小規模校における学務 Web システム導入に伴う 学内 LAN のセキュリティ対策例

田中 健吾 [1),2)]

1) 香蘭女子短期大学 情報センター
2) 香蘭女子短期大学 ライフプランニング総合学科

tanaka@koran.ac.jp

Example of Security Measures for Campus LAN Associated with Implementation of Academic Affairs Web System in Small College

Kengo Tanaka [1),2)]

1) Information Technology Center, Koran Women's Junior College
2) Comprehensive Studies for Life Planning, Koran Women's Junior College

概要

本稿では 2017 年度に本学に導入された学務 Web システムと、それに伴う学内 LAN の統合的なセキュリティ設計とその実装方法について述べる。現状のシステム構成とそれに応じた実現可能なセキュリティ設計に基づき、当面は、ホスティングサーバ上に構築した学務 Web システムを学内 LAN のみからアクセス可能な閉域構成で運用することにした。その際、学務 Web システムの「学生用」のログインアカウントは学内 Wi-Fi 経由でもアクセス可であるが、権限の強い「教職員用」は不可となるアクセス制御を行った。本学と同じような、情報システムの運用に充当できる資源が限られている小規模校にとっては、教育機関向けのセキュリティ対策のガイドラインに準拠したシステム開発のコストを負担することは容易ではない。コストパフォーマンスに優れた開発事例とその開発環境ならびにセキュリティ対策の実装方法について、小規模校向けのガイドラインとして共有することは、システム開発の障壁を下げるための重要な課題であると考えている。この学務 Web システムは管理者権限の無い管理サービス付のホスティングサーバに構築し、VPN 接続の代わりに各通信の暗号化とパケットフィルタリングを用いることで、様々なコストを大幅に抑えることができたので、その事例に資する情報の一つとして本稿を通して報告したい。

1 はじめに

著者は福岡市にある 4 学科、1 専攻科を設置している短期大学に勤務している。2018 年度現在で学生・教職員数を合計すると約 900 名であり、学内の全端末台数は約 400 台である。

学内のネットワーク基盤やセキュリティ対策、電子メール等の情報サービス、パソコン教室、他、の管理・運営を情報センターが行っているが、所属学科と兼任のスタッフ 2 名のみで業務を担当しており、専任のスタッフは不在である。情報センターと学内各部署（事務局各部署、各研究室、他）との間では、情報環境基盤および情報機器の管理に関する責任分界点は定めているものの、事務局には情報システムの部署は無く、情報処理関連の知識・技術を有する人材も不在であり、管轄外の端末や情報システム関連のことにも、しばしば対応したり、相談を受けたりしているという状況である。このような実情から、業務の効率化、サービスの安定稼働、コスト削減、トラブル対応、地方の小規模校としての標準的なサービスの提供などが、常に中心的課題である。

本学でも 2017 年 4 月に学務システムが一部更新され、履修登録や成績提出、授業の出欠登録、他、を Web アクセスで行えるようになった。同じく、2017 年 9 月に校舎内にアクセスポイントを設置したことで、エリアは限られているが Wi-Fi の利用も可能になった。学務システムを Web 化して、ある業者のホスティングサーバ上に開発されることが決定した後に、学内 LAN 上にある学務システムと同期するためのネットワーク接続に関する工事依頼が筆者のところへ来た。その時点で各所にセキュリティ対策の不備に問題点を感じ取り、統

合的なセキュリティ設計と施工に取り組むことにした。2017 年 2 月以降継続して、セキュリティ設計を検討しつつ、決定したものについては随時実装してきた。本稿では、現段階で施工が完了している内容を中心に報告したい。

本学のように、4 年制総合大学のような情報システムに関する十分な組織基盤が、事務側にも教学側にも不在な小規模校であっても、やはり、教育の ICT 化や業務の効率化などは、程度の差こそあれ、等しく存在する。しかし、大規模校と同じような資源を備えていないことは、明白であり、限られた資源の中で実現可能な情報システムの導入やセキュリティ対策が求められることになる。本学での取り組み事例が、同じような状況の小規模校に参考にしていただける情報提供になることを願って、本稿のタイトルにも小規模校という文言を加えた。

2 節では、教育機関向けに示されている一般的なセキュリティ対策や Web アプリケーション開発に関するセキュリティ技術のガイドラインについて、参考にしたものについて簡単に説明したい。3 節では、履修登録や成績提出などで利用される学務 Web システムと学内 LAN の間のネットワーク構成と通信制御を用いたセキュリティ対策について述べる。4 節では、3 節で述べた内容の中で、特に学内 Wi-Fi 経由での学務 Web システムへアクセスする際のセキュリティ対策について述べる。5 節では、開発環境として、管理サービス付のホスティングサーバを利用した際のメリットとデメリットについて述べる。6 節では 2〜4 節までのまとめを行うと共に、実装したセキュリティ対策の内容や現状の問題点などについて考察する。

2 セキュリティ対策のガイドライン

本節では、本稿でのセキュリティ対策を行う際に参考にした、教育機関向けに提示されたものと Web アプリケーション開発についてのガイドラインについて簡単に触れたい。

2.1 教育機関向けのガイドライン

教育機関向けのセキュリティ対策のガイドラインとしては、文献[1-3]が挙げられる。文献[1]は高等教育機関向けであり、多くの大学がこれを参考にして各大学内のセキュリティポリシーを策定する際の雛形として利用している。

文献[2,3]は小・中・高等学校向けのガイドラインであり、特に文献[3]では 2015 年から 2016 年にかけて発生した佐賀県の県立中学校、高等学校の校内 LAN や教育情報システムに不正アクセスされた事件が紹介されている。この事件を受けて、2016 年 7 月に文部科学省生涯学習政策局情報教育課より教育情報セキュリティのための緊急提言[4]が示されたことは記憶に新しい。

文献[2,3]は高等教育機関向けではないものの、文部科学省が小・中・高等学校向けに正式に出したガイドラインであるので、基本的には準拠すべき内容であるといえる。これに相当する高等教育機関向けのガイドラインは、筆者が知る限り存在していないと認識しているが、文献[2,3]は本学のような小規模校にとって、これまで以上に情報セキュリティ対策に真摯に取り組まなければならないということを強く印象付ける存在といえる。

2.2 Web アプリケーション開発のガイドライン

Web アプリケーション開発という点に特化したセキュリティ対策の基本的なガイドラインとしては、情報処理推進機構が公開している文献[5-7]が挙げられる。ここ数年、Web アプリケーションのセキュアな開発に関する書籍も増えてきているが、同文献を書籍中で紹介しているものが多いことから、広く一般的にセキュリティ対策の基本事項として共通認識されているようである。

学務 Web システムの開発業者に対して、最低限のセキュリティ対策として、文献[5-7]に示しているセキュアな実装方法を満たしているか否かを回答していただくのに役立った。文献[5]にはセキュリティ実装のチェックリストも付属している。

3 ネットワーク構成とセキュリティ対策

学務 Web システムと学内 LAN に関連するネットワーク構成と通信制御の概略は図 1 の通りである。学務 Web システムは、学内 LAN 経由でしかアクセスできない閉域構成となっている。この閉域構成は、学務 Web システムを構築しているホスティングサーバ側でのパケットフィルタリングと、学内 LAN 側のパケットフィルタリングで実現し

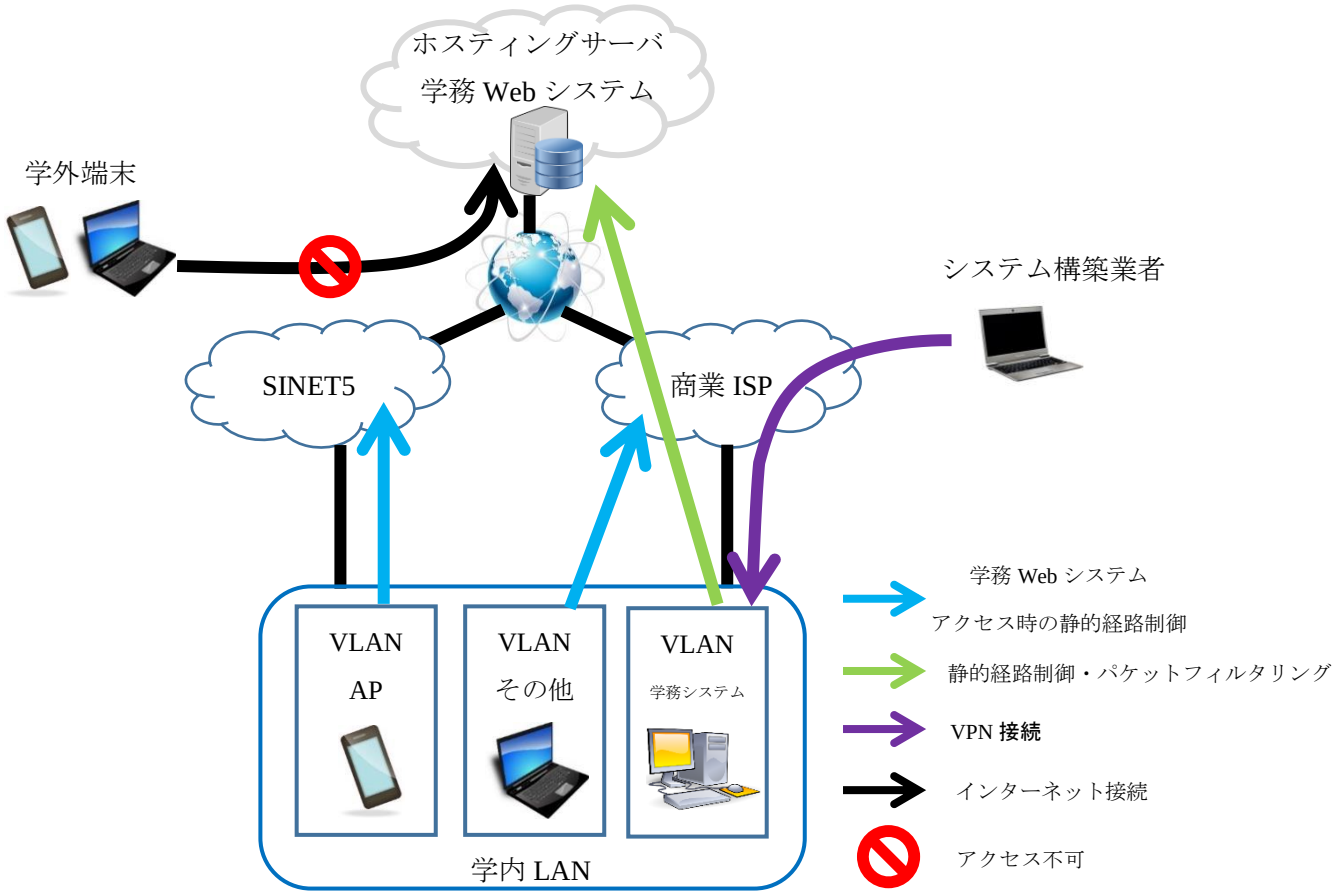

図 1　学務 Web システムと学内 LAN のネットワーク構成ならびに通信制御の概略図

ている。本節では、そのネットワーク構成と通信制御を用いたセキュリティ対策の詳細について、以下で述べる。

3.1 学務 Web システム

学務 Web システムは、ある企業が提供するホスティングサーバ上に、システム開発業者が構築し、稼働している。また、学内 LAN 上にある学務システムと同期する構成になっており、事務局業務は主として学務システムとその業務用端末で行われる。

ホスティングサーバへの通信は、サーバ証明書をインストールするなどして、暗号化通信を採用している。また、ホスティングサーバのパケットフィルタリング機能を用いて、本学が所有する回線に紐づく IP アドレスのみのアクセスを許可している。図 1 のとおり、現状ではインターネットからホスティングサーバへの通信を遮断して、学内 LAN の閉域となっている。

3.2 学内 LAN

学内 LAN の概略は図 1 のとおり、「VLAN AP」「VLAN その他」「VALN 学務システム」の 3 つのセグメントに大別される。ここでは、説明を単純化するために VLAN の種類を 3 つに留めているが、実際にはもっと複雑である。

「VALN AP」は、主として 2017 年度に導入した学内 Wi-Fi のアクセスポイント（AP：Access Point）が所属するセグメントである。主な通信先は、インターネット、学務 Web システム、学内の図書館サーバなどである。

「VLAN 学務システム」は、学務システムが所属するセグメントであり、パケットフィルタリングにより、通信は「ホスティングサーバ」、他、送受信共に必要最低限のアクセス先に限定している。また、システム構築業者は学外から VPN クライアントとして、同セグメントに接続して、学務システムや学務 Web システムのメンテナンスや開

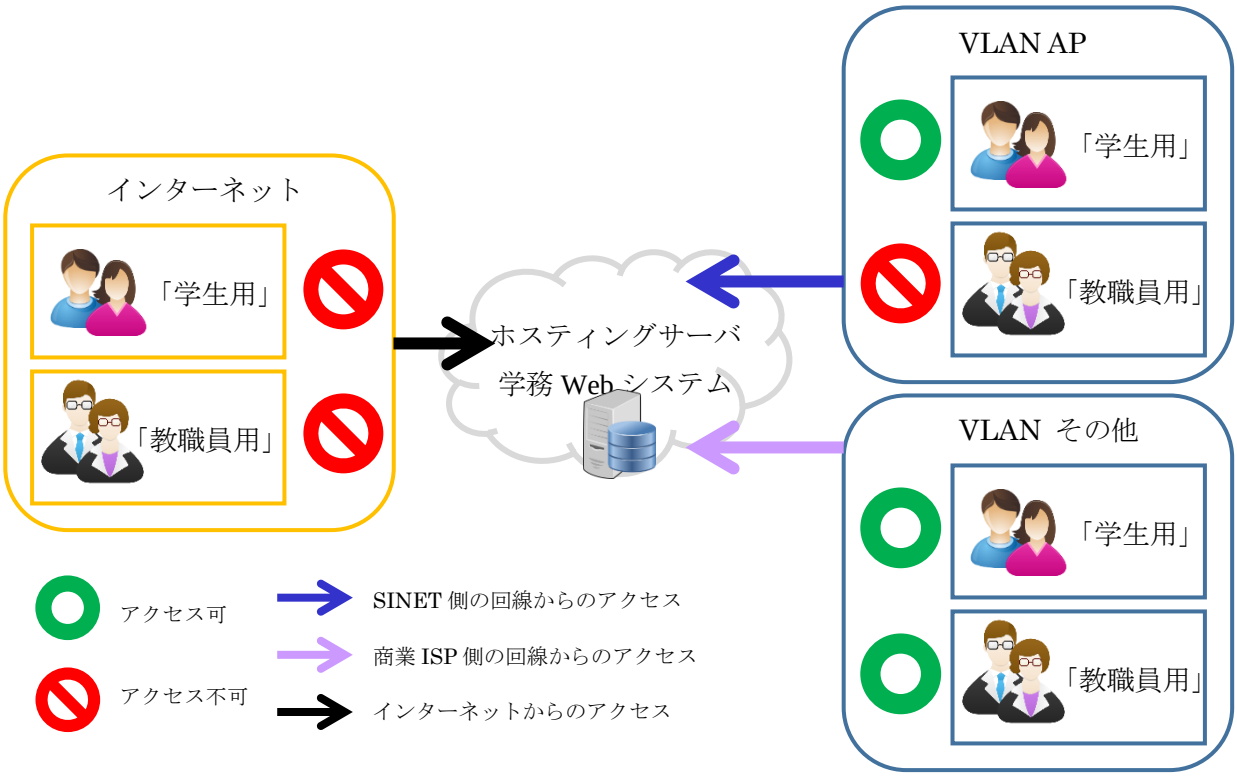

図 2　アカウントとセグメントに応じた学務 Web システムへのアクセス権

発などの業務を行っている。

「VLAN その他」には教職員の端末やパソコン教室などが主に所属しているセグメントであり、学務 Web システムを利用して、学生はパソコン教室で主に履修登録を、教職員は成績登録や出欠登録、他の日常業務を行っている。「VLAN その他」に教職員の端末やパソコン教室が所属するとしているが、実際には異なる VLAN に分かれている。

校舎内に設置したアクセスポイントのセグメントである「VLAN AP」と、それ以外のセグメントである「VLAN その他」からそれぞれ学務 Web システムへアクセスする際には、静的経路制御により、「VLAN AP」からは SINET5 側の回線へ、「VLAN その他」からは商業プロバイダー側の回線へルーティングしている。この静的経路制御と学務 Web システムの認証部分の連携で、学務 Web システムのユーザーアカウントによるアクセス制御を実現している。このことは、次節で述べたい。

4 ユーザーアカウントに応じたセキュリティ対策

学務 Web システムのユーザーアカウントにはいくつか種類があるが、本節では「学生用」「教職員用」の 2 つについて、そのアカウントとセグメントに応じた静的経路制御との連携により実現しているセキュリティ対策について述べる。

4.1 セキュリティ対策の趣旨

「学生用」は現状、履修登録についてのみデータを変更する権限があるが、残りは閲覧権限のみである。他方、「教職員用」は成績データ、他の重要なデータについて、変更権限を有している。したがって、「教職員用」は必然的に高いセキュリティが要求されることになり、本学の Wi-Fi 経由でアクセスすることを論理的に禁止する施工を行うことにした。また、「学生用」のアカウントであっても、図 1 に示した通り、現状、インターネットから学務 Web システムへのアクセスは禁止されているので、利便性向上に配慮して、「学生用」のアカウントは学内 Wi-Fi 経由でアクセスできる状況を実現した。上記に関するアクセス権限について図 2 にまとめた。

専任教職員は、通常、各自の業務用端末を利用して、学務 Web システムへアクセスすることになるが、非常勤講師は非常勤講師室の端末からアクセスすることになっている。この際、非常勤講師室の端末台数が限られていることから、学内 Wi-Fi 経由でのアクセスを試みることも十分考えられる。

非常勤講師は「教職員用」のアカウントに属する権限となるので、専任教職員と同様に学内端末からアクセスするという方針を堅持する必要がある。長期間運用していくことを考えれば、専任教職員も Wi-Fi 経由でアクセスしてしまうことも十分考えられるのでやはり論理的に禁止することが必要となる。

4.2 セキュリティ設計の要点

上記の理由より、本学の Wi-Fi 経由で学務 Web システムにアクセスし、「教職員用」のアカウントでログインを禁止するアクセス制御を、以下の様な方法で実現した。図 1 に示しているとおりであるが、現状、アクセスポイントには複数の VLAN を設定しておらず、「VLAN AP」というセグメントのみであり、アクセスできる先はインターネット、学内の図書館サーバ、学務 Web システムという具合に限定されている。そこで、「VLAN AP」から学務 Web システムへアクセスしようとした場合は、SINET5 へ接続する回線へ、「VLAN その他」からアクセスする場合は、商業 ISP へ接続する回線へと、静的経路制御によりルーティングすることにした。

この静的経路制御により、常に本学の Wi-Fi から学務 Web システムへとアクセスする場合には、SINET5 側の回線に紐づく IP アドレスで NAT されることになる。したがって、学務 Web システムに「教職員用」のアカウントでログインを試みた場合に、発信元が SINET5 側の回線の IP アドレスであれば、認証へ進む前に拒否される処理を実装することで、学内 Wi-Fi から「教職員用」のアカウントでログインすることを論理的に禁止することが実現できた。

5 システム構成とセキュリティ対策のコスト関係

4 節でも述べたが、本稿のセキュリティ対策は、ホスティングサーバ上に学務 Web システムが開発された後に始まっている。このホスティングサーバは、契約者が占有利用できるサーバではあるが、OS やルーター、ファイアウォールなどは業者側で管理されており、管理者権限が無いいわゆる管理サービス付のサーバである。データベースサーバや Web サーバ、メールサーバ、PHP、CMS、各種モジュールなどの開発環境が既に決められており、柔軟な構築ができない反面、サーバやネットワーク機器の管理コストは低い。本来であれば、想定する業務が実現可能な情報システムを、セキュリティ設計まで含めた上で、その実装が可能なシステム構成を担保して開発を開始しなければならない。しかし、後付けの状況からセキュリティ対策を始めたことで、管理者権限のない管理サービス付のホスティングサーバを利用することのメリットとデメリットを、本件施工を通して経験することができたので、本節ではそれらについて述べたい。

5.1 メリット

本学のように情報システム関連の専任スタッフが不在のような小規模校では、システム導入後のメンテナンスコストを抑えることは極めて重要である。上述したように、管理サービス付のホスティングサーバを採用することで、OS やルーター、ファイアウォール等を、自前で構築したり、日常的なメンテナンスや障害時の対応をしたりするコストを抑えることができる。特に、VPN 接続を利用するなどのために、ルーターやファイアウォールを自前で持ち込んで設置している場合は、障害時のオンサイト対応を自前でしなければならないことや、その対応方法を検討して備えることも必要になるが、そのような多大なコストを抑えることもできる。

管理者権限付きのサーバやクラウドをレンタルして、ルーターやファイアウォールまで含めて開発業者に設定や保守管理を依頼することもできるが、初期投資額や保守管理にかかる年間固定費は大幅に増額されることになるので、そのコストを抑えることもできる。

5.2 デメリット

OS の管理者権限がないことで、アプリケーションのインストールはできず、柔軟なシステム構築ができないことが最大のデメリットである。ルーターやファイアウォールは共有で使用するシステム構成になっており、個別の設定はほとんどできない。したがって、VPN での通信はできず、通信を個別に暗号化しなければならない。また、OS や

ルーター、ファイアウォールでのパケットフィルタリングなどの設定もできず、柔軟な通信制御や多層防御ができない。

また、システム導入時には開発環境としての条件を満たしていたとしても、後日、更なる開発が必要になった際に、開発環境の範囲内で必要な開発ができなくなる可能性も十分にある。

6 まとめと考察

本稿では、学務 Web システムが導入されたことで、それに必要となるセキュリティ設計の検討とその実装方法について述べた。本節では、2 節以降の内容について、以下、まとめと考察を行う。

6.1 セキュリティ対策のガイドライン

2 節では、教育機関向けのセキュリティ対策のガイドラインとして文献[1-4]を、Web アプリケーションのセキュアな開発のガイドラインとして文献[5-7]を取り上げた。文献[1]は高等教育機関向け、文献[2,3]は小・中・高等学校向けであるが、いずれも本学のような小規模校が準拠するガイドラインとしてはハードルが高い。

経営資源はヒト・モノ・カネ・情報といわれるが、その観点から、本学で情報システムの運営に利用できる資源を考えてみると、極めて乏しいことが分かる。前述した通り、ヒトを情報システムの専門知識を有する人材と捉えると、教学側に兼任スタッフ 2 人、事務局側には不在という状況である。また、情報はこの場合、ヒトと不可分で、情報システム関連の業務に取り組む人材が、日常的に知識・技術の向上に取り組むことで得られる情報ということになると、やはり乏しいといわざるを得ない。モノは情報システムを構築する際のサーバからネットワーク機器やネットワーク基盤までを含めた開発環境やその運用面と捉えると、既存の開発環境が備える機能性やセキュリティポリシーなどによるセキュリティ対策の充実度合ということになるが、それも十分ではない。カネは情報システムにかけることができる初期コストやランニングコストということになるが、それも極めて限られている。

セキュリティ対策の中心的な単語として、CSIRT やセキュリティ監査、次世代ファイアウォールなどが飛び交うが、いずれも本学にとっては高いハードルである。また、前述したが文献[1-3]のガイドラインも同様である。その最大の理由は、4 年制総合大学や市・県単位の教育委員会という組織規模がゆるやかに想定されていることにあるのではないかと想像している。もちろん、必要なセキュリティ対策の内容が組織規模に応じて変化するものでないことは十分認識しているが、他方、組織規模に応じて負担できるコストが異なることも現実である。

本学と同じような小規模校は、負担できるコストが限られているからといって、教育の情報化が進まなくてよいと、筆者は全く考えていない。むしろ、小規模校こそ教育の情報化がもたらす業務効率化が必要であると考えている。ここで、参考とすべきは、文献[2,3]が市・県単位での開発が前提のガイドラインであることである。また、全国の高等専門学校も、独立行政法人化した際に高専機構として一法人になったことで、高専全体でシステム開発やセキュリティ対策に取り組んでいるという状況である。市・県単位の教育委員会や高専機構と比較すると、本学のような小規模校が単独でシステム開発をしたり、個別にセキュリティポリシーの策定やセキュリティ対策を行ったりすることは、大きな負担となるのは当然といえる。しかし、小規模校がまとまって同じシステムを開発して一緒に利用することは実際には、困難であると思われるが、コストパフォーマンスに優れた開発事例と、それを実現する開発環境ならびにセキュリティ対策を共有することは極めて有意義であると考えている。

文献[5-7]は Web アプリケーション開発における脆弱性とその対策方法のガイドラインであり、開発業者にその対策状況を確認するためには有用な資料になる。それらに加えて、例えば、認証部分などは、脆弱性以外の部分も含めたセキュアで標準的な実装例がガイドラインとして提供されると

より有用であると思われる。

6.2 閉域構成からグローバルオープンへ

3 節では、学務 Web システムとそのネットワーク構成ならびにセキュリティ対策について述べた。

学務 Web システムは、学内 LAN 側とホスティングサーバ側の両方でパケットフィルタリング等を用いて、学内 LAN の閉域として運用している。しかし、筆者のところへ本件の依頼が来たときには、グローバルオープンでの運用が想定されていた。学内にはセキュリティ対策への経験値が全く無く、開発業者への発注も十分なセキュリティ対策を含めていない状況であったので、まずは、閉域構成でスタートすることにした。

例えば、シラバスのようにグローバルオープンで利用できるほうが望ましいコンテンツもある。「教職員用」のアカウントでは、シラバスのアップロードのような一部の機能は、グローバルオープンで、成績提出のような機能は学内 LAN 経由でのアクセスを堅持するというように、機能に応じたアクセス権の設定が望ましい。もしくは、二要素認証を導入することで、「教職員用」のアカウントもグローバルオープンにすることも考えられるが、現在の開発環境では開発が困難である可能性が高い。他方、「学生用」のアカウントはグローバルオープンで運用することで、学生の利便性の向上を図ることも検討する必要があるが、システム構成や認証機能など、まだ解決すべき複数の問題を抱えている。

6.3 学内 Wi-Fi 経由でのアクセスに対するセキュリティ対策

4 節では、静的経路制御と認証部分の処理を連携させて、学内 Wi-Fi 経由での「教職員用」のアカウントのログインを禁止する実装方法について述べた。他方、学生の利便性を確保するために、「学生用」のアカウントでは学内 Wi-Fi 経由で学務 Web システムへログインすることを可能にしている。

学内 Wi-Fi の SSID には、パスワードを設定し、そのパスワードも定期変更しているが、当然ながら秘匿性は低い。また、ユーザーの利便性を優先して、アクセスポイントでの端末の MAC 認証も行っていない。したがって、万が一、「教職員用」のアカウントが流出した場合は、本学の Wi-Fi に接続できるキャンパス内からはもちろん、キャンパス近隣からも、「学務 Web システム」へアクセスし、「教職員用」アカウントでログインされる事態も予想される。その様な事態を避けるために、この節の施工は必要かつ有効であると考えている。

6.4 小規模校向けのセキュリティ対策のガイドラインの必要性

5 節では、管理サービス付のホスティングサーバを利用することのメリットとデメリットについて述べた。

管理者権限のない管理サービス付のホスティングサーバは、柔軟な開発やセキュリティ対策ができないというデメリットがあるが、もし、その開発環境の範囲内で、システム構築やセキュリティ対策が可能であれば、大幅にコストを削減することができるという大きなメリットがある。

5 節では単にメリット・デメリットについて説明したに過ぎないが、本来の目的は 6.1 で述べたように、コストパフォーマンスに優れた開発事例とその開発環境ならびにセキュリティ対策の方法について、ガイドラインのレベルに昇華させて共有することである。文献[1]は高等教育機関向けの優れたたガイドラインであり、多くの大学がセキュリティポリシーの雛形として利用しているが、本学のような小規模校には、それに準拠したシステム開発の初期コストやランニングコストは多大な負担となり、システム開発の大きな障壁といえる。また、4 年制総合大学のような大規模校と本学のような小規模校では、情報システムの開発目的や利用状況も必ずしも同じではなく、オーバースペックな部分も含まれている。

筆者は、文献[1-3]のようなガイドラインが要求するセキュリティ対策の一部を、コストパフォーマンスと機能性に優れた商品を利用することで、自前で負担することから解放されることは極めて重要な課題であると考えている。その一例が、管理サービス付のホスティングサーバの利用である。セキュリティ対策も完全に同質のレベルを保証できないまでも、それに準ずるクオリティをコストの低い商品で実現できるのであれば、意義のある

ことだと考えている。本稿でこの内容に相当するのが、3 節で述べた学務 Web システムと「VLAN 学務システム」の間の通信を、両側でのパケットフィルタリングと各通信を個別に暗号化することで、VPN に準ずる通信を実現していることである。

筆者は文献[1]に相当する小規模校向けのガイドラインが提供されることが望ましいと考えている。より具体的には、どの学校でも共通利用されるような情報システムのコストパフォーマンスに優れた開発事例である。ガイドラインの内容として重要なのは、その情報システムの開発環境とセキュリティ対策の実現方法であり、文献[1]がより具体例化・細分化したものであるといえる。本稿がその一助になれば幸いである。

参考文献

[1] 国立情報学研究所　学術情報ネットワーク運営・連携本部、高等教育機関における情報セキュリティポリシー推進部会、高等教育機関の情報セキュリティ対策のためのサンプル規程集（2015 年版補訂）、2016 年 2 月.

[2] 教育情報セキュリティポリシーに関するガイドライン、文部科学省、2017 年 10 月.

[3] 学校における情報セキュリティ及び ICT 環境整備等に関する研修教材、文部科学省、2017 年 3 月.

[4] 教育情報セキュリティのための緊急提言、文部科学省生涯学習政策局情報教育課、2016 年 7 月.

[5] 独立行政法人情報処理推進機構　セキュリティセンター、安全な Web サイトの作り方（改訂版第 7 版）、2015 年 3 月.

[6] 独立行政法人情報処理推進機構　セキュリティセンター、安全な SQL の呼び出し方、2010 年 3 月.

[7] 独立行政法人情報処理推進機構　セキュリティセンター、ウェブ健康診断仕様、2012 年 12 月.