シスコ IT によるエンタープライズ対応 Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）の社内導入について

シスコ IT の BYOD プログラムは、従業員が自分のデバイスを選択できるようにすることでビジネス コミュニケーションをシンプル化し、生産性を向上させるものです。

エグゼクティブ サマリー

課題

- 人気のスマートフォンやデジタル タブレットのサポートを求める従業員の声が高まっている
- IT コストを削減する必要がある
- セキュアで拡張性に優れ、使いやすいソリューションを提供する

ソリューション

- ガバナンス、セキュリティ、サポート ポリシーを計画する
- 従業員の個人用デバイスからの社内アクセスを可能にし、会社が費用負担するアカウントを減らす
- 社内 SNS にセルフサポート コミュニティを作る

結果

- ユーザの生産性向上：3 億米ドル
- 年間コストが 50 万米ドル、デバイスのアップグレード コストが 85 万ドル削減
- ユーザ 1 人あたりのサポート コストが 25 % 減少

得られた教訓

- 急速な利用の拡大とユーザ ニーズの高まりに備える
- ユーザのセルフサポートに必要なリソースを提供する

次のステップ

- eStore を使用してアプリケーションとサービスの提供を自動化する
- 新しいセキュアなモバイル クラウド サービスをサポートする

背景

2009 年以降、シスコは、従業員がビジネス目的に使用する個人用携帯電話とその関連サービス プランのサポート方法を変更しました。この変更により、スマートフォンをビジネスに使用する従業員が大幅に増え（図 1 を参照）、従業員の生産性、満足度、柔軟性が向上しました。同時に、これまでとは異なるガバナンスおよびサポート モデルである Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）プログラムにより、シスコの負担するコストが減少しました。BYOD プログラムは、シスコ IT の「Any Device（あらゆるデバイス）」イニシアチブの第一段階として実施されました。このイニシアチブは、シスコの従業員が、場所やデバイスを問わずに社内リソースに安全にアクセスできるようにすることを目的としています。

2000 年代初め、音声とデータを扱えるスマートフォンの登場により、シスコ IT はモビリティ サービスを提供することが可能になりました。モビリティ サービスは、営業、カスタマー サポート、およびエグゼクティブレベルの従業員がどこからでもモバイル デバイスを使用して、仕事用の電子メール、予定表、連絡先、社内 Web コンテンツにアクセスできるようにすることで、従業員の生産性向上に寄与しました。

当初シスコは、対象の従業員を限定して、Blackberry や Nokia を主とするモバイル デバイスを会社の負担で購入し、プロビジョニングとサポートを行っていました。しかし現在、コンシューマ向けスマートフォンがモビリティ デバイスとして普及したことで、シスコ IT は新たな課題に直面しています。

以前の戦略では、従業員は限られた種類のモバイル デバイスから希望のデバイスをリクエストすることになっていました。それに対してシスコ IT は、特定のサービスをそのデバイスにプロビジョニングし、事前に定義されたユーザ エクスペリエンスを提供しました。サービスは事前に交渉されたもので、音声、メッセージ、データ プランを提供します。

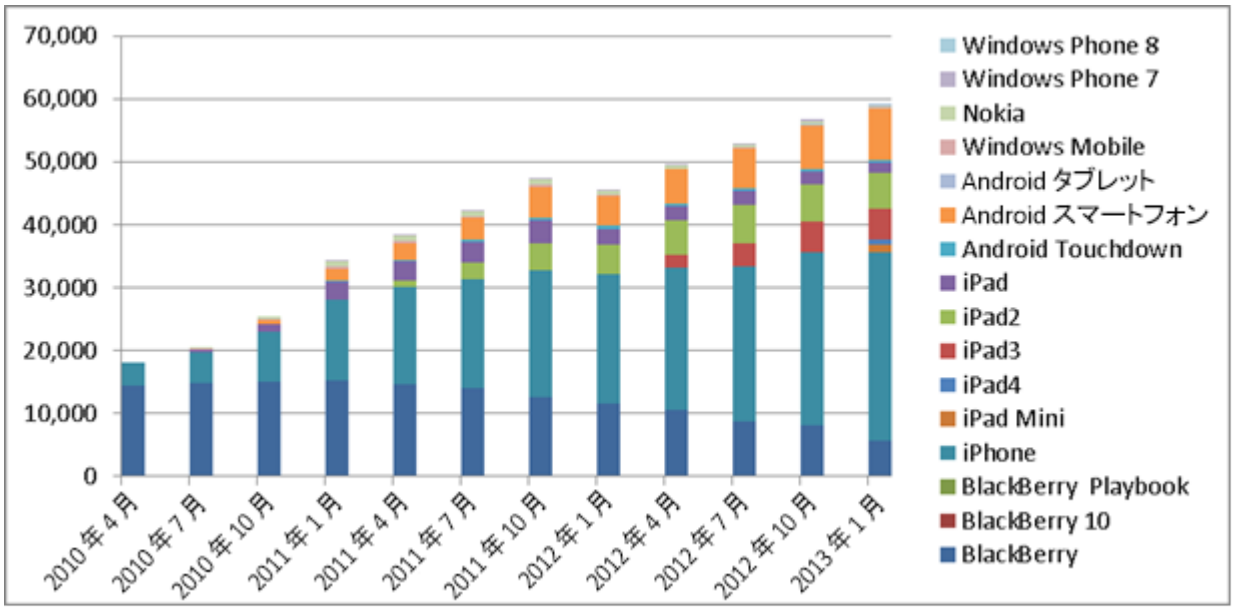
課題

2009 年以降、シスコ IT は、2 つの主要なビジネス推進要因により、モビリティ サービス戦略の重要な側面の見直しと変更を迫られています。

第一に、世界経済の低迷により、経費の抑制および、会社負担の携帯電話サービスの継続的コストの見直しを余儀なくされました。そのため、会社負担の携帯電話およびサービス プランの対象となっている従業員、シスコ IT がサポートするモバイル デバイスの数と種類、従業員がシスコ IT モビリティ サービスを利用した場合に発生する社内予算などの要因を評価しました。

第二に、Apple iPhone などのコンシューマ向けデバイスがより洗練されて、強力かつ使いやすくなり、シスコ従業員の間で、シスコ IT が当時用意していたデバイスよりもはるかに人気になりました。シスコの従業員は、自分のモバイル デバイスを使用することで生産性が向上することを実証しました（内部調査によると、モバイル デバイス ユーザは平均で 1 日あたり少なくとも 15 分の生産的な時間を獲得しています）。iPad などのタブレット デバイスの出現によっても、従業員のモビリティ サービスへの関心がさらに高まりました。そこでシスコ IT は、柔軟性および利便性に対する従業員のニーズを満たす方法を模索し始め、それを確立しました。

図 1. シスコでのモバイル デバイス数の増加



さまざまな新しいプラットフォームにモビリティ プログラムを大幅に拡張する上で、3 つの大きな課題がありました。

第一に、新しい（そしてますます高価になる）モバイル デバイスとサービス プランの使用を求める従業員の数が急増するなか、従業員のサポートとコストの抑制をいかに両立させるか、

第二に、ソリューションの安全性をどのように確保するか、が課題となります。非常に多くの種類のデバイスとサービス プロバイダーが存在するなか、使用可能な何百種類ものプラットフォームを保護するにはどうすればよいのでしょうか。

第三に、これらすべての新しいデバイスを維持する方法です。携帯電話のモデルとサービス プランを限定すれば、IT はサポート スタッフとプロセスを統合し、その数を減らすことができますが、何百種類ものデバイスとサービス プロバイダーの組み合わせに対応し、コストを負担することは、事実上不可能です。

ソリューション

スマートフォンやタブレットの人気の高まりにより、シスコ IT はモビリティ戦略の変革を迫られました。

ガバナンス

シスコ IT は、少数のデバイスと限られたサービスをサポートすることから、BYOD 戦略を導入することに切り替えました。これにより各従業員は、デバイスの費用を自分で負担すれば、さまざまなデバイスとユーザ サービスから自由に選択できるようになりました（表 1 参照）。

> 「モバイル デバイスを会社のネットワークに接続したいというニーズが従業員の間でますます高まっており、複雑化しています。シスコのモビリティ サービス提供モデルにより、このようなニーズの高まりに対応することが可能になります」
>
> **– シスコ IT モビリティ サービス マネージャ Brett Belding**

新しい戦略では、従業員は自分のデバイスを選択し、いずれかのモビリティ サービスへのアクセスを要求します。従業員の部署は、サービスへの要求を承認し、費用を支払います。シスコ IT は、承認されたサービスをプロビジョニングし、従業員がスマートフォンやタブレットなどの複数のデバイスからネイティブに接続できるようにします。従業員は、必要に応じて追加デバイスを設定するだけです。複数のデバイスをアクティブにしても、従業員の部門に対する追加の社内サービス課金は発生せず、従業員のマネージャからの承認も必要ありません。

表 1. ガバナンス：シスコのモビリティ オプション

	デバイス	サービス
元のオプション	• VP に承認された場合はシスコが料金を支払う • BlackBerry モデルまたは Nokia モデルのいずれかに限定 • 従業員の仕事にモバイル デバイスが必要な場合のみ利用可能 • デバイスのリース料は従業員の部署に請求される	• VP に承認された場合はシスコが料金を支払う • 各国内の 1 つまたは少数のサービス プロバイダー/ベンダーが提供 • サービス プランはシスコが交渉 • 毎月のサービス料金は従業員の部署に請求される
BYOD、シスコ費用負担サービス	• マネージャに承認を得て従業員が選択し、料金を支払う • 雇用者がすべての作業用デバイスを提供することが法令で義務付けられている欧州の一部の国では利用できない • サービス接続およびサポートに関する少額の料金は、従業員の部署に請求される	• VP に承認された場合はシスコが料金を支払う • 各国内の 1 つまたは少数のサービス プロバイダー/ベンダーが提供 • サービス プランはシスコが交渉 • 毎月のサービス料金は従業員の部署に請求される
BYOD、従業員費用負担サービス	• マネージャに承認を得て従業員が選択し、料金を支払う • 雇用者がすべての作業用デバイスを提供することが法令で義務付けられている欧州の一部の国では利用できない • サービス接続およびサポートに関する少額の料金は、従業員の部署に請求される	• 従業員が選択し、料金を支払う • 従業員は大手プロバイダーが提供する任意のサービス プランを選択できる • 一部の国の従業員は、交渉によるディスカウントが適用されたシスコ サービス プランから選択できる

対象の従業員と費用負担者/負担内容

シスコは、コストを抑制するために、会社負担のモバイル デバイスと関連サービス プランに関して、対象の従業員を定義する社内全体ポリシーを定めました。基本的には、従業員がモバイル デバイスとその関連サービスの料金を支払います。ただし、各シスコ部門または地域/国の組織は、必要に応じてこの会社ポリシーを現地のビジネス要件や法的要件に合わせて変更できます。一般的に、仕事にモバイル デバイスを使用する必要がある従業員は、限定された基本的な会社提供デバイスから選択できます。

対象となる従業員が少ない場合は、会社ポリシーに定められているとおり、シスコが毎月のモバイル サービス プランのコストを負担します（基本的には、従業員がモバイル デバイスを購入する必要があります）。会社負担のモバイル アカウントの要求は、モバイル通信コストを抑制するため、バイス プレジデントの承認を得る必要があります。

シスコ IT モビリティ サービス担当マネージャの Brett Belding は次のように述べています。「モバイル サービス料金は、回線あたりの平均月額コストが 120 米ドルで、年間コストはたちまち膨大な額になります。このポリシーにより、会社負担のモバイル アカウントを本当に必要とする職種の従業員だけが、VP レベルの承認を求めるようになると想定しています。そうなれば、従業員の利便性が主目的のアカウントの数を制限できます」

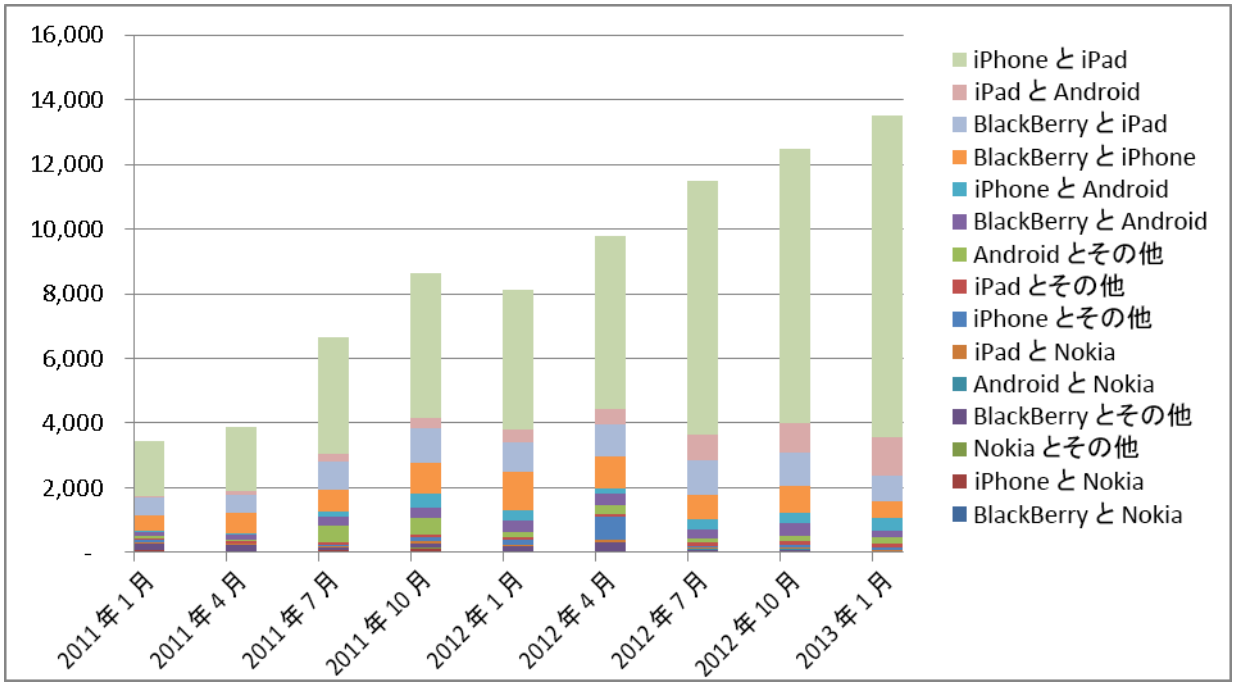
会社負担のスマートフォン サービスの対象となる従業員は、シスコ社内プランに追加され（該当する場合）、モバイル サービス料金は会社に直接請求されます。シスコは、コストを削減するため、世界中の携帯電話会社との契約交渉を行っています。また、シスコ IT は、1 つの国だけで働く従業員や、多少なりともローミングをすると予想される従業員向けの通話プランについても従業員に通知します。問題のある請求を追跡できるように、マネージャには、各従業員のサービス料が例外的に高い場合に、その請求内容を示すレポートが送信されます。マネージャは、状況や通話プランに応じて、問題を解決する最善の方法を決定できます。

会社負担のモバイル サービスが適用されない従業員は、自分の個人用スマートフォンと個人負担のサービス プランを使用してシスコ ネットワークにアクセスすることについて、マネージャに承認を求めることができます（通常は承認されます）。この場合従業員は、アプリの使用料、ファミリ プラン料金、解約手数料、通話時間またはデータ利用量の超過料金、追加のモバイル サービスの料金を支払います。これらのオプションは、会社負担のモバイル アカウントでは利用できません。

シスコ IT も、従業員の部署に少額のモビリティ サービス利用料金を請求します。シスコ IT が請求するユーザあたりの月額料金は、シスコ IT がモビリティ サービスを開発、保守、提供するためのコストに充てられます。この料金は、シスコ IT が、現在のインフラストラクチャの維持およびユーザ数の継続的な増大に対応するために要する、実際のコストに基づいて毎年調整されます。

現在、ほとんどのシスコ従業員がスマートフォンをプライマリ モバイル デバイスとして選択しており、多くの従業員がタブレットをセカンダリ モバイル デバイスとして使用しています。2013 年初めの時点で、モバイル サービスを利用しているシスコ従業員の 35 % 以上が標準のラップトップに加えて 2 台のモバイル デバイスを携帯しており、この傾向はますます高まっています（図 2 参照）。さらに、3 台以上のデバイスを携帯する従業員も増えています（ただし、主な用途は、研究やアプリケーションの開発およびテスト）。

図 2. 1 人で 2 台のモバイル デバイスを所有する従業員の増大



承認されたモバイル デバイス

モビリティ サービスの提供を開始した当初は、シスコ IT で各モバイル デバイスに対する広範なテストを実施し、それに合格したデバイスのみを承認済みリストに追加していました。しかし、大量のモバイル デバイスが市場に登場し、時間の経過と共にますます増えるなか、そのようなサポート モデルでは不可能だと判明しました。

現在、シスコ IT は主に、Apple iOS、Android、BlackBerry など、オペレーティング システムに基づいて新しいモバイル デバイスを承認しています。

シスコ IT のモバイル ソリューション担当技術責任者の Paul Clements は次のように述べています。「電子メールや予定表など、私たちが関心を持つデバイス機能の大部分を提供するのはオペレーティング システムです。デバイスが BlackBerry デバイスでない場合は、シスコで必要となるセキュリティ ポリシーをそのデバイスがサポートしているかどうかも検討します。たとえば、ユーザの電子メール、予定表、連絡先リストを、モバイル デバイスと社内の Microsoft Exchange 環境の間で同期するために使用している、Microsoft ActiveSync テクノロジーを使用できるかどうかなどです」

2011 年半ばの時点で、スマートフォンやタブレットを含む 50 種類以上のモバイル デバイスが、その普及状況とシスコ IT のセキュリティ要件への準拠が認められ、シスコ IT の検証済みリストに登録されていました。ただし、すべてのデバイスが完全に安全と見なされたわけではありません。

Belding は次のように述べています。「現在、最新の Apple iOS バージョンを実行している BlackBerry および Apple デバイスは、会社のイントラネット上のデータやアプリケーションを含む、シスコ IT のさまざまなモビリティ サービスへのアクセスに必要なデバイス セキュリティを備えています。その他のオペレーティング システムを実行しているデバイスは、限られた数のユーザ機能にしかアクセスできません。ユーザの社内電子メール、予定表、連絡先にしかアクセスできないように制限されています」

これらの基本的なサービスへのアクセスでさえも、デバイスは、シスコ IT が定める特定のセキュリティ要件を満たしている必要があります。

モバイル アクセス サービス

Mobile Mail Essentials サービスを利用すれば、モバイル通信事業者またはワイヤレス LAN 接続経由で、シスコ電子メール サーバに直接かつ安全にアクセスできます。このサービスでは、ほとんどの場合、デバイスのネイティブな電子メール、予定表、および連絡先機能を使用できます。シスコ IT は、Mobile Mail Essentials サービスを提供するため、多くのモバイル デバイス オペレーティング システムでサポートされている Microsoft ActiveSync プラットフォームを使用しています。BlackBerry ユーザは、BlackBerry オペレーティング システム独自の BlackBerry Enterprise Server（BES）インフラストラクチャによってサポートされます。

すべてのデバイスですべてのサービス機能がサポートされるわけではありません。たとえば、ワイヤレス LAN 経由で通話を行うために必要な、802.11 ワイヤレス LAN 接続へのアクセスを提供しているのは一部のデバイスのみです。それ以外のデバイスは VPN クライアントをサポートできません。シスコ IT では、ユーザのデバイス購入を支援するため、どのデバイスがどの機能をサポートし、シスコ環境の最低限のセキュリティ要件を満たしているかを示す、一般的なモバイル デバイスのメニューを従業員に提供しています。さらに、シスコ IT は、Cisco AnyConnect® VPN Client やサードパーティのモバイル デバイス管理ソリューションを活用するなどして、承認済みの各デバイスに提供するサービスを増やすことを目標にしています。

シスコ IT は、デバイスのセキュリティ レベルと機能に基づき、表 2 に示すモビリティ サービスを提供しています。

表 2. シスコ IT モビリティ サービス セット

機能	説明
シングル ナンバー リーチ	従業員には単一の仕事用電話番号が割り当てられます。その番号にダイヤルすると、まず仕事用の電話が鳴り、続いてモバイル デバイスが鳴ります。電話に応答しなかった場合は、仕事用ボイスメール システム（Unity Connection）に着信が記録されます。シングル ナンバー リーチは、Cisco Unified Communications Manager の機能で、電源が入っている任意の携帯電話に対して使用できます。
Mobile Mail Essentials	従業員は、任意のスマートフォンから Microsoft ActiveSynch を使用して会社の電子メール、予定表、連絡先リストにアクセスできます。
Cisco Webex® 会議	従業員は、任意のビデオ対応スマートフォンから Cisco® Webex 会議に参加できます。Webex 会議はクラウド サービスであり、イントラネット アクセスは不要です。
Cisco Jabber™	スマートフォンを持っている従業員は、任意の場所から、社内のエンタープライズ ワイヤレス LAN またはベンダーのモバイル データ サービス経由で、会社の IM、プレゼンス、音声およびビデオ、ビジュアル ボイスメールを使用できます。
イントラネット アクセスとアプリケーション	シスコ IT によって「安全」と認定されたスマートフォンを持つ従業員は、Cisco AnyConnect VPN を使用して、会社のイントラネットおよび社内ツールにアクセスできます。社内ツールには、Cisco Webex Social や、さまざまな Cisco eStore アプリケーション（My Expenses、My PTO、My Approvals など）が含まれています。Cisco eStore は、従業員が、各デバイスに必要なあらゆる IT サービスとアプリを 1 ヵ所で見つけることができる便利なソリューションです（図 7）。

キャリア サービスと管理

モビリティ サービスは、シスコがキャリアからの請求を支払っているかどうかに関係なく、すべてのシスコ従業員が利用できます。会社負担サービスの対象外の従業員は、自分のデバイスから、電子メール、予定表、連絡先機能や、VPN およびイントラネットへのアクセスを要求できます。このサービスは、タブレットを含む複数のデバイスでも利用できます。

シスコは、キャリアのグローバル ネットワークを活用してコストを最適化します。頻繁に出張する、大量のデータが必要な従業員のため、シスコはコストと生産性の微妙なバランスを取れる革新的なソリューションを必要としています。従業員は、出張時には可能な限り Wi-Fi を使用することが推奨されます。シスコはまた、キャリアと協力してデータ プール プランも作成しています。これにより IT は、従業員のデータ使用をまとめて管理し、超過料金に関連するコストや過少利用を回避できます。

可能な場合には、シスコは「分割請求」を活用します。分割請求では、使用料はシスコが、選択したハンドセットの料金は従業員が、それぞれキャリアに直接支払います。

セキュリティ

セキュアな BYOD ソリューションを提供し、次の 3 つの事項に対応する

- モバイル デバイス自体やデバイス上のアプリおよびデータの保護：紛失または盗難されたデバイスが使用されたり、読み取られたりしないように保護する。
- ネットワーク アーキテクチャの保護：外部の脅威（マルウェア）からデバイスとデータを保護し、不正なデバイスによる侵入からネットワークを保護する。
- エンド ユーザの保護：モバイル デバイスを使用する際にシスコのセキュリティを確保する責任があることを従業員に教育するとともに、従業員がよくあるセキュリティ ミスを回避できるようにサポートする。

モバイル デバイスの保護

モバイル デバイスのセキュリティ対策の種類と強度に関して、モビリティ サービスを提供する IT 部門には 2 つの重大な課題があります。第一に、モバイル デバイスには連絡先や電子メールなどの機密情報が保存されるため、デバイスが紛失または盗難された場合に、他者が情報にアクセスできないようにする必要があります。第二に、電子メールと Web アプリケーションには機密情報が含まれているため、ユーザとそのモバイル デバイスは、社内リソースにアクセスする前に認証を受けなければなりません。これらの課題は 2 種類のセキュリティ対策によって解決できます。1 つはデバイスのコンテンツを保護すること、もう 1 つはデバイスから社内ネットワークへのアクセスを保護することです（図 3 参照）。

図 3.　モビリティ サービスのためのシスコ IT セキュリティ設計

シスコ IT のモビリティ アーキテクトである Jason Freeth は、「モバイル デバイス セキュリティの原則として、アクセス可能なデバイスが増えるほど必要なセキュリティが増えます」と述べています。

モバイル デバイスがネットワーク エッジのモバイル サービス（図 3 の外側の円の部分）にアクセスするには、下記のセキュリティ要件を満たした上で、シスコ IT によって信頼できるデバイスと見なされなければなりません。これらの基本的な要件を満たしていないデバイスは、シスコのネットワークに接続できません。

- 紛失または盗難されたデバイスをリモートからワイプする機能
- 携帯電話のコンテンツやアプリケーションにアクセスするための 4 桁以上のパスワード
- 非アクティブな状態が 10 分間続いた場合にはパスワードの再入力が必要

シスコのコア ネットワーク（図 3 の内側の円の部分）内のモバイル サービスにアクセスするには、さらに 2 つのセキュリティ対策が必要です。それは Cisco AnyConnect VPN Client と組み込みのデバイス暗号化を使用することです。

また、ユーザは、電話番号またはモバイル デバイスの固有デバイス識別子（UDID）をシスコ IT に登録する必要があります。登録されたデバイスのみが社内サービスにアクセスできます。デバイスを登録すると、シスコ IT がデバイスのコンテンツ（保管中のデータ）に暗号化を適用したり、ソフトウェア バージョンのインベントリやデバイス ステータスの確認などのデバイス管理タスクを実行したりできるようにもなります。

Clements は次のように述べています。「これらのセキュリティ要件はデバイス自体を保護するものですが、シスコのアプリケーションや機密情報に第三者が不正にアクセスするのを防止するのにも役立ちます。さらに、シスコでは、ユーザのデバ

イスに基づいて、ユーザが利用できるサービスを定めています。つまり、ユーザは、使用しているスマートフォンまたはタブレットが保護できないサービスには一切アクセスできません」

製品リスト

インフラストラクチャとクラウド サービス
- Cisco Identity Services Engine
- Cisco クラウド Web セキュリティ
- Cisco E メール セキュリティ
- Cisco Web セキュリティ
- Mobile Device Manager
- Cisco Prime™ Service Catalog
- Cisco Process Orchestrator

ユニファイド コミュニケーション
- Cisco Unity® Connection

ビデオとコラボレーション
- Cisco Webex
- Cisco AnyConnect VPN Client

eStore の Cisco Mobility アプリケーション
- モバイル デバイス向け Cisco AnyConnect
- モバイル デバイス向け Cisco Jabber
- モバイル デバイス向け Cisco Webex Social
- eStore に用意されているその他多数の製品

ユーザ主導のセットアップ プロセス中に「利用規則」ドキュメントが表示され、モビリティ サービス利用の承認を得るために規則を確認することが要求されます。このドキュメントには、モバイル デバイスを「ジェイルブレイク」（ルート レベルまたはコマンド ラインのアクセス権を取得すること）しないこと、機密データを保護すること、デバイスのオペレーティング システム ソフトウェアを定期的に更新することなど、セキュリティ上の問題に関する規則が記載されています。

ネットワーク アーキテクチャの保護

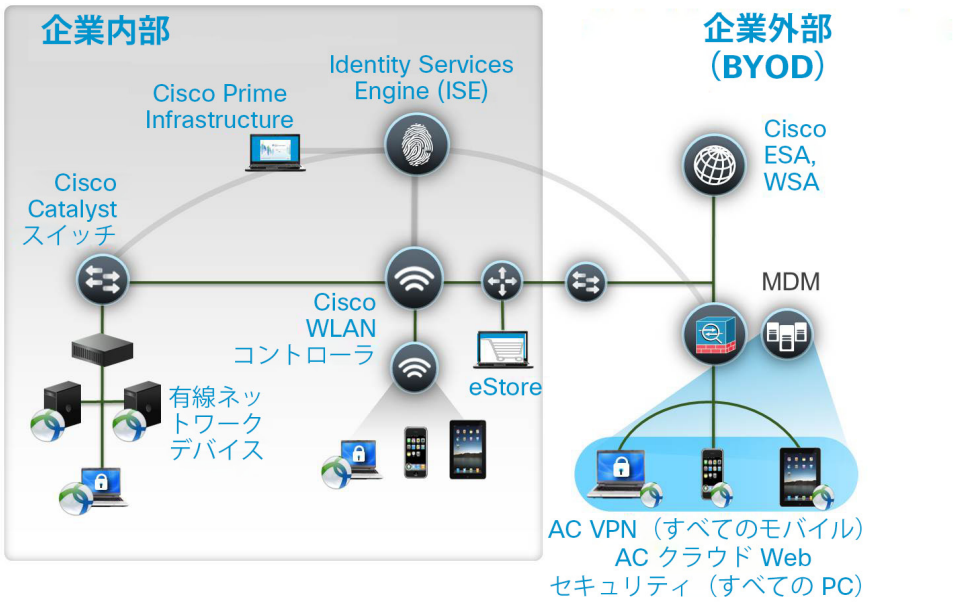
シスコ IT は、ユーザがシスコのキャンパスにいるかどうかにかかわらず、自動化された、セキュアな統合ネットワーク セキュリティ ソリューションをユーザに提供する必要があります。ネットワークはさまざまなネットワーク リソースによって保護されますが、その大半はすでにシスコ ネットワークに組み込まれ、有線およびワイヤレス ネットワークを保護しています。シスコは、モバイル デバイスにまで適用範囲を広げています。ただし、このアーキテクチャの一部は、モバイル環境に特有のものです（図 4 参照）。

このアーキテクチャに含まれるコンポーネントをいくつか次に示します。

Mobile Device Manager（MDM）：デバイスのポスチャとアプリの配信を処理します。MDM は、モバイル デバイスがシスコ ネットワークに接続を試みる際にデータと設定を確認し、デバイスがシスコの MDM に登録されているかどうか、セキュアなポスチャ（最低要件を満たすオペレーティング システム上で動作している、指定されている桁数以上の暗証番号が設定されているか、10 分以内のタイムアウトが設定されている、リモート ワイプが有効になっている、コンテンツが暗号化されている、マルウェア対策が有効になっているなど）に準拠しているかどうかをチェックします。

Cisco AnyConnect セキュア モビリティ クライアント：iPhone や iPad、および、全従業員の PC/Mac ラップトップなど、シスコで使用されているさまざまなモバイル デバイス上で動作します。IPsec インターネット キー エクスチェンジ（IKEv2）とセキュア ソケット レイヤ（SSL）プロトコルを使用して、シスコへのセキュアな接続をサポートします。Cisco AnyConnect セキュア モビリティ クライアントは、シスコ ネットワーク内の Cisco 適応型セキュリティ アプライアンス（ASA）5500 に接続し、イントラネットにアクセスしようとしているユーザを認証します。クライアントは、モバイル データ ストリームを暗号化し、読み取りまたは侵害から保護します。

図 4. BYOD と有線およびワイヤレス アクセス向けのシスコ IT セキュリティ アーキテクチャ



Cisco Web セキュリティ アプライアンス（WSA）：Cisco AnyConnect セキュア モビリティ クライアントを使用した任意のデバイスからシスコ外部の Web サイトへのアクセスをすべてスクリーンします。WSA は、レピュテーションとコンテンツの両面で Web サイトを評価し、シスコの社内セキュリティ ポリシーに基づいて、アクセスまたは特定の機能（チャット、メッセージング、ビデオ、音声など）をブロックまたはモニタリングします。これらのポリシーを使用することで、シスコ IT は Web サイト リクエストの約 2 %（1 日あたり 600 ～ 700 万件のサイト リクエストに相当）をブロックします。これらのリクエストの大部分は、Web のレピュテーション情報を基にブロックされますが、リクエストの 2 % は、トロイの木馬またはトロイの木馬ダウンローダなどのマルウェアを理由にブロックされます（1 日に 500,000 件以上のマルウェア ダウンロードがブロックされます）。

Cisco E メール セキュリティ アプライアンス（ESA）：シスコ外部からスマートフォンを含む各デバイスに送信されるシスコ メール トラフィックをすべてスクリーンします。Cisco ESA は、既知のスパム プロバイダーやスパム コンテンツからの電子メールやその他の不正な電子メールをブロックします。シスコが 1 日に受信する 560 万通の電子メールのうち、約 3 分の 2 がブロックされます。マーケティング コンテンツを含む電子メールの 15 % は受信を許可されますが、ESA サーバによって「マーケティング」または「スパムの可能性あり」とマークされます。

Cisco Identity Services Engine（ISE）：有線、ワイヤレス、および VPN ネットワーク間から社内の有線およびワイヤレス リソースへアクセスするエンド ユーザとエンド デバイスは、その ID、アクセス コントロール、そしてデバイス セキュリティに応じて ISE がアクセスを制御します。ISE は Cisco MDM ソリューションと連携し、すべてのモバイル デバイスがセキュリティ ポリシーに準拠していることを確認してから、ネットワーク接続を許可します。確認内容には、デバイスが MDM に登録されているか、デバイスに 4 桁の暗証番号と 10 分以内のタイムアウトが設定されているか、デバイスのディスクは暗号化されているか、ルート権限が取得されていたり「ジェイルブレイク」されていたりしないか、などがあります。ISE と MDM の統合ソリューションは、継続的にポスチャ チェックも実行し、デバイスがポリシーに準拠していることを確認します。また、シスコの既存の社内セキュリティ ポリシーを適用し、ユーザが利用したデバイスやネットワーク経路に基づいて、セキュリティで保護されたコンテンツ リポジトリごとにユーザ アクセスを制限します。MDM は準拠しているデバイスを識別し、ISE は非準拠デバイスのアクセス

を拒否することによってこれらの規則を適用します。社内リソースへのアクセスを試みる BYOD デバイスは、すでにシスコ インフラストラクチャに組み込まれている、Active Directory ベースの強力なアクセス制御によっても制限されます。

Cisco Prime™ Infrastructure：あらゆるデバイス（モバイル クライアントを含む）からデータセンターへのワイヤレスおよび有線ネットワーク経由のアクセスは、エンドツーエンドで完全に可視化します。これにより、シスコ IT は、アプリケーション/サービス/エンド ユーザ関連の問題を把握し、トラブルシューティングして修正できます。

Cisco Prime Service Catalog と Cisco Process Orchestrator：シスコ従業員が、増え続けるモバイルアプリを社内の Cisco eStore からダウンロードできるようにします（Cisco eStore は、従業員が各デバイスに必要なあらゆる IT サービスとアプリを 1 ヵ所で見つけることができる便利なソリューションです）。このソリューションは、プロビジョニング プロセスの自動化、対象従業員の選別、承認要求の生成、サービスのプロビジョニング、サービス ライフサイクルの管理を行います。

エンド ユーザの保護：トレーニングとコミュニケーション

ビジネス行動規範：シスコの全従業員は、年に一度、シスコにおける倫理的な行動を定義した、シスコ ビジネス行動規範（COBC）を確認する必要があります。COBC のガイドラインに従わないと、解雇される場合があります。全従業員は、COBC を読んでその内容を理解し、それに従うことに同意したことを証明する必要があります。この行動規範には、シスコのコンピューティング デバイス（ラップトップやスマートフォンを含む）の「アクセプタブル ユース ポリシー」の遵守に関して、次のように記載されています。

「シスコは、各国/地域の法令および規制によって禁止されている場合を除き、シスコのビジネスを遂行するため、または内部のネットワークおよびビジネス システムを利用するために使用される、シスコ、従業員、もしくは第三者が所有またはリースしているすべての電子デバイスおよびコンピューティング デバイスにセキュリティ制御を要求する権利を有します」

「シスコのビジネスを遂行するため、または内部のネットワークおよびビジネス システムを利用するために使用される、シスコ、従業員、もしくは第三者が所有またはリースしている電子デバイスおよびコンピューティング デバイスを保護する責任を負います。デバイスを無人の場所に置く場合は、適切にセキュリティ保護する必要があります。シスコのビジネスを遂行するために使用される電子デバイスおよびコンピューティング デバイスの盗難または紛失が発覚した場合は、迅速に報告する責任を負います」

「すべてのコンピューティング デバイスは、パスワード保護付きのスクリーンセーバーでセキュリティ保護する必要があります。スクリーンセーバーは 10 分以下で自動的にアクティブになるように設定しておく必要があります。デバイスを無人の場所に置く場合は、画面をロックするか、またはログオフする必要があります」

「認証制御、企業のデバイス管理ソフトウェア、セキュリティ システム ソフトウェアなどによる（ただし、これに限らない）セキュリティ制御を回避したり、阻害したりすることは許可されていません」

シスコ従業員は、モバイル デバイス用のシスコ サービスを初めて注文するときに、『Cisco Mobility Rules of Use（シスコ モビリティ利用規則）』を読んでこれに同意する必要があります。この利用規則には次のように記載されています。

「シスコは、シスコ機密情報が侵害された可能性があると判断した場合には、従業員が利用しているシスコ対応モバイル デバイスのデータを、直接もしくは「リモートから」削除する権利を有します。また、そのプロセスにおいて、デバイスに保存されている個人データ、サード パーティ製アプリケーション、オペレーティング システム ファイルも削除される可能性があります。従業員は、このアクションの結果として生じた損失または損害についてシスコが一切責任を負わないことを了承し、これに同意するものとします」

これらの利用規則に同意しない従業員は、シスコ サービスにアクセスできません。

モバイル デバイスのセキュリティ確保に関する社内ガイダンスが従業員に提供されています。シスコ IT からのサポートに加え、社内の SNS プラットフォームのモビリティ コミュニティで、継続的なディスカッション フォーラムやトレーニングが提供されます。これには、ユーザ ガイド、ベスト プラクティス、ウェビナーの録画、Show and Share での短いトレーニング デモ ビデオなどが含まれます。BYOD に申し込んだ従業員は、必要に応じて現在のサービスに関連する電子メール通知（脆弱性通知、セキュリティ アドバイザリなど）を受け取ります。

サポート

シスコ従業員は、サービスのライフサイクル全体を通じて次のようなさまざまなレベルのサポートを必要とします。

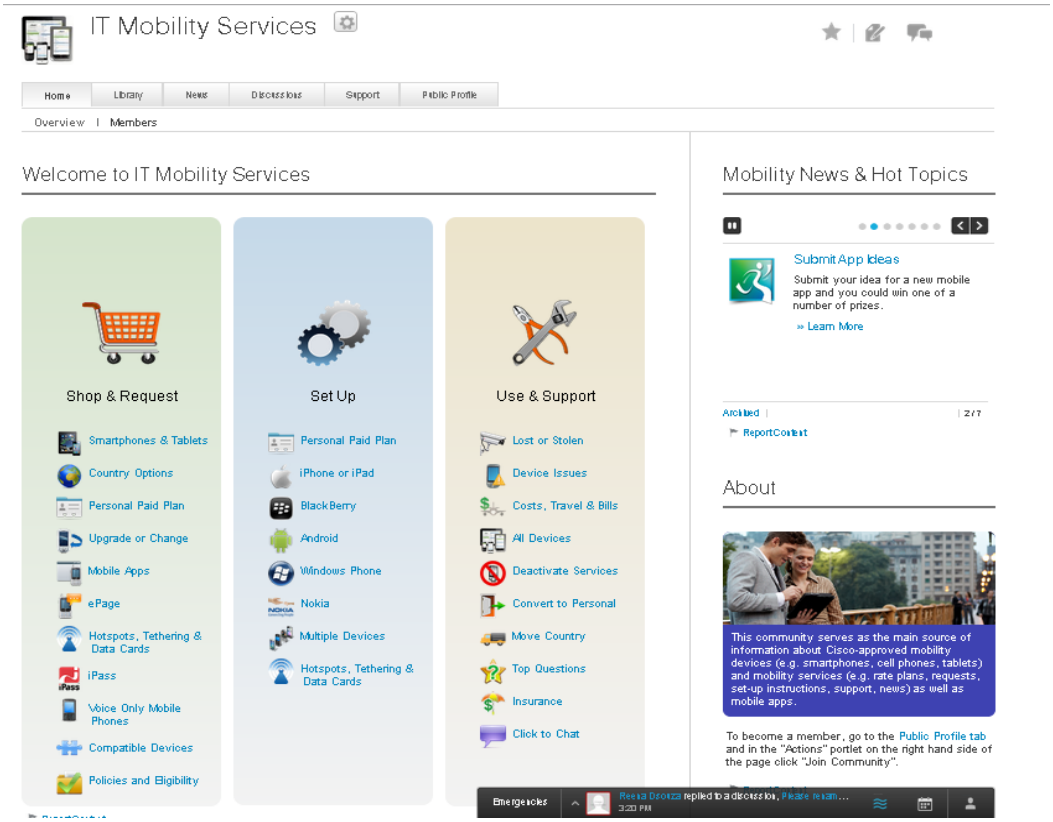
- 適切なデバイスとサービス プランの選択
- マネジメント承認の取得
- 新しいサービスの申し込みとインストール
- 複数のデバイスでのサービスのサポート
- 障害や問題のトラブルシューティング
- 想定外のコストの管理（特に出張時）
- 携帯電話の紛失または盗難への対処
- 新しい携帯電話へのアップグレード

シスコ IT は、社内 SNS 上の社内オンライン モビリティ サービス コミュニティを通じて、ほとんどのユーザ サポートを提供します。従業員は、このコミュニティ（図 5 参照）を活用すれば、上記の一般的なタスクの大部分と、更新や改善に関するトピックに対応できます。

Belding は、「シスコでは、多くのユーザが参加してアイデアや推奨事項を共有し、必要な新サービスを迅速に見つけられるユーザ コミュニティの構築に取り組んでいます」と述べています。

従業員は、セルフサポートを使用するように奨励されていますが、緊急の問題や高レベルの専門知識が必要な問題については、引き続きオンラインでケースをオープンしたり、ヘルプ デスクに電話したりすることも可能です。シスコのデバイスあたりのケース数が 50 % 以上減少していることからわかるように、ほとんどの従業員はセルフサポートのスピードと効率性を評価しています。

図 5. セルフサービス情報、サービス導入、サポートに関する IT モビリティ サービス コミュニティ



結果

シスコ従業員が職場で自分のモバイル デバイスを使用できるようにしたことは、シスコの文化に非常に大きな影響を与えています。モビリティと BYOD は従業員に歓迎され、どこでも作業できるようになったことで生産性が向上しています。

拡大と満足度

モビリティ サービスは、最もユーザ数の多い米国を筆頭に、世界 70 ヵ国以上の営業、カスタマー サポート、およびバックオフィスの従業員が利用しています。

2013 年半ば時点で、シスコ IT は 66,000 台以上のモバイル デバイスにモビリティ サービスを提供しています。これは対前年比で約 40 % の増加です。この劇的な増加率は、減速する気配がありません（図 1 参照）。この増加は、仕事の生産性、柔軟性、満足度を向上させるために、モバイル デバイス、アプリ、サービスを調査して購入する従業員に起因しています。

シスコでのスマートフォン サポートに対するニーズは今後も増え続けるでしょう。現在、シスコ ネットワークに接続するモバイル デバイスの約 35 % は従業員のセカンダリ デバイスです。最も多いデバイスの組み合わせは、iPhone または BlackBerry スマートフォンとタブレットです。会社負担の BlackBerry 携帯電話と自分の個人負担スマートフォンで接続している従業員もいます（図 2 参照）。3 台以上のデバイスを使用している従業員も一部います（通常はアプリケーションのテスト用）。

最も一般的なデバイスは iPhone と iPad ですが、この 2 年間で Android デバイスの数が急速に増えており、iPad の数に近づいています。スマートフォンとタブレット以外に、通常はオンコール ワーカーのチーム内で渡される音声専用の電話とポケットベルが約 7000 台あります。音声専用デバイスは、サービス契約の更新時にスマートフォンに置き換えられ、減少しています。

Belding は次のように述べています。「モバイル デバイスを会社のネットワークに接続したいというニーズが従業員の間でますます高まっており、複雑化しています。シスコのモビリティ サービス提供モデルにより、このようなニーズの高まりに対応することが可能になります」

生産性

シスコ IT は、新しいモバイル ユーザに関する 3 つの社内調査を実施し、モバイル デバイスによってシスコでの仕事がどのように改善されたか尋ねました。これらの調査によると、モバイル デバイス ユーザは、ラップトップが使用できないときにも情報にアクセスできたり、職場の電話やラップトップの Cisco Jabber クライアントから離れているときにも電話に出たりすることによって、平均で 1 日あたり約 15 分の生産的な時間を獲得しています。ユーザは、ほぼ常にスマートフォンを携帯し、好きなときに好きな場所から、予定表や電子メールの確認、問題の調査、ツールの検索、質問や問題への対応を実施できています。この 1 日あたりわずか 15 分の生産性向上でも、シスコ全体では年間 3 億米ドルの価値に相当します。

サービスおよびデバイス コストの削減

サービスおよびサポート コストは、シスコ IT のモビリティ予算の中で突出して高い割合を占め、デバイス自体のリース コストのほぼ 10 倍に達しています。BYOD プログラムにより、サービスおよびサポート コストとデバイス コストを削減する機会が得られました。

Belding は次のように述べています。「2009 年の経済低迷期に、シスコは、モビリティ サービス支出に関する完全な監査を実施し、コスト削減が可能な部分を突き止めました。使用されていなかった回線と、会社負担のモバイル デバイスが職務に実際には必要なかった従業員を特定するだけで、支出を 30 % 削減することができました」

自分のデバイスの持ち込みを希望する従業員が増えるのに伴い、会社負担の携帯電話は、この 2 年間で 3 分の 1 に減り、モバイル デバイス自体や導入管理および故障修理サポートに関するシスコ IT の総支出が減少しました。デバイス数の減少はコストの大幅な削減につながりました。シスコ IT は、このデバイス数の減少によって年間約 500,000 米ドルのコストを削減できました。さらに、BYOD プログラム導入前には、モバイル デバイスのさらなる需要の増大により、850,000 ドルの追加コストが発生すると見込んでいましたが、このコストも BYOD プログラムによって不要になりました。

シスコ IT は、音声およびデータ プラン サービス プロバイダーにターゲットを絞り、シスコに対する割引コストがコンシューマ向けモバイル サービスのコストと同じペースで下がり続けるように、ベンダー コストの削減交渉に懸命に取り組んでいます。また、シスコ所有の携帯電話を提供しているスマートフォン ベンダーとの契約の再交渉も行っています。ただし、従業員は会社所有のデバイスを保持することへの関心を失っており、自分のデバイスを購入することを望んでいます。

サポート コストの削減

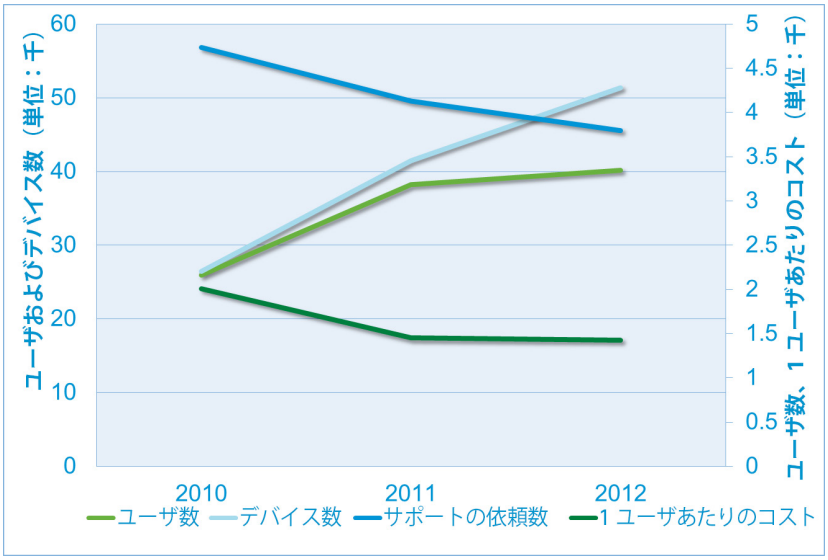
モビリティ サービスに関するオンライン ヘルプ リソースが利用可能になったことで、シスコのヘルプデスクが受け取る関連サポート ケースの数は着実に減少しており、2013 年初めの時点で 100 ユーザあたり 1 ヵ月でわずか 2.4 ケースでした。ユーザとデバイスの数が増え続けるなか、この 2 年間の総ケース数が 33 % 減少しました。ユーザ 1 人あたりのケース対

応負荷は 40 % 減少し、デバイス 1 台あたりのケース対応負荷は 56 % 減少したことも注目に値します（図 6 を参照）。2011 ～ 2013 年の間に各数字は次のように変化しました。

- シスコのモバイル デバイス数が 88 % 増加。
- シスコの新しいモバイル デバイス ユーザ数が 28 % 増加。
- モバイル サービス ケース数が 33 % 減少。
- ユーザ満足度が 28 % 向上（ユーザ サポート調査の測定による）。

「使用されていなかった回線と、会社負担のモバイル デバイスが自分の職務に実際には必要なかった従業員を特定するだけで、支出を 30 % 削減することができました」
– シスコ IT モビリティ サービス マネージャ Brett Belding

図 6. 2010 ～ 2012 年のユーザとデバイスの増加およびサポート ケースおよびユーザ 1 人あたりのコストの減少



得られた教訓

シスコ IT は、10 年以上にわたって従業員にモビリティ サービスを提供しており、その経験からいくつかの貴重な教訓を得ました。

ユーザ エクスペリエンスを損なうことなく、ネットワークへの BYOD アクセスを保護する。シスコ IT は、スマートフォンを使用して特定のトランザクションを処理したり、コラボレーションしたりすることは、ラップトップを使用した場合と同じくらい（それ

以上ではないにしても）簡単であることを非常に早い時期から認識していました。シスコにとってこの機能は、OS のネイティブ リソースをできる限り頻繁に使用すること、そして必要に応じて中間ステップを作成し、それをできる限り透過的にすることを意味します。

iPhone の場合、シスコ従業員は、証明書を使用してユーザを認証する Cisco AnyConnect クライアントを使用し、ユーザと企業データ間のデータ フローを暗号化して制御する必要があります。AnyConnect は、モバイル クライアントで開発されました。検証と証明書の設定が完了すると、AnyConnect は自動的に起動し、任意のツール（ブラウザや Cisco Jabber など）が起動されるたびにセキュアな接続を確立します。このプロセスは 1 ～ 2 秒かかりますが、いったん接続されるとスマートフォンがオフになるまで（短いネットワーク中断の間でさえも）接続されたままになります。シスコ IT は、証明書の代わりに SSL を使用してこの機能を提供できないか調査しています。

Subscriber Identity Module（SIM）カードについてユーザに教育する。従業員は、自分の BYOD サービスの制限を理解する必要があります。各携帯電話は、ネットワークに接続する前に、シスコ IT によって識別され、認定される必要があります。従業員からのトラブル コールには、新しい携帯電話を購入し、モバイル サービス情報を維持するために SIM カードを古い携帯電話から新しい携帯電話に差し替えたものの、期待どおりに動作しないというものが数多くあります。従業員は、新しい携帯電話にシスコ IT サービスをプロビジョニングする必要があることに加え、新しい携帯電話ベンダーが定めているサービス プランとデータ使用量が以前のものとは異なり、古い SIM カードと互換性がない（特に SIM カードが別のキャリアまたはデバイス用に設計されたものである場合）可能性があることを認識する必要があります。これらの違いは従業員のモバイル サービス料金に影響し、請求が予想外に高くなることがあります。この問題を防止するため、シスコ IT は従業員に携帯電話間での SIM カードの差し替えを行わないよう助言しています。

定期的な対象確認でコストを抑制する。シスコが電話サービスの料金を支払うとき、サービス コストが非常に高いことがあります。これは多くの場合、従業員が、iPhone または Android 携帯電話が一般に Blackberry よりもはるかに多くのデータを使用することを知らなかったり、ローミング料金が発生する場合を正確に把握していなかったりすることによるものです。シスコ IT は、従業員に携帯電話の通話時間を短縮するヒントを提供したり、超過料金が発生する可能性があることを伝えたりしています。たとえば、シスコ IT は、携帯電話から音声会議に参加するときに Cisco Webex のコールバック機能を使用するよう推奨しています。データ アクセスにローカルの Wi-Fi サービスを使用すると、ローミング料金を削減できます。

さらに、従業員は、スマートフォンをポータブル Wi-Fi ホットスポットとして使用すると、高額な追加料金がかかる可能性があることを認識していない場合があります。非常に高い料金を請求された従業員とそのマネージャには、シスコ IT からコストに関する月次フィードバックが送信されます。2 つの手続きを追加することでコストを抑制できる場合があります。1 つは、会社負担のアカウントがサービス更新日を迎えたときに、従業員が引き続き対象であることを確認すること、そしてもう 1 つは、社内で職務が変わった従業員に対して、新しいマネージャからモバイル サービスの承認を再度得るように義務付けることです。

時間の経過と共に高まるユーザ ニーズに備える。ある年にシスコ IT が従業員に提供できる最良のサービスに基づいて、その翌年にはさらに広範なサービスが要求されるようになります。2009 年、従業員から、会社が承認した、限られた数の Blackberry および Nokia デバイスと同様に、iPhone を社内デバイスとして利用する要望が出されました。2010 年、iPad とタブレットからイントラネット経由で会社のサービスにアクセスする要望、2011 年、Cisco Webex Meeting Center や Cisco Jabber IM などの社内アプリケーションをモバイル デバイスでサポートする要望、2012 年、既存のツールや今後登場するツールにアクセスできる、シスコ独自のモバイル アプリケーションを取り揃えたアプリケーション ストアに対する要望、そして 2013 年には、セキュアなクラウド ストレージとその他の外部クラウド サービスへのアクセスに対する要望がそれぞれ出されています。

また、職場に複数のデバイス（ラップトップと 1 台以上のタブレットまたはスマートフォン）を持ち込む従業員が増えるのに伴い、シスコ IT はいくつかの拠点で IP アドレスが枯渇しかけていることに気付きました。ネットワーク IT 運用チームは、ネットワーク接続デバイス数の増大に対処するため、特定の拠点でワイヤレス IP アドレスのリソース スペースを増やす必要がありました。

モビリティは目的ではなく手段であり、投資回収率と従業員満足度を最大化するには、明確な戦略とロードマップが必要です。

従業員のクラウド サービスへの要望に対応し、セキュアなクラウド サービスを提供する。シスコの情報セキュリティに関する企業ポリシーでは、従業員が仕事用の電子メールに含まれている機密情報を、Web ページ上でメッセージを閲覧できるようにする外部のファイル ストレージ クラウド サービスに転送または同期することは禁止されています。このようなタイプのサービスの個人利用が一般的になるのに伴い、従業員に対してセキュリティ リスクに関する特定の警告を行うことが必要になる場合があります。シスコ IT は、Cisco eStore を活用し、従業員が仕事を簡単かつ責任を持って遂行できるようにするオプションを提供するとともに、セキュリティの低いコンシューマ向けクラウド ツールと同じ操作性で、セキュアなツールを提供しています。

ユーザのセルフサポートに必要なリソースを提供する。ユーザは、ネットワーク アクセスや携帯電話のセットアップの問題についてどこにサポートを求めればよいかわからない場合があります。たとえば、シスコのヘルプ デスクに連絡すればよいのでしょうか。それとも携帯電話会社や携帯電話の小売店に問い合わせればよいのでしょうか。シスコ IT は、ユーザがサポート情報を自分で見つけられるように、社内オンラインのセルフ サポート コミュニティに継続的にコンテンツを追加し、サポート ページやディスカッション フォーラムの活用を奨励しています。クリックツーコールの機能を追加して、サポート リソースへのアクセスが利用できるようにもしています。さらに、シスコ IT は、苦情や問題に耳を傾け、ときにはユーザに必要な情報へのアクセス方法を示したり、インターフェイスを変更して情報をよりわかりやすくしたりすることで、コミュニティを改善しています。

デバイスのコンテンツを削除するポリシーおよび手順を定める。従業員が退職したときにモバイル デバイスに保存されている機密情報を管理することが重要です。従業員は、利用規則の一部として、雇用契約の終了時にモバイル デバイスのコンテンツが完全に消去されることに同意する必要があります。状況に応じてシスコ IT は、リモートからワイプを実行したり、従業員に消去手順を提供したりする場合があります。

次のステップ

Cisco eStore

シスコ IT は Cisco eStore を開発しています。Cisco eStore は、従業員が各デバイスに必要なあらゆる IT サービスやアプリを 1 ヵ所で見つけることができる便利なソリューションです（図 7）。基本的な BYOD サービスの申し込みや、スマートフォン/ラップトップへのアプリのインストールなどのさまざまなサービスを提供しています。新しいラップトップの注文や Cisco Virtual Office（CVO）経由のホーム アクセス サービスなどの IT サービスのインストールも可能です。また、シスコ従業員が複数のデバイスやプラットフォームから IT サービスやアプリにアクセスするための、シンプルで一貫性のあるユーザ エクスペリエンスを提供しています。サービスを利用開始するために必要なリクエスト等の手続きは全て eStore からできます。従業員が設定のために入力する必要はほとんどなく自動的にプロビジョニングされるため、従業員は、必要なソリューションを設定するために別のツールを利用する必要がありません。

eStore プラットフォームは、リクエストおよびプロビジョニング フレームワークを一元化する、シスコ IT の新しい効率的なアプローチであり、プロビジョニングに要する時間の短縮につながります。最終的に、すべてのシスコ IT ソリューションが eStore に掲載されるようになります。Cisco eStore は、Cisco Prime Service Catalog と Cisco Process Orchestrator を基盤としています。

図 7. シスコ IT eStore の初期表示

サポート可能なデバイスの範囲の拡張。Android は、シスコ IT の AnyDevice プログラム内で、セキュア デバイスとして次に対応する予定の OS です。Android は柔軟性が高く、各サービス プロバイダーが、Android OS を自社のネットワークに適合させ、競合他社から差別化するために独自のカスタマイズを加えてきたため、さまざまな独自の特徴や、悪用の恐れがあるセキュリティ脆弱性を持つバージョンが存在しています。従業員が未発表のデバイスを持ち込み始めたときには、シスコ IT はそれらのデバイスに対処します。

クラウドでのコンテンツの仮想化。さまざまなクラウド サービスが、コンテンツの仮想化および作業アプリケーション プラットフォームをクラウドで提供しています。このモデルは、あらゆる作業リソースに、場所やデバイスを問わず、セキュアにアクセスすることを望むシスコ従業員にとって非常に魅力的です。シスコ IT は、社内プライベート クラウド ソリューション（Virtual Desktop Infrastructure、Virtualization Experience Infrastructure、クラウド ストレージなど）と、契約に基づくセキュアなクラウド プロバイダー サービスの 2 つの異なるオプションを試しています。シスコ IT は、長期的に見て HTML5 がコンテンツおよびアプリケーション仮想化に最適なプロトコルになると予想しています。

BYOD は、広範なモビリティ戦略および IT のコンシューマライズ戦略のほんの一部に過ぎません。目標は、すべてのシスコ従業員が、時間/場所/デバイスを問わずに、あらゆる社内リソースにセキュアにアクセスできるようにすることです。

関連情報

企業における BYOD の財務面の影響の詳細については、https://www.cisco.com/c/ja_jp/about.html を参照してください。

モビリティ サービスに関するシスコ ソリューションの詳細については、http://www.cisco.com/jp/go/mobility/ を参照してください。

Cisco BYOD スマート ソリューションの概要については、
www.cisco.com/web/JP/solution/trends/byod_smart_solution/index.html を参照してください。

モビリティと BYOD をサポートする具体的な Cisco Validated Design については、http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/own_device.html を参照してください。

BYOD に関する Cisco Design Zone の録画ウェビナーについては、https://communities.cisco.com/thread/27357 [英語] を参照してください。

Cisco Identity Services Engine を使用して BYOD 環境を保護する方法については、http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11637/ps11195/qa_c67-703415.html を参照してください。

Cisco on Cisco ブログ（http://blogs.cisco.com/category/ciscoit/）[英語] には、モバイル コミュニケーションのトピックに関する記事が掲載されています。

その他さまざまなビジネス ソリューションに関するシスコ IT のケース スタディについては、「Cisco on Cisco: Inside Cisco IT」（https://www.cisco.com/c/ja_jp/solutions/cisco-on-cisco.html）を参照してください。

注

本書は、シスコ製品の導入から得られる利点について記載したものです。説明された結果およびメリットには多くの要因が影響しており、シスコは他の場合において同様の結果を保証するものではありません。

一部の法域では、明示または黙示保証の責任放棄を許可していないことがあり、その場合には本責任放棄声明は適用されません。

シスコは本文を現状のまま提供し、明示的または黙示的な商品性の保証、特定目的への適合性の保証を含む、明示または黙示の一切の保証もいたしません。

お問い合せ先

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