CHECK POINT™

Quantum Maestro中核のクラスタ構成で柔軟な拡張性を備えた次世代ファイアウォールシステムを構築


提供：東京工業大学

日本最高の理工系総合大学である東京工業大学（以下、東工大）は、2020年にファイアウォールシステムを更新し、チェック・ポイントのハイパースケール・ネットワークソリューション「Quantum Maestro」を中核として、5台のセキュリティゲートウェイを組み合わせたクラスタ型システムで、次世代ファイアウォール（NGFW）システムを構築した。新システム構築により、基幹ネットワークの安定稼働と、柔軟な拡張性を獲得。さらに、チェック・ポイントの使いやすいログ検索とレポートを活用して、NGFWの機能を最大限に引き出す体制を作り上げた。

東京工業大学
Tokyo Institute of Technology

お客様プロフィール

国立大学法人東京工業大学

https://www.titech.ac.jp/

本部所在地：東京都目黒区大岡山2丁目12-1

1881年創立。「世界最高の理工系総合大学の実現」を長期的な目標に掲げる。学生数は学士課程・大学院合わせて約10,500人、教員および職員は約3,600人。日本の大学で初めて学部と大学院を統合して、6つの「学院」制へ移行し、学士課程から博士後期課程まで一貫した教育カリキュラムを組む。創立150周年の節目となる2031年までを「キャンパス・イノベーションエコシステム構想2031」としてキャンパス環境整備を推進中。

課　題

- 将来のスループット変化へ確実に対応できる「柔軟な拡張性」確保
- 次世代ファイアウォール（NGFW）の膨大なログを最大限に有効活用

ソリューション

- Quantum Maestro×2台と、Quantum CP6200 Plus×5台によるクラスタシステム構築
- Quantum Smart-1×2台の使いやすいログ検索とわかりやすいデイリーレポートで、NGFWの機能を日々の運用に活かす

東京工業大学
准教授 博士（工学）
松浦 知史 氏

常にその時点で最良・最適な技術を選択してセキュリティ脅威に備える

東工大は2021年から、田町キャンパスの再開発を契機とする「キャンパス・イノベーションエコシステム構想」に取り組んでいる。大岡山・すずかけ台・田町3キャンパスそれぞれの姿と役割を変え、有機的なキャンパス連携と次世代型産学連携を実現していく一大変革だ。

「常に動きがあることは東工大の特徴です。魅力といってもいいでしょう」と、東京工業大学 学術国際情報センター 准教授であり、東工大CERT（情報システム緊急対応チーム）の統括責任者を務める松浦知史氏は語る。

動きのひとつに、デジタルトランスフォーメーション（DX）もある。東工大は2021年を「DX元年」と位置づけ、ファイル共有、チャット・コミュニケーション、ビデオ会議など、複数のクラウドサービスを全学一斉導入し、教育・研究環境の充実と業務改善を推進中だ。

当然ながらネットワーク・トラフィックは増加している。「基幹ネットワークのスループットは、10年前に比べると3倍近くに増えており、求められるサービスレベルも高くなっています。いま最も重要なのは安定稼働です」と松浦氏は強調する。

一方で、セキュリティの脅威は増すばかりだ。ばらまき型攻撃は日々大量に送信されてくる。特定大学・研究機関にターゲットを絞った標的型攻撃はますます高度化し、手の込んだものが開発されている。

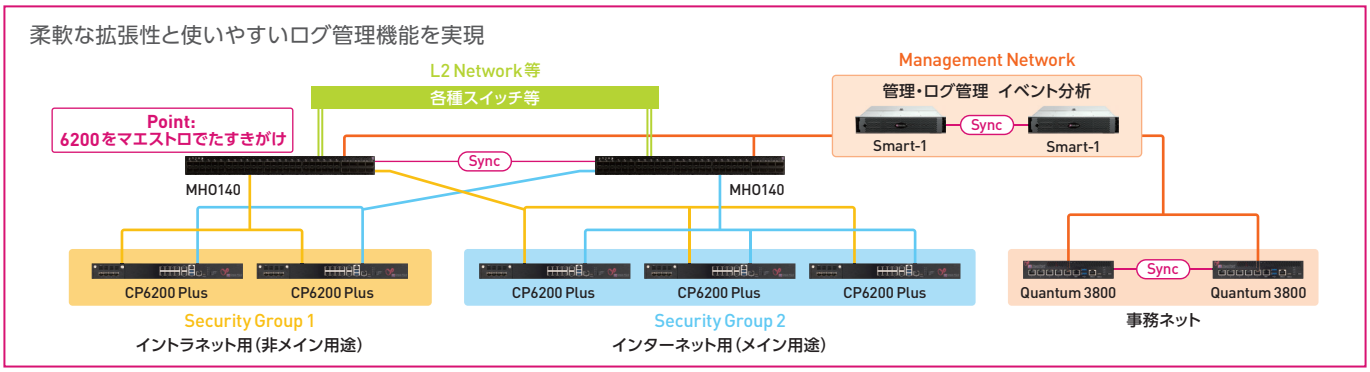
すばやく変化するセキュリティ・トレンドを確実にキャッチアップするため、基幹ネットワークのファイアウォールシステムは5年ごとに刷新し、予算とのバランスの中でその時点での最良のソリューション、最適な技術を選択するのが東工大の情報セキュリティ施策における基本方針である。

将来の不測の変化にも柔軟でリニアな拡張性が性能要件を確保

2020年のシステム更新にあたって重視したのは、「柔軟な拡張性」と、「ログ検索のしやすさ」である。

「ネットワーク状況がどのように変化した場合でも、柔軟に対応できる体制を作っておくために選んだのが、チェック・ポイントのQuantum Maestroを中核にしたソリューションです」と松浦氏。

Maestroは、1.5 Tbpsの脅威保護スループットを実現する現時点で業界最高峰のハイパースケール・ネットワークソリューションである。最大の特長は、接続するゲートウェイの台数を増やせば、リニアにスループットを拡大できることだ。コネクションの同期処理やクラスタリング処理はMaestroが一手に引き受け、



ゲートウェイ側はMaestroからロードシェアリングされるトラフィックのセキュリティ処理に専念するからである。
しかも、Maestroは複数のセキュリティグループを構築できる。東工大は、複数台数のゲートウェイを導入して、メイン用途と非メイン用途で2つのセキュリティグループに振り分け、状況変化に応じて割り振りを変える形で、柔軟な拡張性を確保することにした。この方法であれば、今後5年程度であれば、ゲートウェイを追加購入することなく、セキュリティグループの振り分けを変えるだけで、拡張性を確保できる。
「数年先を見越して大きめの機種を1台導入し、仮想的に区切って運用し続けるよりも、小規模で安価な機種を複数台数使うほうが、投資効率が高いと判断しました」と松浦氏は説明する。
比較検討した他社提案の中には、チェック・ポイント同様にゲートウェイをクラスタ構成にする提案もあったが、チェック・ポイントは他社の半分程度であるゲートウェイ5台だけで目標の拡張スループットを確保できるため、見積り価格も安かった。リニアなハイパースケールならではの強みである。

次世代ファイアウォールの有効活用にはログ検索、レポートの使いやすさが不可欠

ネットワーク更新のもうひとつの要件として、ログ管理、イベント解析のしやすさを重視したのは、次世代ファイアウォール（NGFW）の豊富な機能を最大限に活かすためである。
東工大は、2015年度にNGFWを導入した。IPS（不正侵入防止システム）、アプリケーション制御、アンチボットなどの最新機能を複数組み合わせて、ゼロデイ攻撃をはじめとする未知の脅威にも対応するためだ。2015年時点でも選んだのはチェック・ポイント製品であったが、評価の決め手は、セキュリティ管理アプライアンス「Quantum Smart-1」のログ検索のしやすさだった。
NGFWは、従来型ファイアウォールよりもはるかに大量のログが発生する。重要なログが埋もれてしまうことなく、確実にトレースして解析するには、ログの検索性能がきわめて重要だ。
「Smart-1は、ログ検索が使いやすい。検索項目を入力するフィールドを気にすることなく、『Googleライク』に、単一の検索窓を使った全文検索でドリルダウンしていけます。レポート機能も優れています。きれいで、見やすく、カスタマイズしやすい」と松浦氏。
Smart-1は、ネットワーク管理のエンジニアのみならず、職員からも評価が高い。今回、職員が使う「事務ネット」は、基幹ネットワークとは別に構築した。この事務ネットは、利用者である職員が自らSmart-1を駆使して、ログ管理、インシデント追跡、ポリシーの追加設定などを行っている。

圧倒的な安定稼働とインシデントレスポンスの時間短縮に成功

新システムは、2021年4月、稼働を開始した。基幹ネットワークのゲートウェイとしては、中規模企業向けセキュリティゲートウェイ「Quantum CP6200 Plus」を5台導入。これを、2台のMaestroにすべて「たすきがけ」で接続した。
Maestroは、5台のCP6200 Plusを3台と2台のセキュリティグループに分け、インターネット用とイントラネット用のポリシーを適用して運用している。将来インターネットトラフィックが増大すれば、2台あるイントラネット用ゲートウェイをインターネット用へと順次切り替えて対応していく。
システム更新の最大の効果は、「圧倒的な安定稼働」である。本稼働から1年以上経つが、チェック・ポイント製品が原因のクレーム、遅延などは1件も発生していない。
「Maestroのクラスタリング処理や、ネットワークレイヤでのセッション振り分けのしくみはシンプルでわかりやすい。シンプルだからこそ、トラブルが起きにくく、信頼性が高いというMaestroの設計思想が、運用しているとよくわかります」と松浦氏は指摘する。
新システムのさらなる成果は、NGFWの効果的な運用が実現できたというセキュリティメリットである。
「IPSもアプリケーション管理もログの取りこぼしがないなど、チェック・ポイントのNGFW機能には全体的に満足しています。こうした複合セキュリティの機能を日々の運用に活かしていくには、理解しやすい形で見せてくれるユーザーインターフェースが不可欠です」と松浦氏。
ネットワーク管理者はもちろん、職員も、毎朝Smart-1が自動作成するデイリーレポートを読み、「このアラートが多くなっているから、ちょっと精査して対策を立てておこう」と即座に実行している。レポートやログ検索の使いやすさが、インシデントレスポンスのインターバルを短く回すことに貢献しているのである。
今後も、ネットワーク利用形態は、さまざまな変化が予想される。「どのように変化しても、インシデントが発生したときには必ず詳細まで『調査しきる』のがわれわれの使命です」と松浦氏。
そして、インシデンドの詳細を「漏れなくしっかり見せきる」という重要な任務を担って、MaestroとSmart-1で構築したネットワークセキュリティシステムは今日もフル稼働している。

CHECK POINT™
チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
info_jp@checkpoint.com https://www.checkpoint.com/jp/