シスコ セキュリティ ソリューション導入事例

国立情報学研究所

国立大学 80 校で共同設立する SOC に次世代ファイアウォールを導入して運用を支援

製品 & サービス

・Cisco Firepower 9000 シリーズ
次世代ファイアウォール

課題

・国立大学 80 校のセキュリティ対策強化の一環として、共同で設立する SOC の運営を専門的な知見を基に支援
・大学でセキュリティ対策に携わる人材が不足しており、その育成が急務

ソリューション

・ファイアウォール製品として、Cisco Firepower 9000 シリーズを導入
・Snort ベースの製品で検知ロジックやシグネチャなど仕組みを理解しやすく、チューニングも行いやすい
・人材の育成にあたり、バランスが良く扱いやすい製品として選択

結果～今後

・SOC の正式運用開始に向けて実地検証を継続
・検知したインシデント情報を基にしたベンチマーク データの作成と提供を予定

国立情報学研究所（NII）は、情報学という新しい分野で未来価値の創成につながる研究を行う日本で唯一の学術総合研究所です。社会貢献や国際貢献に努め、産官学連携などを重視した運営を行っています。大学が共同で利用する機関として最先端の学術情報基盤の整備、学術コンテンツの提供などの事業やサービスも行っており、学術コミュニティに大きく貢献しています。

これからセキュリティ対策に取り組む人たちにとって扱いやすく、検知ロジックやシグネチャの仕組みを理解しやすいバランスのとれた製品として Cisco Firepower 9000 シリーズを導入しました。

―― 国立情報学研究所 サイバーセキュリティ研究開発センター・センター長
アーキテクチャ科学研究系教授 博士（工学） 高倉 弘喜 氏

国立情報学研究所が構築、運用している学術コミュニティ向けの最先端学術情報基盤の 1 つに SINET※ があります。2016 年 4 月からは国内回線および米国向け国際回線を 100 Gbps とした SINET5 の本格運用を開始しています。今後は学術情報の保存や提供にクラウドが活用されることを見越して、全国の大学とクラウド間の接続におけるゲートウェイのセキュリティ対策にも取り組んでいます。

課題

近年、行政機関や企業、大学におけるセキュリティ問題が多く報じられるようになり、全国の大学でもセキュリティ対策の強化は喫緊の課題となっています。一方で、必要とされる設備の導入と運用管理にかかるコストの負担や、実際に起こっている事象の把握や脅威の判定、対処を行える人材の不足という問題も指摘されています。そこで、国立大学 80 校が共同でセキュリティ オペレーション センター（SOC）を設立して、今後のセキュリティ対策強化に向けた取り組みを進めることになりました。国立情報学研究所は、この SOC の運営を支援する役割を担っています。

国立情報学研究所 サイバーセキュリティ研究開発センター・センター長の高倉弘喜氏は、このプロジェクトについて次のように話します。

「実際にセキュリティ インシデントが起こったときに、何をすべきか？ どのような情報を集めるべきか？ ということを各大学の担当者に学んでもらい、今後の対策に携わる人材を育てていくことを目的の 1 つとしています。

※Science Information NETwork（サイネット）

取材：2017 年 3 月
組織名、役職名、記載内容は取材時点のものです。

国立情報学研究所
サイバーセキュリティ研究開発センター・センター長
アーキテクチャ科学研究系教授
博士（工学）
高倉 弘喜 様

まずはこちらで疑わしい兆候をデータとして集めてポータル サイトで公開し、起きている事象を見てもらえるようにします。また、簡単な解析を行って本当に脅威の兆候と判断される場合に、対象となる大学へ通知して対応を促します。80 の国立大学を複数のグループに分けて巡回しながら、全体を俯瞰的に見ていくことで、特定の大学が狙われているのか、すべての国立大学で起きていることなのかを判断できるのは民間の SOC サービスにはない特長です。これは対応を行う大学側にも有益な情報となります。

各大学はここで得られた知識と経験を基に、独自に対策するか、外部の SOC サービスへ委託するのか、それぞれの場合のコストや工数を踏まえて判断してもらえるようになればと思っています。」

このプロジェクトは 5 年計画で、SOC の本番運用は 2017 年 7 月から始まる予定です。モニタリングを行うトラフィックの総量は最大で 200 Gbps を超えますが、そこから不要とする情報を間引いた 80 Gbps ほどが実際の監視対象になると高倉氏は話します。SOC では各社のセキュリティ製品を組み合わせ、テストを行っているところだと言います。

「学術系のネットワークでは一般的な通信とは異なるトラフィックが多いので、カタログ スペックではなく、実際の環境に基づいて検証することが重要になります。現在は設計値の数倍の負荷をかけて、機器の限界や不具合の確認を進めています。」

セキュリティに対応できる人材の育成と大学が安心して研究を続けられる環境づくりを目指しています。

ソリューション

Snort ベースの Cisco Firepower 9000 シリーズを利用

国立情報学研究所では、今回の SOC で利用するファイアウォール機器として Cisco Firepower 9000 シリーズを選択しました。データセンターやサービス プロバイダー向けの最上位モデルとして高いスループットとトラフィック監視性能を備えており、侵入防御（IPS）やマルウェア防御、DDoS 攻撃防御などのセキュリティ対策機能も標準で備えています。モジュールによる拡張が可能でスケーラビリティにも優れており、物理、仮想、クラウドのすべての環境におけるワークロードとデータフローに対して一貫したセキュリティを提供します。

検知エンジンやシグネチャはオープン ソースの Snort をベースにしており、高倉氏はこれが選択の大きな理由だったと話します。

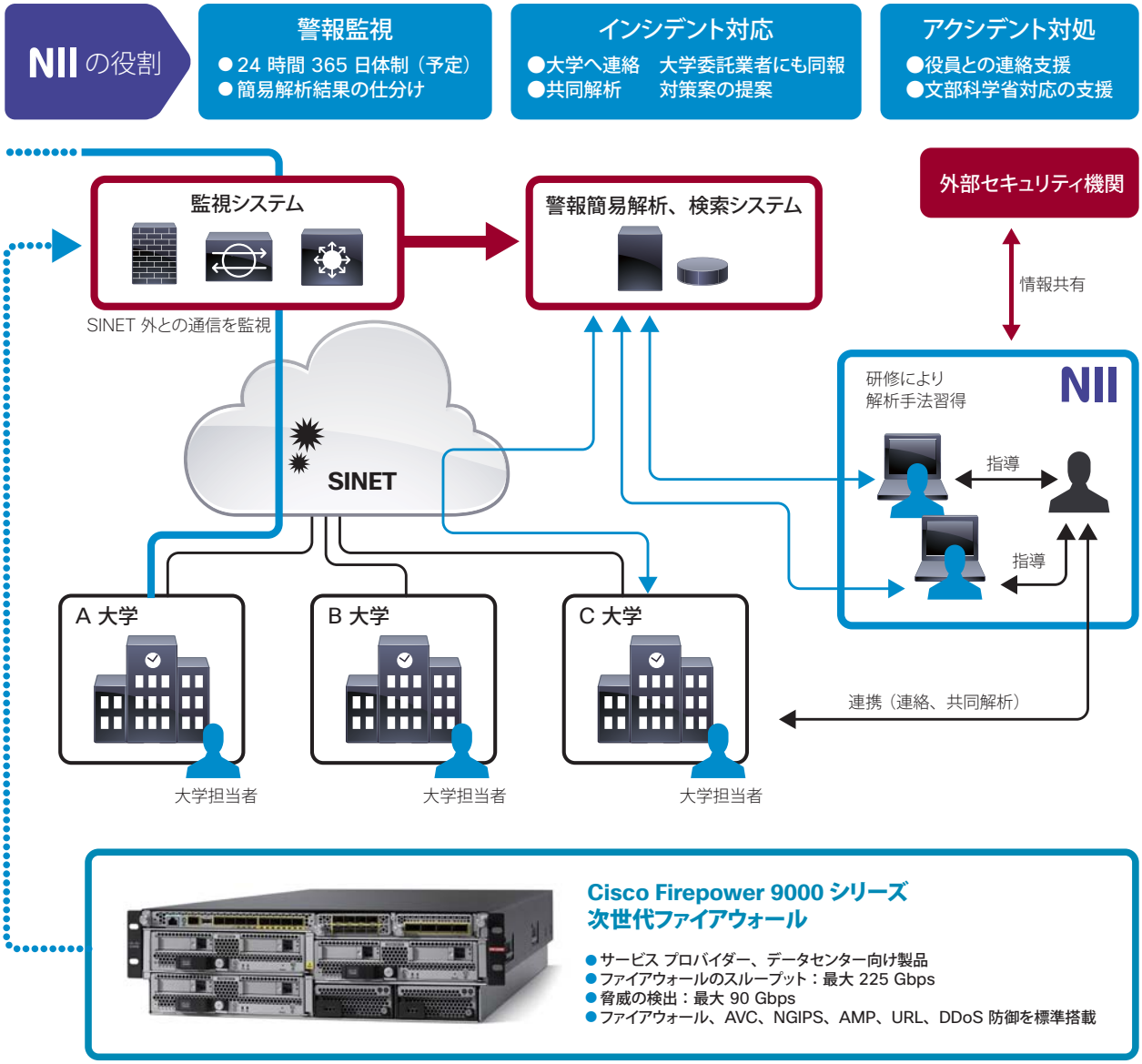
「研究者の多い学術ネットワークでは、ブラック ボックス化されている機器は好まれない傾向があります。たとえば何らかのインシデントが起きていると知らせる場合、その検知の根拠を示せないと相手が納得せず、検知ロジックを教えてほしいという問い合わせがとても多いのです。Cisco Firepower 9000 シリーズは Snort ベースなので、シグネチャ ID の何番を見てください、と伝えることができ、これならたいていの方は納得します。誤検知の場合もありますが、根拠を明確に示して大学側でも詳しい教員などが自分で確認できるのは重要です。また、オープン ソースとして長年扱われてきたものなので、チューニングしやすいことも理由に挙げられます。」

幅広い人が扱いやすいバランスの良さも選択の理由に

高倉氏は、今回の選択は人材の育成というプロジェクトの目的も踏まえたものと話します。

「Snort ベースということで、特にずば抜けた部分はないけれども、逆に劣っている部分もなく、製品としてのバランスを考慮しました。すべてのベンダーの製品を比較検討して、ある特定の機能ではシスコよりも高性能な製品はありますが、人材が不足している今の大学の状況では扱いきれないところがあると判断しました。これから必要な知識と経験を積んでいく人にとって、最もバランスが良い製品がシスコだったということです。将来的にそれぞれの大学がセキュリティ対策に取り組むとき、人的なリソースや予算との兼ね合いから自前で構築と運用を行うケースは相応に出てくると思います。そのときに Snort であれば対応しやすいでしょう。」

国立大学が共同で設置する SOC の運用イメージ



結果～今後

国立情報学研究所では、2017 年 7 月からの正式な SOC 運用開始に向けて、導入したセキュリティ製品の検証を継続し、大学との連携をはじめとする運用体制を整えていくとしています。また、各製品で検知したインシデント情報を基にしたベンチマーク データの作成と提供を月次で行う予定としており、これは 2018 年後半から実施することを目指します。

その他の詳細情報

Cisco Firepower 9000 シリーズの詳細は http://www.cisco.com/c/ja_jp/products/security/firepower-9000-series/index.html を参照してください。

国立情報学研究所

所在地 東京都千代田区一ツ橋 2-1-2
設立 2000 年 4 月
規模 職員数 472 名（平成 29 年 4 月現在）
URL http://www.nii.ac.jp/

大学共同利用機関法人 情報・システム研究機構 国立情報学研究所（NII）は、情報学という新しい学問分野での「未来価値創成」を使命とする国内唯一の学術総合研究所です。情報学における基礎論から人工知能やビッグデータ、IoT、情報セキュリティといった最先端のテーマまでの幅広い分野において、長期的な視点に立つ基礎研究、ならびに、社会課題の解決を目指した実践的な研究を推進しています。また、大学共同利用機関として、学術情報ネットワーク（SINET5）をはじめ、学術コミュニティー全体の研究や教育活動に不可欠な学術情報基盤の構築・運用に取り組むとともに、学術コンテンツやサービスプラットフォームの提供などの事業を展開・発展させています。さらに、事業を通じて得られた知見と学術研究から得られた知見を相互にフィードバックすることにより、実課題に対応した学術研究と、最先端技術を利用した事業を行っています。

お問い合せ

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

1300-1707-000-F