賛助会員だより

フォーティネットジャパン株式会社

BYODの推進に伴う「ゼロトラスト」ネットワークアクセスをFortiNACによる可視化とネットワークセキュリティの強化で実現
～国立大学法人　北海道大学への導入～

導入・構築のポイント

- BYODの推進に伴い、エージェントレスのFortiNACでゼロトラストネットワークの考え方を実現
- ICカードによるユーザー認証に加えて、デバイスの種類やセキュリティ対策状況を可視化
- 既存セキュリティ機器との連携で、インシデント発生時の初動を自動化
- ディレクトリサーバとの連携で、手作業に頼らざるを得なかった利用者およびデバイスの特定を効率化

北海道大学は、フロンティア精神を掲げた札幌農学校の設立から数えて創基150周年を見据えた近未来戦略を立て、学習管理システム（Learning Management System：LMS）を活用したオンライン学習をはじめ、ICTを活用した教育を大規模に導入しつつある。情報環境推進本部と情報基盤センターが連携してアカデミッククラウドやシングルサインオン環境の整備といった基盤を担う一方、オープン教育リソース（OER）を活用した教育面はオープンエデュケーションセンターが推進してきた。

この体制の下で北海道大学は、教育用計算システムの更新を定期的に実施してきた。５年前のシステム更新時には、大学内の無線LAN環境を整備し、それ以前はキャンパス内の限られた場所に数十台程度であった無線LANアクセスポイントをキャンパス全体に拡充し430台以上に増強した。新入生は学部別に進路が分かれる前に「全学教育」を受けるが、それを実施する高等教育推進機構の建屋を中心に無線LAN環境を整備し、大学側が用意する端末だけでなく、学生や教員が個人の端末（BYOD）を持ち込んで円滑に学習を進められるようにした。

「学生が自分の端末を持ち込み、教員と学生、学生同士がコラボレーションしたり、インタラクティブに学べるアクティブラーニング環境を通した教育の高度化を目的に、BYODを推進してきました」（北海道大学　情報基盤センター准教授・高等教育推進機構オープンエデュケーションセンター副センター長、重田勝介氏）。学生証や職員証をICカード化し、自分のIDで認証を行えばどこからでもLMSにアクセスし、オンライン学習を行える環境も整備してきた。

■パーソナライズされた学習を目的に無線LAN環境を整備しBYODを広く導入

2020年３月に更新した新教育用計算システムは、米国のIT教育推進団体が提唱する「Next Generation Digital Learning Environment」（NGDLE）という考え方に基づいて構築されている。

「新システムの目的の１つが、BYODやオープン教育リソースの活用による多様な個別学習に向けたパーソナライズド学習への対応です。このため全学的にBYODに対応した無線LANネットワークを整備して高い通信品質を実現するだけでなく、セキュリティの側面からも質の高いものを用意する必要がありました」（重田氏）

北海道大学ではそれ以前から複数の境界型セキュリティを実装する他、ICカードを組み合わせた強固な本人認証を行ってきた。だがBYODの普及に伴って、根本的に考え方を変える必要性を感じたという。

「北海道大学内のネットワークには学生や教員が持ち込むデバイスが月に約３万台接続されていますが、端末レベルでは制限していません。パッチの当たってないOSや古いOSを搭載したPC、タブレット端末やスマートフォンでも、与えられたIDとパスワードを入力すればネットワークが使えます。そういった古い端末が学内ネットワークのセキュリティホールになるのではないかという懸念がありました」（重田氏）

グローバル化も柱の１つとする北海道大学には多くの留学生が在籍するが、海外からの学生が持ち込む端末に不正なソフトウェアが潜んでいるリスクも考えなくてはならなかった。端末にウイルス対策ソフトウェアを導入できる環境も整えていたが、私物であるBYODの端末すべてにインストールを強制するわけにもいかず、セキュリティレベルを一律に維持するのは難しかったという。

■「学内の端末は信頼できる」という前提は通用しない、ゼロトラストへの転換を

BYODを推進する中、「学内にいる端末はすべて信頼できる」という前提には問題があるのではないか。ゼロトラストの考え方を取り入れる必要があるのではないか――それが、フォーティネットのFortiNAC導入に至る大きなきっかけだった。

しかも、サイバーセキュリティに対する関心は以前とは比較にならないほど高まっており、大学に向けられる目は厳しさを増している。「大学全体のセキュリティレベルを下げるようなことにならないよう、接続端末を監視しておかなければならないという問題意識がありました」と重田氏は述べた。

こうして、新教育用計算システムの一環として、端末のセキュリティレベルを把握できる仕組みを検討した結果、採用したのがFortiNACだった。端末個々にエージェントを導入する必要がなく、ネットワーク側でBYODの可視化と制御が行えることがポイントだった。

■FortiNACで端末の状況を可視化し、ユーザー特定までの時間と手間を大幅削減

北海道大学では2019年夏からFortiNACの導入を進め、本格運用の前にPoCを実施。するとやはり、古いOSを搭載したPCやタブレット端末が多数あることが判明した。「FortiNACによって、モニターのレベルが上がり、内容も充実しました。トラフィックだけでなく、OSの種類や端末がどういう状況にあるのかといった事柄を可視化し、把握できるようになりました」と重田氏は評価する。

もう１つの大きなメリットは、リスクのある端末の特定を、負荷をかけずにスピーディに行えるようになったことだ。インシデント防止には適切な指導をし、脅威の芽が小さいうちに摘み取ることが重要だが、以前は利用者特定までの所要時間の短縮が課題となっていた。

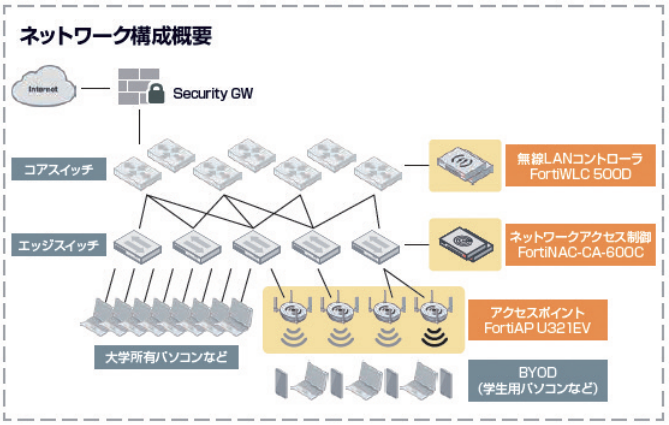
「これまでは何か問題を検知すると、まず端末のIPアドレスを調べてログと照らし合わせ、その時に使っていた学生のIDを調べて利用者を特定していました。情報系の担当者と教育系の担当者が電話でやりとりしながら調査するため、特定までにかなりの時間を要していました。FortiNACと認証サーバのLDAPが連携することによって、どのユーザーが疑わしいか即座にわかるようになりましたし、どちらの担当者の負担も軽減されました」（重田氏）

折悪しく、新型コロナウイルス（COVID-19）の拡大にともない、北海道大学はキャンパスを閉鎖し、LMSを活用したオンライン授業を展開している。「今後はその延長で、BYODでつながる端末はさらに増えてくると予想しています。その時に端末のセキュリティ状況を把握し、パッチが当たっていない場合は何らかの対応を学生に求めるといったことが、FortiNACを活用して容易にできると期待しています」と重田氏は述べる。他にも、授業には無関係なゲーム機などの端末を検出したり、トラフィックや通信状況をモニタリングして無線LANアクセスポイントの適正配置や再調整につなげるなど、さまざまな可能性に期待しているという。

北海道という土地は多様な人々を受け入れてきた。北海道大学も同様だ。「学会に参加したり、研究生として半年だけ滞在したりといった具合に、大学とは常に人が入っては出ていく場所であり、それが良いところでもあります。だとすれば、そこに持ち込まれる端末をガチガチに縛ることはできないでしょう。大学という場所に応じたネットワークセキュリティレベルの確保の仕方を考えると、ゼロトラストネットワークの考え方が非常に有効だと思います」（重田氏）

FortiNACを利用してそのコンセプトを実現した北海道大学では、今後もインシデントを防ぎつつ、多くのユーザーが安全かつ快適に利用できるネットワーク環境を実現していく。

（本文は、2020年５月に取材した内容をもとに作成しています。）



北海道大学
情報基盤センター准教授
高等教育推進機構オープンエデュケーションセンター副センター長
重田　勝介氏

問い合わせ先

フォーティネットジャパン株式会社
パブリックソリューションビジネス本部
E-mail：universities_jp@fortinet.com
URL：https://www.fortinet.com/jp