CA Spectrum®

Secure Domain Manager ユーザ ガイド

リリース 9.4

ca technologies

このドキュメント（組み込みヘルプ システムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。

CA の事前の書面による承諾を受けずに本ドキュメントの全部または一部を複写、譲渡、開示、変更、複本することはできません。 本ドキュメントは、CA が知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、（i）本ドキュメントが関係する CA ソフトウェアの使用について CA とユーザとの間で別途締結される契約または (ii) CA とユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

上記にかかわらず、本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。 いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負います。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。 また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本ドキュメントの制作者は CA です。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2014 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA Spectrum®（CA Spectrum）
- CA Spectrum® Secure Domain Manager
- CA Spectrum® Secure Domain Connector

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

目次

第 1 章: はじめに 7

非常に安全なネットワークの管理に伴う課題 7
IP ドメインの重複 8
SNMP および ICMP トラフィックをブロックするファイアウォール 10
安全でないネットワークを通過する SNMP トラフィック 11
Secure Domain Manager 12
Secure Domain Manager の動作 13
Secure Domain Manager アーキテクチャ 16
Secure Domain Manager を使用する利点 17

第 2 章: Secure Domain Manager プロセスのインストールおよび設定 19

Secure Domain Manager プロセスをセットアップする方法 19
プロセスのインストールおよび設定 19
SpectroSERVER での Secure Domain Manager のセットアップ 20
ハードウェアの推奨事項 20
SDConnector CPU とメモリの使用率について 21
SDConnector プロセスのインストール 21
インストール ファイル 23
証明書の利用 24
アップグレード時の古い証明書ファイルの削除 24
証明書の作成 24
SDConnector プロセスの設定 27
SDManager プロセスの設定 31
Windows での SDConnector プロセスの開始、停止、再起動 34
Solaris および Linux での SDConnector プロセスの開始、停止、再起動 35

第 3 章: Secure Domain Manager の使用 37

SDManager 設定ファイルのインポート 37
SDConnector ホストのモデリング 39
SDConnector モデリング考慮事項 40
SDConnector モデリングおよび CA Spectrum 障害分離 40
セキュア ネットワーク ドメインのデバイスのモデリング 41
IP によるモデル作成 42

ディスカバリ 42
SDConnector ホストを使用したデバイスの検出 43
デバイス セキュア ドメイン メンバシップの保守について 44
Secure Domain Manager 検索へのアクセス 45
セキュア ドメインのデバイス アクセシビリティの確認 45
セキュア ドメインのデバイス MIB の表示 45
SDManager モデル情報ビュー 47
SDConnector モデル情報ビュー 49

第 4 章 : フォールト トレラント環境のプロセスのセットアップ 51

フォールト トレラント SpectroSERVER 環境での SDManager のセットアップ 51
フォールト トレラント SpectroSERVER （SDManager） 52
フォールト トレラント SDConnector のセットアップ 52
フォールト トレラント SDConnector 54

付録 A: Secure Domain Manager のトラブルシューティング 55

エラー メッセージ 55
無効な証明書エラー 55
ポートの競合 56
SDConnector にカスタム SNMP トラップ ポートが必要です 56
インストール問題 56

第 1 章: はじめに

このセクションには、以下のトピックが含まれています。

非常に安全なネットワークの管理に伴う課題 (P. 7)
Secure Domain Manager (P. 12)
Secure Domain Manager の動作 (P. 13)
Secure Domain Manager アーキテクチャ (P. 16)
Secure Domain Manager を使用する利点 (P. 17)

非常に安全なネットワークの管理に伴う課題

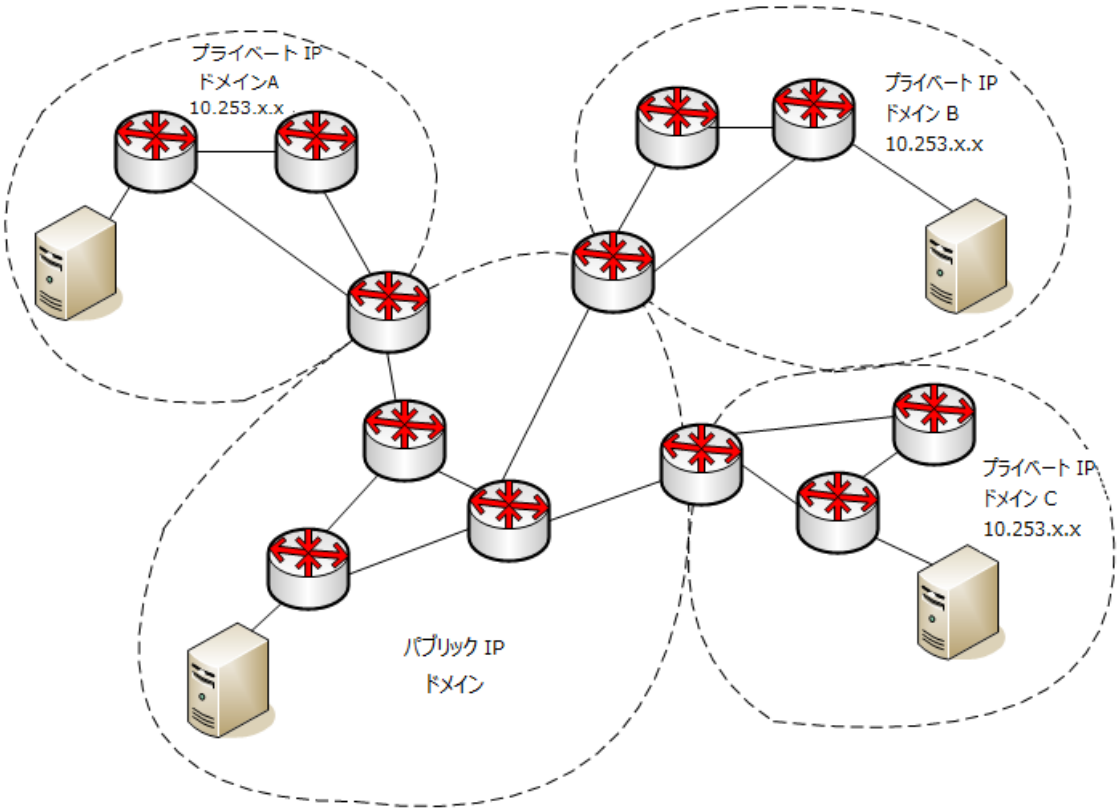
最近のコンピュータ ネットワークは以前より安全になりました。 それに合わせて、安全なネットワークでのデバイスおよびアプリケーションの管理に伴う課題が増えています。 以下のような課題があります。

- 重複する（またはプライベートの） IP ドメイン（NAT 環境）でのネットワーク エレメントの管理
- SNMP および ICMP トラフィックをブロックするように設定するファイアウォールの背後のネットワーク エレメントの管理
- 安全でないネットワーク ドメインのネットワーク エレメントの管理

Secure Domain Manager 製品は、これらの管理課題に独自のソリューションを提供します。

IP ドメインの重複

以下は、パブリック IP ドメインと同じ IP サブネットを含む 3 つのプライベート IP ドメインを含む NAT ネットワークの図です。



ドメインは、会社、大企業の新しく獲得した部門、または空港ターミナルの管理されたワイヤレス ホット スポットの管理されたネットワークを表すことがあります。

以下のタイプの CA Spectrum ユーザは、IP の重複という課題に直面します。

管理対象サービス プロバイダ（MSP）

MSP は CA Spectrum を使用して他の組織のネットワークを管理します。MSP が管理するカスタマは通常、プライベート IP に一般的に使用される IP 範囲（10.x.x.x や 172.16.x.x など）を使用します。 そのため、MSP は、重複する IP アドレスを管理するという課題に対処する必要があります。 この課題は過去に、同じ IP アドレス空間を使用していた各カスタマに専用の CA Spectrum 管理サーバ（SpectroSERVER）を提供することにより対処されました。

これは 2 つの問題を引き起こしました。1 つ目の問題はコストでした。管理対象環境のサイズ、およびそれが使用した重複する IP アドレスの数にかかわらず、カスタマごとに専用の管理サーバが必要でした。2 つ目の問題は管理でした。 MSP はより多くの管理システムの保守を課せられました。 特に IP アドレスが重複する要素の数が少なく、専用管理サーバの経費を拠出するだけの正当な理由がなかったときは、MSP は専用管理システムのそれほど高価でなく、より効率的な代替を必要としました。

ホット スポット（Wi-Fi）**アクセス プロバイダ**

ホット スポット アクセス プロバイダは、空港ターミナル、空港ラウンジ、ホテルの部屋、およびコーヒー ショップなどの場所で Wi-Fi アクセスを提供します。 場所ごとに、同じプライベート IP アドレス空間が発行されます。 この手法は設定、インストール、および管理を簡略化します。プロバイダは何百または何千ものホット スポットを設置することがあります。 新しいホット スポットを迅速に展開するために、ある所有地のホット スポットを確立する機器の各集合が、IP アドレス空間スペースを含めて、同一に設定されます。 ホット スポットが稼働すると、最適なサービス水準を保持するために、ホット スポットの先を見越した管理が課題となります。

企業の経営陣

組織が合併または買収された場合、企業の経営スタッフは、通常、完全に別個に構築された 2 つの IP ネットワークを組み合わせる必要があるため、結果的に多くのインスタンスで複数の IP アドレスが重複します。 このようなシナリオでは、新しい IT 組織は結合したネットワーク、特に IP アドレス空間が同じネットワークの管理に対処する必要があります。 IP アドレスの重複がないように、すべての IP エンティティに IP を再割り当てすることがこの課題の 1 つの解決策です。その解決策は、多くの困難を意味する大事業となります。

Secure Domain Manager を利用すれば、このような場合に以下の方法で重複する IP ドメインの管理という困難を克服できます。

- MSP は、各カスタマのリモート ネットワークのホスト マシンに軽量のエージェント プロセスを 1 つだけ配置すれば良く、完全な CA Spectrum インストールを展開し、管理する必要がありません。
- ホット スポット アクセス プロバイダおよび大企業は、重複するプライベート IP ドメインはそのままにしておき、軽量のエージェント プロセスを使用してネットワークを管理できます。

SNMP および ICMP トラフィックをブロックするファイアウォール

ファイアウォールは多くのネットワーク環境にとって重要なセキュリティを提供します。 ファイアウォールの背後のネットワーク管理にはいくつかの課題が存在します。 まず、ネットワーク管理者は、認められていないソースに対して、SNMP および ICMP トラフィックをブロックするようにファイアウォールを頻繁に設定します。このようなトラフィックは管理対象ネットワークのインフラストラクチャに対する可視性を提供してしまうためです。 また、高度に安全なファイアウォールによるネットワーク エレメントの管理に必要な設定は複雑になります。 完全な管理を可能にするために、関係するすべてのホストおよびポートがファイアウォール上で識別され、開かれるためです。

Secure Domain Manager を利用すれば、ネットワーク管理者は以下の方法で安全なファイアウォールによるネットワーク管理という困難を克服できます。

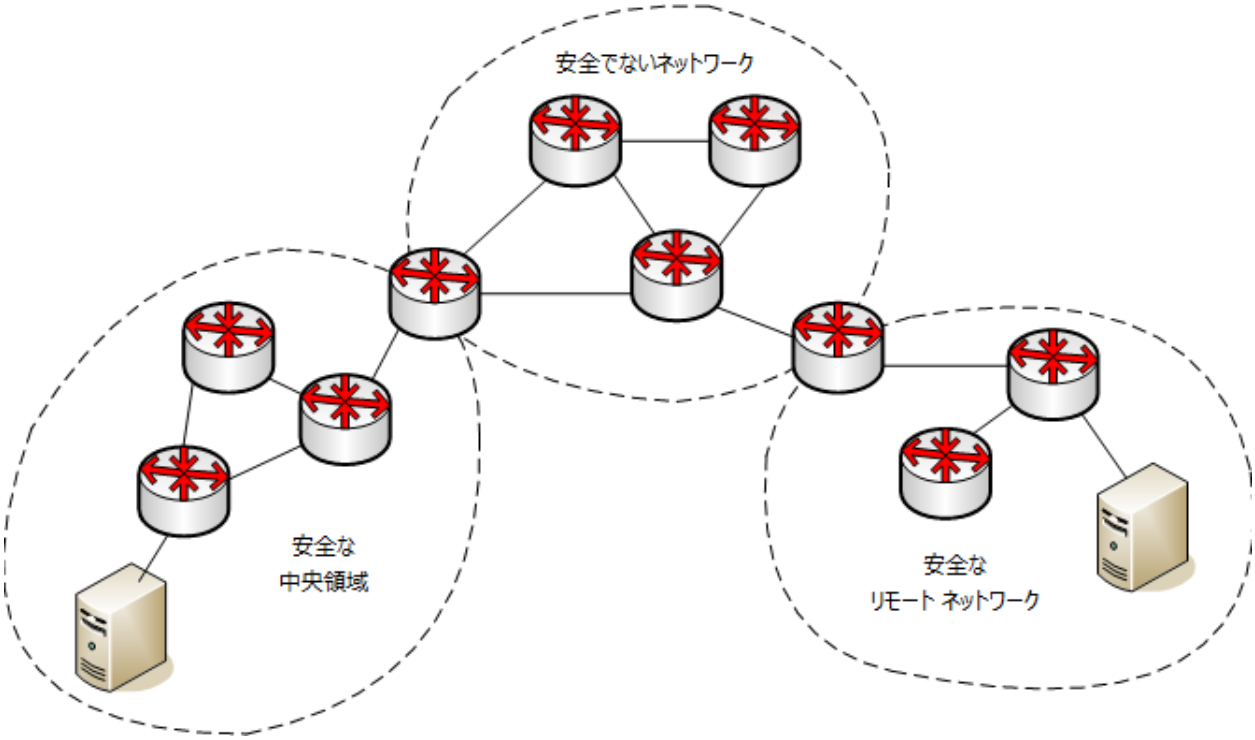
- UDP ベースの SNMP および ICMP パケットを TCP/IP ベースのプロトコルにエンコードすることで、SNMP および ICMP トラフィックに対してより強力なファイアウォールを構築できます。
- 開くポートを 1 つにすることで、ファイアウォールの設定を簡略化します。その 1 つのポートを詳細に定義し、詳細に定義された 2 つのホストの間での SNMP および ICMP トラフィックのフローを許可します。

安全でないネットワークを通過する SNMP トラフィック

SNMPv1 と SNMPv2 は、データが暗号化されず、プロトコル アナライザを使用して参照できるので、安全でないプロトコルです。 そのため、安全でないネットワークを介してこのトラフィックを送信することは望ましくありません。 安全でないネットワークを通過して管理対象ネットワークに到達することを SNMP トラフィックに許可することは難しい問題です。

以下の図は、「安全な中央領域」内のホスト コンピュータ上のネットワーク管理システムが、「安全なリモート ネットワーク」内のデバイスを管理している図です。管理トラフィックは、「安全でないネットワーク」領域を通過する必要があります。 ネットワーク管理者は、ネットワークのこの部分で、SNMPv1 や SNMPv2 などの安全でないプロトコル パケット内のデータを露出しないようにします。

安全でないネットワークを通過する SNMP



Secure Domain Manager では、ネットワーク管理者は SpectroSERVER ホストとリモート管理対象ネットワーク内のホストの間で渡される管理トラフィックをすべて暗号化できます。 これにより、安全でないネットワークを通過する安全でない SNMP トラフィックを保護することができます。トラフィックが中間の安全でないネットワークを通過する場合でもデータのセキュリティが維持されます。

Secure Domain Manager

Secure Domain Manager は、安全なネットワークでのデバイス管理を可能にする CA Spectrum ネットワーク管理ソリューションです。 ローカル SpectroSERVER を展開せずにデバイスを管理できます。 Secure Domain Manager では、安全な接続を介して SNMP および ICMP トラフィックを安全にトンネリングすることで、セキュア ドメインを管理できます。1 つのポートのみがファイアウォールで開かれます。セキュリティ ポリシーに影響を与えずに、管理がますます簡単になります。 このソリューションはエンド ユーザとクライアント アプリケーションに対して透過的であり、管理タスクが増えることがありません。

Secure Domain Manager の動作

Secure Domain Manager は SNMPv1、SNMPv2、および SNMPv3 通信をサポートします。 これは 2 つの異なるプロセス、SDManager および SDConnector から構成されます。

SDManager

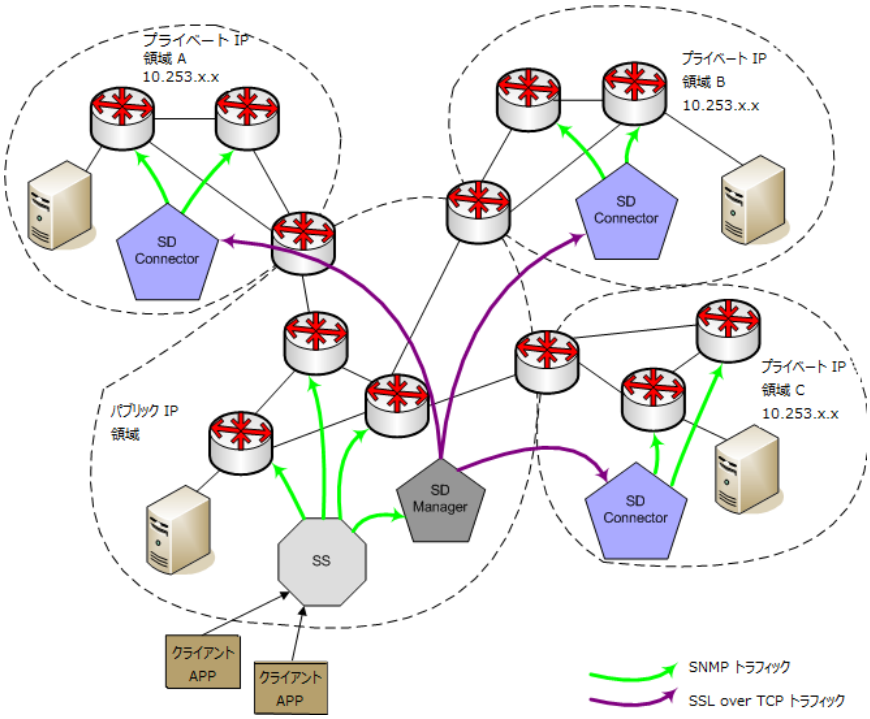
SDManager は SpectroSERVER によってロードされるサーバ メッセージング ライブラリです。

SDConnector

SDConnector は、SpectroSERVER の SDManager との通信を担当するリモート プロセスです。 これはリモート プライベート ネットワークにあるホスト マシンで実行され、プライベート ネットワークのデバイスを管理できるように、（通常、プライベート IP 領域に展開される）SpectroSERVER の代理として SNMP および ICMP メッセージを転送できます。 SDConnector は、プライマリとバックアップの両方の SpectroSERVER 情報を含めることができる設定ファイル（sdc.config）を使用して設定されます。 これは Secure Domain Manager ソリューションの一部です。

以下は、これらのプロセスが安全なネットワーク環境で展開する仕組みを示した図です。

Secure Domain Manager を使用した NAT ネットワーク環境



注: SpectroSERVER と同じ領域に配置されるデバイスは SNMP を使用して管理されますが、Secure Domain Manager を使用しません。

パブリック IP 領域にある SpectroSERVER が、リモートの安全な領域にあるデバイスと通信する必要がある場合、SpectroSERVER は SDManager に要求を送信します。SDManager は SMNP データを独自の形式に変換し、デバイスと同じ領域にある SDConnector にデータを送信します。 SDManager と SDConnector が SSL で実行されるように設定されている場合、SSL over TCP を使用し、データは暗号化され、安全なトンネルを通って SDConnector に送信されます。 SDConnector はデータを受信すると、SNMP にデータを再変換し、適切なデバイスに要求を送信します。

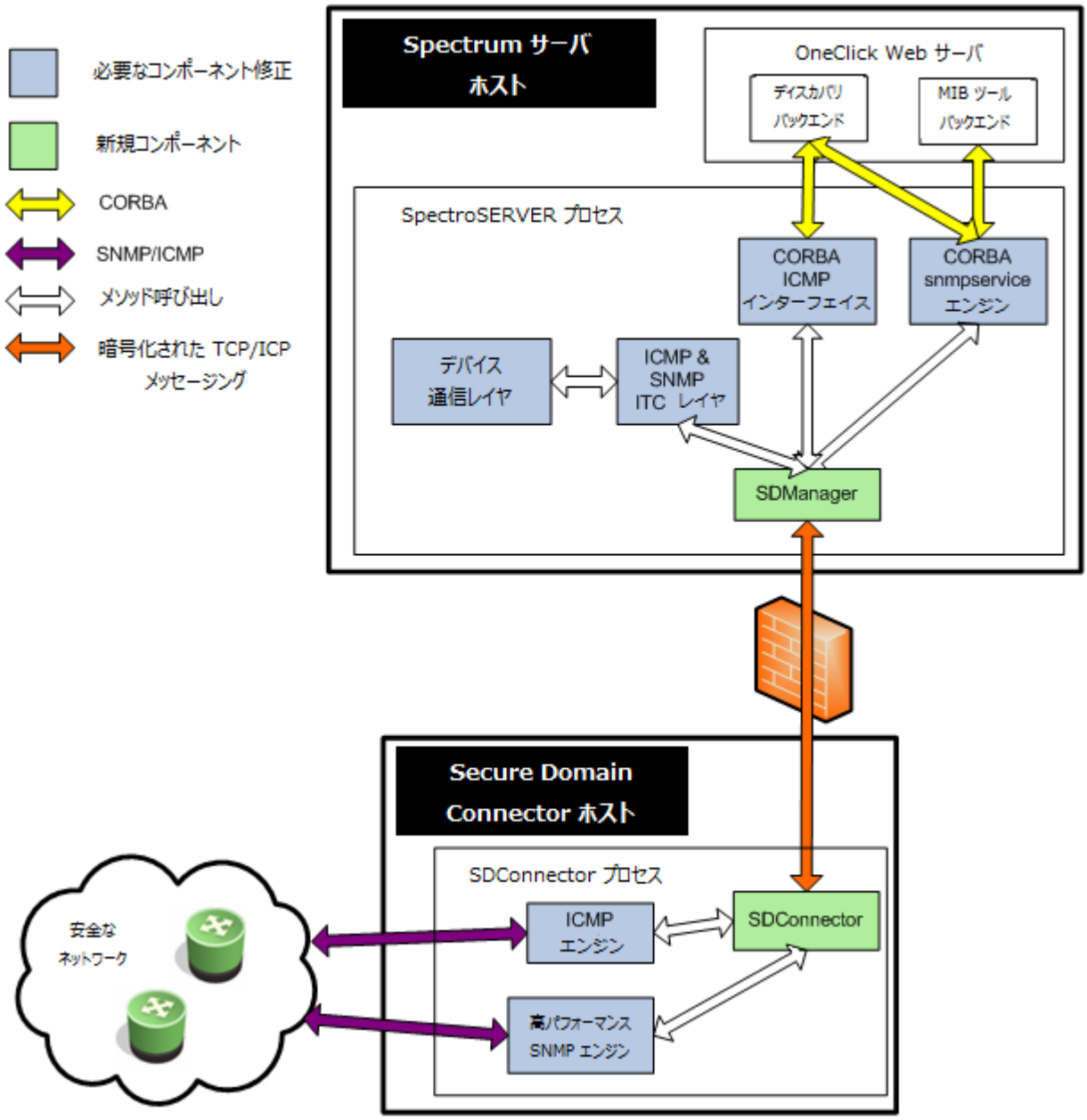
ファイアウォールが展開されている場合も同じように動作します。 ネットワーク管理者は、既知の 2 つのホストの専用のファイアウォールごとに「ホール」を作成する必要があります。 複数のファイアウォールを通過する領域に配置されているデバイスもこのソリューションを使用して管理できます。 この通信を有効にするには、各ファイアウォールでポートを開きます。 そのポートはウェルノウン ポートである必要があります。 ウェルノウン ポートを利用すれば、隣り合う 1 組のウェルノウン ホストで TCP による通信が可能になります。

Secure Domain Manager を展開して重複 IP ドメインを管理する場合、各 SDConnector ホスト マシンに一意のパブリック IP アドレスを与える必要があります。 ホストは、SDConnector が通信する必要があるすべてのデバイスと通信できる必要があります。そのようなデバイスには、SpectroSERVER ホスト マシンとそれが管理する単一のプライベート IP ドメイン内のすべてのデバイスが含まれます。この SDConnector ホストの可能性の高い候補は、NAT から一意の IP アドレスが静的に割り当てられる、NAT の背後のマシンです。 SpectroSERVER は追加の識別子として SDConnector ホスト マシンの一意の IP アドレスを使用し、同じプライベート IP アドレスを持つ複数のデバイスを一意に識別します。

注: Network Configuration Manager （NCM）および IP サービス管理アプリケーション（Multicast Manager および Enterprise VPN Manager を含む）など、特定の CA Spectrum 製品は重複する IP アドレスを管理できません。ただし、SpectroSERVER ではなく SDConnector でデバイスをモデリングする場合、引き続きこれらのアプリケーションと共に Secure Domain Manager を使用できます。 このような設定では、重複する IP アドレスで設定されているデバイスを SDConnector が管理していない限り、各 SpectroSERVER に対して複数の SDConnector を展開できます。 この手法を利用すると、依然としてローカルの SpectroSERVER でデバイスをモデリングできます。ただし、それらのデバイスが、SDConnector によって管理されているデバイスに設定された IP アドレスと重複する IP アドレスで設定されていない場合に限ります。

Secure Domain Manager アーキテクチャ

以下は、Secure Domain Manager の動作を図にしたものです。



Secure Domain Manager を使用する利点

Secure Domain Manager ソリューションは、以下の方法で、CA Spectrum に備わっている既存の管理機能を強化します。

- SNMP 準拠のすべてのデバイス（SNMPv1、SNMPv2、および SNMPv3）と CA Spectrum の通信を可能にします。
- SNMP および ICMP トラフィックをブロックするファイアウォールの背後にあるデバイスと CA Spectrum の通信を可能にします。
- ファイアウォール設定を簡略化します。 それは、1 つのウェルノウンポートの 2 つのウェルノウン ホスト間を通過するトラフィックに対してホールが 1 つのだけ開かれるためです。
- CA Spectrum は、安全でないネットワークを通して、SNMP および ICMP トラフィックを安全に渡すことができます。
- CA Spectrum は、単一の SpectroSERVER を使用して、重複する IP ドメイン（NAT 環境）のデバイスを管理できます。
- ディスカバリ機能が強化され、一度に 1 つの IP アドレス空間に対して、安全な環境でデバイスを検出し、モデリングできます。

第 2 章: Secure Domain Manager プロセスのインストールおよび設定

この章では、Secure Domain Manager ソリューションをインストールし、設定する方法について説明します。これは、SDConnector と SDManager のインストールと設定が含まれるプロセスになります。

このセクションには、以下のトピックが含まれています。

Secure Domain Manager プロセスをセットアップする方法 (P. 19)
ハードウェアの推奨事項 (P. 20)
SDConnector プロセスのインストール (P. 21)
証明書の利用 (P. 24)
SDConnector プロセスの設定 (P. 27)
SDManager プロセスの設定 (P. 31)
Windows での SDConnector プロセスの開始、停止、再起動 (P. 34)
Solaris および Linux での SDConnector プロセスの開始、停止、再起動 (P. 35)

Secure Domain Manager プロセスをセットアップする方法

Secure Domain Manager のセットアップでは、最初に Secure Domain Manager プロセスをインストールして設定し、次に OneClick を使用して SpectroSERVER でそれらのプロセスをセットアップします。

プロセスのインストールおよび設定

Secure Domain Manager プロセスのインストールおよび設定するには、以下の手順に従います。

1. 指定のホストに SDConnector プロセスをインストールします (P. 21)。

   注: SDManager はコア CA Spectrum 製品をインストールしたときにインストールされます。ただし、法人購入のバンドルに含まれている場合にのみアクティブになります。

2. （オプション）SSL 暗号化の SSL 証明書を作成し、展開します (P. 24)。

3. SDConnector ホストで SDConnector の設定ファイルにパラメータを設定します (P. 27)。
4. SpectroSERVER で SDManager の設定ファイルにパラメータを設定します (P. 31)。

SpectroSERVER での Secure Domain Manager のセットアップ

SDConnector と SDManager のプロセスをインストールして設定したら、OneClick を使用して SpectroSERVER ホストで Secure Domain Manager をセットアップします。 このセットアップは以下の手順で行われます。

1. SDManager 設定ファイルをインポートします (P. 37)。
2. SDConnector ホストをモデリングします (P. 39)。
3. 管理するセキュア ドメインでデバイスをモデリングします (P. 41)。

ハードウェアの推奨事項

Secure Domain Manager の最適なパフォーマンスを達成するには、これらの推奨事項に従います。

- SpectroSERVER の最適なモデリング容量を維持するには、SpectroSERVER/SDManager インストール コンピュータに 2 つの CPU が必要です。1 つを SpectroSERVER 専用にし、もう 1 つを SDManager の機能にサービスを提供するための専用にします。 SDManager と SpectroSERVER で 1 つのプロセッサを共有し、ネットワーク エレメントを管理しなければならない場合、SpectroSERVER のモデリング容量が 40% 削減されます。
- 展開する各 SDConnector プロセスを実行するための専用のホスト コンピュータを用意することをお勧めします。 SDConnector インストールのシステム要件は SpectroSERVER のみのインストールのシステム要件と同じです。 複数のディスクを設定する場合の特別な要件を除きます。

  注: インストール要件の詳細については、「インストール ガイド」を参照してください。
- SDConnector は 1 対 1 のみで SDManager に接続されます。 それがセットアップの要件である場合、フォールト トレラント SpectroSERVER からの 2 つの SDManager を 1 つの SDConnector に接続できます。 詳細については、「フォールト トレラント環境のプロセスのセットアップ (P. 51)」を参照してください。

SDConnector CPU とメモリの使用率について

SDConnector は、SpectroSERVER がデバイスの管理に使用する CPU 容量の半分を使用します。 SpectroSERVER コンピュータが CPU 合計の 50 パーセントを使用し、すべてのデバイスが SDManager を使用して管理される場合、SDConnector は等しく強力なシステムで CPU 容量のおよそ 25 パーセントを使用します。 主な違いは、SDConnector があまりメモリを使用しないということです。それが SDConnector 専用である場合、RAM は多いに越したことはないですが、512 MB で十分です。

SDConnector プロセスのインストール

Secure Domain Manager 機能を利用し、CA Spectrum による安全なネットワークでデバイスとアプリケーションを管理する前に、安全なネットワークのホスト コンピュータに単一の SDConnector プロセスをインストールします。 Secure Domain Manager は同じホスト コンピュータでの複数の SDConnector プロセスの実行をサポートしません。 SDConnector をインストールする場合、Windows システムの場合は管理者ユーザで、Solaris と Linux システムの場合は root ユーザで実行する必要があります。

注: 任意のプラットフォームで SDConnector プロセスをアップグレードする前に、ベスト プラクティスとして、プロセスを停止し、必要であれば強制終了します。 プロセスを停止または強制終了することで、アップグレード後にプロセスが正しく実行されます。

SDConnector をインストールする方法

1. SDConnector を実行する nonSpectroSERVER ホスト マシンで、プラットフォームに対応する CA Spectrum インストーラを起動します。

   注: インストールには、ご利用の SpectroSERVER と同じ動作環境の SDConnector のみが使用できます。他の動作環境の SDConnector をインストールする必要がある場合は、CA サポートにお問い合わせください。インストーラの起動に関する詳細については、「インストール ガイド」を参照してください。

   ［インストール］ダイアログ ボックスが表示されます。

2. ［CA Secure Domain Connector のインストール］を選択します。

   ［はじめに］ダイアログ ボックスが表示されます。

3. ［次へ］をクリックして、先に進みます。

   使用許諾契約のダイアログ ボックスが表示されます。

4. 使用許諾契約をスクロールさせて読み、使用許諾契約に同意して、［次へ］をクリックします。

   ［インストール場所］ダイアログ ボックスが表示されます。

5. デフォルトのディレクトリに SDConnector をインストールする場合は、［次へ］をクリックします。デフォルトのディレクトリは Windows では C:¥Program Files¥CA¥SDMConnector で、Solaris および Linux では /usr/SDMConnector です。

   デフォルトのフォルダ以外の場所に SDConnector をインストールする場合、［選択］をクリックしてフォルダを選択し、［次へ］をクリックします。［選択］ボタンはローカル インストールの場合のみ表示されます（ローカルではないリモートからのインストールの場合は非表示）。

   注: 名前にスペースがあるディレクトリに SDConnector をインストールすることはできません。

   ［インストール前のサマリ］ダイアログ ボックスが表示されます。

6. ［インストール］をクリックします。

   SPECTRUM_SDM_Connector のインストール ダイアログ ボックスが表示されます。 SDConnector のインストールが完了すると、ステータスは［インストール完了］に変更され、［完了］ボタンが使用できるようになります。

7. ［完了］をクリックします。

   ダイアログ ボックスが閉じます。

8. 初期インストール ダイアログ ボックスの［閉じる］をクリックします。

   このホスト コンピュータに SDConnector がインストールされます。SDConnector はサービスとしてインストールされ、システムが再起動されるたびに自動的に開始します。

   注: また、SDConnector がインストールされたディレクトリにあるインストール ログを確認し、インストールが正常に完了したことを確認できます。

インストール ファイル

インストール プロセス中に作成される以下のディレクトリおよびファイルに注意してください。

SpectroSERVER で

CA Spectrum インストール プロセスにより、SpectroSERVER の *<$SPECROOT>*/SDM ディレクトリに以下の Secure Domain Manager ディレクトリおよびファイルがインストールされます。

cert

このディレクトリは、SDManager に作成する SSL 証明書のリポジトリです。

Logs

このディレクトリには、SpectroSERVER に設定ファイルをインポートするときに生成される出力ログが含まれます。 実行される作業の詳細です。 ログ ファイルには作業と発生するあらゆるエラーが含まれます。

README

このファイルには、SpectroSERVER ホストに Secure Domain Manager を設定する方法の詳細が記載されています。

SDConnector ホスト

SDConnector インストール プロセスにより、SDConnector ホストの SDMConnector ディレクトリに以下のディレクトリおよびファイルがインストールされます。

bin

このフォルダには SDConnector で使用される以下のアイテムが含まれます。

cert

このディレクトリは、SDConnector に作成する SSL 証明書のリポジトリです。

README

このファイルには、SDConnector ホストに SDConnector プロセスを設定する方法の詳細が記載されています。

SdmConnectorService[.exe]

SDConnector の実行可能ファイルです。

証明書の利用

証明書は SDManager と SDConnector の両方にデフォルトでロードされます。 それにより、SSL 暗号化を利用し、安全でないネットワークを介して SDManager と SDConnector のホスト間で転送される ICMP および SNMP（SNMPv1、SNMPv2c、および SNMPv3）のデータの安全を確保できます。ネットワーク環境のすべての SDManager-SDConnector 接続に SSL 暗号化を使用しない場合、SDManager と SDConnector の設定ファイルに nonsecure オプションを含めます。 nosecure オプションの使用方法に関する詳細は、「SDConnector プロセスの設定 (P. 27)」を参照してください。

アップグレード時の古い証明書ファイルの削除

9.*x* より前のバージョンから Secure Domain Manager をアップグレードする場合、古い証明書ファイルを削除します。 古い証明書（9.*x* より前）は、Secure Domain Manager のこのバージョンで使用できません。 以下の証明書ファイルを削除します。これらのファイルは、Secure Domain Manager の以前のリリースの場合、デフォルトでは SDManager ホストの *<$SPECROOT>*/SDM/srconf/mgr ディレクトリにインストールされています。

- snmpricacert.pem： マスタ証明機関
- dsspmastercert.pem： SDManager 証明機関
- dsspremotecert.pem： SDConnector 証明機関

証明書の作成

Secure Domain Manager はデジタル証明書を使用してセキュリティを確保します。デフォルトの証明書は CA Spectrum のインストールで提供されます。サイト固有の証明書は CertGen ツールを使用して作成できます。

デフォルト証明書

デフォルト証明書を使用する場合は、何も操作する必要がありません。すべてのデフォルト ファイルは *<$SPECROOT>*/SDM/cert ディレクトリに存在し、以下のファイルが含まれます。

SDMCA.pem

証明機関。Secure Domain Manager または Secure Domain Connector を使用するコンピュータにこのファイルを配布します。信頼された CA ファイルとして扱うことができます。

SDMCAKey.pem

CA の秘密鍵。証明書を発行するために使用できますが、必ずしもすべてのマシンに配布するべきではありません。

SDMCert.p12

SDMCA.pem によって署名されるアプリケーション証明書。 これは SDManager と SDConnector の間で使用される証明書ファイルです。 信頼に値するコンピュータに注意深く配布する必要があります。そのコンピュータの身元を主張するために使用されます。

CertGen[.exe]

サイト固有の証明機関、鍵ファイル、証明書ファイルを生成するために使用されるプログラム。使用可能な証明書オプションをすべて確認するには CertGen -h を実行します。

openssl[.exe]

SSL プロトコルの OpenSSL オープンソース実装。

サイト固有の証明書

サイト固有の証明書を作成する場合は、ハード ドライブの別の場所にデフォルト証明書ファイル（*.pem と *.p12）を移動させます。 カスタム証明書を作成して展開するには、以下の手順に従います。

サイト固有 CI の作成

より良いセキュリティのためにサイト固有の証明書を作成します。 有資格者のみがアクセスできる単一のコンピュータにこれらの証明書を作成します。 そのコンピュータは SDManager ホストにすることができます。

重要: Secure Domain Manager の SSL 証明書を作成するには、管理者権限またはルート権限が必要です。

次の手順に従ってください:

1. 以下のコマンドを実行し、証明機関証明書とその証明書機関証明書の秘密鍵を作成します。

   ```
   CertGen -t ca -c US
   ```

   組織に必要な証明機関証明書を作成するには、この手順を 1 回だけ実行する必要があります。

   以下のファイルが作成されます。

   SDMCA.pem

   SDMCAKey.pem

   注: Secure Domain Manager に付属するデフォルトの証明機関および鍵ファイルは読み取り専用ファイルです。許可エラーが発生する場合は、ユーザ権限を確認するか、別の場所に SDMCA.pem と SDMCAKey.pem を移動させて、コマンドを再度実行します。

2. 以下のコマンドを実行し、SDManager の証明書を作成します。

   ```
   CertGen -t cert -c <Country Code>
   ```

   SDMCert.01.p12 ファイルが作成されます。

3. （オプション）セキュリティを強化するために、以下のように -p オプションを使用し、証明書とパスワードを生成します。

   ```
   CertGen -t cert -p <password> -c <Country Code>
   ```

   sdc.config ファイルおよび sdm.config ファイルにパスワードを入力します。

4. SDMCert.01.p12 の名前を SDMCert.p12 に変更します。

   新しいサイト固有証明書が使える状態になります。

サイト固有証明書の展開

証明書ファイルを作成した後に、以下のタスクを実行します。

- SDManager ホストおよび SDConnector ホストに証明書ファイルを展開します。
- SDManager ホストで SpectroSERVER を、SDC ホストで SDConnector プロセスを再起動します。

証明書を展開するには、作成した SDMCA.pem ファイルを、SDManager ホスト コンピュータの *<$SPECROOT>*/SDM/cert ディレクトリと、SDManager に接続する SDConnector ホストの SDConnector インストール下の cert ディレクトリにコピーします。管理者またはルートは SDMCert.p12 ファイルを所有する必要があります。

重要: 証明書を追加作成する計画があるコンピュータに SDMCAKey.pem ファイルを保持します。ファイルは認可された人員のみに限定します。このコンピュータは SDManager ホスト コンピュータにすることができますが、要件ではありません。

証明書が展開された後、SDManager ホストの SpectroSERVER と SDC ホストの SDConnector プロセスの両方を再起動します。 SDConnector プロセスの再起動に関する詳細については、「Windows での SDConnector プロセスの開始、停止、再起動 (P. 34)」または「Solaris および Linux での SDConnector プロセスの開始、停止、再起動 (P. 35)」を参照してください。

SDConnector プロセスの設定

このセクションでは、SDConnector 設定ファイル（sdc.config）に指定できる設定オプションについて説明します。 この設定ファイルは起動時に読み取られます。指定されたオプションはそのときに適用されます。sdc.config では、オプションの 1 行のみが受け取られます。 以下は、sdc.config ファイルからのサンプル行です。 SDConnector が SDManager（192.168.0.2）からの接続を承認するということが指定されています。

```
-accept 192.168.0.2
```

SDConnector を設定する方法

1. テキスト エディタを使用して、SDConnector ホスト マシンの SDMConnector¥bin ディレクトリに「sdc.config」という名前のファイルを作成します（すでに存在する場合は、既存のファイルを開きます）。
2. 特定の要件に基づき、ファイルの 1 行に以下のオプションの詳細を追加し、指定します。

   -accept remote_ipaddr:[local_port]

   アドレス *<ip>* およびローカル ポート番号 *<port>* のホストで実行されている SDManager からの接続を承認します。 接続は指定された IP アドレスが開始する必要があります。そうでないと、接続試行は無視されます。

   このオプションが指定された場合、この SDConnector に接続する SDManager の設定ファイル（sdm.config）に、この SDConnector *<IP>* を指定する -remoteconnect オプションを指定する必要があります。また、このオプションが指定された場合、その SDManager には接続（-connect）できません。

   -buffersize *<size>*

   送受信ソケット バッファのサイズをバイト単位で指定します。

   デフォルト： 262,144 （ほとんどの展開では 256k で十分です）

   -certdir *<dir>*

   デフォルト ディレクトリ（/cert）に配置しない場合、SSL 証明書（アプリケーション証明書、秘密鍵、および証明機関証明書）のディレクトリを指定します。

   -nosecure オプションが指定される場合、証明書はアクセスされません。

   -certpassword <passwd>

   証明書パスワードを指定します。 Secure Domain Manager に付属するデフォルト証明書を使用している場合、-certpassword を指定する必要はありません。 デフォルト証明書を使用しない場合、このオプションを使用して証明書パスワードを指定します。 パスワードにはスペースが含まれる場合、それを引用符（"）で囲む必要があります。 CA Spectrum では、アプリケーション証明書のパスワードが暗号化されるものと想定されます。

   注: -certpassword を使用する場合、それは設定ファイルで宣言される最初のオプションである必要があります。

-connect remote_ipaddr:[remote_port]

IP アドレス *<ip>* およびポート *<port>* のホストで実行される SDManager に接続します。 *<port>* が指定されない場合、6844 が想定されます。

このオプションが指定される場合、この SDConnector が接続する SDManager の設定ファイル（sdm.config）に、この SDConnector の IP アドレスを指定する -remoteaccept オプションを指定する必要があります。

このオプションが指定された場合、この SDConnector は指定された SDManager (sdm.config) からの接続を承認（-accept）せず、またはリスン（-listen）しません。

-keepalive *<n>*

ネットワーク接続が依然として有効であることを確認する目的で SDManager または SDConnector が小さなメッセージを送信するときのデフォルトの内部タイムアウト（秒単位）を変更します。SDManager と SDConnector のいずれかが *<n>* の値の 3 倍以内に他方からの応答を受け取らない場合、接続は終了します。

デフォルト： 10 秒

-listen [port]

デフォルトでは、SDConnector は SDManager からの接続要求をポート 6844 でリスンします。ただし、-connect または -accept オプションが指定されている場合、SDConnector はデフォルトでリスンしません。

-listen オプションに指定されたポートは、-accept オプションに指定されたポートに優先します。すなわち、ポートが -listen オプションで指定されれば、そのポートに対してソース IP アドレスの検証は行われません。

注: -listen および -listen6 は相互に排他的です。

-listen6 [local_port]

指定されたポートの IPv6 SDManager からの接続を承認します。

注: -listen および -listen6 は相互に排他的です。

-loglevel fatal|error|warning|info|debug

ログ記録するメッセージのタイプを指定します。

デフォルト： 警告（エラーと致命的も含みます）

-maxlogsize *<n>*

sdmLog.log の最大サイズをメガバイトで設定します。

デフォルト： 5M

最小： 1M

-nosecure

SSL（セキュア ソケット レイヤ）セキュリティを無効にします。これはデフォルトでは有効です。 -connect または -accept エントリの前に -nosecure オプションが使用された場合、SSL はすべての接続で無効です。 そうでない場合、-connect または -accept の各エントリの後に -nosecure オプションを指定できます。オプションはそのエントリだけに関連します。

SSL セキュリティが要求される場合、データ ストリームが暗号化され、相互に暗号認証が実行されます。SDManager と SDConnector のいずれかがセキュリティを要求する場合、セキュリティはその接続で必須です。

-trappoll *<n>*

トラップを *<n>* 秒おきに SDManager に転送します。

デフォルト： 15 秒

-withfips

FIPS モードで実行するように指定します。 FIPS モードはデフォルトでオフです。

注: 空の sdc.config が作成された場合、SDConnector はポート 6844 で SDManager からの接続をリスンします。SDManager が接続を開始します。

3. ファイルを保存して終了します。

SDConnector が設定されました。

注: sdc.config ファイルを更新するたびに、SDConnector プロセスを再起動する必要があります。

SDManager プロセスの設定

SDManager 設定ファイル（sdm.config）により、SDManager プロセスの動作設定が指定されます。デフォルトでは、SDManager プロセスは無効です。sdm.config ファイルを作成し、ニーズに基づいてそれを設定するまで、SDManager プロセスは動作しません。初めて sdm.config ファイルを設定した後で、またはその設定を変更するたびに、CA Spectrum にそれをインポートし、SpectroSERVER で SDManager 設定を有効にする必要があります。 詳細は、「SDManager 設定ファイルのインポート (P. 37)」を参照してください。 SpectroSERVER の起動前または起動後に sdm.config を設定できます。

sdm.config では、オプションの 1 行のみが受け取られます。 以下は、sdm.config のオプションのサンプル行です。 2 つの SDConnectors（172.24.148.196 と 172.19.32.199）への接続（-remoteconnect）を指定しています。

```
-remoteconnect 172.24.148.196 -remoteconnect 172.19.32.199
```

注: -nosecure オプションを使用して SDConnector プロセスの 1 つまたは複数を起動する場合、対応する -remoteconnect/-remoteaccept エントリの同じ -nosecure オプションを SDManager オプションに指定するか、単純にすべての -remoteconnect/-remoteaccept エントリの前に -nosecure を指定して、すべての接続の SSL を無効にします。

SDManager を設定する方法

1. テキスト エディタを使用して、SpectroSERVER ホスト マシンの *<SPECROOT>*¥SDM ディレクトリに「sdm.config」という名前のファイルを作成します（すでに存在する場合は、既存のファイルを開きます）。
2. 特定の要件に基づき、ファイルの 1 行に以下のオプションの詳細を追加し、指定します。

   -apiclientport [port]

   API クライアント接続をリスンするようにポートを設定します。このパラメータはスタンドアロン SDManager プロセスのみに適用されます。

   -buffersize *<size>*

   送受信ソケット バッファのサイズをバイト単位で指定します。

   デフォルト： 262,144 （ほとんどの展開では 256k で十分です）

-certdir *<dir>*

デフォルト ディレクトリ（/cert）に配置しない場合、SSL 証明書（アプリケーション証明書、秘密鍵、および証明機関証明書）のディレクトリを指定します。

-nosecure オプションが指定される場合、証明書はアクセスされません。

-certpassword <passwd>

証明書パスワードを指定します。 Secure Domain Manager に付属するデフォルト証明書を使用している場合、-certpassword を指定する必要はありません。 デフォルト証明書を使用しない場合、このオプションを使用して証明書パスワードを指定します。 パスワードにはスペースが含まれる場合、それを引用符（"）で囲む必要があります。 CA Spectrum では、アプリケーション証明書のパスワードが暗号化されるものと想定されます。

注: -certpassword を使用する場合、それは設定ファイルで宣言される最初のオプションである必要があります。

-clientServiceThreads *<n>*

要求を処理するクライアントごとのスレッド数を設定します。 このパラメータはスタンドアロン SDManager プロセスのみに適用されます。

-keepalive *<n>*

ネットワーク接続が依然として有効であることを確認する目的で SDManager または SDConnector が小さなメッセージを送信するときのデフォルトの内部タイムアウト（秒単位）を変更します。

デフォルト： 10 秒

SDManager と SDConnector のいずれかが *<n>* の値の 3 倍以内に他方からの応答を受け取らない場合、接続は終了します。

-loglevel fatal|error|warning|info|debug

ログ記録するメッセージのタイプを指定します。

デフォルト： 警告（エラーと致命的も含みます）

-maxapiconnections *<n>*

API クライアント接続の最大数を *<n>* に設定します。このパラメータはスタンドアロン SDManager プロセスのみに適用されます。

-maxlogsize *<n>*

sdmLog.log の最大サイズをメガバイトで設定します。

デフォルト： 5M

最小： 1M

-nosecure

SSL （セキュア ソケット レイヤ）機能を無効にします。これはデフォルトでは有効です。 -remoteconnect または -remoteaccept エントリの前に -nosecure オプションが使用される場合、SSL はすべての接続で無効です。 そうでない場合、-remoteconnect または -remoteaccept の各エントリの後に -nosecure オプションを指定できます。オプションはそのエントリだけに関連します。

SSL セキュリティが要求される場合、データ ストリームが暗号化され、相互に暗号認証が実行されます。SDManager と SDConnector のいずれかがセキュリティを要求する場合、セキュリティはその接続で必須です。

-remoteaccept (-rema) remote_ipaddr[:local_port]

アドレス *<ip>* およびローカル ポート番号 *<port>* のホストで実行されている SDConnector からの接続を承認します。 SDConnector のパブリック IP アドレスを指定する必要があります。

このオプションが指定された場合、この SDManager に接続する SDConnector の設定ファイル（sdc.config）に、この SDManager の IP アドレスを指定する -connect オプションを指定する必要があります。 また、このオプションが指定された場合、SDConnector （sdc.config）には接続（-remoteconnect）できません。

-remotebackup (-remb) remote_ipaddr[:remote_port]

SDConnector のパブリック IP アドレスを使用して、フォールト トレラント Secure Domain Manager セットアップでバックアップ SDConnector を指定します。 詳細については、「フォールト トレラント環境のプロセスの設定 (P. 51)」を参照してください。

-remoteconnect (-remc) remote_ipaddr[:remote_port]

IP アドレス *<ip>* および *<port>* のホストで実行される SDConnector に接続します。*<port>* が指定されない場合、6844 が想定されます。SDConnector のパブリック IP アドレスを指定する必要があります。

このオプションが指定される場合、この SDManager が接続する SDConnector の設定ファイル（sdc.config）に、この SDManager を指定する -accept オプションまたは -listen オプションを指定する必要があります。 また、このオプションが指定された場合、この設定ファイルに指定された SDConnector からの接続を承認（-remoteaccept）できません。

-withfips

FIPS モードで実行するように指定します。 FIPS モードはデフォルトでオフです。 FIPS モードから非 FIPS に、またはその逆に設定を変更する場合、アプリケーションを再起動する必要があります。

注: sdm.config ファイルが空の場合、SDManager プロセスは無効です。

3. sdm.config ファイルを保存して閉じます。

   SDManager が設定されます。

詳細情報:

SDManager 設定ファイルのインポート (P. 37)

Windows での SDConnector プロセスの開始、停止、再起動

サービス マネージャを使用し、SDConnector プロセスを開始、停止、または再起動します。 SDConnector プロセスは「Secure Domain Connector」という名称の下にリスト表示されます。

Solaris および Linux での SDConnector プロセスの開始、停止、再起動

SDConnector プロセスを開始するには、root としてログインし、コマンドライン コンソールを開いて以下のコマンドを入力します。

```
$ cd /etc/init.d
```

```
$ ./sdmconnector start
```

SDConnector プロセスを停止するには、**./sdmconnector stop** コマンドを発行します。

SDConnector プロセスを再起動するには、**./sdmconnector restart** コマンドを発行します。

第 3 章: Secure Domain Manager の使用

この章では、SDManager 設定ファイル（sdm.config）を CA Spectrum にインポートし、セキュア ドメインで SDConnector のホストおよびデバイスをモデリングする方法について説明します。 この章ではまた、Secure Domain Manager コンポーネントを見つけるために使用される OneClick ツールについて説明します。 これらのコンポーネントはセキュア ドメインのデバイスに ping を実行するために使用されます。 デバイスに ping を実行し、デバイス MIB を表示したり、SDManager および SDConnector モデルに関する情報を表示したりします。

このセクションには、以下のトピックが含まれています。

SDManager 設定ファイルのインポート (P. 37)
SDConnector ホストのモデリング (P. 39)
セキュア ネットワーク ドメインのデバイスのモデリング (P. 41)
Secure Domain Manager 検索へのアクセス (P. 45)
セキュア ドメインのデバイス アクセシビリティの確認 (P. 45)
セキュア ドメインのデバイス MIB の表示 (P. 45)
SDManager モデル情報ビュー (P. 47)
SDConnector モデル情報ビュー (P. 49)

SDManager 設定ファイルのインポート

Secure Domain Manager 製品で OneClick を使用する前に、および SDManager 設定を更新するたびに sdm.config ファイルを CA Spectrum にインポートします。 sdm.config パラメータの設定に関する詳細については、「SDManager プロセスの設定 (P. 31)」を参照してください。

注: SDConnector ホストのモデルを作成する前または後に、SDManager 設定ファイルをインポートできます。 ただし、SDConnector ホストのモデルを作成する前に sdm.config ファイルをインポートする場合、CA Spectrum は自動的に SDConnectorProcess モデル タイプとしてホストをモデリングします。 モデリング オプションに関する詳細は、「SDConnector ホストのモデリング (P. 39)」を参照してください。 これには、Pingable および Host_Device モデル タイプとして SDConnector をモデリングする方法が記載されています。

SDManager 設定ファイルをインポートする方法

1. OneClick コンソールの［ナビゲーション］パネルで［Secure Domain Manager］をクリックします。
2. ［コンポーネント詳細］パネルの［情報］タブをクリックし、［設定］サブビューを展開します。
3. ［インポート］をクリックします。

   ［Secure Domain Manager 設定のインポート］確認ダイアログ ボックスが表示されます。
4. ［はい］をクリックし、SDManager 設定ファイル（sdm.config）をインポートすることを確認します。

   ［Secure Domain Manager 設定のインポート］確認ダイアログ ボックスに、インポートが正常に開始したかどうかが示されます。 このダイアログ ボックスにはまた、インポートが動作したかどうかを判断できる出力ログを確認するための情報が提供されます。SDM/Logs ディレクトリのインポート ログ ファイルはトラブルシューティング情報を提供します。 この情報は、インポートが失敗した後にエラーを修正するために使用されます。
5. ［OK］をクリックします。

   設定ファイルが正しくインポートされている場合、［Secure Domain Manager ステータス］フィールドに［設定済み］が表示されます。 SDManager と SDConnector の間の接続の確立方法を定義する引数を含まない sdm.config ファイルがインポートされた場合、SDManager は無効であり、［Secure Domain Manager ステータス］フィールドに［未設定］が表示されます。

   注: SpectroSERVER が実行されていないときに sdm.config ファイルが編集された場合、SpectroSERVER は起動時に新しい sdm.config ファイルを自動的にインポートします。 最新のログ ファイルを確認することで、インポートが成功したかどうかを確認できます。

SDConnector ホストのモデリング

［OneClick トポロジ］ビューで［タイプ別モデリング］オプションを使用し、以下の 3 つのモデル タイプの 1 つとして SDConnector ホスト コンピュータをモデリングします。

SDConnectorProcess

SDConnectorProcess モデル タイプが SDConnector のデフォルト モデル タイプです。 このモデル タイプではデバイス ステータスを管理できませんが、OneClick Secure Domain Manager モデル階層で表されるホスト コンピュータを参照できます。また、「SDConnector モデル情報ビュー (P. 49)」で説明するビューにアクセスできます。

注: SDConnector ホスト モデルには意味のある名前を使用し、ホストを明確に識別します。 モデル名が OneClick の［Secure Domain Manager］ビューに表示されます。

Host_Device

ホスト コンピュータが SNMP エージェントを実行している場合は、Host_Device モデル タイプを使用します。

Pingable

ホスト コンピュータが ICMP だけをサポートする場合は、Pingable モデル タイプを使用します。

Host_Device と Pingable モデル タイプのいずれかを使用する場合、ホスト コンピュータのステータスを監視できます。 Host_Device または Pingable モデルとして SDConnector ホストをモデリングし、CA Spectrum 障害分離機能を活用するための詳細については、「SDConnector モデリングおよび CA Spectrum 障害分離 (P. 40)」を参照してください。

SDConnector モデリング考慮事項

- デフォルトでは、SDManager 設定ファイルを初めてインポートする前にコンピュータのモデルを作成していない場合、CA Spectrum は自動的に SDConnectorProcess モデル タイプとして SDConnector ホスト コンピュータをモデリングします。
- Pingable または Host_Device としてホストをモデリングする場合は、インポートの前に、選択したタイプとしてホストをモデリングします。インポート後は、SDConnectorProcess モデルを破棄します。 次に、Pingable または Host_Device としてホストをモデリングします。

  注: ［IP で作成］オプションを使用して、最初に既存の SDConnectorProcess モデルを破壊することなく、SDConnector ホストを表すモデルを作成する場合、CA Spectrum は SDConnectorProcess をコピーして、［IP で作成］オプションの呼出元の［トポロジ］ビューにコピーします。
- OneClick の SDConnector ホスト モデルを破棄しても、CA Spectrum が実際の SDConnector をデバイス通信に使用するのを防止することにはなりません。 SDConnector は SDManager 設定を再インポートすることによりのみ破棄できます（SDConnector を削除するために sdm.config ファイルを編集した後に）。
- 誤って SDConnectorProcess モデルを破棄した場合、次に SDManager 設定ファイルをインポートしたときに、CA Spectrum はモデルを再作成します。 Pingable または Host_Device のモデルを破棄した場合、次に SDManager 設定ファイルをインポートしたときに、CA Spectrum は SDConnectorProcess モデルを作成します。 Pingable または Host_Device モデルを復元する場合は、明示的にモデルを再作成し、次に設定ファイルをインポートします。

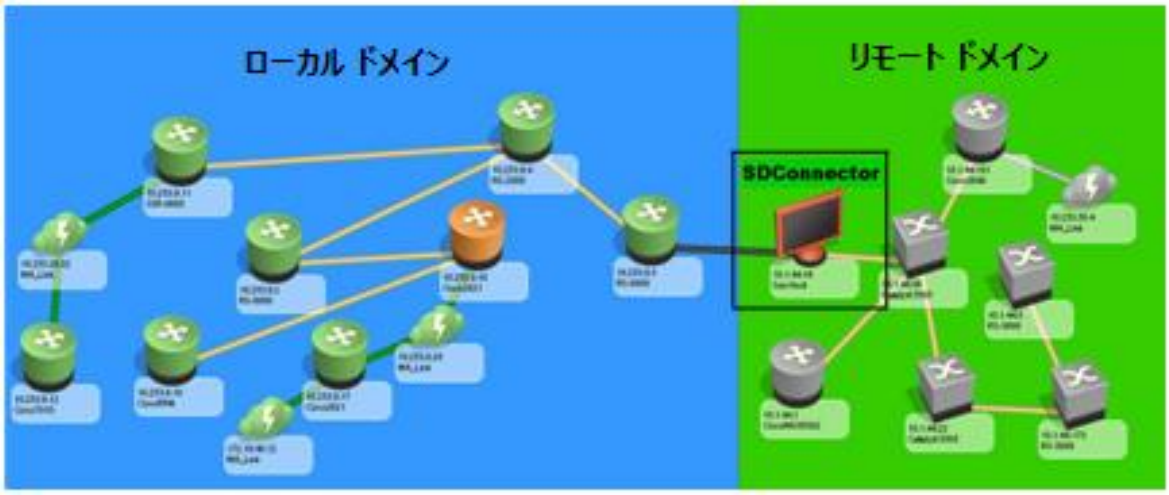
SDConnector モデリングおよび CA Spectrum 障害分離

「SDConnector ホストのモデリング (P. 39)」に記載されているように、SDConnector をモデリングするときは以下のいずれかのモデル タイプを選択できます。

- SDConnectorProcess
- Host_Device
- Pingable

SDConnector ホストは、Host_Device または Pingable のモデル タイプとしてモデリングすることをお勧めします。 これらのモデル タイプを利用すると、リモートの SDConnector プロセスが停止した場合、または接続を失った場合に、CA Spectrum 障害分離が正しく動作します。 CA Spectrum は、停止の原因を SDConnector ホスト モデルに分離し、実質的に未解決の障害アラームを排除します。

SDConnector ホストは、通常はネットワークの端にあるスイッチに接続されています。 ただし、論理的には、パブリック ドメインとセキュア ドメイン領域の間をつないでいます。適宜モデリングしてください。パブリック ドメインおよびセキュア ドメイン領域の間のトラフィックをルーティングしているデバイスの 2 つのモデル間に SDConnector ホスト モデルを配置します。 以下はこの接続の図です。SDConnector を Host_Device モデルとして示しています。



セキュア ネットワークドメインのデバイスのモデリング

SDConnector ホストをモデリングしたら、SDConnector ホストが置かれているセキュア ドメインで管理するネットワーク デバイスをモデリングします。 OneClick の［IP アドレスでモデルを作成］オプションまたは［ディスカバリ］オプションを使用して、ネットワーク デバイスを一度に 1 つずつモデリングします。 モデルは［トポロジ］ビューのあらゆる場所に配置できます。 モデルの作成が完了したら、CA Spectrum は SDConnector プロセスを使用してモデルと通信できます。

IP によるモデル作成

OneClick の［IP アドレスでモデルを作成］オプションを使用し、セキュアドメインの各デバイスをモデリングします。

注: OneClick のモデリングに関する詳細については、「IT インフラストラクチャのモデリング/管理 - 管理者ガイド」を参照してください。

IP アドレスによるモデリングオプションを使用してセキュア ドメインのデバイスをモデリングする方法

1. ［トポロジ］ビューの［IP で作成］オプションをクリックします。

   ［IP アドレスでモデルを作成］ダイアログ ボックスが開きます。

2. ［ネットワーク アドレス］フィールドにモデリングするデバイスのネットワーク アドレスを入力します。

3. ［セキュア ドメイン］ドロップダウン リストから、SDConnector を実行しているホストの IP アドレス、またはモデリングしているデバイスが置かれているセキュア ドメインの SDConnector ホストに設定されている名前を選択します。

   注: OneClick のホスト モデル名を変更することで、SDConnector ホストのセキュア ドメイン名を指定できます。選択オプションとしてセキュア ドメイン名を有効にする方法については、「SDManager モデル情報ビュー (P. 47)」を参照してください。

4. ［SNMP 通信オプション］セクションで管理するデバイスと互換性のある SNMP バージョンを選択します。

5. ［OK］をクリックします。

ディスカバリ

OneClick の［ディスカバリ］オプションを使用し、SDConnector ホストのあるセキュア ドメインのデバイスをすべて検出し、モデリングします。IP アドレスが重複するデバイスを検出するときは、以下の点に注意してください。

- ディスカバリごとに使用できる SDConnector は 1 つだけです。
- レイヤ 2 マッピングを使用できますが、その有効性は［ソース アドレス］および［スパニング ツリー］テーブルの正確性に依存します。

- ［プロトコル オプション］設定：
  - レイヤ 3 自動ディスカバリ マッピングを使用しないでください。［プロトコル オプション］ダイアログ ボックスで［IP アドレス テーブル］および［IP ルート テーブル］を選択解除します。
  - Cisco または Nortel 環境固有のディスカバリ プロトコルを使用しないでください。これらのプロトコルでは近隣の関係を伝えるために IP アドレスが使用されるためです。［プロトコル オプション］ダイアログ ボックスで［専用ディスカバリ プロトコル］を選択解除します。
  - Pingable マッピングを使用しないでください。［プロトコル オプション］ダイアログ ボックスで Pingable の［ARP テーブル］を選択解除します。

SDConnector ホストを使用したデバイスの検出

次の手順に従ってください:

1. メイン メニューで［ツール］-［ユーティリティ］-［ディスカバリ コンソール］をクリックします。

   ディスカバリ コンソールが表示されます。

2. デバイスをモデリングするセキュア ドメインに対してディスカバリ設定に入力します。

   注: ディスカバリ設定の詳細については、「IT インフラストラクチャのモデリング/管理 - 管理者ガイド」を参照してください。

3. ［設定］タブの［詳細オプション］をクリックします。

   ［詳細オプション］ダイアログ ボックスが表示されます。

4. ［ディスカバリ オプション］セクションで、［セキュア ドメイン］ドロップダウン リストから、このセキュア ドメインで SDConnector を実行するホストの IP アドレス、またはセキュア ドメインに指定されている名前を選択します。

   注: OneClick のホスト モデル名を変更することで、SDConnector ホストのセキュア ドメイン名を指定できます。セキュア ドメイン名を選択オプションとして有効にする方法については、「SDManager モデル情報ビュー (P. 47)」を参照してください。

5. ［OK］をクリックします。

   ［詳細オプション］ダイアログ ボックスが閉じられ、変更が保存されます。

6. ［ディスカバリ コンソール］の［ディスカバリ］をクリックします。

   設定したディスカバリが実行されます。ディスカバリの後、その対応する SDConnector ホスト アイコンの［Secure Domain Connector デバイス テーブル］にリスト表示されるデバイスをすべて表示します。

   注: SDConnectorProcess モデルを使用して、リモート SDConnector プロセスを実行するホスト マシンをすでにモデリングしている場合、ホストが存在するネットワーク領域でディスカバリを実行すると、ディスカバリは Host_Device または Pingable モデルを使用して追加のモデルを作成することがあります。その場合、重複するモデルを削除します。あるいは、作成前にフィルタを設定し、そのモデルをディスカバリ結果から除外することができます。

デバイス セキュアドメイン メンバシップの保守について

NAT 環境では、複数の SDConnector が同じ IP 範囲の管理に使用されます。重複する IP 範囲が存在する場合、CA Spectrum は各デバイスを管理する必要がある SDConnector を決定できません。そのため、その情報を指定します。

CA Spectrum で新しいデバイスを検出またはモデリングする場合、OneClick の［IP で作成］ビューまたは OneClick ディスカバリを使用してセキュア ドメインを設定できます。既存のデバイス モデルのセキュア ドメインを更新するには、OneClick 属性エディタを使用し、［セキュア ドメイン アドレス］属性を編集します。これにより、自動的にセキュア ドメイン名が更新されます。新しい SDManager 設定ファイル（sdm.config）が CA Spectrum にインポートされると、古いセキュア ドメインに割り当てられたすべての既存デバイスもそれに割り当てられます。そのようなモデルには赤いアラームが生成される可能性があります。

Secure Domain Manager 検索へのアクセス

OneClick にはさまざまな Secure Domain Manager 検索オプションが事前定義されています。

Secure Domain Manager の検索オプションにアクセスするには、OneClick コンソールの［ロケータ］タブの［Secure Domain Manager］フォルダを展開します。

使用可能な事前定義済みの Secure Domain Manager 検索が表示されます。

セキュア ドメインのデバイス アクセシビリティの確認

OneClick Ping メニュー オプションを使用し、セキュア ドメインに置かれているデバイスに ping を実行することにより、デバイスがアクセス可能かどうかを判断します。

注: ping に成功しても、セキュア ドメインの ping を実行されたデバイスが返したバイトの数が表示されることはありません。

セキュア ドメインのデバイス アクセシビリティを確認するには、OneClick コンソールでアクセシビリティを評価するデバイスを右クリックし、［Ping］をクリックします。

［Ping］ダイアログ ボックスが開き、ping 要求の結果をリスト表示します。例：

```
Secure reply from 10.254.1.5: icmp_seq=4. time =140. ms
```

このデバイスがセキュア ドメインになければ、結果は以下のように表示されます。

```
64 bytes from 10.254.1.5: icmp_seq=4. time =140. ms
```

セキュア ドメインのデバイス MIB の表示

MIB ツールによりセキュア ドメインのデバイス MIB を表示します。 最初に、デバイスが置かれているセキュア ドメインの SDConnector を指定します。 以下の手順で SDConnector を指定する方法について説明します。

注: MIB ツールの使用方法の詳細については、「認定ユーザ ガイド」を参照してください。

次の手順に従ってください:

1. MIB ツールで調査するデバイスを選択します。
2. デバイスを右クリックし、［ユーティリティ］-［MIB ツール］を選択します。

   ［MIB ツール］が開きます。 ［接続条件］には、デバイスの選択した SNMP 接続情報がすでに入力されています。 MIB ツールはデバイスへの接続を試みます。

   MIB ツールがデバイスに接続できない場合、エラー メッセージが表示され、［接続ステータス］インジケータがレッドで表示されます。

   MIB ツールがデバイスに接続できた場合、［接続ステータス］インジケータはグリーンで表示されます。

   さらに MIB ツール データベースの取得とロードの進捗を示すステータス ダイアログ ボックスが表示されます。
3. ［接続条件］セクションの［詳細オプション］をクリックします。

   ［MIB ツール: 詳細オプション］ダイアログ ボックスが表示されます。
4. ［セキュア ドメイン］ドロップダウン リストから該当するセキュアドメインを選択します。
5. ［OK］をクリックします。

   ［詳細オプション］ダイアログ ボックスが閉じられ、変更が保存されます。
6. ［接続条件］セクションの［接続］をクリックし、MIB ツールがデバイスに接続できることを確認します。
7. MIB ツールを閉じます。

   MIB ツールが閉じられると、デバイスの SDConnector が指定されています。

SDManager モデル情報ビュー

［コンポーネント詳細］パネルの［情報］タブは、以下のセクションの選択された SDManager モデルに関する情報およびその設定管理を提供します。

一般情報

［一般情報］セクションは、そのモデル クラスやセキュリティ文字列など、Secure Domain Manager モデルに関する標準情報を提供します。

設定

［設定］セクションには以下のコンテンツが含まれます。

インポート

CA Spectrum に SDManager 設定ファイル（sdm.config）をインポートします。

Secure Domain Manager ステータス

SDManager の設定ステータスを以下のように示します。

- **設定済み：** ファイルが正常にインポートされたことを示します。
- **未設定：** カスタムまたは編集された sdm.config ファイルがインポートされていないこと、引数のない sdm.config ファイルがインポートされたこと、エラーを含む sdm.config ファイルがインポートされたことのいずれかを示します。

セキュアドメイン表示オプション

CA Spectrum で SDConnector ホスト（およびそのドメイン）または SDConnector ホスト IP アドレスの識別に使用される名前を表示するかどうかを指定します。 ドロップダウン リストから［セキュアドメイン名の表示］と［セキュア ドメイン アドレスの表示］のいずれかを選択できます。 これにより、すべての OneClick ビューで使用される SDConnector 識別子のタイプが決まります。

ローカル ドメイン

ローカルで管理されるモデル（セキュア ドメインに含まれていないモデル）の［セキュア ドメイン］列に表示されるテキストを指定します。

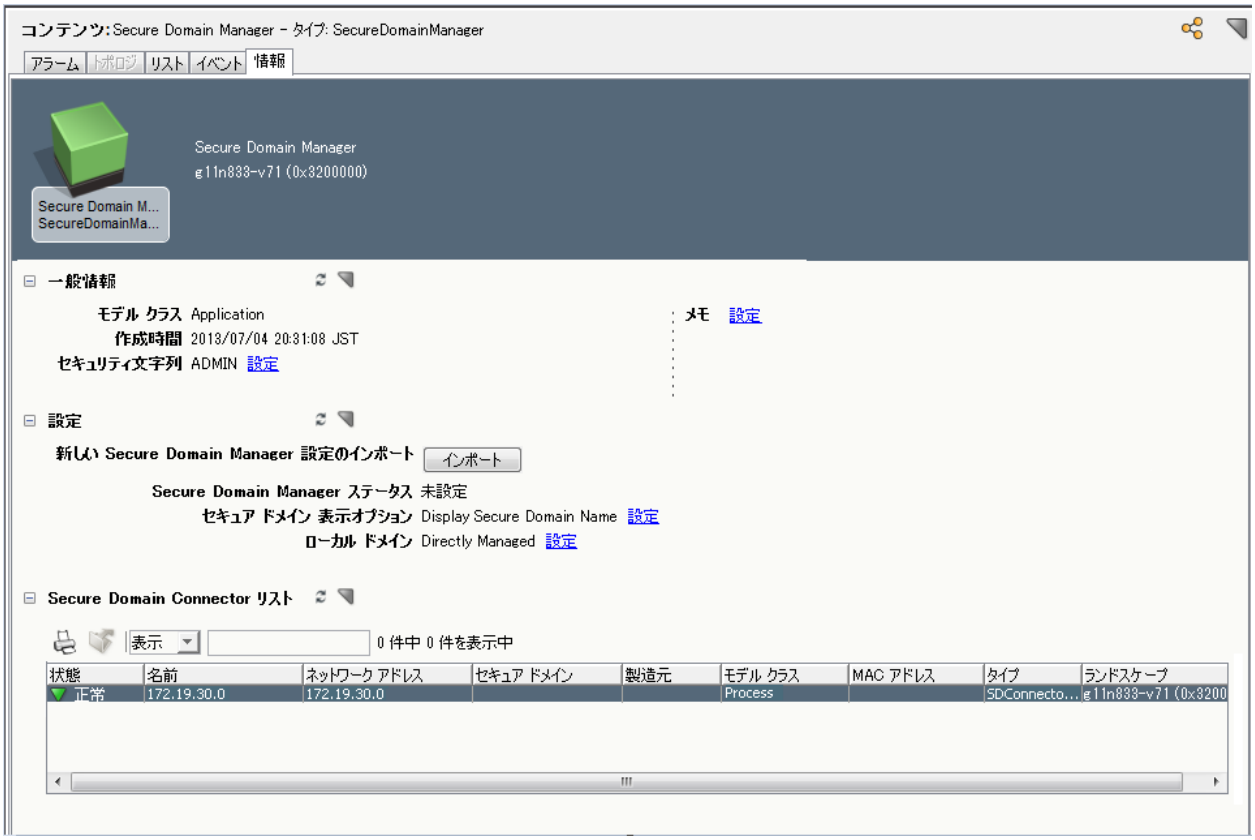
デフォルト： 直接管理

注：［セキュア ドメイン］列は、Secure Domain Manager がインストールされている場合に限り、OneClick リスト ビューに表示されます。

Secure Domain Connector リスト

リモート ネットワーク領域の SDConnector プロセスを現在実行しているホスト マシンをすべて表示します。

以下のイメージは、選択された SDManager モデルの［コンポーネント詳細］パネルのサンプルです。



詳細情報:

SDManager 設定ファイルのインポート (P. 37)

SDConnector モデル情報ビュー

［コンポーネント詳細］パネルにある［情報］タブには、選択された SDConnector に関する情報があります。［一般情報］および［SPECTRUM モデリング情報］カテゴリには、SDConnector モデルに関する標準情報があります。以下のサブセクションを含む［Secure Domain Connector］セクションもあります。

Secure Domain Connector デバイス テーブル

［Secure Domain Connector デバイス テーブル］には、選択された SDConnector によって管理されるすべてのデバイスがリスト表示されます。 また、デバイスの一覧を印刷、エクスポート、フィルタすることができます。 このリストにあるデバイスの［名前］ハイパーリンクをクリックすると、［トポロジ］ビューのそのデバイスに直接移動できます。

第 4 章: フォールトトレラント環境のプロセスのセットアップ

この章では、フォールト トレラント SpectroSERVER 環境のプライマリとバックアップの SpectroSERVER にある SDManager に接続するように SDConnector をセットアップする方法について説明します。 この章ではまた、プライマリとバックアップの SDConnector をセットアップする方法について説明します。

このセクションには、以下のトピックが含まれています。

フォールト トレラント SpectroSERVER 環境での SDManager のセットアップ (P. 51)
フォールト トレラント SDConnector のセットアップ (P. 52)

フォールトトレラント SpectroSERVER 環境での SDManager のセットアップ

フォールト トレラント SpectroSERVER 環境で、SDManager をプライマリ SpectroSERVER とバックアップ SpectroSERVER の両方にインストールします。この SDManager と通信する SDConnector はそれぞれプライマリとバックアップの SpectroSERVER に接続するように設定されます。 プライマリ SpectroSERVER が失敗した場合、バックアップ SpectroSERVER は各 SDConnector との通信を引き継ぎます。

次の手順に従ってください:

1. 管理する各セキュア ドメインに SDConnector を展開します。

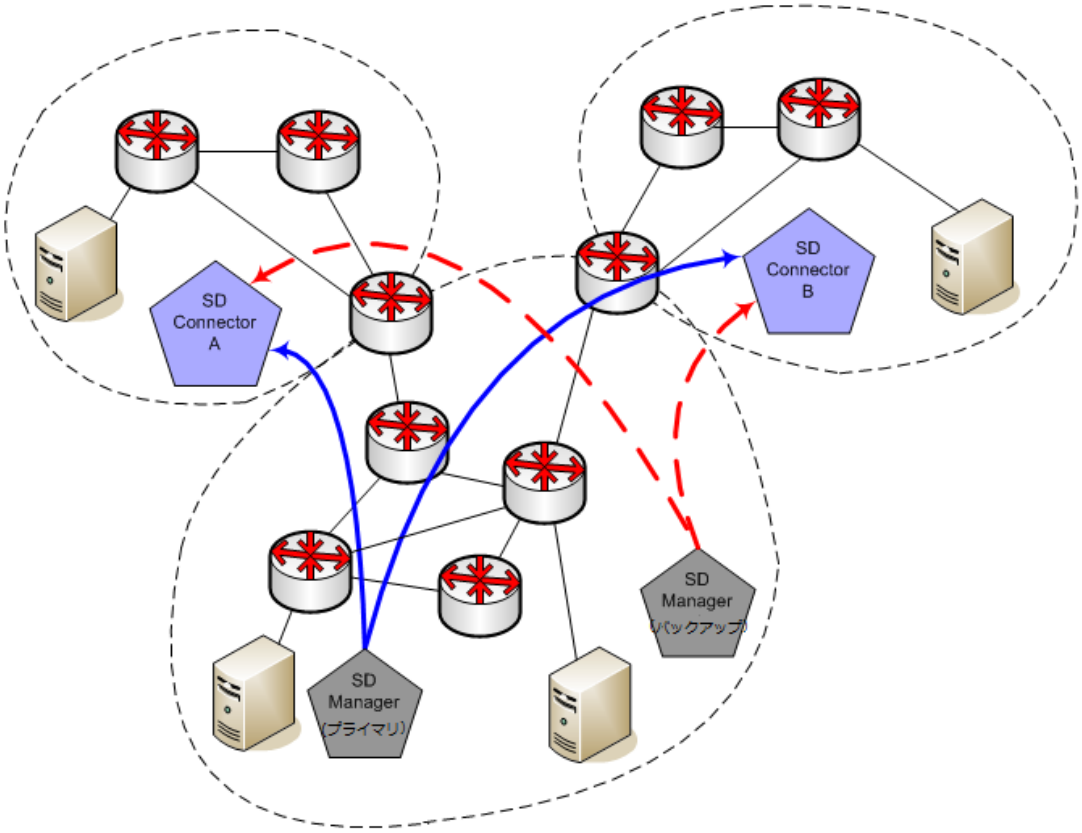
   注: SDConnector を展開する方法の詳細な手順については、「Secure Domain Manager プロセスのインストールおよび設定 (P. 19)」を参照してください。

2. プライマリ SpectroSERVER とバックアップ SpectroSERVER の両方からの接続を承認するように各 SDConnector を設定します。 たとえば、172.24.1.2 と 172.24.3.4 にそれぞれ接続する場合 :

   ```
   -accept 172.24.1.2 -accept 172.24.3.4
   ```

フォールト トレラント SpectroSERVER（SDManager）

以下は、プライマリ SDManager とバックアップ SDManager の両方に 2 つの SDConnector を接続する仕組みを示した図です。



sdm.config の両方の SDManager の設定：

```
-remoteconnect <SDConnector A の IP> -remoteconnect <SDConnector B の IP>
```

sdc.config の両方の SDConnector の設定：

```
-accept <プライマリ SDManager の IP> -accept <バックアップ SDManager の IP>
```

フォールト トレラント SDConnector のセットアップ

Secure Domain Manager は SDConnector 単位でバックアップ機能をサポートします。バックアップ SDConnector は、単なるデバイスの集合ではなく、プライマリ SDConnector が管理するデバイスをすべて管理できる必要があります。

CA Spectrum にバックアップ設定をインポートしても、バックアップ SDConnector は自動的にモデリングされません。 プライマリ SDConnector が停止した場合、バックアップ機能が*透過的に*引き継ぎます。 プライマリ SDConnector の停止は視覚的に表示されません。 また、バックアップはモデリングされていないため、OneClick コンソールの［IP アドレスでモデルを作成］または MIB ツールの［ディスカバリ設定］ビューに表示されません。

次の手順に従ってください:

1. 管理する各リモート ドメインのプライマリとバックアップの両方の SDConnector を展開します。

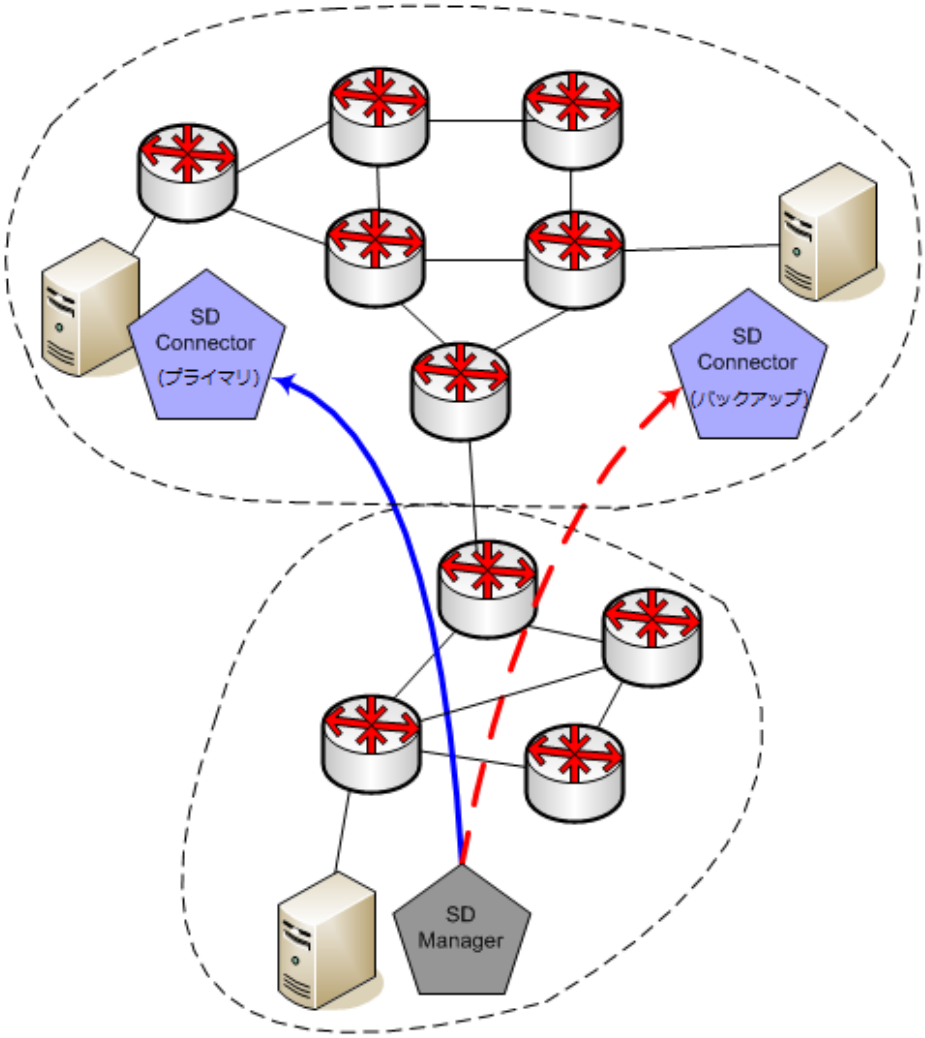
   注: SDConnector を展開する方法の詳細な手順については、「Secure Domain Manager プロセスのインストールおよび設定 (P. 19)」を参照してください。

2. 以下の例のように sdm.config ファイルを変更し、プライマリとバックアップの SDConnector に接続するように SDManager を設定します。

   `-remoteconnect <プライマリ SDC の IP> -remotebackup <バックアップ SDC の IP>`

フォールト トレラント SDConnector

以下は、単一の SDManager に接続された 2 つの SDConnector を示す図です。



sdm.config の SDManager の設定：

```
-remoteconnect <プライマリ SDConnector の IP> -remotebackup <バックアップ
SDConnector の IP>
```

sdc.config の両方の SDConnector の設定：

```
-accept <SDManager の IP>
```

付録 A: Secure Domain Manager のトラブルシューティング

このセクションでは、Secure Domain Manager に潜在するいくつかの問題とその解決策について説明します。

このセクションには、以下のトピックが含まれています。

エラー メッセージ (P. 55)
ポートの競合 (P. 56)
インストール問題 (P. 56)

エラー メッセージ

このセクションでは、Secure Domain Manager のエラー メッセージについて説明します。SDManager エラーは SDManager.out ファイルに表示されます。SDConnector エラーは端末の画面に表示されます。

無効な証明書エラー

Linux、Solaris、および Windows で有効

問題の状況:

以下の SDConnector エラー メッセージは、証明書またはセキュリティ設定に不一致が見つかった場合に表示されます。

`SdmEtpkiConnectEndpoint run()` 無効なソケット セキュリティ。 ホストに対して接続が試行されません。

証明書およびセキュリティ設定が正しいことを確認してください。

解決方法:

SSL が展開されているマシンに一致する証明書があることを確認します。

ポートの競合

SDConnector にカスタム SNMP トラップ ポートが必要です

Linux、Solaris、および Windows で有効

SDConnector が SNMP トラップをリスンするトラップ ポートを変更する必要がある場合は、カスタム リスニング ポートを設定します。

注: 以下の手順では、ポート 951 が新しいカスタム リスニング ポートの例として使用されています。

次の手順に従ってください:

1. 以下のように sdc.rc ファイルを変更し、カスタム ポートのトラップをリスンする SDConnector を設定します。

   ```
   snmp_trap_port = 951
   ```

2. コンピュータを再起動し、SDConnector プロセスを再起動します。

   これで、SDConnector がポート 951 のトラップをリスンします。

インストール問題

一部の Windows インストールで、SDConnector サービスがインストールされません。または、インストールされていても起動しません。その場合、手動で SDConnector サービスを Windows にインストールします。

次の手順に従ってください:

1. コマンド プロンプトから以下のディレクトリに移動します。

   ```
   <SDC Install directory>/bin
   ```

2. 以下のコマンドを実行します。

   ```
   SdmConnectorService.exe --install
   ```

3. Services ウィンドウからサービスを起動するか、以下のコマンドを実行します。

   ```
   SdmConnectorService.exe --start
   ```