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！

脅威はもう防げない時代に ログ活用を通してサイバーレジリエンスの実現へ

インシデント発生後は純利益が平均 21% 減少。後を絶たないサイバー被害

JCIC は、日本国内で情報流出等が発生すると「株価は平均 10%~15% 下落」し、インシデント発生後は「純利益が平均 21% 減少」という調査結果を出している（出典：サイバーリスクの数値化モデル ）

サイバー攻撃を受けると莫大な損害を被るため、セキュリティ対策を実施する企業は年々増加している。それにも関わらず、サイバー攻撃の被害件数は減っていない。

近年では、ファイルやシステムを暗号化して利用不可能な状態にした上で、もとに戻すことと引き換えに身代金を要求する「ランサムウェア」が国内外で多発している。他にも、サプライチェーンの弱点悪用、標的型攻撃による機密情報の窃盗、ゼロデイ攻撃などサイバー攻撃による被害が後を絶たない。

テレワークや AI の普及により攻撃が激化。脅威を防ぎきることは困難に

なぜ、サイバー被害は多発しているのだろうか。その理由として「環境の変化」と「犯罪のビジネス化」が挙げられる。環境の変化でいうと、コロナ渦をきっかけにテレワークやオンライン会議を導入する企業が増加した。さらにクラウド化や AI の普及により、デジタル環境は大きく変化した。

それらに関連した脆弱性や設定不備、認証情報の不備を突かれてランサムウェアに感染した事例が多い。実に感染経路の約 80% がクラウド化やテレワークに関連したものだ。

また、犯罪のビジネス化も進んでおり、攻撃の敷居は年々低下している。例えば、サイバー攻撃を行うためのツールをまとめたパッケージサービス「CaaS」を用いることで、技術力の低い攻撃者でも高度なランサムウェア攻撃や DDoS 攻撃が可能になっている。さらに、不正アクセスするための手段を提供する「イニシャルアクセスブローカー」と呼ばれる存在も多数確認されている。

これらの理由から、サイバー攻撃はより複雑に、より激しくなっている。一方でセキュリティ人材は不足しており、多くの企業にとってサイバー脅威を事前に防ぎきることは困難だと言っても差し支えないだろう。

「防ぎきれない脅威」の対策が求められる中、サイバーレジリエンスが投資対象へ

このように、多くの企業が防ぎきれないサイバー脅威にさらされている中で注目を浴びているのがサイバーレジリエンスだ。

サイバーレジリエンスとは、サイバー脅威に直面することを前提に、どのような状況であっても事業を継続できるようにするための概念のことだ。これには「危機の予測」と「危機に直面したときの耐久、適応、回復できる力」というニュアンスが含まれている。

従来のセキュリティ対策では、一度被害を受けるとシステムの復旧に時間を要する。普及までの時間が長いほど、経済的な損失は増大し、顧客の信頼を失う可能性も高まる。一方でサイバーレジリエンスを実現できた場合、そのダメージを最小限に抑えられる。

実際に、世界最大手規模の IT 企業である IBM では「経済的損失の軽減」「顧客の信頼獲得」「競争上の優位性の向上」の観点から、サイバーレジリエンスの重要性を説いている。また「サイバーセキュリティ経営ガイドライン」では、サイバーレジリエンスは投資すべき重要な位置づけであることを明示化している。

変化が激しい現代では「脅威に直面する」ことを前提とし、その対策としてサイバーレジリエンス実現への投資がますます活発になっていくだろう。

参考情報
https://www.ibm.com/jp-ja/topics/cyber-resilience

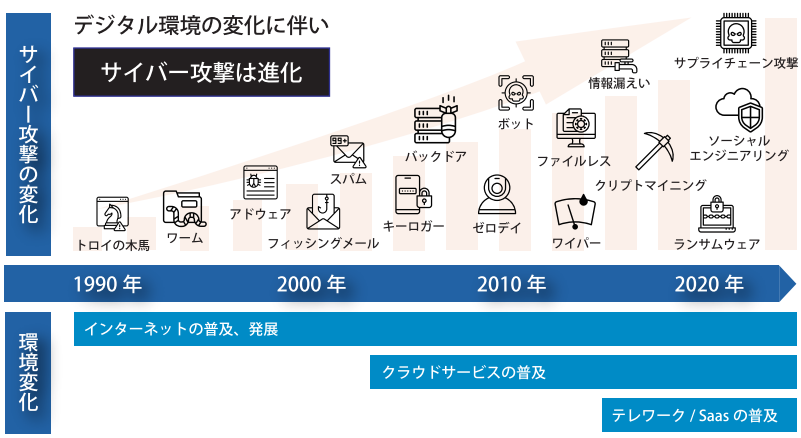
サイバーレジリエンスの実現を支えるログ活用

ここからはサイバーレジリエンスを実現するためのログ活用について見ていこう。先ほど、サイバーレジリエンスには「予測」「耐久」「適応」「回復」のニュアンスが含まれることを説明したが、ログ活用は「予測」と「耐久」の側面で重要視されている。

「予測」の面で言えば、脅威にさらされやすい NW 機器や認証系のログを優先的に定期観測することで、セキュリティポリシーを強化できる。例えば、テレワーク環境下における外部アクセスの IP 傾向を分析することで、普段確認されない IP アドレスがわかるため優先的に調査を行える。

「耐久」の面で言えば、ログ活用を通じた早期発見や被害の正確な把握により、被害の最小化に寄与する。例えば、公開された脆弱性情報を元に過去のログを確認し、侵害の有無を確認するという運用が注目されている。世界的に多く観測された Log4Shell の侵害確認もこれにあたる。

サイバー攻撃とデジタル環境の変遷



課題の多いログ活用

ログ活用は「予測」と「耐久」の面で寄与するが、実は多くの課題がある。よくある課題として、サイバー攻撃者が証拠隠滅のためにログを消してしまうケースが挙げられる。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。

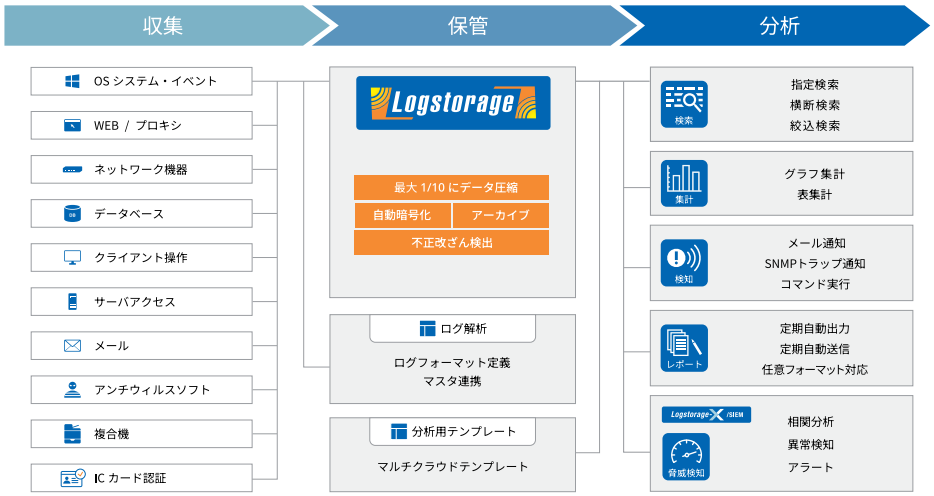
時刻一つ取っても、年月日を - でつなぐもの、/ でつなぐものもあれば、年を先に記述するもの、月を先に記述するもの、年を 4 桁で記述するものと 2 桁で処理するもの……とまちまちで、それらを同一のフォーマットにそろえ、わかりやすく並べるだけで一苦労となる。下手にいじって、時系列が逆転したまま調査しては因果関係の分析もあったものではなく、ノウハウを持ったエンジニアがいなければなかなか難しい。

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。

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。



Logstorage システム概要

クラウドサービス
AWS
Azure
Google Cloud Platform
Microsoft 365
Google Workspace
box
Cybereason

ファイアウォール
Palo Alto Networks NGFW

PC資産管理
CWAT
LANSCOPE
MaLion
SKYSEA Client View
秘文

クライアントログ
DEFESA Logger
MylogStar

特権管理
SecureCube Access Check
iDoperation

データベース監査
PISO
SSDB 監査

Webフィルタリング
i-FILTER

Logstorage 連携製品

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。

サイバーレジリエンスの実現を支える要素として「ログ活用」

予測
脅威にさらされやすいNW機器や認証系を優先的に定期的に観察
↓
ポリシーなどへフィードバックし、脅威への備え
平常状態を理解することで、脅威の早期発見に繋げる

脅威
攻撃を想定、脅威を調査。ルールやレポートを通して異常を検知
↓
早期発見、被害を正確に把握することで
被害の最小化に寄与

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