# CommandCenter®
# Secure Gateway


## CC-SG

管理者ガイド

リリース **3.1**



CCA-0D-J

2007 年 1 月

255-80-5140-00

*本ページは意図的に空白となっています。*

## 著作権および商標情報



## FCC 情報

この装置は試験済みであり、FCC 規則のパート 15 による Class A デジタル装置の制限に準拠することが証明されています。これらの制限は、商業上の設置における有害な干渉を防止するために設計されています。この装置は、無線周波数の生成し、利用し、放射できるので、指示に従って設置および使用しないと、無線通信への有害な干渉を招く恐れがあります。この装置を居住環境で操作すると、有害な干渉を招く場合があります。

## 日本の承認

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

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

CE cULus LISTED 1F61 I.T.E.

*北南米でのサポートは、Raritan 社のテクニカル サポート チームにご連絡ください。電話 (732) 764-8886、ファックス (732) 764-8887、電子メール* ***tech@raritan.com***

*米国東海岸時間 月曜日 – 金曜日 午前 8 時から午後 8 時に、テクニカル サポートにご連絡ください。*

*世界各国でのサポートについては、このガイドの*
*最終ページの各地域の Raritan 社の連絡先をご覧ください。*

## 安全基準

Raritan 社の製品を安全にご利用いただき、重大な故障や危険性のある破壊を避けるために、以下のことにご注意ください。

- 製品の構成には、2 線式の電源コードは使用しないでください。
- コンピュータやモニタの AC 電源コンセントの極性と設置が正しいことを確認してください。
- コンピュータとモニタの両方とも、接地されている電源コンセントのみを使用してください。バックアップ用の UPS を使用している場合、コンピュータ、モニタ、その他のアプライアンスには電源コンセントから電源を供給しないでください。

## ラック マウントの安全基準

ラック マウントが必要な Raritan 社製品を使用する場合、以下のことに注意してください。

- 閉め切ったラック環境では、室温より高くなる場合があります。アプライアンスで指定された最高動作温度を超えないようにしてください（「付録 A：仕様 (G1、V1、および E1)」参照してください）。
- ラック内に十分な空気の流れがあることを確認してください。
- 装置をラックにマウントする際は、機構が平らに搭載されるように注意してマウントしてください。
- 回路に過重電流が流れないよう、装置を電源に接続する際は注意してください。
- すべての装置を正しく接地してください。 特に、パワー ストリップ（直接接続を除く） を分岐回路に接続する場合など、電源への接続には注意してください。

# 目次

# 図表目次

# 第 1 章 : はじめに

CommandCenter Secure Gateway (CC SG) をお買い上げいただき、ありがとうございました。本製品は、さまざまな UNIX サーバ、ファイアウォール、ルータ、ロード バランサ、パワー管理デバイス、Windows サーバを管理するための Raritan の使いやすくセキュアなツールです。

CC-SG を使用すると、一連のシリアルおよび KVM アプライアンスによる集中管理が可能になります。CC-SG は、高密度なサービス プロバイダのデータ センター環境から大規模なリモート オフィスを操作する企業環境に至るまで、実質的にあらゆる環境で動作するように設計されています。

CC-SG と Raritan Dominion または IP-Reach ポートレベル管理アプライアンスを併用すると、ターゲット デバイス (「ノード」と呼ばれています)、の管理が合理化され、簡素化されると同時に、IP ネットワークに接続し、管理対象ネットワーク上に存在する全ノードのシリアル コンソールおよび KVM ポートを表示することでデータ センター設備の管理が容易になります。

## 前提条件

このマニュアルの手順に従って 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 デジタル ソリューション デプロイメント ガイド**』を参照してください。

## 対象読者

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。「**付録 C : ユーザ グループ権限**」を参照してください。管理者ではないユーザは、通常、ノード アクセス権限のみを許可されるなど、与えられる権限はより少数です。このようなユーザは、詳細については Raritan の『CommandCenter Secure Gateway ユーザ ガイド』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。
- **関連** – カテゴリ、カテゴリのエレメント、およびポートまたはデバイス、またはその両方の間の関係です。たとえば、「Location」カテゴリにデバイスを関連付ける場合は、最初に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** - 設定された値またはエレメントを含む変数です。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、サーバをリブートしてください。
- CommandCenter NOC **(CC**-NOC) - CC-SG が管理するサーバ、装置、Raritan デバイスのステータスを監査および監視するネットワーク監視アプライアンスです。
- **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 KX116、Dominion SX48、Dominion KSX440、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 サーバとシステムを制御します。
- **Director Client** - 通常のアクセスを行うユーザおよび管理者の両方が CC-SG を使用できる 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。
- **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」カテゴリに属します。また、「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。詳細は、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ホスト名を使用できます。詳細は、「**第 12 章 : 高度な管理**」の「設定マネージャ」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** - 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。
- **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 サーバ** (Intelligent Platform Management Interface) - 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)、または Multi-Platform Client (MPC) などのアプリケーションを使って、KVM やシリアルのネットワーク上の管理対象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** - 許可、アクセスのタイプ、ユーザ グループがアクセス権を持つノードおよびデバイスを定義します。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、その他の CC-SG ユーザがアクセスできるネットワーク機器などのターゲット システムです。
- **インタフェース** - Dominion KX101 接続などのアウト オブ バンド ソリューション、または 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です。ポートは Raritan デバイスにのみ存在し、該当デバイスからノードへのパスを識別します。
- **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 コマンドのサブネットのみが 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 グループへのポリシーの割り当て方法の詳細は、「**第 12 章 : 高度な管理**」を参照してください。

- **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。たとえば、デフォルトの**システム管理**ユーザグループは、すべての設定タスクおよびターゲット ノードに対しフル アクセスを持っています。

*本ページは意図的に空白となっています。*

# 第 2 章 : CC-SG へのアクセス

CC-SG に IP アドレスを設定したら、CC-SG のユニットを最終的な設置場所に設置します。必要なすべてのハードウェアを接続し、ユニットが動作するようにします。

CC-SG には、次の方法でアクセスすることができ、それぞれ本章の解説に従います。

- **ブラウザ** : CC-SG は多数の Web ブラウザをサポートします。サポートされるブラウザおよびプラットフォームの全リストについては、**CC-SG の互換表** (**http://www.raritan.com/support**) を参照してください。[Support] ページで、[**Firmware Upgrades**] をクリックし、[**CommandCenter Secure Gateway**] をクリックします。
- **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。詳細については、「**第 12 章 : 高度な管理**」を参照してください。
- **Diagnostic Console** : 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。詳細については、「**第 12 章 : 高度な管理**」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、スタンドアロン クライアント、および SSH を使用して同時に接続できます。*

---

## ブラウザベースのアクセス

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「**https://<IP_address>/admin**」と入力します。ここで <**IP_address**> は CC-SG の IP アドレスです。たとえば「**https://10.20.3.30/admin**」のように入力します。
2. 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、警告が表示されます。
3. ポップアップ ウィンドウで、適切な JRE バージョンを CC-SG サーバからダウンロードするか（利用可能な場合のみ）、Sun Microsystems の Web サイトからダウンロードするか、あるいは不適切なバージョンのまま続けるかを選択し、[**OK**] をクリックします。[ログイン] ウィンドウが表示されます。

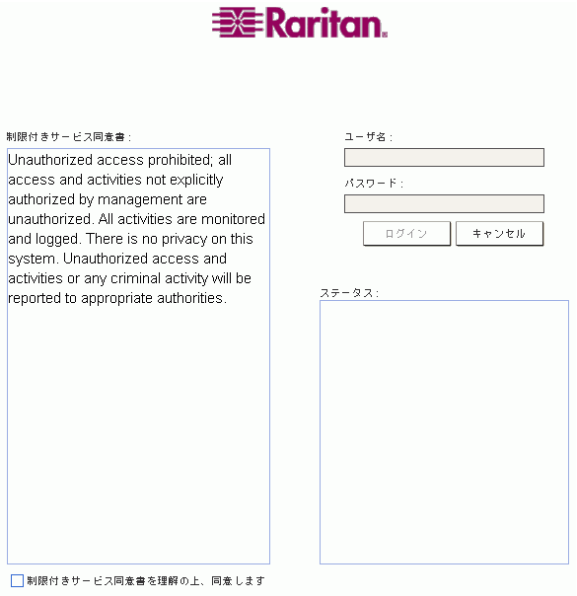


*図 1 ログイン ウィンドウ*

4. 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。
5. [**ユーザー名**] と [**パスワード**] を入力し、[**ログイン**] をクリックします。

## 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。ブラウザの代わりにシック クライアントを使用する利点は、シック クライアントの方が速度と効率性の面でブラウザより優れている点です。

### シック クライアントのインストール

1. CC-SG からシック クライアントをダウンロードするには、Web ブラウザを起動して、URL を「https://<IP_address>/admin」と入力します。ここで <IP_address> は CC-SG の IP アドレスです。
2. セキュリティ警告メッセージが表示されたら、[**開始**] をクリックしてダウンロードを続行します。
3. ご使用のクライアント コンピュータが Java バージョン 1.4 を実行している場合は、[**Desktop Integration**](デスクトップ統合) ウィンドウが表示されます。Java のシック クライアント用ショートカット アイコンをデスクトップに追加したい場合は、[**はい**] をクリックします。
4. ダウンロードが完了したら、CC-SG IP アドレスを指定できる新規ウィンドウが表示されます。


*図 2 シック クライアント IP アドレス指定ウィンドウ*

5. [**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。
6. 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オフに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**] メニューで、[**セキュリティ**] をクリックします。[**全般**] タブで、[**ブラウザ接続プロトコル**] フィールドを参照します。[**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オフにする必要があります。

7. [**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。
8. ログイン画面が表示され、シック クライアントはブラウザベースの Java クライアントと同様の表示および動作を行います。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。
9. 対応するフィールドに**ユーザー名**と**パスワード**を入力し、[**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。このアクセス方法は、使用している Java のバージョンによって決まります。

- **Java 1.4.x**

ご使用のクライアント コンピュータが **Java バージョン 1.4.x** を実行していて、シック クライアントのインストール時に [**Desktop Integration**](デスクトップ統合) ウィンドウで [**はい**] をクリックしている場合、デスクトップのショートカット アイコンをダブルクリックして、シック クライアントを起動し、CC-SG にアクセスすることができます。このショートカット アイコンがない場合は、いつでも作成できます。クライアント コンピュータで **AMcc.jnlp** を検索し、そのファイルにショートカットを作成します。

- **Java 1.5**

ご使用のクライアント コンピュータが **Java バージョン 1.5** を実行している場合は、以下の操作を実行します。

a. 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。

b. Java コントロール パネルの Java Application Cache Viewer を使用して、デスクトップにシンク 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 ウィンドウ コンポーネント

ログインが有効な場合は、CC-SG アプリケーション ウィンドウが表示されます。

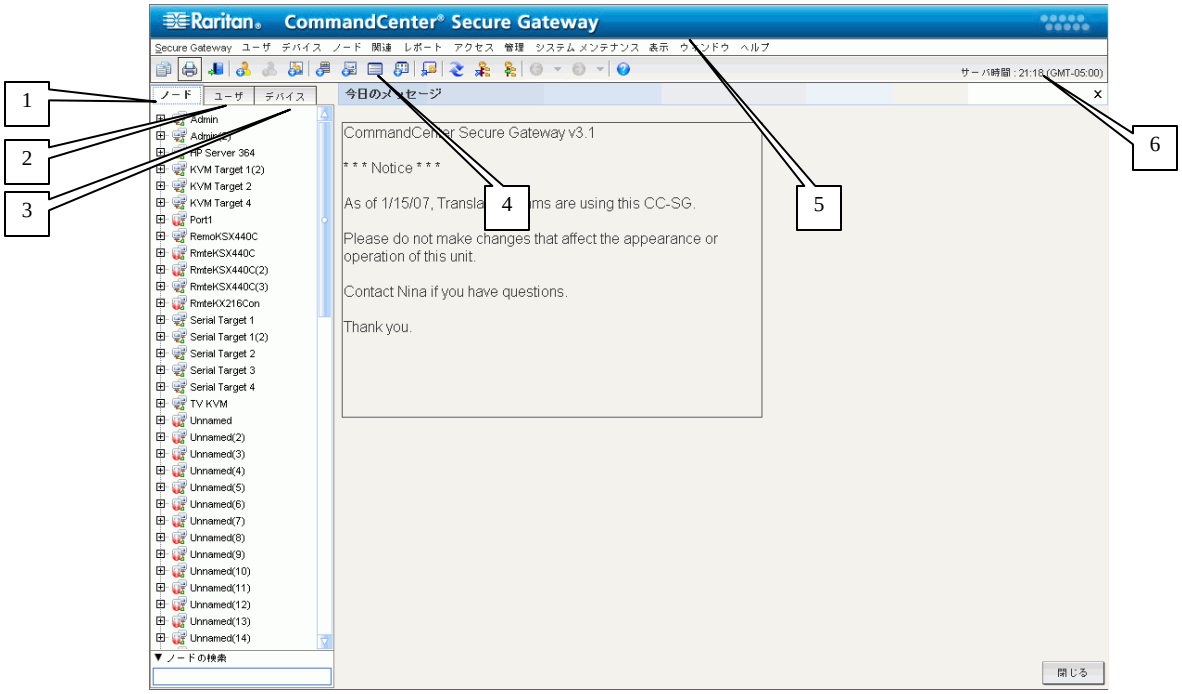


*図 2 CC-SG ウィンドウ コンポーネント*

1. **[ノード] タブ**：[**ノード**] タブをクリックすると、ツリー ビューに既知の全ノードが表示されます。ノードをクリックしてノード プロファイルを表示します。インタフェースは、親ノード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。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) を基準にして並べ替えることができます。ツリー•\Ž¦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。
2. **[ノード] 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。
3. [**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) またはポート ステータス (利用可能、使用中、利用不可) 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。
4. クイック 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。
5. 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、ユーザのアクセス権限により決定します。
6. **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。詳細は、「**第 12 章：高度な管理**」

のタスク管理の項目を参照してください。この時間はクライアントで使用される時間と異なる場合があります。

## IP アドレス、ファームウェア バージョン、およびアプリケーション バージョンのチェック

ログインしたら、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。

### IP アドレスの確認

1. [**管理**] メニューで、[**設定**] をクリックして [**設定マネージャ**] 画面を開きます。
2. [**ネットワーク設定**] タブをクリックします。

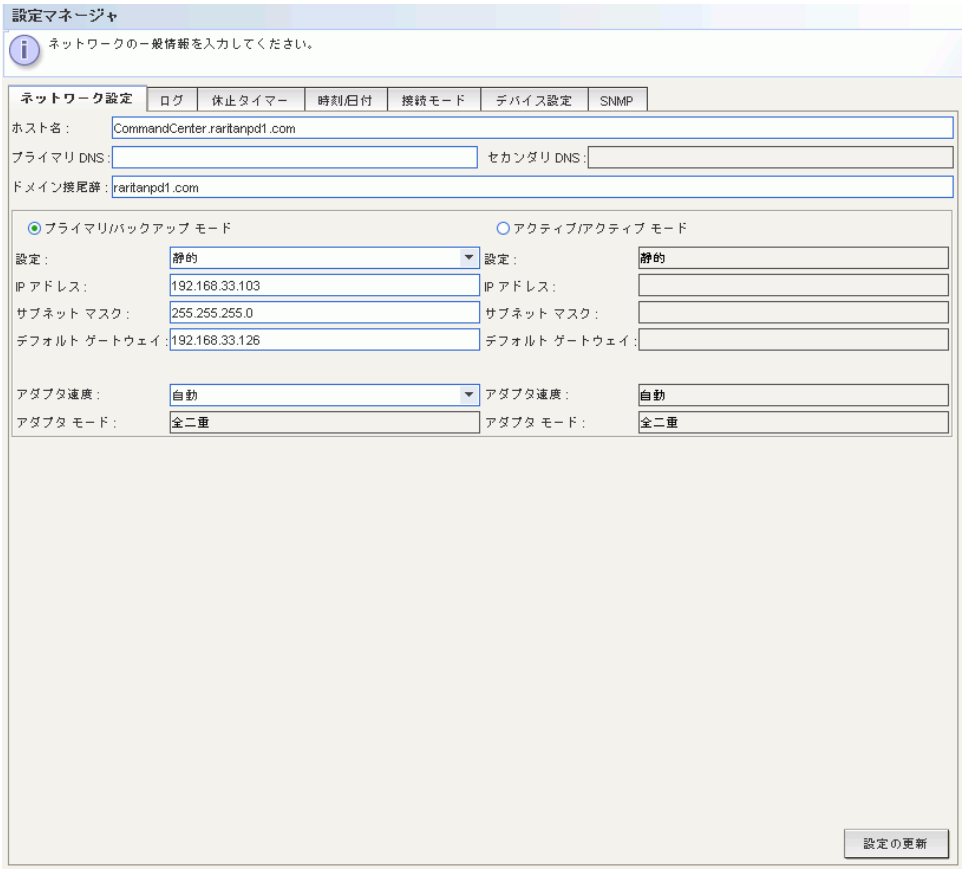


*図 3 IP アドレスの確認*

ネットワーク設定が正しいことを確認するか、または必要に応じて変更を加えます。

3. [**設定の更新**] をクリックして変更を適用します。
4. 設定確認のウィンドウで [**OK**] をクリックし、ログ アウトして CC-SG を再起動します。
5. 新しい IP アドレスを使用して CC-SG にアクセスします。

## CC-SG サーバ時間の設定

1. CC-SG にログオンします。
2. [**管理**] メニューで、[**設定**] をクリックして [**設定マネージャ**] 画面を開きます。
3. [**時刻/日付**] タブをクリックします。

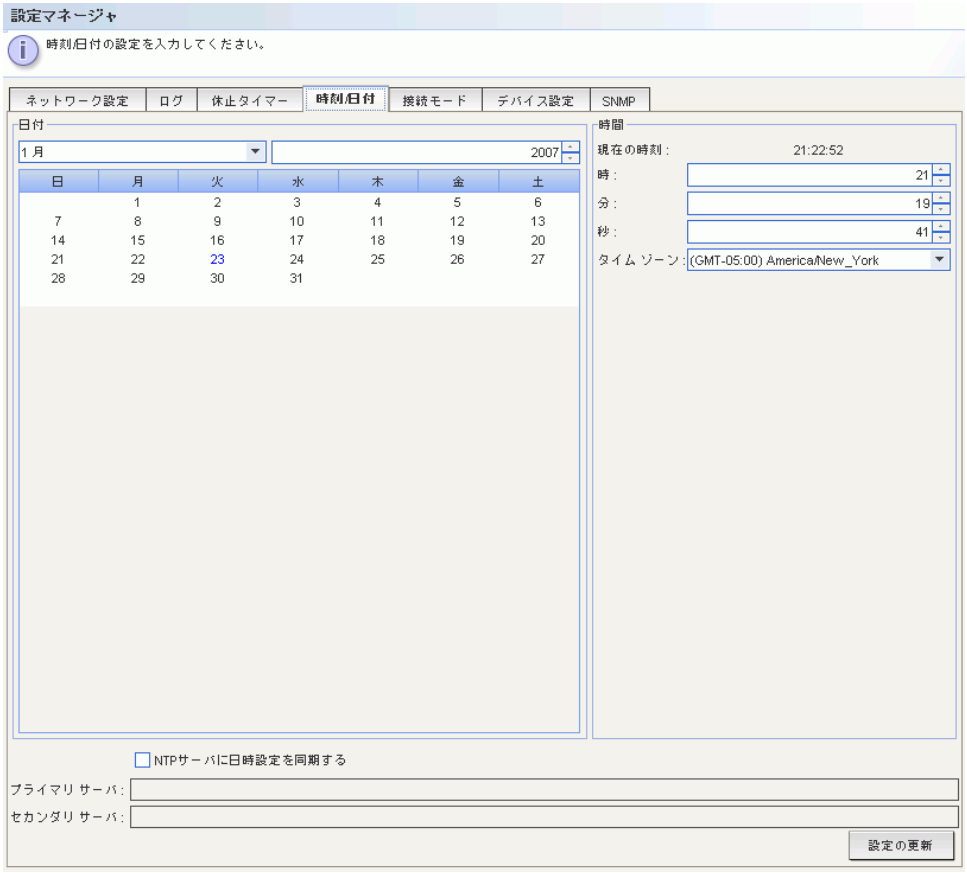


*図 4 時刻/日付の設定*

4. [**管理**] メニューで、[**設定**] をクリックして [**設定マネージャ**] 画面を開きます。
5. [**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**] – 上下矢印を使用して**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。
   b. **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オンにし、**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。*

6. [**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。
7. [**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。
8. [**メンテナンス**] メニューで [**再起動**] をクリックして、CC-SG を再起動します。

## CC-SG ファームウェア バージョンの確認と更新

1. CC-SG にログオンします。
2. [ヘルプ] メニューから、[**バージョン情報**] をクリックします。ファームウェア バージョン番号を表示するポップアップ ウィンドウが開きます。[OK] をクリックします。
3. 最新のバージョンではない場合、ファームウェアをアップグレードします。Raritan Web サイトからファームウェア アップグレード ファイルをダウンロードするか、または Raritan CD から入手します。クライアント PC にファームウェア アップグレード ファイルを保存します。

***注 :*** *CC-SG をアップグレードする前に、メンテナンス モードに切り替える必要があります。詳細は、「**第 11 章 : システム メンテナンス**」の「メンテナンス モード」を参照してください。*

4. [**システム メンテナンス**] メニューで、[**メンテナンス モード**]、[**メンテナンス モードの起動**] をクリックします。
5. [**メンテナンス モードの起動**] 画面で、CC-SG からログオフされるユーザに表示されるメッセージと CC-SG がメンテナンス モードに入るまでの時間を分数で、それぞれ該当するフィールドに入力し、[**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。
7. CC-SG のメンテナンス モードが起動されると、2 番目のメッセージが表示されます。[OK] をクリックします。
8. [**システム メンテナンス**] メニューで、[**アップグレード**] をクリックします。


*図 5 CCSG のアップグレード*

9. [**参照**] をクリックして、表示される [**開く**] ダイアログでファームウェア アップグレード ファイルを選択し、[**開く**] をクリックします。
10. [**CommandCenter のアップグレード**] 画面で [**OK**] をクリックします。

***注 :*** *ファームウェアを zip ファイルとして入手した場合は、ファイルを解凍したうえで、README ファイルの手順に従ってください。*

## 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。

1. [**管理**] メニューで、[**アプリケーション**] をクリックします。

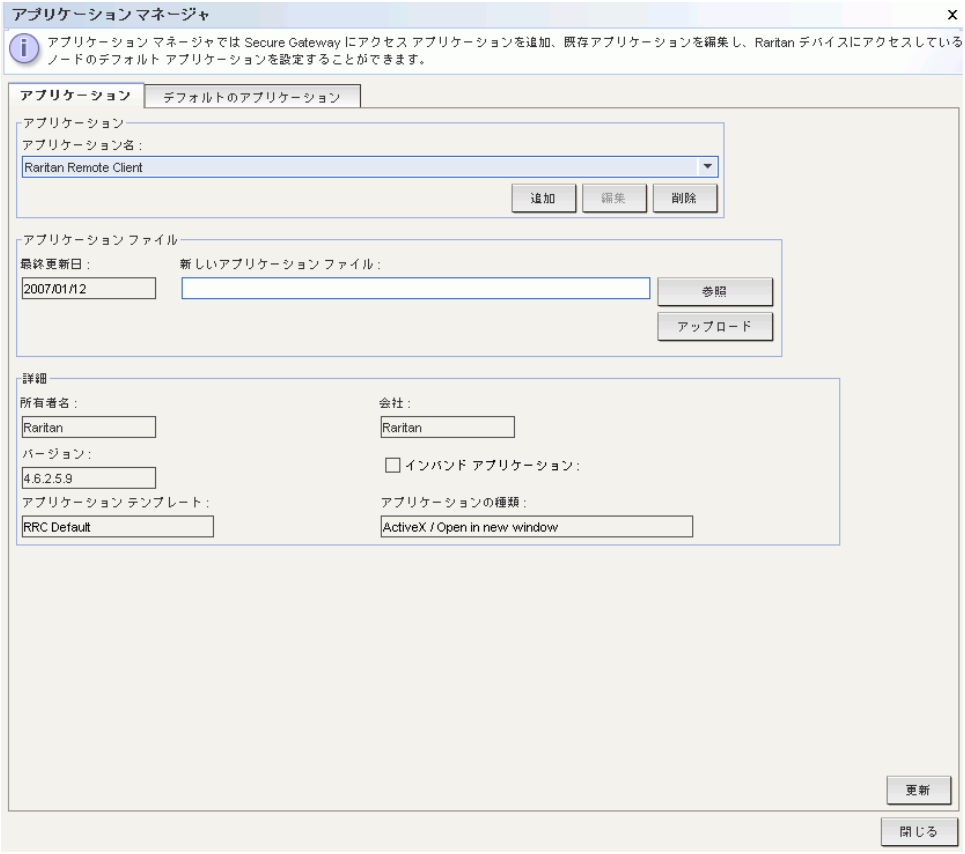


*図 6 CC-SG アプリケーション マネージャ*

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、リストからアプリケーションを選択します。[**バージョン**] フィールドの番号を確認してください。
3. 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。Raritan Web サイトからアプリケーション アップグレード ファイルをダウンロードするか、または Raritan CD から入手します。クライアント PC にアプリケーション アップグレード ファイルを保存します。サポートされるアプリケーション バージョンの全リストについては、**互換表** (**http://www.raritan.com/support**) を参照してください。[**Support**] ページで、[**Firmware Upgrades**] をクリックし、[**CommandCenter Secure Gateway**] をクリックします。
4. [**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。
5. [**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 ファイルを選択し、[**開く**] をクリックします。
6. [**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。
7. [**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、設定や特定のポートへの割り当てが可能なことが示されます。

8. 必要に応じて、**[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。
9. [**更新**] をクリックします。
10. [**閉じる**] をクリックし、[**アプリケーション マネージャ**] 画面を閉じます。

## CC-SG の電源切断

V1 ユニットが稼働していて CC-SG の実行中に AC 電源が切断した場合、V1 ユニット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、V1 ユニットは自動的に再起動します。ただし、V1 ユニット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 V1 ユニット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、次の手順に従うことを推奨します。**

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。G1 ユニットでは、背面に**電源**ボタンがあります。
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 Diagnostic Console 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。

# 互換表

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。

- [**管理**] メニューで、[**互換表**] をクリックします。

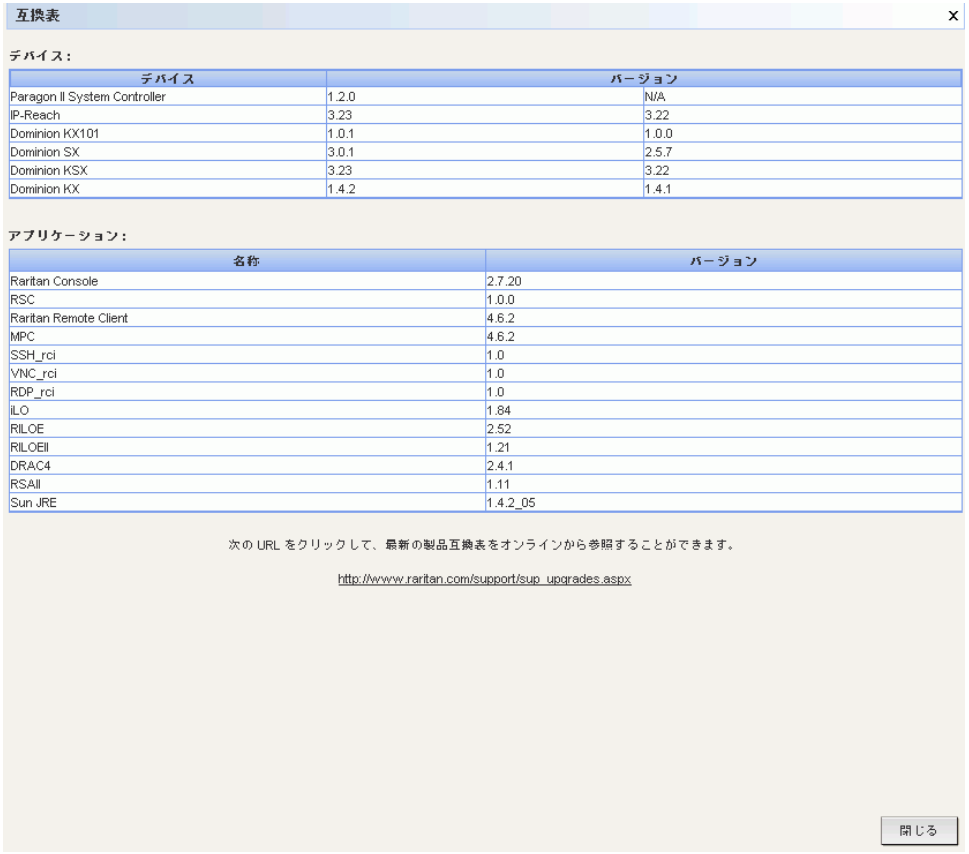


*図 7 互換表*

# 第 3 章 : ガイド付き設定を使用した CC-SG の設定

## ガイド付き設定による CC-SG の設定の準備

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と CC-SG 管理者アカウントの作成を含めて、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。

## ガイド付き設定の概要

ガイド付き設定は、システム構成を完了した後、最初の CC-SG 構成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。

## ガイド付き設定の開始 :

[**管理**] メニューで、[**ガイド付き設定**] をクリックします。[**ガイド付き設定**] ウィンドウが表示されます。ウィンドウの左パネルには、**ガイド付きタスク**がツリー表示されます。ウィンドウの右側には、アクティブ タスクのパネルが表示されます。

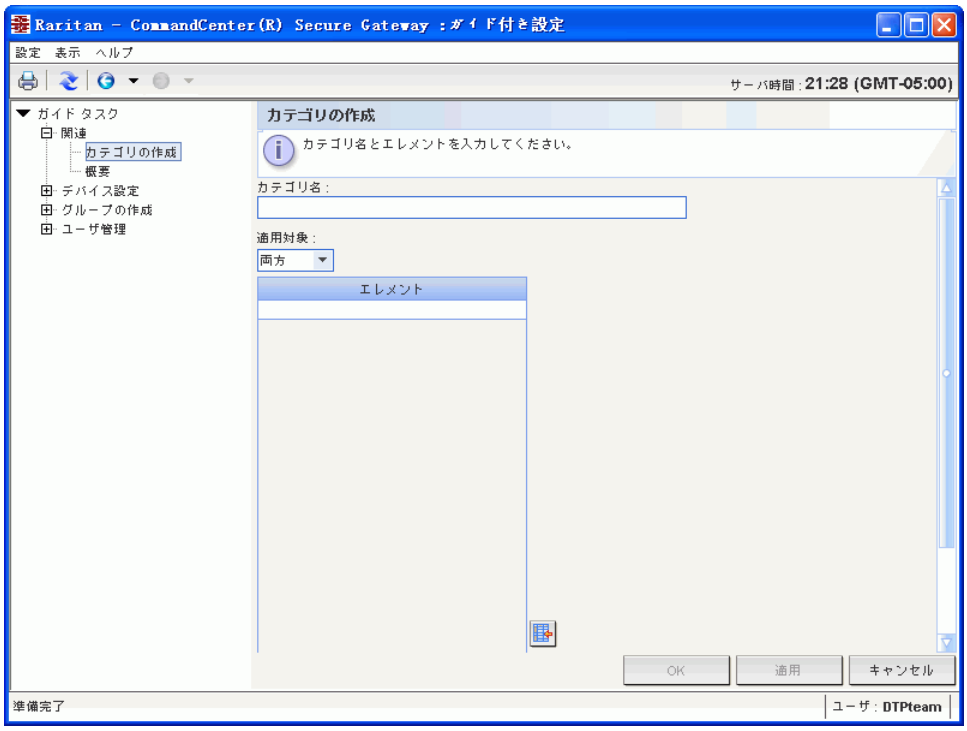


*図 8 ガイド付き設定ウィンドウ*

ガイド付き設定は、4 つのタスクに分類されます。次のセクションで、各分類について説明します。

- **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。
- 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。
- **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。
- **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。

# 関連

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、カテゴリのサブセットである関連エレメントが含まれます。たとえば、場所ごとに装置を整理するために「Location」というカテゴリと、「Philadelphia」、「New York」「New Orleans」など、各サーバの場所に対応するエレメントを作成します。

## カテゴリとエレメントの作成

1. [**ガイド付き設定**] ウィンドウでデフォルトのパネルは [**カテゴリの作成**] です。[**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。

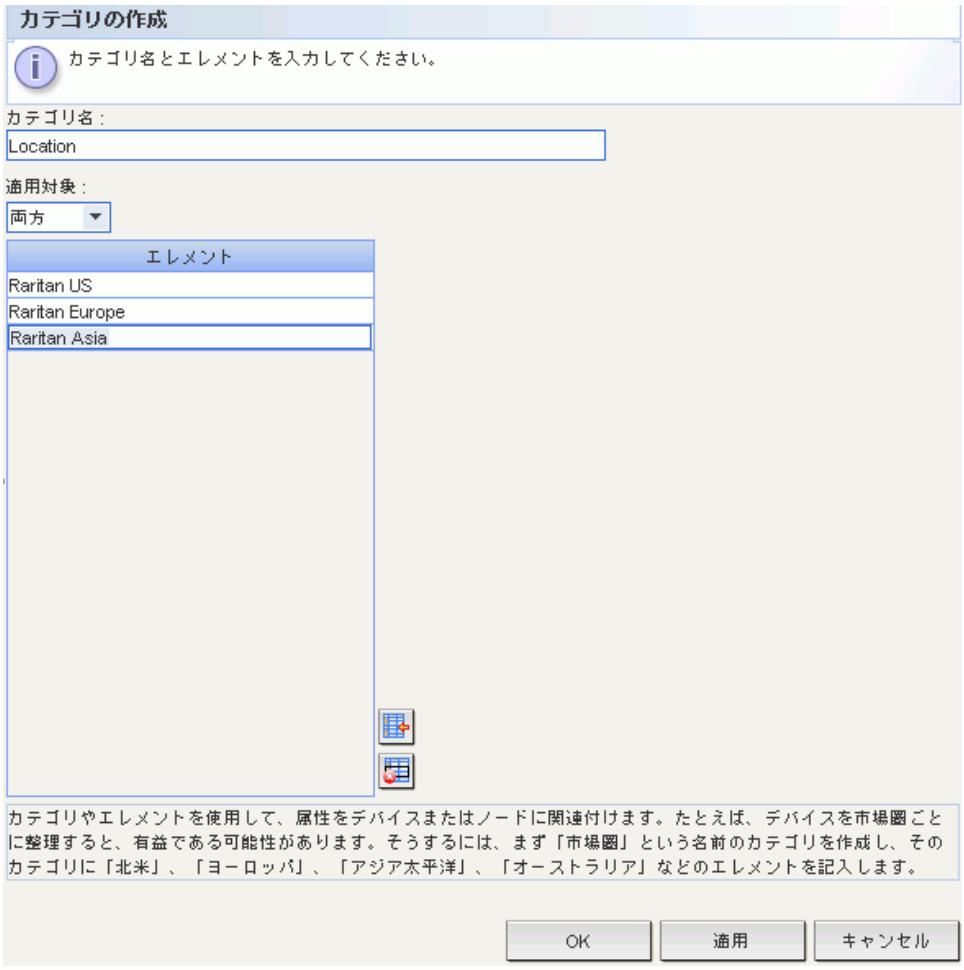


*図 9 ガイド付き設定 - カテゴリとエレメントの作成*

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すことができます。[**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)。

- 必要に応じて、[**新しい行をテーブルに追加**] アイコン  をクリックして、さらに行を [**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、エレメントの行を選択し、[**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。これにより、選択したエレメントが [**エレメント**] テーブルから削除されます。

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。
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

1. ガイド付き設定の第 2 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、デバイスに関連するカテゴリごとに 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イ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

1. 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 [**デバイス検出**] パネルを開くこともできます。

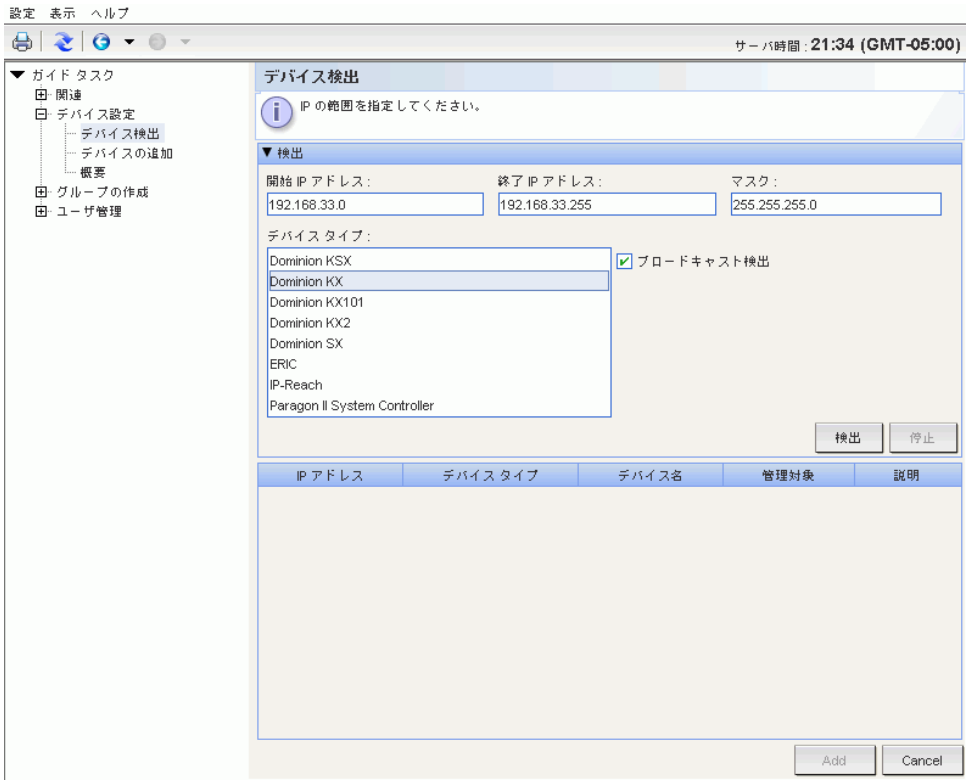


*図 10 ガイド付き設定ウィンドウ - デバイス検出*

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、デバイスの IP アドレスを検索する範囲を入力します。
3. [**マスク**] フィールドに、デバイスを検索するサブネット マスクを入力します。
4. [**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、**CONTROL** キーを押しながらデバイス タイプをクリックします。
5. CC-SG と同じサブネットにあるデバイスを検索する場合は、[ブロードキャスト検出] をオンにします。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] の選択をオフにします。

6. [**検出**] をクリックします。
7. 検出が完了したら、確認メッセージがポップアップ表示されます。確認メッセージで [**OK**] をクリックします。
8. 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、パネルの下部で検出結果の表示が拡張されます。

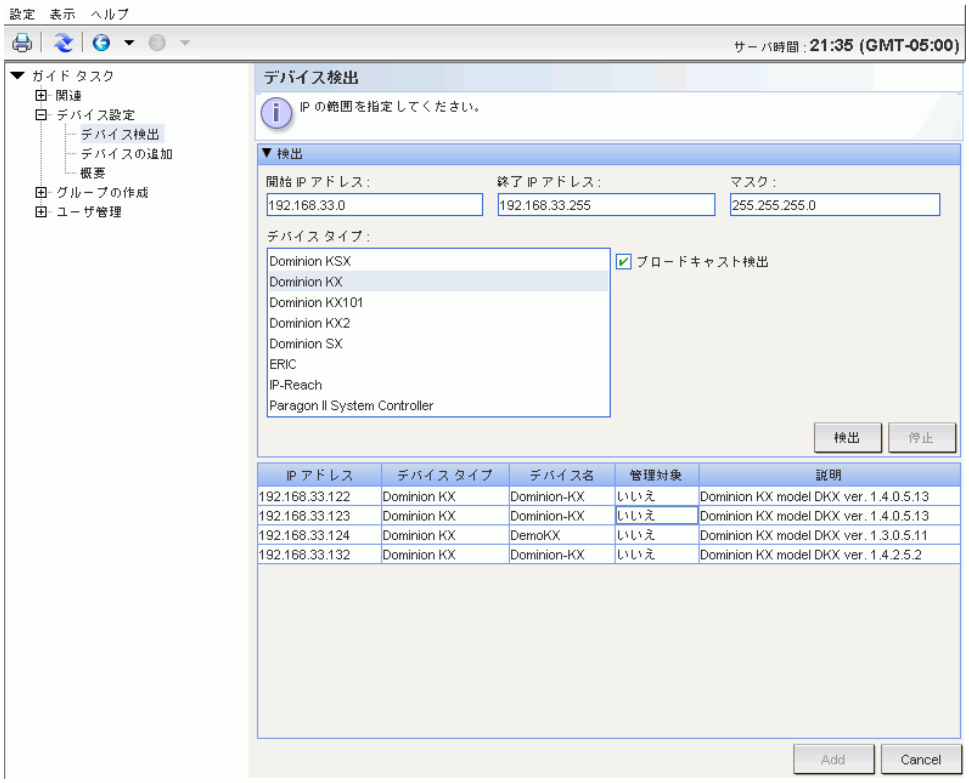


*図 11 ガイド付き設定 - デバイス検出結果*

9. 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応じて若干異なります。

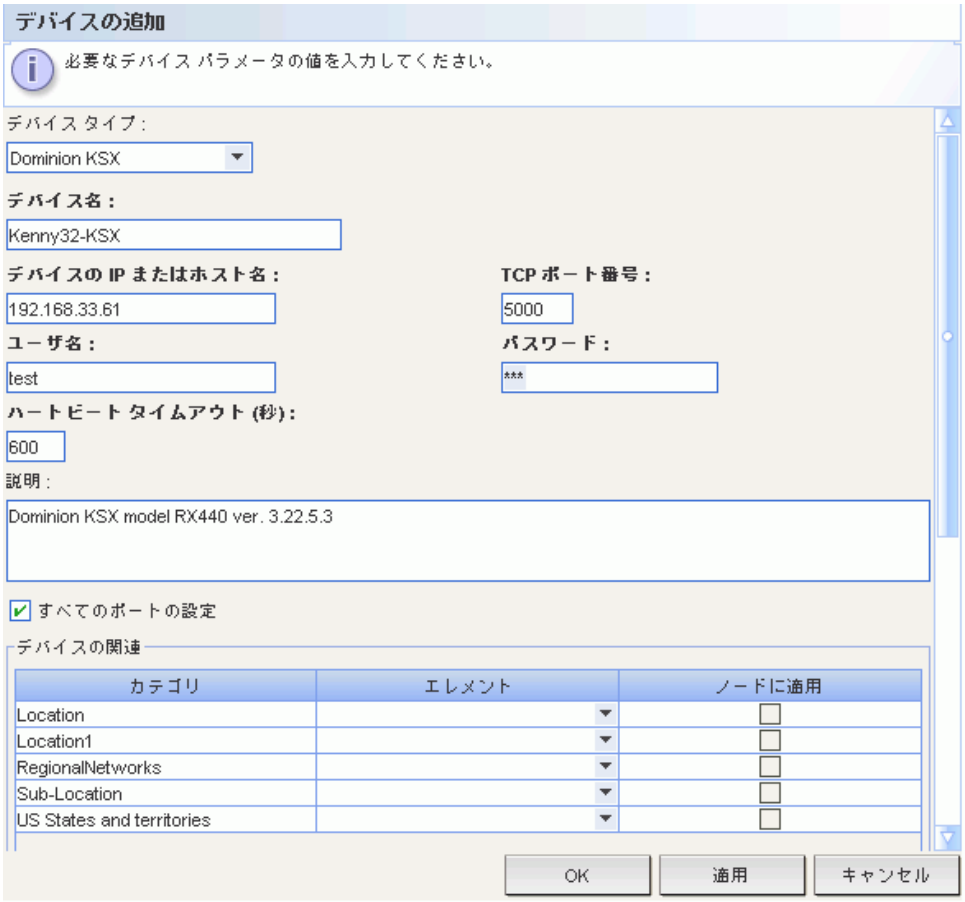


*図 12 ガイド付き設定 - デバイスの追加*

10. [**デバイス名**] と [**説明**] は、新しい情報を入力することにより変更できます。
11. 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し、必要に応じて正しいアドレスをフィールドに入力します。
12. [**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。
13. [**ユーザ名**] フィールドと [**パスワード**] フィールドに、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入力します。
14. [**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。
15. Dominion SX デバイスを追加する場合、デバイスへのローカル アクセスを許可するときは、[**ローカル アクセス**] で [**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。
16. サージ プロテクタ 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、サージ プロテクタに含まれるコンセントの数を選択します。
17. 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 の設定内容に一致させ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。
18. デバイス上で使用可能なすべてのポートを構成する場合は、[**すべてのポートの設定**] チェック ボックスをオンにします。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。

19. 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。
20. 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オンにします。
21. 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た後、このセクションの手順を繰り返してデバイスを追加します。
22. 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**] パネルには、追加したデバイスのリストが表示されます。
23. [**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

ガイド付き設定の第 3 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

1. デバイス設定タスクが終わった後、[**続行**] をクリックすると、[**デバイス グループ マネージャ**] 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 [**デバイス グループの追加**] をクリックして [**デバイス グループ マネージャ**] パネルを開くこともできます。
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 マネージャ**] パネルの [**デバイスの選択**] タブをクリックします。

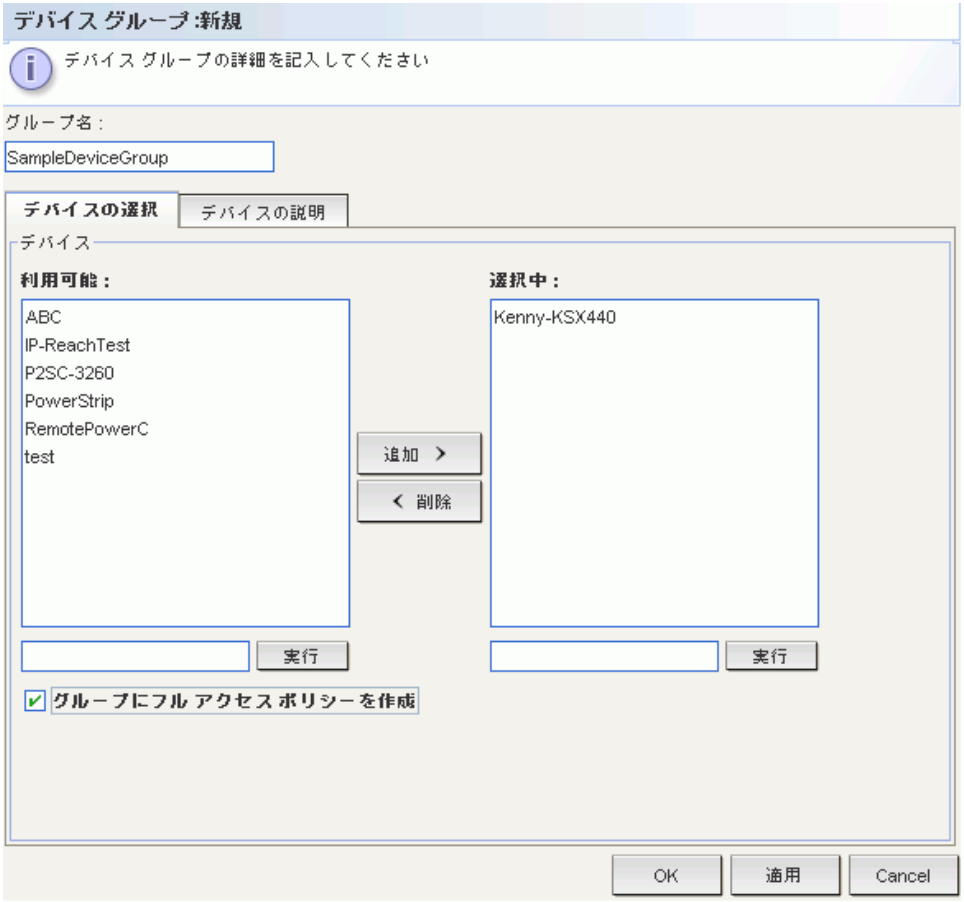


*図 13 ガイド付き設定 - デバイス グループ マネージャ、デバイスの選択*

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。

- グループからデバイスを削除する場合は、[**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**] リストのいずれかで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 マネージャ**] 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。

d. 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オンにします。

e. 別のデバイス グループを追加する場合は、[**適用**] をクリックしてこのグループを保存した後、このセクションの手順を繰り返してデバイス グループを追加します。

f. 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 マネージャ**] 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**] をクリックして [**ノード グループ マネージャ**] パネルを開くこともできます。

g. [グループ名] フィールドに作成するノード グループの名前を入力します。

h. 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. [**デバイス グループ マネージャ**] パネルの [**ノードの選択**] タブをクリックします。

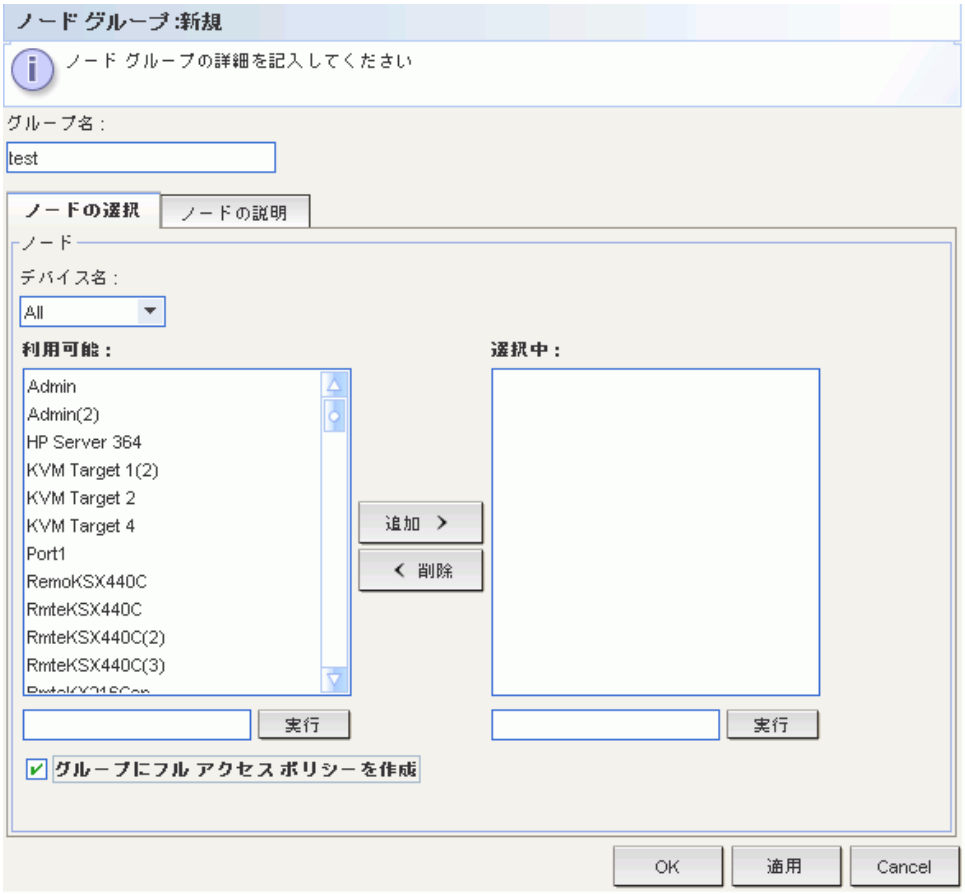


*図 14 ガイド付き設定 ーノード グループ マネージャ、ノードの選択*

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場合は、[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. [**デバイス グループ マネージャ**] 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。詳細については、「第 8 章 : ポリシー」を参照してください。

d. 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オンにします。

e. 別のノード グループを追加する場合は、[**適用**] をクリックしてこのグループを保存した後、このセクションの手順を繰り返してノード グループを追加します。

f. 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。[**Group Summary**](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。

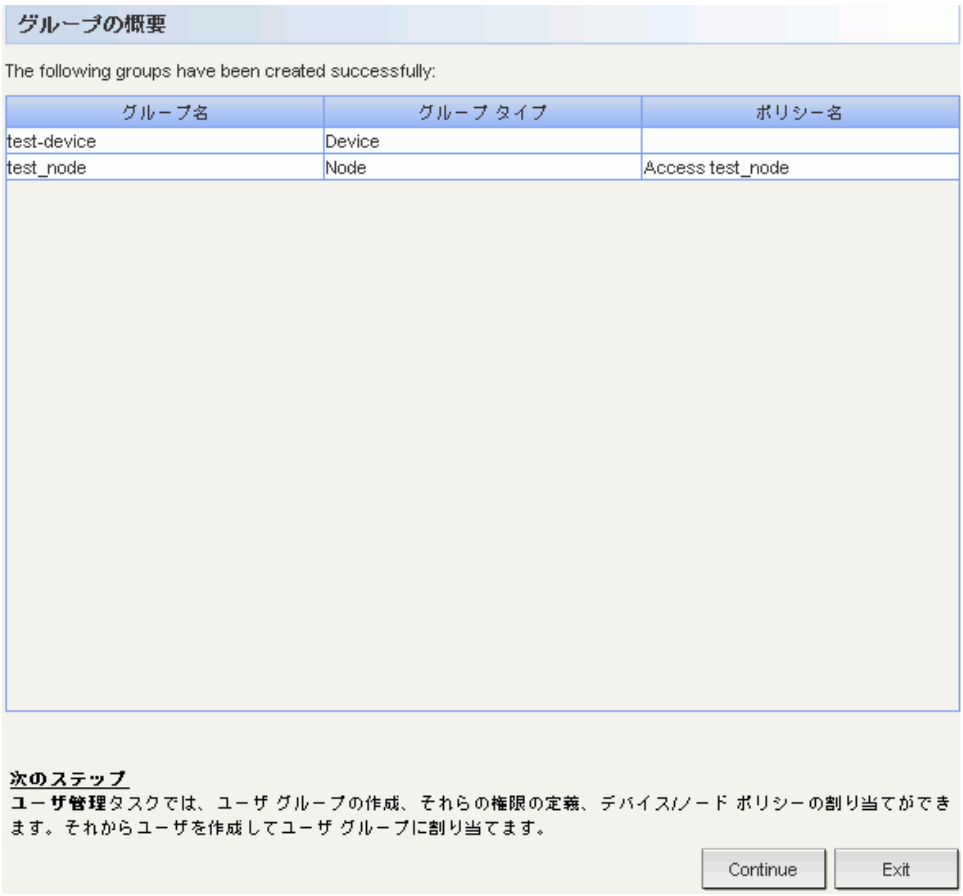


*図 15 ガイド付き設定ーGroup Summary(グループの概要)*

g. [**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

ガイド付き設定の第 4 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 グループのメンバーが実行できる作業を指定します。ポリシーでは、ユーザ グループのメンバー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

1. **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。

2. [**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。
3. [**説明**] フィールドに、ユーザ グループの説明を入力します。
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オンにするか、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オンにします。
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のタイプに対応するチェックボックスをオンにします。

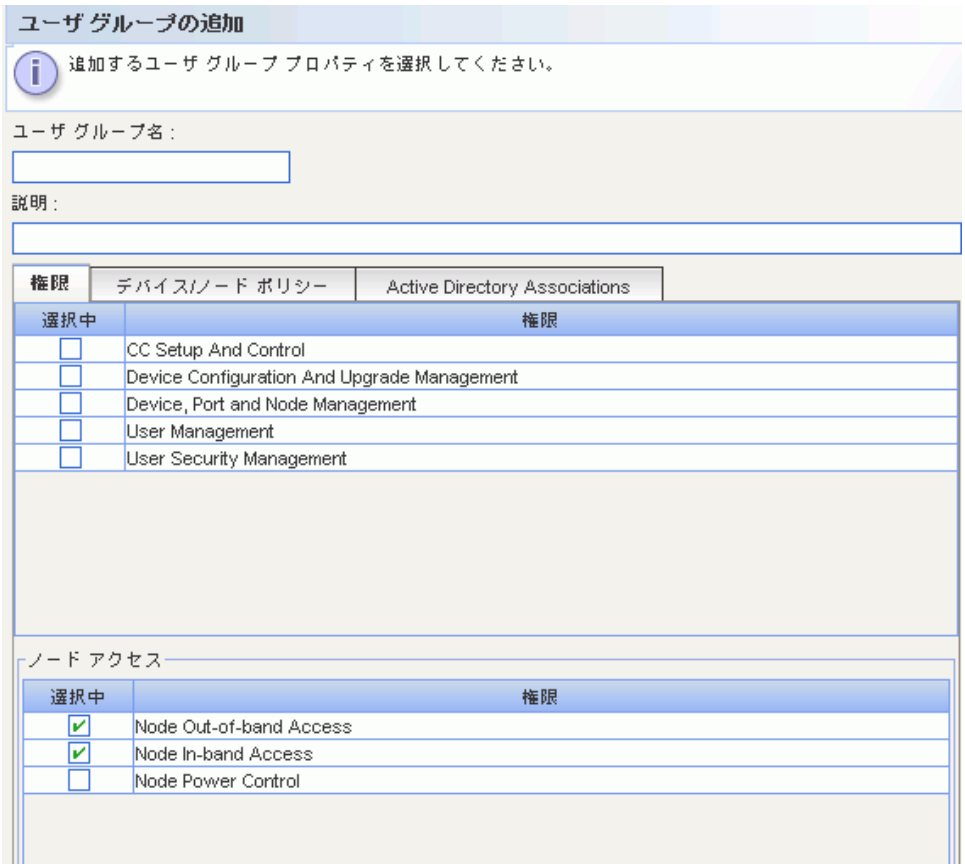


*図 16 ユーザ グループの追加ー権限*

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**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。

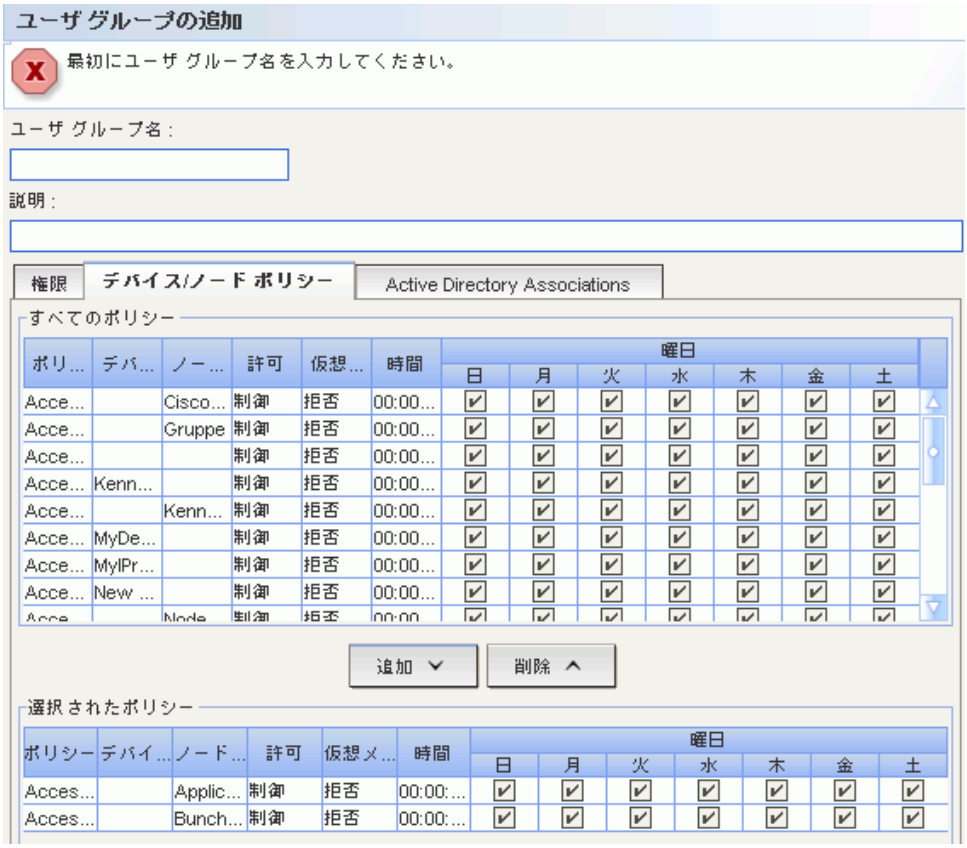


*図 17 ユーザ グループの追加ーポリシー*

8. 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。
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、[**Active Directory Associations**](Active Directory 関連) 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オンにします。
10. 別のユーザ グループを追加する場合は、[**適用**] をクリックしてこのグループを保存した後、このセクションの手順を繰り返してユーザ グループを追加します。
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 [**ユーザの追加**] パネルを開くこともできます。
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オンにします。
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オンにします。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 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オンにします。
18. [**有効期間 (日数)**] フィールドに、変更を強制す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。

# 第 4 章 : 関連の作成

## 関連

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、カテゴリのサブセットである関連エレメントが含まれます。たとえば、New York、Philadelphia、New Orleans 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 (New York、Philadelphia、および New Orleans) 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。次の図は、この例で作成したカスタム表示を示しています。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。

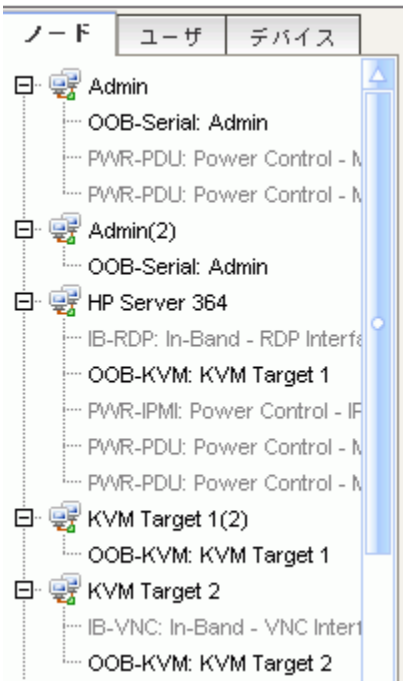


*図 18 CC-SG 関連機能の例*

### 関連の用語

次の定義を読んで、関連に関する理解を深めてください。

- **関連** – カテゴリ、カテゴリのエレメント、およびノードおよびデバイスの間の関係です。たとえば、「Location」カテゴリをデバイスに関連付けるとします。まず関連を作成、あるいは編集してから、デバイスとポートを CC-SG に追加します。
- **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、「New York City」、「Philadelphia」などのエレメントを含む「Location」はカテゴリです。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。CC-SG にデバイスを追加する場合は、この情報を追加対象に関連付けます。
- **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」カテゴリに属します。
- **デバイス** – CC-SG で管理する Dominion KX、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 システムまたはノードを制御します。

- **ノード** – CC-SG がアクセスおよび管理できるターゲット システムまたはサーバです。CC-SG では、インタフェースにより、ノードをクリックし、ノードにアクセスしてそれを管理できます。

## 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。このため、カテゴリとエレメントを定義してから、Raritan デバイスを CC-SG に追加する必要があります。

カテゴリは、同様のエレメントのグループです。たとえば、場所ごとに Raritan デバイスをグループ化するには、カテゴリ Location を定義し、New York、Philadelphia、New Orleans などの一連のエレメントを含めます。

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、New York 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/New York を使用できます。

カテゴリやエレメントの典型的な関連の設定のその他の例を次に示します。

| カテゴリ | エレメント |
|---|---|
| Location | New York City、Philadelphia、New Orleans |
| OS Type | Unix、Windows、Linux |
| Department | Sales、IT、Engineering |

関連は常にシンプルに設定して、サーバ/ノードの整理目的やユーザ アクセスの目的を達成する必要があります。ノードは、単にカテゴリの単一のエレメントに割り当てることができます。たとえば、1 つのターゲット サーバを OS 機種のカテゴリの Windows と Unix の両方のエレメントに割り当てることはできません。

サーバが似通っており、ランダムに整理する必要がある場合、システムの整理に便利な方法を次に示します。

| カテゴリ | エレメント |
|---|---|
| usergroup1 | usergroup1node |
| usergroup2 | usergroup2node |
| usergroup3 | usergroup3node |

デバイスとノードを CC-SG に追加しながら、事前に定義したカテゴリやエレメントにこれらをリンクさせます。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、多くの構成タスクを自動インタフェース内で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。詳細については、「**第 3 章 : ガイド付き設定を使用した CC-SG の設定**」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。構成タスクが自動化されることはありません。詳細については、次の「**関連マネージャ**」を参照してください。

# 関連マネージャ

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。

## カテゴリの追加

1. [**関連**] メニューの [**関連**] をクリックします。[**関連マネージャ**] 画面が表示されます。

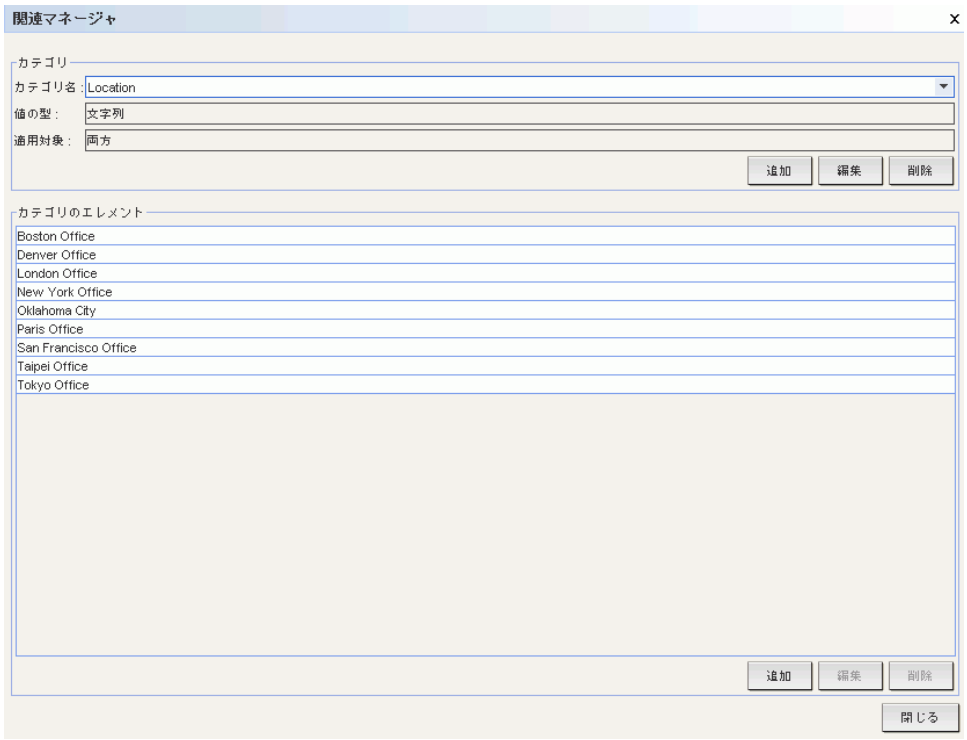


*図 19 関連マネージャ画面*

2. [**カテゴリ**] パネルで [**追加**] をクリックし、新しいカテゴリを追加します。[**カテゴリの追加**] ウィンドウが表示されます。

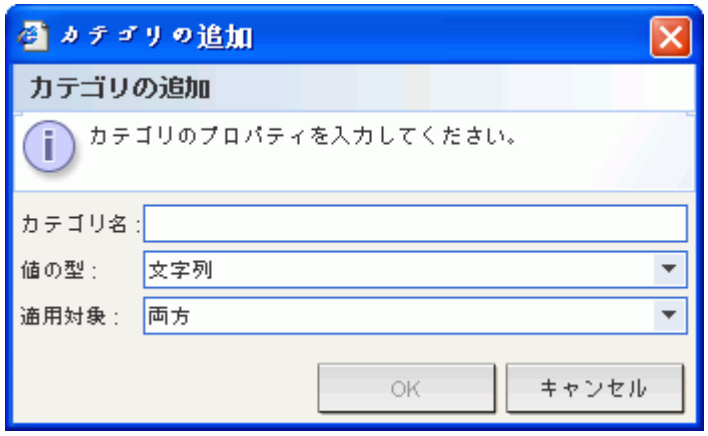


*図 20 カテゴリの追加ウィンドウ*

3. [**カテゴリ名**] フィールドにカテゴリ名を入力します。最大 31 文字で設定します。
4. [**値の型**] ドロップダウン矢印をクリックし、値の型として [**文字列**] または [**整数**] を選択します。
5. [**適用対象**] ドロップダウン矢印をクリックし、このカテゴリを適用するデバイスのタイプ、つまり [**デバイス**]、[**ノード**]、[**両方**] のいずれかを選択します。
6. [**OK**] をクリックして新しいカテゴリを作成します。[**キャンセル**] をクリックすると、作成せずに終了します。[**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。

## カテゴリの編集

1. [**関連**] メニューの [**関連**] をクリックします。[**関連マネージャ**] 画面が表示されます。
2. [**カテゴリ名**] ドロップダウン矢印をクリックし、編集するカテゴリを選択します。
3. 画面の [**カテゴリ**] パネルで [**編集**] をクリックし、カテゴリを編集します。[**カテゴリの編集**] ウィンドウが表示されます。


*図 21 カテゴリの編集ウィンドウ*

4. [**カテゴリ名**] フィールドに新しいカテゴリ名を入力します。
5. [**適用対象**] ドロップダウン矢印をクリックし、このカテゴリを [**デバイス**]、[**ノード**]、[**両方**] のどれに適用するかを変更します。ただし、文字列値を整数値にも、整数値を文字列値にも変更できません。この種の変更が必要な場合は、カテゴリを削除して新しいカテゴリを追加してください。
6. [**OK**] をクリックして変更を保存します。[**カテゴリ名**] フィールドに更新された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。

1. [**関連**] メニューの [**関連**] をクリックします。[**関連マネージャ**] 画面が表示されます。
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**] ウィンドウが表示されます。

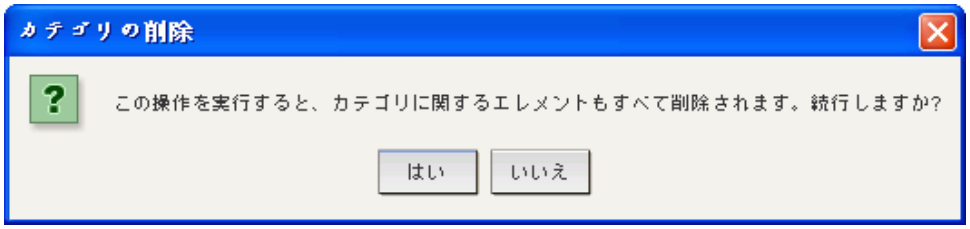


*図 22 カテゴリの削除ウィンドウ*

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

1. [**関連**] メニューの [**関連**] をクリックします。[**関連マネージャ**] 画面が表示されます。

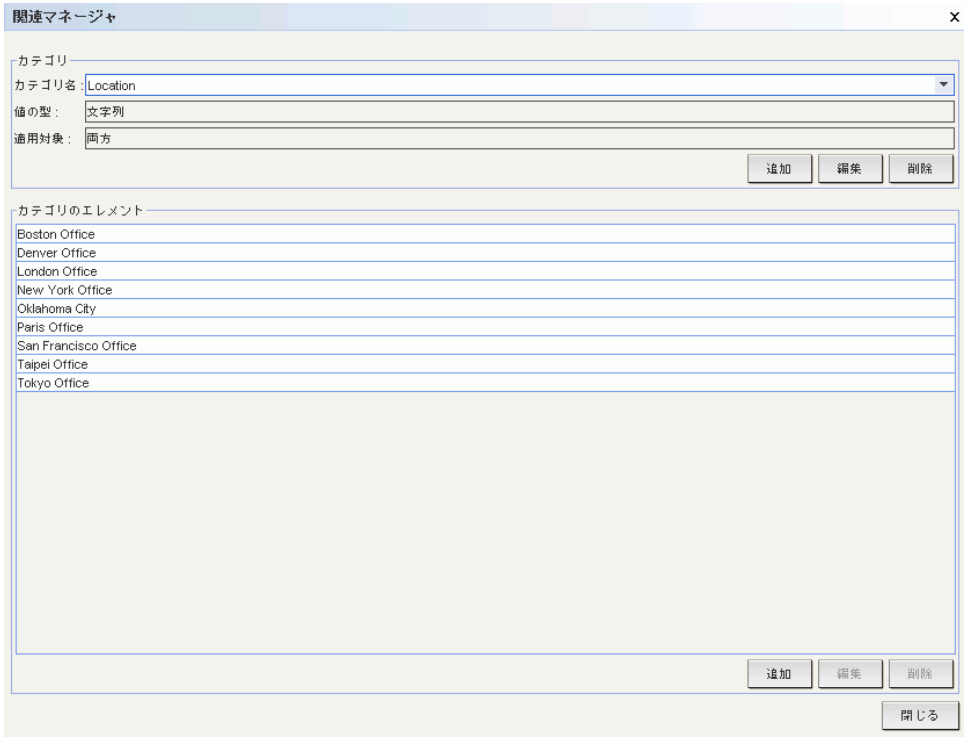


*図 23 関連マネージャ画面*

2. [**カテゴリ名**] ドロップダウン矢印をクリックし、新しいエレメントを追加するカテゴリを選択します。
3. [**カテゴリのエレメント**] パネルで [**追加**] をクリックし、新しいエレメントを追加します。[**エレメントの追加**] ウィンドウが表示されます。

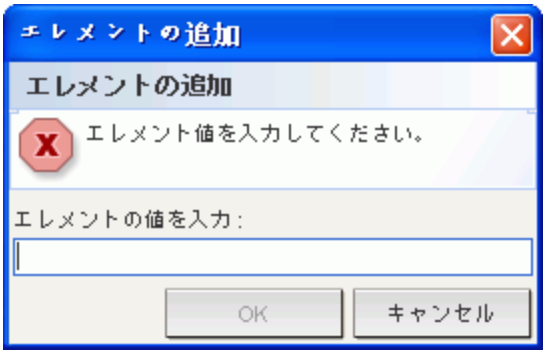


*図 24 エレメントの追加ウィンドウ*

4. [**エレメントの値を入力**] フィールドに新しいエレメントを入力します。
5. [**OK**] をクリックしてエレメントを追加します。[**キャンセル**] をクリックすると、何もせずにウィンドウを閉じます。[**カテゴリのエレメント**] パネルに新しいエレメントが表示されます。

## エレメントの編集

1. [**関連**] メニューの [**関連マネージャ**] をクリックします。[**関連マネージャ**] 画面が表示されます。
2. [**カテゴリ名**] ドロップダウン矢印をクリックし、編集するエレメントの属するカテゴリを選択します。
3. [**カテゴリのエレメント**] リストから編集するエレメントを選択し、[**カテゴリのエレメント**] パネルで [**編集**] をクリックします。[**エレメントの編集**] ウィンドウが表示されます。

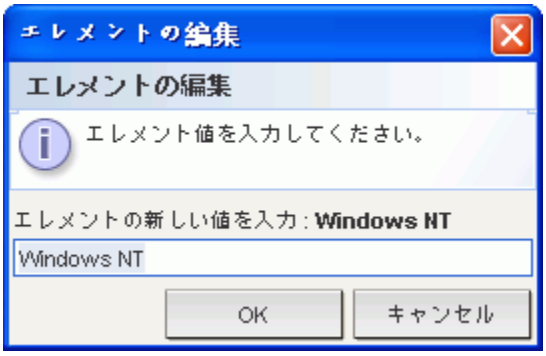


*図 25 エレメントの編集ウィンドウ*

4. [**エレメントの新しい値を入力**] フィールドにエレメントの新しい名前を入力します。
5. [**OK**] をクリックしてエレメントを適用します。[**キャンセル**] をクリックすると、何もせずにウィンドウを閉じます。[**カテゴリのエレメント**] リストに新しいエレメント名が表示されます。

## エレメントの削除

エレメントを削除すると、すべての関連からそのエレメントが削除され、関連フィールドは空白になります。

1. [**関連**] メニューの [**関連**] をクリックします。[**関連マネージャ**] 画面が表示されます。
2. [**カテゴリ名**] ドロップダウン矢印をクリックし、削除するエレメントの属するカテゴリを選択します。
3. [**カテゴリのエレメント**] リストから削除するエレメントを選択し、[**カテゴリのエレメント**] パネルで [**削除**] をクリックします。[**エレメントの削除**] ウィンドウが表示されます。

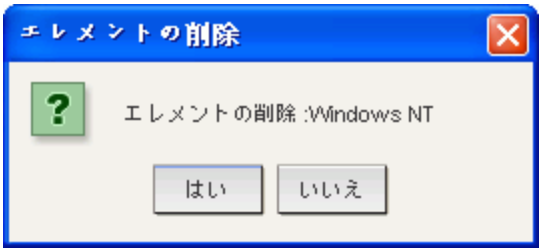


*図 26 エレメントの削除ウィンドウ*

4. [**はい**] をクリックしてエレメントを削除します。[**いいえ**] をクリックすると、何もせずにウィンドウを閉じます。[**カテゴリのエレメント**] リストにエレメント名が表示されなくなります。

---

***注 :*** *エレメントを削除すると、すべてのデバイスおよびノード カテゴリ関連からそのエレメントが削除され、関連付けられていたエレメントのフィールドはすべて空白になります。*

---

*本ページは意図的に空白となっています。*

# 第 5 章 : デバイスおよびデバイス グループの追加

Dominion シリーズ デバイスや IP-Reach ユニットなどの Raritan デバイスを CC-SG により構成および管理するには、まずその Raritan デバイスを CC-SG に追加する必要があります。[**デバイス**] メニューで、デバイスおよびポートに関連するすべての機能を使用できます。また、[**デバイス**] タブでデバイスまたはポートを右クリックし、表示されるメニューから選択することでも、一部の機能にアクセスできます。

***注** : iLO/RILOE デバイス、IPMI デバイス、Dell DRAC デバイス、IBM RSA デバイス、その他の「標準」デバイスを構成する場合は、[**ノードの追加**] メニューを使用し、該当アイテムを接続インタフェースとして追加します。詳細は、「**第 6 章 : ノードとインタフェースの設定**」を参照してください。*

## [デバイス] タブ

[**デバイス**] タブをクリックするとデバイス ツリーが表示されます。

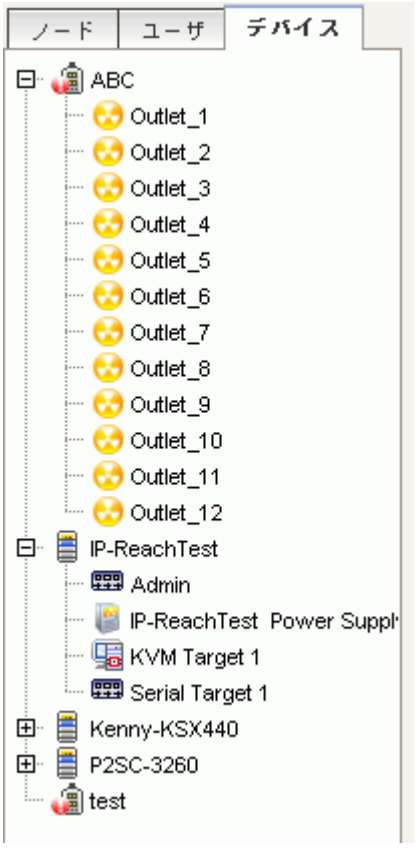


*図 27 デバイス ツリー*

[**デバイス**] タブには、一連のデバイスとその構成済みポートが表示されます。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、隣に + 記号が表示されます。+ 記号をクリックすると、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 |
| | |
| | デバイスが停止した状態 |
| | デバイスが利用不可能 |
| | |
| | サージ プロテクタ |
| | アウトレット ポート |

[**デバイス**] タブでデバイスをクリックすると、[**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。

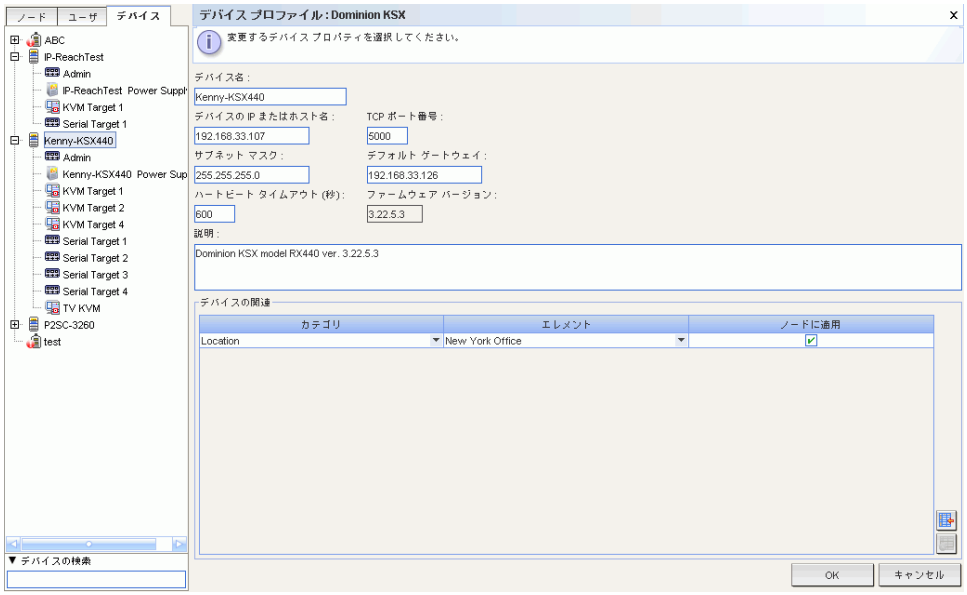


*図 28 デバイス タブおよびデバイス プロファイル*

## 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、「**第 7 章 : ユーザとユーザ グループの追加および管理**」で説明する「**プロファイル**」画面で設定できます。

デバイスを検索するには、デバイス ツリーの下にある [**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。

| ワイルドカード | 説明 |
|---|---|
| ? | 任意の 1 文字を示します。 |
| [-] | 範囲内の 1 文字を示します。 |
| * | ゼロ以上の文字数を示します。 |

たとえば、

| 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。 |

**重要 : メニュー バー コマンドの多くは、デバイス ツリーのデバイスまたはポートを右クリックして表示されるショートカット メニューからも実行できます。**

# デバイスの追加

ポートの構成またはポートを通じたノードへのアウト オブ バンド 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**] 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。

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**] メニューの [**デバイス マネージャ**] をクリックし、さらに [**デバイスの追加**] をクリックします。[**デバイスの追加**] 画面が表示されます。

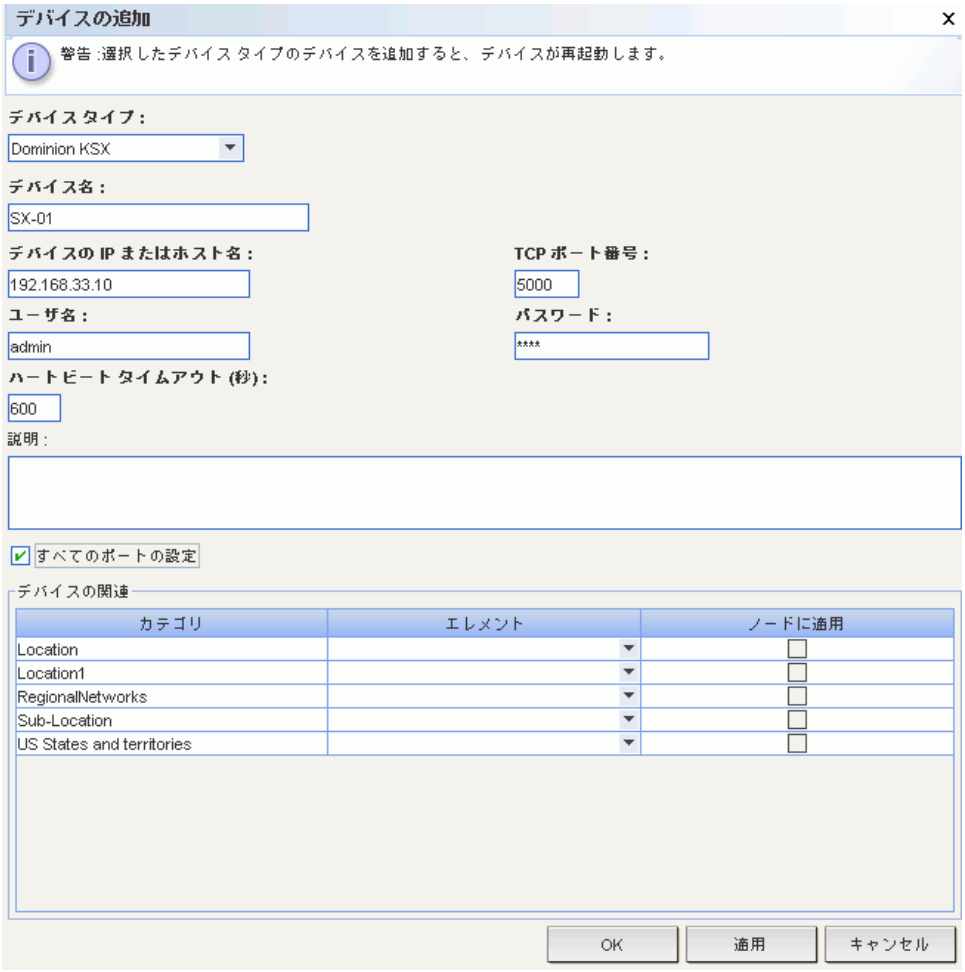


*図 29 デバイスの追加画面*

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。[**サージ プロテクタ**] を選択した場合、わずかに異なる [**デバイスの追加**] 画面が表示されます。

## KVM またはシリアル デバイスの追加

1. [**デバイス名**] フィールドにデバイス名を入力します。
2. [**デバイス IP またはホスト名**] 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。ホスト名の規則については、「**第 1 章 : はじめに**」の「**用語/略語**」を参照してください。
3. デバイスとの通信で使用する TCP 通信ポートを [**TCP ポート番号**] フィールドに入力します。大半の Raritan デバイスのデフォルト ポート番号は 5000 です。
4. [**ユーザー名**] フィールドに、このデバイスへのログオンに使用する名前を入力します。『Raritan デジタル ソリューション デプロイメント ガイド』に従って CC-SG へのデバイス追加の準備を進める場合は、デバイス上で構成した CC-SG 管理ユーザのユーザ名を入力します。

5. [**パスワード**] フィールドに、このデバイスにアクセスするためのパスワードを入力します。『Raritan デジタル ソリューション デプロイメント ガイド』に従って CC-SG へのデバイス追加の準備を進める場合は、デバイス上で構成した CC-SG 管理ユーザのユーザ名を入力します。
6. [**ハートビート タイムアウト (秒)**] フィールドに、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、秒単位で入力します。
7. 必要に応じて、CC-SG により管理されているこのデバイスに対して直接アクセスをユーザに許可する場合は、[**ローカル アクセス**] の下にある[**許可**] をオンにします。
8. オプションとして、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。
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オンにします。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。デバイスの追加時にこのチェックボックスがオンである場合、各ポートについ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。
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**のリストを構成できます。詳細は、「**第 4 章 : 関連の作成**」を参照してください。

カテゴリとエレメントを作成するには

   a. リストに表示された各カテゴリについて、[**エレメント**] ドロップダウン メニューをクリックし、リストからデバイスに適用するエレメントを選択します。使用しないカテゴリでは、[**エレメント**] フィールドで空白のアイテムを選択します。
   b. 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オンにします。

   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。カテゴリおよびエレメントを作成する方法の詳細は、「**第 4 章 : 関連の作成**」を参照してください。

11. このデバイスの設定が終わったら、[**適用**] をクリックしてこのデバイスを追加します。これにより、さらにデバイスを追加できる空白の [**デバイスの追加**] 画面が開きます。また、[**OK**] をクリックすると、別の [**デバイスの追加**] 画面を開くことなく、このデバイスを追加します。
12. 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、警告メッセージが表示され、このまま続行するかどうかをたずねます。[**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。この章の後で説明する「**デバイスのアップグレード**」を参照してください。

## サージ プロテクタ デバイスの追加

サージ プロテクタ デバイスを追加する場合、CC-SG でアウトレットを自動的に構成できます。アウトレットが構成されたら、パワー インタフェースをノードに追加することにより、各アウトレットを電源の提供先ノードに関連付けることができます。詳細については、「第 6 章：ノードとインタフェースの設定」を参照してください。また、CC-SG によるアウトレットの構成を行わず、後で構成することもできます。

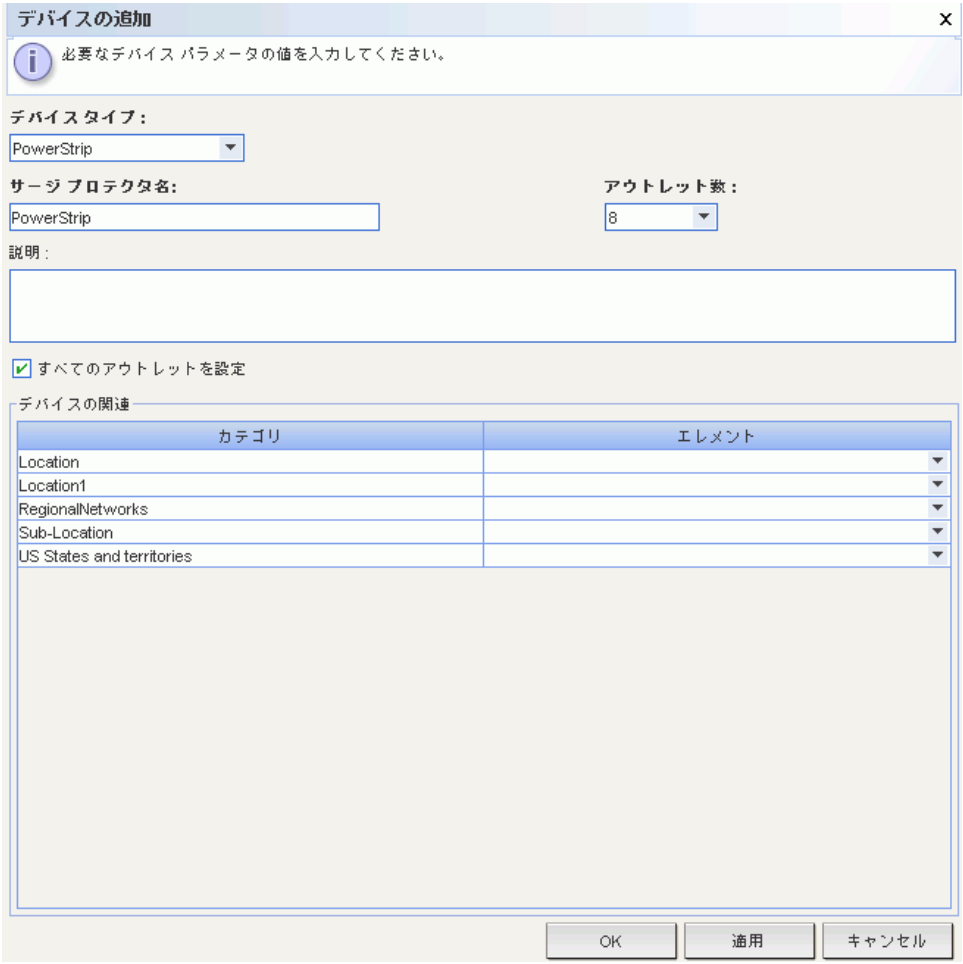


*図 30 サージ プロテクタ デバイスの追加*

1. [**サージ プロテクタ名**] フィールドで、サージ プロテクタの名前を入力します。
2. [**アウトレット数**] ドロップダウン メニューをクリックし、このサージ プロテクタに含まれるアウトレット数を選択します。
3. [**管理デバイス**] ドロップダウン メニューをクリックし、このサージ プロテクタを管理するために使用するデバイスをリストから選択します。
4. [**管理ポート**] ドロップダウン メニューをクリックし、このサージ プロテクタが接続する管理デバイスのポートを選択します。
5. オプションとして、このサージ プロテクタの短い説明を [**説明**] フィールドに入力します。
6. このデバイスの各アウトレットを [**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**] をオンにします。
7. このサージ プロテクタ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**のリストを構成できます。詳細は、「**第 4 章：関連の作成**」を参照してください。

- リストに表示された各カテゴリについて、[エレメント] ドロップダウン メニューをクリックし、リストからデバイスに適用するエレメントを選択します。使用しないカテゴリでは、[エレメント] フィールドで空白のアイテムを選択します。

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。カテゴリおよびエレメントを作成する方法の詳細は、「第 4 章 : 関連の作成」を参照してください。

8. このデバイスの設定が終わったら、[**適用**] をクリックしてこのデバイスを追加します。これにより、さらにデバイスを追加できる空白の [**デバイスの追加**] 画面が開きます。また、[**OK**] をクリックすると、別の [**デバイスの追加**] 画面を開くことなく、このサージ プロテクタを追加します。

## デバイス検出

[**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。この検索により、Paragon II、System Controller、IP-Reach、Dominion KX、Dominion KSX101、Dominion KSX、Dominion SX、eRIC の各ユニットを含む Raritan 製のデバイスで、ネットワークに新しく接続されたものと既存のものすべてが自動的に検出されます。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。

1. [**デバイス**] メニューの [**デバイス検出**] をクリックします。[**デバイス検出**] 画面が表示されます。

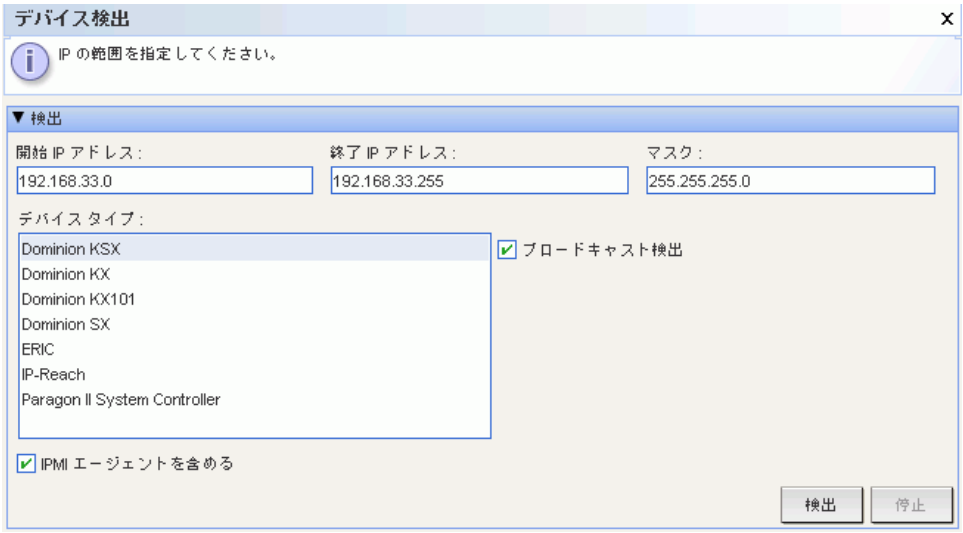


*図 31 デバイス検出画面*

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。この範囲に適用するマスクを指定します。マスクを指定しない場合、255.255.255.255 というブロードキャスト アドレスが送信され、ローカルのネットワーク全体にブロードキャストされます。サブネット間のデバイスを検出するには、マスクを指定する必要があります。

CC-SG と同じサブネットにあるデバイスを検索する場合は、[ブロードキャスト検出] をオンにします。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] の選択をオフにします。

特定の種類のデバイスを検索するには、デバイスの種類のリストで対象となるデバイスを選択します。デフォルトでは、すべてのデバイス タイプが選択されます。Ctrl キーとマウスクリックを使って、1 つかそれ以上のデバイス タイプを選択します。

3. IPMI 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] をオンにします。
4. [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。


*図 32 検出されたデバイスのリスト ウィンドウ*

5. 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] 画面には、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。

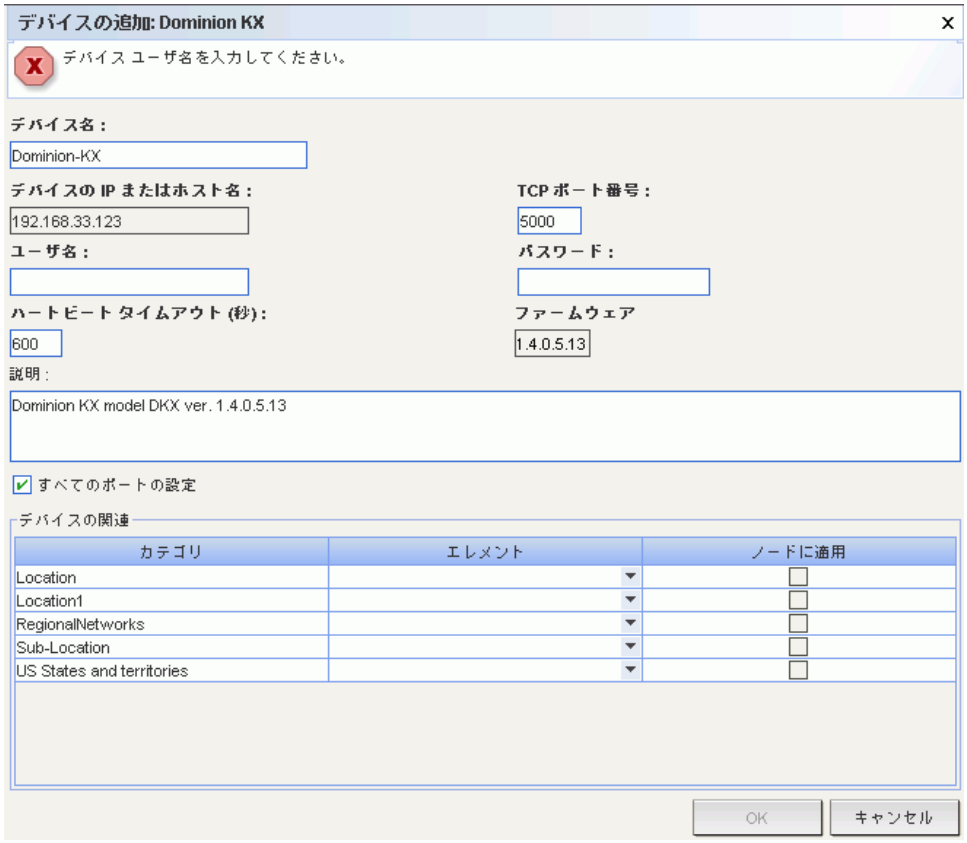


*図 33 検出されたデバイスの追加*

6. [**ユーザ名**] フィールドと [**パスワード**] フィールドにユーザ名とパスワード (各デバイスで CC-SG 用に作成) を入力します。 これで、CC-SG は将来デバイスと通信するときにデバイスを認証することができます。デバイスに適用する [**カテゴリ**] と [**エレメント**] を選択します。デバイスに接続するノードにもカテゴリとエレメントを適用する場合、対応する [**ノードに適用**] チェックボックスをオンにします。
7. オプションで、それぞれのニーズに合わせて、[**デバイス名**]、[**ハートビート タイムアウト**]、[**ローカル アクセス**] (デバイス タイプで使用可能な場合)、[**説明**]、[**すべてのポートの設定**]、および [**デバイスの関連**] フィールドを編集できます。
8. このデバイスの設定が終わったら、[**適用**] をクリックしてこのデバイスを追加します。これにより、次に検出されたデバイスの [**デバイスの追加**] 画面が開きます。また、[**OK**] をクリックすると、別の [**デバイスの追加**] 画面を開くことなく、他に検出されたデバイスを追加します。

9. 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、警告メッセージが表示され、このまま続行するかどうかをたずねます。[**はい**] をクリックして、デバイスを CC-SG に追加します。[**いいえ**] をクリックすると、この操作をキャンセルします。デバイスのファームウェアは、CC-SG へのデバイスの追加後にアップグレードできます。詳細については、本章の後で説明する「**デバイスのアップグレード**」を参照してください。

## デバイスの編集

デバイスは、その名前やプロパティを変更するために編集できます。

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。[**デバイス プロファイル**] 画面が表示されます。

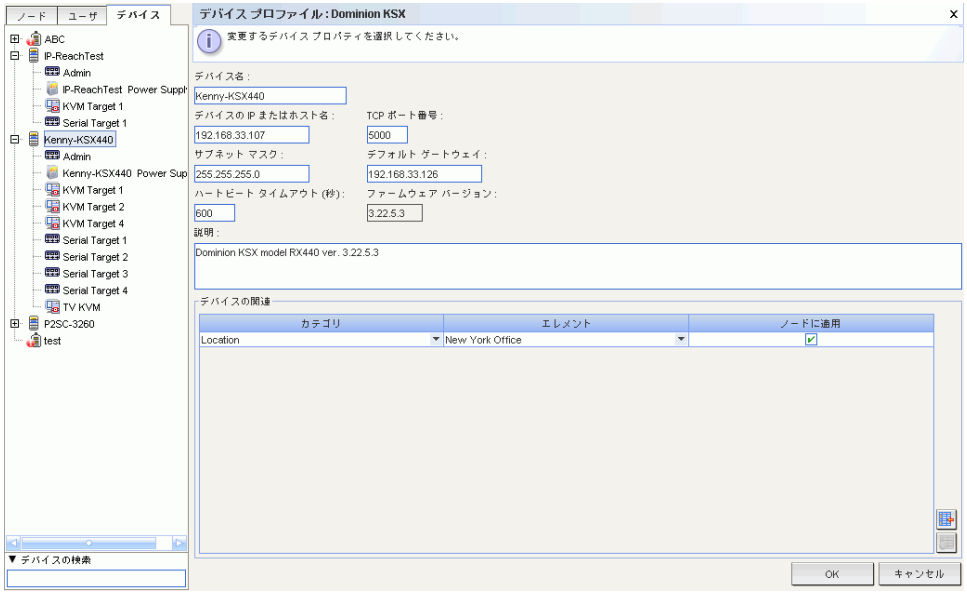


*図 34 デバイス プロファイル画面*

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。

2. [**OK**] をクリックして変更を保存します。「**デバイスが正常に更新されました**」というメッセージが表示され、デバイスが変更されたことを確認します。

### サージ プロテクタ デバイスの編集

管理されているサージ プロテクタ デバイスを編集し、その名前およびプロパティを変更し、アウトレット設定ステータスを表示できます。

1. [**デバイス**] タブをクリックし、編集するサージ プロテクタ デバイスを選択します。[**デバイス プロファイル : サージ プロテクタ**] 画面が表示されます。

この画面で、該当するフィールドに新しいデバイスのプロパティを入力します。必要に応じて、デバイスに関連するカテゴリとエレメントを編集します。

2. [**アウトレット**] タブをクリックすると、このサージ プロテクタのすべてのアウトレットが表示されます。
   - アウトレッ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。
   - アウトレットがノードに関連付けられている場合、アウトレットを選択して [**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。
3. [**OK**] をクリックして変更を保存します。「**デバイスが正常に更新されました**」というメッセージが表示され、デバイスが変更されたことを確認します。

# 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。**

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**] メニューの [**デバイス マネージャ**] をクリックし、さらに [**デバイスの削除**] をクリックします。[**デバイスの削除**] 画面が表示されます。

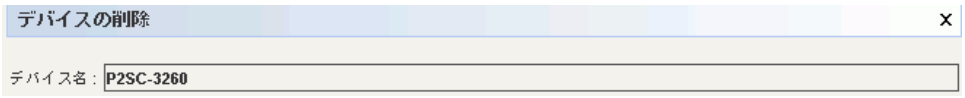


*図 35 デバイスの削除画面*

3. [**OK**] をクリックしてデバイスを削除します。[**キャンセル**] をクリックすると、削除せずに終了します。「**デバイスが正常に削除されました**」というメッセージが表示され、デバイスが削除されたことを確認します。

***注：** CC-SG から KSX デバイスを正常に削除するには、まず KSX デバイスを停止する必要があります。KSX デバイスを停止するには、[**デバイス**] タブでデバイスを右クリックし、[**管理の一時停止**] をクリックします。表示されるメッセージで [**はい**] をクリックして確認します。KSX デバイスが再起動します。デバイスが一時停止したら、CC-SG から削除できます。*

# ポートの設定

[**デバイスの追加**] 画面でのデバイスの追加時に [**すべてのポートの設定**] をオンにすることによりデバイスの全ポートの自動的な追加を選択しなかった場合、[**ポートの設定**] 画面でデバイス上の個別のポートまたはポート セットを CC-SG に追加できます。ポートを使用するアウト オブ バンド インタフェースをノードに追加する前に、そのポートを設定する必要があります。

## シリアル ポートの設定

1. [**デバイス**] タブをクリックし、デバイス ツリーからシリアル デバイスを選択します。
2. [**デバイス**] メニューの [**ポート マネージャ**] をクリックし、さらに [**ポートの設定**] をクリックします。[**ポートの設定**] 画面が表示されます。

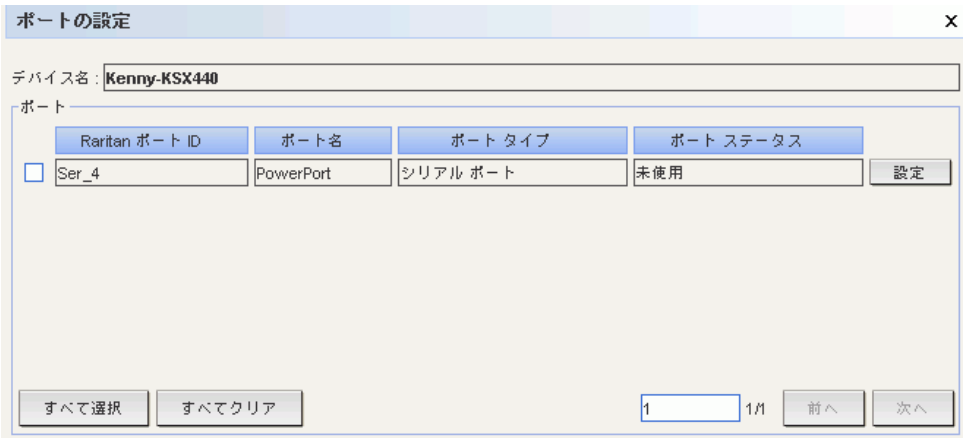


*図 36 ポートの設定画面*

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。[**シリアル ポートの設定**] 画面が表示されます。

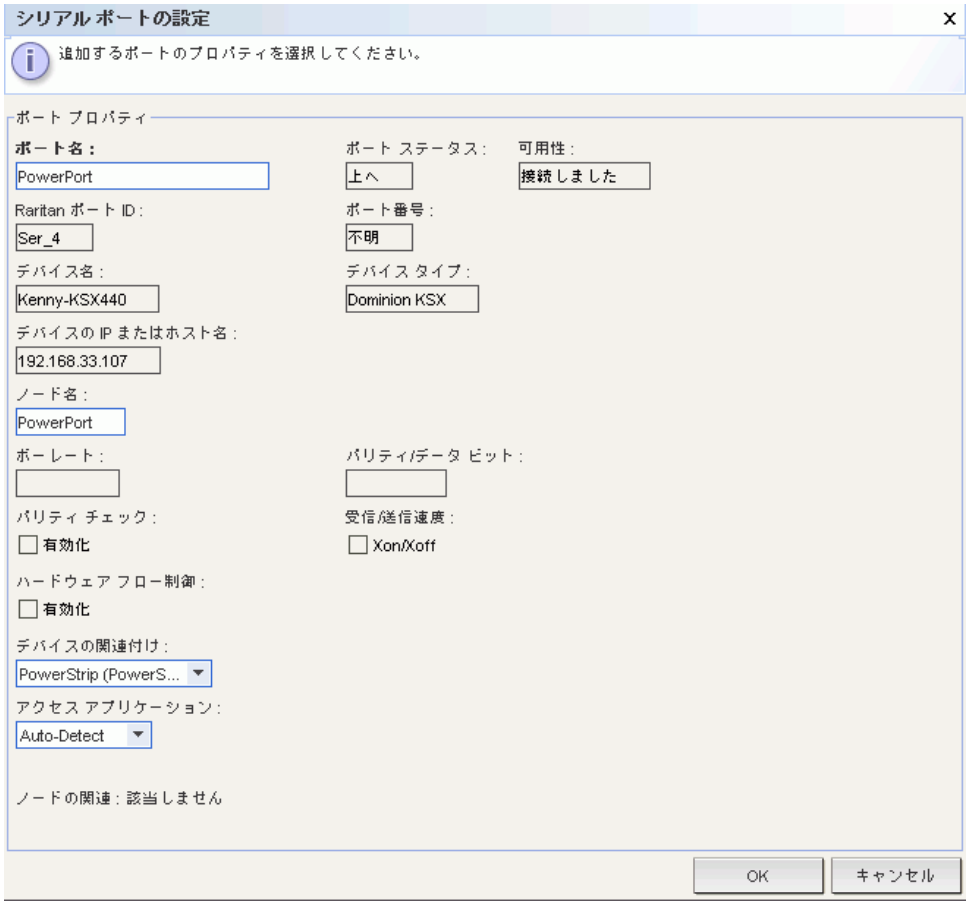


*図 37 シリアル ポートの設定画面*

4. [**ポート名**] フィールドにポート名を入力します。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。
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**] フィールドにノード名を入力します。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 で自動的に選択する場合は、[**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

1. [**デバイス**] タブをクリックし、デバイス ツリーから KVM デバイスを選択します。
2. [**デバイス**] メニューの [**ポート マネージャ**] をクリックし、さらに [**ポートの設定**] をクリックします。[**ポートの設定**] 画面が表示されます。

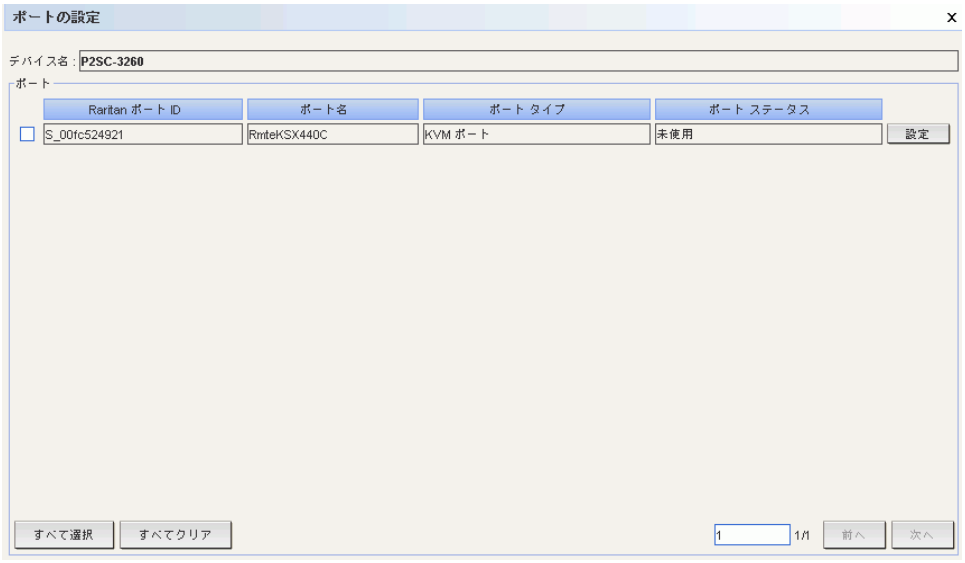


*図 38 ポートの設定画面*

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。[**KVM ポートの設定**] 画面が表示されます。

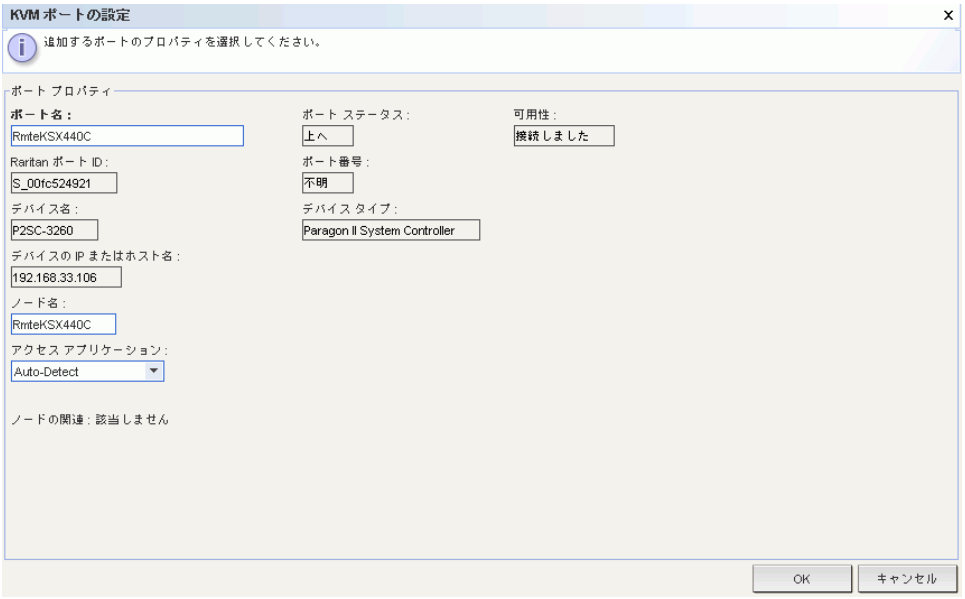


*図 39 KVM ポートの設定画面*

4. [**ポート名**] フィールドにポート名を入力します。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。

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**] フィールドにノード名を入力します。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 で自動的に選択する場合は、[**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。

## ポートの編集

ポートを編集することで、既存の設定済みポートに関連付けられた名前またはアクセス アプリケーションを変更できます。

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**] 画面が表示されます。

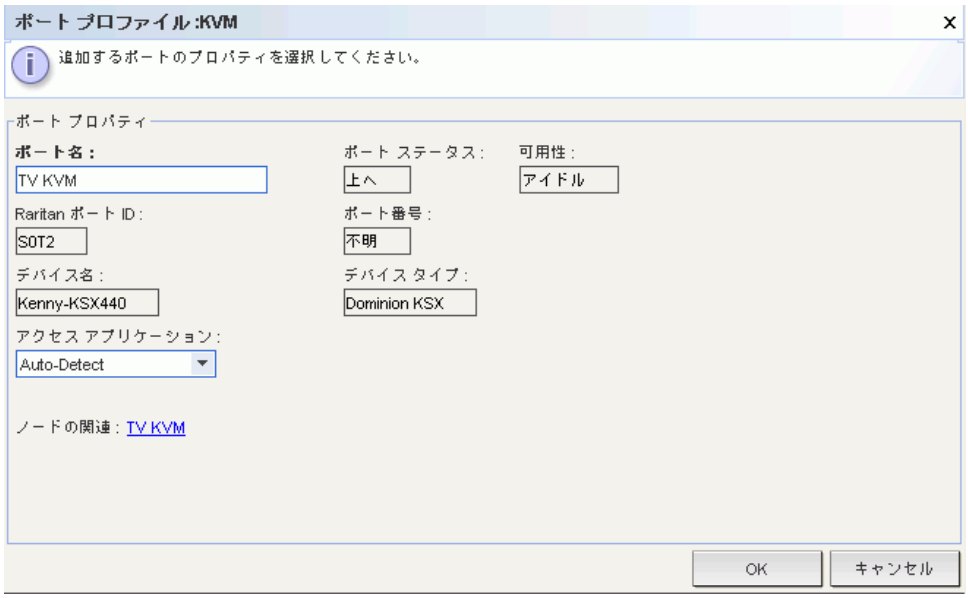


*図 40 ポート プロファイル*

2. 必要に応じて、[**ポート名**] フィールドに、ポートの新しい名前を入力します。
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 で自動的に選択する場合は、[**自動検出**] を選択します。
4. [**OK**] をクリックして、設定済みポートの変更を保存します。

## 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。

**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。**

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**] メニューの [**ポート マネージャ**] をクリックし、さらに [**ポートの削除**] をクリックします。[**ポートの削除**] 画面が表示されます。

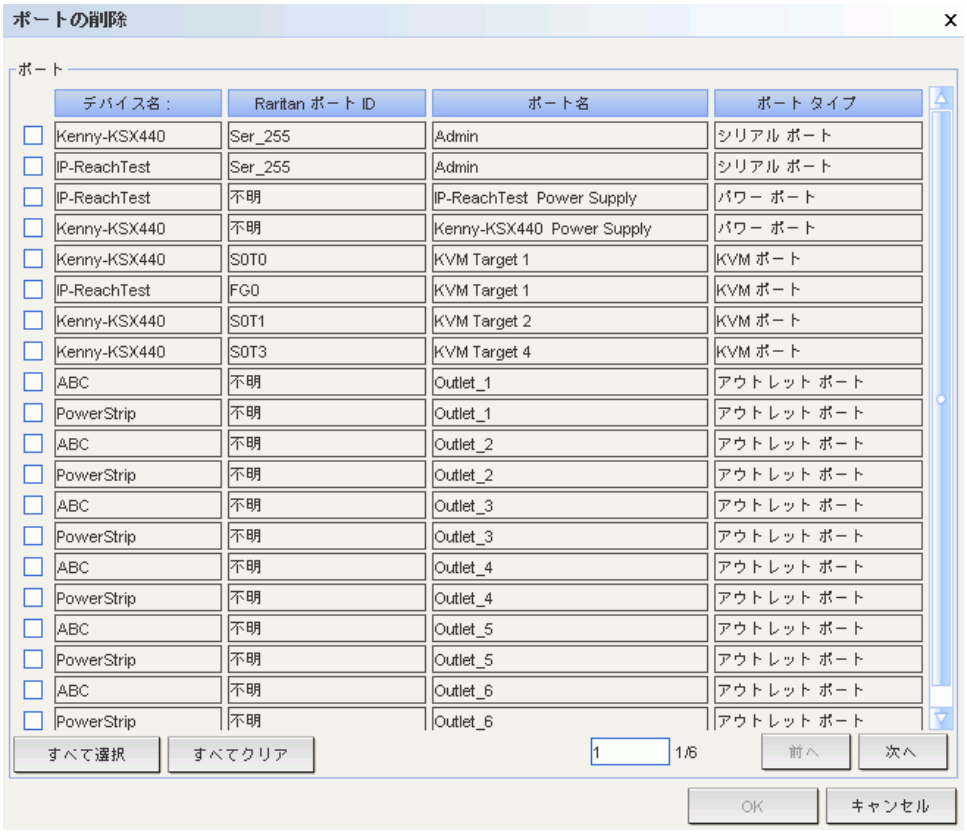


*図 41 ポートの削除画面*

デバイスから削除するポートのチェックボックスをオンにします。

3. [**OK**] をクリックして、選択したポートを削除します。「**ポートが正常に削除されました**」というメッセージが表示され、ユーザが削除されたことを確認します。

# デバイス管理

デバイスが CC-SG に追加されたら、ポートの設定以外の一部の管理機能を実行できるようになります。

## デバイスのカテゴリおよびエレメントのための一括コピー

一括コピー コマンドを使用すると、割り当てられたカテゴリとエレメントを 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カテゴリとエレメントのみです。

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**] メニューの [**デバイス マネージャ**] をクリックし、さらに [**一括コピー**] をクリックします。[**一括コピー**] 画面が表示されます。
3. [**すべてのデバイス**] 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カテゴリとエレメントをコピーするデバイス (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. [**選択されたデバイス**] リストのデバイスを削除するには、デバイスを選択してから [<] をクリックします。
6. [**OK**] をクリックして一括コピーします。[**キャンセル**] をクリックすると、コピーせずに終了します。「**デバイスが正常にコピーされました**」というメッセージが表示され、カテゴリとエレメントがコピーされたことを確認します。

## デバイスのアップグレード

[デバイスのアップグレード] により、新しいバージョンのデバイス ファームウェアがダウンロードされます。

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**] メニューの [**デバイス マネージャ**] をクリックし、さらに [**デバイスのアップグレード**]をクリックします。[**デバイスのアップグレード**] 画面が表示されます。

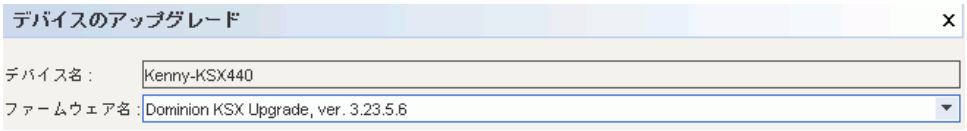


*図 42 デバイスのアップグレード画面*

3. [**ファームウェア名**] ドロップダウン矢印をクリックし、リストから該当するファームウェアを選択します。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、警告メッセージが表示され、このまま続行するかどうかをたずねます。カテゴリおよびエレメントを作成する方法の詳細は、「第 2 章 : CC-SG へのアクセス」を参照してください。[はい] をクリックして、デバイスをアップグレードします。
5. [**再起動**] 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。
6. 「**デバイスが正常にアップグレードされました**」というメッセージが表示され、デバイスがアップグレードされたことを確認します。

## 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。

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**] メニューで、[**デバイス マネージャ**]、[**設定**]、[**バックアップ**] の順にクリックします。[**デバイス設定のバックアップ**] 画面が表示されます。

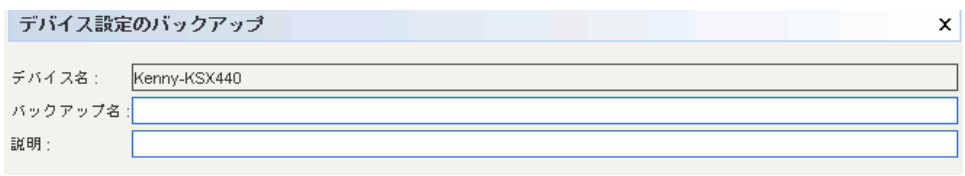


*図 43 デバイス設定のバックアップ画面*

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. オプションとして、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。
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。「**デバイス設定が正常にバックアップされました**」というメッセージが表示され、デバイス設定がバックアップされたことを確認します。

## デバイス設定の復元

前にバックアップしておいたデバイス設定をデバイスに復元できます。

1. [**デバイス**] タブをクリックし、バックアップ設定に復元するデバイスを選択します。
2. [**デバイス**] メニューの [**デバイス マネージャ**]、[**設定**] をクリックし、さらに [**復元**] をクリックします。[**デバイス設定の復元**] 画面が表示されます。

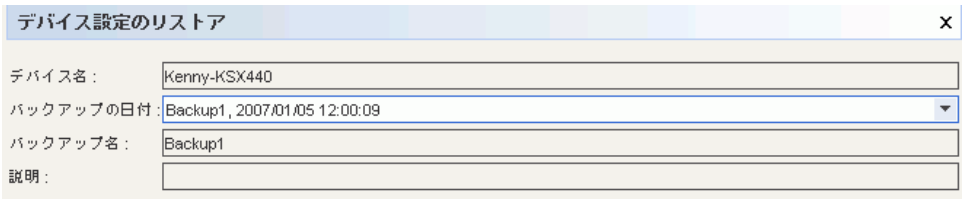


*図 44 デバイス設定の復元画面*

3. [**バックアップの日付**] ドロップダウン矢印をクリックし、リストからデバイス バックアップの最終作成日を選択します。バックアップの名前および説明が対応するフィールドに設定されます。
4. [**OK**] をクリックしてバックアップを復元します。
5. [**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。「**デバイス設定が正常に復元されました**」というメッセージが表示され、ユーザとシステムのすべての設定データが復元されたことを確認します。

## デバイス設定のコピー

このコマンドを実行すると、1 つのデバイスから別のデバイスに設定をコピーできます。

***注 :*** *設定は、ポート数が同じ Dominion SX ユニット間でのみコピーできます。*

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**] メニューの [**デバイス マネージャ**]、[**設定**] をクリックし、さらに [**設定のコピー**] をクリックします。[**デバイス設定のコピー**] 画面が表示されます。
3. このデバイスで [**デバイスのバックアップ**] オプションを使用している場合は、代わりにバックアップした設定をコピーすることもできます。その場合は、[**保存した設定から**] を選択し、さらに保存した保存ドロップダウン メニューからバックアップした設定を選択します。
4. [**使用できるデバイス**] 列にある、設定をコピーしたいデバイスをハイライトして、右矢印をクリックし、[**設定のコピー先**] に移動します。左矢印は、選択したデバイスを [**設定のコピー先**] 列の外に移動します。
5. [**OK**] をクリックして設定を [**設定のコピー先**] 列のデバイスにコピーします。
6. [**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。「**デバイス設定が正常にコピーされました**」というメッセージが表示され、デバイス設定がコピーされたことを確認します。

## 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。

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**] メニューの [**デバイス マネージャ**] をクリックし、さらに [**デバイスの再起動**] をクリックします。[**デバイスの再起動**] 画面が表示されます。

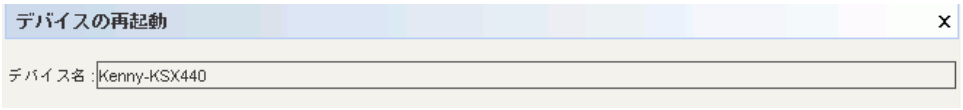


*図 45 デバイスの再起動画面*

3. [**OK**] をクリックして、デバイスを再起動します。「**デバイスが正常に再起動されました**」というメッセージが表示され、デバイスが再起動されたことを確認します。

## 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。

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**] メニューの [**デバイス マネージャ**] をクリックし、さらに [**デバイスの Ping**] をクリックします。[**デバイスの Ping**] 画面に ping の結果が表示されます。

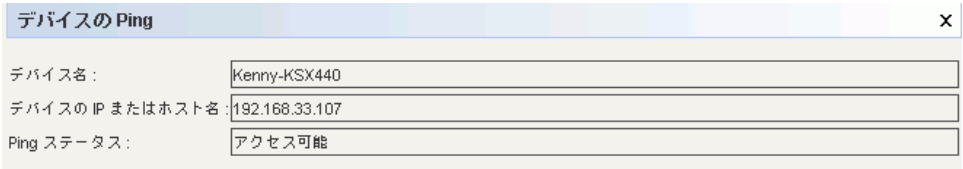


*図 46 デバイスの ping 画面*

## 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。

1. [**デバイス**] タブをクリックし、CC-SG 管理を一時停止するデバイスを選択します。
2. [**デバイス**] メニューの [**デバイス マネージャ**] をクリックし、さらに [**管理の一時停止**] をクリックします。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。

## 再開の管理

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。

1. [**デバイス**] タブをクリックし、デバイス ツリーから停止されたデバイスを選択します。
2. [**デバイス**] メニューの [**デバイス マネージャ**] をクリックし、さらに [**管理の再開**] をクリックします。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。

## デバイス パワー マネージャ

デバイス パワー マネージャでは、サージ プロテクタ デバイスのすべての電源出力に加えて、サージ プロテクタ デバイスのステータス (電圧、電流、温度を含みます) を表示できます。デバイス パワー マネージャでは、個別にノードの電源のオンとオフを切り替えるのではなく、サージ プロテクタ中心のアウトレット表示が提供されます。

デバイス パワー マネージャを使用する前に、サージ プロテクタから 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。サージ プロテクタ 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、サージ プロテクタの管理機能を提供する Dominion SX シリアル ポートまたは Dominion KSX 専用パワー ポートに関連付けられます。

デバイス ツリーで、サージ プロテクタ デバイスを選択します。

1. [デバイス] メニューの [デバイス パワー マネージャ] をクリックします。[デバイス パワー マネージャ] 画面が表示されます。
2. [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。
3. 各コンセントの [オン] と [オフ] のラジオ ボタンをクリックすると、コンセントの電源をオンまたはオフにできます。
4. [電源の再投入] をクリックしてコンセントに接続されたデバイスを再起動します。
5. [閉じる] をクリックして [デバイス パワー マネージャ] 画面を閉じます。

## 管理の起動

[**管理の起動**] コマンドが使用可能である場合、選択したデバイスの管理インタフェースにこのコマンドでアクセスできます。

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] メニューの [デバイス マネージャ] をクリックし、さらに [管理の起動] をクリックします。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。

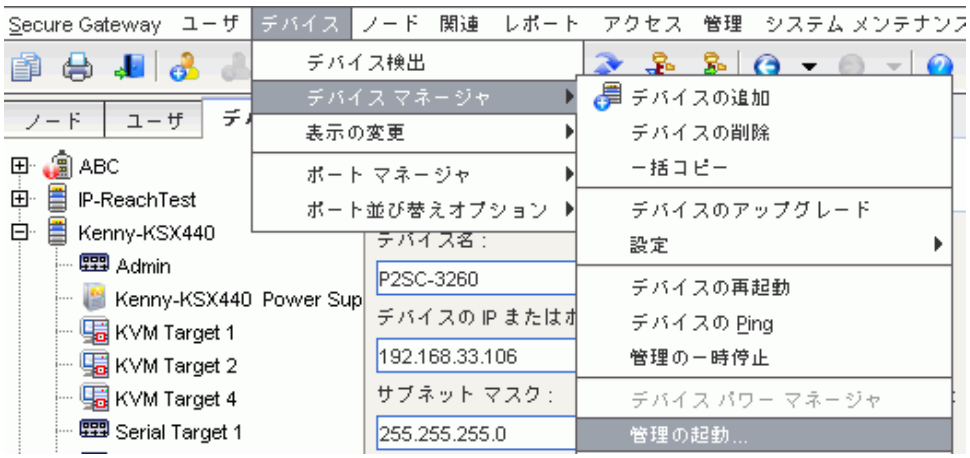


*図 47 KX デバイスの管理の起動*

## 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。

1. [**デバイス**] タブをクリックし、トポロジーを表示するデバイスを選択します。
2. [**デバイス**] メニューの [**デバイス マネージャ**] をクリックし、さらに [**トポロジー表示**] をクリックします。選択したデバイスの [**トポロジー表示**] が表示されます。

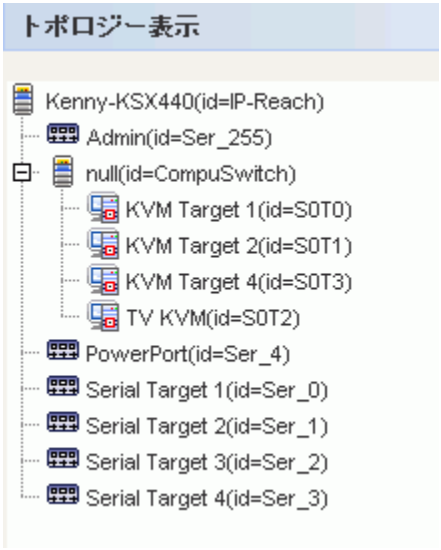


*図 48 トポロジー表示画面*

3. デバイス ツリーでの移動と同じ要領でトポロジー表示での移動を行います。+ 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。
4. [**閉じる**] をクリックして [**トポロジ表示**] 画面を閉じます。

***注：** トポロジー表示を閉じるまで、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トポロジー表示が表示されます。*

## ユーザの切断

管理者はデバイスを使用する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。

***注 :*** *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。*

1. [**デバイス**] タブをクリックし、1 人以上のユーザの接続を切断するデバイスを選択します。
2. [**デバイス**] メニューで [**デバイス マネージャ**]、[**ユーザの切断**] の順にクリックします。[**ユーザの切断**] 画面が表示されます。

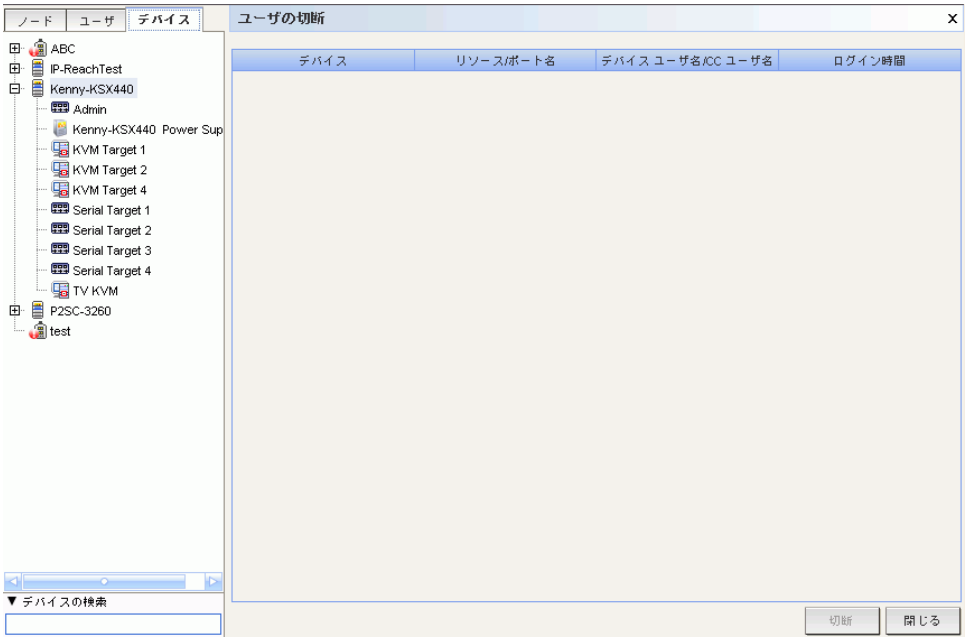


*図 49 ユーザの切断*

3. **ユーザの切断**テーブルで、セッションの接続を切断す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。

***注 :*** *Dominion SX デバイスの場合のみ、直接デバイスにログオ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。*

# デバイスの表示

CC-SG では、[**デバイス**] タブでデバイスを表示するためのさまざまなオプションが用意されています。

## ツリー表示

[**ツリー表示**] を選択すると、デフォルト表示で、グループ化されたデバイス ツリー形式によりデバイスが表示されます。また、[**ツリー表示**] を選択することにより、**カスタム表示**から標準表示に戻ることができます。詳細については、この章の後で説明する「カスタム表示」を参照してください

1. [**デバイス**] メニューの [**表示の変更**] をクリックし、さらに [**ツリー表示**] をクリックします。デバイス ツリーの通常の [**ツリー表示**] が表示されます。

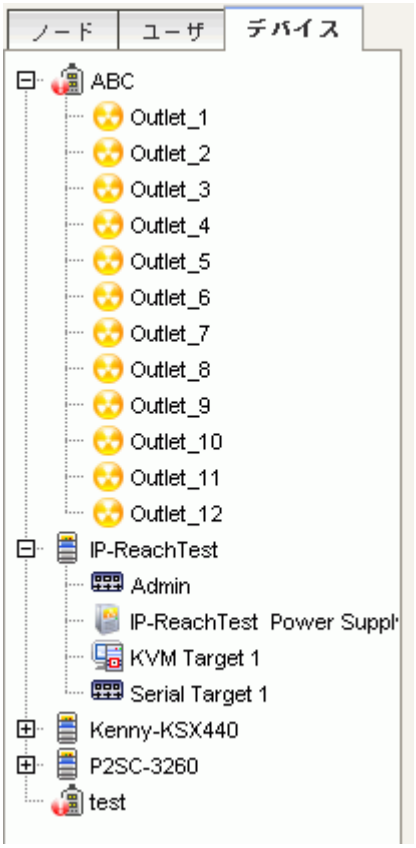


*図 50 デバイス ツリーの通常表示画面*

設定済みポートは親デバイスの下に分類されています。ポートの表示方法を変更するには、[**デバイス**] メニューをクリックし、[**ポート並び替えオプション**] をクリックします。名前のアルファベット順または可用性ステータスを基準にしてデバイス内のポートを整列するには、[**ポート名でソート**] または [**ポート ステータスでソート**] を選択します。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。

## カスタム表示

デバイス ツリーは、特定の形式で表示されるようにデバイスを体系化することでカスタマイズできます。デバイスを区別しやすいように、国ごと、タイム ゾーンごと、あるいは他の任意のオプションごとにデバイスを表示することができます。CC-SG へのカテゴリの追加に関する詳細については、「**第 4 章 : 関連の作成**」を参照してください。

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**] をクリックし、さらに [**カスタム表示の作成**] をクリックします。[**カスタム表示**] 画面が表示されます。

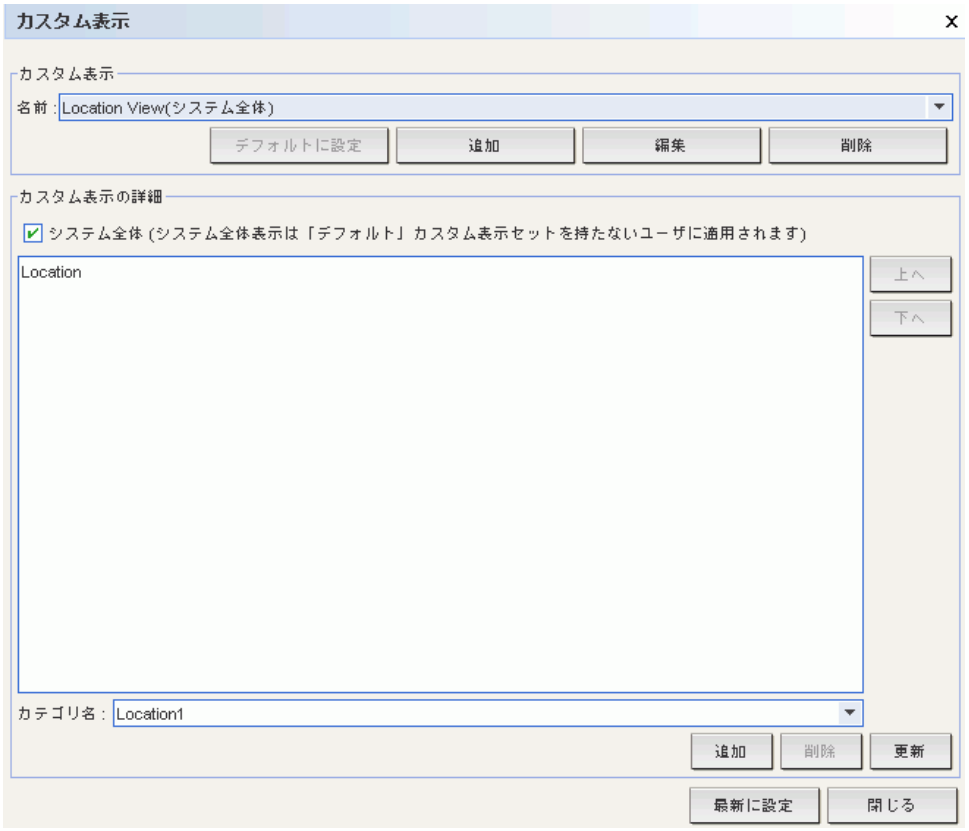


*図 51 カスタム表示画面*

3. 表示をカスタマイズするには、[**名前**] ドロップダウン矢印をクリックし、データベースに保存されているカスタム表示を選択します。[**カスタム表示の詳細**] フィールドに、表示カテゴリの詳細が表示されます。
4. [**最新に設定**] をクリックすると、選択したカスタム表示が反映されます。
5. CC-SG へのログイン時に、選択したカスタムの表示を表示する場合は、[**デフォルトに設定**] をクリックします。
6. 独自のデフォルト カスタム表示を使用していないすべてのユーザに対して、これをデフォルトの表示にするには、[**システム全体**] をオンにします。

### カスタム表示の選択

現在のデバイス ツリー表示を設定済みのカスタム表示にすばやく切り替えるには、次の手順に従います。

1. [**デバイス**] タブをクリックします。
2. [**デバイス**] メニューで、[**表示の変更**] をクリックし、[**カスタム表示の作成**] の下に表示されたカスタム表示名を選択します。デバイス ツリーが選択したカスタム表示に切り替わります。

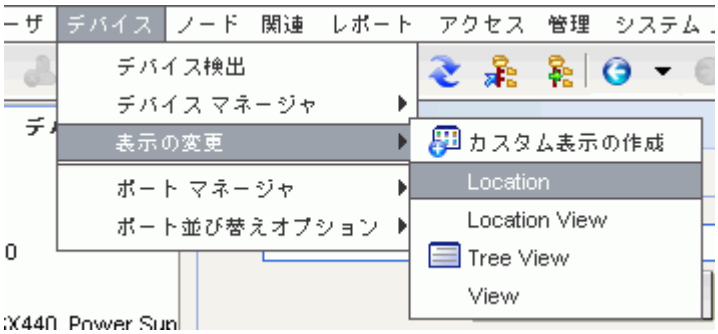


*図 52 カスタム表示の選択*

### カスタム表示の追加

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**] をクリックし、さらに [**カスタム表示の作成**] をクリックします。[**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入力して [**OK**] をクリックします。[**名前**] フィールドに新しい表示名が表示されます。
5. [**カスタム表示の詳細**] パネルで、パネル下部のドロップダウン矢印をクリックします。このリストには、カスタム表示のフィルタに使用できるカテゴリが表示されます。ドロップダウン リストから詳細を選択して [**追加**] をクリックすると、この詳細が [**カスタム表示の詳細**] パネルに追加されます。詳細を必要なだけ選択します。
6. [**カスタム表示の詳細**] パネルに表示される詳細の順序を変更するには、詳細を選択し、[**上へ**] ボタンと [**下へ**] ボタンを使用して詳細がデバイスをソートする順に並ぶようにします。リストから詳細を削除するには、[**カスタム ユーザの詳細**] パネルで詳細を選択して [**削除**] ボタンをクリックします。
7. [**更新**] をクリックしてカスタム表示を更新します。「**カスタム表示が正常に更新されました**」というメッセージが表示され、カスタム表示が更新されたことを確認します。
8. [**最新に設定**] をクリックすると、選択したカスタム表示が反映されます。

### カスタム表示の編集

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**] をクリックし、さらに [**カスタム表示**] をクリックします。[**カスタム表示**] 画面が表示されます。
3. [**カスタム表示**] パネルの [**名前**] ドロップダウン矢印をクリックし、編集するカスタム表示を選択します。[**編集**] をクリックします。[**カスタム表示の編集**] ウィンドウが表示されます。
4. 新しいカスタム表示名を入力し、[**OK**] をクリックして確認します。[**キャンセル**] をクリックすると、何もせずにウィンドウを閉じます。
5. [**カスタム表示の詳細**] パネルで、パネル下部のドロップダウン矢印をクリックします。このリストには、カスタム表示のフィルタに使用できるカテゴリが表示されます。ドロップダウン リストから詳細を選択して [**追加**] をクリックすると、この詳細が [**カスタム表示の詳細**] パネルに追加されます。詳細を必要なだけ選択します。

6. [**カスタム表示の詳細**] パネルに表示される詳細の順序を変更するには、詳細を選択し、[**上へ**] ボタンと [**下へ**] ボタンを使用して詳細がデバイスをソートする順に並ぶようにします。リストから詳細を削除するには、[**カスタム ユーザの詳細**] パネルで詳細を選択して [**削除**] ボタンをクリックします。
7. [**更新**] をクリックしてカスタム表示を更新します。「**カスタム表示が正常に更新されました**」というメッセージが表示され、カスタム表示が更新されたことを確認します。
8. [**最新に設定**] をクリックすると、選択したカスタム表示が反映されます。

**カスタム表示の削除**

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**] をクリックし、さらに [**カスタム表示の作成**] をクリックします。[**カスタム表示**] 画面が表示されます。

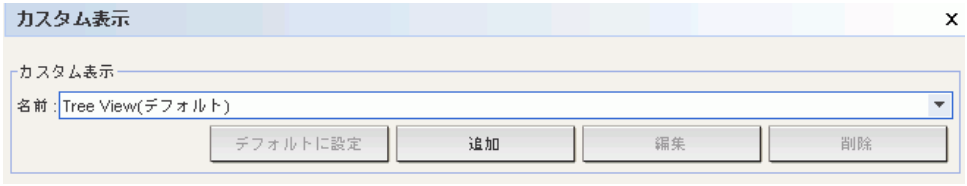


*図 53 カスタム表示画面*

3. [**カスタム表示**] パネルの [**名前**] ドロップダウン矢印をクリックし、削除するカスタム表示を選択します。
4. [**カスタム表示**] パネルの [**削除**] ボタンをクリックします。[**カスタム表示の削除**] ウィンドウが表示されます。
5. [**はい**] をクリックし、カスタム表示を削除します。

# 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 管理の使用の詳細については、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。

Paragon II システム コントローラ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. [**Paragon II システム コントローラ**] を右クリックし、[**管理の起動**] をクリックして、新しいブラウザ ウィンドウで Paragon II システム コントローラ アプリケーションを起動します。これで、PII UMT ユニットを設定できます。

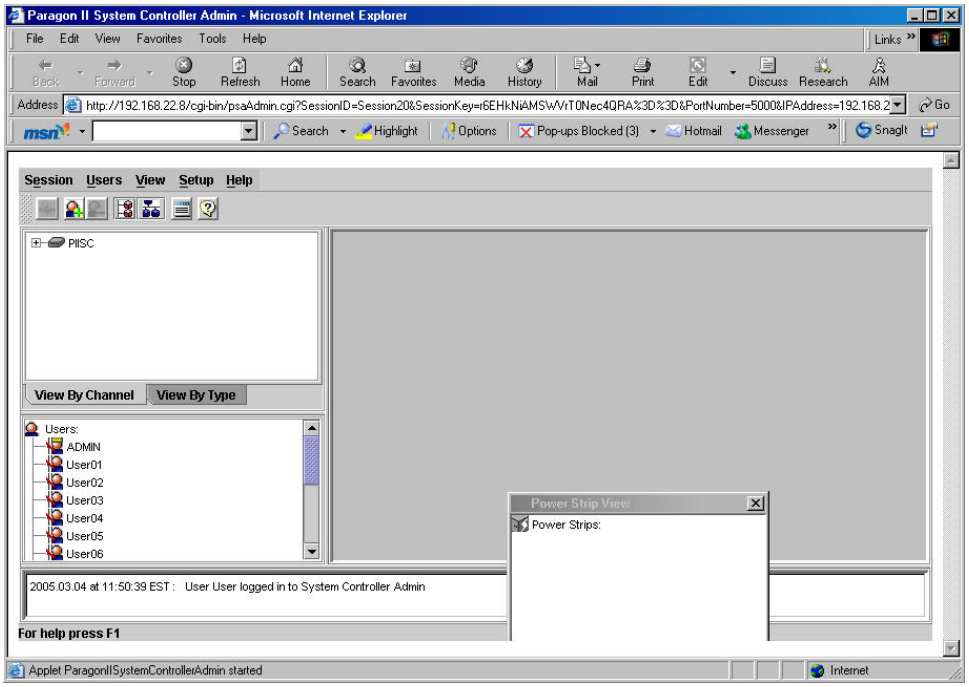


*図 54 Paragon Manager アプリケーション ウィンドウ*

## IP-Reach と UST-IP 管理

Paragon システム構成に接続されている IP-Reach および UST-IP デバイスの管理診断を CC-SG インタフェースから直接実行することもできます。

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. [**Paragon II システム コントローラ**] を右クリックし、[**リモート ユーザ ステーション管理**] をクリックします。リモート ユーザ ステーション管理画面が表示され、接続中のすべての IP-Reach と UST-IP ユニットがリスト表示されます。
3. 作業を行うデバイスの行の [**管理の起動**] ボタンをクリックして、Raritan リモート コンソールをアクティブ化し、新しいウィンドウで青色のデバイス設定画面を起動します。

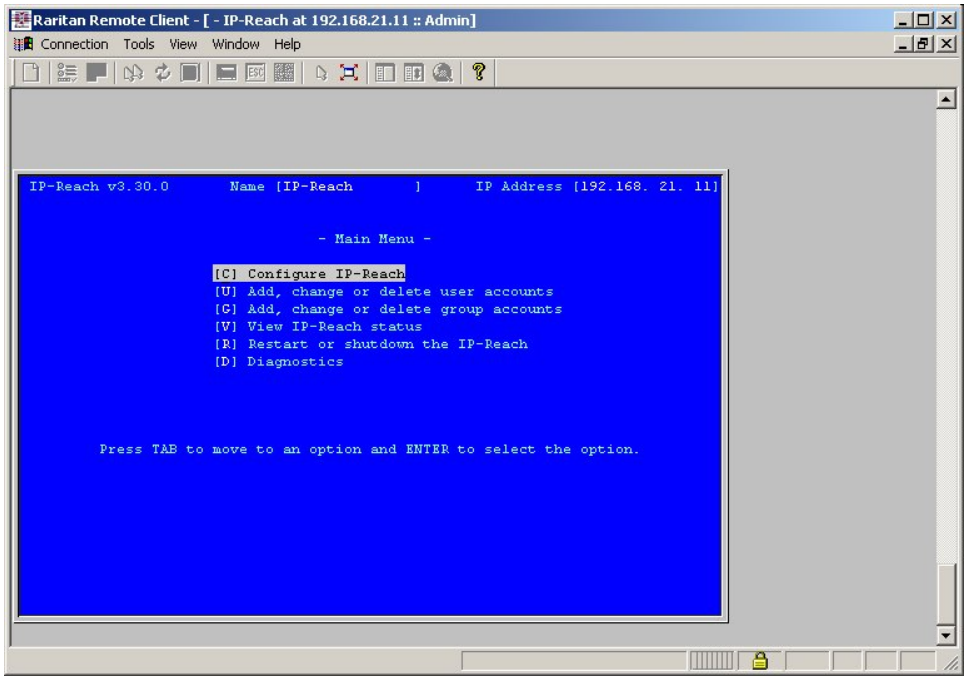


*図 55 IP-Reach 管理画面*

# 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**] 画面を使用して、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。詳細については、「**第 8 章 : ポリシー**」を参照してください。

## デバイス グループの追加

1. [関連] メニューの [デバイス グループ] をクリックします。[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。

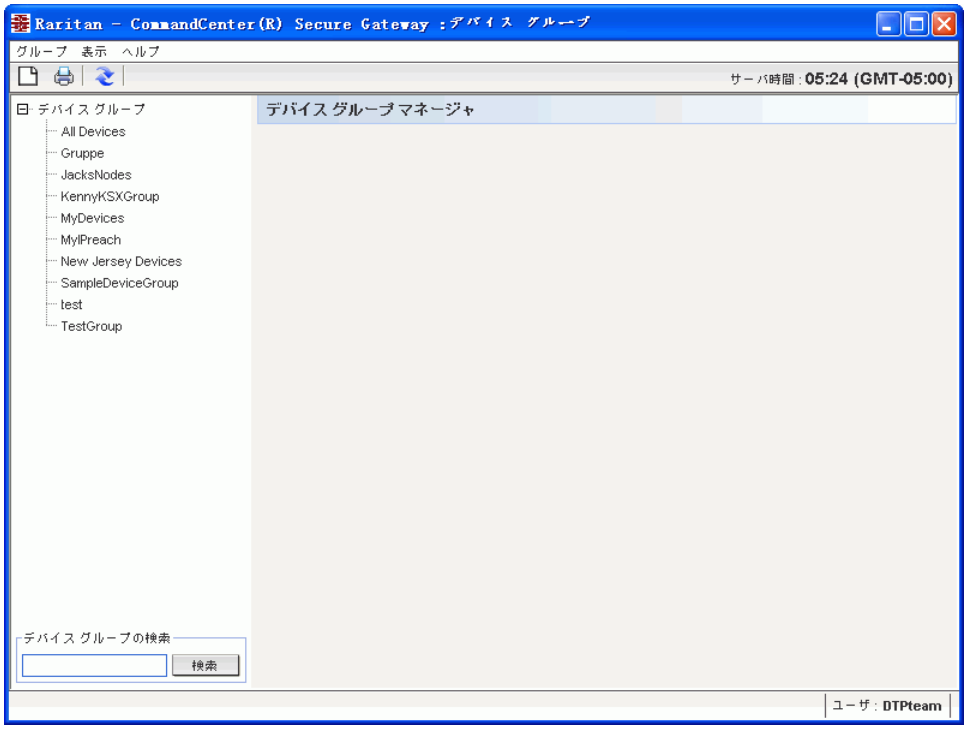


*図 56 デバイス グループ マネージャ*

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。


*図 57 デバイス グループ : 新規パネル、デバイスの選択タブ*

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。
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、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。
   - グループからデバイスを削除する場合は、**[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]** リストのいずれかで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 [**デバイスの選択**] 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。

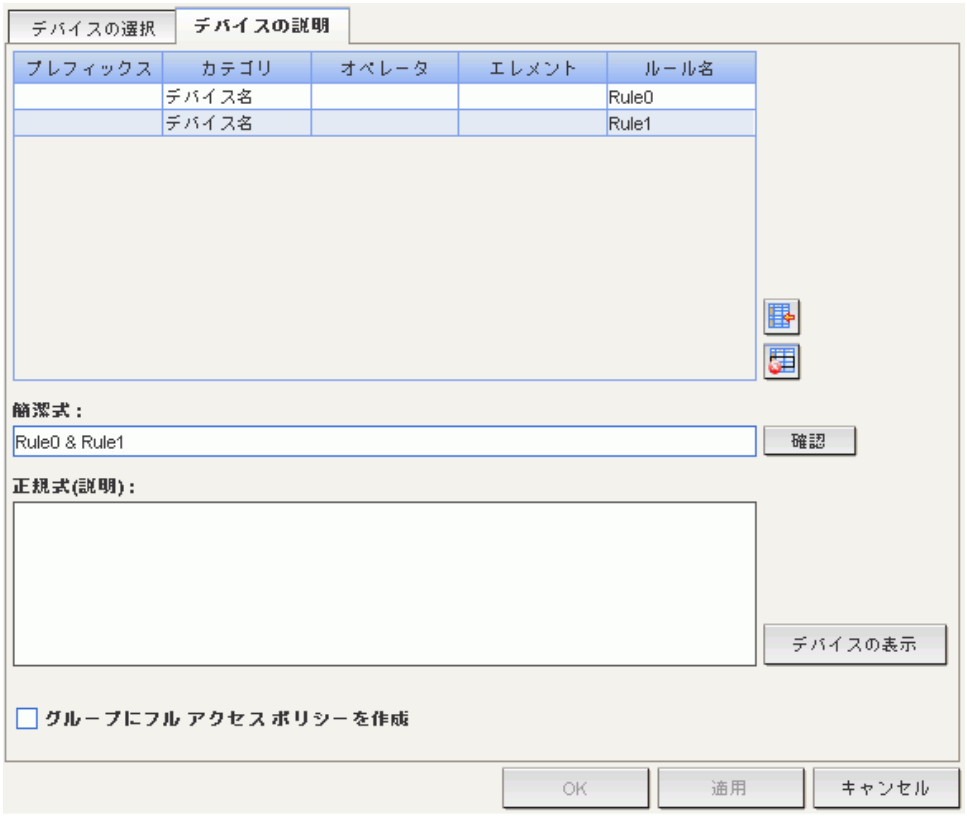


*図 58 デバイスの説明タブ*

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。

- **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。
- **オペレータ** - カテゴリとエレメント アイテム間で実行される比較演算子を選択します。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。[**簡潔式**] フィールドの記述で使用されます。

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デバイスを表します。これは、デバイス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。

d. 別のルールを追加するには、[**新しい行をテーブルに追加**] 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。

e. 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**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するだけです。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両辺またはいずれかのルールを満たす必要があります。
- ( および ) - 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。

たとえば、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。次に、[簡潔式] フィールドに「Rule0」と入力します。

さらに、たとえば、エンジニアリング部門に属するノードのグループ、またはフィラデルフィアにあるノードグループ、さらにすべてのマシンが 1 GB のメモリを持つノード グループを説明するには、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)。そして、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ノードとなるので、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。

- テーブルから行を削除する場合は、その行を選択し、[**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。
- 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場合は、[**デバイスの表示**] をクリックします。

f. [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 (説明)] フィールドに正規化された式が表示されます。

g. [**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に、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、ルール表または [簡潔式] フィールドに戻って、式を調整します。

h. 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オンにします。

i. 別のデバイス グループを追加する場合は、[**適用**] をクリックしてこのグループを保存した後、このセクションの手順を繰り返してデバイス グループを追加します。デバイス グループの追加が終わったら、[**OK**] をクリックしてこのグループを保存し、[**デバイス グループ** : **新規**] パネルを閉じます。

## デバイス グループの編集

1. [**関連**] メニューの [**デバイス グループ**] をクリックします。[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。

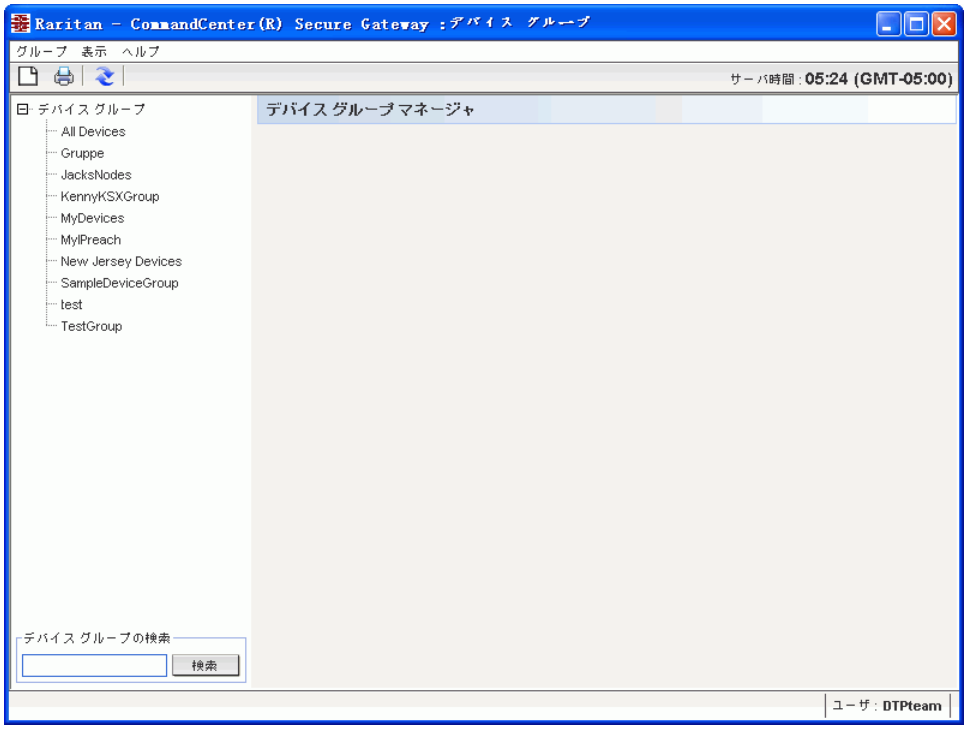


*図 59 デバイス グループ マネージャ画面*

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。

2. デバイス グループ名を編集する場合は、[**グループ名**] フィールドにデバイス グループの新しい名前を入力します。
3. [**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。詳細については、前セクションの「**デバイス グループの追加**」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。

## デバイス グループの削除

1. [**関連**] メニューの [**デバイス グループ**] をクリックします。[**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。

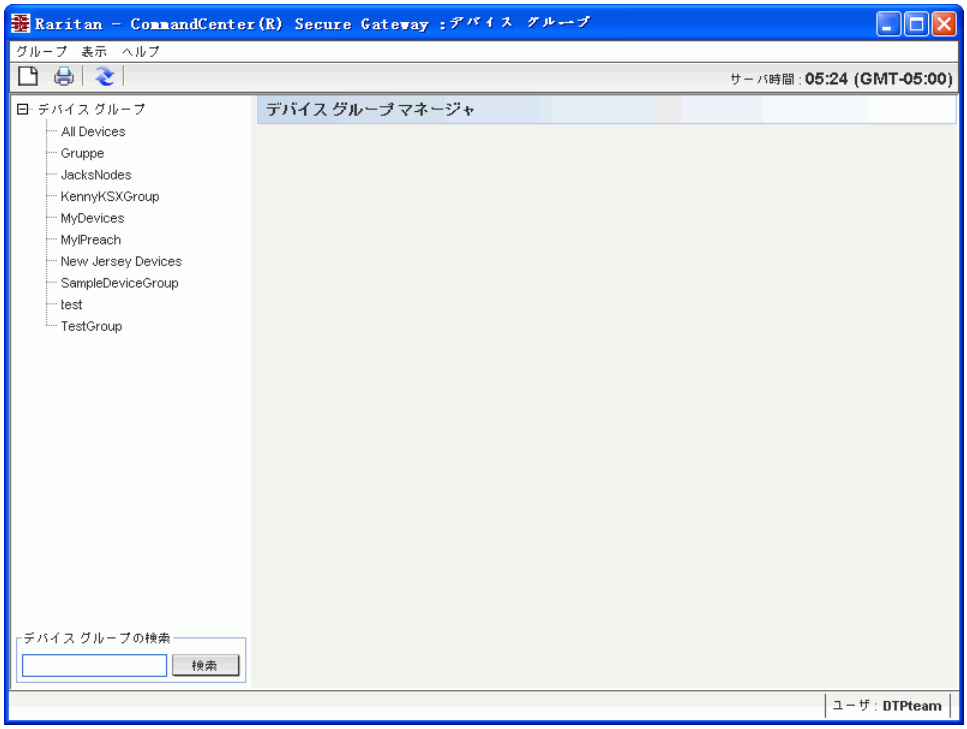


*図 60 デバイス グループ マネージャ画面*

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**] メニューで [**削除**] をクリックします。


*図 61 デバイス グループの削除ウィンドウ*

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。

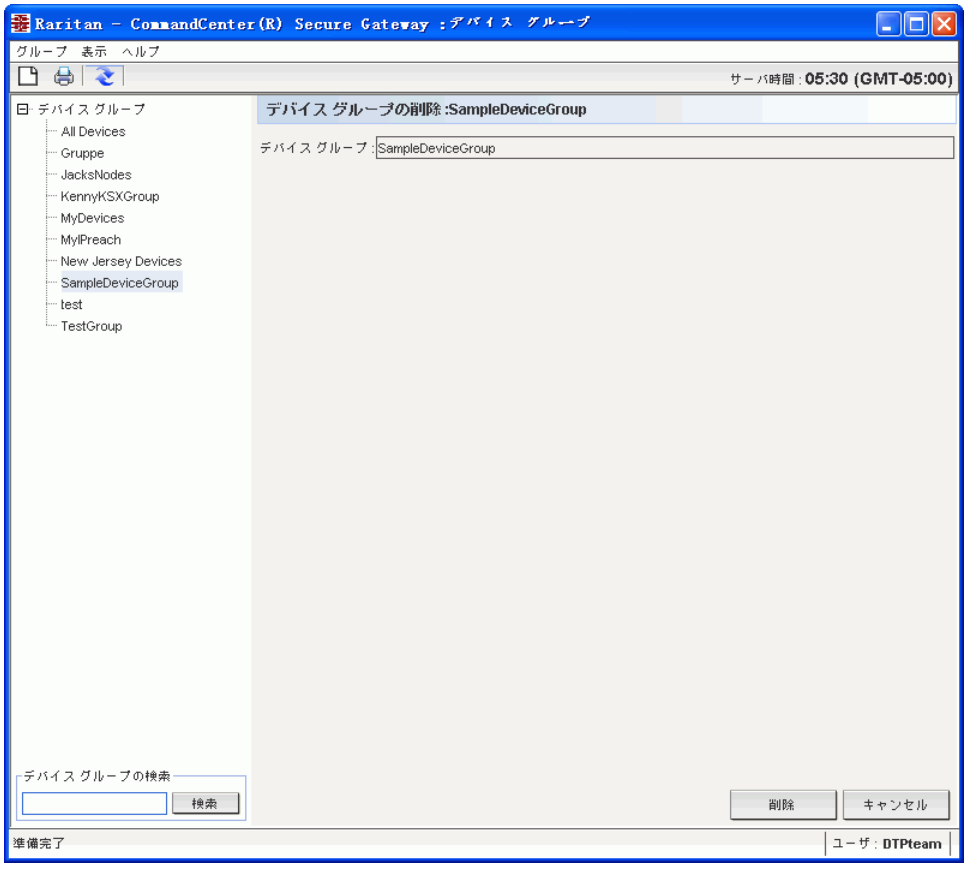


*図 62 デバイス グループの削除パネル*

5. 表示される確認メッセージで [**はい**] をクリックします。

# 第 6 章 : ノードとインタフェースの設定

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、および編集方法について説明します。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。

## ノードの表示

CC-SG では、すべてのノードを [ノード] ツリーで表示できます。ノードを選択して、そのノードのプロファイルを表示します。

### ノード ツリー

[ノード] タブをクリックすると、[ノード] ツリーに利用可能なノードが表示されます。ノードは名前のアルファベット順に配列されるか、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。

### ノード プロファイル

ノード ツリーでノードをクリックして、[**ノード プロファイル**] 画面を開きます。この画面には、ノード、そのインタフェース、デフォルトのインタフェース、カテゴリ、ノードに割り当てられているエレメントに関する情報が表示されます。

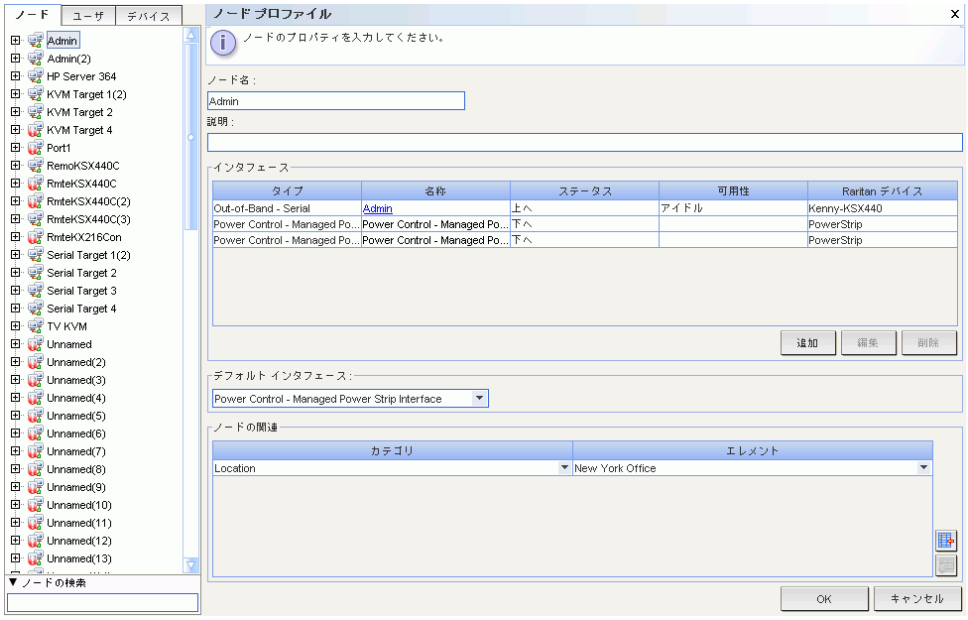


*図 63 ノード タブとノードのプロファイル画面*

### 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。 |

## 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 デバイスへの接続) 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。ただし、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、本章に記載されているように、後でいつでも編集できます。詳細は、「**第 3 章：ガイド付き設定を使用した CC-SG の設定**」または「**第 5 章：デバイスおよびデバイス グループの追加**」を参照してください。

#### 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。

### 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、アウト オブ バンド KVM、シリアル、パワー制御、インバンド SSH/RDP/VNC、DRAC/RSA/ILO など、ノードのタイプによって、異なるタイプのアクセスを提供できます。

1 つのノードに複数のインタフェースを割り当てることはできますが、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 つずつしか割り当てることはできません。たとえば、Windows Server 2003 を実行している PC には、キーボード、マウス、モニタ ポート、パワー インタフェースを通したアウト 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。

**重要：本章に記載されているメニュー バー コマンドの多くは、ノード アイコンを右クリックして表示されるショートカット メニューからも実行できます。**

## ノードの追加

CC-SG に新しい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] メニューで、[**ノードの追加**] をクリックします。[**ノード プロファイル**] 画面が表示されます。

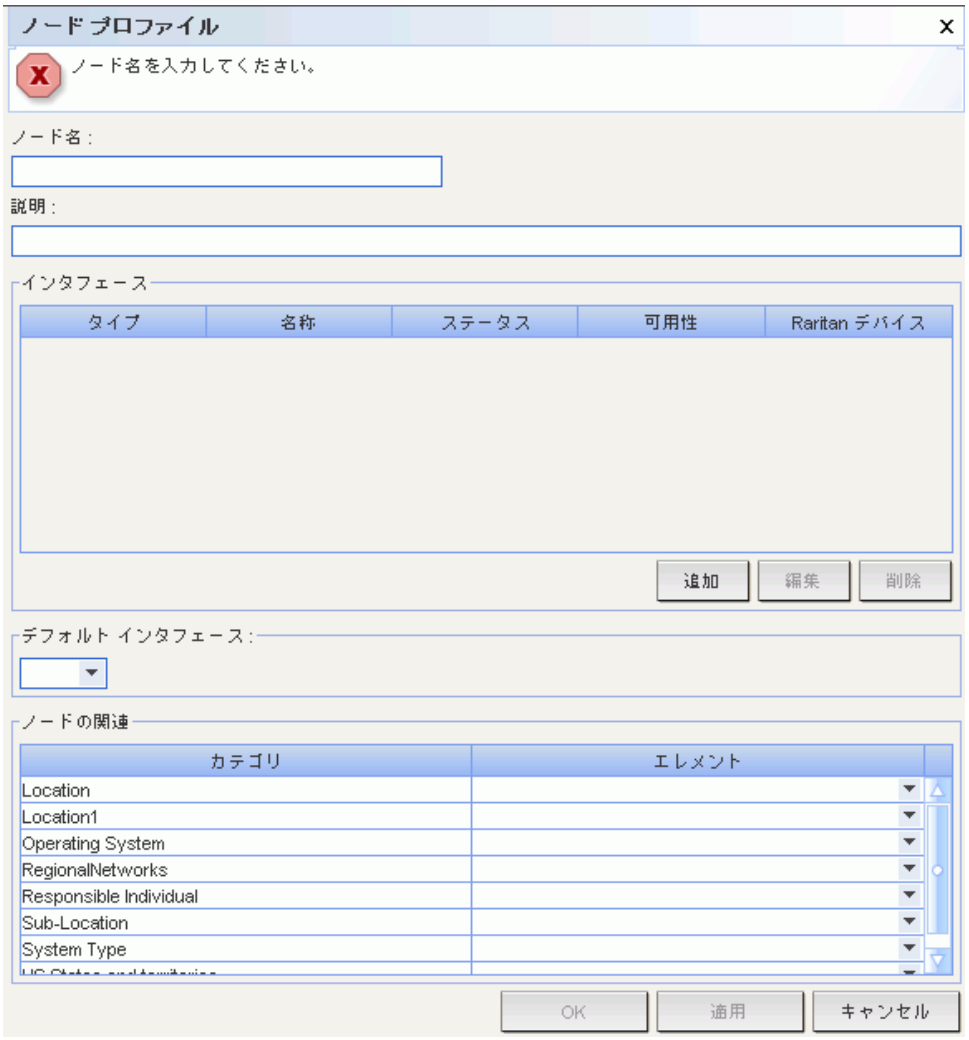


*図 64 ノードの追加画面*

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。
4. オプションとして、[**説明**] フィールドにこのノードの簡単な説明を入力します。
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。この手順についての詳細は、次の「インタフェースの追加」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。詳細は、「第 4 章 : 関連の作成」を参照してください。
   - 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。使用しないカテゴリでは、[**エレメント**] フィールドで空白のアイテムを選択します。
   - 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。カテゴリおよびエレメントを作成する方法の詳細は、「**第 4 章 : 関連の作成**」を参照してください。

7. [**OK**] をクリックしてノードを保存します。ノードがノードのリストに追加されます。

## インタフェースの追加

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] 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**] ウィンドウが表示されます。
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
   - **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。後で、DRAC パワー インタフェースを設定する必要があります。
   - **RDP** : リモート デスクトップ プロトコル (たとえば、Windows サーバのリモート デスクトップ接続) 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。
   - **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。後で、RSA パワー インタフェースを設定する必要があります。
   - **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。
   - **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。
   - **iLO/RILOE 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。

   アウト オブ バンド接続
   - **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。
   - **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。

   パワー制御接続
   - **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。
   - **IPMI** : IPMI 接続を介してノードへのパワー制御接続を作成するには、このアイテムを選択します。
   - **Managed PowerStrip (管理対象サージ プロテクタ)** : Raritan のシリアル管理対象サージ プロテクタを介してノードへのパワー制御接続を作成するには、このアイテムを選択します。
   - **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。
   - **iLO/RILOE** : 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。
3. 選択内容により、[**名称**] フィールドにデフォルト名が表示されます。この名前は、自由に変更できます。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。

**インバンド接続および DRAC、RSA、iLO/RILOE パワー接続 :**

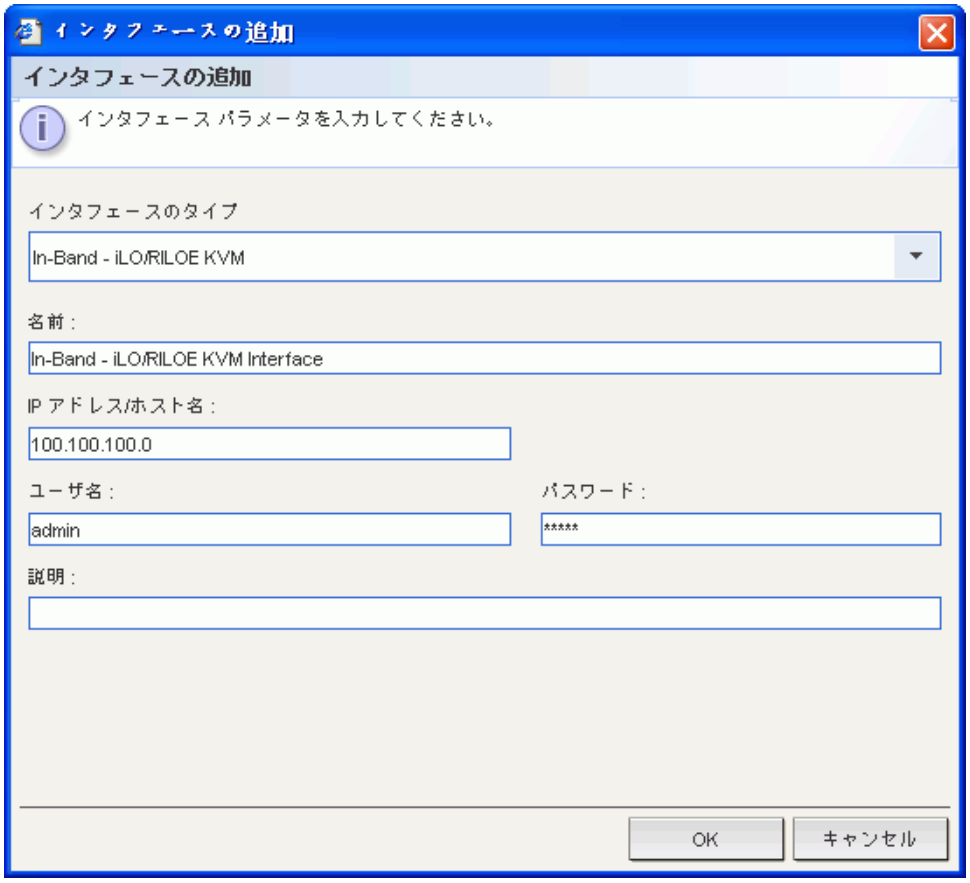


*図 65 インタフェースの追加 - インバンド iLO/RILOE KVM*

a. [**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。
b. 必要に応じて、[**TCP ポート**] フィールドにこの接続の TCP ポートを入力します。
c. [**ユーザ名**] フィールドにこの接続のユーザ名を入力します。
d. 必要に応じて、[**パスワード**] フィールドにこの接続のパスワードを入力します。
e. [**OK**] をクリックしてノードにインタフェースを追加します。[**ノードの追加**] または [**ノード プロファイル**] 画面に戻ります。

**アウト オブ バンド KVM、アウト オブ バンド シリアル接続：**

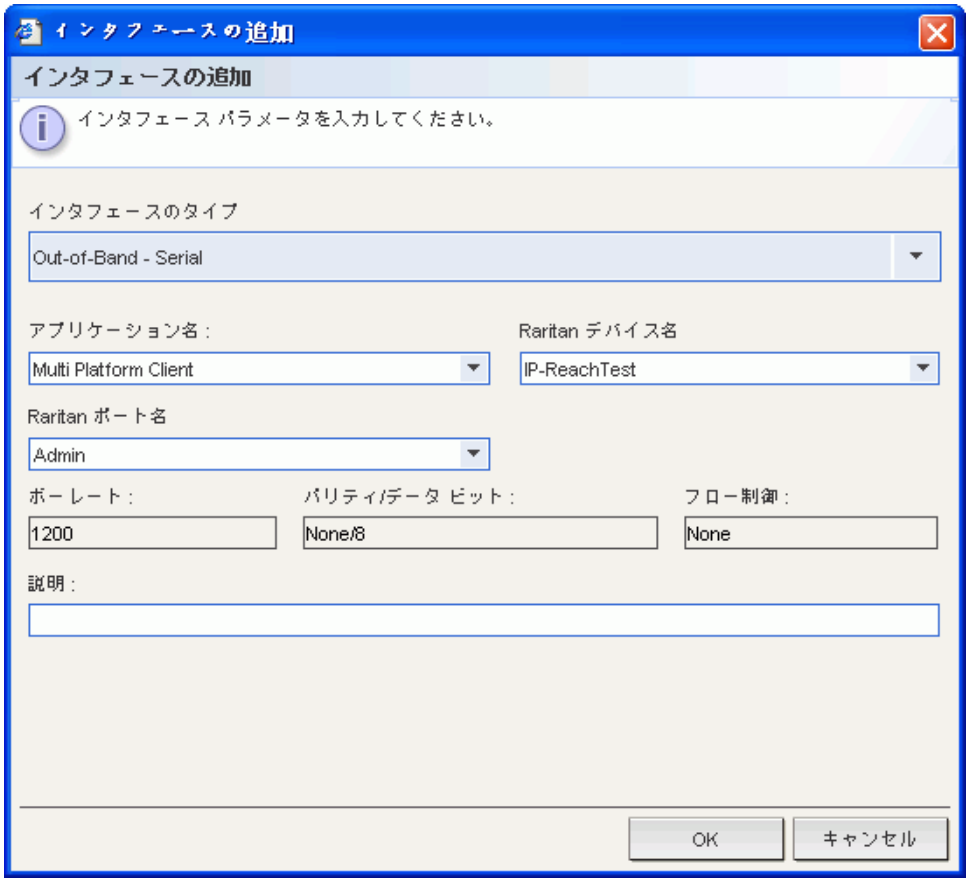


*図 66 アウト オブ バンド KVM 接続の設定*

a. [**アプリケーション名**] ドロップダウン メニューをクリックし、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。
b. [**Raritan デバイス名**] ドロップダウン メニューをクリックし、このノードへの接続を提供する 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、まず CC-SG にデバイスを追加する必要があります。
c. [**Raritan ポート名**] ドロップダウン メニューをクリックし、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。
d. [**OK**] をクリックしてノードにインタフェースを追加します。[**ノードの追加**] または [**ノード プロファイル**] 画面に戻ります。

**管理対象サージ プロテクタ接続 :**

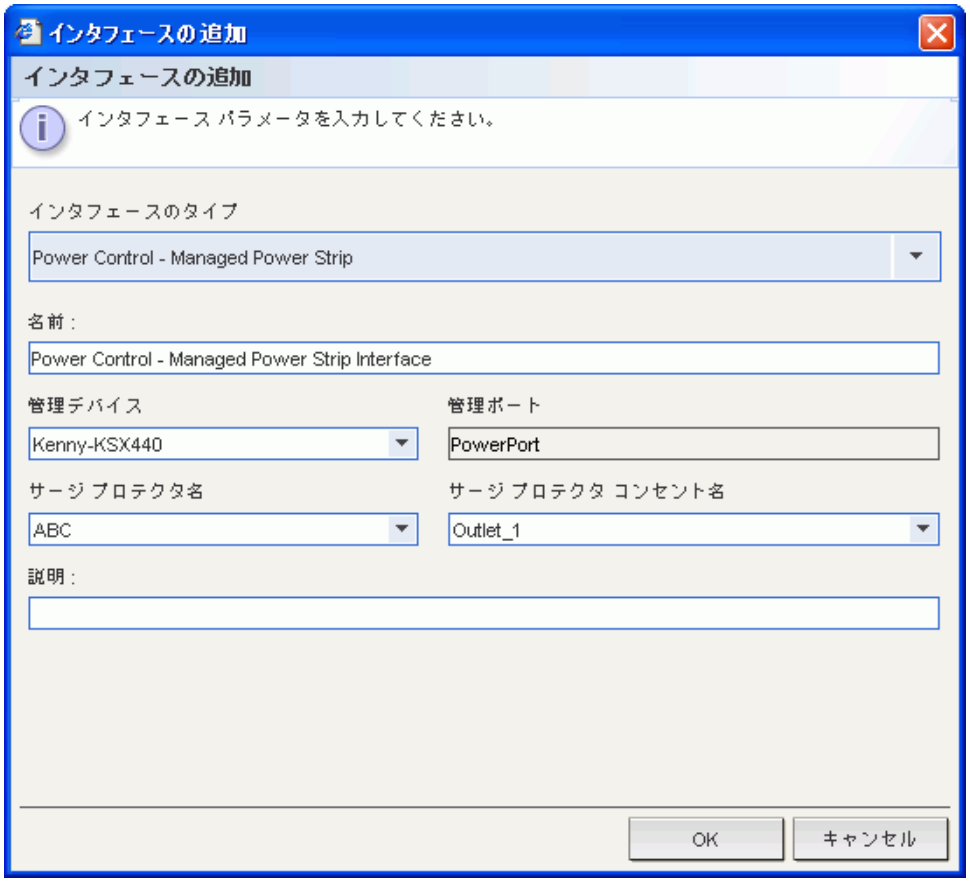


*図 67 管理対象サージ プロテクタ制御インタフェースの設定*

a. [**デバイスの管理**] ドロップダウン メニューをクリックし、ノードへのパワーを提供するサージ プロテクタを管理する Raritan デバイスを選択します。適切なオプションを利用可能にするには、選択するデバイスを、まず CC-SG に追加する必要があります。
b. [**サージ プロテクタ名**] ドロップダウン メニューをクリックし、このノードに電源を提供するサージ プロテクタを選択します。このリストにサージ プロテクタが表示されるようにするには、まず CC-SG にサージ プロテクタを設定する必要があります。
c. [**サージ プロテクタ コンセント名**] をクリックし、ノードを接続しているコンセントの名前を選択します。

オプションとして、[説明] フィールドにこのパワー制御インタフェースの簡単な説明を入力します。

d. [**OK**] をクリックしてノードにインタフェースを追加します。[**ノードの追加**] または [ノード プロファイル] 画面に戻ります。

**IBM パワー制御接続：**

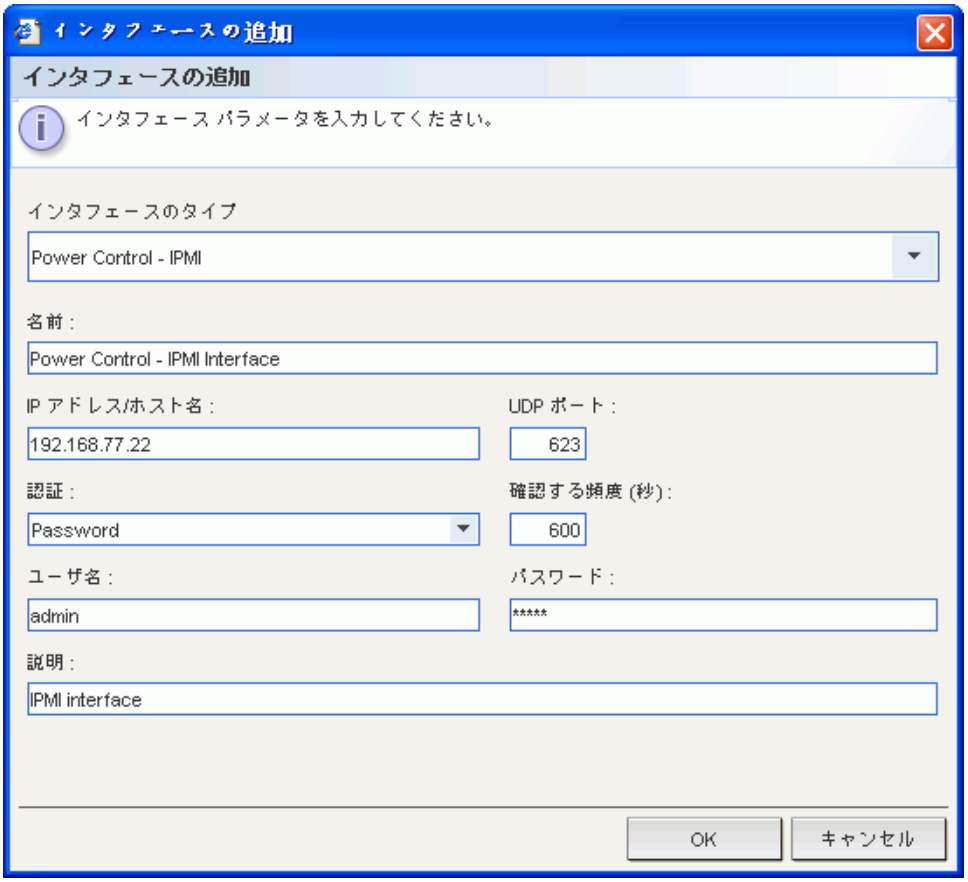


*図 68 IBM パワー制御インタフェースの設定*

a. [**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。
b. [**UDP ポート**] フィールドに、このインタフェースの UDP ポートを入力します。
c. [**認証**] ドロップダウン メニューをクリックし、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。
d. [**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。
e. [**ユーザ名**] フィールドにこのインタフェースのユーザ名を入力します。
f. 必要に応じて、[**パスワード**] フィールドにこのインタフェースのパスワードを入力します。
g. [**OK**] をクリックしてノードにインタフェースを追加します。[**ノードの追加**] または [**ノード プロファイル**] 画面に戻ります。

**インタフェースを追加した結果**

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、アクセスを提供するノード下に階層構造で表示されるノード リストに表示されます。

## ノードへの接続

ノードにインタフェースを割り当てると、多く方法でインタフェースを介してノードに接続できます。詳細は、Raritan の『**CommandCenter Secure Gateway ユーザ ガイド**』を参照してください。

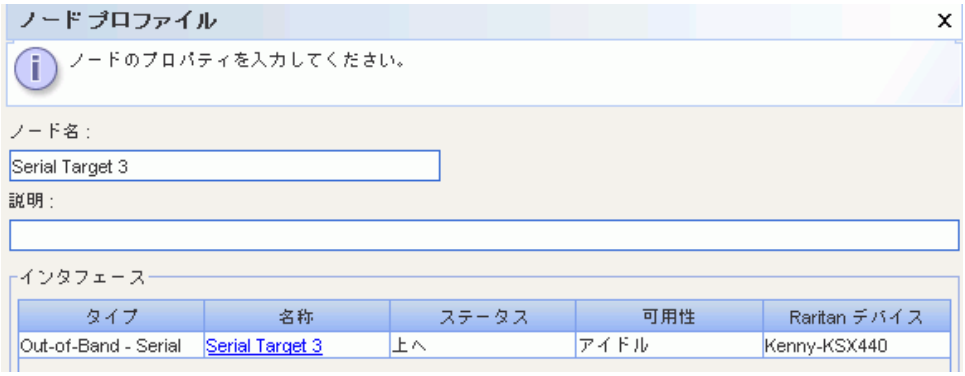


*図 69 ノードが設定されたインタフェースへの接続*

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ます。[**ノード プロファイル**] 画面が表示されます。
3. [**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 :**

1. [**ノード**] タブで、接続するノードの横に表示される + 記号をクリックし、そ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します。

## 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**] タブをクリックします。
2. 編集するインタフェースを持つノードをクリックします。[**ノード プロファイル**] 画面が表示されます。
3. [**インタフェース**] テーブルで、編集するインタフェースの行を選択します。
4. [**編集**] をクリックします。[**インタフェースの編集**] 画面が表示されます。

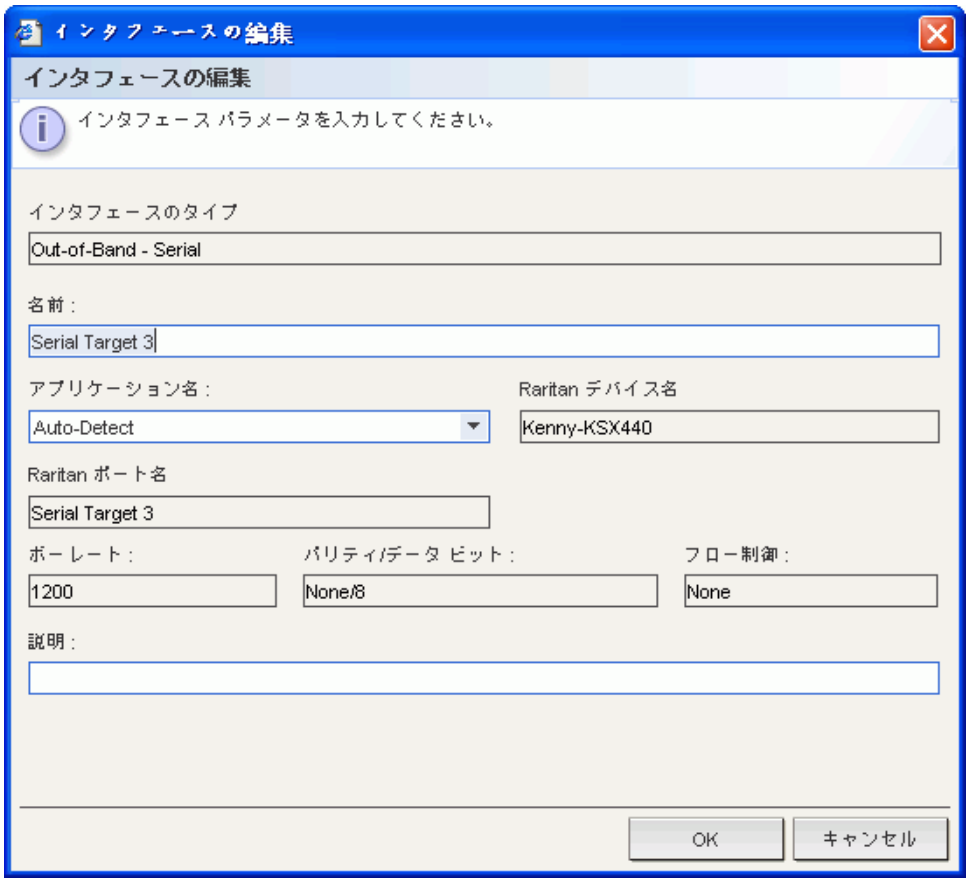


*図 70 インタフェースの編集*

5. 既存のインタフェース タイプを変更することはできません。[**インタフェース名**]、[**説明**]、このタイプの他のフィールド値を変更できます。詳細は、前述の「**インタフェースの追加**」を参照してください。

## 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。[**ノード プロファイル**] 画面が表示されます。
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。削除を確認するプロンプトが表示されます。
5. [**はい**] をクリックして、インタフェースを削除します。

## ノードに Ping を実行

CC-SG からノードに Ping を実行し、接続を確認できます。

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**] メニューで、[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。

## ノードの編集

既存のノードは、[**ノード**] タブに表示され、編集できます。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。

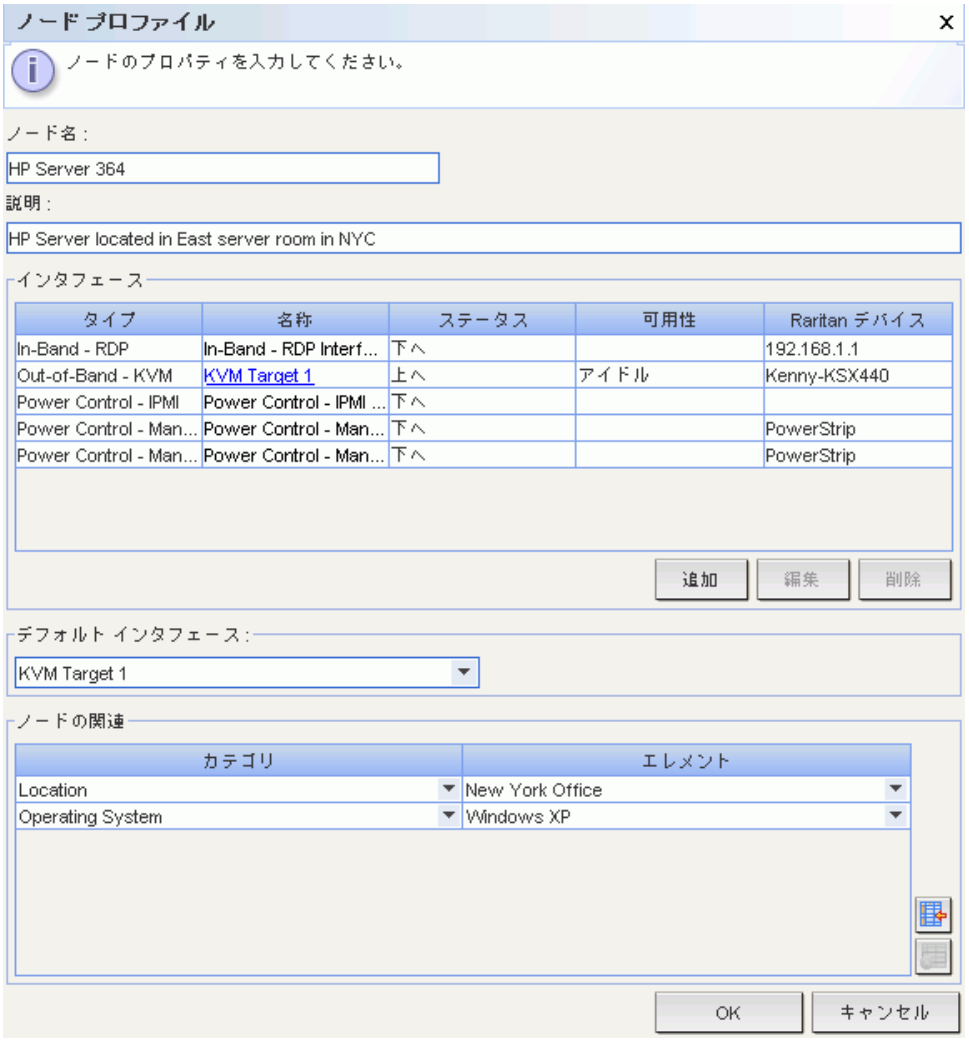


*図 71 ノードの編集画面*

2. 必要に応じて、[**ノード名**] フィールドにノードの新しい名前を入力することができます。CC-SG の全ノードには、固有の名前が必要です。
3. オプションとして、[**説明**] フィールドにこのノードの簡単な新しい説明を入力します。
4. [**インタフェース**] 領域で [追加] をクリックし、新しいインタフェースを追加します。この手順の詳細は、前述の「**インタフェースの追加**」を参照してください。
5. [**インタフェース**] テーブルで既存のノードを選択し、[編集] または [**削除**] をクリックして、ノードを編集するか、ノードからそのインタフェースを削除します。この手順の詳細は、前述の「**インタフェースの編集**」または「インタフェースの削除」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。カテゴリはノードを分類する方法で、エレメントはその分類の特定の値です。たとえば、ノードがエンジニアリング部の PC を表している場合は、カテゴリは「Department」、エレメントは「Engineering」などとなります。

ノードのカテゴリとエレメントを設定するには、以下の手順に従います。

a. リストの値を割り当てる各カテゴリで、その横にある [**エレメント**] をダブルクリックします。フィールドがドロップダウン メニューに変わります。
b. ドロップダウン メニューをクリックし、使用する [**エレメント**] 値を選択します。このカテゴリを使用しない場合は、[なし] 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。カテゴリおよびエレメントを作成する方法の詳細は、「**第 4 章 : 関連の作成**」を参照してください。

7. [**OK**] をクリックしてノードの設定を完了します。

## ノードの削除

ノードを削除すると、ノードのリストからノードが消えます。これで、ユーザはノードにアクセスできなくなり、これまでに設定したインタフェースや関連が失われます。

ノードを削除するには、以下の手順に従います。

1. 左の [**ノード**] タブをクリックします。
2. 削除するノードを右クリックし、[**ノードの削除**] を選択します。[**ノードの削除**] 画面に選択したノードの名前が表示されます。

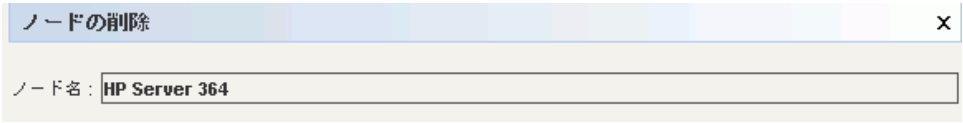


*図 72 ノードの削除*

3. [**OK**] をクリックしてノードを削除します。[キャンセル] をクリックすると、削除せずに終了します。

## チャット

チャットは、ユーザがお互いに通信するために同じノードに接続する方法です。ノードでチャット セッションを開始するには、そのノードに接続する必要があります。同じノードのユーザのみがチャットを行うことができます。

チャット セッションを行うには、以下の手順に従います。

1. 左の [**ノード**] タブをクリックします。
2. 現在接続しているノードを右クリックし、セッションが作成されていない場合は、[**チャット**] - [**チャット セッションの開始**] を選択します。チャット セッションが作成されます。

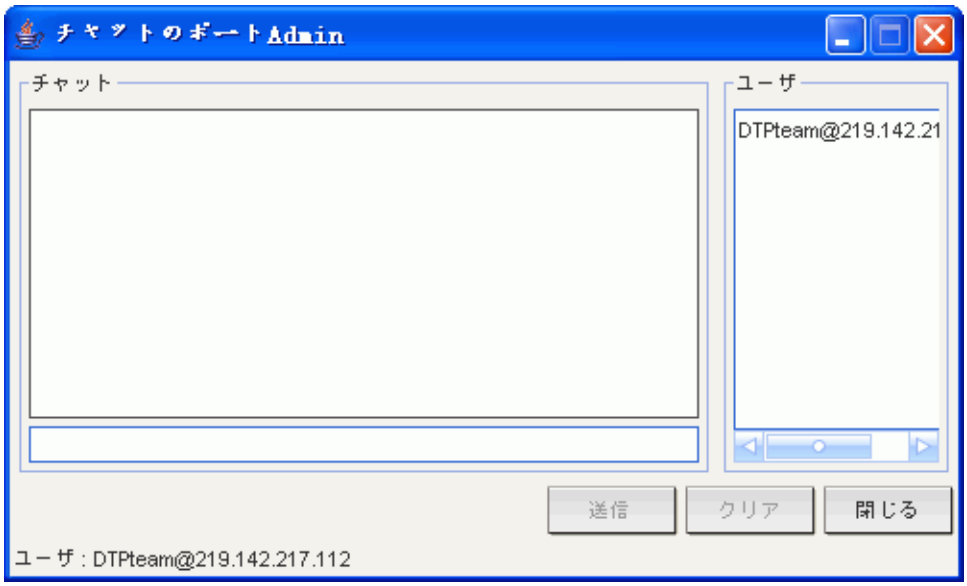


*図 73 ノードのチャット セッション*

チャット セッションが進行中の場合は、ノードを右クリックして、[**チャット**] - [**チャット セッションの表示**] を選択し、チャット セッションに参加します。

左側にメッセージのフィールド、右側にチャット セッションのユーザ リストを含むチャット セッションのウィンドウが表示されます。

3. 新しいメッセージのフィールド (左下) にメッセージを入力し、Enter キーを押すか、[**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、メッセージがチャット フィールド (左上) に表示されます。
4. 新しいメッセージのフィールドに入力たが、まだ送信していないメッセージをクリアするには、[**クリア**] をクリックします。チャット フィールドは [クリア] によってはクリアされません。
5. [**閉じる**] をクリックしてチャット セッションから出るか、チャット セッションを終了します。
6. チャット セッションを閉じるかどうかの確認プロンプトが表示されます。[**はい**] をクリックして、全参加者のすべてのチャット セッションを閉じます。または、[いいえ] をクリックして、チャット セッションは終了するが、他のユーザ用にチャット セッションを実行したままにしておきます。

[ノード] タブから、全参加者のチャット セッションを閉じることもできます。チャット セッションを実行しているノードを右クリックし、[**チャット**] - [**チャット セッションの終了**] を選択します。

## ノード グループ

ノード グループを使用すると、任意、またはアクセス ポリシーの作成に使用するカテゴリやエレメントに基づいて、管理者がノードの論理グループを作成できます。ノード グループの作成およびグループへのポリシーの割り当て方法の詳細は、「**第 8 章 : ポリシー**」を参照してください。

[**ノード グループ**] ウィンドウは、[**ノード**] リストでノードを右クリックし、[**ノード グループ**] を選択して表示できます。

*本ページは意図的に空白となっています。*

# 第 7 章 : ユーザとユーザ グループの追加および管理

ユーザとは、ノードにアクセスし、デバイスを管理するために CC-SG に接続する個人のユーザと管理者を意味します。ユーザ グループとは、メンバ ユーザの権限セットを定義する組織を意味します。ユーザ自身には権限はありません。一般に、すべてのユーザは、ユーザ グループに属する必要があります。

CC-SG は、独自の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、本章で説明される承認を保持します。外部認証スキーマ (RADIUS や Active Directory など) を使用する場合でも、ユーザ グループとポリシー (「**第 8 章 : ポリシー**」を参照) を CC-SG で作成する必要があります。外部認証を使用するように CC-SG を設定する方法についての詳細は、「**第 9 章 : リモート認証**」を参照してください。

## ユーザ ツリー

[**ユーザ**] タブをクリックして、ユーザ ツリーを表示します。

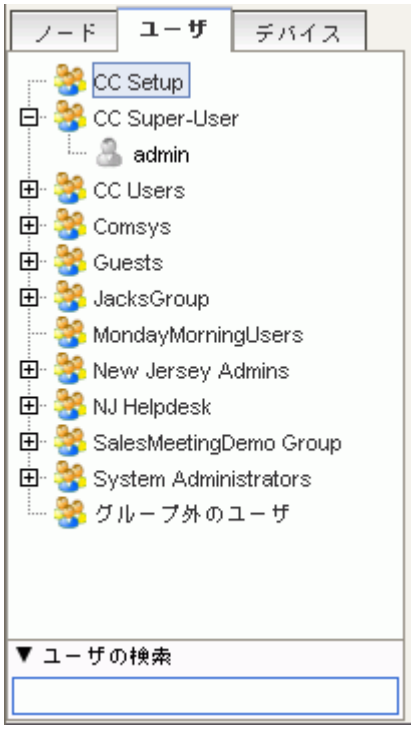


*図 74 ユーザ ツリー*

ユーザ ツリーには、CC-SG でのユーザ グループとユーザがすべて表示されます。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。この記号をクリックすると、メンバ ユーザのリストを広げたり折りたたんだりすることができます。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 ツリーを使用すると、ツリー内でユーザを検索できます。検索方法は、本章で後述する [**プロファイル**] 画面で設定できます。

## 特殊なユーザ 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。

### 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。CC スーパーユーザ グループとは異なり、権限の変更、メンバの追加や削除が可能です。

### 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。

### グループ外のユーザ

**グループ外のユーザ**は権限を持たず、ユーザを作成したり、このグループに手動でユーザを移動したりすることはできません。ユーザは、既存のユーザ グループすべてから削除されると、このグループに割り当てられます。

**重要：本章のコマンドの多くは、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。**

**このセクションで説明されているメニュー バー コマンドの多くは、ユーザ グループまたはユーザを右クリックして表示されるショートカット メニューからも実行できます。**

## 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。各権限の意味についての詳細は、「**付録 D : ユーザ グループ権限**」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示すポリシーを選択する。

新しいユーザ グループを作成するには、以下の手順に従います。

1. [ユーザ] メニューの [ユーザ グループ マネージャ] - [ユーザ グループの追加] をクリックします。[ユーザ グループの追加] 画面が表示されます。

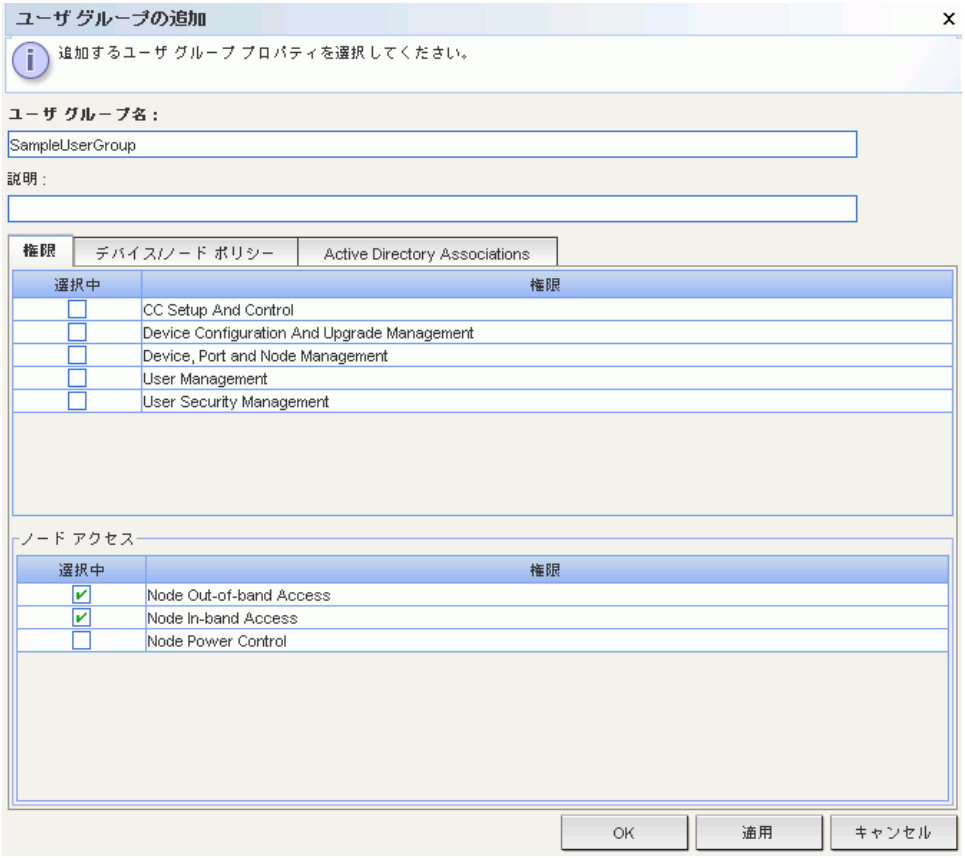


*図 75 ユーザ グループの追加画面*

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。
3. オプションとして、[**説明**] フィールドにこのユーザ グループの簡単な説明を入力します。
4. [**権限**] タブをクリックします。

ユーザ グループに割り当てる各権限に該当するチェックボックスをオンにします。

5. 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該当するチェックボックスをオンにします。

[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。

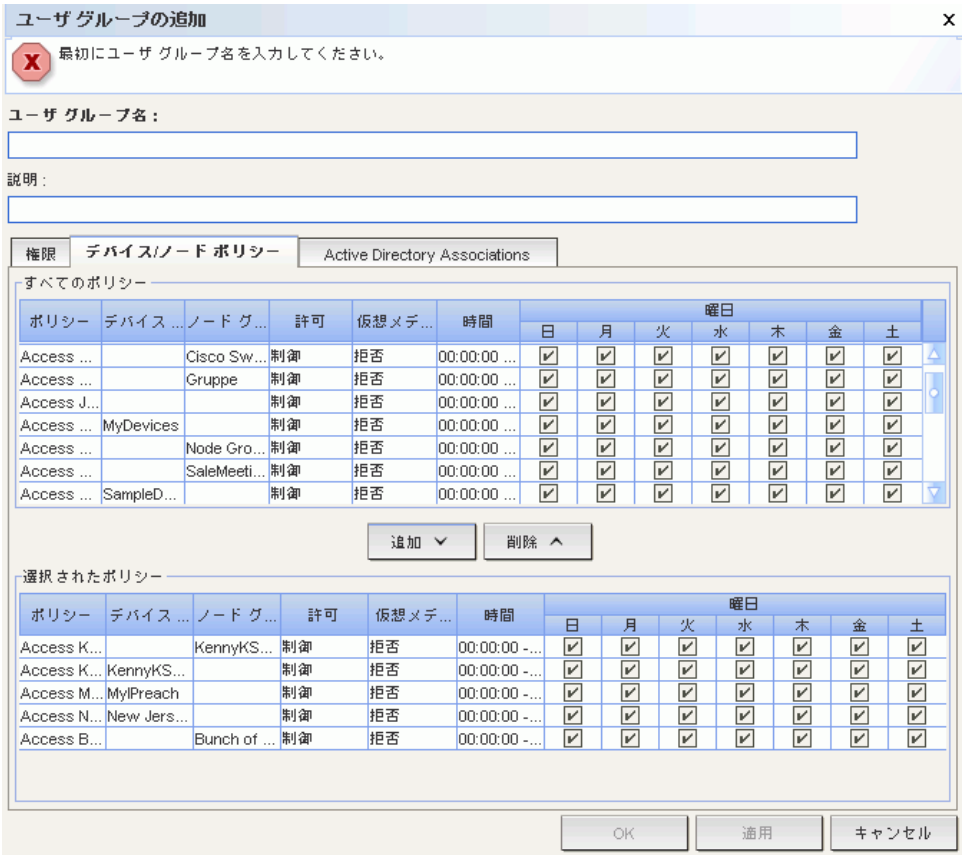


*図 76 ユーザ グループの追加画面のポリシー タブ*

[**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。ポリシーを作成する方法の詳細は、「**第 8 章：ポリシー**」を参照してください。

6. [**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、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。

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。

7. 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、[**すべてのポリシー**] リストで [**Full Access Policy**] を選択してから、[追加] をクリックします。
8. 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。
9. このグループでポリシーを設定したら、[**適用**] をクリックしてこのグループを保存し、さらに新しいグループを作成します。または、[**OK**] をクリックして、ユーザ グループを保存し、グループの作成を終了します。[**適用**] をクリックした場合は、ここで説明されている手順を繰り返し、さらにユーザ グループを追加します。

## 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 グループとグループ外のユーザ** グループの権限またはポリシーは編集できません。*

グループを編集するには、以下の手順に従います。

1. 左の [**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。

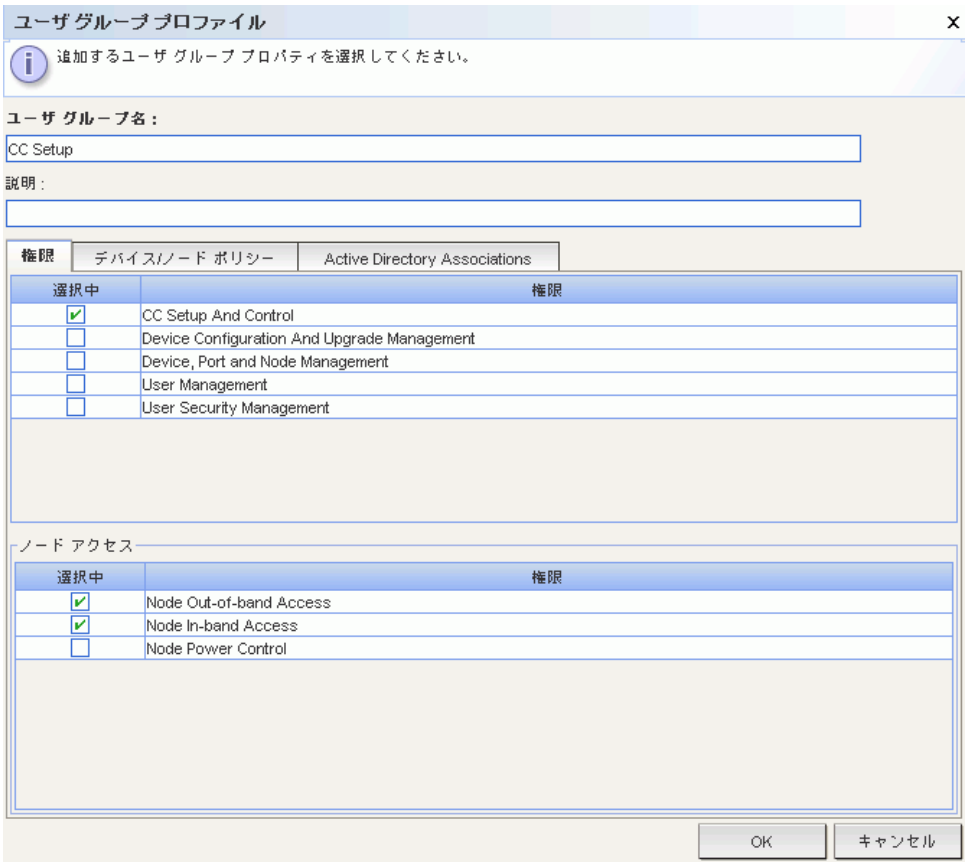


*図 77 選択されたグループの編集*

3. 必要な場合は、[**ユーザ グループ名**] フィールドに新しいグループ名を入力します。
4. オプションとして、[**説明**] フィールドにこのユーザ グループの簡単な新しい説明を入力できます。
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該当するチェックボックスをオンにします。チェックボックスの選択をオフにして、グループからその権限を削除します。
7. [**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。
8. 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。
9. [**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。
10. 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。

11. ユーザ グループから削除するポリシーについて、[**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。
12. このグループのポリシーを設定したら、[**OK**] をクリックしてこのグループへの変更を保存します。または、[**キャンセル**] をクリックして、保存せずに終了します。

## ユーザ グループの削除

ユーザ グループを削除すると、CC-SG からそのグループが削除されます。削除されたグループのユーザは、割り当てられた他のグループには残ります。削除されたグループのユーザが他のどのグループにも属していない場合は、グループ外のユーザ グループに割り当てられます。このグループは、どの権限も持ちません。

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. 左の [**ユーザ**] タブをクリックします。
2. [**ユーザ**] タブで削除するユーザ グループをクリックします。
3. [**ユーザ**] メニューの [ユーザ グループ マネージャ] - [**ユーザ グループの削除**] をクリックします。[ユーザ グループの削除] 画面が表示されます。

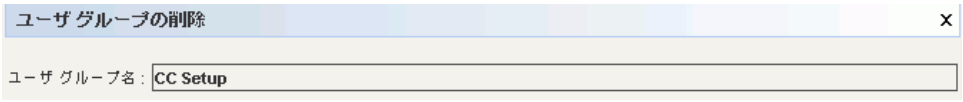


*図 78 ユーザ グループの削除*

4. [**OK**] をクリックしてユーザ グループを削除します。 [**キャンセル**] をクリックすると、グループを削除せずに終了します。

[**OK**] をクリックしたら、グループが削除されたことを確認するステータス メッセージが表示されます。

## ユーザの追加

グループにユーザを追加して、CC-SG でのユーザ アクセス権限を割り当てます。ユーザがノードへのアクセスやデバイスの管理が可能かどうかは、追加されたユーザ グループによって変わります。

ユーザを追加するには、以下の手順に従います。

1. 左の [**ユーザ**] タブをクリックします。
2. [**ユーザ**] タブでユーザを追加するユーザ グループをクリックします (グループを選択せずにユーザを追加することはできません)。
3. [**ユーザ**] メニューの [**ユーザ マネージャ**] - [**ユーザの追加**] をクリックします。[**ユーザの追加**] 画面が表示されます。

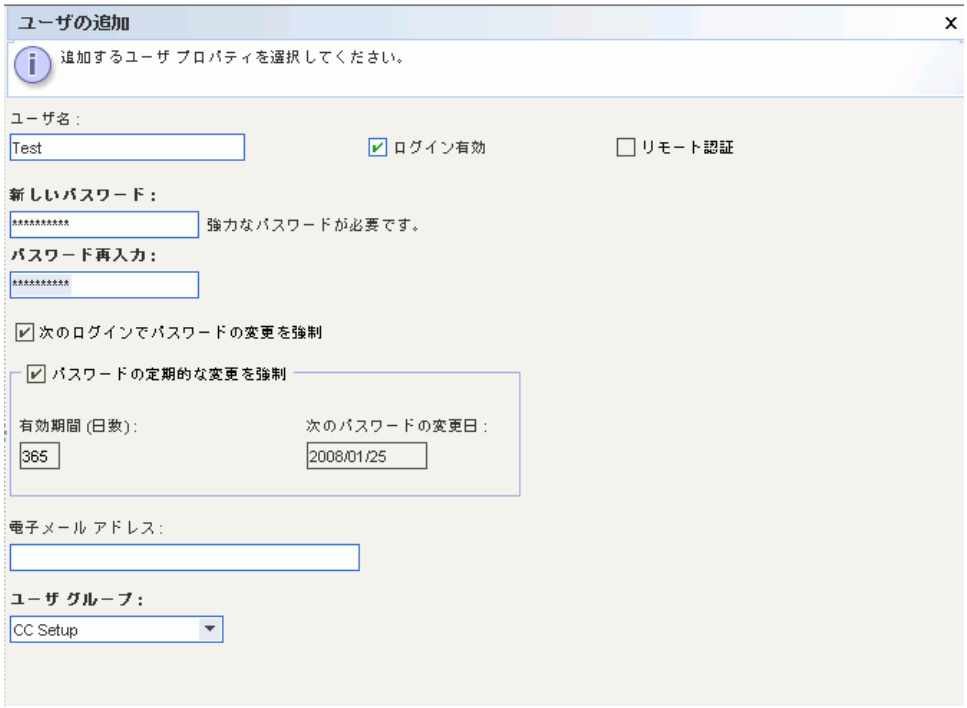


*図 79 ユーザの追加画面*

4. [**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。ユーザは、この名前を使用して、CC-SG にログインします。
5. 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 ボックスをオンにします。
6. TACACS+、RADIUS、LDAP または AD などの外部サーバで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オンにします。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**] のフィールドは使用できません。
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 のログインに使用するパスワードを入力します。

---

***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、「第 12 章 :* ***高度な管理*** *」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 ボックスをオンにすると、このユーザは次回 CC-SG に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。
9. ユーザがパスワードの変更を強制される頻度を指定するには、[**パスワードの定期的な変更を強制**] チェック ボックスをオンにします。

a. このをオンにした場合は、[**有効期間 (日)**] フィールドに、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入力します。

10. [**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。
11. このユーザを追加するグループを変更するには、[ユーザ グループ] ドロップダウン メニューをクリックし、新しいグループを選択します。
12. 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

ユーザを編集するには、以下の手順に従います。

1. 左の [**ユーザ**] タブをクリックします。
2. 編集するユーザが属する [**ユーザ グループ**] の横の + 記号をクリックします。
3. 編集するユーザをクリックします。[**ユーザ プロファイル**] 画面が表示されます。

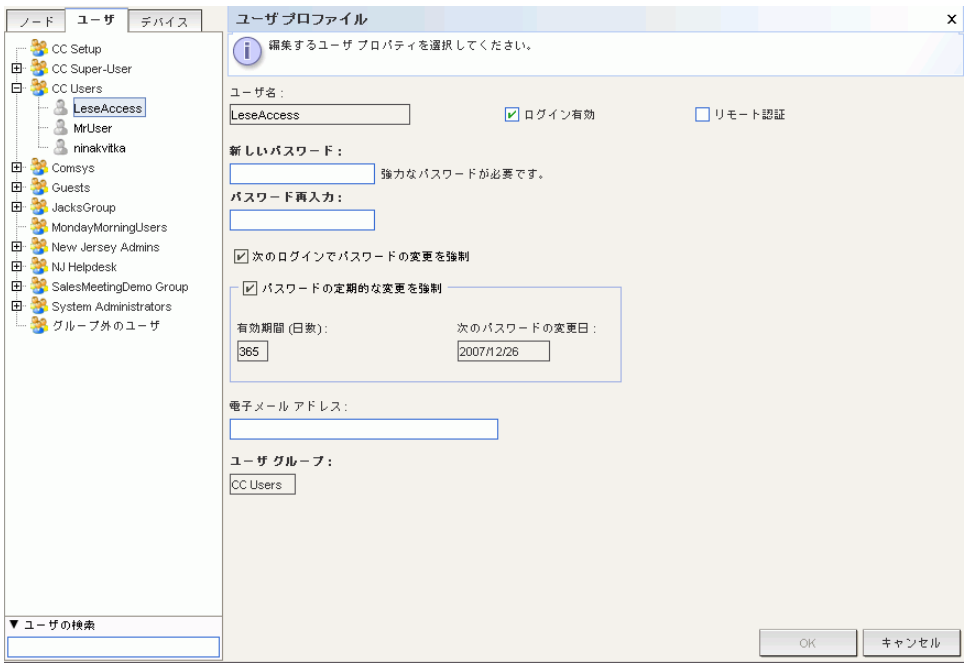


*図 80 選択されたユーザの編集*

4. 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 ボックスをオフにします。ユーザが CC-SG にログインできるようにするには、[**ログイン有効**] チェック ボックスをオンにします。
5. TACACS+、RADIUS、LDAP または AD などの外部サーバで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オンにします。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**] のフィールドは使用できません。
6. [**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、「**第 12 章 : 高度な管理**」を参照してください。*

---

7. [**次のログインでパスワードの変更を強制**] チェック ボックスをオンにすると、このユーザは次回 CC-SG に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。
8. [**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 アドレスに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。
9. このユーザを編集したら、[**OK**] をクリックしてこのユーザへの変更を保存します。または、[**キャンセル**] をクリックして、保存せずに終了します。

***注** : ユーザが属するグループを編集することはできません。詳細は、この後の「**ユーザをグループに追加**」を参照してください。*

## 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、必要のないアカウントを削除するのに便利です。

ユーザを削除するには、以下の手順に従います。

1. 左の [**ユーザ**] タブをクリックします。
2. 削除するユーザが属する [**ユーザ グループ**] の横の + 記号をクリックします。
3. 削除するユーザをクリックします。
4. [**ユーザ**] メニューの [**ユーザ マネージャ**] - [**ユーザの削除**] をクリックします。[**ユーザの削除**] 画面が表示されます。

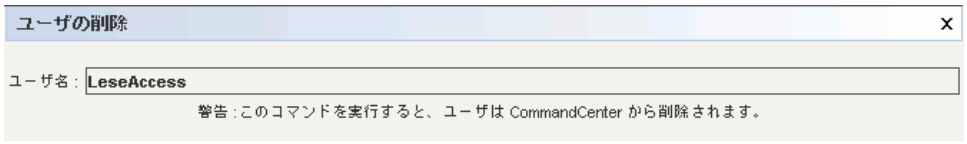


*図 81 ユーザの削除*

5. [**OK**] をクリックして CC-SG からユーザを削除します。[キャンセル] をクリックすると、削除せずに終了します。

***注** : このコマンドは、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を削除します。1 つのグループからのみユーザを削除する場合は、後の「**ユーザをグループから削除**」を参照してください。*

## ユーザをグループに割り当て

このコマンドを使用して、既存のユーザを現在属していないグループに割り当てます。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、後に説明する [**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. 左の [**ユーザ**] タブをクリックします。
2. ユーザを割り当てるユーザ グループをクリックします。
3. [**ユーザ**] メニューの [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] をクリックします。[**ユーザをグループに割り当て**] 画面が表示されます。

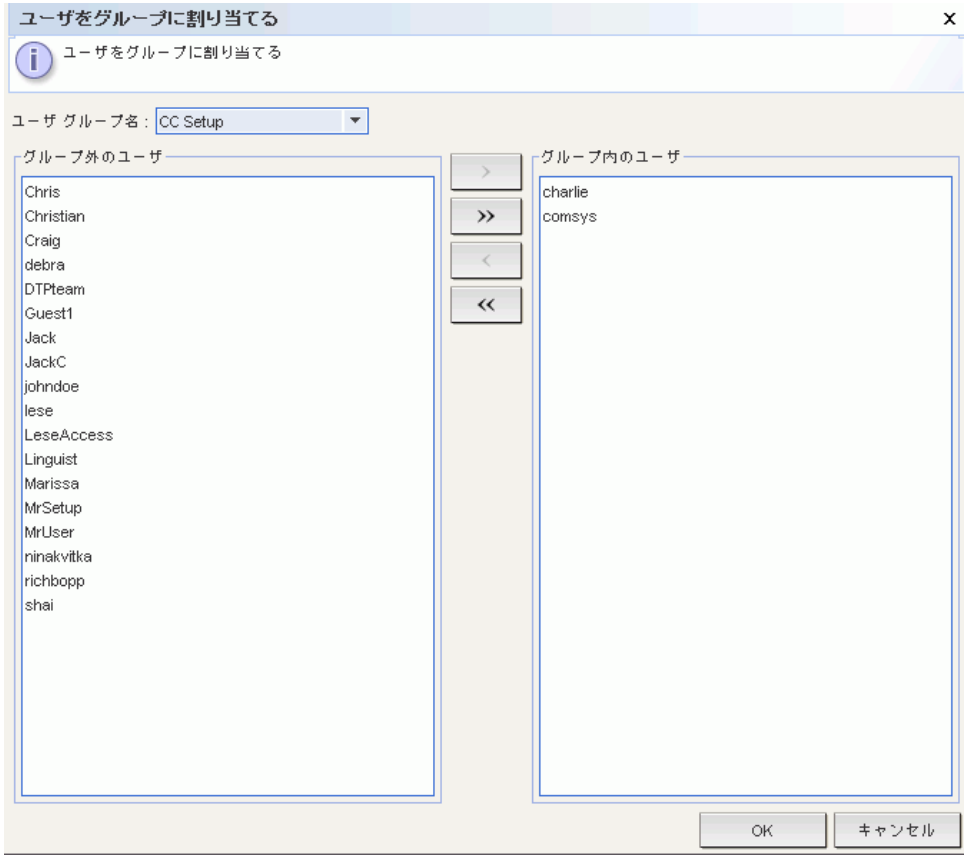


*図 82 ユーザをグループに割り当て画面*

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。ここから追加するユーザを選択し、[>] ボタンをクリックして、ユーザを [**グループ内のユーザ**] リストに移動します。
5. [>>] ボタンをクリックすると、[**グループ内のユーザ**] リストにすべてのユーザが移動します。

ターゲット グループからユーザを削除するには、[グループ内のユーザ] リストでユーザを選択し、[<] ボタンをクリックします。

6. [<<] 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。

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

このコマンドは、選択されているグループから選択したユーザを削除します。このコマンドは、他のグループからユーザを削除したり、CC-SG からユーザを削除したりすることはありません。

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. 左の [**ユーザ**] タブをクリックします。
2. 削除するユーザが属する [**ユーザ グループ**] の横の + 記号をクリックします。
3. 削除するユーザをクリックします。
4. [**ユーザ**] メニューの [**ユーザ マネージャ**] - [**ユーザをグループから削除**] をクリックします。ユーザとユーザが削除されるグループを示す [**ユーザの削除**] 画面が表示されます。

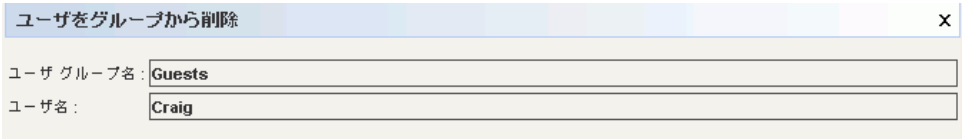


*図 83 ユーザをグループから削除*

5. [**OK**] をクリックしてユーザをグループから削除します。 [**キャンセル**] をクリックすると、削除せずに終了します。

***注** : グループからユーザを削除し、そのユーザが他のグループには属していない場合は、ユーザは、[**グループ外のユーザ**] グループに追加されます。*

## その他のユーザおよびユーザ グループ機能

### 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可能になります。admin アカウントのアカウント名を変更する唯一の方法でもあります。

プロファイルを編集するには、以下の手順に従います。

1. [**Secure Gateway**] メニューの [**プロファイル**] をクリックします。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。

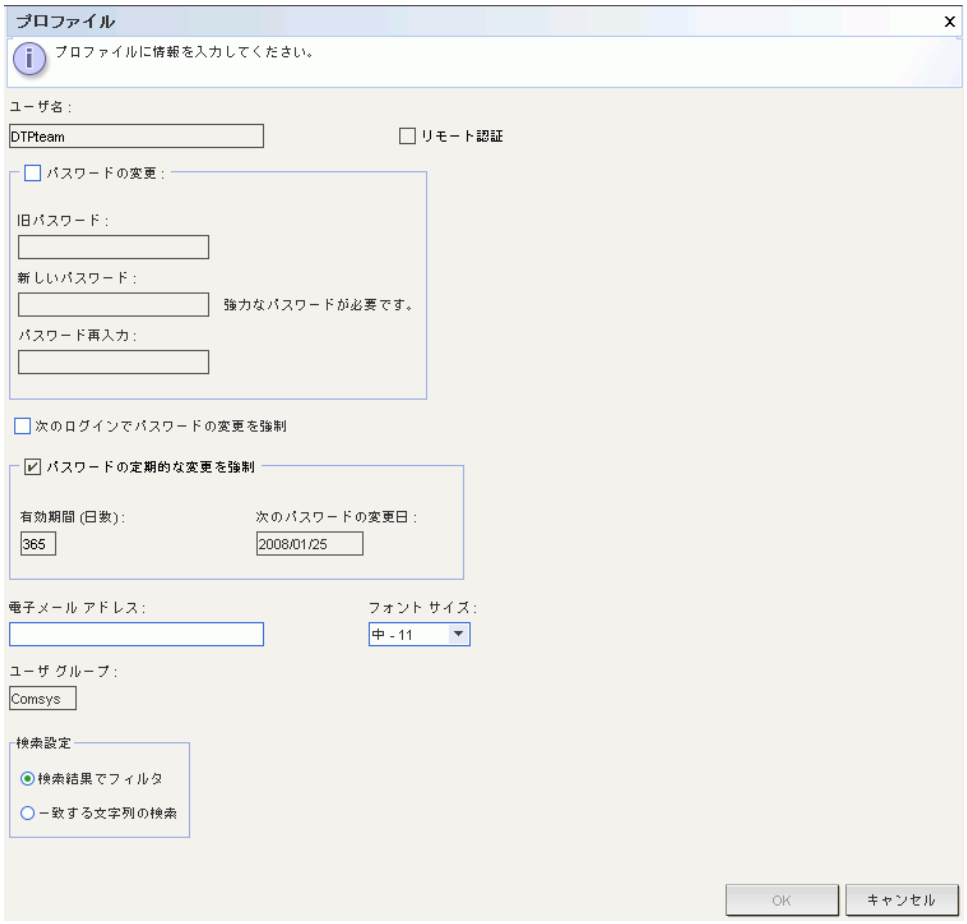


*図 84 プロファイル画面*

2. **admin** アカウントでログインしている場合は、[**ユーザ名**] フィールドに新しい名前を入力して、アカウントの名前を変更できます。
3. パスワードを変更する場合は、[**パスワードの変更**] チェック ボックスをオンにします。
   a. [**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。
   b. [**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。
   c. [**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。
4. [**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。
5. [**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 クライアントで表示するフォントのサイズを調整します。
6. [**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。
7. プロファイルを編集したら、[OK] をクリックして変更を保存します。または、[キャンセル] をクリックして、保存せずに終了します。

## ユーザのログアウト

このコマンドは、CC-GS からアクティブなユーザをログアウトさせるのに使用できます。このコマンドは、CC-GS のアクティブなユーザをすべてログアウトさせるのにも使用できます。

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. 左の [**ユーザ**] タブをクリックします。
2. ログアウトさせるユーザが属する [**ユーザ グループ**] の横の + 記号をクリックします。
3. ログアウトさせるユーザをクリックします。複数のユーザをログアウトさせる場合は、**Ctrl** キーを押しながら、他のユーザをクリックします。
4. [**ユーザ**] メニューの [**ユーザ マネージャ**] - [**ユーザのログアウト**] をクリックします。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。
5. [**OK**] をクリックして CC-SG からユーザをログアウトさせます。[**キャンセル**] をクリックすると、ユーザをログアウトさせずに終了します。

**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. 左の [**ユーザ**] タブをクリックします。
2. ログアウトさせるユーザが属するユーザ グループをクリックします。複数のユーザ グループをログアウトさせる場合は、**Ctrl** キーを押しながら、他のグループをクリックします。
3. [**ユーザ**] メニューの [**ユーザ グループ マネージャ**] - [**ユーザのログアウト**] をクリックします。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。
4. [**OK**] をクリックして CC-SG からユーザをログアウトさせます。[**キャンセル**] をクリックすると、ユーザをログアウトさせずに終了します。

## 一括コピー

[**一括コピー**] を使用すると、既存のユーザを選択したユーザと同じユーザ グループに移動して、あるユーザの権限とポリシーを既存ユーザに複製し、時間を節約できます。一括コピーを実行するには、以下の手順に従います。

1. 左の [**ユーザ**] タブをクリックします。
2. コピーするユーザが属する [**ユーザ グループ**] の横の + 記号をクリックします。
3. コピーするユーザをクリックします。
4. [**ユーザ**] メニューの [ユーザ マネージャ] - [**一括コピー**] をクリックします。[**一括コピー**] 画面が表示されます。

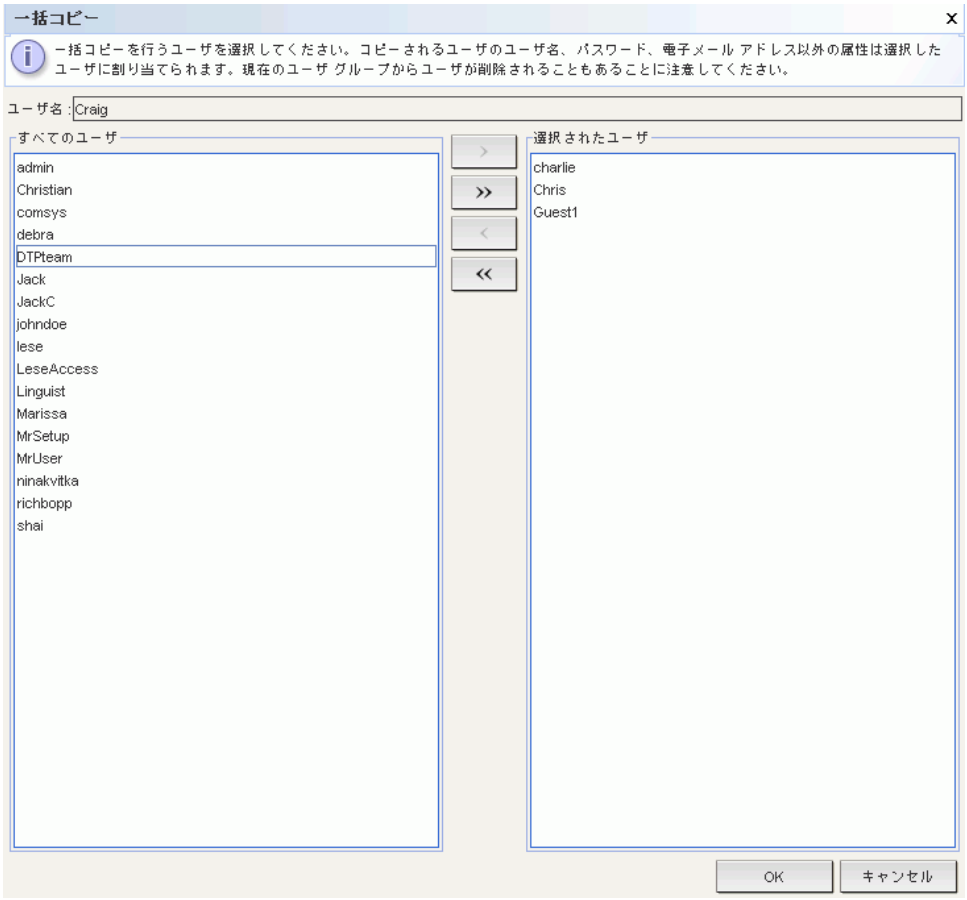


*図 85 一括コピー画面*

5. [**すべてのユーザ**] リストで、[**ユーザ名**] フィールドで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。
6. [>] ボタンをクリックすると、そのユーザ名が [**選択されたユーザ**] リストに移動します。
7. [>>] 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。
8. [**選択されたユーザ**] リストからユーザを削除するには、ユーザを選択してから [<] ボタンをクリックします。
9. [<<] 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。
10. [**OK**] をクリックして、ユーザのプロパティをコピーします。コピーされたユーザは、既存のグループから、選択したユーザが属するグループに移動します。

# 第 8 章 : ポリシー

## ポリシーによるアクセスの制御

新しいポリシーを設定し、ノードへのユーザ アクセスを提供する操作はオプションですが、そのアクセスを制御する CC-SG の機能を効果的に利用できます。すべてのユーザにすべてのノード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 [**Full Access Policy**] を割り当てます。

ノードへのユーザ アクセスをより詳細に制御する場合は、そのアクセスのルールを定義するポリシーを作成する必要があります。すべての権限と同様に、ポリシーは、ユーザ グループに割り当て、グループに属するユーザにアクセス ルールを適用できます。

**ガイド付き設定**を実行した場合は (「**第 3 章 : ガイド付き設定を使用した CC-SG の設定**」を参照)、複数の基本的なポリシーがすでに作成されている場合があります。**ガイド付き設定**を使用しなかった場合、またはポリシーを新たに作成した場合は、以下の指示に従います。次のことを行います。

- 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。
- ノードへのインタフェースを提供する Raritan デバイス用のアクセス ルールを作成する場合は、デバイス グループを作成する。
- ノード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) のポリシーを作成する。
- このポリシーをユーザ グループに適用する。

### ポリシーのまとめ

次の図は、CC-SG でセキュリティを実装する方法を図に表したものです。

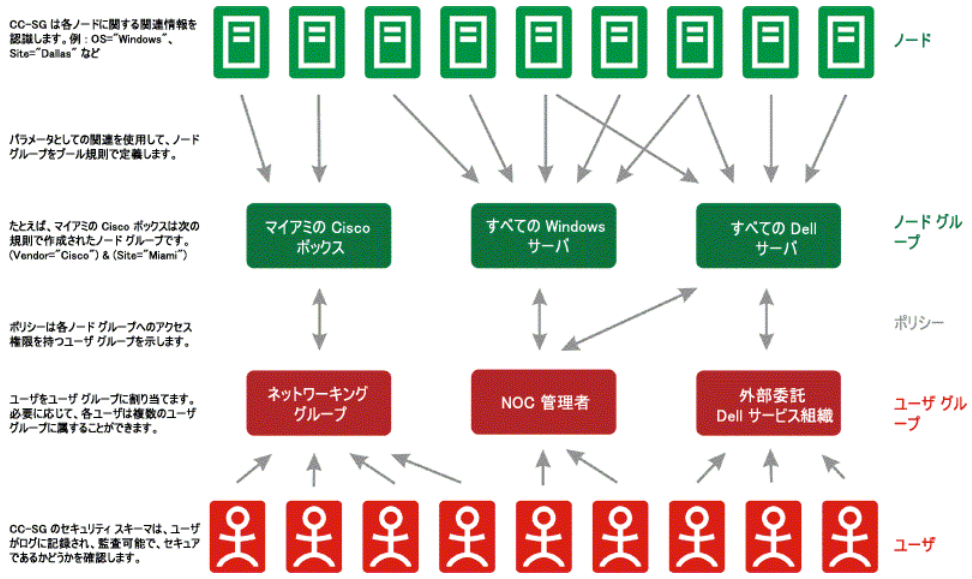


*図 86 ポリシーのまとめ*

# ノード グループ

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。このグループは、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。ノードは自由にグループ化したり、共通の属性のセットを使ってグループ化したりすることができます。

さらに、関連マネージャ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を作成する方法の詳細は、「第 4 章 : **関連**」を参照してください。

既存のノード グループを表示するには、以下の手順に従います。

[関連] メニューで [ノード グループ] をクリックします。[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 グループのリストは左側、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。

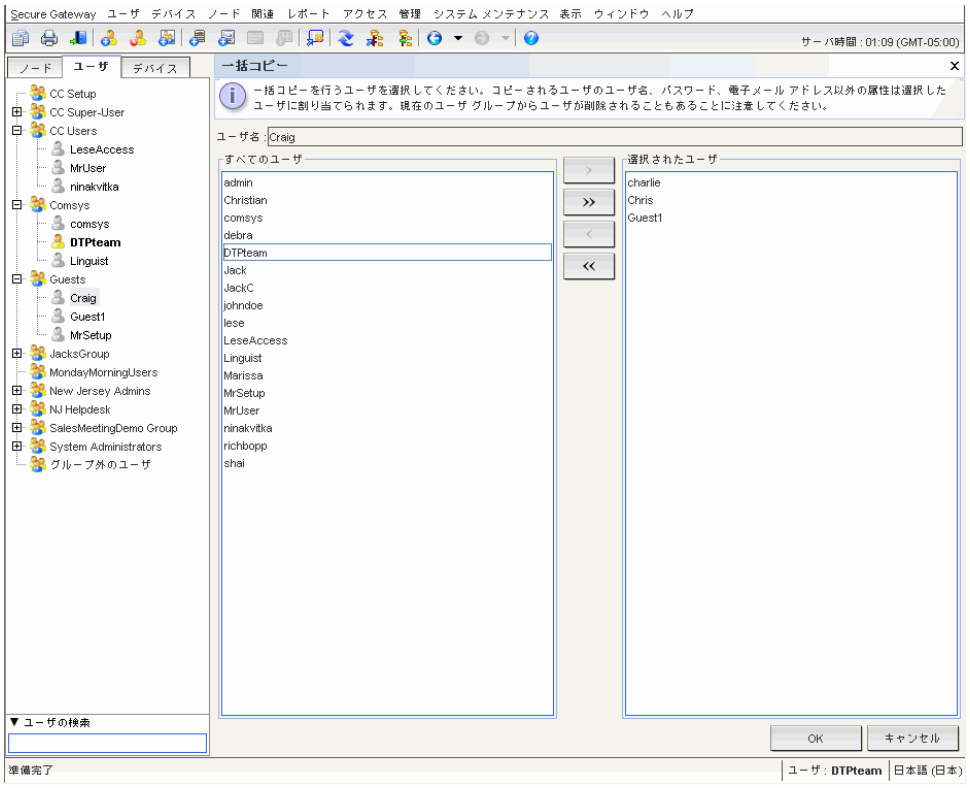


*図 87 ノード グループ マネージャ*

1. 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。
2. [**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。詳細は、**「第 7 章 : ユーザとユーザ グループ」**を参照してください。

3. 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] ウィンドウが表示されます。

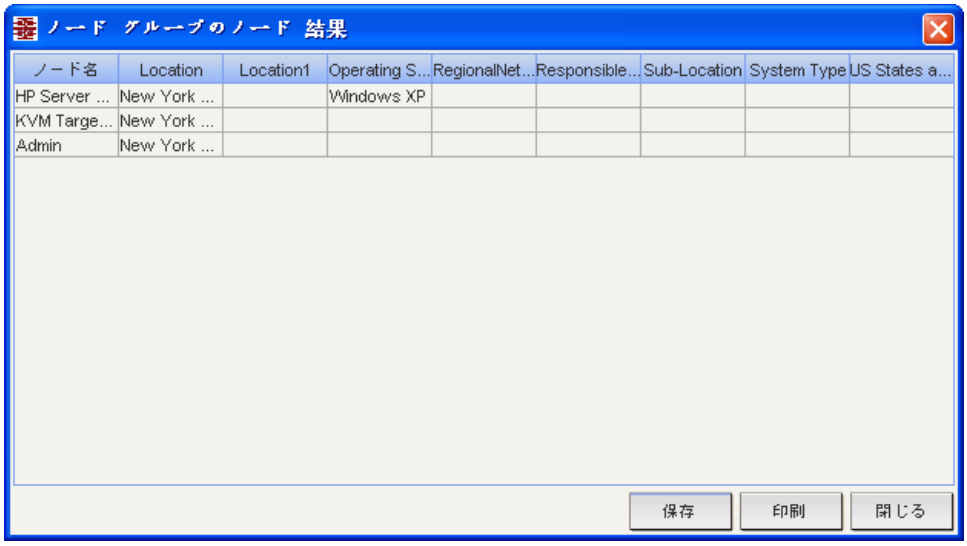


*図 88 属性を基にしたグループのノード*

## ノード グループの追加

新しいノード グループを追加するには、以下の手順に従います。

1. [**関連**] メニューで [**ノード グループ**] をクリックします。[**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**] メニューで、[**追加**] 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. [**グループ名**] フィールドに作成するノード グループの名前を入力します。

グループにノードを追加する方法には、[**ノードの選択**] と [**ノードの説明**] の 2 種類があります。ノードの選択では、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。

## ノードの選択

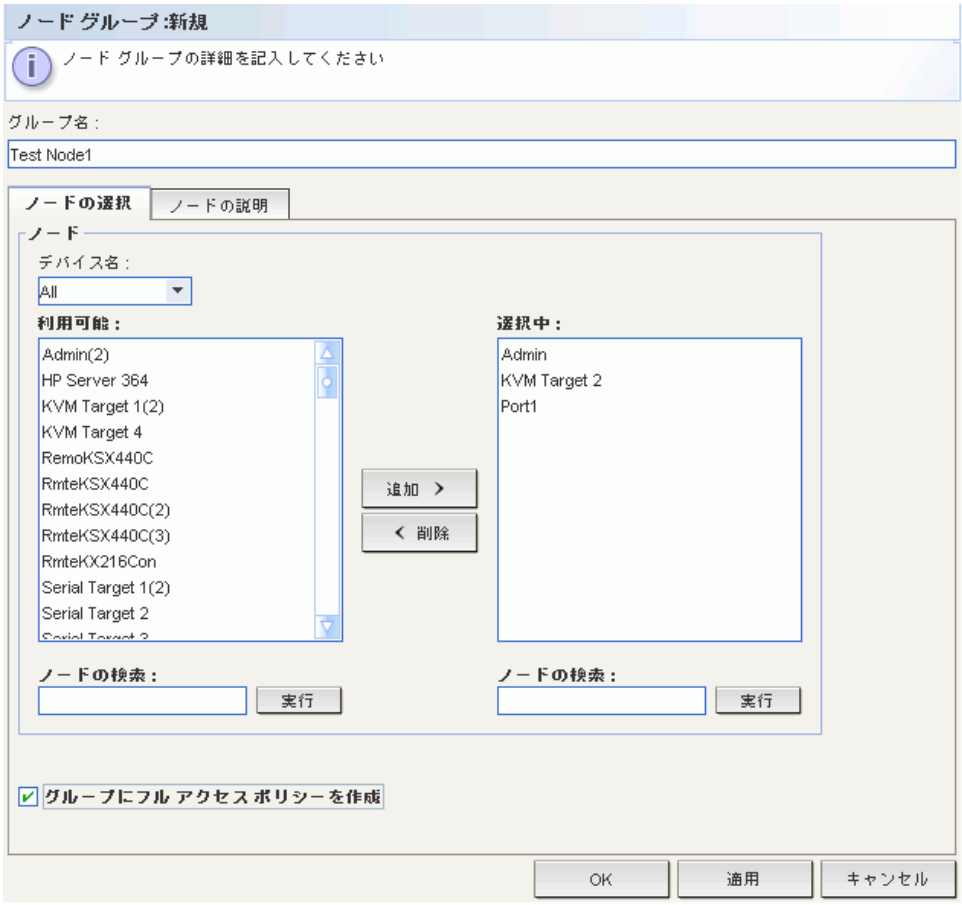


*図 89 ノードの選択によるノードの追加*

1. [**ノードの選択**] タブをクリックします。
2. [**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する場合は、[**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。
4. グループからノードを削除する場合は、[**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。
5. [**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。
6. 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**] をオンにします。
7. グループにノードを追加したら、[**追加**] 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

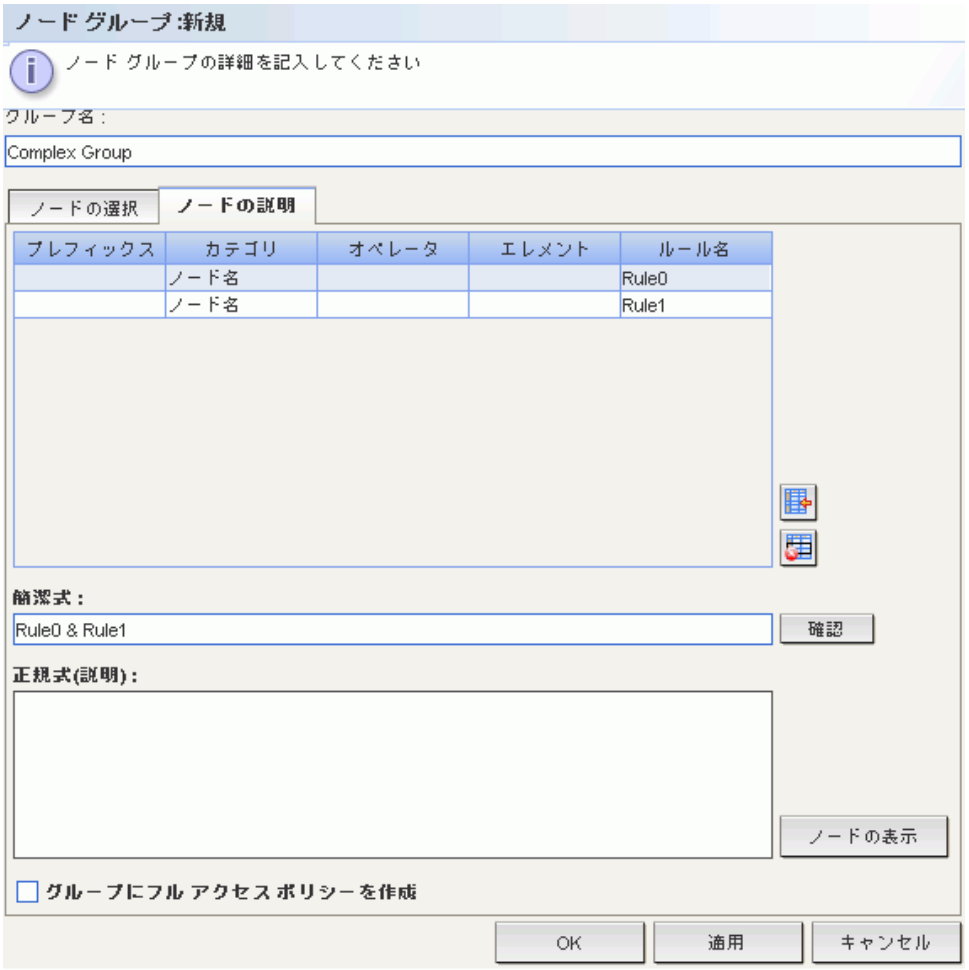


*図 90 複数のルールを持つノード グループの説明*

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**] をクリックして、表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。
   - **オペレータ** - カテゴリとエレメント アイテム間で実行される比較演算子を選択します。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**] 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。
5. ルールを削除する場合は、表内でルールをハイライトし、[**選択した行をテーブルから削除**] をクリックします。
6. 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。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するだけです。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。
   - ( および ) - 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。

   たとえば、エンジニアリング部門に属するノードを説明する場合は、「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。

   さらに、たとえば、エンジニアリング部門に属するノードのグループ、またはフィラデルフィアにあるノード グループ、さらにすべてのマシンが 1 GB のメモリを持つノード グループを説明するには、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)。そして、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ノードとなるので、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。

7. [**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 (説明)**] フィールドに正規化された式が表示されます。
8. [**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か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、ルール表または [**簡潔式**] フィールドに戻って、式を調整します。
9. 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**] をオンにします。
10. このグループに属するノードの説明を入力したら、[**追加**] 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、グループのメンバー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**] メニューで [**ノード グループ**] をクリックします。[**ノード グループ マネージャ**] ウィンドウが表示されます。

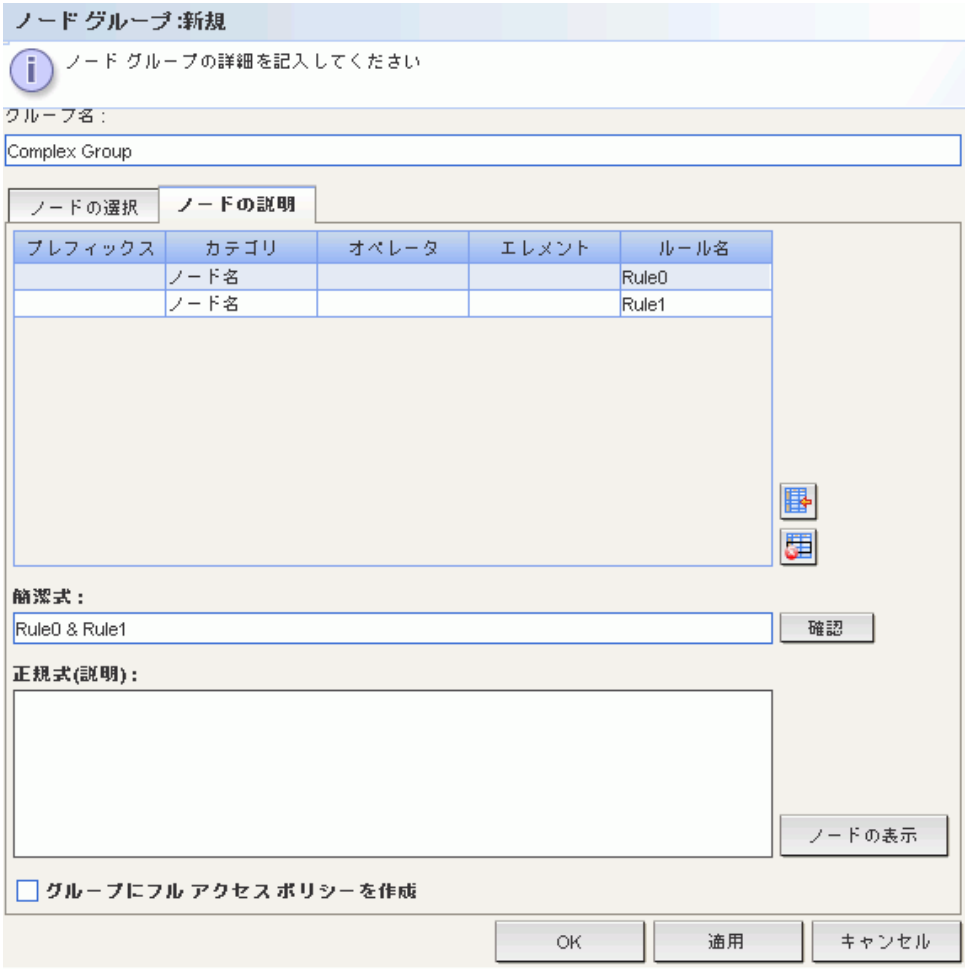


*図 91 ノード グループの編集*

2. 左側の [**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、上記の「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. ノード グループの編集が終わったら、[**編集**] をクリックします。

## ノード グループの削除

1. [**関連**] メニューで [**ノード グループ**] をクリックします。[**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. 左側の [**ノード グループ**] リストで、削除するノードをクリックします。
3. [**グループ**] メニューで [**削除**] をクリックします。

## デバイス グループ

デバイス グループは、ノード グループと同じような方法で動作します。ただし、デバイス グループは、ポリシーによって管理できるよう、Raritan デバイスをセットに整理するために使用されます。

詳細は、「第 5 章 : デバイスおよびデバイス グループの追加」を参照してください。

## ポリシー マネージャ

ノード グループとデバイス グループを作成すると、アクセス ポリシーを作成する基本となります。アクセス ポリシーは、グループのノードやデバイス (またはデバイス グループ) にユーザがアクセスできるかどうかと、このルールが有効となる時間を示すルールです。

### ポリシーの追加

ポリシーを追加するには、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**] 画面が表示されます。

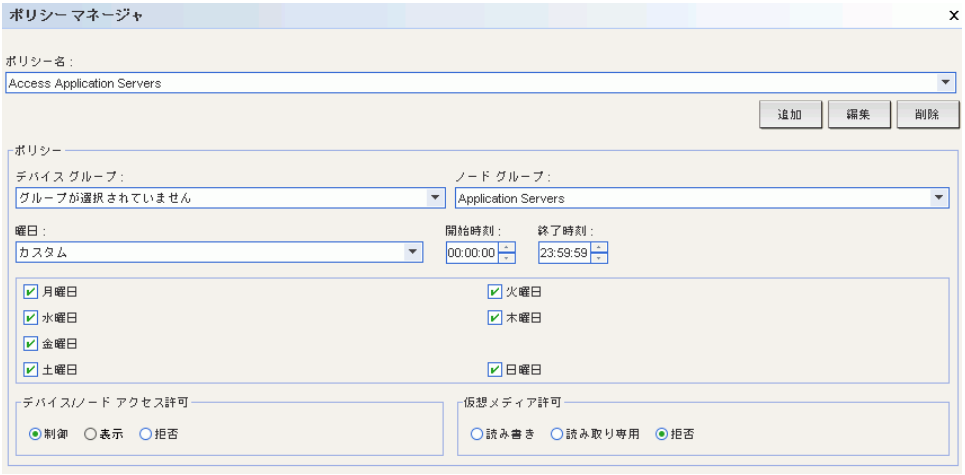


*図 92 ポリシー マネージャ*

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。

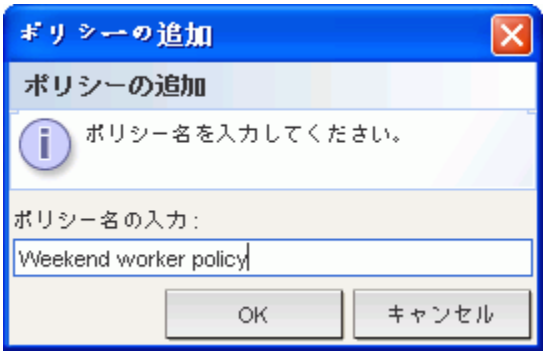


*図 93 ポリシーの追加*

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。
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、このポリシーがアクセスを制御するデバイス グループを選択します。

[**デバイス グループ**] ドロップダウン矢印をクリックし、このポリシーがアクセスを制御するノード グループを選択します。

ポリシーが 1 種類のグループのみに適用される場合は、そのグループの値を選択するだけです。

6. [**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。
   a. 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。
   b. 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オンにします。
7. [**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。
8. [**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。
9. [**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。
10. [**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。

---

***注** : ノード グループまたはデバイス グループに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、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 からログオフされます。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。詳細は、「第 11 章 : システム メンテナンス - メンテナンス モード」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**] 画面が表示されます。
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**] ウィンドウが表示されます。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。
4. [**デバイス グループ**] ドロップダウン矢印をクリックし、このポリシーがアクセスを制御するデバイス グループを選択します。

   [**デバイス グループ**] ドロップダウン矢印をクリックし、このポリシーがアクセスを制御するノード グループを選択します。

   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。
5. [**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。
   a. 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。
   b. 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オンにします。
6. [**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。

7. [**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。
8. [**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。
9. [**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。仮想メディア許可を許可するポリシーを定義するには、[**読み書き**] または [**読み取り専用**] 許可のいずれかを選択します。仮想メディア許可を拒否するポリシーを定義するには、[**拒否**] を選択します。
10. [**更新**] をクリックして、ポリシーへの変更を保存し、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。

### ポリシーの削除

ポリシーを削除するには、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**] 画面が表示されます。
2. [**ポリシー名**] ドロップダウン矢印をクリックし、リストから削除するポリシーを選択します。
3. [**削除**] をクリックし、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。

## ユーザ グループへのポリシーの適用

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。ユーザ グループにポリシーを割り当てる方法の詳細は、「**第 7 章：ユーザとユーザ グループの追加および管理**」を参照してください。

# 第 9 章 : リモート認証の設定

## 認証と承認 (AA)

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 RADIUS、TACACS+、および LDAP 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。

### 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、ローカル認証が実行されます。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。リモート認証を使用するユーザの追加についての詳細は、「**第 7 章 : ユーザとユーザ グループの追加および管理**」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 サーバ上のパスワードを変更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 DN 形式の説明は **RFC2253** を参照してください。このマニュアルの目的上は、識別名の入力方法とその名前がリストされる順序を理解しておく必要があります。

AD 用の識別名の指定でもこの構造に従う必要がありますが、**common name** と **organization unit** の両方を指定する必要がありません。

```
common name (cn), organizational unit (ou), domain component (dc)
```

Netscape LDAP および eDirectory LDAP の DN は次の構造に従って指定します。

```
user id (uid), organizational unit (ou), organization (o)
```

## ユーザ名

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 ユーザを認証すると、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

DN (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。[**ベース DN**] フィールドに DN を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。

# AD の設定

## CC-SG への AD モジュールの追加

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。詳細は、「第 12 章 : 高度な設定」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**] メニューの [**セキュリティ**] をクリックします。[**一般**] タブを示す [**セキュリティ マネージャ**] 画面が表示されます。
2. [**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。

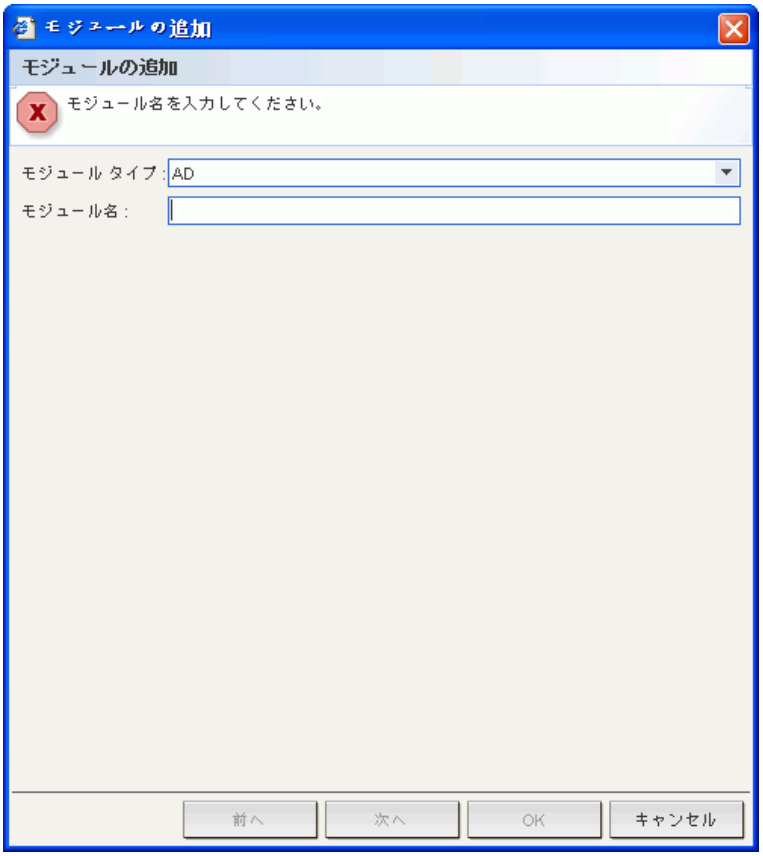


*図 94 モジュールの追加*

3. [**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。
4. [**モジュール名**] に AD サーバの名前を入力します。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。
5. [**次へ**] をクリックして続けます。[**一般**] タブが表示されます。

## AD の一般設定

[**一般**] タブでは、CC-SG が AD サーバを照会できるように情報を追加します。

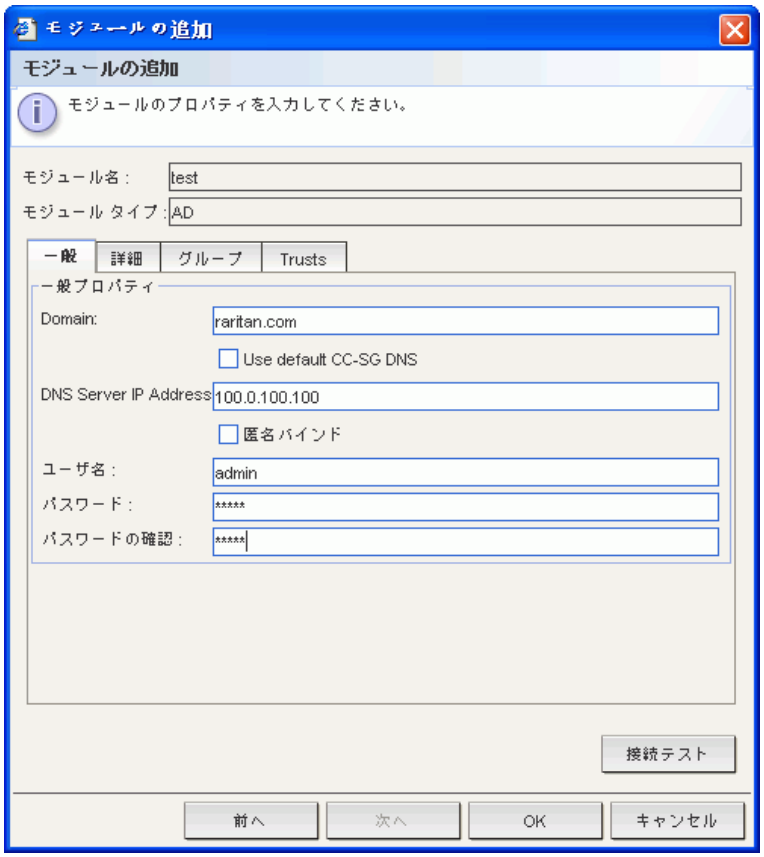


*図 95 AD の一般設定*

1. [**ドメイン**] フィールドに、照会する AD ドメインを入力します。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. [**DNS サーバ IP アドレス**] フィールドに DNS サーバの IP アドレスを入力します。または、[**Use default CC-SG DNS**](デフォルトの CC-SG DNS を使用) チェックボックスをオンにして、CC-SG の設定マネージャで設定されている DNS を使用します。詳細は、「**第 12 章 : 高度な設定**」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オンにします。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、[**ユーザ名**] フィールドに、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次の形式で入力します。**username@domain.com**。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ことが必要です。

5. [**パスワード**] および [**パスワードの確認**] フィールドに、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入力します。
6. [**接続テスト**] をクリックすると指定したパラメータで AD サーバへの接続をテストできます。接続に成功したことを示す確認メッセージが表示されるはずです。確認メッセージが表示されない場合は、設定に誤りがないか確認してやり直します。
7. [**次へ**] をクリックして続けます。[**詳細**] タブが表示されます。

## AD の詳細設定

1. 詳細設定を行うには、[**詳細**] タブをクリックします。

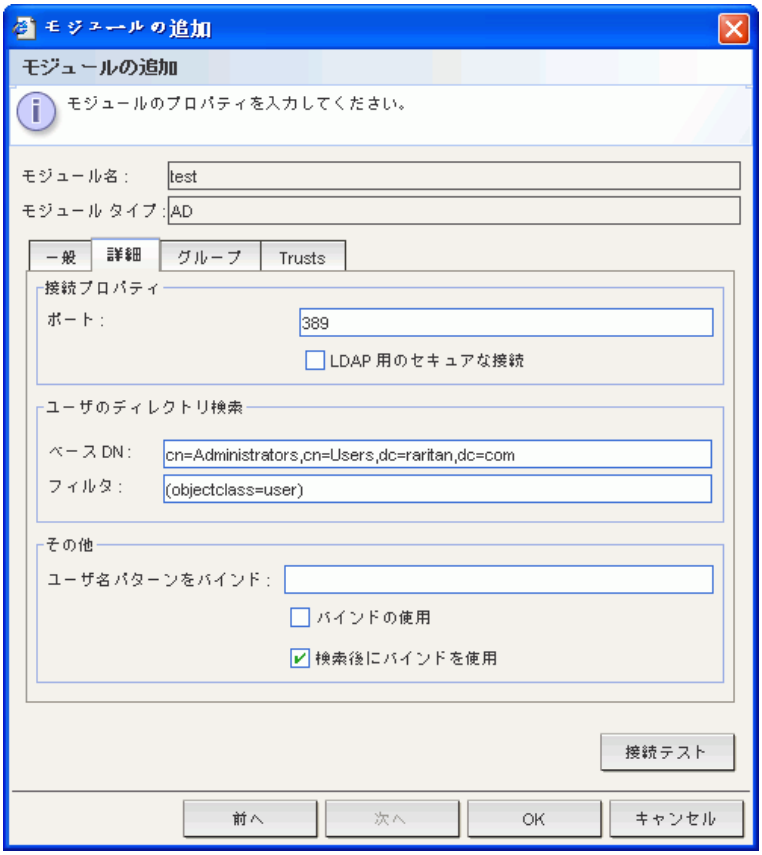


*図 96 AD の詳細設定*

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 (次の手順 3)、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オンにします。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 [**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**] 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。[**バインドの使用**] を選択した場合、CC-SG はアプレットで提供されるユーザ名とパスワードを使って AD ディレクトリに接続またはバインドを試みます。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。
   たとえば、「**cn={0},cn=Users,dc=raritan,dc=com**」のときアプレットで「**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。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のみ、[**バインドの使用**] を選択してください。
7. [**一般**] 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オンにします。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 番目の接続またはバインドが試行されます。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。
8. [**次へ**] をクリックして続けます。[**グループ**] タブが表示されます。

## 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。

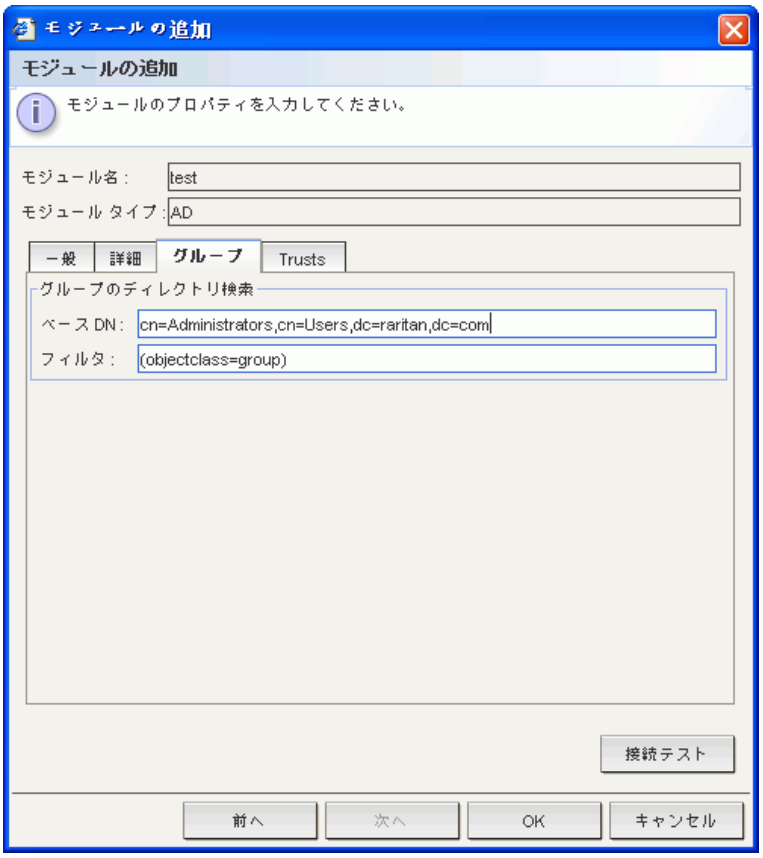


*図 97 AD のグループ設定*

2. 認証するユーザが含まれるグループが検索される [**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** | クルーフ内のユーサの検索照会はテ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** | クルーフ内のユーサの検索照会は Administrators サフティレクトリ (エントリ) に対してのみ実行されます。 |

3. [**フィルタ**] 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。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が **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。[Trusts](信頼) タブが表示されます。

## AD の信頼設定

[Trusts](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。

1. [**Trusts**](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、[Trusts](信頼) タブには、他のドメインもすべて表示されます。

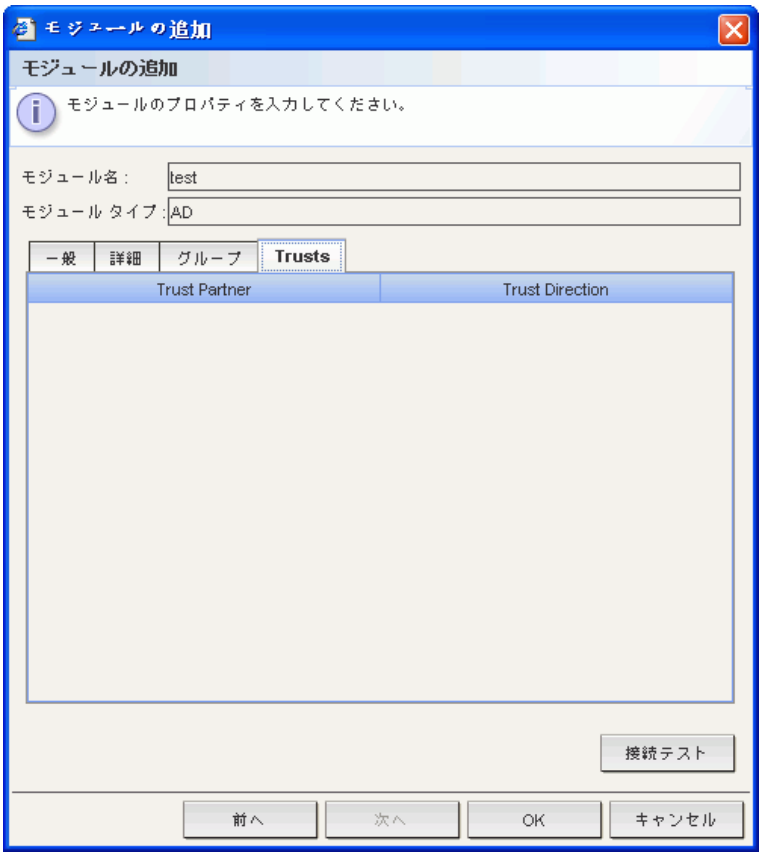


*図 98 AD の信頼設定*

2. [**Trust Partner**](信頼パートナー) 列の各ドメインで、[**Trust Direction**](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。上の図では、AD モジュール 2 は、AD モジュール 1 からの受信情報を信頼します。
   - **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。上の図では、AD モジュール 1 は、AD モジュール 2 からの受信情報を信頼します。
   - **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。

## 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。

1. [**管理**] メニューの [**セキュリティ**] をクリックします。
2. 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。
3. [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。詳細は、前述の「AD の一般設定」、「AD の詳細設定」、「AD のグループ設定」、「AD の信頼設定」を参照してください。
4. 接続情報を変更したら、[**接続テスト**] をクリックし、そのパラメータで 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。
5. [**OK**] をクリックして変更を保存します。変更した AD ユーザ グループを同期させる必要があります。すべてのモジュールですべてのグループとユーザを同期させ、すべての AD モジュールを同期させることもできます。詳細は、「AD ユーザ グループの同期」および「全 AD モジュールの同期」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。112 ページの「AD のグループ設定」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。詳細は、「AD ユーザ グループの同期」および「全 AD モジュールの同期」を参照してください。

***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。詳細は、「第 12 章 : 高度な設定」を参照してください。*

1. [**管理**] メニューの [**セキュリティ**] をクリックします。
2. AD ユーザ グループをインポートする元の AD モジュールを選択します。
3. [**グループのインポート**] 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。
4. CC-SG にインポートするグループの横のチェックボックスをオンにします。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。ユーザ グループを検索するには、[Search for User Group](ユーザ グループの検索) フィールドに検索文字列を入力し、[**実行**] をクリックします。[**すべて選択**] をクリックして、インポート用にすべてのユーザ グループを選択します。[**すべて選択解除**] をクリックして、ユーザ グループの選択をすべて解除します。
5. [**ポリシー**] 列で、フィールドをクリックし、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。これらのポリシーがすでに作成されているはずです。詳細は、「第 8 章 : ポリシー 」を参照してください。
6. [**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。
7. 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 グループの [**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 Associations**](Active Directory 関連) 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 ユーザ グループの同期

AD ユーザ グループを同期させると、CC-SG が、選択した AD モジュールのグループを取得し、その名前を AD からインポートされたユーザ グループの名前を比較して、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、インポートするユーザ グループを選択できます。これにより、CC-SG が最新の AD グループ情報をインポートできます。また、CC-SG は、1 日に 1 回、すべての AD モジュールを自動的に同期させます。詳細は、次の「**AD 同期時間の設定**」を参照してください。

1. [**管理**] メニューの [**セキュリティ**] をクリックします。

AD サーバと同期させるユーザ グループを持つ AD モジュールを選択します。

2. [**Synchronize AD User Groups**](AD ユーザ グループの同期) 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

すべての AD モジュールを同期させると、CC-SG が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、全モジュールのすべてのユーザ、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 自身のローカル キャッシュからそれらを削除します。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。

1. AD モジュールをすべて同期させる前に、メンテナンス モードを起動する必要があります。メンテナンス モードが起動されると、すべてのユーザが CC-SG からログオフされます。[**システム メンテナンス**] メニューで、[**メンテナンス モード**] -、[**メンテナンス モードの起動**] をクリックします。
2. [**メンテナンス モードの起動**] 画面で、CC-SG からログオフされるユーザに表示されるメッセージと CC-SG がメンテナンス モードを起動するまでの時間を分数で、それぞれ該当するフィールドに入力し、[**OK**] をクリックします。
3. 確認のダイアログ ボックスで [**OK**] をクリックします。
4. CC-SG のメンテナンス モードが起動されると、2 番目のメッセージが表示されます。[**OK**] をクリックします。
5. CC-SG のメンテナンス モードが起動されたら、[**管理**] メニューで [**セキュリティ**] をクリックします。
6. [**Synchronize all AD Modules**](全 AD モジュールの同期) 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。

7. メンテナンス モードを終了するには、[**システム メンテナンス**] メニューで、[**メンテナンス モード**] -、[**メンテナンス モードの終了**] をクリックします。
8. 表示される画面で、[**OK**] をクリックします。CC-SG のメンテナンス モードが終了されると、2 番目のメッセージが表示されます。[OK] をクリックします。

## AD 同期時間の設定

デフォルトで、CC-SG は、毎日 23:30 に、設定されている全 AD モジュールを同期させます。自動同期が行われる時間を変更できます。

1. [**管理**] メニューの [**セキュリティ**] をクリックします。
2. 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。
3. [**Update Synchronization Time**](同期時間の更新) をクリックして変更を保存します。

## AD の設定 - CC-SG 3.0.2 からのアップグレード

CC-SG を 3.0.2 から 3.1 にアップグレードした場合は、AD ユーザが CC-SG にログインする前に、AD モジュールを再設定する必要があります。CC-SG 3.1 では、各 AD モジュールで指定される DNS およびドメイン名が必要です。この設定により、CC-SG が、すべてのドメイン コントローラで特定のドメインを照会できるようになります。

**重要 : 3.1 にアップグレードすると、CC-SG は、メンテナンス モードが起動された状態になります。このため、この操作を実行するには、CC スーパーユーザ アカウントでログインする必要があります。3.0.2 からシステムをアップグレードするためのデフォルトの CC スーパーユーザ アカウントは、ccroot/raritan0 です。**

AD モジュールを再設定するには、以下の手順に従います。

1. [**管理**] メニューの [**セキュリティ**] をクリックします。
2. 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。
3. [**一般**] タブで、該当するフィールドに AD モジュールの DNS とドメイン名を入力します。詳細は、次の「AD の一般設定」を参照してください。
4. [**接続テスト**] をクリックすると指定したパラメータで AD サーバへの接続をテストできます。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。
5. [**OK**] をクリックして変更を保存します。
6. 詳細設定、グループ設定、信頼設定を構成するには、該当するタブをクリックして、オプションを表示します。詳細は、前述の「AD の詳細設定」、「AD のグループ設定」、「AD の信頼設定」を参照してください。[**OK**] をクリックして、これらのタブで加えた変更を保存します。
7. これらの手順を繰り返して、すべての AD モジュールを再設定します。
8. 全 AD モジュールを再設定したら、インポートした AD ユーザ グループと AD サーバを同期させることができます。詳細は、「AD ユーザ グループの同期」を参照してください。
9. 各モジュールの AD ユーザ グループを同期させたら、すべての AD モジュールを同期させてください。詳細は、「全 AD モジュールの同期」を参照してください。AD の設定により、同期プロセスには、ドメイン コントローラにつき最高 30 秒かかる場合があります。同期中にドメイン コントローラがオフラインになっていると、プロセスにはさらに時間がかかります。

***注 :*** *CC-SG 3.1 で、AD ユーザ グループの同期がどのように行われるかについては、「全 AD モジュールの同期」および「AD 同期時間の設定」を参照してください。AD ユーザ グループの情報についてのレポートを生成する方法については、「第 10 章 : レポートの生成 – AD ユーザ グループ レポート」を参照してください。*

## CC-SG への LDAP (Netscape) モジュールの追加

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。

1. [**管理**] メニューの [**セキュリティ**] をクリックします。[**一般**] タブを示す [**セキュリティ マネージャ**] 画面が表示されます。
2. [**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。

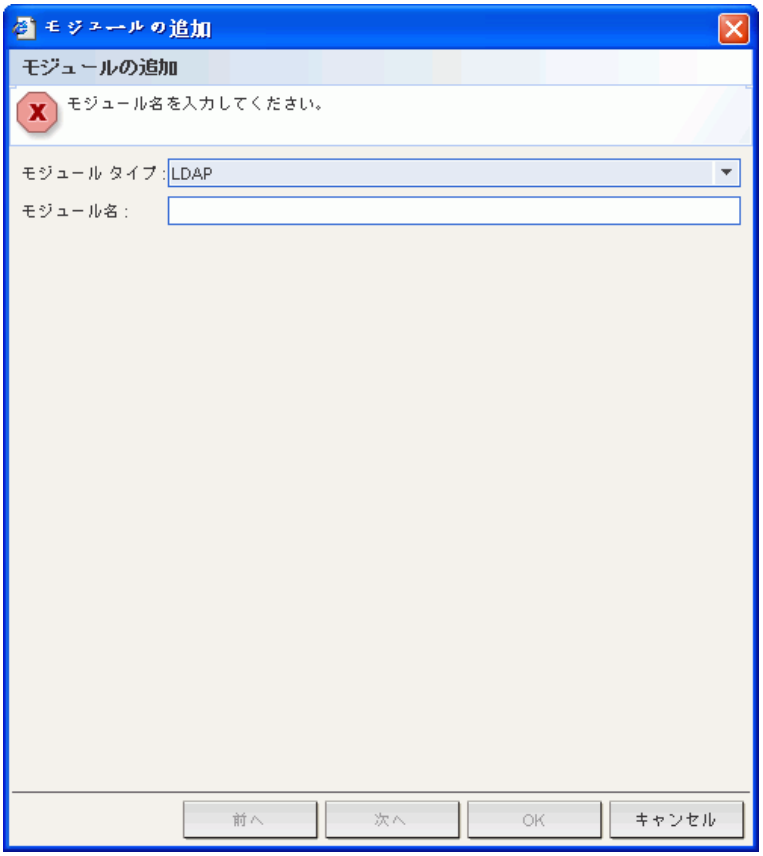


*図 99 LDAP モジュールの追加*

3. [**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。
4. [**モジュール名**] に LDAP サーバの名前を入力します。
5. [**次へ**] をクリックして続けます。[**一般**] タブが表示されます。

## LDAP の一般設定

1. [**一般**] タブをクリックします。

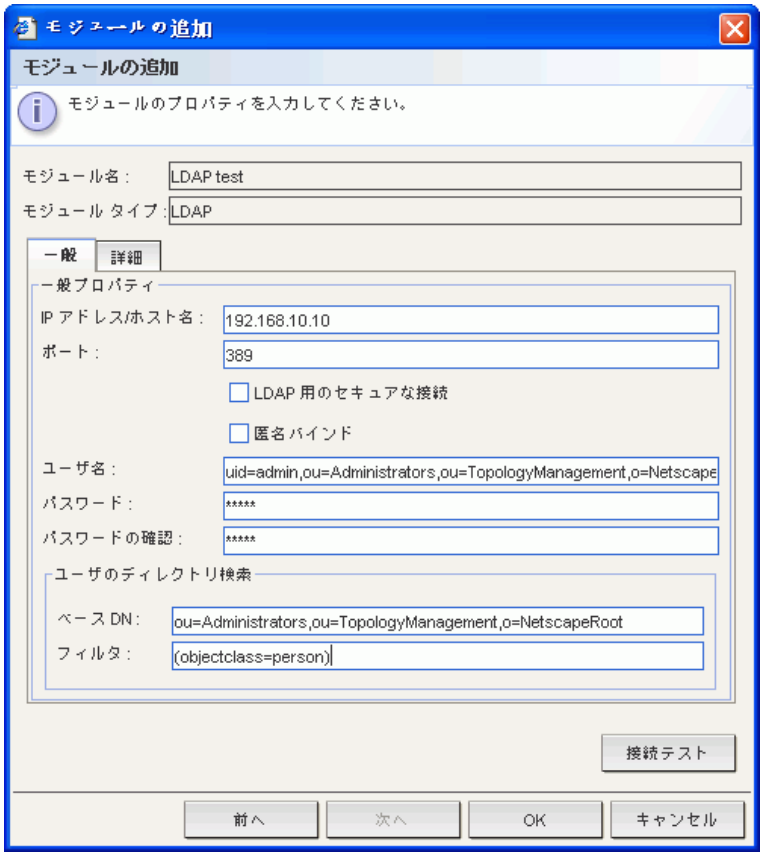


*図 100 LDAP の一般設定*

2. [**IP アドレス/ホスト名**] フィールドに LDAP サーバの IP アドレスとホスト名を入力します。ホスト名の規則については、「**第 1 章 : はじめに**」の「**用語/略語**」を参照してください。
3. [**ポート**] フィールドにポート値を入力します。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 用のセキュアな接続**] 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**] チェックボックスをオンにします。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は [**ユーザ名**] フィールドにユーザ名を入力します。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、値そのものにはスペースを使用できます。
7. [**パスワード**] と [**パスワードの確認**] フィールドにパスワードを入力します。
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。

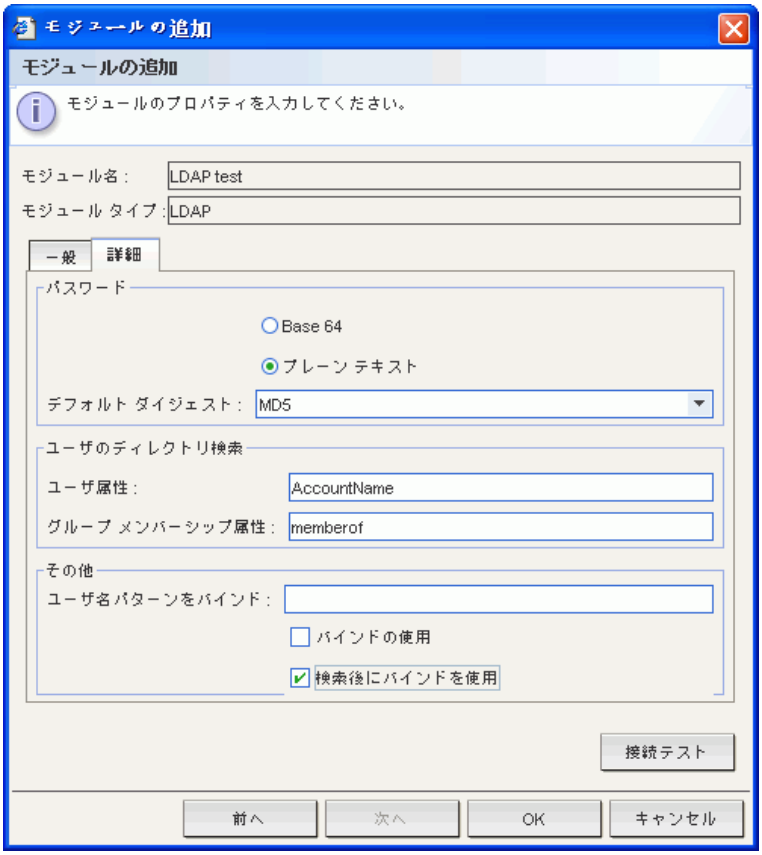


*図 101 LDAP の詳細設定*

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**] のラジオ ボタンをクリックします。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**] のラジオ ボタンをクリックします。
3. [**デフォルト ダイジェスト**] ドロップダウン メニューをクリックし、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**] および [**グループ メンバーシップ属性**] フィールドに、ユーザ属性とグループ メンバーシップ属性パラメータを入力します。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. [**ユーザ名パターンをバインド**] フィールドに、バインド パターンを入力します。
6. 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**] チェックボックスをオンにします。[**バインドの使用**] のチェックボックス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。

7. 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**] のチェックボックスをオンにして、CC-SG がパスワードを 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指示します。
8. [**OK**] 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、パラメータ設定は次の例に従います。

| パラメータ名 | SUN ONE LDAP パラメータ |
|---|---|
| **IP アドレス/ホスト名** | **<Directory Server IP Address>** |
| **ユーザ名** | **CN=<Valid user id>** |
| **パスワード** | ***<Password>*** |
| **ベース DN** | **O=<Organization>** |
| **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** | **<Directory Server IP Address>** |
| **ユーザ名** | **CN=<Valid user id>, O=<Organization>** |
| **パスワード** | **<Password>** |
| **ユーザ ベース** | **O=accounts, O=<Organization>** |
| **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** |

## LDAP の証明書設定

LDAP Certificate settings allow you to upload an LDAP certificate.また、アップロードされた証明書を受け入れたり、拒否したりすることができます。

1. [**詳細**] タブをクリックします。
2. [**参照**] をクリックして、アップロードする証明書を見つけ、[**開く**] をクリックします。
3. [**同意**] をクリックして、CC-SG によって信頼されているものとして証明書を受け入れます。[**拒否**] をクリックして、証明書を削除します。
4. 証明書を削除する場合は、証明書を選択して、[**削除**] をクリックします。
5. [**OK**] をクリックして変更を保存します。

## TACACS+ モジュールの追加

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。リモート認証を使用するユーザの追加についての詳細は、「**第 7 章 : ユーザとユーザ グループの追加および管理**」を参照してください。

1. [**管理**] メニューの [**セキュリティ**] をクリックします。[**一般**] タブを示す [**セキュリティ マネージャ**] 画面が表示されます。
2. [**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。

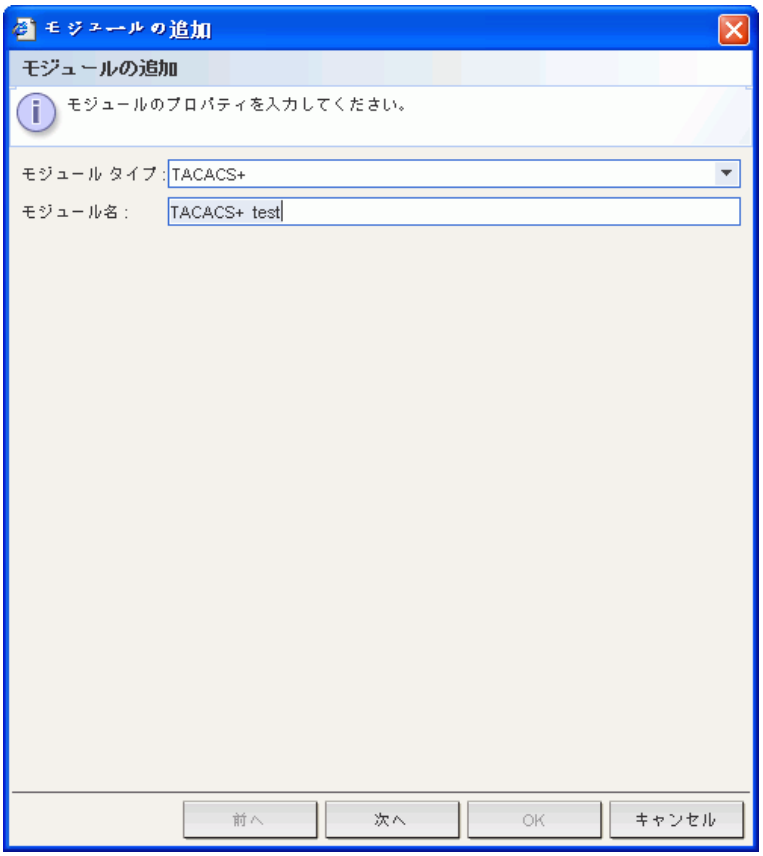


*図 102 TACACS+ モジュールの追加*

3. [**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 TACACS+ を選択します。
4. [**モジュール名**] に TACACS+ サーバの名前を入力します。
5. [**次へ**] をクリックして続けます。[**一般**] タブが表示されます。

## TACACS+ の一般設定

1. [**IP アドレス/ホスト名**] フィールドに TACACS+ サーバの IP アドレスまたはホスト名を入力します。ホスト名の規則については、「**第 1 章 : はじめに**」の「**用語/略語**」を参照してください。

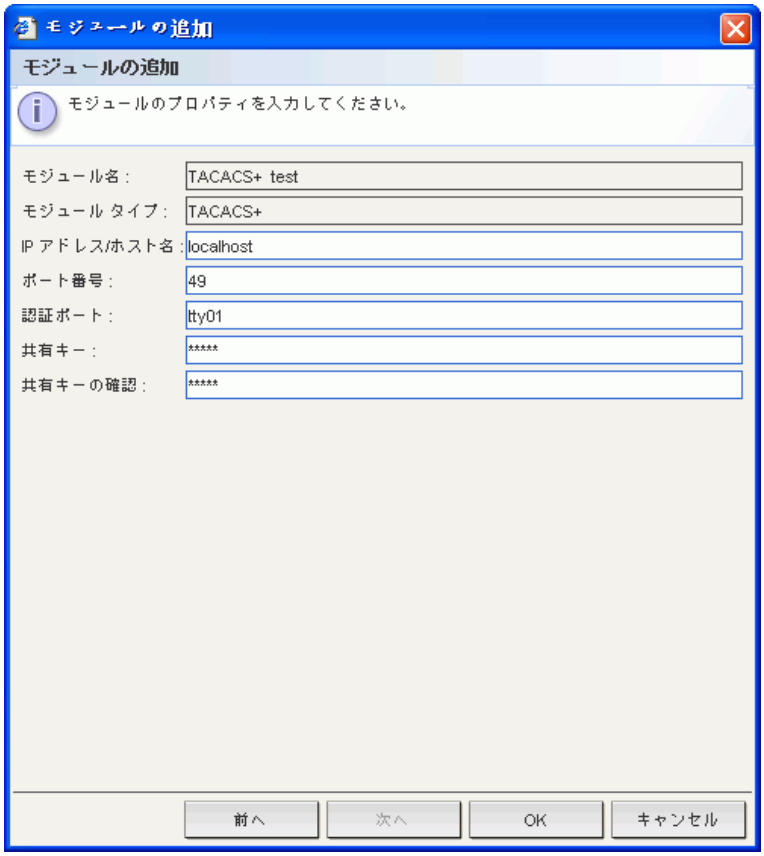


*図 103 TACACS+ の一般設定*

2. [**ポート番号**] フィールドに、TACACS+ 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番号は **49** です。
3. [**認証ポート**] フィールドに認証ポートのタイプを入力します。
4. [**共有キー**] と [**共有キーの確認**] フィールドに共有キーを入力します。
5. [**OK**] をクリックして変更を保存します。

## RADIUS モジュールの追加

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。リモート認証を使用するユーザの追加についての詳細は、「**第 7 章 : ユーザとユーザ グループの追加および管理**」を参照してください。

1. [**管理**] メニューの [**セキュリティ**] をクリックします。[**一般**] タブを示す [**セキュリティ マネージャ**] 画面が表示されます。
2. [**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。

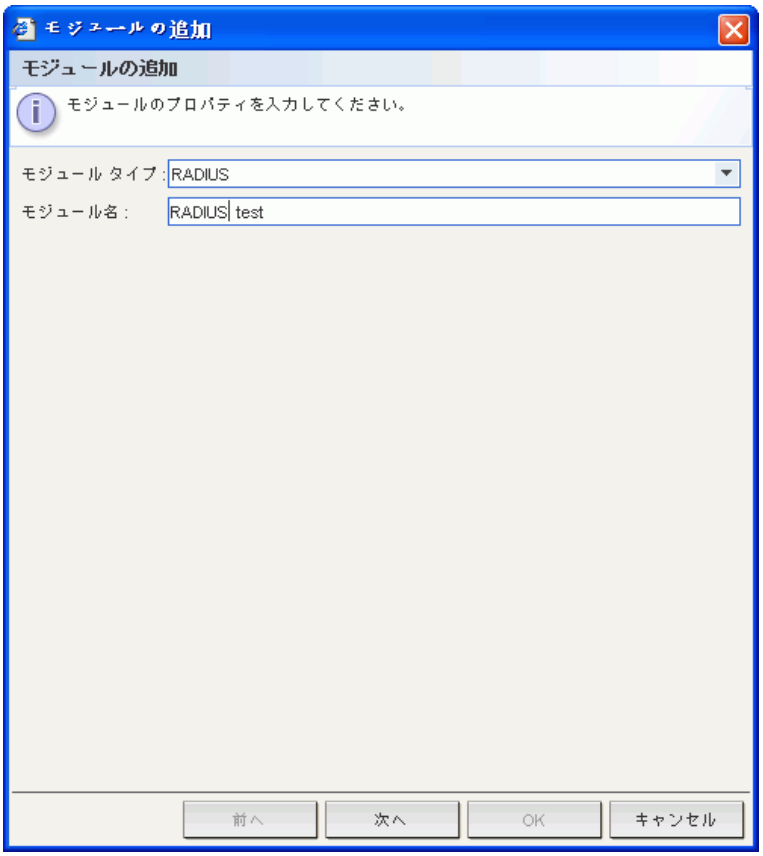


*図 104 セキュリティ マネージャのモジュールの追加画面*

3. [**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。
4. [**モジュール名**] に RADIUS サーバの名前を入力します。
5. [**次へ**] をクリックして続けます。[**一般**] タブが表示されます。

## RADIUS の一般設定

1. [**一般**] タブをクリックします。

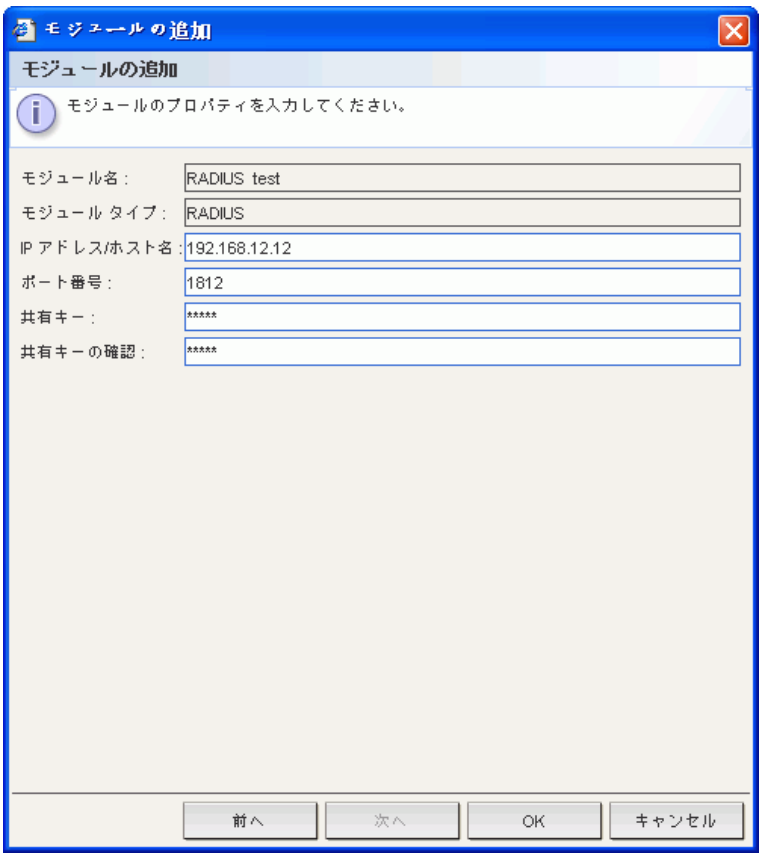


*図 105 RADIUS サーバの指定*

2. [**IP アドレス/ホスト名**] フィールドに RADIUS サーバの IP アドレスまたはホスト名を入力します。ホスト名の規則については、「**第 1 章 : はじめに**」の「**用語/略語**」を参照してください。
3. [**ポート番号**] フィールドにポートの番号を入力します。デフォルトのポート番号は 1812 です。
4. [**認証ポート**] フィールドに認証ポートのタイプを入力します。
5. [**共有キー**] と [**共有キーの確認**] フィールドに共有キーを入力します。
6. [**OK**] 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。

このような環境では、まず、ユーザが [**ユーザ名**] フィールドに自分のユーザ名を入力して、CC-GS にログインします。次に、ユーザが、[**パスワード**] フィールドに固定パスワードと、動的トークンを入力します。

RADIUS サーバ設定と認証サーバを有効にする方法は、本書では説明していません。CC-SG の設定は、前述の標準 RADIUS リモート認証と同じです。RADIUS サーバを指すように、CC-SG を設定する必要があります。詳細は、「付録 **G : 2 ファクタ認証**」を参照してください。

## 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、認証、承認、または両方のいずれを使用するかを指定します。

1. [**管理**] メニューの [**セキュリティ**] をクリックします。[**セキュリティ マネージャ**] 画面が表示されたら、[**一般**] タブをクリックします。設定したすべての外部認証および承認サーバが、[**外部 AA サーバ**] に表示されます。
2. 各サーバで、CC-SG でユーザの認証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。
3. 各サーバで、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

[一般] タブでは、CC-SG が設定されている外部 AA サーバを照会する順番を設定できます。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。

1. [**管理**] メニューの [**セキュリティ**] をクリックします。[**セキュリティ マネージャ**] 画面が表示されたら、[**一般**] タブをクリックします。

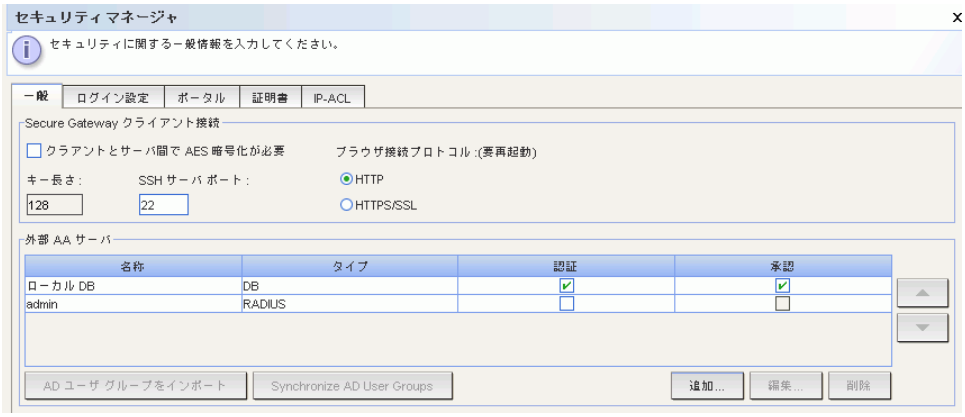


*図 106 セキュリティ マネージャの一般タブ*

2. [**外部 AA サーバ**] には、CC-SG で利用可能な認証および承認オプションがすべて表示されます。リストから名前を選択し、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。
3. [**更新**] をクリックして変更を保存します。

# 第 10 章 : レポートの生成

列のヘッダをクリックすると、レポートをソートできます。 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。

列の幅は、すべてのレポートにおいて変更できます。 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。 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。

使用するソート値と列幅は、次回にログインし CC-SG 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。すべてのレポートで、行をダブルクリックするとそのレポートの詳細を表示できます。

---

***注 :*** *すべてのレポートで、CTRL キーを押したままクリックすると、ハイライト表示されている列が選択解除されます。*

---

## 監査証跡レポート

**監査証跡**レポートには、CC-SG の監査ログとアクセスが表示されます。このレポートには、デバイスやポートの追加、編集、削除、その他の変更が取り込まれます。

CC-SG では、次のイベントの監査証跡が保持されます。

- CC-SG の起動
- CC-SG の停止
- CC-SG へのユーザ ログオン
- CC-SG からのユーザ ログオフ
- ユーザによるノード接続の開始

1. [**レポート**] メニューの [**監査証跡**] をクリックします。[**監査証跡**] 画面が表示されます。

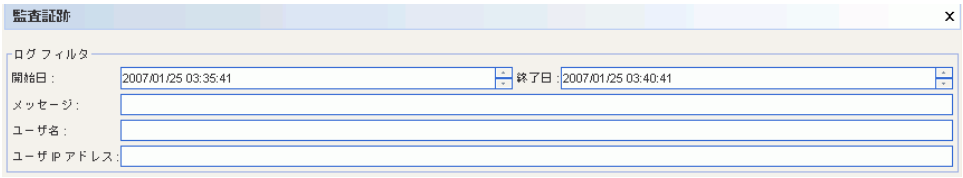


*図 107 監査証跡画面*

2. [**開始日**] フィールドと [**終了日**] フィールドでレポートの期間を設定します。 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。

- レポートの内容をアクティビティに関連したメッセージ テキストで制限する場合、そのテキストを [**メッセージ**] フィールドに入力します。
- レポートの内容を特定のユーザ アクティビティに制限する場合、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。
- レポートの内容を特定の IP アドレスのアクティビティに制限する場合、該当するユーザの 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. [**OK**] をクリックして、レポートを実行します。レポートが生成,され、追加パラメータに一致する指定された時間に発生したアクティビティのデータが表示されます。

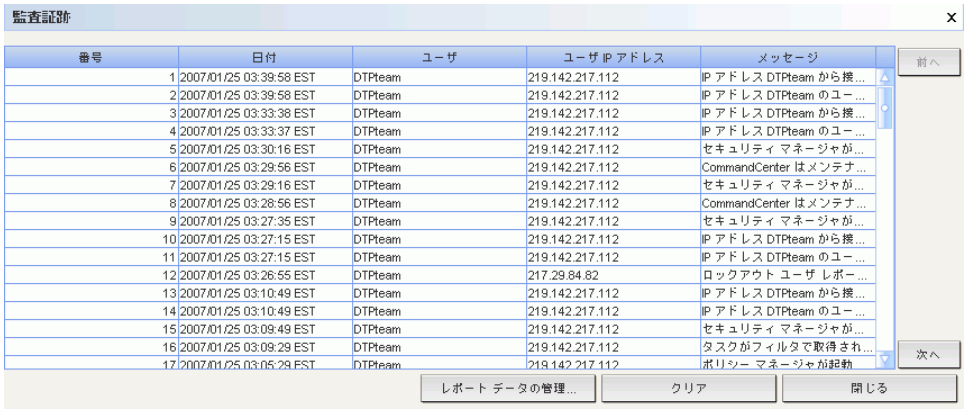


*図 108 監査証跡レポート*

- レポートのページを前後に移動するには、[**次へ**] または [**前へ**] をクリックします。
- レポートを保存または印刷するには、[**レポート データの管理**] をクリックします。 現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。 現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- レポートで使用されたログ ファイルをクリアするには、[**クリア**] をクリックします。
- レポートを閉じるには、[**閉じる**] をクリックします。

## 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。

1. [**レポート**] メニューの [**エラー ログ**] をクリックします。[**エラー ログ**] 画面が表示されます。

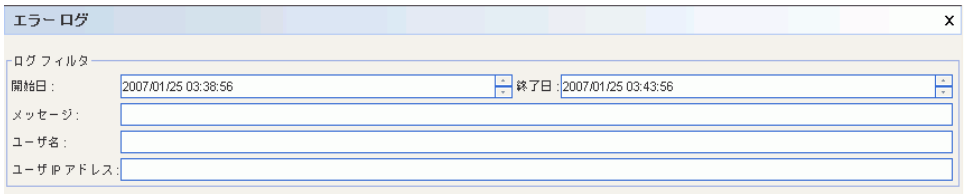


*図 109 エラー ログ画面*

2. [**開始日**] フィールドと [**終了日**] フィールドでレポートの期間を設定します。 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。

- レポートの内容をアクティビティに関連したメッセージ テキストで制限する場合、そのテキストを [**メッセージ**] フィールドに入力します。
- レポートの内容を特定のユーザ アクティビティに制限する場合、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。
- レポートの内容を特定の IP アドレスのアクティビティに制限する場合、該当するユーザの 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. [**OK**] をクリックして、レポートを実行します。レポートが生成,され、追加パラメータに一致する指定された時間に発生したアクティビティのデータが表示されます。

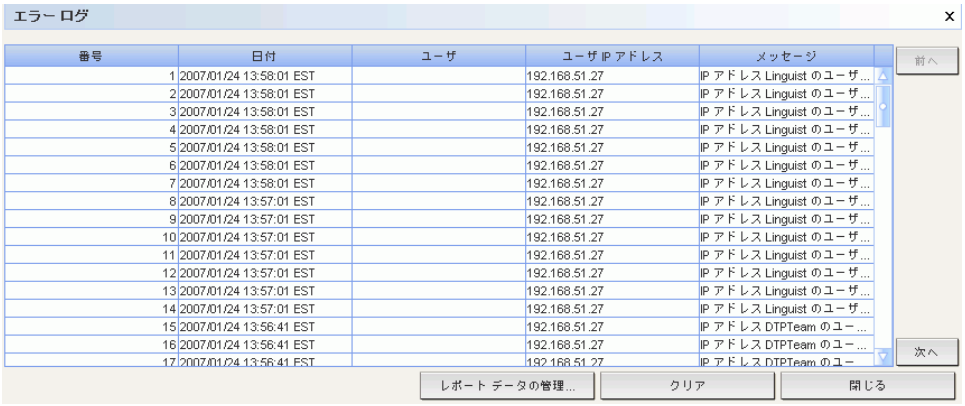


*図 110 エラー ログ レポート*

- レポートのページを前後に移動するには、[**次へ**] または [**前へ**] をクリックします。
- レポートを保存または印刷するには、[**レポート データの管理**] をクリックします。 現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。 現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- レポートで使用されたログ ファイルをクリアするには、[**クリア**] をクリックします。
- レポートを閉じるには、[**閉じる**] をクリックします。

## アクセス レポート

アクセス レポートを実行すると、アクセスされたデバイスとポート、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。

1. [**レポート**] メニューで、**[アクセス レポート]** をクリックします。[**アクセス レポート**] 画面が表示されます。

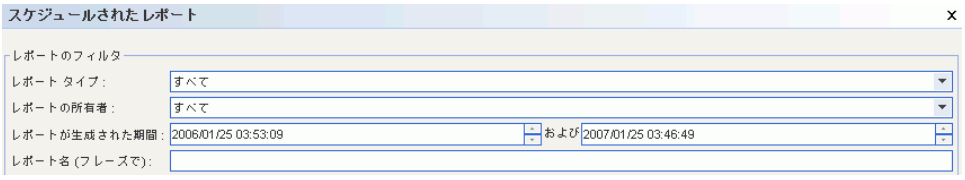


*図 111 アクセス レポート画面*

2. [**開始日**] フィールドと [**終了日**] フィールドでレポートの期間を設定します。 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**]、[**デバイス名**]、[**ポート名**] 、[**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。

- レポートの内容をアクティビティに関連したメッセージ テキストで制限する場合、そのテキストを [**メッセージ**] フィールドに入力します。
- レポートの内容を特定のデバイスに制限する場合は、そのデバイス名を [**デバイス名**] フィールドに入力します。
- レポートの内容を特定のポートに制限する場合は、そのポート名を [**ポート名**] フィールドに入力します。
- レポートの内容を特定のユーザ アクティビティに制限する場合、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。
- レポートの内容を特定の IP アドレスのアクティビティに制限する場合、該当するユーザの 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. [**OK**] をクリックして、レポートを実行します。レポートが生成,され、追加パラメータに一致する指定された時間に発生したアクセスのデータが表示されます。

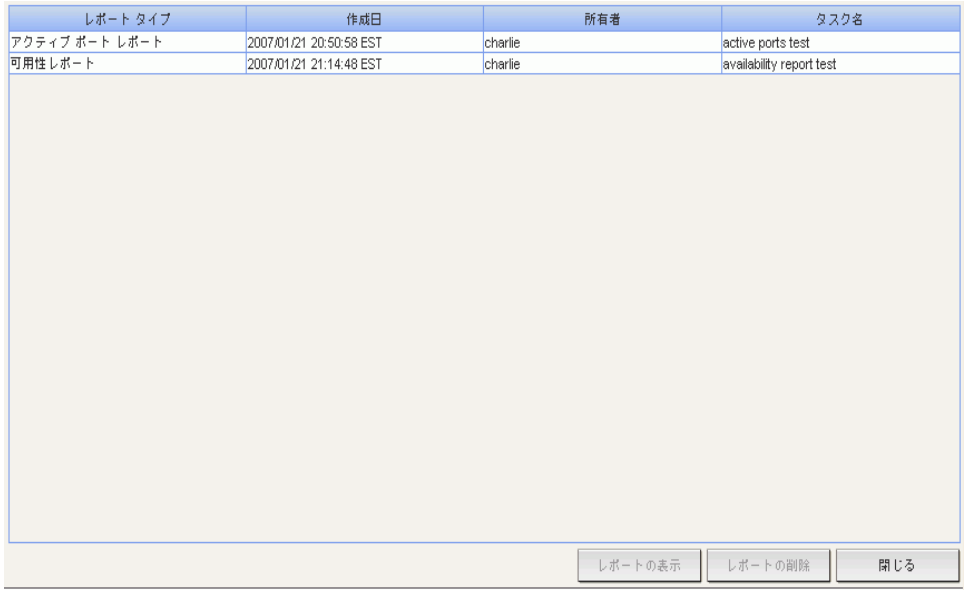


*図 112 アクセス レポート*

- レポートのページを前後に移動するには、[**次へ**] または [**前へ**] をクリックします。
- レポートを保存または印刷するには、[**レポート データの管理**] をクリックします。 現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。 現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- レポートで使用されたログ ファイルをクリアするには、[**クリア**] をクリックします。
- レポートを閉じるには、[**閉じる**] をクリックします。

# 可用性レポート

可用性レポートには、すべての接続のステータスがデバイスの名前と IP アドレス別に表示されます。このレポートには、システム上に存在するすべてのデバイスのアクセス可能性が詳細に表示され、トラブルシューティングの際に役立つ情報が得られます。

1. [**レポート**] メニューで、[**可用性レポート**] をクリックします。[**可用性レポート**] が生成されます。

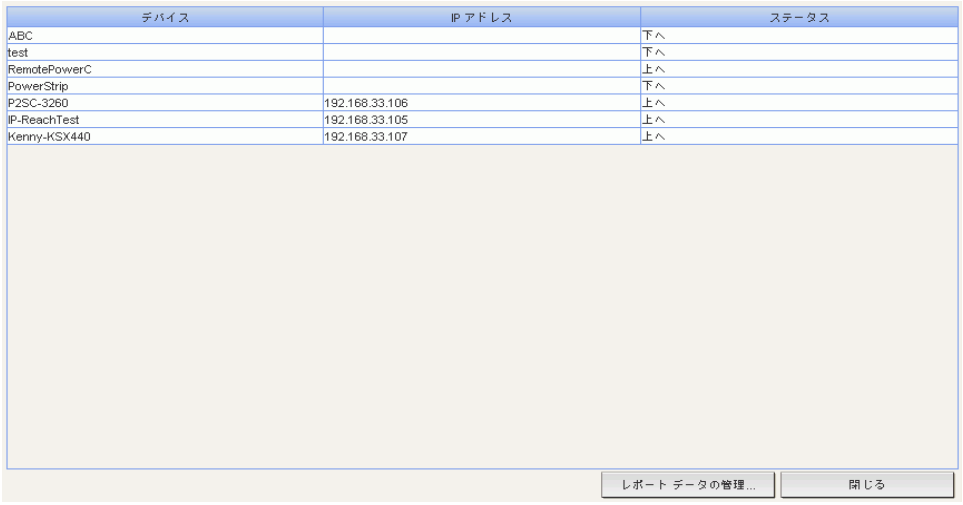


*図 113 可用性レポート*

- レポートを保存または印刷するには、[**レポート データの管理**] をクリックします。現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。 現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- レポートを閉じるには、[**閉じる**] 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。

1. [**レポート**] メニューで、[**ユーザ**] をクリックして、[**アクティブ ユーザ**] をクリックします。 [**アクティブ ユーザ**] レポートが生成されます。

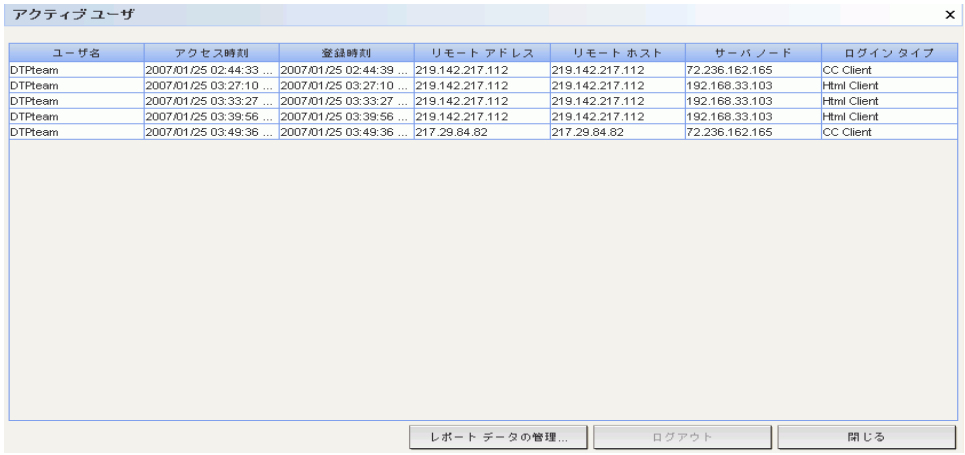


*図 114 アクティブ ユーザ レポート*

- CC-SG でユーザーのアクティブ セッションを切断するには、そのユーザのユーザ名を選択して、[**ログアウト**] をクリックします。
- レポートを保存または印刷するには、[**レポート データの管理**] をクリックします。 現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。 現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- レポートを閉じるには、[**閉じる**] 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。 ロックアウト設定についての詳細は、「**第 12 章 : 高度な管理、ロックアウト設定**」を参照してください。

[レポート] メニューで、[ユーザ] をクリックし、次に [ロックアウト ユーザ] をクリックします。

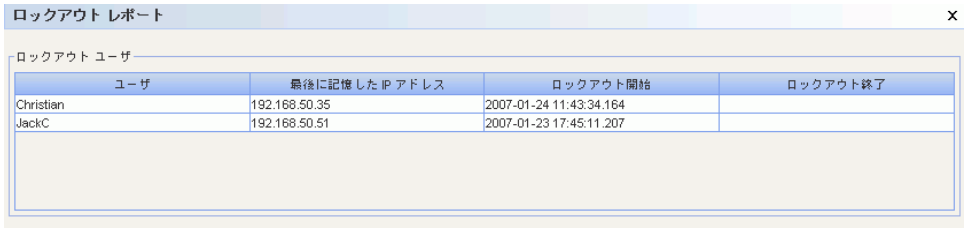


*図 115 ロックアウト ユーザ レポート*

- 現在 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、アンロックするユーザのユーザ名を選択して、[**ユーザのアンロック**] をクリックします。**An**
- レポートを閉じるには、[**キャンセル**] をクリックします。

# 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。

1. [**レポート**] メニューで、[**ユーザ**] をクリックし、[**ユーザ データ**] をクリックします。[**すべてのユーザのデータ**] レポートが生成されます。


*図 116 すべてのユーザのデータ レポート*

- [**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。
- [**電話**] フィールドには、ユーザのダイヤル バック電話番号が表示されます。このフィールドは、モデム内蔵の CC-SG G1 システムのユーザのみに適用されます。
- [**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**] チェック ボックスがオンになっているかどうかによります。詳細は、「**第 7 章 : ユーザとユーザ グループの追加と管理 - ユーザの追加**」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。 詳細は、「**第 7 章 : ユーザとユーザ グループの追加と管理 - ユーザの追加**」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。 詳細は、「**付録 A : 仕様 (G1、V1、および E1)**」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。
- レポートを保存または印刷するには、[**レポート データの管理**] をクリックします。 現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。 現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- レポートを閉じるには、[**閉じる**] をクリックします。

# グループ内のユーザ レポート

グループ内のユーザ 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。

1. [レポート] メニューで、[ユーザ] をクリックして、[グループ内のユーザ] をクリックします。[**グループ内のユーザ**] レポートが生成されます。

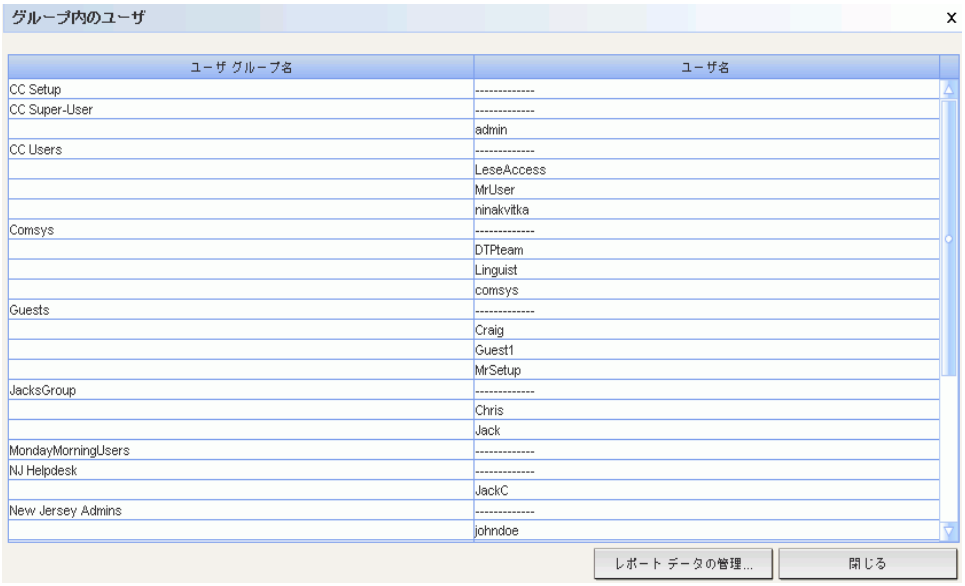


*図 117 グループ内のユーザ レポート*

- レポートを保存または印刷するには、[**レポート データの管理**] をクリックします。現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。 現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- レポートを閉じるには、[**閉じる**] をクリックします。

## グループ データ レポート

[**グループ データ**] レポートには、ユーザ グループ、ノード グループ、およびデバイス グループに関する情報が表示されます。ユーザ グループの名前と説明、ノード グループの名前、デバイス グループの名前がすべて 1 つの画面に表示されます。

1. [**レポート**] メニューで、[**ユーザ**] をクリックし、次に [**グループ データ**] をクリックします。[**グループ**] レポートが生成されます。

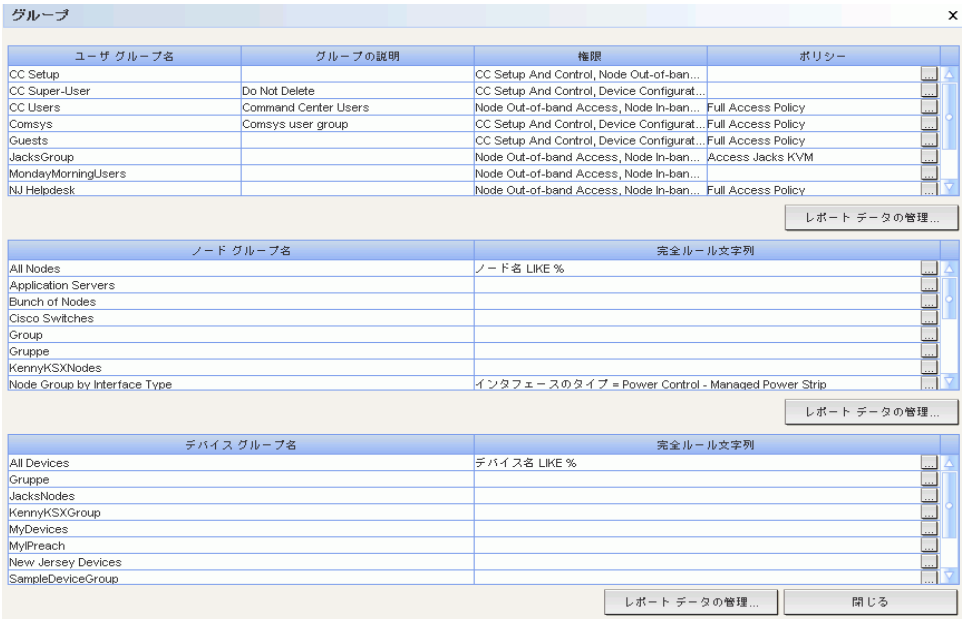


*図 118 グループ レポート*

- レポート セクションを保存または印刷するには、[**レポート データの管理**] をクリックします。現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- レポートを閉じるには、[**閉じる**] をクリックします。
- 行の隣の [...] ボタンをクリックすると、そのユーザ グループに関連付けられているポリシー、ノード グループ ルールに一致するノードのリスト、またはデバイス グループ ルールに一致するデバイスのリストが表示されます。

## 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 Active Directory 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。

1. [**レポート**] メニューで、[**ユーザ**] をクリックし、次に [**AD ユーザ グループ レポート**] をクリックします。[**AD ユーザ グループ レポート**] 画面が表示されます。
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。CC-SG でレポートに含める各 AD サーバのチェックボックスをオンにします。
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**] リストに移動します。

4. [**適用**] をクリックします。[**AD ユーザ グループ**] レポートが生成されます。

- レポート セクションを保存または印刷するには、[**レポート データの管理**] をクリックします。 現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。 現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- レポートを閉じるには、[**閉じる**] をクリックします。

## 資産管理レポート

資産管理レポートには、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。

1. [**レポート**] メニューで、[**デバイス**] をクリックし、次に [**資産管理レポート**] をクリックします。 すべてのデバイスに関する [**資産管理**] レポートが生成されます。
2. デバイス タイプでレポート データをフィルタする場合、[**デバイス タイプ**] ドロップダウン矢印をクリックして、リストからデバイス タイプを選択し、[**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。

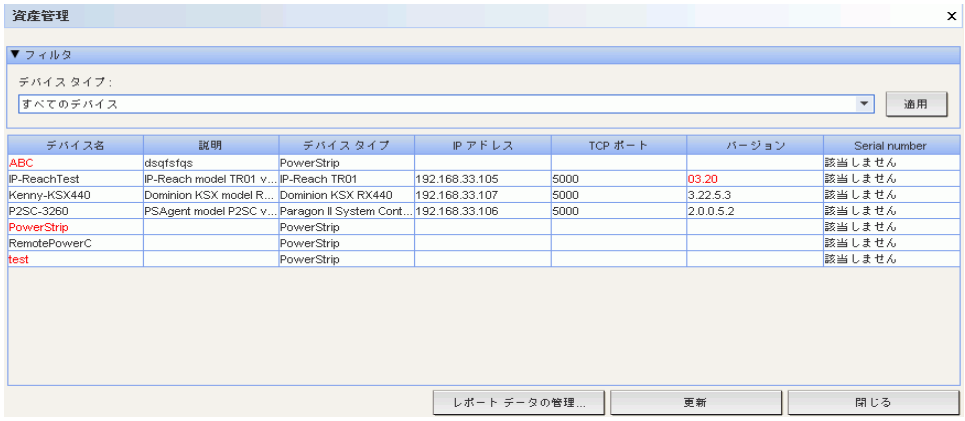


*図 119 資産管理レポート*

- 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。
- レポート セクションを保存または印刷するには、[**レポート データの管理**] をクリックします。 現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。 現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- 新しいレポートを生成するには、**[更新]** をクリックします。 システム設定のサイズによっては、レポートの生成に数分かかることがあります。
- レポートを閉じるには、[**閉じる**] をクリックします。

## 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。

1. [**レポート**] メニューで、[**ノード**] をクリックし、次に [**ノード資産レポート**] をクリックします。[**ノード資産レポート**] 画面が表示されます。

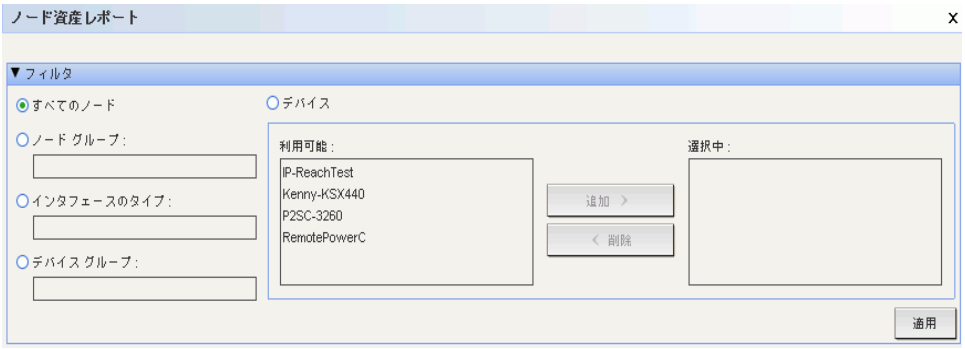


*図 120 ノード資産レポート画面*

2. レポートに適用するフィルタ条件に対応するラジオ ボタン ([**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**]) をクリックします。
   - [**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**] を選択した場合、対応するドロップダウン矢印をクリックして、リストからパラメータを選択します。
   - [**デバイス**] を選択した場合、[**利用可能**] リストで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。

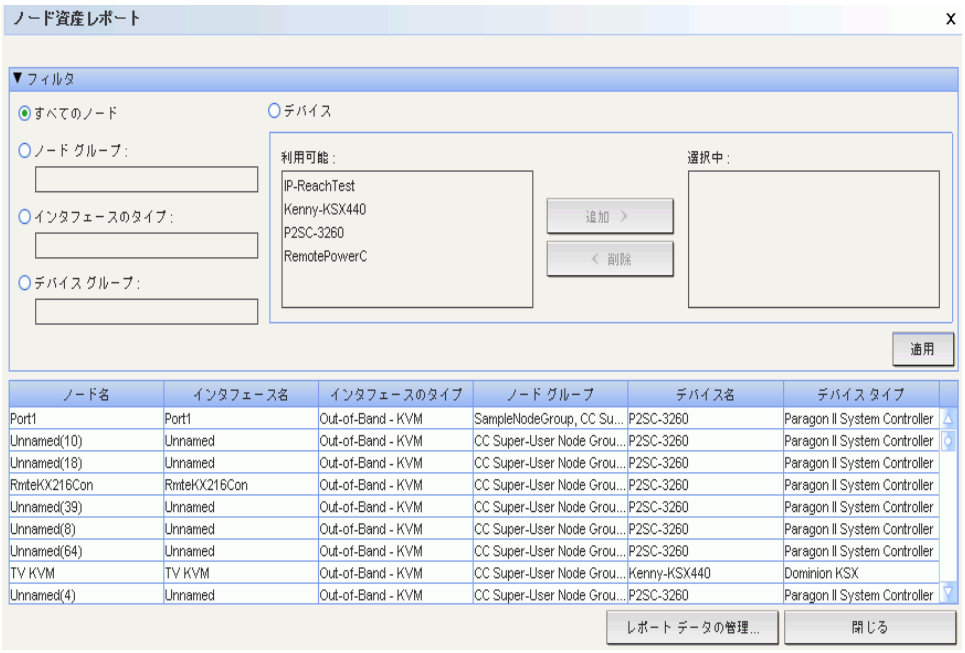


*図 121 ノード資産レポート*

- レポートを保存または印刷するには、[**レポート データの管理**] をクリックします。現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。 現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- レポートを閉じるには、[**閉じる**] をクリックします。

## 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、現在のユーザ、タイムスタンプ、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。

1. [**レポート**] メニューで、[**ノード**] をクリックし、次に [**アクティブ ノード**] をクリックします。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。

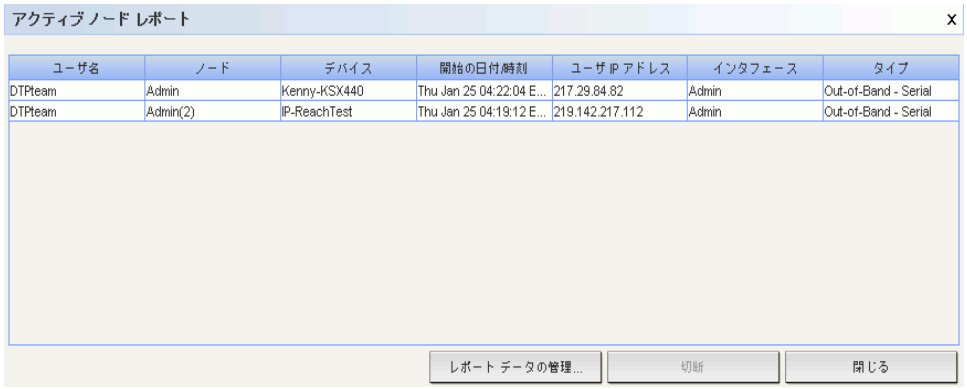


*図 122 アクティブ ノード レポート*

- 現在のセッションからノードを切断するには、切断するノードを選択し、[**切断**] をクリックします。
- レポートを保存または印刷するには、[**レポート データの管理**] をクリックします。現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- レポートを閉じるには、[**閉じる**] 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。

1. [**レポート**] メニューで、[**ノード**] をクリックし、[**ノードの作成**] をクリックします。[**ノードの作成レポート**] 画面が表示されます。

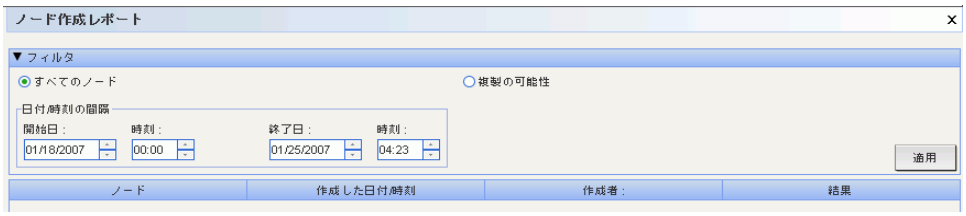


*図 123 ノード作成レポート画面*

2. [**開始日**] フィールドと [**終了日**] フィールドでレポートの期間を設定します。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. 複製の可能性フラグが設定されたノードのみにレポートの内容を制限するには、[**複製の可能性のみ**] チェックボックスをオンにします。
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。

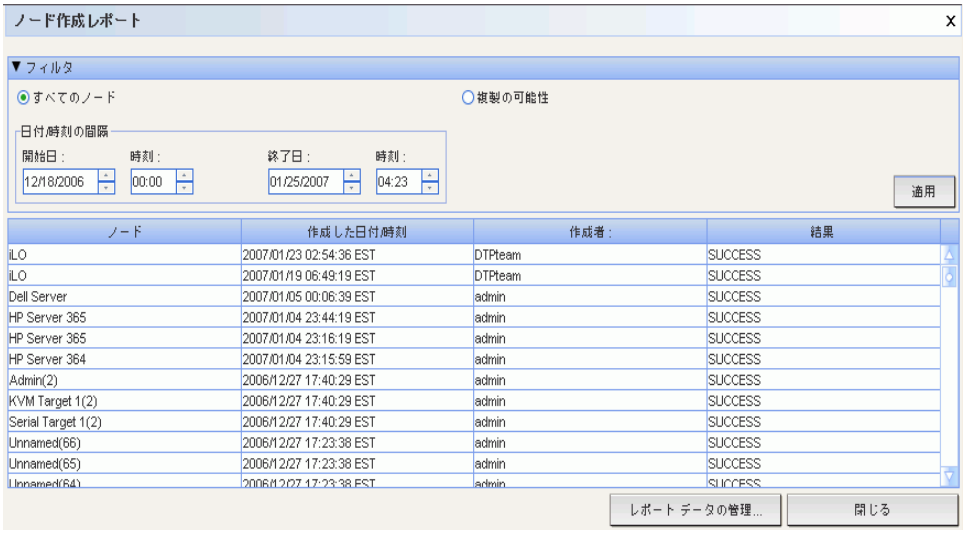


*図 124 ノードの作成レポート*

- [**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。
- レポート セクションを保存または印刷するには、[**レポート データの管理**] をクリックします。 現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。 現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- レポートを閉じるには、[**閉じる**] をクリックします。

## 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。

1. [**レポート**] メニューで、[**ポート**] をクリックして、[**ポートの照会**] をクリックします。

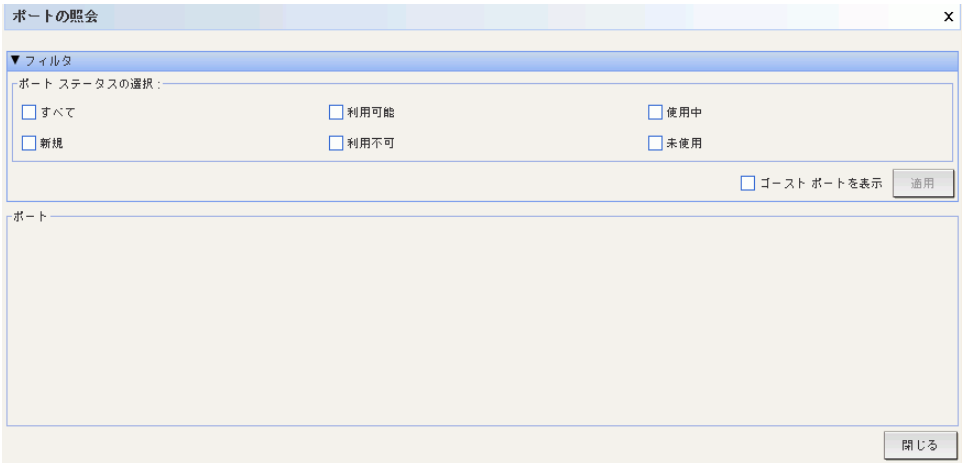


*図 125 ポートの照会画面*

2. [**ポート ステータスの選択**] セクションで、レポートに表示するポート ステータスに対応するチェックボックスをオンにします。 複数のチェックボックスをオンにして [**適用**] をクリックすると、選択したステータスすべてに該当するポートが表示されます。

| ポート ステータス | 定義 |
|---|---|
| すべて | すべてのポート ステータス |
| 新規 | 9. ポートは利用可能 (ターゲット サーバに物理的に接続済み) ですがまだ設定されていません。 |
| 未使用 | ポートは利用可能ではなく (ターゲット サーバに物理的に接続されていない)、まだ設定されていません。 |
| 利用可能 | ポートは設定済みでポートへの接続が可能な状態です。 |
| 使用不可 | 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。 |
| 使用中 | ユーザがこのポートに接続しています。 |

3. 1 つまたは複数のポート ステータスと組み合わせて [**ゴースト ポートを表示**] チェックボックスをオンにすると、ゴースト ポートであり、かつ選択されたポート ステータスに該当するポートが表示されます。 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。 詳細は、Raritan の『Paragon II ユーザ マニュアル』を参照してください。
4. [**適用**] をクリックしてレポートを生成します。

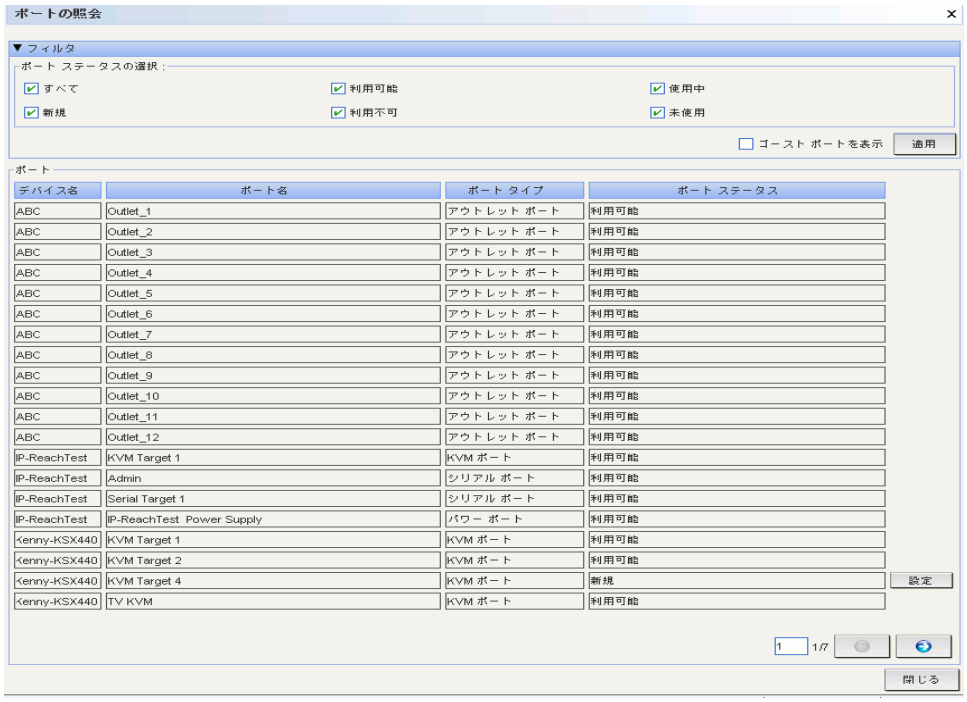


*図 126 ポートの照会レポート*

- レポートの右下にある矢印アイコンをクリックすると、複数のページ間で移動できます。
- ポートを設定するには、新規または未使用ポートの横の [**設定**] をクリックします。
- レポートを閉じるには、[**閉じる**] をクリックします。

## アクティブ ポート レポート

**アクティブ ポート** レポートには、現在使用中のアウト オブ バンド ポートが表示されます。このレポートからアクティブ ポート リストを表示したり、ポートを切断したりできます。

1. [**レポート**] メニューで、[**ポート**] をクリックし、次に [**アクティブ ポート**] をクリックします。[**アクティブ ポート**] レポートが生成されます。

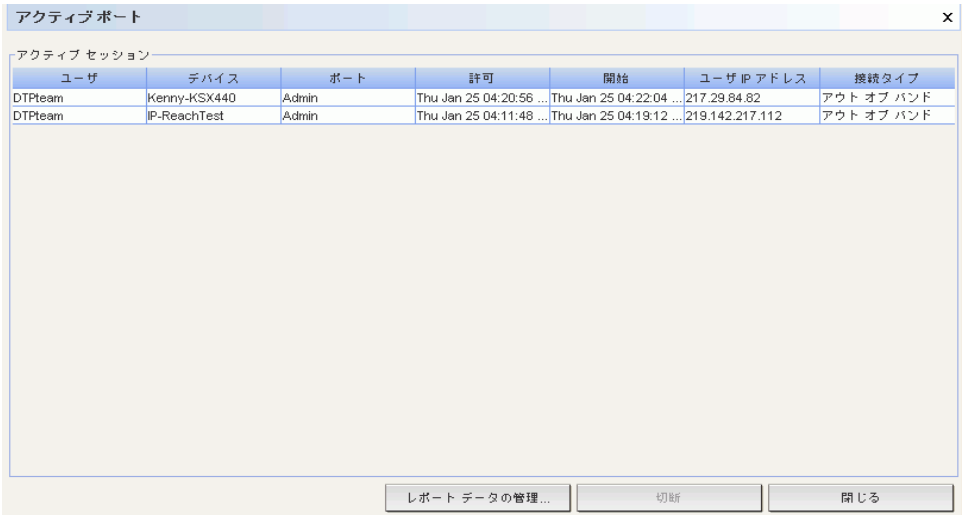


*図 127 アクティブ ポート レポート*

- 現在のセッションからポートを切断するには、切断するポートを選択し、[**切断**] をクリックします。
- レポートを保存または印刷するには、[**レポート データの管理**] をクリックします。現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。
- レポートを閉じるには、[**閉じる**] をクリックします。

## 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は、すべて HTML 形式で表示できます。詳細は、「**第 12 章 : 高度な管理**」を参照してください。

1. [**レポート**] メニューで [**スケジュールされたレポート**] をクリックします。
2. [**レポートの取得**] をクリックして、すべての所有者によって作成されたスケジュールされたすべてのレポートの詳細リストを表示します。デフォルトでは、1 時間前から現在の時刻までにスケジュールされているレポートがすべて表示されます。
3. 表示されるレポートをフィルタするには、アクティブ ポート レポートなどの特定の [**レポート タイプ**] または [**レポートの所有者**] を選択するか、[**レポートが生成された期間**] フィールドで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、上下の矢印を適切な数値になるまでクリックして開始日と終了日を変更することができます。[**レポート名**] フィールドに名前のフレーズまたはフレーズの一部を入力し、レポート名でフィルタすることができます。名前は大文字と小文字が区別されず、ワイルドカードは使用できません。
4. [**レポートの取得**] をクリックすると、フィルタされたリストが表示されます。
5. 個々のレポートを表示するには、リストから対象のレポートをハイライトして [**レポートの表示**] をクリックします。
6. [**閉じる**] をクリックして、レポートを閉じます。

## CC-NOC 同期レポート

CC-NOC 同期レポートには、CC-SG に登録され、特定の検出日に CC-NOC によって監視されているすべてのターゲットとその IP アドレスのリストが表示されます。設定した範囲内で検出された新しいターゲットもここに表示されます。詳細は、「**第 12 章 : 高度な管理**」の「**CC-NOC の追加**」を参照してください。このレポートでは、CC-SG データベースからターゲットを消去することもできます。

1. [**レポート**] メニューの [**CC-NOC 同期**] をクリックします。
2. [検出された最新日付] を選択して [ターゲットの入手] をクリックします。*[検出された最新日付] と同じ日またはそれよりも前に検出されたターゲットが [検出されたターゲット] の下に表示されます。*

- CC-SG データベースからターゲットを消去する場合、消去するターゲットを選択して、[**消去する**] をクリックします。
- ターゲット リスト全体を CC-SG データベースから消去する場合は、[**すべて消去**] をクリックします。
- レポートを保存または印刷するには、[**レポート データの管理**] をクリックします。現在のレポート ページに表示中のレコードを CSV ファイルに保存するには、[**保存**] をクリックし、すべてのレコードを保存するには、[**すべて保存**] をクリックします。 現在のレポート ページに表示中のレコードを印刷するには、[**印刷**] をクリックします。すべてのレコードを印刷するには、[**すべて印刷**] をクリックします。ウィンドウを閉じるには、[**閉じる**] をクリックします。

*本ページは意図的に空白となっています。*

# 第 11 章：システム メンテナンス

## メンテナンス モード

このモードでは、CC-SG へのアクセスが制限され、管理者が中断なくさまざまな操作を行えるようになります。操作は GUI から、または Putty や OpenSSH Client などのクライアントを介して SSH コマンドライン インタフェースから実行できます。詳細は「**第 12 章：高度な管理**」の「**CC-SG へのSSH アクセス**」を参照してください。

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**：メンテナンス モードは、スタンドアロンの CC-SG ユニットでのみ利用可能で、クラスタ設定では利用できません。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。予定タスクの詳細は、「第 12 章：高度な管理 – タスク マネージャ」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

メンテナンス モードを起動するには、以下の手順に従います。

1. [**システム メンテナンス**] メニューで、[**メンテナンス モード**] をクリックして、[**メンテナンス モードの起動**] をクリックします。

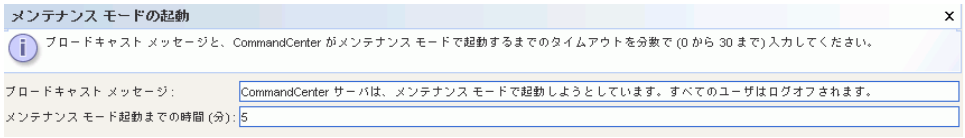


*図 128 メンテナンス モードの起動*

2. [**ブロードキャスト メッセージ**] に入力するか、表示されるデフォルトを受け入れます。このメッセージは、ログインしたすべてのユーザに対して表示され、CC-SG がメンテナンス モードになると、ログオフされることを警告します。
3. [**メンテナンス モード起動までの時間 (分)**] フィールドに時間 (分) を入力します。この時間は、CC-SG がメンテナンス モードになるまでの時間です。**0 ～ 30** 分までの時間を入力できます。**0** の場合、すぐにメンテナンス モードが起動されます。
4. [**OK**] をクリックします。

### メンテナンス モードの終了

メンテナンス モードを終了するには、以下の手順に従います。

1. [**システム メンテナンス**] メニューで [**メンテナンス モード**] をクリックします。
2. [**メンテナンス モードの終了**] をクリックします。[**メンテナンス モードの終了**] 画面が表示されます。
3. [**OK**] をクリックして、メンテナンス モードを終了します。

CC-SG でメンテナンス モードが終了したことを示す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。

1. [**システム メンテナンス**] メニューで [**バックアップ**] をクリックします。[**CommandCenter のバックアップ**] 画面が表示されます。

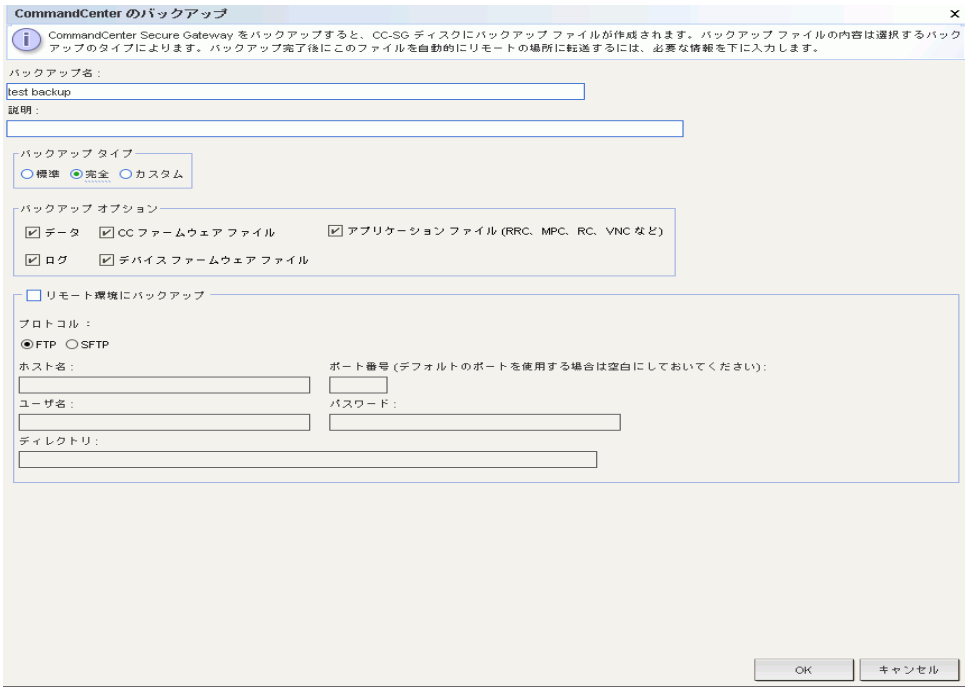


*図 129 CommandCenter のバックアップ画面*

2. [**バックアップ名**] フィールドにこのバックアップの名前を入力します。
3. オプションとして、[**説明**] フィールドにバックアップの簡潔な説明を入力します。
4. [**バックアップ タイプ**] を選択します。
   - **カスタム** - バックアップに追加するコンポーネントを指定できます。その場合、下の [**バックアップ オプション**] 領域でそのコンポーネントを選択します。 次に示すものをバックアップに含める場合は、それぞれを選択します。
     - **データ** – CC-SG 設定、デバイスとノードの設定、およびユーザ データ (標準)
     - **ログ** – 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-SG ファームウェア ファイル** - 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
     - **デバイス ファームウェア ファイル** – 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 ファイル** – 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
   - **完全** - CC-SG に保存されているすべての**データ**、**ログ**、**ファームウェア**、および**アプリケーション ファイル**のバックアップを作成します。 この場合、作成されるバックアップ ファイルのサイズが最大になります。
   - **標準** - CC-SG に保存されている重要な**データ**のみのバックアップが作成されます。この操作の場合、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バックアップされます。この場合、作成されるバックアップ ファイルのサイズは最小になります。

5. このバックアップ ファイルのコピーを外部サーバに保存したい場合は、[**リモート環境にバックアップ**] を選択します。
   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 [**ホスト名**] フィールドに入力します。
   c. 選択したプロトコルにデフォルトのポート (FTP: 21、SFTP: 22) を使用しない場合は、使用する通信ポートを [**ポート番号**] フィールドに入力します。
   d. リモート サーバのユーザ名を [**ユーザ名**] フィールドに入力します。
   e. リモート サーバのパスワードを [**パスワード**] フィールドに入力します。
   f. リモート サーバ上でバックアップを保存するためのディレクトリを [**ディレクトリ**] フィールドに入力します。
6. [**OK**] をクリックします。

10. CC-SG バックアップを確認する完了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

1. [**システム メンテナンス**] メニューで [**リストア**] をクリックします。[**CommandCenter のリストア**] 画面が表示され、CC-SG に使用可能なバックアップ セッションのテーブルが表示されます。このテーブルには、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 ファイルのサイズも一覧表示されます。

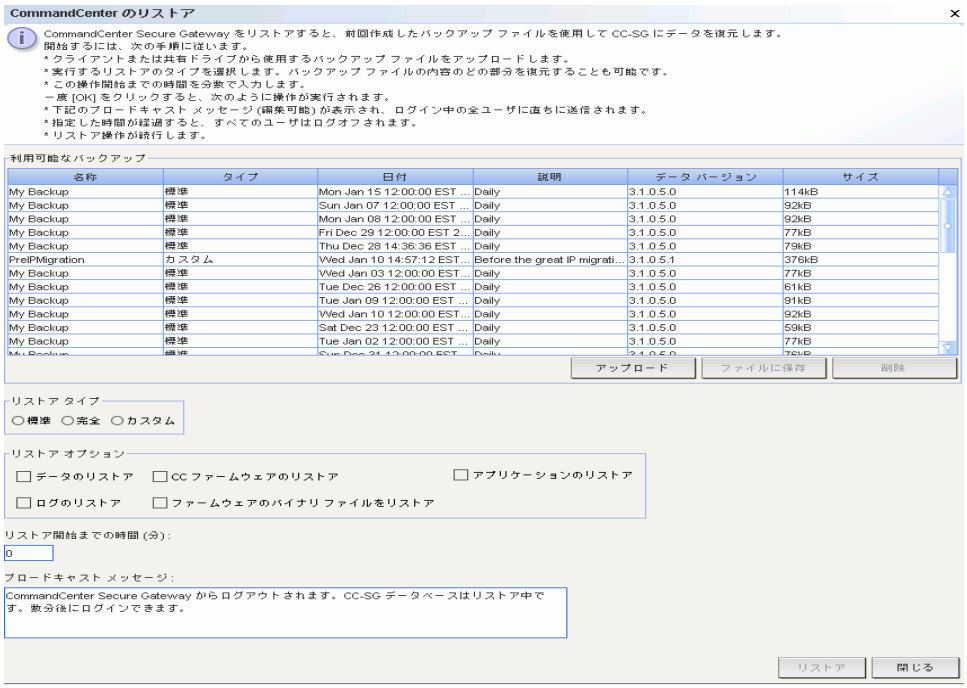


*図 130 CommandCenter のリストア画面*

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、まずこれをアップロードして使用可能にする必要があります。[**アップロード**] をクリックします。[**開く**] ダイアログ画面が表示されます。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。
   a. 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。
   b. [**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。
   c. 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を [**利用可能なバックアップ**] テーブルから選択します
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 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**、および**アプリケーション ファイル**がリストアされます。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。
- **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、下の [**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。
    a. **データ** – CC-SG 設定、デバイスとノードの設定、およびユーザ データ
    b. **ログ** – 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
    c. **CC ファームウェア ファイル** – 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
    d. **デバイス ファームウェア ファイル** – 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
    e. **アプリケーション ファイル** – 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

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、ログオフするまでの時間を確保できます。
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。

11. [**リストア**] をクリックすると、CC-SG では [**リストア開始までの時間**] フィールドに指定された時間が経過してから、選択されたバックアップからその設定がリストアされます。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オフされます。

## バックアップ ファイルの保存および削除

[**CommandCenter のリストア**] 画面から、CC-SG システムに格納されているバックアップを保存したり、削除したりすることもできます。 バックアップの保存では、バックアップ ファイルのコピーを別の PC に保存しておくことができます。一方、不要になったバックアップの削除により、CC-SG 上の領域の節約ができます。

### バックアップを保存するには

1. 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。
2. [**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。

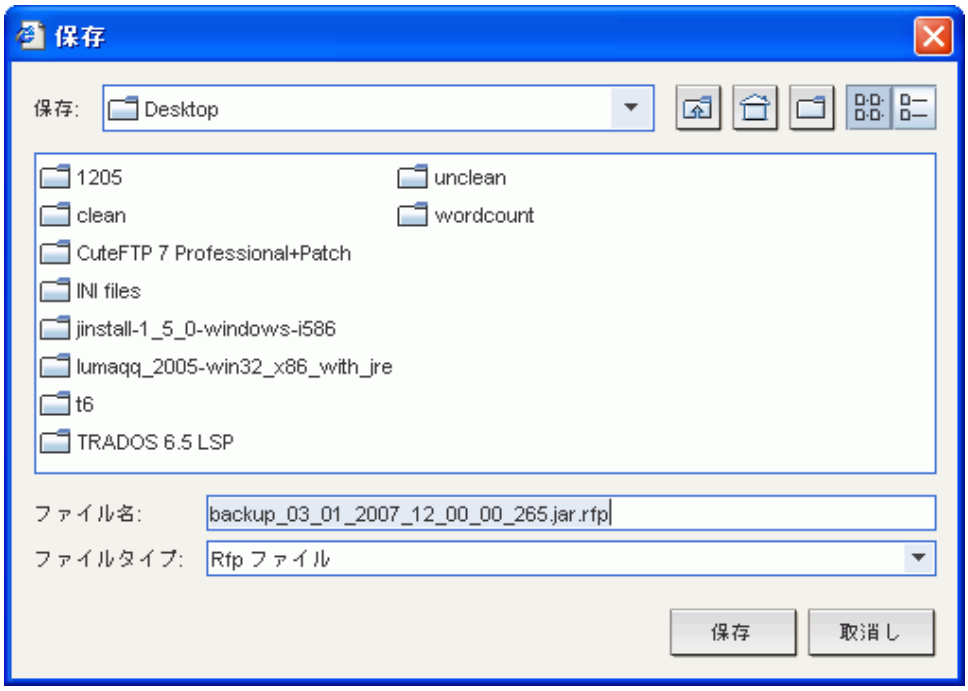


*図 131 バックアップ ファイルの保存*

3. CC-SG バックアップ ファイルの保存場所を指定して、[**保存**] をクリックします。 バックアップ ファイルがクライアント PC にコピーされます。

### バックアップを削除するには

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. CC-SG システムからバックアップを削除する場合は [**OK**] をクリックし、削除せずに終了するには、[**キャンセル**] をクリックします。削除されたバックアップ ファイルは CC-SG から取り除かれます。

***注 :*** *バックアップを CC-SG ユニット間で移動する場合に、保存および復元が使用できます。保存や削除を行うと、システムで完全なアーカイブを保存しておかなくても、CC-SG バックアップを安全にアーカイブとして保存しておくことができます。*

## CC-SG のリセット

[**CommandCenter のリセット**] コマンドを使用すると、CC-SG データベースのデータを消去できます。ただし、CC-SG の IP アドレスなど、システム設定データがリセットされるわけではありません。CC-SG データベースのリセット、SNMP 設定データのリセット、デフォルト ファームウェアへのリセット、デフォルト ファームウェアの CC-SG データベースへのロード、Diagnostic Console のデフォルト値へのリセットが行われます。

1. [**システム メンテナンス**] メニューで [**リセット**] をクリックします。

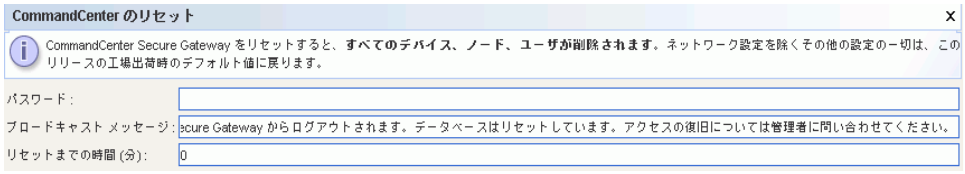


*図 132 CommandCenter のリセット画面*

2. CC-SG の**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**] の現在の設定を受け入れるか、編集して独自のメッセージを作成します。
4. CC-SG でリセット操作が開始されるまでの時間 (0 ～ 60 分) を [**リセット開始までの時間 (分)**] フィールドに入力します。デフォルトは 0 で、CC-SG ユニットはすぐにリセットされます。
5. [**OK**] をクリックして CC-SG ユニットをリセットします。リセットを確認する完了メッセージが表示されます。

**重要：リセット コマンドを使用すると CC-SG のデータベースが消去されます。すべてのデバイス、ノード、ポート、およびユーザが削除されます。認証もローカル DB にリセットされます。リセットを行う前に CC-SG をバックアップしてください。**

## CC-SG を再起動します。

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。

***注 : 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、Diagnostic Console にアクセスするか、ユニット自体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**] メニューで [**再起動**] をクリックします。[**CommandCenter の再起動**] 画面が表示されます。

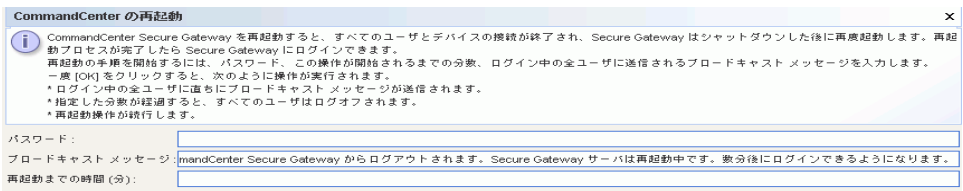


*図 133 再起動画面*

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警告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、システムを再起動する理由を通知します)。CC-SG を再起動すると、すべてのユーザが切断されます。

4. CC-SG で再起動が開始されるまでの時間 (0 ～ 60 分) を [**再起動までの時間 (分)**] フィールドに入力します。
5. [**OK**] をクリックして CC-SG を再起動するか、[**キャンセル**] をクリックして再起動せずに画面を終了します。CC-SG を再起動すると、指定したブロードキャスト メッセージが表示されます。
6. [**OK**] をクリックして CC-SG を再起動します。CC-SG が再起動して使用可能になります。

## CC-SG のアップグレード

CC-SG のファームウェアを新しいバージョンにアップグレードするには、アップグレード コマンドを使用します。CC-SG をアップグレードするには、まず最新ファームウェア ファイルをクライアント PC に保存しておく必要があります。ファームウェア ファイルは、以下の Raritan の Web サイトのサポート セクションにあります。http://www.raritan.com/support/sup_upgrades.aspx

アップグレードの前にまず CC-SG をバックアップしておくことをお勧めします。

---

***注 :*** *CC-SG クラスタを操作している場合は、まずクラスタを削除してから、各ノードを個別に更新してください。*

---

1. [**システム メンテナンス**] メニューで [**メンテナンス モード**] をクリックして、[**メンテナンス モードの起動**] をクリックし、CC-SG をメンテナンス モードにします。この処理を行わない限り、CC-SG をアップグレードすることはできません。詳細は、本章の「メンテナンス モード」を参照してください。
2. 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**] メニューの [**アップグレード**] をクリックします。[**CommandCenter のアップグレード**] 画面が表示されます。


*図 134 CC-SG のアップグレード画面*

3. [**参照**] をクリックして、CC-SG 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。
4. [**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。
5. ファームウェア ファイルが CC-SG にアップロードされたら、成功を示すメッセージが表示されます。つまり、CC-SG にファイルが受け取られ、アップグレード プロセスが開始されたということです。この時点ですべてのユーザが CC-SG から切断されます。[**OK**] をクリックして CC-SG を終了し、再起動できるようにします。
6. CC-SG が再起動するまで、8 分ほどかかります。ブラウザのウィンドウを閉じて、ブラウザ キャッシュをクリアします。
7. 8 分後、新しいブラウザ ウィンドウを開いて、CC-SG を起動します。[ヘルプ] メニューから、[**バージョン情報**] をクリックします。表示されるウィンドウで、バージョン番号をクリックして、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。
8. CC-SG はまだ**メンテナンス モード**になっているので、大部分のユーザはログインできません。メンテナンス モードを終了するには、[**システム メンテナンス**] メニューで、[**メンテナンス モード**] をクリックし、[**メンテナンス モードの終了**] をクリックします。[**OK**] をクリックします。

## CC-SG のシャットダウン

管理者が CC-SG をシャット ダウンする場合は、次の方法をお勧めします。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。

1. [**システム メンテナンス**] メニューで [**CommandCenter のシャットダウン**] をクリックします。[**CommandCenter のシャットダウン**] 画面が表示されます。

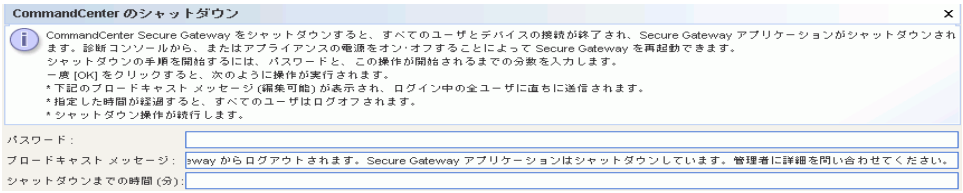


*図 135 CC-SG のシャットダウン画面*

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 ～ 60 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。
5. [**OK**] をクリックして CC-SG をシャットダウンするか、[**キャンセル**] をクリックしてシャットダウンせずに画面を閉じます。シャットダウンすると、CC-SG ログイン ウィンドウが表示されます。

***注** : 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、ログイン画面にリダイレクトされます。CC-SG を再起動するまでは、ユーザは再度ログインできません。再起動については、次で説明します。*

## 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。

1. Diagnostic Console を使用します。「第 12 章 : 高度な管理」の「Diagnostic Console」を参照して、詳細を確認します。

CC-SG ユニットの電源を再投入します。

## CC-SG セッションの終了

### ログ アウト

セッションの終わりに CC-SG を終了する場合、または、ログインしている間に自分または別のユーザが行ったデータベースの変更を反映する場合は、CC-SG を完全にログオフしてからログインし直します。

1. [**Secure Gateway**] メニューの [**ログアウト**] をクリックします。[**ログアウト**] ウィンドウが表示されます。
2. [**はい**] をクリックして CC-SG をログアウトするか、[**いいえ**] をクリックしてウィンドウを閉じます。ログアウトすると、CC-SG ログイン ウィンドウが表示されます。
3. CC-SG に再ログオンするか、[**終了**] をクリックして CC-SG を完全にシャットダウンします。

### CC-SG の終了

CC-SG はいつでも終了できます。このためには、以下の手順に従います。

1. [**Secure Gateway**] メニューの [**終了**] をクリックします。[**終了**] ウィンドウが表示されます。
2. [**はい**] をクリックして CC-SG を終了するか、[**いいえ**] をクリックして [**終了**] ウィンドウを閉じ作業を続行します。

# 第 12 章 : 高度な管理

## ガイド付き設定

**ガイド付き設定**では、関連の作成、Raritan デバイスの設定、ユーザ グループの作成、ユーザの作成など、管理者が CC-SG で最も一般的な作業を行う際の手順が示されます。**ガイド付き設定**の実行についての詳細は、「**第 3 章 : ガイド付き設定を使用した CC-SG の設定**」を参照してください。

## 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、Secure Gateway の管理者は、ログイン時にすべてのユーザ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、管理者に **CC 設定と制御**の権限が必要です。

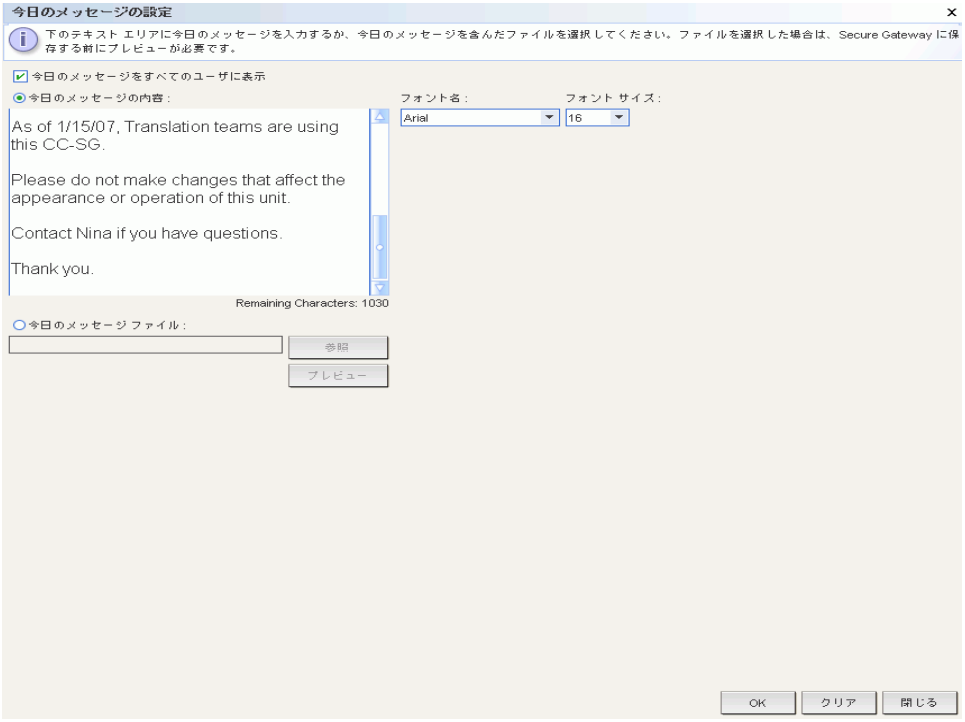


*図 136 今日のメッセージの設定*

1. [**管理**] メニューで [**今日のメッセージの設定**] をクリックします。 [**今日のメッセージの設定**] 画面が表示されます。
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**] をオンにします。
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**] 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**] 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、メッセージを表示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、メッセージを表示するフォント 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. 開くダイアログ 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. [**今日のメッセージの内容**] ダイアログの内容または [**今日のメッセージ ファイル**] のパスを削除する場合は、[**クリア**] をクリックします。
5. [**OK**] をクリックして、設定を CC-SG に保存します。

## アプリケーション マネージャ

アプリケーション マネージャは、管理者が CC-SG にアクセスするアプリケーションを追加したり、既存のアプリケーションを編集したり、Raritan デバイスのノードにアクセスするためのデフォルト アプリケーションを設定したりする際のインタフェースです。

1. [**管理**] メニューで、[**アプリケーション**] をクリックします。[**アプリケーション マネージャ**] 画面が表示されます。

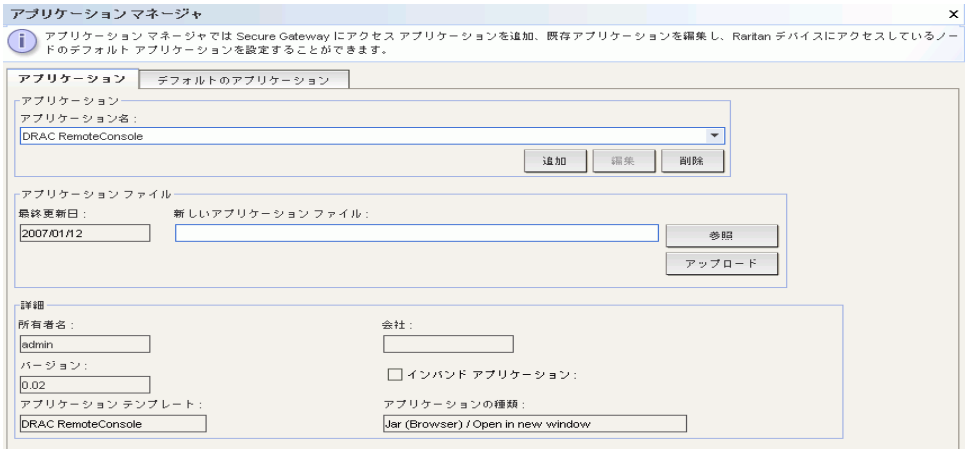


*図 137 アプリケーション マネージャの アプリケーション タブ*

## アプリケーションの追加、編集、および削除

アプリケーションを追加、編集、または削除するには、アプリケーション マネージャの [**アプリケーション**] タブをクリックします。

### アプリケーションの追加

1. [アプリケーション] タブの [アプリケーション] セクションにある [追加] をクリックします。[アプリケーションの追加] ダイアログ ウィンドウが表示されます。

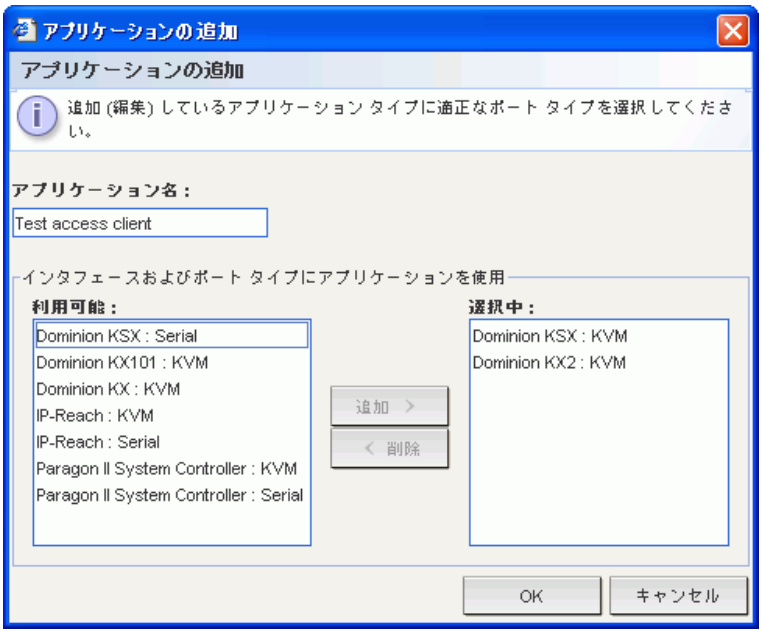


*図 138 アプリケーションの追加*

2. [アプリケーション名] フィールドにアプリケーションの名前を入力します。

3. アプリケーションを使用する 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。アプリケーションが追加されると、[選択中] リストのデバイスがこのアプリケーションを使用できるようになります。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。
4. デバイスでアプリケーション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. アプリケーションを処理する必要なデバイスを選択したら [OK] をクリックします。[開く] ダイアログ画面が表示されます。
6. このウィンドウで、アプリケーション ファイルの場所を検索し (通常は .jar ファイルか .cab ファイル)、ファイルを選択して、[開く] をクリックします。

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編集：**

1. [アプリケーション] タブの [アプリケーション] セクションにある [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。 選択したアプリケーションに関する詳細がタブの [詳細] 領域に表示されます。
2. アプリケーションによっては、この詳細の一部を設定できる場合があります。 必要に応じて [詳細] 領域のパラメータを設定します。
3. [編集] をクリックします。[アプリケーションの編集] ウィンドウが表示されます。

必要な場合、アプリケーションを使用する追加の 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。
デバイスでアプリケーションが使用されないようにする必要がある場合、[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。
アプリケーションを処理する必要なデバイスを選択したら [OK] をクリックします。

**アプリケーションの削除：**

1. [アプリケーション] タブの [アプリケーション] セクションにある [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。 選択したアプリケーションに関する詳細がタブの [詳細] 領域に表示されます。
2. [削除] をクリックして、選択したアプリケーションを削除します。確認ダイアログが表示されます。

削除する場合は [はい]、アプリケーションを削除せずにキャンセルする場合は [いいえ] をクリックします。

## デフォルトのアプリケーション

[**デフォルトのアプリケーション**] タブをクリックすると、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することができます。 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。

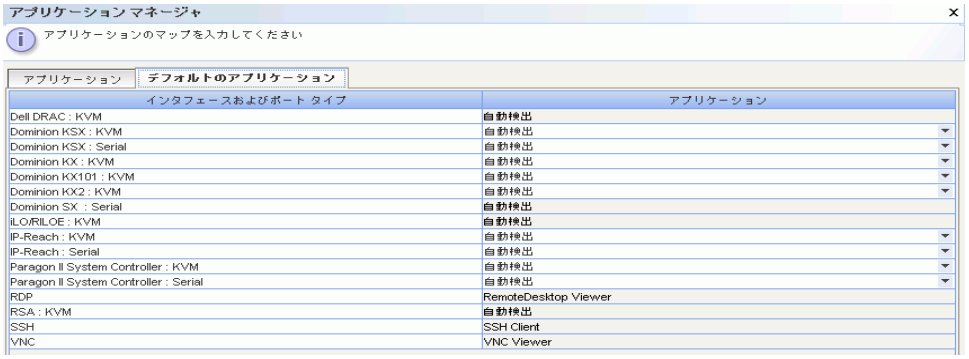


*図 139 デフォルト アプリケーションのリスト*

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編集するには、次の手順に従います。

インタフェースまたはポートのタイプの行を選択します。

1. その行にリストされたアプリケーション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。編集不可能な値はグレー表示になっています。
2. ドロップダウン メニューで、ハイライトされ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] を選択すると、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検出されます。
3. デフォルト アプリケーションがすべて設定されたら、[更新] をクリックして選択内容を CC-SG に保存します。
4. いつでも [閉じる] をクリックして、[アプリケーション マネージャ] 画面を閉じることができます。

# ファームウェア マネージャ

CC-SG は、その制御下にあるデバイスを更新するために Raritan デバイスのファームウェアを保存します。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。

## ファームウェアのアップロード

このコマンドを使用すると、システムにさまざまなバージョンのファームウェアを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。

1. [**管理**] メニューで、[**ファームウェア**] をクリックします。 [**ファームウェア マネージャ**] 画面が表示されます。

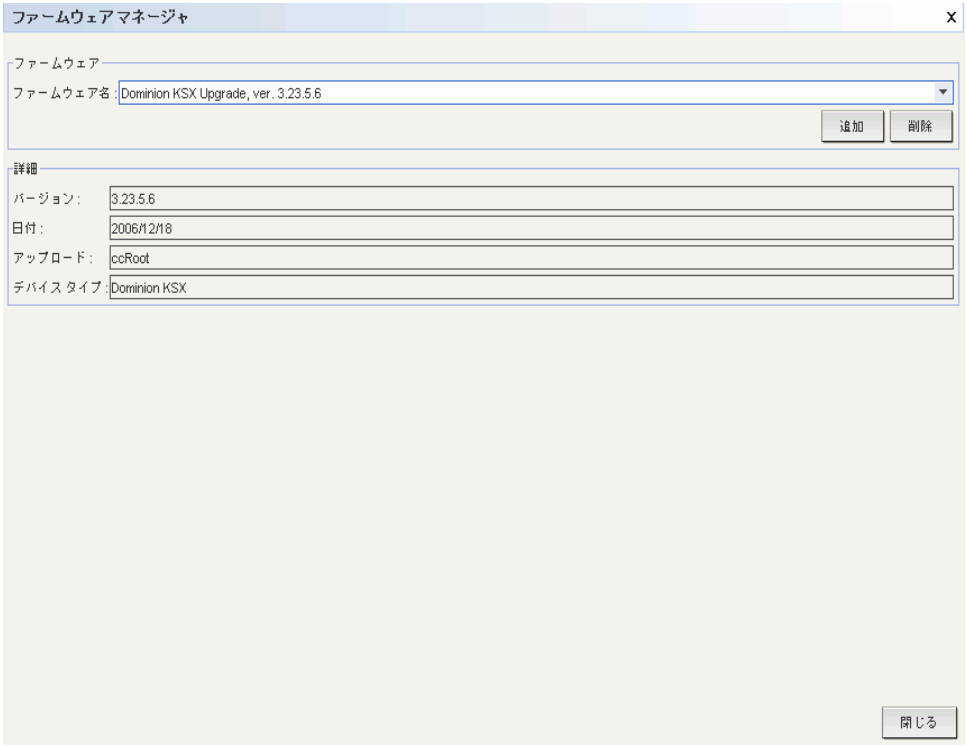


*図 140 ファームウェア マネージャ画面*

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。検索ウィンドウが表示されます。

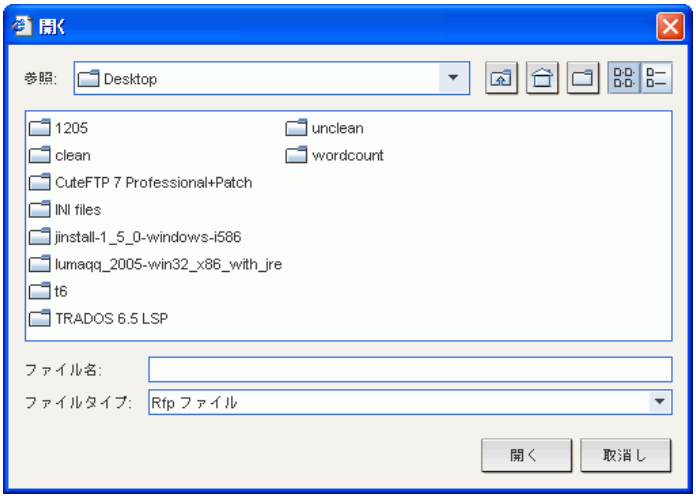


*図 141 ファームウェア検索ウィンドウ*

3. [**参照**] ドロップダウン矢印をクリックし、ナビゲートしてシステム内のファームウェア ファイルを検出します。ファームウェアが見つかったらそれを選択し、[**開く**] をクリックします。追加されたファームウェアの名前が [**ファームウェア マネージャ**] 画面の [**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

1. [**管理**] メニューで、[**ファームウェア**] をクリックします。[**ファームウェア マネージャ**] 画面が表示されます。
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。[**ファームウェアの削除**] ウィンドウが表示されます。


*図 142 ファームウェアの削除ウィンドウ*

4. [**はい**] をクリックしてファームウェアを削除するか、[**いいえ**] をクリックして、何もせずにウィンドウを閉じます。
5. [**閉じる**] をクリックして [**ファームウェア マネージャ**] 画面を閉じます。

## 設定マネージャ

設定マネージャを使用すると、ネットワーク設定など、いくつかの CC-SG のコア設定を管理できます。

## ネットワーク設定

1. [管理] メニューで、[設定] をクリックします。[設定マネージャ] 画面が表示されます。
[ネットワーク設定] タブをクリックします。

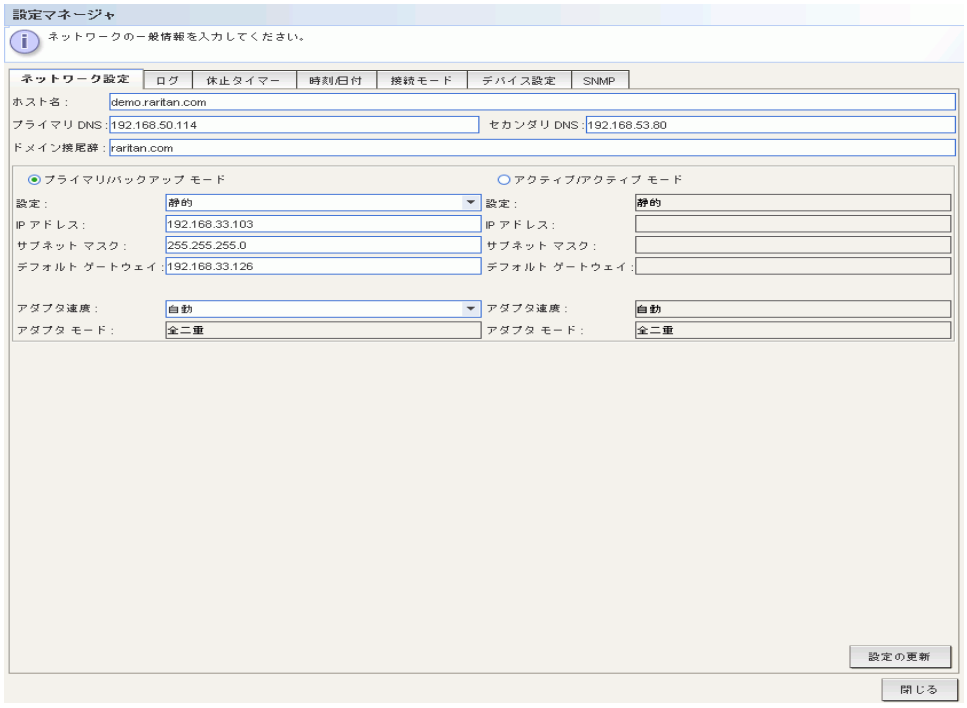


*図 143 設定マネージャのネットワーク設定画面*

2. [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、第 1 章を参照してください。 ドメイン サーバとドメイン接尾辞が設定されている場合、[設定の更新] を選択すると、完全修飾ドメイン名 (FQDN) を反映してフィールドの内容が変更されます。
3. [プライマリ/バックアップ モード] または [アクティブ/アクティブ モード] をクリックします。CC-SG には 2 つの ネットワーク インタフェース コントローラ (NIC) があります。G1 または V1 ユニットの NIC には、次のように背面の左から右にラベルが付いています。

| モデル | 左端の NIC (プライマリ インタフェース) | 右端の NIC |
|---|---|---|
| G1 | LAN1 | LAN0 |
| V1 | LAN1 | LAN2 |

E 1 の NIC は次のように異なります。

| モデル | 上部の NIC (プライマリ インタフェース) | 下部の NIC |
|---|---|---|
| E1 | LAN1 | LAN2 |

1 つのインタフェースだけを使用するか、両方を同時に使用できます。 単純化のために、以下の説明では LAN1 を左の NIC、LAN2 を右の NIC として使用します。一部の内部診断やメッセージでは、これらのインタフェースを「eth0」および「eth1」としている場合があります。

***注：** 両方のインタフェースの接続が切断されると、CC-SG は再起動します。*

A. ネットワーク フェイルオーバーと冗長性を実装するには、[**プライマリ/バックアップ モード**] を選択します。このモードでは、一度に 1 つの NIC のみがアクティブになり、ネットワーク IP アドレスの割り当ては 1 つのみが可能になります。

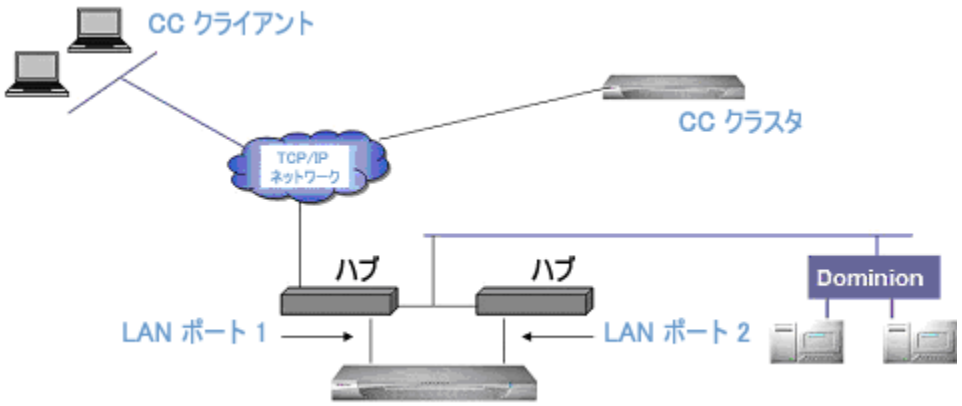


*図 144 プライマリ/バックアップ ネットワーク*

一般的な設定では、NIC は同じ LAN サブネットワークに接続していますが、別のスイッチ（またはハブ）を使って信頼性を向上させることもできます。 両方の NIC を使用すれば、ネットワークの冗長性が得られます。 たとえば、LAN1 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 NIC を使用します。LAN1 に障害が生じても、LAN2 が接続している場合、CC-SG は（DHCP などによって）割り当てられている IP アドレスを LAN2 に移行します。LAN1 が修復されサービスが復帰するまで LAN2 が使用されます。LAN1 が復帰したときには CC-SG は LAN1 に戻ります。

障害が発生したとしても、いずれか一方のインタフェース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。 CC-SG は同じ論理 IP アドレスにありますが、ネットワーク障害が生じた場合にも、通信チャンネルと既存のセッションの維持を試みます。 すべての通信（たとえ

ば PC クライアント、Raritan デバイス管理、クラスタ ピアなど) は両方の NIC によって維持される単一の通信チャンネルを通して行われます。

B. 特殊なネットワーク環境、特にルーティングが存在しない 2 つのネットワークがある場合には、[**アクティブ/アクティブ モード**] を選択します。 ネットワーク セキュリティを重視する場合、およびプロキシ型のデプロイメント環境の場合にも、このモードを選択してください。

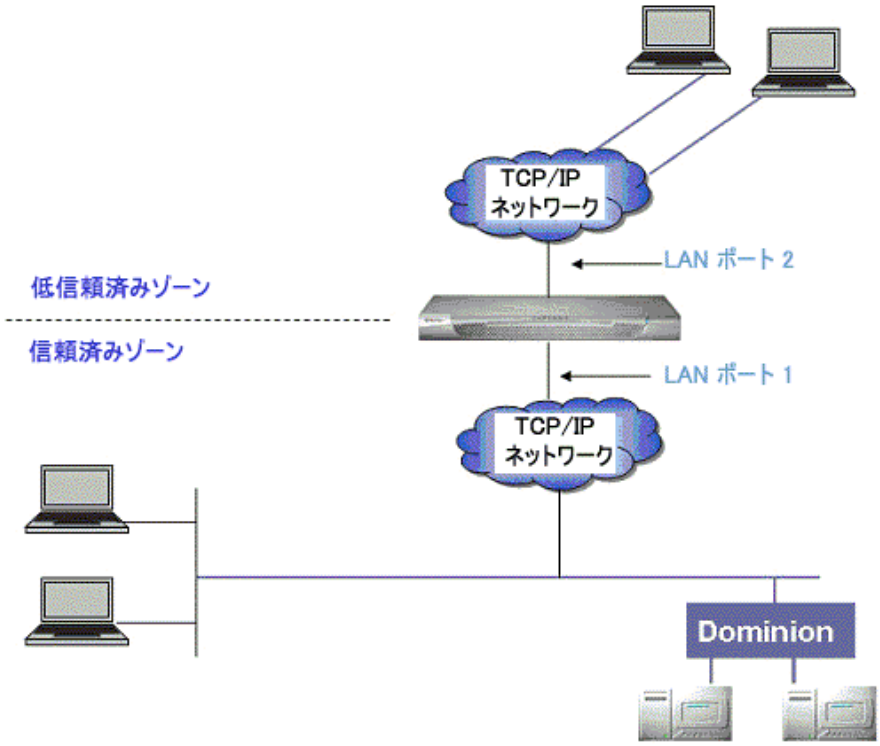


*図 145 アクティブ/アクティブ ネットワーク*

このモードでは、特に**プロキシ** モードを使用する場合、CC-SG は 2 つの別々の IP ドメイン間の「ルータ」または「トラフィック監視ノード」として機能します。 詳細は、本章の後の「**接続モード**」を参照してください。プロキシ モードでは、CC-SG がプロキシの対象となる PC クライアント セッションをそれぞれのノードにルーティングできるようにするため、**アクティブ/アクティブ** モードを使用する必要があります。 Raritan で制御するデバイスを LAN1 に接続し、プロキシ対象の PC クライアントを LAN2 に接続することをお勧めします。 両方の NIC は別々のサブネットワーク上にあるようにします。ただし、DHCP を使用している場合はこれは不可能であるため、このような設定はサポートされていません。 両方の NIC を設定するとき、1 つの NIC のみにデフォルトのゲートウェイ アドレスを指定し、もう 1 つの NIC の設定は空白のままにしておきます。

1 つの NIC に障害が発生すると、CC-SG は現在の IP ルーティング テーブルに従って他の NIC からパケットをルーティングします。 特にファイアウォールが設定されているとき、このルーティングは成功しない場合があります。 追加のルートが必要な場合、Diagnostic Console で追加できます。 詳細については本章の後の「静的ルートの編集 (ネットワーク インタフェース)」を参照してください。

***注 : アクティブ/アクティブ** モードではクラスタリングは設定できません。*

4. [設定] ドロップダウン矢印をクリックし、リストから [DHCP] または [静的] を選択します。 DHCP を選択する場合、DHCP サーバが正しく設定されていることを確認してから、ホスト名を入力します。 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 マスクは、[設定の更新] を選択すると自動的に設定されます。 この情報を使って 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)。登録に成功した後、DHCP の使用時は IP アドレスが不明な場合もあることから、CC-SG にはホスト名でアクセスできるようになります。

[静的] を選択した場合、IP アドレス、サブネット マスク、デフォルト ゲートウェイ、プライマリ DNS、およびセカンダリ DNS をそれぞれ該当するフィールドに入力します。また、ドメイン設定のための文字列を [ドメイン接尾辞] に入力します。

[アダプタ速度] ドロップダウン矢印をクリックし、リストから回線速度を選択します。

5. [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、リストから二重モードを選択します。

[アクティブ/アクティブ] モードを選択した場合、5 ～ 7 の手順に従って、2 番目のネットワーク インタフェースを設定します。

[設定の更新] をクリックしてシステムのネットワーク設定を更新します。

[閉じる] をクリックして [設定マネージャ] 画面を閉じます。

## ログの設定

[**ログ**] タブから、外部ログ サーバにレポートするように、CC-SG を設定できます。それぞれのログでレポートされるメッセージのレベルを設定できます。

## ログ アクティビティの設定：

1. [管理] メニューで、[設定] をクリックします。[設定マネージャ] 画面が表示されます。
2. [ログ] タブをクリックします。

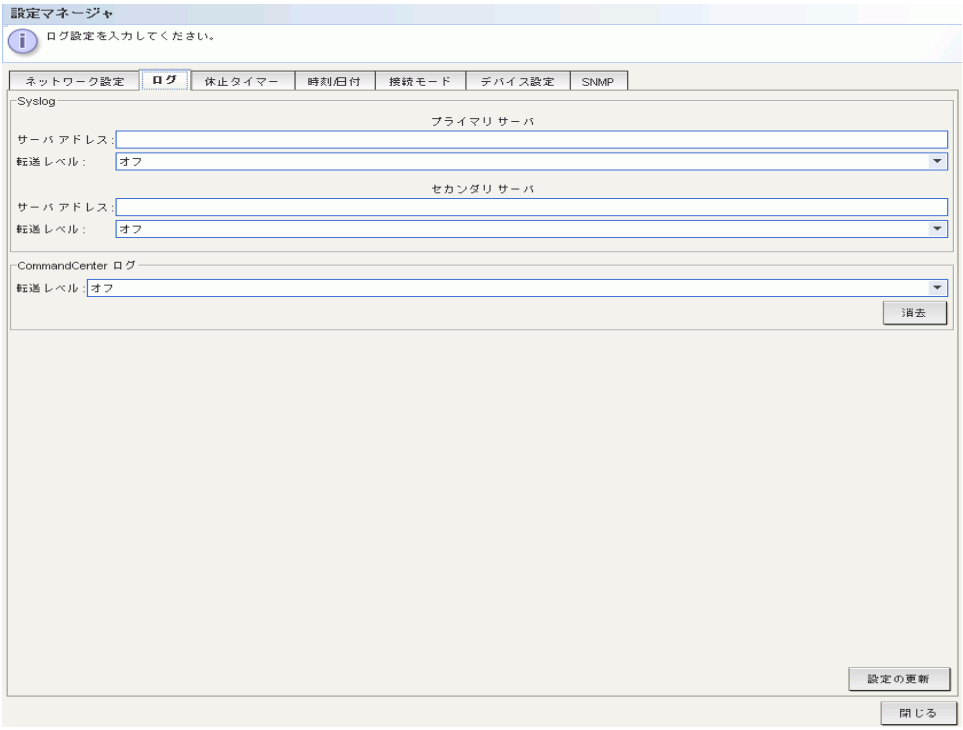


*図 146 設定マネージャのログ画面*

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。

3. [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。

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。

4. [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。

ログの設定を完了したら、[設定の更新] をクリックして設定を CC-SG に保存します。
[閉じる] をクリックして [設定マネージャ] 画面を閉じます。

## CC-SG の内部ログの消去 :

[ログ] タブを使用すると、CC-SG のイベント ログを消去することもできます。このコマンドでは CC-SG のイベント ログがクリアされるだけで、外部ログ サーバに記録されたイベントは消去されません。

1. [管理] メニューで、[設定] をクリックします。[設定マネージャ] 画面が表示されます。
2. [ログ] タブをクリックします。
3. 画面の下部の [消去する] をクリックします。確認のためのダイアログ ウィンドウが表示されます。

[はい] をクリックして、CC-SG イベント ログを消去します。

***注** : 監査証跡およびエラー ログは 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 つのレポートからもデータが消去されます。*

## 休止タイマーの設定

この画面では、セッションがアクティブ状態を保持できるログオフされるまでの時間を設定します。

1. [管理] メニューで、[設定] をクリックします。[設定マネージャ] 画面が表示されます。

[休止タイマー] タブをクリックします。

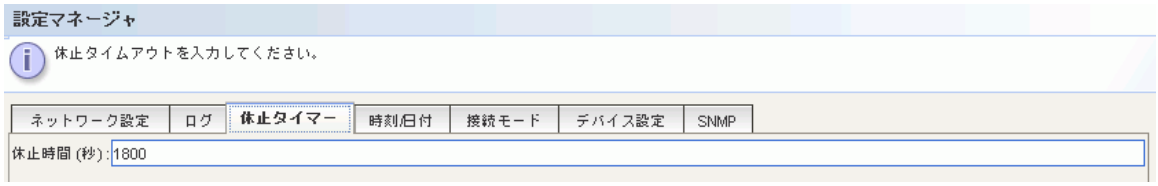


*図 147 休止タイマー タブ*

[休止時間 (秒)] フィールドに適切な休止時間の上限を入力します。
[設定の更新] をクリックして、設定を CC-SG に保存します。

## 時刻/日付の設定

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。 詳細は、「第 12 章 : 高度な管理 – タスク マネージャ」を参照してください。クライアントの時刻設定は 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。

1. [**管理**] メニューで、[**設定**] をクリックして、[**設定マネージャ**] 画面を開きます。
2. [**時刻/日付**] タブをクリックします。

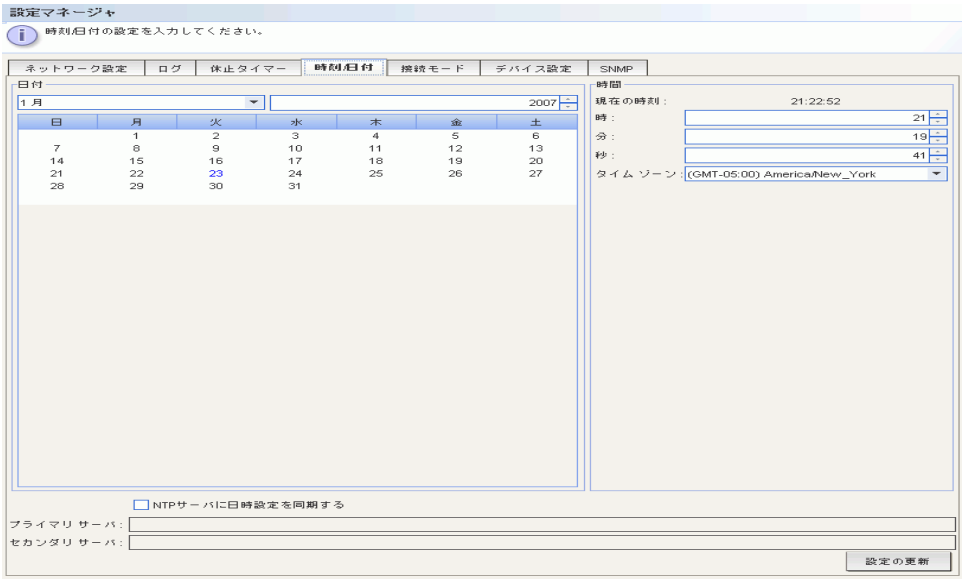


*図 148 設定マネージャの時刻/日付画面*

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。

b. **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オンにし、**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. [**メンテナンス**] メニューで [**再起動**] をクリックして、CC-SG を再起動します。

***注** : 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。*

## モデムの設定

この画面は、クライアント マシンからダイヤルアップ接続で CC-SG G1 にアクセスする際に使用します。緊急の状況では、この方法で CC-SG にアクセスできます。

*注 : V1 または E1 プラットフォームではモデムは使用できないため、設定は行えません。*

### CC-SG の設定

1. [**管理**] メニューで、[**設定**] をクリックします。 [**設定マネージャ**] 画面が表示されたら、[**モデム**] タブをクリックします。

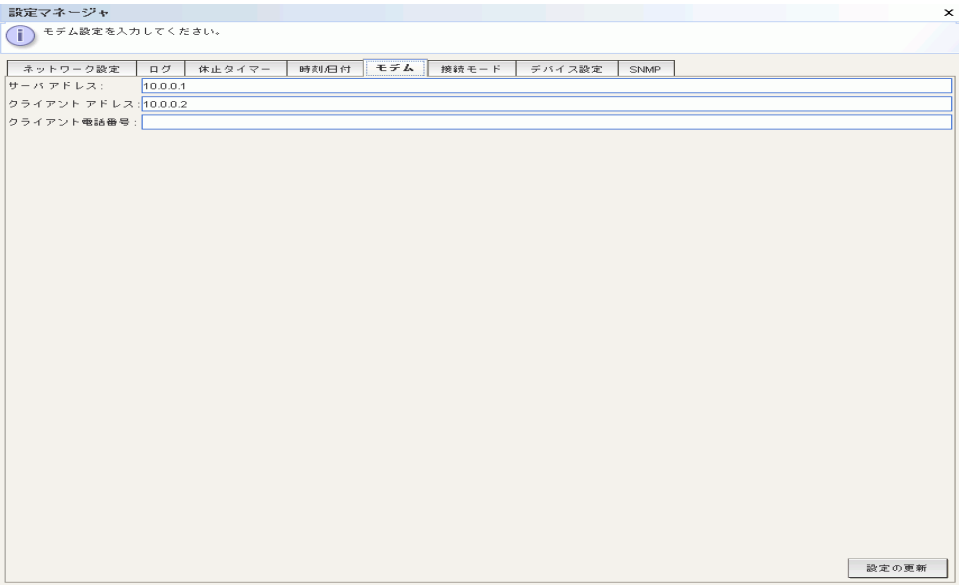


*図 149 設定マネージャのモデム画面*

2. CC-SG の IP アドレスを [**サーバ アドレス**] フィールドに入力します。
3. CC-SG にダイヤルアップ接続するクライアントの IP アドレスを [**クライアント アドレス**] フィールドに入力します。
4. コールバック ダイヤルを使用する場合、CC-SG がクライアントに接続するためにダイヤルするコールバック番号を [**クライアント電話番号**] に入力します。
5. [**設定の更新**] をクリックして、モデム情報を保存します。

### クライアント PC のモデムの設定

電話線を CC-SG GI に接続します。CC-SG G1 にはモデムが内蔵されています。 オプションとして、LAN ケーブルを外します。

ダイヤルインするクライアントで、モデムをクライアント マシン (Windows XP マシンなど) に接続します。クライアントのモデムに電話線を接続します。クライアント マシンを再起動すると、接続しているモデムが新しいハードウェアとして検出されます。 以下の手順に従ってクライアントのモデムをインストールします (これは Windows XP マシン用の手順です)。

1. [**コントロール パネル**] の [**電話とモデムのオプション**] を選択します。

2. [**モデム**] タブをクリックします。

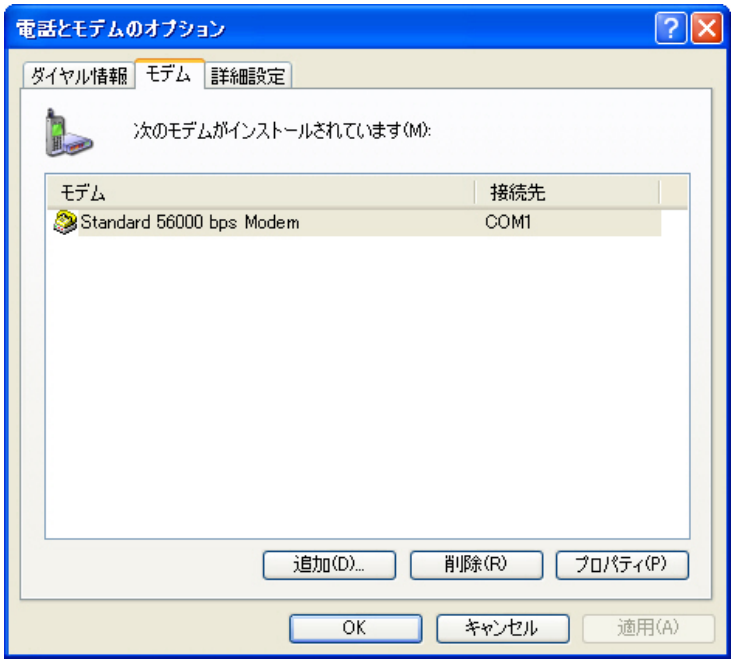


*図 150 モデム タブ*

3. [**プロパティ**] をクリックします。
4. [**詳細**] タブをクリックします。

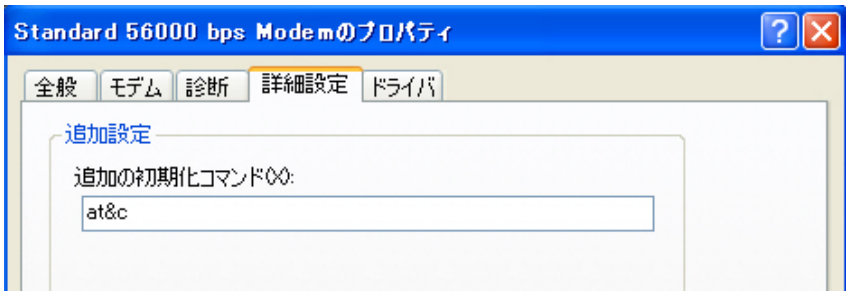


*図 151 追加の初期化コマンド*

5. [**追加の初期化コマンド**] にモデムで「Carrier detection」フラグを設定するために使用される初期化コマンドを入力します。たとえば、SoftK56 Data Fax モデムの場合は「**at&c**」と入力します。これは、開始したモデム接続プロセスが相手 (ダイヤルイン) 側がモデム接続を終了した際に閉じてしまわないよう、Windows に指定するために必要になります。[**OK**] をクリックして設定を保存します。

### ダイヤルアップ接続の設定

ここでは、Windows XP クライアント マシンで CC-SG へのインバウンド ダイヤルアップ接続を作成する手順を説明します。

1. [**スタート**] メニューから [**マイ ネットワーク**] を選択します。
2. ウィンドウを右クリックして [プロパティ] を選択します。

3. [**ネットワーク接続**] ウィンドウの [**ネットワーク タスク**] の下から、[**新しい接続を作成する**] をクリックします。


*図 152 新しい接続を作成する*

4. [**職場のネットワークへ接続する**] (ダイアルアップ接続) をクリックします。
5. CC-SG の名前を入力します (例 **CommandCenter**)。

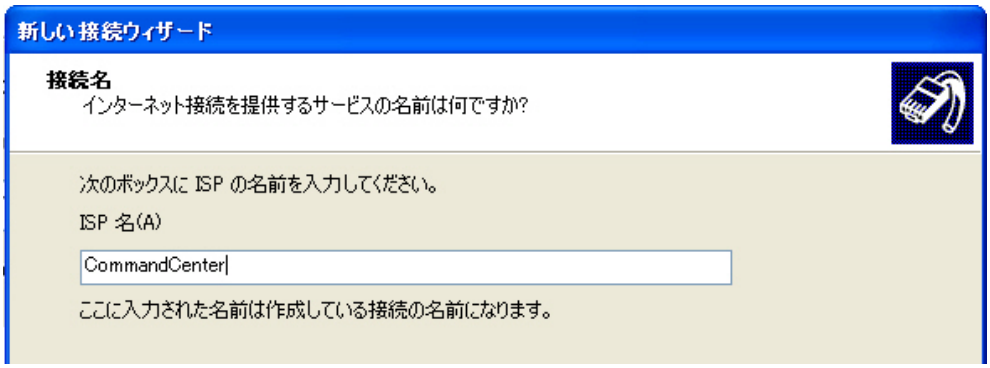


*図 153 接続名*

6. CC-SG に接続するための電話番号を入力し、[**次へ**] をクリックします。これは、CC-SG の [設定マネージャ] の [**モデム**] タブで [**クライアント電話番号**] に入力したダイヤルバック番号とは違います。

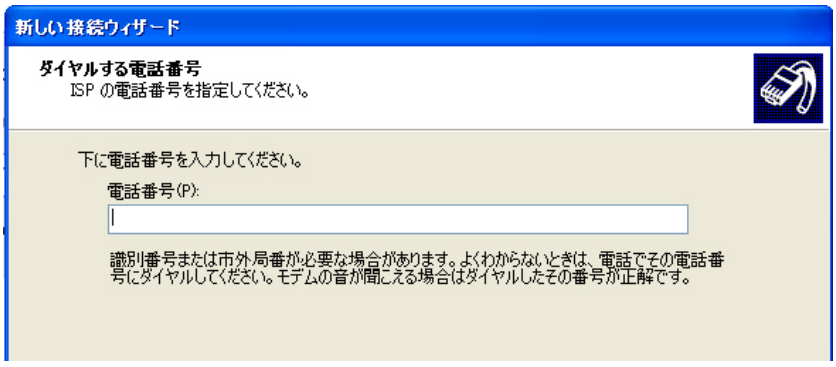


*図 154 ダイヤルする番号*

7. CC-SG にダイヤルするのにスマートカードは必要ありません。スマート カードを使用していない場合は、この接続について [**自分のスマート カードを使わない**] を選択して [**次へ**] をクリックします。
8. 次の画面では、通常はユーザ自身のみがこの接続を使用できるように [**自分専用**] を選択します。
9. 最後の画面で [**完了**] をクリックして接続設定を保存します。

### コールバック接続の設定

CC-SG がコールバック接続を使用する場合、ここで説明するスクリプト ファイルを使う必要があります。コールバック用のスクリプト ファイルを提供するには、以下の手順に従います。

1. [**スタート**] メニューから [**マイ ネットワーク**] を選択します。
2. [**ネットワーク タスク**] の [**ネットワーク接続を表示する**] をクリックします。
3. CommandCenter 接続を右クリックして [**プロパティ**] をクリックします。
4. [**セキュリティ**] タブをクリックします。

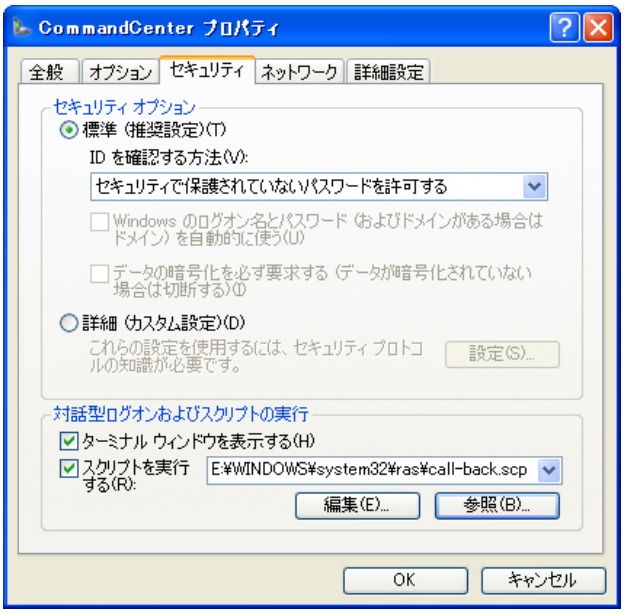


*図 155 ダイヤルアップ スクリプトの指定*

5. [**ターミナル ウィンドウを表示する**] をクリックします。
6. [**スクリプトを実行する**] をクリックし、[**参照**] をクリックしてダイヤルアップ スクリプトを入力します (例 call-back.scp)。
7. [**OK**] をクリックします。

**コールバック スクリプト ファイル例 :**

```
proc main
delay 1
waitfor "ogin:"
transmit "ccclient^M"
waitfor "client:"
transmit "dest^M"
waitfor "callback."
transmit "ATH^M"
waitfor "RING"
transmit "ATA^M"
waitfor "CONNECT"
waitfor "ogin:"
transmit "ccclient^M"
endproc
```

### モデムによる CC-SG への接続

CC-SG に接続するには、以下の手順に従います。

1. [**スタート**] メニューから [**マイ ネットワーク**] を選択します。
2. [**ネットワーク タスク**] の [**ネットワーク接続を表示する**] をクリックします。
3. **CommandCenter** 接続をダブルクリックします。

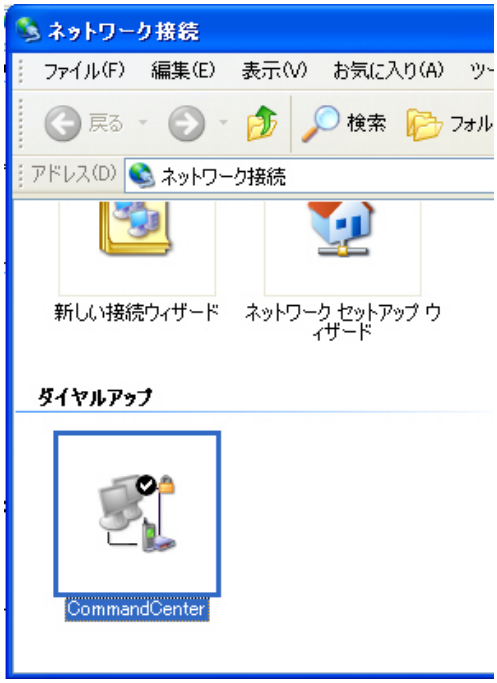


*図 156 CC-SG への接続*

4. ユーザ名「**ccclient**」とパスワード「**cbupass**」を入力します。


*図 157 ユーザ名とパスワードの入力*

5. まだ入力していない場合は、CC-SG に接続する電話番号を入力します。これはダイヤルバック番号とは違います。

6. [**ダイヤル**] をクリックします。コールバックを使用している場合は、モデムが CC-SG にダイヤルした後 CC-SG がクライアント PC にダイヤルします。
7. 本章の「**コールバック接続の設定**」セクションで説明したように、[ターミナル ウィンドウを表示する] チェックボックスをオンにした場合は、下図のようなウィンドウが表示されます。

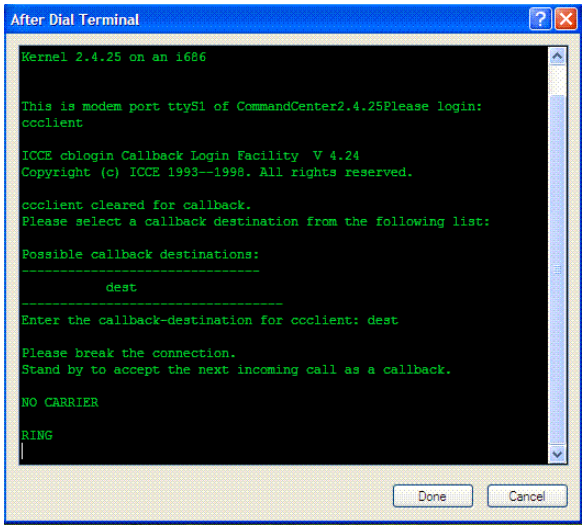


*図 158 ダイヤル後ターミナル*

8. 1 ～ 2 分待ってから、サポートされているブラウザで、[設定マネージャ] の [モデム] タブの [サーバアドレス] で設定した CC-SG の IP アドレスを入力し、CC-SG にログインします。

### 接続モード

ノードに接続されている場合には、そのノードを使って直接データを送受信したり (**ダイレクト モード**)、またはすべてのデータを CC-SG ユニット経由で送受信する (**プロキシ モード**) オプションを使用できます。**プロキシ モード**を使うと CC-SG サーバ上の帯域幅負荷は増加しますが、ファイアウォールで開いている CC-SG の TCP ポート (80、433、2400) のみを保持するだけでかまいません。 詳細については『**Raritan デジタル ソリューション デプロイメント ガイド**』を参照してください。

1. [**管理**] メニューで、[**設定**] をクリックします。[**設定マネージャ**] 画面が表示されます。
2. [**接続モード**] タブをクリックします。

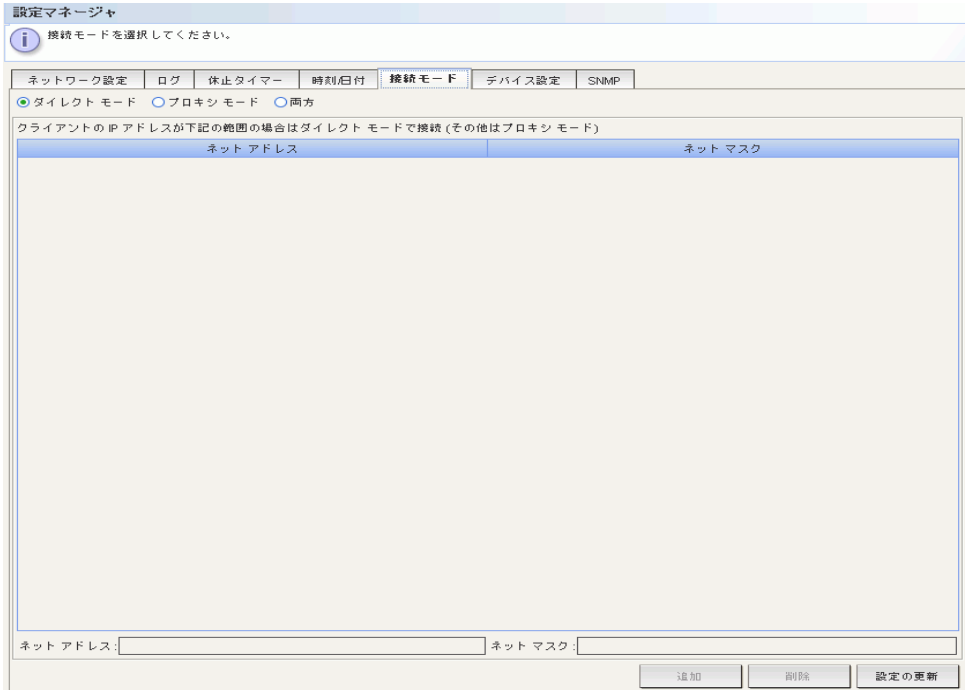


*図 159 設定マネージャの接続画面 – ダイレクト モード*

3. 使用する接続モードのラジオ ボタンをクリックします。
   a. デバイスを直接接続する場合は、[**ダイレクト モード**] ラジオ ボタンをクリックします。
   b. CC-SG ユニット経由でデバイスに接続する場合は、[**プロキシ モード**] ラジオ ボタンをクリックします。
   c. 一部のデバイスを直接接続で、別のデバイスを**プロキシ モード**で接続する場合には、[**両方**] ラジオ ボタンをクリックします。直接接続するデバイスの設定を指定します。
      i. 画面の下部の [**ネット アドレス**] フィールドにクライアントの IP アドレスを入力します。
      ii. [**ネット マスク**] フィールドにクライアントのネット マスクを入力します。
      iii. [**追加**] ボタンをクリックすると、ネット アドレスとマスクが画面に追加されます。[**追加**]/[**削除**]/[**更新**] ボタンを表示するには、画面右側にあるスクロール バーを使用しなければならない場合があります。

### デバイス設定

1. [**管理**] メニューで、[**設定**] をクリックします。[**設定マネージャ**] 画面が表示されます。
2. [**デバイス設定**] タブをクリックします。

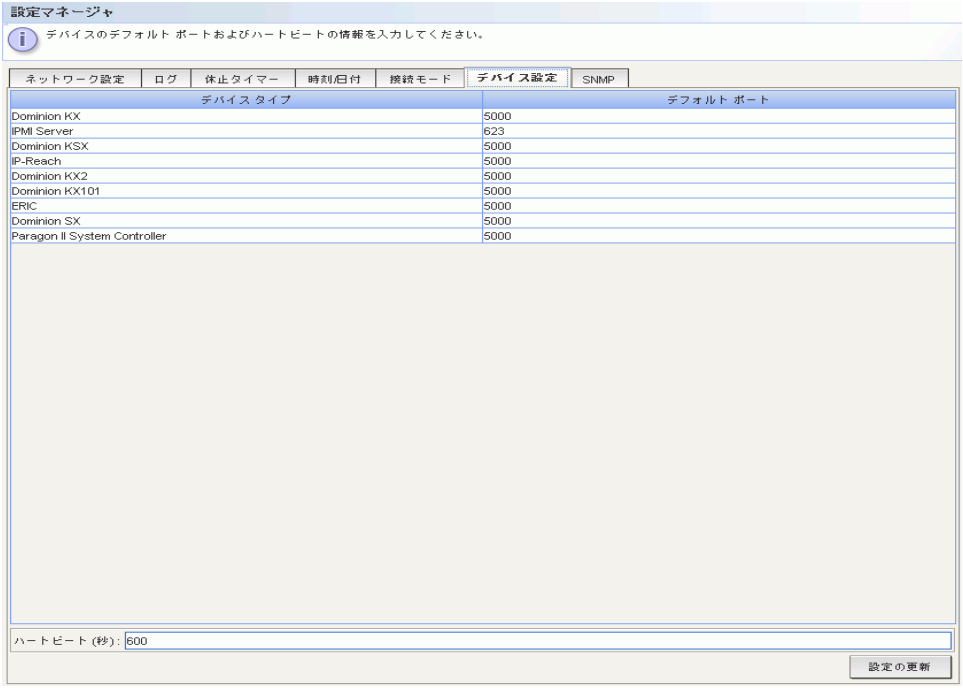


*図 160 設定のデバイス設定画面*

3. デバイスのデフォルト ポートを更新するには、テーブルからデバイス タイプを選択し、デフォルト ポートの値をダブルクリックします。新しいデフォルト ポートの値を入力して **Enter** キーを押します。
4. デバイスのタイムアウト時間を更新するには、画面の下部の [**ハートビート (秒)**] の値をダブルクリックします。このデバイスの新しいタイムアウト時間を入力します。
5. [**設定の更新**] をクリックして新しいデバイスの値を保存します。 関連付けられたデバイス設定がすべて更新されたことを確認する完了メッセージが表示されます。

## 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。 SNMP インフラストラクチャの処理訓練を受けた CC-SG 管理者のみが、CC-SG が SNMP と連携して動作するように設定してください。

CC-SG では、SNMP GET/SET の操作に、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をサポートします。この操作をサポートするには、これらの MIB-II システム グループ オブジェクトである 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。 詳細は、RFC 1213 を参照してください。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。

### MIB ファイル

**CC-SG** は独自の Raritan トラップ セットを送り出すため、Raritan の SNMP トラップ定義を含んだカスタム MIB ファイルですべての SNMP マネージャを更新する必要があります。「付録 A：仕様 (G1、V1、および E1)」を参照してください。このカスタム MIB ファイルは、CC-SG ユニットに付属の CD に収録されています。また、**http://www.raritan.com/support** の [**Firmware Upgrades**] から入手することもできます。

## CC-SG の SNMP の設定

1. [**管理**] メニューで、[**設定**] をクリックします。[**設定マネージャ**] 画面が表示されます。
2. [**SNMP**] タブをクリックします。

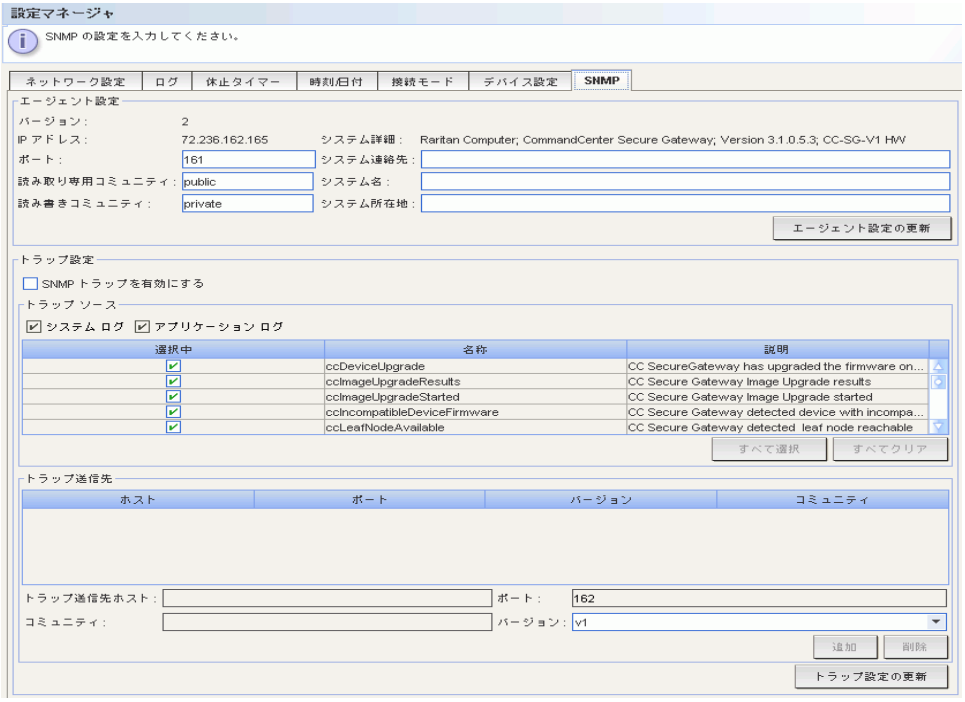


*図 161 設定のデバイス設定画面*

3. サードパーティのエンタープライズ管理ソリューションに CC-SG で実行している SNMP エージェントを認識させるには、[**エージェント設定**] にエージェント情報を入力します。エージェントの**ポート**を入力します (デフォルトは **161**)。**読み取り専用コミュニティ**文字列 (デフォルトは「**public**」) または読み書きコミュニティ文字列 (デフォルトは「**private**」) を入力します。カンマで区切って複数のコミュニティ文字列を指定することもできます。**システム連絡先**、**システム名**、**システム所在地** を指定して、管理対象ノードに該当する情報を入力します。
4. [**エージェント設定の更新**] をクリックして SNMP エージェントの識別情報を保存します。
5. [**トラップ設定**] で [**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 トラップの送信を有効にします。
6. CC-SG が SNMP ホストに送り出すトラップの前にあるチェックボックスをオンにします。
   [**トラップ ソース**] には 2 つの異なるカテゴリにグループ分けされた SNMP トラップのリストがあります。[**システム ログ**] トラップにはハードディスク エラーなどの CC ユニット自体のステータスの通知が、[**アプリケーション ログ**] トラップにはユーザ アカウントへの変更といった CC アプリケーションのイベントで生成された通知が含まれています。タイプ別にトラップを有効にするには、[**システム ログ**] および [**アプリケーション ログ**] のラベルのついたボックスをオンにします。個々のトラップを有効または無効にするには、対応するチェックボックスをチェックします。[**すべて選択**] と [**すべてクリア**] を使って、すべてのトラップを有効にしたり、すべてのチェックボックスをクリアにしたりします。提供される SNMP トラップのリストについては、MIB ファイルを参照してください。詳細は、「**MIB ファイル**」を参照してください。
7. [**トラップ送信先**] パネルで、[**トラップ送信先ホスト**] と [**ポート**]に SNMP ホストが使用する IP アドレスとポート番号を入力します。デフォルトのポートは「**162**」です。
8. SNMP ホストが使用する [**コミュニティ**] 文字列を入力し [**バージョン**] ([**v1**] または [**v2**]) を選択します。

9. [**追加**] をクリックして、この送信先ホストを設定済みホストのリストに追加します。リストからホストを削除するには、ホストを選択して [**削除**] をクリックします。このリストで設定できるマネージャ数に制限はありません。
10. SNMP トラップと送信先を設定したら、[**トラップ設定の更新**] をクリックします。

## クラスタ設定

CC-SG クラスタは、プライマリ CC-SG 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。 クラスタのプライマリ ノードとセカンダリ ノードは、同じバージョンのソフトウェアを実行している必要があります。 特にユーザが定義しない限り、各クラスタ ノードには CC-SG によってデフォルトの名前が割り当てられます。

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 CC-SG ユニット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**:クラスタ設定では、プライマリ CC-SG のみが CC-NOC と通信します。CC-SG がプライマリになると、プライマリ CC-SG はその IP アドレスとセカンダリ CC-SG の IP アドレスを CC- NOC に送信します。*

### クラスタの作成

障害が発生したとき、管理者はすべての CC-SG ユーザに新しいプライマリ CC-SG ノードの IP アドレスを使用するように電子メールで通知する必要があります。

**重要：クラスタを設定する前に、両方のノードの設定をバックアップしておくことを推奨します。**

***注**： クラスタリングで使用するには、CC-SG は、そのネットワーク ポートを**プライマリ/バックアップ** モードで稼動する必要があります。 クラスタリングは、アクティブ/アクティブ設定では機能しません。 詳細についてはこの章の「**ネットワーク接続**」を参照してください)。*

### プライマリ CC-SG ノードの設定

1. [**管理**] メニューで、[**クラスタ設定**] をクリックします。[**クラスタ設定**] 画面が表示されます。
2. [**CommandCenter の検出**] をクリックし、現在使用しているサブセットと同じサブセット上に存在するすべての CC-SG アプライアンスをスキャンして表示します。 または、ウィンドウ下の [**CommandCenter のアドレス**] に IP アドレスを指定して、[**CommandCenter の追加**] をクリックし、別のサブネットにある CC-SG を追加することもできます。

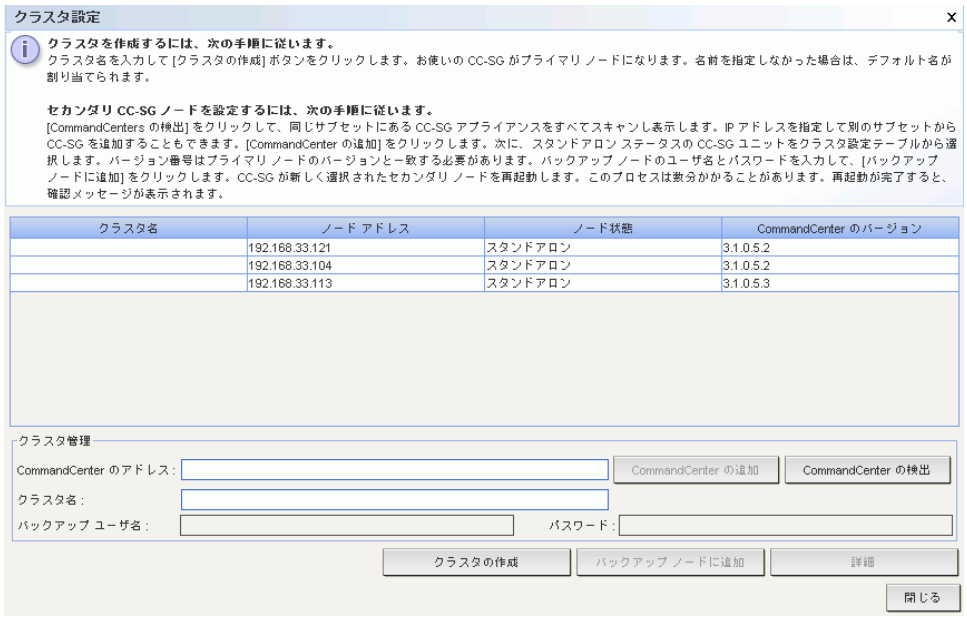


*図 162 クラスタ設定画面*

3. [**クラスタ名**] にこのクラスタの名前を入力します。ここで名前を指定しないと、クラスタの作成時に **cluster192.168.51.124** のようなデフォルトの名前が付与されます。
4. [**クラスタの作成**] をクリックします。
5. プロンプトが表示されたら [**はい**] をクリックして続けます。現在使用している CC-SG がプライマリ ノードになり、先ほどの手順で [クラスタ名] フィールドに名前を指定していない場合はデフォルトの名前が付与されます。

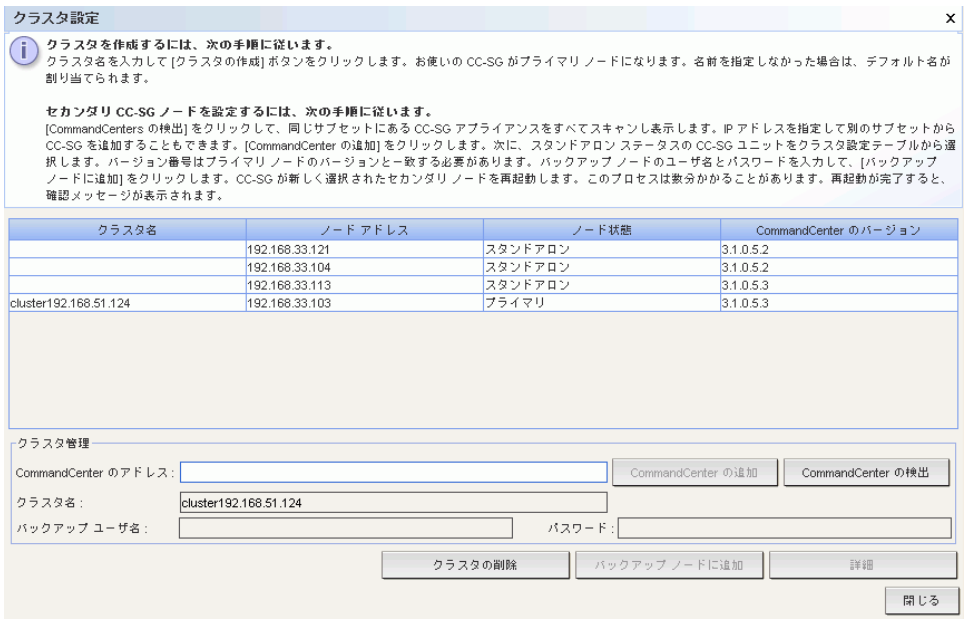


*図 163 クラスタ設定 – プライマリノードの設定*

### セカンダリ CC-SG ノードの設定

1. [**CommandCenter の検出**] をクリックし、現在使用しているサブセットと同じサブセット上に存在するすべての CC-SG アプライアンスをスキャンして表示します。 または、ウィンドウ下の [**CommandCenter のアドレス**] に IP アドレスを指定して、別のサブネットにある CC-SG を追加することもできます。[**CommandCenter の追加**] をクリックします。

***注**：別のサブネットまたはネットワークからバックアップ用の CC-SG を追加すると、1 つのネットワークまたは物理的なロケーションのみに影響する問題を回避することができます。*

2. セカンダリ ノードまたはバックアップ CC-SG ノードを追加するには、クラスタ設定テーブルからステータスが [**スタンドアロン**] の CC-SG ユニットを選択します。バージョン番号がプライマリ ノードのバージョンと同じである必要があります。
3. バックアップ ノードの有効なユーザ名とパスワードを [**バックアップ ユーザ名**] フィールドと [**パスワード**] フィールドにそれぞれ入力します。
4. [**バックアップ ノードに追加**] をクリックします。
5. 確認メッセージが表示されます。 選択されたノードにセカンダリ ステータスを割り当てるには [**はい**] をクリックし、キャンセルするには [**いいえ**] をクリックします。

**重要：追加処理を開始したら、次の手順 6 で示すように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。**

6. [**はい**] をクリックすると、新しく選択されたセカンダリ ノードが CC-SG によって再起動されます。この処理には数分かかることがあります。 再起動が完了すると、画面に確認メッセージが表示されます。
7. [**管理**] メニューの [**クラスタ設定**] をクリックして、更新されたクラスタ設定テーブルを表示します。

***注**：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。接続が回復すると、プライマリ ノードが 2 つになる場合があります。このような場合、1 つのプライマリ ノードを削除してセカンダリ ノードとしてリセットしてください。*

### セカンダリ CC-SG ノードの削除

1. CC-SG ユニットからセカンダリ ノード ステータスを削除し、設定の別のユニットに再び割り当てるには、クラスタ設定テーブルのセカンダリ CC-SG ノードを選択し、[**バックアップ ノードの削除**] をクリックします。
2. 確認メッセージが表示されたら、[**はい**] をクリックしてセカンダリ ノード ステータスを削除します。キャンセルするには [いいえ] をクリックします。

***注**：[**バックアップ ノードの削除**] をクリックすると、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。*

### プライマリ CC-SG ノードの削除

1. CC-SG ユニットからプライマリ ノード ステータスを削除し、設定内の別のユニットに再び割り当てるには、クラスタ設定テーブルのプライマリ CC-SG ノードを選択し、[**クラスタの削除**] をクリックします。
2. 確認メッセージが表示されたら、[**はい**] をクリックしてプライマリ ノード ステータスを削除します。キャンセルするには [**いいえ**] をクリックします。

***注**：[**クラスタの削除**] をクリックしてもプライマリ CC-SG ユニットは設定からは削除されません。プライマリ ノードの指定だけが削除されます。[**クラスタの削除**] はバックアップ ノードが存在しない場合にのみ使用できます。*

## 障害が発生した CC-SG ノードの復元

ノードが失敗し、フェイルオーバが発生すると、失敗したノードは [**待機中**] ステータスで復元します。

1. クラスタ設定テーブルの待機ノードを選択します。
2. [**待機ノードに追加**] をクリックして、バックアップ ノードとして追加します。
3. 確認メッセージが表示されます。選択されたノードにセカンダリ ステータスを割り当てるには [**はい**] をクリックし、キャンセルするには [**いいえ**] をクリックします。[**はい**] をクリックした場合は、[**バックアップ ノードに追加**] のときと同様にセカンダリ ノードが再起動するのを待つ必要があります。

***注 :*** *ノードが [**待機中**] モードになったら、[**スタンドアロン**] モードまたは [**バックアップ**] モードで起動できます。*

## 詳細設定

クラスタ設定の詳細設定を行うには、以下の手順に従います。

1. 作成したばかりのプライマリ ノードを選択します。
2. [**詳細**] をクリックします。[**詳細設定**] ウィンドウが表示されます。

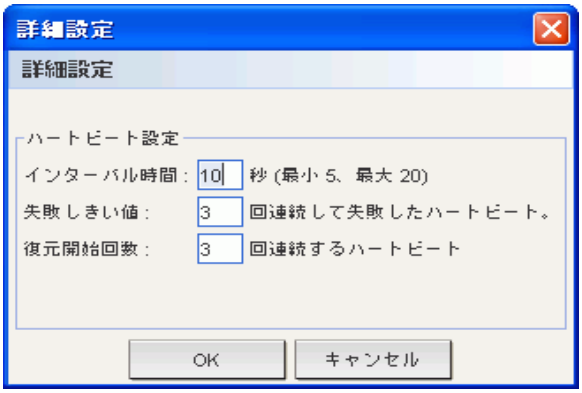


*図 164 クラスタ設定の詳細設定*

3. [**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。

***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。また、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してください。*

4. [**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。
5. [**復元開始回数**] には、失敗した接続が復元したと見なされるまでに正常に返される連続ハートビート数を入力します。
6. [**OK**] をクリックして設定を保存します。

***注** : 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。*

# セキュリティの設定

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、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、「**第 9 章 : リモート認証の設定**」を参照してください。

## サーバ - クライアント接続

セキュリティ マネージャで、CC-SG とのクライアント接続でのセキュリティ設定を定義できます。

1. [**管理**] メニューで、[**セキュリティ**] をクリックします。[**セキュリティ マネージャ**] 画面が表示されます。
2. [**全般**] タブをクリックします。

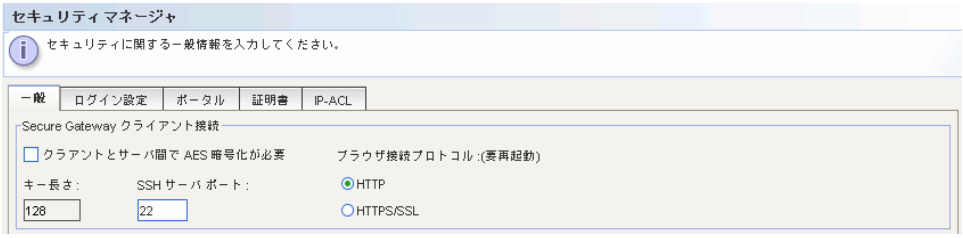


*図 165 セキュアなクライアント接続*

3. CC-SG との暗号化された AES 接続が必要な場合、[**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オンにします。使用する暗号キーの長さを [**キー長さ**] フィールドに入力します。キーのデフォルトの長さは半角で **128** 文字です。
4. SSH を介して CC-SG にアクセスするためのポート番号を [**SSH サーバ ポート**] フィールドに入力します。詳細については、この章の後の「**CC-SG への SSH アクセス**」を参照してください。
5. [**HTTP**] または [**HTTP/SSL**] ラジオ ボタンをクリックして、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。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。
6. [**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**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。

1. [**管理**] メニューで、[**セキュリティ**] をクリックします。[**セキュリティ マネージャ**] 画面が表示されます。
2. [**ログイン設定**] タブをクリックします。

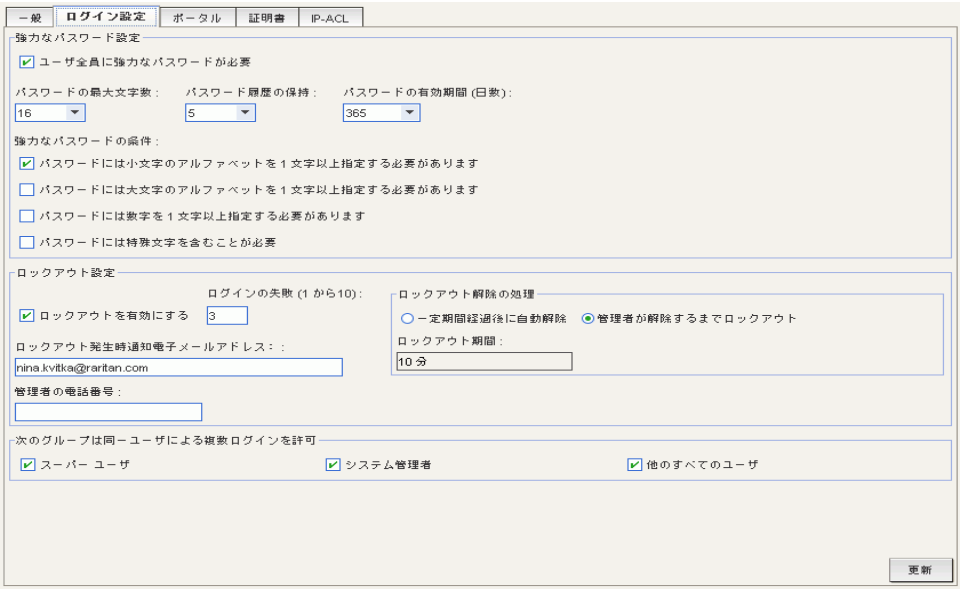


*図 166 ログイン設定*

### 強力なパスワード設定

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。 強力なパスワードを使用するには、管理者は最初に [**ユーザ全員に強力なパスワードが必要**] をオンにします。

---

***注 :*** *CC スーパー ユーザには、強力なパスワードの条件をすべて満たす強力なパスワードが常に必要です。*

---

オンにした後、管理者は [**強力なパスワード設定**] 領域の各フィールドを編集して、そのパスワード ルールをカスタマイズできます。 設定する強力なパスワードはすべて、最低限、次の条件を満たすものでなければなりません。

- **パスワードの最大文字数** – パスワードはすべて必要最小限の文字数を含むようにします。ドロップダウン メニューをクリックして、パスワードの最小長を選択します。
- **パスワード履歴の保持** – ドロップダウン メニューをクリックして、使用されたパスワードがいくつ履歴に保存されるかを指定します。 履歴にある間は、ユーザは、新しいパスワードを選択するように求められたときに、履歴内のパスワードを再使用できません。たとえば、**パスワード履歴**が **5** に設定されている場合、ユーザは直前の 5 つのパスワードはどれも使用できません。
- **パスワード有効期間** – この設定日数後は、すべてのパスワードを期限切れとする必要があります。ドロップダウン メニューをクリックして、パスワードが有効となっている日数を選択します。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。

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。

**強力なパスワードの条件**のほかに、管理者はさらに次のような条件を加えてパスワード ルールを設定できます。

- 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

強力なパスワード ルールを設定したら、[**更新**] をクリックして設定を保存します。 選択するすべてのルールは累積的なものです。すなわちすべてのパスワードは、管理者がこれまで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 ルールを設定した後は、それ以後使用するすべてのパスワードはこれらの条件を満たすものでなければならず、新しいパスワードのほうが従来のパスワードよりも強力になった場合は、既存のすべてのユーザは次回のログイン時に現在の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、認証サーバ自体で管理されます。

Raritan では、「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よう推奨しています。

### 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、CC-NOC ユーザ、SSH ユーザをロックアウトできます。この機能は、CC-SG によってローカルで認証および承認されるユーザのみに適用され、外部サーバによってリモート認証されるユーザには適用されません。 詳細は、「第 9 章 : リモート認証の設定」を参照してください。ユーザ ライセンス数が足りないためにログインが失敗した場合にも適用されません。

---

***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および後の失敗ログイン試行回数は変更できません。*

---

ユーザ ロックアウトを設定するには、以下の手順に従います。

1. [**ロックアウトを有効にする**] をオンにします。
2. 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。
3. ロックアウト戦略を選択します。
   a. [**一定時間ロックアウト**] を選択した場合は、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。デフォルトは **5** 分ですが、**1** ～ **1440** 分 (24 時間) までの値を指定できます。 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。
   b. [**管理者が解除するまでロックアウト**] を選択した場合、管理者が許可するまでユーザはロックアウトされます。ユーザのアンロック方法については、「**第 10 章 : レポートの生成**」を参照してください。
4. 「**ロックアウト通知電子メール**」に電子メール アドレスを入力します。ロックアウトが発生すると、受信者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。
5. 管理者に連絡する必要がある場合は、[**管理者の電話番号**] に電話番号を入力します。
6. [**更新**] をクリックして設定を保存します

### 同一ユーザ名での複数ログインを許可

この設定により、CC-SG で同じユーザ名による複数の同時セッションが許可されます。

1. admin アカウントの下で CC-SG への複数の同時接続を許可する場合は、[**スーパー ユーザ**] をオンにします。
2. [**システム管理者**] ユーザ グループの下のアカウントで同時ログインを許可する場合は、[システム管理者] をオンにします。
3. 他のすべてのアカウント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**] をオンにします。

## ポータル

ポータル設定により、管理者は、ユーザがクライアント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**] メニューで、[**セキュリティ**] をクリックします。[**セキュリティ マネージャ**] 画面が表示されます。
2. [**ポータル**] タブをクリックします。

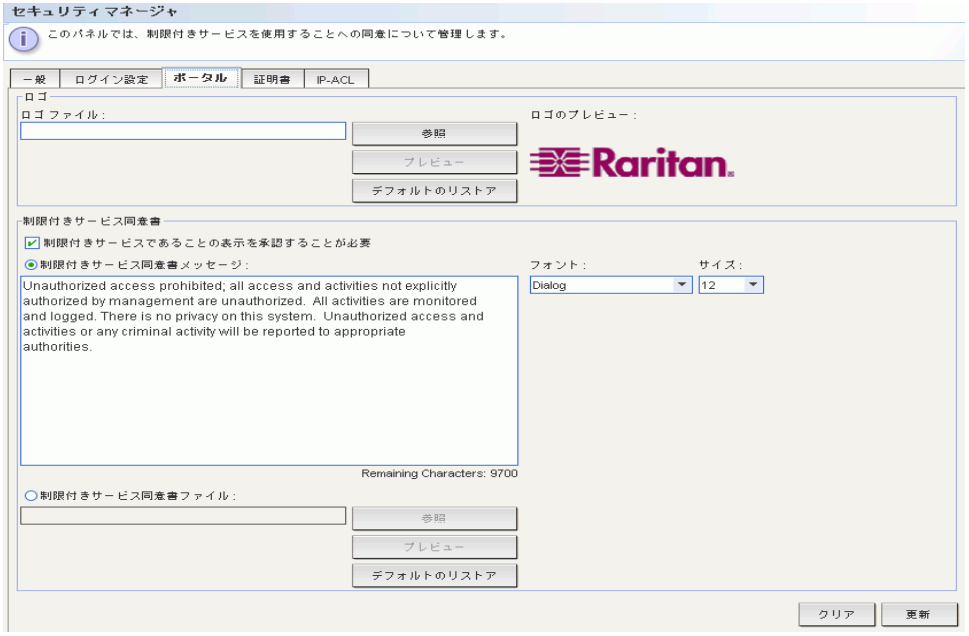


*図 167 ポータル設定*

### 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. 必要に応じて、[**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、変更したロゴを CC-SG に保存します。

### 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。

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**] をオンにして、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. 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。
   a. 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。
   b. [**フォント**] ドロップダウン メニューをクリックして、メッセージを表示する際のフォントを選択します。
   c. [**サイズ**] ドロップダウン メニューをクリックして、メッセージを表示する際のフォント サイズを選択します。

   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、**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。
   a. [**参照**] をクリックします。ダイアログ ウィンドウが表示されます。
   b. 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。
   c. ファイルに含まれるテキストをプレビューする場合は、[**プレビュー**] をクリックします。テキストが上のバナー 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、制限付きサービス使用条件バナーの変更を CC-SG に保存します。

ロゴおよび制限付きサービス使用条件の設定が更新されたら、次回にユーザがクライアントにアクセスする際にログイン画面に表示されます。


*図 168 ログイン ポータルの限定使用条件*

## 証明書

このウィンドウのオプションは、証明書署名依頼 (CSR または証明書依頼とも呼ばれます) の生成に使用できます。CSR は、デジタル身元証明書を取得するために依頼主から証明機関に送信されるメッセージです。CSR を作成する前に、依頼主はキー ペアを生成し、プライベート キーは秘密にします。CSR には依頼主の身元を証明する情報 (X.509 証明書の場合はディレクトリ名など) と依頼主が選択した公開キーが含まれています。

***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。*

1. [**管理**] メニューで、[**セキュリティ**] をクリックします。[**セキュリティ マネージャ**] 画面が表示されます。

2. [**証明書**] タブをクリックします。

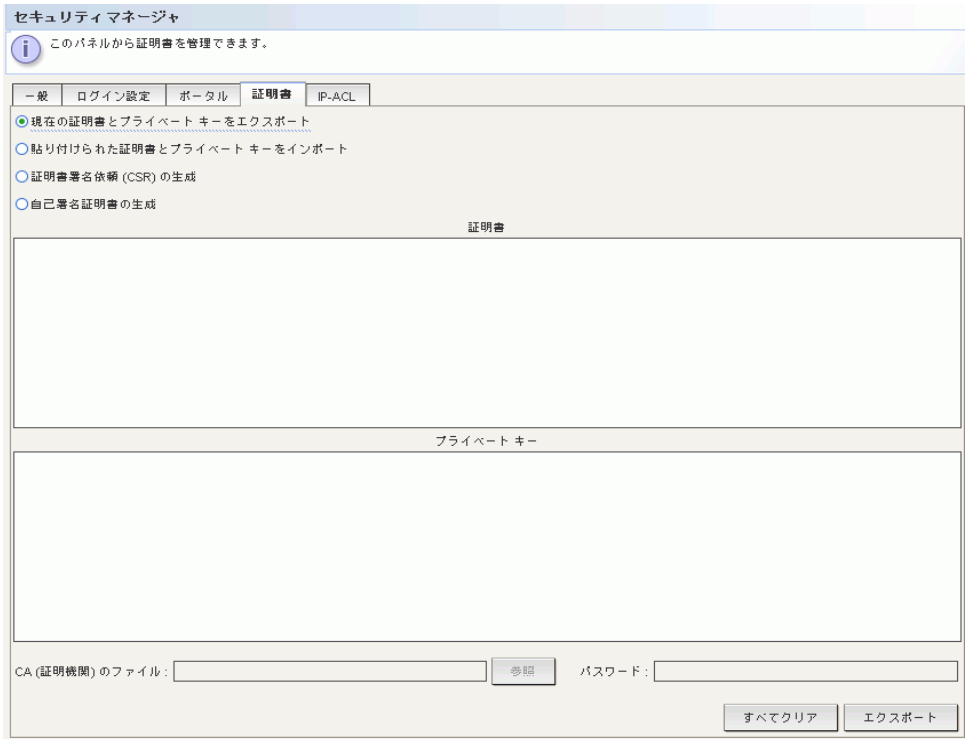


*図 169 セキュリティ マネージャの証明書画面*

### 現在の証明書とプライベート キーをエクスポート

[**現在の証明書とプライベート キーをエクスポート**] をクリックします。[**認証**] パネルに証明書が表示され、[**プライベート キー**] パネルにプライベート キーが表示されます。[**エクスポート**] をクリックすると、**証明書**と**プライベート キー**のテキストがコピーされ、送信されます。

### 証明書署名依頼 (CSR) の生成

CC-SG における CSR とプライベート キーの生成方法を説明します。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。署名証明書、ルート証明書、プライベート キーがインポートされます。

1. [**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**] ウィンドウが表示されます。

2. CSR に必要なデータを各フィールドに入力します。

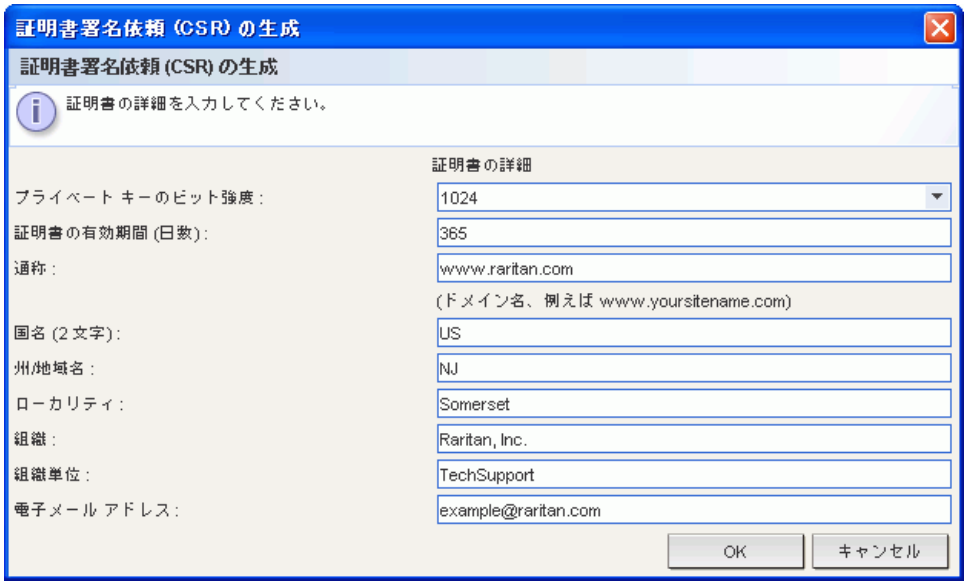


*図 170 証明書署名依頼 (CSR) の生成画面*

3. [**OK**] をクリックして CSR を生成します。[**キャンセル**] をクリックすると、何もせずにウィンドウが閉じます。[**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。


*図 171 生成された証明書依頼*

4. ASCII エディタ (メモ帳など) を使って CSR をコピーしてファイルに貼り付け、拡張子 **.cer** で保存します。
5. ASCII エディタ (メモ帳など) を使ってプライベート キーをコピーしてファイルに貼り付け、テキスト形式で保存します。
6. 手順 4 で保存した CSR ファイル (**.cer**) を証明書サーバに送信し、サーバから署名証明書を取得します。
7. 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。
8. 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。

9. 署名証明書をコピーして [**証明書リクエスト**] フィールドに貼り付けます。先ほど保存したプライベート キーを [**プライベート キー**] フィールドに貼り付けます。
10. [**CA (証明機関) のファイル**] の横の [**参照**] をクリックし、手順 6 で保存したルート証明書ファイルを選択します。
11. 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の生成

[**自己署名証明書の生成**] オプション ボタンをクリックし、[**生成**] をクリックします。[**自己署名証明書の生成**] ウィンドウが表示されます。 自己署名証明書に必要なデータを各フィールドに入力します。[**OK**] をクリックして証明書を生成します。[**キャンセル**] をクリックすると、何もせずにウィンドウが閉じます。[**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。

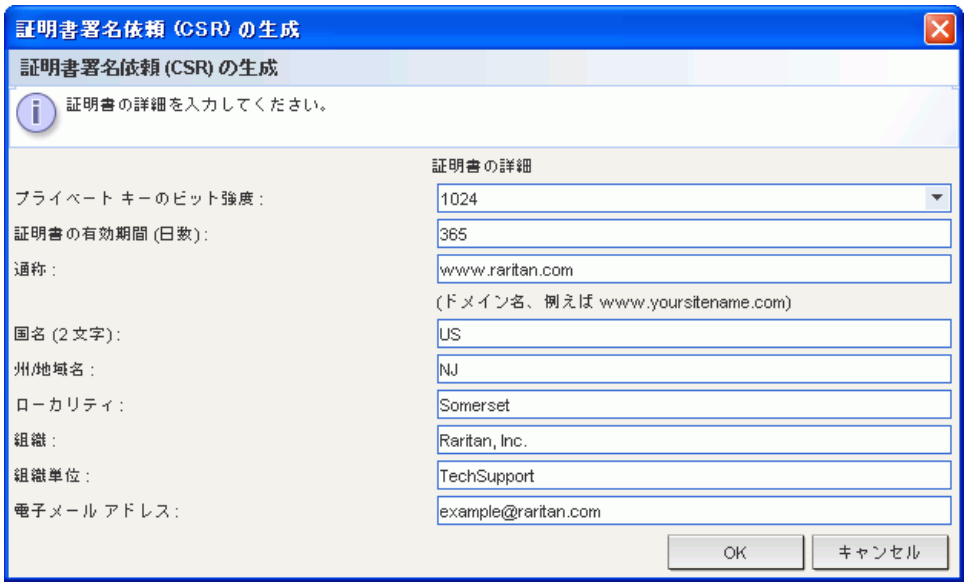


*図 172 自己署名証明書の生成 ウィンドウ*

## IP-ACL

この機能は、IP アドレスを基準にして CC-SG へのアクセスを制限します。 IP アドレスの範囲、その範囲が適用されるグループ、拒否/許可権限を入力して、IP アクセス制御リスト (IP-ACL) を指定します。

1. [**管理**] メニューで、[**セキュリティ**] をクリックします。[**セキュリティ マネージャ**] 画面が表示されます。

2. [**IP-ACL**] タブをクリックします。

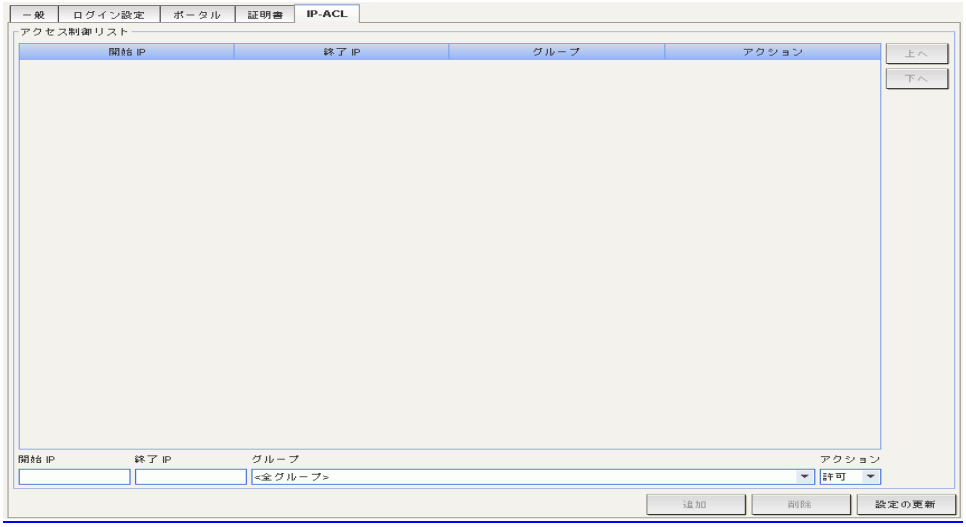


*図 173 セキュリティ マネージャの IP-ACL 画面*

3. [**アクセス制御リスト**] のライン アイテムの順序を変更するには、ライン アイテムを選択し、[**上へ**] または [**下へ**] をクリックします。ユーザの接続は、適用される最初のルール (上位から下位) に従って許可または拒否されます。
4. 新しいアイテムをリストに追加するには、[**開始 IP**] フィールドに開始 IP 値、[**終了 IP**] フィールドに終了 IP 値をそれぞれ入力して、ルールの適用範囲を指定します。
5. [**グループ**] ドロップダウン矢印をクリックし、ルールを適用するグループを選択します。
6. [**アクション**] ドロップダウン矢印をクリックし、グループの IP 範囲へのアクセスの [**許可**] または [**拒否**] を選択します。
7. [**追加**] をクリックして、[**アクセス制御リスト**] に新しいルールを追加します。
8. ライン アイテムを削除する場合は、該当するライン アイテムを選択して [**削除**] をクリックします。
9. [**設定の更新**] をクリックして、新しいアクセス制御ルールでシステムを更新します。

## 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。詳細についてはこの章の後の「タスク マネージャ」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 サーバを設定するには、以下の手順に従います。

1. [**管理**] メニューで、[**通知**] をクリックします。[**通知マネージャ**] 画面が表示されます。

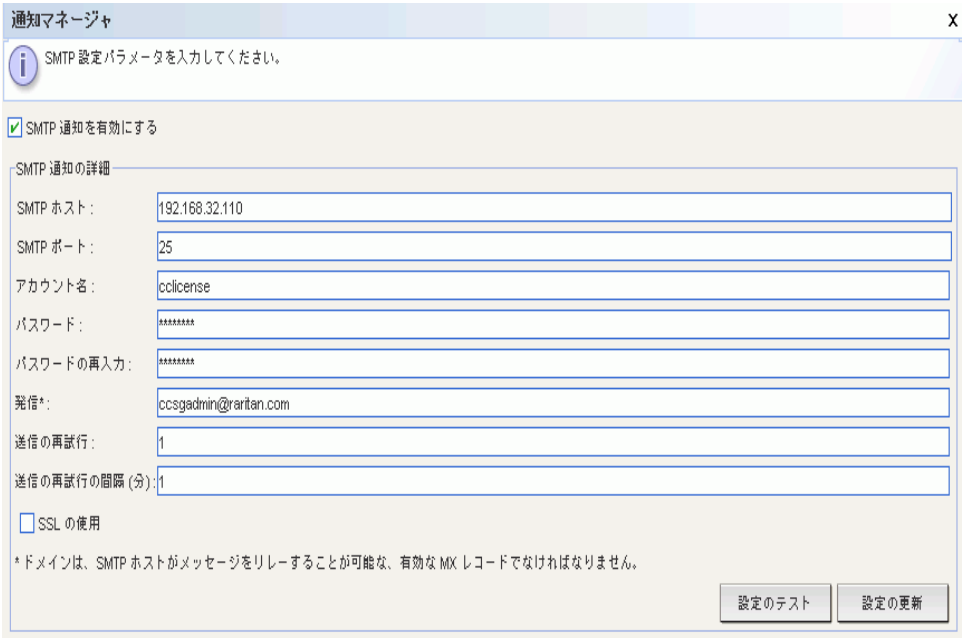


*図 174 通知マネージャ*

2. [**SMTP 通知を有効にする**] チェックボックスをオンにします。
3. [**SMTP ホスト**] フィールドに SMTP ホストを入力します。ホスト名のルールについては、「**第 1 章 : はじめに**」の「**用語/略語**」を参照してください。
4. 有効な SMTP ポート番号を [**SMTP ポート**] フィールドに入力します。
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。
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。
7. メッセージが CC-SG からのものであると分か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 画面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。

- 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）
- 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）このタスクをスケジュールする前に、そのファームウェアが利用可能になっている必要があります。
- CC-SG のバックアップ
- デバイスの再起動（デバイス グループには適用されません）
- アウトレット ポート パワー管理（電源オン/オフ/アウトレット ポートの再投入）
- すべてのレポートの生成（HTML または CSV 形式）
- ログの消去

## 連続したタスクのスケジュール

予測通りの動作が実行され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。

## 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と送信方法 (たとえば SSL によるセキュア送信) を指定できます。詳細は、この章の後の「通知マネージャ」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。

[**終了**] ステータスのすべてのレポートは CC-SG に 30 日間保存され、[**レポート**] メニューの [**スケジュールされたレポート**] を選択すると HTML 形式で表示できます。詳細は、「第 10 章：レポートの生成、スケジュールされたレポート」を参照してください。

## 新しいタスクの作成

新し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**] メニューで、[**タスク**] をクリックします。[**タスク マネージャ**] 画面が表示されます。

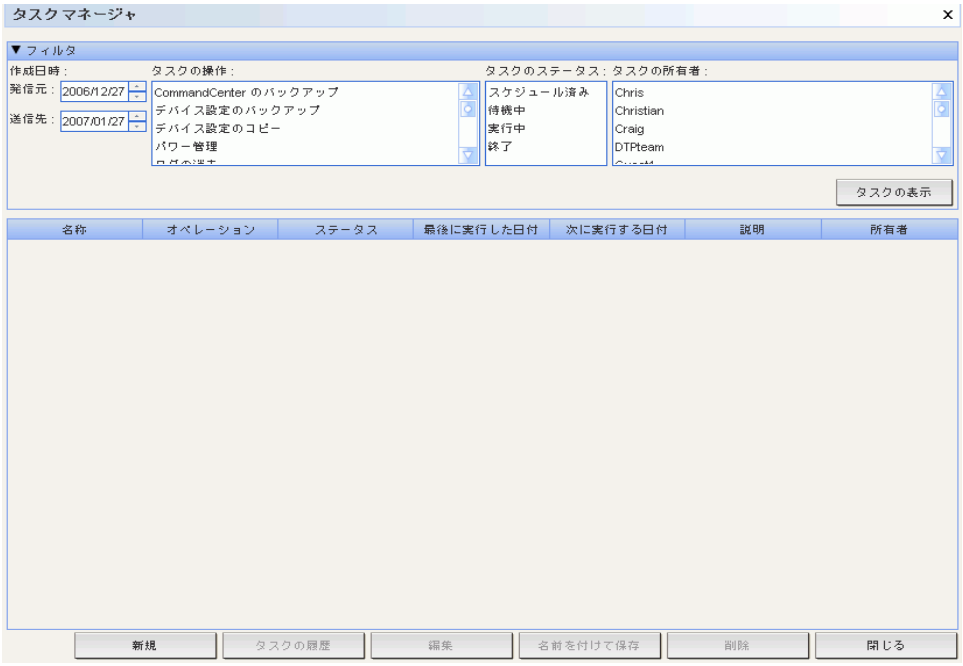


*図 175 タスク マネージャ*

2. [**新規**] をクリックします。
3. [**メイン**] タブで、タスクの名前 (半角英数字またはアンダースコアで 1 ～ 32 文字、スペース不可) と説明を入力します。
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 ([**デバイス ファームウェアのアップグレード**] など) をリストから選択します。 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。
6. [**再発**] タブをクリックします。
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。
   - **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。
   - **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。
   - **日単位 :** 毎週 7 日タスクを繰り返す場合は、[**毎日**] の横のラジオ 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**] の横のラジオ ボタンをクリックします。
   - **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オンにします。
   - **月単位 :** タスクが実行される日を [**日**] フィールドに入力し、タスクが実行される月の横のチェックボックスをオンにします。
   - **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**] セクションに追加します。 上下の矢印を使って**開始時刻**と**開始日**を選択します。

無限を指定してタスクを繰り返す場合は、[**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の繰り返しが停止する日を選択します。

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できます。 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。詳細は、「第 7 章: ユーザとユーザ グループの追加と管理」を参照してください。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、表示される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**] チェックボックスをオンにします。
13. [**OK**] をクリックしてタスクを保存します。

### タスク、タスクの詳細、タスクの履歴の表示

タスクを表示するには、以下の手順に従います。

1. [**管理**] メニューで、[**タスク**] をクリックします。[**タスク マネージャ**] 画面が表示されます。
2. タスクを検索するには、上下の矢印ボタンを使って、検索する日付の範囲を選択します。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。[**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。

- タスクを削除するには、そのタスクを選択して、[**削除**] をクリックします。

***注**：現在実行中のタスクを削除することはできません。*

- タスクの履歴を表示するには、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、タスクをダブルクリックします。
- 予定タスクを変更するには、タスクを選択し、[**編集**] をクリックして [**タスクの編集**] ウィンドウを開きます。必要に応じてタスク仕様を変更し、[**更新**] をクリックします。タブについては、この章の前の「**新しいタスクの作成**」を参照してください。
- 前に設定されたタスクに基づいて新しいタスクを作成するには、コピーするタスクを選択し、[**名前を付けて保存**] をクリックして [**タスクを名前を付けて保存**] ウィンドウを開きます。前に設定されたタスクから情報とともにタブも取り込まれます。必要に応じてタスクの仕様を変更し、[**更新**] をクリックします。タブについては、この章の前の「**新しいタスクの作成**」を参照してください。

***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。*

## CommandCenter NOC

設定に CommandCenter NOC (CC-NOC) を追加すると、シリアルおよび KVM ターゲット システムの監視機能、レポート機能、および警告サービスが搭載され、ターゲットの管理機能が拡大します。CC-

NOC のインストールと操作の詳細については、Raritan CommandCenter NOC のマニュアルを参照してください。

**重要 : 次の手順では、パスコードが生成されます。 このパスコードは CC-NOC 管理者に提供してください。CC-NOC 管理者は 5 分間以内に CC-NOC でそのパスコードを設定する必要があります。パスコードが自動システムによってインターセプトされることを防ぐため、電子メールやその他の電子的手段でパスコードを送信することは避けてください。 信頼できる関係者間で電話または書面でコードを交換する方が、自動インターセプトを効果的に防ぐことができます。**

## CC-NOC の追加

*注 : 有効な接続を作成するには、CC-NOC と CC-SG の両方で時間設定を同期させる必要があります。この同期を保つ上で最もよい方法は、共通の NTP (Network Time Protocol) サーバを使用することです。このため、NTP サーバを使用するよう CC-NOC と CC-SG を設定する必要があります。*

1. [**アクセス**] メニューで [**CC-NOC 設定**] をクリックします。[**CC-NOC 設定**] 画面が表示されます。
2. [**追加**] をクリックします。[**CC-NOC 設定の追加**] 画面が表示されます。
3. 追加する CC-NOC のソフトウェア バージョンを選択し、[**次へ**] をクリックします。バージョン 5.1 はバージョン 5.2 以降よりも統合機能が少なく、名前と IP アドレスの追加のみが必要となります。CC-NOC 5.1 の詳細は、www.raritan.com/support を参照してください。 [**Product Documentation**] をクリックして [**CommandCenter NOC**] を選択します。

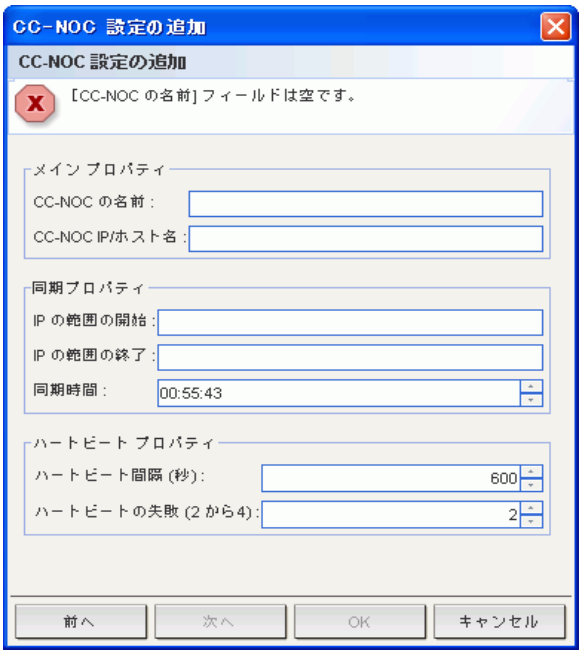


*図 176 CC-NOC 設定の追加画面*

4. [**名前**] フィールドに CC-NOC の記述的な名前を入力します。半角英数字で最大 50 文字で設定します。
5. [**CC-NOC IP/ホスト名**] フィールドに CC-NOC の IP アドレスまたはホスト名を入力します。これは必須フィールドです。ホスト名のルールについては、「**第 1 章 : はじめに**」の「**用語/略語**」を参照してください。
6. CC-NOC データベースからターゲット デバイスに関する毎日の情報を取得するには、[**IP の範囲の開始**] フィールドと [**IP の範囲の終了**] フィールドに検出範囲を入力します。この IP 範囲は、CC-SG が対象とするアドレスの範囲を表し、これらのデバイスのイベントを CC-SG に送信するように

CC-NOC に指示します。この範囲は、CC-NOC で設定されている検出範囲に関連しています。詳細は、Raritan の『**CommandCenter NOC 管理者ガイド**』を参照してください。次のルールに留意しながら範囲を入力します。

| IP アドレス範囲 | 説明 |
|---|---|
| **もしも**ここで入力する CC-SG 範囲が CC-NOC で設定した範囲のサブセットの場合 | CC-NOC はこの範囲内のターゲット デバイスについて得られる情報をすべて返します。 |
| **もしも**ここで入力する CC-SG 範囲が CC-NOC で設定した範囲の一部のリスト (非 null インターセクション) を含む場合 | CC-NOC は交差している範囲内のターゲット デバイスについて得られる情報をすべて返します。 |
| **もしも**ここで入力する CC-SG 範囲が CC-NOC で設定した範囲のスーパーセットの場合 | CC-NOC はこの範囲内のターゲット デバイスについて得られる情報をすべて返します。原則的に、CC-NOC は CC-NOC 範囲で定義されているターゲットを返します。 |
| **もしも**ここで入力する CC-SG 範囲が CC-NOC で設定した範囲と重ならない場合 | CC-NOC はターゲット デバイスの情報を一切返しません。 |

CC-NOC によるデバイスの監視を停止するには、デバイスを *管理対象外* とすることができます。詳細については、『**CommandCenter NOC 管理者ガイド**』を参照してください。

---

***注** : CC-NOC 同期レポートを使って CC-SG が登録しているターゲットを表示します。このレポートには、CC-NOC によって検出された新しいターゲットも表示されます。詳細は、「第 10 章 : レポートの生成」の「CC-NOC 同期レポート」を参照してください。*

---

7. [**同期時間**] で、CC-NOC データベースからターゲット情報を取得するスケジュールを指定します。これにより、ターゲットが検出されるか、管理対象外になると、データベースが更新されます。デフォルトは、クライアント マシンで設定されている現在の時刻です。同期操作が他のプロセスのパフォーマンスに影響しないようにするため、オフピーク時に同期をスケジュールすることをお勧めします。
8. [**ハートビート間隔**] には、CC-SG から CC-NOC にハートビート メッセージが送信される間隔を秒で設定します。ハートビート メッセージは、CC-NOC が稼動し利用可能な状態であることを確認します。デフォルトは **60** 秒です。有効な値は **30** ～ **120** 秒です。通常は、この値を変更する必要はありません。
9. [**ハートビートの失敗**] には、応答がない場合、CC-NOC のノードが使用不可と見なされるまでの連続ハートビート数を入力します。デフォルトは **2** 回です。有効な値は **2** ～ **4** 回です。通常は、この値を変更する必要はありません。
10. [**次へ**] をクリックします。

11. CC-NOC 管理者の場合は、パスコードをコピーして CC-NOC のフィールドに貼り付けます。管理者以外のユーザは、2 つのパスコードを CC-NOC 管理者に提出します。『**CommandCenter NOC Administrator Guide**』で説明しているように、CC-NOC 管理者はユーザから受け取ったパスコードを CC-NOC に入力し、セキュリティ証明書の交換を開始します。

**重要 : セキュリティ上の配慮から、CC-SG でパスコードが生成された後 5 分以内に CC-NOC にパスコードを入力する必要があります。 これにより、侵入者が brute-force (総当り) 攻撃でシステムを侵害する可能性を最小限に抑えることができます。 パスコードが自動システムによってインターセプトされることを防ぐため、電子メールやその他の電子的手段でパスコードを送信することは避けてください。 信頼できる関係者間で電話または書面でコードを交換する方が、自動インターセプトを効果的に防ぐことができます。**

12. 証明書の交換プロセスが完了すると、CC-NOC と CC-SG の間にセキュアなチャンネルが確立されます。CC-NOC データが CC-SG にコピーされます。[**OK**] をクリックして、プロセスを完了します。プロセスが 5 分以内に完了しないと、そのプロセスはタイムアウトになり、データは CC-SG に保存されず、保存された証明書はすべて削除されます。191 ページの「**CC-NOC の追加**」の手順 1 からやり直してください。

***注 :** CommandCenter NOC は、スタンドアロンまたはプライマリ ノードの CC-SG サーバにのみ追加できます。*

## CC-NOC の編集

1. [**アクセス**] メニューで [**CC-NOC 設定**] をクリックします。[**CC-NOC 設定**] 画面が表示されます。
2. リストから CC-NOC をハイライトして [**編集**] をクリックします。[**CC-NOC 設定の編集**] 画面が表示されます。
3. 必要に応じて設定を変更します。その他の情報フィールドについては、前の「**CC-NOC の追加**」を参照してください。

## CC-NOC の起動

CC-SG から CC-NOC を起動するには、以下の手順に従います。

1. [**アクセス**] メニューで [CC-NOC 設定] をクリックします。
2. [**CC-NOC 設定**] 画面で、利用可能な CC-NOC を選択します。
3. [**起動**] をクリックします。設定済みの CC-NOC ユニットに接続します。

## CC-NOC の削除

CC-SG から CC-NOC を削除して登録解除するには、以下の手順に従います。

1. [**アクセス**] メニューで [**CC-NOC 設定**] をクリックします。[**CC-NOC 設定**] 画面が表示されます。
2. CC-SG から削除する CC-NOC を選択して、[**削除**] をクリックします。削除を確認するプロンプトが表示されます。
3. [**はい**] をクリックして、CC-NOC を削除します。「**CC-NOC が正常に削除されました**」というメッセージが表示され、CC-NOC が削除されたことを確認します。

## CC-SG への SSH アクセス

CC-SG の SSH (v2) サーバのコマンドライン インタフェースへのアクセスには、Putty または OpenSHH クライアントなどのセキュア シェル (SSH) クライアントを使用します。 CC-SG コマンドのサブセットのみが SSH から提供され、デバイスと CC-SG 自体を管理します。

SSH クライアントのユーザは CC-SG で認証されます。このとき、既存の認証および承認ポリシーが SSH クライアントに適用されます。 SSH クライアントで利用できるコマンドは、その SSH クライアント ユーザが属しているユーザ グループの許可に応じて決定されます。

SSH を使って CC-SG にアクセスしている管理者は、CC スーパーユーザ SSH ユーザをログアウトすることはできませんが、システム管理者を含むその他すべての 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 アドレスを入力し、ポートに「**22**」を指定して、接続を開きます。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。詳細については、この章の前の「セキュリティ マネージャ」を参照してください。
3. プロンプトが表示されたら、CC-SG ユーザ名とパスワードを使ってログインします。
4. シェル プロンプトが表示されます。「**ls**」と入力して利用可能なすべてのコマンドを表示します。「**?**」または「**help**」と入力すると、すべてのコマンドについて入力する際の説明と形式が表示されます。

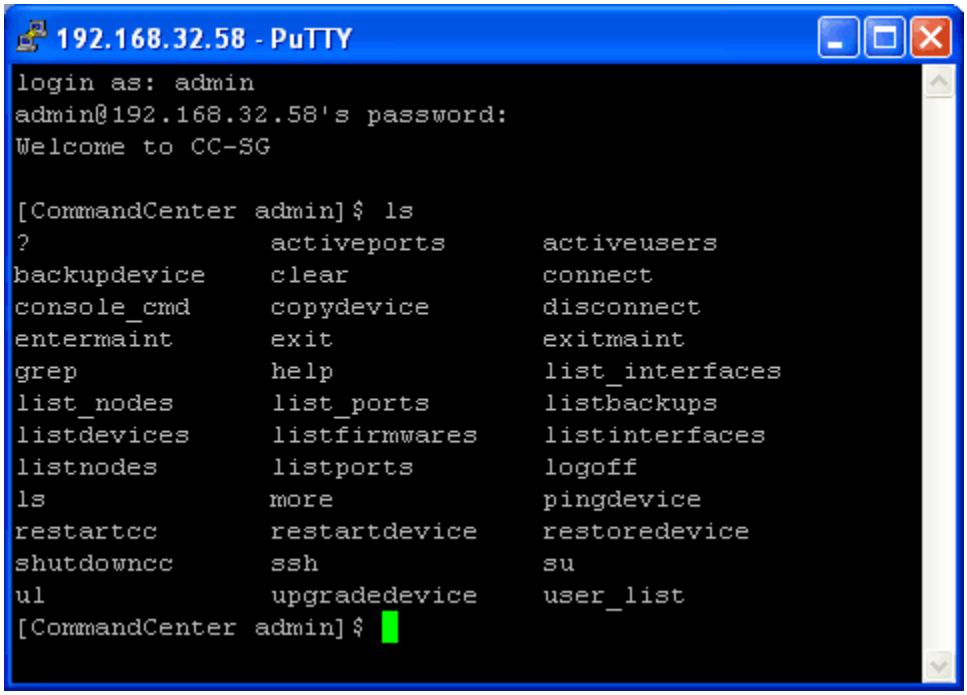


*図 177 SSH を介した場合の CC-SG コマンド*

## SSH コマンド

以下の表では、SSH で利用可能なすべてのコマンドについて説明します。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。

| コマンド<br>説明 |
|---|
| **activeports**<br>アクティブ ポートをリストします。 |
| **activeusers**<br>アクティブ ユーザをリストします。 |
| **backup device <[-host <host>] \| [-id <device_id>]> backup_name [description]**<br>デバイス設定をバックアップします。 |
| **clear**<br>画面をクリアします。 |
| **connect [-d <device_name>] [-e <escape_char>] <[-i <interface_id>] \| [-n <port_name>] \| [port_id]>**<br>シリアル ポートとの接続を確立します。 <port_name> または <device_name> にスペースが入っている場合は、引用符で囲みます。 |
| **copydevice <[-b <backup_id>] \| [source_device_host]> target_device_host**<br>デバイス設定をコピーします。 |
| **disconnect <[-u <username>] [-p <port_id>] [-id <connection_id>]>**<br>ポート接続を閉じます。 |
| **entermaint minutes [message]**<br>CC-SG をメンテナンス モードにします。 |
| **exitmaint**<br>CommandCenter のメンテナンス モードを終了します。 |
| **grep search_term**<br>パイプ出力ストリームからテキストを検索します。 |
| **help**<br>ヘルプ画面を表示します。 |
| **listbackups <[-id <device_id>] \| [host]>**<br>利用可能なデバイス設定バックアップをリストします。 |
| **listdevices**<br>利用可能なデバイスをリストします。 |
| **listfirmwares [[-id <device_id>] \| [host]]**<br>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します。 |
| **listinterfaces [-id <node_id>]**<br>すべてのインタフェースをリストします。 |
| **listnodes**<br>すべてのノードをリストします。 |
| **listports [[-id <device_id>] \| [host]]**<br>すべてのポートをリストします。 |
| **logoff [-u <username>] message**<br>ユーザをログオフします。 |
| **ls**<br>コマンドをリストします。 |

| |
|---|
| **more [-p <page_size>]**<br>ページングを行います。 |
| **pingdevice <[-id <device_id>] \| [host]>**<br>デバイスを Ping します。 |
| **restartcc minutes [message]**<br>CC-SG を再起動します。 |
| **restartdevice <[-id <device_id>] \| [host]>**<br>デバイスを再起動します。 |
| **restoredevice <[-host <host>] \| [-id <device_id>]> [backup_id]**<br>デバイス設定をリストアします。 |
| **shutdowncc minutes [message]**<br>CC-SG をシャットダウンします。 |
| **ssh [-e <escape_char>] <[-id <device_id>] \| [host]>**<br>SX デバイスとの SSH 接続を開きます。 |
| **su [-u <user_name>]**<br>ユーザを変更します。 |
| **upgradedevice <[-id <device_id>] \| [host]>**<br>デバイス ファームウェアをアップグレードします。 |
| **exit**<br>SSH セッションを終了します。 |

コマンドを入力して「**–h**」スイッチを付けると（例「**listfirmwares –h**」）、そのコマンドのヘルプが表示されます。

## コマンドのヒント

SSH コマンドについて留意すべき点を説明します。

- 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、「**第 1 章：はじめに**」の「用語/略語」を参照してください。
- copydevice コマンドと restartdevice コマンドは、Dominion SX. IPMI などの一部の Raritan デバイスにのみ適用します。IPMI サーバ、汎用デバイスはこれらのコマンドではサポートされていません。

## SX デバイスへの SSH 接続の作成

SX デバイスに管理操作を実行するために SSH 接続を作成することができます。接続後は、その SX 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、対象の SX 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. SX が CC-SG に追加されていることを確認するため、「**listdevices**」と入力します。

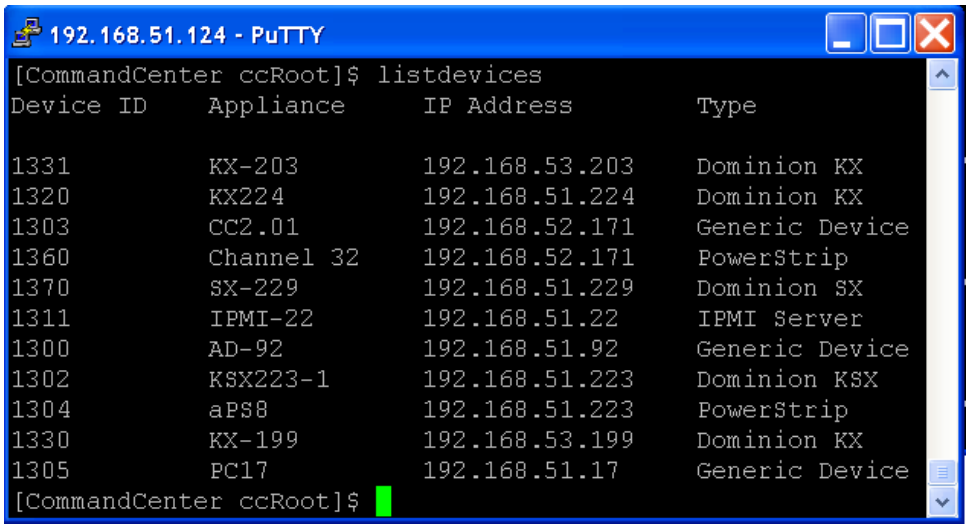


*図 178 CC-SG のデバイスのリスト*

2. 「**ssh -id <device id>**」と入力して、SX デバイスに接続します。たとえば、上の画面では「**ssh –id 1370**」と入力することで SX-229 に接続できます。

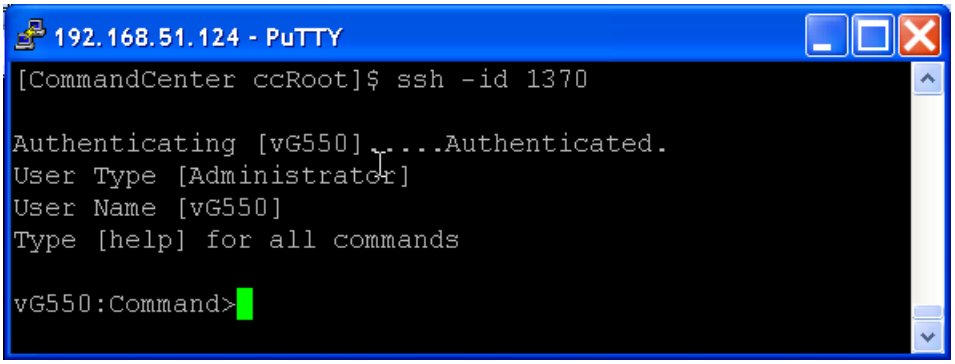


*図 179 SSH による SX デバイスへのアクセス*

## 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。

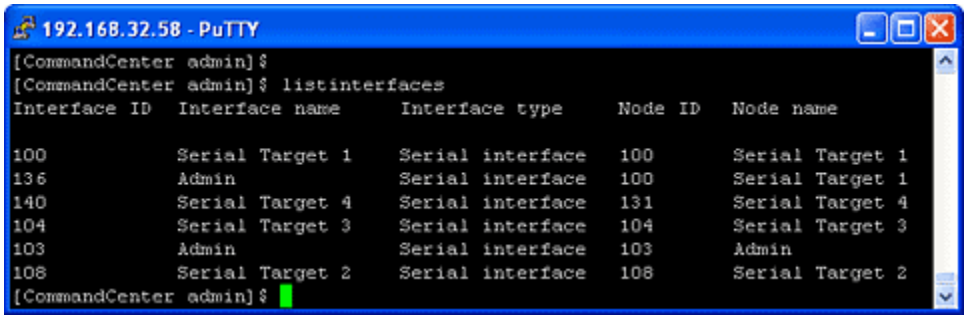


*図 180 SSH でのインタフェースのリスト*

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。

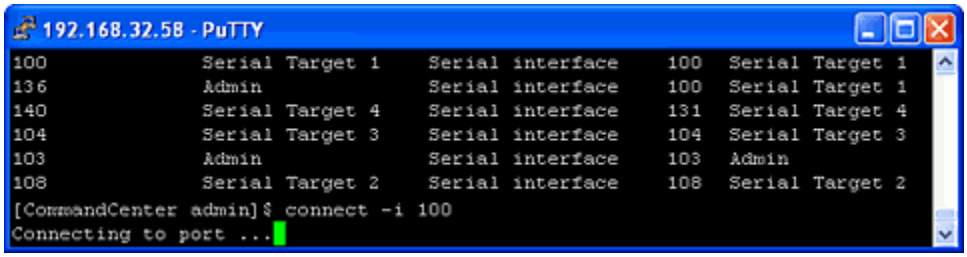


*図 181 シリアル アウト オブ バンド インタフェース経由でノードに接続*

3. ノードに接続されたら、‘~’ とドット ‘.’ からなるデフォルトのエスケープ キーを入力します。表示されるプロンプトで、下に説明するように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。 |
| **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。 |

## セッションの終了

CC-SG への SSH 接続全体を終了するには、「**exit**」と入力します。

# Diagnostic Console

Diagnostic Console は、CC-SG へのローカル アクセスを提供する標準の非グラフィカル インタフェースです。 Diagnostic Console にはシリアル ポートまたは KVM ポートから、あるいは Putty または OpenSSH Client などのセキュア シェル (SSH) クライアントからアクセスできます。

2 つのログインが提供されています。1 つは **status** で、Status Console へのアクセスを可能にします。もう 1 つは **admin** で、Administrator Console へのアクセスを可能にします。 すべてのログイン ユーザ名とパスワードで大文字と小文字が区別されます。

## Status Console について

デフォルトの設定では、Status Console はパスワードを必要としません。［*ログイン*］プロンプトに「**status**」と入力すると、現在のシステム情報が表示されるので、この情報を使って 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。

## Administrator Console について

Administrator Console のデフォルトのユーザ名/パスワードは **admin**/**raritan** です。**admin** アカウントでは、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。 Diagnostic Console の **admin** アカウントは別個のものであり、CC-SG 管理者の Director Client および HTML ベースの Access Client で使用される **admin** アカウントおよびパスワードとは区別されます。ただし、両方のアカウントに同じパスワードを使用しても、別のパスワードを使用してもかまいません。 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。

***注** : SSH から Diagnostic Console にアクセスしている場合、Status Console と Administrator Console には、お使いの SSH クライアントで設定されている表示設定とキーボードのバインドが使用されますが、場合によってはこれらが部分的に本書の説明と一致しないこともあります。*

## VGA/キーボード/マウス ポートからの Diagnostic Console 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. ビデオ モニタが信号を検出し、キーボードで <CR> または <Return> を入力すると、次のように画面にログイン プロンプトが表示されます。

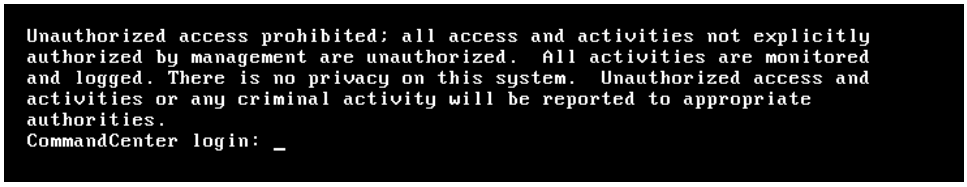


*図 182 Diagnostic Console へのログイン*

## SSH による Diagnostic Console 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 (CC-SG が DNS サーバに登録されている場合) を指定し、ポートに **23** を指定します。
3. 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 へのアクセス

Status Console へのアクセスにパスワードは必要ありませんが、パスワードの使用を義務付けることができます。

1. ログイン プロンプトに「**status**」と入力します。読み取り専用の Status Console が表示されます。

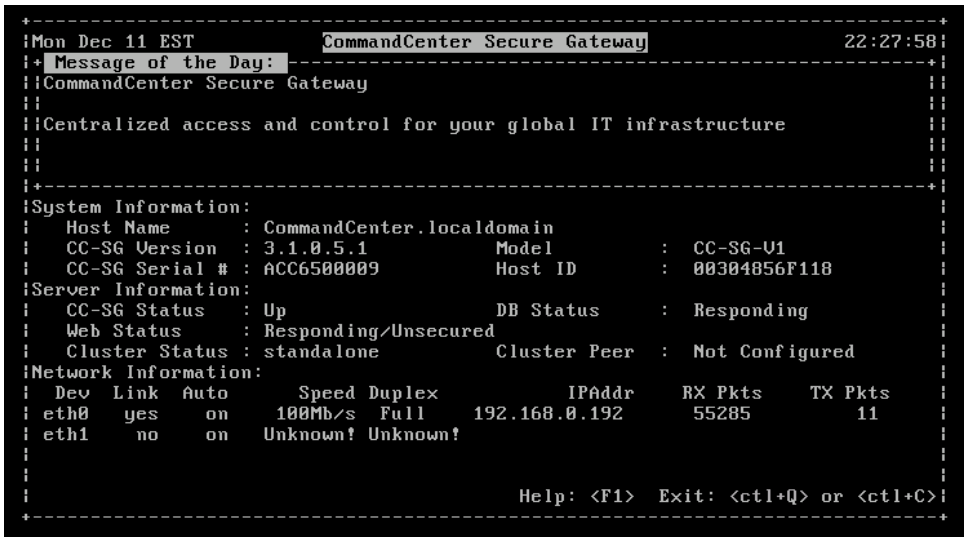


*図 183 Status Console*

- 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。
- 画面右上に表示される時刻は、最後に CC-SG データがポーリングされた時間です。
- この画面の情報はほぼ 5 秒ごとに更新されます。
- 「**CTRL-L**」と入力すると、現在の画面がクリアされて、更新された情報が表示されます。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、画面が終了します。
- Status Console では他の入力を行ったり、画面ナビゲーションは行えません。他の入力はすべて無視されます。

以下の表では、CC-SG および CC-SG データベースのステータスについて説明しています。

| ステータス | 説明 |
|---|---|
| **CC-SG ステータス : Up** | CC-SG は利用可能です。 |
| **CC-SG ステータス : Down** | CC-SG はリブート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。 |
| **CC-SG ステータス : Restarting** | CC-SG は再起動中です。 |
| | |
| **DB ステータス : Responding** | CC-SG のデータベースは利用可能です。 |
| **DB ステータス : Down** | CC-SG はリブート中である可能性があります。 |

## Administrator Console へのアクセス

*注 : Administrator Console に表示される情報はすべて静的です。CC-SG GUI または Diagnostic Console 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 にログインしなおす必要があります。*

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。パスワード強度の設定については、この章の後の「**Diagnostic Console のパスワード (Admin)**」を参照してください。
3. Administrator Console メイン画面が表示されます。システム ネットワーク インタフェースの初期設定、ステータス ウィンドウの [今日のメッセージ] の編集、ログ ファイルの表示などの操作を行うことができます。[**File**] メニューには、次のように Administrator Console の終了方法が表示されます。

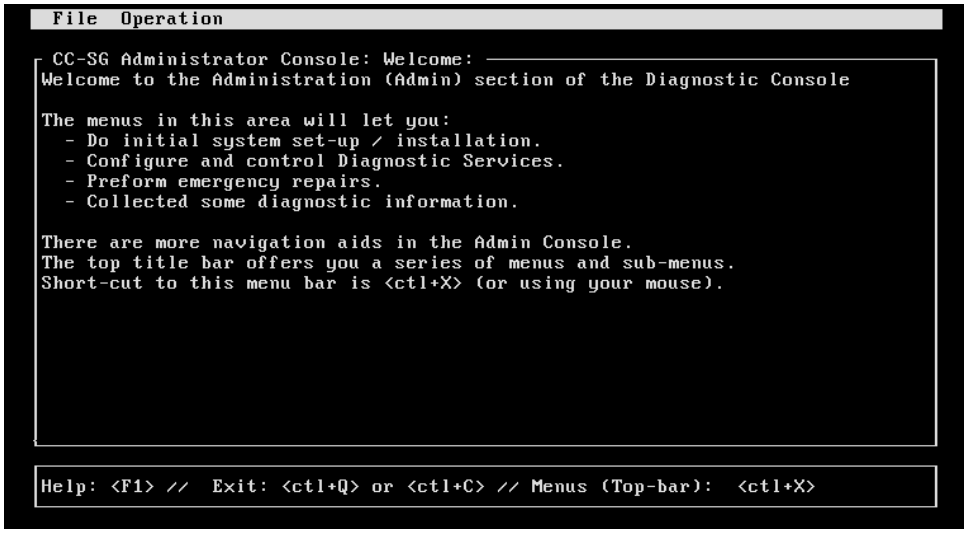


*図 184 Administrator Console*

### Administrator Console のナビゲート

以下の表には、Diagnostic Console でのさまざまなナビゲーション手段が示されています。一部のセッション (特に SSH) では、マウスを使ってさまざまなフォームを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+C** または **CTRL+Q** | Diagnostic Console 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。 |
| **SPACE** | 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。 |
| マウス | 使用可能な場合、オプションをポイントして選択できます。 |

### Diagnostic Console での制限付きサービス使用条件および今日のメッセージの編集

制限付きサービス使用条件 (RSA) メッセージは、Administrator Console でログイン ユーザ名を入力した後、パスワードを入力する前に表示されます。今日のメッセージ (MOTD) は Status Console の一番上に表示されます。

1. RSA メッセージ (Diagnostic Console ではログイン前メッセージ) または MOTD メッセージを編集するには、[**Operation**]、[**Diagnostic Console Config**] の順にクリックして、[**Edit Pre-Login Message**] または [**Edit MOTD**] をクリックします。
2. **Delete** キーと **Backspace** キーを使い、ボックスに新しいメッセージを入力します。MOTD の場合、半角で 76 文字まで入力できます。

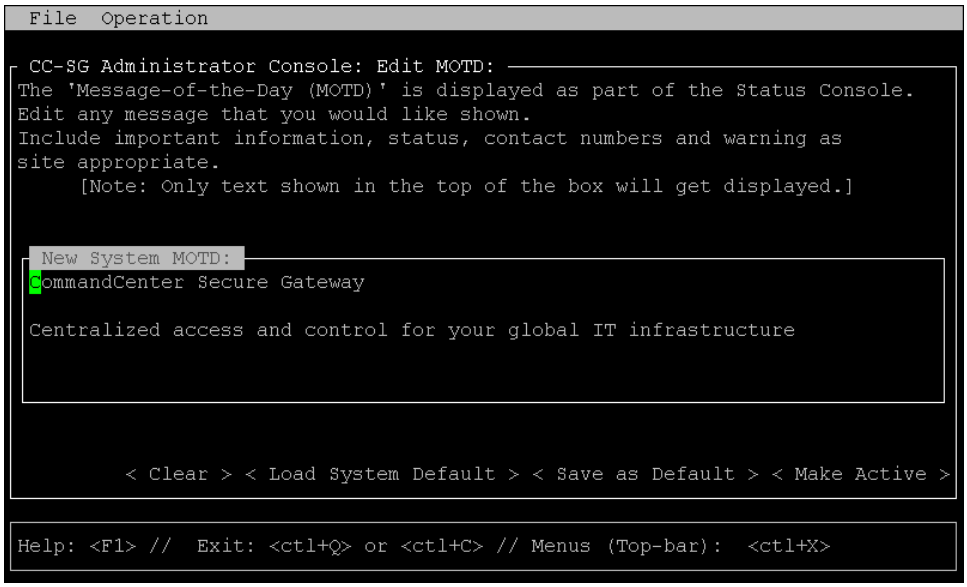


*図 185 Status Console の MOTD の編集*

3. 画面の下部の [**Make Active**] をクリックするか、[**Make Active**] が選択されるまで、**TAB** キーを押し、Space キーを 1 回押します。

ログイン前のメッセージおよび今日のメッセージには 3 つの別々のバッファまたは領域があります。

- Admin Console 画面 – 最初に Active Message バッファのコピーが表示されます。このユーザ/セッションによって編集できます。
- 原型メッセージまたはモデル メッセージが入っており、システムのリセットの間にも保持される System Buffer。
- Active Message バッファ（ユーザがシステムに操作を行う際に表示されます）。システムの再起動およびリブート間でも保存されます。

| ボタン | 説明 |
|---|---|
| **Clear** | 現在表示されている Admin Console 画面のテキストをすべて削除します。システムが使用する値には影響しません。 |
| **Load System Default** | Admin Console 画面を System Buffer の内容に置き換えます。 |
| **Save as Default** | Admin Console 画面の現在の表示内容を System Buffer に入れます。Active Message 表示には影響しません。 |
| **Make Active** | 現在の Active Message を Admin Console 画面の内容に置き換えます。すべての新しいユーザに新しいメッセージが表示されます。 |

### Diagnostic Console 設定の編集

Diagnostic Console は、シリアル ポート (COM1)、VGA/キーボード/マウス (KVM) ポート、またはセキュア シェル (SSH) クライアントからアクセスできます。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 Diagnostic Console 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。

Diagnostic Console 設定を編集するには、次の手順に従います。

1. [**Operation**]、[**Diagnostic Console Config**]、[**Diagnostic Console Service**] の順にクリックします。
2. クリックするか、**TAB** キー 、↓↓ キー、**Enter** キーを使って、Diagnostic Console の設定およびアクセス方法を決定します。Diagnostic Console には、シリアル ポート (COM1)、KVM コンソール、SSH (IP ネットワーク) という 3 つのアクセス メカニズムがあります。Diagnostic Console には 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。
3. Diagnostic Console 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。

**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。**

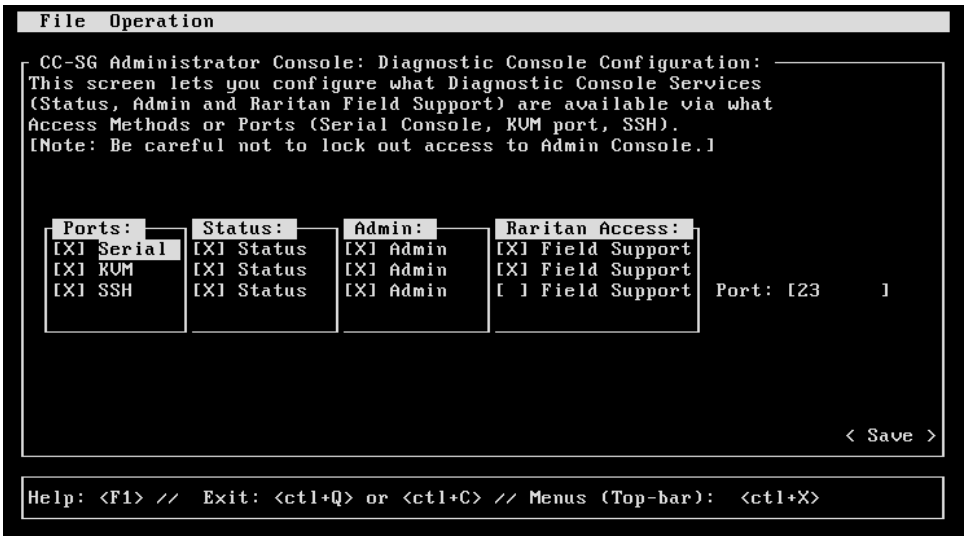


*図 186 Diagnostic Console 設定の編集*

4. 画面の下部の [**Save**] をクリックするか、**TAB** キーを押して [**Save**] を選択し、**Enter** キーを押します。

### ネットワーク インタフェース設定の編集 (Network Interfaces)

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。マウス クリックまたは TAB キーと矢印キーでナビゲートします。Enter キーを押して値を選択します。

1. ネットワーク インタフェース情報を編集するには、[**Operation**]、[**Network Interfaces**] の順にクリックし、[**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 GUI (管理者の Director 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。ここで次のようなデフォルトの [**Network Interface Configuration**] 画面が表示されます。

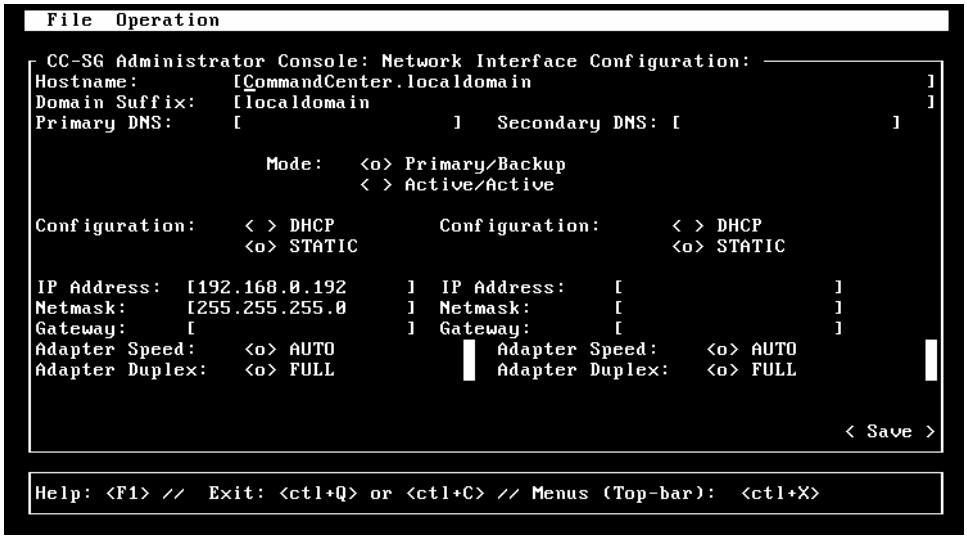


*図 187 ネットワーク インタフェースの編集*

3. ホスト名を [**Host Name**] 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、「**第 1 章：はじめに**」の「**用語/略語**」を参照してください。
4. [**Mode**] フィールドでは、[**Primary/Backup Mode**] または [**Active/Active Mode**] のいずれかを選択します。 詳細は、この章の前の「**ネットワーク設定**」を参照してください。 **TAB** キーを押してフィールドを選択し、矢印キーを押して 2 つのモードから選択します。 モードを選択するには、**Space** キーを押します。
5. クリックまたは **TAB** キーで [**Configuration**] フィールドに移動し、リストから [**DHCP**] か [**Static**] のいずれかを選択します。
   - [**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** ([**IP Address**]) (必須)、**ネットマスク** ([**Netmask**]) (必須)、**デフォルトのゲートウェイ** ([**Gateway**]) (オプション)、**プライマリ DNS** ([**Primary DNS**]) (オプション)、**セカンダリ DNS** ([**Secondary DNS**]) (オプション)、**ドメイン接尾辞** ([**Domain Suffix**]) 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. **TAB** キーまたはクリックで [**Adapter Speed**] に移動し、↓↓ キーを使ってリストから回線速度を選択します。スクロール リストに 10、100 という他の値と 1000 Mbps (一度に表示される値は 1 つだけ) があります。必要に応じて、↓↓ キーを使って値を表示し、**Space** キーで選択する値を切り替えることができます。
7. [**Adapter Speed**] に [**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、↓↓ キーを使ってリストから二重モード (**FULL** または **HALF**) を選択します。二重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. [**Active/Active Mode**] 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. [**Save**] をクリックして、変更を保存します。CC-SG が再起動され、すべての CC-SG GUI ユーザがログオフされ、そのセッションが終了されます。 **警告の**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**] をクリックして続けます。
10. システム操作の進行状態は、Diagnostic Console のステータス画面で監視できます。KVM ポートの場合、**ALT+F2** キーを使い、**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** で元のターミナル セッションに戻ることができます。**F1** ～ **F6** で 6 つのターミナル セッションを利用できます。 SSH アクセスの場合、ネットワークの再設定で接続が許可されていれば、クライアントから別の SSH セッションを起動し、**status** としてログインできます。

### IP アドレスの Ping (Network Interfaces)

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。問題があると想定する前に、ターゲットと介在するネットワークで Ping か許可されているかを確認してください。***

1. [**Operation**]、[**Network Interfaces**]、[**Ping**] の順にクリックします。
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. オプションとして次を選択します。

| 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 オプションが設定されます。 |
| 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. オプションで、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 (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) 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。
5. ウィンドウの右下の [**Ping**] をクリックします。 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どこかに障害が発生しています。 この場合は、次の手順で traceroute を実行します。次のセクション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。システムは “**Return?**” のプロンプトを表示してから、Diagnostic Console に戻ります。これで適宜出力を表示して分析できます。

***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 (Network Interfaces)

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**] の順にクリックします。
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. オプションとして次を選択します。

| 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. オプションとして、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)、プローブに使用する 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。
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 (Network Interfaces)

**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と、実際にネットワークのパフォーマンスが向上する場合もあり、これにより重要なビジネス 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ます。また、各インタフェースが別々の IP ドメインに接続しているアクティブ/アクティブ モードのネットワーク設定においても有効です。詳細は、「第 12 章 : 高度な管理」の「ネットワーク設定」を参照してください。 マウスでクリックするか、**TAB** キー、↓↓ キーで移動して **Enter** キーで値を選択します。

静的ルートを表示または変更するには、以下の手順に従います。

1. [**Operation**]、[**Network Interfaces**]、[**Static Routes**] の順にクリックします。
2. 現在の IP ルーティング テーブルが表示されます。 ホストまたはネットワーク ルートを追加したり、ルートを削除できます。 **[Refresh]** ボタンをクリックすると、上のテーブルのルーティング情報が更新されます。

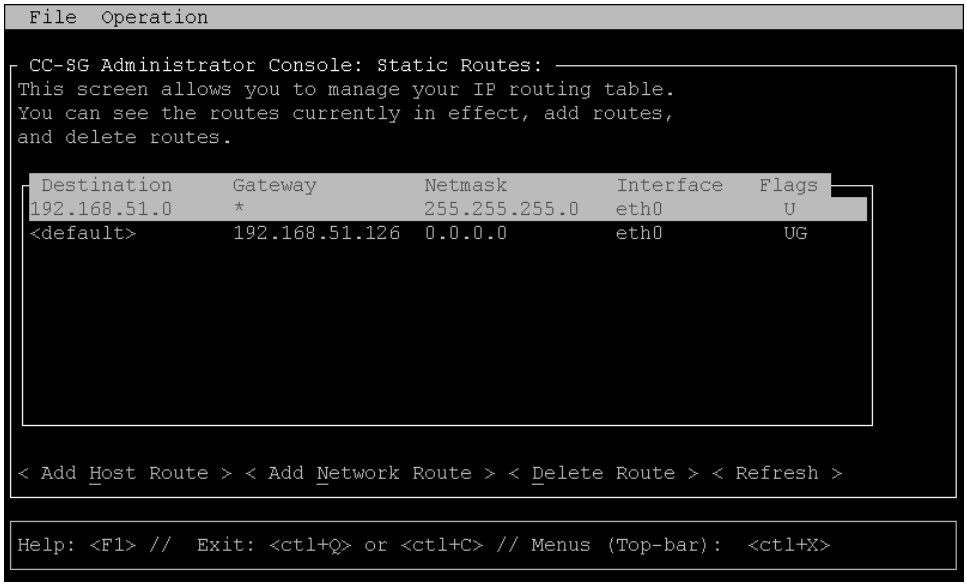


*図 188 静的ルートの編集*

### ログ ファイルの表示 (Admin)

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 ファイルを表示するには、以下の手順に従います。

1. [**Operation**]、[**Admin**]、[**System Logfile Viewer**] **の順にクリックします。**
2. [**Logviewer**] 画面は主に次の 4 つの領域に分かれています (以下の画面参照)。
   - 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 (以下を参照)。
   - 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、Space キーを押してログ 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。

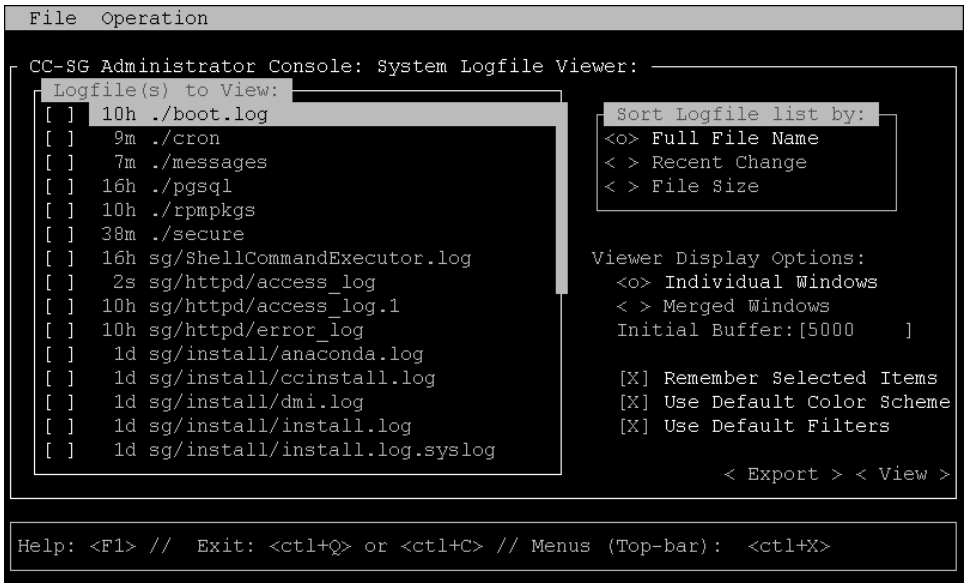


*図 189 表示するログ ファイルの選択*

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 (たとえばユーザが ログファイル リスト領域に入った) 場合、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。タイムスタンプは s = 秒、m = 分、h = 時、d = 日となっています。ファイル サイズは B = バイト、K = キロ (1000) バイト、M = メガ (1,000,000) バイト、G = ギガバイトとなっています。 並び替えオプションが絶対名または変更日である場合は、タイムスタンプが使用され、ファイル サイズの場合はファイル サイズが使用されます。

[**Sort Logfile list by**] ウィンドウは、ラジオ ボタンのセット (必ず 1 つのみ選択状態となる) があり、[**Logfile to View**] ウィンドウでのログファイルの表示順序を制御します。

| オプション | 説明 |
|---|---|
| Individual Windows | 別のサブウィンドウが開いて選択したログが表示されます。 |
| Merged Windows | 選択したすべてのログ ファイルが 1 つの表示ウィンドウにマージされます。 |
| Initial Buffer | 初期バッファまたは履歴のサイズを設定します。 デフォルトは **5000** です。 このシステムは、新しく入ってきたすべての情報をバッファするように設定されています。 |
| Remember Selected Items | このボックスを選択すると、現在のログファイルの選択情報があれば記憶されます。 選択しないと、新しいログファイル リストが生成されるたびに、選択がリセットされます。 これは、複数のファイルを通して確認したい場合に便利です。 |
| Use Default Color Scheme | このボックスを選択すると、一部のログファイルが標準配色で表示されます。 注：multitail コマンドを使用すると、表示中であっても、ログファイルの配色を変更できます。 |
| Use Default Filters | このボックスを選択すると、一部のログファイルに自動フィルタが適用されます。 |
| 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] とともにに選択した場合、次のような LogViewer が表示されます。

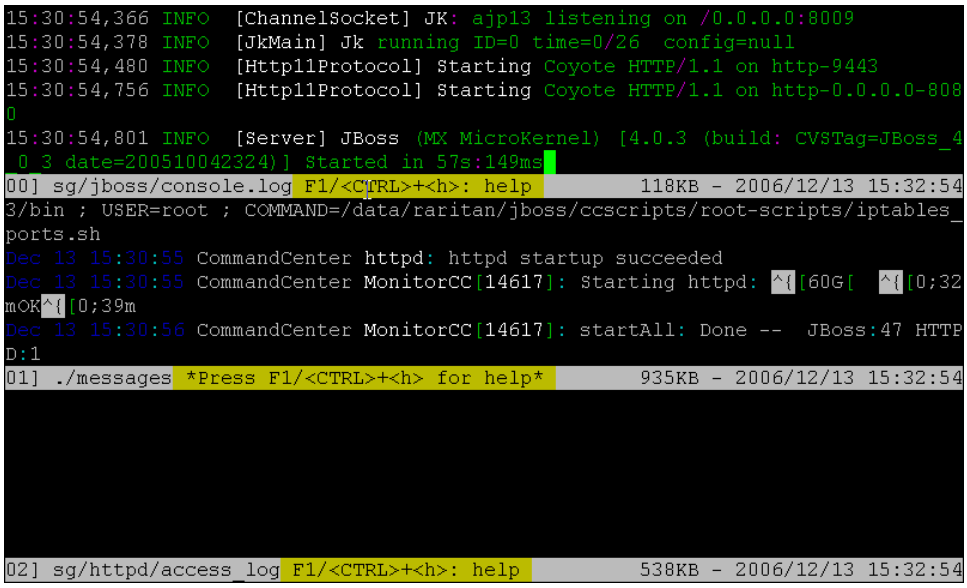


*図 190 表示するログ ファイルの選択*

4. 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。
5. 必要に応じて、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、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。

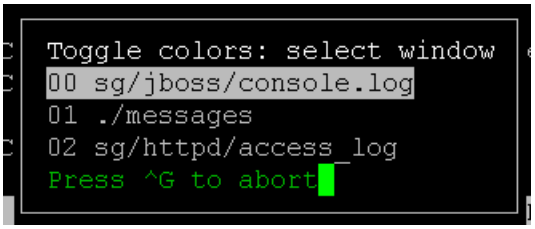


*図 191 ログ ファイルの色の変更*

6. 「**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 ロードはこの 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。*

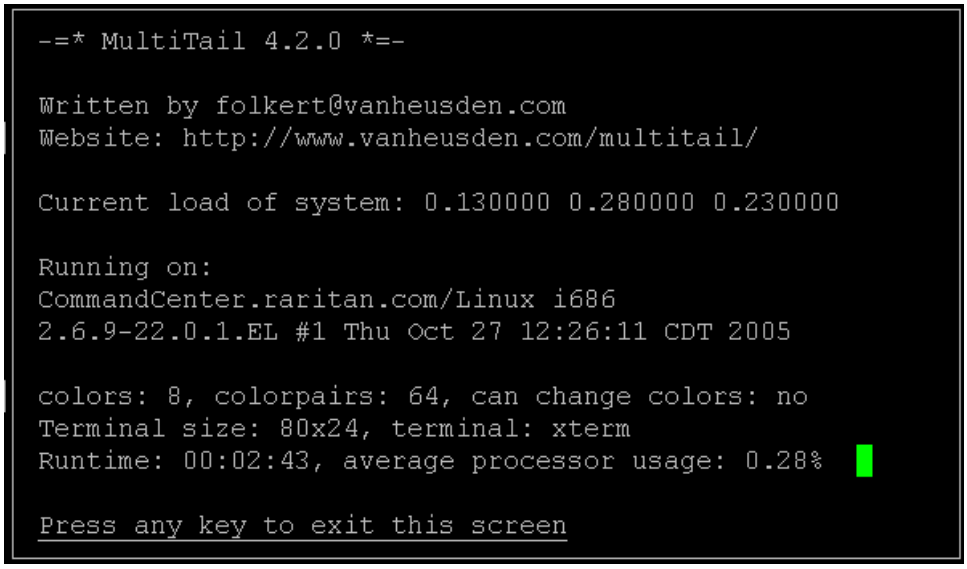


*図 192 情報の表示*

7. 必要に応じて、正規表現でログ ファイルをフィルタできます。 正規表現を追加または編集するには「**e**」と入力し、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。

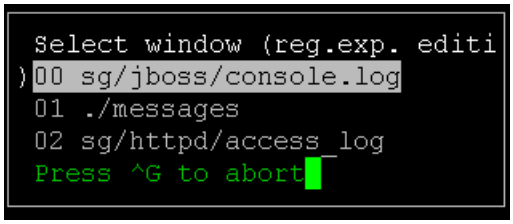


*図 193 ログ ファイルへの正規表現の追加*

8. 正規表現を追加するには「**a**」と入力します。 たとえば、**sg/jboss/console.log** ログ ファイルの **WARN** 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。*


*図 194 ログ ファイルの正規表現の指定*

9. LogViewer のすべてのオプションについてのヘルプを表示するには **F1** キーを押します。 **CTRL+C** キーおよび **CTRL+Q** を押すと、この LogViewer セッションが終了します。

### CC-SG の再起動 (Admin)

CC-SG を再起動することができます。これにより、現在の CC-SG ユーザがすべてログ オフされ、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 Diagnostic Console で再起動しなければならない場合以外は、CC-SG GUI から CC-SG を再起動することを強く推奨します。詳細は、「第 11 章 : システム メンテナンス」の「CC-SG を再起動します。」を参照してください。 Diagnostic Console から CC-SG を再起動した場合、CC-SG GUI のユーザには再起動している ことは通知されません。**

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**] の順にクリックします。
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。

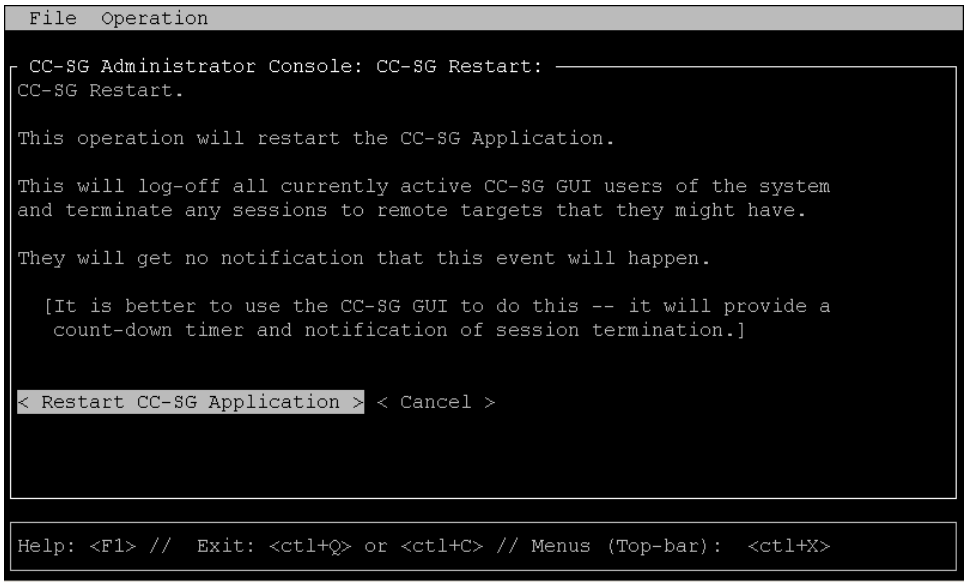


*図 195 Diagnostic Console からの CC-SG の再起動*

### CC-SG のリブート (Admin)

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、Diagnostic Console 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。

CC-SG をリブートするには、次の手順に従います。

1. [**Operation**]、[**Admin**]、[**CC-SG System Reboot**] の順にクリックします。
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。

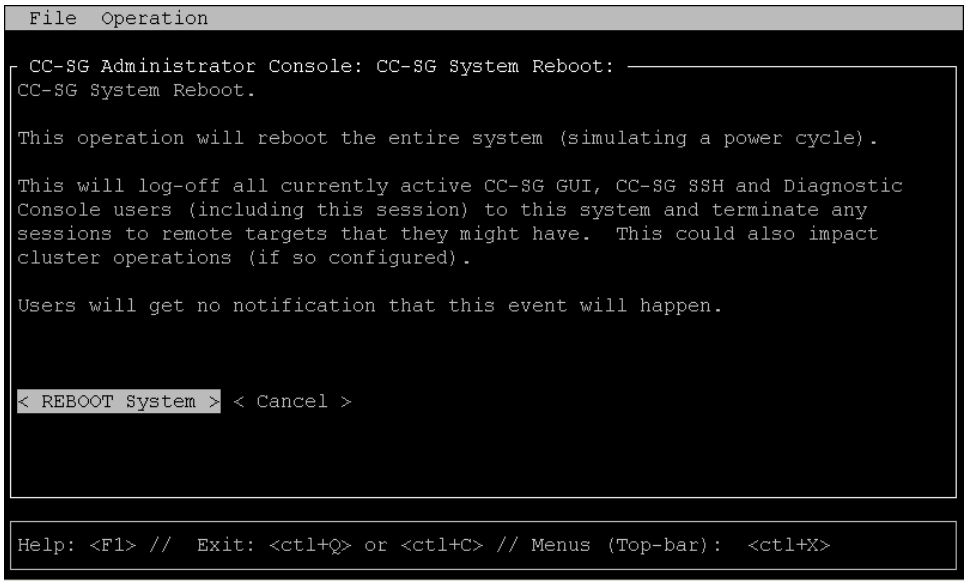


*図 196 Diagnostic Console からの CC-SG のリブート*

### CC-SG システムの電源オフ (Admin)

このオプションでは、CC-SG 全体の電源がオフになります。ユーザに通知は表示されません。CC-SG、SSH、Diagnostic Console 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**] の順にクリックします。
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。

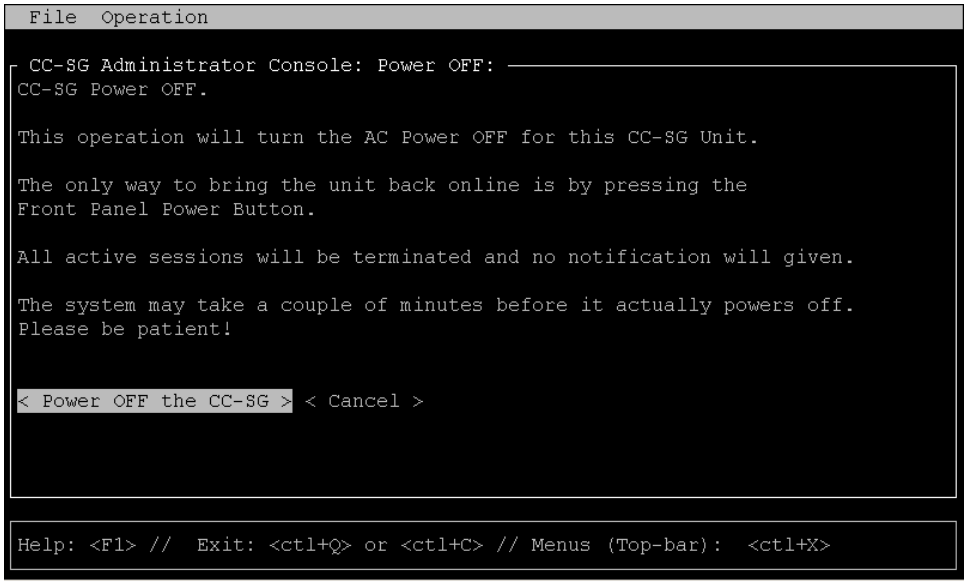


*図 197 Diagnostic Console からの CC-SG の電源オフ*

### CC-SG (GUI) Admin パスワードのリセット (Admin)

このオプションでは、admin アカウント CC-SG GUI ユーザ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。

---

***注 :** これは、Diagnostic Console の admin ユーザのパスワードではありません。このアカウントのパスワードの変更については、後の DiagCon パスワード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**] の順にクリックします。
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。

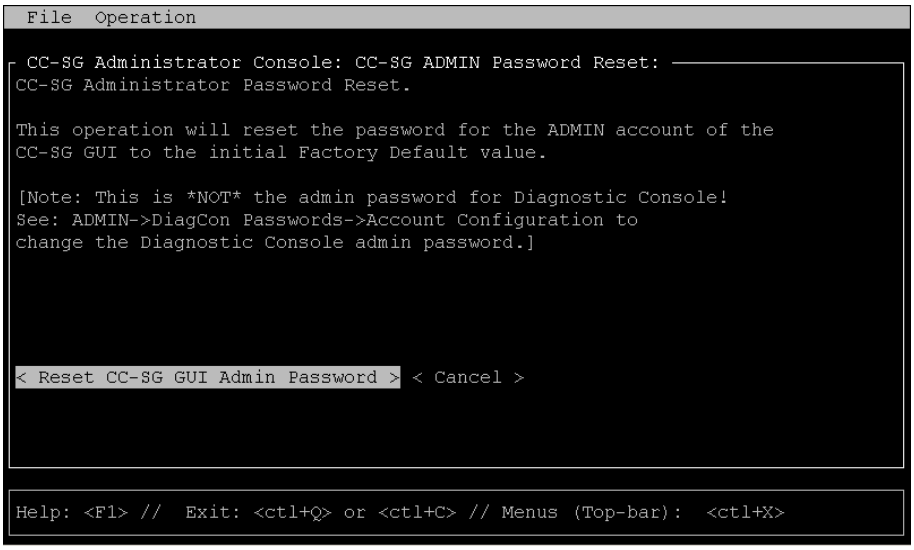


*図 198 Diagnostic Console での CC-SG GUI の Admin パスワードのリセット*

### CC-SG 工場出荷時設定へのリセット (Admin)

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オフされ、SNMP 処理が停止します。この操作を開始する前に CC-SG を**メンテナンス モード**にするように強くお勧めします。 可能であれば、CC-SG のリセットは、Diagnostic Console ではなく管理者の Director Client から行ってください。[**Director Client Reset**] オプションでは、ここにリストされたすべての操作を実行できますが、ネットワーク値はリセットできません。

1. [**Operation**] メニューで、[**Admin**] をクリックして、[**Factory Reset**] をクリックします。7 つの**リセット オプション**がある次の画面が表示されます。

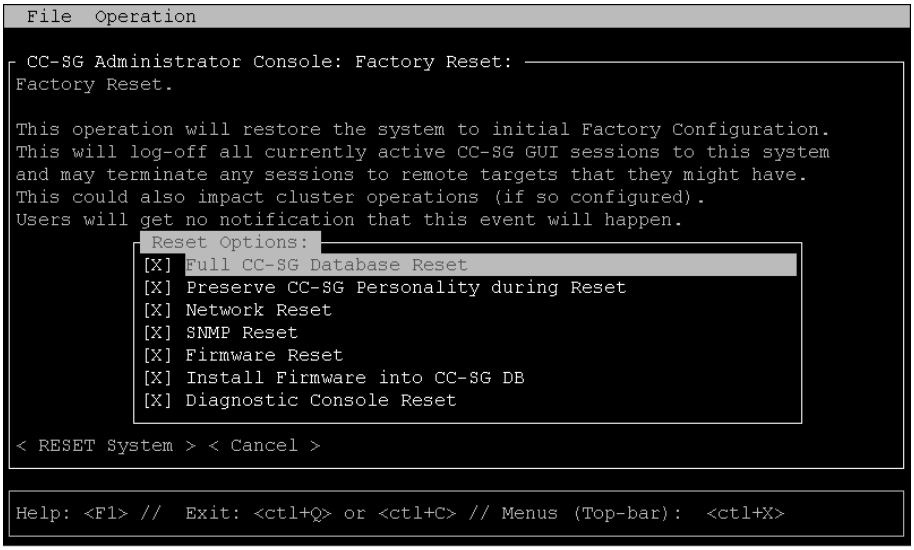


*図 199 CC-SG 工場出荷時にリセット*

| オプション | 説明 |
|---|---|
| Full CC-SG Database Reset | このオプションを選択すると、既存の CC-SG データベースが完全に削除され、すべての値が工場出荷時の状態になった新しいバージョンが最初から作成されます。 |
| Preserve CC-SG Personality during Reset | 12. このオプションは、前のオプションが選択された場合にのみ有効で、効力をもちます。CC-SG データベースが再作成される (前のオプション) ので、次の値が新しいバージョンのデータベースにマイグレーションされます (これらの値が読み取り可能で、利用できる場合。それ以外はデフォルト値が使用されます)。次の情報が保存されます。デフォルト値は [] 内で示されています。<br>PC クライアントと CC-SG 間のセキュア通信 [unsecured]<br>強力なパスワード強制を有効にするかどうかを決定する強力なパスワード検査の選択 [off]<br>PC クライアントがアウト オブ バンド ノードに接続するために使用するのは直接接続かプロキシ接続かの選択 [Direct]<br>アイドル セッションがログアウトされるまでの休止タイマー時間 [1800]<br>モデムのサーバ IP アドレス、クライアント IP アドレス、およびコールバック電話番号を示すモデム設定 [10.0.0.1/10.0.0.2/<none>] |
| Network Reset | このオプションではネットワーク機能が次のような工場出荷時のデフォルトにリセットされます。<br>▪ ホスト名 = CommandCenter<br>▪ ドメイン名 = localdomain<br>▪ モード = Primary / Backup<br>▪ 設定 = Static<br>▪ IP アドレス = 192.168.0.192<br>▪ ネットマスク = 255.255.255.0<br>▪ ゲートウェイ = <none><br>▪ プライマリ DNS = <none><br>▪ セカンダリ DNS = <none><br>▪ アダプタ速度 = Auto |
| SNMP Reset | SNMP 設定が工場出荷時のデフォルトにリセットされます。<br>▪ ポート : 161<br>▪ 読み取り専用コミュニティ : public<br>▪ 読み書きコミュニティ : private<br>▪ システム連絡先の名前と場所 : <empty><br>▪ SNMP トラップ構成<br>▪ SNMP トラップ送信先 |
| Firmware Reset | アップロードされたファームウェア ファイルが削除され、デフォルトのバージョンがファイル システム リポジトリにリストアされますが、CC-SG DB は変更されません。 |

| | |
|---|---|
| Install Firmware into CC-SG DB | ファームウェア ファイルがファイル システム ベースのリポジトリから CC-SG DB にロードされます。 |
| Diagnostic Console Reset | Diagnostic Console が元の工場出荷時の設定、アカウント設定、デフォルトにリストアされます。 |

### Diagnostic Console のパスワード (Admin)

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、Diagnostic Console 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。

**Password Configuration**

1. [**Operation**]、[**Admin**]、[**DiagCon Passwords**]、[**Password Configuration**] の順にクリックします。
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。

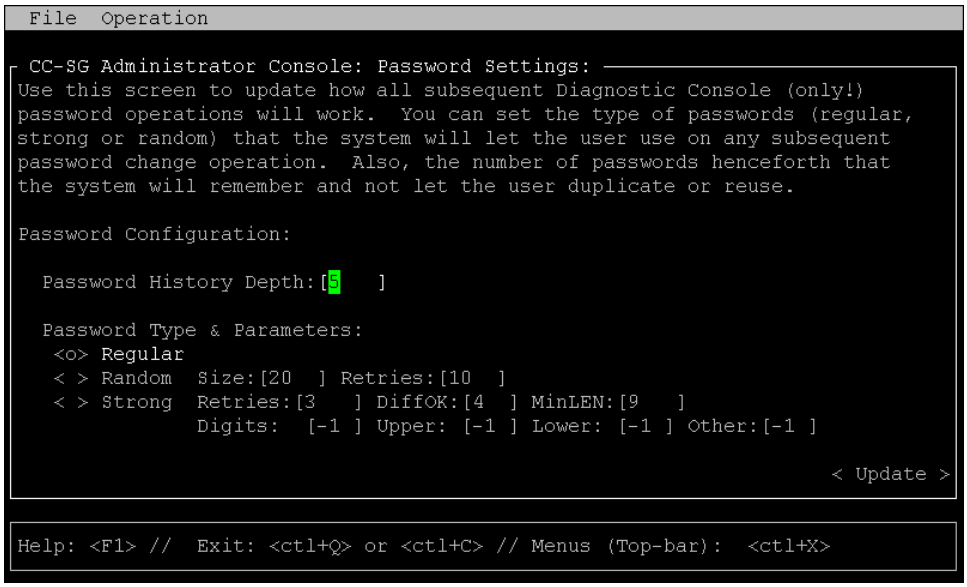


*図 200 パスワードの設定*

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。パスワードは半角英数字で 4 文字以上である必要があり、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)」カウントに対してその文字クラスの「credit (持ち点)」を加算できる最大数を意味します。負の数は、その文字クラスの文字を少なくともその数以上はパスワードに入れる**必要がある**ことを意味します。つまり、数に **-1** を指定した場合、すべてのパスワードに少なくとも 1 桁 の数字が必要になります。 |

### Account Configuration

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。

1. アカウントを設定するには、[**Operation**]、[**Admin**]、[**DiagCon Passwords**]、[**Account Configuration**] の順にクリックします。
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。

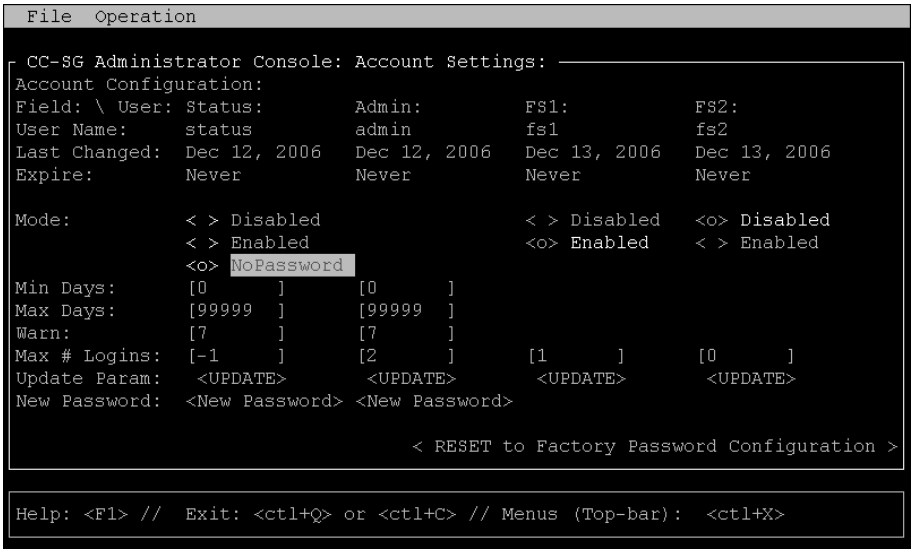


*図 201 アカウントの設定*

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。
- 一番下のセクションは、パスワードの設定をファクトリ 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。 Diagnostic Console 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。 |
| **13. New Password** | このアカウントの新しいパスワードを入力します。 |

### ディスク ステータスの表示 (Utilities)

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。ディスクのサイズ、システムがアクティブで稼動中かどうか、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 Status**] の順にクリックします。

2. [**Refresh**] をクリックするか、**Enter** 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。

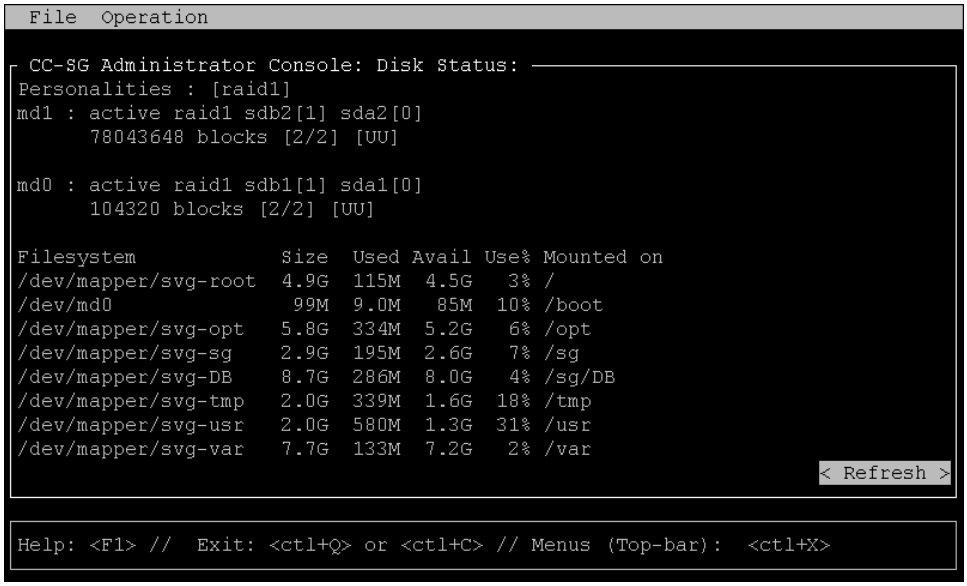


*図 202 Diagnostic Console での CC-SG のディスク ステータスの表示*

***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。*

### トップ ディスプレイの表示 (Utilities)

このオプションでは、現在 CC-SG で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が表示されます。

1. CC-SG で実行中のプロセスを表示するには、[**Operation**]、[**Utilities**]、[**Top Display**] の順にクリックします。
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。

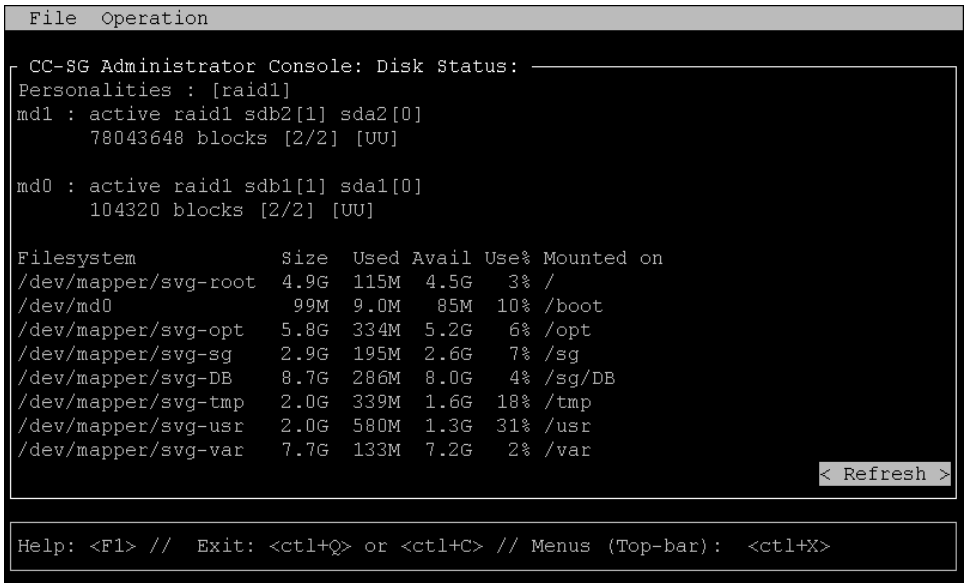


*図 203 Diagnostic Console での CC-SG プロセスの表示*

3. 「**h**」と入力すると、トップ コマンドの詳細なヘルプ画面が表示されます。標準の **F1** ヘルプ キーはここでは機能しません。Admin Console に戻るには、**CTL+Q** または **CTL+C** キーを使います。

### NTP (Network Time Protocol) ステータスの表示 (Utilities)

CC-SG で NTP タイム デーモンが設定され、稼働中であれば、このオプションでそのステータスが表示されます。

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**] の順にクリックします。
2. NTP デーモンは、CC-SG 管理者の Director Client でしか設定できません。NTP が有効でなく、また正しく設定されていない場合は、次の画面が表示されます。

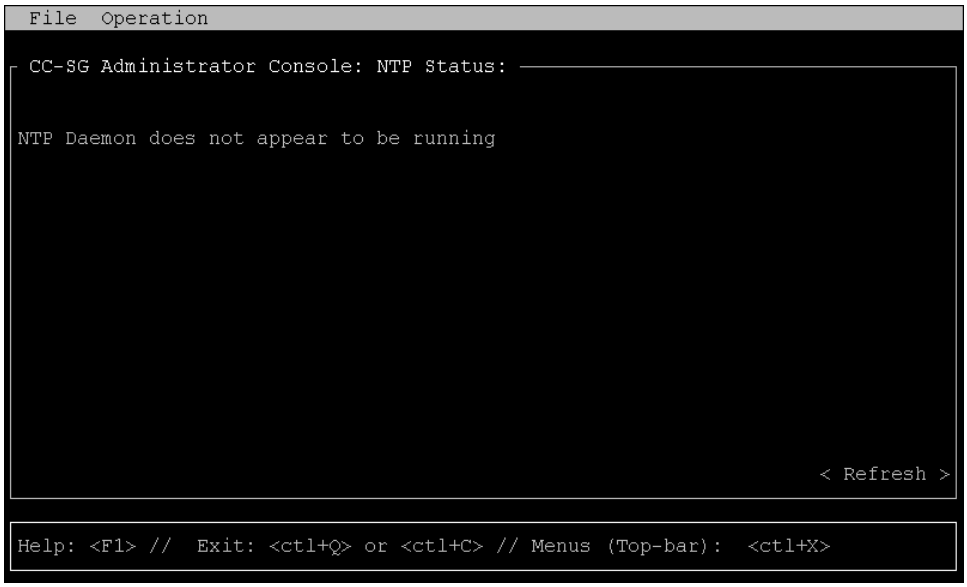


*図 204 CC-SG GUI で NTP が設定されていない*

3. CC-SG で NTP が正しく設定され、稼働中の場合は、次のような画面が表示されます。

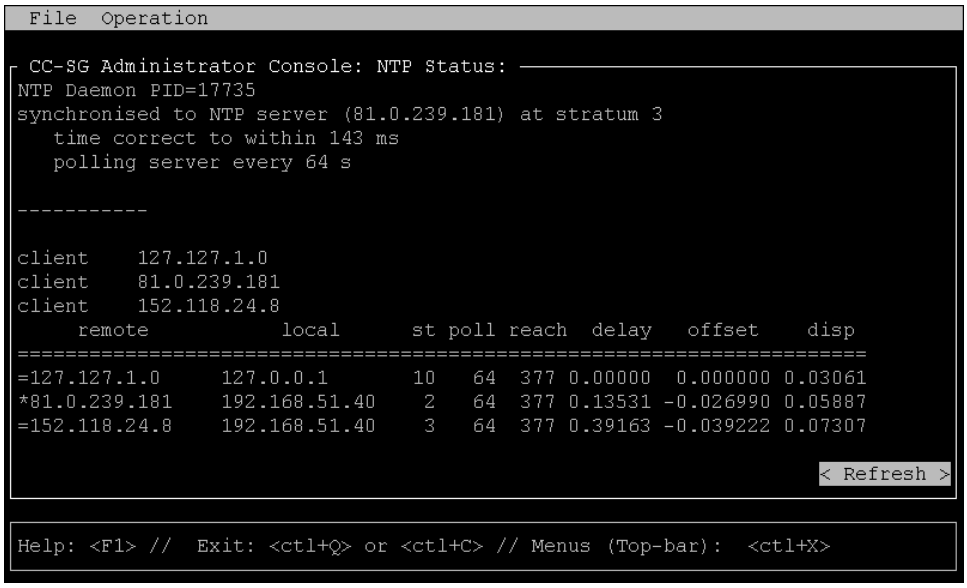


*図 205 CC-SG GUI で NTP が稼働中*

4. [**Refresh**] を選択すると、この画面の情報が更新されます。

*本ページは意図的に空白となっています。*

# 付録 A：仕様 (G1、V1、および E1)

## G1 プラットフォーム

### 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)** | 563 mm x 440 mm x 44 mm |
| **重量** | 10.92 kg |
| **電源** | 二重化電源、ホットスワップ可能、オートセンシング<br>110/200V 2.0A |
| **平均故障間隔 (MTBF)** | 38,269 時間 |
| **KVM 管理ポート数** | (DB15 + PS2 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** | 該当せず |

### ハードウェア仕様

| | |
|---|---|
| **プロセッサ** | Intel® Pentium® III 1 GHz |
| **メモリ** | 512 MB |
| **ネットワーク インタフェース** | (2) 10/100 Ethernet (RJ45) |
| **ハードディスク/コントローラ** | (2) 40-GB IDE @7200 rpm, RAID 1 |
| **CD-ROM ドライブ** | CD/ROM 40x 読み取り専用 |

### 環境要件

| **動作時** | |
|---|---|
| **湿度** | 20% ～ 85% 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** | 該当せず |
| **非動作時** | |
| **温度** | 0 ～ 30 deg C (32 ～ 104 deg F) |
| **湿度** | 10% ～ 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** | 該当せず |

# V1 プラットフォーム

## 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)** | 615mm x 485mm 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 |

## ハードウェア仕様

| | |
|---|---|
| **プロセッサ** | AMD Opteron 146 |
| **メモリ** | 2 GB |
| **ネットワーク インタフェース** | (2) 10/100/1000 Ethernet (RJ45) |
| **ハードディスク/コントローラ** | (2) 80-GB SATA @ 7200 rpm, RAID 1 |
| **CD-ROM ドライブ** | DVD-ROM |

## 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。<br>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、<br>軸 (X、Y、Z) ごとに 30 分 |
| **衝撃** | 該当せず |
| **非動作時** | |
| **温度** | -40℃ - +60℃ (-40℉-140℉) |
| **湿度** | 5% ～ 95% RH |
| **海抜高度** | 0 ～ 3,000 m の高度で適切に作動。<br>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、<br>軸 (X、Y、Z) ごとに 30 分 |
| **衝撃** | 該当せず |

# E1 プラットフォーム

## 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)** | 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 deg 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 |

## ハードウェア仕様

| | |
|---|---|
| **プロセッサ** | (2) AMD Opteron 250 2.4G 1MB プロセッサ |
| **メモリ** | 4 GB |
| **ネットワーク インタフェース** | Intel PRO/1000 PT Dual Port Server Adapter |
| **ハードディスク/コントローラ** | (2) WD740ADFD SATA 74GB 10K RPM 16MB キャッシュ |
| **CD-ROM ドライブ** | DVD-ROM |

## 環境要件

| **動作時** | |
|---|---|
| **湿度** | 5 ～ 90%、結露なし |
| **海抜高度** | 海抜 2500 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) |
| **非動作時** | |
| **温度** | セ氏 -40 ～ -70 度 |
| **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) |

*本ページは意図的に空白となっています。*

# 付録 B : CC-SG およびネットワーク設定

## はじめに

この付録では、一般的な CC-SG (CC-SG) 配備のネットワーク要件 (アドレス、プロトコル、ポート) について説明します。この中で、外部アクセスの場合 (必要に応じて) 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 (使用する場合) 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。場合によっては CC-SG 管理者を超える役割と責任を負い、CC-SG とそのコンポーネントをサイトのセキュリティ アクセスとルーティング ポリシーに組み込むことを計画している、TCP/IP ネットワーク管理者にとっても有益な詳細情報が記載されています。

次の図に示すような一般的な CC-SG 配備では、ファイアウォールや VPN (Virtual Private Network) などの機能がまったく組み込まれない場合、一部が組み込まれる場合、すべてが組み込まれる場合があります。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。ファイアウォールまたは VPN がネットワークに組み込まれ、ネットワークでアクセス ポリシーおよびセキュリティ ポリシーを強化しようとする場合は特にこれらを理解することが不可欠になります。

## 要旨

14. 以下では、CC-SG とその関連コンポーネントによる通信およびポートの使用に関する、完全かつ徹底的な分析が行われています。CC-SG とその制御下にあるターゲットにアクセスするためにファイアウォールで開くポートは、次のとおりです。

| ポート番号 | プロトコル | 目的 |
|---|---|---|
| 80 | TCP | CC-SG への HTTP アクセス |
| 443 | TCP | CC-SG への HTTPS (SSL) アクセス |
| 8080 | TCP | CC-SG と PC クライアント間 |
| 2400 | TCP | ノード アクセス (プロキシ モードとインバンド アクセス) |
| 5000[1] | TCP | ノード アクセス (ダイレクト モード) |
| 51000[1] | TCP | SX ターゲット アクセス (ダイレクト モード) |

この表をまとめると、次のようになります。

- 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 を除外できます。
- 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 を除外できます。

そのため、最小限の設定の場合、CC-SG への外部アクセスを可能にするには、443、8080、および 2400 の 3 つのポートを開くだけです。

次に、各種の設定コントロールおよびオプションとともに、アクセス方式とポートの詳細を示します。

[1] 外部的にアクセスされる Raritan デバイスごとにこれら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。

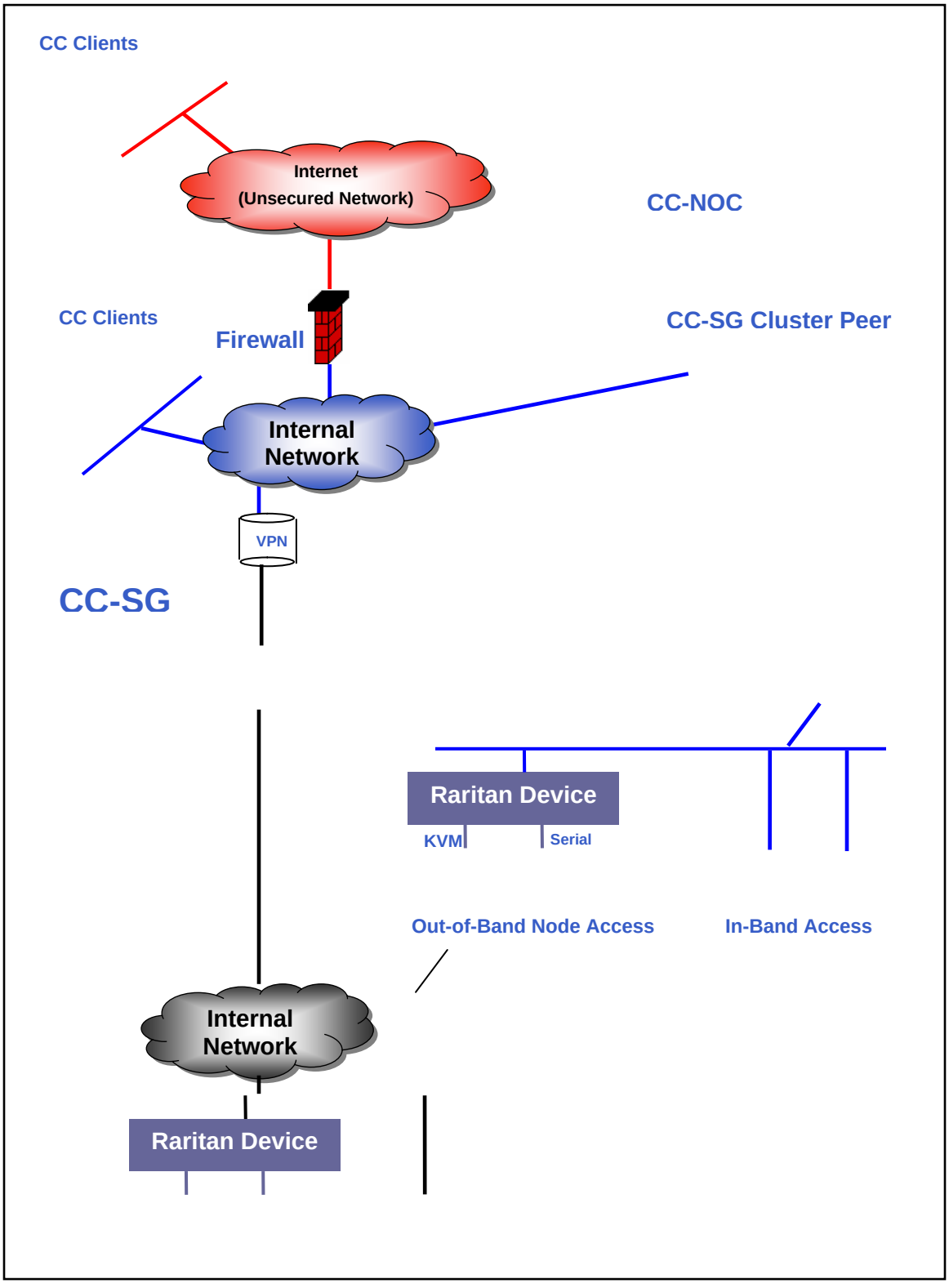


*図 206 CC-SG 配備の要素*

CC-SG 通信チャンネル

通信チャンネルは次のように区分されています。

- CC-SG ↔ Raritan デバイス
- CC-SG ↔ CC-SG クラスタリング (オプション)
- CC-SG ↔ インフラストラクチャ サービス
- クライアント ↔ CC-SG
- クライアント ↔ ターゲット (ダイレクト モード)
- クライアント ↔ ターゲット (プロキシ モード)
- クライアント ↔ ターゲット (インバンド)
- CC-SG ↔ CC-NOC

各通信チャンネルについては、次の点に注意してください。

- 通信者によって使用されるシンボリック **IP アドレス**を示しています。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**を示しています。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**を示しています。
- ポートが**設定可能**であるかどうかを示しています。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以外の値に変更できるようなフィールドを、GUI または Diagnostic Console が提供しているかどうかを示しています。

## 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、KSX 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 |
|---|---|---|---|
| CC-SG → ローカル ブロードキャスト | 5000 | UDP | 可 |
| CC-SG → リモート LAN IP | 5000 | UDP | 可 |
| CC-SG → Raritan デバイス | 5000 | TCP | 可 |
| Raritan デバイス → CC-SG | 5001 | UDP | 不可 |

## CC-SG クラスタリング

オプションの CC-SG クラスタリング機能を使用する (つまり 2 台の CC-SG ユニットが内部的に接続され、1 つのユニットとして機能する) 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。オプションのクラスタリング機能を使用しない場合、これらのどのポートもネットワークで利用可能にする必要はありません。

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。

| 通信方向 | ポート番号 | プロトコル | 設定可否 |
|---|---|---|---|
| CC-SG → ローカル ブロードキャスト | 10000 | UDP | 不可 |
| CC-SG → リモート LAN IP | 10000 | UDP | 不可 |
| CC-SG ↔ CC-SG | 5432 | TCP | 不可 |
| CC-SG ↔ CC-SG | 8732 | TCP | 不可 |
| CC-SG ↔ CC-SG | 3232 | TCP | 不可 |

## 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。CC-SG がこれらのオプション サーバと通信するには、次のポートおよび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 |
|---|---|---|---|
| DHCP サーバ → CC-SG | 68 | UDP | 不可 |
| CC-SG → DHCP サーバ | 67 | UDP | 不可 |
| NTP タイム サーバ ↔ CC-SG | 123 | UDP | 不可 |
| CC-SG → DNS | 53 | UDP | 不可 |

## 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 / Java Applet CC-SG GUI インタフェース
- SSH 経由 CC-SG コマンド ライン インタフェース
- CC-SG Diagnostic Console

最初のモードは、ユーザおよび管理者が CC-SG に接続するための主な手段です。他の 2 つのモードは、これに比べてあまり使用されません。これらのモードには次のネットワーク設定が必要です。

| 通信方向 | ポート番号 | プロトコル | 設定可否 |
|---|---|---|---|
| クライアント ↔ CC-SG GUI | 443 | TCP | 不可 |
| クライアント ↔ CC-SG GUI | 80 | TCP | 不可 |
| クライアント ↔ CC-SG GUI | 8080 | TCP | 不可 |
| クライアント → CC-CLI SSH | 22 | TCP | 可 |
| クライアント → CC Diagnostic Console | 23 | TCP | 可 |

## 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ターゲット（ノード) に接続することです。こうしたターゲットは、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)。もう 1 つのモードでは、VNC (Virtual Network Computer)、Windows RDP (Remote Desktop)、SSH (Secure Shell) などのイン バンド アクセス (IBA) 方式が使用されます。

さらに PC クライアントとターゲット間通信では、次のいずれかの特性があります。

- PC クライアントをターゲットに直接接続する (Raritan デバイスまたはイン ハント アクセスを使用)。このような状態を**ダイレクト モード**といいます。
- PC クライアントが CC-SG と介して接続される場合、これはアプリケーション ファイアウォールとして機能します。このような状態を**プロキシ モード**といいます。

| 通信方向 | ポート番号 | プロトコル | 設定可否 |
|---|---|---|---|
| Client → CC-SG (プロキシ モード) → ターゲット | 2400 (CC-SG 上) | TCP | 不可 |
| クライアント ↔ Raritan ターゲット (ダイレクト モード) | 5000 (デバイス上) | TCP | 可 |
| クライアント → Dominion SX → (ダイレクト モード) | 51000 | TCP | 可 |

## CC-SG と IPMI、iLO/RILOE、DRAC、RSA のクライアント

さらに CC-SG のもう 1 つの重要な役割は、iLO/RILOE、Hewlett Packard の Integrated Lights Out/Remote Insight Lights Out サーバなど、サードパーティ デバイスを管理することです。iLO/RILOE デバイスのターゲットの電源は、直接にオン、オフ、再投入されます。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。

| 通信方向 | ポート番号 | プロトコル | 設定可否 |
|---|---|---|---|
| CC-SG → IPMI | 623 | UDP | 不可 |
| CC-SG → iLO/RILOE (HTTP ポート使用) | 80 または 443 | UDP | 不可 |
| CC-SG → DRAC | 80 または 443 | UDP | 不可 |
| CC-SG → RSA | 80 または 443 | UDP | 不可 |

## 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 |
|---|---|---|---|
| SNMP マネージャ → CC-SG | 161 | UDP | 可 |
| CC-SG → SNMP マネージャ | 162 | UDP | 可 |

## CC-SG と CC-NOC

**CC-NOC は、CC-SG とともに配備可能なオプション アプライアンスです。CC-SG が管理するサーバ、装置、Raritan デバイスのステータスを監査および監視する Raritan ネットワーク監視アプライアンスです。**

| 通信方向 | ポート番号 | プロトコル | 設定可否 |
|---|---|---|---|
| CC-SG ↔ CC-NOC | 9443 | TCP | 不可 |

## 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、および 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 ポートのペアをオープン状態にしている場合があります。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)/443 (SSL)[2]、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)。

イン バンド アクセス (IBA) 接続ではすべて、CC-SG がプロキシ接続として使用されるので、追加設定は必要ありません。 ファイアウォールが使用されるアウト オブ バンド (OBA) 接続の場合、[**設定**]、[**設定マネージャ**]、[**接続モード**] メニューの順に選択し、プロキシ モードを使用できるよう設定する必要があります。このように CC-SG はさまざまなターゲットに接続 (IBA または OBA のいずれか) 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。

[2] 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。

## セキュリティおよびオープン ポート スキャン

CC-SG 品質保証プロセスの一部としていくつかのオープン ポート スキャナが製品に適用されているので、Raritan は製品が以下に示すような既知の攻撃を受けにくくなっていることを保証します。オープン ポートまたはフィルタ/ブロック状態のポートは、前にすべてリストされています。 一般的な脅威を以下に一部示してあります。

| 問題 ID[3] | 概要 | 解説 |
|---|---|---|
| CVE-1999-0517<br>CVE-1999-0186<br>CVE-1999-0254<br>CVE-1999-0516 | snmp (161/UDP) - リモート SNMP サーバのコミュニティ名を推測できる。 | デフォルトの CC-SG SNMP コミュニティ名は「public」です。これをサイト固有の値に変更することをお勧めします（[**設定**]、[**設定マネージャ**]、[**SNMP**] **メニューの順に選択**して設定）。詳細については、『**CC-SG 管理者ガイド**』を参照してください。 |
| CVE-2000-0843 | 長いユーザ名の後にパスワードが続くと、リモート テレネット サーバが突然接続をシャットダウンする。 | 従来から テレネット サービスにはポート 23 が使用されています。ただし、CC-SG ではこのポートは SSH V2 Diagnostic Console セッションに使用されます。ユーザは、ポートを変更するか、Diagnostic Console で SSH アクセス方式をまったく使用できないようにするか、その両方を行うことができます。詳細については、『**CC-SG 管理者ガイド**』を参照してください。 |
| CVE-2004-0230 | リモート ホストはシーケンス番号を予測できる脆弱性にさらされている。このため攻撃者が変造された RST パケットをリモート ホストに送りつけて、確立されたセッションを切断してしまう危険性があります。 | CC-SG で使用される基盤の TCP/IP プロトコル スタックは、こうしたデータ漏れに対して脆弱でないことが証明されています。 |
| CVE-2004-0079<br>CVE-2004-0081<br>CVE-2004-0112 | リモート ホストは、0.9.6m または 0.9.7d よりも古いバージョンの OpenSSL を使用している。 | 次のパッチが OpenSSL に適用されているので、このことが原因のデータ漏れの危険性が回避されます。<br>• RHSA-2004:120<br>• RHSA-2005:830<br>• RHSA-2003:101-01 |

[3] CVE は http://cve.mitre.org にあります。

# 付録 C : ユーザ グループ権限

| 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* | |
| | 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 グループの削除 | ユーザ管理 | |
| | > ユーザのグループへの割り当て | ユーザ管理 | |
| | > ユーザのログアウト | 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。**<br>**デバイス、ポート、およびノードの管理**<br>**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 | デバイスの設定およ | |

| メニュー> サブメニュー | メニュー項目 | 必要な権限 | 説明 |
|---|---|---|---|
| | ド | 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 | |
| | > **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 | |
| | > 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 | | |
| | > 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 | |

| メニュー> サブメニュー | メニュー項目 | 必要な権限 | 説明 |
|---|---|---|---|
| | | 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 | |
| | > ポートの設定 | デバイス、ポート、およびノードの管理 | |
| | > ブックマーク ポート | 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 | |
| | > 一括コピー | 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 | |
| **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。**<br>**デバイス、ポート、およびノードの管理**<br>**ノードのイン バンド アクセス**<br>**ノードのアウト オブ バンド アクセス**<br>**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> | イン バンド アクセス/アウト オブ バンドア | |

| メニュー> サブメニュー | メニュー項目 | 必要な権限 | 説明 |
|---|---|---|---|
| | | クセス | |
| | 切断 | イン バンド アクセス/<br>アウト オブ バンドアクセス | |
| | パワー制御 | パワー制御 | |
| | グループパワー制御 | パワー制御 | |
| > ノード並び替えオプション | > ノード名でソート | 次のいずれか :<br>デバイス、ポート、およびノードの管理 /<br>イン バンド アクセス/<br>アウト オブ バンド アクセス/<br>パワー制御 | |
| | > ノード ステータスでソート | 次のいずれか :<br>デバイス、ポート、およびノードの管理 /<br>ノードのイン バンド アクセス/<br>ノードのアウト オブ バンド アクセス/<br>ノードのパワー制御 | |
| > チャット | > チャットの開始 | ノードのイン バンド アクセス/<br>ノードのアウト オブ バンド アクセス/<br>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/<br>ノードのアウト オブ バンド アクセス/<br>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/<br>ノードのアウト オブ バンド アクセス/<br>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 :<br>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 |
|---|---|---|---|
| | | ノードのイン バンド アクセス/<br>ノードのアウト オブ バンド アクセス/<br>ノードのパワー制御 | |
| | > ツリー表示 | 次のいずれか :<br>デバイス、ポート、およびノードの管理 /<br>ノードのイン バンド アクセス/<br>ノードのアウト オブ バンド アクセス/<br>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** | **このメニューはすべてのユーザが使用できます。** | | |
| | 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 | システム管理者グループのユーザのみが使用できます。 | |
| | 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 ユーザー | CC の設定と制御 | |
| | > 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<br>自身のユーザ データを表示する場合 : なし | |

| メニュー> サブメニュー | メニュー項目 | 必要な権限 | 説明 |
|---|---|---|---|
| | > グループ内のユーザ | ユーザ管理 | |
| | > グループ データ | ユーザ セキュリティ管理 | |
| | > AD ユーザ グループ レポート | CC の設定と制御/ユーザ管理 | |
| > デバイス | 資産管理 | デバイス、ポート、およびノードの管理 | |
| > 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 | |
| > ポート | > ポートの照会 | デバイス、ポート、およびノードの管理 | |
| | > アクティブ ポート | デバイス、ポート、およびノードの管理 | |
| | スケジュールされたレポート | CC の設定と制御 | |
| | CC-NOC 同期 | CC の設定と制御 | |
| **アクセス** | | | |
| | CC-NOC 設定 | 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。**<br>**CC の設定と制御**<br>**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 :<br>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 | |
| | 設定 | 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 | デバイスの設定およびアップグレードの管理 | |
| **システム メンテナンス** | | | |

| メニュー> サブメニュー | メニュー項目 | 必要な権限 | 説明 |
|---|---|---|---|
| | 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* | |

*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。

# 付録 D：SNMP トラップ

CC-SG には次の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。 |
| 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 Diagnostic Console にログインしました。 |
| ccDiagnosticConsoleLogout | ユーザが CC-SG Diagnostic Console からログアウトしました。 |
| ccNOCAvailable | CC-SG が、ACC-NOC が利用可能であることを検出しました。 |
| ccNOCUnavailable | CC-SG が、CC-NOC が使用不能であることを検出しました。 |
| 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 パスワードが変更されました。 |
| ccSuperuserPasswordChanged | CC-SG スーパーユーザ 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。 |

*本ページは意図的に空白となっています。*

# 付録 E：トラブルシューティング

- Web ブラウザから CC-SG を起動するためには 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 の場合：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、再起動して、ブラウザのキャッシュを空にしてください。

## クライアントのブラウザ要件

サポートされるブラウザおよびプラットフォームの詳しいリストについては、**http://www.raritan.com/support** の**互換表**を参照してください。[**Support**] ページで、[**Firmware Upgrades**]、[**CommandCenter Secure Gateway**] の順にクリックします。

*本ページは意図的に空白となっています。*

# 付録 F：2 ファクタ認証

CC-SG RADIUS ベースのリモート認証の一部として、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 CC-SG を設定できます。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。

## サポート環境

次の RSA 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。

## 設定条件

RSA RADIUS サーバおよび RSA Authentication Manager の適正な設定についての説明は、本書では説明していません。詳細は、RSA のマニュアルを参照してください。

ただし、次の手順を完了しておく必要があります。

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。

## 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。

*本ページは意図的に空白となっています。*

# 付録 G : 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。 |
| CommandCenter NOC とは何ですか? | CommandCenter NOC は、CC-SG からアクセスできるサーバ、装置、Raritan デバイスのステータスを監査および監視するネットワーク監視デバイスです。 |
| CC-SG はどの Raritan 製品をサポートしていますか？ | CC-SG はすべての Dominion 製品をサポートしています。<br>- Raritan の KVM over IP 製品 - Dominion KX<br>- Raritan のセキュア コンソール サーバ製品 - Dominion SX<br>- Raritan のリモート オフィス管理製品 - Dominion KSX CC-SG は、オプションの IP ユーザ ステーションと併用した場合は Paragon II もサポートします。 |
| 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。 |
| PDA アクセスはできますか? | 一般的な回答は「はい」です。PDA に Java 対応のブラウザがあり、128 ビット (一部の地域ではこれを下回る) SSL 暗号化をサポートする場合は可能です。 詳細は Raritan テクニカル サポートにお問い合わせください。この分野ではテストされていません。 |
| CC-SG のステータスは、プロキシの対象となるデバイスのステータスによって制限されますか? | いいえ。CC-SG ソフトウェアは専用のサーバ上にあるので、CC-SG のプロキシの対象となるデバイスの電源がオフでも、CC-SG にアクセスできます。 |
| CC-SG ソフトウェアの新しいバージョンがリリースされた場合は、新バージョンにアップグレードできますか? | はい。お近くの Raritan 正規販売店または直接 Raritan, Inc. にお問い合わせください。 |
| CC-SG にはノード、Dominion ユニット、IP-Reach ユニットを合計で何台接続できますか? | 接続できるノードと、Dominion または IP-Reach ユニットの台数に特定の制限はありませんが、無制限ではありません。 ホスト サーバに搭載されたプロセッサの性能やメモリの容量によって、実際に接続できるポートの数が決まります。 |
| Microsoft Internet Explorer を使用する場合に、その性能を最適化することができますか? | コンソールにアクセスする時に IE の性能を向上させるには、「バーチュアル マシン(VM)の Java JIT コンパイラの使用」、「Java のログの使用」、「Java コンソールの使用」を無効にしてください。 メイン メニュー バーで、[**ツール**]、[**インターネット オプション**]、[**詳細設定**] の順に選択します。 上の各項目が表示されるまでスクロール ダウンし、 |

| 質問 | 回答 |
|---|---|
| | チェックが**オンでない**ことを確認します。 |
| 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。<br>- Dominion ユニットがアクティブ<br>- Dominion ユニットはユーザ アカウントの最大設定数に達していない |
| Raritan CC-SG ではどのバージョンの Java をサポートしますか? | サーバ側およびクライアント側の Java 最小要件については、**http://www.raritan.com/support** の互換表を参照してください。[**Firmware Upgrades**]、[**CommandCenter Secure Gateway**] の順にクリックします。 |
| 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。<br>80: Web ブラウザ による HTTP アクセス用<br>443: Web ブラウザ による HTTPS アクセス用<br>8080: CC-SG サーバ操作用<br>2400: プロキシ モード接続用<br><br>5001: IPR/DKSX/DKX/ P2-SC イベント通知用<br><br>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。<br>8732: クラスタ ノードのハートビート用<br>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。<br>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。<br>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。 |
| **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。 CC-SG で作成できるユーザ アカウントの数に特定の制限はありませんが、無限というわけではありません。ホスト サーバ上のデータベース サイズ、プロセッサの性能、 |

| 質問 | 回答 |
|---|---|
| | 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) の認証には、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。<br>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。 |
| **セキュリティ** | |
| 時々ログオンしようとすると、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 へのログオンを開始する度に送られる、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オンをしないと、セッション ID は無効になります。**Shift-再ロード** によって、CC-SG からページを更新することができます。 または、現行のブラウザを閉じ、新しいブラウザを開いてから再度ログオンをしてください。 Web キャッシュに保存された情報を呼び戻してユニットにアクセスすることができないように、より高いセキュリティ機能が提供されます。 |
| パスワードはどのように保護されますか? | パスワードは、一方向性ハッシュである MD5 暗号化を使用して暗号化されます。 これでセキュリティが強化され、許可のないユーザはパスワード リストにアクセスできません。 |
| 特定の時間、ワークステーションをアイドル状態にしておいてから CC-SG のメニューをクリックすると、「ログインしていません」という内容のメッセージが表示されることがあります。なぜでしょうか? | CC-SG は各ユーザ セッションを計時します。 事前に定義した時間アクティブでなければ、CC-SG ではユーザがログアウトされます。 時間の長さはあらかじめ 60 分に設定されていますが、設定を変更することができます。 セッションが完了したら、CC-SG を**終了**することをお勧めします。 |
| Raritan にはサーバへのルート アクセス権があり、管理機関との問題の原因になる恐れがあります。 顧客にもルート アクセス権がありますか? または Raritan は監査機能または管理機能を提供しますか? | Raritan, Inc.からユニットが出荷されると、サーバへのルート アクセス権はどの企業にもありません。 |
| SSL 暗号化は内部と外部の両方ですか (WAN だけでなく LAN も)? | 両方です。 セッションは、ソース (LAN か WAN か) に関係なく暗号化されます。 |
| CC-SG は CRL リストすなわ | いいえ。 |

| 質問 | 回答 |
| --- | --- |
| ち無効な証明書の LDAP リストをサポートしますか? | |
| 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。 |
| **アカウンティング** | |
| 監査証跡レポートのイベント発生時刻が正しくないようです。なぜでしょうか? | ログ イベント時間は、クライアント コンピュータの時間設定に従ってログに記録されます。 コンピュータの日付と時刻の設定は調整できます。 |
| 監査とログの機能で、だれが電源プラグを接続または切断したかを追跡できますか? | 電源スイッチ自体の切断はログには記録されませんが、CC-SG によるパワー制御は監査ログに記録されます。 |

| | |
|---|---|
| **パフォーマンス** | |
| 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 へのログオ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、多くのノードを割り当てないようにしてください。 |
| クライアントあたりの帯域幅利用はどれほどですか? | シリアル コンソールへの TCP/IP によるリモート アクセスは、テレネット セッションのネットワーク活動とほぼ同レベルです。 ただし、コンソール ポート自体の RS232 帯域幅と SSL/TCP/IP オーバーヘッドに限定されます。<br>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** | |
| 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。<br>たとえば、Sun in NYC は、グループ Sun: "Ostype = Solaris" とグループ New York: "location = NYC" の一部です。 |
| コンソール ポートの利用がアクティブになると、他のポートの利用にどのような影響がありますか? たとえば、一部の UNIX バリアントでは、ネットワーク インタフェース経由の管理ができません。 | 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。<br>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? | 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。 この移動は自動的にシステム設定に反映され、CC-SG に伝えられます。 しかし、CIM が別のサーバに移動する場合は、管理者がその名前を変更する必要があります。 |
| **相互運用性** | |
| CC-SG は、ブレード シャーシ製品とどのように統合されますか? | CC-SG は、透過なパスとして KVM またはシリアル インタフェースを備えた任意のデバイスをサポートします。 |
| CC-SG セキュア ゲートウェイは、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 | 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 |

| | |
|---|---|
| ルですか? それとも単にボックス レベルですか? | 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。 他のプロジェクトの方が優先順位が高いのでこの計画はまだ完了していませんが、8 パス ソリューションの市場でのニーズとユース ケースについてのご意見をお待ちしております。 |
| 承認 | |
| RADIUS/TACACS/LDAP を使用して承認を実行できますか<br>LDAP はどうですか? | 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** | |
| 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：ログ機能はどうなりますか? CC-SG はローカル管理を取り込みますか? それともローカル管理は失われますか? | CC-SG コンソール自体から CC-SG にログオンすると、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 にはこのような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。 |

# 付録 H：キーボード ショートカット

Director Client では、次のキーボード ショートカットを使用できます。

| 操作 | キーボード ショートカット |
|---|---|
| 更新 | F5 |
| 画面印刷 | Ctrl + P |
| ヘルプ | F1 |
| 関連テーブルへの行の挿入 | Ctrl + I |

## 北米

**Raritan**
400 Cottontail Lane
Somerset, NJ 08873
U.S.A.
電話 : (732) 764-8886 (732) 764-8886
または (800) 724-8090
Fax : (732) 764-8887
電子メール : sales@raritan.com
Web サイト : Raritan.com

**Raritan NC**
4901 Waters Edge Dr.
Suite 101
Raleigh, NC 27606
電話 : (919) 277-0642
電子メール : **sales.nc@raritan.com**
Web サイト : Raritan.com

**Raritan カナダ**
4 Robert Speck Pkwy, Suite 1500
Mississauga, ON L4Z 1S1 Canada
電話 : (905) 949-3650
Fax : (905) 949-3651
電子メール : sales.canada@raritan.com
Web サイト : Raritan.ca

## ヨーロッパ

**Raritan オランダ**
Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
電話 : (31) 10-284-4040
Fax : (31) 10-284-4049
電子メール : **sales.europe@raritan.com**
Web サイト : Raritan.info

**Raritan ドイツ**
Lichtstraße 2
D-45127 Essen, Germany
電話 : (49) 201-747-98-0
Fax : (49) 201-747-98-50
電子メール : **sales.germany@raritan.com**
Web サイト : Raritan.de

**Raritan フランス**
120 Rue Jean Jaurés
92300 Levallois-Perret, France
電話 : (33) 14-756-2039
Fax : (33) 14-756-2061
電子メール : **sales.france@raritan.com**
Web サイト : Raritan.fr

**Raritan イギリス**
36 Great St. Helen's
London EC3A 6AP,United Kingdom
電話 : (44) 20-7614-7700
Fax : (44) 20-7614-7701
電子メール : sales.uk@raritan.com
Web サイト : Raritan.co.uk

**Raritan イタリア**
Via dei Piatti 4
20123 Milan, Italy
電話 : (39) 02-454-76813
Fax : (39) 02-861-749
電子メール : **sales.italy@raritan.com**
Web サイト : Raritan.it

## 日本

**日本ラリタン東京本社**
〒104-0033 東京都中央区新川 1-26-2
新川 NS ヒルティンク 4F
電話 : (81) 03-3523-5991
Fax : (81) 03-3523-5992
電子メール : sales@raritan.co.jp
Web サイト : Raritan.co.jp

**大阪事務所**
1-15-8 〒550-0005 大阪市西区西本町 1-15-8
本町フェニックスヒル 8F
電話 : (81) (6) 4391-7752
Fax : (81) (6) 4391-7761
電子メール : sales@raritan.co.jp
Web サイト : Raritan.co.jp

## アジア太平洋

**Raritan 台湾**
5F, 121, Lane 235, Pao-Chiao Road
Hsin Tien City
Taipei Hsien, Taiwan, ROC
電話 : (886) 28919-1333
Fax : (886) 28919-1338
電子メール : **sales.taiwan@raritan.com**
中国語 Web サイト : Raritan.com.tw
英語 Web サイト : Raritan-ap.com

**Raritan China 上海**
Rm 17E Cross Region Plaza
No. 899 Lingling Road
Shanghai, China 200030
電話 : (86) 215425-2499
Fax : (86) 215425-3992
電子メール : **sales.china@raritan.com**
Web サイト : Raritan.com.cn

**Raritan China 北京**
Unit 1310, Air China Plaza
No.36 XiaoYun Road
Chaoyang District
Beijing 100027, China
電話 : (86) 108447-5706
Fax : (86) 108447-5700
電子メール : **sales.china@raritan.com**
Web サイト : Raritan.com.cn

**Raritan China 広州**
Room 1205/F, Metro Plaza
183 Tian He Bei Road
Guangzhou 510075 China
電話 : (86-20)8755 5581
Fax : (86-20)8755 5571
電子メール : **sales.china@raritan.com**
Web サイト : Raritan.com.cn

**Raritan Korea**
#3602, Trade Tower,
World Trade Center
Samsung-dong, Kangnam-gu
Seoul, Korea
電話 : (82) 2 557-8730
Fax : (82) 2 557-8733
電子メール : sales.korea@raritan.com
Web サイト : Raritan.co.kr

**Raritan オーストラリア**
Level 2, 448 St Kilda Road,
Melbourne, VIC 3004, Australia
電話 : (61) 39866-6887
Fax : (61) 39866-7706
電子メール : sales.au@raritan.com
Web サイト : Raritan.co.au

**Raritan インド**
210 2nd Floor Orchid Square Sushant Lok 1,
Block B, Gurgaon 122 002 Haryana India
電話 : (91) 124 5107881
Fax : (91) 124 5107880
電子メール : **sales.india@raritan.com**
Web サイト : Raritan.co.in

**Raritan OEM 事業部**
Peppercon AG, Raritan OEM Division
Scheringerstrasse 1
08056 Zwickau Germany
電話 : (49) 375-27-13-49-0
電子メール : **info@peppercon.com**
Web サイト : www.peppercon.de