サイバー攻撃へ対抗するための インシデントレスポンスの自動化

EY ストラテジー・アンド・コンサルティング（株）
Technology Consulting／Cybersecurity Leader　松下 直

▶ Naoshi Matsushita

サイバーセキュリティにおいて、20年以上の業務経験を有し、セキュリティアセスメント、セキュリティシステムの導入、セキュリティインシデント検知・対応サービス、インシデント対応シミュレーション、セキュリティ教育などを官公庁、金融、製造、小売、商社などの多数の国内外組織に提供してきた。国内外の先進的ベンチャー企業との提携、海外での事業の立ち上げの経験も有する。

Ⅰ　はじめに

企業におけるサイバー攻撃の被害はますます深刻になっています。一方、セキュリティ関連業務は増え続けており、セキュリティ人材は常に不足しています。本稿では、サイバー攻撃によるセキュリティインシデントの検知と、対応を自動化することで人手をかけずにサイバーリスクを軽減する方法について紹介します。

Ⅱ　サイバーアタックの被害の甚大化

独立行政法人 情報処理推進機構（IPA）が発表した2021年上半期のコンピュータウイルス・不正アクセスの届け出事例によると、「身代金を要求するサイバー攻撃」、「IDとパスワードによる認証突破」や「脆弱性をついた不正アクセス」が依然として多く報告されています（＜表1＞参照）。一方、「コンピュータウイルスの検知・感染被害」は減少傾向にあります。これは、昨年猛威を振るった「Emotet」と呼ばれるコンピュータウイルスの攻撃基盤が停止された効果と考えられていますが、怪しいメールの添付ファイルを安易にクリックしないといった啓蒙や、パッチ適用の自動化といった企業の地道な努力も徐々に効果を上げていると考えてもよいでしょう。

▶表1　コンピュータウイルス・不正アクセスの届出事例の傾向

インシデントの分類	件数
コンピュータウイルスの検知・感染被害	14
身代金を要求するサイバー攻撃の被害	30
ID とパスワードによる認証を突破された不正アクセス	31
脆弱性や設定不備を悪用された不正アクセス	24
サプライチェーンに関するインシデント	23
その他	6

出典：IPA「コンピュータウイルス・不正アクセスの届出事例［2021年上半期（1月～6月）］」
www.ipa.go.jp/files/000093083.pdf

ウイルス感染が減少傾向であることは望ましいことですが、サイバー攻撃の被害としては、より実害の大きい攻撃の報告が増えているという見方をすべきです。身代金要求といっても、ウイルスの一種であるランサムウェアに感染させてデータを暗号化し、復号のための鍵が欲しければ身代金を払えと脅迫するような攻撃だけではありません。企業ネットワークに侵入後、顧客情報など企業にとって外部に漏らしてはならない機密情報を詐取し、身代金の支払いに応じなければ外部に公開するといった脅迫や、ウェブサイトをマヒさせる攻撃を仕掛けておき、身代金を支払わないと再度攻撃すると脅すようなものまで含め、二重三重の脅迫を行う攻撃も実際に起きています。

企業はこのようなサイバー攻撃によるセキュリティインシデントを一刻も早く検知し、迅速に対応する必要に迫られています。

Ⅲ　枯渇するセキュリティ人材

前述の「コンピュータウイルス・不正アクセスの届出事例」には、今年新たに「サプライチェーンに関するインシデント」という分類が登場しています。企業が業務を委託する際に顧客情報などの機密情報を渡し

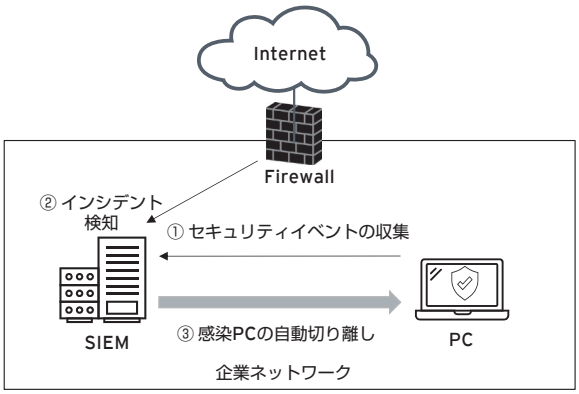
たり、あるいはクラウド上に保存したりした後、その委託先やクラウドがサイバー攻撃の被害に遭って情報漏洩が発生するというようなケースがこの分類に含まれます。このようなリスクを軽減するために、企業は委託先や利用するクラウドについてもセキュリティ対策が十分かを事前に確認することが求められています。また、コロナ禍によりここ1年半の間に企業はテレワーク環境への急速な移行を迫られました。全員もしくは半数の従業員がテレワークを行う状況に、リモートアクセスのインフラの増強だけでは追いつかず、どこからでもアクセスできるクラウドの利用が加速化しています。企業のセキュリティ担当者は、自社システムのセキュリティ対策で手いっぱいであった状況に加えて、コロナ禍で急速に拡大したテレワーク導入の際に積み残したセキュリティ対策、さらには利用するクラウドや委託先のセキュリティ対策の確認業務も加わり、ますますセキュリティ人材の不足が深刻化しています。

Ⅳ　SOARを用いたセキュリティインシデントへの自動対応

企業はサイバー攻撃によるセキュリティインシデントの検知と対応を迅速に行わなくてはなりません。攻撃の初期段階でインシデントを検知し、侵害を受けたPCやユーザーアカウントを停止すれば、顧客情報の漏洩といった深刻な被害に至る前に対処できる可能性があります。セキュリティインシデントの検知と対応を24時間365日の体制で行うセキュリティオペレーションセンター（SOC）においては、SOCアナリストがこのような業務を担うのが一般的です。自社でSOCを構築する代わりに、SOCを外部に委託している場合もあります。

SOCにおいては、ファイアーウォールやアンチウイルスソフトに代表されるセキュリティ製品からセキュリティイベントを収集し、サイバー攻撃や社内システムにおいての怪しい挙動を監視します。その際に用いられるのがSecurity Information and Event Management（SIEM）です。SIEMは、セキュリティ製品から収集するセキュリティイベントを常時分析し、ランサムウェアへの感染といったセキュリティインシデントを検知した場合にはアラートをSOCアナリストに通知します。SOCアナリストはインシデントの内容を確認し、セキュリティ製品を操作して、感染したPCを切り離すといったインシデント対応を行います。SOCアナリストによる手動でのインシデント対応にはある程度の時間を要し、対応手順が複雑な場合や同時に複数のインシデントの対応を行わなくてはならない状況では数時間かかる場合もあります。サイバー攻撃の被害が深刻化している現状を考えると、この対応の遅れが被害の拡大を招きかねません。SIEMの主要な製品では、Security Orchestration, Automation and Response（SOAR）というセキュリティ製品と連携してインシデント対応を自動化する機能が利用できます。発生し得るセキュリティインシデントを洗い出し、インシデント対応を実施する条件を決め、セキュリティ機器との自動連携のAPIを利用したインシデント対応のフローを組み込んでいく作業を事前に行う必要がありますが、インシデント発生時には迅速に対応を行うことができます（＜図1＞参照）。当社での利用実績においては、インシデントの種類にもよりますが、対応時間を10分の1以下に短縮することができています。

▶図1　SOARによるインシデント対応の自動化



Ⅴ　おわりに

本稿で紹介したSOARは決して新しいものではなく、当社においても海外を中心に十分な利用実績のある技術ですが、日本ではインシデントの誤検知により誤った対応がとられるリスクを危惧し、導入に二の足を踏む企業がほとんどでした。セキュリティ人材が枯渇する一方、サイバー攻撃の被害がますます深刻化する昨今の状況において、人手をかけずにサイバー攻撃の被害を極小化できるSOARの導入を改めて検討すべき時期に来ています。

お問い合わせ先
EYストラテジー・アンド・コンサルティング（株）
E-mail：Naoshi.Matsushita@jp.ey.com