# 学内LAN更新及び次期ネットワークシステム

樁　　一　喜

## Renewed University LAN and Next Network System

Kazuki Kaba

近年、情報は組織にとって価値ある資産と考えられ経営基盤の重要な要素であると認識されているが、情報の盗聴・改ざん・なりすましなど不正アクセスによる脅威が問題となっている。本学の学内LANにおいては、ネットワーク機器のスイッチ類を学内に配置し、ファイアウォール、サーバをデータセンターに設置し学術ネットワークSINETに接続するハウジング方式の形態を取っている。ネットワークでは、セグメント分けとファイアウォールによってセキュリティを確保し、2019年度から第３期更新による運用を開始した。

［キーワード］　VLAN、標的型攻撃、IDS、IPS、プロキシサーバ、IEEE802.1X認証

## １．はじめに

近年、情報は経営活動の基盤となり組織にとって価値ある資産と考えられ情報システムへの依存度が高まり、経営活動の効率化は飛躍的に向上した。その反面、データの盗聴・改ざん・なりすましなどの内外からの不正アクセスなどの脅威によりリスクが生じ問題になっている。過去には、(特殊法人) 日本年金機構への標的型攻撃によるものや(株)ベネッセコーポレーションにおけるIT業者による個人情報の流失、さらに、資生堂は2016年12月２日、子会社の「イプサ」が運営する「イプサ公式オンラインショップ」から、最大42万1313人分の個人情報と5万6121件のクレジットカード情報が流出した可能性があり、「システム上の脆弱性を突かれ不正アクセスを受けた」と発表している[1、2]。また、防衛省と自衛隊の情報基盤において、駐屯地や基地を相互に結ぶ高速・大容量の通信ネットワークがサイバー攻撃を受け、陸上自衛隊のシステムに侵入されていたことが、複数の同省関係者の話で分かった[3]。防衛省が構築した堅固なシステムの不備を突く高度な手法と確認された。詳細な記録が残されておらず被害の全容は判明していないが、陸自の内部情報が流出した可能性が高いとマスコミに報じられている。この様な事故が発生して大きな社会問題となっている。

本学の学内LANでは、LANの基本構成[4、5、6]は初期のままであるが、平成２４年度の第２期の運用から、最新ネットワーク機器のスイッチ類を学内に、ファイアウォール、サーバをデータセンターに設置して、国立情報学研究所の学術ネットワークSINETに接続するハウジング形態のネットワークにおけるVLANによって、教員・事務・学生・管理系とセグメント分けされたシステム構築によって運用されている。内容は、授業用の情報処理室、ELC教室のパソコン約１００台と教職員の業務用パソコン及びインターネットサーバ並び教務用データベースサーバ等多数が接続されて、サーバには個人・業務用の重要なデータが保存・更新され新たに情報が書き込まれ運用されている。令和元年度からは、第２期に対する課題として全教室の無線化による第３期の運用を開始した。これらの事から、本学においても標的型に対するセキュリティ問題[7、8]が避けて通れないのが現状である。そこで、現在本学のLANにおける課題として次世代セキュリティについて検証し、学内LANにおける次期ネットワークシステムについて提案する。

## ２．学内LAN更新

### 2.1　学内LANの回線系統

本学ネットワークの特徴は、国立情報学研究所の学術ネットワークSINETに接続してインターネット網に出て行っている。そのSINETのノードがデータセンターにあるために、本学のデータ保管用のサーバ類はデータセンターに設置して運用しており、黒髪キャンパスのネットワークとデータセンターまでの回線の系統図を図１に示す。図より黒髪キャンパスではＬ３，Ｌ２スイッチ類によって、情報処理室用のWindows Active Directoryとセグメント分けされたネットワークが構築され運用されている。

### 2.2　学内LANの論理構成

本学のネットワーク構成の特徴は、図２に示す様に従来から大学内の人員の業務種別等により、一つは学生系で、次に教員系、さらに事務系並び保守管理用の４系統の区分に分類されている。最初に、ネットワーク末端のPC等の機器からの信号は、その回線の各部位に設置されたＬ２スイッチのエッジスイッチに入力され、そこから上位Ｌ３スイッチのディストリビューションスイッチに纏められ、さらに本学ネットワーク中枢のＬ３スイッチであるコアスイッチに集約されている。即ち、学内LANの機器構成図からも分かる通りディストリビューションスイッチにより４系統の教員・学生・事務及び管理用の回線がVLANでセグメント構成されている。

今回、そのネットワークにAll無線化を行う為に、追加されたのが図２の無線LANに示すアクセスポイントを各教室等に設置して、さらにそのアクセスポイントからの信号をフロア／PoEスイッチに入力し、従来同様のフロアースイッチに繋ぎ各セグメント分けされた回線のネットワークが構築されている。

### 2.3　学内無線LANについて

#### (1)　無線LANのネットワーク構成

無線LANネットワークの構成は、図３に示す様にアクセスポイント、フロア／PoEスイッチを経てコアスイッチへの系統がVLANによって構成されている。ネットワークはVLANによりセグメント毎に分離されている為に、無線の端末間機器での通信はできないようになっている。そのために各教室等に設置されているアクセスポイントからの信号も教員・事務系統から分離されている。即ち、学生・教職員・事務の無線LANを利用する場合、ACLによる制御で相互（学生＜－＞教職員／教職員＜－＞事務／学生＜－＞事務）間の通信をすることは出来ない仕組みになっている。

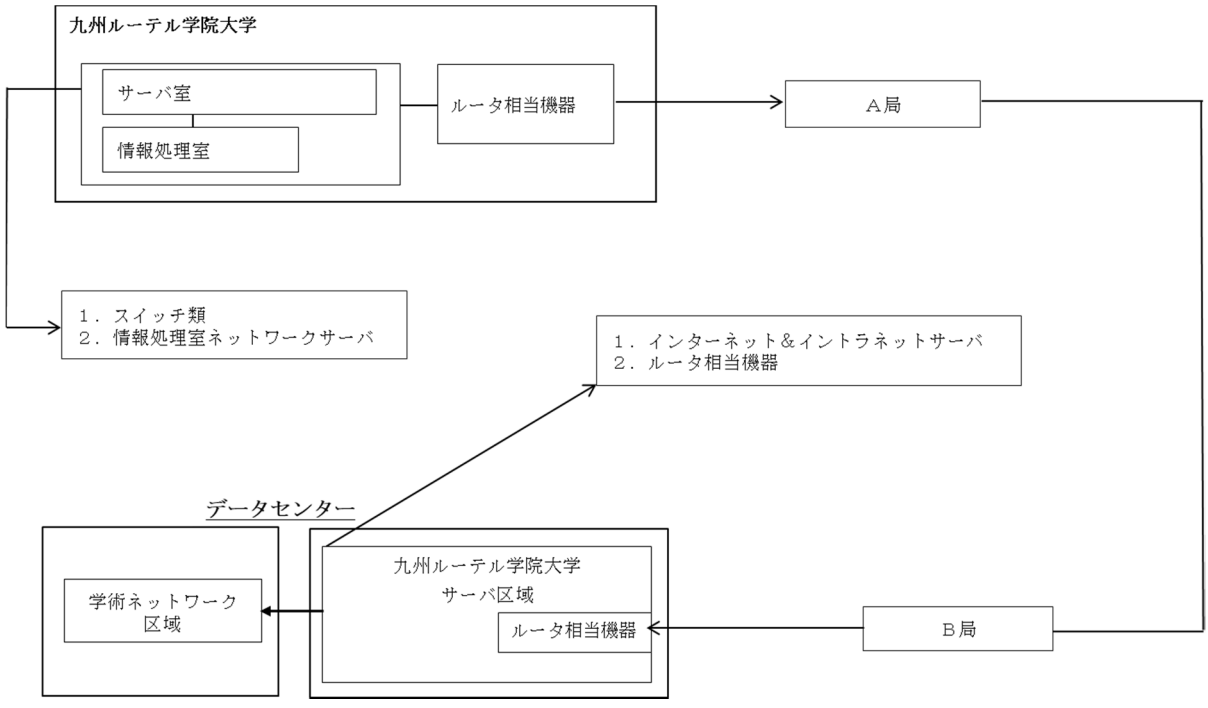


図１　学内LANの回線系統

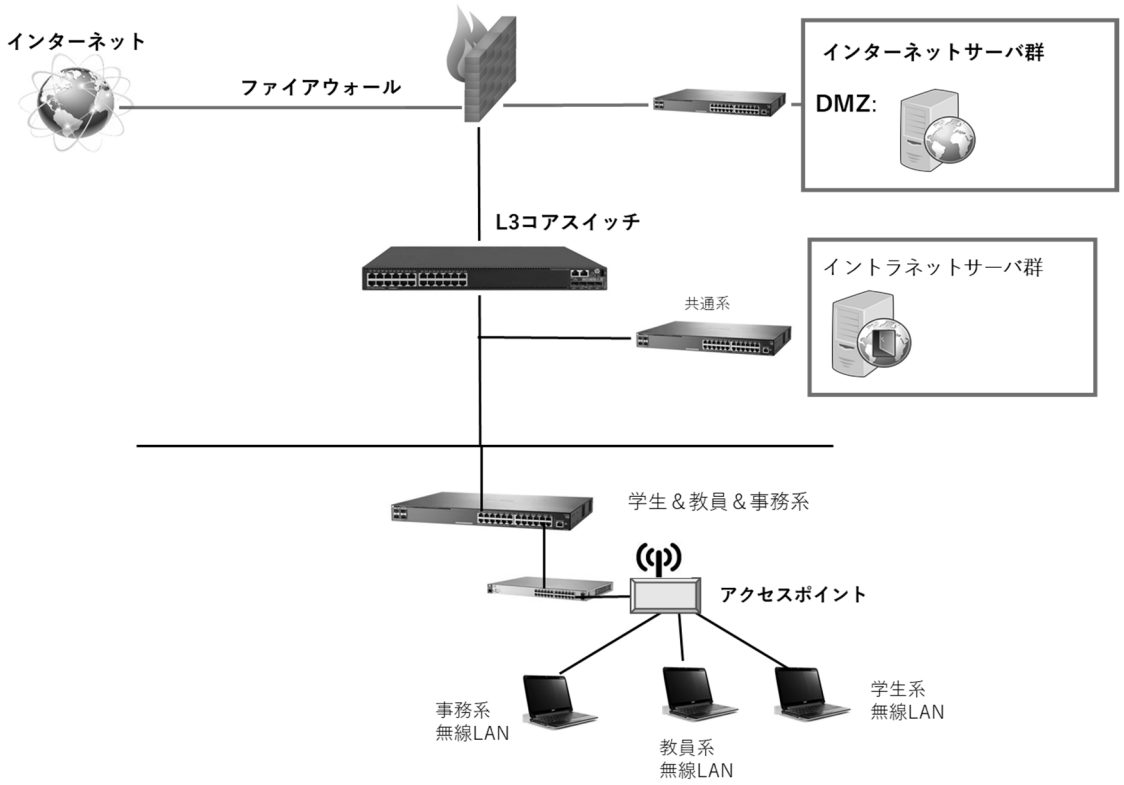


図２　学内LANのネットワーク構成

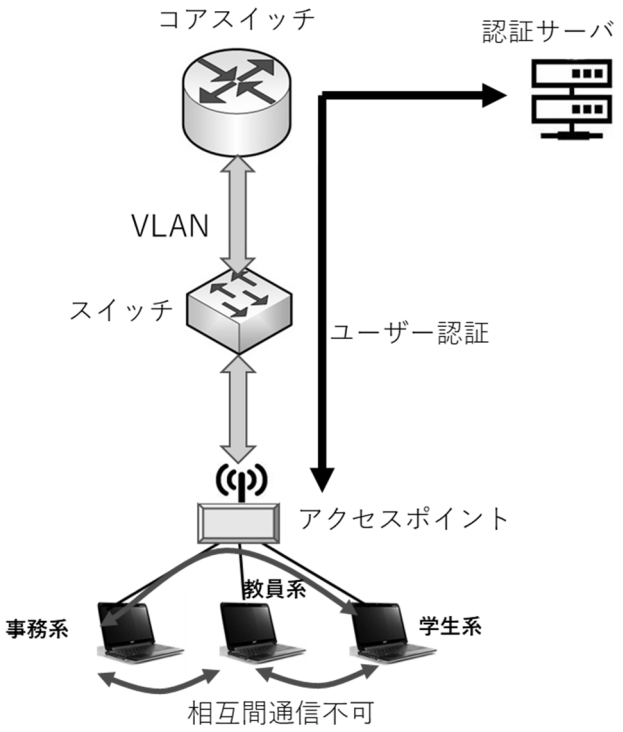


図３　無線LANのネットワーク構成

### (2)　無線LAN認証

学内LANのセキュリティを確保するためにセグメント分けされた系統の末端からネットワーク経由で各種サーバ類にアクセスするには、従来からのネットワーク認証システム（メール・WindowsAD等）におけるID、Password認証を行っている。そのために端末の機器類から無線LANでネットワークに参加するには、ユーザー名／パスワードによる認証が必要であり、接続する機器の状況によってMACアドレスや802.1X認証を用いた認証も可能とし、ユーザー情報は認証サーバにより一元管理され認証サーバのユーザー登録・削除がWindowsADサーバに反映される。また、Web認証や802.1X認証を利用するアクセスポイントなどは認証サーバに問い合わせを行い、アクセスポイント＜－＞端末間暗号化通信（WPA2）を行う。そのシステムの特徴は、従来の認証ゲートサーバFERECを省略して、表１に示す様なIEEE802.1X認証のRADIUSとLDAP認証を用い、無線の形式・規格として802.11acの周波数帯５及び2.4GHzで伝達速度最大6.9Gbpsの仕様で無線LANのアクセスポイントからスイッチを経由して認証サーバAXIOLEにおいてID、Passwordによる直接認証を可能とする方法である。

表１　学内LANの認証方式

| 機器 | 形式 | 認証規格及びアクセス制御 |
|---|---|---|
| 認証サーバ、スイッチ、<br>無線LANアクセスポイント | IEEE802.1X認証 | RADIUS／LDAP認証 |

## ３．次期ネットワークシステムに必要なセキュリティ技術

ネットワークシステムに必要な要素の一つにはネットワークセキュリティがあり、次世代ネットワークシステムのシステム構成を検討する上で、第１には、不正侵入に対する検知及び防止システムにおけるネットワークセキュリティ機器によるネットワーク監視・制御の導入が挙げられる。第２には、代理サーバの役目を果たすプロキシサーバによる公開サーバのIPアドレスを秘匿する機密性がある。第３には、グローバルネットワークにおける接続マシンの確認を行う認証システムによるセキュリティ確保がある。よって、本学の次期ネットワークシステムに必要なセキュリティ技術としては、上記３項目について述べる。

### 3.1　ネットワークセキュリティ機器（IDS、IPS）についての要素技術

ネットワークセキュリティ機器による構成を図４に示す。図よりIDS（Intrusion Detection System）は、侵入検知システムの事で、IDSの名のとおり不正アクセスなどの悪意あるトラフィックを検出して通知するシステムである。例えば、Firewall前に置かれたIDSは、ネットワーク上を流れるトラフィックを監視していて、不正アクセスと思われるパケットを検知するとネットワーク管理者に通知する。不正アクセスのパケットであるかの判断はシグネチャと呼ばれる攻撃パターンのデータベースを使用し、侵入検知の通知を受けて、管理者は例えばファイアウォールのフィルタリングを強化して攻撃に備える事ができる。次に、ネットワークセキュリティ機器のIPS（Intrusion Prevention System）は侵入防止システムの事で、IPSとは、その名のとおり不正アクセスなどの悪意あるトラフィックを検出して通知するだけでなく、シグネチャを参照して不正アクセスに該当するパケットを破棄したり、セッションを切断して即座に防御する事からセキュリティ実装の要と言える位置づけである。IPSは、ワームやDoSなどのパケットが持つ特徴をとらえた瞬間リアルタイムに防衛を開始することから、IDSのような手間のかかる管理者のメンテナンスが発生しない特徴を有する。

### 3.2　プロキシサーバ

プロキシサーバとは[9]、一般的にはインターネット接続ができない内部のコンピュータに代わって代理としてインターネット接続を行うサーバのことで、プロキシサーバは、図５に示す様に企業の内部ネットワークとインターネットの境界に配置されることが多いサーバである。プロキシサーバには、プロトコルやアプリケーションの違いで様々な種類があり、一般的にプロキシサーバといえば、HTTPトラフィックを対象としたWebプロキシ（HTTPプロキシ）を指す。

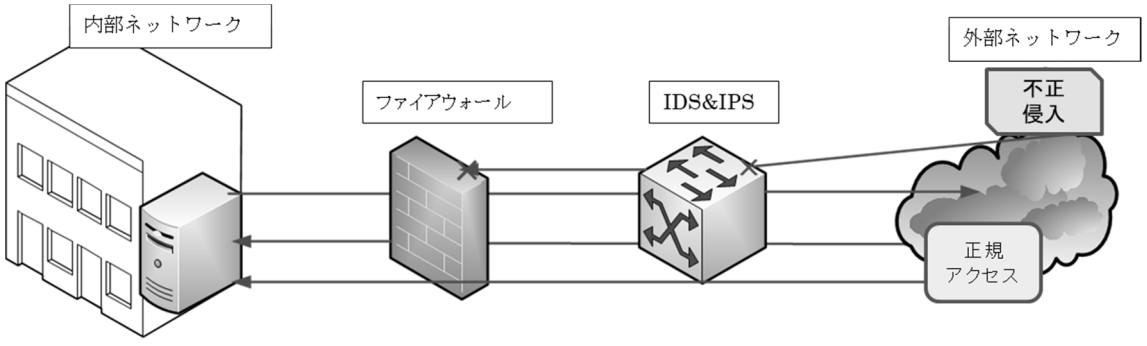


図４　IDS，IPSによるネットワークセキュリティ

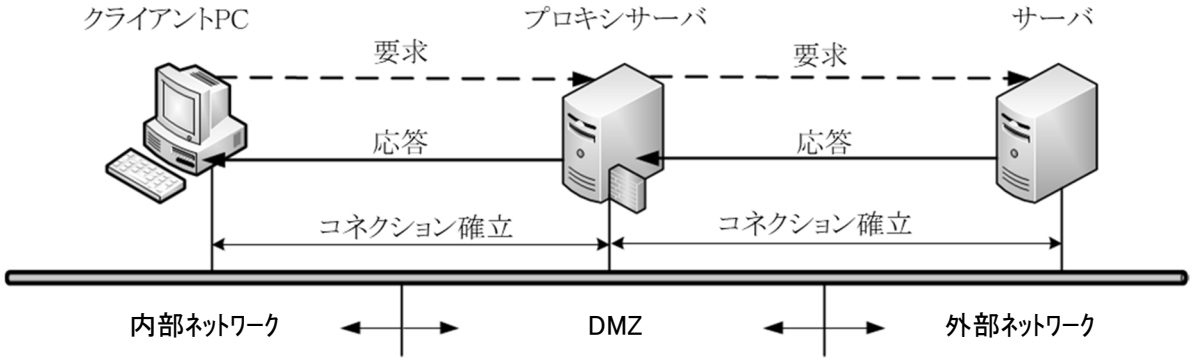


図５　プロキシサーバシステム

### 3.3　認証システムの要素技術

端末をLANに接続する際に許可・不許可を管理する方法は、①IEEE802.1X認証　②WEB認証　③MACアドレス認証と３つが存在する。小規模なネットワークの場合　②③は、RADIUSなどの外部認証サーバを用いるのが一般的であり、RADIUSサーバ機能を併せ持ったWEB認証スイッチ（認証ゲートウェイ）という製品を用いて導入コストや管理コストを下げる方法もある。しかし、次世代ネットワークにおける有線や無線LANの認証では、図６に示す様にIEEE802.1X認証方式が主たる方式になると予測できるので、IEEE802.1X認証について以下に述べる。

IEEE802.1X認証[10]とは、有線LANや無線LANにおけるユーザー認証の規格で、IEEE802.1X（Port Based Network Access Control）はネットワークに接続する際に、ポートごとにユーザー認証を行ない、登録されていないクライアントからの通信をすべて遮断し、登録されたユーザーのみに通信を許可することができ、この機能を使用することで不正アクセスからネットワーク全体を防御することが可能になる。IEEE802.1X認証の構成要素としては、IEEE802.1X認証を行うためのサプリカント、認証装置、認証サーバの３つの構成要素が必要となり、

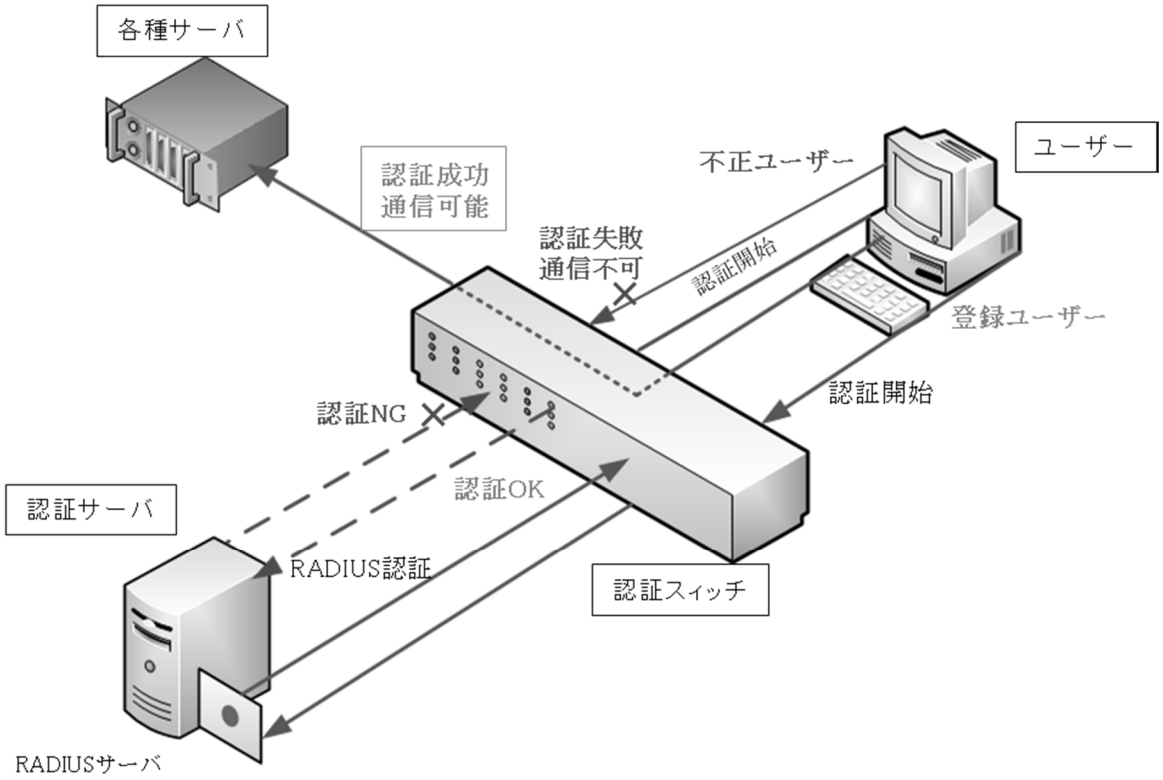


図６　次期認証システム

表２　３種類の構成要素

| 構成要素 | 内　　容 |
|---|---|
| サプリカント（Supplicant） | IEEE802.1Xにおけるクライアントのこと、または、クライアントにインストールするソフトウェアのことでもある。認証を受けるクライアントはPCにインストールする必要があるが、最近のPCには標準搭載されている。 |
| 認証装置（Authenticator） | サプリカントと認証サーバの仲介役となるネットワーク機器のことであり、IEEE802.1X対応のLANスイッチまたは、無線LANアクセスポイントのことである。これらの機器は、サプリカントと認証サーバとの認証結果を受けて、ネットワークへのアクセス制御を行う。 |
| 認証サーバ（Authentication Server） | ユーザー認証を行うサーバのことで、IEEE802.1X／EAPに対応したRADIUSサーバを使用する。 |

注）これら３つの構成要素以外に、クライアント認証の際に「証明書」を使用する場合は、証明書を発行するためのCA（認証局）が必要である。

その内容を上記の表２に示す。

## ４．学内LANにおける次期ネットワークシステム構築

本学の学生、教員、事務員すべての業務を一元管理するためにファイアウォール２重化によるネットワークを構成する。その概念設計は、ネットワークセキュリティを確保する必要性から業務内容を区別・分割して、ファイアウォール２の最下部に事務系サーバと事務のユーザーを配置して最もセキュリティを厳しく、その右側のポートに教員ユーザーと教員用サーバを配置し下部の事務系ネットワークには侵入できなくする。本構成のセキュリティポリシーを表３に示す。最上位には、従来のイントラネット用サーバ（内部用メール、Web, DNS等）と学生ユーザーを配置し、学生はイントラネット用サーバ以外アクセスできないセキュリティポリシーにより内

表３　次期ネットワークのセキュリティポリシー

| 目的およびポリシー | 管理方法 |
|---|---|
| 学生用・教職員用・外部公開用ネットワーク（DMZ）を分離し、必要な通信をルーティングする。 | Ｌ３・Ｌ２スイッチによる VLANによる分離及びＬ３コアスイッチによるルーティングを行う。 |
| ユーザー認証アカウントの一元管理を可能とし、不許可端末の学内ネットワーク接続を排除し、持込端末の接続を管理する。 | Active Directory と LDAP とのネットワーク認証及びRADIUSサーバ間での連携が可能なユーザー認証機器を用いて、802.1X認証、WEB認証、もしくはMAC認証を経たもの以外は接続不可とする。 |
| 端末設定、接続先ポートなど故意もしくはヒューマンエラーでの意図しないネットワークセグメントへの接続を防ぐ。 | 認証後、許可されたVLANへ自動でアサインされる認証VLAN（ダイナミックVLAN＋ネットワーク認証）構成を用いる。 |
| 外部ネットワークからの不正侵入を防ぎ、不要・危険な既知のWebサイトへのアクセスを制限し管理する。また、既知の脆弱性やマルウェアを検知し、ウィルス、マルウェア対策及び、未知のぜい弱性攻撃や成りすまし型マルウェアのセキュリティ対策を行う。 | IDS・IPS機器による不正侵入検知・防御及びUTM型ファイアウォールのWebフィルタリング機能及びアンチウィルススキャンとシグネチャ型端末ウィルス対策ソフトによる制限を行う。また、サンドボックス型の検知／遮断機能を有する機器で未知のぜい弱性攻撃や成りすまし対策をする。 |
| 情報流出やセキュリティリスクのあるインターネットでのWebサービス、クラウドサービスなど、サービスやアプリケーションの学内利用を管理する。 | アプリケーションレベルで制御可能な次世代ファイアウォールを用いて制御する。 |
| 経営や人事情報、学生成績などの教務系情報をより強固に守るため、事務／教員用ネットワークセグメント用UTM型ファイアウォールを配備する。 | 機密性の高い情報を扱うネットワークセグメントに対して個別のUTM型ファイアウォールを設置して制御する。 |
| 標的型攻撃への対策として外部へのWebアクセスの一元化。 | プロキシサーバを構築して用いる。 |
| 入口対策では防げなかったマルウェアに対して、インターネットへのアウトバンドで情報漏洩の脅威を検知し遮断する。 | アウトバンドのトラフィック情報漏洩の脅威を、リアルタイムに発見し情報流出を防ぐアプライアンス機器を用いる。 |
| ネットワーク認証、UTM、プロキシサーバ等のセキュリティログを収集し保存、一元化する。 | ログ用サーバおよび可視化、レポートソフトウェアを用いて有事でのレポーティングやログ調査を迅速化する。 |

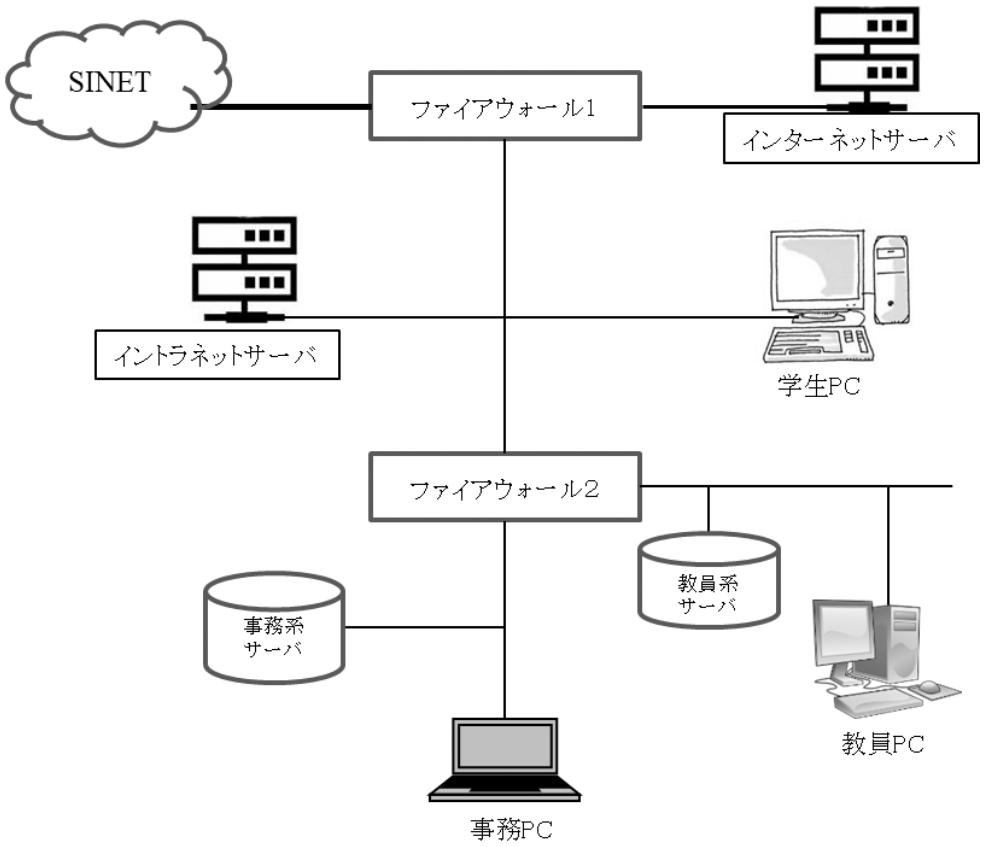


**図７　ファイアウォール２重化によるネットワーク構成概念**

部ネットワークを構成する。次に、インターネットへの出入り口となる最上部のファイアウォール１のDMZには、従来のセキュリティポリシーに基づく外向きインターネットサーバを配置するネットワークとし、上下のファイアウォールで２重化するネットワーク構成としたものでありその構成図を図７に示す。

## ５．おわりに

本学の学内LANにおいては、学内にスイッチ類をデータセンターにファイアウォールとサーバを設置し、学術ネットワークSINETへ接続するハウジング形態のネットワークにおいて、VLANにて教員・事務・学生・管理系とセグメント分けされたシステム構成によって、情報処理室、ELC教室と教職員の業務用パソコン約１５０台及びインターネット・イントラネットサーバ並び教務用データベースサーバ等多数が接続されて、また履修登録や成績登録においてはWebサービスにて行えるようIT化され運用されている。サーバには個人・業務用の重要なデータが保存・更新され日々新たに情報が書き込まれ運用されている。これらの事から本学においても、標的型に対するセキュリティ問題が避けて通れないのが現状である。

そこで、次期ネットワーク構築にける提案は、最初に、従来のインターネット及びイントラネットにおける学内や学生サービス業務の規則化で、次に、機器においてはアプリケーションレベルでの制御が可能な次世代ファイアウォール及び標的型攻撃にリアルタイムで対応可能な次世代標的型対策アプライアンスや各島ハブにて認証可能な認証装置などの高機能型の機器を導入し、さらに、ネットワークにおいてはファイアウォールを２重化することで、各クライアントPCは、上位ネットワークへの接続に限定し下位には接続できないネットワークポリシーによって、ネットワークセキュリィティを強化するシステムである。

## 参考文献


1 資生堂子会社，カード情報５万6000件流出，日本経済新聞，
https://www.nikkei.com/article/DGXLASDZ02HPH_S6A201C1TJC000/，2019年３月４日

2 資生堂子会社に不正アクセス，個人情報42万人分が流出か，
https://www.itmedia.co.jp/enterprise/articles/1612/02/news106.html，2019年３月４日

3 陸自システムにサイバー攻撃，情報流出か　国家関与も被害の全容不明，産経ニュース
https://www.sankei.com/affairs/news/161128/afr1611280003-n1.html，2019年３月４日

4 赤坂　亮，学内LANの現状及び今後の課題，九州ルーテル学院大学VISIO第30号，2003年，pp.64-67.

5 Gene，ネットワーク構築の基礎，VLAN間ルーティングとレイヤ３スイッチの基礎，株式会社毎日コミュニケーションズ，2009，pp.214-242.

6 日経NETWORK，絶対わかる！Windowsサーバー＆ネットワーク運用管理　超入門第２版，企業ネット実践ノウハウ　後任者に管理業務を引き継ぎたい，日経BP社，2009年，pp.192-197.

7 三上信男，セキュリティ超入門，ネットワーク超入門講座，SBクリエイティブ株式会社，2015年，pp.182-217.

8 Firewall/IDS/IPS,
http://www.infraexpert.com/study/security3.html, 2019年３月４日

9 「プロキシーサーバー」って何のこと？,
http://trendy.nikkeibp.co.jp/article/qa/internet/20030902/105779/，2019年３月４日

10 セキュリティ管理に有効なIEEE802.1X（ユーザ認証）機能,
http://panasonic.co.jp/es/pesnw/product/detail/05.html , 2019年３月４日