学校法人帝京大学

個別最適化の解消と境界型防御からの脱却
学修と医療を支える強固な新情報セキュリティ基盤

社会的なセキュリティリスクの高まりなどを受け、帝京大学は全学的なセキュリティの強化に取り組みました。大きなテーマは、拠点ごとに分散していた個別最適の解消と、境界型防御からの脱却でした。コンサルティングから実際のソリューションの提供まで、シスコは、その取り組みを一貫してサポートしました。

学校法人帝京大学

本部所在地
東京都板橋区加賀 2-11-1

創立
1931 年

学生数
約 2 万 3000 人

「自分流」を教育理念に掲げる帝京大学。約 2 万 3000 人の学生が在籍し、10 学部 31 学科を擁する総合大学です。国内に 5 つのキャンパスを展開し、3 つの附属病院も運営。附属病院を含めた従業員数は約 8000 人に及びます。

課題

- キャンパスや附属病院ごとにセキュリティ対策が個別最適化されている
- 巧妙で亜種も多い最近のサイバー攻撃は境界型防御では防ぐのが難しい
- 異なる施設や立場の人、直接の対策が難しい機器などに対応できるセキュリティが必要

ソリューション

- 自社製品に縛られない客観的なセキュリティコンサルティングを評価
- エンドポイント防御、脅威検知、Web セキュリティなど、対策を網羅的に提供できる
- ソリューションの提供だけでなく SOC 支援も行える

結果

- 巧妙なサイバー攻撃や帝京大学の複雑な状況に対応できる新情報セキュリティ基盤を実現
- SOC 支援によって限られた人員でのセキュリティ運用を効率化
- シスコのコンサルタントやエンジニアの支援で、短期間で導入を完了

今後

- 複数拠点に対して段階的に新情報セキュリティ基盤を導入
- 導入プロジェクトと並行して CSIRT も整備

新情報セキュリティ基盤は
攻撃を迅速に検知し
適切に対処することができます

明石 喜哉（よしや） 氏

帝京大学
本部情報センター
課長

課題

標準化を柱に全学的なセキュリティ強化に取り組む

近年、帝京大学は、学習環境や学修の質の向上、教職員の業務効率化などを目的にデジタル活用に積極的に取り組んでいます。例えば、学生向けでは、履修状況や休講情報などを一元的に確認できる「情報集約」、教員、学生、学生課をつなぐ「コミュニケーション」、そして、学生が自身の学習成果や活動を記録する「自己管理」の 3 つの機能を持つポータルアプリや、学内の様々な質問に 24 時間体制で回答する AI チャットボットを開発して提供しています。

このようなデジタル活用と並行して、同大学は、キャンパスだけでなく附属病院も含む全学的なセキュリティの強化に取り組みました。

まず、重視したのがセキュリティ対策の標準化です。「従来のセキュリティ対策は、キャンパスや附属病院ごと整備しており、個別最適が進んでいました。その状況では、重大な脆弱性情報が公開された際などに、それが帝京大学に影響があるのか、ないのかをすぐに把握することができません。また、仮に一部のキャンパスに影響があることがわかっても、個々の対策を踏まえて影響範囲を把握したり、対処したりするのは時間と工数がかかります。全学的にセキュリティを強化するには、まず標準化を図り、各拠点のセキュリティレベルを均一にしなければなりません」と帝京大学の明石 喜哉氏は話します。

しかし、様々なセキュリティ製品の中から、どれを選択し、どのように組み合わせるのが帝京大学にとって最適かを見極めるのは、非常に難しい課題でした。「セキュリティ製品は、目的ごとに細分化され、同じ分野の製品であっても異なる特徴を持っています。さらに帝京大学には、特有の複雑な状況があります。大学のキャンパスと附属病院という性格の異なる施設がある。キャンパスには、教員、職員、学生と、異なる立場の人が混在している。医療機器や研究のための機器、学生所有のデバイスなど、直接対策を行うのが難しい機器が存在するなどです。私たちだけで、このような状況を整理し、対策を講じていくことはリスクが大きいと感じていました」と明石氏は言います。

客観性と説得力のあるコンサルティング

ソリューション

自社製品に縛られないシスコのコンサルティングを評価

そこで、同大学が考えたのがセキュリティコンサルティングの活用です。専門家の力を借りて、帝京大学のセキュリティ構想や新情報セキュリティ基盤、構築ロードマップを策定していこうと考えたのです。

コンサルタントには、シスコを選択しました。「製品やサービスを提供しているセキュリティベンダーのコンサルティングは、どうしても自社製品に偏る傾向がある。一方、セキュリティの実装を手がけることのない “非製品ベンダー” のコンサルタントの提案は、ともすると机上の空論に陥りやすい。客観性と実現力を備えたコンサルティングを期待して、シスコに依頼しました。シスコは、セキュリティベンダーではありますが、製品を提供するチームとコンサルタントは独立性を保っており、自社製品に縛られないコンサルティングを提供すると約束してくれたからです」と明石氏は話します。

依頼を受けたシスコは、コンサルティングサービス「Cisco Professional Service」を通じて、用語解説や最新の攻撃動向といった基礎的な情報提供から、対策の土台となるセキュリティ規定の原案作成、さらには具体的なセキュリティモデルの提案まで、網羅的なコンサルティングを行いました。「サイバー攻撃がどのように変化し、どのようなリスクが高まっているのか。それに対して、どのようなセキュリティ強化の対策を講じていくべきかをはっきりと認識できました。我々にとっては非常に価値のあるコンサルティングサービスでした」と明石氏は言います。

新情報セキュリティ基盤については、外部ネットワークと学内ネットワークの間にファイアウォールなどのセキュリティ機器を設置し、不正なアクセスや攻撃を防ぐ境界防御ではなく、平常時の挙動と異常を見極め、攻撃の兆候を捕捉す

るふるまい検知を中核に据えた仕組みを提案しました。「巧妙な手法で攻撃を隠蔽し、亜種も多く存在する現在のサイバー攻撃の侵入を完全に防ぐのは困難。したがって、対策の鍵は、いかに迅速に侵入を検知し、適切に対処するかとなる。しかも帝京大学は、エンドポイントでの対策が難しいため、ふるまい検知はデバイス上ではなくネットワーク上で行うなどの工夫が必要。提案されたセキュリティモデルは、大学の環境にあった内容でした」（明石氏）。

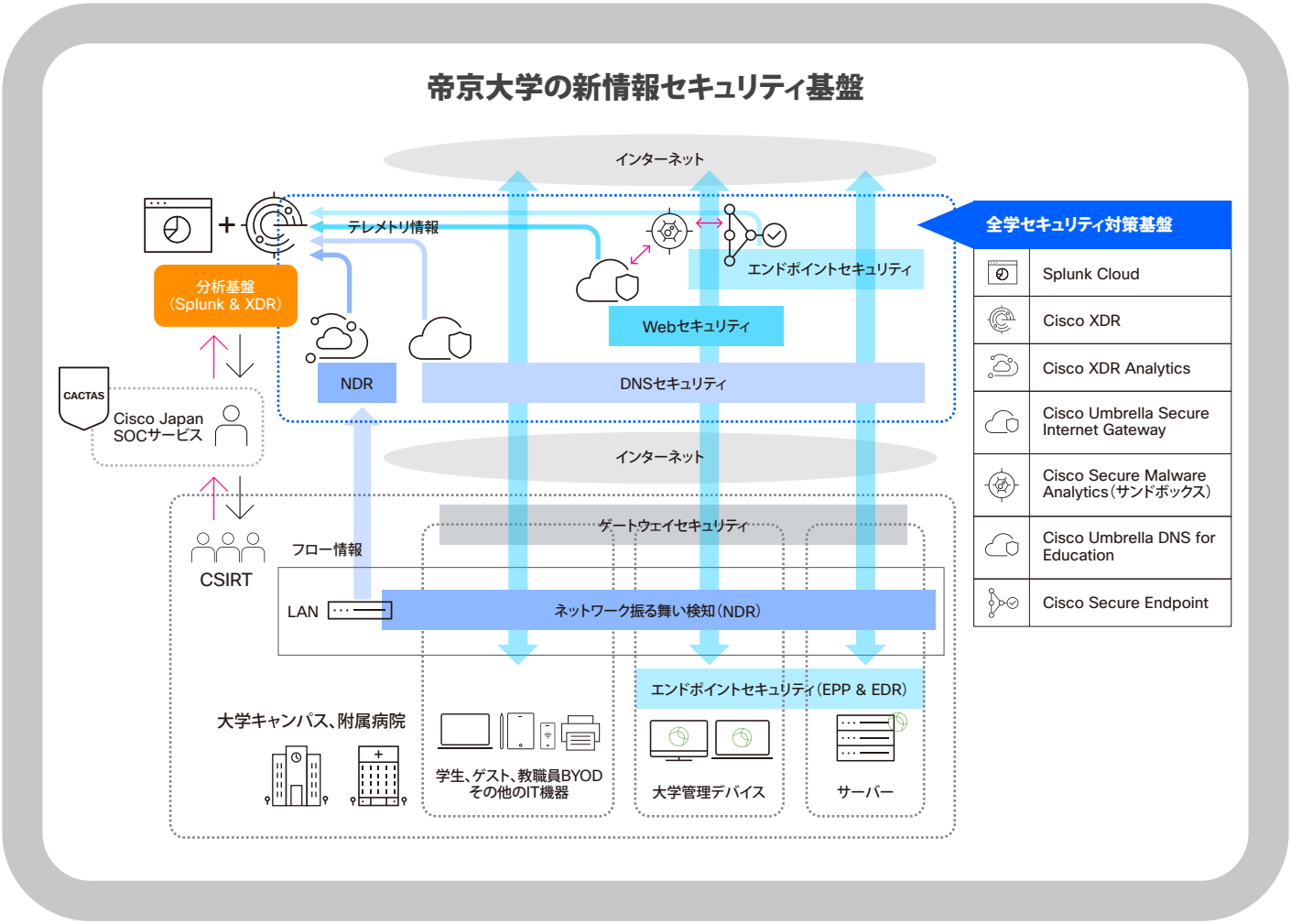
結果～今後

対策の整合性を考えると単一ベンダーが最適

シスコのコンサルティングを踏まえ、帝京大学は実際の導入プロジェクトを開始。フラットな視点で製品の比較と検討を行い、最終的にシスコのソリューションを組み合わせたセキュリティ環境を帝京大学の新情報セキュリティ基盤に決めました。

「『ベスト・オブ・ブリード』の考え方で、領域ごとに異なるベンダーの製品を選ぶこともできます。しかし、刻々と変化するサイバー攻撃に対応するため、セキュリティ製品も進化し続けています。そうした中、導入した製品が、数年後、どのように変化するのかを正確に予測するのは困難です。現時点では整合性が取れていても、ベンダーの考え方の違いによって、5 年後、10 年後には、その整合性が失われ、対策に抜け漏れや穴が生じてしまうかもしれない。そのリスクを避けるため、単一ベンダーで対応可能な組み合わせの中から、価格と機能面を考慮し、シスコの製品を選択しました」と明石氏は言います。

具体的に、帝京大学の新情報セキュリティ基盤は、シスコの以下のソリューションを組み合わせています。



エンドポイント防御と EDR
「Cisco Secure Endpoint」

アンチウイルス、次世代アンチウイルス、EDR（Endpoint Detection and Response）の機能を備えるエンドポイント用のソリューション。脅威防御だけでなく、感染後の検知・対応もできる。

脅威検知と SOC 支援
「Cisco XDR（Extended Detection and Response）」

エンドポイント、ネットワーク、クラウドなど複数のセキュリティ製品から得られる脅威情報を統合。相関分析を行って攻撃を検知する。AI を駆使して、検知の精度を高めたり、検知後の対策を自動化したりして、SOC（Security Operation Center）の運用業務を支援する。

DNS セキュリティ
「Cisco Umbrella DNS for Education」

DNS セキュリティのためのソリューション。Cisco Talos の知見と機械学習による脅威ドメイン分析をもとに、危険なサイトへのアクセスをブロックする。エージェント不要で広範な端末に適用でき、対策が難しい学生の持ち込みデバイスにも有効。教育機関向けの専用ライセンスモデルでコストも最適化できる。

クラウド型包括ゲートウェイ
「Cisco Umbrella Secure Internet Gateway」

SWG（Secure Web Gateway）、CASB（Cloud Access Security Broker）、FWaaS（Firewall as a Service）などの機能を統合した、包括的なクラウド型セキュリティゲートウェイ。ユーザがどこにいても安全なインターネットアクセスを実現する。

ログの集約と分析
「Splunk」

ネットワーク機器、サーバー、アプリケーション、セキュリティ製品など、あらゆるシステムから生成されるログを取り込む SIEM 製品。高速にログの検索・分析を行える。

また、同大学は「Cisco SOC CACTAS（Cisco Advanced Cloud Threat Analytics Service）」によって、24 時間 365 日の監視をシスコに委託しています。「日々の監視はシスコに任せ、緊急度の高いアラートについては報告を受ける体制になっています。私たちの限られた人員で監視を行い、膨大なアラートの中から重大なリスクを選別するのは、現実的ではありません。SOC 支援も併せて提供できることは、シスコソリューションを採用した 1 つの理由です」と明石氏は話します。

段階的な導入と並行して CSIRT も整備

新セキュリティモデルは、ネットワーク機器更改のタイミングと併せて、八王子キャンパスから導入を開始。「シスコのコンサルタントとエンジニアが詳細設計を行い、実際の構築にも参加してくれたことで、短期間でスムーズに導入を終えました。八王子キャンパスのネットワーク機器は、シスコ製品ではありませんが、セキュリティ情報は適切に連携されています」と明石氏は話します。

2024 年度は八王子キャンパスの情報セキュリティ強化を実施しましたが、2025 年度以降、他のキャンパスや附属病院への導入も数年の内に終える計画となっており、計画には CSIRT（Computer Security Incident Response Team）の整備も含まれています。「シスコのコンサルティングを通じて策定した規程やルール、ポリシーが、CSIRT の整備にも活きています」と明石氏は言います。

全学的なセキュリティ強化に向けて大きな一歩を踏み出した帝京大学の取り組みは、教育機関のセキュリティ対策における新たな指針となるはずです。

帝京大学
本部情報センター
課長
明石（よしや） 喜哉 氏

帝京大学
Teikyo University

自分で考え、判断し、行動し、その結果に対して自ら責任を持つ「自分流」が教育理念。教育理論より社会に直結した実学を重視している。現在は10学部31学科11研究科（2専門職大学院）、学生数2万3千人を擁する国内有数の総合大学である。
URL https://www.teikyo-u.ac.jp/

製品 & サービス

- Cisco Professional Service
- Cisco Secure Endpoint
- Cisco XDR
- Cisco Umbrella Secure Internet Gateway
- Cisco Umbrella DNS for Education
- Splunk
- Cisco SOC CACTAS

2510-0-xx