経営者にこそ知ってほしい

アフターコロナの
最新セキュリティ事情と対策

近年、サイバー攻撃はますます活発になっています。
身代金要求による財務への影響、情報漏えいによる企業イメージの毀損や
訴訟などさまざまなリスクが内在し、セキュリティ対策はいまや
経営課題として取り組むべきものとなっています。世界の社会的な情勢が
変わりつつある今後、改めてどのようなセキュリティリスクが
考えられるでしょうか。適切な優先順位でセキュリティ対策に投資し、
従業員が安全に働けるようにするために、本ホワイトペーパーでは
「アフターコロナ」の時代で考えるべきセキュリティトレンドと
それに対する対策を解説します。

必ず知っておきたいセキュリティの最新事情

中小企業もいまやサイバー攻撃の標的に

サイバー攻撃は増加している

社会全体のデジタル化が進展し、テレワークやオンライン授業など新しいスタイルが採用されています。それに伴い、これまであまりデジタルに慣れていなかった人たちもさまざまなITサービスを利用するようになり、インターネットに接続される機器やアプリケーションなども増加しています。

こうした脆弱なところを狙ったサイバー攻撃が急増しています。情報処理推進機構（IPA）が公表した「情報セキュリティ10大脅威2021」では、組織に対する脅威として、1位に「ランサムウェアによる被害」、2位に「標的型攻撃による機密情報の窃取」が挙げられています。これらは以前から大きな課題となっていましたが、3位には新たに「テレワーク等のニューノーマルな働き方を狙った攻撃」がランクインしました。

さらに、一般社団法人 JPCERTコーディネーションセンターの調査によると、同センターに寄せられたセキュリティインシデントの報告件数は、コロナ禍とテレワークが広がり始めた2020年3月頃から急激な勢いで増加していることがわかります（右図）。

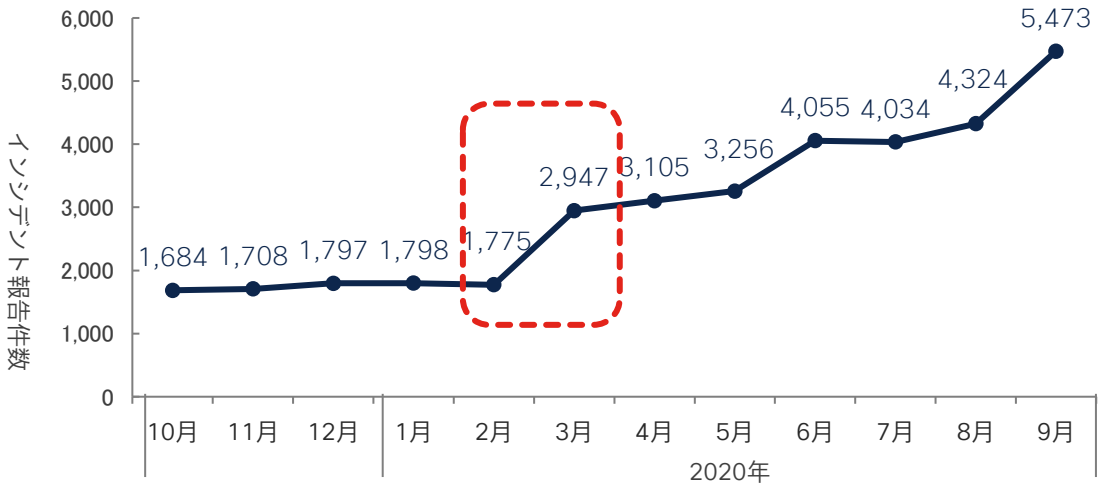
中小企業が狙われる理由

サイバー攻撃は、セキュリティ対策が間に合っておらず手薄なところ、利用者のリテラシーが低いところなどを集中的に狙ってきます。加えて、その手口はますます巧妙化しており高度化しています。

その際、サイバー攻撃のターゲットは「必ずしも大企業だけではない」ということを強く認識しておく必要があります。

情報漏えいやサイバー攻撃のリスクは大企業ほど高くなるのではという考えを抱く人もいるかもしれません。確かに、世間では大企業の情報漏えい事件などが報じられることが多いのですが、大企業への攻撃を仕掛けるための“踏み台”として、大企業と取引する中小企業やテレワーク中の個人が狙われる事例が発生しています。いまや決して中小企業も無関係ではなくなっているのです。そこで次ページから今後特に気をつけたいセキュリティのポイントと対策を紹介します。

テレワークが普及し始めた時期からセキュリティ事故が急増



出典：JPCERT/CC インシデント報告対応レポート[2020年7月1日 ~ 2020年9月30日]

アフターコロナで気をつけたいポイント①：ネットワーク

社内へのリモートアクセスが攻撃の対象に

セキュリティの盲点となるVPN

テレワークと言えば、育児や介護などを理由とする一部の従業員を対象とした制度と考える企業も少なくありませんでした。しかし働き方改革やコロナ禍をきっかけに、あらゆる従業員の一般的な業務・勤務形態として拡大しています。アフターコロナの世界でもこの働き方は継続していくでしょう。

しかし、これに伴ってセキュリティ被害も増大しています。テレワークでは自宅などから社内のシステムにアクセスすることになりますが、その途中経路となる端末やネットワーク機器が狙われるのです。中でも見落としがちなのが、リモートアクセスの方法として多くの企業で広く用いられるVPNです。VPNを利用すれば、基本的に端末と社内システムの間は盗聴されず安全に通信できますが、それは「正しいユーザーがアクセスしているか」までを保証するわけではありません。つまり、なりすましへの注意が必要です。

VPNの脆弱性を狙った サイバー攻撃の被害例

実際に2020年には、VPN機器に潜む脆弱性が原因でサイバー攻撃に遭い、ユーザーのアカウントやパスワード情報が流出し、社内への不正アクセスが発生してしまった事例がメディアで度々報道されています。なお脆弱性情報は提供元のベンダーから公開されますが、対応を行わないまま放置した場合に、このようなサイバー攻撃の被害にあってしまうのです。

実際に下記に示す例のように、多くの企業がVPNの脆弱性を狙ったサイバー攻撃の被害を受けています。

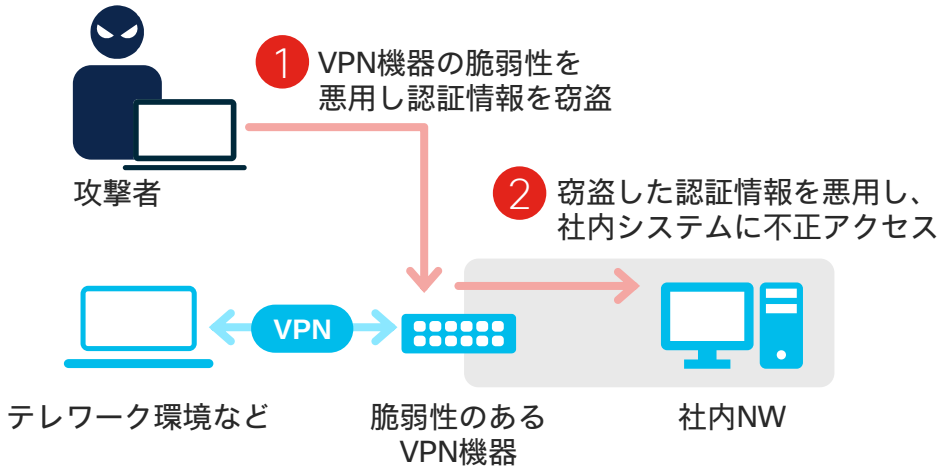
●製造系企業：VPN機器の脆弱性を突かれ、社外からのリモートアクセスを管理するシステムに対しての不正アクセスがあり、リモートアクセスのログ情報が流出した。これに伴いVPN機器の使用を停止。

●金融系企業：社員のアクセスログ情報が不正アクセスを受けて窃取

●教育機関：VPNの脆弱性を突かれ、事務職員のテレワーク用のシステムが不正アクセスされ、事務職員9名分のIDが漏えい

VPNの脆弱性を狙ったサイバー攻撃は、機密情報や顧客の個人情報にもつながるために注意が必要です。

VPNが原因で発生する代表的なセキュリティインシデントの例



安全な社内ネットワークアクセスを実現する

VPN機器をより安全に使う方法

先述したVPN機器の脆弱性はメーカー側から提供される修正用の更新プログラム（パッチ）を適用することで対策することができます。つまり、すでにパッチが提供されているにもかかわらず、適用しないまま放置していることは今まで以上に重大なリスクを招きかねません。メーカー側からの通知や情報公開を常にチェックするとともに、アップデートを見落としたままになっているVPN機器が残っていないか、あらためて確認してください。

そして、脆弱性管理の重要性はVPN機器に限った話ではありません。ここ数年間で、世界中で数多くの被害をもたらしたランサムウェアの中にも、攻撃者がWindows PCに存在する脆弱性を利用して引き起こしたものがあります。つまりは、脆弱性をしっかり対処していれば防ぐことができたものが数多くあるということです。

より安全な社内ネットワークアクセス

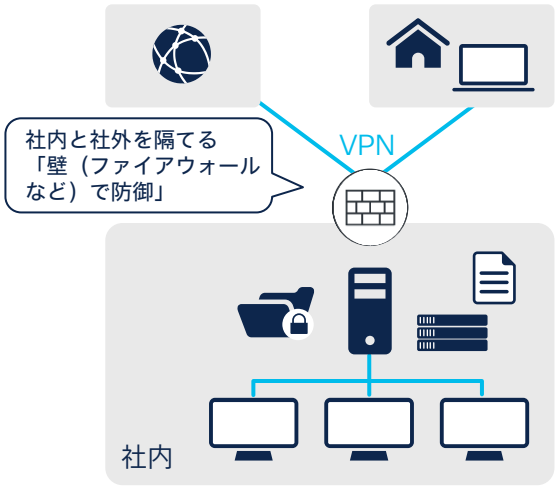
VPNの不正アクセス対策は、上述のVPN機器の脆弱性対策を行うことはもちろん、認証情報が人的な不注意によって漏えいしてしまう可能性を考えて、認証自体を強化する方法もあります。例えば、VPN接続の際にID＆パスワードのほかに、生体認証やモバイルデバイスなどを組み合わせた多要素認証を施したり、接続許可するデバイスを限定したりなどの対策も有効です。

「ゼロトラスト」の考えも取り入れる

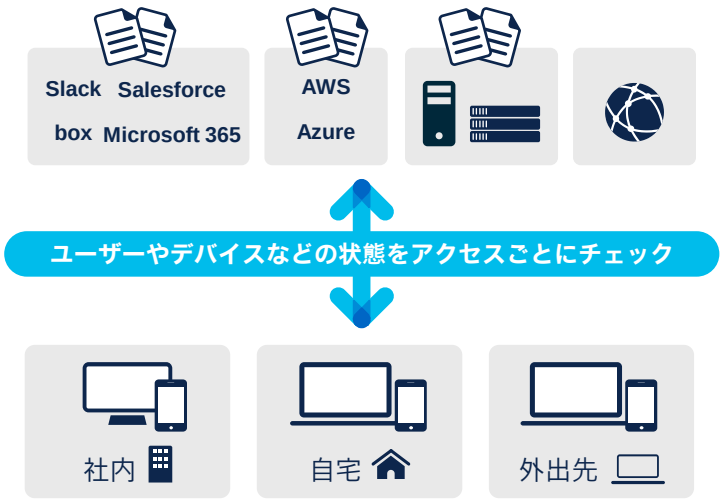
従来のセキュリティの多くは、社内と社外に「関所」となる境界線を設け、社内に入ったものは安全とみなす、いわゆる「境界線防御」の考え方が主流でした。しかし、テレワークが広まった現在では、この考え方で社外の端末の安全性は担保できません。そこで近年注目されているのが、ゼロトラストネットワークアクセス（ZTNA）と呼ばれる方法です。

ZTNAでは例えば、アクセスしてくるものを「信用せずにすべて検証する」という考え方をもとに、ユーザーが社内のシステムやクラウドサービスを利用しようとするたびに、認証やデバイスチェックを行うものです。VPNは引き続き有用ですが、それだけではなくこのような考え方をベースとした対策を取り入れるのも有効でしょう。

従来の「境界型」による防御と「ゼロトラスト」による防御の違い



「境界型防御」の考え方



「ゼロトラスト」の考え方

アフターコロナで気をつけたいポイント②：脆弱な自宅環境

社内と同等のネットワークセキュリティを

自宅ネットワーク環境の課題

テレワークは実質的に在宅勤務という形で行われることが多いでしょう。しかしオフィスのネットワーク環境と違って、従業員が自宅で利用しているネットワーク環境は十分なセキュリティ対策が施されていない場合があります。それにより、誤って不審なサイトへ接続してしまう可能性もあります。

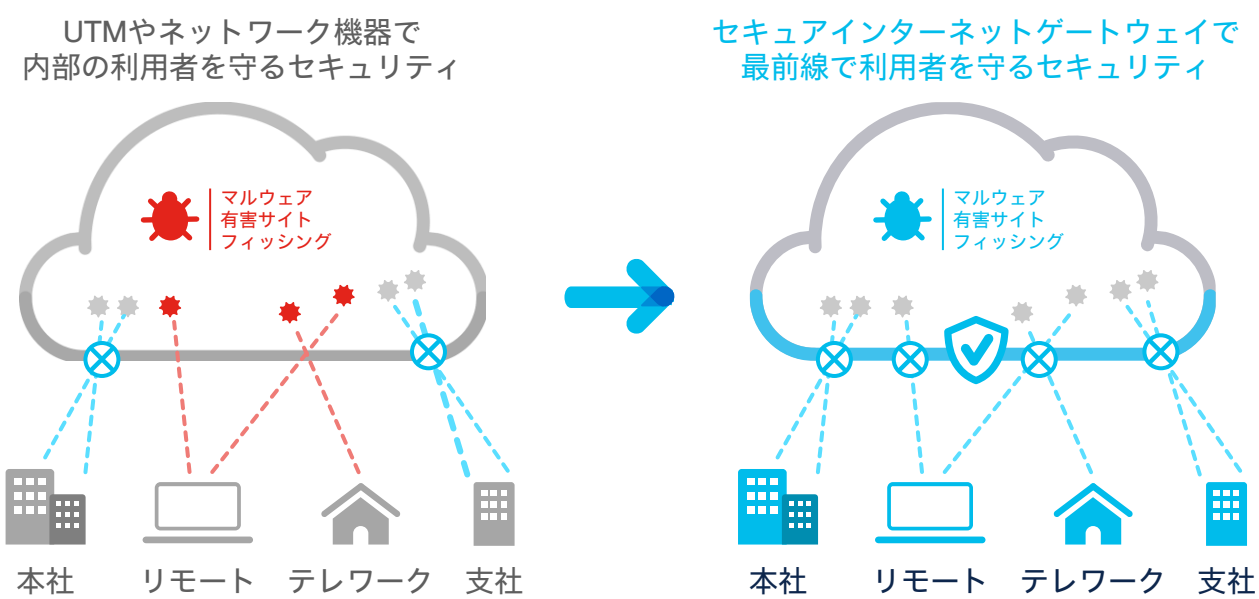
在宅勤務環境では、もし自身のPCに不審な動きが発見されたとしても、社内のようにすぐ隣の人に気がするに相談することも難しいでしょう。また在宅勤務時に社用PCでSNSを利用し、同サイト経由で本人の知らない間にマルウェアに感染してしまい、その後社内ネットワークに接続した際に感染を拡大してしまった事例も報告されています。在宅時のインターネット利用には思わぬリスクが存在しているのです。

自宅ネットワーク環境に依存しない対策

在宅勤務だけに限らず安全なテレワークを実現するためには、その場所でのネットワーク環境に依存しないセキュリティ対策を施す必要があります。そのために、クラウド型のセキュアインターネットゲートウェイを利用することも有効な対策の1つとなります。これにより、ユーザーがどこにいても、どのデバイスを用いても、たとえ VPN に接続して社内を経由しなくても、安全なインターネットアクセスを実現できます。

このようなソリューションでは、具体的にインターネットにアクセスする際に宛先の安全性を確認して、マルウェアやランサムウェアの感染、フィッシングサイトへの誘導といった脅威から防御します。クラウド型で提供されるセキュアインターネットゲートウェイは新たな機器の調達・設置が不要、在宅勤務環境へ容易に導入できることに加え、全社的なセキュリティポリシーを一元化し、すべてのテレワーク環境に対して一括適用できるといったメリットがあります。

インターネットアクセスを社内・社外で同じく安全にする方法



アフターコロナで気をつけたいポイント③：端末管理

多様化するデバイスを漏らさず管理する

社内外の端末管理の抜け漏れに注意

テレワークやハイブリッドワークなど場所を問わない働き方が多くの社員に定着していくに伴い、PCだけでなくその時々の場所やシーンに応じてタブレットやスマートフォンなど複数のデバイスを使い分けるケースが増えていきます。PCに関しても必ずしも会社支給の端末だけを利用するとは限らず、個人所有の端末（BYOD：Bring Your Own Device）を利用する可能性もあります。また一方でオフィスにも各種センサー、ネットワークカメラなど、さまざまなIoT端末が導入されスマート化が進んでいます。

多様化するデバイスすべてに対して適切なセキュリティ対策が必要ですが、その前にまず社内にどのような機器が存在し、どのようなソフトウェアが使用されているのかを把握できなければ、先に解説したVPN機器やPCなどの脆弱性対策を行うこともできません。

資産管理はセキュリティ対策の基本であると理解する

セキュリティ対策といえば、アンチウイルスなどサイバー攻撃を直接防御する、わかりやすいものを第一にイメージしがちです。しかし、「守るべきものは何か」すべて知っていなければ、本当に守りたいものも守れません。そのためには、まずは社内でどのようなハードウェアやソフトウェアが利用されているのかを把握して適切に管理する、いわゆる「IT資産管理」を確実に実施する必要があります。

アメリカのインターネットセキュリティ標準化団体CIS（Center for Internet Security）では、「最初に最低限行わなければならないもの」を明らかにして、セキュリティ対策をシンプルにするために作成したセキュリティ対策のフレームワーク「CIS Controls」を提唱しており、その最も基本となる「Basic」の第1、第2に挙げられているのが、「資産管理」なのです。

自社内でどんなIT資産が利用されているか、まずはしっかり棚卸を行って把握したうえで必要なセキュリティ対策を考えるべきでしょう。

「CIS Controls 7」による20のセキュリティ対策フレームワーク

Basic

1. ハードウエア資産のインベントリとコントロール
2. ソフトウエア資産のインベントリとコントロール
3. 継続的な脆弱性管理
4. 管理権限のコントロールされた使用
5. モバイルデバイス、ラップトップ、ワークステーション及びサーバに関するハードウエア及びソフトウエアのセキュアな設定
6. 監査ログの保守、監視及び分析

Foundational

7. 電子メールとWebブラウザの保護
8. マルウエア対策
9. ネットワークサポート、プロトコル、及びサービスの制限及びコントロール
10. データ復旧能力
11. ファイアウォール、ルータ、スイッチなどのネットワーク機器のセキュアな設定
12. 境界防御
13. データ保護
14. Need to knowに基づいたアクセスコントロール
15. 無線アクセスコントロール
16. アカウントの監視及びコントロール

Organizational

17. セキュリティ意識向上トレーニングプログラムを実施する
18. アプリケーションソフトウエアセキュリティ
19. インシデントレスポンスと管理
20. ペネトレーションテスト及びレッドチームの訓練

アフターコロナで気をつけたいポイント③：端末管理

対策が見過ごされがちなIoTデバイス管理も必ず行う

IoTデバイスも攻撃の対象に

近年では、社内で用いられるデバイスにはIoT機器も含まれるようになりました。それは、セキュリティ対策の対象が増えたとも言えます。情報処理通信機構が観測したサイバー攻撃のうち、約半数がIoT機器を狙った攻撃であるとしています。今後さまざまなモノがインターネットに接続するようになり、場合によっては社内のIT部門を通さずに導入されるものも増えてくるでしょう。その中で、まず社内で使われているIoT端末をしっかり洗い出した上で、次のようなセキュリティ対策を行うことが重要です。

1. 適切なIDとパスワードを設定し直す

IoT端末は、工場出荷時に初期値として設定されているIDやパスワードをそのまま利用しているケースが少なくありません。こうしたIDやパスワードは世間に公開されているのとほぼ同じであり、サイバー攻撃者もさまざまなIoT端末について情報を入手しています。実際にIoT端末への侵入する手口として多く使われているのが、この初期設定のIDとパスワードの悪用なのです。

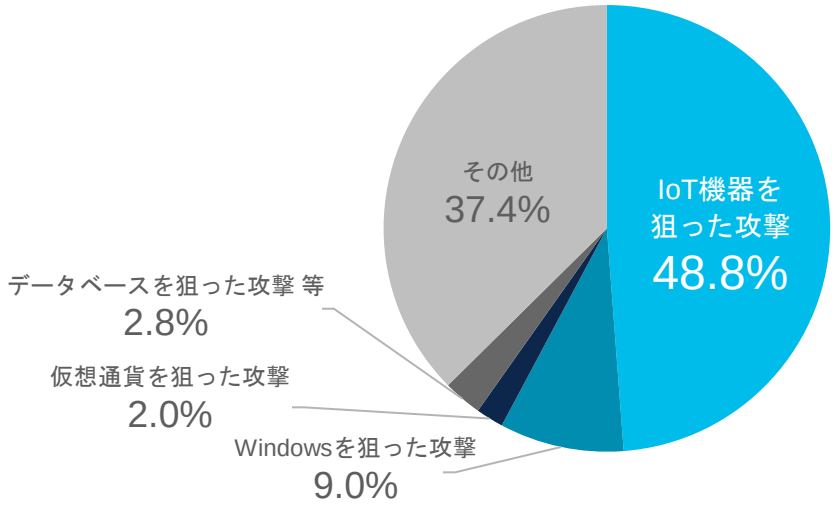
したがってIDとパスワードを変更しておくことは最低限の対策として必須です。加えて言えば、IoT端末を直接インターネットに接続することを避けるべきです。PCと同様にファイアウォールの配下で運用することをお勧めします。

2. 継続的にアップデートを行う

PCやスマートフォンと同様にIoT端末も高度なIT機器です。そのため、製品発売後に発覚した不具合や脆弱性を解消するためのパッチ（修正プログラム）が配布さ るなど、導入後もソフトウェア（ファームウェア）の 継続的なアップデートが必要になることもあります。 これを素早く適用しておかないと、サイバー攻撃者にとっての格好のターゲットにされてしまいます。

自社内で運用しているIoT端末について、メーカーのWebサイトのサポートページなどを通じて定期的にアップデート情報をチェックし、常に最新の状態に保つこともセキュリティ対策の必須項目と認識しておくべきです。

約半数がIoT機器を狙った攻撃



出典：総務省サイバーセキュリティタスクフォース事務局「サイバー攻撃の最近の動向等について」（令和２年12月３日）

アフターコロナで気をつけたいポイント④：不正アクセス

クラウドサービスは「なりすまし」に特に注意

クラウドサービスならでの利用上の注意点

中小企業の間でもクラウドサービスの利用が広がっています。特にコロナ禍でテレワークに移行した中で多くの従業員がオンライン会議やグループウェアなど、さまざまなクラウドサービスの便利さを体験しました。オフィスワークに戻ってからも、アフターコロナの働き方でもクラウドサービスは欠かせないものになるでしょう。

クラウドサービスの最大のメリットは、自宅かオフィスかといった場所を問わず、またPCやスマートフォンなどデバイスを問わずに利用できる手軽さにあります。ただしクラウドサービスを利用する上では、従来型のアプリケーションを利用していた際にあまり考える必要のなかったリスクがあります。それが、なりすましによる不正アクセスです。

「認証の強化」が強力な対策に

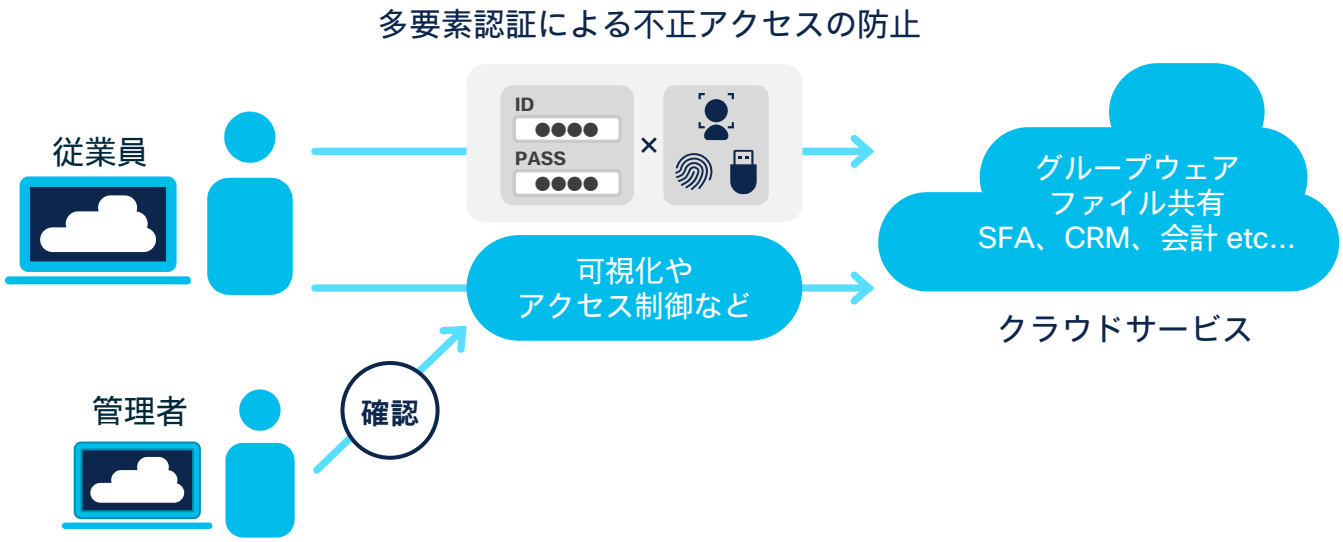
利用場所がオフィス内のみに限られるオンプレミスのアプリケーションと違って、多くのクラウドサービスはアカウントIDとパスワードさえ合ってさえいればアクセスできる、つまり、なりすましを簡単に行えてしまう弱点があります。

これを防ぐための強力な手段は、クラウドアクセス時の「本人認証」を強化することです。具体的に、IDとパスワードの認証に加えて、スマートフォンへのプッシュ通知や指紋や顔などの生体認証など、複数の認証を組み合わせてログインする「多要素認証」を採用するだけでも、安全性はかなり高まります。またあらかじめ登録したデバイスのみクラウドサービスへアクセスできるようにするサービスもあります。

このほかに、アクセスする端末が安全な状態であるかどうかも忘れてはならない重要なポイントです。

例えば、OS やブラウザのバージョンが古いままのデバイスは、そこに脆弱性が発見されることもあります。デバイス側のセキュリティ状態を可視化し、安全性が確認できないデバイスに対してはアプリケーションへのアクセスをブロックする、またはアップデートを促す通知を出すことで一貫したセキュリティポリシー適用できるようになります。

クラウドへの不正アクセスやパスワード管理リスクを防ぐ工夫



セキュリティの高度化を支えるシスコのソリューション

高度なインテリジェンスを備えたパートナーを

企業自身での対策には限界がある

ここまでさまざまなリスクとその対策を紹介してきました。セキュリティ対策の主体となるのは企業自身です。しかし中小企業にとっては、専門的な知識やスキルをもった人材を採用したり専任担当として配置したりすることが難しいという問題があり、セキュリティ対策になかなか時間やコストをかけられない現状があります。

だからこそ導入や運用も容易に行えるクラウドサービスを導入したり、運用自体をまるごとアウトソースできるサービス（マネージドサービス）を利用したりするほか、セキュリティのノウハウを持つ外部の専門家や企業に頼りながら、サイバー攻撃にうまく対処しつつ業務負荷を下げる工夫をしたいところです。

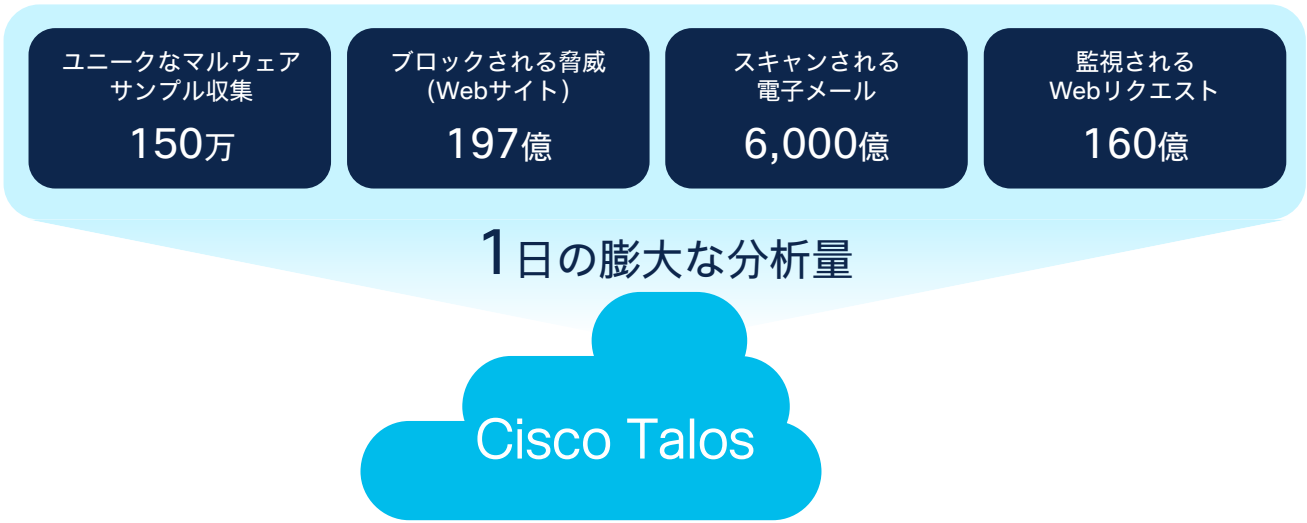
シスコのセキュリティへの取り組み「Cisco Talos」

セキュリティ製品がどれだけ防御に力を発揮できるかどうかは、脅威インテリジェンスを備えているかどうか、つまり提供ベンダーがセキュリティの脅威に関する情報をいかに収集・蓄積して徹底した分析を行っているかにも左右されます。これによってセキュリティ製品は、次々に新手を繰り出してくる多様なサイバー攻撃に対応できるようになっているのです。

その観点からシスコでは、250人を超えるセキュリティ専門家が集結した世界最大規模の脅威インテリジェンス組織「Cisco Talos」を有しています。この専門家チームが中心となって、世界中から収集したサイバーセキュリティに関するビッグデータを解析しており、そこから得られた最新の知見がさまざまなシスコ製品にフィードバックされていきます。例えば Cisco Talos が1日あたりに収集する新たなマルウェアのサンプル数は150万個、ブロックする脅威は197億件に上ります。こうしたデータ収集および分析能力の高さが、シスコ製品の高度なセキュリティ対策を支えています。

シスコのセキュリティ対策製品を導入することで、Cisco Talosの卓越した脅威インテリジェンスをダイレクトに活用することができます。

シスコではセキュリティの膨大な情報を収集し製品にフィードバック



セキュリティの高度化を支えるシスコのソリューション

中小企業にも導入しやすく高性能なセキュリティ製品

シスコでは、中小規模の企業の皆様が、より安全に多彩なクラウドサービスを利用できるようにするためのセキュリティソリューションを提供しています。

Cisco Umbrella

マルウェアやフィッシングサイト、有害サイトへのアクセスをブロックし、オフィスや在宅を問わず、どの場所からでも安全なインターネットアクセスを実現するセキュアインターネットゲートウェイです。SaaSとして提供されており、いわばこれまでオフィス内にあったUTMの機能をクラウドに拡張して実現したソリューションともいえるでしょう。

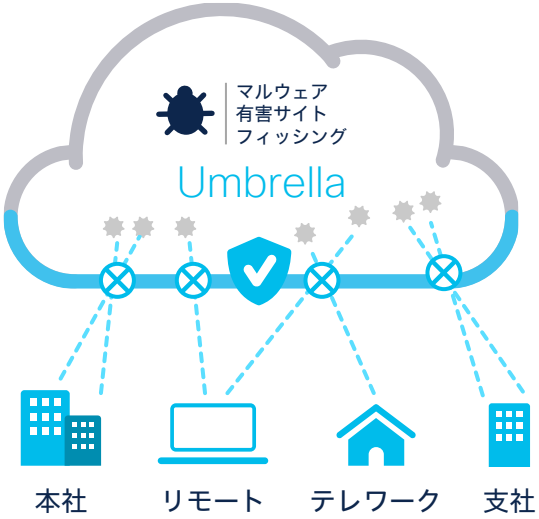
Cisco Duo

多要素認証と、デバイスの可視化を行うことができるソリューションです。多要素認証があれば、たとえIDとパスワードが流出しても犯罪者の不正ログインを防ぐことができます。また、多数のアプリケーションへのシングルサインオン機能を提供しており、ユーザーのパスワード管理を不要にし、ユーザビリティとセキュリティを両立することができます。

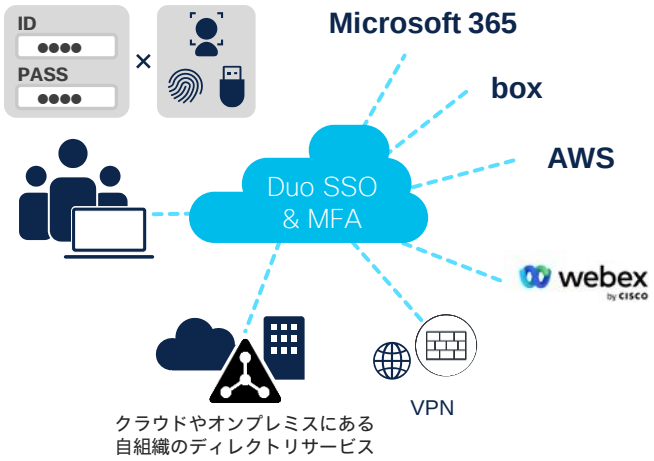
Cisco Meraki

デジタル時代に適した、クラウドで一元管理可能なネットワークソリューションです。多彩なラインアップのうち、UTMやVPN機能を持つセキュリティゲートウェイ「Meraki MX」や、簡単にVPN接続でき、自宅を拠点化できる在宅環境向け機器の「Meraki Z3」を導入することで、安全なリモートワーク環境を手軽に整備することができます。

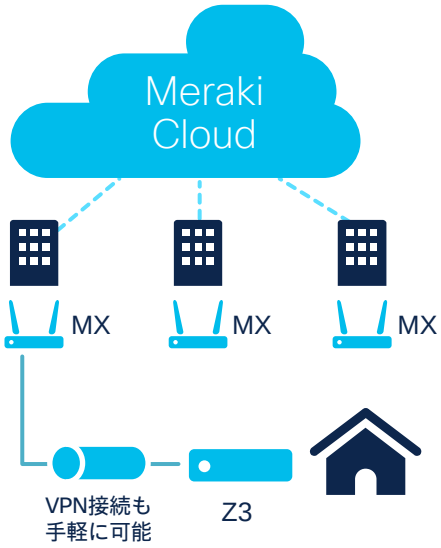
安全なインターネットアクセス



多要素認証とシングルサインオン



ネットワークのクラウド管理と簡単VPN接続



物理セキュリティの強化とIoT機器のクラウド管理

簡単に導入できる クラウド管理型セキュリティカメラ

防犯対策にネットワークカメラを導入する企業は多いでしょう。シスコでも、設置後ネットワークに接続するだけで、クラウド上への録画・視聴・管理を簡単に行えるクラウド管理型スマートカメラの「Meraki MV」を提供しており、防犯という観点からも企業のセキュリティ対策に貢献しています。

「Meraki MV」ではカメラの設定・管理や録画・視聴のために別途サーバーやソフトウェアなどは必要ありません。防犯だけでなく、顧客の行動分析、従業員の安全監視などさまざまな用途に利用でき、企業のIoTやデータ活用を促進することができます。

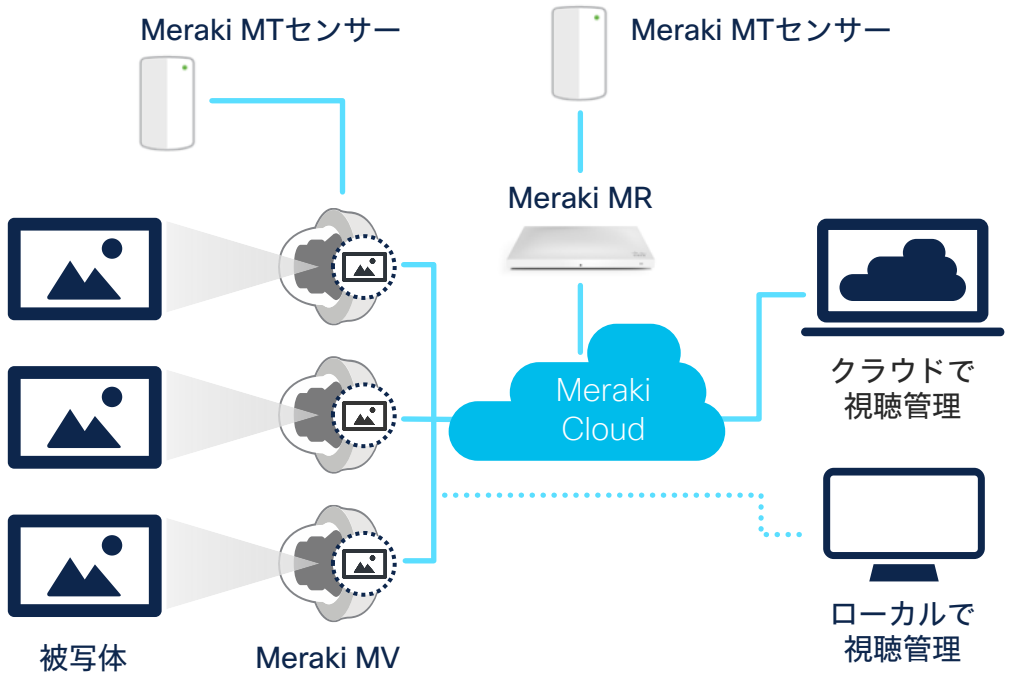
管理性の高いIoTセンサー

またCisco Merakiシリーズでは、IoTセンサーとして「Meraki MT」を提供しています。Meraki MTでは温湿度のデータ、漏水、不正侵入（ドアやキャビネットなどの開閉状態）をリアルタイムでモニタリングでき、重要なインフラや環境変化に敏感な資産の管理に役立ちます。

市場にはさまざまなIoTセンサーが流通していますが、どれも複雑で専用のゲートウェイやオンプレミスの管理サーバーを必要とするため、導入には時間がかかるものも多く存在します。

一方で、Meraki MTセンサーは、ネットワーク内に設置した既存のワイヤレスアクセスポイント「Meraki MR」や先述のMeraki MVスマートカメラをゲートウェイとして使用して自動的に接続できるため、すばやく導入できます。このMTセンサーもMerakiプラットフォームで稼動するため、完全にクラウドで管理できることも強みです。

IoT対応のカメラやIoTセンサーの管理にもMerakiだけで対応



中小企業向けセキュリティはこちらをご覧ください

cisco.com/c/ja_jp/solutions/small-business/cloud/security.html

無料デモ・トライアル・お問い合わせはこちら

cisco.com/c/ja_jp/solutions/small-business/contact.html

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。

製品に関して ｜ サービスに関して ｜ 各種キャンペーンに関して ｜ お見積依頼 ｜ 一般的なご質問

お問い合わせ先

お電話での問い合わせ

平日10:00-12:00, 13:00-17:00

0120-092-255

お問い合わせウェブフォーム

cisco.com/jp/go/vdc_callback

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

2290-2112-000-X