

Cisco Incident Control System

Q. Cisco Incident Control System とは何ですか。

A. Cisco[®] Incident Control System (ICS) は、ネットワークが新しいウイルスやワームに感染する前に、それらの脅威に対処し、防止できるようにするソリューションです。ICS は、新たな大規模感染に迅速に対応することで、さまざまなシスコ製デバイスが新たな脅威に対する感染抑制ポイントとして機能できるようにします。

Q. 具体的には、Cisco ICS はこの機能をどのように実現するのですか。

A. Cisco ICS は、トレンドマイクロ社のトレンドラボへの直接リンクを使用することで、この機能を実現します。トレンドラボにおいて、ICS は悪意のあるソフトウェアの新たな脅威に対する警告を早期に取得し、迅速な対応を可能にする感染抑制ポリシーを取得して、それらをシスコのインフラストラクチャ デバイスにプッシュします。これにより、シスコ製デバイスが新たな脅威に対する感染抑制ポイントとして機能できるようにします。

Q. Cisco ICS の主要なコンポーネントは何ですか。

A. Cisco ICS は、Cisco ICS サーバ ソフトウェア、およびさまざまなインフラストラクチャ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。

Q. Cisco ICS サーバとは何ですか。

A. Cisco ICS サーバは、Cisco ICS に固有の機能の管理と配信を行う管理センターです。Cisco ICS サーバは、Access Control List (ACL; アクセス コントロール リスト) および Intrusion Prevention System (IPS; 侵入防御システム) プロビジョニングのための管理プラットフォームまたはデバイス マネージャとして機能するには設計されていません。Cisco ICS サーバの機能は、Cisco ICS に関連する機能に限定されています。

Q. 感染抑制デバイスとは何ですか。

A. 感染抑制デバイスとは、シスコのネットワークング デバイスまたはセキュリティ デバイスです。これらのデバイスは、Cisco ICS 保障の対象となることにより、新たな大規模感染に対する防御ポイントとして機能することができるようになります。感染抑制デバイスには、現在主流の Cisco IOS[®] ソフトウェアベースのルータおよびスイッチから、Cisco IPS 4200 シリーズ センサ、Catalyst[®] スイッチ用 IDSM2 ブレード、Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス、サービス統合型ルータなどの IPS 対応シスコ製品まで、さまざまなデバイスがあります。

Q. 感染抑制デバイスのライセンスとは何ですか。

A. 感染抑制デバイスのライセンスとは、購入したうえで Cisco ICS ソフトウェアにインストールする必要がある年間ライセンスです。このライセンスにより、感染抑制デバイスが Cisco ICS 保障の対象となります。保障の対象となる感染抑制デバイスごとに、ライセンスが必要です。

Q. すべての定期的なシグニチャ更新を入手可能になった直後にインストールしている場合でも、なぜ Cisco ICS が必要になるのですか。

A. Cisco ICS を使用すると、新たな脅威に迅速に対応し、ネットワークに感染が広がる可能性を最初の時点で大幅に軽減できます。標準のシグニチャ更新は、大規模感染防止ストラテジにとって重要ですが、開発と配信が必要なため、Cisco ICS が提供する更新よりも時間がかかります。

Q. Cisco ICS と Cisco Services for IPS 製品の違いは何ですか。

A. Cisco ICS は、Cisco Services for IPS の重要な付加機能で、シスコのプレミアム クラスの製品です。Cisco ICS は、大規模感染に対応するための新たな標準を業界に提供します。Cisco ICS は、状況に応じて、ネットワーク全体を保護するさまざまな感染抑制デバイスに、ほぼリアルタイムでの更新を提供します。Cisco Services for IPS は、大規模感染防止ストラテジの重要なコンポーネントであり、さまざまな Cisco IPS 対応製品にシグニチャ更新をタイムリーに提供します。これにより、Cisco IPS 対応製品で使用される保護プロファイルの定期的な更新が可能になります。

Q. Cisco ICS では、異なるタイプの保障を提供していますか。それはどのような保障ですか。

A. Cisco ICS では、ACL 保障と IPS 保障の 2 つのタイプの保障を使用できます。ACL 保障は、標準(セキュリティ イメージなし)の Cisco IOS ソフトウェアを実行するルータやスイッチなど、IPS 機能を持たないデバイス用です。これらのデバイスは、低密度の Outbreak Prevention ACL(OPACL)のみを受信します。IPS 保障は、Cisco IPS 4200 シリーズ センサ、SSM-AIP モジュールを搭載した Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、IDSM2 を搭載した Catalyst 6500 モジュール、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ルータなど、ロード可能なシグニチャ IPS 機能を備えたデバイス用です。これらのデバイスは、OPACL と Outbreak Prevention Signature(OPSig)の両方を受信します。

Q. OPACL とは何ですか。

A. OPACL は、Cisco ICS によって感染抑制デバイスに導入される、最初の時点での迅速な対応策です。OPACL は、新たに検出された脅威を遮断するための広範囲かつ低密度の ACL またはシグニチャの形式で提供されます。OPACL は、OPSig の開発とテストを行う間に迅速に配信することに重点を置いています。

Q. OPSig とは何ですか。

A. OPSig は、Cisco ICS によって感染抑制デバイスに導入される、2 番目の迅速な対応策です。OPSig は、新たに検出された脅威を遮断するための高性能かつ限定的なシグニチャの形式で提供され、正確性に重点を置いています。このシグニチャは、OPACL の受信直後に感染抑制デバイスで利用できるようになり、検出された大規模感染に対して最終的かつ永続的な保護を提供します。

Q. すべての感染抑制デバイスが、Cisco ICS の一部として OPACL を受信できますか。

A. はい。ACL 保障デバイスと IPS 保障デバイスの両方が、OPACL を受信できます。

Q. すべての感染抑制デバイスが、Cisco ICS サービスの一部として OPSig を受信できますか。

A. いいえ。OPSig を受信できるのは、IPS 保障デバイスだけです。

Q. OPACL と OPSig の一般的な応答時間と目標の応答時間は、どのようになっていますか。

A. トレンドラボは、OPACL と OPSig を配信する際の応答時間を着実に改善しています。一般的な応答時間は、OPACL では 15 分、OPSig では 90 分です。規定の目標応答時間は、OPACL では 30 分、OPSig では 150 分です。

Q. Cisco ICS サーバがネットワーク上の ACL を自動的に変更するという考え方に不安があります。ポリシー展開を自分でどの程度制御できますか。

A. Cisco ICS サーバでは、OPACL を手動で展開できます。このモードでは、Cisco ICS サーバで OPACL が入手できるようになると、管理者に自動的に通知が送信されます。管理者は、ACL を検査または変更することができ、目的の感染抑制デバイスだけに手動で展開することもできます。

Q. Cisco ICS を導入するには、どのコンポーネントを発注する必要がありますか。

A. Cisco ICS サーバ ソフトウェア、および感染抑制デバイスに必要な数のライセンスを発注する必要があります。表 1 に、発注可能なシスコの製品番号を示します。

表 1 製品番号

製品番号	説明
ICS-SVR-V10-K9	Cisco Incident Control Server Software v1.0
ICS-LIC-IPS-HE-1	ICS ライセンス:ハイエンド デバイス用 IPS サービス × 1
ICS-LIC-IPS-LE-5	ICS ライセンス:ローエンド デバイス用 IPS サービス × 5
ICS-LIC-ACL-25	ICS ライセンス:ACL サービス × 25
ICS-EVAL-K9	ICS 60 日間評価キット(ICS SW、ACL × 25、IPS-LE × 5、IPS-HE × 1)

前提条件として、IPS 対応のすべての感染抑制デバイスに有効な Cisco Services for IPS SMARTnet[®] サービス契約が適用されていることも確認してください。

Q. バンドルに含まれているライセンスの一部が不要な場合は、どうすればいいですか。すべてのライセンスを同時に有効にする必要はありますか。

A. いいえ。利便性を考慮し、Cisco ICS ライセンスは登録時に部分的に実行できます。つまり、購入したライセンスをすべて有効にする必要はありません。必要なときに残りのライセンスを有効にできます。

Q. Cisco ICS を導入するために必要なその他の機器には、どのようなものがありますか。

A. Cisco ICS サーバをインストールするには、Windows ベースのサーバ プラットフォームが必要です。Cisco ICS 保障を展開するための 1 つ以上の感染抑制デバイスも必要です(表 2 を参照)。

表 2 サポートされる感染抑制デバイスのタイプと最小限必要なソフトウェア

感染抑制デバイス
Cisco IPS 4200 シリーズ センサ(ソフトウェア v5.1 以上を使用) *
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 カード搭載、ソフトウェア v5.1 以上を使用) *
Catalyst 6500 用 Cisco IDSM2 センサ ブレード(ソフトウェア v5.1 以上を使用) *
シスコ ルータ(Cisco IOS セキュリティイメージ ソフトウェア リリース 12.4(4)T 以上を使用) *
シスコ ルータ(Cisco IOS ソフトウェア リリース 12.3M 以上を使用)
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 以上を使用)
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 以上を使用)
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 以上を使用)

* これらのデバイスには、有効な Cisco Services for IPS SMARTnet サービス契約も必要です。Cisco Services for IPS 契約がない場合、これらの製品は OPSig を処理できません。

表 3 に、ICS サーバ ソフトウェアの最小システム要件を示します。

表 3 ICS サーバ の最小システム要件

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

オペレーティング システム
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 v5.5 SP2

Q. Cisco ICS サーバと Cisco ICS を導入する場合、トレンドマイクロ社に何か発注する必要がありますか。

A. いいえ。すべてのソリューションをシスコから入手できます。

Q. 感染抑制デバイスを Cisco ICS 保障に対応させるために必要な準備はありますか。

A. はい。IPS 保障の対象となる、ロード可能な IPS シグニチャ機能を備えた感染抑制デバイスには、前提条件として、有効な Cisco Services for IPS SMARTnet サービス契約が適用されている必要があります。ACL 保障の対象となる感染抑制デバイスには、前提条件として、有効な SMARTnet サービス契約が適用されている必要があります。

Q. 感染抑制デバイスで実行する必要がある、最小限必要なソフトウェア リビジョンはありますか。

A. はい。感染抑制デバイスでは、Cisco ICS のサポート、および Cisco ICS サーバとの通信機能を含む、最小限必要なソフトウェア バージョンが実行されている必要があります。表 2 に、感染抑制デバイスのタイプまたはファミリごとに最小限必要なソフトウェアのバージョンを示しています。表 4 に、特定の感染抑制デバイスごとに最小限必要なソフトウェアのバージョンを示しています。

Q. 発注する際、Cisco ICS 感染抑制デバイスのライセンスのタイプは、どのように確認できますか。

A. Cisco ICS 感染抑制デバイスのライセンスは、感染抑制デバイスの機能とスループットに基づいて分類されており、便利なバンドルとして入手できます。そのため、使用する感染抑制デバイスとその数量を決定し、表 4 に従って、必要なライセンスのタイプを発注するだけで済みます。

表 4 互換性のあるデバイス、必要なソフトウェアのバージョン、ライセンスのタイプ、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	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)	SMARTnet または同等のパートナー サポート プログラム
	Cisco 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 と 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	IPS v5.1		
	Cisco IPS 4240 センサ	IPS v5.1		
	Cisco IPS 4250 センサ	IPS 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	必要なサービス契約
	Cisco IPS 4250 XL センサ	IPS v5.1		
	Cisco IPS 4255 センサ	IPS v5.1		
	Cisco IDSM2 Catalyst モジュール	IPS 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)	ASA v7.0/IPS v5.1		
	Cisco IPS 4215 センサ	IPS 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)	ASA v7.0/IPS 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、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		

- Q. Cisco ICS では、どのようなスケーラビリティ テストが行われましたか。その結果、推奨事項はどのようになっていますか。**
- A.** 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シスコのラボで検証されています。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。ICS 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。
- Q. 感染抑制デバイスのライセンスは更新が必要ですか。頻度はどれくらいですか。**
- A.** はい。感染抑制デバイスのライセンスは、1 年間有効です。ただし、利便性とライセンス管理の簡素化のため、すべてのライセンスは、3 月 31 日、6 月 30 日、9 月 30 日、および 12 月 31 日のいずれかの日に失効します。ライセンスはシスコへの製品登録時に初期化され、失効日は、登録日から最低 12 か月後となります。また、感染抑制デバイスのライセンス更新の一部として、対象となる感染抑制デバイスの SMARTnet または Cisco Services for IPS 契約も更新する必要があります。
- Q. Cisco ICS サーバは、トレンドラボの ActiveUpdate(AU)サーバとのコミュニケーションにどのようなメカニズムおよびプロトコルを使用していますか。**
- A.** Cisco ICS サーバは HTTPS を使用して、トレンドラボの AU サーバから情報のポーリングとダウンロードを行います。このコミュニケーションは、常に Cisco ICS サーバからトレンドラボの AU サーバへのアウトバウンド接続になります。

- Q. Cisco ICS とトレンドラボの AU サーバは、どのくらいの頻度でコミュニケーションを行っていますか。**
- A. Cisco ICS サーバがトレンドラボの AU サーバにポーリングする頻度は、デフォルトでは 5 分ごとになっていますが、このパラメータは Cisco ICS サーバのユーザ インターフェイスで設定変更できます。**
- Q. Cisco ICS サーバがトレンドラボの AU サーバとコミュニケーションを行えるようにするためには、特別な処理が必要ですか。**
- A. Cisco ICS サーバからトレンドラボの AU サーバへのアウトバウンド接続がファイアウォールを通過できるようにするには、ファイアウォール設定の変更が必要になる場合があります。**
- Q. Cisco ICS サーバは、感染抑制デバイスとのコミュニケーションにどのようなメカニズムおよびプロトコルを使用していますか。**
- A. 感染抑制デバイスによって異なります。ACL 保障の場合、Cisco ICS サーバは Secure Shell (SSH) プロトコルを使用します。IPS 保障の場合、Cisco ICS サーバは HTTPS を使用して OPACL および OPSig を展開し、Security Device Event Exchange (SDEE) を使用してイベント ログへのクエリーを行います。**
- Q. ネットワークへの感染の可能性が高くなった場合でも、中断できないミッションクリティカルなアプリケーションを稼働しています。Cisco ICS では、このようなシナリオに対応できますか。**
- A. はい。Cisco ICS サーバでは、OPACL の影響を受けないポートまたはプロトコルをグローバルに設定することが可能です。**
- Q. Trend Micro Damage Cleanup Service (DCS) とは何ですか。**
- A. Trend Micro DCS はトレンドマイクロ社が提供する製品で、Cisco ICS と統合して、Windows ベース マシンの感染除去を行います。DCS サービスでは、Cisco ICS から取得された情報を使用して、感染したマシンを特定し、クリーンアップの対象とします。詳細については、トレンドマイクロ社またはトレンドマイクロ社認定リセラーにお問い合わせください。**
- Q. ネットワークを Cisco ICS 保障に対応させるために必要な準備はありますか。**
- A. はい。ネットワークを Cisco ICS に対応させるには、シスコのサービス ポートフォリオを考慮する必要があります。シスコのサービス ポートフォリオでは、ネットワークのライフサイクルの各段階に対応した、反応型かつ予防的なコンサルティング サービスを広範囲にわたって提供しています。**
- ICS ソリューションの導入後、シスコではテクニカル サポート サービスを提供します。これにより、シスコ製品が効率的に稼働し、ハイ アベイラビリティを維持し、最新のシステム ソフトウェアの利点を最大限に活用できるようにします。
- シスコのサービスおよびサポートについての詳細は、<http://www.cisco.com/jp/services/> を参照してください。
- Q. 感染抑制デバイスを Cisco ICS に対応させる場合、どのテクニカル サポート サービスを参照すればよいですか。**
- A. 感染抑制デバイスの前提条件となっているシスコ テクニカル サポート サービスは、Cisco SMARTnet サービスおよび Cisco Services for IPS です。Cisco ICS を導入する前に、適用対象となる感染抑制デバイス用に、これらのサービスを購入しておく必要があります。**

Q. Cisco Services for IPS とは何ですか。

A. Cisco Services for IPS は、シスコの自己防衛型ネットワーク ストラテジに不可欠のコンポーネントであり、シスコ テクニカル サポート サービス ポートフォリオの重要な要素です。また、Cisco IPS 対応の感染抑制デバイスに標準的なリリース間隔でタイムリーな情報およびシグニチャ ファイル更新を配信することにより、包括的なサポートとして機能します。Cisco Services for IPS を使用すると、IPS 対応の感染抑制デバイスが最新の脅威に常に対応できる状態を維持し、悪意のある、または有害なトラフィックを正確に識別および分類し、リアルタイムで阻止できるようになります。

Q. Cisco Services for IPS を購入すると、どのようなサービスを受けられますか。

A. 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
- 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)

このサービスについての詳細は、次の URL を参照してください。

<http://www.cisco.com/jp/services/portfolio/tss/ips.shtml>

Q. Cisco SMARTnet サービスとは何ですか。

A. 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、シスコ ネットワーキング製品のサポート要件に対応し、投資保護を実現する、Cisco SMARTnet サービスが含まれています。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 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 SMARTnet サービスについての詳細は、次の URL を参照してください。

<http://www.cisco.com/jp/services/portfolio/tss/snt.shtml>

Q. Software Application Support plus Upgrades とは何ですか。

A. 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

SASU についての詳細は、次の URL を参照してください。

<http://www.cisco.com/jp/services/portfolio/tss/sas.shtml>

表 5 に、Cisco SMARTnet サービス、Cisco Services、および SASU のサポート内容を示します。

表 5 Cisco SMARTnet サービス、Cisco Services、および SASU のサポート内容

サポート内容	Cisco SMARTnet サービス	Cisco Services for IPS	SASU
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	○	○	–
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	ICS サーバ

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、シスコ テクノロジーへの投資を保護できるように設計されたさまざまなサービスが含まれています。これらを活用することにより、お客様はシスコの感染抑制デバイス、オペレーティング システム ソフトウェア、およびアプリケーション ソフトウェアの運用ライフサイクルを延長し、強化できます。

テクニカル サポート サービスについての詳細は、次の URL を参照してください。

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

©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