テレワークの拡大に伴うレスポンス悪化も解消 セキュアで快適な外部接続を実現するWeb分離

テレワークの普及拡大とともに、外部アクセスへのレスポンス低下が問題として浮上している。自宅などからVPNを利用して社内ネットワークを経由し、外部に接続するための回線が逼迫しているためだ。これを回避するために、直接外部ネットワークに接続したならば、マルウェア感染のリスクを高めてしまう。これらの課題を解決するのが「分離による無害化」対策だ。本書では、分離による無害化の仕組み、そしてもたらされるメリットについて解説していく。

VPN利用の急増による回線逼迫が 快適なテレワーク推進の妨げに

新型コロナウイルスの感染拡大を背景に、企業にはニューノーマルに対応した働き方へと早急に変革していくことが求められている。事実、オフィス業務は在宅勤務に、社内外のコミュニケーションもWeb会議へと移行するなど、多くの企業においてテレワークの導入が加速している。

しかし、テレワークの普及拡大とともにサイバー攻撃のリスクも増大しており、企業には、「ユーザーの利便性を損なうことなく、セキュリティを強化する」という難題が降りかかっている。特に悩みの声として多々寄せられているのが、VPNの利用増に伴う回線の逼迫と、付随して発生するセキュリティリスクへの対処だ。

テレワークでのセキュリティを確保するために、いったん自宅などからVPNで社内ネットワークに接続した後、外部のインターネットや業務利用しているクラウドサービスへアクセスさせる、といった対策は多くの企業で行われている。だが、テレワークの普及拡大による社内ネットワークへのVPN接続急増や、テレワークの普及以前からの課題ではあるが、クラウドサービスの業務利用が増えていることによる社内ネットワークからインターネットへの通信急増のため回線が逼迫する傾向にあり、利用者から「遅くて、使いにくい」といった不満が上がり始めているのだ。

VPNを介さずに利用者が自宅などから直接、外部にアクセスすれば回線逼迫の問題は解消されるが、当然、マルウェア感染の危険が高まってしまう。社外からの外部へのアクセス用に別途、セキュリティ対策を導入するという手段もあるが、社内のセキュリティシステムとの間で二重管理や投資の問題が生じてしまう。

分離による無害化で PCのマルウェア感染を防止

これらの課題に対する有効な解決策は、社内・社外共通のセキュリティ対策をクラウドで導入することだ。その具体的な手法が「分離による無害化」である。これは、悪意の有無に関わらず、すべてのアクセスを安全なものに変換する「分離環境」をクラウド上に用意することでマルウェアを無害化したり、侵入を防いだりするもの。アクセス先のWebサイトが有害か無害かを判断する必要がなく、また、未知のマルウェアにも対応できることが特長だ。ここからは、分離による無害化の仕組みについて、詳しく説明していこう。

サイバー攻撃による被害のほとんどは、Webとメール経由での感染と言われている。例えば、Webコンテンツにはスクリプトを含んだアクティブコンテンツが数多く存在するほか、ExcelやWordなどのドキュメントにもマクロが含まれていることがある。これらのアクティブコンテンツやマクロにマルウェアが仕込まれていた場合、PCにダウンロードして実行したならば、感染を引き起こしてしまう。

分離による無害化は、外部の分離環境でアクティブコンテンツを読み込み・実行し、結果の表示情報だけをPCに転送する。これにより、マルウェアが仕込まれていても分離環境に留められるため、感染を防げるようになる。

また、メールについても、悪意のあるWebサイトのURLやマルウェアが仕込まれた添付ファイルを開かせる、といった手口が増えている。分離による無害化ならば、メールに記載のURLからWebにアクセスしても先述のようにマルウェアを無害化できる。添付ファイルも、一旦、

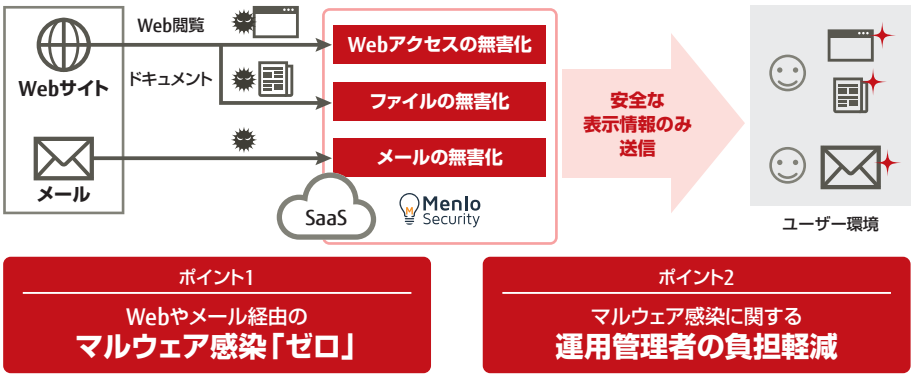

図1 富士通のIGSの概要

分離環境でしか開けないようにすることで、PCのマルウェア感染を防げるようになる。

Menlo Security社のWeb分離・無害化サービスを採用した富士通のIGS

富士通は、分離、無害化を実現するソリューションとして「アイソレーションゲートウェイサービス(IGS)」を提供している(図1)。IGSは、Menlo Security社のWeb分離・無害化サービスを採用したものである。Menlo Securityの国内導入実績は、2020年6月時点で累計135社、約45万ユーザーにも達している※。

IGSの特長は、専用ソフトウェアのインストールが不要で、インターネットアクセスにも日常的に利用しているWebブラウザをそのまま利用できる点だ。また、インターネットで取得したドキュメントをPCにダウンロードすることなくWebブラウザ上で安全に閲覧可能なため、ドキュメントに仕込まれたマルウェアを遮断できる。Webブラウザ上での閲覧だけでなく、ドキュメントを無害化してPDFでダウンロードすることや、セキュリティ対策を実施しオリジナルファイルをダウンロードすることも可能だ。

IGSはメールのセキュリティも強化する。メール本文内にあるURLを開いて悪意のあるWebサイトに誘導されても、IGSが無害化する。また、ドキュメントの無害化により、添付ファイルも安全に閲覧できるようになる。

これらの特長により、IGSは「セキュアなインターネット閲覧」「Webブラウザ経由のマルウェア感染の防止」、そしてマルウェア感染の防止により「運用管理者の負担の軽減」をもたらし、ひいてはVPNの利用による回線の逼迫、およびレスポンスの悪化による業務効率の低下を解消する。

IGSのメリットを活かした利用シーンを紹介しよう。1つ目が、社外環境での快適かつセキュアなインターネットアクセスの実現だ(図2)。冒頭でも述べたように、テレワークの増加に伴い社内ネットワークへアクセスするVPN回線が逼迫、レスポンスの悪化が業務に支障をきたしている。対して、IGSの導入により、社外環境のユーザーによるWebアクセスにおいて、VPN回線や社内ネットワークを通らず、直接インターネットへセキュリティを確保しながら接続できるようになる。これにより、快適かつ安全なアクセスが実現できるほか、回線の逼迫も解消されるため、VPN接続ユーザーや社内ユーザーのレスポンスも改善されるようになる。

2つ目は、不特定のWebサイトへのアクセスによる情報収集での利用例だ。マルウェアの侵入を防ぐ手段の1つに、インターネット接続用の端末と社内用の業務用端末を使い分ける「物理分離」がある。しかし、運用管理者には、インターネット接続用端末にはマルウェア感染のリスクが生じること、また、資産の二重管理という問題が発生していた。また、エンドユーザーも端末の使い分けや、入手した情報に対するセキュリティ対策の適用といった負担が生じていた。対してIGSを利用すれば、Webブラウザ経由のマルウェア感染をゼロにできるため、インターネット接続のための端末を分けずに済むようになり、資産管理の手間も軽減できる。

3つ目の利用シーンが、運用管理者の負担軽減だ。社内でセキュリティ教育を実施しても悪意のあるWebサイトにアクセスしたり、危険な添付ファイルを開いたりすることでマルウェア感染を引き起こすケースは後を絶たない。そうしたマルウェア感染への対処や影響調査などに、運用管理者は多くの負担を強いられているのが実情だろう。IGSは悪意の有無に関わらず、すべてのWebアクセスを分離し無害化するため、社員のITリテラシーに依存せず一貫したセキュリティ担保が可能になる。これにより、運用管理者もインシデント対応から解放されるようになる。

ニューノーマルに対応したテレワークの利用がますます加速していく中で、富士通はIGSの提供により、快適かつセキュアな外部へのアクセスを支援していく。

※ マクニカネットワークス調べ

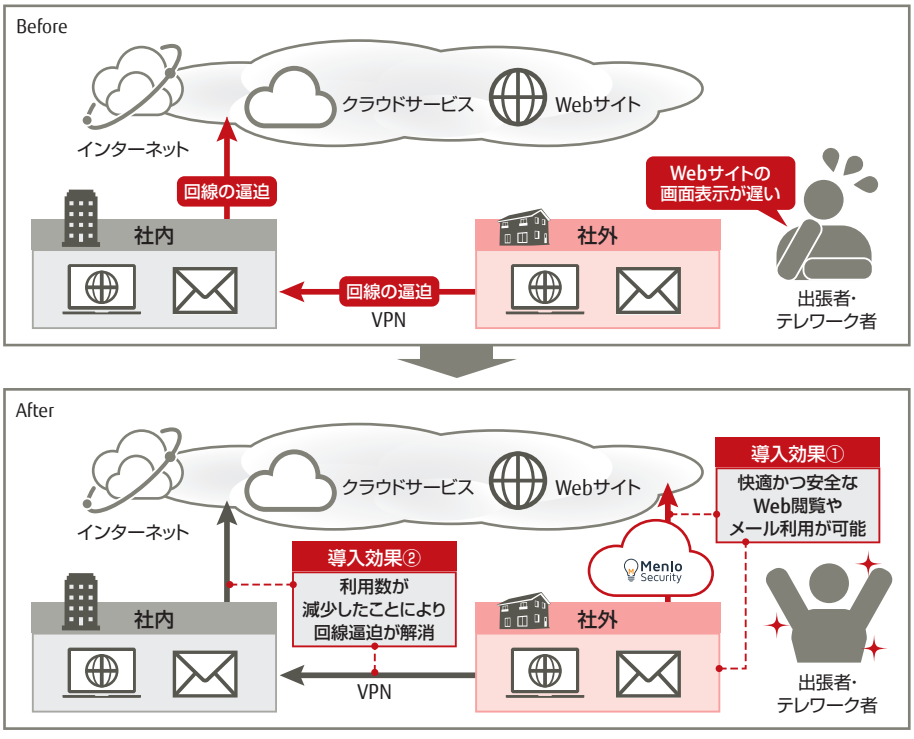

図2 IGSの導入により、社外からの快適かつセキュアなインターネットアクセスを実現

お問い合わせ先
富士通コンタクトライン(総合窓口)　0120-933-200
受付時間 9:00 ～ 17:30 (土曜・日曜・祝日・当社指定の休業日を除く)
富士通株式会社
https://www.fujitsu.com/jp/solutions/business-technology/security/secure/global-managed-security/isolation/