セキュリティ

ITマネジメント（内部統制）

「検知」しないでエンドポイントを防御！

コンテンツの「無害化」で安全なWebアクセスを実現

- 効果の高いセキュリティ対策として政府も推奨
- Webブラウザを使い分けることでリスクを低減
- クラウドで無害化を実現するMenlo Security

ランサムウェアを使って多くの企業に影響を与える、大規模なサイバー攻撃が立て続けに発生するなど、インターネットにおけるセキュリティリスクは高まり続けているのが現状であり、対策の強化は喫緊の課題となっています。こうしたサイバー攻撃に対抗する、新たなセキュリティ対策として広まり始めたWeb分離について詳しく解説します。

効果の高いセキュリティ対策として政府も推奨

機密情報を多く扱っているリスク感度の高い企業や地方自治体において、新たなセキュリティ対策として広まりつつあるのがネットワーク分離やWeb分離などと呼ばれる考え方です。これは業務システム利用とインターネット利用でネットワークや端末を切り分けるというもので、仮にインターネット経由でマルウェアに感染しても、業務システムなどへの侵入や機密情報の漏えいを阻止できる可能性が高まります。

ユーザーが直接扱う端末上で対策を行うエンドポイントセキュリティとしては、すでに既知のマルウェアを検出するウイルス対策ソフトや、外部との通信を制御するパーソナルファイアウォールが普及しています。またマルウェア対策という観点では、ネットワーク上でウイルスを検知・駆除するプロダクトが活用されているほか、未知のマルウェアを検出できるホワイトボックスもあります。

ただサイバー攻撃は巧妙化し続けており、さまざまなセキュリティソリューションを組み合わせても確実に脅威を検知するのは難しいのが現状です。そこで既存のセキュリティ対策のように脅威を検知し、有害であるかどうかを判定するのではない、まったく新たなアプローチに基づくエンドポイントセキュリティとしてWeb分離に注目が集まっているという背景があります。

こうした対策が浸透するきっかけとなったのは、2015年に起きた政府系機関における大規模情報漏えい事件です。この後、各自治体に対して住民基本台帳システムとインターネット用の端末を完全に分離することが求められたほか、経済産業省と情報処理推進機構が策定した「サイバーセキュリティ経営ガイドライン」においてもネットワーク分離の考え方が示されるようになりました。

2015 年 5 月の日本年金機構の情報漏えい事件を契機に、総務省や IPA は相次いで業務端末をインターネット環境から分離するように推奨

日時	内容
2015年7月	政府は、「サイバーセキュリティ戦略」の見直し案の中に、重要情報を扱う政府機関の情報システムを、インターネットから分離する対応策を盛り込む方針。
2015年8月12日	日本年金機構の個人情報流出問題を踏まえた緊急対策として、各自治体の住民基本台帳システムとインターネット用の端末とを完全に分けるよう求めた。
2015年10月13日	約1,700の全市区町村で、住民基本台帳ネットワークシステム（住基）とインターネット間の通信を遮断する措置を完了したことを発表。
2015年12月28日	経済産業省は、IPAとともに一般企業の経営者向けに策定した「サイバーセキュリティ経営ガイドライン」において、サイバーセキュリティリスクに応じた対策の例として、多層防御やネットワーク分離などを示した。

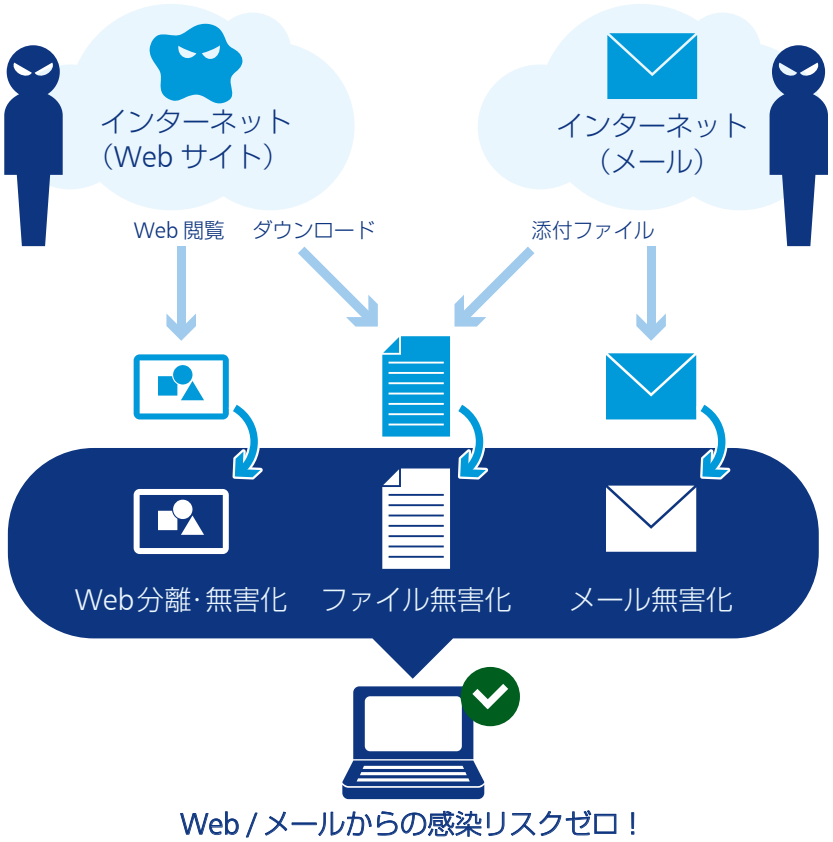
Webブラウザを使い分けることでリスクを低減

このネットワーク分離の実現方法の1つがWeb分離です。具体的には、社内の業務システムを利用する際にはパソコンにインストールされているWebブラウザ、インターネットにアクセスする際にはクラウド上で実行するWebブラウザを遠隔操作で利用と、2つのWebブラウザを使い分けます。

このようにアクセス先に応じてWebブラウザを使い分けることで、仮にマルウェアが仕掛けられたインターネット上のWebサイトにアクセスしても、感染するのはクラウド上の環境であり、実際に利用しているパソコンには影響しません。ただデメリットはクラウド上に別のデスクトップ環境を用意する必要があり、そのコスト負担が発生すること、そしてWebブラウザを使い分ける手間をユーザーに強いることです。

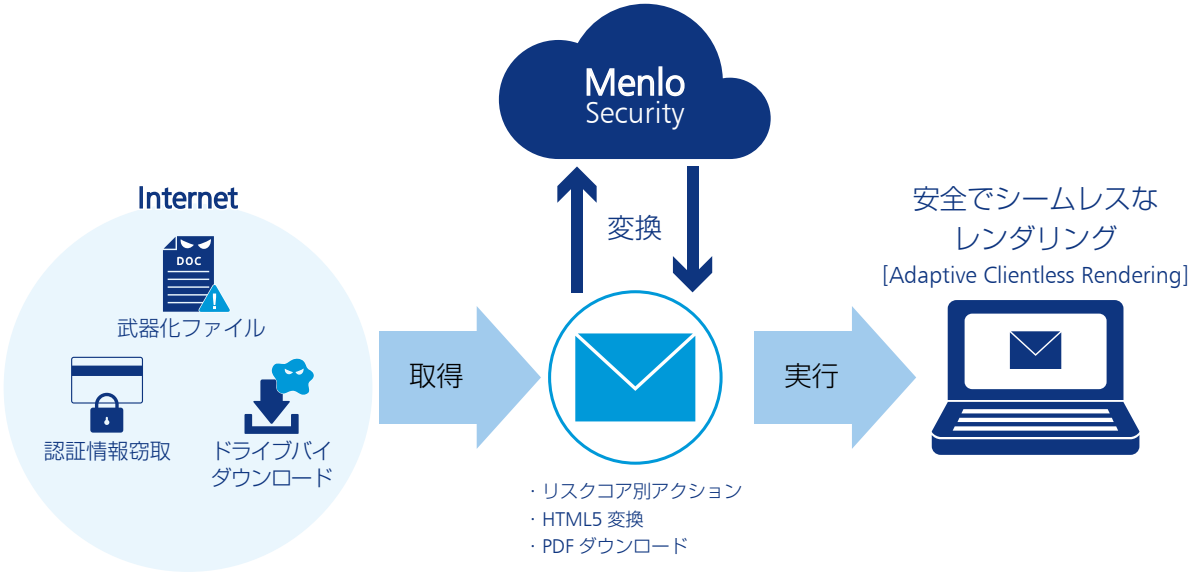
そこで注目されているのが、無害化と呼ばれるセキュリティ対策です。従来のセキュリティ対策は、マルウェアや攻撃コード、悪意のあるコンテンツなど「検知」することを前提としていますが、新手の攻撃手法が次々と現れることを考えると、100%検知することはほぼ不可能です。

無害化ソリューションでは、受信するすべてのコンテンツに悪意があると仮定し、仮想環境でコンテンツを実行した上で画面に描画する内容だけをパソコンに送信します。これにより、たとえばWebコンテンツに不正なスクリプトが含まれていても、その内容がパソコンで実行されることはなく安全だというわけです。

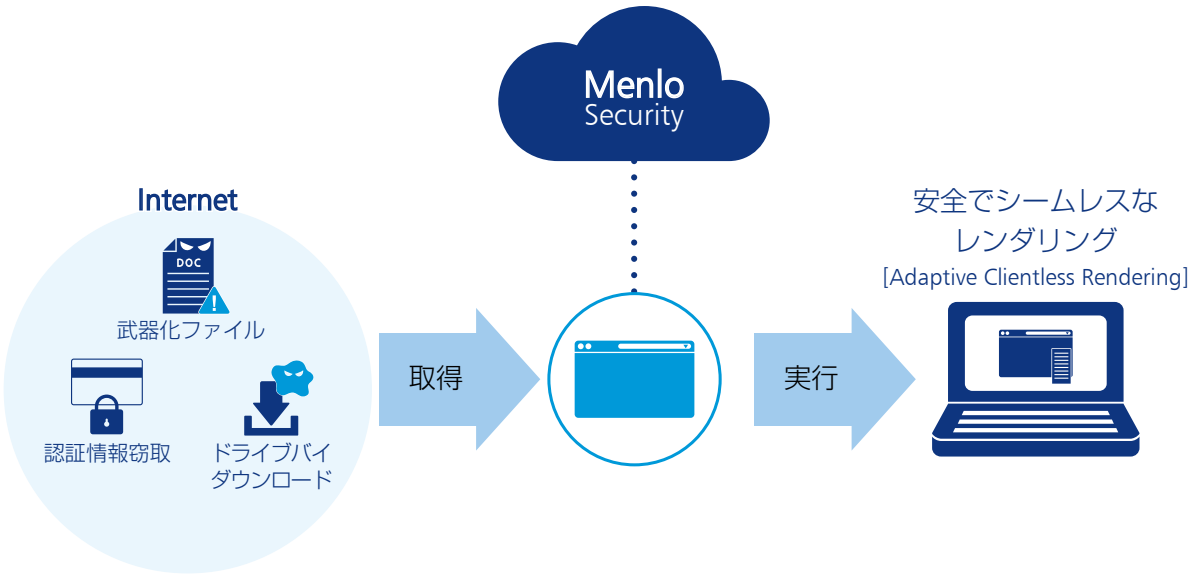


クラウドで無害化を実現するMenlo Security

こうした無害化を実現するソリューションの1つが「Menlo Security」です。インターネット上から取得したコンテンツをクラウド上で実行し、安全な情報だけをパソコンに転送することで無害化を行うソリューションであり、クラウドサービスとして提供されています。



受信したメールを無害化する仕組みも用意されています。添付ファイルとして送られてきたWordファイルなどをHTMLに変換し、無害化した上で表示する機能があるほか、メール本文中のURLも自動で書き換え、コンテンツを無害化した上で配信することが可能です。



NTT Comでは幅広いセキュリティソリューションを提供しているほか、Menlo Securityの導入を支援するサービスも提供し、お客さまのセキュリティ対策強化をトータルでサポートしています。

おすすめソリューションサービスはこちら

Menlo Security Web Isolation Service

お客さま端末とインターネット上のWebサーバーの間の通信を代理サーバーで中継しつつ、インターネット側から送られてきたコンテンツに代理サーバーが無害化処理を施し、お客さま端末に転送する仕組みです。これにより、インターネット経由でのマルウェア感染のリスクを低減することが可能になります。