



## はじめに

---

このマニュアルでは、高可用性（HA）環境やディザスタリカバリ（DR）環境に Cisco Security Management Suite（Security Manager）をインストールする方法について説明します。Security Manager HA/DR ソリューションは、Veritas Storage Foundation and High Availability Solutions に基づいています。

VMware ベースの高可用性（HA）またはディザスタリカバリ（DR）環境に Security Manager をインストールする手順については、[仮想マシンの高可用性とディザスタリカバリ](#)を参照してください。

- [対象読者](#)（1 ページ）
- [表記法](#)（4 ページ）
- [関連資料](#)（5 ページ）

## 対象読者

このマニュアルの主な対象読者は、HA/DR ソリューションのインストールおよび管理を担当するシステム管理者です。このマニュアルでは、[表](#)の内容をよく理解していることを前提としています。

表 1: このマニュアルの内容

設定	トピック
ローカル冗長性	<ul style="list-style-type: none"> <li>• Cisco Security Management Suite</li> <li>• Microsoft Windows Server 2019 Standard および Datacenter エディション、Microsoft Windows Server 2012 Standard および Datacenter エディション、または Microsoft Windows Server 2012 R2 Standard および Datacenter エディションまたは Microsoft Windows Server 2016 Standard および Datacenter エディション</li> </ul> <p>(注) CSM 4.27 の Microsoft Windows Server 2019 および 2016 プラットフォームでテスト済み。</p> <ul style="list-style-type: none"> <li>• Veritas Storage Foundation HA for Windows 6.0.1、6.0.2、6.1、Veritas InfoScale 7.0、Veritas InfoScale 7.2、Veritas InfoScale 7.4 <ul style="list-style-type: none"> <li>• Veritas InfoScale 7.4.2 以降は Windows Server 2019 をサポートしていません。</li> <li>• Windows 2019 : Veritas Storage Foundation for Windows Version : 7.4.2</li> <li>• Windows 2016 : Veritas Storage Foundation for Windows Version : 7.4</li> </ul> </li> </ul>

設定	トピック
地理的冗長性	<ul style="list-style-type: none"><li>• Cisco Security Management Suite</li><li>• Microsoft Windows Server 2019 Standard および Datacenter エディション、Microsoft Windows Server 2012 Standard および Datacenter エディション、または Microsoft Windows Server 2012 R2 Standard および Datacenter エディションまたは Microsoft Windows Server 2016 Standard および Datacenter エディション</li></ul> <p>(注) CSM 4.27 の Microsoft Windows Server 2019 および 2016 プラットフォームでテスト済み。</p> <ul style="list-style-type: none"><li>• Veritas Storage Foundation HA for Windows 6.0.1、6.0.2、6.1、Veritas InfoScale 7.0、Veritas InfoScale 7.2、Veritas InfoScale 7.4<ul style="list-style-type: none"><li>• Veritas InfoScale 7.4.2 以降は Windows Server 2019 をサポートしています。</li><li>• Windows 2019 : Veritas Storage Foundation for Windows Version : 7.4.2</li><li>• Windows 2016 : Veritas Storage Foundation for Windows Version : 7.4</li></ul></li><li>• Veritas Volume Replicator Option</li></ul>

設定	トピック
地理的冗長性 (クラスタリングなし)	<ul style="list-style-type: none"> <li>• Cisco Security Management Suite</li> <li>• Microsoft Windows Server 2019 Standard および Datacenter エディション、Microsoft Windows Server 2012 Standard および Datacenter エディション、または Microsoft Windows Server 2012 R2 Standard および Datacenter エディションまたは Microsoft Windows Server 2016 Standard および Datacenter エディション</li> </ul> <p style="margin-left: 40px;">(注) CSM 4.27 の Microsoft Windows Server 2019 および 2016 プラットフォームでテスト済み。</p> <ul style="list-style-type: none"> <li>• Veritas Storage Foundation HA for Windows 6.0.1、6.0.2、6.1、Veritas InfoScale 7.0、Veritas InfoScale 7.2、Veritas InfoScale 7.4               <ul style="list-style-type: none"> <li>• Veritas InfoScale 7.4.2 以降は Windows Server 2019 をサポートしています。</li> <li>• Windows 2019 : Veritas Storage Foundation for Windows Version : 7.4.2</li> <li>• Windows 2016 : Veritas Storage Foundation for Windows Version : 7.4</li> </ul> </li> <li>• Veritas Volume Replicator Option</li> </ul>

Security Manager HA/DR ソリューションは Veritas Storage Foundation and High Availability Solutions for Windows を利用するため、ローカル冗長性ソリューションに関する次のコースを推奨します。

- Veritas Storage Foundation for Windows
- Veritas Cluster Server for Windows

地理的冗長性については、次のコースを受講することを強く推奨します。

- Veritas Volume Replicator for Windows
- Disaster Recovery Using Veritas Volume Replicator and Global Cluster Option for Windows

## 表記法

このマニュアルでは、次の表記法を使用しています。

項目	表記法
手順で選択する必要があるコマンド、キーワード、特殊な用語、およびオプション	太字
ユーザが値を指定する変数、および新しい用語や重要な用語	<i>italic</i> フォント
セッション情報、システム情報、パス、およびファイル名の表示出力	screen font
ユーザーが入力する情報	太字の screen フォント
ユーザーが入力する変数	イタリック体の screen フォント
メニュー項目およびボタン名	太字
メニュー項目の選択順序	[オプション (Option)] > [ネットワーク設定 (Network Preferences)]



ヒント 製品を最大限に活用できる情報を示します。



(注) 「注釈」です。次に進む前に検討する必要がある重要情報、役に立つ情報、このマニュアル以外の参照資料などを紹介しています。



注意 「要注意」の意味です。機器の損傷、データの損失、またはネットワークセキュリティの侵害を予防するための注意事項が記述されています。



警告 ユーザの身体、ソフトウェアの状態、または機器に被害が及ぶのを防ぐために、留意する必要がある注意事項が記述されています。記載された注意事項に従わない場合に、結果として発生するセキュリティ侵害が明確に特定されています。

## 関連資料

追加情報については、次のシスコの資料を参照してください。このドキュメントは <http://www.cisco.com/c/en/us/support/security/security-manager/tsd-products-support-series-home.html> から入手できます。

- 『*Installation Guide for Cisco Security Manager 4.27*』 [英語]

- 『*User Guide for Cisco Security Manager 4.27*』 [英語]
- 『*Release Notes for Cisco Security Manager 4.27*』 [英語]

Veritas Storage Foundation に関連する詳細情報については、次の資料を参照してください。

- 『*Veritas Storage Foundation™ and High Availability Solutions Getting Started Guide*』 [英語]
- 『*Veritas Storage Foundation™ and High Availability Solutions Release Notes*』 [英語]
- 『*Veritas Storage Foundation™ and High Availability Solutions Installation and Upgrade Guide*』 [英語]
- 『*Veritas Storage Foundation™ Administrator's Guide*』 [英語]
- 『*Veritas™ Cluster Server Release Notes*』 [英語]
- 『*Veritas™ Cluster Server Installation and Upgrade Guide*』 [英語]
- 『*Veritas™ Cluster Server Bundled Agents Reference Guide*』 [英語]
- 『*Veritas™ Cluster Server Administrator's Guide*』 [英語]
- 『*Veritas™ Volume Replicator Administrator's Guide*』 [英語]
- 『*Veritas™ Volume Replicator Advisor User's Guide*』 [英語]
- 『*Hardware Compatibility List (HCL) for Veritas Storage Foundation™ and High Availability Solutions for Windows*』 [英語]
- 『*Software Compatibility List (SCL) for Veritas Storage Foundation™ and High Availability Solutions for Windows*』 [英語]

#### 通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) [英語] でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[シスコサービス](#) [英語] にアクセスしてください。
- サービス リクエストを送信するには、[シスコサポート](#) [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco Marketplace](#) [英語] にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) [英語] にアクセスしてください。

### Cisco バグ検索ツール

[Cisco バグ検索ツール](#) (BST) [英語] は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。