CC-SG で KX2 デバイスを適切に設定します。「KVM またはシリ アル デバイスの追加 『61p. 』」を参照してください。
- CC-SG は、*仮想*ブレード シャーシを自動的に作成し、1 つのタブ にブレード シャーシ アイコンを追加します。仮想ブレード シャー シが [ノード] タブにノードとして表示されることはありません。
 - [デバイス] タブでは、仮想ブレード シャーシ デバイスが、仮 想ブレード シャーシの下に表示されるブレード サーバの仮想 コンテナとして、KX2 デバイスの下に表示されます。

注: CC-SG で KX2 を設定する前にブレード サーバのブレード ポート グループを設定していなかった場合は、[デバイス]>[デバイス マネー ジャ]>[管理の起動] を選択して、ブレード ポート グループを設定し ます。その後、CC-SG でブレード サーバを設定します。「ブレード シ ャーシ デバイスのスロットの設定 『73p.』」を参照してください。



ブレード シャーシ デバイスのスロットの設定

ブレード サーバまたはスロットがまだ CC-SG で設定されていない場 合は、このセクションの手順に従って、それらを設定する必要がありま す。これらを設定しないと、ブレード サーバは [デバイス] タブと [ノ ード] タブに表示されません。アウト オブ バンド KVM インタフェー スは、自動的にブレード サーバ ノードに追加されます。

- ブレード シャーシ プロファイルからスロットを設定するには、以下の手順に従います。
- [デバイス] タブで、ブレード シャーシ デバイスに接続されている KX2 デバイスの横の + をクリックします。
- 2. 設定するスロットを持つブレード シャーシを選択します。
- 3. [デバイス プロファイル] 画面で、[ブレード] タブを選択します。
- 4. 設定する各スロットのチェックボックスを選択し、[OK] をクリック します。
- [ポートの設定] 画面からスロットを設定するには、以下の手順に従います。
- [デバイス] タブで、ブレード シャーシ デバイスに接続されている KX2 デバイスの横の + をクリックします。
- 2. 設定するスロットを持つブレード シャーシを選択します。
- 3. [デバイス]>[ポート マネージャ]>[ポートの設定] を選択します。
 - 複数のスロットを画面に表示されたデフォルト名で設定するには、設定する各スロットのチェックボックスを選択し、[OK] を クリックしてデフォルト名で各スロットを設定します。
 - 各スロットを個別に設定するには、スロットの横の[設定]ボタンをクリックします。次に、[ポート名]フィールドにスロットの名前を入力し、[ノード名]フィールドにノード名を入力します。[アクセス アプリケーション]のデフォルトは、アプリケーションマネージャの[ブレード シャーシ: KVM] で選択されているデフォルト アプリケーションに応じて設定されます。これを変更するには、[アクセス アプリケーション]ドロップダウンメニューをクリックして、設定するアプリケーションをリストから選択します。[OK] をクリックして、スロットを設定します
- [ブレードの設定] コマンドを使用してスロットを設定するには、以下の手順に従います。
- [デバイス] タブで、ブレード シャーシ デバイスに接続されている KX2 デバイスの横の + をクリックします。
- 2. 設定するスロットを持つブレード シャーシを選択します。
- 3. [ノード]>[ブレードの設定]を選択します。



- 複数のスロットを画面に表示されたデフォルト名で設定するには、設定する各スロットのチェックボックスを選択し、[OK] を クリックしてデフォルト名で各スロットを設定します。
- 各スロットを個別に設定するには、スロットの横の[設定]ボタンをクリックします。次に、[ポート名] フィールドにスロットの名前を入力し、[ノード名] フィールドにノード名を入力します。[アクセス アプリケーション] のデフォルトは、アプリケーション マネージャの [ブレード シャーシ: KVM] で選択されているデフォルト アプリケーションに応じて設定されます。これを変更するには、[アクセス アプリケーション] ドロップダウンメニューをクリックして、設定するアプリケーションをリストから選択します。[OK] をクリックして、スロットを設定します。

ブレード サーバのステータスの変更

このセクションは、KVM スイッチが統合されたブレード シャーシ (Dell PowerEdge や IBM BladeCenter シリーズなど) にのみ適用され ます。

対応するブレード サーバまたはスロットのインストール済みステータ スが KX2 デバイスで有効ではない場合、CC-SG は、ブレード サーバ のポート ステータスとして常に [使用不可] を表示します。いずれかの ブレード スロットにブレード サーバがインストールされ稼働している ことがわかっている場合は、そのステータスが CC-SG で適切に反映さ れるように、KX2 デバイスでステータスを変更します。

- ブレード サーバのステータスを変更するには、以下の手順に従います。
- [デバイス] タブをクリックし、ブレード スロットのステータスを変 更する KX2 デバイスを選択します。
- [デバイス]>[デバイス マネージャ]>[管理の起動] を選択します。
 KX2 Admin Client が表示されます。
- 3. [デバイス設定]>[ポート設定] をクリックします。
- 4. 設定するブレード シャーシ ポートをクリックします。
- ブレード スロット セクションが表示されるまでページをスクロー ル ダウンします。ブレード サーバがインストールされた稼働中の ブレード スロットの横のインストール済みを表すチェックボックス を選択します。
- 6. [OK] をクリックして変更を保存します。



ブレード シャーシ デバイスのスロットの削除

未使用のブレード サーバまたはスロットは、[デバイス] タブおよび [ノ ード] タグに表示されないように削除できます。

- [ポートの削除] 画面からスロットを削除するには、以下の手順に従います。
- [デバイス] タブで、ブレード シャーシ デバイスに接続されている KX2 デバイスの横の + をクリックします。
- 2. スロットを削除するブレード シャーシを選択します。
- 3. [デバイス]>[ポート マネージャ]>[ポートの削除] を選択します。
- 4. 削除する各スロットのチェックボックスを選択し、[OK] をクリック してスロットを削除します。
- [ブレードの削除] コマンドを使用してスロットを削除するには、以下の手順に従います。
- [デバイス] タブで、ブレード シャーシ デバイスに接続されている KX2 デバイスの横の + をクリックします。
- スロットを削除するブレード シャーシ デバイスの横の + をクリッ クします。
- 3. 削除するブレード スロットを右クリックします。
- 4. [ブレードの削除] を選択し、[OK] をクリックしてスロットを削除します。

ブレード シャーシ デバイスの編集

ブレード シャーシ デバイスを編集してその名前およびプロパティを変 更し、スロット設定ステータスを表示できます。

- ▶ ブレード シャーシを編集するには、以下の手順に従います。
- [デバイス] タブで、ブレード シャーシ デバイスに接続されている KX2 デバイスの横の + をクリックします。
- 2. 編集するブレード シャーシ デバイスを選択します。
- 3. この画面で、該当するフィールドに新しいデバイスのプロパティを 入力します。必要に応じて、デバイスに関連するカテゴリとエレメ ントを編集します。
- [ブレード] タブをクリックして、このブレード シャーシ デバイス のすべてのスロットを表示します。
- スロットがノードとして設定されている場合は、[ノード]のハイパ ーリンクをクリックするとノード プロファイルが開きます。オプション。
- 6. [OK] をクリックして変更を保存します。デバイスが変更されるとメ ッセージが表示されます。



ブレード シャーシ デバイスの削除

KX2 デバイスに接続されたブレード シャーシ デバイスを、CC-SG から削除できます。KX2 デバイスからブレード シャーシ デバイスを削除 すると、ブレード シャーシ デバイスと設定済みのすべてのブレード サーバまたはスロットが [デバイス] タブと [ノード] タブに表示されな くなります。

- ブレード シャーシ デバイスを削除するには、以下の手順に従います。
- [デバイス] タブをクリックし、ブレード シャーシ デバイスを削除 する KX2 デバイスを選択します。
- 2. [デバイス]>[ポート マネージャ]>[ポートの削除] を選択します。
- 削除するブレード シャーシ ポートのチェックボックスを選択します。
- [OK] をクリックして、選択したブレード シャーシ ポートを削除し ます。ブレード シャーシ デバイスをそのすべてのブレード サーバ とともに削除することについての確認を求めるメッセージが表示さ れます。

別のポートへのブレード シャーシ デバイスの移動

ブレード シャーシ デバイスを現在の KX2 デバイスまたはポートから 別の KX2 デバイスまたはポートに物理的に移動する場合は、CC-SG はブレード シャーシ デバイスの設定データを検出して新しいポートで 自動的に更新することができません。ブレード シャーシ デバイスを CC-SG で再度設定する必要があります。

- ブレード シャーシ デバイスを別の KX2 デバイスまたはポートに 移動するには、以下の手順に従います。
- CC-SG からブレード シャーシ デバイスを削除します。「ブレード シャーシ デバイスの削除 『76p. 』」を参照してください。
- 2. ブレード シャーシを取り外して、別の KX2 デバイスまたはポート に取り付けます。
- 3. CC-SG でブレード シャーシ デバイスを追加します。「ブレード シャーシ デバイスの追加 『71p. 』」を参照してください。



ブレード サーバ ポートの標準 KX2 ポートへのリストア

このセクションは、KVM スイッチが統合されていないブレード シャーシ (HP BladeSystem シリーズなど) にのみ適用されます。

[デバイス] タブで、仮想ブレード シャーシの下のブレード サーバを、 標準 KX2 ポートとして再設定できます。

- ブレード サーバを標準 KX2 ポートにリストアするには、以下の手順に従います。
- 1. [デバイス] タブで、ブレード サーバを標準 KVM ポートとして再 設定する KX2 デバイスを選択します。
- これらのブレード サーバのブレード ポート グループを、非ブレード ポート グループに変更します。
 - a. CC-SG で、[デバイス] > [デバイス マネージャ] > [管理の起動] を選択します。KX2 Admin Client が表示されます。
 - b. [Port Group Management (ポート グループ管理)] をクリックします。
 - C. グループ プロパティを変更するブレード ポート グループをク リックします。
 - d. [Blade Server Group (ブレード サーバ グループ)] チェックボ ックスを選択解除します。
 - e. [OK] をクリックします。
 - f. KX2 Admin Client を終了します。
- 3. [デバイス] タブに仮想ブレード シャーシが表示されなくなります。 これで、CC-SG でブレード サーバ ポートを標準 KX2 ポートとし て再設定できます。「*KVM ポートの設定* 『67p. 』」を参照してく ださい。

デバイスの関連、場所、および連絡先の一括コピー

ー括コピー コマンドを使用すると、カテゴリ、エレメント、場所、お よび連絡先の情報を 1 つのデバイスから他の複数のデバイスにコピー することができます。ただし、このプロセスでコピーされるプロパティ は選択した情報のみです。選択したデバイスに同じタイプの情報が存在 する場合は、一括コピー コマンドを実行すると、既存のデータが新し く割り当てた情報と置き換えられます。

- デバイスの関連、場所、および連絡先情報を一括コピーするには、 以下の手順に従います。
- [デバイス] タブをクリックし、デバイス ツリーからデバイスを選択 します。



- 2. [デバイス]>[デバイス マネージャ]>[一括コピー] を選択します。
- [使用できるデバイス] リストで、[デバイス名] フィールドに表示されたデバイスの関連、場所、および連絡先情報のコピー先となるデバイス(1 つ以上)を選択します。
- [>] をクリックすると、デバイスが [選択されたデバイス] リストに 追加されます。
- 5. デバイスを選択して、< をクリックし、[選択されたデバイス] リス トから削除します。
- 6. [関連] タブで、[関連のコピー] チェックボックスを選択して、デバ イスのすべてのカテゴリとエレメントをコピーします。
 - このタブで、データを変更、追加、または削除できます。変更 されたデータは、[選択されたデバイス] リストの複数のデバイ ス、および [デバイス名] フィールドに表示されている現在のデ バイスにコピーされます。オプション。
- 7. [ロケーションと連絡先] タブで、コピーする情報のチェックボック スを選択します。
 - [ロケーション情報のコピー] チェックボックスを選択すると、[ロケーション] セクションに表示される場所の情報がコピーされ ます。
 - [連絡先情報のコピー] チェックボックスを選択すると、[連絡先] セクションに表示される連絡先の情報がコピーされます。
 - これらのタブで、データを変更、追加、または削除できます。
 変更されたデータは、[選択されたデバイス] リストの複数のデバイス、および [デバイス名] フィールドに表示されている現在のデバイスにコピーされます。オプション。
- 8. [OK] をクリックして一括コピーします。選択した情報がコピーされ るとメッセージが表示されます。

KX2 2.3 以降に接続するアナログ KVM スイッチの設定

KX2 バージョン 2.3 を使用すると、汎用のアナログ KVM スイッチを ターゲット ポートに接続できます。汎用のアナログ KVM スイッチと そのポートは、CC-SG へのノードとして利用できます。 最初にこのスイッチを KX2 Web インタフェースで設定し、次に KX2 を CC-SG に追加する必要があります。



KX2 に接続する KVM スイッチの追加

この手順では、Admin Client を使用して、KX2 に接続する KVM スイ ッチを追加します。また、CSV のインポートによって KVM スイッチ を追加することもできます。「デバイスの CSV ファイルの要件 『87p. 』」を参照してください。

- KX2 に接続する KVM スイッチを追加するには、以下の手順に従います。
- KX2 で KVM スイッチを適切に設定します。『Dominion KX II ユー ザ ガイド』の「Configuring and Enabling Tiering, and Configuring KVM Switches(階層化の設定と有効化、および KVM スイッチの設 定)」を参照してください。Dominion KX II オンライン ヘルプにアク セスするには、http://www.raritan.com/support/online-help/ を参照し てください。
- CC-SG で KX2 デバイスを適切に設定します。「KVM またはシリ アル デバイスの追加 『61p. 』」を参照してください。
- 3. KX2 のポートの KVM スイッチが検出され、次の 1 つまたは 2 つ のタブにデバイス アイコンが追加されます。
 - [デバイス] タブでは、KVM スイッチ デバイスが、接続されている KX2 デバイスの下に表示されます。
 - [ノード] タブでは、KX2 デバイス上の KVM スイッチへのアク セス URL を入力した場合、KVM スイッチは、Web ブラウザ インタフェースが追加されたノードとして表示されます。

KX2 に接続するアナログ KVM スイッチ デバイスのポートの設定

アナログ KVM スイッチ デバイスのポートがまだ CC-SG で設定され ていない場合は、このセクションの手順に従って、それらを設定する必 要があります。これらを設定しないと、アナログ KVM スイッチとその ポートは [デバイス] タブと [ノード] タブに表示されません。アウト オブ バンド KVM インタフェースは、自動的に KVM スイッチ ノード に追加されます。

- KVM スイッチ デバイス プロファイルからポートを設定するには 、以下の手順に従います。
- [デバイス] タブで、KVM スイッチ デバイスに接続されている KX2 デバイスの横の [+] をクリックします。
- 2. 設定するポートがある KVM スイッチを選択します。
- 3. [デバイス プロファイル] 画面で、[KVM Switch Ports(KVM スイッ チ ポート)] タブを選択します。
- 4. 設定する各スロットのチェックボックスを選択し、[OK] をクリック します。



- [ポートの設定] 画面からスロットを設定するには、以下の手順に従います。
- [デバイス] タブで、KVM スイッチ デバイスに接続されている KX2 デバイスの横の [+] をクリックします。
- 2. 設定するポートがある KVM スイッチ デバイスを選択します。
- 3. [デバイス]>[ポート マネージャ]>[ポートの設定] を選択します。
 - 複数のポートをページに表示されたデフォルト名で設定するには、設定する各ポートのチェックボックスをオンにし、[OK] を クリックしてデフォルト名で各ポートを設定します。
 - 各ポートを個別に設定するには、ポートの横の[設定]ボタンを クリックします。次に、[ポート名] フィールドにポートの名前 を入力し、[ノード名] フィールドにノード名を入力します。[ア クセス アプリケーション] のデフォルトは、アプリケーション マネージャの [KVM Switch: KVM(KVM スイッチ: KVM)] で選択 されているデフォルト アプリケーションに応じて設定されます。 これを変更するには、[アクセス アプリケーション] ドロップ ダウン メニューをクリックして、設定するアプリケーションを リストから選択します。[OK] をクリックして、ポートを設定し ます。
- [ブレードの設定] コマンドを使用してスロットを設定するには、以下の手順に従います。
- [デバイス] タブで、KVM スイッチ デバイスに接続されている KX2 デバイスの横の [+] をクリックします。
- 2. 設定するポートがある KVM スイッチ デバイスを選択します。
- 3. [ノード]>[ポートの設定]を選択します。
 - 複数のポートをページに表示されたデフォルト名で設定するには、設定する各ポートのチェックボックスをオンにし、[OK] を クリックしてデフォルト名で各ポートを設定します。
 - 各ポートを個別に設定するには、ポートの横の[設定]ボタンを クリックします。次に、[ポート名] フィールドにポートの名前 を入力し、[ノード名] フィールドにノード名を入力します。[ア クセス アプリケーション] のデフォルトは、アプリケーション マネージャの [KVM Switch: KVM(KVM スイッチ: KVM)] で選択 されているデフォルト アプリケーションに応じて設定されます。 これを変更するには、[アクセス アプリケーション] ドロップ ダウン メニューをクリックして、設定するアプリケーションを リストから選択します。[OK] をクリックして、ポートを設定し ます。



デバイス グループ マネージャ

デバイス グループ マネージャを使用して、デバイス グループの追加 、編集、および削除を行います。新しいデバイス グループを追加する 場合は、グループのフル アクセス ポリシーを作成できます。「*アクセ ス制御のポリシー*『**197**p. 』」を参照してください。

デバイス グループの概要

デバイス グループは、デバイスをセットとして整理するために使用されます。デバイス グループは、特定のデバイス セットへのアクセスを 許可または拒否するポリシーの基本となります。「ポリシーの追加 『 198p. 』」を参照してください。デバイスの手動によるグループ化は、 Select メソッドを使用して行うことも、Describe メソッドを使用して 共通の属性のセットを示すブール式を作成して行うこともできます。

ガイド設定を使用してノードのカテゴリとエレメントを作成した場合は 、共通属性に従ってデバイスを整理する方法がすでに作成されています 。CC-SG は、これらのエレメントを基にして、デフォルトのアクセス ポリシーを自動的に作成します。カテゴリおよびエレメントの作成の詳 細については、「*関連、カテゴリ、エレメント* 『47p. 』」を参照して ください。

- ▶ デバイス グループを表示するには、以下の手順に従います。
- [関連]>[デバイス グループ]を選択します。[デバイス グループ マネージャ]ウィンドウが表示されます。既存のデバイス グループのリストが左側に、選択したデバイス グループに関する詳細がメインパネルに表示されます。
 - 既存のデバイス グループのリストは、左側に表示されます。デバイス グループをクリックして、デバイス グループ マネージャでデバイスの詳細を表示します。
 - グループが任意に形成されている場合は、グループに属しているデバイスと属していないデバイスのリストを示す[デバイスの 選択]タブが表示されます。
 - グループが共通の属性を基にして形成されている場合は、[デバイスの説明] タブが表示されます。このタブには、グループのデバイス選択を制御するルールが含まれます。
 - [デバイス グループ] リストでデバイスを検索するには、リストの下部にある [検索] フィールドに文字列を入力し、[検索] をクリックします。検索方法は、[プロファイル] 画面で設定されます。「ユーザとユーザ グループ 『176p. 』」を参照してください。



- 属性を基にしたグループを表示している場合は、[デバイスの表示] をクリックして、デバイス グループに現在属しているデバイスのリストを表示します。デバイスとそのすべての属性を示す [デバイス グループのデバイス] ウィンドウが開きます。
- [レポート]>[デバイス]>[デバイス グループ データ] を選択します。既存のデバイス グループのリストが表示されます。行をダブルクリックして、任意のデバイス グループのデバイスを表示します。

デバイス グループの追加

- ▶ デバイス グループを追加するには、以下の手順に従います。
- [関連]>[デバイス グループ] を選択します。[デバイス グループ マネージャ] ウィンドウが表示されます。既存のデバイス グループが 左のパネルに表示されます。
- ツールバーの [新しいグループ] アイコン C をクリックします。[デバイス グループ: 新規] パネルが表示されます。
- [グループ名] フィールドで、作成するデバイス グループの名前を入 力します。名前の長さに関する CC-SG のルールについての詳細は 、「命名規則 『435p. 』」を参照してください。
- グループにデバイスを追加するには、[デバイスの選択] と [デバイスの説明] の 2 つの方法があります。[デバイスの選択] タブでは、 グループに割り当てるデバイスを使用可能なデバイスのリストから 選択できます。[デバイスの説明] タブでは、デバイスについて記述 するルールを指定できます。このルールに従うパラメータを持つデ バイスがグループに追加されます。
- [デバイスの選択] オプションによってデバイス グループを追加するには、以下の手順に従います。
- [デバイス グループ:新規] パネルの [デバイスの選択] タブをクリ ックします。
- [利用可能] リストで、グループに追加するデバイスを選択し、[追加] をクリックしてデバイスを [選択中] リストに移動します。[選択中] リストのデバイスがグループに追加されます。
 - グループからデバイスを削除するには、[選択中] リストでデバイス名を選択し、[削除] をクリックします。
 - [利用可能] リストまたは [選択中] リストのいずれでもデバイス を検索できます。リストの下にあるフィールドに検索語を入力 し、[実行] をクリックします。
- このデバイス グループに対して、グループ内のすべてのデバイスへの制御許可付きアクセスを常に許可するポリシーを作成するには、[グループにフル アクセス ポリシーを作成] チェックボックスを選択します。



- 4. 別のデバイス グループを追加するには、[適用] をクリックしてこの グループを保存し、上記の手順を繰り返します。オプション。
- 5. デバイス グループの追加が終わったら、[OK] をクリックして変更 を保存します。
- [デバイスの説明] オプションによってデバイス グループを追加するには、以下の手順に従います。
- [デバイス グループ:新規] パネルの [デバイスの説明] タブをクリ ックします。[デバイスの説明] タブで、グループに割り当てるデバ イスを説明するルールのテーブルを作成できます。
- 2. [新しい行をテーブルに追加] アイコン
 と たりリックして行をテーブルに追加します。
- 各列で作成したセルをダブルクリックしてドロップダウン メニュー を開きます。各リストから使用するルール コンポーネントを選択し ます。
 - プレフィックス これは空白のままにしておくか、NOT を選択 します。NOT を選択すると、このルールにより、表現全体の反 対の値によりフィルタされます。
 - カテゴリ・ルールで評価される属性を選択します。ここでは、
 関連マネージャで作成した全カテゴリを使用できます。任意の
 ブレード シャーシがシステムで設定されている場合、デフォル
 トでブレード シャーシ カテゴリが利用可能になります。
 - 演算子 カテゴリとエレメント項目間で実行される比較操作を 選択します。3 つの演算子 = (に等しい)、LIKE (名前のエレメ ントを検索するのに使用される)、<> (に等しくない)を使用で きます。
 - エレメント・比較の対象となるカテゴリ属性の値を選択します。 選択したカテゴリに関連付けられたエレメントのみがここに 表示されます(たとえば、「Department」カテゴリを評価する場 合は、「Location」エレメントはここに表示されません)。
 - ルール名 これは、この行のルールに割り当てられた名前です。この名前は、編集できませんが、[簡潔式] フィールドの記述で使用されます。
- 1. 別のルールを追加するには、[新しい行をテーブルに追加] アイコン

 をクリックして、必要な設定を行います。複数のルールを設定
 すると、デバイスの評価に複数の条件を適用することができるため
 、より正確な説明が可能になります。



- ルールの表は、ノードを評価するための条件を利用可能にするだけです。デバイスグループの説明を入力するには、ルール名でルールを[簡潔式]フィールドに追加します。説明に1つのルールしか必要ない場合は、フィールドにルールの名前を入力します。複数のルールが評価される場合は、以下のように、それぞれの関係を説明する論理演算のセットを使用して、フィールドにルールを入力します。
 - & AND 演算子。true と評価されるためには、説明(または説明の一部)で、ノードがこの演算子の両辺にあるルールを満たす必要があります。
 - |-OR 演算子。true と評価されるためには、説明 (または説明 の一部) で、デバイスがこの演算子のいずれかの辺にあるルー ルを満たす必要があります。
 - (と)-グループ化演算子。これは、カッコ内に含まれるサブセクションに説明を分割します。カッコ内のセクションは、説明の残りの部分がノードと比較される前に評価されます。カッコで囲まれたグループは、他のカッコで囲まれたグループ内にネストすることができます。

例 1: エンジニアリング部門に属するデバイスを記述する場合は 、「Department = Engineering」というルールを作成します。こ れを、Rule0 とします。[簡潔式] フィールドに「Rule0」と入力 します。

例 2: エンジニアリング部門に属するデバイス グループ、また はフィラデルフィアにあるデバイス グループを説明し、さらに すべてのマシンが 1 GB のメモリを持つ必要があることを指定 するには、次の 3 つのルールを作成する必要があります。 Department = Engineering (Rule0) Location = Philadelphia (Rule1) Memory = 1GB (Rule2)。これらのルールを相互に関連付 ける必要があります。デバイスは、エンジニアリング部門に属 するか、フィラデルフィアにあるいずれかのデバイスとなるの で、OR 演算子 ())を使用して、Rule0|Rule1 のように 2 つの ルールを結合します。これを (Rule0|Rule1) のようにカッコで 囲み、この比較をまず行います。最後に、デバイスは、この比 較を満たし、さらに 1GB のメモリを持つ必要があるので、 AND 演算子 & を使用して、(Rule0|Rule1)&Rule2 のようにこ のセクションを Rule2 と結合します。この最終的な式を、[簡潔 式] フィールドに入力します。

注: 演算子 & および | の前後にはスペースを入れる必要がありま す。スペースを入れない場合、テーブルからすべてのルールを削除 すると、[簡潔式] フィールドがデフォルトの式 (Rule0 & Rule1 & Rule2 など) を返します。



- テーブルから行を削除する場合は、その行を選択し、[行の削除]
 アイコン 2 をクリックします。
- 定義したルールに従うパラメータを持つデバイスのリストを表示するには、[デバイスの表示]をクリックします。
- [簡潔式] フィールドに説明を入力したら、[確認] をクリックします 。説明が正しく入力されなかった場合は、警告が表示されます。説 明を正しく入力すると、[正規式] フィールドに正規化された式が表 示されます。
- [デバイスの表示]をクリックすると、この式を満たすノードが表示 されます。デバイス グループ内のデバイスの結果を示すウィンドウ が開き、現在の式によりグループ化されるデバイスが表示されます 。これは、説明が正しく記述されているかどうかを確認するため使 用できます。正しく記述されていない場合は、ルール テーブルまた は[簡潔式]フィールドに戻って、式を調整できます。
- このデバイス グループに対して、グループ内のすべてのデバイスへの制御許可付きアクセスを常に許可するポリシーを作成するには、[グループにフル アクセス ポリシーを作成] チェックボックスを選 択します。
- 9. 別のデバイス グループを追加するには、[適用] をクリックしてこの グループを保存し、上記の手順を繰り返します。オプション。
- 10. デバイス グループの追加が終わったら、[OK] をクリックして変更 を保存します。

describe メソッドと select メソッドの対比

describe メソッドは、カテゴリやエレメントなど、ノードまたはデバイ スの一部の属性に基づいてグループを作成したい場合に使用します。 describe メソッドの利点は、記述された同じ属性を持つデバイスまたは ノードを複数追加する場合に、それらが自動的にグループを形成すると いう点です。

select メソッドは、特定のノードのグループを手動で作成する場合に使用します。CC-SG に新しいノードおよびデバイスを追加しても、グループが自動的に形成されることはありません。CC-SG に追加後、新しいノードまたはデバイスを手動でグループに追加する必要があります。

これら2 つのメソッドは併用できません。

ー方のメソッドで作成したグループは、編集の際に同じメソッドを使用 する必要があります。メソッドを切り替えると、現在のグループ設定が 上書きされます。



デバイス グループの編集

- ▶ デバイス グループを編集するには、以下の手順に従います。
- 1. [関連] > [デバイス グループ] を選択します。[デバイス グループ マ ネージャ] ウィンドウが表示されます。
- 既存のデバイス グループが左のパネルに表示されます。編集するデバイス グループの名前を選択します。デバイス グループの詳細パネルが表示されます。
- 3. デバイス グループの新しい名前を [グループ名] フィールドに入力 します。オプション。
- [デバイスの選択] または [デバイスの説明] タブを使用して、デバイス グループに含まれるデバイスを編集します。「 デバイス グループの追加 『82p. 』」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。

デバイス グループの削除

- ▶ デバイス グループを削除するには、以下の手順に従います。
- 1. [関連] > [デバイス グループ] を選択します。[デバイス グループ マ ネージャ] ウィンドウが表示されます。
- 既存のデバイス グループが左のパネルに表示されます。削除するデ バイス グループを選択します。デバイス グループの詳細パネルが 表示されます。
- 3. [グループ]>[削除] を選択します。
- 4. [デバイス グループの削除] パネルが表示されます。[削除] をクリッ クします。
- 5. 表示される確認メッセージで [はい] をクリックします。

CSV ファイルのインポートによるデバイスの追加

値が含まれている CSV ファイルをインポートすることによって、デバ イスを CC-SG に追加できます。デバイスをインポートおよびエクスポ ートするには、デバイス、ポート、およびノードの管理権限、および CC の設定と制御権限が必要です。

関連するすべてのデバイスとノードへのアクセスを付与するポリシーが 割り当てられている必要があります。すべてのノードおよびすべてのデ バイスに対するフル アクセス ポリシーを推奨します。

注: CSV ファイルのインポートによって P2SC デバイスを追加するこ とはできません。



デバイスの CSV ファイルの要件

デバイスの CSV ファイルでは、デバイス、ポート、およびそれらを CC-SG に追加するために必要な詳細が定義されています。

- ポートに接続された電源タップをサポートするデバイス (SX、KX、 KX2、KSX2) では、ポートを設定すると電源タップも設定されます。
- デバイス ポートを設定すると、CC-SG によって、ポートごとにアウト オブ バンド KVM インタフェースまたはアウト オブ バンドシリアル インタフェースを持つノードの追加も行われます。
- ブレードを追加するには、CIM を使用してブレード サーバを KX2 デバイスに接続する必要があります。KX2 デバイスは、すでに CC-SG に追加されているか、または同じ CSV ファイルに含まれ ている必要があります。
- 有効な CSV ファイルの作成に必要なすべてのタグとパラメータが 含まれているコメントを参照するには、CC-SG からファイルをエ クスポートします。「デバイスのエクスポート 『92p. 』」を参照し てください。
- すべての CSV ファイルの追加要件を満たします。「CSV ファイル の共通要件 『412p. 』」を参照してください。

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	DEVICE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	デバイス タイプ	必須フィールド。 以下に示すデバイス タイプを入力し ます。 KX、KX2、KSX、KSX2、KX101、 KX2-101、IP-Reach、SX、または PX
4	デバイス名	必須フィールド。 デバイス名にスペースまたは特定の 特殊文字を含めることはできません 。 Dominion PX デバイス名にピリオド を含めることはできません。インポ

CSV ファイルにデバイスを追加する場合



列番号	タグまたは値	詳細
		ート時に、ピリオドはハイフンに変 換されます。
5	IP アドレスまたはホスト 名	必須フィールド。
6	ユーザ名	必須フィールド。
7	パスワード	必須フィールド。
8	ハートビート	デフォルトは、Admin Client の [管 理] > [設定] > [デバイス設定] タブで 設定します。
9	TCP ポート	デフォルトは、Admin Client の [管 理] > [設定] > [デバイス設定] タブで 設定します。
10	すべてのポートの設定	TRUE または FALSE Dominion PX デバイスの場合、デフ オルトは TRUE です。 その他のすべてのデバイス タイプの 場合、デフォルトは FALSE です。 TRUE に設定すると、すべてのポー トが設定され、適切なアウト オブ バンド インタフェースを持つノード が作成されます。 FALSE に設定すると、対応する ADD DEVICE-PORT レコードが CSV ファイルに含まれているポート のみが設定されます。
11	直接アクセスを許可	TRUE または FALSE デフォルトは FALSE です。 この設定は、SX デバイスと KX2 バージョン 2.2 以降のデバイスにの み適用されます。
12	説明	オプション。



CSV ファイルにポートを追加する場合

DEVICE-PORT タグは、[すべてのポートの設定] が FALSE に設定されたデバイスを追加してポートを個別に指定する場合にのみ使用します。CSV ファイルをインポートする場合は、追加するポートの設定を CC-SG で解除する必要があります。

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	DEVICE-PORT	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	デバイス名	必須フィールド。
4	ポート タイプ	必須フィールド。 以下に示すポート タイプを入力しま す。 KVM SERIAL OUTLET または POWER "OUTLET" または "POWER" は、PX デバイスのコンセントを設定する場 合に使用します。
5	ポート番号またはアウトレ ット番号	必須フィールド。
6	ポート名またはアウトレッ ト名	オプション。空白のままにした場合 は、デフォルト名またはデバイス レ ベルですでに割り当てられている名 前が使用されます。
7	ノード名	KVM ポートおよびシリアル ポート の場合は、このポートの設定時に作 成されるノードの名前を入力します 。

CSV ファイルにブレードを追加する場合

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。



列番号	タグまたは値	詳細
2	DEVICE-BLADE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	デバイス名	必須フィールド。
4	ポート番号	必須フィールド。
5	ブレード番号	必須フィールド。
6	ブレード名	オプション。空白のままにした場合 は、デバイス レベルで割り当てられ ている名前が使用されます。名前を CSV ファイルに入力すると、その名 前はデバイス レベルにコピーされま す。
7	ノード名	このブレードの設定時に作成される ノードの名前を入力します。

▶ KX2 に接続する階層化された KVM スイッチを追加するには、以下の手順に従います。

階層化された KVM スイッチが接続されている KX2 ポートは、タイプ "KVM" としてインポートする必要があります。

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	DEVICE-KVMSWITCHPORT	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	デバイス名	必須フィールド。
4	ポート番号	KVM スイッチを接続するポート。 必須フィールド。
5	KVM スイッチ ポート番号	必須フィールド。
6	KVM スイッチ ポート名	オプション。空白のままにした場合 は、デバイス レベルで割り当てられ ている名前が使用されます。名前を CSV ファイルに入力すると、その名 前はデバイス レベルにコピーされま す。


Ch 6: デバイス、デバイス グループ、ポート

列番号	タグまたは値	詳細
7	ノード名	この KVM スイッチ ポートの設定 時に作成されるノードの名前を入力 します。

CSV ファイルでカテゴリとエレメントをデバイスに割り当てる場合

カテゴリとエレメントが **CC-SG** ですでに作成されている必要があります。

CSV ファイルで同じカテゴリの複数のエレメントをデバイスに割り当 てることができます。

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	DEVICE-CATEGORYELEME NT	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	デバイス名	必須フィールド。
4	カテゴリ名	必須フィールド。
5	エレメント名	必須フィールド。

デバイスの CSV ファイルの例

ADD, DEVICE, DOMINION KX2, Lab-Test, 192.168.50.123, ST Lab
KVM, username, password,,,,
ADD, DEVICE-PORT, Lab-Test, KVM, 1, Mail Server, Mail
Server
ADD, DEVICE-PORT, Lab-Test, KVM, 2, DNS Server, DNS Server
ADD, DEVICE-PORT, Lab-Test, KVM, 3
ADD, DEVICE-PORT, Lab-Test, KVM, 4
ADD, DEVICE-CATEGORYELEMENT, Lab-Test, Location, Rack17



デバイスのインポート

CSV ファイルを作成したら、エラーがないかどうかを確認してからインポートします。

重複するレコードはスキップされ、追加されません。

- ▶ デバイスをインポートするには、以下の手順に従います。
- 1. [管理]>[インポート]>[デバイスのインポート]を選択します。
- [参照] をクリックし、インポートする CSV ファイルを選択します。
 [開く] をクリックします。
- 3. [確認] をクリックします。[分析レポート] 領域にファイルの内容が 表示されます。
 - ファイルが有効でない場合は、エラー メッセージが表示されます。[OK] をクリックし、ページの [問題] 領域でファイルに関する問題の説明を参照します。[ファイルに保存] をクリックして問題リストを保存します。CSV ファイルを修正し、再度検証します。「CSV ファイルの問題のトラブルシューティング 『414p.』」を参照してください。
- 4. [インポート] をクリックします。
- [アクション] 領域でインポート結果を確認します。正常にインポートされたアイテムは、緑色のテキストで表示されます。インポートに失敗したアイテムは、赤いテキストで表示されます。重複するアイテムがすでに存在するか、またはすでにインポートされているためにインポートに失敗したアイテムも赤いテキストで表示されます。
- 6. インポート結果の詳細を参照するには、監査証跡レポートを確認し ます。「*インポートに関する監査証跡エントリ* 『413p. 』」を参照 してください。

デバイスのエクスポート

エクスポート ファイルの一番上には、ファイル内の各アイテムを説明 するコメントが含まれています。コメントは、インポートするファイル を作成するための指示として使用できます。

注: P2SC デバイスはエクスポートされません。

▶ デバイスをエクスポートするには、以下の手順に従います。

- 1. [管理]>[エクスポート]>[デバイスのエクスポート]を選択します。
- 2. [ファイルにエクスポート] をクリックします。
- 3. ファイルの名前を入力し、保存する場所を選択します。
- 4. [保存] をクリックします。



デバイスのアップグレード

デバイス ファームウェアの新しいバージョンが入手可能になったら、 デバイスをアップグレードできます。

重要: 互換表を参照して、新しいデバイス ファームウェア バージョンに、 ご使用の CC-SG ファームウェア バージョンとの互換性があることを 確認してください。CC-SG とデバイスまたはデバイスのグループの両方 をアップグレードする必要がある場合は、まず CC-SG のアップグレー ドを実行してから、デバイスのアップグレードを実行してください。

- ▶ デバイスをアップグレードするには、以下の手順に従います。
- [デバイス] タブをクリックし、デバイスをデバイス ツリーから選択 します。
- [デバイス]>[デバイス マネージャ]>[デバイスのアップグレード] を選択します。
- [ファームウェア名]: 適切なファームウェアをリストから選択します。この情報については、Raritan またはお近くの販売代理店にお問い合わせください。
- 4. [OK] をクリックして、デバイスをアップグレードします。
 - SX デバイスおよび KX デバイスのアップグレードには、約 20 分かかります。
 - デバイスのファームウェア バージョンに CC-SG との互換性が ない場合、メッセージが表示されます。[はい] をクリックして 、デバイスをアップグレードします。アップグレードをキャン セルするには、[いいえ] をクリックします。
- 5. メッセージが表示されます。[はい] をクリックして、デバイスを再 起動します。デバイスがアップグレードされるとメッセージが表示 されます。
- アップグレードされたすべてのファイルがブラウザにロードされる ようにするため、ブラウザ ウィンドウを閉じて、新しいブラウザ ウィンドウで CC-SG にログインします。



デバイス設定のバックアップ

選択したデバイスのすべてのユーザ設定ファイルおよびシステム設定フ ァイルをバックアップできます。デバイスに何らかの問題が生じた場合 は、作成済みのバックアップ ファイルを使用して CC-SG から以前の 設定を復元できます。

CC-SG にはデバイスごとに 3 つまでバックアップ ファイルを保存で きます。さらにバックアップが必要な場合は、バックアップ ファイル をネットワークに保存して、CC-SG から削除します。あるいは一番古 いバックアップ ファイルを削除することもできます。4 番目のバック アップを試みると、このオプションが警告として表示されます。「全設 定データを KX2、KSX2、または KX2-101 デバイスにリストア 『97p. の"すべての設定データの KX2、KSX2、または KX2-101 デバイスへの リストア"参照 』」を参照してください。

デバイスごとに、設定の異なるコンポーネントをバックアップできます。バックアップするデバイスの詳細は、『ユーザ ガイド』を参照してください。

注: SX 3.0.1 デバイスをバックアップしても、接続されている電源タッ プの設定はバックアップされません。SX 3.0.1 デバイスをバックアップ からリストアする場合、電源タップを再設定する必要があります。

- デバイス設定をバックアップする場合:
- [デバイス] タブをクリックし、バック アップするデバイスを選択します。
- [デバイス]>[デバイス マネージャ]>[設定]>[バックアップ] を選 択します。
- 3. このバックアップを識別する名前を [バックアップ名] フィールドに 入力します。
- 4. このバックアップの短い説明を [説明] フィールドに入力します。オ プション。
- 5. [OK] をクリックしてデバイス構成をバックアップします。デバイス 設定がバックアップされるとメッセージが表示されます。



デバイス設定のリストア

次のデバイス タイプでは、デバイス設定の完全バックアップをリスト アできます。

- KX
- KSX
- KX101
- SX
- IP-Reach

KX2、KSX2、KX2-101 デバイスでは、デバイスにリストアするバック アップのコンポーネントを選択できます。

- 保護: ネットワーク設定(個人パッケージ)を除く、選択したバック アップ ファイルの内容全体、および KX2 デバイスの場合はポート 設定がデバイスにリストアされます。またこのオプションを使用す ると、1 つのデバイスのバックアップを同じモデルの別のデバイス にリストアできます(KX2,、KSX2、KX2-101のみ)。
- 完全: 選択したバックアップ ファイルの内容全体がデバイスにリス トアされます。
- カスタム: デバイス設定か、ユーザとユーザ グループの設定か、またはその両方をリストアできます。

デバイス設定のリストア (KX、KSX、KX101、SX、IP-Reach)

KX、KSX、KX101、SX、および IP-Reach デバイスには、完全バック アップ設定をリストアできます。

- 完全バックアップデバイス設定をリストアするには、以下の手順に 従います。
- [デバイス] タブをクリックし、バックアップ設定にリストアするデバイスを選択します。
- [デバイス]>[デバイス マネージャ]>[設定]>[リストア] を選択します。
- 3. [利用可能なバックアップ] テーブルで、デバイスにリストアするバ ックアップ設定を選択します。
- 4. [OK] をクリックします。
- 5. [はい] をクリックして、デバイスを再起動します。すべてのデータ がリストアされるとメッセージが表示されます。



ネットワーク設定以外のすべての設定データの KX2、KSX2、または KX2-101 デバイスへのリストア

[保護] リストア オプションを使用すると、ネットワーク設定を除く、 バックアップ ファイル内のすべての設定データを KX2、KSX2、 KX2-101 デバイスにリストアできます。またこのオプションを使用する と、1 つのデバイスのバックアップを同じモデルの別のデバイスにリス トアできます (KX2,、KSX2、KX2-101 のみ)。

- ネットワーク設定以外のすべての設定データを KX2、KSX2、また は KX2-101 デバイスヘリストアするには、以下の手順に従います。
- [デバイス] タブをクリックし、バックアップ設定にリストアするデバイスを選択します。
- [デバイス]>[デバイス マネージャ]>[設定]>[リストア] を選択します。
- 3. [利用可能なバックアップ] テーブルで、デバイスにリストアするバ ックアップ設定を選択します。
- 4. リストア タイプ:[保護] を選択します。
- 5. [OK] をクリックします。
- [はい]をクリックして、デバイスを再起動します。すべてのユーザ およびシステム設定データがリストアされるとメッセージが表示さ れます。

デバイス設定またはユーザとユーザ グループのデータのみの KX2、 KSX2、KX2-101 デバイスへのリストア

[カスタム] リストア オプションを使用すると、デバイス設定、ユーザ およびユーザ グループの設定のいずれか、または両方をリストアでき ます。

- デバイス設定またはユーザとユーザ グループのデータのみを KX2、 KSX2、KX2-101 デバイスヘリストアするには、以下の手順に従います。
- [デバイス] タブをクリックし、バックアップ設定にリストアするデバイスを選択します。
- [デバイス]>[デバイス マネージャ]>[設定]>[リストア] を選択します。
- 3. [利用可能なバックアップ] テーブルで、デバイスにリストアするバ ックアップ設定を選択します。
- 4. リストア タイプ: [カスタム] を選択します。



- リストア オプション: デバイスにリストアするコンポーネントを、[デバイス設定]、[ユーザとユーザ グループのデータ]の中から選択 します。
- 6. [OK] をクリックします。
- 7. [はい] をクリックして、デバイスを再起動します。データがリスト アされるとメッセージが表示されます。

すべての設定データの KX2、KSX2、または KX2-101 デバイスへのリ ストア

[完全] リストア オプションを使用すると、バックアップ ファイル内の すべての設定データを KX2、KSX2、または KX2-101 デバイスにリス トアできます。

- すべての設定データを KX2、KSX2、または KX2-101 デバイスへ リストアするには、以下の手順に従います。
- [デバイス] タブをクリックし、バックアップ設定にリストアするデバイスを選択します。
- [デバイス]>[デバイス マネージャ]>[設定]>[リストア] を選択します。
- 3. [利用可能なバックアップ] テーブルで、デバイスにリストアするバ ックアップ設定を選択します。
- 4. リストア タイプ: [完全] を選択します。
- 5. [OK] をクリックします。
- 6. [はい] をクリックして、デバイスを再起動します。すべてのユーザ およびシステム設定データがリストアされるとメッセージが表示さ れます。

デバイス バックアップ ファイルの保存、アップロード、削除

[デバイス設定のリストア] ページで、デバイス バックアップ ファイル をネットワークまたはローカル マシン上の場所に保存できます。 **CC-SG** に保存される新しいバックアップのためのスペースを作る必要 がある場合、デバイス バックアップ ファイルをいくつか削除できます 。ネットワークに保存されたデバイス バックアップ ファイルをアップ ロードして **CC-SG** に戻し、デバイス構成のリストアで使用することも できます。

- 以下の手順で CC-SG からデバイス バックアップ ファイルを保存 します。
- 1. [デバイス] タブをクリックし、デバイスを選択します。
- [デバイス]>[デバイス マネージャ]>[設定]>[リストア] を選択します。



- 3. 保存するデバイス バックアップ ファイルを選択します。[ファイル に保存] をクリックします
- 4. ファイルの保存先の場所を表示します。[保存] をクリックします。
- 以下の手順で CC-SG からデバイス バックアップ ファイルを削除 します。
- 1. [デバイス] タブをクリックし、デバイスを選択します。
- [デバイス]>[デバイス マネージャ]>[設定]>[リストア] を選択します。
- 3. 削除するデバイス バックアップ ファイルを選択します。[削除] を クリックします。
- 4. [はい] をクリックして確認します。
- 以下の手順でデバイス バックアップ ファイルを CC-SG にアップ ロードします。
- 1. [デバイス] タブをクリックし、デバイスを選択します。
- [デバイス]>[デバイス マネージャ]>[設定]>[リストア] を選択します。
- [アップロード] をクリックします。デバイス バックアップ ファイ ルを表示して、選択します。ファイル タイプは .rfp です。[開く] をクリックします。
 デバイス バックアップ ファイルが CC-SG にアップロードされ、 ページに表示されます。



デバイス設定のコピー

以下のデバイスのタイプでは、1 台のデバイスから 1 台以上の他のデ バイスに設定をコピーできます。

- SX
- KX2
- KSX2
- KX2-101

設定は、同じポート数の同一モデル間でのみコピーできます。たとえば、1 台の KX2-864 デバイスからは、他の KX2-864 デバイスにのみ設 定をコピーできます。

[設定のコピー] コマンドを使用すると、ネットワーク設定 (個人パッケ ージ) を除くすべての設定データ、および KX2 デバイスの場合はポー ト設定がコピーされます。デバイス設定、およびユーザとユーザ グル ープのデータがこの処理ですべてコピーされます。

デバイス設定をコピーするには、以下の手順に従います。

- 1. [デバイス] タブをクリックし、別のデバイスにコピーしようとする 設定を持つデバイスをデバイス ツリーから選択します。
- [デバイス]>[デバイス マネージャ]>[設定]>[設定のコピー] を選 択します。
- 3. 設定のコピー方法を選択します。
 - 現在の設定データをコピーするには、[Copy From Device (デバイスからコピー)]を選択します。
 - CC-SG で前に保存したバックアップ ファイル内の設定データ をコピーするには、[Copy From Backup File (バックアップ フ ァイルからコピー)]を選択し、ドロップダウン リストからファ イルを選択します。利用できるバックアップ ファイルがない場 合、このオプションは無効です。
- [デバイス グループ] ドロップダウン矢印をクリックし、リストから デバイス グループを選択します。選択したデバイス グループのす べてのデバイスが [利用可能] 列に表示されます。
- 5. この設定のコピー先となるデバイスを [利用可能] 列でハイライトして、右矢印をクリックし、[選択中] 列に移動します。左矢印をクリックすると、選択したデバイスが [選択中] 列の外に移動します。
- 6. [OK] をクリックして、[選択中] 列のデバイスに設定をコピーします。
- 7. [再起動] メッセージが表示されたら、[はい] をクリックしてデバイ スを再起動します。デバイス設定がコピーされるとメッセージが表 示されます。



デバイスの再起動

[デバイスの再起動]機能を使って、デバイスを再起動します。

- ▶ デバイスを再起動するには、以下の手順に従います。
- 1. [デバイス] タブをクリックし、再起動するデバイスを選択します。
- [デバイス]>[デバイス マネージャ]>[デバイスの再起動] を選択し ます。
- 3. [OK] をクリックして、デバイスを再起動します。
- [はい]をクリックして、デバイスにアクセスしているすべてのユー ザがログオフされることを確認します。

デバイスの ping

デバイスを ping すると、そのデバイスがネットワークで使用可能かど うかを確認できます。

- ▶ デバイスを ping する場合:
- 1. [デバイス] タブをクリックし、ping するデバイスを選択します。
- [デバイス]>[デバイス マネージャ]>[デバイスの ping] を選択しま す。[デバイスの Ping] 画面に ping の結果が表示されます。

CC-SG のデバイス管理の一時停止

デバイスを停止して、CC-SG の管理を一時的に中断することができます。CC-SG に保存された設定データは失われません。

デバイスを一時停止または再開するタスクをスケジュールするには、「 タスクのスケジュール 『313p. 』」を参照してください。

- ▶ デバイスの CC-SG 管理を一時停止するには、以下の手順に従いま す。
- 1. [デバイス] タブをクリックし、CC-SG 管理が一時停止されるデバ イスを選択します。
- 2. [デバイス]>[デバイス マネージャ]>[管理の一時停止] を選択しま す。デバイス ツリー内のデバイスのアイコンは、デバイスの停止状 態を示します。



デバイスの管理の再開

停止したデバイスの CC-SG 管理を再開し、CC-SG の制御下に戻すことができます。

- 一時停止されたデバイスの CC-SG 管理を再開するには、以下の手順に従います。
- 1. [デバイス] タブをクリックし、一時停止されたデバイスをデバイス ツリーから選択します。
- 2. [デバイス]>[デバイス マネージャ]>[管理の再開] を選択します。 デバイス ツリー内のデバイスのアイコンは、デバイスのアクティブ 状態を示します。

スケジュールされたタスクを使用したデバイス管理の一時停止と再開

複数のデバイスまたはデバイス グループを一度に一時停止または再開 するには、デバイスのグループで操作を連続して実行するタスクをスケ ジュールします。

[Pause/Resume Device Management(デバイス管理の一時停止/再開)] タ スクは、管理対象デバイスに接続されているブレード シャーシ、管理 対象デバイスに接続されている電源タップ、および管理対象の電源タッ プには適用されません。

タスク実行時に、すべてのデバイス操作が成功した場合は成功と記録されます。タスクは終了したが、再試行を可能な回数繰り返しても一部の デバイス操作に失敗した場合は、タスクは例外付きの成功と記録されま す。すべてのデバイス操作が失敗した場合、タスクは失敗として記録されます。

- スケジュール タスクを使用してデバイスの一括一時停止および再開 を行うには、以下の手順に従います。
- [管理]>[タスク]を選択します。新しいタスクの作成、および [メイン]、[定期実行]、[再試行]、[通知]の各タブの入力については、「タスクのスケジュール 『313p. 』」を参照してください。
 - [定期実行]: 定期実行の間隔は、時間単位または日単位でのみ指 定できます。
 - [再試行]: CC-SG は一時停止または再開に失敗したデバイスでの み操作を再試行します。
- [タスクのデータ] タブの [タスクの操作] フィールドで、
 [Pause/Resume Device Management(デバイス管理の一時停止/再開)] を選択します。
- [管理の一時停止] または [管理の再開] を選択します。両方のタスクの実行が必要な場合は、それぞれのタスクをスケジュールし、2 つのタスクの間のタイミングを調整します。



- 4. [間隔 (秒)] フィールドで、CC-SG で 1 つの操作を完了してから次 の操作を開始するまでの遅延時間となる秒数を選択します。
- 選択したデバイスで再起動が必要な場合はそのデバイスの一時停止 または再開操作をスキップさせるには、[Skip Device if Restart Required(再起動が必要な場合はデバイスをスキップ)] チェックボッ クスをオンにします。
- 6. [デバイス グループ] ドロップダウン リストからデバイス グループ を選択する方法で、タスクに含めるデバイスを選択します。含める デバイスを[利用可能] リストで選択し、矢印ボタンを使用して、デ バイスを [選択中] リストに移動します。[選択中] リスト内のデバイ スは、一時停止または再開操作の対象となります。
 - 選択中のデバイスのうち再起動が必要なデバイスは、[Skip Device if Restart Required(再起動が必要な場合はデバイスをス キップ)] チェックボックスをオンにしている場合、タスク実行 時にスキップされます。
- 7. [OK] をクリックします。

デバイス パワー マネージャ

デバイス パワー マネージャを使用すると、電源タップ デバイスのス テータス (電圧、電流、温度など)を表示して、電源タップ デバイスの すべての電源コンセントを管理できます。デバイス パワー マネージャ には、電源タップ中心のコンセント表示が用意されています。

デバイス パワー マネージャを使用する前に、電源タップから Dominion SX または Dominion KSX ユニットへの物理接続を作成する 必要があります。電源タップ デバイスを追加する場合、接続の提供元 となる Raritan デバイスを定義する必要があります。これにより、電源 タップ デバイスが電源タップの管理機能を提供する SX シリアル ポー トまたは KSX 専用パワー ポートに関連付けられます。

- デバイス パワー マネージャを表示するには、以下の手順に従います。
- 1. [デバイス] タブで、電源タップ デバイスを選択します。
- 2. [デバイス]>[デバイス パワー マネージャ] を選択します。
- [コンセント ステータス] パネルにコンセントがリスト表示されます。 すべてのコンセントを閲覧するには、スクロールしなければならない場合があります。
 - 各コンセントのドロップダウン リストから [オン] または [オフ] を選択すると、コンセントの電源をオンまたはオフにできます。
 - ドロップダウン リストから [電源の再投入] を選択すると、コンセントに接続されたデバイスを再起動できます。



デバイスの管理ページの起動

選択したデバイスで[管理の起動] コマンドが使用可能な場合、そのコ マンドを使用してそのデバイスの管理インタフェースにアクセスできま す。

- デバイスの管理ページを起動するには、以下の手順に従います。
- 1. [デバイス] タブをクリックし、起動する管理インタフェースのデバ イスを選択します。
- 2. [デバイス]>[デバイス マネージャ]>[管理の起動] を選択します。 選択したデバイスの管理インタフェースが表示されます。

ユーザの切断

管理者はデバイスでのユーザのセッションを終了できます。これには、 ポートへの接続、デバイスの設定のバックアップ、デバイスの設定の復 元、またはデバイスのファームウェアのアップグレードといった、デバ イスでさまざまな操作を実行中のユーザが対象となります。

ファームウェアのアップグレードおよびデバイス設定のバックアップと 復元などの操作は、終了してからデバイスを使うユーザ セッションが 中断されます。その他すべての操作は、すぐに中断されます。

Dominion SX デバイスの場合のみ、直接デバイスにログインするユーザ および、CC-SG からデバイスに接続するユーザを切断できます。

- ▶ デバイスからユーザを切断するには、以下の手順に従います。
- [デバイス] タブをクリックし、ユーザが切断されるデバイスを選択 します。
- [デバイス]>[デバイス マネージャ]>[ユーザの切断] を選択します。
- 3. [ユーザの切断] テーブルで、セッションの接続が切断されるユーザ を選択します。
- 4. [切断] をクリックし、デバイスからユーザを切断します。



Paragon II システム デバイスへの専用アクセス

Paragon II システム コントローラ (P2-SC)

Paragon II システム統合のユーザは、P2-SC デバイスを CC-SG デバ イス ツリーに追加して、CC-SG 内から P2-SC 管理アプリケーション を使用して設定を行うことができます。P2-SC 管理の使用法について の詳細は、Raritan の『Paragon II System Controller User Guide』を 参照してください。

CC-SG に Paragon システム デバイス (Paragon システムには P2-SC デバイス、接続された UMT ユニットおよび IP-Reach ユニッ トが含まれる) を追加すると、デバイス ツリーに Paragon システム デバイスが表示されます。

- CC-SG から Paragon II システム コントローラにアクセスするに は、以下の手順に従います。
- 1. [デバイス] タブをクリックし、Paragon II システム コントローラ を選択します。
- [デバイス]>[デバイス マネージャ]>[管理の起動] を選択して、 Paragon II システム コントローラ アプリケーションを新しいブラ ウザ ウィンドウで起動します。PII UMT ユニットを設定できます。

IP-Reach と UST-IP 管理

CC-SG インタフェースから直接 Paragon システム設定に接続されて いる IP-Reach および UST-IP デバイスの管理診断を実行することがで きます。

CC-SG に Paragon システム デバイスを追加すると、デバイス ツリーに Paragon システム デバイスが表示されます。

- リモート ユーザ ステーション管理にアクセスするには、次の手順 に従います。
- 1. [デバイス] タブをクリックし、Paragon II システム コントローラ を選択します。
- 2. [デバイス]>[デバイス マネージャ]>[ユーザ ステーション管理の 起動] を選択します。



Ch7 管理対象電源タップ

CC-SG で電源タップを使用してパワー制御を設定するには、3 通りの 方法があります。

- サポートされるすべての Raritan 社製電源タップは、別の Raritan デバイスに接続して、電源タップ デバイスとして CC-SG に追加 できます。Raritan 社製電源タップには Dominion PX 電源タップと RPC 電源タップがあります。互換表からサポートされるバージョン を確認してください。CC-SG でこのタイプの管理対象電源タップ を設定するには、どの Raritan デバイスに電源タップが物理的に接 続されているかがわかっている必要があります。「CC-SG 内の別の デバイスによって管理される電源タップの設定 『107p. 』」を参照 してください。
- 2. Dominion PX 電源タップは、IP ネットワークに直接接続し、PX デ バイスとして CC-SG に追加できます。IP ネットワークに直接接 続されている PX 電源タップは、別の Raritan デバイスに接続する 必要はありません。
- Raritan の Power IQ サービス インタフェースを設定することで、 PDU のマルチベンダ サポートを利用できます。「Power IQ IT デ バイスのパワー制御 『377p. 』」を参照してください。



上記のどの方法でも、管理対象電源タップ インタフェースをノードに 追加して、コンセントとその電源供給対象のノードの間でパワー関連を 作成する必要があります。「*管理対象電源タップ接続用インタフェース* 『**146**p. 』」を参照してください。

Dominion PX に関する特別な注意

PX の設定にいずれの方法を選択しても、すべてのパワー関連を単一の 方法で、すなわち管理対象デバイスの電源タップとしてか、PX デバイ スとして (両方ではない) 設定する必要があります。Dominion PX が Power IQ によって管理されている場合は、ノードのパワー制御 - 管理 対象電源タップ インタフェース、またはパワー制御 - Power IQ Proxy インタフェース (両方ではない)を作成できます。

さらに、PX を管理デバイスに接続してパワー関連を設定することも、 同じ PX デバイスを IP ネットワークに接続し、PX Web クライアント を使用してパワー データを表示および収集することもできます。 Raritan Web サイトのサポート セクションのファームウェアおよびマ ニュアルにある Raritan 『Dominion PX ユーザ ガイド』を参照してく ださい。

この章の内容

CC-SG 内の別のデバイスによって管理される電源タッ	アの設定107
KX、KX2、KX2-101、KSX2、P2SC に接続された電源	原タップの設定 108
SX 3.0 および KSX に接続された電源タップの設定	109
SX 3.1 に接続された電源タップの設定	111
電源タップのコンセントの設定	113



CC-SG 内の別のデバイスによって管理される電源タップの設定

CC-SG では、次のいずれかのデバイスに管理対象電源タップを接続することができます。

- Dominion KX
- Dominion KX2
- Dominion KX2-101
- Dominion SX 3.0
- Dominion SX 3.1
- Dominion KSX
- Dominion KSX2
- Paragon II/Paragon II システム コントローラ (P2SC)
- Power IQ 「*Power IQ IT デバイスのパワー制御* 『377p. 』」を参照してください。

管理対象電源タップが物理的に接続されている Raritan デバイスを認識 している必要があります。

注: IP ネットワークに接続されているが、他のどの Raritan デバイスに も接続されていない Dominion PX 電源タップを使用することもできま す。これらの電源タップのパワー制御設定の詳細は、「管理対象電源タ ップ 『105p. 』」を参照してください。

- ▶ CC-SG で管理対象電源タップを設定するには、以下の手順に従い ます。
- デバイス、電源タップ、および電源タップにより電力が供給されているノードをすべて物理的に接続します。電源タップ、デバイス、およびノード間の物理接続の詳細は、『RPC Quick Setup Guide』、 『Dominion PX クイック スタート ガイド』、および『CC-SG デプロメント ガイド』を参照してください。
- 管理デバイスを CC-SG に追加します。手順は、Raritan デバイス によって異なります。次のうち、電源タップが接続されているデバ イスに対応するセクションを参照してください。
 - KX、KX2、KX2-101、KSX2、P2SC に接続された電源タップ の設定 『108p. 』
 - SX 3.0 および KSX に接続された電源タップの設定 『109p. 』
 - SX 3.1 に接続された電源タップの設定 『111p. 』
- 3. コンセントを設定します。「**電源タップでのコンセントの設定**『 113p. の"**電源タップのコンセントの設定**"参照 』」を参照してくだ さい。
- 各コンセントを、電力の供給先のノードと関連付けます。「 管理対象 電源タップ接続用インタフェース 『146p. 』」を参照してください



KX、KX2、KX2-101、KSX2、P2SC に接続された電源タップの設定

CC-SG では、KX、KX2、KX2-101、KSX2、P2SC デバイスに接続された電源タップが自動的に検出されます。CC-SG で次のタスクを実行すると、これらのデバイスに接続された電源タップを設定および管理できます。

- KX、KX2、KX2-101、KSX2、または P2SC デバイスに接続された 電源タップ デバイスの追加 『108p. 』
- KX、KX2、KX2-101、KSX2、または P2SC の電源タップの別のポ ートへの移動『108p.』
- KX、KX2、KX2-101、KSX2、または P2SC デバイスに接続された 電源タップの削除 『109p. 』

KX、KX2、KX2-101、KSX2、または **P2SC** デバイスに接続された電 源タップ デバイスの追加

電源タップに接続された KX、KX2、KX2-101、KSX2、または P2SC デバイスを CC-SG に追加すると、電源タップが自動的に追加されます 。電源タップは、[デバイス] タブで、接続されたデバイスの下に表示さ れます。

次に、以下の手順に従います。

- コンセントを設定します。「**電源タップでのコンセントの設定**『 113p. の"**電源タップのコンセントの設定**"参照 』」を参照してくだ さい。
- 2. 各コンセントを、電力の供給先のノードと関連付けます。「*管理対象 電源タップ接続用インタフェース* 『146p. 』」を参照してください

KX、KX2、KX2-101、KSX2、または **P2SC** の電源タップの別のポー トへの移動

KX、KX2、KX2-101、KSX2、または P2SC の各デバイスまたはポート に接続された電源タップを、別の KX、KX2、KX2-101、KSX2、または P2SC の各デバイスまたはポートに物理的に移動すると、CC-SG によ り電源タップが自動的に検出され、正しいデバイスになるようにその関 連が更新されます。電源タップを CC-SG に別個に追加する必要はあり ません。

注: 電源タップを P2SC ポートから物理的に取り外したが、別のポート に接続しない場合、CC-SG で電源タップは古いポートから削除されま せん。電源タップが接続されている UMT の部分または完全データベー ス リセットを実行して、電源タップを [デバイス] タブから削除する必 要があります。『Raritan P2SC ユーザ ガイド』を参照してください。



KX、KX2、KX2-101、KSX2、または **P2SC** デバイスに接続された電 源タップの削除

KX、KX2、KX2-101、KSX2、または P2SC デバイスに接続された電源 タップを CC-SG から削除することはできません。電源タップをデバイ スから物理的に取り外して、電源タップを CC-SG から削除する必要が あります。電源タップをデバイスから物理的に取り外すと、電源タップ と設定されたすべてのコンセントは [デバイス] タブに表示されなくな ります。

SX 3.0 および KSX に接続された電源タップの設定

CC-SG で次のタスクを実行すると、**SX 3.0** デバイスと **KSX KX** デバイスに接続された電源タップを設定および管理できます。

注: 電源タップは、KSX デバイスのパワー ポートに物理的に接続する 必要があります。

- SX 3.0 デバイスまたは KSX デバイスに接続された電源タップの追加 『109p. 』
- SX 3.0 デバイスまたは KSX デバイスに接続された電源タップの削除 『110p. 』
- ・ 電源タップのデバイスまたはポートの関連の変更 (SX 3.0、KSX)
 『111p. 』

SX 3.0 デバイスまたは KSX デバイスに接続された電源タップの追加

- SX 3.0 デバイスまたは KSX デバイスを CC-SG に追加します。 「KVM またはシリアル デバイスの追加 『61p. 』」を参照してく ださい。
- 2. [デバイス]>[デバイス マネージャ]>[デバイスの追加] を選択します。
- [デバイス タイプ] ドロップダウン メニューをクリックし、[電源タップ] を選択します。
- 電源タップの名前を [電源タップ名] フィールドに入力します。カー ソルをフィールドの上に置いたままにし、名前に使用できる文字数 を参照します。スペースは使用できません。
- 5. [アウトレット数] ドロップダウン メニューをクリックし、この電源 タップに含まれるコンセント数を選択します。
- 6. [管理デバイス] ドロップダウン メニューをクリックし、この電源タ ップに接続されている SX 3.0 デバイスまたは KSX デバイスを選 択します。
- [管理ポート] ドロップダウン メニューをクリックし、この電源タッ プが接続されている SX 3.0 デバイスまたは KSX デバイスのポー トを選択します。



- 8. この電源タップの短い説明を [説明] フィールドに入力します。オプ ション。
- この電源タップ デバイスの各コンセントを [デバイス] タブに自動 的に追加する場合は、[すべてのアウトレットを設定] を選択します 。すべてのコンセントをすぐに設定しない場合は、後で設定するこ とができます。「電源タップでのコンセントの設定 『113p. の" 電源 タップのコンセントの設定 参照 』」を参照してください。オプショ ン。
- リストされている [カテゴリ] ごとに、[エレメント] ドロップダウン メニューをクリックし、デバイスに適用するエレメントを選択しま す。不要な [カテゴリ] については、それぞれの [エレメント] フィ ールドで空白の項目を選択します。「*関連、カテゴリ、エレメント* 『47p.』」を参照してください。オプション。
- この電源タップの設定が完了して、[適用] をクリックすると、この デバイスが追加され、新しいブランクの [デバイスの追加] 画面が開 きます。この画面で引き続きデバイスを追加することができます。
 [OK] をクリックすると、この電源タップが追加されますが、新たに [デバイスの追加] 画面は表示されません。

次に、以下の手順に従います。

- コンセントを設定します。「*電源タップでのコンセントの設定*『 113p. の"*電源タップのコンセントの設定*"参照 』」を参照してくだ さい。
- 2. 各コンセントを、電力の供給先のノードと関連付けます。「*管理対象 電源タップ接続用インタフェース* 『146p. 』」を参照してください

SX 3.0 デバイスまたは KSX デバイスに接続された電源タップの削除

SX 3.0、KSX、または P2SC の各デバイスに接続された電源タップは、物理的に接続されたままの状態であっても画面から削除できます。関連付けられた SX 3.0、KSX、または P2SC の各デバイスから電源タッ プを物理的に取り外しても、[デバイス] タブにはその電源タップが該当 デバイスの下にまだ表示されています。画面から削除するには、電源タッ ップを削除する必要があります。

- 1. [デバイス] タブで、削除する電源タップを選択します。
- [デバイス]>[デバイス マネージャ]>[デバイスの削除] を選択します。
- [OK] をクリックして、電源タップを削除します。電源タップが削除 されるとメッセージが表示されます。電源タップのアイコンが [デ バイス] タブから削除されます。



電源タップのデバイスまたはポートの関連の変更 (SX 3.0、KSX)

SX 3.0、KSX の各デバイスまたはポートに接続された電源タップを別 の SX 3.0、KSX の各デバイスまたはポートに物理的に移動した場合、 CC-SG の電源タップのプロファイルで関連を変更する必要があります

- 1. [デバイス] タブで、移動された電源タップを選択します。
- 2. [管理デバイス] ドロップダウン メニューをクリックし、この電源タ ップに接続されている SX 3.0 デバイスまたは KSX デバイスを選 択します。
- 3. [管理ポート] ドロップダウン メニューをクリックし、この電源タッ プが接続されている SX 3.0 デバイスまたは KSX デバイスのポー トを選択します。
- 4. [OK] をクリックします。

SX 3.1 に接続された電源タップの設定

CC-SG で次のタスクを実行すると、**SX 3.1** デバイスに接続された電源 タップを設定および管理できます。

- SX 3.1 デバイスに接続された電源タップの追加 『111p. 』
- SX 3.1 の電源タップの別のポートへの移動 『112p. 』
- SX 3.1 デバイスに接続された電源タップの削除 『112p. 』

SX 3.1 デバイスに接続された電源タップの追加

SX 3.1 デバイスに接続された電源タップの追加手順は、SX 3.1 デバイ スが CC-SG に追加されているかどうかによって異なります。

電源タップが SX 3.1 デバイスに接続されており、デバイスがまだ CC-SG に 追加されていない場合:

- CC-SG へ SX 3.1 デバイスを追加します。「KVM またはシリアル デバイスの追加 『61p. 』」を参照してください。
- 2. CCSG により電源タップが検出され、自動的に追加されます。電源 タップは、[デバイス] タブで、接続された SX 3.1 デバイスの下に 表示されます。

SX 3.1 デバイスがすでに **CC-SG** に追加されていて、後で電源タップがデバイ スに接続された場合:

- 1. CC-SG へ SX 3.1 デバイスを追加します。「KVM またはシリアル デバイスの追加 『61p. 』」を参照してください。
- SX 3.1 デバイスのポートの設定。「ポートの設定 『67p. 』」を参照してください。



- 3. [デバイス] タブで、電源タップが接続されている SX 3.1 デバイス を選択します。
- 4. デバイス アイコンの横の + 記号をクリックすると、ポートのリス トが拡張されます。
- 5. 電源タップが接続されている SX 3.1 ポートを右クリックし、ポッ プアップ メニューから [電源タップの追加] を選択します。
- 6. 電源タップに含まれるコンセントの数を入力し、[OK] をクリックし ます。

次に、以下の手順に従います。

- コンセントを設定します。「*電源タップでのコンセントの設定*『
 113p. の"*電源タップのコンセントの設定*"参照 』」を参照してください。
- 2. 各コンセントを、電力の供給先のノードと関連付けます。「*管理対象 電源タップ接続用インタフェース* 『146p. 』」を参照してください

SX 3.1 の電源タップの別のポートへの移動

SX 3.1 デバイスまたはポートに接続された電源タップを別の SX 3.1 デバイスまたはポートに物理的に移動した場合、古い SX 3.1 ポートか ら電源タップを削除して、新しい SX 3.1 ポートに追加する必要があり ます。「SX 3.1 デバイスに接続された電源タップの削除 『112p. 』」 および「SX 3.1 デバイスに接続された電源タップの追加 『111p. 』」 を参照してください。

SX 3.1 デバイスに接続された電源タップの削除

SX 3.1 デバイスに物理的に接続されたままの状態の電源タップであっても、画面から削除できます。関連付けられた SX 3.1 デバイスから物理的に取り外した電源タップは、[デバイス] タブでそのデバイスの下にまだ表示されています。画面から削除するには、電源タップを削除する必要があります。

- SX 3.1 デバイスに接続された電源タップを削除するには、以下の手順に従います。
- 1. [デバイス] タブで、削除する電源タップを選択します。
- 2. [デバイス]>[デバイス マネージャ]>[デバイスの削除] を選択します。
- 3. [OK] をクリックして、電源タップを削除します。電源タップが削除 されるとメッセージが表示されます。電源タップのアイコンが [デ バイス] タブから削除されます。



電源タップのコンセントの設定

電源タップ コンセントをノードに関連付ける前に、管理対象電源タッ プ インタフェースをそのノードに追加して、そのコンセントを設定す る必要があります。「*管理対象電源タップ接続用インタフェース*『146p. 』」を参照してください。

- 電源タップ プロファイルからコンセントを設定するには、以下の手順に従います。
- 1. [デバイス] タブで、電源タップに接続されているデバイスの横の + をクリックします。
- 2. 設定するコンセントがある電源タップを選択します。
- 3. [デバイス プロファイル]: 電源タップ] 画面で、[アウトレット] タブ を選択します。
- 4. 設定する各コンセントのチェックボックスを選択し、[OK] をクリッ クします。

[デバイス] タブの電源タップ アイコンの下にコンセントが表示されます。

- [ポートの設定] 画面からコンセントを設定するには、以下の手順に 従います。
- 1. [デバイス] タブで、電源タップに接続されているデバイスの横の + をクリックします。
- 2. 設定するコンセントがある電源タップを選択します。
- 3. [デバイス]>[ポート マネージャ]>[ポートの設定] を選択します。
 - 画面に表示されたデフォルト名を持つ複数のコンセントを設定 するには、設定する各コンセントのチェックボックスを選択し 、[OK] をクリックしてデフォルト名を持つ各コンセントを設定 します。
 - 各コンセントを個別に設定するには、コンセントの横の[設定] ボタンをクリックし、コンセントの名前を[ポート名]フィール ドに入力します。[OK]をクリックして、ポートを設定します。
- ▶ コンセントを削除するには、以下の手順に従います。
- 1. [デバイス] タブで、電源タップに接続されているデバイスの横の + をクリックします。
- 2. 電源タップの横の + をクリックします。
- 3. [デバイス]>[ポート マネージャ]>[ポートの削除] を選択します。
- 4. 削除する各コンセントのチェックボックスを選択し、[OK] をクリッ クしてコンセントを削除します。



ノード、ノード グループ、インタフ エース

本章では、ノードとノードに関連付けられるインタフェースの表示、設定、および編集方法と、ノード グループの作成方法について説明します。ノードへの接続については簡単に説明します。ノードへの接続についての詳細は、Raritan の『CommandCenter Secure Gateway ユーザ ガイド』を参照してください。

この章の内容

 ノードの表示	ノードとインタフェースの概要	115
サービス アカウント119ノードの追加、編集、および削除123ノード プロファイルへの場所と連絡先の追加125ノード プロファイルへの注意の追加125CC-SG での仮想インフラストラクチャの設定126仮想ホスト ノードのリブートまたは強制リブート137仮想ホスト ノードのリブートまたは強制リブート138[Virtual Topology] (仮想トポロジー) 表示へのアクセス138ノードへの接続139ノードへの回回 の実行139インタフェースの追加、編集、削除140インタフェースをブックマークに設定152ノードへのダイレクト ポート アクセスの設定153ノードの関連、場所、および連絡先の一括コピー155CSV ファイルのインポートによるノードの追加156CSV ファイルのインポートを利用した IP アドレスの編集169ノード グループの追加、編集、削除170	ノードの表示	116
 ノードの追加、編集、および削除	サービス アカウント	119
 ノード プロファイルへの場所と連絡先の追加	ノードの追加、編集、および削除	123
 ノード プロファイルへの注意の追加	ノード プロファイルへの場所と連絡先の追加	125
CC-SG での仮想インフラストラクチャの設定126仮想インフラストラクチャと CC-SG の同期137仮想ホスト ノードのリブートまたは強制リブート138[Virtual Topology] (仮想トポロジー) 表示へのアクセス138ノードへの接続139ノードへの ping の実行139インタフェースの追加、編集、削除140インタフェースをブックマークに設定152ノードへのダイレクト ポート アクセスの設定153ノードの関連、場所、および連絡先の一括コピー154チャットの使用155CSV ファイルのインポートによるノードの追加156CSV ファイルのインポートを利用した IP アドレスの編集169ノード グループの追加、編集、削除170	ノード プロファイルへの注意の追加	125
 仮想インフラストラクチャと CC-SG の同期	CC-SG での仮想インフラストラクチャの設定	126
仮想ホスト ノードのリブートまたは強制リブート	仮想インフラストラクチャと CC-SG の同期	137
[Virtual Topology] (仮想トポロジー)表示へのアクセス	仮想ホスト ノードのリブートまたは強制リブート	138
 ノードへの接続	[Virtual Topology] (仮想トポロジー) 表示へのアクセス	138
 ノードへの ping の実行	ノードへの接続	139
インタフェースの追加、編集、削除140インタフェースをブックマークに設定152ノードへのダイレクト ポート アクセスの設定153ノードの関連、場所、および連絡先の一括コピー154チャットの使用155CSV ファイルのインポートによるノードの追加156CSV ファイルのインポートを利用した IP アドレスの編集169ノード グループの追加、編集、削除170	ノードへの ping の実行	139
 インタフェースをブックマークに設定	インタフェースの追加、編集、削除	140
 ノードへのダイレクト ポート アクセスの設定	インタフェースをブックマークに設定	152
 ノードの関連、場所、および連絡先の一括コピー154 チャットの使用	ノードへのダイレクト ポート アクセスの設定	153
 チャットの使用	ノードの関連、場所、および連絡先の一括コピー	154
CSV ファイルのインポートによるノードの追加156 CSV ファイルのインポートを利用した IP アドレスの編集169 ノード グループの追加、編集、削除170	チャットの使用	155
CSV ファイルのインポートを利用した IP アドレスの編集169 ノード グループの追加、編集、削除170	CSV ファイルのインポートによるノードの追加	156
ノード グループの追加、編集、削除170	CSV ファイルのインポートを利用した IP アドレスの編集	169
	ノード グループの追加、編集、削除	170



ノードとインタフェースの概要

ノードについて

各ノードは、インバンド (直接 IP) またはアウト オブ バンド (Raritan デバイスに接続) のいずれかの方法で CC-SG を介してアクセス可能な ターゲットを表しています。たとえば、ノードは、IP デバイスを介し て Raritan KVM に接続されるラックのサーバ、HP iLO カードを備えた サーバ、VNC を実行しているネットワーク上の PC、リモート シリア ル管理接続を備えたネットワーク インフラストラクチャの一部などに なります。

接続されているデバイスを追加した後で、CC-SG にノードを手動で追 加できます。ノードは、デバイスを追加する際に、[デバイスの追加] 画 面の [すべてのポートの設定] チェックボックスを選択することで、自 動的に作成することもできます。このオプションを使用すると、CC-SG ですべてのデバイス ポートを自動的に追加し、ノード、アウト オブ バンド KVM または各ポートのシリアル インタフェースを追加できる ようになります。これらのノード、ポート、インタフェースは、いつで も編集できます。

ノードの名前

ノードには、固有の名前が必要です。既存のノード名を持つノードを手動で追加しようとすると、CC-SG により、オプションが表示されます。 CC-SG が自動でノードを追加する場合は、固有のノード名を付けるため、ナンバリングシステムにより固有の名前が付けられます。 名前の長さに関する CC-SG のルールについての詳細は、「命名規則『 435p. 』」を参照してください。



Ch 8: ノード、ノード グループ、インタフェース

インタフェースについて

CC-SG では、ノードにはインタフェースを介してアクセスします。新 しいノードには、少なくとも 1 つのインタフェースを追加する必要が あります。ノードには、異なるタイプのインタフェースを追加し、ノー ドのタイプによって、アウト オブ バンド KVM またはシリアル、パワ ー制御、インバンド SSH/RSA/VNC、DRAC/RSA/ILO、Web、Telnet アクセスなど、異なるタイプのアクセスを可能にできます。

複数のインタフェースを使用できますが、アウト オブ バンド シリア ルまたは KVM インタフェースは 1 つだけです。たとえば、Windows サーバには、キーボード、マウス、モニタ ポート、パワー インタフェ ース用のアウト オブ バンド KVM インタフェースを設定し、接続され ているコンセントを管理できます。

CC-SG でプロキシ モードを使用するように設定している場合であって も、一部のインタフェースはダイレクト モードでのみ機能します。こ のようなインタフェースには、ILO、RSA、Microsoft RDP、DRAC、 Web ブラウザ、VMware Viewer があります。Java RDP インタフェー スはプロキシ モードで使用できます。「接続モードについて『280p.』 」を参照してください。

ノードの表示

CC-SG では、すべてのノードを [ノード] タブで表示し、ノードを選択 して、そのノード固有のプロファイルを表示できます。

[ノード] タブ

[ノード] タブをクリックすると、アクセス可能なすべてのノードがツリ ー構造に表示されます。

ノードは名前のアルファベット順に表示されるか、または利用可能なス テータスごとに分類されます。利用可能なステータスごとに分類された ノードは、グループ内でアルファベト順に配列されます。配列方法を変 更する場合は、ツリーを右クリックして、[ノード並べ替えオプション] をクリックし、さらに [ノード名でソート] または [ノード ステータス でソート] をクリックします。

各種の方法での [ノード] タブの表示についての詳細は、「*デバイスおよ びノードのカスタム表示* 『202p. 』」参照してください。



ノード プロファイル

[ノード] タブでノードをクリックして、[ノード プロファイル] ページ を開きます。[ノード プロファイル] ページには、ノードに関する情報 を含むタブがあります。

🕨 [インタフェース] タブ

[インタフェース] タブには、ノードの全インタフェースが含まれます。 このタブでインタフェースを追加、編集、削除したり、デフォルト イ ンタフェースを選択したりできます。仮想メディアをサポートするノー ドには、仮想メディアが有効になっているかどうかを示す追加の列も表 示されます。

▶ [関連] タブ

[関連] タブには、ノードに割り当てられたすべてのカテゴリとエレメン トが含まれます。関連を変更するには、選択を変更します。

「*関連、カテゴリ、エレメント* 『47p. 』」を参照してください。

▶ [場所 & 連絡先] タブ

[場所 & 連絡先] タブには、デバイスに対して作業を行っている際に必要になる場合があるデバイスの場所と連絡先に関する情報 (電話番号など) が含まれます。フィールド内の情報は、新しい情報を入力して変更できます。

「ノード プロファイルへの場所と連絡先の追加 『125p. 』」を参照してください。

🕨 [メモ] タブ:

[メモ] タブには、他のユーザの参照用にデバイスに関するメモを残して おくことができるツールがあります。タブ内のすべてのメモには、メモ を追加した時点の日付、ユーザのユーザ名と IP アドレスが表示されま す。

デバイス、ポート、ノードの管理権限がある場合は、ノード プロファ イルからすべてのメモをクリアすることができます。[クリア] ボタンを クリックします。

「ノード プロファイルに関するメモの追加『125p. の"ノード プロファ イルへの注意の追加'参照 』」を参照してください

▶ [監査] タブ

[監査] タブでノードがアクセスされた理由を表示できます。ノード監査 がユーザ グループに対して有効になっていた場合、ノードに接続する 前に、アクセスの理由を入力する必要があります。



Ch 8: ノード、ノード グループ、インタフェース

ノード監査機能が無効になっている場合、または、ノードにアクセスす る理由がまったく入力されていない場合、[監査] タブは表示されません 。

「**ユーザ グループのアクセス監査の設定 『183**p. **』**」を参照してください。

▶ [制御システム データ] タブ

VMware の Virtual Center などの制御システム サーバ ノードには、[制御システム データ] タブがあります。[制御システム データ] タブに は、制御システム サーバ ノードからの情報が含まれ、この情報は、こ のタブが開くたびに更新されます。仮想インフラストラクチャのトポロ ジ表示にアクセスしたり、関連ノード プロファイルにリンクしたり、 制御システムに接続して [概要] タブを開いたりできます。

▶ [仮想ホスト データ] タブ

VMware の ESX サーバなどの仮想ホスト ノードには、[仮想ホスト デ ータ] タブがあります。[仮想ホスト データ] タブには、仮想ホスト サ ーバからの情報が含まれ、この情報は、このタブが開くたびに更新され ます。仮想インフラストラクチャのトポロジ表示にアクセスしたり、関 連ノード プロファイルにリンクしたり、仮想ホストに接続して [概要] タブを開いたりできます。デバイス、ポート、ノードの管理許可がある 場合、仮想ホスト サーバのリブートおよび強制リブートを行うことが できます。

[Virtual Machine Data] (仮想マシン データ) タブ

VMware の仮想マシンなどの仮想マシン ノードには、[Virtual Machine Data] (仮想マシン データ) タブがあります。[Virtual Machine Data] (仮 想マシン データ) タブには、仮想マシンからの情報が含まれ、この情報 は、このタブが開くたびに更新されます。仮想インフラストラクチャの トポロジ表示にアクセスしたり、関連ノード プロファイルにリンクし たり、仮想ホストに接続して [概要] タブを開いたりできます。

▶ [ブレード] タブ

IBM BladeCenter などのブレード シャーシ ノードには、[ブレード] タ ブが含まれます。[ブレード] タブには、ブレード シャーシに常駐する ブレード サーバについての情報が表示されます。



ノードとインタフェースのアイコン

区別しやすいように、各ノードをツリーに個別のアイコンで表します。 マウス ポインタをノード ツリーのアイコンに合わせると、ノードに関 する情報を含むツールのヒントが表示されます。

アイコン	意味
	ノードは利用可能 - ノードには、アップされているインタ フェースが少なくとも 1 つあります。
с г	ノードは利用不可能 - ノードには、アップされているイン タフェースがありません。

サービス アカウント

サービス アカウントの概要

サービス アカウントは、複数のインタフェースに割り当てることがで きる特殊なログイン資格認定です。パスワード変更が必要になることが 多いインタフェースのセットにサービス アカウントを割り当てると、 時間の節約になります。サービス アカウント内のログイン資格認定を 更新できます。この変更は、このサービス アカウントを使用するすべ てのインタフェースに反映されます。

アウトオブバンド インタフェースまたは管理対象電源タップインタフ ェースには、サービス アカウントを使用できません。

- DRAC、iLO、RSA インタフェースの場合、ログイン インタフェー スは基盤 OS ではなく、内蔵プロセッサ カードに適用されます。
- RDP、SSH、Telnet インタフェースの場合、ログイン資格認定は OS に適用されます。
- VNC インタフェースの場合、ログイン資格認定は VNC サーバに 適用されます。
- Web ブラウザの場合、ログイン資格認定は、インタフェースで指定 された URL で使用可能なフォームに適用されます。
- ▶ サービス アカウントを表示するには、以下の手順に従います。
- [ノード]>[サービス アカウント] を選択します。[サービス アカウント] ページが開きます。
- 列のヘッダをクリックすると、テーブルがその属性によって昇順に 並べ替えられます。ヘッダを再度クリックすると、テーブルが降順 に並び替わります。オプション。



Ch 8: ノード、ノード グループ、インタフェース

フィールド	説明
サービス アカウント名	この名前は、インタフェース ダイアログおよび [サ ービス アカウントの割り当て] ページでサービス ア カウントを特定するために使用されます。
ユーザ名	このユーザ名は、サービス アカウントがインタフェ ースに割り当てられる際に、ログイン資格認定の一部 として使用されます。
パスワード	このパスワードは、サービス アカウントがインタフ ェースに割り当てられる際に、ログイン資格認定の一 部として使用されます。
パスワードの再入力	このフィールドは、パスワードが正しく入力されたこ との確認に使用されます。
説明	この説明には、サービス アカウントに関して追加す る補足の情報を含めることができます。

サービス アカウントの追加、編集、削除

- ▶ サービス アカウントを追加するには、以下の手順に従います。
- [ノード]>[サービス アカウント] を選択します。[サービス アカウント] ページが開きます。
- 3. このサービス アカウントの名前を [サービス アカウント名] フィー ルドに入力します。
- 4. ユーザ名を [ユーザ名」フィールドに入力します。
- 5. パスワードを [パスワード] フィールドに入力します。
- 6. パスワードを [パスワード再入力] フィールドに再入力します。
- 7. このサービス アカウントの説明を [説明] フィールドに入力します。
- 8. [OK] をクリックします。

▶ サービス アカウントを編集するには、以下の手順に従います。

- [ノード]>[サービス アカウント] を選択します。[サービス アカウント] ページが開きます。
- 2. 編集するサービス アカウントを見つけます。
- 3. 各フィールドを編集します。[サービス アカウント名] は編集できま せん。



Ch 8: ノード、ノード グループ、インタフェース

注: ユーザ名またはパスワードを変更すると、CC-SG は、新しいロ グイン資格認定にこのサービス アカウントを使用するすべてのイン タフェースを更新します。

- 4. [OK] をクリックします。
- ▶ サービス アカウントを削除するには、以下の手順に従います。
- [ノード]>[サービス アカウント] を選択します。[サービス アカウント] ページが開きます。
- 2. 削除するサービス アカウントを選択します。
- [行の削除] ボタン
 をクリックします。
- 4. [OK] をクリックします。

サービス アカウントのパスワードの変更

- サービス アカウントのパスワードを変更するには、以下の手順に従います。
- [ノード]>[サービス アカウント] を選択します。[サービス アカウント] ページが開きます。
- 2. パスワードが変更されるサービス アカウントを見つけます。
- 3. 新しいパスワードを [パスワード] フィールドに入力します。
- 4. パスワードを [パスワード再入力] フィールドに再入力します。
- 5. [OK] をクリックします。

注: ユーザ名またはパスワードを変更すると、CC-SG は、新しいログ イン資格認定にこのサービス アカウントを使用するすべてのインタフ ェースを更新します。



サービス アカウントをインタフェースに割り当て

1 つのサービス アカウントを複数のインタフェースに割り当てること ができます。サービス アカウントが割り当てられる各インタフェース では、接続用に同じログイン情報が使用されます。

ユーザ名またはパスワードを変更すると、CC-SG は、新しいログイン 資格認定にこのサービス アカウントを使用するすべてのインタフェー スを更新します。

インタフェースの設定時に、サービス アカウントを選択することもで きます。「*インタフェースの追加、編集、削除* 『140p. 』」を参照して ください。

サービス アカウントをインタフェースに割り当てるには、デバイス、 ポート、ノードの管理権限が必要です。「**ユーザ グループの追加、編集** 、**削除** 『**179**_D. 』」を参照してください。

- サービス アカウントをインタフェースに割り当てるには、以下の手順に従います。
- [ノード] > [Assign Service Account] (サービス アカウントの割り当 て) を選択します。[Assign Service Account] (サービス アカウント の割り当て) ページが開きます。
- 2. [サービス アカウント名] フィールドで、ノードに割り当てるサービ ス アカウントを選択します。
- 3. [利用可能] リストで、サービス アカウントが割り当てられるインタ フェースを選択します。Ctrl または Shift を押しながらクリックす ると、一度に複数のインタフェースを選択できます。

ヒント: ノード名を検索フィールドに入力するとリスト内のノード 名がハイライトされます。部分名の後に * を入力すると、リスト内 の類似したすべての名前がハイライトされます。

列のヘッダをクリックすると、リストがアルファベット順に並べ替 えられます。

- 4. [追加] をクリックして、選択したインタフェースを [選択中] リスト に移動します。
- 5. [OK] をクリックします。サービス アカウントが [選択中] リスト中 のすべてのノードに割り当てられます。

注: ユーザ名またはパスワードを変更すると、CC-SG は、新しいログ イン資格認定にこのサービス アカウントを使用するすべてのインタフ ェースを更新します。



ノードの追加、編集、および削除

ノードの追加

- ▶ CC-SG にノードを追加するには、以下の手順に従います。
- 1. [ノード] タブをクリックします。
- 2. [ノード]>[ノードの追加]を選択します。
- [ノード名] フィールドにノードの名前を入力します。CC-SG の全 ノードには、固有の名前が必要です。名前の長さに関する CC-SG のルールについての詳細は、「命名規則 『435p. 』」を参照してく ださい。
- 4. このノードの短い説明を [説明] フィールドに入力します。オプション。
- 少なくとも 1 つのインタフェースを設定する必要があります。[ノ ードの追加] 画面の [インタフェース] 領域で [追加] をクリックし 、インタフェースを追加します。「インタフェースの削除『140p. の "インタフェースの追加参照 』」を参照してください。
- [カテゴリ] および [エレメント] のリストは、このノードをわかりや すく整理するために設定することができます。「*関連、カテゴリ、エ レメント* 『47p. 』」を参照してください。オプション。
 - 各 [カテゴリ] で、[エレメント] ドロップダウン メニューをク リックし、リストからノードに適用するエレメントを選択しま す。

注: デフォルトで、CC-SG では、デフォルト カテゴリ名 "System Type" および "US States and territories" は英語のままになります

- 不要な [カテゴリ] については、それぞれの [エレメント] フィ ールドで空白の項目を選択します。
- 使用する [カテゴリ] または [エレメント] 値が表示されない場合は、[関連] メニューから追加できます。「関連、カテゴリ、エレメント 『47p. 』」を参照してください。
- 7. [OK] をクリックして変更を保存します。ノードがノードのリストに 追加されます。

重要: ブレード シャーシをある Dominion デバイス ポートから別の Dominion デバイス ポートに移動する場合、CC-SG でブレード シャー シ ノードに追加されたインタフェースが CC-SG で失われます。他の情 報はすべて維持されます。



ポートの設定により作成されるノード

デバイスのポートを設定すると、ポートごとにノードが自動的に作成さ れます。インタフェースもノードごとに作成されます。

ノードが自動的に作成されると、関連付けられたポートと同じ名前が付けられます。このノード名がすでに存在する場合は、ノード名に拡張部分が追加されます。たとえば、Channel1(1)などです。拡張部分は、数字をカッコで囲んだものです。この拡張部分は、ノード名の文字数には含まれません。ノード名を編集した場合、新しい名前は最大文字数によって制限されます。「命名規則『435p.』」を参照してください。

ノードの編集

ノードを編集すると、その名前、説明、インタフェース、デフォルト インタフェース、または関連を変更できます。

ノードを編集するには、以下の手順に従います。

- 1. [ノード] タブをクリックし、編集するノードを選択します。[ノード プロファイル] 画面が表示されます。
- 2. 必要に応じてフィールドを編集します。
- 3. [OK] をクリックして変更を保存します。

注 1: ブレード シャーシのノード名を変更しても、そのシャーシ名は変 更されません。シャーシ名を変更するには、[デバイス プロファイル] 画面で編集します。「ブレード シャーシ デバイスの編集 『75p. 』」 を参照してください。

注 2: 仮想ホスト ノードまたは仮想制御システム ノードのノード名を 変更すると、仮想化テーブル内の名前も変更されます。

ノードの削除

ノードを削除すると、[ノード] タブからそのノードが消えます。ユーザ がノードにアクセスすることができなくなります。ノードを削除すると 、すべてのインタフェース、関連、および関連付けられたポートが削除 されます。

▶ ノードを削除するには、以下の手順に従います。

- 1. [ノード] タブで、削除するノードを選択します。
- 2. [ノード]>[ノードの削除] を選択します。[ノードの削除] 画面が表示されます。
- 3. [OK] をクリックして、ノードを削除します。



 [はい]をクリックして、ノードを削除するとインタフェースおよび 関連付けられたポートもすべて削除されることを確認します。削除 が完了すると、削除されたすべてのアイテムのリストが表示されま す。

ノード プロファイルへの場所と連絡先の追加

ノードの場所に関する詳細およびノードを管理または使用する人物の連 絡先情報を入力します。

- ノード プロファイルに場所および連絡先を追加するには、以下の手順に従います。
- [ノード] タブでノードを選択します。[ノード プロファイル] ページ が開きます。
- 2. [Location & Contacts] (場所&連絡先) タブをクリックします。
- 3. 場所情報を入力します。
 - Department:最大 64 文字です。
 - Site:最大 64 文字です。
 - Location:最大 128 文字です。
- 4. 連絡先情報を入力します。
 - 主連絡先名と二次連絡先名:最大 64 文字です。
 - 電話番号と携帯電話番号:最大 32 文字です。
- 5. [OK] をクリックして変更を保存します。

ノード プロファイルへの注意の追加

[Notes](注意)タブを使用すると、他のユーザの参照用にノードに関する注意を追加できます。すべてのメモがこのタブに表示されます。その際、メモが追加された日付、および、メモを追加したユーザの名前と IP アドレスも表示されます。

デバイス、ポート、ノードの管理権限がある場合は、[Notes](注意)タブに表示されるすべての注意をクリアすることができます。

- ノード プロファイルに注意を追加するには、以下の手順に従います。
- [ノード] タブでノードを選択します。[ノード プロファイル] ページ が開きます。
- 2. [Notes] (注意) タブをクリックします。
- 3. 注意を [New Notes] (新しい注意) フィールドに入力します。
- 4. [追加] をクリックします。注意が [Notes] (注意) リストに表示され ます。



Ch 8: ノード、ノード グループ、インタフェース

- ▶ すべての注意をクリアするには、以下の手順に従います。
- 1. [Notes] (注意) タブをクリックします。
- 2. [Clear Notes] (注意のクリア) をクリックします。
- 3. [はい] をクリックして確認します。すべての注意が [Notes] (注意) タブから削除されます。

CC-SG での仮想インフラストラクチャの設定

仮想インフラストラクチャの用語

CC-SG では、仮想インフラストラクチャ コンポーネントに以下の用語 を使用します。

用語	定義	例
制御システム	制御システムは管理サーバです。制御システムは、1 つ以上の仮想ホストを管理します。	VMware Ø Virtual Center
仮想ホスト	仮想ホストは、1 つ以上の仮想マシンを含む物理 ハードウェアです。	VMware O ESX
仮想マシン	仮想マシンは、仮想ホストに存在する仮想「サー バ」です。仮想マシンは、別の仮想ホストにリロ ケートできます。	VMware の仮想マシン (VM)
VI クライアント インタフェース	制御システム ノードおよび仮想ホスト ノードに は、仮想化システムのインフラストラクチャ ク ライアント アプリケーションへのアクセスを可 能にする VI クライアント インタフェースがあ ります。	VMware の仮想インフラスト ラクチャ Web アクセス
VMW ビューア インタフェース	仮想マシン ノードには、仮想マシンのビューア アプリケーションへのアクセスを可能にする VMW ビューア インタフェースがあります。	VMware の仮想マシン リモー ト コンソール
VMW パワー イ ンタフェース	仮想マシン ノードには、CC-SG によるノードの パワー制御を可能にする VMW パワー インタフ ェースがあります。	なし


仮想ノードの概要

仮想インフラストラクチャを CC-SG からアクセスできるように設定し ます。[仮想] ページには、制御システム、仮想ホスト、およびそれらの 仮想マシンを正確に追加する上で役立つ 2 つのウィザード ツール (「制 御システムの追加」ウィザードと「仮想ホストの追加」ウィザード) があ ります。

設定を完了すると、制御システム、仮想ホスト、および仮想マシンがす べて CC-SG 内のノードとしてアクセスできるようになります。各タイ プの仮想ノードは、アクセス用のインタフェースとパワー用のインタフ ェースを伴って設定されます。

- 制御システム ノードと仮想ホスト ノードは、VI クライアント インタフェースを伴って設定されます。VI クライアント インタフェースは、仮想化システムのインフラストラクチャ クライアントへのアクセスを可能にします。VMware コントロール センタの場合、VI クライアント インタフェースが、VMware 仮想インフラストラクチャ Web アクセスを通じてコントロール センタ サーバへのアクセスを可能にします。VMware ESX サーバの場合、VI クライアント インタフェースが、VMware 仮想インフラストラクチャ Web アクセスを通じて ESX サーバへのアクセスを可能にします。
- 仮想マシン ノードは、VMW ビューア インタフェースと VMW パ ワー インタフェースを伴って設定されます。VMW ビューア イン タフェースは、仮想マシンのビューア アプリケーションへのアクセ スを可能にします。VMware 仮想マシンの場合、VMW ビューア イ ンタフェースが仮想マシン リモート コンソールへのアクセスを可 能にします。VMW パワー インタフェースは、CC-SG を通じてノ ードにパワー制御を可能にします。
- CC-SG 5.0 からは、VMWare リモート コンソールの [デバイス] メニューには、CC-SG からアクセスする vSphere 4.0 ノードでア クセスできるようになりました。これにより、デバイスおよびイメ ージを仮想ノードに接続できるようになります。
- CC-SG では、VMware 製品の無料試用版のライセンスを使用する ESXi 仮想ノードの管理またはアクセスはできません

仮想ホストと仮想マシンを持つ制御システムの追加

制御システムを追加すると、ウィザードのガイドに従って、制御システムに組み込まれた仮想ホストおよび仮想マシンを追加することができま す。

- 仮想ホストおよび仮想マシンを持つ制御システムを追加するには、
 以下の手順に従います。
- 1. [ノード]>[仮想] を選択します。
- 2. [制御システムの追加] をクリックします。



- 3. ホスト名/IP アドレス:制御システムの IP アドレスまたはホスト名 を入力します。最大 64 文字です。
- 接続プロトコル: 制御システムと CC-SG 間の HTTP または HTTPS 通信を指定します。
- 5. TCP ポート: TCP ポートを入力します。デフォルトのポートは 443 です。
- 6. 確認する頻度 (秒): 制御システムと CC-SG 間でタイムアウトが起 こるまでの時間を秒単位で入力します。
- 7. 以下の手順で認証情報を入力します。
 - 認証にサービス アカウントを使用するには、[サービス アカウント資格情報の使用] チェックボックスを選択します。使用するサービス アカウントを [サービス アカウント名] メニューで選択します。
 または
 - 認証用のユーザ名とパスワードを入力します。それぞれ最大 64 文字です。
- この制御システムにアクセスするユーザが VI クライアント インタ フェースに自動的にログインできるようにするには、[VI] クライア ントのシングル サイン オンを有効にする] チェックボックスを選 択します。オプション。
- 9. [次へ] をクリックします。CC-SG は、制御システムの仮想ホスト および仮想マシンを検出します。
 - 列のヘッダをクリックすると、テーブルがその属性によって昇順に並べ替えられます。ヘッダを再度クリックすると、テーブルが降順に並び替わります。オプション。
- CC-SG に仮想マシンを追加します。仮想マシンごとに 1 つのノードが作成されます。関連した各仮想ホストも設定されます。仮想ホストが複数の仮想マシンに関連付けられていても、追加される仮想ホストノードは 1 つだけです。
 - 1 つの仮想マシンを追加するには、以下の手順に従います。
 - 追加する仮想マシンの横の[設定]チェックボックスを選択 します。
 - VNC、RDP、または SSH インタフェースを仮想ホスト ノ ードおよび仮想マシン ノードに追加するには、仮想マシン の横のチェックボックスを選択します。オプション。
 - すべての仮想マシンを追加するには、以下の手順に従います。



- [設定]列の一番上のチェックボックスを選択して、すべての 仮想マシンを選択します。
- VNC、RDP、または SSH インタフェースをすべての仮想ホ スト ノードおよびすべての仮想マシン ノードに追加する には、VNC、RDP、または SSH 列の一番上のチェックボ ックスを選択します。オプション。
- 複数の仮想マシンを追加するには、以下の手順に従います。
 - Ctrl または Shift を押しながらクリックして、追加する複数の仮想マシンを選択します。
 - [選択した行のチェックボックスのオン/オフを切り替え] セクションで、[仮想マシン] チェックボックスを選択します。
 - 作成する仮想ホスト ノードおよび仮想マシン ノードに VNC、RDP、または SSH インタフェースを追加するには、 [選択した行のチェックボックスのオン/オフを切り替え] セクションで [VNC]、[RDP]、または [SSH] チェックボッ クスを選択します。オプション。
 - [チェックボックスをオン]をクリックします。
- 11. [次へ] をクリックします。CC-SG は、追加されるインタフェース タイプのリストを表示します。タイプごとに名前とログイン資格認 定を追加できます。
- 12. インタフェース タイプごとに名前とログイン資格認定を入力します 。名前とログイン資格認定は、設定済みの各仮想マシン ノードおよ び仮想ホスト ノードに追加されたすべてのインタフェースで共有さ れます。オプション。

名前とログイン資格認定をインタフェースごとに個別に追加するこ とにした場合、これらのフィールドをブランクにしておきます。 フィールドがブランクの場合、インタフェースでノードの名前が使 用されます。

- a. インタフェースの名前を入力します。最大 32 文字です。
 - 仮想ホスト VI クライアント インタフェース
 - VMware ビューア インタフェース
 - 仮想パワー インタフェース
 - 指定した場合は RDP、VNC、および SSH インタフェース
- b. 必要であればログイン資格認定を入力します。インタフェース のタイプによっては、ログイン資格認定は必要ありません。
 - サービス アカウントを使用するには、[サービス アカウント 資格情報の使用] チェックボックスを選択して、サービス アカウントの名前を選択します。

または



- インタフェース タイプのユーザ名とパスワードを入力します。それぞれ最大 64 文字です。
- 13. [OK] をクリックします。

CC-SG は以下のものを作成します。

- 仮想マシンごとに 1 つのノード。各仮想マシン ノードには VMW ビューア インタフェース、VMW パワー インタフェー ス、指定したその他のインバンド インタフェースがあります。 仮想マシン ノードは、仮想ホスト システムから仮想マシン名 を使って命名されます。
- 仮想ホストごとに 1 つのノード。各仮想ホスト ノードには VI クライアント インタフェースがあります。仮想ホスト ノード は、その IP アドレスまたはホスト名を使って命名されます。
- 制御システムに 1 つのノード。制御システムには VI クライア ント インタフェースがあります。制御システム ノードには、 "Virtual Center" に IP アドレスを付加した名前が付けられます 。たとえば、「Virtual Center 192.168.10.10」という名前になり ます。

仮想マシンを持つ仮想ホストの追加

仮想ホストを追加すると、ウィザードのガイドに従って、仮想ホストに 組み込まれた仮想マシンを追加することができます。

- ▶ 仮想マシンを持つ仮想ホストを追加するには、以下の手順に従います。
- 1. [ノード]>[仮想] を選択します。
- 2. [仮想ホストの追加] をクリックします。
- 3. [ノード]>[仮想] を選択します。
- 4. [仮想ホストの追加] をクリックします。
- 5. ホスト名/IP アドレス: 仮想ホストの IP アドレスまたはホスト名を 入力します。最大 64 文字です。
- 接続プロトコル: 仮想ホストと CC-SG 間の HTTP または HTTPS 通信を指定します。
- TCP ポート: TCP ポートを入力します。デフォルトのポートは 443 です。
- 8. 確認する頻度 (秒): 仮想ホストと CC-SG 間でタイムアウトが起こ るまでの時間を秒単位で入力します。
- 9. 以下の手順で認証情報を入力します。
 - 認証にサービス アカウントを使用するには、[サービス アカウント資格情報の使用] チェックボックスを選択します。使用するサービス アカウントを [サービス アカウント名] メニューで選択します。



または

- 認証用のユーザ名とパスワードを入力します。それぞれ最大 64 文字です。
- この仮想ホストにアクセスするユーザが VI クライアント インタフ ェースに自動的にログインできるようにするには、[VI クライアン トのシングル サイン オンを有効にする] チェックボックスを選択 します。オプション。
- **11.** [次へ] をクリックします。CC-SG は、仮想ホストの仮想マシンを 検出します。
 - 列のヘッダをクリックすると、テーブルがその属性によって昇順に並べ替えられます。ヘッダを再度クリックすると、テーブルが降順に並び替わります。オプション。
- 12. CC-SG に仮想マシンを追加します。仮想マシンごとに 1 つのノードが作成されます。関連した各仮想ホストも設定されます。仮想ホストが複数の仮想マシンに関連付けられていても、追加される仮想ホストノードは 1 つだけです。
 - 1 つの仮想マシンを追加するには、以下の手順に従います。
 - 追加する仮想マシンの横の[設定]チェックボックスを選択 します。
 - VNC、RDP、または SSH インタフェースを仮想ホスト ノードおよび仮想マシン ノードに追加するには、仮想マシンの横のチェックボックスを選択します。オプション。
 - すべての仮想マシンを追加するには、以下の手順に従います。
 - [設定]列の一番上のチェックボックスを選択して、すべての 仮想マシンを選択します。
 - VNC、RDP、または SSH インタフェースをすべての仮想ホ スト ノードおよびすべての仮想マシン ノードに追加する には、VNC、RDP、または SSH 列の一番上のチェックボ ックスを選択します。オプション。
 - 複数の仮想マシンを追加するには、以下の手順に従います。



- Ctrl または Shift を押しながらクリックして、追加する複数の仮想マシンを選択します。
- [選択した行のチェックボックスのオン/オフを切り替え] セクションで、[仮想マシン] チェックボックスを選択します
- 作成する仮想ホスト ノードおよび仮想マシン ノードに VNC、RDP、または SSH インタフェースを追加するには 、[選択した行のチェックボックスのオン/オフを切り替え] セクションで [VNC]、[RDP]、または [SSH] チェックボッ クスを選択します。オプション。
- [チェックボックスをオン]をクリックします。
- [次へ] をクリックします。CC-SG は、追加されるインタフェース タイプのリストを表示します。タイプごとに名前とログイン資格認 定を追加できます。
- 14. インタフェース タイプごとに名前とログイン資格認定を入力します 。名前とログイン資格認定は、設定済みの各仮想マシン ノードおよ び仮想ホスト ノードに追加されたすべてのインタフェースで共有さ れます。オプション。

名前とログイン資格認定をインタフェースごとに個別に追加するこ とにした場合、これらのフィールドをブランクにしておきます。 フィールドがブランクの場合、インタフェースでノードの名前が使 用されます。

- a. インタフェースの名前を入力します。最大 32 文字です。
 - VI クライアント インタフェース
 - VMware ビューア インタフェース
 - 仮想パワー インタフェース
 - 指定した場合は RDP、VNC、および SSH インタフェース
- b. 必要であればログイン資格認定を入力します。インタフェース のタイプによっては、ログイン資格認定は必要ありません。
 - サービス アカウントを使用するには、[サービス アカウント 資格情報の使用] チェックボックスを選択して、サービス アカウントの名前を選択します。

または

- インタフェース タイプのユーザ名とパスワードを入力します。それぞれ最大 64 文字です。
- 15. [OK] をクリックします。

CC-SG は以下のものを作成します。



- 仮想マシンごとに 1 つのノード。各仮想マシン ノードには VMW ビューア インタフェース、VMW パワー インタフェー ス、指定したその他のインバンド インタフェースがあります。 仮想マシン ノードは、仮想ホスト システムから仮想マシン名 を使って命名されます。
- 仮想ホストごとに 1 つのノード。各仮想ホスト ノードには VI クライアント インタフェースがあります。仮想ホスト ノード は、その IP アドレスまたはホスト名を使って命名されます。

制御システム、仮想ホスト、仮想マシンの編集

CC-SG で設定された制御システム、仮想ホスト、仮想マシンを編集し、そのプロパティを変更できます。仮想マシンの[設定] チェックボックスを選択解除すると、仮想マシン ノードを CC-SG から削除できます。

注: 仮想ホストまたは制御システムのノード名を変更するには、ノード を編集します。「ノードの編集 『124p. 』」を参照してください。名前 の変更は、仮想化テーブルにも表示されます。

- 制御システム、仮想ホスト、仮想マシンを編集するには、以下の手順に従います。
- 1. [ノード]>[仮想] を選択します。
- 列のヘッダをクリックすると、テーブルがその属性によって昇順に 並べ替えられます。ヘッダを再度クリックすると、テーブルが降順 に並び替わります。オプション。
- 3. 編集する制御システムまたは仮想ホストを選択します。
- 4. [編集] をクリックします。
- 必要に応じて情報を変更します。フィールドの詳細については、「仮 想ホストと仮想マシンを持つ制御システムの追加 『127p. 』」および「仮想マシンを持つ仮想ホストの追加 『130p. 』」を参照してください。
- 6. [次へ] をクリックします。
- 7. CC-SG から 1 つまたは複数の仮想マシンを削除します。
 - 仮想マシンを削除するには、[設定] チェックボックスを選択解 除します。
 - 複数の仮想マシンを削除するには、Ctrl または Shift を押しな がらクリックして複数の仮想マシンを選択します。次に、[選択 した行のチェックボックスのオン/オフを切り替え] セクション で、[仮想マシン] チェックボックスを選択し、[チェックボック スをオフ] をクリックします。
- VNC、RDP、または SSH インタフェースを仮想ホスト ノードお よび仮想マシン ノードに追加するには、各仮想マシンの横のチェッ クボックスを選択します。



このページでは、SSH、VNC、RDP インタフェースを仮想ホスト ノードまたは仮想マシン ノードから削除することはできません。こ れらのインタフェースの削除は、ノード プロファイルから行う必要 があります。「インタフェースの削除 『152p. 』」を参照してくだ さい。

- 9. [次へ] をクリックします。仮想マシンの削除を選択した場合、警告 メッセージが表示されます。
- 10. インタフェース タイプごとに名前とログイン資格認定を入力します 。名前とログイン資格認定は、設定済みの各仮想マシン ノードおよ び仮想ホスト ノードに追加されたすべてのインタフェースで共有さ れます。オプション。名前とログイン資格認定をインタフェースご とに個別に追加することにした場合、これらのフィールドをブラン クにしておくことができます。
 - a. インタフェースの名前を入力します (最大 32 文字)。
 - 仮想ホスト VI クライアント インタフェース
 - VMware ビューア インタフェース
 - 仮想パワー インタフェース
 - 指定した場合は RDP、VNC、および SSH インタフェース
 - b. 以下のようにログイン資格認定を入力します。
 - サービス アカウントを使用するには、[サービス アカウント 資格情報の使用] チェックボックスを選択して、サービス アカウントの名前を選択します。

または

インタフェース タイプのユーザ名とパスワードを入力します。それぞれ最大 64 文字です。

11. [OK] をクリックします。



制御システムおよび仮想ホストの削除

制御システムおよび仮想ホストを CC-SG から削除できます。

制御システムを削除しても、関連付けられた仮想ホストと仮想マシンは 削除されません。

仮想ホストを削除しても、関連付けられた制御システムと仮想マシンは 削除されません。

関連付けられた制御システムと仮想ホストが削除されても、仮想マシン ノードが自動的に削除されることはありません。「*仮想マシン ノードの 削除*『135p.』」を参照してください。

- 制御システムと仮想ホストを削除するには、以下の手順に従います。
- 1. [ノード]>[仮想] を選択します。
- 2. 削除する制御システムと仮想ホストをリストから選択します。Ctrl を押しながらクリックすると、複数項目を選択できます。
- 3. [削除] をクリックします。

仮想マシン ノードの削除

仮想マシン ノードの削除には、以下の2通りの方法があります。

- ノード削除機能を使用します。「ノードの削除 『124p. 』」を参照 してください。
- 仮想マシンの[設定] チェックボックスを選択解除します。「制御シ ステム、仮想ホスト、仮想マシンの編集 『133p. 』」を参照してく ださい。

仮想インフラストラクチャの削除

以下の手順を用いると、制御システム、仮想ホスト、仮想マシンを含め、仮想インフラストラクチャ全体を CC-SG から削除することができます。

- 仮想インフラストラクチャを削除するには、以下の手順に従います。
- 各仮想マシンの [設定] チェックボックスを選択解除して、すべての 仮想マシン ノードを削除します。「*制御システム、仮想ホスト、仮 想マシンの編集* 『133p. 』」を参照してください。
- 制御システムと仮想ホストを削除します。「制御システムおよび仮想 ホストの削除 『135p. 』」を参照してください。
 制御システム ノード、仮想ホスト ノード、仮想マシン ノード、さらにそれらの関連インタフェースを含め、仮想インフラストラクチャのすべてのコンポーネントが削除されます。



vSphere 4 ユーザは新しいプラグインをインストールする必要がある

仮想環境を前のバージョンから vSphere 4 にアップグレードする場合 は、VMware リモート コンソール プラグインをブラウザから削除する 必要があります。プラグインを削除したら、vSphere4 の正しいプラグ インは、次回 CCSG から仮想マシンに接続するときにインストールさ れます。

- Internet Explorer から古いプラグインを削除するには、以下の手順 に従います。
- [ツール] > [Manage Add-Ons(アドオンの管理)] > [Enable Add-Ons(アドオンの有効化)] または [Disable Add-Ons(アドオンの無効化)] を選択します。
- 表示リストの [Add-Ons that have been used by Internet Explorer(Internet Explorer で使用されたアドオン)] を選択します。
- 3. [VMware Remote Console Plug-in(VMware リモート コンソール プ ラグイン)] まで下にスクロールして、それを選択します。
- 4. [Delete Active-X(Active-X の削除)] ボタンが有効になります。古い プラグインをクリックして削除します。
 - 削除ボタンが有効にならない場合は、コントロール パネル > [プログラムの追加と削除] に移動して、より古い VI クライアン トを調べます。VI クライアント 2.5 がインストールされている 場合は、それをアンインストールします。VI クライアント 2.5 をアンインストールした後に、プラグインが削除されます。
- Firefox ユーザから古いプラグインを削除するには、以下の手順に 従います。
- 1. [ツール] > [Add-Ons(アドオン)] を選択します。
- 2. [Plug-Ins(プラグイン)] タブをクリックします。
- 3. 古いプラグインを選択し、[Disable(無効化)] をクリックします。
- 新しいプラグインをインストールするには、以下の手順に従います。
- 古いプラグインを削除したら、CCSG にログインして仮想マシンに 接続します。
- 2. vSphere 4 のプラグインをインストールするよう要求されます。



仮想インフラストラクチャと CC-SG の同期

同期により、**CC-SG** には仮想インフラストラクチャに関する最新の情報が保たれます。同期では、各仮想マシン ノードに固有の情報と仮想 インフラストラクチャ トポロジ情報が更新されます。

設定されたすべての制御システムと仮想ホストの日次同期を自動的に行 うように設定できます。また、選択した制御システムと仮想ホストの同 期をいつでも実行することもできます。

仮想インフラストラクチャの同期

CC-SG と仮想インフラストラクチャの同期を実行できます。

制御システムを選択して同期を行うと、仮想ホストの選択の有無に関係 なく、関連付けられた仮想ホストも同期されます。

- 仮想インフラストラクチャを同期するには、以下の手順に従います。
- 1. [ノード]>[仮想] を選択します。
- ノードのリストで、同期するノードを選択します。Ctrl を押しなが らクリックすると、複数項目を選択できます。
- 3. [同期] をクリックします。前回の同期後、仮想インフラストラクチャが変更された場合、CC-SG 内の情報が更新されます。
 - [Secure Gateway で設定済み]列には、CC-SG で設定されている仮想マシンまたは仮想ホストの数が示されます。
 - [Last Synchronization Date] (前回の同期日) には、同期の日時が 示されます。
 - [ノード ステータス]列には、仮想ノードのステータスが示されます。

仮想インフラストラクチャの日次同期の有効化または無効化

CC-SG と仮想インフラストラクチャの自動同期を設定できます。毎日 指定した時刻に自動同期が実行されます。

- 仮想インフラストラクチャの日次同期を有効にするには、以下の手順に従います。
- 1. [ノード]>[仮想] を選択します。
- 2. [日次自動同期を有効にする] チェックボックスを選択します。
- 3. 日次同期の開始時刻を [開始時刻] フィールドに入力します。
- 4. [更新] をクリックします。



- 仮想インフラストラクチャの日次同期を無効にするには、以下の手順に従います。
- 1. [ノード]>[仮想] を選択します。
- 2. [日次自動同期を有効にする] チェックボックスを選択解除します。
- 3. [更新] をクリックします。

仮想ホスト ノードのリブートまたは強制リブート

仮想ホスト サーバのリブートまたは強制リブートを実行できます。仮 想ホスト サーバがメンテナンス モードになっている場合、リブート操 作でその通常のリブートが実行されます。強制リブート操作では、メン テナンス モードになっていない仮想ホスト サーバであっても、そのリ ブートが強制されます。

これらのコマンドを使用するには、ノードのインバンド アクセス権限 とノード パワー制御権限が必要です。またリブートまたは強制リブー トの対象のノードにアクセスするためのポリシーを割り当てられている ユーザ グループのメンバである必要があります。

- 仮想ホスト ノードのリブートまたは強制リブートを実行するには、 以下の手順に従います。
- リブートまたは強制リブートの対象の仮想ホスト ノードを選択します。
- 2. [仮想ホスト データ] タブをクリックします。
- 3. [リブート] または [強制リブート] をクリックします。

[Virtual Topology] (仮想トポロジー) 表示へのアクセス

[トポロジー] 表示は、選択したノードに関連付けられた制御システム、 仮想ホスト、および仮想マシンの相互関係を示すツリー構造です。 [トポロジー] 表示を開くには、デバイス、ポート、ノードの管理権限が 必要です。

- ▶ 仮想ノード プロファイルから [トポロジー] 表示を開きます。
- ノード プロファイルで、ノードに関する仮想化情報が含まれている [仮想マシン データ] タブ、[仮想ホスト データ] タブ、[制御システム] タブのいずれかをクリックします。いずれをクリックするかは 、ノード タイプによります。
- [トポロジー表示] リンクをクリックします。[トポロジー] 表示が新 しいウィンドウで開きます。CC-SG で設定されている仮想ノード がリンクとして表示されます。
 - ノードのリンクをダブルクリックして、仮想ノードのノード プロファイルを開きます。



- インタフェース リンクをダブルクリックして、ノードに接続します。
- 仮想パワー インタフェース リンクをダブルクリックして、ノードの [パワー制御] ページを開きます。

ノードへの接続

ノードにインタフェースがあると、いくつかの方法でそのインタフェー スを介してそのノードに接続できます。Raritan の『CommandCenter Secure Gateway ユーザ ガイド』を参照してください。

- ▶ ノードに接続するには、以下の手順に従います。
- 1. [ノード] タブをクリックします。
- 2. 接続するノードを選択し、次の作業を行います。
 - [インタフェース] テーブルで、接続するインタフェースの名前 をクリックします。

または

 [ノード] タブで、接続するノードの下にあるインタフェースの リストを展開します。接続するインタフェースの名前をダブル クリックするか、インタフェースを右クリックして [接続] を選 択します。

Access Client の **Firefox** ユーザは **JNLP** ファイルのダウンロードが 必要

Access Client の Firefox ユーザには、アウト オブ バンド KVM ポイ ント接続を確立するたびに .JNLP ファイルのダウンロードを求めるプ ロンプトが表示されます。

[Do this automatically for files like this from now on(今後同様のファイル に対してこれを自動実行する)] チェックボックスをオンにすると、今後 の接続で Firefox が自動的にファイルをダウンロードできます。

ノードへの ping の実行

CC-SG からノードに ping を実行し、接続を確認できます。

- ノードに ping を実行するには、以下の手順に従います。
- 1. [ノード] タブをクリックし、ping を実行するノードを選択します。
- [ノード]>[ノードに Ping を実行] を選択します。ping の結果が画面に表示されます。



インタフェースの追加、編集、削除

インタフェースの追加

注: 制御システム、仮想ホスト、仮想マシンなどの仮想ノードのインタ フェースは、[ノード]>[仮想]の下で仮想化ツールを使用することによ ってしか追加できません。「CC-SG での仮想インフラストラクチャの設 定 『126p. 』」を参照してください。

▶ インタフェースを追加するには、以下の手順に従います。

 既存のノードの場合: [ノード] タブをクリックし、インタフェースを 追加するノードを選択します。表示される [ノード プロファイル] 画面の [インタフェース] セクションで [追加] をクリックします。 新しいノードを追加する場合: [ノードの追加] 画面の [インタフェー ス] で [追加] をクリックします。

[インタフェースの追加] ウィンドウが開きます。

2. [インタフェース タイプ] ドロップダウン メニューをクリックし、 以下の中から、ノードへの接続のタイプを選択します。

インバンド接続:

- インバンド DRAC KVM: DRAC インタフェースを介して Dell DRAC サーバへの KVM 接続を作成するには、このアイテムを 選択します。DRAC パワー インタフェースも設定する必要が 生じます。
- インバンド iLO Processor KVM: iLO または RILOE インタフ ェースを介して HP サーバへの KVM 接続を作成するには、こ のアイテムを選択します。
- インバンド RDP: Java または Microsoft リモート デスクトップ プロトコルを使用してノードへの KVM 接続を作成するには、このアイテムを選択します。
- インバンド RSA KVM: RSA インタフェースを介して IBM RSA サーバへの KVM 接続を作成するには、このアイテムを選 択します。RSA パワー インタフェースも設定する必要が生じ ます。
- インバンド SSH: ノードへの SSH 接続を作成するには、この アイテムを選択します。
- インバンド VNC: VNC サーバ ソフトウェアを介してノードへの KVM 接続を作成するには、このアイテムを選択します。
 「インバンド接続のインタフェース 『142p. 』」を参照してください。

アウト オブ バンド接続:



- アウト オブ バンド KVM: Raritan KVM (KX、KX101、KSX、 IP-Reach、Paragon II) を介してノードへの KVM 接続を作成す るには、このアイテムを選択します。
- アウト オブ バンド シリアル: Raritan シリアル デバイス (SX、KSX) を介してノードへのシリアル接続を作成するには、 このアイテムを選択します。

「*アウト オブ バンド KVM、アウト オブ バンド シリアル接 続のインタフェース* 『143p. 』」を参照してください。

パワー制御接続:

- パワー制御 DRAC: Dell DRAC サーバへのパワー制御接続を作 成するには、このアイテムを選択します。
- パワー制御 iLO Processor: HP iLO/RILOE サーバへのパワー制 御接続を作成するには、このアイテムを選択します。
- パワー制御 IPMI: IPMI 接続を使用してノードへのパワー制御 接続を作成するには、このアイテムを選択します。
- パワー制御 Integrity ILO2: Integrity ILO2 をサポートする HP Integrity サーバまたはその他のサーバへのパワー制御接続を作 成するには、このアイテムを選択します。
- Power Control Power IQ Proxy (パワー制御 Power IQ Proxy): Power IQ IT デバイスへのパワー制御接続を作成するには、このアイテムを選択します。
- パワー制御 RSA: RSA サーバへのパワー制御接続を作成する には、このアイテムを選択します。

「**DRAC パワー制御接続のインタフェース 『144**p. **』**」を参照 してください。

ILO Processor、Integrity ILO2、および RSA のパワー制御接 続のインタフェース 『145p. 』

Power IQ Proxy のパワー制御接続のインタフェース 『**147**p. 』 管理対象電源タップ接続:

 Managed PowerStrip (管理対象電源タップ): Raritan の電源タッ プまたは Dominion PX デバイスを介してノードへのパワー制 御接続を作成するには、この項目を選択します。

「*管理対象電源タップ接続用インタフェース* 『146p. 』」を参照してください。

Web ブラウザ接続:

 Web ブラウザ: Web サーバが組み込まれたデバイスへの接続を 作成するには、このアイテムを選択します。

「*Web ブラウザ インタフェース* 『149p. 』」を参照してくだ さい。



 3. 選択したインタフェースのタイプに応じて、[名前] フィールドにデ フォルト名が表示されます。デフォルト名は変更できます。この名 前は、[ノード] リストのインタフェースの横に表示されます。名前 の長さに関する CC-SG のルールについての詳細は、「命名規則『 435p.』」を参照してください。

インバンド接続のインタフェース

インバンド接続には、RDP、VNC、SSH、RSA KVM、iLO Processor KVM、DRAC KVM、TELNET が含まれます。

Telnet はセキュア アクセス方式ではありません。ユーザ名、パスワード、トラフィックはすべてクリア テキスト形式で送信されます。

- インバンド接続のインタフェースを追加するには、以下の手順に従います。
- 1. [IP アドレス/ホスト名] フィールドに、このインタフェースの IP アドレスまたはホスト名を入力します。
- 2. この接続の TCP ポートを [TCP ポート] フィールドに入力します 。オプション。
- RDP インタフェースの場合、[Java (Java)] または [Windows (Windows)] を選択し、[コンソール] または [リモート ユーザ] を選 択します。[コンソール] ユーザがノードにアクセスすると、他のす べてのユーザが切断されます。複数のリモート ユーザが同時にノー ドにアクセスできます。
- 4. 以下の手順で認証情報を入力します。
 - 認証にサービス アカウントを使用するには、[サービス アカウント資格情報の使用] チェックボックスを選択します。使用するサービス アカウントを [サービス アカウント名] メニューで選択します。

または

- 認証用のユーザ名とパスワードを入力します。VNC インタフェ ースの場合、パスワードのみが必要です。
- 5. 言語のキーボード レイアウトを選択します。Microsoft RDP インタ フェースの場合、このオプションは使用できません。
- 6. このインタフェースの説明を [説明] フィールドに入力します。オプ ション。
- 7. [OK] をクリックして変更を保存します。



DRAC5 接続の詳細

Internet Explorer を使用して DRAC 5 サーバに接続する場合は、DRAC 5 に有効な証明書がインストールされている必要があります。インストールされていない場合、Internet Explorer にエラーが表示されます。 証明書が信頼された CA によって署名されていない場合は、同じ証明書

をブラウザの信頼されたルート証明機関ストアにもインストールします 。

Microsoft RDP 接続の詳細

- Windows XP クライアントを使用する場合は、CC-SG から Microsoft RDP インタフェースに接続するために Terminal Services クライアント 6.0 以上が必要です。Terminal Services クライアン トを 6.0 に更新するには、http://support.microsoft.com/kb/925876 を参照してください。
- Internet Explorer にのみ対応します。
- Microsoft RDP をプロキシ モード接続に使用することはできません。 「*接続モードについて*『280p. 』」を参照してください。
- サポートされているターゲットは、Vista、Windows Server 2008、 Windows 7、およびそれ以前のすべての Windows リリース (Windows XP、Windows 2003 ターゲットなど)です。
- 使用方法などの Microsoft RDP についての詳細は、以下を参照して ください。
 http://www.microsoft.com/downloads/details.aspx?FamilyID=469eee 3a-45b4-4b40-b695-b678646a728b&displaylang=en

Java RDP 接続の詳細

- Java RDP インタフェースでは、Windows XP および Windows
 2003 ターゲットがサポートされます。
- Java RDP をプロキシ モード接続に使用できます。「接続モードについて 『280p.』」を参照してください。

アウト オブ バンド KVM、アウト オブ バンド シリアル接続のインタフェー ス

- アウト オブ バンド KVM 接続またはアウト オブ バンド シリア ル接続のインタフェースを追加するには、以下の手順に従います。
- アプリケーション名: リストからインタフェースを持つノードへの 接続に使用するアプリケーションを選択します。
 - ブラウザに基づき、CC-SG でアプリケーションを自動的に選択 するには、[自動検出]を選択します。



- Active KVM Client を使用するための必要条件があります。「
 AKC を使用するための必要条件『269p.の"AKC を使用するため前提条件"参照』」および「AKC ダウンロード サーバ証明書の検証を有効にする『283p.の"AKC ダウンロード サーバ証明書の検証の有効化"参照』」を参照してください。
- 2. Raritan デバイス名: このノードへのアクセスを提供する Raritan デバイスを選択します。このリストにデバイスが表示されるように するには、CC-SG にデバイスを追加する必要があります。
- Raritan ポート名: このノードへのアクセスを提供する Raritan デ バイスのポートを選択します。このリストにポートが表示されるよ うにするには、まず CC-SG にポートを追加する必要があります。 シリアル接続では、ポートの設定により、[ボー レート]、[パリティ]、[フロー制御] 値が自動的に入力されます。
- 4. このインタフェースの説明を [説明] フィールドに入力します。オプ ション。
- 5. [OK] をクリックして変更を保存します。

DRAC パワー制御接続のインタフェース

- ▶ DRAC パワー制御接続のインタフェースを追加するには、以下の手順に従います。
- 1. [IP アドレス/ホスト名] フィールドに、このインタフェースの IP アドレスまたはホスト名を入力します。
- この接続の TCP ポートを [TCP ポート] フィールドに入力します
 DRAC 5 の場合のみ必須です。DRAC 4 の場合、[TCP ポート] は必須ではありません。
- 3. 以下の手順で認証情報を入力します。
 - 認証にサービス アカウントを使用するには、[サービス アカウント資格情報の使用] チェックボックスを選択します。使用するサービス アカウントを [サービス アカウント名] メニューで選択します。

または

- 認証用のユーザ名とパスワードを入力します。
- 4. このインタフェースの説明を [説明] フィールドに入力します。オプ ション。
- 5. [OK] をクリックして変更を保存します。



ILO Processor、Integrity ILO2、および RSA のパワー制御接続のインタフェ ース

- ILO Processor、Integrity ILO2、および RSA のパワー制御接続の インタフェースを追加するには、以下の手順に従います。
- 1. [IP アドレス/ホスト名] フィールドに、このインタフェースの IP アドレスまたはホスト名を入力します。
- 2. 以下の手順で認証情報を入力します。
 - 認証にサービス アカウントを使用するには、[サービス アカウント資格情報の使用] チェックボックスを選択します。使用するサービス アカウントを [サービス アカウント名] メニューで選択します。

または

- 認証用のユーザ名とパスワードを入力します。
- 3. このインタフェースの説明を [説明] フィールドに入力します。オプ ション。
- 4. [OK] をクリックして変更を保存します。

RSA インタフェースの詳細

インバンド RSA KVM またはパワー インタフェースを作成すると、イ ンタフェースに関連付けられたユーザ名とパスワードが CC-SG によっ て破棄され、RSA サーバに 2 つのユーザ アカウントが作成されます 。これにより、KVM インタフェースとパワー インタフェースから同時 に RSA サーバにアクセスできるようになります。

新しいユーザ名:

- cc_kvm_user
- cc_power_user

インタフェースを作成するときに入力したユーザ名は、これらのユーザ 名に置き換えられます。CCSG では、これらの新しいユーザ アカウン トを使用してインタフェースから RSA サーバに接続します。

RSA サーバ上のこれらのユーザ アカウントのパスワードを削除、編集、または変更しないでください。**CC-SG** でインタフェースを使用して 接続できなくなります。

サービス アカウントを使用してインタフェースを作成した場合は、 RSA サーバ上にユーザ アカウントは作成されません。インタフェース でサービス アカウントを使用する場合は、KVM インタフェースとパワ ー インタフェースから RSA サーバに同時にアクセスすることはでき ません。



JRE との RSA の互換性

IBM RSA II バージョン 1.14 は、JRE バージョン 1.6.0_10 および 1.6.0_11 と互換性があります。

CC-SG は、さらに高位の JRE バージョンもサポートしていますが、 高位の JRE バージョンは IBM RSA II カードでは正しく機能しません

管理対象電源タップ接続用インタフェース

管理デバイスとして KX を指定する管理対象電源タップ インタフェー スを作成すると、指定したコンセントの名前が、関連付けられたノード の名前に変更されます。

- 管理対象電源タップ接続のインタフェースを追加するには、以下の 手順に従います。
- 1. 管理デバイス:
 - 電源タップが接続された Raritan デバイスを選択します。 CC-SG にデバイスを追加する必要があります。

または

- このパワー制御インタフェースで IP ネットワーク上の別の Raritan デバイスに接続されていない PX デバイスが使用され る場合、Dominion PX を選択します。
- 管理ポート:電源タップが接続された Raritan デバイスのポートを 選択します。PX を管理デバイスとして選択すると、このフィール ドは無効になります。
- 電源タップ名: ノードに電力を供給する電源タップまたは PX デバイスを選択します。電源タップまたは PX デバイスは、CC-SG に 設定しない限り、このリストには表示されません。
- 4. コンセント名: ノードが差し込まれているコンセントの名前を選択 します。オプション。
- 5. このインタフェースの説明を [説明] 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。

注: 管理対象電源タップ インタフェースは、ブレード シャーシ ノード には追加できますが、ブレード サーバ ノードには追加できません。

IPMI パワー制御接続のインタフェース

- ▶ IPMI パワー制御接続のインタフェースを追加するには、以下の手順 に従います。
- 1. [IP アドレス/ホスト名] フィールドに、このインタフェースの IP アドレスまたはホスト名を入力します。



- 2. このインタフェースの UDP ポート番号を [UDP ポート] フィール ドに入力します。
- 3. [認証]: このインタフェースに接続するための認証スキーマを選択し ます。
- 4. [確認する頻度(秒)] フィールドに、このインタフェースを確認する 間隔を入力します。
- 5. 以下の手順で認証情報を入力します。
 - 認証にサービス アカウントを使用するには、[サービス アカウント資格情報の使用] チェックボックスを選択します。使用するサービス アカウントを [サービス アカウント名] メニューで選択します。

または

- 認証用のユーザ名とパスワードを入力します。オプション。
- このインタフェースの説明を[説明] フィールドに入力します。オプ ション。
- 7. [OK] をクリックして変更を保存します。

IBM IMM モジュール接続の詳細

IPMI パワー制御インタフェースを使用して、パワー制御操作のために CC-SG を通じて IBM IMM モジュールの標準バージョンに接続できま す。電源オン、電源オフ、および電源のリセット機能がサポートされて います。

「*IPMI パワー制御接続のインタフェース* 『146p. 』」を参照してくだ さい。

注: CC-SG を通じた IBM IMM モジュールへの KVM アクセスはできま せん。

Power IQ Proxy のパワー制御接続のインタフェース

ノードとして CC-SG に追加した Power IQ IT デバイスのパワー制御 を CC-SG で行う場合は、Power IQ Proxy のパワー制御インタフェー スを追加します。これにより、CC-SG で管理されていない PDU に接 続されたノードのパワー制御が可能になります。

- Power IQ Proxy のパワー制御接続のインタフェースを追加するには、以下の手順に従います。
- IT デバイスの外部キーを入力します。外部キーは、Power IQ と CC-SG で同じである必要があります。最大 255 文字です。カンマ は使用できません。デフォルト値はノード名です。この値は変更で きます。



- IT デバイスがすでに Power IQ に追加されている場合は、[Data Center (データ センター)] タブの IT デバイスのページで外部 キーを探し、そのテキストを [External Key (外部キー)] フィー ルドに入力します。
- IT デバイスがまだ Power IQ に追加されていない場合は、外部 キーのデフォルト値をそのまま使用するか、変更します。ただ し、IT デバイスを Power IQ に追加するときに同じ値を使用す る必要があります。すべてのノードとインタフェースの情報を 含むファイルをエクスポートによって簡単に作成できます。「ノ ードのエクスポート 『169p. 』」を参照してください。
- [管理デバイス] フィールドで、IT デバイスを管理する Power IQ を 選択します。このフィールドに Power IQ が表示されるようにする には、CC-SG にその Power IQ に関する情報を追加する必要があ ります。「Power IQ サービスの設定 『378p. 』」を参照してくだ さい。
- 3. このインタフェースの説明を [説明] フィールドに入力します。
- 4. [OK] をクリックして変更を保存します。



Web ブラウザ インタフェース

Web ブラウザ インタフェースを追加すると、Dominion PX などの Web サーバが組み込まれたデバイスへの接続を作成できます。「*例: PX* ノードへの Web ブラウザ インタフェースへの追加 『151p. の"例: PX ノードへの Web ブラウザ インタフェースの追加 参照 』」を参照して ください。KVM スイッチが統合されたブレード シャーシについては、 KX2 デバイスでそうしたシャーシに URL または IP アドレスを割り当 てると、Web ブラウザ インタフェースが自動的に追加されます。

Web ブラウザ インタフェースを使用して、Web アプリケーション (RSA、DRAC、または ILO Processor カードに関連した Web アプリ ケーションなど) に接続することもできます。

Web アプリケーションにより、セッション ID など、ユーザ名とパス ワード以外の情報が求められる場合、Web ブラウザ インタフェースで は自動ログインを行うことができません。

ユーザが、Web ブラウザ インタフェースにアクセスするには、ノード のイン バンド アクセス権限が必要です。

DNS を設定しないと、URL が解決されません。IP アドレスに対して DNS を設定する必要はありません。

- Web ブラウザ インタフェースを追加するには、以下の手順に従い ます。
- Web ブラウザ インタフェースのデフォルト名は Web Browser で す。名前は、[名前] フィールドで変更できます。名前の長さに関す る CC-SG のルールについての詳細は、「命名規則 『435p. 』」を 参照してください。
- 2. この接続の TCP ポートを [TCP ポート] フィールドに入力します 。URL で HTTPS を使用する場合は、TCP ポートを 443 に設定 する必要があります。オプション。
- [URL] フィールドに Web アプリケーションの URL またはドメイン名を入力します。Web アプリケーションがユーザ名とパスワードを読み取ると予想される URL を入力する必要がある点に注意してください。最大 120 文字で設定します。次の正しい形式の例に従ってください。
 - http(s): //192.168.1.1/login.asp
 - http(s): //www.example.com/cgi/login
 - http(s): //example.com/home.html
- 4. 以下の手順で認証情報を入力します。オプション。
 - 認証にサービス アカウントを使用するには、[サービス アカウント資格情報の使用] チェックボックスを選択します。使用するサービス アカウントを [サービス アカウント名] メニューで選択します。



または

 認証用のユーザ名とパスワードを入力します。このインタフェ ースへのアクセスを可能にするユーザ名とパスワードを入力し ます。

注: DRAC、ILO、RSA Web アプリケーションの場合、認証情報を 入力しないでください。さもないと接続が失敗します。

- [ユーザ名フィールド] と [パスワード フィールド] に、Web アプリ ケーションのログイン画面で使用されるユーザ名フィールドとパス ワード フィールドのフィールド名を入力します。ログイン画面の HTML ソースを参照して、フィールド名 (フィールド ラベルではな く)を見つける必要があります。「Web ブラウザ インタフェースの 追加のヒント 『150p. 』」を参照してください。
- このインタフェースの説明を[説明]フィールドに入力します。オプ ション。
- 7. [OK] をクリックして変更を保存します。

Web ブラウザ インタフェースの追加のヒント

Web ブラウザ インタフェースを設定するには、ユーザ名フィールドと パスワード フィールドの実際のフィールド名を特定するのに役立つ情 報を HTML ソースから収集する必要があります。これらの認証フィー ルドの実装はすべてのベンダ間で異なるため、これらのフィールドの名 前は、デバイスによっても、特定のデバイスのファームウェア バージ ョンによっても異なります。このため、フィールド名を見つける方法は 1 つではありません。可能な方法については、以下の手順を参照してく ださい。

適切なフィールド名を見つけて特定する方法について、ソフトウェア エンジニアやシステム管理者にたずねることもできます。

▶ フィールド名を見つけるヒント

- 1. Web アプリケーションのログイン ページの HTML ソース コード で、ユーザ名やパスワードなどのフィールドのラベルを探します。
- フィールド ラベルを見つけたら、タグに隣接する次のようなコード を参照します。name="user"
 引用符に囲まれた語がフィールド名です。



例: PX ノードへの Web ブラウザ インタフェースの追加

Dominion PX 管理対象電源タップは、ノードとして CC-SG に追加で きます。次に、Web ブラウザ インタフェースをノードに追加できます 。このインタフェースにより、ユーザが Dominion PX の Web ベース 管理アプリケーションにアクセスできるようになります。

Dominion PX ノードに Web ブラウザ インタフェースを追加する には、次の値を使用します。

URL: <DOMINION PX IP ADDRESS>/auth.asp

TCP ポート: 80

ユーザ名: Dominion PX 管理者のユーザ名

パスワード: Dominion PX 管理者のパスワード

ユーザ名フィールド = login

パスワード フィールド = password

インタフェースを追加した結果

ノードにインタフェースを追加すると、[ノードの追加] または [ノード プロファイル] 画面の [インタフェース] テーブルと [デフォルト イン タフェース] ドロップダウン メニューにそのインタフェースが表示され ます。このドロップダウン メニューをクリックし、ノードへの接続に 使用するデフォルト インタフェースを選択します。

[ノードの追加] または [ノード プロファイル] 画面への変更を保存する と、インタフェースの名前が、これによりアクセスが可能になるノード の下に階層構造で表示される [ノード] リストにも表示されます。

管理デバイスとして KX を指定する管理対象電源タップ インタフェー スを追加すると、指定したコンセントの名前が、関連付けられたノード の名前に変更されます。

インタフェースの編集

▶ インタフェースを編集するには、以下の手順に従います。

- [ノード] タブをクリックし、編集するインタフェースのあるノード を選択します。[ノード プロファイル]ページが開きます。
- 2. [インタフェース] タブで、編集するインタフェースの行を選択します。
- 3. [編集] をクリックします。
- 必要に応じてフィールドを編集します。フィールドの詳細は、「イン タフェースの追加 『140p. 』」を参照してください。一部のフィー ルドは読み取り専用です。



5. [OK] をクリックして変更を保存します。

インタフェースの削除

ノードからインタフェースを削除できます。ただし、以下を除きます。

- 仮想マシン ノードの VMW ビューア インタフェースまたは VMW パワー インタフェース。
- KVM スイッチが統合され、KX2 デバイスで URL または IP ア ドレスが割り当てられているブレード シャーシの Web ブラウ ザ インタフェース。
- ノードからインタフェースを削除するには、以下の手順に従います。
- 1. [ノード] タブをクリックします。
- 2. 削除するインタフェースを持つノードをクリックします。
- 3. [インタフェース] テーブルで、削除するインタフェースの行をクリ ックします。
- 4. [削除] をクリックします。確認メッセージが表示されます。
- 5. [はい] をクリックして、インタフェースを削除します。

インタフェースをブックマークに設定

特定のインタフェースから頻繁にノードにアクセスする場合は、そのイ ンタフェースをブックマークに設定すると、ブラウザから簡単に使用で きます。

- ブラウザでインタフェースをブックマークに設定するには
- [ノード] タブで、ブックマークに設定するインタフェースを選択します。インタフェースを表示するには、ノードを展開する必要があります。
- [ノード] メニューの [ノード インタフェースをブックマークに設定] を選択します。
- 3. [URL をクリップボードにコピー] を選択します。
- 4. [OK] をクリックします。URL がクリップボードにコピーされます。
- 5. 新しいブラウザ ウィンドウを開き、URL をアドレス フィールドに 貼り付けます。
- 6. Enter キーを押して URL に接続します。
- 7. URL をブックマーク ("お気に入り" とも呼ばれます) としてブラウ ザに追加します。



- Internet Explorer でインタフェースをブックマークに設定する (インタフェースをお気に入りに追加する) には
- [ノード] タブで、ブックマークに設定するインタフェースを選択し ます。インタフェースを表示するには、ノードを展開する必要があ ります。
- [ノード] メニューの [ノード インタフェースをブックマークに設定] を選択します。
- 3. [ブックマークに追加 (IE のみ)] を選択します。
- 4. ブックマークのデフォルト名が [ブックマーク名] フィールドに表示 されます。Internet Explorer の [お気に入り] リストに表示される名 前を変更できます。
- 5. [OK] をクリックします。[お気に入りの追加] ウィンドウが表示され ます。
- 6. [OK] をクリックして、[お気に入り] リストにブックマークを追加し ます。
- ブックマークに設定したインタフェースにアクセスするには
- **1**. ブラウザ ウィンドウを開きます。
- ブラウザのブックマークのリストから、ブックマークに設定したインタフェースを選択します。
- 3. CC-SG Access Client が表示されたら、インタフェースへのアクセ ス権を持つユーザとしてログインします。インタフェースへの接続 が開始されます。
- すべてのノードのブックマーク URL を取得するには、以下の手順 に従います。
- ノード資産レポートですべてのノードのブックマーク URL を取得できます。「ノード資産レポート 『241p. 』」を参照してください。

ノードへのダイレクト ポート アクセスの設定

「ノード インタフェースをブックマークに設定」機能を使用して、ノードへダイレクト ポート アクセスを設定できます。

「*インタフェースをブックマークに設定* **『152**p. **』**」を参照してください。



ノードの関連、場所、および連絡先の一括コピー

ー括コピー コマンドを使用すると、カテゴリ、エレメント、場所、お よび連絡先の情報を 1 つのノードから他の複数のノードにコピーする ことができます。ただし、このプロセスでコピーされるプロパティは選 択した情報のみです。選択したノードに同じタイプの情報が存在する場 合、一括コピー コマンドを実行すると、既存のデータが新しく割り当 てた情報と置き換えられます。

- ノードの関連、場所、および連絡先情報を一括コピーするには、以下の手順に従います。
- 1. [ノード] タブをクリックしてノードを選択します。
- 2. [ノード]>[一括コピー]を選択します。
- [使用できるノード] リストで、[ノード名] フィールドに表示された ノードの関連、場所、および連絡先情報のコピー先となるノード (1 つ以上) を選択します。
- [>] をクリックすると、ノードが [選択されたノード] リストに追加 されます。
- 5. [選択されたノード] リストからノードを削除するには、ノードを選 択し、[<] をクリックします。
- 6. [関連] タブで、[ノードの関連のコピー] チェックボックスを選択して、ノードのすべてのカテゴリとエレメントをコピーします。
 - このタブで、データを変更、追加、または削除できます。変更 されたデータが、[選択されたノード] リストの複数のノード、 および [ノード名] フィールドに表示されている現在のノードに コピーされます。オプション。
- 7. [ロケーションと連絡先] タブで、コピーする情報のチェックボック スを選択します。
 - [ロケーション情報のコピー] チェックボックスを選択すると、[ロケーション] セクションに表示される場所の情報がコピーされ ます。
 - [連絡先情報のコピー] チェックボックスを選択すると、[連絡先] セクションに表示される連絡先の情報がコピーされます。
 - このタブで、データを変更、追加、または削除できます。変更 されたデータが、[選択されたノード] リストの複数のノード、 および [ノード名] フィールドに表示されている現在のノードに コピーされます。オプション。
- 8. [OK] をクリックして一括コピーします。選択した情報がコピーされ るとメッセージが表示されます。



チャットの使用

チャットにより、同じノードに接続されているユーザが互いに通信でき ます。ノードでチャット セッションを開始するには、そのノードに接 続されている必要があります。同じノード上のユーザのみが、互いにチ ャットすることができます。

- ▶ チャット セッションに参加するには、以下の手順に従います。
- 1. [ノード]>[チャット]>[チャット セッションの開始] を選択します
- 左下のフィールドにメッセージを入力し、[送信] をクリックします。 すべてのユーザに表示されるよう、メッセージが左上のフィール ドに表示されます。
- すでに進行中のチャット セッションに参加するには、以下の手順に 従います。
- [ノード]>[チャット]>[チャット セッションの表示] を選択します。
- ▶ チャット セッションを終了するには、以下の手順に従います。
- 1. チャット セッションで [終了] をクリックします。確認メッセージ が表示されます。
 - [はい]をクリックして、すべての参加者のチャット セッション を閉じます。
 - 他の参加者に対しては実行したままにしてチャット セッション を閉じるには、[いいえ]をクリックします。



CSV ファイルのインポートによるノードの追加

値が含まれている CSV ファイルをインポートすることによって、ノー ドとインタフェースを CC-SG に追加できます。

ノードをインポートおよびエクスポートするには、デバイス、ポート、およびノードの管理権限、および **CC** の設定と制御権限が必要です。

関連するすべてのデバイスとノードへのアクセスを付与するポリシーが 割り当てられている必要があります。すべてのノードおよびすべてのデ バイスに対するフル アクセス ポリシーを推奨します。

アウト オブバンド KVM インタフェースまたはアウト オブ バンド シ リアル インタフェース、およびパワー インタフェースをインポートま たはエクスポートするには、関連するすべてのデバイスへのアクセスを 付与するポリシーが割り当てられている必要があります。

制御システム、仮想ホスト、仮想マシンなどの仮想インフラストラクチ ャのノードとインタフェースは、エクスポートまたはインポートされま せん。



ノードの CSV ファイルの要件

ノードの CSV ファイルでは、ノード、インタフェース、およびそれら を CC-SG に追加するために必要な詳細が定義されています。

- ノードには、固有の名前が必要です。重複するノード名を入力する と、名前が一意になるようにカッコで囲まれた数字が名前に付加さ れてノードが追加されます。CSV ファイルでノードにカテゴリとエ レメントも割り当てる場合は、ノード名が重複していると、カテゴ リとエレメントが間違ったノードに割り当てられることがあります 。これを防ぐには、各ノードのに一意の名前を付けます。または、 まずノードをインポートし、CC-SG で名前を確認してから別のフ ァイルをインポートして、カテゴリとエレメントを正しいノード名 に割り当てます。
- アウト オブ バンド インタフェースを追加するには、関連ポートが CC-SG で未設定である必要があります。
- 仮想インフラストラクチャのノードとインタフェースをインポート することはできません。[ノード]>[仮想]のオプションを使用しま す。
- CSV ファイル内で ADD NODE コマンドの後にある最初のインタ フェースが、ノードのデフォルト インタフェースとして割り当てら れます。
- 有効な CSV ファイルの作成に必要なすべてのタグとパラメータが 含まれているコメントを参照するには、CC-SG からファイルをエ クスポートします。「ノードのエクスポート 『169p. 』」を参照し てください。
- すべての CSV ファイルの追加要件を満たします。「CSV ファイル の共通要件 『412p. 』」を参照してください。

CSV ファイルにノードを追加する場合

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	NODE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ノード名	必須フィールド。
4	説明	オプション。



列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	NODE-OOBKVM-INTERFAC E	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ノード名	[Raritan ポート名] に入力したのと 同じ値を入力します。
4	Raritan デバイス名	必須フィールド。 デバイスはすでに CC-SG に追加さ れている必要があります。
5	ポート番号	必須フィールド。
6	ブレード スロット/KVM スイッチ ポート	ノードがブレードに関連付けられて いる場合は、スロット番号を入力し ます。 階層化された汎用のアナログ KVM スイッチにノードが関連付けられて いる場合は、ポート番号を入力しま す。
7	Raritan ポート名	空白のままにした場合は、デバイス の既存のポート名が使用されます。 新しい値を入力すると、SX デバイ スを除いて、名前はデバイスにコピ ーされます。
8	インタフェース名	[Raritan ポート名] に入力したのと 同じ値を入力します。
9	説明	オプション。

CSV ファイルにアウト オブ バンド KVM インタフェースを追加 する場合

CSV ファイルにアウト オブ バンド シリアル インタフェースを追加する場合

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。



列番号	タグまたは値	詳細
2	NODE-OOBSERIAL-INTER FACE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ノード名	[Raritan ポート名] に入力したのと 同じ値を入力します。
4	Raritan デバイス名	必須フィールド。
5	ポート番号	必須フィールド。
6	Raritan ポート名	空白のままにした場合は、デバイス の既存のポート名が使用されます。 新しい値を入力すると、SX デバイ スを除いて、名前はデバイスにコピ ーされます。
7	インタフェース名	[Raritan ポート名] に入力したのと 同じ値を入力します。
8	ボーレート	SX ポートにのみ有効です。
9	パリティ	SX ポートにのみ有効です。
10	フロー制御	SX ポートにのみ有効です。
11	説明	オプション。

▶ CSV ファイルに RDP インタフェースを追加する場合

CSV ファイル 内の列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	NODE-RDP-INTERFACE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ノード名	必須フィールド。
4	インタフェース名	必須フィールド。
5	IP アドレスまたはホスト 名	必須フィールド。
6	TCP ポート	デフォルトは 3389 です。
7	サービス アカウント名	オプション。



CSV ファイル 内の列番号	タグまたは値	詳細
8	ユーザ名	オプション。
9	パスワード	オプション。
10	ユーザ タイプ	REMOTE または CONSOLE デフォルトは REMOTE です。
11	キーボード タイプ	US、UK、Arabic、Danish、 German、Spanish、Finnish、 French、Belgian、Croatian、 Italian、Japanese、 Lithuanian、Latvian、 Macedonian、Norwegian、 Polish、Portuguese、 Brazilian、Russian、 Slovenian、Swedish、または Turkish デフォルトは US です。
12	説明	オプション。
13	RDP タイプ	Java または Microsoft デフォルトは Java です。

CSV ファイルに SSH または TELNET インタフェースを追加する 場合

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	SSH インタフェースの場 合は NODE-SSH-INTERFACE TELNET インタフェース の場合は NODE-TELNET-INTERFAC E	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ノード名	必須フィールド。
4	インタフェース名	必須フィールド。
5	IP アドレスまたはホスト 名	必須フィールド。



列番号	タグまたは値	詳細
6	TCP ポート	SSH の場合、デフォルトは 22 で す。
		TELNET の場合、テフォルトは 23 です。
7	サービス アカウント名	オプション。ユーザ名とパスワード を指定する場合は空白のままにしま す。
8	ユーザ名	オプション。サービス アカウントを 指定する場合は空白のままにします 。
9	パスワード	オプション。
10	説明	オプション。

▶ CSV ファイルに VNC インタフェースを追加する場合

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	NODE-VNC-INTERFACE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ノード名	必須フィールド。
4	インタフェース名	必須フィールド。
5	IP アドレスまたはホスト 名	必須フィールド。
6	TCP ポート	デフォルトは 5900 です。
7	サービス アカウント名	オプション。パスワードを指定する 場合は空白のままにします。
8	パスワード	オプション。サービス アカウントを 指定する場合は空白のままにします 。
9	説明	オプション。



CSV ファイルに DRAC KVM、DRAC パワー、ILO KVM、ILO パワー、Integrity ILO2 パワー、または RSA パワー インタフェースを追加する場合

DRAC、ILO、および RSA インタフェースをインポートするときに、 KVM インタフェースとパワー インタフェースの両方を指定する必要が あります。そうしなければ、インポートは失敗します。

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	DRAC KVM インタフェース の場合は NODE-DRAC-KVM-INTERFAC E DRAC パワー インタフェー スの場合は NODE-DRAC-POWER-INTERF ACE iLO KVM インタフェースの場 合は NODE-ILO-KVM-INTERFACE iLO パワー インタフェースの 場合は NODE-ILO-POWER-INTERFA CE Integrity ILO2 パワー インタ フェースの場合は NODE-INT-ILO2-POWER-IN TERFACE RSA パワー インタフェース の場合は NODE-RSA-POWER-INTERFA CE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ノード名	必須フィールド。
4	インタフェース名	必須フィールド。
5	IP アドレスまたはホスト名	必須フィールド。
6	サービス アカウント名	サービス アカウント、またはユーザ 名とパスワードを入力する必要があ ります。 ユーザ名とパスワードを指定する場


Ch 8: ノード、ノード グループ、インタフェース

列番号	タグまたは値	詳細
		合は空白のままにします。
7	ユーザ名	サービス アカウント、またはユーザ 名とパスワードを入力する必要があ ります。 サービス アカウントを指定する場合 は空白のままにします。
8	パスワード	サービス アカウント、またはユーザ 名とパスワードを入力する必要があ ります。 サービス アカウントを指定する場合 は空白のままにします。
9	説明	オプション。
10*	TCP ポート	*NODE-DRAC-POWER-INTERFACE のみの場合、TCP ポートを指定しま す。 デフォルトは 22 です。

▶ CSV ファイルに RSA KVM インタフェースを追加する場合

DRAC、ILO、および RSA インタフェースをインポートするときに、 KVM インタフェースとパワー インタフェースの両方を指定する必要が あります。そうしなければ、インポートは失敗します。

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	NODE-RSA-KVM-INTERFA CE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ノード名	必須フィールド。
4	インタフェース名	必須フィールド。
5	IP アドレスまたはホスト 名	必須フィールド。
6	TCP ポート	デフォルトは 2000 です。
7	サービス アカウント名	ユーザ名とパスワードを指定する場 合は空白のままにします。
8	ユーザ名	サービス アカウントを指定する場合



Ch 8: ノード、ノード グループ、インタフェース

列番号	タグまたは値	詳細
		は空白のままにします。
9	パスワード	サービス アカウントを指定する場合 は空白のままにします。
10	説明	オプション。

▶ CSV ファイルに IPMI パワー インタフェースを追加する場合

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	NODE-IPMI-INTERFACE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ノード名	必須フィールド。
4	インタフェース名	必須フィールド。
5	IP アドレスまたはホスト 名	必須フィールド。
6	UDP ポート	デフォルトは 623 です。
7	認証	MD5、None、OEM、または PASSWORD デフォルトは PASSWORD です。
8	間隔	確認する頻度を秒単位で入力します 。デフォルトは 550 です。
9	サービス アカウント名	ユーザ名とパスワードを指定する場 合は空白のままにします。
10	ユーザ名	サービス アカウントを指定する場合 は空白のままにします。
11	パスワード	サービス アカウントを指定する場合 は空白のままにします。
12	説明	オプション。



列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	NODE-POWER-INTERFACE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ノード名	必須フィールド。
4	インタフェース名	必須フィールド。
5	電源タップ名	必須フィールド。
6	アウトレット	必須フィールド。
7	管理デバイス	電源タップが接続されているデバイ スの名前。 Dominion PX を除くすべての電源タ ップの必須フィールドです。
8	管理ポート	電源タップが接続されているデバイ スのポートの名前。 Dominion PX を除くすべての電源タ ップの必須フィールドです。
9	説明	オプション。

CSV ファイルに管理対象電源タップ インタフェースを追加する場合

▶ CSV ファイルに Web ブラウザ インタフェースを追加する場合

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	NODE-WEB-INTERFACE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ノード名	必須フィールド。
4	インタフェース名	必須フィールド。
5	URL	必須フィールド。
6	TCP ポート	デフォルトは 80 です。



列番号	タグまたは値	詳細
7	サービス アカウント名	オプション。ユーザ名とパスワード を指定する場合は空白のままにしま す。
8	ユーザ名	オプション。サービス アカウントを 指定する場合は空白のままにします 。
9	パスワード	オプション。サービス アカウントを 指定する場合は空白のままにします 。
10	ユーザ名フィールド	オプション。「 Web ブラウザ イン <i>タフェースの追加のヒント</i> 『 150 p. 』 」を参照してください。
11	パスワード フィールド	オプション。「 Web ブラウザ イン <i>タフェースの追加のヒント</i> 『 150 p. 』 」を参照してください。
12	説明	オプション。

▶ CSV ファイルに Power IQ Proxy のパワー制御インタフェースを 追加する場合

このインタフェース タイプの設定についての詳細は、「**Power IQ IT デ** バイスのパワー制御 『377p. 』」を参照してください。

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	NODE-POWER-PIQ-INTERFA CE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ノード名	必須フィールド。
4	インタフェース名	必須フィールド。
5	外部キー	 IT デバイスがすでに Power IQ に追加されている場合は、[Data Center (データ センター)] タブの IT デバイスのページで外部キー を探し、そのテキストをこのフィ ールドに入力します。 IT デバイスがまだ Power IQ に



Ch 8: ノード、ノード グループ、インタフェース

列番号	タグまたは値	詳細
		追加されていない場合は、テキス ト値を入力します。ただし、IT デバイスを Power IQ に追加する ときに同じ値を使用する必要があ ります。すべてのノードとインタ フェースの情報を含むファイルを エクスポートによって簡単に作成 できます。「ノードのエクスポー ト 『169p. 』」を参照してくださ い。
6	管理 Power IQ 名	IT デバイスを管理する Power IQ の 名前を入力します。この名前は、[ア クセス] > [Power IQ Services (Power IQ サービス)] > [Power IQ Device Name (Power IQ デバイス名)] ダイ アログ ボックスの [Power IQ Device Name (Power IQ デバイス名)] フィ ールドの値と一致する必要がありま す。 「 <i>Power IQ サービスの設定</i> 『378 p. 』」を参照してください。
7	説明	オプション。

CSV ファイルでカテゴリとエレメントをノードに割り当てる場合

カテゴリとエレメントが CC-SG ですでに作成されている必要があります。

CSV ファイルで同じカテゴリの複数のエレメントをノードに割り当て ることができます。

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	NODE-CATEGORYELEMENT	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ノード名	必須フィールド。
4	カテゴリ名	必須フィールド。
5	エレメント名	必須フィールド。



ノードの CSV ファイルの例

ADD, NODE, NJSomersetEmailServer, Physical Server

ADD, NODE-OOBKVM-INTERFACE, NJSomersetEmailServer, NJSomersetEmailServer, DKX2-NY-Rack7, NJSomersetEmailServer ADD, NODE-RDP-INTERFACE,

NJSomersetEmailServer,,192.168.53.42,,admins,,,,,

ADD, NODE-POWER-INTERFACE, NJSomersetEmailServer, Power,,,,Rack17,4

ADD, NODE-CATEGORYELEMENT, NJSomersetEmailServer, Location, Somerset

ノードのインポート

CSV ファイルを作成したら、エラーがないかどうかを確認してからイ ンポートします。

重複するレコードはスキップされ、追加されません。

- 1. [管理]>[インポート]>[ノードのインポート]を選択します。
- [参照] をクリックし、インポートする CSV ファイルを選択します。
 [開く] をクリックします。
- 3. [確認] をクリックします。[分析レポート] 領域にファイルの内容が 表示されます。
 - ファイルが有効でない場合は、エラー メッセージが表示されます。[OK] をクリックし、ページの [問題] 領域でファイルに関する問題の説明を参照します。[ファイルに保存] をクリックして問題リストを保存します。CSV ファイルを修正し、再度検証します。「CSV ファイルの問題のトラブルシューティング 『414p.』」を参照してください。
- 4. [インポート] をクリックします。
- [アクション] 領域でインポート結果を確認します。正常にインポートされたアイテムは、緑色のテキストで表示されます。インポートに失敗したアイテムは、赤いテキストで表示されます。重複するアイテムがすでに存在するか、またはすでにインポートされているためにインポートに失敗したアイテムも赤いテキストで表示されます。
- 6. インポート結果の詳細を参照するには、監査証跡レポートを確認し ます。「インポートに関する監査証跡エントリ 『413p. 』」を参照 してください。



ノードのエクスポート

エクスポート ファイルの一番上には、ファイル内の各アイテムを説明 するコメントが含まれています。コメントは、インポートするファイル を作成するための指示として使用できます。

- ▶ ノードをエクスポートするには、以下の手順に従います。
- 1. [管理]>[エクスポート]>[ノードのエクスポート]を選択します。
- 2. [ファイルにエクスポート] をクリックします。
- 3. ファイルの名前を入力し、保存する場所を選択します。
- 4. [保存] をクリックします。

CSV ファイルのインポートを利用した IP アドレスの編集

CSV ファイルのインポートを利用して新たに IP アドレスをアップロードすることによって変更された IP アドレスを編集します。

この方法は、多くの IP アドレスを迅速に更新する場合に最適です。

- CSV ファイルのインポートを利用して IP アドレスを編集するには 、以下の手順に従います。
- ノードの CSV ファイルをエクスポートします。「ノードのエクスポ ート 『169p. 』」を参照してください。
- 2. エクスポートしたファイルを Microsoft Excel などのスプレッドシ ート プログラムで開きます。すぐにファイルを .csv として保存し 、正しいファイル タイプになっていることを確認します。
- 3. 変更する IP アドレスが含まれている行を検索します。新しい IP アドレスをセルに入力します。
- 4. 変更する各行の最初のセルで、"ADD" コマンドを削除し、 "MODIFY" コマンドを入力します。
- 5. 変更しない行をすべて削除します。
- 6. ファイルを .csv として保存します。
- .csv ファイルをインポートします。「ノードのインポート『168p. 』」を参照してください。



ノード グループの追加、編集、削除

ノード グループの概要

ノード グループは、ノードをセットとして整理するために使用されま す。ノード グループは、特定のノード セットへのアクセスを許可また は拒否するポリシーの基本となります。「ポリシーの追加 『198p. 』」 を参照してください。ノードの手動によるグループ化は、Select メソッ ドを使用して行うことも、Describe メソッドを使用して共通の属性の セットを示すブール式を作成して行うこともできます。

ガイド設定を使用してノードのカテゴリとエレメントを作成した場合は 、共通属性に従ってノードを整理する方法がすでに作成されています。 CC-SG は、これらのエレメントを基にして、デフォルトのアクセス ポ リシーを自動的に作成します。カテゴリおよびエレメントの作成の詳細 については、「*関連、カテゴリ、エレメント*『47p.』」を参照してく ださい。

- ▶ ノード グループを表示するには、以下の手順に従います。
- [関連]>[ノード グループ] を選択します。[ノード グループ マネージャ] ウィンドウが表示されます。既存のノード グループのリストが左側に、選択したノード グループに関する詳細がメイン パネルに表示されます。
 - 既存のノード グループのリストは、左側に表示されます。ノード グループをクリックして、ノード グループ マネージャでノードの詳細を表示します。
 - グループが任意に形成されている場合は、グループに属しているノードと属していないノードのリストを示す[ノードの選択] タブが表示されます。
 - グループが共通の属性を基にして形成されている場合は、[ノードの説明]タブが表示されます。このタブには、グループのノード選択を制御するルールが含まれます。
 - [ノード グループ] リストでノードを検索するには、リストの下部にある [検索] フィールドに文字列を入力し、[検索] をクリックします。検索方法は、[プロファイル] 画面で設定されます。
 「ユーザとユーザ グループ 『176p. 』」を参照してください。
 - 属性を基にしたグループを表示している場合は、[ノードの表示] をクリックして、ノード グループに現在属しているノードのリ ストを表示します。ノードとそのすべての属性を示す [ノード グループ内のノード] ウィンドウが開きます。



ノード グループの追加

- ▶ ノード グループを追加するには、以下の手順に従います。
- 1. [関連]>[ノード グループ] を選択します。[ノード グループ マネー ジャ] ウィンドウが表示されます。
- 2. [グループ]>[新規] を選択します。ノード グループのテンプレート が表示されます。
- 3. 作成するノード グループの名前を [グループ名] フィールドに入力 します。名前の長さに関する CC-SG のルールについての詳細は、 「*命名規則* 『435p. 』」を参照してください。
- グループにノードを追加する方法には、[ノードの選択] と [ノードの説明]の2種類があります。ノードの選択では、利用可能なノードのリストからノードを選択して、自由にノードをグループに割り当てることができます。ノードの説明では、ノードを説明するルールを指定でき、説明に一致するノードがグループに含まれます。

describe メソッドと select メソッドの対比

describe メソッドは、カテゴリやエレメントなど、ノードまたはデバイ スの一部の属性に基づいてグループを作成したい場合に使用します。 describe メソッドの利点は、記述された同じ属性を持つデバイスまたは ノードを複数追加する場合に、それらが自動的にグループを形成すると いう点です。

select メソッドは、特定のノードのグループを手動で作成する場合に使用します。CC-SG に新しいノードおよびデバイスを追加しても、グループが自動的に形成されることはありません。CC-SG に追加後、新しいノードまたはデバイスを手動でグループに追加する必要があります。

これら2 つのメソッドは併用できません。

ー方のメソッドで作成したグループは、編集の際に同じメソッドを使用 する必要があります。メソッドを切り替えると、現在のグループ設定が 上書きされます。

ノードの選択

[ノードの選択] オプションによってノード グループを追加するには、以下の手順に従います。

- 1. [ノードの選択] タブをクリックします。
- [デバイス名] ドロップダウン メニューをクリックし、デバイスを選択し、[利用可能] リストでそのデバイスからのインタフェースを備えたノードのみを表示するようフィルタします。



Ch 8: ノード、ノード グループ、インタフェース

- 3. [利用可能] リストで、グループに追加するノードを選択し、[追加] をクリックして、そのノードを [選択中] リストに移動します。[選 択中] リストのノードがグループに追加されます。
 - グループからノードを削除するには、[選択中] リストでノード 名を選択し、[削除] をクリックします。
 - [利用可能] または [選択中] リストのいずれでも、ノードを検索 できます。リストの下にあるフィールドに検索条件を入力し、[実行] をクリックします。
- このグループのノードへのアクセスを常に許可するポリシーを作成 する場合は、[グループにフル アクセス ポリシーを作成] チェック ボックスを選択します。
- グループにノードを追加したら、[OK] をクリックして、ノード グ ループを作成します。グループが左側にあるノード グループのリス トに追加されます。

ノードの説明

- [ノードの説明] オプションによってノード グループを追加するには、以下の手順に従います。
- 1. [ノードの選択] タブをクリックします。
- 2. [新しい行をテーブルに追加] アイコン アイコン たクリックして、テーブルに新しいルール用の行を追加します。ルールには、ノードに対して比較できる説明を含めます。
- 3. 行の各欄をダブルクリックして、該当するセルをドロップダウンメ ニューに含め、各コンポーネントの値を以下の中から選択します。
 - プレフィックス これは空白のままにしておくか、NOT を選択 します。NOT を選択すると、このルールにより、表現全体の反 対の値によりフィルタされます。
 - カテゴリ・ルールで評価される属性を選択します。ここでは、
 関連マネージャで作成した全カテゴリを使用できます。また、
 ノード名とインタフェースも含まれます。任意のブレードシャーシがシステムで設定されている場合、デフォルトでブレードシャーシカテゴリが利用可能になります。
 - 演算子 カテゴリとエレメント項目間で実行される比較操作を 選択します。3 つの演算子 = (に等しい)、LIKE (名前のエレメ ントを検索するのに使用される)、<> (に等しくない) を使用で きます。
 - エレメント 比較の対象となるカテゴリ属性の値を選択します 。選択したカテゴリに関連付けられたエレメントのみがここに 表示されます (たとえば、「Department」カテゴリを評価する場 合は、「Location」エレメントはここに表示されません)。



 ルール名 - これは、この行のルールに割り当てられた名前です 。これらの値は編集できません。[簡潔式] フィールドに説明を 入力する際に、これらの値を使用します。

たとえば、「Department = Engineering」というルールがあると すると、カテゴリ「Department」が「Engineering」に設定され ているすべてのノードを意味します。これは、ノードの追加操 作中に関連を設定する場合に実行される操作と同じです。

- 4. 別のルールを追加するには、[新しい行をテーブルに追加] アイコン をもう一度クリックして、必要な設定を行います。複数のルールを 設定すると、ノードの評価に複数の条件を適用することができるた め、より正確な説明が可能になります。
 - ルールを削除する場合は、テーブル内でルールをハイライトし 、[行の削除] アイコン 🗾 をクリックします。
- 5. ルールの表は、ノードを評価するための条件を利用可能にします。 ノード グループの説明を入力するには、ルール名によりルールを 簡潔式] フィールドに追加します。説明に 1 つのルールしか必要な い場合は、フィールドにルールの名前を入力します。複数のルール が評価される場合は、以下のように、それぞれの関係を説明する論 理演算のセットを使用して、フィールドにルールを入力します。
 - & AND 演算子。true と評価されるためには、説明 (または説 明の一部)で、ノードがこの演算子の両辺にあるルールを満た す必要があります。
 - |-OR 演算子。true と評価されるためには、説明 (または説明) の一部)で、ノードがこの演算子の両辺またはいずれかのルー ルを満たす必要があります。
 - (と)-グループ化演算子。これは、カッコ内に含まれるサブセ クションに説明を分割します。カッコ内のセクションは、説明 のその他の部分がノードと比較される前に評価されます。カッ コで囲まれたグループは、別のカッコで囲まれたグループ内に ネストすることができます。

例 1: エンジニアリング部門に属するノードを記述する場合は、 「Department = Engineering」というルールを作成します。これ を、Rule0 とします。次に、[簡潔式] フィールドに「Rule0」と 入力します。



例 2: エンジニアリング部門に属するデバイス グループ、また はフィラデルフィアにあるデバイス グループを説明し、さらに すべてのマシンが 1 GB のメモリを持つ必要があることを指定 するには、次の 3 つのルールを作成する必要があります。 Department = Engineering (Rule0) Location = Philadelphia (Rule1) Memory = 1GB (Rule2)。これらのルールを相互に関連付 ける必要があります。デバイスは、エンジニアリング部門に属 するか、フィラデルフィアにあるいずれかのデバイスとなるの で、OR 演算子 ())を使用して、Rule0|Rule1 のように 2 つの ルールを結合します。これを (Rule0|Rule1) のようにカッコで 囲み、この比較をまず行います。最後に、デバイスは、この比 較を満たし、さらに 1GB のメモリを持つ必要があるので、 AND 演算子 & を使用して、(Rule0|Rule1)&Rule2 のようにこ のセクションを Rule2 と結合します。この最終的な式を、[簡潔 式] フィールドに入力します。

注: 演算子 & および | の前後にはスペースを入れる必要がありま す。スペースを入れない場合、テーブルからすべてのルールを削除 すると、[簡潔式] フィールドがデフォルトの式 (Rule0 & Rule1 & Rule2 など) を返します。

- [簡潔式] フィールドに説明を入力したら、[確認] をクリックします。説明が正しく入力されなかった場合は、警告が表示されます。説明を正しく入力すると、[正規式] フィールドに正規化された式が表示されます。
- [ノードの表示]をクリックして、この式を満たすノードを表示します。現在の式でグループ化されるノードを示す[ノード グループ内のノード]ウィンドウが開きます。これは、説明が正しく記述されているかどうかを確認するため使用できます。正しく記述されていない場合は、ルール テーブルまたは[簡潔式]フィールドに戻って、式を調整できます。
- このグループでノードへのアクセスを常に許可するポリシーを作成 する場合は、[グループにフル アクセス ポリシーを作成] チェック ボックスを選択します。
- このグループに属するノードの説明を入力したら、[OK] をクリック して、ノード グループを作成します。グループが左側にあるノード グループのリストに追加されます。

ノード グループの編集

ノード グループを編集して、グループのメンバシップや説明を変更し ます。

- ノード グループを編集するには、以下の手順に従います。
- [関連]>[ノード グループ] を選択します。[ノード グループ マネージャ] ウィンドウが開きます。



Ch 8: ノード、ノード グループ・インタフェース

- 2. [ノード グループ] リストで編集するノードをクリックします。その ノードの詳細が、[ノード グループ] ウィンドウに表示されます。
- 3. ノード グループの設定方法についての詳細は、「ノードの選択」または「ノードの説明」にある指示を参照してください。
- 4. [OK] をクリックして変更を保存します。

ノード グループの削除

- ▶ ノード グループを削除するには、以下の手順に従います。
- [関連]>[ノード グループ] を選択します。[ノード グループ マネージャ] ウィンドウが開きます。
- 2. 左側の [ノード グループ] リストで、削除するノードを選択します。
- 3. [グループ]>[削除] を選択します。
- 4. [ノード グループの削除] パネルが表示されます。[削除] をクリック します。
- 5. 表示される確認メッセージで [はい] をクリックします。



ユーザとユーザ グループ

ユーザ アカウントは、ユーザにユーザ名とパスワードを割り当てて CC-SG にアクセスできるようにするために作成されます。

ユーザ グループは、そのメンバの権限のセットを定義します。ユーザ 自信に権限を割り当てることはできません。ユーザ グループのみに割 り当てることができます。すべてのユーザは、少なくとも 1 つのユー ザ グループに属する必要があります。

CC-SG は、一元化されたユーザ リスト、認証用のユーザ グループ リ スト、および承認を保持します。

外部認証を使用するように、CC-SG を設定することもできます。「**リモ** ート認証 『210p. 』」を参照してください。

ユーザ グループに割り当てることができるアクセス用のポリシーを作 成する必要もあります。「*アクセス制御のポリシー*『**197**p.』」を参照 してください。

この章の内容

[ユーザ] タブ	177
デフォルトのユーザ グループ	178
ユーザ グループの追加、編集、削除	179
ユーザあたりの KVM セッション数の制限	182
ユーザ グループのアクセス監査の設定	183
ユーザの追加、編集、削除	183
ユーザのグループへの割り当て	186
ユーザをグループから削除	187
CSV ファイルのインポートによるユーザの追加	187
ユーザ プロファイル	193
ユーザのログアウト	195
ユーザの一括コピー	196



Ch 9

[ユーザ] タブ

[ユーザ] タブをクリックすると、CC-SG のすべてのユーザ グループと ユーザが表示されます。

CC Super-User CC Users CC Users IeseUser NinaUser System Administrators Charles Charles Charlie Charlie Charlie Charlie Charlie Charlie Charlie Charlie Charlie Charlie Charlie Charlie Charlie Charlie Charlie Charles Charle	Nodes	Users	Devices
▼ Search For User	■ *** CCC ■ *** CCCC	Super-Us Users leseUser NinaUser stem Adm charles charlesm Charlie charlie2 hetal karl kunalg lese monica nina owenc raritan richardr shail victor	inistrators
	▼ Search For User		
Search Clear			

ユーザは、所属するユーザ グループ下にネストされます。ユーザが割 り当てられているユーザ グループには、その横に + 記号が表示されま す。+ または - をクリックすることで、リストを広げたり、折りたたん だりします。CC-SG に現在ログインしているアクティブなユーザは、 太字で表示されます。

[ユーザ] タブを使用すると、ツリー内でユーザを検索できます。



デフォルトのユーザ グループ

CC-SG は、次のデフォルトのユーザ グループで設定されています。 **CC** スーパーユーザ、システム管理者、**CC** ユーザ。

CC スーパーユーザ グループ

CC スーパーユーザ グループは、すべての管理およびアクセス権限を 持ちます。このグループのメンバになれるのは、1 人だけです。デフォ ルトのユーザ名は admin です。デフォルトのユーザ名は変更できます 。CC スーパーユーザ グループを削除することはできません。また、 CC スーパーユーザ グループに割り当てられた権限の変更、メンバの 追加、メンバの削除も行うことはできません。CC スーパーユーザ グ ループのメンバには、強力なパスワードが必要です。強力なパスワード の条件は次のとおりです。

- パスワードには少なくとも1文字を使用する。
- パスワードには少なくとも1文字を使用する。
- パスワードには少なくとも1文字は数字を使用する。
- パスワードには少なくとも 1 文字は特殊文字 (感嘆符やアンパ ーサンドなど)を使用する

注: CSV ファイルのインポートによって CC スーパーユーザ グループ を変更することはできません。

システム管理者グループ

システム管理者は、すべての管理およびアクセス権限を持ちます。権限 を変更することはできません。メンバの追加または削除は可能です。

CC ユーザ グループ

CC ユーザ グループは、インバンドおよびアウト オブ バンド ノード へのアクセス権を持ちます。権限の変更、メンバの追加や削除が可能で す。

重要: メニュー項目の多くは、適切なユーザ グループまたはユーザを選 択しない限り、選択できません。



ユーザ グループの追加、編集、削除

ユーザ グループの追加

最初にユーザ グループを作成すると、ユーザを追加する際に整理しや すくなります。ユーザ グループを作成すると、権限セットがそのユー ザ グループに割り当てられます。そのグループに割り当てられるユー ザは、それらの権限を継承します。たとえば、グループを作成してユー ザ管理権限を割り当てると、このグループに割り当てられたユーザはす べて、[ユーザ管理] メニューのコマンドを表示して実行できるようにな ります。「ユーザ グループ権限 『398p.』」を参照してください。

ユーザ グループの設定には、次の 4 つの基本的な手順あります。

- グループに名前を付けて、説明を加える。
- ユーザ グループが持つ権限を選択する。
- ユーザ グループがノードのアクセスに使用できるインタフェース タイプを選択する。
- ユーザ グループがどのノードにアクセスできるかを指定するポリシーを選択する。
- ユーザ グループを追加するには、以下の手順に従います。
- 1. [ユーザ]>[ユーザ グループ マネージャ]>[ユーザ グループの追加] を選択します。[ユーザ グループの追加] 画面が表示されます。
- [ユーザ グループ名] フィールドに、ユーザ グループ名を入力します。ユーザ グループには、固有の名前が必要です。名前の長さに関する CC-SG のルールについての詳細は、「命名規則 『435p. 』」を参照してください。
- 3. このグループの短い説明を [説明] フィールドに入力します。オプション。
- このユーザ グループのユーザごとに、この機能が有効になっている デバイスへのアクセス時の最大 KVM セッション数を設定するには 、[Limit Number of KVM Sessions per Device (デバイスあたりの KVM セッション数を制限する)] チェックボックスをオンにし、 [Max KVM Sessions (1-8) (最大 KVM セッション (1 ~ 8))] フィー ルドで許可するセッション数を選択します。オプション。詳細は、 「ユーザあたりの KVM セッション数の制限 『182p. 』」を参照し てください。
- 5. [権限] タブをクリックします。
- 6. ユーザ グループに割り当てる各権限に対応するチェックボックスを 選択します。



- 権限表の下には、次の3種類のノードアクセスに関する権限を提供する[ノードアクセス]エリアがあります。[アウトオブバンドアクセス]、[インバンドアクセス]、[パワー制御]。ユーザグループに割り当てる各ノードアクセスのタイプに対応するチェックボックスを選択します。
- 8. [デバイス/ノード ポリシー] タブをクリックします。ポリシーの表 が表示されます。

[すべてのポリシー] には、CC-SG で使用できるポリシーがすべて 表示されます。各ポリシーは、ノードのグループにアクセスを許可 または拒否するルールを表します。ポリシーおよびその作成方法の 詳細については、「*アクセス制御のポリシー*『197p. 』」を参照し てください。

 [すべてのポリシー] リストで、ユーザ グループに割り当てるポリシ ーを選択し、[追加] をクリックして、そのポリシーを [選択された ポリシー] リストに移動します。[選択されたポリシー] リストのポ リシーは、ポリシーによって制御されるノードまたはデバイスへの アクセスを許可または拒否できるようにします。ポリシー相互の影 響については、「ユーザ グループのポリシーの割り当て『201p. の "ユーザ グループへのポリシーの割り当で"参照 』」を参照してくだ さい。

この手順を繰り返して、ユーザ グループにポリシーを追加します。

- このグループに、使用可能な全ノードへのアクセスを許可する 場合は、[ポリシーの追加] リストで [フル アクセス ポリシー] を選択してから、[追加] をクリックします。
- ユーザ グループからポリシーを削除する場合は、[選択されたポリシー] リストでポリシー名を選択し、[削除] をクリックします。
- このグループのポリシーの設定が終わったら、[適用] をクリックしてこのグループを保存し、別のグループを作成します。ユーザ グループを追加するには、このセクションの該当する手順を繰り返します。オプション。
- 11. [OK] をクリックして変更を保存します。

ユーザ グループの編集

ユーザ グループを編集して、既存の権限やそのグループのポリシーを 変更します。

注: CC スーパー ユーザ グループの権限またはポリシーを編集するこ とはできません。

▶ ユーザ グループを編集するには、以下の手順に従います。

1. [ユーザ] タブをクリックします。



- [ユーザ] タブでユーザ グループをクリックします。[ユーザ グルー プ プロファイル] 画面が表示されます。
- 3. ユーザ グループの新しい名前を [ユーザ グループ名] フィールドに 入力します。オプション。
- 4. ユーザ グループの新しい説明を [説明] フィールドに入力します。 オプション。
- このユーザ グループのユーザごとに、この機能が有効になっている デバイスへのアクセス時の最大 KVM セッション数を設定するには 、[Limit Number of KVM Sessions per Device (デバイスあたりの KVM セッション数を制限する)] チェックボックスをオンにし、 [Max KVM Sessions (1-8) (最大 KVM セッション (1 ~ 8))] フィー ルドで許可するセッション数を選択します。オプション。詳細は、 「ユーザあたりの KVM セッション数の制限 『182p. 』」を参照し てください。
- 6. [権限] タブをクリックします。
- 7. ユーザ グループに割り当てる各権限に対応するチェックボックスを 選択します。選択解除して、グループからその権限を削除します。
- [ノード アクセス] エリアのドロップダウン メニューでこのグルー プがアクセスするインタフェースのタイプをクリックし、[制御] を 選択します。
- このグループがアクセスできないインタフェースのタイプをクリックし、[拒否]を選択します。
- **10.** [ポリシー] タブをクリックします。**2** つのポリシー表が表示されます。
- グループに追加する各ポリシーについて、[すべてのポリシー] でポ リシーを選択し、[追加] をクリックして、そのポリシーを [選択さ れたポリシー] リストに移動します。[選択されたポリシー] リスト のポリシーは、このポリシーによって制御されるノード (またはデ バイス) へのユーザ アクセスを許可または拒否します。
- 12. ユーザ グループから削除するポリシーごとに、[選択されたポリシー] リストでポリシー名を選択し、[削除] をクリックします。
- 13. [OK] をクリックして変更を保存します。

ユーザ グループの削除

割り当てられたメンバがない場合は、ユーザ グループを削除できます。

▶ ユーザ グループを削除するには、以下の手順に従います。

- 1. [ユーザ] タブをクリックします。
- 2. 削除するユーザ グループをクリックします。
- 3. [ユーザ]>[ユーザ グループ マネージャ]>[ユーザ グループの削除] を選択します。



Ch 9: ユーザとユーザ グループ

4. [OK] をクリックして、ユーザ グループを削除します。

ユーザあたりの KVM セッション数の制限

Dominion KXII、KSXII、および KX (KX1) デバイスとのセッションにつ いて、1 人のユーザに許可する KVM セッション数を制限できます。こ れにより、1 人のユーザが利用可能なすべてのチャネルを一度に使用す ることはできなくなります。

制限を超えてノードに接続しようとすると、現在のセッションに関する 情報を含む警告メッセージが表示されます。このイベントは、接続が拒 否されたことを示すメッセージとしてアクセス レポートに記録されま す。別の新しいセッションを開始する前に、デバイスでセッションを切 断する必要があります。

完全なメッセージ テキストは以下のとおりです。

Connection Denied: Exceeds the allotted number of sessions for the KVM switch this node is attached to. (接続が拒否されました: このノードの接続先 KVM スイッチに割り当てられているセッション数を超えました。) If possible, please disconnect an existing session to the same KVM switch. (可能な場合は、同じ KVM スイッチへの既存のセッションを切断してください。)

KVM スイッチへのアクティブな接続のリストがメッセージに含まれて います。

注: アクセス レポートをメッセージ テキストでフィルタして、トラフ ィックが多いデバイスを見つけることができます。「アクセス レポート 『236p.』」を参照してください。

KVM セッション数の制限は、ユーザ グループごとに設定します。ガイ ド付き設定または CSV のインポートによってユーザ グループを手動 で追加または編集するときに、制限を有効にすることができます。「ユ ーザ グループの追加 『179p. 』」を参照してください。

Dominion KXII デバイスの場合のみ、デバイスの最大接続数に達したときに警告が表示されます。このイベントは、接続が拒否されたことを示すメッセージとしてアクセス レポートに記録されます。

完全なメッセージ テキストは以下のとおりです。

Connection Denied: Exceeds the number of available video channels on the KVM switch this node is attached to. (接続が拒否されました: このノ ードの接続先 KVM スイッチで使用可能なビデオ チャネルの数を超え ました。)



ユーザ グループのアクセス監査の設定

アクセス許可の前にノードにアクセスする理由を入力するために、ユー ザ グループのメンバとなるように要求できます。選択したユーザ グル ープの全メンバにダイアログが表示されます。ユーザがアクセス理由を 入力しない限り、ノード接続は確立されません。この機能は、パワー制 御を含め、あらゆるインタフェース タイプのあらゆるタイプのアクセ スに適用されます。

アクセス理由は、監査証跡およびノード プロファイルの [監査] タブに 記録されます。

- ユーザ グループのアクセス監査を設定するには、以下の手順に従います。
- 1. [ユーザ]>[ノード監査] を選択します。
- [ノードへの接続時にユーザはアクセス情報を入力する必要があります] チェックボックスを選択します。
- [ユーザへのメッセージ] フィールドに、ノードへのアクセス時にユ ーザに表示されるメッセージを入力します。デフォルトのメッセー ジが提供されています。最大長は 256 文字です。
- 矢印ボタンをクリックして、アクセス監査が有効になるユーザ グル ープを [選択中] リストに移動します。Ctrl を押しながらクリックす ると、複数項目を選択できます。

ヒント: 検索フィールドにユーザ グループ名を入力して、リスト内 でハイライトします。部分名の後に * を入力すると、リスト内の類 似したすべての名前がハイライトされます。

列のヘッダをクリックすると、リストがアルファベット順に並べ替 えられます。

5. [更新] をクリックします。

ユーザの追加、編集、削除

ユーザの追加

CC-SG にユーザを追加するときは、ユーザ グループを指定して、ユー ザ グループに割り当てられたアクセス権限をそのユーザに与えます。

ユーザを追加するには、以下の手順に従います。

- 1. [ユーザ] タブで、ユーザが追加されるグループを選択します。
- 2. [ユーザ]>[ユーザ マネージャ]>[ユーザの追加] を選択します。



- [ユーザ名] フィールドに、追加するユーザのユーザ名を入力します。この名前は、CC-SG へのログインに使用されます。名前の長さに関する CC-SG のルールについての詳細は、「命名規則『435p. 』」を参照してください。
- [フルネーム] フィールドに、ユーザの氏名を入力します。名前の長 さに関する CC-SG のルールについての詳細は、「命名規則『435p. 』」を参照してください。
- 5. ユーザが CC-SG にログインできる場合は、[ログイン有効] チェッ クボックスを選択します。
- TACACS+、RADIUS、LDAP、AD などの外部サーバによりユーザ を認証する必要がある場合のみ、リモート認証を確認するチェック ボックスを選択します。リモート認証を使用する場合は、パスワー ドは不要なので、[新しいパスワード] と [パスワード再入力] のフィ ールドは無効になっています。
- 7. [新しいパスワード] と [パスワード再入力] フィールドに、ユーザが CC-SG へのログインに使用するパスワードを入力します。

*注: 名前の長さに関する CC-SG のルールについての詳細は、「*命名 規則 『435*p. 』」を参照してください。*

強力なパスワードを有効にする場合は、入力するパスワードが、確 立されたルールに適合している必要があります。画面上部の情報バ ーには、パスワードの条件を示すメッセージが表示されます。強力 なパスワードの詳細は、「高度な管理 『265p. 』」を参照してくだ さい。

- [次のログインでパスワードの変更を強制] チェックボックスを選択 すると、このユーザは次回のログイン時に、割り当てられたパスワ ードの変更を強制されます。
- ユーザにパスワードを変更することを強制する頻度を指定する場合 は、[パスワードの定期的な変更を強制] チェックボックスを選択し ます。
- 10. 選択した場合は、ユーザが変更を強制されるまで同じパスワードを 使用できる日数を [有効期間 (日)] フィールドに入力します。
- 11. [電子メール アドレス] フィールドに、ユーザの電子メール アドレ スを入力します。このアドレスは、ユーザに通知を送信するのに使 用されます。
- 12. [電話番号] フィールドに、ユーザの電話番号を入力します。
- [ユーザ グループ] ドロップダウン メニューをクリックし、ユーザ が追加されるグループを選択します。



Ch 9: ユーザとユーザ グループ

- 選択するユーザ グループに応じて、[ノードへの接続時にユーザ はアクセス情報を入力する必要があります]チェックボックスを 選択または選択解除します。選択した場合、このユーザは、ノ ードへの接続時に情報を入力する必要があります。「ユーザ グ ループのアクセス監査の設定 『183p. 』」を参照してください
- 14. このユーザを設定したら、[適用] をクリックしてこのユーザを保存 し、さらに新しいユーザを作成します。または、[OK] をクリックし て、ユーザを保存し、ユーザの作成を終了します。作成したユーザ が、[ユーザ] タブに表示されます。ユーザは、属しているユーザ グ ループの下に分類されます。

ユーザの編集

ユーザが属するグループを編集することはできません。「**ユーザのグル** ープへの割り当て 『186p. 』」を参照してください。

▶ ユーザを編集するには、以下の手順に従います。

- [ユーザ] タブで、+ 記号をクリックして編集するユーザが含まれる ユーザ グループを展開し、ユーザを選択します。[ユーザ プロファ イル] 画面が表示されます。
- このユーザが CC-SG にログインできないようするには、[ログイン 有効] チェックボックスを選択解除します。このユーザが CC-SG にログインできるようするには、[ログイン有効] チェックボックス を選択します。
- TACACS+、RADIUS、LDAP、AD などの外部サーバによりユーザ を認証する必要がある場合のみ、[リモート認証] チェックボックス を選択します。リモート認証を使用する場合は、パスワードは不要 なので、[新しいパスワード] と [パスワード再入力] のフィールドは 無効になっています。
- 4. [新しいパスワード] と [パスワード再入力] フィールドに、新しいパ スワードを入力し、このユーザのパスワードを変更します。

注: 強力なパスワードを有効にする場合は、入力するパスワードが 、確立されたルールに適合している必要があります。画面上部の情 報バーには、パスワードの条件を示すメッセージが表示されます。 強力なパスワードの詳細は、「高度な管理 『265p. 』」を参照して ください。

- 5. ユーザが次回のログイン時に、割り当てられたパスワードの変更を 強制されるようにしたい場合、[次のログインでパスワードの変更を 強制] チェック ボックスを選択します。
- [電子メール アドレス] フィールドに、新しい電子メール アドレス を入力し、ユーザの設定済みの電子メール アドレスを追加または変 更します。このアドレスは、ユーザに通知を送信するのに使用され ます。



7. [OK] をクリックして変更を保存します。

ユーザの削除

ユーザを削除すると、CC-SGからユーザが完全に削除されます。これは、必要のないユーザアカウントを削除するのに便利です。

この手順では、ユーザが複数のユーザ グループに存在している場合で も、ユーザの全インスタンスが削除されます。ユーザを CC-SG から削 除せずにグループから削除する場合は、「**ユーザをグループから削除**『 **187**p. 』」を参照してください。

- ▶ ユーザを削除するには、以下の手順に従います。
- [ユーザ] タブで、+ 記号をクリックして削除するユーザが含まれる ユーザ グループを展開し、ユーザを選択します。[ユーザ プロファ イル] 画面が表示されます。
- 2. [ユーザ]>[ユーザ マネージャ]>[ユーザの削除] を選択します。
- 3. [OK] をクリックして、ユーザを CC-SG から完全に削除します。

ユーザのグループへの割り当て

既存のユーザを別のグループに割り当てるには、このコマンドを使用し ます。この方法で割り当てられるユーザは、これまで割り当てられたグ ループに属したまま、新しいグループに追加されます。ユーザを移動す るには、このコマンドとともに、[ユーザをグループから削除]を使用し ます。

- ユーザをグループに割り当てるには、以下の手順に従います。
- 1. [ユーザ] タブで、ユーザが割り当てられるユーザ グループを選択し ます。
- [ユーザ]>[ユーザ グループ マネージャ]>[ユーザをグループに割 り当て]を選択します。
- 3. 選択したユーザ グループが [ユーザ グループ名] フィールドに表示 されます。
- 4. ターゲット グループに属していないユーザが、[グループ外のユー ザ] リストに表示されます。
 - 追加するユーザをこのリストから選択し、[>] をクリックしてそのユーザを [グループ内のユーザ] リストに移動します。
 - [>>] ボタンをクリックすると、グループにないすべてのユーザが が[グループ内のユーザ]リストに移動します。
 - [グループ内のユーザ]リストから削除するユーザを選択し、[<] ボタンをクリックしてそのユーザを削除します。
 - [<<] ボタンをクリックすると、[グループ内のユーザ] リストからすべてのユーザが削除されます。



5. 適切な欄にすべてのユーザが移動されたら、[OK] をクリックします。[グループ内のユーザ] リストのユーザが、選択した [ユーザ グル ープ] に追加されます。

ユーザをグループから削除

ユーザをグループから削除する場合、ユーザは指定されたグループから のみ削除されます。割り当てられた他のすべてのグループには残ります 。グループからユーザを削除しても、ユーザは CC-SG からは削除され ません。

ユーザが 1 つのグループにのみ属している場合、ユーザをグループから削除することはできません。CC-SG からの削除のみ行うことができます。

- ▶ ユーザをグループから削除するには、以下の手順に従います。
- [ユーザ] タブで、+ 記号をクリックし、削除するユーザが含まれる ユーザ グループを展開して、ユーザを選択します。[ユーザ プロフ ァイル] 画面が表示されます。
- 2. [ユーザ]>[ユーザ マネージャ]>[ユーザをグループから削除] を選 択します。[ユーザの削除] 画面 が表示されます。
- 3. [OK] をクリックして、ユーザをグループから削除します。

CSV ファイルのインポートによるユーザの追加

値が含まれている CSV ファイルをインポートすることによって、ユー ザ情報を CC-SG に追加できます。

隣接システムに複数の CC-SG ユニットがある場合は、ある CC-SG か らユーザをエクスポートしてそれらのユーザを別の CC-SG にインポー トすると、簡単にすべてのローカル認証ユーザを両方のメンバとして存 在させることができます。

ユーザ情報をインポートおよびエクスポートするには、ユーザ管理権限 および CC の設定と制御権限が必要です。



ユーザの CSV ファイルの要件

インポートによって、ユーザ グループ、ユーザ、および AD モジュー ルを追加したり、ポリシーと許可をユーザ グループに割り当てたりす ることができます。

- ポリシーが CC-SG ですでに作成されている必要があります。イン ポートでは、ポリシーがユーザ グループに割り当てられます。イン ポートによって新しいポリシーを作成することはできません。
- ユーザ グループ名では大文字と小文字が区別されます。
- ユーザ名では大文字と小文字は区別されません。
- ユーザ グループを作成するには、CSV ファイルで USERGROUP ごとに USERGROUP-PERMISSIONS タグと USERGROUP-POLICY タグを定義する必要があります。
- 有効な CSV ファイルの作成に必要なすべてのタグとパラメータが 含まれているコメントを参照するには、CC-SG からファイルをエ クスポートします。「ユーザのエクスポート 『193p. 』」を参照し てください。
- すべての CSV ファイルの追加要件を満たします。「CSV ファイル の共通要件 『412p. 』」を参照してください。

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	USERGROUP	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ユーザ グループ名	必須フィールド。 ユーザ グループ 名では大文字と小文字が区別されま す。
4	説明	必須フィールド。
5	デバイスあたりの KVM セ ッション数の制限	TRUE または FALSE デフォルトは FALSE です。
6	ユーザごとに許可する最大 KVM セッション数	1~ 8 の範囲内の数字のみを入力し ます。 デフォルトは 2 です。

CSV ファイルにユーザ グループを追加する場合



▶ CSV ファイルでユーザ グループに許可を割り当てる場合

0

ユーザ グループに許可を割り当てるには、値 TRUE を入力します。ユ ーザ グループに許可を割り当てない場合は、値 FALSE を入力します

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	USERGROUP-PERMISSION S	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ユーザ グループ名	必須フィールド。 ユーザ グループ 名では大文字と小文字が区別されま す。
4	CC の設定と制御	TRUE または FALSE
5	デバイス設定のアップグレ ード管理	TRUE または FALSE
6	デバイス ポート ノードの 管理	TRUE または FALSE
7	ユーザ管理	TRUE または FALSE
8	ユーザ セキュリティ管理	TRUE または FALSE
9	ノード IBA	TRUE または FALSE デフォルトは TRUE です。
10	ノード OOB	TRUE または FALSE デフォルトは TRUE です。
11	ノード パワー	TRUE または FALSE

CSV ファイルでユーザ グループにポリシーを割り当てる場合

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	USERGROUP-POLICY	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ユーザ グループ名	必須フィールド。



Ch 9: ユーザとユーザ グループ

列番号	タグまたは値	詳細
		ユーザ グループ名では大文字と小文 字が区別されます。
4	ポリシー名	必須フィールド。

CSV ファイルでユーザ グループに AD モジュールを関連付ける場合

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	USERGROUP-ADMODULE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ユーザ グループ名	必須フィールド。 ユーザ グループ 名では大文字と小文字が区別されま す。
4	AD モジュール名	必須フィールド。

▶ CC-SG にユーザを追加する場合

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	USER	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ユーザ グループ名	必須フィールド。 ユーザ グループ 名では大文字と小文字が区別されま す。 ユーザを 1 つのユーザ グループに 追加する必要があります。 USERGROUP-MEMBER タグを使 用すると、ユーザを複数のユーザ グ ループに追加できます。
4	ユーザ名	必須フィールド。
5	パスワード	必須フィールド。



Ch 9: ユーザとユーザ グループ

列番号	タグまたは値	詳細
6	ユーザの氏名	オプション。
7	電子メール アドレス	オプション。 電子メール アドレスは、システム通 知で使用されます。
8	電話番号	オプション。
9	ログイン有効	TRUE または FALSE デフォルトは TRUE です。 ユーザが CC-SG にログインできる ようするには、ログインを有効にし ます。
10	リモート認証	TRUE または FALSE
11	パスワードの定期的な変更 を強制	TRUE または FALSE
12	有効期間	パスワードの定期的な変更を強制を TRUE に設定する場合は、パスワー ドの変更が必要になるまでの日数を 指定します。1 ~ 365 の範囲内の 数字のみを入力します。

ユーザをユーザ グループに追加する場合

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	USERGROUP-MEMBER	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	ユーザ グループ名	必須フィールド。 ユーザ グループ名では大文字と小文 字が区別されます。
4	ユーザ名	必須フィールド。



ユーザの CSV ファイルの例

ADD, USERGROUP, Windows Administrators, MS IT Team

ADD, USERGROUP-PERMISSIONS, Windows Administrators, FALSE, TRUE, TRUE, TRUE, TRUE, TRUE, TRUE, TRUE, TRUE

ADD, USERGROUP-POLICY, Windows Administrators, Full Access Policy

ADD, USERGROUP-ADMODULE, Windows Administrators, AD-USA-57-120

ADD, USERGROUP-MEMBER, Windows Administrators, user1

ADD, USERGROUP-MEMBER, Windows Administrators, user2

ADD, USER, Windows Administrators, user1, password, userfirstname userlastname, user1@company.com, 800-555-1212, TRUE,,,

ADD, USER, Windows Administrators, user2, password, userfirstname userlastname, user2@raritan.com, 800-555-1212, TRUE,,,

ADD, USERGROUP-MEMBER, System Administrators, user1

ADD, USERGROUP-MEMBER, CC Users, user2

ユーザのインポート

CSV ファイルを作成したら、エラーがないかどうかを確認してからイ ンポートします。

重複するレコードはスキップされ、追加されません。

- 1. [管理]>[インポート]>[ユーザーのインポート]を選択します。
- [参照] をクリックし、インポートする CSV ファイルを選択します。
 [開く] をクリックします。
- 3. [確認] をクリックします。[分析レポート] 領域にファイルの内容が 表示されます。
 - ファイルが有効でない場合は、エラー メッセージが表示されます。[OK] をクリックし、ページの [問題] 領域でファイルに関する問題の説明を参照します。[ファイルに保存] をクリックして問題リストを保存します。CSV ファイルを修正し、再度検証します。「CSV ファイルの問題のトラブルシューティング 『414p.』」を参照してください。
- 4. [インポート] をクリックします。
- 5. [アクション] 領域でインポート結果を確認します。正常にインポートされたアイテムは、緑色のテキストで表示されます。インポートに失敗したアイテムは、赤いテキストで表示されます。重複するアイテムがすでに存在するか、またはすでにインポートされているためにインポートに失敗したアイテムも赤いテキストで表示されます



インポート結果の詳細を参照するには、監査証跡レポートを確認します。「インポートに関する監査証跡エントリ 『413p. 』」を参照してください。

ユーザのエクスポート

エクスポート ファイルには、CC-SG でユーザ アカウントが作成され ているすべてのユーザが含まれます。これには AD で認証されたユーザ は含まれませんが、CC-SG でもユーザ アカウントが作成されている場 合を除きます。

エクスポート ファイルには、ユーザ、ユーザ プロファイルからの詳細 、ユーザ グループ、ユーザ グループの許可とポリシー、関連付けられ ている AD モジュールが含まれます。

パスワードは、空白フィールドとしてエクスポートされます。

▶ ユーザをエクスポートするには、以下の手順に従います。

- 1. [管理]>[エクスポート]>[ユーザーのエクスポート]を選択します。
- 2. [ファイルにエクスポート] をクリックします。
- 3. ファイルの名前を入力し、保存する場所を選択します。
- 4. [保存] をクリックします。

ユーザ プロファイル

[プロファイル] を使用すると、自分のアカウントに関する詳細の表示、 一部詳細の変更、可用性の設定のカスタマイズが全ユーザに可能になり ます。これは、CC スーパー ユーザ アカウントがアカウント名を変更 できる唯一の方法です。

プロファイルを参照するには、以下の手順に従います。

[Secure Gateway] > [プロファイル] を選択します。アカウントの詳細を 示す [Change My Profile] (プロファイルの変更) 画面が表示されます。

パスワードの変更

- 1. [Secure Gateway] > [プロファイル] を選択します。
- [Change Password (For Local Authentication Only)] (パスワードの変 更 (ローカル認証の場合のみ)) チェックボックスをオンにします。
- 3. [旧パスワード] フィールドに現在のパスワードを入力します。
- 4. [新しいパスワード] フィールドに新しいパスワードを入力します。 強力なパスワードが必要な場合は、メッセージが表示されます。
- 5. [パスワード再入力] フィールドに新しいパスワードをもう一度入力 します。
- 6. [OK] をクリックして変更を保存します。



名前の変更

ユーザ名を変更することはできません。ユーザ名に関連付けられた氏名 は変更できます。

- ▶ 名前を変更するには、以下手の手順に従います。
- 1. [Secure Gateway] > [プロファイル] を選択します。
- [フルネーム] フィールドに氏名を入力します。 名前の長さに関する CC-SG のルールについての詳細は、「命名規則 『435p. 』」を参 照してください。

デフォルトの検索設定の変更

- 1. [Secure Gateway] > [プロファイル] を選択します。
- [検索設定] エリアで、ノード、ユーザ、デバイスを検索するための 優先方法を選択します。
 - 検索結果でフィルタ・ワイルドカードの使用を許可し、検索条件を含む名前を持つノード、ユーザ、デバイスのみを表示します。
 - 一致する文字列の検索 ワイルドカードの使用は許可されません。入力した名前に最も近いノード、ユーザ、デバイスがハイライトされます。[検索]をクリックすると、検索条件を含むアイテムのみが表示されます。
- 3. [OK] をクリックして変更を保存します。

CC-SG デフォルト フォント サイズの変更

- 1. [Secure Gateway] > [プロファイル] を選択します。
- [フォント サイズ] ドロップダウン メニューをクリックして、標準の CC-SG クライアントで使用するフォントのサイズを調整します。
- 3. [OK] をクリックして変更を保存します。

電子メール アドレスの変更

- 1. [Secure Gateway] > [プロファイル] を選択します。
- 2. [電子メール アドレス] フィールドに新しいアドレスを入力し、 CC-SG が通知の送信に使用するアドレスを追加または変更します。
- 3. [OK] をクリックして変更を保存します。



CC-SG スーパー ユーザのユーザ名の変更

CC スーパー ユーザのユーザ名を変更するには、CC スーパー ユーザ アカウントを使用して CC-SG にログインしている必要があります。デ フォルト CC スーパー ユーザのユーザ名は admin です。

- 1. [Secure Gateway] > [プロファイル] を選択します。
- 2. 新しい名前を [ユーザ名] フィールドに入力します。
- 3. [OK] をクリックして変更を保存します。

ユーザのログアウト

アクティブ ユーザを、個別またはユーザ グループごとに CC-SG から ログアウトさせることができます。

▶ ユーザをログアウトさせるには、以下の手順に従います。

- 1. [ユーザ] タブで、+ 記号をクリックしてログアウトさせるユーザが 含まれるユーザ グループを展開し、そのユーザを選択します。
 - 複数のユーザを選択するには、Shift キーを押しながら、他のユ ーザをクリックします。
- 2. [ユーザ]>[ユーザ マネージャ]>[ユーザのログアウト] を選択しま す。選択したユーザのリストを含む [ユーザのログアウト] 画面が表 示されます。
- 3. ユーザを CC-SG からログアウトさせるには [OK] をクリックしま す。
- ユーザ グループの全ユーザをログアウトさせるには、以下の手順に 従います。
- [ユーザ] タブで、CC-SG からログアウトさせるユーザ グループを 選択します。
 - 複数のユーザ グループをログアウトさせるには、Shift キーを押 しながら、他のユーザ グループをクリックします。
- 2. [ユーザ]>[ユーザ マネージャ]>[ユーザのログアウト] を選択しま す。選択したグループに属するアクティブなユーザのリストを含む [ユーザのログアウト] 画面が表示されます。
- 3. ユーザを CC-SG からログアウトさせるには [OK] をクリックしま す。



ユーザの一括コピー

ユーザを一括コピーすると、ユーザのユーザ グループ所属を別のユー ザやユーザのリストにコピーできます。加入するユーザに既存のグルー プ所属がある場合、既存の所属は削除されます。

- ▶ ユーザの一括コピーを実行するには、以下の手順に従います。
- [ユーザ] タブで、+ 記号をクリックしてコピーされるポリシーと権 限を持つユーザが含まれるユーザ グループを展開し、そのユーザを 選択します。
- 2. [ユーザ]>[ユーザ マネージャ]>[一括コピー] を選択します。[ユー ザ名] フィールドに、コピーされるポリシーと権限を持つユーザが 表示されます。
- 3. [すべてのユーザ] リストで、[ユーザ名] フィールドのユーザの権限 とポリシーを適用するユーザを選択します。
 - [>] をクリックすると、ユーザ名が [選択されたユーザ] リスト に移動します。
 - [>>] ボタンをクリックすると、すべてのユーザが [選択されたユ ーザ] リストに移動します。
 - [選択されたユーザ] リストのユーザを選択し、< をクリックしてそのユーザを削除します。
 - [<<] をクリックすると、[グループ内のユーザ] リストからすべてのユーザが削除されます。
- 4. [OK] をクリックしてコピーします。



アクセス制御のポリシー

ポリシーは、ユーザがどのノードとデバイスにアクセスできるか、それ らにいつアクセスできるか、および仮想メディア許可が有効かどうか(該当する場合)を定義するルールです。ポリシーを作成する最も簡単な 方法は、ノードとデバイスをノード グループとデバイス グループに分 類し、各グループ内のノードとデバイスへのアクセスを許可および拒否 するポリシーを作成することです。ポリシーを作成したら、ユーザ グ ループに割り当てます。「ユーザ グループへのポリシーの割り当て『 201p.』」を参照してください。

CC-SG には、フル アクセス ポリシーも用意されています。すべての ユーザに常にすべてのノードとデバイスへのアクセスを許可する場合は 、すべてのユーザ グループにフル アクセス ポリシーを割り当てます

ガイド付き設定を実行した場合、多数の基本的なポリシーがすでに作成 されています。「*ガイド付き設定を使用した CC-SG の設定* **『38**p. **』** 」を参照してください。

- ポリシーを使用してアクセスを制御するには、次の手順に従います。
- アクセス ルールを作成するノードを整理するために、ノード グル ープを作成する。「ノード グループの追加 『171p. 』」を参照して ください。
- アクセス ルールを作成するデバイスを整理するために、デバイス グループを作成する。「デバイス グループの追加 『82p. 』」を参 照してください。
- そのノードまたはデバイスへのアクセスが発生する場合を示すノードまたはデバイス グループのポリシーを作成する。「ポリシーの追加『198p.』」を参照してください。
- ポリシーをユーザ グループに適用する。「ユーザ グループへのポリ シーの割り当て『201p.』」を参照してください。

この章の内容

ポリシーの追加	
ポリシーの編集	
ポリシーの削除	
仮想メディアのサポート	
ユーザ グループへのポリシーの割り当て	201



Ch 10

ポリシーの追加

ノード グループまたはデバイス グループのアクセスを拒否するポリシ ー (拒否)を作成する場合は、選択したノード グループまたはデバイス グループのアクセスを許可するポリシー (制御)も作成する必要があり ます。ユーザは、[拒否] ポリシーが有効でない場合に、[制御] 権限を自 動的に取得することはありません。

- ポリシーを追加するには、以下の手順に従います。
- [関連]>[ポリシー]を選択します。[ポリシー マネージャ] 画面が開きます。
- 2. [追加] をクリックします。ポリシーの名前を要求するダイアログ ウ ィンドウが表示されます。
- 3. [ポリシー名の入力] フィールドに新しいポリシーの名前を入力しま す。名前の長さに関する CC-SG のルールについての詳細は、「 *命 名規則* 『435p. 』」を参照してください。
- [OK] をクリックします。新しいポリシーが、[ポリシー マネージャ] 画面の [ポリシー名] リストに追加されます。
- 5. [デバイス グループ] ドロップダウン矢印をクリックし、このポリシ ーでアクセスを制御するデバイス グループを選択します。
- 6. [ノード グループ] ドロップダウン矢印をクリックし、このポリシー でアクセスを制御するノード グループを選択します。
- 7. ポリシーが 1 種類のグループのみに適用される場合は、その種類の 値を選択するだけです。
- [曜日] ドロップダウン矢印をクリックして、このポリシーを適用する曜日を選択します。オプションは、[毎日]、[平日](月曜日から金曜日のみ)、[土日](土曜日と日曜日のみ)、[カスタム](特定の曜日を選択)です。
- 9. 独自の曜日セットを選択するには、[カスタム] を選択します。個々 の曜日のチェックボックスが有効になります。
- **10.** ポリシーを適用する曜日の該当するチェックボックスを選択します。
- 11. [開始時刻] フィールドに、このポリシーが有効となる時刻を入力し ます。時刻は、24 時間制で入力してください。
- 12. [終了時刻] フィールドに、このポリシーが終了される時刻を入力し ます。時刻は、24 時間制で入力してください。
- 13. [デバイス/ノード アクセス許可] フィールドで、[制御] を選択し、 指定した時刻と曜日で選択したノードまたはデバイスにアクセスを 許可するポリシーを定義します。[拒否] を選択し、指定した時刻と 曜日で選択したノードまたはデバイスにアクセスを拒否するポリシ ーを定義します。


- 14. [デバイス/ノード アクセス許可] フィールドで [制御] を選択すると、[仮想メディア許可] が有効になります。[仮想メディア許可] フィールドで、指定した時刻と曜日に、選択したノード グループまたはデバイス グループで使用可能な仮想メディアへのアクセスを許可または拒否するオプションを選択します。
 - [読み書き]を選択すると、仮想メディアの読み取りと書き込みの両方が許可されます。
 - [読み取り専用]を選択すると、仮想メディアの読み取りのみが 許可されます。
 - [拒否]を選択すると、仮想メディアへのすべてのアクセスが拒 否されます。
- 15. [更新] をクリックして、新しいポリシーを CC-SG に追加し、確認 のメッセージが表示されたら [はい] をクリックします。

ポリシーの編集

ポリシーを編集しても、現在 CC-SG にログインしているユーザには適 用されません。変更は、次のログインから有効になります。 変更が有効になることを次のログインより前に確認する必要がある場合 は、まずメンテナンス モードを起動して、ポリシーを編集します。メ ンテナンス モードを起動すると、メンテナンス モードを終了するまで 、すべてのユーザが CC-SG からログアウトされます。メンテナンス モードを終了すると、ユーザが再びログインできるようになります。「 メンテナンス モード 『2460.』」を参照してください。

- ▶ ポリシーを編集するには、以下の手順に従います。
- [関連] メニューの [ポリシー] をクリックします。[ポリシー マネージャ] 画面が開きます。
- 2. [ポリシー名] ドロップダウン矢印をクリックし、リストから編集す るポリシーを選択します。
- 3. ポリシーの名前を編集するには、[編集] をクリックします。[ポリシ ーの編集] ウィンドウが開きます。フィールドに、ポリシーの新し い名前を入力し、[OK] をクリックしてポリシーの名前を変更します 。オプション。
- 4. [デバイス グループ] ドロップダウン矢印をクリックし、このポリシ ーでアクセスを制御するデバイス グループを選択します。
- 5. [ノード グループ] ドロップダウン矢印をクリックし、このポリシー でアクセスを制御するノード グループを選択します。
- 6. ポリシーが 1 種類のグループのみに適用される場合は、その種類の 値を選択するだけです。



- [曜日] ドロップダウン矢印をクリックして、このポリシーを適用する曜日を選択します。オプションは、[毎日]、[平日](月曜日から金曜日のみ)、[土日](土曜日と日曜日のみ)、[カスタム](特定の曜日を選択)です。
- 8. 独自の曜日セットを選択するには、[カスタム] を選択します。個々の曜日のチェックボックスが有効になります。
- 9. ポリシーを適用する曜日の該当するチェックボックスを選択します。
- 10. [開始時刻] フィールドに、このポリシーが有効となる時刻を入力し ます。時刻は、24 時間制で入力してください。
- 11. [終了時刻] フィールドに、このポリシーが終了される時刻を入力し ます。時刻は、24 時間制で入力してください。
 - [デバイス/ノード アクセス許可] フィールドで、次の手順に従い ます。
 - [制御]を選択し、指定した時刻と曜日に選択したノードまたは デバイスへのアクセスを許可するポリシーを定義します。
 - [拒否]を選択し、指定した時刻と曜日で選択したノードまたは デバイスにアクセスを拒否するポリシーを定義します。
- [デバイス/ノード アクセス許可] フィールドで [制御] を選択すると、[仮想メディア許可] が有効になります。[仮想メディア許可] フィールドで、指定した時刻と曜日に、選択したノード グループまたはデバイス グループで使用可能な仮想メディアへのアクセスを許可または拒否するオプションを選択します。
 - [読み書き]を選択すると、仮想メディアの読み取りと書き込みの両方が許可されます。
 - [読み取り専用]を選択すると、仮想メディアの読み取りのみが 許可されます。
 - [拒否] を選択すると、仮想メディアへのすべてのアクセスが拒 否されます。

13. [更新] をクリックして変更を保存します。

14. 表示される確認メッセージで [はい] をクリックします。

ポリシーの削除

不要になったポリシーは、削除できます。

- ポリシーを削除するには、以下の手順に従います。
- 1. [関連] > [ポリシー] を選択します。[ポリシー マネージャ] 画面が開 きます。
- 2. [ポリシー名] ドロップダウン矢印をクリックし、削除するポリシー を選択します。



- 3. [削除] をクリックします。
- 4. 表示される確認メッセージで [はい] をクリックします。

仮想メディアのサポート

CC-SG は、仮想メディア対応 **KX2、KSX2、KX2-101** デバイスに接続 されたノードにリモート仮想メディア サポートを提供します。デバイ スによる仮想メディアの詳しいアクセス手順については、次のマニュア ルを参照してください。

- Dominion KX II User Guide
- Dominion KSX II User Guide
- Dominion KXII-101 User Guide

ポリシーを作成して CC-SG でユーザ グループに仮想メディア許可を 割り当てる方法についての詳細は、「ポリシーの追加 『198p. 』」を参 照してください。

ユーザ グループへのポリシーの割り当て

ポリシーを有効にするには、ユーザ グループに割り当てる必要があり ます。ポリシーをユーザ グループに割り当てると、グループのメンバ が、そのポリシーによって制御されているアクセス権を持つようになり ます。ポリシーをユーザ グループに割り当てる方法についての詳細は 、「ユーザとユーザ グループ 『176p. 』」を参照してください。 ユーザが複数のグループに属している場合は、ユーザには、それらのグ ループのうちでより制限の少ないポリシーが適用されます。

🕨 たとえば、

ポリシー 123: サーバ 123 にアクセスできます。

- ポリシー 456: サーバ 456 にアクセスできます。
- グループ A: グループはポリシー 123 に割り当てられています。
- グループ B: グループ B はポリシー 456 に割り当てられています。

ユーザはグループ A と B の両方に属しています。したがって、ユーザ はサーバ 123456 にアクセスできます。

次に、「ポリシー拒否 1: サーバ 1 へのアクセスを拒否します」を作成 します。

ポリシー拒否 1 をグループ A に割り当てます。ユーザがアクセスでき るのは 23456 だけになります。

ポリシー拒否 1 がグループ A からグループ B に切り替えられた場合、ユーザは 123456 にアクセスできます。



Ch 11 デバイスおよびノードのカスタム表示

カスタム表示では、カテゴリ、ノード グループ、デバイス グループを 使用して、左パネルのノードおよびデバイスの表示方法を指定できます。

この章の内容

カスタム表示	の種類	
Admin Client	でのカスタム表示の使用	

カスタム表示の種類

カスタム表示には、カテゴリ別の表示、ノード グループ別のフィルタ 、デバイス グループ別のフィルタという **3** 種類があります。

カテゴリ別の表示

[カテゴリ別の表示] カスタム表示を適用した時点で、指定したカテゴリ で説明されるすべてのノードおよびデバイスがノード リストまたはデ バイス リストに表示されます。割り当てられているカテゴリがないノ ードまたはデバイスは、「関連なし」として表示されます。

ノード グループでフィルタ

[ノード グループでフィルタ] カスタム表示を適用した時点で、指定し たノード グループのみがノード リストに表示されます。組織の最初の レベルは、ノード グループ名です。カスタム表示で定義されている複 数のノード グループにノードが属している場合は、ノードがリストに 複数回表示されることがあります。カスタム表示で指定されたノード グループに属していないノードは、リストに表示されません。

デバイス グループでフィルタ

[デバイス グループでフィルタ] カスタム表示を適用した時点で、指定 したデバイス グループのみがデバイス リストに表示されます。組織の 最初のレベルは、デバイス グループ名です。カスタム表示で定義され ている複数のデバイス グループにデバイスが属している場合は、デバ イスがリストに複数回表示されることがあります。カスタム表示で指定 されたデバイス グループに属していないデバイスは、リストに表示さ れません。



Admin Client でのカスタム表示の使用

ノードのカスタム表示

ノードのカスタム表示の追加

- ノードのカスタム表示を追加するには、以下の手順に従います。
- 1. [ノード] タブをクリックします。
- 2. [ノード] メニューの [表示の変更] を選択し、さらに [カスタム表示 の作成] を選択します。[カスタム表示] 画面が表示されます。
- 3. [カスタム表示] パネルで、[追加] をクリックします。[カスタム表示 の追加] ウィンドウが開きます。
- 4. 新しいカスタム表示の名前を [カスタム表示名] フィールドに入力し ます。
- 5. [カスタム表示タイプ] セクションで、次の操作を行います。
 - 指定したノード グループのみを表示するカスタム表示を作成するには、[ノード グループでフィルタ]を選択します。
 - 指定したカテゴリに基づいてノードを表示するカスタム表示を 作成するには、[カテゴリ別の表示]を選択します。
- 6. [OK] をクリックします。
- 7. [カスタム表示の詳細] セクションで、次の操作を行います。
 - a. [利用可能] リストでカスタム表示に組み込む項目を選択し、[追加] をクリックして、その項目をリストに追加します。この手順を繰り返し、必要な数だけ項目を追加します。
 - b. [選択中] リストの項目は、[ノード] タブに表示する各グループ の順序にします。項目を選択し、その項目が目的の順序になる ように、上下の矢印ボタンをクリックして項目を移動します。
 - c. リストから項目を削除する場合は、項目を選択して [削除] をク リックします。
- 8. [保存] をクリックします。メッセージが表示され、カスタム表示が 追加されたことを確認します。
- 新しいカスタム表示を適用するには、[Set Current] (現在の表示に設定) をクリックします。

ノードのカスタム表示の適用

- カスタム表示をノードリストに適用するには、以下の手順に従います。
- [ノード]>[表示の変更]>[カスタム表示] を選択します。[カスタム 表示] 画面が表示されます。



- 2. [名前] ドロップダウン矢印をクリックし、リストから [カスタム表示] を選択します。
- 3. [表示を適用] をクリックします。

または

[ノード] メニューの [表示の変更] を選択します。定義済みのすべてのカスタム表示がポップアップ メニューにオプションとして表示されます。適用するカスタム表示を選択します。

ノードのカスタム表示の変更

- 1. [ノード] タブをクリックします。
- 2. [ノード] メニューの [表示の変更] を選択し、さらに [カスタム表示 の作成] を選択します。[カスタム表示] 画面が表示されます。
- [名前] ドロップダウン矢印をクリックし、リストから [カスタム表示] を選択します。[カスタム表示の詳細] パネルに、含まれる項目の詳細とその順番が表示されます。

▶ カスタム表示名を変更するには

- 1. [カスタム表示] パネルで [編集] をクリックします。[カスタム表示 の編集] ウィンドウが開きます。
- カスタム表示の新しい名前を [カスタム表示の新しい名前を入力] フィールドに入力し、[OK] をクリックします。[カスタム表示] 画面の [名前] フィールドに新しい表示名が表示されます。

カスタム表示の内容を変更するには

- 1. [カスタム表示の詳細] セクションで、次の操作を行います。
 - a. [利用可能] リストでカスタム表示に組み込む項目を選択し、[追加] をクリックして、その項目をリストに追加します。この手順を繰り返し、必要な数だけ項目を追加します。
 - b. [選択中] リストの項目は、[ノード] タブに表示する各グループ の順序にします。項目を選択し、その項目が目的の順序になる ように、上下の矢印ボタンをクリックして項目を移動します。
 - c. リストから項目を削除する場合は、項目を選択して [削除] をク リックします。
- 2. [保存] をクリックします。メッセージが表示され、カスタム表示が 追加されたことを確認します。
- 新しいカスタム表示を適用するには、[Set Current] (現在の表示に設定) をクリックします。



ノードのカスタム表示の削除

- ノードのカスタム表示を削除するには、以下の手順に従います。
- 1. [ノード] タブをクリックします。
- 2. [ノード] メニューの [表示の変更] を選択し、さらに [カスタム表示 の作成] を選択します。[カスタム表示] 画面が表示されます。
- 3. [名前] ドロップダウン矢印をクリックし、リストから [カスタム表示] を選択します。[カスタム表示の詳細] パネルに、含まれる項目の詳細とその順番が表示されます。
- 4. [カスタム表示] パネルで [削除] をクリックします。[カスタム表示 の削除] の確認メッセージが表示されます。
- 5. [はい] をクリックします。

ノードのデフォルトのカスタム表示の指定

- ノードのデフォルトのカスタム表示を割り当てるには、以下の手順 に従います。
- 1. [ノード] タブをクリックします。
- 2. [ノード] メニューの [表示の変更] を選択し、さらに [カスタム表示 の作成] を選択します。[カスタム表示] 画面が表示されます。
- 3. [名前] ドロップダウン矢印をクリックし、リストから [カスタム表示] を選択します。
- [カスタム表示] パネルで [デフォルトに設定] をクリックします。次 回ログインするときに、選択したカスタム表示がデフォルトで使用 されます。

ノードのデフォルトのカスタム表示をすべてのユーザに指定

CC の設定と制御の権限がある場合は、デフォルトのカスタム表示をすべてのユーザに指定できます。

- ノードのデフォルトのカスタム表示をすべてのユーザに割り当てる には、以下の手順に従います。
- 1. [ノード] タブをクリックします。
- 2. [ノード] メニューの [表示の変更] を選択し、さらに [カスタム表示 の作成] を選択します。
- 3. [表示の名前] ドロップダウン矢印をクリックして、システム全体の デフォルト表示として割り当てるカスタム表示を選択します。
- 4. [システムの表示] チェックボックスを選択して、[保存] をクリック します。



CC-SG にログインするすべてのユーザに、選択したカスタム表示に従ってノードがソートされた [ノード] タブが表示されます。ユーザはカスタム表示を変更できます。

デバイスのカスタム表示

デバイスのカスタム表示の追加

- ▶ デバイスのカスタム表示を追加するには、以下の手順に従います。
- 1. [デバイス] タブをクリックします。
- 2. [デバイス] メニューの [表示の変更] を選択し、さらに [カスタム表示の作成] を選択します。[カスタム表示] 画面が表示されます。
- 3. [カスタム表示] パネルで、[追加] をクリックします。[カスタム表示 の追加] ウィンドウが表示されます。
- 4. 新しいカスタム表示の名前を [カスタム表示名] フィールドに入力します。
- 5. [カスタム表示タイプ] セクションで、次の操作を行います。
 - 指定したデバイス グループのみを表示するカスタム表示を作成 するには、[デバイス グループでフィルタ]を選択します。
 - 指定したカテゴリに基づいてデバイスを表示するカスタム表示 を作成するには、[カテゴリ別の表示]を選択します。
- 6. [OK] をクリックします。
- 7. [カスタム表示の詳細] セクションで、次の操作を行います。
 - a. [利用可能] リストでカスタム表示に組み込む項目を選択し、[追加] をクリックして、その項目をリストに追加します。この手順を繰り返し、必要な数だけ項目を追加します。
 - b. [選択中] リストの項目は、[ノード] タブに表示する各グループ の順序にします。項目を選択し、その項目が目的の順序になる ように、上下の矢印ボタンをクリックして項目を移動します。
 - c. リストから項目を削除する場合は、項目を選択して [削除] をク リックします。
- 8. [保存] をクリックします。メッセージが表示され、カスタム表示が 追加されたことを確認します。
- 新しいカスタム表示を適用するには、[Set Current] (現在の表示に設定) をクリックします。



デバイスのカスタム表示の適用

- カスタム表示をデバイス リストに適用するには、以下の手順に従います。
- 1. [デバイス]>[表示の変更]>[カスタム表示] を選択します。[カスタ ム表示] 画面が表示されます。
- 2. [名前] ドロップダウン矢印をクリックし、リストから [カスタム表示] を選択します。
- 3. [Set Current] (現在の表示に設定) をクリックしてカスタム表示を適 用します。

または

[デバイス] メニューの [表示の変更] を選択します。定義済みのすべて のカスタム表示がポップアップ メニューにオプションとして表示され ます。適用するカスタム表示を選択します。

デバイスのカスタム表示の変更

- 1. [デバイス] タブをクリックします。
- 2. [デバイス] メニューの [表示の変更] を選択し、さらに [カスタム表 示の作成] を選択します。[カスタム表示] 画面が表示されます。
- 3. [名前] ドロップダウン矢印をクリックし、リストから [カスタム表示] を選択します。[カスタム表示の詳細] パネルに、指定された項目の詳細とその順番が表示されます。

▶ カスタム表示名を変更するには

- 1. [カスタム表示] パネルで [編集] をクリックします。[カスタム表示 の編集] ウィンドウが開きます。
- カスタム表示の新しい名前を [カスタム表示の新しい名前を入力] フィールドに入力し、[OK] をクリックします。[カスタム表示] 画面の [名前] フィールドに新しい表示名が表示されます。

カスタム表示の内容を変更するには

- 1. [カスタム表示の詳細] セクションで、次の操作を行います。
 - a. [利用可能] リストでカスタム表示に組み込む項目を選択し、[追加] をクリックして、その項目をリストに追加します。この手順を繰り返し、必要な数だけ項目を追加します。
 - b. [選択中] リストの項目は、[ノード] タブに表示する各グループ の順序にします。項目を選択し、その項目が目的の順序になる ように、上下の矢印ボタンをクリックして項目を移動します。
 - c. リストから項目を削除する場合は、項目を選択して [削除] をク リックします。



- 2. [保存] をクリックします。メッセージが表示され、カスタム表示が 追加されたことを確認します。
- 新しいカスタム表示を適用するには、[Set Current] (現在の表示に設定) をクリックします。

デバイスのカスタム表示の削除

- ▶ デバイスのカスタム表示を削除するには、以下の手順に従います。
- 1. [デバイス] タブをクリックします。
- 2. [デバイス] メニューの [表示の変更] を選択し、さらに [カスタム表示の作成] を選択します。[カスタム表示] 画面が表示されます。
- [名前] ドロップダウン矢印をクリックし、リストから [カスタム表示] を選択します。[カスタム表示の詳細] パネルに、含まれる項目の詳細とその順番が表示されます。
- 4. [カスタム表示] パネルで [削除] をクリックします。[カスタム表示 の削除] の確認メッセージが表示されます。
- 5. [はい] をクリックします。

デバイスのデフォルトのカスタム表示の指定

- デバイスのデフォルトのカスタム表示を割り当てるには、以下の手順に従います。
- 1. [デバイス] タブをクリックします。
- 2. [デバイス] メニューの [表示の変更] を選択し、さらに [カスタム表示の作成] を選択します。[カスタム表示] 画面が表示されます。
- 3. [名前] ドロップダウン矢印をクリックし、リストから [カスタム表示] を選択します。
- [カスタム表示] パネルで [デフォルトに設定] をクリックします。次 回ログインするときに、選択したカスタム表示がデフォルトで使用 されます。

デバイスのデフォルトのカスタム表示をすべてのユーザに指定

デバイス、ポート、およびノードの管理権限がある場合は、デフォルト のカスタム表示をすべてのユーザに割り当てることができます。

- デバイスのデフォルトのカスタム表示をすべてのユーザに割り当てるには、以下の手順に従います。
- 1. [デバイス] タブをクリックします。
- 2. [デバイス] メニューの [表示の変更] を選択し、さらに [カスタム表示の作成] を選択します。



- 3. [表示の名前] ドロップダウン矢印をクリックして、システム全体の デフォルト表示として割り当てるカスタム表示を選択します。
- 4. [システム全体] チェックボックスを選択して、[保存] をクリックします。

CC-SG にログインするすべてのユーザに、選択したカスタム表示に従ってソートされた [デバイス] タブが表示されます。ユーザはカスタム表示を変更できます。



Ch 12 リモート認証

この章の内容

認証と承認 (AA) の概要	210
LDAP と AD の識別名	211
認証および承認のモジュール指定	212
外部 AA サーバの順序の確立	213
AD および CC-SG の概要	213
CC-SG への AD モジュールの追加	213
AD モジュールの編集	218
AD ユーザ グループのインポート	219
AD と CC-SG の同期	221
AD グループの名前の変更および移動	225
LDAP と CC-SG について	225
CC-SG への LDAP (Netscape) モジュールの追加	225
TACACS+ と CC-SG について	229
TACACS+ モジュールの追加	229
RADIUS と CC-SG について	230
RADIUS モジュールの追加	230

認証と承認 (AA) の概要

CC-SG のユーザは、ローカルで **CC-SG** への認証と承認を行うか、またはサポートされる次のディレクトリ サーバを使ってリモート認証することができます。

- Microsoft Active Directory (AD)
- Netscape ライトウェイト ディレクトリ アクセス プロトコル (LDAP)
- TACACS+
- RADIUS

任意の数のリモート サーバを外部認証に使用できます。たとえば、3 台の AD サーバ、2 台の iPlanet (LDAP) サーバ、3 台の RADIUS サ ーバといったシステム構成を使用できます。

ユーザのリモート承認には、AD サーバのみを使用できます。

LDAP 実装で LDAP v3 が使用されます。



認証の流れ

リモート認証が有効になっているとき、認証と承認は次の手順に従いま す。

- 1. ユーザが適切なユーザ名とパスワードで CC-SG にログインします。
- 2. CC-SG が外部サーバに接続してユーザ名とパスワードを送信しま す。
- ユーザ名とパスワードは、承認または拒否されて送り返されます。
 認証が拒否されると、ログインに失敗します。
- 認証に成功すると、承認が実行されます。CC-SG は、入力された ユーザ名が CC-SG で作成されたグループまたは AD からインポー トされたグループに一致するかどうかを確認し、割り当てられたポ リシーに従って権限を付与します。

リモート認証が無効になっている場合、認証と承認の両方が CC-SG においてローカルで実行されます。

ユーザ アカウント

リモート認証を行うには、認証サーバにユーザ アカウントを追加する 必要があります。認証と承認の両方に AD を使用する場合以外は、すべ てのリモート認証について、該当するユーザを CC-SG 上に作成してお く必要があります。ユーザのユーザ名には認証サーバと CC-SG で同じ 名前を使用する必要がありますが、パスワードは異なっていてもかまい ません。ローカルの CC-SG パスワードはリモート認証が無効になって いる場合にのみ使用されます。リモートで認証するユーザを追加する方 法についての詳細は、「ユーザとユーザ グループ 『176p.』」を参照 してください。

注: リモート認証を使用する場合、ユーザは管理者に連絡してリモート サーバ上の自身のパスワードの変更を依頼する必要があります。リモー ト認証を使用するユーザのパスワードを CC-SG で変更することはでき ません。

LDAP と AD の識別名

LDAP または AD サーバでリモート認証されるユーザを設定するには、DN (Distinguished Name: 識別名) 形式でユーザ名を入力して検索する必要があります。完全な識別名形式については、RFC2253 (http://www.rfc-editor.org/rfc/rfc2253.txt) を参照してください。

CC-SG を設定するには、識別名の入力方法とその名前の各コンポーネントがリストされる順序を理解しておく必要があります。



AD の識別名の指定

AD の識別名は、次の構造に従って指定します。common name と organization unit の両方を指定する必要はありません。

common name (cn), organizational unit (ou), domain component (dc)

LDAP の識別名の指定

Netscape LDAP および **eDirectory LDAP** の識別名は次の構造に従って 指定します。

• user id (uid), organizational unit (ou), organization (o)

AD のユーザ名の指定

AD サーバでユーザ名に「cn=administrator,cn=users,dc=xyz,dc=com」 と指定して CC-SG ユーザを認証する場合、CC-SG ユーザがインポー トされた AD グループと関連付けられていれば、ユーザはこれらの資格 認定でアクセスを付与されます。通称 (cn)、組織ユニット (ou)、ドメ イン コンポーネント (dc) は複数指定できます。

ベース DN の指定

識別名は、ユーザ検索の開始点を指定するために使用することもできま す。識別名を [ベース DN] フィールドに入力することにより、ユーザ を検索する AD コンテナを指定します。たとえば、「 ou=DCAdmins,ou=IT,dc=xyz,dc=com」と入力すると、xyz.com ドメイン の DCAdmins と IT という組織ユニットに属すユーザがすべて検索さ れます。

認証および承認のモジュール指定

CC-SG で、モジュールとして外部サーバをすべて追加したら、そのそれぞれを認証、承認、または両方のいずれに使用するかを指定します。

▶ 認証および承認のモジュールを指定するには

- 1. [管理]>[セキュリティ]を選択します。
- [認証] タブをクリックします。設定したすべての外部承認および認 証サーバが、テーブルに表示されます。
- **3.** リストされたサーバごとに、次の手順に従います。
 - a. CC-SG でユーザの認証にこのサーバを使用する場合は、[認証] チェックボックスを選択します。
 - b. CC-SG でユーザの承認にこのサーバを使用する場合は、[承認] チェックボックスをオンにします。承認には、AD サーバのみ を使用できます。



4. [更新] をクリックして変更を保存します。

外部 AA サーバの順序の確立

CC-SG は、設定された外部承認および認証サーバを、指定した順序で 照会します。CC-SG では、最初にチェックされたオプションが使用で きない場合は 2 番目の認証、2 番目が使用できない場合は 3 番目、以 下同様に成功するまで繰り返されます。

- CC-SG が外部認証および承認サーバを使用する順序を確立するには、以下の手順に従います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [認証] タブをクリックします。設定したすべての外部承認および認 証サーバが、テーブルに表示されます。
- 3. リストからサーバを選択し、上下矢印をクリックして認証と承認の 優先順位を設定します。
- 4. [更新] をクリックして変更を保存します。

AD および CC-SG の概要

CC-SG は AD ドメイン コントローラからインポートされたユーザ認 証と承認をサポートするため、ユーザは CC-SG でローカルに定義され る必要はありません。これにより、AD サーバでユーザが排他的に維持 されます。AD サーバが CC-SG でモジュールとして設定されていれば 、CC-SG は、すべてのドメイン コントローラでそのドメイン名を照会 できます。CC-SG が AD ユーザ グループについて最新の承認情報を 持つように、CC-SG の AD モジュールと AD サーバを同期できます

重複 AD モジュールを追加しないでください。ユーザがログインを試み たときに、「グループのメンバではありません」という内容のメッセー ジが表示された場合、重複 AD モジュールを設定している可能性があり ます。設定したモジュールを調べ、記述するドメイン領域がオーバーラ ップしていないかを確認してください。

CC-SG への AD モジュールの追加

重要: 適切な AD ユーザ グループを作成し、この処理を開始する前に、 AD ユーザを AD ユーザ グループに割り当ててください。また、設定 マネージャで、CC-SG DNS とドメイン サフィックスを設定したことを 確認してください。「*CC-SG ネットワークの設定* **『271p.』」を参**照 してください。



- CC-SG に AD モジュールを追加するには、以下の手順に従います
- 1. [管理]>[セキュリティ]を選択します。
- 2. [認証] タブをクリックします。
- 3. [追加] をクリックして [モジュールの追加] ウィンドウを開きます。
- [モジュール タイプ] ドロップダウン メニューをクリックし、リストから AD を選択します。
- 5. AD サーバの名前を [モジュール名] フィールドに入力します。
 - 最大 31 文字で設定します。
 - 印刷可能なすべての文字を使用できます。
 - モジュール名は必須ではなく、CC-SG で他に設定するサーバがある場合に、この AD サーバ モジュール他のサーバから区別する目的のみに使用されます。この名前は実際の AD サーバ名には一切関連がありません。
- 6. [次へ] をクリックして続けます。[全般] タブが開きます。

AD の一般設定

[全般] タブでは、CC-SG が AD サーバを照会できるようにする情報を 追加する必要があります。

重複 AD モジュールを追加しないでください。ユーザがログインを試み たときに、「グループのメンバではありません」という内容のメッセー ジが表示された場合、重複 AD モジュールを設定している可能性があり ます。設定したモジュールを調べ、記述するドメイン領域がオーバーラ ップしていないかを確認してください。

 照会する AD ドメインを [ドメイン] フィールドに入力します。た とえば、AD ドメインが xyz.com ドメインにインストールされてい る場合は、[ドメイン] フィールドに「xyz.com」と入力します。照会 する CC-SG および AD サーバは、同じドメイン、またはお互いに 信頼関係にある異なるドメインで設定されている必要があります。

注: CC-SG は、指定したドメインで、すべての既知ドメイン コン トローラを照会します。

 プライマリおよびセカンダリ DNS サーバの IP アドレスをそれぞ れプライマリ DNS の [DNS サーバ IP アドレス] およびセカンダ リ DNS の [DNS サーバ IP アドレス] フィールドに入力するか、[デフォルトの CC-SG DNS の使用] チェックボックスを選択して、 CC-SG の設定マネージャ セクションで設定された DNS を使用し ます。「*高度な管理* 『265p. 』」を参照してください。



 ユーザ名とパスワードを指定せずに AD サーバに接続する場合は [匿名バインド] チェックボックスを選択します。このオプションを 使用する場合は、AD サーバが匿名照会を許可するかどうかを確認 してください。

注: Windows 2003 の場合、デフォルトでは匿名照会は許可されてい ません。Windows 2000 サーバは特定の匿名操作を許可しています が、照会結果は各オブジェクトの許可設定に従います。

 匿名バインドを使用しない場合は、AD サーバを照会するのに使用 するユーザ アカウントのユーザ名を [ユーザ名] フィールドに入力 します。必要な形式は、AD のバージョンと設定により異なります 。次のいずれかの形式を使用します。

名前が User Name のユーザで、raritan.com ドメインでのログイン 名が UserN の場合、次のように入力します。

- cn=UserName,cn=users,dc=Raritan,dc=com
- UserName@raritan.com
- Raritan/UserName

注: 指定したユーザは、AD ドメインで検索照会を実行する権限を 持っている必要があります。たとえば、ユーザは、[Group scope] (グループ スコープ) が [グローバル]、[グループ タイプ] が [セキ ュリティ] に設定されている AD 内のグループに属している場合が あります。

- 5. AD サーバを照会するのに使用するユーザ アカウントのパスワード を [パスワード] と [パスワードの確認] フィールドに入力します。 最大 32 文字で設定します。
- 6. [接続テスト]をクリックすると、指定したパラメータで AD サーバ への接続がテストされます。接続に成功したことを示す確認メッセ ージが表示されるはずです。確認メッセージが表示されない場合は 、設定に誤りがないか確認してやり直します。
- 7. [次へ] をクリックして続けます。[詳細] タブが開きます。

AD の詳細設定

- ▶ AD の詳細設定を行うには、以下の手順に従います。
- 1. [詳細] タブをクリックします。
- AD サーバがリスニングするポート番号を入力します。デフォルトのポートは 389 です。LDAP のセキュアな接続を使用する場合は、このポートを変更しなければならない場合があります。セキュアな LDAP 接続の標準ポートは、636 です。



- 3. 接続にセキュア チャンネルを使用する場合は、[LDAP 用のセキュ アな接続] チェックボックスを選択します。オンにすると、CC-SG が、SSL を介した LDAP を使用して、AD に接続します。このオ プションは、AD 設定によってサポートされていない場合がありま す。
- 4. 認証検索照会が実行される際の [ベース DN] (ディレクトリ レベル/ エントリ) を指定します。CC-SG は、このベース DN から下流に 再帰的な検索を行うことができます。

例	説明
dc=raritan,dc=com	ユーザ エントリの検索 照会はディレクトリ構 造全体に対して実行さ れます。
cn=Administrators,cn=Users,dc=raritan,dc =com	ユーザ エントリの検索 照会は Administrators サブディレクトリ (エ ントリ) に対してのみ 実行されます。

- [フィルタ] フィールドにユーザの属性を入力し、検索照会の対象が その条件と一致するエントリのみに制限されるようにします。デフ オルトのフィルタは「objectclass=user」で、これはタイプが user の エントリのみが検索されることを意味します。
- 6. ユーザ エントリの検索照会が実行される方法を指定します。
 - アプレットからログインするユーザが AD サーバで検索照会を 実行する許可を持っている場合、[バインドの使用] チェックボ ックスを選択してください。ただし、[ユーザ名パターンをバイ ンド] でユーザ名パターンが指定されている場合は、このパター ンがアプレットで提供されるユーザ名とマージされ、マージさ れたユーザ名が AD サーバへの接続に使用されます。

例: 「cn={0},cn=Users,dc=raritan,dc=com」を指定し、アプレットで「TestUser」が提供された場合、CC-SG は「

cn=TestUser,cn-Users,dc=raritan,dc=com」を使用して AD サーバに接続します。



Ch 12: リモート認証

- [全般] タブで指定したユーザ名とパスワードを使って AD サーバに接続する場合は、[検索後にバインドを使用] チェックボックスを選択します。指定したベース DN からエントリが検索され、指定したフィルタ条件に一致し、属性「samAccountName」がアプレットで入力されたユーザ名と同じ場合には、エントリが検出されます。次に、アプレットで提供されたユーザ名とパスワードを使って 2 番目の接続が試行されます。この 2 番目のバインドはユーザが入力したパスワードが正しいことを確認します。
- 7. [次へ] をクリックして続けます。[グループ] タブが開きます。

AD のグループ設定

[グループ] タブでは、AD ユーザ グループのインポート元の正確な場所 を指定できます。

重要: AD からグループをインポートする前に、グループ設定を指定する 必要があります。

- 1. [グループ] タブをクリックします。
- 認証するユーザが含まれるグループが検索される際の [ベース DN] (ディレクトリ レベル/エントリ)を指定します。

例	説明
dc=raritan,dc=com	グループ内のユーザの検索照 会はディレクトリ構造全体に 対して実行されます。
cn=Administrators,cn=Users,dc=raritan,dc=c om	グループ内のユーザの検索照 会は Administrators サブデ ィレクトリ (エントリ) に対 してのみ実行されます。

3. [フィルタ] フィールドにユーザの属性を入力し、グループ内のユー ザの検索照会の対象がこの条件と一致するエントリのみに制限され るようにします。

たとえば、ベース DN に「cn=Groups,dc=raritan,dc=com」を指定し、フィルタに「(objectclass=group)」を指定した場合、Groups エントリの中のタイプ group のエントリがすべて返されます。

4. [次へ] をクリックして続けます。[信頼] タブが開きます。



AD の信頼設定

[信頼] タブでは、この新しい AD ドメインと既存ドメイン間の信頼関係 を設定できます。信頼関係により、認証されたユーザがドメインを超え てリソースにアクセスできるようになります。信頼関係は、受信、送信 、双方向、または無効となります。AD で異なるフォレストを表す AD モジュールがお互いの情報にアクセスできるようにするには、信頼関係 を設定します。CC-SG で設定した信頼は、AD で設定した信頼と一致 している必要があります。

- 1. [信頼] タブをクリックします。複数の AD ドメインを設定している 場合は、[信頼] タブには、他のドメインもすべて表示されます。
- [信頼パートナー]列のドメインでごとに、[信頼の方向]ドロップダウンメニューをクリックし、ドメイン間で確立する信頼の方向を選択します。1つのモジュールに変更を加えると、すべてのADモジュールで信頼の方向が更新されます。
 - 受信:ドメインから受信される情報は信頼されます。
 - 送信:選択したドメインに送信される情報が信頼されます。
 - 双方向:各ドメインからの双方向の情報が信頼されます。
 - 無効:ドメイン間では情報は交換されません。
- [適用] をクリックして変更を保存するか、[OK] をクリックして AD モジュールを保存してウィンドウを閉じます。
 [セキュリティ マネージャ] 画面の [External AA Servers] (外部 AA サーバ) の下に新しい AD モジュールが表示されます。
- CC-SG でユーザの認証にこの AD モジュールを使用する場合は、[認証] チェックボックスを選択します。CC-SG でユーザの承認に AD モジュールを使用する場合は、[承認] チェックボックスを選択 します。
- 5. [更新] をクリックして変更を保存します。

AD モジュールの編集

AD モジュールを設定したら、いつでも編集できます。

▶ AD モジュールを編集するには、以下の手順に従います。

- 1. [管理]>[セキュリティ] を選択します。
- [認証] タブをクリックします。設定したすべての外部承認および認 証サーバが、テーブルに表示されます。
- 3. 編集する AD モジュールを選択して、[編集] をクリックします。



Ch 12: リモート認証

- [モジュールの編集] ウィンドウの各タブをクリックし、構成されている設定を表示します。必要に応じて変更を加えます。「AD の一般設定『214p.』」、「AD の詳細設定『215p.』」、「AD のグループ設定『217p.』」、「AD の信頼設定『218p.』」を参照してください。
- 5. 接続情報を変更したら、[接続テスト] をクリックし、指定したパラ メータで AD サーバへの接続をテストします。接続に成功したこと を示す確認メッセージが表示されるはずです。確認メッセージが表 示されない場合は、設定に誤りがないか確認してやり直します。
- 6. [OK] をクリックして変更を保存します。
- 変更した AD ユーザ グループを同期させる必要があります。すべてのモジュールですべてのグループとユーザを同期させ、すべてのAD モジュールを同期させることもできます。「すべてのユーザ グループの AD との同期『222p.』」および「すべての AD モジュールの同期『223p.の"全 AD モジュールの同期"参照』」を参照してください。

AD ユーザ グループのインポート

AD サーバからグループをインポートする前に、AD モジュールでグル ープ設定を指定する必要があります。「AD のグループ設定 『217p. 』 」を参照してください。

インポートしたグループまたはユーザに変更を加えたら、変更した AD ユーザ グループを同期させて、インポートしたグループが AD の適切 なグループに対応付けられるようにする必要があります。さらに、すべ ての AD モジュールを同期させ、すべてのモジュールですべてのグルー プとユーザを同期させる必要もあります。「**すべてのユーザ グループの** AD との同期 『222p. 』」および「**すべての AD モジュールの同期** 『 223p. の"全 AD モジュールの同期 参照 』」を参照してください。

AD からはネストしたグループをインポートできます。

注: AD ユーザ グループのインポートを試みる前に、設定マネージャで、 CC-SG DNS とドメイン サフィックスを設定したことを確認してく ださい。「高度な管理 『265p. 』」を参照してください。

- AD ユーザ グループをインポートするには、以下の手順に従います。
- 1. [管理] > [セキュリティ] を選択します。
- 2. [認証] タブをクリックします。設定したすべての承認および認証サ ーバが、テーブルに表示されます。
- 3. インポートする AD ユーザ グループがある AD サーバを選択しま す。



- [AD ユーザ グループをインポート] をクリックし、AD サーバに保存されているユーザ グループ値のリストを取得します。ユーザ グループが CC-SG ユニットにない場合は、ここにインポートしてアクセス ポリシーを割り当てることができます。
- 5. CC-SG にインポートするグループを選択します。
 - インポートしたユーザ グループ名には、最大 64 文字を含める ことができます。
 - ユーザ グループを検索するには、検索文字列をユーザ グルー プを検索するフィールドに入力し、[実行] をクリックします。
 - 列ヘッダをクリックして、その列の情報でユーザ グループのリ ストを並べ替えます。
 - [すべて選択] をクリックすると、インポート用にすべてのユー ザ グループが選択されます。
 - [すべて選択解除]をクリックすると、ユーザ グループの選択が すべて解除されます。
- 6. [ポリシー] 列で、リストから CC-SG アクセス ポリシーを選択し て、選択したグループにポリシーを割り当てます。
- 7. [インポート] をクリックして選択したユーザ グループをインポート します。

ヒント: グループが正しくインポートされているか確認し、インポート したグループの権限を表示するには、[ユーザ] タブをクリックし、イン ポートされたグループを選択して、[ユーザ グループ プロファイル] 画 面を開きます。[権限] および [デバイス/ノード ポリシー] タブで情報を 確認します。[Active Directory の関連付け] タブをクリックし、ユーザ グループに関連付けられた AD モジュールの情報を表示します。



AD と CC-SG の同期

CC-SG にある情報を AD サーバの情報と同期させるには、いくつかの 方法があります。

- [すべてのモジュールの日次同期]: スケジュールされた同期を有効にして、毎日選択した時間に CC-SG をすべての AD モジュールと同期できます。「全 AD モジュールの同期『223p.』」を参照してください。この同期は、承認に AD を使用している場合のみ必要です。
- タスク マネージャを使用した [スケジュールされた同期]: 「タスク のスケジュール 『313p. 』」を参照してください。
- [オン デマンド同期]: 以下を選択する場合、常に 2 種類の同期を実 行できます。
 - 「すべての Active Directory モジュール]: このオプションでは 、すべてのモジュールの日次同期と同じ操作が実行されますが 、いつでもオン デマンドで同期する場合に使用できます。この 同期は、承認に AD を使用している場合のみ必要です。「 *AD モジュールの同期* 『223p. 』」を参照してください。
 - [すべてのユーザ グループ]: このオプションは、ユーザ グルー プを変更したときに使用します。すべてのユーザ グループを同 期すると、インポートしたローカル ユーザ グループを、AD モジュールの一部として識別されるユーザ グループに対応付け ることができます。ユーザ グループを同期しても、CC-SG 内 のアクセス情報は更新されません。日次同期の実行を待つか、 すべてのモジュールのオン デマンド同期を実行することにより 、すべての AD モジュールを同期させて、アクセス情報を更新 する必要があります。「すべてのユーザ グループの AD との同 期『222p.』」を参照してください。



すべてのユーザ グループの AD との同期

1 つのユーザ グループに変更を加えた場合 (ユーザ グループを別の AD モジュールに移動するなど)、すべてのユーザ グループを同期させ てください。ユーザ グループ プロファイルの [Active Directory の関連 付け] タブで、ユーザ グループの AD 関連を手動で変更することもで きます。

ユーザまたはドメイン コントローラに変更を加えた場合は、すべての AD モジュールを同期させてください。「*全 AD モジュールの同期*『 223p. 』」を参照してください。

AD ユーザ グループを同期させると、CC-SG は選択した AD モジュ ールのグループを取得し、その名前を CC-SG 内のユーザ グループの 名前と比較して、一致を確認します。CC-SG は一致したユーザ グルー プを表示します。これで、CC-SG と関連付ける AD 内のグループを選 択できます。この操作を行っても、CC-SG 内のユーザアクセス情報は 更新されません。AD ユーザ グループを同期しても、AD のグループ名 が CC-SG に対応付けられるだけです。

すべてのユーザ グループを AD と同期するには、以下の手順に従います。

- 1. [管理]>[セキュリティ] を選択します。
- 2. [認証] タブをクリックします。設定したすべての承認および認証サ ーバが、テーブルに表示されます。
- 3. CC-SG 内のユーザ グループと同期させるユーザ グループを持つ AD サーバを選択します。
- [オン デマンド同期] リストで [すべてのユーザ グループ] を選択し、 (今すぐ同期] をクリックします。
- CC-SG 内のユーザ グループと名前が一致する AD モジュールで見 つかったすべてのユーザ グループのリストが表示されます。同期さ せるユーザ グループを選択して、[OK] をクリックします。 選択したモジュールにあるインポートされたユーザ グループがすべ て同期されたら、確認のメッセージが表示されます。



全 AD モジュールの同期

AD のユーザを変更または削除した場合、AD のユーザ許可を変更した 場合、ドメイン コントローラに変更を加えた場合は、必ずすべての AD モジュールを同期する必要があります。

すべての AD モジュールを同期させると、CC-SG は設定されているす べての AD モジュールでユーザ グループを取得し、その名前を CC-SG にインポートされたユーザ グループまたは CC-SG 内の AD モジュールに関連付けられたユーザ グループの名前と比較して、 CC-SG ローカル キャッシュを更新します。CC-SG のローカル キャッ シュには、各ドメインの全ドメイン コントローラ、CC-SG のモジュー ルに関連付けられているすべてのユーザ グループ、既知の AD ユーザ のユーザ情報が含まれます。ユーザ グループが AD モジュールから削 除されると、CC-SG は削除されたグループに対するすべての関連を自 身のローカル キャッシュからも削除します。これにより、CC-SG は最 新の AD グループ情報を維持できます。

▶ すべてのモジュールを同期するには、以下の手順に従います。

- 1. [管理]>[セキュリティ]を選択します。
- 2. [認証] タブをクリックします。設定したすべての承認および認証サ ーバが、テーブルに表示されます。
- [オン デマンド同期] リストで [すべての Active Directory モジュー ル] を選択し、[今すぐ同期] をクリックします。すべての AD モジ ュールが同期されると、確認のメッセージが表示されます。

MSFT Windows Server 2003 AD でユーザのパスワードを変更する場合は、古いパスワードと新しいパスワードの両方が約 30 分間有効になります。この間、ユーザはどちらのパスワードを使っても CC-SG にログインできます。これは、AD が新しいパスワードを完全に更新するまでの 30 分間古いパスワードをキャッシュするからです。

すべての AD モジュールの日次同期の有効化または無効化

同期の頻度を増やすには、すべての AD モジュールを同期するようにタ スクをスケジュールします。「タスクのスケジュール 『313p. 』」を参 照してください。

- ▶ すべての AD モジュールの日次同期を有効にするには、以下の手順 に従います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [認証] タブをクリックします。設定したすべての承認および認証サ ーバが、テーブルに表示されます。
- 3. [すべてのモジュールの日次同期] チェックボックスをオンにします



- [同期時間] フィールドで、上下矢印をクリックし、CC-SG により 行われるすべての AD モジュールの日次同期の実行時刻を選択しま す。
- 5. [更新] をクリックして変更を保存します。
- ▶ すべての AD モジュールの日次同期を無効にするには、以下の手順 に従います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [認証] タブをクリックします。設定したすべての承認および認証サ ーバが、テーブルに表示されます。
- 3. [すべてのモジュールの日次同期] チェックボックスを選択解除しま す。
- 4. [更新] をクリックして変更を保存します。

AD の日次同期の時刻の変更

日次同期が有効な場合、自動同期が行われる時間を指定できます。デフ オルトでは、日次同期は 23:30 に実行されます。

- ▶ AD の日次同期の時刻を変更するには、以下の手順に従います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [認証] タブを選択します。[すべてのモジュールの日次同期] チェッ クボックスが選択されていることを確認します。
- 3. 画面の下部にある [AD Synchronization Time] (AD 同期時間) フィ ールドで、上下矢印をクリックし、CC-SG により毎日行われる全 AD モジュール同期化の実行時刻を選択します。
- 4. [更新]をクリックして変更を保存します。



AD グループの名前の変更および移動

▶ AD グループ名の変更:

CC-SG にインポートされた AD グループの名前が AD で変更された 場合は、同期時または影響を受けた AD ユーザの初めてのログイン時に 名前の変更が検出されると、監査証跡で警告が報告されます。

"User group <group name> has been renamed to <group new name> in AD module <module name>.(ユーザ グループ <グルー プ名> は、AD モジュール <モジュール名> で名前が <新しいグループ 名> に変更されました。)"

AD グループの削除または移動:

CC-SG にインポートされた AD グループが削除されたか、グループの 検索ベースから移動された場合は、監査証跡で警告が報告されます。グ ループの AD の関連付けが削除されます。

"User group <group name> cannot be found in AD module <module name>.(ユーザ グループ <グループ名> は、AD モジュール <モジュー ル名> で見つかりません。)"

▶ 検索ベース内の AD グループの移動:

検索ベース内で AD グループが移動されても、警告は報告されず、グル ープは通常どおり機能します。

LDAP と CC-SG について

CC-SG を起動し、ユーザ名とパスワードを入力すると、CC-SG を介し て、または LDAP サーバに直接照会されます。ユーザ名とパスワード が LDAP ディレクトリ内のものと一致すれば、ユーザが認証されます 。そのユーザは LDAP サーバのローカル ユーザ グループに対して承 認されます。

CC-SG への LDAP (Netscape) モジュールの追加

- CC-SG に LDAP (Netscape) モジュールを追加するには、以下の 手順に従います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [認証] タブをクリックします。
- 3. [追加] をクリックして [モジュールの追加] ウィンドウを開きます。
- [モジュール タイプ] ドロップダウン メニューをクリックし、リストから LDAP を選択します。
- 5. LDAP サーバの名前を [モジュール名] に入力します。



6. [次へ] をクリックして続けます。[全般] タブが開きます。

LDAP の一般設定

- 1. [全般] タブをクリックします。
- LDAP サーバの IP アドレスまたはホスト名を [IP アドレス/ホスト 名] フィールドに入力します。ホスト名のルールについては、「用語 /略語 『2p. 』」を参照してください。
- 3. ポート値を [ポート] フィールドに入力します。デフォルトのポート は 389 です。
- 4. セキュアな LDAP サーバを使用する場合は、[LDAP over SSL (SSL を介した LDAP)] を選択します。
- 5. LDAP サーバで匿名照会が許可される場合は、[匿名バインド] を選 択します。匿名バインドでは、ユーザ名とパスワードを入力する必 要はありません。

注: Windows 2003 の場合、デフォルトでは匿名照会は許可されてい ません。Windows 2000 サーバは特定の匿名操作を許可しています が、照会結果は各オブジェクトの許可設定に従います。

6. 匿名バインドを使用しない場合、ユーザ名を [ユーザ名] フィールド に入力します。識別名 (DN) を入力して LDAP サーバの照会に使 用する資格認定を指定します。DN には、通称、組織ユニット、ド メインを入力します。

たとえば、「

uid=admin,ou=Administrators,ou=TopologyManagement,o=Netscape Root」と入力します。値はカンマで区切りますが、カンマの前後にス ペースは入れません。Command Center のように、値にはスペース を使用できます。

- 7. パスワードを [パスワード] と [パスワードの確認] フィールドに入力します。
- ユーザの検索を開始する位置を指定するには、[ベース DN] に識別 名を入力します。たとえば、「 ou=Administrators,ou=TopologyManagement,o=NetscapeRoot」では このドメインの下のすべての組織ユニットが検索されます。
- 特定のオブジェクト タイプのみに検索を絞り込む場合は、[フィル タ] フィールドに値を入力します。たとえば、「(objectclass=person) 」では person オブジェクトのみに検索が絞り込まれます。
- 指定したパラメータで LDAP サーバをテストするには、[接続テスト] をクリックします。接続に成功したことを示す確認メッセージが表示されるはずです。表示されない場合は、設定に誤りがないか確認してやり直します。
- 11. [次へ] をクリックして [詳細] タブを開き、LDAP サーバ用の詳細 設定オプションを設定します。



LDAP の詳細設定

- 1. [詳細] タブをクリックします。
- 暗号化を使用してパスワードを LDAP サーバに送信する場合は、 [Base 64] を選択します。プレーン テキストを使用してパスワード を LDAP サーバに送信する場合は、[プレーン テキスト] を選択し ます。
- 3. デフォルト ダイジェスト: ユーザ パスワードのデフォルトの暗号 化を選択します。
- ユーザ属性とグループ メンバシップ属性パラメータを、[ユーザ属 性] および [グループ メンバシップ属性] フィールドに入力します 。これらの値は LDAP ディレクトリ スキーマから取得する必要が あります。
- 5. バインド パターンを [ユーザ名パターンをバインド] フィールドに 入力します。
 - CC-SG を使って、ログイン時に入力したユーザ名とパスワードをLDAPサーバに送信し認証を行う場合には、[バインドの使用]を選択します。[バインドの使用]がオンになっていない場合、CC-SGはLDAPサーバからユーザ名を検索します。見つかった場合には、LDAPオブジェクトを取得し、ローカルで関連パスワードを入力されたパスワードと比較します。
 - 一部の LDAP サーバでは、パスワードを LDAP オブジェクト の一部として取得できません。[検索後にバインドを使用] チェ ックボックスを選択して、パスワードを LDAP オブジェクトに 再度バインドし、認証用にサーバに送り返すよう CC-SG に指 示します。
- 6. [OK] をクリックして変更を保存します。[セキュリティ マネージャ] 画面の [External AA Servers] (外部 AA サーバ) の下に新しい LDAP モジュールが表示されます。
- 7. CC-SG でユーザの認証に LDAP モジュールを使用する場合は、[認 証] チェックボックスを選択します。
- 8. [更新] をクリックして変更を保存します。

Sun One LDAP (iPlanet)の設定

リモート認証に Sun One LDAP サーバを使用している場合、次の例に 従います。

パラメータ名	SUN One LDAP パラメータ
IP アドレス/ホスト名	<ディレクトリ サーバの IP アド レス>
ユーザ名	CN=<有効なユーザ ID>



パラメータ名	SUN One LDAP パラメータ
パスワード	<パスワード>
ベース DN	O=<組織>
フィルタ	(objectclass=person)
パスワード ([詳細] 画面)	プレーン テキスト
パスワード デフォルト ダイジェスト (詳細)	SHA
バインドの使用	チェックボックスをオフ
検索後にバインドを使用	チェックボックスをオン

OpenLDAP (eDirectory)の設定

リモート認証に OpenLDAP サーバを使用している場合、次の例に従い ます。

パラメータ名	Open LDAP パラメータ
IP アドレス/ホスト名	<ディレクトリ サーバの IP アドレス>
ユーザ名	CN=<有効なユーザ ID>, O=<組織>
パスワード	<パスワード>
ユーザ ベース	O=accounts, O=<組織>
ユーザ フィルタ	(objectclass=person)
パスワード ([詳細] 画面)	Base64
パスワード デフォルト ダイジェス ト (詳細)	Crypt
バインドの使用	チェックボックスをオフ
検索後にバインドを使用	チェックボックスをオン

IBM LDAP の設定

リモート認証に IBM LDAP サーバを使用している場合、次の例に従います。

パラメータ名	IBM LDAP パラメータ
IP アドレス/ホスト名	<ディレクトリ サーバの IP アドレス>



Ch 12: リモート認証

パラメータ名	IBM LDAP パラメータ
ユーザ名	CN=<有効なユーザ ID>
パスワード	<パスワード>
	たとえば、
ユーザ ベース	cn=users,DC=raritan,DC=com,DC=us
ユーザ フィルタ	(objectclass=person)
パスワード ([詳細] 画面)	Base64
パスワード デフォルト ダイジェス	
ト (詳細)	[なし]
ユーザ属性	uid
グループ メンバーシップ属性	空白のままにします。
	たとえば、
ユーザ名パターンをバインド	cn={0},cn=users,DC=raritan,DC=com,DC=us
バインドの使用	チェックボックスをオフ
検索後にバインドを使用	チェックボックスをオン

TACACS+ と CC-SG について

TACACS+ サーバによってリモート認証される CC-SG ユーザは、 TACACS+ サーバと CC-SG に作成する必要があります。ユーザ名には TACACS+ サーバと CC-SG で同じ名前を使用する必要がありますが、 パスワードは異なっていてもかまいません。「ユーザとユーザ グループ 『176p.』」を参照してください。

TACACS+ モジュールの追加

- ▶ TACACS+ モジュールを追加するには、以下の手順に従います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [認証] タブをクリックします。
- 3. [追加] をクリックして [モジュールの追加] ウィンドウを開きます。
- 4. [モジュール タイプ] > [TACACS+] を選択します。
- 5. TACACS+ サーバの名前を [モジュール名] フィールドに入力しま す。
- 6. [次へ] をクリックします。[全般] タブが開きます。



TACACS+ の一般設定

- TACACS+ サーバの IP アドレスまたはホスト名を [IP アドレス/ホ スト名] フィールドに入力します。ホスト名のルールについては、 「*用語|略語* 『2p. 』」を参照してください。
- 2. TACACS+ サーバがリスニングするポート番号を [ポート番号] フ ィールドに入力します。デフォルトのポート番号は 49 です。
- 3. 認証ポートを [認証ポート] フィールドに入力します。
- 4. 共有キーを [共有キー] と [共有キーの確認] フィールドに入力しま す。最大 128 文字で設定します。
- [OK] をクリックして変更を保存します。[セキュリティ マネージャ] 画面の [External AA Servers] (外部 AA サーバ) の下に新しい TACACS+ モジュールが表示されます。
- 6. CC-SG でユーザの認証に TACACS+ モジュールを使用する場合は 、[認証] チェックボックスを選択します。
- 7. [更新] をクリックして変更を保存します。

RADIUS と CC-SG について

RADIUS サーバによってリモート認証される CC-SG ユーザは、 RADIUS サーバと CC-SG に作成する必要があります。ユーザ名には RADIUS サーバと CC-SG で同じ名前を使用する必要がありますが、 パスワードは異なっていてもかまいません。「ユーザとユーザ グループ 『176p.』」を参照してください。

RADIUS モジュールの追加

- ▶ RADIUS モジュールを追加するには、以下の手順に従います。
- 1. [管理]>[セキュリティ] を選択します。
- 2. [認証] タブをクリックします。
- 3. [追加] をクリックして [モジュールの追加] ウィンドウを開きます。
- [モジュール タイプ] ドロップダウン メニューをクリックし、リストから RADIUS を選択します。
- 5. RADIUS サーバの名前を [モジュール名] フィールドに入力します。
- 6. [次へ] をクリックして続けます。[全般] タブが開きます。

RADIUS の一般設定

1. [全般] タブをクリックします。



- 2. RADIUS サーバの IP アドレスまたはホスト名を [IP アドレス/ホ スト名] フィールドに入力します。ホスト名のルールについては、 「*用語/略語* **[2**p. **』**」を参照してください。
- 3. ポート番号を [ポート番号] フィールドに入力します。デフォルトの ポート番号は 1812 です。
- 4. 認証ポートを [認証ポート] フィールドに入力します。
- 5. 共有キーを [共有キー] と [共有キーの確認] 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。
- [セキュリティ マネージャ] 画面の [External AA Servers] (外部 AA サーバ) の下に新しい RADIUS モジュールが表示されます。
 CC-SG でユーザの認証に RADIUS モジュールを使用する場合は、
 [認証] チェックボックスを選択します。
- 8. [更新] をクリックして変更を保存します。

RADIUS による 2 ファクタ認証

RSA 認証マネージャとともに 2 ファクタ認証をサポートする RSA RADIUS サーバを使用すると、CC-SG が、動的トークンで 2 ファク タ認証スキーマを使用できるようになります。

こうした環境では、ユーザは、CC-SG にログインします。その場合、 まずそのユーザ名を [ユーザ名] フィールドに入力してから、その固定 パスワードと動的トークン値を [パスワード] フィールドに入力します

CC-SG の設定は、前述の標準 RADIUS リモート認証と同じです。「2 ファクタ認証 『422p. 』」を参照してください。



Ch 13



この章の内容

レポートの使用	232
監査証跡レポート	234
エラー ログ レポート	235
アクセス レポート	236
可用性レポート	237
アクティブ ユーザ レポート	237
ロックアウト ユーザ レポート	238
全ユーザ データ レポート	238
ユーザ グループ データ レポート	239
デバイス資産レポート	239
デバイス グループ データ レポート	239
ポートの照会レポート	240
ノード資産レポート	241
アクティブ ノード レポート	242
ノード作成レポート	242
ノード グループ データ レポート	243
AD ユーザ グループ レポート	243
スケジュールされたレポート	244
デバイス ファームウェアのアップグレード レポート	245

レポートの使用

レポートのデフォルト フィルタはユーザ ポリシーです。たとえば、ユ ーザがアクセス許可を持たないノードまたはデバイスは、レポートには 表示されません。

レポート データのソート

- 列のヘッダをクリックすると、レポート データはその列の値でソートされます。データはアルファベット、数字、または年代ごとに昇順で更新されます。
- 列のヘッダを再度クリックすると、降順でソートされます。

レポートの列幅の変更

選択した列幅は、次回にログインしてレポートを実行する場合に、デフ オルトのレポート ビューとなります。

- 1. 変更するには、マウス ポインタが両向きの矢印に表示される、ヘッ ダ行の列の境界に置きます。
- 2. 矢印を左右にクリック アンド ドラッグし、列幅を調整します。



レポートの詳細の表示

- 行をダブルクリックするとそのレポートの詳細が表示されます。
- 詳細を表示するには、行がハイライトされているときに Enter キー を押します。

ダイアログ ボックスが表示され、レポート画面で表示できる詳細だけ でなく、選択したレポートの詳細がすべて表示されます。たとえば、ノ ードの [アクセス レポート] 画面には、インタフェースのタイプおよび メッセージは表示されませんが、[ノード アクセスの詳細] ダイアログ ボックスではこれらを使用できます。

複数ページ レポート間の移動

 レポートの下にある矢印アイコンをクリックすると、複数ページの レポート間で移動できます。

レポートの印刷

CC-SG には 2 つの印刷オプションがあります。レポート ページを画 面の表示通りに印刷するか (スクリーンショットの印刷)、各項目の詳細 を含む完全なレポートを印刷できます。

注:印刷オプションは、すべての CC-SG ページで機能します。

- レポートのスクリーンショットを印刷するには、以下の手順に従い ます。
- 1. 印刷するレポートを生成します。
- 2. [Secure Gateway] > [画面印刷] を選択します。
- レポート詳細をすべて印刷するには、以下の手順に従います。
- 1. 印刷するレポートを生成します。[表示するエントリ] フィールドで [すべて] を選択していることを確認します。
- 2. [Secure Gateway] > [印刷] を選択します。

ファイルへのレポートの保存

レポートは、Excel で表示可能な .CSV ファイルに保存できます。レポ ートをファイルに保存すると、レポート画面に表示された詳細だけでな く、すべてのレポートの詳細が保存されます。たとえば、ノードの [ア クセス レポート] 画面には、[タイプ] および [メッセージ] 列は表示さ れませんが、[アクセス レポート] を保存して Excel で開くと、これら の列を使用できます。

- 1. ファイルに保存するレポートを生成します。
- 2. [ファイルに保存] をクリックします
- 3. ファイルの名前を入力し、保存する場所を選択します。



4. [保存] をクリックします。

CC-SG からのレポートのデータの消去

監査証跡レポートとエラー ログ レポートに表示されるデータを消去で きます。これらのレポートを消去すると、使用された検索条件を満たす すべてのデータが削除されます。たとえば、2008 年 3 月 26 日から 2008 年 3 月 27 日までのすべての監査証跡のエントリを検索する場合 、該当するレコードのみが消去されます。3 月 26 以前または 3 月 27 日以後のエントリは、監査証跡に残ります。

消去されたデータは、CC-SG から完全に削除されます。

- CC-SG からレポートのデータを消去するには、以下の手順に従い ます。
- 1. CC-SG から削除するデータを含むレポートを生成します。
- 2. [消去] をクリックします。
- 3. [はい] をクリックして確認します。

レポート フィルタの非表示または表示

一部のレポートでは、レポート画面の上部に一連のフィルタ条件が用意 されています。フィルタ セクションを非表示にすると、レポート領域 を拡張できます。

- レポートフィルタを非表示または表示にするには、以下の手順に従います。
- 画面の上部にあるフィルタ ツールバーをクリックして、フィルタ セクションを非表示にします。
- フィルタ ツールバーを再度クリックして、フィルタ セクションを 表示します。

監査証跡レポート

イベントの監査証跡は、CC-SG によってシステムに保持されます。監 査証跡には、デバイスやポートの追加、編集、削除、システムへのその 他の変更が記録されます。

注: 監査証跡には、ユーザがブックマーク ポートに接続したときにエン トリが記録されますが、接続に使用されたブラウザ インスタンスが閉 じるまでログアウト エントリは記録されません。

- 監査証跡レポートを生成するには、以下の手順に従います。
- 1. [レポート]>[監査証跡] を選択します。


- [開始日付/時刻] フィールドと [終了日付/時刻] フィールドでレポー トの日付範囲を設定します。デフォルトの日付の各部分 (月、日、 年、時、分、秒) をクリックして選択し、適切な数値になるまで上 下の矢印をクリックします。
- [メッセージ タイプ]、[メッセージ]、[ユーザ名]、および [ユーザ IP アドレス]の各フィールドに追加パラメータを入力して、レポート に含まれるデータを制限できます。これらのフィールド ([メッセー ジ タイプ]フィールドを除く)では、ワイルドカードを使用できま す。
 - レコードを一定タイプのメッセージに限定するには、[メッセージ タイプ]フィールドでタイプを選択します。
 - レポートをアクティビティに関連したメッセージ テキストで限 定するには、そのテキストを [メッセージ] フィールドに入力し ます。
 - レポートを特定のユーザ アクティビティに限定するには、その ユーザのユーザ名を [ユーザ名] フィールドに入力します。
 - レポートを特定の IP アドレスのアクティビティに限定するには、ユーザの IP アドレスを [ユーザ IP アドレス] フィールドに入力します。
- 4. [表示するエントリ] フィールドで、レポート画面に表示するエント リの数を選択します。
- 5. [適用] をクリックしてレポートを生成します。
 - レポート内のレコードを消去するには、[消去] をクリックします。「CC-SG からのレポートのデータの消去 『234p. 』」を参照してください。

エラー ログ レポート

CC-SG では、エラー メッセージが一連のエラー ログ ファイルに保存 され、問題をトラブルシューティングする場合にこれらのファイルにア クセスして利用できます。エラー ログには、エラー条件に関連付けら れた監査証跡エントリのサブセットが含まれています。

▶ エラー ログ レポートを生成するには、以下の手順に従います。

- 1. [レポート]>[エラー ログ] を選択します。
- [開始日付/時刻] フィールドと [終了日付/時刻] フィールドでレポー トの日付範囲を設定します。デフォルトの日付の各部分 (月、日、 年、時、分、秒) をクリックして選択し、適切な数値になるまで上 下の矢印をクリックします。
- [メッセージ]、[ユーザ名]、および [ユーザ IP アドレス] の各フィー ルドに追加パラメータを入力して、レポートに含まれるデータを制 限できます。これらのフィールドでは、ワイルドカードを使用でき ます。



- レポートをアクティビティに関連したメッセージ テキストで限 定するには、そのテキストを [メッセージ] フィールドに入力し ます。
- レポートを特定のユーザアクティビティに限定するには、その ユーザのユーザ名を [ユーザ名] フィールドに入力します。
- レポートを特定の IP アドレスのアクティビティに限定するには、ユーザの IP アドレスを [ユーザ IP アドレス] フィールドに入力します。
- 4. [表示するエントリ] フィールドで、レポート画面に表示するエント リの数を選択します。
- 5. [適用] をクリックしてレポートを生成します。
 - [消去] をクリックして、エラー ログを削除します。「CC-SG からのレポートのデータの消去 『234p. 』」を参照してください

アクセス レポート

アクセス レポートを生成すると、アクセスされたデバイスとノード、 そのアクセス時点、およびそれらにアクセスしたユーザに関する情報が 表示されます。

▶ アクセス レポートを生成するには、以下の手順に従います。

- 1. [レポート]>[アクセス レポート] を選択します。
- 2. デバイスまたはノードを選択します。
- [開始日付/時刻] フィールドと [終了日付/時刻] フィールドでレポー トの日時範囲を設定します。デフォルトの日付の各部分 (月、日、 年、時、分、秒) をクリックして選択し、適切な数値になるまで上 下の矢印をクリックします。
- [デバイス名]、[ノード名]、[ユーザ名]、および [ユーザ IP アドレス]の各フィールドに追加パラメータを入力して、レポートに含まれるデータを制限できます。これらのフィールドでは、ワイルドカードを使用できます。
 - レポートをアクティビティに関連したメッセージ テキストで限 定するには、そのテキストを [メッセージ] フィールドに入力し ます。
 - レポートを特定のデバイスに限定するには、そのデバイス名を[デバイス名]フィールドに入力します。
 - レポートを特定のノードに限定するには、そのノード名を[ノー ド名]フィールドに入力します。
 - レポートを特定のユーザ アクティビティに限定するには、その ユーザのユーザ名を [ユーザ名] フィールドに入力します。



- レポートを特定の IP アドレスのアクティビティに限定するには、ユーザの IP アドレスを [IP アドレス] フィールドに入力します。
- 5. [表示するエントリ] フィールドで、レポート画面に表示するエント リの数を選択します。
- 6. [適用] をクリックしてレポートを生成します。

可用性レポート

可用性レポートには、デバイスまたはノードへのすべての接続のステー タスが表示されます。このレポートでは、CC-SG で管理するネットワ ーク内のすべてのデバイスまたはノードに関するすべての可用性情報を 参照できます。

- ▶ 可用性レポートを生成するには、以下の手順に従います。
- 1. [レポート]>[可用性レポート]を選択します。
- 2. [ノード] または [デバイス] を選択します。
- 3. [適用] をクリックします。

アクティブ ユーザ レポート

アクティブ ユーザ レポートには、現在のユーザとユーザ セッション が表示されます。レポートからアクティブ ユーザを選択し、**CC-SG** か ら切断できます。

- アクティブ ユーザ レポートを生成するには、以下の手順に従います。
- [レポート]>[ユーザ]>[アクティブ ユーザ] を選択します。
- CC-SG のアクティブなセッションからユーザを切断するには、以下の手順に従います。
- 1. アクティブ ユーザ レポートで、切断するユーザ名を選択します。
- 2. [ログアウト] をクリックします。



ロックアウト ユーザ レポート

ロックアウト ユーザ レポートには、ログインを試みて何度も失敗した ために CC-SG から現在ロックアウトされているユーザが表示されます 。このレポートからユーザをアンロックできます。「*ロックアウト設定* 『*302*p.』」を参照してください。

- ロックアウト ユーザ レポートを生成するには、以下の手順に従います。
- [レポート]>[ユーザ]>[ロックアウト ユーザ] を選択します。
- CC-SG からロックアウトされているユーザをアンロックするには 、以下の手順に従います。
- アンロックするユーザを選択して、[ユーザのアンロック]を選択し ます。

全ユーザ データ レポート

ユーザ データ レポートには、**CC-SG** データベース内のすべてのユー ザに関するデータが表示されます。

- 全ユーザ データ レポートを生成するには、以下の手順に従います。
- [レポート]>[ユーザ]>[全ユーザ データ] を選択します。
 - [ユーザ名] フィールドには、すべての CC-SG ユーザのユーザ 名が表示されます。
 - [有効] フィールドには、ユーザが CC-SG にログインできる場合は [true] が表示され、ログインできない場合は [false] が表示されます。どちらが表示されるかは、ユーザ プロファイルで [ログイン有効] オプションが選択されいるかどうかによります。「ユーザの追加 『183p. 』」を参照してください。
 - [パスワードの有効期間] フィールドには、ユーザが同じパスワード使用し続けられる日数が表示されます。この期間が過ぎると、必ずパスワードを変更しなければならなくなります。「ユーザの追加 『183p. 』」を参照してください。
 - [グループ] フィールドには、ユーザが所属するユーザ グループ が表示されます。
 - [権限] フィールドには、ユーザに割り当てられている CC-SG 権限が表示されます。「ユーザ グループ権限 『398p. 』」を参 照してください。
 - [電子メール] フィールドには、ユーザ プロファイルで指定され たユーザの電子メールアドレスが表示されます。



[ユーザ タイプ] フィールドには、ユーザのアクセス方法に応じて[ローカル] または [リモード] が表示されます。

ユーザ グループ データ レポート

ユーザ グループ データ レポートには、ユーザとユーザが関連するグ ループに関するデータが表示されます。

- ユーザ グループ データ レポートを生成するには、以下の手順に従います。
- 1. [レポート]>[ユーザ]>[ユーザ グループ データ] を選択します。
- ユーザ グループをダブルクリックして、割り当てられたポリシーを 表示します。

デバイス資産レポート

デバイス資産レポートには、現在 CC-SG の管理下にあるデバイスに関 するデータが表示されます。

- デバイス資産レポートを生成するには、以下の手順に従います。
- [レポート]>[ノード]>[デバイス資産レポート]を選択します。すべてのデバイスに関するレポートが生成されます。
- デバイス タイプでレポート データをフィルタするには、以下の手順に従います。
- デバイス タイプを選択して、[適用] をクリックします。選択したフィルタが適用された状態でレポートが再生成されます。
 - 互換表に準拠しないバージョンのデバイスは、[デバイス名] フィールドに赤で表示されます。

デバイス グループ データ レポート

デバイス グループ データ レポートには、デバイス グループ情報が表示されます。

- デバイス グループ データ レポートを生成するには、以下の手順に 従います。
- 1. [レポート]>[デバイス]>[デバイス グループ データ] を選択します
- 行をダブルクリックして、グループ内のデバイスのリストを表示します。



ポートの照会レポート

ポートの照会レポートには、ポート ステータス別に全ポートが表示さ れます。

- ▶ ポートの照会レポートを生成するには、以下の手順に従います。
- 1. [レポート]>[ポート]>[ポートの照会]を選択します。
- [ポート ステータス/可用性] セクションで、レポートに含めるポートの状態を選択します。複数のチェックボックスをオンにすると、 選択したすべての状態のポートが含められます。[ステータス] オプションを指定した場合は、少なくとも1つの[可用性] オプション を選択する必要があります。

状態タイプ	ポートの状態	定義
	すべて	すべてのポート。
ステータス:		
	Up	
	Down	デバイス停止しているか利用可能で はないためポートに接続できません 。
可用性:		
	アイドル	ポートは設定済みでポートへの接続 が可能な状態です。
	接続しました	
	使用中	ユーザがこのポートに接続していま す。
	電源オン	
	電源オフ	
未設定:		
	新規	ポートにターゲット サーバが接続 されていますが、ポートはまだ設定 されていません。
	未使用	ポートにターゲット サーバが接続 されておらず、ポートはまだ設定さ れていません。



- ゴーストになっているポートを含めるには、[ゴースト ポート] を 選択します。ゴースト ポートは、CIM またはターゲット サーバが Paragon システムから削除されるか、電源がオフになる (手動また は偶発的に) 場合に生じます。Raritan の『Paragon II ユーザ マニ ュアル』を参照してください。オプション。
- 一時停止またはロックされたポートを含めるには、[一時停止ポート] または [ロック ポート] を選択します。一時停止ポートは、デバイ スの CC-SG 管理が一時停止されると発生します。ロック ポート は、デバイスのアップグレード中に生じます。オプション。
- 5. [表示するエントリ] フィールドで、レポート画面に表示するデータ の行数を選択します。

注: この設定は、レポートをタスクとして生成する場合は適用され ません。

6. [適用] をクリックしてレポートを生成します。

ノード資産レポート

ノード資産レポートには、CC-SG の管理下にあるノードの名前、イン タフェースの名前とタイプ、デバイスの名前とタイプ、すべてのノード のノード グループが表示されます。レポートをフィルタして、指定し たノード グループ、インタフェース タイプ、デバイス タイプ、また はデバイスに対応したノードに関するデータのみを表示することもでき ます。

ノード資産レポートを生成するには、以下の手順に従います。

- 1. [レポート]>[ノード]>[ノード資産レポート]を選択します。
- 2. レポートに適用するフィルタ条件 ([すべてのノード]、[ノード グル ープ]、[デバイス グループ]、または [デバイス]) を選択します。
 - [ノード グループ]、[インタフェース タイプ]、または [デバイス グループ] を選択する場合、対応するメニューからパラメーター を選択します。
 - [デバイス] を選択した場合、レポートに含められるノード資産 に関連するデバイスを [利用可能] リストで選択し、[追加] をク リックして、[選択中] リストに移動します。
- 3. [適用] をクリックしてレポートを生成します。ノード資産レポート が生成されます。
- ノードのブックマーク URL を取得するには、以下の手順に従います。
- ノード資産レポートを生成し、ノードをダブルクリックして詳細ダ イアログを表示します。



- 2. [ファイルに保存] をクリックします。すべてのレポート情報が .csv ファイルに保存されます。
- URL 列には各ノードへの直接リンクがあります。各ノードに個別に ブックマークを設定する代わりに、この情報を使用して各ノードへ のリンクを持つ Web ページを作成できます。「インタフェースをブ ックマークに設定『152p.』」を参照してください。

アクティブ ノード レポート

アクティブ ノード レポートには、アクティブな接続のある各ノードに ついて、各アクティブ インタフェースの名前とタイプ、接続モード、 関連デバイス、タイムスタンプ、現在のユーザ、ユーザ IP アドレスが 表示されます。このレポートからアクティブ ノード リストを表示した り、ノードを切断したりできます。

- アクティブ ノード レポートを生成するには、以下の手順に従います。
- [レポート]>[ノード]>[アクティブ ノード] を選択します。現在ア クティブ ノードがある場合は、アクティブ ノード レポートが生成 されます。
- アクティブ セッションからノードを切断するには、以下の手順に従います。
- アクティブ ノード レポートで、切断するノードを選択し、[切断] をクリックします。

ノード作成レポート

ノード作成レポートには、指定した時間枠内に試みられたノード作成操 作がその成否に関わらずすべてリストされます。ノード作成操作をすべ て表示するか、ノード複製の可能性のあるもののみを表示するかを指定 できます。

ノード作成レポートを生成するには、以下の手順に従います。

- 1. [レポート]>[ノード]>[ノードの作成] を選択します。
- 2. [すべてのノード] または [複製の可能性] を選択します。[複製の可能性] は、レポートを複製の可能性のあるものとしてフラグをつけられたノードのみに限定します。
- [すべてのノード] を選択した場合、[Start Date and Time] (開始日時) フィールドと [End Date and Time] (終了日時) フィールドでレポー トの日付範囲を設定します。デフォルトの日付の各部分 (月、日、 年、時、分、秒) をクリックして選択し、適切な数値になるまで上 下の矢印をクリックします。



- 4. [適用] をクリックします。[ノードの作成レポート] が生成されます
 - [結果] フィールドには、[成功]、[失敗]、または [複製の可能性] が表示され、ノード作成操作の結果を示します。

ノード グループ データ レポート

ノード グループ データ レポートには、各グループに属しているノー ドのリストと各ノード グループにアクセスできるユーザ グループが表 示されます。該当する場合は、ノード グループを定義するルールも表 示されます。ノードのリストは、レポート詳細に含まれています。レポ ート詳細は、レポート ページの行をダブルクリックして表示したり、 CSV ファイルに保存したりできます。「ファイルへのレポートの保存 『233p.』」を参照してください。

ノード資産レポートには、各ノードが属しているグループのリストが表示されます。「ノード資産レポート 『241p. 』」を参照してください。

- ノード グループ データ レポートを生成するには、以下の手順に従います。
- 1. [レポート]>[ユーザ]>[ノード グループ データ] を選択します。
- 行をダブルクリックして、グループ内のノードのリストを表示します。

AD ユーザ グループ レポート

AD ユーザ グループ レポートには、認証と承認の両方に対して設定さ れた AD サーバから CC-SG にインポートされたグループ内のすべて のユーザが表示されます。このレポートには、CC-SG を介してローカ ルで AD ユーザ グループに追加されたユーザは表示されません。

- AD ユーザ グループ レポートを生成するには、以下の手順に従い ます。
- [レポート]> [Active Directory]> [AD ユーザ グループ レポート] を 選択します。
- [AD サーバ] リストには、認証と承認の両方に対して CC-SG で設定されているすべての AD サーバが表示されます。レポートに含める各 AD サーバに対応するチェックボックスを選択します。
- [AD ユーザ グループ] セクションの [利用可能] リストには、[AD サーバ] リストで選択した AD サーバから CC-SG にインポートさ れたすべてのユーザ グループが表示されます。レポートに含めるユ ーザ グループを選択して、[追加] をクリックし、ユーザ グループ を [選択中] リストに移動します。
- 4. [適用] をクリックしてレポートを生成します。



スケジュールされたレポート

スケジュールされたレポートには、タスク マネージャでスケジュール されたレポートが表示されます。[スケジュールされたレポート] 画面に は、デバイス ファームウェアのアップグレード レポートとデバイスの 再起動レポートが表示されます。スケジュールされたレポートは、 HTML 形式でのみ表示できます。「タスク マネージャ 『311p. 』」を 参照してください。

- スケジュールされたレポートにアクセスするには、以下の手順に従います。
- 1. [レポート]>[スケジュールされたレポート]を選択します。
- 2. [レポート タイプ] を選択します。
- 3. [レポートの所有者]を選択します。
- 名前でフィルタするには、レポート名を入力します。完全な名前、 または名前の一部を入力できます。大文字と小文字は区別されません。ワイルドカードは使用できません。
- [開始日付/時刻] フィールドと [終了日付/時刻] フィールドでレポー トの日付範囲を設定します。デフォルトの日付の各部分 (月、日、 年、時、分、秒) をクリックして選択し、適切な数値になるまで上 下の矢印をクリックします。
- 6. [適用] をクリックします。スケジュールされたレポートのリストが 生成されます。
- スケジュールされたレポートを表示するには、以下の手順に従います。
- 1. リストでレポートを選択します。
- 2. [レポートの表示] をクリックします。

注: 監査証跡レポート、エラー ログ レポート、およびアクセスレ ポー トの手動レポートには、レポートのすべてのエントリが表示されます。 一方、スケジュールされたタスクから生成されたレポートには、最大 10,000 行が表示されます。

- スケジュールされたレポートを削除するには、以下の手順に従います。
- 削除するレポートを選択します。Ctrl または Shift を押しながらク リックすると、複数のレポートを選択できます。
- 2. [レポートの削除] をクリックします。
- 3. [はい] をクリックして確認します。



デバイス ファームウェアのアップグレード レポート

デバイス ファームウェアのアップグレード レポートは、[スケジュール されたレポート] リストにあります。このレポートは、デバイス ファー ムウェアのアップグレード タスクが実行されているときに生成されま す。レポートを参照して、タスクに関するリアルタイムのステータス情 報を取得します。タスクが完了すると、レポート情報は静的になります。

レポートの表示の詳細は、「*スケジュールされたレポート* **『244**p. **』**」 を参照してください。



Ch 14 システム メンテナンス

この章の内容

メンテナンス モード	246
メンテナンス モードの起動	247
メンテナンス モードの終了	247
CC-SG のバックアップ	248
バックアップ ファイルの保存および削除	250
CC-SG のリストア	251
CC-SG のリセット	253
CC-SG の再起動	255
CC-SG のアップグレード	256
クラスタのアップグレード	259
CC-SG データベースのマイグレーション	
CC-SG のシャットダウン	262
CC-SG のシャットダウン後の再起動	
CC-SG の電源切断	
CC-SG セッションの終了	263

メンテナンス モード

メンテナンス モードでは、CC-SG へのアクセスが制限され、管理者が 中断なく操作を行えるようになります。メンテナンス モードで実行す るのが最適な操作の例として、休止タイマーの変更、CC-SG のバック アップなどがあります。メンテナンス モードでは、休止タイマーなど のシステム全体の設定は、すべてのユーザに対して変更されます。

メンテナンス モードを起動した管理者以外の現在オンラインのユーザ には、警告が表示され、指定の時間を過ぎるとログアウトされます。メ ンテナンス モードの間は、他の管理者は CC-SG にログインできます が、管理者以外のユーザはログインが禁止されます。CC-SG のメンテ ナンス モードが開始するときと終了するときに、SNMP トラップが生 成されます。

注 1: メンテナンス モードは、クラスタ設定にないスタンドアロンの CC-SG ユニットでのみ利用可能です。

注 2: メンテナンス モードになるまで、CC-SG のアップグレードは行 えません。



予定タスクとメンテナンス モード

CC-SG がメンテナンス モードになっている間は、予定タスクは実行で きません。「タスク マネージャ『311p. 』」を参照してください。CC-SG のメンテナンス モードが終了すると、その直後に予定タスクが実行さ れます。

メンテナンス モードの起動

- [システム メンテナンス]>[メンテナンス モード]>[メンテナンス モードの起動] を選択します。
- 2. パスワード: パスワードを入力します。CC の設定と制御権限を持 つユーザだけが、メンテナンス モードを起動できます。
- 3. [ブロードキャスト メッセージ]: CC-SG からログアウトするユーザ に表示されるメッセージを入力します。
- メンテナンス モード起動までの時間 (分): CC-SG がメンテナンス モードになるまでに経過する必要がある時間を分単位 (0 ~ 720) で入力します。0 と入力すると、すぐにメンテナンス モードになり ます。

10 分より長い時間を指定すると、ブロードキャスト メッセージが 即座にユーザに表示され、その後、イベント発生の **10** 分前および **5** 分前に、メッセージが再表示されます。

- 5. [OK] をクリックします。
- 6. 確認のダイアログ ボックスで [OK] をクリックします。

メンテナンス モードの終了

- [システム メンテナンス]>[メンテナンス モード]>[メンテナンス モードの終了]を選択します。
- 2. [OK] をクリックして、メンテナンス モードを終了します。
- 3. CC-SG でメンテナンス モードが終了するとメッセージが表示され ます。これですべてのユーザが CC-SG に通常通りアクセスできる ようになります。



CC-SG のバックアップ

CC-SG をバックアップする場合、メンテナンス モードを起動するよう にお勧めします。メンテナンス モードを起動すると、バックアップ中 にデータベースに変更が加えられることがなくなります。

最大 50 個のバックアップ ファイルを CC-SG に保存できます。バッ クアップ ファイルの数が 50 個に到達すると、古いバックアップ ファ イルを CC-SG から削除するまでは新しいバックアップを作成できませ ん。「バックアップ ファイルの保存および削除 『250p. 』」を参照し てください。

- CC-SG をバックアップするには、以下の手順に従います。
- 1. [システム メンテナンス]>[バックアップ] を選択します。
- 2. このバックアップの名前を [バックアップ名] フィールドに入力しま す。
- 3. このバックアップの説明を [説明] フィールドに入力します。オプション。
- バックアップ タイプを選択します。[完全] または [標準] の中から 選択できます。「*完全バックアップと標準バックアップの違いは何で すか。*『250p.』」を参照してください。
- 5. このバックアップ ファイルのコピーを外部サーバに保存するには、 [リモート環境にバックアップ] チェックボックスを選択します。オ プション。
 - a. リモート サーバに接続するためのプロトコル (FTP または SFTP のいずれか)を選択します。
 - b. サーバの IP アドレスまたはホスト名を [IP アドレス/ホスト名] フィールドに入力します。
 - c. 選択したプロトコルにデフォルトのポート (FTP: 21、SFTP:
 22) を使用しない場合は、使用する通信ポートを [ポート番号] フィールドに入力します。
 - d. リモート サーバのユーザ名を [ユーザ名] フィールドに入力し ます。
 - e. リモート サーバのパスワードを [パスワード] フィールドに入 力します。
 - f. [Directory (Relative Path) (ディレクトリ (相対パス))] フィール ドで、FTP サーバ上でバックアップを保存するための場所を指 定します。



- バックアップ ファイルを FTP サーバ上のデフォルト ホーム ディレクトリに保存する場合は、このフィールドを空白のままにします。
- バックアップ ファイルを FTP サーバ上のデフォルト ホーム ディレクトリより下位のレベルに保存する場合は、デフォルト ホーム ディレクトリからの相対パスを入力します。たとえば、バックアップ ファイルをデフォルト ホームディレクトリの下にある "Backups" という名前のフォルダに保存するには、[Directory (Relative Path) (ディレクトリ (相対パス))] フィールドに「Backups」と入力します。
- g. [ファイル名 (デフォルトのファイル名規則を使用する場合は空 欄にしてください)] フィールドに、リモート サーバ上のバック アップのファイル名を入力します。デフォルト名をそのまま使 用する場合は空白のままにします。デフォルト名は、"backup" の後に日時が付加された名前になります。
- h. 現在のリモート サーバの設定をデフォルト値として保存する場合は、[デフォルトとして保存] をクリックします。確認メッセ ージが表示されます。[OK] をクリックします。オプション。
- 6. [OK] をクリックします。
 - バックアップが完了すると、メッセージが表示されます。バックア ップ ファイルは CC-SG ファイル システムに保存され、また [リ モート環境にバックアップ] フィールドで指定した場合は、リモー ト サーバにも保存されます。このバックアップは、後でリストアで きます。「CC-SG のリストア『251p.』」を参照してください。

重要: 隣接システムの設定は、CC-SG バックアップ ファイルに含まれ るので、バックアップ時に設定を覚えておくか書き留めておいてくださ い。これは、リストアする CC-SG ユニットでそのバックアップ ファイ ルが適切かどうかを判断するときに役立ちます。



完全バックアップと標準バックアップの違いは何ですか。

▶ 標準バックアップ:

標準バックアップには、すべての CCSG ページにあるすべてのフィー ルドのデータがすべて含まれます。ただし、次のページのデータを除き ます。

- [管理]>[設定マネージャ]>[ネットワーク] タブ
- [管理] > [クラスタ設定]

CCSG に保存されている CCSG バックアップ ファイルもバックアッ プされません。CCSG に保存されているバックアップ ファイルのリス トは、[システム メンテナンス]>[リストア] ページで確認できます。 標準バックアップでは、レポート ページの日付範囲などのフィールド にあるその他の一時データも除外されます。

▶ 完全バックアップ:

完全バックアップでは、標準バックアップのすべてのデータと、CC-SG ファームウェア ファイル、デバイス ファームウェア ファイル、アプ リケーション ファイル、およびログもバックアップされます。アプリ ケーション ファイルには、RRC、MPC、RC、および VNC が含まれ ます。

バックアップ ファイルの保存および削除

[CommandCenter のリストア] 画面を使用すると、CC-SG にバックア ップを保存したり、保存されたバックアップを削除したりできます。バ ックアップを保存すると、別の PC にバックアップのコピーを保持でき ます。バックアップ ファイルのアーカイブを作成できます。別の場所 に保存されたバックアップ ファイルを他の CC-SG ユニットにアップ ロードした後、リストアして設定を CC-SG 相互間でコピーすることが できます。

必要のないバックアップを削除すると、CC-SG 上の領域を節約できます。

バックアップ ファイルの保存

- [システム メンテナンス]>[CommandCenter のリストア] を選択し ます。
- 2. PC に保存するバックアップを [利用可能なバックアップ] テーブル から選択します。
- 3. [ファイルに保存] をクリックします [保存] ダイアログが表示されま す。
- 4. ファイルの名前を入力し、保存する場所を選択します。



5. [保存] をクリックして、バックアップ ファイルを指定の場所にコピーします。

バックアップ ファイルの削除

- 1. 削除するバックアップを [利用可能なバックアップ] テーブルから選 択します。
- 2. [削除] をクリックします。確認のダイアログが表示されます。
- 3. [OK] をクリックして、CC-SG システムからバックアップを削除し ます。

CC-SG のリストア

作成したバックアップ ファイルを使用して、CC-SG をリストアできます。

重要: 隣接システムの設定は、CC-SG バックアップ ファイルに含まれ るので、バックアップ時に設定を覚えておくか書き留めておいてくださ い。これは、リストアする CC-SG ユニットでそのバックアップ ファイ ルが適切かどうかを判断するときに役立ちます。

- CC-SG をリストアするには、以下の手順に従います。
- [システム メンテナンス]>[リストア] を選択します。
 [CommandCenter のリストア] ページが開き、CC-SG で使用可能 なバックアップ ファイルのリストが表示されます。バックアップの タイプ、バックアップ日付、説明、バックアップが行われた CC-SG のバージョン、およびバックアップ ファイルのサイズが表 示されます。
- CC-SG システムの外部に保存されたバックアップからリストアする場合、まずバックアップファイルを CC-SG にアップロードする必要があります。オプション。
 - a. [アップロード] をクリックします。
 - b. バックアップ ファイルを検索して、ダイアログ ウィンドウで 選択します。クライアントのネットワークのどこからでもファ イルを取得できます。
 - c. [開く] をクリックして、このファイルを CC-SG にアップロードします。完了すると、バックアップ ファイルが [利用可能なバックアップ] テーブルに表示されます。
- 3. リストアするバックアップ ファイルを [利用可能なバックアップ] テーブルで選択します。
- **4.** 可能な場合、このバックアップから実行するリストア タイプを次の 中から選択します。



- 標準 重要なデータのみが CC-SG にリストアされます。この 場合、CC-SG 設定情報、デバイスとノードの設定、およびユー ザ設定がリストアされます。「*完全バックアップと標準バックア ップの違いは何ですか。*『250p.』」を参照してください。
- 完全 バックアップ ファイルに保存されているすべてのデータ、ログ、ファームウェア、アプリケーション ファイル、およびライセンス ファイルがリストアされます。「完全バックアップと標準バックアップの違いは何ですか。『250p.』」を参照してください。この場合、ファイルの完全バックアップを行っておく必要があります。利用可能な完全バックアップを確認するには、[利用可能なバックアップ]テーブルの [タイプ] 列を参照します。
- カスタム CC-SG にリストアするバックアップのコンポーネ ントを指定できます。その場合、[リストア オプション] 領域で そのコンポーネントを選択します。次に示すものをリストアす る場合は、それぞれを選択します。
 - データのリストア CC-SG 設定、デバイスとノードの設定 、およびユーザ データデータを選択すると、完全バックア ップ ファイルの標準バックアップ部分がリストアされます 。「*完全バックアップと標準バックアップの違いは何ですか* 。『250p.』」を参照してください。
 - ログのリストア CC-SG に保存されているエラー ログお よびイベント レポート
 - CC ファームウェアのリストア CC-SG サーバ自体を更新 するための保存ファームウェア ファイル
 - ファームウェアのバイナリ ファイルをリストア CC-SG によって管理される Raritan デバイスを更新するための保 存ファームウェア ファイル
 - アプリケーションのリストア ユーザをノードに接続する ために CC-SG によって使用される保存アプリケーション
 - Restore Licenses(ライセンスのリストア) CC-SG 機能およびノードへのアクセスを可能にする保存ライセンスファイル。「使用可能なライセンス『13p.』」を参照してください。
- 5. CC-SG でリストア操作が開始されるまでの時間 (0 ~ 60 分) を [リストア開始までの時間] フィールドに入力します。これにより、 ユーザは作業を完了し、ログアウトするまでの時間を確保できます。

10 分より長い時間を指定すると、ブロードキャスト メッセージが 即座にユーザに表示され、その後、イベント発生の 10 分前および 5 分前に、メッセージが再表示されます。



- 6. リストアが実行されることを CC-SG の他のユーザに知らせるため のメッセージを [ブロードキャスト メッセージ] フィールドに入力 します。
- [リストア] をクリックします。CC-SG は、指定された時間待って から、選択されたバックアップから設定をリストアします。リスト アが実行される際には、他のすべてのユーザがログアウトされます。
 バックアップ ファイルが破損している場合は、メッセージが表示さ

ハックアップ ファイルか破損している場合は、メッセーンが表示され、監査証跡に書き込まれます。破損したバックアップ ファイルは CC-SG のリストアに使用できません。

CC-SG のリセット

CC-SG をリセットすると、データベースを消去したり、他のコンポー ネントを工場出荷時のデフォルト設定にリセットしたりできます。リセ ット オプションを使用する前に、必ずバックアップを実行して、バッ クアップ ファイルを別の場所に保存してください。

選択済みのデフォルト オプションを使用するようにお勧めします。

注: CC-SG ユニットに保存されている CC-SG バックアップ ファイル は、CC-SG をリセットしても削除されません。CC-SG から CC-SG バックアップ ファイルを削除するには、各ファイルを手動で削除する 必要があります。「バックアップ ファイルの保存および削除 『250p. 』 」を参照してください。

オプション	説明
フル データベース	このオプションの場合、既存の CC-SG データベースが削除され、工場出荷時のデフォルト値で新しいバージョンが作成されます。ネットワーク設定、SNMP エージェント、ファームウェア、診断コンソール設定は、CC-SG データベースの一部ではありません。
	SNMP の設定とトラップはリセットされます。SNMP エージェ ントはリセットされません。
	IP-ACL 設定は、IP ACL テーブル オプションの選択の有無に関 わらず、フル データベース リセット操作でリセットされます。
	リセットにより隣接システムの設定が削除されるので、隣接システムのメンバだったとしても、CC-SG ではその記憶が失われます。
	データベースが削除されると、すべてのデバイス、ノード、ユー ザが削除されます。すべてのリモート認証および承認サーバが削 除されます。
	CC スーパー ユーザ アカウントは、デフォルトにリセットされ ます。リセット操作の完了後、デフォルトのユーザ名とパスワー



Ch 14: システム メンテナンス

オプション	説明
	ド admin/raritan を使ってログインする必要があります。
パーソナリティ設定の保存	このオプションは、フル CC-SG データベース リセットを選択 する場合にのみ選択できます。 このオプションでは、 CC-SG データベースが再作成されるとき
	に、前に設定された一部のオプションが保存されます。 - 強力なパスロードが強制されます
	 ・ 強力なパスシートが強制されより。 ・ アウト オブ バンド ノードへの直接接続とプロキシ接続。
	■ 休止タイマーの設定。
ネットワーク設定	このオプションでは、ネットワーク設定が工場出荷時のデフォル ト値に戻ります。
	■ ホスト名: CommandCenter
	 ドメイン名: localdomain
	■ モード: IP フェイルオーバ
	 設定:静的
	■ IP アドレス: 192.168.0.192
	 ネットマスク: 255.255.0 ビーレウーズ・カリ
	$ \begin{array}{c} & \mathcal{I} = \mathcal{I} =$
	 アダプタ速度: 自動
SNMP 設定	このオプションでは、SNMP 設定が工場出荷時のデフォルト値 に戻ります。
	 ポート: 161
	 読み取り専用コミュニティ: public
	■ 読み書きコミュニティ: private
	 システム連絡先の名前と場所:なし
	 SNMP トラップ構成
	 SNMP トラップ送信先
デフォルト ファームウェ ア	このオプションでは、すべてのデバイス ファームウェア ファイ ルが工場出荷時のデフォルト値にリセットされます。このオプシ ョンでは、CC-SG データベースは変更されません。
リセット後にファームウェ アをデータベースにアップ ロード	このオプションでは、現在の CC-SG バージョンのファームウ ェア ファイルが CC-SG データベースにロードされます。
診断コンソール	このオプションでは、診断コンソール設定が工場出荷時のデフォ ルト値に戻ります。



オプション	説明
IP-ACL テーブル	このオプションでは、IP-ACL テーブルからすべてのエントリが 削除されます。
	IP-ACL 設定は、IP ACL テーブル オプションの選択の有無に関わらず、フル データベース リセット操作でリセットされます。
ライセンス	このオプションでは、 CC-SG からのすべてのライセンス ファ イルが削除されます。

- CC-SG をリセットするには、以下の手順に従います。
- リセット前に、CC-SG をバックアップして、バックアップ ファイ ルをリモートの場所に保存してください。「CC-SG のバックアップ 『248p. 』」を参照してください。
- 2. [システム メンテナンス]>[リセット] を選択します。
- 3. リセット オプションを選択します。
- 4. CC-SG のパスワードを入力します。
- 5. [ブロードキャスト メッセージ]: CC-SG からログオフするユーザに 表示されるメッセージを入力します。
- 6. CC-SG でリセット操作を実行するまでに経過する必要がある時間 を分単位 (0 ~ 30) で入力します。
 10 分より長い時間を指定すると、ブロードキャスト メッセージが 即座にユーザに表示され、その後、イベント発生の 10 分前および 5 分前に、メッセージが再表示されます。
- 7. [OK] をクリックします。リセットを確認するメッセージが表示され ます。

リセット中に CC-SG の電源オフ、電源オン・オフ、または中断操作 をしないでください。これらを実行すると、CC-SG データが失われ る恐れがあります。

CC-SG の再起動

CC-SG ソフトウェアを再起動するには、再起動コマンドを使用します 。**CC-SG** を再起動すると、すべてのアクティブ ユーザが **CC-SG** から ログアウトされます。

再起動しても、CC-SG への電源は再投入されません。完全なリブート を実行するには、診断コンソールにアクセスするか、CC-SG ユニット の電源スイッチをオンにする必要があります。

- 1. [システム メンテナンス]>[再起動] を選択します。
- 2. [パスワード] フィールドにパスワードを入力します。



- [ブロードキャスト メッセージ]: デフォルト メッセージを使用する か、それを編集します。メッセージは、CC-SG からログオフする ユーザに表示されます。
- 4. [再起動までの時間 (分)]: CC-SG が再起動するまでに経過する必要がある時間を分単位 (0 ~ 720) で入力します。
 10 分より長い時間を指定すると、ブロードキャスト メッセージが 即座にユーザに表示され、その後、イベント発生の 10 分前および 5 分前に、メッセージが再表示されます。
- 5. [OK] をクリックして CC-SG を再起動します。

CC-SG のアップグレード

新しいバージョンがリリースされたら、CC-SG のファームウェアをア ップグレードできます。ファームウェア ファイルは、Raritan の Web サイトのサポート セクションにあります。CC-SG をバージョン 3.x からバージョン 4.1 にアップグレードする場合は、まず、4.0 にアップ グレードする必要があります。CC-SG をバージョン 4.x から 5.0 より 上のバージョンにアップグレードする場合は、まず、5.0 にアップグレ ードする必要があります。

CC-SG バージョン 4.0 以降は、G1 ハードウェアと互換性がありま せん。CC-SG G1 ユニットをバージョン 4.0 またはそれ以降にアッ プグレードしないでください。

アップグレードを始める前に、クライアント PC にファームウェア フ ァイルをダウンロードします。

CC の設定と制御権限を持つユーザだけが、**CC-SG** をアップグレード できます。

アップグレードの前に、CC-SG をバックアップし、そのバックアップ ファイルを PC に送信して保管する必要があります。「CC-SG のバッ クアップ『248p.』」および「バックアップ ファイルの保存『250p.』 」を参照してください。

CC-SG クラスタを操作している場合は、クラスタを削除してから、ア ップグレードする必要があります。各 CC-SG ノードを個別にアップグ レードしてから、クラスタを再作成してください。

重要: **CC-SG** とデバイスまたはデバイスのグループの両方をアップグレードする必要がある場合は、まず **CC-SG** のアップグレードを実行してから、デバイスのアップグレードを実行してください。

アップグレード プロセスの一部として **CC-SG** がリブートします。アッ プグレード中に、プロセスの停止、ユニットの手動リブート、ユニット の電源オフまたは電源の再投入を行わないでください。



- CC-SG をアップグレードするには、以下の手順に従います。
- 1. クライアント PC にファームウェア ファイルをダウンロードしま す。
- 2. CC の設定と制御権限を持つアカウントによって CC-SG Admin Client にログインします。
- メンテナンス モードを起動します。「メンテナンス モードの起動 『247p. 』」を参照してください。
- CC-SG がメンテナンス モードになったら、[システム メンテナンス]>[アップグレード] を選択します。
- 5. [参照] をクリックします。CC-SG ファームウェア ファイル (.zip) を表示して選択し、[開く] をクリックします。
- [OK] をクリックして、このファームウェア ファイルを CC-SG に アップロードします。
 ファームウェアが CC-SG にアップロードされたら、CC-SG がア ップグレード プロセスを開始したことを示す成功メッセージが表示 されます。この時点ですべてのユーザが CC-SG から切断されます。
- アップグレードが完了するのを待ってから、再度 CC-SG にログインする必要があります。アップグレード状況は、診断コンソールで 監視できます。
 - a. admin アカウントを使用して、診断コンソールにアクセスします。「Administrator Console へのアクセス 『340p. 』」を参照してください。
 - b. [Admin] > [System Logfile Viewer] (システム ログ ファイル ビューア) を選択します。sg/upgrade.log を選択して、[View] (表示) を選択し、アップグレード ログを表示します。
 - アップグレード プロセスの完了を待ちます。アップグレード プロセスが完了すると、アップグレード ログに「アップグレー ド完了」メッセージが表示されます。または、SNMP トラップ cclmageUpgradeResults が「成功」メッセージとともに表示さ れるまで待ちます。
 - d. サーバをリブートする必要があります。リブート プロセスが開始すると、アップグレード ログに「Linux リブート」メッセージが表示されます。サーバがシャットダウンし、リブートします。

注: CC-SG 3.x から 4.0.x へのアップグレードの場合、システムは 2 回リブートします。これは、想定された正常な動作です。

- e. リブートしてから約 2 分で、admin アカウントを使用して診断 コンソールに再アクセスし、アップグレード プロセスの進行状 況を監視できるようになります。オプション。
- 8. [OK] をクリックして CC-SG を終了します。



- ブラウザ キャッシュをクリアして、ブラウザ ウィンドウを閉じます。「ブラウザ キャッシュのクリア 『258p. 』」を参照してください。
- Java キャッシュをクリアします。「Java キャッシュのクリア 『
 258p. 』」を参照してください。
- 11. 新しい Web ブラウザ ウィンドウを起動します。
- **12. CC** の設定と制御権限を持つアカウントによって **CC-SG Admin Client** にログインします。
- 13. [ヘルプ] > [バージョン情報] を選択します。バージョン番号を確認 して、アップグレードが成功したかを確認します。
 - バージョンがアップグレードされていない場合、ここまでの手順を繰り返します。
 - アップグレードが成功した場合、次の手順に進みます。
- 14. メンテナンス モードの終了。「メンテナンス モードの終了『247p. 』」を参照してください。
- 15. CC-SG をバックアップします。「CC-SG のバックアップ『248p. 』 」を参照してください。

ブラウザ キャッシュのクリア

この手順は、ブラウザのバージョンによって若干異なります。

- Internet Explorer でブラウザ キャッシュをクリアするには、以下の手順に従います。
- 1. [ツール]>[インターネット オプション] を選択します。
- 2. [全般] タブで、[ファイルの削除] をクリックして、[OK] をクリック して確認します。
- FireFox 2.0 および 3.0 の場合の手順:
- 1. [ツール]>[プライバシー情報の消去]を選択します。
- 2. [キャッシュ] が選択されていることを確認して、[今すぐ消去] をク リックします。

Java キャッシュのクリア

Java のバージョンおよびオペレーティング システムの種類によっては、手順が若干異なる場合があります。

🕨 Java 1.6 搭載 Windows XP の場合:

- 1. [コントロール パネル] > [Java] を選択します。
- 2. [全般] タブで [設定] をクリックします。



- 3. 開いたダイアログ ボックスで [ファイルの削除] をクリックします
- [アプリケーション] および [アプレット] チェックボックスが選択されていることを確認して、[OK] をクリックします。

クラスタのアップグレード

CC-SG クラスタをアップグレードするには、この推奨アップグレード 手順に従います。クラスタに構成できるのは、物理 **CC-SG** ユニットの みです。

CC-SG クラスタ ライセンスは、クラスタ内の 2 つの CC-SG ユニットで共有できる特別な種類のライセンス ファイルです。詳細については、「クラスタ ライセンス 『292p. 』」を参照してください。

この手順の実行時にプライマリ ノードのアップグレードが失敗した場合、「プライマリ ノードのアップグレード エラー 『260p. 』」を参照 してください。

- クラスタをアップグレードするには、以下の手順に従います。
- [管理]>[クラスタ設定]を選択して、プライマリ ノードからバック アップ ノードに強制的にフェイルオーバします。[設定] タブで、[プライマリとバックアップを切り替えます] をクリックします。詳 細は、「プライマリ ノードとセカンダリ ノードのステータスの切り 替え 『290p. 』」を参照してください。
 - バックアップ ノードがプライマリになります。それまでのプラ イマリ ノードは待機ステータスになります。
- 新しいプライマリ ノードで、[システム メンテナンス]>[シャット ダウン] を選択して、CC-SG アプリケーションをシャットダウンし ます。
 - CC-SG アプリケーションをシャットダウンする場合、ユニットの電源はオンのままのため、診断コンソールからアクセスできます。詳細は、「CC-SG のシャットダウン『262p.』」を参照してください。
- 待機ステータスになっている、以前のプライマリ ノードを再起動し ます。再起動の詳細は、「診断コンソールを使用した CC-SG の再 起動 『354p. 』」を参照してください。
 - 再起動した CC-SG ユニットは、再びプライマリ ステータスに なります。シャットダウンしたバックアップ ノードは失敗ステ ータスと見なされます。
- [管理] > [クラスタ設定] を選択してクラスタを削除します。[Delete Cluster (クラスタの削除)] をクリックします。
- メンテナンス モードに切り替え、プライマリ ノードをアップグレ ードします。「メンテナンス モードの起動 『247p. 』」および「 CC-SG のアップグレード 『256p. 』」を参照してください。



- プライマリ ノードをアップグレードできたら、診断コンソールにア クセスし、[Operation(操作)] > [Admin(管理)] > [Factory Reset(工場 出荷時リセット)] > [Full CC-SG DatabaseReset(CC-SG データベー スの完全リセット)] オプションを選択して、バックアップ ノードを 工場出荷時設定にリセットします。「CC-SG 工場出荷時設定へのリ セット 『357p. 』」を参照してください。
 - プライマリ ノードのアップグレードに失敗した場合は、「プラ イマリ ノードのアップグレード エラー 『260p. 』」を参照し てください。
- リセットしたバックアップ ノードをアップグレードします。「
 CC-SG のアップグレード 『256p. 』」を参照してください。
- 8. クラスタを再作成します。「**クラスタの作成『288**p.**』**」を参照してください。プライマリノードのデータがバックアップノードと同期されます。

プライマリ ノードのアップグレード エラー

「クラスタのアップグレード『259p.』」の手順に従ったプライマリノードのアップグレードが失敗した場合は、以下の手順に従ってクラスタのアップグレードを完了します。

- プライマリ ノードのアップグレードが失敗した場合は、[システム メンテナンス]>[シャットダウン] を選択して、CC-SG アプリケー ションをシャットダウンします。CC-SG アプリケーションをシャ ットダウンする場合、ユニットの電源はオンのままのため、診断コ ンソールからアクセスできます。詳細は、「CC-SG のシャットダウ ン『262p.』」を参照してください。
- 2. バックアップ ノードを再起動します。再起動の詳細は、「*診断コン* ソールを使用した CC-SG の再起動 『354p. 』」を参照してください。
- 3. バックアップ ノードがプライマリ ステータスになります。
- ラリタン社のテクニカル サポートに連絡して、アップグレードが失敗した理由を特定します。

CC-SG データベースのマイグレーション

物理 CC-SG ユニットを新しいものと交換するか、物理 CC-SG ユニットから仮想 CC-SG に移行するには、以下の推奨マイグレーション手順に従います。



マイグレーションの要件

- 両方の CC-SG ユニットは、ファームウェアのバージョンが同じで、バージョン 5.1 以降であることが必要です。
- マイグレーション後の CC-SG が完全に機能するためには、データ ベースのマイグレーション先の CC-SG で有効なライセンスが必要 です。

CC-SG データベースのマイグレーション

- CC-SG データベースをマイグレーションするには、以下の手順に 従います。
- すべてのデバイスの管理を一時停止します。オプションとして、 CC-SG ファームウェア バージョン 5.1 以降を使用している場合は 、すべてのデバイスを一時停止するタスクをスケジュールできます 。「タスクのスケジュール 『313p. 』」を参照してください。
- マイグレーション元の CC-SG の完全バックアップを実行します。[バックアップ タイプ] で [完全] を選択していることを確認し、リ モートの場所にバックアップ ファイルを保存します。「CC-SG の バックアップ 『248p. 』」を参照してください。
- 3. マイグレーション元の CC-SG で、[システム メンテナンス]>[シ ャットダウン] を選択して、CC-SG アプリケーションをシャットダ ウンします。
- マイグレーション先の CC-SG で、完全バックアップ ファイルを アップロードし、完全リストアを実行します。[リストア タイプ] で [完全] を選択していることを確認します。「CC-SG のリストア 『 251p. 』」を参照してください。

注:移行先の CC-SG を完全に機能させるには、それ自体の有効な ライセンスが必要です。完全リストアの実行には、有効なライセン スは不要です。

- すべてのデバイスの管理を再開します。CC-SG ファームウェア バージョン 5.1 以降を使用している場合は、すべてのデバイスを再開するタスクをスケジュールできます。「タスクのスケジュール『 313p.』」を参照してください。
- 6. デバイス可用性レポートを実行して、管理対象デバイスのステータ スを確認します。「*可用性レポート* 『237p. 』」を参照してくださ い。



 新しい CC-SG が正常に実行されたら、マイグレーション元の CC-SG のデータベースをリセットします。これは、何らかの事情 で両方がオンラインになったときに競合が発生しないようにするた めです。データベースをリセットするには、診断コンソールにアク セスし、[Operation(操作)] > [Admin(管理)] > [Factory Reset(工場出 荷時リセット)] > [Full CC-SG Database Reset(CC-SG データベー スの完全リセット)] オプションを選択します。「CC-SG 工場出荷時 設定へのリセット 『357p. 』」を参照してください。

CC-SG のシャットダウン

CC-SG をシャットダウンすると、CC-SG ソフトウェアがシャットダウンされますが、CC-SG ユニットの電源はオフになりません。

CC-SG がシャットダウンすると、すべてのユーザがログアウトされま す。**CC-SG** を再起動するまでは、ユーザは診断コンソールを使用して も、**CC-SG** の電源を再投入しても、再度ログインできません。

CC-SG をシャットダウンする場合:

- 1. [システム メンテナンス]>[シャットダウン] を選択します。
- 2. [パスワード] フィールドにパスワードを入力します。
- [ブロードキャスト メッセージ] フィールドで、デフォルトのメッセ ージを受け入れるか、現在オンラインのユーザに向けて表示するメ ッセージを入力します (たとえば、指定した短い時間内に CC-SG のタスクを完了するようにユーザに指示し、システムがいつ再開す るかを通知します)。CC-SG をシャットダウンすると、すべてのユ ーザが切断されます。
- 4. CC-SG でシャットダウンが開始されるまでの時間 (0 ~ 720 分) を [シャットダウンまでの時間 (分)] フィールドに入力します。
 10 分より長い時間を指定すると、ブロードキャスト メッセージが 即座にユーザに表示され、その後、イベント発生の 10 分前および 5 分前に、メッセージが再表示されます。
- 5. [OK] をクリックして CC-SG をシャットダウンします。

CC-SG のシャットダウン後の再起動

CC-SG をシャットダウンしたら、次の 2 つの方法のいずれかによりユ ニットを再起動します。

- 診断コンソールを使用します。「診断コンソールを使用した CC-SG の再起動 『354p. 』」を参照してください。
- CC-SG ユニットの電源を再投入します。



CC-SG の電源切断

CC-SG の実行中に AC 電源が切断した場合、CC-SG では最後の電源 ステータスが記憶されます。AC 電源が復旧すると、CC-SG は自動的 に再起動します。ただし、CC-SG の電源がオフの状態で AC 電源が切 断されると、AC 電源が復旧しても CC-SG の電源はオフのままとなり ます。

重要: CC-SG の電源を強制的に切断するために電源ボタンを押し続けな いでください。CC-SG の電源をオフにする場合は、診断コンソールの [CC-SG System Power OFF] コマンドを使用することを推奨します。 「*診断コンソールからの CC-SG システムの電源オフ* **『355**p. **』」を参** 照してください。

▶ CC-SG の電源をオフにするには、以下の手順に従います。

- 1. ベゼルを外して、電源ボタンを強く押します。
- 2. 正常に CC-SG の電源がオフになるまで、約 1 分待ちます。

注: CC-SG ユニットの電源を切断すると、CC-SG にログインした ユーザは診断コンソールで短いブロードキャスト メッセージを受け 取ります。CC-SG ユニットの電源を切断しても、Web ブラウザま たは SSH で CC-SG にログインしたユーザはメッセージを受け取 りません。

 AC 電源コードを取り外す必要がある場合は、電源を完全にオフに してから、電源コードを外してください。電源を取り外す場合には 、CC-SG のすべてのトランザクションを終了し、データベースを 閉じて、ディスク ドライブを安全な状態にすることが必要です。

CC-SG セッションの終了

CC-SG セッションを終了する方法は 2 つあります。

- クライアント ウィンドウを開いたままにしてセッションを終了する には、ログアウトします。「CC-SG からのログアウト 『263p. の "CC-SG のログアウト"参照 』」を参照してください。
- セッションを終了してクライアントウィンドウを閉じるには、終了します。「CC-SG の終了 『264p. 』」を参照してください。

CC-SG のログアウト

- [Secure Gateway] > [ログアウト] を選択します。[ログアウト] ウィンドウが開きます。
- 2. CC-SG からログアウトするには [はい] をクリックします。ログア ウトすると、CC-SG ログイン ウィンドウが開きます。



CC-SG の終了

- 1. [Secure Gateway] > [終了] を選択します。
- 2. CC-SG を終了するには [はい] をクリックします。



Ch 15 高度な管理

この章の内容

今日のメッセージの設定	265
ノードにアクセスするためのアプリケーションの設定	266
デフォルトのアプリケーションの設定	269
デバイス ファームウェアの管理	270
CC-SG ネットワークの設定	271
ログ アクティビティの設定	278
CC-SG サーバ時間および時刻の設定	279
接続モード:ダイレクトおよびプロキシ	280
デバイス設定	281
カスタム JRE 設定の定義	284
SNMP の設定	
CC-SG クラスタの設定	287
隣接システムの設定	293
セキュリティ マネージャ	298
通知マネージャ	310
タスク マネージャ	311
CC-SG への SSH アクセス	319
シリアル管理ポート	328
Web サービス API	329
CC-NOC	331

今日のメッセージの設定

今日のメッセージ機能によって、すべてのユーザのログオン時に表示されるメッセージを作成できます。今日のメッセージを設定するには、 CC の設定と制御権限が必要です。

- 今日のメッセージを設定するには、以下の手順に従います。
- 1. [管理] > [今日のメッセージの設定] を選択します。
- ログイン後にすべてのユーザに今日のメッセージを表示する場合は、 (今日のメッセージをすべてのユーザに表示] チェックボックスを 選択します。オプション。
- CC-SG にメッセージを入力する場合は [今日のメッセージの内容] チェックボックスを、既存のファイルからメッセージをロードする 場合は [今日のメッセージ ファイル] チェックボックスを選択しま す。
 - [今日のメッセージの内容]を選択した場合は、以下の手順に従います。



- a. 表示されているダイアログ ボックスにメッセージを入力します。
- b. [フォント名] ドロップダウン メニューをクリックして、メッセ ージに使用するフォントを選択します。
- C. [フォント サイズ] ドロップダウン メニューをクリックして、 メッセージに使用するフォント サイズを選択します。
- [今日のメッセージ ファイル]を選択した場合は、以下の手順に 従います。
- a. [参照] をクリックして、メッセージ ファイルを検索します。
- b. 開いたダイアログ ウィンドウでファイルを選択し、[開く] をク リックします。
- c. [プレビュー] をクリックして、ファイルの内容を確認します。
- 4. [OK] をクリックして変更を保存します。

ノードにアクセスするためのアプリケーションの設定

ノードにアクセスするためのアプリケーションについて

CC-SG には、ノードへのアクセスに使用可能なさまざまなアプリケー ションが用意されています。アプリケーション マネージャを使用する と、アプリケーションの表示、新しいアプリケーションの追加、アプリ ケーションの削除、各デバイス タイプのデフォルト アプリケーション の設定を行うことができます。

- CC-SG で使用可能なアプリケーションを参照するには、以下の手順に従います。
- 1. [管理]>[アプリケーション]を選択します。
- [アプリケーション名] ドロップダウン矢印をクリックし、CC-SG で使用可能なアプリケーションのリストを表示します。

アプリケーション バージョンの確認とアップグレード

Raritan Console (RC) や Raritan Remote Client (RRC) などの CC-SG アプリケーションを確認およびアップグレードします。

- アプリケーション バージョンを確認するには、以下の手順に従います。
- 1. [管理]>[アプリケーション]を選択します。
- リストからアプリケーション名を選択します。[バージョン] フィー ルドの番号を確認してください。一部のアプリケーションは、バー ジョン番号が自動的に表示されません。



アプリケーションをアップグレードするには、以下の手順に従います。

アプリケーションのバージョンが最新でない場合は、アプリケーション をアップグレードする必要があります。アプリケーション アップグレ ード ファイルは、Raritan の Web サイトからダウンロードできます。 サポートされるアプリケーションのバージョンをまとめたリストが必要 な場合は、Raritan のサポート Web サイトで互換表を参照してください。

アプリケーションをアップグレードする前に、メンテナンス モードで 起動することをお勧めします。「メンテナンス モードの起動 『247p. 』 」を参照してください。

- 1. クライアント PC にアプリケーション ファイルを保存します。
- [アプリケーション名] ドロップダウン矢印をクリックし、アップグレードする必要があるアプリケーションをリストから選択します。アプリケーションが表示されない場合は、まず追加する必要があります。「アプリケーションの追加 『268p. 』」を参照してください。
- 3. [参照] をクリックして、表示されるダイアログでアプリケーション アップグレード ファイルを見つけて選択し、[開く] をクリックしま す。
- 4. [アプリケーション マネージャ] 画面の [新しいアプリケーション ファイル] フィールドにアプリケーション名が表示されます。
- [アップロード] をクリックします。進捗ウィンドウに新しいアプリ ケーションをアップロード中であることが示されます。完了すると 、別のウィンドウが表示され、新しいアプリケーションが CC-SG データベースに追加されて、使用可能なことが示されます。
- [バージョン] フィールドが自動的に更新されない場合は、[バージョン] フィールドに新しいバージョン番号を入力します。一部のアプリケーションについては、[バージョン] フィールドが自動的に更新されます。
- 7. [更新] をクリックします。

注: アップグレード時にログインしていたユーザは、いったん CC-SG からログアウトしてから、再度ログインし、新しいバージョンのアプリ ケーションが起動されるようにする必要があります。「アップグレード 後に古いバージョンのアプリケーションが開く 『268p. 』」も参照して ください。



アップグレード後に古いバージョンのアプリケーションが開く

接続を試行すると、想定される最新バージョンのアプリケーションでは なく、古いバージョンが開く場合は、Java キャッシュをクリアします 。これは、CC-SG をアップグレードしてからキャッシュをクリアして いない場合に発生する可能性があります。

「Java キャッシュのクリア 『258p. 』」を参照してください。

アプリケーションの追加

CC-SG にアプリケーションを追加するときは、アプリケーションが機 能するデバイス タイプを指定する必要があります。KVM アクセスとシ リアル アクセスの両方を提供するデバイスの場合は、それぞれに 1 回 ずつ、2 回リストされます。

アプリケーションを追加するには、以下の手順に従います。

- 1. [管理]>[アプリケーション]を選択します。
- 2. [追加] をクリックします。[アプリケーションの追加] ウィンドウが 開きます。
- 3. アプリケーションの名前を [アプリケーション名] フィールドに入力 します。
- アプリケーションが機能する Raritan デバイスを [利用可能] リストから選択し、[追加] をクリックして [選択中] リストに追加します。
 - アプリケーションでデバイスが使用されないようにするには、[選択中]リストでデバイスを選択し、[削除]をクリックします。
- 5. [OK] をクリックします。[開く] ダイアログが表示されます。
- アプリケーション ファイル (通常は .jar または .cab ファイル) を 表示して選択し、[開く] をクリックします。
- 7. 選択したアプリケーションが CC-SG にロードされます。

アプリケーションの削除

▶ アプリケーションを削除するには、以下の手順に従います。

- 1. [管理]>[アプリケーション]を選択します。
- [アプリケーション名] ドロップダウン メニューからアプリケーションを選択します。
- 3. [削除] をクリックします。確認のダイアログが表示されます。
- 4. [はい] をクリックして、アプリケーションを削除します。



AKC を使用するため前提条件

AKC を使用するには、以下の手順に従います。

- アクセスするデバイスの IP アドレスからの Cookie が現在ブロッ クされていないことを確認します。
- Windows Vista、Windows 7、および Windows 2008 Server のユー ザは、アクセスするデバイスの IP アドレスがブラウザの [信頼済 みサイト] ゾーンに含まれ、デバイスへのアクセス時に保護モード が有効になっていないことを確認する必要があります。

AKC ダウンロード サーバ証明書の検証を有効にする

デバイス (または CC-SG) の管理者が [Enable AKC Download Server Certificate Validation] (AKC ダウンロード サーバ証明書の検証を有効に する) オプションを有効にした場合は、以下の手順に従います。

- 管理者は、有効な証明書をデバイスにアップロードするか、自己署 名証明書をデバイスで生成する必要があります。証明書で有効なホ ストが指定されている必要があります。
- 各ユーザは、CA 証明書 (または自己署名証明書のコピー) をブラウ ザの信頼されたルート証明機関ストアに追加する必要があります。

CC-SG 管理クライアントから **AKC** を起動する場合は、**JRE[™] 1.6.0_10** 以上が必要です。

デフォルトのアプリケーションの設定

デフォルトのアプリケーションについて

CC-SG が各デバイス タイプにデフォルトで使用するアプリケーション を指定できます。

デフォルト アプリケーションの割り当ての表示

- アプリケーションのデフォルト割り当てを表示するには、以下の手順に従います。
- 1. [管理]>[アプリケーション]を選択します。
- [デフォルトのアプリケーション] タブをクリックして、さまざまな 種類のインタフェースおよびポートの現在のデフォルト アプリケー ションを表示および編集します。ここにリストされたアプリケーシ ョンは、選択したインタフェースを介してアクセスできるようにノ ードを設定する際のデフォルトとなります。



インタフェースまたはポートのタイプのデフォルト アプリケーション の設定

- あるタイプのインタフェースまたはポートのデフォルト アプリケー ションを設定するには、次の手順に従います。
- 1. [管理]>[アプリケーション]を選択します。
- 2. [デフォルトのアプリケーション] タブをクリックします。
- 設定するデフォルトのアプリケーションがあるインタフェースまた はポートのタイプを選択します。
- その行にリストされた [アプリケーション] 矢印をダブルクリックします。値がドロップダウンメニューになります。グレー表示の値は変更できません。
- 5. 選択したタイプのインタフェースまたはポートに接続する際に使用 されるデフォルト アプリケーションを選択します。
 - 自動検出: クライアント ブラウザに基づいて CC-SG によりア プリケーションが自動選択されます。
- [OK] をクリックして変更を保存します。これらのデフォルト設定は、新しいポートにのみ適用されます。これらの設定を既存のデバイス上のポートに適用するには、[Apply Selections to Exisiting Devices (選択内容を既存のデバイスに適用する)] をクリックし、変更するデバイスを選択して [OK] をクリックします。

デバイス ファームウェアの管理

CC-SG には、その制御下にあるデバイスのアップグレードに使用可能 な Raritan デバイスのファームウェアが保存されます。CC-SG に対し てデバイス ファームウェア ファイルをアップロードおよび削除するに は、ファームウェア マネージャを使用します。ファームウェア ファイ ルがアップロードされたら、そのファイルにアクセスしてデバイス ア ップグレードを実行できます。「デバイスのアップグレード『93p.』 」を参照してください。

ファームウェアのアップロード

さまざまなバージョンのファームウェアを CC-SG にアップロードでき ます。新しいファームウェア バージョンが利用可能になると、そのバ ージョンは Raritan の Web サイトに掲載されます。

- ファームウェアを CC-SG アップロードするには、以下の手順に従います。
- 1. [管理]>[ファームウェア]を選択します。


- 2. [追加] をクリックして新しいファームウェア ファイルを追加します 。検索ウィンドウが開きます。
- CC-SG にアップロードするファームウェア ファイルを表示して選択し、[開く] をクリックします。アップロードが完了すると、新しいファームウェアが [ファームウェア名] フィールドに表示されます。

ファームウェアの削除

- ファームウェアを削除するには、以下の手順に従います。
- 1. [管理]>[ファームウェア]を選択します。
- 2. [ファームウェア名] ドロップダウン矢印をクリックし、削除するフ ァームウェアを選択します。
- 3. [削除] をクリックします。確認メッセージが表示されます。
- 4. [はい] をクリックし、ファームウェアを削除します。

CC-SG ネットワークの設定

設定マネージャでは、CC-SG で管理するネットワークのネットワーク 設定を行うことができます。

重要: すでに*隣接システムのメンバ 『293*p. の"*隣接システムとは*"参 照 』になっている CC-SG ユニットの IP アドレスを変更するには、ま ず隣接システムの設定からそれを削除する必要があります。そうしない と、CC-SG を隣接システムから削除することはできません。

ネットワーク設定について

CC-SG には、2 つのモードのネットワーク設定があります。

- IP フェイルオーバ モード:「IP フェイルオーバ モードとは 『 273p. 』」を参照してください。
- IP 分離モード: 「*IP 分離モードとは* 『275p. 』」を参照してくだ さい。

重要:新規の設置には IP フェイルオーバ モードを使用することをお勧めします。

さらに、CC-SG では、静的 IP アドレスと DHCP により割り当てら れた IP アドレスのいずれかを使用できます。CC-SG で DHCP を使 用する場合の推奨事項については、「CC-SG で推奨される DHCP 設定 『277p.』」を参照してください。



CC-SG LAN ポートについて

CC-SG には、プライマリ LAN とセカンダリ LAN の 2 つのメイン LAN ポートがあります。次の表を参照して、ご使用の CC-SG モデル のプライマリ LAN ポートとセカンダリ LAN ポートの場所を確認して ください。

▶ V1 LAN ポート:

モデル	プライマリ LAN 名	プライマリ LAN の場 所	セカンダリ LAN 名	セカンダリ LAN の場所
V1-0 ま たは V1-1	LAN1	左側の LAN ポート	LAN2	右側の LAN ポー ト

▶ E1 LAN ポート:

モデル	プライマリ LAN 名	プライマリ LAN の場 所	セカンダリ LAN 名	セカンダリ LAN の場所
E1-0	ラベルなし	ユニット背面パネルの 中央にある 2 つのポー トのうち上側の LAN ポート	ラベルなし	ユニット背面パネ ルの中央にある 2 つのポートのうち 下側の LAN ポー ト
E1-1	LAN1	左側の LAN ポート	LAN2	右側の LAN ポー ト



IP フェイルオーバ モードとは

IP フェイルオーバ モードでは、2 つの CC-SG LAN ポートを使用して ネットワーク フェイルオーバと冗長性を実装できます。一度に 1 つの LAN ポートだけがアクティブになります。

各 CC-SG モデルのプライマリ LAN ポートとセカンダリ LAN ポート の場所については、「CC-SG LAN ポートについて 『272p. 』」を参照 してください。



プライマリ LAN が接続しており、リンクの整合性信号を受信している 場合、CC-SG はすべての通信にこの LAN を使用します。プライマリ LAN がリンク整合性を失っており、セカンダリ LAN が接続している場 合、CC-SG は割り当てられた IP アドレスをセカンダリ LAN にフェ イルオーバします。セカンダリ LAN は、プライマリ LAN のサービス が復帰するまで使用されます。プライマリ LAN のサービスが復帰する と、CC-SG は自動的にプライマリ LAN の使用に戻ります。

障害が発生したとしても、いずれか一方の LAN 接続が利用可能であれば、PC クライアントでサービスが中断することはありません。

IP フェイルオーバ モードの設定:

CC-SG ネットワークの IP フェイルオーバ モードを実装するには、以下の手順に従います。

- 両方の CC-SG LAN ポートを、同じ LAN サブネットワークに接続 します。
- 各 LAN ポートを同じサブネットワーク上の異なるスイッチまたは ハブに接続して信頼性を向上させることができます。オプション。
- CC-SG で IP フェイルオーバ モードを設定するには、以下の手順 に従います。
- 1. [管理] > [設定] を選択します。
- 2. [ネットワーク設定] タブをクリックします。



- 3. [IP Failover mode (IP フェイルオーバ モード)] を選択します。
- [ホスト名] フィールドに CC-SG ホスト名を入力します。ホスト名のルールについては、「用語/略語 『2p. 』」を参照してください。 トップ レベル ドメイン (たとえば、「.com」)を含めます。トップレベル ドメインは 2 ~ 6 文字で入力する必要があります。
- 5. [設定] ドロップダウン矢印をクリックし、[DHCP] または [静的] を 選択します。

DHCP:

- [DHCP] を選択した場合、このネットワーク設定を保存して CC-SG を再起動すると、プライマリ DNS、セカンダリ DNS 、ドメイン接尾辞、IP アドレス、サブネット マスク、デフォ ルト ゲートウェイの各フィールドが自動的に記入されます (DHCP サーバがこの情報を提供するように設定されている場合)。
- DHCP サーバが提供する情報を使って CC-SG は DNS サーバ に動的に登録されます (DNS サーバが動的な更新を許可する場 合)。
- 「CC-SG で推奨される DHCP 設定 『277p. 』」を参照してく ださい。

静的:

- [静的] を選択した場合、プライマリ DNS、セカンダリ DNS、 ドメイン接尾辞、IP アドレス、サブネット マスク、デフォル ト ゲートウェイをそれぞれ対応するフィールドに入力します。
- [アダプタ速度] ドロップダウン矢印をクリックし、リストから回線 速度を選択します。選択内容がスイッチのアダプタ ポート設定と一 致することを確認します。スイッチで1 ギガの回線速度が使用され ている場合、[自動] を選択します。
- [アダプタ速度] フィールドで [自動] を選択した場合、[アダプタ モード] フィールドは無効になり、[全二重] が自動的に選択されます。[自動] 以外のアダプタ速度を選択した場合、[アダプタ モード] ドロップダウン矢印をクリックして、リストからデュプレックスモードを選択します。
- 8. [設定の更新] をクリックして変更を保存します。CC-SG が再起動 するまで、変更は反映されません。
 - CC-SG をすぐに自動的に再起動する場合は、[すぐに再起動] を クリックします。
 - 後で手動で CC-SG を再起動する場合は、[後で再起動] をクリ ックします。「CC-SG の再起動 『255p. 』」を参照してください。



 変更を保存せずに [ネットワーク設定] パネルに戻るには、[キャンセル] をクリックします。[設定の更新] クリックし、 [すぐに再起動] または [後で再起動] をクリックして、変更 を保存する必要があります。

IP 分離モードとは

IP 分離モードでは、クライアントを別のサブネットワークに配置し、 クライアントに CC-SG を介してデバイスにアクセスするように強制す ることで、クライアントをデバイスから分離できます。このモードでは 、CC-SG は 2 つの別個の IP ドメイン間のトラフィックを管理します 。IP 分離モードでは、フェイルオーバは提供されません。どちらかの LAN 接続でエラーが発生した場合、ユーザはアクセスできなくなりま す。

各 CC-SG モデルのプライマリ LAN ポートとセカンダリ LAN ポート の場所については、「CC-SG LAN ポートについて 『272p. 』」を参照 してください。

注: IP 分離モードではクラスタリングは設定できません。





IP 分離モードの設定:

CC-SG ネットワークの IP 分離モードを実装するには、以下の手順に 従います。

- 各 CC-SG LAN ポートを、異なる LAN サブネットワークに接続す る必要があります。
- Raritan デバイスは、プライマリ LAN にのみ接続する必要があり ます。
- 分離するクライアントをセカンダリ LAN に接続します。分離する 必要がないクライアントは、プライマリ LAN に接続できます。「ダ イレクト モードとプロキシ モードの組み合わせを設定 『281p. 』 」を参照してください。

注: セカンダリ LAN 上の分離されたクライアントでは、プロキシ モードを使用します。プライマリ LAN 上のクライアントでは、ダ イレクト モードを使用できます。 プロキシ モードとダイレクト モ ードの組み合わせを設定するには、【接続モード】を【両方】に設定し ます。

- CC-SG の [ネットワーク設定] パネルで多くとも 1 つのデフォル ト ゲートウェイを指定します。必要であれば、診断コンソールを使 用してさらに静的ルートを追加します。「**静的ルートの編集**『348p. 』 | を参照してください。
- ▶ CC-SG で IP 分離モードを設定するには、以下の手順に従います 0
- 1. [管理] > [設定] を選択します。
- 2. [ネットワーク設定] タブをクリックします。
- 3. [IP Isolation mode (IP 分離モード)] を選択します。
- 4. [ホスト名] フィールドに CC-SG ホスト名を入力します。ホスト名 のルールについては、「用語/略語 『2p. 』」を参照してください。 DNS とドメイン接尾辞が設定されている場合、[設定の更新] をク リックして設定を保存すると、完全修飾ドメイン名 (FQDN) を反映 して [ホスト名] フィールドの内容が更新されます。
- 5. 左側の列でプライマリ LAN を設定し、右側の列でセカンダリ LAN を設定します。
- 6. [設定] ドロップダウン矢印をクリックし、[DHCP] または [静的] を 選択します。 DHCP:





- [DHCP] を選択した場合、このネットワーク設定を保存して CC-SG を再起動すると、プライマリ DNS、セカンダリ DNS 、ドメイン接尾辞、IP アドレス、サブネット マスク、デフォ ルト ゲートウェイの各フィールドが自動的に記入されます (DHCP サーバがこの情報を提供するように設定されている場合)。
- DHCP サーバが提供する情報を使って CC-SG は DNS サーバ に動的に登録されます (DNS サーバが動的な更新を許可する場 合)。
- 「CC-SG で推奨される DHCP 設定 『277p. 』」を参照してく ださい。

静的:

- [静的] を選択した場合、プライマリ DNS、セカンダリ DNS、 ドメイン接尾辞、IP アドレス、サブネット マスクをそれぞれ 該当するフィールドに入力します。
- デフォルト ゲートウェイを、両方ではなく 1 つだけ指定します。
- [アダプタ速度] ドロップダウン矢印をクリックし、リストから回線 速度を選択します。選択内容がスイッチのアダプタ ポート設定と一 致することを確認します。スイッチで1 ギガの回線速度が使用され ている場合、[自動] を選択します。
- [アダプタ速度] フィールドで [自動] を選択した場合、[アダプタ モード] フィールドは無効になり、[全二重] が自動的に選択されます。[自動] 以外のアダプタ速度を選択した場合、[アダプタ モード] ドロップダウン矢印をクリックして、リストからデュプレックスモードを選択します。
- 9. [設定の更新] をクリックして変更を保存します。CC-SG が再起動 します。

CC-SG で推奨される DHCP 設定

推奨される次の DHCP 設定を確認します。CC-SG で DHCP の使用を 設定する前に、DHCP サーバが正しく設定されていることを確認してく ださい。

- CC-SG の IP アドレスを静的に割り当てるように DHCP を設定し ます。
- DHCP が IP アドレスを CC-SG に割り当てるときに、DNS に CC-SG を自動的に登録するように DHCP サーバと DNS サーバを 設定します。
- CC-SG からの認証されていない動的ドメイン名システム (DDNS)
 登録要求を受け入れるように DNS を設定します。



ログ アクティビティの設定

外部ログ サーバにレポートするように CC-SG を設定し、各ログに報告されるメッセージのレベル指定できます。

- CC-SG ログ アクティビティを設定するには、以下の手順に従います。
- 1. [管理] > [設定] を選択します。
- 2. [ログ] タブをクリックします。
- 3. CC-SG で使用する外部ログ サーバを割り当てるには、IP アドレ スを [プライマリ サーバ] の下の [サーバ アドレス] フィールドに 入力します。
- [転送レベル] ドロップダウン矢印をクリックし、イベントの重大度 レベルを選択します。このレベル以上のすべてのイベントがログ サ ーバに送られます。
- 5. 2 番目の外部ログ サーバを設定するには、[セカンダリ サーバ]の 下のフィールドで手順3と4を繰り返します。
- 6. [CommandCenter ログ] の下の [転送レベル] ドロップダウン メニ ューをクリックして、重大度レベルを選択します。このレベル以上 のすべてのイベントが CC-SG 自体の内部ログにレポートされます
- 7. [設定の更新] をクリックして変更を保存します。

CC-SGの内部ログの消去

CC-SGの内部ログは、消去することができます。この操作では、外部 ログ サーバに記録されたイベントは削除されません。

注: 監査証跡レポートおよびエラー ログ レポートは CC-SG 内部ログ ベースです。CC-SG 内部ログを消去すると、これら 2 つのレポートも 消去されます。これらのレポートを別々に消去することもできます。「 CC-SG からのレポートのデータの消去 『234p.』」を参照してくださ い。

- ▶ CC-SG の内部ログを消去するには、以下の手順に従います。
- 1. [管理] > [設定] を選択します。
- 2. [ログ] タブをクリックします。
- 3. [消去] をクリックします。
- 4. [はい] をクリックします。



CC-SG サーバ時間および時刻の設定

CC-SG では、デバイス管理機能の信頼性のため、常に正確な日付と時刻を表示する必要があります。

重要:時刻/日付設定は、タスク マネージャでタスクをスケジュールする 際に使用されます。「タスク マネージャ 『311p. 』」を参照してくだ さい。クライアント PC の時刻設定は CC-SG の時刻設定と異なってい ても構いません。

時刻と日付を設定できるのは、CC スーパーユーザおよび同等の権限を 持つユーザだけです。

クラスタ設定ではタイム ゾーンの変更は無効になっています。

- ▶ **CC-SG** サーバ時間および時刻を設定するには、以下の手順に従います。
- 1. [管理]>[設定] を選択します。
- 2. [時刻/日付] タブをクリックします。
 - a. 日付と時刻を手動で設定するには、以下の手順に従います。
 - 日付 ドロップダウン矢印をクリックして月を選択し、上下の 矢印を使用して年を選択してから、カレンダー領域で日をクリ ックします。
 - 時刻 上下矢印を使って時、分、秒を設定し、次に [タイム ゾ ーン] ドロップダウン矢印をクリックして CC-SG が動作する タイム ゾーンを選択します。
 - a. 日付と時刻を NTP 経由で設定するには、以下の手順に従います。ウィンドウ下部の [ネットワーク時間プロトコルを有効にする] チェックボックスを選択し、プライマリ NTP サーバとセカンダリ NTP サーバの IP アドレスを対応するフィールドに入力します。

注: Network Time Protocol (NTP) は、接続されたコンピュータの日 付と時刻のデータを参照用 NTP サーバに同期させるためのプロト コルです。CC-SG を NTP で設定すると、そのクロックの時刻を 適切な NTP 参照サーバに同期させ、正確で一貫した時刻を維持す ることができます。

- 3. [設定の更新] をクリックして日付と時刻の変更を CC-SG に適用し ます。
- 4. [更新] をクリックして、新しいサーバ時刻を [現在の時刻] フィール ドに再ロードします。
- 5. [システム メンテナンス]>[再起動] を選択して CC-SG を再起動し ます。



接続モード:ダイレクトおよびプロキシ

接続モードについて

CC-SG は、インバンドおよびアウト オブ バンド接続用に「ダイレクト」、「プロキシ」、「両方」という **3** つの接続モードを提供します。

- ダイレクト モードでは、CC-SG 経由でデータを渡さずに、ノード やポートに直接接続できます。ダイレクト モードの接続の方が通常 は高速です。
- プロキシ モードでは、すべてのデータを CC-SG 経由で渡すことにより、ノードやポートに接続できます。プロキシ モードでは、CC-SG サーバの負荷が大きくなるため、接続が低速になる場合があります。しかし、接続のセキュリティを重視する場合はプロキシモードが推奨されます。ファイアウォールで CC-SG の TCP ポート(80、8080、443、2400)を開いておく必要があります。

注: CC-SG 4.2 より、Dominion KXII リリース 2.1.10 以降を使用す る場合にプロキシ モードで KVM データの暗号化がサポートされ ます。この構成では、KVM データは KXII デバイスのセキュリティ 設定に従って暗号化されます。Dominion KXII 2.1.10 より前のデバ イスでは、暗号化はサポートされません。

 両方モードでは、ダイレクト モードとプロキシ モードの組み合わ せを使用するように CC-SG を設定できます。両方モードの場合は プロキシ モードがデフォルトですが、指定した範囲のクライアント IP アドレスを使用して接続が行われたときはダイレクト モードを 使用するように CC-SG を設定できます。

注: CC-SG でプロキシ モードを使用するように設定している場合であ っても、一部のインタフェースはダイレクト モードでのみ機能します。 このようなインタフェースには、ILO、RSA、Microsoft RDP、DRAC、 Web ブラウザ、VMware Viewer があります。Java RDP インタフェー スはプロキシ モードで使用できます。 「インタフェースについて『116p. 』」を参照してください。

すべてのクライアント接続にダイレクト モードを設定

- すべてのクライアント接続にダイレクト モードを設定するには、以下の手順に従います。
- 1. [管理]>[設定] を選択します。
- 2. [接続モード] タブをクリックします。
- 3. [ダイレクト モード] を選択します。
- 4. [設定の更新] をクリックします。



すべてのクライアント接続にプロキシ モードを設定

- すべてのクライアント接続にプロキシ モードを設定するには、以下の手順に従います。
- 1. [管理] > [設定] を選択します。
- 2. [接続モード] タブをクリックします。
- 3. [プロキシ モード] を選択します。
- 4. [設定の更新] をクリックします。

ダイレクト モードとプロキシ モードの組み合わせを設定

ダイレクト モードとプロキシ モードの組み合わせを使用するように CC-SG を設定すると、プロキシ モードがデフォルトの接続モードとな り、指定したクライアント IP アドレスにはダイレクト モードが使用 されます。

- ダイレクト モードとプロキシ モードの組み合わせを設定するには、以下の手順に従います。
- 1. [管理] > [設定] を選択します。
- 2. [接続モード] タブをクリックします。
- 3. [両方] を選択します。
- [ネット アドレス] フィールドと [ネット マスク] フィールドで、ダ イレクト モードでノードおよびポートに接続するクライアント IP アドレスの範囲を指定して、[追加] をクリックします。
- 5. [設定の更新] をクリックします。

デバイス設定

すべてのデバイスに適用する一部の設定を定義し、各デバイス タイプ のデフォルト ポート番号を設定できます。

- デバイスのデフォルト ポート番号を設定するには、以下の手順に従います。
- 1. [管理] > [設定] を選択します。
- 2. [デバイス設定] タブをクリックします。
- 3. テーブルでデバイス タイプを選択し、デフォルト ポート値をダブ ルクリックします。
- 4. 新しいデフォルト ポート値を入力します。
- 5. [設定の更新] をクリックして変更を保存します。



- デバイスのタイムアウト期間を設定するには、以下の手順に従います。
- 1. [管理]>[設定] を選択します。
- 2. [デバイス設定] タブをクリックします。
- 3. 新しいタイムアウト期間を [ハートビート (秒)] フィールドに入力 します。有効な値の範囲は 30 秒から 50,000 秒です。
- 4. [設定の更新] をクリックして変更を保存します。
- すべてのパワー制御操作で警告メッセージを有効または無効にする には、以下の手順に従います。

[すべての電源操作に警告メッセージを表示する] チェックボックスを選択し、要求された電源操作が実行される前に、ユーザへ警告メッセージが表示されるようにします。電源操作を開始したユーザしか、このメッセージを見れません。メッセージ内の [はい] をクリックすると電源操作が取り消され、[いいえ] をクリックすると操作が実行されます。

- 1. [管理] > [設定] を選択します。
- 2. [デバイス設定] タブをクリックします。
- 3. 警告メッセージを有効にするには、[すべての電源操作に警告メッセ ージを表示する] チェックボックスを選択します。警告メッセージ を無効にするには、このチェックボックスを選択解除します。
- 4. [設定の更新] をクリックして変更を保存します。



AKC ダウンロード サーバ証明書の検証の有効化

AKC クライアントを使用する場合は、[Enable AKC Download Server Certificate Validation] (AKC ダウンロード サーバ証明書の検証を有効に する) 機能を使用するかどうかを選択できます。

オプション 1: AKC ダウンロード サーバ証明書の検証を有効にしない (デフォルト設定)

AKC ダウンロード サーバ証明書の検証を有効にしない場合、すべての Dominion デバイス ユーザおよび CC-SG Bookmark and Access Client ユーザは、次のことを行う必要があります。

- アクセスするデバイスの IP アドレスからの Cookie が現在ブロッ クされていないことを確認します。
- Windows Vista、Windows 7、および Windows 2008 Server のユー ザは、アクセスするデバイスの IP アドレスがブラウザの [信頼済 みサイト] ゾーンに含まれ、デバイスへのアクセス時に保護モード が有効になっていないことを確認する必要があります。

オプション 2: AKC ダウンロード サーバ証明書の検証を有効にする AKC ダウンロード サーバ証明書の検証を有効にする場合は、以下の操 作を行います。

- 管理者は、有効な証明書をデバイスにアップロードするか、自己署 名証明書をデバイスで生成する必要があります。証明書で有効なホ ストが指定されている必要があります。
- 各ユーザは、CA 証明書 (または自己署名証明書のコピー) をブラウ ザの信頼されたルート証明機関ストアに追加する必要があります。
- Windows Vista[®] または Windows 7[®] を使用する場合、自己署名証 明書をインストールするには、以下の手順に従います。
- [信頼済みサイト] ゾーンに CommandCenter Secure Gateway の IP アドレスを追加し、保護モードがオフになっていることを確認し ます。
- 2. URL に CommandCenter Secure Gateway の IP アドレスを使用 して Internet Explorer[®] を起動します。証明書エラー メッセージが 表示されます。
- 3. [証明書の表示] を選択します。
- [全般] タブで、[証明書のインストール] をクリックします。証明書 が信頼されたルート証明機関ストアにインストールされます。
- 5. 証明書のインストール後、CommandCenter Secure Gateway の IP アドレスを [信頼済みサイト] ゾーンから削除できます。



- ▶ AKC ダウンロード サーバ証明書の検証を有効にするには
- [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
- [Enable AKC Download Server Certificate Validation] (AKC ダウンロ ード サーバ証明書の検証を有効にする) チェック ボックスをオン にします。なお、この機能は無効のままにしておくこともできます (デフォルト設定は無効)。
- 3. [OK] をクリックします。

カスタム JRE 設定の定義

指定した最小限度の JRE バージョンを持たないユーザが CC-SG にア クセスを試みると警告メッセージが表示されます。サポートされる最小 限度の JRE バージョンについては、互換表を確認してください。[管理]>[互換表] を選択します。

CC-SG へのログインを試みるユーザが指定の JRE バージョンをイン ストールしていない場合、[JRE 互換性に関する警告] ウィンドウが開き ます。このウィンドウには、デフォルトの最小限度の JRE バージョン をダウンロードするためのいくつかのオプションがあります。メッセー ジを変更して、他のテキストやダウンロード オプションへのリンクを 表示させることができます。ユーザは新しい JRE バージョンをダウン ロードすることも、現在インストールされている JRE バージョンで **CC-SG** へのアクセスを続行することもできます。

- ログイン用のカスタム JRE を有効または無効にするには、以下の 手順に従います。
- この機能を有効または無効にする前に、CC-SG をバックアップし、バックアップ ファイルをリモートの場所に保存します。「CC-SG のバックアップ 『248p. 』」を参照してください。
- 2. [管理]>[設定] を選択します。
- 3. [カスタム JRE] タブをクリックします。
- オプションを有効にするには、[ログインのカスタム JRE を有効に する] チェックボックスを選択します。オプションを無効にするに は、このチェックボックスを選択解除します。
- 必要な最小限度の JRE バージョンを [必要な最小限度の JRE] フィールドに入力します。3 つ以上の部分で構成される完全なバージョン番号を入力する必要があります。たとえば 1.6.0 は正しいバージョン番号ですが、1.6 は正しいバージョン番号ではありません。 JRE 「アップデート」バージョンの場合、下線文字を使用します。 たとえば、1.6.0_5 は JRE バージョン 1.6.0 アップデート 5 を示 す正しいバージョン番号です。



- 6. [更新] をクリックします。
- [JRE 互換性に関する警告] ウィンドウのメッセージをカスタマイズ するには、以下の手順に従います。
- 1. [管理] > [設定] を選択します。
- 2. [カスタム JRE] タブをクリックします。
- 3. HTML コードを使用して、[JRE 互換性に関する警告] ウィンドウに 表示されるメッセージを入力します。
- 4. [更新] をクリックします。
- デフォルト メッセージおよび最小限度の JRE バージョンをリスト アするには、以下の手順に従います。
- 1. [管理]>[設定] を選択します。
- 2. [カスタム JRE] タブをクリックします。
- 3. [デフォルトのリストア] をクリックします。
- 4. [更新] をクリックします。
- デフォルト メッセージおよび最小限度の JRE バージョンをクリア するには、以下の手順に従います。
- [管理] > [設定] を選択します。[カスタム JRE] タブをクリックします。
- 2. [クリア] をクリックします。

SNMP の設定

SNMP (Simple Network Management Protocol (簡易ネットワーク管理プロトコル)) を使うと、CC-SG は SNMP トラップ (イベント通知) をネットワーク上の既存の SNMP マネージャに送り出すことができます。 CC-SG が SNMP と連携して動作するように設定するには、SNMP インフラストラクチャの処理訓練を受ける必要があります。

CC-SG は、HP OpenView などサードパーティのソリューションによ る SNMP GET/SET の操作もサポートします。この操作をサポートす るには、MIB-II システム グループ オブジェクトの sysContact、 sysName、sysLocation などの SNMP エージェント識別子情報を提示 する必要があります。これらの識別子は、管理対象ノードに関する連絡 先、管理、所在地の情報を提供します。詳細は RFC 1213 を参照して ください。

CC-SG で SNMP を設定するには、以下の手順に従います。

- 1. [管理]>[設定] を選択します。
- 2. [SNMP] タブをクリックします。
- 3. [SNMP デーモンを有効にする] チェックボックスを選択して、 SNMP 操作を有効にします。



- 4. サードパーティのエンタープライズ管理ソリューションに CC-SG で実行している SNMP エージェントを認識させるには、[エージェ ント設定] にエージェント情報を入力します。エージェントのポー トを入力します (デフォルトは 161)。読み取り専用コミュニティ文 字列 (デフォルトは「public」)または読み書きコミュニティ文字列 (デフォルトは「private」)を入力します。カンマで区切って複数のコ ミュニティ文字列を指定することもできます。システム連絡先、シ ステム名、システム所在地を入力して、管理対象ノードに関する情 報を提供します。
- 5. [エージェント設定の更新]をクリックして変更を保存します。
- [SNMP トラップを有効にする] チェックボックスを選択し、
 CC-SG から SNMP ホストへの SNMP トラップの送信を有効にします。
- 7. [トラップ送信先] セクションで、SNMP ホストが使用するトラップ 送信先ホスト IP アドレスとポート番号を入力します。デフォルト のポートは 162 です。
- 8. SNMP ホストが使用するコミュニティ文字列およびバージョン (v1 または v2) を [トラップ送信先] セクションに入力します。
- CC-SG が SNMP ホストに送り出すトラップの前にあるチェックボ ックスを選択します。[トラップ ソース] には 2 つの異なるカテゴ リにグループ分けされた SNMP トラップのリストがあります。[シ ステム ログ] トラップにはハードディスク エラーなどの CC ユニ ット自体のステータスの通知が、[アプリケーション ログ] トラップ にはユーザ アカウントの変更といった CC アプリケーションのイ ベントで生成された通知が含まれています。タイプ別にトラップを 有効にするには、[システム ログ] および [アプリケーション ログ] のラベルのついたボックスを選択します。該当するチェックボック スを選択すると、個別のトラップを有効または無効にできます。[選 択中] 列ヘッダ内のチェックボックスを使用してすべてのトラップ を有効にするか、すべてのチェックボックスを選択解除します。提 供される SNMP トラップのリストについては、MIB ファイルを参 照してください。詳細は、MIB ファイルを参照してください。
- [追加] をクリックして、この送信先ホストを設定済みホストのリストに追加します。このリストで設定できるマネージャ数に制限はありません。
- 11. [トラップ設定の更新] をクリックして変更を保存します。



MIB ファイル

CC-SG は独自の Raritan トラップ セットを送り出すため、Raritan の SNMP トラップ定義を含んだカスタム MIB ファイルですべての SNMP マネージャを更新する必要があります。「SNMP トラップ 『 408p. 』」を参照してください。カスタム MIB ファイルは、Raritan の サポート Web サイトにあります。

CC-SG クラスタの設定

CC-SG クラスタは、プライマリ ノードの障害時に備えたバックアップ として、プライマリ ノードとセカンダリ ノードの 2 つの **CC-SG** ノ ードを使用します。両方のノードは、アクティブ ユーザとアクティブ 接続に対して共通のデータを共有しています。

CC-SG クラスタ内のデバイスは、ステータス変更イベントをプライマ リノードに通知できるように、プライマリ CC-SG ノードの IP を認 識している必要があります。プライマリ ノードに障害が発生すると、 セカンダリノードが直ちにすべてのプライマリノードの機能を引き継 ぎます。これには、CC-SG のアプリケーションおよびユーザ セッショ ンの初期化が必要となります (プライマリ CC-SG ノードから行われた 既存のセッションはすべて終了します)。プライマリノードに接続され たデバイスは、プライマリノードが応答していないことを認識し、セ カンダリノードからの要求に応答するようになります。

CC-SG クラスタの要件

- クラスタのプライマリ ノードとセカンダリ ノードは、同じハード ウェア バージョン (V1 または E1) で同じバージョンのファームウ ェアを実行している必要があります。
- クラスタリングで使用するには、CC-SG ネットワークが IP フェ イルオーバ モードで稼動している必要があります。クラスタリング は、IP 分離モードでは機能しません。「*ネットワーク設定について* 『271p.』」を参照してください。
- 日付、時刻、タイム ゾーンの設定は、プライマリ ノードからセカ ンダリ ノードに複製されません。クラスタを作成する前に、これら の設定を各 CC-SG で行う必要があります。



CC-SG クラスタへのアクセス

クラスタが作成されると、ユーザはプライマリ ノードに直接アクセス できます。また、ブラウザでセカンダリ ノードをポイントすると、リ ダイレクトされます。

リダイレクトはすでにダウンロードされている Admin Client アプレットでは機能しません。Web ブラウザを閉じ、新しいセッションを開い て新しいプライマリ システムをポイントする必要があります。

CC-SG への **SSH** アクセスでは、特定のプライマリ ノードにアクセス する必要があります。

クラスタの作成

クラスタを作成する前に、両方の **CC-SG** ユニットの設定をバックアッ プしてください。

- クラスタを作成するには、以下の手順に従います。
- 1. [管理]>[クラスタ設定] を選択します。
- 現在アクセスしている CC-SG がプライマリの [Secure Gateway の IP アドレス/ホスト名] フィールドに表示され、それがプライマ リ ノードになることが示されます。
- バックアップの [Secure Gateway の IP アドレス/ホスト名] でセカ ンダリ (バックアップ) ノードを指定します。指定する CC-SG の ファームウェア バージョンとハードウェアのタイプは、プライマリ ノードと同じであることを確認します。次のいずれかの方法で指定 します。
 - [Secure Gateway の検出] をクリックし、現在アクセスしている サブネットと同じサブネット上に存在するすべての CC-SG ユニットをスキャンして表示します。次に、検出された CC-SG ユニットのテーブルでスタンドアロン状態の CC-SG ユニット をクリックして選択します。
 - バックアップの [Secure Gateway の IP アドレス/ホスト名] フ ィールドに IP アドレスまたはホスト名を入力して、別のサブ ネットにある CC-SG を指定できます。次に、[バックアップの 確認] をクリックして、ファームウェア バージョンとハードウ ェアのタイプがプライマリ ノードと同じかどうかを確認します。
- 4. このクラスタの名前を [クラスタ名] フィールドに入力します。
- 5. バックアップ Secure Gateway の [ユーザ名] フィールドと [パス ワード] フィールドに、バックアップ ノードの有効なユーザ名とパ スワードを入力します。



- [ホスト名でリダイレクト] チェックボックスをオンにして、セカン ダリからプライマリへのリダイレクト アクセスを DNS 経由で行う ように指定します。オプション。「CC-SG クラスタへのアクセス 『288p.』」を参照してください。IP アドレスではなくホスト名を 使用する場合は、ホスト名を解決できるように、DNS サーバに CC-SG の IP アドレスの逆引き参照レコードが含まれている必要 があります。
- 7. [クラスタの作成] をクリックします。メッセージが表示されます。
- 8. [はい] をクリックします。

重要: クラスタ作成処理を開始したら、その処理が完了するまでは CC-SG で他の操作を実行しないでください。

- 9. 画面にメッセージが表示されたら [OK] をクリックします。バック アップ ノードが再開されます。処理には数分かかります。
- **10.** クラスタ作成が終了すると、バックアップ ノードが正常に追加され たことを示すメッセージが表示されます。

クラスタの設定

クラスタ設定ではタイム ゾーンを変更することができません。

- クラスタの設定を行うには、以下の手順に従います。
- 1. [管理]>[クラスタ設定]を選択します。
- 2. [設定] タブで、新規設定するか、設定を変更します。
 - 必要な場合は、クラスタ名を変更します。
 - [インターバル時間] には、CC-SG が他のノードとの接続を確認 する頻度を入力します。有効な値は 5 ~ 20 秒です。

注: インターバル時間を低く設定すると、ハートビート チェックに よって生成されるネットワーク トラフィックが増加します。それぞ れ離れた場所に配置されているノード付きクラスタには高いインタ ーバルを設定できます。

- [失敗しきい値]には、応答がない場合、CC-SGのノードが失敗 と見なされるまでの連続ハートビート数を入力します。有効な 値は 2 ~ 10 回です。
- 3. [更新] をクリックして変更を保存します。



プライマリ ノードとセカンダリ ノードのステータスの切り替え

セカンダリ (バックアップ) ノードが "追加" 状態である場合は、プライ マリ ノードとセカンダリ ノードの機能を交換することができます。セ カンダリ ノードが "待機" 状態である場合は、切り替えが無効になりま す。

機能が切り替わると、前のプライマリ ノードは "待機" 状態になります 。クラスタ設定を復元するには、"待機" ノードをバックアップとして追 加します。

「クラスタの復元 『290p. 』」を参照してください。

- プライマリ ノードとセカンダリ ノードを切り替えるには、以下の 手順に従います。
- 1. [管理]>[クラスタ設定]を選択します。
- [設定] タブで、[プライマリとバックアップを切り替えます] をクリ ックします。
- 3. 新しいセカンダリ ノードをバックアップ ノードとして追加します 。「クラスタの復元 『290p. 』」を参照してください。

クラスタの復元

ノードの障害によってクラスタが破損した場合、または障害のあるセカ ンダリ ノードを待機ステータスにした場合は、クラスタを再作成して プライマリ ノードおよびセカンダリ ノードのステータスを復元する必 要があります。

プライマリ ノードとセカンダリ ノードが互いに通信できなくなると、 セカンダリ ノードがプライマリ ノードの機能を引き継ぎます。このた め、接続が回復したときに、プライマリ ノードが 2 つになる場合があ ります。2 つのプライマリ ノードでクラスタを復元することはできま せん。復元は、1 つのプライマリ ノードと 1 つの待機ノードが存在す る場合にのみ機能します。

2 つのプライマリ ノードでクラスタを復元するには、2 つの方法があ ります。各プライマリ ノードにログインし、それぞれのノードでクラ スタを削除してからクラスタを再作成します。または、いずれかのプラ イマリ ノードにログインし、ノードを再起動して待機ステータスにし ます。その後、手順に従ってクラスタを復元します。

クラスタを復元するには、以下の手順に従います。

- 1. [管理]>[クラスタ設定]を選択します。
- 2. [復元] タブをクリックします。ここで、クラスタをすぐに、または 指定した時刻に自動的に再作成できます。



Ch 15: 高度な管理

- [Rebuild Now (すぐに再作成)] をクリックすると、クラスタが即 座に再作成されます。
- [Enable Automatic Rebuild (自動再作成を有効にする)] チェック ボックスを選択し、[開始時刻] フィールドと [終了時刻] フィー ルドでクラスタを再作成する時刻を指定します。[更新] をクリ ックして変更を保存します。

注: クラスタ化された複数の CC-SG ユニットのタイムゾーンが異 なる場合は、プライマリ ノードで障害が発生し、セカンダリ ノー ドが新しいプライマリ ノードになった場合でも、自動再作成に指定 された時刻は古いプライマリ ノードのタイムゾーンでの時刻になり ます。

クラスタの削除

クラスタを完全に削除すると、クラスタについて入力されていた情報が 完全に削除され、プライマリ CC-SG ノードとセカンダリ CC-SG ノー ドの両方がスタンドアロン状態にリストアされます。さらに、セカンダ リ ノード上で、ネットワーク設定 (個人パッケージ) を除くすべての設 定データが、CC スーパー ユーザのパスワードを含めて、デフォルト にリセットされます。

- ▶ クラスタを削除するには、以下の手順に従います。
- 1. [管理]>[クラスタ設定] を選択します。
- 2. [Delete Cluster (クラスタの削除)] をクリックします。
- [はい] をクリックし、プライマリ ノードとセカンダリ ノードのス テータスを削除します。
- 4. クラスタが削除されるとメッセージが表示されます。

クラスタのアップグレード

「クラスタのアップグレード 『259p. 』」を参照してください。



クラスタ ライセンス

同じノード数の別のスタンドアロン ライセンス、またはクラスタ キッ ト ライセンスを使用して、**CC-SG** クラスタを運用できます。

クラスタ ライセンスは、スタンドアロン ライセンスとは異なり、クラ スタ内の両方の CC-SG ユニットのホスト ID を含んでいます。1 セッ トのライセンスだけで、クラスタ内の両方の CC-SG ユニットを運用で きます。

クラスタ ライセンスは、プライマリ **CC-SG** ユニットに追加する必要 があります。クラスタを作成すると、ライセンスが自動的にバックアッ プ ノードにコピーされます。

CC-SG クラスタをバージョン 5.0 以降にアップグレードする場合は、 ファームウェアのアップグレード手順に従って、各 CC-SG で同一セッ トのライセンスが作成されるようにします。「クラスタのアップグレー ド『259p.』」を参照してください。

クラスタ内の各 CC-SG はプライマリとしての引き継ぎ可能であること が必要なので、ライセンスされているノード数はどちらでも常に同じで なければなりません。クラスタ キット ライセンスは、プライマリから バックアップにコピーされているので、同一であることが自動的に確認 されます。クラスタをスタンドアロン ライセンスで運用している場合 は、クラスタ追加時のライセンス ノード数チェックによってこれを実 行できます。

バックアップのホスト ID は、クラスタの追加時にチェックされます。 このチェックではライセンス ファイルの内容との整合性が確認されま す。ホスト ID がライセンスと一致しない場合、バックアップをクラス タに追加することはできません。

クラスタの最初の作成にクラスタ キット ライセンスを使用した場合は 、バックアップがクラスタに正常に追加されるまで、プライマリ CC-SG の動作モードが制限されます。

プライマリが動作状態になった後に、ファームウェアのアップグレード などのメンテナンス作業をサポートする必要性から、クラスタが一時的 に削除され再構築されることがあります。クラスタは、30日の猶予期 間内に再作成する必要があります。クラスタが一時的に削除されるたび に、30日の猶予期間が付与されます。



隣接システムの設定

隣接システムとは

隣接システムは、最大 10 の CC-SG ユニットのコレクションです。 Admin Client で隣接システムが設定されていると、ユーザは、Access Client を使用して、同じ隣接システム内の複数の CC-SG ユニットにシ ングル サインオンでアクセスできます。

隣接システム構成を設定または管理する前に、以下の隣接システムの基 準に留意してください。

- CC-SG ユニットは 1 つの隣接システムのみに属します。
- 同じ隣接システムのすべての CC-SG ユニットのファームウェア バージョンは同じにする必要があります。
- 隣接システムの CC-SG ユニットは、スタンドアロンの CC-SG ユニット、またはクラスタ化された CC-SG ユニットのプライマリノードである必要があります。
- 隣接システムには物理および仮想 CC-SG ユニットの両方を含める ことができます。

隣接システムの作成

まだどの隣接システムのメンバにもなっていない CC-SG ユニットのうち、隣接システムを作成するユニットにログインできます。隣接システムの作成後は、隣接システムのすべてのメンバが同じ隣接システム情報を共有します。いずれかのメンバがクラスタ化された CC-SG ユニットのプライマリ ノードである場合は、セカンダリ (バックアップ) ノードの IP アドレスまたはホスト名も隣接システム設定に表示されます。

- 隣接システムを作成するには、以下の手順に従います。
- 1. [管理]>[隣接システム]を選択します。
- 2. [隣接システムの名前フィールドに名前を入力します。
- 3. [隣接システムの作成] をクリックします。
- 現在の CC-SG の IP アドレスまたはホスト名が [Secure Gateway の IP アドレス/ホスト名] テーブルに表示されます。ドロップダウンの矢印をクリックして、完全なホスト名、短いホスト名、または IP アドレスのいずれかの表示に切り替えることができます。
- 5. テーブルに 1 つ以上の CC-SG ユニットを追加します。
 - a. 次の空行をクリックするか、Tab または上または下の矢印キー を押します。
 - b. 追加する新しい CC-SG ユニットの IP アドレスまたはホスト 名を入力し、Enter キーを押します。ホスト名のルールについ ては、「*用語/略語* **『2**p. **』**」を参照してください。



- c. CC-SG ユニットをすべて追加し終わるまで、前の手順を繰り返 します。
- 6. [次へ] をクリックします。
 - 1 つ以上の CC-SG ユニットが見つからない場合は、メッセージが表示され、テーブル内でこれらの CC-SG ユニットが黄色でハイライトされます。これらのユニットを削除するか、その IP アドレスまたはホスト名を変更して、[次へ] を再度クリックします。
- 7. CC-SG ユニットとそのファームウェア バージョンおよび状態のリ ストが [隣接システムの設定] テーブルに表示されます。

注: 隣接システムの基準 『293p. の"隣接システムとは"参照 』を満 たしていない CC-SG ユニットは、自動的に無効になります。

- 8. 必要に応じて、隣接システムの設定を調整します。オプション。
 - CC-SG の Secure Gateway 名を変更するには、名前をクリックし、新しい名前をクリックし、Enter キーを押します。デフォルトは短い CC-SG ホスト名です。この名前は、Access Client ユーザが隣接システムのメンバを切り替えるときに表示されるので、それぞれの名前が一意である必要があります。
 - いずれかの CC-SG ユニットを無効にするには、そのユニットの横の [有効化] チェックボックスを選択解除します。無効化した CC-SG ユニットは、スタンドアロン ユニットとして動作し、Access Client ユーザに隣接システムのメンバの 1 つとして表示されることはありません。
 - 列のヘッダをクリックすると、テーブルがその属性によって昇順に並べ替えられます。ヘッダを再度クリックすると、テーブルが降順に並び替わります。
- 9. 前の画面に戻るには、[戻る] をクリックし、前の手順を繰り返しま す。オプション。

10. [終了] をクリックします。

注: Raritan では、以下を推奨します。

(1) すべての隣接システムのメンバについて、同じ制限付きサービス同 意書の設定およびテキストを設定する。「ポータル 『304p. 』」を参照 してください。

(2) SSL が有効である場合は、すべての隣接システムのメンバについて 信頼された証明書または公式の証明書を使用する。



隣接システムの編集

つの CC-SG ユニットで隣接システムを設定すると、同じ隣接システムのすべての CC-SG ユニットで同じ隣接システム情報が共有されます。
 したがって、隣接システムの任意の CC-SG ユニットにログインして、隣接システム設定を変更することができます。

注: 隣接システムのメンバに対するすべての変更は、[隣接システムの設 定] パネルで [更新の送信] をクリックすると送信されます。ただし、現 在隣接システムにログインしているユーザに対しては、いったんログア ウトして再度ログインするまでこの変更は反映されません。

隣接システムのメンバの追加

- 隣接システムに新しい CC-SG ユニットを追加するには、以下の手順に従います。
- 1. [管理] > [隣接システム] を選択します。
- 2. [メンバの追加] をクリックします。[メンバの追加] ダイアログ ボッ クスが表示されます。
- CC-SG ユニットを追加します。追加できる CC-SG ユニットの数 は、隣接システムの既存のメンバの数によって異なります。隣接シ ステムの最大メンバ数は 10 です。
 - a. 次の空行をクリックするか、**Tab** または上または下の矢印キー を押します。
 - b. 追加する CC-SG ユニットの IP アドレスまたはホスト名を入 力します。ホスト名のルールについては、「*用語/略語* 『2p. 』 」を参照してください。
 - CC-SG ユニットをすべて追加するまで、前の手順を繰り返します。
 - d. [OK] をクリックします。
- 隣接システムの基準を満たす新しい CC-SG ユニットが検出された 場合は、それが [隣接システムの設定] テーブルに表示されます。そ れ以外の場合は、メッセージが表示され、[メンバの追加] ダイアロ グ ボックスに戻ります。ダイアログ ボックス内で必要に応じて変 更を加えます。
- 5. 新しい CC-SG ユニットそれぞれの横にある [アクティブ] チェッ クボックスを選択します。
- CC-SG の Secure Gateway 名を変更するには、名前をクリックし、新しい名前をクリックし、Enter キーを押します。デフォルトは短い CC-SG ホスト名です。オプション。
- 7. [更新の送信] をクリックして、変更を保存し、最新の隣接システム 情報を他のメンバに配布します。



隣接システムの設定の管理

隣接システムの設定で、CC-SG ユニットの無効化や名前の変更ができ ます。CC-SG ユニットを無効にすると、それを Access Client の [隣 接システムのメンバ] リストで使用できなくなります。また、隣接シス テム設定で、すべてのメンバのデータ (ファームウェアのバージョンや ユニットのステータスなど) をリフレッシュできます。

- 隣接システムの CC-SG ユニットの無効化、名前の変更、または最 新データの取得を行うには、以下の手順に従います。
- 1. [管理] > [隣接システム] を選択します。
- 2. 列のヘッダをクリックすると、テーブルがその属性によって昇順に 並べ替えられます。ヘッダを再度クリックすると、テーブルが降順 に並び替わります。オプション。
- 3. ここでメンバを管理します。
 - CC-SG ユニットを無効にするには、そのユニットの横の [アク ティブ] チェックボックスを選択解除します。
 - Secure Gateway 名を変更するには、名前をクリックし、新しい 名前を入力し、Enter キーを押します。名前は、固有のものに する必要があります。
 - すべての CC-SG ユニットの最新のデータを取得するには、[メ ンバ データの更新] をクリックします。
 - ユーザが別の CC-SG ユニットに切り替えるときに既存の接続 セッションを常に終了する場合は、[Secure Gateways の切り替 え時、アクティブ セッションを切断する] チェックボックスを 選択します。それ以外の場合は、このチェックボックスを選択 解除します。
- 4. [更新の送信] をクリックして、変更を保存し、最新の隣接システム 情報を他のメンバに配布します。



隣接システムのメンバの削除

隣接システムの CC-SG ユニットが適切でなくなった場合は、隣接シス テム設定でそれを削除するか無効にすることができます。そのままにし ておくと、Access Client ユーザがこれらのユニットに切り替えようと してもアクセスできないことになります。たとえば、隣接システムのメ ンバは次の場合に不適切になります。

- クラスタ設定で CC-SG ユニットを、*隣接システムの基準* 『293p. の"*隣接システムとは*"参照 』を満たす状態ではないバックアップ CC-SG ノードとして設定した場合。
- CC-SG ユニットをリセットしたために、その隣接システム設定が 削除され、工場出荷時のデフォルト値に戻った場合。

メンバを削除する場合は、少なくとも 2 つの CC-SG ユニットが隣接 システムに残ることを確認します。メンバが 1 つだけになると、 CC-SG ユニットによってこの隣接システムが削除されます。

- 隣接システムから CC-SG ユニットを削除するには、以下の手順に 従います。
- 1. [管理]>[隣接システム]を選択します。
- 削除する CC-SG ユニットをクリックし、[メンバの削除] をクリッ クします。目的の CC-SG ユニットをすべて削除するまで、この手 順を繰り返します。
- 3. [更新の送信] をクリックして、変更を保存し、最新の隣接システム 情報を他のメンバに配布します。

重要: すでに*隣接システムのメンバ 『293*p. の"*隣接システムとは*"参 照 』になっている CC-SG ユニットの IP アドレスを変更するには、ま ず隣接システムの設定からそれを削除する必要があります。そうしない と、CC-SG を隣接システムから削除することはできません。

隣接システムの更新

すべての隣接システムのメンバの最新のステータスは、[隣接システムの 設定]パネルですぐに取得できます。

- 1. [管理] > [隣接システム] を選択します。
- 2. [メンバ データの更新] をクリックします。
- 3. [更新の送信] をクリックして、変更を保存し、最新の隣接システム 情報を他のメンバに配布します。



隣接システムの削除

- 隣接システムを削除するには、以下の手順に従います。
- 1. 隣接システムの設定を削除する CC-SG ユニットにログインします。
- 2. [管理]>[隣接システム]を選択します。
- 3. [隣接システムの削除] をクリックします。
- 4. [はい] をクリックして削除を確認します。

セキュリティ マネージャ

セキュリティ マネージャを使用すると、CC-SG によるユーザへのアク セス許可方法を管理できます。セキュリティ マネージャにより、認証 方法、SSL アクセス、AES 暗号化、強力なパスワード ルール、ロック アウト ルール、ログイン ポータル、証明書、アクセス制御リストを設 定できます。

リモート認証

リモート認証サーバの設定手順の詳細は、「**リモート認証『210**p. **』**」 を参照してください。

AES 暗号化

クライアントと CC-SG サーバ間で AES -128 または AES-256 暗号 化を要求するように CC-SG を設定できます。AES 暗号化が要求され ると、すべてのユーザは AES が有効なクライアントを使用して CC-SG にアクセスする必要があります。AES 暗号化が要求される場合 に AES 非対応のブラウザを使用して CC-SG にアクセスしようとする と、CC-SG に接続できません。



AES 暗号化に関するブラウザのチェック

CC-SG は **AES-128** および **AES-256** をサポートしています。使用しているブラウザで **AES** が使用されているかどうかわからない場合、ブラウザの製造元に確認してください。

暗号化方法をチェックするブラウザを使用して、Web サイト https: //www.fortify.net/sslcheck.html

https://www.fortify.net/sslcheck.html にアクセスすることもできます。この Web サイトでは、ブラウザの暗号化方法が検出され、レポート が表示されます。この Web サイトは、Raritan とは関係がありません

注: Internet Explorer 6 は AES-128 または -256 暗号化をサポートして いません。

AES-256 の必要条件およびサポートされている設定

AES-256 暗号化は以下の Web ブラウザでのみサポートされています

-)
- Firefox 2.0.0.x 以降
- Internet Explorer 7

注: Internet Explorer 7 は、Windows Vista においてのみ、AES-128 または AES -256 暗号化をサポートしています。Windows XP では、AES 暗号化はサポートされていません。

ブラウザ サポートに加えて、AES-256 暗号化には、Java Cryptography Extension (JCE) 無制限強度の管轄ポリシー ファイル 6 のインストールが必要です。

ブラウザで AES -256 暗号化を有効にするには、以下の手順に従います。

- http://java.sun.com/javase/downloads/index.jsp 『
 http://java.sun.com/javase/downloads/index.jsp参照 』から JCE
 無制限強度の管轄ポリシー ファイル 6 をダウンロードします。
- ファイルを Java ディレクトリの \lib\securiry\ の下に解凍し ます。たとえば、C: \Program Files\Java 1.6.0\lib\security\ に解凍します。

クライアントおよび CC-SG 間での AES 暗号化の要求

セキュリティ マネージャでは、クライアントと CC-SG サーバ間のセ ッションに AES 暗号化を要求するように CC-SG を設定できます。

- 1. [管理]>[セキュリティ]を選択します。
- 2. [暗号化] タブを開きます。
- 3. [クライアントとサーバ間で AES 暗号化が必要] チェックボックス を選択します。



- このオプションをオンにすると、クライアントが CC-SG に接続するには AES 暗号化の使用が必要になることを警告するメッセージが表示されます。[OK] をクリックして確認します。
 - [キーの長さ] ドロップダウン矢印をクリックして、暗号化レベル (128 または 256) を選択します。
 - [CC-SG ポート] フィールドには 80 と表示されます。
 - [ブラウザ接続プロトコル] フィールドには、[HTTPS/SSL] が選 択状態で表示されます。
- 5. [更新] をクリックして変更を保存します。

ブラウザ接続プロトコルの設定: HTTP または HTTPS/SSL

セキュリティ マネージャでは、クライアントから通常の HTTP 接続を 使用するか、HTTPS/SSL 接続を要求するように CC-SG を設定できま す。この設定変更を有効とするには、CC-SG を再起動する必要があり ます。

デフォルト設定は [HTTPS/SSL] です。

- ▶ ブラウザ接続プロトコルを設定するには、以下の手順に従います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [暗号化] タブを開きます。
- 3. [HTTP] または [HTTPS/SSL] オプションを選択して、CC-SG に接 続する際にクライアントで使用するブラウザ接続プロトコルを選択 します。
- 4. [更新] をクリックして変更を保存します。

CC-SG への SSH アクセスに使用するポート番号の設定

セキュリティ マネージャでは、CC-SG への SSH アクセスに使用する ポート番号を設定できます。「 CC-SG への SSH アクセス 『319p. 』 」を参照してください。

- CC-SG への SSH アクセスに使用するポート番号を設定するには 、以下の手順に従います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [暗号化] タブで、SSH を介して CC-SG にアクセスするためのポ ート番号を [SSH サーバ ポート] フィールドに入力します。
- 3. [更新] をクリックして変更を保存します。

ログイン設定

[ログイン設定] タブにより、強力なパスワード設定およびロックアウト 設定を定義できます。



ログイン設定の表示

- 1. [管理]>[セキュリティ]を選択します。
- 2. [ログイン設定] タブをクリックします。

すべてのユーザに強力なパスワードを要求

- 1. [管理]>[セキュリティ]を選択します。
- 2. [ログイン設定] タブをクリックします。
- 3. [ユーザ全員に強力なパスワードが必要] チェックボックスを選択し ます。
- 4. [パスワードの最大文字数]を選択します。パスワードには、最大文 字数より少ない文字を含める必要があります。
- 5. [パスワード履歴の保持] を選択します。この数は、履歴に保持して 再使用できないようにする直前のパスワードの数を指定します。た とえば、[パスワード履歴の保持] が 5 に設定されている場合、ユー ザは直前の 5 つのパスワードはどれも使用できません。
- [パスワードの有効期間(日数)]を選択します。この設定日数後は、 すべてのパスワードが期限切れとなります。パスワードが期限切れ になると、ユーザは、次回にログオンするときに、新しいパスワー ドを選択するように求められます。
- 7. [強力なパスワードの条件] を選択します。
 - パスワードには少なくとも 1 文字は小文字を使用する。
 - パスワードには少なくとも 1 文字は大文字を使用する。
 - パスワードには少なくとも1文字は数字を使用する。
 - パスワードには少なくとも 1 文字は特殊文字 (感嘆符やアンパ ーサンドなど)を使用する
- 8. [更新] をクリックして変更を保存します。



CC-SG パスワードについて

すべてのパスワードは、管理者が設定したすべての条件を満たす必要が あります。強力なパスワード ルールを設定すると、それ以降のすべて のパスワードはこれらの条件を満たす必要があります。新しい条件が前 の条件より強力な場合、すべての既存のユーザは次回のログイン時にパ スワードを変更する必要があります。強力なパスワード ルールは、ロ ーカルに保存されたユーザ プロファイルにのみ適用されます。認証サ ーバ上のパスワード ルールは、認証サーバで管理されます。

さらに、パスワードにユーザ名の一部を使用する場合は、連続して 4 文字以上が一致することのないようにしてください。

強力なパスワード ルールとは、ユーザがパスワードを作成する際に、 推測が難しく、理論上よりセキュアなパスワードにするための厳密なガ イドラインを遵守するよう義務付けるものです。CC-SG のデフォルト では強力なパスワードは有効になっていません。CC スーパー ユーザ には、強力なパスワードのパラメータをすべて満たす強力なパスワード が常に必要です。

「今日のメッセージ」機能を使用して、強力なパスワード ルールがいつ 変更されるか、また新しい条件がどのようなものであるかをユーザに詳 しく知らせることができます。

ロックアウト設定

管理者は、ログイン試行回数を指定し、その回数ログインが失敗した後 で CC-SG ユーザと SSH ユーザをロックアウトできます。この機能を ローカル認証ユーザ、リモート認証ユーザ、またはすべてのユーザに対 して有効にできます。

注: デフォルトでは、admin アカウントはログインに 3 回失敗すると 5 分間ロックアウトされます。admin では、ロックアウトされる前後の 失敗ログイン試行回数は設定できません。

▶ ロックアウトを有効にするには、以下の手順に従います。

- 1. [管理]>[セキュリティ] を選択します。
- 2. [ログイン設定] タブをクリックします。
- ローカルに認証されるユーザに対してロックアウトを有効にするに は、[Lockout Enabled for Local Users] (ローカル ユーザにロックア ウトを有効にする) チェックボックスを選択します。リモートに認 証されるユーザに対してロックアウトを有効にするには、[Lockout Enabled for Remote Users] (リモート ユーザにロックアウトを有効 にする) チェックボックスを選択します。



- ユーザがロックアウトされるまでの失敗ログイン試行回数のデフォ ルトは3です。1~10までの数値を入力してこの値を変更でき ます。
- 5. ロックアウト戦略を選択します。
 - [一定期間経過後に自動解除]: ユーザが次回に再びログインできるようになるまでロックアウトされる時間を分で指定します。 デフォルト値は5分です。1分から1440分(24時間)までの時間を指定できます。指定した時間が経過すると、ユーザは再びログインできるようになります。ロックアウト時間内でも、管理者がそのユーザにCC-SGへのログインを再び許可する場合は、管理者の設定が優先されます。
 - [管理者が解除するまでロックアウト]:管理者がユーザアカウントのロックを解除するまで、ユーザはロックアウトされます。
- 6. 電子メール アドレスを [ロックアウト発生時通知電子メールアドレス] フィールドに入力します。ロックアウトが発生すると、この電子メール アドレスに通知が送信されます。このフィールドが空白のままの場合、通知は送信されません。オプション。
- 7. 電話番号を [管理者の電話番号] フィールドに入力します。この電話 番号は、ロックアウト発生時に送信される電子メール通知に表示さ れます。オプション。
- 8. [更新] をクリックして変更を保存します。
- ロックアウトを無効にするには、以下の手順に従います。

ロックアウトを無効にすると、現在 CC-SG からロックアウトされてい るすべてのユーザがログインできるようになります。

- 1. [管理]>[セキュリティ]を選択します。
- 2. [ログイン設定] タブを開きます。
- ローカルに認証されるユーザに対してロックアウトを無効にするには、[Lockout Enabled for Local Users] (ローカル ユーザにロックアウトを有効にする) チェックボックスを選択解除します。リモートに認証されるユーザに対してロックアウトを無効にするには、 [Lockout Enabled for Remote Users] (リモート ユーザにロックアウトを有効にする) チェックボックスを選択解除します。
- 4. [更新] をクリックして変更を保存します。

同一ユーザ名での複数ログインを許可

同じユーザ名による複数の同時 CC-SG セッションを許可することができます。

- 1. [管理]>[セキュリティ]を選択します。
- 2. [ログイン設定] タブをクリックします。



- CC スーパー ユーザ アカウントによる複数の同時ログインを許可する場合は、[スーパー ユーザ] チェックボックスを選択します。
- システム管理者ユーザ グループによる同時ログインを許可する 場合は、[システム管理者] チェックボックスを選択します。
- 他のすべてのユーザによる同時ログインを許可する場合は、[他のすべてのユーザ]チェックボックスを選択します。
- 3. [更新] をクリックして変更を保存します。

休止タイマーの設定

休止タイマーを設定すると、CC-SG セッションが非アクティブになっ てから、ユーザが CC-SG からログアウトされるまでの時間を指定でき ます。

ユーザがノードへの接続を開いている場合、セッションはアクティブで あると見なされ、休止タイマーの時間が経過してもユーザはログアウト されません。

- 休止タイマーを設定するには、以下の手順に従います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [ログイン設定] タブをクリックします。
- 3. 必要な時間制限を [休止タイマー] フィールドに入力します。
- 4. [更新] をクリックして変更を保存します。

ポータル

ポータル設定により、管理者は、ユーザが CC-SG にアクセスする際に 付与するロゴおよびアクセス同意書を設定できます。

ポータル設定を行うには、以下の手順に従います。

- 1. [管理]>[セキュリティ]を選択します。
- 2. [ポータル] タブを開きます。

ロゴ

ログイン ページのバナーとして使用する小さなグラフィック ファイル を CC-SG にアップロードできます。ロゴの最大サイズは 998 x 170 ピクセルです。

▶ ロゴをアップロードするには、以下の手順に従います。

- 1. [ポータル] タブの [ロゴ] 領域で [参照] をクリックします。[開く] ダイアログが表示されます。
- 2. ロゴとして使用するグラフィック ファイルをこのダイアログで選択 して、[開く] をクリックします。



- 3. [プレビュー] をクリックしてロゴをプレビューします。選択したグ ラフィック ファイルが右側に表示されます。
- 4. [更新] をクリックして変更を保存します。

制限付きサービス使用条件

ログイン画面のログイン フィールドの左に表示されるメッセージを設 定できます。これは、制限付きサービス使用条件、すなわちユーザが CC-SG にアクセスする際に同意する文書として使用されるものです。 ユーザが制限付きサービス使用条件に同意すると、そのことがログ フ ァイルおよび監査証跡レコードに記録されます。

- 制限付きサービス使用条件を CC-SG ログイン画面に追加するには、以下の手順に従います。
- [制限付きサービスであることの表示を承認することが必要] チェッ クボックスを選択して、ユーザがログイン画面の同意ボックスをオ ンにしてからでないと、そのログイン情報を入力できないようにし ます。
- 2. 次のようにしてメッセージを入力します。
 - a. バナー テキストを直接入力する場合は、[制限付きサービス同意 書メッセージ]を選択します。
 - 同意メッセージをテキストフィールドに入力します。この テキストメッセージの最大長は半角で10,000文字です。
 - [フォント] ドロップダウン メニューをクリックして、メッ セージに使用するフォントを選択します。
 - [サイズ] ドロップダウン メニューをクリックして、メッセ ージに使用するフォント サイズを選択します。
 - b. テキスト (.TXT) ファイルからメッセージをロードしたい場合 は、[Restricted Service Agreement Message File] (制限付きサー ビス同意書メッセージ ファイル) を選択します。
 - [参照] をクリックします。ダイアログ ウィンドウが開きます。
 - 使用したいメッセージが入っているテキスト ファイルをこのダイアログ ウィンドウで選択し、[開く] をクリックします。このテキスト メッセージの最大長は半角で 10,000 文字です。
 - ファイルに含まれるテキストをプレビューするには、[プレビ ュー]をクリックします。プレビューが上のバナーメッセ ージフィールドに表示されます。
- 3. [更新] をクリックして変更を保存します。次回ユーザが CC-SG に アクセスするときに、ログイン画面に更新内容が表示されます。



証明書

[証明書] タブでは、デジタル身元証明書に適用するために証明機関に送 信する証明書署名依頼 (CSR) の生成、自己署名証明書の生成、証明書 とそれらのプライベート キーのインポートおよびエクスポートを行う ことができます。

証明書タスク

注: 画面の下部のボタンは、選択した証明書オプションに応じて、[エク スポート]→[インポート]→[生成] と変わります。

- 現在の証明書とプライベートキーをエクスポートするには、以下の 手順に従います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [証明書] タブをクリックします。
- 3. [現在の証明書とプライベート キーをエクスポート] を選択します。
- [エクスポート] をクリックします。証明書が [認証] パネルに表示され、プライベート キーが [プライベート キー] パネルに表示されます。
- 5. 各パネルで、テキストを選択し、Ctrl+C を押してコピーします。次 に、必要な場所にテキストを貼り付けることができます。

証明書署名依頼を生成し、貼り付けられた証明書およびプライベートキーをインポートするには、以下の手順に従います。

CSR は、署名証明書を発行する証明書サーバに送信されます。証明書 サーバからはルート証明書もエクスポートされ、ファイルに保存されま す。証明書署名機関から署名証明書を受信したら、署名証明書、ルート 証明書、およびプライベート キーをインポートできます。

- 1. [管理]>[セキュリティ]を選択します。
- 2. [証明書] タブをクリックします。
- 3. [証明書署名依頼 (CSR) の生成] をクリックして [生成] をクリック します。[証明書署名依頼 (CSR) の生成] ウィンドウが開きます。
- 4. 必要なデータを各フィールドに入力します。
 - a. 暗号化モード:[管理]>[セキュリティ]>[暗号化] 画面で [クライ アントとサーバ間で AES 暗号化が必要] が選択されている場合 、デフォルトは AES-128 です。AES が要求されない場合は、 DES 3 がデフォルトです。
 - b. [プライベート キーの長さ]: デフォルトは 1024 です。
 - c. [有効期間 (日数)]: 最大 4 文字の数値です。
 - d. [国コード]: CSR タグが国コードです。


- e. [州または地域]: 最大 64 文字です。州または地域の完全名を入力します。短縮形は使用しないでください。
- f. [市/ローカリティ]: CSR タグがローカリティ名です。最大 64 文字です。
- g. [登録された会社名]: CSR タグが組織名です。最大 64 文字です。
- h. [事業部/部署名]: CSR タグが組織単位名です。最大 64 文字で す。
- i. [完全修飾ドメイン名]: CSR タグが通称です。
- j. [管理者の電子メール アドレス]: 証明書依頼の責任者である管 理者の電子メール アドレスを入力します。
- k. [チャレンジ パスワード]: 最大 64 文字です。
- 5. [OK] をクリックして、CSR を生成します。[証明書] 画面の該当す るフィールドに CSR とプライベート キーが表示されます。
- 6. [証明書リクエスト] ボックスでテキストを選択し、Ctrl+C を押して コピーします。ASCII エディタ (メモ帳など) を使って CSR をフ ァイルに貼り付け、拡張子 .cer で保存します。
- [プライベート キー] ボックスでテキストを選択し、Ctrl+C を押し てコピーします。ASCII エディタ (メモ帳など) を使ってプライベ ート キーをファイルに貼り付け、拡張子 .txt で保存します。
- 8. .cer ファイルを証明書サーバに送信して、署名証明書を取得します。
- 9. 証明書サーバからルート証明書をダウンロードまたはエクスポート し、拡張子.cerのファイルに保存します。これは、この次の手順 で証明書サーバから発行される署名証明書とは別の証明書です。
- 10. [CA (証明機関) のファイル] の横の [参照] をクリックし、ルート証明書ファイルを選択します。
- 証明書サーバから署名証明書を受信したら、[貼り付けられた証明書 とプライベート キーをインポート] をクリックします。
- 12. 署名証明書のテキストをコピーし、Ctrl+V を押して [証明書] ボッ クスに貼り付けます。
- 13. 前の手順で.txt ファイルとして保存したプライベート キーのテキ ストをコピーし、Ctrl+V を押して [プライベート キー] ボックスに 貼り付けます。
- 14. CC-SG で生成された CSR の場合は、[パスワード] フィールドに 「raritan」と入力します。他のアプリケーションで生成された CSR の場合は、そのアプリケーションのパスワードを使用します。



注: インポートした証明書がルートおよびサブルート CA (証明機関) の 両方によって署名されたものである場合、ルートまたはサブルート証明 書のいずれか一方のみを使用すると失敗します。これを解決するために は、ルート証明書とサブルート証明書をコピーして 1 つのファイルに 貼り付けてからインポートします。

- ▶ 自己署名証明書依頼を生成するには、以下の手順に従います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [証明書] タブをクリックします。
- 3. [自己署名証明書の生成] をクリックして [生成] をクリックします。 [自己署名証明書の生成] ウィンドウが開きます。
- 4. 必要なデータを各フィールドに入力します。
 - a. 暗号化モード:[管理]>[セキュリティ]>[暗号化] 画面で [クライ アントとサーバ間で AES 暗号化が必要] が選択されている場合 、デフォルトは AES-128 です。AES が要求されない場合は、 DES 3 がデフォルトです。
 - b. [プライベート キーの長さ]: デフォルトは 1024 です。
 - c. [有効期間 (日数)]: 最大 4 文字の数値です。
 - d. [国コード]: CSR タグが国コードです。
 - e. [州または地域]: 最大 64 文字です。州または地域の完全名を入 力します。短縮形は使用しないでください。
 - f. [市/ローカリティ]: CSR タグがローカリティ名です。最大 64 文字です。
 - g. [登録された会社名]: CSR タグが組織名です。最大 64 文字です。
 - h. [事業部/部署名]: CSR タグが組織単位名です。最大 64 文字で す。
 - i. [完全修飾ドメイン名]: CSR タグが通称です。
 - j. [管理者の電子メール アドレス]: 証明書依頼の責任者である管 理者の電子メール アドレスを入力します。
 - k. [チャレンジ パスワード]: 最大 64 文字です。
- 5. [OK] をクリックして、証明書を生成します。[証明書] 画面の該当す るフィールドに、証明書とプライベート キーが暗号化されて表示さ れます。



アクセス制御リスト

IP アクセス制御リストでは、CC-SG へのアクセスを拒否または許可す るクライアント IP アドレスの範囲が指定されます。アクセス制御リス トの各エントリは、特定の IP アドレスを持つ、特定のグループ内のユ ーザが CC-SG にアクセスできるかどうかを判断するルールとなります 。オペレーティング システム レベルで CC-SG システム全体に適用さ れるルールを設定することもできます (ユーザ グループの代わりに [System] (システム)を選択します)。ルールを作成したら、リストでそ れらを並べ替えて、適用される順序を指定できます。リスト内で上にあ るルールが、リスト内の下の位置にあるルールより優先されます。

- アクセス制御リストを表示するには、以下の手順に従います。
- 1. [管理]>[セキュリティ] を選択します。
- 2. [アクセス制御リスト] タブをクリックします。
- アクセス制御リストにルールを追加するには、以下の手順に従います。
- 1. [管理]>[セキュリティ] を選択します。
- 2. [アクセス制御リスト] タブをクリックします。
- 3. [行の追加] アイコン 「「」 をクリックして行をテーブルに追加します。
- 開始 IP 値を [開始 IP] フィールドに、終了 IP 値を [終了 IP] フ ィールドにそれぞれ入力して、ルールを適用する IP アドレスの範 囲を指定します。
- 5. [グループ] ドロップダウン矢印をクリックし、ルールを適用するユ ーザ グループを選択します。[System] (システム) を選択すると、 ルールが CC-SG システム全体に適用されます。
- 6. [アクション] ドロップダウン矢印をクリックし、[許可] または [拒 否] を選択して、IP 範囲内の指定したユーザが CC-SG にアクセス できるかどうかを指定します。
- 7. [更新] をクリックして変更を保存します。
- オペレーティング システム レベルでアクセスを許可または拒否す るルールを、アクセス制御リストに追加するには、以下の手順に従 います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [アクセス制御リスト] タブをクリックします。



- 4. 開始 IP 値を [開始 IP] フィールドに、終了 IP 値を [終了 IP] フ ィールドにそれぞれ入力して、ルールを適用する IP アドレスの範 囲を指定します。
- 5. [グループ] > [System] (システム) を選択します。
- 6. [アクション] ドロップダウン矢印をクリックし、[許可] または [拒 否] を選択して、IP 範囲内の指定したユーザが CC-SG にアクセス できるかどうかを指定します。
- 7. [更新] をクリックして変更を保存します。
- CC-SG でルールが適用される順序を変更するには、以下の手順に 従います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [アクセス制御リスト] タブをクリックします。
- 3. リスト内の上または下に移動するルールを選択します。
- 4. ルールが目的の位置に移動するまで上または下矢印をクリックしま す。
- 5. [更新] をクリックして変更を保存します。
- アクセス制御リストからルールを削除するには、以下の手順に従います。
- 1. [管理]>[セキュリティ]を選択します。
- 2. [アクセス制御リスト] タブをクリックします。
- 3. 削除するルールを選択し、[行の削除] アイコンをクリックします。
- 4. [更新] をクリックして変更を保存します。

通知マネージャ

通知マネージャを使って、外部 SMTP サーバを設定し、CC-SG から 通知を送信できるようにします。通知を使用すると、スケジュールされ たレポートを電子メールで送信したり、ユーザがロックアウトされた場 合にそれを電子メールで知らせたり、予定タスクの成否ステータスを電 子メールで知らせたりできます。「タスク マネージャ 『311p. 』」を 参照してください。SMTP サーバを設定したら、指定した受信者にテス ト メールを送信し、受信者にテストの結果を通知することもできます

外部 SMTP サーバの設定

- 1. [管理] > [通知] を選択します。
- 2. [SMTP 通知を有効にする] チェックボックスを選択します。



- 3. SMTP ホストを [SMTP ホスト] フィールドに入力します。ホスト 名のルールについては、「*用語/略語* 『2p. 』」を参照してください 。
- 4. 有効な SMTP ポート番号を [SMTP ポート] フィールドに入力しま す。
- SMTP サーバにログインするために使用できる有効なアカウント名 を [アカウント名] フィールドに入力します。オプション。このアカ ウント情報が必要かどうかを電子メール サーバの管理者に確認しま す。
- アカウント名のパスワードを [パスワード] フィールドと「パスワードの再入力] フィールドに入力します。オプション。このアカウント情報が必要かどうかを電子メール サーバの管理者に確認します。
- メッセージが CC-SG からのものであると特定する有効な電子メール アドレスを [発信] フィールドに入力します。
- 8. 送信操作が失敗した場合に電子メールを再送信する回数を [送信の 再試行] フィールドに入力します。
- 送信再試行間の経過時間 (1 ~ 60 分) を [送信の再試行の間隔 (分)] フィールドに入力します。
- SSL (Secure Sockets Layer) を使って電子メールをセキュア送信す る場合は、[SSL の使用] チェックボックスをオンにします。
- 11. [設定のテスト] をクリックして、指定した SMTP アカウントにテ スト電子メールを送信します。電子メールが到着したかを確認して ください。
- 12. [設定の更新] をクリックして変更を保存します。

タスク マネージャ

タスク マネージャを使って、CC-SG のタスクを毎日、毎週、毎月、ま たは毎年のペースでスケジュールできます。タスクは、1 回のみ実行さ れるようにスケジュールすることもできますが、指定された曜日に定期 的に実行したり、特定の間隔を置いて実行するようにスケジュールする こともできます。たとえば、デバイスのバックアップを 2 週間おきに 金曜日にスケジュールしたり、1 人または複数の受信者に毎週月曜日に 電子メールが送信されるようにするなどです。

注: タスク マネージャは、個々のクライアント PC の時間ではなく、 CC-SG で設定されているサーバ時間をスケジュールに使用します。サ ーバ時間は、各 CC-SG ページの右上隅に表示されます。



タスクのタイプ

次のようなタスクにスケジュールを設定できます。

- Active Directory 同期
- **CC-SG** のバックアップ
- デバイス設定のバックアップ (個々のデバイスまたはデバイスのグ ループ)
- デバイス管理の一時停止と再開
- デバイス設定のコピー (個々のデバイスまたはデバイスのグループ)
- グループ パワー制御
- 電源コンセント制御
- ログの消去
- デバイスの再起動
- デバイス設定のリストア (デバイス グループには適用されません)
- デバイス ファームウェアのアップグレード (個々のデバイスまたは デバイスのグループ)
- すべてのレポートの生成

連続したタスクのスケジュール

予測通りの動作が発生したことを確認するために、タスクを連続してス ケジュールする場合があります。たとえば、特定のデバイス グループ にデバイス ファームウェアのアップグレード タスクをスケジュールす る場合、その直後に資産管理レポート タスクをスケジュールすること により、正しいバージョンのファームウェアがアップグレードされたこ とを確認できます。

タスクの電子メール通知

タスクの完了時に、指定した受信者に電子メール メッセージが送信されるようにできます。通知マネージャで、電子メールの送信場所を指定し、SSL により電子メールをセキュアに送信することを選択できます。 「*通知マネージャ*『310.』」を参照してください。



スケジュールされたレポート

スケジュールされたレポートは、指定した受信者に電子メール送信され ます。電子メール レポートのバージョンとして CSV か HTML のいず れかを指定できます。

[終了] ステータスのすべてのレポートは CC-SG に 30 日間 HTML 形 式で保存されます。[レポート] メニューの [スケジュールされたレポー ト] を選択した場合にのみ、終了したレポートを HTML 形式で表示で きます。「*スケジュールされたレポート* **『244**p. **』**」を参照してくださ い。

タスクの検索および表示

選択した基準でフィルタされたリストでタスクを表示できます。各タス クについて詳細および履歴を表示できます。

注: タスクが変更または更新された場合、変更または更新される前の履 歴は適用されなくなり、[最後に実行した日付] が空白になります。

タスクを表示するには、以下の手順に従います。

- 1. [管理]>[タスク] を選択します。
- 2. タスクを検索するには、上下の矢印ボタンを使って、表示するタス クの日付の範囲を選択します。
- 3. リストから 1 つまたは複数 (Ctrl+ クリック) のタスク、ステータ ス、または所有者を選択してリストをさらに絞り込むこともできま す。
- 4. [タスクの表示] をクリックして、タスクのリストを表示します。
- タスクの履歴を表示するには、以下の手順に従います。
 - タスクを選択して、[タスクの履歴]をクリックします。
- タスクの詳細を表示するには、以下の手順に従います。
 - タスクをダブルクリックして、タスクの詳細が表示されるダイ アログを開きます。

タスクのスケジュール

このセクションでは、スケジュール可能なほとんどのタスクについて説 明します。デバイス ファームウェアのアップグレード スケジュールの 詳細は、「デバイス ファームウェアのアップグレードのスケジュール タスク 『316p. の"デバイス ファームウェアのアップグレードのスケジ ュール"参照 』」を参照してください。

- タスクをスケジュールするには、以下の手順に従います。
- 1. [管理]>[タスク] を選択します。



- 2. [新規] をクリックします。
- [メイン] タブに、タスクの名前と説明を入力します。名前には、1 ~ 32 文字の半角英数字またはアンダースコアを使用できます。スペースは使用できません。
- 4. [タスクのデータ] タブをクリックします。
- [タスクの操作] ドロップダウン メニューをクリックし、スケジュー ルするタスク。データ入力が必要になるフィールドは、選択したタ スクによって異なります。各タスクの詳細は、次のセクションを参 照してください。
 - Active Directory 同期: 「全 AD モジュールの同期 『223p. 』
 」を参照してください。
 - CommandCenter のバックアップ:「CC-SG のバックアップ『 248p. 』」を参照してください。
 - デバイス設定のバックアップ:「デバイス設定のバックアップ『 94p. 』」を参照してください。
 - デバイス管理の一時停止と再開:個別デバイスの一時停止および 再開については、「CC-SG のデバイス管理の一時停止『100p.』 」および「管理の再開『101p.の"デバイスの管理の再開"参照』 」を参照してください。複数のデバイスまたはデバイス グルー プを一時停止または再開するタスクのスケジュールの詳細は、 「スケジュールされたタスクを使用したデバイス管理の一時停 止と再開『101p.』」を参照してください。
 - デバイス設定のコピー:「デバイス設定のコピー『99p.』」を 参照してください。
 - グループパワー制御:「ノード グループ パワー制御」を参照してください。
 - 電源コンセント制御: 『CC-SG ユーザ ガイド』を参照してください。
 - Power IQ の同期:「Power IQ および CC-SG の同期 『381p. 』 」を参照してください。
 - ログの消去:「ログ アクティビティの設定 『278p. 』」を参照 してください。
 - デバイスの再起動:「デバイスの再起動 『100p. 』」を参照して ください。
 - デバイス設定のリストア:「デバイス設定のリストア 『95p. 』 」を参照してください (デバイス グループには適用されません)
 - デバイス ファームウェアのアップグレード (個々のデバイスまたはデバイスのグループ):「デバイス ファームウェアのアップグレードのスケジュール 『316p. 』」を参照してください。



- すべてのレポートの生成:「レポート 『232p. 』」を参照してく ださい。
- 6. [再発] タブをクリックします。デバイス ファームウェアのアップグ レード タスクでは、[定期実行] タブは無効になっています。
- 7. [期間] フィールドで、スケジュールしたタスクを繰り返す間隔に対応するラジオ ボタンをクリックします。
 - a. 1 回のみ: 上下の矢印を使って、タスクの開始時刻を選択します。
 - b. 定時間隔:上下の矢印を使って、タスクの開始時刻を選択します。タスクの実行回数を [繰り返し回数] フィールドに入力します。反復の間隔を [繰り返し間隔] フィールドに入力します。ドロップダウン メニューをクリックして、時間の単位をリストから選択します。タスクを選択した間隔で無限に実行するか、またはタスクを変更または削除するまで実行するように設定するには、[進行中 タスクが変更されるか、キャンセルされるまで。]チェックボックスをオンにします。[繰り返し回数] が無効になります。[繰り返し間隔] を設定します。
 - c. 日単位: タスクを毎日繰り返す場合は、[毎日] ラジオ ボタンを クリックします。毎週月曜日から金曜日までタスクを繰り返す 場合は、[平日] ラジオ ボタンをクリックします。
 - d. 週単位:上下の矢印を使って、タスクを何週おきに実行するかを 選択し、タスクが実行される曜日の横のチェックボックスを選 択します。
 - e. 月単位:タスクが実行される日を[日]フィールドに入力し、指定した日にタスクが実行される月の横のチェックボックスを選択します。
 - f. 年単位: ドロップダウン メニューをクリックし、タスクが実行 される月をリストから選択します。上下の矢印を使って、タス クが実行される月の日を選択します。
- 8. 日単位、週単位、月単位、年単位で実行されるタスクの場合、タス クの開始時刻と終了時刻を [定期実行期間] セクションに追加する必 要があります。上下の矢印を使って開始時刻と開始日を選択します。タスクを無制限に繰り返す場合は、終了日なしの横のラジオ ボタ ンをクリックします。あるいは終了日の横のラジオ ボタンをクリッ クし、上下の矢印を使ってタスクが反復を停止する日付を選択します。
- 9. [再試行] タブをクリックします。
- 10. タスクが失敗した場合、CC-SG ではタスクを [再試行] タブで指定 したとおりに後から再試行できます。CC-SG でタスクを再試行す る回数を [再試行の回数] フィールドに入力します。再試行の間隔を [再試行の間隔] フィールドに入力します。ドロップダウン メニュー をクリックして、時間の単位をリストから選択します。



重要: SX または KX デバイスをアップグレードするタスクをスケジュールする場合、[再試行の間隔] を 20 分より長くします。これらのデバイスを正常にアップグレードするには、約 20 分かかるためです。

- 11. [通知] タブをクリックします。
- 12. タスクの完了または失敗時に通知が送信される電子メールアドレス を指定します。デフォルトでは、現在ログインしているユーザの電 子メール アドレスが有効になります。ユーザの電子メールアドレス はユーザ プロファイルで設定されています。別の電子メール アド レスを追加するには、[追加]をクリックし、開くウィンドウでその 電子メール アドレスを入力して [OK] をクリックします。デフォル トでは、タスクが成功すると電子メールが送信されます。失敗した タスクの通知を受信者に送信する場合は、[失敗時]を選択します。
- 13. [OK] をクリックして変更を保存します。

デバイス ファームウェアのアップグレードのスケジュール

KX や SX など、デバイス グループ内の同じタイプの複数のデバイス をアップグレードするタスクをスケジュールできます。タスクが開始す ると、[レポート]>[スケジュールされたレポート] メニューのデバイス ファームウェアのアップグレード レポートでアップグレード ステータ スをリアルタイムで参照できます。[通知] タブでオプションを指定した 場合、このレポートは電子メールでも送信されます。

各デバイスのアップグレード予想時間については、『Raritan User Guide 』を参照してください。

- デバイス ファームウェアのアップグレードをスケジュールするには 、以下の手順に従います。
- 1. [管理]>[タスク] を選択します。
- 2. [新規] をクリックします。
- 3. [メイン] タブに、タスクの名前と説明を入力します。選択した名前 は、タスクと、タスクに関連付けられたレポートを識別するために 使用されます。
- 4. [タスクのデータ] タブをクリックします。
- 5. デバイス アップグレードの詳細を指定します。
 - a. [タスクの操作]: [デバイス ファームウェアのアップグレード] を 選択します。
 - b. [デバイス グループ]: アップグレードするデバイスを含むデバイス グループを選択します。



- C. [デバイス タイプ]: アップグレードするデバイスのタイプを選択します。複数のデバイス タイプをアップグレードする必要がある場合、タイプごとにタスクをスケジュールする必要があります。
- d. [同時アップグレード]: アップグレードのファイル転送の部分を 同時に開始するデバイスの数を指定します。最大値は 10 です 。ファイル転送が完了するたびに、新しいファイル転送が開始 し、一度に行われる同時転送の数が最大数を超えることはあり ません。
- [アップグレード ファイル]: アップグレード後のファームウェ ア バージョンを選択します。選択したデバイス タイプに適し たアップグレード ファイルだけがオプションとして表示されま す。
- 6. アップグレードの期間を指定します。
 - a. [開始日付/時刻]: タスクを開始する日付と時刻を選択します。開 始日付/時刻は、現在の日付/時刻より後にする必要があります。
 - b. [制限付きアップグレード ウィンドウ] および [最新アップグレ ードの開始日付/時刻]: 特定の時間ウィンドウ内にすべてのアッ プグレードを完了する必要がある場合、これらのフィールドを 使用して、新しいアップグレードを開始できなくする日付と時 刻を指定します。[最新アップグレードの開始日付/時刻] フィー ルドを有効にするには、[制限付きアップグレード ウィンドウ] を選択します。
- 7. アップグレードするデバイスとその順番を選択します。優先順位の 高いデバイスを、リストの上部に配置します。
 - a. [利用可能] リストで、アップグレードする各デバイスを選択し 、[追加] をクリックしてそのデバイスを [選択中] リストに移動 します。
 - b. [選択中] リストで、デバイスを選択し、矢印ボタンを使用して アップグレードを進める順番にデバイスを移動します。
- 8. 失敗したアップグレードを再試行するかどうかを指定します。
 - a. [再試行] タブをクリックします。
 - b. [再試行の回数]: CC-SG が失敗したアップグレードを再試行す る回数を入力します。
 - c. [再試行の間隔]: 次の再試行を行うまでの時間を入力します。デ フォルト時間は 30、60、および 90 分です。最適な再試行間 隔があります。
- 成功または失敗の通知を受信する電子メール アドレスを指定します 。デフォルトでは、現在ログインしているユーザの電子メール アド レスが有効になります。ユーザの電子メールアドレスはユーザ プロ ファイルで設定されています。
 - a. [通知] タブをクリックします。



- b. [追加] をクリックし、開いたウィンドウでその電子メール アド レスを入力して [OK] をクリックします。
- c. アップグレードが失敗した場合に電子メールを送信する場合は 、[失敗時]を選択します。
- d. すべてのアップグレードが正常に完了した場合に電子メールを 送信する場合は、[成功時]を選択します。
- 10. [OK] をクリックして変更を保存します。

タスクが実行を開始すると、スケジュールされた期間中いつでもデ バイス ファームウェアのアップグレード レポートを開いて、アッ プグレードのステータスを参照できます。「デバイス ファームウェ アのアップグレード レポート 『245p. 』」を参照してください。

スケジュールしたタスクの変更

スケジュールしたタスクをその実行前に変更できます。

- スケジュールしたタスクを変更するには、以下の手順に従います。
- 1. 変更するタスクを選択します。
- 2. [編集] をクリックします。
- 必要に応じてタスク仕様を変更します。タブについては、「タスクの スケジュール 『313p. 』」と「デバイス ファームウェアのアップグ レードのスケジュール タスク 『316p. の"デバイス ファームウェア のアップグレードのスケジュール"参照 』」を参照してください。
- 4. [更新] をクリックして変更を保存します。

タスクのスケジュール変更

タスク マネージャの「名前を付けて保存」機能を使用すると、すでに終 了したタスクを再度実行するようスケジュールすることができます。終 了したタスクに類似した新しいタスクを作成する場合にも便利です。

- ▶ タスクのスケジュールを変更するには、以下の手順に従います。
- 1. [管理]>[タスク] を選択します。
- 2. [タスク マネージャ] ページで、スケジュール変更するタスクを選択 します。絞込み条件を使用してタスクを検索します。
- 3. [名前を付けて保存] をクリックします。
- 4. [タスクを名前を付けて保存] ウィンドウが開きます。それぞれのタ ブには前に設定されたタスクの情報が入力されています。
- 5. 必要に応じてタスク仕様を変更します。タブについては、「タスクの スケジュール 『313p. 』」と「デバイス ファームウェアのアップグ レードのスケジュール タスク 『316p. の"デバイス ファームウェア のアップグレードのスケジュール"参照 』」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。



別のタスクと類似したタスクのスケジュール

前に設定されたタスクを「テンプレート」として使用し、同様の仕様を 持つ新しいタスクをスケジュールすることができます。

- 別のタスクと類似したタスクをスケジュールするには、以下の手順 に従います。
- 「*タスクのスケジュール変更* 『318p. 』」を参照してください。

タスクの削除

タスクを削除して CC-SG 管理から除外できます。現在実行中のタスク を削除することはできません。

- タスクを削除するには、以下の手順に従います。
- タスクを選択して、[削除]をクリックします。

CC-SG への SSH アクセス

CC-SG の SSH (v2) サーバのコマンドライン インタフェースへのアク セスには、Putty または OpenSHH クライアントなどのセキュア シェ ル (SSH) クライアントを使用します。CC-SG コマンドのサブセットの みが SSH から提供され、デバイスと CC-SG 自体を管理します。

SSH クライアントのユーザは CC-SG で認証されます。このとき、既 存の認証および承認ポリシーが SSH クライアントに適用されます。 SSH クライアントで利用できるコマンドは、その SSH クライアント ユーザが属しているユーザ グループの許可に応じて決定されます。

SSH を使って CC-SG にアクセスしている管理者は、CC スーパーユ ーザ SSH ユーザをログアウトすることはできませんが、システム管理 者を含む他のすべての SSH クライアント ユーザをログアウトできま す。

- SSH を介して CC-SG にアクセスするには、次の手順に従います
- 1. PuTTY などの SSH クライアントを起動します。
- 2. CC-SG の IP アドレスを指定します。
- SSH ポート番号を指定します。デフォルトは 22 です。セキュリ ティ マネージャで SSH アクセス用にポートを設定できます。「セ キュリティ マネージャ 『298p. 』」を参照してください。
- 4. 接続を開きます。
- 5. 自分 CC-SG のユーザ名とパスワードでログインします。
- 6. シェル プロンプトが表示されます。



▶ すべての SSH コマンドを表示するには、以下の手順に従います。

 シェル プロンプトから Is を入力して、利用可能なすべてのコマン ドを表示します。

# 192.168.32.58	- PuTTY		
login as: admir admin@192.168.3 Welcome to CC-S	1 32.58's password: 3G		~
[CommandCenter	admin]\$ ls		
?	activeports	activeusers	
backupdevice	clear	connect	
console_cmd	copydevice	disconnect	
entermaint	exit	exitmaint	
grep	help	list_interfaces	
list_nodes	list_ports	listbackups	
listdevices	listfirmwares	listinterfaces	
listnodes	listports	logoff	
ls	more	pingdevice	
restartcc	restartdevice	restoredevice	
shutdowncc	ssh	su	
ul	upgradedevice	user list	
[CommandCenter	admin] \$ 📙	—	

SSH コマンドのヘルプの表示

すべてのコマンドの限定的ヘルプを一度に表示できます。1 度に 1 つ のコマンドの詳細ヘルプを表示することもできます。

- 1 つの SSH コマンドのヘルプを表示するには、以下の手順に従い ます。
- シェル プロンプトで、ヘルプが必要なコマンドを入力し、その後に スペースと -h を続けます。たとえば、 connect -h
- 2. コマンド、パラメーター、使用法に関する説明が画面に表示されます。
- すべての SSH コマンドのヘルプを表示するには、以下の手順に従います。
- 1. シェル プロンプトで次のコマンドを入力します。 help
- 2. それぞれの SSH コマンドの簡単な説明と例が画面に表示されます。



SSH コマンドとパラメーター

以下の表には、SSH で利用可能なすべてのコマンドをリストしてあり ます。それぞれのコマンドを使用するには、CC-SG で適切な権限が必 要です。

ー部のコマンドには、その実行のために入力する必要がある追加パラメ ーターがあります。コマンドの入力方法についての詳細は、「コマンド のヒント 『323p. 』」を参照してください。

アクティブ ポートをリストする場合:

activeports

アクティブ ユーザをリストする場合:

activeusers

▶ デバイス設定をバックアップする場合:

backup device <[-host <host>] | [-id <device_id>]>
backup name [description]

▶ 画面を消去する場合:

clear

シリアル ポートとの接続を確立する場合:

<port_name> または <device_name> にスペースが入っている場合は
、名前を引用符で囲みます。

```
connect [-d <device_name>] [-e <escape_char>] <[-i
<interface id>] | [-n <port name>] | [port id]>
```

デバイス設定をあるデバイスから別のデバイスにコピーする場合。 ポート数が同じ SX デバイスの場合のみ。

copydevice <[-b <backup_id>] | [source_device_host]>
target_device_host

ポート接続を閉じる場合:

disconnect <[-u <username>] [-p <port_id>] [-id <connection id>]>

メンテナンス モードを起動する場合:

entermaint minutes [message]

メンテナンス モードを終了する場合:

exitmaint

パイプ出力ストリームからテキストを検索する場合:



```
grep search_term
```

```
すべてのコマンドのヘルプ画面を表示する場合:
help
```

利用可能なデバイス設定バックアップをリストする場合:
 listbackups <[-id <device id>] | [host]>

▶ 利用可能なデバイスをリストする場合:

listdevices

アップグレード可能なファームウェア バーションをリストする場合:
 listfirmwares [[-id <device_id>] | [host]]
 すべてのインタフェースをリストする場合:

listinterfaces [-id <node id>]

▶ すべてのノードをリストする場合:

listnodes

すべてのポートをリストする場合:
 listports [[-id <device id>] | [host]]

ユーザをログオフする場合:
 logoff [-u <username>] message

すべてのコマンドをリストする場合:
 1s

ページングを指定する場合:more [-p <page_size>]

デバイスを ping する場合:
 pingdevice <[-id <device id>] | [host]>

CC-SG を再起動する場合:
 restartcc minutes [message]

デバイスを再起動する場合:
 restartdevice <[-id <device_id>] | [host]>

▶ デバイス設定をリストアする場合:



```
restoredevice <[-host <host>] | [-id <device_id>]>
[backup id]
```

CC-SG をシャットダウンする場合:

shutdowncc minutes [message]

▶ SX デバイスとの SSH 接続を開く場合:

ssh [-e <escape char>] <[-id <device id>] | [host]>

▶ ユーザを変更する場合:

su [-u <user_name>]

デバイス ファームウェアをアップグレードする場合:

upgradedevice <[-id <device_id>] | [host]>

▶ すべての現行ユーザをリストする場合:

userlist

SSH セッションを終了する場合:

exit

コマンドのヒント

ことはできません。

- upgradedevice など、IP アドレスを渡すコマンドでは、IP アドレスの代わりにホスト名を使用することもできます。ホスト名のルールについては、「用語/略語 『2p.』」を参照してください。
- copydevice と restartdevice コマンドは、一部の Raritan デ バイスにしか適用しません。Dominion SX および IPMI サーバでは 、これらのコマンドはサポートされません。
- 四角で囲まれたコマンドの部分はオプションです。コマンドのこの 部分は使用しなくてもかまいません。
- コマンドによっては、「Or」記号 ()) で分けられた 2 つのセグメントを持つものがあります。
 いずれか 1 つを必ず入力しなければいけませんが、両方を入力する
- コマンドの山カッコで囲まれた部分は、入力必須のテキストを示します。山カッコは、入力しないでください。たとえば、

コマンド構文	デバイス ID 値	入力
ssh -id <device_id></device_id>	100	ssh -id 100

デフォルトのエスケープ文字はチルドとそれに続くピリオドです。
 たとえば、

~ .



エスケープ文字と終了コマンドの使用法についての詳細は、「SSH 接続の終了 『327p. 』」を参照してください。

Linux ターミナルまたはクライアントではエスケープ文字の使用で問 題が発生することがあります。Raritan では、ポート接続を確立する ときに新しいエスケープ文字を定義することを推奨します。コマンド は、connect [-e <escape_char>] [port_id] です。たとえば 、ID が 2360 のポートに接続するときにエスケープ文字として "m" を定義するには、「connect -e m 2360」と入力します。

シリアル対応デバイスへの SSH 接続の作成

デバイスに管理操作を実行するために、シリアル対応デバイスへの SSH 接続を作成することができます。接続後は、そのシリアル対応デ バイスでサポートされている管理コマンドを利用できます。

注: 接続する前に、シリアル対応デバイスが CC-SG に追加されている ことを確認してください。

1. 「listdevices」と入力して、シリアル対応デバイスが CC-SG に 追加されていることを確認します。

🛃 192. 168. 51. 1	24 - PuTTY		
[CommandCente	er ccRoot]\$.	listdevices	^
Device ID	Appliance	IP Address	Туре
1331	KX-203	192.168.53.203	Dominion KX
1320	KX224	192.168.51.224	Dominion KX
1303	CC2.01	192.168.52.171	Generic Device
1360	Channel 32	192.168.52.171	PowerStrip
1370	SX-229	192.168.51.229	Dominion SX
1311	IPMI-22	192.168.51.22	IPMI Server
1300	AD-92	192.168.51.92	Generic Device
1302	KSX223-1	192.168.51.223	Dominion KSX
1304	aPS8	192.168.51.223	PowerStrip
1330	KX-199	192.168.53.199	Dominion KX
1305	PC17	192.168.51.17	Generic Device 📃
[CommandCente	er ccRoot]\$		*



 [ssh -id <device_id>」と入力して、デバイスに接続します。
 たとえば、上記の例では、「ssh -id 1370」と入力すると、SX-229 に 接続できます。



SSH を使用してシリアル アウト オブ バンド インタフェース経由で ノードに接続

SSH を使用すると、関連のシリアル アウト オブ バンド インタフェ ースを介してノードに接続できます。SSH 接続はプロキシ モードにな ります。

1. 「listinterfaces」と入力して、ノード ID とその関連インタフ ェースを表示します。

📌 192.168.32.5	8 - PuTTY			
[CommandCenter	r admin]\$			^
[CommandCenter	r admin]\$ listinter	faces		
Interface ID	Interface name	Interface type	Node ID	Node name
100	Serial Target 1	Serial interface	100	Serial Target 1
136	Admin	Serial interface	100	Serial Target 1
140	Serial Target 4	Serial interface	131	Serial Target 4
104	Serial Target 3	Serial interface	104	Serial Target 3
103	Admin	Serial interface	103	Admin
108	Serial Target 2	Serial interface	108	Serial Target 2 🛁
[CommandCenter	r admin]\$			~

 「connect -i <interface_id>」と入力して、インタフェースに 関連したノードに接続します。

🛃 192.168.32.58	- PuTTY									×
100	Serial	Target	1	Serial	interface	100	Serial	Target	1	^
136	Admin			Serial	interface	100	Serial	Target	1	
140	Serial	Target	4	Serial	interface	131	Serial	Target	4	
104	Serial	Target	3	Serial	interface	104	Serial	Target	3	
103	Admin			Serial	interface	103	Admin			
108	Serial	Target	2	Serial	interface	108	Serial	Target	2	
[CommandCenter	admin]\$	connect	-i	100						-
Connecting to p	ort									~

3. 表示されるプロンプトで、特定のコマンドまたはエイリアスを入力 できます。



Ch 15: 高度な管理

コマンド	エイリア ス	説明
quit	d	接続を終了して、SSH プロンプトに戻りま す。
get_write	дм	書き込みアクセスを取得します。SSH ユー ザに、ターゲット サーバてコマンドを実行 することを許可します。ブラウサ ユーザは 処理を表示することしかできません。
get_history	gh	履歴を入手します。ターゲット サーバでの 過去数回のコマンドとその結果を表示しま す。
send_break	sb	ブレークを送信します。ブラウザ ユーザに よって起動されたターゲット サーバのルー プをブレークします。
help	?,h	ヘルプ画面を表示します。



SSH 接続の終了

CC-SG のみを対象にした SSH 接続を作成することもできますし、 CC-SG への接続を作成後、CC-SG の管理対象であるポート、デバイス 、またはノードへの接続を作成することもできます。これらの接続の終 了方法は、終了させる箇所に応じて異なります。

▶ CC-SG への SSH 接続全体を終了するには、以下の手順に従います。

このコマンドは、CC-SG を介したポート、デバイス、ノードへの接続 を含め、SSH 接続全体を終了します。

• プロンプトで次のコマンドを入力し、Enter キーを押します。 exit

CC-SG への接続を維持しながら、ポート、デバイス、またはノードへの接続を終了するには、以下の手順に従います。

エスケープ文字を使用すると、CC-SG への接続を開いたままにしてポ ート、デバイス、またはノードへの接続を終了することができます。 デフォルトのエスケープ文字はチルドとそれに続くピリオドです。

- プロンプトで次のコマンドを入力し、Enter キーを押します。
- ~.

Linux ターミナルまたはクライアントではエスケープ文字の使用で問題が発生することがあります。Raritan では、ポート接続を確立する ときに新しいエスケープ文字を定義することを推奨します。コマンドは、connect [-e <escape_char>] [port_id] です。たとえば、ID が 2360 のポートに接続するときにエスケープ文字として "m" を定義するには、「connect -e m 2360」と入力します。



シリアル管理ポート

CC-SG のシリアル管理ポートは、Dominion SX または KSX などの Raritan シリアル デバイスに直接接続できます。

SX や KSX には、ハイパーターミナルや PuTTY など、端末エミュレ ーション プログラムを使用して IP アドレス経由で接続できます。端 末エミュレーション プログラムで、SX または KSX のボーレートと同 じボーレートを設定します。

▶ SX 要件:

ASCSDB9F アダプタを使用して CC-SG ユニットを SX に接続します 。既定の SX ポート設定の 9600bps、パリティ = なし/8、フロー制御 = なし、エミュレーション = VT100 を使用します。

▶ V1 シリアル管理ポート



E1 シリアル管理ポート



または





端末エミュレーション プログラム

ハイパーターミナルは、多くの Windows OS で使用できます。ハイパ ーターミナルは、Windows Vista では使用できません。

PuTTY は無料のプログラムで、インターネットからダウンロードできます。

CC-SG シリアル ナンバーの検出

- CC-SG シリアル ナンバーを検出するには、以下の手順に従います。
- 1. Admin Client にログインします。
- 2. [ヘルプ]>[バージョン情報]を選択します。
- 3. 新しいウィンドウが開き、CC-SG シリアル ナンバーが表示されま す。

Web サービス API

Web サービス API クライアントを CC-SG に追加するまえに、エンド ユーザ使用条件に同意する必要があります。最大で 5 つの WS-API ク ライアントを追加できます。API の使用法についての詳細は、『CC-SG Web Services API Guide (CC-SG Web サービス API ガイド)』を参照し てください。

- Web サービス API を追加するには、以下の手順に従います。
- 1. [アクセス] > [Web サービス API の追加] を選択します。このオプ ションを利用できるユーザは、CC 設定および制御権限を持つユー ザのみです。
- 2. エンド ユーザ使用条件を読みます。
 - テキストをコピーして貼り付けてから保存するか、[Secure Gateway] > [印刷] を選択することができます。
 - 設定が完了すると、この使用条件は [アクセス] メニューで参照 できます。
- 3. [同意] をクリックします。[新しい Web サービス API 設定] ウィ ンドウが開きます。
- 4. Web サービス クライアントに関する必要なデータを入力します。
 - [Web サービス クライアント名]: 最大 64 文字です。
 - [ライセンス キー]: Raritan から提供されたライセンス キーです。各 CC-SG ユニットに一意のライセンス キーが必要です。
 - [IP アドレス/ホスト名]: 最大 64 文字です。



- [HTTPS Web サービス ポート]: 読み取り専用フィールドです。 CC-SG では、信頼が確立されると、ポート 9443 が使用され ます。
- [ライセンスされたベンダ名]: 最大 64 文字です。
- 5. 自己署名証明書を生成します。
 - a. 暗号化モード:[管理]>[セキュリティ]>[暗号化] 画面で [クライ アントとサーバ間で AES 暗号化が必要] が選択されている場合 、デフォルトは AES-128 です。AES が要求されない場合は、 DES 3 がデフォルトです。
 - b. [プライベート キーの長さ]: デフォルトは 1024 です。
 - c. [有効期間 (日数)]: 最大 4 文字の数値です。
 - d. [国コード]: CSR タグが国コードです。
 - e. [州または地域]: 最大 64 文字です。州または地域の完全名を入 力します。短縮形は使用しないでください。
 - f. [市/ローカリティ]: CSR タグがローカリティ名です。最大 64 文字です。
 - g. [登録された会社名]: CSR タグが組織名です。最大 64 文字です。
 - h. [事業部/部署名]: CSR タグが組織単位名です。最大 64 文字で す。
 - i. [完全修飾ドメイン名]: CSR タグが通称です。
 - j. [管理者の電子メール アドレス]: 証明書依頼の責任者である管 理者の電子メール アドレスを入力します。
 - k. [チャレンジ パスワード]: 最大 64 文字です。

注: チャレンジ パスワードは、証明書を生成するために CC-SG の 内部で使用されるものです。覚えておく必要はありません。

- パスワード: 鍵ストアのパスワードを入力します。このパスワードを使用して、手順7 で保存する.P12 ファイルを開きます。 代わりに、生成された証明書をコピーして独自の鍵ストアにインポートする場合は、この鍵ストアのパスワードを覚えておく必要はありません。
- 6. [証明書の生成] をクリックします。[証明書] ボックスにテキストが 表示されます。
- 7. [ファイルに保存] をクリックして、証明書を .P12 ファイルに保存 します。または、生成された証明書をコピーし、独自の鍵ストアに インポートします。
- 8. [追加] をクリックして変更を保存します。



CC-NOC

CC-SG リリース 4.2 では、CC-SG から CC-NOC にアクセスできま せん。



Ch 16 診断コンソール

診断コンソールは、CC-SG へのローカル アクセスを提供する非グラフ ィカルのメニューベースのインタフェースです。診断コンソールには、 シリアル ポートまたは KVM ポートからアクセスできます。「VGA/キ ーボードツマウス ポートからの診断コンソールへのアクセス 『332p. 』 」を参照してください。また PuTTY や OpenSSH クライアントなどの セキュア シェル (SSH) クライアントから診断コンソールにアクセスで きます。「SSH による診断コンソールへのアクセス『332p. の"SSH を 介した診断コンソールへのアクセス"参照 』」を参照してください。

診断コンソールには、次の2つのインタフェースがあります。

- 1. Status Console: 「*Status Console について* **『333**p. **』**」を参照してください。
- Administrator Console について 『340p. 』」を参照してください。

注: SSH 経由で診断コンソールにアクセスすると、Status Console と Administrator Console では SSH クライアントの表示設定とキーボード バインドが継承されます。これらの表示設定は、本書と異なる場合があ ります。

この章の内容

診断コンソールへのアクセス	
Status Console	
Administrator Console	340

診断コンソールへのアクセス

VGA/キーボード/マウス ポートからの診断コンソールへのアクセス

- 1. VGA モニタと PS2 キーボード、さらにマウスを CC-SG ユニッ トの背面に接続します。
- 2. Enter キーを押すと、画面にログイン プロンプトが表示されます。

SSH を介した診断コンソールへのアクセス

- 1. CC-SG にネットワーク接続されたクライアント PC で PuTTY な どの SSH クライアントを起動します。
- 2. CC-SG の IP アドレスまたは IP ホスト名を指定します (CC-SG が DNS サーバに登録されている場合)。



- ポートに 23 を指定します。デフォルトの SSH ポートは 22 です 。ポートを 23 に変更しない場合、SSH クライアントは、診断コ ンソールではなく CC-SG のコマンド ライン インタフェースにア クセスします。
- 接続するためのボタンをクリックします。ウィンドウが開き、ログ インのプロンプトが表示されます。

Status Console

Status Console について

- Status Console を使用すると、CC-SG、CC-SG によって使用され るさまざまなサービス、接続されたネットワークのヘルスを確認で きます。
- デフォルトでは、Status Console はパスワードを必要としません。
- CC-SG を、Web インタフェースを介して Status Console 情報を 提供するように設定できます。Web Status Console 関連のオプショ ンを有効にする必要があります。「Web ブラウザからの Status Console へのアクセス『334p.』」を参照してください。Web 上 の Status Console 情報はアカウントおよびパスワードで保護でき ます。

Status Console へのアクセス

Status Console 情報を表示するには、VGA/キーボード/マウス ポート 、SSH、または Web ブラウザを使用する方法があります。

VGA/キーボード/マウス ポートまたは SSH からの Status Console へのアク セス

- VGA/キーボード/マウス ポートまたは SSH から Status Console にアクセスするには、以下の手順に従います。
- 診断コンソールにアクセスします。「診断コンソールへのアクセス 『332p. 』」を参照してください。
- 2. ログイン プロンプトに「status」と入力します。
- 3. 現在のシステム情報が表示されます。



Web ブラウザからの Status Console へのアクセス

Web 経由で Status Console 情報を取得するには、関連するオプション を診断コンソールで有効にする必要があります。また、Web サーバが 稼働し機能している必要があります。

- 1: 診断コンソールで、Web Status Console 関連のオプションを有効にします。
- 1. [Operation] > [Diagnostic Console Config] を選択します。
- 2. [ポート] リストで [Web] を選択します。
- 3. [Status] リストで、Web の横の [Status] チェックボックスを選択 します。
- 4. [保存] をクリックします。
- 2: Web ブラウザから Status Console にアクセスします。
- サポートされているインターネット ブラウザを使用して URL を「 http(s): //<IP_address>/status/」と入力します。
 <IP_address> は、CC-SG の IP アドレスです。/status の後の スラッシュ (/) は必須です。たとえば「https: //10.20.3.30/status/」のように入力します。
- 2. ステータス ページが開きます。このページには、Status Console と同じ情報が含まれます。



Status Console 情報

VGA/キーボード/マウス ポートまたは SSH からの Status Console

ログイン プロンプトで「status」と入力すると、読み取り専用の Status Console が表示されます。

Mon Dec 2008-12-01 EST CommandCenter S	ecure Gateway	12:54:08 EST -05	60
CommandCenter Secure Gateway			
Centralized access and control for your	global IT int	frastructure	
L System Information:			
Host Name : CC-SG-Demo.raritan.c	om		
CC-SG Version : 4.1.0.5.2	Model	: CC-SG-E1-0	
CC-SG Serial # : ACD7900052	Host ID	: 0030485C05EB	
Server Information:			
CC-SG Status : Up	DB Status	: Responding	
Web Status : Responding/Unsecured	RAID Status	: Active	
Cluster Status : standalone	Cluster Peer	: Not Configured	
Network Information:			
Dev Link Auto Speed Duplex	IPAddr	RX Pkts TX Pkts	
eth0 yes on 100Mb/s Full 19	2.168.51.26	13561 2804	
eth1 no on Unknown! Unknown!			
	Help: <fl></fl>	<pre>Exit: <ctl+q> or <ctl+< pre=""></ctl+<></ctl+q></pre>	c>

この画面には、システム ヘルスや、CC-SG およびそのサブコンポーネ ントの稼動状況を確認するために役立つ情報が動的に表示されます。こ の画面の情報はほぼ 5 秒ごとに更新されます。

Status Console は以下の 4 つの領域で構成されます。

- CC-SG のタイトル、日付および時刻
- 今日のメッセージ
- システム、サーバ、およびネットワークのステータス
- ナビゲーション キーのリマインダ

CC-SG のタイトル、日付および時刻

CC-SG のタイトルは、ユーザが **CC-SG** ユニットに接続されているこ とがわかるように一定です。

画面上部に表示される日付と時刻は、最後に CC-SG データがポーリン グされた時刻です。日付と時刻は、CC-SG サーバに保存されている時 刻の値を反映します。

今日のメッセージ

[今日のメッセージ] (MOTD) ボックスに、CC-SG Admin Client に入力 される MOTD の最初の 5 行が表示されます。各行は最大 78 文字で 、特殊な形式はサポートされていません。



システム、サーバ、およびネットワークのステータス

画面のこの領域には、さまざまな CC-SG コンポーネントの状態につい ての情報が表示されます。以下の表では、CC-SG および CC-SG デー タベースの情報およびステータスについて説明しています。

情報	説明					
Host Name	CC-SG の完全修飾ドメイン名 (FQDN)。ユニットのホスト名および関連付けられたドメイン名の両方で構成されます。					
CC-SG Version	CC-SG の現 されます。	CC-SG の現在のファームウェア バージョン。5 タプルの値で構成 されます。				
CC-SG Serial #	CC-SG のシ	CC-SG のシリアル ナンバー。				
モデル	CC-SG のモ	デバ	レタイプ。			
Host ID	CC-SG 그=	ニット	トのライセンスを得るための番号。			
CC-SG Status	ほとんどの= タス。以下の	ュー・ のス・	ザ リクエストを処理する CC-SG サーバのス テータスが表示されます。	ステー		
	Up	CC 受i	-SG は利用可能で、ユーザ リクエストを け付けることができます。			
	Down	CC 性が 合い	-SG は停止しているか再起動中である可能 があります。[Down] のステータスが続く場 は、CC-SG を再起動してみてください。			
	Restarting		CC-SG は再起動中です。			
DB Status	CC-SG サー します。 CC 答している#	-バに -SG 公要:	は、その処理の中で内部データベース (DB) を が機能するには、このデータベースが、稼働 があります。以下のステータスが表示されま	を使用 動し応 す。		
	Responding		CC-SG データベースは利用可能です。			
	Up		データベース ルーチンの一部は実行され ていますが、ローカル リクエストには応 答していません。			
	Restoring		CC-SG はそれ自体のリストア中なので、 データベース照会は一時的に中断されてい ます。			
	Down		データベース サーバはまだ起動されてい ません。			
Web Status	CC-SG サー す。このフィ スが表示され	-バ~ イー, しま	へのアクセスのほとんどは Web を介して行れ ルドには、Web サーバの状態と、以下のステ す。	つれま ニータ		



情報	説明				
	Responding/Un	secured	Web サーバは稼働中であり、 http (セキュリティ保護なし) リクエストに応答しています 。		
	Responding/Se	cured	Web サーバは稼働中であり、 http (セキュリティで保護) リ クエストに応答しています。		
	Up		Web サーバ プロセスの一部 は実行されていますが、ロー カル リクエストには応答して いません。		
	Down		現在 Web サーバは利用でき ません。		
RAID Status	CC-SG は、そのデータをミラー化された 2 つの (R クに保存します。以下の RAID ディスクのステータス す。			ディス	
	Active	RAID が完全に機能しています。			
	Degraded	raded 1 つ以上のディスク ドライブで問題が発 生しています。ラリタン社のテクニカル サポートにご連絡ください。			
Cluster Status	CC-SG は、別の CC-SG と連携してクラスタを形成しています。 「 CC-SG クラスタの設定 『287p. 』」を参照してください。フィ ールドに "standalone" と表示されている場合、 CC-SG はクラスタ 設定には含まれていません。それ以外の場合は、フィールドにクラ スタの状態が表示されます。				
Cluster Peer	CC-SG がクラスタ設定に含まれている場合、フィールドにはその クラスタ内の他の CC-SG ユニットの IP アドレスが表示されます 。				
Network Information	ネットワーク インタフェースごとに、スクロール可能なテーブルを使用して情報が表示されます。				
	Dev	インタフェー	-スの内部名。		
	Link	リンク整合性 損傷のないク スイッチ ポ [、] を示します。	Eの状態、つまりこのポートが、 ーブルで稼働中のイーサネット ートに接続されているかどうか		
	自動 オート ネゴシエーションがこのポートに適 用されているかどうかを示します。				



Ch 16: 診断コンソール

情報	説明	
	Speed	このインタフェースが動作している速度 (10 、100、または 1000 メガビット/秒)。
	Duplex	インタフェースが全二重か半二重かを示しま す。
	IPAddr	このインタフェースの現在の lpv4 アドレス です。
	RX -Pkts	CC-SG のブート後にこのインタフェースで 受信した IP パケット数。
	TX -Pkts	CC-SG のブート後にこのインタフェースで 送信した IP パケット数。

ナビゲーション キーのリマインダ

画面の一番下の行には、ヘルプの呼び出し、および Status Console の 終了に使用されるキーボードのキーが表示されます。Status Console で は、以下に説明するキー以外のキー入力は無視されます。

- F1 を押すと、ヘルプ画面が表示されます。ここには診断コンソー ルのバージョンと、使用できるオプションが表示されます。
- Ctrl+L を押すと、現在の画面がクリアされて、更新された情報が再 表示されます。1 秒ごとに 1 回画面を更新できます。
- Ctrl+Q または Ctrl+C を押すと、Status Console が終了します。
- [ネットワーク情報] 画面の範囲よりも多くのデータがある場合は、 矢印キーを押して画面を上下左右にスクロールします。



Web ブラウザからの Status Console

Web ブラウザ経由で Status Console に接続すると、読み取り専用の [Status Console] Web ページが表示されます。

	2008-	12-01 E	ST Com	mandCenter S	ecure Gateway	19:22:40 E	ST -0500
lessage of	the the	Day:					
onnandCe	nter	Secure	Gateway				
entraliz	ed a	ccess a	nd control	for your glob	al IT infrastru	cture	
System in	forma	ation:					
н	ost N	lame: (C-SG-Demo	aitan com			
CC-SC	G Ver	rsion: 4	.1.0.5.2		Model:	CC-SG-E1-0	
cc-s	G Se	erial#: A	CD7900052		Host ID:	0030485C05	ΞB
Server Inte	orma	llon:					
cc-s	sg s	latus: L	lp		DB Status:	Responding	
w	eb S	latus: F	lesponding/Ur	secured	RAID:	Active	
Clus	ter S	latus: s	tandalone		Cluster Peer:	Not Configure	sd
letwork in	ntorm	allon:					
Device L	lnk	Auto	Speed	Duplex	iP_Addr	RX_Pkts	TX_Pkt
eth0	yes	on	100Mb/s	Full	192.168.51.26	100244	32533
eth1	no	on	Unknown!	Unknown!			
Historical	cc-s	SG Mon	itors				

Web ページには、Status Console と同じ情報が表示され、さらに約5 秒ごとに情報が更新されます。Web ページの下部にある CC-SG Monitor へのリンクについては、「*履歴データ傾向分析レポートの表示* 『365p. 』」および「CC-SG ディスクの監視 『419p. の"CC-SG ディ スク監視"参照 』」を参照してください。



Administrator Console

Administrator Console について

Administrator Console では、いくつかの初期パラメータを設定したり、 初期ネットワーク設定を提供したり、ログ ファイルをデバッグしたり 、一部の限定された診断を実行したり、CC-SG を再起動したりできま す。

Administrator Console のデフォルトのログインは以下のとおりです。

- ユーザ名: admin
- パスワード: raritan

重要:診断コンソールの admin アカウントは別個のものであり、Java ベースの CC-SG Admin Client および HTML ベースの Access Client で使用される CC スーパー ユーザの admin アカウントおよび パスワードとは区別されます。いずれか一方のパスワードを変更しても、 他方には影響がありません。

Administrator Console へのアクセス

Administrator Console に表示される情報はすべて静的です。CC-SG Admin Client または診断コンソールから設定に変更を加えた場合、その 変更が Administrator Console に表示されるようにするには、変更が反 映された後に Administrator Console にログインし直す必要があります

- ▶ Status Console にアクセスするには、以下の手順に従います。
- 1. ログイン プロンプトに「admin」と入力します。
- CC-SG のパスワードを入力します。デフォルトのパスワードは raritan です。最初のログインでは、このパスワードは期限切れとな っており、新しいパスワードを選択する必要があります。このパス ワードを入力し、プロンプトが表示されたら新しいパスワードを入 力します。パスワードの強度の設定についての詳細は、「診断コンソ ールのパスワード設定 『360p. 』」を参照してください。



Administrator Console メイン画面が表示されます。

File Operation
CC-SG Administrator Console: Welcome: Welcome to the Administration (Admin) section of the Diagnostic Console
The menus in this area will let you: - Do initial system set-up / installation. - Configure and control Diagnostic Services. - Perform emergency repairs. - Collected some diagnostic information.
There are more navigation aids in the Admin Console. The top title bar offers you a series of menus and sub-menus. Short-cut to this menu bar is <ctl+x> (or using your mouse).</ctl+x>
SN:ACD7900052, Ver:4.1.0.5.2 [Created:Mon Dec 2008-12-01 19:31:52 EST -0500]
<pre>Help: <f1> // Exit: <ctl+q> or <ctl+c> // Menus (Top-bar): <ctl+x></ctl+x></ctl+c></ctl+q></f1></pre>

Administrator Console 画面

Administrator Console の画面は、以下の 4 つの主要な領域で構成され ます。

メニュー バー:

メニュー バーを有効にして Administrator Console の機能を実行で きます。SSH クライアント経由で Administrator Console にアクセ スしている場合は、Ctrl+X を押してメニュー バーを有効にするか 、マウスを使用してメニュー項目をクリックします。



[File] メニューには診断コンソールを終了するための代替オプション があります。[Operation] メニューには、4 つのメニュー コマンド があり、1 つ以上のサブメニューを持つものもあります。各メニュ ー コマンドおよびサブメニューについては、Administrator Console の残りのセクションを参照してください。

メイン表示領域:

表示される内容は、選択されている操作によって異なります。



• ステータス バー:

ステータス バーはナビゲーション キー バーのすぐ上にあります。 ここには、CC-SG のシリアル ナンバー、ファームウェア バージ ョン、メイン表示領域に表示されている情報がロードまたは更新さ れた時刻など、重要なシステム情報の一部が表示されます。この情 報を含むスクリーンショットは、ラリタン社のテクニカル サポート に問題を報告するときに役立つことがあります。

ナビゲーション キー バー:

「Administrator Console のナビゲート 『342p. 』」を参照してく ださい。

Administrator Console のナビゲート

キーボードのキーを使用して、Administrator Console を操作します。 部のセッションでは、マウスを使ってナビゲートすることもできます。 ただし、すべての SSH クライアントや KVM コンソールではマウスは 機能しない場合があります。

キー	操作
Ctrl+X	メニュー バーを有効にします。メニュー からメニュー コマンドを選択し、さまざ まな Administrator Console 操作を実行し ます。
F1	診断コンソールのバージョンと使用できる オプションが表示されたヘルプ画面が表示 されます。
Ctrl+C または Ctrl+Q	診断コンソールを終了します。
Ctrl+L	画面をクリアして、情報を再描画します (情報そのものは更新も再表示もされません)。
Tab	次に利用可能なオプションに移動します。
スペース バー	現在のオプションを選択します。
Enter	現在のオプションを選択します。
矢印キー	オプション内で別のフィールドに移動しま す。


診断コンソール設定の編集

診断コンソールは、シリアル ポート (COM1)、VGA/キーボード/マウス (KVM) ポート、または SSH クライアントからアクセスできます。 Status Console にアクセスする場合は、もう 1 つのアクセス メカニズ ムである Web アクセスも利用できます。

各ポート タイプに対し、status または admin ログインを許可するかど うか、訪問サポート担当者 (field support) がそのポートを使って診断コ ンソールにアクセスできるかどうかなどを設定できます。SSH クライ アントの場合、使用するポート番号も (他の CC-SG サービスが使用中 でない限り) 設定できます。Status Console に対する Web アクセスで は、アクセスを制限するために、システムの他のアカウントとは別のア カウントを指定できます。アカウントを指定しない場合は、Web 経由 で CC-SG にアクセスできるすべてのユーザが Status Console の Web ページにアクセスできます。

重要: すべての Admin または Field Support アクセスを完全にロック アウトしてしまわないように注意してください。

- ▶ 診断コンソール設定を編集するには、以下の手順に従います。
- 1. [Operation] > [Diagnostic Console Config] を選択します。
- 2. 診断コンソールを設定してアクセスする方法を決定します。
 - 診断コンソールには、シリアル ポート (COM1)、KVM コンソール 、SSH (IP ネットワーク)、Web という 4 つのアクセス メカニズ ムがあります。また、Status Display、Admin Console、Raritan Field Support という 3 つのサービスがあります。この画面では、 それぞれのアクセス メカニズムで利用できるサービスを指定できま す。

[Web] オプションおよび [Status] オプションが有効になっている場合は、Web サーバが稼働し機能している限り、常に [Status Console] Web ページを利用できます。[Status Console] Web ページに対するアクセスを制限するには、アカウントとパスワードを入力します。

3. 診断コンソールへの SSH アクセスのために設定するポート番号を [Port] フィールドに入力します。デフォルトのポートは 23 です。



4. [保存] をクリックします。

File Operati	ion			
r CC-SG Adminis This screen le (Status, Admin Access Methods [Note: Be care	strator Conso ets you config h and Raritan s or Ports (S eful not to l	le: Diagnosti gure what Dia Field Suppor erial Console ock out all a	c Console Configura gnostic Console Ser rt) are available vi e, KVM port, SSH and eccess to Admin Cons	ition: vices a what Web). Web).
Ports: [X] Serial [X] KVM [X] SSH [] Web Web ID:	Status: [X] Status [X] Status [X] Status [] Status []	Admin: [X] Admin [X] Admin [X] Admin [X] Admin	r Raritan Access: [X] Field Support [X] Field Support [X] Field Support	Port: [23]
Web Passwd: SN:ACD7900052	2, Ven:4.1.0.	1 5.2 [Created:	:Mon Dec 2008-12-01	< Save > 19:31:52 EST -0500]
Help: <f1> //</f1>	Exit: <ctl+< td=""><td>Q> or <ctl+c></ctl+c></td><td>- // Menus (Top-bar)</td><td>: <ctl+x></ctl+x></td></ctl+<>	Q> or <ctl+c></ctl+c>	- // Menus (Top-bar)	: <ctl+x></ctl+x>

ネットワーク インタフェース設定の編集 (ネットワーク インタフェース)

ネットワーク インタフェースの設定では、CC-SG のホスト名および IP アドレスの設定などの初期設定タスクを実行できます。

- 1. [Operation] > [Network Interfaces] > [Network Interface Config] を選 択します。
- ネットワーク インタフェースが設定済みの場合は、インタフェース の設定を CC-SG Admin Client で行うことを推奨する警告メッセー ジが表示されます。続ける場合は [YES] をクリックします。
- 3. ホスト名を [ホスト名] フィールドに入力します。保存後、このフィ ールドが更新され、完全修飾ドメイン名 (FQDN) がわかっていれば 表示されます。ホスト名のルールについては、「*用語/略語* 『2p.』 」を参照してください。
- [モード] フィールドでは、[IP Isolation (IP 分離)] または [IP Failover (IP フェイルオーバ)] のいずれかを選択します。「ネットワ ーク設定について『271p.』」を参照してください。
- 5. [Configuration] フィールドから、[DHCP] または [Static] を選択します。
 - [DHCP] を選択した場合、DHCP サーバが適切に設定されていれば、保存後、Admin Console を終了して再び開くと、DNS 情報、ドメイン接尾辞、IP アドレス、デフォルトゲートウェイ、サブネットマスクが自動的に記入されます。



- [Static] を選択した場合、IP アドレス (必須)、ネットマスク (必須)、デフォルトのゲートウェイ (オプション)、プライマリ DNS (オプション)、セカンダリ DNS (オプション)、ドメイン接 尾辞のドメイン名 (オプション) を入力します。
- インタフェースの IP 設定を指定するために DHCP を使用して いる場合でも、正しい形式の IP アドレスおよびネットマスク を指定する必要があります。
- [Adapter Speed] で、回線速度を選択します。10 Mbps、100 Mbps 、1000 Mbps のうち一度に 1 つだけが表示されており、他の値は スクロール リストにあります。他の値を表示するには、矢印キーを 使用します。表示されたオプションを選択するには、スペース バー を押します。1 GB の回線速度の場合、AUTO を選択します。
- [Adapter Speed] で [AUTO] を選択していない場合は、[Adapter Duplex] をクリックし、必要に応じて、矢印キーを使ってリストか らデュプレックスモード (FULL または HALF) を選択します。デ ュプレックスモードはいつでも選択できますが、[Adapter Speed] が [AUTO] でない場合にのみ効果があります。
- [IP Isolation Mode (IP 分離モード)] を選択した場合は、2 番目のネ ットワーク インタフェースについてもこれらの手順を繰り返します。
- [保存] をクリックします。CC-SG が再起動され、すべての CC-SG GUI ユーザがログアウトされ、そのセッションが終了されます。警告画面が表示され、もうすぐネットワーク設定が変更されようとしていて、関連の CC-SG GUI ユーザに影響が出ることが通知されます。
 YES> を選択して続けます。
 システム操作の進行状態は、診断コンソールのステータス画面で監視できます。KVM ポートの場合、Alt+F2 キーを押して、status としてログインすれば、別のターミナル セッションを選択できます。
 Alt+F1 を押して元のターミナル セッションに戻ります。F1 ~ F6 で 6 つのターミナル セッションを利用できます。

IP アドレスの ping

CC-SG コンピュータと特定の IP アドレス間の接続が正しく機能して いるかを確認するには、ping を実行します。

注: 一部のサイトでは Ping 要求を明示的にブロックしています。Ping に失敗した場合、ターゲットと介在するネットワークで Ping か許可さ れているかを確認してくたさい。

- 1. [Operation] > [Network Interfaces] > [Ping] を選択します。
- 確認したいターゲットの IP アドレスまたはホスト名を [Ping Target] フィールドに入力します (CC-SG で DNS が適切に設定さ れている場合)。



3. 選択: オプション。

オプション	説明
Show other received ICMP packets	冗長出力。ECHO_RESPONSE パケットに 加えて受信された他の ICMP パケットもリ ストされます。あまり表示されません。
No DNS Resolution	アドレスをホスト名に解決しません。
Record Route	ルートの記録。IP ヘッダの中にパケットの 到達経路を記録する IP レコード ルート オプションを有効にします。
Use Broadcast Address	ブロードキャスト メッセージの ping が許 可されます。
Adaptive Timing	アダプティブ ping。パケット間のインター バルがラウンド トリップ タイムに適応し 、ネットワーク上に応答のないプローブが 一度に 1 つ以上存在することがないように します。最小インターバルは 200 ミリ秒 です。

- ping コマンドが実行される期間(秒)、送信される ping リクエストの数、ping パケットのサイズの値を入力します。デフォルトは 56 で、8 バイトの ICMP ヘッダ データを加えると 64 ICMP データバイトになります。空白のままにした場合はデフォルト値が使用されます。オプション。
- アダプティブ ping。一連の応答が結果に表示される場合は、接続は 機能しています。時間は接続の処理速度を表します。応答ではなく 「timed out」エラーが表示された場合は、お使いのコンピュータと ドメインの間の接続が機能していません。「*静的ルートの編集* 『 348p. 』」を参照してください。
- 6. Ctrl+C を押して Ping セッションを終了します。

注: Ctrl+Q キーを押すと、その時点までのセッションの統計サマリーが 表示され、ping の実行が続行されます。



Traceroute の使用

Traceroute はネットワークのトラブルシューティングによく使用されま す。順番に確認されたルータのリストが表示されるので、お使いのコン ピュータがネットワークの特定の宛先に到達するために経たパスを識別 することができます。コンピュータが宛先に到達するまでに通ったルー タ、またはアクセスが失敗および取り消されたルータがすべてリストさ れます。さらに、ルータからルータへの「hop」にかかる時間も表示され ます。この情報は、サイトへのアクセスをブロックしている可能性があ るルーティングの問題またはファイアウォールを識別する上で役立ちま す。

- ▶ IP アドレスまたはホスト名の traceroute を実行するには、以下の 手順に従います。
- 1. [Operation] > [Network Interfaces] > [Traceroute] を選択します。
- 2. 確認するターゲットの IP アドレスまたはホスト名を [Traceroute Target] フィールドに入力します。
- 3. 選択: オプション。

オプション	説明
Verbose	冗長出力。TIME_EXCEEDED と UNREACHABLE 以外の受信された ICMP パケットがリストされます。
No DNS Resolution	アドレスをホスト名に解決しません。
Use ICMP (vs. normal UDP)	UDP データグラムの代わりに ICMP ECHO を使用します。

- traceroute コマンドが送信プローブ パケットに使用する hop の数 (デフォルトは 30)、プローブで使用する UDP 送信先ポート (デフ ォルトは 33434)、traceroute パケットのサイズの値を入力します。 空白のままにした場合はデフォルト値が使用されます。オプション
- 5. ウィンドウの右下の [Traceroute] をクリックします。
- Ctrl+C または Ctrl+Q キーを押して traceroute セッションを終了 します。[Return?] プロンプトが表示されます。Enter キーを押して [Traceroute] メニューに戻ります。[Return?] プロンプトは、「 destination reached」または「hop count exceeded」イベントが発生 したために Traceroute が終了した場合にも表示されます。



静的ルートの編集

Static Routes では、現在の IP ルーティング テーブルを表示してルートを編集、追加、または削除できます。静的ルートの使用と配置を慎重に設定することで、実質的にネットワークのパフォーマンスが向上して、重要なビジネス アプリケーションのために帯域幅を確保することができる場合があります。マウスでクリックするか、Tab キーと矢印キーで移動して Enter キーで値を選択します。

- ▶ 静的ルートを表示または変更するには、以下の手順に従います。
- 1. [Operation] > [Network Interfaces] > [Static Routes] を選択します。
- 現在の IP ルーティング テーブル ページが表示されます。[Add Host Route] または [Add Network Route] を選択すると、関連付け られる IP ルートをルーティング テーブルに追加できます。ルーテ ィング テーブル内の項目は選択可能です。[Delete Route] を選択す ると、テーブルからルートを削除できます。[Refresh] ボタンをクリ ックすると、テーブルのルーティング情報が更新されます。
 - [Add Host Route] には、送信先のホスト IP アドレスと、Status Console に表示されているゲートウェイ IP アドレスとインタ フェース名の一方または両方を指定します。
 - [Add Network Route] も同様ですが、送信先のネットワークおよびネットマスクを指定します。
 - テーブルで任意の項目を選択またはハイライトした状態で、 [Delete Route] を選択すると、ルートを削除できます。ただし、現在のホストおよびインタフェースに関連付けられているルートだけは例外です。CC-SG ではこの削除は許可されていません。



デフォルト ゲートウェイを含むその他のルートはすべて削除できま すが、これを行うと **CC-SG** との通信が大きな影響を受けます。

File Operation CC-SG Administr This screen allo You can see the and delete route	ator Console: Sta Ws you to manage routes currently S.	tic Routes:	table. routes,	
, Destination	Gateway	Netmask	Interface	Flags
192.168.51.0	*	255.255.255.0	eth0	U
<default></default>	192.168.51.126	0.0.0	eth0	UG
<pre>< Add Host Route SN:ACD7980052, Help: <fl> // E</fl></pre>	<pre>> < Add <u>N</u>etwork Ver:4.1.0.5.2 [Cr xit: <ctl+0> or <</ctl+0></pre>	Route > < Delet reated:Mon Dec 2 ccl+C> // Menus	e Route > < F 008-12-01 19: (Top-bar):	<pre>lefresh > 31:52 EST -0500] <ctl+x></ctl+x></pre>



診断コンソールでのログ ファイルの表示

システム アクティビティを調査するために複数のファイルを同時にブ ラウズできる LogViewer では、1 つまたは複数のログ ファイルを同時 に表示できます。

ログファイル リストが更新されるのは、関連のリストがアクティブに なった場合 (ユーザがログファイル リスト領域に入った場合など)、あ るいは新しいソート オプションが選択された場合だけです。ファイル 名の前には、ログファイルの受信されたデータがどの程度新しいかを示 すタイムスタンプまたはログファイルのサイズが伴います。

▶ タイムスタンプとファイル サイズの略語

タイムスタンプ

- s = 秒
- m = 分
- h = 時間
- d = ∃

ファイル サイズ

- B = バイト
- K = キロバイト (1,000 バイト)
- M = メガバイト (1,000,000 バイト)
- G = ギガバイト (1,000,000,000 バイト)

▶ ログ ファイルを表示するには、以下の手順に従います。

- 1. [Operation] > [Admin] > [System Logfile Viewer] を選択します。
- 2. [Logviewer] 画面は主に次の 4 つの領域に分かれています。
 - システムで現在使用可能なログファイルのリスト。リストが表示ウィンドウより長い場合は、矢印キーでスクロールできます。
 - ログファイル リストのソート基準。ログファイルは、ファイル の絶対名、最終変更日、サイズでソートできます。
 - ビューア表示オプション。
 - エクスポート/表示セレクタ。



3. マウスでクリックするか、矢印キーでナビゲートし、スペース バー を押してログ ファイルを選択すると、選択されたファイルが X で マークされます。一度に複数のログ ファイルを表示できます。

File Operation	
CC-SG Administrator Console: System Logfile V	/iewer:
Logfile(s) to View:	
<pre>1d ./boot.log</pre>	Sort Logfile list by:
[] 3m ./cron	<o> Full File Name</o>
[] 2m ./messages	< > Recent Change
[] 13h ./rpmpkgs	< > File Size
[] 3m ./secure	l
[] 1d sg/ShellCommandExecutor.log	
[] 4s sg/httpd/access_log	Viewer Display Options:
[] 13h sg/httpd/access_log.1	<o> Individual Windows</o>
[] 13h sg/httpd/error_log	< > Merged Windows
[] 13h sg/httpd/mod_jk.log	Initial Buffer:[5000]
[] ld sg/jboss/boot.log	
<pre>[] 1d sg/jboss/cc_access.2008-12-01.log</pre>	[X] Remember Selected Items
<pre>[] 37m sg/jboss/console.log</pre>	[X] Use Default Color Scheme
<pre>[] ld sg/jboss/console.log.l2-01-16_25</pre>	[X] Use Default Filters
<pre>[] 37m sg/jboss/console.log.l2-01-16_36</pre>	
	< Export > < View >
SN:ACD7900052, Ver:4.1.0.5.2 [Updated:Tue Dec	: 2008-12-02 17:13:57 EST -0500]
Help: <f1> // Exit: <ct1+q> or <ct1+c> // Mer</ct1+c></ct1+q></f1>	nus (Top-bar): <ctl+x></ctl+x>

[Logfiles to View] リストを並べ替えるには、以下の手順に従います。

[Sort Logfile list by] オプションは、ログファイルが [Logfile to View] リストに表示される順序を制御できます。

オプション	説明
Individual Windows	別のサブウィンドウが開いて選択したログが表示されます。
Merged Windows	選択したすべてのログ ファイルが 1 つの表示ウィンドウに マージされます。
Initial Buffer	初期バッファまたは履歴のサイズを設定します。デフォルト は 5000 です。このシステムは、新しく入ってきたすべての 情報をバッファするように設定されています。
Remember Selected Items	このボックスを選択すると、現在のログファイルの選択情報 があれば記憶されます。選択しないと、新しいログファイル リストが生成されるたびに、選択がリセットされます。これ は、複数のファイルを通して確認したい場合に便利です。
Use Default Color Scheme	このボックスを選択すると、一部のログファイルが標準配色 で表示されます。注: multitail コマンドを使用すると、表示 中であっても、ログファイルの配色を変更できます。
Use Default Filters	このボックスを選択すると、一部のログファイルに自動フィ ルタが適用されます。



Ch 16: 診断コンソール

オプション	説明
Export	このオプションでは、選択されたすべてのログ ファイルが パッケージ化され、Web からアクセスできるようになるた め、取り出して、Raritan のテクニカル サポートに送ること ができます。このパッケージの内容には、ユーザはアクセス できません。エクスポートされたログファイルは最大 10 日 間利用でき、それ以降はシステムから自動的に削除されます 。
表示	選択したログが表示されます。

[View] を [Individual Windows] とともに選択した場合、次のような LogViewer が表示されます。

000 day and UTTD/1 1# 000 27046	
eap-day.phg hitry1.1 200 57040	Istatus/CC_SC/CC_SC_if otho
192.100.31.43 [02/Dec/2000:17:14:37 -0300] 001 /	status/cc-so/cc-so-il_etno-
102 168 51 45 [02/0ac/2009.17.14.27 0500] "CET	Istatus (CC SC/CC SC 1f ath]
day ppg HTTP/1 1= 200 18213	status/cc-so/cc-so-il_etili-
102 158 51 45 [02/Doc/2008-17-14-38 .05001 "CET .	(status/logo ppg HTTP/1 1" 3
A4 .	status, togotping mini / 1.1 5
AAl su/httpd/access log El/s(TRLs+shs; help	2MB . 2008/12/02 17:18:20
56396K, >48191K(1040512K) 0 3504499 secs1	210 - 2000/12/02 17:10:20
51079K-551057K/1040512K) 0 4303580 secs1	
55710V \$52450V/1040576V) 0 2506670 cocc1	
56212V > 49157V(1040576V) 0 2596129 cocc1	
50212K+24015/K(10405/0K), 0.3300120 5865	
51960K->48191K(10405/6K), 0.3510230 Sec5]	
51982K->51953K(1040040K), 0.349/310 secs]	
55735K->52511K(1040704K), 0.4299940 secs]	
01] sg/jboss/console.log F1/ <ctrl>+<h>: help</h></ctrl>	237KB - 2008/12/02 17:18:20
Dec 2 14:18:23 CommandCenter Status-Console[3413]: 5	Sleeping 1
Dec 2 15:22:35 CommandCenter smartd[2974]: Device: /	/dev/sda, SMART Usage Attrib
ute: 194 Temperature Celsius changed from 116 to 117	
Dec 2 15:52:36 CommandCenter smartd[2974]: Device: A	/dev/sda, SMART Usage Attrib
ute: 194 Temperature Celsius changed from 117 to 116	
Dec 2 16:22:35 CommandCenter smartd(2974): Device: A	/dev/sda, SMART Usage Attrib
ute: 194 Temperature Celsius changed from 116 to 117	
A21 /messages *Press F1/c(TRiatcha for help*	330KB . 2008/12/02 17-18-20

- ログファイルの表示中、「q」と入力するか、Ctrl+Q または Ctrl+C キーを押すと、前の画面に戻ることができます。
- ログ ファイルの色を変更して重要な部分をハイライトできます。
 ログ ファイルの色を変更するには「C」と入力し、リストから対象のログを選択します。



• [info] に「I」と入力すると、システム情報が表示されます。



注: システム負荷はこの Admin Console セッションの開始時の静的な 情報です。システム リソースを動的に監視する場合は TOP ユーティ リティを使用してください。

- 正規表現を使用してログファイルをフィルタするには、以下の手順 に従います。
- 1. 正規表現を追加または編集するために「e」と入力し、表示に複数の ログ ファイルが選択されている場合はリストから対象のログを選択 します。



 「A」と入力して、正規表現を追加します。たとえば、 sg/jboss/console.log ログ ファイルの警告メッセージについての情報を表示する必要がある場合は、「WARN」と入力して [match] を 選択します。

注: この画面には、console.log のデフォルトのフィルタ スキーム も表示されます。これにより、ほとんどの Java ヒープ メッセージ が除外されます。

ay.pn 192.1	9 HTTP/1.1" 200 43231	-ethl-
week. 192.1	Edit reg.exp. sg/jboss/console.log Edd. Edit Molate Audt move News Meyer The Foset counter	eth1-
192.1	nv Unloading class Full GC \[GC 1560	.1" 3
04 · 00] s		21:57
5639 5197		
5571 5621		
5196 5198		
5573 011 s		21.57
Dec		theib
ute:		ttath
ute:		LUTID
ute:		ttrib
02].		21:57



診断コンソールを使用した CC-SG の再起動

CC-SG を再起動すると、現在の **CC-SG** ユーザがすべてログアウトされ、それらのユーザのリモート ターゲット サーバに対するセッション が終了します。

重要: どうしても診断コンソールから再起動しなければならない場合以 外は、Admin Client で CC-SG を再起動することを強く推奨します。 「*CC-SG の再起動* 『255p. 』」を参照してください。診断コンソール から CC-SG を再起動した場合、ユーザには再起動していることは通知 されません。

- ▶ 診断コンソールを使用して CC-SG を再起動するには、以下の手順 に従います。
- 1. [Operation] > [Admin] > [CC-SG Restart] を選択します。
- 2. [Restart CC-SG Application] をクリックするか、Enter キーを押し ます。次の画面で再起動することを確認して、続行します。

 File Operation

 CC-SG Administrator Console: CC-SG Restart:

 CC-SG Restart.

 This operation will restart the CC-SG Application.

 This will log-off all currently active CC-SG GUI users of the system and terminate any sessions to remote targets that they might have.

 They will get no notification that this event will happen.

 [It is better to use the CC-SG GUI to do this -- it will provide a count-down timer and notification of session termination.]

 < Restart CC-SG Application >

 < Restart CC-SG Application >

 SN:ACD7900052, Ver:4.1.0.5.2 [Created:Mon Dec 2008-12-01 19:31:52 EST -0500]

 Help: <F1> // Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar): <ctl+X>

診断コンソールを使用した CC-SG のリブート

このオプションは CC-SG 全体をリブートし、電源の再投入をシミュレ ートします。ユーザに通知は表示されません。CC-SG、SSH、診断コン ソールのユーザ (このセッションを含む) がログアウトされます。リモ ート ターゲット サーバへの接続もすべて終了します。

CC-SG をリブートするには、以下の手順に従います。

1. [Operation] > [Admin] > [CC-SG System Restart] を選択します。



2. [REBOOT System] をクリックするか、Enter キーを押して CC-SG をリブートします。次の画面でリブートすることを確認して、続行します。

File Operation
CC-SG Administrator Console: CC-SG System Reboot: CC-SG System Reboot.
This operation will reboot the entire system (simulating a power cycle).
This will log-off all currently active CC-SG GUI, CC-SG SSH and Diagnostic Console users (including this session) to this system and terminate any sessions to remote targets that they might have. This could also impact cluster operations (if so configured).
Users will get no notification that this event will happen.
<mark>< REBOOT System ></mark> < Cancel >
SN:ACD7980052, Ver:4.1.0.5.2 [Created:Thu Dec 2008-12-04 13:46:04 EST -0500]
<pre>Help: <f1> // Exit: <ctl+q> or <ctl+c> // Menus (Top-bar): <ctl+x></ctl+x></ctl+c></ctl+q></f1></pre>

診断コンソールからの CC-SG システムの電源オフ

このオプションでは、CC-SG ユニットの電源がオフになります。ログ インしているユーザに通知は表示されません。CC-SG、SSH、診断コン ソール ユーザ (このセッションを含む) がログオフされます。リモート ターゲット サーバへの接続もすべて終了します。

ユニットの前面パネルの電源ボタンを押さない限り、CC-SG ユニットの電源を再度オンにすることはできません。

▶ CC-SG の電源をオフにするには、次の手順に従います。

0

1. [Operation] > [Admin] > [CC-SG System Power OFF] を選択します



 [Power OFF the CC-SG] をクリックするか、Enter キーを押して CC-SG の AC 電源をオフにします。次の画面で電源をオフにする ことを確認して、続行します。



診断コンソールを使用した **CC** スーパー ユーザのパスワードのリセッ ト

このオプションでは、**CC** スーパー ユーザ アカウントのパスワードが 工場出荷時のデフォルト値にリセットされます。

工場出荷時のデフォルト パスワード: raritan

注: これは、診断コンソールの admin ユーザのパスワードではありません。「診断コンソールのパスワード設定 『360p. 』」を参照してください。

- CC-SG GUI admin パスワードをリセットするには、以下の手順に 従います。
- 1. [Operation] > [Admin] > [CC-SG ADMIN Password Reset] を選択し ます。



 [Reset CC-SG GUI Admin Password] をクリックするか、Enter キ ーを押して admin パスワードを工場出荷時のデフォルト値に戻し ます。次の画面でパスワードをリセットすることを確認して、続行 します。



CC-SG 工場出荷時設定へのリセット

このオプションでは、CC-SG システムのすべてまたは一部が工場出荷 時のデフォルト値にリセットされます。アクティブなすべての CC-SG ユーザは通知なしにログアウトされ、SNMP 処理が停止します。

File Operation
r CC-SG Administrator Console: Factory Reset:
Factory Reset will restore the system to initial Default Configuration.
This will log-off all currently active CC-SG GUI sessions to this system
and may terminate any sessions to remote targets that they might have.
This could also impact cluster operations (if so configured).
Users will get no notification that this event will happen!
Reset Options:
X Full CC-SG Database Reset
[X] Preserve CC-SG Personality during Reset
[] Network Reset
[X] SNMP Reset
[X] Firmware Reset
[X] Install Firmware into CC-SG DB
[X] Diagnostic Console Reset
[] IP Access Control Lists Reset
< RESET System > < Cancel >
SN:ACD7900052, Ver:4.1.0.5.2 [Created:Mon Dec 2008-12-01 19:31:52 EST -0500]
<pre>Help: <f1> // Exit: <ct1+q> or <ct1+c> // Menus (Top-bar): <ct1+x></ct1+x></ct1+c></ct1+q></f1></pre>

選択済みのデフォルト オプションを使用するようにお勧めします。



Ch 16: 診断コンソール

オプション	説明
Full CC-SG Database Reset	このオプションの場合、既存の CC-SG データベースが削除され、工場 出荷時のデフォルト値で新しいバージョンが作成されます。ネットワー ク設定、SNMP 設定、ファームウェア、診断コンソール設定は、CC-SG データベースの一部ではありません。
	IP-ACL 設定は、IP ACL テーブル オプションの選択の有無に関わらず フル データベース リセット操作でリセットされます。
	リセットにより隣接システムの設定が削除されるので、隣接システムの メンバだったとしても、CC-SG ではその記憶が失われます。
Preserve CC-SG Personality during Reset	このオプションは、フル CC-SG データベース リセットを選択すると 有効になります。
	CC-SG データベースが再作成されるときには、前に設定された一部の オプションが保存されます。
	 PC クライアントと CC-SG 間のセキュア通信
	 ・ 強力なバスワードの強制 ・ アウト オブ バンド ノードへの直接接続とプロキシ接続
	 休止タイマーの設定
Network Reset	このオプションでは、ネットワーク設定が工場出荷時のデフォルト値に 戻ります。
	 ホスト名: CommandCenter
	 ドメイン名: localdomain
	 モート: IP フェイルオーハ 設定: 静的
	■ IP アドレス: 192.168.0.192
	 ネットマスク: 255.255.255.0
	 ゲートウェイ:なし
	 プライマリ DNS: なし
	 セカンダリ DNS: なし アダプタ速度: 自動
SNMP Reset	このオプションでは、SNMP 設定が工場出荷時のデフォルト値に戻りま す。
	■ ポート: 161
	 読み取り専用コミュニティ: public
	 読み書きコミュニティ: private
	 システム連絡先の名前と場所:なし SNIAD トラップ様式
	 SNMF トラップ送信先



オプション	説明
Firmware Reset	このオプションでは、すべてのデバイス ファームウェア ファイルが工 場出荷時のデフォルト値にリセットされます。このオプションでは、 CC-SG データベースは変更されません。
Install Firmware into CC-SG DB	このオプションでは、現在の CC-SG バージョンのファームウェア フ ァイルが CC-SG データベースにロードされます。
Diagnostic Console Reset	このオプションでは、診断コンソール設定が工場出荷時のデフォルト値 に戻ります。
IP アクセス制御リストのリ セット	このオプションでは、IP-ACL テーブルからすべてのエントリが削除されます。 このオプションでは、パスワード (status と admin) の強さとパスワー ドの属性を設定できます。パスワードの属性とは、パスワードの変更 ([Account Configuration] メニューで行います) が必要になる期限までの 日数などの設定です。 「 <i>アクセス制御リスト</i> 『309 p. 』 」を参照してください。

▶ **CC-SG** を工場出荷時設定にリセットするには、以下の手順に従います。

- 1. [Operation] > [Admin] > [Factory Reset] を選択します。
- 2. リセット オプションを選択します。
- 3. [Reset System] をクリックします。
- 4. 画面に警告メッセージと進捗バーが表示されます。進捗バーには、 現在のリセット ステータスが示されます。リセットが完了するまで CC-SG を制御することはできません。

リセット中に CC-SG の電源オフ、電源オン・オフ、または中断操作 をしないでください。これらを実行すると、CC-SG データが失われ る恐れがあります。



診断コンソールのパスワード設定

このオプションでは、パスワード (status と admin) の強さとパスワードの属性を設定できます。パスワードの属性とは、パスワードの変更 ([Account Configuration] メニューで行います) が必要になる期限までの 日数などの設定です。このメニューでの操作は、診断コンソール アカウント (status または admin) とパスワードのみに適用され、通常の CC-SG GUI アカウントまたはパスワードには効果がありません。

- 診断コンソール パスワードを設定するには、以下の手順に従います。
- 1. [Operation] > [Admin] > [DiagCon Passwords] > [Password Configuration] を選択します。
- 2. 記憶されるパスワードの数を [Password History Depth] フィールド に入力します。デフォルト設定は 5 です。

File Operation
r CC-SG Administrator Console: Password Settings:
Use this screen to update how all subsequent Diagnostic Console (only!)
password operations will work. You can set the type of passwords (regular.
strong or random) that the system will let the user use on any subsequent
nassword channe operation. Also, the number of nasswords beneforth that
the system will remember and not let the user dunlicate or reuse
the system with remember and not tet the user auptricate of rease.
Password Configuration-
Password History Denth: 15 1
Passiona history bench. [5]
Password Type & Parameters
Zoo Regular
<pre>c> Regular c> Reg</pre>
< > Admuoni Size, [20] Actives, [10] < > Strong Potrios, [2] DiffOV.[4] Min[EN.[0]
District [1] Unrow [1] Larger [1] Others [1]
brights: [-r] opper: [-r] cower: [-r] other:[-r]
 Indate a
<pre>< opuace ></pre>
CN. ACD7080052 Nor.4 1 0 5 2 [Crostal-Man Dec 2009 12 01 10-21-52 ECT 0500]
SW:ACD/960632, Ver:4.1.0.5.2 [Created:Mon Det 2008-12-01 19:51:52 EST -0500]
Help: cF15 // Evit: cctl+0s or cctl+0s // Menus (Top.bar); cctl+Xs
here, size // exec. sectors // here's (top-bar). sectors

3. admin および status (有効な場合) のパスワードに対し、[Regular] 、[Random] または [Strong] のいずれかを選択します。

パスワード設定	説明
Regular	標準のパスワードです。パスワードは 5 文字以上で指定する必要があ りますが、その他の制限はほとんどありません。これはパスワード設 定のシステム デフォルトです。
Random	パスワードがランダムに生成されます。パスワードの最大サイズ (size) をビットで指定し (最小値 14、最大値 70、デフォルト 20)、 再試行の回数 (retries) を指定します (デフォルト 10)。再試行の回数 は、新しいパスワードを受け入れるかどうかを選択できる回数を意味



パスワード設定	説明
	します。ユーザはランダムに生成されたパスワードを受け入れる(新しいパスワードを2回入力して)か拒否するかのいずれかを選択できます。自分でパスワードを選択することはできません。
Strong	強力なパスワードが強制されます。
	[Retries] はエラー メッセージが表示されるまでにプロンプトが表示される回数を意味します。
	[DiffOK] は新しいパスワードの中で、古いパスワードと同じ文字を何 文字まで使用できるかを指定します。
	[MinLEN] はパスワードの最小長さを指定します。[Digits] はパスワードに必要な数字の桁数、[Upper] はパスワードに必要な大文字の数、 [Lower] は小文字の数、[Other] はその他の特殊文字の数を指定します。
	正の数は、「simplicity (簡潔さ)」カウントに対してこの文字クラスの「 credit (持ち点)」を加算できる最大数を意味します。
	負の数は、その文字クラスの文字を少なくともその数以上はパスワードに入れる必要があることを意味します。つまり、数に -1 を指定した場合、すべてのパスワードに少なくとも 1 桁の数字が必要になります。

診断コンソール アカウント設定

デフォルトでは、status アカウントにはパスワードは必要ありませんが、ここでパスワードを義務付けることができます。他にも、admin パス ワードの設定や Field Support アカウントの有効化または無効化などを 行うことができます。

- ▶ アカウントを設定するには、以下の手順に従います。
- 1. [Operation] > [Admin] > [DiagCon Passwords] > [Account Configuration] を選択します。



2. 表示される画面で、各アカウント (Status、Admin、FS1、FS2) の 設定を確認できます。

File Operati	on			
- CC-SG Adminis	trator Console:	Account Sett	ings:	
Account Config	uration:			
Field: \ User:	Status:	Admin:	FS1:	FS2 :
User Name:	status	admin	fs1	fs2
Last Changed:	Dec01,2008	Dec01,2008	Dec01,2008	Dec01,2008
Expire:	never	never	never	never
Mode:	< > Disabled		< > Disabled	<o> Disabled</o>
	<pre>< > Enabled <o> NoPassword</o></pre>		<o> Enabled</o>	< > Enabled
Min Days:	[0]	[0]		
Max Days:	[99999]	[99999]		
Warn:	[7]	[7]		
Max # Logins:	[-1]	[2]	[1]	[<mark>0</mark>]]
Update Param:	<update></update>	<update></update>	<update></update>	<update></update>
New Password:	<new passworda<="" td=""><td><new passworn<="" td=""><td>d></td><td></td></new></td></new>	<new passworn<="" td=""><td>d></td><td></td></new>	d>	
		< RESET	to Factory Pass	word Configuration >
SN:ACD7900052	, Ver:4.1.0.5.2	[Created:Mon	Dec 2008-12-01	19:31:52 EST -0500]
Help: <f1> //</f1>	Exit: <ctl+q></ctl+q>	or <ctl+c> //</ctl+c>	Menus (Top-bar)	: <ctl+x></ctl+x>

この画面は主に3 つの領域に分かれています。

- 一番上には、システム上のアカウントに関する読み取り専用の 情報が表示されます。
- 中央のセクションには、各 ID に関連および該当するさまざまな パラメータが、パラメータの更新やアカウントの新しいパスワ ードの付与を行うボタンのセットとともに表示されます。
- 一番下の領域では、パスワードの設定を工場出荷時のデフォルト(システムの出荷時の設定)にリセットします。
- 3. Status アカウントのパスワードを必須にするには、[Status] の下で [Enabled] を選択します。
- **4.** Admin および Status アカウントについて、次のような設定を行え ます。

設定	説明
User \ User Name	(読み取り専用) このアカウントの現在のユーザ名または ID です。
Last Changed	(読み取り専用) このアカウントのパスワードを前回変更した日付です。
Expire	(読み取り専用) このアカウントのパスワードの変更が必要になる日です。
Mode	アカウントの無効 (ログイン禁止) または有効 (認証トークンが必要)、アクセス許可、およびパスワード不要などの設定可能なオプション。Admin と FS1 のアカウントを同時にロックアウトしないで



設定	説明
	ください。診断コンソールを使用できなくなります。
Min Days	パスワードを変更した後、再び変更できるようになるまでに経過し なければならない最低日数です。デフォルトは 0 です。
Max Days	パスワードが有効である最大日数です。デフォルトは 99999 です。
Warning	パスワードが有効期限切れになる何日前に警告メッセージを発行す るかを指定します。
Max # of Logins	アカウントに一度に許可されるログインの回数です。負の値は制約 がないことを示します (-1 は status ログインのデフォルトです)。 0 の場合、誰もログインできません。整数は、同時にログインでき るユーザの数を決定します (admin ログインの場合 2 がデフォル トです)。
UPDATE	この ID に対して行った変更を保存します。
New Password	このアカウントの新しいパスワードを入力します。



リモート システム監視の設定

リモート システム監視機能を有効にすると、GKrellM ツールを使用で きます。GKrellM ツールは、CC-SG ユニットでのリソース使用率のグ ラフィック表示を提供します。このツールは、Windows Task Manager の [パフォーマンス] タブに似ています。

- 1: CC-SG ユニットのリモート システム監視を有効にする場合の手順:
- 1. [Operation] > [Utilities] > [Remote System Monitoring] を選択します

File Operation	
CC-SG Administrator Console: Remote Enable Remote System Monitoring.	e System Monitoring:
This operation configures the abilit via the gkrellm protocol and utiliti	ty to remotely monitor the CC-SG ies on your remote PC Client.
Enable Remote System Monitoring and Then download and install the tool f	Enter your Client PC IP address below. from http://www.gkrellm.net.
<pre>Remote Monitoring Service: < > Enabled</pre>	Allowed Remote Monitoring IP Address(es): IP Addr #1: [127.0.0.1]
<pre><0> Disabled</pre>	IP Addr #2: [IP Addr #3: []
	Port: [19150]
	< Submit >
SN:ACD7900052, Ver:4.1.0.5.2 [Creat	ted:Mon Dec 2008-12-01 19:31:52 EST -0500]
<pre>Help: <f1> // Exit: <ctl+q> or <ctl< pre=""></ctl<></ctl+q></f1></pre>	l+C> // Menus (Top-bar): <ctl+x></ctl+x>

- 2. [Remote Monitoring Service] フィールドで [Enabled] を選択します。
- CC-SG ユニットの監視を許可されるクライアント PC の IP アド レスを [Allowed Remote Monitoring IP Addresses] フィールドに入 力します。最大 3 つの IP アドレスを入力できます。
- 4. GKrellM ツールのデフォルト ポートは 19150 です。このポートは 変更できます。
- 5. [Submit] を選択します。
- 2: リモート システム監視クライアント ソフトウェアのダウンロー ドする場合の手順:
- 1. www.gkrellm.net にアクセスします。
- 2. クライアント PC に適切なパッケージをダウンロードして、インス トールします。



3: CC-SG で機能するように、リモート システム監視クライアント を設定します。

Read Me ファイルの手順に従って、CC-SG ユニットを監視対象として 設定します。

Windows ユーザは、コマンドラインを使用して、Gkrellm インストール ディレクトリを見つけ、Read Me ファイルに指定されたコマンドを 実行する必要があります。

履歴データ傾向分析レポートの表示

履歴データ傾向分析では、CPU 使用率、メモリ使用率、Java ヒープ スペース、およびネットワーク トラフィックについての情報を収集し ます。この情報は、CC-SG からの Web ページとして表示されるレポ ートにコンパイルされます。このレポートには、CC-SG のステータス および履歴データへのリンクが含まれます。

CC-SG システムの日時が以前の日時に変更されると、履歴データ傾向 分析レポートでデータ収集が停止します。日時が元の日時に達すると、 データ収集が再開します。日時が後の日時に変更されると、レポートに 表示されるデータに空白部分が生じます。

- 1:履歴データ傾向分析の表示を有効にする場合の手順:
- 1. [Operation] > [Diagnostic Console Config] を選択します。
- 2. [ポート] リストで [Web] を選択します。
- 3. [Status] リストで、Web の横の [Status] チェックボックスを選択 します。
- 4. [保存] をクリックします。
- 2: 履歴データ傾向分析レポートを表示する場合の手順:
- サポートされているインターネット ブラウザを使用して URL を「 http(s): //<IP_address>/status/」と入力します。
 <IP_address> は、CC-SG の IP アドレスです。/status の後の スラッシュ (/) は必須です。たとえば「https: //10.20.3.30/status/」のように入力します。
- ステータス ページが開きます。このページには、Status Console と同じ情報が含まれます。「*Status Console* 『333p. 』」を参照し てください。
 - [Historical CC-SG Monitors] データ傾向分析では、CPU 使用率、メモリ使用率、Java ヒープ スペース、およびネットワークトラフィックについての情報を収集します。各グラフをクリックして、詳細を新しいページに表示します。



RAID ステータスとディスク使用率の表示

このオプションでは、**CC-SG** ディスクのステータスが表示されます。 ディスク サイズ、アクティブで稼動中ステータス、**RAID-1** の状態、さ まざまなファイル システムによって現在使用中の領域量などです。

- CC-SG のディスク ステータスを表示するには、以下の手順に従い ます。
- 1. [Operation] > [Utilities] > [Disk / RAID Utilities] > [RAID Status + Disk Utilization] を選択します。

File Operation			_	tus + Di	isk Utilization:
Person Diagnostic Con md0 : Network Interfa Admin	sole C aces	onfig	* *		
Utilities			>>	Remote	DATE Contract Distant Had Manada
72501248 blocks	[2/2]	[00]		Top Dis NTP Sta	s Manual Disk / RAID Tests S Schedule Disk Tests
Filesystem	Size	Used	Avail	System	Repair / Rebuild RAID
/dev/mapper/svg-root	4.8G	306M	4.36		
/dev/mapper/svg-sg	2.96	344M	2.46	13% /s	59
/dev/mapper/svg-DB	8.6G	217M	7.96	3% /s	sg/DB
/dev/mapper/svg-opt	5.7G	495M	5.0G	98 /0	opt
/dev/mapper/svg-usr	2.06	976M	877M	53% /u	usr
/dev/mapper/svg-tmp	2.06	36M	1.86	2% /t	tmp
/dev/mapper/svg-var	7.6G	211M	7.06	3% /V	var
/dev/md0	99M	12M	82M	13% /b	boot
tmpfs	2.06	Θ	2.06	0% /d	dev/shm < Refresh
SN:ACD7900052, Ver:4 Help: <f1> // Exit: -</f1>	.1.0.5 <ctl+0< td=""><td>.2 (U) > or ·</td><td>pdated <ctl+c:< td=""><td>:Tue Dec > // Men</td><td>c 2008-12-02 17:44:21 EST -0500) nus (Top-bar): <ctl+x></ctl+x></td></ctl+c:<></td></ctl+0<>	.2 (U) > or ·	pdated <ctl+c:< td=""><td>:Tue Dec > // Men</td><td>c 2008-12-02 17:44:21 EST -0500) nus (Top-bar): <ctl+x></ctl+x></td></ctl+c:<>	:Tue Dec > // Men	c 2008-12-02 17:44:21 EST -0500) nus (Top-bar): <ctl+x></ctl+x>

 [Refresh] をクリックするか、Enter キーを押して表示を更新します 。表示の更新は、アップグレードやインストールを行っているとき 、RAID ディスクの再構築や同期の進行状況を表示するために便利 な機能です。

注: 上図のような画面が表示されたら、ディスク ドライブは完全に同期 されており、完全な RAID-1 保護を実施できます。md0 配列と md1 配列のステータスはともに [UU] です。



ディスクまたは RAID テストの実行

SMART ディスク ドライブ テストまたは RAID チェックおよび修復処 理を手動で実行できます。

- ディスク ドライブ テストまたは RAID チェックおよび修復処理を 実行するには、以下の手順に従います。
- 1. [Operation] > [Utilities] > [Disk / RAID Utilities] > [Manual Disk/RAID Tests] を選択します。



- SMART ディスク ドライブ テストを実行するには、以下の手順に 従います。
 - a. [Disk Test] セクションで、テストのタイプとテストするディス ク ドライブを選択します。
 - b. [Submit] を選択します。
 - c. テストがスケジュールされ、SMART 情報画面が表示されます。
 - d. 画面で示されている所要時間が過ぎたら、[Repair/Rebuild RAID] 画面で結果を確認できます。「RAID ディスクの修復また は再作成 『371p. 』」を参照してください。
- 3. RAID テストおよび修復処理を実行するには、以下の手順に従いま す。
 - a. [RAID Test] セクションで、テストのタイプとテストする RAID アレイを選択します。md0 アレイは小さいブート パーティシ ョンであり、md1 アレイはシステムの残りをカバーしています
 - b. [Submit] を選択します。



- c. テストの進行状況は、[RAID Status+Disk Utilization] 画面で追跡
 できます。「*RAID ステータスとディスク使用率の表示*『366p.
 』」を参照してください。オプション。
- d. テストが終了したら、結果を [Repair/Rebuild RAID] 画面で確認できます。「RAID ディスクの修復または再作成 『371p. 』」を参照してください。特定のアレイの [Mis-Match] 列に、問題が発生している可能性があることを示す 0 以外の値が表示されている場合は、ラリタン社のテクニカル サポートにご連絡ください。



ディスク テストのスケジュール

ディスク ドライブの SMART ベースのテストが定期的に実行されるようにスケジュールすることができます。ディスク ドライブのファームウェアがこれらのテストを実行します。結果は、[Repair/Rebuild] 画面で確認できます。「*RAID ディスクの修復または再作成* 『371p.』」を参照してください。

SMART テストは、CC-SG が機能し、使用されている間に実行できま す。これらが CC-SG のパフォーマンスに与える影響はほとんどありま せんが、CC-SG アクティビティによって、SMART テストの完了が大 幅に遅れる可能性はあります。したがって、テストを頻繁に実行するよ うにスケジュールしないことを推奨します。

SMART テストをスケジュールする場合は、以下のガイドラインに注意 してください。

- 指定した時刻に一度に実行できるテストは1 つだけです。
- ドライブがテスト中である場合は、別のテストはスケジュールされ ません。
- 2 つのテストを同じタイム スロットにスケジュールした場合は、時間がかかるテストが優先されます。
- テストは、指定された時間帯に実行されます。その時刻ちょうどに 開始されるとは限りません。
- 大量の CC-SG ロード、または毎日真夜中または正午に実行される バキューム処理など、負荷の高いディスク アクティビティが実行される時間帯に SMART テストをスケジュールしないでください。

注: デフォルトで、CC-SG では、毎日午前 2 時に Short テストを、また毎週日曜日の午前 3 時に Long テストを実行するようにスケジュールされています。これらのスケジュール済みのテストは両方のディスクドライブに適用されます。

- ディスク テストのスケジュールを変更するには、以下の手順に従い ます。
- 1. [Operation] > [Utilities] > [Disk / RAID Utilities] > [Schedule Disk Tests] を選択します。



File Operatio	n	r Cons	ole: S	chodult	a Nisk Te	ete						
SMART Test Disk sda:	Mo 1-	nth >12	Day of 1-:	Month >31	Day of	Wei >7	ek Hou 0->:	r 23				
[X] Long [X] Short [] Conveyance [] Offline]]]]]]]	[[[]	[7 [[[]]]	[03 [02 []]]	-			
Disk: sdb: [X] Long [X] Short [] Conveyance [] Offline	[[[]]]]]]	[7 [[[1 1 1	[03 [02 []]]	-			
											Submi	t >
SN:ACD7900052,	Ver	:4.1.6	.5.2 [Creater	d:Tue Dec	20	88-12-02	18	:04:36	EST	-050	0]
Help: <f1> //</f1>	Exit	: <ct]< td=""><td>.+Q> or</td><td><ctl+0< td=""><td>C> // Men</td><td>us</td><td>(Top - bain</td><td>):</td><td><ctl+< td=""><td><></td><td></td><td></td></ctl+<></td></ctl+0<></td></ct]<>	.+Q> or	<ctl+0< td=""><td>C> // Men</td><td>us</td><td>(Top - bain</td><td>):</td><td><ctl+< td=""><td><></td><td></td><td></td></ctl+<></td></ctl+0<>	C> // Men	us	(Top - bain):	<ctl+< td=""><td><></td><td></td><td></td></ctl+<>	<>		

- マウスでクリックするか、矢印キーでナビゲートし、スペース バー を押してテストのタイプを選択すると、そのタイプが X でマーク されます。異なるテストは異なる時間帯に実行します。
 - Short テストは、システムの負荷が小さい場合、約2分で終了 します。
 - Conveyance テストには約 5 分かかります。
 - Long テストには約 50 分かかります。
 - OffLine テストには最長 50 分かかります。
- 3. このテストを実行する日時を指定します。[Month]、[Day of Month] 、[Day of the Week]、[Hour] の各フィールドに数字を入力します。
 - [Day of the Week] フィールドでは、1 (月曜日) ~ 7 (日曜日) を 使用します。
 - [Hour] は 24 時間制で入力する必要があります。

注: フィールドを空にすると、すべての値と一致します。

4. [Submit] を選択します。



RAID ディスクの修復または再作成

このオプションには、ディスク ドライブおよび RAID アレイの詳細な ステータス情報の一部が表示され、また、ディスク ドライブの交換や RAID-1 ミラー アレイの再作成が必要かどうかが示されます。ディスク ドライブの交換またはホット スワップを行う前に、ラリタン社から交 換ユニットを入手します。

- ▶ RAID を交換または再作成するには、以下の手順に従います。
- 1. [Operation] > [Utilities] > [Disk / RAID Utilities] > [Repair/Rebuild RAID] を選択します。
- 2. [Replace??] 列または [Rebuild??] 列に [No] と表示されていない 項目がある場合は、ラリタン社のテクニカル サポートにご連絡くだ さい。
 - 正常なシステム:

CC-SG Administrator Console: Repair / Rebuild RAID: Disk Drive Status: Drive Health Attributes Errors Self Tests Replace?? sda OK OK OK OK No sdb OK OK OK OK No <hr/> <hr/> <h< th=""><th>File Operat</th><th>ion</th><th></th><th></th><th></th><th></th></h<>	File Operat	ion				
Disk Drive Status: Drive Health Attributes Errors Self Tests Replace?? sda OK OK OK OK No sdb OK OK OK OK No <hr/> <hr/> <	CC-SG Admini	strator Console:	Repair / Rebui	ld RAID: —		
Drive Nearth Attributes Errors Sett Tests Replace?? sda OK OK OK No sdb OK OK OK No	Disk Drive	Status:	Contract Contract	C-16 T-		
sdd OK OK OK NO sdb OK OK OK OK No <htps: td="" www.second.com<=""> <htps: td="" www.second.com<=""> <htps: td="" www.second.com<=""> <htps: td="" www.second.com<=""> RAID Array Status: <htps: td="" www.second.com<=""> <htps: td="" www.second.com<=""> <htps: td="" www.second.com<=""> <htps: td="" www.second.com<=""> Array State Events Elements Mis-Match Rebuild?? <htps: td="" www.second.com<=""> <htps: td="" www.second.com<=""> <htps: td="" www.second.com<=""> Md0 clean 48 2/2 0 No md0 clean 48 2/2 0 No md1 active 803765 2/2 0 No</htps:></htps:></htps:></htps:></htps:></htps:></htps:></htps:></htps:></htps:></htps:>	Drive	neatth Attr.	av	Sett le	sts keptace??	
Sub OK OK OK NO <health> <attributes> <errors> <self-tests> <all> RAID Array Status: Array State Events Elements Mis-Match Rebuild?? md0 clean 48 2/2 0 No md1 active 803765 2/2 0 No</all></self-tests></errors></attributes></health>	sua		OK	OK	No	
<pre><health> <attributes> <errors> <self-tests> <all> RAID Array Status: Array State Events Elements Mis-Match Rebuild?? md0 clean</all></self-tests></errors></attributes></health></pre>	500	UK UK	UK	UK	NO	
RAID Array Status: Array State Events Elements Mis-Match Rebuild?? md0 clean 48 2/2 0 No md1 active 803765 2/2 0 No Potential Operations: Replace Disk Drive > SN:ACD8505011 Ver:4.1.0.111 (Updated:Wed Dec 2008-12-03 10:50:24 EST -05001		<health> <attri< th=""><th>butes> <errors></errors></th><th><self-tes< th=""><th>sts> <all></all></th><th></th></self-tes<></th></attri<></health>	butes> <errors></errors>	<self-tes< th=""><th>sts> <all></all></th><th></th></self-tes<>	sts> <all></all>	
Array State Events Elements Mis-Match Rebuild?? md0 clean 48 2/2 0 No md1 active 803765 2/2 0 No Potential Operations: < Replace Disk Drive > SN:ACD8605011, Ver:4.1.0.1.11 (Updated:Wed Dec 2008-12-03 10:50:24 EST -05001)	RAID Array	Status:				
md0 clean 48 2/2 0 No md1 active 803765 2/2 0 No Potential Operations: Replace Disk Drive > Rebuild RAID Array > <	Array Stat	e	Events Elemen	ts Mis-Mat(ch Rebuild??	
mdl active 803765 2/2 0 No Potential Operations: <	md0 clean		48 2/2	0	No	
SN:ACD8605011, Ver:4.1.0.1.11 [Updated:Wed Dec 2008-12-03 10:50:24 EST -0500]	mdl activ	e	803765 2/2	0	No	
Potential Operations: < Replace Disk Drive > < Rebuild RAID Array > SN:ACD8605011, Ver:4.1.0.1.11 [Updated:Wed Dec 2008-12-03 10:50:24 EST -0500]	L					
SN:ACD8605011, Ver:4.1.0.1.11 [Updated:Wed Dec 2008-12-03 10:50:24 EST -0500]		Detect	isl Oserstient			
<pre></pre>		Potent.	Tal Uperations:	Derive a		
SN:ACD8605011, Ver:4.1.0.1.11 [Updated:Wed Dec 2008-12-03 10:50:24 EST -0500]		i	< Replace DISK	Drive >		
SN:ACD8605011, Ver:4.1.0.1.11 [Updated:Wed_Dec_2008-12-03_10:50:24_EST0500]			< Rebuild RAID /	Array >		
SN:ACD8605011, Ver:4.1.0.1.11 [Updated:Wed_Dec_2008-12-03_10:50:24_EST0500]						
SN:ACD8605011, Ver:4.1.0.1.11 [Updated:Wed Dec 2008-12-03 10:50:24 EST -0500]						
the second s	SN:ACD8605011	, Ver:4.1.θ.1.11	[Updated:Wed_D	ec 2008-12	-03 10:50:24 EST	-0500]
<pre>Help: <f1> // Exit: <ct1+q> or <ct1+c> // Menus (Top-bar): <ct1+x></ct1+x></ct1+c></ct1+q></f1></pre>	Help: <f1> //</f1>	Exit: <ctl+q></ctl+q>	or <ctl+c> // M</ctl+c>	enu <mark>s (Top-</mark> I	bar): <ctl+x></ctl+x>	



File Operation					
CC-SG Administra	tor Console: Repai	ir / Rebui	ld RAID: —		
Disk Drive Stat	US:				
Drive Hea	lth Attributes	s Errors	Self Tes	ts Replace??	1
sda OK	Pre-Fail	Errors	OK	Yes-PreFail	
sdb OK	OK	Errors	Errors	Yes-Warn	
<hr/> <hr/>	alth> <attributes< th=""><th><pre>> <errors></errors></pre></th><th><self-tes< th=""><th>ts> <all></all></th><th></th></self-tes<></th></attributes<>	<pre>> <errors></errors></pre>	<self-tes< th=""><th>ts> <all></all></th><th></th></self-tes<>	ts> <all></all>	
RAID Array Stat	us:				
Array State	Evei	nts Elemen	ts Mis-Matc	h Rebuild??	
md0 degraded,	clean 6	1/2	0	Yes->sdal	
mdl active	5	2/2	Θ	No	
	<mark>Potential O</mark> < Rep < Rebu	perations: lace Disk Hild RAID ,	D <mark>rive ></mark> Array >		
SN:ACD7900052, V	er:4.1.0.5.2 (Upda	ated:Tue D	ec 2008-12-	02 19:58:53 EST	-0500]
Help: <f1> // Ex</f1>	it: <ctl+q> or <ct< td=""><td>tl+C> // M</td><td>enus (Top-b</td><td>ar): <ctl+x></ctl+x></td><td></td></ct<></ctl+q>	tl+C> // M	enus (Top-b	ar): <ctl+x></ctl+x>	

複数の問題が表示された不自然なシステム:

Tab キーまたはマウス クリックを使用して、[**Disk Drive Status**]、 [**RAID Array Status**]、[**Potential Operations**] ボックス間を移動する と、表示されている情報が更新されます。

- 3. 詳細な SMART 情報を表示するには、[Disk Drive Status] セクショ ンでテーブルの下にあるいずれかのボタンを選択できます。オプシ ョン。
- 4. [Replace Disk Drive] または [Rebuild RAID Array] を選択した後、 画面の指示に従って操作を完了します。

診断コンソールでのトップ ディスプレイの表示

トップ ディスプレイでは、現在実行中のプロセスおよびそのプロセスの属性のリストと、システムの全体的なヘルスを表示できます。

- ▶ **CC-SG** で実行されているプロセスを表示するには、以下の手順に 従います。
- 1. [Operation] > [Utilities] > [Top Display] を選択します。



2. 実行中のプロセスの合計、スリープ中のプロセスの合計、全プロセ スの合計、停止したプロセスが表示されます。

top - Tasks	20:46:55	up 1	day 1	/, 9:2 cunning	5, 1	8 user 8 slee	rs,	, loa ing	ad ave	rage: 0.27, 0.32, 0.28
Cpu(s)	: 0.2%us	, Θ	.389	iy, θ.	0%n1	99.5	\$	id, (9.0%wa	, 0.0%hi, 0.0%si, 0.0%st
Mem:	4152196	(tot	al,	16467	16k I	used,		250548	30k fre	ee, 608628k buffers
Swap :	2031608	tot	al,		0K I	used,		203160	98k fro	ee, S65668k cached
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	SMEN	TIME+ COMMAND
19043	sg	25	- 0	1343m	272m	10m	S	. 0	6.7	2:02.46 java
1	root	15	0	2060	580	504	s	0	0.0	0:00.91 init
2	root	RT	-5	0	0	0	s	0	0.0	0:00.64 migration/0
3	root	34	19	0	0	0	s	0	0.0	0:00.22 ksoftirqd/0
4	root	RT	-5	θ	0	θ	s	0	0.0	0:00.00 watchdog/0
5	root	RT	-5	θ	0	θ	s	θ	0.0	0:49.48 migration/1
6	root	- 34	19	θ	0	θ	s	θ	θ.0	0:00.27 ksoftirqd/l
7	root	RT	-5	θ	0	θ	s	θ	θ.0	0:00.00 watchdog/1
8	root	10	- 5	0	0	θ	s	θ	θ.Θ	0:00.84 events/0
9	root	10	-5	•	0	•	s	θ	0.0	0:00.21 events/1
10	root	10	-5	0	0	•	s	•	0.0	0:03.04 khelper
11	root	10	-5	0	Θ	0	s		0.0	0:00.00 kthread
15	root	10	- 5	0	Θ	0	s		0.0	0:00.10 kblockd/0
16	root	10	- 5	0	Θ	. 0	s		0.0	0:00.00 kblockd/1
17	root	15	- 5	0	0		S		0.0	0:00.00 kacpid
170	root	15	- 5	0	0	0	S	. 0	0.0	0:00.00 cqueue/0
171	root	15	-5	θ	0	0	S	θ.	θ.0	0:00.00 cqueue/1

3. 「h」と入力すると、トップ コマンドのヘルプ画面が表示されます。ヘルプを表示する F1 は、ここでは機能しません。

NTP ステータスの表示

CC-SG で NTP タイム デーモンが設定され、稼働中であれば、そのス テータスを表示できます。NTP デーモンは、CC-SG 管理者の GUI で ある Admin Client でしか設定できません。

- CC-SG NTP デーモンのステータスを表示するには、次の手順に従います。
- 1. [Operation] > [Utilities] > [NTP Status Display] を選択します。



• 次の画面の場合は、NTP が有効になっていないか、正しく設定 されていません。

Fi	le Ope	ration									
[-SG Adm	inistra	ator L	onsote	: 11	P Status					
NTP	Daemon	does	not ap	pear t	o be	running					
											< Refresh >
SN	: ACD798	9052,	Ver:4.	1.0.5.	2 [U	pdated:T	ue Dec	2008-	12-02 2	0:47:35	EST -0500]
Hel	o: <f1></f1>	77 E	xit: <	ctl+Q>	or	<ctl+c></ctl+c>	// Men	us (To	p-bar):	<ctl+< td=""><td>X></td></ctl+<>	X>

■ 次の画面の場合は、NTP が正しく設定され、実行されています

0

time correct polling serve	to within 26 ms er every 64 s	. 100.91		Stratom		
client 127.12 client 192.10 remote	27.1.0 58.51.11 local	st po	ll reac	ı delay	offset	disp
=127.127.1.0 *192.168.51.11	127.0.0.1 192.168.51.26	10 5	64 377 64 377	0.00000 0.00043	0.0000000 -0.013413	0.03058 0.08279
						< Refre



システム スナップショットの取得

CC-SG が適切に機能していない場合、システムのログ、設定、または データベースなど、CC-SG に保存されている情報を取得してラリタン 社のテクニカル サポートに提供できると、分析とトラブルシューティ ングを行う上で非常に役立ちます。

- ▶ 1: CC-SG のスナップショットを取得する場合の手順:
- 1. [Operation] > [Utilities] > [System Snapshot] を選択します。
- [Yes] をクリック、または選択します。[System Snapshot] メニュ ーが表示されます。
- 画面に表示されている [%Used] の値が 60% 未満であることを確認します。これで、スナップショット操作で使用する十分な空き領域があることを確認できます。空き領域がない場合は、操作を中断し、クリーンアップ操作を実行するか、ラリタン社のテクニカル サポートにご連絡ください。
- 4. [System Snapshot] オプションは 2 つの領域に分かれています。
 - [Snapshot Configuration] には、スナップショットを作成できる CC-SG データのリストが表示されます。
 - [Snapshot Configuration] には、スナップショット操作が有効で あるときに実行できる操作のリストが表示されます。
- 通常は、デフォルトのスナップショット選択を変更する必要はあり ませんが、ラリタン社のテクニカル サポートから要求されている場 合は例外です。要求されている場合は、マウスでクリックするか、 矢印キーでナビゲートし、スペース バーを押して、実行するスナッ プショット オプションを選択します。これで、選択されたオプショ ンが X でマークされます。
- 6. [Submit] をクリックまたは選択して、スナップショット操作を続け ます。
- 7. スナップショット処理中、画面で項目のリストが高速でスクロール 表示されます。ときどき CC-SG がしばらく停止しますが、これは 正常です。
- 8. スナップショット処理が終了したら、CC-SG によって、スナップ ショットについての以下のような情報が表示されます。
 - CC-SG スナップショット ファイルの場所およびファイル名
 - サイズ
 - MD5 チェックサム

スナップショット情報は参照用なので、書き留める必要はありませ ん。

9. Enter キーを押して [System Snapshot] メニューに戻ります。



- ▶ 2: CC-SG スナップショット ファイルを取得する場合の手順:
- サポートされているインターネット ブラウザを使用して URL を「 http(s): //<IP_address>/upload/」と入力します。
 <IP_address> は、CC-SG の IP アドレスです。/upload の後のスラッシュ (/) は必須です。たとえば「https: //10.20.3.30/upload/」のように入力します。
- [Enter Network Password] ダイアログ ボックスが表示されます。診 断コンソールの admin アカウントのユーザ名とパスワードを入力 し、[OK] をクリックしてログインします。
- 3. CC-SG でこれまで取得した、利用可能なスナップショット ファイ ルがすべて表示されます。

注: CC-SG はスナップショット ファイルを 10 日間だけ保持する ので、その間にファイルを取得する必要があります。

- 適切なファイル名のスナップショット ファイル、または最新のスナ ップショット ファイルである "snapshot" という名前のファイルを クリックします。ファイルはすでに圧縮され、暗号化され、署名さ れているので、それをバイナリ モードで転送する必要があります。
- 5. ファイルを IE で保存する場合は、[名前を付けて保存] ダイアログ ボックスの [ファイルの種類] ドロップダウン リストから [すべて のファイル] を選択して、raw ファイルとして保存します。

診断コンソールのビデオ解像度の変更

Raritan は、メニューを適切に表示するために、モニタで診断コンソー ルのビデオ解像度を調整することを推奨します。

- ▶ ビデオ解像度を調整するには、以下の手順に従います。
- CC-SG をリブートします。「診断コンソールを使用した CC-SG の リブート 『354p. 』」を参照してください。
- 以下のメッセージが表示されたら、5 秒以内に Esc または矢印キ ーなどのいずれかの文字キーを押して、GRUB メニューに入ります。

Press any key to enter the menu

Booting CentOS (x.x.x) in x seconds....

3. 上下の矢印キーを使用して [1024x768 / 24-bit] オプションをハイラ イトし、Enter キーを押します。



Ch 17 Power IQ の統合

CC-SG と Power IQ がある場合、それらを併用するにはいくつかの方 法があります。

- CC-SG から Power IQ IT デバイスのパワー制御を行います。 たとえば、CC-SG ノードでもある Power IQ IT デバイスのパワー 制御を行う場合は、Power IQ Proxy インタフェースを使用して CC-SG でパワー制御コマンドを指定できます。
- 2. CSV ファイルのインポートとエクスポートによって、これらの 2 つのシステム間でデータを共有します。

たとえば、IP ネットワーク上に設置された多数の Dominion PX デ バイスを CC-SG で管理している場合、すべてのノード名を含む CSV ファイルを CC-SG からエクスポートし、指定どおりに編集 してから Power IQ にインポートできます。「Power IQ で使用する Dominion PX データのエクスポート 『385p. 』」を参照してくだ さい。

または、設置された多数の Dominion PX デバイスを Power IQ で 管理し、現在の IT デバイス名をノードとして CC-SG に取り込む 場合は、ファイルを Power IQ からエクスポートし、指定どおりに 編集してから CC-SG にインポートできます。「*Power IQ からの電 源タップのインポート*『383p.』」を参照してください。

 Power IQ を CC-SG と同期し、Power IQ で設定された IT デバイ スを CC-SG に自動的にインポートします。「Power IQ および CC-SG の同期の設定 『380p. 』」を参照してください。

この章の内容

Power IQ IT デバイスのパワー制御

ノードとして CC-SG に追加した Power IQ IT デバイスのパワー制御 を CC-SG で行うことができます。

これにより、CC-SG で管理されていない PDU に接続されたノードの パワー制御が可能になります。



Power IQ サービスの設定

Power IQ プロキシ インタフェースをノードに追加する前に Power IQ サービスを設定するか、または Power IQ を CC-SG と同期して IT デバイスを CC-SG にノードとして追加する必要があります。これは、 CC-SG の [アクセス] メニューから行います。

Power IQ サービスを設定する場合は、CC の設定と制御の権限が必要です。

- Power IQ サービスを設定するには、以下の手順に従います。
- Power IQ で Web API が有効になっていることを確認します。[設定] タブで、[Security and Encryption(セキュリティと暗号化)] セクションの [Web API(Web API)] をクリックします。

[Enable Web API(Web API を有効にする)] チェックボックスをオン にして、[保存] をクリックします。

- Power IQ でパワー制御が有効になっていることを確認します。[設定] タブで、[Appliance Administration(装置の管理)] セクションの [Power Control Options(パワー制御オプション)] をクリックします。 [Enable Power Control(パワー制御を有効にする)] チェックボック スをオンにして、[保存] をクリックします。
- CC-SG Admin Client で、[アクセス] > [Power IQ Services (Power IQ サービス)] > [Add Power IQ Services (Power IQ サービスの追加)] を選択します。[New Power IQ Services Configuration (新規 Power IQ サービスの設定)] ダイアログ ボックスが表示されます。
- [Power IQ Device Name (Power IQ デバイス名)] フィールドにデバ イス名を入力します。サービスを提供する Power IQ デバイスの名 前は一意である必要があります。重複する名前は使用できません。 名前の長さに関する CC-SG のルールについての詳細は、「命名規 則 『435p. 』」を参照してください。
- [IP アドレス/ホスト名] フィールドにデバイスの IP アドレスまた はホスト名を入力します。ホスト名のルールについては、「用語/略 語『2p.』」を参照してください。
- 新しいデバイスと CC-SG との間でのタイムアウトまでの時間を、[ハートビート タイムアウト (秒)] フィールドに秒単位 (30~ 50,000) で入力します。
- 7. 以下の手順で認証情報を入力します。
 - 認証にサービス アカウントを使用するには、[サービス アカウント資格情報の使用] チェックボックスを選択します。使用するサービス アカウントを [サービス アカウント名] メニューで選択します。

または

• 認証用のユーザ名とパスワードを入力します。


- 8. このデバイスの短い説明を [説明] フィールドに入力します。オプション。
- [接続テスト] をクリックします。エラー メッセージについての詳細は、「Power IQ への接続のトラブルシューティング 『379p. 』」 を参照してください。同期を使用している場合は、「Power IQ および CC-SG の同期の設定 『380p. 』」を参照してください。

Power IQ への接続のトラブルシューティング

Power IQ への接続のトラブルシューティングを行うには、想定される 以下のエラー メッセージおよび解決策を確認してください。

原因を特定し、設定を編集して修正します。「**Power IQ サービスの設定 『378**p. 』」を参照してください。

メッセージ	解決策
Unable to communicate with managing device <name> at <ip>.(<ip> の管理デバイス <名前> と通信できません。)</ip></ip></name>	 このエラーは、複数の状況を示している可能性があります。 接続がリモートで拒否されました。リモートアドレスまたはリモートポートでプロセスが受信していません。 ファイアウォールを確認してください。ファイアウォールが介在しているため、または中間ルータが停止している場合は、リモートホストに到達できません。 ホストが不明です。入力されたホスト名から IP アドレスを解決できませんでした。
Authentication failed.(認証に 失敗しました。)	ユーザ名およびパスワードが正しく ありません。
Unable to communicate with managing device <name> at <ip>, make sure its Web API is enabled.(<ip> の管理デバ イス <名前> と通信できませ ん。Web API が有効になっ ていることを確認してくださ い。)</ip></ip></name>	Web API が Power IQ で有効にな っていません。Power IQ にログイ ンし、[設定] > [Web API(Web API)] に移動します。次に、[Enable Web API(Web API を有効にする)] を選択 し、[保存] をクリックします。



Power IQ IT デバイスのパワー制御の設定

Power IQ サービスを設定したら、**CC-SG** を設定して必要なノードとインタフェースを追加できます。

- 1. パワー制御を実行する IT デバイスを追加します。「ノードの追加 『123p. 』」を参照してください。
- ノードに Power IQ Proxy のパワー制御インタフェースを追加します。「インタフェースの追加 『140p. 』」および「Power IQ Proxy のパワー制御接続のインタフェース 『147p. 』」を参照してください。

Power IQ および CC-SG の同期の設定

CC-SG は、Power IQ で設定された IT デバイスをノードとして **CC-SG** に追加するために、Power IQ と同期します。同期時には、識別 された新しい IT デバイスごとに Power IQ プロキシ インタフェース を使用してノードが作成されます。重複するノードが検出されると、選 択した同期ポリシーにより、ノードの統合、名前の変更、または拒否を 行うかどうかが決定されます。

いつでも手動で同期できます。あるいは、繰り返し実行する作業をタス クとして設定できます。「タスク マネージャ 『311p. 』」を参照して ください。

また、すべての IT デバイスを Power IQ から取得するか、または CC-SG がフィルタで許可された IT デバイスとだけ同期するようにフ ィルタを設定することもできます。

- ▶ 手順 1 CC-SG と同期される Power IQ に接続を追加する:
- 「Power IQ サービスの設定 『378p. 』」を参照してください。
- ▶ 手順 2- フィルタを作成する(オプション):

フィルタはオプションです。フィルタを作成しない場合は、この Power IQ で設定されたすべての IT デバイスが、同期ポリシーに従って CC-SG に追加されます。フィルタは、選択した Power IQ インスタン スだけに適用されます。

- [アクセス] > [Power IQ Services(Power IQ サービス)] を選択し、同 期する Power IQ の名前を選択します。
- 2. [Synchronization(同期)] セクションで、フィールドの一覧からフィ ールド名を選択します。一覧表示されるフィールド名は、Power IQ のフィールドを参照します
- 3. 演算子の一覧から検索演算子を選択します。



- LIKE では、指定したフィールドの値に指定したテキストを含む IT デバイスが返されます。たとえば、値 "win" は、"windows" 、"windows2k"、"win7" などに含まれています。
- EQUAL では、指定したフィールドの値と正確に同じ値を含む IT デバイスだけが返されます。
- 4. 指定した演算子を使用して、指定したフィールドに検索する値を入 力します。
- 5. [OK] をクリックして保存するか、このダイアログを開いたまま手順 3 に進みます。
- 手順 3- 同期ポリシーを作成する:

注: 同期ポリシーは、CC-SG で設定されたすべての Power IQ インス タンスに適用されます。各ポリシーおよびその他の同期結果についての 詳細は、「Power IQ 同期ポリシー 『382p. 』」を参照してください。

- 1. [Synchronization(同期)] セクションで、同期ポリシーに関する以下 のラジオ ボタンを選択します。
 - Consolidate Nodes(ノードの統合)
 - Rename Duplicate Nodes(重複するノードの名前の変更)
 - Reject Duplicate Nodes(重複するノードの拒否)
- [OK] をクリックして保存します。手動での同期およびタスクによる 同期についての詳細は、「Power IQ および CC-SG の同期『381p. 』」を参照してください。

Power IQ および CC-SG の同期

同期設定を指定したら、いつでも手動で同期できます。または、定期的 に同期するタスクを作成できます。

同期するには、デバイス、ポート、およびノードの管理権限が必要です。

同期設定を指定する方法についての詳細は、「**Power IQ および CC-SG** の同期の設定 『380p. 』」および「**Power IQ** 同期ポリシー 『382p. 』 」を参照してください。

今すぐ Power IQ および CC-SG を同期するには、以下の手順に従 います。

[今すぐ同期] をクリックすると、選択した Power IQ インスタンスだけ が同期されます。スケジュールに従ってすべての Power IQ インスタン スを同期する場合は、タスクを作成できます。次の手順を参照してくだ さい。

 [アクセス] > [Power IQ Services (Power IQ サービス)] を選択し、同 期する Power IQ インスタンスを選択します。



- 2. フィルタおよびポリシーが正しいことを確認したら、[今すぐ同期] をクリックします。
- 3. [Synchronization Status Message(同期ステータス メッセージ)] ダ イアログが開きます。同期の結果のメッセージを確認します。
- Power IQ および CC-SG をタスクとして同期するには、以下の手順に従います。
- "PowerIQ Synchronization(Power IQ 同期)" タスクを作成します。
 「タスクのスケジュール 『313p. 』」を参照してください。

Power IQ 同期ポリシー

重複するノードが検出されると、選択した同期ポリシーにより、ノード の統合、名前の変更、または拒否を行うかどうかが決定されます。

同期ポリシーを設定するには、「**Power IQ および CC-SG の同期の設** 定 **『380**p. **』**」を参照してください。

- ▶ 同期ポリシー:
- Consolidate Nodes(ノードの統合):
 IT デバイス (外部キーで特定) を複数の Power IQ から取得する場合、ノードには、Power IQ ごとに Power IQ プロキシ インタフェースが設定されます。CC-SG では、1 つのノードに重複したインタフェース名を付けることができます。
- Rename Duplicate Nodes(重複するノードの名前の変更):
 IT デバイス (外部キーで特定)を複数の Power IQ から取得する場合は、1 つの Power IQ プロキシ インタフェースを備えた Power IQ ごとに 1 つのノードが作成されます。カッコ付きの数字をノード名に付加することで、ノード名が変更され、ノードが一意になります。たとえば、node、node(2)、node(3) のようになります。
- Reject Duplicate Nodes(重複するノードの拒否): IT デバイス (外部キーで特定) を複数の Power IQ から取得する場合、最初のインスタンスには、1 つのノードおよび作成された Power IQ プロキシ インタフェースが設定されますが、それ以降の インスタンスは拒否され、エラーとしてログに記録されます。これ はデフォルトです。



▶ その他の同期結果:

同期時に、外部キーで特定された IT デバイスが存在しておらず、ノードには Power IQ プロキシ インタフェース タイプの 1 つのインタフェースしか関連付けられていない場合、そのノードは CC-SG から削除されます。

ノードに、1 つの Power IQ プロキシ インタフェースおよび他のイン タフェースが関連付けられている場合は、その Power IQ プロキシ イ ンタフェースだけが CC-SG から削除されます。

Power IQ インスタンスが CC-SG から削除されると、これらの結果は 同じになります。

Power IQ からの Dominion PX データのインポートとエクスポート

Power IQ から Dominion PX データをインポートおよびエクスポート するには、CC の設定と制御権限、およびデバイス、ポート、およびノ ードの管理権限が必要です。

Power IQ からの電源タップのインポート

Dominion PX デバイスとそのコンセント名を Power IQ からインポー トできます。Dominion PX デバイスがすでに CC-SG によって管理さ れている場合は、まずそれらのデバイスを削除する必要があります。イ ンポートによって Dominion PX デバイスが追加され、CSV ファイルで 指定されているコンセントの設定と命名が行われます。

CSV ファイル内の Dominion PX 以外のデバイスとコンセントは、イン ポート時に無視されます。

Power IQ サービスを使用して、Dominion PX デバイスおよび Power IQ からインポートできない他のベンダの電源タップに接続されている Power IQ IT デバイスのノードを作成できます。「*Power IQ IT デバイス* のパワー制御『377p.』」を参照してください。

- ▶ 手順 1: CSV ファイルを Power IQ からエクスポートする
- 1. Power IQ にログインし、ダッシュボードに移動します。
- 2. [Outlet Naming (コンセントの命名)] をクリックします。
- 3. [インポート] の横のリンクをクリックして、現在のコンセント名の CSV ファイルをエクスポートします。
- 4. ファイルを開くか保存します。ファイルに Power IQ 内のすべての コンセントが格納されます。
- ▶ 手順 2: CSV ファイルを編集する
- 1. エクスポートした CSV ファイルを編集します。



- 2. PX 名を含む列を削除します。後で各 PX デバイスを追加するコマ ンドを含む行を追加します。
- 3. すべての行の先頭に 2 つの列を挿入します。
 - a. 1 列目にはコマンド ADD を入力します。
 - b. 2 列目にはタグ OUTLETS を入力します。
- 4. 追加する PX デバイスごとに行を挿入します。

列番号	タグまたは値	詳細
1	ADD	すべてのタグの最初の列はコマンド ADD です。
2	PX-DEVICE	左記のとおりにタグを入力します。 タグでは大文字と小文字は区別され ません。
3	PX デバイスの IP アドレ スまたはホスト名	必須フィールド。
4	ユーザ名	必須フィールド。
5	パスワード	必須フィールド。
6	すべてのアウトレットを設 定	TRUE または FALSE デフォルトは FALSE です。
7	説明	オプション。

▶ 手順 3: 編集した CSV ファイルを CC-SG にインポートする

- CC-SG Admin Client で、[管理] > [インポート] > [電源タップのイン ポート] を選択します。
- 2. [参照] をクリックし、インポートする CSV ファイルを選択します。[開く] をクリックします。
- 3. [確認] をクリックします。[分析レポート] 領域にファイルの内容が 表示されます。
 - ファイルが有効でない場合は、エラー メッセージが表示されます。[OK] をクリックし、ページの [問題] 領域でファイルに関する問題の説明を参照します。[ファイルに保存] をクリックして問題リストを保存します。CSV ファイルを修正し、再度検証します。「CSV ファイルの問題のトラブルシューティング 『414p.』」を参照してください。
- 4. [インポート] をクリックします。



- 5. [アクション] 領域でインポート結果を確認します。正常にインポートされたアイテムは、緑色のテキストで表示されます。インポート に失敗したアイテムは、赤いテキストで表示されます。重複するア イテムがすでに存在するか、またはすでにインポートされているた めにインポートに失敗したアイテムも赤いテキストで表示されます
- 6. インポート結果の詳細を参照するには、監査証跡レポートを確認し ます。「*インポートに関する監査証跡エントリ* 『413p. 』」を参照 してください。

Power IQ で使用する Dominion PX データのエクスポート

CC-SG で設定されている Dominion PX デバイスに関するデータを CSV ファイルにエクスポートできます。ファイルにエクスポートされ たデータは、CSV ファイルの一部として、Power IQ へのデータのイン ポートに使用できます。ファイルの情報には、Dominion PX デバイス、 コンセント名、および IT デバイス名が含まれます。

エクスポートできるのは、IP ネットワークに接続された Dominion PX デバイスのみです。これには、管理対象電源タップとしてのみ設置され 、IP ネットワーク上でデバイスとしてアクセスできない Dominion PX 電源タップは含まれません。

注: エクスポートした Power IQ データは、ファイルを指定どおりに編 集した後、Power IQ へのインポートにのみ使用します。ファイルを CC-SG にインポートすることはできません。

▶ 手順 1: CSV ファイルを CC-SG からエクスポートする

- [エクスポート]>[パワー IQ データのエクスポート] をクリックします。
- 2. [ファイルにエクスポート] をクリックします。
- 3. ファイルの名前を入力し、保存する場所を選択します。
- 4. [保存] をクリックします。

▶ 手順 2: CSV ファイルを編集して Power IQ にインポートする

エクスポート ファイルには、3 つのセクションが含まれています。各 セクションを Power IQ の複数タブの CSV インポート ファイルの一 部として使用する方法については、CSV ファイルのコメントを参照し てください。

Raritan.com の「Support」 セクションの「Firmware and Documentation」ページにある『Power IQ ユーザ ガイド』および CSV Import Template を参照してください。



Ap AV1 および E1 の仕様

この章の内容

V1	モデル
E1	モデル

V1 モデル

V1 一般仕様	
フォーム ファクタ	1U
外形寸法 (幅 x 奥行き x 高さ)	24.21"x 19.09" x 1.75"615 mm x 485 mm x 44 mm
重量	10.80kg
電源	単一電源 (1 x 300 W)
動作温度	10° - 35° (50°- 95°)
平均故障間隔 (MTBF)	36,354 時間
KVM 管理ポート数	(DB15 + PS2 または USB キーボード/マウス)
シリアル管理ポート	DB9
コンソール ポート	2 x USB 2.0 ポート

V1 環境要件

動作時	
湿度	8% \sim 90% RH
海抜高度	0 ~ 3,000 m の高度で適切に作動。 保管は 12,000 m まで (推定)
振動	5-55-5 HZ、0.38 mm、1 サイクル 1 分、 軸 (X、Y、Z) ごとに 30 分
衝擊	なし
非動作時	
温度	-40° - +60° (-40°-140°)



Ap A: V1 および E1 の仕様

動作時	
湿度	5% \sim 95% RH
海抜高度	0 ~ 3,000 m の高度で適切に作動。 保管は 12,000 m まで (推定)
振動	5-55-5 HZ、0.38 mm、1 サイクル 1 分、 軸 (X、Y、Z) ごとに 30 分
衝撃	なし

E1 モデル

E1 一般仕様	
フォーム ファクタ	2U
外形寸法 (幅 x 奥行き x 高さ)	27.05"x 18.7" x 3.46"-687 mm x 475 mm x 88 mm
重量	20 kg
電源	SP502-2S ホットスワップ可能 500W 2U 電源
動作温度	$0~\sim~50^\circ{ m C}$
平均故障間隔 (MTBF)	53,564 時間
KVM 管理ポート数	PS/2 キーボード/マウス ポート、1 VGA ポート
シリアル管理ポート	UART 16550 高速シリアル ポート
コンソール ポート	2 x USB 2.0 ポート

E1 環境要件

動作時	
湿度	5 ~ 90%、結露なし
海拔高度	海抜 2,500 m まで
振動	毎時 0.5g の等加速度で 10 Hz ~ 500 Hz スイー プ (X 軸、Y 軸、Z 軸方向)
衝撃	½ 正弦波で 5g/11 ms X 軸、Y 軸、Z 軸方向)



動作時	
非動作時	
温度	-40 \sim 70° C
湿度	5 ~ 90%、結露なし
海抜高度	海抜 12,000 m まで
振動	毎時 2g の等加速度で 10 Hz ~ 500 Hz スイープ (X 軸、Y 軸、Z 軸方向)
衝撃	½ 正弦波で 30 g/11 ms X 軸、Y 軸、Z 軸方向)



この付録では、一般的な CC-SG 配備のネットワーク要件 (アドレス、 プロトコル、ポート) について説明します。この中で、外部アクセスの 場合と、内部セキュリティおよびルーティング ポリシーを強化する場 合の両方について、ネットワークを設定する方法を説明します。TCP/IP ネットワーク管理者向けの詳細情報も記載されています。場合によって は、TCP/IP 管理者が CC-SG 管理者の超える役割と責任を持つことが あります。この付録は、管理者が CC-SG とそのコンポーネントをサイ トのセキュリティ アクセス ポリシーおよびルーティング ポリシーに 統合する上で役立ちます。

CC-SG とその関連コンポーネントで必要になるプロトコルとポートを 以下の表に示します。

この章の内容

CC-SG	3 ネットワークに必要なオープン ポート: 要旨	
CC-SG	3 通信チャンネル	

CC-SG ネットワークに必要なオープン ポート: 要旨

次のポートを開いてください。

ポート番号	プロトコル	目的	詳細
80	ТСР	CC-SG への HTTP アクセス	暗号化されません。
443	TCP	CC-SG への HTTPS (SSL) ア クセス および Dominion KXII に接続されたノ ードへのノード アクセス (ダ イレクト モード)	SSL/AES-128/AES-256 暗号化。
8080	ТСР	CC-SG → PC クライアント	設定されている場合は SSL/AES-128/AES-256 暗号化。
2400	TCP	ノード アクセス (プロキシ モ ード)	外部的にアクセスされる Raritan デバイスごとにこのポートを開く 必要があります。この表の他のポ ートは、CC-SG にアクセスする 場合にのみ開く必要があります。 デバイスで暗号化が設定されてい



ポート番号	プロトコル	目的	詳細
			る場合、リリース 2.1.10 以降の Dominion KX II デバイスでのみ 暗号化されます。
5000	TCP	ノード アクセス (ダイレクト モード)	外部的にアクセスされる Raritan デバイスごとにこのポートを開く 必要があります。この表の他のポ ートは、CC-SG にアクセスする 場合にのみ開く必要があります。 設定されている場合は AES-128/AES-256 暗号化。
制御システム ノードの場 合 80 および 443 仮想ホスト ノードおよび 仮想マシン ノードの場合 80、443、902、903	ТСР	仮想ノード アクセス	なし
51000	TCP	SX ターゲット アクセス (ダイ レクト モード)	設定されている場合は AES-128/AES-256 暗号化。

▶ 必要なオープン ポートに対する可能性のある例外:

CC-SG へのすべてのアクセスが HTTPS アドレスを介して行われる場合は、ポート 80 を閉鎖できます。

ファイアウォールからの接続に CC-SG プロキシ モードを使用する場 合は、ポート 5000 と 51000 を閉鎖できます。



CC-SG 通信チャンネル

各通信チャネルについて説明します。通信チャネルごとに表には以下の ものが含まれます。

- 通信者によって使用されるシンボリック IP アドレス。こうした IP アドレスは、通信エンティティ間のすべての通信経路上で許可され たものになっている必要があります。
- 通信が開始される方向。これは、特定のサイト ポリシーにとっては 重要になる場合があります。CC-SG が所定の役割を果たすには、 通信者間のパスが利用可能になっている必要があり、またネットワ ーク障害の場合に使用できる代替経路が準備されている必要があり ます。
- CC-SG によって使用されるポート番号とプロトコル。
- ポートが設定可能であるかどうか。つまり、ネットワークの他のア プリケーションとの整合性のため、あるいはセキュリティ上の理由 のために、ポート番号をリストされたデフォルトと異なる値に変更 できるようなフィールドを、Admin Client または診断コンソールが 提供しているかどうかを示しています。
- 通信方式、通信チャネルを介して渡されるメッセージ、その暗号化 に関する詳細。

CC-SG と Raritan デバイス

CC-SG の主な役割の 1 つに Raritan デバイス (Dominion KX など) を 管理して、制御することがあります。一般的には、CC-SG は TCP/IP ネットワーク (ローカル、WAN、または VPN) 上でこれらのデバイス と通信します。その際、次に示すように TCP と UDP の両方のプロト コルが使用されます。

通信方向	ポート番号	プロトコル	設定可否	詳細
CC-SG → ローカル ブロー ドキャスト	5000	UDP	ा	ハートビート
CC-SG→ リモート LAN IP	5000	UDP	म	ハートビート
CC-SG → Raritan デバイス	5000	ТСР	ा	RDM プロトコル RC4/AES-128/AES-2 56 暗号化。
Raritan デバイス → CC-SG	5001	UDP	不可	ハートビート
$\text{CC-SG} \rightarrow \text{Dominion PX}$	623 443	UDP	不可 不可	



通信方向	ポート番号	プロトコル	設定可否	詳細
CC-SG → Dominion KXII (ダ イレクト モード)	443	TCP	不可	

CC-SG クラスタリング

オプションの CC-SG クラスタリング機能を使用する場合、内部接続の サブネットワーク用に次のポートが利用可能になっている必要がありま す。この機能を使用しない場合、これらのどのポートも開く必要はあり ません。

クラスタ内の各 CC-SG は別個の LAN にあってもかまいません。ただし、ユニット間の内部接続の信頼性が極めて高く、ネットワーク競合の 傾向が低い場合に限ります。

CC-SG クラスタ内でのプライマリからバックアップへの切り替えに よって、複数の TCP/IP 接続が保持され、開始されます。これらの接 続は、長期間アイドル状態になる可能性がありますが、クラスタの動 作に必要です。

VPN またはファイアウォールを介した CC-SG から CC-SG クラス タへのすべての接続がタイムアウトしたり、ブロックされたりしない ようにしてください。これらの接続がタイムアウトすると、クラスタ が失敗します。

通信方向	ポート番号	プロトコル	設定可否	詳細
CC-SG → ローカル ブロー ドキャスト	10000	UDP	不可	ハートビート
CC-SG → リモート LAN IP	10000	UDP	不可	ハートビート
CC-SG → CC-SG	5432	TCP	不可	プライマリの HA-JDBC からバッ クアップ PostgreSQL DB サー バまで。 暗号化されません。
$CC\text{-}SG\toCC\text{-}SG$	8732	TCP	不可	プライマリ バックア ップ サーバ同期のク ラスタ化制御データ 交換。 MD5 暗号化。
$CC\text{-}SG\toCC\text{-}SG$	3232	TCP	不可	プライマリ バックア ップ SNMP 同期構



通信方向	ポート番号	プロトコル	設定可否	詳細
				成変更転送。
				暗号化されません。

インフラストラクチャ サービスへのアクセス

CC-SG は、DHCP、DNS、NTP など、いくつかの業界標準のサービス を使用するよう設定できます。これらのポートおよびプロトコルは、 CC-SG とこれらのオプション サーバとの通信を可能にするために使用 されます。

通信方向	ポート番号	プロトコル	設定可否	詳細
DHCP サーバ \rightarrow CC-SG	68	UDP	不可	IPv4 DHCP 標準
CC-SG → DHCP $+-$ バ	67	UDP	不可	IPv4 DHCP 標準
NTP サーバ → CC-SG	123	UDP	不可	NTP 標準
$CC\text{-}SG\toDNS$	53	UDP	不可	DNS 標準

PC クライアントから CC SG

PC クライアントは、以下の 3 つのモードのいずれかで CC-SG と接続されます。

- Web ブラウザを介した Admin Client または Access Client。
 CC-SG は、ブラウザ接続に SSL v2、SSL v3、TLS v1 をサポートします。これらの暗号化方式は、ブラウザで設定できます。
- SSH 経由のコマンド ライン インタフェース (CLI)
- 診断コンソール

通信方向	ポート番 号	プロトコル	設定可否	詳細
PC クライアント→ CC SG	443	ТСР	不可	クライアント - サーバ通信。 設定されている場合は SSL/AES-128/AES-256 暗号 化。
PC クライアント→ CC SG	80	ТСР	不可	クライアント - サーバ通信。 暗号化されません。SSL が有 効な場合は、ポート 80 が 443 にリダイレクトされます 。



通信方向	ポート番 号	プロトコル	設定可否	詳細
PC クライアント→ CC SG	8080	TCP	不可	クライアント - サーバ通信。 設定されている場合は SSL/AES-128/AES-256 暗号 化。 ポート 8080 は、PC クライ アントではなく CC-SG で開 きます。
PC クライアント → CLI SSH	22	ТСР	Π	クライアント - サーバ通信。 設定されている場合は SSL/AES-128/AES-256 暗号 化。
PC クライアント→診 断コンソール	23	ТСР	Π	クライアント - サーバ通信。 設定されている場合は SSL/AES-128/AES-256 暗号 化。

PC クライアントとノード

CC-SG のもう 1 つの重要な役割は、PC クライアントをさまざまなノ ードに接続することです。こうしたノードは、Raritan デバイスにシリ アルまたは KVM コンソールで接続することができます (この状態をア ウト オブ バンド接続といいます)。別のモードでは、VNC、RDP、 SSH などのインバンド アクセス方式を使用します。

さらに PC クライアントとノード間通信では、次のいずれかの特性があります。

- PC クライアントが、Raritan デバイスまたはインバンド アクセス によってノードに直接接続されるかどうか。これはダイレクト モー ドと呼ばれます。
- PC クライアントは、アプリケーション ファイアウォールとして機能する CC-SG によってノードに接続されるかどうか。これはプロキシ モードと呼ばれます。

通信方向	ポート番号	プロトコル	設定可否	詳細
クライアント → CC-SG (プロキシ → ノード経由)	2400 (CC-SG 上)	ТСР	不可	クライアント - サーバ通 信。 暗号化されません。



通信方向	ポート番号	プロトコル	設定可否	詳細
クライアント → Raritan デバイス→ア ウト オブ バンド KVM ノード (ダイレクト モード)	5000 (Raritan デバイ ス上)	TCP	Π	クライアント - サーバ通 信。 設定されている場合は SSL/AES-128/AES-256 暗 号化。
クライアント → Raritan Dominion SX デバイス → アウト オ ブ バンド シリアル ノ ード (ダイレクト モード)	51000 (Raritan デバイ ス上)	TCP	Π	クライアント - サーバ通 信。 設定されている場合は SSL/AES-128/AES-256 暗 号化。

CC-SG と IPMI、iLO/RILOE、DRAC、RSA のクライアント

CC-SG で iLO/RILOE サーバや iLO2/RILOE2 サーバなどのサード パ ーティ デバイスを管理するには、追加のポートを開かなければならな い場合があります。iLO/RILOE デバイスのターゲットの電源は、直接オ ン、オフ、リセットされます。IPMI (Intelligent Platform Management Interface) サーバも、CC-SG で制御できます。さらに Dell DRAC およ び RSA ターゲットも CC-SG で管理できます。

注: 一部のイン バンド インタフェースでは、追加のポートを開く必要 があります。詳細は、それぞれのガイドを参照してください。

通信方向	ポート番号	プロトコル	設定可否	詳細
$CC\text{-}SG\toIPMI$	623	TCP	不可	IPMI 標準
CC-SG → iLO/RILOE (HTTP ポート使用)	80 または 443	TCP	不可	ベンダ標準
$\text{CC-SG} \rightarrow \text{DRAC}$	80 または 443	ТСР	不可	ベンダ標準
$CC\text{-}SG\toRSA$	80 または 443	TCP	不可	ベンダ標準

CC-SG と SNMP

SNMP (Simple Network Management Protocol (簡易ネットワーク管理プ ロトコル)) を使うと、CC-SG は SNMP トラップ (イベント通知) をネ ットワーク上の既存の SNMP マネージャに送り出すことができます。 CC-SG は、HP OpenView などサードパーティのエンタープライズ管 理ソリューションによる SNMP GET/SET の操作もサポートします。



通信方向	ポート番号	プロトコル	設定可否	詳細
SNMP マネージャ → CC-SG	161	UDP	пj	SNMP 標準
CC-SG → SNMP マネ ージャ	162	UDP	п]	SNMP 標準

CC-SG 内部ポート

CC-SG はいくつかのポートを内部機能に使用し、そのローカル ファイ アウォール機能でそれらのポートへのアクセスがブロックされます。た だし、外部スキャナの一部はこれを「ブロック状態」または「フィルタ 状態」として検出する場合があります。こうしたポートへの外部アクセ スは必要ないため、ブロックすることができます。現在使用中のポート は次のとおりです。

- 1088
- 1098
- 2222
- 4444
- 4445
- 8009
- 8083
- 8093

これらのポートに加えて、CC-SG は、32xxx 以上の範囲にある TCP ポートと UDP ポートのペアを使用する場合があります。こうしたポー トへの外部アクセスは必要ないため、ブロックすることができます。



NAT 対応ファイアウォール経由の CC-SG アクセス

ファイアウォールで NAT (Network Address Translation) が PAT (Port Address Translation) とともに使用されている場合、このファイアウォ ールが使用されるすべての接続にプロキシ モードを使用してください 。さらに、ポート 80 (非 SSL) または 443 (SSL)、8080、および 2400 への外部接続にはファイアウォールを設定して CC-SG に転送する必要 があります (PC クライアントがこれらのポートでセッションを開始す るため)。

注: ファイアウォールを介して非 SSL トラフィックを実行することは お勧めできません。

ファイアウォールが使用される接続では、プロキシ モードを使用する ように設定する必要があります。「*接続モード: ダイレクトおよびプロキ* シ『280p.』」を参照してください。CC-SG は、さまざまなターゲッ トに接続して、PC クライアント リクエストを代行します。ただし、 CC-SG は、ファイアウォールを経由した PC クライアントからターゲ ットへの TCP/IP 接続を終了します。

ノードへの RDP アクセス

ノードへの RDP アクセスの場合、ポート 3389 を開く必要があります。

ノードへの VNC アクセス

ノードへの VNC アクセスの場合、ポート 5800 または 5900 を開く 必要があります。

ノードへの SSH アクセス

ノードへの SSH アクセスの場合、ポート 22 を開く必要があります。

リモート システム監視ポート

リモート システム監視機能が有効になっている場合、デフォルトでポ ート 19150 が開きます。「*リモート システム監視の設定* 『364p. 』」 を参照してください。



ユーザ グループ権限

この表には、CC-SG メニュー項目にアクセスするためにユーザに割り 当てる必要がある権限が示されています。

*特定の権限が必要ないことを意味します。CC-SG にアクセスできれば、どのユーザでもこれらのメニューおよびコマンドを表示したり、使用したりできます。

メニュー > サ ブメニュー	メニュー項目	必要な権限	説明
Secure Gateway	このメニューはす	べてのユーザが使用できます。	
	プロファイル	なし*	
	今日のメッセー ジ	なし*	
	印刷	なし*	
	画面印刷	なし*	
	ログアウト	なし*	
	終了	なし*	
ユーザ	このメニューおよう が使用できます。	びユーザ ツリーは、ユーザ管理	権限を持つユーザのみ
> ユーザ マネ ージャ	> ユーザの追加	ユーザ管理	
	(ユーザの編集)	ユーザ管理	ユーザ プロファイル を使用
	> ユーザの削除	ユーザ管理	
	> ユーザをグル ープから削除	ユーザ管理	
	> ユーザのログ アウト	ユーザ管理	
	> 一括コピー	ユーザ管理	
> ユーザ グル ープ マネージャ	> ユーザ グルー プの追加	ユーザ管理	
	(ユーザ グループ の編集)	ユーザ管理	ユーザ グループ プロ ファイルを使用
	> ユーザ グルー	ユーザ管理	



Ap C

メニュー > サ ブメニュー	メニュー項目	必要な権限	説明
	プの削除		
	> ユーザをグル ープに割り当て	ユーザ管理	
	> ユーザのログ アウト	ユーザ管理	
	ノード監査	ユーザ管理	
デバイス	このメニューおよ ザのみが使用でき	びデバイス ツリーは、次のいず ます。	れかの権限を持つユー
	デバイス、ポート、	、およびノードの管理	
	デバイスの設定お	よびアップグレードの管理	
	デバイスの検出	デバイス、ポート、およびノ ードの管理	
> デバイス マ ネージャ	> デバイスの追 加	デバイス、ポート、およびノ ードの管理	
	(デバイスの編集)	デバイス、ポート、およびノ ードの管理	デバイス プロファイ ルを使用
	> デバイスの削 除	デバイス、ポート、およびノ ードの管理	
	> 一括コピー	デバイス、ポート、およびノ ードの管理	
	> デバイスのア ップグレード	デバイスの設定およびアップ グレードの管理	
設定	>> バックアップ	デバイスの設定およびアップ グレードの管理	
	>> リストア	デバイスの設定およびアップ グレードの管理	
	>> 設定のコピー	デバイスの設定およびアップ グレードの管理	
	> デバイスの再 起動	デバイス、ポート、およびノ ードの管理/デバイスの設定お よびアップグレードの管理	
	> デバイスの ping	デバイス、ポート、およびノ ードの管理/デバイスの設定お よびアップグレードの管理	



メニュー > サ ブメニュー	メニュー項目	必要な権限	説明
	> 管理の一時停 止	デバイス、ポート、およびノ ードの管理/デバイスの設定お よびアップグレードの管理	
	> デバイス パワ ー マネージャ	デバイス、ポート、およびノ ードの管理、およびノード パ ワー制御	
	> 管理の起動	デバイス、ポート、およびノ ードの管理/デバイスの設定お よびアップグレードの管理	
	> ユーザ ステー ション管理の起 動	デバイス、ポート、およびノ ードの管理	
	> ユーザの切断	デバイス、ポート、およびノ ードの管理/デバイスの設定お よびアップグレードの管理	
	> トポロジー表 示	デバイス、ポート、およびノ ードの管理	
> 表示の変更	> カスタム表示 の作成	デバイス、ポート、およびノ ードの管理/デバイスの設定お よびアップグレードの管理	
	> ツリー表示	デバイス、ポート、およびノ ードの管理/デバイスの設定お よびアップグレードの管理	
> ポート マネ ージャー	> 接続	デバイス、ポート、およびノ ードの管理、およびノードの アウト オブ バンド アクセス	
	> ポートの設定	デバイス、ポート、およびノ ードの管理	
	> ポートの切断	デバイス、ポート、およびノ ードの管理	
	> ポートの削除	デバイス、ポート、およびノ ードの管理	
	> ポート パワー マネージャ	デバイス、ポート、およびノ ードの管理、およびノード パ ワー制御	



メニュー > サ ブメニュー	メニュー項目	必要な権限	説明
	> 電源タップの 追加	デバイス、ポート、およびノ ードの管理	
> ポート並び替 えオプション	> ポート名でソ ート	デバイス、ポート、およびノ ードの管理/デバイスの設定お よびアップグレードの管理	
	> ポート ステー タスでソート	デバイス、ポート、およびノ ードの管理/デバイスの設定お よびアップグレードの管理	
	> ポート番号で ソート	デバイス、ポート、およびノ ードの管理/デバイスの設定お よびアップグレードの管理	
ノード	このメニューおよ のみが使用できま	びノード ツリーは、次のいずれ す。	かの権限を持つユーザ
	デバイス、ポート、	、およびノードの管理	
	ノードのイン バン	/ド アクセス	
	ノードのアウト オ	ーブ バンド アクセス	
	ノードのパワー制	御	
	ノードの追加	デバイス、ポート、およびノ ードの管理	
	(ノードの編集)	デバイス、ポート、およびノ ードの管理	ノード プロファイル を使用
	ノードの削除	デバイス、ポート、およびノ ードの管理	
	<インタフェース 名>	ノードのイン バンド アクセ ス/	
		ノードのアウト オブ バンド アクセス	
	切断	次のいずれか:	
		ノードのイン バンド アクセ ス/	
		ノードのアウト オブ バンド アクセス/	
		デバイス、ポート、およびノ ードの管理/	
		デバイスの設定およびアップ	



メニュー > サ ブメニュー	メニュー項目	必要な権限	説明
		グレードの管理	
	仮想化	デバイス、ポート、およびノ ードの管理	
	一括コピー	デバイス、ポート、およびノ ードの管理	
	パワー制御	パワー制御	
	サービス アカウ ント	デバイス、ポート、およびノ ードの管理	
	サービス アカウ ントの割り当て	デバイス、ポート、およびノ ードの管理	
	グループ パワー 制御	パワー制御	
	ブレードの設定	デバイス、ポート、およびノ ードの管理	
	ノードに Ping を 実行	デバイス、ポート、およびノ ードの管理	
	ノード インタフ ェースをブック マークに設定	ノードのイン バンド アクセ ス/ノードの アウト オブ バンド アクセス	
> ノード並べ替 えオプション	> ノード名でソ ート	次のいずれか: デバイス、ポート、およびノ ードの管理/ ノードのイン バンド アクセ ス/ ノードのアウト オブ バンド アクセス/ パワー制御	
	> ノード ステー タスでソート	次のいずれか: デバイス、ポート、およびノ ードの管理/ ノードのイン バンド アクセ ス/ ノードのアウト オブ バンド アクセス/	



メニュー > サ ブメニュー	メニュー項目	必要な権限	説明
		ノードのパワー制御	
> チャット	> チャット セッ ションの開始	ノードのイン バンド アクセ ス/	
		ノートのアリト オノ ハント アクセス/ ノードのパワー制御	
	> チャット セッ ションの表示	ノードのイン バンド アクセ ス/	
		ノードのアウト オブ バンド アクセス/	
		ノードのパワー制御	
	> チャット セッ ションの終了	ノードのイン バンド アクセ ス/	
		ノードのアウト オブ バンド アクセス/	
		ノードのパワー制御	
> 表示の変更	> カスタム表示	次のいずれか:	
	の作成	デバイス、ポート、およびノ ードの管理/	
		ノードのイン バンド アクセ ス/	
		ノードのアウト オブ バンド アクセス/	
		ノードのパワー制御	
	> ツリー表示	次のいずれか:	
		デバイス、ポート、およびノ ードの管理/	
		ノードのイン バンド アクセ ス/	
		ノードのアウト オブ バンド アクセス/	
		ノードのパワー制御	
関連	このメニューは、 用できます。	ユーザ セキュリティ管理の権限	を持つユーザのみが使
	> 関連	ユーザ セキュリティ管理	追加、変更、削除の権



メニュー > サ ブメニュー	メニュー項目	必要な権限	説明
			限を含みます。
	> デバイス グル ープ	ユーザ セキュリティ管理	追加、変更、削除の権 限を含みます。
	> ノード グルー プ	ユーザ セキュリティ管理	追加、変更、削除の権 限を含みます。
	> ポリシー	ユーザ セキュリティ管理	追加、変更、削除の権 限を含みます。
レポート	このメニューは、、 ユーザ セキュリテ	ユーザ管理権限を持つユーザが使 ィ管理の権限のみを持つユーザ	を用できます。ただし、 は除きます。
	監查証跡	CC の設定と制御	
	エラー ログ	CC の設定と制御	
	アクセス レポー ト	デバイス、ポート、およびノ ードの管理	
	可用性レポート	デバイス、ポート、およびノ ードの管理/デバイスの設定お よびアップグレードの管理	
> ユーザ	> アクティブ ユ ーザ	ユーザ管理	
	> ロックアウト ユーザ	CC の設定と制御	
	>全ユーザ デー タ	全ユーザのデータを表示する 場合: ユーザ管理 自身のユーザ データを表示す ろ場合: [な]」	
	> ユーザ グルー プ データ	ユーザ管理	
> デバイス	>デバイス資産レ ポート	デバイス、ポート、およびノ ードの管理/デバイスの設定お よびアップグレードの管理	
	> デバイス グル ープ データ	デバイス、ポート、およびノ ードの管理	
	> ポートの照会	デバイス、ポート、およびノ ードの管理	



メニュー > サ ブメニュー	メニュー項目	必要な権限	説明
> ノード	> ノード資産レ ポート	デバイス、ポート、およびノ ードの管理	
	> アクティブ ノ ード	デバイス、ポート、およびノ ードの管理	
	> ノードの作成	デバイス、ポート、およびノ ードの管理	
	> ノード グルー プ データ	デバイス、ポート、およびノ ードの管理	
> Active Directory	AD ユーザ グル ープ レポート	CC の設定と制御/ユーザ管理	
	スケジュールさ れたレポート	CC の設定と制御/ デバイスの設定およびアップ グレードの管理	
アクセス			
	Web サービス API の追加	CC の設定と制御	
管理	このメニューは、	次のいずれかの権限を持つユーサ	ドのみが使用できます。
	CC の設定と制御		
	デバイス、ポート、 ティ管理の組み合:	、およびノードの管理、ユーザ管 わせ	管理、ユーザ セキュリ
	ガイド付き設定	次のすべて:	
		デバイス、ポート、およびノー 、ユーザ セキュリティ管理	ドの管理、ユーザ管理
	今日のメッセー ジの設定	CC の設定と制御	
	アプリケーショ ン	CC の設定と制御	
	ファームウェア	CC の設定と制御/ デバイスの設定およびアップ グレードの管理	
	設定	CC の設定と制御	
	クラスタ設定	CC の設定と制御	



メニュー > サ ブメニュー	メニュー項目	必要な権限	説明
	隣接システム	CC の設定と制御	
	セキュリティ	CC の設定と制御	
	通知	CC の設定と制御	
	タスク	CC の設定と制御	
	互換表	デバイス、ポート、およびノ ードの管理/デバイスの設定お よびアップグレードの管理	
> インポート	カテゴリのイン ポート	CC の設定と制御、 ユーザ セキュリティ管理	
	ユーザのインポ ート	CC の設定と制御、 ユーザ管理	
	ノードのインポ ート	CC の設定と制御、 デバイス、ポート、およびノ ードの管理	
	デバイスのイン ポート	CC の設定と制御、 デバイス、ポート、およびノ ードの管理	
	Import Powerstrips (電源 タップのインポ ート)	CC の設定と制御、 デバイス、ポート、およびノ ードの管理	
> エクスポート	カテゴリのエク スポート	CC の設定と制御、 ユーザ セキュリティ管理	
	ユーザのエクス ポート	CC の設定と制御、 ユーザ管理	
	ノードのエクス ポート	CC の設定と制御、 デバイス、ポート、およびノ ードの管理	
	デバイスのエク スポート	CC の設定と制御、 デバイス、ポート、およびノ ードの管理	



メニュー > サ ブメニュー	メニュー項目	必要な権限	説明
	パワー IQ デー タのエクスポー ト	CC の設定と制御、 デバイス、ポート、およびノ ードの管理	
システム メンテ ナンス			
	バックアップ	CC の設定と制御	
	リストア	CC の設定と制御	
	リセット	CC の設定と制御	
	再起動	CC の設定と制御	
	アップグレード	CC の設定と制御	
	シャットダウン	CC の設定と制御	
> メンテナン ス モード	> メンテナンス モードの起動	CC の設定と制御	
	> メンテナンス モードの終了	CC の設定と制御	
表示		なし*	
ウィンドウ		なし*	
ヘルプ		なし*	



Ap D SNMP トラップ

CC-SG には次の SNMP トラップがあります。

SNMP トラップ	説明
ccUnavailable	CC-SG アプリケーションが使用不能です。
ccAvailable	CC-SG アプリケーションが利用可能です。
ccUserLogin	CC-SG ユーザがログインしています。
ccUserLogout	CC-SG ユーザがログアウトしています。
ccPortConnectionStarted	CC-SG セッションが開始しました。
ccPortConnectionStopped	CC-SG セッションが停止しました。
ccPortConnectionTerminated	CC-SG セッションが終了しました。
ccImageUpgradeStarted	CC-SG イメージ アップグレードが開始しました。
ccImageUpgradeResults	CC-SG イメージ アップグレード結果。
ccUserAdded	新しいユーザが CC-SG に追加されました。
ccUserDeleted	ユーザが CC-SG から削除されました。
ccUserModified	CC-SG ユーザが変更されました。
ccUserAuthenticationFailure	CC-SG ユーザの認証に失敗しました。
ccLanCardFailure	CC-SG が LAN カード エラーを検出しました 。
ccHardDiskFailure	CC-SG がハード ディスク エラーを検出しま した。
ccLeafNodeUnavailable	CC-SG がリーフ ノードへの接続失敗を検出しました。
ccLeafNodeAvailable	CC-SG がアクセス可能なリーフ ノードを検出 しました。
ccIncompatibleDeviceFirmware	CC-SG がファームウェアに互換性のないデバ イスを検出しました。
ccDeviceUpgrade	CC-SG がデバイスのファームウェアをアップ グレードしました。
ccEnterMaintenanceMode	CC-SG がメンテナンス モードになりました。
ccExitMaintenanceMode	CC-SG のメンテナンス モードが終了ました。



SNMP トラップ	説明
ccUserLockedOut	CC-SG ユーザはロックアウトされています。
ccDeviceAddedAfterCCNOCNotificati on	CC-SG が CC-NOC から通知の受信後にデバ イスを追加しました。
ccScheduledTaskExecutionFailure	予定タスクの実行が失敗した理由。
ccDiagnosticConsoleLogin	ユーザが CC-SG 診断コンソールにログインし ました。
ccDiagnosticConsoleLogout	ユーザが CC-SG 診断コンソールからログアウ トしました。
ccUserGroupAdded	新しいユーザ グループが CC-SG に追加され ました。
ccUserGroupDeleted	CC-SG ユーザ グループが削除されました。
ccUserGroupModified	CC-SG ユーザ グループが変更されました。
ccSuperuserNameChanged	CC-SG スーパーユーザのユーザ名が変更されました。
ccSuperuserPasswordChanged	CC-SG スーパーユーザのパスワードが変更さ れました。
ccLoginBannerChanged	CC-SG ログイン バナーが変更されました。
ccMOTDChanged	CC-SG 今日のメッセージ (MOTD) が変更され ました。
ccDominionPXReplaced	Dominion PX デバイスが別の Dominion PX デ バイスと交換されました。
ccSystemMonitorNotification	CC-SG がメモリ不足です。
ccNeighborhoodActivated	CC-SG 隣接システムが有効になりました。
ccNeighborhoodUpdated	CC-SG 隣接システムが更新されました。
ccDominionPXFirmwareChanged	Dominion PX のファームウェア バージョンが 変更されました。
ccClusterFailover	プライマリ CC-SG ノードが失敗したので、現 在はバックアップ CC-SG ノードが新しいプラ イマリ CC-SG ノードとして機能しています。
ccClusterBackupFailed	バックアップ CC-SG ノードが失敗しました。
ccClusterWaitingPeerDetected	プライマリ CC-SG ノードが待機モードのピア を検出しました。
ccClusterOperation	クラスタ操作が実行されました。



Ap D: SNMP トラップ

SNMP トラップ	説明
ccCSVFileTransferred	CSV ファイルがインポートされました。
ccPIQAvailable	CC-SG が、 Power IQ が利用可能であることを 検出しました。
ccPIQUnavailable	CC-SG が、 Power IQ が利用不能であることを 検出しました。



Ap E CSV ファイルのインポート

このセクションでは、CSV ファイルのインポートの詳細について説明 します。

この章の内容

CSV ファイルの共通要件	412
インポートに関する監査証跡エントリ	413
CSV ファイルの問題のトラブルシューティング	414



CSV ファイルの共通要件

CSV ファイルを作成するには、CC-SG からファイルをエクスポートし、そのファイルを例として参照しながら独自のファイルを作成することをお勧めします。エクスポート ファイルの一番上には、ファイル内の 各アイテムを説明するコメントが含まれています。コメントは、インポ ートするファイルを作成するための指示として使用できます。

インポート ファイルを Microsoft Excel などのスプレッドシート プロ グラムで作成することをお勧めします。そのセルに各アイテムを入力し ます。ファイルを保存するときに、ファイルの種類として CSV を選択 します。これにより、各セルの最後にカンマ区切りが自動的に追加され 、データがカンマで区切られた列に整理されます。CSV ファイルはテ キスト エディタで作成できますが、その場合は各アイテムの後に手動 でカンマを追加する必要があります。

ファイルを初めて Excel で保存するときに、[名前を付けて保存] を 選択し、ファイルの種類として [CSV] を選択する必要があります。 それ以降は、ファイルは CSV として保存されます。 ファイルの種類を正しく設定しないと、ファイルは破損し、インポートに使用できません。

- すべてのインポート ファイルは ASCII テキストのみにする必要が あります。
- 各行の最初の列には、コマンド ADD を含める必要があります。基本構造は、コマンド、タグ、属性です。ここでは、ADD はコマンドです。
- 列名はサポートされていません。データ行の上にコメント行を追加 できます。コメント行は # 記号で始めます。
- フィールドにデフォルト値を使用するには、値を入力するか、フィールドを空白のままにします。
- 名前の長さに関する CC-SG のルールについての詳細は、「命名規 則 『435p. 』」を参照してください。
- CSV ファイルをスプレッドシート プログラムではなくテキスト エディタで作成する場合は、カンマおよび二重引用符の使用方法が、スプレッドシート プログラムでの場合と異なります。カンマまたは二重引用符を含む値は、全体を二重引用符で囲む必要があります。 値の中に二重引用符がある場合は、その前に別の二重引用符を付ける必要があります。

たとえば、



Ap E: CSV ファイルのインポート

特殊文字を含む値	CSV ファイルでの形式
DeviceA,B	"DeviceA,B"
Device"A"	"Device""A"""

インポートに関する監査証跡エントリ

CC-SG にインポートされた各アイテムは、監査証跡に記録されます。 スキップされた重複アイテムは、監査証跡に記録されません。

監査証跡では、メッセージ タイプ [設定] の下に以下のアクションのエ ントリが記録されます。

- CSV ファイルのインポートの開始
- CSV ファイルのインポートの完了。正常に追加されたレコードの数、 追加に失敗したレコードの数、無視された重複レコードの数など が含まれます。

監査証跡には、レコードのインポート時に行われた各変更に関するエン トリが含まれています。これらのエントリは、インポートの開始のエン トリとインポートの完了のエントリの間に記録されます。エントリは、 実行したインポートのタイプに応じて、異なるメッセージ タイプの下 に記録されます。

- ユーザのインポートは、[ユーザ メンテナンス]の下に記録されます。
- デバイスのインポートは、[デバイス/ノード/ポート]の下に記録されます。
- ノードのインポートは、[デバイス/ノード/ポート]の下に記録されます。
- カテゴリのインポートは、[設定]の下に記録されます。
- 電源タップのインポートは、[デバイス/ノード/ポート]の下に記録されます。

目的のインポートに関連するすべてのエントリを見つけるには、[Audit Report (監査レポート)] ページの日付フィールドと時刻フィールドによ るフィルタを使用します。

レコードがインポートされるたびに、複数のエントリが監査証跡に記録 されることがあります。



CSV ファイルの問題のトラブルシューティング

CSV ファイルの検証のトラブルシューティングを行うには、以下の 手順に従います。

[インポート] ページの [問題] 領域にエラー メッセージが表示されます 。エラー メッセージには、検証中に CSV ファイルで見つかった問題 が示されています。

エラーのリストを CSV ファイルに保存できます。

各エラーには、エラーが見つかった CSV ファイル内の行番号が含まれています。

エクスポート ファイルの一番上にあるコメントがエラーの修正に役立 ちます。ファイルを修正したら、再度検証します。

CSV ファイルのインポートのトラブルシューティングを行うには、 以下の手順に従います。

[インポート] ページの [問題] 領域に、インポート中に見つかった問題 を知らせる警告およびエラー メッセージが表示されます。

エラーが見つかった場合、ファイルのその行内の情報はインポートされ ていません。

重複エントリはインポートされず、監査証跡にも記録されません。


Ap F トラブルシューティング

- Web ブラウザから CC-SG を起動するには、Java プラグインが必要です。お使いのマシンに必要なバージョンがインストールされていない場合、CC-SG によりインストール手順のガイドが表示されます。お使いのマシンに Java プラグインがインストールされていない場合、CC-SG は自動的に起動できません。この場合は、古いJava バージョンをアンインストールするか無効にしてから、CC-SG にシリアル ポート接続を設定して正しく機能するようにします。
- CC-SG アプレットがロードされない場合は、Web ブラウザ設定を 調べてください。
 - Internet Explorer で Java (Sun) が有効になっていることを確認 します。
 - コントロール パネルで Java プラグインを開き、ブラウザの設 定を調整します。
- デバイスの追加に問題がある場合は、デバイスのファームウェアの バージョンが適正かどうかを確認します。
- デバイスと CC-SG の間のネットワーク インタフェース ケーブル が切断されている場合、ハートビートに設定されている時間 (分) だけ待ってから、もう一度ネットワーク インタフェース ケーブル を接続します。設定されたハートビート期間中、デバイスはスタン ドアロン モードで動作し、RRC、MPC、または RC からアクセス できます。
- クライアントのバージョンがサーバのバージョンと異なっており、 予測できない動作が発生する可能性があるなどのエラー メッセージ が表示される場合は、ブラウザのキャッシュと Java キャッシュを クリアして、ブラウザを再起動してください。「ブラウザ キャッシュ ュのクリア『258p.』」および「CJava キャッシュのクリア『258p. の"Java キャッシュのクリア"参照』」を参照してください。
- Internet Explorer の使用中に MPC インタフェースを介した KX2 ポートへのアクセスで問題が発生する場合は、ブラウザのキャッシ ュをクリアして、ポートに再アクセスする必要があります。「ブラウ ザ キャッシュのクリア 『258p. 』」を参照してください。
- メモリの使用率が劇的に増加するか、ブラウザ セッションがアクションに対する応答を中止した場合は、クライアントの Java ヒープサイズを増やす必要がある可能性があります。
 - a. コントロール パネルで Java プラグインを開きます。
 - b. [Java] タブをクリックします。
 - c. [Java アプレットのランタイム設定] グループ ボックス内の [表示] をクリックします。



d. 実行している現在の Java バージョンの行を選択し、[Java ラ ンタイム パラメータ]列に「-xmx<size>m」と入力します。た とえば、Java ヒープ サイズを最大の 300 MB に増やす場合は 、「-xmx300m」と入力します。

Java ヒープ サイズをクライアント コンピュータのメモリの半分よ り多い値に設定することはお勧めできません。たとえば、クライア ント コンピュータに 1.0 GB の RAM が搭載されている場合は、 パラメータを -Xmx512m 以下に設定します。

- 同じクライアントと Firefox を使用して複数の CC-SG ユニットに アクセスすると、証明書が無効であることを知らせる「Secure Connection Failed (セキュアな接続に失敗しました)」というメッセー ジが表示されることがあります。ブラウザから無効な証明書を削除 すると、アクセスを再開できます。
 - a. Firefox で [ツール] > [オプション] を選択します。
 - b. [詳細] をクリックします。
 - c. [暗号化] タブをクリックします。
 - d. [証明書を表示] をクリックし、リストで「Raritan」を検索します。
 - e. [CommandCenter] を選択し、[削除] をクリックします。[OK] をクリックして確認します。



診断ユーティリティ

CC-SG には、いくつかの診断ユーティリティが付属しています。これ らは、ユーザまたはラリタン社のテクニカル サポートが **CC-SG** での 問題の原因の分析とデバッグを行う際に非常に役に立つ場合があります

この章の内容

0

メモリ診断	417
デバッグ モード	418
CC-SG ディスク監視	419

メモリ診断

Ap G

CC-SG には、Memtest86+ 診断プログラムが付属しています。これは GRUB メニューから呼び出すことができます。メモリの問題が発生した 場合は、Memtest86+ 診断テストを実行してトラブルシューティングで きます。

- ▶ 1: Memtest86+ 診断プログラムを実行する場合の手順:
- 1. CC-SG をリブートします。「*診断コンソールを使用した CC-SG の リブート* **『354**p. **』**」を参照してください。
- 以下のメッセージが表示されたら、5 秒以内に Esc または矢印キ ーなどのいずれかの文字キーを押して、GRUB メニューに入ります。

```
Press any key to enter the menu
```

Booting CentOS (x.x.x) in x seconds....

- 3. 上下の矢印キーを使用して [Memtest86+ vX.X] オプション (vX.X は現在のバージョン) をハイライトし、Enter キーを押します。
- CC-SG は Memtest86+ 診断プログラムをロードして実行します。 プログラムを少なくとも 1 回最後まで実行します。これで、[Pass] 列に "1" と表示されます。詳細なテストを実行するには、プログラ ムを数時間または一晩中実行したままにします。
- 5. 以下の項目を確認して、メモリ エラーがあるかどうかを判断します
 - [Memory]: 総メモリ容量は、CC-SG のタイプと合致している必要があります (G1 の場合は 512M、V1 の場合は 2048M、E1 の場合は 4096M)。
 - [Errors]: 列には "0" が表示されている必要があります。



エラー表示領域: これは、[WallTime] 行のすぐ下の領域です。この領域に何も表示されない場合は、エラーがないことを示します。

上の項目のいずれかによってメモリ エラーがあることが示されてい る場合は、以下を実行できます。

- メモリ エラーが表示された Memtest86+ 画面を取得して、ラ リタン社のテクニカル サポートに連絡します。
- CC-SG をシャットダウンし、メモリ DIMM モジュールを取り 付け直して、しっかり接続されていることを確認します。次に 、Memtest86+ 診断を実行して、メモリの問題が解決されてい るかどうかを確認します。
- 2: Memtest86+ 診断プログラムを終了する場合の手順:
- 1. Esc キーを押します。
- 2. CC-SG がリセットされ、リブートされます。

デバッグ モード

デバッグ モードを有効にすると、トラブルシューティングに大いに役 立ちますが、CC-SG の処理とパフォーマンスに影響を与える可能性が あります。このため、デバッグ モードはラリタン社のテクニカル サポ ートから指示された場合のみ有効にしてください。トラブルシューティ ングが終わったら、デバッグ モードを無効にする必要があります。

- 1: デバッグ モードを有効にする場合の手順:
- サポートされているインターネット ブラウザを使用して URL を「 http(s): //<IP_address>: 8080/jmx-console/」と入力し ます。<IP_address> は、CC-SG の IP アドレスです。たとえば 、「https: //10.20.3.30: 8080/jmx-console/」のように入 力します。
- 2. [Username] フィールドに「admin」と入力します。
- 3. [Password] フィールドにスーパーユーザのパスワードを入力します。
- [com.raritan.cc.bl.logger] が表示されるまでスクロール ダ ウンします。
- 5. ハイパーリンク [service=LoggerService] をクリックします。 画面にデバッグ オプションのリストが表示されます。
- 6. ラリタン社のテクニカル サポートから指示されたデバッグ オプションの値を、INFO から DEBUG に変更します。
- 7. ウィンドウの下部の [Apply Changes] をクリックします。
- 8. 問題を再現し、スナップショットを取得します。「システム スナッ プショットの取得 『375p. 』」を参照してください。



- 2: デバッグ モードを無効にする場合の手順:
- 1. 前のセクションの最初の 4 つの手順に従って、デバッグ オプショ ンのウィンドウを開きます。
- 2. デバッグ オプションの値を、DEBUG から INFO に変更します。
- 3. ウィンドウの下部の [Apply Changes] をクリックします。

CC-SG ディスク監視

1 つ以上のファイル システムで CC-SG ディスク領域を使い果たした 場合は、操作に悪影響を及ぼし、エンジニアリング データの一部が失 われる可能性があります。このため、CC-SG ディスクの使用率を監視 し、問題の防止と解決のために適切な対応を取る必要があります。ディ スク監視は、診断コンソールまたは Web ブラウザ経由で実行できます 。熟練したユーザであれば、gkrellm によるリモート監視を使用できま す。「**リモート システム監視の設定 『364**p. **』**」を参照してください

重要: クラスタ設定の CC-SG ユニットの場合は、両方の CC-SG ユニ ットを監視する必要があります。

- 診断コンソールでディスク領域を監視するには、以下の手順に従います。
- 診断コンソールにログインし、[Disk Status] 画面を呼び出します。
 「RAID ステータスとディスク使用率の表示 『366p. 』」を参照してください。
- 2. ディスク関連の情報を確認し、必要に応じて対応します。
 - 両方の RAID パーティションに、[U_] または [_U] ではなく
 [UU] と表示されている必要があります。それ以外の場合はディ スク エラーを意味するので、ラリタン社のテクニカル サポー トにご連絡ください。



 ファイル システムの [Use%] の値 (画面の 5 列目) がいずれ も 50% を超えないようにする必要があります。異なるファイ ル システムには、異なるデータが含まれているので、対応策も 異なります。

md0 : Network Interf	aces	onrig	>>				
Admin			>>				
Utilities			>>	Remot	te j		
mdl : L				Disk	4	RAID Status + Di	sk Utilization
/2501248 blocks	[2/2]	[00]		NTP 5	015 Sta	Manual Disk / R/ Schedule Disk Te	AID Tests ests
Filesystem	Size	Used	Avail	Syste	em –	Repair / Rebuild	I RAID
/dev/mapper/svg-root	4.8G	306M	4.36				
/dev/mapper/svg-sg	2.9G	344M	2.46	13%	/ 50	9	
/dev/mapper/svg-DB	8.6G	217M	7.96	3%	/ 50	g/DB	
/dev/mapper/svg-opt	5.7G	495M	5.0G	- 9%	/op	ot	
/dev/mapper/svg-usr	2.06	976M	877M	53%	/us	50	
/dev/mapper/svg-tmp	2.06	36M	1.86	2%	/tr	np 🛛	
/dev/mapper/svg-var	7.6G	211M	7.06	3%	148	ar	
/dev/md0	99M	12M	82M	13%	/bc	oot	
tmpfs	2.06	Θ	2.06	0%	/de	ev/shm	< Refresh a
SN:ACD7900052, Ver:4	.1.0.5	.2 (Up	odated: <ctl+c:< td=""><td>Tue (</td><td>)ec Ieni</td><td>2008-12-02 17:44 us (Top-bar): <0</td><td>1:21 EST -0500]</td></ctl+c:<>	Tue ()ec Ieni	2008-12-02 17:44 us (Top-bar): <0	1:21 EST -0500]

ファイル シ ステム	データ	対応策
/sg/DB	CC-SG データベース	ラリタン社のテクニカル サポートにご連絡ください。
/opt	CC-SG バックアップおよ びスナップショット	 新しいスナップショット ファイルをリモート クライ アント PC に保存します。取得方法については、「シ ステム スナップショットの取得 『375p. 』」を参照 してください。 [System Snapshot] メニューに入ります。「システム スナップショットの取得 『375p. 』」を参照してくだ さい。 [Pre-Clean-up SNAP] 領域を選択します。 [Pre-Clean-up UPLOAD] 領域を選択します。 [SNAP] を選択解除します。 [Package & Export] を選択解除します。 [Package & Export] を選択解除します。 ディスク領域の問題が解決しない場合は、Admin Client を使用して CC-SG に接続し、CC-SG バック アップをクライアント PC にアップロードした後、
		アップをクライアント PC にアップロードした後、 それらを CC-SG から削除します。



Ap G: 診断ユーティリティ

ファイル シ ステム	データ	対応策
/var	ログ ファイルおよびシス テム アップグレード	ラリタン社のテクニカル サポートにご連絡ください。
/tmp	スクラッチ領域 (スナップ ショットが使用)	 [System Snapshot] メニューに入ります。「システム スナップショットの取得『375p.』」を参照してくだ さい。 2 [SNAP] を選択解除します
		 [SINAF] を選択解除します。 [Package & Export] を選択解除します。 [Clean-up /tmp] を選択します。 [Submit] をクリック、または選択します。

▶ Web ブラウザでディスク領域を監視するには、以下の手順に従い ます。

この方法は、CC-SG リリース 4.0 またはそれ以降にのみ適用されます 。Web ブラウザを使用してディスク領域を監視するには、あらかじめ 診断コンソールで Web Status Console 関連のオプションを有効にし ておく必要があります。「Web ブラウザからの Status Console への アクセス 『334p.』」を参照してください。

- サポートされているインターネット ブラウザを使用して URL を「 http(s): //<IP_address>/status/」と入力します。
 <IP_address> は、CC-SG の IP アドレスです。/status の後の スラッシュ (/) は必須です。たとえば「https: //10.20.3.30/status/」のように入力します。
- 2. ステータス ページが開きます。このページには、Status Console と同じ情報が含まれます。
- **3.** ページ下部の [Evaluation] の下にある [CC-SG Monitors] をクリッ クします。
- 4. ディスク関連の情報を確認し、必要に応じて対応します。詳細については、前のセクションを参照してください。

注: このセクションで説明していないファイル システムの問題について 、または実施した対応策では問題を解決できない場合の対処については 、ラリタン社のテクニカル サポートにご連絡ください。



Ap H 2 ファクタ認証

関連の RSA Authentication Manager 経由で 2 ファクタ認証をサポー トする RSA RADIUS サーバをポイントするように、CC-SG を設定す ることができます。CC-SG は、RADIUS クライアントとして機能し、 ユーザ認証リクエストを RSA RADIUS サーバに送信します。この認証 リクエストには、ユーザ ID、固定パスワード、動的トークン コードが 含まれます。

この章の内容

2	ファクタ認証のサポート環境4	22
2	ファクタ認証の設定条件4	22
2	ファクタ認証の既知の問題4	23

2 ファクタ認証のサポート環境

次の 2 ファクタ認証コンポーネントが CC-SG で機能します。

- Windows Server 2003 上の RSA RADIUS Server 6.1
- Windows Server 2003 上の RSA Authentication Manager 6.1
- RSA Secure ID SID700 ハードウェア トークン

従来のバージョンの RSA 製品も CC-SG で機能しますが、検証はされ ていません。

2 ファクタ認証の設定条件

- 2 ファクタ認証を設定するには、以下のタスクを完了する必要がありま す。RSA マニュアルを参照してください。
- 1. トークンをインポートします。
- 2. CC-SG ユーザを作成して、そのユーザにトークンを割り当てます。
- 3. ユーザ パスワードを生成します。
- 4. RADIUS サーバ用のエージェント ホストを作成します。
- 5. CC-SG 用にエージェント ホスト (タイプ: 通信サーバ) を作成しま す。
- 6. RADIUS CC-SG クライアントを作成します。



2 ファクタ認証の既知の問題

チャレンジ パスワード/PIN を必要とする RSA RADIUS の「新規 PIN」モードは機能しません。この方法を用いるすべてのユーザには、固定 パスワードを割り当てる必要があります。



Ap I FAQ

この章の内容

一般的な FAQ	424
認証に関する FAQ	426
セキュリティに関する FAQ	427
アカウントに関する FAQ	429
パフォーマンスに関する FAQ	429
グループ化に関する FAQ	430
相互運用性に関する FAQ	431
承認に関する FAQ	431
使い心地に関する FAQ	431
ライセンス設定に関する FAQ	433

一般的な FAQ

質問	回答
一般	
CC-SG とは何ですか?	CC-SG は、通常はデータ センターに配置され、 Raritan IP 対応製品に接続される複数のサーバや ネットワーク機器を統合するためのネットワーク 管理デバイスです。
CC-SG はなぜ必要なのです か?	データ センターに配置するサーバやデバイスが増 えると、それらの管理の複雑さは指数関数的に増 大します。CC-SG を使用すると、システム管理者 や経営者は 1 台のデバイスからすべてのサーバ、 装置、ユーザにアクセスし、それらを管理するこ とができます。
CC-SG はどのラリタン製品 をサポートしていますか?	Raritan のサポート セクションの Web サイトで ファームウェアおよびマニュアルにある互換表を 参照してください。
CC-SG は、他の Raritan 製 品とどのように統合しますか ?	CC-SG は、優れた独自の検索と検出の技術を使用 し、既知のネットワーク アドレスから特定の Raritan デバイスを識別し、そのデバイスに接続し ます。CC-SG を接続し、設定すると、CC-SG に 接続されたデバイスが透過になり、操作と管理が 非常にシンプルになります。
CC-SG のステータスは、プ	いいえ。CC-SG ソフトウェアは専用のサーバ上に



Ap I: FAQ

質問	回答
ロキシの対象となるデバイス のステータスによって制限さ れますか?	あるので、CC-SG のプロキシの対象となるデバイ スの電源がオフでも、CC-SG にアクセスできます 。
CC-SG ソフトウェアの新し いバージョンがリリースされ た場合は、新バージョンにア ップグレードできますか?	はい。お近くの Raritan 正規販売店または直接 Raritan, Inc. にお問い合わせください。
CC-SG にはノード、 Dominion ユニット、 IP-Reach ユニットを合計で 何台接続できますか?	接続できるノードと、Dominion または IP-Reach ユニットの台数に特定の制限はありませんが、無 制限ではありません。ホスト サーバに搭載された プロセッサの性能やメモリの容量によって、実際 に接続できるノードの数が決まります。
CC-SG にコンソールまたは シリアル ポートを追加でき ない場合はどうすればよいで すか?	コンソールまたはシリアル デバイスが Dominion 製品の場合は、次の条件が満たされていることを 確認します。 - Dominion デバイスがアクティブ - Dominion デバイスはユーザ アカウントの最大 設定数に達していない
Raritan CC-SG ではどのバー ジョンの Java をサポートし ますか?	Raritan のサポート セクションの Web サイトで ファームウェアおよびマニュアルにある互換表を 参照してください。
管理者が CC-SG データベー スに新しいノードを追加して 割り当ててくれました。どう すればこのノードがノード ツリーに表示されますか?	ツリーを更新して新しく割り当てたノードを表示 するには、ツール バーの [更新] ショートカット ボタンをクリックします。ただし、更新すると CC-SG は現在のコンソール セッションをすべて 閉じます。
Windows デスクトップは今 後どのようにサポートされま すか?	ファイアウォールの外から CC-SG にアクセスす るには、ファイアウォール上で適切なポートを設 定する必要があります。次のポートは標準のポー トです。 80: Web ブラウザによる HTTP アクセス用 443: Web ブラウザによる HTTPS アクセス用 8080: CC-SG サーバ操作用 2400: プロキシ モード接続用 5001: IPR/DKSX/DKX/ P2-SC イベント通知用 2 つのクラスタ ノード間にファイアウォールがあ る場合は、クラスタが正常に動作するように次の ポートを開けてください。



Ap I: FAQ

質問	回答
	8732: クラスタ ノードのハートビート用 5432: クラスタ ノードの DB 複製用
大規模システムの場合の設計 上の指針は何ですか?制約や 前提条件はありますか?	Raritan ではサーバの拡張性を追求したデータ セ ンター モデルとネットワーク モデルという 2 つ のモデルを提供します。 データ センター モデルでは、Paragon を使用す ると 1 つのデータ センターで数千システムまで 拡張できます。これは、1 つの場所を拡張するた めの最も効果的で費用効率の高い方法です。 IP-Reach と IP ユーザ ステーション (UST-IP) を使用したネットワーク モデルもサポートします。 ネットワーク モデルでは、TCP/IP ネットワーク を使用して CC-SG 経由のアクセスを統合するの で、ユーザはアクセス デバイスの IP アドレスも トポロジーも知る必要はありません。便利なシン
ある KX2 ポートから別の KX2 ポートにブレード シャ ーシを移動した場合、CC-SG によってブレード シャーシ 設定が自動検出され更新され ますか?	ブレード シャーシを別の KX2 ポートまたはデバ イスに移動した場合に、CC-SG によって、ブレー ド シャーシ設定が自動検出および更新がされるこ とはありません。設定は失われるので、再度 CC-SG でブレード シャーシを設定する必要があ ります。
ブレード サーバ ノードと仮 想ホスト ノードが同じサー バを参照する場合、これらを どのようにマージすればいい ですか?	ブレード スロットを設定する前に、仮想化機能を 設定する必要があります。ブレード スロットを設 定する場合は、仮想ホスト ノードと同じ名前を入 力し、メッセージが表示されたら、このインタフ ェースを既存のノードに追加することを選択しま す。

認証に関する FAQ

質問	回答
認証	
CC-SG では、ユーザ アカ ウントをいくつ作成できま すか?	ライセンスの制限を確認してください。時々ログイン しようとすると、正しいユーザ名やパスワードを入力 しているにも関わらず、「ログイン情報が正しくない



質問	回答
	」という内容のメッセージが表示されます。 ユーザ アカウントの数に特定の制限はありませんが、無限と いうわけではありません。ホスト サーバ上のデータ ベース サイズ、プロセッサの性能、メモリ容量によ って、実際に作成できるユーザ アカウントの数が決 まります。
特定のノード アクセスを 特 定のユーザに割り当てるこ とができますか?	管理者の許可があればできます。管理者は、各ユーザ に固有のノードを割り当てることができます。
ユーザが 1,000 人以上の場 合はどのように管理すれば よいでしょうか。Active Directory はサポートされて いますか?	CC-SG では、Microsoft Active Directory、Sun iPlanet、Novell eDirectory を使用できます。ユーザ アカウントが認証サーバに登録されている場合、 CC-SG は AD/TACACS+/RADIUS/LDAP 認証によ るリモート認証をサポートします。
ディレクトリ サービスとセ キュリティ ツール (LDAP 、AD、RADIUS など) によ る認証には、どのようなオ プションがありますか?	CC-SG では、ローカル認証とリモート認証が可能で す。 サポート対象のリモート認証サーバには、AD、 TACACS+、RADIUS、LDAP があります。
CC-SG にログインするとき に有効なユーザ名とパスワ ードを正しく入力している のに、エラー メッセージ「 Incorrect username and/or password (ユーザ名とパス ワードの一方または両方が 誤っています)」が表示される のはなぜですか?	AD でユーザ アカウントを確認します。AD で、 [Logon To] にドメインの固有のコンピュータが設定 されている場合、CC-SG へのログインは許可されま せん。この場合は、AD で [Logon To] の制限を削除 します。

セキュリティに関する FAQ

質問	回答
セキュリティ	
時々ログインしようとする と、正しいユーザ名やパス ワードを入力しているにも 関わらず、「ログイン情報が 正しくない」という内容のメ	CC-SG へのログインを開始するたびに送られる、セ ッションに特有の ID があります。この ID にはタイ ム アウト機能があり、タイム アウトになる前にユニ ットにログインしないと、セッション ID は無効にな ります。Shift-再ロードを実行すると、CC-SG によっ



Ap I: FAQ

質問	回答
ッセージが表示されます。 なぜでしょうか ?	てページが更新されます。あるいは現行ブラウザを閉 じて、新しいブラウザを開き、再度ログインできます 。Web キャッシュに保存された情報を呼び戻してユ ニットにアクセスすることができないように、より高 いセキュリティ機能が提供されます。
パスワードはどのように保 護されますか ?	パスワードは、一方向性ハッシュである MD5 暗号化 を使用して暗号化されます。これでセキュリティが強 化され、許可のないユーザはパスワード リストにア クセスできません。
特定の時間、ワークステー ションをアイドル状態にし ておいてから CC-SG のメ ニューをクリックすると、 「ログインしていません」と いう内容のメッセージが表 示されることがあります。 なぜでしょうか?	CC-SG は各ユーザ セッションを計時します。事前 に定義した時間アクティブでなければ、 CC-SG では ユーザがログアウトされます。時間の長さはあらかじ め 60 分に設定されていますが、設定を変更すること ができます。セッションが完了したら、 CC-SG を終 了することをお勧めします。
Raritan にはサーバへのルー ト アクセス権があり、管理 機関との問題の原因になる 恐れがあります。顧客にも ルート アクセス権がありま すか? または Raritan は監 査機能または管理機能を提 供しますか?	Raritan, Inc. からユニットが出荷されると、サーバへのルート アクセス権はどの企業にもありません。
SSL 暗号化は内部と外部の 両方ですか (WAN だけでな く LAN も)?	両方です。セッションは、ソース (LAN か WAN か) に関係なく暗号化されます。
CC-SG は CRL リストすな わち無効な証明書の LDAP リストをサポートしますか?	いいえ。
CC-SG はクライアントの証 明書リクエストをサポート しますか?	いいえ。



アカウントに関する FAQ

質問	回答
アカウンティング	
監査証跡レポートのイベン ト発生時刻が正しくないよ うです。なぜでしょうか?	ログ イベント時間は、クライアント コンピュータの 時間設定に従ってログに記録されます。コンピュータ の日付と時刻の設定は調整できます。
監査とログの機能で、だれ が電源プラグを接続または 切断したかを追跡できます か?	電源スイッチ自体の切断はログには記録されませんが 、CC-SG によるパワー制御は監査ログに記録されま す。

パフォーマンスに関する FAQ

質問	回答
パフォーマンス	
CC-SG 管理者として、500 以上のノードを追加し、そ のすべてを自分自身に割り 当てました。CC-SG へのロ グインに時間がかかります。	管理者として多くのノードを自分自身に割り当てると 、CC-SG はすべてのノードに関するすべてのノード 情報をダウンロードするので、このプロセスにかなり の時間がかかります。管理者アカウントは基本的に CC-SG の設定を管理するために使用し、多くのノー ドにアクセスできるような割り当てはしないようにし てください。
クライアントあたりの帯域 幅利用はどれほどですか?	シリアル コンソールへの TCP/IP によるリモート アクセスは、テレネット セッションのネットワーク 活動とほぼ同レベルです。ただし、コンソール ポー ト自体の RS232 帯域幅と SSL/TCP/IP オーバーへ ッドに限定されます。 Raritan リモート クライアント (RRC) は、KVM コ ンソールへのリモート アクセスを制御します。この アプリケーションは、LAN レベルからリモート ダイ ヤルアップ ユーザ向けまで調整できる帯域幅を提供 します。



430

質問	回答
グループ	
特定のサーバを複数のグル ープ内に配置できますか?	はい。ユーザが複数のグループに所属できるのとまったく同様に、1 台のデバイスが複数のグループに所属できます。 たとえば、Sun in NYC は、グループ Sun: "Ostype = Solaris" とグループ New York: "location = NYC" の一部です。
コンソール ポートの利用が アクティブになると、他の ポートの利用にどのような 影響がありますか? たとえ ば、一部の UNIX バリアン トで、ネットワーク インタ フェース経由の管理ができ なくなりますか?	コンソールは、一般に最後の手段となるセキュアで信頼性の高いアクセスパスと考えられます。一部の UNIX システムは、コンソール上でのみルート ログ インが許可されます。セキュリティ上の理由で他のシ ステムでは複数ログインが許可されないので、管理者 がコンソールにログインすると、他のアクセスは拒否 されます。最終的に、管理者は他のすべてのアクセス をブロックする必要がある場合に、コンソールからネ ットワーク インタフェースを無効にすることもでき ます。 コンソール上の標準のコマンド操作は、他のインタフ ェースから同等のコマンドを実行する場合ほど大きな 影響はありません。しかし、ネットワークに依存しな いので、ネットワーク ログインへの応答で過負荷に なるシステムでもコンソール ログインをサポートし ます。そのため、コンソール アクセスの別の利点と して、システムまたはネットワークの問題に関するト ラブルシューティングや診断があります。
CIM の物理レベルでの移動 または交換と論理データベ ースの変更の問題はどう処 理すればよいでしょうか?た とえば、ターゲット サーバ のある CIM を別のポート (同じデバイス上または別の デバイス上) に物理的に移動 した場合にどうなりますか? パードはどうなりますか? ノードはどうなりますか? インタフェースはどうなりま すか?	各 CIM には、シリアル番号とターゲット システム 名があります。Raritan システムでは、CIM はスイッ チ間で接続を移動してもその名前のターゲットへの接 続は保持されます。この移動は、CC-SG のポートお よびインタフェースに自動的に反映され、ポート名と インタフェース名が変更に合わせて更新されます。イ ンタフェースは、ポートに関連したノードの下に表示 されます。ただし、ノード名は変更されません。ノー ドを編集して、手動でノード名を変更する必要があり ます。このシナリオでは、対象となっているすべての ポートが事前に設定済みであることが前提です。ター ゲット サーバおよび CIM を別の未設定ポートに物 理的に移動した場合、CC-SG でポートを設定できま

グループ化に関する FAQ

Ap I: FAQ

質問

回答 す。この場合、ノードは自動的に作成されます。

相互運用性に関する FAQ

質問	回答
相互運用性	
CC-SG は、ブレード シャ ーシ製品とどのように統合 されますか?	CC-SG は、透過なパスとして KVM またはシリアル インタフェースを備えた任意のデバイスをサポートし ます。
CC-SG は、サード パーテ ィ KVM ツールとどのレベ ルまで統合できますか? KVM ポート レベルですか? それとも単にボックス レベ ルですか?	サード パーティ KVM スイッチ統合は、サード パ ーティ KVM ベンダが KVM スイッチの通信プロト コルを公表しない場合、キーボード マクロを使用し て行うのが一般的です。サード パーティ KVM スイ ッチの機能によって、統合の緊密度が変わります。
IP-Reach ボックス経由で同時に 4 つのパスという制限を緩和して、8 つのパスに対応するボックスをロードマップに組み込むにはどうすればよいでしょうか?	現時点での最善の策は、IP-Reach ボックスを CC-SG に統合することです。Raritan では、今後ボ ックスあたりの同時アクセス パスの追加を計画して います。8 パス ソリューションの市場でのニーズと ユース ケースについての必要性を調査中です。

承認に関する FAQ

質問	回答
承認	
RADIUS/TACACS/LDAP を 使用して承認を実行できま すか?	LDAP と TACACS によるリモート認証は可能ですが 、承認はできません。

使い心地に関する **FAQ**

質問

回答

使い心地



Δr	 1) 	FΔ	0
γh	<i>л</i> т.		

質問	回答
ネットワーク ポートまたは ローカル シリアル ポート (たとえば、COM2) を介した コンソール管理について: ロ ギングはどうなりますか ?CC-SG はローカル管理を 取り込みますか?	CC-SG コンソール自体から CC-SG にログインする と、CC-SG が動作するオペレーティング システム (Linux) の root 権限を取得したのと同じことになり ます。Syslog にはこのイベントが記録されますが、 CC-SG コンソール自体でユーザが入力した内容は失 われます。



ライセンス設定に関する FAQ

インストールされているライセンスの置換が必要な場合は、以下のルー ルに従います。

基本ライセンスを最初に置換する必 要があります。	たとえば、スタンドアロン ライセンス CC-E1-512 # CCL-512 を、クラスタ ライセンス CC-2XE1-512 # CCL-512 と置換する場合は、CCL-512 アドオン ラ- り前に基本ライセンス CC-E1-512 を置換する必要が 。 アドオン機能 CCL-512 はスタンドアロンでもクラス
	してすか、フィセンス ファイルに含まれているホス スタンドアロン ライセンスの場合は 1 つ、クラスタ スの場合は 2 つであることに注意してください。この 、アドオン ライセンスの置換も必要です。
基本ライセンスを置換したときに、 異なるタイプのアドオンはすべてク リアされます。	スタンドアロンの基本ライセンスをクラスタの基本ラ に、またはその逆に置換する場合、アドオンは自動的 されるので、正しいホスト ID の新しいライセンスが ります。
基本ライセンスを置換したときに、 アドオンのタイプが同じでホスト ID が一致する場合は、すべてのアドオ ンはクリアされません。	たとえば、CC-E1-512 は CC-E1-256 の置換にも使用 。ホスト ID が両方のライセンスで同じである場合、 ライセンスは引き続き有効になります。
クラスタをスタンドアロン ライセン スで運用している場合は、スタンド アロン ライセンスを置換するために クラスタを削除し、その後再追加す	スタンドアロン ライセンスはクラスタ メンバで共有 ので、スタンドアロン ライセンスで動作しているクラ 各 CC-SG は、ライセンスされているノード数が同じ とが必要です。
る必要があります。	ライセンスされるノード数を CC-SG ユニットそれそ する代わりに、顧客が 2 つの CC-SG ユニット間で スを共有できるように、クラスタ ライセンスに置き を希望する場合があります。
	クラスタを一時的に削除し、ライセンスを置換し、ク 再構築します。
基本ライセンスを置換するには、ユ ーザが機能をチェックアウトする必 要があります。	ライセンスを置換した後、[ライセンス マネージャ] - 動し、利用可能な機能を確認し、必要に応じてそれら クアウトします。これらは自動的にはチェックアウト ん。「 ライセンスをインストールしてチェックアウト 』」を参照してください。



Ap J ショートカット キー

Java ベースの Admin Client では、次のショートカット キーを使用で きます。

操作	ショートカット キー
更新	F5
パネルの印刷	Ctrl + P
ヘルプ	F1
関連テーブルへの行の挿入	Ctrl + I



Ap K 命名規則

この付録では、CC-SG で使用される命名規則について説明します。 CC-SG 設定のどの部分に名前を付けるときも、文字の最大長を守って ください。

この章の内容

ユーザ情報	435
ノード情報	
Location Information (ロケーション情報)	
連絡先情報	
サービス アカウント	
デバイス情報	
ポート情報	
関連	
管理	

ユーザ情報

CC-SG のフィールド	CC-SG で使用可能な文字数
ユーザ名	64
フルネーム	64
User Password (not strong password) (ユーザ パスワード (強 力なパスワード以外))	6-16
User Password (strong password) (ユーザ パスワード (強力なパスワー ド))	設定可能な文字数 最小: 8 最大: 16-64
User Email Address (ユーザの電子メ ール アドレス)	60
User Phone Number (ユーザの電話 番号)	32
ユーザ グループ名	64
User Group Description (ユーザ グ ループの説明)	160



ノード情報

CC-SG のフィールド	CC-SG で使用可能な文字数
ノード名	64
Node Description (ノードの説明)	160
メモ	256
Audit Information (監査情報)	256

Location Information (ロケーション情報)

CC-SG のフィールド	CC-SG で使用可能な文字数
Department	64
サイト	64
Location	128

連絡先情報

CC-SG のフィールド	CC-SG で使用可能な文字数
プライマリ担当者名	64
電話番号	32
携帯電話番号	32
セカンダリ担当者名	64
電話番号	32
携帯電話番号	32

サービス アカウント

CC-SG のフィールド	CC-SG で使用可能な文字数
サービス アカウント名	64
ユーザ名	64
パスワード	64



Ap K: 命名規則

CC-SG のフィールド	CC-SG で使用可能な文字数
説明	128

デバイス情報

CC-SG のフィールド	CC-SG で使用可能な文字数
デバイス名	64
PX デバイス名にピリオドを含める ことはできません。ピリオドを含む PX デバイス名をインポートすると 、ピリオドはハイフンに変換されま す。	
Device Description (デバイスの説明)	160
Device IP/Hostname (デバイス IP / ホスト名)	64
ユーザ名	64
パスワード	64
メモ	256

ポート情報

CC-SG のフィールド	CC-SG で使用可能な文字数
ポート名	32

関連

CC-SG のフィールド	CC-SG で使用可能な文字数
カテゴリ名	32
エレメント名	32
デバイス グループ名	40
ノード グループ名	40

管理



CC-SG のフィールド	CC-SG で使用可能な文字数
クラスタ名	64
隣接システムの名前	64
Authentication Module Name (認証モ ジュール名)	31
バックアップ名	64
Backup File Description (バックアッ プ ファイルの説明)	255
ブロードキャスト メッセージ	255



診断コンソール起動メッセージ

バージョン 4.0 より前の CC-SG 診断コンソールでは、起動のたびに 多くのメッセージが画面に表示されます。これらのメッセージは、標準 の Linux 診断および警告メッセージであり、通常はシステムの問題を暗 示するものではありません。以下の表には、よく表示されるいくつかの メッセージについて簡単に説明しています。

メッセージ	説明
hda:	 メッセージは、システム内の何かが DVD-ROM ドライブと通信しようとしていることを示します。このメッセージはさまざまな状況で呼び出されます。たとえば、 ユーザが DVD-ROM ドライブのドアを開いた、または閉じた場合。 起動時にオペレーティング システムが DVD-ROM ドライブをチェックし、メディアがないことを検出した場合。 他にもこのメッセージが呼び出されるシナリオがありますが、
	ここでは説明しません。
avc:	このメッセージは、内部セキュリティ監査および制御システム (SELinux サブシステム) から表示されます。システムは、セ キュリティ ポリシーを強制することなく警告を発行するので 、システムで問題があることは示していません。
ipcontracks:	メッセージは、CC-SG が起動されるたびに常に表示されるの で、これは正常です。

CC-SG では、バージョン 4.0 以降これらのメッセージが無効になって いますが、内部ログでは今でも使用できる点に注意してください。した がって、CC-SG を 3.x から 4.x にアップグレードすると、これらの診 断コンソール メッセージが表示されなくなります。



Ap L

索引

E

[Virtual Topology] (仮想トポロジー)表示への アクセス - 138 [デバイス プロファイル] 画面 - 57 [デバイス] タブ - 54 [デバイス] タブの右クリック オプション -58 [ノード] タブ - 116 [ユーザ] タブ - 177

ſ

『CC-SG 管理者ガイド』中の新規機能 - xvii

2

2 ファクタ認証 - 231,422
 2 ファクタ認証のサポート環境 - 422
 2 ファクタ認証の既知の問題 - 423
 2 ファクタ認証の設定条件 - 422

Α

Access Client の Firefox ユーザは JNLP フ ァイルのダウンロードが必要 -139 AD および CC-SG の概要 - 213 AD グループの名前の変更および移動 - 225 AD と CC-SG の同期 - 221 AD のグループ設定 - 217, 219 AD のユーザ名の指定 - 212 AD の一般設定 - 214, 219 AD の識別名の指定 - 212 AD の詳細設定 - 215, 219 AD の信頼設定 - 218, 219 AD の日次同期の時刻の変更 - 224 AD モジュールの編集 - 218 AD ユーザ グループ レポート - 243 AD ユーザ グループのインポート - 219 Admin Client でのカスタム表示の使用 - 203 Administrator Console - 340 Administrator Console について - 332, 340 Administrator Console のナビゲート - 342 Administrator Console へのアクセス - 257, 340 Administrator Console 画面 - 341

AES 暗号化 - 298
AES 暗号化に関するブラウザのチェック - 299
AKC ダウンロード サーバ証明書の検証の有効化 - 144, 283
AKC を使用するため前提条件 - 144, 269

С

CC スーパーユーザ グループ - 178 CC ユーザ グループ - 178 CC-NOC - 331 CC-SG Admin Client - 9 CC-SG Admin Client を介したブラウザ ベー スのアクセス -5 CC-SG LAN ポートについて - 272, 273, 275 CC-SG およびネットワーク設定 - 389 CC-SG からのレポートのデータの消去 - 234. 235, 236, 278 CC-SG クラスタの設定 - 18, 287, 337 CC-SG クラスタの要件 - 287 CC-SG クラスタへのアクセス - 288, 289 CC-SG クラスタリング - 392 CC-SG サーバ時間および時刻の設定 - 279 CC-SG サーバ時間の設定 - 35 CC-SG シリアル ナンバーの検出 - 329 CC-SG スーパー ユーザのユーザ名の変更 -195 CC-SG セッションの終了 - 263 CC-SG ディスク監視 - 339,419 CC-SG データベースのマイグレーション xvii, 260, 261 CC-SG での仮想インフラストラクチャの設 定 - 126, 140 CC-SG デフォルト フォント サイズの変更 -194 CC-SG で推奨される DHCP 設定 - 271, 274, 277 CC-SG と IPMI、iLO/RILOE、DRAC、RSA の クライアント - 395 CC-SG と Raritan デバイス - 391 CC-SG と SNMP - 395 CC-SG にログインする - 26 CC-SG ネットワークに必要なオープン ポー F



索引

要旨 - 389 CC-SG ネットワークの設定 - 213, 271 CC-SG のアップグレード - 33, 256, 259, 260 CC-SG のシャットダウン - 259, 260, 262 CC-SG のシャットダウン後の再起動 - 262 CC-SG のタイトル、日付および時刻 - 335 CC-SG のデバイス管理の一時停止 - 100, 314 CC-SG のデフォルト設定 - 26 CC-SG のバックアップ - 248, 255, 256, 258, 261, 284, 314 CC-SG のリストア - 249, 251, 261 CC-SG のリセット - 253 CC-SG のログアウト - 263 CC-SG の再起動 - 255, 274, 354 CC-SG の終了 - 263, 264 CC-SG の電源切断 - 263 CC-SG の内部ログの消去 - 278 CC-SG パスワードについて - 302 CC-SG への AD モジュールの追加 - 213 CC-SG への LDAP (Netscape) モジュールの 追加 - 225 CC-SG への SSH アクセス - 300, 319 CC-SG への SSH アクセスに使用するポー ト番号の設定 - 300 CC-SG へのアクセス -5 CC-SG 工場出荷時設定へのリセット - 260, 262, 357 CC-SG 通信チャンネル - 391 CC-SG 内の別のデバイスによって管理され る電源タップの設定 - 105, 107 CC-SG 内部ポート - 396 CommandCenter Secure Gateway $\hat{\mathcal{E}}$ VMware ESX Server 4.0 にインストールす る - 25 CSV ファイルのインポート - 411 CSV ファイルのインポートによるカテゴリと エレメントの追加 - 50 CSV ファイルのインポートによるデバイスの 追加 - 86 CSV ファイルのインポートによるノードの追 加 - 156 CSV ファイルのインポートによるユーザの追 加 - 187

CSV ファイルのインポートを利用した IP アドレスの編集 - 169
CSV ファイルの共通要件 - 50, 87, 157, 188, 412
CSV ファイルの問題のトラブルシューティング - 51, 92, 168, 192, 384, 414

D

describe メソッドと select メソッドの対比 -85, 171 Dominion PX デバイスの追加 - 60, 61, 63 DRAC 5 接続の詳細 - 143 DRAC パワー制御接続のインタフェース -141, 144

E

E1 モデル - 387 E1 一般仕様 - 387 E1 環境要件 - 387

\mathbf{F}

FAQ - 424

Ι

IBM IMM モジュール接続の詳細 - xvii, 147
IBM LDAP の設定 - 228
ILO Processor、Integrity ILO2、および RSA の パワー制御接続のインタフェース - 141, 145
IP アドレスの ping - 345
IP アドレスの確認 - 34
IP フェイルオーバ モードとは - 271, 273
IP 分離モードとは - 271, 275
IPMI パワー制御接続のインタフェース - 146, 147
IP-Reach と UST-IP 管理 - 104

J

Java RDP 接続の詳細 - 143 Java キャッシュのクリア - 258, 268, 415 JRE との RSA の互換性 - 146 JRE 非互換性 - 5, 6



Κ

KVM スイッチが統合されたブレード シャー シ-71 KVM スイッチが統合されていないブレード シャーシ - 71 KVM ポートの設定 - 67,77 KVM またはシリアル デバイスの追加 - 60, 61, 72, 79, 109, 111 KX、KX2、KX2-101、KSX2、P2SC に接続さ れた電源タップの設定 - 107, 108 KX、KX2、KX2-101、KSX2、または P2SC デ バイスに接続された電源タップ デバイスの 追加 - 108 KX、KX2、KX2-101、KSX2、または P2SC デ バイスに接続された電源タップの削除 -108, 109 KX、KX2、KX2-101、KSX2、または P2SC の 電源タップの別のポートへの移動 - 108 KX2 2.3 以降に接続するアナログ KVM スイ ッチの設定 - 78 KX2 デバイス用の HTTP ポートおよび HTTPS ポートの変更 - 64 KX2 に接続されたブレード シャーシ デバイ スの設定 - 70 KX2 に接続する KVM スイッチの追加 - 79 KX2 に接続するアナログ KVM スイッチ デ バイスのポートの設定 - 79

L

LDAP と AD の識別名 - 211 LDAP と CC-SG について - 225 LDAP の一般設定 - 226 LDAP の識別名の指定 - 212 LDAP の詳細設定 - 227 Linux のサーバ - 20, 24 Linux または Windows サーバにライセンス サーバ ソフトウェアをインストールする -20 Location Information (ロケーション情報) - 436

M

MIB ファイル - 287 Microsoft RDP 接続の詳細 - 143

Ν

NAT 対応ファイアウォール経由の CC-SG ア クセス - 397 NTP ステータスの表示 - 373

0

OpenLDAP (eDirectory) の設定 - 228

Ρ

Paragon II システム コントローラ (P2-SC) -104 Paragon II システム デバイスへの専用アクセ ス - 104 PC クライアントから CC SG - 393 PC クライアントとノード - 394 Power IQ IT デバイスのパワー制御 - 105. 107, 166, 377, 383 Power IQ IT デバイスのパワー制御の設定 -380 Power IQ Proxy のパワー制御接続のインタフ ェース - 141, 147, 380 Power IQ および CC-SG の同期 - 314, 381 Power IQ および CC-SG の同期の設定 - 377, 379, 380, 381, 382 Power IQ からの Dominion PX データのイン ポートとエクスポート - 383 Power IQ からの電源タップのインポート -377, 383 Power IQ サービスの設定 - 148, 167, 378, 379, 380 Power IQ で使用する Dominion PX データの エクスポート - 377, 385 Power IQ の統合 - 377 Power IQ への接続のトラブルシューティング - 379 Power IQ 同期ポリシー - 381, 382

R

RADIUS と CC-SG について - 230 RADIUS による 2 ファクタ認証 - 231 RADIUS の一般設定 - 230 RADIUS モジュールの追加 - 230 RAID ステータスとディスク使用率の表示 -366, 368, 419



索引

RAID ディスクの修復または再作成 - 367, 368, 369, 371 RSA インタフェースの詳細 - 145

S

SNMP トラップ - 287, 408 SNMP の設定 - 285 SSH コマンドとパラメーター - 321 SSH コマンドのヘルプの表示 - 320 SSH を介した診断コンソールへのアクセス -332 SSH を使用してシリアル アウト オブ バン ド インタフェース経由でノードに接続 -325 SSH 接続の終了 - 324, 327 Status Console - 333, 365 Status Console について - 332, 333 Status Console へのアクセス - 333 Status Console 情報 - 335 Sun One LDAP (iPlanet)の設定 - 227 SX 3.0 および KSX に接続された電源タップ の設定 - 107, 109 SX 3.0 デバイスまたは KSX デバイスに接続 された電源タップの削除 - 109, 110 SX 3.0 デバイスまたは KSX デバイスに接続 された電源タップの追加 - 109 SX 3.1 デバイスに接続された電源タップの削 除 - 111, 112 SX 3.1 デバイスに接続された電源タップの追 加-111.112 SX 3.1 に接続された電源タップの設定 - 107. 111 SX 3.1 の電源タップの別のポートへの移動 -111, 112

Т

TACACS+ と CC-SG について - 229 TACACS+ の一般設定 - 230 TACACS+ モジュールの追加 - 229 Traceroute の使用 - 347

\mathbf{V}

V1 および E1 の仕様 - 386 V1 モデル - 386 V1 一般仕様 - 386 V1 環境要件 - 386 VGA/キーボード/マウス ポートからの診断コ ンソールへのアクセス - 332 VGA/キーボード/マウス ポートまたは SSH からの Status Console - 335 VGA/キーボード/マウス ポートまたは SSH からの Status Console へのアクセス - 333 VMware ツールをインストールまたはアップ グレードする - 31 vSphere 4 ユーザは新しいプラグインをイン ストールする必要がある - 136

W

Web サービス API - 329 Web ブラウザ インタフェース - 141, 149 Web ブラウザ インタフェースの追加のヒン ト - 150, 166 Web ブラウザからの Status Console - 339 Web ブラウザからの Status Console へのア クセス - 333, 334, 421 Windows のサーバ - 21, 24, 25

あ

アウト オブ バンド KVM、アウト オブ バン ド シリアル接続のインタフェース - 141, 143 アカウントに関する FAQ - 429 アクセス レポート - 182, 236 アクセス制御のポリシー - 43, 48, 81, 176, 180.197 アクセス制御リスト - 309,359 アクティブ ノード レポート - 242 アクティブ ユーザ レポート - 237 アップグレード後に古いバージョンのアプリ ケーションが開く - 37, 267, 268 アプリケーション バージョンの確認とアップ グレード - 36,266 アプリケーションの削除 - 268 アプリケーションの追加 - 37, 267, 268 インストール ファイルをダウンロードする -20 インタフェースについて -116,280 インタフェースの削除 - 134, 152 インタフェースの追加 - 123, 140, 151, 380 インタフェースの追加、編集、削除 - 122.140



インタフェースの編集 - 151 インタフェースまたはポートのタイプのデフ ォルト アプリケーションの設定 - 270 インタフェースをブックマークに設定 - 152, 153, 242 インタフェースを追加した結果 - 151 インバンド接続のインタフェース - 140, 142 インフラストラクチャ サービスへのアクセス - 393 インポートに関する監査証跡エントリ - 52, 92, 168, 193, 385, 413 エラー ログ レポート - 235 エレメントの追加 - 49

か

ガイド付き設定の関連 - 38, 39 ガイド付き設定を使用した CC-SG の設定 -11, 38, 48, 197 ガイド付き設定を使用する前に - 38 カスタム JRE 設定の定義 - 6,284 カスタム表示の種類 - 202 カテゴリとエレメントの CSV ファイルの要 件 - 50 カテゴリとエレメントの CSV ファイルの例 - 51 カテゴリとエレメントのインポート - 51 カテゴリとエレメントのエクスポート - 50. 52 カテゴリとエレメントの作成 - 39 カテゴリとエレメントの追加、編集、削除-48 カテゴリの削除-49 カテゴリの追加-48 カテゴリ別の表示 - 202 クライアントおよび CC-SG 間での AES 暗 号化の要求 - 299 クライアントのブラウザ要件 -4 クラスタ ライセンス - xvii, 259, 292 クラスタのアップグレード - xvii, 259, 260, 291, 292 クラスタの作成 - 19, 260, 288 クラスタの削除 - 291 クラスタの設定 - 289 クラスタの復元 - 290 グループの作成 - 38,41 グループ化に関する FAQ - 430 コマンドのヒント - 321,323

さ

サービス アカウント - 119,436 サービス アカウントのパスワードの変更 -121 サービス アカウントの概要 - 119 サービス アカウントの追加、編集、削除 - 120 サービス アカウントをインタフェースに割り 当て - 122 システム スナップショットの取得 - 375, 418, 420, 421 システム メンテナンス - 246 システム、サーバ、およびネットワークのステ ータス - **336** システム管理者グループ - 178 シック クライアント アクセス -6 シック クライアントのインストール -7 シック クライアントの使用 -8 ショートカット キー - 434 シリアル ポートの設定 - 67 シリアル管理ポート - 328 シリアル対応デバイスへの SSH 接続の作成 - 324 スケジュールされたタスクを使用したデバイ ス管理の一時停止と再開 - xvii, 101, 314 スケジュールされたレポート - 244, 245, 313 スケジュールしたタスクの変更 -318 すべての AD モジュールの日次同期の有効化 または無効化 - 223 すべてのクライアント接続にダイレクト モー ドを設定 - 280 すべてのクライアント接続にプロキシ モード を設定 - 281 すべてのユーザ グループの AD との同期 -219, 221, 222 すべてのユーザに強力なパスワードを要求 -301 すべての設定データの KX2、KSX2、または KX2-101 デバイスへのリストア - 94,97 セキュリティ マネージャ - 298,319 セキュリティに関する FAQ - 427

た

ダイレクト モードとプロキシ モードの組み 合わせを設定 - 276, 281



索引

タスク マネージャ - 10, 35, 244, 247, 279, 310, 311, 380 タスクのスケジュール - 100, 101, 221, 223, 261, 313, 318, 382 タスクのスケジュール変更 - 318, 319 タスクのタイプ - 312 タスクの検索および表示 - 313 タスクの削除 - 319 タスクの電子メール通知 - 312 チャットの使用 - 155 ディスク テストのスケジュール - 369 ディスクまたは RAID テストの実行 - 367 デバイス グループ データ レポート - 239 デバイス グループ マネージャ - 81 デバイス グループおよびノード グループの 追加-42 デバイス グループでフィルタ - 202 デバイス グループの概要 - 81 デバイス グループの削除 -86 デバイス グループの追加 - 82,86,197 デバイス グループの編集 -86 デバイス バックアップ ファイルの保存、アッ プロード、削除 - 97 デバイス パワー マネージャ - 102 デバイス ファームウェアのアップグレード レポート - 245, 318 デバイス ファームウェアのアップグレードの スケジュール - 313, 314, 316, 318 デバイス ファームウェアの管理 - 270 デバイス プロファイルへの場所と連絡先の追 加-57,66 デバイス プロファイルへの注意の追加 - 57, 65 デバイス、デバイス グループ、ポート - 53 デバイスおよびノードのカスタム表示 - 116, 202 デバイスとポートのアイコン - 54 デバイスの CSV ファイルの要件 - 79,87 デバイスの CSV ファイルの例 - 91 デバイスの ping - 100 デバイスのアップグレード - 62, 93, 270 デバイスのインポート - 92 デバイスのエクスポート - 87,92 デバイスのカスタム表示 - 206 デバイスのカスタム表示の削除 - 208

デバイスのカスタム表示の追加 - 206 デバイスのカスタム表示の適用 - 207 デバイスのカスタム表示の変更 - 207 デバイスのデフォルトのカスタム表示の指定 - 208 デバイスのデフォルトのカスタム表示をすべ てのユーザに指定 - 208 デバイスの管理の再開 - 101,314 デバイスの管理ページの起動 - 103 デバイスの関連、場所、および連絡先の一括コ ピー - 77 デバイスの検索 - 58 デバイスの検出 - 59,60 デバイスの検出と追加-40 デバイスの再起動 - 100.314 デバイスの削除 - 57,66 デバイスの追加-60 デバイスの表示 - 54 デバイスの編集 - 63, 64 デバイス資産レポート - 239 デバイス情報 - 437 デバイス設定 - 38, 39, 281 デバイス設定のコピー - 99,314 デバイス設定のバックアップ - 94,314 デバイス設定のリストア - 95,314 デバイス設定のリストア (KX、KSX、KX101、 SX、IP-Reach) - 95 デバイス設定またはユーザとユーザ グループ のデータのみの KX2、KSX2、KX2-101 デ バイスへのリストア - 96 デバッグ モード - 418 デフォルト アプリケーションの割り当ての表 示 - 269 デフォルトのアプリケーションについて -269 デフォルトのアプリケーションの設定 - 269 デフォルトのユーザ グループ - 178 デフォルトの検索設定の変更 - 58, 194 トポロジー表示 - 58 トラブルシューティング - 415

な

ナビゲーション キーのリマインダ - 338 ネットワーク インタフェース設定の編集 (ネ ットワーク インタフェース) - 344



ネットワーク設定について -3,34,271,287, 344 ネットワーク設定以外のすべての設定データ の KX2、KSX2、または KX2-101 デバイス へのリストア - 96 ノード グループ データ レポート - 243 ノード グループでフィルタ - 202 ノード グループの概要 - 170 ノード グループの削除 - 175 ノード グループの追加 - 171, 197 ノード グループの追加、編集、削除 - 170 ノード グループの編集 - 174 ノード プロファイル - 117 ノード プロファイルへの場所と連絡先の追加 - 117, 125 ノード プロファイルへの注意の追加 - 117, 125 ノード、ノード グループ、インタフェース -53.114 ノードとインタフェースのアイコン - 119 ノードとインタフェースの概要 - 115 ノードにアクセスするためのアプリケーショ ンについて - 266 ノードにアクセスするためのアプリケーショ ンの設定 - 266 ノードについて - 115 ノードの CSV ファイルの要件 - 157 ノードの CSV ファイルの例 - 168 ノードのインポート - 168, 169 ノードのエクスポート - 148, 157, 166, 169 ノードのカスタム表示 - 203 ノードのカスタム表示の削除 - 205 ノードのカスタム表示の追加 - 203 ノードのカスタム表示の適用 - 203 ノードのカスタム表示の変更 - 204 ノードのデフォルトのカスタム表示の指定 -205 ノードのデフォルトのカスタム表示をすべて のユーザに指定 - 205 ノードの関連、場所、および連絡先の一括コピ — - 154 ノードの削除 - 124, 135 ノードの説明 - 172 ノードの選択 - 171 ノードの追加 - 123,380 ノードの追加、編集、および削除 - 123

ノードの表示 - 116
ノードの編集 - 124, 133
ノードの名前 - 115
ノードへの ping の実行 - 139
ノードへの RDP アクセス - 397
ノードへの SSH アクセス - 397
ノードへの VNC アクセス - 397
ノードへのダイレクト ポート アクセスの設定 - 153
ノードへの接続 - 139
ノード作成レポート - 242
ノード資産レポート - 153, 241, 243
ノード情報 - 436

は

はじめに -1 パスワードの変更 - 193 バックアップ ファイルの削除 - 251 バックアップ ファイルの保存 - 250, 256 バックアップ ファイルの保存および削除 -248, 250, 253 パフォーマンスに関する FAQ - 429 ファームウェアのアップロード - 270 ファームウェアの削除 - 271 ファイルへのレポートの保存 - 233, 243 プライマリ ノードとセカンダリ ノードのス テータスの切り替え - 259, 290 プライマリ ノードのアップグレード エラー - xvii, 259, 260 ブラウザ キャッシュのクリア - 258,415 ブラウザ接続プロトコルの設定 HTTP または HTTPS/SSL - 300 ブレード サーバ ポートの標準 KX2 ポート へのリストア - 56,77 ブレード サーバのステータスの変更 -74 ブレード シャーシ デバイスのスロットの削 除 - 75 ブレード シャーシ デバイスのスロットの設 定 - 58, 71, 72, 73 ブレード シャーシ デバイスの削除 -76 ブレード シャーシ デバイスの追加 - 71,76 ブレード シャーシ デバイスの編集 - 75, 124 ブレード シャーシの概要 -70 ベース DN の指定 - 212 ポータル - 294, 304 ポートの削除 - 70



索引

ポートの照会レポート - 240 ポートの設定 - 67, 111 ポートの設定により作成されるノード - 67, 68, 124 ポートの編集 - 69 ポート情報 - 437 ポート並び替えオプション - 55 ポリシーの削除 - 200 ポリシーの追加 - 81, 170, 197, 198, 201 ポリシーの編集 - 199

ま

マイグレーションの要件 - xvii, 261 メモリ診断 - 417 メンテナンス モード - 199, 246 メンテナンス モードの起動 - 36, 247, 257, 259, 267 メンテナンス モードの終了 - 247, 258

Þ

ユーザ アカウント - 211 ユーザ グループ データ レポート - 239 ユーザ グループのアクセス監査の設定 - 118, 183, 185 ユーザ グループの削除 - 181 ユーザ グループの追加 - 179, 182 ユーザ グループの追加、編集、削除 - 122, 179 ユーザ グループの編集 - 180 ユーザ グループへのポリシーの割り当て xvii, 180, 197, 201 ユーザ グループ権限 - 179, 238, 398 ユーザ プロファイル - 193 ユーザあたりの KVM セッション数の制限 -44, 179, 181, 182 ユーザとユーザ グループ - 81, 170, 176, 201, 211, 229, 230 ユーザとユーザ グループの追加 - 44 ユーザの CSV ファイルの要件 - 188 ユーザの CSV ファイルの例 - 192 ユーザのインポート - 192 ユーザのエクスポート - 188, 193 ユーザのグループへの割り当て - 185, 186 ユーザのログアウト - 195 ユーザの一括コピー - 196 ユーザの削除 - 186

ユーザの切断 - 103 ユーザの追加 - 183, 238 ユーザの追加、編集、削除 - 183 ユーザの編集 - 185 ユーザをグループから削除 - 186, 187 ユーザ管理 - 38, 44 ユーザ情報 - 435

6

ライセンス サーバの障害 -28 ライセンス サーバを起動する -24 ライセンス サーバ管理用のコマンド ライン ユーティリティ - 29 ライセンス サーバ通信 -27 ライセンス ファイルをライセンス サーバに コピーする - 24 ライセンスにアクセスする -28 ライセンスの追加 - xvii, 34 ライセンスをインストールしてチェックアウ トする - 27, 28, 433 ライセンスを取得する - 15, 20, 22 ライセンス設定 - クラスタ - 新規顧客 - 18 ライセンス設定 - はじめに - 新規顧客および 既存の顧客 - 12 ライセンス設定 - ライセンス サーバを使用 する仮想アプライアンス - 12, 13, 19 ライセンス設定 - ライセンスのインストール 前の限られた動作 - 12, 18, 28, 32 ライセンス設定 - 基本的なライセンス情報 -13 ライセンス設定 - 既存の顧客 - 12, 13, 33 ライセンス設定 - 再ホスト - 33 ライセンス設定 - 新規顧客 - 物理アプライア ンス - 12, 13, 15, 16, 18, 19 ライセンス設定に関する FAQ - xvii, 34, 433 リモート システム監視の設定 - 364.397. 419 リモート システム監視ポート - 397 リモート ストレージ サーバを使用する仮想 アプライアンス - 31 リモート認証 - 176, 210, 298 レポート - 232, 315 レポート データのソート - 232 レポート フィルタの非表示または表示 - 234 レポートの印刷 - 233



レポートの使用 - 232 レポートの詳細の表示 - 233 レポートの列幅の変更 - 232 ログ アクティビティの設定 - 278,314 ログイン設定 - 300 ログイン設定の表示 - 301 ロックアウト ユーザ レポート - 238 ロックアウト設定 - 238,302

わ

ワイルドカードの例 - 59

漢字

一般的な FAQ - 424 仮想アプライアンスおよびストレージ サーバ のバックアップとスナップショットを設定 する - 31 仮想アプライアンスのインストール要件 -19 仮想インフラストラクチャと CC-SG の同期 - 137 仮想インフラストラクチャの削除 - 135 仮想インフラストラクチャの同期 - 137 仮想インフラストラクチャの日次同期の有効 化または無効化 - 137 仮想インフラストラクチャの用語 - 126 仮想ノードの概要 - 127 仮想ホスト ノードのリブートまたは強制リブ 一下 - 138 仮想ホストと仮想マシンを持つ制御システム の追加 - 127, 133 仮想マシン ノードの削除 - 135 仮想マシンを持つ仮想ホストの追加 - 130. 133 仮想メディアのサポート - 201 可用性レポート - 237,261 外部 AA サーバの順序の確立 - 213 外部 SMTP サーバの設定 - 310 完全バックアップと標準バックアップの違い は何ですか。 - 248, 250, 252 監査証跡レポート - 234 管理 - 437 管理対象電源タップ - 53, 60, 63, 105, 107 管理対象電源タップ接続用インタフェース -106, 107, 108, 110, 112, 113, 141, 146 関連 - 437 関連 - カテゴリとエレメントの定義 - 47

関連、カテゴリ、エレメント - 47,57,62,64, 81, 110, 117, 123, 170 関連について - 47 関連の作成方法 - 48 関連の用語 - 47 休止タイマーの設定 - 304 検索用ワイルドカード - 58 互換表の確認 - 36 高度な管理 - 184, 185, 214, 219, 265 今日のメッセージ - 335 今日のメッセージの設定 - 265 使い心地に関する FAQ - 431 使用を始める際に - 11 使用可能なライセンス - 13, 17, 252 承認に関する FAQ - 431 証明書 - 306 証明書タスク - 306 障害後にライセンス サーバを再起動する -28 診断コンソール - 5,332 診断コンソール アカウント設定 - 361 診断コンソールからの CC-SG システムの電 源オフ - 263,355 診断コンソールでのトップ ディスプレイの表 示 - 372 診断コンソールでのログ ファイルの表示 -350 診断コンソールにログインし CC-SG IP アド レスを設定する - 26 診断コンソールのパスワード設定 - 340, 356, 360 診断コンソールのビデオ解像度の変更 - 376 診断コンソールへのアクセス - 332,333 診断コンソールを使用した CC スーパー ユ ーザのパスワードのリセット - 356 診断コンソールを使用した CC-SG のリブー ŀ - 354, 376, 417 診断コンソールを使用した CC-SG の再起動 - 259, 260, 262, 354 診断コンソール起動メッセージ - 439 診断コンソール設定の編集 - 343 診断ユーティリティ - 417 制御システム、仮想ホスト、仮想マシンの編集 - 133. 135 制御システムおよび仮想ホストの削除 - 135 静的ルートの編集 - 276, 346, 348



449

索引

接続モード ダイレクトおよびプロキシ - 280, 397 接続モードについて - 116, 143, 280 全 AD モジュールの同期 - 219, 221, 222, 223, 314 全ユーザ データ レポート - 238 相互運用性に関する FAQ - 431 端末エミュレーション プログラム - 329 通知マネージャ - 310, 312 電源タップ デバイスの追加 - 60, 61, 63 電源タップ デバイスまたは Dominion PX デ バイスの編集 - 65 電源タップのコンセントの設定 - 107, 108, 110, 112, 113 電源タップのデバイスまたはポートの関連の 変更 (SX 3.0、KSX) - 109, 111 電子メール アドレスの変更 - 194 同一ユーザ名での複数ログインを許可 - 303 認証および承認のモジュール指定 - 212 認証と承認 (AA) の概要 - 210 認証に関する FAQ - 426 認証の流れ - 211 必要条件 -1 複数ページ レポート間の移動 - 233 物理アプライアンスのホスト ID の検索およ びデータベース内のノード数の確認 - 15, 17, 18 別のタスクと類似したタスクのスケジュール - 319 別のポートへのブレード シャーシ デバイス の移動 - 76 名前の変更 - 194 命名規則 - 38, 49, 61, 63, 67, 68, 82, 115, 123, 124, 142, 149, 171, 179, 184, 194, 198, 378, 412, 435 予定タスクとメンテナンス モード - 247 用語/略語 - 2, 61, 63, 226, 230, 231, 274, 276, 293, 295, 311, 323, 344, 378 履歴データ傾向分析レポートの表示 - 339, 365 隣接システムとは - 271, 293, 294, 297 隣接システムのメンバの削除 - 297 隣接システムのメンバの追加 - 295 隣接システムの更新 - 297 隣接システムの作成 - 293 隣接システムの削除 - 298

隣接システムの設定 - 293 隣接システムの設定の管理 - 296 隣接システムの編集 - 295 例 PX ノードへの Web ブラウザ インタフ ェースの追加 - 149, 151 連続したタスクのスケジュール - 312 連絡先情報 - 436

Raritan.
😻 Raritan.

▶ 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:+81-3-3523-5991 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