Logstorage

純国産 統合ログ管理システム
国内導入 / ログの収集実績多数！

「防御一辺倒」では不十分なサイバー攻撃対策 ログ管理・分析を通してより本質的な対策を

近年、サイバー攻撃によって社内の情報が漏洩したり、システムの正常稼働が妨げられるといった被害を耳にする機会が増加しているのではないだろうか。IT 技術、デジタル技術がビジネスに欠かせない柱となっていることの裏返しでもあるが、サイバー攻撃はかつてのような「対岸の火事」ではなく、どの会社にとっても「自分事」となりつつある。

もしかすると中堅・中小企業の場合、「サイバー攻撃は名前の知られた組織や大企業を狙うものであり、自社は関係ない」と考えているかもしれない。しかしその思い込みは危険だ。

サイバー攻撃者は常に、より少ない手間で多くのリターンが得られる手法を探っている。セキュリティリスクを認識し、ある程度の対策を講じてきた組織や大手企業よりも、そうした企業と取引のある周辺の中堅・中小企業をまず狙い、本丸となる組織・企業へ侵入する際の踏み台として悪用するケースが増えているのだ。サプライチェーンや商流に乗じた攻撃が増えていることを踏まえ、取引先から何らかの対策や対応体制のチェックを求められる場面も増えている。

こうした背景から、規模や業種を問わず、いよいよサイバーセキュリティ対策は待ったなしの状況だ。

「防御」だけでは不十分、攻撃を前提とした対策にも目を

セキュリティ対策と言うとまず頭に浮かぶのは、いかに「守るか」だろう。インターネットとの出入り口をファイアウォールで守り、普段業務に利用する端末にはアンチウイルス製品を導入し、ウイルスやマルウェアの感染から防ぐ、といった「定石」ならばすでに講じており、それで十分と思われるかもしれない。

しかし、グローバルなセキュリティ対策の指針である米国国立標準研究所（NIST）の「サイバーセキュリティフレームワーク」では、防御を含む 5 つの機能を求めている。社内に存在する資産・リソースと、そこに含まれる脆弱性を整理・把握する「特定」、前述の「防御」、セキュリティインシデントを早期に把握する「検知」、発生したサイバー攻撃に対処する「対応」、そしてシステムを元通りの状態にして事業を継続させる「復旧」だ。

サイバー攻撃の手口が知られれば知られるほど、それを「いかに防ぐか」という部分に目が行きがちだ。確かに、脆弱性管理やさまざまな防御策を通してサイバー攻撃が起こる可能性を極力下げていく努力は必要だが、攻撃と防御はいたちごっこの関係にあり、どれだけ対策を講じてもサイバー攻撃者はそれをかいくぐる手法を取ってくる。技術ではなく、だまされやすいという人間の性質につけこむフィッシング詐欺のような手口も多々用いられている。

こう考えると、被害を 100%未然に防ぐことは非現実的だ。NIST のサイバーセキュリティフレームワークに示されているとおり、攻撃はあり得ることを前提に、検知や対応、復旧といった部分にもバランス良く力を注ぐことが重要だ。

たとえば検知に関しては、近年、EDR と呼ばれる製品が注目を集めている。PC をモニタリングして異常な兆候があれば深く調査したり、場合によっては被害を受けた端末をネットワークから切り離し、影響範囲の拡大を抑えることができる。また対応についても、CSIRT と呼ばれる組織を整備して事故発生時のマニュアルを整え、仮にランサムウェアなどに感染してもバックアップから復旧して、影響を最小限にとどめる体制を整備する企業が増えている。

だが、やるべきことはそれだけで終わらない。原因をきちんと追跡してシステムを復旧させ、再発防止策を講じることが重要だ。原因を取り違えたまま対策を打っても、見当違いでただ投資を無駄にしただけ、となりかねない。何が原因となってどのように侵害されたかを正確に把握することで、本質的な対策が取れるはずだ。

それでなくても取引先や顧客に影響が及んでいる場合には、「何が起きたか」を明らかにして適切な対応を示す姿勢が必要だろう。もはやこうした対処は企業にとって社会的責任の一つと言えるだけでなく、個人情報保護法の改正によって、個人情報などが流出した場合には一定の期間内に本人への通知と個人情報委員会への報告が求められている。

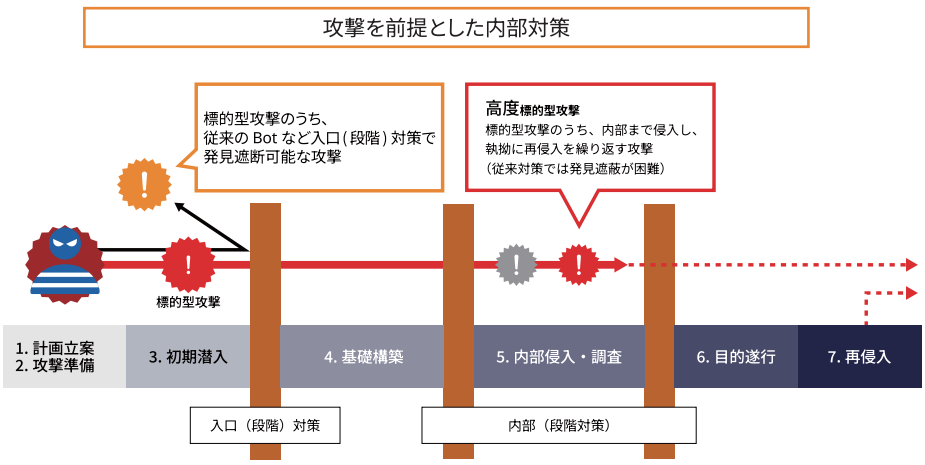
サイバー攻撃の調査に不可欠でありながら、管理に課題のある「ログ」

だが、いざ「そのとき」が来て調査を進めようにも、できないケースが目立つ。専門家に相談し、調査を行おうにも、システムで何が起きたかを記録する「ログ」が保存されておらず、調査に必要な証拠やデータが記録されていないケースが多いからだ。

たとえば、従業員が普段の業務で何をしたかは「日報」を見ればわかるだろう。何月何日、誰とコンタクトを取ってどんな打ち合わせを行い、成果物は何かといった事柄を記録し、保存しておくことで、後からどんな取引が行われたかを把握できる。ここに出勤記録などを付き合わせれば、正確に労働時間を把握した上で、行動の裏付けを取ることができる。

IT システムにおいて同じような役割を果たすのが「ログ」「イベントログ」と呼ばれるデータだ。PC やファイルサーバ、あるいはネットワーク機器などで、いつ、どのような挙動が行われたかを記録するもので、システムの安定稼働のためにもっぱら役立てられてきた。

実はこのログは、不正アクセスやサイバー攻撃の調査にも非常に有用だ。いつ、どの機器でどんな操作が行われたかが記録されているのだから、それをたどれば攻撃のプロセスが見えて



くる。何がきっかけとなったのか、どのようなデータが被害に遭い、どこまで被害が及んだのかといった事柄も把握できるし、一番証明が難しい「被害は確認されなかった」ということも、ログが残っており、重要なデータへのアクセスがないことがわかればある程度の確度を持って断言できる。社外からの攻撃はもちろん、攻撃者が誰かのアカウントを乗っ取って不正な操作を行った場合でも、振る舞いを分析することで判断できる。

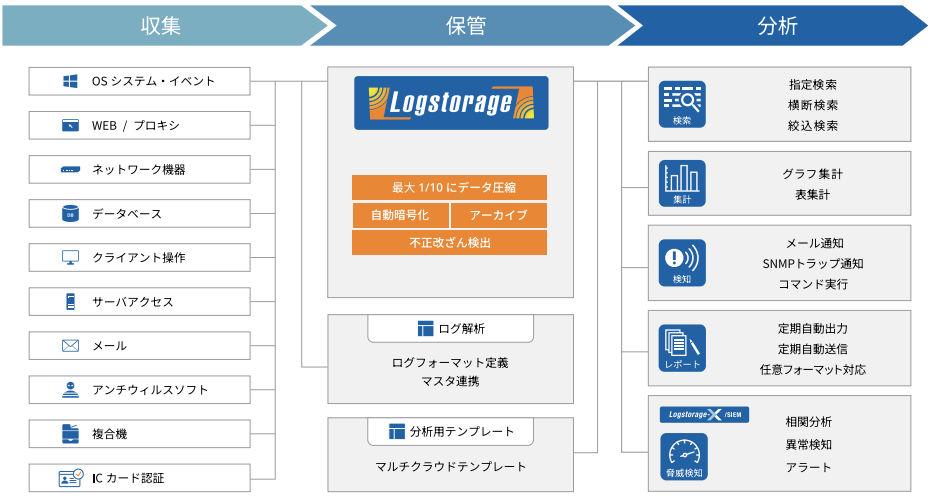
にもかかわらず、この「ログ」が残っていないケースが多い。一つは、サイバー攻撃者が証拠隠滅のために消してしまうケースだ。だが、情報システム部がそもそも収集を諦めてしまっているケースが少なくない。一度保存に取り組んでみても、質と量、二つの側面で負荷が高いためあきらめてしまう場合があるのだ。

まずは「質」、つまり種類が多様なことだ。ログと一口に言っても、PC が出力するものもあればサーバが出力するものなど、多様な種類がある。その上にフォーマットも多様だ。時刻一つ取っても、年月日を「-」でつなぐもの、「/」でつなぐものもあれば、年を先に記述するもの、月を先に記述するもの、年を 4 桁で記述するものと 2 桁で処理するもの…とまちまちで、それらを同一のフォーマットにそろえ、わかりやすく並べるだけで一苦労となる。下手にいじって、時系列が逆転したまま調査しては因果関係の分析もあったものではなく、ノウハウを持ったエンジニアがいなければなかなか難しい。

そして、ログというものは地味だが確実に増え続ける。システムの規模に比例して日々増大する、大量のログデータをどう保存するかも悩みの種となっている。そもそもログ管理というものは、営業支援や業務アプリケーションのように、日々の業務に直接関与するものではなく、システム障害や不正アクセスのような不測の事態が起こったときに、原因を把握するための黒子的な存在だ。それだけに、なかなか投資にも理解が得られにくく、高価なストレージを用意するのは難しい状況だ。

ログにまつわる問題を解決する「Logstorage」

こうした問題を解決するソリューションが、インフォサイエンスの「Logstorage」だ。ログの管理・分析にまつわる質と量、両面の問題を解決する。



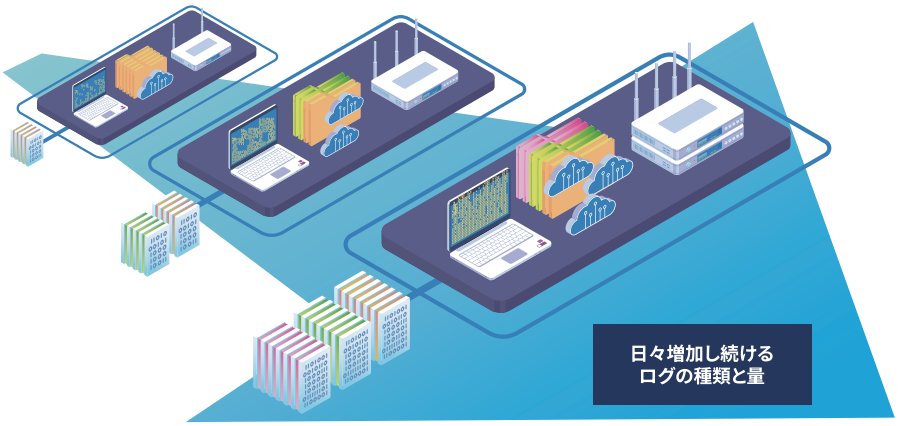
Logstorage システム概要

クラウドサービス	ファイアウォール	クライアントログ	データベース監査
AWS Azure Google Cloud Platform Microsoft 365 Google Workspace box Cybereason	Palo Alto Networks NGFW	DEFESA Logger MylogStar	PISO SSDB 監査
PC資産管理		**特権管理**	**Webフィルタリング**
CWAT LANSCOPE MaLion SKYSEA Client View 秘文		SecureCube Access Check iDoperation	i-FILTER

Logstorage 連携製品

まず質の面では、400 種類以上のソフトウェアやネットワーク機器に対応し、さまざまな種類のログを取り込めることが特徴だ。日報の例で言うならば、従業員それぞれ、異なるフォーマットで日報を書いても文脈を読み取って、部署や企業全体で横断的に「いつ、誰がどんなことを行ったか」を整理し、ぱっと見ればわかる形で可視化できる。

そして量の面では、ログのデータを圧縮し、効率よく保管できる。生のログデータを保存する場合に比べ、最大 5 ～ 10 分の 1 に圧縮することで、保存先のストレージ容量も削減できる。また、攻撃者が証拠隠滅や改ざんを図ろうとしてもそれを防ぎ、安全にログデータを保管しておく仕組みも備えている。



法規制の強化もあり、もしサイバー攻撃を受けてしまった時には速やかな調査と報告が求められる。何より利用者や取引先といったステークホルダーが気にするのは、「どんな被害が発生し、自分たちは影響を受けるのかどうか」だろう。ではそうしたニーズに応え、被害範囲を特定できる検索機能を備えており、迅速な報告に活用できる。

普段の仕事の中で、日報の書き方や整理・分析の仕方一つで業務改善につながる。同じように、PC やさまざまなシステムが吐き出すログも、うまく生かせばセキュリティ強化や事故対応を助けることができる。それも無償で生成される「宝の山」だ。

繰り返しになるがサイバー攻撃は高度化しており、なかなか防ぎきることは難しい。ログをきちんと管理し、保存し、必要に応じて迅速に分析できる体制を唱えておくことは、これまでのセキュリティ対策を補い、より強固にする最後の砦となる。

問い合わせ先

インフォサイエンス株式会社
プロダクト事業部
〒108-0023 東京都港区芝浦 2-4-1
インフォサイエンスビル
TEL: 03-5427-3503
URL: https://logstorage.com/
E-Mail: info@logstorage.com