FORTINET

伊藤忠テクノソリューションズグループ
CTC SP

FortiGate 導入事例

学校法人 神奈川大学

ファイアウォールの性能を次の世代へ、P2P対策を一本化へ。

学校法　人 神奈川大学
情報システム推進部 メディア教育課 課長
村山 宏幸 氏
http://www.kanagawa-u.ac.jp/

課　題

- ファイアウォールの機能、スループット不足
- P2P対策機器等の一元管理と自動分析
- TCO削減とSSL-VPNへの布石

導入前
- ファイアウォール：既存の他社ファイアウォール製品 2台
- P2P機器：帯域制御装置 1台

導入後
- ファイアウォール：FortiGate-1240B 2台
- ログ収集分析機器：FortiAnalyzer-400B 1台

神奈川大学様は、創立100周年に向けた将来構想を策定され、さらなる大学・附属学校の質的向上と発展に向けて新たな建学の道を歩み始めた総合大学です。その総合情報ネットワーク「MIYAMO-NET（みやもねっと）」は、横浜キャンパスを中心にして、湘南ひらつかキャンパス、附属中・高の中山キャンパスなどを専用回線で結ぶ構成です。近年、インターネット接続の出入り口となる横浜キャンパスの回線を50Mbpsから100Mbpsに増速したことで、外部からのウイルス攻撃も増大し、ファイアウォールの通信テーブルが飽和状態となり、通信が切れてしまう事態が発生していました。また、同ネットワークではP2P対策の製品も導入していましたが、今回各社の評価機テストを踏まえて、次世代のファイアウォール環境とP2P対策の一本化を図るFortiGate-1240B、およびアクセス分析・レポートのためのFortiAnalyzer-400Bの導入を選択されました。なぜFortiGateの選択が最適だったのか、従来製品からの移行に不安や課題はなかったのか。情報システム部 メディア教育課 課長 村山氏にお聞きしました。

■課題と導入の経緯

スループットの向上とコスト削減の両立を求めて

村山氏（以下同）：従来利用していたファイアウォール製品では、セキュリティゾーンを切っていくのが難しくなり、パフォーマンスの限界がきていました。また、100Mbpsの回線に増速したことでウイルス等の進入も増大した結果、ポートスキャンが増えました。それにともないファイアウォールの負荷が増大し、回線が飽和状態になる前に過負荷で通信が切れてしまうこともあり、回線を増速してもファイアウォールがボトルネックになっていました。そこで、機能と処理能力の両面でファイアウォールが限界にきていたことから更新を決意したわけです。また、従来のファイアウォール製品では、P2Pを介したコンテンツの遮断ができませんでした。別途、P2P遮断のための製品を導入してなんとか管理していたのですが、今回の更新でこれらをひとつに統合し、コスト削減と管理の簡素化を図りたいと考えました。こうした要求を満たせる製品は、FortiGate以外に何社かあったのですが高価でしたし、スループットの面で不安が残りました。

FortiGateは、スループットを格段に上げたうえでファイアウォールとしての機能を満たす設計でした。一方、競合する他製品はアーキテクチャを見直してスループットを上げて機能を満たすものでFortiGateと比べて製品コンセプトが異なっていました。FortiGateと競合製品ともに検証機を借りてテストしました。セキュリティ上の課題は、いろいろな研究室で使われている持ち込みPCなどの見えにくいアクセスから生じます。

■競合製品との比較検証

いかにアクセスの自由度と安全性を高めるか

今までのファイアウォール製品とFortiGateでは使い方がどのように変わるのか、どのような新しい使い方ができるのかなど、事前に検証機をお借りして評価しました。概ね同じような使い方ができるとわかったので、既存製品の後継機ではなく、FortiGateを選んでも問題ないと判断したわけです。実際に通信上に流れているものと同じ通信内容を評価機に流し、同じ設定ができるのか、振る舞い方が変わるのかなどをチェックしました。

大学のファイアウォールと企業のファイアウォールは、考え方が大きく異なります。一般的にはファイアウォールという名の通り、いかに防御するかが最大の使命です。しかし、大学ではいかに自由な情報アクセス環境を用意するかが求められます。それぞれの研究室ごとに先生方の求める自由度も異なりますし、アクセスの基本は“できるようにすること”が前提で、セキュリティを担保したがために先生方が望む通信を遮断してしまわないかを入念に検証しました。従来のファイアウォール製品では閾値を下げていたため通信可能であったものが、FortiGateでは遮断されはしないかなど、自由度と安全性の担保の仕方を評価するのがポイントでした。

学校法人 神奈川大学

■選択の理由

本学が求めるUTMとしての総合力を見極めて

村山氏(以下同):本学ではWebフィルタ、アプリケーション制御などに特化した製品を個別に導入しており、そのためにセキュリティの一元管理が困難になっていました。今回、FortiGateの選定にあたっては機能とスループットの高さを第一に選びましたが、UTM(統合脅威管理)としての機能を一体化した製品であることと、そうした統合化による管理コスト削減の面でも優位であることが決め手になりました。また、大学関係の遠隔地施設を結ぶVPNゲートウェイとして導入しているFortiGate-50Bおよび80Cの動作が安定しており、Webユーザインターフェースが今までのファイアウォール製品と類似していることからリプレースによる混乱が少ないことも理由となりました。

さらに、従来はファイアウォールのトラフィックを集計することができず、そのつど手作業で集計・グラフ化していましたが、工数が多く、リアルタイムに通信状態を可視化することができませんでした。今回、併せてFortiAnalyzer-400Bを導入することで、運用管理を一新することも狙っています。

■移行作業

約1,700ステップものポリシーの異機種間移行を可能に

使い方はほぼ従来製品と同じように可能なことが分かっていたのですが、1,700ステップ以上あるセキュリティポリシーを簡単に右から左へ移行することはできませんでした。企業とは異なり、大学では研究室やテーマごとにポリシーを記述するため、ステップ数が予想以上に大量になってしまいます。デフォルトの設定に隠れていたコンフィグの抜き出しに苦労したり、あるセキュリティゾーン間で通信ができなくなったりするなど、問題点も見られましたがCTCSPさんのナレッジと経験を活かしてもらい、何とか移行作業を完了させることができました。

実際には、従来機種に置き換える更新だったため、1,700ステップのポリシーのすべてを移行してテストすることはできませんでしたが、半年以上経過して未だトラブルは発生していません。

■導入メリットと今後の展望

TCO削減の次は、SSL-VPNへの道

FortiGateにファイアウォールとP2P対策の機器を一本化することによって、トータルな運用コストを抑えることができ、運用管理もシンプルになりました。また、従来のファイアウォール製品に比べ、次の世代へと進化したファイアウォールの導入ができたことに満足しています。おかげさまで通信の遮断や遅延も発生せず、先生方からもまだクレームはきていません。

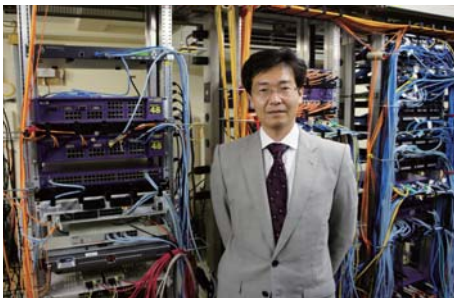
今後は、SSL-VPNによって自宅にいながら大学のリソースを使う環境の整備へも道が開けたといえます。学内の図書館では各種新聞や雑誌などのオンラインメディアや学術論文を閲覧できるデータベースなどと契約しており、学内からでなければアクセスできない仕組みでしたが、近い将来には学外からもSSL-VPNで利用可能にしたいと考えています。もちろん、サービスの種類によって規制が必要ですので、精査しなければなりません。

また、最近はデータ量の多い映像や音声などのアプリケーションが増えています。次の取り組みとして、インターネット接続回線の高速化や多重化などの対策を視野に入れています。

なお、FortiAnalyzer-400Bの採用によって、ネットワークの利用状況や攻撃先を可視化し、レポートにまとめる作業が格段に自動化されると期待しています。今後はその分析レポートを基に、一歩進んだ最適なネットワーク利用を目指していく予定です。

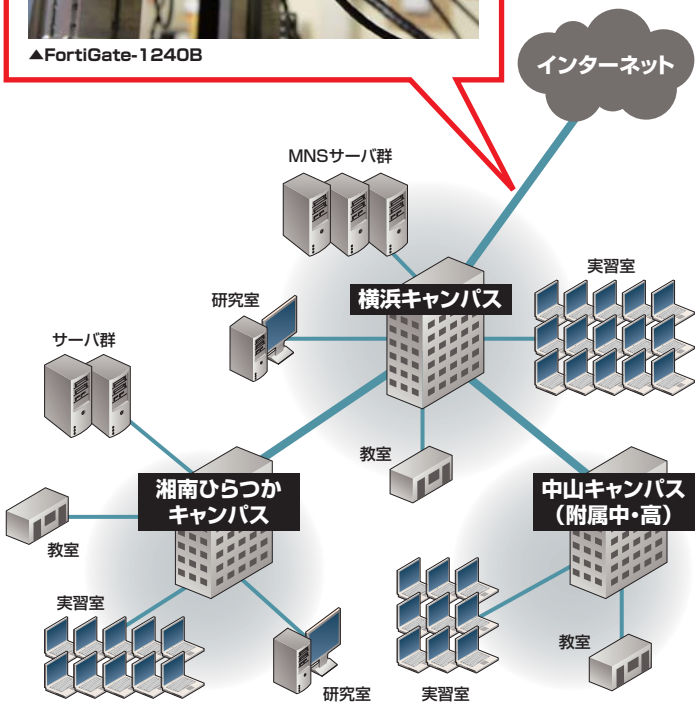
●神奈川大学 総合情報ネットワーク「MIYAMO-NET」に導入されたFortiGate

※MIYAMO-NETの「ミヤモ」は、神奈川大学・横浜キャンパス周囲の古い地名「宮面ヶ丘(みやもがおか)」に由来しています。



▲冗長構成のFortiGate-1240BとFortiAnalyzer-400B

▲FortiGate-1240B



●お問い合わせは

伊藤忠テクノソリューションズグループ
CTC SP
シーティーシー・エスピー株式会社
本　社:〒154-0012 東京都世田谷区駒沢1-16-7
TEL.03-5712-8070 FAX.03-3419-9679
http://www.ctc-g.co.jp/~ctcsp/
sp-admin@ctc-g.co.jp

国内販売代理店
・霞が関:TEL.03-6203-5190
・大　崎:TEL.03-6417-5950
・名古屋:TEL.052-203-2239
・大　阪:TEL.06-6151-8860
・福　岡:TEL.092-734-6251

開発・製造元
FORTINET