Dell™ Remote Console Switchシステム
ユーザー・ガイド

注、注意および警告

注:「 注」は、コンピュータをより良く使用するために役立つ重要な情報を意味します。

注意:「 注意」は、指示に従わない場合、ハードウェアの破損やデータの喪失の危険があることを意味します。

警告:「 警告」は、物的損害、人身傷害、または死亡に至る危険があることを意味します。

590-1021-510C

Model 1082DS/2162DS/4322DS Remote Console Switch

2012年7月

目次

1

製品概要

Dell 1082DS/2162DS/4322DS RCS(RCS) のIPを介したデジタル・キーボード、ビデオ、マウス(KVM) およびシリアル・コンソール・スイッチは、アナログとデジタルのテクノロジーを統合して、データセンター・サーバーの柔軟な中央集中制御を提供し、訓練されたオペレーターがいない遠隔地にある支店での操作、起動、管理を容易にします。IPベースのRCSを使用して、いつでも、どこからでもRCSソフトウェアまたはOBWI(内蔵型Webインターフェイス) を介した柔軟なターゲット・デバイスの管理制御およびセキュアなリモート・アクセスが可能です。

特長とメリット

RCSは企業のお客様に次の特長とオプションを提供します。

- ケーブル量を大幅に低減
- アナログ(ローカル) またはデジタル(リモート) 接続構成が可能なバーチャル・メディア(VM) 機能
- スマート・カード／Common Access Card(CAC) 機能
- セキュア・シェル(SSH) およびTelnetによるトゥルー・シリアル機能
- ビデオ解像度のサポート強化により、ターゲットからリモートにネーティブで最大1600 x 1200または1680 x 1050(ワイドスクリーン) 対応
- オプションのデュアル電源モデルで冗長性を確保

- インテリジェント電源装置を管理するためにオプションのサポート
- 独立したデュアル・ローカル・ポート・ビデオ・パス(ACI専用)
- 同時アクセスのためのデュアル・スタックIPv4(DHCP)およびIPv6(DHCPv6およびステートレス自動構成)
- 10/100/1000BaseT LANポートを経由してのターゲット・デバイスへのアクセシビリティ
- イーサネット接続が利用できない場合でも、V.34、V.90、V.92対応モデムをサポートするモデム・ポートによりスイッチへのアクセスが可能
- FIPSサポート

ケーブル量の低減

サーバーの高密度化に伴い、ネットワーク管理者にとってはケーブル量が大きな考慮事項となっています。RCSは、革新的なサーバー・インターフェイス・ポッド(SIP)モジュールと単一の、業界標準である非シールド・ツイスト・ペア(UTP)ケーブルを活用して、ラック内のKVMケーブル量を大幅に削減します。これによって、気流を大きくし、冷却能力を増やしながら、サーバー密度をさらに高めることができます。

KVMスイッチ機能

RCSは、ターゲット・デバイスから直接電力が供給されるSIPをサポートしているため、スイッチに電源が入っていないときも「キープ・アライブ」機能を提供します。CAT 5設計を採用したSIPでは、ケーブルの乱雑状態が大幅に解消され、また最適な解像度とビデオ設定が提供されます。SIPの内蔵メモリーにより、固有のデバイス名または電子ID(EID)番号が個々の接続デバイスに指定され保持されるため、構成が簡単です。

PS/2とUSB SIPが使用可能で、KVMをデバイスに直接接続できます。USB2およびCAC用SIPも利用できます。RCSにはSIP接続用

に8、16、32のいずれかのアナログ・ラック・インターフェイス（ARI）ポートが備えられています。SIPを利用することで、追加のスイッチを接続してRCSシステムを拡張できます。この柔軟性により、データ・センターの拡大に伴う容量の増大が可能になります。

マルチプラットフォームのサポート

Dell SIPをRCSと組み合わせて、PS/2、USB、USB2、USB2およびCAC用の各デバイス環境との接続をサポートします。さらに、これらのモジュールをOBWIと組み合わせることで、異なるプラットフォーム間の切り替えを容易に行うことができます。

相互運用性のあるAvocent® IQモジュール・インテリジェント・ケーブルを使用しても、デバイスをRCSに接続できます。PS/2、USB、Sun®、およびシリアル・モジュールが使用可能です。詳細については、ご使用の製品に対応するアボセント製品の『インストーラ／ユーザー・ガイド』を参照するか、またはavocent.com/manualsで確認してください。

トゥルー・シリアル機能

RCSはTelnetを介して、トゥルー・シリアル機能を提供するSIPをサポートします。SIPを使用して、SSHセッションを起動するか、OBWIからシリアル・ビューアを起動して、RCSに接続されているシリアル・ターゲットに接続できます。

ローカルおよびリモート・ユーザー・インターフェイス

ローカル・ポートに直接接続することにより、ローカル・ユーザー・インターフェイス（ローカルUI）を使用してRCSを管理できます。リモートのOBWIを使用して、スイッチを管理することもできます。OBWIはWebブラウザ・ベースであり、スイッチから直接起動されます。また、スイッチに接続されているすべてのデバイスが自動的に検出されます。

バーチャル・メディアおよびスマート・カード対応スイッチ

RCSにより、あらゆるターゲット・デバイス間で、バーチャル・メディアのデータを表示、移動、コピーできます。オペレーティング・システムのインストール、オペレーティング・システムのリカバリ、ハード・ドライブのリカバリや複製、BIOSの更新、ターゲット・デバイスのバックアップが可能になり、リモート・システムを効率よく管理できます。

RCSでは、ご使用のスイッチ・システムとスマート・カードを組み合わせて使用することもできます。スマート・カードは情報を格納および処理するポケット・サイズのカードです。CACなどのスマート・カードは、コンピューターやネットワークにアクセスしたり、セキュリティで保護された部屋やビルに入るためのIDや認証を格納するために使用できます。

バーチャル・メディアおよびスマート・カード・リーダーは、スイッチのUSBポートに直接接続できます。さらに、バーチャル・メディアおよびスマート・カード・リーダーは、リモートのOBWI、Dell RCSソフトウェア、Avocent管理ソフトウェアのいずれかを実行している任意のリモート・ワークステーションに接続でき、イーサネット接続を使用してスイッチに接続されます。

注: ターゲット・デバイスとのバーチャル・メディアまたはスマート・カードのセッションを開始するには、最初にSIPを使用してターゲット・デバイスをスイッチに接続する必要があります。

OBWI

OBWIを使用するとRCSソフトウェアと同様の管理機能を実行でき、ソフトウェア・サーバーは不要で、インストールの必要もありません。OBWIはスイッチから直接起動されます。また、RCSに接続されているすべてのサーバーが自動的に検出されます。OBWIを使用して、WebブラウザからRCSを構成できます。OBWIからビューアを起動すると、ターゲット・デバイスに対しKVMセッションとバーチャル・メディア・セッションが確立されます。また、OBWIはLDAP

認証をサポートしています。これにより、単一のインターフェイスから複数のRCSに対するアクセス権を管理できます。

標準TCP/IPネットワークを使用したスイッチへのアクセス

スイッチはエージェントレスのリモート制御およびアクセスが可能です。接続されたサーバーまたはクライアントに特別のソフトウェアやドライバーをインストールする必要はありません。

注: クライアントは、インターネット・ブラウザを使用してスイッチに接続します。

スイッチおよびすべての接続されているシステムには、イーサネットまたはV.34、V.90、V.92のいずれかのモデム経由でクライアントからアクセスできます。クライアントは、有効なネットワーク接続さえ確立されていればどこにでも設置できます。

暗号化

RCSでは、キーボード／ビデオ／マウスのセッションとバーチャル・メディア・セッションの128ビットSSL(ARCFOUR)、およびAES／DES／3DES暗号化がサポートされています。

ビデオ

RCSは、アナログのVGA、SVGAおよびXGAビデオ用に最適な解像度を提供します。スイッチとサーバー間のケーブル長により、最大1600 x 1200、または1680 x 1050(ワイドスクリーン)の解像度での表示が可能です。

FLASHアップグレード対応

RCSとSIPのアップグレードは随時可能です。アップグレードは定期的に行い、常に最新のファームウェア・バージョンで稼動してください。FLASHアップグレードは、OBWIまたはシリアル・コンソールから起動できます。RCSはSIPの自動ファームウェア・アップグレードを実行するように構成できます。詳細については、「RCSファームウェアのアップグレード」(ページ 57)を参照してください。

階層の拡張

RCSでは、スイッチの各アナログ・ラック・インターフェイス(ARI) ポート から追加のDell RCSをティア接続できます。ティアド・スイッチは他のデバイスと同じ方法で接続します。装置にこのようにティア(階層) を追加することで、1つのシステム内に最大1024台のサーバーを接続できます。「 ティアド・スイッチの追加」(ページ 33) を参照してください。

Avocent管理ソフトウェア・プラグイン

スイッチでAvocent管理ソフトウェアを使用すると、単一のWebベースのユーザー・インターフェイスから、複数のプラットフォームにあるターゲット・デバイスのリモート からのアクセス、監視、および制御が可能になります。詳細については、Avocent管理ソフトウェアの「 技術告示」を参照してください。

FIPS暗号モジュール

RCSスイッチはFIPS 140-2のレベル1 暗号セキュリティ 要件に対応しています。FIPS の操作モード は、OBWIまたはローカル・ポート を介し有効または無効して、再起動の後に実行することができます。FIPSを有効にすると、スイッチの再起動で、FIPSモード の完全性チェックのために約2分ほど要します。また、FIPSが有効なとき、キーボード 、マウスまたはビデオの暗号化が128ビット のSSL (ARCFOUR) またはDESに設定されている場合は、暗号化のレベルは自動的に AESの暗号化レベルに変更されます。

注: FIPSの操作モード はデフォルト では無効になっているので有効にして操作する必要があります。

注:「 Setup」ポート の工場出荷時のデフォルト 設定では、FIPSモジュールが自動的に無効になります。

注: FIPSモード は、DSViewソフト ウェア・プラグインを介して変更することができます。

RCSスイッチでは、FIPS 140-2 実装ガイダンスのセクション G.5ガイドラインに従ってLinux PPCプラットフォームで稼動する組み込み式のFIPS 140-2認定暗号モジュール(証明書番号1051) を使用します。

このFIPSモードは、OBWI、ローカル・ポート、DSViewプラグインを介して有効／無効にすることができます。FIPSモードを有効／無効するには、再起動が必要です。このバージョンにファームウェアをアップグレードするまたはデフォルト状態に設定を戻すと(「Setup Port」メニュー) 、FIPSモードは無効になります。

FIPSモードでは、暗号化による暗号はAESまたは3DESに限定されます。FIPSが有効なとき、キーボード、マウスまたはビデオの暗号化が128ビットのSSLまたはDESに設定されている場合は、暗号化レベルは自動的にAESに変更されます。FIPSが有効になっていると、これらのファイルは、FIPS互換アルゴリズムであるAESを使用して保存(または復元) できます。FIPSが無効なときは、アプライアンスから保存するまたはアプライアンスへ復元するファイルは、DESを使用して外部ファイルとして暗号(復号) されます。

これは、ユーザーがOBWIの保存(読み込み) ダイアログでパスワード・パラメータを入力しない(この場合、デフォルトのOEMパスワードは暗号化または復号化に使用されます) ときにも該当します。

FIPSモジュールを有効にすると、結果の1つとして、以前に保存したユーザー・データベースとアプライアンス構成ファイルが非互換になります。この場合、FIPSモードを一時的に無効にし、アプライアンスを再起動し、以前に保存したデータベースまたは構成を復元して、FIPSを再度有効にし、再起した後に、FIPSを有効にしているときにファイルを外部的にもう一度保存することができます。この新しく保存された外部ファイルは、アプライアンスがFIPSモード有効で作動している限り、アプライアンスと互換性を保ちます。

これはの逆の場合にも当てはまります。すなわち、FIPSモードを有効にした状態で保存したデータベースと構成ファイルは、FIPSモジュールを有効にしていないアプライアンスへの復元、またはFIPS

モードに対応していない古いファームウェアがインストールされているアプライアンスでの復元に対して互換性を持ちません。

構成例

図 1.1. RCSの構成例

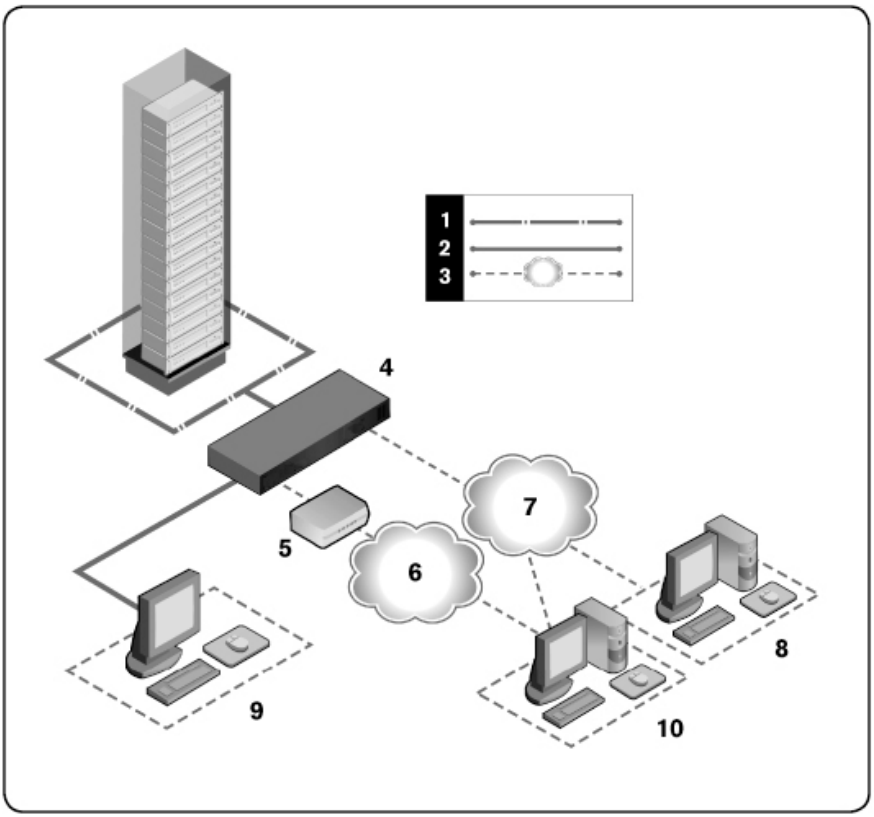


表 1.1: 図 1.1の説明

番号	説明	番号	説明
1	UTP接続	6	電話回線ネットワーク
2	RCSへのKVM接続	7	イーサネット
3	リモートIP接続	8	Avocent管理ソフトウェア・サーバー
4	RCS	9	アナログ・ユーザー(ローカルUI)
5	モデム	10	デジタル・ユーザー(リモートOBWIまたはDell RCSソフトウェア用にインターネット・ブラウザを搭載したコンピューター)

安全に関する注意事項

身体の安全を守り、使用システムや作業環境を損傷から保護するために、次の安全に関するガイドラインに従ってください。

△ **注意: システムの電源は高電圧および高エネルギーを発出して人身に危害を及ぼす可能性があります。カバーを取り外してシステム内のコンポーネントにアクセスするといった作業は、必ず訓練を受けたサービス技術者に任せてください。この警告はDell™リモート・コンソール・スイッチ、Dell™ PowerEdge™ サーバーおよびDell PowerVault™ ストレージ・システムに適用されます。**

本マニュアルはDell 1082DS/2162DS/4322DS Remote Console Switchのみを対象としています。追加の安全事項も併せてお読みいただき、その指示に従ってください。

- Dellリモート・コンソール・スイッチ・ユーザー・ガイド

- Dell安全シート
- Dell RTF規制技術告示

全般

- サービス・マークを確認し、その指示に従います。
- Dellシステムのマニュアルに記載されている以外の修理、メンテナンス作業は行わないでください。
- 電光のイラストの三角形記号が付いているカバーを開くと感電の危険があります。
- これらの格納区画内の部品については、訓練を受けたサービス技術者だけが修理を行います。
- 本製品には修理可能な部品は含まれていません。ユニットを開けようとしないでください。

次のいずれかの状態が発生した場合は、電源コンセントから製品の電源ケーブルを抜いて、部品を交換するか、Dell認定サービス業者に問い合わせてください。

- 電源ケーブル、延長ケーブル、またはプラグが破損した。
- 製品内部に物体が落ちてしまった。
- 製品が水に晒されてしまった。
- 製品を落としたか、破損させた。
- 操作手順に従っても製品が正常に作動しない。

- システムは暖房器具や熱源から離して設置してください。また、冷却用の通気孔をふさがないでください。
- システム・コンポーネントに食べ物や液体をこぼさないでください。また、水分のある環境では製品を操作しないでください。システムに水が入った場合、トラブルシューティング・ガイドの

該当する項を参照するか、認定サービス業者にお問い合わせください。

- 本製品は認定機器のみと併用してください。
- カバーを外す／内部コンポーネントにアクセスする際は、製品が常温に戻ってから行ってください。
- 必ず、電気定格ラベルに記載の外部電源タイプを使用して製品を作動してください。適合する電源タイプが不明の場合は、認定サービス業者または地域の電力会社にお問い合わせください。

注: システム破損を避けるため、電源装置の電圧選択スイッチ(備わっている場合)は、必ずご使用地域のAC電源に適合した電圧になるよう設定してください。また、モニターと接続デバイスの電気定格が適切であることを確認してください。

- 使用モニターおよび周辺機器の電気定格が設置場所の電源に適合していることを確認してください。
- 本製品に付属の電源ケーブルのみを使用してください。
- 感電を避けるため、システムおよび周辺機器の電源ケーブルは、正しい方法でアース処理されたコンセントに接続してください。これらの電源ケーブルは、正しくアースするために、三本ピン・プラグが使用されています。アダプター・プラグを使用したり、アースピンをケーブルから取り外したりしないでください。
- 延長ケーブルおよびケーブルタップは定格に従って使用してください。電源ストリップに接続する製品全部の合計定格アンペアが電源ストリップの最大定格アンペアの80%を超えていないことを確認してください。
- 突発的に起きる一時的な電源の増減からシステムを保護するために、サージ・サプレッサー、ライン・コンディショナ、または無停電電源装置(UPS)を使用してください。

- システム・ケーブルおよび電源ケーブルは慎重に配置してください。ケーブルは踏んだりつまずいたりすることのない形で配線してください。ケーブルには何も載せないでください。
- 電源ケーブルやプラグは改造しないでください。設置場所での電気的改修については、有資格の電気技術者または地域の電力会社にお問い合わせください。必ず使用の地域または国の配線規定に従ってください。

LANオプション

- 雷雨中のLANへの接続や使用は避けてください。雷によって感電する危険があります。
- 湿潤環境でのLANへの接続や使用は避けてください。

2

設置

RCSでは、スイッチに接続されているオペレーターとターゲット・デバイス間で、KVM情報とシリアル情報を送信します。これは、イーサネットまたはモデム接続を使用してネットワークを介して送られます。RCSではイーサネットの通信にTCP/IPを使用します。最適なシステム・パフォーマンスのためには、専用スイッチ付き100BaseTネットワークまたは1000BaseTネットワークを使用します。10BaseTイーサネットを使用することもできます。

RCSでは、V.34、V.90、V.92のモデムを介する通信にポイント・ツー・ポイント・プロトコル(PPP)を使用します。OBWIまたはAvocent管理ソフトウェアを使用して、KVMおよびシリアル・スイッチ・タスクを実行できます。Avocent管理ソフトウェアの詳細については、http://www.avocent.comを参照してください。

RCSボックスには、RCS、RCSソフトウェア、OBWIが含まれています。システムの管理には、RCSソフトウェアまたはOBWIのいずれかを選択して使用できます。OBWIは1台のRCSとその接続を管理するのに対し、RCSソフトウェアは複数のスイッチとその接続を管理できます。OBWIのみを使用する場合は、RCSソフトウェアをインストールする必要はありません。

注: RCSソフトウェアを使用すると、複数のスイッチを管理できます。詳細については、ご使用の製品に対応する「インストーラ/ユーザー・ガイド」を参照してください。

注: 使用中のRCSがすべて最新バージョンのファームウェアにアップグレードされていることを確認してください。OBWIを使用するRCSのアップグレードの詳細については、「RCSツール」(ページ 56)を参照してください。

RCSクイック・セットアップ

次にクイック・セットアップを一覧で示します。最初にRCSをラックに設置します。詳細な設置手順については、「はじめに」(ページ 15) を参照してください。

1 各サーバーで、マウス加速度をSlowまたはNoneに調整します。

2 RCSのハードウェアを設置し、各サーバーまたはティアド・スイッチに、サーバー・インターフェイス・ポッド (SIP) またはAvocent® IQモジュールを接続します。各SIPまたはAvocent IQモジュールをCAT 5ケーブルを使用してRCSに接続し、さらにキーボードとモニター、およびマウス・コネクターをRCSのアナログ・ポートに接続します。

3 ローカル・ポートの周辺機器をRCSの背面パネルにある適切なポートに接続し、ネットワーク構成をセットアップします。IPアドレスはここから、またはRCSソフトウェアから設定できます。Dellでは、構成を容易にするため、静的IPアドレスを使用されることをお薦めします。

4 ローカル・ポートを使用して、OBWIインターフェイスからすべてのサーバー名を入力します。

RCSソフトウェアをセットアップするには (RCSソフトウェア・ユーザー・ガイドを参照してください) :

1 各クライアント・ワークステーションにRCSソフトウェアをインストールします。

2 1つのクライアント・ワークステーションから、RCSソフトウェアを起動します。

3 **New RCS task**ボタンをクリックして、新しいスイッチをRCSソフトウェア・データベースに追加します。前述のとおりにIPアドレスが構成されている場合は、**Yes, the product already has an IP address**を選択し、それ以外の場合は、**No, the product does not have an IP address**を選択します。

RCSソフトウェアはRCSとRCSに接続されているすべてのSIPを検出し、Explorer内に名前を表示します。

注: RCSソフトウェアを使用したDell RCSの追加と管理以外にも、複数のAvocentスイッチを追加および管理できます。

4 Explorerを使用してプロパティを設定し、目的に従ってサーバーをロケーション、サイト、またはフォルダーにグループ分けします。

5 OBWIを使用して、ユーザー・アカウントを作成します。詳細については、「ユーザー・アカウントのセットアップ」(ページ 86)を参照してください。

6 クライアント・ワークステーションの1台がセットアップされたら、**File → Database → Save**の順に選択して、データベースのコピーをすべての設定内容とともに保存します。

7 2台目のクライアント・ワークステーションから、**File → Database → Load**の順にクリックし、保存したファイルを参照して検索します。ファイルを選択し、Loadをクリックします。

8 このファイルを読み込んだ後で、ローカル・ユーザーがいずれかのSIPの追加、削除、名前の変更を行った場合、RCSを選択して**Resync**をクリックすると、ローカル・スイッチを再同期化できます。接続されているサーバーを制御するには、Explorerでサーバーを選択して**Connect Video**タスク・ボタンをクリックし、ビューアでサーバー・セッションを起動します。

9 ビューアでサーバー・ビデオの解像度(View → Scalingを選択)と画質(View → Colorを選択)を調整します。

はじめに

Remote Console Switchには次のアイテムが同梱されています。RCSを設置する前に、正しく設置するために必要なアイテムを手元に準備してください。

- Remote Console Switch

- ジャンパー・コード
- 0U収納用金具
- 1U取り付け用ブラケット・ハードウェア・キット（RCSに事前に取り付け済みの2本の追加レールはキット・アッセンブリーに含まれています）
- SETUPとMODEM用のケーブルとアダプター
- CD収録版Remote Console Switchシステム・ユーザー・ガイド
- Dell安全シート
- Dell RTF規制技術告示

この他に必要なアイテム：

- Dell SIPモジュールまたは Avocent IQモジュール（接続デバイスにつきに1個）
- CAT 5パッチ・ケーブル（最長45m）（接続デバイスにつき1本）

オプションのアイテム：

- V.34、V.90、またはV.92対応モデムおよびケーブル
- 電源管理装置
- ポート拡張モジュール（PEM）

注： PEMを介してサーバーが接続されていると、バーチャル・メディア・セッションまたはCACセッションは開始できません。

ネットワークのセットアップ

スイッチはIPアドレスを使用して、スイッチとターゲット・デバイスを個別に識別します。RCSは、Dynamic Host Configuration Protocol（DHCP）と静的IPアドレスの両方をサポートしています。IPアドレスを各スイッチに予約して、スイッチがネットワークに接続している間、各IPアドレスは静的のままになるようにします。

キーボード

USBキーボード およびマウスをRCSのアナログ・ポート に接続できます。

注: また、RCSは、アナログ・ポート に対する複数のキーボード やマウスの接続にも対応しています。ただし、同時に複数の入力機器を使用すると、予期しない結果を生じることがあります。

RCSのラック収納

RCSは、ラックの棚、または直接19インチ幅のEIA-310-E準拠のラック(4ポスト、2ポスト、ネジ穴式) に設置できます。1U前面ラック、1U背面ラック、および2ポスト 設置用に、Dell ReadyRails™ システムが用意されています。ReadyRailsシステムには、個別に梱包されたレール組立部品が2組と、RCSの側面に取り付けられて同梱されるレール2本が含まれます。さらに、0U構成用に取り付け用ブラケット が1つ、背面ラック設置用にブランク・パネルが1枚付属しています。

警告: この説明はあくまで参考のためのものであり、要約されています。始める前に、「 安全、環境、および規制に関する情報」の小冊子に記載されている安全に関する指示をお読みください。

注: この文書中の図は、特定のスイッチを表すものではありません。

機器をラックに収納する際の安全措置

- ラックへの収納について: ラックに過負荷や不均一な負荷をかけると、棚やラックの故障の原因となり、機器および身体に対する損傷を引き起こすことがあります。設置を始める前に、まず最終設置箇所にラックを固定させてください。コンポーネントをラックの底部から収納していき、上に向かって作業を続けてください。ラックの荷重定格を超えてはいけません。
- 電源に関する注意事項: 装置指定の電源以外には接続しないでください。複数の電気コンポーネントをラックに設置する場合は、コンポーネント の総出力定格が回路容量を超えないことを

確認してください。電源および延長コードが過負荷状態となると、火災やショックの危険性が生じます。

- 周辺温度の上昇: 密閉型のラック・アッセンブリーに設置する場合、ラック収納環境の作動温度が室温より高くなることがあります。スイッチの最高周囲温度は50℃です。これを超えないように注意してください。
- 通気の減少: ラックに装置を設置する際には、機器の安全な動作に必要な気流の量が損なわれないよう配慮する必要があります。
- 確実なアース処理: ラックに取り付けられた装置については、常時確実なアースを確保してください。分岐回路に対し直接接続以外の給電接続を行う場合(例: テーブルタップの使用)は、特に注意を払う必要があります。
- リア・パネルが下向きになった状態で製品を収納しないでください。

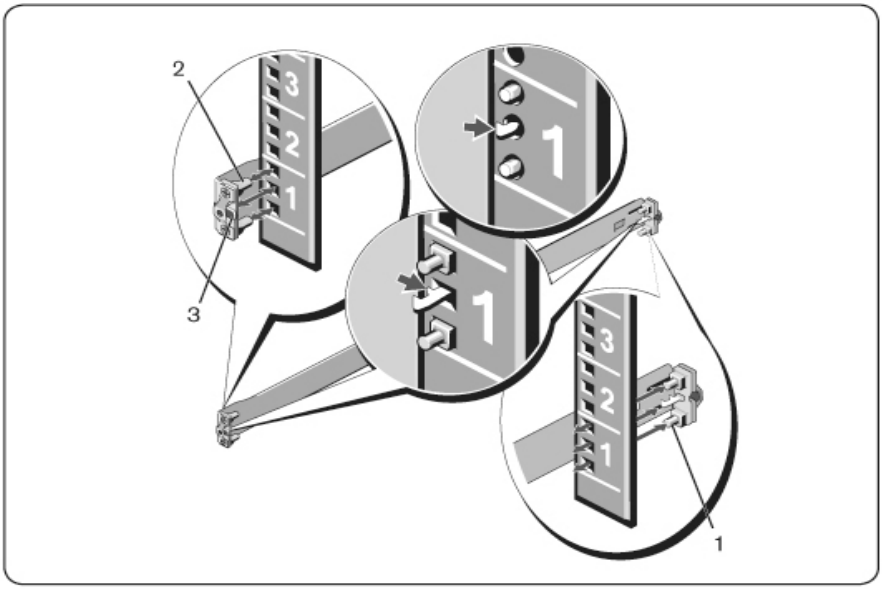
Dell ReadyRails™ システムの取り付け

ReadyRailsシステムを使用すると、RCS設置用に、ラックを簡単に構成できます。ReadyRailsシステムは、1Uツールレス方法、または1Uツール方法の利用可能な3つのうち1つを使用して設置できます(2ポスト・フラッシュ・マウント、2ポスト・センター・マウント、または4ポスト・ネジ穴式)。

1Uツールレス構成(4ポストの角穴または非ネジ式丸穴)

1 ReadyRailsのフランジの端が外側に向いた状態で、1本のレールを左右の垂直ポストの間に設置します。背面フランジのレール・ペグを背面の垂直ポスト・フランジに揃えて固定します。図2.1のアイテム1とその部分拡大図は、角穴および非ネジ式丸穴の両方のケースでペグが取り付けられた様子を示しています。

図 2.1. 1Uツールレス構成



2 ラック正面のフランジ・ペグを垂直柱の前面の穴に入るように合わせ、固定します(アイテム2) 。

3 この手順を2番目のレールでも繰り返します。

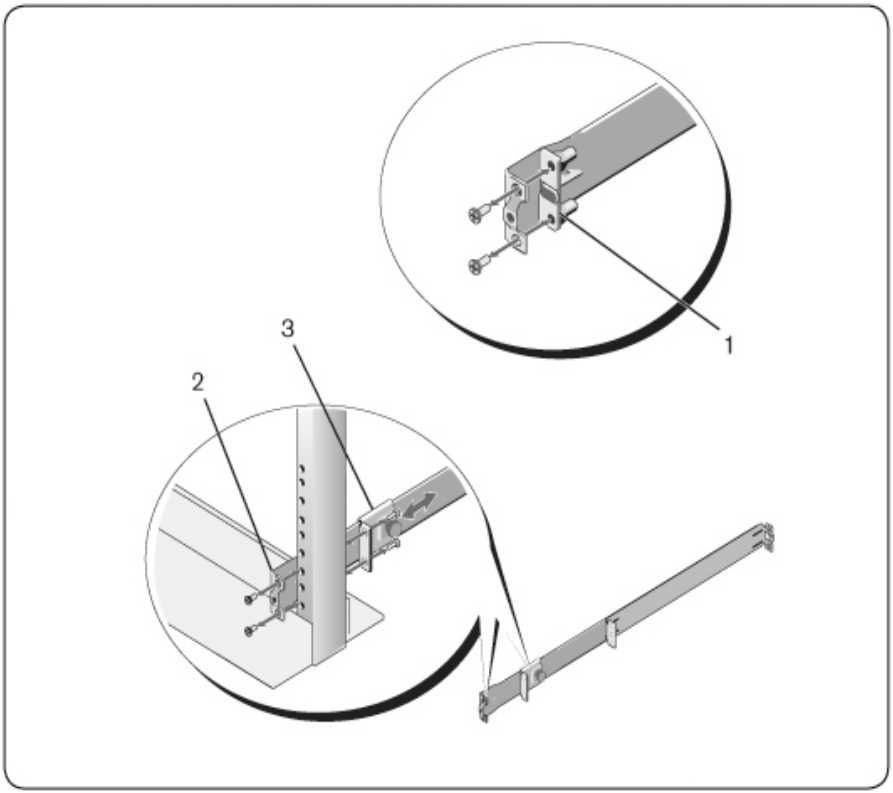
4 各レールを取り外すには、各フランジの端(アイテム3) にあるラッチ・リリース・ボタンを引いて、各レールを取り外します。

2ポスト・フラッシュ・マウント 構成

1 この構成では、各ReadyRailsアッセンブリーの前面からキャストを取り外す必要があります(図 2.2、アイテム1) 。Torx™ドライバーを使用して、前面フランジの端(レールのデバイス側にある) から2つのネジを取り外し、各キャストを取り外します。今後ラックで必要になったときのために、キャストは保管して

おきます。背面フランジ・キャストを取り外す必要はありません。

図 2.2. 2ポスト・フラッシュ・マウント構成



2 ユーザー供給の2個のネジで1本のレールを前面ポスト・フランジに取り付けます(アイテム2) 。

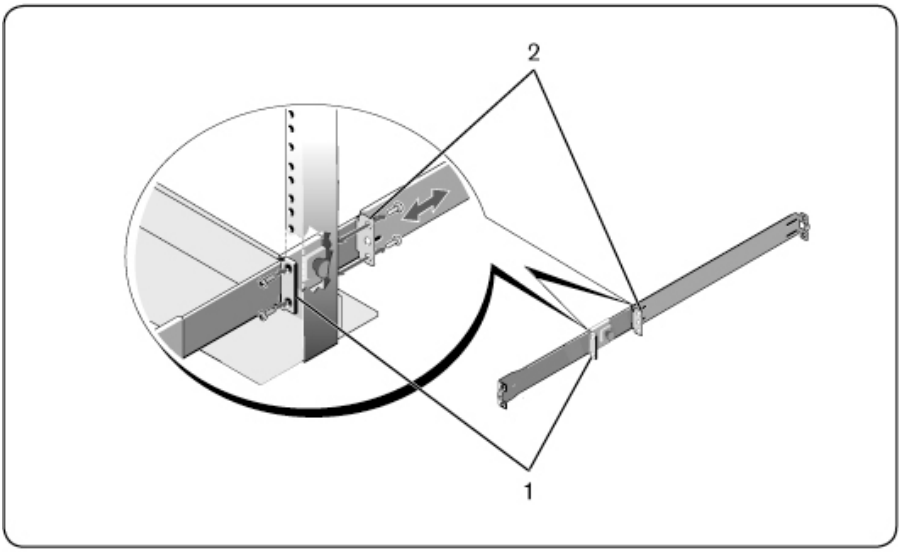
3 プランジャー・ブラケットを垂直ポストに向かって前面にスライドさせて、ユーザー供給の2個のネジでプランジャー・ブラケットをポスト・フランジに固定します(アイテム3) 。

4 この手順を2番目のレールでも繰り返します。

2ポスト・センター・マウント構成

1 カチッという音がして所定の位置に納まるまでプランジャー・ブラケットを後方にスライドさせて、ユーザー供給の2個のネジでプランジャー・ブラケットを前面ポスト・フランジに固定します（図2.3、アイテム1）。

図 2.3. 2ポスト・センター・マウント構成



2 背面ブラケットをポストに向かってスライドさせて、ユーザー供給の2個のネジでポスト・フランジに固定します（アイテム2）。

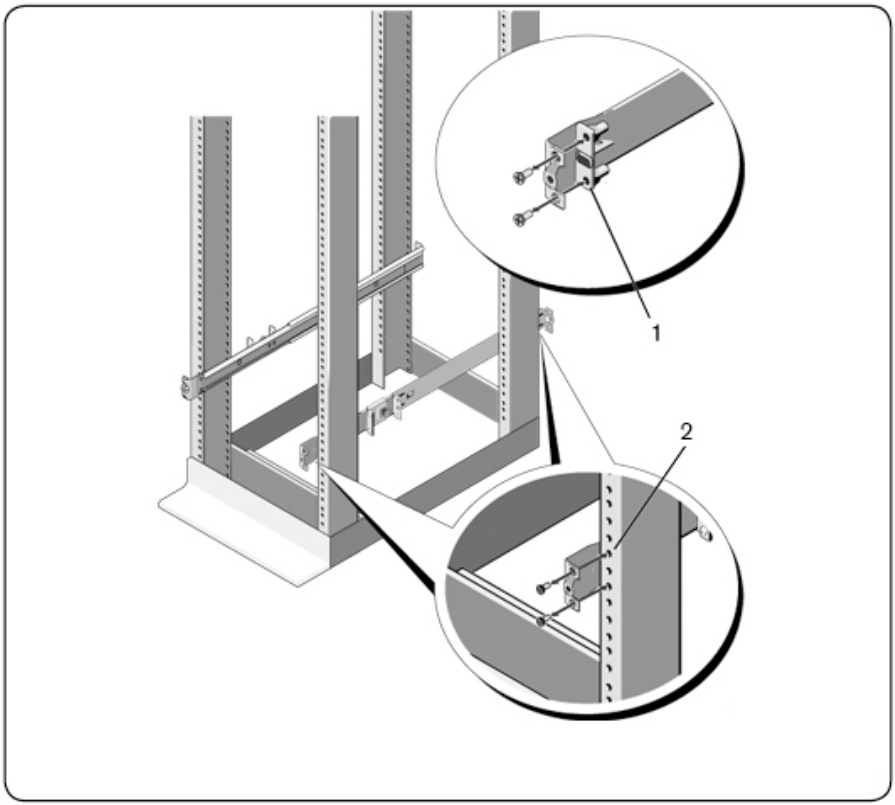
3 この手順を2番目のレールでも繰り返します。

4ポスト・ネジ穴構成

1 この構成では、ReadyRailsアッセンブリーの各端からフランジの端のキャストを取り外す必要があります。Torx™ドライバーを使用して、フランジの各端から2つのネジを取り除き、各キャストを取り除きます(図 2.4、アイテム1) 。今後ラックで必要になったときのために、キャストは保管しておきます。

2 各レールで、ユーザー供給の2個のネジで前面フランジと背面フランジの各端をポストに取り付けます(アイテム2) 。

図 2.4. 4ポスト・ネジ穴構成



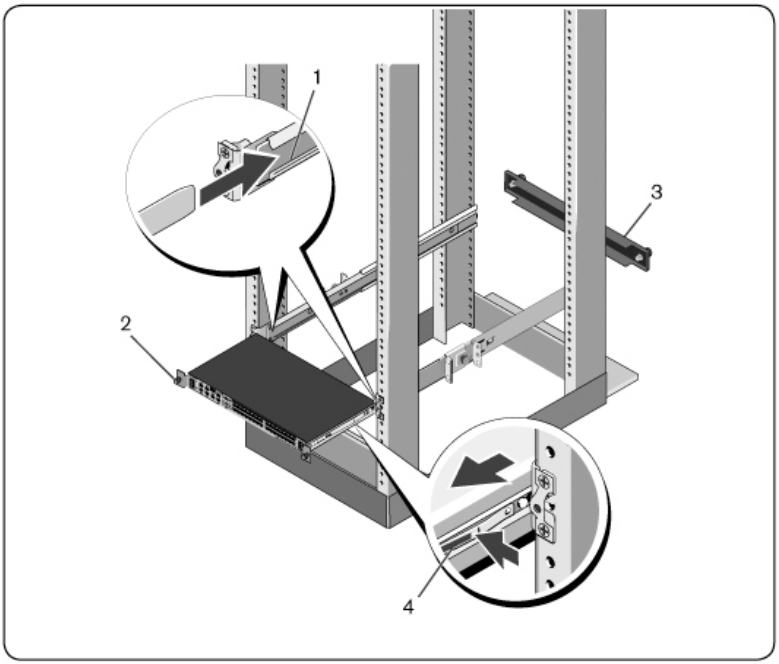
RCSの設置

スイッチは1U背面ラック、1U前面ラック、1U2ポスト（フラッシュおよびセンター）、および0U構成に収納できます。次は、1U背面ラック、1U前面ラック、および0U構成の例です。1U2ポスト（フラッシュおよびセンター）構成では、4ポスト構成と同じ方法で、スイッチをレールにスライドさせることができます。

1U背面ラックの設置

1 スイッチに付いているレールの端をReadyRailsアッセンブリーに挿入し、スイッチをラックに押し入れます(図 2.5、アイテム1) 。

図 2.5. 1U背面ラックの設置



2 各スイッチ・レールを蝶ネジで固定します(アイテム2) 。

3 (オプション) ブランク・パネルをラック前面のレールに取り付け、蝶ネジを固定します(アイテム3) 。

スイッチをラックから取り外すには次の手順を実行します。

1 蝶ネジを外し、トラベル・ストップに達するまで、スイッチ・アッセンブリーをラックから引き出します。トラベルストップの位置は、レールグリップの位置を変えるためのものであり、修理・交換の対象とはしていません。

2 スイッチ・レールの側面にある青いタブを見つけます(アイテム4) 。

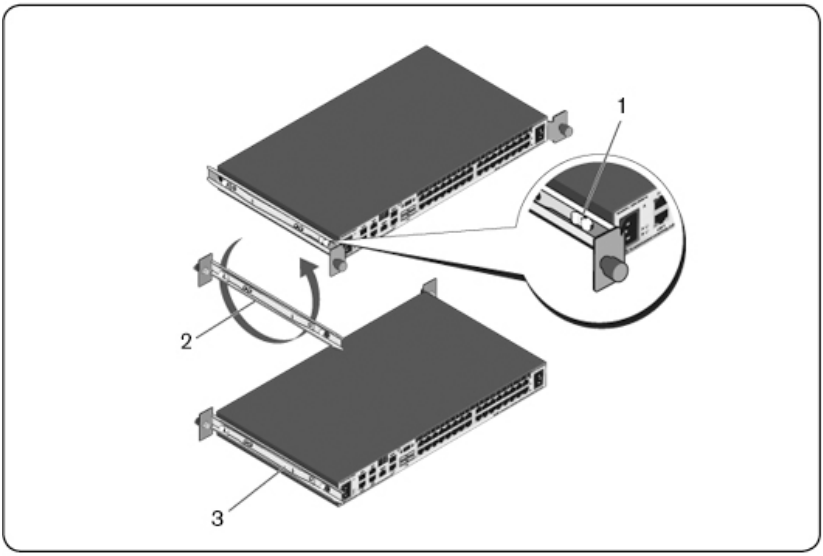
3 タブを内側に押して、スイッチ・レールがReadyRailsアッセンブリーから完全に離れるまでアッセンブリーを引きます。

1U前面ラックの設置

設置する前に、スイッチに取り付けられているレールを再構成する必要があります。

1 各スイッチ・レールで、前面スタンドオフの下にあるタブを持ち上げ、スイッチからレールを持ち上げながらレールを前方にスライドさせます(図 2.6、アイテム1) 。

図 2.6. スイッチ・レールの回転



2 各レールを180°回転させ(アイテム2)、各レールをスイッチに再度取り付けます(アイテム3)。

3 ReadyRailsシステムでのスイッチ・アッセンブリーの挿入と取り外しについては、1U背面ラックの手順を参照してください。

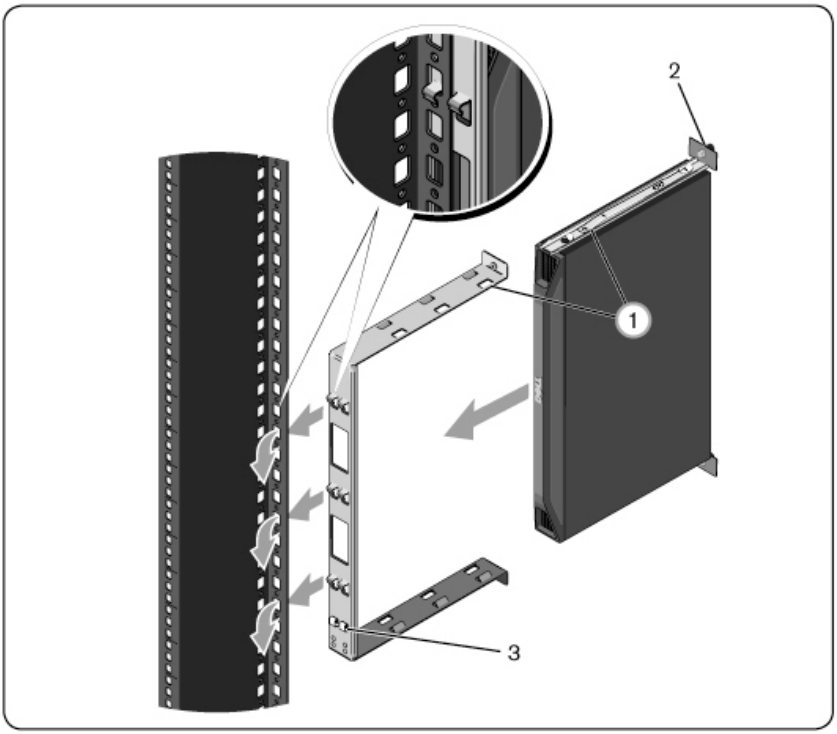
注: この構成ではブランク・パネルは必要ありません。

0U RCSの設置

1 0U取り付け用ブラケットをスイッチ・レールに揃えて取り付けます(図 2.7、アイテム1) 蝶ネジを締めます(アイテム2)。

2 取り付け用ブラケットのフックをラックの穴に挿入し、青いボタンが飛び出してブラケットが所定の位置にロックされるまで押し下げます。

図 2.7. 0Uの設置



スイッチ・アッセンブリーを取り外すには、青いボタン(アイテム3) を押してブラケットの固定を外し、アッセンブリーをポストから持ち上げます。

RCSハードウェアの接続

次の図は、RCSハードウェアの構成の一例です。

図 2.8. 基本的なRCS構成

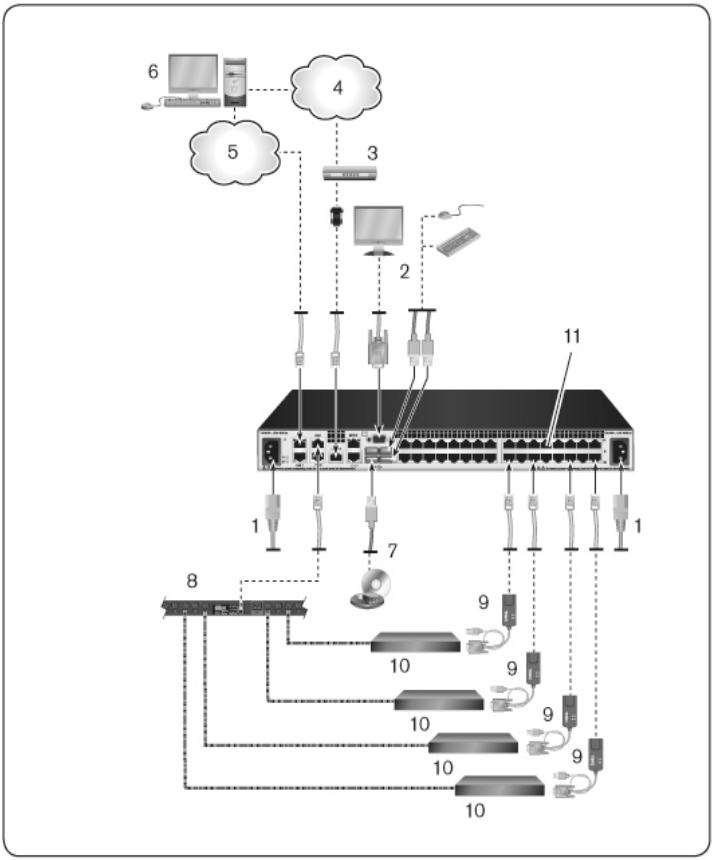


表 2.1: 基本的なRCS構成の説明

番号	説明	番号	説明
1	ジャンパー・コード	7	外部バーチャル・メディア

番号	説明	番号	説明
2	アナログ・ユーザー	8	電源管理装置
3	モデム	9	SIP
4	電話回線ネットワーク	10	ターゲット・デバイス
5	ネットワーク	11	RCS(表示は32ポート・モデル)
6	デジタル・ユーザー		

スイッチを接続して電源を投入するには:

注意: 使用機器への感電や損傷のリスクを抑えるため、ジャンパー・コードの接地プラグは無効にせずにそのまま使用してください。接地プラグは安全上重要な役割を果たします。ジャンパー・コードは、常に容易にアクセスできる接地処理されたコンセントに差し込んでください。装置の電源を切る際は、電源または装置のどちらかの側でジャンパー・コードを引き抜いてください。

注: 建物に3相AC電源がある場合は、コンピューターとモニターが同じ相になっていることを確認します。相が異なっていると、これが原因でビデオやキーボードの機能が正しく作動しないことがあります。

注: スイッチとデバイス間のケーブル長は30 mまではサポートされます。

- 電源の接地プラグを無効にしないでください。接地プラグは安全上重要な役割を果たします。
- ジャンパー・コードは、常に容易にアクセスできる接地処理されたコンセントに接続してください。
- 製品の電源を切る際は、電源または製品のどちらかの側でジャンパー・コードを引き抜いてください。
- 本製品をオフにするには、通常、ACコンセントからコードを抜いてください。AC電源取入口が複数ある製品の場合

は、電源を完全に取り除くために、すべてのACコードの接続を外してください。

- 本製品の筐体内には、ユーザーが修理できる部品はありません。製品のカバーを開けたり取り外したりしないでください。

1 VGAモニター、USBキーボード、およびマウスのケーブルをラベル付きの適切なポートに接続します。

2 UTPケーブル(4ペア、最長45 m)の一方の端を、番号が付いた利用可能なポートに接続します。もう一方の端をSIPのRJ-45コネクターに接続します。

3 SIPをターゲット・デバイスの背面にある適切なポートに接続します。接続するすべてのターゲット・デバイスについて手順2と3を繰り返します。

注: Sun Microsystemsのターゲット・デバイスに接続する際は、VGAとSync on Greenの両方またはComposite Sync(複合同期)機能を備えたSunコンピューターに対応するため、ローカル・ポートで必ずマルチシンク・モニターを使用してください。

4 ユーザーが用意したUTPケーブルをイーサネット・ネットワークからRCS背面のLANポートに接続します。ネットワーク・ユーザーはこのポートを介してRCSにアクセスします。冗長LANポートを個別のイーサネット・スイッチに差し込むと、1つのイーサネット・スイッチが故障した場合の冗長性が高まります。

5 (オプション)スイッチは、ITU V.92、V.90、またはV.24に対応するモデムを使用してもアクセスできます。RJ-45ケーブルの一方の端をスイッチのモデム・ポートに接続します。もう一方の端を付属のRJ-45/DB-9(オス)変換アダプターに接続し、次にこのアダプターをモデム背面にある適切なポートに接続します。

注: LAN接続ではなくモデム接続を使用した場合、スイッチの性能は制限されます。

6 (オプション)サポート対象のPDUをRCSに接続するには、CAT 5ケーブルの一方の端をスイッチのPDU1ポートに接続します。

もう一方の端をPDUに接続します。ターゲット・デバイスからの電源コードをPDUに接続します。PDUを電源に接続します。必要に応じて、同じ手順でPDU2ポートをもう1台のPDUに接続します。

7 各ターゲット・デバイスをオンにし、次にスイッチに付属のジャンパー・コードを取り出します。スイッチ背面にある電源ソケットにコードの一方の端を接続します。もう一方の端を適切な電源に接続します。デュアル電源が装備されているRCSを使用する場合、2番目のジャンパー・コードを使用してRCSの背面にある2番目の電源ソケットに接続し、もう一方の端を別の電源に差し込みます。

注: 冗長電源を個別の分岐回路に差し込むと、外部AC電源が切れた場合の冗長性が高まります。

8 (オプション) バーチャル・メディア・デバイスまたはスマート・カード・リーダーをスイッチの任意のUSBポートに接続します。

注: すべてのバーチャル・メディア・セッションには、USB2またはUSB2およびCAC用SIPを使用する必要があります。

SIPの接続

SIPを各サーバーに接続するには:

1 お使いのRCS用のSIPを見つけます。

2 PS/2 SIP接続を使用している場合、このRCSに接続する最初のサーバーのキーボード、マウス、モニターの適切なポートに、SIPケーブルの色別された両端を接続します。USB接続を使用している場合、このRCSに接続する最初のサーバーのUSBポートに、SIPからプラグを接続します。

3 SIPのRJ-45コネクターに、SIPからRCSに延びるCAT 5ケーブル配線の一方の端を接続します。図 2.9を参照してください。

4 CAT 5ケーブルのもう一方の端を、RCS背面にある目的のAvocent Rack Interface (ARI) ポートに接続します。

5 接続するサーバーすべてで2～4の手順を繰り返します。

注: 使用する前にRCSの電源を切ります。必ず、ジャンパー・コードを電源から抜いてください。

注: RCSのデバイスへの接続には、Dell SIPのほかに、Avocent IQモジュール(Sunモジュールおよびシリアル IQモジュールを含む) を使用することもできます。

図 2.9. SIP接続

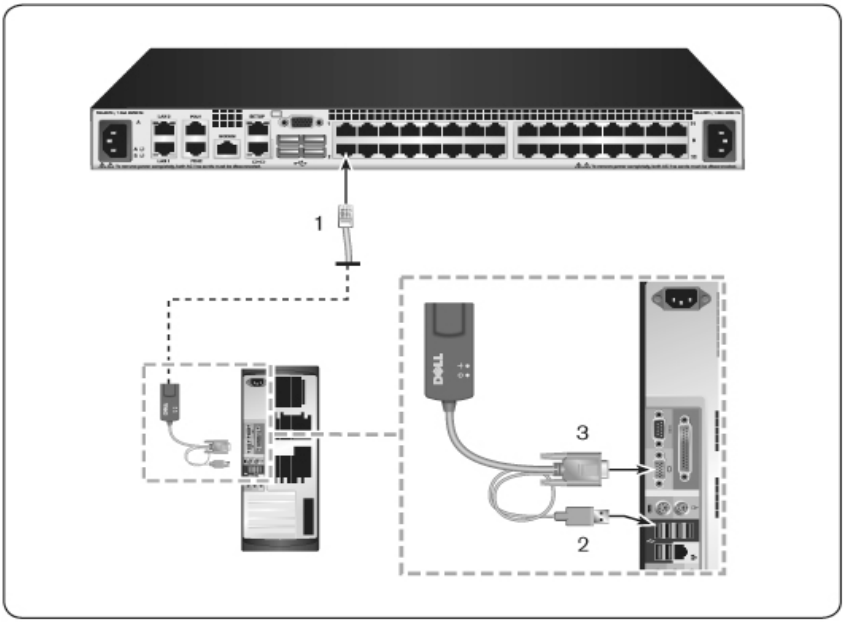


表 2.2: 図 2.9の説明

番号	説明
1	CAT 5
2	USB接続
3	VGA接続

UTPコネクターを使用してSIPをシリアル・デバイスに接続するには次の手順を実行します。

1 SIPのRJ-45コネクターをシリアル・デバイスに接続します。

-または-

SIPをRJ-45／9ピン(メス)変換アダプターに接続します。アダプターをシリアル・デバイスのシリアル・ポートに接続します。

2 UTPケーブル(4ペア、最長45 m)の一方の端を、スイッチの背面にある番号が付いた利用可能なポートに接続します。もう一方の端をSIPのRJ-45コネクターに接続します。

3 USB／バレル間電源コードをSIPの電源コネクターに接続します。USB／バレル間電源コードのUSBコネクターを、シリアル・ターゲット・デバイスの任意の使用可能なUSBポートに接続します。

ティアド・スイッチの追加

注: RCSはEL80-DTをサポートしていません。

注: M1000eモジュラー・エンクロジャーは、ティアド構成に対応しています。CAT 5ケーブルの一端を、RCSスイッチのターゲット・ポートに接続します。もう一方の端を、M1000eシャーシの後部にあるiKVMモジュールのPJ45ポートと互換性のあるアナログ・コンソール・インターフェイス(ACI)に取り付けます。M1000eモジュール・エンクロージャーの構成部品に対するファームウェアのアップデートは、このティアド構成を介してはできません。

スイッチを2レベルまでティア接続して、ユーザーを最大1024台のサーバーに接続できます。ティアド(階層形式)システムでは、メイン・スイッチの各ターゲット・ポートを、各ティアド・スイッチのACIポートに接続します。各ティアド・スイッチは、SIPまたはAvocent IQモジュールが接続されているデバイスに接続できます。

複数のスイッチをティア接続するには次の手順を実行します。

1 UTPケーブルの一端をスイッチのターゲット・ポートに接続します。

2 UTPケーブルのもう一方の端を、ティアド・スイッチの背面にあるACIポートに接続します。

3 ティアド・スイッチにデバイスを接続します。

4 システムに接続するすべてのティアド・スイッチに対して、この手順を繰り返します。

注: システムが自動的に2つのスイッチを統合します。ローカルUIのメイン・スイッチの一覧には、ティアド・スイッチに接続されているすべてのスイッチが表示されます。

注: スイッチは、メイン・スイッチのターゲット・ポートごとに1つのティアド・スイッチをサポートしています。ティアド・スイッチに、スイッチを接続することはできません。

注: RCSでカスケード接続を行う場合、8ポートまたは16ポートのアナログ・コンソール・スイッチはティアド構成のプライマリー・ユニットとしては使用できません。RCSはプライマリー・ユニットである必要があります。

図 2.10. UTPアナログ・スイッチとのRCSのティア接続

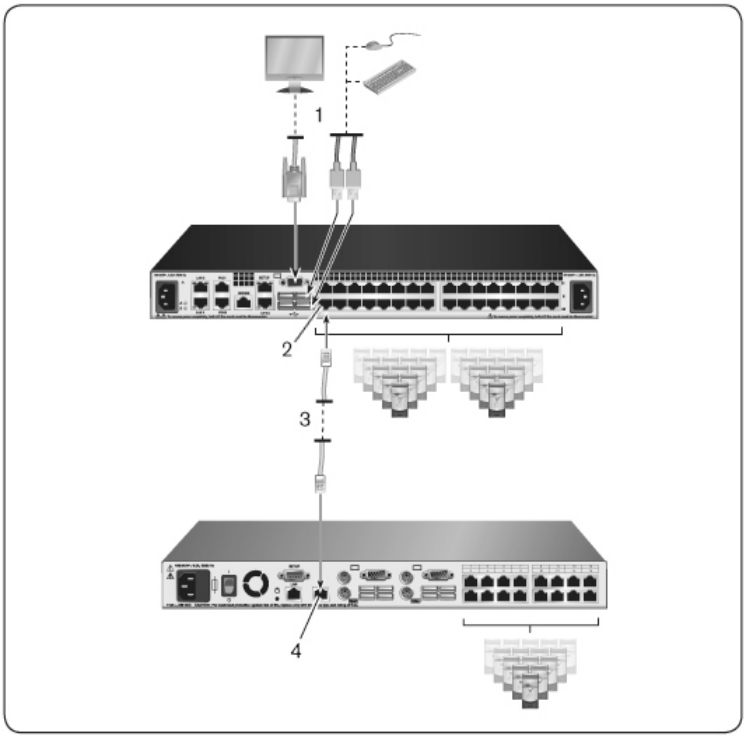


表 2.3: 図 2.10の説明

番号	説明
1	ローカル・ユーザー
2	ARI接続
3	UTP接続
4	ACI接続

レガシー・スイッチでのカスケード接続

レガシー・スイッチ(オプション)を追加するには:

1 スイッチをラックに収納します。RCSとレガシー・スイッチを接続するUTPケーブルを用意します。

2 UTPケーブルの一端をコンソール・スイッチのARIポートに接続します。

3 UTPケーブルのもう一方の端をPS/2 SIPに接続します。

4 スイッチ・メーカーの推奨事項に従って、SIPをレガシー・スイッチに接続します。

5 スイッチに取り付けるすべてのレガシー・スイッチで1～4の手順を繰り返します。

注: RCSはARIポートごとに1つのスイッチのみをサポートしています。この最初のスイッチの下に他のスイッチをカスケード接続することはできません。

注: RCSでカスケード接続を行う場合、8ポートまたは16ポートのアナログ・コンソール・スイッチはプライマリー・ユニットとしては使用できません。RCSはプライマリー・ユニットである必要があります。

図 2.11. レガシー・スイッチのカスケード 接続

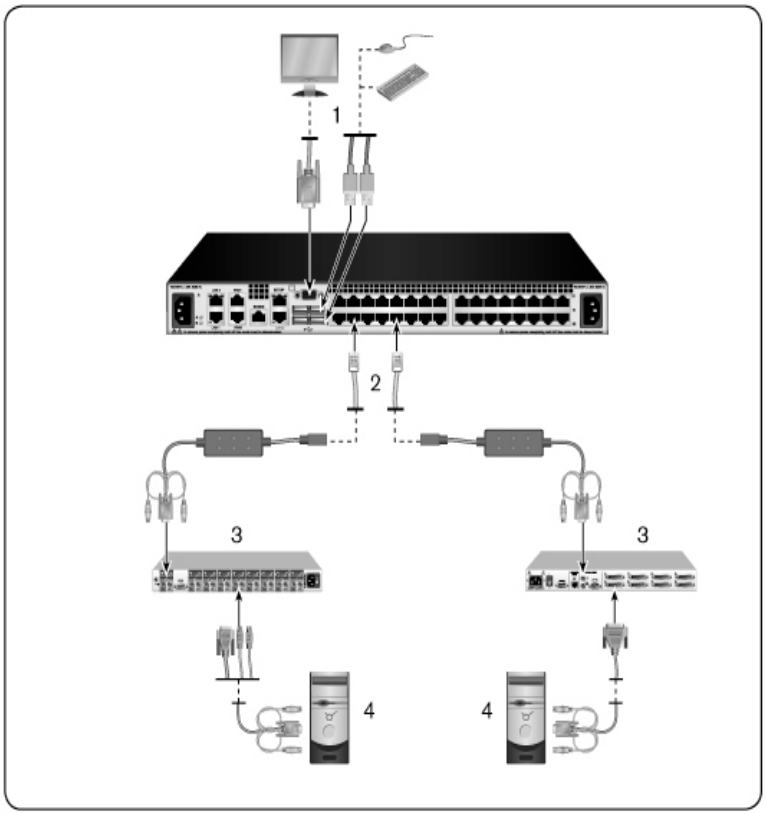


表 2.4: 図 2.11の説明

番号	説明
1	ローカル・ユーザー
2	ARI接続

番号	説明
3	PS2接続
4	ターゲット 接続

PEM(オプション) の追加

ポート 拡張モジュール(PEM) により、各ARIポート を拡張して対応デバイス数を1台から最大で8台にすることができます。次の図および図の説明の表を参照してください。

注: PEMは受動的に作動します。従って、PEMに接続されたデバイスのうちの1台にユーザーがアクセスすると、その後にこのPEMに接続されている他のデバイスのいずれかに他のユーザーがアクセスしようとしてもすべてブロックされます。

注: PEMが働いている状態でのVMまたはCAC SIPの使用はサポート されていません。

注: トゥルー・シリアルSIPはPEMが働いている状態では作動しません。

PEM(オプション) を追加するには次の手順を実行します。

1 PEMをラックに収納します。UTPケーブルは9本まで使用できます。このうちの1本はRCSを PEMに接続するために使用し、他の8本は各デバイスに接続されている SIPに PEMを 接続するために使用します。

2 PEMと RCSをつなぐ UTPケーブルの一方の端を、PEM上の他のコネクターからは若干離れた位置のRJ-45コネクターに接続します。UTPケーブルのもう一方の端を、RCSの後面にある目的のARIポート に接続します。

3 PEM背面に並んでいる8つのRJ-45コネクターのいずれか1つに、PEMと各デバイスのSIPをつなぐ UTPケーブルを接続します。

4 UTPケーブルのもう一方の端を最初のSIPに接続します。

5 接続したいデバイスのすべてで3～4の手順を繰り返します。

図 2.12. PEMと のRCS構成

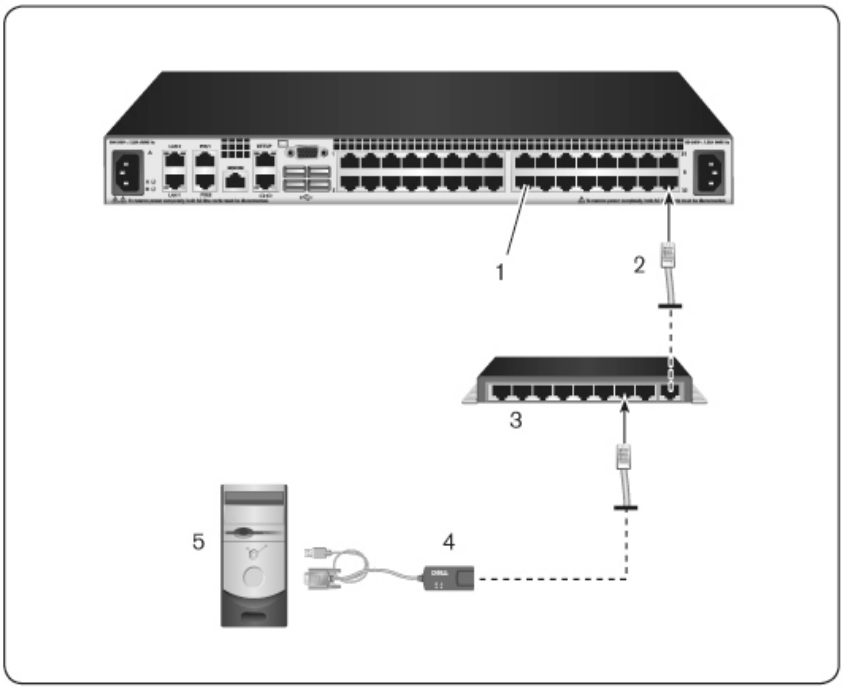


表 2.5: 図 2.12の説明

番号	説明
1	ARIポート
2	UTP
3	PEM
4	SIPまたはAvocent IQモジュール
5	サーバー

Remote Console Switchの構成

すべての物理接続が完了したら、スイッチ・システム全体で使用するためにスイッチを構成する必要があります。これを実行するには2つの方法があります。

Avocent管理ソフトウェアを使用してスイッチを構成するには、ご使用の製品の『インストーラ／ユーザー・ガイド』掲載の詳細な手順を参照してください。

ローカルUIを使用してスイッチを構成するには次の手順を実行します。

ローカルUIを使用して最初のネットワーク・セットアップを構成する詳細な手順については、「ネットワーク設定」(ページ 61) を参照してください。

組み込みWebサーバーの設定

組み込みWebサーバーを使用してスイッチにアクセスして、スイッチに関する日常作業のほとんどを処理できます。Webサーバーを使用してスイッチにアクセスする前に、まずスイッチの背面パネルにあるSETUPポートまたはローカルUIを介してIPアドレスを指定します。スイッチのユーザー・インターフェイスを使用する詳細な手順については、第3章を参照してください。

ファイアウォールを使ったOBWIへの接続

アクセスにOBWIを使用するスイッチの設置では、外部にアクセスする必要がある場合は、ファイヤーウォールで次のポートが開いている必要があります。

表 2.6: ファイヤーウォールでのOBWIポート

ポート番号	機能
TCP 22	SIPへのシリアル・セッションのSSHに使用されます。
TCP 23	(Telnetが有効な場合) Telnetに使用されます。
TCP 80	ビデオ・ビューアの最初のダウンロードに使用されます。RCS管理者はこの値を変更できます。
TCP 443	スイッチの管理とKVMセッションの起動を行うWebブラウザ・インターフェイスに使用されます。RCS管理者はこの値を変更できます。
TCP 2068	スイッチでのKVMセッション・データ(マウス／キーボード)の伝送またはビデオの伝送に使用されます。
TCP/UDP 3211	検出用です。
TCP 389	(オプション) LDAP Directory Servicesによって使用される - 標準アクセス・ポート
TCP 636	(オプション) LDAP Directory Servicesによって使用される - セキュア／SSLポート
TCP 3268	(オプション) Microsoft Active Directory Servicesによって使用される - 標準アクセス・ポート
TCP 3269	(オプション) Microsoft Active Directory Servicesによって使用される - セキュア／SSLアクセス・ポート

次の図と表は一般的な構成を示します。この構成では、ユーザーのコンピューターはファイヤーウォールの外側に位置し、スイッチはファイヤーウォールの内側に位置します。

図 2.13. 一般的なRCSファイヤーウォールの構成

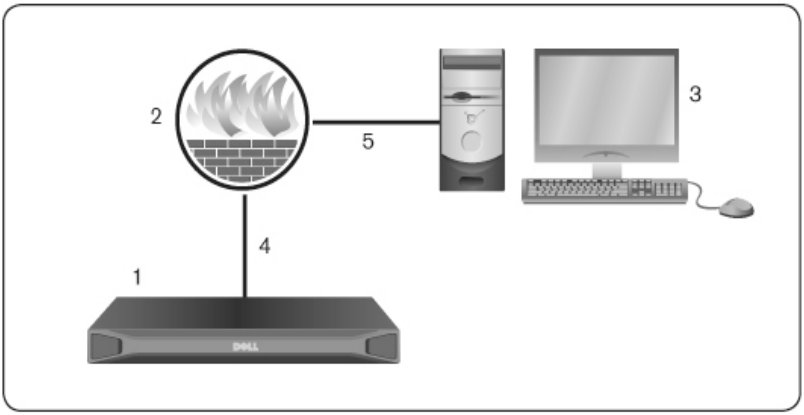


表 2.7: 図 2.13の説明

番号	説明
1	RCS
2	ファイアウォール
3	ユーザーのコンピューター
4	ファイヤーウォールはHTTP要求とKVMトラフィックをスイッチへ転送します。
5	ユーザーはファイヤーウォールの外部IPアドレスを参照します。

ファイヤーウォールを構成するには次の手順を実行します。

ファイヤーウォールの外側からスイッチにアクセスするには、ファイヤーウォールの内部インターフェイスを介して、外部インターフェイスからKVMスイッチにポート22、23(Telnetが有効な場

合）、80、443, 2068、3211が転送されるようにファイヤーウォールを構成します。ファイヤーウォールの特定ポートの転送手順については、マニュアルを参照してください。

注: 管理者はポート 80と 443を再構成できます。

OBWIの起動の詳細については、「OBWI」（ページ 49）を参照してください。

接続の確認

リア・パネルのイーサネット接続LED

RCSのリア・パネルには、イーサネット LAN1の接続状態を示すLEDと、イーサネット LAN2の接続状態を示すLEDがそれぞれ2つあります。

- ネットワークへの有効な接続が確立されると緑のLEDが点灯し、ポートにアクティビティがあるときは点滅します。
- 両色LEDは、緑または黄色に点灯します。
  - 通信速度が1000Mの時には緑色に点灯します。
  - 通信速度が100Mの時には黄色に点灯します。
  - 通信速度が10Mの時には点灯しません。

リア・パネルの電源状態LED

各RCSのリア・パネルには、電源LEDが電源ごとに1つあります。デュアル電源モデル（16ポート および32ポート）には電源LEDが2つあり、8ポート・モデルのLEDは1つのみです。スイッチに電源が入り正常に動作しているとき、LEDは緑に点灯します。

- 電源が入っていなかったり、エラーが発生すると、LEDはオフになります。
- ユニットが準備完了になると、LEDは点灯します。

- スイッチの起動中またはアップグレード処理中は、LEDは点滅します。
- 電源エラー、周辺温度の上昇、ファンのエラーなどの障害が検出されたとき、LEDは「SOS」を点滅します。障害が続く限り、LEDは「SOS」を点滅し続けます。

モジュールの電源が失われた場合、スイッチは接続されているデバイスからのシリアル・ブレークを防止します。ただし、シリアル・セッション・ビューアの**シリアル・ブレーク**を押すことにより、接続されているデバイスでシリアル・ブレークを生成できます。

ターゲット・デバイスのマウス設定の調整

スイッチに接続したコンピュータをリモート・ユーザー制御用に使用するには、ターゲット・マウスの速度の設定を行い加速をオフにする必要があります。Microsoft® Windows®(Windows NT®、2000、XP、Server 2003)を稼動しているマシンでは、デフォルトのPS/2マウス・ドライバーを使用してください。

ローカル・マウスの動きとリモート・カーソルの表示の間で同期が保たれるように、KVMスイッチを介してリモート・システムにアクセスするすべてのユーザー・アカウントでは、マウス加速度を「なし」に設定する必要があります。また、マウス加速度は、各リモート・システムで「なし」に設定する必要があります。特殊なカーソルは使用しないでください。また、カーソルの表示(ポインターの軌跡、*Ctrl*キーでカーソルの位置表示、アニメーション、カーソルの影の有効、カーソルの非表示など)のオプションもオフにしてください。

注: Windowsオペレーティング・システムからマウス加速度を無効にできない場合や、すべてのターゲット・デバイスの設定を変更したくない場合は、ビデオ・ビューア・ウィンドウにある *Tools* → *Single Cursor Mode* コマンドを使用できます。このコマンドにより、ビデオ・ビューア・ウィンドウが「透明マウス」モードになります。これにより、表示しているターゲット・システムのマウス・ポインターとクライアント・コンピューターのマウス・ポインターの制御とを手動で切り替えることができます。

3

ローカルおよびリモート の構成

RCSには、「 ポイント ･アンド ･クリック」インターフェイスである、ローカル･ユーザー･インターフェイス(ローカルUI) およびリモート OBWIが備えられています。これらのインターフェイスで利用できる構成オプションを使用して、特定のアプリケーションに合わせてスイッチを調整したり、接続デバイスを制御したり、すべての基本的なKVMまたはシリアル･スイッチのニーズを処理したりできます。

注: ローカルUIとリモート OBWIはほとんど同じものです。指定がない限り、この章のすべての情報は両方のインターフェイスに適用されます。

どちらのインターフェイスからも、2種類のセッションを起動できます。

- ビデオ･ビューア･ウインドウでは、スイッチに接続された個々のターゲット ･デバイスのキーボード 、モニター、マウスの機能をリアルタイムで制御できます。また、ビデオ･ビューア･ウィンドウ内では、事前に定義されたグローバル･マクロを使用して操作を実行することもできます。ビデオ･ビューアの使用方法については、第4章を参照してください。
- シリアル･ビューア･ウィンドウでは、コマンドまたはスクリプトを使用して、個々のシリアル･ターゲット ･デバイスを管理できます。

ローカル・ユーザー・インターフェイス (LUI)

スイッチの背面にはローカル・ポートがあります。このポートを使用してキーボード、モニター、およびマウスをスイッチに直接接続して、ローカルUIを使用できます。

次の任意のキーストロークを選択して構成し、ローカルUIを開いたり、ローカルUIとアクティブ・セッション間を切り替えるようにできます。使用できるキーストロークは、<Print Screen>、<Ctrl + Ctrl>、<Shift + Shift>、<Alt + Alt>です。デフォルトは<PrintScreen>と <Ctrl-Ctrl>です。

ローカルUIを起動するには次の手順を実行します。

1 モニター、キーボード、マウスのケーブルをスイッチに接続します。詳細については、「RCSハードウェアの接続」(ページ 27) を参照してください。

2 任意の有効なキーストロークを押して、ローカルUIを起動します。

3 ローカルUI認証が有効にされている場合は、ユーザー名とパスワードを入力します。

注: スイッチがAvocent管理ソフトウェア・サーバーに追加されている場合は、ユーザー認証のために、Avocent管理ソフトウェア・サーバーにアクセスします。スイッチがAvocent管理ソフトウェア・サーバーに追加されていない場合や、Avocent管理ソフトウェア・サーバーに接続できない場合は、ユーザー認証のために、スイッチのローカル・ユーザー・データベースにアクセスします。デフォルトのローカル・ユーザー名はAdminです。パスワードはありません。ローカル・ユーザー・データベースのユーザー名は、大文字と小文字が区別されます。

ローカル・ポートのユーザー・インターフェイスに接続されたターゲット・デバイスは、左側ナビゲーション・ツールバーから選択できる2つの個別の画面から表示して管理することができます。ターゲットの数が20未満の場合は、「Target List-Basic」画面が操作用として推奨

されます。20個以上のターゲット・デバイスの場合は、「Target List-Full」画面で追加の操作ツールが提供されます。「Target List-Full」画面では、ページ番号の入力、ページ操作ボタンの使用、フィルターの使用を活用する操作が可能です。「Basic」、「Full」画面のいずれかを、ターゲット・デバイス選択用のデフォルト画面として設定することができます。

フィルタリング機能

一致項目を取得するために使用するテキスト・ストリングを入力して、ターゲット・デバイスのリスト情報をフィルタリングすることができます。フィルタリングによって、項目のより短く、正確なリストが提供可能になります。フィルタリングを実行すると、Name列を対象として、指定したテキスト・ストリングを検索します。この検索では大文字／小文字を区別しません。フィルタリングでは、テキスト・ストリングの前後にワイルドカードとしてアスタリスク(*)を使用することができます。例えば、*emailserver**と入力して*Filter*をクリックすると、emailserverから始まる項目(emailserver、emailserverbackupなど)が表示されます。

OBWI

スイッチのOBWIは、リモートのWebブラウザ・ベースのユーザー・インターフェイスです。システム・セットアップの詳細については、「RCSハードウェアの接続」(ページ 27)を参照してください。次の表に、OBWIでサポートされているオペレーティング・システムとブラウザの一覧を示します。必ず最新バージョンのWebブラウザを使用してください。

表 3.1: OBWIでサポート されているオペレーティング・システム

オペレーティング・システム	ブラウザ	
	Microsoft® Internet Explorer バージョン6.0 SP1以降	Firefox バージョン2.0以降
Microsoft Windows 2000 WorkstationまたはServer (Service Pack 2)	はい	はい
Microsoft Windows Server® 2003 Standard、EnterpriseまたはWeb Edition	はい	はい
Microsoft Windows Server® 2008 Standard、EnterpriseまたはWeb Edition	はい	はい
Windows XP Professional(Service Pack 3)	はい	はい
Windows Vista® Business(Service Pack 1)	はい	はい
Red Hat Enterprise Linux® 4および5 Standard、EnterpriseまたはWeb Edition(スマート・カード はオペレーティング・システムでサポート されていない場合があります)	いいえ	はい
Sun Solaris® 9および10(スマート・カード はオペレーティング・システムでサポート されていない場合があります)	いいえ	はい
Novell SUSE Linux Enterprise 10および11(スマート・カード はオペレーティング・システムでサポート されていない場合があります)	いいえ	はい
Ubuntu 8 Workstation(スマート・カード はオペレーティング・システムでサポート されていない場合があります)	いいえ	はい

スイッチのOBWIにログインするには:

1 Webブラウザを起動します。

2 ブラウザのアドレス欄に、アクセスするスイッチに割り当てられているIPアドレスまたはホスト名を入力します。
「 http://xxx.xx.xx.xx」または「 https://xxx.xx.xx.xx」の形式を使用してください。

注: IPv6モードを使用している場合は、IPアドレスを角括弧で囲む必要があります。「 http://[<ipaddress-] 」の形式を使用します。

3 ブラウザがスイッチに接続されたらユーザー名とパスワードを入力し、*Login*をクリックします。スイッチのOBWIが表示されます。

注: デフォルトのユーザー名はAdminです。パスワードは必要ありません。

ファイヤーウォールの外側からスイッチのOBWIにログインするには、上記の手順を繰り返し、代わりにファイヤーウォールの外部IPアドレスを入力します。

注: RCSは、お使いのコンピューターにJavaがすでにインストールされているかどうか、検出を試みます。インストールされていない場合、OBWIを使用するにはインストールが必要です。また、JNLPファイルをJava WebStartに関連付ける必要もあります。

注: OBWIを使用するには、Java Runtime Environment(JRE) バージョン1.6.0_11以降が必要です。

注: OBWIにいったんログインすると、ログアウトするか、セッションのアイドル時間が管理者指定のタイムアウトを超過した場合を除いて、新規セッションを起動する際にログインしなおす必要はありません。

ユーザー・インターフェイスの使用

認証後に、ユーザー・インターフェイスが表示されます。ここでは、スイッチの表示、アクセス、管理を行ったり、システム設定の指定とプロファイル設定の変更を行うことができます。次の図に、ユー

ザー・インターフェイスのウィンドウ領域を示します。画面の説明を、続く表に示します。

図 3.1. ユーザー・インターフェイス・ウィンドウ

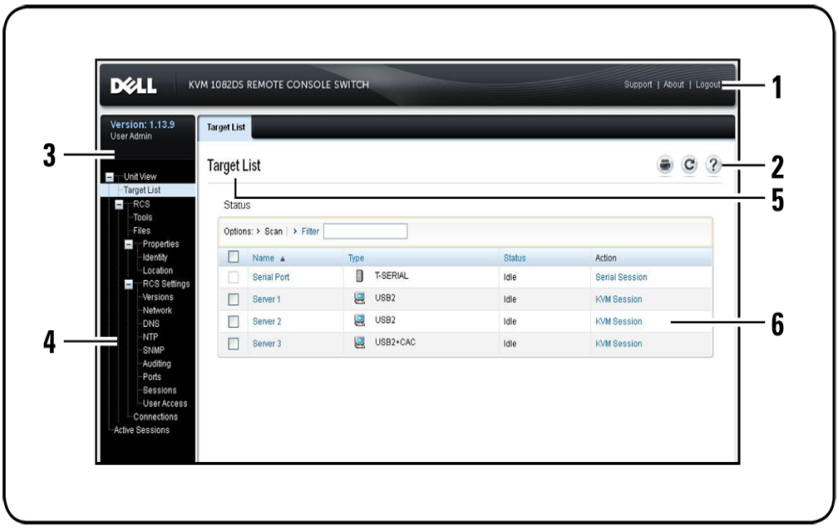


表 3.2: ユーザー・インターフェイスの説明

番号	説明
1	トップ・オプション・バー: トップ・オプション・バーを使用して、テクニカル・サポートに連絡したり、ソフトウェアの一般情報を表示したり、OBWIセッションからログアウトしたりします。
2	2番目のオプション・バー: このバーを使用して、Webページを印刷したり、現在のWebページを更新したり、ヘルプ・ツールにアクセスしたりします。

番号	説明
3	バージョン・ブロック: 製品のファームウェアのバージョンと現在ログインしているユーザー名が、トップ・オプション・バーの左側に表示されます。
4	サイド・ナビゲーション・バー: サイド・ナビゲーション・バーを使用して、表示する情報を選択します。サイド・ナビゲーション・バーでは、設定の変更や操作を実行するためのウィンドウを表示できます。
5	ナビゲーション・タブ: 選択したタブのコンテンツ領域にシステム情報が表示されます。一部のタブにはサブタブがあり、クリックして表示し、カテゴリ内の詳細を変更できます。
6	コンテンツ領域: コンテンツ領域を使用して、スイッチのOBWIシステムを表示したり、変更したりすることができます。

セッションの起動

注: セッションを起動するには、Java 1.6.0_11以降が必要です。

セッションを起動するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、Target Listを選択します。利用可能なデバイスの一覧が表示されます。

2 Action列に、KVMセッションまたはシリアル・セッションのうち適用可能な操作が表示されます。適用可能な操作は、セッションを起動するように選択したターゲット・デバイスによって異なります。指定したターゲット・デバイスに適用可能な操作が複数ある場合は、ドロップダウン矢印をクリックして、一覧から適用する操作を選択します。

ターゲット・デバイスが使用中の場合、プリエンプト操作のレベルが現在のユーザーのレベルと同等またはそれ以上であれば、デバイスに強制的に接続してアクセスできます。

また、RCSでは外部TelnetまたはPuTTYなどのSSHアプリケーションを介して、シリアルSIPへのシリアル・セッションを行えます。TelnetおよびSSHのセッションはシリアルSIPへの接続にのみ使用され、RCSまたはKVMのターゲット・デバイスへのアクセスまたは管理には使用できません。

TelnetまたはSSHアプリケーションからシリアル・セッションを起動するには次の手順を実行します。

1 シリアルSIPが接続されているRCSホスト IPアドレスを入力します。

2 <RCSユーザー名>:<シリアルSIP名>、たとえば、jsmith:routerを入力します。

3 RCSユーザーのパスワードを入力します。

注: Telnet機能はデフォルトでは無効です。Telnetサポートを有効にするには、「シリアル・セッションの構成」(ページ 85) を参照してください。

ローカルUIからアクティブなセッションに切り替えるには(ローカル・ユーザーのみ):

1 サイド・ナビゲーション・バーから、**Local Session**を選択します。

2 **Resume Active Session**チェックボックスをオンにします。「ビデオ・ビューア」ウィンドウが表示されます。

スキャン・モード

スキャン・モードでは、スイッチにより複数のターゲット・デバイスがスキャンされます。スキャンは、一覧内でターゲット・デバイスが表示されている順序に従って実行されます。また、スキャンが一覧の次のターゲット・デバイスに移動するまでの時間を設定できます。

注: モデム経由で接続している場合、「Scan」ボタンは無効です。

スキャン・リストにターゲット・デバイスを追加するには

1 サイド・ナビゲーション・バーから、**Unit View → TTarget List**の順に選択して、Target Devices画面を開きます。

2 スキャンするターゲット・デバイスの横にあるチェックボックスをオンにします。

3 **スキャン** をクリックします。

スキャン時間を構成するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、**Ports → Local Port UI**の順に選択して、Local Port UI Settings画面を開きます。

2 「スキャン・モード」ヘッダーの下で、「Scan Time」フィールドに時間を秒単位(3〜255)で入力します。

3 **Save**をクリックします。

システム情報の表示

ユーザー・インターフェイスの以下の画面では、スイッチおよびターゲット・デバイスの情報を表示することができます。

表 3.3: システム情報

カテゴリ	操作画面の選択順	表示内容
RCS	*Unit View → RCS → Tools*	RCS名とタイプ、RCSツール(メンテナンス、診断、証明書およびとトラップMIB)
	Unit View → RCS → Files	RCS構成、ユーザー・データベース、およびターゲット・デバイス

カテゴリ	操作画面の選択順	表示内容
	Unit View → *RCS* → *Properties* → *Identity*	部品番号、シリアル番号、およびEID
	Unit View → *RCS* → *Properties* → *Location*	サイト、部門およびロケーション
	Unit View → *RCS Settings* → *Versions*	現在のアプリケーションおよびブート・バージョン
ターゲット・デバイス	*Unit View* → *Target Devices*	接続されているターゲット・デバイスの一覧、ならびに、名前、タイプ、状態、および各デバイスの操作 以下の追加情報を表示するには、ターゲット・デバイスをクリックします: 名前、タイプ、EID、使用できるセッション・オプションおよび接続パス

RCSツール

Tools → Maintenance → Overview画面では、アプライアンス名とタイプを表示できます。また、基本的なアプライアンス・タスクを実行できます。

RCSの再起動

RCSを再起動するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、**Unit View** → **RCS** → **Tools** → **Maintenance** → **Overview**のタブの順に選択して、Unit Maintenance 画面を開きます。

2 *Reboot*をクリックします。

3 ダイアログ・ボックスが表示され、すべてのアクティブ・セッションの接続が解除されることを警告します。*OK*をクリックします。

注: ローカルUIを使用している場合、スイッチの再起動中、画面は空白になります。リモート OBWIを使用している場合、アプライアンスでインターフェイスが再起動の完了を待機していることを通知するメッセージが表示されます。

RCSファームウェアのアップグレード

RCSを最新のファームウェアにアップデート できます。

アップグレード によりFLASHメモリーが再プログラムされると、スイッチはソフト・リセットを実行し、すべてのSIPセッションを終了します。ターゲット・デバイスでSIPのファームウェア・アップデートを実行中の場合に、表示されなくなるか、または接続されていないと表示されることがあります。フラッシュ・アップデート が完了すると、ターゲット・デバイスは正常に表示されるようになります。

注意: ファームウェア・アップデート 中にSIPの接続を解除したり、ターゲット・デバイスのパワー・サイクリング(一旦電源を切って入れ直す) を行ったりすると、モジュールが作動不能となりSIPの工場返送や修理の必要が生じる場合があります。

スイッチのファームウェアをアップグレード するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、*Unit View* → *RCS* → *Tools* → *Maintenance* → *Upgrade*のタブの順に選択して、Upgrade RCS Firmware

ウィンドウを開きます。

2 *Upgrade*をクリックして、Upgrade Appliance Firmwareを開きます。

3 ファームウェア・ファイルを読み込むには、次の方法のなかから1つを選択します: *Filesystem*、*TFTP*、*FTP*、*HTTP*。

注:「 Filesystem」オプションは、リモート OBWIでのみ使用できます。

4 Filesystemを選択した場合、*Browse*を選択して、ファームウェア・アップグレード・ファイルの場所を指定します。

-または-

「 TFTP」を選択した場合、サーバーのIPアドレスと読み込むファームウェア・ファイルを入力します。

-または-

「 FTP」または「 HTTP」を選択した場合、ユーザー名とユーザー・パスワード、およびサーバーのIPアドレスと読み込むファームウェア・ファイルを入力します。

5 *Upgrade*をクリックします。

RCSの構成およびRCSユーザー・データベースの保存と復元

スイッチの構成はファイルに保存できます。保存する構成ファイル内には、管理アプライアンスに関する情報が含まれます。また、スイッチのローカル・ユーザー・データベースを保存できます。いずれかのファイルを保存後、以前に保存した構成ファイル、またはローカル・ユーザー・データベース・ファイルをスイッチに復元することもできます。

管理アプライアンスの構成または管理アプライアンスのユーザー・データベースを保存するには次の手順を実行します。

1 サイド・ナビゲーション・バーで、*Unit View* → *RCS* → *Files*タブを順にクリックします。

2 *RCS Configuration*タブまたは*User Database*のいずれかをクリックし、次に*Save*タブをクリックします。

3 ファイルの保存方法を、Filesystem、TFTP、FTP、HTTP PUTから選択します。

4 「TFTP」を選択した場合、サーバーIPアドレスと読み込むファームウェア・ファイル名を入力します。

-または-

「FTP」または「HTTP」を選択した場合、サーバーIPアドレス、ユーザー名、ユーザー・パスワード、読み込むファームウェア・ファイル名を入力します。

5 ダウンロード前にデータを暗号化する場合は、暗号化パスワードを入力します。

6 *Download*をクリックします。「名前を付けて保存」ダイアログ・ボックスが開きます。

7 対象の場所に移動し、ファイルの名前を入力します。Saveをクリックします。

管理アプライアンスの構成または管理アプライアンスのユーザー・データベースを復元するには次の手順を実行します。

1 サイド・ナビゲーション・バーで、*Unit View* → *RCS* → *Files*タブを順にクリックします。

2 *RCS Configuration*タブまたは*User Database*のいずれかをクリックし、次に*Restore*タブをクリックします。

3 ファイルの保存方法を、Filesystem、TFTP、FTP、HTTPから選択します。

4 Filesystemを選択した場合、*Browse*を選択して、ファームウェア・アップグレード・ファイルの場所を指定します。

-または-

「TFTP」を選択した場合、サーバーIPアドレスと読み込むファームウェア・ファイル名を入力します。

-または-

「FTP」または「HTTP」を選択した場合、サーバーIPアドレス、ユーザー名、ユーザー・パスワード、読み込むファームウェア・ファイル名を入力します。

5 **Browse**をクリックします。対象の場所に移動し、ファイル名を選択します。**Upload**をクリックします。

6 元のファイルが暗号化されている場合は、復号化パスワードを入力します。

7 完了の画面が表示されたら、管理アプライアンスを再起動して、復元した設定を有効にします。「RCSの再起動」(ページ57)を参照してください。

FLASHアップデートのエラーを復旧するには次の手順を実行します。

FLASHの手順後、RCSが新しいファームウェアのバージョンで起動されない場合、次の手順を使用して、以前のファームウェアのバージョンに戻すことができます。

1 シリアル・ケーブルをRCSのリア・パネルにあるSETUPポートに接続します。

2 Setupポートに接続されているコンピューターでターミナル・プログラムを実行します。このシリアル・ポートの設定は、9600ボー、8データ・ビット、1ストップ・ビット、パリティなし、フロー・コントロールなし、です。

3 RCSの電源を入れます。

4 ターミナル・プログラムで、「Hit any key to stop autoboot」というメッセージが表示されたら、いずれかのキーを押します。メニューが表示されます。

5 1(Boot Alternate)を入力して、Enterキーを押します。RCSは自動的に以前のファームウェアのバージョンで再起動します。

6 RCSの再起動後、FLASHアップグレードを試行できます。

ネットワーク設定

注: ネットワーク・ダイアログ・ボックスの設定を変更できるのは、スイッチ管理者のみです。他のユーザーには、表示のみのアクセスが許可されています。

サイド・ナビゲーション・バーから、**Network**をクリックして、General、IPv4、IPv6のタブを表示します。

一般ネットワーク設定を構成するには次の手順を実行します。

1 *Network*タブをクリックし、次に**General**タブをクリックして、RCS General Network Settings画面を表示します。

2 「LAN Speed」ドロップダウン・メニューから、*Auto-Detect*、*10 Mbps Half Duplex*、*10 Mbps Full Duplex*、*100 Mbps Half Duplex*、*100 Mbps Full Duplex*、*1 Gbps Full Duplex* のオプションのいずれか1つを選択します。

注: イーサネット・モードを変更した場合は、再起動する必要があります。

3 「ICMP Ping Reply」ドロップダウン・メニューから、*Enabled*または*Disabled* のいずれかを選択します。

4 HTTPまたはHTTPSポートを確認もしくは変更します。設定はデフォルトのHTTP 80およびHTTPS 443となります。

5 *Save*をクリックします。

IPv4ネットワーク設定を構成するには次の手順を実行します。

1 **IPv4**タブをクリックして、IPv4 Settings画面を表示します。

2 **Enable IPv4**チェックボックスをクリックしてオンまたはオフにします。

3 「Address」、「Subnet」、「Gateway」の各フィールドに適切な情報を入力します。IPv4のアドレスは、xxx.xxx.xxx.xxxのドット記号式で入力します。

4 DHCPドロップダウン・メニューから、*Enabled*または*Disabled*のいずれかを選択します。

注: DHCPを有効にすると、「Address」、「Subnet」、「Gateway」の各フィールドに入力した情報は無視されます。

5 *Save*をクリックします。

IPv6ネットワーク設定を構成するには次の手順を実行します。

1 **IPv6**タブをクリックして、IPv6 Settings画面を表示します。

2 **Enable IPv6**チェックボックスをリックしてオンまたはオフにします。

3 「Address」、「Subnet」、「Prefix Length」の各フィールドに適切な情報を入力します。IPv6のアドレスは、FD00:172:12000033または省略FD00:172:12:33の16進数表記で入力します。

4 DHCPドロップダウン・メニューから、*Enabled*または*Disabled*のいずれかを選択します。

注: DHCPv6を有効にすると、「Address」、「Gateway」、「Prefix length」の各フィールドに入力した情報は無視されます。

5 *Save*をクリックします。

DNS設定

手動でDNSサーバーを割り当てることも、DHCPまたはDHCPv6を使用して取得したアドレスを使用することもできます。

DNS設定を手動で構成するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、*DNS*を選択して、RCS DNS Settings画面を表示します。

2 *Manual*、*DHCP*(IPv4が有効な場合)、*DHCPv6*(IPv6が有効な場合)のいずれかを選択します。

3 *Manual*を選択した場合は、Primary、Secondary、Tertiaryの各フィールドにDNSサーバー番号を入力します。

4 *Save*をクリックします。

NTP設定

スイッチは、証明書の期限が切れていないことを確認するために、現在の時刻にアクセスする必要があります。NTPからの時刻更新を要求するようにスイッチを構成できます。第5章の「NTPの構成」を参照してください。

SNMP設定

SNMPは、ネットワーク管理アプリケーションとスイッチ間で管理情報を通信するために使用されるプロトコルです。他のSNMPマネージャーは、MIB-IIにアクセスすることにより、スイッチと通信できます。SNMP画面を開くと、OBWIはユニットからSNMPパラメーターを取得します。

SNMP画面から、システム情報とコミュニティー・ストリングを入力できます。また、スイッチを管理するステーション、さらにスイッチからSNMPトラップを受信するステーションを指定できます。**Enable SNMP**を選択すると、ユニットはUDPポート161を介したSNMP要求に応答します。

一般SNMP設定を構成するには次の手順を実行します。

1 **SNMP**をクリックして、SNMP画面を開きます。

2 **Enable SNMP**チェックボックスをクリックして有効にし、スイッチがUDPポート161を介したSNMP要求に応答できるようにします。

3 「Name」フィールドにシステムの完全修飾ドメイン名を、「Contact」フィールドにノードの連絡先担当者を入力します。

4 「Read」、「Write」、「Trap」の各コミュニティー名を入力します。これらの名称は、SNMPアクションで使用が必須となっているコミュニティー・ストリングを指定します。「Read」と「Write」のストリングは、UDPポート161を介したSNMPにのみ適用され、スイッチへのアクセスを保護するパスワードとして機能します。この値は、64文字以内の範囲で受け入れられます。これらのフィールドを空欄のまま残すことはできません。

5 スイッチの管理を許可する最大4台の管理ワークステーションのアドレスを、「Allowable Managers」フィールドに入力します。または、これらのフィールドを空欄のままにして、すべてのワークステーションにRCSの管理を許可することもできます。

6 **Save**をクリックします。

監査イベントの設定

イベントはスイッチによって管理ステーションに送信される通知で、何らかの処置が必要である事象が発生したことを示します。

個別のイベントを有効にするには次の手順を行います。

1 **Auditing**をクリックして、Events画面を開きます。

2 一覧の適切なチェックボックスをオンにして、通知を生成するイベントを指定します。

-または-

Event Nameの横にあるチェックボックスをオン／オフにすると、リスト内のすべてをオンまたはオフにできます。

3 **Save**をクリックします。

イベント送信先の設定

監査イベントを、SNMPトラップ送信先とSyslogサーバーに送信されるように構成できます。イベント画面で有効にされたイベントは、

イベント送信先画面に一覧で表示されているすべてのサーバーに送信されます。

1 **Auditingと Destinations**タブをクリックして、Event Destinations画面を開きます。

2 「SNMP Trap Destination」フィールドに、このスイッチがイベントを送信する管理ワークステーションのアドレスとSyslogサーバーをそれぞれ4つまで入力します。

3 **Save**をクリックします。

ポート - SIPの構成

スイッチから、接続されているSIPの一覧や、各SIPの電子ID (EID)、ポート、状態、アプリケーション、インターフェイス・タイプ、およびUSB速度の情報を表示できます。SIPの1つをクリックすると、スイッチ・タイプ、ブート・バージョン、アプリケーション・バージョン、ハードウェア・バージョン、FPGAバージョン、最新バージョン、アップグレード・ステータスなどの追加情報が表示できます。

また、実行できるタスクには、オフラインSIPの削除、SIPファームウェアのアップグレード、USB速度の設定、ケーブルの停止があります。

オフラインSIPを削除するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、*Ports* → *SIPs*の順にクリックして、SIP画面を開きます。

2 *Delete Offline*をクリックします。

SIPのアップグレード

SIP FLASHのアップグレード機能を使用すると、RCS管理者はSIPを利用可能な最新のファームウェアにアップデートできます。このアップデートは、スイッチのユーザー・インターフェイスまたはAvocent管理ソフトウェアを使用して実行できます。

アップグレードによりFLASHメモリーが再プログラムされると、スイッチはソフト・リセットを実行し、すべてのSIPセッションを終了します。SIPのファームウェアがアップデート中のターゲット・デバイスは、接続解除されたと表示される場合があります。フラッシュ・アップデートが完了すると、ターゲット・デバイスは正常に表示されるようになります。

SIPの自動アップグレードを行うようにRCSが構成されている場合は、スイッチがアップデートされると、SIPも自動的にアップデートされます。スイッチのファームウェアをアップデートするには、「RCSツール」(ページ 56)、またはAvocent管理ソフトウェアのオンライン・ヘルプを参照してください。通常のアップグレード処理中に問題が発生した場合も、必要に応じて、SIPは強制的にアップグレードされることがあります。

注: ファームウェア・アップグレード・ファイルについては、http://www.dell.comを確認してください。

SIPの自動アップグレード機能を変更するには:

1 サイド・ナビゲーション・バーから、*Ports* → *SIPs*の順にクリックして、SIP画面を開きます。

2 アップグレードするSIPの横にあるチェックボックスを選択し、*Enable Auto* → *Upgrade*をクリックします。

注意: ファームウェア・アップデート中にSIPの接続を解除したり、ターゲット・デバイスのパワー・サイクリング(一旦電源を切って入れ直す)を行ったりすると、モジュールが作動不能となりSIPの工場返送や修理の必要が生じる場合があります。

SIPファームウェアをアップグレードするには:

1 サイド・ナビゲーション・バーから、*Ports* → *SIPs*の順にクリックして、SIP画面を開きます。

2 変更するSIPの横にあるチェックボックスを選択します。

3 *Choose an operation*を選択して、*Upgrade*を選択します。

4 設定が正しい場合は、*Upgrade*をクリックします。

USB速度を設定するには次の手順を実行します。

注: この選択は、USB2 SIPにのみ適用されます。

1 サイド・ナビゲーション・バーから、 *Ports* → *SIPs*の順にクリックして、SIP画面を開きます。

2 変更するSIPの横にあるチェックボックスを選択します。

3 *Choose an operation*を選択して、 *Set USB 1.1 Speed*または *Set USB 2.0 Speed*選択します。

電源装置の設定

注: 電源装置の設定を変更するには、管理者の権限が必要です。

注: サポート 対象のPDU一覧については、www.dellkvm.comを参照してください。

RCS Power Devices画面から、接続されている電源装置の一覧や、各電源装置の名前、ポート、状態、バージョン、モデル、ブザー、アラーム、および温度の情報を表示できます。また、電源装置を選択して、Settingsを選択すると、その電源装置の名前、説明、状態、バージョン、ソケット、ベンダー名、モデル、および入力フィードの詳細を表示できます。

電源管理装置のアウトレットにターゲット・デバイスが接続されている場合は、ターゲット・デバイスの電源のオン／オフ、またはオフ／オン(電源の入れ直し) を行うことができます。

ターゲット・デバイスの電源のオン、オフ、またはオフ／オンを行うには次の手順を実行します。

1 サイド・ナビゲーション・バーから、*Ports* → *Power Devices*の順にクリックして、Power Devices画面を開きます。

2 構成するユニットの名前をクリックして、*Outlet List*をオンにします。

3 構成するアウトレットの左側にあるチェックボックスを選択します(複数可) 。

4 *On*、*Off*、または*Cycle*を目的に応じてクリックします。

オフラインの電源装置を削除するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、*Ports* → *Power Devices*の順にクリックして、Power Devices画面を開きます。

2 *Delete Offline*をクリックします。

最小オン時間、オフ時間またはウェイク・アップ状態を変更するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、*Ports* → *Power Devices*の順にクリックして、Power Devices画面を開きます。

2 構成するユニットの名前をクリックして、*Outlets*を選択します。

3 変更するアウトレットの名前をクリックします。

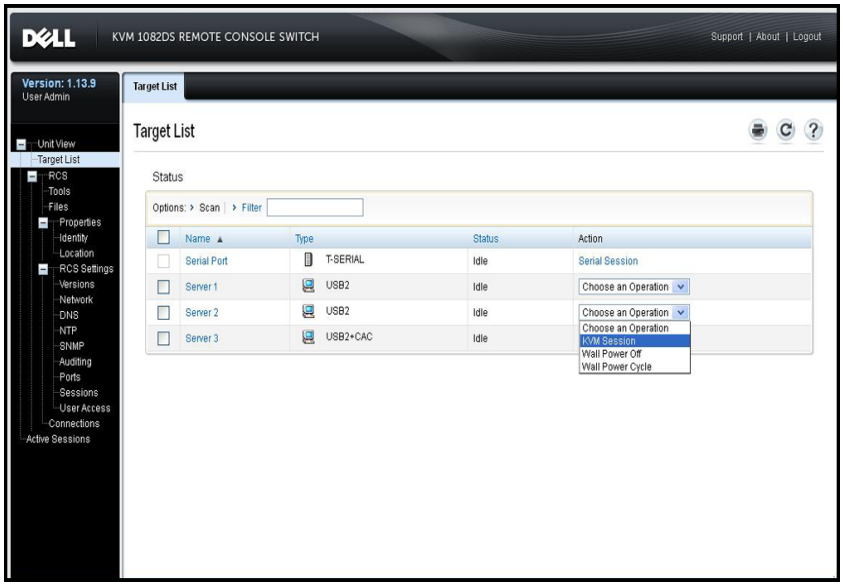
4 ドロップダウン・ウィンドウを使用して対象の設定を変更し、*Save*をクリックします。

ターゲット・サーバーと電源アウトレットの関連付け

OBWIの「Target List」ページでは、リンクされたアウトレットを持つターゲットの電源管理操作を選択できます。Ports → Power Devices タブを順に選択し、次にデバイス名をクリックすると、Device Settings、Device Firmware Upgrade、およびOutlet List の各タブが表示されます。Outlet Listタブをクリックすると、ターゲット・デバイスにリンクされているアウトレットが表示されます。

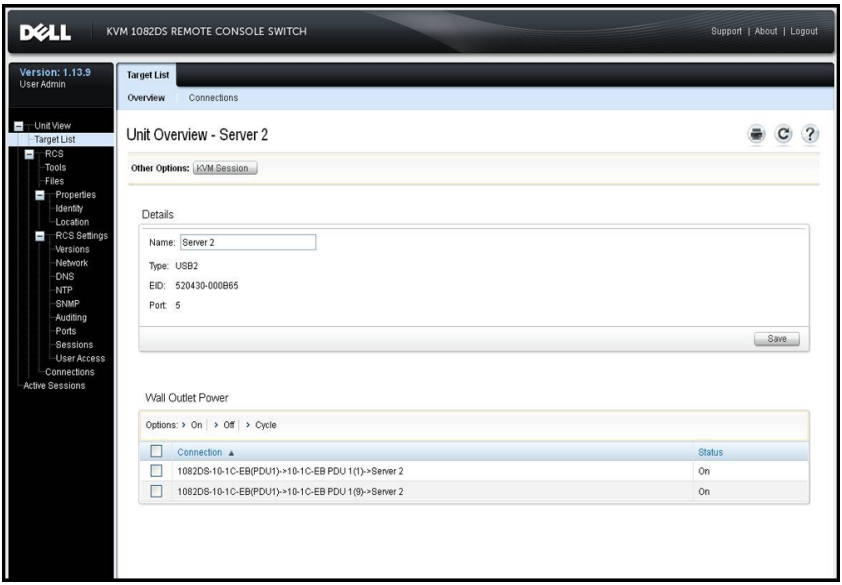
次の図に、リンクされた電源アウトレットを持つServer2という名前のターゲット・デバイスを示します。「Action」列のドロップダウン・メニューの矢印をクリックすると、利用可能なオプションの電源操作が表示されます。

図 3.2. Target List



次の図では、ターゲットのServer2のUnit Overviewページに、Wall Outlet Powerが表示されています。ここでは、PDU1からのアウトレット 1とアウトレット 9がServer2にリンクされています。

図 3.3. ターゲットの概要 - Server2



電源アウトレットのグループ化

アウトレットは、制御を容易にするために、ターゲット・サーバーにリンクまたは関連付けることができます。アウトレット（すなわちサーバーに対するアウトレット）をグループにするには、名前を付ける最初のデバイスで、Manual Nameフィールドを使用されなければなりません。二番目およびそれ以降のデバイスでは、Link to Target Deviceメニューを使用し、次にドロップ・ダウン・リストから最初のデバイスのターゲット名を選択しなければなりません。

「Target List」ページで実行された電源操作は、適用可能なすべてのアウトレットに適用されます。「ユニットの表示」ページでは、ターゲットの特定の電源アウトレットに対して電源管理操作を実行できます。次の図に、PDU1からの電源アウトレット4と5という組み合わせを持つ、Group2という名前のターゲットを示します。

ソケット4および5をグループにするには:

1 アウトレット 4を選択して、*Power Devices Outlet Settings*ページを表示します。

2 *Manual*を選択して、Group2を入力します。

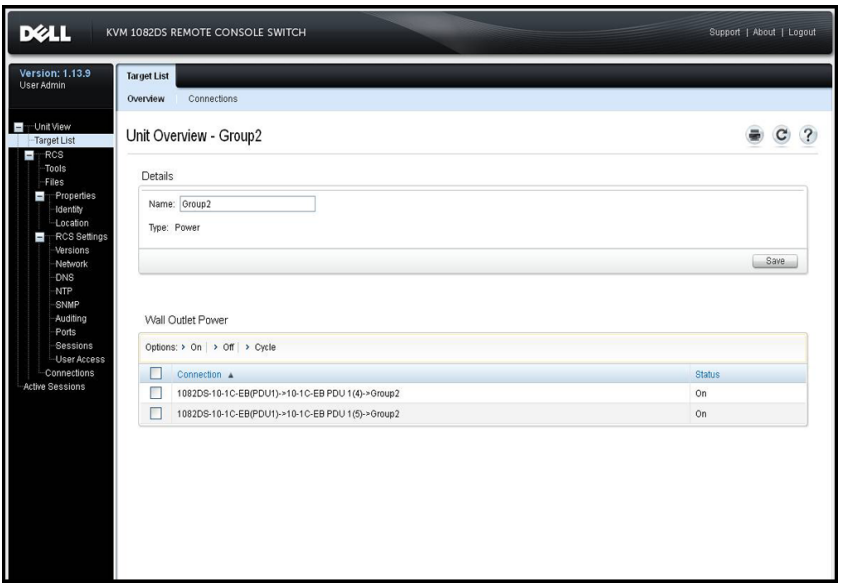
3 *Save*をクリックします。

4 アウトレット 5を選択して、*Power Devices Outlet Settings*ページを表示します。

5 *Link to Target Device*を選択して、ドロップ・ダウン・メニューから *Group2*を選択します。

6 *Save*をクリックします。Outlet Listに戻ると、アウトレット 4および5は同じ名前を持つことになります。

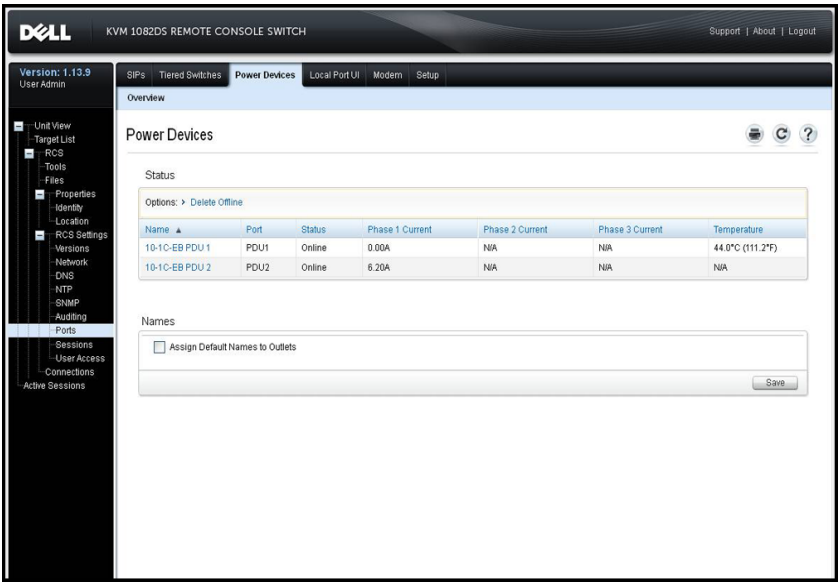
図 3.4. ターゲットの概要 - Group2



デフォルト のアウト レット 名

次の図に示すとおり、Power Devicesページの Assign Default Names to Outletsチェックボックスを使用して、電源アウトレットに電源デバイスのデフォルトの名前を指定するかどうか制御します。名前の付いた電源アウトレットのみが「ターゲット」ページに一覧表示されます。Assign Default Names to Outletsチェックボックスをオフにして保存すると、デフォルトで割り当てられた電源アウトレット名を削除できます。「Assign Default Names to Outlets」チェックボックスをオンにして保存すると、名前のない電源アウトレットにデフォルトの名前を割り当てられます。

図 3.5. RCS Power Devicesページ

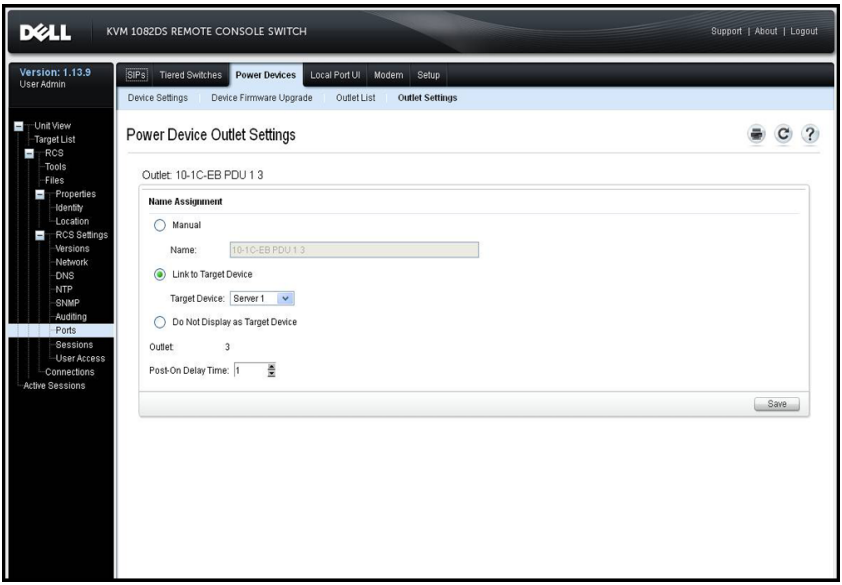


アウト レット 名の割り 当て

次の図に示すとおり、「電源装置アウトレットの設定」ページには、アウトレットの名前を割り当てるための3つのオプションがあ

ります。オプションは、「手動」割り当て、「ターゲット・デバイスへのリンク」、「ターゲット・デバイスとして表示しない」です。

図 3.6. 電源装置アウトレット設定ページ



- Manual Nameでは、出力に固有の名前を指定します。名前は、すべてのSIPおよび電源アウトレット名に対して固有である必要があります。固有でない名前を手動で指定しようとするとエラーになり、名前は保存されません。
- Link to Target Deviceでは、別のターゲット名(アウトレットまたはSIPのいずれか)にアウトレットをリンクして、指定されたターゲットの電源を管理します。アウトレットがSIPターゲット名にリンクされると、通常そのアウトレットはリンクされたSIPに接続されているサーバーに物理的に電源を供給します。
- 「Do Not Display as Target Device」オプションは、アウトレットの名前を空白にします。これにより、アウトレットは「Target

List」ページに表示されません。このオプションを予備のアウトレットに使用して、予備のアウトレットを「Target Lis」ページに表示されないようにできます。

アクセス制御の継承

ターゲットに電源アウトレットをリンクすることにより電源アウトレット名を変更すると、アウトレットはそのターゲット名に既に構成されているアクセス制御を継承します。SIPが追加され、そのSIPから取得された名前が既存のターゲットの名前と一致すると、新しいSIPはそのターゲットからアクセス制御を継承します。ターゲット・デバイスの名前が変更されると、そのターゲットのすべてのSIPおよびアウトレットの名前は変更され、古いターゲット名に構成されていたアクセス制御を継承し続けます。

ターゲット・デバイスの名前の変更

「Target List - Overview」ページでは、ターゲットの名前を任意の固有ターゲット名に変更できます。名前は、SIPおよび電源アウトレットを含むすべてのターゲットに対して固有である必要があります。ターゲットの名前が変更されると、そのターゲットにリンクしているすべてのアウトレットにも、新しいターゲット名が指定されます。

ターゲット・デバイスの優先付けされる状態

「Target Lis」ページでは、リンクされた電源アウトレットを持つターゲットにより複数のデバイスが制御されます。ターゲットに表示されている「状態」値は、デバイスのすべての状態値のうちでもっとも優先度の高いものとして選択されます。次の表に、状態値の種類を優先度順(優先度の高い順から低い順)と適用可能なターゲット・デバイス・タイプを示しています。

表 3.4: ターゲットの状態値

状態値	適用対象		状態の説明
	SIP	電源アウトレット	
使用中	x	なし	セッションがアクティブです
パスがブロック状態	x	なし	ターゲットへのパスは別のセッションが使用中です
アップグレード中	x	なし	SIPはアップグレード中です
電源オン中	なし	x	1つ以上のアウトレットが電源投入中です
電源オフ中	なし	x	1つ以上のアウトレットが電源遮断中です
電源なし	x	なし	SIPで電源が検出されません
電源の一部	なし	x	ターゲットにはオン／オフ状態のアウトレットが両方あります
ロック解除状態	なし	x	1つ以上のアウトレットがロックされています
電源オフ状態	なし	x	1つ以上のアウトレット の電源がオフです
ロック状態	なし	x	1つ以上のアウトレットがロック解除されています

状態値	適用対象		状態の説明
	SIP	電源アウトレット	
アイドル	x	なし	アクティブなセッションはありません。SIPには電源が投入されています
電源オン状態	なし	x	アウトレットの電源はオンです

ターゲット・デバイスに名前でリンクされている複数の電源アウトレットがあり、それらが共通の電源状態にない場合、RCSはLocked-Offのアウトレット状態をOffと見なし、Locked-Onのアウトレット状態をOnと見なす場合があります。次の表に、2つのアウトレットの状態値が組み合わされたときに生じる状態値の一覧を示します。

表 3.5: 複数のアウトレットの状態値と表示される状態

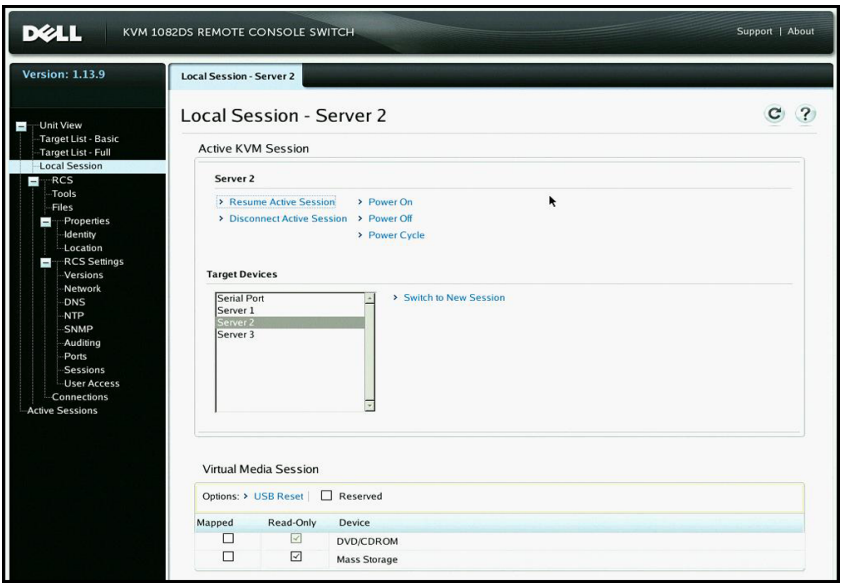
アウトレット1の状態	アウトレット2の状態	結果となる状態
オフ	オフ	オフ
オフ	オン	電源の一部
オン	オン	電源がオンになりました
ロック状態	オン	電源がオンになりました
ロック状態	ロック状態	ロック状態
ロック状態	オフ	電源の一部
ロック解除状態	オン	電源の一部
ロック解除状態	ロック解除状態	ロック解除状態
ロック解除状態	オフ	電源がオフになりました

アウトレット 1の状態	アウトレット 2の状態	結果となる状態
ロック状態	ロック解除状態	電源の一部

ローカル・ポート のLocal Sessionページ

ローカル・ポート の「ローカル・セッション」ページでは、アクティブ・セッションのターゲットにリンクされている電源アウトレットがある場合、3つの電源コントロールがアクティブ・セッションの下に表示されます。次の図に、Server2という名前のターゲット のアクティブ・ローカル・ポート ・セッションで表示される電源コントロールを示します。

図 3.7. ローカル・セッション・ページの電源管理



ローカル・ポート UIの設定

ローカルUIの起動方法を変更するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、*Ports* → *Local Port UI*の順に選択して、Local Port UI Settings画面を開きます。

2 「Invoke Local Port UI」ヘッダーの下で、一覧で表示されている1つまたは複数の方法の横にあるチェックボックスをオンにします。

3 *Save*をクリックします。

ローカル・ポートのユーザー・インターフェイス認証をオン／オフしたり、ユーザー・アクセス・レベルを選択したりできます。ローカル・ポートのユーザー・インターフェイス認証をオンにする場合は、インターフェイスを使用するためにログインする必要があります。

また、ローカル・ポートのキーボード言語やスキャン・モード時間を選択したり、ローカル・ポートのパスワードを有効／無効にしたり、ユーザーのプリエンプト操作レベルを選択したりできます。ユーザーが、ターゲット・デバイスとの間で別のユーザーが実行中のシリアル・セッションまたはKVMセッションを中断／切断できるかどうかは、ユーザーのプリエンプト操作レベルによって決まります。プリエンプト操作レベルは1～4まであり、4が最高レベルです。たとえば、プリエンプト操作レベルが4のユーザーは、他のレベル1、2、3のユーザー、およびレベル4のユーザーを切断できます。

ローカル・ポート・ユーザー認証を変更するには次の手順を実行します(管理者のみ)。

1 サイド・ナビゲーション・バーから、**Ports → Local Port UI**の順に選択して、Local Port UI Settings画面を開きます。

2 **Disable Local Port User Authentication**チェックボックスをオンまたはオフにします。

3 **Disable Local Port User Authentication**をチェックする場合は、User Access Levelドロップダウン・メニューのオプションから1つ選択します: **User**、**User Administrator**、または**RCS Administrator**。

4 **Save**をクリックします。

モデムの設定

RCS Modem Settings画面から、一部のモデム設定を構成できます。また、モデムのローカル・アドレス、リモート・アドレス、サブネット・マスク、ゲートウェイの設定を表示できます。

スイッチのモデムへの接続に関する詳細は、「RCSハードウェアの接続」(ページ 27) を参照してください。

モデム設定を構成するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、**Ports** → **Modem**の順に選択して、Modem Settings画面を開きます。

2 **Modem sessions can preempt digital sessions**チェックボックスをオンまたはオフにします。

3 「Authentication Timeout」で認証がタイムアウトする時間(30秒～300秒)を選び、「Inactivity Timeout」で非アクティブ・タイムアウト時間(1分～60分)を選びます。

4 **Save**を選択します。

設定のセットアップ - ポート・セキュリティ

シリアル・セットアップ・ポートから、アプライアンスのネットワーク構成を変更したり、デバッグ情報を有効にしたり、アプライアンスをリセットすることができます。

パスワードを有効にして、シリアル・セットアップ・ポートへのアクセスを制限するには:

1 サイド・ナビゲーション・バーで、*RCS Settings* → *Ports* → *Setup*を順に選択して、Setup Port Settingsページを表示します。

2 *Enable Setup Port Security*ボックスをクリックして有効にします。

3 パスワードを入力して確認します。

4 *Save*をクリックします。

セッション

「Active Sessions」画面から、アクティブなセッションの一覧と各セッションについての以下の情報を表示することができます: ターゲット・デバイス、所有者、リモート・ホスト、継続時間、タイプに関する情報を表示できます。

一般セッションの設定

一般セッションを構成するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、*Sessions* → *General*の順に選択します。General Session Settings画面が表示されます。

2 *Enable Inactivity Timeout*チェックボックスをオンまたはオフにします。

3 「Inactivity Timeout」フィールドには、セッションを閉じる非アクティブ時間を入力します(1分～90分)。

4 「Login Timeout」フィールドには、再ログインを必要とする非アクティブ時間を入力します。(21秒～120秒)

5 Enable Preemption Timeoutチェックボックスをオンまたはオフにします。

6 「Preemption Timeout」フィールドには、セッションがプリエンプトされることを知らせるメッセージを表示する時間を入力します(1秒～120秒)。

7 適用できるセッションの共有オプション (Enabled、Automatic、Exclusive、またはStealth) を選択します。

8 1～50からInput Control Timeoutの値を選択します。ただし、1は0.1秒を表します。

9 Saveをクリックします。

KVMセッションの構成

KVMセッションを構成するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、Sessions → KVMの順に選択します。KVM Session Settings画面が表示されます。

2 キーボード信号およびマウス信号の暗号化レベル(128ビットSSL (ARCFOUR)、DES、3DES、またはAES) およびビデオ信号の暗号化レベル(128ビットSSL(ARCFOUR)、DES、3DES、AES、またはNone (なし) を選択します。

3 キーボード・ドロップダウン・メニューから言語を選択します。

4 ハードウェアにUSB2+CAC SIPが含まれている場合は、ビデオ解像度を選びます。

5 Saveをクリックします。

ローカル・バーチャル・メディア・セッションの構成

バーチャル・メディア・オプションを設定するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、**Sessions → Virtual Media**の順に選択して、Virtual Media Session Settings画面を開きます。

2 *Virtual Media locked to KVM Sessions*チェックボックスをオンまたはオフにします。

3 **Allow Reserved Sessions**チェックボックスをオンまたはオフにします。

4 ドロップダウン・メニューの「バーチャル・メディア・アクセス・モード」から、*Read-Only*または*Read-Write*のオプションのいずれかを選択します。

5 サポートする暗号化レベルを選択します。

6 *Save*をクリックします。

7 バーチャル・メディアを有効にする各SIPの横にあるチェックボックスをオンにし、*Enable VM*をクリックします。

-または-

バーチャル・メディアを無効にする各SIPの横にあるチェックボックスをオンにし、*Disable VM*をクリックします。

バーチャル・メディア・オプション

Virtual Media Session Settings画面に表示されるオプションを使用して、バーチャル・メディア・セッション中のスイッチの動作を指定できます。表3.4は、バーチャル・メディア・セッションに対して設定できるオプションの概要です。

KVMセッションでのバーチャル・メディア・セッションの使用に関する詳細は、「バーチャル・メディア」(ページ 108)を参照してください。

表 3.6: バーチャル・メディア・セッションの設定

設定	説明
セッションの設定: バーチャル・メディアがKVMセッションにロック状態	ロック・オプションは、バーチャル・メディア・セッションをターゲット・デバイス上のKVMセッションにロックされたままの状態にするかどうかを指定します。ロックが有効(デフォルト) である場合にKVMセッションが終了すると、バーチャル・メディア・セッションも終了します。ロックが無効である場合にKVMセッションが終了すると、バーチャル・メディア・セッションはアクティブのままになります。
セッションの設定: 予約済みセッションを許可する	特定のユーザー名にのみバーチャル・メディア接続へのアクセスを許可し、それ以外のユーザーがターゲット・デバイスにKVM接続を確立できないようにします。KVMセッションの接続が解除されたとき、「 バーチャル・メディア」ダイアログ・ボックスの「 ロック状態」の設定により、バーチャル・メディア・セッションの接続が解除されることがあります。

設定	説明
ドライブのマッピング: バーチャル・メディア・アクセス・モード	マッピングされたドライブのアクセス・モードは、読み取り専用か読み取り／書き込みに設定できます。アクセス・モードが読み取り専用の場合、クライアント・サーバー上でマッピングされたドライブにデータを書き込むことはできません。アクセス・モードが読み取り／書き込みの場合は、マッピングされたドライブとの間でデータの読み取りと書き込みを行うことができます。マッピングされるドライブが設計上読み取り専用(CD-ROMドライブ、DVD-ROMドライブ、ISOイメージなど) の場合は、設定された読み取り／書き込みアクセス・モードは無視されます。読み取り専用モードに設定すると、大容量記憶装置や外付けUSBメディアのような読み取り／書き込み対応ドライブをマッピングした後に誤って上書きされることを回避できます。 DVDドライブ(1台) と大容量記憶装置(1台) は同時にマッピングできます。CDドライブ、DVDドライブ、ISOディスク・イメージ・ファイルは、バーチャルのCD／DVDドライブとしてマッピングされます。
暗号化レベル	バーチャル・メディア・セッションの暗号化レベルを設定できます。選択肢には、なし(デフォルト) 、128-bit SSL(ARCFOUR) 、DES、3DES、AESです。
バーチャル・メディア・アクセス(SIP使用) VMの有効／無効	Virtual Media Access(SIP使用) セクションには、すべてのバーチャル・メディアSIPが一覧で表示されます。一覧には、各ケーブルのバーチャル・メディアを有効化／無効化するオプションを含む、各ケーブルの詳細が含まれます。

ローカル ユーザー

ローカル・ユーザーも、ローカル・セッション画面からバーチャル・メディアの動作を指定できます。バーチャル・メディア・セッションの接続／接続解除に加えて、次の表に示す設定を構成できます。

表 3.7: ローカル・バーチャル・メディア・セッションの設定

設定	説明
CD ROM/ DVD ROM	最初に検出されたCD-ROMドライブまたはDVD-ROM(読み取り専用) ドライブに、バーチャル・メディア・セッションを確立できます。このチェックボックスをオンにすると、バーチャル・メディアのCD-ROMまたはDVD-ROMからターゲット・デバイスへの接続が確立します。無効にすると、バーチャル・メディアのCD-ROMまたはDVD-ROMからターゲット・サーバーへの接続が終了します。
大容量記憶装置	バーチャル・メディア・セッションを最初に検出された大容量記憶装置に確立することができます。このチェックボックスをオンにすると、バーチャル・メディアの大容量記憶装置からターゲット・デバイスへの接続が確立します。無効にすると、バーチャル・メディアの大容量記憶装置からターゲット・デバイスへの接続が終了します。
予備	特定のユーザー名にのみバーチャル・メディア接続へのアクセスを許可し、それ以外のユーザーがターゲット・デバイスにKVM接続を確立できないようにします。

シリアル・セッションの構成

シリアル・セッションを構成するには次の手順を実行します。

1 サイド・ナビゲーション・バーから、*Sessions* → *Serial*の順にクリックして、Serial Session Settings画面を表示します。

2 *Telnet Access Enabled*チェックボックスをオンまたはオフにします。

3 **Save**をクリックします。

ユーザー・アカウント のセットアップ

ローカル・アカウント の管理

スイッチのOBWIでは、管理者が定義したユーザー・アカウントを通して、ローカル・アクティビティおよびログインがセキュアに実行されます。管理者は、サイド・ナビゲーション・バーの *User Accounts*をオンにすることで、ユーザーの追加と削除、ユーザーのプリエンプト操作の定義、アクセス・レベルの変更、パスワード の変更などを実行できます。

アクセス・レベル

ユーザー・アカウント が追加されるとき、ユーザーに対して割り当てられるアクセス・レベルには、RCS Administrator、User Administrator、Userがあります。

表 3.8: アクセス・レベルによって許可される操作

操作	RCS Administrator	User Administrator	Users
インターフェイスのシステム・レベル設定の構成	可	不可	不可
アクセス権の構成	可	可	不可
ユーザー・アカウントの追加、変更、削除	すべてのアクセス・レベルで可	可(UserおよびUser Administratorのみ)	不可
自分自身のパスワードの変更	可	可	可
ターゲット・デバイスへのアクセス	可(すべてのターゲット・デバイス対象)	可(すべてのターゲット・デバイス対象)	許可されていれば可

新規のユーザー·アカウントを追加するには(User Administratorまたは RCS Administratorのみ) 次の手順を実行します。

1 サイド·ナビゲーション·バーで、*User Accounts* → *Local User Accounts*の順にオンにして、Local User Accounts画面を開きます。

2 *Add*ボタンをクリックします。

3 新規ユーザーのユーザー名とパスワードを該当欄に入力します。

4 新規ユーザーのアクセス·レベルを選択します。

5 ユーザー·アカウントに割り当てる、任意の使用可能なターゲット·デバイスをオンにして、Addをクリックします。

注: User Administratorと RCS Administratorは、すべてのターゲット·デバイスにアクセスできます。

6 *Save*をクリックします。

ユーザー·アカウントを削除するには(User Administratorまたは RCS Administratorのみ) 次の手順を実行します。

1 サイド·ナビゲーション·バーで、*User Accounts* → *Local Accounts*の順にオンにして、Local User Accounts画面を開きます。

2 削除するアカウントの左にあるチェックボックスをそれぞれクリックして、*Delete*をクリックします。

ユーザー·アカウントを編集するには(管理者またはアクティブ·ユーザーのみ) 次の手順を実行します。

1 サイド·ナビゲーション·バーで *User Accounts* → *Local Accounts*の順にオンにします。Local User Accounts画面が表示されます。

2 編集するユーザーの名前をクリックします。ユーザー·プロファイルが表示されます。

3 画面にユーザー情報を入力し、*Save*をクリックします。

Avocent管理ソフトウェアのデバイスIPアドレス

Avocent管理ソフトウェア・サーバーのIPアドレスを指定すると、管理ソフトウェア・サーバーを使って、管理されていないスイッチに接続して登録できます。

サーバーIPアドレスを構成するには

1 サイド・ナビゲーション・バーで User Accounts →Avocentの順に選択します。Avocent Management Software Settings画面が表示されます。

2 接続するサーバーIPアドレスを入力します。IPアドレスは最大で4つ入力できます。

3 スクロール・バーを使用して、再試行間隔を選択します。

4 サーバーに登録されているRCSの関連を解除するには、**Disassociate**ボタンをクリックします。

5 *Save*をクリックします。

LDAP

Dell 1082DS/2162DS/4322D RCSは、ローカル・データベースを介して、またはLDAP(Lightweight Directory Assistance Protocol) サポートのDell RCSソフトウェアやOBWIを使用している外部のスケーラブルな分散型ディレクトリ・サービスによって、ユーザーを認証および承認できます。RCSでのLDAPの構成および使用に関する詳細情報については、LDAPのセクションを参照してください。

Override Admin

ネットワーク障害の発生に備え、LDAPサーバーに照会し、認証するユニットの性能に関係なく使用できるアカウントが用意されています。第5章の「 Override Adminアカウントの構成」を参照してください。

アクティブ・セッション

「Active Sessions」画面から、アクティブなセッションの一覧と各セッションについての以下の情報を表示することができます: ターゲット・デバイス、所有者、リモート・ホスト、継続時間、タイプに関する情報を表示できます。

セッションの終了

セッションを終了するには次の手順を実行します。

1 サイド・ナビゲーション・バーで、*Active Sessions* を選択して、RCS Active Sessions画面を表示します。

2 目的のターゲット・デバイスの横にあるチェックボックスをオンにします(複数可)。

3 *Disconnect*をクリックします。

注: 関連付けられているロック状態のバーチャル・メディア・セッションがある場合は、そのセッションも接続解除されます。

セッションを終了するには(ローカル・ユーザーのみ):

1 **サイド・ナビゲーション・バーから、Local Sessionを選択します。**

2 **Disconnect Active Session**チェックボックスをオンにします。

4

ビデオ・ビューア・ウィンドウ

OBWIを使用してスイッチに取り付けられているターゲット・デバイスとのKVMセッションを操作するには、ビデオ・ビューアを使用します。ビデオ・ビューアを使用してデバイスに接続すると、ターゲット・デバイスのデスクトップが別個のウィンドウに表示されます。このウィンドウには、ローカル・カーソルとターゲット・デバイスのカーソルの両方が含まれています。

スイッチのOBWIソフトウェアでは、Javaベースのプログラムを使用して、「ビデオ・ビューア」ウィンドウを表示します。スイッチのOBWIは、初めて起動したときにビデオ・ビューアを自動的にダウンロードして、インストールします。

注: セッションを起動するには、Java 1.6.0_11以降が必要です。

注: スイッチのOBWIは、Java Resource Engine(JRE) をインストールしません。JREは無料でhttp://www.sun.comからダウンロードできます。

注: スイッチのOBWIは、システム・メモリーを使用して、「ビデオ・ビューア」ウィンドウ内にイメージを保存して表示します。開かれた「ビデオ・ビューア」ウィンドウには、追加のシステム・メモリーがそれぞれ必要です。クライアント・サーバーで色を8ビットに設定すると、「ビデオ・ビューア」ウィンドウあたり1.4 MBのメモリーが必要です。16ビットに設定すると2.4 MB、32ビットに設定すると6.8 MBのメモリーが必要です。システム・メモリーが許容する(通常4つ) 以上の「ビデオ・ビューア」ウィンドウを開こうとすると、メモリー不足エラーが発生し、要求した「ビデオ・ビューア」ウィンドウは開きません。

アクセスしようとしているデバイスを別のユーザーが表示中である場合、このユーザーのプリエンプト操作レベルと同等またはそれ以上のプリエンプト操作レベルが自分に許可されていれば、相手のユーザーをプリエンプトするよう指示するメッセージが表示されま

す。また、RCS管理者も、Active Sessionのページから、アクティブなユーザーの接続を解除できます。詳細については、「アクティブ・セッション」(ページ 89) を参照してください。

図 4.1. ビデオ・ビューア・ウィンドウ(通常のウィンドウ・モード)

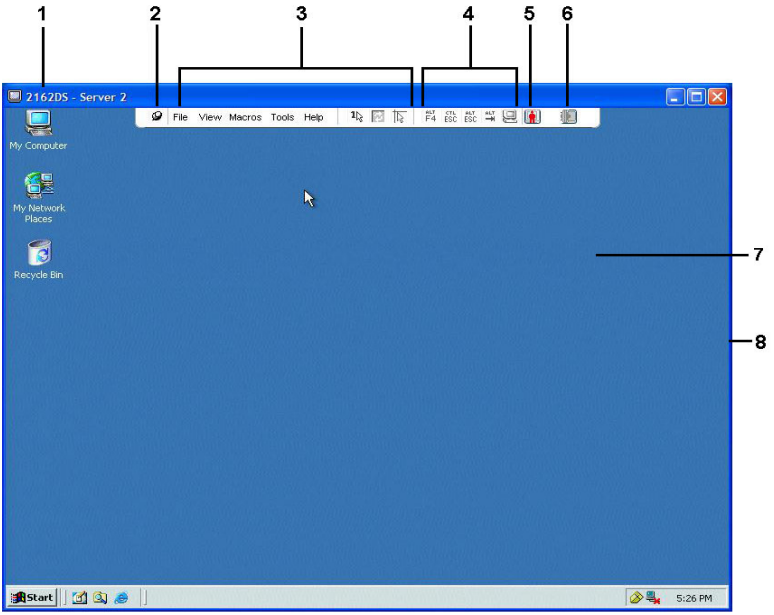


表 4.1: ビデオ・ビューアの説明

番号	説明
1	タイトル・バー: 表示されているターゲット・デバイスの名前を表示します。全画面表示モードではタイトル・バーが隠され、ターゲット・デバイス名がメニューとツールバーの間に表示されます。

番号	説明
2	画鋲アイコン: メニューとツールバーをロックして、常に表示されるようにします。
3	メニューおよびツールバー:「ビデオ・ビューア」ウィンドウ機能の多くには、ここからアクセスできます。画鋲を使用していない場合、メニューとツールバーは表示／非表示状態になります。ツールバー上にカーソルを移動すると、メニューとツールバーが表示されます。ツールバーには10個までのコマンドやマクロ・グループ・ボタンを表示できます。デフォルトでは、ツールバーには、シツールバー上には「シングル・カーソル」モード、更新、自動ビデオ調整、ローカルカーソルを合わせるの各ボタンが表示されます。詳細については、「ツールバーの変更」(ページ 94) および「ツールバーの変更」(ページ 94) を参照してください。
4	マクロ・ボタン: ターゲット・デバイスへの送信に通常使われるキーボード・シーケンスです。
5	接続ステータス・インジケーター: このサーバーのRCSに接続されているユーザーの状態を示します。モードは、排他、基本的なアクティブ接続、プライマリ・アクティブ共有、セカンダリ・アクティブ共有、パッシブ共有、ステルス、スキャンです。
6.	スマート・カードのステータス・インジケーター: スマート・カードがスマート・カード・リーダーに挿入されているかどうかを示します。ビデオ・ビューア画面のスマート・カード・アイコンが半透明の場合は、スマート・カード・オプションが使用できないか、または無効であることを示します。スマート・カードがマッピングされている場合は、アイコンは緑です。
7	表示領域: サーバーのデスクトップにアクセスします。
8	フレーム:「ビデオ・ビューア」ウィンドウのサイズを変更するには、フレームをクリックしてホールドします。

ツールバーの変更

表示／非表示状態(つまり、画鋲によって所定の位置にロックされていない) にあるツールバーが「ビデオ･ビューア」ウィンドウで非表示になるまでの秒数を指定することができます。

ツールバーの非表示時間を指定するには次の手順を実行します。

1 「ビデオ･ビューア」ウィンドウのメニューから、Tools → Session Optionsの順に選択します。

-または-

Session Optionsボタンをクリックします。

「Session Options」ダイアログ･ボックスが表示されます。

2 **Toolbar**タブをクリックします。

3 矢印キーを使用して、ツールバーが非表示になるまでの待ち時間(秒数) を指定します。

4 OKをクリックして変更を保存し、ダイアログ･ボックスを閉じます。

セッションの起動

注: 非プロキシ接続を使用している場合、低速のネットワーク接続では最適のビデオ･パフォーマンスが得られないことがあります。一部の色設定(グレースケールなど) では他の設定(色－最適化など) ほどネットワーク帯域を使用しないため、色設定を変更するとビデオ･パフォーマンスを改善できることがあります。低速のネットワーク接続で最適のビデオ･パフォーマンスを得るには、「グレースケール／圧縮－最適化」または「色－低／圧縮－高」などの色設定を使用してください。詳細については、「ビューの調整」(ページ 96) を参照してください。

注: ユーザーがローカル･コンピューターより高い画面解像度でターゲット･デバイスに接続した場合には、ターゲット･デバイス画面の一部が「ビデオ･ビューア」ウィンドウに表示され、画面残りの部分はスクロール･バーで参照するようになります。この場合は、ターゲット･デバイスまたはローカル･コンピューター(またはこの両方) の解像度を調整すれば、画面全体が表示できるようになります。

スイッチのExplorerウィンドウからKVMセッションを起動するには次の手順を実行します。

1 「Target List」画面で一覧表示されたデバイスをクリックし、「Unit Overview」ウィンドウを開きます。

2 *KVM Session*リンクをクリックし、新しいウィンドウでビデオ・ビューアを開きます。

セッション・タイムアウト

一定の時間枠内に「Session」ウィンドウでアクティビティがなかった場合、リモート・セッションはタイムアウトとなることがあります。セッションのタイムアウト値は、RCS KVM Session Settingsウィンドウで構成できます。指定したタイムアウト値は、次にスイッチのOBWIにアクセスしたときに使用されます。

セッションのタイムアウトを有効／無効にする、またはタイムアウト値を構成するには次の手順を実行します。

1 サイド・メニューで、*Unit View* → *RCS* → *RCS Settings* → *Sessions* → *General*の順に選択します。

2 *Enable Activity Timeout*ボックスの目的の設定を選びます。

3 必要に応じて、アクティビティなしによるタイムアウトの時間枠を指定します。

4 *Save*をクリックします。

ウィンドウ・サイズ

注: View → Scalingコマンドは、「ビデオ・ビューア」ウィンドウが全画面表示(Full Screen)モードになっている場合は使用できません。また、共有セッションの非プライマリ・ユーザーは使用できません。

スイッチのOBWIを初めて使用した場合、開いている「ビデオ・ビューア」ウィンドウはすべて、ユーザーが値を変更するま

で、1024 x 768の解像度で表示されます。「ビデオ・ビューア」ウィンドウは、それぞれ異なる解像度に設定できます。

自動スケールが有効になっている場合は、セッション中にウィンドウ・サイズが変わっても、スイッチのOBWIは表示を自動調整します。ターゲット・デバイスの解像度がセッション中に変更された場合でも、表示は自動調整されます。

「ビデオ・ビューア」ウィンドウの解像度を変更するには次の手順を実行します。

1 *View* → *Scaling*コマンドを選択します。

2 希望の解像度を選択します。

ビューの調整

「ビデオ・ビューア」ウィンドウ内のメニューやタスク・ボタンでは、次の機能を実行できます:

- マウス・カーソルの位置を合わせる。
- 画面を更新する。
- 全画面表示モードを有効／無効にする。全画面表示モードが有効の場合は、イメージはデスクトップに合わせて最大1600 x 1200または1680 x 1050(ワイドスクリーン)のサイズまで調整されます。デスクトップの解像度がより高い場合は、次の現象が発生します。
  - 全画面画像はデスクトップの中央に表示され、この外枠となる「ビデオ・ビューア」ウィンドウ領域が黒く表示されます。
  - メニューとツールバーはロックされ、常に表示された状態になります。
- セッション画像の自動／フル／手動スケールのサイズ調整を有効にする。

- フル・スケールでは、デスクトップ・ウィンドウは固定され、デバイスの画像はウィンドウに合わせてサイズ調整されます。
- 自動スケールでは、表示中のターゲット・デバイスの解像度に合わせてデスクトップ・ウィンドウのサイズが調整されます。
- 手動スケールでは、サポートされている画像スケーリング解像度がドロップダウン・メニューに表示されます。

- セッション画像の色の階調を変更する。

マウスのカーソルの位置を合わせるには:

「ビデオ・ビューア」ウィンドウのツールバーで、*Align Local Cursor*ボタンをクリックします。ローカル・カーソルの位置がリモート・デバイス上のカーソルと揃います。

注: カーソルが調整した位置からずれた場合は、接続されているデバイスでのマウス加速度をオフにしてください。

画面を更新するには、ビデオ・ビューア・ウィンドウで、*Refresh Image*ボタンをクリックするか、またはビデオ・ビューア・ウィンドウ・メニューから *View* → *Refresh*の順に選択します。デジタル化されたビデオ画像が完全に再生成されます。

全画面表示モードを有効にするには、*Maximize*ボタンをクリックするか、ビデオ・ビューア・ウィンドウ・メニューから *View* → *Full Screen*の順に選択します。デスクトップ・ウィンドウは非表示の状態になり、アクセス中のデバイスのデスクトップのみが表示されます。画面は最大1600 x 1200または1680 x 1050(ワイドスクリーン) にサイズ変更されます。モニターのデスクトップ解像度がこれより高い場合は、フル・スクリーン画像が黒の背景で縁取られます。浮動ツールバーが表示されます。

全画面表示モードを無効にするには、浮動ツールバー上の*Full Screen Mode*ボタンをクリックして、デスクトップ・ウィンドウに戻ります。

フル・スケーリングを有効にするには、ビデオ・ビューア・ウィンドウ・メニューから *View* → *Scaling*の順に選択して、Full Scaleを選択します。表示中のターゲット・デバイスの解像度に合わせて、デバイスの画像が自動的に調整されます。

手動スケーリングを有効にするには、ビデオ・ビューア・ウィンドウ・メニューから *View* → *Scaling*の順に選択します。ウィンドウに適用するサイズを選択します。利用可能な手動スケールのサイズはシステムによって異なります。

イメージの更新

手動ビデオ調整ダイアログ・ボックスの*Refresh Image*ボタンをクリックすると、デジタル化されたビデオ画像が完全に再生成されます。

注: またイメージは、「ビデオ・ビューア」ウィンドウのメニューから *View* → *Refresh*の順に選択して更新することもできます。

ビデオの設定

その他のビデオ調整

通常、「ビデオ・ビューア」ウィンドウの自動調整機能を選択した場合には、調整可能な範囲で最高のビデオ画像に最適化されます。ただし、Dellテクニカル・サポートとの連携で「ビデオ・ビューア」ウィンドウのメニューの*Tools* → *Manual Video Adjust*コマンドを使用するか、*Manual Video Adjust*ボタンをクリックすると、ユーザーは画質を微調整できます。これにより、手動ビデオ調整ダイアログ・ボックスが表示されます。ビデオ調整はターゲット単位の設定です。

ユーザーは、ダイアログ・ボックスの左下にあるパケット・レートを見ながら、静的画面をサポートするために必要なパケット数／秒のレベルを確認できます。

ウィンドウのビデオ画質を手動で調整するには次の手順を実行します。

注: 次のビデオ調整を行うには、必ずDellテクニカル・サポートとの連携が必要です。

1 「ビデオ・ビューア」ウィンドウのメニューから、*Tools* → *Manual Video Adjust*の順に選択します。

-または-

*Manual Video Adjust*ボタンをクリックします。

手動ビデオ調整ダイアログ・ボックスが表示されます。

図 4.2. Manual Video Adjustダイアログ・ボックス

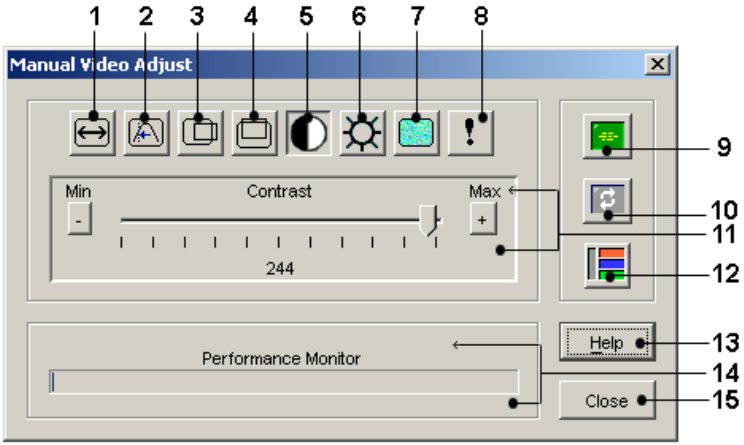


表 4.2: 図 4.2の説明

番号	説明	番号	説明
1	画像キャプチャーの幅	9	自動ビデオ調整
2	ピクセル・サンプリング／微調整	10	画像の更新

番号	説明	番号	説明
3	画像キャプチャーの水平位置	11	調整バー
4	画像キャプチャーの垂直位置	12	ビデオ・テスト・パターン
5	コントラスト	13	Help
6	明るさ	14	Performance Monitor
7	ノイズのしきい値	15	Closeボタン
8	しきい値優先順位		

2 調整したい機能に対応するアイコンをクリックします。

3 まず、コントラスト・スライダー・バーを移動し、その後*Min*(-) または*Max*(+) ボタンをクリックして、押されている各アイコンに対応するパラメータを微調整します。調整は即座に「ビデオ・ビューア」ウィンドウに表示されます。

4 完了したら*Close*ボタンをクリックして、手動ビデオ調整ダイアログ・ボックスを閉じます。

ターゲット・ビデオの設定

イメージ・キャプチャーの幅、ピクセル・サンプリング／微調整、イメージ・キャプチャーの水平位置、イメージ・キャプチャーの垂直位置の調整は、目的のビデオがどのようにキャプチャーされ、デジタル化されるかに影響しますが、ほとんど変更されることはありません。

イメージ・キャプチャ・パラメータは、自動調整機能によって自動的に変更されます。正確な調整を個別に行うためには、ターゲットに特別のイメージが必要になります。

自動ビデオ調整

大抵の場合、ビデオ設定をデフォルト設定から変更する必要はありません。システムが自動的に調整を行い、最適なビデオ・パラメータが適用されます。スイッチのOBWIは、ビデオ・パラメータが静的画面用ビデオ・パケットの送信なし（ゼロ）に設定されているときに最高の性能を発揮します。

ビデオ・パラメータは、手動ビデオ調整ダイアログ・ボックスの*Auto Adjust Video*ボタンから、簡単に希望の設定に調整できます。

注: また、ビデオを自動調整することもできます。この場合は、「ビデオ・ビューア」ウィンドウのメニューから、*Tools* → *Automatic Video Adjust*を選択するか、または*Automatic Video Adjust*ツールバー・アイコンをクリックします。

ビデオ・テスト・パターン

手動ビデオ調整ダイアログ・ボックスの*Video Test Pattern*ボタンをクリックすると、ビデオ・テスト・パターンの表示に切り替わります。*Video Test Pattern*ボタンをもう一度クリックすると、通常のビデオ画像に切り替わります。

ベンダー固有のビデオ設定

ビデオ設定はメーカー間で大幅に変わります。Dellのオンライン・データベースでは、さまざまなビデオ・カード（特にSun固有の製品）での最適なビデオ設定に関するデータを提供しています。この情報は、Dellのオンライン・ノレッジ・ベースから検索していただくか、Dellテクニカル・サービスまでお電話にてお問い合わせください。

色の設定

色の深度の調整

Dambrackas Video Compression® (DVC) アルゴリズムでは、リモート・セッション・ウィンドウでの表示色数を調整できます。表示色を増やすと色の忠実度がベストになり、色数を減らすとネットワーク・データ転送量を減らすことができます。必要に応じて調整してください。

「ビデオ・ビューア」ウィンドウは、「色ー最適化」(更新レートは最も遅くなります) 、「圧縮ー最適化」(最も速い更新レート) 、またはこの2つの組み合わせ、または「グレースケール」で表示できます。

個々のポートとチャンネルの色の階調は、リモート・セッション・ウィンドウで *View Color*コマンドを選択して指定できます。この設定はチャンネル別に保存されます。

コントラストと明るさ

「ビデオ・ビューア」ウィンドウの画像が暗すぎたり明るすぎたりする場合は、*Tools* → *Automatic Video Adjust*の順に選択するか、*Automatic Video Adjust*ボタンをクリックします。このコマンドはまた、自動ビデオ調整ダイアログ・ボックスでも使用できます。大概の場合、これでビデオの問題は修正されます。

*Auto Adjust*を数回クリックしてもコントラストと明るさが希望どおりに調整されない場合は、これらを手動で調整することで改善できる場合があります。明るさのレベルを上げてみます。コントラストを変える前に、10目盛り以上増やさないでください。一般的に、コントラストはほんのわずかの変更ですむはずです。

ノイズの設定

検出しきい値

ビデオ通信のノイズがパケット／秒の読み取り値に影響して値が高くなることがあります。この場合、カーソルを動かすとカーソルの周りで小さなドットが変動するため分かります。しきい値を変更すると、「より安定した」画面が得られ、カーソル・トラッキングを改善できます。

通常のビデオ圧縮を使用している場合、ノイズのしきい値と優先順位のしきい値は変更できます。しきい値をデフォルトに戻すには、*Auto Adjust Video*をクリックします。

注: ノイズのしきい値をゼロに設定すると、ビデオが継続的に更新されるため、ネットワーク利用率が上がり、ビデオのちらつきが起こります。ノイズのしきい値は最大に設定し、移動するマウス・カーソルの下のピクセルの色が復元される間も、システム性能を効率化することをお薦めしています。

注: ノイズのしきい値を調整する場合、大きく調整するにはスライダー・バーを、微調整するにはスライダー・バーの両端のPlus(+) ボタンとMinus(-) ボタンを使用します。

色の階調の変更に関する詳細は、「ビューの調整」(ページ 96) を参照してください。

マウスの設定

マウス・オプションの調整

「ビデオ・ビューア」ウィンドウのマウス・オプションでは、カーソル・タイプ、カーソル・モード、マウス・スケール、位置合わせ、およびリセットを調整できます。マウスの設定は、デバイスで固有です。すなわち、デバイスごとに異なる設定ができます。

注: マウスをプラグ・アンド・リプラグする機能をデバイスでサポートしていない場合(新しいPCのほとんどがこの機能をサポートしています) 、マウスは使用不能になり、デバイスの再起動が必要になります。

カーソル・タイプ

「ビデオ・ビューア」ウィンドウのメニューではローカルのマウス・カーソル用に5種類の表示オプションがあります。また、カーソル「なし」か、デフォルト設定にすることもできます。

「Single Cursorル」モードでは、「ビデオ・ビューア」ウィンドウのローカル(第二) カーソルの表示がオフになり、ターゲット・デバイスのマウス・ポインターだけが表示されます。表示されるマウスの動きは、ターゲット・デバイスのリモート・カーソルのものだけになります。「Single Cursor」モードは、ローカル・カーソルが不要な場合に使用します。

図 4.3. ローカルとリモートの両方のカーソルが表示された状態の「ビデオ・ビューア」ウィンドウ

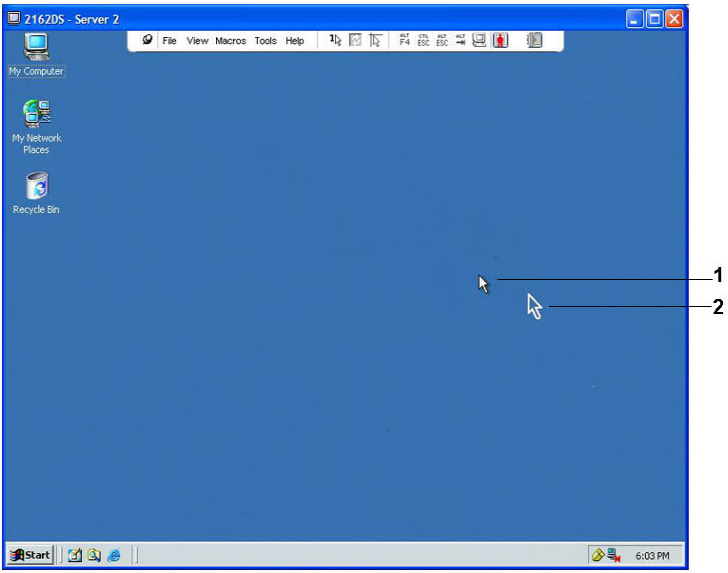


表 4.3: 図 4.3の説明

番号	説明
1	リモート・カーソル
2	ローカル・カーソル

「ビデオ・ビューア」ウィンドウがどのカーソル・モードになっているかは、タイトル・バーに、「Single Cursor」モードの終了に使用するキーストロークと共に表示されます。「Single Cursor」モードを終了させるためのキーストロークは、「セッション・オプション」ダイアログ・ボックスで定義できます。

注: クライアント・サーバーに送られる前にキーストロークをキャプチャーするデバイスを使用している場合は、マウス・ポインターの復元にこれらのキーを使用することは避けてください。

「Single Cursor」モードを開始するには、「ビデオ・ビューア」ウィンドウ・メニューから *Tools* → *Single Cursor Mode*の順に選択するか、または*Single Cursor Mode*ボタンをクリックします。ローカル・カーソルは表示されず、すべての動きがターゲット・デバイスに対応します。

既存の「Single Cursor」モードを終了するためのキーを選択するには:

1 「ビデオ・ビューア」ウィンドウのメニューから、*Tools* → *Session Options* の順に選択します。

-または-

*Session Options*ボタンをクリックします。

「Session Options」ダイアログ・ボックスが表示されます。

2 *Mouse*タブをクリックします。

3 「Single Cursor」モード領域内のドロップダウン・メニューから、終了用キーストロークを選択します。

4 *Save*をクリックして、設定内容を保存します。

「Single Cursor」モードを有効にした場合、先ほど指定したキーを使用すれば、「通常のデスクトップ」モードに戻れます。

「Single Cursor」モードを終了するには、タイトル・バーに表示されている終了用のキーを押します。

マウス・カーソルの設定を変更するには次の手順を実行します。

1 「ビデオ・ビューア」ウィンドウのメニューから、*Tools* → *Session Options*の順に選択します。

-または-

*Session Options*ボタンをクリックします。

「Session Options」ダイアログ・ボックスが表示されます。

2 *Mouse*タブをクリックします。

3 「Local Cursor」パネルでマウス・カーソル・タイプを選択します。

4 *OK*をクリックして設定内容を保存します。

マウス・スケール

Linuxの以前バージョンの一部では、マウス加速度の調整がサポートされていませんでした。これらの古いバージョンにインストールする必要がある場合は、事前設定されている3種類のマウス・スケール・オプションから選ぶか、またはカスタム・スケールを設定できます。前もって構成されている設定は、Default (1:1)、High (2:1) または Low (1:2) の3つです。

- 1:1のスケール率では、デスクトップ・ウィンドウでのマウスのすべての動きは、実際のマウスの動きと等しい動きとしてターゲット・デバイスに送られます。
- 2:1のスケール率では、同一のマウスの動きは2倍速の動きとして送られます。
- 1:2のスケール率では、この値は2分の1になります。

マウス・スケールを設定するには:

1 「ビデオ・ビューア」ウィンドウのメニューから、*Tools* → *Session Options*の順に選択します。

-または-

Session Options ボタンをクリックします。

「Session Options」ダイアログ・ボックスが表示されます。

2 *Mouse*タブをクリックします。

3 規定の設定の1つを使用するには、該当するオプション・ボタンをオンにします。

-または-

カスタム・スケールを設定するには:

a. *Custom*オプション・ボタンをクリックして、Xフィールドと Yフィールドを有効にします。

b. スケール値を「X」フィールドと「Y」フィールドに入力します。マウスの各入力に対し、マウスの動きは、Xと Yの各スケール係数を乗じた動きとなります。有効な入力範囲は、0.25～3.00です。

マウス位置合わせと同期

スイッチのOBWIではマウスからのフィードバックを継続的に得ることはできないため、スイッチでのマウスの動作がホスト・システムのマウス動作と同期しなくなることがあります。マウスやキーボードが正しく応答しなくなった場合は、マウスを調整して適切なトラッキングが得られるようにできます。

位置合わせを調整することで、ローカル・カーソルがリモート・ターゲット・デバイスのカーソルと揃うようになります。リセットを行うと、マウスとキーボードを一度接続解除して接続し直したかのような効果が得られます。

マウスの位置を再度合わせるには、「ビデオ・ビューア」ウィンドウのツールバーで *Align Local Cursor* ボタンをクリックします。

バーチャル・メディア

バーチャル・メディア機能を使用すると、クライアント・サーバー上のユーザーは、そのマシンの物理ドライブをバーチャル・ドライブとしてターゲット・デバイス上にマッピングできます。また、クライアント・サーバーはISOまたはフロッピーのイメージ・ファイルをバーチャル・ドライブとしてターゲット・デバイス上に追加し、マッピングできます。同時にマッピングできるのは、CDドライブ1台と大容量記憶装置1台です。

- CD／DVDドライブ、ディスク・イメージ・ファイル（ISOまたはフロッピーのイメージ・ファイルなど）は、バーチャルCD／DVD-ROMドライブとしてマッピングされます。
- フロッピー・ドライブ、USBメモリー・デバイス、その他のメディア・タイプは、バーチャル大容量記憶装置としてマッピングされます。

OBWIを使用するバーチャル・メディア・セッション設定の構成に関する詳細は、「ローカル・バーチャル・メディア・セッションの構成」（ページ 81）を参照してください。

要件

ターゲット・デバイスは、バーチャル・メディアをサポートし、USB2またはUSB2およびCAC用SIPを備えたKVMスイッチに接続されている必要があります。

ターゲット・デバイスは、バーチャルにマッピングしようとしているUSB2対応メディア・タイプを利用可能なデバイスである必要があります。すなわち、ターゲット・デバイスがポータブルUSBメモリー・デバイスをサポートしていない場合は、クライアント・サーバー上のメモリー・デバイスをバーチャル・メディア・ドライブとしてターゲット・デバイスにマッピングすることはできません。

ユーザー(またはユーザーが所属するユーザー･グループ) には、ターゲット･デバイスに対するバーチャル･メディア･セッションや予約済みバーチャル･メディア･セッションを確立するアクセス権が必要です。「 ユーザー･アカウントのセットアップ」(ページ 86) を参照してください。

ターゲット･デバイスに対してアクティブにできるバーチャル･メディア･セッションは、一度に1つだけです。

共有およびプリエンプト 操作の考慮事項

KVMセッションとバーチャル･メディア･セッションは別個のものです。したがって、共有／専用／プリエンプト･セッションには多くのオプションがあります。Avocent管理ソフトウェアには、さまざまなシステム･ニーズに対応できる柔軟性があります。

たとえば、KVMセッションとバーチャル･メディア･セッションを同時にロックできます。このモードでは、KVMセッションの接続が解除されると、関連付けられているバーチャル･メディア･セッションの接続も解除されます。これらのセッションが同時にロックされていない場合は、バーチャル･メディア･セッションをアクティブにしたまま、KVMセッションを終了できます。この機能は、ユーザーがバーチャル･メディア･セッションを使用して時間がかかるタスク(オペレーティング･システムのロードなど) を実行しているときに、処理の進行中に他の機能を実行するために異なるターゲット･デバイスとKVMセッションを確立したい場合などに役立ちます。

関連するKVMセッションなしにバーチャル･メディア･セッションがターゲット･デバイスでいったんアクティブになった場合は、そのチャンネルにオリジナル･ユーザー(ユーザーA) が再接続するか、別のユーザー(ユーザーB) が接続できます。「 バーチャル･メディア」ダイアログ･ボックスにあるオプション(「 予約済み」) を設定すると、KVMセッションでそのチャンネルへのアクセスをユーザーAにのみ許可できます。

ユーザーBにこのKVMセッションへのアクセスを許可した(「 Reserved」オプションが無効になっている) 場合は、ユーザーB

がバーチャル・メディア・セッションで使用されているメディアを制御できます。ティアド（階層）接続環境で「Reserved」オプションを使用すると、ユーザーAにのみ下層スイッチへのアクセスを許可し、また上層スイッチと下層スイッチ間のKVMチャンネルをユーザーA用に予約できます。

Virtual Mediaダイアログ・ボックス

「バーチャル・メディア」ダイアログ・ボックスでは、バーチャル・メディアのマッピングとアンマッピングを管理できます。このダイアログ・ボックスには、バーチャル・ドライブとしてマッピング可能なクライアント・サーバー上の物理ドライブがすべて表示されます。「バーチャル・メディア」ダイアログ・ボックスを使用すると、ISOやフロッピーのイメージ・ファイルを追加した後で、それらをマッピングすることもできます。

デバイスをマッピングすると、「バーチャル・メディア」ダイアログ・ボックスの詳細表示に、転送されたデータ量と、デバイスのマッピング後に経過した時間に関する情報が表示されます。

バーチャル・メディア・セッションは、予約済みとして指定できます。セッションが予約され、関連付けられているKVMセッションが終了した場合は、他のユーザーがこのターゲット・デバイスへのKVMセッションを起動することはできません。セッションが予約されていない場合は、別のKVMセッションを起動できます。

Virtual Mediaダイアログ・ボックスからは、SIPをリセットすることもできます。この操作により、ターゲット・デバイス上のすべてのUSBメディアがリセットされます。この操作はターゲット・デバイスが応答しない場合にのみ、注意して実行してください。

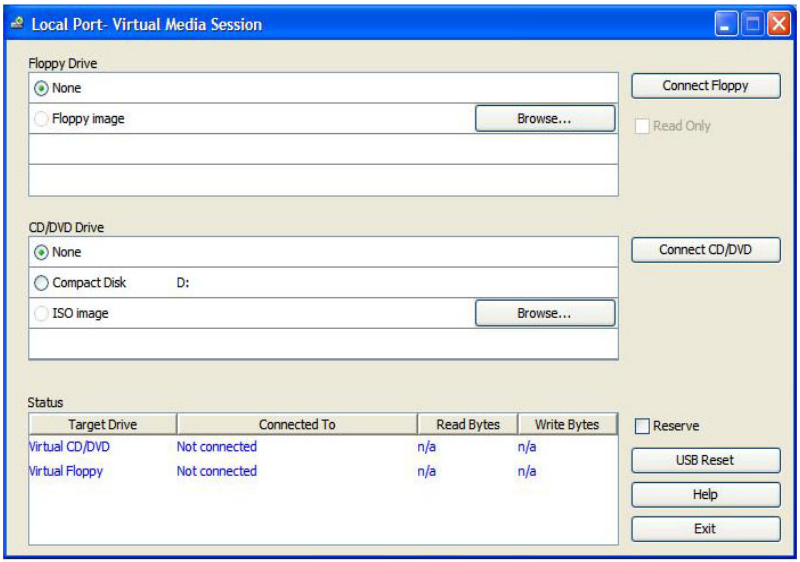
バーチャル・メディア・セッションの開始

バーチャル・メディア・セッションを起動するには次の手順を実行します。

ビデオ・ビューアのメニューから、*Tools* → *Virtual Media*を選択します。「バーチャル・メディア」ダイアログ・ボックスが表示されます。

セッションを予約済みにするには、*Details*をクリックしてから、*Reserved*チェックボックスをオンにします。

図 4.4. ビデオ・ビューアの「バーチャル・メディア」ダイアログ・ボックス



バーチャル・メディア・ドライブをマッピングするには次の手順を実行します。

1 ビデオ・ビューア・メニューから、*Tools* → *Virtual Media*を選択してバーチャル・メディア・セッションを開始します。

2 バーチャル・メディア・ドライブとして物理ドライブをマッピングするには次の手順を実行します。

a. 「バーチャル・メディア」ダイアログ・ボックスで、マッピングするドライブの横にある*Mapped*チェックボックスをオンにします。

b. マッピングするドライブを読み取り専用アクセスに制限する場合は、ドライブの横にある*Read Only*チェックボックスを

オンにします。マッピングされたすべてのドライブがバーチャル・メディア・セッションの設定で既に読み取り専用になっている場合は、このチェックボックスがあらかじめオンになり、これを変更することはできません。

セッションの設定で読み取り／書き込みアクセスが有効になっているものの、特定のドライブへのアクセスを読み取り専用に制限したい場合は、*Read Only* チェックボックスをオンにします。

3 ISOまたはフロッピー・イメージをバーチャル・メディア・ドライブとして追加してマッピングするには次の手順を実行します。

a. 「バーチャル・メディア」ダイアログ・ボックスで、*Add Image* をクリックします。

b. 共通のファイル・ダイアログ・ボックスが表示され、ディスク・イメージ・ファイル(.isoか.imgの拡張子を持つファイル) を格納しているディレクトリが表示されます。ISOまたはフロッピー・イメージ・ファイルを選択して、*Open*をクリックします。

-または-

クライアント・サーバーのオペレーティング・システムがドラッグ・アンド・ドロップをサポートしている場合は、ISOまたはフロッピー・イメージ・ファイルを共通ファイル・ダイアログ・ボックスから選択し、それを「バーチャル・メディア」ダイアログ・ボックスにドラッグします。

c. 確認のため、ファイル・ヘッダーにチェック印がつきます。チェック印がつくと共通ファイル・ダイアログ・ボックスが閉じ、選択したイメージ・ファイルが「バーチャル・メディア」ダイアログ・ボックスに表示されます。このダイアログ・ボックスの*Mapped*チェックボックスをオンにすると、ファイルのマッピングが可能になります。

d. 他にもISOやフロッピー・イメージを追加したい場合は、これらの手順を繰り返します。イメージ・ファイルは(メモリーの容量範囲内で)いくつでも追加できますが、バーチャルのCD、DVDまたは大容量記憶装置は同時に1つしかマッピングできません。

マッピングしようとしているドライブの数が多すぎたり(1台のCDまたはDVDドライブと1台の大容量記憶装置)、特定タイプのドライブの数が多すぎる(2台以上のCDまたはDVDドライブか大容量記憶装置)場合は、メッセージが表示されます。新しいドライブをマッピングする場合は、まず現在マッピングされているドライブをアンマップしてから別のドライブをマッピングする必要があります。

物理ドライブかイメージのマッピングが完了すると、ターゲット・デバイスで使用できるようになります。

バーチャル・メディア・ドライブのマッピングを解除するに:

1 「バーチャル・メディア」ダイアログ・ボックスで、アンマップするドライブの横にある*Mapped*チェックボックスをオフにします。

2 確認を求めるメッセージが表示されます。アンマップを確定するか、キャンセルします。

3 アンマップするバーチャル・メディア・ドライブごとに上記の手順を繰り返します。

バーチャル・メディア・ドライブの詳細を表示するには次の手順を実行します。

「バーチャル・メディア」ダイアログ・ボックスで、*Details*をクリックします。ダイアログ・ボックスが拡張され、「詳細」の表が表示されます。各行の情報は、次のとおりです:

- ターゲット・ドライブ – マッピングされたドライブの名前(バーチャルCD 1やバーチャルCD 2など)。

- マッピング先 ー「 クライアント 表示」の「 ドライブ」 列に表示されているドライブ情報と同じ。
- 読み取りバイト 数および書き込みバイト 数 ー マッピングを行ってから転送されたデータ量。
- Duration ー ドライブをマッピングしてから経過した時間。

「 詳細」 表示を閉じるには、*Details*を再度クリックします。

ターゲット・デバイス上のすべてのUSBデバイスをリセットするには次の手順を実行します。

注: USBリセット 機能は、ターゲット・デバイス上のすべてのUSBメディア(マウスおよびキーボードを含む) をリセットします。この操作を実行するのはターゲット・デバイスが応答しない場合のみに限定してください。

1 「 バーチャル・メディア」 ダイアログ・ボックスで、*Details*をクリックします。

2 「 Details」 ビューが表示されます。*USB Reset*をクリックします。

3 リセットした場合の影響を警告するメッセージが表示されます。リセットを確定するか、キャンセルします。

4 「 詳細」 表示を閉じるには、*Details*を再度クリックします。

バーチャル・メディア・セッションの終了

「 バーチャル・メディア」 ダイアログ・ボックスを閉じるには次の手順を実行します。

1 *Exit*をクリックします。

2 マッピングしたドライブがある場合は、アンマップされる旨のメッセージが表示されます。操作を確定するか、キャンセルします。

バーチャル・メディア・セッション、もしくはバーチャル・メディア・セッションが関連付けられてロックされたアクティブなKVMセッ

ションをユーザーが接続解除しようとすると、バーチャル・メディアのマッピングが失われる旨の確認メッセージが表示されます。

スマート・カード

クライアント・サーバーの利用可能なUSBポートにスマート・カード・リーダーを接続して、スイッチ・システムに接続されているターゲット・デバイスにアクセスできます。その後、KVMセッションを起動してビデオ・ビューアを開き、スマート・カードをマッピングできます。

注: すべてのスマート・カード・リーダーには、DellのUSB2およびCAC用SIPまたはAvocent VMC IQモジュールを使用する必要があります。

スマート・カードの状態は、ビデオ・ビューアのツールバーの右端にあるスマート・カード・アイコンに表示されます。次の表にスマート・カードのステータス・アイコンの概要を示します。

表 4.4: スマート・カードのアイコン

アイコン	説明
	スマート・カードがスマート・カード・リーダーに挿入されていないか、またはスマート・カード・リーダーが接続されていません。
	スマート・カードはスマート・カード・リーダーに挿入されていますが、まだマッピングされていません。
	スマート・カードはマッピングされています(緑のアイコン)。

スマート・カードをマッピングするには次の手順を実行します。

1 KVMセッションを開始し、「ビデオ・ビューア」ウィンドウのメニューを表示します。

2 クライアント・サーバーに接続されているスマート・カード・リーダーにスマート・カードを挿入します。

3 「ビデオ・ビューア」ウィンドウ・メニューで、*Tools* → *Map Smart Card*の順にクリックします。

4 ターゲット・デバイスにマッピングされているスマート・カードがない場合は、「マッピング済みのカードはありません」オプションの横にドットが表示されます。このオプションの下の一覧からスマート・カードを選び、スマート・カードをマッピングします。

スマート・カードをアンマップするには、「ビデオ・ビューア」ウィンドウのメニューの*X*をクリックしてKVMセッションを終了し、*Tools* → *No Card Mapped*の順に選択し、スマート・カード・リーダーからスマート・カードを取り外すか、またはクライアント・サーバーとスマート・カード・リーダーとの接続を解除します。

キーボード・パススルー

ユーザーが入力するキーストロークは、「ビデオ・ビューア」ウィンドウの画面表示モードに従って2種類に解釈されます。

- 「ビデオ・ビューア」ウィンドウが全画面表示(Full Screen)モードの場合、すべてのキーストロークおよび*Ctrl-Alt-Del*を除くキーストロークの組み合わせのすべてが、表示中のリモート・ターゲット・デバイスに送られます。
- 「ビデオ・ビューア」ウィンドウが通常のデスクトップ・モードの場合、特定のキーストロークやキーの組み合わせをリモート・ターゲット・デバイスとローカル・コンピュータのどちらで認識させるようにするかを、キーボード・パススルー・モードによって制御できます。

これには、キーボード・パススルーを「セッション・オプション」ダイアログ・ボックスで設定する必要があります。キーボード・パス・スルー・モードが有効になっていると、「ビデオ・ビューア」ウィンド

ウがアクティブであれば、すべてのキーストロークおよびCtrl-Alt-Delを除くキーストロークの組み合わせのすべてが、表示中のリモート・ターゲット・デバイスに送られます。ローカル・デスクトップがアクティブになっている場合、ユーザーが入力したキーストロークとキーストロークの組み合わせはローカル・コンピュータに反映されます。

注: Ctrl-Alt-Deleteのキーストロークの組み合わせは、マクロを使用しなければリモート・ターゲット・デバイスに送ることはできません。

注: 日本語キーボードのALT - 半角／全角キーストロークの組み合わせは、画面モードやキーボード・パススルー・モードの設定に関係なく、常にリモート・ターゲット・デバイスに送られます。

キーボード・パススルーを指定するには:

1 「ビデオ・ビューア」ウィンドウのメニューから、*Tools* → *Session Options*の順に選択します。

-または-

*Session Options*ボタンをクリックします。

「セッション・オプション」ダイアログ・ボックスが表示されます。

2 *General*タブをクリックします。

3 *Pass-through all keystrokes in regular window mode*を選択します。

4 *OK*をクリックして設定内容を保存します。

マクロ

スイッチのOBWIには、Windows、Linux、およびSunのプラットフォーム用にマクロが既定されています。

マクロを実行するには、「ビデオ・ビューア」ウィンドウのメニューから*Macros* → *<目的のマクロ>*を選択するか、またはビデオ・ビューア・メニューにあるボタンから実行するマクロを選択します。

表示の保存

「ビデオ・ビューア」の表示は、ファイルに保存するか、またはクリップボードにコピーして、ワード・プロセッサーやその他のプログラムで使用できます。

「ビデオ・ビューア」ウィンドウをファイルにキャプチャーするには:

1 「ビデオ・ビューア」ウィンドウのメニューから、*File* → *Capture to File*の順に選択します。

-または-

*Capture to File*ボタンをクリックします。

「名前をつけて保存」ダイアログ・ボックスが表示されます。

2 ファイル名を入力し、ファイルの保存先を指定します。

3 *Save*ボタンをクリックし、ウィンドウの画像をファイルに保存します。

「ビデオ・ビューア」ウィンドウをクリップボードにキャプチャーするには、「ビデオ・ビューア」ウィンドウのメニューから*File* → *Capture to Clipboard*にキャプチャの順に選択するか、または*Capture to Clipboard*ボタンをクリックします。イメージ・データがクリップボードに保存されます。

セッションの終了

「ビデオ・ビューア」ウィンドウ・セッションを終了するには次の手順を実行します。

「ビデオ・ビューア」ウィンドウから*File* → *Exit*の順に選択します。

5

RCSのLDAP機能

LDAPは、TCP/IPを使用するディレクトリのアクセスおよび更新に使用されるプロトコルの規格です。Dell RCSソフトウェアおよびOBWIは、標準スキーマとDell拡張スキーマの両方をサポートしており、認証、プライバシー、および統合性などの強固なセキュリティ機能を提供します。

注: IPv6モードでLDAPを使用するには、Windows 2008 Serverが必要です。

注: Active Directoryを使用してRCSユーザーを認識する機能は、Microsoft Windows® 2000およびWindows Server 2003オペレーティング・システムでサポートされています。

Active Directoryの構造

Active Directory(AD) 配置は、オブジェクトの階層構造を持つ分散型データベースで構成されています。各オブジェクトは、そのオブジェクトに保存できるデータの種類を決定するオブジェクト・クラスと関連付けられています。階層的構造はADドメインを表すオブジェクトで始まり、ドメイン名の階層を形成するように配置されており、この階層は、DNS名前空間が通常描かれるのと同じ方法のツリー図で表現できます。Dell RCSは、浅いまたは深い階層的名前構造に展開されたドメインの単一ツリーをサポートするように設計されています。

ドメイン・コントローラー・コンピューター

ドメイン階層には、ADがLDAPサービスを提供しているドメイン・コントローラー・コンピューターの対応する階層が関連付けられていま

す。各ドメインが、複数のピア・ドメイン・コントローラーを持つ場合や、地理的なサイト全般にもわたっている場合があります。Dell RCSのパッケージは、ADのこれらの両側面をサポートするように設計されています。Dell RCSは、DNSを使用してそれぞれのドメイン・コントローラーのネットワーク座標を決定するため、ネットワーク上で一部のドメイン・コントローラーが使用できない状況でも正常に処理できます。DNS SRVレコードがこの目的で使用されるため、Dell RCSは、SRVレコードに構成された管理設定に基づいて、常にもっとも近いサイトから先に代替ドメイン・コントローラーとの接続を試みます。

オブジェクト・クラス

各ドメイン内に、さまざまなエンティティやエンティティのグループ分けについての情報を保存するために設計された別のオブジェクト階層があります。これらのエンティティはAD内で、オブジェクトのグループ分けを編成する役割を果たす「コンテナ」を定義するために使用されるオブジェクト・クラスによって表現されています。ほかのオブジェクト・クラスは、ネットワーク・ユーザー、コンピューター、プリンター、またはネットワーク・サービスなどのエンティティを表します。コンテナ・オブジェクト・クラスの中で特に興味深いものは、グループと組織単位(OU)の2種類です。これらの2つのオブジェクト・クラスを使用して、エンティティのグループ分けを定義できるため、AD管理者はアクセス制御やその他の管理ポリシーの適用を簡素化できます。たとえば、ドメインをEngineeringという名前のOUコンテナを持つように構成し、その中にHardware、Software、Supportなど機能に応じた名前の付けられた複数のグループ・オブジェクトを含め、各グループにはUserオブジェクトのメンバーシップ・リスト、またコンピューター・オブジェクトのメンバーシップ・リストなどを構成します。さらに、グループをネストすることで、さらにもう1つの階層レベルを構成できます。ネストは、グループ・オブジェクトの名前を別のグループ・オブジェクトのメンバーシップに含めることによって形成されます。各ADグループ・オブジェクトには関連付けられたスコープがあり、他のグループとの間で許可されるネスト関係のタイプを構成するために使

用されることに注意してください。たとえば、スコープがユニバーサルに設定されている場合、グループはドメイン境界を越えるネストに参加できますが、スコープがローカルに設定されている場合は、グループはそのようなネストに参加できません。ネストの規則は、Microsoft社から入手可能なAD製品のマニュアルに記載されています。Dell RCSのパッケージは、ADに定義されているすべてのネスト規則をサポートするように設計されています。

属性

ADで使用される階層は、もう1つあります。各オブジェクト・クラスには、表現されているエンティティについての特定の情報を保存するために使用される一連の「属性」が関連付けられています。たとえば、Userオブジェクト・クラスには、SAM ACCOUNT NAMEという名前の属性タイプや、FIRST NAME、SURNAME、PASSWORDなどを関連付けられます。Dellリモート・コントロール・スイッチのパッケージでは、SAM ACCOUNT NAMEとPASSWORDの属性を使用して、ユーザーを認証します（これらの2つの属性の正式なAD名は、それぞれsAMAccountNameとunicodePWDです）。

スキーマの拡張

ADには、コンピューター・オブジェクトとユーザー・オブジェクトのデフォルト・コンテナを含む多くのオブジェクト・クラスのほか、OUコンテナのクラス、およびコンピューターとユーザーのエンティティを表現するクラスが同梱されています。ADを拡張して、アクセス制御の管理を簡単にするためにDellが提供する新しいオブジェクト・クラスなどを含むことができます。このような拡張は通常、「スキーマ拡張」と呼ばれ、このマニュアルで説明されているDell Extended Schema機能の根幹です。これらのスキーマ拡張により、カスタマイズされたオブジェクト・クラスを利用して、Dell RCS、アクセス制御情報、および特定のアクセス制御情報と特定のDell RCSインスタンスやユーザー・インスタンスを関連付けるために使用されるコンテナの型を表すことができます。ADで使用されるそれぞれの属性タイプとオブジェクト・クラスは、オブジェクト

識別子(OID) というグローバル一意識別子を持っている必要がある点に、注意することが大切です。これらの一意識別子は、最終的には国際的に認知された機関によって管理されています。ADの場合、OID空間はMicrosoftによって補助的に管理されています。Dellは、Dell Extended Schema機能で使用されるカスタム・オブジェクト・クラスと属性タイプのためのOIDを取得しています。以下は、Dellが取得したOIDの概略です。

Dell拡張は: dell

Dellベース OIDは: 1.2.840.113556.1.8000.1280

RCS LinkID範囲は: 12070から 12079

Dell RCSのパッケージは、ADに組み込まれているクラスにあるオブジェクト・クラスのみを使用しても機能するように設計されています。このオプションは標準スキーマと呼ばれています。このオプションでは、コンピュータ・オブジェクト・クラスを使用して、Dell RCSオブジェクトと標準のGroupオブジェクトが表されます。これらのオブジェクトは、特定のアクセス制御情報をDell RCSとUserの特定インスタンスに関連付けるために使用されます。この場合、アクセス制御情報は、グループ・オブジェクト内の特定の属性タイプに保存されます。

ADに存在する階層構造のため、ディレクトリ・オブジェクトに保存された情報にアクセスすることが難しい場合があります。階層のナビゲーションに伴う遅れを避けるために、Dell Remote Console Switchのパッケージは、グローバル・カタログ(GC) というADの特性を使用するように設計されています。GCは、完全なADデータベースに保存されているデータのサブセットへのアクセスを可能にすることと、階層と地理的分布のすべてを比較的に平らな単一構造に「折りたたむ」ことによって、「クイック検索」サービスを提供します。GCは、完全なADデータベースで作用するのと同じLDAPディレクトリ・クエリを使用してクエリされます。GCサービスも提供するように設定するためには、AD製品は企業内に最低1つのドメイン・コントローラを必要とし、ADの実際の配置では、ドメイン・コントローラの一部またはすべてがGCサービスを提供するように設

定できます。Dell RCSのパッケージは、DNSを使用して各GCサーバーのネットワーク座標を決定します。これにより、Dell RCSは、ネットワーク上の一部のGCサーバーが使用できない状況も問題なく処理できます。DNS SRVレコードがこの目的で使用されるため、Dell RCSは、SRVレコードに構成された管理設定に基づいて、常にもっとも近いサイトから先に代替GCサーバーとの接続を試みます。

Standard SchemaとDell Extended Schema

多数の顧客環境で最大の柔軟性を提供できるよう、Dellは、希望する結果に応じてユーザーが設定できる1組のオブジェクトを提供しています。Dellは、Association、Device、およびPrivilegeのオブジェクトを含むようにスキーマを拡張しています。Associationオブジェクトは、ユーザーまたはグループを、1つ以上のSIPに対する特権の特定のセットとリンクするために使用されます。Deviceオブジェクトは、Active Directory構造内の個々のRCSスイッチを定義します。Privilegeオブジェクトは Associationオブジェクトを介してDeviceオブジェクトにリンクされ、使用アクセス権を割り当てます。

このモデルは、あまり複雑さを増すことなく、ユーザー、特権、およびRemote Console Switch上のSIPの異なる組み合わせに対して、最大の柔軟性を管理者に提供します。

Dell Schema Extensionsをインストールする前に、管理者はこの章の説明を通読して、個々のインストール状況にはどのスキーマが適切かを判断してください。スキーマ・オブジェクトを変更するとActive Directory全体に適用しますので、一旦作成したら削除できません。非アクティブにすることしかできません。このため、スキーマを変更する前に、そのメリットを慎重に考慮してください。

Dell Schema Extensionをインストールすることで得られる主なメリットは、混乱を排除できることです。標準のActive Directoryスキーマを使用する場合、Remote Console Switchはコンピュータ・デバイス・オブジェクトに最もよく一致し、その1つとして設定されます。RCS

はコンピュータ ーではないため、すべてのスキーマ機能が適用されるわけではありません。この方法で指定されたRCSスイッチを正しく構成するためには、注意が必要です。

さらに、Dell Schema Extensionを使用すると、スイッチ・デバイスの検索と識別が簡単になります。コンピュータ ー・デバイス・オブジェクトを使用して設定されたスイッチは、Active Directory構造内のすべてのコンピュータ ー・デバイスとともに検索されます。

RCSは、どちらのスキーマを使用しても同様に認証でき、どちらの方法を使用しても機能性は失われません。個々のインスト ールに適した方法を、管理者が自由に選択できます。Dell Schema Extensionがある場合とない場合のどちらについても、インスト ールの操作説明が提供されています。1つのスキーマ・セット のみに関する説明はそのように記載されていますので、そのスキーマが使用されないインスト ールの場合には、その説明を無視しても構いません。

標準インスト ール

Dell RCSでActive Directoryを使用して認証するためには、次を行います。

1 Override Admin Accountを構成します。

2 DNS設定を構成します。

3 NTP(Network Time Protocol) 設定します。

4 認証パラメータ ーを構成します。

5 グループ・オブジェクトを構成します。

6 CAルート 証明書を作成し、ダウンロードします。

7 ログイン・タイムアウトを設定します。

Override Admin Accountを構成します。

ネットワーク障害の発生に備え、LDAPサーバーに照会し、認証するユニットの性能に関係なく使用できるアカウントが用意されています。ほかの設定を構成する前に、このアカウントを構成する必要があります。Override Admin AccountをOBWIで構成するには次の手順を実行します。

1 *User Accounts*をクリックして、*Override Admin*をクリックします。

2 ユーザーに割り当てるユーザー名とパスワードを入力し、「Verify Password」フィールドにパスワードを再度入力して確認します。

3 **Save**をクリックします。

注: このオプションのadmin権限でログインする必要があります。

DNSの設定

LDAPクライアントが名前を解決できるようにするには、最低1つのDNSサーバーを指定する必要があります。

Networkサブカテゴリーに RCSの名前が表示され、IPアドレス、サブネット・マスク、ゲートウェイ、LAN速度、DHCP/BootP設定などのネットワーク設定を変更できます。表示されるRCSの名前は、SNMPカテゴリー内のSystem Nameフィールドに指定される名前と同じです。

Networkサブカテゴリーでは、最大3つのDNSサーバーの入力および管理を行うことができます。これらのDNSサーバーは、LDAP認証パネルに提示されるDNS名を解決するために使用されます。

注: 最低1つのDNSサーバーが、LDAP機能が作動するように構成されている必要があります。プライマリ・サーバーが使用できないときは常に、RCSソフトウェアで自動的にフェールオーバー機能が働き、ここで確認されるとDNSサーバーをバックアップします。

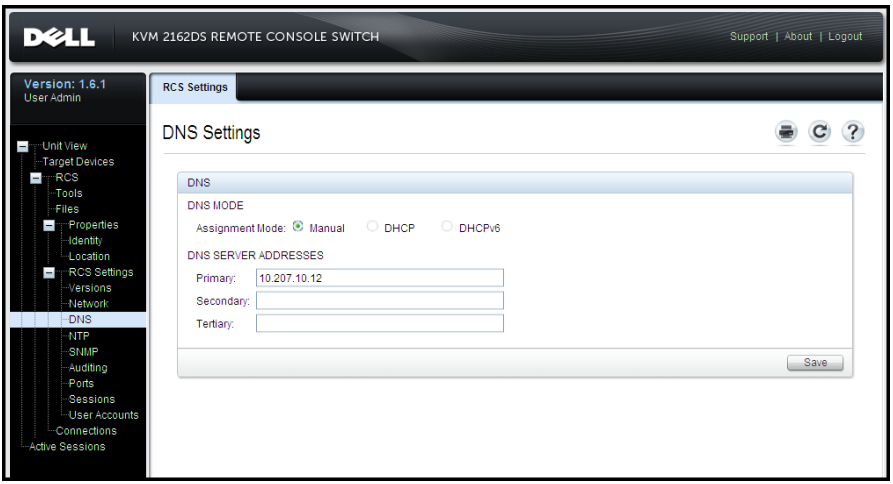
注: RCSのシリアル管理インターフェイスを使用しても、DNSサーバー・アドレスを設定できます。シリアル管理インターフェイスの使用に関する詳細は、RCSのマニュアルを参照してください。

OBWIでDNSを設定するには次の手順を実行します。

1 *DNS*をクリックして、DNS Settings画面を開きます。

2 DNSモードを指定し、サーバー・アドレスを入力してSaveをクリックします。

図 5.1. OBWI - DNS Settings



NTP(Network Time Protocol) の設定

スイッチは、証明書の期限が切れていないことを確認するために、現在の時刻にアクセスする必要があります。NTPからの時刻更新を要求するようにスイッチを構成できます。OBWIでNTP設定を構成するには次の手順を実行します。

1 *NTP*をクリックして、NTP画面を開きます。

2 Enable NTPボックスをクリックします。

3 所定のボックスにネットワーク時刻のソースの名前を入力します。時刻更新を要求する頻度を指定するために、1時間刻みの間隔を設定することもできます。間隔が0に設定されている場合は、RCSの起動時、またはGlobal → NTPメニューが変更された場合にのみ、要求が行われます。

4 Saveをクリックします。

LDAP認証パラメータの設定

認証パネルにより、RCS管理者がLDAP Directory Services.にアクセスするのに必要なパラメータを構成することができるようになります。ユーザーからアクセス・リクエストを受信すると、RCSはLDAPプロトコルを使用してユーザー名、パスワード、およびその他の情報をDirectory Serviceに送信してユーザーの持つアクセス権を特定します。

注: LDAP構成の確立で用いられるアクセス権は、KVM User、KVM User Admin、KVM Appliance Adminで、これらはUser、User Administrator、RCS Administratorにそれぞれ相当します。これらのアクセス・レベルは変更されていませんが、指示に従って新しいアクセス権を使用してください。

LDAP認証の有効

LDAP構成オプション画面の操作モードのセクションでは、LDAPサービスの適切なタイプを選択してユーザー認証に使用することができます。使用できるモードは以下の通りです。

- 標準LDAPディレクトリ・サービス(非Microsoft)
- Microsoft Active Directoryサービス
- LDAP認証の無効化

使用する代替(非LDAP)の認証方法が既に選択されている場合は、LDAP認証は自動的に無効になります。LDAP Directory Servicesを使用するには、この方法の選択を解除する必要があります。

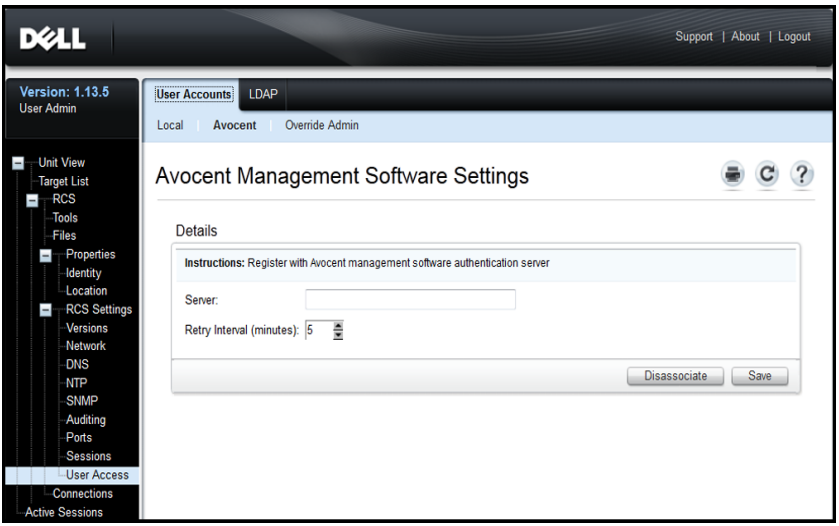
LDAP認証を使用するための機能を復元するには:

1 「User Access」で、*Avocent*タブを選択して、図 5.2を参照してください。

2 *Disassociate*をクリックして、Avocent管理認証サーバーの使用を選択解除します。

3 *Save*をクリックします。

図 5.2. Avocent認証画面

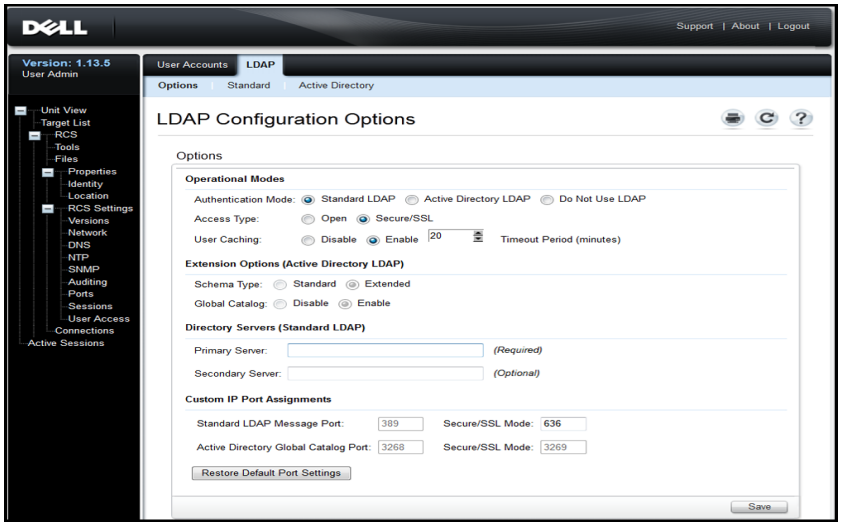


注: この手順を実行しないでAvocent認証の関連付けを外部的に破棄することは可能です。しかしながら、ユーザー認証用にAvocentサーバーの関連付けが作成されていた場合には、LDAP認証構成を続行できるようにするために、明示的にこの手順に従って削除する必要があります。

LDAP認証の有効化

1 「User Access」で、LDAPタブを選択して、図 5.3を参照してください。

図 5.3. LDAP構成オプション画面



2 「Operational Modes」画面で使用できるLDAP認証モードのなかから1つ選択します。

3 構成オプションは、LDAP認証をすべて有効にして使用できるように設定する必要があります。オプションのそれぞれについて、この章で詳細します。

4 *Save*をクリックします。

LDAP認証を無効にするには、*Do Not Use LDAP*オプションを選択して、*Save*をクリックします。 画面の他のオプションすべてが無効になり、これ以外の他のフィールドの編集はできなくなります。さらに、標準およびActive Directoryの両方のタブの下に表示される追加の構成画面も無効になります。

LDAP認証が無効になっていると、ユーザー・アクセスは、ローカルで定義されたユーザー・アクセス・リストまたはAvocent管理ソフトウェアのいずれかによって判定されます(「ユーザー・アクセス」のセクションを参照してください)。

LDAP認証が有効になっていると、ローカルで定義されたユーザー・アクセス・リストがLDAP Directory Serversへのリクエストよりも優先します。ユーザー・アクセスはRCS定義のユーザーについて最初のチェックを求めます。一致するものがない場合は、リクエストは構成に従ってLDAP Directory Serversに送信されます。

認証パラメータの入力 - 操作モード

アクセス・タイプ

LDAPディレクトリ・サーバーはオープン・モードまたはセキュア・モード（SSL-セキュア・ソケット・レイヤー暗号化を使用）のいずれかで操作するようにセットアップできます。この選択したモードはホスト・ディレクトリ・サーバーのものと一致する必要があります。セキュア／SSLモードを選択する場合は、暗号化された操作の要件を満たすためのガイダンスとして、「LDAP SSL証明書」のタイトルが付いたセクションも参照してください。

ユーザーのキャッシュ保存

LDAPを介したユーザーの認証が正しく完了すると常に、RCSでLDAPディレクトリ・サーバーから取得した結果が選択した期間保持されます。もし、その期間に、別のアクセスが生成された場合、通常は、結果としてディレクトリ・サーバーの繰り返しリクエストになりますが、それらのリクエストは内蔵のRCSでローカルに取り扱われます。これにより、ほぼ瞬時に近い応答が出されることになるので、ユーザーが最小限度の遅延で操作を続けることが可能になります。

この構成オプションには、「無効にする」、「有効にする」、「タイムアウト」の3種類の設定が設けられています。

無効にする - ユーザーのキャッシュ保存を認めないで、常にLDAPディレクトリ・サーバーにすべてのユーザーついて、要求したときはいつも、認証状態についてガイダンスを求めます。デフォルトでは、ユーザーのキャッシュ保存は無効です。

有効にする - 最新のユーザー認証リクエストの結果をLDAPディレクトリ・サーバーによる決定に従って保持します。事前に決められた期間内に同一の認証結果を受けたときには、それらの以前の結果を使用して新規リクエストを処理します。

タイムアウト期間 - タイム・ウィンドウの期間を定めます。値は分単位で記録されます。ボックスの中には数字のみを入力するか、矢印コントロールを使用します。

- デフォルトのタイムアウト値: 15 分
- 最小タイムアウト: 1 分
- 最大タイムアウト: 1000 分

注: 構成を更新するすべての場合と同様に、*Save*をクリックして変更内容を安全に保存する必要があります。LDAP構成の変更内容は大概の場合、RCSで再起動の必要なしで、直ちに使用可能になります。

拡張オプションの入力 - Active Directory LDAP

Active Directoryモードを選択したら、管理者はStandardまたはExtendedスキーマを使用するかを決定する必要があります。さらに、管理者は、Microsoft Global Catalogのオプションを使用するかどうかも宣言する必要もあります。

認証パラメータの入力 - 標準LDAP

標準LDAP (Microsoft Active Directory LDAPでなく) を使用するときは、最低1つの該当するディレクトリ・サーバーのアドレスの直接エントリが必要になります。各アドレスをプライマリ・サーバーとセカンダリ・サーバーのフィールドに入力します。プライマリ・サーバーのエントリは必須です。

サーバー・アドレスは、次の形式のなかの1つで入力することができます。

- DNSアドレス (例、myldapserver.com)
- IPv4アドレス (例、10.20.255.255)
- IPv6アドレス (例、fe80::200:f8af:fe20:76ce)

認証パラメータの入力 - カスタムIPポート の割り当て

このセクションで、これまでLDAP用として使用されてきた業界標準のIPポート 番号への変更が許されます。大部分の例では、これらの値を変更する必要はありません。しかしながら、使用しているLDAPディレクトリ・サーバーの管理者が別のポート の割り当てを必要としている場合は、それらをここに入力することができます。

正確な構成によっても変わりますが、LDAPでは異なるIPポート を最高4つまで、また同時に2つまで使用することができます。これらの4つのそれぞれのスロット は、LDAP構成オプション画面に示されます。同一画面の他の設定は、変更が可能なポート を識別するのに使用されます。以下の表では、使用できるポート ・スロット を有効にして編集できる条件を定義しています。

表 5.1: IPポート の割り当ての編集

有効にして、カスタマイズできるポート ・スロット のリスト	オープン・モード	セキュア/SSLモード
グローバル・カタログを使用しない	標準LDAPメッセージ・ポート	標準LDAPメッセージ・ポート - セキュア/SSLモード
グローバル・カタログを使用する	標準LDAPメッセージ・ポート およびActive Directoryグローバル・カタログ・ポート	標準LDAPメッセージ・ポート - セキュア/SSLモード およびActive Directoryグローバル・カタログ・ポート - セキュア/SSLモード

元の業界標準のIPポート の送信先を復元する必要がある場合はいつでも、「 Restore Default Port Settings」ボタンをクリックしてください。4つのポート 値がすべて元の値に戻ります。それらは次のとおりです。

標準LDAPメッセージ・ポート - 389

標準LDAPメッセージ・ポート 、SSL経由 - 636

Active Directory、グローバル・カタログ・サーバー経由 - 3268

Active Directory、グローバル・カタログ・サーバー/SSL経由 - 3269

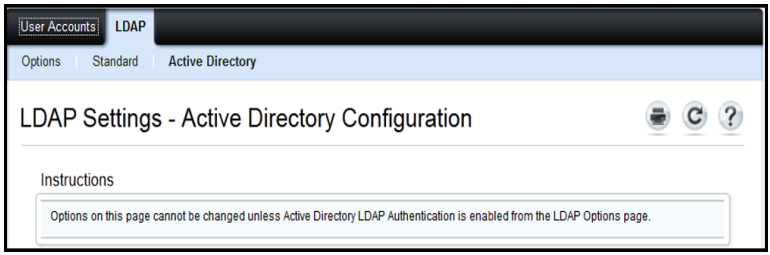
IPポート の番号は、1 ～ 65535の範囲が使用できます。 LDAPディレクトリ・サーバーによって使用されているポート 番号に一致しないと、当該サーバーとの通信が正しく確立できない結果となります。

LDAP構成の完了

標準とActive Directory LDAPモード の両方で、 LDAP Directory Serversへの適切な接続を確保するために追加のパラメータ ーが必要です。以下のセクションでそれぞれのパラメータ ーについて説明を加えます。しかしながら、パラメータ ーのアップデート が該当ページで作成されることを確実にし、管理者を支援するためにOBWIページに「インターロック」機能が設けてあることをご承知ください。

例えば、Active Directory LDAPタブを選択していて、画面に以下の表示が画面に示された場合は、図 5.4を参照してください。

図 5.4. 通知メッセージ - LDAPモード が有効になっていません



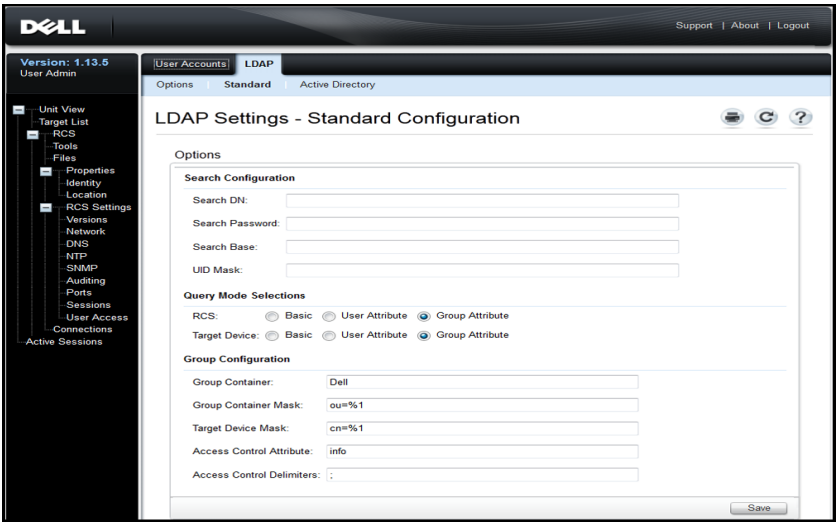
この場合は、Active Directoryモード が有効になっていないか、または有効になっていたけれども、保存されていないことを示しています。LDAP Options画面に戻り、*Active Directory LDAP*を選択して、当該するページでこのモード のセカンダリ・パラメータ ーをメモに記録してください。この画面に戻る前に、*Save*をクリックしてください。

標準LDAPモードでも、当該モードが有効になっていないときにいつも示される同様な表示があります。

セカンダリLDAP設定 - 標準構成

LDAP Active Directory構成の場合と同様に、標準LDAPの認証、検索、およびクエリ・パラメータはリモートOBWIを使用して構成されます。本セクションでの設定は、この図5.5に示されているOBWIウィンドウを介してUser Access / LDAP / Standardタブからアクセスできます。

図 5.5. セカンダリLDAP設定 -標準構成



注: このセクションでは、標準LDAP Directoryサーバーとの間でなされる接続のセットアップ・パラメータについて記述していますが、同時に、このセクションは、より汎用バージョンのActive Directoryサービスとの接続を確立するためにも使用できる点に注意を払ってください。

標準LDAPクエリ実行のためのRCSのセットアップ

注: クエリ・モードをActive Directoryで使用する前に、特定のクエリ・モードがユーザーに対する正しい承認レベルを割り当てられるよう、Active Directoryに変更を加える必要があります。

グループ・クエリをセットアップするには次の手順を実行します。

1 管理者特権で、使用のLDAP Directory Serverソフトウェアにログインします。

2 グループ・コンテナとして使用する組織単位(OU)を作成します。

3 アプライアンスのクエリ用のスイッチ・システム名と同一名、またはターゲット・デバイスのクエリ用の、接続されているターゲット・デバイス名と同一名のコンピューター・オブジェクトをActive Directory内に作成します。名前は、大文字/小文字の区別も含めて完全に一致していなければなりません。

4 グループ・クエリ用のアプライアンス名とターゲット・デバイス名は、アプライアンスに保存されています。リモートOBWIのAppliance Overview画面で指定したアプライアンス名とターゲット・デバイス名は、大文字、小文字、数字、ハイフンの任意の組み合わせからなり、LDAPサーバー上のオブジェクト名に一致していなければなりません。

5 グループ・コンテナの組織単位の下にグループ(1つまたは複数)を作成します。

6 ユーザー名、ターゲット・デバイス、アプライアンス・オブジェクトを手順4で作成したグループに加えます。

7 アクセス制御属性を実行する上で必要な各属性値を指定します。

検索構成の設定

正しいLDAP接続を行うために必要となる設定が4つあります。「検索DN」、「検索パスワード」、「検索ベース」、および「UIDマ

スク」です。

検索 DN

「検索DN」フィールドでは、ディレクトリ・サービスにログインする際にターゲット・デバイスが使用する管理者レベルのユーザーを定義できます。ターゲット・デバイスが認証されると、ディレクトリ・サービスによりディレクトリへのアクセスが許可され、「LDAPクエリ」ページで指定されたユーザー認証クエリが実行されます。検索DNに入力する個々の値は、カンマで区切る必要があります。代表的なエントリは次のようになります:

```
cn=Administrator,cn=Users,dc=MyDomainName,dc=com
```

検索パスワード

「検索パスワード」フィールドは、検索オプションでパスワードが必須の場合に使用されます。これにより、検索DNフィールドで指定した管理者またはユーザーを認証します。任意の印刷可能なASCII文字の使用ができます。

検索ベース

「検索ベース」フィールドでは、LDAP検索を開始する際の起点を定義します。デフォルト値は、dc=yourDomainNameおよびdc=comです。検索DNに入力する個々の値は、カンマで区切る必要があります。例えば、test.comでの検索ベースを定義するには、dc=test、dc=comと入力します。

UID マスク

「UIDマスク」フィールドでは、LDAPターゲット・デバイスでのユーザーID検索のための検索基準を指定します。形式は、<名前>=<%1>です。デフォルト値はsAMAccountName=%1です。これはActive Directoryと併用する場合の値となっています。

クエリ・モード

アプライアンスとターゲット・デバイス用のクエリ・モード・パラメータを構成します。アプライアンスは、管理者およびユーザーがコ

ンソール・スイッチにアクセスしようとしている場合に、管理者およびユーザーの認証に使用されます。ターゲット・デバイスは、接続されているターゲット・デバイスにユーザーがアクセスしようとしている場合に、そのユーザーの認証に使用されます。

使用できるクエリ・モードは、基本、ユーザー属性、グループ属性の3種類です。

基本

ユーザーのユーザー名とパスワードに関するクエリがディレクトリ・サービスに送信されます。有効なユーザーとして認証されると、ユーザーには、アプライアンスと接続されている任意のターゲット・デバイスへのアクセスが与えられます。

ユーザー属性

ユーザーのユーザー名、パスワード、アクセス制御属性に関するクエリがディレクトリ・サービスに送信されます。アクセス制御属性はActive Directory内のユーザー・オブジェクトから読み込まれます。値が見つからない場合は、ユーザーにアプライアンスまたはターゲットへのアクセス権は与えられません。

グループ属性

ユーザー名、パスワード、グループ・クエリは、クエリ・モード（アプライアンス）時はアプライアンスと接続のターゲット・デバイスに関して、クエリ・モード（デバイス）時には特定のターゲット・デバイスに関してディレクトリ・サービスに送信されます。クエリ・モード（アプライアンス）時の場合、該当ユーザーとアプライアンス名を含むグループが検索されると、グループ・コンテンツの内容に従って、アプライアンスまたは接続されているターゲット・デバイスへのユーザー・アクセスがユーザーに与えられます。クエリ・モード（ターゲット・デバイス）の場合、該当ユーザーとターゲット・デバイスIDを含むグループが検索されると、アプライアンスに接続されている特定ターゲット・デバイスへのユーザー・アクセスがユーザーに与えられます。

注: 選択したクエリ・モードによって異なりますが、この画面で示された構成項目の一部がそれぞれ適用できるかどうかによって有効または無効になります。

グループ構成パラメータ

以下のいくつかのグループ構成パラメータが使用できます。

グループ・コンテナ

グループ・コンテナでは、管理者がActive Directory内にグループ・オブジェクト用位置として作成したOU(組織ユニット)を指定します。グループ・オブジェクトには、ユーザー、コンピューター、連絡先、他のグループなどに特定のアクセス・レベルの割り当て付きで含めることができます。

グループ・コンテナ・マスク

グループ・コンテナ・マスクでは、グループ・コンテナのオブジェクト・タイプ、通常、OUを定義します。デフォルト値は「ou=%1」です。

ターゲット・デバイス・マスク

ターゲット・デバイス・マスクではターゲット・デバイスの検索フィルターを定義します。デフォルト値は「cn=%1」です。

アクセス制御属性

アクセス制御属性では、クエリ・モードが「ユーザー属性」または「グループ属性」に設定されている場合に使用する属性名を指定します。デフォルト値は「**info**」です。

アクセス制御区切り文字

LDAP標準では、セミコロン(;)を単一名の属性内にある複数のプロパティの区切り文字として使用するように指定します。通常の操作では、これを変更する必要はありません。例えば、LDAP Directoryに速乾タイプのボードマーカー・オブジェクトがあると想定した場合に、属性「Color」を用いてこのマーカーが持つ色を識別できます。

Color: red;blue;green;black;purple

「Color」が属性の名前で、残りはこの属性の値となり、この場合は複合値を表します。複合値では、1つの要素の終わりと次の要素の始まりを示めすのに、セミコロンを区切り文字として使用します。

稀ですが、LDAP管理者が、値そのものの一部としてセミコロンを必要とする場合があります。そのときは、区切り文字を別のものに変更する必要があります。該当する場合は、このフィールドを使用して、アクセス制御属性の区切り方法を識別する文字のすべてを指定します(最低1つの文字が必要でが、2つ以上でも構いません)。例、区切り文字フィールドで次のように設定します: **#$;**(3文字)

Color: red#blue$green;black#purple

これらの区切り文字で、上記の最初に示した5つ同じ値要素が検索されます。LDAP管理者は、定義されたアクセス制御の区切り文字が、区切りの目的以外で属性の文字として他で一切使用されていないことを確認する必要があります。

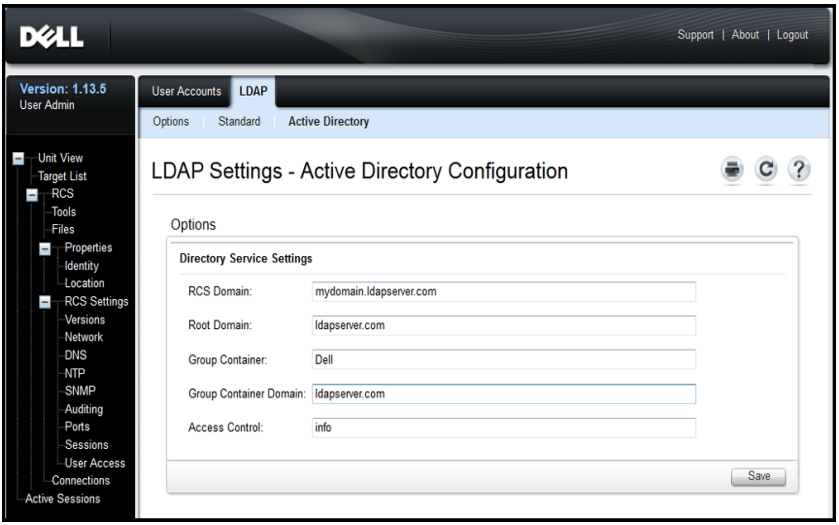
上に示すように、アクセス制御属性(ACA)は名前と値の組み合わせからなりたっています。デフォルトでは、ユーザーとターゲット・デバイスに一致するLDAP Directoryエントリを、「info」と名付けられた属性で検索します。見つかったときは、該当する属性の値により、そのデバイスでのユーザーの認証レベルが知らされることになります。LDAPサービスの管理者が「info」以外の属性を使用したい場合は、上に示したフィールドを使ってカスタマイズすることができます。

ユーザーがいくつかのグループのメンバーであり、各グループが異なるデバイスに対して異なる認証レベルを有しているため、結果についての集計の実行が保管されます。LDAP標準では、報告された最終の認証レベルが、セキュリティの下での特定のユーザーとデバイス用として検索された該当するすべての結果のなかで見つけられる最高(最も高い許可)レベルです。

セカンダリ LDAP設定 - Active Directory構成

本セクションでの設定は、このに示されているOBWIウィンドウを介してUser Access / LDAP / Standardタブからアクセスできます。

図 5.6. セカンダリ LDAP設定 - Active Directory構成



Dell Extended Schemaをインストールする場合は、使用するRCSとルート･ドメインのみを入力します。

Dell Extended Schemaを使用しない場合、設置されているRCSとアクセス制御されているSIPは、Active Directory内でコンピューター･オブジェクトとして構成されます。これを行うには、アクセス制御されたRCSおよび接続されているSIPにユーザーを関連付けるグループ･オブジェクトを格納する組織単位を構成する必要があります。これは以前に作成したOUでも、特にこの目的のために作成したOUでも構いませんが、グループ･コンテナ･ドメイン内のすべてのOUオブジェクトで一意である必要があります。

次に、任意アクセス制御情報を含むために使用される、LDAPディレクトリ内の属性を選択します。これは、文字列の値を格納できる

未使用の属性である必要があります。(デフォルトはグループ・オブジェクトの「 info」属性。)

最後に、 OBWI ウィンドウの空欄に、グループ・コンテナの場所、グループ・コンテナ・ドメイン、アクセス制御属性を入力する必要があります。

図 5.6に示す各フィールドの詳細については、表 5.2を参照してください。

表 5.2: Active Directory構成フィールドの説明

フィールド	説明
RCS Domain	RCS Domainフィールドには、RCSと SIPを表すすべてのオブジェクトの格納に選択されたActive Directoryドメインの名前が入ります。
Root Domain	Active Directoryフォレスト内の最上部のドメイン。
Group Container (Standard スキーマ・セットのみ)	このフィールドは、Standardスキーマが選択されているときに使用でき、組織単位(OU) オブジェクトの識別名の一部を含みます。OUは、アクセス制御されたRemote Console Switchおよび接続されたSIPにユーザーを関連付けるグループ・オブジェクトを格納するために使用されます。 たとえば、選択されたOUの識別名がou=KVM-AccessControls, dc=MyCom,dc=comだとします。この場合、Group Containerフィールドは「 KVM-AccessControls」に設定してください。Group Containerフィールドに入力する名前は、Group Containerドメイン内のすべてのOUオブジェクトのなかで固有でなければなりません。 以前にそのGroup Containerに作成したOUでも、特にこの目的のために作成したOUでも使用できます。 デフォルトのGroup Containerは、KVMです。

フィールド	説明
Group Container Domain (Standard スキーマ・セットのみ対象)	このフィールドは、グループ・コンテナが配置されているActive Directoryドメインの DNS名で、Standardスキーマが選択されているときに使用できます。
Access Control Attribute (Standard スキーマ・セットのみ対象)	このフィールドの値は、LDAPディレクトリ内のどの属性が任意アクセス制御情報の格納に使用されるかを指定し、Standardスキーマが選択されているときにのみ有効になります。 Access Control Attributeは、LDAPディレクトリ・オブジェクト内の属性から選択されます。この属性は、ユーザーおよびアクセスしようとしているRCSまたは接続されたコンピュータの両方がメンバーシップに含まれるグループを表します。 Standardスキーマを使用している場合、グループ・コンテナ内のグループ・オブジェクトが持つ属性は、そのグループと関連付けられた許可レベルを含むように選択されている必要があります。Access Control Attributeフィールドは、Standardスキーマが選択されているときに使用でき、選択された属性の名前を含みます。選択された属性は、文字列値を格納できる必要があります。たとえば、デフォルト属性は「info」属性で、Active Directory ユーザーとコンピュータ(ADUC)のスナップインからアクセス可能です。ADUCを使用し、グループ・オブジェクトの「Notes」プロパティにアクセスすることによって、info属性の値が設定されます。

LDAP SSL証明書

すべてのLDAPプロトコル交換(RCSとActive Directoryサーバー間) は、SSLによってセキュリティ保護されています。LDAPプロトコルがSSLで保護されているときは、LDAPS(Lightweight Directory Access Protocol over SSL) と呼ばれます。各LDAPS接続はプロトコル・ハンドシェイクで始まり、それにより、応答側のActive Directoryサーバーからの RCSにセキュリティ証明書が転送されます。証明書が受信されると、RCSによって証明書が確認されます。証明書を確認するには、RCSにルート証明機関(CA) 証明書のコピーを構成する必要があります。これを行うには、まず、証明書を作成する必要があります。

ドメイン・コントローラー上のSSLの有効

Microsoftエンタプライズのルート CAを使用してすべてのドメイン・コントローラーSSL証明書を自動的に割り当てる場合、各ドメイン・コントローラー上のSSLが有効になっていなければ、以下の手順を行って有効にする必要があります。

1 Microsoftエンタプライズのルート CAをドメイン・コントローラーにインストールします。

   a. **スタート → コントロール パネル → プログラムの追加と削除**を選択します。

   b. **Windowsコンポーネント の追加と削除**を選択します。

   c. Windows コンポーネント ウィザードで、**証明書サービス** チェックボックスをオンにします。

   d. [CAの種類]として**Enterprise root CA**を選択して、**Next**をクリックします。

   e. このCAに[共通名]を入力し、**Enterprise root CA**をクリックして、**Finish**をクリックします。

2 ドメイン・コントローラのそれぞれにSSL証明書をインストールすることによって、各コントローラでSSLを有効にします。

a. **スタート → 管理ツール → ドメイン セキュリティ ポリシー**をクリックします。

b. 公開キーのポリシー・フォルダを拡張して、**自動証明書要求の設定**を右クリックし、**自動証明書要求**をクリックします。

c. 自動証明書要求セットアップ ウィザードで、**Next**をクリックし、**Domain Controller**を選択します。

3 **Next**をクリックし、**Finish**をクリックします。

Linux環境では、openssを使用して証明書／秘密鍵ファイルを作成できます。Openssは openssl.orgからダウンロードできます。<>で囲まれたテキスト付きの手順説明は、ユーザーが条件に基づいてその行の最後に設定する必要がある箇所を示しています。

注: <>で囲まれたテキスト付きの手順説明は、ユーザーが条件に基づいてその行の最後に設定する必要がある箇所を示しています。

インポートする証明書を作成するには:

1 Linuxのコマンド・プロンプトで、**openssl**openと入力し、Enterキーを押します。OpenSSLプロンプトに切り替わります。

```
OpenSSL> genrsa -out privatekey.pem <512>
Generating RSA private key, 512 bit long modulus
.....+++++++++++++
.....+++++++++++++
e is 65537 (0x10001)
OpenSSL req -new -key privatekey.pem -x509 -out certificate.pem-batch
-days 365
```

2 識別名(DN) には、証明書要求に組み込まれる情報を入力します。一部のフィールドにはデフォルト値があります。必要に応

じて'.'と入力することで、フィールドを空欄のまま残すことができます。

```
-----
国名(2文字の略称) [GB]:<US>
都道府県名(正式表記) [Berkshire]:<Texas>
市町村名(市など) [Newbury]:<Austin>
組織名(会社名など) [My Company Ltd]:<Dell, Inc.>
組織単位名(部など) []:Round Rock<Round Rock>
一般名(自分の名前、サーバーのホスト名など) []:<RCS
DNS名またはIP>
Email Address []:<support@dell.com>
OpenSSL> quit
```

3 Linuxのコマンド・プロンプトに**cat certificate.pem privatekey.pem > webserver.pem**と入力し、さらに**unix2dos webserver.pem**と入力してファイルの改行タイプをUNIXからDOSに変換します。

CA証明書をエクスポートするには次の手順を実行します。

1 Windowsオペレーティング・システムで証明機関管理ツールを開くには、**スタート → すべてのプログラム → 管理ツール → 証明機関**の順にクリックします。

2 ツリー表示で証明機関を右クリックして**プロパティ**を選択することで、証明機関のプロパティを表示できます。[CAプロパティ]ダイアログ・ボックスが開きます。

3 **全般**タブと**証明書の表示**ボタンをクリックして、[証明書]ダイアログ・ボックスを開きます。

4 **詳細**タブをクリックし、**次に**ファイルにコピーボタンをクリックします。証明書のエクスポート・ウィザードが開きます。

5 **次へ**をクリックして、ウィザードの使用を開始します。

6 [エクスポート ファイルの形式]画面で、Base-64 encoded X.509 (.CER)オプション・ボタンを選択し、**次へ**ボタンを押します。

7 **エクスポートするファイル**画面で、ファイル名とエクスポートされる証明書のパスを入力または参照します。**次へ**ボタンを押します。

8 **完了**ボタンを押します。

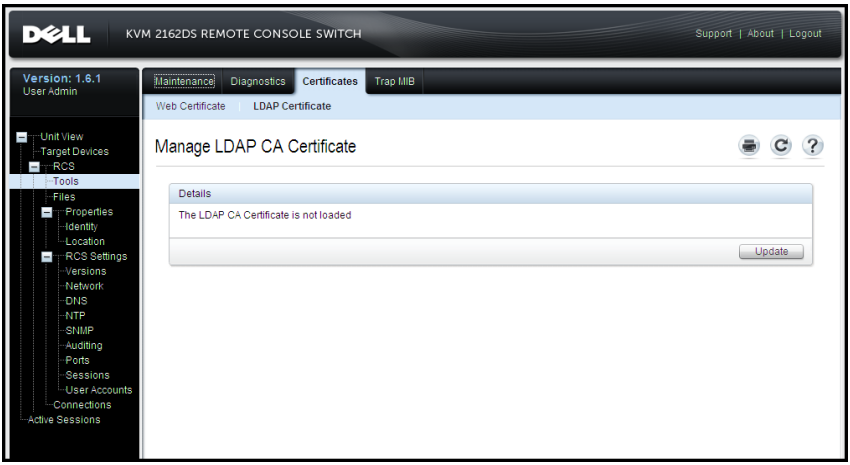
この結果作成された証明書ファイルは正しい形式で、OpenSSLで読み取り可能です。

一般に、CA証明書は一度だけアップロードする必要がありますが、証明書が失効されていたり期限切れの場合、またはシリアル・コンソール・メニューから「Restore Factory Defaults」が選択されている場合は、再度アップロードする必要があります。

注：上記の説明は、Microsoft Root CA証明書に関して書かれています。他のCAについては、CAベンダーにお問い合わせください。

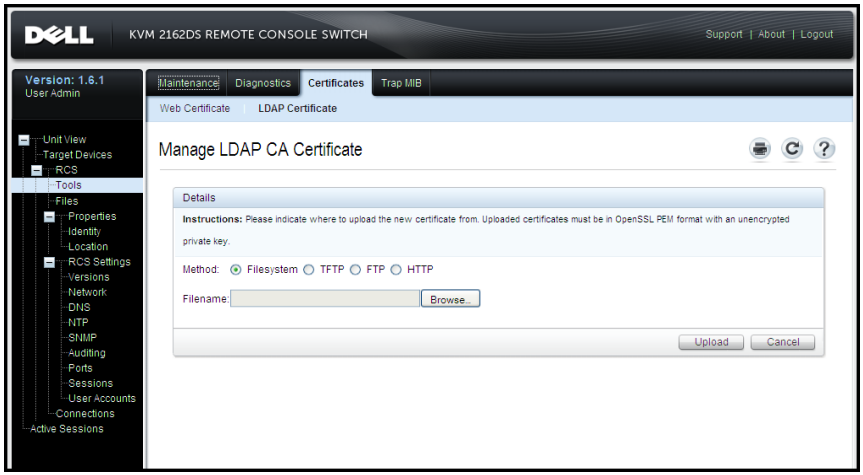
注：LDAPSが機能できるように、NTP(Network Time Protocol)が有効になっている必要があります。

図 5.7. OBWI - LDAP証明書



Updateをクリックしたら、次のウィンドウが表示されます。

図 5.8. OBWI - LDAP証明書の更新



証明書ファイルは、参照ダイアログ・ボックスで選択して開くことができます。証明書が開かれ、その内容が表示されたら、証明書をRCSに送信できます。

ログイン・タイムアウト

ディレクトリ・ツリーのサイズが大きいためにLDAP認証に時間がかかる場合に備え、Sessionsウィンドウには Login Timeoutの設定ボックスがあります。デフォルトのタイムアウトは30秒に設定されています。ログイン・タイムアウトは、Loginダイアログ・ボックスでユーザーがOKボタンを押した時点から、最終的にRCSが応答していないと判定されるまでの時間です。RCSはこの値を使用して、認証に関するLDAP要求のタイムアウトを決定します。

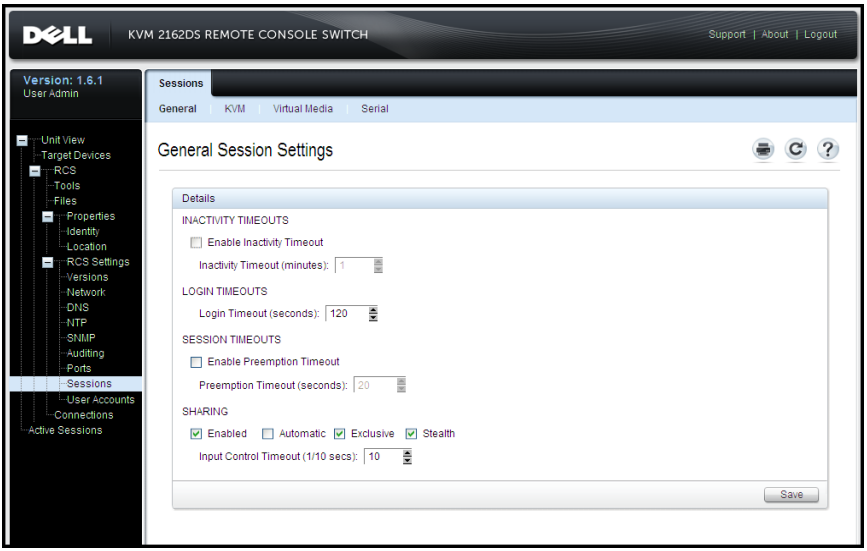
OBWIでログイン・タイムアウトを指定するには次の手順を実行します。

1 Sessionsをクリックして、General Session Settings画面を開きます。

2 Login Timeoutメニューでタイムアウトの長さ(秒単位)を指定します。

3 Saveをクリックします。

図 5.9. OBWI - ログイン・タイムアウト



注: ログイン・タイムアウトは、ユーザー・ログイン・キャッシュ保存機能とは別のものです。後者は、ログイン後に機能し、認証結果を一定の期間キャッシュ保存し、繰り返しのLDAP通信リクエストを解消して、完了します。

CA証明書情報の表示

RCSでは、公開キーの長さが2048ビット以下の場合にのみ、このウィンドウに完全なCA証明書情報を表示できます。キーの長さが2048ビットを超える場合、サブジェクト、発行者、有効期間のデータはこのウィンドウに完全には表示されなくなります。[1]

下記はCA証明書情報の例です:

1 クライアントからRCSにCA証明書をダウンロードします。

2 シリアル・コンソールのメイン・メニューで**オプション**8を指定し、LDAP CA証明書を表示します。

RCSには次のタイプの情報が表示されます:

Begin CA certificate information display
subject= /DC=msft/DC=ldaptest/CN=MyCertificate
issuer= /DC=msft/DC=ldaptest/CN=MyCertificate
notBefore=Dec 7 20:0956 2005 GMT
notAfter=Dec 7 20:1834 2010 GMT
serial=7BA146C0221A08B447B989292074329F
MD5 Fingerprint=6D:70:30:31E5:1B:C0:90:BB:DB:32:B2:C9:D15A
End CA certificate information display

Microsoft Windows Server 2003プラットフォームにRCSソフトウェアをインストールできるようにするには、次の手順を実行します。

1 **スタート**メニューを選択
2 **マイ コンピュータ**を右クリックし、**プロパティ**を選択します。
3 **詳細設定**タブを選択
4 **パフォーマンス**ボタンをクリック
5 **データ実行防止**タブを選択
6 **重要なWindowsプログラムおよびサービスについてのみ有効にする**のオプション・ボタンを選択します。
7 OKをクリックします。
8 「システムのプロパティ」ダイアログ・ボックスでOKをもう一度クリックします。

グループ・オブジェクトの構成

Group Container内のグループのメンバーシップにユーザーを含めることで、アクセス制御が特定のActive Directoryユーザー・アカウントに適用されます。グループのメンバーシップには、ユーザーにアクセスを許可するRCSとSIPを表すオブジェクトも含める必要があります。許可されるアクセスのレベルは、グループ・オブジェクト

(Standardスキーマ) またはAssociationオブジェクト(Extendedスキーマ) 内の特定の属性の値によって決定されます。3種類の許可レベルがあり、これらは、アクセス権が増える順に「 KVM User」、「 KVM User Admin」、および最も強力なレベルの「 KVM Appliance Admin」となっています。

注: KVM Userのアクセス・レベルが使用されていない場合は、両方の管理者アクセス権はデフォルト ですべてのSIPにアクセスできるため、SIPオブジェクトを構成する必要はありません。

表 5.3: アクセス・レベルによって許可される操作

操作	KVM Appliance Admin	KVM User Admin	KVM User
プリエンプト	別のKVM Appliance AdminまたはKVM User Adminをプリエンプトできます。Directory内の適切なグループ・オブジェクトにTDを含めることにより、ターゲット・デバイスごとに許可を構成する必要があります。	別のUser Adminをプリエンプト できます。Directory内の適切なグループ・オブジェクトにターゲット・デバイスを含めることにより、ターゲット・デバイスごとに許可を構成する必要があります。	不可
ネットワーク・パラメーターとグローバル設定の構成	可 - Directory内の適切なGroupオブジェクトにRCSを含めることにより、RCSごとにアクセス権を構成する必要があります。	不可	不可

操作	KVM Appliance Admin	KVM User Admin	KVM User
再起動	可 - Directory内の適切なGroupオブジェクトにRCSを含めることにより、RCSごとにアクセス権を構成する必要があります。	不可	不可
フラッシュ・アップグレード	可 - Directory内の適切なGroupオブジェクトにRCSを含めることにより、RCSごとにアクセス権を構成する必要があります。	不可	不可
ユーザー・アカウントの管理	可 - Directory内の適切なGroupオブジェクトにRCSを含めることにより、RCSごとにアクセス権を構成する必要があります。	可 - Directory内の適切なGroupオブジェクトにRCSを含めることにより、RCSごとにアクセス権を構成する必要があります。	不可
ポート設定の構成	可 - Directory内の適切なGroupオブジェクトにRCSを含めることにより、RCSごとにアクセス権を構成する必要があります。	不可	不可

操作	KVM Appliance Admin	KVM User Admin	KVM User
ターゲット・デバイスへのアクセス	可 - Directory内の適切なGroupオブジェクトにRCSを含めることにより、RCSごとにアクセス権を構成する必要があります。	可 - Directory内の適切なGroupオブジェクトにRCSを含めることにより、RCSごとにアクセス権を構成する必要があります。	可(管理者として構成されている場合) Directory内の適切なグループ・オブジェクトにTDを含めることにより、ターゲット・デバイスごとに許可を構成する必要があります。

RCS管理者アクセス権でのAuthenticationパネルのフィールド変更を許可する前に、RCS管理者(KVM Appliance Admin) アクセス権を受信するようにADユーザー・アカウントを構成する必要があります。特に、Authentication Settingsを変更できるのは、RCS管理者のみです。

標準スキーマのActive Directoryオブジェクトの概要

認証および承認のためにネットワーク上の物理RCSをActive Directoryに統合する場合、各物理RCSを表すコンピューター・オブジェクトを少なくとも1つ作成する必要があります。また、KVM User特権レベルを使用して制御されるRCSに接続されているSIPごとに、コンピューター・オブジェクトを作成する必要があります。SIPを表現するコンピューター・オブジェクトは、管理者レベルのグループには必要ありません。KVM Userグループのユーザーは、KVM Userグループ内にあるSIPにのみアクセスできます。管理者特権を持つユーザーは、デフォルトにより、すべてのSIPにアクセスできます。

RCSのGroupオブジェクトをセットアップするには次の手順を実行します。

1 インストールされたスイッチに関連したグループ・オブジェクトを含む組織単位がまだ作成されていない場合は、作成します。

2 この組織単位内に、ユーザー特権レベルを表すグループ・オブジェクトを3つ作成します。KVM Appliance Administrator、KVM User Administrator、およびKVM Userのそれぞれに1つずつ作成してください。

3 MSADUCツールを使用して、KVM Appliance Administrator Group オブジェクトを開き、Notesプロパティを選択します。Notesフィールドに、そのグループのアクセス・レベル(「KVM Appliance Admin」)を入力して保存します。ほかの2つのグループ・オブジェクトについても、それぞれの名前を使用して、この手順を繰り返します。

注: すべてのアクセス制御の属性の値に、次の単一の構文を使用します。

"[<属性文字列> <区切り文字>] <特権レベル> [<区切り文字> <任意の文字列>]"

ここで、<特権レベル> : =「KVM User」または「KVM User Admin」または「KVM Appliance Admin」

<区切り文字> ::区切り文字 := 以下のうちの1つまたは複数:「改行」、「c/r」、「コンマ」、「セミコロン」、「タブ」のいずれかです(複数可)。

<任意の文字列>は、任意の英数文字列で、Null(空の)文字列にすることも可能です。

角かっこは、オプションのアイテムを示します。たとえば、次のテンプレートは、オプションの文字列と区切り文字と、それに続く必要な特権レベルを示しています。"[<任意の文字列> <区切り文字>] < 特権レベル1>"

4 RCSを表すコンピューター・オブジェクトを作成します。

5 KVM User特権レベルでアクセス制限されるサーバーに接続されている各SIPごとに、コンピューター・オブジェクトを作成します。

6 スイッチを表すコンピューター・オブジェクトを適切なグループ・オブジェクトに追加します。

7 ユーザー・オブジェクトを、アクセス・レベルに応じて適切なグループ・オブジェクトに追加します。

8 アクセス制御されたSIPのコンピューター・オブジェクトをKVM User Groupに追加します。

Dell Extended SchemaのActive Directoryオブジェクトの概要

認証と承認のためにActive Directoryと統合する、ネットワーク上にあるそれぞれの物理RCSには、物理スイッチを表す少なくとも1つのRCSデバイス・オブジェクトと1つのAssociationオブジェクトを作成する必要があります。Associationオブジェクトは、ユーザーまたはグループを、1つ以上のSIPに対する特権の特定のセットとリンクするために使用されます。このモデルを使用することにより、管理者は設定を複雑にし過ぎることなく、ユーザー、RCS特権、およびRemote Console Switch上のSIPのさまざまな組み合わせを、最大限柔軟に活用できます。

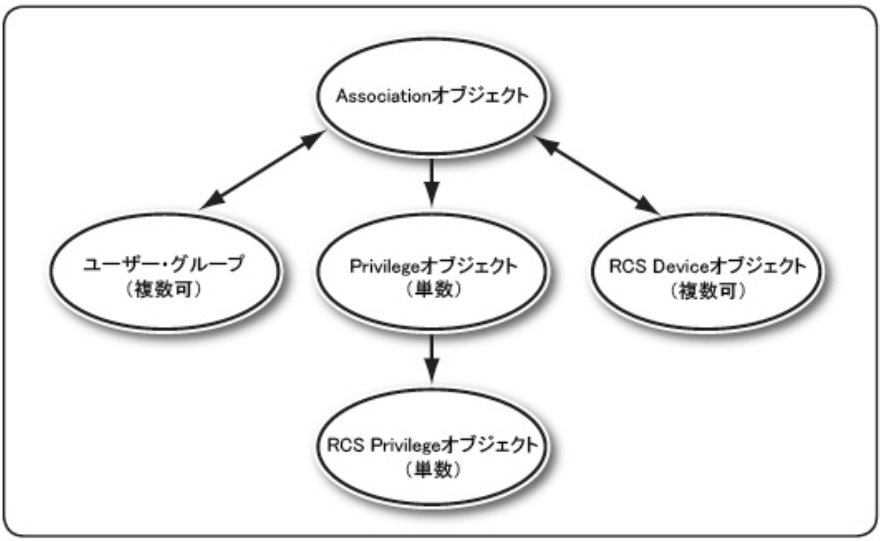
RCSデバイス・オブジェクトが、認証と承認のためにActive Directoryをクエリするための RCSへのリンクです。RCSをネットワークに追加したら、管理者はActive Directory名でRCSとそのデバイス・オブジェクトを構成し、ユーザーがActive Directoryで認証と承認を行えるようにする必要があります。ユーザーが認証できるように、管理者は少なくとも1つのAssociationオブジェクトにもRemote Console Switchを追加する必要があります。

Associationオブジェクトはいくつでも作成でき、各Associationオブジェクトは無限数のユーザー、ユーザーのグループ、RCS Deviceオブジェクトにリンクできます。ユーザーとRCS Deviceオブジェクトは、エンタプライズ内のどのドメインのメンバーであっても構いません。

ただし、各Associationオブジェクトは、(ユーザー、ユーザーのグループ、またはRCS Deviceオブジェクトを) 1つのPrivilegeオブジェクトにのみリンクできます。Privilegeオブジェクトにより、管理者は、どのユーザーが特定のSIPに関してどの種類の特権を持っているかをコントロールできます。

次の図では、Associationオブジェクトが、すべての認証と承認に必要な接続を提供する様子を示します。

図 5.10. Active Directoryオブジェクトの一般的なセットアップ



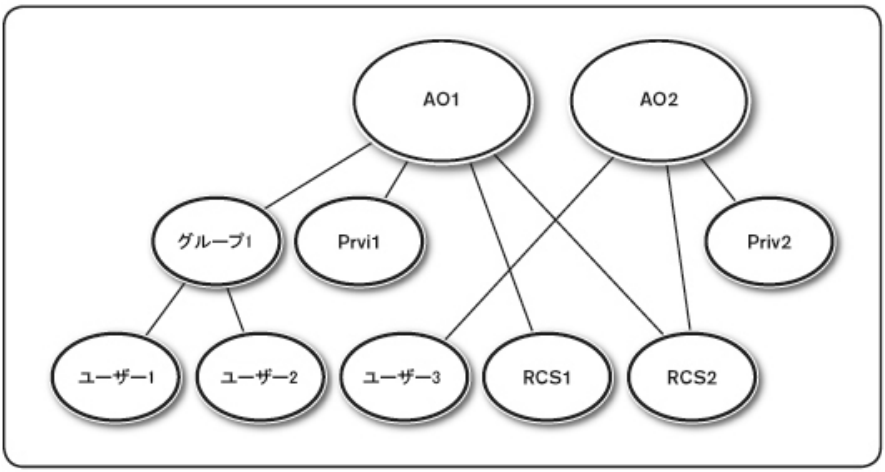
希望や必要に応じて、多数または少数のAssociationオブジェクトを作成できます。ただし、少なくとも1つのAssociationオブジェクトを作成する必要があり、また、認証と承認のためにActive Directoryと統合するネットワーク上にある、それぞれのRCSに対して1つのRCSデバイス・オブジェクトを持っている必要があります。Associationオブジェクトは、RCS Deviceオブジェクトのほかに、必要に応じて多数または少数のユーザーまたはグループ、あるいはその両方を持つことができます。ただし、Associationオブジェクト1つにつき、1つのPrivilegeオブジェクトしか持てません。Associationオブジェクトは、RCSで特権を持つユーザーを接続します。

さらに、単一ドメインまたは複数ドメインでActive Directoryオブジェクトをセットアップできます。たとえば、2つのRCS（RCS1とRCS2）があり、3人の既存Active Directoryユーザー

(User1、User2、User3) がいるとします。User1とUser2に両方のRCSの管理者特権を与え、User3にRCS2へのログイン特権を与えるとします。

次の図に、このシナリオでのActive Directoryオブジェクトのセットアップ方法を示します。

図 5.11. 単一ドメインでのActive Directoryオブジェクトの設定



単一ドメインのシナリオの場合にActive Directoryオブジェクトを設定するには、以下の作業を行います。

1 2つのAssociationオブジェクトを作成します。

2 2つのRCSを表すために、RCS1とRCS2という2つのRCSデバイス・オブジェクトを作成します。

3 Priv1とPriv2という2つのPrivilegeオブジェクトを作成し、Priv1はすべての特権(管理者) を持ち、Priv2はログイン特権を持つようにします。

4 User1とUser2をGroup1にグループ化します。

5 Group1をメンバーとしてAssociationオブジェクト 1(AO1) に、Priv1をPrivilegeオブジェクトとしてAO1に、RCS1とRCS2をRCS Deviceとしてao1に追加します。

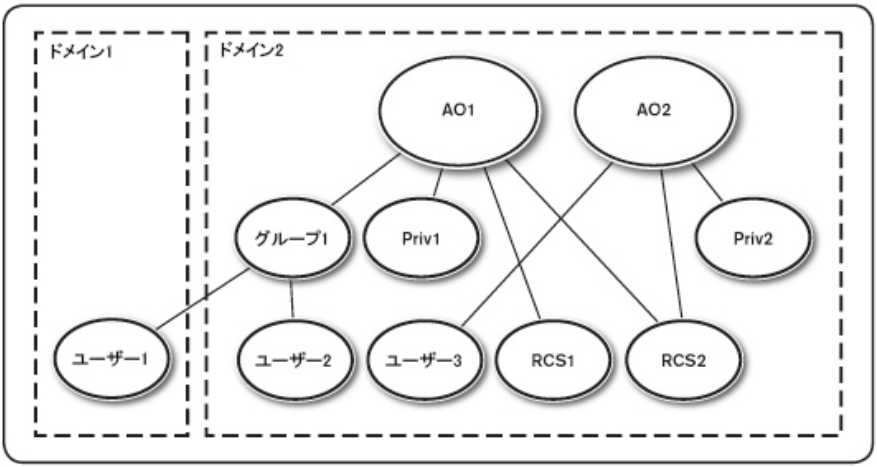
6 User3をメンバーとしてAssociationオブジェクト 2(AO2) に、Priv2をPrivilegeオブジェクトとしてAO2に、RCS2をRCSデバイスとしてAO2に追加します。

詳細な手順については、「 Dell Schema Extensionを使用するActive Directoryへのユーザーと特権の追加」を参照してください。

次の図に、複数ドメインでのActive Directoryオブジェクトのセットアップ方法を示します。このシナリオでは、2つのRCS(RCS1とRCS2) があり、3人の既存Active Directoryユーザー(User1、User2、User3) がいるとします。

User1はDomain1に、User2とUser3はDomain2に属します。User1とUser2に両方のRCSの管理者特権を与え、User3にRCS2へのログイン特権を与えるとします。

図 5.12. 複数ドメインでのActive Directoryオブジェクトの設定



複数ドメインのシナリオの場合にActive Directoryオブジェクトを設定するには、以下の作業を行います。

1 ドメイン・フォレスト機能は、必ずネイティブまたはWindows 2003モードにします。

2 任意のドメインにAO1(ユニバーサル・スコープ)とAO2という2つのAssociationオブジェクトを作成します。図は、Domain2内のオブジェクトを示しています。

3 2つのRCSを表すために、RCS1とRCS2という2つのRCSデバイス・オブジェクトを作成します。

4 Priv1とPriv2という2つのPrivilegeオブジェクトを作成し、Priv1はすべての特権(管理者)を持ち、Priv2はログイン特権を持つようにします。

5 User1とUser2をGroup1にグループ化します。Group1のグループ・スコープは、ユニバーサルである必要があります。

6 Group1をメンバーとしてAssociationオブジェクト1(AO1)に、Priv1をPrivilegeオブジェクトとしてAO1に、RCS1とRCS2をRCS DeviceとしてAO1に追加します。

7 User3をメンバーとしてAssociationオブジェクト2(AO2)に、Priv2をPrivilegeオブジェクトとしてAO2に、RCS2をRCSデバイスとしてAO2に追加します。

RCSアクセスのためのDell Schema Extensionを使用したActive Directoryの構成

Active Directoryを使用してRCSにアクセスできるようにするには、次の手順を番号順に実行して、Active Directoryソフトウェアと Remote Console Switchを構成する必要があります。

1 Active Directoryスキーマを拡張します。

2 Active Directoryユーザーとコンピューター・スナップインを拡張します。

3 RCSユーザーと特権をActive Directoryに追加します。

Active Directoryスキーマの拡張(オプション)

Active Directoryスキーマを拡張すると、Dellの組織単位、スキーマ・クラスと属性、および特権の例とAssociationオブジェクトが、Active Directoryスキーマに追加されます。

注: スキーマを拡張するには、ドメイン・フォレストのスキーマ・マスタ・フレキシブル・シングル・マスタ操作(FSMO)の役割所有者に関して、スキーマ管理者の特権を持っている必要があります。

スキーマは、2つの異なる方法で拡張できます。Dell Schema Extenderユーティリティを使用するか、またはLDIFスクリプト・ファイルを使用できます。

注: LDIFスクリプト・ファイルを使用する場合は、Dellの組織単位は追加されません。

LDIFファイルとDell Schema Extenderは、dell.com/supportより入手できます。

LDIFファイルを使用する場合は、LDIFファイル・ディレクトリのreadmeファイルの説明を参照してください。Dell Schema Extenderを使用してActive Directoryスキーマを拡張するには、「Dell Schema Extenderの使用」の手順を実行してください。

Schema ExtenderまたはLDIFファイルは、任意の場所にコピーして実行できます。

Dell Schema Extenderの使用

注: Dell Schema ExtenderはSchemaExtenderOem.iniファイルを使用します。Dell Schema Extenderユーティリティが確実に正常な機能を果たすようにするために、このファイルの名前を変更しないでください。

1 Welcome画面でNextをクリックします。

2 警告文を読んで、もう一度Nextをクリックします。

3 Use Current Log In Credentialsをオンにするか、またはスキーマ管理者アクセス権を持つユーザー名とパスワードを入力します。

4 Nextをクリックして Dell Schema Extenderを実行します。

5 Finishをクリックします。

Active Directoryユーザーとコンピュータ ー・スナップインへのDell Extensionのインスト ール(オプション)

Active Directoryでスキーマを拡張する場合、管理者がRCSデバイス、ユーザー、ユーザー・グループ、RCS関連付け、SIP特権を管理できるように、Active Directoryユーザーとコンピュータ ーのスナップインも拡張する必要があります。Active Directoryユーザーとコンピュータ ー・スナップインへのDell Extensionのインスト ールは、「 Dell Systems Management Consoles CD」を使用してシステム管理ソフト ウェアをインスト ールするときに行うことができるオプションです。システム管理ソフト ウェアのインスト ールの詳細については、『 Dell OpenManage Software Quick Installation Guide』を参照してください。

注: Active DirectoryのRCSオブジェクトを管理している各システムに、管理パックをインスト ールする必要があります。インスト ールの手順については、後続の「 Active Directoryユーザーとコンピュータ ー・スナップインを開く」のセクションを参照してください。コンテナに含まれている Dell SIP オブジェクト は、Administrator Packをインスト ールしなければ参照できません。

注: Active Directoryユーザーとコンピュータ ー・スナップの詳細については、Microsoft のマニュアルを参照してください。

Active Directoryユーザーとコンピュータ ー・スナップインを開く

Active Directoryユーザーとコンピュータ ー・スナップインを開くには、以下の手順を行います。

ドメイン・コント ロ ーラ ー上で操作している場合は、**スタート → 管理ツール → Active Directoryユーザーとコンピュータ ー**をクリックします。

-または-

ドメイン・コント ロ ーラ上で操作していない場合は、ローカル・システムに適切なMicrosoft Administrator Packがインスト ールされている必

要があります。この管理パックをインストールするには、**スタート → ファイル名を指定して実行**をクリックし、「MMC」と入力して、Enterキーを押します。この操作で、Microsoft Management Console (MMC) が開かれます。

1 [コンソール1]ウィンドウで**ファイル**(または、Windows 2000を実行しているシステムでは、[コンソール]) をクリックします。

2 **スナップインの追加と削除**をクリックします。

3 **Active Directoryユーザーとコンピュータのスナップイン**を選択して、**追加**をクリックします。

4 **閉じる**をクリックして、**OK**をクリックします。

Dell Schema Extensionを使用するActive Directoryへのユーザーと特権の追加

Dell拡張Active Directoryユーザーとコンピュータのスナップインでは、SIP、Association、およびPrivilegeの各オブジェクトを作成することで、RCSのユーザーと特権を追加できます。オブジェクトのそれぞれの種類を追加するには、それぞれの項の手順に行ってください。

SIPオブジェクトの作成

1 MMCの[コンソール ルート]ウィンドウ内で、コンテナを右クリックします。

2 **新規 → Dell SIP Object**を選択します。この操作で[新規オブジェクト]ウィンドウが表示されます。

3 新しいオブジェクトの名前を入力します。この名前は、「Remote Console Switchの構成」(ページ 40) の手順4で入力するRCS名と一致している必要があります。

4 **SIP Device Object**を選択します。

5 **OK**をクリックします。

Privilegeオブジェクトの作成

Privilegeオブジェクトは、関連付けられるオブジェクトと同じドメインで作成される必要があります。

1 [コンソールルート](MMC)ウィンドウ内で、コンテナを右クリックします。

2 **新規 → Dell SIP Object**を選択して、[新規オブジェクト]ウィンドウを開きます。

3 新しいオブジェクトの名前を入力します。

4 **Privilege Object**を選択します。

5 **OK**をクリックします。

6 作成したPrivilegeオブジェクトを右クリックして、プロパティを選択します。

7 **RCS Privileges**タブをクリックし、ユーザーに割り当てるRCS特権を選択します。

Dell Associationオブジェクト構文の使用

Dell Associationオブジェクト構文では、Dell LDAPスキーマ内のオブジェクト・タイプはユーザーおよびグループにデフォルト設定されています。Dell拡張スキーマの場合には、次の4つの新規オブジェクト・クラスに対して固有のオブジェクトIDが追加されています:

- KVM RCSオブジェクト
- KVM SIPオブジェクト
- Privilegeオブジェクト
- Associationオブジェクト

これらの新規オブジェクト・クラスはそれぞれ、Active Directoryでのデフォルトのクラスの様々な組み合わせ(階層)とDellでの固有属性タイプに従って定義されています。Dell固有属性タイプはそれぞ

れ、Active Directoryでのデフォルトの属性構文に従って定義されています。

MicrosoftのActive Directoryでのデフォルトのオブジェクト・クラスにはユーザーおよびグループがあります。ユーザー・クラスとは通常、単一エンティティの情報を含むActive Directoryオブジェクトをさします。グループ・クラスはネスト用のコンテナを表し、オブジェクト群の情報を含んでいます。

各KVM RCSオブジェクトは、Active Directory内の個々のRemote Console Switchを表します。これらは単一エンティティであるため、LDAPデフォルト言語ではグループ・オブジェクトではなくユーザー・オブジェクトになっています。

各Privilegeオブジェクトはそれぞれ独特の特権の組み合わせを規定します。個々の組み合わせは別個のエンティティとして扱われます。従って、グループ・オブジェクトではなくユーザー・オブジェクトとなります。

Associationオブジェクトには、特定のRCSやSIPに関して特定のユーザー・アカウントに付与された特権の情報一式が含まれています。RCSオブジェクト内のユーザー・アカウントは、次の任意の組み合わせによって指定できます。

- 個別アカウント
- ユーザー・アカウントのActive Directoryセキュリティ・グループ
- ユーザー・アカウントのActive Directoryセキュリティ・グループ（複数）

同様に、Associationオブジェクト内のRCSやSIPの場合、Associationオブジェクトは複数のセキュリティ・グループを同様に使用できるため、自身がGroupオブジェクトとして定義されます。

Associationオブジェクトの作成

Associationオブジェクトはグループから派生しており、グループの種類を含んでいる必要があります。Associationスコープは、Association

オブジェクトのセキュリティ・グループの種類を指定します。Associationオブジェクトを作成する場合は、追加しようとしているオブジェクト・タイプに適用されるAssociationスコープを選択する必要があります。たとえば、ユニバーサルを選択すると、Active Directoryドメインがネイティブまたはより上位のモードで機能しているときにのみ、Associationオブジェクトが使用可能になります。

Associationオブジェクトを作成するには:

1 [コンソール ルート](MMC) ウィンドウ内で、コンテナを右クリックします。

2 **New → Dell SIP Object**を選択して、[新規オブジェクト]ウィンドウを開きます。

3 新しいオブジェクトの名前を入力します。

4 **Association Object**を選択します。

5 Association Objectのスコープを選択します。

6 **OK**をクリックします。

Association Objectへのオブジェクトの追加

Associationオブジェクトの[プロパティ]ウィンドウを使用すると、ユーザーやユーザー・グループ、Privilegeオブジェクト、およびSIPデバイスやSIPデバイス・グループを関連付けることができます。

注: Windows 2000モードまたはそれ以上を使用している場合は、ユニバーサル・グループを使用して、ユーザーやSIPオブジェクトでドメインを補う必要があります。

ユーザーとSIPデバイスのグループを追加できます。Dell関連のグループの作成は、他のグループの作成と同じ方法で行うことができます。

ユーザーまたはユーザー・グループを追加するには:

1 Associationオブジェクトを右クリックして、**Properties**を選択します。

2 **Users**タブを選択して、**Add**をクリックします。

3 ユーザーまたはユーザー・グループの名前を入力し、OKをクリックします。

Privilege Objectタブをクリックして、SIPデバイスへの認証時にユーザーまたはユーザー・グループの特権を定義するAssociationオブジェクトに、Privilegeオブジェクトを追加します。

注: 1つのAssociationオブジェクトには、1つのPrivilegeオブジェクトのみを追加できます。

特権を追加するには:

1 **Privileges Object**タブを選択して、**Add**をクリックします。

2 Privilegeオブジェクトの名前を入力して、**OK**をクリックします。

Productsタブをクリックして、1つまたは複数のSIPデバイスをAssociationに追加します。関連付けられたデバイスは、定義されたユーザーやユーザー・グループが利用できる、ネットワークに接続されたSIPデバイスを指定します。

注: 1つのAssociationオブジェクトに複数のSIPデバイスを追加できます。

SIPデバイスまたはSIPデバイス・グループを追加するには:

1 **Products**タブを選択して、**Add**をクリックします。

2 SIPデバイスまたはSIPデバイス・グループの名前を入力し、**OK**をクリックします。

3 [プロパティ]ウィンドウで、**Apply**と**OK**を順にクリックします。

コンソール・リダイレクション・アクセスのセキュリティ

RCSの運用環境では、いずれのユーザー特権でもOBWIを起動できます。そのユーザーに対するOBWIの機能は、RCS内に設定されているユーザーの特権レベルによって制限されます。Dell Extended Schema

を使用するLDAPでは、管理者がOBWIへのユーザーのアクセスを制限できるため、RCS管理のセキュリティを強化できます。

OBWIの使用の承認は、Dell Privilegeオブジェクト（DPO）のKVM RCS Privilegesタブで、ユーザーの特権レベルが構成されているかどうかによって定義されます。DPOのKVM SIP Privilegesタブにある Console Redirection Accessチェックボックスを選択すると、OBWIを表示できないユーザーがRCSクライアントからSIPのサブセットに対してビデオ・ビューア・セッションを起動できるようになります。この認証は、DPOで設定した構成パラメーターと、Dell Associationオブジェクト（DAO）に含まれるSIPオブジェクトを組み合わせて実行されます。

OBWIへのアクセス権を持たないユーザーがRCSクライアントからビューア・セッションを起動できるようにするには、下記の手順に従ってください。

1 そのユーザーのアクセスを許可するSIPごとにDell SIPオブジェクトを作成する。

2 対象となるユーザーそれぞれにActive Directoryユーザー・アカウントを作成する。

3 DPOを作成する。KVM RCS Privilegesタブの3つのボックスについては、いずれにもチェックを入れないでください。KVM SIP Privilegesタブの Console Redirection Accessボックスにチェックを入れます。

注： KVM RCS Privilegesチェックボックスのいずれかにチェックを入れ、Console Redirection Accessボックスにもチェックを入れると、Console Redirection Accessチェックボックスよりも KVM RCS Privilegesボックスで選択した特権レベルに関連付けられた標準のユーザー特権が優先されるため、ユーザーはAMPを表示できます。

4 DAOを作成する。

5 手順4で作成したDAOのプロパティを開く。

a. 手順2で作成したすべてのユーザー・アカウントを追加する。

b. 手順3で作成したDPOを追加する。

c. 手順1で作成したSIPオブジェクトを追加する。

Active Directoryを使用したRCSへのログイン

Active Directoryを使用して、RCSソフトウェアまたはOBWIを介してRCSにログインできます。

ログイン構文は、以下の3つの方法すべてに共通です。

<username@domain>または<domain>\<username>または<domain>/<username>(ここで、usernameは1～256バイトのASCII文字列です)。空白や特殊文字(\、/、@など)は、ユーザー名、ドメイン名のどちらにも使用できません。

注: AmericasなどのNetBIOSドメイン名は解決できないので、指定することができません。

注: ドメイン名が含まれていない場合は、Remote Console Switchのローカル・データベースがユーザーの認証に使用されます。

LDAPの実装でターゲット・デバイス名を指定する際の要件

下記のエラー:

Login Failure.Reason:Access cannot be granted due to Authentication Server errors

Active Directory内にSIPオブジェクトが作成されていることと、その名前がコンソール・スイッチでOBWIを介してそのSIPに割り当てられている名前に完全に一致していることを確認してください。

Dell Standard SchemaおよびDell Extended Schemaでは、Microsoft Windows Active Directory内でSIPを表すために固有のオブジェクト・クラスを使用しています。これらのオブジェクト・クラスに対するMicrosoftの通常の命名規則では特殊文字やスペースは使用できな

いことになっています。SIP内のターゲット・デバイス名にスペースや特殊文字が現在含まれている場合、LDAPを使用するにはこれらの文字を含まないよう名前を変更する必要があります。

SIP内のターゲット・デバイス名を変更するには、まずコンソール・スイッチでOBWIを介して行い、次にRCSソフトウェアから再同期化します。OBWIではSIPに割り当てられる名前にスペースを使用できますが、Active Directoryでは使用できないことに注意してください。SIPでのオブジェクト名はMicrosoftのActive Directoryの規則に準じて指定しなければなりません。

よくある質問

次の表に、よくある質問とその答えを示します。

表 5.4: よくある質問

複数のフォレストにわたるActive Directoryを使用してRemote Console Switchにログインできますか?	RCS Active Directoryクエリのアルゴリズムは、単一フォレスト内の単一ツリーのみをサポートしています。
混在モードで動作するActive Directory(つまり、Microsoft Windows NT® 4.0、Windows 2000、またはWindows Server 2003などの異なるオペレーティング・システムを実行している複数のドメイン・コントローラーがフォレスト内に存在する）を使用してRemote Console Switchにログインすることはできますか。	はい。混在モードでは、RCSクエリ処理(ユーザー、SIP Deviceオブジェクト、およびAssociationオブジェクト間）で使用されるすべてのオブジェクトが同じドメイン内に存在している必要があります。Dell拡張のActive Directoryユーザーとコンピューター・スナップインはモードを確認して、混在モードの場合は各ドメインでオブジェクトを作成できるようにユーザーを制限します。

Active DirectoryでのRCSの使用は、複数ドメインの環境をサポートしていますか。	はい。ドメイン・フォレスト 機能レベルは、ネイティブ・モード またはWindows 2003モード である必要があります。さらに、Associationオブジェクト 、Remote Console Switchユーザー・オブジェクト 、およびSIP Deviceオブジェクト（ Associationオブジェクト を含む）中では、グループはユニバーサル・グループでなければなりません。
これらのDell拡張オブジェクト（ Dell Associationオブジェクト 、Dell Remote Console Switch Device、およびDell Privilegeオブジェクト）は、異なるドメインに存在できますか?	Associationオブジェクト と Privilegeオブジェクト は、同じドメインに存在している必要があります。Dell拡張Active Directoryユーザーとコンピューター・スナップインは、強制的にこれらの2つのオブジェクトを同じドメイン内に作成させます。他のオブジェクト は、別のドメインにあっても構いません。
ドメイン・コントローラ SSLの構成に制限はありますか?	はい。RCSには信頼できるCAのSSL証明書を1つしかアップロード できないため、フォレスト 内のすべてのActive Directoryサーバーの SSL証明書は、同一のルート CAによって署名されている必要があります。

Active Directory認証を使用してRCSにログインできない場合は、どうしたらよいですか。	以下のようにトラブルシューティングしてください。 ドメイン名が指定されていない場合には、ローカル・データベースが使用されます。AD認証が機能していないときにログインするには、デフォルトのローカル管理者アカウントを使用してください。 RCS Active Directory構成ページで、Enable Active Directoryチェック・ボックス（RCSソフトウェアの場合）またはUse LDAP Authenticationチェック・ボックス（OBWIの場合）にチェックを入れていることを確認します。 RCS Networking構成ページのDNS設定が正しいことを確認します。 NTPパネルで指定されたサーバーのうち、少なくとも1つのサーバーでNTP（Network Time Protocol）が有効になっていることを確認します。 Active Directoryの証明書をActive Directoryルート CAからRCSへアップロード済みであることを確認します。 ドメイン・コントローラーSSL証明書の期限が切れていないことを確認します。 「Remote Console Switch Name」、「Root Domain Name」、「RCS Domain Name」が、Active Directory環境の構成と一致していることを確認します。 NetBIOS名ではなく、正しいユーザー名とドメイン名を使用してログインしていることを確認します。

A

付録 A: ターミナルの操作

各RCSは、SETUPポートからアクセスされるコンソール・メニュー・インターフェイスを介して、スイッチ・レベルで構成できます。すべてのターミナル・コマンドは、ターミナル・エミュレーション・ソフトウェアを実行しているターミナルまたはコンピューターを介してアクセスされます。

注: 推奨方法は、ローカルUIでの構成設定です。

ターミナルをスイッチに接続するには次の手順を実行します。

1 付属のRJ-45/DB-9(メス)変換アダプターとRJ-45フラット・ケーブルを使用して、ターミナル・エミュレーション・ソフトウェア(HyperTerminalなど)を実行しているターミナルまたはコンピューターを、スイッチの背面パネルにあるSETUPポートに接続します。ターミナル設定の種類は、9600bps、8ビット、1ストップ・ビット、パリティなし、フロー・コントロールなしです。

2 各ターゲット・デバイスをオンにしてから、スイッチの電源をオンにします。スイッチの起動が完了すると、コンソール・メニューに次のメッセージが表示されます。「Press any key to continue」(**続行するには任意のキーを押してください**)。

コンソール・ブート・メニュー・オプション

スイッチの電源投入中に、キーを押してブート・メニューを表示できます。このメニューからは、次の4つのオプションのいずれかを選択できます。

- Boot Normal(**通常ブート**)
- Boot Alternate Firmware(**代替ファームウェアのブート**)

- Reset Factory Defaults(出荷時デフォルトへのリセット)
- Full-Factory Reset(完全出荷時リセット)

コンソール・メイン・メニュー・オプション

電源がオンになると、メイン・メニューに製品の名前とバージョンが表示されます。このメニューからは、次の4つのオプションのいずれかを選択できます。

- Network configuration(ネットワーク構成) : このメニュー・オプションでは、RCSのネットワーク設定を構成できます。
- Debug messages(デバッグ・メッセージ) : このメニュー・オプションで、コンソール・ステータス・メッセージをオンにできます。Dell™この操作を行うと性能が大幅に低減することがあるため、テクニカル・サポートからの指示を受けた場合にのみデバッグ・メッセージを有効化してください。メッセージの閲覧が終了したら、任意のキーを押してこのモードを終了します。
- Reset RCS(RCSのリセット) : このメニュー・オプションでは、スイッチのソフト・リセットを実行できます。
- Exit(終了) : このメニューを選択すると、入力待機のプロンプトに戻ります。コンソール・メニュー・インターフェイスのパスワードが有効になっている場合には、次のユーザーにユーザー名とパスワードのログイン画面によるメッセージが出されるように、コンソールのメイン・メニューを終了する必要があります。

付録 B: SIPの使用

各シリアルSIPポートは、Avocent ACSコンソール・サーバーまたはCiscoのピン配列から選択できます。これは、ローカル・ユーザー・インターフェイスまたはリモート OBWIから選択できます。ACSがデフォルトです。

ピン配列をCiscoモードに変更するには次の手順を実行します。

1 *Unit View* → *RCS* → *RCS Settings* → *Ports* → *SIPs* の順に選択します。

2 対象のSIPをクリックします。

3 *Settings* → *Pinout* の順に選択します。

注: DB-9アダプターを使用している場合は、ACSコンソール・サーバーのピン配列を選択します。

ACSコンソール・サーバー・ポート のピン配列

次の表に、SIPのACSコンソール・サーバー・シリアル・ポート のピン配列を一覧で示します。

表 B.1: ACSコンソール・サーバー・シリアル・ポート のピン配列

ピン番号	信号名	入力／出力
1	RTS - Request to Send(送信要求)	出力
2	DTR - Data Terminal Ready(データ・ターミナル・レディー)	出力

ピン番号	信号名	入力／出力
3	TXD - Transmit Data(送信データ)	出力
4	GND - Signal Ground(信号用接地)	なし
5	CTS - Clear to Send(送信可)	入力
6	RXD - Receive Data(受信データ)	入力
7	DCD/DSR - Data Set Ready(データ・セット・レディ ー)	入力
8	N/C - Not Connected(未接続)	なし

Ciscoポート のピン配列

次の表に、SIPのCiscoシリアル・ポート のピン配列を一覧で示します。

表 B.2: Ciscoシリアル・ポート のピン配列

ピン番号	信号名	入力／出力
1	CTS - Clear to Send(送信可)	入力
2	DCD/DSR - Data Set Ready(データ・セット・レディ ー)	入力
3	RXD - Receive Data(受信データ)	入力
4	GND - Signal Ground(信号用接地)	なし
5	N/C - Not Connected(未接続)	なし
6	TXD - Transmit Data(送信データ)	出力

ピン番号	信号名	入力／出力
7	DTR - Data Terminal Ready(データ・ターミナル・レディー)	出力
8	RTS - Request to Send(送信要求)	出力

C

付録 C: MIBとSNMPトラップ

Dell RCSには監査イベントをSNMPマネージャーに送信する機能があります。SNMPトラップは、SNMPトラップMIBに定義されています。

Save Trap MIB機能を使用して、トラップMIBファイルをRCSからアップロードできます。その後、アップロードされたトラップMIBファイルは、SNMPトラップ・レシーバー・アプリケーションに読み込むことができます。

監査イベントは「syslog」送信先に送ることもできます。各syslogメッセージの形式は、トラップMIBファイルに定義されている各トラップの、対応する「--#SUMMARY」コメントに指定されます。

この付録では、RCSが生成できるトラップ・イベントを説明します。この付録内の情報は、努めて最新のものとしていますが、トラップMIBファイルに含まれているトラップ情報が最も正確です。

SNMPマネージャーは、IPv4またはIPv6プロトコルを使用して、RCSのMIB-IIオブジェクトにアクセスできます。

設計上、RCS内の企業固有のMIBオブジェクトには、SNMPを使用してアクセスすることはできません。

RCSトラップの定義では、次のRFC(Request For Comments) で説明する構造を使用しています。

- RFC-1155-SMI

  TCP/IPベースのインターネットで使用する管理情報の定義に対する一般的な構造と同定法を説明します。

- RFC-1212

簡潔で記述的なMIBモジュールを作成するための形式を説明します。

- RFC-1213-MIB

  TCP/IPベースのインターネットワークでのネットワーク管理プロトコルでの使用に対するインターネット標準MIB-IIを説明します。

- RFC-1215

  SNMP標準トラップを説明し、企業固有のトラップを定義する方法を提供します。各トラップによって報告される特定のオブジェクトは、RCSからアップロードされたトラップMIBファイルに定義されています。次の表に、生成されたトラップ・イベントの一覧を示します。

表 C.1: 生成されたトラップ・イベント

トラップ・イベント	トラップ番号
再起動が開始しました	1
ユーザーログイン	2
ユーザーログアウト	3
ターゲット セッションが開始しました	4
ターゲット セッションが停止しました	5
ターゲット セッションが終了しました	6
トラップ7～9は廃止されました	7-9
イメージ・ファイルのアップグレードが開始しました	10
イメージ・ファイルのアップグレード結果	11
ユーザーが追加されました	12

トラップ・イベント	トラップ番号
ユーザーが削除されました	13
ユーザーが変更されました	14
ユーザーはロック状態です	15
ユーザーはロック解除されています	16
ユーザー認証の失敗	17
SIP が追加されました	18
SIP が取り外されました	19
SIPが移動されました	20
ターゲット デバイス名が変更されました	21
ティアド スイッチが追加されました	22
ティアド スイッチが取り外されました	23
ティアド スイッチの名前が変更されました	24
構成ファイルが読み込まれました	25
ユーザー データベース ファイルが読み込まれました	26
CA証明書が読み込まれました	27
SIP イメージのアップグレード が開始しました	28
SIP イメージのアップグレード 結果	29
SIP が再起動しました	30
バーチャル メディア セッションが開始しました	31

トラップ・イベント	トラップ番号
バーチャルメディア セッションが停止しました	32
バーチャルメディア セッションが終了しました	33
バーチャルメディア セッションが予約されました	34
バーチャルメディア セッションが予約解除されました	35
バーチャルメディアドライブがマッピングされました	36
バーチャルメディアドライブがマップ解除されました	37
トラップ38～44は廃止されました	38-44
画面解像度が変更されました	45
集約ターゲット・デバイスの状態が変更されました	46
出荷時デフォルト 設定	47
電源エラー	48
電源が復元されました	49
PDUデバイスはオンラインです	50
PDUデバイスはオフラインです	51
PDUソケット・オン・コマンド	52
PDUソケット・オフ・コマンド	53
PDUソケット 再起動コマンド	54
PDUソケット・オンの検出失敗	55
PDUソケット・オフの検出失敗	56

トラップ・イベント	トラップ番号
PDU状態ソケット・オン	57
PDU状態ソケット・オフ	58
PDUポート 名が変更されました	59
PDUソケット 名が変更されました	60
PDU入力フィード 合計負荷高	61
PDU入力フィード 合計負荷低	62
PDUデバイス名が変更されました	63
PDU入力フィード 名が変更されました	64
PDUソケット・ロック・コマンド	65
PDUソケット・ロック解除コマンド	66
PDU状態ソケット・ロック	67
PDU状態ソケット・ロック解除	68
PDUイメージ・ファイルのアップグレード が開始しました	69
PDUイメージ・ファイルのアップグレード 結果	70
PDU回路名が変更されました	71
PDUデバイス合計負荷高	72
PDU回路合計負荷高	73
PDUソケット 合計負荷高	74
ファン・エラー	75

トラップ・イベント	トラップ番号
温度範囲	76
スマート カード が挿入されました	77
スマート カード が取り外されました	78

D

付録 D: ケーブルのピン配列情報

注: すべてのスイッチには、モデム・ポートとコンソール／セットアップ・ポート用にRJ45(8ピン・モジュラー) ジャックが付いています。

モデムのピン配列

モデム・ポートのピン配列と説明を次の図および表に示します。

図 D.1. モデムのピン配列

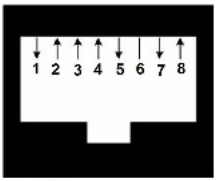


表 D.1: モデムのピン配列の説明

ピン番号	説明	ピン番号	説明
1	送信要求(RTS: Request to Send)	5	送信データ (TXD: Transmit Data)
2	データ・セット・レディー (DSRData Set Ready)	6	信号用接地(SG: Signal Ground)

ピン番号	説明	ピン番号	説明
3	データ・キャリア検出 (DCD: Data Carrier Detect)	7	データ・ターミナル・レディー (DTR: Data Terminal Ready)
4	受信データ (RXD: Receive Data)	8	送信可(CTS: Clear to Send)

コンソール／セットアップのピン配列

コンソール／セットアップ用ポートのピン配列と説明を次の図および表に示します。

図 D.2. コンソール／セットアップのピン配列

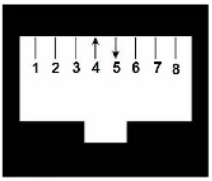


表 D.2: コンソール／セットアップのピン配列の説明

ピン番号	説明	ピン番号	説明
1	接続なし	5	送信データ (TXD: Transmit Data)
2	接続なし	6	信号用接地(SG: Signal Ground)
3	接続なし	7	接続なし
4	データ受信(RXD: Receive Data)	8	接続なし

E

付録 E: UTPケーブル

以下に、接続媒体のさまざまな特徴を説明します。RCSシステムではUTPケーブル配線を使用します。スイッチ・システムの性能は、高品質の接続が得られるかどうかに依存します。品質が優れないケーブル、設置や保守に問題のあるケーブルは、システムの性能を損なう結果となる場合があります。

注: この付録は情報の提供のみを目的としています。設置する前に、当地のコード当局やケーブル関連の専門家に確認してください。

銅製UTPケーブル

RCSでサポートされている3種類のUTPケーブルの基本的な定義は次のとおりです。

- CAT 5 (4ペア) 高性能ケーブルは、ツイスト・ペア電線で構成されており、主にデータ送信に使用されます。ペア線がより合わされていることで、このケーブルでは不要な干渉の混入からある程度免れることができます。CAT 5ケーブルは通常、10～100 Mbpsの範囲で動作するネットワークに使用します。
- CAT 5E(強化) ケーブルの特徴はCAT 5と同様ですが、製造規格が若干厳しいものになっています。
- CAT 6ケーブルは、CAT 5Eケーブルに比べより厳しい要件に合わせて製造されています。CAT 6はより高い測定周波数範囲を持ち、同一周波数においてはCAT 5Eに比べ明らかに分かる優れた性能要件を示します。

配線規格

8導線(4ペア) RJ-45終端処理済みUTPケーブルには、2種類の推奨配線規格があります。EIA/TIA 568AおよびB。これらの規格は、UTPケーブル仕様によるインストールに適用されます。RCSシステムではこれらの規格のいずれかがサポートされています。次の表は、各ピンの規格を説明しています。

表 E.1: UTP配線規格

ピン固定	EIA/TIA 568A	EIA/TIA 568B
1	白／緑	白／オレンジ
2	緑	オレンジ
3	白／オレンジ	白／緑
4	青	青
5	白／青	白／青
6	オレンジ	緑
7	白／茶	白／茶
8	茶	茶

ケーブルの設置、保守、および安全情報

次に、ケーブルの設置や保守を実行する前に目を通しておくべき重要な安全注意事項を一覧で示します。

- 各UTPの長さは最長で9.1 m(30フィート) としてください。
- ペア線は、必ず終端箇所までツイストされた(より合わされた) 状態を保つか、またはツイストになっていない部分が1.3

cm(半インチ) を超えないようにしてください。終端処理の際、外被を2.5 cm(1インチ) 以上剥がさないでください。

- ケーブルを曲げる必要がある場合は、半径が2.5 cm(1インチ) より小さくならない範囲で緩やかに行ってください。ケーブルを鋭角に曲げたりねじったりすると、ケーブル内部に恒久的な損傷が生じるおそれがあります。
- ケーブルは、ケーブル・タイを用いて低～中程度の圧力で束ねてまとめてください。ケーブル・タイは締め過ぎないでください。
- ケーブルは必要に応じて、定格のパンチ・ブロック、パッチ・パネル、その他のコンポーネントを用いて交差接続します。ケーブルは絶対に繋ぎ合わせたりブリッジにしたりしないでください。
- UTPケーブルは、電線、トランス、電灯などのようなEMI源となり得る品物からはできるだけ距離を持たせてください。ケーブルを電線用導管に結びつけたり、電気機器上に配置したりしないでください。
- 設置部分は必ずケーブル・テスターでテストしてください。トーニングのみではテストとして適切ではありません。
- ジャックの設置は、接点に埃や他の汚染物質が蓄積しないような形で行ってください。ジャックの接点は、埋め込み型のプレート上では上向きに、表面実装型ボックスの場合は左／右／下向きにします。
- ケーブルには常に遊びをもたせ、天井部分あるいは付近の引込んだ箇所にはコイル状に整然と配置します。少なくとも、コンセント側では1.5 m(5フィート) 、パッチ・パネル側では4.5 m(15フィート) のケーブルの長さを残しておいてください。
- 作業を開始する前に、568Aと568Bのどちらの配線規格を使用するかを決めておいてください。ジャックおよびパッチ・パネルはすべて、同一の配線方式で配線します。同一の設置に568Aと568Bのワイヤーを混在させないでください。

- 常に、地方／国の消防規則および建築条例のすべてに従ってください。防火壁を通過するケーブルには必ず火炎止めをしてください。規定に応じてプレナム・ケーブルを使用してください。

F

付録 F: Sunアドバンスト・キー・エミュレーション

標準タイプ 5 (US) Sun キーボードの特定のキー、ローカル・ポートのUSBキーボードでキーを連続して押すことにより、エミュレートすることができます。Sun Advanced Key Emulation(Sunアドバンスト・キー・エミュレーション) モードを有効にしてこれらのキーを使用するには、Ctrl+Shift+Altキーを押したままScroll Lockキーを押します。Scroll LockのLEDが点滅します。Sunキーボードのアドバンスト・キーを使用するのと同様に、次の表のキーを使用します。
例: Stop+Aは、Ctrl+Shift+Altキーを押したままScroll Lockキーを押し、F1+Aキーを押します。

これらのキー・コンビネーションは、Dell USB、USB2、USB2とCAC用SIPおよびAvocent USB、USB2、VMC IQモジュールで使用できます。これらのキー・コンビネーションは、F12を除き、Microsoft Windows製品では認識されません。F12キーは、Windowsのキープレスを実行します。終了したら、Ctrl+Shift+Altキーを押したまま Scroll Lockキーを押し、Sunアドバンスト ·キー・エミュレーション ·モードを切り替えてオフにします。

表 F.1: Sunキー・エミュレーション

Compose	アプリケーション[1]
Compose	キーパッド
電源	F11キー
開く	F7キー

ヘルプ	Num Lock
Props	F3キー
前面	F5キー
停止	F1キー
Again	F2キー
元に戻す	F4キー
切り 取り	F10キー
コピー	F6キー
貼り 付け	F8キー
Find	F9キー
Mute	keypad /
Vol.+	keypad +
Vol.-	keypad -
Command(左) [2]	F12キー
Command(左) [2]	Win (GUI) 左 [1]
Command(右) [2]	Win (GUI) 右 [1]

備考 :

(1) Windows 95 104キー・キーボード 。

(2) CommandキーはSun Meta(ダイヤモンド) キーです。

G

付録 G: 技術仕様

表 G.1: RCS技術仕様

ポートの個数	1082DS: 8 2162DS: 16 4322DS: 32
タイプ	Dell PS/2、USB、USB2、USB2+CAC、およびシリアルSIP。Avocent PS/2、PS2M、USB、Sun、USB2、VMC、およびシリアル・モジュール。
コネクター	8ピン・モジュラー(RJ-45)
同期タイプ	垂直／水平同期信号分離

入力ビデオ解像度	標準 640 x 480 @ 60 Hz 800 x 600 @ 75 Hz 960 x 700 @ 75 Hz 1024 x 768 @ 75 Hz 1280 x 1024 @ 75 Hz 1600 x 1200 @ 60 Hz ワイド スクリーン 800 x 500 @ 60 Hz 1024 x 640 @ 60 Hz 1280 x 800 @ 60 Hz 1440 x 900 @ 60 Hz 1680 x 1050 @ 60 Hz
推奨ケーブル	4ペア UTP、最長45メートル
寸法	
フォーム・ファクター	1Uまたは0Uラック収納
寸法	1.72. x 17.00 x 9.20 (高さ x 幅 x 奥行き)
重量 (ケーブルを除く)	1082DS: 6.6 lb (3.0 kg) 2162DS: 7.0 lb (3.2 kg) 4322DS: 7.6 lb (3.4 kg)
SETUPポート	
番号	1

プロトコル	RS-232シリアル
コネクター	8ピン・モジュラー(RJ-45)
ローカル・ポート	
個数／タイプ	1 VGA/4 USB
ネットワーク接続	
番号	2
プロトコル	10/100/1000イーサーネット
コネクター	8ピン・モジュラー(RJ-45)
USBデバイス・ポート	
番号	4
プロトコル	USB 2.0
MODEMポート	
番号	1
プロトコル	RS-232シリアル
コネクター	8ピン・モジュラー(RJ-45)

PDUポート	
番号	2
プロトコル	RS-232シリアル
コネクター	8ピン・モジュラー(RJ-45)
電源仕様	
コネクター	1082DS: 1 IEC C14 2162DS: 2 IEC C14 4322DS: 2 IEC C14
タイプ	内部
電源	18W
熱放散	47 BTU/時
AC入力範囲	100～240 VAC
AC周波数	50/60 Hz自動検知
AC入力電流定格	1.25 A
AC入力電源(最大)	40 W

周囲大気条件定格	
温度	0～50℃(動作時) 、-20～70℃(非動作時)
湿度	作動時: 20%～80% 相対湿度(結露なし) 5%～95% 相対湿度、38.7℃ 最大湿球温度
安全規格およびEMC規格認証、マーキング類	UL / cUL、CE - EU、N (Nemko)、GOST、C-Tick、NOM / NYCE、MIC (KCC)、SASO、TUV-GS、IRAM、FCC、ICES、VCCI、SoNCAP、SABS、Bellis、FIS/ Kvalitet、Koncar、INSM、Ukrtest、STZ、KUCAS 本製品の安全性証明書およびEMC証明書は、次の1つまたは複数の題名の下でご覧いただけます。CMN(証明書モデル番号) 、MPN (製造元部品番号) 、販売段階で付く型式名称。EMCおよび／または安全性の報告書および証明書で参照されている題名は、製品に使用されているラベル上に印刷されています。

H

付録 H: テクニカル・サポート

Dell製品のインストールや操作について問題や疑問点が生じた場合には当社のテクニカル・サポートまでご連絡ください。担当スタッフがお手伝いいたします。万一問題が生じた場合は、より良いサービスをお受けいただけるよう、次の手順に従ってください。

問題を解決するには:

1 問題の該当箇所をマニュアルで調べ、記載されている手順に従って解決できるかどうかを試してください。

2 弊社のWebサイト(dell.com/support)にある「Knowledge Base(ノレッジ・ベース)」のデータベースからご検索いただくか、または「Online Service Request(オンライン・サービス・リクエスト)」をご利用ください。

3 最寄りのDellテクニカル・サポートまでお電話にてご連絡ください。