私用のモバイル端末を業務に活用

シスコは、スマートフォン、タブレットなど、社員の私用モバイル端末の業務利用にポリシーを制定し、コスト効率の高いモバイル端末サービスを実現しました。

シスコIT ケーススタディ／モバイル端末サービス: このケーススタディでは、業務電話やイントラネットへのアクセスにモバイル端末の利用を希望する社員のために、シスコIT が用意したネットワーク サービスについて説明します。シスコでは、以前からスマートフォンを生産性向上ツールとして活用しており、対象者と利用機種を限定して会社負担で提供していました。ところが、このスマートフォンに機能面で勝る新機種が続々と登場し、また、不況下でコスト削減を迫られる一方、社員が私用のモバイル端末から社内のネットワークに接続する際のセキュリティを確保する必要がありました。こうした変化に応えるべくシスコIT が取り組み、私用端末を業務利用するBYOD（Bring Your Own Device）に幅広く対応できるモバイル端末サービスを確立することができました。シスコIT の実事例が、モバイル端末サービスの導入にご関心のお客様のご参考になれば幸いです。

背景

2007年、シスコは、社員が業務に利用する携帯電話とそのサービスプランの承認、支払い、サポート方法の変革に着手しました。

「私用のモバイル端末を会社のネットワークに接続したいという要望が増え複雑になってきましたが、新しいサービス提供モデルは、こうした変化にも十分対応できます」

– Brett Belding（シスコITモバイル端末サービス担当マネージャ）

2000年代初頭、音声やデータの処理が可能な携帯電話が登場したのを機に、シスコIT はモバイル端末サービスを提供することになりました。このサービスは、携帯電話から 業務用の電子メール、予定表、連絡先リスト、イントラネット、専用アプリケーションへのアクセスを提供し、営業部門、カスタマーサポート部門、そして経営層の生産性を向上させることを意図していました。

当初のモバイル端末サービスでは、要件を満たす社員が使用する特定機種のモバイル端末とそのサービスプランに対して、シスコIT がオーナーとなり、費用の負担、サービスのセットアップ（プロビジョニング）、サポートの全てを行っていました。会社負担のモバイル端末の利用が承認された社員は、会社支給PC と同様のポリシーでシスコIT によるモバイル端末サービスを受けることができました。ただし、会社から経費の負担とサポートを受けるには、承認されたごく少数の機種から端末を選ぶ必要がありました。

私用の携帯電話から社内ネットワークへのアクセスは許可されませんでした。当時はまだ、必要性を否定し、セキュリティ面のリスクを危惧する声が多数を占めていました。このため、多くの社員が業務用と私用の2台の携帯電話を持っていました。そして、Apple iPhone のリリース後、私用携帯にもスマートフォンを選ぶ社員が増えていきました。

当時のモバイル端末サービスは、外部で開発された安全性の高いメッセージング プラットフォームで提供されており、ごく少数の機種のみを対象としていました。シスコIT の推奨は BlackBerry のプラットフォームで、このプラットフォームで世界中の様々なキャリア（携帯電話事業者）から提供されるBlackBerry 携帯サービスのすべてに対応していました。

概 要

背景
- 2007 年、業務利用の携帯電話と関連サービスの承認、経費負担、サポートの方法を変更

課題
- 利用者急増のスマートフォン／タブレット端末への対応
- 不況対策のためのコスト削減
- モバイル端末サービス提供プラットフォームの乗り替え

ソリューション
- OS の安全性に基づく端末認証
- モバイル端末のセキュリティを徹底
- 会社負担サービスの利用者を減らし、私用端末からのアクセスを許可
- セルフサポート用 Wiki サイトの提供

成果
- 30%のコスト削減、サービス対象のモバイル端末を 42,000 台に増大
- ユーザ数、端末数の増加に対応可能なサービス提供モデルの確立

教訓
- 未承認の端末からのアクセスブロックが必要
- SIM カードの利用について注意を促すこと
- 定期的にサービス利用要件を確認しコストを管理すること
- 社内サイトのサービスの利用を奨励すること
- 機密情報の漏洩を避けること
- セルフサポート用サイトを提供すること

次へのステップ
- 対応可能なサービス、機種を増やす
- VPN アクセスの向上
- セルフサポート用サイトを Wiki から社内 SNS サイト IWE へ移行

課題

2007年以降、三つの困難な課題が浮上し、シスコ IT はモバイル端末サービス戦略の鍵となる要素の見直しと改善を迫られていました。

第一の課題は、シスコ社員の間で人気が急上昇した Apple iPhone や、各社が続々と市場に投入してきたスマートフォンへの対応です。Apple iPad や Cisco Cius ビジネスタブレットなどのタブレット端末の参入もあり、社員の間でモバイル端末サービスへの関心が高まっていました。

第二は、世界的な不況の影響でシスコもコスト削減を迫られていたことです。会社負担の携帯電話サービスのコストや、機種ごとのテストに費やす時間と労力も見直しの対象となりました。このため、会社負担の端末とサービスの利用条件、サポート対象の機種と台数、社員のモバイル端末サービス利用に負担できる予算の額について検証が行われました。

第三は、プラットフォーム変革の時期を迎えていたことです。それまで、シスコIT はすべての機種に共通のモバイル メッセージング プラットフォームを利用していましたが、新型スマートフォンでは、それぞれに固有なプラットフォームが使われようになりました。「認証の時間とコストを削減するためにも、メッセージング プラットフォームを乗り換えたい」と、モバイル端末ソリューション担当 IT アーキテクトの Jason Freeth も考えておりました。

ソリューション

シスコ IT は、三つの課題に対処するにあたり、戦略とポリシーを次の四つの分野に定めることを決定しました:

- 端末の認証とセキュリティ確保の方法
- 提供するサービスとサービス提供プラットフォーム
- 社員とシスコ IT へのコスト還元方法
- セルフサポート用 Wiki サイトの提供

端末の認証基準

モバイル端末サービスの提供を開始した頃は、認定機種リストに加える前に、シスコIT が個々の機種に対して詳細なテストを実施していました。しかし、モバイル端末の種類は膨大に増え、当時のサポートモデルではすべての機種に対応できなくなりました。

現在では、新しい機種に対しては、シスコ IT が主に Apple iOS、Android、BlackBerry など、OS に基づいて認定を行っています。「各機種のセキュリティはOSで決まり、その他の注意が必要な機能もOSで提供されます。BlackBerry 以外の場合、シスコのセキュリティ ポリシーに準拠しているかも認定機種の選考基準となります。例えば、シスコでモバイル端末とMicrosoft Exchange 環境間の電子メールなどの同期に使われている、Microsoft ActiveSync に対応できることも条件です」と、シスコIT のモバイル ソリューション担当技術責任者 Paul Clements は述べています。

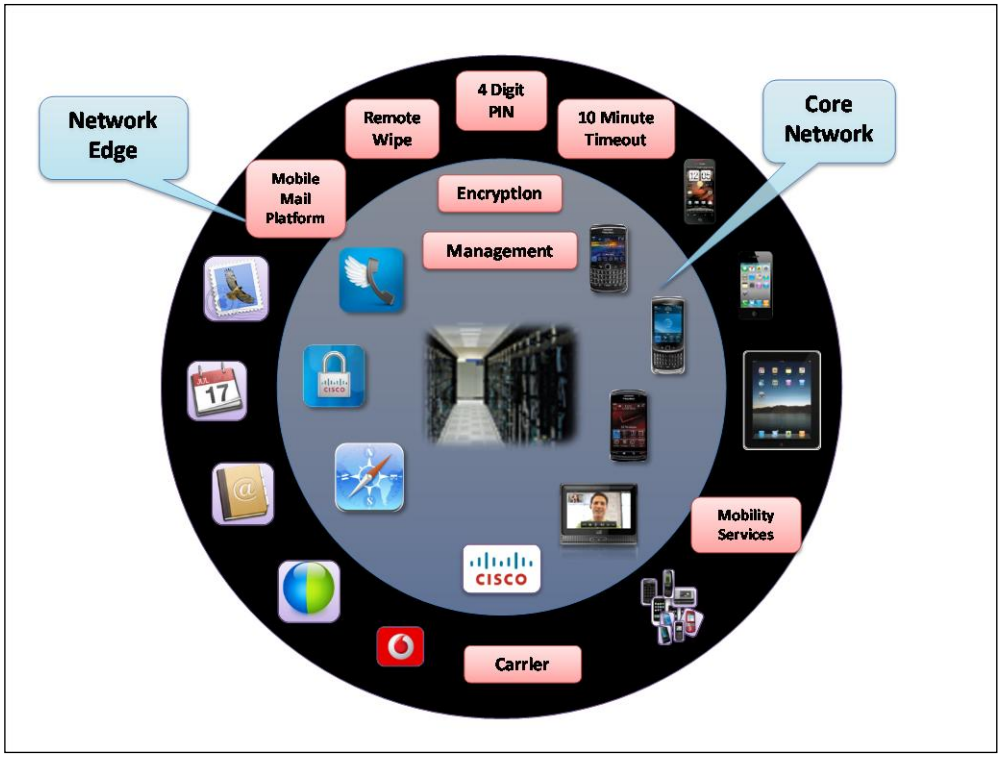
2011年半ばには、スマートフォン、タブレットなど、50種類のモバイル端末が認証機種のリストに挙げられました。幅広い可用性を備え、シスコ IT のセキュリティ要件のコンプライアンスを満たしていることが選択基準となりました。

「現在、セキュリティ基準を満たし、シスコIT のモバイル端末サービスを最も広範囲に利用できるのは、RIM BlackBerry、最新バージョンの Apple iOS 搭載の Apple 社製端末、そしてCisco Cius です。社内イントラネットのデータやアプリケーションにもアクセスできます。他のOS の機種の場合、アクセスできる機能が制限されているか、電子メール、予定表、連絡先リストへのアクセスのみに限定されています」と、シスコIT モバイル端末サービス担当マネージャ Brett Belding は語ります。シスコ IT が要求するセキュリティ要件を満足できない機種は、基本サービスにアクセスすることもできません。

モバイル端末のセキュリティ対策

モバイル端末のセキュリティ対策を徹底するうえで、サービス提供者が考慮すべき、二つの極めて重大な注意点があります。第一は、モバイル端末には連絡先やメールアドレスなど利用者の個人情報が保存されており、紛失時や盗難時にも漏洩を防ぐ対策が必要なことです。第二は、電子メールや Web アプリケーションにも機密情報が含まれており、社内サイトにアクセスする前に、ユーザとモバイル端末が認証を受ける必要があることです。つまり、端末内、アクセス先の、2種類の機密情報にセキュリティ対策が必要なのです（図1）。

図1　モバイル端末サービスのセキュリティ対策



「アクセスする端末が多いほど、多くのセキュリティ対策が求められるようになります」と、Freeth。ネットワークのエッジ（図1の外側の円）でモバイル端末サービスにアクセスするには、シスコIT が信頼性を検証する以前に、次のセキュリティ要件を満たしている必要があります。これらの基本的な要件を満足できない端末は、シスコのネットワークに接続することができません。

- 紛失時や盗難時に連絡先や電子メールなどの機密情報の表示を禁止する、データ暗号化機能が組み込まれていること
- データやアプリケーションへのアクセスに 4 桁以上のパスワードを要求すること
- 10 分以上利用を中断した場合、パスワードの再入力を要求すること
- パスワードの入力を 10 回以上失敗した場合、そのデータを自動的に削除すること

シスコのコアなネットワーク内のサービス（p.3 図 1 の内側の円）にアクセスする場合は、さらに厳しいセキュリティ要件が追加され、Cisco AnyConnect VPN クライアントの利用が必須となります。

また、利用するモバイル端末の電話番号や UDID（端末識別番号）をシスコ IT に登録する必要があり、登録された端末だけが社内サービスにアクセスできるようになります。シスコ IT は、登録された端末の保存済みデータ暗号化を行い、ソフトウェアバージョン情報や状態の確認などの端末管理を行います。

「セキュリティ要件を満たしていれば、端末自体が保護されるだけではなく、部外者がシスコのアプリケーションや機密情報に不正にアクセスするのを防ぐこともできます。また、保護されないスマートフォンやタブレットではアクセスできません。さらに、利用可能なサービスは各ユーザの端末に基づいて定義されているので、各自のスマートフォンやタブレットで保護できない情報にはアクセスできません」（Clements）。

関連CISCO製品一覧

モビリティ
- Cisco Mobile ソリューション
- Cisco Cius
- Cisco AnyConnect VPN クライアント
- Cisco Virtual Office

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

ビデオ & コラボレーション
- Cisco WebEx

ユーザが自分で設定を行う際のセキュリティ対策については、モバイル端末サービスの承認を得る際に確認する利用規約に明記されています。この利用規約には、Jailbreak（ルートレベルやコマンドラインへのアクセス）の防止、機密データの保護、OS の定期更新などのセキュリティ対策について規定があります。

提供するモバイル端末サービス

スマートフォンやタブレット端末の利用者急増のため、シスコIT は、対応機種とサービスを少数に限定する戦略から、多種多様な機種やサービスに対応する戦略に切り替えました。

以前の戦略では申請できる機種は限定されており、シスコIT は対象機種のみにサービスのセットアップを行い、規定のユーザ体験を提供していました。

新しい戦略では、社員が利用するモバイル端末サービスのタイプを選んでアクセスを申請し、所属部署が承認し経費を負担します。シスコIT が承認されたサービスのセットアップを行うと、スマートフォンやタブレットなど、複数の端末からサービスに接続できるようになります。同じ社員が他の私用端末も利用したい場合は同じアクセス認証番号を使って簡単に設定することができます。利用する端末の数が増えても、所属部署の課金が増えることも、その都度所属長の承認が求められることもありません。

今日では、多くの社員が第一のモバイル端末にスマートフォンを選択し、第二にタブレットを選択しています。2011年半ばの時点で、モバイル端末サービス利用者の15%が、ノートPC、スマートフォン、タブレットの3種類を所有しており、今後も3種類を使い分ける例が増えそうです。表1に、各端末のセキュリティレベルや機能に応じて提供されるモバイル端末サービスの一覧を示します。

表 1　シスコ IT 提供のモバイル端末サービス

基本サービス：社内メール、予定表、連絡先リストへのアクセス モバイル端末からの WebEx 会議参加 社内インスタントメッセージ（チャット） イントラネットへのアクセス：データ／アプリケーションの利用 デュアルモード音声のサポート：従量課金プラン対象外のワイヤレスLANを使用、各機種の Cisco Mobile ソリューション経由で提供	SNR (Single Number Reach) ：着信したコールを単一の電話番号を経由して転送する機能 ビジュアルボイスメール機能：ボイスメッセージングシステム Cisco Unity Connection のボイスメール受信ボックス内のメッセージの表示と操作ツールの提供 IWE（Cisco Quad で稼働する社内 SNS）へのアクセス

基本サービスでは、キャリアやワイヤレス LAN を経由しセキュリティを確保した状態で、シスコのメールサーバに直接のアクセスを提供し、多くの場合、各端末固有の機能で電子メール、予定表、連絡先リストを利用できます。このサービスには、多くの機種のOS に対応が可能な Microsoft ActiveSync プラットフォームを使用し、BlackBerry には、専用の BlackBerry Enterprise Server (BES) のインフラを使用します。

利用できるサービスは、機種によって異なります。例えば、ワイヤレス LAN を経由する通話に必要な 802.11 ワイヤレス LAN へのアクセスは一部の機種に限定されており、他の機種では VPN クライアントに対応できません。端末を購入する際に参考にできるように、シスコ IT は、主なモバイル端末の機種別対応サービスの一覧を提供しています。シスコ IT は、Cisco AnyConnect VPN クライアントや他社のモバイル端末管理ソリューションを活用して、提供できるサービスをさらに広げていきたいと考えています。

各サービスプランの対象者、経費の負担について

コストを効率的に管理するため、モバイル端末サービスの利用要件ポリシーが制定されました。このポリシーにより、通常、モバイル端末の購入とサービス利用の経費は利用者個人が負担することになりました。ただし、このポリシーは、部門や地域／国によって業務上必要な場合や制度上必要な場合に限り、例外が認められます。

ポリシーで定められた例外に相当する少数の社員が、会社が月々のサービス料を負担する「会社負担プラン」の対象となりました。ただし、端末デバイスの購入については、BYOD（Bring Your Own Device）を基本とし、社員の自己負担となります。コスト管理を徹底するため、コーポレートプラン（会社負担）の利用申請には、副社長の承認が必須となります。「回線ごとの利用料が月間で平均約120US ドルになるので、年間のモバイル端末サービスの経費総額は莫大な金額になります。このポリシーで、業務上本当に必要な社員だけが副社長レベルの承認を得てコーポレートプランを申請するようになり、そうでない社員のための負担を減らすことができました」（Belding）。

コーポレートプラン対象者の月々のサービス利用料金は、会社に直接請求されます。コストを抑えるため、シスコは世界中のキャリアに交渉を行いました。

コーポレートプランの対象とならない場合、自己負担で自分のスマートフォンからイントラネットにアクセスする「パーソナルプラン」の承認を所属長に申請します。このプランでは、アプリケーション、ファミリープラン、契約解除手数料、通話やデータ利用の超過料金などがすべ自己負担となります。

このパーソナルプランの場合も、モバイル端末サービスの利用は所属部門に課金され、シスコIT の開発、メンテナンス、モバイル端末サービスの提供の資金に還元されます。利用料の金額はシスコIT が最新インフラの整備のために支出した実際の金額に基づき、またユーザ数の増加を想定して、毎年調整されます。

セルフサポート

モバイル端末の機種、サービス、サービスプランは、国やキャリアによって、多種多様に存在します。種類の多さがユーザを混乱させ、シスコ IT にサポートのリクエストが殺到しました。

このため、シスコIT は、モバイル端末サービス用の社内 Wiki を提供し、次のような頻度の高い問題に関しては、ユーザ各自でこの Wiki サイトを参照できるようになりました:

- モバイル端末サポートの適用範囲、利用可能な機種、利用対象者の要件、コーポレートプランの利用申請方法、パーソナルプランでサービスにアクセスする方法
- FAQ サイト、ディスカッションフォーラムなど、特殊な機種の設定に役立つオンラインサポートの利用方法
- 紛失、盗難時の報告方法
- セットアップ方法、サポート手順の調べ方とヒント

これらの情報は社内 Wiki サイトで公開されたので、社員同士でトピックを更新し改善しながら助け合えるようになりました。シスコ IT はさらに、「参加意識が高まったところで、ユーザ同士でアイデアや提案を交換し合うコミュニティを構築しましたこのコミュニティは、どんなサービスが求められているかいち早く知るためにも役立ちました」(Belding)。

成果

「不況のためモバイルサービスの支出を徹底監査した結果、コスト削減が可能であると判断しました。利用のない回線と、コーポレートプランを適用する必要のない社員を特定するだけで、30% ものコスト削減を達成することができました」(Belding)。

「利用のない回線と、コーポレートプラン(会社負担のモバイル端末サービス)を適用する必要のない社員を特定するだけで、30% のコスト削減を達成することができました」

– Brett Belding(シスコITモバイル端末サービス担当マネージャ)

2011年半ば現在で、約42,000台のモバイル端末がシスコ IT のモバイル端末サービスの対象となっており、前年比で 40% の増加となりました。このうち7,000 台近くは待機業務のある社員に配布されていた通話専用の携帯電話とポケットベルが占めておりますが、サービス更新時にスマートフォンに変える例が増え、通話専用端末の利用者は減っています。

「私用のモバイル端末を会社のネットワークに接続したいという要望が増え複雑になってきましたが、新しいサービス提供モデルは、こうした変化にも対応可能です」(Belding)。

現在、70カ国以上でモバイル端末サービスが利用されており、利用者数が多い国はアメリカ、職種では、営業、カスタマーサポート、業務部門となっています。社内ネットワークに接続されるモバイル端末のうち約15%は、社員の第二端末です。第一端末に iPhone か BlackBerry のスマートフォン、第二端末にタブレットという組み合わせが多いようです。コーポレートプランで BlackBerry を、パーソナルプランで別のスマートフォンを利用している例もあります。

モバイル端末サービスのオンラインヘルプを充実させた結果、ヘルプデスクへのサポート依頼は少なくなり、2011年初頭の月間サポート件数は100ユーザにつきわずか3件となりました。

このサービス構築で学んだこと

10年以上もモバイル端末サービスを提供してきた経験から、シスコIT は数々の貴重な教訓を得ることができました。

VPN アクセスの安全性を確保すること　シスコの社内ネットワークの安全性と通信の機密性を保護するため、社員がシスコのオフィス外で接続する際にはCisco AnyConnect VPN クライアントを利用して安全性を確保することが義務づけられています。ただし、オフィスでセキュアなワイヤレスLANを利用する場合や、自宅で Cisco Virtual Office ルータを利用する場合は、モバイル端末から自由に接続することができます。

SIM カードについて注意を促すこと　通常、電話機の購入時に、サービス情報保持のため SIM（Subscriber Identity Module）カードを旧い電話機から取り出して新しい電話機に挿入することができます。しかし、キャリアや機種によってサービスプランやデータの利用方法が異なり、SIM カードとの互換性がない場合もあります。このため、機種によってはサービス料に影響し、高額な料金を請求されることがあります。この問題を防ぐため、シスコIT は携帯電話間で SIM カードを入れ替えないように注意を促しています。

サービス利用要件を定期的に確認しコスト管理を徹底すること　副社長以上の承認を必須とすることが、コスト管理の第一歩でした。そして、さらに徹底するため、二つの必須事項が加わりました。一つは、サービス更新時に利用要件を満たしているか再確認すること、もう一つは、職務が変わった際は異動先の所属長の承認を再度申請することです。

社内ネットワーク サービスの利用を奨励すること　シスコ IT は、携帯電話の利用時間を減らし超過料金の発生を防ぐためのヒントを提供しています。例えば、携帯電話から音声会議に参加する際はWebEx（SaaS 型 Web 会議アプリ）のコールバック機能（電話をかけてもらう機能）を利用することを薦めています。他に、ローミングをオフにして Wi-Fi サービスを利用すると利用料を減らせる場合があること、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利用すると追加料金が生じることなど、役立つヒントを提供しています。

機密情報の露出を防ぐこと　情報セキュリティに関するシスコのコーポレート ポリシーでは、社内メールを外部サービス（Apple MobileMe など）へ転送／同期してWeb ページでメッセージを閲覧することを禁止しています。この種のサービスは私用の端末では一般的に利用されていますが、特定通信を受信する際はセキュリティ上のリスクを考慮する必要があります。

セルフサポート資料を提供すること　ネットワークへのアクセスや設定の際に問題が生じた場合、どこにサポートを求めればよいのか、ユーザにはわかりにくいものです。シスコ、キャリア、販売店の、どこのヘルプデスクに電話すればよいのでしょうか？ シスコ IT は自分でサポート情報を入手することを奨励しておりますが、サポートWiki、サービス開始メールなどに最新情報の提供を続けています。しかし、特に設定時などにはヘルプデスクに問い合わせる方を好む傾向があり、また、中にはセルフサポート資料を全く利用しないユーザもおりますが、ほとんどは自分で解決できています。

端末内の情報削除のポリシーと手順を確立すること　退職者のモバイル端末に保存された機密情報をどう処理するかは、重要な問題です。このため、シスコでは、雇用終了時にモバイル端末内のデータの完全消去に同意することを義務づけています。消去の処理はシスコIT が遠隔操作で行うか、退職者本人が行えるようにマニュアルを提供しています。

次へのステップ

シスコIT は、今後も Cisco AnyConnect クライアントで VPN アクセスのセキュリティを強化するとともに、サービス、機種の対応範囲を広げていけるように、モバイル端末サービスの拡充に注力していきます。

また、オンラインのセルフサポート資料を充実させるため、モバイル端末サービス用の Wiki を Cisco Quad をプラットフォームとする社内 SNSサイト IWE のコミュニティに移動する予定です（図2）。IWE を活用することで、ニュースやスマートフォン比較など情報の共有、モバイル端末サービス申請用ポータルサイトへのアクセスが容易になり、世界中の社内ユーザからサポートを受けることが可能になります。

図 2　セルフサポート資料をオンラインで提供する Cisco IT Mobility Services コミュニティ

詳しい情報はこちら

モバイル端末サービスに関するシスコのソリューションについて、さらに詳しく知りたい方は、
www.cisco.com/web/JP/product/hs/wireless/ をご覧ください。

Cisco on Cisco ブログ（http://blogs.cisco.com/category/ciscoit/）から、モバイル コミュニケーションに関する記事もご覧いただけます。

様々なビジネスソリューションを提供するシスコ IT のケーススタディは、Cisco IT 内のCisco on Cisco ウェブサイト (www.cisco.co.jp/go/ciscoit)　からご覧いただけます。

付記

この文書に記載されている事例は、シスコが自社製品の展開によって得たものであり、この結果には様々な要因が関連していると考えられるため、同様の結果を別の事例で得られることを保証するものではありません。

この文書は、明示、黙示に関わらず、商品性の保証や特定用途への適合性を含む、いかなる保証をも与えるものではありません。

司法権によっては、明示、黙示に関わらず上記免責を認めない場合があります。その場合、この免責事項は適用されないことがあります。

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