

Cisco Incident Control System

Cisco® ICS (Incident Control System) を使用すると、ネットワーク自身が事態に迅速に対応して被害の拡散を防止できるようになるため、新しいワームやウイルスへの大規模感染の影響が業務に及ぶことを防止できます。

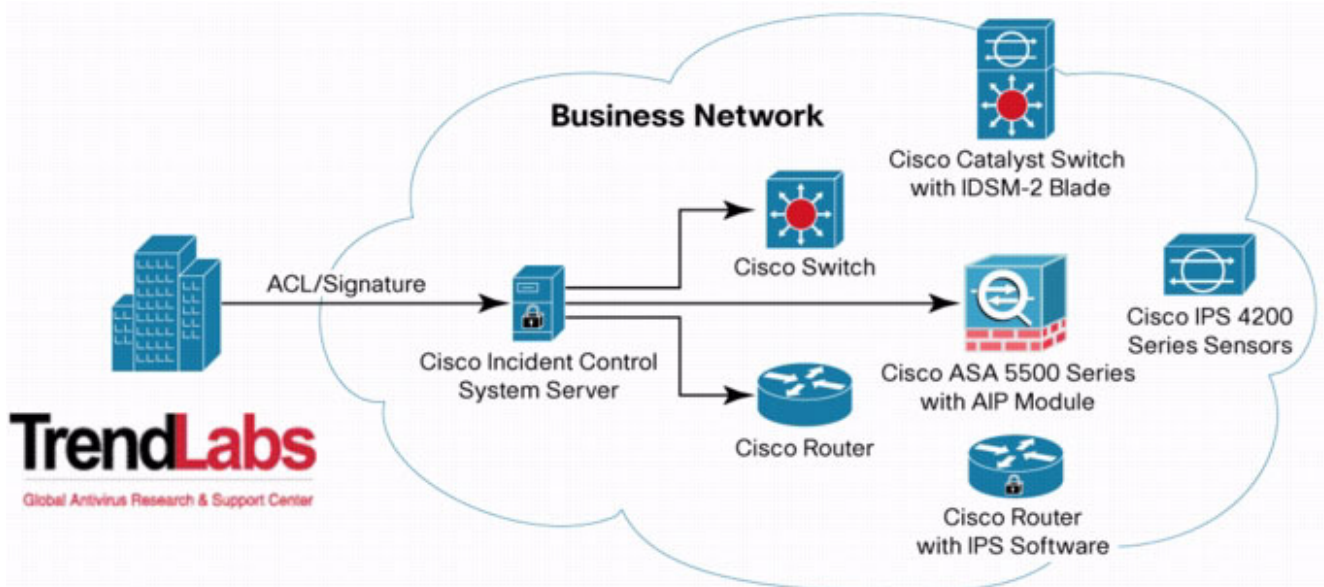
発生したワームまたはウイルスが世界中に広がる時間は、数日から数分へと短期化しています。業務ネットワークの安全性を保つためには、脅威の発生場所に関係なく、発生後すぐに予防的な拡散防止措置を講じる必要があります。Cisco ICS ソリューションではこうしたニーズに対応し、世界中のどこでワームやウイルスが発生しても、数分以内にネットワーク全体を防御することができます。Cisco ICS では、トレンドラボによるグローバル モニタリング機能を活用しており、シスコの既存のネットワーク デバイスおよびセキュリティ デバイスと連携して、ワームやウイルスに対する予防策をネットワーク全体に迅速に展開できます。この迅速かつ予防的なアプローチによって、ワームやウイルスが拡散するのを防ぎ、ネットワークの可用性を保って、被害の復旧に付随するコストを削減できます。

システムの主な機能は、次のとおりです。

- アンチウイルスおよびワーム軽減対策の専門企業として業界をリードするトレンドマイクロ社から提供される、最新の脅威に関する情報を利用
- ワームおよびウイルスへの予防的な防御を可能にする迅速な拡散防止措置
- 既存のシスコ製ネットワーク デバイスとセキュリティ デバイスを、ネットワーク全体での組織的な拡散防止措置にリアルタイムで適応できるよう強化
- 業務ネットワークで、Cisco ICS による感染抑制ポリシーの実施を詳細に制御可能

図 1 は、トレンドラボで悪意のあるソフトウェアの出現が確認されたあと、Cisco ICS ソリューションによって迅速に防御対策が展開される様子を示しています。Cisco ICS ソリューションによって脅威への適切な防御対策がインテリジェントに判断され、ネットワーク インフラストラクチャ全体に対抗策を講じることができます。

図 1 Cisco ICS によるネットワーク全体の防御機能



トレンドラボによる専門知識の提供

Cisco ICS ソリューションはトレンドラボとの連携体制にあります。トレンドラボは、トレンドマイクロ社のグローバルなウイルス対策専門家チームです。トレンドラボは 700 人を超えるセキュリティの専門家で構成され、1 年を通じて、24 時間体制でワームおよびウイルスの活動をグローバルに監視しています。トレンドマイクロ社では全世界にわたって監視を行い、新たな脅威を迅速に発見しています。これによって、多くの企業では、脅威の拡散や感染を未然に食い止めることができます。このチームは、各ネットワーク ウイルスをラボで複製し、ウイルスの活動を分析して、その情報を予防的な感染抑制ソリューションへと逐次追加しています。厳しいテストを実施して新たなワクチンが適切に機能することを確認し、最も効果的な保護策を提供します。

迅速かつ予防的な防御策

迅速な防御対策と品質管理の両方のニーズを満たすため、チームでは 2 段階のアプローチによってネットワークでの大規模感染を防止します。まず、ACL (Access Control List; アクセスコントロールリスト) を使って高水準のポリシー アップデートを実行し、発生から数分以内に感染源をブロックします。まもなく、ACL に代わる、より詳細かつ厳密な IPS (侵入防御システム) シグニチャがリリースされ、新たな脅威に対して恒常的な保護策を実施できます。この 2 段階アプローチの利点は、次のとおりです。

- 新たな脅威の確認後、数分以内に最も効果的な保護策を実施
- 脅威の分析完了後にシグニチャを提供し、より集中的なセキュリティ対策を実施

ポリシーまたはシグニチャはアップデートされるとすぐに、セキュアな通信を使用して、ネットワーク内の Cisco ICS サーバへと配布されます。次に、そのサーバを通じて、ネットワーク全体に配置された、さまざまなシスコ製の脅威感染抑制デバイスへと更新データが配布されます。Cisco ICS の中央集中型管理コンソールを使用すると、自動配布または手動配布を選択するなど、管理者は感染抑制デバイスへの感染防止ポリシーおよびシグニチャの展開方法を制御できます。

この迅速な防御対策ソリューションは、Cisco Services for IPS を強化するために設計されています。Cisco Services for IPS は、シグニチャに関する標準レベルのサービスです。アプライアンス、ルータ モジュール、スイッチ モジュール、Cisco IOS[®] ソフトウェアなど、さまざまな Cisco IOS デバイス用の更新データを 1 つのファイルにまとめ、脅威発生の数時間後に提供します。

全ネットワーク規模の防御対策

イントラネット、エクストラネット、ブランチ オフィス、ホーム オフィス、外出先など、ワームやウイルスはさまざまな場所からネットワークに侵入する可能性があるため、幅広いアプローチが必要です。Cisco ICS ソリューションは、シスコのさまざまな脅威感染抑制デバイスと連携して、業務ネットワークへのあらゆる侵入経路をカバーします。その結果、ネットワーク インフラストラクチャ内の全デバイスに対して事前に防御策を講じることができ、新たな脅威の侵入を組織的に防ぐことができます。こうした全ネットワーク規模の予防的なアプローチによって、感染源からのアクセスを拒否できる可能性が高まり、侵入経路が発見された場合にも、迅速な阻止が可能になります。

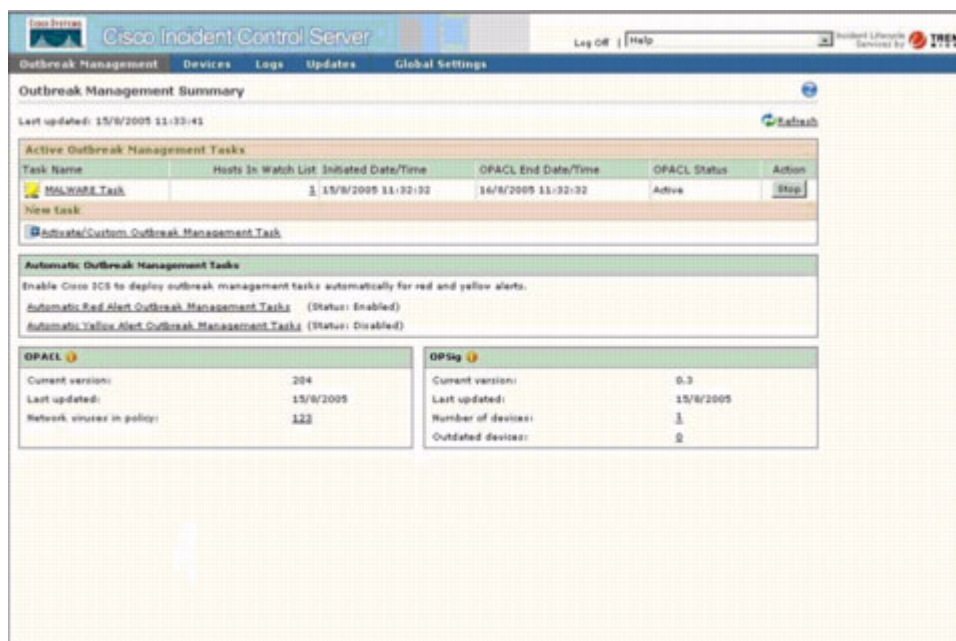
ネットワーク デバイスやセキュリティ デバイスの種類に応じて、提供できる感染抑制対策の制御レベルは異なります。インターフェイスベースの ACL に対応したシスコ ルータとスイッチでは、基本レベルのサービスを提供し、脅威発生の数分後に提供される ACL タイプのアップデートを幅広くサポートします。シスコのネットワーク デバイスの多くは ACL をサポートしているため、このレベルのサービスによって、ネットワーク インフラストラクチャ全体を深刻な大規模感染から保護することができます。また、シスコ ルータ、スイッチ、およびアプライアンスの多くには、IPS シグニチャのアップデート機能があります。これらのデバイスでは、より高度なサービスを提供でき、防御対策の第 2 段階でリリースされる詳細なシグニチャ アップデートをサポートしています。この高度なサービスをサポートするデバイスには、Cisco IPS 4200 シリーズ センサ、Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス (AIP モジュール搭載時)、Cisco Catalyst スイッチ用の IDS/IPS (Intrusion Detection System Services Module) ブレード、および Cisco IOS ソフトウェア セキュリティ イメージを実行するシスコ ルータなどがあります。これらのデバイスの多くは ACL タイプのアップデートもサポートしているため、1 つのデバイスで、ACL による初期保護サービスと IPS シグニチャによる長期の感染抑制サービスの両方を提供できます。Cisco ICS は、シスコの包括的な

大規模感染防止ソリューションの一部として機能し、CS-MARS（Cisco Security Monitoring, Analysis and Response System）との完全な互換性を備えています。CS-MARSを使用すると、ネットワークへの攻撃をすばやく正確に識別、管理、および除去して、ネットワークのセキュリティポリシーを維持できます。

大規模感染抑制ポリシーの詳細な制御

Cisco ICS サーバは Web ベースの GUI ポリシー サーバで、大規模感染を抑制するための情報の展開方法を、各環境に応じて詳細に制御できます。たとえば管理者は、ICS 感染抑制サービスを適用するシスコ ネットワーク エレメントを指定し、脅威の重大度に基づいて、ICS サービスを自動または手動で適用するように定義できます。また、推奨される ACL ポリシーをローカルに作成した ACL で上書きしたり、特定のルータに適用される ACL のタイプ（プロトコルまたはポート固有の ACL など）を制御したりすることも可能です。このポリシー制御環境の豊富な機能によって、ローカルでの高度なカスタマイズが可能になり、業務への影響を最小限に抑えながら、幅広い保護機能を実現できます（図 2）。

図 2 Cisco ICS サーバ



仕様

Cisco ICS サーバのシステム要件

以下に、最小限必要なバージョンを示します。

オペレーティング システム

- Windows 2000 Server または Advanced Server（SP3 適用）
- Windows 2003 Server Standard Edition または Enterprise Edition（英語版）

Web サーバ

- IIS : Windows 2000 IIS 5.0 または Windows 2003 IIS 6.0
- Apache : 2.0

Web ブラウザ (Web コンソール アクセス用)

- Internet Explorer バージョン 5.5 SP2

ハードウェア

- 866 MHz Intel Pentium III または同等のプロセッサ
- 512 MB の RAM
- 350 MB のディスク領域

大規模感染抑制デバイスのライセンス要件

表 1 に、大規模感染抑制デバイスで利用可能なサービスのタイプと、デバイスをサポートするために必要な関連ライセンスを示します。

表 1 大規模感染抑制デバイスのライセンス要件

Cisco ICS 保障タイプ	感染抑制デバイス	最小限必要なソフトウェア バージョン	必要なライセンス
ACL 保障	Cisco 800 シリーズ ルータ、Cisco 1700 シリーズ モジュラ アクセス ルータ、Cisco ISR 1800 シリーズ、Cisco 2600XM ルータ、Cisco ISR 2800 シリーズ ルータ、Cisco 3600 シリーズ ルータ、Cisco 3700 シリーズ マルチサービス アクセス ルータ、Cisco ISR 3800 シリーズ ルータ、Cisco 7200 シリーズ ルータ、および Cisco 7301 ルータ	Cisco IOS ソフトウェア リリース 12.3M	ICS-LIC-ACL-25
	Cisco Catalyst 3550 シリーズ スイッチ	Cisco IOS ソフトウェア リリース 12.1(22)EA5	
	Cisco Catalyst 6500 シリーズ スイッチ	Cisco IOS ソフトウェア リリース 12.2(18)SXD5	
	Cisco 7600 シリーズ ルータ	Cisco IOS ソフトウェア リリース 12.2(17)SXB8	
ACL+IPS 保障	Cisco ISR 3800 シリーズ ルータ、Cisco 7200 シリーズ ルータ、および Cisco 7301 ルータ	Cisco IOS ソフトウェア リリース 12.4(4)T	ICS-LIC-IPS-HE-1
	Cisco IPS 4215 センサ	Cisco IPS センサ ソフトウェア v5.1	
	Cisco IPS 4235 センサ	Cisco IPS センサ ソフトウェア v5.1	
	Cisco IPS 4240 センサ	Cisco IPS センサ ソフトウェア v5.1	
	Cisco IPS 4250 センサ	Cisco IPS センサ ソフトウェア v5.1	
	Cisco IPS 4250XL センサ	Cisco IPS センサ ソフトウェア v5.1	
	Cisco IPS 4255 センサ	Cisco IPS センサ ソフトウェア v5.1	
	Cisco IDSM-2 Catalyst モジュール	Cisco IPS センサ ソフトウェア v5.1	
Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス (AIP-SSM-20 使用時)	Cisco ASA ソフトウェア v7.0/ Cisco IPS センサ ソフトウェア v5.1		

Cisco ICS 保障タイプ	感染抑制デバイス	最小限必要なソフトウェア バージョン	必要なライセンス
	Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス (AIP-SSM-10 使用時)	Cisco ASA ソフトウェア v7.0/Cisco IPS センサ ソフトウェア v5.1	ICS-LIC-IPS-LE-5
	Cisco 800 シリーズ ルータ、Cisco 1700 シリーズ モジュラ アクセス ルータ、Cisco ISR 1800 シリーズ ルータ、Cisco 2600XM ルータ、Cisco ISR 2800 シリーズ ルータ、Cisco 3600 シリーズ ルータ、および Cisco 3700 シリーズ マルチサービス アクセス ルータ	Cisco IOS ソフトウェア リリース 12.4(4)T	

発注情報

Cisco ICS サーバ ソフトウェアは、すべての構成について発注する必要があります。また、感染抑制デバイス用のライセンスを1つ以上発注する必要があります。評価バージョン（60日間試用可。各 ICS 大規模感染抑制デバイス ライセンス [表 2]×1）の発注も可能です。

表 2 発注情報

シスコ製品番号	説明
ICS-EVAL-K9	Cisco ICS 60 日間評価キット（次の 4 つの製品番号を含む）
ICS-SVR-V10-K9	Cisco ICS ソフトウェア v1.0
ICS-LIC-IPS-HE-1	Cisco ICS ライセンス：ハイエンド デバイス用 ACL+IPS サービス×1
ICS-LIC-IPS-LE-5	Cisco ICS ライセンス：ローエンド デバイス用 ACL+IPS サービス×5
ICS-LIC-ACL-25	Cisco ICS ライセンス：ACL サービス×25

シスコ ライフサイクル サービス

効率的な Cisco ICS ソリューションの計画、設計、展開、および運用

シスコのサービス ポートフォリオでは、お客様のネットワーク ライフサイクルの各段階で、高度なテクニカル サポート サービスを幅広く提供します。

シスコ アドバンスド サービス

シスコでは、要件分析、計画、設計、実装コンサルティングなどの高度なサービスを提供し、Cisco ICS ソリューションを効果的に利用するために不可欠な専門的アドバイスを提供します。シスコ アドバンスド サービスのコンサルタントは、Cisco ICS の展開をサポートするため、以下のサービスを提供します。

1. Cisco ICS の即応性評価
2. Cisco ICS の設計開発
3. Cisco ICS の実装エンジニアリング

シスコ テクニカル サポート サービス

シスコのテクニカル サポート サービス ポートフォリオの 1 つである Cisco Software Application Support plus Upgrades (SASU) は、Cisco ICS サーバ ソフトウェアで必要となるサポートに対応しています。Cisco SASU プログラムでは、Cisco ICS ソフトウェア アップデート、Cisco Technical Assistance Center、Cisco.com に世界中からいつでもアクセスできます。

Cisco ICS ソリューションでは、すべての感染抑制デバイスが有効なサポート契約によってカバーされている必要があります。ACL 保障の対象となる感染抑制デバイスには、有効な Cisco SMARTnet[®] 契約が適用されている必要があります。また、IPS 保障の対象となる感染抑制デバイスには、有効な Cisco Services for IPS 契約が適用されている必要があります。

関連情報

Cisco ICS の詳細については、以下の URL にアクセスしてください。

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

Cisco IPS ソリューションの詳細については、以下の URL にアクセスしてください。

<http://www.cisco.com/jp/product/hs/security/ids4200/>

シスコ テクニカル サポート サービスの詳細については、以下の URL にアクセスしてください。

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

シスコ アドバンスド サービスの詳細については、以下の URL にアクセスしてください。

<http://www.cisco.com/jp/service/contact/as.shtml>

©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。(0609R)

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/service/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