シスコ セキュリティ ソリューション導入事例

学校法人同志社 同志社大学

クラウド時代の、より自由なネットワークを目指し 利便性向上と通信可視化、セキュリティ強化を実現

製品 & サービス

- Cisco Firepower 4100 シリーズ NGFW アプライアンス
- Cisco Firepower Management Center 2500
- Cisco Advanced Malware Protection（AMP）for Networks
- 次世代 IPS（NGIPS）、URL フィルタリング ライセンス

課題

- Office 365 などクラウド、SaaS との安全、安定した接続
- プロキシによる二段階認証で利便性に不満
- 通信の見える化、証跡管理の強化

ソリューション

- Cisco Firepower に IPS、アンチマルウェア、URL フィルタなどゲートウェイ セキュリティを統合、強化
- IEEE 802.1X 認証によるユーザ利便性の向上
- AMP による高度なマルウェア防御
- 機器シンプル化、自動チューニングと FMC による一元管理で運用性向上

結果～今後

- セキュリティ機能統合と強化、機器構成と運用をシンプル化
- 通信パフォーマンス、セキュリティを維持してユーザ利便性を向上
- さらなる自由かつ安全なネットワークを目指す

同志社大学は 1875 年に新島襄が同志社英学校を創立して以来、「良心を手腕に運用する人物の育成」を目指し、「キリスト教主義」「自由主義」「国際主義」を教育の理念としています。創立 150 周年を迎える 2025 年に向けて、世界水準の教育、研究活動をさらに発展させ、「学びのかたちの新展開」「『国際主義』の更なる深化」など “ALL DOSHISHA” で「同志社大学 VISION 2025」を推進しています。

教育理念である『自由主義』。何が起きているかをしっかり可視化した上で、より自由なネットワーク環境の実現へ発想を転換しました。

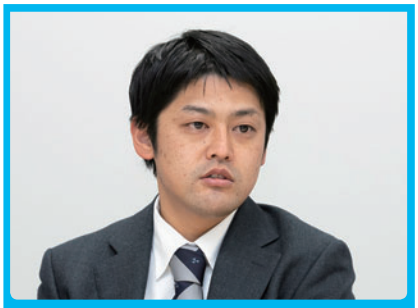
—— 同志社大学 総務部情報企画課 情報ネットワーク係長 山北 英司 氏

課題

同志社大学では変化の激しい現代社会において「良心を手腕に運用する人物の育成」を目指し、ICT を活用した新しいスタイルの教育を実践。教育研究環境および大学運営強化の観点から、周期的なネットワーク システム更改が行われます。同志社大学 総務部情報企画課 情報ネットワーク係長 IT サポートオフィス 山北 英司氏は、全学ネットワーク システム リプレースのセキュリティにおけるポイントを、次のように話します。

「今回は全学のメール基盤として Office 365 と新たなオンライン ストレージの導入があり、クラウドにアクセスするための安定した接続が求められました。また、ネットワーク接続時に都度ユーザ ID とパスワードを入力する Web 認証、さらにインターネット利用時にプロキシ認証という二段階方式で、ユーザの利便性も低く、加えて、最近のスマートフォン アプリでプロキシ認証対応外のものが増え、使いたいのに使えない、という声が高まっていました。これまでも利便性とセキュリティの両立を追及してきましたが、これまでの学内ネットワークは、問題が起こったときに何が起こったかを追跡できる、という発想でした。しかし、環境の大きな変化と、本学の教育理念である『自由主義』に立ち返って、何が起きているかをしっかり把握できる仕組みを導入した上で、可能な限り自由にネットワークを利用できる環境を構築しよう、と発想を転換したのです。」

同志社大学では更改に向け教職員による作業部会で要望や課題を検討。ユーザの利便性向上、入口出口対策、通信の見える化、そして安定稼働といった観点から、機器の選定を進めていきました。その中で IPS（Intrusion Prevention System：侵入防御システム）の必要性が高まりますが、「導入には不安もあった」と総務部情報企画課 情報ネットワーク係 IT サポートオフィス 藤江 悠五氏は話します。



同志社大学
総務部情報企画課
情報ネットワーク係長
IT サポートオフィス
山北 英司 様

同志社大学
総務部情報企画課
情報ネットワーク係
IT サポートオフィス
藤江 悠五 様

同志社大学
総務部情報企画課
情報ネットワーク係
IT サポートオフィス
藤堂 慈 様

「IPS は誤検知が多く止め過ぎてしまうのではないか、またチューニングが煩雑で日々の運用負荷が高いのでは、といった不安があり、これまでは他社製の IDS（Intrusion Detection System：不正侵入検知システム）の運用に留まっていました。しかし、今回提案されたシスコの次世代ファイアウォールに統合された IPS であれば、それらの不安を払拭できる、という期待がありました。」
他社製品との検知精度など、さまざまな指標での比較検討の結果、Cisco Firepower NGFW & NGIPS（次世代ファイアウォール & 侵入防御システム）の採用が決定し、2018 年 9 月より運用が開始されました。山北氏は次のように話します。
「採用にあたっては、構築パートナーの担当者が熱意を持って説明、さらに試験導入での POC ※1 も行っていただき、われわれがいま、やるべきことを示していただけました。」

通信のパフォーマンスを落とさない、可視化と安全性、運用性を評価しました。

ソリューション

利便性向上、通信パフォーマンスを損なうことなくゲートウェイ セキュリティ強化

山北氏は、セキュリティ機能の統合と強化による効果を、次のように話します。
「利便性を高めるため、Web 認証に代わりユーザ Credential を端末内に保存可能な IEEE802.1X 認証方式を採用し、Cisco Firepower により IPS、アンチ マルウェア、URL フィルタなどゲートウェイ セキュリティを統合、強化しました。クラウド、SaaS 利用などでインターネット通信は確実に増加傾向にありますが、パフォーマンスの劣化もなく、通信も安定しています。機能統合で機器構成がシンプル化したことに加え、通信ログの一元管理も実現しました。」

IPS 自動チューニングとインパクト フラグ

当初懸念された IPS の誤検知や運用負荷増大について、藤江氏は次のように話します。
「実際に運用してみると誤検知も少なく、手がかかりませんし、OS の脆弱性を考慮した攻撃検知レポートや、実際の攻撃パケットを自動キャプチャ保存する機能は、従来の IDS シグネチャ分析に比べ精度向上と、時間短縮面でメリットを感じます。また、検知した際はメール通知により挙動が把握できる安心感がありますし、検知したインシデントの緊急度に合わせて 0 ～ 4 の数字で優先度を表示するインパクト フラグ機能も、可視化という点で非常に有効です。」

AMP（Advanced Malware Protection）ライセンスを NGFW に搭載、ネットワーク上でアンチマルウェア対策を一本化

藤江氏は AMP for Networks によるマルウェア防御と、可視化機能について次のように評価しています。
「過去に遡って何が起きていたのかを把握して対応することが可能なレトロスペクティブも、証跡管理という観点から非常に頼もしい機能です。」

Cisco Firepower Management Center（FMC）による一元管理

Cisco Firepower NGFW & NGIPS 製品は、集中管理解析サーバ Cisco Firepower Management Center（FMC）との連携により、通信から判断できる情報（プロトコル、アプリケーション、OS 情報など）をデータベース化。このデータベースの内容に基づいて、IPS シグネチャの自動選択やインシデントの緊急度などに関する識別機能を提供することで、セキュリティ運用にかかる負荷を軽減します。総務部情報企画課 情報ネットワーク係 IT サポートオフィス 藤堂 慈氏は、その有効性を次のように話します。
「導入後に Cisco TAC ※2 トレーニングを受講し、ファイアウォール、IPS の機能とポリシーの追加など設定方法を学びました。ホワイトリストへの登録追加や反映の確認も簡単な操作で行えますし、FMC は一目で全体が把握できるため、管理、運用面で助かります。」

※1 POC
Proof of concept、概念実証

※2 Cisco TAC
導入されたシスコ製品のテクニカル サポートを担うテクニカル アシスタンス センター（TAC）。主にユーザ システム部門の技術者や、パートナーのサポート技術者では解決できない複雑な問題に対する調査、解析とソリューションの提供を行います。

導入ソリューション

Cisco Firepower NGFW & NGIPS 次世代 ファイアウォール & 侵入防御システム

導入製品

- Cisco Firepower 4100 シリーズ NGFW アプライアンス
- Cisco Firepower Management Center 2500
- Cisco Advanced Malware Protection（AMP）for Networks
- 次世代 IPS（NGIPS）、URL フィルタリング ライセンス

巧妙化を続けるサイバー攻撃に対抗できる、高度な防御機能を搭載

Cisco Firepower NGFW & NGIPS 製品は、絶えず巧妙化を続けるサイバー攻撃に対抗するために、IPS（Intrusion Prevention System；侵入防御システム）や AMP（Advanced Malware Protection；高度なマルウェア防御）に代表される、脅威対策に必要不可欠な防御機能を搭載しています。IPS によって、外部から侵入する脅威をシャットアウト。さらに AMP が、今まさに侵入しようとしているマルウェアだけでなく、侵入してしまったマルウェアに対してもアラートを発することで、侵入被害を最小化するとともに新たな侵入を防ぎます（これらの機能はソフトウェア ライセンスによって有効化できます）。

NGIPS

世界で 30 万台以上の利用実績があり、高い検知率と信頼性で業界標準となっているオープン ソース「Snort」を IPS コア エンジンとして搭載し、精度向上や運用軽減機能を独自に追加。脅威検知に欠かせない IPS シグネチャの開発にも定評があり、新しい脅威への迅速な対応が可能です。

Cisco AMP for ネットワーク & Cisco Threat Grid サンドボックス

Cisco AMP for ネットワークは、ネットワークを行き来するファイルを観測、記憶し続けます。それにより過去に侵入したマルウェアも含めて、どこから来てどこへ到達したのか、どんな特性なのかを管理者へ通知する、レトロスペクティブ（遡及可能な）セキュリティを提供。標準で Cisco Threat Grid サンドボックスによるマルウェア解析機能も提供します。

Cisco Talos

IPS や AMP だけでなく、その他にも高度な脅威対策機能を、他社を圧倒する高度な脅威対策の専門家集団であるセキュリティ インテリジェンス & リサーチ グループ「Cisco Talos」によって提供します。Cisco Talos の専門家たちは、毎日、何百万ものマルウェア サンプルやテラ バイト単位のデータを分析し、その成果を Cisco Firepower NGFW & NGIPS 製品に提供しています。

可視化でセキュリティ運用にかかる負荷を軽減

Cisco Firepower NGFW & NGIPS 製品は、集中管理解析サーバである Cisco Firepower Management Center（FMC）と連携することで、ネットワーク環境を学習して最適な防御体制を整えます。相互連携によって、通信から判断できる情報（プロトコル、アプリケーション、OS 情報など）をデータベース化。このデータベースの内容に基づいて、IPS シグネチャの自動選択やインシデントの緊急度などに関する識別機能を提供することで、セキュリティ運用にかかる負荷を軽減します。

IPS 自動チューニング

Cisco FMC によって、保護対象ネットワークで収集したデバイス情報から脆弱性データベースを構築。本来必要な IPS シグネチャを自動選択することによって、誤検知率の低下と検知率の向上、およびスループットの最適化に対応します。

インパクト解析と侵入痕跡

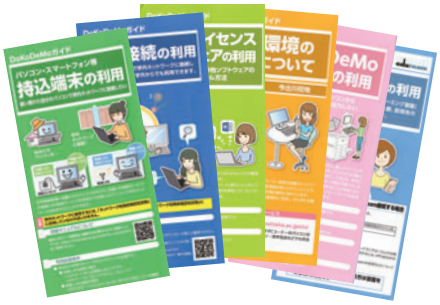
脅威を発見した際、そのインシデントが保護対象ネットワークに対して本当に影響があるものなのか、影響はないが注視すべきものなのかなど、影響を重み付けして緊急度を通知。それぞれのインシデントの相関関係を導出して、侵入の可能性を警告することも可能です。

感染デバイスの自動隔離

デバイスの認証情報とアクセス制御を司る Cisco Identity Services Engine（ISE）と連携することで、Cisco Firepower NGFW & NGIPS 製品が発見した脅威に基づいて、Cisco ISE がデバイスへ許可しているアクセス制御を動的に変更。感染デバイスを自動的に隔離して、迅速に脅威を封じ込めることが可能となります。

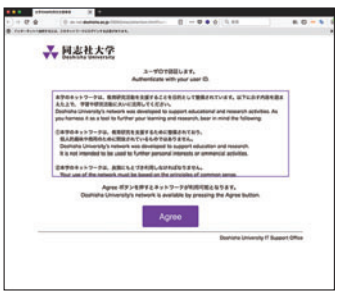
同志社大学の IT リテラシー教育とセキュリティ啓蒙活動

同志社大学では 2000 年代初頭より全学生を対象とした「ネットワーク利用資格認定試験」を実施。合格しなければ学内ネットワークが利用できない仕組みになっています。内容はネットワーク、セキュリティからインターネット上のトラブル、著作権や肖像権などを網羅しています。そのほか、IT 利用者向けに、さまざまな利用ガイド小冊子を配布しています。



認証のシンプル化に伴う抑止力画面

今回の認証シンプル化による学内ネットワーク利用意識の低下を防ぐため、ネットワーク接続時に利用規約への同意画面を表示。これは、シスコ無線 LAN ソリューション、ワイヤレス LAN コントローラ（WLC）との連携により実現しています。



学校法人同志社
同志社大学

所在地
今出川校地
今出川キャンパス　京都市上京区今出川通烏丸東入
新町キャンパス　京都市上京区新町通今出川上ル近衛殿表町 159-1
烏丸キャンパス　京都市上京区烏丸通上立売上る相国寺門前町 647-20
室町キャンパス　京都市上京区烏丸通上立売下ル御所八幡町 103
京田辺校地
京田辺キャンパス　京田辺市多々羅都谷 1-3
多々羅キャンパス　京都府京田辺市多々羅西平川原 39-16
学研都市キャンパス　京都府木津川市木津川台 4 丁目 1-1
東京サテライト・キャンパス　東京都中央区京橋 2 丁目 7 番 19 号京橋イーストビル 3 階
大阪サテライト・キャンパス　大阪市北区梅田 1-12-17 梅田スクエアビルディング 17 階
創立　1875 年（明治 8 年）
学生数　学部 27,024 人、大学院 2,248 人（2018 年 5 月 1 日現在）
教員数　専任教員 800 人（うち外国人教員 79 人）
嘱託講師 1,557 人
（2018 年 5 月 1 日現在）
URL　https://www.doshisha.ac.jp/

同志社大学は、1875 年京都・寺町に同志社英学校として新島襄により創立されました。建学の精神に基づく「良心教育」を原点とし、「キリスト教主義」「自由主義」「国際主義」の 3 つを教育理念に掲げ、良心を手腕に知識、能力を運用し、社会に貢献する人物の育成を目指しています。14 学部 16 研究科を有する総合大学で、2017 年にはドイツに EU キャンパスを開設しました。また、学校法人同志社は幼稚園から大学・大学院までを擁し、建学の精神に基づく一貫教育を実現しています。

結果～今後

山北氏は今回の成果と今後の展開について、次のように話します。
「今回、Cisco Firepower によるセキュリティ機能の統合と強化により、クラウド時代のネットワーク基盤が実現しました。パフォーマンスを落とさずユーザの利便性を向上し、機器構成も IPS を含む運用も、シンプル化できました。少数の人的リソースで 3 万人規模のネットワークを管理、運用するわれわれにとって、セキュリティの日常運用において手がかからない、困ることがないということが最大のメリットです。今後、機能を使いこなしさらに利便性と安全性を高めていきたいと考えていますので、シスコには教育機関ネットワークの現状課題解決だけではなく、夢を描けるソリューションの開発と提供に期待しています。」

その他の詳細情報

シスコ セキュリティの詳細は、https://www.cisco.com/jp/go/security/ を参照してください。

シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

お問い合せ先

2042-1902-01A-F