■ 解 説

「クラウド時代のゼロトラスト・セキュリティ」の重要な考え方とセキュリティ手段

統合ログ管理

ハイブリッドクラウド環境で重要な統合ログ管理とログの長期保管

サイバー攻撃を受けた後の対策や監督官庁、メディアへの報告を行うためには、ログの分析が必要となる。しかし、ハイブリッドクラウド環境では各クラウドサービス、オンプレミス設備のログのフォーマットが異なり、可読性が低い。そこで有効なのが、統合ログ管理による横断分析だ。

（取材・構成：渡辺 元・本誌編集長）

安達賢一郎
インフォサイエンス株式会社
プロダクト事業部 ジェネラルマネージャー 兼 コンサルティング統括マネジャー

堀江 翼
インフォサイエンス株式会社
プロダクト事業部
セールス統括マネジャー

攻撃を受けた後の対策が必要

コロナ禍によるテレワーク、ハイブリッドワークが浸透しつつある中で、業務のクラウドサービス移行が進み、オンプレとクラウドを組み合わせたシステムであるハイブリッドクラウドの利用拡大も加速している。オンプレとクラウドにそれぞれデータが混在する環境下では、過去の「境界型防御」（社内外のネットワークを分離し、境界で防御するモデル）が通用しなくなりつつあり、社内外のネットワークを通過する個別の通信に着目したゼロトラスト・セキュリティが注目を浴びている。

ハイブリッドクラウド環境では構成が複雑化しており、セキュリティソフトの設定に漏れがあったり、対応しきれない新たな攻撃を受けたりする可能性がある。アンチウイルスソフトをはじめとするエンドポイントセキュリティ、次世代ファイアウォールをはじめとするネットワークセキュリティがそれぞれ国内では予防策として普及しているが、どちらも攻撃に対する予防策であり、攻撃を受けた後の対策が必要となる。

また、標的型攻撃は実際の攻撃の発生から数カ月程度経過してから発覚することがある。万が一このような攻撃を受けた場合に、「自社のシステムに何が起きたのかがわからない」「どこまでの範囲に攻撃を受け、調査する必要があるのかわからない」「監督官庁やメディアへの報告が適切に行えるのか」といった課題が生じるのである。

クラウド・PC・ネットのログを統合管理

これらの課題に対して有効なのが、オンプレかクラウドかを問わずあらゆるPC、サーバ、端末、機器、サービスから出力される「ログ」（システムのアクティビティを示す記録データ）を統合管理することである。

まず、クラウドのログを管理することが必要である。海外の事例だが、実際にAWS環境の利用企業でWAFの設定ミスによる情報漏洩が発生してしまった。その企業はきちっとログを取っていたためAWA側の設定で脆弱なポイントがあるということはわかったが、ログを取っていなければどこから侵入されたか把握することはできなかった。クラウドの脆弱なポイントを特定するためにはログ管理が非常に重要である。

インシデントが発生した場合、クラウドに接続するPC側のログによる通信経路の把握も必要になる。クラウド、端末、接続したすべてのネットワークを含めた統合ログ管理を行わなければ、どの経路でどのようなインシデントが起こったかを包括的に調査することはできない。ケーブルテレビ事業者や放送局は、リモートプロダクションやテレワーク、リモートワークなどでクラウド、インターネット、VPNを使う。部門も制作、報道、顧客管理などに分かれている。そのため統合ログ管理ソリ

ューションなどでクラウド側のログだけでなく包括的にログを取っておく必要がある。

多様なログを共通フォーマットに変換

統合ログ管理では、各システムから多種多様な形式で出力されるログを、複数の方式で収集し集約、圧縮し、長期的なログの保管を実現することが重要である。これにより多岐にわたるフォーマットで記録されるハイブリッドクラウドのログを一貫性のある観点で分析することができる。

ログは出力するシステムによってフォーマットが全然異なる。AWS や Azure など複数のパブリッククラウドサービス間でも、それぞれのサービスでログのフォーマットが別個に設定されている。各システムのログをそれぞれに分析する必要があるが、例えば当社が提供している統合ログ管理システム「Logstorage」が提供するマルチクラウドテンプレートを利用することで、異なるフォーマットのログを共通フォーマットに変換して可視化し、一元的かつ横串でのログ分析が可能となる。運用の観点でも、クラウド、端末、ネットワークなどでシステム担当者が分かれている場合、部署をまたいで調査するためには、各システムのログを同じフォーマットで統一的な UI で見ることができるメリットは大きい。

統合ログ管理を行うためには、進化を続けるパブリッククラウドのログを収集する方式を考慮する必要がある。AWS や Azure などパブリッククラウドはサービスが頻繁にバージョンアップやリニューアルされ、新しいサービスもどんどん増えていく。ログの収集方式も早いものでは 1～2 年程度で変更され、利用企業はそれにどう対応するかが重要な課題になっている。AWS を利用している技術者のブログなどからログ収集の方法を把握することもできるが、一般の情シス担当者がそれをフォローし続けるのは大変である。統合ログ管理システムには、進化し続けるパブリッククラウドに追随してログを収集して、圧縮して長期的に保管し、効率的に可視化する機能を提供しているものがある。

ログの長期的で調査コストを削減

統合ログ管理では、ログを長期的に保管し、過去の事例・インシデントに対する調査を行うことができるようにすることが重要である。特に標的型攻撃は発生後数カ月経過してから発覚するケースが多い。攻撃の発生ポイントからの影響度調査をログ中心に行うことで、影響範囲や調査対象を絞り込むことができるが、数カ月前の攻撃が発生した時点のログが残っていないと、システムへの侵害が発生、または疑われた場合に、どこまで調査を広げる必要があるのかが特定できなくなる。

具体的な事例では、2021 年 12 月ごろに特定のログを出力する OSS（オープンソースソフトウェア）のライブラリである Apache Log4j に脆弱性があることが明らかとなり、NHK のニュースでも報道されるくらい話題になり、当社にも顧客企業からクラウドで使っていた Apache Log4j に関して相談があった。この企業では Apache Log4j のバージョンアップを行っていなかったため、半年前以降に侵入された可能性があったが、当時のクラウドや周辺のサーバなどのログを保管していなかったためインシデント調査の範囲を限定できず、広範囲を調査しなければならなくなり、時間とコストがかかってしまった。

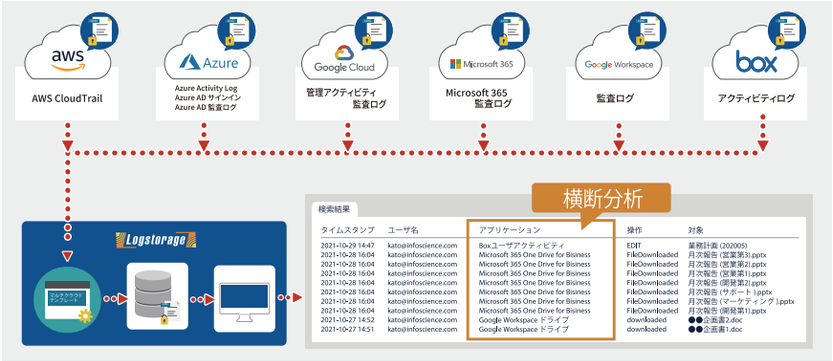
パブリッククラウドサービスのログは保存期間が数十日程度に設定されているケースがある。いざインシデント調査で振り返ろうとしても、攻撃発生時期のログがすでに保存されていないこともあるため、統合ログ管理システムなどで利用企業側でも適切にログを別途保管しておくことが重要となる。ログを保管していない場合はセキュリティ調査会社に調査を外部委託しなければならないが、調査するシステムの台数に従って金額が上がっていく。ある有名なセキュリティ調査会社の場合、PC 1 台当たり約 100 万円の費用がかかる。このリスクも踏まえてログ管理を行わなければならない。

改正個人情報保護法への対応

ログを長期的に保管することは、数カ月前の標的型攻撃のなどのインシデント調査だけでなく、必要に応じて監督官庁に報告する際にも役立つ。2022 年に改正個人情報保護

法が施行されたため、監督官庁の個人情報保護委員会への報告が必要となるインシデントが増えた。個人情報が侵害された場合、1週間以内になるべく早く一度報告し、その後確定報告もしなければならない。そのための調査には、長期的に保管したログが必要となる。インシデント対応だけでなく、監督官庁への報告などコンプライアンス対応も含めて長期的にログ管理をしておかなければならない。

【図1】 統合ログ管理で各クラウドサービスのログを横断分析
（インフォサイエンスの統合ログ管理システム「Logstorage」の例）



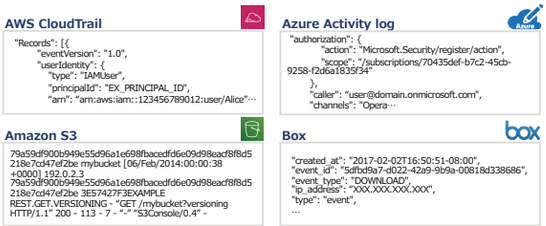
ただ、ハイブリッドクラウドなど使用しているシステムが大きくなるほど保管するログが増え、大量のストレージを使ってしまう。この課題に対しては、ログを圧縮して保管・活用できる統合ログ管理システムを利用することで解決できる。

サプライチェーン攻撃対策にも有効

近年、統合ログ管理システムを利用する企業が増えている。例として、当社が提供している統合ログ管理システム「Logstorage」の場合、国内の大小の民放など放送事業者をはじめとして、中央官庁、地方自治体、金融・生保、製造業、インフラなど、業種・業界・規模を問わずさまざまな企業・組織で導入されている。主に上記のような「インシデントに備えてのログの長期保管・調査」でのニーズをはじめとして、重要インフラなど各種業界のガイドライン、コンプライアンスへの対応といった目的で利用されている。

独立行政法人情報処理推進機構（IPA）が発表した「情報セキュリティ10大脅威 2022」で、「テレワーク等のニューノーマルな働き方を狙った攻撃」は前年の3位から4位になった。一方、前年の4位から3位に置き換わったのが「サプライチェーンの弱点を悪用した攻撃」である。セキュリティが手薄な関連企業や取引先企業を経由して大手企業に侵入するサプライチェーン攻撃の動きが活発になっているため、今後もサプライチェーン間のデータ連携に使われているクラウドのセキュリティに対するニーズは、高まることが想定される。放送業界でもコンテンツ制作などの関連企業や取引先企業を経由したサプライチェーン攻撃に対する、クラウドのセキュリティ対策が必要となっている。

【図2】 クラウドサービスごとに異なるログのフォーマット



【図3】 各クラウドサービスのログ保管期間は短い

製品	ログ保管期間（※）
AWS	90日
Azure	90日
GCP	30日
Microsoft 365	90日
Google Workspace	180日

※ ログが保管される期間はログの種類により異なる。

統合ログ管理はエンドポイントセキュリティやネットワークセキュリティのような防御ではないが、クラウドのセキュリティ対策として絶対に行う必要がある。現在の日本企業が取り組んでいるセキュリティ対策において、統合ログ管理は海外企業に比べて十分とは言えない。だが、放送業界を含めて統合ログ管理への認知度は上がってきている。最近、インフラ整備がしっかりしている首都圏の大企業よりも、地方の中小企業がターゲットとして狙われ始めているため、統合ログ管理の重要性をさらに全国で広く認知いただけるよう、働きかけていきたいと考えている。（談）