

学究活動に不可欠になった キャンパスネットワーク構築の一事例

河野 英太郎

前田 香織

†井上 智生

†北村 俊明

†岩根 典之

†末松 伸朗

kouno@ipc.hiroshima-cu.ac.jp

広島市立大学 情報処理センター , †広島市立大学 情報科学部
〒 731-3194 広島市安佐南区大塚東 3-4-1

あらまし

キャンパスネットワークシステムは大学における必須の情報基盤になっている。システムはサーバやネットワーク機器の安定稼働, 認証基盤確立, セキュリティ確保という基本的な機能を備えるとともに, 様々なニーズに対応したサービス提供が要求される。こうした背景の中, 1) 認証システム, 2) セキュリティ対策, 3) 教育支援形態, 4) ユビキタス性の実現について特に大きな変化が生じていると考え, その視点で広島市立大学の平成16年度の機種更新について報告する。セキュリティ対策については, 3年間の試験運用期間に行った実証実験を経て本格運用に移ったので, 試験運用で得られた知見もまとめる。

キーワード セキュリティ, 認証, 教育支援, ユビキタス性

A Case Study of Construction of a Campus Network for Academic Activity

Eitaro KOHNO

Kaori MAEDA

†Tomoo INOUE

†Toshiaki KITAMURA

†Noriyuki IWANE

†Nobuo SUEMATSU

Information Processing Center, Hiroshima City University

† Faculty of Information Science, Hiroshima City University

3-4-1 Ozuka-Higashi, Asa-minami, Hiroshima, 731-3194 , Japan

Abstract

A campus information network system is an essential infrastructure. The required functions of the system are stable running of servers and network equipments, authentication, security and so on. At the same time, the system should be flexible for various services required by users. Especially, the requirements have changed for a few years in four points; 1) Authentication, 2) Security, 3) Education assisted method and 4) Realization of ubiquity. In this paper, we describe new network system of our campus from these viewpoints. Also, we conclude the results of practical experiments of network security for three years in beforehand with the renewal.

key words Security, Authentication, Education assisted system, Ubiquity

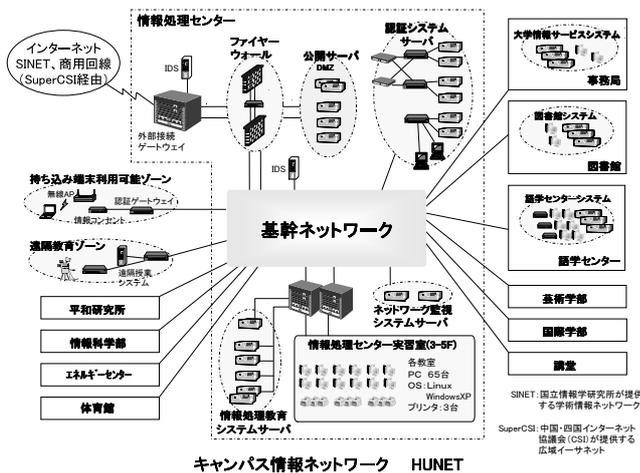


図 1: HUNET 構成概要

1 はじめに

大学におけるキャンパスネットワークの役割は大きく変わりつつある。研究対象としてのネットワークから、教育・研究活動を支える基盤のみならず、地域や社会との関わりに必須の情報基盤となってきた。稼働中の各種システムの停止の影響力は大きくなり、システム停止のない稼働を目的に、外部委託による運用モデルも提案されている [1]。このような目的とは無関係に、組織としての技術支援や管理が困難な場合や規模の小さな組織の場合、既に運用・管理を外部委託でシステムを運用しているケースも多い。

一方で、セキュリティポリシーを踏まえ、また、大学の教育、研究の実情や将来構想にあわせたキャンパスネットワークシステムの設計・構築は依然大学自身がその役割を担っている。広島市立大学(以降、本学)でも、平成16年10月に、開学以来2回目の大きな機種更新を行った。これに向け全学組織として機種更新検討のためのワーキンググループを組み、本学のネットワークシステムシステム「HUNET」の設計と運用方針について計画してきた。更新後のHUNETの概要は図1である。計画にあたって、近年の学術活動を支えるネットワークシステムの在り方の変化を考慮し、今後の変化を予想すると、1) 認証システム、2) セキュリティ対策、3) 教育支援形態、4) ユビキタス性(サービス利用可能範囲の拡大)の実現における変化が重要になると考えた。

本稿ではHUNETの機種更新について、この4つの視点から報告する。セキュリティ対策に関しては、前回の1999年[2]の機種更新では十分な対策がなかったため、今回の機種更新に向けて、2001年から3年間の試験運用期間を設け、本格的なセキュリティ対策システムを導入した。試験運用期間の実証実験は文献[3]で概要と途中報告を述べているので、本稿でその後の調査で得られた知見をまとめる。

2 認証システム

認証システムで考慮した点は、構成員のアカウント管理と各種情報の通信の暗号化である。機種更新以前の構成員のアカウントは情報処理センターの教育用機器の利用(ログイン)、メールサーバアクセス、ダイヤルアップやVPN接続のリモートアクセスの際に必要なものであった。更新後はこれに相当するアカウントをネットワークシステム用アカウント(HUNETアカウント)とした。この他に教務システム(履修登録、成績確認・登録、シラバス)や教員情報システム等教職員や学生全員の使用が必須となるサービスが開始する。こうしたサービス用のアカウントをサービスアカウントと称し、HUNETアカウントと分離した。利用者にとっては2つのアカウントとパスワード管理は煩雑になるが敢えて分離することにした。これは、構成員の従来のアカウントに対する管理意識の問題と、新規のサービスアカウントのセキュリティレベルの高さを考慮し、利用者に変更してアカウントに対する意識を高めてもらうためである。

移行に際しては、更新以前のHUNETと独立していた教務システムや図書システムの構成員情報とHUNETアカウントの情報を統合した。構成員の身分や実体のない情報などが発見したものの、管理主体が事務局と情報処理センターのみに集約されていたことと、構成員数は約3000という規模により、それほど大きな混乱はなかった。また、改めて構成員の分類等を見直す機会となった。総合認証システムを導入した佐賀大学の事例[4]等を参考にし、構成員情報の管理とサービスアカウントの管理は事務部門で行い、この情報から必要に応じて、情報処理センターでHUNETアカウントの登録作業を行う。

アカウント管理は従来NISを、認証にはRADIUS等を用いていた。機種更新後の多様なサービスシステムで共通に使用できる認証方法であることと同時多数アクセス負荷に対応できることを考慮してLDAPにした。利用者の一次認証先として教務システム、PCログイン(Linux, Windows)、図書システム、e-learningシステム、無線LANアクセス等11種類の認証先がある。これらのクライアントと一次認証先サーバとの間の多くの認証プロトコルにはHTTPSを用いる。一次認証先サーバとLDAPサーバ間もできる限り暗号化通信を図っている。認証先によっては暗号化対応されていないものがあり、部分的に平文が流れる通信区間があるが、専用VLANを設けたり、物理的に利用者が侵入できない場所とするなどの配慮をしている。

後期から新システムで授業を開始したが、認証の負荷等で問題は生じていない。負荷テストも行ったが、最も負荷のかかる新入生のパスワードの一斉同時変更は平成17年4月が最初となり、そこで評価を受けることとなる。

3 セキュリティ対策

今やインターネットに接続する組織ではセキュリティポリシーの策定やセキュリティ対策は必須といえるが、セキュリティ対策方法はそれぞれのキャンパ

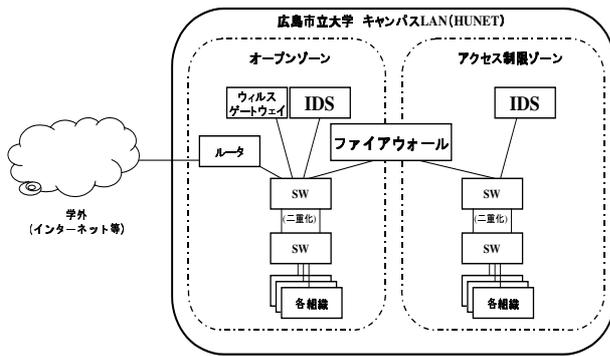


図 2: 実証実験に用いたネットワーク構成

表 1: サブネットのゾーン所属推移

ゾーン	2001年8月 (実験開始時)	2004年1月
FW外 (独自FW)	18 (1)	14 (7)
FW内	41	45

ネットワークの事情や使い方にあわせたものが求められる。本学では試行錯誤しながらセキュリティ強化を進めてきた

3.1 試験運用

本学の需要にあわせながらの強化を進めるべく、2001年8月から2004年3月までの期間、2004年度の機種更新に向けたセキュリティ対策の実証実験を行なった。2001年頃には関連機器の動向が不透明であったこともその背景にある。

3.1.1 ゾーン分割

試験運用の特徴は、学内を2つのゾーンに分け、サブネット単位でどちらに属するかを選択する点にある。1つは制限なく利用できるが、自己責任で安全を確保するオープンゾーンで、もう1つはファイアウォールの配下で通信制限を行い、ある程度の安全性が確保できるアクセス制限ゾーンである。図2に実証実験で用いたネットワークの構成図を示す。物理的な配線を変更することなく、VLANを多用してこれを実現した。2つの選択肢を設けて、利用者の事情にあわせて使用できるようにしたことは、それぞれの教育・研究におけるネットワークの使い方をあまり損なう事なく、結果的には利用者のセキュリティに対する意識レベルを向上することができた。

このことの現れとして、ゾーン所属数の変化を表1に示す。実験終了時には完全にファイアウォールの外部に存在するサブネット数は7となり、全学的な意識の高まりとともに何らかのセキュリティ機器を設置するサブネットが増えてきている。

表 2: ウィルスゲートウェイの利用

	2003年3月	2004年1月
登録済	28	32
未登録	16	12

3.1.2 段階的強化

ファイアウォールで防ぐことができないウィルスやワームについては、電子メールを媒介とした感染が多い。本学でもウィルス感染が不正侵入以上に深刻となり、ファイアウォールに続いて、2002年5月よりウィルスゲートウェイサーバを設置した。これも、画一的に義務づけることなく、管理サブネット単位で申告により設定する。各管理サブネットの登録状況を表2に示す。

次の強化策として公開サーバ数を減らすことを検討した。本学では、必要に応じて、Web、ネームサーバ、メールサーバ等公開サーバが設置され、管理者が独自に運用している。サーバがアクセス制限ゾーンの場合、ファイアウォールにHTTP、DNS、SMTP等を通させる必要がある。これによってアクセス制限ゾーン内に対する攻撃の可能性が高くなる。また、サブネット管理者はサーバのセキュリティ対策が随時必要だが、メンテナンスが間に合わない場合がある。そこで、対策が十分でない公開サーバを極力減らすために、従来通りのドメインを使用できるようなホスティングサーバを準備した。

3.1.3 予防策

セキュリティ対策の一つとして設置した、侵入検知システム (Intrusion Detection System; 以後IDSと呼ぶ) について述べる。IDSの欠点として、誤検知の問題がある。これに対応するためには、シグニチャの絞り込みなどいくつかの手法が考えられているが、決定的な手法がない。本学では、IDSのログをリアルタイムに問題を検知をするためのツールと位置づけず、むしろ、問題発生時に状況を確認するために使用してきた。また、IDSのシグニチャを観測し、1ヶ月に1度の間隔で情報を整理し、動向を調査することで、問題とおぼしき点があれば利用者への警告に使用している。

大学全体としてはファイアウォールやウィルスゲートウェイなどの導入により、ある程度のセキュリティを確保してきた。しかし、学内には既知の脆弱性が存在するまま運用されているPCやWSも多く存在している。特に多くの機器を抱えている情報科学部ではこれらの発見や情報収集が負担となる。そこで、学内に対して不定期に脆弱性診断を行ない、サブネットの管理者に対して報告した。脆弱性診断にはCSI [9] で提供されているNESSUS [8] を用いた脆弱性診断ツール [10] [11] を利用した。表3に2003年に行なった脆弱性診断の結果を示す。なお、括弧内には調査を行なった対象における割合を記す。

表 3: 2003 年診断時の脆弱性件数

所属	サブネット数	マシン数	項目数
FW 外	10 (71%)	70 (23%)	116 項目
FW 内	15 (57%)	29 (27%)	94 項目

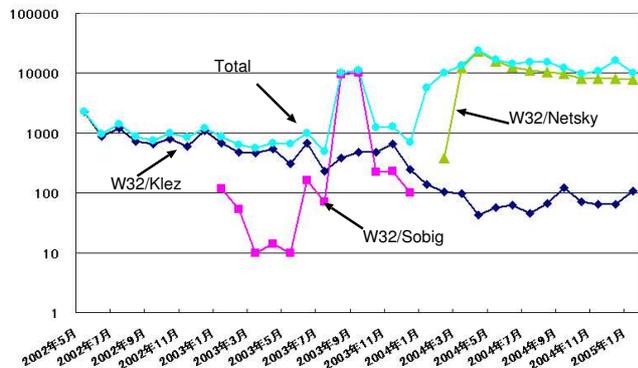


図 3: ウイルスゲートウェイによる検知状況

3.1.4 定例ミーティングによる分析

試験運用期間は毎月 1 回、機器の納入及び保守業者とともに定例ミーティングを行なう。ここでは、関連データの集計結果をもとに、以下のような点について議論をしている。

- 月間のセキュリティ対策のまとめ
- IDS の検出された全シグニチャの傾向分析
- メールウイルス検出の分析
- VPN 接続, ダイアルアップ接続, 持ち込み端末利用状況
- 通信トラフィック状況

データ集計の一例を図 3 に示す。こうした分析は 4 年目に入り、蓄積データもかなりのボリュームとなっている。新たなウイルス発生や何らかのきっかけで過去に感染したウイルスが発生するなど特定の発生件数が大幅に増加するが、これらには前後関係がないので、定式化できるような傾向を見出せず、問題発生の子測は難しい。しかし、管理者で状況を把握することは予防として効果を見出すことも多く、本格運用後も継続している。

3.2 本格運用

3 年の試験運用を経て、2 つのゾーン設置は本学においては、無理なくセキュリティの強化をできる方法だったと考えている。本格運用も引き続き、この方針を続けることとした。また、試験運用で使用した機器は検討の上、すべて本格運用にも導入することとし、予防策や定例ミーティングも継続している。導入した機器の選定においては、以下のような点を考慮した。

- ファイアウォール
試験運用では、プロキシ型とフィルタリング型の通信性能や安全の強度の違いを調査したが、本学の通信トラフィックでは、通常時にはほとんど通信性能が問題なることはなかった。結果的に一番困ったことは、ウイルス発生等異常時に大量のログが生成され、指定したファイルサイズごとに発生するログ処理やデータベース更新の頻度が高くなり、その負荷によって、通信のボトルネックや通信断が生じることであった。また、プロキシ型は通信制限の柔軟な設定ができないことも問題であった。本学のように、利用者の使用方法も考慮しながらのセキュリティ確保を行なう場合、運用中にポリシー変更にともない、TCP や UDP のサービスポート単位での設定が発生することもある。プロキシ型の場合、サービス単位でのアクセス制限のために、同時に複数のポートで通信制限の設定がなされたり、ポート単位のフィルタリングを設定に混在すると性能低下を招くこともあって、本学の需要には対応しにくい部分が多かった。

そこで、本格運用ではステートフルインスベクション機能をもつパケットフィルタ型の機器を導入した。これにより基本的にはパケットフィルタ型と同じような設定の容易さを持ちながら、FTP など状態を持つプロトコルへの対応などが可能となる。ファイアウォールが通常時、異常時ともに通信ボトルネックにならないことも配慮した。また、試験運用期間にはコスト等の制約で冗長構成がとれなかったが、機器の障害時に対応できるように、冗長構成をとっている。公開サーバの安全レベルを上げるため DMZ を新たに設け、試験運用時にはオープンゾーンに設置していた全学の認証サーバ、Web サーバやホスティングサーバなど公開サーバは DMZ に設置した。

- IDS
試験運用期間に使用していた IDS は、ファイアウォールと同様に、異常時にログの整理で高負荷になり、CPU 性能の限界もあって、十分なパケット採取ができなかった。また、ログが IDS 独自のフォーマットのために、後に管理者が分析するためのデータの加工において困難な点が問題点であった。

そこで、本格運用ではログ処理の負荷が高くないような、データベースのシンプルなものを採用した。また、増大する通信トラフィックにも耐えられるようにパケットキャプチャが可能なものを選定した。IDS の位置付けは試験運用と同様、リアルタイム監視をするものではなく、異常時の分析と通常時の予防に使用している。試験運用と同じく、月例で検出された全シグニチャ情報の集計を行う。これにより、SoftEther や P2P ソフトの使用などが観測されている。各管理サブネットのトラフィックの急激な上昇とあわせて観測することで、ウイルスなどの感染拡大や踏み台攻撃の拡散を見つけることもある。

- メールサーバとメールウィルスゲートウェイ
従来、メールサーバは UNIX WS の sendmail
を使用して構築していたが、sendmail だけ
でなく、OS そのものの脆弱性対応も頻繁に必
要になっている。また、メールサーバとウィ
ルスゲートウェイが分離していたことから、同
一メールサーバを使用するメールの送受信の
ウィルス検知ができていなかった。

そこで、機種更新後はメールサーバをアプ
ライアンスに変更し、SMTP/POPサーバを1台
に集約した(情報科学部は順次対応)。また、
メールウィルスゲートウェイとも連動させ、学
内外のメール送信、受信ともウィルス検知し
ている。認証はLDAPとし、冗長化構成とし
ている。アプライアンスそのものでは、メー
リングリストのアーカイブができなくなった
ため、アーカイブは別のサーバで行っている。
利用者によっては、学内でも商用プロバイダ
のWebメールを使用している場合があり、そ
れによって感染しているケースが生じた。Web
メールではメールウィルス検知がなされない
ことを認識できていない利用者もあり、広報
に努めている。

4 教育支援

情報処理教育の在り方について検討し、近年の
教育形態の変化に追従すべく、以下のような教育
支援システムが導入された。

4.1 情報処理教育

情報処理センターには情報処理教育用の実習室
が3室(各65人収容)ある。ここでは情報処理や
プログラミングなどの科目が開講され、引続き実
施されることとなった。端末を設置しない形態や
シンクライアントなどについて議論を経て、結局、
LinuxとWindowsのデュアルブートのPCを各実
習室に65台ずつ設置し、必要なソフトを導入した。
学生への端末購入は保守体制の確保が困難(生協
などの支援が受けられない)、シンクライアントの
場合はコスト削減が困難などの理由による。3フロ
アともほぼ同じ環境である。バージョンアップやセ
キュリティ対応、障害復旧のためにPCイメージの
一斉配布用の管理ツールや電源ON/OFFの遠隔操
作など約200台のPCの集中管理用のシステムが
導入されている。

また、今回の機種更新から語学センターの
PC(Windows,平成16-17年度で約300台を順次
更新)を中心とした語学教育システムの運用管理を
情報処理センターと語学センターとで連携して行
うこととなった。これにより、両センターで設置す
るPCの機能を可能な範囲で共通化させることが
できた。学生の利用可能場所の選択肢を広げること
ができた。

4.2 e-learning システムの導入

学生の初等中等教育における情報処理の習得レ
ベルや家庭での利用経験にはかなりの個人差があ



図 4: 遠隔授業の様子

る。そもそも、情報処理教育の講義内容につい
ては議論が分かれるところである。個人のレベル差
の解決の1つとして、e-learningシステムを採用し
た。今回の機種更新では、WebCT[5]とそのコンテ
ンツ(Microsoft社のWord, Excel, PowerPoint習
得用と情報倫理)が導入されている。

e-learningシステムへの教員の関心は高く、コン
テンツ作成の講習会の受講希望者は多い。履修シ
ステムと連携しており、教員の担当講義ごとに履
修者のみがアクセス可能なコンテンツ用フォルダ
(コース)が自動的に作成される。各コースには大
学で計画されている授業評価用アンケートがコン
テンツの1つとして自動的に作成される。それ以
外の授業コンテンツの作成は教員に委ねられるが、
今後5年の間に豊富な教材がそろふことを期待し
ている。

4.3 遠隔講義対応教室

大学の将来構想計画を受け、通常教室に遠隔教育
用の設備を設置し、遠隔講義教室を構築した。遠
隔教育の様子や教室の利活用方法を学内に周知す
るために、ワーキンググループ主体で大学間遠隔
授業や高大連携などを実験的な試みとして実施し
てきた[7]。このうち、平成16年度後期に実施し
た慶応義塾大学、京都大学との遠隔講義を平成17
年度は単位認定の授業として開講することが決まっ
ている。図4は3地点授業の広島市大の受講の様
子である。

この教室には、教室前方に3面スクリーン、そ
れに照射用の天吊の液晶プロジェクタが3台設置
されている。また、講師画像、資料映像用の3台の
カメラと本学の映像用の2台のカメラが設置され
た。映像、音声の入出力操作やレベル調整はラック
内の機器のマトリクス・スイッチや操作卓で行う。
この教室へのネットワークは遠隔教育ゾーンとし
て帯域を確保し、ポリシを分離している。

5 ユビキタス性の実現

今回の機種更新以前に、構成員が家庭や出張先から HUNET を利用できるように、ダイヤルアップ接続や VPN 接続が可能な設備を設置している。これにより HUNET への利用範囲が拡大されている。家庭のインターネット接続の普及が高まり、VPN 利用はダイヤルアップを抜いている。

さらに HUNET には、学究活動の支援として、いつでもどこでも様々なサービスが享受できる環境づくりへのニーズが高まっている。そこで、以下のような仕組みを導入した。

5.1 持ち込み端末ゾーンの設置

本学では学生が利用可能な端末の台数は比較的恵まれているものの、自宅で使用している PC を大学で使用したいという要望が出てきている。また、大学の構成員以外へのネットワーク資源の提供が必要な場面も増えている。そこで、認証ゲートウェイとして FEREC[6] を図書館、情報処理センター等 4 箇所を設置した。これらのセグメントは持ち込み端末ゾーンとして、学内のオープンゾーンやアクセス制限ゾーンと異なるポリシーで運用している。認証ゲートウェイの運用についても、実証実験期間を半年位設け、このゾーンのポリシー決定や運用上のセキュリティ等について検討した。

5.2 大学情報サービスシステムの導入

5 年前の機種更新の際にも、教務関連のシステムと HUNET と連携させ、学生の成績管理や施設予約をオンラインで行いたい、履修状況をタイムリーにみたい教員からの要望があったものの、セキュリティ確保の面から前回は分離した。今回は大学情報サービスシステムと称して、大学生活に密着したシステムが導入され、各種手続きがオンラインでできるようになった。学生は履修登録、成績確認、就職支援システム、休講・補講・教室変更等が、教員は履修状況確認、成績入力/確認、シラバス入力、教員情報公開、施設予約、庶務関連がオンラインで手続きできる。このサービスは HUNET 接続な環境であれば、Web ブラウザで利用でき、自宅など遠隔地からも VPN 接続に限り可能である。

6 まとめ

学生も教員も新たに導入された HUNET を平成 16 年 10 月から使い始めている。2 つのアカウントの意味や使い分けについては、まだ十分に浸透していないが、Web ページや掲示による広報、ガイダンスの開催などを実施し、授業や自習における使用で大きな混乱は起きていない。教員は次年度のシラバス入力など必要に迫られて、授業担当者は全員、大学情報サービスシステムを使用し始めた。何とか入力作業は進んだものの、入力インタフェースの悪さなど既に改善すべき点も挙っている。大学情報サービスシステムのコアとなる教務関連の手続きの本格始動は平成 17 年 4 月である。学生へのアカウントやパスワードの配布方法の検討、

利用方法のガイダンス等の準備を進めていかなければならない。並行して、更新後のシステムが 1. 章に掲げた 1) 4) について、技術的な、また、利用者の視点での評価が必要と考えている。

謝辞

機種更新においては情報処理センター機種更新ワーキンググループの方々にお世話になった。また、セキュリティの実証実験には本学情報処理センタースタッフおよび本学情報処理センター専門委員会各位にご協力を頂いた。ここに記して謝意をあらわす。

参考文献

- [1] 八代一浩, 菊池豊, 林英輔, “稼働率の改善を目的とした自律分散型大学ネットワークシステムの実装と運用,” 情報処理学会研究報告, 2004-DSM-32, pp.7-12, 2004.
- [2] 前田香織, 河野英太郎, 石田賢治, 岩根典之, “キャンパス情報ネットワークシステムの分散管理の粒度,” 情報処理学会研究報告, 2000-DSM-18-5, pp. 25-30, 2000.
- [3] 河野英太郎, 前田香織, 三好哲也, 浅田尚紀, “相反するポリシーを実現するセキュリティ強化の試み,” 情報処理学会研究報告, 2002-DSM-26-8 pp. 43-48, 2002.
- [4] 江藤博文, 渡辺健次, 只木進一, 渡辺義明, “全学的な共通情報アクセス環境のための総合認証システム,” 情報処理学会研究報告, 2002-DSM-27, pp.31-36, 2002.
- [5] WebCT ホームページ, http://www.emit-japan.com/webct_japan/.
- [6] FEREC ホームページ, <http://www.ferec.jp/>.
- [7] 平成 15-16 年度広島市立大学特定研究「IT を用いた初等中等教育と高等教育のシームレスな学習空間の形成とその応用に関する研究」研究成果報告書, 2005. (<http://lab.ipc.hiroshima-cu.ac.jp/projectHCU/>)
- [8] NESSUS Project, <http://www.nessus.org/>.
- [9] 中国・四国インターネット協議会ホームページ, <http://www.csi.ad.jp/>.
- [10] 田島浩一, 西村浩二, 相原玲二, “脆弱性診断サービス,” CSI インターネット利用研究会 2005, pp.15-18, 2005.
- [11] 田島浩一, 西村浩二, 岸場清悟, 相原玲二, “セキュリティ脆弱性診断支援システムの構築,” 情報処理学会分散システム/インターネット運用技術シンポジウム 2004 論文集, pp.7-12, 2004.