

Cisco Incident Control System

2004年に、トレンドマイクロ社の World Tracking Center では計 37,822,805 件のウイルス感染が記録されました。アンチウイルス ソフトウェアを販売する他のベンダーでも、同様の件数が記録され、実際の感染はこの数値の 10 倍であると推測されています。感染が世界中で報告され、数千から数百万のユーザに影響が及ぶと、通常は大規模感染とみなされます。2004年には、トレンドマイクロ社は 28 件のウイルスの大規模感染を宣言しました。ICSA の Tenth Annual Virus Prevalence Survey によると、大規模感染によってウイルスに感染した組織における復旧コストは、平均で 130,000 米ドルでした。

このように増加し続けるウイルスの脅威に対抗するために、シスコシステムズとトレンドマイクロ社は、ネットワークの脅威に対する高レベルの保護や、より高度なサービスを、リアルタイムで脅威を軽減する形式で業界に提供するための共同イニシアティブに着手しました。この共同の取り組みにより、シスコおよびトレンドマイクロ社は、セキュリティ プロフェッショナル向けの新しい強力なソリューションとなる Cisco Incident Control System (ICS)を開発しました。Cisco ICS ソリューションの中心となっているのは、Cisco ICS サーバです。このソフトウェアは、管理センターおよび配信センターとして機能し、お客様がさまざまなシスコ製ネットワーク デバイスに、感染への迅速な対応を可能にする感染抑制ポリシーを導入できるようにします。Cisco ICS を使用すると、新たに検出された大規模感染から引き起こされる脅威のネットワークへの侵入を、これらのネットワーク デバイス上で効率的かつ迅速に防御できるようになります。

Cisco ICS ソリューションのネットワークに対する総合的なアプローチおよび認識方法に、トレンドマイクロの脅威に関する優れた専門知識および対応機能を組み合わせることにより、Cisco ICS は、Cisco Services for IPS サービス製品向けの重要な付加機能になります。Cisco ICS は、ウイルスの脅威がネットワーク全体に侵入して伝播するのを防ぐ優れた効果を発揮するだけでなく、侵入が限定されている場合はそれらのウイルスを全滅させます。また、新たな脅威をほぼ即時に認識して対応する機能をネットワーク全体に提供し、シスコのインフラストラクチャ デバイスがこれまでよりも迅速に感染抑制ポイントとして機能できるようにします。

製品コンポーネントの概要

Cisco ICS ソリューションは、Cisco ICS サーバ ソフトウェアと感染抑制デバイス用ライセンスの 2 つのコンポーネントで構成されています。感染抑制デバイスとは、Cisco ICS が提供する大規模感染防止ポリシーの受信側として Cisco ICS サーバが認識する、シスコのネットワーク製品です。ライセンスには、次の異なる 3 種類があり、これらは感染抑制デバイスの機能の 1 つとなります。

- **Access Control List (ACL; アクセス コントロール リスト) デバイス ライセンス**— 標準 (非セキュリティ) の Cisco IOS[®] ソフトウェア イメージを実行する、互換性のある Cisco ルータおよびスイッチで使用されます。
- **Intrusion Prevention System (IPS; 侵入防御システム) ローエンド デバイス ライセンス**— Cisco IOS ソフトウェア セキュリティ イメージを実行する IPS 対応の Cisco IOS ソフトウェアベースのルータを含む、互換性のあるローエンド Cisco IPS デバイスで使用されます。ローエンド Cisco IPS デバイスには、Application Inspection and Prevention Security Services

Module 10 (SSM-AIP-10)を搭載した、すべての Cisco IPS 4215 センサおよび Cisco ASA 5500 シリーズ適応型セキュリティアプライアンスが含まれます。

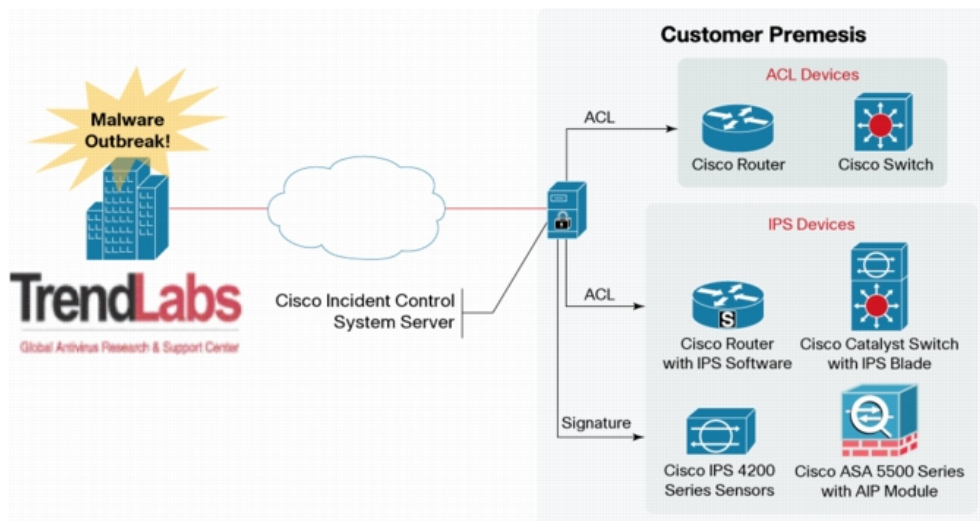
- **IPS ハイエンド デバイス ライセンス**— Cisco IOS ソフトウェア セキュリティ イメージを実行する IPS 対応の Cisco IOS ソフトウェア ルータを含む、互換性のあるハイエンド IPS デバイスで使用されます。ハイエンド IPS デバイスには、Cisco ISR 3800 シリーズ、Cisco 7200 シリーズ ルータ、Cisco IPS 4235、4240、4250、4250 XL、4255 センサ、Cisco Catalyst® 6500 シリーズ スイッチ用 Intrusion Detection System Module (IDSM-2) ブレード、SSM-AIP-20 を搭載した Cisco ASA 5500 シリーズ適応型セキュリティアプライアンスが含まれます。

この運用モデルは、Cisco ICS サーバ ソフトウェアのコピーおよび必要な数の Cisco ICS ライセンスを購入する管理者が対象となります。製品を登録し、すべてのコンポーネントのライセンス キーを取得したあとで、お客様が使用するハードウェアに Cisco ICS サーバ ソフトウェアがインストールされ、ICS サーバにライセンス キーがインストールされます。管理者は、Cisco ICS ライセンスを適切な感染抑制デバイスに関連付ける必要があります。この関連付けにより、これらのデバイスが新たに検出された大規模感染の感染抑制ポイントになります。

Cisco ICS

図 1 に Cisco ICS の動作を示します。この図では、トレンドラボで識別された悪意のあるソフトウェアによる大規模感染に対して Cisco ICS が迅速に反応し、脅威に対応するためのインテリジェンスをネットワーク インフラストラクチャ全体に提供しています。

図 1 Cisco ICS の動作



動作

設定と構成が完了すると、Cisco ICS はいくつかの段階を経て動作します。ここでは、それについて説明します。

脅威の検出および識別と OPACL の展開

トレンドラボでは、世界中のインターネットおよびその他の情報ソースを監視し、新たな大規模感染がないか調査しています。また、脅威の分析、迅速かつ永続的な対応が可能なシングニチャの作成、目視検査、機能テスト、障害アラームのテスト、企業の ActiveUpdate (AU) サーバへのパターンのアップロードなどを通して、詳細な対応を行っています。悪意のあるソフトウェアによる新たな感染が検出されると、トレンドラボのウイルス専門家は、脅威の分析、分類、および識別を開始しま

す。この迅速な初期段階の作業により、Outbreak Prevention Access Control List(OPACL)が作成されます。OPACL は、通常はその性質上、きめ細かな対策を提供するものではありません。つまり、短期間のソリューションとして、ポートまたはプロトコルを遮断し、悪意のあるソフトウェアのネットワークへの侵入または拡大を防ぐのが目的となります。この性質上、OPACL は通常のネットワークの動作に悪影響を及ぼす可能性があるため、一時的な手段と考える必要があります。通常、OPACL は、ウイルスの大規模感染が検出されてから 15 分以内にトレンドラボからリリースされます。OPACL は その後、トレンドマイクロ社の AU サーバに配置され、Outbreak Management Task(OMT)の一部として Cisco ICS サーバでダウンロードできるようになります。Cisco ICS サーバは、トレンドラボの AU サーバを常にポーリングし、大規模感染の発生と OMT の存在を確認します。Cisco ICS サーバで OMT の存在が確認されると、Cisco ICS によるタスクの作成、管理者への通知の送信、および OPACL の自動ダウンロードが行われ、この OPACL が設定済みのシスコの感染抑制デバイスに自動的に展開されます(自動展開が設定されている場合)。Cisco ICS サーバの自動展開を設定していない場合、管理者は OPACL を検査し、必要な変更を行ってから手動で導入することができます。OPACL は HTTPS を使用して Cisco IPS デバイスに送信され、デフォルトの Secure Shell (SSH) プロトコルまたは Telnet を使用してルータおよびスイッチに送信されます。

OPSig の作成と展開

OPACL のリリース後、トレンドラボは、その他のすべてのタイプのトラフィックから脅威を一意に識別する Outbreak Prevention Signature(OPSig)を引き続き作成します。通常、トレンドラボはウイルスの大規模感染の検出から 90 分以内にこの OPSig を作成し、トレンドマイクロ社の AU サーバで使用できるようにします。この時点で、OPSig は進行中の OMT の一部として Cisco ICS サーバでダウンロードできるようになります。Cisco ICS サーバはこの OPSig を自動的にダウンロードし、永続的な手段として IPS 対応の感染抑制デバイスに展開するとともに、以前にインストールされた OPACL と置き換えます。これにより、以前に配布された OPACL によって中断が発生していた場合でも、完全に正常なネットワーク運用に戻ることができます。OPSig が提供する保護は、Cisco Signature Development Team でも使用できるようになるとともに、有効な Cisco Services for IPS サービス契約を結んでいるすべての Cisco IPS 対応製品で使用できる標準のシグニチャ更新の一部としてリリースされます。通常、この更新は、大規模感染が識別されてから 6 ~ 8 時間以内に使用可能になります。

製品の詳細

サービス タイプ

Cisco ICS ソリューションでは、ACL 保障と IPS 保障の 2 つのタイプの保障を提供しています。

ACL 保障

ACL 保障では、感染抑制デバイスに OPACL を提供します。ACL 保障は、IDS ソフトウェアまたは IPS ソフトウェアを実行しておらず、ACL またはフィルタをサポートしているシスコ製品に適用されます。このレベルの保障の対象となる Cisco ACL 対応製品は表 1 に示されています。また、以下が含まれます。

- 互換性のあるシスコ ルータ
- 互換性のあるシスコ スイッチ

Cisco ICS の要件として、ACL 保障の対象となるすべてのデバイスには、有効な Cisco SMARTnet[®] 契約または同等のパートナー サポート プログラムが必要です。

IPS 保障

IPS 保障では、感染抑制デバイスに OPACL と OPSig を提供します。IPS 保障は、完全にロード可能な IPS シグニチャ機能を備えたすべてのシスコ製品に適用できます。このレベルの保障の対象となる Cisco IPS 対応製品は、次のとおりです。

- Cisco IPS Sensor Software v5.1 以降を実行している Cisco IPS 4200 シリーズ センサ
 - SSM で Cisco IPS Software v5.1 以降を実行している、SSM-AIP モジュール搭載の Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
 - Cisco IPS Software v5.1 以降を実行している Cisco Catalyst 6500 IDSM2 ブレード
 - Cisco IOS ソフトウェア リリース 12.4(4)T 以降のセキュリティ イメージを搭載したシスコ ルータ
- Cisco ICS の要件として、IPS 保障の対象となるすべてのデバイスには、有効な Cisco Services for IPS サポート契約が必要です。

また、この資料の前半で説明したように、IPS 対応デバイスの IPS パフォーマンス関連機能に基づいた IPS ライセンスには、2 つのタイプ(ハイエンド IPS ライセンスおよびローエンド IPS ライセンス)があります。この 2 つのタイプの IPS ライセンスの機能と動作は同じです。Cisco ICS サーバにインストールし、特定の感染抑制デバイスに割り当てる必要のある、感染抑制デバイスのライセンス タイプが異なるだけです。

表 1 に、サービスとライセンスのタイプ、および感染抑制デバイスに最小限必要なソフトウェアのバージョンを示します。

表 1 互換性のあるデバイス、必要なソフトウェア バージョン、ライセンス タイプ、およびサービスの前提条件

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 (デバイスごとに1つ)	必要なサービス契約
ACL 保障 (OPACL のみ)	Cisco 800、1700、ISR 1800、2600XM、ISR 2800、3600、ISR 3800、7200、および 7301 シリーズ ルータ	Cisco IOS® ソフトウェア リリース 12.3M	ACL (ICS-LIC-ACL-25)	Cisco SMARTnet® サポートまたは同等のパートナーサポート プログラム
	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		
IPS 保障 (OPACL および OPSig)	Cisco ISR 3800 シリーズ	Cisco IOS ソフトウェア リリース 12.4(4)T	IPS ハイエンド (ICS-LIC-IPS-HE-1)	Cisco Services for IPS
	Cisco 7200 シリーズ ルータ	Cisco IOS ソフトウェア リリース 12.4(4)T		
	Cisco IPS 4235 センサ	Cisco IPS Sensor Software v5.1		
	Cisco IPS 4240 センサ	Cisco IPS Sensor Software v5.1		
	Cisco IPS 4250 センサ	Cisco IPS Sensor Software v5.1		
	Cisco IPS 4250XL センサ	Cisco IPS Sensor Software v5.1		
	Cisco IPS 4255 センサ	Cisco IPS Sensor Software v5.1		
	Cisco Catalyst 6500 シリーズ Intrusion Detection System Services Module (IDSM-2s)	Cisco IPS Sensor Software 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 を使用)	Cisco ASA Software v7.0/ Cisco IPS Sensor Software 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 (デバイスごとに1つ)	必要なサービス契約
	Cisco IPS 4215 センサ	Cisco IPS Sensor Software v5.1	IPS ローエンド (ICS-LIC-IPS-LE-5)	Cisco Services for IPS
	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 を使用)	Cisco ASA Software v7.0/ Cisco IPS Sensor Software v5.1		
	Cisco 870 シリーズ ルータ、Cisco 1700 シリーズ モジュール 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、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		

要件および設定

企業で Cisco ICS ソリューションを実装するには、Cisco ICS サーバソフトウェアをインストールするためのサーバプラットフォームが必要です。前述のとおり、迅速な対応が可能な大規模感染抑制ポリシーの受信側として機能する、シスコの感染抑制デバイスも必要です。

Cisco ICS ソフトウェアは、表 2 に示すハードウェアおよび OS の最小要件を満たすサーバプラットフォームにインストールする必要があります。

表 2 ハードウェアおよび OS の最小要件

オペレーティングシステム
<ul style="list-style-type: none"> Windows 2000 Server または Advanced Server (Service Pack 3) Windows 2003 Server Standard Edition または Enterprise Edition (英語版)
ハードウェア
<ul style="list-style-type: none"> 866 MHz Intel Pentium III 以上のプロセッサ 512 MB の RAM 350 MB のディスク領域
Web サーバ
<ul style="list-style-type: none"> IIS: Windows 2000 IIS 5.0 または Windows 2003 IIS 6.0 Apache: 2.0
Web ブラウザ(管理インターフェイス アクセス用)
<ul style="list-style-type: none"> Internet Explorer バージョン 5.5 SP2

大規模感染防止サービスに必要なコンポーネントで発注可能なものは、シスコ製品番号で示されています。これにより、お客様はご使用の環境と必要な構成シナリオに応じて、Cisco ICS サーバソフトウェアと 3 つのタイプの Cisco ICS 年間ライセンスを発注できます。表 3 に発注可能なシスコ製品番号を示します。

表 3 発注可能な製品番号

シスコ製品番号	説明
ICS-SVR-V10-K9	Cisco Incident Control System (ICS) Server Software v1.0
ICS-LIC-IPS-HE-1	Cisco ICS ライセンス:ハイエンド デバイス用 IPS 保障× 1
ICS-LIC-IPS-LE-5	Cisco ICS ライセンス:ローエンド デバイス用 IPS 保障× 5
ICS-LIC-ACL-25	Cisco ICS ライセンス:ACL 保障× 25
ICS-EVAL-K9	Cisco ICS 60 日間評価キット(Cisco ICS ソフトウェア、ACL ライセンス× 25、IPS ローエンドライセンス× 5、および IPS ハイエンドライセンス× 1 を含む)

Cisco ICS サーバをインストールする前に、管理者は出荷製品ごとの指示に従って、製品コンポーネントを登録し、適用可能なライセンス キーを取得する必要があります。Cisco ICS サーバのインストール時に、メッセージが表示され、管理者は Cisco ICS ソフトウェアおよび感染抑制デバイスライセンスのライセンス キーを入力するように要求されます。このインストールを完了したあとで、必要な感染抑制デバイス、展開ポリシー、および例外規則について、ソフトウェアを設定できます。

Cisco ICS サーバのライセンス管理は、従来のライセンス更新とは異なります。Cisco ICS サーバでは、管理者にとってより利便性が高く、ライセンスに関する管理上のオーバーヘッドの削減が可能なモデルを実装しています。Cisco ICS ライセンス モデルは、2 つの点で従来のモデルとは異なります。

- Cisco ICS サーバは、ライセンスが最初からインストールされている「デビットカード」ライセンス方式を使用しており、失効時には、Cisco ICS サーバで同じタイプ(必要な場合は異なるタイプ)の追加ライセンスを購入して再インストールできます。これにより、管理者が製品番号の管理と購入製品の追跡調査を行う際の負担が軽減されます。
- Cisco ICS サーバでは、ライセンスの有効期限の満了日が、固定された 4 つの失効日(3 月 31 日、6 月 30 日、9 月 30 日、および 12 月 31 日)のいずれかとなります。これにより、管理者が留意すべき失効日の数を少なくできます。

表 4 に、さまざまな感染抑制デバイスの機能について、詳細を示します。

表 4 感染抑制デバイスの詳細

感染抑制デバイスのタイプ	シスコ製品またはファミリ	アカウント認定証	OPACL の展開先	OPSig の展開	OPACL モード
IPS デバイス	<ul style="list-style-type: none"> • Cisco IPS 4200 シリーズ センサ • Cisco Catalyst 6500 シリーズ IDSM-2 プレード • Cisco ASA 5500 適応型セキュリティアプライアンス(AIP-SSMを搭載) 	<ul style="list-style-type: none"> • 管理者 	<ul style="list-style-type: none"> • インターフェイス (インバウンドおよびアウトバウンドトラフィック) 	<ul style="list-style-type: none"> • あり 	<ul style="list-style-type: none"> • ブロッキングとロギング
Cisco IOS ソフトウェア IPS デバイス	<ul style="list-style-type: none"> • Cisco IOS ソフトウェア セキュリティイメージを搭載したルータ 	<ul style="list-style-type: none"> • 管理者 	<ul style="list-style-type: none"> • インターフェイス (インバウンドおよびアウトバウンドトラフィック) 	<ul style="list-style-type: none"> • あり 	<ul style="list-style-type: none"> • ブロッキングとロギング
スイッチ	<ul style="list-style-type: none"> • Cisco IOS ソフトウェアを実行する標準のスイッチ 	<ul style="list-style-type: none"> • レベル 15 または ルート ビュー 	<ul style="list-style-type: none"> • 物理インターフェイス(インバウンドトラフィックのみ) • VLAN(インバウンドおよびアウトバウンドトラフィック) 	<ul style="list-style-type: none"> • なし 	<ul style="list-style-type: none"> • ブロッキングのみ
ルータ	<ul style="list-style-type: none"> • Cisco IOS ソフトウェアを実行する標準のルータ 	<ul style="list-style-type: none"> • レベル 15 または ルート ビュー 	<ul style="list-style-type: none"> • 物理インターフェイス(インバウンドおよびアウトバウンドトラフィック) • VLAN(インバウンドおよびアウトバウンドトラフィック) 	<ul style="list-style-type: none"> • なし 	<ul style="list-style-type: none"> • ブロッキングのみ

スケーラビリティの推奨事項

シスコシステムズでは、さまざまな企業のお客様のネットワーク アーキテクチャのテストを行っているラボで、Cisco ICS ソリューションのスケーラビリティとパフォーマンスを検証しています。Cisco ICS ソリューションは、規模(200 以上のデバイス)、ネットワーク イベント収集のパフォーマンス(毎秒 1000 以上)、大規模ネットワーク上の多数のデバイスへのシグニチャおよび ACL 更新の迅速な展開(8 分以内)の面で、対象となる企業のお客様のニーズを満たしていることがテストによって

証明されています。このテストに基づいて、製品チームは最大 500 個の感染抑制デバイスの導入を保証しています。1 台の ICS サーバに 500 以上のデバイスを展開する場合、製品の投入の前に、それが可能かどうかをお客様の環境で検証およびテストする必要があります。より多くのデバイスを必要とする構成の場合、必要とされる感染抑制デバイスの総数に合わせて、複数のシングル CPU サーバ、または 1 台のデュアル CPU サーバを使用することを推奨します。Cisco ICS サーバ ソフトウェアの将来のリリースでは、階層型の ICS サーバをサポートすることにより、大規模な展開を単一ポイントでより集中的かつ総合的に管理できるようになります。

アーキテクチャおよび機能

Cisco ICS サーバは、Cisco ICS ソリューションのすべての OMT において管理および展開の中心として機能します。Cisco ICS サーバは、OMT コンポーネント(脅威に関する情報、OPACL、および OPSig)のダウンロードと展開を行い、管理者が感染抑制デバイスへこれらの OMT コンポーネントを展開する方法や時期について管理できるようにします。Cisco ICS サーバ データベースには包括的なログが作成されます。このデータベースには、OPACL および OPSig の展開に関する情報だけでなく、感染抑制デバイスを通るトラフィック照合によって発生する照合関連情報も含まれます。これらのログを使用して、Cisco ICS サーバはリアルタイムの Syslog イベントおよび定期的なレポートを生成し、管理者がそれぞれの大規模感染に関するセキュリティ ポスチャを完全に理解できるようにします。また、Cisco ICS サーバは Trend Micro Damage Cleanup Service (DCS)と統合することにより、ウイルス感染した Windows エンドポイントを特定し、ネットワーク内の感染源を効率的に駆除します。

次に、Cisco ICS の主要な機能の一部について説明します。

OPACL のドロップ モードとログ モード

OPACL では、Cisco ICS チューニングを容易にし、より柔軟な展開を可能にするために、2 つの動作モードが設定されています。OPACL は、トラフィック照合が検出された際にパケットを廃棄するか、トラフィック照合を記録するだけで、トラフィック フローは中断しないかのいずれかで動作するよう、グローバルに設定できます。トラフィック照合の記録は、IPS 保障でのみ適用されます。この設定は、ACL 保障の対象となる感染抑制デバイスには使用できません。

OPACL の自動モードと手動モード

Cisco ICS サーバでは、ネットワークに悪影響を及ぼす潜在的な可能性を持つ OPACL の動作を管理者が詳細に制御できるようにするために、OPACL を 2 つのモードのいずれかで動作するように設定できる機能を実装しています。

- **自動モード:** OPACL は感染抑制デバイスに自動的にプッシュされるため、管理者が介入する必要はありません。このモードは、応答時間を最小限に短縮し、最も迅速に展開できる防御策です。
- **手動モード:** すべての OPACL は Cisco ICS サーバ上で保持されます。管理者は OPACL のアベイラビリティに関する通知を受け取り、OPACL を調査または編集してから、それらを感染抑制デバイスに手動でプッシュするかどうかを決めることができます。

OMT の集中的な設定

Cisco ICS サーバでは、すべての OMT を完全に制御できます。これにより、管理者は、新規または展開済みの OMT を変更したり、新しいカスタム OMT を作成したりできます。また、管理者は、OMT の影響を受けないプロトコルまたはポートについてのグローバルなルールを設定し、ミッションクリティカルなアプリケーションや機能が Cisco ICS の影響を受けないようにすることもできます。これらの機能は主に Cisco ICS サーバ内で実行され、個別の感染抑制デバイス、デバイスの論理グループ、または登録されているデバイス全体に展開されます。

デバイスの論理的な命名とグループ化

Cisco ICS サーバに感染抑制デバイスが登録されると、これらのデバイスに論理名、および論理グループへのメンバーシップを割り当てることができるようになります。これにより、管理者は、感染抑制デバイス グループをニーズに応じてカスタマイズし、ネットワーク トポロジ、機能、ロケーション、管理責任、またはその他の基準に基づいて整理することができます。

複数の同時 OMT

複数の大規模感染が同時に発生する可能性があります。そのため、Cisco ICS サーバは、複数の OMT (最大 32) を同時に処理できるように設計されています。

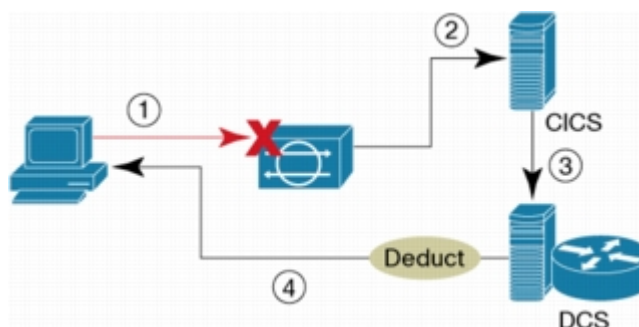
インシデントのリアルタイムでの追跡および監視

OMT を展開することにより、管理者は、あらゆる大規模感染に関するネットワーク上の対策の効果度を極めて柔軟に監視できるようになります。この柔軟な対応は、感染抑制デバイスに展開された OPACL と OPSig に対するトラフィック照合を監視することにより可能になります。Cisco ICS サーバは、統合型の強力なモニタリング ツールおよびレポート ツールを提供します。また、Syslog および Cisco Security Monitoring, Analysis and Response System (CS-MARS) 製品のサポートにより、管理者はモニタリング ツールおよび関連付けツールを選択して使用することもできます。

Trend Micro DCS との統合

OPACL と OPSig は、感染がネットワーク全体に侵入し伝播するのを防ぎますが、大規模感染防止サービスの展開時のすき間や予想外のエン트리 ポイントでの感染により、ネットワークがウイルスに感染する可能性は常にあります。このような可能性に対抗するために、管理者には内部の感染源を処理する手段が必要です。Cisco ICS サーバでは、OPSig を作成して対応する必要があるトラフィックを生成しているホストを記録および追跡できます。このデータベースは、トレンドマイクロ社の DCS で使用できます。Trend Micro DCS サーバを Cisco ICS サーバに登録することにより、DCS サービスを使用して、Cisco ICS が内部の感染源として識別した感染 Windows マシンを自動的にリモートで駆除できるようになります。図 2 に、DCS サーバと Cisco ICS サーバの統合を示します。

図 2 DCS の統合



1. ウイルス感染したコンピュータは、悪意のあるペイロードをネットワークに送信します。適切な OPSig が設定されている Cisco ICS 感染抑制デバイスでは、悪意のあるトラフィックが遮断されます。
2. Cisco ICS サーバは Security Device Event Exchange (SDEE) プロトコルを使用して感染抑制デバイスのログへのクエリーを行い、感染源の IP アドレスを特定します。さらに、Cisco ICS サーバは、この IP アドレスを感染したデバイスの Watch List データベースに追加します。
3. Cisco ICS サーバは、Trend Micro DCS サーバに Watch List データベース内のデバイスを通知し、感染したデバイスのリモート クリーンアップを起動させます。

4. トレンドマイクロ社の DCS サーバは、Damage Cleanup Engine (DCE) および Damage Cleanup Template (DCT) を感染源に送信し、対象となるマシン上でリモート クリーンアップを実行します。マシンのクリーンアップが完了すると、DCS は Cisco ICS サーバに通知し、Cisco ICS サーバは感染源の IP アドレスを Watch List から削除します。

Cisco ICS 向けのサービス: ICS の効率的な準備、計画、設計、導入、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(準備、計画、設計、実装、運用、および最適化)に対応する、各種の高度なサービスおよびテクニカル サポート サービスを提供しています。これらのサービス製品は、各段階を効果的に実行するために不可欠です。次に、これらのサービス製品について説明します。

Cisco ICS 向けの Technical Support Services *

シスコでは、お客様の社内リソースを補完し、シスコ製品の効率的な運用、ハイ アベイラビリティの維持、および最新のシステム ソフトウェアの利点を活用できるようにする、Technical Support Services (TSS) を提供しています。Cisco TSS のポートフォリオでは、Cisco SMARTnet[®] サポート、Software Application Support plus Upgrade (SASU)、および Cisco Services for IPS の 3 つのサービス プログラムを提供し、Cisco ICS の確実な準備および運用を可能にしています。

• Cisco SMARTnet サポート

Cisco SMARTnet サポートは、シスコ ネットワーキング製品のサポート要件に対応し、投資保護を実現します。Cisco IOS ソフトウェア リリース 12.3M がインストールされているスイッチやルータなど、ACL 保障対応デバイスの場合、Cisco SMARTnet サービスは、Cisco ICS 向けプレミアム サービスの前提条件であり、次のサービスを提供します。

- Cisco IOS ソフトウェアなどのシスコのオペレーティング システム更新への継続的なアクセス
- シスコのハードウェアおよびオペレーティング システム ソフトウェアの技術的問題を迅速に解決する Cisco Technical Assistance Center (TAC) へのアクセス(24 時間 365 日、世界中からアクセス可能)
- Cisco.com および技術情報の包括的なナレッジ ベースへのアクセス
- ハードウェアのアドバンス交換オプション(障害が発生したハードウェアを交換するフィールドエンジニアの有無は問わない)

• Cisco Services for IPS

Cisco Services for IPS を使用すると、Cisco SMARTnet サービスの内容を IPS シグニチャの入手と組み合わせて 1 つの包括的なサービス プログラムにすることができます。IPS 対応の感染抑制デバイスの場合、Cisco Services for IPS は、Cisco ICS 向けプレミアム サービスの前提条件であり、次のサービスを提供します。

- さまざまな脅威に対応した Cisco IPS シグニチャへの標準的なリリース間隔でのアクセス
- IPS v5.x などのオペレーティング システムのソフトウェア アップデートへのアクセス
- TAC へのアクセス(24 時間 365 日、世界中からアクセス可能)
- Cisco.com および技術情報の包括的なナレッジ ベースへのアクセス
- ハードウェアのアドバンス交換オプション(障害が発生したハードウェアを交換するフィールドエンジニアの有無は問わない)

• Cisco Software Application Support plus Upgrade

シスコ テクニカル サポート サービスのポートフォリオには、Cisco ICS サーバソフトウェアなどのアプリケーション ソフトウェアのサポート要件に対応し、投資保護を実現する Software Application Support plus Upgrades (SASU) が含まれています。SASU は次の機能を提供します。

- バグ修正、メンテナンス、マイナーおよびメジャー リリースなど、アプリケーション ソフトウェア アップデートへのアクセス
- シスコのアプリケーション ソフトウェアの技術的問題を迅速に解決する TAC へのアクセス (24 時間 365 日、世界中からアクセス可能)
- Cisco.com および技術情報の包括的なナレッジベースへのアクセス

表 5 に各プログラムのコンポーネントを示します。

表 5 Cisco ICS 向けのテクニカル サポート サービス

サポートするコンポーネント	Cisco SMARTnet サポート	Cisco Services for IPS	Cisco SASU
対象製品	IPS 機能を備えていない感染抑制デバイス	IPS 機能を備えた感染抑制デバイス	Cisco ICS サーバ ソフトウェア
シスコが作成したシグニチャ更新	—	○	—
オペレーティング システム更新へのアクセス	○	○	—
Cisco.com ナレッジベースへのアクセス	○	○	○
テクニカル サポートへのアクセス	○	○	○
ハードウェアのアドバンス交換オプション	○	○	—

* Cisco ICS の前提条件として、すべての感染抑制デバイスには、Cisco SMARTnet サポート契約または Cisco Services for IPS 契約が適用されている必要があります。ACL 保障の対象となるデバイスには、有効な Cisco SMARTnet 契約が適用されている必要があります。IPS 保障の対象となるデバイスまたはモジュールには、有効な Cisco Services for IPS 契約が適用されている必要があります。

まとめ

Cisco ICS ソリューションを使用すると、ワームおよびウイルスに対する免疫機能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り、ワームとウイルスの蔓延を防ぎ、ネットワーク アベイラビリティを保証しながら、障害復旧にかかるコストを削減できます。Cisco ICS は、Cisco Services for IPS の重要な付加機能です。Cisco ICS ソリューションは、シスコのネットワーキング デバイスで構成されたあらゆる規模のインフラストラクチャに適用でき、新たな大規模感染に対する迅速な対応に重点を置いた、新しい保護レイヤを提供します。

©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

お問い合わせ先