

最新情報セキュリティ対策総覧(第8回)

外部脅威と内部脅威を同時に対策する

2021.09.15



企業のセキュリティ対策は、ランサムウェアや不正アクセスなど「外部の脅威」に備える取り組みに意識がいきがちだ。しかし、実際には社員によるデータ持ち出し、紛失といった「内部の脅威」が引き起こす問題も多く、双方を意識した対策を講じなくてはならない。ただし、あまりにも厳しい対策で仕事の効率低下は避けたい。脅威に備えつつ業務効率化を進める方法を考えてみよう。

「セキュリティおまかせプランプライム」と「おまかせAI働き方みえ〜る」セットで幅広い脅威対策

NTT西日本が提供する「セキュリティおまかせパッケージ」は、同社の「セキュリティおまかせプランプライム」と、「おまかせAI働き方みえ〜る」の2ソリューションを組み合わせたパッケージサービスだ。それぞれの主な機能を以下に示す。

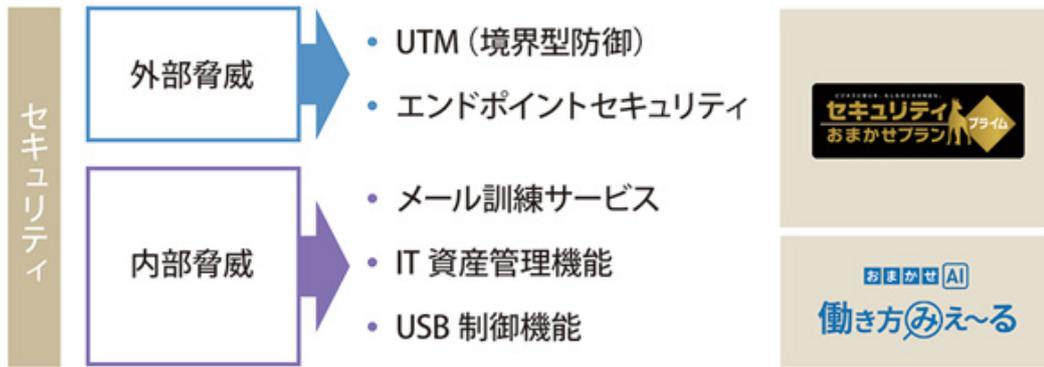
・「セキュリティおまかせプラン プライム」

標的型サイバー攻撃やランサムウェア侵入を防ぐ「UTM(ゲートウェイセキュリティ)」と、パソコン、スマートフォンなど各種IT機器のセキュリティを一元管理する「エンドポイントセキュリティ」により、さまざまな脅威から企業のシステムを防御する。

・「おまかせAI働き方みえ〜る」

業務で利用するパソコンの操作ログ(履歴)を専用アプリケーションで収集し、独自のAIを使って多角的に分析。その結果を定量的にレポートする。

本ソリューションは、「セキュリティおまかせプランプライム」が主に外部からもたらされる脅威に備える部分に特化しているのに対し、「おまかせAI働き方みえ〜る」は内部の脅威を対象にしている。なお、サービスの提供に際しては、いずれのソリューションも導入後のサポートを重視し、専門スタッフによる定期的な報告を継続するとともに、新たな対策が必要な場合には随時アドバイスを行うなど、きめ細かな支援を実施する。



それぞれの守備範囲とメリット紹介

では、セキュリティ対策として本ソリューションを活用した場合の具体的なメリットを考えてみよう。まずセキュリティおまかせプラン プライムについては、悪質化・巧妙化が著しいサイバー攻撃への対応力が挙げられる。

ご存じの通り、サイバー攻撃の手法は絶えず変化しており、対策が後手に回ってしまうケースが少なくない。多額の予算をかけて対策を講じて、少し経過するとたちまち「時代遅れ」になってしまう場合もある。そこで、本ソリューションでは不測の事態に備えてシステムを常時監視し、重大なインシデント発生時にはNTT西日本のサポートセンターがお客さまへの能動連絡を実施。被害の拡大を未然に防ぐと同時に、必要時には西日本エリア内最寄りの保守拠点から専門スタッフが駆け付ける体制を整備している。

一方、おまかせAI 働き方みえ〜るは、外部脅威に比べて軽視されがちな内部脅威(社員の不正、ミスを原因とするインシデント)の発生を防ぐ部分に重点が置かれている。本ソリューションはパソコンの操作ログ分析により業務効率化を図るのを目的に開発されたものだが、分析結果には作業時間、業務の進め方といった「働き方」に関する要素だけでなく、重要データの持ち出しや不自然な操作など、内部脅威となり得るものが多く含まれる。

月次レポート(月1回提供)に加え、日々確認できる日次レポートの中で普段の行動と異なるもの、注意が必要なものについてはアラートを出す機能を具備する。現在、あるいは将来的に内部脅威へとつながりかねない行動の気付きにつなげ、セキュリティ向上に役立てられる。

例えば、どのファイルを持ち出しているか、機密度の高いファイルをUSBなどに格納した場合は気付きとしてアラートで管理者にお知らせがいく、またUSB制御機能を活用すれば利用制限をかけられる。

一元的なセキュリティ対策だけでなく業務効率化も

セキュリティおまかせパッケージ導入のメリットとして、もう1つ見逃せないポイントがある。外部・内部脅威の「統合管理が可能」という点だ。最近では各社からさまざまなセキュリティ対策ソリューションが提供されているが、それぞれ別会社から個別に導入すると万が一のときの対応や相談ごとがあったときなど、どこに連絡すればよいか迷ってしまう懸念がある。その点、パッケージ化されていればサポート的にも相談先を選ばずに対応を依頼できる安心感がある。

さらに、本ソリューションは業務効率化を支援する役割を担っている。ログ解析から効率化に必要な社員の働き方を分析し、離れた拠点間のマネジメントやリモートワーク時のマネジメントにも活用できる。内部にセキュリティ専任者を置く必要もないので、人的資本を思い切って本来業務に投入できる。一見相反するセキュリティ対策と業務効率化を、同時に充実させる心強いサービスだといえるだろう。

※掲載している情報は、記事執筆時点のものです