SOLUTION BRIEF

テレワーク推進のために必要なセキュリティ環境の構築

テレワークを推進するために必要なセキュリティ環境の構築。

自宅でや営業先、海外赴任先で、場所を選ばず業務を行うテレワークスタイル。日本においては働き方改革の後押しもあって、さまざまな企業がテレワークの実現を推進しています。しかしテレワークの実現に対して重要なのがサイバーセキュリティ対策です。本シートではテレワーク環境のセキュリティ課題を提示し、インターネット通信とエンドポイント (デバイス) の 2 つのセキュリティポイントにおいて、効果的なソリューションを紹介します。

- テレワークを推進するにあたってのセキュリティ課題
- テレワーク環境の Web セキュリティを高次元に変えるクラウドサービス型の Web ゲートウェイ
- デバイスを暗号化して、紛失や盗難、内部不正に対策
- McAfee Web Gateway シリーズの特長
- エンドポイントセキュリティでは、デバイスを暗号化して、紛失や盗難、内部不正に対策

テレワークを推進するにあたってのセキュリティ課題

会社以外の場所での業務遂行を実現するテレワーク。ノート PC を活用して、出張先や外出先で業務を行うノマドワークやコワークといったスタイルは、業務効率の向上などの理由で以前から普及しつつありました。それが、東日本大震災をはじめとする大地震やゲリラ豪雨などの自然災害の増加などにより需要が増え、さらに政府が推進する「働き方改革」に対応する手段として導入が本格化しています。しかし、社外にあるデバイスで業務を行うテレワークでは、セキュリティ対策も重要なポイントになります。

導入障壁が下がったテレワーク

営業先や出張先から会社に戻ることなく業務が行えるテレワークは、現在でも多くの企業が活用しています。社員にとっては直行・直帰が可能になり、自宅でも業務を行えることから、社員側から積極的にテレワークを行うケースが増えています。

その背景には、社員が持つノート PC やスマートデバイスの高性能化、高機能化により、業務アプリを快適に実行できるようになったことや、複数のネットワーク接続方法に対応したことなどが挙げられます。また、喫茶店やホテル、公園など多くの場所で Wi-Fi を利用できるようになり、さらに業務を効率的に行えるクラウドサービスが普及しました。テレワークの環境はすでに整っているのです。

デバイスのセキュリティには差がある

デバイス、Wi-Fi 、クラウドサービスと、テレワークの環境は整っていますが、現状ではこれらのセキュリティ対策が万全とはいえません。デバイスでは、企業で利用する業務端末はノート PC やタブレットが一般的ですが、個々のデバイスにセキュリティ対策のばらつきが見受けられるのが現状です。社内ではファイアウォールや IDS/IPS 、プロキシの Web ゲートウェイなどによる多層防御が構築されていますが、テレワーク環境ではデバイスに搭載されたエンドポイントセキュリティのみで脅威から保護しなければなりません。ところが従来のエンドポイントセキュリティでは進化する脅威に対して万全の対応ができていると言えません。

また、外出先では、デバイスを持ち歩くことが前提になります。そのため紛失や盗難のリスクが常につきまといます。ほとんどのデバイスにはログインパスワードが設定されていると思いますが、ログインパスワードは破られる可能性が高く、それだけでは安全な対策とはいえません。

ネットワークのセキュリティも万全ではない

ノート PC やスマートデバイスは、LAN 接続の有線ネットワーク、Wi-Fi を使用した無線ネットワーク、さらに携帯電話キャリアによる通信など、複数のネットワーク接続方法が用意されています。しかし、外出先でよく使用される Wi-Fi には、セキュリティ対策が十分でないケースが多くあります。店舗やホテル、空港などで提供される無料の Wi-Fi サービスでは、速度向上や利用者の手間の軽減のために、Wi-Fi の暗号化を弱く設定していたり、暗号化をしないケースもあります。こうした場合は、無線通信を傍受され、内容を盗み見られる可能性があります。

また、最近は Wi-Fi で一般的に使用されている暗号化形式「WPA2」に脆弱性が発見され、暗号を解読されるおそれがあります。現在、Wi-Fi 機器メーカーやデバイスの OS メーカーが対策を進めていますが、対策されていない Wi-Fi サービスも多くあります。この場合 VPN を活用することが推奨されていますが、VPN で私的な利用は接続をためらいますし、VPN サーバーに接続するまでは脆弱な状態になります。

有料／無料で異なるクラウドサービスのセキュリティレベル

ほとんどのクラウドサービスは、無料の個人向けサービスのほかに有料の企業向けのサービスも用意されており、企業向けのサービスはセキュリティ対策がより強化されています。しかし、現状では無料の個人向けサービスを業務でも使用しているケースが多く、共有設定をうっかり間違えて重要なデータが漏えいしてしまうこともあります。また、個人向けサービスではクラウドサービスを利用した際の記録が残らないので、漏えいした際の原因究明が難しくなります。

テレワークに対応したセキュリティ環境の構築が必要

このようにデバイスのセキュリティにばらつきがあること、そしてネットワークやクラウドサービスの利用にもセキュリティの落とし穴があることを踏まえると、現段階ではクラウドサービス型の強力な Web ゲートウェイを活用することが有効な対策だといえます。

さらに顧客情報など機密保持義務が高いデータを持つデバイスは、盗難や紛失対策として、ハードディスクドライブ全体を暗号化させる保護がより万全なセキュリティ対策といえるでしょう。

テレワークが推進しきれていない原因のひとつに、一般的に IT 技術者は内勤者が多く、外出の多い営業セクション等のセキュリティ環境を実感しきれていないという意見も聞きます。セキュリティを構築する際に、IT 技術者は一度、テレワーク環境をロールプレイしてみるのも良いかもしれません。

Solution Brief
McAfee Together is power.

テレワーク環境の Web セキュリティを高次元に変えるクラウドサービス型の Web ゲートウェイ

いつでもどこでも最新・最高水準のゲートウェイセキュリティが保護

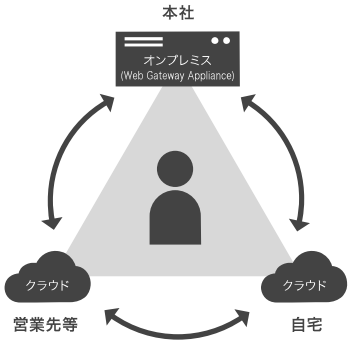
マカフィーでは、クラウドサービス型のウェブ セキュリティ ゲートウェイ McAfee Web Gateway Clouod Service (MWGCS) を提供しています。
ユーザーは、どこにいてもインターネットへの接続は MWGCS を介して行われます。オンプレミス環境と同様、URL フィルタリング、マルウェア対策の機能を実装しているだけでなく、オンプレミス環境とクラウド環境も同じセキュリティポリシーを適用できます。しかも、クラウド上で常に最新の状態を維持しているので、いつでもどこでも最新、最高水準のゲートウェイセキュリティが保護します。

導入コストが調整しやすく、運用コストも効率化しやすい

MWGCS はクラウドサービスなのでハードウェアやソフトウェアの購入といったイニシャルコストが必要ありません。ユーザーごとにライセンスが付与されるのでセキュリティコストに細かい調整ができます。

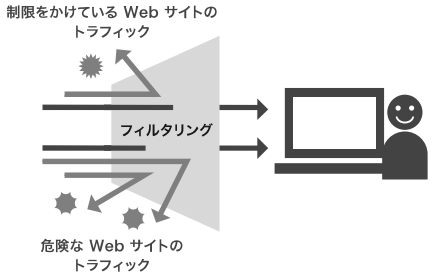
さらに、ハイブリッド型の McAfee Web Protection を導入すれば、ユーザーは1つのライセンスでオンプレミスとクラウドをシームレスに利用できます。McAfee Web Protection シリーズは、社員のそれぞれの働く環境によって、オンプレミス（例: 本社事務系）、クラウドサービス（例: 拠点駐在系）、モバイルかテレワークどちらか（例: 営業系）と柔軟性を持った配備が可能。セキュリティ総保有コストの削減につながります。

また運用面でも、オンプレミス環境とクラウド環境のポリシーを一元化することが可能。社内環境からの Web アクセスポリシーも、リモート環境からクラウドサービス経由でアクセスするユーザーでも、均一のセキュリティポリシーを適用し、より効率のいい運用を実現できます。



場所を選ばず Web ゲートウェイが護る
セキュリティ環境

McAfee Web Gateway シリーズの特長

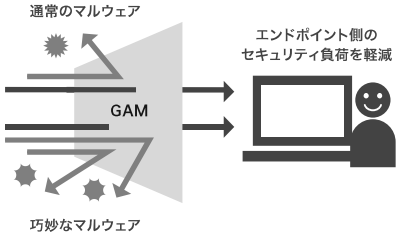


包括的な URL フィルタリング データベースを使用して 受信/送信トラフィックを保護

Web ゲートウェイが発動すると、まず URL フィルタリングが業務上不要な Web サイトやセキュリティ的に危険な Web サイトをカテゴリー化してフィルタリングします。カテゴリーのデータベースは McAfee 側で常にアップデートされ、最新のフィルタリングが適用されます。

ランサムウェアやゼロデイ攻撃など 巧妙なマルウェアを検知

Gateway Anti-Malware (GAM) は、Web の脅威に対抗するために開発された強力な振る舞い検知エンジンです。Web の振る舞いも含めたシグネチャレスの解析が可能で、ランサムウェアやゼロデイ攻撃を含む巧妙なマルウェアを高い精度で検出します。

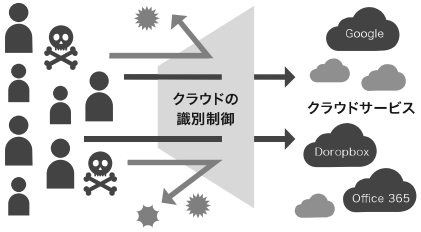


SSL 通信のスキャニング対応

SSL スキャナーによって通信を復号化し、アクセス元・アクセス先を常に監視することができ SSL 通信を悪用した脅威も検知します。安全なはずの SSL 通信を悪用した高度な攻撃からも防御性が向上します。

クラウドサービス制御によるシャドー IT 対策

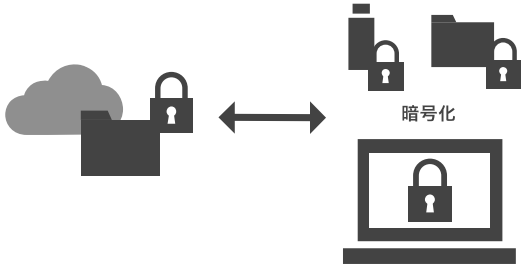
企業が把握できていない状況で、従業員は IT 活用をすることを「シャドー IT 」と呼びます。最近では、企業でも様々な形でクラウドサービスを積極的に活用するようになり、企業の IT 管理部門がクラウドサービスの活用を制御することが困難になっています。
マカフィーの McAfee Web Gateway シリーズは、約6000種類のクラウドサービスを識別し制御することが可能です。セキュリティ運用者側でリスクレベルを設定して高いリスクのサービスを防止することができます。



Solution Brief

エンドポイントセキュリティでは、 デバイスを暗号化して、紛失や盗難、内部不正に対策

テレワークでは、社員の業務環境となる PC などがさまざまな場所に移動するようになるので、紛失や盗難のリスクが増えます。紛失した PC が悪意のある第三者の手に渡ってしまったり、情報を目的とした盗難に遭ってしまった場合には、PC などの ID とパスワードによる基本的なログイン制御だけでは、それを突破され中身を見られてしまう可能性があります。そうすると、PCに保存されている情報だけでなく、グループウェアなどから社内にある情報にもアクセスされてしまいます。
McAfee Complete Data Protection は、強力なハードディスク暗号化機能でエンドポイント (Windows、Mac) の重要なデータを暗号化し保護します。また、ネットワーク ファイル共有、USB メモリなどのリムーバブル メディア、クラウド ストレージサービスなどの重要なデータも暗号化し保護します。



ニュース&キーワード

テレワーク先駆者百選

テレワークを推進するために、総務省では2015年度から、テレワークの導入・活用を進めている企業・団体を「テレワーク先駆者」と認定し、その中から十分な実績を持つ企業等を「テレワーク先駆者百選」として公表しています。
2016年度からは「テレワーク先駆者百選　総務大臣賞」を創設し、「テレワーク先駆者百選」の中から特に優れた取組を表彰しています。2017年度はNTTドコモ、沖電気工業グループの特例子会社沖ワークウェル、大同生命保険、日本マイクロソフトとマイクロソフトディベロップメント、ネットワンシステムズの5グループ6社が表彰されました。
表彰された各社は、在宅勤務者の増加や時間外労働の削減、女性の離職率削減、重度障害者の労働参加といった成果を出しています。またペーパーレス化、旅費・交通費の削減など経費削減などの効果も生み出しています。
海外企業と比較してはムダの多い企業体質を指摘されることが多い日本企業ですが、テレワークによる労務マネジメントの向上と経費削減の潮流は今後も広がっていくでしょう。