

あらゆるデバイスからのリモート VPN 接続を実現する シスコのボーダレスネットワーク

シスコのVPN クライアント **Cisco AnyConnect** が、ノートPC、タブレット端末、モバイル端末からの安全なリモート接続を可能にしました。

「シスコでは、真のボーダレス企業になれるかということは問題ではありません。いつなれるのかが問題なのです。**Cisco AnyConnect** を利用することで、シスコのモバイルワーカーは、あらゆるデバイスから安全に社内ネットワークに接続できるようになり、ボーダレス化推進の道をまた一步、前進することができました」

Rami Mazid, Vice President of Client Services, Cisco IT

シスコ IT ケーススタディ / ボーダレスネットワーク / **Cisco AnyConnect セキュア モビリティ クライアント**: シスコのモバイルワーカーは、社外で仕事をするときも、ノートPC、タブレット端末、モバイル端末などからリモートVPN 接続を利用することにより、生産性を維持することができます。いつでも、どこでも、どのデバイスでも安全な接続を確保することが、シスコが推進するボーダレスネットワーク戦略の目標の一つです。このため、シスコ IT は、モバイルワーカーにシンプルなユーザエクスペリエンスを提供し、VPN クライアントのライフサイクル管理を簡素化することを目指しました。このケーススタディでは、VPN クライアントに **Cisco AnyConnect セキュア モビリティ クライアント**、セルフプロビジョニングのためのセンター側システムに **Cisco IOS ソフトウェア**、VPN トンネル終端装置に

Cisco ASA 5000 シリーズ 適応型セキュリティ アプライアンス を利用することによって、シスコがこの戦略目標を達成していった事例について説明します。シスコ IT の実事例が、お客様がボーダレスネットワーク戦略を策定する際のご参考になれば幸いです。

背景

シスコ IT は、場所やデバイスに制約されることなく柔軟に働くことのできるボーダレスなエクスペリエンスを世界中のシスコ従業員に提供するため、取り組んでまいりました。シスコのネットワークはオフィスの壁を越えて、デスクトップ、ノートなどPCの種類を選ばず、つながっていきます。さらに、お客様やパートナー様のオフィス、電車の中、ホテル、自宅の裏庭から、また、ノートPCだけではなく、タブレット端末やスマートフォンからも、場所やデバイスにとらわれることなく、つながりを広げています。ボーダレス化が求められる中、利用するデバイスを選択できることで、生産性が向上し、コラボレーションが手軽になり、仕事の充実感も高まるなど、様々な恩恵を得ることができます。

課題

1999年、シスコはノートPC で VPN 接続の提供を開始し、2007年にはスマートフォンへの対応を開始しました。これまでは、シスコ IT が全従業員に VPN 接続のアカウントを用意する必要があり、クライアント ソフトウェアのインス

ツールと定期更新には他社製のツールを利用していました。しかし、この方法だけでシスコのニーズを満足するのは難しくなってきました。そこで、シスコ IT は、生産性向上、コラボレーション促進を目指すボーダレスネットワーク戦略の一貫として、三つの目標を定めました。

第一の目標は、社内ネットワークに社外から接続する際のエクスペリエンスを向上させることでした。「ボーダレスなエクスペリエンスとは、どこからでも、どのデバイスでも、安全かつ確実に接続できることを意味します。しかし、それまでの VPN クライアントでは、接続可能領域を出て接続が切れると、手動操作で再接続し再認証を求める必要がありました」と、シスコ IT の顧客サービス担当テクニカルリードの Adam Cobbsky は回想しています。

第二の目標は、VPN ソフトウェアのワンタイムパスワードに要するヘルプデスクのコストを削減することでした。サポートコストは、年間50万USDにも達していました。パスワードによる認証ではなくクライアント証明書を用いることにより、このコストを削減し、堅牢な ID 管理フレームワークを確立することも可能になります。

第三は、利用数が増えているデバイスに対応する様々な VPN クライアントのサポートに要するオーバーヘッド(諸経費)を低減することでした。たとえば、Symbian OS 搭載 Nokia デュアルモードフォン、Windows Mobile OS 搭載デバイス、Apple iPhone、Android フォン、Apple iPad、[Cisco Cius ビジネスタブレット](#)や、Windows、Mac、Linux 搭載のデスクトップPC やノートPC への対応が必要でした。

「安全性が高く、デスクトップ/モバイルを問わず社内ですべてのプラットフォームに対応する、統合 VPN ソリューションが求められてきました。数ある既存のクライアントと、新しいクライアントやエージェントを統合することが当面の目標です。[Cisco EnergyWise Orchestrator](#)、[Cisco Wide Area Application Services \(WAAS\) Mobile](#) ソフトウェア、802.1X クライアント、VXI クライアントなどの統合が予定されています。統合することで、デバイスに制約されない一貫性のあるエクスペリエンスを提供し、デバイス間を途切れることなくスムーズに接続することができます」と、シスコ上級エンジニアの Plamen Nedeltchev は語っています。

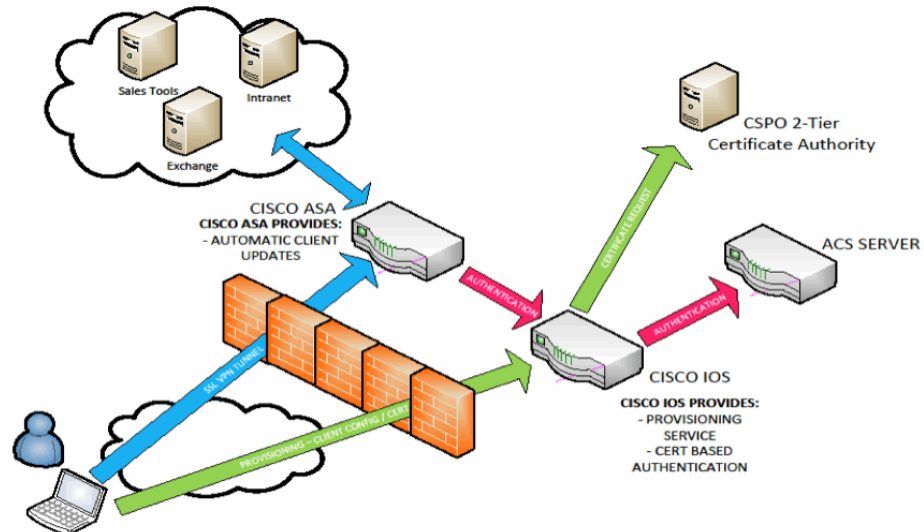
ソリューション

シスコ IT は、Cisco AnyConnect セキュア モビリティ クライアントを利用することで、これらの目標を達成していきましました。Cisco AnyConnect の VPN ソフトウェアを利用可能なので、まずは社内ですべての業務に使用されている Windows や Mac を搭載のPCから取り組んでいきました。「Cisco AnyConnect を利用することで、どこでも、どのデバイスでも安全に接続できるので、ボーダレスなエクスペリエンスが実現します。シスコ IT が一元管理し、常時接続することも可能になります」と、Nedeltchev。

常時接続が実現したため、パスワードを入力し接続を待つ煩わしさから解放されました。移動しながら仕事をするときも、Cisco AnyConnect が最適なVPNヘッドエンドとトンネリングプロトコルを自動的に選択します。また、リアルタイム アプリケーションの利用時にも優れたユーザエクスペリエンスを提供します。たとえば、自宅やホテルで [Cisco Unified Personal Communicator](#) を使用して[WebEx](#) 会議に参加する場合は、音声やビデオなど遅延の影響を受けやすいトラフィックに最適なプロトコルDatagram Transport Layer Security (DTLS)を自動的に選択します。

シスコ IT が Cisco AnyConnect の管理のために費やす時間はわずかなものでした。自分のPC からダウンロード用のサイトにアクセスして Cisco AnyConnect を選択すればセルフプロビジョニングを行えるので、全従業員約 70,000名分のプロビジョニングに要する時間がゼロになり、全社規模では莫大な時間を節減することができました。「このサイトは、デバイスのシリアル番号を検索しシスコの管理デバイスであることを認証できるようにプログラムされています」と、Cobbsky。入力後、自動的に作成された各自のアカウントと、プロビジョニングのセンター側システムに使用する Cisco IOS ソフトウェアのURLが記載された電子メールが届きます(図1)。この URL をクリックしワンタイムパスワードで認証を求めると、センター側システムからクライアント証明書が発行され、各自のデバイスで Cisco AnyConnect を利用できるようになります。このセンター側システムはまた、世界中で提供される様々な VPN 終端装置に関連するプロファイルをインストールすることもできます。

図1 シスコ IT による Cisco AnyConnect の展開



プロビジョニングが完了したら、どこからでもオフィスにいるのと変わらない状態で、社内ネットワークに接続することができます。Cisco AnyConnect モビリティ クライアントは、6台の ASA 5000 シリーズ適応型セキュリティ アプライアンスのうち1台を終端とする安全なトンネルを確立しますが、ユーザは全く意識する必要がありません。「将来的には、プロビジョニングにCisco IOS のセンター側システムの代わりに、Cisco ASA SCEP [Simple Certificate Enrollment Protocol] Proxy を用いることを計画しており、さらに簡素化する予定です」と、Cobbsky。

シスコ IT は、まずは新入社員や新しいPCの使用を開始する人を対象に、Cisco AnyConnect のダウンロードを勧めてきました。同じCisco ASA シリーズ適応型セキュリティ アプライアンスで終端する場合も含め、Cisco AnyConnect のインストール時に旧 VPN クライアントを消去する必要はありません。旧 VPN クライアントと Cisco AnyConnect セキュア モビリティ クライアントがそれぞれ、IPSec、SSL と、異なるプロトコルを使用するため、同じデバイスに共存することができるのです。

成果

ボーダレスなエクスペリエンスが実現し、生産性と満足度が向上

「シスコでは、真のボーダレス企業になれるかということは問題ではありません。いつなれるのかが問題なのです。Cisco AnyConnect を利用することで、シスコのモバイルワーカーは、あらゆるデバイスから安全に社内ネットワークに接続できるようになり、ボーダレス化推進の道をまた一歩、前進することができました」と、グローバルクライアントサービス部門の IT 担当副社長 Rami Mazid は述べています。

Cisco AnyConnect モビリティ クライアントは、ユーザに場所やデバイスの選択枝をあたえることで、シスコのボーダレスネットワーク戦略を支援します。「Cisco AnyConnect は、プラットフォームの統合化、ユーザエクスペリエンスの簡素化を推進していく流れの一環を成すものです。社内 SNS のプラットフォーム [Cisco Quad](#) がコラボレーションに必要なものを全て提供しているのと同じように、Cisco AnyConnect は、VPN 接続、セキュリティ、認証といった安全性の高いリモート接続を実現するために必要な機能を全て提供してくれます」(Cobbsky)。

接続が切れる度にワンタイムパスワードを入力し直す手間がなくなったと、世界のシスコから喜びの声があがっています。トンネル内の走行中や、Wifi や携帯電話のサービスエリア間のローミング時も、再入力の必要はありません。その日の業務を開始するときに一度だけパスワードを入力すればよいのです。「特に、ロンドンオフィスの電車通勤者は、接続が切れることが多く頭を抱えておりました。しかし今では、Cisco AnyConnect の VPN セッションが自動的に再接続してくれるので、パスワードの再入力を繰り返す必要はなくなりました。これで、通勤中も簡単に生産性を維持することができます」(Cobbsky)。

プロビジョニングと開発の簡素化、運用コストの節減

一元管理を行うことで、シスコ IT はクライアントソフトウェアのライフサイクル全体で時間を削減することができました。センター側システムが自動的に最新のソフトウェアをインストールするので、プロビジョニングとアップグレードに割いていた時間を省くことができました。さらに、VPN 接続ソフトウェアのトラブルシューティングにかかる時間も削減できました。

「これまでは、出向中のシスコのエンジニアは VPN クライアントの問題が発生したらシスコのオフィスに戻って再インストールする必要がありました。それが今では、シスコ管理のデバイスを使っている場合、インターネットカフェなど、どこからでも、プロビジョニング用のURLにアクセスしてソフトウェアのダウンロードを行い、5分以内に完全に操作可能な状態にすることができます」(Nedeltchev)。

「通常の営業日に、15,000以上のクライアントが一つのソフトウェア VPN クライアントで、シスコのイントラネットに同時に接続することができます。Cisco AnyConnect のクライアント証明書に基づいて実装されたデバイスプールを拡張することによって、シスコ IT は展開コストやサポートコストを増加することなく、安全性の高い方法で、より多くのクライアントをサポートすることができます」と、リモートソリューションのプロジェクトリーダーを務めるDavid Lacobacci も語っています。

End-to-End のセキュリティ

End-to-End の安全管理は、シスコのボーダレスネットワーク戦略の最重要事項の一つです。「スマートフォンのOSには高度なセキュリティ機能がありますが、適切に設定されていなければ効果はありません。Cisco AnyConnect は、認証機能と、PKI ベースのデバイス認証の両機能を備え、IT スタッフの労力が全くかからない完全自動化の方法を提供します。70,000名企業のシスコでセキュリティのソリューションを統合することは、莫大なコスト削減につながります」(Nedeltchev)。

Cisco AnyConnect はまた、管理対象外の資産も柔軟に利用できるように、安全上の課題にも取り組んでいます。現在では、登録済みのデバイスのみがシスコ IT のサポート対象となっています。SSL VPN セッションの確立を試みているデバイスが登録済か否かを確認するために、デバイスのシリアル番号の証明書をチェックします。「デバイスを登録することで、ユーザとデバイスが関連づけられてセキュリティを確認し、エンドユーザの責任を確認することもできます」(Nedeltchev)。

「Cisco AnyConnect のリリース時に、シスコ IT はCisco ASA 5000 シリーズ適応型セキュリティ アプライアンスの機能を利用して、デバイスが企業のセキュリティ基準に対してコンプライアンスを得られているか確認しました。基準を満たしていないデバイスはネットワークへの接続を許可されません」と、Cisco Security Programs Office グループの情報セキュリティアーキテクト Rich West は語ります。たとえば、スクリーンロック用のパスワードを入力していないユーザは、入力するまで VPN 接続を確立することができません。

また、Cisco AnyConnect を利用することで、社外の者がデバイスを盗んでシスコのネットワークに侵入するのを防ぐことができます。デバイスの紛失を届け出た時点で、シスコ IT は、センター側システムに登録されているそのデバイスのアクティブな VPN セッションを直ちに停止し、その後の VPN 接続をすべて禁止します。また、退職者のアカウントも簡単に終了させることができます。

次へのステップ

シスコ IT は、Cisco AnyConnect に関して次の事項を計画しています：

- [Cisco AnyConnect セキュア モビリティ ソリューション](#)を、セキュリティポリシーの強化に活用します。
- Cisco AnyConnect を構内用 [Cisco IronPort Web セキュリティ アプライアンス](#)に統合します。「将来的には、Cisco ScanSafe SaaS Web セキュリティ クラウド サービスで構内ソリューションを強化する予定です」(IT Customer Strategy and Success チーム 部長 Jawahar Sivasankaran)。
- IEEE 802.1X に対応し、ネットワーク基盤の ID 管理機能を提供します。モバイルワーカーがシスコの各事業所で共有するキオスクにログインし適切なアクセス権を得られるように、ユーザ認証にスマートカードを導入することを検討しています。
- シスコの [IPv6 導入戦略](#)にも Cisco AnyConnect を活用していきます。

「Cisco AnyConnect を導入するのは、それほど大変なことではありません。しかし、莫大な利益を得ることができません。ボーダレスなエクスペリエンスが実現すれば、どこでも生産性を上げることができ、またデバイスを選択する自由を得られるのです」(Nedeltchev)。

詳しい情報はこちら

様々なビジネスソリューションに対するシスコ IT の取り組みについては、シスコ IT 内の Cisco on Cisco ウェブサイト <http://www.cisco.com/jp/go/ciscoit> からご覧になれます。

Cisco AnyConnect モビリティ クライアントについて詳しく知りたい方は、<http://www.cisco.com/web/JP/product/hs/security/smc/index.html> をご参照ください。

ボーダレス エクスペリエンスの取り組みについて詳しく知りたい方は、<http://www.cisco.com/web/JP/solution/borderless/index.html> をご参照ください。

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。

©2011 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。(0809R)

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>

お問い合わせ先