

Cisco CRS-1 のセキュリティ

Cisco® キャリア ルーティング システムおよび、それに搭載された分散型モジュラ式の Cisco IOS® XR ソフトウェアのマイクロカーネル アーキテクチャを使用すると、アクセス制御、および管理、制御、データの各プレーン間におけるプロセス分離という内蔵セキュリティ制御機能を介して高セキュリティな常時稼働のシステムを実現します。

サービス プロバイダーの収益拡大に対する脅威

サービス プロバイダーにとって、ネットワーク セキュリティはビジネスの存続にもかかわる問題です。ウィルス、侵入、オペレータの誤操作、およびソフトウェアの誤設定によりセキュリティ問題が発生すると、必然的にサービスの中断、財務上の損失、お客様の不満、生産性の低下といった結果を招き、メディアの注目を集めることさえあります。また、それに伴う損益も膨大となります。サービス プロバイダーは収益を守るために、インフラストラクチャを保護し、安全な接続、セキュリティを脅かす問題の阻止、エンドポイント保護を提供できるマネージド サービスを整備する必要があります。

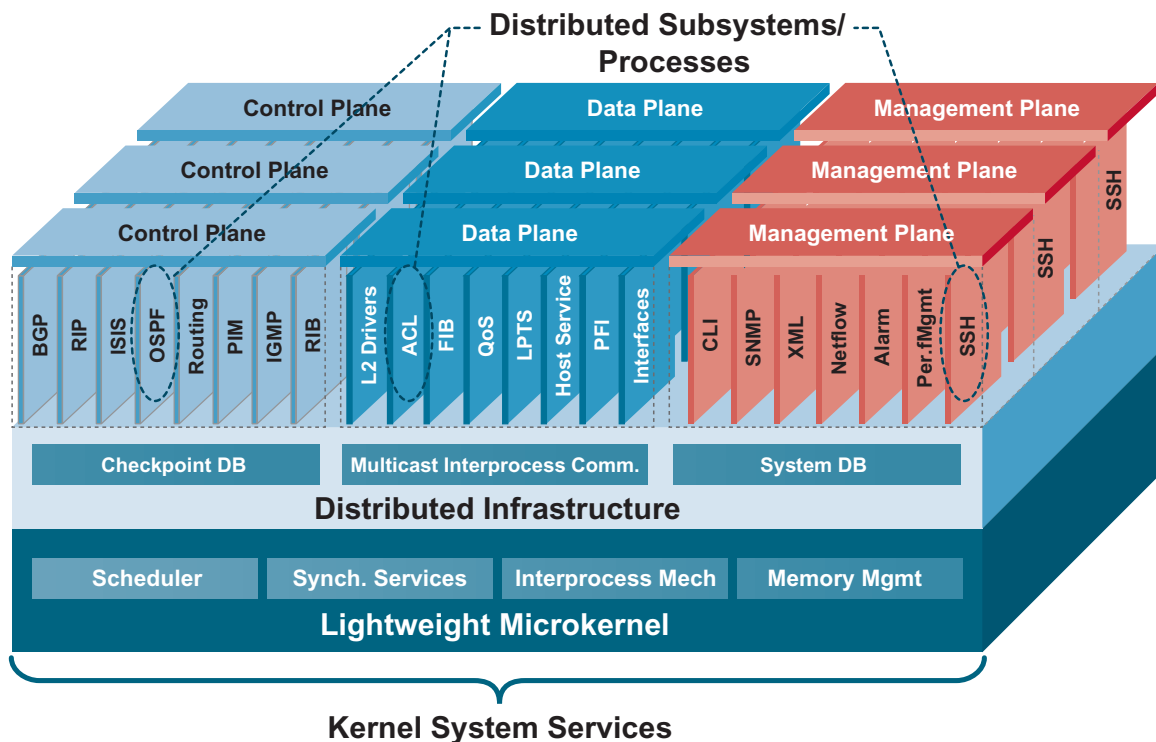
セキュリティへの脅威（Distributed-DoS[分散 DoS] 攻撃など）がますます増加し、ポリシーが複雑になっていく環境においてハイ アベイラビリティを維持するために、サービス プロバイダーは新たな自己防衛型のネットワークを実現できるルーティングおよびスイッチング ソリューションを模索しています。つまり、内蔵型でハードウェアベースのセキュリティ制御機能を備えたソリューションが必要とされています。新たな常時稼働のシステムがこれらの今までにない高セキュリティ ソリューションを実現するためには以下の項目をサポートする必要があります。

- サービスの分離、障害の隔離、およびメモリの保護
- シームレスなソフトウェアとハードウェアの回復
- コンフィギュレーションと管理の保護
- 障害を予測し、かつ迅速な対処

Cisco キャリア ルーティング システム

Cisco Carrier Routing System (CRS-1; キャリア ルーティング システム -1) は、モジュラ式の分散型マイクロカーネル オペレーティング システム、Cisco IOS XR を基盤としたマルチシェルフ ルーティング プラットフォームです (図 1 を参照)。

図 1
Cisco IOS XR ソフトウェアのアーキテクチャ



Cisco Systems[®]の開発チームは、長年に渡る、Cisco IOS ソフトウェアでのインターネットセキュリティにおける経験を活用して、CRS-1 を設計しました。Cisco IOS XR ソフトウェアのモジュラ式で、物理的にも論理的にも分散されたアーキテクチャ (図 1) を使用すると、アベイラビリティの高い安全なルーティングプラットフォームとネットワークを構築するための数々の利点を享受することができます。個々のソフトウェアコンポーネント (サブシステム) は、専用の保護されたメモリアドレススペースで稼働する個別のソフトウェアプロセスとして実装されます。これにより、1つのサブシステム上で障害が発生しても、ほかのサブシステムへの悪影響を防ぐことができるため、実際にセキュリティ問題が発生しても障害を隔離し、ほかの部分から区分できます。

FreeBSD UNIX などのモノリシックなカーネルアーキテクチャとは異なり、TCP などのネットワークスタックはマイクロカーネル外部の個別のプロセスとして稼働します。したがって、TCP スタックに障害が発生した場合でも、システムの稼働は継続されます。サービスを再開する際には、人手を煩わせることなく、関連するプロセスが自動的に再起動されます。さらに、モジュラ式のソフトウェアアーキテクチャと In-Service Software Upgrade (ISSU; サービス稼働中のソフトウェアアップグレード) 機能を使用して、たとえば、システム全体のリロードを実行せずに、パッチをすばやくインストールできます。

Cisco IOS XR ソフトウェア内での高度な障害の隔離とセキュリティ制御機能の実装は、3つのプレーンにまたがる論理的なプロセス分散に基づいています。各プレーンは、安全なネットワーク運用を行うための専用のアクセス制御を備えています。

- 制御プレーン
- データプレーン
- 管理プレーン

制御プレーンの保護

制御プレーンでは、すべてのルーティング制御情報が交換されるため、制御プレーンおよびそのコンポーネントが攻撃対象になることがあります。制御プレーンの回復力は、CPU の処理性能とスケーラビリティに依存するため、CPU に対して「out-of-resources」攻撃が仕掛けられることも珍しくありません。

スケーラビリティとパフォーマンスをサポートするために、CRS-1 制御プレーンの設計では、Symmetric MultiProcessing (SMP; 対称型マルチプロセッシング) CPU を使用する分散型の冗長ルート プロセッサが採用されています。正常な動作時には、CRS-1 の転送トラフィックは内蔵のラインカードによってワイヤレートで処理されます。ただし、パケットがルータ自身に転送される場合は例外です。これらの「パントされたパケット」には、ルーティングプロトコル、Internet Control Message Protocol (ICMP)、ネットワーク管理パケットが含まれており、ラインカードパケットプロセッサから、ラインカードCPUまたはルートプロセッサCPUのどちらかへ転送されます。

オープンな環境で制御プレーンを DoS 攻撃から守るために、ラインカードおよびパケットプロセッサには、複数の階層化されたセキュリティ機能が分散されています。これらの機能には、次のものがあります。

- Dynamic Control Plane Protection (DCPP; ダイナミック制御プレーン保護)
- 自動制御プレーン輻輳フィルタ
- 制御プレーン Time-to-Live(TTL)サニティチェック (RFC 3682、Generalized TTL Security Mechanism[GTSM])
- Border Gateway Protocol (BGP)によるルーティングプロトコルのフィルタリングとRoute Policy Language (RPL)

ダイナミック制御プレーン保護

侵入者がネットワークトラフィックの迂回や分析を行ってセキュリティを侵害した場合、未許可の、または悪意を持つルーティングアップデートが意図的に作成され、ネットワークセキュリティが危険にさらされることがあります。スプーフィングを回避する方法としては、Message Digest Algorithm 5 (MD5) を使用して近接ルータの認証を実装する手法が一般的です。これにより、ルータが信頼された送信元から信頼できる情報を受信できるようになります。ただし、これは単なる第 1 ステップにすぎません。偽装された BGP パケットがルータ方向へばら撒かれ始めると、これらのパケットの進行方向は、受信パス Access Control List (ACL; アクセス制御リスト) と Modular QoS CLI (MQC) レート制限機能によって厳密に制御されます。ただし、ACL と MQC の制御は自動的に実行されません。BGP ピアがダウンする、または再起動した場合には、セッションが再確立されるたびに、レイヤ 4 ポート番号が変わります。そのため、ネットワーク設計者は、設定済みの BGP ピアリングセッションは許可し、未設定のセッションは廃棄できる、自動化された動的な手法を探し求めてきました。

この要求に応え、CRS-1 では、ラインカードパケット処理用に DCPP 方式が搭載されています。DCPP を使用すると、明示的に設定された BGP ピアリングセッションには自動的に十分なリソースが割り当てられる一方、未設定のセッションは拒否されるか最低限の処理だけが実行されます。この許可/拒否モデルは、静的に設定された IP アドレスと動的なレイヤ 4 ポート番号の関連付けに基づいています。アドミッション制御を最大限活用できる認証と確立が実現される以前は、初期接続に関するさまざまなリソースポリシーが存在していました。制御プレーンパケットは、内部検索テーブルによって許可され、十分なリソースが割り当てられるまで、複数階層からなる事前スクリーニング方式の各階層を経由する必要がありました。このプロセスの自動化が実現されたことにより、ネットワーク管理者は手動設定に費やしていた時間をそのほかのミッションクリティカルなタスクに使用できるようになります。

自動制御プレーン輻輳フィルタ

ラインカードの負荷が CRS-1 スロットのキャパシティを超えてしまうほど極度な DoS または DDoS 攻撃を受けると、制御メカニズムは、ラインカードのキャパシティを上回るハードウェア Application-Specific Integrated Circuit (ASIC; 特定用途向け IC) レートで稼働し、パケットをレイヤ 3 Modular Services Card (MSC) 上の Silicon Packet Processor (SPP; シリコンパケットプロセッサ) へ転送し、制御プレーンのパケット処理が優先されるように保証します。この機能によりトポロジーが維持されている間に、ネットワーク管理者はそのほかのセキュリティツールを使用して問題を解決するための移行方式をインストールできます。

制御プレーン TTL サニティ チェック (RFC 3682、GTSM)

制御プロトコルのピアリング セッションの大半は、隣接ルータまたは直接接続されたルータとの間で確立されます。GTSM (以前は、BGP TTL Security Hack[BTSH] と呼ばれた) が開発されるまでは、方向性を持たないピアリング ポイントからルータへ向けて転送された BGP パケットは、ルータ CPU によって処理する必要がありました。これらのパケットが大量に生成されると、事実上、大規模な DDoS 攻撃を受けた場合と同様に CPU リソースが使い果たされてしまいました。今では、GTSM を使用し、BGP ピアリング パケットの TTL をチェックすることで、方向性を持たないすべての BGP スプーフィングを MSC SPP 内で効果的に阻止できます。

これらの技術は、汎用的な GTSM の機能を利用できる Label Distribution Protocol (LDP) や Resource Reservation Protocol (RSVP) などのそのほかの多数のアプリケーションにも適用されることがあります。CRS-1 内の MSC アーキテクチャは完全にプログラム可能なため、そのほかのアプリケーション プロトコルに対応する GTSM サポートも簡単に MSC に追加できます。

BGP ルーティング プロトコル フィルタリングと RPL

BGP は、インターネットのもっとも基本的なルーティング プロトコルの 1 つです。残念ながら、適切なプレフィクスフィルタリングが実装されていない状態で BGP が攻撃を受けると、トラフィック「ガベージ」(不要データ) がインターネット全体にフラディングされてしまうことがあります。そのため、プレフィクスフィルタリングの使用が、長年の間、サービス プロバイダーのベスト プラクティスの 1 つとなってきました。詳細については、<http://www.ispbook.com> を参照してください。

しかし、ルーティング ポリシーがますます複雑になり、各ピアリング ルータが通信する必要のあるピアの数が増えるにつれ、問題なくプレフィクスフィルタリングを実装するのが困難になってきました。これに対処するため、シスコは RPL を採用し、Cisco IOS XR ソフトウェアに統合しました。大規模なルーティング コンフィギュレーションをサポートしようとする取り組みの中で開発された RPL には、従来のルートマップや ACL/プレフィクスリスト指向のコンフィギュレーションで見られる機能に拡張を加えたいくつかの基本機能があります。

第 1 の拡張機能として、共通のポリシーブロックを定義し、独立して管理できるようにするモジュラ方式のポリシー作成機能があります。これらの共通のブロックは、完全なポリシーを作成するためにほかのポリシーブロックに適用することが可能であり、このため管理する設定情報の量を削減できます。さらに、これらの共通のポリシーブロックにはパラメータを設定できます。これにより、同じ構造を共有し設定または比較する特定の値が異なるポリシーを作成し、独立したポリシー ブロックとして維持できます。たとえば、ローカルプリファレンス値以外は同一の 3 つのポリシーを、ポリシーのパラメータに応じてローカルプリファレンス値のみが異なる単一の共通ポリシーとして表すことができます。

また、RPL ではセットのコンセプトも導入されています。セットとは、ルート属性の比較操作や設定操作で利用できる類似データのコンテナです。プレフィクスセット、コミュニティセット、AS パスセット、拡張コミュニティセットなど、対応するグループを保持するさまざまなセット タイプがあります。これらのセットは、従来の Cisco IOS ソフトウェア設定で使用されているプレフィクスリスト、コミュニティリスト、AS パスリスト、拡張コミュニティリストに非常に似ていますが、1 点だけ重要な例外があります。それは、対応する Cisco IOS ソフトウェアには存在する「受け入れ」と「拒否」のコンセプトがセットには含まれていない点です。セットは、単なるデータのコンテナにすぎません。また、大半のセットには、完全にインラインで指定された少数のデータ値のみを比較することができるインライン版があります。したがって、少数のデータ値を比較するために、わざわざ数個の値しか含まない特定の名前付きセットを参照する必要はありません。

ルートを受け入れるか廃棄するかといった意思決定は、ポリシー定義によって明示的に制御されます。RPL を使用すると、ユーザは比較演算子 (セットのデータを使用することもある) と従来のブーリアン論理演算子 (「and」、「or」、「not」) を組み合わせ、複雑な条件式を作成できます。比較操作はすべて、結果として真 (true) または偽 (false) のどちらかを返します。また、ユーザが指定した単純な「if-then, else-if, else」構造を使用して、これらの条件式と関連するアクションの実行を制御できます。つまり、完全にユーザ設定可能なポリシーを使用して評価することができます。

RPL の導入によって、ピアリング ポリシーは現在のルートマップベースのピアリング ステートメントに比べ、さらにモジュラ化され、より効率的になると期待されています。RPL により、CRS-1 が実現する単一のマルチシェルフ ルーティング システムから、数千のピア間でピアリングを作成するために必要な今までにない高スケーラビリティの提供が可能になります。

データ プレーンの保護

データ プレーンは、ネットワーク エLEMENT 間でネットワーク データを受信し、処理を行い、送信します。これらは、ルータへ転送され、また、通過するネットワーク トラフィックの大部分に相当します。CRS-1 転送エンジンには、CRS-1 データ プレーンのトラフィックを既知の攻撃から保護するために多数のサニティチェック（これらはインターネット コミュニティについて収集された豊富な知識に基づいて決定された内容）がデフォルトで組み込まれています。さらに、CRS-1 では、ACL、Unicast Reverse Path Forwarding (uRPF)、MSC 上で専用の入出力処理が実行される NetFlow アカウンティングなどの機能とツールが提供されています。

- **ACL** — ACL は、IPv4 および IPv6 の両方で、多数のルータ データ プレーン アプリケーション（パケット分類、レート制限、統計情報とアカウンティング、パケットの permit/deny 演算子など）の重要なエレメントとなっています。

Cisco CRS-1 は、ネットワーク負荷が高い状態でもラインレートで ACL を処理できるように、もっとも厳しい条件を想定したパフォーマンスとスケーラビリティの要件を満たせるよう設計されています。たとえば、200 万のルートと 500 の BGP ピアがある場合、CRS-1 はパフォーマンスを劣化させることなく数千の ACL とそれらのエンタリを処理できます。

- **uRPF** — 検証可能な IP 送信元アドレスが欠落している IP パケットを廃棄すると、不正な形式または偽装された IP 送信元アドレスがネットワークに流入することがあります。Cisco CRS-1 は、これによって引き起こされる問題を軽減するために、uRPF（ストリクト モードとルーズ モード）をサポートしています。uRPF ストリクト モードがインターフェイス上で有効な場合、すべての受信パケットを調べ、送信元アドレスとインターフェイスがルーティング テーブルに登録されており、パケットを受信したインターフェイスが合致することを確認します。

uRPF ルーズ モードは、サービスプロバイダーのコミュニティで広く使用されているトリガードブラック ホールフィルタリング技術の基礎となっています。ルーズ モードでは、uRPF が、送信元 IP アドレスに基づいて DoS および DDoS 攻撃のパケットを効果的に廃棄し、非常に短時間で数千のルータへその方式を伝えます。

- **NetFlow** — アカウンティングは、トラフィック エンジニアリング、ネットワーク管理、課金といった分野でのネットワーク管理に必要不可欠な部分です。本来アカウンティング アプリケーションである NetFlow は、個々のパケット ヘッダーの内部を調べ、パケットをトラフィック クラスに集約し、各トラフィック クラスの統計情報と詳細なルーティング情報を収集するメカニズムを備えています。Cisco IOS XR ソフトウェア内に実装された NetFlow の統計情報は、貴重なデータベースを構成します。このデータベースは、トラフィック エンジニアリングとセキュリティ分析に使用でき、微細なレベルのネットワーク トラフィックであっても、その動作をキャプチャできます。

- **スタティック NetFlow とパケット スニフィング** — Cisco IOS XR ソフトウェアは、NetFlow を上回る機能を提供するスタティック NetFlow もサポートしています。NetFlow が動的であるのに対し、スタティック NetFlow は ACL がデータ パケットを処理するのと同じ方法でパケット フローを処理します。ただし、処理する際には、宛先または宛先自律システム番号、Multiprotocol Label Switching (MPLS) ラベルなどの拡張フィールドを使用します。スタティック NetFlow では、拡張 ACL を使用してフローフィルタを定義し、特定のフローのパケット カウンタまたはバイト カウンタを追跡できます。大量の NetFlow データを拡張 ACL に関連付けることができるため、オペレータは目的とするフローを正確に取り出し、それを対象にして、DoS と DDoS 攻撃を防御するための効果的なツールを作成できます。

Cisco IOS XR スタティック NetFlow から派生した帯域内パケット スニフィングは、ACL 同様のフィルタリングなど、スタティック NetFlow と同じ機能を使用しますが、サンプルを収集して設定済みの宛先へそれらを転送することができます。

管理プレーンの保護

管理プレーンは、ルーティングプラットフォームのシステム管理に関連するすべてのトラフィックの論理パスです。分散されたモジュラ式環境では、管理プレーンの存在により別の新たなレベルの複雑さが生じるため、安全なアクセスを維持するための要件が高くなります。このような安全なアクセスを最適に実現するには、次の機能を使用します。

- **デフォルトのアクセス拒否** — システムに共通する周知の脆弱性として、いくつかのプロトコルがデフォルトでイネーブルになっている点があります。これらのオープンポートは、システムへの侵入を招くセキュリティ上の抜け穴を生み出します。サービスプロバイダーの要求に応え、オペレータが手動でイネーブルにするまでこれらのサービスをオフにしておくデフォルト設定が CRS-1 計測機能に搭載されています。
- **Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントिंग) と暗号化プロトコル** — ルータを経由するすべてのアクセスを暗号化し、アクセスを制御する必要があります。Cisco CRS-1 は、AAA 認証および、暗号化プロトコルとして SSH、SSL、IPSec、SNMPv3 をサポートしています。ACL を使用して制御をさらに追加し、アクセスを特定の送信元ホストだけに制限できます。各ユーザは、ユーザのアクセス権限に応じて、AAA ドメイン内で明確に定義できます。
- **管理ポートの隔離** — コア ルータとコア スイッチには、通常専用の管理イーサネットポートが組み込まれており、これが時に装置への不正な侵入を招くことがあります。Cisco CRS-1 イーサネット管理ポートはルータブルであるため、AAA アクセス制御と暗号化を使用して制御することで、データプレーンと制御プレーンのトラフィックは互いに「飛び越えて (ホッピング)」行き来できないように隔離します。ACL を使用してホッピングを阻止することもできます。特にマルチシェルフ ルータ管理用に設計された付加価値 GUI ツールである Cisco Craft Works Interface (CWI) を使用すれば、数回のクリックだけで、複数のポートにまたがり効率的に ACL を実装できます。
- **役割ベースの権限モデル** — 未許可の、または未熟なネットワーク オペレータもシステム アベイラビリティに脅威をもたらすことがあるため、サービスプロバイダーには、ユーザが定義した条件に基づいてオペレータ権限を割り当てる柔軟な方法が必要です。

Cisco IOS XR ソフトウェアでは、使いやすい柔軟な方法で役割に応じた権限モデルを設定することができます。特定のオペレータやチームに適切なアクセスレベルを割り当てることができ、各種の操作をタスクとして認識します。たとえば、BGP の設定は 1 つのタスクであり、Open Shortest Path First (OSPF) の設定は別の 1 つのタスクです。システムのリロードも個別のタスクとなります。各タスクには、タスク ID と呼ばれる識別番号が一意に割り当てられ、読み取り権限または書き込み権限が定義されます。ユーザは、タスクグループに関連付けて、適切なアクセス権を継承させることもできます。セキュリティを設けるために、タスク ID は AAA サーバと連携して動作し、ルータへのアクセスを最大限中央で集中して制御します。

まとめ

DoS 攻撃と DDoS 攻撃は、今日のインターネットに現存し、サービスプロバイダーの収益を脅かすもっとも深刻な脅威の 1 つです。サービスプロバイダーの利益を守るために、高度なセキュリティ制御機能に加え、実績のあるシステム、およびネットワーク全体に関するベストプラクティスアプローチを駆使して、次世代ルーティングシステムに基づいた自己防衛型ネットワークを構築する必要があります。

Cisco CRS-1 の分散型モジュラアーキテクチャを使用することで、メモリ保護、論理ルータ内でのサービスの分離、および管理、制御、データの各プレーン間でのプロセスの隔離を通じて、安全性の高い常時稼働のシステム運用が可能になります。

CRS-1 に内蔵される高度な機能、および推奨されるベストプラクティスのほかにも、お客様のシスコ製品に関するセキュリティ問題を迅速に解決し、製品の弱点を克服するために、24 時間体制で対応する専門家のチームとして、Cisco Product Security Incident Response Team (PSIRT) のご利用も可能です。ネットワーキング分野の市場リーダーの専門知識を活用した先見のかつ迅速な対応により、シスコのお客様に数々の利点を提供します。

Cisco CRS-1 セキュリティ機能の詳細については、シスコのお客様担当窓口にお問い合わせるか、
<http://www.cisco.com> を参照してください。Cisco PSIRT の最新情報と現時点での推奨事項については、
<http://www.cisco.com/go/psirt> を参照してください。

参考文献

『CRS-1 System Overview』

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

Barry Greene、Philip Smith 共著、『ISP Essentials』

<http://www.ispbook.com>

Vijay Gill、John Heasley、David Meyer 共著、『RFC 3682 — The Generalized TTL Security Mechanism (GTSM)』

<http://www.ietf.org/rfc/rfc3682.txt>

Vijay Gill 著、『Lack of Priority Queuing on Route Processors Considered Harmful!』

<http://www.nanog.org/mtg-0302/gill.html>

『Improving Security on Cisco Routers』

<http://www.cisco.com/warp/public/707/21.html>

P. Ferguson、D. Senie 共著、『RFC 2827 — Network Ingress Filtering:Defeating Denial of Service Attacks which Employ IP Source Address Spoofing』

<http://www.ietf.org/rfc/rfc2827.txt>

©2004 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。
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

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

問合せ URL: <http://www.cisco.com/jp/go/contactcenter/>

〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL: 03-6670-2992

電話でのお問合せは、以下の時間帯で受付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問合せ先