Case Study

メディカル・データ・ビジョン株式会社

WE MAKE APPS GO FASTER. SMARTER. SAFER.

標的型攻撃対策のためFireEye NXを導入、SSL処理にBIG-IPを活用することで、暗号化された攻撃も速度低下なく検知可能に

データによる医療改革を目指し、医療ビッグデータ活用に関するビジネスを展開しているメディカル・データ・ビジョン株式会社（以下、MDV）。ここでは標的型攻撃対策として、FireEye NXとBIG-IPを連携させたソリューションが導入されている。SSLの復号と暗号化をBIG-IPで処理することで、SSLで隠蔽された攻撃もパフォーマンスを低下させることなく検知・遮断できるようにしているのだ。これによって社外に対する説明責任が果たしやすくなった。また、これまで築き上げてきた病院との信頼関係にもとづく競争優位を、維持し続けるための基盤としても重要な役割を果たしている。

「最近では標的型攻撃が急増しており、医療データを扱う当社としては先手先手で、今まで以上に強固なセキュリティを構築することにしました。セキュリティ対策は、事業推進の根幹であるので、特に力を入れています」。

メディカル・データ・ビジョン株式会社
さくらDB部門長 シニアマネージャ 渡邉 幸広 氏

背景

医療の質を高める上で、重要な課題の1つとなっている医療データの利活用。医療ビッグデータを分析することで、新たな医薬品の開発や診断･治療支援が可能になると期待されており、その市場規模は2025年に約8,000億円に上ると予測されている。その一方で、病院経営は約7割が赤字だと言われており、経営の効率化も急務だ。2003年4月に厚生労働省が導入した「DPC/PDPS(※1)」によってその必要性はさらに高まっている。従来の「出来高払い」から、病名や診療内容毎の「定額支払い」へと変化したことで、健康保険からの支払い額が頭打ちになったからである。

このような2つの課題を解決するビジネスを展開しているのが、MDVだ。同社はデータにもとづく医療改革の実現を目指し、2003年8月に設立。現在は、病院経営システムを提供し匿名化された診療情報を集積する「データネットワークサービス」と、集めた診療情報を分析して提供する「データ利活用サービス」という、2本柱で事業を展開している。また2016年からは「診療データを患者個人の手元に」というビジョンのもと、患者自身が診療情報の一部を管理･閲覧できるソリューション「CADA-BOX」の提供も開始。データ利活用ビジネスのさらなる急拡大に向け、積極的な取り組みを進めている。

ビジネス上の課題

このような医療データ利活用ビジネスを本格的に展開している企業は、珍しい存在だといえる。同社のデータベースには、2017年11月末時点で2080万人のデータが蓄積されており、その規模も他社の追随を許さない。このような実績は市場からも高く評価されており、2016年11月には東京証券取引所第一部指定となっている。ここで大きな課題として浮上したのが、社内システムのセキュリティ強化だった。

「当社は匿名化されているとはいえ、診療データを扱う企業であるため、当初からデータセキュリティの確保には全社を挙げて取り組んできました」と語るのは、MDVでさくらDB部門長 シニアマネージャを務める渡邉　幸広氏。すでに情報セキュリティマネジメントシステム（ISMS）の認証は取得済みであり、適切なアクセス制御を徹底するためのシングルサインオンなども実現していると説明する。「最近では標的型攻撃が急増しており、医療データを扱う当社としては先手先手で、今まで以上に強固なセキュリティを構築することにしました。セキュリティ対策は、事業推進の根幹であるので、特に力を入れる必要があるのです」。

<脚注>
※1 DPC/PDPS：Diagnosis Procedure Combination / Per-Diem Payment System。急性期病院における入院時医療の包括払い制度。

Overview

業種

エンタープライズ

課題

- 標的型攻撃が急増する中、ビジネスの根幹であるセキュリティ強化が必須であった。
- そのためにFireEye NXを導入することになったが、SSLで隠蔽された攻撃への対応も必要だった。
- SSL通信の複合・最暗号化処理を行うと、パフォーマンスが大幅に低下する懸念があった。

ソリューション

- FireEye NX
- BIG-IP アドオンライセンスSSL Forward Proxy
  BIG-IP にSSL Forward Proxyのライセンスを適用しSSL Orchestratorの機能を有効にすることで、アウトバウンド方向のSSL通信可視化を実現

メリット

- BIG-IP でSSL Orchestrator の機能を有効にすることで、システム全体のパフォーマンス低下を心配することなく、SSLで隠蔽された攻撃の検知・遮断が可能になった。
- 社外に対する説明責任が果たしやすくなった。
- 病院との信頼関係にもとづく競争優位を維持する上でも、重要な基盤となっている。

Customer Profile

メディカル・データ・ビジョン株式会社

データによる医療改革を目指し、2003年8月に設立。病院経営システムを提供し匿名化された診療情報を集積する「データネットワークサービス」と、集めた診療情報を分析して提供する「データ利活用サービス」という、2本柱で事業を展開している。すでに2,000万人超の診療データを収集・蓄積し、日本最大級の量と質を誇る医療ビッグデータを独自構築。製薬会社等への分析データ提供等を通じ、医療の質向上に貢献し続けている。

その一環として検討されたのが、マルウェア等に感染した社内端末やサーバから攻撃者サイトへの通信を、可視化・遮断することである。そのためにMDVではFireEye NXの採用を決定。しかし最近の標的型攻撃ではSSLで通信を隠蔽していることも多く、また、SSL通信の復号・暗号化処理を行うと、システム全体のパフォーマンスが著しく低下することが懸念されたのである。

ソリューション

この問題を解決するため、FireEye NXの導入パートナーとなった東京エレクトロン デバイス株式会社（以下、TED）が提案したのが、FireEye NXにBIG-IPを組み合わせ、そのBIG-IPをSSL Orchestratorとして活用するという構成である。「SSL処理をBIG-IPで実行すれば、パフォーマンス低下を心配することなく、SSLで隠蔽された通信を可視化・遮断できます。またF5とFireEyeは2015年10月にパートナーシップを結んでおり、安心して導入できる提案内容だと評価しました」（渡邉氏）。

MDVでは、ファイアウォールの前段にインラインモードでBIG-IPを設置することで、SSL Orchestratorの機能を追加。アウトバウンドのSSLを利用した通信をここで復号した上でFireEye NXへと送り、チェックされた通信を再びSSL化している。これらの機器の設置や設定もTEDが担当。導入前にはTED社内に検証環境を構築し、実機による動作検証も行っている。

「TEDのエンジニアはまるで当社の社員のように、積極的に動いてくれました。また運用開始後の課題解決にもご協力いただいています」。

「SSL処理をBIG-IPで実行すれば、パフォーマンス低下を心配することなく、SSLで隠蔽された通信を可視化・遮断できます。またF5とFireEyeは2015年10月にパートナーシップを結んでおり、安心して導入できる提案内容だと評価しました」。

メディカル・データ・ビジョン株式会社
さくらDB部門長 シニアマネージャ 渡邉 幸広 氏

メリット

■標的型攻撃を受けた場合でも早期の検知・対応が可能

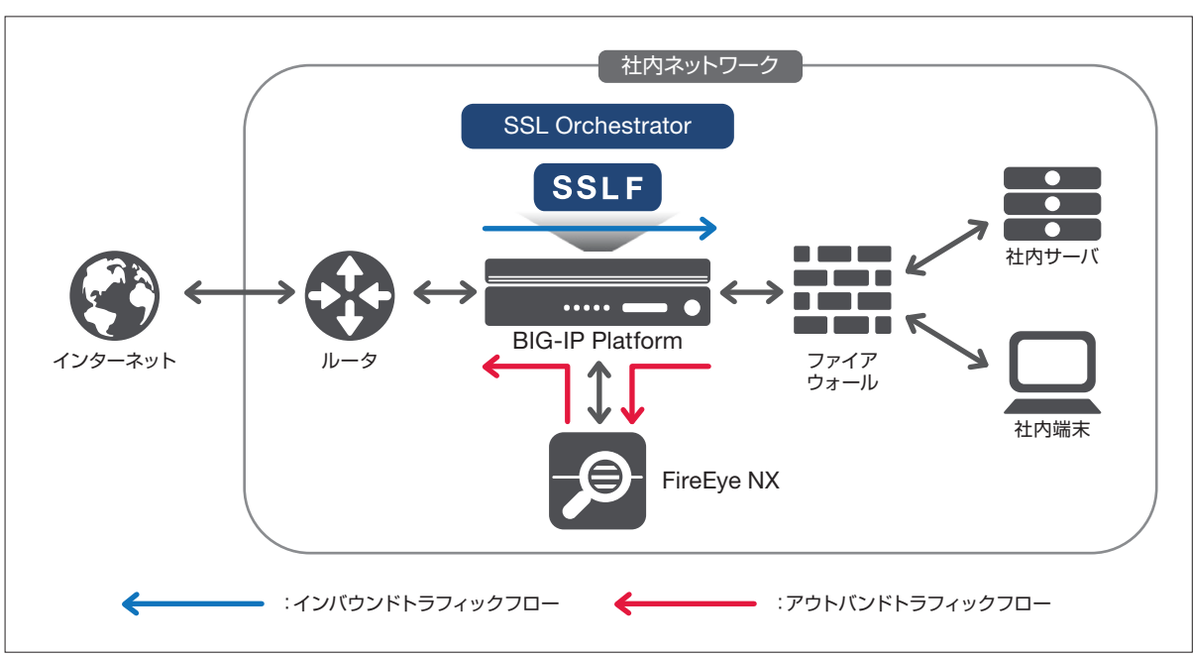
FireEye NXとBIG-IPを組み合わることで、ファイアウォールだけでは検知できないC&Cサーバなどへの SSL通信を、短時間で検知できるようになった。標的型攻撃を100%防ぐことは難しいが、仮にマルウェアが社内システムに侵入したとしても、その後の通信からマルウェアの存在を検出し、早い段階で対処することが可能なのである。なおMDVではこのメリットを最大限に活用するため、社内CSIRTの設置も進めつつあるという。

■取得・蓄積された通信ログはフォレンジックでも活用可能

BIG-IPは通信ログを取得でき、それを外部のログ管理システムに転送することも可能だ。将来はこのログデータを蓄積し、セキュリティインシデントが発生した際のデジタルフォレンジックに活用することも視野に入っているという。

■社外への説明責任や病院との信頼関係維持にも貢献

標的型攻撃への早期対応が行えるようになったことで、これまで築き上げてきた病院との信頼関係も維持しやすくなったと渡邉氏は語る。「病院との信頼関係を強化できれば、使えるデータも増えて当社の強みがより強化され、事業の成長に大きく貢献します。今回導入した仕組みは、このような事業の継続やさらなる発展の上でも、欠かせない基盤になっています」。



F5 ネットワークスジャパン合同会社

東京本社
〒107-0052 東京都港区赤坂4-15-1 赤坂ガーデンシティ19階
TEL 03-5114-3210 FAX 03-5114-3201

西日本支社
〒530-0012 大阪府大阪市北区芝田 1-1-4 阪急ターミナルビル 16 階
TEL 06-7222-3731 FAX 06-7222-3838

お問合わせ先：https://f5.com/jp/fc/

2017 年 12 月