CUSTOMER STORY

セキュリティ対策にFireEyeのソリューションを利用する大手証券取引所

概要

業界

金融

ソリューション

- FireEyeネットワーク・セキュリティ
- FireEyeエンドポイント・セキュリティ
- FireEye Central Management
- Mandiant Managed Defense
- FireEyeネットワーク・フォレンジック・プラットフォーム
- FireEye調査解析システム
- FireEye脅威解析プラットフォーム
- FireEye Platinum Priority Plus サポート

利点

- 世界中の多様なインフラにわたって、複数経路をシームレスに保護
- 直感的かつ一元的に環境全体を監視、管理
- リアルタイムで脅威を検知し、迅速に調査、復旧

企業紹介
世界的な大手証券取引所

知名度の高いこの証券取引所は、サイバー犯罪者の格好の標的となっています。組織の主任セキュリティ・スペシャリストは次のようにコメントしています。「私たちは世界の金融エコシステムの中心にいます。巨額の資金を扱っているだけでなく、何らかの障害が起きれば世界的に大きな影響が生じ、広い範囲で不安定な状態に陥る可能性があります。2010年に、組織の内部システムに対して、統合された脅威管理対策を強化する必要があるとの結論に達しました。従来のセキュリティ・ソリューションでは、拡大を続ける脅威の一歩先を行くには、十分な体制が得られないと判断したのです」

世界的に有名な組織には、世界レベルのセキュリティが必要

この証券取引所が擁する大規模なインフラには、さまざまなハードウェア・コンポーネント、オペレーティング・システム、アプリケーションが含まれています。「利用可能なオプションとしては、少なくとも、Windows、UNIX、Linux、Mac OSをベースとする各種プラットフォームといった、組織の多様な環境に完全に対応したものでなければなりません」と、セキュリティ・スペシャリストは語ります。

この証券取引所では、IT環境に対する総合的なアプローチをとっています。プロジェクト・チームが協力体制をとり、セキュリティ防御の定義も含め、幅広い要件をリストアップしました。セキュリティ・スペシャリストはこう回想します。「私たちは、組織の環境を総合的に保護するために必要なものについて戦略を立てました。業界でFireEyeのソリューションの評判が高いことを耳にしており、その真偽を確認したいと思いました。

「5年以上にわたって提携してきましたが、FireEyeのソリューションは今なお、革新性と敏捷性で群を抜いています」

— **主任セキュリティ・スペシャリスト**、世界有数の大手証券取引所

FireEyeのプラットフォームを選んで組み合わせ、概念実証を行いました。その性能が実際に期待を上回ることを確認した後で、そのソリューションを本番環境にそのまま移行しました」

現在、この証券取引所では、FireEyeのセキュリティ・ポートフォリオの中から以下のコンポーネントを導入しています。

- FireEye® ネットワーク・セキュリティ・ソリューション：Webベースのサイバー攻撃に対する保護
- FireEye® Eメール・セキュリティ製品：Eメールによる攻撃の阻止
- FireEye® CMシリーズ：FireEyeの防御体制の集中管理
- Mandiant® Managed Defense：マネージド・セキュリティ・サービス
- FireEye® ネットワーク・フォレンジック・プラットフォーム（PXシリーズ）：迅速な特定と解決
- FireEye® 調査解析システム（IAシリーズ）：詳細な調査を促進する機能
- FireEye® 脅威解析プラットフォーム（TAP）：攻撃への対応時間の改善
- FireEye® Platinum Priority Plusサポート：レベル2の上級エンジニアリングのサポートへの優先アクセス

マルチベクター型攻撃には多層的な防御が必要

セキュリティ・スペシャリストはこう語っています。「FireEyeのソリューションは、まさに私たちが望んでいることを実行してくれます。すべてがインラインで機能しており、過検知はほぼゼロです。即座にマルウェアをブロックし、優先順位の高いアラートは2時間以内に解決されます」

FireEye Platinum Priority Plusサポート・プログラムは、ハードウェアもソフトウェアもカバーしており、Eメール、ライブ・チャット、Web、電話といったサポート・チャネルを通じて、1分以内の応答時間を目標としています。「Platinumサポートは、すばらしいの一言に尽きます。週末であっても即座に対応してくれます。Platinumの担当エンジニアは、組織のチームの延長のように機能しています。いつでも相談に乗ってくれて、すばらしいアドバイスを提供してくれます」と、セキュリティ担当者は語ります。

「私は特に、CMシリーズのコンソールが気に入っています。広大で複雑な環境内ですべてを管理するのは悪夢のような状況にもなりかねませんが、このコンソールでは直感的なインターフェイスでエコシステム全体を管理することができるうえ、接続されているすべてのプラットフォームからのアラートを相関分析できます。全体像を、まるで一枚レンズを通して眺めるかのように把握することができるので、当組織のようなグローバル組織にとっては非常にありがたいことです。シフト交代の際に特に効果的だと実証されています。交代したチームが、インフラ全体にわたるすべてのアプライアンスとすべての階層の状況を即座に把握できるからです」

この証券取引所のセキュリティ体制は非常に複雑ですが、1つの主要ベンダーから複数の保護ソリューションを導入したことで、付加的なメリットが生まれました。セキュリティ・スペシャリストはこう説明しています。「多層保護のすばらしさを実感し、周囲にも伝えています。単一の会社から提供される防御層を備えるということは、隙間や取りこぼしがないことを意味することにも確信を持っています。FireEyeの長年のクライアントとして言えることは、FireEyeの統合アプリケーションが、さまざまなドメインと攻撃経路を動き回る脅威への対処において、昔も今も変わらず優れているということです。Eメール、Webサイト、ネットワークのいずれでも、脅威の経路を問わず、見落とされることはないと確信しています」

「FireEyeネットワーク・フォレンジック・プラットフォームと調査解析は、強力な調査機能によって境界の防御を補完してくれます。これにより、攻撃を迅速に調査し、復旧できます」

— **主任セキュリティ・スペシャリスト**、世界有数の大手証券取引所

敏捷性と革新性を併せ持つ

FireEyeのソリューションとサービスのポートフォリオは、グローバルのインフラ全体に、シームレスなマルチベクター防御機能を提供しています。個々の要素が業界屈指の保護を、この証券取引所にもたらしています。

「FireEyeの各コンポーネントに、それぞれのメリットがあります。たとえば、ネットワーク・セキュリティ・シリーズは柔軟な導入オプションがあり、ダイナミックなローカル・ルールの生成が可能です。どちらも私たちにとっては非常に重要な点です。メール・セキュリティ・シリーズも導入時にさまざまなオプションが利用可能で、さらにネットワーク・セキュリティ・プラットフォームと自動的に通信し、常に同期しています」と、スペシャリストは語ります。

「FireEye脅威解析プラットフォームの機能によって、マネージド・サービスに対する全体的なシステム状況を報告することが可能になり、組織の世界的なインフラ全体でセキュリティ関連のアップデート情報を迅速に提供できます。また、あらゆる産業、あらゆる地域に組み込まれた数百万の仮想マシンに接続された、FireEyeのグローバルなインテリジェンス・ネットワークに接続しているため、脅威に関する通知を即座に受け取り、実際のイベントから収集された、復旧に関するインテリジェンスに自動的にアクセスできます」

彼はこう続けます。「Mandiant Managed Defenseは、潜在的な侵害の兆候に対して、脅威の高度な検証と予防的措置を提供してくれます。私たちはFireEyeネットワーク・フォレンジック・プラットフォームと調査解析システムを追加して、強力な調査機能によって境界の防御を補完しました。これにより、攻撃を迅速に調査し、復旧できます」

証券取引所のセキュリティ・スペシャリストは次のように結論付けています。「脅威は高度化し続け、数も増えていきます。また、状況は分刻みで変化しています。100%の安全を求めようとするのは短絡的かもしれませんが、FireEyeのソリューションの機敏性は、組織が業界トップレベルの保護を受けているという安心感を与えてくれます」

FireEyeの詳細については、**www.FireEye.jp**をご覧ください。

ファイア・アイ株式会社
〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 | 03-4577-4401 |
Japan@fireeye.com

FireEyeについて

FireEyeは、インテリジェンス主導型のセキュリティ企業です。お客様は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデントレスポンスといった、組織がサイバー攻撃対策をする上での課題となっていた複雑性や負担を解消します。