Cisco Security Agent for Cisco Unified Communications Manager のインストール

このドキュメントでは、Cisco Unified Communications Manager（以前は Cisco Unified CallManager）の次のリリースに対応する Cisco Security Agent（CSA）のインストール手順および関連情報について説明します。

- Release 4.x
- Release 5.x
- Release 6.x

（注） Cisco Security Agent は、自動的に Releases 5.x および 6.x 対応としてインストールされます。

Cisco Unified Communications Manager と Cisco Customer Response Solutions（CRS）が同一サーバ上に共存する場合、どちらの製品も同じセキュリティ ポリシーを使用するので、このドキュメントまたは『*Installing Cisco Security Agent for Cisco Customer Response Solutions*』のドキュメントに従って、その共存サーバに Cisco Security Agent をインストールすることができます。

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

OL-12365-01-J

目次

このマニュアルは、次の内容で構成されています。

はじめに

Cisco Security Agent は、Cisco Unified Communications Manager クラスタに侵入検知および侵入防止の機能を提供します。シスコシステムズでは、これを Cisco Unified Communications Manager の音声クラスタ内でサーバを共用する際のスタンドアロンのセキュリティ エージェントとして無料で提供します。このエージェントは、一連の検証済みセキュリティ規則（ポリシー）に基づいて、プラットフォームのセキュリティを実現します。このポリシーには、ホスト侵入検知と侵入防止に関する厳密なレベルが設定されています。システム リソースへのアクセスが行われる前に、このエージェントは特定のシステム動作を許可または拒否するポリシーを適用することにより、システム運用を制御します。

この処理は透過的に行われるためユーザからは見えず、システム全体のパフォーマンスにも影響しません。

（注） Cisco Security Agent for Cisco Unified Communications Manager は、特に Cisco Unified Communications Manager および Cisco CRS ソフトウェアに対応するように設計されていますが、そのほかシスコが承認したサードパーティ製のアプリケーションもサポートしています。また、Web サービスおよびデータベース サービスのセキュリティも実現します。さらに、ホストベースの侵入検知システムとして機能する Network Shim がインストールされていれば、TCP/IP のセキュリティ チェックも実行します。エージェントの最新バージョンが提供されたときは、そのバージョンをインストールすることを強くお勧めします。

また、シスコが提供するオペレーティング システム サービスの最新リリースおよびアップグレードと、このエージェントを連動させることを強くお勧めします。シスコが提供するオペレーティング システム サービスのリリースとアップグレードを取得するには、表 1 を参照してください。

場合によっては、DMA を稼動するために、事前に Cisco Security Agent for Cisco Unified Communications Manager をアンインストールする必要が生じることがあります。詳細については、『*Data Migration Assistant ユーザ ガイド Release 5.1(1)*』およびそれ以降のリリースの該当するマニュアルを参照してください。

スタンドアロンの Cisco Security Agent は、変更ができない静的ポリシーを使用します。ただし、Cisco Unified Communications Manager 以外および Cisco Unified Contact Center Express 以外を対象とするポリシーを変更する場合の詳細については、P.16 の「Management Center for Cisco Security Agent への移行」を参照してください。

このドキュメントのインストール手順に従って、Cisco Unified Communications Manager、Cisco CRS、リモート データベース サーバ、音声サーバ、スピーチ サーバなど、音声クラスタ内のすべてのサーバに CSA をインストールしてください。クライアント マシンにはエージェントをインストールしないでください。

Cisco Security Agent for Cisco Unified Communications Manager のポリシーは、シスコが承認した多数のサードパーティ製モニタリング ツールもサポートします。たとえば、次のアプリケーションをサポートします。

- BMC Patrol
- Concord eHealth Monitor
- Diskeeper Server Standard Edition 8.0.478.0
- HP OpenView Operations Agent 7.1
- HP OpenView Performance Manager 3.3
- Integrated Research Prognosis

- McAfee VirusScan 7.0
- Micromuse Netcool
- NAI Epolicy Agent
- NetIQ Vivinet Manager
- RealVNC
- Symantec Corporate Edition 8.0
- Trend Anti-Virus

（注） Cisco Unified Communications Manager Release 5.x および Release 6.x は、上記のアプリケーションをサポートしていません。

シスコが承認していないサードパーティ製のソフトウェア ツールを使用する場合の詳細については、P.16 の「Management Center for Cisco Security Agent への移行」を参照してください。

システム要件

次の要件は、Cisco Unified Communications Manager Release 4.x に適用されます。

- Cisco Unified Communications Manager :『*Cisco Unified Communications Manager Compatibility Matrix*』には、サポートされている Cisco Unified Communications Manager のリリースについて記載されています。『*Cisco Unified Communications Manager Compatibility Matrix*』を入手するには、表 1 を参照してください。
- Microsoft Windows 2000 Server（英語版）

次の要件は、Cisco Unified Communications Manager Release 5.x および 6.x に適用されます。

- 管理者は、Cisco Unified Communications オペレーティング システムの管理ページのローカル管理権限を保持している必要があります。
- Cisco Security Agent は、Cisco Unified Communications Manager プラットフォームの初回インストール時に自動的にインストールされます。

インストールを始める前に

Cisco Security Agent for Cisco Unified Communications Manager をインストールする前に、次の情報を確認してください。

- Cisco Unified Communications Manager Release 5.x および Release 6.x では、Cisco Security Agent は自動的にインストールされます。
- Cisco Security Agent は、Cisco Media Convergence Server（MCS）およびシスコが承認したカスタマー向けのサーバをサポートします。これらの MCS やカスタマー向けのサーバには、Cisco Unified Communications Manager およびシスコが提供するオペレーティング システムをインストールする必要があります。ただし、『*Cisco Unified Communications Manager Compatibility Matrix*』に別途指示がある場合は、それに従います。『*Cisco Unified Communications Manager Compatibility Matrix*』を入手するには、表 1 を参照してください。
- このセキュリティ エージェントは、Cisco Unified Communications Manager および Cisco Customer Response Solutions/Cisco Customer Response Applications を実行している共存サーバも含め、Cisco Unified Communications Manager クラスタ内のすべてのサーバにインストールしてください。
- 最初にエージェントをパブリッシャ データベース サーバにインストールし、そのインストールが正常に完了したことを確認してください。次に、エージェントをすべてのサブスクライバ サーバに 1 台ずつ順次インストールしてください。
- エージェントのインストールは、オペレーティング システムのインストールと Cisco Unified Communications Manager のインストールの間には行わないでください。

（注） 上記の内容は、Release 5.x または 6.x には適用されません。

- Cisco Unified Communications Manager をアップグレードする前に、P.11 の「Release 4.x 対応の Cisco Security Agent サービスの無効化と有効化」およびP.13 の「Release 5.x および 6.x 対応の Cisco Security Agent サービスの無効化と有効化」の手順を実行して Cisco Security Agent サービスを無効にする必要があります。また、Cisco Unified Communications Manager のインストール中は、サービスを有効に戻さないでください。

注意 オペレーティング システム、Cisco Unified Communications Manager、メンテナンス リリース、サービス リリース、サポート パッチ、プラグインなどのソフトウェアをインストール、アンインストール、またはアップグレードする前に、Cisco Security Agent のサービスを無効にする必要があります。

エージェントを無効にするには、P.11 の「Release 4.x 対応の Cisco Security Agent サービスの無効化と有効化」およびP.13 の「Release 5.x および 6.x 対応の Cisco Security Agent サービスの無効化と有効化」の手順を実行する必要があります。インストールまたはアップグレード中は、サービスを有効に戻さないでください。このときサービスを有効に戻すと、インストールまたはアップグレードで問題が発生する可能性があります。

ソフトウェアをインストールまたはアップグレードした後は、Cisco Security Agent サービスを有効に戻す必要があります。

サービスが無効になっていると、エージェントはサーバへの侵入を検知しません。

- エージェントをインストールまたはアップグレードする前に、Cisco Unified Communications Manager のデータをバックアップしてください。この作業の実行方法の詳細については、該当バージョンの Cisco Unified Communications Manager のバックアップに関するドキュメントを参照してください。Cisco Unified Communications Manager のバックアップに関するドキュメント

を入手するには、表 1 を参照してください。

- エージェントをインストールまたはアップグレードする前に、クラスタ内で実行するすべてのアプリケーションをバックアップしてください。詳細については、バックアップに関する該当のドキュメントを参照してください。
- Terminal Services を使用してエージェントをインストールまたはアップグレードしないでください。シスコは Terminal Services をインストールしますが、これは、Cisco Technical Assistance Center が管理タスクや設定タスクをリモートで実行できるようにするためです。また、Integrated Lights Out を使用してエージェントをインストールまたはアップグレードしないでください。

  必要な場合は、Virtual Network Computing（VNC）を使用してエージェントをインストールまたはアップグレードすることができます。VNC のドキュメントを入手するには、表 1 を参照してください。

（注） Cisco Unified Communications Manager Release 5.x および Release 6.x は VNC をサポートしていません。

注意 サーバで Cisco HIDS Agent（Entercept）を実行している場合は、Cisco Security Agent をインストールする前に、Add/Remove Programs からこのソフトウェアをアンインストールする必要があります。Cisco HIDS Agent をアンインストールせずに Cisco Security Agent をインストールすると、TCP スタックが削除されるため、セキュリティに必要なファイアウォール コンポーネントがインストールされません。このことは、Cisco Unified Communications Manager Release 4.x のみに適用されます。

- エージェントのインストールにより、CPU の使用率が一時的に上昇します。コール処理の中断を最小限に抑えるために、エージェントのインストールは、コール処理が最小の時間帯に行うことをお勧めします。エージェントは、ソフトウェアのインストール直後からサーバの保護を開始しますが、サーバをリブートしなければ、エージェントの機能は完全には動作しません。

注意 サーバをリブートすると、コール処理が中断される場合があります。そのため、サーバのリブートは、営業時間の終了後、またはコール処理が最小の時間帯に実行することをお勧めします。

- エージェントをアップグレードするか、サーバにエージェントを再インストールするには、事前にエージェントをアンインストールしてから、ソフトウェアを再インストールする必要があります。

  [Add/Remove Programs]、または **[Start] > [Programs] > [Cisco Systems] > [Cisco Security Agent] > [Uninstall Security Agent]** を使用してエージェントをアンインストールする際に、アンインストールの確認を求めるプロンプトが表示されます。ここで、**[Yes]** をクリックして保護を無効にするには、一定時間内に **[Yes]** をクリックする必要があります。**[No]** を選択するか、保護が無効になるまで待つ場合は、セキュリティ モードが自動的に有効になり、インストールが打ち切られます。

（注） 上記の項目は、Cisco Unified Communications Manager Release 5.x および Release 6.x には適用されません。

注意 Cisco Unified Communications Manager Release 4.x サーバからソフトウェアをアンインストールしたら、すぐにサーバをリブートしてください。サーバをすぐにリブートしないと、Windows 2000 のシステム トレイにはフラグが引き続き表示され、Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）の [Message] タブにはエラーが表示されますが、この状態では、ソフトウェアによる保護は機能しません。

- インストール後に、エージェント設定タスクを実行する必要はありません。ソフトウェアはすぐに正常に作動します。Cisco Unified Communications Manager Release 4.x の場合、セキュリティ ログがエージェント GUI の [Message] タブおよび Microsoft Event Viewer に表示され、security.txt ファイル（< インストールしたドライブ >:\Program Files\Cisco\CSAgent\log）にも記録されます。
- Cisco Unified Communications Manager Backup and Restore Utility は、エージェントが生成したログ ファイルやテキスト ファイルをバックアップしません。

  何らかの理由で Cisco Unified Communications Manager のデータをサーバに復元する場合は、Cisco Unified Communications Manager のデータを復元した後に、エージェントを再インストールする必要があります。

ヒント エージェントのインストールまたはアンインストールに関する問題が発生した場合は、P.20 の「Release 4.x の場合のトラブルシューティング」および P.23 の「Release 5.x および Release 6.x の場合のトラブルシューティング」を参照してください。

Cisco Security Agent for Cisco Unified Communications Manager Release 4.x のインストール

確実にインストールするために、P.5 の「インストールを始める前に」の情報を再確認してください。

（注） Cisco Security Agent ファイルをダウンロードする前に、Cisco Unified Communications Manager の暗号化されたサイトにアクセスする必要があります。ダウンロード アクセスを申し込んでいない場合、http://www.cisco.com/kobayashi/sw-center/telephony/crypto/voice-apps/ にアクセスしてください。**[Apply for Cisco 3DESCryptographic Software under export licensing control]** をクリックします。表示された画面上で、製品のドロップダウン リストから [Communications Manager] をクリックし、**[Submit]** をクリックします。表示されたフォームで適切なチェックボックスをオンにし、**[Submit]** をクリックします。ダウンロード アクセスができるようになるタイミングを示すメッセージが表示されます。

Cisco Security Agent をインストールするには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager サーバから、http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des にある CallManager & Voice Apps Crypto Software Download サイトにアクセスします。

ステップ 2 ファイルのリストから、最新バージョンの Cisco Unified Communications Manager CSA ファイルを選択します。

（注） ファイル名は、*CiscoCM-CSA-n.n.n.nnn-n.n.n-K9.exe* の形式に従っています。*n.n.n.nnn-n.n.n* は、エージェントとポリシーのバージョンを示します。たとえば、CiscoCM-CSA-4.0.1.539-1.1.4-K9.exe というファイル名は、4.0.1.539 がエージェントのバージョンで、1.1.4 がポリシーのバージョンを示します。

エージェントとポリシーの最新バージョンの番号が付いているファイルを選択します。

ステップ 3 ダウンロードしたファイルの保存先を書き留めます。

ステップ 4 ダウンロードしたファイルをダブルクリックして、インストールを開始します。

ステップ 5 [Welcome] ウィンドウが表示されたら、**[Next]** をクリックします。

ステップ 6 **[Yes]** をクリックして使用許諾契約に同意します。

ステップ 7 **[Next]** をクリックすると、デフォルトの保存先（C:\Program Files\Cisco\CSAgent）を受け入れます。

注意 Cisco Unified Communications Manager のポリシー規則はディレクトリ固有であるため、デフォルトのディレクトリを使用する必要があります。

ステップ 8 Network Shim をインストールするには、**[Next]** をクリックします。

注意 エージェントの全機能を利用するには、Network Shim をインストールする必要があります。

ステップ 9 選択したオプションがステータス ウィンドウに表示されます。現在の設定値を受け入れる場合は、**[Next]** をクリックします。

ステップ 10 インストールが完了するまで待ちます。[Cancel] はクリックしないでください。

ステップ 11 サーバをリブートするには、**[Yes]** をクリックします。

注意 サーバのリブートは、必要に応じて、営業時間の終了後に実行してもかまいません。サーバをリブートすると、コール処理が中断される場合があります。エージェントは、ソフトウェアのインストール直後からサーバの保護を開始しますが、サーバをリブートしなければ、エージェントの機能は完全には動作しません。

ステップ 12 **[Finish]** をクリックします。

ヒント インストールが完了すると、Windows 2000 のシステム トレイに赤色のフラグが表示されます。また、ソフトウェアがインストールされたことは、［プログラムの追加と削除］ウィンドウでも確認できます。ソフトウェアのインストールが完了していれば、このウィンドウに Cisco Security Agent が表示されます。

ステップ 13 この手順をクラスタ内の各サーバに対して実行します。

サーバにインストールされているエージェントおよびポリシーのバージョンの確認

Cisco Unified Communications Manager Release 4.1 および 4.2 の場合

サーバにインストールされているエージェントおよびポリシーのバージョンを確認および表示するには、CSA の赤色のフラグ アイコンをダブルクリックして、ステータスを確認します。

Cisco Unified Communications Manager Release 5.0 の場合

CSA エージェントとポリシーのバージョンを確認するには、次の CLI コマンドを入力します。

show packages active csa

この CLI コマンドを使用する以外にも、次の手順を実行して CSA 情報を確認できます。

1. Cisco Unified Communications Manager Real-Time Monitoring Tool（RTMT）のトレース収集ツールを使用して、CSA ログ（csalog および securitylog.txt）を表示し収集します。
2. [Collect Files] オプションを使用して、[Cisco Security Agent in System Logs] を選択します。
3. [Remote Browse] オプションを使用して、ログを表示します。
4. [Collect CSA log files by using the Trace Collection tool] を選択します。
5. [Remote Browse] オプションを使用して CSA ログ ファイルを表示するには、ウィンドウ内に表示された csalog ファイルをダブルクリックします。

Release 4.x 対応の Cisco Security Agent サービスの無効化と有効化

ソフトウェアのインストール、アップグレード、アンインストールなど、サーバの再起動が必要な作業を実行する際には、CSA サービスを無効にしておく必要があります。CSA サービスが無効になっているときに、Cisco Unified Communications Manager サーバのモニタリングを再開するには、事前に CSA サービスを有効に戻してください。

注意 コマンド シェルで「net stop csagent」コマンドを使用したり、CSA アイコン（システム トレイにある赤色のフラグ）を右クリックして表示される一時停止オプションを使用したりして、CSA を一時停止することができます。ただし、実際にこの方法ではエージェントは無効になりません。単に一時停止するだけです。シスコでは、エージェントの一時停止をお勧めしません。また、サポートも行っていません。これは、インストーラがマシンをリブートしたり、インストール処理を続行する場合は、再度アクティブになった CSA サービスが他のソフトウェアのインストールを邪魔する可能性があるためです。

注意 オペレーティング システム、Cisco Unified Communications Manager、メンテナンス リリース、サービス リリース、サポート パッチ、プラグインなどのソフトウェアをインストール、アンインストール、またはアップグレードする前に、この項の手順に従って CSA サービスを無効にする必要があります。インストールまたはアップグレード中は、サービスを有効に戻さないでください。このときサービスを有効に戻すと、インストールまたはアップグレードで問題が発生する可能性があります。

ソフトウェアをインストール、アップグレード、またはアンインストールした後は、Cisco Security Agent サービスを有効に戻す必要があります。

サービスが無効になっていると、エージェントはサーバへの侵入を検知しません。

注意 次の手順を各サーバに対して 1 台ずつ順次実行することをお勧めします。ソフトウェアのインストール、アップグレード、またはアンインストールが完了したら、そのサーバのサービスを有効に戻します。続いて、次のサーバのサービスを無効にして同様にソフトウェアのインストール、アップグレード、またはアンインストールを実行します。

CSA の無効化

Cisco Unified Communications Manager Release 4.1 または 4.2 対応の CSA サービスを無効にするには、次の手順を実行します。

手順

ステップ 1 **[Start] > [Settings] > [Control Panel] > [Administrative Tools] > [Services]** を選択します。

ステップ 2 [Services] ウィンドウで Cisco Security Agent を右クリックし、**[Properties]** を選択します。

ステップ 3 [Properties] ウィンドウで、**[General]** タブをクリックします。

ステップ 4 [Service Status] 領域で **[Stop]** をクリックします。

ステップ 5 [Startup type] ドロップダウン リストボックスから **[Disabled]** を選択します。

ステップ 6 **[OK]** をクリックします。

注意 [Service] ウィンドウで、CSA サービスの [Startup Type] が無効になっていることを確認します。

ステップ 7 [Services] ウィンドウを閉じます。

ステップ 8 この手順を、Cisco Unified Communications Manager をインストールまたはアップグレードする対象の各サーバに対して実行します。

注意 ソフトウェアをインストール、アップグレード、またはアンインストールした後は、Cisco Security Agent サービスを有効に戻す必要があります。P.12 の「CSA の再有効化」を参照してください。

CSA の再有効化

ソフトウェアをインストール、アップグレード、またはアンインストールした後に、Cisco Unified Communications Manager Release 4.x 対応の Cisco Security Agent サービスを有効に戻すには、次の手順を実行します。

手順

ステップ 1 **[Start]** > **[Settings]** > **[Control Panel]** > **[Administrative Tools]** > **[Services]** を選択します。

ステップ 2 [Services] ウィンドウで [Cisco Security Agent] を右クリックし、**[Properties]** を選択します。

ステップ 3 [Properties] ウィンドウで、**[General]** タブをクリックします。

ステップ 4 **[Startup type]** ドロップダウン リストボックスから **[Automatic]** を選択します。

ステップ 5 **[Apply]** をクリックします。

ステップ 6 **[Start]** をクリックします。

ステップ 7 サービスが開始されたら、**[OK]** をクリックします。

ステップ 8 [Services] ウィンドウを閉じます。

Release 5.x および 6.x 対応の Cisco Security Agent サービスの無効化と有効化

ソフトウェアのインストール、アップグレード、アンインストールなど、サーバの再起動が必要な作業を実行する際には、CSA サービスを無効にしておく必要があります。CSA サービスが無効になっているときに、Cisco Unified Communications Manager サーバのモニタリングを再開するには、事前に CSA サービスを有効に戻してください。

（注） Cisco Unified Communications Manager のアップグレード時には、CSA は自動的に、アップグレード前に停止しアップグレード後に再開します。何らかの理由で CSA が自動的に停止および再開しない場合は、手動で CSA を無効にし、さらに有効に戻すことができます。

CSA を手動で停止するには、Cisco Unified Communications オペレーティング システムの管理ページで Command Line Interface（CLI; コマンドライン インターフェイス）を使用します。

CSA を停止するには、次の CLI コマンドを入力します。

utils csa disable

CSA を開始するには、次の CLI コマンドを入力します。

utils csa enable

CSA のステータスを確認するには、次の CLI コマンドを入力します。

utils csa status

（注） 停止するとエージェント　システムのすべての規則が無効となり、再開するとすべての規則が有効に戻ります。

Cisco Security Agent のアンインストール

この項の内容は、Cisco Unified Communications Manager Release 5.x または Release 6.x には適用されません。Release 5.x または 6.x でソフトウェアをアップグレードする方法の詳細については、『*Cisco Unified Communications Operating System アドミニストレーション ガイド*』を参照してください。

P.5 の「インストールを始める前に」で、Cisco Security Agent のアンインストールについての情報を確認します。

注意 すでにインストールされたバージョンに対して、同じバージョンのエージェントをインストールすることはできません。エージェントをアンインストールしてから、ソフトウェアを再インストールする必要があります。エージェントをアンインストールする場合は、アンインストールの確認を求めるプロンプトが表示されます。ここで、[Yes] をクリックして保護を無効にするには、一定時間内に [Yes] をクリックする必要があります。[No] を選択するか、保護が無効になるまで待つ場合は、セキュリティ モードが自動的に有効になります。

Cisco Unified Communications Manager Release 4.x からセキュリティ エージェントをアンインストールするには、次の手順を実行します。

手順

ステップ 1 **[Start] > [Programs] > [Cisco Systems] > [Uninstall Cisco Security Agent]** を選択します。

ステップ 2 すべての質問に対して、**[Yes]** または **[Yes to All]** をクリックします。

ステップ 3 サーバをリブートします。

注意 ソフトウェアをアンインストールしたら、すぐにサーバをリブートしてください。サーバをすぐにリブートしないと、Windows 2000 のシステム トレイにはフラグが引き続き表示され、GUI の [Message] タブにはエラーが表示されますが、この状態では、ソフトウェアによる保護は機能しません。

（注） アンインストーラは、ポリシーのバージョンが格納されているレジストリのエントリを削除しません。削除する場合は、手動で削除する必要があります。

Cisco Security Agent のアップグレード

Cisco Unified Communications Manager Release 4.x の場合

Cisco Unified Communications Manager Release 4.x サーバの Cisco Security Agent をアップグレードする前に、次の作業を実行してください。

1. サーバにインストールされている現在のバージョンをアンインストールします。

   P.14 の「Cisco Security Agent のアンインストール」を参照してください。

2. サーバに新しいバージョンをインストールします。

   P.8 の「Cisco Security Agent for Cisco Unified Communications Manager Release 4.x のインストール」を参照してください。

Cisco Unified Communications Manager Release 5.x または 6.x の場合

Cisco Unified Communications Manager Release 5.x または Release 6.x サーバの Cisco Security Agent をアップグレードする前に、次の作業を実行してください。

1. Cisco Unified Communications オペレーティング システムの管理ページで、[**ソフトウェアアップグレード**] > [**インストール / アップグレード**] を選択することで、CSA エージェントをアップグレードできます。
2. [オプション / アップグレード] ドロップダウン リスト ボックスに、platform-csa-x.xxxx.cop ファイルが表示されます。
3. CSA をアップグレードするには、platform-csa-x.xxxx.cop ファイルを選択し、[**次へ**] ボタンをクリックし、[**アップグレード**] ボタンをクリックします。
4. Cisco Unified Communications Manager をアップグレードすると、適用可能な場合には、最新の COP ファイルが適用されます（アップグレード パッチ内の CSA RPM のバージョンが COP ファイルを使用して適用されるバージョンより古い場合）。
5. サーバを再起動します。

Management Center for Cisco Security Agent への移行

この項の内容は、Cisco Unified Communications Manager Release 5.x または Release 6.x には適用されません。

Cisco Unified Communications Manager に含まれているセキュリティ エージェントは、変更や表示ができない静的ポリシーを使用します。統合管理型のコンソール製品である Management Center for Cisco Security Agent（CSA MC）を購入してインストールすると、ポリシーを追加、変更、削除、または表示できます。ただし、そのような変更されたポリシーは、Cisco CRS では使用できません。

CSA MC は次の 2 つのコンポーネントで構成されています。

- Management Center。このコンポーネントは、セキュアなサーバにインストールされ、Web サーバ、構成データベース、および Web ベースのインターフェイスで構成されています。Management Center によって、規則やポリシーを定義することができます。また、他のネットワーク システムやサーバにインストールされているエージェントに配布するためのエージェント キットを作成することもできます。
- Cisco Security Agent（管理対象エージェント）。このコンポーネントは、クラスタ内のすべての Cisco Unified Communications Manager サーバにインストールされ、セキュリティ ポリシーを運用します。管理対象エージェントは Management Center に登録され、ポリシーや規則のアップデートを受信します。また、Management Center にイベント ログ レポートを送信します。

作業を始める前に、次に示す CSA MC のドキュメントの最新版を入手する必要があります。

- *Management Center for Cisco Security Agents インストレーション ガイド*
- *Management Center for Cisco Security Agents ユーザ ガイド*
- *Release Notes for Management Center for Cisco Security Agents*

これらのドキュメントは、http://www.cisco.com/en/US/customer/products/sw/cscowork/ps5212/ からダウンロードできます。

Cisco Unified Communications Manager 環境では、Management Center コンポーネントは別々のセキュアなサーバにインストールし、管理対象エージェント コンポーネントはクラスタ内のすべての Cisco Unified Communications Manager サーバにインストールする必要があります。Management Center として使用するサーバは、『*Management Center for Cisco Security Agents インストレーション ガイド*』に記載されているシステム要件を満たしていなければなりません。

注意 Management Center は、Cisco Unified Communications Manager がインストールされているサーバにはインストールしないでください。そのようなインストールを実行しようとすると、CSA MC のインストール時に、サーバで実行中の Microsoft SQL Server が検出され、CSA MC のインストールが自動的に打ち切られます。

CSA MC のパッケージとドキュメントを入手したら、次の手順を実行します。

手順

ステップ 1 個別のサーバ（Cisco Unified Communications Manager 以外のサーバ）上に、http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des にある Communications Manager & Voice Apps Crypto Software Download サイトから最新バージョンの Cisco Unified Communications Manager ポリシーの XML ファイルをダウンロードします。

ステップ 2 ダウンロードしたファイルの保存先を書き留めます。

ステップ 3 Cisco Security Agent がすでにインストールされている場合は、「Cisco Security Agent のアンインストール」の項の手順に従って、これをアンインストールします。

ステップ 4 『*Management Center for Cisco Security Agents インストレーション ガイド*』の手順に従って、CSA MC をインストールします。

ステップ 5 ステップ 1 でダウンロードしたポリシー ファイルを、『*Management Center forCisco Security Agents ユーザ ガイド*』の手順に従ってインポートします。

ステップ 6 『*Management Center for Cisco Security Agents インストレーション ガイド*』の手順に従って、CSA MC の構成を完了します。

Cisco Security Agent のテスト

エージェントがインストールされたことを確認したら、ご使用のシステムを攻撃してエージェントをテストすることができます。その場合、『*Management Center for Cisco Security Agents 4.0 インストレーション ガイド*』の付録「Cisco Security Agent の評価」の「システムへの攻撃」の項を参照してください。

メッセージおよびログ

Cisco Unified Communications Manager Release 4.x の場合

Cisco Security Agent では、システム トレイのアイコン（赤色のフラグ）をなびかせて、ユーザにメッセージの到着を知らせます。メッセージを読むには、アイコンをダブルクリックして、次に [Messages] タブをクリックします。

表示されるメッセージは、アクションが拒否されたかまたはクエリーを生成した際に生成されたメッセージです。最後に生成されたメッセージが 2 つだけ表示されます。

<インストールしたドライブ>:\Program Files\Cisco\CSAgent\log にある次のログファイルを検索します。

- securitylog.txt：このイベント ログには規則違反および他の該当するイベントのログが含まれています。
- csalog.txt：このファイルにはエージェントの起動およびシャットダウンの履歴が記録されています。
- driver_install.log : このログ ファイルには、ドライバのインストール プロセスが記録されています。
- Cisco Security AgentInstallInfo.txt : このファイルにはインストール プロセスの詳細な記録があります。

Notepad を使用して securitylog.txt を表示できます。また、次の作業を行うと、ファイルをもっと簡単に読むことができます。

1. Excel または他のスプレッドシートがインストールされているコンピュータにファイルをコピーする。
2. ファイル名を securitylog.csv に変更する。
3. ファイルをダブルクリックして、スプレッドシート アプリケーションで表示する。

フィールド名は、スプレッドシートの最初の行に表示されます。さらに便利な使い方として、セルをクリックしたり、スプレッドシートの表のフィールドの内容を見たりして、スプレッドシートのセルの内容を表示することができます。

問題の診断に最も重要なフィールドには、[DateTime]、[Severity]、[Text]、および [User] が含まれています。[RawEvent] フィールドは無視します。これは、基本的に他のフィールドと同じ内容で、加工されておらず、読み取りの難しい形式になっています。

重大度のレベルは、Information、Notice、Warning、Error、Alert、Critical、Emergency の順に最も軽いものから重いものへとレベルが上がります。

（注） 通常、エントリがログに表示されることはほとんどありません。特別な場合に一時的にエントリが表示されますが、これは注意すべきことが発生したことを示します。普通は、そのイベントを記述しているテキストで、内部の問題（エージェントを無効にしないでソフトウェアをインストールしようとしているなど）によるものか外部の問題（エージェントが検出および防御しているシステムへの攻撃など）によるものかを判定できます。

Cisco Unified Communications Manager Release 5.x および Release 6.x の場合

CSA 情報を表示するには、次の手順を実行します。

1. Cisco Unified Communications Manager Real-Time Monitoring Tool（RTMT）のトレース収集ツールを使用して、CSA ログ（csalog および securitylog.txt）を表示し収集します。
2. [Collect Files] オプションを使用して、[Cisco Security Agent in System Logs] を選択します。
3. [Remote Browse] オプションを使用して、ログを表示します。
4. [Collect CSA log files by using the Trace Collection tool] を選択します。
5. [Remote Browse] オプションを使用して CSA ログ ファイルを表示するには、ウィンドウ内に表示された csalog ファイルをダブルクリックします。

Release 4.x の場合のトラブルシューティング

Cisco Technical Assistance Center（TAC）に問い合せる前に、トラブルシューティングのヒントをこの項で確認します。

エージェントのインストールまたはアンインストールに関する問題

エージェントのインストールまたはアンインストールに関する問題が発生した場合は、次の作業を実行してください。

- サーバをリブートしたことを確認します。
- ソフトウェアのインストールまたはアップグレードに Terminal Services を使用しなかったことを確認します。
- インストールの前に Cisco HIDS Agent（Entercept）をアンインストールしたことを確認します。
- <インストールしたドライブ>:\Program Files\Cisco\CSAgent\log のインストール ログを入手します。Cisco Security AgentInstallInfo.txt ファイルおよび driver_install.log ファイルの内容を検査します。
- インストールの場合、Network Shim がインストールされていることを確認します。driver_install.log には、csanet2k.inf がインストールされたことが記述されていなければなりません。Network Shim がインストールされていない場合は、エージェントをアンインストールしてから再インストールしてください。

Cisco Unified Communications Manager を実行する場合の問題または CSA エラー

Cisco Security Agent for Cisco Unified Communications Manager をインストールした後に次の問題が発生した場合、この項の手順を実行してください。

- 説明できない Cisco Unified Communications Manager の問題
- Windows のイベント ログまたは CSA のログ ファイル（<インストールしたドライブ>:\Program Files\Cisco\CSAgent\log\securitylog.txt）にある CSA のエラー
- 画面に表示される CSA エラー メッセージ

CSA のログ エントリまたはエラー メッセージの原因を特定できない場合、Cisco TAC に問い合せてください。ただし、問い合せる前に、P.22 の「TAC へのお問い合せの前に」を参照してください。

Cisco Unified Communications Manager の問題または Cisco Security Agent のエラーをトラブルシュートするには、次の手順を実行します。

手順

ステップ 1 Windows のタスクバーで、[Cisco Security Agent] アイコン（Windows のシステム トレイにある赤色のフラグ）を右クリックし、**[Suspend security]** をクリックしてください。

ステップ 2 エラー メッセージの原因となった操作を実行します。

ステップ 3 Windows のタスクバーで、[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実行します。

ステップ 5 Cisco Security Agent を一時停止すると操作が正常終了し、Cisco Security Agent を有効にすると失敗する場合、Cisco Unified Communications Manager サーバ上で実行しているソフトウェア アプリケーションすべてが P.3 の「はじめに」に記載された、サポートされているサードパーティのアプリケーションであ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、このソフトウェアを削除してこの手順を繰り返し実行します。

問題を解決できない場合は、P.22 の「TAC へのお問い合せの前に」を参照してください。

ソフトウェアの 2 回目のインストールが警告なしで失敗

Cisco Security Agent では、クエリーに対する応答が 1 時間キャッシュに格納されます。この便利な機能によって、繰り返し行う操作のたびに表示されるポップアップに対して応答する手間が省けますが、このために予期しない結果を招くことがあります。

次の場合では、ソフトウェアをインストールしようとすると警告なしに失敗します。

1. Cisco Security Agent サービスの停止および無効化を先に行わずにソフトウェアをインストールします。Cisco Security Agent では、次のメッセージが表示されます。

   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.

2. **[No]** をクリックします（この操作を行うと、次回インストールを実行したときに問題が発生します。次を参照してください）。
3. Cisco Security Agent サービスを停止し、無効にします。
4. 2 回目のソフトウェアのインストールを行いますが、インストールは開始されません。

これは、上記のステップ 2 で、**[No]** をクリックしたとき、メモリ内に応答内容が格納されたためです。1 時間後にキャッシュの内容が自動的に消去されます。

ソフトウェアをインストールできるように、すぐにキャッシュを消去するには、次の手順を実行します。

手順

ステップ 1 P.12 の「CSA の再有効化」を参照して、サービスを有効に戻します。

ステップ 2 Windows のタスクバーで、Windows のシステム トレイにある [Cisco Security Agent] アイコン（赤色のフラグ）を右クリックします。

ステップ 3 **[Advanced]** タブをクリックします。

ステップ 4 **[Clear]** をクリックします。

ステップ 5 Cisco Security Agent Control Panel を閉じます。

（注） サーバ上でソフトウェアのインストールを再度試みる前に、Cisco Security Agent サービスを無効にします。ソフトウェアをインストールした後に、Cisco Security Agent サービスを有効に戻します。P.11 の「Release 4.x 対応の Cisco Security Agent サービスの無効化と有効化」を参照してください。

TAC へのお問い合せの前に

トラブルシューティングのヒントを参照しても問題を解決できない場合、Cisco TAC に問い合せる前に次の手順に従ってください。

手順

ステップ 1 <インストールしたドライブ >:\Program Files\Cisco\CSAgent\bin で、csainfo.bat. をダブルクリックします。これによって、ハードウェアおよびソフトウェアのデータが収集されます。

ステップ 2 csainfo では、エージェントの停止の確認を求められます。**[Yes]** をクリックします。csainfo.log ファイルが作成されます。

ステップ 3 < インストールしたドライブ >:\Program Files\Cisco\CSAgent\ ディレクトリ（csainfo.log ファイルおよび securitylog.txt ファイルがあります）を ZIP 形式で圧縮します。

ステップ 4 CSA エンジンおよび CSA ポリシーのバージョンを確認します（手順については、P.10 の「サーバにインストールされているエージェントおよびポリシーのバージョンの確認」の項を参照してください）。

ステップ 5 TAC に問い合せます。ステップ 3 で作成した ZIP ファイルとステップ 4 で収集した情報を提供する準備をします。

Release 5.x および Release 6.x の場合のトラブルシューティング

Cisco Technical Assistance Center（TAC）に問い合せる前に、トラブルシューティングのヒントをこの項で確認します。

サポートのタイプ

次の Cisco Unified Communications Manager ポリシー関連の問題が存在しています。

- Cisco Unified Communications Manager Release 5.0/6.0 および承認されたサードパーティ アプリケーションのパフォーマンスが制限されます。
- システムは、攻撃に対して脆弱なままです。

次の CSA アプリケーションの問題が存在しています。

- CSA アプリケーションがクラッシュします。
- システム メモリがリークします。

問題は、Cisco Unified Communications Manager Release 5.0/6.0 または承認されたサードパーティ アプリケーションで発生します。承認されたサードパーティのプログラムの場合は、必ず、デフォルトのインストール パスでインストールしてください。

TAC に問い合せるためのトラブルシューティング情報の収集

シスコシステムズの TAC は、問題を解決するために次の情報の提供を要求します。

- たとえば、オペレーティング システム、サービス パック、ハードウェア構成などのお客様の環境に関連する情報を収集します。
- ログ ファイルを検査します。問題が再現でき理解できる場合、お客様がこれを実行する必要はありません。問題に再現性がなく、ログ ファイルを調べる必要がある場合は、サポート スタッフがログ ファイルを検査します。
- RTMT を使用して CSA エージェントのログ ファイルにアクセスします。ログ ファイル名は、csalog および securitylog.txt です。
- 可能な場合は、メモリ ダンプ ファイルにアクセスします。

CSA が原因ですべてのコール処理がダウンした場合は、CLI コマンド「utils csa disable」を入力して、要求されたデータを収集します。他のケースで使用するエスカレーション プロセスと同じプロセスに従います。問題が判明した場合は、新しいポリシーが生成され、新しい CSA インストールが CCO に掲示されます。

Cisco Security Agent の追加情報の入手

この項は、Cisco Unified Communications Manager Release 5.0 および Release 6.0 には適用されません。

Cisco Security Agent の追加情報を入手するには、次の手順を実行します。

手順

ステップ 1 次のいずれかの作業を実行します。

- Windows 2000 のシステム トレイで、フラグを右クリックし、**[Open Control Panel]** を選択し、ステップ 2 に進みます。
- **[Start] > [Programs] > [Cisco Security Agent] > [Cisco Security Agent]** を選択し、ステップ 2 に進みます。

ステップ 2 ウィンドウの右上隅にある **?** アイコンをクリックします。

Cisco Security Agent のドキュメントが表示されます。

ヒント Cisco Security Agent 4.0 のドキュメントを入手するには、次の URL をクリックしてください。

http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/index.html

Cisco Unified Communications Manager の関連ドキュメントの入手

表 1 に記載されている URL をクリックすると、Cisco Unified Communications Manager の関連ドキュメントにナビゲートできます。

表 1　URL のクイック リファレンス

関連情報およびソフトウェア	URL および追加情報
オペレーティング システムのドキュメントおよび Virtual Network Computing（VNC）のドキュメント	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm **（注）** この情報は、Windows プラットフォーム上で稼動する Cisco Unified Communications Manager に適用されます。
Cisco MCS のデータシート	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
ソフトウェア専用のサーバ（IBM、HP、Compaq）	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
Cisco Unified Communications Manager Compatibility Matrix	お使いのソフトウェア リリースに該当する互換性マトリクスのリンクの検索については、『*Cisco Unified Communications Manager Release Notes*』を参照してください。
Cisco Unified Communications Manager のドキュメント	http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
Cisco Unified Communications Manager のバックアップと復元に関するドキュメント	Cisco Unified Communications Manager Release 4.x の場合： http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm Cisco Unified Communications Manager Release 5.0、5.1、および 6.0 の場合、お使いのリリースに該当する『*Disaster Recovery System アドミニストレーション ガイド*』を検索してください。 **（注）** Release 5.1 の場合は、『*Disaster Recovery System アドミニストレーション ガイド Release 6.0(1)*』を参照してください。
Cisco Unified Communications Manager、SQL Server、オペレーティング システムのサービス リリース、アップグレード、readme に関するドキュメント	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml **（注）** オペレーティング システムおよび SQL Server 2000 のサービス リリースは、ボイス製品オペレーティング システムの Cryptographic Software ページに掲載されています。Cisco Unified Communications Manager ソフトウェア ページからサイトにナビゲートできます。この情報は、Windows プラットフォーム上で稼動する Cisco Unified Communications Manager に適用されます。
Cisco IP テレフォニー アプリケーションに関するドキュメント	http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html
Cisco Emergency Responder	http://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html

技術情報の入手方法、サポートの利用方法、およびセキュリティ ガイドライン

技術情報の入手、サポートの利用、技術情報に関するフィードバックの提供、セキュリティ ガイドライン、推奨するエイリアスおよび一般的なシスコのマニュアルに関する情報は、月刊の『*What's New in Cisco Product Documentation*』を参照してください。ここには、新規および改訂版のシスコの技術マニュアルもすべて記載されています。次の URL からアクセスできます。

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

シスコ製品のセキュリティの概要

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

シスコの暗号化製品に適用される米国の法律の概要については、次の URL で参照できます。
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

何かご不明な点があれば、export@cisco.com まで電子メールを送信してください。

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0612R)

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 © 2007 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せください。

Copyright © 2007, Cisco Systems Inc.

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

OL-12365-01-J