導入事例

FortiDeceptorで ラテラルムーブメントの検知と インシデント対応の優先順位付けを 低コストで実現

相模女子大学は「高潔善美」を建学の精神に、発想力を養い、女性の美質を高める女子教育を120年以上にわたって行ってきた。神奈川県相模原市のキャンパス内には幼稚部から小学部、中学部・高等部、そして大学および大学院までがそろい、約5000名の学生・生徒が日々学業に励んでいる。
GIGAスクール構想に代表される近年の教育のデジタル化を受け、小学部ではiPadやクラウドサービスを利用した授業を行うほか、中学部・高等部、大学でもパソコンやタブレットを教育に活用。大学事務部情報システム課ではそれら学園支給端末の運用や、700名に上る教職員が利用するパソコン、ネットワークやサーバの運用管理を担っている。

課題1：環境もリテラシーもばらばらな中で利用者に負担をかけない対策を

幼稚部から大学まで幅広い教育機関が一つのキャンパス内にある相模女子大学。IT環境の利用者も、学生・生徒から研究者、教員まで多様だ。利用する端末の種類やOSのバージョンもさまざまならば、ITリテラシー、そしてセキュリティリテラシーもまちまちとなっている。「たとえばWindows Update一つとっても、自力でアップデートできる人もいればできない人もいる、という具合です」（薄氏）
そんな中、情報システム課では、どこか一つの組織だけに偏りすぎないよう留意しながら、学園全体のITインフラの運用・管理に当たっている。
セキュリティ面では、インターネットとの境界部分にファイアウォールを設置して外部からの攻撃に備えるほか、学生・生徒が利用する端末向けのネットワークと教職員向けのネットワークをレイヤ3スイッチで分離し、関係者以外が不用意にアクセスできない環境を整備。さらに、学園支給の端末については、アップデートによる脆弱性対応やウイルス対策ソフトの導入といった対策を打ってきた。
この際に重視しているのは、いかに利用者の負担にならない形で必要なセキュリティを担保するかだ。「時には学生・生徒が個人のパソコンをBYOD的に持ち込んで利用することもありますが、この場合、学園側からウイルス対策ソフトの導入を強制するわけにはいきません。セキュリティリテラシー教育を実施し、対策の必要性を周知することに力を注いできました」（薄氏）

課題2：防御をすり抜けた脅威が動き始めた段階で把握する方法を模索

薄氏は昨今のサイバー攻撃の高度化を踏まえ、ファイアウォールでの境界防御を実施しつつ、さらに「侵入される前提での対策」も必要だと考えるようになった。具体的には、防御の網をすり抜けて侵入してきた脅威を検知し、ラテラルムーブメント（横展開）を始めて実害が生じる前に封じ込める対策だ。
しかし、多種多様な端末が混在し、時には持ち込み端末も生じる相模女子大のような教育機関では、EPPやEDRのようにエージェントソフトウェアのインストールを前提とする対策は実施が困難だった。
次に考えたのが、パケットをミラーリングしたり、フロー情報を収集・分析し、ネットワーク内部のトラフィックを監視して脅威を検知する方法だ。しかし、収集すべきデータやログが膨大な量に上るため、限られた人手で運用を回している情報システム課にとっては運用工数が大きすぎる上、コスト面でも導入が難しいと判断した。

Sagami Women's University

詳細

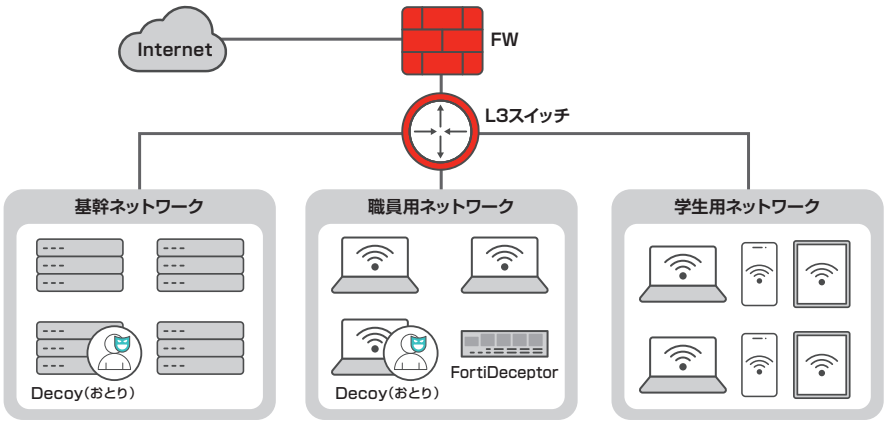
顧　客：学校法人 相模女子大学
業　種：教育
所在地：神奈川県
学生数：約5000人

ソリューション

- FortiDeceptor

導入の効果

- FortiDeceptorのアラートがなければ緊急性は低いと判断でき、インシデント対応の優先順位付けが容易に
- コストや工数をかけずに、内部に侵入した脅威を検知できる環境を整備
- エージェントのインストールなど利用者に負担をかけることなく対策を実施



学校法人 相模女子大学
大学事務部
情報システム課課長
薄 龍興氏

「FortiDeceptorからのアラートがなければ、少なくともラテラルムーブメントは発生していないだろうと判断でき、優先順位を付ける際の非常に有用なメルクマールになっています」

Fortinetを選んだ理由／導入の効果

そんな時に耳にしたのが「FortiDeceptor」の存在だ。
薄氏は以前から、ハニーポット技術によって、どのようなサイバー攻撃があるかをモニターしている取り組みを耳にし、興味を抱いていた。学内に侵入した脅威を検知するため、このようなセンサーを自力で構築することも考えたが、学習・研究用途ならばともかく、実ネットワークでは踏み台化されるリスクなどを懸念し悩んでいたところに、FortiDeceptorは渡りに船のソリューションだった。
「学内ネットワークの通信が見えないことに課題を感じ、何らかの形でモニターできる手段を探していたところにFortiDeceptorの説明を聞き、『これならば、感染した端末がほかの端末に総当たりのアクセス試行やスキャンを実施するような動きがあれば検知、対応できる』と考え、試すことにしました。コストもリーズナブルで導入しやすかったこともポイントでした」（薄氏）
フォーティネットジャパンの担当者がFortiDeceptorの関連ドキュメントを日本語化し、要点を数枚の資料にまとめて提供したため、初めて触れるユーザーインターフェイスでもそれほど戸惑うことはなかった模様。また、おとり用仮想マシンの構築で行き詰まった際には、リモート会議を通してフォーティネットのエンジニアと画面を共有しながら作業することで、導入はスムーズに進んだ。
「実は一番緊張したのは、評価用ライセンスを用いて初めておとり資産を立ち上げた時でした。もし直後にアラートが飛んでくれば、すでに何らかの脅威が侵入済みだったことになりますが、幸いなことに何もなく、安心できました」（薄氏）。学内の典型的な環境を模し、2024年5月から本格稼働を始めた後も、時折薄氏が自らの手でポートスキャンを実施して稼働確認を取っている程度で、平穏な状態が続いている。

解決方法：FortiDeceptor

FortiDeceptorの導入によって得られたのは大きな安心感だ。「セキュリティ製品を運用していると、時折、ファイアウォールやウイルス対策ソフトからアラートが飛んでくることがあります。しかしそうした事態でも、FortiDeceptorからのアラートがなければ、少なくとも横方向に広がってはいないだろうと判断でき、インシデント対応時に優先順位を付ける際の非常に有用なメルクマールになっています」（薄氏）
逆に、FortiDeceptorが何らかの動きを検知してメールやSNMPトラップでアラートを受け取った場合には、攻撃元の端末の特定と所有者への連絡、隔離などの対処を取るフローを整え、よりリスクの高い状態に陥る前に対応を取れる準備を整えた。
アラートを受け取ったらある程度調査してみないと、それがどの程度危険なのか、レベル感を判定するのは困難だが、それには相応のスキルと手間が必要だ。FortiDeceptorでは、検知した段階で危ないことがわかるため、必ずしも全員がセキュリティの専門家ではない教育機関の情報システム部門にとって有効なソリューションだと考えた。利用者側に負担をかけることなく、通信そのものをチェックしたり、ブロックすることがない点でも安心だ。
相模女子大学では今後、機密データを扱う職員の端末を中心に、エンドポイントでの検知を行うEDR製品の導入も検討している。「ファイルレス攻撃など、痕跡を残さない高度な攻撃も登場している中で重要な端末を守るため、さまざまな角度から脅威を検知していく仕組みも整備し、引き続き多層防御を追求していきます」（薄氏）

フォーティネットジャパン合同会社
〒106-0032　東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact