# 福岡女子短期大学における多層防御による情報セキュリティ対策の強化

古市 恵美子 [1)], 牧 幸浩 [2)]

1) 学校法人九州学園　情報処理室
2) 福岡女子短期大学

furuichi@fukuoka-int-u.ac.jp

# Security Enhancement by the Second Firewall Controlling Packets at Application Level

Emiko Furuichi [1), 2)], Yukihiro Maki [2)]

1) Kyushu Gakuen, Management Office of Network and Computer Systems
2) Fukuoka Women's Junior College

**概要**

九州学園では、全学ファイアウォールを導入して学内ネットワークの情報セキュリティ向上に努めている。しかしながら、2015 年の標的型攻撃の増加などにより、それまでの外部からの攻撃の防御を目的とするファイアウォールだけでは不十分であるとの結論に至り、2016 年 4 月より内部から外部への通信を可視化できるファイアウォールを追加してさらなる情報セキュリティ対策の強化に努めている。本稿では、新しく導入した出口対策用ファイアウォールの役割と運用状況、あわせて学内のセキュリティ教育について報告する。

## 1　はじめに

福岡女子短期大学（以下「短大」という。）の学内ネットワークと教育用情報システムは、学校法人九州学園・情報処理室によって「九州学園総合情報ネットワークシステム」の一部として管理・運用されている。ファイアウォール等のセキュリティ製品や教育用情報システムは、約 5 年ごとにリプレースが行われており、現在のシステムは2014年3月に更新されたものである[1]。学外との接続点に全学ファイアウォールを設置して学内ネットワークを防御することで、情報セキュリティ対策に努めている。

2014 年のシステム更新以降も組織に対するサイバー攻撃は巧妙になっており、日本年金機構の個人情報流出事件に代表されるような標的型攻撃や未知の脅威などが急増している。標的型攻撃による被害の多くは、電子メールに添付されたファイルの開封やウェブサイトの閲覧によるウイルス感染が原因である。ウイルス感染したコンピュータは外部と通信するため、内部のコンピュータがウイルス感染した場合の被害を防ぐには、学内から学外への通信を管理する必要がある。この管理は、入口対策を担う全学ファイアウォールでは困難である。こうした脅威に対応するために、出口対策の必要性が確認され、学内から学外への通信を管理する出口対策用のファイアウォールを導入することが決定された。一方、ウイルス感染を防ぐには、利用者がウイルスに関する知識とその対策を知ることも重要である。そのための利用者への情報セキュリティ教育を定期的に実施することにした。

本稿では、2016 年 4 月から運用を開始した出口対策用ファイアウォールと以前から運用していた入口対策用ファイアウォールによる多段のセキュリティ対策、教職員や学生のセキュリティ意識を向上させるための利用者教育など、本学の多層防御を考慮したセキュリティ対策の強化について報告する。

## 2　ネットワーク構成

本学のネットワークは、1Gbps の専用回線で SINET に接続しており、SINET との接続に使用しているルータの下に全学ファイアウォールを設置して学内ネットワークを防御している。さらに、学内ネットワークのコアスイッチとの間

には、パロアルトネットワーク社のファイアウォールを設置している。学外からアクセスできるのは、DMZ に設置しているウェブ／メール／DNS サーバと Moodle サーバのみである。

図 1 にネットワーク構成の概要を示す。

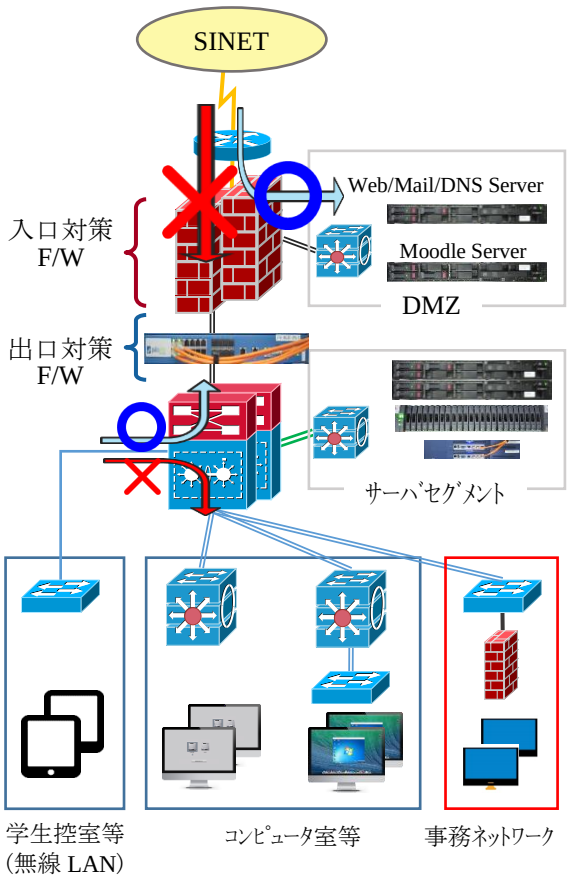


図 1 短大ネットワークの概要図

学外からアクセスする必要のない学内用 DHCP/DNS サーバや認証サーバは、学内ネットワーク内のサーバセグメントにまとめて設置している。本学では、研究室で独自のサーバを設置することはほとんどない。DMZ 及び学内のサーバセグメントに配置したサーバは、全て情報処理室で一元的に管理している。

事務ネットワークは、専用ファイアウォールを介して学内ネットワークに接続されている。事務ネットワークから外部への通信は可能だが、学内ネットワークからアクセスできるのは事務専用ファイアウォールの DMZ に設置されたウェブサーバのみである。

学生が自由に使用できる無線 LAN は、学生控室や食堂に設置しているが、セキュリティを考慮してインターネットへの通信のみ許可しているため学内ネットワーク内には通信できない。

学内ネットワークに接続する機器は、セキュリティポリシーの規定により、全て MAC アドレスを登録しなければならない。これにより、学内ネットワークに接続される機器を一元的に管理している。ただし、学生用の無線 LAN は、使用時に認証させるため、MAC アドレスを登録せずに使用できるようになっている。

## 3 情報セキュリティ対策

### 3.1 全学ファイアウォールによる入口対策

学外と学内ネットワーク間の通信を管理している全学ファイアウォールは、2014 年 3 月のシステム更新時に導入した Fortinet 社の FortiGate で運用している。FortiGate は、ファイアウォール機能のほか、次のような機能を使って学外からの侵入を防ぐ入口対策を担っている。

- スパムメール検知
- アンチウイルス
- 不正侵入防御

学外から学内への通信は、原則としてファイアウォールで全通信を遮断している。学外から DMZ への通信は、ウェブ、メール、DNS サービスへの通信を許可している。事務ネットワークは学内ネットワーク内にあるため、学外から事務システムに直接アクセスすることはできない。DMZ から学内への通信は許可していない。

学内から学外への通信は、ウェブ閲覧等の一部サービスのみ許可し、それ以外の通信については遮断している。学内から DMZ に対しては、DMZ のウェブサーバやメールサーバにアクセスするため、学内から学外へのポリシーとは異なるポリシーを適用しており、ウェブ閲覧のほかにメールやリモートアクセスに関するサービスへの通信を許可している。

ファイアウォールのログは、FortiAnalyzer で収集と分析を行い、分析結果から得られた情報をセキュリティ対策の見直しに利用している。

### 3.2 出口対策

本学の情報システムを更新した 2014 年 3 月

以降、2015 年の日本年金機構の個人情報流出事件にみられるように、標的型攻撃や未知の脅威などが急増した。こうした脅威には全学ファイアウォールの入口対策としての機能だけでは対応できず、学内から学外への通信を監視し、個人情報等の漏えいを防いだり、マルウェアが外部と通信することを防ぐための出口対策が必要になった。

全学ファイアウォールに URL フィルタリング機能やサンドボックス機能を追加して未知のマルウェア対策や危険なウェブサイトへのアクセスを遮断することも検討したが、スパムメールやアンチウイルス等の機能をすでに利用していたことから、さらなる機能追加はスループット低下によりファイアウォールとしての運用が難しくなる可能性があった。このため、全学ファイアウォールを学外から学内への侵入を防御する入口対策用とし、学内から学外への通信を監視する出口対策用として、パロアルトネットワークス社のファイアウォール PA-3020 を導入することを決定した。選定にあたり評価したのは、アプリケーションレベルで通信を確認・制御できることと、いろいろな機能を利用してもスループットが低下しない点だった。

2016 年 4 月に運用を開始したファイアウォールの役割は、次のとおりである。

- 学内ネットワークから学外へのユーザ単位の通信をアプリケーションレベルで確認・制御。危険な通信やアプリケーションを遮断。
- URL フィルタリングを利用してマルウェアサイト等への通信を遮断。事務ネットワークからは、業務に必要のないウェブサイトへの通信も遮断。
- 既知のマルウェアをブロック。全学ファイアウォールで検知できないウイルスについても、入口対策と異なるアンチウイルス機能で防御。
- 未知のマルウェア等に対して、サンドボックス環境の WildFire で対応。

### 3.3 多層防御

ファイアウォールによる入口対策や出口対策に加え、利用者に次のようなルールを守ることを徹底させることで多層防御を行っている。

- 学内ネットワークに接続する PC にはウイルス対策ソフトを導入し、定義ファイルを更新して常に最新の状態にしておくこと。
- ウイルス対策ソフトを使い、ディスク等のウイルスの完全スキャンを定期的に実施すること。
- OS やアプリケーション等のソフトウェアに脆弱性が発見された時は、ソフトウェアを更新し、脆弱性のない状態で PC を使用すること。
- 学内ネットワークに接続する PC で使用するソフトウェアは、正規ライセンスを使用すること。業務 PC にソフトウェアをインストールする必要がある場合は、管理者に相談すること。業務 PC 以外の場合は、インストールされたソフトウェア名とシリアル番号を登録すること。

### 3.4 運用管理

本学では、セキュリティ業者等への委託による不正アクセス等の 24 時間監視は行っておらず、全学ファイアウォールの不正侵入検知／防御機能で不正アクセス等を監視している。監視対象を少なくするため、全学ファイアウォールに厳しいポリシーを適用して学外から学内ネットワークへの全通信を遮断している。これにより、監視対象をファイアウォールと DMZ に設置しているサーバに限定している。サーバについては、攻撃対象になりやすいソフトウェアをインストールしないこと、ソフトウェアに脆弱性が発見された場合には早急に対応することなどで不正アクセス等のリスクを減らしている。

学内ネットワークの内部については、全学ファイアウォールのログの分析レポートで異常な通信をしているコンピュータが存在していないかを監視している。急激に通信量が増加するなど通常と異なる現象が発生した場合には、さらに詳細な通信状況を調べ、同時に出口対策用ファイアウォールにおいてアプリケーションレベルでの通信状況を確認するようにしている。

出口対策用ファイアウォールでは、侵入、ウイルス、スパイウェアなど各セキュリティのアラーム情報は「脅威」ログに記録される。未知

のマルウェアの疑いがあるものがみつかった場合には、サンドボックス環境で識別するため、「WildFire への送信」ログに記録される。また、「URL フィルタリング」ログには、特定のウェブサイトやウェブサイトカテゴリへのアクセスをブロック、または警告を生成した時の情報が記録される。導入から約半年経過した 9 月末までの各種ログの件数は、表 1 のとおりである。「脅威」ログについては、学外から入ってくるウイルスなどの検出やウェブサイトの攻撃になりそうなブラウザの通信のブロックなどで、重大なインシデントにつながるものはなかった。「WildFire への送信」ログからは、未知のマルウェアが少なからずみつかったことがわかった。

表 1　各種ログの件数

| ログの種類 | 件数 |
|---|---|
| 脅威 | 134 |
| WildFire への送信 | 43 |
| URL フィルタリングログ | 23,020 |

これらのログ等を使って、ボット感染の疑いがある端末を検知するためにボットネット検知機能がある。ボットネットの疑いありと判断されると、5 段階の信頼スコアを付けてリストアップされるようになっている。出口対策用ファイアウォールの導入直後には、ボットネット検知機能で、ウイルス対策ソフトで検出されないが学外と通信を頻繁に行うソフトウェアがインストールされた PC が発見された。このソフトウェアは、天気予報をデスクトップに表示するもので、悪意のあるサイトへ多数アクセスしようとしていたのを、URL フィルタリングでブロックされたことによりわかった。

導入から約半年間で、約 30 台が高いスコアでボットネットの疑いありとされたが、ほとんどは学生用 PC だった。学生用 PC には環境復元ツールがインストールされているため、一時的にウイルスを持ち込んでいたとしても、電源を切ると環境が復元される。今のところ、大きな問題にはなっていない。

出口対策のファイアウォールのログは、インシデント対応時にログが必要になることを考慮して約 1 年間保存できるようになっている。運用開始時には、大量のログが発生していたが、利用者に使用していないソフトウェアの削除や設定の変更を依頼したことにより、ログの量を減らすことができた。ただし、新しい OS やアプリケーションは外部と多数の通信を行うため、最近ログの量が増加している。ログの保存領域は限られているため、ログが長期間保存できない可能性が出てきた。

## 4 情報セキュリティ教育

日本の組織に対するネットワークを利用した攻撃は年々巧妙になっており、情報漏えい等の被害が後を絶たない。被害の多くは、メールの添付ファイルを開いたり、メール内のリンクをクリックしたり、ウェブサイトを閲覧したことによるウイルス感染が原因である。このようなウイルス感染による情報漏えいは、ファイアウォールのようなセキュリティ対策製品を導入しただけでは被害を防ぐことができない。ウイルス感染を防ぐには、利用者がウイルスに関する知識とその対策を知ることである。そのための利用者への情報セキュリティ教育が重要となる。本学では多層防御の一つとして、利用者教育を実施している。

### 4.1 教職員に対する教育

教職員については、総務省の「国民のための情報セキュリティサイト」[3]の内容をまとめ、「情報漏えいを防ぐために知っておくこと」と題した研修を行った。教職員一人ひとりが、個人情報を取り扱っているという事実を認識し、自組織のネットワーク環境を理解した上で、情報漏えいをさせないための方策を理解し実践することを目的とした。以下に研修の詳細を示す。

1. 情報セキュリティの重要性の認識
   - 学生、教職員の個人情報を取扱っているという責任を自覚
   - 過去の情報漏えい事例から、社会的な責任の重さを理解
   - 情報セキュリティ対策の必要性を理解
   - 情報漏えい対策に自覚を持って取り組む姿勢を養成

2. 自組織のネットワーク環境とセキュリティ対策の理解
   - 自組織のネットワーク環境の理解
   - 技術的なセキュリティ対策の理解
3. 情報漏えいをさせないための方策の理解と実践
   - 安全なパスワード管理
   - ウイルス対策
   - ソフトウェアの情報セキュリティ対策
   - メールの誤送信
   - 標的型攻撃への対策
   - 悪意のあるホームページ
   - アプリケーションのライセンスと利用規約の確認
   - ソフトウェアと著作権
   - 安全な無線 LAN の利用

定期試験によって学生の理解度を確認できる講義と異なり、教職員研修では理解度を把握することが難しい。2016 年に実施したセキュリティ研修では、その 2 週間後に行った e ラーニング研修の中で、セキュリティに関するウェブテストに解答させることで理解度を調べた。教職員 31 名が解答したウェブテストの結果は、平均 80 点であったため、教職員の理解度が高かったことを確認できた。問題の中で正解率が低かったものは、ボットの感染防止対策に関するものだった。ボットはウイルスのように一般的に使われる用語ではないため、なじみがなかったものと思われる。

### 4.2 学生に対する教育

短大の学生に対しては、1 年前期の「基礎情報科学演習 1」において情報セキュリティ教育を行っている。高校の共通教科「情報」に情報セキュリティの内容が含まれているが、入学時には高校で学習した内容を忘れている学生が多いため、入学後に学内ネットワークの利用法とあわせてセキュリティ教育を行っている。

著者らは、非常勤講師として短大の 4 つの学科（食物栄養科、音楽科、文化コミュニケーション学科、保育学科）のうち 2 つの学科の授業を担当している。担当している授業では、サイバー犯罪や情報セキュリティに関する最新情報を交え、次のような内容で情報セキュリティに関する教育を行っている。なお、最近はほとんどの学生がスマートフォンを所有しているため、無線 LAN の安全な利用方法を含めてスマートフォンの情報セキュリティについても教育するようにした。

1. サイバー犯罪について
   - インターネットの脅威
   - コンピュータウイルス
   - 迷惑メール
   - 不正アクセス
   - 詐欺等の犯罪
   - 個人情報の悪用
2. 情報セキュリティとは
3. 情報セキュリティ対策
   - ソフトウェアを最新状態に保つ
   - ウイルス対策
   - ID とパスワードの管理
4. SNS 利用上の注意
5. 無線 LAN を安全に利用するために
6. スマートフォンの情報セキュリティ

毎回の授業では確認テストを行っているが、前期の定期試験にも情報セキュリティを重点内容として含めることで、学生に情報セキュリティの重要性を認識させている。

### 4.3 情報セキュリティに関する学生の意識

短大では、2014 年から “情報機器の利用状況等に関する調査”[2]と題して、学生が日頃どのような情報端末を利用し、どのように活用しているのか、さらにコンピュータウイルスやコンピュータ犯罪に対してどのような意識を持っているかを調査している。このアンケートは、4 つの学科において「基礎情報科学演習 1」を履修後の 1 年生を対象に実施しており、2014 年は 166 名、2015 年は 156 名、2016 年は 159 名の回答を得た。

自宅 PC やスマートフォン等の携帯情報端末のセキュリティに関する集計結果からは、学生の情報セキュリティに関する意識がわかる。セキュリティに関する各設問と 3 年間の結果および考察を以下に示す。

設問 1 は、PC を対象としたセキュリティの意識を問うものである。

1. コンピュータウイルスやコンピュータ犯罪による被害が多数報告されています。あなたは PC (自宅、大学、インターネットカフェ等も含む)を使っていて、コンピュータウイルスやコンピュータ犯罪による被害を受けるのではないかという不安はありますか。

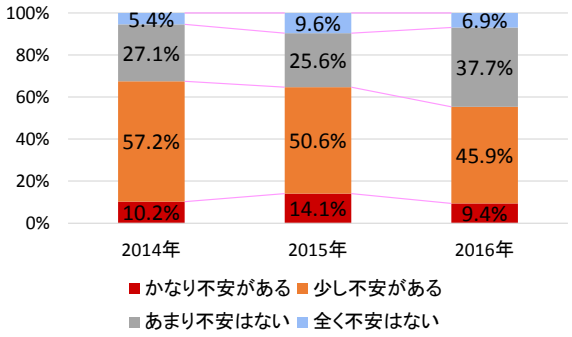


図 2：設問 1 の回答

PC 利用時、コンピュータウイルスやコンピュータ犯罪に多少なりとも不安を抱いている学生（かなり不安がある、少し不安があると回答した学生）の割合は、2014 年の 67.4%から 2016 年の 55.3%へと、3 年間で減少していた(図 2)。

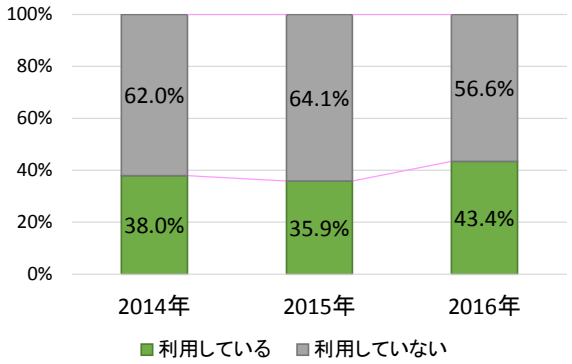


図 3：自宅における PC 利用

自宅で PC を利用している学生の割合を図 3 に示すが、いずれの年度も 40%前後だった。自宅で PC を利用している学生のみ（2014 年は 63 名、2015 年は 56 名、2016 年は 69 名）の設問 1 の結果は、図 4 のとおりである。多少なりとも不安を感じている学生の割合は、図 2 に示した結果よりも高かった。図 5 には、自宅で PC を利用している学生が PC のセキュリティ対策を行っているかを示したものである。2014 年には 71.4%がウイルス対策を行っていると回答していたが、2016 年には 56.5%と減少していた。また、対策していないと回答した学生が、11.6%いた。これは、ほとんどの学生が利用している携帯に比べると、自宅で PC を利用している学生が少ないことが、PC 利用時のセキュリティに対する意識が低下している一因と思われる。

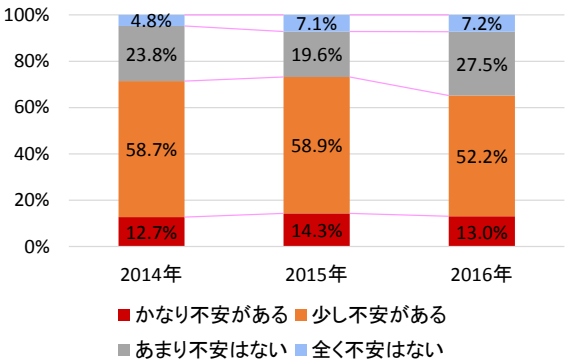


図 4：設問 1 の回答
（自宅における PC 利用者のみ）

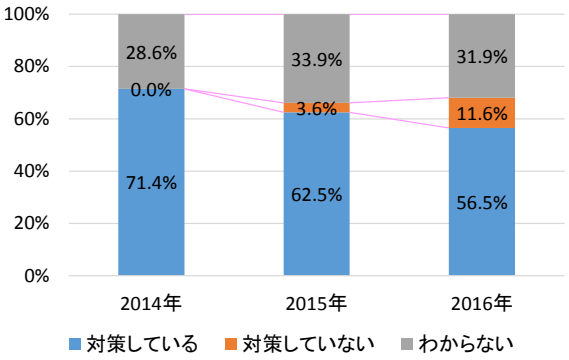


図 5： PC 利用時のウイルス対策の有無
（自宅における PC 利用者のみ）

設問 2～3 は、個人所有の情報携帯端末を対象としたセキュリティの意識を問うものである。

2. スマートフォンやタブレットでも、コンピュータウイルスやコンピュータ犯罪による被害が多数報告されています。あなたは携帯情報端末(スマートフォン、タブレット)を使っていて、コンピュータウイルスやコンピュータ犯罪による被害を受けるのではないかという不安はありますか。

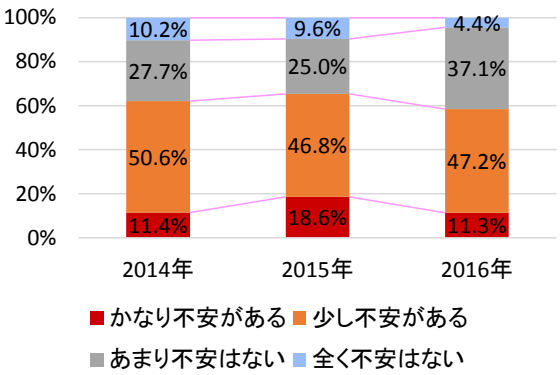


図 6：設問 2 の回答

携帯情報端末の利用において、コンピュータウイルスやコンピュータ犯罪に対して多少なりとも不安を抱いている学生は、3 年間とも約 60 %であった（図 6）。

3. 携帯情報端末(スマートフォン、タブレット)にウイルスなどのセキュリティ対策をしていますか。

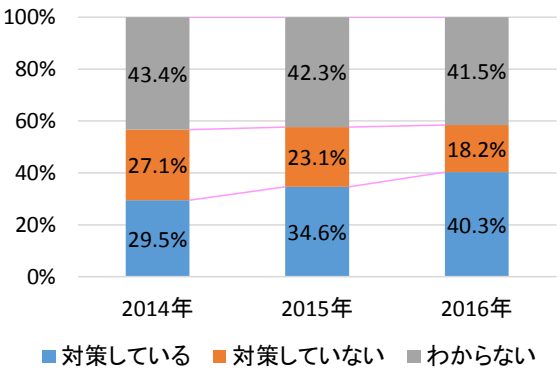


図 7：設問 3 の回答

ウイルス対策ソフトの導入などにより、携帯にセキュリティ対策を行っている学生は、2014 年は 29.5%だったが、2016 年には 40.3%と増加した（図 7）。

わからないと回答した学生の多くは、iPhone 利用者である。スマートフォンのセキュリティについては、授業でも最新事件を取り入れた教育を行っており、Android 端末については、ウイルス対策ソフトを導入するように指導している。セキュリティ対策を行っている学生の割合が増加していることから、教育の効果があったものと思われる。

## 5 まとめ

本稿では、未知の脅威や標的型攻撃に対応するために 2016 年 4 月から運用を開始した出口対策用ファイアウォールの役割と、以前から運用していた入口対策を組み合わせた 2 台のファイアウォールによる多段のセキュリティ対策、教職員や学生のセキュリティ意識を向上させるための利用者教育など、本学の多層防御を考慮したセキュリティ対策の強化について報告した。

入口対策用の全学ファイアウォールで学外と学内間の全通信を監視し、出口対策用ファイアウォールで学内コンピュータから外部への通信に関する詳細情報を得るという、2 台のファイアウォールの特性にあわせた運用方法でセキュリティ対策を行っている。出口対策用ファイアウォールを導入して約半年経過したが、学内ネットワークから学外への通信を監視して危険な通信を遮断するなどの制御ができるようになったため、ほぼ期待どおりのセキュリティ対策を行うことができていると考える。

セキュリティ教育は、利用者にセキュリティ対策の重要性を理解させるとともに、その対策に関心を持たせるような教育を行う必要がある。最新の事例や対策などを紹介しながら定期的に実施する必要があるため、教職員研修の時期や学生教育の内容などを今後も検討していく。

セキュリティの強化と利用者の利便性は相反するため、どこまでセキュリティを強化するかについても、今後の課題である。

## 参考文献

[1] 古市恵美子、牧幸浩、「小規模大学における MacOS と Windows 共存環境による情報教育基盤構築と教育活用」、大学 ICT 推進協議会 2014 年度年次大会講演論文集、2014 年 12 月

[2] 牧幸浩、平川幹和子、「乖離した習熟度と意識レベル：学生のコンピュータリテラシとビジネスマナーおよびセキュリティ」、大学 ICT 推進協議会 2014 年度年次大会講演論文集、2014 年 12 月

[3] 総務省、「国民のための情報セキュリティサイト」、http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/