

Cisco Security Agent for IP Communications

Q. スタンドアロンの Cisco® Security Agent は、MS Blaster などのインターネット ワームに対して有効ですか。

A. はい。Cisco Security Agent は、MS Blaster ワームおよびその他の類似のワームが定着および伝播するのを防止します。また、これらのワームによって開始されることの多い DoS 攻撃も阻止します。

Q. Cisco Security Agent は、ワーム、ウイルス、および DoS 攻撃に対する最適な防御策ですか。

A. 最適な防御策となるのは、システムレベルの包括的なセキュリティ アプローチです。自己防衛型ネットワークは、社内外のさまざまな脅威の検出と防御を行い、それらの脅威に適応することによって企業のビジネス プロセスを保護するシスコの長期的な戦略です。自己防衛型ネットワークを利用すると、企業は自社のネットワーク リソースでインテリジェントな機能を活用できるようになり、ビジネス プロセスの改善とコストの削減が可能になります。シスコの自己防衛型ネットワークの詳細については、[ここをクリック](#)してください。

Q. Cisco IP Communications アプリケーション サーバで Management Center for Cisco Security Agents を稼働できますか。

A. いいえ。Management Center は、『[Installing Management Center for Cisco Security Agents](#)』に記載されているシステム要件を満たす、個別のセキュアなサーバにインストールする必要があります。

Q. スタンドアロンの Cisco Security Agents for Unified Communications を作成する際に、Cisco Security Agent のどの標準ポリシーが適用されましたか。

A. Cisco Unified CallManager、Cisco Emergency Responder、Cisco Conference Connection、Cisco Unified IP Interactive Voice Response (Cisco Unified IP IVR)、Cisco IP Queue Manager、および Cisco Unified Contact Center Express のスタンドアロン エージェントについては、次の Cisco Security Agent ポリシーが適用されました。

- 汎用サーバ
- 汎用デスクトップ
- Microsoft Internet Information Services (IIS) バージョン 4.0 および 5.0
- Apache v1.3
- Microsoft SQL Server
- Microsoft Exchange
- Sendmail
- Domain Name System (DNS; ドメイン ネーム システム)
- Dynamic Host Configuration Protocol (DHCP) サーバ
- ネットワーク タイム サーバ
- ドメイン コントローラ
- 分散型ファイアウォール
- ブラウザ保護

- インスタント メッセージャー コントロール
- Microsoft Office 保護
- データ盗難防止
- Cisco Security Agent Manager 保護
- CiscoWorks VPN/Security Management Solution (VMS)
- Cisco Unified CallManager 保護

Cisco Unity[®]、Cisco Unity Bridge、および Cisco Personal Assistant スタンドアロン エージェントについては、次の Cisco Security Agent ポリシーが適用されました。

- Required Windows System Module
- Common Security Module
- Common Web Server Security Module
- Restrictive MS IIS Module
- Restrictive SQL Server Module (Cisco Unity エージェントのみ)
- Server Module
- User Authentication Auditing Module
- Virus Scanner Module

Cisco Unified Intelligent Contact Manager (Enterprise および Hosted) および Cisco Unified Contact Center Enterprise スタンドアロン エージェントについては、次の Cisco Security Agent ポリシーが適用されました。

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

Cisco Internet Service Node (ISN) スタンドアロン エージェントについては、次の Cisco Security Agent ポリシーが適用されました。

- Required Windows System Module
- Common Security Module
- Common Web Server Security Module
- Restrictive Microsoft IIS Module
- Restrictive SQL Server Module
- Virus Scanner Module

Q. カスタマイズ可能なポリシー制御と中央集中型のイベント レポートを利用するには、スタンドアロンの Cisco Security Agent から標準の Cisco Security Agent 製品へのアップグレードをどのように行えばよいですか。

A. アップグレードを行う場合は、製品番号 : CSA-IPT-UPGRADE-K9 を発注してください。Cisco Security Agent は各テレフォニー サーバに特別なポリシーを提供しているため、完全に管理されたソリューションを比較的容易に導入できます。

Q. Cisco Security Agent ヘッドレス エージェントを稼働する Cisco Unified Communications サーバにロードできるその他のソフトウェアには、どのようなものがありますか。

A. Cisco Security Agent ポリシーは、シスコが承認した複数のサードパーティ製モニタリング ツールおよび共存アプリケーションをサポートしています。各製品でサポートされるアプリケーションおよびバージョンを確認するには、その製品用にダウンロードしたスタンドアロン Cisco Security Agent に付属するリリース ノートおよびインストール ガイドを参照してください。

Q. どのようなユーザが Cisco Security Agent ソフトウェアのインストールを必要としていますか。

A. お客様がご利用中の Cisco Unified Communications 製品で次のアプリケーションを実行している場合、Cisco Security Agent をサーバにインストールする必要があります。

- Cisco Unified CallManager 3.2(3)、3.3 およびそれ以降のバージョン
- Cisco Emergency Responder 1.1(4) および 1.2(1)
- Cisco Conference Connection 1.2(2)
- Cisco Unified Intelligent Contact Management(Enterprise および Hosted)、Cisco Unified Contact Center(Enterprise および Hosted) 5.0(0)(SR8 以降)
- Cisco Unified Intelligent Contact Management および Unified Contact Center Enterprise 6.0(0) 以降のバージョン
- Cisco Internet Service Node 2.0 および 2.1
- Cisco Unified Contact Center Express 2.2(5)、3.0(3a)、3.1(3)、3.5(2) およびそれ以降のバージョン
- Cisco Unified IP IVR 2.2(5)、3.0(3a)、3.1(3)、3.5(2) およびそれ以降のバージョン
- Cisco IP Queue Manager 2.2(5)、3.0(3a)、3.1(3)、3.5(2) およびそれ以降のバージョン
- Cisco Unity 4.0 以降のバージョン
- Cisco Unity Bridge 3.0 以降のバージョン
- Cisco Personal Assistant 1.4(1) 以降のバージョン

Q. ソフトウェアの入手方法を教えてください。

A. Management Center for Cisco Security Agents で使用するスタンドアロン エージェントとセキュリティポリシーは、Cisco.com から無料でダウンロードできます。

Cisco Unified CallManager、Cisco Conference Connection、Cisco Emergency Responder、Cisco Unified IP IVR、Cisco IP Queue Manager、および Cisco Unified Contact Center については、次の URL からソフトウェアを入手できます。

<http://www.cisco.com/pcgi-bin/tablebuild.pl/cmva-3des>

Cisco Unity については、次の URL からソフトウェアを入手できます。

<http://www.cisco.com/pcgi-bin/tablebuild.pl/unity3d>

Cisco Unity Bridge については、次の URL からソフトウェアを入手できます。

<http://www.cisco.com/pcgi-bin/tablebuild.pl/bridg3d>

Cisco Personal Assistant については、次の URL からソフトウェアを入手できます。

<http://www.cisco.com/pcgi-bin/tablebuild.pl/PA3des>

Cisco Internet Service Node については、次の URL からソフトウェアを入手できます。

<http://www.cisco.com/pcgi-bin/tablebuild.pl/csa11-crypto>

Cisco Unified Intelligent Contact Management および Cisco Unified Contact Center Enterprise については、次の URL からソフトウェアを入手できます。

<http://www.cisco.com/pcgi-bin/tablebuild.pl/csa10-crypto>

©2007 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)
この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

〒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>

0120-092-255 (通話料無料)

電話受付時間：平日10:00～12:00、13:00～17:00

お問い合わせ先