ホワイト ペーパー

Cisco Any Device：生産性、セキュリティ、競争力を実現する未来の計画

概要

従来の企業ネットワークの境界が消滅し続け、企業環境のボーダレス化がますます進行する中、スマートフォン、タブレットなどのエンドポイント デバイスや Web アプリケーションによって、オンラインでの仕事のやり方や遊び方は後戻りできないほどの大きな変化を遂げています。シスコは、今までどおりのユーザ エクスペリエンスを保持しながら、従業員が使用するデバイスの選択肢を拡大する「Any Device」構想を提唱しています。これにより、グローバルな組織の競争力、生産性、およびセキュリティが維持または強化されます。

企業や大規模な組織は、特定のユーザ、デバイス、および場所から会社のネットワーク、データ、およびサービスへのアクセスを許可するか拒否するかを判断する必要があります。このホワイト ペーパーでは、シスコでの実際の経験と結果に基づいて、Any Device への変革に着手する際に、情報およびセキュリティ責任者、企業の IT および情報セキュリティ アーキテクトが考慮すべきステップとビジネス上の判断について説明します。

はじめに

あるグローバル企業では、毎日、80,000 人の従業員がさまざまな Windows デバイスの電源を入れ、17,000 人が Macintosh コンピュータにログインし、7,000 人が Linux マシンを使用しています。また、35,000 人が各自の Blackberry、iPhone、および Android でカレンダーをチェックし、E メールを送信しています[1]。この会社は、米国シスコシステムズ社です。当社の 70,000 人を超える従業員と 30,000 社を超えるグローバルな契約業者、コンサルタント、およびビジネス パートナーは、仕事に使用するデバイスの選択肢が広がること、またそれらのデバイスを使用して企業ネットワーク、システム、アプリケーション、データ、およびオンライン サービスにアクセスできる場所の選択肢が広がることを強く望んでいます。シスコ社員の大多数は、コンピュータとスマートフォンの両方を使用して会社の IT サービスにアクセスしています。しかも 20 % 以上が 3 種類以上のデバイスを使用しています。また、それらのデバイスの多様性も急激に拡大しつつあります。

前に述べたように、シスコは Any Device（任意のデバイス）という長期的な構想に着手しています。その目的は、これまでの一般的なユーザ エクスペリエンスを保持しながら、デバイスの選択肢を拡大することです。これにより、グローバルな組織の競争力とセキュリティが維持または強化されます。

[1] 2011 年第 2 四半期時点におけるシスコ社内の計測

Any Device 構想が必要となるビジネス上の主な理由は、次のとおりです。

- 生産性：シスコでは、技術に精通した従業員が各自の好みのスマートフォン、タブレット、またはラップトップを使用しており、必要な時に必要な場所で会社の仕事を行えるようにすることで、仕事に対する満足度と生産性の向上を図っています。**仕事に関連する生産性は、1 日あたり 30 分向上すると推定されます**[2]。
- 労働力の進化：最新の技術に精通した世代が、ビジネスの現場に登場してきています。彼らは、作業ツールや環境を各自で管理してきたメンバーであり、**最も生産性を上げられる方法を各自で選択する**ことを望んでいます。
- イノベーション：新しい次世代デバイスを発売後すぐに社員が使用できるようにすることで、生産性がさらに向上する可能性があります。このような**早期導入者は、より大きな市場の変化の前兆となる場合が多く**、シスコ IT の対応やシスコ製品戦略にもプラスの影響を及ぼします。
- 買収統合：シスコはこれまで多数の企業を買収してきましたが、その度に各社から非標準デバイスが持ち込まれてきました。Any Device は、新しい事業部門の迅速な統合と、付随するセキュリティ リスクの最小化に役立ちます。**買収統合に要する期間は、17 週間短縮されると推定されます。**
- 資本コスト：シスコでは、世界中で数万の契約業者やコンサルタントが業務に携わっています。この拡大する労働力にシスコ所有のラップトップやスマートフォンを供与することは、資金的に不可能です。契約業者やコンサルタントを Cisco® Virtualization Experience Client（VXC）デバイスに移行させることにより、シスコでは、既存デスクトップの総所有コストと比較して、**ユーザあたり年間 25 % のコスト削減を実現できると推定しています**。

他の組織には、リアルタイム データへの共有アクセスの必要性について、データ セキュリティ、モビリティの拡大、コラボレーション作業環境など、それぞれ独特の理由が存在します。エンドポイント デバイスの選択肢と台数の増加に伴って、企業では、自社のアプリケーションやデータへのアクセスを許可するかしないかを、企業ネットワークの内部と外部の両方について検討する必要があります。次に、それらのポリシーの計画、追跡、責任、および適用の方法を決定する必要があります。

このホワイト ペーパーでは、ビジネス、IT、およびセキュリティ ポリシーにもたらすリスク、効果、および変化、そしてシスコが現在実装しているソリューションについて説明し、シスコがこれまで Any Device への変革の途上で直面したその他の考慮事項についても説明します。

シスコが Any Device へと変革を進めるまでのステージ

ステージ 1：内部アクセス

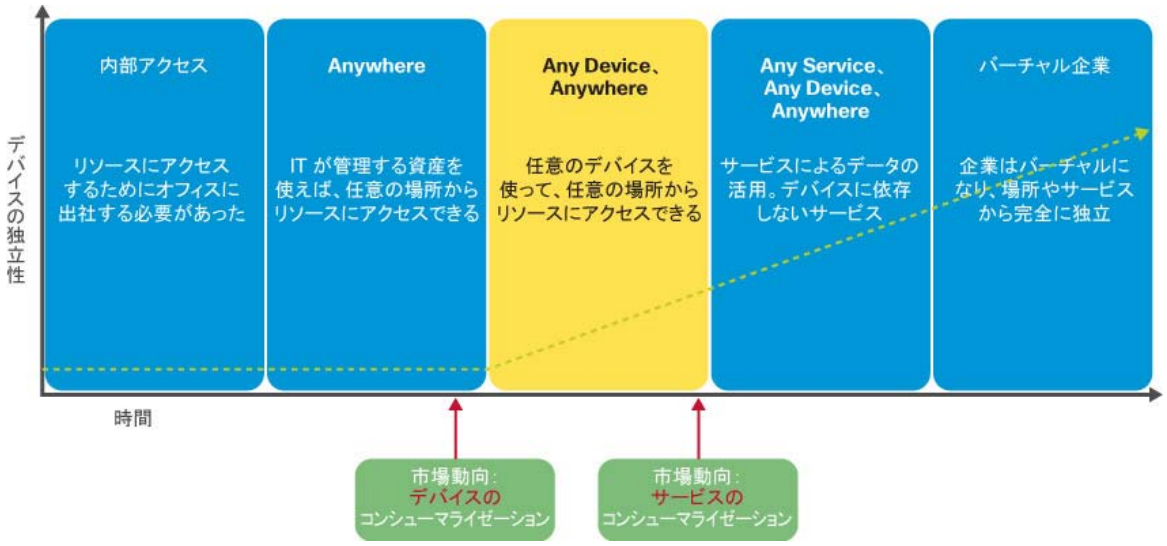
過去 15 年の間に、ユーザがシスコ ネットワークにアクセスする方法は大きく変化しました。20 世紀の終わり頃は、すべての IT デバイスが企業内に存在し、図 1 のステージ 1 に示すように、従業員は IT リソースへの**内部アクセス**のために、物理的にオフィス内にいる必要がありました。

ステージ 2：Anywhere

時の経過とともに、ラップトップと VPN が従業員にモビリティをもたらしました。また、労働力のグローバル化が進んだことで、より柔軟な労働形態の必要性が高まりました。ステージ 2 は、お客様サイトや自宅、カフェ、ホテルなど **Anywhere**（任意の場所）から企業の IT リソースにアクセスするモバイル ワーカーが増加するにつれて、作業環境や正規の勤務時間が生産性の制約要因ではなくなったことを示しています。このように場所の境界が消滅することで、ユーザは IT の管理対象資産を使用して、任意の場所からリソースにアクセスできるようになります。

[2] 2011 年 4 月 時点におけるシスコ社内の計測

図 1　Any Device 変革とともに変わってきた従業員の IT リソースへのアクセス



ステージ 3：Any Device、Anywhere

近年、スマートフォン、タブレット、およびラップトップは、優れた新機能、機能のアップグレード、フォーム ファクタの効率化、およびデバイス ライフサイクルの短縮に加えて、コモディティ化が進んでいます。その結果、従業員は、会社の E メールやイントラネットへのアクセスから企業のビジネス アプリケーションの使用まで、あらゆることを各自のデバイスで行いたいと希望するようになりました。企業の IT サポートにとっては大変なことではありますが、これらの要素はどれも比較的短い時間枠で具現化されました。買収によりシスコに加わった従業員は、すでに各自のデバイスを仕事に使用していて、それを使用し続けることを希望しました。数千に及ぶシスコのエクストラネット パートナーも、特定のアプリケーションにアクセスする必要がありましたが、シスコ IT が管理するエンドポイントを提供することは、資本コストと運用コストを伴う解決策でした。

シスコ IT は、新しいテクノロジーの社内への導入を制限して管理する従来の方式を取るのではなく、これらの次世代テクノロジーをすぐに採用して生産性の向上を可能にする必要性を認識しました。さらに、新しいクライアント テクノロジーを迅速に導入した結果、ユーザのコミュニティを作成し、IT がサポートを提供する方法を変革して、エンドユーザが同僚の知識を使って共通の問題を解決するという新しいアプローチ、ツール、およびテクノロジーの企業での利用および実装が生まれました。

このようなコミュニティ内でシスコ IT が果たす役割は、それを所有することではなく、同僚の一人として参加し、貢献することです。たとえば、シスコ内への Apple 製品の導入は、当初、業務のために使いたいツールやプラットフォームとして Apple デバイスを職場に持ち込んだユーザが先頭に立って進められました。シスコ IT がより多くのスタッフに対してこれらのツールを正式に使用できるようにする前に、シスコ内には 3,000 人の Mac ユーザがいたと推定されます。Mac ユーザは IT サポートがなくても、E メール エイリアス、Wiki、イントラネット、ビデオ コンテンツを通して、必要なセットアップ、使用、およびメンテナンスの支援を提供する新たな取り組みを始めていました。シスコ IT が PC のハードウェア更新ポリシーの一環としてオプションで Mac の提供を開始した際には、Mac コミュニティに混乱や変更を及ぼすことなく、セルフサポート モデルが導入され、サポートされました。IT はこの基盤を採用し、これを使用してセルフサポートをさらに進めたサービスを開発したのです。

同時に、これらの要素は、抜本的で避けることのできない問題に対応する新しい企業デバイス戦略の必要性を知らせるものでした。その問題とは、デバイスの境界が消滅していく中で、ユーザが**任意の場所（Anywhere）から任意のデバイス（Any Device）で企業リソースにアクセスできるようにする方法です。**

すべてのワーカーが、企業インフラストラクチャに対して同じレベルやタイプのアクセスを必要とするわけではありません。スマートフォンからメールやカレンダーのサービスを利用できるだけでよい人もいれば、より高いレベルのアクセスを必要とする人もいます。たとえば、シスコの営業担当者は、各自のスマートフォンから発注ツールにアクセス

できるので、取引を成立させる可能性が高まっています。シスコのエクストラネット パートナーは、自分のワークステーションを使用して仮想デスクトップ環境にアクセスできるので、シスコは自社の企業資産に対してより大きな制御を維持できます。

ステージ 4：Any Service、Any Device、Anywhere

シスコでは現在、オンプレミスで管理された企業リソースへのアクセスをユーザに許可しています。将来的には、サービス（アプリケーション、ディスク、およびサーバ）のコンシューマライゼーションによって、インハウスの IT サービスよりも高い柔軟性とコスト上の利点がもたらされます。一部のデバイスとシナリオでは、すでに企業取引用の外部クラウド サービスへのアクセスが必要となっています（図 2 を参照）。この新しいアプリケーションとサービスのボーダレス化の動向については、このホワイト ペーパーでは取り上げませんが、Cisco Any Device 戦略は堅固な基盤であり、その上に将来、**Any Service、Any Device、Anywhere** アーキテクチャと、最終的には仮想企業を構築することができます。

ステージ 5：バーチャル企業

バーチャル企業は、ステージ 4 からの論理的な進化で、企業は場所やサービスへの依存からますます解放されます。企業はきめ細かなアクセス コントロールと外部コラボレーションを可能にする成熟した ID モデルを備え、最大限のセキュリティ制御と機能が企業データに適用されています。バーチャル企業については、この将来的な状態に向けてさらに進んだ段階で取り上げます。

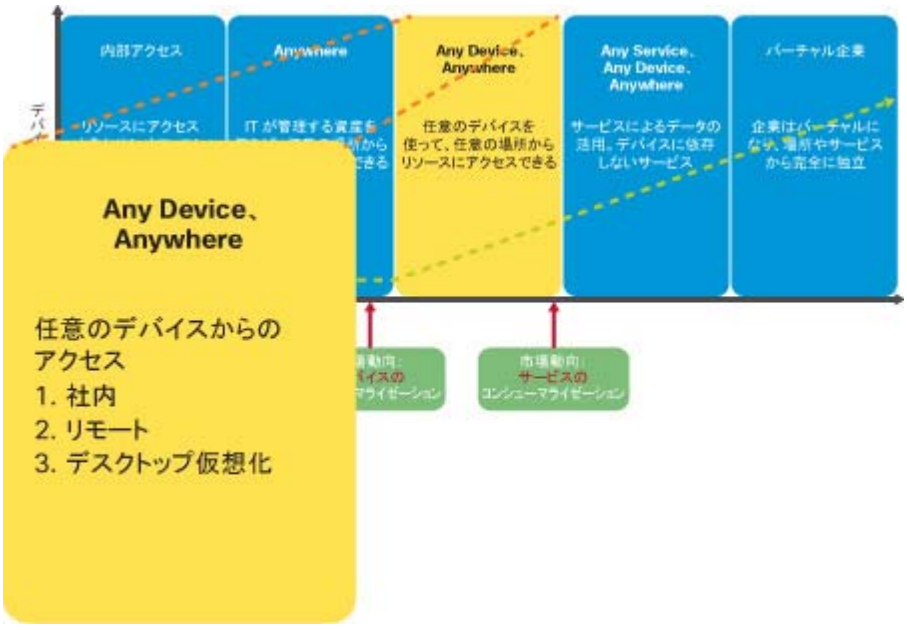
任意の場所から任意のデバイスでアクセス

この項では、Any Device が従来のセキュリティ パラダイムにどのような課題をもたらすかを含め、シスコがより成熟した Any Device アーキテクチャに到達するために取っているステップについて説明します。また、シスコが自社のネットワークに導入したソリューションについても説明します。

さまざまな Any Device ソリューションを実装するなかで、シスコは次の 3 つのシナリオに焦点を当てました。

- リモート アクセス
- 内部アクセス
- デスクトップ仮想化アクセス

図 2　Any Device で企業ネットワークにアクセスする 3 つの方法



任意のデバイスからのリモート アクセス

ステップ 1:任意のデバイスからのプロキシベースのアクセス

過去 5 年にわたるモバイル スマートフォンの大規模な導入により、シスコ IT では、Palm、Windows Mobile、Nokia、iPhone、Android などのデバイスから企業リソースにアクセスできるようにするためのプレッシャーが高まりました。このアクセスを提供すれば、シスコには生産性のメリットがもたらされますが、これには重大なリスクもありました(サイドバー:「潜在的な Any Device のリスク」を参照)。シスコはモバイル デバイスに対して、プロキシベースのアクセスによる制御されたサービス セット(E メールとカレンダー)を提供するという実際的なアプローチを選択しました。ユーザが各自のデバイスを選択できる一方で、シスコはデータ セキュリティと機密性を最大化するセキュリティ ポリシーを適用することができます。たとえば、ユーザが E メールやカレンダーにアクセスするためには、4 桁の PIN を設定して入力する必要があります。試行に 10 回失敗するとサービスがロックされ、非アクティブの状態が 10 分間続くと接続がタイムアウトになります。また、スマートフォンが紛失または盗難にあった場合、ユーザがシスコのヘルプデスク担当者に電話をすれば、担当者はデバイスにワイプ コマンドを発行することができます。

このアプローチが絶対に確実であるとは言えませんが、このソリューションを提供しないことを選択していた場合、組織はもっと大きなリスクにさらされていたでしょう。Yahoo IM や Gmail など、企業の制御を超えるアクセス手段が利用され、モバイル デバイスがワイヤレス LAN(WLAN)経由で企業ネットワークに絶えずアクセスしていたため、このサービスを開始する前は、事実上、セキュリティ ポスチャを制御できない状態でした。モバイル メール アクセスを可能にすることで、シスコは、シンプルでありながら効果的なアクセス コントロールを組み込んだ魅力的なアクセス パッケージをユーザに提供しました。シスコは現在、このモバイル メール アクセスによって約 35,000 台[3] のハンドヘルド デバイスを保護しています。シスコがスマートフォンから他の企業リソースへのアクセスを新たに提供する際には、それに応じてセキュリティ要件も増加することになります。

[3] 2011 年 5 月時点におけるシスコ社内の計測

信頼済みデバイス ポリシー

アーキテクチャ上の原則は、技術的な仕様に変換され、組織を実装可能なソリューションへと導く必要があります。信頼済みデバイスは、次のポリシー適用および資産管理要件に従う必要があります。

ポリシー適用

企業サービスにアクセスするデバイスは、接続前に次のセキュリティ制御の実装を検証する必要があります。これらの制御が不正に解除された場合は、企業リソースへのアクセスを無効にする必要があります。

- 強力なパスワード（複雑度）、10 分間の非アクティブ状態でのタイムアウト、およびログイン試行失敗 10 回でのロックアウトを適用するローカル アクセス コントロール
- デバイスおよびリムーバブル メディアの暗号化を含むデータ暗号化
- 従業員が退職した場合やデバイスが紛失または盗難にあった場合のリモート ワイプおよびロック機能
- 特定のセキュリティ ソフトウェア、パッチ アップデート、および企業アプリケーションの存在をチェックするインベントリ トラッキング機能

資産管理

企業サービスにアクセスするデバイスは、次の制御事項に従う必要があります。

- 一意に識別可能で、識別情報が簡単に詐称されないこと
- 企業アクセスを明示的かつ個別に許可されており、特定のユーザに登録されトレース可能であること
- 企業アクセスをブロック可能であること
- 今後考えられる調査で必要な場合にフォレンジック ログ データ（セキュリティ ソフトウェアのログ、ユーザ認証および許可、設定変更など）を生成できること

ステップ 2：任意のデバイスからのフル リモート アクセス

ハンドヘルド デバイス向けのモバイル メール サービスを実装した後、シスコ IT は、すべてのポータブル デバイスのためにリモート アクセスのアップグレードと拡張に取り組みました。

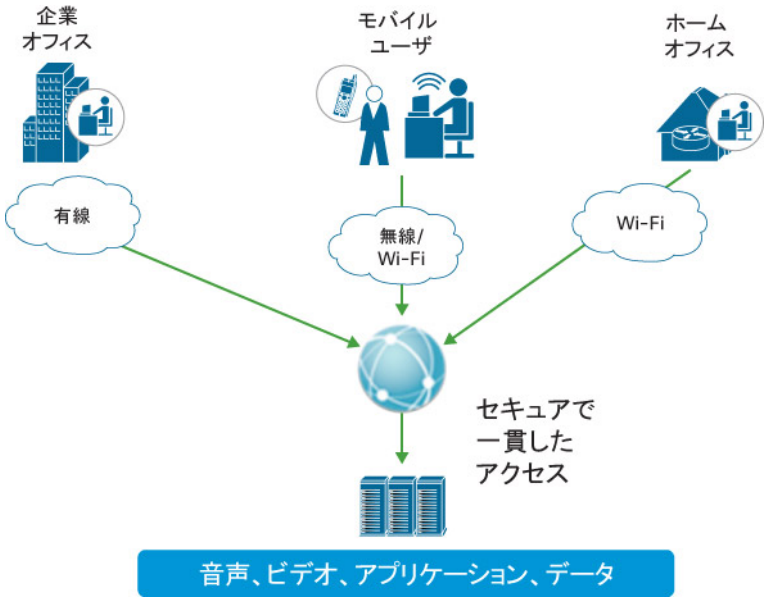
従来のリモート ワーカーは、IT から提供されるラップトップで、VPN を使用してシスコの企業ネットワークにアクセスしていました。しかし、IT から提供されるかどうかに関係なく、Mac、Windows、Linux PC などさまざまな端末の使用を希望するワーカーからの要求は、ますます大きくなっていきました。さらに、タブレット PC の人気が高まったことで、これらのデバイスのユーザもリモート アクセスを希望するようになったのです。これらの要求は、IT が管理する資産のシスコ セキュリティ パラダイムに大きな課題をもたらしました。

その結果、シスコは「信頼済みデバイス」という概念を導入しました。どのデバイスでも信頼済みデバイスになることができますが、企業ネットワークへのフル リモート アクセスを得るためには、一定のセキュリティ ベースラインに従う必要があります。シスコでは、次のアーキテクチャ上の原則を使用して信頼済みデバイスを定義しています。

- デバイスのセキュリティ ポスチャの保証：シスコは、デバイスが企業ネットワークに入ってきたときに、それを一意に識別して特定のユーザに結び付けると同時に、企業サービスへの接続に使用されるデバイスのセキュリティ ポスチャを制御できる必要があります。これはシスコのインシデント管理チームにとって重要な機能です。
- ユーザ認証および許可：シスコでは企業ユーザに認証を要求します。認証では、ユーザ証明書情報への不正アクセスを防止しながら、ユーザを識別します。さらに、シスコでは退職した従業員が認証されることを防止し、企業の資産やデータへのアクセスができないようにしています。
- 保存データのセキュリティ確保：企業サービスで使用される活動（E メールを読む、文書へのアクセス、Cisco Quad™ エンタープライズ コラボレーション プラットフォームを使用したコラボレーションなど）では、デバイス上にローカルに保存されたすべてのデータのセキュリティを確保する必要があります。ユーザは、企業データを残したままにする（不正アクセスにつながる可能性のある状況）リスクなしに、データへのアクセスや保存ができなければなりません。

非常に多くのユーザが自分のモバイル デバイスを使って企業ネットワークに接続することで、ネットワークはセキュリティ ホールに対して脆弱になり、IT やデータ資産は危険にさらされます。Cisco AnyConnect™ セキュア モビリティは、VPN クライアント、Web セキュリティ、および適応型セキュリティ アプライアンスによって、この問題に対応します。コンテキストに連動した、包括的で、予防的なセキュリティ ポリシー適用と、今日の急増する管理対象および管理対象外モバイル デバイス全体にわたるセキュアなモビリティを実現した、インテリジェントでトランスペアレントな「常時」接続を可能にします（図 3）。

図 3　Cisco AnyConnect セキュア モビリティ



Cisco AnyConnect Secure Sockets Layer（SSL）VPN クライアントは、IT の制御または管理下にないデバイスを使用する柔軟性をシスコ従業員に提供することに付随する、多くのセキュリティ課題に対処します。シスコ IT は、登録されたデバイスだけにネットワークへの接続を許可します。SSL VPN セッションの確立を試行するデバイスが確実に登録されるように、Cisco AnyConnect アプリケーションはデバイスの証明書とシリアル番号を照合します。また、デバイス登録の要求により、デバイスが個人に関連付けられることで、セキュリティ調査の助けとなり、ユーザのアカウンタビリティ確保にも役立ちます。

潜在的な Any Device のリスク

組織は、次の潜在的な Any Device のリスクに対処する計画を立てる必要があります。

- デバイスに保存された企業データ（規制上のデータや顧客データを含む）に対する制御の喪失
- デバイスのポスチャに対する制御の喪失：
  - 全体的なデバイス セキュリティの制御が低下すると、悪用のリスクが増大し、シスコのインフラストラクチャやサービスに対する攻撃ベクトルが作り出される可能性があります。
  - デバイスがポリシーや運用モデルに準拠しなくなる場合があり、ビジネス関係を損なったり、法的要件や規制要件に影響したりするおそれもあります。
- ネットワークに接続されるデバイスに対する可視性（つまり、デバイスの場所、所有および操作者）の低下は、セキュリティ、ライセンス、規制上や法的な保証、および監査の課題につながります。

シスコ IT では、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスを使用して、企業のセキュリティ基準に基づいてデバイスのコンプライアンスをチェックします。たとえば、シスコのユーザは、画面ロック パスワードを設定するまでは VPN 接続を確立できません。Cisco AnyConnect アプライアンスは、紛失したデバイスを使用して従業員以外の人がシスコ ネットワークに接続することを防止するのにも役立ちます。従業員がデバイスの紛失をシスコ IT に通知した場合、シスコ IT は、すべてのアクティブな VPN セッションを速やかに終了して、当該デバイスがさらに VPN 接続を行うのを防止することができます。また、シスコ IT は会社を退職する従業員のアカウントも容易に終了できます[4]。iPhone、Nokia、および Android モバイル デバイスでは、Mobile Device Management ソリューションによって証明書が配布されるため、セキュリティはさらに厳しくなります。このソリューションでは、より詳細なセキュリティ ポリシーの適用とインベントリ管理が可能で、デバイスを紛失した場合や従業員が退職した場合にデバイスのリモート ワイプを行うことができます。

シスコは現在、Cisco AnyConnect クライアントを Cisco ScanSafe ソリューション（クラウドベースの Web セキュリティ用）および Cisco IronPort™ Web Security Appliance（WSA; Web セキュリティ アプライアンス）（オンプレミス型 Web セキュリティ用）に統合する段階に入っています。これらの補完的なソリューションにより、ユーザはアクティブな SSL VPN 接続でつながっているかどうかに関係なく、Web ベースのマルウェアから保護されます。Cisco ScanSafe ソリューションは、デバイスがネットワーク上にもなく VPN 経由でも接続されていないときにユーザが悪意のある URL を閲覧した場合でも、マルウェアの感染をブロックし、デバイスと企業ネットワークの安全を確保します。

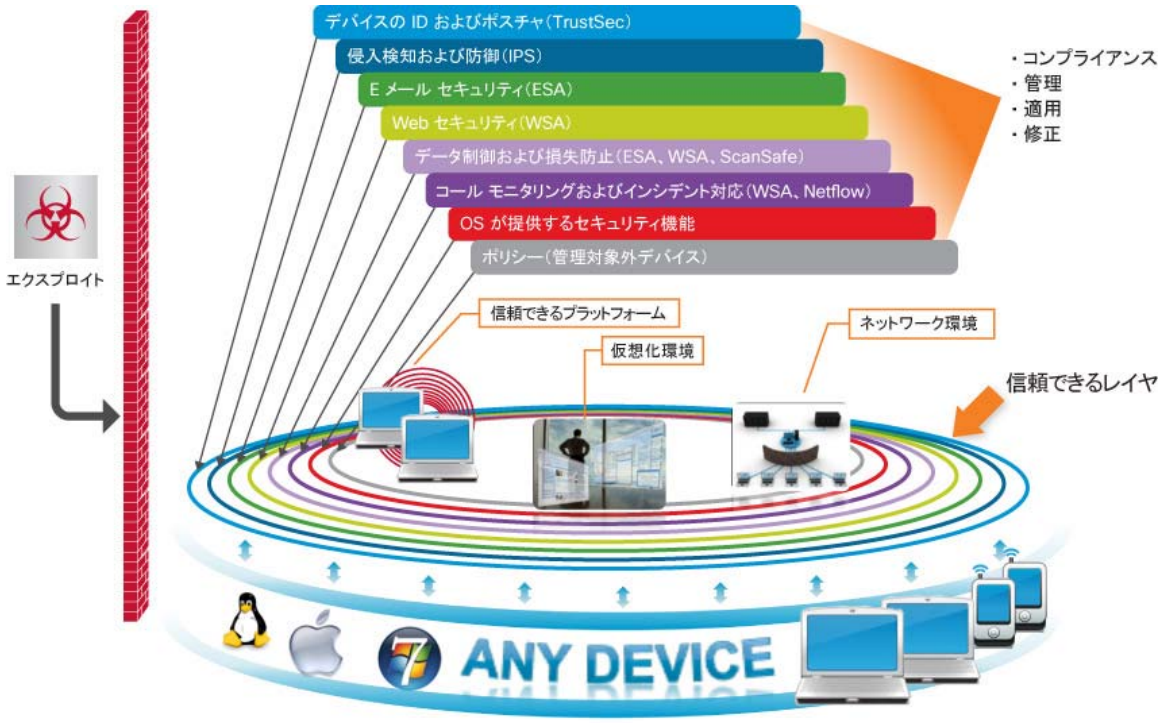
Cisco Any Device による内部アクセス

ステップ 1：ネットワークベースのマルウェア制御への注力

IT 管理のデバイスは、企業データのセキュリティと整合性を維持するうえで重要なツールです。シスコは、IT 管理下にあるコンピュータに、アンチスパム、アンチスパイウェア、マネージド アンチウイルス、ホストベースの侵入防御、パッチ管理を含む複数の防御レイヤをインストールして管理するなど、マネージド ホスティング環境の保護には優れた実績があります。しかし、マネージド ホスティング環境と IT 管理デバイスだけではなくなれば、この同じ制御をエンドポイントから切り離してマネージド ネットワークに組み込まなければなりません。シスコは現在、Cisco IronPort Web Security Appliance（WSA; Web セキュリティ アプライアンス）、Cisco IronPort Email Security Appliance（ESA; E メール セキュリティ アプライアンス）、Cisco Intrusion Prevention Systems（IPS; 侵入防御システム）に加えて、サードパーティ製の NetFlow 保護、ゼロデイ マルウェア対策、およびイベント管理などのツールを使用して、ネットワークを保護しています（図 4 を参照）。

[4] http://www.cisco.com/web/JP/ciscoitatwork/doc/Cisco_IT_Case_Study_AnyConnect_Deployment_JP_Revised.pdf を参照してください。

図 4　Cisco Any Device 環境におけるネットワーク セキュリティ制御



インターネット エッジに置く Cisco IronPort WSA などのセキュリティ プロキシは、有線およびワイヤレス ネットワークから入ってくる脅威を大幅に軽減します。Cisco IronPort WSA の導入は、Cisco Any Device 戦略のネットワーク セキュリティ要件を満たすと同時に、企業の保護にも役立ちます。米国東部のシスコ インターネット ゲートウェイにおける最初の導入では、WSA [5] が 45 日間[6] で 3,000,000 を超える悪意のあるトランザクションをブロックしました。

Cisco IronPort ESA は、業界をリードするスパム、ウイルス、マルウェア、およびターゲット攻撃用の脅威対策を備えた E メール ゲートウェイです。これにはデータ損失防止、アクセプタブル ユース ポリシーの適用、メッセージベースの暗号化によるアウトバウンド制御が組み込まれています。E メール セキュリティからネットワーク セキュリティへの移行により、さまざまなデバイスの保護だけでなく、生産性の向上も実現します。たとえば、ある月には、Cisco Ironport ESA が Cisco.com のアドレスに対する 2 億 8,000 万[7] の E メール メッセージをブロックしました。これは試行された全メッセージの 88 % に相当します。

また、シスコはネットワーク全体のインテリジェンス モニタリングおよびアラート用に Cisco IPS の検知機能も活用しています。シスコ IT とセキュリティ部門は、脅威に対してあらゆるインテリジェンスをすばやく運用可能にできるので、エンドポイントに依存することなく識別と対応を行うことができます。Cisco IPS は専用アプライアンスで使用するか、シスコ ファイアウォール、スイッチ、およびルータ プラットフォームに統合されるので、世界中のあらゆるシスコの場所に導入されています。このカバレッジのおかげで、Cisco Computer Security Incident Response Team（CSIRT）は、ネットワーク全体で発生するすべてのインシデントにすばやく対応することができます。シスコ IT がリースの管理対象デバイスからユーザ提供のデバイスに移行する際には、ネットワーク レイヤを詳細に検査できる能力が最も重要になります。デバイスに対する可視性が低下するため、ネットワーク レイヤにおける脅威の包括的かつリアルタイムな状況認識を実現するテクノロジーに対して投資を行う必要があります。

5　マルウェアのダウンロード、ブラウザ ハイジャック ソフトウェア、不要な広告ソフトウェア、ボットネットからのチェックイン、およびトロイの木馬（バックドア）の接続を含む

6　2011 年 4 月 14 日から 5 月 31 日まで

7　2011 年第 1 四半期からのデータ

ステップ 2:デバイス アクセス コントロールの強化

これまで、Cisco CSIRT では、インベントリ、資産管理、ホスト管理システムなどの IT システムに大きく依存して、インシデントに関与するデバイスをユーザに結び付けていました。デバイスが危険にさらされた場合、Cisco CSIRT はハードウェアとソフトウェアのインベントリ システムでデバイスを検索し、特定のユーザに結び付けた後、そのユーザに連絡を取って問題を修正できました。この解決策は、Any Device の世界では不可能です。Cisco CSIRT は Any Device 戦略のために IT システムを一新しました。たとえば、ユーザ ID の特定に役立てるために、Dynamic Host Configuration Protocol(DHCP)レコードと MAC アドレスをデバイス ログイン情報ではなくアプリケーション ログイン情報と関連付けました。

近い将来には、ポリシーベースのアクセス コントロール、ID 認識ネットワーキング、データの整合性および機密性サービスを提供する Cisco TrustSec® アーキテクチャが、この問題の解決に役立つと考えられます。Cisco TrustSec ネットワークのログインでは、802.1x プロトコルを使用してユーザを識別し、各自のデバイスに関連付けます。また、シスコはこれによって、動的なネットワーク環境で識別化されたアクセスを提供し、多様なコンシューマとネットワーク対応デバイスにもコンプライアンスを徹底させることができます。たとえば、Cisco TrustSec テクノロジーでは信頼済みデバイスのセキュリティ ベースラインを活用できます。デバイスは、信頼済みと見なされると、内部ネットワークの企業リソースへのフル アクセスが許可されます。さらに、シスコの統合された ID およびアクセスコントロール ソリューションである Cisco Identity Services Engine(ISE)プラットフォームでも、ID およびポリシー管理のための次世代アーキテクチャが提供されます。

デスクトップ仮想化のメリットと課題

デスクトップ仮想化は、プログラム、アプリケーション、サービス、およびデータを一元化するコンピューティング モデルです。そのユーザ エクスペリエンスは標準的なコンピュータ エクスペリエンスとほとんど同じですが、データ、オペレーティング システム、およびアプリケーションは、エンド ユーザのデバイスに完全には存在しません。このコンピューティング モデルは Virtual Desktop Infrastructure（VDI; 仮想デスクトップ インフラストラクチャ）とも呼ばれ、多くの利点をもたらす可能性を持っています。

- 一貫したエクスペリエンス：ユーザは、すべての VDI 対応デバイスで同じインターフェイスを使用できます。
- 生産性の向上：ユーザは、場所に関係なく、任意の VDI 対応デバイスからデータおよびアプリケーションにアクセスできます。多くの場合、VDI 環境はデータセンターにあるので、アプリケーションへのアクセスは速くなります。
- マルウェアのリスクの低減：IT では、アプリケーションが最新の状態に維持され、パッチが常に強化され、ユーザがパッチをインストールすることを確認できます。
- データや知的財産損失のリスクの低減：デバイスに障害が発生したり、紛失や盗難にあったりした場合でも、データは一元化され、バックアップされ、使用できる状態にあります。
- 市場投入期間の短縮：独自のデバイスを持つ買収先やパートナーなどの重要ユーザを、より迅速に企業環境に統合できます。
- アプリケーションの互換性：デスクトップ仮想化は、既知の運用環境で企業アプリケーションを実行するために、互換性確保のブリッジとして機能させることができます。
- サポートの容易化：仮想デスクトップのプロビジョニングは、新しい PC を支給するよりも迅速に実行できます。仮想化は一元化された IT サポート モデルにも適しています。

デスクトップ仮想化は、すべてのアプリケーションやユーザ コミュニティに適したソリューションではない場合もあります。重要な課題は次のとおりです。

- 特定のアプリケーションに適さない：現在は、CAD、ビデオ、およびユニファイド コミュニケーションなどの高帯域幅アプリケーションに課題があります。
- 特定のデバイスに適さない：デスクトップ仮想化のユーザ エクスペリエンスは、小さな画面のスマートフォンやタブレットなどの特定デバイスに合わせて作られたものではありません。
- プラットフォームの制限：ほとんどのデスクトップ仮想化ソリューションは、主として Windows デバイスに重点を置いています。
- 遅延の大きい環境：VDI は遅延の大きいネットワーク環境に課題を抱えています。

任意のデバイスからのデスクトップ仮想化アクセス

Cisco Any Device 戦略は、モビリティと新しいデバイスによって加速され、すぐに第三の要素が浮上しました。それは、買収先の統合や海外およびオフサイトでのアウトソーシング関係の管理をどのように行うかという要素です。

過去数年の間に、シスコは多数の会社を買収し、それらの統合が、シスコ IT とセキュリティ部門に課題をもたらしました。買収された会社には、それぞれ独自のデバイスやセキュリティ ポリシー、標準がありましたが、多くの場合、それらはシスコで使用されているものとはまったく異なっていました。シスコの情報セキュリティ チームは、エンドポイント デバイスがシスコのポリシーと標準に適合していることを確認する役割を担いました。実施可能なソリューションは 2 つだけでしたが、どちらにもそれぞれ課題がありました。1 番めは、買収先のデバイスをシスコ IT から提供されるサポート対象デバイスに置き換え、その使い方について従業員にトレーニングを実施するものです。このプロセスは、コストと時間がかかり、週または月単位で生産性に影響を与える可能性がありました。2 番めの選択肢は、既存のデバイスを適切に維持するものですが、企業全体のセキュリティ ポスチャが低下するリスクを伴います。つまり別のソリューションを見つける必要があったのです。

また、既存の企業ポリシーにも、アウトソーシングへの移行によって無理が生じていました。15 年前は、アウトソーシングは簡単な作業に限られていました。今日では、組織のほとんどの部分でアウトソーシングが発生し、多くのビジネス プロセスに関わっています。現在、シスコで働く派遣社員は 45,000 人を超えており、17,000 人が 350 のサードパーティの所在地から日々の活動を行っています。また、シスコは 200 社を超えるサードパーティ企業とアウトソーシング パートナー関係を維持しています。

現在までに、オンサイトおよびオフサイトの出向あるいは派遣社員の大部分に対して、シスコ ポリシーに準拠した、シスコ IT のサポート対象デバイスが提供されています。海外およびオフサイトでのアウトソーシングについては、シスコ IT がすべてのサードパーティ ネットワーク接続をサポートするエクストラネット インフラストラクチャを整備しています。シスコ IT は、サードパーティ所在地のデバイス、WAN 接続、リモート ネットワークを含む、すべてのエクストラネット接続の 70 % をエンドツーエンドで管理しています。しかし、アウトソーシングのボリュームと複雑さが増大したために、このモデルは、効果が出るまでの期間と TCO に対する企業の期待に応えられなくなりました。

デスクトップ仮想化は、このホワイト ペーパーの前の方で説明したネットワーク セキュリティ機能と相まって、これらの課題の克服に役立つと同時に、大きなメリットを提供すると考えられます（サイドバー「デスクトップ仮想化のメリットと課題」を参照）。シスコは、デスクトップ仮想化によって、買収先や海外およびオフサイトのアウトソーシング先で 20 % を超えるコスト削減を実現し、効果が出るまでの期間も 40 ～ 60 % 短縮できると推定しています。また、この一元化された、完全にスケーラブルな、場所に依存しないサービスにより、データ セキュリティとデバイスのコンプライアンスも向上します。シスコは、すでに米国で 2,000 人のユーザによるデスクトップ仮想化のパイロットを開始しており、2011 年の後期には他の場所がこれに続く予定です。

シスコが得た教訓

Any Device 戦略の立案と実装は、すべての組織にとって重大な変化です。このような変革は、一貫したガバナンス構造を持つことで、よりスムーズかつ確実に受け入れられます。この全社的な Any Device への変革を進める間に、シスコ IT とセキュリティ部門のプロフェッショナルは、多くの教訓を得てきました。

- Any Device への変革では、デスクトップ、セキュリティ、ネットワーク インフラストラクチャ、および通信部門の領域を超えた取り組みが必要となります。
- 組織は、職務横断的なチームを編成し、エグゼクティブを教育し、結果と測定基準を報告する責任を負う 1 人のエグゼクティブ スポンサーを募る必要があります。
- ユーザ群を分割してユーザ分析を実施するために必要な作業量を、少なく見積もらないでください。この分析は、どのユーザにどのサービスの利用資格を与えるかを決定するものであり、Any Device への変革に着手するにあたって最初に取るべきアクションです。

組織は、データ セキュリティ、整合性、プライバシー、および監査に関する適用規制を遵守するために多大な投資を行います。シスコは 2010 年にビジネス行動規範をアップデートし、個人所有デバイスの使用上のガイドラインを盛り込みました。情報セキュリティ部門では、そのセキュリティ ポリシーの多くを、よりデータが中心になるように書き直す作業を進めています。しかし、時には、これらの投資が Any Device 構想と矛盾する場合もあります。たとえば、シスコは現地で医師と臨床看護師を雇用して、従業員に医療サービスを提供しています。タッチスクリーンのタブレットは、これらの看護師が医療現場で患者を回る際に持ち歩いたり、Cisco TelePresence® 会議と併用して患者の診断や処置を行ったりするのに有用なツールです。しかし、これらのタブレットは、**Health Insurance Portability and Accountability Act**（HIPAA; 医療保険の相互運用性と説明責任に関する法律）データにアクセスします。シスコでは、当社の医療従事者が個人のタブレットを医療現場で使用することを許可しておらず、IT 管理下にあるデバイスに対してのみ、適切なセキュリティとデータ管理プロトコルに確実に従わせるようにしています。

Any Device への変革を進める最初のステップ

シスコは、Any Device への変革に乗り出した際に、この新しいパラダイムの影響を受ける 13 の重要なビジネス分野を特定しました。表 1 では、これらの重点分野を取り上げ、シスコが潜在的な問題を認識して方向転換し、考慮事項に取り組む最善の方法を判断するのに役立った質問のリストを示します。これは読者が各自の変革を開始する際にも役立つ可能性があります。変革に着手する際には、これらの質問について検討し、細心の注意を払って率直に回答してください。

表 1　Any Device への変革に関する質問

ビジネス分野	ビジネス上の質問
ビジネス継続性計画とディザスタ リカバリ	• ビジネス継続性計画（BCP）のなかで、非社有デバイスのアクセスを許可する必要がありますか、あるいは制限する必要がありますか。 • エンド デバイスが紛失または盗難にあった場合、ネットワークにアクセスするすべてのエンド デバイスをリモートでワイプする機能が必要ですか。
ホスト管理（パッチの適用）	• 非社有デバイスに、既存の企業ホスト管理の流れへの参加を許可しますか。
クライアント設定管理およびデバイスのセキュリティ検証	• セキュリティ プロトコルに対するデバイスのコンプライアンスをどのように検証し、最新の状態に維持しますか。
リモート アクセス戦略	• 組織は、企業システムにリモートからアクセスする非社有デバイスをどのように管理しますか。
ポリシーおよび権限付与	• 誰が、どのデバイスでどのサービスおよびプラットフォームへの権限を付与される必要がありますか。 • 臨時ワーカーは、エンド デバイス、アプリケーション、およびデータに対して同じ権限を付与される必要がありますか。
ソフトウェア ライセンス	• 企業にライセンス供与されたソフトウェアを、非社有デバイスにインストールすることを許可するようにポリシーを変更する必要がありますか。 • 既存のソフトウェア契約は、ユーザが複数のデバイスから同じソフトウェア アプリケーションにアクセスすることに対応していますか。
暗号化要件	• 非社有デバイスは、既存のディスク暗号化要件に従う必要がありますか。
認証および認可	• 非社有デバイスが既存の Microsoft Active Directory モデルに参加することを想定または許可しますか。

ビジネス分野	ビジネス上の質問
規制遵守の管理	• 高いコンプライアンスが必要な場合や高いリスクを伴う場合の非社有デバイスの使用について、組織のポリシーをどのようにしますか。
インシデント管理および調査	• 企業の IT セキュリティおよびプライバシー部門は、非社有デバイスのインシデントや調査をどのように管理しますか。
アプリケーションの相互運用性	• 組織は、非社有デバイスのアプリケーション相互運用性テストにどのように対処しますか。
資産管理	• 組織は、所有するデバイスの識別方法を変更して、非所有のデバイスも識別できるようにする必要がありますか。
サポート	• 非社有デバイスに対するサポートの提供について、組織のポリシーをどのようにしますか。

今後の道のり

シスコでの Any Device への変革は、将来に続く継続的かつ長期的な投資です。今後数年にわたって、シスコは、重要なデータとアプリケーションをデバイスからネットワークまたはクラウドに移動し、ネットワーク セキュリティを強化し、デバイスがネットワークと通信する際のデバイスの ID 制御とポリシー制御を統合する計画を継続していきます。この計画の次のステップは、次のビジネス分野における Any Device の課題に対処するのに役立ちます。

アプリケーションの相互運用性

現在シスコ ネットワークに接続されているデバイスの約 60 % は Windows デスクトップですが、この割合は、他のデバイスを使用するユーザの増加に伴って縮小しています。今後、シスコでは、デバイスにインストールされるソフトウェアの種類やバージョンの制御が低下し、アプリケーション、ブラウザ、バージョン、およびランタイム環境間で相互運用性の問題が生じる可能性が高くなります。この問題は Web アプリケーションの普及によって簡素化されていますが、解決はされていません。さまざまなデスクトップ、スマートフォン、およびタブレットが増加し続けるにつれて、ブラウザ環境の数も増加します。シスコのエグゼクティブは、World Wide Web Consortium（W3C）標準に基づいて、内部 Web アプリケーション用の「ブラウザ標準」イニシアチブを支持しています。業界の Web 開発標準によって、異なるブラウザ、オペレーティング システム、およびエンド デバイスを含むエコシステムでのアプリケーションの相互運用性は促進されます。

また、シスコでは、任意のオペレーティング システムに互換性のある運用環境を提示するために、デスクトップ仮想化も利用しようとしています。現在、数千に上るユーザで実施されているデスクトップ仮想化のパイロットは、2012 年 7 月までに 18,000 人のワーカーに提供される予定です。

ソフトウェア ライセンス

シスコでは、ほとんどの企業と同様に、資産管理システムを使用してソフトウェア ライセンスを追跡しています。シスコは Any Device ソフトウェア ライセンス シナリオに関連して、次のような多くのポリシー上の質問に取り組む必要があります。

- ユーザは、企業のソフトウェアを各自のデバイスにインストールすることを許可されますか。
- ソフトウェア ベンダーとの既存の契約で、非社有デバイス上に企業のソフトウェアを置くことは許可されますか。
- シスコは非社有デバイスを追跡する必要がありますか。その場合、どのような方法で行いますか。

シスコでは、すべてのデバイスを追跡する資産管理システムと、非社有のハードウェアおよびソフトウェア資産に対応する詳細なレポート メカニズムを実装するために、Cisco TrustSec テクノロジーによって収集される情報（ユーザ ID や MAC アドレス）の使用について調査しています。

ビジネス継続性計画（BCP）とディザスタ リカバリ

シスコには、他社の所在地で、社有の資産を使用して仕事をする従業員がいます。また、世界中のシスコのオフィスで、多くの派遣社員が仕事をしています。データが安全で元の状態のままであることを確認する責任は、誰にあるのでしょうか。シスコは Windows PC を一元的にバックアップしていますが、パートナーの多くは、自社の知的財産を他社のシステムにバックアップされたくありません。ユーザが企業のビジネス継続性サービスに含まれない場合、障害の発生時にこれらのユーザが迅速に仕事に戻れるように、ほかにどのような準備を整えられるでしょうか。1 つの

考えられるソリューションは、デスクトップ仮想化です。これにより、機密データとデバイスの関連付けを解除することができます。

シスコは、ネットワーク経由のユーザ インタラクションの管理を開始しています。シスコはデスクトップ仮想化とSoftware as a Service（SaaS）またはクラウド コンピューティングを組み合わせて使用することで、デスクトップに存在するアプリケーションとデータがより少なくなる将来に向けて、確実に進んでいます。一部の企業アプリケーションまたは場所については、ユーザ、アクション、およびデータを一貫して管理、追跡、およびバックアップできる、よりトランザクション主体のアプローチに移行します。この進化によって、シスコ IT は今後、効果的でセキュアな「Any service、Any Device、Anywhere」の状態に進み、最終的にはバーチャル企業へと向かっていきます。

関連情報

シスコは、自社組織への Any Service、Any Device、Anywhere 環境の実装に向けて大きく前進しています。今後も、読者が実装の過程で出現する問題を回避できるように、その経験と得られた教訓を引き続きお知らせしていく予定です。シスコがビジネスと IT の環境を Any Device 以上の状態に変えるために使用した知識と方法は、規模の大小を問わず他の組織にも適用できます。

ビジネス、IT、およびセキュリティ インフラストラクチャを戦略的に位置付け、Any Device アーキテクチャへの移行に備える方法を学ぶ際は、シスコ担当者にご相談ください。

Any Device を可能にするシスコ ソリューションの詳細については、次のリンク先を参照してください。

- Cisco AnyConnect セキュア モビリティ クライアント
- 仮想化ストラテジー
- Cisco TrustSec テクノロジー
- Cisco IronPort メール セキュリティ アプライアンス
- Cisco IronPort Web セキュリティ アプライアンス

お問い合わせ先

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間:平日10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/

12.01