# テレワーク：セキュアな環境を確保

## シスコが自社のセキュアなテレワーク環境を拡張した方法

シスコの従業員は、時間の差はあるものの全員テレワークを行っています。そのため、コロナ禍によって全員自宅で業務することになった際も、すでにテクノロジー、文化、プロセスは整っていました。大きな変化は、既存の VPN を拡張したことと、スプリットトンネリングを導入したことでした。この記事では、シスコの IT 部門とセキュリティ & トラスト部門がコラボレーションした、シスコのソリューションについて説明します。

# 目標：従業員が滞りなく業務を遂行できるようにする

シスコが最も重視したのは、従業員が自宅で効率よく業務を遂行するために必要なサービスやデータにアクセスできるようにすることです。それができなければ業務は停まってしまいます。確信を持ってリモートアクセスを許可するには、ネットワーク、モバイルデバイス、サーバ、アプリケーション、情報を保護し、従業員に適切なふるまいをとってもらう必要があります。

同時に、セキュリティソリューションとポリシーによって業務の進みが悪くなり、従業員がその業務を後回しにするようなことが起こらないよう注意する必要があります。従業員がシスコのポリシーを遵守するには、セキュリティを負担にするのではなく、むしろ業務を可能にするものでなければなりません。

シスコの Secure Remote Worker ソリューションには 2 つのポイントがあります。1 つは、ユーザのデバイスが信頼でき、コンテンツの利用や生成を認められるものかどうかを判断することです。もう 1 つは、シスコのデータセンターとクラウドで提供されているサービスを、従業員の自宅で安全に利用できるようにすることです。

# デバイスは信頼できるか。デバイスを 1 つのコンテナとして扱う

シスコのデータセンターまたはブランチオフィスで提供されているシスコ IT のアプリケーションを使用する従業員、協力会社、パートナーは、アプリケーションに VPN でアクセスできます。VPN ユーザは、各自の PC やモバイルデバイスに Cisco AnyConnect Secure Mobility Client をインストールしています。フルタイムのテレワーカーは、ハードウェアベースの VPN サービスを備えた Cisco Virtual Office を自宅に設置しています。

その他のユーザも、シスコ IT に登録されている社内管理の PC、個人用タブレット、スマートフォンから VPN に接続できます（BYOD の事例についてはこちらをご覧ください）。

## 多要素認証

従業員が VPN に接続する場合は AnyConnect を起動します。起動すると Cisco Duo が呼び出され、多要素認証(MFA)が行われます。Duo では、TouchID などの組み込みの生体認証機能から、物理トークンによって生成された安全なパスワードに至るまで、本人認証をするためのさまざまなオプションが用意されています。最も一般的なのは、従業員がユーザ名とパスワードを入力し、さらにモバイルデバイスに送信されるワンタイムコードを入力する方法です。ユーザが認証されると、AnyConnect Network Visibility Module（NVM）で、キャパシティとサービスのプランニング、監査、コンプライアンス、セキュリティ分析に使用するフローデータの収集が始まります。

## デバイスのセキュリテイポスチャの確認

AnyConnect クライアントは、従業員を認証する前に、最も近くで利用可能な VPN ヘッドエンドに接続します。AnyConnect とヘッドエンドは、デバイスで負荷の軽いセキュリティ ポスチャ チェックを行います。デバイスが最低限備えているべき要件には、最新バージョンのオペレーティングシステム、暗号化、パスワードで保護された 10 分での画面ロック、Cisco Secure Remote Worker ソフトウェアスイート（AnyConnect、Duo Umbrella、AMP for Endpoints）を導入していることなどがあります。モバイルデバイスの場合は、Meraki Systems Manager が発行した VPN アクセス用の証明書も必要です。

セキュリティ ポスチャ チェックは、世界中の遊園地で見られる「この高さに届かない人は乗れません」という看板と同様のチェックだと考えてください。デバイスがチェックをパスするとネットワークに接続されます。

シスコ IT では、Windows デバイスは Microsoft SCCM で管理し、Mac は JAMF、スマートフォンとタブレットは Meraki Systems Manager でそれぞれ管理しています。

## DNS レベルのセキュリティ

従業員が Web サイトにアクセスすると、Umbrella クラウドサービスは、接続が確立される前に悪意のあるドメイン、IP アドレス、クラウドアプリケーションをブロックします。DNS レベルで保護することで、マルウェア、フィッシング、ランサムウェアを防御できます。

Umbrella は、デバイスが VPN に接続されているかどうかにかかわらず機能するため、テレワークの際に特に役立ちます。シスコ IT では、セキュリティとプライバシーを両立する方法の例として、ブロックしているサイトにデバイスがアクセスするたびに通知するように Umbrella を設定していますが、それ以外のサイトにアクセスした場合には通知するようにはしていません。

## Advanced Malware Protection（AMP）for Endpoints

シスコ IT は長年、マルウェアがネットワークに侵入する前にブロックするエンドポイント保護ソリューション（ポイントインタイム検出）を利用していました。しかし、一部のマルウェアはどうしても侵入してしまうため、マルウェアを検出するには*レトロスペクティブ検出機能*が必要です。

そこで、ポイントインタイム検出とレトロスペクティブ検出を組み合わせたクラウドサービス Cisco Advanced Malware Protection（AMP）for Endpoints を利用しています。現在シスコ IT では、Windows、Mac、Linux、Android デバイスに AMP for Endpoints を導入しています。詳細については、こちらを参照してください。

AMP for Endpoints では、従来のエンドポイント保護ソリューションの 2 倍のマルウェアが検出されます。AMP for Endpoints は、PC 上の重要なサードパーティソフトウェアに脆弱性があった場合、そのソフトウェアが実行されていなくても特定できます。この機能は、テレワーカーが休暇を取得した場合などに便利です。AMP が感染を通知した際に自宅のデバイスを検疫する機能はテスト済みです。デバイスが VPN に接続されていなくても、「検疫スペース」に移すことができます。

2020 年初頭には、Orbital Advanced Search と呼ばれる AMP の機能をアクティブにし、セキュリティ調査と脅威検出をシンプルにしました。この機能を利用することで、特定の時点ですべての従業員のデバイスを調査し、脅威を検出できます。また、シスコ IT のインシデント対応チームは、インシデントの根本原因を迅速に特定するためにも Orbital を利用しています。根本原因を迅速に特定できれば、それだけ速く修復でき、リスクにさらされている期間を短縮できます。

# VPN の拡張

多くの企業が、在宅勤務、出張、バックエンドシステムの管理など、限られた用途で VPN を使用するように設計しています。しかしシスコでは、多くの従業員が 1 週間に一度はテレワークするため、大半の企業よりも堅牢な VPN を構築しています。主要な拠点では、たとえば、いずれかの建物で停電が発生しても、別の建物から全ユーザにサービスを提供できる体制がすでに整っています。また、拠点全体がダウンした場合、フェイルオーバーできる拠点があります。たとえば、米国中部の拠点は米国本社のバックアップ拠点になっています。

しかし、今回のコロナ禍のような世界的な事象が発生して、すべての従業員が毎日 VPN を使用するようになったことで、平時はバックアップとして機能していた拠点が、すでにキャパシティの上限に近い状態で稼働しているという事態に陥りました。そのため、コロナ禍でも業務を円滑に進めるためには、VPN インフラの拡張が必要でした。シスコ IT では、必要な場所に IP アドレス、VPN ハブ、ファイアウォールを追加することで拡張できました。

- **IP アドレス。**シスコ IT では、自動化したスクリプトを使用して IP アドレスの使用状況をモニタリングしています。そのため、感染が拡大し始めた最初の数週間に、デバイスのキャパシティに近づいている場所にアドレスを追加できました。
- **VPN ハブ。** 感染が拡大したことで、地域によっては新しい VPN ハブを導入する計画を早めました。近くのサイトに接続することで遅延が減少し、ユーザエクスペリエンスが向上します。
- **直接接続。**遅延をさらに少なくするために、Microsoft 社などのクラウドプロバイダーと同じ施設内に自社用スイッチを導入しました。スイッチとサービスプロバイダーの間は光ファイバで接続し、20Gbps の直接接続を確立しています。こちらからブログをお読みください。

- **サービスプロバイダーのキャパシティ。** シスコ IT では通常、必要時にバースト転送を行うオプションに加え、通常の使用量より少し高い認定情報レート（CIR）を契約します。たとえば大規模な拠点では、10 Gbps の回線に 2 Gbps の CIR を契約し、さらに最大 10 Gbps のバースト転送ができるようにしています。バースト転送にはコストがかかりますが、場合によっては、CIR を増やすよりも月々のコストは安くなります。シスコ IT では、最も経済的な方法を判断するために、バースト転送が発生している回線の数とその時間を確認しています。ヒント：現在契約している回線がバースト転送に対応しているか、サービスプロバイダーに確認することをおすすめします。感染拡大時に VPN を拡張した際にシスコ IT が調査したところ、中国のサービスプロバイダーで転送レートが制限されていることがわかったため、他の回線に変更することにしました。

詳細については、「Q&A：世界中のシスコ従業員がテレワークに移行した際に、どのように VPN を全従業員に提供したか？」をお読みください。

## 特定のクラウドサービスに対するスプリットトンネリング

コロナ禍によって世界中でテレワークすることになり、スプリットトンネリングに関する現在の計画を早めました。2020 年 3 月初旬の 3 日間で、シスコのデータセンター宛てのトラフィックは VPN 経由にし、特定のクラウド向けトラフィックはインターネットに直接転送するように VPN クライアントを設定しました。特定のクラウド向けトラフィックについては VPN を経由させないことで速度が向上し、エンタープライズ ネットワークおよびインターネットへのリンクに対する負荷が軽減されます。

ただし、すべてのインターネットトラフィックをスプリットトンネリングすると、大きなリスクにさらされます。たとえば、短時間の休憩中に Facebook や Twitter のリンクをクリックしただけで、PC がマルウェア感染リスクにさらされ、会社全体に拡散する可能性があります。そのためシスコ IT では、ほとんどの一般的なトラフィックをいったんシスコに戻し、階層化されたセキュリティスタックを適用したいと考えています。シスコ IT はリスクを最小限に抑えるため、データの安全性や Duo MFA との互換性といった厳格なセキュリティ基準を満たしている特定のクラウドサービスに対してのみ、スプリットトンネリングを適用しています。対象となるサービスには、Cisco TV、Office 365、Box、Apple 社および Microsoft 社の更新プログラム配信サービスなどがあります。これらのクラウドサービスは、シスコのインターネットトラフィックの約 3 分の 1 を占めています。

スプリットトンネリングの実環境でのテストは、2020 年 3 月初旬に行われました。その際シスコの CEO が、コロナ禍に関する最初の Q & A を、クラウドサービスである Cisco TV で実施しました。10 万人以上が同時にライブでビデオストリームを視聴しました。VPN スプリットトンネリング機能がなければ、一部の ISP リンクが飽和状態になり、速度が大きく低下しているところでした。

# 変更管理

2020 年 3 月にオフィスを閉鎖する前に、シスコ IT は各チームのリーダーに対して、パスワードのリセット、ビジネスアプリケーションの更新、オフィス勤務最終日前の VPN へのログインテストを促す電子メールを部下に送信するよう呼びかけました（最新のセキュリティパッチを適用しない限り、ユーザはネットワークにログインできません）。Cisco Virtual Office（自宅用ルーター）ユーザに対しては、セキュリティパッチを確実に受け取れるように、夜間もデバイスの電源をオフにせず、常に電源を入れたままにしておくように指示しています。

また、各チームのリーダーと各地域の IT チームには、テレワークに関する以下のヒントを従業員と共有するよう指示しました。

- 社内ツールを使用して PC の状態を確認する。
- 必ず最新バージョンの AnyConnect を使用する。
- Cisco Duo Security の機能を確認できるサイト（シスコ IT がセットアップ）にアクセスして、機能を確認する。
- アプリケーションのアップグレードとバックアップは、VPN が輻輳しないように通常の勤務時間外にスケジュールする。

# 今後の対応

シスコ IT では、Secure Remote Worker ソリューションの強化を続けていきます。以下を計画しています。

- 証明書を使用して、Windows デバイスおよび Mac デバイスでの VPN のユーザエクスペリエンスをシンプルにする（モバイルデバイスと同様）。
- 新規採用者の受け入れ処理と PC の調達プロセスを見直す。新規採用者や新規採用者の受け入れ担当者がオフィスに来られない場合のプロセスが必要。
- パブリッククラウドに Desktop-as-a-Service（DaaS）を導入する。感染拡大によるロックダウン中には、米国外の協力会社に仮想デスクトップ環境を提供し、物理的な PC を提供することによるリスクと物流上の問題を回避する。

© 2020 Cisco and/or its affiliates. All rights reserved. シスコおよびシスコのロゴは、米国およびその他の国におけるシスコおよびその関連会社の商標または登録商標です。シスコの商標の一覧は http://www.cisco.com/jp/go/trademarks でご確認いただけます。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。