CommandCenter Secure Gateway

管理者ガイド
リリース **5.3**

CCA-0P-v5.3-J
2012 年 7 月
255-80-5140-00-0O

FCC 情報

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

VCCI 情報 (日本)

この装置は、情報処理装置等電波障害自主規制協議会（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。

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

同梱された電源ケーブルは、本製品専用に使われるものです。

目次

高度な管理 282

『CC-SG 管理者ガイド』中の新規機能

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。

- *ライセンス設定オプション - 仮想アプライアンス* 『*19*p. 』
- *VMware ツールをインストールまたはアップグレードする* 『*20*p. 』
- *IPv6 ネットワーク デバイスの検出および追加* 『*54*p. 』
- *IPv6 で受信するように DNS サーバを設定* 『*55*p. 』
- *デバイスの検出* 『*55*p. 』
- *KVM またはシリアル デバイスの追加* 『*57*p. 』
- *ホスト名でデバイスを追加* 『*60*p. 』
- *デバイスの編集* 『*61*p. 』
- *IPv6 対応の KX II デバイスの証明書* 『*64*p. 』
- *デバイスの CSV ファイルの要件* 『*85*p. 』
- *デバイスの ping* 『*97*p. 』
- *CC-SG での仮想インフラストラクチャの設定* 『*124*p. 』
- *仮想ホストと仮想マシンを持つ制御システムの追加* 『*125*p. 』
- *仮想マシンを持つ仮想ホストの追加* 『*128*p. 』
- *VCenter の必要最小限の許可* 『*134*p. 』
- *VCenter が追加されていない場合は VMware リモート コンソール プラグインを手動でインストール* 『*135*p. 』
- *インバンド接続のインタフェース - RDP、VNC、SSH、RSA KVM、iLO Processor KVM、DRAC KVM、TELNET* 『*141*p. 』
- *Microsoft RDP 接続の詳細* 『*143*p. 』
- *Java RDP 接続の詳細* 『*143*p. 』
- *VNC 接続の詳細* 『*144*p. 』
- *ILO Processor、Integrity ILO2、および RSA のパワー制御接続のインタフェース* 『*147*p. 』
- *Web ブラウザ インタフェース* 『*151*p. 』
- *IPv6 を使用したノードのインタフェースの追加* 『*154*p. 』
- *認証と承認（AA）の概要* 『*224*p. 』
- *AD の詳細設定* 『*229*p. 』
- *統合 Windows 認証による SSO の設定* 『*239*p. 』
- *レポートでの IP アドレス* 『*250*p. 』
- *デバイス資産レポート* 『*256*p. 』
- *デバイス グループ データ レポート* 『*256*p. 』
- *ノード資産レポート* 『*258*p. 』
- *CC-SG のバックアップ* 『*265*p. 』

- *IPv4 を使用する IP フェイルオーバ モードまたは IPv6 を使用するデュアル スタック モードの設定* 『*291*p. 』
- *IPv4 を使用する IP 分離モードまたは IPv6 を使用するデュアル スタック モードの設定* 『*294*p. 』
- *IPv6 のサポート* 『*297*p. 』
- *IP アドレスに対する CC-SG ホスト名を DNS に登録* 『*297*p. 』
- *重大度レベルの例をログに記録* 『*299*p. 』
- *SNMP の設定* 『*306*p. 』
- *CC-SG クラスタの要件* 『*310*p. 』
- Cluster Status の定義
- *隣接システムの設定* 『*316*p. 』
- *証明書タスク* 『*331*p. 』
- *アクセス制御リスト* 『*334*p. 』
- *タスクのスケジュール* 『*339*p. 』
- *SSH アクセスの有効化* 『*346*p. 』
- *Dominion SX シリアル ターゲットへのダイレクト ポート アクセス* 『*354*p. 』
- *ディスク ステータスの確認* 『*403*p. 』
- *システム スナップショットの取得* 『*406*p. 』
- *Power IQ の統合* 『*408*p. 』
- *E1 モデル ユニットの LED* 『*419*p. 』
- *E1 モデル ユニットの音響アラームと赤色 LED* 『*420*p. 』
- *CC-SG ディスク監視* 『*451*p. 』
- *Dominion KX2 デュアル ビデオ ポートの設定および推奨設定* 『*455*p. 』
- *CC-SG でのデュアル ポート ビデオの設定および使用* 『*456*p. 』
- *CC-SG 仮想アプライアンスによる VMware High Availability または Fault Tolerance の活用* 『*471*p. 』
- *ライセンス設定に関する FAQ* 『*483*p. 』
- *デバイス情報* 『*488*p. 』

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。

Ch 1 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

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 Deployment 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* 『*288*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* 『*362*p. 』」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

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。

1. 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 *『*6*p. 』」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。

3. ［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* 『*304*p. 』」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［インターネット一時ファイル］タブの［コンピュータに一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。

1. 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。
3. [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。
4. 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。

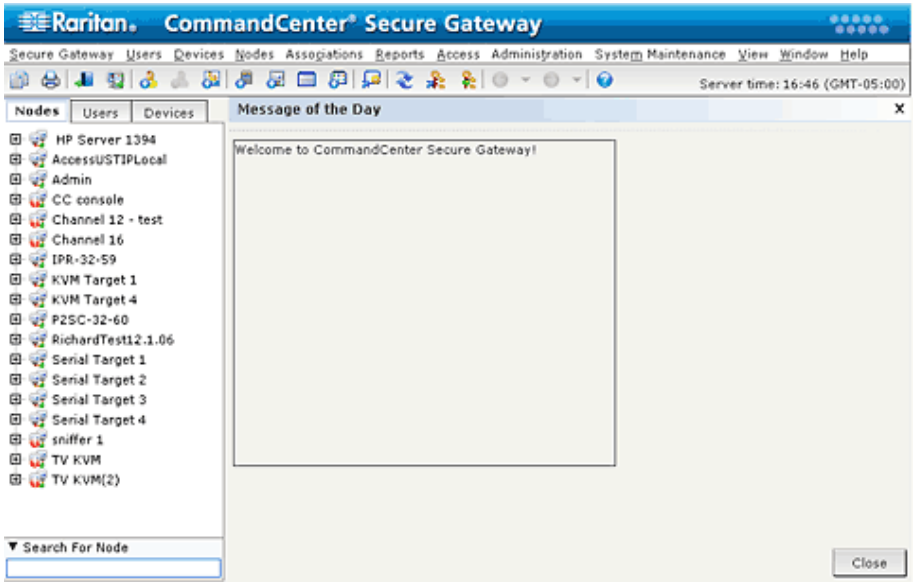
シック クライアントがインストールされたら、ご使用のクライアント コンピュータで 2 通りの方法でこのシック クライアントにアクセスできます。

▶ **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

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 『337p. 』*」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。

Ch 3 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* 『*33*p. 』」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

CC-SG 5.0 以降を使い始めるには、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*『*21*p. 』」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* 『*15*p. 』」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* 『*19*p. の"*ライセンス設定オプション – 仮想アプライアンス*"参照 』」を参照してください。

CC-SG 5.0 以降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* 『*22*p. 』」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。

未処理モード（ライセンス サーバなし）での物理アプライアンスおよび仮想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 または CC-SG 仮想マシンのホスト 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* 『*15*p. 』」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* 『*22*p. 』」を参照してください。
- CC-SG 5.3 以降の新しい仮想アプライアンス ユーザである場合は、ライセンス サーバなしで、未処理モードを使用してインストールする必要があります。「*ライセンス設定オプション - 仮想アプライアンス* 『*19*p. 』」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-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-E1-256	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
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
CC-SG128-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	▪ 未処理モード: CC-SG 仮想アプライアンス マシンのホスト ID ▪ 処理モード: 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

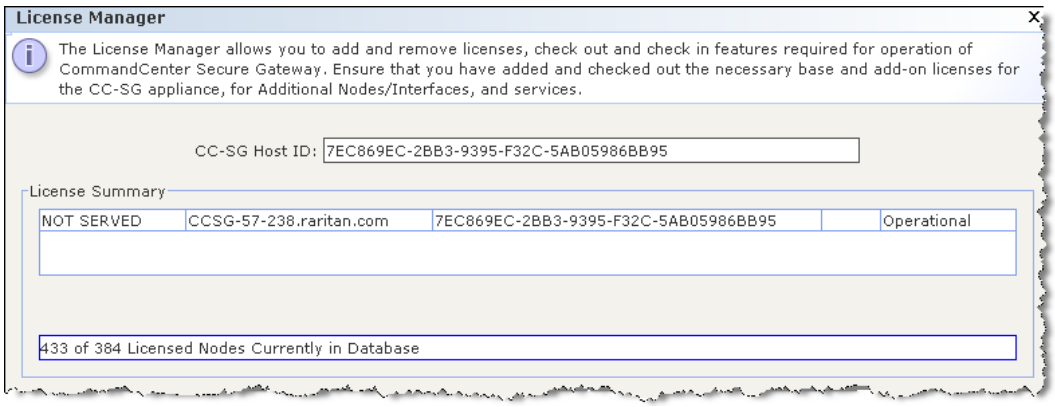
ホスト ID の検索およびデータベース内のノード数の確認

[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。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、CommandCenter Secure Gateway 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* 『*15*p. 』」を参照してください。

処理モードの仮想アプライアンスがある場合は、ライセンス サーバを使用して、Status Console からホスト ID を取得する必要があります。「*Status Console へのアクセス* 『*363*p. 』」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。
2. 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。 処理モードの仮想 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、処理モードの CC-SG と未処理モードの CC-SG で少し異なります。
3. 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。

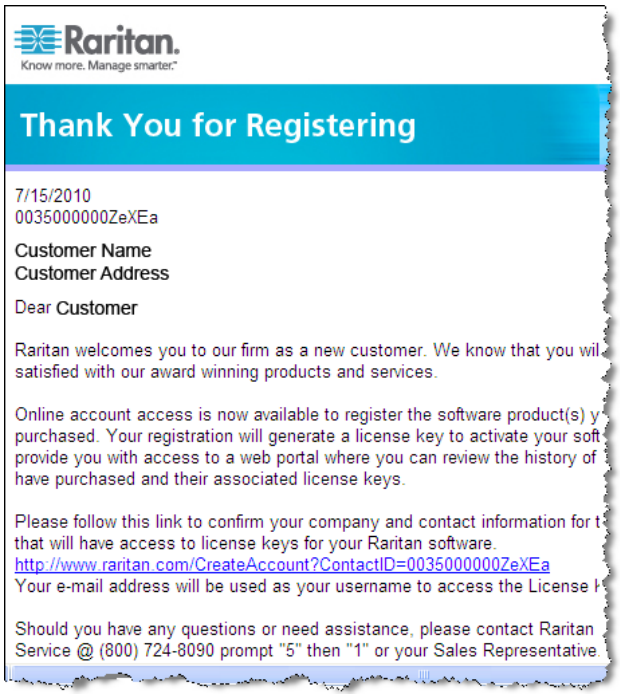


ライセンス設定 - 新規顧客 - 物理アプライアンス

CC-SG 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:

1. 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。


Raritan.
Know more. Manage smarter.

Thank You for Registering

7/15/2010
0035000000ZeXEa

Customer Name
Customer Address

Dear Customer

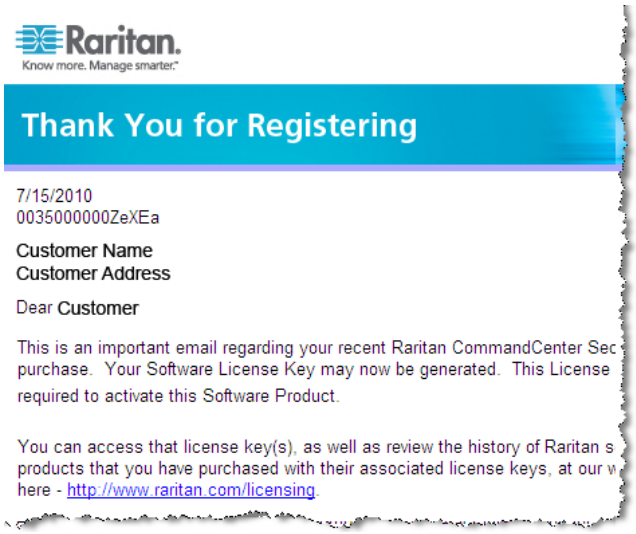
Raritan welcomes you to our firm as a new customer. We know that you wil
satisfied with our award winning products and services.

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.
http://www.raritan.com/CreateAccount?ContactID=0035000000ZeXEa
Your e-mail address will be used as your username to access the License I

Should you have any questions or need assistance, please contact Raritan
Service @ (800) 724-8090 prompt "5" then "1" or your Sales Representative.

2. 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。
3. 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。


Raritan.
Know more. Manage smarter.

Thank You for Registering

7/15/2010
0035000000ZeXEa

Customer Name
Customer Address

Dear Customer

This is an important email regarding your recent Raritan CommandCenter Sec
purchase. Your Software License Key may now be generated. This License
required to activate this Software Product.

You can access that license key(s), as well as review the history of Raritan s
products that you have purchased with their associated license keys, at our w
here - http://www.raritan.com/licensing.

4. 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。「*使用可能なライセンス『12p. 』*」を参照してください。
6. 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 『14p. 』*」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。

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 サポートに修正を依頼する必要があります。

---

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** 『21p. 』」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* 『*309*p. 』」を参照してください。

1. クラスタ化する両方の CC-SG ユニットを導入します。導入についての詳細は、『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。
2. 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* 『*14*p. 』」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* 『*15*p. 』」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* 『*310*p. 』」を参照してください。

5. 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* 『*15*p. 』」を参照してください。
6. 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* 『*15*p. 』」を参照してください。

ライセンス設定オプション - 仮想アプライアンス

CC-SG 仮想アプライアンスは、処理モードか、未処理モードで実行することができます。処理モードでは、物理マシンまたは仮想マシンのライセンス サーバを使用します。未処理モードでは、ライセンスは、仮想 CC-SG アプライアンスが実行している仮想マシンにバインドされます。未処理モードでは、ライセンス サーバは必要ありません。

新規にインストールする場合は、より単純な未処理モードを使用することをお勧めします。未処理モードを使用する場合は、CC-SG 5.3 以降が必要です。処理ライセンスを使用した以前のインストール環境は、未処理モードに変更しない限り、変更する必要はありません。設定からライセンス サーバを削除する場合は、Raritan ライセンス ポータルで新しいライセンスを再生成する必要があります。Raritan のテクニカル サポートまでお問い合わせください。

さまざまなインストール環境の詳細については、使用するライセンス モードに応じたクイック セットアップ ガイドをダウンロードしてください。

www.raritan.com を開き、「Support」>「Firmware and Documentation」>「CommandCenter Secure Gateway」をクリックします。使用する CC-SG リリースの［Quick Setup Guides］リンクをクリックし、必要なクイック セットアップ ガイドを選択します。

- CC-SG 仮想アプライアンスのクイック セットアップ ガイド - ライセンス サーバなし
- CC-SG 仮想アプライアンスおよび lmadmin ライセンス サーバ管理クイック セットアップ ガイド
- CC-SG 仮想アプライアンスおよび lmgrd ライセンス サーバ管理クイック セットアップ ガイド

注: ライセンス サーバは、2 つのライセンス サーバ マネージャ、lmgrd または lmadmin のいずれかを使用して、管理できます。Flexera の lmgrd は、ライセンス サーバ管理用のコマンドライン ユーティリティです。Flexera の lmadmin は、ライセンス サーバ管理用の GUI ベースのアプリケーションで、ライセンス サーバからリモートで、またはローカルでアクセスできます。どちらかのマネージャを選択し、それのみをインストールする必要があります。両方を使用することはできません。

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。

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導入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。
3. 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。[Interactive Tools Upgrade(対話型ツールのアップグレード)] を選択し、[OK] をクリックします。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導入したら、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 『273p. 』*」を参照してください。

手順 2: ライセンス ファイルの表示:

1. 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。ライセンス サーバを使用して、処理モードで導入された仮想アプライアンス ライセンスは、1 つの特定のライセンス サーバに関連付けられます。ライセンス サーバなしで、未処理モードで導入された仮想アプライアンス ライセンスは、CC-SG 仮想マシン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 サーバを削除して未処理モードに変更する必要がある場合、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*『*483*p. 』」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。
5. [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*** *『288*p. *』*」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。

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します。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、30 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 30 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* 『*21*p. 』」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」を参照してください。

サービスとしてのライセンス サーバ マネージャの実行

オペレーティング システムが再起動すると自動的に起動するよう、ライセンス サーバ マネージャはサービスとしてインストールすることをお勧めします。

lmadmin のインストールの詳細:

lmadmin を Windows にインストール時に、[Run as Service(サービスとして実行)] チェックボックスを選択し、この設定を許可します。lmadmin の UNIX インストールの場合は、『FlexNet Publisher License Administration Guide』の「Installing lmadmin License Server Manager as an Operating System Service」(オペレーティング システムのサービスとしての lmadmin ライセンス サーバ マネージャのインストール) で、この設定の手順を参照してください。

lmgrd のインストールの詳細:

lmgrd ライセンス サーバ マネージャは、Linux で自動的に起動するよう設定するか、Windows で自動的に開始されるサービスとして設定する必要があります。

詳細については、『Publisher License Administration Guide』を参照してください。

- UNIX プラットフォームでのライセンス サーバ マネージャの起動、自動起動
- Windows でのライセンス サーバ マネージャの起動
- Windows サービスとしてのライセンス サーバ マネージャの設定

障害後にライセンス サーバを再起動する

お使いのライセンス サーバ マネージャが、サーバが起動したときに自動的に起動するサービスとしてインストールされていない場合は、障害後にサーバを再起動する必要があります。たとえば、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。

lmgrd を使用してライセンス 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 `lmdown` 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。

lmadmin を使用してライセンス サーバを再起動するには、以下の手順に従います。

- 『FlexNet Publisher License Administration Guide』を参照してください。

ライセンス サーバ管理用の lmgrd コマンドライン ユーティリティ

lmgrd 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、″CC-SG128-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
lmborrow	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。
lmdiag	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。 `lmdiag -c <ライセンス ファイル名> <機能名> -n`
lmdown	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、`lmdown -vendor raritan` を使用します。
lmhostid	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。
lminstall	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。

コマンド	説明
lmnewlog	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。
lmpath	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。
lmremove	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、lmremove を許可なく実行できないように設定できます。
lmreread	`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。
lmswitchr	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。
lmswitch	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。
lmstat	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>
lmver	lmgrd、lmadmin、lmdown、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。

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

1. 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。
3. 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。
4. 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。

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* 『*337*p. 』」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 のファームウェア 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。
2. 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* 『*264*p. 』」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。
2. [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* 『*285*p. 』」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。
5. [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。
6. [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** 『285*p.* 』」*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* 『*34*p. 』」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* 『*34*p. 』」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* 『*36*p. 』」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* 『*39*p. 』」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* 『*486*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

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。**

1. [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)。
3. [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。
4. [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)。
   - [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 [エレメント] テーブルに追加します。
   - 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。
6. 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)**
7. 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。

サポートされているデバイスおよびそのデバイスを追加する方法の詳細については、「*IPv6 ネットワーク デバイスの検出および追加* 『*54*p. 』」を参照してください。

▶ 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 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。
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] 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。
4. [検出] をクリックします。
5. 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。
6. 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。
7. [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。
8. 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。
9. [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。
10. 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。
11. [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。

12. 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。
13. 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。
14. 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。
15. 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。
16. 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。
17. 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。
18. 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。**
19. 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。
20. [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。**

1. [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。
3. 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。

4. 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。**
6. 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。
8. 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* 『*211*p. 』」を参照してください。

9. 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。**

1. [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。
3. 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*** *『196*p. *』*」を参照してください。

4. [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。
5. [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。
7. [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。
8. 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。
9. 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。**
11. 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。
14. 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。
16. [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。

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

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
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* 『*211*p. 』」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* 『*33*p. 』」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* 『*43*p. 』」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* 『*486*p. 』」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。
4. 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* 『*486*p. 』」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『47p. 』*」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 『444p. 』*」を参照してください。

CSV ファイルにカテゴリを追加する場合

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

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。
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*『*446*p. 』」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* 『*445*p. 』」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 『103p. 』*」を参照してください。

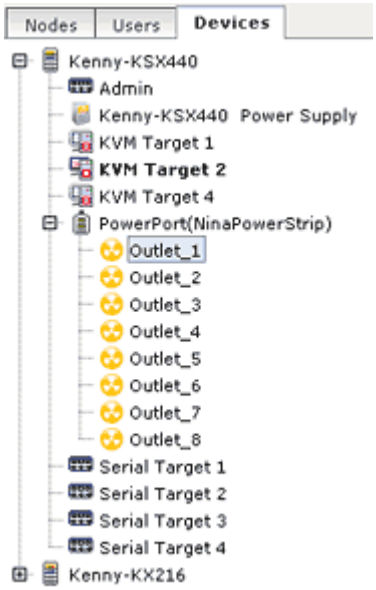
注: iLO/RILOE デバイス、IPMI デバイス、Dell DRAC デバイス、IBM RSA デバイス、またはその他の Raritan 以外のデバイスを設定する場合は、[ノードの追加] メニューを使用し、これらの項目をインタフェースとして追加します。「ノード、ノード グループ、インタフェース 『112p. 』」を参照してください。

この章の内容

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
	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
	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。
	デバイスが停止した状態
	デバイスが利用不可能
	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
	ブレード サーバが利用可能
	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。
2. 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** 『74p. 』」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 『63p. 』*」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 『42p. 』*」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 『63p. 』*」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 『62p. 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* 『*70*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* 『*208*p. 』」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* 『*53*p. 』」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。
*	0 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。

IPv6 ネットワーク デバイスの検出および追加

CC-SG リリース 5.3 以降では、IPv6 上で Dominion KX2 リリース 2.5 以降のデバイスの検出および追加を行うことができます。以前のリリースの KX2 は、IPv4 専用のデバイスとしてしか使用できません。

IPv6 は、Dominion KX1、SX、KSX、および KX-101 V2 デバイスではサポートされていません。

以前のバージョンで Dominion KX2 デバイスを追加しようとすると、警告メッセージが表示されます。

「Device firmware does not support CC-SG communicating on a IPv6 address.(デバイスのファームウェアが、IPv6 アドレスでの CC-SG との通信をサポートしていません。) You may try upgrading the device.(デバイスをアップグレードしてください。) Do you wish to continue adding the device?(デバイスの追加を続行しますか?) If so device will be managed only on IPv4 address.(続行する場合、デバイスは IPv4 アドレスのみで管理されます。)」

CC-SG 管理下で IPv6 を使用して動作するように KX2 デバイスをリリース 2.5 にアップグレードする必要があります。

CSV ファイルのインポートによってデバイスを追加すると、メッセージ中のすべての情報が監査証跡レポートに記録されます。「*インポートに関する監査証跡エントリ* 『*445*p. 』」を参照してください。

IPv6 で受信するように DNS サーバを設定

CC-SG では、ホスト名を使用してデバイスが追加されるときに DNS が使用されます。

DNS 用に設定されたアドレスと同じアドレスで DNS サーバが受信していることを確認します。DNS は、[管理] > [設定] の [ネットワーク設定] タブで設定されます。「*CC-SG ネットワークの設定* 『*288*p. 』」を参照してください。

詳細については、http://technet.microsoft.com/en-us/library/cc783049(ws.10).aspx を参照してください。次の手順は、Windows DNS サーバの例です。CC-SG は DNS の IPv6 アドレスで設定されます。

IPv6 で受信するように DNS サーバを設定するには:

1. Windows サポート ツールをインストールします。
2. コマンド プロンプトを開きます。
3. コマンド「dnscmd /config /EnableIPv6 1」を入力します。
4. DNS サーバ サービスを再起動します。

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。

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。
2. [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。[From(開始)] フィールドと [To(終了)] フィールドには、ローカル サブネットまたはローカル リンクの IP 範囲があらかじめ設定されています。

注: 場合によっては、あらかじめ設定された範囲が非常に広いことがあります。フィールドを編集するか、または、検出開始後は、[停止] をクリックして検索を停止することができます。

IP 分離モードで動作している場合、ブロードキャスト/マルチキャストは、eth0 と eth1 の両方のインタフェースに適用されます。指定したアドレス範囲を使用して、検出されたデバイスの表示がフィルタされます。

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] チェックボックスを選択します。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。
4. 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。デュアル スタック モードで動作している場合、リストには、検出された各デバイスのホスト名、IPv6 アドレス、および IPv4 アドレスが表示されます。
7. 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* 『*57*p. 』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* 『*59*p. 』」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* 『*59*p. 』」を参照してください。
9. [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* 『*55*p. 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* 『*103*p. 』」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。
2. [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* 『*57*p. 』」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* 『*59*p. 』」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* 『*59*p. 』」を参照してください。

KVM またはシリアル デバイスの追加

一部の 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。

1. 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* 『*486*p. 』」を参照してください。
2. 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* 『*2*p. 』」を参照してください。

*注: IPv6 は、一部のデバイスでサポートされています。「*IPv6 ネットワーク デバイスの検出および追加 *『54p. 』」を参照してください。*

3. 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。
4. 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。
5. 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。
6. 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。
7. 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。**
9. 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* 『*42*p. 』」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。
12. 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* 『*42*p. 』」を参照してください。
13. 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。
14. 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* 『*90*p. 』」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* 『*103*p. 』」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* 『*59*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* 『*103*p. 』」を参照してください。

1. ［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* 『*486*p. 』」を参照してください。
2. ［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* 『*2*p. 』」を参照してください。

3. 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。
4. 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** *『61p. 』」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。
7. ［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*** *『42p. 』」を参照してください。*
8. 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。

ホスト名でデバイスを追加

ホスト名でデバイスを追加するには、デバイス、CC-SG、およびクライアントがすべて同じドメイン内になければなりません。それらの一部が同じドメイン内にない場合は、すべての権限のあるドメイン名（FQDN）を使用してデバイスを追加します。これにより、インタフェースの起動時に CC-SG で FQDN が設定されます。

デュアル スタックの追加によってホスト名でデバイスを有効にしたときに、ホスト名の解決で IPv4 と IPv6 のどちらのアドレスも返されない場合は、そのデバイスを IP アドレスで追加する必要があります。その際は、ホスト名をどちらのアドレスにも解決できなかったことを警告するメッセージが表示されます。

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 プロファイルに加えた変更は、監査証跡に記録されます。記録される内容には、デバイス名、デバイス IP/ホスト名、検出ポート、HTTP ポート、HTTPS ポート、サブネット マスク、デフォルトのゲートウェイ、デバイスの直接アクセスを許可、ハートビート、関連付け、場所などがあります。「*監査証跡レポート 『251*p. 』」を参照してください。

▶ **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。
   - デバイスがデュアル スタック モードで動作している場合は、IPv6 アドレス、プレフィックス長、および IPv6 のデフォルトのゲートウェイを編集できます。
   - デバイスが DHCP で動作している場合、IPv4 アドレスを設定すると、IPv4 アドレスは静的 IP アドレスとして設定されます。
   - デバイスがルータ検出で動作している場合、IPv6 アドレスを設定すると、IPv6 アドレスは静的 IP アドレスとして設定されます。
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。
2. 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。
5. 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。

1. [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。

1. [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。

IPv6 対応の KX II デバイスの証明書

CC-SG により管理され、IP アドレスに基づいて CC-SG に追加された IPv6 対応の KX2 デバイスで証明書エラーを回避するには、証明書内の CN の先行ゼロ抑制の値が [] で囲まれていることを確認します。

CC-SG により管理されている KX II とやり取りする場合は、jar のダウンロード用の URL に「先行ゼロ抑制のホスト」が設定されます。つまり、証明書には、CN として [] で囲まれた先行ゼロ抑制の値が必要であるということです。

また、KX II デバイスに CN としてホスト名を使用することもできます。あるいは、証明書署名リクエスト (CSR) にサブジェクトの別名 (SAN) を使用し、外部の証明機関で署名された CSR を取得して、その証明書を KX II にアップロードできます。

▶ **例:**

- 正しい CN:

[fd00:c:d:2400:0:2:3:4]

- 正しくない CN:

[fd00:c:d:2400::2:3:4]

- 正しくない CN:

[fd00:000c:000d:2400:0000:0002:0003:0004]

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 『66p. 』*」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。
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。
4. ［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* 『*486*p. 』」を参照してください。
5. 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。
6. ［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。
4. 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* 『*486*p. 』」を参照してください。
5. 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。
6. ［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* 『*486*p. 』」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。
3. [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。
6. [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。**

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。[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* 『*68*p. 』」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* 『*70*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

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* 『*68*p. 』」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。

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 『57p. 』*」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** *『70p. 』」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。

1. 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 『57p. 』*」を参照してください。
3. 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** *『70p. 』」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。**

1. ［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。**

1. ［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。**

1. ［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。**

1. [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。
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。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。
5. 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。**

1. [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。**

1. [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 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。**

1. [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。
4. [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。
5. 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。

1. [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。
3. 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。
4. [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。

1. 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* 『*73*p. 』」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* 『*68*p. 』」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。
2. 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* 『*65*p. 』」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

一括コピー 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。

1. [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。
3. [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。
4. [>] 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* 『*85*p. 』」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。

1. 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。
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* 『*57*p. 』」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。

1. [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。

1. [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。

1. [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* 『*211*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* 『*212*p. 』」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* 『*42*p. 』」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* 『*190*p. 』」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。

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。
2. ツールバーの [新しいグループ] アイコン 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。
3. [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* 『*486*p. 』」を参照してください。
4. 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。

1. [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。
2. [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。
3. 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。

1. [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  をクリックして行をテーブルに追加します。
3. 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。
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。
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  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。

6. [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。

7. [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。
8. 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。

一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。
2. 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。**

4. [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* 『*80*p. 』」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。
2. 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。
- IPv6 対応の KX2 デバイスを追加する場合、サポートに関する詳細については、「*IPv6 ネットワーク デバイスの検出および追加* 『*54*p. 』」を参照してください。
- 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* 『*90*p. 』」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* 『*444*p. 』」を参照してください。

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
1	ADD	すべてのタグの最初の列はコマンドです。
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。インポー

列番号	タグまたは値	詳細
		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。 サポートされているデバイスの IPv4 または IPv6 アドレス。
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、デフォルトは 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です。
2	DEVICE-BLADE	左記のとおりにタグを入力します。

列番号	タグまたは値	詳細
		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。
7	ノード名	この KVM スイッチ ポートの設定

列番号	タグまたは値	詳細
		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です。
2	DEVICE-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	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。

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*『*446*p. 』」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* 『*445*p. 』」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。

1. [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。
2. [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。
3. [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。
6. 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『95*p. 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:

1. [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。
2. [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。**

1. [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。
2. [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 デバイスへリストアするには、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。
2. [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。
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 デバイスへリストアするには、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。
2. [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。
5. 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。**

1. [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。
2. [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。
2. [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。
2. [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。
2. [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. [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。
2. [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。
4. [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。
2. [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。
4. [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。

デバイスがデュアル スタック モードで動作している場合は、各アドレスに対して順番に ping が実行され、アドレスごとに結果が表示されます。デバイスがホスト名で管理されている場合は、ping の結果にホスト名が表示されます。

▶ **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。

2. [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* 『*339*p. 』」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。

デュアル スタック デバイスの管理を再開する場合は、デバイスが管理対象外になっている間にデュアル スタックが有効または無効にされている可能性があります。CC-SG では、管理対象の他のデバイスと IPv6 アドレスが競合していないかを確認する必要があります。競合が検出された場合、そのデバイスは、IPv4 アドレスのみを使用して管理下に置かれ、エラーがログに記録されます。

エラーには、「An IPv6 address conflict was detected.(IPv6 アドレスの競合が検出されました。)Device management resumed with IPv4 address only.(デバイス管理は IPv4 アドレスのみで再開されます。)」というメッセージが含まれます。

▶ 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。**

1. [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 『339p. 』*」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。
2. [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。
3. [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。
5. 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。
3. [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。

1. [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。
2. [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。
2. [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。

Ch 7 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。

1. 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* 『*105*p. 』」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。
3. 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* 『*408*p. 』」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*『*148*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* 『*408*p. 』」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** *『103p. 』」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。

1. 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。
2. 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* 『*106*p. 』
   - *SX 3.0 および KSX に接続された電源タップの設定* 『*107*p. 』
   - *SX 3.1 に接続された電源タップの設定* 『*109*p. 』
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* 『*111*p. 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。
4. 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* 『*148*p. 』」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* 『*106*p. 』
- *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* 『*106*p. 』
- *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* 『*107*p. 』

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。

1. 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***『*111*p. 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***『*148*p. 』」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* 『*107*p. 』
- *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* 『*108*p. 』
- *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*p. 』

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

1. 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* 『*57*p. 』」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。
3. ［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。
4. 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。
7. ［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。**
9. 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***『*111*p. 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。**
10. 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***『*42*p. 』」を参照してください。**オプション。**
11. 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。

1. 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***『*111*p. 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***『*148*p. 』」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。
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* 『109p. 』
- *SX 3.1 の電源タップの別のポートへの移動* 『110p. 』
- *SX 3.1 デバイスに接続された電源タップの削除* 『110p. 』

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:

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* 『57p. 』」を参照してください。
2. CC-SG 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* 『57p. 』」を参照してください。
2. SX 3.1 デバイスのポートの設定。「*ポートの設定* 『64p. 』」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。

1. 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『111*p. 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『148*p. *』*」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『110*p. *』*」および「*SX 3.1 デバイスに接続された電源タップの追加 『109*p. *』*」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* 『*148*p. 』」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。

Ch 8 ノード、ノード グループ、インタフェース

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* 『*486*p. 』」を参照してください。

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* 『*300*p. 』」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ッ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* 『*216*p. 』」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* 『*42*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。

「*ノード プロファイルへの場所と連絡先の追加* 『*123*p. 』」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* 『*123*p. 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。

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* 『*197*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。
	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。**

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。**

1. ［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. ［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。
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。**

1. ［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。

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。**

1. [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。
3. [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。**

1. [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* 『*138*p. 』」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* 『*193*p. 』」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。**

1. [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。
3. [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* 『*486*p. 』」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。**
5. 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* 『*138*p. の *"インタフェースの追加"*参照 』」を参照してください。
6. [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* 『*42*p. 』」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* 『*42*p. 』」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* 『*486*p. 』」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** 『72p. 』」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。

4. [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。

1. [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。

1. [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。

▶ 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 の 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 の 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 255 文字です。IPv6 がサポートされています。
4. 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。
8. 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。**
10. 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 255 文字です。IPv6 がサポートされています。
6. 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。
7. 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。

10. 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。
13. [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** 『122p. 』」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。
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. 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。
5. 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*** *『125*p. *』*」および「***仮想マシンを持つ仮想ホストの追加*** *『128*p. *』*」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。
8. 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** 『154p. 』」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* 『*133*p. 』」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* 『*122*p. 』」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* 『*131*p. 』」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。**

1. 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* 『*131*p. 』」を参照してください。
2. 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* 『*132*p. 』」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 CC-SG 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。**

1. ［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。
2. 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。

1. 古いプラグインを削除したら、CC-SG 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。

VCenter の必要最小限の許可

CC-SG から VCenter にアクセスしてノードおよびノードに関連付けられているインタフェースを管理できるように、VCenter アプリケーションで最小限の許可をいくつか設定する必要があります。

vSphere 4.1/5.0 で最小限の許可を設定するには、以下の手順に従います。

- [ホスト] > [設定] > [System Management(システム管理)]
- [ホスト] > [設定] > [メンテナンス]
- [仮想マシン] > [Interaction(操作)] > [電源投入]
- [仮想マシン] > [Interaction(操作)] > [電源切断]
- [仮想マシン] > [Interaction(操作)] > [中断]
- [仮想マシン] > [Interaction(操作)] > [リセット]
- [仮想マシン] > [Interaction(操作)] > [Console Interaction(コンソール操作)]
- [タスク] > [Create(作成)]
- [Scheduled Task(スケジュールされたタスク)] > [Create Tasks(タスクの作成)]
- [Scheduled Task(スケジュールされたタスク)] > [Run Task(タスクの実行)]

さらに、VMware リモート コンソールからメディアやネットワーク デバイスに対する接続/切断ができるように、[仮想マシン] > [Interaction(操作)] > [Device Connection(デバイス接続)] で設定を行う必要があります。

VCenter が追加されていない場合は VMware リモート コンソール プラグインを手動でインストール

CC-SG に VCenter が含まれている場合は、VMware リモート コンソール プラグインを自動的にダウンロードするプロンプトが表示され、プラグインが VCenter から取得されます。

このときに、「Failed to run vmware remote console plugin.(vmware リモート コンソール プラグインの実行に失敗しました。)Either the browser is not supported or you have a previous version of the console installed.(ブラウザがサポートされていないか、旧バージョンのコンソールがインストールされています。)」というエラー メッセージが表示されることがあります。

VCenter が追加されておらず、ホストしか追加されていない場合、プラグインのプロンプトは表示されません。その場合は、Web から手動でプラグインをダウンロードする必要があります。

プラグインのファイル名は「vmware-vmrc-win32 x86.exe」です。64 ビット OS の場合は、異なるプラグイン ファイルをダウンロードする必要があります。

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。
2. 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。

1. 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。

1. 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。
2. [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。
2. [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

IPv6 は、一部のインタフェース タイプでサポートされています。「*IPv6 を使用したノードのインタフェースの追加* 『*154*p. 』」を参照してください。

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 『124*p. 』」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。**

1. 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 『141*p. の*″インバンド接続のインタフェース – RDP、VNC、SSH、RSA KVM、iLO Processor KVM、DRAC KVM、TELNET″*参照 *』*」を参照してください。
- インバンド – UCS KVM: Cisco Integrated Management Controller (CIMC) を使用して、Cisco UCS シャーシのブレードに対して KVM 接続を作成するには、このアイテムを選択します。

  「*Cisco UCS KVM 接続のインタフェース 『145*p. *』*」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 『144*p. *』*」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* 『*146*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 『*147*p. 』

  Power IQ Proxy のパワー制御接続のインタフェース 『*149*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* 『*148*p. 』」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* 『*151*p. 』」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* 『*486*p. 』」を参照してください。

インバンド接続のインタフェース - RDP、VNC、SSH、RSA KVM、iLO Processor KVM、DRAC KVM、TELNET

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。

Microsoft RDP、SSH、Telnet、VNC、DRAC (iDRAC6 のみ) の各インタフェースは、IPv6 アドレスをサポートしています。Java RDP、RSA KVM、iLO Processor KVM の各インタフェースは、IPv6 アドレスをサポートしていません。「*IPv6 を使用したノードのインタフェースの追加* 『*154*p. 』」を参照してください。

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。**
3. 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。

DRAC 5 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、DRAC 証明書の署名に使用された CA の証明書を、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。

また、DRAC5 .jnlp ファイルへのアクセスを許可するには、Internet Explorer ダウンロードの情報バーも無効にする必要があります。

Internet Explorer のダウンロードの情報バーを無効にするには、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. [セキュリティ] タブで [インターネット ゾーン] を選択します。
3. [レベルのカスタマイズ] をクリックします。[ダウンロード] まで下にスクロールします。
4. [ファイルのダウンロード時に自動的にダイアログを表示] で [有効] をクリックします。
5. [OK] をクリックします。[インターネット オプション] ダイアログに戻ります。
6. [セキュリティ] タブで [インターネット ゾーン] を選択します。
7. [レベルのカスタマイズ] をクリックします。[ダウンロード] まで下にスクロールします。
8. [ファイルのダウンロード時に自動的にダイアログを表示] で [有効] をクリックします。
9. [OK] をクリックします。

Internet Explorer 9 で DRAC インタフェースを接続するには、以下の手順に従います。

1. Internet Explorer 9 で [ツール] メニュー > [オプション] をクリックします。
2. [プライバシー] タブで、スライダを [低] に設定して、クッキーが DRAC インタフェースにアクセスできるようにします。
3. [Do you want to open or save vkvm.jnlp(vkvm.jnlp を開くか、または保存しますか?)] プロンプトで [開く] をクリックし、DRAC インタフェースを起動します。

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 『300*p. 』」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=469eee3a-45b4-4b40-b695-b678646a728b&displaylang=en
- Windows 7 に RDP インタフェースを追加する場合は、 ICMPv4 と ICMPv6 が Windows 7 のファイアウォールで許可されていることを確認します。

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 『300*p. 』」を参照してください。
- Windows 7 に RDP インタフェースを追加する場合は、 ICMPv4 と ICMPv6 が Windows 7 のファイアウォールで許可されていることを確認します。

VNC 接続の詳細

IPv6 のサポート:

すべての VNC バージョンが IPv6 をサポートしているわけではありません。

RealVNC は、IPv6 をサポートしています。RealVNC サーバ設定で [Prefer On(オンを選択)] を選択しなければ、IPv6 および VNC は CC-SG と連動しません。

TightVNC クライアントは、サーバ設定が [Prefer On(オンを選択)] に変更された場合、CC-SG と連動します。

RealVNC の無償版は、IPv6 をサポートしていません。

RealVNC の Personal Edition は、IPv6 をサポートしていますが、30 日間の試用版なので、ライセンスを購入する必要があります。

ライセンスを購入すると、RealVNC の Enterprise Edition は IPv6 をサポートします。

Windows 7 への VNC 接続:

Windows 7 用の VNC インタフェースを追加する場合は、ICMPv4 と ICMPv6 が Windows 7 のファイアウォールで許可されていることを確認します。

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

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。

1. 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 『286p. 』*」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 『303p. 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。

3. 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。

Cisco UCS KVM 接続のインタフェース

UCS-KVM 接続は、Cisco Integrated Management Controller (CIMC) を使用し、Cisco UCS シャーシのブレードに KVM アクセス権を与えます。

▶ **Cisco UCS KVM 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. インタフェース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* 『*486*p. 』」を参照してください。
2. [Chassis IP/Hostname(シャーシ IP/ホスト名)] フィールドに、Cisco UCS の IP アドレスかホスト名を入力します。
3. 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。デフォルトのポートは 443 です。
4. [Blade IP/Hostname(ブレード IP/ホスト名)] フィールドに、ブレードの IP アドレスかホスト名を入力します。
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。シャーシとブレードの両方にアクセス権を持つアカウントのユーザ名とパスワードを指定してください。
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。

Cisco UCS の詳細

Cisco UCS 5100 シリーズのブレード サーバ シャーシとそのコンポーネントは、Cisco Unified Computing System (UCS) の一部です。設定が終了すると、CC-SG ユーザは、ブレードの Cisco Integrated Management Controller (CIMC) を介して KVM および IPMI 機能にアクセスできます。

▶ **Cisco UCS のブレードにパワー制御を追加するには、以下の手順に従います。**

ノードに IPMI パワー制御インタフェースを追加します。「*IPMI パワー制御接続のインタフェース* 『*148*p. 』」を参照してください。

▶ **Cisco UCS のブレードに Serial Over LAN (SOL) アクセスを追加するには、以下の手順に従います。**

ノードに SSH インタフェースを追加します。「*インバンド接続のインタフェース – RDP、VNC、SSH、RSA KVM、iLO Processor KVM、DRAC KVM、TELNET* 『*141*p. 』」を参照してください。

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。
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。**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

IPv6 は、iLO や RSA への接続ではサポートされていません。

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。CC-SG 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。
2. 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。
3. 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。**
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。

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* 『*148*p. 』」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。

1. 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* 『*184*p. 』」を参照してください。

2. [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* 『*409*p. 』」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* 『*153*p. 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 インタフェースは、IPv6 アドレスをサポートしています。「*IPv6 を使用したノードのインタフェースの追加* 『*154*p. 』」を参照してください。

▶ 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。

1. 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* 『*486*p. 』」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。**
3. [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 255 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
   - http(s)://[fd07:2fa:6cff:2500:20f:3dff:fef6:fa1e]/index.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。

---

5. [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*** *『152*p. *』*」を参照してください。
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。

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。
2. 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。**

1. [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。
4. 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* 『*138*p. 』」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。

IPv6 を使用したノードのインタフェースの追加

CC-SG は、次のインタフェース タイプで IPv6 を使用したノードへのアクセスをサポートしています。

- Microsoft RDP
- SSH
- Telnet
- VNC
- Web
- DRAC (iDRAC6 のみ)

CC-SG では、他のインタフェース タイプ向けに設定された IPv6 ネットワーク IP アドレスは無効な送信先と見なされます。

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

1. [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。
2. [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

1. [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。
2. [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。
2. 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*『*258*p. 』」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*『*155*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

一括コピー 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。
3. [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。
4. [>] 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。
2. 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、更新、および削除

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、更新、および削除できます。

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。

同じ CSV ファイルのインポートで、ノードとインタフェースを追加、更新、および削除できます。

ノードの CSV ファイルの要件の追加

The nodes CSV file defines the nodes, interfaces, and their details required to add them to CC-SG.

- Node names must be unique. If you enter duplicate node names, CC-SG adds a number in parentheses to the name to make it unique, and then adds the node. If you are also assigning categories and elements to nodes in the CSV file, and you have duplicate node names, categories and elements may be assigned to the wrong nodes. To prevent this, give each node a unique name. Or, import nodes first, check their names in CC-SG, and then import a separate file to assign categories and elements to the correct node names.
- To add out-of band interfaces, the associated port must not be configured in CC-SG.
- You cannot import virtual infrastructure nodes and interfaces. Use the options in Nodes > Virtualization.
- The first interface in the CSV file after the ADD NODE command is assigned as the node's default interface.
- 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* 『*184*p. 』」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* 『*444*p. 』」を参照してください。
- 一部のインタフェースは、IPv6 をサポートしています。「*インバンド接続のインタフェース - RDP、VNC、SSH、RSA KVM、iLO Processor KVM、DRAC KVM、TELNET* 『*141*p. 』」および「*Web ブラウザ インタフェース* 『*151*p. の"*Web ブラウザ インタフェース*"参照 』」を参照してください。詳細については、「*Microsoft RDP 接続の詳細* 『*143*p. 』」、「*Java RDP 接続の詳細* 『*143*p. 』」、「*VNC 接続の詳細* 『*144*p. 』」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。

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

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です。
2	NODE-OOBKVM-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	[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 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です。

列番号	タグまたは値	詳細
2	NODE-OOBSERIAL-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	[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-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	SSH の場合、デフォルトは 22 です。

列番号	タグまたは値	詳細
		TELNET の場合、デフォルトは 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です。
2	DRAC KVM インタフェースの場合は NODE-DRAC-KVM-INTERFACE DRAC パワー インタフェースの場合は NODE-DRAC-POWER-INTERFACE 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-INTERFACE Integrity ILO2 パワー インタフェースの場合は NODE-INT-ILO2-POWER-INTERFACE RSA パワー インタフェースの場合は NODE-RSA-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	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

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 UCS KVM インタフェースを追加する場合

シャーシとブレードの両方にアクセス権を持つアカウントのユーザ名とパスワードを指定してください。

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です。
2	NODE-UCS-KVM-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	UCS シャーシ 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 443 です。
7	ブレードの IP アドレスまたはホスト名	
8	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。

列番号	タグまたは値	詳細
9	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。
10	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。
11	説明	オプション。

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です。
2	NODE-RSA-KVM-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 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です。

列番号	タグまたは値	詳細
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。

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

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。

列番号	タグまたは値	詳細
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 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。
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 インタフェースの追加のヒント* 『*152*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 インタフェースの追加のヒント* 『*152*p. 』」を参照してください。

列番号	タグまたは値	詳細
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* 『*408*p. 』」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-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	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* 『*184*p. 』」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。

列番号	タグまたは値	詳細
		「*Power IQ サービスの設定* 『*409*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。

カテゴリとエレメントでサポートされているのは、ADD コマンドだけです。CSV インポートを使用し、カテゴリとエレメントを更新、または削除できません。

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 ファイルの要件の更新

CSV ファイルを使用してノードとインタフェースを更新する場合、ファイル内で UPDATE コマンドを使用し、すべての名前変更について、古い名前と新しい名前を定義する必要があります。

CC-SG は、CSV ファイルの各行を順番に処理します。名前を変更した後、古い名前は存在しなくなり、ノードは新しい名前でのみ検索されます。

CSV ファイルに名前変更を含める場合、ファイル内で名前を変更した後のすべての行において、ノードを参照する際には新しいノード名を使用する必要があります。たとえば、1 行目でノードの名前を変更し、2 行目でノードのインタフェースのいずれかを更新する場合、2 行目では新しい名前を使用してノードを識別する必要があります。

- ノードには、固有の名前が必要です。CSV ファイルに含まれる新しい名前が重複している場合は、検証中に警告メッセージが表示されます。ファイルをインポートする前に、重複名を修正する必要があります。
- インタフェース名を更新せずにインタフェースの詳細を更新するには、CSV ファイル内の「インタフェース名」および「新しいインタフェース名」の両方の列に、現在のインタフェース名を入力します。
- カテゴリとエレメントは更新できません。
- アウト オブ バンド KVM またはシリアル インタフェースに対する、アクセス アプリケーションの選択は更新できません。
- 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更新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。
- Power IQ Proxy パワー制御インタフェースは更新できません。Power IQ の同期を使用します。「*Power IQ および CC-SG の同期* 『*412*p. 』」を参照してください。
- 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* 『*184*p. 』」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* 『*444*p. 』」を参照してください。

CSV によるノード名の更新

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

列番号	タグまたは値	詳細
		ません。
3	ノード名	必須フィールド。 現在のノード名。
4	新規ノード名	必須フィールド。 新しいノード名。 CSV ファイル内の他の行でこのノードを参照する場合は、新しい名前を使用します。
5	説明	オプション。

CSV によるアウト オブ バンド KVM またはシリアル インタフェースの更新

列番号	タグまたは値	詳細
1	UPDATE	すべてのタグの最初の列はコマンドです。
2	NODE-OOBKVM-INTERFACE (アウト オブ バンド KVM インタフェースの場合)、NODE-OOBSERIAL-INTERFACE (アウト オブ バンド シリアル インタフェースの場合)	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。 このインタフェースが属するノード。
4	インタフェース名	必須フィールド。 現在のインタフェース名。
5	新しいインタフェース名	必須フィールド。 新しいインタフェース名。
6	説明	オプションのフィールド。

CSV による RDP インタフェースの更新

列番号	タグまたは値	詳細
1	UPDATE	すべてのタグの最初の列はコマンドです。
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。 このインタフェースが属するノード。
4	インタフェース名	必須フィールド。 現在のインタフェース名。
5	新しいインタフェース名	必須フィールド。 新しいインタフェース名。
6	IP アドレス/ホスト名	
7	TCP ポート	デフォルトは 3389 です。
8	サービス アカウント名	オプション。
9	ユーザ名	オプション。
10	パスワード	オプション。
11	ユーザ タイプ	REMOTE または CONSOLE デフォルトは REMOTE です。
12	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。
13	説明	オプション。
14	RDP タイプ	Java または Microsoft デフォルトは Java です。

CSV による SSH または Telnet インタフェースの更新

列番号	タグまたは値	詳細
1	UPDATE	すべてのタグの最初の列はコマンドです。
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-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	新しいインタフェース名	必須フィールド。
6	IP アドレスまたはホスト名	必須フィールド。
7	TCP ポート	SSH の場合、デフォルトは 22 です。 TELNET の場合、デフォルトは 23 です。
8	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。 新しいサービス アカウント名を入力し、更新します。
9	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。 新しいユーザ名を入力し、更新します。
10	パスワード	オプション。 新しいパスワードを入力し、更新します。
11	説明	オプション。

CSV による VNC インタフェースの更新

列番号	タグまたは値	詳細
1	UPDATE	すべてのタグの最初の列はコマンドです。
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	新しいインタフェース名	必須フィールド。
6	IP アドレスまたはホスト名	必須フィールド。
7	TCP ポート	デフォルトは 5900 です。
8	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。 新しいサービス アカウント名を入力し、更新します。
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。 新しいパスワードを入力し、更新します。
10	説明	オプション。

CSV による Web ブラウザ インタフェースの更新

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

列番号	タグまたは値	詳細
5	新しいインタフェース名	必須フィールド。
6	URL	必須フィールド。
7	TCP ポート	デフォルトは 80 です。
8	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。 新しいサービス アカウント名を入力し、更新します。
9	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。 新しいユーザ名を入力し、更新します。
10	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。 新しいパスワードを入力し、更新します。
11	ユーザ名フィールド	オプション。「*Web ブラウザ インタフェースの追加のヒント* 『*152*p. 』」を参照してください。
12	パスワード フィールド	オプション。「*Web ブラウザ インタフェースの追加のヒント* 『*152*p. 』」を参照してください。
13	説明	オプション。

CSV による DRAC KVM、DRAC Power、iLO KVM、iLO Power、Integrity iLO2 Power、または RSA パワー インタフェースの更新

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	`UPDATE`	すべてのタグの最初の列はコマンドです。
2	DRAC KVM インタフェースの場合は `NODE-DRAC-KVM-INTERFAC`	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

列番号	タグまたは値	詳細
	E DRAC パワー インタフェースの場合は NODE-DRAC-POWER-INTERFACE 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-INTERFACE Integrity ILO2 パワー インタフェースの場合は NODE-INT-ILO2-POWER-INTERFACE RSA パワー インタフェースの場合は NODE-RSA-POWER-INTERFACE	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。 現在のインタフェース名。
5	新しいインタフェース名	必須フィールド。新しいインタフェース名。
6	IP アドレスまたはホスト名	必須フィールド。
7	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合は空白のままにします。 新しいサービス アカウント名を入力し、更新します。
8	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。 新しいユーザ名を入力し、更新しま

列番号	タグまたは値	詳細
		す。
9	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。 新しいパスワードを入力し、更新します。
10	説明	オプション。
11*	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 による RSA KVM インタフェースの更新

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	UPDATE	すべてのタグの最初の列はコマンドです。
2	NODE-RSA-KVM-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。 現在のインタフェース名。
5	新しいインタフェース名	必須フィールド。 新しいインタフェース名。
6	IP アドレスまたはホスト名	必須フィールド。
7	TCP ポート	デフォルトは 2000 です。

列番号	タグまたは値	詳細
8	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。 新しいサービス アカウント名を入力し、更新します。
9	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。 新しいユーザ名を入力し、更新します。
10	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。 新しいパスワードを入力し、更新します。
11	説明	オプション。

CSV による IPMI インタフェースの更新

列番号	タグまたは値	詳細
1	UPDATE	すべてのタグの最初の列はコマンドです。
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。 現在のインタフェース名。
5	新しいインタフェース名	必須フィールド。 新しいインタフェース名。
6	IP アドレスまたはホスト名	必須フィールド。
7	UDP ポート	デフォルトは 623 です。
8	認証	MD5、None、OEM、または PASSWORD デフォルトは PASSWORD です。
9	間隔	確認する頻度を秒単位で入力します。

列番号	タグまたは値	詳細
		デフォルトは 550 です。
10	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。 新しいサービス アカウント名を入力し、更新します。
11	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。 新しいユーザ名を入力し、更新します。
12	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。 新しいパスワードを入力し、更新します。
13	説明	オプション。

CSV による UCS KVM インタフェースの更新

シャーシとブレードの両方にアクセス権を持つアカウントのユーザ名とパスワードを指定してください。

列番号	タグまたは値	詳細
1	UPDATE	すべてのタグの最初の列はコマンドです。
2	NODE-UCS-KVM-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。 現在のインタフェース名。
5	新しいインタフェース名	必須フィールド。 新しいインタフェース名。
6	シャーシの IP アドレスまたはホスト名	必須フィールド。
7	TCP ポート	デフォルトは 443 です。

シャーシとブレードの両方にアクセス権を持つアカウントのユーザ名とパスワードを指定してください。

列番号	タグまたは値	詳細
8	ブレードの IP アドレスまたはホスト名	必須フィールド。
9	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。 新しいサービス アカウント名を入力し、更新します。
10	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。 新しいユーザ名を入力し、更新します。
11	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。 新しいパスワードを入力し、更新します。
12	説明	オプション。

ノードの CSV ファイルの要件の削除

CSV ファイルを使用してインタフェースを削除する場合、ノードに少なくとも 1 つのインタフェースが必要です。インタフェースがなければ、削除操作は失敗します。

ノードのカテゴリまたはエレメントは削除できません。

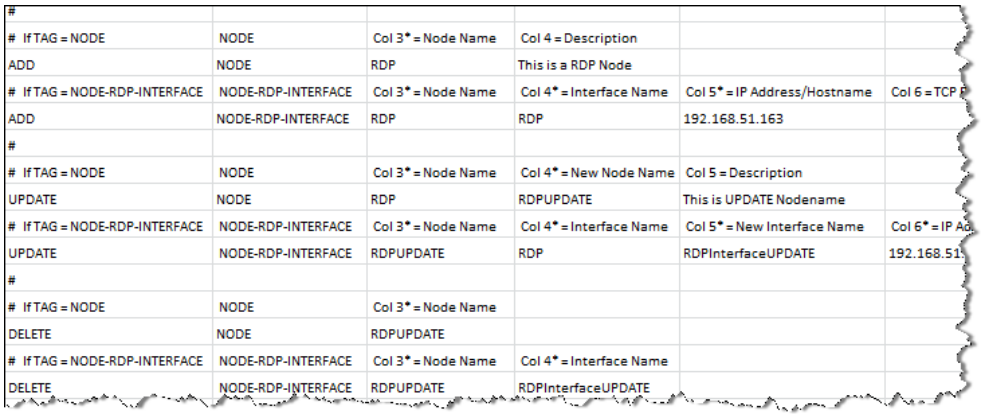
CSV によるノードの削除

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

CSV によるインタフェースの削除

列番号	タグまたは値	詳細
1	DELETE	すべてのタグの最初の列はコマンドです。
2	NODE-OOBKVM-INTERFACE NODE-OOBSERIAL-INTERFACE NODE-RDP-INTERFACE NODE-SSH-INTERFACE NODE-TELNET-INTERFACE NODE-VNC-INTERFACE NODE-WEB-INTERFACE NODE-DRAC-KVM-INTERFACE NODE-DRAC-POWER-INTERFACE NODE-ILO-KVM-INTERFACE NODE-ILO-POWER-INTERFACE NODE-INT-ILO2-POWER-INTERFACE NODE-RSA-KVM-INTERFACE NODE-RSA-POWER-INTERFACE NODE-IPMI-INTERFACE NODE-UCS-KVM-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。 どのインタフェースも削除できます。
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。

ノードの CSV ファイルの例



#					
# If TAG = NODE	NODE	Col 3* = Node Name	Col 4 = Description		
ADD	NODE	RDP	This is a RDP Node		
# If TAG = NODE-RDP-INTERFACE	NODE-RDP-INTERFACE	Col 3* = Node Name	Col 4* = Interface Name	Col 5* = IP Address/Hostname	Col 6 = TCP P
ADD	NODE-RDP-INTERFACE	RDP	RDP	192.168.51.163	
#					
# If TAG = NODE	NODE	Col 3* = Node Name	Col 4* = New Node Name	Col 5 = Description	
UPDATE	NODE	RDP	RDPUPDATE	This is UPDATE Nodename	
# If TAG = NODE-RDP-INTERFACE	NODE-RDP-INTERFACE	Col 3* = Node Name	Col 4* = Interface Name	Col 5* = New Interface Name	Col 6* = IP Ad
UPDATE	NODE-RDP-INTERFACE	RDPUPDATE	RDP	RDPInterfaceUPDATE	192.168.51
#					
# If TAG = NODE	NODE	Col 3* = Node Name			
DELETE	NODE	RDPUPDATE			
# If TAG = NODE-RDP-INTERFACE	NODE-RDP-INTERFACE	Col 3* = Node Name	Col 4* = Interface Name		
DELETE	NODE-RDP-INTERFACE	RDPUPDATE	RDPInterfaceUPDATE		

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。
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*『*446*p. 』」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* 『*445*p. 』」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。

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* 『*212*p. 』」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* 『*42*p. 』」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* 『*190*p. 』」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* 『*486*p. 』」を参照してください。
4. 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。

一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。
2. [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。
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。
4. 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。
5. 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  をクリックして、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。

6. [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。
7. [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。
8. 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。
9. 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。

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] ウィンドウが開きます。

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。**

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。

Ch 9 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* 『*224*p. 』」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* 『*211*p. 』」を参照してください。

この章の内容

[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。

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

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* 『*430*p. 』」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。
2. [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* 『*486*p. 』」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。**
4. 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* 『*196*p. 』」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。

7. 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* 『*211*p. 』」を参照してください。
9. [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* 『*215*p. の"*ユーザ グループへのポリシーの割り当て*"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。
10. 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。
2. [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。**
5. 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*** *『196*p. *』*」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。
8. ［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。
9. 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。
11. 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。
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**『252p. 』」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*** *『193*p. 』」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。
2. ［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。
3. ［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。
4. 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。

3. [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* 『*486*p. 』」を参照してください。
4. [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* 『*486*p. 』」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。
6. 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 『486*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 『282*p. 』」を参照してください。*

---

8. [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。
9. 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。
13. [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。
    - 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* 『*197*p. 』」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*** *『200p. 』*」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。**

1. [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。
2. このユーザが CC-SG にログインできないようにするには、[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にするには、[ログイン有効] チェックボックスを選択します。
3. 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*** *『282p. 』」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。
6. [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* 『*201*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。**

1. [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。
2. [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 [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。

1. [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* 『*207*p. 』」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* 『*444*p. 』」を参照してください。

CSV ファイルにユーザ グループを追加する場合

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 ファイルでユーザ グループに許可を割り当てる場合

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です。
2	USERGROUP-PERMISSIONS	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。 ユーザ グループ名では大文字と小文

列番号	タグまたは値	詳細
		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。
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。

列番号	タグまたは値	詳細
		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にするには、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

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。
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*『*446*p. 』」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 『445p. 』*」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。
2. [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。
2. [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* 『*486*p. 』」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。
2. [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。
2. [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。

1. ［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。

1. ［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。

Ch 10 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* 『*215*p. 』」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* 『*33*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* 『*185*p. 』」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* 『*80*p. 』」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* 『*212*p. 』」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* 『*215*p. 』」を参照してください。

この章の内容

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。**

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. [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* 『*486*p. 』」を参照してください。
4. [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。
8. [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* 『*263*p. 』」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。

1. [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。

7. [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。
12. [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* 『*212*p. 』」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* 『*190*p. 』」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 1 2 3 にアクセスできます。

ポリシー 456: サーバ 4 5 6 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 1 2 3 4 5 6 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 2 3 4 5 6 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 1 2 3 4 5 6 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

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。
9. 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。

1. [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。
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。

▶ 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。
2. 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。
3. 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。
4. [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。
9. 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。
2. 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。
3. 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。
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。

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。
4. [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

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。

IPv6 は、すべてのディレクトリ サーバでサポートされています。

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。
3. 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。
4. 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*『*190*p. 』」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。
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* 『*288*p. 』」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。
4. [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。

1. 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。

2. 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* 『*282*p. 』」を参照してください。
3. 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。

4. 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。

   注: ［接続テスト］ボタンは、詳細設定、グループ設定、および信頼設定を行った後に有効になります。このタブに戻って、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. ［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*** *『229*p. *』*」を参照してください。

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。
2. 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。

5. ［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。デフォルトのフィルタは「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。
   - ［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。
   - CC-SG が AD サーバを検索しているときに、照会先オブジェクトに遭遇した場合は、［Follow Referrals(照会先に従う)］チェックボックスを選択しておくと、AD は照会先に従って検索を完了できます。

- すでにドメインにログインしている場合、ユーザが Internet Explorer で IWA を介したシングル サイン オンを利用して CC-SG にアクセスできるようにするには、[統合 Windows 認証を使用する] チェックボックスをオンにします。「*統合 Windows 認証による SSO の設定* 『*239*p. 』」を参照してください。

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。
2. 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=com	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* 『*232*p. 』」を参照してください。

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。
2. [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。
3. [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。
4. 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。
6. [全般] タブをクリックし、[接続テスト] をクリックして、設定を確認します。 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。

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。
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. 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。
4. [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 『228p. 』*」、「*AD の詳細設定 『229p. 』*」、「*AD のグループ設定 『231p. 』*」、「*AD の信頼設定 『232p. 』*」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。
7. 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 『236p. 』*」および「*すべての AD モジュールの同期 『237p. 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 『231p. 』*」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『236p. 』*」および「*すべての AD モジュールの同期『237p. 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** 『282p. 』」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。

4. [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* 『*237*p. 』」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* 『*339*p. 』」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。
  1. [**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。「*全 AD モジュールの同期* 『*237*p. 』」を参照してください。
  2. [**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* 『*236*p. 』」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* 『*237*p. 』」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。
4. [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。
5. 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。
3. [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* 『*339*p. 』」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。

4. [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。デフォルトでは、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。

統合 Windows 認証による SSO の設定

すでにドメインにログインしている場合、ユーザは、統合 Windows 認証を介したシングル サイン オンにより、資格情報を明示的に提示しなくても Internet Explorer から CC-SG にアクセスできます。

IWA による SSO の要件

- SSO では、Kerberos のみがサポートされています。
- CC-SG Access Client および Admin Client は、SSO をサポートしています。
- Kerberos をサポートし IWA が有効になっている Windows クライアントの Internet Explorer。

IWA による SSO の設定

以下の手順では、例として次の前提条件が使用されています。

ドメイン: raritan.com

ドメイン ログイン名: example_user

ホスト名: example

信頼されたドメイン: nj.raritan.com、eu.raritan.com

1. AD サーバでサービス プリンシパル名を設定します。
   a. CC-SG のドメインで Active Directory にユーザ アカウント「example_user」を作成します。この手順では、「raritan.com」はドメインであり、ログイン名は「example_user」です。
   b. [User has to change(次回ログオン時にパスワードを変更する)] を無効にします。
   c. パスワードを割り当てます。
   d. CC-SG ホスト名が「example」であると仮定します。AD サーバで次のコマンドを実行し、CC-SG のサービス プリンシパル名を設定します。

   ```
   Setspn -A HTTP/example example_user
   Setspn -A HTTP/example.raritan.com example_user
   ```

2. CC-SG で SSO を有効にします。
   a. CC-SG Admin Client にログインします。
   b. Example AD モジュールを編集します。[全般] タブで、[ユーザ名] にサービス プリンシパル名を使用します。[ユーザ名] では、ドメイン名をすべて大文字にする必要があります。

   ```
   example_user@EXAMPLE.RARITAN.COM
   ```

   c. パスワードを変更します。AD で example_user のパスワードを変更するたびに、ここでもパスワードを変更する必要があります。

   注: 他の信頼されたドメインすべてにこうした変更を加える必要はありません。他のドメインでログインしたままにします。

   d. [詳細] タブで、[その他] の [統合 Windows 認証を使用する] チェックボックスをオンにします。SSO を許可する、他の信頼されたドメインすべてについてこのオプションを有効にします。
   e. [OK] をクリックして保存します。

   注: 信頼されたドメイン (nj.raritan.com、eu.raritan.com など) にログインするユーザは、それぞれのモジュールで統合 Windows 認証を有効にした場合、SSO を介して example.raritan.com にもアクセスできます。

3. Windows 認証を使用するように Internet Explorer ブラウザを設定します。ほとんどの設定は IE のデフォルトです。

a. ローカル イントラネット ドメインを設定します。
   - [ツール] > [インターネット オプション] > [セキュリティ] > [ローカルイントラネット] > [サイト] を選択します。
   - [ローカル イントラネット] ポップアップで、[プロキシ サーバーを使用しないサイトをすべて含める] および [ほかのゾーンにないローカル (イントラネット) のサイトをすべて含める] オプションが選択されていることを確認します。
   - または、[詳細設定] をクリックします。[ローカル イントラネット] (詳細設定) ダイアログ ボックスで、CC-SG にアクセスするためにユーザが使用する相対ドメイン名をすべて追加します。たとえば、example.raritan.com および example を追加して、[OK] をクリックします。

b. イントラネット認証を設定します。
   - [ツール] > [インターネット オプション] > [セキュリティ] > [ローカルイントラネット] > [レベルのカスタマイズ] を選択します。
   - [セキュリティ設定] ダイアログで、[ユーザ認証] セクションにスクロールします。[イントラネット ゾーンでのみ自動的にログオンする] を選択します。[OK] をクリックします。
   - [ツール] > [インターネット オプション] > [詳細設定] > [セキュリティ] > [統合 Windows 認証を使用する] を選択します。

IWA による SSO のトラブルシューティング

- CC-SG に、ドメインの時刻設定と同期する正しい時刻が設定されていることを確認します。デフォルトの許容最大値は 5 分です。
- ホスト名を使用して CC-SG (example、example.raritan.com など) にアクセスし、イントラネットでアクセス可能であることを確認します。
- クライアント マシンの OS で Active Directory から Kerberos チケットを取得できることを確認します。場合によっては、Windows 7 OS で DES を有効にする必要があります。

  詳細については、
  http://technet.microsoft.com/en-us/library/dd560670%28WS.10%29.aspx
  を参照してください。

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。
4. [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。
2. 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=NetscapeRoot」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。

8. 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。
9. 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。
10. 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。
2. 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。
4. 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>
ユーザ名	CN=<有効なユーザ ID>
パスワード	<パスワード>
ユーザ ベース	たとえば、 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。
ユーザ名パターンをバインド	たとえば、 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『190p. 』*」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

1. 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。
5. [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* 『*190*p. 』」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。
4. [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。
7. [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* 『*454*p. 』」を参照してください。**

Ch 13 レポート

この章の内容

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、デフォルトのレポート 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 日以前または 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。

レポートでの IP アドレス

デュアル スタック モードで CC-SG を実行しており、IPv4 および IPv6 のどちらのアドレスも使用できる場合は、レポートの列ラベルが両方のタイプのアドレスに対応するように変化します。

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。
2. [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。
3. [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* 『*250*p. 』」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。
2. [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。
3. [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* 『250p. 』」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。

3. [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。
4. [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* 『*327*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 『197p. 』*」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 『197p. 』*」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 『430p. 』*」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。
2. 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。

ホスト名で追加されたデバイスは、レポートにはホスト名でのみ表示されます。IP アドレスで追加されたデバイスは、IP アドレスで表示されます。CC-SG がデュアル スタック モードに設定されている場合、レポートおよび詳細ダイアログには、IPv6 をサポートするデバイスの IPv4 アドレスと IPv6 アドレスが表示されます。

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。

デバイスのホスト名と IP アドレスは、詳細ダイアログにのみ表示されます。

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。
2. 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。

2. [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。

3. 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。**
4. 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。

1. 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。
3. URL 列には各ノードへの直接リンクがあります。URL は、クライアント ブラウザで使用される、CC-SG への URL で構成されます。たとえば、クライアント ブラウザで https://<ホスト名、IPv4、または [IPv6]>/admin が使用されており、クライアントによってホスト名が <IPv4 または IPv6> に解決される場合は、<IPv4 または IPv6> がブックマークの作成に使用されます。これにより、引き続き NAT を介して CC-SG を機能させることができます。

4. 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『155*p. 』」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。
3. [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*『*249*p. 』」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* 『*258*p. 』」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。
2. 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。**

1. [レポート] > [Active Directory] > [AD ユーザ グループ レポート] を選択します。
2. [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。
3. [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 『337*p. 』」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。
4. 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。
5. [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。

1. 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* 『*261*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

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『337p. 』*」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

1. [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。
4. 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

1. [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* 『*267*p. 』」を参照してください。

CC-SG バックアップをタスクとして実行する場合は、[Automatic Delete when Maximum Reached (上限に達したら自動的に削除)] を選択すると、バックアップ ファイルの数が最大に達したときに最も古いバックアップ ファイルが自動的に削除されます。この設定は、バックアップ CC-SG タスクを作成するときにしか利用できません。バックアップ ファイルがバックアップ CC-SG タスクの一部として削除される場合、監査ログには、削除される各ファイルが記録されます。「*タスクのスケジュール* 『*339*p. 』」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。**
4. 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。* 『*267*p. 』」を参照してください。
5. [管理] > [タスク] ページでこのバックアップをタスクとして設定している場合、[Automatic Delete when Maximum Reached (上限に達したら自動的に削除)] チェックボックスをオンにすると、ファイルの数が最大に達したときに、ローカルに保存されている最も古いバックアップ ファイルを削除できます。[Maximum Backup Files(バックアップ ファイルの最大数)] フィールドに最大数を設定します。バックアップ ファイル数のデフォルト値は 50 です。**オプション。**
6. 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。IPv6 がサポートされています。

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。**

7. ［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* 『*268*p. 』」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 CC-SG 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]

CC-SG に保存されている CC-SG バックアップ ファイルもバックアップされません。CC-SG 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

1. [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。

1. ［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。
2. 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。* 『*267*p. 』」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。* 『*267*p. 』」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。* 『*267*p. 』」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* 『*12*p. 』」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。
7. [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** 『267p. 』」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。 ▪ 強力なパスワードが強制されます。 ▪ アウト オブ バンド ノードへの直接接続とプロキシ接続。

オプション	説明
	▪ 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: 255.255.255.0 ▪ 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 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。
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。

1. 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『265p. 』*」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。
3. [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* 『*265*p. 』」および「*バックアップ ファイルの保存* 『*267*p. 』」を参照してください。

アップグレードする前に CC-SG のディスク ステータスを確認する必要があります。「*ディスク ステータスの確認* 『*403*p. 』」を参照してください。**ドライブを交換する必要がある、ドライブに問題がある、RAID アレイを再構築する必要がある、ステータスに問題がある、などが示される場合は、ファームウェアをアップグレードする前に Raritan のテクニカル サポートまでお問い合わせください。**

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。

3. 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『264p. 』*」を参照してください。
4. 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。
6. [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。
7. 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 『369p. 』*」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。
   c. 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 ccImageUpgradeResults 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。
9. 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 『275p. 』*」を参照してください。
10. Java キャッシュをクリアします。「*Java キャッシュのクリア 『275p. 』*」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『264p. 』*」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『265p. 』*」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。
4. [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* 『*315*p. 』」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* 『*277*p. 』」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。**

1. [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* 『*312*p. 』」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。
2. 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* 『*279*p. 』」を参照してください。
3. 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* 『*385*p. 』」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。
4. [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。
5. 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* 『*264*p. 』」および「*CC-SG のアップグレード* 『*273*p. 』」を参照してください。

6. 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 『388p. 』*」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 『277p. 』*」を参照してください。
7. 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 『273p. 』*」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 『310p. 』*」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 『276p. 』*」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。

1. 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 『279p. 』*」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 『385p. 』*」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。
4. 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。**

1. 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* 『*339*p. 』」を参照してください。
2. 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* 『*265*p. 』」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。
4. 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* 『*268*p. 』」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。
5. 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* 『*339*p. 』」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* 『*253*p. 』」を参照してください。

7. 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* 『*388*p. 』」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。
3. [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* 『*385*p. 』」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* 『*386*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。

3. 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* 『*280*p. 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* 『*281*p. 』」を参照してください。

CC-SG のログアウト

1. [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

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。
2. 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。**
3. 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。
2. ［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。
2. 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* 『*264*p. 』」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。
2. [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* 『*285*p. 』」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。
5. [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。
6. [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** *『*285*p. 』」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* 『*275*p. 』」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。
4. 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。
6. 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。
2. [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 を使用するための必要条件

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 Admin Client 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。
2. ［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。
3. 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。
4. 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。
6. [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 Exisitng 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『90p. 』*」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。

3. 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* 『*290*p. 』」を参照してください。
- IP 分離モード: 「*IP 分離モードとは* 『*293*p. 』」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* 『*296*p. 』」を参照してください。

IPv4 アドレスで、またはデュアル スタック モードで CC-SG を操作できます。デュアル スタック モードは、IPv4 および IPv6 の両方のアドレスに対応します。

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

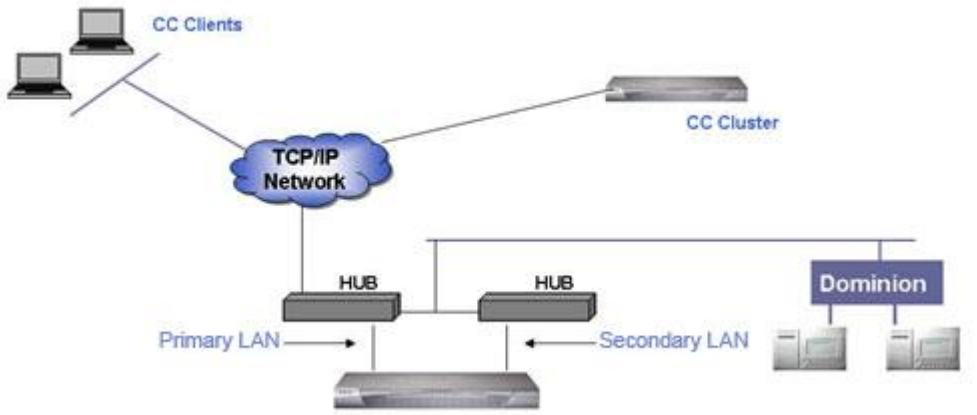
▶ **E1 LAN ポート:**

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* 『*289*p. 』」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

▶ 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。**

IPv4 を使用する IP フェイルオーバ モードまたは IPv6 を使用するデュアル スタック モードの設定

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。
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 『2*p. 』」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. IPv4 のみを使用するには、IPv4 のセクションにのみ入力し、IPv6 のチェックボックスがオンになっていないことを確認します。デュアル スタック モードを使用するには、IPv6 のチェックボックスをオンにし、IPv4 と IPv6 の両方のセクションに入力します。IPv4 とデュアル スタック モードを切り替える場合は、CC-SG を再起動する必要があります。今すぐまたは後で再起動するよう要求されるので、パスワード、ブロードキャスト メッセージ、および再起動のタイミングを入力する必要があります。無効にするモードに依存しているサービスがないことを確認します。
6. IPv4 アドレス セクションの [設定] ドロップダウン リストで [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 『296*p. 』」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。
7. デュアル スタック モードで実行するには、IPv6 設定のセクションに入力します。IPv4 のみを使用する場合は、この手順をスキップしてください。
   a. [Enable IPV6(IPv6 を有効にする)] チェックボックスをオンにします。

b. [設定] ドロップダウン リストで [Router Discovery(ルータ検出)] または [静的] を選択します。

8. [Router Discovery(ルータ検出)] を選択すると、[Global/Unique Local IPV6 Address(グローバル アドレスまたは固有のローカル IPv6 アドレス)]、[Prefix Length(プレフィックス長)]、[Default Gateway IPV6 Address(デフォルトのゲートウェイ IPv6 アドレス)]、[Link-Local IPV6 Address and Zone ID(リンクローカル IPv6 アドレスとゾーン ID)] の各フィールドが自動的に入力されます。
   a. [静的] を選択すると、[Global/Unique Local IPV6 Address(グローバル アドレスまたは固有のローカル IPv6 アドレス)]、[Prefix Length(プレフィックス長)]、および [Default Gateway IPV6 Address(デフォルトのゲートウェイ IPv6 アドレス)] が入力されます。
9. [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。
10. [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は、[アダプタ モード] ドロップダウン リストでデュプレックス モードを選択します。
11. [設定の更新] をクリックして変更を保存します。IPv6 を有効または無効にする場合は、CC-SG を再起動する必要があります。他のすべての変更で再起動が必要です。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『272*p. *』*」を参照してください。必要に応じて CC-SG が再起動されます。
      - 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] をクリックし、再起動オプションを選択して、変更を保存する必要があります。

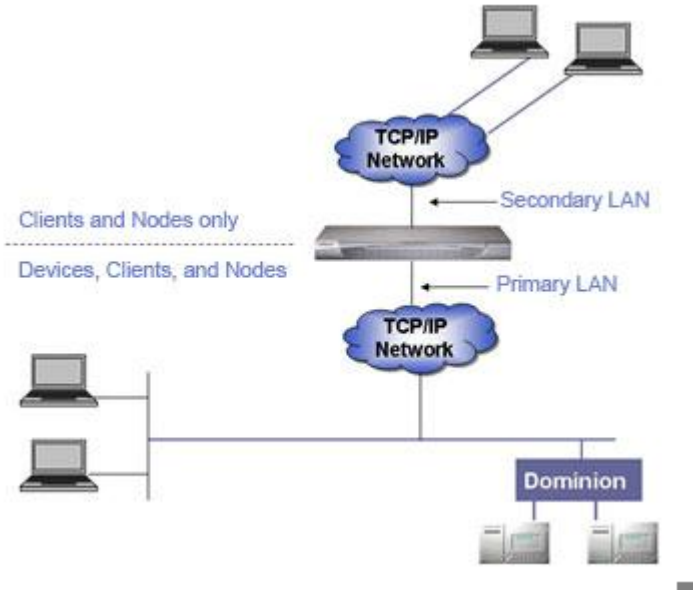
注: CC-SG で DHCP が設定されている場合、DNS サーバへの登録が成功するとホスト名を使用して CC-SG にアクセスできます。

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* 『*289*p. 』」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

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* 『*301*p. 』」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* 『*379*p. 』」を参照してください。

IPv4 を使用する IP 分離モードまたは IPv6 を使用するデュアル スタック モードの設定

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。

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. [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* 『*2*p. 』」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。

4. IPv4 のみを使用するには、IPv4 のセクションにのみ入力し、IPv6 のチェックボックスがオンになっていないことを確認します。デュアル スタック モードを使用するには、IPv6 のチェックボックスをオンにし、IPv4 と IPv6 の両方のセクションに入力します。IPv4 とデュアル スタック モードを切り替える場合は、CC-SG を再起動する必要があります。今すぐまたは後で再起動するよう要求されるので、パスワード、ブロードキャスト メッセージ、および再起動のタイミングを入力する必要があります。無効にするモードに依存しているサービスがないことを確認します。
5. [IP Isolation mode (IP 分離モード)] を選択します。
6. 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。
7. IPv4 設定セクションの [設定] ドロップダウン リストで [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* 『*296*p. 』」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。
8. デュアル スタック モードで実行するには、IPv6 設定のセクションに入力します。IPv4 のみを使用する場合は、この手順をスキップしてください。
   a. [Enable IPV6(IPv6 を有効にする)] チェックボックスをオンにします。
   b. [設定] ドロップダウン リストで [Router Discovery(ルータ検出)] または [静的] を選択します。
9. [Router Discovery(ルータ検出)] を選択すると、[Global/Unique Local IPV6 Address(グローバル アドレスまたは固有のローカル IPv6 アドレス)]、[Prefix Length(プレフィックス長)]、[Default Gateway IPV6 Address(デフォルトのゲートウェイ IPv6 アドレス)]、[Link-Local IPV6 Address and Zone ID(リンクローカル IPv6 アドレスとゾーン ID)] の各フィールドが自動的に入力されます。

10. [静的] を選択すると、[Global/Unique Local IPV6 Address(グローバルアドレスまたは固有のローカル IPv6 アドレス)]、[Prefix Length(プレフィックス長)]、および [Default Gateway IPV6 Address(デフォルトのゲートウェイ IPv6 アドレス)] が入力されます。
11. [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。
12. [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。
13. [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。

IPv6 のサポート

CC-SG で IPv6 アドレスを入力する場合は、圧縮形式およびゼロ抑制表現を使用できます。CC-SG では、保存および表示用に IPv6 アドレスが拡張されます。

次の通信は、IPv6 上ではサポートされていません。

- DHCPv6
- クラスタ
- ネットワーク ネイバーフッド
- モバイル クライアント
- KX2 2.5 より前の OOB-KVM インタフェースは IPv4 のみです。
- OOB-Serial インタフェース
- IPMI サポート (PX1 PDU 用など)
- SSH、Telnet、Web、VNC、MS-RDP、および iDRAC6 以外のインバンド インタフェース
- Power IQ
- CC-SG への SSH アクセス
- ライセンス サーバ
- システムレベルのアクセス制御リスト

IP アドレスに対する CC-SG ホスト名を DNS に登録

ネットワーク内で CC-SG を設定しており、DNS が利用可能な場合は、CC-SG のホスト名が、設定された静的 IP に解決されるように DNS にエントリが自動的に追加されます。

ネットワーク外で CC-SG を設定している場合、または DNS サーバが更新を許可されていない場合は、この情報を使用して DNS にエントリを手動で追加する必要があります。

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。

4. [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。「*重大度レベルの例をログに記録* 『*299*p. 』」を参照してください。
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 『250p. 』」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。

重大度レベルの例をログに記録

選択する重大度レベルによって、syslog に転送されるイベントのタイプが決まります。

- オフ

「オフ」に設定すると、イベントは syslog に転送されません。

- 致命的

実行停止につながる内部エラー（ディスク障害、両方のハードディスクの取り外し、ネットワーク接続の喪失など）。

- エラー

不正なユーザ名やパスワードでのログイン。

- 警告

名前がすでに存在するユーザまたはデバイスの追加。

- 情報

ユーザ、デバイスなどの追加または削除。

- デバッグ

成功したログインやログアウト、および不正なユーザ名やパスワードでのログイン。

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* 『*337*p. 』」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* ***『114p. 』***」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。

4. [アドレス] フィールドに IPv4 または IPv6 アドレスを入力し、プレフィックス長を指定して、ダイレクト モードでノードやポートに接続する範囲を作成します。プレフィックス長は、IPv4 アドレスの場合は 1 ～ 32、IPv6 アドレスの場合は 1 ～ 128 を指定できます。
5. [追加] をクリックします。
6. [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。

注: [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）機能と共に IPv4 および IPv6 デュアル スタック モードで動作している場合、Microsoft® ClickOnce® では、サーバ証明書 CN に IPv6 アドレスのゼロ圧縮形式を含めてはなりません。ゼロ圧縮形式を含めると、AKC を正常にダウンロードして起動することができなくなります。ただし、これは IPv6 アドレスの形式に対するブラウザの設定と競合する場合があります。共通名（CN）でサーバのホスト名を使用するか、証明書の「サブジェクトの別名」に IPv6 アドレスの圧縮形式や非圧縮形式を含めてください。

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は、以下の操作を行います。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。

1. ［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。
4. [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には、以下の手順に従います。

1. [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。
2. [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。

1. 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* 『*265*p. 』」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。
4. 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。

5. 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。

1. ［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) を使用すると、CC-SG から 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。

SNMP v3 を有効にすると、ユーザベースのセキュリティ モデルおよびビューベースのアクセス制御モデルによる暗号化ができます。CC-SG は、SNMP v3 トラップをサポートしています。

SNMP エージェントの設定

設定できるエージェント数に制限はありません。

▶ CC-SG で SNMP エージェントを設定するには、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. [Listening Port(リスニング ポート)] フィールドに SNMP エージェントのポート番号を入力します。デフォルトは 161 です。
4. SNMP v1/v2 エージェントを有効にするには、[Enable SNMP v1/v2c(SNMP v1/v2c を有効にする)] チェックボックスをオンにします。
   a. 読み取り専用コミュニティ文字列を入力します。デフォルトは「public」です。
   b. 読み書きコミュニティ文字列を入力します。デフォルトは「private」です。
   c. 複数のコミュニティ文字列を追加するには、各文字列をカンマで区切ります。
5. SNMP v3 エージェントを有効にするには、[SNMP v3(SNMP v3)] チェックボックスをオンにします。
   a. チェックボックスの下のテーブルで、[行の追加] アイコンをクリックします。  5 つの入力フィールドを持つ行が表示されます。

b. [Security Name(セキュリティ名)] フィールドに SNMP マネージャの「ユーザ」名を入力します。セキュリティ名は 1 ～ 32 文字で指定できます。

c. [Authentication Protocol(認証プロトコル)] ドロップダウン リストから [MD5(MD5)] または [SHA(SHA)] を選択します。

d. フィールドに認証パスフレーズを入力します。パスフレーズは 8 ～ 64 文字で指定できます。認証パスフレーズは、最適なセキュリティを実現するためにプライバシー パスフレーズとは異なるものにする必要があります。これらのパスフレーズが同じ場合、一部の MIB ブラウザはうまく機能しない場合があります。

e. [Privacy Protocol(プライバシー プロトコル)] ドロップダウン リストで [なし]、[DES(DES)]、または [AES(AES)] を選択します。

f. プライバシー パスフレーズを入力します。パスフレーズは 8 ～ 64 文字で指定できます。認証パスフレーズは、最適なセキュリティを実現するためにプライバシー パスフレーズとは異なるものにする必要があります。これらのパスフレーズが同じ場合、一部の MIB ブラウザはうまく機能しない場合があります。

6. 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。
7. [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。

Raritan MIB ファイルによる SNMP エージェントの更新

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* 『*440*p. 』」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。

SNMP トラップおよび SNMP 通知の設定

SNMP トラップおよび SNMP 通知を設定するには、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] タブで、エージェントが [Agents(エージェント)] タブで設定されていることを確認します。[Traps(トラップ)] タブをクリックします。
4. [SNMP トラップを有効にする] チェックボックスをオンにし、CC-SG から SNMP ホストへの SNMP v1/v2c トラップの送信を有効にします。SNMP v3 トラップだけを設定する場合は、この手順をスキップし、手順 6 に進みます。

5. チェックボックスの下のテーブルで、[行の追加] アイコンをクリックします。  4 つの入力フィールドを持つ行が表示されます。
   a. トラップ送信先ホストの IP アドレスを [ホスト] フィールドに入力します。
   b. SNMP ホストで使用される、トラップ送信先ホストのポート番号を [ポート] フィールドに入力します。デフォルトのポートは 162 です。
   c. [バージョン] ドロップダウン リストで v2 または v1 を選択します。
   d. SNMP ホストで使用されるコミュニティ文字列を [コミュニティ] フィールドに入力します。
6. [Enable SNMP v3 Notifications(SNMP v3 通知を有効にする)] チェックボックスをオンにして、CC-SG から SNMP ホストへの SNMP v3 通知の送信を有効にします。SNMP v1/v2c トラップのみを設定する場合は、この手順をスキップして、手順 4 ～ 5 を実行したことを確認し、手順 7 に進みます。
   a. チェックボックスの下のテーブルで、[行の追加] アイコンをクリックします。  6 つの入力フィールドを持つ行が表示されます。
   b. トラップ送信先ホストの IP アドレスを [ホスト] フィールドに入力します。
   c. SNMP ホストで使用される、トラップ送信先ホストのポート番号を [ポート] フィールドに入力します。デフォルトのポートは 162 です。
   d. [Security Name(セキュリティ名)] フィールドに SNMP マネージャの「ユーザ」名を入力します。セキュリティ名は 1 ～ 32 文字で指定できます。
   e. [Authentication Protocol(認証プロトコル)] ドロップダウン リストから [MD5(MD5)] または [SHA(SHA)] を選択します。
   f. フィールドに認証パスフレーズを入力します。パスフレーズは 8 ～ 64 文字で指定できます。認証パスフレーズは、最適なセキュリティを実現するためにプライバシー パスフレーズとは異なるものにする必要があります。これらのパスフレーズが同じ場合、一部の MIB ブラウザはうまく機能しない場合があります。
   g. [Privacy Protocol(プライバシー プロトコル)] ドロップダウン リストで [なし]、[DES(DES)]、または [AES(AES)] を選択します。

h. プライバシー パスフレーズを入力します。パスフレーズは 8 ～ 64 文字で指定できます。認証パスフレーズは、最適なセキュリティを実現するためにプライバシー パスフレーズとは異なるものにする必要があります。これらのパスフレーズが同じ場合、一部の MIB ブラウザはうまく機能しない場合があります。

7. ページの下部の［トラップ ソース］リストで、CC-SG から SNMP ホストに送り出すトラップのチェックボックスをオンにします。トラップは次の 2 つのカテゴリに分類されます。［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-SG 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 アカウントの変更などの CC-SG 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。
   a. 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］のチェックボックスをオンにします。
   b. 個々のトラップを有効にするには、それぞれのチェックボックスをオンにします。
   c. 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。詳細については、「*SNMP トラップ* 『*440*p. 』」を参照してください。
8. ［トラップ設定の更新］をクリックして変更を保存します。

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。

注: シック クライアントを使用して CC-SG にアクセスする場合、プライマリ ノードに障害が発生すると、バックアップ ノードに自動的にリダイレクトされません。シック クライアントを使用してアクセスするには、バックアップ ノードに手動で IP アドレスを入力する必要があります。

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*『*288*ﾍﾟｰｼﾞ.』」を参照してください。
- クラスタは IPv6 上ではサポートされていません。
- 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。
2. 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。
3. 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。
6. [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* 『*310*p. 』」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。

セカンダリ CC-SG ノードの削除

セカンダリ ノードまたはバックアップ ノードを削除すると、セカンダリ ノードの指定が削除されます。セカンダリ CC-SG ユニットが設定から削除されるわけではありません。

▶ CC-SG ユニットからセカンダリ ノード ステータスを削除するには、以下の手順に従います。

1. クラスタ設定テーブルでセカンダリ CC-SG ノードを選択します。
2. [バックアップ ノードの削除] をクリックします。
3. [はい] をクリックし、セカンダリ ノード ステータスを削除します。

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* 『*313*p. 』」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。
2. [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* 『*313*p. 』」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。
   - [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。
3. [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* 『*276*p. 』」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『276p. 』*」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。
- ネイバーフッドのメンバは、IPv4 ネットワーク上に存在する必要があります。IPv6 通信は、ネイバーフッドではサポートされていません。

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。
4. 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。証明書に記載されているもの、およびアクセスに使用する CC-SG の URL に含まれるものと、完全に一致する IP アドレスまたはホスト名を使用してください。「*ネイバーフッドの証明書要件* 『*321*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。「***隣接システムの設定** 『316*p. 』」を参照してください。*

---

8. 必要に応じて、ネイバーフッド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** 『330p. 』」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

1 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。
3. 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。
   c. 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。
4. 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。
6. 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。
   - 隣接システムのメンバにアクセスするユーザが、隣接システムのすべてのメンバに対する検索を実行し、検索結果からターゲット接続を実行できるようにするには、［Enable Extended Network Neighborhood Search(拡張ネットワーク隣接システムの検索の有効化)］チェックボックスを選択します。拡張ネットワーク隣接システムの検索を無効にするには、チェックボックスを選択解除します。「拡張ネットワーク隣接システムの検索」を参照してください。

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。

拡張ネットワーク隣接システムの検索

拡張ネットワーク隣接システムの検索が有効になっていると、Access Client のみを使用して、隣接システムの任意のメンバのノードを検索し、アクセスするオプションがユーザに提供されます。

検索を実行する場合、検索の対象を [In Neighborhood(隣接システム)] のすべてのメンバとするか、[Local Only(ローカルのみ)] にするかを指定できます。

拡張ネットワーク隣接システムの検索を実行した結果として、隣接システムの検索結果が取得されると、隣接システム ノードのステータスと可用性、およびノード データが表示されます。検索結果が表示されている間は、このデータは隣接システム ノードにリアルタイムで更新されません。

注: ノードの仮想マシン データは、隣接システムの CC-SG からの VM についてではなく、ホーム CC-SG の VM ノードについてのみ表示されます。

[All Nodes(すべてのノード)] グループでパワー制御操作を実行する場合、拡張隣接システム検索が有効になっている間は、隣接システムの CC-SG ユニットのノードは含まれません。[All Nodes(すべてのノード)] グループは、"ホーム" CC-SG でのみ作成され、隣接システムのノードを含めることはできません。

隣接システムのメンバの削除

隣接システムの CC-SG ユニットが不要になった場合は、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。

2. 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。

ネイバーフッドの証明書要件

証明書エラーなしでネイバーフッドを使用するには、以下の手順に従う必要があります。

1. 各 CC-SG ネイバーフッドのメンバについて、証明書に記載されているもの、ネイバーフッドの作成時に使用したもの、および URL による CC-SG へのアクセス時に使用するものと、同じ IP アドレスまたはホスト名を使用してください。正しい証明書を確保するには、証明書（自己署名または CA 発行）をアクセス URL/DNS 名と一致する名前で生成してインストールします。「*証明書* 『*331*p. 』」を参照してください。
2. CC-SG を起動すると、証明書エラーが表示されます。その場合は、ネイバーフッドで各 CC-SG の証明書をインストールします。
3. 信頼されたストアに証明書を配置します。
4. Internet Explorer ブラウザでは、ネイバーフッドの各 CC-SG の IP/ホスト名が 2 つのセクションに追加されます。[インターネット オプション] を選択し、[セキュリティ] タブをクリックし、[信頼済みサイト] アイコンをクリックします。[信頼済みサイト] のリストに各 CC-SG の IP/ホスト名を追加し、[プライバシー] > [サイト] タブでも同じ操作を行います。IP またはホスト名が、CC-SG へのアクセスに使用される URL と完全に一致していることを確認します。

5. ブラウザが Internet Explorer 8 および Internet Explorer 9 の場合は、[インターネット オプション] > [プライバシー] タブを選択します。[インターネット ゾーン] の設定で [すべての Cookie を受け入れる] を設定します。
6. Internet Explorer ブラウザで、ネイバーフッドに含まれる CC-SG の IP アドレス/ホスト名がすべて表示されていることを確認します。確認するには、[インターネット オプション] > [コンテンツ] > [証明書] で、[信頼されたルート証明機関] タブを選択します。

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。

ネイバーフッドのアップグレード

ネイバーフッド内のすべての CC-SG ユニットでは、同じバージョンのファームウェアを使用する必要があります。CC-SG ユニットは、ネイバーフッドのアクティブなメンバである間はアップグレードできません。各メンバを無効にしてアップグレードした後、もう一度各メンバを有効にして、ネイバーフッドの設定を更新します。

▶ **ネイバーフッドをアップグレードするには、以下の手順に従います。**

1. アップグレードの準備ができたら、各 CC-SG ユニットを無効にします。「*ネイバーフッドの設定の管理* 『*319*p. の"*隣接システムの設定の管理*"参照 』」を参照してください。
2. アップグレードの推奨事項に従って、各 CC-SG ユニットを個々にアップグレードします。「*CC-SG のアップグレード* 『*273*p. 』」を参照してください。
3. ネイバーフッドのメンバがアップグレードされたら、そのメンバを有効にします。「*ネイバーフッドの設定の管理* 『*319*p. の"*隣接システムの設定の管理*"参照 』」を参照してください。
4. ネイバーフッドを更新します。「*ネイバーフッドの更新* 『*321*p. の"*隣接システムの更新*"参照 』」を参照してください。

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* 『*224*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。**

1. *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。
2. 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。

4. 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。

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。
6. [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。
3. 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。
4. 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。
3. 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。

モバイル クライアントのタイムアウトの設定

モバイル クライアントのタイムアウトを設定すると、非アクティブなモバイル アクセス クライアントおよびモバイル KVM クライアント (MKC) セッションはタイムアウト期間の終了後に終了します。これにより、セッションが非アクティブであるにもかかわらず、ビジーとして保留されているリソースが解放されます（ターゲット接続が正常に終了しなかった場合など)。タイムアウトを設定すると、単一ログイン制限が存在する場合に、突然切断された管理ユーザがログインし直すこともできるようになります。セッションがアクティブである場合は、終了しません。

デフォルトのモバイル クライアント タイムアウトは 8 分です。モバイル クライアント タイムアウトは常に有効です。

このタイムアウトは、モバイル クライアント アクセスにのみ適用されます。また、休止タイマおよびデバイス固有のアイドル タイムアウト値に対する追加的な設定です。これは、モバイル クライアント アクセスに対して短いタイムアウト時間を定義し、適用できるようにするためのものです。

セッションの不適切な終了の例には、左上隅の X をタッチしてブラウザ ウィンドウを閉じた場合、ブラウザ ウィンドウを開いたままデバイスをオフにした場合、ブラウザ ウィンドウがバックグラウンドにある場合などがあります。

非アクティブであるために終了したモバイル クライアント セッションについて、監査ログにメッセージ "Inactivity timeout occurred for SessionID {0}" (SessionID {0} で非アクティビティ タイムアウトが発生しました）が記録されます。有効である場合は、ccPortConnectionTerminated SNMP 通知も生成されます。

▶ **モバイル クライアント タイムアウトを構成するには、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. ［ログイン設定］タブをクリックします。
3. ［Mobile Client Timeout(モバイル クライアント タイムアウト)］フィールドで、セッションが終了する前に非アクティブの状態を維持する時間を、5 ～ 30 分までの分単位で設定します。
4. ［更新］をクリックします。

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。

1. [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

インポートする証明書は PEM 形式でなければなりません。

証明書の作成時には、サブジェクトの別名がすべて含まれ、名前の不一致がないことを確認します。

Java クライアントの jar ダウンロード アクティビティでは、ダウンロード URL で指定されているホスト名が正確に一致しているかが確認されます。

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。

4. [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。

7. [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。
11. 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。

IPv6 アドレスは、システムレベルのルールでは使用できません。他のすべてのルールでは、ルールの両方の IP エントリが、同じタイプ (つまり、両方とも IPv4 または両方とも IPv6) でなければなりません。

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。
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] 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。
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。
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* 『*337*p. 』」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* 『*2*p. 』」を参照してください。IPv6 がサポートされています。
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。
5. 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。
6. 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。
7. 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。
9. 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。
10. 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 『336p. 』*」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 『261p. 』*」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* 『*341*p. 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。
3. [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。
5. [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* 『*237*p. 』」を参照してください。
   - CommandCenter *のバックアップ*: バックアップの詳細、および古いバックアップ ファイルの自動削除を設定する方法の詳細については、「*CC-SG のバックアップ* 『*265*p. 』」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* 『*92*p. 』」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* 『*98*p. 』」および「*管理の再開* 『*98*p. 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* 『*99*p. 』」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* 『*96*p. 』」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* 『*412*p. 』」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* 『*297*p. 』」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* 『*97*p. 』」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* 『*93*p. 』」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* 『*341*p. 』」を参照してください。
- **すべてのレポートの生成:** 「*レポート* 『*248*p. 』」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。
   e. [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。

9. 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* 『*262*p. 』」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。
3. 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* 『*339*p. 』」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* 『*341*p. 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* 『*339*p. 』」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* 『*341*p. 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* 『*343*p. 』」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 OpenSSH 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。

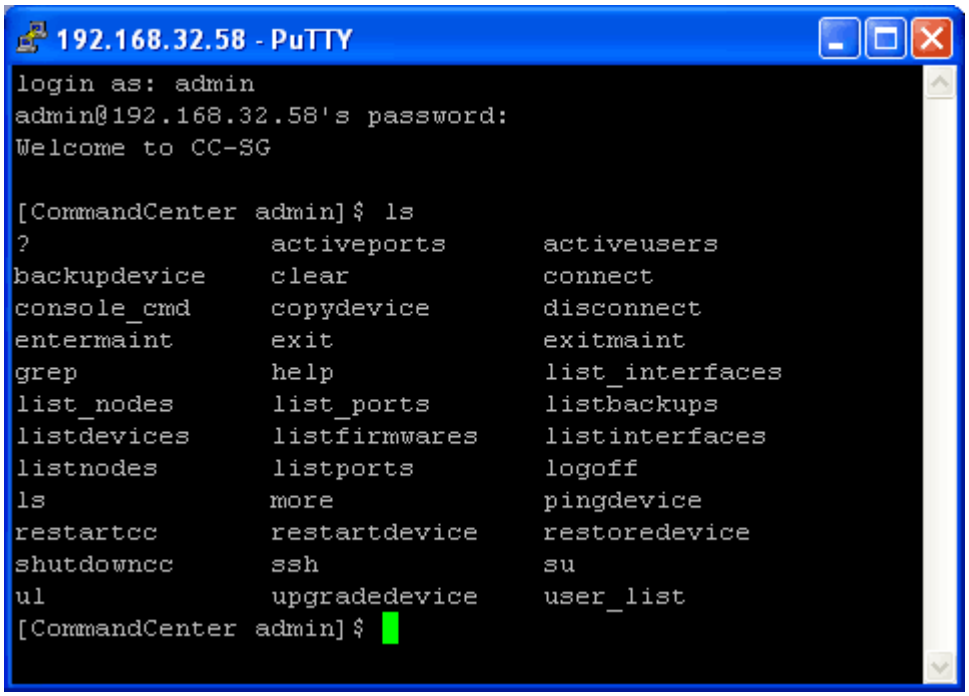
SSH を使って CC-SG にアクセスしている管理者は、CC スーパーユーザ SSH ユーザをログアウトすることはできませんが、システム管理者を含む他のすべての SSH クライアント ユーザをログアウトできます。

▶ 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。
3. 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* 『*323*p. 』」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 ls を入力して、利用可能なすべてのコマンドを表示します。



SSH アクセスの有効化

Admin Client で SSH アクセスを有効にすると、ユーザが SSH を使用して CC-SG にアクセスできるようになります。

SSH 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. [暗号化] タブで、[Enable SSH Access(SSH アクセスを有効にする)] チェックボックスをオンにします。
3. SSH アクセスの他のオプションを設定します。
   a. SSH アクセス用のポート番号を [SSH サーバ ポート] フィールドに入力します。デフォルトは 22 です。
   b. [Enable SSH DPA(SSH DPA を有効にする)] チェックボックスをオンにすると、SSH を使用して SX シリアル ポート ターゲットに直接接続できるようになります。このチェックボックスがオンになっていない場合は、ダイレクト ポート アクセスを使用してシリアル ポート ターゲットに接続しようとしても拒否されます。
4. [更新] をクリックします。

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。**

1. 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。

一部のコマンドには、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 『350*p. 』」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 バージ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:**

```
ls
```

- **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

- 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* 『*2*p. 』」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、両方を入力することはできません。
- 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>	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 『353p. 』*」を参照してください。

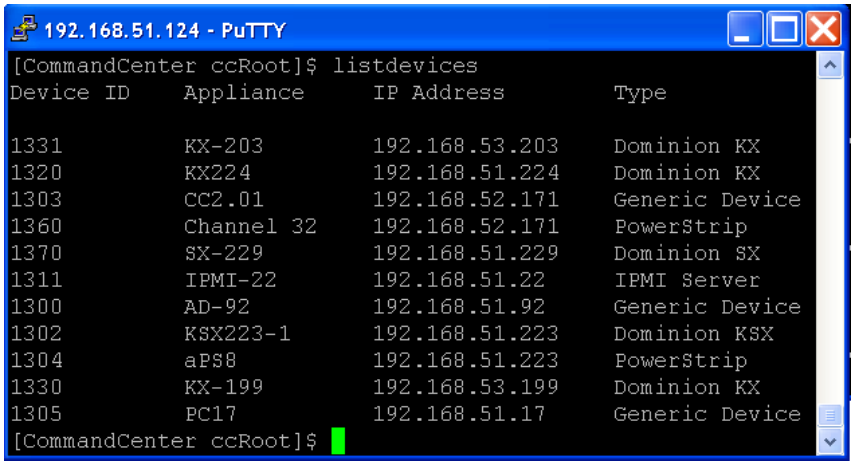
Linux ターミナルまたはクライアントではエスケープ文字の使用で問題が発生することがあります。Raritan では、ポート接続を確立するときに新しいエスケープ文字を定義することを推奨します。コマンドは、`connect [-e <escape_char>] [port_id]` です。たとえば、ID が 2360 のポートに接続するときにエスケープ文字として "m" を定義するには、「`connect -e m 2360`」と入力します。

シリアル対応デバイスへの SSH 接続の作成

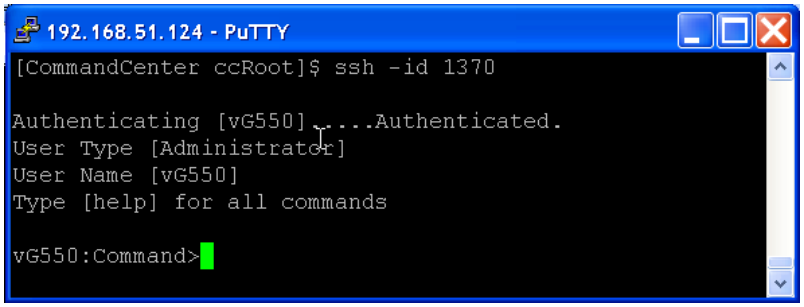
デバイスに管理操作を実行するために、シリアル対応デバイスへの SSH 接続を作成することができます。接続後は、そのシリアル対応デバイスでサポートされている管理コマンドを利用できます。

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。



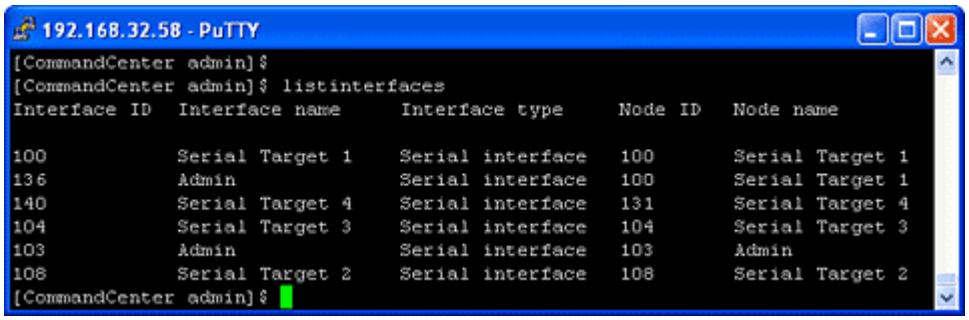
2. 「`ssh -id <device_id>` 」と入力して、デバイスに接続します。たとえば、上記の例では、「`ssh -id 1370`」**と入力すると、SX-229 に接続できます。**



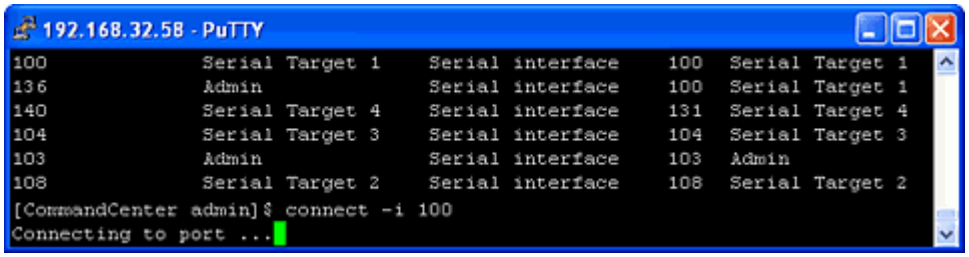
SSH を使用してシリアル アウト オブ バンド インタフェース経由でノードに接続

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。



2. 「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。



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。

コマンド	エイリアス	説明
quit	q	接続を終了して、SSH プロンプトに戻ります。
get_write	gw	書き込みアクセスを取得します。SSH ユーザに、ターゲット サーバでコマンドを実行することを許可します。ブラウザ 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。

コマンド	エイリアス	説明
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。

Dominion SX シリアル ターゲットへのダイレクト ポート アクセス

CC-SG では、CC-SG で管理されている Dominion SX デバイスのシリアル ターゲットに対する SSH ダイレクト ポート アクセスが考慮されています。最初にこのオプションを有効にする必要があります。「*SSH アクセスの有効化* 『*346*p. 』」を参照してください。

すべての SSH パススルー セッションは、CC-SG でプロキシ処理されます。

設定可能なエスケープ文字を使用すると、ユーザは、ターゲットでの SSH セッション中に必要に応じてポート メニューにエスケープし、ポートに対して使用可能なコマンド（write lock、history など）にアクセスできます。

最大 30 の同時セッションが可能です。

ダイレクト ポート アクセスによるシリアル ターゲットのポートおよびノードの命名

Dominion SX のシリアル ターゲットへのダイレクト ポート アクセスと、CC-SG を使用しない SX のポートへのアクセスを併用する場合は、ターゲットのポート名とノード名を同じにしておくことをお勧めします。

ポート名とノード名が同じでない場合は、両方の名前を把握し、アクセス方法によっては正しい名前を使用する必要があります。たとえば、CC-SG を介してアクセスするか、SX を介して直接アクセスするかによって異なります。

CC-SG では、固有のノード名を使用する必要があります。以下の手順に従って CC-SG のすべての変更を行い、固有の名前がポートに反映されていることを確認し、名前の同期を維持して、間違ったターゲットに接続されないようにします。

▶ **ダイレクト ポート アクセスでシリアル ターゲットのポートおよびノードに名前を付けるには、以下の手順に従います。**

1. CC-SG で SX ポートを設定する場合は、ノード名およびポート名を同じ名前に設定します。ポート名は SX に反映されます。
2. CC-SG ノードごとに 1 つのシリアル インタフェースだけを設定します。これにより、ノードにポート名と同じ固有名が付けられます。
3. CC-SG ノード名を変更する場合は、ポート名も同じ名前に変更し、SX ポート名とその関連ノードとの同期を維持します。新しいポート名は SX に反映されます。

ダイレクト ポート アクセス SSH コマンド

次のコマンドを使用すると、Dominion SX デバイスのターゲットにダイレクト ポート接続できます。Dominion SX デバイスは CC-SG で管理する必要があります。ダイレクト ポート アクセスを実現するには、CC-SG ユーザ名、ノード名、セッションのエスケープ文字、および CC-SG のホスト名または IP アドレスを 1 つのコマンドで指定します。

サンプル コマンド:

```
ssh -l
username[:ccsg_node_name[:[escape_mode][:escape_char]
]]{hostname | IP_address}
```

ダイレクト ポート アクセス コマンドのパラメータ

パラメータ	詳細
username	接続元ユーザの CC-SG ユーザ名。 ユーザには、ターゲットに対するアクセス許可が必要です。
ccsg_node_name	シリアル ターゲットのノード名。この名前はポート名と同じでなければなりません。「*ダイレクト ポート アクセスによるシリアル ターゲットのポートおよびノードの命名* 『*354*p. 』」を参照してください。 ▪ コロン「:」は、名前には使用できません。 ▪ ″:″ は、username、ccsg_node_name、escape_mode、および escape_character の間の区切り文字としてのみ使用できます。 ▪ 名前に空白文字が含まれている場合は、名前を二重引用符で囲む必要があります。 ▪ 名前に使用されている左右のカッコ「(」および「)」は、円記号「¥」でエスケープする必要があります。 例: 「Port32(2)」のカッコをエスケープするには、次のようにします。 `ssh -l admin:Port32¥(2¥) 10.0.20.11`
escape_mode	オプション。escape_mode パラメータは、エスケープ モードをデフォルトから変更するために使用されます。 `control` または `none` control は、デフォルトのモードであり、空白のままでかまいません。空白のままの場合でも「:」を使用してください。 escape_mode への変更は、ポートごとに行われ、セッション中のみ有効です。変更は永続的ではありません。

パラメータ	詳細
escape_char	オプション。escape_character パラメータは、エスケープ文字をデフォルトから変更するために使用されます。 デフォルトのエスケープ文字は「]」です。 escape_char への変更は、ポートごとに行われ、セッション中のみ有効です。変更は永続的ではありません。
hostname|IP_address	Dominion SX を管理する CC-SG のホスト名または IP アドレス。

例: DPA でエスケープ文字を左角カッコ「[」に変更

- **ダイレクト ポート アクセス セッションでエスケープ文字を左角カッコ「[」に変更するには、次のようにします。**

```
ssh -l username:ccsg_node_name::[ {hostname|IP_address}
```

ターゲットに接続している場合、ユーザは、Ctrl+[を押すと、ポート メニューにエスケープします。

例: DPA でエスケープ モードを「none」に変更

- **ダイレクト ポート アクセス セッションでエスケープ モードを「none」に変更するには、次のようにします。**

```
ssh -l username:ccsg_node_name:none
{hostname|IP_address}
```

ターゲットに接続している場合、ユーザは、](デフォルトのエスケープ文字) を押すと、ポート メニューにエスケープします。

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。

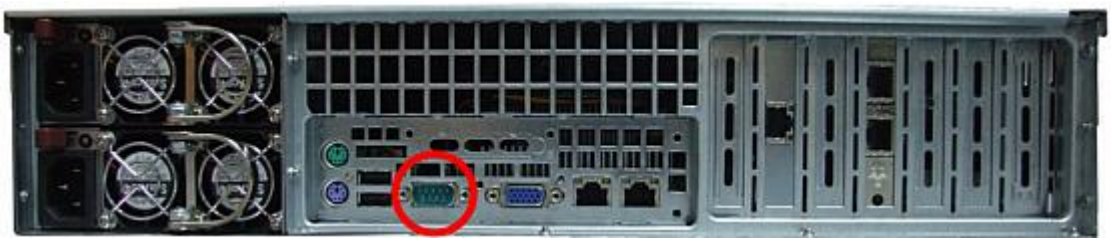
SX 要件:

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。

管理者には、特に仮想アプライアンスの場合、CC-SG シリアル ナンバーのレコードを保持することをお勧めします。テクニカル サポートが FS2 パスワードを使用して支援する場合に、シリアル ナンバーが必要になるためです。

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。

   l. 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/マウス ポートからの診断コンソールへのアクセス『362*p. 』」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『362*p. 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『363*p. 』」を参照してください。
2. Administrator Console .「*Administrator Console について『369*p. 』」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

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)。

3. 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。
4. 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* 『*363*p. 』」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。**

1. 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* 『*362*p. 』」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。

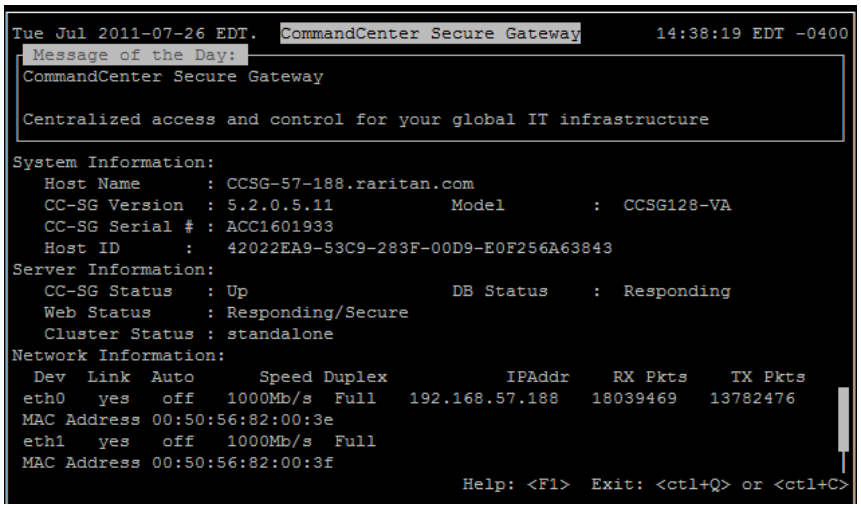
2: Web ブラウザから Status Console にアクセスします。

1. 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。



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 のシリアル ナンバー。	
モデル	CC-SG のモデル タイプ。	
Host ID	CC-SG ユニットのライセンスを得るための番号。	
CC-SG Status	ほとんどのユーザ リクエストを処理する CC-SG サーバのステータス。以下のステータスが表示されます。	
	Up	CC-SG は利用可能で、ユーザ リクエストを受け付けることができます。
	Down	CC-SG は停止しているか再起動中である可能性があります。[Down] のステータスが続く場合は、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 サーバは、その処理の中で内部データベース (DB) を使用します。CC-SG が機能するには、このデータベースが、稼働し応答している必要があります。以下のステータスが表示されます。	
	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

情報	説明	
		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 サーバへのアクセスのほとんどは Web を介して行われます。このフィールドには、Web サーバの状態と、以下のステータスが表示されます。	
	Responding/Unsecured	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/Secured	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 (RAID-1) ディスクに保存します。以下の RAID ディスクのステータスが表示されます。	
	Active	RAID が完全に機能しています。
	Degraded	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* 『*309*p. 』」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	

情報	説明	
	使用して情報が表示されます。仮想 CC-SG の場合、各 NIC の MAC アドレスは、ここに示す列の下に表示されます。	
	MAC Address	仮想 CC-SG の場合、表示される各 NIC の MAC アドレスです。
	Dev	インタフェースの内部名。
	Link	リンク整合性の状態、つまりこのポートが、損傷のないケーブルで稼働中のイーサネットスイッチ ポートに接続されているかどうかを示します。
	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。
	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 Ipv4 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。

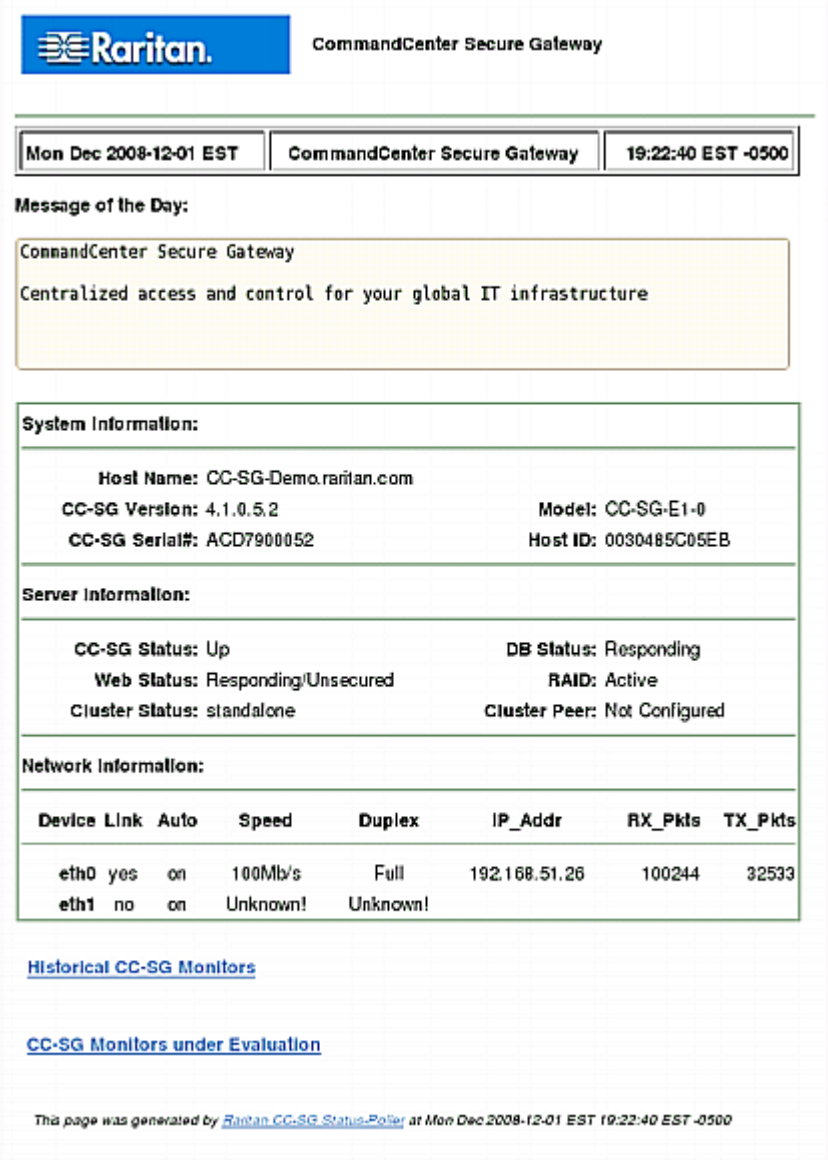
ナビゲーション キーのリマインダ

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。



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*『*395*p. 』」および「*CC-SG ディスクの監視* 『*451*p. 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。

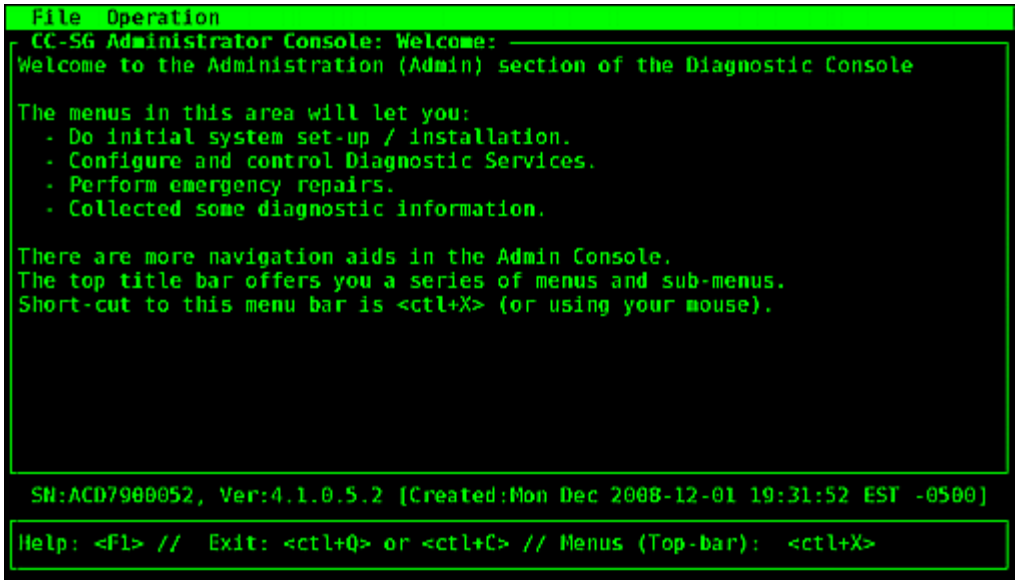
Administrator Console へのアクセス

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。
2. 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* 『*390*p. 』」を参照してください。

Administrator Console メイン画面が表示されます。



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* 『*371*p. 』」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。一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。

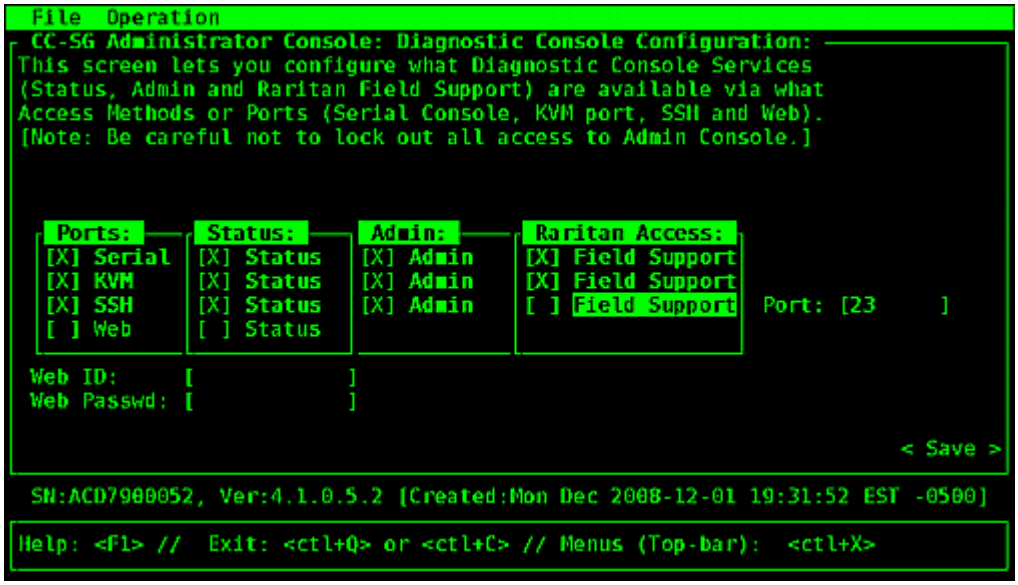
▶ 診断コンソール設定を編集するには、以下の手順に従います。

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。



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。
2. 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* 『*2*p. 』」を参照してください。
4. [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* 『*288*p. 』」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。

6. [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。
7. [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。
8. [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。
9. [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。

IPv6 ネットワーク インタフェース設定の編集

[IPv6 Network Interface Configuration(IPv6 ネットワーク インタフェース設定)] ページで、デュアル スタックを有効または無効にします。これには、CC-SG の再起動が必要です。

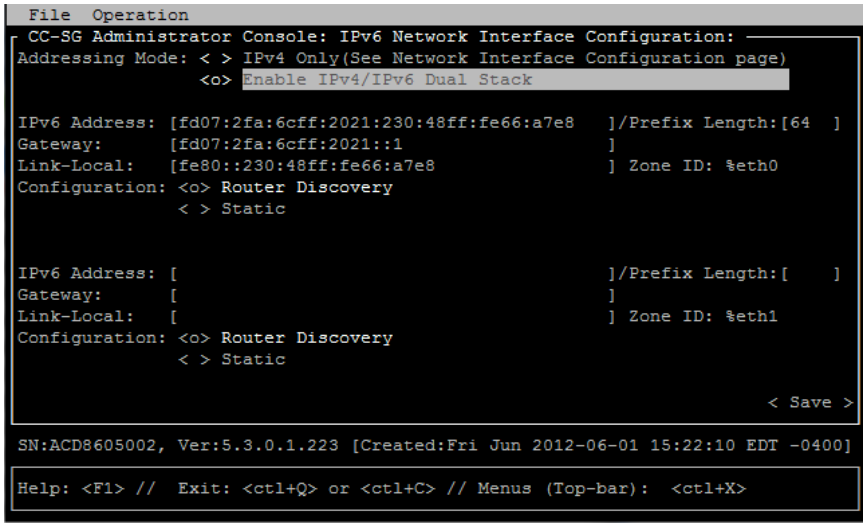
IPv4 のみを使用している場合は、[IPv4 Only(IPv4 のみ)] を選択し、[Operation(操作)] > [Network Interface Configuration(ネットワーク インタフェース設定)] ページに移動して設定を入力します。「*ネットワーク インタフェース設定の編集 『373p. の"ネットワーク インタフェース設定の編集 (ネットワーク インタフェース)"参照 』*」を参照してください。

IPv6 ネットワーク情報を入力する前に、[Operation(操作)] > [Network Interface Configuration(ネットワーク インタフェース設定)] ページで [IP Isolation (IP 分離)] モードまたは [IP Failover (IP フェイルオーバ)] モードを選択する必要があります。「*ネットワーク インタフェース設定の編集 『373p. の"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)"参照 』*」を参照してください。

1. デュアル スタックの IPv6 ネットワーク向けに CC-SG を設定するには、[Enable IPv4/IPv6 Dual Stack(IPv4/IPv6 デュアル スタックを有効にする)] を選択します。
2. [Router Discovery(ルータ検出)] または [静的] を選択します。

   Admin Console で、[Global/Unique Local IPv6 Address(グローバル アドレスまたは固有のローカル IPv6 アドレス)] が [IPv6 Address(IPv6 アドレス)] というラベルになります。
3. [Router Discovery(ルータ検出)] を選択すると、[Global/Unique Local IPV6 Address(グローバル アドレスまたは固有のローカル IPv6 アドレス)]、[Prefix Length(プレフィックス長)]、[Default Gateway IPV6 Address(デフォルトのゲートウェイ IPv6 アドレス)]、[Link-Local IPV6 Address and Zone ID(リンクローカル IPv6 アドレスとゾーン ID)] の各フィールドが自動的に入力されます。

4. [静的] を選択すると、[Global/Unique Local IPV6 Address(グローバルアドレスまたは固有のローカル IPv6 アドレス)]、[Prefix Length(プレフィックス長)]、および [Default Gateway IPV6 Address(デフォルトのゲートウェイ IPv6 アドレス)] が入力されます。



5. [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。
6. 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 が許可されているかを確認してください。

1. [Operation] > [Network Interfaces] > [Ping] を選択します。
2. 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。

4. 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。**
5. 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*** 『*379*p. 』」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。

4. 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。
6. 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

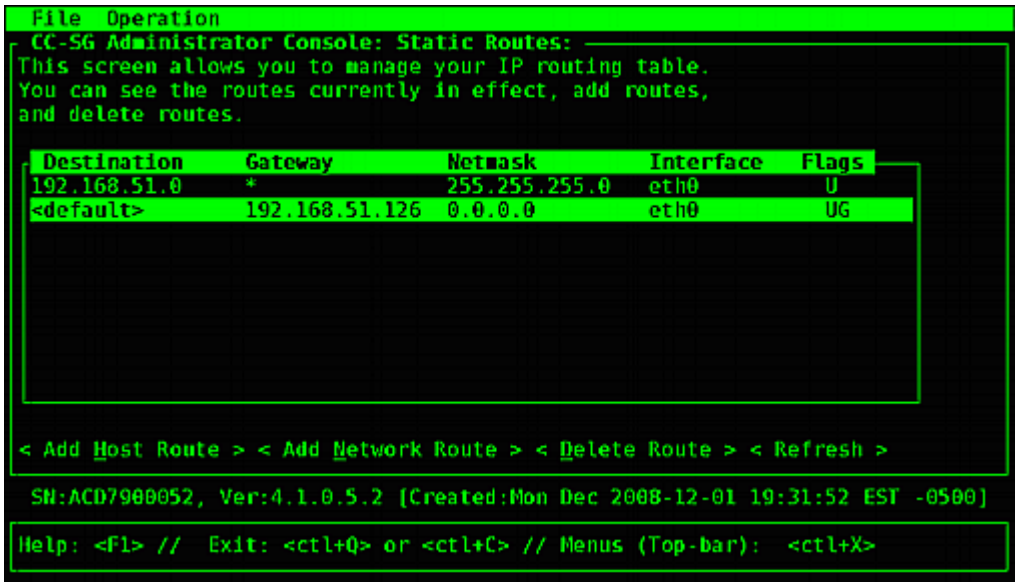
Static Routes では、現在の IP ルーティング テーブルを表示してルートを編集、追加、または削除できます。静的ルートの使用と配置を慎重に設定することで、実質的にネットワークのパフォーマンスが向上して、重要なビジネス アプリケーションのために帯域幅を確保することができる場合があります。マウスでクリックするか、Tab キーと矢印キーで移動して Enter キーで値を選択します。

注: IPv6 ネットワークの静的ルートを設定することもできます。[Operation] > [Network Interfaces] > [Static Routes] を選択します。こうしたルートは、CC-SG の再起動後またはフェイルオーバ後には保存されていません。

▶ **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。
2. 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。



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 = 日

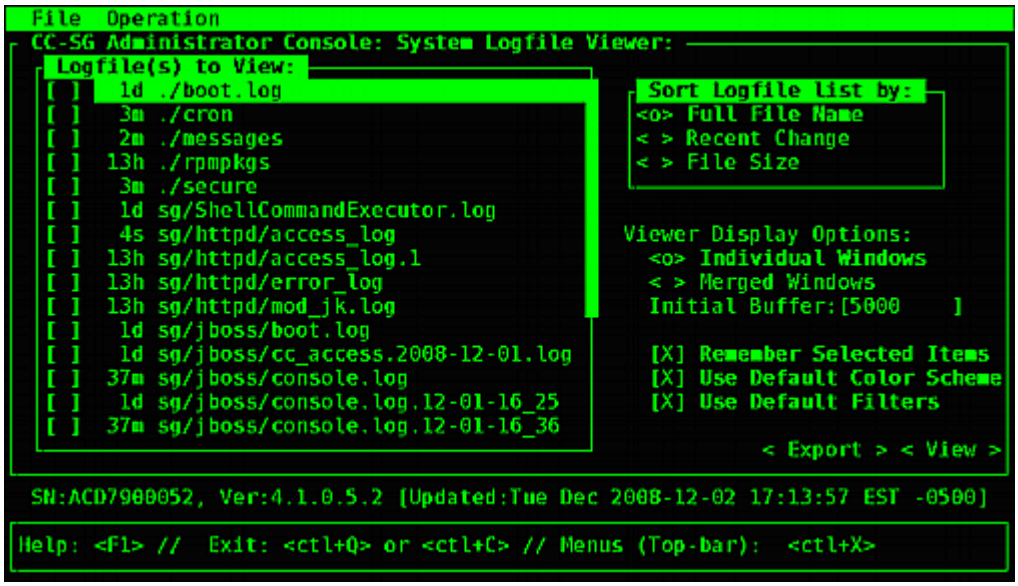
ファイル サイズ

- 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。



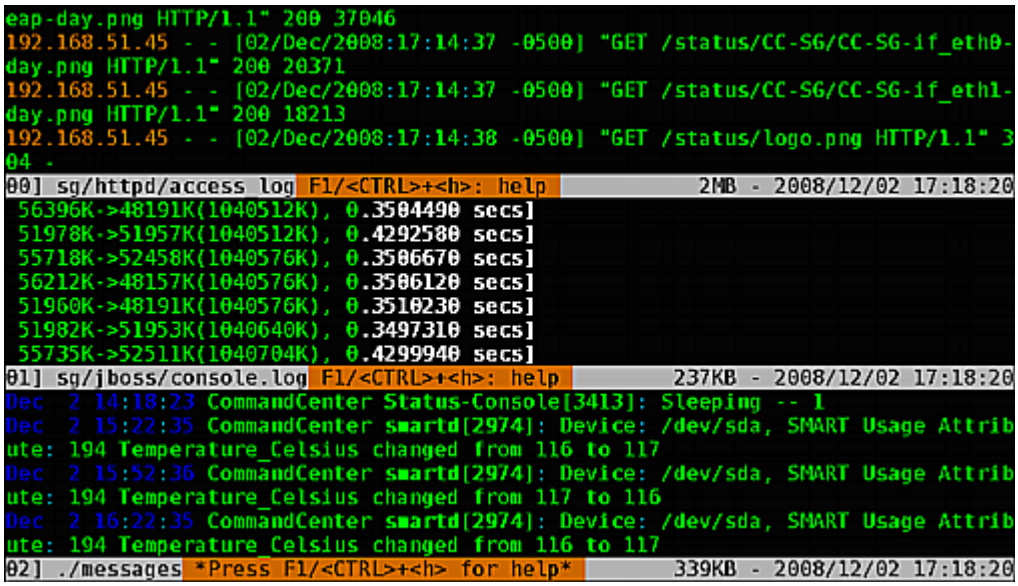
[Logfiles to View] リストを並べ替えるには、以下の手順に従います。

[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。

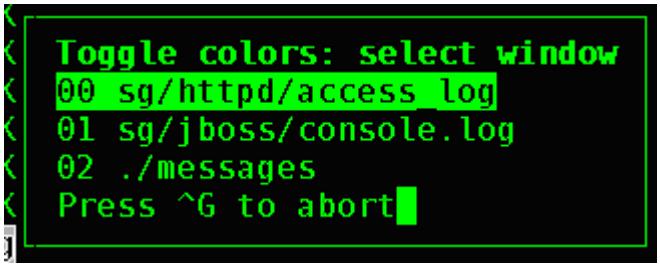
オプション	説明
Individual Windows	別のサブウィンドウが開いて選択したログが表示されます。
Merged Windows	選択したすべてのログ ファイルが 1 つの表示ウィンドウにマージされます。
Initial Buffer	初期バッファまたは履歴のサイズを設定します。デフォルトは 5000 です。このシステムは、新しく入ってきたすべての情報をバッファするように設定されています。
Remember Selected Items	このボックスを選択すると、現在のログファイルの選択情報があれば記憶されます。選択しないと、新しいログファイル リストが生成されるたびに、選択がリセットされます。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

オプション	説明
	ルタが適用されます。
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。



- 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。

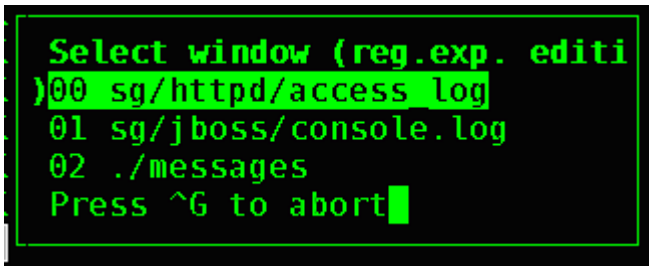


- [info] に「I」と入力すると、システム情報が表示されます。

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。



2. 「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。

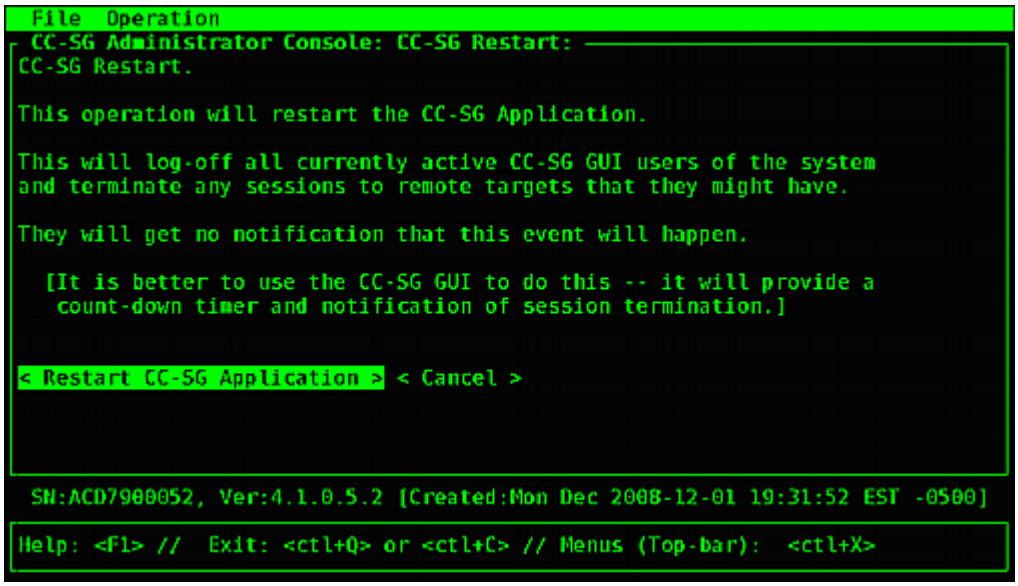
診断コンソールを使用した CC-SG の再起動

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* 『272p. 』」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。



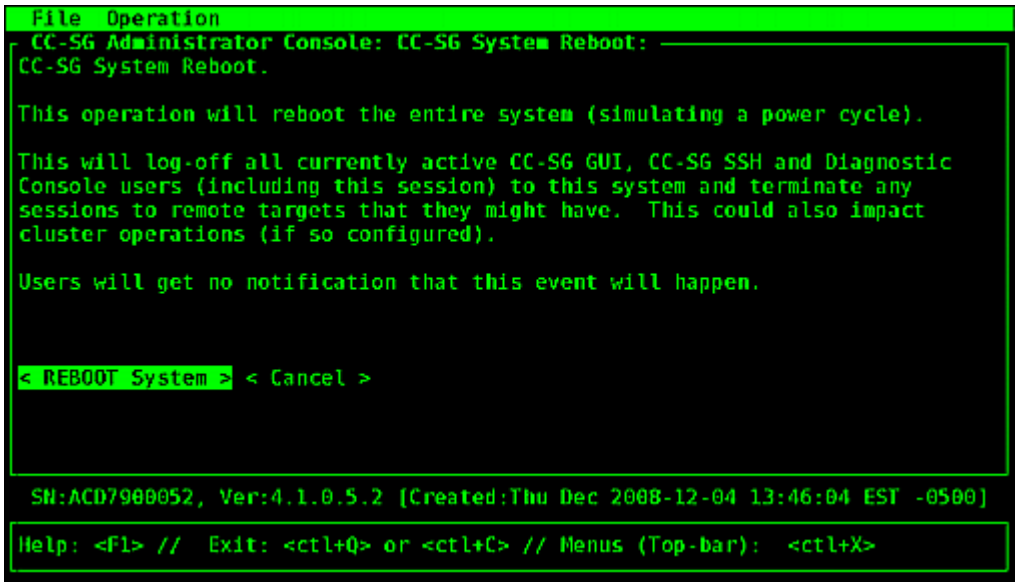
診断コンソールを使用した CC-SG のリブート

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。



診断コンソールからの CC-SG システムの電源オフ

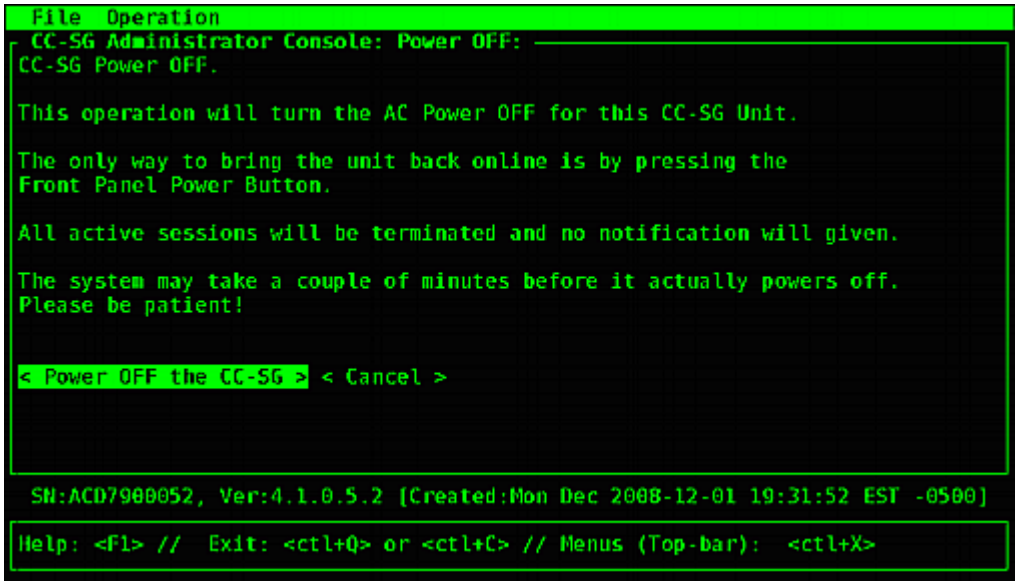
このオプションでは、CC-SG ユニットの電源がオフになります。ログインしているユーザに通知は表示されません。CC-SG、SSH、診断コンソール ユーザ（このセッションを含む）がログオフされます。リモート ターゲット サーバへの接続もすべて終了します。

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。**

1. [Operation] > [Admin] > [CC-SG System Power OFF] を選択します。

2. [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。

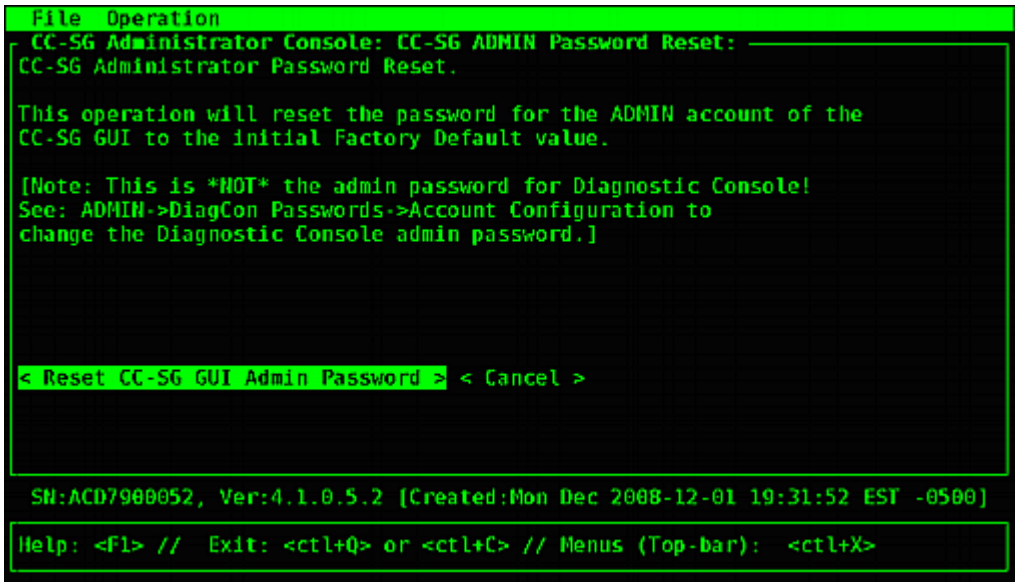
工場出荷時のデフォルト パスワード: raritan

*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** 『390p. 』」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。**

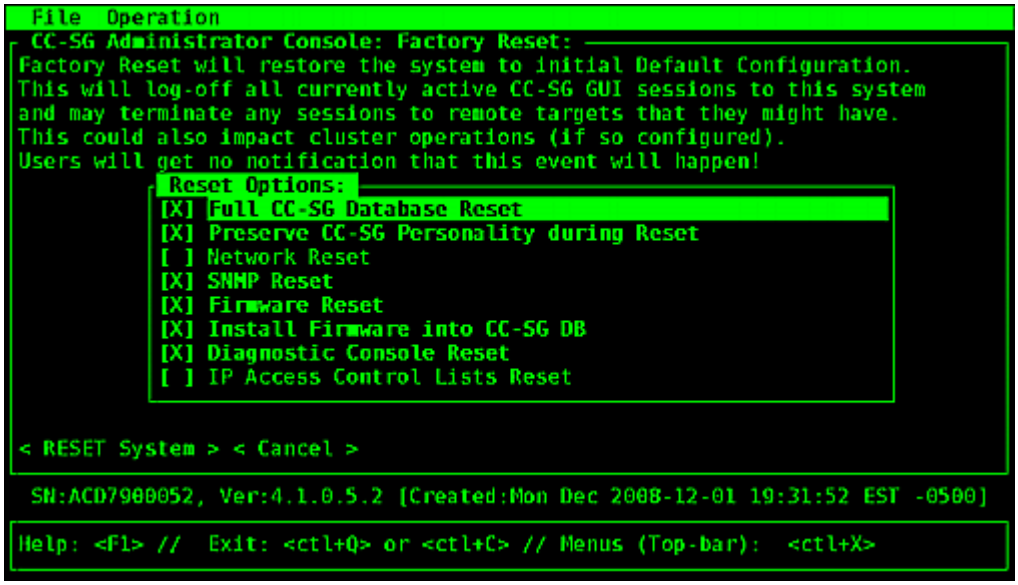
1. [Operation] > [Admin] > [CC-SG ADMIN Password Reset] を選択します。

2. [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。



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。

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 ▪ 強力なパスワードの強制 ▪ 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: 255.255.255.0 ▪ 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 ▪ SNMP トラップ構成 ▪ SNMP トラップ送信先
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

オプション	説明
	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。 「*アクセス制御リスト 『334p. 』*」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。

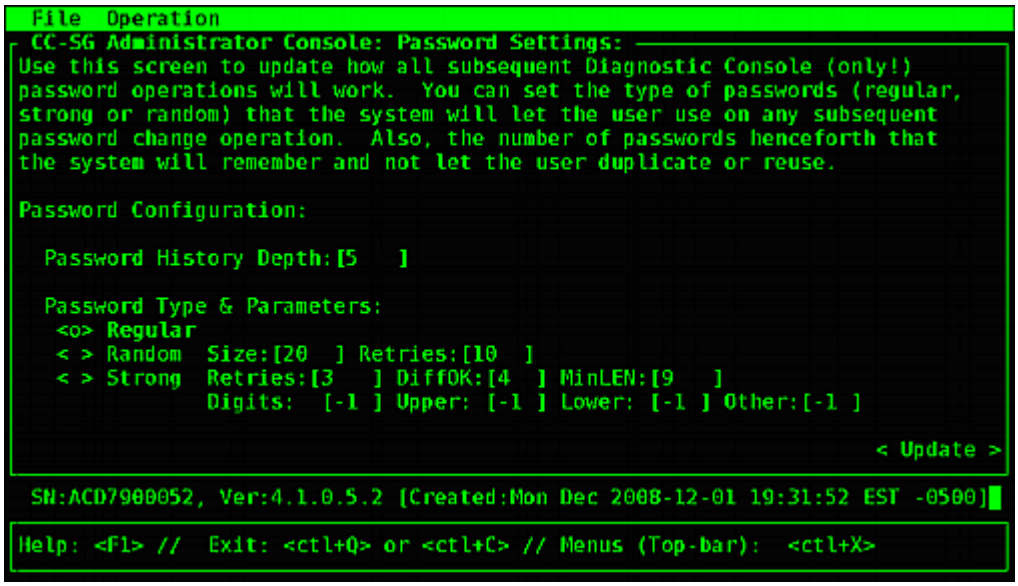
診断コンソールのパスワード設定

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。



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。

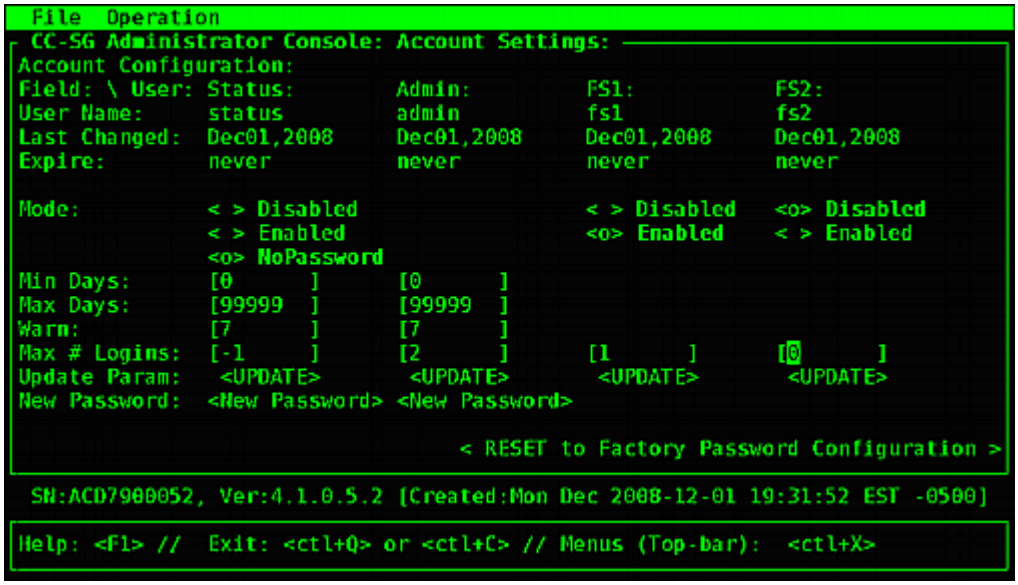
パスワード設定	説明
	負の数は、その文字クラスの文字を少なくともその数以上はパスワードに入れる必要があることを意味します。つまり、数に -1 を指定した場合、すべてのパスワードに少なくとも 1 桁の数字が必要になります。

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。



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。

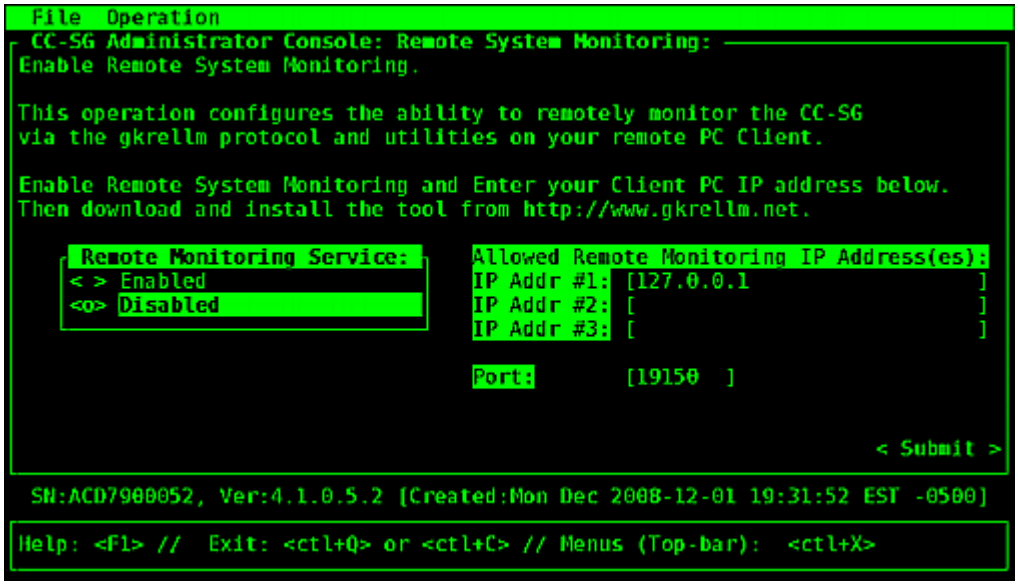
設定	説明
User ¥ User Name	(読み取り専用) このアカウントの現在のユーザ名または ID です。
Last Changed	(読み取り専用) このアカウントのパスワードを前回変更した日付です。
Expire	(読み取り専用) このアカウントのパスワードの変更が必要になる日です。
Mode	アカウントの無効 (ログイン禁止) または有効 (認証トークンが必要)、アクセス許可、およびパスワード不要などの設定可能なオプション。Admin と FS1 のアカウントを同時にロックアウトしないでください。診断コンソールを使用できなくなります。
Min Days	パスワードを変更した後、再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。



2. ［Remote Monitoring Service］フィールドで［Enabled］を選択します。
3. 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:

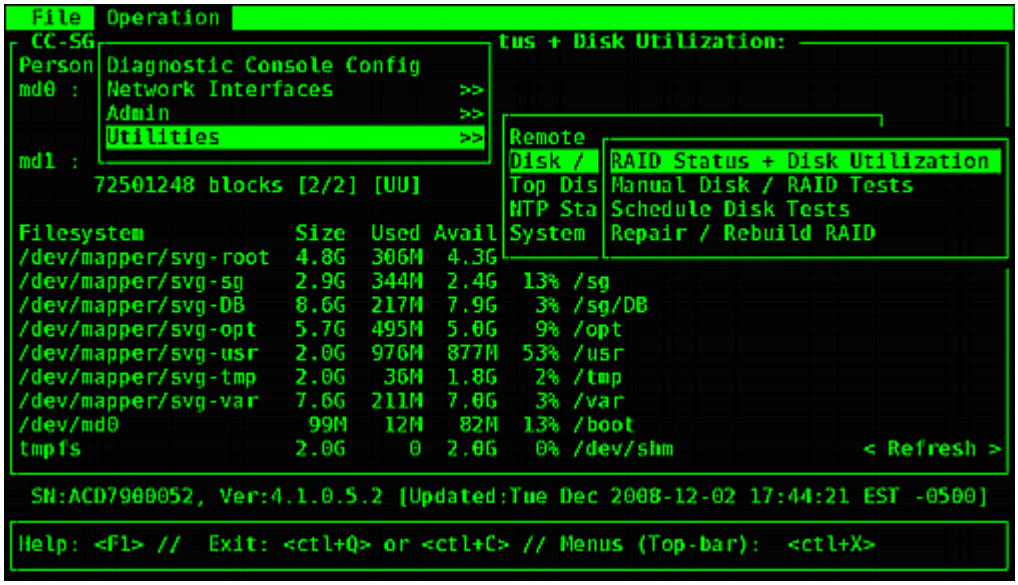
1. サポートされているインターネット ブラウザを使用して URL を「`http(s): //<IP_address>/status/`」と入力します。`<IP_address>` は、CC-SG の IP アドレスです。/status の後のスラッシュ (/) は必須です。たとえば「`https: //10.20.3.30/status/`」のように入力します。
2. ステータス ページが開きます。このページには、Status Console と同じ情報が含まれます。「*Status Console* 『*363*p. 』」を参照してください。
   - [Historical CC-SG 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。



2. [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。

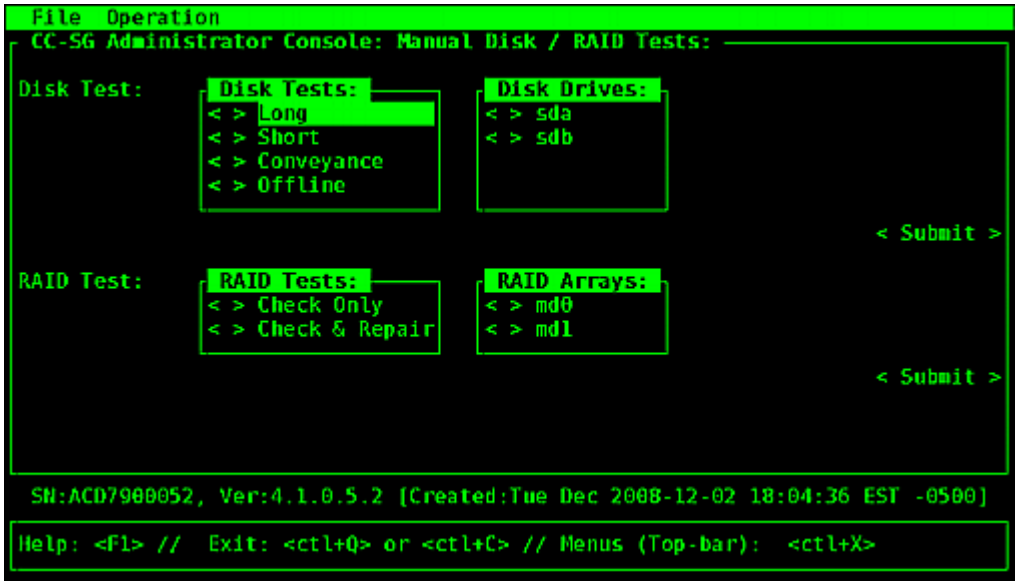
注: 上図のような画面が表示されたら、ディスク ドライブは完全に同期されており、完全な RAID-1 保護を実施できます。md0 配列と md1 配列のステータスはともに [UU] です。

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。



2. 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* 『*401*p. 』」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* 『*396*p. 』」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 『401*p. 』」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* 『*401*p. 』」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。

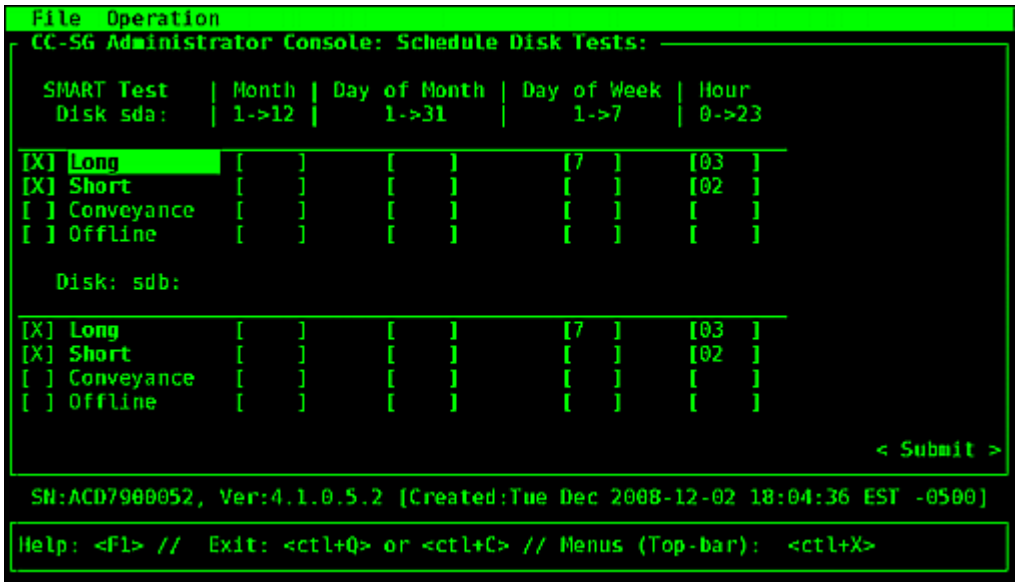
SMART テストをスケジュールする場合は、以下のガイドラインに注意してください。

- 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。



2. 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。

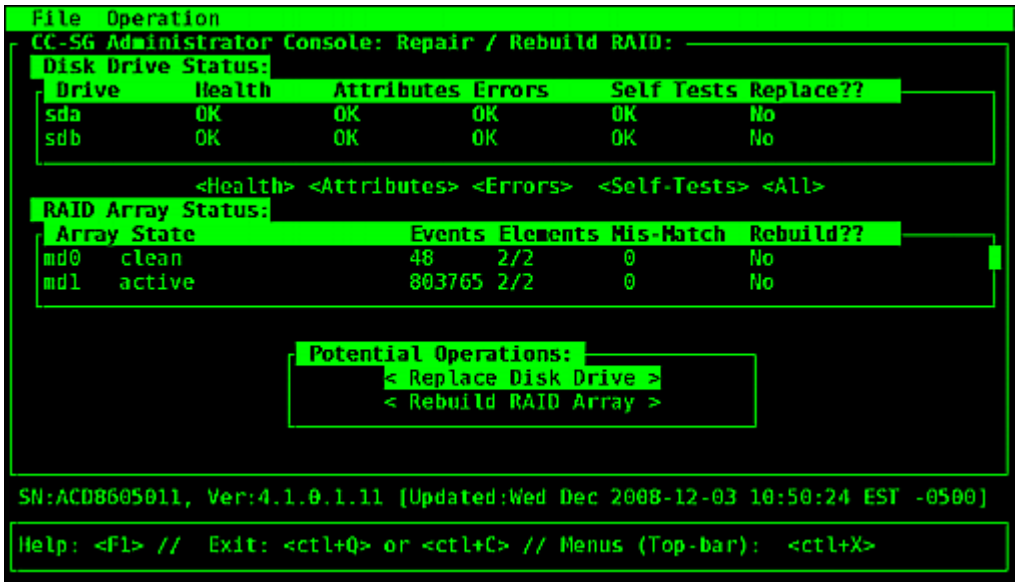
   注: フィールドを空にすると、すべての値と一致します。
4. [Submit] を選択します。

RAID ディスクの修復または再作成

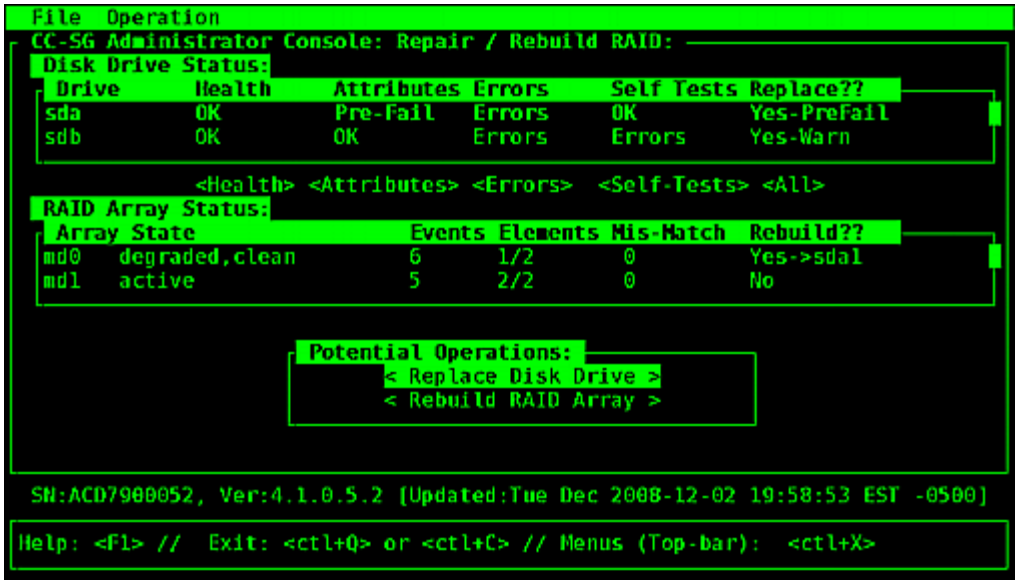
このオプションには、ディスク ドライブおよび RAID アレイの詳細なステータス情報の一部が表示され、また、ディスク ドライブの交換や RAID-1 ミラー アレイの再作成が必要かどうかが示されます。ディスク ドライブの交換またはホット スワップを行う前に、ラリタン社から交換ユニットを入手します。

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:



- 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。

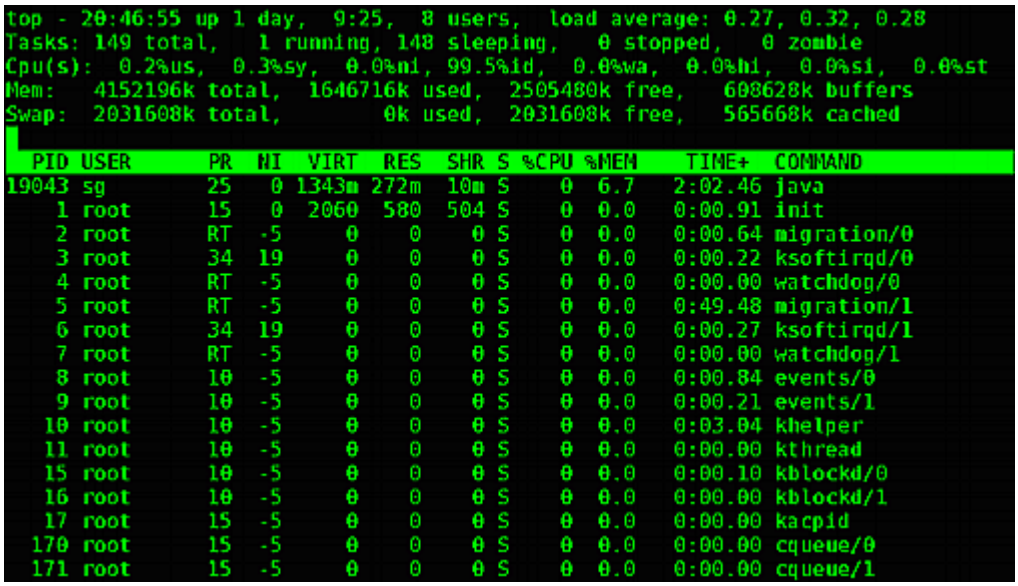
診断コンソールでのトップ ディスプレイの表示

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(操作)] > [Utilities(ユーティリティ)] > [Top Display(トップ ディスプレイ)] 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。



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。

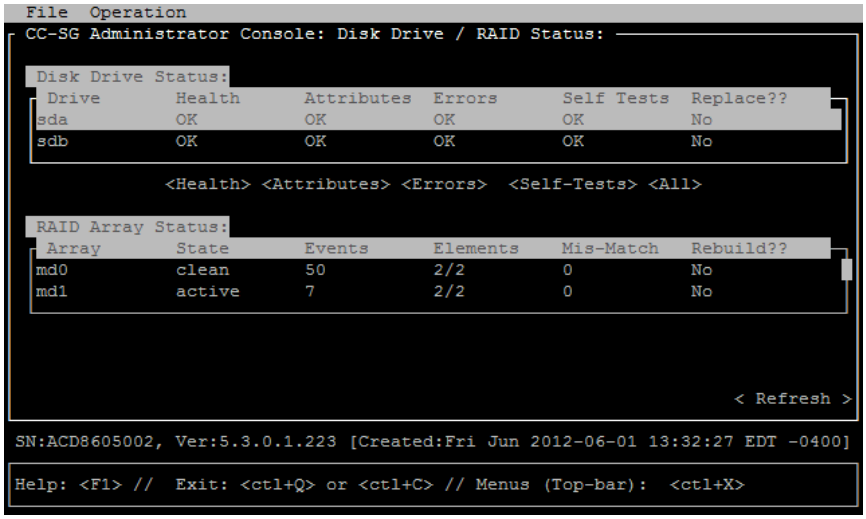
ディスク ステータスの確認

CC-SG のファームウェアアップグレードを開始する前に、CC-SG ディスク ステータスを確認します。**ドライブを交換する必要がある、ドライブに問題がある、RAID アレイを再構築する必要がある、ステータスに問題がある、などが示される場合は、ファームウェアをアップグレードする前に Raritan のテクニカル サポートまでお問い合わせください。**「*CC-SG のアップグレード* 『*273*p. 』」を参照してください。

▶ ディスク ステータスを確認するには、以下の手順に従います。

1. [Operation(操作)] > [Utilities(ユーティリティ)] > [Disk Drive / RAID Status(ディスク ドライブ/RAID ステータス)] を選択します。このオプションを使用すると、ディスク ドライブの交換や RAID アレイの再構築を開始できなくても、ステータスを表示できます。

2. ディスク ドライブを交換する必要がないこと、およびディスク ドライブが問題のある状態でないことを確認します。



NTP ステータスの表示

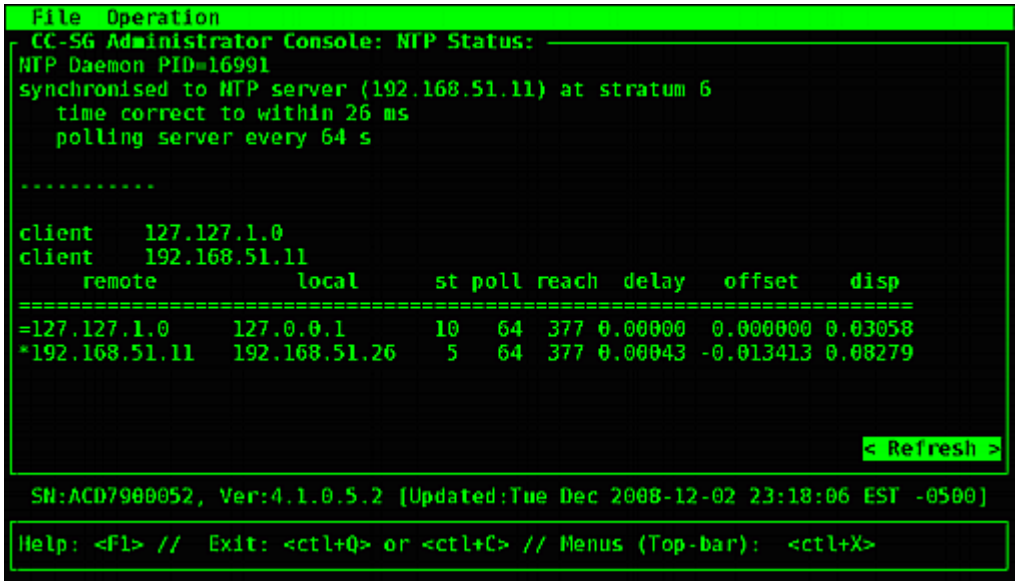
CC-SG で NTP タイム デーモンが設定され、稼働中であれば、そのステータスを表示できます。NTP デーモンは、CC-SG 管理者の GUI である Admin Client でしか設定できません。

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。

- 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。



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。
2. [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。
3. 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。
5. 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。デフォルトでは、[Clean-up JBoss heap dump(JBoss ヒープ ダンプのクリーンアップ)] オプションが選択されています。これにより、スナップショットが実行された後に JBoss ヒープ ファイルは自動的に削除されます。
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:

1. 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。
2. ［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。
4. 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。

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* 『*385*p. 』」を参照してください。
2. 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。

IPv6 では、Power IQ との通信はサポートされていません。

1. 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 『416p. 』*」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 『414p. 』*」を参照してください。

3. 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 『411p. 』*」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。

1. 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［Other Security Settings(その他のセキュリティ設定)］をクリックします。

   ［Web API Settings(Web API 設定)］で、［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。
2. 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。
3. 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。
4. ［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『486p. 』*」を参照してください。
5. ［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。
6. 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。**
9. ［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* 『*410*p. 』」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* 『*411*p. 』」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* 『*409*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。)	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。)	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* 『*121*p. 』」を参照してください。
2. 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* 『*138*p. 』」および「*Power IQ Proxy のパワー制御接続のインタフェース* 『*149*p. 』」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、繰り返し実行するタスクを設定できます。「*タスク マネージャ* 『*337*p. 』」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* 『*409*p. 』」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。

1. [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 『413p. 』」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)
2. [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 『412p. 』*」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 『411p. 』*」および「*Power IQ 同期ポリシー 『413p. 』*」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。

1. [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。

1. "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* 『*339*p. 』」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* 『*411*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* 『*408*p. 』」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です。

列番号	タグまたは値	詳細
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

1. 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*『*446*p. 』」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* 『*445*p. 』」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

1. [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 A V1 および E1 の仕様

この章の内容

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% ～ 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
衝撃	なし
非動作時	
温度	–40° – +60° (–40° –140°)

動作時	
湿度	5% ～ 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

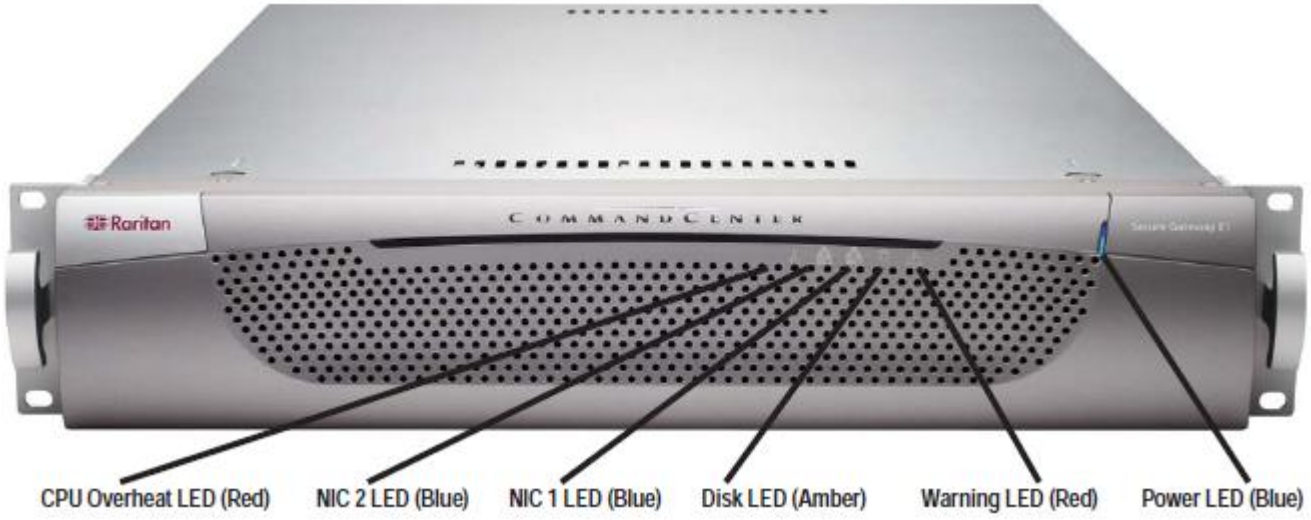
フォーム ファクタ	2U
外形寸法（幅 x 奥行き x 高さ）	27.05”x 18.7” x 3.46”-687 mm x 475 mm x 88 mm
重量	20 kg
電源	SP502-2S ホットスワップ可能 500W 2U 電源
動作温度	0 ～ 50° C
平均故障間隔（MTBF）	53,564 時間
KVM 管理ポート数	PS/2 キーボード/マウス ポート、1 VGA ポート
シリアル管理ポート	UART 16550 高速シリアル ポート
コンソール ポート	2 x USB 2.0 ポート

E1 環境要件

動作時	
湿度	5 ～ 90%、結露なし
海抜高度	海抜 2,500 m まで
振動	毎時 0.5 g 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 5 g/11 ms X 軸、Y 軸、Z 軸方向）

動作時 非動作時	
温度	-40 ～ 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 2 g 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)

E1 モデル ユニットの LED



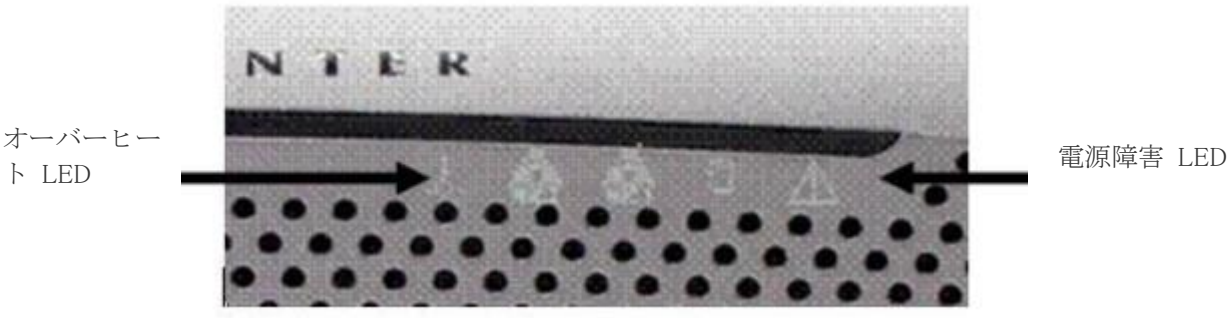
1	CPU オーバーヒート LED - 赤	「*E1 モデル ユニットの音響アラームと赤色 LED* 『*420*p. 』」を参照してください。
2	NIC 2/LAN 2 LED - 青	点灯する場合は、LAN 2 が動作しています。
3	NIC 1/LAN 1 LED - 青	点灯する場合は、LAN 1 が動作しています。
4	ディスク LED - オレンジ	点灯する場合は、ハードディスクが動作しています。
5	警告 LED - 赤	「*E1 モデル ユニットの音響アラームと赤色 LED* 『*420*p. 』」を参照してください。

6	電源 LED – 青	点灯する場合は、CC-SG ユニットの電源がオンになっています。

E1 モデル ユニットの音響アラームと赤色 LED

E1 アプライアンスには 2 つの赤色のインジケータがあります。

電源障害およびオーバーヒート。どちらも音響アラームが生成されます。



通常、電源障害 LED は、ユニットに両方の電源コードが接続されていないことが原因で点灯します。実際の電源装置に障害が発生している場合もあります。

オーバーヒート LED は、ヒートシンクの取り付けが緩いか適切でない、ファンが回転していないなどの原因でシステムが過熱状態にある場合に点灯します。動作温度については、「*E1 一般仕様* 『*418*p. 』」を参照してください。

Ap B CC-SG およびネットワーク設定

この付録では、一般的な CC-SG 導入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 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	TCP	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	TCP	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	TCP	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	可	ハートビート
CC-SG → リモート LAN IP	5000	UDP	可	ハートビート
CC-SG → Raritan デバイス	5000	TCP	可	RDM プロトコル RC4/AES-128/AES-256 暗号化。
Raritan デバイス → CC-SG	5001	UDP	不可	ハートビート
CC-SG → Dominion PX	623 443	UDP	不可 不可	
CC-SG → Dominion KXII（ダ	443	TCP	不可	

通信方向	ポート番号	プロトコル	設定可否	詳細
イレクト モード)				

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-SG → CC-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-SG → CC-SG	3232	TCP	不可	プライマリ バックアップ SNMP 同期構成変更転送。

通信方向	ポート番号	プロトコル	設定可否	詳細
				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 → CC-SG	68	UDP	不可	IPv4 DHCP 標準
CC-SG → DHCP サーバ	67	UDP	不可	IPv4 DHCP 標準
NTP サーバ → CC-SG	123	UDP	不可	NTP 標準
CC-SG → DNS	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	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。
PC クライアント→ CC SG	80	TCP	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。
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

通信方向	ポート番号	プロトコル	設定可否	詳細
				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	TCP	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→診断コンソール	23	TCP	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)	TCP	不可	クライアント - サーバ通信。 暗号化されません。
クライアント → Raritan デバイス→アウト オブ バンド KVM ノード	5000 (Raritan デバイス上)	TCP	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

通信方向	ポート番号	プロトコル	設定可否	詳細
(ダイレクト モード)				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	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。

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-SG → IPMI	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
CC-SG → DRAC	80 または 443	TCP	不可	ベンダ標準
CC-SG → RSA	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 →	161	UDP	可	SNMP 標準

通信方向	ポート番号	プロトコル	設定可否	詳細
CC-SG				
CC-SG → SNMP マネージャ	162	UDP	可	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*** *『300*p. *』*」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*** *『394*p. *』*」を参照してください。

Ap C 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	このメニューおよびユーザ ツリーは、ユーザ管理権限を持つユーザのみが使用できます。		
> 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	

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	このメニューおよびデバイス ツリーは、次のいずれかの権限を持つユーザのみが使用できます。 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	このメニューおよびノード ツリーは、次のいずれかの権限を持つユーザのみが使用できます。 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		
	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	> カスタム表示の作成	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	
	> 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、ユーザ セキュリティ管理の権限を持つユーザのみが使用できます。		
	> 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、ユーザ管理権限を持つユーザが使用できます。ただし、ユーザ セキュリティ管理の権限のみを持つユーザは除きます。		
	監査証跡	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 データを表示する場合:[なし]	
	> 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ザのみが使用できます。 CC の設定と制御 デバイス、ポート、およびノードの管理、ユーザ管理、ユーザ セキュリティ管理の組み合わせ		
	ガイド付き設定	次のすべて: デバイス、ポート、およびノードの管理、ユーザ管理、ユーザ セキュリティ管理	
	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。
ccUserLockedOut	CC-SG ユーザはロックアウトされています。

SNMP トラップ	説明
ccDeviceAddedAfterCCNOCNotification	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。
ccCSVFileTransferred	CSV ファイルがインポートされました。

SNMP トラップ	説明
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

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* 『*486*p. 』」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、

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 キャッシュのクリア* 『*275*p. 』」および「*CJava キャッシュのクリア* 『*275*p. 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* 『*275*p. 』」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。

Ap G 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

メモリ診断

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* 『*385*p. 』」を参照してください。
2. 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。
4. 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:

1. 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。
4. [`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 『406*p. 』」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。

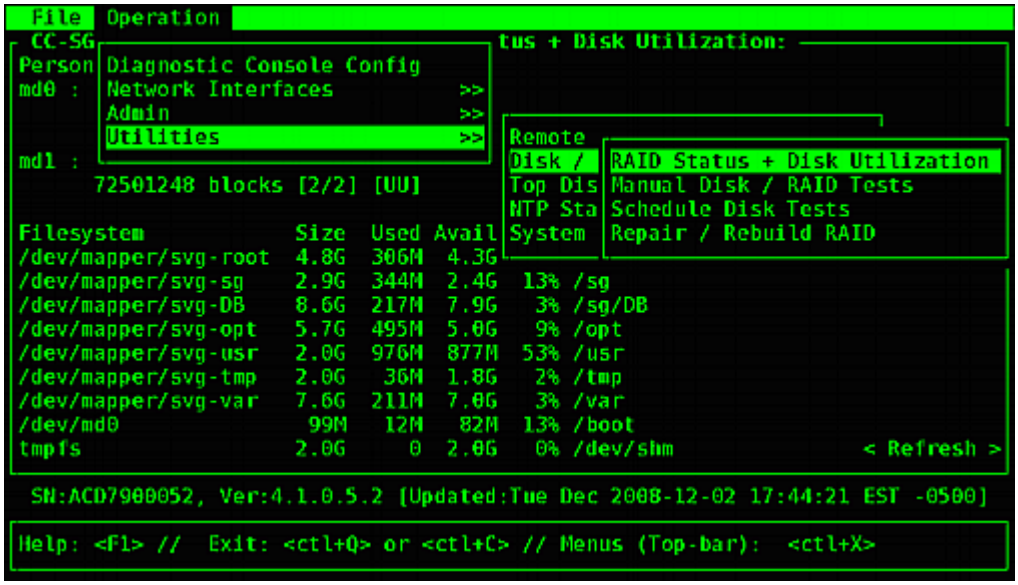
CC-SG ディスク監視

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* 『*394*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。

1. 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* 『*396*p. 』」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。



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	1. 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* 『*406*p. 』」を参照してください。 2. [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* 『*406*p. 』」を参照してください。 3. [Pre-Clean-up SNAP] 領域を選択します。 4. [Pre-Clean-up UPLOAD] 領域を選択します。 5. [SNAP] を選択解除します。 6. [Package & Export] を選択解除します。 7. [Submit] をクリック、または選択します。 8. 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、それらを CC-SG から削除します。
/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）	1. [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* 『*406*p. 』」を参照してください。 2. [SNAP] を選択解除します。 3. [Package & Export] を選択解除します。 4. [Clean-up /tmp] を選択します。 5. [Submit] をクリック、または選択します。
/sg	CC-SG 管理対象デバイスのファームウェア ファイル。	Admin Client で、[管理] > [ファームウェア] を選択します。追加しようとしているファームウェア ファイルがまだ存在していないことを確認します。 ディレクトリ使用率が 85% を超えている場合は、不要なデバイス ファームウェア ファイルを削除してください。Admin Client で、[管理] > [ファームウェア] を選択し、削除するファームウェア ファイルを選択します。

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『363*p. *』*」を参照してください。

1. 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

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 Dominion KX2 デュアル ビデオ ポートの設定および推奨設定

この章の内容

概要

ビデオ カードを 2 枚搭載したサーバには、拡張デスクトップ設定を利用してリモートからアクセスできます。この設定は、リモート ユーザが利用できます。このためには、デュアル ポート ビデオ グループを作成します。

拡張デスクトップ設定により、標準的な 1 台のモニタでの表示に対して 2 台のモニタでターゲット サーバのデスクトップを表示できるようになります。デュアル ポート ビデオ グループを選択すると、そのグループのポート チャネルがすべて同時に開かれます。デュアル ポート ビデオ グループの作成方法については、「*デュアル ビデオ ポート グループの作成* 『*463*p. 』」を参照してください。

デュアル ポート ビデオ グループに関する重要な情報については、このセクションの内容を確認してください。

注: デュアル ポート ビデオ グループは、KX2-108 や KX2-116 のような、KVM チャネルが 1 つしかない CommandCenter Secure Gateway モデルではサポートされません。

CC-SG でのデュアル ポート ビデオの設定および使用

デュアル ビデオ ポートは、アウト オブ バンド KVM ポートとしての CC-SG を意味します。ポートがグループになっている場合は、設定に関する以下の注意事項が適用されます。

- **Admin Client でデュアル ビデオ ポートを設定するには、以下の手順に従います。**

プライマリ ポートを設定すると、セカンダリ ポートも設定されます。セカンダリ ポートでの制御は無効です。プライマリ ポートからのみ接続または切断できます。プライマリ ポートからのみ接続アプリケーションを選択します。アプリケーションの選択は、セカンダリ ポートに適用されます。

- **CSV ファイルのインポートを介してデュアル ビデオ ポートを設定するには、以下の手順に従います。**

デュアル ビデオ ポート グループをインポートする場合は、両方のポートを設定する必要があります。そうしなければ、操作が失敗します。エラー メッセージでは、デュアル ディスプレイ ポート グループのプライマリ ポートとセカンダリ ポートの両方を設定する必要があることが示されます。

- **デュアル ビデオ ポートを削除するには、以下の手順に従います。**

デュアル ビデオ ポート グループに含まれているポートを削除する場合は、プライマリ ポートを削除します。プライマリ ポートを削除すると、セカンダリ ポートも削除されます。

CSV ファイルのインポートを利用してポートを削除する場合は、両方のポートを指定する必要があります。そうしなければ、操作は失敗します。

- **デュアル ビデオ ポートに関連付けられているノードに接続するには、以下の手順に従います。**

プライマリ ポートに関連付けられているノード (プライマリ ノード) からのみ接続または切断できます。プライマリ ノードにのみインタフェースを追加できます。セカンダリ ポートに関連付けられているノードでの制御は無効です。

- **デュアル ビデオ ポートが含まれているノード グループを設定するには、以下の手順に従います。**

グループのノードを選択する場合は、デュアル ビデオ ポートの 1 つを選択すると、もう 1 つのポートは自動的に選択されます。ポートは、グループに対してペアでしか追加または削除できません。

デュアル ビデオ ポートでブックマークや直接接続 URL を使用するには、以下の手順に従います。

ブックマークおよび直接接続 URL は、デュアル ビデオ ポート グループのプライマリ ノードおよびセカンダリ ノードの両方で利用できますが、セカンダリ ノードへの接続は失敗します。セカンダリ ノードへの接続要求は拒否されます。

ユーザに対して、ブックマークまたは URL によってセカンダリ ポートに接続しようとしていることを示す通知「Connection to port denied.(ポートへの接続が拒否されました。)Contact your system administrator.(システム管理者にお問い合わせください。)」が表示されます。

デュアル ビデオ ポートへのアクセスを設定するには、以下の手順に従います。

デュアル ビデオ ポート グループ内のポートおよびノードにアクセスするための許可が必要です。プライマリ ノードおよびセカンダリ ノードの両方が CC-SG の同じノード グループに追加されているのを確認することをお勧めします。

両方のポートへのアクセス許可がない場合、Admin Client はプライマリ ノードを示しますが、すべての制御は無効になり、ノード プロファイルの［情報］セクションに、ユーザがセカンダリ ポート ノードにもアクセスする必要があることを示すメッセージが表示されます。Access Client はプライマリ ノードを示しますが、すべてのハイパーリンクおよび制御は無効になり、ユーザがセカンダリ ポート ノードにもアクセスする必要があることを示すメッセージが表示されます。

KX2 デバイスレベルのプライベート モードによるデュアル ビデオ ポートへの接続:

KX2 がデバイスレベルのプライベート モードで動作している場合、どちらかのポートがビジー状態であれば、KX2 では両方の接続要求が拒否されます。この動作は、VM 共有モードで排他アクセスが必要な場合にも発生します。

KVM セッション制限付きでのデュアル ビデオ ポートの使用:

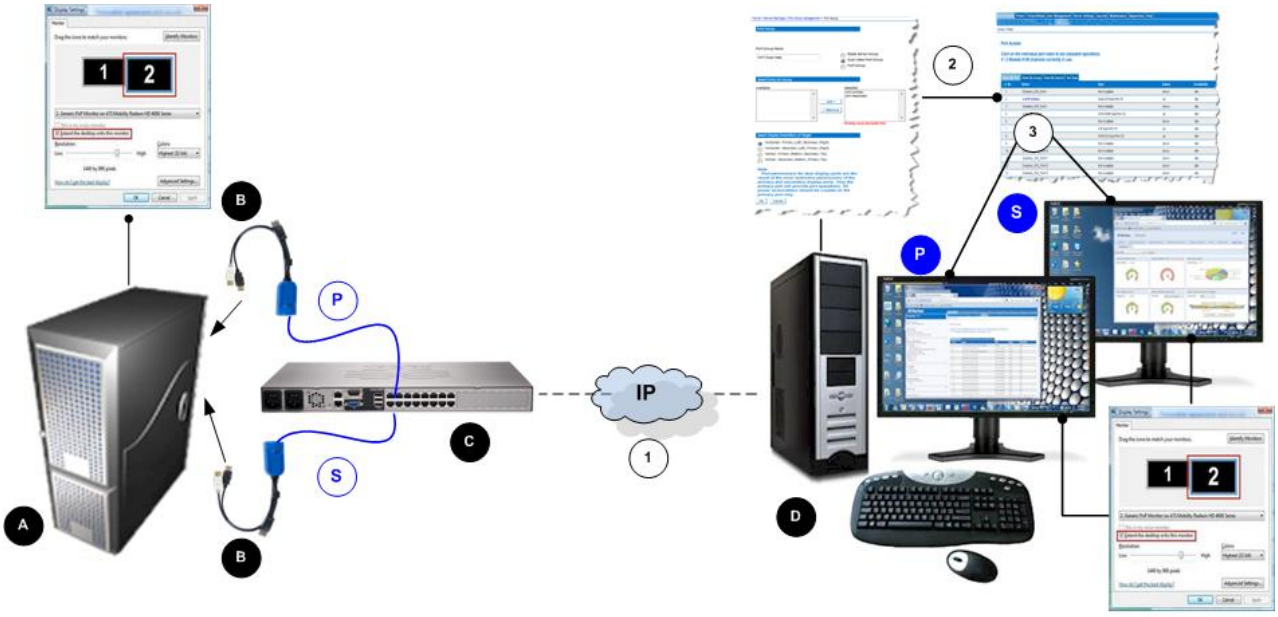
KVM セッション制限が有効になっている場合は、ユーザが 2 つのセッションを利用できなければ、どちらの接続も拒否されます。

デュアル ポート ビデオ グループ設定の例

以下の手順は、一般的な例として示しています。設定は、使用する CIM のタイプ、プライマリ ポートとして指定するポート、接続先の CommandCenter Secure Gateway ポートなどによって変わる可能性があります。

この例では、以下を前提にしています。

- 2 つのビデオ ポートを搭載したターゲット サーバ
- ターゲット サーバのビデオ ポート 1 がプライマリ ポート、およびビデオ ポート 2 がセカンダリ ポート
- CommandCenter Secure Gateway-832 デバイス
- D2CIM-DVUSB-DP CIM
- Microsoft® Windows 7® オペレーティング システムが稼動しているターゲット サーバおよびリモート クライアント
- インテリジェント マウス モード
- ターゲット サーバおよびリモート クライアントで拡張デスクトップを表示するので、画面の方向が「水平 - プライマリ（左）、セカンダリ（右）」になるように CommandCenter Secure Gateway を設定しています。



図の説明	
A	ターゲット サーバ
B	デジタル CIM
C	CommandCenter Secure Gateway
D	リモート クライアント
P	ターゲットの最初のビデオ ポートから CommandCenter Secure Gateway への接続
S	ターゲットの 2 番目のビデオ ポートから CommandCenter Secure Gateway への接続
1	CommandCenter Secure Gateway とリモート クライアント間の IP 接続
2	CommandCenter Secure Gateway でのデュアル ビデオ ポート グループの作成
3	デュアル ビデオ ポート グループを開く
P	プライマリ ポートの表示（CommandCenter Secure Gateway の［Port Group Management］（ポート グループ管理）ページで定義済み）
S	セカンダリ ポートの表示（CommandCenter Secure Gateway の［Port Group Management］（ポート グループ管理）ページで定義済み）

手順 1: ターゲット サーバの画面の設定

CommandCenter Secure Gateway で設定されている、ターゲットの方向設定が、ターゲットのオペレーティング システムでの実際の設定と一致している必要があります。できれば、接続元のクライアントの画面方向が同じに設定されていることが望まれます。

画面の方向およびマウス モードについては、「デュアル ビデオ ポート グループの画面の方向、位置合わせ、およびマウス モード」を確認してください。

注: 画面の設定の指定方法に関する正確な手順については、ターゲット サーバまたはオペレーティング システムのユーザ マニュアルを参照してください。

▶ **ターゲット サーバの画面の設定およびマウスの設定を指定するには、以下の手順に従います。**

1. ターゲット サーバで、ビデオ ポートごとにターゲット サーバの画面の方向を、リモート クライアントの画面の方向と一致するように設定します。

   たとえば、リモート クライアントで 2 つのモニタにわたって左から右に移動するように拡張デスクトップの方向を設定している場合は、ターゲット サーバの画面の方向を同じに設定します。
2. ターゲット サーバのビデオが、サポートされている解像度とリフレッシュ レートに設定されていることを確認します。「サポートされている画面解像度」を参照してください。

   注: ターゲットのプライマリ画面およびセカンダリ画面が異なる解像度に設定されている場合、マウスは同期が維持されなくなるので、左上のターゲット ウィンドウで定期的に再同期する必要があります。

手順 2: CommandCenter Secure Gateway へのターゲット サーバの接続

デュアル ポート ビデオ グループは、既存のポート接続または新しいポート接続から作成できます。ここに示す手順では、新しい接続を作成すると想定しています。既存の接続からデュアル ポート ビデオ グループを作成する場合は、「*手順 4: デュアル ビデオ ポート グループの作成* 『*462*p. 』」を参照してください。

▶ **機器を接続するには、以下の手順に従います。**

1. まだの場合は、製造元の手順に従ってターゲット サーバを設置し、電源を投入します。

2. 各 CIM のビデオ コネクタをターゲットの各ビデオ出力ポートに接続し、USB ケーブルをターゲット上の使用可能な USB ポートに接続します。
3. CAT5/6 ケーブルを使用して各 CIM を CommandCenter Secure Gateway に接続します。
4. まだの場合は、用意されている電源ケーブルを使用して CommandCenter Secure Gateway を AC 電源に接続し、CommandCenter Secure Gateway のネットワーク ポートとローカル ポート（必要な場合）に接続して、CommandCenter Secure Gateway を設定します。CommandCenter Secure Gateway の使用を開始するために必要な手順については、「入門」を参照してください。
5. CommandCenter Secure Gateway には、Microsoft .NET® または Java Runtime Environment® (JRE) がインストールされている、ネットワーク接続機能を備えた任意のコンピュータからログインできます (JRE® は *Java の Web サイト http://java.sun.com/*から入手できます)。
6. サポートされている Web ブラウザ (Internet Explorer® や Firefox® など) を起動します。
7. .NET の URL 「*http://IP-ADDRESS*」または「*http://IP-ADDRESS/akc*」を入力します。IP-ADDRESS は CommandCenter Secure Gateway に割り当てられる IP アドレスです。また、HTTPS を使用することや、管理者によって割り当てられた CommandCenter Secure Gateway の DNS 名を使用することもできます (DNS サーバが設定されている場合)。IP アドレスをそのまま入力してもかまいません (CommandCenter Secure Gateway では常に IP アドレスが HTTP から HTTPS にリダイレクトされます)。
8. ユーザ名とパスワードを入力します。[Login] (ログイン) をクリックします。
9. ターゲット サーバのマウス モードを設定します。

   たとえば、リモート クライアントでインテリジェント マウス モードを使用している場合は、インテリジェント マウス モードを使用するようにターゲット サーバを設定します。使用しているオペレーティング システムに基づいて適用する必要があるマウス モードの設定については、「マウスの設定」を参照してください。

手順 3: マウス モードおよびポートの設定

ターゲット サーバのビデオ ポートを介してターゲット サーバを CommandCenter Secure Gateway に接続すると、CommandCenter Secure Gateway で接続が検出され、[Port Configuration] (ポート設定) ページに該当するポートが表示されます。手順については、「標準ターゲット サーバの設定」を参照してください。

ポートを設定した後に、それらのポートをデュアル ビデオ ポート グループにまとめることができます。

*注: 設定済みの既存のポートを設定する必要はありません。デュアル ポート ビデオ グループの作成方法については、「**デュアル ビデオ ポート グループの作成** 『463p. 』」を参照してください。*

ターゲットに接続した後にターゲット サーバのマウス モードを設定します。たとえば、リモート クライアントでインテリジェント マウス モードを使用している場合は、インテリジェント マウス モードを使用するようにターゲット サーバを設定します。使用しているオペレーティング システムに基づいて適用する必要があるマウス モードの設定については、「マウスの設定」を参照してください。

手順 4: デュアル ビデオ ポート グループの作成

「*デュアル ビデオ ポート グループの作成* 『*463*p. 』」を参照してください。

デュアル ビデオ ポート グループの作成

デュアル ビデオ ポート グループ機能により、2 つのビデオ ポートを 1 つのグループにまとめることができます。この機能は、2 つのビデオ カードまたはビデオ ポートを搭載したサーバに接続する必要がある場合や、同じリモート クライアントから同時に両方のポートにアクセスする場合に使用します。

注: デュアル ポート ビデオ グループは、KX2-108 や KX2-116 のような、KVM チャネルが 1 つしかない CommandCenter Secure Gateway モデルではサポートされません。

注: デュアル ビデオ ポート グループは、作成すると、ローカル コンソールおよびリモート クライアントから利用できます。ただし、ローカル コンソールでは拡張デスクトップはサポートされていません。

デュアル ビデオ ポート グループは、[Port Access] (ポート アクセス) ページにデュアル ポート タイプとして表示されます。ポート グループに属しているプライマリ ポートおよびセカンダリ ポートは、[Port Access] (ポート アクセス) ページに、それぞれ [Dual Port (P)] (デュアル ポート (P)) および [Dual Port (S)] (デュアル ポート (S)) として表示されます。たとえば、CIM タイプが DCIM である場合は、[DCIM Dual Port (P)] (DCIM デュアル ポート (P)) が表示されます。

各グループには、プライマリ ポートおよびセカンダリ ポートが含まれている必要があります。プライマリ ポートに適用される設定は、グループ内のすべてのセカンダリ ポートに適用されます。グループから削除されたポートは、独立したポートと見なされ、新しい設定を適用することができます。

リモート クライアントからデュアル ポート ビデオ グループにアクセスする場合は、プライマリ ポートに接続すると、デュアル ポート グループのプライマリ ポートおよびセカンダリ ポートの両方に対する KVM 接続ウィンドウが開きます。

セッションを開始し、必要に応じてリモート クライアントから 1 つ以上のモニタに表示できます。

CommandCenter Secure Gateway で設定されている、ターゲットの方向設定が、ターゲットのオペレーティング システムでの実際の設定と一致している必要があります。できれば、接続元のクライアントの画面方向が同じに設定されていることが望まれます。

重要: 特定の環境に影響を与える可能性がある制限、推奨設定などについては、「デュアル ビデオ ポート グループ」の情報を確認してください。

デュアル ポート ビデオ グループを作成するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Group Management] (ポート グループ管理) を選択します。[Port Group Management] (ポート グループ管理) ページが開きます。既存のポート グループすべてが表示されます。
2. [Add] (追加) をクリックします。[Port Group] (ポート グループ) ページが開き、利用可能なすべてのポートが [Select Ports for Group] (グループ化するポートの選択) セクションに表示されます。

   注: ポートが既にブレード サーバ ポート グループ、別のデュアル ビデオ ポート グループ、または「標準の」ポート グループに属している場合、そのポートを選択することはできません。これは、ポートは一度に 1 つのポート グループにしか属すことができないためです。
3. [Dual Video Port Group] (デュアル ビデオ ポート グループ) ラジオ ボタンを選択します。
4. [Select Ports for Group] (グループ化するポートの選択) セクションで、プライマリ ポートとして指定するポートをクリックし、[Add] (追加) をクリックして該当するポートを [Selected] (選択) テキスト ボックスに追加します。必ず最初にプライマリ ポートを追加してください。

   *注: 理想的には、ポート グループの各ポートに適用される権限は、同じでなければなりません。権限が同じでない場合は、最も制限の厳しいポートの権限がポート グループに適用されます。たとえば、あるポートに [VM Access] (VM アクセス) の [Deny] (拒否) が適用されており、別のポートに [VM Access] (VM アクセス) の [Read-Write] (読み取り/書き込み可能) が適用されている場合、ポート グループには、[VM Access] (VM アクセス) の [Deny] (拒否) が適用されます。ポートの権限によりデュアル ビデオ ポート グループがどのような影響を受けるかについては、「**権限およびデュアル ビデオ ポート グループ アクセス** 『**469***p. 』」を参照してください。*
5. セカンダリ ポートとして指定するポートをクリックし、[Add] (追加) をクリックして該当するポートを [Selected] (選択) テキスト ボックスに追加します。
6. ページの方向を選択します。選択する方向は、現在のモニタ設定に対する最適性によって異なります。
7. [OK] をクリックして、ポート グループを作成します。

デュアル ビデオ ポート グループは、[Port Access] (ポート アクセス) ページにデュアル ポート タイプとして表示されます。ポート グループに属しているプライマリ ポートおよびセカンダリ ポートは、[Port Access] (ポート アクセス) ページに、それぞれ [Dual Port (P)] (デュアル ポート (P)) および [Dual Port (S)] (デュアル ポート (S)) として表示されます。たとえば、CIM タイプが DCIM である場合は、[DCIM Dual Port (P)] (DCIM デュアル ポート (P)) が表示されます。

注: カスケード接続デバイスに接続されているデュアル ビデオ ポートのターゲットには、カスケード接続ベース デバイス以外のカスケード接続デバイスを介して接続する必要があります。

手順 5: デュアル ビデオ ポート グループを開く

デュアル ビデオ ポート グループを作成したら、そのグループを [Port Access] (ポート アクセス) ページで使用できます。プライマリ ポートをクリックしてリモートでデュアル ビデオ ポート グループに接続するには、2 つの KVM チャネルが必要です。2 つのチャネルが利用できない場合、[Connect] (接続) リンクは表示されません。

CommandCenter Secure Gateway で設定されているセッション タイムアウトは、デュアル ビデオ グループの両方のポートに適用されます。

▶ **デュアル ポート ビデオ グループを開くには、以下の手順に従います。**

- [Port Access] (ポート アクセス) ページで、プライマリ ポート名をクリックし、[Connect] (接続) をクリックします。一度に両方の接続が開かれ、2 種類のウィンドウに表示されます。

ウィンドウが表示されたら、使用している画面の設定に基づいてウィンドウを移動できます。たとえば、拡張デスクトップ モードを使用している場合は、ポート ウィンドウをモニタ間で移動できます。

デュアル ポート ビデオに関する推奨事項

マウスの同期を維持して定期的な再同期を最小限に抑えるために、ターゲット サーバのプライマリ画面およびセカンダリ画面を同じ画面解像度に設定してください。

設定する方向に応じて、上の画面（垂直方向）または左の画面（水平方向）をプライマリ画面として指定する必要があります。この画面で、仮想メディア、音声、スマート カード、およびマウスを操作するためのアクティブなメニュー選択が可能になります。

直観的なマウスの動作や制御を実現するために、クライアント PC のプライマリ画面とセカンダリ画面、CommandCenter Secure Gateway のデュアル ビデオ ポート グループ設定、およびターゲット サーバのプライマリ画面とセカンダリ画面は、画面の方向を同じにする必要があります。

デュアル ポート ビデオ画面には、次のクライアント起動設定だけが適用されます。

- KVM クライアントを起動する場合は、標準画面または全画面ウィンドウ モードを選択します。
- ビデオの拡大/縮小を有効にします。
- 全画面モードのときにメニュー ツールバーの固定機能を有効にします。

1 台のクライアント モニタでデュアル ビデオ ポートを全画面モードで表示する場合、シングル マウス モードの使用はお勧めできません。このような場合は、シングル マウス モードを終了してから、他方の画面にアクセスして表示する必要があります。

サポートされているマウス モード

対象のオペレーティング システム	サポートされているマウス モード	コメント
すべての Windows® オペレーティング システム	インテリジェント モード、標準モード、およびシングル マウス モード	ターゲット サーバのビデオ カードで「ストレッチ」モードがサポートされている場合は、ずれないマウス モードが正しく動作します。 ストレッチ モードにより、ターゲット サーバでは、2 つの画面が 1 つの仮想画面として管理されます。それに対して、拡張モードで設定されている

対象のオペレーティング システム	サポートされているマウス モード	コメント
		場合、各画面は 2 つの独立した画面と見なされます。拡張モードの場合は、インテリジェント マウス モードにすることをお勧めします。
Linux®	インテリジェント マウス モードおよび標準マウス モード	Linux® VKC/MPC ユーザは、シングル マウス モードを使用すると画面やマウスの動作に関する問題が発生する場合があります。Linux ユーザは、できればシングル マウス モードを使用しないでください。
Mac® オペレーティング システム	シングル マウス モード	マウスは、Mac のデュアル ビデオ ポートのターゲットでは同期しません。

デュアル ビデオ サポートに必要な CIM

次のデジタル CIM は、デュアル ビデオ ポート機能をサポートしています。

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-DP
- D2CIM-DVUSB-HDMI
- DCIM-USBG2

デジタル CIM に関する重要な情報については、「デジタル CIM ターゲット サーバのタイミングおよび画面解像度」を確認してください。CIM の仕様については、「サポートされているコンピュータ インタフェース モジュール（CIM）の仕様」を参照してください。

プライマリ ビデオ ポートまたはセカンダリ ビデオ ポートに最初に接続されていた CIM がつながらなくなったので別の CIM に交換すると、そのポートはデュアル ポート ビデオ グループから削除されます。必要に応じて、ポートをグループに追加し直します。

注: 使用する CIM は、ターゲット サーバの要件によって異なります。

デュアル ポート ビデオ グループの使いやすさに関する注意事項

以下は、デュアル ポート ビデオ グループ機能を使用するときに影響を受ける各種機能です。

- [Tools]（ツール）メニューの [Options]（オプション）の [Client Launch Settings]（クライアント起動設定）を介して VKC、AKC、MPC の各クライアントで設定されるクライアント起動設定は、次のようにデュアル ビデオ ポート グループに適用されます。
  - ウィンドウ モード設定が適用されます。
  - モニタ設定は適用されません。代わりに、[Port Group Management]（ポート グループ管理）で設定した「画面の方向」が適用されます。
  - その他 – [Enable Single Mouse Cursor]（シングル マウス カーソルを有効にする）設定は適用されません。
  - その他 – [Enable Scale Video]（ビデオの拡大、縮小を有効にする）設定が適用されます。
  - その他 – [Pin Menu Toolbar]（メニュー ツールバーを常に表示）設定が適用されます。
- プライマリ ターゲットとセカンダリ ターゲットのウィンドウ間で項目をドラッグして移動する場合は、マウス ボタンを押したまま移動して離すと、一方のウィンドウから他方のウィンドウに項目が移動されます。
- Linux® および Mac® のターゲット サーバで、Caps Lock および Num Lock をオンにすると、プライマリ ポート ウィンドウのステータス バーに Caps Lock インジケータが表示されますが、このインジケータは、セカンダリ ポート ウィンドウのステータス バーには表示されないことがあります。
- デュアル ポートのターゲットが全画面モードで開かれている場合、MPC メニューを有効にすることはできません。このメニューを有効にするには、もう一方のポート ウィンドウに切り替えた後、元のポート ウィンドウに戻ります。

権限およびデュアル ビデオ ポート グループ アクセス

理想的には、ポート グループの各ポートに適用される権限は、同じでなければなりません。権限が同じでない場合は、最も制限の厳しいポートの権限がポート グループに適用されます。

たとえば、あるポートに [VM Access] (VM アクセス) の [Deny] (拒否) が適用されており、別のポートに [VM Access] (VM アクセス) の [Read-Write] (読み取り/書き込み可能) が適用されている場合、ポート グループには、[VM Access] (VM アクセス) の [Deny] (拒否) が適用されます。

デュアル ポート ビデオ グループに属しているポートにアクセスするための適切な権限がないユーザには、アクセスできるポートだけが表示されます。どのポートにアクセスする権限もない場合、アクセスは拒否されます。

それでもポートにアクセスしようとすると、ポートを利用できないか、ポートにアクセスするための権限がないことを示すメッセージが表示されます。

デュアル ビデオ ポート グループを使用する際の Raritan クライアントの画面操作

画面操作

クライアントで全画面モードを使用する場合は、次の方法でポートを切り替えます。

- VKC

  Alt+Tab キーを押す

  Mac® クライアントの場合は、F3 キーを押して、ポート画面を選択する

- AKC

  表示ウィンドウの外でマウスをクリックし、Alt+Tab キーを押す

- MPC

  「接続されているサーバ」のツールバーからポートを選択する

ダイレクト ポート アクセスおよびデュアル ポート ビデオ グループ

ダイレクト ポート アクセス機能を利用した場合、ユーザはデバイスの [Login] (ログイン) ダイアログ ボックスと [Port Access] (ポート アクセス) ページを使用する必要がなくなります。この機能を使用すると、ユーザ名とパスワードが URL に含まれていない場合に、ユーザ名とパスワードを直接入力してターゲットにアクセスすることもできます。

デュアル ポート ビデオ グループに属しているターゲットにアクセスする場合は、ダイレクト ポート アクセスにより、プライマリポートを使用して、プライマリ ポートおよびセカンダリ ポートの両方を開きます。セカンダリ ポートへのダイレクト ポート接続は拒否され、通常の権限ルールが適用されます。デュアル ポート ビデオ グループ機能については、「*デュアル ビデオ ポート グループの作成* 『*463*p. 』」を参照してください。ダイレクト ポート アクセスについては、「URL を経由したダイレクト ポート アクセスの有効化」を参照してください。

[Ports] (ポート) ページに表示されるデュアル ポート ビデオ グループ

注: デュアル ビデオ プライマリ ポートは、ポート グループの作成時に定義されます。

注: プライマリ ポートをクリックしてリモートでデュアル ビデオ ポート グループに接続するには、2 つの KVM チャネルが必要です。2 つのチャネルが利用できない場合、[Connect] (接続) リンクは表示されません。

デュアル ビデオ ポート グループでは、プライマリ ポートはポート スキャンの対象になりますが、リモート クライアントから接続している場合、セカンダリ ポートは対象になりません。両方のポートをローカル ポートからスキャンの対象にすることができます。

[Ports] (ポート) ページに表示される内容の詳細については、「[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ)」を参照し、スキャンの実行については、「ポートのスキャン」を参照してください。

Ap J CC-SG 仮想アプライアンスによる VMware High Availability または Fault Tolerance の活用

High Availability (HA) や Fault tolerance (FT) に関心のある VM 管理者は、使用中のバージョンの『vSphere 可用性ガイド ESX』を十分に理解しておく必要があります。

High Availability:

- HA により停電から迅速な復元を実現 – HA により、障害発生後わずか 3 ～ 5 分のうちに仮想 CC-SG の新しいインスタンスでサービスを提供できるようになります。
- 新しい仮想 CC-SG VM は、最初に実行していたホストで障害の発生が検出されると、使用可能な別のホストで起動されます。
- ホストではなく VM に障害が発生した場合は、VM が再起動されます。この処理は、ハートビートおよび I/O の監視に基づいています。テストして確認する場合は、その点に留意してください。

『vSphere 可用性ガイド ESX 4.1』の「仮想マシンとアプリケーションの監視」セクションには、次のように記載されています。「場合によっては、正常に機能している仮想マシンやアプリケーションが、ハートビートの送信を停止することがあります。不必要なリセットを防ぐため、仮想マシンの監視サービスでは、仮想マシンの I/O アクティビティも監視されます。障害間隔の間にハートビートが受信されなかった場合は、I/O 統計間隔（クラスタ レベルの属性）がチェックされます。I/O 統計間隔では、過去 2 分間（120 秒間）に、仮想マシンでディスクまたはネットワーク アクティビティが発生しているかどうかが確認されます。発生していない場合、その仮想マシンはリセットされます。」

Fault tolerance:

- Fault tolerance により、連続した可用性が実現されます。仮想 CC-SG のセカンダリ インスタンスは数秒以内に有効になるため、接続を維持したままデータ ストリームを復元し、データの損失を最小限に抑えて再開できます。
- 2 つの VM（プライマリとセカンダリ）が同時に実行しますが、プライマリのみが応答します。
- 障害発生時には、セカンダリが、接続やデータを失うことなくプライマリを引き継ぎます。また、新しいセカンダリが起動され、保護が継続されます。

比較:

HA と FT では、復元時間の増大や潜在的なデータ損失と、リソース使用率の増大や潜在的なパフォーマンス低下というトレードオフが生じます。

FT には、HA クラスタの可用性が求められます。HA は、以下に基づいて構築されます。

- 複数のホストから VM データストアにアクセスできる共有ストレージ
- 高可用性ストレージが前提（データストアは VM）
- 冗長ネットワーク インタフェース
- ストレージへの冗長パス

その他の主要な要件は、障害が発生しても HA が正しく機能するように使用可能なリソースを用意することです。これは、アドミッション コントロールを介して実施できます。また、アドミッション コントロールを無効にして想定を上回るフェイルオーバ容量を使用できるようにした場合、想定を上回るリソースの競合は、VM に優先度を割り当てて VM 再起動用のポリシーを定義することによって管理されます。HA クラスタが継続的に存続できるように、リソースの可用性も監視されます。

HA 向けのクラスタ設定:

- [VMware HA(VMware HA)] 設定を指定するには、HA クラスタの [Edit Settings(設定の編集)] ダイアログにアクセスします。
- Cluster Features(クラスタ機能) – VMware HA を有効にします。
- VMware HA(VMware HA) – HA モードでの動作中にホストの監視を有効にし、使用可能なフェイルオーバ容量を確保するためにアドミッション コントロールを有効にして、クラスタのホスト障害の許容数に合わせてアドミッション コントロール ポリシーを設定します。
- Virtual Machine Options(仮想マシン オプション) – デフォルトの動作は、「分離」と判断されたホスト上で再起動優先度が [Medium(中)] のシャットダウンされている VM を対象としています。
- VM Monitoring(VM の監視) – VM の監視が無効にされます。VM の監視のみに設定することもできます。
- Monitoring Sensitivity(監視感度) – High(高)

クラスタの設定が完了し、クラスタがホストおよび VM に割り当てられたら、HA フェイルオーバをテストできます。

FT 向けの VM 設定:

FT operates on a per VM basis(VM 単位の FT 動作) – HA クラスタが設定済みで使用可能になっている場合。また、FT に対するホスト、プロセッサ、およびネットワークの追加要件もあります。

『vSphere 可用性ガイド ESX 4.1』には、クラスタ、ホスト、および VM が FT に適合するための要件について詳しく説明する 2 つのセクションがあります。そこには、FT ペアでの ESX ホストと ESXi ホストの混在に関する主要な注意事項が記載されています。当初問題が発生しなくても、混在させないでください。

少なくとも 2 つの FT 認定ホストで同じ Fault Tolerance バージョンまたはホスト ビルド番号が実行されていること。Fault Tolerance バージョン番号は、vSphere Client でホストの［概要］タブに表示されます。

注: ESX/ESXi 4.1 より前のホストの場合、このタブには、ホスト ビルド番号が表示されます。パッチを適用すると、インストールされている ESX と ESXi のホスト ビルド番号が変わる場合があります。ホストを FT に確実に適合させるために、FT ペアで ESX ホストと ESXi ホストを混在させないでください。

Fault Tolerance に対するホストの要件

主要な要件として、ホストが FT 適合のプロセッサを装備し、Fault Tolerance を使用するためのライセンスと認定を受けている必要があります。BIOS でホストのハードウェア仮想化サポートが有効になっていることを確認してください。vSphere Client ホストの［概要］タブで、バージョン情報および FT 設定情報にアクセスできます。

ホストが FT 対応に設定されていなくても、FT に適合するとわかっている場合は、BIOS 設定を確認します。Dell R610 の例では、BIOS > [Processor Settings] > [Virtualization Technology] が［Enabled］に設定されていることを確認します。

Fault Tolerance を使用するための仮想マシンの要件

- 1 つの vCPU を備えた仮想マシンのみが Fault Tolerance に適合します。
- サポートされていないデバイスは仮想マシンに接続されません。

VM ノードを右クリックし、[Fault Tolerance(Fault Tolerance)] > [Turn On Fault Tolerance(Fault Tolerance を有効にする)] を選択すると、FT を有効にすることができます。上記の項目が正しく設定されていない場合は、エラーが表示され、一部の設定を修正する必要があります。

詳細については、『vSphere 可用性ガイド ESX 4.1』の表 3-1「フォールト トレランスと互換性のない機能とデバイス、および対策」を参照してください。

想定されるエラーおよび修正:

対称型マルチプロセッサ (SMP) 仮想マシン。1 つの vCPU を備えた仮想マシンのみが Fault Tolerance に適合します。

仮想マシンを 1 つの vCPU として再設定します。1 つの vCPU として設定されると、さまざまな負荷に対して優れたパフォーマンスを発揮します。

VM の Fault Tolerance を有効にすると、「The virtual machine has more than one virtual CPU (仮想マシンに複数の仮想 CPU があります)」というエラーが表示されます。

[Edit Settings(設定の編集)] にアクセスして、vCPU の数を 1 に減らします。

物理デバイスまたはリモート デバイスによってバックアップされた CD-ROM またはフロッピー仮想デバイス。CD-ROM またはフロッピー仮想デバイスを削除するか、共有ストレージにインストールされている ISO でバックアップを再設定します。VM の Fault Tolerance を有効にすると、「Device 'CD-ROM1' has a backing type that is not supported(デバイス「CD-ROM1」のバックアップ型はサポートされていません)」というエラーが表示されます。

[Edit Settings(設定の編集)] にアクセスしてハードウェア デバイスのリストからデバイスを削除します。必要な場合は、このデバイスを追加し直して、FT を無効にした後にメンテナンス機能を実行できます。

仮想マシンは、Fault Tolerance と互換性のない監視モードで実行しています。Fault Tolerance を有効にする前に VM の電源を切ります。これは、CPU バージョンおよび実行しているゲストのタイプに基づく制限です。最初に VM の電源を切ってから、FT を有効にする必要があります。

こうした設定が修正されたら、VM に戻って FT を有効にします。

Ap K FAQ

この章の内容

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、プロ	いいえ。CC-SG ソフトウェアは専用のサーバ上に

質問	回答
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。お買い上げのラリタン販売店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 デバイスがユーザ 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。

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。便利なシングル サインオンも可能です。
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」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

質問	回答
	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」という内容のメッセージが表示されます。なぜでしょうか?	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

質問	回答
	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	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

質問	回答
うです。なぜでしょうか?	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、telnet 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 オーバーヘ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。

グループ化に関する FAQ

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 =

質問	回答
	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? ポート名はどうなりますか? 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	CC-SG は、透過なパスとして KVM またはシリアル

質問	回答
シ製品とどのように統合されますか?	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	
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 および CCL-512 を、クラスタ ライセンス CC-2XE1-512 および CCL-512 と置換する場合は、CCL-512 アドオン ライセンスより前に基本ライセンス CC-E1-512 を置換する必要があります。 アドオン機能 CCL-512 はスタンドアロンでもクラスタでも同じですが、ライセンス ファイルに含まれているホスト ID が、スタンドアロン ライセンスの場合は 1 つ、クラスタ ライセンスの場合は 2 つであることに注意してください。この状況では、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イセンスに、またはその逆に置換する場合、アドオンは自動的にクリアされるので、正しいホスト ID の新しいライセンスが必要となります。
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 の置換にも使用できます。ホスト ID が両方のライセンスで同じである場合、アドオン 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、その後再追加する必要があります。	スタンドアロン ライセンスはクラスタ メンバで共有されないので、スタンドアロン ライセンスで動作しているクラスタ内の各 CC-SG は、ライセンスされているノード数が同じであることが必要です。 ライセンスされるノード数を CC-SG ユニットそれぞれに追加する代わりに、顧客が 2 つの CC-SG ユニット間でライセンスを共有できるように、クラスタ ライセンスに置き換えること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、クラスタを再構築します。
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] ページに移動し、利用可能な機能を確認し、必要に応じてそれらをチェックアウトします。これらは自動的にはチェックアウトされません。「ライセンスをインストールしてチェックアウトする」を参照してください。
ライセンス サーバを削除して未処理モードに切り替えるためにライセンスを交換すると、アップロードしたすべてのライセンスが消去されます。	再ホスト対象の未処理モードの基本ライセンスをアップロードした後に、CC-SG を再起動する必要があります。もう一度ログインすると、CC-SG は制限モードになるため、他の機能のライセンスのアップロードを完了し、すべてのライセンスをチェックアウトして、制限付きの操作モードを終了することができます。

Ap L 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 M 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

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
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

空白文字 ( ) およびピリオド (.) はデバイス名に使用できません。

その他の特殊文字をデバイス名に含めることはできますが、デバイス名の先頭に特殊文字は使用できず、英数字を使用する必要があります。

メイン画面の「デバイスが正常に更新されました」メッセージで、デバイス名に「より小」(<) または「より大」(>) の文字が含まれている場合、文字の使用場所によっては、デバイス名の「より小」または「より大」の文字は表示されません。

引用符内の文字の例を次に示します。

- ″KX2-<232>″ では、「より大」の記号は表示されますが、「より小」の文字は表示されません。
- ″KX2-232,/<>?″ では、「より大」と「より小」のどちらの文字も表示されません。

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

Ap N 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。

索引

D

E

F

I

J

K

L

T

V

W

あ

か

さ

た

な

は

ま

や

ら

わ

漢字

米国/カナダ/ラテン アメリカ

月曜日～金曜日
午前 8 時～午後 8 時 (米国東海岸時間)
電話 :800-724-8090 または 732-764-8886
CommandCenter NOC に関するお問い合わせ :6 を押してから 1 を押してください。
CommandCenter Secure Gateway に関するお問い合わせ :6 を押してから 2 を押してください。
Fax :732-764-8887
CommandCenter NOC に関する電子メール :tech-ccnoc@raritan.com
その他のすべての製品に関する電子メール :tech@raritan.com

中国

北京

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-10-88091890

上海

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-21-5425-2499

広州

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-20-8755-5561

インド

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+91-124-410-7881

日本

月曜日～金曜日
午前 9 時 30 分～午後 5 時 30 分
電話 : 03-5795-3170
電子メール :support.japan@raritan.com

ヨーロッパ

ヨーロッパ

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 :+31-10-2844040
電子メール :tech.europe@raritan.com

英国

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT)
電話 : +44(0)20-7090-1390

フランス

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 :+33-1-47-56-20-39

ドイツ

月曜日～金曜日
午前 8 時 30 分～午後 5 時 30 分 (GMT+1 CET)
電話 :+49-20-17-47-98-0
電子メール : rg-support@raritan.com

メルボルン (オーストラリア)

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+61-3-9866-6887

台湾

月曜日～金曜日
午前 9 時～午後 6 時 (標準時 : GMT -5、夏時間 : GMT -4)
電話 :+886-2-8919-1333
電子メール : support.apac@raritan.com