学習院大学 様

ともに成長していけるSOCとして、シーイーシーをパートナーに。
1万台を超える端末が接続するネットワークをCEC SOCが監視。

CEC
Computer Engineering & Consulting

CEC SOC®

導入事例

写真提供 学校法人 学習院

導入ポイント 導入効果

1. マルチベンダー対応で複数の機器を監視できる
2. 運用サービスの選択はスタート後でもOK
3. 相談しながら一緒に成長していくSOC

導入の背景と狙い

学習院の大部分のITを管轄する計算機センター

学習院大学 計算機センター（以下、計算機センター）は、一般企業でいうところの情報システム部門。計算機センターは大学だけではなく、財務会計や人事といった事務システムを除いた幼稚園から大学まで学校法人学習院全体（以下､学習院）の90%以上のITを管轄している。守備範囲は、情報管理はもちろん、サーバーやネットワークといったインフラの構築から運用・保守までと幅広い。それだけに、計算機センターのスタッフは一般企業と同等以上の高度なITリテラシーを有している。

ネットワークには1万台を超える端末が接続

その計算機センターが管理する端末は膨大だ。「我々が直接管理する端末は約3,600台。教員が校費によって自前で設置する端末を入れると約5,000台がネットワークに接続しています」と語るのは計算機センターの城所 弘泰氏。

そのほか、学生たちが持っているスマートフォンなどは、Wi-Fi経由で学習院のネットワークに接続し、インターネットにアクセスできる。「2018年の6月から9月24日まで、1回でも本院のWi-Fiにアクセスしたことがある端末は6,000台以上。この数字は校内5,000台の端末とは別です」と計算機センターの村上 登志男氏は語る。

計1万台を超える端末がアクセスするだけに、学習院のネットワークはセキュリティ対策が強固だ。複数のセキュリティ製品による監視、フィルタリング、メールの添付ファイルなどを検証するサンドボックス機能など､何重にも防御がなされている。

「本院のネットワークは、怪しい動き、不正な通信を高い確率で検出できます。例えば、本院以外の場所でインストールしたアプリが実はマルウェアだったということが、本院のセキュリティに引っ掛かって分かるケースが珍しくありません。そんなときは、感染している端末を持つものが、学生であれば呼び出して告知しますし、教員であれば連絡を取り対処を行います」と計算機センターの磯上 貞雄氏は語る。

監視精度の低下が避けられない人的リソース不足

こうした検出率の高さは、計算機センターがセキュリティ製品のログを厳しく監視しているからに他ならない。だからこそ、浮かび上がってくるのは人的リソース不足という課題。「我々はセキュリティだけでなく、サーバーの運用・保守はもちろん、ネットワークにつながっている機器すべてを管理しなければなりません。例えば、本院のどこかで通信ができないという問い合わせがきた場合、一次受付のヘルプデスクで解決できれば良いのですが、解決できないとなると我々が見に行って調査と対応まで行います。こうした数多くの業務を踏まえると、セキュリティに必要なものは一通り導入して対策しているとはいえ、我々だけですべて監視するのは不可能に近いといえます」（城所氏）

そこで計算機センターでは、人的リソース問題の解決と監視を強化するため、以前からSOC（Security Operation Center）の導入を思案していた。「本院の監視業務は規模が大きいだけに大変。我々も厳しく見てはいますが、怪しい動きを見逃す可能性がゼロではありません。ですから、外から監視するSOCを導入して2つの視点で見ていれば、見逃す可能性は大きく低下するだろうと考えました」（村上氏）

導入の決め手と効果

スタート後に運用・コストの取捨選択ができる

2018年4月、全システムのリプレースを機に計算機センターはSOC導入を決断。今回のリプレースに関わっている複数のベンダーに対し、RFIの形でSOC導入を明記した。SOC導入に手を上げたのは5社。そのなかの1社にシーイーシーも含まれていた。

「当初、どのベンダーからも松竹梅のような提案がありました。つまり、梅なら監視はここまで、レポートは随時、それ以上を望む場合は松といった具合です。5社横並びの提案ではありませんが、選定は難しいと感じました。そこで我々は次の2点でベンダーを絞ることにしました」（城所氏）

学習院大学 様

ともに成長していけるSOCとして、シーイーシーをパートナーに。
1万台を超える端末が接続するネットワークをCEC SOCが監視。

CEC SOC®

CEC Computer Engineering & Consulting

導入事例

<マルチベンダーへの対応>

導入している複数のセキュリティ製品を監視できるベンダーを要件とした。「監視できるセキュリティ製品が限定されてしまうと身動きが取れません。そこで、さまざまなセキュリティ製品の監視について、積極的に取り組んでいただけるベンダーのみとさせていただきました」（村上氏）

<スタート後に運用サービスを柔軟に変更できる>

もっとも頭を悩ませたのは、計算機センター自身がSOCに何を依頼すべきか分からないことだ。SOC導入が初めてだったため、サービス内容とコストを判断することができない。

「もちろん、希望すればどのベンダーも対応してくれるのは分かっています。ただ、我々としては、分からないことだらけのまま、運用サービスをガチガチに決めることはできません。運用・コストありきで『決めてくれないとスタートできない』というベンダーは選択肢から外させてもらいました。我々としては、運用をスタートしてからの対応が大事。『スタート後に運用・コストを柔軟に変更できる』そういったわがままを聞いてもらえるベンダーを探していました」（磯上氏）

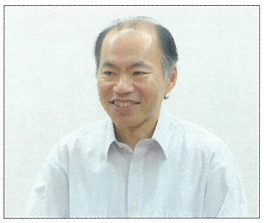
最初にすべて決めるのではなく、運用してから次のステップへ進めるベンダー、学習院に合ったセキュリティ対策を一緒に考えていくことができるベンダー、それがシーイーシーだった。

CEC SOCは2つのセキュリティ製品を監視

計算機センターでは、リプレース全体の把握に追われているため、導入したCEC SOCとの綿密な連携は構築の途中だ。そもそもリプレースではネットワーク、セキュリティ製品、3,600台の端末に至るまで、ほぼすべての機器を更新もしくは新機種にアップデート。つまり、計算機センターも機器の特性を理解している最中で、セキュリティ製品も同様に機器の振る舞いを理解するまで時間を要している。

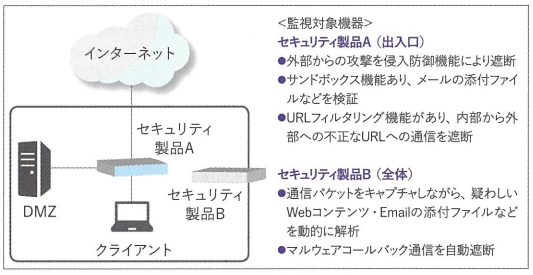
そのような状況のなか、CEC SOCは出入口のセキュリティ製品と広範囲のネットワークをカバーするセキュリティ製品の2つを監視している。「相関的に監視することで、精度の高い監視が可能になると思っています。CEC SOCはSIEM（シーム）を使った統合ログ管理・仕分けも行っているとのことで、レポートにも期待しています」（城所氏）

学習院大学 計算機センター
村上 登志男氏



学習院大学 計算機センター
城所 弘泰氏

学習院大学 計算機センター
磯上 貞雄氏



今後の活用と展望

期待するのは一緒に成長するSOC

「現在は本院の環境に出やすいイベントへの対策を探っており、ようやく傾向が見えてきました。ただ、毎月同じではなく、イベントは変わっていくので常に相談はしています。お互いが良いパートナーシップをどうしたら築けるかを考えながら、少しずつ進歩していると思っています」（村上氏）

今後は2つのセキュリティ製品だけでなく、他のセキュリティ製品も監視してほしいというのが計算機センターの本音。そのためにはコストを考慮しつつ、共通認識の精度を高めていかなければならない。ただ、こうしたスタイルの運用を実現できているのは、柔軟に対応できるCEC SOCだからというのは計算機センターも認めている。

「キックオフから100%にするには、ガチガチに決めてスタートした方が良いはず。しかし、本院は一緒に歩んで最終的に100%になれば良いと思っています。そういう意味でいえば、CEC SOCは理想的な運用方法かもしれません」（磯上氏）

計算機センターはCEC SOCに対して、一緒に成長していくことを期待している。

お客様プロフィール

1847年、公家の教育機関として京都御所に設置された学問所が学習院の始まり。1877年には、かつて京都にあった学習院の名を継承した華族学校が神田錦町に開設され、現在の学習院はこのときを創立としています。現在の学習院大学は5学部17学科、大学院6研究科、専門職大学院（法科大学院）が目白のワンキャンパスに集い、充実した教育環境を提供。「ひろい視野 たくましい創造力 ゆたかな感受性」という教育目標のもと、自ら課題を発見し、その解決に必要な方策を提案・遂行する力を十分に身につけた人材を学習院大学は育成し続けています。

学習院大学 GAKUSHUIN UNIVERSITY

- 所在地　東京都豊島区目白1-5-1
- 教員数　1,088人
- 学生人数　9,613人
- URL　http://www.univ.gakushuin.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/

CEC SOC® https://security.cec-ltd.co.jp/soc/ cec soc 検索

販売代理店

201811-002-083CW