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

Installing Cisco Security Agent for Cisco Unified Communications Manager

OL-18363-01-J

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

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

このマニュアルでは、Cisco Unified Communications Manager（旧称 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と関連情報について説明します。

- リリース 4.x
- リリース 5.x
- リリース 6.x
- リリース 7.x

（注） リリース 5.x 以降では、Cisco Security Agent は自動的にインストールされます。

Cisco Unified Communications Manager が Cisco Customer Response Solutions（CRS）と同じサーバ上にある場合、これらの製品は同じセキュリティ ポリシーを使用するため、このマニュアルまたは『*Installing Cisco Security Agent for Cisco Customer Response Solutions*』のマニュアルを使用してその共存サーバにエージェントをインストールできます。

目次

このマニュアルは、次のトピックで構成されています。

概要

Cisco Security Agent は Cisco Unified Communications Manager クラスタに侵入検知と侵入防止機能を提供します。シスコシステムズは、Cisco Unified Communications Manager 音声クラスタでサーバと共に使用するために、これを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。エージェントは、一連の検証済みのセキュリティ規則（ポリシー）に基づいたプラットフォーム セキュリティを実現します。これは、厳密なレベルでホストの侵入検知と侵入防止を行います。エージェントは、システム リソースにアクセスする前に、特定のシステムの処理を許可または拒否するポリシーを使用し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実行され、全体のシステム パフォーマンスを妨害しません。

（注） Cisco Unified Communications Manager および Cisco CRS ソフトウェア用にだけでなく、Cisco Security Agent for Cisco Unified Communications Manager は、シスコ認定の多くのサードパーティ製アプリケーションもサポートします。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提供します。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 をインストールしている場合、CSA は TCP/IP のセキュリティ チェックも行います。新しいバージョンのエージェントが入手可能になった場合は、新しい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。

シスコが提供するオペレーティング システムの最新のサービス リリースおよびアップグレードと併用す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 システムのサービス リリースおよ

びアップグレードを入手するには、表 1 を参照してください。

場合によっては、DMA を実行する前に 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場合もあります。詳細については、『*Data Migration Assistant User Guide Release 5.1(1)*』以降を参照してください。

スタンドアロンの Cisco Security Agent は、変更できない静的ポリシーを使用します。ただし、Cisco Unified Communications Manager および Cisco Unified Contact Center Express 以外のポリシーを変更する場合は、詳細について「Management Center for Cisco Security Agents の移行」（P.11）を参照してください。

Cisco Unified Communications Manager、Cisco CRS サーバ、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 をインストールするには、このマニュアルのインストール手順に従ってください。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 に含まれるポリシーは、次のアプリケーションを含む、シスコ認定の多くのサードパーティのモニタリング ツールをサポートします。

- 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 リリース 5.x 以降は上記のアプリケーションをサポートしません。

シスコが認定していないサードパーティのソフトウェア ツールを使用する場合は、詳細について「Management Center for Cisco Security Agents の移行」（P.11）を参照してください。

システム要件

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

- Cisco Unified Communications Manager :『*Cisco Unified Communications Manager Software Compatibility Guide* 』には、サポートされている Cisco Unified Communications Manager のリリースが含まれます。『*Cisco Unified Communications Manager Software Compatibility Guide*』を入手するには、表 1 を参照してください。
- Microsoft Windows 2000 Server または Windows Server 2003（英語版）

次の要件は、Cisco Unified Communications Manager リリース 5.x 以降に適用されます。

- 管理者は、Cisco Unified Communications Operating System 管理のためのローカルの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 リリース 5.x 以降では、Cisco Security Agent は自動的にインストールされます。
- 『*Cisco Unified Communications Manager Software Compatibility Guide* 』で特に指示されていない限り、Cisco Security Agent は Cisco Media Convergence Server（MCS）、または Cisco Unified Communications Manager およびシスコが提供したオペレーティング システムがインストールされたカスタマーが提供したシスコ認定サーバをサポートします。『*Cisco Unified Communications Manager Software Compatibility Guide*』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 が実行されている共存サーバを含む、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ます。
- パブリッシャ データベース サーバに最初にエージェントをインストールし、インストールが正常に完了したことを確認してから、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ます。
- 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） 上記の記述は、リリース 5.x 以降には適用されません。

- 各 Cisco Unified Communications Manager をアップグレードする前に、「リリース 4.x の Cisco Security Agent サービスのディセーブル化と再イネーブル化」（P.8）と「リリース 5.x 以降の Cisco Security Agent サービスのディセーブル化と再イネーブル化」（P.10）に示した手順を使用して、Cisco Security Agent サービスをディセーブルにする必要があります。また、Cisco Unified Communications Manager のインストール中に、サービスが再度イネーブルにならないようにしてください。

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、およびプラグ 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も Cisco Security Agent サービスをディセーブルにする必要があります。

エージェントをディセーブルにするには、「リリース 4.x の Cisco Security Agent サービスのディセーブル化と再イネーブル化」（P.8）および「リリース 5.x 以降の Cisco Security Agent サービスのディセーブル化と再イネーブル化」（P.10）で説明されている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にサービスが再度イネーブルにならないようにしてください。イネーブルになると、インストールまたはアップグレードに問題が発生する場合があります。

ソフトウェアのインストールまたはアップグレードの後に、Cisco Security Agent サービスを再度イネーブルにする必要があります。

サービスをディセーブルにすると、エージェントはサーバの侵入検知を行わなくなります。

- 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 データをバック アップしてください。この作業を実行する方法の詳細については、該当するバージョンの Cisco Unified Communications Manager バックアップ マニュアルを参照してください。Cisco Unified Communications Manager バックアップ マニュアルを入手するには、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アプリケーションをすべてバック アップしてください。詳細については、該当するバックアップ マニュアル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。シスコが Terminal Services をインストールするのは、Cisco Technical Assistance Center はリモート管理と設定タスクを実行するためです。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できます。VNC のマニュアルを入手するには、表 1 を参照してください。

（注） Cisco Unified Communications Manager リリース 5.x 以降は、VNC をサポートしません。

注意 サーバ上で現在 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 Security Agent のインストールの前に Cisco HIDS Agent をアンインストールできなかった場合、インストールによって TCP スタックが削除され、Cisco Security Agent は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。これは、Cisco Unified Communications Manager リリース 4.x だけに適用されます。

- エージェントのインストールによって、CPU の使用率に短いスパイクが発生します。コール処理の中断を最低限に抑えるために、コール処理が最小の時間帯にエージェントをインストールすることをお勧めします。エージェントはソフトウェアをインストールすると直ちにサーバを保護しますが、エージェントはサーバをリブートするまで十分な機能性を発揮しません。

注意 サーバのリブートによって、コール処理が中断する場合があります。営業時間の終了後またはコール処理が最小の時間帯にサーバをリブートすることをお勧めします。

- Cisco Unified Communications Manager リリース 4.x の場合、エージェントのアップグレードやサーバへの再インストールを行う前に、エージェントをアン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場合は、エージェントをアンインストールするか尋ねるプロンプトが表示されます。[Yes] をクリックして保護をディセーブルにする時間は限られています。[No] を選択した場合や、保護をディセーブルにするまでに時間がかかると、セキュリティ モードが自動的にイネーブルになり、インストールが中止されます。

注意 Cisco Unified Communications Manager リリース 4.x サーバからソフトウェアをアンインストールした後、サーバを直ちにリブートします。サーバを直ちにリブートしないと、フラグが Windows システム トレイに引き続き表示され、graphical user interface（GUI; グラフィカル ユーザ インターフェイス）の [Message] タブにエラーが表示されますが、ソフトウェアは保護を行いません。

- インストール後、エージェントの設定作業を行う必要はありません。ソフトウェアは直ちに設計どおりの作業を開始します。Cisco Unified Communications Manager リリース 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、Microsoft Event Viewer、securitylog.txt ファイル（<InstallDrive>:¥Program Files¥Cisco¥CSAgent¥log）に表示されます。
- Cisco Unified Communications Manager Backup and Restore Utility は、エージェントが作成するログ 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 データをサーバに復元する必要がある場合は、Cisco Unified Communications Manager データを復元した後で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で問題が発生した場合は、「リリース 4.x のトラブルシューティング」（P.15）および「リリース 5.x 以降のトラブルシューティング」（P.17）を参照してください。

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

インストールを確実に行うため、「インストールを始める前に」（P.4）に記載された情報を再度確認してください。

（注） Cisco Security Agent ファイルをダウンロードする前に、Cisco Unified Communications Manager 暗号化サイトへのアクセス権が必要です。ダウンロード アクセス権を申請していない場合は、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。表示されるウィンドウで製品のドロップダウン リストから [Communications Manager] を選択し、[Submit] をクリックします。フォームが表示されますので、適切なチェックボックスをオンにして、[Submit] をクリックします。ダウンロード アクセス権を取得でき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 の Communications Manager & 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 Cisco Unified Communications Manager CSA ファイルの最新バージョンを選択します。

（注） ファイル名の構造は *CUCM-CSA-n.n.n.nnn-n.n.n-K9.exe* の形式に従います。ここで *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、ファイル名 CUCM-CSA-4.0.1.539-1.1.4-K9.exe はエージェント バージョン 4.0.1.539 とポリシーのバージョン 1.1.4 を示します。

最新のエージェント バージョンと最新のポリシーのバージョンを持つ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場所を記録します。

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

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 ライセンス契約を受け入れるには、[Yes] をクリックします。

ステップ 7 デフォルトの場所（C:¥Program Files¥Cisco¥CSAgent）を受け入れるには、[Next] をクリックします。

注意 Cisco Unified Communications Manager 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 ディレクトリを使用する必要があります。

ステップ 8 ステータス ウィンドウに選択したオプションが表示されます。現在の設定を受け入れるには、[Next] をクリックします。

ステップ 9 インストールが完了するまで待ちます。[Cancel] をクリックしないでください。

ステップ 10 サーバをリブートするには、[Yes] をクリックします。

注意 ここでリブートしない場合は、営業日の終了時にサーバをリブートできます。サーバのリブートによって、コール処理が中断する場合があります。エージェントはソフトウェアをインストールすると直ちにサーバを保護しますが、エージェントはサーバをリブートするまで十分な機能性を発揮しません。

ステップ 11 [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 システム トレイに赤いフラグが表示されます。[Add/Remove Programs] ウィンドウで Cisco Security Agent の場所を特定することによって、インストールされたソフトウェアを確認することもできます。

ステップ 12 クラスタ内のすべてのサーバでこの手順を実行します。

サーバ上のエージェントとポリシーのバージョンの確認

Cisco Unified Communications Manager リリース 4.x の場合

サーバ上のエージェントとポリシーのバージョンを確認し、表示するには、CSA の赤いフラグ アイコンをダブルクリックして [Status] に進みます。

Cisco Unified Communications Manager リリース 5.x 以降の場合

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

show packages active csa

前述の CLI コマンドに加え、次の手順を実行して CSA 情報を表示できます。

1. Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool（RTMT）の Trace & Log Central 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、システム ログの Cisco Security Agent 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. Trace & Log Central ツールを使用して、Collect CSA ログ ファイルを選択します。
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、ウィンドウに表示される **csalog** ファイルをダブルクリックします。

リリース 4.x の Cisco Security Agent サービスのディセーブル化と再イネーブル化

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タスクを実行する場合は、CSA サービスをディセーブルにする必要があります。CSA サービスをディセーブルにした場合は、Cisco Unified Communications Manager サーバのモニタリングを再開する前にサービスを再度イネーブルにする必要があります。

注意 コマンド シェルの「net stop csagent」コマンド、または CSA アイコン（システム トレイの赤いフラグ）を右クリックして選択できる一時停止オプションを使用して、CSA を一時停止できます。ただし、これらの方法は実際にエージェントをディセーブルにしません。一時停止にするだけです。エージェントの一時停止はお勧めしません。また、サポートも行いません。これは、インストーラがマシンをリブートし、インストール動作を続行する場合に、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に干渉する場合があるためです。

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、およびプラグ 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も、この方法を使用して CSA サービスをディセーブル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にサービスが再度イネーブルにならないようにしてください。イネーブルになると、インストールまたはアップグレードに問題が発生する場合があります。

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の後に、Cisco Security Agent サービスを再度イネーブルにする必要があります。

サービスをディセーブルにすると、エージェントはサーバの侵入検知を行わなくなります。

注意 次の手順をサーバに 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の完了後に、サーバ上のサービスを再度イネーブルにしてから、同じソフトウェア動作を実行する次のサーバでサービスをディセーブルにできます。

CSA のディセーブル化

Cisco Unified Communications Manager リリース 4.x の CSA サービスをディセーブルにするには、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] を右クリックして [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] エリアで [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 [Services] ウィンドウで CSA サービスの [Startup Type] がディセーブル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 Cisco Unified Communications Manager をインストールまたはアップグレードするすべてのサーバでこの手順を実行します。

注意 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後に Cisco Security Agent サービスを再度イネーブルにする必要があります。「CSA の再イネーブル化」（P.9）を参照してください。

CSA の再イネーブル化

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後に Cisco Unified Communications Manager リリース 4.x の Cisco Security Agent サービスを再度イネーブルにするには、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] を右クリックして [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 サービスの開始後に、[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。

リリース 5.x 以降の Cisco Security Agent サービスのディセーブル化と再イネーブル化

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タスクを実行する場合は、CSA サービスをディセーブルにする必要があります。CSA サービスをディセーブルにした場合は、Cisco Unified Communications Manager サーバのモニタリングを再開する前にサービスを再度イネーブルにする必要があります。

（注） Cisco Unified Communications Manager のアップグレード中、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起動します。何らかの理由によって CSA が自動的に停止および起動しない場合は、CSA を手動でディセーブルおよびイネーブルにできます。

CSA を手動で停止するには、Cisco Unified Communications Operating System 管理で入手できる 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 を起動するには、次の CLI コマンドを入力します。

utils csa enable

CSA のステータスをチェックするには、次の CLI コマンドを入力します。

utils csa status

（注） 停止 / 開始はエージェント システム上のすべての規則をディセーブル / 再イネーブルにします。

Cisco Security Agent のアンインストール

次のセクションは Cisco Unified Communications Manager リリース 5.x 以降には適用されません。リリース 5.x 以降でのソフトウェアのアップグレードについては、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

「インストールを始める前に」（P.4） 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 以前にインストールしたバージョンの上に同じバージョンのエージェントはインストールできません。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、エージェントをアンインストールするか尋ねるプロンプトが表示されます。[Yes] をクリックして保護をディセーブルにする時間は限られています。[No] を選択したり、保護をディセーブルにするまで時間がかかると、セキュリティ モードが自動的にイネーブルになります。

Cisco Unified Communications Manager リリース 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 すべての質問の回答に [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後、サーバを直ちにリブートします。サーバを直ちにリブートしないと、フラグが Windows システム トレイに引き続き表示され、グラフィカル ユーザ インターフェイス（GUI）の [Message] タブにエラーが表示されますが、ソフトウェアは保護を行いません。

（注） アンインストーラはポリシーのバージョンが保存されたレジストリ エントリは削除しません。これらを削除する場合は、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 リリース 4.x の場合

Cisco Unified Communications Manager リリース 4.x サーバ上で Cisco Security Agent をアップグレードする前に、次のタスクを実行します。

1. サーバにインストールされた既存のバージョンをアンインストールします。

   「Cisco Security Agent のアンインストール」（P.10）を参照してください。

2. サーバで実行する予定の新しいバージョンをインストールします。

   「Cisco Security Agent for Cisco Unified Communications Manager リリース 4.x のインストール」（P.6）を参照してください。

Cisco Unified Communications Manager リリース 5.1(3) 以降の場合

シスコは Cisco Unified Communications Manager リリースで CSA アップグレードを提供します。常に最新の CSA ソフトウェアを実行するために、クラスタ内のすべてのサーバに最新の Cisco Unified CallManager サービス リリースをインストールすることを強くお勧めします。
http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des で最新のダウンロードを入手できます。

Management Center for Cisco Security Agents の移行

このセクションは Cisco Unified Communications Manager リリース 5.x 以降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、変更または表示できない静的ポリシーを使用します。完全に管理されたコンソール製品である Management Center for Cisco Security Agent（CSA MC）を購入および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、このように変更したポリシーは Cisco CRS では使用できないことに注意してください。

CSA MC には 2 つのコンポーネントが含まれています。

- Management Center は、セキュアなサーバにインストールされ、Web サーバ、設定データベース、Web ベースのインターフェイスで構成されています。Management Center では、規則とポリシーを定義し、エージェント キットを作成できます。これらは、他のネットワーク システムとサーバにインストールされるエージェントに配布されます。
- Cisco Security Agent（管理対象エージェント）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 ポリシーを強制的に適用します。管理対象エージェントは Management Center に登録され、ポリシーと規則の更新を受信できます。また、イベント ログ レポートの Management Center への返信も行います。

開始前に、次の CSA MC マニュアルの最新バージョンを入手する必要があります。

- 『*Installing Management Center for Cisco Security Agents*』
- 『*Using Management Center for Cisco Security Agents*』
- 『*Release Notes for Management Center for Cisco Security Agents*』

これらのマニュアルは、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 Management Center コンポーネントが個別のセキュアなサーバにインストールされ、管理対象エージェントのコンポーネントが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ていることを確認します。Management Center 用のサーバが『*Installing Management Center for Cisco Security Agents*』にリストされているシステム要件を満たしていることを確認します。

注意 Cisco Unified Communications Manager をインストールしたサーバに Management Center をインストールしないでください。こ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上で実行中の Microsoft SQL Server が検出され、管理対象のコンソールのインストールは自動的に中止されます。

ACSA MC パッケージとマニュアルを入手した後、次の手順を実行します。

手順

ステップ 1 個別の（Cisco Unified Communications Manager 以外の）サーバで最新バージョンの Cisco Unified Communications Manager .export ファイルを http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des の Communications Manager & Voice Apps Crypto Software Download サイトから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場所を記録します。

ステップ 3 Cisco Security Agent が存在する場合は、「Cisco Security Agent のアンインストール」セクションの手順に従ってアンインストールします。

ステップ 4 CSA MC のインストールについては、『*Installing Management Center for Cisco Security Agents* 』の手順に従います。

ステップ 5 ステップ 1 でダウンロードしたポリシー ファイルのインポートについては、『*Using Management Center for Cisco Security Agents*』の手順に従います。

ステップ 6 CSA MC の設定の完了については、『*Installing Management Center for Cisco Security Agents*』の手順に従います。

memRegRepair ユーティリティの実行についての注意事項

このセクションでは、MCS-7845-XX の memRegRepair ユーティリティ（CiscoCM-CSA-memRegRepair-k9.exe）を実行する方法について説明します。管理対象エージェントまたはスタンドアロン エージェント 3.0(6) 以前を実行している場合は、memRegRepair ユーティリティを実行します。一般的に、CSA の Management Center によってエージェント キットが生成されるすべての CSA インストールの後で、ユーティリティを実行する必要があります。

次のことに注意してください。

- MCS-OS 2003 を実行している Cisco 7845 シリーズ サーバの新規インストール時に、Cisco Security Agent がインストールされてから、サーバをリブートする前に、memRegRepair ユーティリティを実行してください。
- MCS-OS 2003 SR を実行している Cisco 7845 シリーズ サーバでは以下に従ってください。
  - Cisco Security Agent があらかじめインストールされている場合、ユーティリティを実行する必要はありません。
  - プラットフォームのアップグレード後に Cisco Security Agent がインストールされた場合は、ユーティリティを実行する必要があります。
- MCS-OS 2003 を実行している Cisco 7845 シリーズ サーバで、何らかの理由によって Cisco Security Agent がアンインストールされ、再インストールされた場合は、ユーティリティを実行する必要があります。

memRegRepair ユーティリティは次の URL で入手できる場合があります。

http://tools.cisco.com/support/downloads/go/ImageList.x?relVer=3.0(6)&mdfid=280771554&sftType=Security+Agent+System+Software+for+Unified+Communications+Manager%2FCallManager&optPlat=&nodecount=7&edesignator=null&modelName=Cisco+Unified+Communications+Manager+Version+4.3&treeMdfId=278875240&modifmdfid=null&imname=&treeName=Voice+and+Unified+Communications&hybrid=Y&imst=N

Cisco Security Agent のテスト

Agent がインストールされたことを確認してから、システムを攻撃することによって Agent をテストできます。この場合は、『Installing Management Center for Cisco Security Agents 4.0』の付録「Evaluating the Cisco Security Agent」の「Attack your system」セクションを参照してください。http://www.cisco.com/en/US/partner/docs/security/csa/csa52/install_guide/AppexB.html からアクセスできます。

メッセージとログ

Cisco Unified Communications Manager リリース 4.x の場合

Cisco Security Agent にメッセージがある場合は、システム トレイ内のアイコン（赤いフラグ）がなびきます。メッセージを読むには、アイコンをダブルクリックしてから [Messages] タブをクリックします。

表示されるメッセージは、処理が拒否されるか、照会を生成した際に生成されたメッセージです。最新の 2 つのメッセージだけが表示されます。

<InstallDrive>:¥Program Files¥Cisco¥CSAgent¥log でログ ファイルを見つけます。

- securitylog.txt：このメイン イベント ログには規則違反やその他の関連イベントのログが含まれます。
- csalog.txt：このファイルは、Agent の起動とシャットダウンの履歴を記録します。
- driver_install.log：このログ ファイルはドライバのインストール プロセスを記録します。
- Cisco Security AgentInstallInfo.txt：このファイルはインストール プロセスの詳細な記録を示します。

securitylog.txt ファイルは Notepad を使用して表示できます。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 またはその他のスプレッドシートがインストールされたコンピュータにファイルをコピーします。
2. ファイル名を securitylog.csv に変更します。
3. 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します。

スプレッドシートの最初の行にフィールド名が表示されます。セルをクリックしてスプレッドシート マトリクスの上のフィールドの内容を表示し、スプレッドシートのセルの内容を確認すると、さらに便利です。

診断の問題の場合、最も重要なフィールドには [DateTime]、[Severity]、[Text]、および [User] が含まれます。[RawEvent] フィールドは無視します。ここには基本的に他のフィールドと同じ情報が含まれていますが、処理されていないため読み取りが難しい形式になっています。

重大度は、低い方から高い方へ順に [Information]、[Notice]、[Warning]、[Error]、[Alert]、[Critical]、[Emergency] となります。

（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。ある特定の場合に立て続けにエントリが表示されると、注意事項が発生したことを示しています。通常は、内部的な問題（誰かが Agent をディセーブルにせずにソフトウェアをインストールしようとしているなど）によるものであるか、外部的な問題（エージェントが検出し、防御しているシステムに対する攻撃など）によるものであるかは、イベントを説明するテキストから判断できます。

Cisco Unified Communications Manager リリース 5.x 以降の場合

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 Cisco Unified Real-Time Monitoring Tool（RTMT）の Trace & Log Central 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、システム ログの Cisco Security Agent 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. Trace & Log Central ツールを使用して、Collect CSA ログ ファイルを選択します。
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、ウィンドウに表示される **csalog** ファイルをダブルクリックします。

ヒント トレース収集の詳細については、『*Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide*』を参照してください。

リリース 4.x のトラブルシューティング

Cisco Technical Assistance Center（TAC）に問い合わせる前に、このセクションのトラブルシューティングのヒントを参照してください。

エージェントのインストールまたはアンインストールの問題

エージェントのインストールまたはアンインストールで問題が発生した場合は、次のタスク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/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。
- <InstallDrive>:¥Program Files¥Cisco¥CSAgent¥log からインストール ログを入手します。Cisco Security AgentInstallInfo.txt と driver_install.log ファイルを調べます。
- インストールについて、Network Shim をインストールしたことを確認します。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エージェントを再インストールします。

Cisco Unified Communications Manager の実行に関する問題または CSA エラー

Cisco Security Agent for Cisco Unified Communications Manager のインストール後に次の問題が発生した場合は、このセクション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 イベント ログまたは CSA ログ ファイル（<InstallDrive>:¥Program Files¥Cisco¥CSAgent¥log¥securitylog.txt）の CSA エラー
- CSA エラー メッセージが表示される

CSA 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は、Cisco TAC にお問い合わせください。ただし、問い合わせの前に 「TAC に問い合わせる前に」（P.17）を参照してください。

Cisco Unified Communications Manager の問題や Cisco Security Agent からのエラーのトラブルシューティングを行うには、次の手順を実行します。

手順

ステップ 1 Cisco Security Agent をディセーブルにします。「CSA のディセーブル化」（P.9）を参照してください。

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 を一時停止すると動作が正常に完了し、Cisco Security Agent をイネーブルにすると失敗することが続く場合は、Cisco Unified Communications Manager サーバで実行されているすべてのソフトウェア アプリケーションが 「概要」（P.2）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。

サーバにサポートされていないソフトウェアが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。

問題が解決できない場合は、「TAC に問い合わせる前に」（P.17）を参照してください。

ソフトウェアの 2 度目のインストールが警告なしで失敗

Cisco Security Agent は照会への応答を 1 時間キャッシュします。この便利な機能によって、処理を繰り返すたびにポップアップに応答する必要がなくなります。ただし、特定の状況では、この機能によって望ましくない結果が生じることがあります。

次の場合では、警告なしでソフトウェアのインストールに失敗します。

1. 最初に Cisco Security Agent サービスを停止して、ディセーブルせずにソフトウェアをインストールしようとします。Cisco Security Agent は次のメッセージを表示します。

   「*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（この処理によって、次回インストールを実行するときに問題が発生します。以下を参照してください）。
3. Cisco Security Agent サービスを停止してディセーブルにします。
4. ソフトウェアをもう 1 度インストールしようとしますが、何も起こりません。

上記の手順 2 で [No] をクリックすると、システムがメモリに回答をキャッシュします。システムは 1 時間後に自動的にキャッシュをクリアします。

ソフトウェアをすぐにインストールできるように、すぐにキャッシュをクリアするには、次の手順を実行します。

手順

ステップ 1 セクション「CSA の再イネーブル化」（P.9）での説明に従ってサービスを再度イネーブルにします。

ステップ 2 Windows のタスクバーで、Windows システム トレイ内の Cisco Security Agent アイコン（赤いフラグ）をダブルクリックします。

ステップ 3 [User Query Response] 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 コントロール パネルを閉じます。

（注） サーバへのソフトウェアのインストールを再試行する前に、Cisco Security Agent サービスをディセーブルにします。ソフトウェアをインストールした後、Cisco Security Agent サービスを再度イネーブルにします。「リリース 4.x の Cisco Security Agent サービスのディセーブル化と再イネーブル化」（P.8）を参照してください。

TAC に問い合わせる前に

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

手順

ステップ 1 <InstallDrive>:¥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、有効なハードウェアとソフトウェアのデータが収集できます。

ステップ 2 csainfo は Agent を停止するかどうかの確認を求めます。[Yes] をクリックします。ファイル csainfo.log が作成されます。

ステップ 3 <InstallDrive>:¥Program Files¥Cisco¥CSAgent¥ ディレクトリを圧縮します（これには csainfo.log と securitylog.txt が含まれます）。

ステップ 4 CSA エンジンと CSA ポリシーのバージョンを特定します（この作業の方法については、セクション「サーバ上のエージェントとポリシーのバージョンの確認」（P.7）を参照してください）。

ステップ 5 TAC に問い合わせます。手順 3 で作成した zip ファイルと手順 4 で収集した情報を提供する準備を行います。

リリース 5.x 以降のトラブルシューティング

Cisco Technical Assistance Center（TAC）に問い合わせる前に、このセクションのトラブルシューティングのヒントを参照してください。

サポートのタイプ

次のような Cisco Unified Communications Manager ポリシーに関連した問題が存在します。

- Cisco Unified Communications Manager リリース 5.x 以降のパフォーマンスと認定されたサードパーティのアプリケーションが制限されます。
- 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ます。

- CSA アプリケーションのクラッシュ
- システム メモリのリーク

問題は、Cisco Unified Communications Manager リリース 5.x 以降または認定されたサードパーティのアプリケーションで発生することを確認してください。これらの認定されたプログラムについては、必ずデフォルトのインストール パスにインストールされる必要があります。

TAC 用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、問題の解決に次の情報を必要とします。

- たとえば、オペレーティング システム、サービス パック、ハードウェア設定など、お客様の環境について関連する情報を収集します。

- ログ ファイルを調べます。問題が再現できて、わかっている場合は、この作業を行う必要はありません。問題が再現できず、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 ファイルを調べます。
- RTMT を使用して CSA Agent のログ ファイルにアクセスします。ログ ファイル名は csalog と securitylog.txt です。

（注） CLI コマンド **utils create report csa** でログ ファイルにアクセスすることもできます。CLI セッションの開始と CLI コマンドの使用の詳細については、『Cisco Unified Communications Operating System Administration Guide』を参照してください。

- 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 によってコール処理がダウンしている場合は、CLI コマンド **utils csa disable** を入力して CSA Agent を停止し、必要なデータを収集します。他の場合に使用するのと同じエスカレーション プロセスに従います。問題が正当なものであると判明した場合は、新しいポリシーが生成され、新しい CSA インストールが CCO に公開されます。

Cisco Security Agent についての追加情報の入手

次のセクションは Cisco Unified Communications Manager リリース 5.x 以降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 次のいずれかのタスクを実行します。

- Windows システム トレイでフラグを右クリックし、[Open Control Panel] を選択して、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 ウィンドウの右上にある **?** アイコンをクリックします。

Cisco Security Agent マニュアルが表示されます。

ヒント Cisco Security Agent マニュアルを入手するには、次の URL をクリックします。

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

Cisco Unified Communications Manager の関連マニュアルの入手方法

表 1 の URL をクリックして、Cisco Unified Communications Manager の関連マニュアルにアクセスします。

表 1　URL のクリック リファレンス

関連情報とソフトウェア	URL と追加情報
オペレーティング システムのマニュアルと Virtual Network Computing（VNC）のマニュアル	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実行する Cisco Unified Communications Manager に適用されます。
Cisco MCS 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 Software Compatibility Guide	お使いのソフトウェア リリースの該当する互換性マトリクス リンクについては、『Cisco Unified Communications Manager Release Notes』を参照してください。
Cisco Unified Communications Manager のマニュアル	http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
Cisco Unified Communications Manager のバックアップおよび復元マニュアル	Cisco Unified Communications Manager リリース 4.x の場合 http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm Cisco Unified Communications Manager リリース 5.x 以降の場合（お使いのリリースの『*Disaster Recovery System Administration Guide*』を参照してください）。 http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html **（注）** リリース 5.1 には、『*Disaster Recovery System Administration Guide* Release 6.0(1)』を使用してください。
Cisco Unified Communications Manager、SQL サーバ、オペレーティング システム サービス リリース、アップグレード、readme マニュアル	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml **（注）** 音声製品のオペレーティング システム暗号化ソフトウェア ページ上にポストされたオペレーティング システムおよび SQL サーバ 2000 サービス リリース Cisco Unified Communications Manager ソフトウェア ページからサイトに移動できます。この情報は、Windows プラットフォーム上で実行する Cisco Unified Communications Manager に適用されます。
関連する Cisco IP テレフォニー アプリケーション マニュアル	http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
Cisco Emergency Responder	http://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

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

シスコ製品のセキュリティ

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を管理す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

さらに詳しい情報が必要な場合は、export@cisco.com 宛てに電子メールでお問い合わせください。
