CHAPTER 2

システム要件

この章では、HA または DR 環境に Security Manager をインストールするための参照コンフィギュレーションについて説明します。この章は、次の内容で構成されています。

（注） 各種のハードウェアのセットアップを使用したさまざまなコンフィギュレーションが存在します。該当する Microsoft ハードウェア互換性リスト（HCL）および Symantec/Veritas ハードウェア互換性リスト（HCL）を参照してください。

（注） 当社は、Security Manager 用として指定されたサード パーティ製ハードウェアおよびソフトウェア プラットフォームの入手性を可能な限り確認しますが、当社の管理の及ばないサード パーティ ベンダー製品の入手性または変更により、システム要件の変更や修正を行う権利を留保します。

単一ノード サイトのハードウェア要件

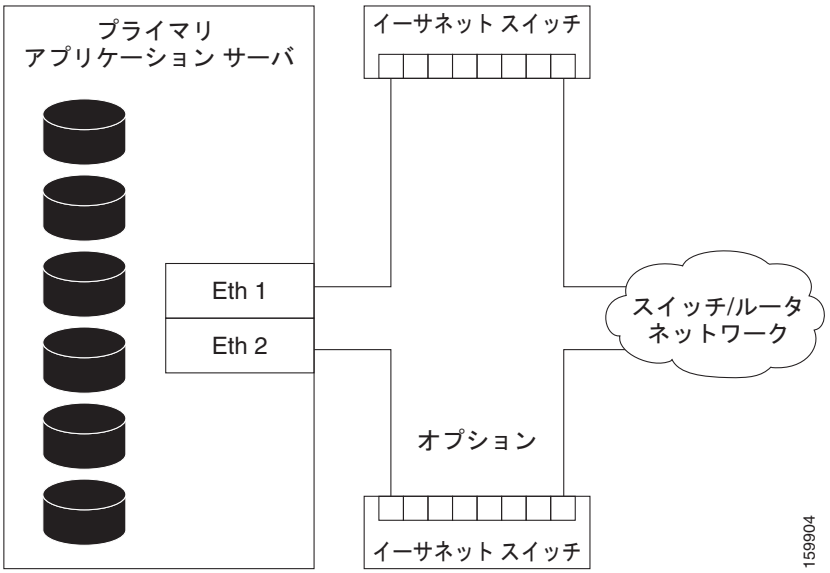
Security Manager を単一ノード HA 環境にインストールするには、フォールト トレラント ストレージ アレイを設定するか、内部ディスクを使用できます。

単一ノード サイトのハードウェア仕様は、次のとおりです。

- 『*Installation Guide for Cisco Security Manager 4.0*』に記載された基本プロセッサ要件および RAM 要件を満たすサーバ
- 1 個以上のイーサネット インターフェイス（2 個を推奨）
- 2 台以上の物理ドライブ（6 台を推奨）

図 2-1 に、サーバからスイッチ ネットワーク / ルータ ネットワークへ 2 つのイーサネット接続を使用し、冗長性を得る例を示します。イーサネット ポートまたはスイッチに障害が発生しても、サーバへの通信は維持されます。このレベルのネットワーク冗長性が不要な場合は、スイッチ ネットワーク / ルータ ネットワークへの単一接続を使用できます（つまり、Eth 2 とその関連イーサネット スイッチはオプションです）。

図 2-1　単一ノード サイトのイーサネット接続



デュアル ノード サイトのハードウェア要件

Security Manager をデュアル ノード HA 環境にインストールするには、共有ストレージ アレイにアクセスできる 2 台のサーバが必要です。

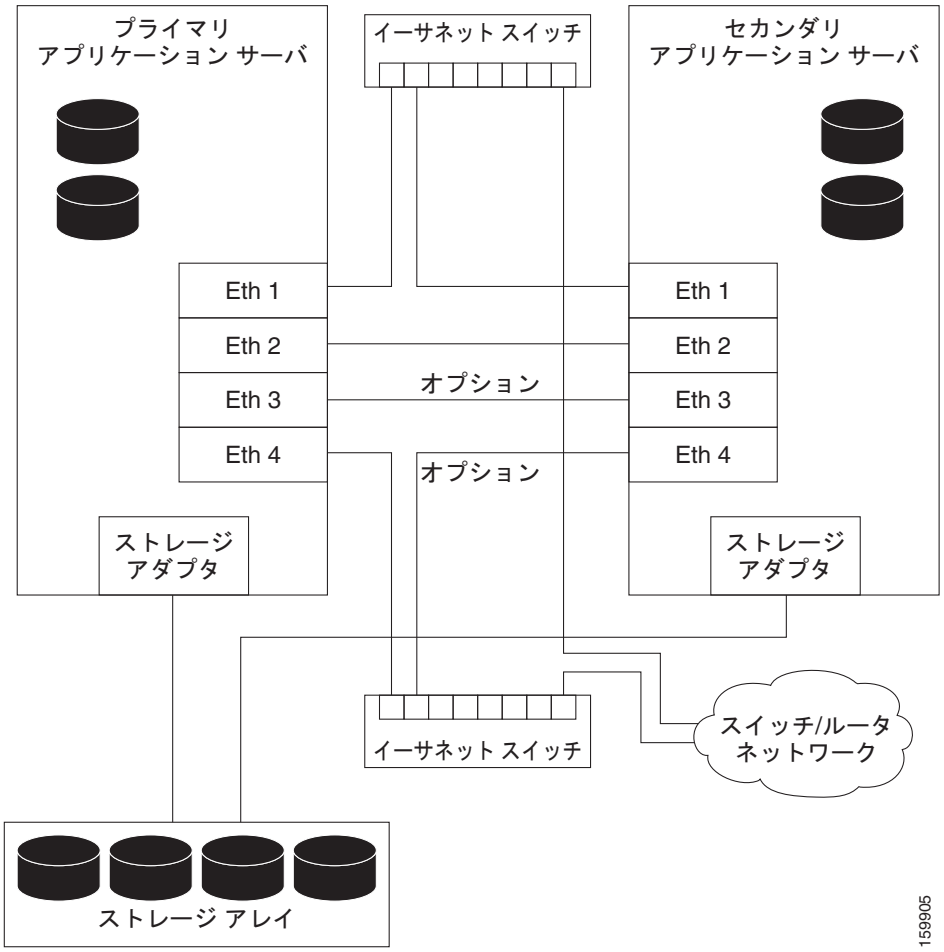
デュアルノード サイトのハードウェア仕様は、次のとおりです。

- 『*Installation Guide for Cisco Security Manager 4.0*』に記載された基本プロセッサ要件および RAM 要件を満たすサーバ
- 2 個以上のイーサネット インターフェイス（4 個を推奨）
- 1 台以上の内部物理ドライブ（2 台を推奨）
- 1 台以上の外部ドライブ（2 台を推奨。レプリケーションを使用している場合は 4 台を推奨）

図 2-2 には、イーサネット ストレージ接続および外部ストレージ接続を示すデュアル ノード サイトの構成を示します。冗長性を確保するために、2 個のイーサネット接続が、サーバからスイッチ ネットワーク / ルータ ネットワークで使用されています。イーサネット ポートまたはスイッチに障害が発生しても、サーバへの通信は維持されます。このレベルのネットワーク冗長性が不要な場合は、スイッチ

ネットワーク / ルータ ネットワークへの単一接続を使用できます（つまり、Eth 4 とその関連イーサネット スイッチはオプションです）。2 個の直接イーサネット接続が、クラスタ ハートビート接続用としてサーバ間に作成されます。2 番目のハートビート接続（Eth 3）はオプションです。

図 2-2　　デュアル ノード サイトのイーサネット接続およびストレージ接続



ローカル冗長性コンフィギュレーションのソフトウェア要件

ローカル冗長性 HA コンフィギュレーションに Security Manager をインストールするには、次のソフトウェアが必要です。

- Cisco Security Manager 4.0
- Symantec Veritas Storage Foundation HA for Windows 5.1
- Symantec Dynamic Multipathing Option

Security Manager のライセンスは、HA/DR コンフィギュレーションでのアクティブ サーバにのみ必要です。スタンバイ サーバ用の追加ライセンスは不要です。

Veritas Storage Foundation HA for Windows は、ノード単位でライセンス許諾されています。同じローカル冗長性コンフィギュレーションの例で、各サーバは Veritas Storage Foundation HA for Windows を実行するために固有のライセンスを所有している必要があります。

Veritas Dynamic Multipathing Option は、サーバとストレージ間に複数のパスを提供する複数のホスト バス アダプタを備えた外部ストレージを、1 台のサーバで使用する予定がある場合にのみ必要です。

地理的冗長性（DR）コンフィギュレーションのソフトウェア要件

地理的冗長性（DR）コンフィギュレーションに Security Manager をインストールするには、次のソフトウェアが必要です。

- Cisco Security Manager 4.0
- Symantec Veritas Storage Foundation HA/DR for Windows 5.1
- Symantec Veritas Volume Replicator Option
- Symantec Veritas Dynamic Multipathing Option

Security Manager は、HA/DR コンフィギュレーションでのアクティブ サーバ単位でライセンス許諾されています。たとえば、サイト A とサイト B に単一ノード クラスタを備えた地理的冗長性コンフィギュレーションでは、Security Manager は常に 1 台のサーバでのみアクティブなため、購入が必要な Security Manager は 1 つだけです。

Veritas Storage Foundation HA for Windows は、ノード単位でライセンス許諾されています。同じ地理的冗長性コンフィギュレーションの例で 2 台のサーバ（クラスタごとに 1 台）を備えている場合、個々のサーバに Veritas Storage Foundation HA for Windows を実行するために固有のライセンスが必要です。

Veritas Volume Replicator Option はノード単位でライセンス許諾されています。

Veritas Dynamic Multipathing Option は、サーバとストレージ間に複数のパスを提供する複数のホスト バス アダプタを備えた外部ストレージを、1 台のサーバで使用する予定がある場合にのみ必要です。

クラスタリングなしのレプリケーションのソフトウェア要件

クラスタリングなしの地理的冗長性（DR）コンフィギュレーションに Security Manager をインストールするには、次のソフトウェアが必要です。

- Cisco Security Manager 4.0
- Symantec Veritas Storage Foundation Basic for Windows 5.1
- Symantec Veritas Volume Replicator Option
- Symantec Veritas Dynamic Multipathing Option

Security Manager は、HA/DR コンフィギュレーションでの個々のアクティブ サーバにライセンス許諾されています。たとえば、プライマリ サーバとセカンダリ サーバ間で動作するレプリケーションを備えた地理的冗長性コンフィギュレーションでは、Security Manager は常に 1 台のサーバでのみアクティブなため、購入が必要な Security Manager は 1 つだけです。

Veritas Storage Foundation for Windows は、ノード単位でライセンス許諾されています。同じ地理的冗長性コンフィギュレーションの例で 2 台のサーバを備えている場合、個々のサーバに Veritas Storage Foundation for Windows を実行するために固有のライセンスが必要です。

Veritas Storage Foundation Basic for Windows 5.1 は、最大 4 台のボリュームで動作し、Symantec から無料でダウンロードできます。

Veritas Volume Replicator Option はノード単位でライセンス許諾されています。

Veritas Dynamic Multipathing Option は、サーバとストレージ間に複数のパスを提供する複数のホスト バス アダプタを備えた外部ストレージを、1 台のサーバで使用する予定がある場合にのみ必要です。

インストール前のワークシート

インストール前のワークシートを使用して、インストールを計画し、設定時に必要となる情報を収集します。ここでは、次の内容について説明します。

- 「ローカル冗長性コンフィギュレーションのワークシート」（P.2-5）
- 「地理的冗長性（DR）コンフィギュレーションのワークシート」（P.2-6）

ローカル冗長性コンフィギュレーションのワークシート

Security Manager をローカル冗長性 HA コンフィギュレーションにインストールする前に、表 2-1 に記載されている情報を記録して、インストールの実行に役立ててください。

表 2-1　ローカル冗長性コンフィギュレーション用のインストール前のワークシート

情報	**プライマリ サイト**	
共有ディスク グループ名	**datadg**	
共有ボリューム名	**cscopx**	
Security Manager データのドライブ文字		
イベント データ用の共有ディスク グループ名[1]	**datadg_evt**	
イベント データ用の共有ボリューム名[1]	**cscopx_evt**	
Security Manager イベント データ用のドライブ文字[1]		
クラスタ名	**CSManager_Primary**	
クラスタ ID	0[2]	
Security Manager 仮想 IP アドレス/サブネット マスク		
クラスタ サービスの仮想 IP アドレス/サブネット マスク[3]		
	プライマリ サーバ	**セカンダリ サーバ**
ホスト名		
パブリック ネットワーク インターフェイス #1 および IP アドレス/サブネット マスク		
パブリック ネットワーク インターフェイス #2[4] および IP アドレス/サブネット マスク		
専用クラスタ相互接続 #1		
専用クラスタ相互接続 #2		

1. 任意：イベント データを別々に格納した場合に、このフィールドを使用します。

2. 0 ～ 255 の整数で、同じサブセット内のクラスタで固有のものにする必要があります。
3. これは Security Manager の仮想 IP アドレス / サブネット マスクです。
4. 2 番目の NIC が冗長性を確保するためにパブリック ネットワークにアクセスするために使用される場合に必要です。

地理的冗長性（DR）コンフィギュレーションのワークシート

Security Manager を地理的冗長性（DR）コンフィギュレーションにインストールする場合は、表 2-2 に記載されている情報を記録して、インストールの実行に役立ててください。

表 2-2　地理的冗長性（DR）コンフィギュレーション用のインストール前のワークシート

情報	プライマリ サイト		セカンダリ サイト	
ディスク グループ	**datadg**		**datadg**	
データ ボリューム	**cscopx**		**cscopx**	
Security Manager のドライブ文字				
イベント データ用ディスク グループ[1]	**datadg_evt**		**datadg_evt**	
イベント データ用データ ボリューム	**cscopx_evt**		**cscopx_evt**	
イベント データ用のドライブ文字				
ストレージ レプリケーション ログ ボリューム	**data_srl**		**data_srl**	
レプリケーションされるデータセット	**CSM_RDS**			
レプリケーションされるボリューム グループ	**CSM_RVG**			
クラスタ名	**CSManager_Primary**		**CSManager_Secondary**	
クラスタ ID	**0**[2]		**1**[2]	
Security Manager 仮想 IP アドレス / サブネット マスク				
レプリケーション仮想 IP アドレス / サブネット マスク				
クラスタ サービスの仮想 IP アドレス / サブネット マスク[3,4]				
	プライマリ サーバ	**セカンダリ サーバ**	**プライマリ サーバ**	**セカンダリ サーバ**
ホスト名				
パブリック ネットワーク インターフェイス #1 および IP アドレス / サブネット マスク				
パブリック ネットワーク インターフェイス #2 および IP アドレス / サブネット マスク[5]				
専用クラスタ相互接続 #1[6]				
専用クラスタ相互接続 #2[6]				

1. 任意：イベント データを別々に格納した場合に、このフィールドを使用します。

2. 0 ～ 255 の整数で、同じサブセット内のクラスタで固有のものにする必要があります。
3. パブリック ネットワークにアクセスするために 2 台のサーバを使用するクラスタまたは複数のアダプタのみに必要です。パブリック ネットワークにアクセスするためにネットワーク アダプタを 1 個だけ備えた単一サーバ クラスタの場合、このアダプタの固定 IP アドレスが使用できます。
4. これは Security Manager の仮想 IP アドレス / サブネット マスクです。
5. 冗長性を確保するためにパブリック ネットワークにアクセスするために 2 番目の NIC を使用する場合に必要です。
6. 2 台のサーバを使用するクラスタのみに必要です。