Vol.2013-IOT-20 No.9
2013/3/14

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[1,a)]　奥村 勝[1,b)]　中國 真教[1,c)]

概要：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（Fukuoka University Telecommunication Utilities for Research and Education）を、平成 22 年 9 月に更改した。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。

キーワード：認証、検疫、検疫システム

Installation of user authentication and quarantine system for campus network

FUJIMURA Sho[1,a)]　OKUMURA Masaru[1,b)]　NAKAKUNI Masanori[1,c)]

Abstract: We updated the education and research information system named FUTURE4 (Fukuoka University Telecommunication Utilities for Research and Education) which we had managed from October, 2005 in September, 2010. We installed user certification and quarantine system on our LAN in this system of this fourth generation for the first time. And we updated LAN, client PC environment, servers and so on in this system at the same time. We in particular describe that we installed user certification and quarantine system at the time of our LAN use.

Keywords: user certification, quarantine, quarantine system

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。

[1] 福岡大学 総合情報処理センター 研究開発室
Research & Development Office, Information Technology Center, Fukuoka University
[a)] fujimura@fukuoka-u.ac.jp
[b)] okkun@fukuoka-u.ac.jp
[c)] nak@fukuoka-u.ac.jp

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。

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 25 年 1 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, 7, 8, 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 についても検疫システム上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。そのため、検疫システムが検疫可能な OS 全てを接続可能とせずに、サポートが打ち切られた OS や古い OS などは、学内 LAN に接続できないようにしている。平成 25 年 1 月現在、本学が学内 LAN に接続することを許可している 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。

(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

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 学内 LAN に接続可能な OS（平成 25 年 1 月現在）

(1) のウイルス対策ソフトウェアの種類については、平成 24 年 10 月現在以下のように定めている。

Windows
(1) TrendMicro ウイルスバスターコーポレートエディション V8.0SP1〜10.5
(2) ウイルスバスター クラウド
(3) TrendMicro ウイルスバスター 2011〜2012 クラウド
(4) TrendMicro ServerProtect 5.80
(5) Symantec AntiVirus コーポレート・エディション V10.0〜10.2
(6) Symantec Endpoint Protection 11.0, 12.1
(7) Norton Internet Security 2008〜2012
(8) Norton AntiVirus 2008〜2012
(9) Norton 360 Ver1(32bit OS のみ)
(10)McAfee VirusScan Enterprise Ver 8.7i, 8.8
(11)McAfee AntiVirus Plus
(12)McAfee SaaS Endpoint Protection

Mac OS X
(1) Trend Micro Security for Mac
(2) TrendMicro ウイルスバスター for Mac
(3) Norton AntiVirus for Mac 10, 11

なお、総合情報処理センターでは、上記下線のウイルス対策ソフトウェアを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、あまり種類が多すぎ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特定の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

3.3.1 暫定検疫除外

検疫システムの動作 OS としては第 3.1 節で述べたが、新しく発売された OS やアップデートされた OS などは、検疫システムが認識できずに動作しない場合がある。これらの OS については順次検疫システムがアップデートされるタイミングで検疫可能となるが、おおよそ 3 ヶ月から半年ほどが必要である。

このため、その期間それらの OS を利用可能とするために、暫定除外申請（当該機器の MAC アドレス申請）を設けている。2010 年 10 月現在 Windows 8 や Windows Server 2012、OS X v10.8.x については検疫システムが対応していないため、暫定除外申請を行うことで暫定的に学内 LAN が利用可能となる。有効期間は、検疫システムがこれらの OS に対応するまでの期間となる。

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。他の検疫除外ケースも同様である。

3.3.2 検疫を実行できない OS や機器

現在導入している検疫システムで検疫を行うことができる OS は、Windows と Mac OS X である。よって、UNIX や UNIX ライクな OS、ネットワークプリンタ、ネットワークスキャナ、NAS、各種ネットワーク機器、無線 LAN 基地局（NAT なし、管理用 IP アドレス）、iOS、Android などについては検疫を実行することはできない。そのため、これらの機器や OS などについては除外申請を行うことにより、学内 LAN が利用可能となる。

3.3.3 サーバ（要塞ホスト）

Web や電子メールなどのサーバ（要塞ホスト）については、検疫システムの対象となっているとそれらのサービスを提供できない。そのため、これらの機器については除外申請を行う必要がある。これにより、サーバへのアクセスが可能となる。

3.3.4 エージェントソフトウェア

検疫の実行は Internet Explorer もしくは Safari のプラグイン機能を用いて実行するが、その際には管理者権限が必要となる。よって、複数人数で利用している共有端末で各ユーザに管理者権限がない場合には、検疫が実行できないことになる。そこで、これらの端末において検疫を実行するために、検疫を管理者権限で行うソフトウェア（エージェントソフトウェア）をあらかじめインストールしておく。これにより、共有端末に一般ユーザ（管理者権限を持たないユーザ）がログインすると、管理者権限を持ったエージェントソフトウェアによって、バックグランドで検疫を自動的に実行することができる。ただし、このエージェントソフトウェアが対応している OS は Windows のみである。また、検疫実行時には各ユーザのアカウント名とパスワードが必要だが、このエージェントソフトウェア利用時にはそれらをあらかじめ設定し（記憶させ）ておく必要がある。このことは、セキュリティ上あまり好ましくないため、運用では専用のアカウントを発行してそれを利用することにしている。

3.3.5 ブロードバンドルータ

ブロードバンドルータについては、そのネットワークの内部に検疫可能な OS が少なくとも 1 台ある場合、検疫を行った後はその配下にある機器は、検疫を行わなくても学内 LAN に接続することが可能である。これはブロードバンドルータの MAC アドレスにて検疫が行われるためであり、その仕組み上やむを得ない。よって、ネットワーク内部に Windows がある場合には、第 3.3.4 節のエージェントソフトウェアをインストールして、自動的に検疫を行うこととしている。Mac OS X がある場合には、エージェントソフトウェアが Mac OS X に対応していないため、これについては手動で検疫を実施することとしている。

なお、ネットワーク内部に検疫可能な OS がない場合には、第 3.3.2 節と同じように除外申請が必要となる。

3.3.6 自主管理ネットワーク

自主管理ネットワークとは、第 2.2 節で述べたネットワークのことである。これらのネットワークと学内 LAN の接続点に独自のルータや FireWall などを設置している場合には、第 3.3.5 節と同じような取り扱いとなる。独自

のルータや FireWall などを設置していない場合には、他の学内 LAN 接続の端末と同様の扱いとなる。平成 24 年 10 月現在、学内には 19(1 つは/24 のネットワーク) の自主管理ネットワークが存在する。

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。 ある日初

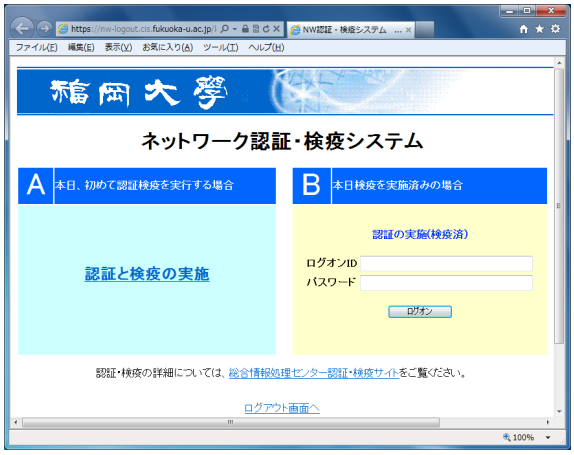

図 1 ネットワーク認証検疫システム選択画面

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。

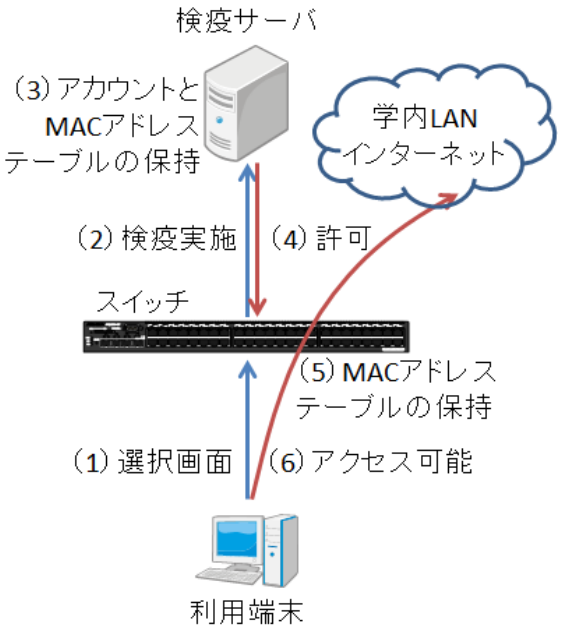

図 2 ネットワーク認証検疫システム構成

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)。

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、第 4.1 節の STEP1

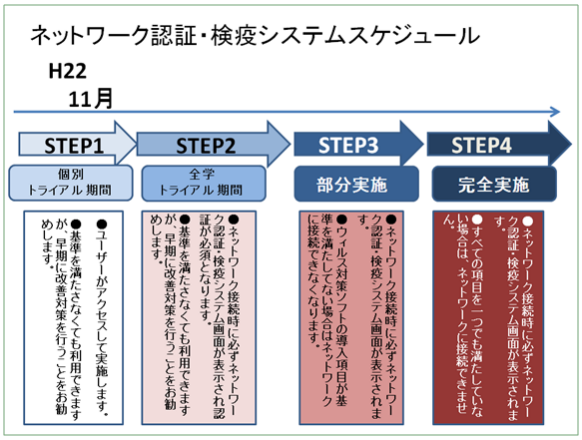

図 3 完全実施までの段階 (STEP)

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。 以下では、

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 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

各 STEP 毎に実施した内容について述べていく。

4.1 STEP1

STEP1 については、FUTURE4 が稼働してから約 2 ヶ月後の平成 22 年 11 月 8 日に開始し、STEP2 を開始する平成 23 年 9 月 1 日までの約 11 ヶ月をテスト期間とした。このテスト期間とは、学内 LAN はネットワーク認証と検疫システムを実行しなくてもこれまでと変わりなく利用す

ることが可能であり、このシステムの URL を利用者自身で入力してアクセスし、利用することができる期間である。この期間では、利用者にこのシステムの仕組みや操作方法の習得、利用端末での動作確認などを自ら体験してもらい、実施に対して問題があればそれらを事前に解決するための準備期間である。また、次の STEP2 の実行にあたって、以下の除外申請を提出して検疫除外登録をしておく必要があった。もし登録がない場合には、SETP2 実行後当該機器が学内 LAN に接続できないことになる。

- 業務上必要なメーカーサポート切れの OS についての暫定検疫除外 (例:Windows 2000)
- 第 3.3.2 節の検疫を実行できない OS や機器
- 第 3.3.3 節のサーバ
- 第 3.3.4 節のエージェントソフトウェア
- 第 3.3.5 節の配下に検疫可能な OS が存在しない場合のブロードバンドルータ
- 第 3.3.6 節のルータや FireWall を設置している自主管理ネットワーク

なお、STEP1 実施にあたって Web や掲示などの広報を行っていたが実施率が低迷していたため、その向上と各種除外申請提出の重要性を広めるにあたり、各学部および両病院に対して順次個別の説明会を開催した。これにより、STEP2 を実施するための準備を行うことができ、STEP1 から STEP2 へのスムースな移行を行うことが可能となった。

4.2 STEP2

STEP2 については、平成 23 年 9 月 1 日に開始した。この STEP2 は、学内 LAN 利用時に必ずネットワーク認証と検疫を実行する必要がある期間である。ただし検疫の実行結果においてたとえ第 3.2 節の基準を満たしていない項目があったとしても、学内 LAN に接続できなることはない。言い換えれば、条件を満たしていなくても、学内 LAN に接続することができる。ただし、第 4.1 節にある除外申請をを行っていないと、当該機器は学内 LAN に接続できないことになる。

利用者はこの期間を使用して、基準を満たすように利用端末を改善することが目的となる。また、検疫が実行できない機器に対する除外申請を確実に行うことも、この期間の重要な目的である。

4.3 STEP3

STEP3 については、平成 23 年 10 月 18 日に開始した。この STEP3 は第 4.2 節の STEP2 に引き続き、学内 LAN 利用時に必ずネットワーク認証と検疫を実行する必要がある期間である。ただし、STEP2 の条件に加えて、第 3.2 節のウイルス対策ソフトウェアの基準項目を満たしていない場合には、学内 LAN に接続することができない。いわゆるネットワーク認証と検疫システムの全面実施に対する部分実施にあたる。利用者はこの期間を利用して、本番稼働に対する最終準備を行う期間となる。

4.4 STEP4

STEP4 については、平成 23 年 11 月 8 日に開始した。この STEP4 は、ネットワーク認証と検疫システムの全面実施（本番稼働）である。よって利用者は、学内 LAN 利用時に認証と検疫の実行が必要になり、かつ第 3.2 節の基準項目をすべて満たしておく必要がある。

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（第 4.4 節）を開始してから平成 25 年 1 月までで、おおよそ 15 ヶ月が経過した。現在の実施台数や各 STEP の実施段階について、次に示していく。

5.1 実施台数

平成 25 年 1 月現在において、検疫を実行した台数や除外数などを表 3 に示す。 この内訳の詳細としては、次のようになっている。

項目	台数
IP アドレス管理数 (A)	6,790
要塞ホスト（サーバ）申請数 (B)	152
除外申請数 (C)	1,226
暫定除外申請数 (D)	84
実施対象 (A)-(B)-(C)-(D)	5,328
実施総数	3,792
実施率	71.2%

表 3 ネットワーク認証と検疫システム実施台数

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）と第 3.3.6 節の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、第 3.3.3 節の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、第 3.3.2 節の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、第 3.3.1 節の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 3,792 台、率にして 71.2%となる。

5.2 STEP1 における実施台数

STEP1 とは、図 3 の最初の段階であり、第 4.1 節の内容である。STEP1 の期間としては、平成 22 年 11 月 8 日から平成 23 年 9 月 1 日である。図 4 は、STEP1 開始当初の平成 22 年 11 月 8 日から STEP2 にかけての検疫実施台数である。

検疫システム導入当初は約 160 台から始まり、平成 22 年内には 1,300 台まで実施された。これ以降 STEP2 開始の平成 23 年 9 月 1 日までは緩やかな伸びを続け、最終的には約 2,000 台の実施台数をもって STEP2 に入ることとなった。

STEP2 を開始するにあたり、当初どの程度の実施台数をもって開始すると業務に支障を来さず、かつ混乱なく開始できるのか目標を立てることが非常に困難であった。先に述べたとおり、平成 23 年に入ってからは緩やかな伸びしかなかったため、これらの資料を元にして平成 23 年 9 月 1 日から STEP2 に移行することを決定し実行することとなった。

5.3 STEP2 における実施台数と STEP3 および STEP4 について

STEP2 とは、図 3 の第 2 段階であり、第 4.2 節の内容である。学内 LAN 利用にあたっては、ネットワーク認証と検疫を実行する必要がある期間である。よって、認証は必ず必要だが、ネットワーク接続検疫結果は問わない。実施期間は STEP3 までの平成 23 年 9 月 1 日から平成 23 年 10 月 18 日までである。

図 4 において、STEP2 初日の平成 23 年 9 月 1 日では実施台数約 1,100 台と、STEP1 の最終台数より少なくなっている。これは STEP2 を実行するにあたりより正確な台数を把握したいため、検疫システムのデータベースを一度リ

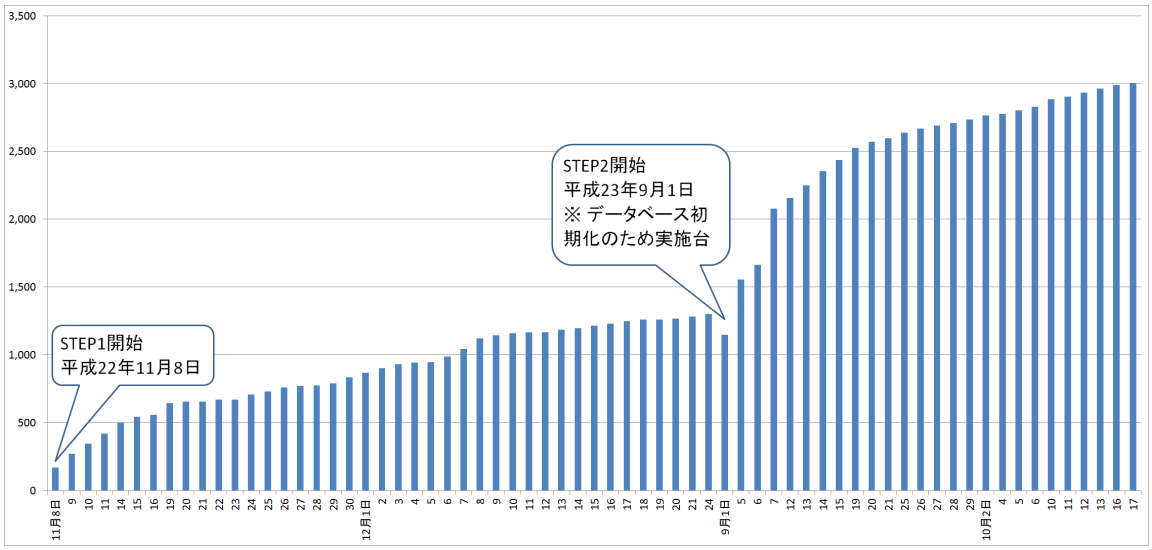

図 4 STEP1 および 2 における実施台数の伸び

セットしたためである。また、このグラフ以降大幅な増加はなく緩やかな伸びを続け、平成 25 年 1 月現在総実行台数は約 3,800 台となっている。

なお、STEP3 と STEP4 については、STEP2 を実施した段階で検疫のシステムの実行や除外申請など、システムを実行するという大きな段階を終えており、残りの要素として第 3.2 節のセキュリティ基準（安全判定の基準）を満たすことが条件となる。これらの条件は、検疫実行台数の緩やかな伸び率とシステムを実行するという大きな段階は超えていることなどから、長い時間をかける必要性がないと判断して、STEP3 を STEP2 開始から約 2 ヶ月半後に開始し、STEP4（全面実施）を STEP3 開始後から約 3 週間後にそれぞれ開始した。

6. 障害

STEP4（全面実施）以降に大きな障害が 2 度発生した。障害発生時にはすべてもしくは多くの利用端末が検疫実行不可能となり、学内 LAN に接続することができなくなった。このような障害発生時において復旧に時間がかかると判断した場合には、対象のネットワークスイッチに対してネットワーク認証と検疫の無効化を設定する。対象スイッチは約 200 台、設定にかかる時間はおおよそ 15 分である。設定を戻す際にはあらかじめ日時を広報しておき、その日時にネットワークスイッチに対して再度設定を行う。

1 つめ障害は、定期メンテナンス後に発生した。原因は検疫のデータベースを冗長化するためのソフトウェアに不都合が生じたためで、結果として検疫データベースが起動できない状態となった。よって、全ユーザが学内 LAN に接続することができなくなった。障害発見後直ちに対象のネットワークスイッチに対してネットワーク認証と検疫の無効化を設定し、後日復旧した。

2 つめの障害は、検疫システムバージョンアップ後に発生した問題で、多くの Windows 端末で検疫を行うことができなくなった。原因は、検疫システムをバージョンアップした際に Internet Explorer の ActiveX プログラムもバージョンアップされており、利用端末において検疫を実行しようとするとキャッシュに残っている古い ActiveX のプログラムを使用して検疫を実行しようとしたために、検疫を実行できずにエラーとなっていた。Internet Explorer のキャッシュをクリアすれば検疫を実行することはできたが、すぐにこのことが原因であると判断することができなかったため、検疫を一時中断して対処した。障害発生同日中に対処方法の広報を行い、後日復旧した。

7. 最後に

第 4.4 節の STEP4（全面実施）から平成 25 年 1 月現在で 15 ヶ月が経過した。FUTURE4 の導入は平成 22 年 9 月だったが、STEP4（全面実施）までおおよそ 1 年と 2 ヶ月を要した。第 4.2 節の STEP2 でも約 1 年を要しており、ネットワーク認証と検疫システムの稼働についてはそれだけ影響が大きく、かつ準備に多くの時間が必要であることが分かった。

今後の課題としては、第 5.1 節の表 3 を見ても分かるとおり、実施率が 71.2%であり未実施端末数が約三割ほどあることに疑問に残る。これは、機器接続申請をしたものの未使用の IP アドレス数なのか、かつては使用されていて現在は使用されていないのか、他に何か理由があるのか定かではない。この実施率がどのような意味を持っているのか、調査を行っていきたい。また、除外の申請数も 1,226 件と非常に多い。これは、iOS や Android、Linux などの検疫できない OS について除外申請を出す必要があることに起因していると思われる。一つ一つ除外申請を提出しなくてもある程度自動的に OS を判別して、検疫を実行する必要があるのかどうか判断できるようなシステムにしていきたいと思う。加えて、現在は検疫システムをまずは実行するために、申請はすべて紙ベースとして処理を行っている。これをオンラインで申請でき即時反映ができれば、利用者の利便性も大幅に向上する事になるため、これらのシステムについても検討を行っていきたい。

なお、これだけの規模でこのネットワーク認証と検疫システムを導入できたことは、システム構築スタッフ、事務スタッフはもとより、利用者一人一人のセキュリティに対する意識が向上した事の結果であることは間違いない。今後も引き続き、セキュリティのレベルを向上させつつ、利便性も同時に向上をさせ続けていきたいと考えている。

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
[2] 藤村 丞、奥村 勝、中國 真教「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」、I4-1、大学 ICT 推進協議会、2012 年度年次大会論文集、2012 年 12 月