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！

「ゼロトラスト」でも求められる「ログの有効活用」とは？

近年、クラウドサービスの普及、ワークプレイスの自由化が加速するにつれ、IT 環境が大きく変化しています。これに伴い、セキュリティを取り巻く状況は一変し、従来の境界防御モデルでは対応が難しい様々なセキュリティの課題が明らかになりました。そこで注目され始めたのが、「ゼロトラスト」です。「信頼せず、常に確認する」という言葉で表されるように、ゼロトラストは認証・認可とイコールに捉えられがちですが、ゼロトラストは本来、複数の要素から構成される継続的なセキュリティ戦略を指し、認証・認可はあくまで一つの要素にすぎません。ゼロトラストなシステムを実現する上で重要な要件は「必要最低限の認可をユーザーに与えること」「全ての通信を可視化すること」「全てのログを残すこと」となります。本稿では、ゼロトラスト実現におけるログの重要性とその有効活用についてご説明します。

境界防御モデルの限界

環境の大きな変化に伴い、従来の境界防御モデルでは解決できない様々なセキュリティ課題が明らかになりました。以下に示した課題は多くのリスクをはらんでおり、境界防御モデルの運用が限界を迎えていると言っても過言ではありません。

境界防御範囲拡大に伴う防衛対象の増加

ワークプレイスが自由化し、従業員の自宅など管理されていないネットワークや端末からの通信が増加したことにより、攻撃しやすいポイントが増え、セキュリティに対するリスクとコストも比例して増加しています。

内部犯による不正行為

内部ネットワークは信頼できると油断しているため、組織内部に悪意を持った人間がいた場合、容易に不正行為を許してしまい、さらにその犯行を検知しづらい状況となっています。

脅威の横展開に対する耐性の抵さ

一度、攻撃者に内部に侵入されてしまうと、横展開が容易であるため、複数台の端末やサーバーが乗っ取られ、除去が困難になってしまいます。

ゼロトラストとは

ゼロトラストは、「内部ネットワークは信頼できる」「外部ネットワークは信頼できない」という考え方の境界防御モデルと異なり、ユーザーのアクセスが信頼できるか検証することに着目しています。2020年8月にNIST（米国標準技術研究所）よりSP800-207「Zero Trust Architecture」が公開されており、ゼロトラストにおけるデファクトスタンダードとも言えるこのドキュメントでは以下のように定義されています。

> 情報システムやサービスにおいて、名リクエストを正確かつ最小の権限となるようにアクセス判断する際の不確実性を最小化するために設計された概念とアイデアの集合体

従って、ゼロトラストとは暗黙の信頼を最小化するために、認証や通信の正当性にフォーカスを当てた戦略的なセキュリティフレームワークであると言えます。

ログの有効活用の重要性

昨今のセキュリティ情勢では未知の脆弱性を突く高度サイバー攻撃の増加により、攻撃者の侵入を避けることはできない状況になっています。そのため、被害範囲の特定や脅威の早期検出の必要性が増大し、最近のセキュリティトレンドとしてログの有効活用が注目されることとなりました。具体的には、図1　に示すように、以下のようなログの有効活用が求められるケースが増加しています。

フォレンジック

フォレンジックとは、セキュリティ上の問題が発生した際に、証拠保全、被害範囲の特定や原因調査を行うことです。セキュリティインシデント発生の際には、速やかなフォレンジックが必要になります。速やかなフォレンジックを実現するには、ログの有効活用は必須であり、複数種のログを横断し、集計、分析できる必要があります。また、ログそのものの信ぴょう性も求められるため、ログを保全することができるログ管理システムが必要になります。

脅威兆候の検知

未知の脆弱性など通常のセキュリティ製品で検出できない脅威が増加しているため、おのずとログを利用した脅威兆候の検知のニーズが増しています。従ってログやそれらをサマリにしたレポートをトリガーとして脅威兆候を検知し、調査やインシデント対応者に通知を行うことができる必要があります。

セキュリティポリシーへのフィードバック

セキュリティにおいて継続的な評価を行い、ポリシーを最適化することは非常に重要な事項です。ポリシーを最適化するためのインプット情報は多数あり、ログもその情報源の一つです。ログは実際にシステムを利用したという記録であるため、ユーザーの実情に沿ったポリシーを作成する上で、重要な存在となります。例えば、ログを基に特権を持ったユーザーのログイン情報を時間別に集計・レポート化します。これを精査することで、夜間にログインが発生しないという事実があらかじめ明確になっていれば、「夜間に特権ユーザーのログインが発生した」場合にアラートをあげるというポリシーを環境に反映することが可能となります。

ゼロトラストでより重要となったログの有効活用

では、ゼロトラストにおけるログの有効活用の重要性はどうでしょうか。
ログの有効活用の重要性はゼロトラストにおいても同様であり、先に挙げたSP800-207でも言及されています。例えば、図2（裏面参照）に示すようにゼロトラストを実現する論理モデルの項目では、認証・認可を支えるアクセスの信頼に必要な情報のコンポーネントのうち、4つがログと密接に関係します。

アクティビティログ

トラフィックログや各リソースの動作ログを集約し、認証・認可を実現する体制に対してフィードバックする機能が必要になります。

イベント分析／ふるまい分析

いわゆるSIEMについて言及しています。ログやセキュリティに関連する事項を集約し、分析を行うことで、脅威を検出します。

脅威インテリジェンス

脅威インテリジェンスとは、攻撃者の攻撃パターンを

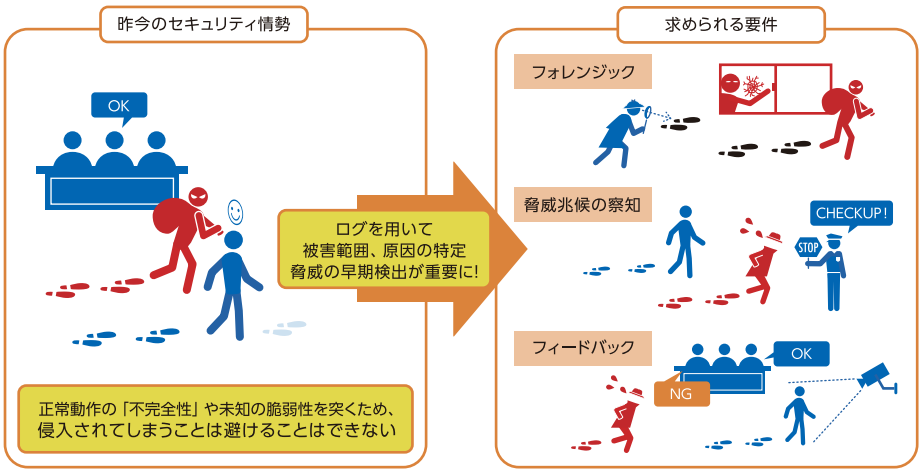

図1　ログ有効活用の重要性

理解するために収集、分析されたデータのことです。ゼロトラストでは脅威インテリジェンスを収集、活用し、脅威インテリジェンスとログを照合することで脅威の検知に役立つ仕組みを提供する必要があります。また、インシデント発生時のログ自体を経験的な脅威インテリジェンスとして扱うこともできます。

規格、規則への準拠

ゼロトラストでは、コンプライアンスや業界ごとのセキュリティ基準を考慮して実現する必要があると言及しており、各セキュリティガイドラインでは、ログの有効活用の重要性について多く言及されています。

以上のようにSP800-207でもログの有効活用について記載されていることから、ゼロトラストにおいても、ログの有効活用は今まで以上に重要になったことがわかります。
これには、大きく2つの理由があります。
1つ目は、ゼロトラストにおいて、守るべき各リソースはクラウドなどに散在し、それらにアクセスするユーザーも場所に依存しないことに起因しています。誰がどこにどのようにアクセスしたかを把握することが今まで以上に難しくなり、ログを統合、管理し、横断して有効活用することで、全体の状態を理解する必要性が以前より高くなったためです。
2つ目は、ゼロトラストでは、認証・認可は重要であり、今まで以上にその正当性や厳密性を担保しなければならないことに起因します。これによりログが持つ情報にさらに大きな価値が生まれ、このログを有効活用することで、実態に即したポリシーを適用することができ、ログを有効活用することの価値が相対的に向上したためです。

統合ログ管理システムLogstorage

ゼロトラストは、企業のデジタルインフラと重要な資産を守るための戦略です。
単一のセキュリティ製品を導入するだけで実現できるものではなく、お客様の環境に応じて複数の製品やサービス、ソリューションを組み合わせる必要があります。そのため、ゼロトラストで求められるログの有効活用の実現には、様々な製品・サービスのログを収集できることが重要となります。
Logstorageは、様々なログ出力方式に対応したモジュールやレシーバ、図3にあるような主要なクラウドサービスをはじめ様々な製品に対応した連携パックが提供されているため、多種多様なログを収集することができる統合ログ管理製品です。
Logstorageの特徴として、図4に示すように、ログデータの改竄検知や圧縮、暗号化をはじめ、フォレンジックに必要なログ保全機能の他、ログの集計、レポート機能といった分析に役立つ機能を有しており、ログから実態の傾向を理解することも可能です。
そのため、運用改善、外部脅威の検知や内部脅威対策、PCIDSSや各種ガイドラインへの対応といった目的で導入されているユーザーも多く、Logstorageを導入いただくことで目的を達成できたという声を多くいただいております。
また、純国産のソフトウェアであり、官公庁や地方公共団体、金融業、製造業など、様々な業種・業態の多くのユーザーに支持され、5,100社以上(2024年2月時点）の導入実績もあり、統合ログ管理製品の分野で17年連続シェアNo.1（出典:デロイトトーマツミック経済研究所株式会社「内部脅威対策ソリューション市場の現状と将来展望2023年度版（統合ログ管理ツール部門）」https://mic-r.co.jp/mr/03010/）を誇るソフトウェアとして高く評価されております。
ゼロトラスト実現にもお役に立てる統合ログ製品ですので、是非ご活用ください。

図3 様々な製品に対応する連携パック

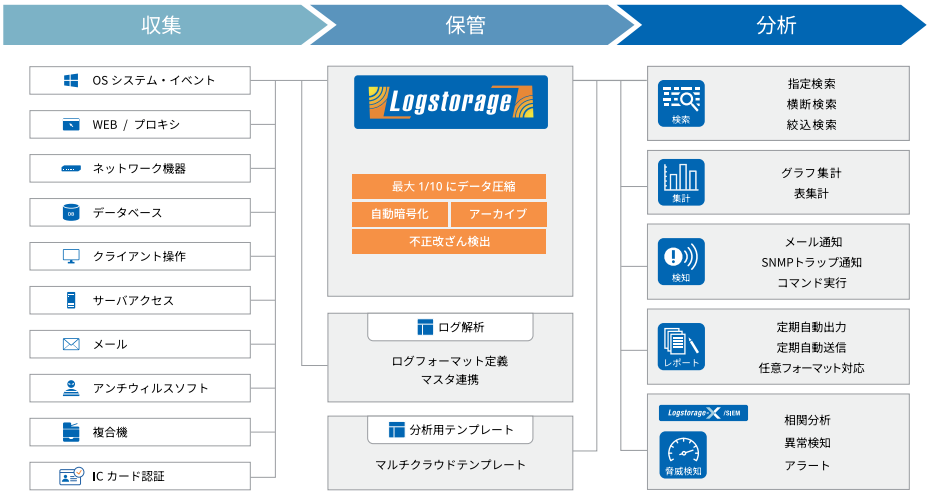

図4 Logstorage システム概要

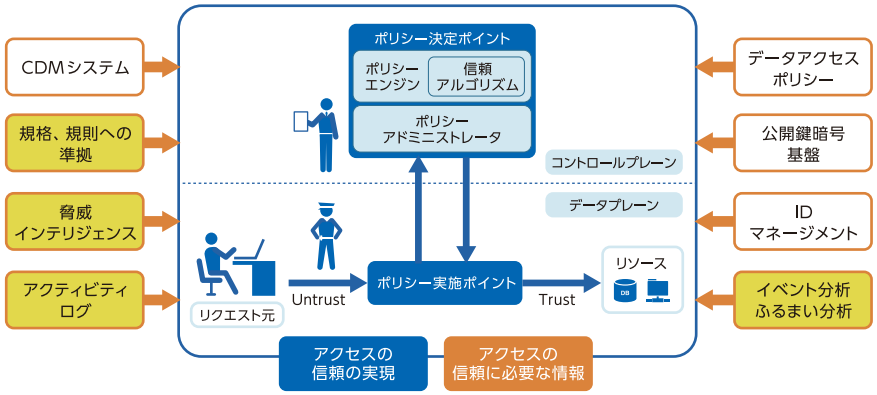

図2 ゼロトラストの論理モデル

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