可視化と分離で築くゼロトラスト構想

ランサムウェア攻撃に挑むSBIの防衛線「マイクロセグメンテーション」

金融業界や重要インフラを狙うサイバー攻撃が激化する中、SBIホールディングスはグループ全体のセキュリティ強化に向けてレジリエンスの強化とゼロトラストの実現にまい進している。何が実現のカギになったのか、同社の取り組みに迫った。

潜伏型攻撃への早期検知

マイクロセグメンテーションによる防水隔壁の実現

ゼロトラスト戦略の中核構築

近年、社会の基盤を支える組織を狙ったサイバー攻撃が後を絶たない。港湾システムや医療機関をはじめ、重要社会インフラが被害を受けた事例も記憶に新しく、直近ではDDoS攻撃による航空会社のフライトの欠航や銀行のサービス停止など被害は広範囲に及んでいる。特に深刻なのは企業の存続を強く脅かすランサムウェア攻撃の激化だ。この種の攻撃では、2024年に発生した大手出版グループの事例が示すように、子会社への侵入がグループ全体に拡大し、情報流出やサービスの長期停止を招くなど、大規模な被害が生じている。さらに直近では、飲料メーカーの出荷停止や、法人向け通販、物流業での配送停止が多方面のサプライチェーンに影響を与えるなど、被害は一企業の事業継続性の問題にとどまらず、実体経済にも広がりを見せている。

こうした脅威に対して組織はどうすれば対抗できるのか。SBIホールディングスの取り組みから、その答えを探る。

サイバー脅威への強烈な危機感から導き出された3つの教訓とは？

SBIグループは銀行、証券、保険を中核とする国内有数の総合金融グループだ。SBIホールディングスを持ち株会社として、グループ全体で600を超える連結子会社、約1万8千人の従業員を擁しており、特にオンライン金融サービスに強みがある。同社のセキュリティ戦略を統括するのがIT統括部長の浦輝征氏だ。浦氏はグループ全体の

SBI GROUP

位置

日本
https://www.sbigroup.co.jp/

業種

Financial Services

ソリューション

- Akamai Guardicore Segmentation
- Akamai Hunt

Akamai

CSIRTを指揮するとともに、総務省ではサイバーセキュリティ統括官の下で、同省のサイバーセキュリティ政策の企画・立案への助言や、国内外における最新のサイバーセキュリティ脅威動向の分析にも携わっている。

「従来、金融機関としてサイバーセキュリティはトッププライオリティでした。しかし、もはや従来の延長線では通用しない局面に入っています。社会の基盤を支えるミッションクリティカルなサービスを提供する企業が次々と攻撃を受ける中、私たちは対策のギアを一段上げています」と浦氏は危機感を募らせる。

特に深刻な脅威として浮上したのが、「Living off the Land」（LotL：環境寄生型）攻撃だ。正規のシステムツールやプロセスを悪用して不正な活動を隠蔽（いんぺい）する攻撃手法であり、従来の手法では発見が困難だ。2025年に入ってからは官公庁や金融業種でも広く使われていた国内大手ISPが提供する法人向けのメールサービスがこの攻撃を受けて、長期間潜伏していた侵害の存在に気付かなかったという事案が発生した。

浦氏は「AIの発展によって多様な手口を組み合わせた攻撃がますます巧妙化しています。だからこそわれわれは、“事を起こさせない”ための予防と、“起きてしまった事象を素早く検知して封じ込める”対処の両軸を同時に強化する必要があると感じています。具体的にはゼロトラストを前提に、環境全体の可視化やプロセス制御、脅威ハンティングを組み合わせ、予防と検知・封じ込めを両軸で回しています」と強調する。

危機感の背景には規制当局からの要請もある。金融庁は近年、金融機関に「サプライチェーン全体のセキュリティ確保」と「オペレーショナルレジリエンス」の2つを強く促している。オペレーショナルレジリエンスとは、未然防止を尽くしてもなお発生するインシデントに対して、迅速にサービスや業務を回復させる能力を指す。

浦氏はこうした規制や要請に先だって、これまで明らかになった大規模なインシデント事例を詳細に分析し、そこから3つの重要な教訓を導き出した。

第1の教訓は「防水隔壁」だ。1つの組織への侵害がグループ全体への拡大につながってはならない。ある事例では、子会社への攻撃が親会社の基幹システムに波及してグループ全体のサービス停止に至った。こうした被害の拡大を防ぐには、ネットワークや権限、データの境界を明確に分離する「防水隔壁」の設計が不可欠だ。

第2の教訓は「卵は一つのかごに盛るな」だ。ある事例では、顧客データや経理機能といった基幹系システムと子会社のシステムがデータセンター内で隣接しており、この近接性が被害の拡大を招いたとされている。つまりミッションクリティカルなシステムと通常のシステムを適切に分離する必要がある。

第3の教訓は「たる理論」だ。複数の板で構成されたたるに水を注いだとき、水は最も低い板の高さまでしかたまらない。この比喩が示すように、グループ全体のセキュリティ強度は最も脆弱（ぜいじゃく）な構成要素の水準に引き下げられてしまう。全体のセキュリティレベルを上げるには、最も弱い組織の底上げが必要だ。

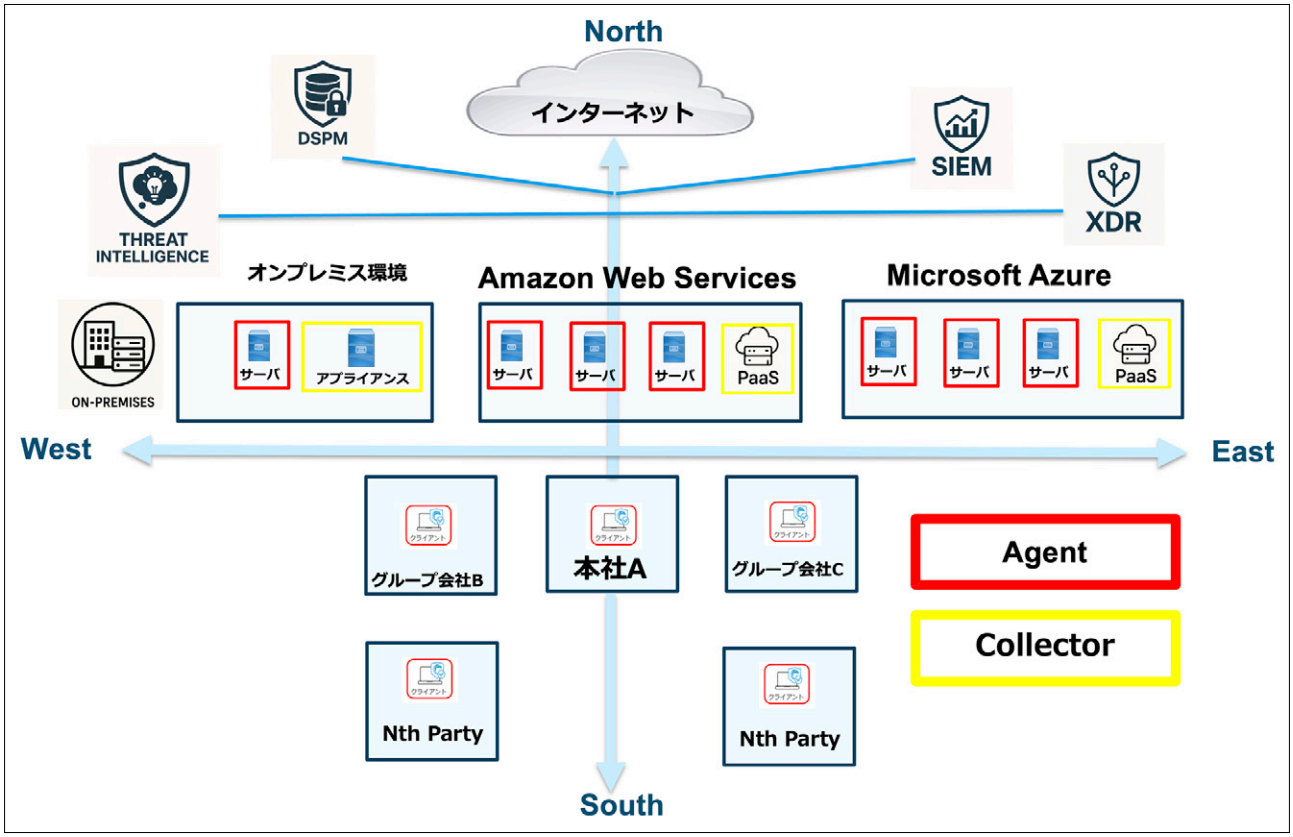
SBIグループはこの教訓を踏まえて、新たなソリューションの導入の検討を開始した。注力したのはグループ全体の「防水隔壁」を実現して、攻撃の横展開を防ぐマイクロセグメンテーション製品の採用だ。

金融業界の厳しい要件を満たすマイクロセグメンテーション製品とは？

SBIグループのIT環境は多様だ。「Amazon Web Services」（AWS）や「Microsoft Azure」（Azure）といったパブリッククラウドやオンプレミスのデータセンター、レガシーシステムなど多様なプラットフォームが混在しており、グループ全体で数千台の端末と数百台のサーバが稼働している。

「グループ内には金融サービス事業を展開する企業もあれば、資産運用、ベンチャーキャピタル、暗号資産、バイオ・ヘルスケア、メディア事業など複数の事業ドメインにまたがる企業群が存在します。これら全体を一貫したセキュリティポリシーで保護する必要がありました」

こうした多様な環境を前提に、同グループが選定するマイクロセグメンテーション製品の要件を3つ設定した。第一に、マルチクラウド、マルチOS環境で統一して利用できることだ。AWSやAzure、オンプレミスのどこでも同一のセキュリティポリシーを適用できなければならない。



第二に、データガバナンスの観点から国内リージョンに対応していることだ。金融業界では、自社が管理するデータのリージョンを明確に把握し、機密性が高い情報について厳格なガバナンスを維持することが求められる。海外のデータセンターではこの要件を満たすのが困難になる。

第三に、運用の効率性だ。そもそも組織に属する高度なセキュリティ人材には限りがある。複雑な運用を要するシステムではグループ全体への展開は持続可能なセキュリティ対策にはならない。そのため、限られた人的リソースで、グループ全体を一元管理できる効率的な運用が必須条件となった。

こうした要件を基に、浦氏は複数のベンダーの製品を比較検討した。最終候補として残った2社の製品で決定的な差となったのが、国内リージョン対応だ。競合製品はSaaS版が海外サーバでの運用だったため、要件を満たせなかった。

その結果、選定されたのが「Akamai Guardicore Segmentation」だ。同製品はネットワークをマイクロレベルでセグメント化して、グループ内、組織内でやり取りされている通信を可視化・制御でき、攻撃の横展開を防ぐゼロトラストセキュリティソリューションだ。

PoCで見えた課題と可能性　Akamai Guardicore Segmentationの実力

導入に当たっての懸念点はエージェント型製品特有の既存システムへの影響だ。Akamai Guardicore Segmentationは保護対象のサーバやクライアントにエージェントソフトウェアをインストールする必要がある。だが、金融機関ではわずかな処理遅延も業務に深刻な影響を及ぼしかねない。

浦氏は「処理が重くなったり、既存システムに過度な負荷が発生したりしないか、さらにパフォーマンスの劣化がないか入念に確認するプロセスを設けました」と振り返る。約4カ月、クライアント40台とサーバ5台で検証した結果、懸念していたパフォーマンスへの悪影響は確認されなかった。同時に、既存のセキュリティ製品との機能競合やプロキシ経由での接続など、技術的な課題を一つずつクリアしていった。

PoCの過程で予期せぬ発見もあった。Akamai Guardicore Segmentationのネットワーク可視化機能により、これまで把握していなかった通信の実態が明らかになったのだ。「意図してなかった通信経路が確認できました。今まで見えなかった課題を把握できたのは大きな収穫です」

同製品のネットワーク可視化機能は、IT環境内のアクティビティーを詳細に把握できる。アプリケーションの依存関係をユーザーレベルとプロセスレベルでマッピングして、ITインフラ全体を動的なマップとして表示する。ネットワークレベルだけでなくサーバ内のプロセスも特定できるため、問題のある通信を素早く発見して実際のトラフィックを見ながらポリシーを設定できる。

続いて、詳細に可視化された情報に基づいて、ホスト単位の細かい制御を実現する。IPアドレスをベースにするのではなく役割や環境、アプリケーションを示すラベルベースでポリシーを管理できるため、管理対象の実態が分かりやすく、管理対象の物理的な場所に依存せず、IPアドレスが動的に変化するクラウド環境でも一貫したセキュリティポリシーを維持できる。

もう一つ注目すべきなのは、脅威ハンティング機能だ。AIと機械学習を使ってネットワーク内の正常な状態を学習した後、通常とは異なる通信パターンを自動的に検知して、LotL攻撃のような潜伏型の脅威が発する活動の兆候を早期に発見する。

脅威ハンティング機能の役割は単なる脆弱性検知だけではない。ネットワーク内でのスキャン行為などの偵察活動の検知や、最初に緩めに設定したセグメンテーションルールをより厳密に制御するためのアドバイスの提供など、運用品質の向上にも寄与する。ユーザー自身がセルフで診断できる製品の機能に加えて、Akamaiのマネージド型脅威ハンティングサービスによって専門アナリストが実行する高度な脅威分析も利用できる。

Akamaiは世界中で膨大なユーザー数を抱えており、そこから得られる脅威インテリジェンスをAkamai Guardicore Segmentationでリアルタイムに利用して脅威を発見できるだけでなく、ネットワーク内に攻撃者をおびき寄せるハニーポット（わな）を動的に配置する機能も備えている。

PoCでは運用面での効率性も確認できた。数千台を超える端末と数百台のサーバの個別管理は通常であれば膨大なワークロードになる。しかしAkamai Guardicore Segmentationのラベルベース管理機能に加えて、ランサムウェア対策などの一般的なユースケース用の事前構築済みテンプレートを使うことで、最小限のリソースで効率的な運用が可能だと実証された。

「グループ全体のセキュリティのレベルを引き上げながら担当者の運用負荷を重くしないという、一見矛盾する要求をAkamai Guardicore Segmentationで実現できました」と浦氏は評価する。

浦 輝征 氏
SBIホールディングス株式会社 IT統括部長

ゼロトラストセキュリティ構築に“必要不可欠なパーツ”

10年以上前からAkamaiのDDoS対策サービスを利用してきたSBIホールディングスは、Akamaiのサポート体制を高く評価している。

「PoCから設計フェーズまで、直面した技術課題に、質の高いサポートを提供していただきました。サイバーセキュリティの世界においては、海外で発生した脅威がその後日本に波及する傾向があります。Akamaiはグローバル企業として、この最新の脅威情報やトレンドをいち早く提供してくれるため当社のセキュリティ戦略のアップデートに非常に役立っています」

浦氏はこのソリューションがグループ全体のゼロトラストアーキテクチャ構築において重要な役割を担うと位置付けた。

「『何も信頼しない』というゼロトラストの考え方と、Akamai Guardicore Segmentationの可視化・検証機能は非常に相性が良いアプローチと言えます。このソリューションは当グループのゼロトラストセキュリティ戦略の重要なパーツになると考えています」

さらに、セキュリティ人材の不足という業界共通の課題の解消にも大きな期待を寄せている。

「セキュリティ人材の不足を解決するには、AIによる自動化や効率化、そしてセキュリティ部門以外のリテラシーに依存しないシンプルな仕組みが必要です。Akamai Guardicore Segmentationのようなサービスには、直感的かつビジュアルに現状を把握し、ポリシーを設定できる高い操作性が不可欠です。その運用の容易性こそが限られたセキュリティ人材やIT人材をより戦略的な業務に集中させることを可能にし、われわれの持続可能なセキュリティ対策の要件となります。だからこそAkamaiには引き続き、グループ全体の防御力向上に向けた支援を期待しています」

SBIグループの事例は「防水隔壁」「卵は一つのかごに盛るな」「たる理論」といった教訓を具現化し、セキュリティ向上と運用効率化を両立させる一つの解を示した。Akamai Guardicore Segmentationは、次世代のセキュリティアーキテクチャの中核を担うソリューションと言えるだろう。

SBIグループは、日本におけるインターネット金融サービスのパイオニアとして1999年に設立され、証券・銀行・保険を中心に金融商品や関連するサービスの提供等を行う「金融サービス事業」、ベンチャーキャピタルをはじめとする各種ファンドの運営等を行う「PE投資事業」、資産運用に関連するサービス提供等を行う「資産運用事業」、国内の暗号資産取引所の運営やマーケットメイカー事業等を行う「暗号資産事業」、バイオ・ヘルスケア＆メディカルインフォマティクス事業やWeb 3に関連する事業等を行う「次世代事業」を中心に事業を展開しています。

Akamai はオンラインビジネスの力となり、守るサイバーセキュリティおよびクラウドコンピューティング企業です。市場をリードするセキュリティソリューション、優れた脅威インテリジェンス、世界中の運用チームが、あらゆる場所で企業のデータとアプリケーションを多層防御により保護します。Akamai のフルスタック・クラウド・コンピューティング・ソリューションは、世界で最も分散化されたプラットフォームで優れたコストパフォーマンスを実現しています。安心してビジネスを展開できる業界トップクラスの信頼性、スケール、専門知識の提供により、Akamai は、グローバル企業の信頼を獲得しています。詳細については、akamai.com および akamai.com/blog をご覧いただくか、X や LinkedIn で Akamai Technologies をフォローしてください。

※この冊子は、2025年11月に掲載されたアイティメディア編集局制作コンテンツを再構成したものです。
https://techtarget.itmedia.co.jp/tt/news/2511/07/news01.html