2008－IOT－2 (8)
2008／7／25

学生宿舎への認証・検疫ネットワークシステムの導入

佐藤 聡[†1] 横山憲彦[†1] 真中剛司[†1]
中井央[†1] 片岸一起[†1] 板野肯三[†1]

約4000室からなる筑波大学学生宿舎用の情報ネットワークシステムの構築と運用について報告する．このシステムの運用については，いままでのキャンパスネットワークシステムとは異なり，トラフィック量のピーク時刻が運用担当者の勤務時間外であることと，単一のネットワークに接続される端末数が大規模であること，それらの端末が学生の所有物であるなどの特徴を有している．検疫・認証システムを導入して，学生宿舎用情報ネットワークシステムを安定的に運用することを試みている．本稿では，学生宿舎用の情報ネットワークシステムの詳細とその運用状況について報告する．

Case Study : Installation of Authentication and Quarantine Network System for Student Residence Hall

Akira Sato,[†1] Norihiko Yokoyama,[†1] Takeshi Manaka,[†1]
Hisashi Nakai,[†1] Kazuki Katagishi[†1] and Kouzo Itano[†1]

We report on the construction and operation of information network system for Student Residence Hall of University of Tsukuba which consist of about 4000 rooms. The operation of this system is different from one of the current campus network systems. This system has the following features; a traffic peak time of this system is outside of working hours of parsons in charge, the number of terminals connected to this system is large-scale, and those terminals are students' ownership things. We are trying safely and sustainable operation of this system by using the authentication and quarantine system. In this paper, we describe the details and the operation situation of this system.

1. はじめに

筑波大学では，約4000室のからなる学生宿舎を有している．この室数については，国立大学法人の中では最大である．近年，インターネット接続環境は大学生が教育，研究活動を行う際に必要不可欠なものとなってきている．筑波大学では，新入生が多数入居する学生宿舎に対してもインターネット接続環境を提供することは重要と認識している．2007年度までには，無線LANを中心としたネットワーク環境を提供していた．全室に情報コンセントを配備したシステムを導入する必要があると判断し，その運用，構築について，本学において教育と研究のための学内の情報基盤の整備と運用を行う役割を担っている学術情報メディアセンターが担当することとなった．

学生宿舎用の情報ネットワークシステムでは，キャンパスネットワークシステムとは異なる以下のような特徴がある．

- 利用される主な時間帯が平日夜間，休日であり，これらは運用を担当する職員の勤務時間外であること．
- 居室が約4000室あり，それぞれの居室から一台以上の端末を接続してくる可能性があること．
- それらの端末は学生の所有物であること．すなわち，想定される端末の種類は限定できず，また，ネットワーク接続に対して，必要となるソフトウェアの費用負担はできる限り最小限にする必要があること．

これらの特徴を踏まえて，できる限り安全かつ安定的な運用を行うために，我々は，認証・検疫ネットワークシステムを学生宿舎用情報ネットワークに導入し運用することを試みている．2007年度後半から構築を行い，2008年度初めから運用を開始し，現在までに約3ヶ月運用を行ってきた．本稿では，構築の詳細，および運用状況について報告する．

2. 筑波大学の学生宿舎

筑波大学では，学生に良好な勉学の環境を提供し，自律的な市民生活を体験させることを目的として学生

†1 筑波大学学術情報メディアセンター
Academic Computing and Communications Center, University of Tsukuba

宿舎を設置している．学生宿舎は一の矢地区，平砂地区，追越地区，及び春日地区に計 60 棟があり，個室 3482 室，2 人室 327 室，世帯室 186 室がある．

宿舎の各居室にはベッド，机，椅子，洗面台，宿舎内線電話等が備えつけられ，生活に必要な身の回り品等を揃えれば生活できるようになっている．宿舎各棟に談話室，洗濯室，補食室なども併設されている．また，春日地区を除く地区の共用棟には，食堂，浴場，売店，理・美容室など日常生活に必要な施設が設けられている．

学生宿舎については，学群[*1]の新入生及び留学生の入居希望者が優先的に入居できるように配慮されている．

2.1 学生宿舎へのネットワーク配備の変遷

2000 年度に初めて，学生宿舎については情報ネットワークが整備された．当時，図書館情報大学の学生宿舎であった春日地区については，各個室に情報コンセントを配備し，情報コンセントに接続したネットワーク端末を認証せずにキャンパスネットワークに接続可能とした．一方，一の矢，平砂，追越地区の共用棟には IEEE802.11b に対応した無線 LAN のアクセスポイントを配備し，それらを集線する位置にファイアウォール装置を配備し，アプリケーションレイアでの認証の仕組みをファイアウォール装置が代行する方式を用いて，許可された利用者が用いているネットワーク端末のみを特定のプロトコルだけ許可してキャンパスネットワークに接続可能としていた．

2002 年度の大学統合に伴い，4 地区の全ての学生宿舎のネットワークの統合的管理を行うように構成変更を行った．その際に，4 地区の学生宿舎のネットワークを集線する位置に認証機能付きの L2 スイッチを配備し，その認証機能を用いて，許可された利用者が用いているネットワーク端末のみをキャンパスネットワークに接続可能とした．このとき利用できるプロトコルに関する制限を緩和した．

2006 年に一の矢，平砂，追越地区のアクセスポイント不足を解消するために，いくつかの建物の屋上にワイヤレスメッシュネットワーク装置を配備し，屋外からの無線 LAN によるネットワーク運用試験を開始した．このワイヤレスメッシュネットワーク装置は L3 での運用が必須であったため，既存の L2 スイッチの認証機能を使うことができず，このシステム専用にファイアウォール装置を導入し，その装置の認証機能を用いて，許可された利用者が用いているネットワーク端末のみをキャンパスネットワークに接続可能とした．

2.2 統一認証システム

筑波大学では 2006 年度からいくつかの計算機システムにおいてパスワードを共通化し，同じパスワードで統一的に認証が行えるようにしている．これを「統一認証システム」と呼んでいる．統一認証システムにより共通化されたパスワードの変更や登録されている情報の閲覧は統一認証システムのウェブサイトで行うようになっている．これらは LDAP を用いてパスワードを管理している．統一認証システム用の ID が発行され，それぞれの計算機システムなどでは，その ID とそれぞれのシステムのアカウント名をマッピングすることでパスワードの共通化を実現している．

学生宿舎に設置された無線 LAN システムの認証には当初，教育用計算機システムのアカウントとパスワードを利用していたが，統一認証システムが稼動してからは，統一認証システムの ID とパスワードを利用している．

2.3 大学が提供する以外のインターネット接続環境

学生宿舎において提供されているインターネット接続環境としては，以下のようなものが利用可能であるが，どれも帯域が小さいという課題が存在していた．

- 携帯電話や PHS 等
- 宿舎内線電話システムを用いた DSL 接続サービス

光回線やケーブルテレビによる接続サービスなどが近隣の地域では利用可能であった．しかしながら，宿舎全体でそれらのインフラを整備するためには宿舎の建物数が多いために多額の設備投資が必要となることもあり，サービス提供側は学生宿舎をサービス対象予定地域としていない．

3. 学生宿舎用の新しい情報ネットワークシステム

学生宿舎におけるより高速なインターネット環境の整備に対する学生からの要求の高まりを受けて，筑波大学は，2006 年度に，一の矢，追越，平砂の各地区の学生宿舎に対しても，春日地区の学生宿舎と同様に，各個室に情報コンセントを整備するとの大方針を決定した．これに伴い，学生宿舎用の新しい情報ネットワークシステムの設計および導入後の運用については学術情報メディアセンターが行うこととなった．

学術情報メディアセンターでは，学生宿舎用の新しい情報ネットワークシステムの設計にあたり，限られた人的資源の中で，他のキャンパスネットワークシステムと同様に，できる限り安全で安定的な運用が可能となるように，この新しいシステムの特徴を考慮して，以下のような目標を定めた．

- 多数のパソコンが接続されるネットワークの利用者を把握する．
- ウィルス感染等を含む不正な利用形態によるネットワークの不安定化を最小限に留める．

この詳細目標を達成するために，認証・検疫ネットワークシステムを導入し，管理，監視等については既設のキャンパスネットワークシステムと一元的に行え

---

*1 筑波大学では，他大学における学部段階の学生に教育を行う組織のことを学群と呼ぶ．

るように設計を行った．

まず，春日地区の学生宿舎では既設の情報コンセントを用い，一の矢，平砂，追越地区の各居室では情報コンセントを新たに設置することにした．そして，4地区とも，情報コンセントを集線するスイッチ群，認証検疫システムを新たに導入し，既設の認証システムと連携し，全体のシステムとして構築することとした．新たに導入する装置の生存監視やログ管理などは，キャンパスネットワークシステムに統合する形をとった．これらのシステム構築作業は2007年度末までに実施し，2008年度初めから運用を開始する計画を立てた．このシステムの新規部分については，機能，性能について設計を行い，その設計に基づいて入札が行われ，利用する機器の詳細が決定した．また，構築作業当初は，ネットワークアクセス制御の部分には，キャンパスネットワークシステムにおける基幹スイッチが有するアクセス制御機能を用いる予定であったが，キャンパスネットワークシステム全体の安定的な運用を考慮し，その制御機能を実現するファイアウォール装置を追加導入した．

3.1 システム構成

3.1.1 認証検疫システム

認証検疫システムとしては，Nortel社製Secure Network Access Switch 4050[4](以下，SNASと呼ぶ）を用いている．この製品の特徴は，ネットワークを構成するL2/L3スイッチの機能を用いて3つのネットワークに分割しておき，認証・検疫を受けるネットワーク端末をその結果に応じて，3つのネットワークの何れかに所属させることとを制御している点にある．3つのネットワークとは以下の通りである．

- ネットワーク端末に対して，認証と検疫を行うために一時的に所属させておくネットワーク．
- 認証と検疫が成功したネットワーク端末を所属させるネットワーク．
- 認証は成功したが，検疫に問題があるネットワーク端末を接続させておくネットワーク．

SNASでは，ネットワーク端末に予め特殊なソフトウェアのインストールをする必要がなく，認証を受ける際にアクセスするポータルサイトからダウンロードされるJAVAアプレットがネットワーク端末の情報取得を行う．現在のバージョン(1.6)では，Windows2000/XP/VISTA，MacOS，Linuxに対応している．また認証にはRADIUSサーバとの連携が可能となっている．

SNASにおけるネットワークを切り替える方法は，ネットワークスイッチのポートVLANを切り替える方法と，ネットワーク端末に払い出すIPアドレスレンジを切り替える方法の2種類がサポートされている．前者の場合は，SNASが認証・検疫を行っているネットワーク端末の情報からそのネットワーク端末が接続されているネットワークスイッチのポートを調査し，そのネットワークスイッチに対して，そのポートの所属するVLANを変更する命令を発行する．この方法では，ネットワークスイッチのVLANに対してアクセス制限を予め設定しておく必要がある．後者の場合は，SNAS自体がDHCPサーバとしても稼動する．ネットワーク端末側で稼動しているアプレットからDHCPのアドレス再取得命令をオペレーティングシステムに発行する*1．その結果，その端末はSNASにアドレスの再取得要求を行う．SNASはネットワーク端末の認証結果，および検疫結果に基づいて再度払い出すIPアドレスのレンジを決定する．この方法では，ネットワークスイッチのアクセスコントロール機能を用いて，各々のIPアドレスレンジにおいてアクセス可能なネットワークを設定しておく必要がある．

SNASでは以下のようなものを検疫の対象とすることができる．

- ディスク上のファイル（ファイル名，パス，ファイルサイズ，日付，チェックサムなど）
- メモリ上のプロセス（プロセス名，ロードパス，サイズ，日付チェックサムなど）
- レジストリの項目および値など

本学では，学生宿舎に設置される情報コンセントに複数台の端末が接続される可能性があること，及び，情報コンセント数が大量であることから，ネットワーク切り替えの方法については，ネットワーク端末に払い出すIPアドレスレンジを切り替える方法を用いた．また，アクセス制限を実施するために学生宿舎のネットワークとキャンパスネットワークの境界点にファイアウォールを設置した．

3.1.2 集線スイッチ

集線スイッチとしては，各建物の情報コンセントを階を単位として集線するための階用集線スイッチとしてFXC社製のESシリーズのイーサネットスイッチ製品[1]を，また，それらのスイッチの上流接続を集線する棟用集線スイッチとして，H3C社製のS5500シリーズのL3スイッチ製品[2]を用いている．階用集線スイッチはL2スイッチとして運用している．棟用集線スイッチもL2スイッチとして運用しているが，監視機能を用いて階用集線スイッチ間の接続監視をしている．

3.1.3 ファイアウォール装置

ファイアウォール装置としては，Juniper Networks社製SSG 350[3]を用いている．前述の通り，このファイアウォール装置では，SNASが切り替える3つのIPアドレスレンジ毎に，それらを発信元，または，送信先となるセッションに関しての制限をするために用いている．

---

*1 この命令を実行するためにいくつかのオペレーティングシステムでは，管理者権限が必要になる．

3.2 検疫の運用ポリシー

検疫において，主要なセキュリティ製品がインストールされていることを検疫対象にすることも可能であったが，それを必須項目とした際の学生への費用負担を考えて，今回はセキュリティ維持に対し最低限学生にお願いしたい，セキュリティパッチの更新を自動化するように設定していることを検疫対象とした．通常，セキュリティパッチはオペレーティングシステムの開発元から無償で提供されており，これを適用することにより学生に費用的負担をかけることがないと判断したためである．ただし，現在のバージョンでは，Windows 以外のオペレーティングシステムに関しては，それを検疫対象とすることができないため，今回は Windows のみを対象とした（すなわち，MacOSX, Linux については検疫を行っていない）．

3 つのネットワークについては，ファイアウォール装置にてそれぞれ異なるアクセス制限をするようにしている．検疫に成功した時に接続されるネットワークに対しては，ほぼ制限はしていない．検疫に問題が発生した時に接続されるネットワークに対しては，検疫に成功した時に接続されるネットワークと同等の制限のみをかけている．利用者からみれば，検疫ポリシーに違反していても，警告がでるだけで，利用上に問題がない設定にしている．認証を行うために接続されるネットワークからは，学内の一部の Web サーバのみアクセス可が可能となっている．

3.3 運用体制

学生宿舎用情報ネットワークシステムの障害対応は，学術情報メディアセンターのネットワーク担当技術職員（2 名）および事務職員（4 名）が，キャンパスネットワークシステムの障害対応等の通常業務と併行して行っている．具体的な対応としては，窓口専用の電話番号に対する対応，及び，窓口専用のメールアドレス宛てのメールによる回答，および直接対面による対応である．これらの対応は，電子メールの受付を除いて，平日の 8 時半から 17 時までとした．故障等の機器の取替えなどについても，平日に，学術情報メディアセンターのネットワーク担当職員が対応することとした．ただし，学生宿舎入居後約 1ヶ月強（4 月 1 日から 5 月 11 日まで）には問い合わせが多数起こることを想定し，障害対応窓口をアウトソースした．対応時間は平日夜（17 時から 20 時まで）と休日の昼（10 時から 18 時まで）とした．障害発生をアナウンスする手段として，携帯電話から閲覧できる Web ページを作成し，機器運用状況を速報するようにした．接続手順や，障害対応窓口に関する情報等をまとめたリーフレットを作成し，学生宿舎の入居時に配布した．

3.4 現　　状

3.4.1 利用状況

図 1，**図 2**，**図 3**，**図 4** に，順に一の矢，平砂，追越，春日の各地区の学生宿舎全体の過去 1 年間のトラフィック量の推移のグラフを示す．これらのグラフは，各地区への回線を収容しているキャンパスネットワーク側の基幹スイッチ側にて測定した結果を示している．また，一の矢地区，平砂地区，追越地区の 3 地区を収容している基幹スイッチは冗長構成となっており，それら 3 地区は地区ごとに 2 回線で接続されている．グラフは 1 回線ごとの流量の測定結果を表しているため，3 地区についてはグラフは二つづつとなる．また，この基幹ネットワークは昨年の 9 月にリプレイスを行ったため，9 月以降のデータが収集されている．

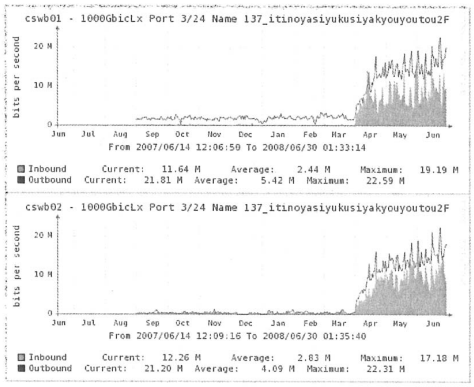

図 1　一の矢地区のトラフィック量の推移
Fig. 1　Traffic graph of Ichinoya residence hall

各地区毎のトラフィック量をまとめると以下の表のようになる．

区分		最大値	平均値
一の矢地区	流入量	約 45Mbps	約 9Mbps
	流出量	約 36Mbps	約 5Mbps
平砂地区	流入量	約 49Mbps	約 2Mbps
	流出量	約 30Mbps	約 4Mbps
追越地区	流入量	約 30Mbps	約 5Mbps
	流出量	約 27Mbps	約 3Mbps
春日地区	流入量	約 13Mbps	約 3Mbps
	流出量	約 7Mbps	約 1Mbps

地区毎のトラフィック量は部屋数とほぼ相関があるといえる．またどの地区においても，4 月にトラフィック量が増えており，その後も増加か傾向にあるといえる．また，一日におけるトラフィックの推移を観察したところ，トラフィックのピークは夜間となっており，当初の想定どおりになっていることが確認できた．

図 5 に，一日毎の利用された端末の総計と利用した延べ回数の総計の推移のグラフを示す．このグラフより，現在は一日平均約 1500 台の端末が接続をしており，1 台あたり 2 回以上利用していることがわかる．また，統一認証のパスワード配布が行われた 4 月 8 日以降から利用数が増えており，ゴールデンウィークを除いてほぼ利用数は増加傾向にあることがわかる．学

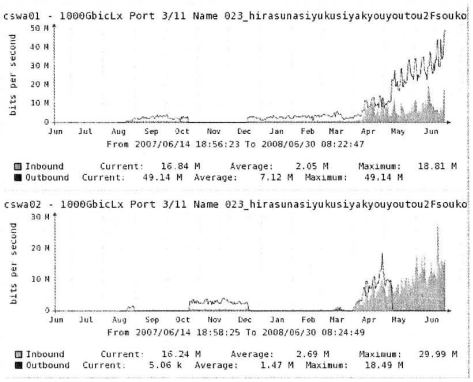

図 2　平砂地区のトラフィック量の推移
Fig. 2　Traffic graph of Hirasuna residence hall

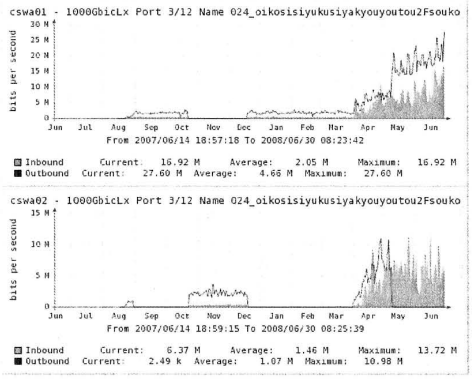

図 3　追越地区のトラフィック量の推移
Fig. 3　Traffic graph of Oikoshi residence hall
Fig. 3　English caption

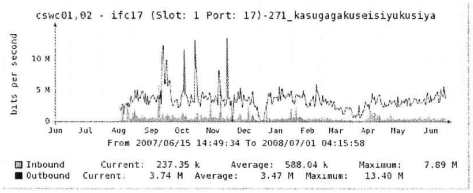

図 4　春日地区のトラフィック量の推移
Fig. 4　Traffic graph of Kasuga residence hall

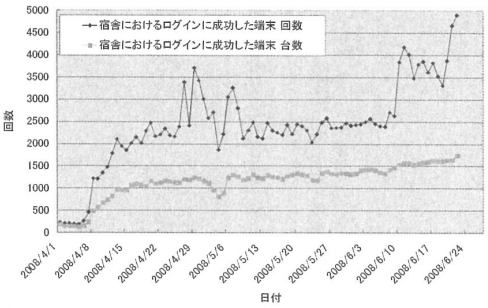

図 5　利用回数の推移
Fig. 5　Graph of use frequency

生宿舎は約 4000 室から構成されていることからも，増加傾向は今後も続くことが予想される．

3.4.2　障害の発生状況

4 月 1 日からの運用開始後，新しい学生宿舎用情報ネットワークシステム全体の運用が不安定になるような障害については 2 回発生している．

そのひとつの事例は，学生によるブロードバンドルータの間違った接続によるものであった．新しいシステムでは，認証を受けた端末がシステムから払い出される IP を直接受け取る必要があるため，ブロードバンドルータは利用できない．この事例では，ブロードバンドルータの LAN 側ポートを情報コンセントに接続したために，システム以外の DHCP サーバが起動したことになり，このサーバにより IP アドレスの払い出しを受けた端末が利用不可能になったものである．これについては，棟用集線スイッチに DHCP SNOOP 機能があるため，今後はスイッチの性能をみながらサービスポートに対してその設定を有効化することを検討している．

もうひとつの事例は，ウィルスに感染している端末がネットワークに接続された．ウィルスにより，IP アドレスを詐称して不正な通信を実施したために，ファイアウォール装置が過負荷状態になり，正規利用の通信に影響を与えてしまった．これについても，棟用集線スイッチに送信元 IP ガード機能があるため，今後はスイッチの性能を見ながらサービスポートに対してその設定を有効にすることを検討している．

これらの障害についての問題点は，認証していない端末が不正利用をした場合に，その発生源を遠隔地から部屋単位で特定できないことである．現在末端に接続している集線スイッチは単純な L2 スイッチであり，遠隔監視ができない．これについては台数も多く，アップグレードすることは金銭的負担が大きいため，実現しにくい．運用方法でこれをカバーする方法について現在検討しているところである．

それ以外の障害としては，階用スイッチの故障が数

件発生している．

3.5 窓口対応の状況

窓口対応については，入学式直後からほぼ2週間，30件程度の問い合わせがあった．その後，ゴールデンウィークまでは毎日20件程度あり，ゴールデンウィーク後には多い日で10件程度，6月以降は多い日で5件程度の問い合わせとなり，問い合わせ回数は導入から日が経つにつれて少なくなる傾向である．しかしながら，問い合わせ内容がより高度な障害となってきており，1件あたりの対応時間は長くなる傾向にある．

導入後約1ヶ月間の窓口業務をアウトソースしたが，その際に作業日報の提出を依頼した．その日報を集計した結果を以下に示す．

相談内容	件数
ID/PW にて login できない	5
JRE がインストールできない	16
login 画面が表示されない	2
検疫作業中に停止する	38
システム自身に対する問い合わせ	74
その他	50

3.6 課　　題

学生宿舎用の情報ネットワークシステムに認証・検疫システムを導入して，安定的なネットワーク運用を試みて，3ヶ月が経過してきた．その経験をもとに今後検討していきたい課題について述べる．

JRE のインストール

この認証・検疫システムを使うためにはJAVAの実行環境(JRE)が必要になる．最近のオペレーティングシステムにはJREは含まれていないため，初めてPCを購入した学生はJREのインストール作業が必要になる．この作業によるトラブルも発生しているため、インストール作業をサポートする仕組みが必要になる．

多言語対応

筑波大学の学生宿舎には多数の留学生が入居している．しかしながら，認証の際にアクセスするポータルサイトは1言語の表示しかサポートしていないために，ユーザビリティが若干低下している．また，JAVAの言語設定とOSの言語設定の不一致による障害が発生し，問題解決が複雑化している．

多様性への対応

オペレーティングシステムごとに設定や推奨されるブラウザの起動方法が異なり；その結果，接続できない事例が多数発生した．オペレーティングシステムや利用しているブラウザなどを解釈してガイドを表示するシステムの開発が必要である．

セキュリティソフトへの対応

セキュリティソフトによっては，ポータルサイトのアクセスを不正なアクセスと判断し，接続できない事例が発生した．また，このシステムにおいてダウンロードされるJAVAアプレットが不正なプログラムと判断され，実行されない事例などが発生した．

ノウハウ/FAQ の整備

設定ミスや起動方法のミスによる障害回復において，若干のノウハウが必要となり，そのためのガイドラインなどを整備する必要がある．

検疫の運用ポリシーアクセス制限の見直し

現在，不正なポートスキャンが行われているとの報告がある．また，今後コンテンツを中心とした次世代ネットワークに適した利用形態に変化することなどが予想される．これらの考慮して，運用ポリシーや検疫に問題のあるネットワーク端末が接続されるネットワークのアクセス制限について見直しをする必要がある．

4. おわりに

約4000室からなる筑波大学学生宿舎用の情報ネットワークシステムの構築と運用について報告した．このシステムでは，認証・検疫ネットワークシステムを導入し，安定的に運用することを試みている．運用開始後3ヶ月間の運用状況について，障害の内容や窓口対応の内容等について述べた．それらを通して，よりよいシステムにするための課題等についてもまとめた．今後は，本稿で述べた課題について一つ一つ対応策を検討し，実施していく．

参考文献

1) FXC: FXC 製品一覧，http://www.fxc.jp/products/index_fxc.html (Accessed 2008 Jul 1).
2) H3C: S5500 シリーズ・スイッチ，http://www.h3c.jp/jp/Products%5F%5F%5FSolutions/Products/Switches/H3C%5FS5500%5FSeries%5FSwitches/ (Accessed 2008 Jul 1).
3) Juniper Networks: Juniper Networks SSG 300 Series Datasheet，http://www.juniper.net/products/integrated/dsheet/100203.pdf (Accessed 2008 Jul 1).
4) Nortel: Secure Network Access Switch(SNAS) 4050 概要，http://products.nortel.com/go/product_content.jsp?segId=0&parId=0&prod_id=55260&locale=ja-JP (Accessed 2008 Jul 1).