技術解説

知っておきたい！注目の情報セキュリティ技術

巧妙化しているサイバー攻撃に対応するために情報セキュリティの技術開発も積極的に進められている。
しかし、新しいセキュリティ技術に対応した新たなサイバー攻撃が次々と登場しているのが現状だ。
病気のウイルスと同様、コンピュータのウイルスも絶えず変異・進化している。ウイルスの情報とその対策としての技術情報を常にチェックすることがウイルスから重要情報を守る最初の防御となる。
今回は標的型攻撃対策とスマートデバイス対策を中心に注目の技術を紹介する。

標的型攻撃対策

標的型攻撃に対するセキュリティ対策では、ウイルスを社内に入れない入口対策や、社内にウイルスが侵入後の感染防止や情報の保護、流出の防止まで総合的な対策が必要となる（図1）。ここでは、キーポイントとなる入口対策、感染防止と出口対策におけるセキュリティ技術を紹介する。

●入口対策、感染防御

従来のアンチウイルス型の手法は、データをスキャンしてパターンファイルと照合し、ウイルスを検出していた。しかし、標的型攻撃はターゲットごとに新種のマルウェアを作成したり、なりすましメールなどの巧妙な手段でパターンファイルの網をすり抜けてしまう。

現在、こうしたパターン非依存マルウェアへの技術的対策として振る舞い検知型のマルウェア対策技術が注目されている。例えば、振る舞い検知型のクラウドサービスを利用する企業は、ダウンロードするファイルをサービス提供者の仮想クラウド環境に転送して実行し、その動作を観察する。外部との不自然な通信、アンチウイルスプログラムからの隠ぺいなど不審な動作を行ったファイル（プログラム）はマルウェアの疑いがあると判断できる。

実環境で動いている他のアプリケーションやOS自体に影響を与えず、ネットワークやホストマシンのスループットを損なうこともなく不審なファイルを検出することが可能となる。

また、社内のマルウェア感染状況を可視化するSaaS型サービスも登場。社員が使うクライアントPCやサーバにエージェントソフトをインストールし、リアルタイムに情報を収集することで、社内LANにおけるマルウェアの感染状況や感染経路などを可視化する。

●出口対策

標的型攻撃は、事前に標的対象の企業を十分に調査したうえで執拗な攻撃を仕掛けるため、マルウェアの内部環境への侵入を防ぎきることは難しい。これからは、外部に公開している環境への対策だけではなく、イントラネット環境についても侵入を前提とした対策が必要だ。

出口対策では内部の情報流出を防止することが目的となる。標的型攻撃における情報流出は、マルウェアに感染したPCが社内のサーバから個人情報や機密情報などの重要な情報を詐取し、外部へ送信することで行われる。この対策として認証プロキシの導入がある。プロキシサーバを利用する際には認証が必要となるため、ウイルスがプロキシサーバ経由で通信する機能を持っていても、ユーザー名やパスワードがわからない限りインターネットにアクセスすることはできない。

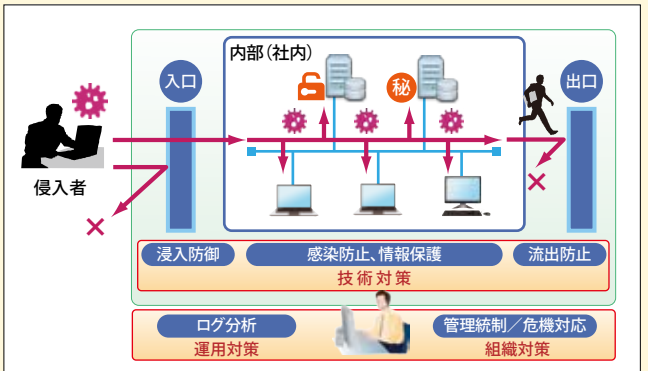

図1 入口から感染防御・情報保護、流出防止まで総合的な対策が必要

しかし、いずれはマルウェア側が新たな手口で対抗することも考えられるため、接続先Webサーバのフィルタリング、HTTP/HTTPS以外のアウトバウンド通信の制限、送信メールのコンテンツチェックなどの対策と組み合わせることが大切だ。

独立行政法人 情報処理推進機構（IPA）が公開している『「新しいタイプの攻撃」の対策に向けた設計・運用ガイド』では、ウイルスの活動増強や深部への侵攻を指令するバックドア通信を遮断するための出口対策について8つのポイントを挙げている。

1.サービス通信経路設計の実施
　対策目的：経路ルール違反通信の遮断

2.ブラウザ通信パターンを模倣するhttp通信検知機能の設計
　対策目的：httpメソッド利用バックドア通信の遮断

3. RAT※の内部proxy通信（CONNECT接続）の検知遮断設計
　対策目的：RAT通信の遮断

4.最重要部のインターネット直接接続の分離設計
　対策目的：最重要部へのバックドア設置の回避

5.重要攻撃目標サーバの防護
　対策目的：攻撃対象となる重要サーバの防護

6.スイッチなどでのVLAN（Virtual LAN）ネットワーク分離設計
　対策目的：バックドアウイルスの拡散範囲の限定

7.容量負荷監視による感染動作の検出
　対策目的：バックドアウイルスの内部拡散検知

8.P2P到達範囲の限定設計
　対策目的：ローカルセグメント上に感染したバックドアウイルス間の一斉機能更新などの防止

※RAT（Remote Access Trojan/Remote Administration Tool）：侵入したシステムを遠隔から操作するためのプログラム。潜伏活動や窃取活動で利用されている

スマートデバイス対策

●モバイルデバイス管理 MDM（Mobile Device Management）

スマートデバイスの業務活用における脅威とリスクは端末だけではなくネットワークやシステム全体に及ぶため、セキュリティ対策もシステム全体を俯瞰的にとらえることが必要となる（図2）。ここでは、ユーザーに関わる端末のセキュリティ対策に有効なMDMを紹介する。

MDMは統一したポリシーのもと、遠隔から端末やデータの集中管理を実現する。その機能は以下の3つに分けることができる。

1. 紛失・盗難時の情報漏えい対策

紛失・盗難時にはリモートロックやリモートワイプを活用して情報漏えいを防止。またセキュリティポリシーを配布し、パスワードロックや桁数指定を含む複雑なパスワードなどを強制する。

2. 不正利用の防止

特定のアプリケーションの利用やカメラ機能、アプリケーションのインストールなど情報漏えいにつながる可能性のある機能を無効化する。

3. スマートデバイス管理の一元化と業務効率化の実現

MDMは、端末ID、OSのバージョン、セキュリティポリシーの適用状況など、社員に配布したスマートデバイスの情報を収集し一元的に管理できる。ポリシーを更新した場合も遠隔からの適用が可能だ。

MDMシステムのタイプには、ネットワークを介し必要に応じて利用できるSaaS型と自社で運用するオンプレミス型の2種類がある。SaaS型はスモールスタートに適し、オンプレミス型は企業の方針として情報を社内で管理するといったニーズに応える。

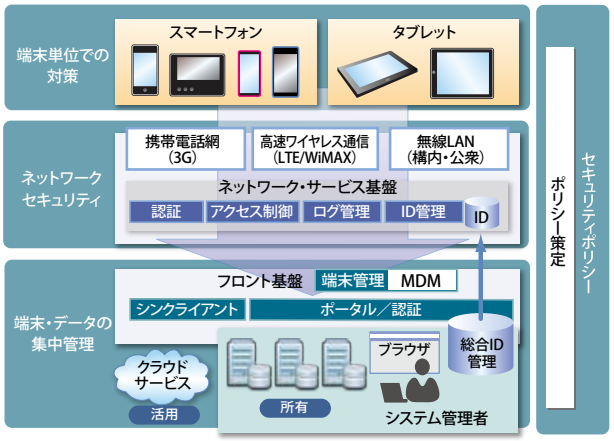

図2 端末のみではなくシステム全体のセキュリティ対策が重要

統合的セキュリティ対策

●統合脅威管理 UTM（Unified Threat Management）

現在、さまざまな脅威に対応するために、ファイアーウォールに加え、不正侵入検知・防御、Webコンテンツフィルタリング、アンチウイルス、アンチスパムなど多くのセキュリティ機能が必要となる。しかし、すべてを個別に組み合わせていてはコストが増えるばかりだ。また、導入時の設定や導入後の運用管理も複雑になる。特に専任のセキュリティ担当者が社内にいない中堅・中小企業にとって管理面の負担は深刻だ。大企業においても分散する拠点やオフィスに対し、セキュリティ機能を個別に導入していたのでは管理コストが増大する。

こうした課題を解決するのが、複数のセキュリティ機能を統合的に管理できるUTMだ。運用面、コスト面などのメリットに加え、多数のセキュリティ機能をゲートウェイレベルで統合することにより、複数の攻撃手法を組み合わせた脅威にも有効な対策を施せる。しかし、複数の機能を集約しているため機能性やパフォーマンス、拡張性が専用機に比べて劣る場合もある。また、UTMがダウンするとインターネット接続まで使用できなくなる可能性もあり、セキュリティに対する自社の要求とコストのバランスを考慮したうえで選択することが大切になる。

情報漏えい対策としても有効なビジネスWebメール

Webメールというとサービスプロバイダーが提供するサービスを思い浮かべるかもしれない。しかしここで紹介するのは、企業が自社内に構築するビジネスWebメール環境のことである。

Webブラウザを利用するWebメールのメリットは、どこからでもアクセスできるという特長から、ワークスタイル変革や事業継続性の観点から語られることが多い。しかしWebメールでは送受信データもアドレス帳もサーバ側にあり、Webブラウザはその内容を表示するだけなので情報漏えい対策にも有効だ。端末内にデータが一切存在しないため、標的型攻撃によるメールアドレスなどの悪用も防止できる。

情報セキュリティと内部統制、コンプライアンス対策をより確実にするために自社内にこうした環境を構築することは有利だ。さらに現在は、ビジネス向けにSaaS型のWebメールサービスが提供されている。最新のセキュリティ対策が施されていることに加え、コストや災害対策面でも有利で、多くのユーザーを獲得しつつある。

仮想マシンの安全性を高めるセキュリティ技術

従来のセキュリティ対策の多くは物理サーバ環境を対象としており、そのままでは仮想マシンへの適用が難しいケースも多い。例えば、共通の物理サーバで稼働する複数の仮想マシンがマルウェアスキャンを実行すると、物理サーバのCPUに過度の負荷がかかったり、ディスクの読み書きが頻繁に発生するといった課題がある。また仮想マシンが物理サーバ間を移動した際、常に同一のセキュリティポリシーに基づいた制御を行うことが困難な場合もある。こうした課題に対し、ハイパーバイザーの機能（VLAN機能を備える仮想スイッチ）を活かしたセキュリティ技術の開発も始まっている。サーバ仮想化を本格的に活用していく時代を迎え、仮想マシンのセキュリティに関わるリスクも拡大していくだろう。今後はハイパーバイザーの機能を利用したセキュリティ対策にも注目しておく必要がある。