



## Cisco Security Agent for Cisco Unity リリース ノート Release 3.1(4)

---

**【注意】** シスコ製品をご使用になる前に、安全上の注意  
([www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)) をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。  
米国サイト掲載ドキュメントとの差異が生じる場合があるため、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。  
また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Published May 21, 2008

このリリース ノートには、Cisco Security Agent for Cisco Unity リリース 3.1(4) のダウンロード手順、インストール手順、アップグレード手順、新規および変更された要件、サポート、および機能、さらに警告に関する情報が記載されています。

Cisco Security Agent for Cisco Unity ソフトウェアは、シスコのソフトウェア ダウンロード ページから入手できます(ダウンロード元となる場所は、各リリース ノートのダウンロード手順の項に記載されています)。



**(注)** Cisco Security Agent for Cisco Unity は、日本語 OS には対応していません。Cisco Unity 環境、Cisco Unity Connection 環境でご利用になる場合は、英語 OS をご利用ください。

---

## 内容

このリリース ノートの内容は次のとおりです。

- [はじめに \(P.3\)](#)
- [要件とサポートされているソフトウェア \(P.4\)](#)
- [関連資料 \(P.8\)](#)
- [新規および変更されたサポート：リリース 3.1\(4\) \(P.9\)](#)
- [新規および変更された機能：リリース 3.1\(4\) \(P.9\)](#)
- [インストールとアップグレードに関する情報 \(P.10\)](#)
- [Cisco Security Agent for Cisco Unity の使用に関する特記事項 \(P.15\)](#)
- [警告 \(P.17\)](#)
- [トラブルシューティング情報 \(P.19\)](#)
- [マニュアルの入手方法および Service Request ツールの使用方法 \(P.21\)](#)

## はじめに

Cisco Security Agent for Cisco Unity は、次のソフトウェアと連携して使用するために、シスコシステムズによって無料で提供されているスタンドアロン Cisco Security Agent です。

- Cisco Unity
- Cisco Unity 音声認識
- Cisco Unity Connection 1.x
- Cisco Unity Connection 1.x 音声認識
- Cisco Unity Bridge

このスタンドアロン Cisco Security Agent は、次の機能を提供します。

- 侵入検知と防御
- アンチウイルス ソフトウェアと同様の、シグニチャを必要としないために以前は未知だった攻撃に対する防御。
- ダウンタイム、攻撃の広がり、および対策費用を低減。

このエージェントは、テスト済みのセキュリティ規則セット（いわゆるポリシー）に基づいて、Windows プラットフォームのセキュリティ（ホスト侵入検知および防御）を提供します。このポリシーは次の基準に基づいて、システム リソースへのアクセスが行われる前に、特定のシステム アクションを許可または拒否します。

- リソースがアクセスされていること。
- オペレーションが呼び出されていること。
- プロセスが処理を呼び出していること。

これは透過的に行われ、システム全体のパフォーマンスを大きく妨げることはありません。

スタンドアロン Cisco Security Agent for Cisco Unity バージョン 3.1(4) は、Cisco Security Agent バージョン 5.2.0 ビルド 245 でコンパイルされています。



### 注意

Cisco Security Agent for Cisco Unity は、サポートされる製品の完全なセキュリティを提供する製品ではありません。この製品は、追加の防御策であり、アンチウイルス ソフトウェアやファイアウォールなどの他の一般的な防御製品と共に正しく使用した場合に、セキュリティを高めるものと考えする必要があります。Cisco Security Agent for Cisco Unity は、さまざまなインストール環境やコンフィギュレーションに対して防御を強化します。このため、発信または受信のネットワークトラフィックをブロックするようなネットワーク アクセス制御規則に強制的に従わせたり、ホストベースのファイアウォールとして機能したりすることはできません。

セキュリティおよび音声製品を参照する場合は、<http://www.cisco.com/go/ipcsecurity> にアクセスしてください。そこで、『*IP Telephony Security Operations Guide to Best Practices*』をご覧ください。ご閲覧いただくことをお勧めします。

また、[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html) にある該当するバージョンの『*Cisco Unity セキュリティ ガイド*』を参照してください。

## 要件とサポートされているソフトウェア

各製品に該当する項を参照してください。

- 要件およびサポートされているソフトウェア：Cisco Unity または Cisco Unity 音声認識 (P.4)
- 要件とサポートされているソフトウェア：Cisco Unity Connection 1.x または Connection 1.x 音声認識 (P.6)
- 要件とサポートされているソフトウェア：Cisco Unity Bridge (P.7)
- ソフトウェア バージョンの特定 (P.8)

## 要件およびサポートされているソフトウェア: Cisco Unity または Cisco Unity 音声認識

各製品に該当する項を参照してください。

- ソフトウェア要件：Cisco Unity (P.4)
- ソフトウェア要件：Cisco Unity 音声認識 (P.5)
- サポートされているオプション ソフトウェア：Cisco Unity または Cisco Unity 音声認識 (P.5)

### ソフトウェア要件：Cisco Unity

- Cisco Unity サーバ上で動作する Cisco Unity バージョン 4.0(1) 以降。
- Cisco Unity サーバ上で動作する英語版 Microsoft Windows Server 2003、英語版 Windows 2000 Server、または英語版 Windows 2000 Advanced Server。他の言語バージョンはサポートされていません。



(注)

日本語版 Windows を実行しているサーバに Cisco Security Agent for Cisco Unity をインストールすると、一部の非 ASCII 文字の表示が破損します。

- 適合性が確認されたメッセージストア：
  - メッセージストアが Cisco Unity サーバにインストールされる場合は、メッセージストア用の Microsoft Exchange 2003、Microsoft Exchange 2000 または Exchange 5.5。
  - メッセージストアが Cisco Unity サーバにインストールされない場合は、メッセージストア用の IBM Lotus Domino、Exchange 2007、Exchange 2003、Exchange 2000、または Exchange 5.5。
- Cisco Security Agent for Cisco Unity は、Cisco Unity がボイス メッセージ コンフィギュレーションでインストールされている場合のみ、Exchange 2003 または Exchange 2003 サーバ上、およびドメイン コントローラ / グローバル カタログ サーバ (DC/GC) 上にインストールできます。次の場所には、Cisco Security Agent for Cisco Unity をインストールしないでください。
  - Cisco Unity がユニファイド メッセージ コンフィギュレーションでインストールされている場合、メッセージストア サーバ上や DC/GC 上。
  - Domino サーバ上。
  - 64 ビットバージョンの Windows を実行しているサーバ上。

## ソフトウェア要件 : Cisco Unity 音声認識

- Cisco Unity 音声認識サーバ上で動作している Cisco Unity バージョン 5.0(1) 以降の音声認識ソフトウェア。
- Cisco Unity 音声認識サーバ上で動作している英語版の Microsoft Windows Server 2003。他の言語バージョンはサポートされていません。



(注)

日本語版 Windows を実行しているサーバに Cisco Security Agent for Cisco Unity をインストールすると、一部の非 ASCII 文字の表示が破損します。

## サポートされているオプションソフトウェア : Cisco Unity または Cisco Unity 音声認識

Cisco Security Agent for Cisco Unity を実行している Cisco Unity サーバまたは Cisco Unity 音声認識サーバとの適合性が確認されているのは、次のオプションソフトウェアだけです。

- Adobe Acrobat Reader バージョン 4 以降。
- CA Anti-Virus for the Enterprise バージョン 8.0 以降 (旧製品名 : eTrust Antivirus )
- McAfee NetShield for Microsoft Windows NT and Windows 2000 バージョン 4.5 以降。
- NetIQ AppManager for Cisco Voice Mail バージョン 6.0 以降 (Cisco Unity サーバにはエージェントのみインストールしてください)。
- Symantec
  - AntiVirus Corporate Edition バージョン 8.1 以降。
  - Norton AntiVirus for Microsoft Windows NT and Windows 2000 バージョン 5.02 以降。
- Trend Micro
  - ScanMail for Microsoft Exchange 2000 バージョン 5 以降。
  - ServerProtect for Microsoft Windows バージョン 5.5 以降。
- VERITAS
  - Backup Exec for Microsoft Windows NT and Windows 2000 バージョン 8.6 以降。
  - NetBackup バージョン 4.5 以降。
- Windows 自動更新。これは、Cisco Unity サーバにアップデートを自動的にダウンロードしないように設定されている必要があります。
- WinZip バージョン 7 以降。

Cisco Unity サーバおよび Cisco Unity 音声認識サーバのオプションソフトウェアのサポートポリシーは、[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html) にある適切なバージョンの『Cisco Unity サポートされるハードウェアとソフトウェアおよびサポートポリシー』で入手できます。

お客様が、Cisco Security Agent for Cisco Unity との併用がサポートされていないサードパーティ製ソフトウェア (変更された CSA ポリシーを含む) の使用をご希望の場合は、CiscoWorks Management Center for Cisco Security Agents のライセンスが付与されたバージョンを使用して、希望するサードパーティ製ソフトウェアとの互換性を持つ Cisco Security Agent を作成、カスタマイズ、展開、および管理できます。

## 要件とサポートされているソフトウェア：Cisco Unity Connection 1.x または Connection 1.x 音声認識

各製品に該当する項を参照してください。

- [ソフトウェア要件：Cisco Unity Connection 1.x または Connection 1.x 音声認識 \(P.6\)](#)
- [サポートされるオプションソフトウェア：Cisco Unity Connection 1.x または Connection 1.x 音声認識 \(P.6\)](#)

### ソフトウェア要件：Cisco Unity Connection 1.x または Connection 1.x 音声認識

- Cisco Unity Connection バージョン 1.x (Cisco Unity Connection または Connection 音声認識サーバ上にインストールされている場合)



(注) Cisco Unity Connection 2.x 以降では、Cisco Security Agent は Linux オペレーティングシステムおよび Connection のインストールの一部としてインストールされ、個別にインストールまたはアップグレードすることはできません。

Cisco Security Agent for Cisco Unity がさまざまな展開をサポートできるように、エージェントは受信ポートと受信プロトコルに基づいたネットワーク アクセス制御を強制することはありません。Connection の場合は、Windows Server 2003 のファイアウォールが受信ポートと受信プロトコルに基づいたネットワーク アクセス制御を強制します。このファイアウォールは、Connection セットアップ時の Connection の機能については例外が設定されています。このファイアウォールの設定を変更したり、ファイアウォールを無効化したりするには、Connection サーバの G:\Cisco Systems\Cisco Unity Connection\TechTools ディレクトリにある Cisco Unity Connection ネットワーク セキュリティ ウィザード (NetworkSecurityWizard.exe) を使用してください。

- Cisco Unity Connection サーバ上で動作する英語版 Microsoft Windows Server 2003 Standard Edition。他の言語バージョンはサポートされていません。



(注) 日本語版 Windows を実行しているサーバに Cisco Security Agent for Cisco Unity をインストールすると、一部の非 ASCII 文字の表示が破損します。

### サポートされるオプションソフトウェア：Cisco Unity Connection 1.x または Connection 1.x 音声認識

Cisco Security Agent for Cisco Unity を実行している Cisco Unity Connection 1.x または Connection 1.x 音声認識サーバとの適合性が確認されているのは、次のオプション ソフトウェアだけです。

- Adobe Acrobat Reader バージョン 4 以降。
- CA eTrust Antivirus バージョン 7.0。
- McAfee VirusScan Enterprise 8.0i 以降。
- Symantec AntiVirus Corporate Edition バージョン 9.0 以降。
- Trend Micro Server Protect for Microsoft Windows バージョン 5.56 以降。
- Windows 自動更新。これは、Cisco Unity サーバにアップデートを自動的にダウンロードしないように設定されている必要があります。
- WinZip バージョン 7 以降。

Cisco Unity Connection または Connection 音声認識サーバのオプション ソフトウェアのサポート ポリシーは、[http://www.cisco.com/en/US/products/ps6509/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html) にある適切なバージョンの『Cisco Unity Connection サポートされるハードウェア/ソフトウェアおよびサポートポリシー』で入手できます。

お客様が、Cisco Security Agent for Cisco Unity との併用がサポートされていないサードパーティ製ソフトウェア（変更された CSA ポリシーを含む）の使用をご希望の場合は、CiscoWorks Management Center for Cisco Security Agents のライセンスが付与されたバージョンを使用して、希望するサードパーティ製ソフトウェアとの互換性を持つ Cisco Security Agent を作成、カスタマイズ、展開、および管理できます。

## 要件とサポートされているソフトウェア：Cisco Unity Bridge

各製品に該当する項を参照してください。

- [ソフトウェア要件：Cisco Unity Bridge \(P.7\)](#)
- [サポートされているオプション ソフトウェア：Cisco Unity Bridge \(P.7\)](#)

### ソフトウェア要件：Cisco Unity Bridge

- Bridge サーバ上で動作する Cisco Unity Bridge バージョン 3.1(1) 以降。
- Bridge サーバ上で動作している英語版の Microsoft Windows Server 2003 または Windows 2000 Server。他の言語バージョンはサポートされていません。



**(注)** 日本語版 Windows を実行しているサーバに Cisco Security Agent for Cisco Unity をインストールすると、一部の非 ASCII 文字の表示が破損します。

### サポートされているオプション ソフトウェア：Cisco Unity Bridge

Cisco Security Agent for Cisco Unity を実行している Bridge サーバとの適合性が確認されているのは、次のオプション ソフトウェアだけです。

- McAfee NetShield for Microsoft Windows NT and Windows 2000 バージョン 4.5 以降。
- VERITAS
  - Backup Exec for Microsoft Windows NT and Windows 2000 バージョン 8.6。
  - NetBackup バージョン 4.5 以降。
- Windows 自動更新。これは、Bridge サーバにアップデートを自動的にダウンロードしないように設定されている必要があります。

Cisco Unity Bridge のオプション ソフトウェアのサポート ポリシーは、[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html) にある適切なバージョンの『Cisco Unity Bridge System Requirements, and Supported Hardware and Software』で入手できます。

お客様が、Cisco Security Agent for Cisco Unity との併用がサポートされていないサードパーティ製ソフトウェア（変更された CSA ポリシーを含む）の使用をご希望の場合は、CiscoWorks Management Center for Cisco Security Agents のライセンスが付与されたバージョンを使用して、希望するサードパーティ製ソフトウェアとの互換性を持つ Cisco Security Agent を作成、カスタマイズ、展開、および管理できます。

## ソフトウェアバージョンの特定

Cisco Security Agent for Cisco Unity のバージョンと、このエージェントの作成時に使用したポリシーのバージョンは同じです。次の手順を実行して、エージェントとポリシー双方のバージョンを特定してください。

### Cisco Security Agent for Cisco Unity のバージョンと、使用しているポリシーのバージョンを特定する

- 
- ステップ 1** [ Cisco Security Agent ] タスクバー アイコン をダブルクリックします。
- ステップ 2** Cisco Security Agent Panel の左側にあるツリー コントロールで、[ Status ] をクリックします。
- ステップ 3** 製品 ID フィールドのバージョン番号は、Cisco Security Agent for Cisco Unity と、エージェントの作成時に使用したポリシーの双方に適用します。
- 

### Cisco Security Agent Engine のバージョンを特定する

[ Cisco Security Agent ] タスクバー アイコンを右クリックし、[ About ] をクリックします。

---

## 関連資料

- Cisco.com 上の Cisco Unity に関するドキュメントの説明および URL については、『*Documentation Guide for Cisco Unity*』を参照してください。このドキュメントは Cisco Unity に同梱されており、[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products\\_documentation\\_roadmaps\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_documentation_roadmaps_list.html) でも入手可能です。
- Cisco.com 上の Cisco Unity Connection に関するドキュメントの説明および URL については、『*Documentation Guide for Cisco Unity Connection*』を参照してください。このマニュアルは Cisco Unity Connection に同梱されており、[http://www.cisco.com/en/US/products/ps6509/products\\_documentation\\_roadmaps\\_list.html](http://www.cisco.com/en/US/products/ps6509/products_documentation_roadmaps_list.html) でも入手可能です。
- Cisco.com 上の Cisco Unity Bridge に関するドキュメントについては、[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products\\_feature\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html) を参照してください。
- Cisco Security Agent for Cisco Unity バージョン 3.1(4) のコンパイルに使用された Cisco Security Agent バージョン 5.2.0 ビルド 245 の詳細については、<http://cisco.com> で readme ファイルの CSA\_5.2.0.245\_readme.txt を検索し参照してください。



**(注)** readme にアクセスするには、Cisco.com に登録ユーザとしてログオンしている必要があります。

---

## 新規および変更されたサポート：リリース 3.1(4)

この項では、Cisco Security Agent for Cisco Unity リリース 3.1(4) 限定の新規および変更されたサポートについて説明します。以前のバージョンの Cisco Security Agent for Cisco Unity の新規および変更されたサポートについては、該当するバージョンのリリース ノートを参照してください。Cisco Security Agent for Cisco Unity のすべてのバージョンに対応するリリース ノートは、[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html) から入手可能です。

### CA Anti-Virus バージョン 8.0 以降

Cisco Security Agent for Cisco Unity は、Cisco Unity サーバおよび Cisco Unity 音声認識サーバへの CA Anti-Virus for the Enterprise バージョン 8.0 以降（旧製品名：eTrust Antivirus）のインストールをサポートしています。

## 新規および変更された機能：リリース 3.1(4)

このリリースには、新規または変更された機能はありません。P.17 の「[解決済みの警告：リリース 3.1\(4\)](#)」を参照してください。以前のバージョンの Cisco Security Agent for Cisco Unity の新規および変更された機能については、該当するバージョンのリリース ノートを参照してください。Cisco Security Agent for Cisco Unity のすべてのバージョンに対応するリリース ノートは、[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html) から入手可能です。

## インストールとアップグレードに関する情報

- Cisco Security Agent for Cisco Unity 3.1(4) のダウンロード ( P.10 )
- Cisco Security Agent for Cisco Unity 3.1(4) のインストール ( P.11 )
- Cisco Security Agent for Cisco Unity 3.1(4) へのアップグレード ( P.13 )
- Cisco Security Agent サービスの無効化と再有効化 ( P.13 )
- Cisco Security Agent for Cisco Unity のアンインストール ( P.14 )

### Cisco Security Agent for Cisco Unity 3.1(4) のダウンロード

Cisco Security Agent for Cisco Unity は、Cisco Unity Server Updates ウィザードに組み込まれています。Cisco Security Agent for Cisco Unity 自体をダウンロードすることもできますが、最新の Server Updates ウィザードをダウンロードして実行し、Cisco Security Agent for Cisco Unity および推奨されている最新の Microsoft アップデートをインストールすることをお勧めします

( このウィザードによってインストールされる Microsoft アップデートの一覧については、[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/unity/updates/wizard/cuupwz.html](http://www.cisco.com/en/US/docs/voice_ip_comm/unity/updates/wizard/cuupwz.html) にある『Cisco Unity Server Updates ウィザードでインストールされるソフトウェア』を参照してください )

#### Server Updates ウィザードをダウンロードする

- ステップ 1** 高速インターネット接続が可能なコンピュータで、Cisco Unified Communications Applications Downloads ページ ( <http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278875240> ) にアクセスします。



**(注)** Software Download ページにアクセスするには、Cisco.com に登録ユーザとしてログオンしている必要があります。

- ステップ 2** Voice Mail and Unified Messaging > Cisco Unity を展開し、Cisco Unity Version 7.0 をクリックして、さらに Microsoft Updates for Cisco Unity/Unity Connection をクリックします。

- ステップ 3** [ Latest Releases ] の下にある最新バージョンへのリンクをクリックし、使用するコンピュータのハードディスクに、ダウンロードするファイルおよび抽出するウィザードのための十分な空き領域があることを確認します。必要な空き領域は、ダウンロード ファイルの合計サイズの約 2 倍です。

- ステップ 4** 画面の指示に従ってダウンロードを完了します。MD5 値を書き留めておいてください。

- ステップ 5** ダウンロード ファイルについて、チェックサム ジェネレータを使用して MD5 チェックサムが Cisco.com に記載されているチェックサムと一致することを確認します。値が一致しない場合、ダウンロード ファイルは損傷しています。



**注意** 損傷したファイルを使用してソフトウェアをインストールしないでください。インストールしようとする、予想外の結果をもたらすことがあります。MD5 値が一致しない場合は、ダウンロード ファイルのチェックサム値が Cisco.com に記載された値と一致するまで、再度ファイルをダウンロードしてください。

Microsoft File Checksum Integrity Verifier ユーティリティなどの無料のチェックサム ツールをインターネットから入手できます。このユーティリティの説明は、Microsoft サポート技術情報 841290 『Availability and Description of the File Checksum Integrity Verifier Utility』に記載されています。このサポート技術情報には、ユーティリティをダウンロードするためのリンクもあります。

**ステップ 6** Cisco Unity Server Updates ウィザードをハードディスクに抽出します。

- a. Windows エクスプローラで、ファイルをダブルクリックします。
- b. WinZip で、ウィザードを抽出するディレクトリを指定します。

**ステップ 7** ウィザード用の CD を 1 枚作成し、「Cisco Unity Server Updates ウィザード <日付 >」とラベルを貼っておきます。次の点を考慮してください。

- 最大 64 文字長のファイル名に対応する Joliet ファイル システムを使用する。
- 使用するディスク作成アプリケーションに作成したディスクの内容を確認するオプションがある場合は、そのオプションを選択する。これを選択すると、アプリケーションが作成したディスクの内容とソース ファイルを比較します。

**ステップ 8** ウィザードの抽出が完了したら、ダウンロードした .exe ファイルを削除してディスク領域を解放します。

## Cisco Security Agent for Cisco Unity 3.1(4) のインストール



(注)

Cisco Security Agent for Cisco Unity をバージョン 3.1(4) にアップグレードする場合は、P.13 の「Cisco Security Agent for Cisco Unity 3.1(4) へのアップグレード」を参照してください。

インストール プロセスによりシステムのパフォーマンスに影響が及ぼされるため、通常の営業時間後に Cisco Security Agent for Cisco Unity をインストールすることをお勧めします。さらに、インストールの完了後、作業を開始するには、Cisco Security Agent for Cisco Unity をインストールしたサーバを再起動する必要があります。



注意

Windows ターミナル サービスを使用して Cisco Security Agent for Cisco Unity をインストールしないでください。Windows ターミナル サービスを使用してインストールすると、インストールに失敗します。

### Cisco Security Agent for Cisco Unity 3.1(4) のインストール

**ステップ 1** ローカルの Administrators グループのメンバーであるアカウントを使用して、サーバにログオンします。

**ステップ 2** Windows 自動更新が Microsoft の Web サイトからアップデートを自動的にダウンロードするように設定されている場合は、それを無効にします。

- ステップ 3** サーバにアンチウイルス ソフトウェアがインストールされている場合は、次の手順に従って、それらのスキャン サービスを無効にして停止します。
- Windows の [ Start ] メニューで、[ Programs ] > [ Administrative Tools ] > [ Services ] をクリックします。
  - 右ペインで、最初のウイルス スキャン サービスの名前をダブルクリックします。
  - [ General ] タブの [ Stop ] をクリックし、サービスをすぐに停止します。
  - [ Startup Type ] リストで、[ Disabled ] をクリックします。この操作により、サーバの再起動時にサービスが起動しなくなります。
  - [ OK ] をクリックして [ Properties ] ダイアログボックスを閉じます。
  - 残りのウイルス スキャン サービスについてもステップ b ~ e を繰り返します。
  - すべてのウイルス スキャン サービスが無効になったら、Services MMC を閉じます。

**ステップ 4** Cisco Unity Server Updates ウィザード CD を DVD ドライブに挿入します。

**ステップ 5** ルート ディレクトリを表示し、ServerUpdatesWizard.exe をダブルクリックします。

**ステップ 6** 画面の指示に従って、Cisco Security Agent for Cisco Unity および Microsoft アップデートをインストールします。



**(注)** Remote Desktop または VNC クライアントを使ってサーバにアクセスしている場合は、その Remote Desktop または VNC セッションは、Cisco Security Agent for Cisco Unity がネットワーク インターフェイスを再起動するときに接続解除されます。このセッションが自動的に再接続しない場合は、手動で再接続を行い、Server Updates ウィザードを終了してください。

**ステップ 7** インストールが完了したら、[ Yes, I Want to Restart My Computer Now ] をクリックし、[ Finish ] をクリックします。

サーバを再起動するとすぐに、Cisco Security Agent for Cisco Unity が動作を開始します。このアプリケーションを設定する必要はありません。

**ステップ 8** サーバにアンチウイルス ソフトウェアがインストールされている場合は、次の手順に従って、それらのスキャン サービスを再度有効にして開始します。

- Windows の [ Start ] メニューで、[ Programs ] > [ Administrative Tools ] > [ Services ] をクリックします。
- 右ペインで、最初のウイルス スキャン サービスの名前をダブルクリックします。
- [ General ] タブの [ Startup Type ] リストで、[ Automatic ] をクリックし、サービスを再度有効にします。
- [ Start ] をクリックし、サービスを開始します。
- [ OK ] をクリックして [ Properties ] ダイアログボックスを閉じます。
- 残りのウイルス スキャン サービスについてもステップ b ~ e を繰り返します。
- すべてのウイルス スキャン サービスが有効になったら、Services MMC を閉じます。

## Cisco Security Agent for Cisco Unity 3.1(4) へのアップグレード

Cisco Security Agent for Cisco Unity をバージョン 3.1(4) にアップグレードするには、次のタスクを順番通りに実行します。各タスクには、このリリース ノート内の対応する項が記載されています。

1. ソフトウェアをダウンロードします。P.10 の「Cisco Security Agent for Cisco Unity 3.1(4) のダウンロード」を参照してください。
2. Cisco Security Agent サービスを停止して無効にします。P.13 の「Cisco Security Agent サービスの無効化と再有効化」の「Cisco Security Agent サービスを停止して無効にする」の手順を参照してください。
3. 以前のバージョンをアンインストールします。P.14 の「Cisco Security Agent for Cisco Unity のアンインストール」を参照してください。
4. バージョン 3.1(4) をインストールします。P.11 の「Cisco Security Agent for Cisco Unity 3.1(4) のインストール」を参照してください。インストールが完了すると、Cisco Security Agent サービスが自動的に有効になります。

## Cisco Security Agent サービスの無効化と再有効化

Cisco Security Agent for Cisco Unity がインストールされているサーバに任意のソフトウェアをインストールまたはアップグレードするには、Cisco Security Agent サービスを停止して無効にする必要があります

(これ以外に Cisco Security Agent サービスを無効にする必要のある場合については、P.15 の「特定のタスクでは Cisco Security Agent サービスを無効にする必要がある」を参照してください)。

この項では、次の 2 つの手順について説明します。

- Cisco Security Agent サービスを停止して無効にする (P.13)
- Cisco Security Agent サービスを再度有効にして開始する (P.14)



### 注意

Cisco Security Agent サービスを停止して無効にした場合、このサービスによってサーバを再度監視するには、このサービスを再度有効にして開始する必要があります。

### Cisco Security Agent サービスを停止して無効にする

- ステップ 1** Windows の [ Start ] メニューで、[ Programs ] > [ Administrative Tools ] > [ Services ] をクリックします。
- ステップ 2** 右ペインで、[ Cisco Security Agent ] をダブルクリックします。
- ステップ 3** [ General ] タブの [ Stop ] をクリックし、サービスをすぐに停止します。
- ステップ 4** [ Startup Type ] リストで、[ Disabled ] をクリックします。この操作により、サーバの再起動時にサービスが起動しなくなります。
- ステップ 5** [ OK ] をクリックして [ Cisco Security Agent Properties ] ダイアログボックスを閉じます。
- ステップ 6** サービスが無効になったら、Services MMC を閉じます。

---

### Cisco Security Agent サービスを再度有効にして開始する

---

- ステップ 1** Windows の [ Start ]メニューで、[ Programs ] > [ Administrative Tools ] > [ Services ]をクリックします。
  - ステップ 2** 右ペインで、 [ Cisco Security Agent ] をダブルクリックします。
  - ステップ 3** [ General ]タブの [ Startup Type ]リストで、[ Automatic ]をクリックし、サービスを再度有効にします。
  - ステップ 4** [ Start ] をクリックし、サービスを開始します。
  - ステップ 5** [ OK ] をクリックして [ Cisco Security Agent Properties ] ダイアログボックスを閉じます。
  - ステップ 6** サービスが再度有効になったら、 Services MMC を閉じます。
- 

## Cisco Security Agent for Cisco Unity のアンインストール

### Cisco Security Agent for Cisco Unity をアンインストールする

---

- ステップ 1** Cisco Security Agent サービスが有効になっている場合は、それを停止し無効にします。P.13 の「[Cisco Security Agent サービスを停止して無効にする](#)」を参照してください。
  - ステップ 2** Windows の [ Start ]メニューで、 [ Programs ] > [ Cisco Systems ] > [ Uninstall Cisco Security Agent ] をクリックします。
  - ステップ 3** [ Yes ] をクリックして、 Cisco Security Agent for Cisco Unity のアンインストールを確定します。
  - ステップ 4** もう一度 [ Yes ] をクリックして、サーバを再起動します。
-

## Cisco Security Agent for Cisco Unity の使用に関する特記事項

次の各項では、Cisco Security Agent for Cisco Unity の使用に関する注意事項を示します。

- 特定のタスクでは Cisco Security Agent サービスを無効にする必要がある ( P.15 )
- Cisco Security Agent がイベントを記録する場所 ( P.16 )
- カスタム SQL サーバのバックアップは SQLBackups ディレクトリ内に書き込む( Cisco Unity のみ)( P.16 )
- Cisco Security Agent for Cisco Unity がインストールされているサーバからの Web ブラウジング ( P.16 )

### 特定のタスクでは Cisco Security Agent サービスを無効にする必要がある

次の場合には Cisco Security Agent サービスを停止し無効にします。無効にしないと、Cisco Security Agent for Cisco Unity が選択したアクションを中断またはブロックする可能性があります。

- Cisco Unity の場合のみ、次の場所で任意のツールを使用する前。
  - CommServer\Utilities ディレクトリ
  - CommServer\TechTools ディレクトリ
- Cisco Unity Connection の場合のみ、次の場所で任意のツールを使用する前。
  - Cisco Unity Connection\Utilities ディレクトリ
  - Cisco Unity Connection\TechTools ディレクトリ
- Cisco Unity Tools Web サイトからダウンロードしたツールを使用する前。
- Cisco Security Agent for Cisco Unity がインストールされているサーバにソフトウェアをインストールする前。
- Cisco Unity の場合のみ、Cisco Unity フェールオーバー コンフィギュレーション ウィザードを実行する前。
- Cisco Security Agent for Cisco Unity がインストールされているサーバにソフトウェアをアップグレードする前。これは、自動アップグレード (たとえば、グループ ポリシー オブジェクトやカスタム スクリプトを使用したサービス パックのインストール) にも当てはまります。Cisco Security Agent for Cisco Unity では、サポートされているアンチウイルス アプリケーションが、アンチウイルス コンポーネントへのアップグレードを自動的にダウンロードしてインストールできます。
- Windows レジストリで値を追加、変更、または削除する前。
- Windows のシステム ファイルまたはブート ファイルを変更する前。



#### 注意

Cisco Security Agent サービスを停止して無効にした場合、このサービスによってサーバを再度監視するには、このサービスを再度有効にして開始する必要があります。

このサービスを無効にして再度有効にする方法については、P.13 の「Cisco Security Agent サービスの無効化と再有効化」を参照してください。

## Cisco Security Agent がイベントを記録する場所

Cisco Security Agent は、次の 3 つの場所にイベントを記録します。

Windows アプリケーション イベント ログ	Cisco Security Agent によって生成されるイベントは、CSAgent というイベントソースを持ちます。
Securitylog.txt	<p>Cisco Security Agent は、1 行ごとに 1 つのイベントを記録します。ファイル内のデータは、コンマ区切り値形式です。通常、このファイルにはあまり多くのエントリが含まれていないため、メモ帳などのテキスト エディタでこのファイルを読むことができます (ワードラップをオフにすることをお勧めします)。多くのエントリが存在する場合は、スプレッドシートアプリケーションがインストールされているコンピュータにこのファイルをコピーし、ファイル名拡張子を .txt から .csv に変更して、スプレッドシートアプリケーションでこのファイルを開くと、データを簡単に参照できます。</p> <p>ログを表示するには、[ Cisco Security Agent ] タスクバー アイコンをダブルクリックします。Cisco Security Agent Panel の左側のツリー コントロールにある [ Messages ] をクリックします。続いて、[ View Log ] をクリックします (ログが Program Files\Cisco Systems\CSAgent\Log ディレクトリに表示されます)。</p>
現在のメッセージ	Windows にログオンした後に発生したイベントを表示させるには、[ Cisco Security Agent ] タスクバー アイコンをダブルクリックしてから、Cisco Security Agent Panel にある [ Messages ] をクリックしてください。

## カスタム SQL サーバのバックアップは SQLBackups ディレクトリ内に書き込む (Cisco Unity のみ)

カスタム スクリプトを使用して Cisco Unity 向けの SQL サーバまたは MSDE データベースのバックアップを行う場合、および SQL サーバまたは MSDE がインストールされているディレクトリ以外の場所にバックアップする場合は、SQLBackups というディレクトリを作成し、そのディレクトリにバックアップを保存してください。このように設定すると、SQL Server プロセスに関する Cisco Security Agent の制限によって発生する問題が回避されます。

SQLBackups ディレクトリは、そのパスのどの場所にも作成することができます ( D:\SQLBackups や G:\Backups\SQLBackups\UnityDBBackups など )。



**(注)** Cisco Unity Connection は、サードパーティ製バックアップ ソフトウェアのサポートはしていません。

## Cisco Security Agent for Cisco Unity がインストールされているサーバからの Web ブラウジング



### 注意

Cisco Security Agent for Cisco Unity がインストールされているサーバは Web ブラウジング用に使用しないでください。使用すると、悪意のあるコンテンツが誤ってダウンロードされる可能性があります。Cisco Unity システム管理および Cisco Unity Connection の管理機能が正しく機能できるように、Internet Explorer 用の Cisco Security Agent の保護機能の一部が Cisco Security Agent for Cisco Unity から削除されています。

## 警告

この項では、重大度 1、2、および 3 の警告について説明します。

顧客が必要に応じて問題点を問い合わせることができるオンライン ツール、Bug Toolkit を使用して、すべてのリリースについての重大度の警告だけでなく、Cisco Security Agent for Cisco Unity 3.1(4) に関する最新の警告情報も検索できます。Bug Toolkit は、<http://www.cisco.com/go/bugs> から入手できます。



**(注)** Bug Toolkit にアクセスするには、Cisco.com に登録ユーザとしてログオンしている必要があります。

ここでは、Cisco Security Agent for Cisco Unity 3.1(4) のみに関する警告情報を示しています。以前のバージョンの Cisco Security Agent for Cisco Unity の警告情報については、該当するバージョンのリリース ノートを参照してください。Cisco Security Agent for Cisco Unity のすべてのバージョンに対応するリリース ノートは、[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html) から入手可能です。

### 未解決の警告：リリース 3.1(4)

Bug Toolkit で警告に関する最新情報を表示するには、警告番号の列のリンクをクリックしてください（警告の記載順序は、1 番目に重大度が優先され、2 番目にコンポーネント、3 番目に警告番号の順で並べられます）。

表 1 Cisco Security Agent for Cisco Unity リリース 3.1(4) の未解決の警告

警告番号	コンポーネント	重大度	説明
<a href="#">CSCsm33672</a>	voicecsa	3	CSA - Uninstalling enables Windows Firewall breaking Unity Failover7.0

### 解決済みの警告：リリース 3.1(4)

Bug Toolkit で警告に関する最新情報を表示するには、警告番号の列のリンクをクリックしてください（警告の記載順序は、1 番目に重大度が優先され、2 番目にコンポーネント、3 番目に警告番号の順で並べられます）。



**(注)** 次の表には、Cisco Security Agent for Cisco Unity に固有の解決済みの警告だけが記載されています。Cisco Unity バージョン 3.1(4) のコンパイルに使用した Cisco Security Agent バージョン 5.2.0 ビルド 245 で解決された警告に関する別のリストについては、<http://cisco.com> で、readme ファイル CSA\_5.2.0.245\_readme.txt を検索し参照してください。

表2 Cisco Security Agent for Cisco Unity リリース 3.1(4) の解決済みの警告

警告番号	重大度	コンポーネント	説明
<a href="#">CSCef04484</a>	3	voicecsa	Trend Micro updates blocked by Cisco Security Agent on Unity
<a href="#">CSCef26489</a>	3	voicecsa	CSA Rules Conflict with Exchange Data Paths
<a href="#">CSCef52573</a>	3	voicecsa	SQL Backup Failure with CSA for Unity
<a href="#">CSCef73516</a>	3	voicecsa	CSA for Unity impacts service control manager
<a href="#">CSCef73638</a>	3	voicecsa	CSA for Unity stops automatic service startup
<a href="#">CSCeg70939</a>	3	voicecsa	CSA for Unity prevents Veritas BackupExec 9 and later from running
<a href="#">CSCeg85461</a>	3	voicecsa	CSA for Unity stops Norton AntiVirus 9
<a href="#">CSCsa64708</a>	3	voicecsa	CSA: CsEventSync StoreFiles message copy prevented by CSA
<a href="#">CSCsa73982</a>	3	voicecsa	CSA for Unity does not allow SQL to write UnityDistributionDb.bak
<a href="#">CSCsc79687</a>	3	voicecsa	New registry activity causes conflict with CSA
<a href="#">CSCse00695</a>	3	voicecsa	CSA prevents Subscriber page to load in SA when alias contains .log
<a href="#">CSCse51014</a>	3	voicecsa	CSA prevents Subscriber page to load in SA when name contains [
<a href="#">CSCse68141</a>	3	voicecsa	VUI: CSA blocks start of mrpc-server and compilation-server processes
<a href="#">CSCsg26990</a>	3	voicecsa	CSA prevents Unity logging to data_inetinfo file in non-default location
<a href="#">CSCsh15515</a>	3	voicecsa	CSA 4.5.1.639 with Unity 4.2.1 blue screened upon installation
<a href="#">CSCsi51247</a>	3	voicecsa	BSOD on 7845-H2 with CSA and Windows 2003 SP2

## トラブルシューティング情報

次の各項では、Cisco Security Agent for Cisco Unity のトラブルシューティングについて説明します。

- [ブルー スクリーン状態 \(Cisco Unity のみ\) \(P.19\)](#)
- [MAPI ネットワーク エラー \(Cisco Unity のみ\) \(P.19\)](#)
- [不明な問題、または Cisco Security Agent からのエラー \(P.19\)](#)
- [ソフトウェアの 2 回目のインストール試行が警告なしで失敗する \(P.20\)](#)

### ブルー スクリーン状態 (Cisco Unity のみ)

Cisco Security Agent for Cisco Unity により、Windows 2000 Advanced Server および Cisco Unity-CM TSP バージョン 7.0(3) 以前を実行している Cisco Unity 4.0(3) 以前のサーバでブルー スクリーンが発生することがあります (Cisco Unity 警告 CSCed14125)。

この問題を防止または解決するには、Cisco Unity バージョン 4.0(4) 以降および Cisco Unity-CM TSP バージョン 7.0(4) 以降をインストールします。

### MAPI ネットワーク エラー (Cisco Unity のみ)

Cisco Unity システムで、ユーザがメールボックスにアクセスできず、ネットワークの問題を示す MAPI エラーがイベント ログに記録されるなど、ネットワーク タイプの問題が発生することがあります (Cisco Unity 警告 CSCee13192)。このような問題は、Cisco Security Agent for Cisco Unity がインストールされた Cisco Unity 4.0(4) 以前のシステムが、膨大な負荷のかかった状態で、ハイパースレッドをオンにした 4 プロセッサ サーバ上で実行されている場合に確認されています。この症状が発生し始めると、すべての通話の 5 ~ 10% が影響を受けます。

この問題を防止または解決するには、Cisco Unity サーバ上の BIOS でハイパースレッドを無効にするか、Cisco Unity-CM TSP バージョン 7.0(4b) 以降をインストールしてハイパースレッドをオンにしたままにします。

### 不明な問題、または Cisco Security Agent からのエラー

Cisco Security Agent for Cisco Unity のインストール後に次のいずれかの問題が発生した場合は、この項の手順を実行してください。

- 特定できないシスコ アプリケーションの問題
- Windows のイベント ログ内または Cisco Security Agent のログ ファイル  
<Drive>:\Program Files\Cisco\CSAgent\log\securitylog.txt 内の Cisco Security Agent エラー
- 画面に表示される Cisco Security Agent エラー メッセージ

Cisco Security Agent のログ エントリまたはエラー メッセージの原因が特定できない場合は、Cisco TAC に問い合せてください。

#### 不明な問題、または Cisco Security Agent からのエラーのトラブルシューティング

**ステップ 1** Cisco Security Agent サービスを停止します。

- Windows の [ Start ] メニューで、[ Programs ] > [ Administrative Tools ] > [ Services ] をクリックします。
- 右ペインで、[ Cisco Security Agent ] をダブルクリックします。

- c. [ General ] タブの [ Stop ] をクリックし、サービスをすぐに停止します。
- d. [ OK ] をクリックして [ Cisco Security Agent Properties ] ダイアログボックスを閉じます。

**ステップ 2** エラー メッセージの原因となった操作を行います。

**ステップ 3** Cisco Security Agent サービスを再起動します。

- a. Windows の [ Start ] メニューで、[ Programs ] > [ Administrative Tools ] > [ Services ] をクリックします。
- b. 右ペインで、[ Cisco Security Agent ] をダブルクリックします。
- c. [ General ] タブの [ Start ] をクリックし、サービスを再起動します。
- d. [ OK ] をクリックして [ Cisco Security Agent Properties ] ダイアログボックスを閉じます。

**ステップ 4** エラー メッセージの原因となった操作を行います。

**ステップ 5** Cisco Security Agent を一時停止すると操作が正常に完了し、Cisco Security Agent を有効にすると操作がまた失敗する場合は、サーバ上で動作しているすべてのソフトウェアが、サポートされているソフトウェアとして P.4 の「要件とサポートされているソフトウェア」のリストに記載されていることを確認します。

サポートされていないソフトウェアがサーバにインストールされている場合は、サポートされていないソフトウェアを削除して、この手順を繰り返します。

**ステップ 6** 問題を解決できない場合は、Cisco TAC に連絡して、Cisco Security Agent のログ ファイル <Drive>:\Program Files\Cisco\CSAgent\log\securitylog.txt を送信します。

## ソフトウェアの 2 回目のインストール試行が警告なしで失敗する

次の場合は、ソフトウェアのインストール試行が警告なしで失敗します。

1. 最初に Cisco Security Agent サービスを停止して無効にする操作を行わずに、ソフトウェアのインストールを試みた。
2. Cisco Security Agent により、次のメッセージが表示された。  
「Cisco Security Agent: A problem was detected, press one of the action buttons below.  
Are you installing/uninstalling software?If not, this operation is suspicious.」
3. [ No ] をクリックした。
4. Cisco Security Agent サービスを停止して無効にした。
5. ソフトウェアのインストールを再度試みたが、何も起こらなかった。

ステップ 3. で [ No ] をクリックすると、その応答はメモリにキャッシュされたこととなります。キャッシュは 1 時間後に自動的に消去されます。ソフトウェアをただちにインストールできるようにキャッシュをすぐに消去するには、次の手順を実行します。

**ソフトウェアをインストールできるように Cisco Security Agent のメモリ キャッシュを消去する**

**ステップ 1** Windows タスクバーで、[ Cisco Security Agent ] アイコンをダブルクリックします。

- ステップ 2** Cisco Security Agent Panel の左側のツリー コントロールにある [ User Query Responses ] をクリックします。
- ステップ 3** [ Clear ] をクリックします。
- ステップ 4** [ OK ] をクリックして Cisco Security Agent Panel を閉じます。
- ステップ 5** サーバにソフトウェアを再度インストールしようとする前に、Cisco Security Agent サービスを停止して無効にします。P.13 の「Cisco Security Agent サービスを停止して無効にする」の手順を参照してください。
- ステップ 6** ソフトウェアをインストールしたら、Cisco Security Agent サービスを再度有効にして再起動します。P.14 の「Cisco Security Agent サービスを再度有効にして開始する」の手順を参照してください。

## マニュアルの入手方法および Service Request ツールの使用方法

マニュアルの入手方法、Service Request ツールの使用方法、および追加情報の収集方法については、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。『*What's New in Cisco Product Documentation*』には、シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Really Simple Syndication (RSS) フィードとして『*What's New in Cisco Product Documentation*』に登録し、リーダアプリケーションを使用して、コンテンツがデスクトップに直接配信されるように設定します。RSS フィードは無料サービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.(0805R)

このドキュメントで使用しているインターネット プロトコル (IP) アドレスは、実在のアドレスではありません。ドキュメント中で示される例、コマンドの画面出力、および図は、いずれも視覚的な説明のみを目的としています。実在する IP アドレスが例示されていた場合、それらは意図して使用したものではありません。

Copyright © 2008 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2008, シスコシステムズ合同会社 .  
All rights reserved.

お問い合わせは、購入された各代理店へご連絡ください。

シスコシステムズでは以下のURLで最新の日本語マニュアルを公開しております。  
本書とあわせてご利用ください。

Cisco.com 日本語サイト

[http://www.cisco.com/japanese/warp/public/3/jp/service/manual\\_j/](http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/)

日本語マニュアルの購入を希望される方は、以下のURLからお申し込みいただけます。

シスコシステムズマニュアルセンター

<http://www2.hipri.com/cisco/>

上記の両サイトで、日本語マニュアルの記述内容に関するご意見もお受けいたしますので、  
どうぞご利用ください。

なお、技術内容に関するご質問は、製品を購入された各代理店へお問い合わせください。



シスコシステムズ合同会社

〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先 (シスココンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-933-122 (通話料無料)、03-6670-2992 (携帯電話、PHS)

電話受付時間: 平日 10:00 ~ 12:00、13:00 ~ 17:00