recomot

テレワークにおける
セキュリティリスクと対策

これからのテレワークに必要な
ゼロトラスト・セキュリティの構築とは

INDEX

これからの働き方
テレワークのあり方とは

はじめに

新型コロナウィルスの感染拡大により働き方は大きく変わりました。もはや当たり前となったテレワークですが、今後も継続して企業成長を続けるには、テレワークを経営に組み込むことが重要です。それができない企業は生産性向上が見込めず、人材流出も避けられません。

一方で、緊急事態宣言などにより、急遽テレワーク環境を準備したという企業も多かったことでしょう。これら突貫工事のテレワーク環境においては、セキュリティ対策が万全ではない企業も少なくありません。

これからのニューノーマル時代に企業が成長を続けるためのテレワークと、そのセキュリティにはどのようなものが必要とされるのでしょうか。

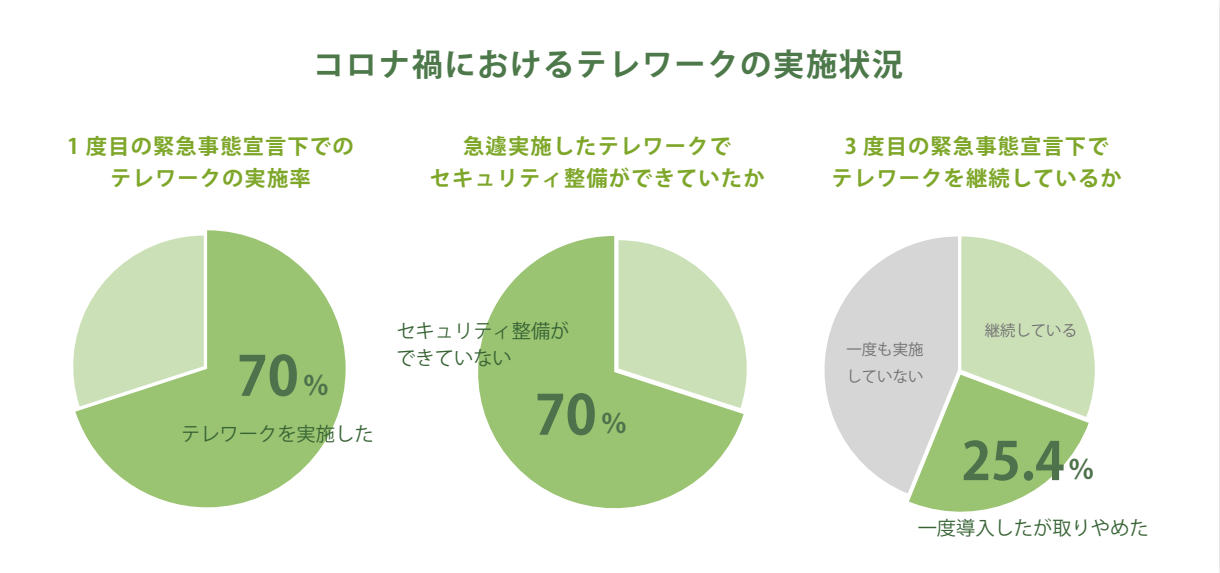
1. テレワークのセキュリティにおける日本企業の現状

2020 年 4 月、2021 年 1 月と 2 回にわたり発令された緊急事態宣言。株式会社レコモットが、経営陣 200 名と IT 管理者 200 名の計 400 名を対象に行った「コロナ禍における働き方に関する意識調査」によると、緊急事態宣言により 70%もの企業がテレワークを実施していたことがわかりました（n＝400 名）。

また、緊急事態宣言発令後にテレワークを実施したが、セキュリティの整備ができていない企業は 70%（n＝283 名）、その状況の中でセキュリティに脅威を感じていた IT 管理者は 55%（n＝74 名）という結果になり、セキュリティ環境が未整備であることに危機を感じながらもテレワークをせざるを得なかった状況がわかります。

一方で、緊急事態宣言が解除された後も 60%もの企業がテレワークを継続しています（n＝400 名）。（楽天インサイトによるインターネット調査、2020 年 7 月 10 日（金）～ 7 月 12 日（日）の期間、全国の経営陣 200 名／IT 管理者 200 名（計 400 サンプル）を対象に実施）

しかし、感染流行の第 3 波が到来した 2020 年 11 月以降に東京商工リサーチが実施した調査によると、テレワークを実施している企業は 30.7%にとどまり、テレワークを一度導入したが取りやめたという企業は 25.4% に上りました。



テレワークを取りやめた理由として、業務がテレワークに適していないという回答が多いものの、情報セキュリティに不安がある、生産効率が下がるといったテレワーク環境が整っていないことによって取りやめたという回答も多く見られました。（インターネット調査、2020 年 11 月 9 日（月）～11 月 16 日（月）の期間、全国の資本金 1 億円以上の大企業、1 億円未満の中小企業 1 万 1,076 社を対象に実施）

コロナ禍により一度は導入が進んだテレワークですが、セキュリティの不安やテレワーク環境の未整備といった理由から、思ったように導入が進んでいないことが伺えます。

また日本だけでなく 2020 年 2 月～4 月の間には、世界中で金融機関へのサイバー攻撃が 238％増えています（VMware Carbon Black の調査による）。そのほか、大手自動車メーカーのマルウェア感染、EC サイトや宅配業者を装ったフィッシング詐欺も増加。未整備なセキュリティ環境や脆弱性を狙った標的型攻撃やサイバー攻撃の危険に晒されています。

企業は正しいセキュリティリスクの知識をもち、安全なテレワーク環境を整えることが急務となっているのです。

2. テレワークの セキュリティリスクと脅威

IPA（独立行政法人情報処理推進機構）の「情報セキュリティ 10 大脅威 2021」によると 2020 年に社会的影響が大きかった組織の情報システムの脅威として、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、3 位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挙げられています。

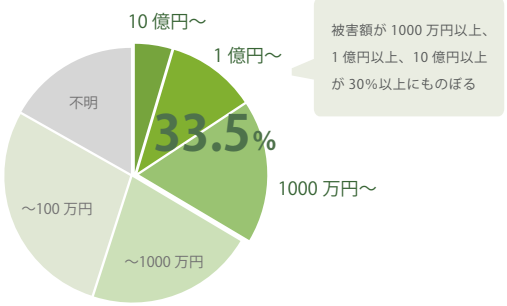
個人情報や機密情報などの情報漏えいは企業側に賠償責任が生じることもあります。それだけでなく、企業の信頼が大きく損なわれ、売り上げに影響がでたり、取引先との取引を停止されたりする可能性もあるでしょう。企業が情報漏えいの原因調査や改善、サービス停止による損失や賠償金などの対応を含めた被害金額は平均で 1 億 4800 万円だったといいます（トレンドマイクロ「法人組織のセキュリティ動向調査 2020」による）。

2020 年に社会的影響が大きかった 組織の情報システムの脅威

1 位 ランサムウェアによる被害
2 位 標的型攻撃による機密情報の窃取
3 位 テレワーク等のニューノーマルな働き方を狙った攻撃

「情報セキュリティ 10 大脅威 2021」より

情報漏えいによる企業の被害額



平均被害額は 1 億 4800 万円

一度失われた社会的信用を取り戻すのは非常に困難です。このようなことが起こらないように企業はセキュリティインシデントが発生することがないよう事前の対策を行うことが重要です。

2-1. 情報漏えいの原因

情報漏えいの原因には不正アクセスやマルウェア感染などによる外的要因と、端末の紛失や情報の持ち出しといった従業員の過失などによる内的要因があります。また、テレワークで急増したVPN環境の脆弱性や、自宅におけるネットワーク環境の脆弱性を狙った攻撃にも注意が必要です。

2-1-1. 外的要因（サイバー攻撃）

外的要因は大きくはマルウェア等への感染によるものと、脆弱性攻撃や不正アクセスによるものがあります。マルウェアとは悪意のあるソフトウェアのことで、マルウェアにはウィルス、ワーム、金銭目的のランサムウェアなどがあります。

最近ではこれらの悪意のあるサイバー攻撃のうち、標的型攻撃が増加しています。テレワークが増加し、従業員のセキュリティに対するリテラシーの低さや、管理されていない自宅のPCやネットワークからのアクセスもこれらのサイバー攻撃を増長させる原因になっています。

サイバー攻撃の分類

攻撃分類	攻撃方法	進入経路
不特定多数の攻撃 （マスメール型）	ウイルス（マルウェア）	メール・サイト閲覧からの感染
	スパムメール	メール
	フィッシング	メール・Web サイトの偽装
公開サーバー への攻撃 （脆弱性攻撃など）	不正侵入	社内外ネットワークからの侵入（脆弱性等を利用）
	DoS 攻撃 / DDoS 攻撃	Web サイト等への大量アクセスや大量データの送付
	なりすまし	総当りパスワード解析等を利用した ID 情報等の窃取
	ゼロデイ攻撃	脆弱性の発見後、パッチ等が出るまでの間の攻撃
標的型攻撃 （標的型メール）	マルウェア （ワーム・自己増殖型）	メール、添付ファイル、リンクからのサイト閲覧
	ランサムウェア （金銭目的）	メール、添付ファイル、リンクからのサイト閲覧

2-1-2. 内的要因（紛失、持ち出し）

一方で、情報漏えいの原因はウィルスや不正アクセスなどの外的要因だけではなく、実のところ従業員の過失や、不正といった内的要因も多いといわれています。これらの内的要因には以下のようなものがあります。

・メールの誤送信による情報漏えいやデータの損失
・設定や操作のミスにより社内データに誰でもアクセスできる状態になっていた
・USB や端末などの紛失や置き忘れ、盗難、悪意ある従業員による持ち出し

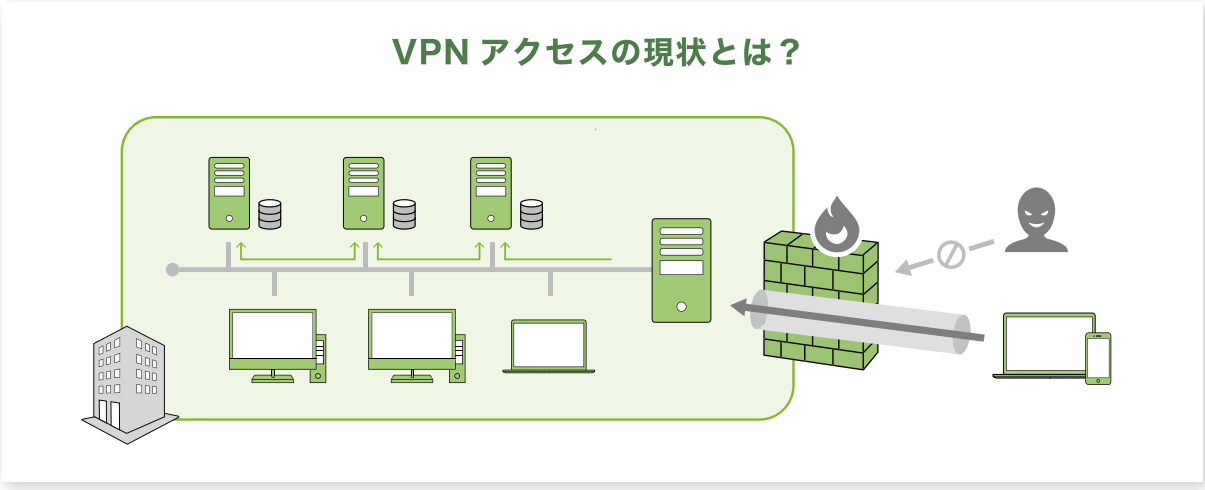
・個人情報などの情報持ち出しルールの形骸化
・シャドウ IT など従業員のリテラシーの低さからの不注意による内部脅威

このような内的要因にはセキュリティルールの徹底や誤送信を防止するシステムの導入、適切なアクセス権限の設定、端末やアプリケーション管理の導入などの対策が必要です。

2-1-3. 境界型防御の限界（VPN、ネットワーク）

急増したテレワークを支える VPN ですが、この VPN 機器の脆弱性を狙ったサイバー攻撃も急増しており、2020 年 5 月には大手企業で大規模なサイバー攻撃が発生し、防衛に関する機密情報や個人情報が流出しました。その他、同年 8 月には別の企業でも VPN 接続に使用する認証情報が漏えいした事件も起きています。

背景には脆弱性への認識の甘さや、セキュリティ人材の不足、高コストで拡張性が低い VPN の負の特徴なども考えられますが、本質的には企業の内部だけを守れば安全、という境界型セキュリティ対策だけでは限界が来ているという現実があります。



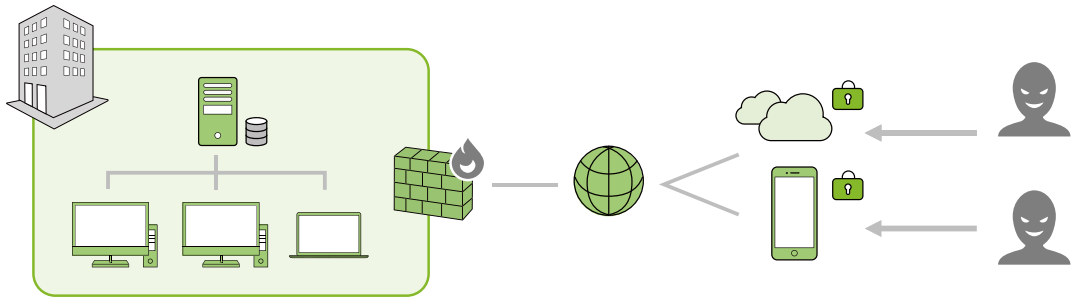
このようにテレワークにはさまざまな原因によるセキュリティリスクが伴います。企業は早急な対策を講じる必要に迫られているのです。これからのニューノーマル時代のテレワークに必要なセキュリティとはどのようなものなのでしょうか？またどのようなセキュリティ方法を選び、安全なテレワーク環境を構築していけば良いのでしょうか？

3. これからのテレワークに必要なゼロトラスト・セキュリティ

前述したとおり、コロナ禍によって急速に普及したテレワークと、それに対する脅威の増加に加え、近年では業務効率化やテレワーク普及によるシステムのクラウドシフトが進み、企業の情報資産がクラウドと連携することで、新たなセキュリティリスクが生まれています。

従来、企業情報は社内にあり、社内と社外の境界線にフォーカスして防御をしていました。しかしクラウドシフトにより従来型の「境界防御モデル」だけではセキュリティを維持することが難しくなっています。

VPN などの「境界型防御モデル」の限界



最近ではこれらの悪意のあるサイバー攻撃のうち、標的型攻撃が増加しています。テレワークが増加し、従業員のセキュリティに対するリテラシーの低さや、管理さ

れていない自宅の PC やネットワークからのアクセスもこれらのサイバー攻撃を増長させる原因になっています。

そこで注目されるようになったのが「ゼロトラストモデル」です。ゼロトラストモデルとは、「何も信用しない」つまり攻撃されることを前提とし全てを検証するというもの。あらゆるユーザー、ID、パスワード、デバイス、ネットワーク、アプリケーションは安全ではなく、攻撃される可能性があるという考えに基づき、ネットワークやクラウド環境、エンドポイントのデバイスまで、総合的にセキュリティを高めていくセキュリティの概念です。

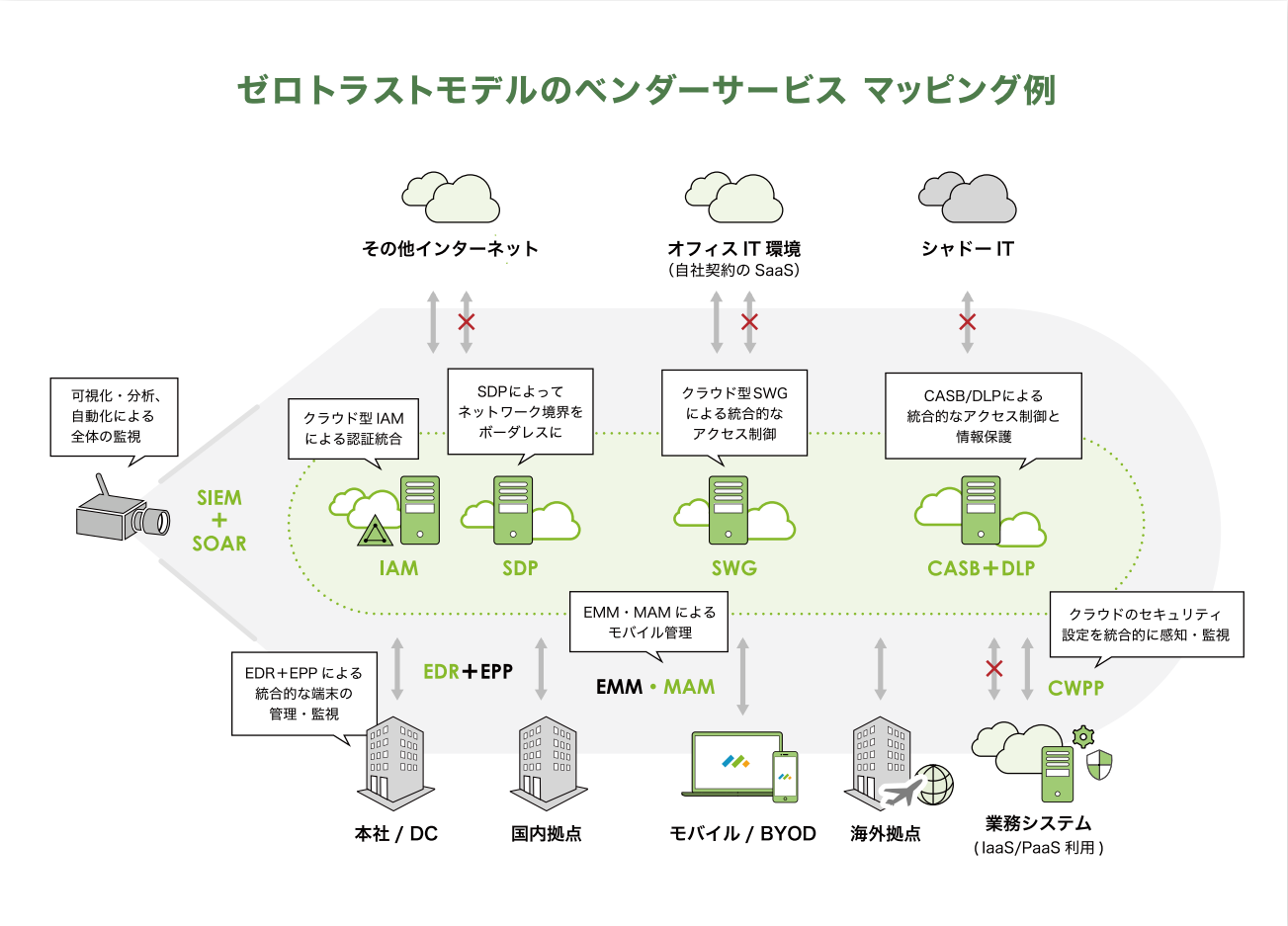
もともとはセキュリティの概念であったゼロトラストは、2020 年 2 月に米国標準技術研究所（通称 NIST）によりアーキティクチャーとして定義されています。

NIST の提唱するゼロトラストアークディクチャの 7 要件

1. すべてのデータソースとコンピューティングサービスは**リソースとみなす**。
2. **ネットワークの場所に関係なく**、すべての通信を保護する。
3. 企業リソースへのアクセスは、**セッション単位で付与する**。
4. リソースへのアクセスは、クライアント ID、アプリケーション、要求する資産の状態、その他の行動属性や環境属性を含めた**動的ポリシーによって決定する**。
5. 企業はすべての資産の整合性とセキュリティ動作を**監視し測定する**。
6. すべてのリソースの認証と認可は動的に行われ、**アクセスが許可される前に幻覚に実施する**。
7. 企業は資産やネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、それを**セキュリティ改善に利用する**。

最近ではさまざまなセキュリティベンダーがこのゼロトラストアーキティクチャを自己解釈し、自社に優位なポジショントーク合戦を繰り広げており、これがゼロトラストアーキティクチャを分かりにくくしている要因となっています。

以下に主なセキュリティベンダーが提唱する概念とサービスマップ、概要を説明します。



主なゼロトラストサービスの概要

要　件	ソリューション例	概　要
ネットワーク セキュリティ	**GASB**（Cloud Access Security Broker） **SWG**（Secure Web Gateway） **SDP**（Software Defined Perimeter）	・クラウド型 SWG で統合的なアクセス制御 ・CASB と SWG の統合でアクセスポイントを集約 ・SDP でネットワーク境界をボーダレスに
デバイス セキュリティ	**EPP**（Endpoint Protection Platform） **EDR**（Endpoint Detection and Response） **EMM**（Enterprise Mobility Management） **MAM**（Mobile Application Management）	・EPP による事前対策 ・EDR による事後対策 ・EMM に統合的な端末の管理・監視 ・MAM によるアプリケーション管理
アイデンティティ セキュリティ	**IAM**（Identity and Access Management）	・クラウド型 IAM による認証統合 ・ディレクトリ統合
データ セキュリティ	**DLP**（Data Loss Prevention）	・DLP によるデータの暗号化・保護

テレワークのセキュリティ対策として、ゼロトラストの注目度は高いですが、どのセキュリティサービスにも一長一短があり、どれかひとつを取り入れれば安全とは言い切れません。また、ゼロトラストの要素すべてをひとつのサービスで実現することもできません。

すべてのセキュリティリスクをカバーするとなると高額なサービスを複数導入しなければならず、専門の運用チームも必要です。結果、膨大なコストがかかり現実的ではないでしょう。

そこでゼロトラストモデルに対応し、ニューノーマル時代のセキュリティ対策の鍵を握るソリューションが moconavi（モコナビ）です。

4. ゼロトラストなテレワーク・プラットフォーム moconavi

moconavi（モコナビ）はゼロトラストの要素を含んだテレワークのセキュリティ対策を行うことができるサービスです。

「moconavi」、「moconavi RDS」、「moconavi 050」をシリーズで使用することで、総合的なテレワークのセキュリティ対策が可能で、さまざまな脅威から情報資産、従業員を守り、かつ作業効率を落とすことなく快適なテレワーク環境を実現します。

4-1. moconavi

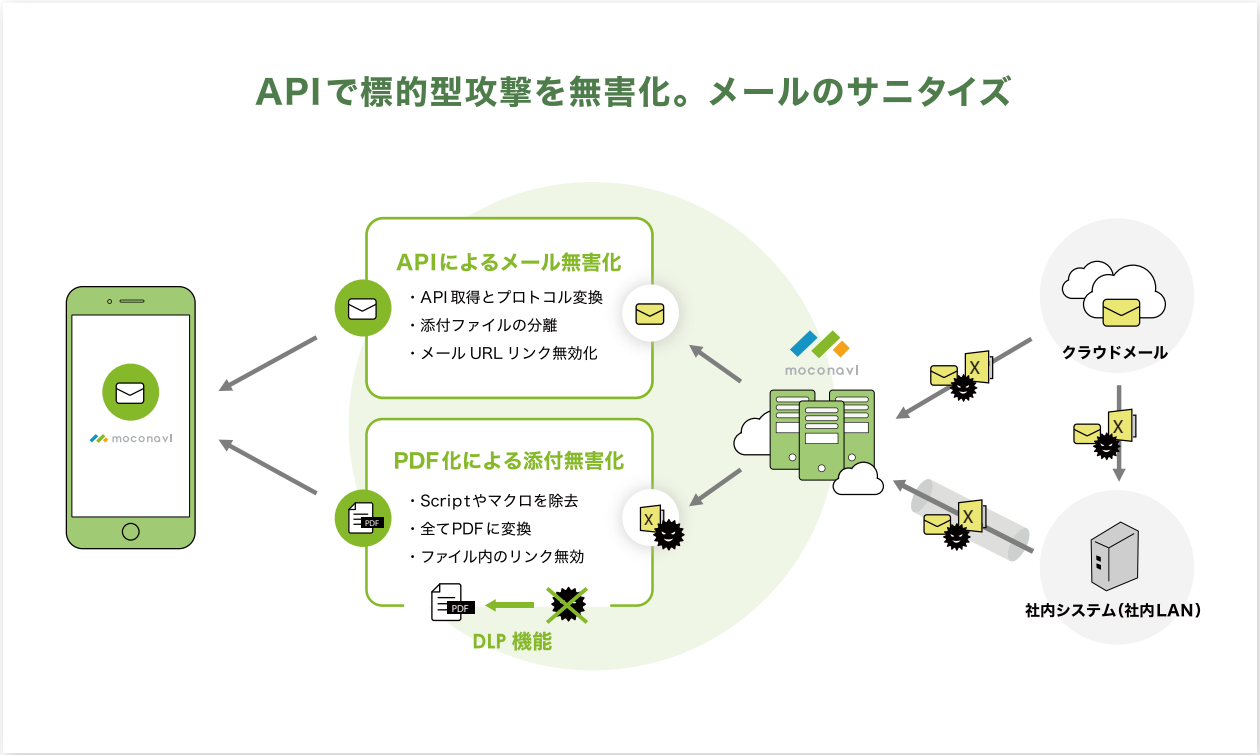
moconavi は Microsoft365 などのグループウェアや Box などのストレージ、kintone などの CRM といった 50 種類以上のさまざまな業務ツールと連携し、普段使っているデバイスでセキュアな環境のなか業務を行えます。そしてゼロトラストの要素を含むこれからのセキュリティ対策として必要な以下の 4 つのポイントをカバーしています。

4-1-1. データを端末に残さない、エンドポイントセキュリティ

MAM（モバイルアプリケーション管理）である moconavi。moconavi アプリのサンドボックス（セキュアコンテナ）内に業務アプリを配置することで端末に業務専用の作業環境を作ります。その隔離された環境で業務アプリを使用するので、端末自体にデータを残しません。万が一端末がマルウェアに感染しても moconavi アプリ内に侵入されることはなく、端末にデータも残らないので機密情報や顧客情報など窃取されません。

4-1-2. メールの無害化でマルウェア感染を防御

マルウェア感染の多くが標的型メールによるものです。添付されている Word や Excel などのファルデータや、URL リンク、html メールに埋め込まれたスクリプトなどにより感染してしまいます。moconavi は添付ファイルの PDF 化、URL リンクの無効化、スクリプトの除去により全てを無害化。マルウェア感染を防ぎます。



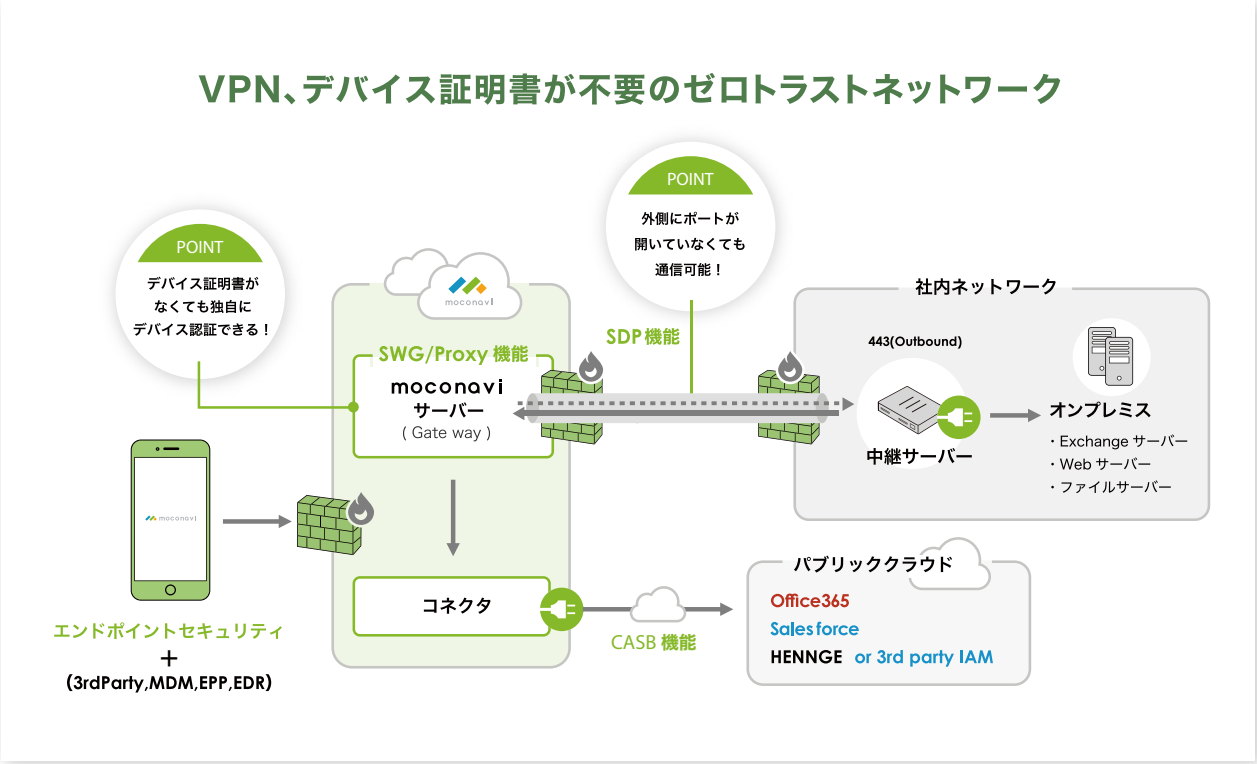
4-1-3. moconavi アプリは VPN、デバイス証明書が不要

moconavi アプリは、さまざまな CRM や SFA、グループウェアなどを利用することが可能でモバイル表示にも対応しています。ファイルデータは moconavi のドキュメントビューアで表示し、端末にダウンロードされませ

ん。Office ファイルは PDF に変換して表示崩れを低減し、同時にファイルの無害化も行います。

セキュアブラウザなのでもちろんキャッシュや Cookie、閲覧履歴などのデータは削除され端末に残りません。また、moconavi では端末識別 ID を利用したデバイス認証を行なっているため、新たにデバイス証明書を用意する必要がありません。

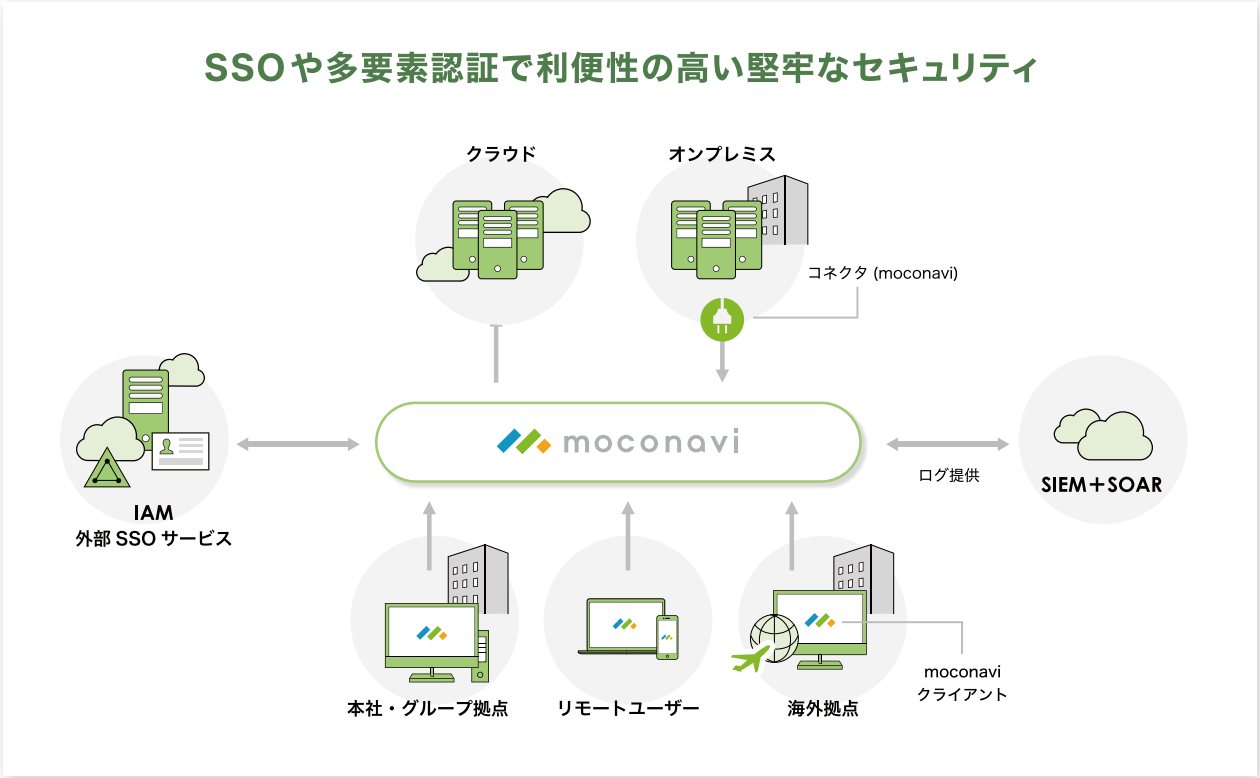
moconavi のアプリは、moconavi クラウドセンターのグローバルプロキシとお客様の社内に設置した中継ソフトとで通信を行います。社内からのアウトバウンドのみの通信となるため外部からのアクセスは受け付けません。お客様の VPN を使用せずに安全に社内システムにアクセスすることが可能です。



4-1-3. さまざまな認証方法や SSO で利便性の高い堅牢なセキュリティ

moconavi へのログインは ID/PW と端末識別 ID による多要素認証です。また、PIN コードと生体認証を利用してログイン作業を簡略化しています。連携する業務ツールへのログインは API が公開されていれば OAuth 認証、それ以外はセキュアブラウザでログイン画面を表示しログインを行います。

また、メジャーな IdP と連携した SSO（シングルサインオン）が可能です。業務ツールごとの ID/PW の入力が不要で、ID/PW の入力は moconavi1 回のみ。moconavi で IP 制限、端末識別 ID によるデバイス制限ができ、経路とデバイスの特定が行えるため端末ごとのデバイス証明書は不要です。堅牢なセキュリティでありながら、管理者、利用者双方の利便性を損ないません。

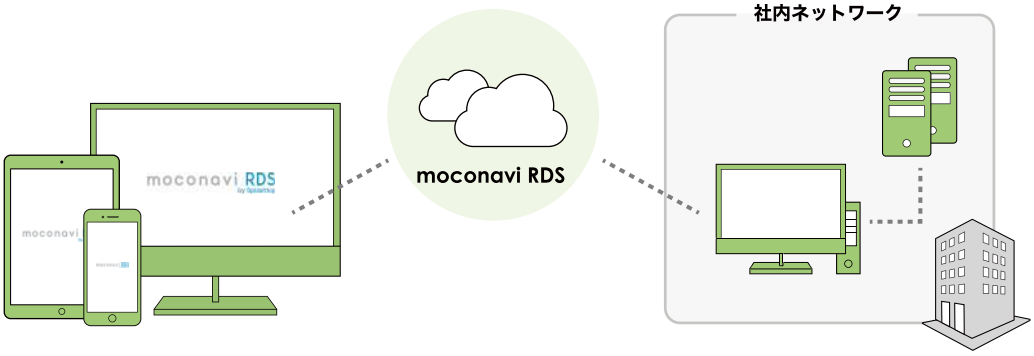


4-2. moconavi RDS

moconavi RDS は社外から社内の PC にアクセスし、画面転送技術を利用して普段と同じように業務アプリを使ってデータの閲覧や編集ができるリモートデスクトップサービスです。VPN を利用しないので、急速なテレワーク普及による VPN の逼迫や、脆弱性を狙ったサイバー攻撃といった影響を受けずに安全に社内システムにアクセスすることができます。導入もアクセス先の会社にある PC にはストリーマーを、操作する側の PC やタブレットなどにアプリを入れるだけと簡単ステップでご利用いただけます。

Windows や Mac といった OS に標準搭載されているリモートアクセスは手軽ではありますが、セキュリティ面での不安が残るため、別途 VPN やゲートウェイ、デバイス証明書などの設定が必要です。moconavi RDS は VPN や新たなサーバーは不要で、SSL によるネットワークの暗号化、デバイス認証や 2 段階認証の機能が備わっているほか、moconavi と連携すれば SSO を利用することも可能。意識することなく、高いセキュリティ環境を実現します。

moconavi RDS なら VPN 不要で社内 PC に安全アクセス！



VPN の逼迫・脆弱性を狙ったサイバー攻撃の影響もありません

4-3. moconavi 050

moconavi 050 は個人の携帯電話に 050 番号を付与することでビジネスとプライベートで電話番号と通話料を使い分けできる法人向けの 050 番号サービスです。テレワーク時の会社宛の電話対応や、個人の携帯電話を使用して通話料が個人負担となってしまったり、プライベートの番号を知られてしまったりといった課題解決に役立ちます。

標準機能であるクラウド電話帳でアドレス情報を一元管理でき、端末自体のアドレス帳に顧客のアドレス情報を保存する必要はありません。発着信時にはクラウド電話帳の情報を参照するだけなので発着信履歴も端末に残しません。万が一端末を紛失してしまってもアドレス情報も発着信履歴も端末に残っていないので情報漏えいすることがありません。

企業資産の顧客情報と従業員のプライバシーの両方を守りつつ、テレワークの電話に対する課題を解決します。

終わりに

コロナ禍によるテレワークの急激な普及で安全なテレワーク環境の整備が間に合わないことやセキュリティの脆弱性を狙って増加したサイバー攻撃、クラウドシフトによる全てを信用しないというゼロトラストの流れ。今必要なテレワークとそのセキュリティについて解説しました。

企業はこれらのニューノーマルの流れを的確に捉え、中長期的なセキュリティ対策を見直すタイミングにきています。企業の情報資産、また従業員を守り、ひいては企業成長へとつながるよう moconavi というソリューションが、皆さまのセキュリティを兼ね備えたテレワーク環境構築の一助となれば幸いです。

株式会社レコモット