[2022 年最新版]

サイバー攻撃監視

はカンタンに自動化できないのか？

専門知識不要、コスト不要の 徹底自動化ガイド

AMIYA

目次

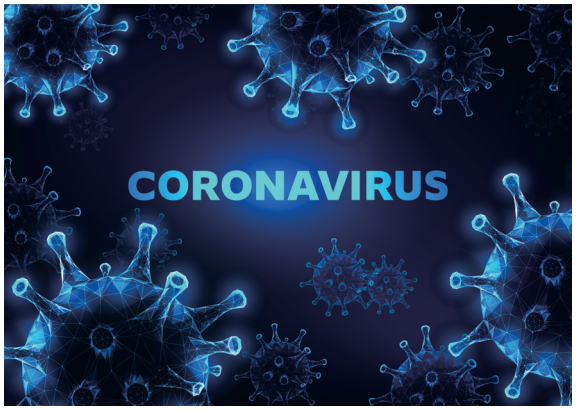
- はじめに ―― P3
- 1. 標的型攻撃のおさらい ―― P4
- 2. 実は、既存のログで対処できる？？ ―― P6
- 3. ガイドラインは既に出されている ―― P7
- 4. SIEM でログの集約と分析を解決せよ ―― P8
- 5. ALog の SIEM 実績は既に 100 社超え ―― P9
- 6. サイバー攻撃自動検知パック ―― P10
- おわりに ―― P14

本ホワイトペーパーの対象となる方

セキュリティやネットワーク部門の管理者、情報セキュリティ責任者など、セキュリティログに関連する担当の方

本書は、エンタープライズ規模に対してログ管理手法を定義、導入、維持する実用的なガイドラインです

はじめに



新型コロナウィルスの蔓延により、世界中の企業が**突然かつ強制的に**テレワークの導入を迫られることとなりました。そのためネットワーク環境や情報セキュリティリスクについて十分に吟味する猶予もなく、急かされるように導入を進めた企業も多くありました。
脆弱な体制を突いた**サイバー攻撃事件**が一気に増え、Apple や Amazon に扮する日常的ななりすましメールのほかにも、給付金や雇用調整助成金の案内を偽るこの時勢特有のメールが多数報告され、2020 年 3 月の件数は 2 月と比べ、6.7 倍にも急増しました。

それらはいわゆる**標的型攻撃**ですが、やっかいなのは「間違ってメールを開封してしまっても不思議ではないくらい精巧」であり、更に感染しても**「侵入に気づけない」**ことです。

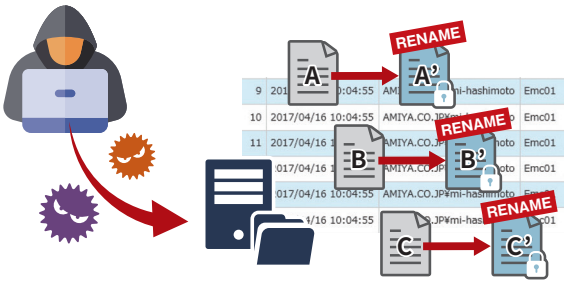
そして、その侵入が皆さんの**想像をはるかに超える量で実際に起きてしまっている**ことです。

1. 標的型攻撃のおさらい

標的型攻撃とは**「明確な目的をもとに、特定のターゲットを狙ったサイバー攻撃」**をいいます。標的型メールや Web サイトなどを踏み台に、対象が利用する PC に感染して侵入し、組織の機密情報を詐取します。

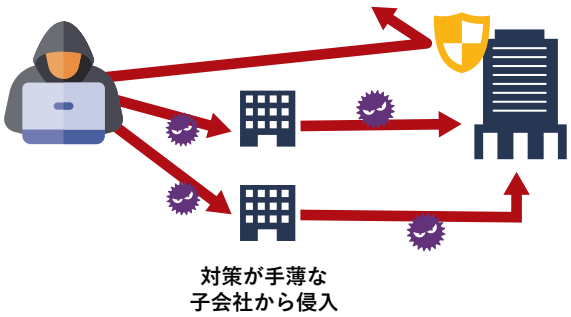
またそのデバイスから別の PC やネットワークに攻撃を仕掛けるなど**潜伏的、拡散連鎖的である**のが特徴で、**被害が PC 単体に留まらない**ため深刻になりやすい傾向があります。

攻撃パターン



主に「金銭要求目的」である場合、ランサムウェアに感染させます。ランサムウェアは使用しているコンピュータを強制的にロックし、格納されているファイルを暗号化、元の状態に戻すことと引き換えに、身代金を要求します。バックアップなどの情報セキュリティ対策が充分に行われている大企業よりも、中小企業がターゲットになりやすいとされています。

最近は**「スパイ行為（情報の搾取）」**の目的で「国防や自動車開発、コロナのワクチン開発などがターゲットになっています。大企業のセキュリティは中小企業に比べ、コストをかけて対策を講じているため、攻撃者は直接大企業を狙わずに、中小企業の取引先や海外の子会社などに侵入、踏み台にしてから本体の大企業を攻撃します。
この手法を一般的にサプライチェーン攻撃と呼びます。



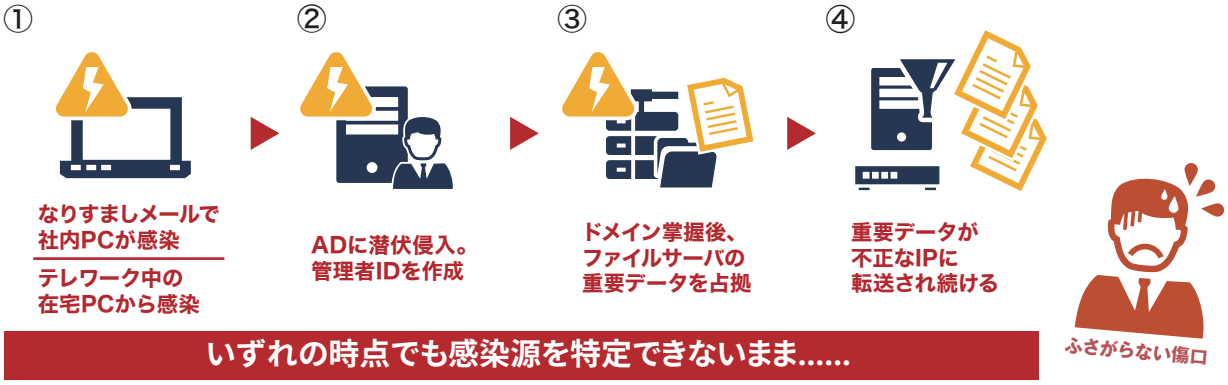
攻撃の手順

しかし、これらの脅威に**ほとんどの企業が気づけていない**のが実情です。
下記は、「機密情報が永続的に社外に転送されていた」という**実例**です。

ターゲットは名の知れた大手企業。本社はセキュリティ対策が万全であったため、攻撃者はまず、セキュリティ管理が脆弱と思われる海外の子会社や、派遣員の PC を狙います。それを踏み台に本社の AD サーバに侵入、管理者権限を奪取し、ファイルサーバ内の重要データを、継続的に抜き取っていました。

攻撃の実例

① 侵入	メールや Web 閲覧により、ターゲットをマルウェアに感染
② 初期活動	最初に侵入した端末を踏み台に、さらに権限の高い端末への侵入
③ 機密情報の奪取&送信	攻撃が検知されないよう、長い時間をかけて少しずつ情報を奪取し、外部へ送信
④ 痕跡の消去	検知されることを防ぐため、ログの書き換え、消去を行う



国家ぐるみのサイバー攻撃は減る見込みなし

侵入されながら気付けない大半の日本企業

ネットワークの弱点をふさいでも効果なし

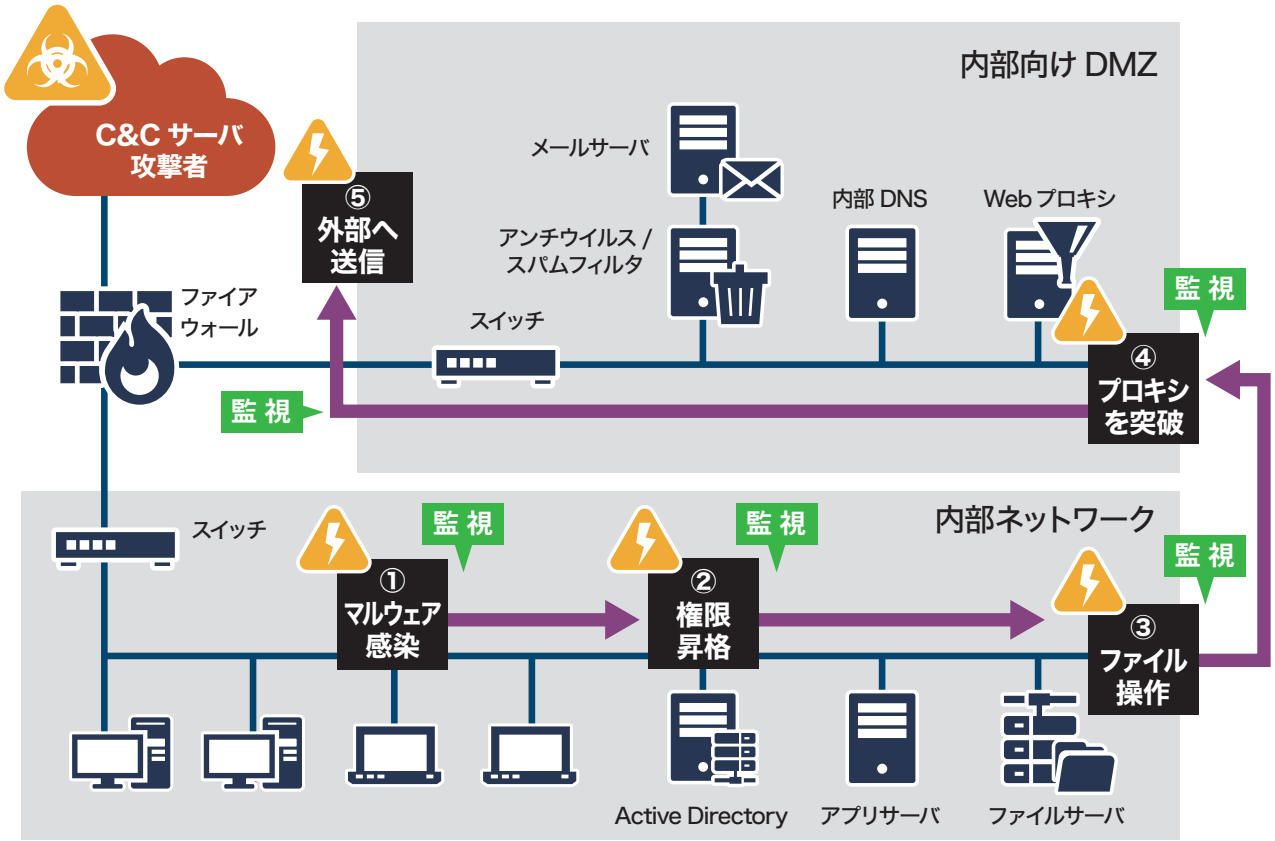
2. 実は、既存のログで対処できる？？

従来までの「FW や UTM などの入口対策」では全く対応できない状態にあります。**「疑わしくないメールを開封しただけ」**ですんなり侵入・攻撃されてしまうため、入口対策の増強は、既に無駄なセキュリティ投資になりつつあります。

今の最善のセキュリティは、「突破されることを前提とした対策」です。

侵入後の「スピーディな察知」「範囲 / 侵入経路の特定」に重きを置き、**大きな投資を行わず、既存のログだけで対処する**のです。

下記は一般的な攻撃パターンを図解したものですが、①～⑤それぞれの機器から出されるログデータを見るだけで、迅速に脅威を検知できます。

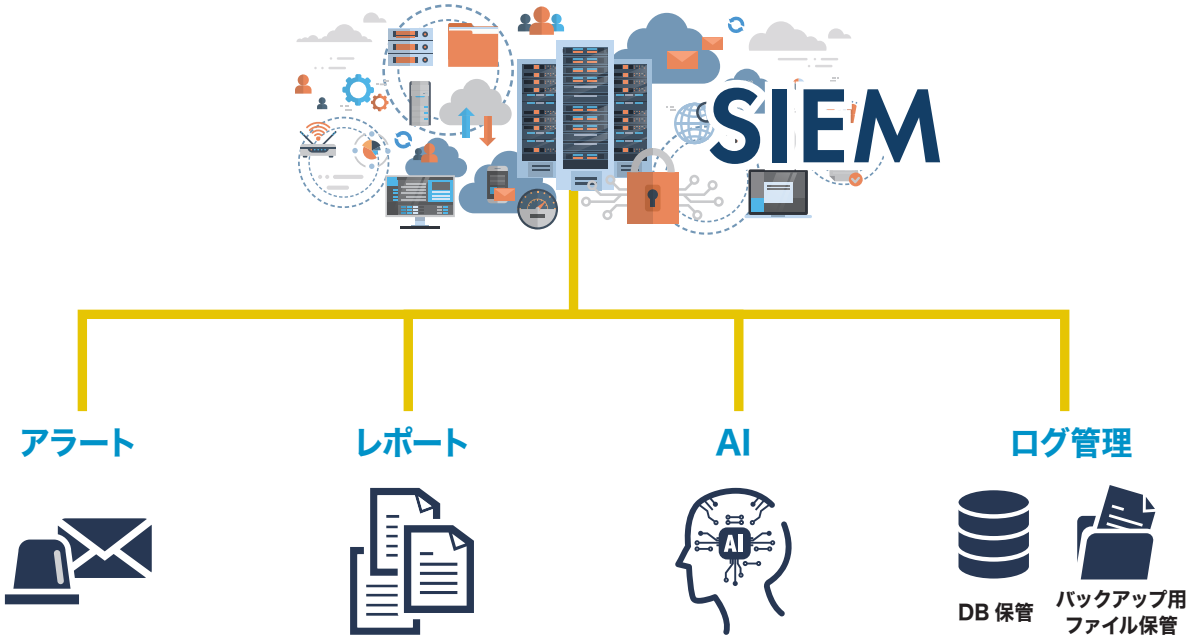


3. ガイドラインは既に出されている

前述したような典型的な攻撃の対策方法については、IPA ※や JPCERT※など国内のセキュリティインシデントに詳しい機関が既に対策方法を公表しています。
例えば、攻撃者が 侵入後に真っ先に向かうのは、ユーザー ID を取得する意図での AD サーバです。AD サーバにログインをひたすらチャレンジし、突破すればドメインの管理権限を掌握し、あとは好き放題です。ガイドラインには、大量のログイン失敗は侵入の最も典型的なサインであると指摘しています。

※ IPA：独立行政法人 情報処理推進機構
※ JPCERT：Japan Computer Emergency Response Team

4. SIEM でログの集約と分析を解決せよ



脅威を事前検知するためには、ひとつのログ（例えば PC ログ）を監視するだけでは不十分です。サーバやネットワークなど多角的にあらゆるシステムのログを集約 / 分析することで初めて有意義な対策になります。

しかし、一つの操作が何十行にもなる複雑難解なログのすべてを人の目で判断するには大変な労力を伴います。重要なのはいかに手間をかけずに、効果的な運用をするか。
つまり**「ログ監視の自動化」**です。

実現のためには、SIEM（Security Information and Event Management）と呼ばれる、**「データを統合管理・長期保管し、データ分析する」**ための統合ログ管理ツールが必要です。

SIEM があれば 、ログの自動集約、検知アラート、レポート、検索、分析が可能になります。

5. ALog の SIEM 実績は既に 100 社超え

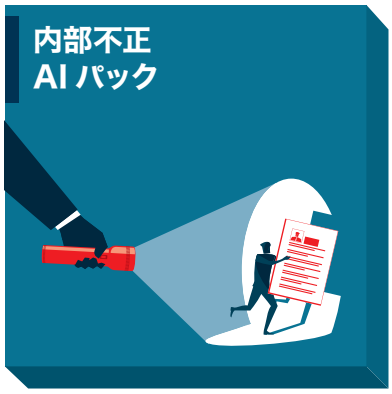
海外製の SIEM は、相当のコストがかかるだけでなく、構築 / 運用に専門的なノウハウも必要になります。実装には専門の サービサーに運用を委託せざるを得ないため、長期運用に多額のコストが伴います。

そんな折、国産製品でサーバログで知名度の高い ALog が、既に SIEM 化していた？！ ということで、次章では **SIEM になっていた「ALog」**を、より具体的にご紹介します。

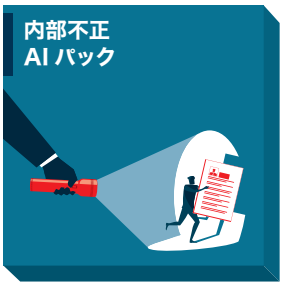
6. サイバー攻撃自動検知パック

「実際に標的型攻撃を受けていることが分かる仕組みはありますか？」「実際に漏えいが起きた時にどこから / どういう範囲かの特定はできますか？」「あらかじめ不審な挙動を検知する仕組みはありますか？」

そのようなお客様の声から、ALog は SIEM 化しました。既に**サイバー攻撃自動検知パック**という各種ガイドラインに則した形でのソリューションパッケージを提供開始しています。



1 適用したいパックを選ぶ



2 インポートする

インポートファイルは 1 つだけ

3 機器名を登録したら完了

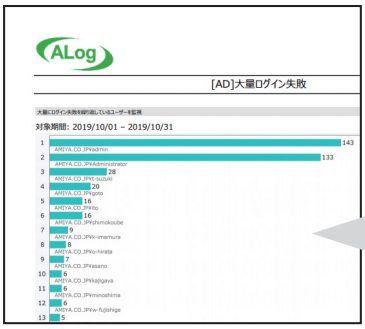
設定はこれで終了です。
あとは AI とアラートが自動検知

設定例

イベント ID「4625」（ログインの失敗）を
“同じユーザーが 30 回以上行ったら” レポートの作成+報告を自動化。

出力例

30 回を超えたユーザーを迅速に察知
自動作成したレポート（報告書）を添えて管理者へアラート通知



**回数の異常だけでなく、v8 から
“普段と違う異常” も検知可能に**

おわりに

システムには標的型攻撃の傷跡が残る

▼

まずは記録。
記録を取ることは最短、最善、必然

バラバラ管理は最大のタイムロス、人力ロス

▼

影響範囲を最小化するため、
「集約＆統一化」+「素早く検知する仕組み」が必須

記録されたデータは溜めることで武器化する

▼

不正や攻撃の温床は、
AI で自動検知できる

サーバアクセスログ

ALog ConVerter®

ALog ConVerter は、重要データへのアクセス記録をエージェントレスで取得する製品です。重要データが格納されるサーバ側からログを取得することにより、ストレスのない効率的なログ管理を実現します。

統合ログ

ALog EVA

ALog EVA は、ALog シリーズの守備範囲を飛躍的に拡張します。
高度な専門技術を要求する従来の統合ログ製品から一線を画した手軽さと柔軟さを備えた新しい統合データマネジメントツールです。

詳しい製品のご紹介、評価版のご依頼は以下にお問い合わせください。

お問い合わせ先

株式会社網屋
データセキュリティ事業部
TEL：03-6822-9996　E-mail bv-sales@amiya.co.jp

詳しい製品概要資料はこちら ＞

開発元

AMIYA 株式会社 網屋

〒103-0007 東京都中央区日本橋浜町3-3-2 トルナーレ日本橋浜町 11F
TEL: 03-6822-9999 FAX: 03-6822-9998
https://www.amiya.co.jp/

販売元

ALog ConVerterは株式会社網屋の登録商標です。
記載された製品の仕様・機能等は改良のため予告なく変更される場合があります。
このパンフレットの内容の一部またはすべての複写・転用・転載等を株式会社網屋に無断で行った場合、著作権の侵害になります。