



Cisco Security Agent for Cisco Unity リリース ノート Release 2.0(3)

Published March 6, 2006

このリリース ノートには、Cisco Security Agent for Cisco Unity リリース 2.0(3) 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サポート、および警告に関する情報が記載されています。

Cisco Security Agent for Cisco Unity は、Cisco Unity および Cisco Unity Connection 用にサポートされます。

Cisco Security Agent for Cisco Unity ソフトウェアは、<http://www.cisco.com/cgi-bin/tablebuild.pl/unity3d> の Cisco Unity Crypto Software Download ページから入手可能です。



(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 \(P.7\)](#)
- [新規および変更されたサポート：リリース 2.0\(3\) \(P.7\)](#)
- [インストールとアップグレードに関する情報 \(P.8\)](#)
- [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 \(P.18\)](#)
- [技術情報の入手方法 \(P.22\)](#)
- [シスコ製品のセキュリティの概要 \(P.24\)](#)
- [シスコ製品のセキュリティの概要 \(P.24\)](#)
- [テクニカル サポート \(P.25\)](#)
- [その他の資料および情報の入手方法 \(P.27\)](#)

はじめに

Cisco Security Agent for Cisco Unity は、スタンドアロン Cisco Security Agent であり、P. 4 の「要件とサポートされているソフトウェア」に記載されている要件を満たす Cisco Unity および Cisco Unity Connection のインストール用にシスコシステムズによって無料で提供されます。

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

- Cisco Unity および Cisco Unity Connection ソフトウェアに対する進入検知と防御。
- 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 2.0(3) は、Cisco Security Agent バージョン 4.5.1 ビルド 639 でコンパイルされています。



注意

Cisco Security Agent for Cisco Unity は、Cisco Unity または Cisco Unity Connection のインストール環境に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 Cisco Unity と Cisco Unity Connection の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。お読みいただくことをお勧めします。

また、『*Cisco Unity Security Guide, Release 4.x*』も参照してください。

- このマニュアルの Domino 版は、http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_administration_guide_book09186a008043ea53.html から入手可能です。
- このマニュアルの Exchange 版は、http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_administration_guide_book09186a008043ea54.html から入手可能です。

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。

- [ソフトウェア要件 : Cisco Unity \(P.4 \)](#)
- [サポートされているオプション ソフトウェア : Cisco Unity \(P.4 \)](#)
- [ソフトウェア要件 : Cisco Unity Connection \(P.5 \)](#)
- [サポートされているオプション ソフトウェア : Cisco Unity Connection \(P.5 \)](#)
- [ソフトウェア バージョンの特定 \(P.6 \)](#)

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。
- 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 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 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、メッセージストア 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。

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は、メッセージストア サーバ上や DC/GC 上に Cisco Security Agent for Cisco Unity をインストールしないでください。



(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

Cisco Security Agent for Cisco Unity を実行している Cisco Unity 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。
- 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。
- 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、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 にある適切なバージョンの『Cisco Unity で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。

ソフトウェア要件 : Cisco Unity Connection

- Cisco Unity Connection バージョン 1.1(1) 以降 (Cisco Unity Connection または音声認識サーバ上にインストールされている場合)

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。

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

Cisco Security Agent for Cisco Unity を実行している Cisco Unity Connection、または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。
- Computer Associates eTrust Antivirus バージョン 7.0 以降。
- McAfee VirusScan Enterprise 8.0i。
- 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 にある適切なバージョンの『Cisco Unity Connection システム要件およびサポートされるハードウェアとソフトウェア』で入手できます。

オプション ソフトウェアのサポート ポリシー

シスコのサポート ポリシーでは、お客様は Cisco Unity、Cisco Unity Connection、または Connection 音声認識サーバで、サポートされている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)を展開できます。ただし、シスコは、お客様(またはお客様のシステム統合パートナー)がこのような製品と Cisco Unity または Cisco Unity Connection との相互運用性をテストした上で製品を展開することをお勧めします。このテスト作業により、実稼動環境で、Cisco Unity または Cisco Unity Connection と、サーバにロードされたサードパーティ製品との間で検出される問題のリスクを軽減できます。

問題が発生してお客様が Cisco TAC に連絡した場合、Cisco TAC エンジニアによって、トラブルシューティングの間、このようなサードパーティ製ソフトウェアをオフにするように、または Cisco Unity や Cisco Unity Connection、あるいは Connection 音声認識サーバから削除するように要求されることがあります。サードパーティ製ソフトウェアと、Cisco Unity または Cisco Unity Connection との相互運用性が問題の根本的な原因であると判明した場合、お客様が Cisco Unity または Cisco Unity Connection システムを引き続き使用するには、相互運用性の問題が解決するまでサードパーティ製ソフトウェアを無効にするか、Cisco Unity、Cisco Unity Connection、または Connection の音声認識サーバから削除する必要があります。

適合性が確認されたオプション サービス パックを Cisco Unity、Cisco Unity Connection、または Connection の音声認識サーバにインストールする前に、サーバにインストールする(またはすでにインストールした)オプションのソフトウェアまたはハードウェアの製造元も、その製品でそのサービス パックをサポートしていることを確認してください。

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、『*Cisco Unity Documentation Guide*』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_roadmap09186a00801179df.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、『*Cisco Unity Connection Documentation Guide*』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 でも入手可能です。

新規および変更されたサポート：リリース 2.0(3)

この項では、Cisco Security Agent for Cisco Unity リリース 2.0(3) 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 から入手可能です。

NetIQ AppManager for Cisco Voice Mail バージョン 6.0

Cisco Security Agent for Cisco Unity は、NetIQ AppManager for Cisco Voice Mail バージョン 6.0 をサポートしています。Cisco Unity サーバに、AppManager エージェントをインストールしてください。



注意

Cisco Unity サーバには、このエージェントのみインストールしてください。これを守らないと、Cisco Unity が正しく機能しません。

Cisco Unity Connection サーバへの AppManager のインストールは、現在はサポートされていません。

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 2.0\(3\) のダウンロード \(P.8 \)](#)
- [Cisco Security Agent for Cisco Unity 2.0\(3\) のインストール \(P.10 \)](#)
- [Cisco Security Agent for Cisco Unity 2.0\(3\) へのアップグレード \(P.13 \)](#)
- [インストールとアップグレードに関する注意事項 \(P.13 \)](#)
- [Cisco Security Agent for Cisco Unity のアンインストール \(P.14 \)](#)

Cisco Security Agent for Cisco Unity 2.0(3) のダウンロード

各製品に該当する項を参照してください。

- [Cisco Unity 環境の Cisco Security Agent for Cisco Unity 2.0\(3\) のダウンロード \(P.8 \)](#)
- [Cisco Unity Connection 環境の Cisco Security Agent for Cisco Unity 2.0\(3\) のダウンロード \(P.9 \)](#)

Cisco Unity 環境の Cisco Security Agent for Cisco Unity 2.0(3) のダウンロード

Cisco Unity 環境の Cisco Security Agent for Cisco Unity 2.0(3) をダウンロードする

ステップ 1 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 ファイルおよびインストールするファイル用の 20 MB の空き領域があることを確認します。

ステップ 2 高速インターネット接続が可能なコンピュータで、Cisco Unity Crypto Software Download ページ (<http://www.cisco.com/cgi-bin/tablebuild.pl/unity3d>) 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。

強力な暗号化に対するエクスポート制御のため、Cisco Security Agent for Cisco Unity を初めてダウンロードする場合は、簡単な質問に答える必要があります。画面の指示に従います。

ステップ 3 CiscoUnity-CSA-4.5.1.639-2.0.3-K9.exe をクリックします。

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。

ステップ 5 CD から Cisco Security Agent for Cisco Unity をインストールする場合は、CD を作成します。

Cisco Unity Connection 環境の Cisco Security Agent for Cisco Unity 2.0(3) のダウンロード

Cisco Unity Connection では、Cisco Security Agent for Cisco Unity は Cisco Unity Connection Server Updates ウィザードの一部となっています。P. 8 の「Cisco Unity 環境の Cisco Security Agent for Cisco Unity 2.0(3) のダウンロード」でも説明しているとおり、Cisco Security Agent for Cisco Unity を個別に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 Connection 用に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/products/ps6509/prod_pre_installation_guide09186a008055e2d4.html にある『Cisco Unity Connection 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)

Cisco Unity Connection 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 Unity Connection Software Download ページ (<http://www.cisco.com/cgi-bin/tablebuild.pl/unityconnection>) 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** 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(ダウンロード ファイルのサイズは、Cisco Unity Connection Software Download ページに表示されます)。

- ステップ 3** Cisco Unity Connection Server Updates ウィザード ファイルの名前をクリックします。

- 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。

- ステップ 5** Cisco Unity Connection 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 6** ウィザード用の CD を 1 枚作成し、「Cisco Unity Connection Server Updates ウィザード <日付>」とラベルを貼っておきます。

シスコ製品に付属の Cisco Unity Connection Server Updates ウィザード CD をお持ちの場合は、インストール時にこの付属 CD を誤って使用しないよう、別の場所に保管しておいてください。

- ステップ 7** 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 2.0(3) のインストール

各製品に該当する項を参照してください。

- [Cisco Unity 環境の Cisco Security Agent for Cisco Unity 2.0\(3\) のダウンロード \(P.10 \)](#)
- [Cisco Unity Connection 環境の Cisco Security Agent for Cisco Unity 2.0\(3\) のインストール \(P.11 \)](#)

Cisco Unity 環境の Cisco Security Agent for Cisco Unity 2.0(3) のダウンロード



(注) Cisco Security Agent for Cisco Unity をバージョン 2.0(3) にアップグレードする場合は、[P. 13 の「Cisco Security Agent for Cisco Unity 2.0\(3\) 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 Cisco Unity 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 Cisco Unity 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 Unity 環境の Cisco Security Agent for Cisco Unity 2.0(3) をインストールする

- ステップ 1** Administrators グループまたはローカルの 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** サーバのハードディスクに、ダウンロード ファイルおよびインストールするファイル用の少なくとも 20 MB の空き領域があることを確認します。
- ステップ 3** サーバに別の侵入検知アプリケーションがインストールされている場合は、Cisco Security Agent for Cisco Unity をインストールする前に、そのアプリケーションをアンインストールします。該当するドキュメントを参照してください。
- ステップ 4** 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 5** 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 [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。
 - [Stop] をクリックし、サービスをすぐに停止します。

- e. [OK] をクリックして [Properties] ダイアログボックスを閉じます。
- f. 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。
- g. 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 6 Windows エクスプローラで、Cisco Security Agent for Cisco Unity ファイルをダウンロードしたディレクトリを表示し、CiscoUnity-CSA-4.5.1.639-2.0.3-K9.exe をダブルクリックします。

ステップ 7 画面の指示に従います。



注意 デフォルト値は変更しないでください。変更すると、Cisco Security Agent for Cisco Unity が正しく機能しない可能性があります。

ステップ 8 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 9 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、それらのウイルス スキャン サービスを再度有効にして開始します。

- 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、最初のスキャン サービスの名前をダブルクリックします。
- c. [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。
- d. [Start] をクリックし、サービスを開始します。
- e. [OK] をクリックして [Properties] ダイアログボックスを閉じます。
- f. 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。
- g. 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 Unity Connection 環境の Cisco Security Agent for Cisco Unity 2.0(3) のインストール



(注) Cisco Security Agent for Cisco Unity をバージョン 2.0(3) にアップグレードする場合は、[P. 13 の「Cisco Security Agent for Cisco Unity 2.0\(3\) へのアップグレード」](#)を参照してください。

Connection サーバ、および音声認識サーバ（存在する場合）で Cisco Unity Connection Server Updates ウィザードを実行します。

Cisco Unity Connection 環境の Cisco Security Agent for Cisco Unity 2.0(3) をインストールする

- 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 Connection 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。

- d. [Start] をクリックし、サービスを開始します。
- e. [OK] をクリックして [Properties] ダイアログボックスを閉じます。
- f. 残りのウィルス 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。
- g. すべてのウィルス 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 2.0(3) へのアップグレード

Cisco Security Agent for Cisco Unity のバージョン 2.0(3) にアップグレードするには、この項のタスク リストを使用します。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。

アップグレードのタスク リスト

1. ソフトウェアをダウンロードします。P. 8 の「Cisco Security Agent for Cisco Unity 2.0(3) 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 2.0(3) をインストールします。P. 10 の「Cisco Security Agent for Cisco Unity 2.0(3) 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。

インストールとアップグレードに関する注意事項

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 サービスを停止します。
 - 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 [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** 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 Unity、Cisco Unity Connection、または Connection 音声認識サーバからの 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 サービスを無効にして停止する必要があります。

- 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ィルス アプリケーションが、アンチウィルス 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で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 Unity、Cisco Unity Connection、または Connection 音声認識サーバからの Web ブラウジング



注意

Web ブラウジングに Cisco Unity、Cisco Unity Connection、または Connection 音声認識サーバを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を誤ってダウンロードしてしまう可能性があります。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 2.0(3) 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/cgi-bin/Support/Bugtool/launch_bugtool.pl から入手可能です。



(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 2.0(3) 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 から入手可能です。

公開されている警告：リリース 2.0(3)

Cisco Security Agent for Cisco Unity リリース 2.0(3) について公開されている警告はありません。

解決済みの警告：リリース 2.0(3)

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 2.0(3) の解決済みの警告

警告番号	コンポーネント	重大度	説明
CSCsc56607	voicecsa	3	Unity Connection Disaster Recovery Tool (DiRT) が、CSA が有効の状態でも失敗する
CSCsc79687	voicecsa	3	新しいレジストリのアクティビティにより、CSA との障害が生じる

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。

- [Cisco Personal Communications Assistant または Cisco Unity Inbox へのアクセス問題 \(P.18\)](#)
- [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 \(Cisco Unity のみ\)\(P.19\)](#)
- [Cisco Unity、Cisco Unity Connection、または音声認識での問題、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 \(P.20\)](#)

Cisco Personal Communications Assistant または Cisco Unity Inbox へのアクセス問題

Cisco Security Agent for Cisco Unity がユーザ ワークステーションにインストールされている場合、Cisco Personal Communications Assistant (PCA) への最初のログオン時、または Cisco Unity Inbox の最初の使用時に、偽陽性の悪質コード検出ダイアログボックスが表示されることがあります。さらに、Cisco Unity Inbox または Cisco Unity Assistant で Media Master コントロール バーを使用できない場合があります。ダイアログボックスに表示されるテキストは、使用している Cisco Security Agent for Cisco Unity ポリシーによって異なりますが、必ず「Cisco Security Agent: A problem was detected, press one of the actions below.」で始まります。

ユーザが Cisco PCA にログオンしようとしたとき、または Cisco Unity Inbox にアクセスしようとしたときに、Cisco Security Agent for Cisco Unity ダイアログボックスが表示される場合は、次のうち該当する手順を実行します。

ユーザ ワークステーションで Cisco Security Agent for Cisco Unity を使用している場合の Cisco PCA または Cisco Unity Inbox へのアクセス問題を解決する

ステップ 1 Cisco Security Agent for Cisco Unity ダイアログボックスで、[Yes] または [Yes to All] をクリックします。この操作により、ソフトウェアのインストールが認められます。このアクションは、Media Master コントロール バーを使用できるようにするために必要です。これ以降の手順は不要です。

ユーザが、問題を報告する前に、[Yes] または [Yes to All] ではなく [No] または [No to All] をクリックした場合は、[ステップ 2 ~ ステップ 8](#) を実行します。

ステップ 2 Cisco PCA からログアウトします。

ステップ 3 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 4 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 5 [Clear] をクリックします。

ステップ 6 [OK] をクリックして Cisco Security Agent Panel を閉じます。

ステップ 7 Cisco PCA にログオンします。必要に応じて、Cisco Unity Inbox にアクセスします。

- ステップ 8** Cisco Security Agent for Cisco Unity ダイアログボックスが表示されたら、[Yes] または [Yes to All] をクリックします。Media Master コントロール バーが表示されます。

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。

Cisco Unity、Cisco Unity Connection、または音声認識での問題、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。

- ほかに原因の考えられない Cisco Unity、Cisco Unity Connection、または音声認識での問題
- 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。

Cisco Unity、Cisco Unity Connection、または音声認識での問題、または Cisco Security Agent からのエラーのトラブルシューティングを行う

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

- 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 [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、Cisco Unity 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。
-

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

マニュアルの最新版は、次の URL で参照できます。

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

シスコの Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com>

各国のシスコ Web サイトには、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

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

このマニュアルには、日本語化されたマニュアル名と英語版 URL が併記された箇所があります。日本語版マニュアルを参照する場合は、次の URL にアクセスしてください。

http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/index_uc_cu.shtml

Product Documentation DVD (英語版)

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納した、包括的なライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関する複数のバージョンのマニュアルにアクセスできます。また、この DVD を使用すると、シスコの Web サイトで参照できるのと同じ HTML マニュアルに、インターネットに接続せずにアクセスできます。一部の製品については、PDF 版のマニュアルもご利用いただけます。

Product Documentation DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザ (Cisco Direct Customers) の場合は、Cisco Marketplace から Product Documentation DVD (Product Number DOC-DOCDVD= または DOC-DOCDVD=SUB) を発注できます。次の URL にアクセスしてください。

<http://www.cisco.com/go/marketplace/>

マニュアルの発注方法 (英語版)

Cisco.com 登録ユーザの場合は、Cisco Marketplace の Product Documentation Store からシスコ製品の英文マニュアルを発注できるようになっています。次の URL にアクセスしてください。

<http://www.cisco.com/go/marketplace/>

Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

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

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

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

なお、技術内容に関するお問い合わせは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合わせください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル (英文のみ) を無料で提供していません。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトで、次に関する情報を確認できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告、セキュリティ注意事項、およびセキュリティ対応に関する最新のリストには、次の URL からアクセスできます。

<http://www.cisco.com/go/psirt>

セキュリティ勧告、セキュリティ注意事項、およびセキュリティ対応がアップデートされた時点でリアルタイムに確認する場合は、Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) フィードを利用できます。PSIRT RSS フィードの利用方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合 : security-alert@cisco.com (英語のみ)
緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと思なされます。
- 緊急でない場合 : psirt@cisco.com (英語のみ)

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302 (英語のみ)
- 1 408 525-6532 (英語のみ)



ヒント

シスコに機密情報をお送りいただく際には、PGP (Pretty Good Privacy) または互換製品 (GnuPG など) を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.x から 9.x で暗号化されている情報に対応しています。

無効になった、または有効期限が切れた暗号キーは、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

PGP を持っていない、または使用していない場合は、機密情報を送信する前に前述のメールアドレスまたは電話番号で PSIRT に問い合わせ、他のデータ暗号化方法を確認してください。

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center (TAC) のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合わせください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

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

Cisco Technical Support & Documentation Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://tools.cisco.com/RPF/register/register.do>



(注)

Web または電話でサービス リクエストを発行する前に、Cisco Product Identification (CPI) ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support & Documentation Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト (<http://www.cisco.com/tac>) のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

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

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

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

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます (S3: ネットワークに軽微な障害が発生した、S4: 製品情報が必要である)。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

<http://www.cisco.com/techsupport/servicerequest>

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合わせください (S1: ネットワークがダウンした、S2: ネットワークの機能が著しく低下した)。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

<http://www.cisco.com/techsupport/contacts>

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1 (S1): 既存のネットワークがダウンした状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2 (S2): 既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3 (S3): ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4 (S4): シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- 『Cisco Product Quick Reference Guide』は手軽でコンパクトな参照ツールです。チャネルパートナー経由で販売される多くのシスコ製品に関する簡単な製品概要、主要な機能、サンプル部品番号、および簡単な技術仕様を記載しています。年 2 回の更新の際には、シスコの最新情報が収録されます。『Cisco Product Quick Reference Guide』の注文方法および詳細については、次の URL にアクセスしてください。

<http://www.cisco.com/go/guide>

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

<http://www.cisco.com/go/marketplace/>

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版物やその他の情報を調べるには、次の URL から Cisco Press にアクセスしてください。

<http://www.ciscopress.com>

- 『Packet』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『Packet』には、次の URL からアクセスしてください。

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

日本語版『Packet』は、米国版『Packet』と日本版のオリジナル記事で構成されています。日本語版『Packet』には、次の URL からアクセスしてください。

<http://www.cisco.com/japanese/warp/public/3/jp/news/packet/>

- 『iQ Magazine』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、事例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『iQ Magazine』には、次の URL からアクセスしてください。

<http://www.cisco.com/go/iqmagazine>

デジタル版には、次の URL からアクセスできます。

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- 『Internet Protocol Journal』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『Internet Protocol Journal』には、次の URL からアクセスしてください。

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

- シスコシステムズが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共有できます。次の URL にアクセスしてディスカッションに参加してください。

<http://www.cisco.com/discuss/networking>

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

<http://www.cisco.com/en/US/learning/index.html>

CCSP、CCVP、Cisco Square Bridge のロゴ、Follow Me Browsing、および StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、および iQuick Study は、Cisco Systems, Inc. のサービス マークです。Access Registrar、Aironet、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Cisco Unity、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、FormShare、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、ScriptShare、SlideCast、SMARTnet、The Fastest Way to Increase Your Internet Quotient、および TransPath は、米国および一部の国における Cisco Systems, Inc. とその関連会社の登録商標です。

このマニュアルまたは Web サイトで言及されているその他の商標はすべて、それぞれの所有者のもです。「パートナー」という語の使用は、シスコと他社の提携関係を意味するものではありません。(0601R)

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 © 2006, Cisco Systems, Inc.
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/

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。



シスコシステムズ株式会社

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

問合せ URL:<http://www.cisco.com/jp/service/contactcenter/>

〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL.03-5549-6500 FAX.03-5549-6501