福岡大学キャンパスネットワークにおける利用者認証と検疫システムの導入

藤村 丞, 奥村 勝, 中國 真教

福岡大学
総合情報処理センター 研究開発室
{fujimura, okkun, nak}@fukuoka-u.ac.jp

概要： 福岡大学では平成 22 年 9 月に、平成 17 年 10 月より運用してきた教育研究システム FUTURE（Fukuoka University Telecommunication Utilities for Research and Education）を更改した。第 4 世代目となる新教育研究システム（FUTURE4：FUTURE Ver.4）では利用者認証と検疫システムの新規導入をはじめとして、学内 LAN やクライアント PC 環境（PC 教室・オープン端末室）、サーバ環境など情報処理教育研究環境のすべてを同時に一新した。本稿では、その中でも学内 LAN 利用時における利用者認証と検疫システムを導入したことに重点をおき、導入の経緯や適用範囲、これらの仕組み、問題点などについて分析し述べる。

1 はじめに

福岡大学は福岡県福岡市に所在地を置き、9 学部 31 学科、10 研究科 33 専攻、学生数約 21,000 名、大学病院 2 病院、附属高校 2 校、付属中学校 1 校を有する私立の総合大学である。

平成 22 年 9 月に福岡大学では、平成 17 年 10 月より運用してきた教育研究システム FUTURE を更改した。第 4 世代目となる新教育研究システム（FUTURE4：FUTURE Ver.4）では、学内 LAN やクライアント PC 環境（PC 教室・オープン端末室）、サーバ環境など情報処理教育研究環境のすべてを同時に一新した。この FUTURE4 の特徴の一つとして、学内 LAN 利用時における利用者認証と接続端末があらかじめ決められたセキュリティ基準に達しているかを機械的に（自動的に）チェックする検疫システムの導入を行った。

以前の教育研究システムでは、学内 LAN への機器接続申請を総合情報処理センターに行うと IP アドレスが割り振られ、それを利用端末に設定することにより学内 LAN に接続することができた。今回導入したシステムでも機器接続申請は引き続き必要であるが、学内 LAN の利用を開始する際にブラウザを用いて利用者認証を行い、続けてセキュリティ基準の達成度を検疫システムによってチェックする仕組みへと変更した。

本稿では、この利用者認証と検疫システムについて、その導入の経緯や適用範囲、これらの仕組み、問題点などについて分析し述べていく。

2 導入について

2.1 導入の背景

先にも述べたが、以前の教育研究システムでは利用端末を学内 LAN に接続する際、特別な作業は必要なかった。また、利用端末における OS ならびに各ソフトウェアのセキュリティアップデートやウイルス対策ソフトウェアの導入、パターンファイルの最新化などの確認と実施は、利用者各個人に委ねていた。なお、ウイルス対策ソフトウェアについては、総合情報処理センターで学内端末分を一括契約し利用者に対して提供している。よって利用者は、本学が所有している端末に対して、ウイルス対策ソフトウェアをインストールすることができる。

学内 LAN 利用においてはこのような状況であったため、利用者によっては OS や各種ソフトウェアのセキュリティアップデートが行われていない場合やウイルス対策ソフトウェアがインストールされていない場合、インストールされていてもパターンファイルが古かったり対策ソフトウェア自体が古くメーカーサポートが切れている場合など、セキュリティ対策には多くの課題があった。

また、学内 LAN（ネットワークとして）のセキュリティ環境としては、インターネット接続点における FireWall の導入やその直下に IPS(Intrusion Prevention System) を配置していた。また学内通信においては、各学部学科の研究室やゼミ室などの数セグメントでグループを作成し、そのグループ間通信についても IPS を配置してセキュリティ向上を図っていた。これらの対策を行っていたため、ネットワーク的に異常な通信や振る舞いはこの IPS が遮断をしていたが、遮断される端末の数は一定数存在し、このことも前述のセキュリティ対策も含めて重要な課題であった。

このような中、本学では平成 19 年に「学校法人福岡大学情報セキュリティに関する規程」をはじめとする関連 5 規程を策定し、OS や利用しているソフトウェアのセキュリティパッチを適用することや、ウイルス対策ソフトウェアの導入と定義ファイルを適切に管理することが明文化された。だが規程を策

定したものの、学内の情報関連を統括する総合情報処理センターとしてはなんら強制力を持つものではなかったため、利用者の端末に対して具体的な改善を行うことが出来ず、さらなるセキュリティ対策とそれらの向上を行うことが出来なかった。

このため、教育研究システム（FUTURE4）のネットワーク設計に当たっては、これら規程を遵守することができるためのシステムとして、ネットワーク認証と検疫システムを各種委員会に提案した。これらの仕組みにより、利用者は学内 LAN 利用時に認証を行いその後検疫システムによって、利用端末のセキュリティ基準を自動的に確認することが可能になる。また、一定のセキュリティ基準に達していない端末についてはその理由と改善方法が明示され、それらを元にセキュリティ基準を改善することができる。このシステムは各種委員会に提案後、議論を行い導入することを決定した。

2.2 導入範囲

本学の学内 LAN については、全て総合情報処理センターで管理運用を行っている。ただし大学病院のオーダリングシステムや附属高校、中学校は、各部門で行っている。学内 LAN の設置先を分類すると、おおよそ以下のように分けることができる。

1. 各学部学科の研究室および大学病院の研究室・カンファレンスルーム
2. 自主管理ネットワーク
3. DHCP 情報コンセント（有線・無線）
4. 総合情報処理センターが管理運用する PC 教室・オープン端末室
5. 事務情報ネットワーク

各学部学科の研究室および大学病院の研究室・カンファレンスルームとは、文字通り本学の学生や教育職員が教育・研究を行う場所である。また、病院のカンファレンスルームとは、勉強会などに利用する場所のことである。

自主管理ネットワークとは、学部学科や研究室、各部門などで独自に運用しているネットワークである。DNS を独自に運用することが条件となっており、学内 LAN の一部（24 ビットマスクのネットワーク）を割り当てられ、自身で運用することができるネットワークである。平成 24 年 10 月現在、19 セグメントを割り当て運用を行っている。

DHCP 情報コンセントとは、教室や一部の研究室、無線 LAN などによって提供されるネットワークで、持ち込みパソコンやタブレットなどを接続することができる。接続には、認証が必要である。

総合情報処理センターが管理運用する PC 教室・オープン端末室とは、これも文字通り PC を用いた講義や自学自習などに利用される教室である。

事務情報ネットワークとは、管理部門や大学運営に関する事務系サーバが書属するネットワークである。

本学にはおおよそこのようなネットワークが存在するが、今回のネットワーク認証と検疫システムについては、上記のうち「各学部学科の研究室および大学病院の研究室・カンファレンスルーム」および「自主管理ネットワーク」について導入を行った。なお、DHCP 情報コンセントに検疫システムの導入を行わなかったのは、各個人の持ち込みパソコンに対してセキュリティ対策ソフトウェアの指定や検疫の動作に対する本学のサポート体制、検疫システムが未対応の OS に対する除外処理、講義実施時において検疫の実施による開始時刻の遅延など、多くの課題に対処することが困難であったためである。また、PC 教室・オープン端末室、事務情報ネットワークについては、本学総合情報処理センターがディスクイメージを一括管理し、セキュリティ水準を統括して維持していることや、利用者に対して管理者権限がないことなどから今回は導入を行っていない。ただし、これらの検疫システムの導入を行っていないネットワークについては、ネットワーク接続時もしくは端末利用時に「認証」のみ行っている。

3 ネットワーク認証と検疫システムの仕組み

3.1 動作環境と接続可能 OS

学内 LAN にアクセスする際には、利用者はブラウザを用いてネットワーク認証を行いその後検疫システムを実行し、利用端末のセキュリティレベルが定められた基準に達しているかどうかのチェックを自動的に行う。検疫システムもネットワーク認証と同じくブラウザを用いて行うのだが、これは今回導入した検疫システムがブラウザのプラグインを利用して動作するためである。平成 24 年 10 月現在、検疫（プラグイン）が実行可能なブラウザは以下の通りである。

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Safari 4 以降

Internet Explorer は Windows 上でのみ実行可能であり、Safari は Mac OS X 上のみ実行可能である。

なお、OS については Windows 2000 や Mac OS X v10.4 などの古い OS についても検疫は実行可能であるが、これらの OS はメーカーのサポートが打ち切られており、セキュリティパッチの未提供やウイルス対策ソフトウェアでの保護ができないなど、多くの問題点があることから意図的に利用ができないようにしている。平成 24 年 10 月現在、学内 LAN に接続可能としている OS を表 1 に示す。

3.2 セキュリティ基準（安全判定の基準）

認証後、検疫システムによって、利用端末が一定のセキュリティ基準を満たしているかどうかの判定が実行される。このセキュリティ基準については様々な設定が可能であるが、本学の運用では以下のように定めている。

対応 OS とバージョン	
バージョン	サービスパック
Windows XP	SP3
Windows XP x64	SP2
Windows Vista	SP2
Windows 7	SP なし、SP1
Windows Server 2003	SP2
Windows Server 2003 R2	SP2
Windows Server 2008	SP2
Windows Server 2008 R2	SP1
Mac OS X v10.5.8	
Mac OS X v10.6.8	
Mac OS X v10.7.4	
Mac OS X v10.7.5	

表 1: 検疫システムにおける利用可能 OS

1. 総合情報処理センターが指定するウイルス対策ソフトウェアが導入されており、ウイルス定義ファイルが一定期間内において更新されていること
2. 外部からの不要な通信を遮断するパーソナルファイアウォールが機能していること
3. Windows や Mac OS X などの OS セキュリティ修正プログラムが一定期間内において適用されていること

なお、ウイルス対策ソフトウェアについては総合情報処理センターで一括契約し、学内利用者（教職員のみ）に提供している。そのため Windows と Mac OS X には、このウイルス対策ソフトウェアをインストールしてセキュリティ対策を行うことができるようになっている。ただし、個人所有の PC の場合にはライセンス上このウイルス対策ソフトウェアはインストールできない。だが、個人所有の PC であっても学内 LAN に接続する際には、検疫システムによりウイルス対策ソフトウェアが導入されているかどうかチェックが行われる。そのため、利用可能なウイルス対策ソフトウェアが一括契約しているソフトウェアのみであると、持ち込み PC の場合必ずしもこのウイルス対策ソフトウェアがインストールされているとは限らない。とはいえ、多くの種類が利用可能（検疫システムが対応している範囲）であると総合情報処理センターのサポート体制やその内容に影響が出てくることや、検疫における確実な動作を行いたいことなどの理由から、利用者の利便性を残しつつある種類に限定して運用を行っている。

3.3 ネットワーク認証と検疫の除外

検疫システムの動作 OS としては第 3.1 節で述べたが、これらの OS 以外では検疫システムは動作しない。しかし、学内には Windows や Mac OS X 以外にも様々な OS が動作している。また、検疫システムの仕組み上（MAC アドレスで管理する仕組み上）、検疫を除外しないと学内 LAN を利用できない場合が発生してくる。よって、運用上やむを得ない場合に限り、検疫の除外を行って運用している。以下にその場合を示す。

1. 検疫システム未対応 OS 暫定除外（例：Windows 8）
2. 検疫を実行できない OS や機器（例:iOS、ネットワークプリンタ）
3. サーバ（要塞ホスト）
4. ブロードバンドルータ
5. FireWall や独自のルータを設置している自主管理ネットワーク

これらの機器や OS については検疫の除外を行い、学内 LAN を利用可能としている。ただし、利用端末については検疫が行われないことから、セキュリティ対策については利用者にそれ相応の責任と対策やその能力などが求められることになる。

3.4 ネットワーク認証と検疫システムの利用手順とその仕組み

利用者は利用端末を起動し Web ブラウザで任意のサイトにアクセスを試みるとリダイレクトされ、図 1 のようなネットワーク認証検疫システム選択画面になる。

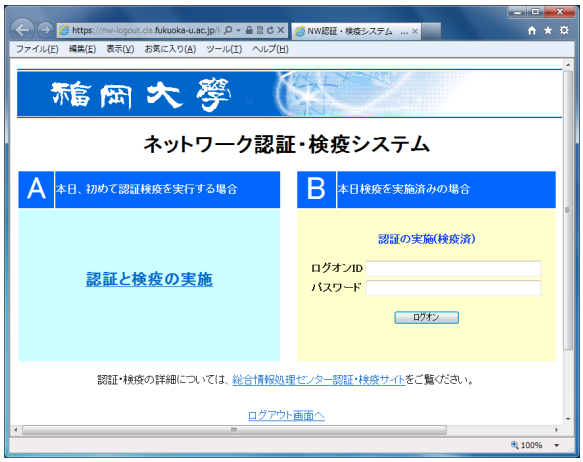

図 1: ネットワーク認証検疫システム選択画面

ある日初めて学内 LAN に接続する場合には左側の A を選択し、認証と検疫を実行する必要がある。また、検疫を実行した同日中に再び学内 LAN に接続する場合には検疫を行う必要はなく、右側の B において認証を行うのみで学内 LAN に接続することが可能である。

まず A の場合の仕組みだが、図 2 の様になっている。利用者が図 1 にアクセスし（1）、A を選択して検疫を実行する（2）。検疫が成功すると、検疫サーバに実行時のアカウントと MAC アドレスが記憶される（3）。その後、ネットワークスイッチに対して接続許可を通知して（4）利用者の端末が学内 LAN に接続可能となる（5）。

B の場合には、ネットワークスイッチに対して利用端末が登録されておらず、検疫サーバのみに登録されている状態である。この場合、利用者は認証のみを行い（1）、ネットワークスイッチがアカウントと利用端末の MAC アドレスを検疫サーバに問い合わせ（2）、ネットワークスイッチに対して接続許可を通知して（4）利用者の端末が学内 LAN に接続可能となる（5）。

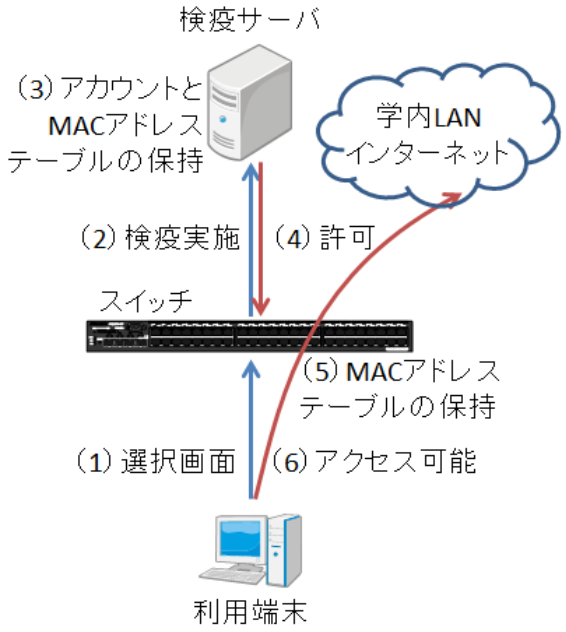

図 2: ネットワーク認証検疫システム構成

なお、検疫サーバが何らかの理由で停止していた場合には、ネットワークスイッチ側でフェイルオープンの設定を行っているため利用者はネットワーク認証と検疫を行うことなく学内 LAN を使用することができるようになっている。これは、検疫サーバを複数台で冗長化しており、かつ学内の異なった場所に分散配置をしていることで停止する確率を低く抑えていることと、万が一すべてのサーバが停止した場合による業務への影響を考えてフェイルオープンの設定とした。

4 導入スケジュール

現在稼働している教育研究システム（FUTURE4）は平成 22 年 9 月に稼働を開始したが、このネットワーク認証と検疫システムは FUTURE4 の稼働と同時に実施したわけではない。導入については、操作手順方法や動作確認、検疫システム未対応の機器に対する事前の除外申請などの多くの事前準備が必要であり、利用者が突然学内 LAN を使えなくなることがないように、全面実施にあたっては図 3 のような 4 つの段階（STEP）を設け、各 STEP に応じたパンフレットの作成やそれを用いた広報活動、説明会の実施などを行い段階的に導入した。なお、STEP1 開始時点では残りの STEP 開始時期は決めておらず、学内への浸透具合を分析しながら決めていった。最終的には全面実施に約 1 年と 2ヶ月を費やすこととなった。表 2 は、STEP1 から 4 までの全体スケジュールである。

5 統計

平成 23 年 11 月にネットワーク認証と検疫システムの全面実施（STEP4）を開始してから平成 24 年 10 月までで、おおよそ 11ヶ月が経過した。平成 24 年 10 月現在において、検疫を実行した台数や除

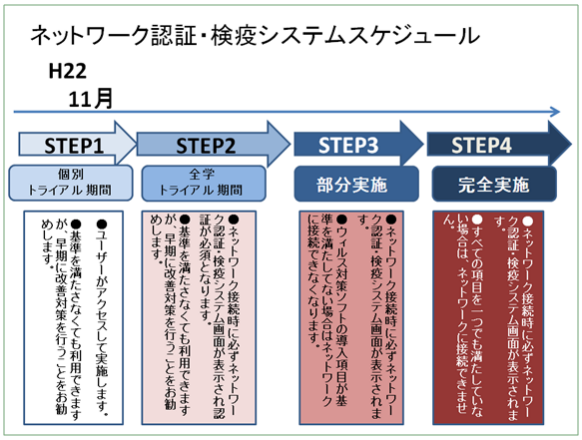

図 3: 完全実施までの段階（STEP）

導入スケジュール		
段階	内容	実施年月
FUTURE4 稼働	認証と検疫未実施	平成 22 年 9 月
STEP1	テスト期間	平成 22 年年 11 月
STEP2	トライアル期間	平成 23 年 9 月
STEP3	部分実施	平成 23 年 10 月
STEP4	完全実施	平成 23 年 11 月

表 2: ネットワーク認証と検疫実施スケジュール

外数などを表 3 に示す。この内訳の詳細としては、

ネットワーク認証と検疫システム実施台数	
項目	台数
IP アドレス管理数	6,684(A)
要塞ホスト（サーバ）申請数	152(B)
除外申請数	1,138(C)
暫定除外申請数	41(D)
実施対象 (A)-(B)-(C)-(D)	5,353
実施総数	3,675
実施率	68.7%

表 3: ネットワーク認証と検疫システム実施台数

次のようになっている。

IP アドレス管理数とは、総合情報処理センターに提出された機器接続申請によって割り当てられた IP アドレスの総払い出し数のことであり、研究室が主な対象である。よって、第 2.2 節で述べた導入範囲以外のネットワーク（DHCP 情報コンセントや総合情報処理センター管理の端末、事務情報ネットワーク）と自主管理ネットワークについては、この数に含まれていない。

要塞ホスト（サーバ）申請数とは、サーバ機能を果たすために申請された申請数（台数）のことである。除外申請数とは、検疫を実行できない OS や機器のために申請された申請数（台数）のことである。暫定除外申請数とは、暫定検疫除外のために申請された申請数（台数）のことである。よって、これら除外の申請数（台数）を IP アドレス管理数から引いた値が実施総数となる。実施総数は 3,675 台、率にして 68.7%となる。

参考文献

[1] 藤村 丞「ネットブート型 PC による大規模情報処理教育環境の構築」、pp.111-114、平成 22 年度情報教育研究集会講演論文集、2010 年 12 月