■ Network Security Platform 導入事例 — 福岡大学

福岡大学

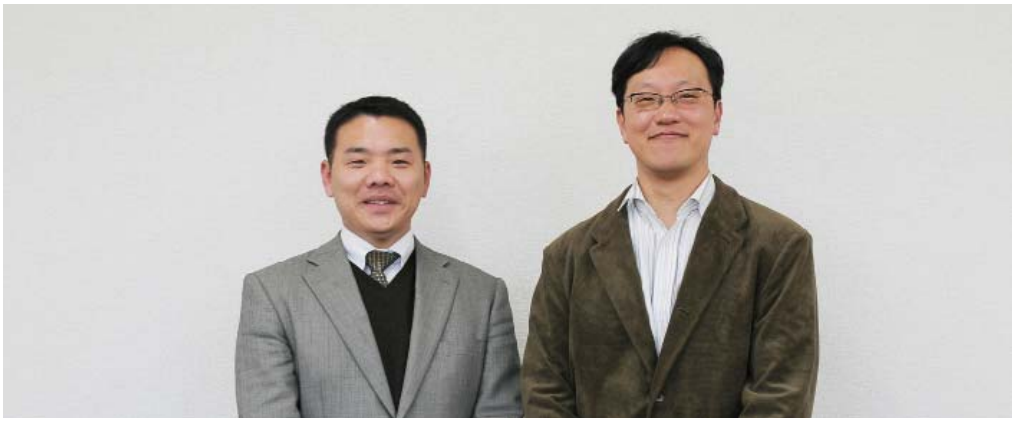
福岡大学

プロファイル

学生数約2万1,000人、教職員3,500人の九州最大の私立大学。人文学部、法学部から工学部、医学部まで9学部31学科を有する総合大学。創立は昭和9年。近年はコンピューター及びネットワークの教育への活用に力を入れている。

教育研究システムFUTUREについて

福岡大学では5年に一度、学内のコンピューターおよびネットワーク環境を全面更新している。平成22年10月には第四次システム「FUTURE4」がカットオーバー。インターネット接続は二系統(10GB+1GB)の広帯域仕様。DHCP情報コンセントも約4000口を備え、学生や教職員の私用パソコンの持ち込み接続もOK。だが自由度の高さはセキュリティ脆弱性につながる恐れがある。その問題を解決するため今回マカフィーのNetwork Security Platformを採用した。



左：福岡大学 情報支援室　服部和文氏　右：准教授　研究開発室　奥村勝氏

「大学のネットワークで、全てのマシンのウイルス定義ファイルやOSのセキュリティパッチを最新の状態に保つのは原理的に不可能です。根本解決策として、パケットレベルで不正コードを検出できるIPSを採用しました」

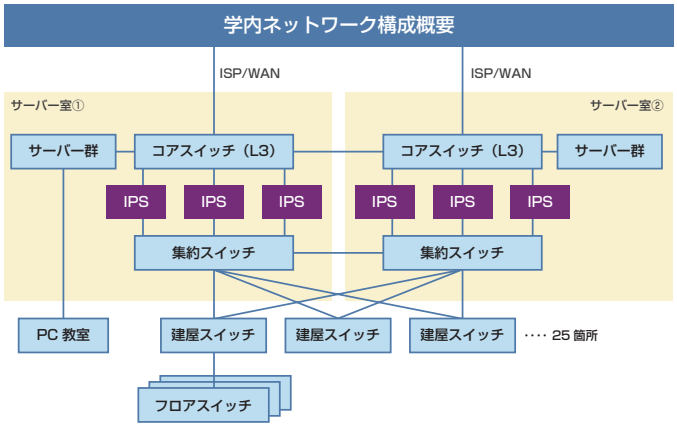
10GB広帯域ネットワークのセキュリティ強化のためにMcAfee Network Security Platformを導入

— 福岡大学ではNetwork Security Platform(以下 NSP)をどう活用していますか。

福岡大学では、学内情報ネットワークシステム(FUTURE)において、ウイルス、ワーム、P2Pソフト※1など不正コード(システム)を、ネットワーク(パケット)レベルで検出、遮断するためのシステムとして、平成22年10月よりマカフィーのNSPを活用しています。活用の概況は次のとおりです。

項目	内容	備考
導入台数	6台	ネットワーク2系統※2に対し、NSPを3台※3ずつ配備。
用途	学内ネットワークにおける不正コードの検出、遮断	学内ネットワークの帯域幅は10GB(学外は1GB)
導入機種	M-8000	ハイエンド機種
運用体制	高度運用業務は外部パートナーに委託	ログ解析、チューニング、重大インシデント対応など
P2P(ファイル共有)ソフトの扱い	一律禁止	Winnyだけでなく「あらゆるファイル共有ソフト」を一律禁止 (共有ソフトが入っているパソコンは大学ネットワークに接続できない)

※1 WinnyなどP2Pファイル共有ソフトが「悪質プログラム」かどうかは議論の余地がありますが、福岡大学のネットワーク使用基準においては「使ってはいけないプログラム」、すなわち不正プログラムと定義しています。
※2 系統はいずれもアクティブ運用。仮に片方がダウンした場合でも、もう片方の系統に、全てのトラフィックを集中させることで、ネットワーク全体のダウンを防止します。
※3 NSPの他、McAfee Web Gatewayも導入(URLフィルタリング、ウイルス対策、キャッシュ、SSLスキャナーとして活用)しています。



— 福岡大学ではNSPの他にどんなウイルス対策を行っていますか。

「大学のネットワークでは『管理』が原理的に困難です」

大学内にある、事務系パソコン（およびサーバー）、パソコン教室のパソコン、その他、メールサーバーなど総合情報処理センターが管理しているサーバーには、それぞれウイルス対策ソフトを導入しています。しかし、大学のネットワーク環境では、これら通常のウイルス対策だけでは、原理的に不十分なので、「根本解決策」としてNSPを導入しました。

一般企業よりも管理が難しい、大学ネットワークのセキュリティ

— 「大学のネットワーク環境では普通のウイルス対策だけでは不十分である」のはなぜですか。

大学ネットワークでは、接続パソコン（サーバー）のウイルス定義ファイルやセキュリティパッチを最新の状態に保つことが原理的に困難だからです。このことを、順を追って説明すると、次のようになります。

大学ネットワークは『管理』が困難

一般企業のネットワークは、基本的に「会社組織の目的に適うよう、決められた方法で使う」ものであり、自由な（勝手な）使用は許されません。一方、大学のネットワークは、教員や学生が「自分の研究（学習）を推進するために、自由に使うもの」です。たとえば、企業では、勝手にサーバーを立てることは原則禁止ですが、大学の場合、「先生が、研究のためにサーバーを立てること」を禁止することはできません。大学では「（学問の）自由が第一。管理は二の次」なのです。

セキュリティは自主性に任せる部分が大きくなる

ネットワーク使用が自由である場合のセキュリティは、「学生、教職員の自主性に期待する」という一種の「性善説」に頼って確保することになります。しかし、セキュリティは、本来、「人間の自主性はあてにならない。人はうっかりミスをする。魔が差すこともある」という「性悪説」に基づいて運用すべきものであり、ここに矛盾が生じます。

接続されるすべてのマシンのウイルス定義ファイルを最新に保つことは原理的に困難

私用パソコンや研究用サーバーが接続されるネットワークにおいて、セキュリティ確保を自主性に頼った場合、「接続パソコン（サーバー）にウイルス対策が施されていること」「ウイルス定義ファイルが最新であること」は担保できません。仮に強制したとしても、本当に実行されているかどうか確かめる手段がありません。同様に、OSのセキュリティパッチについても、それが確実に更新されていることは、担保できません。

OSの種類やバージョンも多様

学内には、Windows各種、Mac OS、UNIX、Linuxなど多様なOSが混在しています。最近はiPadやスマートフォンなどの新種デバイスも現れてきました。このようにOSがバラバラであることは、セキュリティ確保の観点からはマイナスですが、大学が自由を重視する場所である以上、強いて統一はできません。

利用者（学生）のセキュリティ意識が水準に達していない

学生は、18歳から20代前半の若者であり、社会経験はまだなく、セキュリティ事故や情報漏えいの重大性についても、頭では理解していても、「体感、実感」はまだありません。たとえばUSBメモリーによるウイルス感染や情報漏えいの危険は、社会人にはほぼ周知のことですが、学生はそれを「実感」していません。（パソコン教室で私用USBメモリーを使って、ウイルス感染が発見された場合多くの学生は、そこではじめて事の重大さに気づき、平謝りになります）

それでもセキュリティの確保は必須

いくら管理が困難であっても、ネットワーク社会の一員として、セキュリティは十全に確保する必要があります。

以上、大学という環境では「個々のパソコン（サーバー）に依存したセキュリティ確保は原理的に無理」「しかしセキュリティレベルは確保しなければいけない」という矛盾があることを述べました。

この矛盾を解決する方法として、福岡大学では、前述したとおり、IPS（不正侵入防御）を導入することを決めました。5年前の第三次システム更新（FUTURE3）の時期のことです。

IPSがウイルス対策の根本解決策になる理由

— IPSが根本解決策になると考えたのはなぜですか。

先ほど大学ネットワークの困難は、「接続機器のウイルス定義ファイルが最新であることも」「セキュリティパッチがくまなく当たっていることも」「利用者が高いセキュリティ意識を以てネットワークを使うことも」、いずれも当てにできないことだと述べました。しかしIPSならば、ネット

ワーク（パケット）レベルで不正コードを検出・遮断するので、そうした困難をクリアできます。

またIPSの「利用者から見て透過的（普段は存在していることすらわからない）」という特徴も、大学のネットワーク環境に向いています。IPSならば「ふだんはネットワークを好きなように使える　→　自由度を損ねない」「しかしウイルス感染パソコンに対しては直ちに強権発動、接続停止　→　学内、学外への迷惑防止」というコンセプトの運用が可能です。以上の理由に基づき、5年前にIPSをはじめて導入しました。当時はNSPでない他の製品Aを採用したのですが、その製品は安定性に難があり、ネットワーク可用性のボトルネックとなっていました。

この問題を解決するべく、2010年の第四次システム更新（FUTURE4）においては、改めて各種IPS製品を比較検討しなおしました。

IPSを選定した際の要件

―　各種IPSを比較検討するにあたり、何を要件にしましたか。

IPSを比較検討した際の要件は次の三点です。

要件1. IPSとしての基本的な検出・防御機能が十全であること

ワームやウイルスなど不正コードを検出、停止するというIPSとしての基礎機能が十全であることは必須要件でした。

要件2. スループットと安定性が高いこと

FUTURE4では、帯域幅を10GBに拡張しました。この広帯域においてバーストトラフィックが発生した場合でも、ネットワークのボトルネックとなることのないような、堅牢な製品であることが必要でした。

要件3. ユーザーフレンドリーな接続停止メッセージを表示する運用が可能なこと

ワーム感染パソコンの利用者に対しては、「あなたのパソコンはネットワークに接続できません」といった素っ気ない通告をするのではなく、「この後、具体的にどう行動すればよいのか」「どこに連絡すれば良いのか」などを、一般学生にも分かるような親切な日本語で指示できる仕様を求めました。

以上の要件を元に各製品を相互比較したところ、マカフィーのNSPが、要件を最も良く満たしていたので、これを採用しました。その後、NSPは、2010年10月に、第四次ネットワーク（FUTURE4）に組み込む形で、利用を開始しました。

NSPの導入効果

―　NSPの導入効果を教えてください。

導入以後の3カ月にわたり、NSPは高い安定性を以て稼働しております。当初の期待通りです。

NSP導入後の三ヶ月間で、30件の重大インシデント※4に対処しました。

P2P（ファイル共有ソフト）も厳格に検出（隔離）できています。かつてに比べセキュリティレベルが大きく向上した実感があります。

感染パソコンを接続したときの具体的な処理プロセス

―　利用者がウイルス感染パソコンを大学ネットワークに接続しようとした場合、具体的にどのように処理されるのですか。

感染パソコンを大学ネットワークに接続しようとした場合の処理手順は次のとおりです。

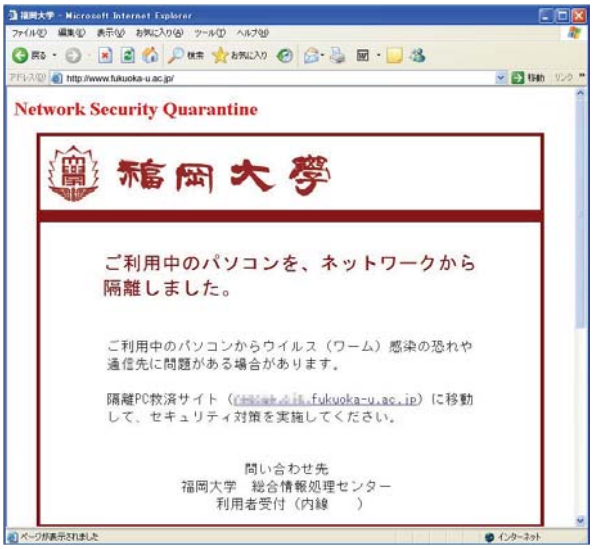
1. 感染パソコン接続

感染パソコンが接続されウイルス（ワーム）がネットワーク内に不正コードを放出しようとしますが…。

2. NSPが検知（遮断）

NSPがそれを検知（ストップ）。そのパソコンは、ただちにネットワーク接続を停止されます

（利用者からは「あれ、ネットワークにつながらない、おかしいな」というように見えます）



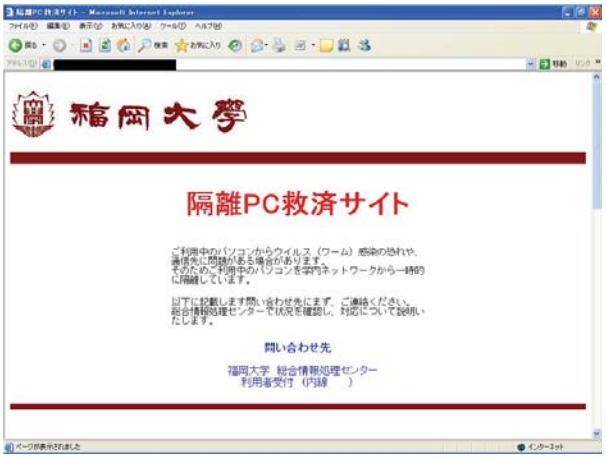
3. パソコン利用者への通知

その後、ユーザーがブラウザーを開いて、何かのホームページを見ようとすると、自動的に「感染・隔離通知ページ」にリダイレクトされます。

※4 外部運用パートナーが検知し、報告を受けた重大なインシデント。

4. 対処方法の通知

その「隔離通知ページ」には、「あなたのパソコンがウイルス（ワーム）感染している可能性があること」「駆除ツールや手動駆除方法のページへのリンク」「対応窓口への連絡方法」などが書かれています。



5. ウイルス（ワーム）の駆除

利用者は、通知ページの指示に従って、ウイルス（ワーム）を駆除します。

6. ネットワーク接続の復活

ウイルスの駆除が確認され次第、そのパソコンは再びネットワーク接続ができるようになります。

現在、IPS導入を検討しているユーザーへのアドバイス

— 現在IPSの導入を検討しているユーザーに、「ある種の先輩ユーザー」としてのアドバイスなどあればお聞かせください。

アドバイスというほどでもなく、私見としてですが、まず可用性、安定性に優れた製品を選ぶことをお薦めします。IPSの長所はネットワークレベルで不正コードを見つけることです。しかし、安定性の低い製品を選んだ場合、その長所は、「ネットワーク全体を遅く不安定にする」という短所に変わってしまいます。安定性は非常に重要です。

「運用プロセスを入念に策定することが重要です」

第二に「パソコン隔離の際の運用プロセスを事前によく練り込むこと」をお薦めします。IPSがウイルスを見つけて機器を遮断するまでは自動ですが、その後、利用者にウイルスを駆除させる部分は、人が行うプロセスになります。このプロセスを念入りに策定すれば、導入後の運用負荷を軽減できます。

第三に専門知識を持つパートナーと組むことをお薦めします。IPSはネットワークの根幹部分で動作する機器なので、チューニングやログ解析、インシデント対応には専門知識が必要になります。先に述べた運用プロセスを含め、総合的な支援が可能なSIパートナーと組むのが良いと考えます。

今後の期待

— マカフィーへの今後の期待をお聞かせください。

今回、NSPの導入を通じ、福岡大学の教育ネットワークは、自由度や利便性を損ねることなく、セキュリティレベルを大きく高めることができました。マカフィーには、今後とも福岡大学の教育ネットワーク環境のセキュリティ強化を、優れた技術、製品、サポートの継続提供を通じて支援していただくことを希望します。今後ともよろしくお願いいたします。

取材日時 2011年1月

McAfee マカフィー株式会社
www.mcafee.com/jp

●製品、サービスに関するお問い合わせは下記へ

東京本社　〒150-0043 東京都渋谷区道玄坂1-12-1 渋谷マークシティウエスト20F
TEL:03-5428-1100(代) FAX:03-5428-1480

西日本支店　〒530-0003 大阪府大阪市北区堂島2-2-2 近鉄堂島ビル18F
TEL:06-6344-1511(代) FAX:06-6344-1517

名古屋営業所　〒460-0002 愛知県名古屋市中区丸の内3-20-17 中外東京海上ビルディング3F
TEL:052-954-9551(代) FAX:052-954-9552

福岡営業所　〒810-0801 福岡県福岡市博多区中洲5-3-8 アクア博多5F
TEL:092-287-9674(代) FAX:092-287-9675

MCACS-FUV-1102-MC