学校法人北里研究所／北里大学 様

Deep Discovery Inspector（DDI）で事務系ネットワークを防御
CEC SOCで24時間365日の監視・運用体制を実現

CEC
Computer Engineering & Consulting

CEC SOC® マネージドフラットDDI

導入事例

北里大学情報基盤センター
管理運用課 係長 有井 宏敏氏

「もっとも重要な事務系ネットワークに対し、Deep Discovery Inspector（DDI）とCEC SOCで強固なセキュリティを築きました」

課 題

- 標的型脅威に対するセキュリティ対策が不十分
- セキュリティ製品を監視・運用するリソースが不足している
- 新たなセキュリティ製品を導入する予算が限られている

効 果

- 入口／出口対策、内部対策、サンドボックスを搭載したDDIで脅威を検知
- CEC SOCがDDIを24時間365日体制で監視・運用
- 月々定額のマネージドサービスで導入

導入の背景・課題

北里大学情報基盤センターの役割

北里大学情報基盤センターは企業でいう情報システム部門にあたり、全学全法人的な事務系システムやメールシステム、そしてネットワークおよびセキュリティの運用・保守を管轄している。

同センターの発足は2000年で、発足以前はそれぞれの学部でシステムやネットワークを構築していたため、今でも一部は学部に運用・保守を任せている。徐々に直接管轄する領域が増えた現在は、病院を除く全学全法人のインフラ基盤状況は把握済みだ。

同センターがセキュリティ対策としてトレンドマイクロ社のDDIに着目したのが3年前の2017年。「当時、内部の端末に潜伏し次々と別の端末に拡散、最終的にはサーバーに到達してデータを搾取していく脅威が問題になっていました。実際、大きな被害を被った企業もあったようです。当学はそのとき、一般的なファイアウォールを導入したばかり。次世代型ファイアウォールではなかったため、脅威の検知はもちろん、IDS（不正侵入検知システム）やIPS（不正侵入防止システム）、アプリケーションの制御などのセキュリティ対策機能は備わっていません。脅威の振る舞いを検知し防御できるセキュリティ製品を探していたところ、入口／出口対策、内部対策、サンドボックスなどの機能を装備したDDIにたどり着きました。」と北里大学情報基盤センター 管理運用課 係長 有井 宏敏氏は語る。

事務系ネットワークにDDIを導入

同センターではDDIの実機を借りてPoCを実施。DDIのセキュリティ能力については高い評価を下したが、2つの理由で導入は先送りになった。1つは実行ファイル形式の脅威が大半だったこと。「実行ファイル形式なら、迷惑メールフィルターで拒否設定にすれば防御できます。」（有井氏）

2つ目は、セキュリティポリシーの刷新が優先されたことだ。「まず、どこに守るべき情報資産があるのか棚卸をする必要があります。そのうえで情報資産の格付け基準を明確にし、新たなセキュリティポリシーを策定したうえで、どういうセキュリティ対策をとっていくのがベストか議論しなければなりません。DDIを見当違いなところに入れても意味はありませんから、まずは新しいセキュリティポリシーの策定を優先しました。」（有井氏）

ところが、情報資産の棚卸は遅々として進まず、セキュリティポリシーの策定に着手できない状況が続いた。実は情報資産の棚卸は同センターだけでは推進できない。業務を主幹している部門の協力を得る必要がある。「情報資産の棚卸が完了するのを待っていたら、いつになるか分かりません。とりあえず、情報資産の格付けで最上位に値する学生の個人情報、成績情報、教職員の個人情報などが保管されている事務系ネットワークは、セキュリティポリシーの新旧を問わず、セキュリティを強化する必要があります。そこで、まずは事務系ネットワークにDDIの導入を決めました。」（有井氏）

学校法人北里研究所／北里大学 様

Deep Discovery Inspector（DDI）で事務系ネットワークを防御
CEC SOCで24時間365日の監視・運用体制を実現

CEC Computer Engineering & Consulting

CEC SOC® マネージドフラットDDI

導入事例

DDIとCEC SOCの導入効果

シーイーシーを選定した決め手

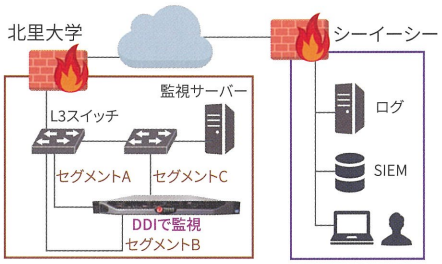
事務系ネットワークにDDIを導入したのは2019年の7月。導入に携わったのは、トレンドマイクロ社から紹介されたシーイーシーだった。同センターがシーイーシーをベンダーとして選定したのは以下の理由からだ。

＜トレンドマイクロ社との実績＞

シーイーシーは2003年からトレンドマイクロ社のセキュリティコンサルティングサービスを提供。2010年には、トレンドマイクロ社と共同でエンタープライズセキュリティサービスの提供も開始している。シーイーシーはトレンドマイクロ社のゴールドパートナーであり、パートナーアワード特別賞を受賞している点も評価し、トレンドマイクロ製品に深い知見があると判断した。

＜CEC SOCの存在＞

DDIを導入しても、同センターだけでネットワークのインシデントを監視し、運用を続けていくにはリソースに不安がある。そこで、同センターがシーイーシーの提案で注目したのがCEC SOC（セキュリティオペレーションセンター）。セキュリティに関するログやイベント情報から標的型サイバー攻撃につながる脅威を24時間365日体制で検知・対処するCEC SOCに、DDIの運用支援・監視・セキュリティ診断を委ねることにした。



DDIを監視するCEC SOCの概要図

＜導入の敷居を下げたマネージドサービス＞

DDIの導入およびCEC SOCを利用するうえでコストがネックになると思われたが、シーイーシーから提示されたのは月々定額のマネージドサービス。いわゆるサブスクリプションで初期費用もかからない。月々固定費用で利用できるため、導入の敷居は大きく下がった。

DDI導入によってインシデントの可視化を実現

DDIの導入後、高レベルのカテゴリーに分類されるような検知はいくつかあったものの、とくに大きなインシデントはない。「以前も大きなインシデントはなかったと思いますが、確証はありませんでした。しかし、DDIを導入してからはネットワークの状況が可視化され、大きなインシデントがないことが目に見える形で判明しました。大事なのは脅威の有無ではなく、可視化という安心感です。」（有井氏）

CEC SOCにも高い評価

CEC SOCはDDIを24時間365日体制で監視し続け、その結果をレポートにして月に一回提出している。「我々が手探りだったこともあって、初めの3カ月は『アドウェアや不要ソフトといったものを検知しました』『脅威に相当するメールを受信しているユーザーがいるので注意してください』など、詳しく教えていただきました。こうした運用は我々だけではできなかったと感じていますので、かなり助かりました。」（有井氏）

今後の展開と期待

重要な部分へのセキュリティ対策は早急に実施すべき

同センターは事務系ネットワークでセキュリティ対策は終わりとは思っていない。新しいセキュリティポリシーをリリースできれば、優先順位の高いところから順にDDIなどのセキュリティ対策を施していく予定だ。「残念ながらポリシー設定はまだまだ時間がかかりそうです。ただ、当学に限らず、重要な部分に対して何もしないのは問題です。兆候がないから何も起きていないとは言い切れません。すでに潜伏している、もしくはバックドアをつくられて検知できないだけかもしれません。DDIはそういう見えないところを可視化し防御するための安心材料としておすすめです。」（有井氏）

シーイーシーに対しても、有井氏は高い期待を持っている。「すでに大まかな当学のネットワーク構成は把握されていると思いますので、シーイーシーが考える防御すべき場所や気づきがあれば、ぜひ積極的にご指南いただきたいですね。また、セキュリティのトレンドや最新のセキュリティ関係サービスなど、さまざまな情報の提供も期待しています。」（有井氏）

お客様プロフィール

学校法人北里研究所／北里大学 様

社団法人北里研究所と学校法人北里学園が統合し学校法人北里研究所が発足。学校法人北里研究所を構成する部門のひとつ北里大学は、1962年に北里研究所創立50周年を記念して創設。北里柴三郎博士が顕現した「開拓」「報恩」「叡智と実践」「不撓不屈」を建学の精神としており、「実学」を通して社会に貢献している。教育・研究の特徴は医療系学部・併設校と4病院連携によるチーム医療教育、食・環境・健康をテーマとする農医連携教育・研究、北里研究所創立当初からの歴史を持つ感染制御教育・研究、知財を活用した医工連携教育・研究、さらには我が国の東洋医学の中核的な役割を担ってきた東洋医学教育・研究など。社会からの要請として、国際化、内部質保証体制の確立などにも、積極的に取り組んでいる。

学校法人 北里研究所 THE KITASATO INSTITUTE

法人本部所在地	〒108-8641 東京都港区白金五丁目9番1号
代表者	理事長　小林 弘祐
学生数（北里大学）	9,524名（在籍者）
学部（北里大学）	薬学部、獣医学部、医学部、海洋生命科学部、看護学部、理学部、医療衛生学部、一般教育部
URL	法人サイト https://www.kitasato.ac.jp/ 大学サイト https://www.kitasato-u.ac.jp/

お問い合わせ

CEC 株式会社シーイーシー
Computer Engineering & Consulting

〒150-0022　東京都渋谷区恵比寿南1-5-5　JR恵比寿ビル
TEL：03-5789-2442 FAX：03-5789-2585
Email：marketing@cec-ltd.co.jp
URL：https://www.cec-ltd.co.jp/

販売代理店

202003-003-006CI