テレワークの拡大とともに高まるリスクにどう対処する? 「EDR」と「UEBA」で実現する端末防御と内部情報漏えい対策

働き方改革の推進、昨今の新型コロナウイルス感染拡大抑止を目的に企業・組織におけるテレワークの活用が加速している。だが、ゼロデイ攻撃や内部からの情報漏えいなど、情報システム担当を悩ますセキュリティ脅威はますます増大しており、テレワーク下における端末セキュリティの強化が喫緊の課題として浮上している。本書では、脅威からの防御と運用負荷の抑制を両立する、ニューノーマルな時代に対応した端末セキュリティの最新動向について解説していく。

ニューノーマルで 新しいセキュリティ対策の適用が急務

世界経済フォーラムが発表した「グローバルリスク報告書2020年版」によれば、2020年に悪化が予測されるリスクとしてサイバー攻撃が5位にランクされるなど、世界の経営トップは増大するセキュリティの脅威を重要な課題として挙げている。事実、攻撃者以外は誰も知らない弱点を突くような「ゼロデイ攻撃」のツールが安価に売買されるなど一般化し、サイバー攻撃は巧妙化とともにさらなる拡大の様相を呈している。

一方、テレワークやWeb会議、オンラインセミナーといったニューノーマルな時代の働き方が拡大するのに伴い、サイバー攻撃も受けやすくなっている。企業においてはオフィス外で利用されている端末の管理は困難となり、また、サイバー攻撃を受けた際の状況の把握や調査がしづらくなる、という課題が浮上している。加えて、社外に持ち出された端末などに監視するべき範囲、対象が広がったことで、情報漏えい事故を未然に捉えることが難しくなる、というリスクも危惧されている。

このような背景から、新しい働き方に対応するサイバー攻撃対策と、内部情報漏えい対策の実施が喫緊の課題となっているのだ。そのための具体的な手法が「端末単独で動作する強力なサイバー攻撃対策」と「ユーザーの普段と異なる振る舞いの可視化」である。

運用負荷を抑制しながら 端末セキュリティを大幅に強化

はじめに端末へのサイバー攻撃対策について見ていこう。従来、企業のセキュリティ対策はファイアウォール、アンチウイルス、Webフィルターといった「入口対策」「出口対策」を主軸としてきた。しかし近年では、先に述べたようなゼロデイ攻撃や、複数の防御をすり抜けるマルウェアの登場に加え、オフィス外での端末の利用拡大も考慮し、「侵入を前提としたセキュリティ対策」へのシフトが喫緊の課題となっている。

そうした要請に応えるものが、「EDR(Endpoint Detection & Response)」だ。EDRとは、端末の動作ログを収集・分析するとともに、悪意のある動作を検出、必要な対策を施すというもの。富士通は、高い第三者評価と数多くの導入実績、そして優れた機能性を有する米国Cybereason社のEDR製品を活用した「FUJITSU Security Solution Cybereason EDRサービス(Cybereason EDRサービス)」を提供している(図1)。EDRは強固な端末セキュリティを実現するものの、自社で運用していくにあたっては、挙げられたアラートへの適切な判断、過検知への対処、さらには高度な分析を行うセキュリティ担当者のアサインといった課題が生じる。Cybereason EDRサービスはそうした課題を解決するものだ。

EDR運用に特化した富士通の専門チームが、企業のEDR環境を24時間監視、EDRアラートの監視から問題発生時の連絡を行い、万が一、被害が発生してしまった際にはインシデントレスポンスを

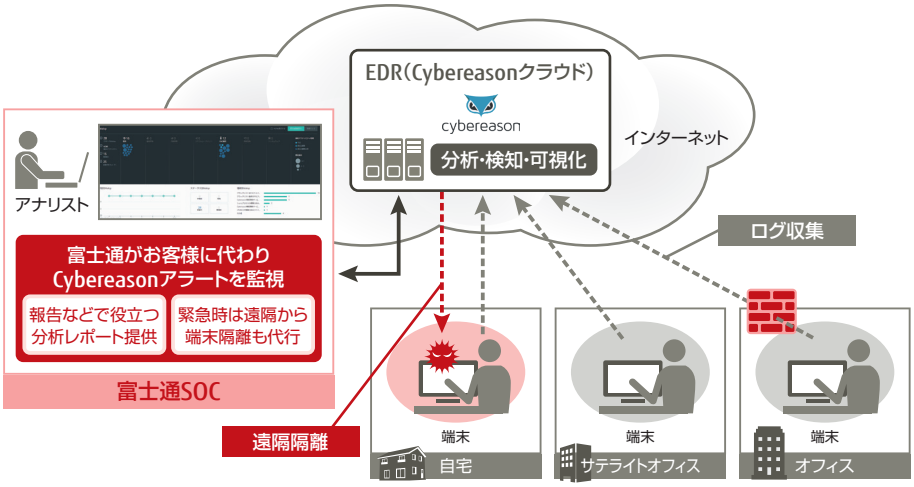

図1 Cybereason EDRサービス

提供することも可能だ。さらには事象のさらなる深掘りや、場合によってはディスクのフォレンジックなどを通じて、証拠保全、恒久対策、復旧なども支援する。

具体的な動作としては端末にインストールしたCybereasonエージェントから端末の動作ログをCybereasonクラウド上にアップロードして分析、不審な行動を検出し、アラートを発生させる。これらの過程はすべて自動で行われる。さらに、アラートに対して富士通のアナリストが様々な観点で分析を行い、最終的に影響を及ぼしそうなものについてのみ、ユーザーに通知を行うなどの対応を実施する。このようなインシデント通知だけでなく、分析レポート提供や、端末隔離の作業代行も統合セキュリティ運用サービスの中で実施するので、EDRを利用する際の運用負荷を大幅に抑制できるようになる。

ユーザーの不審な行動を分析し 不正行為や内部からの情報漏えいを未然に防止

続いて、ユーザーの普段と異なる振る舞いの可視化について見ていこう。近年、調査会社のレポートからも、従業員による管理ミスも含めた情報の紛失、退職者による不正な情報の持ち出しによる被害の拡大が報告されている。そうしたリスクを解消する手段として、人の行動分析によるセキュリティリスクの検出・可視化を実現する「UEBA（User Entity Behavior Analysis:ユーザー行動分析）」が注目されている。

UEBAは人の行動を分析、不正な行動をしているかどうか判定を行うことで脅威の予兆を検知し、被害を未然に防止するというもの。しかし、人の行動監視による内部脅威対策を実施していくにあたっては、分析や監視を行うための専門知識やスキルをもった人員が社内に不足していることをはじめ、取得した膨大なログデータから関連情報のみを抽出し分析するのに多大な時間と労力を要すること、さらにテレワークの推進に伴い、オフラインでの行動ログが収集できないといった課題が挙げられている。

そうした課題を解消するため、富士通では、グローバルでの豊富な導入実績を有する米Dtex Systems社のUEBA製品「Dtex」を活用したソリューションを提供している（図2）。

Dtexの特長は、ユーザーの行動の可視化に特化していること、そして、振る舞い分析によって内部脅威の発生が予兆できることだ。Dtexは、Cybereasonと同様に端末にエージェントを導入することでユーザーの意図を把握するための行動情報を収集、特に内部不正に関わるデータを抽出して、管理サーバーにログを送付する。具体的には、セッション情報からインタフェース情報まで人の行動分析の観点から必要なログだけを取得し、内部からの情報漏えいの予兆に関する行動特性などをカテゴライズした上で分析する。オフラインでもログを収集できるので、テレワーク環境下でも利用可能だ。そうした「悪意ある行動」や「不注意な行動」の予兆や、脅威となる予兆の度合いが高いユーザーの行動は、Dtexのダッシュボード画面を通じて一元的に参照できる。

しかし、ユーザーの不審な行動が可視化されるとはいえ、それらの行動を自社内で分析してリスクをいち早く把握したり、適切な対処を行うことが困難なケースもあるだろう。このような事象に対して富士通では、Dtexの運用に際して、専門的なスキルと知識を有するアナリストによるリスク分析や適切な対応、そして改善提案もサービスとして提供している。

安全なテレワーク環境の実現、ひいてはニューノーマルに対応したセキュリティ対策を実施していくにあたっては、強固な端末セキュリティと人の行動に視点を置いた不正対策が必要と富士通は考える。富士通は、運用サポートも含めたEDRおよびUEBAソリューションの提供により、企業・組織におけるセキュリティ対策の強化を全方位で支援していく。

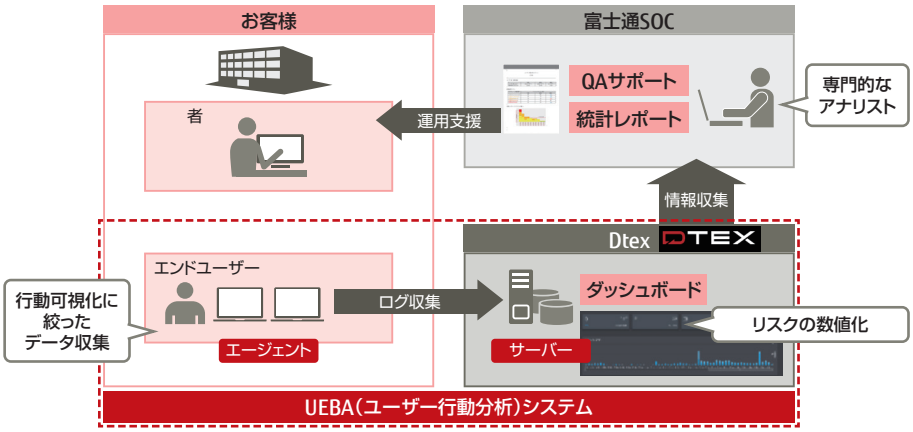

図2「Dtex」を活用した富士通のUEBAソリューションの概要

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/security/