



## Cisco Security Agent 1.1(5) for Cisco Unity リリースノート

---

*Published April 14, 2005*

このリリース ノートには、Cisco Security Agent for Cisco Unity リリース 1.1(5) 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機能、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 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 \( P.4 \)](#)
- [ソフトウェア バージョンの特定 \( P.6 \)](#)
- [Cisco Security Agent for Cisco Unity の使用に関する注意事項 \( P.8 \)](#)
- [Cisco Security Agent for Cisco Unity 1.1\(5\) のダウンロード \( P.10 \)](#)
- [Cisco Security Agent for Cisco Unity 1.1\(5\) のインストール \( P.11 \)](#)
- [Cisco Security Agent for Cisco Unity 1.1\(5\) 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 \( P.14 \)](#)
- [Cisco Security Agent for Cisco Unity のアンインストール \( P.15 \)](#)
- [新規および変更された機能：リリース 1.1\(5\) \( P.16 \)](#)
- [警告 \( P.17 \)](#)
- [トラブルシューティング \( P.18 \)](#)
- [Cisco Unity ドキュメンテーション \( P.21 \)](#)
- [技術情報の入手方法 \( P.21 \)](#)
- [シスコ製品のセキュリティの概要 \( P.23 \)](#)
- [テクニカル サポート \( P.24 \)](#)
- [その他の資料および情報の入手方法 \( P.26 \)](#)

## 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」に記載されているシステム要件を満たす Cisco Unity サーバ用にシスコシステムズによって無料で提供されます。このエージェントは、テスト済みのセキュリティ規則（ポリシー）セットに基づいて、侵入防御、悪意のあるモバイル コードに対する保護、オペレーティング システムの完全性保証、および監査ログの統合を提供します。このエージェントは、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することによって、システムの動作を制御します。このプロセスは透過的に行われ、全体的なシステム パフォーマンスに大きな影響を及ぼしません。



### 注意

Cisco Security Agent for Cisco Unity は、Cisco Unity サーバ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、ウィルス スキャン ソフトウェアやファイアウォールなど、他の防御製品と共に使用した場合に、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 インストールやコンフィギュレーションに対して防御を強化するように設計されています。このため、ネットワーク アクセス制御規則を強制的に実行したり、ホストベース 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。

このエージェントは、CiscoWorks Management Center for Cisco Security Agents を使用して作成され、次の Management Center for Cisco Security Agents バージョン 4.0.3 ビルド 736 ポリシーに基づいています。

- Required Windows System Module
- Common Security Module
- Common Web Server Security Module
- Restrictive MS IIS Module
- Server Module
- User Authentication Auditing Module
- Virus Scanner Module
- Restrictive SQL Server Module

Cisco Security Agent for Cisco Unity バージョン 1.1(5) には、Unity Base Group Exceptions ポリシーも含まれています。このポリシーでは、他のポリシーが許可しない一般的な Cisco Unity 動作が許可されます。

Cisco Security Agent for Cisco Unity に含まれるポリシーを追加、削除、または表示するには、CiscoWorks Management Center for Cisco Security Agents を実行し、CiscoUnity-CSA-4.0.30.736-1.10.5.export ファイルをインポートします。このファイルは、<http://www.cisco.com/cgi-bin/tablebuild.pl/unity3d> から入手可能です (CiscoWorks Management Center for Cisco Security Agents を使用するために、部品 CSA-IPT-UPGRADE-K9 を注文する必要もあります)。

CiscoWorks Management Center for Cisco Security Agents および Cisco Security Agent の詳細については、<http://www.cisco.com/en/US/products/sw/cscowork/ps5212/index.html> 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

### ソフトウェア要件

- 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 2000 Server、英語版 Windows 2000 Advanced Server、または英語版 Windows Server 2003。他の言語バージョンはサポートされていません。
- 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。



(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 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。
- 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。
- 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。
- 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。

## 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、バックアップ、監視、およびセキュリティのために、Cisco Unity サーバで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 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 サーバにロードされた Cisco Unity と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 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 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 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 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 サーバにインストールする前に、Cisco Unity 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

この項では、次のソフトウェアについて使用しているバージョンを特定する手順を説明します。

- [Cisco Security Agent \( P.6 \)](#)
- [Cisco Security Agent for Cisco Unity のポリシー \( P.7 \)](#)

### Cisco Security Agent

#### 使用している Cisco Security Agent のバージョンを特定する

---

ステップ 1 Regedit を起動します。



**注意** 間違ったレジストリ キーを変更、または不正な値を入力すると、サーバが正しく動作しなくなることがあります。レジストリを編集する前に、問題が発生した場合にレジストリを復元する方法を知っておく必要があります(レジストリ エディタ ヘルプの Restoring トピックを参照してください)。レジストリ キー設定の変更に関する質問がある場合は、Cisco TAC に連絡してください。

---

ステップ 2 現在のレジストリのバックアップがない場合は、**Registry > Export Registry File** をクリックし、レジストリ設定をファイルに保存します。

ステップ 3 次のキーを展開します。  
HKEY\_LOCAL\_MACHINE\Software\Cisco Systems, Inc.\System Info\CSA Agent\Version

ステップ 4 Regedit を閉じます。

---

## Cisco Security Agent for Cisco Unity のポリシー

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

ステップ 1 Regedit を起動します。



**注意** 間違ったレジストリ キーを変更、または不正な値を入力すると、サーバが正しく動作しなくなることがあります。レジストリを編集する前に、問題が発生した場合にレジストリを復元する方法を知っておく必要があります(レジストリ エディタ ヘルプの Restoring トピックを参照してください)。レジストリ キー設定の変更に関する質問がある場合は、Cisco TAC に連絡してください。

ステップ 2 現在のレジストリのバックアップがない場合は、**Registry > Export Registry File** をクリックし、レジストリ設定をファイルに保存します。

ステップ 3 次のキーを展開します。  
HKEY\_LOCAL\_MACHINE\Software\Cisco Systems, Inc.\System Info\Unity-CSA Policy\Version

ステップ 4 Regedit を閉じます。

## Cisco Security Agent for Cisco Unity の使用に関する注意事項

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.8)
- Cisco Security Agent タスクバー アイコンは、Windows に最初にログオンしたユーザだけが使用できる (P.9)
- Cisco Security Agent がイベントを記録する場所 (P.9)
- Cisco Unity バックアップ用のカスタム SQL スクリプトは SQLBackups ディレクトリ内に記述 (P.9)
- Cisco Unity サーバからの Web ブラウジング (P.9)

### 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。

- 次の場所で任意の Cisco Unity ツールを使用する前。
  - Cisco Unity Tools Depot
  - CommServer\Utilities ディレクトリ
  - CommServer\TechTools ディレクトリ
- CiscoUnityTools.com からダウンロードした任意の Cisco Unity ツールを使用する前。
- Cisco Unity サーバに任意のソフトウェアをインストールする前。
- 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 Unity サーバ上で任意のソフトウェア (Cisco Unity を含む) 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ウイルス スキャン アプリケーションが、ウイルス スキャン 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

net stop コマンドやタスクバーの Cisco Security Agent アイコンを使用して Cisco Security Agent サービスを停止しないでください。これらの方法はサポートされていません。



注意

Cisco Security Agent サービスを無効にして停止した場合、このサービスによって Cisco Unity 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.14 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 タスクバー アイコンは、Windows に最初にログオンしたユーザだけが利用できる

2人のユーザが Cisco Unity サーバ上の Windows にログオンした場合（1人はサーバで、もう1人は Windows ターミナル サービスを使用して、または両者ともターミナル サービスを使用して）、最初にログオンしたユーザだけが Cisco Security Agent アイコンにアクセスできます。

## 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。

<b>Windows アプリケーション イベント ログ</b>	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。
<b>Securitylog.txt</b>	Cisco Security Agent は、1行ごとに1つのイベントを記録します。Cisco Unity サーバにログオンする各管理者が Securitylog.txt へのショートカットを Windows デスクトップに追加することをお勧めします。このファイルは、<InstallDirectory>\Cisco\CSAgent\Log ディレクトリにあります。  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。
<b>CSA Control Panel</b>	CSA Control Panel 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、Messages タブをクリックします。Windows にログオンした後に発生したイベントだけが、CSA Control Panel に表示されます。

## Cisco Unity バックアップ用のカスタム SQL スクリプトは SQLBackups ディレクトリ内に記述

カスタム SQL スクリプトを使用して Cisco Unity をバックアップする場合は、スクリプトを SQLBackups ディレクトリ内のパスに記述するように設定してください。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 ディレクトリが存在しない場合は、作成してください（D:\SQLBackups や G:\Backups\SQLBackups\UnityDBBackups など）。

## Cisco Unity 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 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 システム管理が正しく機能できるように、Internet Explorer 用の Cisco Security Agent 保護機能の一部が Cisco Security Agent for Cisco Unity から削除されています。

## Cisco Security Agent for Cisco Unity 1.1(5) のダウンロード

### Cisco Security Agent for Cisco Unity 1.1(5) 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-4.0.30.736-1.10.5-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 Security Agent for Cisco Unity 1.1(5) のインストール



(注) Cisco Security Agent for Cisco Unity をバージョン 1.1(5) にアップグレードする場合は、P.13 の「Cisco Security Agent for Cisco Unity 1.1(5) 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 Security Agent for Cisco Unity 1.1(5) 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 Cisco Unity 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 Cisco Unity サーバに Cisco IDS Host Sensor または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。Cisco IDS Host Sensor のドキュメントまたは他の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 Cisco Unity サーバにウィルス スキャン 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。
- a. Windows の Start メニューで、**Program > Administrative Tools > Services** をクリックします。
  - b. 右ペインで、最初のウィルス 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、**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。
  - d. **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. 残りのウィルス スキャン サービスごとにステップ 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参照し、**CiscoUnity-CSA-4.0.30.736-1.10.5-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 デフォルト値を変更しないでください。変更すると、Cisco Security Agent 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。

Cisco Unity 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 Cisco Unity サーバにウイルス スキャン 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。

- a. Windows の Start メニューで、**Program > Administrative Tools > Services** をクリックします。
- b. 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。
- 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 サービスごとにステップ 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 Security Agent for Cisco Unity 1.1(5) へのアップグレード

Cisco Security Agent for Cisco Unity のバージョン 1.1(5) 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.10 の「[Cisco Security Agent for Cisco Unity 1.1\(5\) のダウンロード](#)」を参照してください。
2. Cisco Security Agent サービスを無効にします。P.14 の「[Cisco Security Agent サービスの無効化と再有効化](#)」の「[Cisco Security Agent サービスを無効にして停止する](#)」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.15 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 1.1(5) をインストールします。P.11 の「[Cisco Security Agent for Cisco Unity 1.1\(5\) 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 Unity サーバ上で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前に、Cisco Security Agent サービスを無効にして停止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.8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)。



注意

Cisco Security Agent サービスを無効にして停止した場合、このサービスによって Cisco Unity 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。



注意

net stop コマンドやタスクバーの Cisco Security Agent アイコンを使用して Cisco Security Agent サービスを停止しないでください。これらの方法はサポートされていません。

### Cisco Security Agent サービスを無効にして停止する

- ステップ 1 Windows の Start メニューで、**Program > 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、**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 4 **Stop** をクリックし、サービスをすぐに停止します。
- 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、**Program > 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** Windows タスクバーで **Cisco Security Agent** アイコンを右クリックし、**Suspend Security** をクリックします。

このアイコンがタスクバーにない場合は、Windows の Start メニューで **Programs > Administrative Tools > Services** をクリックし、**Cisco Security Agent** サービスを停止します。

**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、Cisco Unity サーバを再起動します。

---

## 新規および変更された機能：リリース 1.1(5)

この項では、Cisco Security Agent for Cisco Unity リリース 1.1(5) 限定の新規および変更された機能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。

## バージョン 1.1(5) は Cisco Security Agent バージョン 4.0.3.736 でコンパイル

Cisco Security Agent for Cisco Unity 1.1(5) は、Cisco Security Agent バージョン 4.0.3 ビルド 736 でコンパイルされています。

## 警告

この項では、重大度 1 と 2、および重大度 3 の警告（抜粋）について説明します。

Cisco.com のアカウントを持っている場合は、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、この項の警告の詳細も検索できます。Bug Toolkit は、Web サイト ([http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)) から入手可能です。

この項では、Cisco Security Agent for Cisco Unity バージョン 1.1(5)、および Cisco Security Agent for Cisco Unity に影響を及ぼす可能性のある Cisco Security Agent バージョン 4.0.1 ビルド 539 ~ 4.0.3 ビルド 736 の警告情報を示していることに注意してください。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。

### 公開されている警告：リリース 1.1(5)

Cisco Security Agent for Cisco Unity リリース 1.1(5) 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 1.1(5)

表 1 Cisco Security Agent for Cisco Unity リリース 1.1(5) の解決済みの警告

警告番号	重大度	コンポーネント	説明
CSCeg67061	2	csa	あるスレッドで使用中の変数を別のスレッドで Null に設定した場合に、ブルー スクリーンが発生する。
CSCef52573	3	voicecsa	CSA for Cisco Unity 実行中に SQL バックアップが失敗する。
CSCeg70939	3	voicecsa	CSA for Cisco Unity が原因で、Veritas BackupExec 9 以降が実行できない。
CSCeg85461	3	voicecsa	CSA for Cisco Unity により Norton AntiVirus 9 が停止する。
CSCsa64708	3	voicecsa	CSA が原因で、CsEventSync StoreFiles メッセージをコピーできない。
CSCsa73982	3	voicecsa	SQL の UnityDistributionDb.bak への記述が CSA for Cisco Unity で許可されない。

## トラブルシューティング

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 \(P.18\)](#)
- [Cisco Unity サーバでのブルー スクリーン状態 \(P.19\)](#)
- [MAPI ネットワーク エラー \(P.19\)](#)
- [Cisco Unity 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( Cisco 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 7](#) 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** **Advanced** タブをクリックします。

**ステップ 5** **Clear** をクリックします。

**ステップ 6** 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 7** 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。

---

## Cisco Unity サーバでのブルー スクリーン状態

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 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 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 での問題
- Windows のイベント ログまたは 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 に問い合わせてください。

### Cisco Unity 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 Windows タスクバーで、Cisco Security Agent アイコンを右クリックし、Suspend Security をクリックします。
- 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 Windows タスクバーで、Cisco Security Agent アイコンを右クリックし、Resume Security をクリックします。
- 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 サービスを無効にして停止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 サービスを無効にして停止した。
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** **Advanced** タブをクリックします。

**ステップ 3** **Clear** をクリックします。

**ステップ 4** Cisco Security Agent Control 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 サービスを無効にします。P.14 の「Cisco Security Agent サービスを無効にして停止する」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。

## Cisco Unity ドキュメンテーション

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、Cisco.com ([http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/about/aboutdoc.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/about/aboutdoc.htm)) でも入手可能です。

## 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/univercd/home/home.htm>

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](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 からアクセスできます。

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

### Documentation DVD (英語版)

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Documentation DVD パッケージでご利用いただけます。Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。また、この Documentation DVD パッケージのみを発注することもできます。

Cisco.com 登録ユーザ (Cisco Direct Customers) の場合、Ordering Tool または Cisco Marketplace から Cisco Documentation DVD (Product Number DOC-DOCDVD=) を発注できます。

Cisco Ordering tool :

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace :

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

## マニュアルの発注方法（英語版）

英文マニュアルの発注方法については、次の URL にアクセスしてください。

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

シスコ製品の英文マニュアルは、次の方法で発注できます。

- Cisco.com ( Cisco Direct Customers ) に登録されている場合、Ordering Tool からシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。  
<http://www.cisco.com/en/US/partner/ordering/>
- 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](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

このサイトは、次の目的に利用できます。

- 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および注意事項の最新のリストには、次の URL からアクセスできます。

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

勧告および注意事項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、次の URL から Product Security Incident Response Team Really Simple Syndication ( PSIRT RSS ) フィードにアクセスしてください。

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](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](mailto:security-alert@cisco.com) ( 英語のみ )
- 緊急でない場合 : [psirt@cisco.com](mailto:psirt@cisco.com) ( 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 8.x と互換性のある暗号化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キーは、次の公開キー サーバのリストで作成日が最新のキーです。

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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 )

## テクニカル サポート

シスコと正式なサービス契約を交わしているすべてのお客様、パートナー、および代理店は、Cisco Technical Support で 24 時間テクニカル サポートを利用することができます。Cisco.com の Cisco Technical Support 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、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 Web サイト

Cisco Technical Support 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 365 日、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 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 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、Cisco TAC 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、Cisco TAC 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): 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 Marketplace では、シスコの書籍やリファレンス ガイド、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、ネットワーキング全般、トレーニング、および認定資格に関する書籍を広範囲にわたって出版しています。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>

- 『*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>

CCIP、CCSP、Cisco Arrow のロゴ、Cisco Powered Network のマーク、Cisco Unity、Follow Me Browsing、FormShare、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。Aironet、ASIST、BPX、Catalyst、CCDA、CCDP、CCIE、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco IOS のロゴ、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Empowering the Internet Generation、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、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、Registrar、ScriptShare、SlideCast、SMARTnet、StrataView Plus、SwitchProbe、TeleRouter、The Fastest Way to Increase Your Internet Quotient、TransPath、および VCO 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ので、「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。(0403R)

Copyright © 2005, 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/](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