FUJITSU

国立大学法人 山形大学様

学内セキュリティ強化にiNetSec MP2040を活用
～標的型サイバー攻撃やインシデント対応の効率化を実現～

山形大学
Yamagata University

国立大学法人 山形大学様では、情報セキュリティのさらなる強化に向け、富士通が提供するサイバー攻撃検知・SOC 運用効率化アプライアンス「iNetSec MP2040」を導入。
インシデント発生時の初動対応を迅速に行うことで、キャンパス内の安全・安心確保に役立てています。

※ロゴマーク：山形大学様ご提供

課　題

- 効率的に標的型サイバー攻撃への対策を実施したい
- NII-SOCSからの通知を含む多様なインシデントの内容を効率的に把握したい
- 攻撃発生時の影響把握や対処方法の検討などを迅速かつ効率的に行いたい

効　果

- ネットワークの構成変更や工数増大を伴うことなくサイバー攻撃検知を実現
- 独自観点での攻撃解析を行うことで、脅威の重大さをスピーディに判定
- 検知前後の経緯の把握や分析をタイムラインで簡単に判断することが可能に

採用のポイント

・脅威をリアルタイム判定する機能を装備しており、その後の対処に必要な情報が 簡単に確認でき、大幅な効率化や負荷低減が可能
・スイッチのミラーポート接続設置で既存ネットワーク環境の改修は不要

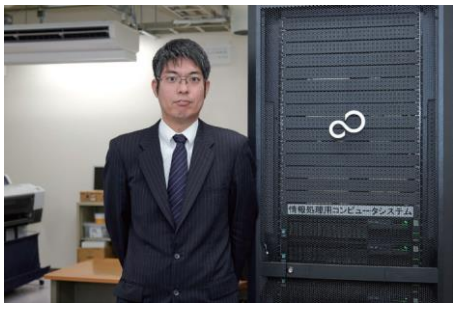
導入の背景

セキュリティインシデント発生時の初動対応をいかに効率化するか

山形市・米沢市・鶴岡市の3地区に、4つのキャンパスを有する山形大学。6つの学部と7つの大学院研究科を備える同大学は、東日本でも有数の規模を誇る総合国立大学です。その同大学において、学内情報基盤の構築・運用を一手に担っているのが情報ネットワークセンターです。同センターでは、先進的なICT環境の実現に向けた様々な取り組みを展開。大学院理工学研究科兼 情報ネットワークセンター 准教授 伊藤 智博氏は「たとえば、柔軟で安定的なネットワーク環境を提供するために、各キャンパスとNII(国立情報学研究所)が提供する学術情報ネットワーク『SINET』を直結。バックアップ回線も別途用意し、完全二重化を実現しています。また、極力コストを抑えつつ最大限のサービスを追求することで、教育研究に振り向けるリソースの最大化を図っています」と話します。

こうした中、大きな課題となっていたのが情報セキュリティのさらなる強化でした。

伊藤氏は「近年では国立大学法人に対しても、セキュリティに対する要請が高まっており、安全・安心な体制を築くことが強く求められています。
もちろん本学でも、独自開発のセキュリティ監視システムなどによる対策を行っていますが、マルウェアや不正な通信などが検知された際には解析を行わなければなりません。
しかも、最近では、NIIのセキュリティ組織『NII-SOCS』からの警報通知も送られてきますので、対応に非常に手間が掛かってしまう。この初動対応を、なんとか効率化できないものかと感じていました」と話します。



導入の理由と選定ポイント

検知能力と使いやすさに優れたiNetSec MP2040を新たに導入

こうした課題を解決すべく、同センターでは様々なセキュリティ製品の情報収集を実施。
そこで目に止まったのが、富士通が提供するサイバー攻撃検知・SOC運用効率化アプライアンス「iNetSec MP2040(以下、MP2040)」です。
MP2040は、ネットワーク通信の内容から攻撃者の行動となる特徴を抽出・追跡し、脅威をリアルタイム判定する機能を装備。
また、攻撃プロセスだけでなく、その後の対処に必要な情報も簡単に確認できるため、セキュリティ運用の大幅な効率化や作業量低減が実現できます。また、スイッチのミラーポートに接続することで設置できるため、既存ネットワーク環境の改修なども不要です。

伊藤氏はMP2040に着目したポイントを「まず一つ目は、シグネチャーなどを使うことなくふるまい検知によって未知の攻撃を検知できる点です。また、これに加えて、ユーザインター

フェースが非常に分かりやすく整理されている点も高く評価しました。
同種の機器の中には多機能を売り物にする製品も見受けられますが、これでは運用コストが逆に嵩んでしまいかねない。何でもできる製品は、結局何もできないということが多いのですね。その点、本学には既に独自開発のセキュリティ監視システムがありますので、これとMP2040を組み合わせることで、インシデント発生時の初動対応に掛かる工数や運用コストを最小限に抑えられるのでは、と感じました」と話します。
その効果を確かめるべく、同センターではMP2040の実機を用いたPoC(概念実証)を実施。既存セキュリティ監視システムとの連携が期待通りに行えること、米沢キャンパスに設置したMP2040で全キャンパスの通信を一元的に監視できることなどをしっかりと検証で確認しました。ここでは富士通とPFUの支援も大いに活用されました。

さらに、もう一つ大きな決め手となったのが、導入コストのリーズナブルさです。4キャンパス分のトラフィックの総量は約2.5Gbpsに上るが、これに対応できるだけの性能を備えたIPS/IDS装置などを導入するとなると、膨大な費用が掛かってしまいます。その点、MP2040なら、多大なコスト負担を抱え込む心配もないため、その結果MP2040の採用が決定しました。

導入の効果

4つのキャンパスを1台で監視
脅威のレベルに応じた対処が可能に

今回導入されたMP2040は、2018年秋より本番稼働を開始。オプションの「Webレピュテーション機能」も利用されています。システム構築面の工夫としては、先にも触れた通り米沢キャンパスに設置した1台のMP2040で、全キャンパスの通信を監視している点が挙げられます。まさに同センターが掲げる「最小限の投資で最大限のサービス」を具現化した格好です。

伊藤　智博 氏
国立大学法人　山形大学
大学院理工学研究科
兼 情報ネットワークセンター
准教授

「工学部がある米沢キャンパスの通信量が一番多いので、ここに他キャンパスのミラーパケットを転送して一元監視するのが最も効率的と考えました。各キャンパスに個別に機器を置かなくとも済むのは非常にありがたかったですね。MP2040の情報については、山形／飯田／鶴岡キャンパスの情報ネットワークセンターでも見られるようにしていますので、それぞれの実情に合わせて活用してもらっています」と伊藤氏は話します。

最大の懸案であったセキュリティ運用の効率化についても、大きな改善効果が期待されているとのこと。

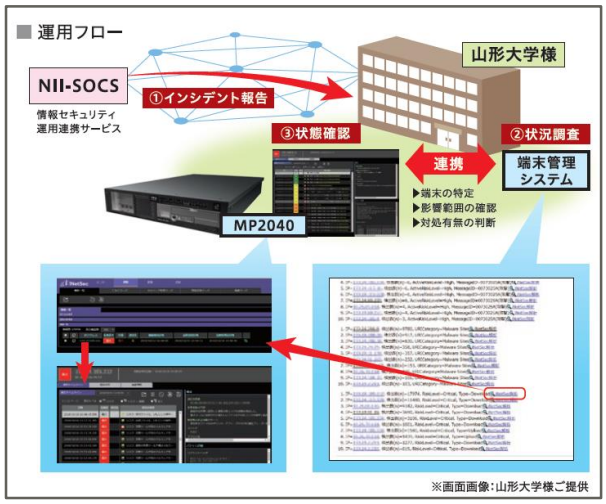
「インシデントが確認された場合には、まず本学のセキュリティ監視システムで該当IPアドレスの特定を行いますが、その後の対応が格段に効率化できると考えています。該当IPアドレスの時系列情報をMP2040のタイムライン画面でチェックすれば、ログ解析などの対処が即座に必要な状況なのか、それともそうでないのかといったことをスピーディに判断できます。全ての通知に対して毎回最高レベルの対応を行ったのでは運用側も疲弊してしまいますが、状況が正確に掴めればそうした負担も減らせます」と伊藤氏は話します。

同様にNII-SOCSからの通知に対しても、MP2040の情報と突き合わせることで、脅威のレベルに応じた対処が可能になります。従来は通知を受けて対応を行ったものの、結局マルウェア感染や不正ダウンロードの痕跡などが見つからないケースも多い状況でした。こうしたものについても、今後はMP2040で脅威が検知されなければ、緊急対応の必要性は薄いと判断できます。

加えて、もう一つ見逃せないのが、MP2040を学生へのセキュリティ教育にも活用している点です。「MP2040が収集した情報は、まさに本学で今起きている生のセキュリティ教材とも言えます。これを元に改善に向けた議論などを行うことで、今後のセキュリティ人材の育成にも役立てていければ」と伊藤氏は話します。

同センターでは今回導入したMP2040を、学内の安全・安心確保やセキュリティ運用の効率化に役立てていく考えです。「AI技術の活用など、今後のMP2040の進化にも大いに期待しています」と伊藤氏は語ります。

（2018年12月1日現在）



国立大学法人 山形大学概要


旧米沢高等工業学校本館（現・工学部資料館）
※画像：山形大学様ご提供

■ 所在地
・米沢キャンパス
〒990-8560　山形県米沢市城南 4-3-16
■ 学　長：小山 清人氏
■ 設　立：1949（昭和24）年 5月
■ 学部・学科：6学部 7大学院研究科
■ ＵＲＬ：https://www.yamagata-u.ac.jp/

大学概要
約1万人の学生が学ぶ総合大学。2017年度からは、基盤共通教育と基盤専門教育を連動させた3年一貫の基盤教育プログラムをスタート。幅広い教養教育と学習技能・知識・能力の習得、並びに社会で力強く生きるための「人間力」の育成を目指しております。

標的型サイバー攻撃への対応と SOC運用の効率化に貢献


iNetSec MP2040

情報セキュリティの確保は全ての企業・団体にとって共通の課題ですが、その運用に多くの負担を強いられるケースも少なくありません。
富士通が提供する「iNetSec MP2040」は、「攻撃者行動遷移モデル」を用いて、攻撃者の行動プロセスを時系列で見える化。
攻撃の全容を的確に把握することで、迅速かつ効率的なセキュリティ運用を実現します。

製品・サービスについてのお問い合わせは
富士通コンタクトライン（総合窓口）　0120-933-200
受付時間 9:00～17:30(土・日・祝日・年末年始を除く)
富士通株式会社　〒105-7123　東京都港区東新橋1-5-2　汐留シティセンター