

Cisco Security Agent バージョン 5.2

製品概要

Cisco® Security Agent セキュリティ ソフトウェアは、サーバおよびデスクトップ コンピューティング システムをセキュリティ上の脅威から保護します。Cisco Security Agent は、従来のエンドポイント セキュリティ ソリューションにない高度な機能として、標的型攻撃、スパイウェア、ルートキット、および Day Zero 攻撃といった脅威に対する先進の保護機能を提供します。Cisco Security Agent の予防的な防御機能を利用すると、公開されて間もない脆弱性を悪用した未知や新種の脅威と改良型の脅威にも対応できます。Cisco Security Agent を利用すると、サービスを停止してオペレーティング システムやアプリケーションの脆弱性パッチを適用することができない重要なサーバの場合でも、アップデートを行うことなくシステムの整合性を保護することができます。したがって、脆弱性が公開されるたびに急いでパッチを適用する必要がなくなるため、パッチの適用に伴うダウンタイムと IT 運用コストを最小限に抑えることができます。企業は脅威が発生してから急いでパッチを適用するのではなく、予定したスケジュールに沿ってパッチを適用することができるようになります。

強力なポリシー準拠管理機能では、機密性の高いデータ ファイルや重要なサーバを保護できます。重要なファイル、アプリケーション、およびサーバへのアクセスをモニタリングまたは制御して、故意または不正によるデータ損失を防ぐことができます。また、リムーバブル メディアの利用を制限することで、リスクを軽減し職務規則の徹底を図ることができます。必要に応じてきめ細かな管理を実施して、ユーザ、アプリケーション、システム、ロケーション、およびネットワーク アドレスに関するポリシーへの準拠を管理することができます。

Cisco Security Agent を利用すると、単独のエンドポイント セキュリティ ソリューションでは実現できない優れた保護が可能になります。Cisco Security Agent は、ネットワーク セキュリティ デバイスと連携して、ネットワーク全体のセキュリティを向上させます。Cisco VPN デバイスは、Cisco Security Agent のパーソナル ファイアウォールおよびホスト侵入防御 (HIPS) 機能を利用して、IPSec (IP Security) および SSL (Secure Sockets Layer) VPN リモートアクセス ユーザに対して優れたエンドポイント セキュリティを提供できます。Cisco Security Agent が収集するホスト情報をシスコのネットワーク IPS デバイスと共有すると、ネットワーク内で実行する IPS 処理の精度を向上させることができます。また、Cisco ASA および Cisco PIX® セキュリティ アプライアンスのファイアウォールおよびアプリケーション検査機能と Cisco Security Agent を組み合わせて使用すると、Cisco Security Agent のトラフィック マーキングに基づいて特定のアプリケーションを検査することができます。

ネットワーク統合機能

表 1 に、Cisco Security Agent のネットワーク統合機能を示します。

表 1 ネットワーク統合機能

機能	説明
ワイヤレス ポリシー制御	Cisco Security Agent のワイヤレス ポリシー制御では、総合的なセキュリティの強化と、ワイヤレス構成の帯域幅の最適化が可能。ポリシーを利用すると、ワイヤレス接続を特定の条件に制限できる(たとえば、ユーザがオフィスの外にいる場合は、ワイヤレス トラフィックに VPN 接続が必要)。また、重要なアプリケーションを優先的に処理して、ワイヤレス LAN インフラストラクチャでの遅延を最小限に抑えることができる。Cisco Security Agent のロケーションベースのポリシー制御を利用すると、ユーザの外出時にも保護を提供できる
トラフィック マーキング	Cisco Security Agent は無線および有線ネットワーク上でアプリケーションごとにトラフィックを分類できるため、Oracle ベースの会計システムや音声/映像システムといった重要なアプリケーションに QoS (Quality of Service) を提供できる。また、Web ブラウジングや E メールなどの重要性の低いアプリケーションには低い優先度を設定して、利用可能なネットワーク帯域幅を最適化することができる。Cisco Security Agent のトラフィック マーキング機能と、Cisco ASA 5500 シリーズおよび Cisco PIX セキュリティ アプライアンスのファイアウォール検査機能を組み合わせて使用すると、特定のアプリケーション検査ポリシーを適用することが可能

機能	説明
IPS との統合	Cisco Security Agent をシスコのネットワーク IPS デバイスと統合すると、ネットワーク内での攻撃を効果的に識別できる。Cisco Security Agent から Cisco IPS 4200 シリーズ アプライアンスや Cisco ASA 5500 シリーズおよび Cisco Catalyst® 6500/7600 シリーズの IPS モジュールに対して重要なエンドポイント セキュリティ情報が提供されるため、完全なエンドツーエンドのセキュリティ ソリューションを実現できる
NAC との統合	Cisco NAC (Network Admission Control) アプライアンスまたは NAC フレームワークでは、Cisco Security Agent が稼働するホストを識別および信頼して、フル ネットワーク アクセスを許可できる。条件を満たさないホストは、修復されて条件を満たすようになるまで隔離することが可能。Cisco Security Agent は、エンドポイント上の NAC エージェントの整合性を保護し、無用な変更が行われるのを防止する。これにより、DoS 攻撃 (サービス拒絶攻撃) やマルウェアによる攻撃を緩和して、企業ネットワークの自己防御力を高めることが可能
CS-MARS イベントとの統合	Cisco Security Agent から CS-MARS (Cisco Security Monitoring, Analysis and Response System) に重要なエンドポイント情報を提供することで、CS-MARS はネットワーク内の脅威の発見や調査をより効果的に実施できる

機能および利点

Cisco Security Agent は、次のようなさまざまな利点を備えています。

- 規制ポリシー順守の実施
- 標的型攻撃からの予防的防御
- ルートキットの識別と隔離
- 先進のホスト侵入防御、パーソナル ファイアウォール、および Day-Zero 攻撃の防御
- Wi-Fi 帯域幅の最適化
- 重要なクライアントサーバ型アプリケーションおよびトランザクションの可用性の確保

製品のアーキテクチャ

Cisco Security Agent ソリューション

Cisco Security Agent は、ミッションクリティカルなデスクトップおよびサーバにインストールするホストベースのエージェントで構成されます。ホストベースのエージェントは CSA-MC (Management Center for Cisco Security Agents) に管理用データを送信します。Management Center は Cisco Security Agent の設定を行うスタンドアロンのアプリケーションです。エージェントの管理インターフェイスおよびエージェントと Management Center 間の通信には、HTTP および 128 ビットの SSL が使用されます。Cisco Security Agent のアラートは、CS-MARS を使用して他のシスコ製セキュリティ製品から発生するアラートと統合できます。

エージェントのアーキテクチャ

Cisco Security Agent はアプリケーションとカーネルの間に位置し、基盤となるオペレーティング システムの安定性とパフォーマンスにほとんど影響を与ることなく、アプリケーションの動作を最大限に把握します。エージェントは独自のアーキテクチャにより、ファイル、ネットワーク、およびレジストリ リソースに対するオペレーティング システム コールのほか、メモリ ページ、共有ライブラリ モジュール、COM オブジェクトなどの動的な実行時リソースへのシステム コールをすべて代行受信します。エージェントは独自のインテリジェンスを利用し、特定のアプリケーションまたはすべてのアプリケーションにとって不適切または許容不可とされる動作を定義したルールに基づいて、これらのシステムコール動作の関連付けを行います。この関連付けと、その後のアプリケーション動作を認識することにより、未知の方法による侵入をセキュリティ担当者の指示に従って阻止することが可能になります。

アプリケーションが何らかの動作を実行しようとする、Cisco Security Agent はその動作をアプリケーションのセキュリティ ポリシーと照合し、動作を続行するか拒否するかをリアルタイムで判断するとともに、要求をログに記録するのが妥当かどうかを決定します。セキュリティ ポリシーとは、保護対象のサーバおよびデスクトップに対し、個別または全社的に IT 管理者またはセキュリティ管理者が割り当てるルールの集合です。これらのルールによって、必要なリソースへの安全なアプリケーション アクセスを確保できます。Cisco Security Agent は、分散型ファイアウォール、オペレーティング システムのロックダウン、整合性の保証、悪意のモバイル コードからの保護、監査イベントの収集といった各

機能を実装するセキュリティ ポリシーを、サーバおよびデスクトップのデフォルト ポリシーに組み合わせることで、外部に開かれた企業システムを階層的に保護します。

不審な動作を阻止することが保護機能の基本となっているため、デフォルトのポリシーを更新しなくても、既知の攻撃と未知の攻撃の両方に対処できます。エージェントと Management Center コンソールの両方で関連付けが実行されます。エージェントでの関連付けにより、精度が大幅に向上し、正当なアクティビティを妨害せずに攻撃と誤用を区別できます。また、Management Center での関連付けにより、ネットワーク ワームや分散スキャンなどのグローバルな攻撃を認識できます。

集中管理

CSA-MC は、すべてのエージェントを集中的に管理するためのさまざまな管理機能を提供します。Web ブラウザを使用してロールベースでアクセスできるので、管理者によるエージェント ソフトウェア配布パッケージの作成、セキュリティ ポリシーの作成または修正、アラートの監視、レポートの生成などの作業を簡単に行うことができます。Management Center は、あらかじめ設定済みのデフォルトポリシーを 20 以上組み込んだ状態で出荷されるので、管理者は数千のエージェントを簡単に全社で展開できます。Management Center を「IDS モード」で展開することも可能です。IDS モードでは、アクティビティに対するアラートが生成されますが、アクティビティ自体は阻止されません。

Management Center には、シンプルでありながら強力なカスタマイズ機能が備わっているため、管理者はデフォルト ポリシーを環境にすばやく適合させることができます。特別なニーズや要件に合わせたルールの修正や完全に新規のルールの作成も、簡単に行えます。規制準拠の監査に役立つ機能として、「ルール説明」機能があります。これは、指定したルールまたはポリシーが何を意図したものであるかの説明を、人間が読める言語形式で管理者が出力できる機能です。

エージェントは Management Center からサーバとデスクトップに直接配布され、このマネージャによって制御および更新されます。各エージェントは自律的に動作します。マネージャと通信できない場合（たとえば、ノート型パソコンを使用するリモート ユーザがまだ VPN 経由で接続していない場合）にも、エージェントは継続的にセキュリティ ポリシーに基づく検査を実施します。その間に発生したセキュリティ アラートは、エージェントによってすべてキャッシュされ、通信が回復したときにマネージャにアップロードされます。

シスコでは、Management Center から分析レポートを作成する一連のツールも提供しています。配置分析機能は、すべてのエージェントにインストールされているアプリケーションの詳細、およびそのアプリケーションの使用に関する情報を提供します。動作分析機能は、特殊な、または未知のアプリケーションや環境に対する包括的なデータ分析ツールを提供します。この機能はアプリケーションの動作に関する詳細なレポートを提供するため、お客様は、お客様固有の環境に合わせて高度にカスタマイズされた非常に複雑なアプリケーションも含め、すべてのアプリケーションを理解できるようになります。

まとめ

Cisco Security Agent は、シスコ自己防衛型ネットワーク ソリューションの中心となるコンポーネントです。お客様は、相互に連携するエンドポイントおよびネットワーク コンポーネントに投資することにより、異種システム間では実現できない新しい重要なセキュリティ サービスを実現できます。

製品仕様

表 2 に、Cisco Security Agent バージョン 5.2 の製品仕様を示します。

表 2 製品仕様

説明	仕様
Cisco Security Server Agent のソフトウェア互換性	<ul style="list-style-type: none"> • Windows 2003 (Standard Edition、Enterprise Edition、Web Edition、または Small Business Edition) • Windows 2000 Server および Advanced Server • Windows NT 4.0 Server および Enterprise Server (Service Pack 6a) • Solaris 8 SPARC アーキテクチャ (64 ビット カーネル) • Solaris 9 SPARC アーキテクチャ (64 ビット カーネル) • Red Hat Enterprise Linux 3.0 ES および AS • Red Hat Enterprise Linux 4.0 ES および AS
Cisco Security Desktop Agent のソフトウェア互換性	<ul style="list-style-type: none"> • Windows XP Professional • Windows XP Tablet Edition • Windows 2000 Professional • Windows NT 4.0 Workstation (Service Pack 6a) • Red Hat Enterprise Linux 3.0 WS • Red Hat Enterprise Linux 4.0 WS
Cisco Security Agent のハードウェア互換性 (Windows OS の最小要件)	<ul style="list-style-type: none"> • 200 MHz x86 プロセッサ • 25 MB のハードドライブの空き領域 • 128 MB RAM • イーサネットまたはダイヤルアップ ネットワーク接続
Cisco Security Agent のハードウェア互換性 (Solaris OS の最小要件)	<ul style="list-style-type: none"> • UltraSPARC 400 MHz プロセッサ • 25 MB のハードドライブの空き領域 • 256 MB RAM • イーサネット ネットワーク接続
Cisco Security Agent のハードウェア互換性 (Linux OS の最小要件)	<ul style="list-style-type: none"> • 500 MHz x86 プロセッサ • 25 MB のハードドライブの空き領域 • 256 MB RAM • イーサネット ネットワーク接続
CSA-MC のソフトウェア互換性	<ul style="list-style-type: none"> • Windows 2003 R2 Server
CSA-MC のハードウェア互換性 (最小要件)	<ul style="list-style-type: none"> • 1 GHz x86 プロセッサ • 1 GB RAM • 2 GB 仮想メモリ
各国語対応	<ul style="list-style-type: none"> • 英語 (アメリカ英語) および国際的な (アラビア語、ヘブライ語を除く) の Windows オペレーティング システム • Windows オペレーティング システムにおける、英語 (アメリカ英語)、中国語 (簡体字)、フランス語、ドイツ語、イタリア語、日本語、韓国語、およびスペイン語でのユーザ インターフェイスの提供 • Linux および Solaris オペレーティング システムについては、英語 (アメリカ英語) のみに対応

発注情報

Cisco Security Agent ソリューションは、2 つの主要コンポーネント (Cisco Security Agent [デスクトップ エージェントとサーバ エージェント] および Management Center) で構成されています。エージェントを使用するには Management Center が必要です。ライセンスを受けていないコンソールでエージェントを使用することはできません。CSA-MC は、Cisco Security Agent スターター バンドル (CSA-START-5.2-K9) に同梱されます。

表 3 に Cisco Security Agent の製品番号、表 4 にメンテナンス製品番号を示します。シスコ製品の購入方法の詳細は、「[発注方法](#)」を参照してください。

表 3 Cisco Security Agent の発注情報

製品名	製品番号
Cisco Security Agent バージョン 5.2 用スターター バンドル (CSA-MC、サーバ エージェント × 1、およびデスクトップ エージェント × 10 を含む)	CSA-START-5.2-K9
Cisco Security Server Agent (Windows、Linux、および Solaris)、1 エージェント	CSA-SRVR-K9
Cisco Security Server Agent (Windows、Linux、および Solaris)、10 エージェント バンドル	CSA-B10-SRVR-K9
Cisco Security Server Agent (Windows、Linux、および Solaris)、25 エージェント バンドル	CSA-B25-SRVR-K9
Cisco Security Server Agent (Windows、Linux、および Solaris)、50 エージェント バンドル	CSA-B50-SRVR-K9
Cisco Security Server Agent (Windows、Linux、および Solaris)、100 エージェント バンドル	CSA-B100-SRVR-K9
Cisco Security Server Agent (Windows、Linux、および Solaris)、500 エージェント バンドル	CSA-B500-SRVR-K9
Cisco Security Server Agent (Windows、Linux、および Solaris)、1,000 エージェント バンドル	CSA-B1000-SRVR-K9
Cisco Security Server Agent (Windows、Linux、および Solaris)、2,500 エージェント バンドル	CSA-B2500-SRVR-K9
Cisco Security Server Agent (Windows、Linux、および Solaris)、5,000 エージェント バンドル	CSA-B5000-SRVR-K9
Cisco Security Server Agent (Windows、Linux、および Solaris)、10,000 エージェント バンドル	CSA-B10000-SRVR-K9
Cisco Security Desktop Agent (Windows および Linux)、25 エージェント バンドル	CSA-B25-DTOP-K9
Cisco Security Desktop Agent (Windows および Linux)、100 エージェント バンドル	CSA-B100-DTOP-K9
Cisco Security Desktop Agent (Windows および Linux)、250 エージェント バンドル	CSA-B250-DTOP-K9
Cisco Security Desktop Agent (Windows および Linux)、500 エージェント バンドル	CSA-B500-DTOP-K9
Cisco Security Desktop Agent (Windows および Linux)、1,000 エージェント バンドル	CSA-B1000-DTOP-K9
Cisco Security Desktop Agent (Windows および Linux)、2,500 エージェント バンドル	CSA-B2500-DTOP-K9
Cisco Security Desktop Agent (Windows および Linux)、5,000 エージェント バンドル	CSA-B5000-DTOP-K9
Cisco Security Desktop Agent (Windows および Linux)、10,000 エージェント バンドル	CSA-B10000-DTOP-K9
Cisco Security Desktop Agent (Windows および Linux)、25,000 エージェント バンドル	CSA-B25000-DTOP-K9
Cisco Security Desktop Agent (Windows および Linux)、50,000 エージェント バンドル	CSA-B50000-DTOP-K9
Cisco Security Desktop Agent (Windows および Linux)、75,000 エージェント バンドル	CSA-B75000-DTOP-K9
Cisco Security Desktop Agent (Windows および Linux)、100,000 エージェント バンドル	CSA-B100000-DTOP-K9
Cisco Security Desktop Agent (Windows および Linux)、200,000 エージェント バンドル	CSA-B200000-DTOP-K9
Cisco Security Desktop Agent (Windows および Linux)、300,000 エージェント バンドル	CSA-B300000-DTOP-K9

サービスおよびサポート

シスコは、お客様がそのネットワーク サービスを最大限に活用するため、各種サービス プログラムを用意しています。これらのサービスは、スタッフ、プロセス、ツールをそれぞれに組み合わせて提供され、お客様から高い評価を受けています。ネットワークへの投資を無駄にすることなく、ネットワーク運用を最適化しネットワーク インテリジェンスの強化や事業拡張を進めていただくためにシスコのサービスを是非お役立てください。サービスについての詳細は、以下の URL を参照してください。

テクニカル サポート サービス

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

サービス プログラム

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

表 4 Cisco Security Agent のメンテナンスに関する発注情報

製品名	製品番号
Cisco Security Agent スターター バンドルの Software Application Support plus Upgrades (SASU)	CON-SAU-CSA-STR52
1 Server Agent (Windows、Linux、および Solaris) の SASU	CON-SAU-CSA-SRVR
10 Server Agent (Windows、Linux、および Solaris) の SASU	CON-SAU-CSA-B10S
25 Server Agent (Windows、Linux、および Solaris) の SASU	CON-SAU-CSA-B25S
50 Server Agent (Windows、Linux、および Solaris) の SASU	CON-SAU-CSA-B50S
100 Server Agent (Windows、Linux、および Solaris) の SASU	CON-SAU-CSA-B100S
250 Server Agent (Windows、Linux、および Solaris) の SASU	CON-SAU-CSA-B250S
500 Server Agent (Windows、Linux、および Solaris) の SASU	CON-SAU-CSA-B500S
1,000 Server Agent (Windows、Linux、および Solaris) の SASU	CON-SAU-CSA-B1000S
2,500 Server Agent (Windows、Linux、および Solaris) の SASU	CON-SAU-CSA-B2500S
5,000 Server Agent (Windows、Linux、および Solaris) の SASU	CON-SAU-CSA-B5000S
10,000 Server Agent (Windows、Linux、および Solaris) の SASU	CON-SAU-CSA-B10000S
25 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B25D
100 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B100D
250 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B250D
500 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B500D
1,000 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B1000D
2,500 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B2500D
5,000 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B5000D
10,000 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B10KD
25,000 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B25KD
50,000 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B50KD
75,000 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B75KD
100,000 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B100KD
200,000 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B200KD
300,000 Desktop Agent バンドル (Windows および Linux) の SASU	CON-SAU-CSA-B300KD

©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。(0701R)

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

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館

<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