全学プライベート IP 網の構築と運用

Construction of Private Network in Shizuoka University

長谷川孝博・望月邦昭・高橋秀年・高田重利・井上春樹・八巻直一
Takahiro Hasegawa, Kuniaki Mochizuki, Hidetoshi Takahashi,
Shigetoshi Takata, Naokazu Yamaki

center@sains.ipc.shizuoka.ac.jp

国立大学法人 静岡大学 総合情報処理センター
〒432-8561 静岡県浜松市城北 3-5-1

Information Processing Center, Shizuoka University
Johoku 3-5-1, Hamamatsu, Shizuoka 432-8561, Japan

概要

2006 年度に行われた新情報基盤整備において，全学規模のプライベート IP ネットワークの新設を行い，学内 LAN の移行・運用プロジェクトを実施した．A クラスのプライベート IP とグローバル IP ネットワークを各棟のフロアスイッチへ導くマルチフォーミング方式は，全学のサーバサービスの継続性を保証するとともに，多数の端末のプライベート IP 化を円滑に進行させた．認証機能付 L2 フロアスイッチが提供する認証ポートは，全学に散在していた部局運用の情報コンセント教室等の統合化を促進した．アカウント統合認証システムを導入し，全ユーザにパスワードの定期変更を要求する管理策を実施した.全学プライベート IP ネットワークの導入により，幅広いユーザ層への情報セキュリティに対する意識向上と実践的セキュリティの向上が図られた．全学規模のプライベート IP ネットワークの構築，切り替え，運用について，技術および情報セキュリティの観点より報告する．

キーワード

Private Network, Information Infra-Structure, ISMS, LDAP, Network Authentication

1. はじめに

静岡大学では B クラス約 65000 本のグローバル IP(GIP)を有し,事務系や一部の研究室で運用される NAT 環境を除いて，研究・教育活動の多くを GIP のネットワークに依存してきた．WAN 直結の学内 GIP ネットワーク(以下「GIP 網」という)の単純さと透過性は便利なものとして，全学ユーザに長期間に渡り受け入れられてきた．このように長く続いた旧情報基盤の GIP に依存したネットワーク環境は，その脅威や安全対策への意識までも GIP 網の枠内に閉じてしまう傾向にある．

これに対して，情報セキュリティの基本的な対策のひとつである社内 LAN（プライベート IP ゾーンの構築）の考えを大学ネットワークに適用するためには，1)学内の多様なネットワーク利用の実情，2)適用スケールの物理的広さ,3)ユーザに与える利便性，可用性，サービスの継続性への不安，などいくつもの課題が列挙され，その実現には極めて多くの困難が予想される．

静岡大学総合情報処理センター(以下「IPC」という)では，情報セキュリティマネジメントシステム(Information Security Management System：ISMS)[1)]の事実上の標準規格であったBS7799-2:2002 およびISMS認証基準Ver.2.0 を 2003 年 12 月に取得し，現在も運用中である．ISMSの認証取得は，全学的な情報セキュリティへの機運を高めるよい契機となった．

表-1: 新旧情報基盤における全学ネットワークの変化

	IP	サーバ	クライアント
旧情報基盤 平成 17 年度以前	旧 GIP 網	サーバ	端末（クライアント）ただし GIP 利用
	旧 PIP 網	情報基盤による全学的な提供はなし	
新情報基盤 平成 18 年度以降	GIP 網	GIP サーバ（DMZ サーバ）	GIP 端末
	PIP 網	PIP サーバ（イントラサーバ）	PIP 端末

静岡大学では ISMS 認証取得直後より，2006 年 3 月に行われた情報基盤整備の中心課題として，全学を包括するプライベート IP ゾーン(以下「PIP 網」という)の新設を計画してきた.技術的な導入に留まることなく，全学のユーザが PIP 網へ参加していく真のイントラネットワークの実現を目指し，同時に情報セキュリティの抜本的な改革と推進を図るものである．すなわち，新情報基盤の基本コンセプトを情報セキュリティの確保とする整備を行った.

PIP 網の整備は，サーバ・クライアント(端末)という側面からみても，1)無用の脅威に晒されてきた GIP 網の端末群の一掃，2)セキュリティ意識や管理スキルの脆弱なサーバ群の大幅な縮小，PIP 網への移動によるイントラサーバ化，3)セキュリティ管理の行き届いた真の公開サーバ群の認可と保護，などいくつかの効果が期待される．しかしながら，前述のようにその実現には，技術・組織・人（ユーザ）・時間という次元の異なる階層での問題の解決を同時進行しなければならない．確固たる情報セキュリティ理念に基づく準備と仕組みを備えることが重要である.

2006 年の新情報基盤整備の主な調達物品リストは，研究用計算サーバ 1 式，基幹各種サーバ 14 台，認証系サーバ 4 台，ストレージ 2 基，長距離伝送装置 4 台，センターL3 コアスイッチ 2 台，L2 棟・フロアスイッチ 339 台（うち 100 台は認証機能付），ファイアウォール，L4 スイッチ，IPS 装置，教育用情報端末 493 台，授業支援システム，授業支援のための各種 AV 装置，研究用・教育用の各種アプリケーションソフトウェア,他多数の周辺機器などが含まれる．本学のキャンパスは,浜松市と静岡市に約 80km の距離をおいて位置しており,その間を 10Gbps の長距離伝送装置で接続している．新情報基盤整備は，両キャンパスの全棟全フロアの L2 スイッチ 339 台の総入れ替えを含む本学における最大規模の事業のひとつである．IPC のユーザアカウント数は約 12500 で，全学教職員数にほぼ同じである.

本論文では，新情報基盤整備プロジェクトにおいて行われた全学 PIP 網の実現方法について，技術と情報セキュリティの両側面から，運用開始前後の動向を含めて報告する.

2. 全学 PIP 網の構築と実装

旧情報基盤における学内グローバル IP ネットワークでは，サーバとクライアントの単純な関係しか存在しなかったが，新情報基盤では,「PIP／GIP」および「サーバサービスの有／無」の組み合わせから，GIP サーバ，PIP サーバ，GIP 端末，PIP 端末の 4 つの計算機運用形態が学内に混在する結果となる．これらの関係を**表-1** に示した．ここで，旧情報基盤における学内グローバル IP ネットワークを旧 GIP 網と称し,新情報基盤におけるグローバル IP ネットワークおよびプライベート IP ネットワークをそれぞれ GIP 網，PIP 網と称している.

長期に渡る旧情報基盤における旧 GIP 網の運用実績は，複雑化した新情報基盤の受容の難しさを想像させる．その一因として，次のような大学特有の事情が列挙できよう.

1) 情報リテラシやセキュリティ意識の個人格差
2) 利用者の大規模な更新（学生の入学と卒業・修了）
3) 教育・研究活動の継続性の優先度の高さ
4) 可用性や多様性への強い要求

本プロジェクトでは，幅広いユーザ層に生じる新情

表-2：フロア L2 スイッチのマルチフォーミング

IP	VLAN	ユーザへの説明
GIP	a.b.v.0	GIP はそのまま利用できます.
PIP	10.b.v.0	a を 10 に変更するだけです.

報基盤への移行の問題を最小限に抑えつつ，その環境下でユーザ自身が自発的に PIP 網へ移行していける仕組みやサービスを提供することが重要であると考えた. 可用性や多様性を重んじる多くのユーザは，新情報基盤に対して「より安全に」よりも「より早く便利に」との期待感が高い．旧 GIP 網のサービス継続性は必須の要件であるが，同時に PIP 網を利用することが，さらに便利になるという印象を持たせることが重要である．これらの問題を解決するための新情報基盤の仕組みを次のように提供した.

2.1 端末の PIP への切り替えの容易さ

単なる PIP 網の導入だけではなく，PIP 網の全学的な利用促進を目的とした本プロジェクトでは，全学に 10000 台を超えて散在するユーザ端末の PIP 化をユーザ自身が混乱なく簡単に行えなければならない. その手続きは，情報リテラシの個人差に依存しない解り易いものであり，研究室や教員居室におけるハブ分岐やサーバ環境などの末端ネットワークの再構築を要求してはならない．これらの問題を解決するために，本プロジェクトでは，フロア L2 スイッチの任意のポートから PIP 網と GIP 網のマルチフォーミング方式を採用した．ここで構築したマルチフォーミングとは，PIP と GIP の異なる 2 つのセグメントを基幹のコアスイッチからフロアスイッチまで並行に導き，フロアスイッチの同一ポートから PIP または GIP のいずれかを選択的に利用可能とする．ユーザは，利用機器を PIP へ変更する際にもフロアスイッチのポート変更を行なう必要がない．さらにハブで分岐した場合，その配下の異なる機器においても GIP と PIP のいずれかを選択し取得することが可能である.

マルチフォーミングの片方の GIP 網を旧 GIP 網と同じにすることで，切り替え直後において設定変更を行わないユーザ機器が，自動的に切り替え前の GIP を取得するようにした．これは，通常の基盤更新で行われる継続性を保証するための一般的な手法である．本プロジェクトの最大の工夫のひとつは，１オクテット値が 10 で，かつ GIP 側の VLAN 値の等しい A クラスの PIP 網をマルチフォーミングの片方に採用したことである．この選択により，ユーザへの PIP 網へ移行説明を簡単に行うことができる．その様子は表-2 にまとめられる．ここで，a.b. は本学の B クラスの IP であり，v はフロアスイッチ単位に設定される VLAN 値を表す．このとき，PIP 網内の名前解決を行うために DNS サーバも従来の外部向けか

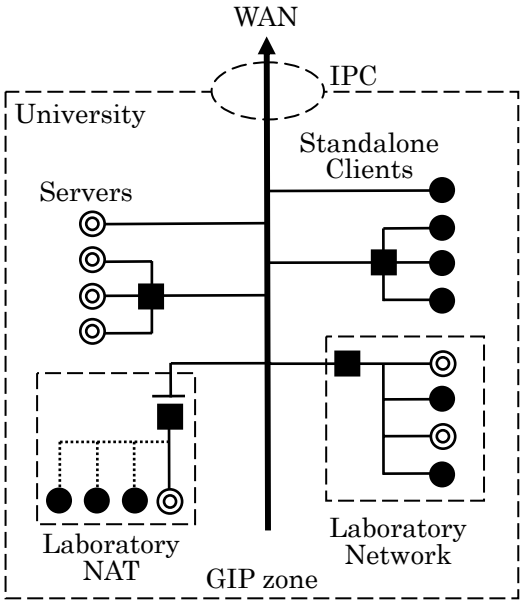

図-1：旧情報基盤ネットワーク

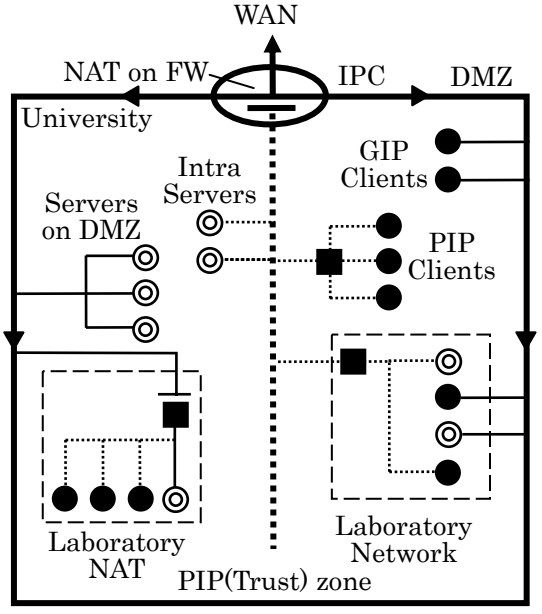

図-２：新情報基盤ネットワーク

ら内部向けに変更しなければならない煩わしさは回避できなかったが，多くのユーザにとっては使い慣れた IP 値が大きく変化しないことに安心を覚えるようであった．また本手法は，旧情報基盤で行われていた部局内や学科内のVLANの使い分けをPIP網へもそのまま適用できるという長所がある.すなわち，新情報基盤では，B クラスの旧 GIP 網に，新しく A クラスの PIP 網が導入されるため，理論的に利用可能な IP 数は 250 倍強に増加したことになるが，旧 GIP 網に対応する PIP 網のひとつの VLAN のみをユーザに示すことで，ユーザの混乱を低減させることを優先させた.

2.2 サービス継続性確保について

旧 GIP 網で提供されていた各種の学内情報サービスの継続性を保証することは，端末の GIP，PIP の別に依存することなく優先されなければならない．とくに，PIP 端末への移行したユーザが既存サービスの利用障害に直面することは，PIP 利用の意欲を大きく低下させることになりかねない.

近年，多くの大学においては，会計支援，教員データベース,図書館サービス,ドキュメントシェア，学術リポジトリ[2] などの学内情報サービスが稼働している．本学においても，これら各種の情報サービスが旧GIP網の上で整備され,キャンパス毎または全学的規模で運用されてきた．さらに，部局や学科，各研究室において運用される局所的なサーバサービスは学内の各所に散在し，その数や運用実態を正確に把握することは困難な状況にある.

図-1 は旧情報基盤における旧GIP網のイメージである．旧情報基盤では，ごく限られたセキュリティ意識の高い研究室や部署において，NAT 構成による PIP 網（破線）が存在した．これらはブロードバンドルータ等（図中：|■）の配下に局所的に存在したのみである．多くのユーザは，サーバ（図中：◎）／クライアント（図中：●）の別なく無尽蔵に GIP 網（実線）を利用している状況であった.

新情報基盤では，IPC の基幹ネットワーク構造の大変革を行い，旧情報基盤下において存在すらしなかった A クラス PIP 網からのユーザアクセスに対しても学内サーバサービスの継続性を可能な限り保証することを試みた.**図-2** は,新情報基盤における GIP 網と PIP 網(Trust zone)のイメージであり，**表-1** に示した 4 種類のサーバとクライアント（◎実線：GIP サーバ，◎破線：PIP サーバ，●実線：GIP 端末，●破線：PIP 端末）が混在する様子が示されている．IPC 内では，ギガのスループットを有するファイアウォール（以下「FW」という）で全学規模の NAT を実現し，学内 LAN（PIP 網）を隔離した．このとき旧 GIP 網は DMZ を構成することになる.DMZ の上に位置する学外向けの GIP サーバは，隣接する PIP 端末に対しても IPC 内の FW によるアドレス変換を受けてアクセスされる．ネットワーク的に遠くなる学外向けサーバの代替手段として，PIP 網に設置するイントラサーバが経路の短縮とセキュリティ確保を同時に実現できることをユーザに説明した．同時に，学内向け／学外向けのサーバサービスの明確な運用の切り分けは，新情報基盤における前提条件であることへの理解を求めた.

イントラサーバは，その概念において新規性はなくとも，セキュリティ管理レベルや意識にばらつきのある学内のサーバ管理者に，その利点や意味を深く理解してもらい，移行作業を行なわなければならない．したがって，全てのエンドユーザはもちろんであるが,サーバ管理者にも負担を与えることなく，切り替えの時間的猶予を与える情報基盤整備を行うことが重要である．本プロジェクトでは，切り替え直後の端末の PIP 化の重点的な実施を呼びかけたが，その一方で，切り替え後にも多数の GIP 端末利用者が残留することを想定したシステム構築を行なった.切り替え直後の GIP 端末では，WEB 閲覧やメール利用は可能であるが，すでにパスワード変更は GIP 端末に対して制限されており，PIP 端末から行なわなければならない．その事実を知ったユーザが自発的に端末の PIP 化を実施していくことを期待した．この他にも，WEB サーバへのコンテンツのアップロードや，メールの転送設定などを段階的に PIP 専用サービスに切り替えていくことで，ユーザの問い合わせや混乱を時間遅れに分散させながら端末の PIP 化を確実なものとした．現在，PIP 端末への切り替えは，全学的に順調に進行中であり，切り替え日から

表-3：全学アドレス変換テーブル

PIP/24	DMZ	WAN
10.b.0.0～10.b.3.0	a.b.d.16	a.b.w.16
10.b.4.0～10.b.7.0	a.b.d.17	a.b.w.17
10.b.8.0～10.b.11.0	a.b.d.18	a.b.w.18
10.b.12.0～10.b.15.0	a.b.d.19	a.b.w.19
…	…	…
10.b.248.0～10.b.251.0	a.b.d.79	a.b.w.79
10.b.252.0～10.b.254.0	a.b.d.80	a.b.w.80
10.x.0.0	a.b.d.81	a.b.w.81
10.y.0.0	a.b.d.82	a.b.w.82
新設可能	…	…

半年経過した 10 月を目標に,会計支援システムなどの全学規模の主要サービスを PIP 網へ移行する計画である.

2.3 アドレス変換(NAT)規則

旧 GIP 網のサーバサービスの継続性確保のために FW に実装した NAT 規則例を**表-3** に示す.

１行目の変換は,B クラス GIP(a.b.0.0/16)に対応する 10.b.0.0/16 からはじまる 4 つの VLAN (10.b.0.0～10.b.3.0)を GIP 側の空き VLAN のひとつ d を決めて GIP(a.b.d.16)へ静的に変換した．同時に WAN (INTERNET)側へ d とは異なる別の空き VLAN のひとつ w を決めて 4 オクテット目の値が同じ値の GIP へ変換した．この規則を繰り返し適用し，10.b.0.0 の B クラス PIP への変換テーブルを網羅するように構成した．さらに変換規則の終盤では，10.b.0.0/16 とは異なる 10.x.0.0/16 や 10.y.0.0/16 などへ運用目的の異なる特殊なサービスネットワークをまとめることができた．A クラス PIP が持つアドレス空間の広さはこのような場合に有効に機能した．導入した FW は，最大約 250 の変換規則に対応していたため，表-3 の変換規則を一括定義，実装することが可能であった．運用開始後も十分なスループットが得られており，PIP 端末から DMZ サーバへのアクセス障害や遅延などのユーザ報告は皆無である．また，多くの DMZ 上のサーバサービスは，a.b.0.0/16 の GIP の識別によってアクセス制限されているため，全学的

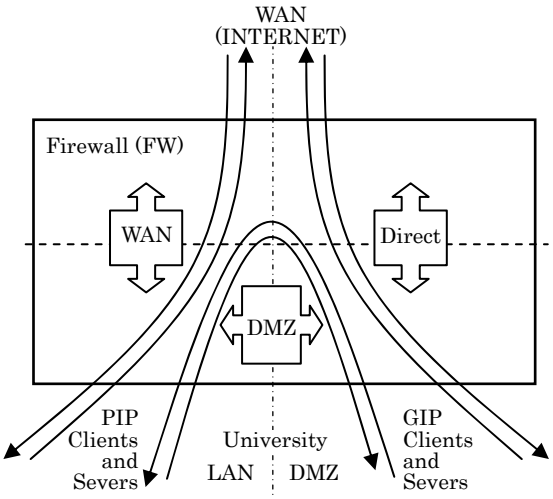

図-3：FW における全学アドレス変換の実装イメージ

な主要サービスになるほどこの変換規則は問題なく運用可能であった．**図-3** に FW における表-3 の実装イメージを示す.

一方で，このような変換規則によれば，理論的に 1000 を超える PIP クライアントがアドレス変換後の 1 つの GIP で DMZ 上の学内サーバへアクセスを行なう可能性があり，PIP 端末から GIP サーバへの経路において組織や個人端末を識別する精細なアクセス制御が困難になる．例えば，旧情報基盤で行われていたような学科，フロア，研究室単位，あるいは個人を接続 GIP から識別することは事実上できなくなる．このようなアクセス要求の解決が容易でない理由は「外部向け，内部向けサーバの明確な住み分け運用を行う」と謳った基本方針に反しているためである．このことは，サーバ管理者に対して次のことへの理解と認識を深めるための契機を与える.

1) 運用するサーバサービスが，対象組織からのアクセスに対して閉じるべきか否かを判断し，方針を決めなければならない.
2) 外部向けと内部向けのサービスが混在している場合は，サーバを分離することを検討しなければならない.
3) 内部向けサービスをイントラサーバに移行することで，学内にある対象組織からの精細なアクセス制御の要求に応えることができる．そのために，サーバ管理者は対象組織のメンバに対して端末の PIP 化を励行する必要があ

表-4: Instant Messenger の機能とネットワークの関係．○：利用可能，×：利用不能

アクション			メッセージ送信	ファイル送信	音声・ビデオ招待	アプリケーション共有招待	リモートアシスタント要求
旧情報基盤(GIP→GIP)			○	○	○	○	○
新情報基盤	学内通信	PIP→PIP	○	○	○	○	○
		PIP→DMZ	○	×	×	×	×
	PIP(学内)→WAN		○	×	×	×	○
	DMZ→PIP(学外)		○	○	×	×	○

る．

いずれも全学的な情報セキュリティ向上という目的達成のための好ましい動機付けとなる．サーバ管理者に高度な判断や作業を集約させる一方で，エンドユーザには端末の PIP 化を早期に行うことが，各種サービスの継続性を高めるための唯一の選択肢であることを強調できる．さらには，学外向けのサーバを運用する管理者の責任意識を高める効果もあると期待している．これらのことは，社内 LAN を利用することの既知の利点であるとしても，多様なサーバサービスと管理方針の混在する大学組織において，本手法の持つ柔軟性と有効性は改めて評価できるものと考える．

2.4 GIP 端末の運用方針

新情報基盤では， GIP 端末（表-1，図-3 参照）数を全学的に縮小することが重要な目的のひとつである．本プロジェクトでは，公のサーバサービスは行っていないにもかかわらず，GIP のまま利用している端末群を GIP 端末と総称した．その内訳は次に示される．

1) 旧情報基盤から GIP 設定のまま利用している端末.
2) 学外から特定個人向けのみのサーバサービスを提供する GIP サーバ.
3) 外部サーバサービス機関から個人を識別するために GIP の利用を求められている端末.
4) ビデオ会議やインタラクティブ性のある高度なコミュニケーションツールを学外拠点間で利用する端末.
5) 2)～4)の利用目的が混在している端末.

ここで，1)は端末の PIP 化の実施努力によって PIP 化が容易な端末群であり，全体に占める割合が最も多い．

2)は，Windows XP などのリモートデスクトップサーバなどを利用して学外からの接続を行う少数のユーザである．これらのユーザは，学内に閉じたメールシステムの遠隔利用を目的としている場合が多いため，まもなく予定している WEB メールシステムの導入によって，打開策を示すことができると考えている．

3)は，教育・研究活動の優位性と新情報基盤の基本方針が矛盾を起こす難しい問題のひとつである．本プロジェクトにおいては，図書館のデータベースサービスと学会が運用する会員接続サービスに関する問い合わせが実際に寄せられた．広く展開されている学術サービスにおいても，会員個人を識別する手段として固定 GIP を要求している事実は，全学規模の PIP 網の整備や運用が多くの大学組織でまだ一般的でないことを裏付ける．この問題の解決策として，次の選択をユーザに提示している．i)外部サーバサービス機関に新情報基盤への理解を求め，アドレス変換（表-3）後の WAN 側 GIP からのアクセス許可を得る.ii)外部サーバサービス機関の要求を満たすために個人を識別可能な GIP 端末を利用する.

4)は，端末の PIP 化を行うことにより生じる通信上の制限である．当初，メールによる添付ファイルの送受信やブラウザからのフォーム投稿，ファイル投稿ができなくなるのではとの不安が寄せられた．これらの基本機能は PIP 端末からでも問題なく利用可能である．実際に影響を受ける通信機能は IM（インスタントメッセンジャー)のようなより高度なコミュニケーションツールにおいて現れる.**表-4** に IM の機能とネットワークの関係を示す．GIP しか存在しなかった旧情報基盤においては，全ての機能が利

用可能である．これに対して新情報基盤では，ネットワークの組み合わせによって 4 種類（表-4 の新情報基盤：PIP→PIP，PIP→DMZ，PIP→WAN，DMZ→PIP）に場合分けされる．いずれの場合でも，最も利用頻度が高いと思われるテキストメッセージ送信が可能である．また学内の通信(PIP→PIP)においては，双方の端末が PIP であれば，旧情報基盤と同様にすべての機能が利用可能である．このことは，端末の PIP 化の促進にも寄与するものと思われる．

大多数のユーザは,PIP 端末への移行によって GIP 端末時の利便性を大きく損なうことはないが，その一方で，通信需要の多様化や研究・教育に対する優先度から一部のユーザにおいては，GIP 端末の利用を許容せざるを得ないことも事実である．これらのユーザは，PIP 網に閉じた必須のサービスを利用するために端末環境の二重化（GIP 端末と PIP 端末の共存環境の構築）が避けられない．そのオーバーヘッド対応は，当事者負担の理解と協力をお願いしている現状である．しかしながら，GIP 端末の選択を強く抑制することなく，内向きと外向きの端末の明確な分離を求めるという基本方針は，多くのユーザにとって受容可能なものであると判断している．

3. アカウント統合認証システム

旧情報基盤において，サーバサービス毎に同期しない複数のパスワード管理はユーザ，IPC スタッフともに大きな負担のひとつであった．安易にパスワードを消失してしまうユーザが存在する一方，ISMS の観点から，パスワード再発行の手続きを厳密に処理したい IPC との意識の差は大きい．

新情報基盤では，LDAP によるパスワード同期を実現し，メールシステム，情報教育用端末，情報コンセント等の主要な情報システムにおいて全学規模の統合認証環境を実現した．システムの概要を**図-4** に示す．本システムに関連する新しい 2 つの取り組みについて述べる．

3.1 L2 フロアスイッチ認証

アカウント統合認証システムは，認証機能付きの L2 フロアスイッチ（日立電線 Apresia）の大量導入によって実現した．学内の必要各所に配置された 100 機の認証スイッチは,上位の Radius サーバ,DHCP サーバとの連係を経て，認証を受けたクライアントへ PIP の配信を行う．フロアレベルでの認証導入の長所は次のとおりである．1)認証負荷の分散，2)上位ネットワークの構成に左右されない，3)セキュリティゾーンの拡大が容易，4)ポート単位に認証の要・不要が設定可能であるため，同じ階下の部屋毎の必要性に応じて認証ポートの配布を行うことができる，5)特別なクライアントソフトウェアのインストールが必要ないため，学内の変化に富む機器更新

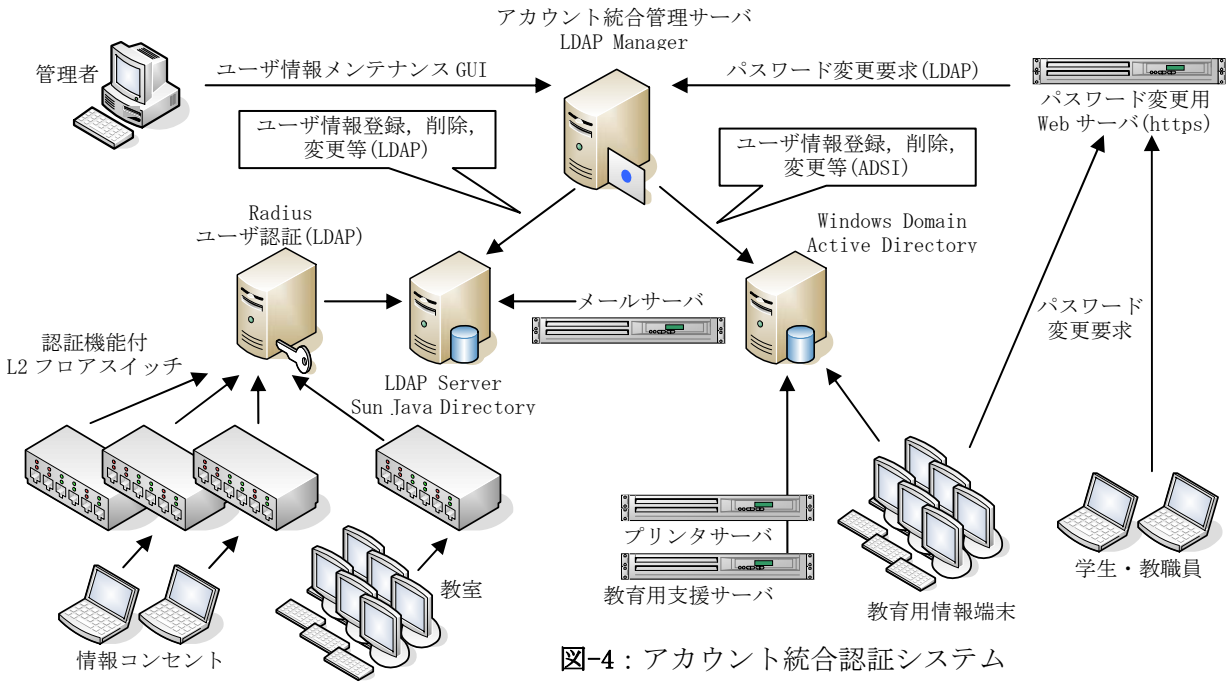

図-4：アカウント統合認証システム

にも柔軟に対応できる．1 機あたり 250 以上の同時認証能力があり，数教室分の認証をまかなうことができる．とくに 2)，5)の特長は，無線 AP 領域を新設，拡大していくなど各部局独自の運用を受容可能にしている．

各部局や学科で独自に運用されていた情報コンセント教室は，大型のルータで構築されていたものが多かった．これらの教室では，ルータをブリッジモードへ切り替えるだけで室内の情報コンセントを認証システムへ統合することができる．この移行の容易さは，認証システムの IPC 統合化を全学的に大きく促進させた．各部局は管理コストが低減され，同時にユーザの利便性と情報セキュリティは全学的に向上した．Apresia には，MAC ベースの認証ポート機能も有するが，本プロジェクトでは次に示す WEB ブラウザベースの認証方式のみを採用した．

情報コンセントからのネットワーク接続は次のように行われる．ユーザがパソコンを情報コンセントへ接続するだけでは，ネットワークは不接続の状態である．認証スイッチが唯一応答する予約 URL へユーザがアクセスすると，ネットワーク認証画面がブラウザ上に表示される．そこに，統合認証の管理下にあるアカウント情報を入力し，認証が成功すれば，基幹から DHCP で配布される PIP を受けてネットワーク接続の状態となる．ユーザは同ページより意図してネットワークからの接続解除も選択できる．認証スイッチは，最大接続時間やポーリング間隔等のパラメータを持っており，用途に合わせたセキュリティレベルの設定が可能である．

運用面では，一部特殊なポート監視を行うソフトウェアが原因での接続障害が数件のみ報告された．100 人規模の一斉認証は支障なく行われている．認証ポートの適用箇所は，図書館，リフレッシュスペース，情報コンセント教室，会議室等の設置にとどめ，研究フロアへの適用は全面的に控えた．

3.2 定期的パスワードの変更要求

統合認証システムの導入を契機に全ユーザに対して 120 日間隔の定期的なパスワードの変更要求を行う管理策を実施した．アカウント管理の意識向上と，アカウント未使用者を系統的に判断し，資源の有効活用を図ることが目的である．ユーザは 120 日毎にパスワード変更を繰り返し求められる．年間最低 3 回のパスワード変更を行う必要がある．変更されなかった場合は，当該アカウントはロックされ，そのユーザが利用可能なサービスは大きく制限される．パスワードの定期的な変更要求を行なうには，可能な限りのシステム上の支援策が必要である．本システムでは，アカウント権限を失効する 30 日，14 日，3 日，2 日，1 日前に，パスワードの変更依頼のリマインダをメール通知することでユーザへの注意を促した．パスワードの変更は指定の URL にアクセスしてブラウザ上から容易に行うことができる．このとき PIP 端末からの接続が必須条件であるため，パスワード変更を契機に，多くのユーザが端末の PIP 化を実施するに至った．

パスワードを失効したユーザは IPC にてパスワードの再発行の手続きを行ない，同アカウントを継続利用できる．まだ実施して間もないこともあり，初期の 120 日後にパスワードを失効してしまうユーザは数百名におよんだ．これは現状のアカウント管理意識の低さを表す結果とも受け取れる．今後も本管理策の有効性についての測定を行っていく予定である．この試みは，ユーザが新しいシステムから利便性だけを享受するのではなく，その管理責任を負うことへの自覚と義務を求める情報セキュリティ活動の取り組みのひとつに位置づけている．

4. 切り替えと運用開始

旧情報基盤から新情報基盤への切り替えは，約 100 日間の綿密な切り替え予備工事期間を経て，約 6 時間の全学ネットワークの停止時間で行われた．機器の更新だけではなく，ネットワーク，アカウント統合管理システム，メールシステムなどいくつもの変革を含む本システム更新を短時間で成し遂げるには，導入ベンダの献身的な努力や学内各組織との綿密な意思連携と協力態勢は不可欠であった．

4.1 メールサービスの切り替え

新規導入したアカウント統合管理システムのもとでは，全学ユーザのパスワードのリセットを回避できなかった．IPC では，約 12500 通のパスワード帳

票を，学内の全ユーザに対して，切り替え工事の約 10 日前から配布した．切り替え工程上やむを得なかったとはいえ，配布期間が不十分であったことは否めない．

多くのユーザにとってメールサービスの継続性の保証は最大の関心事であり，事実，切り替え工事の行われた年度末において，長期間のメールサービスの停止は学内の主要業務に甚大な被害を与えかねなかった．PIP 網の学内での利用推進は，新情報基盤の最も大きな目的のひとつであるが，切り替え直後においては PIP 網を意識することなくメールサービスの継続性を確保することが重要な局面である．メールシステムの切り替えは，1)メール中継（DMZ 上）とメールスプール（LAN 内）の 2 台のサーバ連係構築，2）mbox 形式から Maildir 形式へのメールスプール形式の変更，3）POP サービスに加えて IMAP サービスの並行運用を開始，など複数の新しい試みが盛り込まれていた．メールサービスの切り替え工程は週末の 48 時間内に完了し，学内業務への大きな損失を与えることはなかった．

4.2 ポータルサイトの重要性

メールシステム設定や端末の PIP 化の設定解説を含む新情報基盤に係わるすべての情報は，ひとつの専用ポータルサイトに集約され，その存在を複数の手段で学内ユーザへ事前に通知した．各ユーザへ手渡されるパスワード帳票への URL 記載などは有効な手段のひとつであった．**図-5** は本プロジェクトで構築したポータルサイトトップページのフレームメニュである．各説明は，図解説明を多用し，エンドユーザからサーバ管理者レベルにまで対応した最新情報の提供に努めた．全学に約 500 台を導入した教育用情報端末においては，ログイン時にスタートアップ機能からポータルトップページが起動する固定設定を採用した．この試みは情報リテラシレベルにばらつきのある学部学生への確かな情報伝達手段として有効であった．年度初めの IPC の窓口問い合わせ数が例年よりも低くなるという現象が観察された．

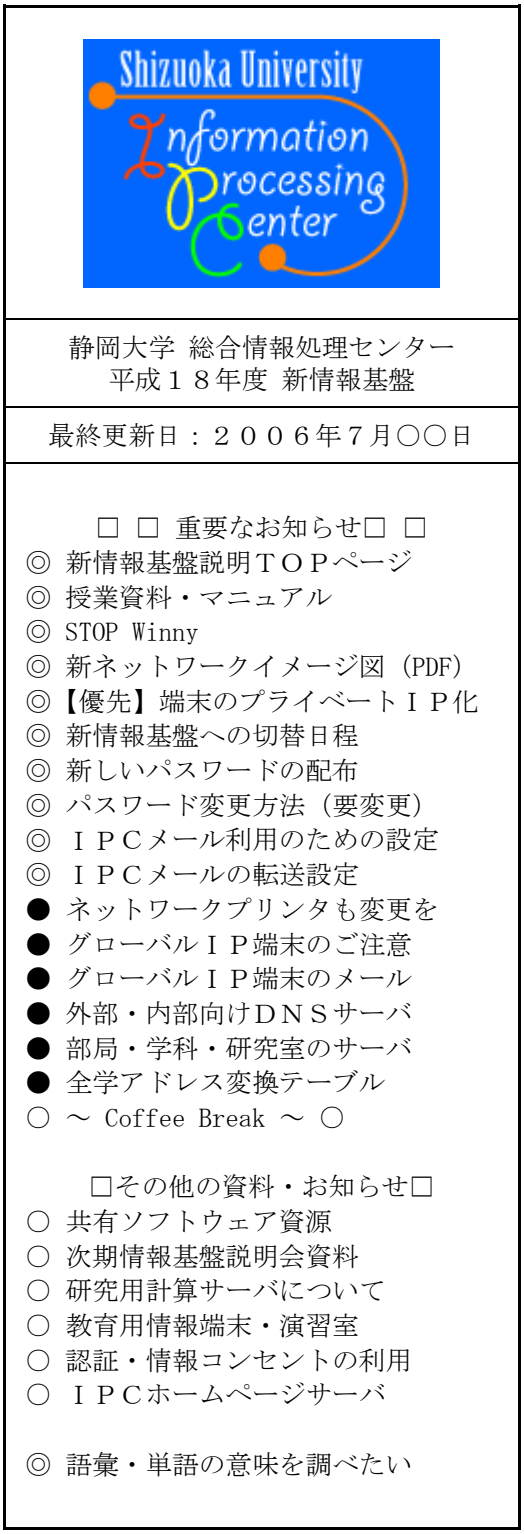

図-5：ポータルサイトメインメニュ

5. まとめ

本学で2006年3月に行われた新情報基盤整備において，旧 GIP 網の単一ネットワーク構造から，全学 GIP 網と PIP 網を共存させるネットワーク構造の変革を行った．本プロジェクトの成果は次のようにまとめられる．

1）a.b.0.0/16 の旧 GIP 網に 10.b.0.0/16 の PIP 網を新設することにより円滑な PIP 網への切り替

え手段を提供できた．L2 フロアスイッチにおいて採用したGIP網とPIP網のマルチフォーミング方式は,多様なネットワークサービスに対する継続性を保証するとともに,端末 PIP 化の移行促進に有効であった．

2) 全学 PIP 網の運用において，GIP 端末に対する運用方針が最も重要であることが分かった．GIP 端末を選択せざるを得ないユーザは,同時に PIP 網上の必須サービス用の PIP 端末を準備する負担を強いられる．しかしながら，GIP 端末の選択を抑制することなく，端末の明確な分離運用を求める基本方針は多くのユーザにとって受容可能なものであると判断している．

3) 全学 PIP 網の促進により，学内情報を提供するイントラサーバの運用意義が各サーバ管理者において再発見され，全学的な情報提供手段の住み分けが促進した．結果，全学的情報セキュリティを向上させることができた．

4) 認証機能付き L2 フロアスイッチ(最大 24 ポート)を学内 100 箇所に配置することで，認証の負荷は分散され，上位ネットワークの構成に左右されない認証システムを全学に配備できた．IPC による認証ポートの提供は，全学に散在していた部局運用の情報コンセントシステムの統合化を促進し，管理部局独自の発展利用を許容できる有効な選択であった．

5) アカウント統合認証システムの導入によりユーザへの利便性を高めることができた．同時にパスワードの変更を 120 日毎にユーザに対して要求する情報セキュリティの管理策を実施した．アカウントの死活の識別を容易にするために資源の有効利用および管理コストの低減が期待できる．全学ユーザがアカウントの管理意識を高めることで，全学的な情報セキュリティの向上が期待できる．

6) ネットワーク構造の変革を伴う情報基盤整備は，約 100 日間の詳細設計期間，段階的な棟・フロアスイッチ機器の更新作業，基幹装置やサーバ群のホットスタンバイなどを含む移行計画の下で行われた．その結果，約 6 時間の全学ネットワーク完全停止時間と約 48 時間のメールサービスの停止時間で滞りなく完了することができた．

7) 新情報基盤整備に関する専用ポータルサイトを準備し，学部学生から部局サーバ管理者まで対応できる情報を整理して提供した．その効果は大きく，切り替え前後の混乱を大きく低減できた．切り替え直後の約 2 日間で PIP 化に伴う問い合わせ対応は，ほぼ収束した．また新学期における窓口対応が例年より減少した．

動画像サービスの隆盛，あるいは大学間の動画像による講義や会議が日常化している近年の情勢において，本プロジェクトが目標とする PIP 化の促進がどこまでユーザに広く受容されていくのか，まだ明確な答えは得られていない．今後数年の観察を要するものと思われる．しかしながら，切り替え直後の混乱が予想をはるかに下回る規模で短期間であったこと，GIP 端末から PIP 端末専用サービスへの段階的移行がすみやかに進行している状況から，新情報基盤に対するユーザの理解は予想以上に進んでいると判断できる．ISMS が提唱するところの「資産としての情報の価値」は，機密性，完全性，可用性のバランスを考慮して保護されなければならない．一部のユーザが渇望する可用性の高いサービスに応えるIPC の姿勢や努力は，今後も必要不可欠である．しかしながら，劇的に進化する情報インフラ技術においてこそ，全学に分散する情報資産を抜本的に保護できるバランスのとれた情報基盤を整備することも，また必要である．ユーザと IPC との，ときに激しい意見の衝突の中で，最良の情報基盤整備を模索していくことは今後も重要であると考える．

謝辞：本プロジェクトの推進にあたり，鋭意，ご尽力賜りました NTT 西日本-静岡 戸塚純一氏をはじめとする NTT 西日本スタッフの皆様に心より厚く御礼申し上げます．

1) 日本情報処理開発協会（JPDEC）
http://www.jipdec.jp/

2) 学術リポジトリ構築ソフトウェア実装実験プロジェクト
http://www.nii.ac.jp/metadata/irp/