



宮崎大学

～ セキュリティソリューション ～

キャンパスネットワークの内部対策に 「iNetSec Intra Wall」が貢献

国立大学法人 宮崎大学様



宮崎県の中核教育研究機関である国立大学法人 宮崎大学では、PFUのネットワークセキュリティ製品「iNetSec Intra Wall」による内部対策システムを新たに構築した。キャンパスネットワーク内部に侵入した脅威の活動を迅速にキャッチすると同時に、マルウェア感染端末や禁止アプリケーション利用端末の通信を速やかに遮断することで被害の拡大を未然に抑止。また、ネットワークを利用する各種端末の見える化により、インシデント管理の効率化に役立てている。

キャンパスネットワークの 内部対策が大きな課題に

「地域と共に興す『新たに光る宮崎ブランド』の確立と発信」「異分野融合を軸に『地の利、人の利』を活かした教育研究等の推進」の二つの柱を軸とする「宮崎大学未来Vision」の下、次世代を担うグローバル人材の育成や先端学術研究に取り組む宮崎大学。地域社会の活性化を支える重要拠点としても、大きな役割を果たし続けている。

また、同大学では、学内情報セキュリティの強化に向けても、幅広い領域にわたる取り組みを展開。情報基盤センター 技術専門職員 園田 誠氏は「大学の情報インフラにはある程度の柔軟さ、自由さが求められるため、民間企業のような統一的なガバナンスを効かせにくい面があります。とはいえ、情報資産の安全を守ることは非常に重要なテーマですから、入口対策の徹底やユーザーへの啓蒙活動など、様々な対策を講じてきました」と説明する。

さらに今回、こうした取り組みの一環として着手したのが、キャンパスネットワークの内部対策だ。最近のサイバー攻撃は一段と巧妙化・悪質化が進んでおり、管理者が気付かないうちに内部に侵入されているケースも少なくない。金銭や情報の窃取を目的とした標的型サイバー攻撃の被害も増えつつある中、同大学としても未知の脅威への対応に強い危機感を抱いていたのだ。

マルウェアの活動を察知する 「振る舞い検知機能」に高評価

内部対策を実施するにあたっては、「キャンパスネットワーク内部で今何が起きているのか」「どのような端末や機器がネットワークを利用しているのか」といったことを、迅速・的確に見える化することがポイントとなった。

「ネットワークの安全性向上はもちろん大前提ですが、政府が定める『政府機関の情報セキュリティ対策のための統一基準』では、セキュリティ・インシデントに関する詳細な報告も求められています。ただ被害を防げたというだけでは不十分で、どういう経緯でどのような事態が発生し、どう対策を打ったのかをきちんと説明できないといけません。こうしたセキュリティ運用を実現していくためには、通信や端末の状況を正確に見える化できるツールが不可欠でした」と園田氏は語る。

このようなニーズを満たす製品として導入されたのが、PFUのネットワークセキュリティ機器「iNetSec Intra Wall」だ。「従来型の手法では、未知マルウェアの侵入や活動を検出することが難しいので、『振る舞い検知機能』を備えている点は大きな魅力でしたね。また、既存ネットワークに組み込むインライン型の製品と異なり、ネットワークの改修作業などが不要な点も高く評価しました」と語るのは、情報基盤センター 技術職員 黒木 亘氏。また、同 川畑 圭一郎氏も「同様の機能を備えた製品もいろいろチェックしましたが、不要な機



<お客様概要>

名称：国立大学法人 宮崎大学
所在地：宮崎市学園木花台西1-1(木花キャンパス)
：宮崎市清武町木原5200(清武キャンパス)
設立：1949年5月31日(旧宮崎大学)
公式HP：<http://www.miyazaki-u.ac.jp/>

大学概要：旧宮崎大学と宮崎医科大学の統合を受け新生・宮崎大学として発足。2016年度より教育学部、医学部、工学部、農学部、地域資源創成学部の5学部構成となる。「宮崎大学未来ビジョン」の下、異分野融合を軸とした研究・技術開発の推進など、様々な施策を展開している。

能が多すぎたり価格が高額すぎたりで、なかなか本学の要件にフィットするのがありませんでした。その点、iNetSec Intra Wallは機能とコストのバランスに優れており、本学のネットワーク規模にもピッタリ。この点も、採用の大きな決め手となりました」と続ける。

ネットワークの安全性を向上 利用端末の見える化も実現

キャンパスネットワークへの本格導入に先立ち、同大学ではiNetSec Intra Wallの実機検証も実施。木花キャンパス・清武キャンパスの両キャンパスを対象に、約2ヶ月間にわたってネットワークの内部調査を行った。

「その結果、本学のネットワークには、未知マルウェアの侵入などが行われていないことが確認できました。これまでの対策が実を結んでいたことが確認でき、一安心でしたね」と黒木氏は振り返る。日頃からネットワークの維持管理をしっかりと行っていることもあり、検証機の導入も非常にスムーズだったとのこと。川畑氏は「使いやすさに優れている点も好印象でしたね。いろいろと設定を変えてみたりもしましたが、特に操作に迷うような場面もありませんでした」と語る。

また、もう一つの懸案であった、端末の見える化についても大きな効果を発揮。「事前検証の際には、WindowsXP搭載PCなど、サポートの終了した端末がまだ一部で利用されていることが確認できました。今後はこれらの端末のユーザーに対し、適切なネットワーク利用を促していきたい。iNetSec Intra Wallはまずユーザーに通知した上で止める、あるいは即座に自動遮断するなど、柔軟に制御方法を選べますので、セキュリティ運用の効率化にも役立ってくれそうです」と川畑氏は語る。

こうした事前検証での成果も踏まえて、同大学では2016年3月よりiNetSec Intra Wallによる内部対策システムの本稼働を開始。1台で16VLANまで管理できるため、ネットワーク規模に合わせて木花キャンパスに7台、清武キャンパスに3台のiNetSec Intra Wallが導入されている。これにより、教職員や生徒の持ち込みPCなど約1万人近くが利用するキャンパスネットワークの安全性を大幅に高めることができた。

さらに見逃せないのが、国立大学に求められる充実したセキュリ



国立大学法人 宮崎大学
情報基盤センター
技術専門職員
園田 誠 氏

国立大学法人 宮崎大学
情報基盤センター
技術職員
黒木 亘 氏

国立大学法人 宮崎大学
情報基盤センター
技術職員
川畑 圭一郎 氏

ティ環境を実現できた点だ。「学内のセキュリティ対策に不備が認められた場合には、大学評価にも大きな影響が生じてしまう可能性があります。しかし、今回内部対策を行ったことで、万一のセキュリティ・インシデントにも的確に対応できる体制が整いました」と園田氏は語る。

禁止アプリケーションの 利用制限にも適用範囲を拡大

同大学では、iNetSec Intra Wallのその他の機能についても、積極的な活用を進めていく考えだ。「特に注目しているのが、禁止アプリケーション利用端末の遮断機能です。今のところアプリケーションを特定しての利用禁止は行っていないものの、やはりファイル共有ソフトなどはリスクが大きい。現在は他の製品で止めていますが、これもiNetSec Intra Wallに集約していければと考えています」と川畑氏は語る。

こうした取り組みを進めていく上では、PFUの提案や支援にも大きな期待が寄せられている。黒木氏は今後の展望を「検証機の提供や技術面でのサポートなど、今回のプロジェクトではPFUの支援にも大いに助けられました。今後も出口対策との連携など、学内の安心・安全を確保するための様々な取り組みを展開していきますので、ぜひこれまで同様の後押しを期待しています」と語った。

(2016年4月1日現在)

未知マルウェアの活動を迅速に検知・遮断 効果的な内部対策を実現する「iNetSec Intra Wall」

一段と深刻化するセキュリティ被害。情報や金銭の窃取を目的とする標的型サイバー攻撃に対抗していくためには、従来の入口・出口対策だけでなく内部対策も欠かせません。こうしたニーズにお応えするのが、PFUのネットワークセキュリティ製品「iNetSec Intra Wall」です。高度な振る舞い検知機能により、内部に潜入したマルウェアの活動をリアルタイムで検知。マルウェア感染端末／禁止アプリケーション利用端末の自動遮断機能も搭載しており、脅威への迅速・的確な対応を実現します。



お問い合わせ先

株式会社 PFU

■横浜本社
〒220-8567 横浜市西区みなとみらい4-4-5 横浜アイマークプレイス ☎(045)305-6000

■北海道支店 ☎(011)242-2212 ■東海支店 ☎(052)202-0871
■東北支店 ☎(050)3786-2204 ■関西支店 ☎(06)6152-8153
■北陸支店 ☎(050)3819-9160 ■九州支店 ☎(050)3819-9180

<http://www.pfu.fujitsu.com/>