シ	ス	テ	ム	技	術	分	科	会		選	出
2008 年度 システム技術分科会 第 1 回会合 より											

日本大学における SaaS の導入

ーGoogle との協調による「NU-AppsG」の導入経緯・運用についてー

日本大学総合学術情報センター

吉田 誠、 相川 成周

日本大学におけるSaaSの導入

～Googleとの協調による「NU-AppsG」の
導入経緯・運用について～

日本大学総合学術情報センター

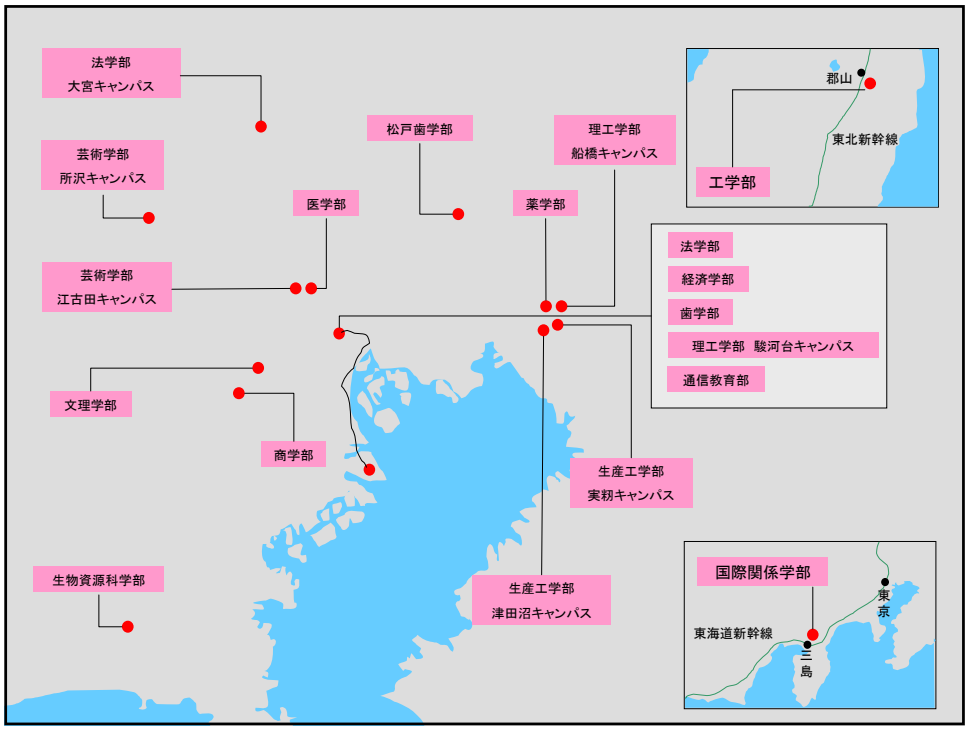
情報企画課課長　吉　田　　誠

日本大学について

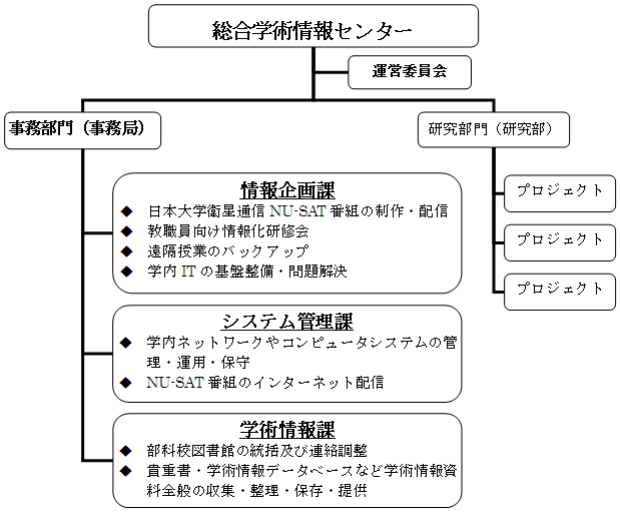
- １４学部７９学科２０研究科
- 学生数　　約８１，０００人
- 教職員数　約　８，０００人

自主創造
日本大学

あなたとともに
１００万人の仲間とともに


法学部
大宮キャンパス
芸術学部
所沢キャンパス
芸術学部
江古田キャンパス
医学部
松戸歯学部
理工学部
船橋キャンパス
薬学部
郡山
東北新幹線
工学部
法学部
経済学部
歯学部
理工学部　駿河台キャンパス
通信教育部
文理学部
商学部
生産工学部
実籾キャンパス
生物資源科学部
生産工学部
津田沼キャンパス
国際関係学部
東京
東海道新幹線
三島

組　織　図


総合学術情報センター
運営委員会
事務部門（事務局）
研究部門（研究部）
情報企画課
◆ 日本大学衛星通信 NU-SAT 番組の制作・配信
◆ 教職員向け情報化研修会
◆ 遠隔授業のバックアップ
◆ 学内 IT の基盤整備・問題解決
システム管理課
◆ 学内ネットワークやコンピュータシステムの管理・運用・保守
◆ NU-SAT 番組のインターネット配信
学術情報課
◆ 部科校図書館の統括及び連絡調整
◆ 貴重書・学術情報データベースなど学術情報資料全般の収集・整理・保存・提供
プロジェクト
プロジェクト
プロジェクト

日本大学総合学術情報センターの役割

- 本学の情報受発信基地としての役割
- 情報関連の企画・立案
- 学内ﾈｯﾄﾜｰｸやｼｽﾃﾑの管理・運用・保守
- 映像制作・配信拠点（日大テレビ・遠隔授業）
- 学術情報データベースの管理・運用・保守
- その他

部科校システムの統合化

学生向けサービス
- メールシステム　NU-mailG
- ｳｪﾌﾞｱﾌﾟﾘｹｰｼｮﾝｼｽﾃﾑ　NU-AppsG
- 就職支援システム　NU就職ナビ

教職員ポータルシステム
- 情報共有システム「事務の友」

その他システム
- 入試願書一括受付システム，
- 全学共通図書システムetc..

→統合化することにより，経費節減を図っている

NUーAppsG（学生サービス向け）導入経緯

- 導入前は学部独自でメールシステムを構築

課　題　点

- 非効率なメールシステムの運用・管理
- システム管理経費の無駄遣い
- セキュリティレベルがまちまち
- 学生サービスのレベル格差が著しい
- その他

導入までの流れ

2006年

- 9月　　ﾒｰﾙｼｽﾃﾑ開発ﾜｰｷﾝｸﾞﾁｰﾑ立上げ
- 11月　　ﾜｰｷﾝｸﾞﾁｰﾑにてGoogle導入を決定
- 12月中旬 常務理事会等諸会議にて導入承認

2007年

- 1月　ｱｶｳﾝﾄ管理ｼｽﾃﾑ　構築開始
  （2.5ヶ月で構築終了）
- 3月　Google社と契約文書にて締結
  4月　運用開始（８学部にて運用開始）

2008年

- 4月　学部，研究科及び短期大学追加導入

現在：１１学部・４研究科・１短大・専門学校
にて運用中

NUメールのリースアップを機に,
新システム移行の検討開始

検討テーマ

「安全性・情報化経費節減・利便性・安定化・
学生サービス等の学部間格差の解消」

①独自システム開発の検討
②既存WEBサービスの活用

執行部の意識改革を求める！

メール送付は葉書郵便と同様である！！

学生データ提供プロセス

学生基本情報DB（全データ）
↓
アカウント管理システム（IDデータ生成）
↓
Googleメールシステム（IDデータのみ提供）

導入後の反響

- メディア取材　　約２０社
- 他大学からの問合せ　約３０校

今後の展開

- 全教職員向けて「NU-AppsG」の導入
- ＮＵ－ＳＳＯの展開
  図書・就職・ＳＮＳ・研究者情報等

ご静聴ありがとうございました

自主創造
日本大学

日本大学におけるSaaSの導入

Googleとの協調による「NU-AppsG」の導入経緯・運用について

技術編

日本大学総合学術情報センターシステム管理課
相川成周（あいかわしげちか）

技術的背景

- NU-Mail
  - 2006年4月運用開始
  - 全教職員向け（ユーザ数約1万人）
  - オープンソース
- NU-AppsG（NU-MailG）
  - 2007年4月運用開始
  - 全学生向け（ユーザ数約10万人）
  - Google Apps Education Edition

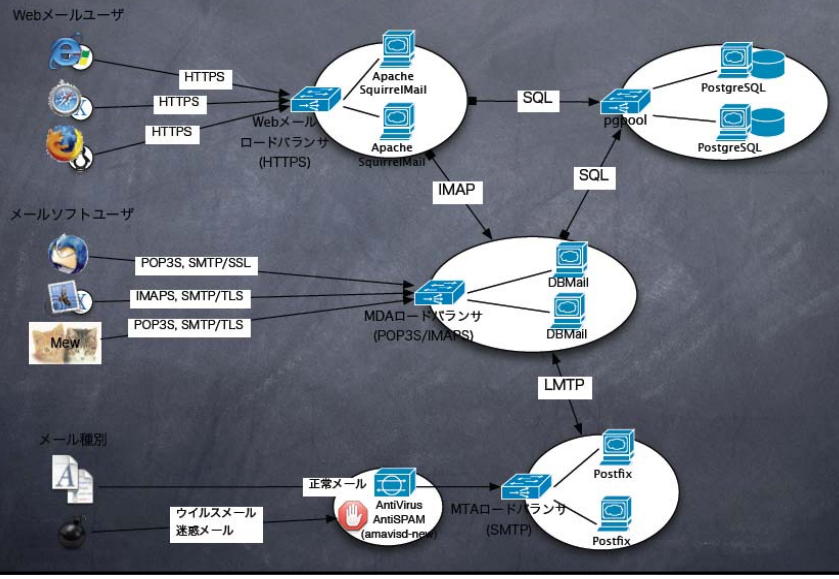
NU-Mail

- ユーザにとってのメリット
  - ウイルス対策，迷惑メール対策
  - WebMail
    - 難しい設定無しで利用可能
  - メールソフトユーザ
    - SMTP認証必須
- 管理者にとってのメリット
  - 人事データベースと連携
    - 異動処理がスムースになる
  - 分散管理に対応
    - 学部アカウントは学部管理者

NU-Mailシステム

- メールサーバ
  - MTA：postfix
    - SPF，DomainKey対応
  - MDA：dbmail
    - データベースでメールを管理するメールサーバ
    - POP3・IMAP4・SIEVEサーバを搭載
  - ウイルス・迷惑メール対策：ClamAV + SpamAssassign
  - WebMail：Apache + SqirrelMail
  - メーリングリスト：Mailman
- データベース
  - PostgreSQL
  - pgpool

NU-Mailシステム概略図



NU-Mailサーバ内訳

導入時（2006/4）	現在（2008/8）
MTA x 2 MDA x 2 DB x 2 Web x 2	MTA x 4 MDA x 2 DB x 2 Web x 2 ML x 1 FALLBACK x 1
計8台	計12台

NU-Mailまとめ

- 成果
  - オープンソースで構築
    - 開発コスト削減
  - 日大組織にあった管理機能の実現
- 改善点
  - WebMail
    - 検索機能，検索速度
  - システム負荷

NU-AppsG（NU-MailG）

- 2006年9月　学生向けメールWG発足
- 仕様
  - 利用者：全学生約10万人
  - 学生基本情報DBと連携
  - 日大組織にあった管理機能
- システム設計方針案
  - 案1 NU-Mailをベースに独自開発
  - 案2 SaaS利用

Google Apps for Educationに注目

Google Apps for Education

- http://www.google.com/a/edu/
  - 教育機関限定サービス
  - ドメイン持ち込み可能
  - 無料
  - 学生（生徒），教職員，校友利用可能
  - 歴史
    - 8/28 Google Apps for Your Domain発表
    - 10/10 Google Apps for Education発表
    - 11/1　日本語版発表
- 実績
  - アリゾナ州立大学（学生6万5000人以上）

概略比較

項目	NU-Mailベース 独自開発	Google Apps for Education
Mail	○	○
Messaging	×	○
Calendar	×	○
web pages	×	○
開発費用	数千万円	無料
開発期間	3ヶ月以上	即日

メール機能比較(1)

	NU-Mail現状	Google Apps for Education
メールボックス容量	100MB	2GB
メール1通最大容量	15MB	20MB
暗号化(over SSL)	○	○
WebMail	○	◎
POP	○	○
転送機能	×	○
多重化	2重化	7重化以上
24時間 x 365日	×	○

2006年11月WG資料抜粋

メール機能比較(2)

	NU-Mail現状	Google Apps for Education
IMAP	○	×
AntiVirus	○	○
AntiSPAM	○	◎
SMTP-AUTH	○	○
SPF	○	○
DomainKeys	○	×
Submission	○	×
管理機能	日大組織に合致	シンプル

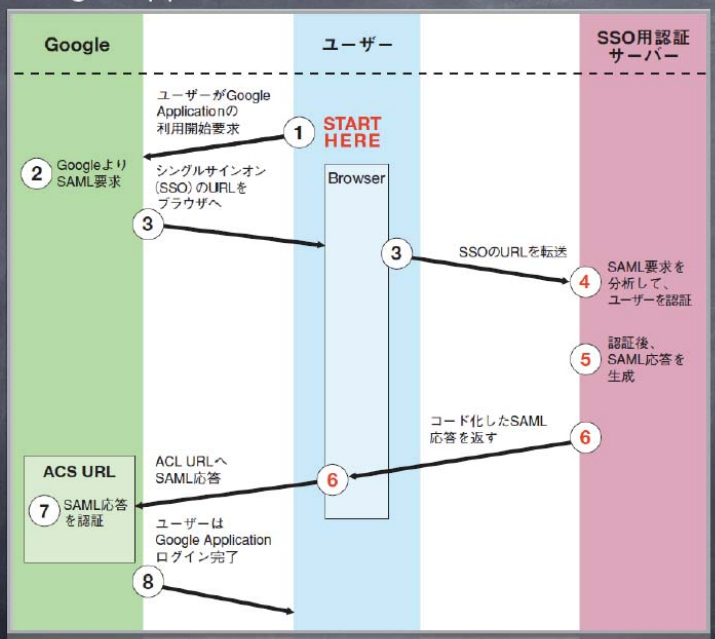
2006年11月WG資料抜粋

Goole Apps APIs

- http://code.google.com/apis/apps/
- プロビジョニング
  - アカウントのCRUD（Create・Read・Update・Delete）
  - アカウント情報（氏名，ID，パスワード）
- SSO（Single Sign-On）
  - シングルサインオンを用いれば学生基本情報DBとの連携の実現性あり
- 日大組織にあった管理機能が作れそう！

プロビジョニングAPI

Google Appsシングルサインオンの流れ（SAML）



http://www.sios.com/pdf/si/017_nihon-u_2007.pdfより抜粋

開発

- サーバ4台追加（DB x 2，Web x 2）
- APIバグ？
  - 仕様通りに動かない
    - Google Apps APIs discussion groupに質問する
      - 個人宛に詳細を求む連絡がある
        - 詳細を添えて返信
          - 翌日直る
- メールアドレス
  - 自動生成
  - 先着順は避けたい
  - フルネームだと重複多数
  - 乱数は避けたい（愛情欠落，紛失対策）
  - 連番を避けたい（総当たり攻撃対策）
  - 短くしたい
  - 結果→xxsi07011@g.nihon-u.ac.jp（９桁）
    - 学部2文字，乱数2文字，西暦2桁，学生番号3桁

実行例（ユーザ）

実行例（管理者）

運用（死活監視）

NU-Mail	conn	cpu	disk	files	http	imap	info	memory	mags	pop	ports	procs	smtp	ssh	sslcert	trends
mail.nihon-u.ac.jp	◆	-	-	-	●	◆	◆	-	-	●	-	-	●	-	◆	◆
g.nihon-u.ac.jp	◆	-	-	-	●	-	◆	-	-	-	-	-	-	-	◆	◆
ml.nihon-u.ac.jp	◆	-	-	-	●	-	◆	-	-	-	-	-	-	-	-	◆
smtp.nu-mail	◆	-	-	-	-	-	◆	-	-	-	-	-	-	-	-	◆
lmtp.nu-mail	◆	-	-	-	-	-	◆	-	-	-	-	-	-	-	-	◆
imap.nu-mail	◆	-	-	-	-	-	◆	-	-	-	-	-	-	-	-	◆
pgpool.nu-mail	◆	-	-	-	-	-	◆	-	-	-	-	-	-	-	-	◆
sieve.nu-mail	◆	-	-	-	-	-	◆	-	-	-	-	-	-	-	-	◆
gpgpool.nu-mail	◆	-	-	-	-	-	◆	-	-	-	-	-	-	-	-	◆
mta1.nu-mail	◆	◆	◆	⊠	-	-	◆	◆	⊠	-	-	⊠	◆	●	-	◆
mta2.nu-mail	◆	◆	◆	⊠	-	-	◆	◆	◆	-	⊠	⊠	◆	●	-	◆
mta3.nu-mail	◆	●	◆	⊠	-	-	◆	●	◆	-	⊠	⊠	◆	◆	-	◆
mta4.nu-mail	◆	◆	◆	⊠	-	-	◆	●	◆	-	⊠	⊠	◆	◆	-	◆
mda1.nu-mail	◆	◆	◆	⊠	-	◆	◆	◆	◆	◆	⊠	⊠	-	●	-	◆
mda2.nu-mail	◆	●	◆	⊠	-	◆	◆	◆	◆	●	⊠	⊠	-	●	-	◆
wm1.nu-mail	◆	◆	◆	⊠	◆	-	◆	◆	◆	-	⊠	⊠	-	●	-	◆
wm2.nu-mail	◆	◆	◆	⊠	◆	-	◆	◆	◆	-	⊠	⊠	-	●	-	◆
dbms1.nu-mail	◆	●	◆	⊠	-	-	◆	◆	◆	-	⊠	⊠	-	●	-	◆
dbms2.nu-mail	◆	●	●	⊠	-	-	◆	◆	◆	-	⊠	⊠	-	●	-	◆
gweb1.nu-mail	◆	◆	◆	⊠	◆	-	◆	◆	⊠	-	⊠	⊠	-	◆	-	◆
gweb2.nu-mail	◆	●	◆	⊠	◆	-	◆	◆	⊠	-	⊠	⊠	-	◆	-	◆
gdbms1.nu-mail	◆	●	◆	⊠	-	-	◆	◆	⊠	-	⊠	⊠	-	◆	-	◆
gdbms2.nu-mail	◆	●	◆	⊠	-	-	◆	◆	⊠	-	⊠	⊠	-	◆	-	◆
ml1.nu-mail	◆	◆	◆	⊠	◆	-	◆	◆	⊠	-	⊠	◆	-	◆	●	◆
fallback.nu-mail	◆	◆	◆	⊠	-	-	◆	◆	◆	-	⊠	⊠	◆	◆	-	◆
wal.nu-mail	●	⊠	⊠	⊠	-	-	◆	⊠	⊠	-	⊠	⊠	-	⊠	-	◆

NU-AppsG（NU-Mail）まとめ

- Google Apps Education Edition
  - APIを活用し日大組織にあった管理機能構築成功
- NU-SSO
  - Google Apps SSOを学内利用可能にした
    - 教職員ポータルシステムとの連携成功

今後

- NU-Mail 2.0（仮称）開発
  - 全教職員向け（約1万人）
  - 2008年10月運用開始（鋭意開発中）
  - Google Apps Education Edition採用
    - Reporting API
      - 統計情報
    - SMTP Gateway機能
      - ロギング
- NU-SSO
  - シングルサインオンを学内システムへ展開
    - 図書・就職，SNS等

システム技術分科会 選出
2008 年度 システム技術分科会 第 2 回会合 より

日本最大規模の キャンパス認証ネットワーク

～HINET2007 の構築と運用～

広島大学情報メディア教育研究センター

西村 浩二

サイエンティフィック・システム研究会　　2009 年 1 月 29 日
システム技術分科会 2008 年度第 2 回会合資料

日本最大規模のキャンパス認証ネットワーク
～ HINET2007 の構築と運用 ～

広島大学情報メディア教育研究センター
西村 浩二,
相原 玲二, 近堂 徹, 大東 俊博,
田島 浩一, 岸塲 清悟, 岩田 則和
kouji@hiroshima-u.ac.jp

[Abstract]
広島大学では平成 20 年度より新キャンパスネットワーク HINET2007 の運用を開始した。HINET2007 では、全学約 450 台のエッジスイッチが全学電子認証システムと連携してすべてのネットワーク利用者を認証するほか、全教員数に相当する約 2,000 個の独立したファイアウォール機能を有するなど、安全かつ柔軟な環境を提供している。
本報告では、HINET2007 の概要とその構築手法、それぞれの機能の性能評価の結果、移行を支援する体制やシステムについて述べる。

[Keyword]
利用者認証、仮想ネットワーク、アクセス制御、リナンバリング

1 はじめに

大学などの高等教育研究機関では、さまざまな教育研究を実施するために高度かつ柔軟なネットワークが求められる。大規模な組織では、学部や学科などの部局単位でサブネットを構成し、サブネット内の管理運用は当該組織が責任を持つことを条件に、自由度の高い運用を許してきた経緯がある。しかし、ネットワークがライフライン化するにつれ、インターネット上で発生するセキュリティの問題も複雑化していることから、大幅な管理方針の見直しが迫られている。

このような背景のもと、広島大学では平成 19 年度からセキュアでスケーラブルなキャンパスネットワーク HINET2007 の構築を開始し、平成 20 年 5 月から運用を開始した[1]。HINET2007 では、これまでの部局単位でのサブネット管理体制から全学的な一元管理体制へ移行するとともに、利用形態により分類される「ゾーン」という概念を導入し、それぞれの目的に応じた学内外からのアクセス制御を提供する。さらに、すべてのネットワーク接続点(ポート)において接続機器の利用者を特定するための認証を行うことで、セキュリティレベルの底上げ、維持を図っている。またこれらの運用管理を支援するための体制作りやシステムの開発を行っている。

本稿では、HINET2007 の概要と運用・移行の方針、設計・構築のポイント、移行の支援体制とシステムについて述べる。

2 HINET2007 の概要

今回構築した HINET2007 の概要を図 1 に示す。主な特徴は以下のとおりである[2]。

(1) 全学的な一元管理体制
これまでのサブネット管理は多くがボランティアにより行われていた。その結果、サブネットにおいて発生したセキュリティの問題に対する責任の所在があいまいになったり、サブネットによって対応に違いが生じたりする原因となった。HINET2007 では全学的な一元管理体制をとるため、建物集約スイッチやフロアスイッチの全ポートを管理対象とし、各部屋の情報コンセントへの接続状況を把握できるようにしている。

(2) VLAN による柔軟な仮想配線の提供
柔軟な組織体制で教育研究が行われる場合、同一の組織や研究グループが必ずしも同一の建物内や

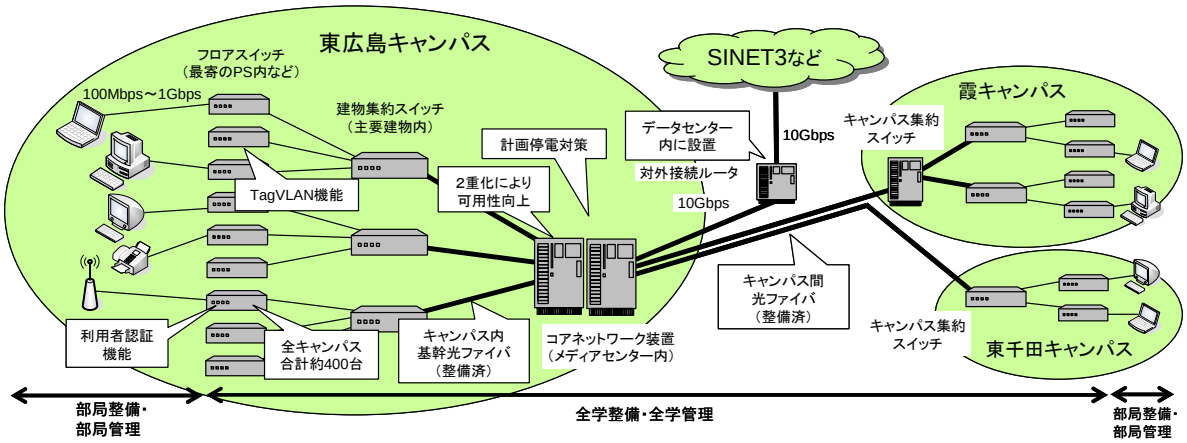


図 1　HINET2007 概要図

フロア内に分布しているとは限らない。HINET2007 では IEEE802.1q(Tag VLAN)を従来以上に積極的に活用し、地理的条件の影響を受けないネットワーク構築を可能としている。

(3) 個別ファイアウォール機能の提供

外部からのセキュリティの脅威からネットワーク機器を保護するため、研究室にファイアウォール機能を持つ機器(ブロードバンドルータなどを含む)を設置するケースが多く見られた。しかし、複数の建物に部屋が分散している場合は機器間を VPN で接続するなど、設定や管理が煩雑であるという問題もあった。そこで HINET2007 では、約 2,000 個の個別ファイアウォールをネットワークの機能として提供している。

(4) すべての接続場所において利用者認証を要求

これまでサブネット管理者が行ってきた接続機器の管理を全学的な一元管理とするため、約 450 台のすべての建物集約スイッチとフロアスイッチに利用者認証機能を持たせ、ネットワークの利用に際して何らかの認証が要求されるようにしている。

3　管理・運用・移行の方針

3.1　ゾーン構成とアクセス制御

先に述べたように、HINET2007 では各部局等のセキュリティレベルの底上げと均一化を図るため、これまでのサブネット単位に分散した独自管理から全学的な一元管理へと大きく運用方針を転換した。これにともなって、利用形態により学内外からのアクセスの可否パターンで区別される「ゾーン」という概念を導入した。主要なゾーンは表 1 に示す 4 種類である。またこれらのゾーン間および外部ネットワーク(インターネット)間のアクセス制御の概要を図 2 に示す。IEEE802.1q を利用することで、ゾーンは基本的にキャンパスや建物、フロアなどの地理的条件に影響を受けることなく、自由に構成することができる。

表 1　HINET2007 が提供するゾーン種別

ゾーン名 略称	グローバルゾーン ゾーンA	ファイアウォールゾーン ゾーンB	ローカルゾーン ゾーンC	公衆ゾーン ゾーンD
主な用途	学外向けサーバ接続	学内共有サーバ接続	一般クライアント接続	オープンスペース
外部IPアドレス	グローバル　固定割当	グローバル　固定割当	グローバル　固定割当	グローバル　DHCP割当
内部IPアドレス	外部IPアドレスと同じ	外部IPアドレスと同じ	プライベート(NAPT) DHCPまたは固定割当	外部IPアドレスと同じ
ゾーン外からの アクセス	学内外とも制限なし	学外から不可 ゾーンAを除く学内から可	同一ローカルゾーン以外 から不可	学外から不可 ゾーンAを除く学内から可
学外へのアクセス	制限なし	制限なし	原則制限なし (NAPTによる制限あり)	制限なし
端末認証	MACアドレス認証	MACアドレス認証	Web認証または MACアドレス認証	Web認証

3.2　運用方針

表 1 に示すように、HINET2007 では原則としてすべての接続端末に認証が求められる。認証方式は Web 認証と MAC アドレス認証のいずれかで、ゾーンによって利用できる認証方式は異なっている。Web 認証はネットワークを利用する都度 Web ブラウザを使用して利用者認証を行うが、MAC アドレス認証を行うには事前に利用者と被認証機器の MAC アドレスの対応を申請しておく必要がある。また図 2 におけるローカルゾーン(ゾーン C)では、約 2,000 個の個別ファイアウォール機能を提供している。基幹スイッチ等の設定はあらかじめ行っておき、利用者の申請に応じてフロアスイッチ等の VLAN 設定を変更することで、希望する場所で個別ファイアウォール機能が利用できるようにしている。ただし、ファイアウォールのポリシー設定については以下のような運用方針を定めている。

- 個別ファイアウォールの例外設定(特定ポートへのアクセス許可など)は受け付けない。
- 個別ファイアウォールのローカル側／グローバル側アドレスの希望は受け付けない(情報メディア教育研究センター(以下、メディアセンター)が指定)。
- 希望すればフロアスイッチの下流ポートへ Tagged で接続ができるが、VLAN ID の希望は受け付けない(メディアセンターが指定)。

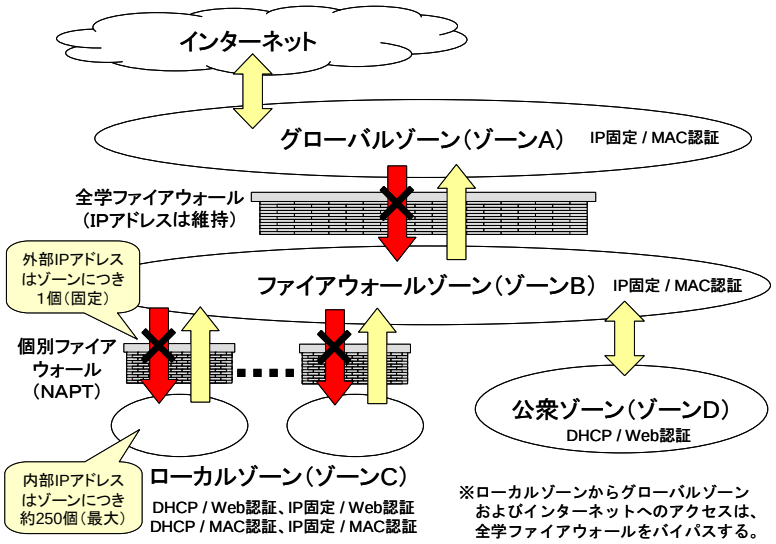


図 2　ゾーン間のアクセス制御

3.2　運用方針

HINET2007 はこれまでのキャンパスネットワークに比べて、全端末の IP アドレスのリナンバリングが必要である、ネットワークの利用に先立って認証が必要であるなど、運用方法が大幅に異なるため、全学が一括して移行することは困難であると判断した。そのため、既存の HINET2001 との並行運用期間を定めた上で、その期間内で利用者が研究科や専攻、研究室の単位で移行時期を決定できるようにした。並行運用の期限は 2008 年度末としており、2009 年 3 月末に HINET2001 を停止する予定である。

具体的な移行作業は、フロアスイッチ等の設定変更とフロア配線の差し替えである。フロアスイッチ等の設定変更にはコネクタの指定を受けるための申請、ゾーンの指定を受けるための申請、そしてコネクタとゾーンとを関連づけるための申請の 3 つのステップが必要であるが、手続きの詳細については MAC アドレスの登録を含めて後述する。フロア配線の差し替えについては、ほとんどの場合はフロア内の最寄りのパイプスペースに新旧のスイッチが設置されているため、すべての申請が完了した後、利用者の都合がよいときに旧スイッチから新スイッチへ配線を差し替える。その後その配線に接続されている機器の IP アドレスを変更し、接続テスト(認証テスト)が完了すれば移行が完了となる。

4　設計・構築のポイント

本節では、HINET2007 を設計・構築する際に特に考慮した事項について概要を述べる。個々の事項の詳細については、それぞれで引用されている文献を参照されたい。

4.1　個別ファイアウォール機能の実現

HINET2007 のコアネットワーク装置周辺の構成を図 3 に示す。装置やリンクの故障に備えて、基幹部分は概ね二重化されている。さらに L3 コアスイッチの内部構成を図 4 に示す。今回導入した L3 コアスイッチ(Cisco Catalyst 6509)には、ファイアウォールモジュール(FWSM)を 3 基搭載している。さらに 2 つの独立した L3 機能(VRF と MSFC)とポリシールーティングを駆使して、各ゾーンに提供する接続性(アクセス可否の制御)を実現した。L3 コアスイッチに搭載する FWSM は、1 基を全学ファイアウォール用、2 基を個別ファイアウォール用に割当てている。FWSM は 1 基あたり、20 の仮想ファイアウォール(VFW)が設定可能であり、それぞれの VFW には 50 の内部ネットワーク(内部インタフェース)が設定できる。FWSM を 2 基使用することで、2,000 の内部ネットワークを構成した。ただしこの方法では、同一 VFW の内部ネットワーク間は VFW のルーティング機能により通信可能となるため、互いの内部ネットワークが通信できないようにフィルタを設定している。各内部ネットワークは一部の例外を除いて /24 のサイズであり、原則として DHCP 機能が提供されている。外部へは NAPT 機能によりそれぞれ異なる外部 IP アドレスに変換されてアクセスを行う。

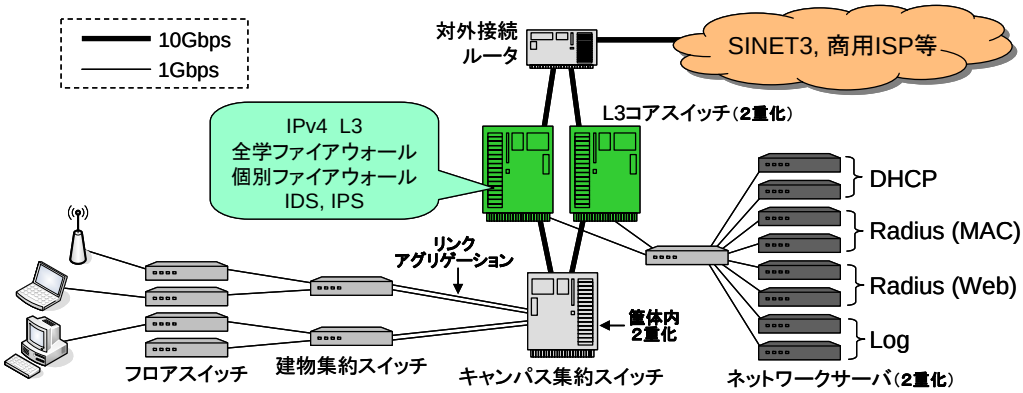


図 3　基幹ネットワーク構成図

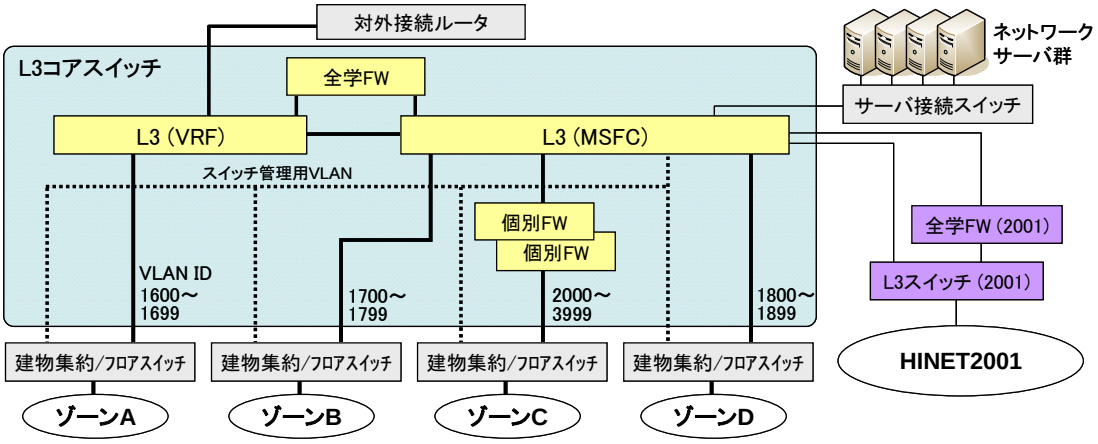
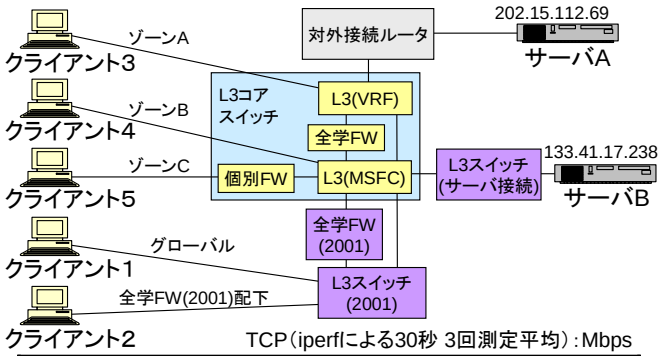


図 4　L3 コアスイッチ設定概要図

コアネットワーク装置の設計にあたっては、ファイアウォールが通信に与える影響を調べるため、HINET2007 導入の前後で通信速度の測定を行った[3]。HINET2007 を導入することによる HINET2001 への影響は見られなかった。HINET2007 導入後の測定結果を図 5 に示す。利用者はクライアント 1,2 の環境からクライアント 3,4,5 の環境に移行することになる。クライアント 1, 2 からクライアント 3,4 へはほぼ



TCP(iperfによる30秒 3回測定平均):Mbps

	サーバA		サーバB	
	送信	受信	送信	受信
クライアント1	471	517	704	709
クライアント2	--	365	691	615
クライアント3	637	685	712	878
クライアント4	--	348	696	801
クライアント5	--	292	--	433

図 5 スループット(HINET2007 移行後)

同様な結果となっているが、クライアント 5 の通信速度はやや低くなっている。これは 1 基の FWSM に 20 の VFW を設定し、1,000 の内部ネットワークを構成しているためと思われるが、実用上は問題ないと判断している。

4.2 利用者認証機能の実現

移行が完了するとHINET2007は広島大学の構成員約20,000名が日常的に利用する認証ネットワークとなる。認証システムの設計においては、次の 2 点を特に考慮した。1 点目は、大学には新旧さまざまな OS、ネットワーク機器が混在している点である。広島大学では、以前より利用者認証機能を持つ情報コンセントシステムの開発、運用を行っていた経験[4]から、Web ブラウザを用いた利用者認証を基本とし、Web ブラウザを持たない機器に対しては利用者を特定した上で Mac アドレス認証を行うこととした。2 点目は、事務職員が利用する事務用端末の起動時間が始業時間前後に集中するという点である。図 6 に HINET2001 において観測した端末増減数の時間推移を示す。この結果から、8 時 20 分から 35 分の 15 分間に約 600 台の端末が接続されていることがわかる。またこの負荷は一部(事務棟)の認証スイッチに集中するため、認証スイッチ自身の性能も考慮する必要がある。

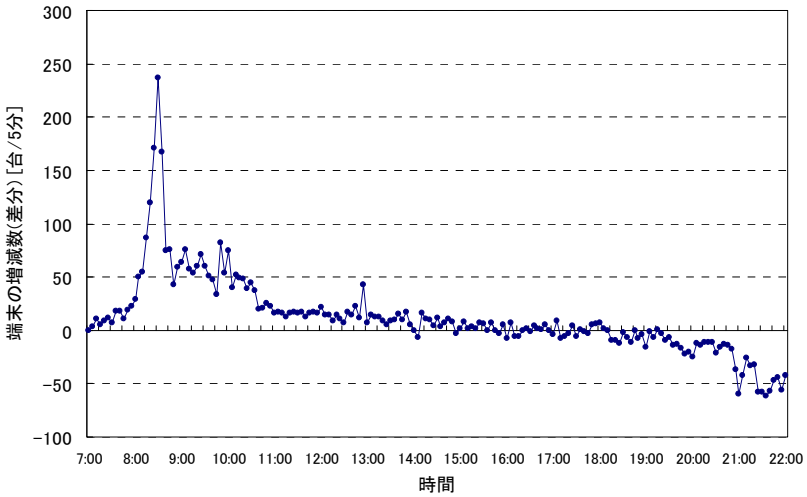


図 6 HINET2001 における端末の増減数

これらの要件を実現するため、図7に示す認証システムを構築した。DHCPサーバは約2,000の各ゾーンに対して最大120アドレスを割当てる機能を、ログサーバはフロアスイッチの認証ログやファイアウォールログを保存する機能を提供する。ホスト登録装置およびRadius サーバは、MACアドレス登録および利用者認証で利用する。各サーバは高可用性が要求されるため、HA(High Availability)クラスタを構成し、冗長化されている。フロアスイッチ(Alaxala AX2430S)は認証機能を持つL2スイッチで、本スイッチの各ポートが認証ポイントとなる。Web 認証と MAC アドレス認証に対応し、Web 認証では外部 Web ページへのアクセスが認証ページにリダイレクトされる。認証ページはhttps接続でのみ提供しており、約450台の認証スイッチが使用するサーバ証明書には国立情報学研究所のサーバ証明書プロジェクト[5]が発行する中間CA証明書を採用した。

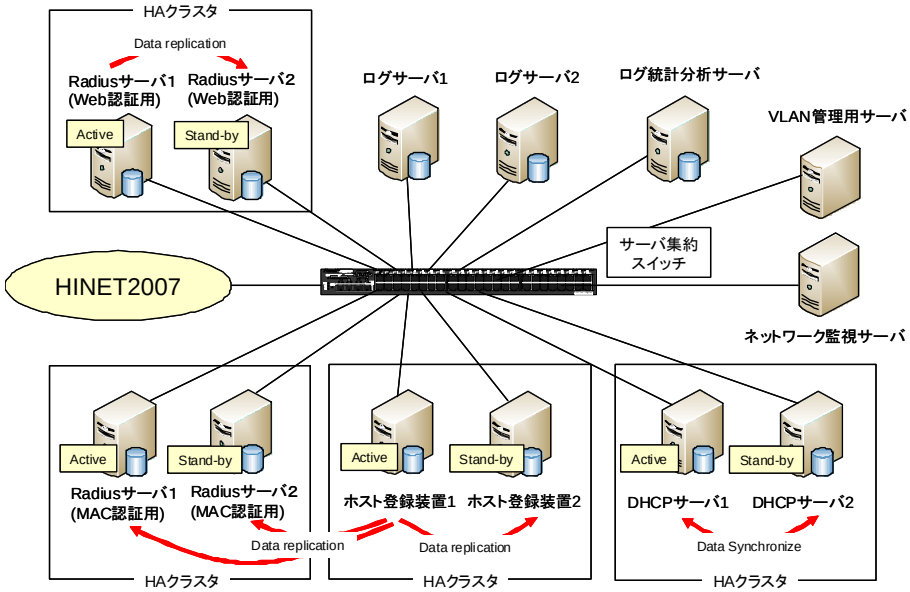


図7 認証システムの構成

構築する認証システムが要求どおりに機能することを確認するため、仕様策定段階あるいは構築段階において、以下の性能評価を行った[6]。

(1) DHCPサーバのIPアドレス払い出し性能

同時リクエスト数を変化させて、すべてのリクエストへの応答が完了するまでの時間(最小／平均／最大)を測定した。測定結果を図8に示す。この結果から、450台からの同時リクエストに対して最大0.12秒以内に処理が完了していることがわかる。

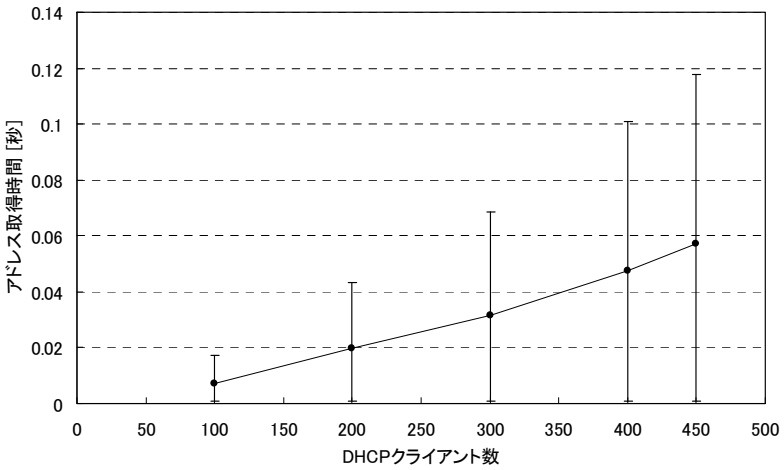


図8 DHCPサーバの応答時間

(2) Radius サーバの同時認証性能

Web 認証用 Radius サーバは外部 LDAP を、MAC アドレス認証用 Radius サーバは内部 LDAP を参照するため、それぞれについて同時リクエスト数を変化させて、すべての認証が完了するまでの時間(最小／平均／最大)を測定した。測定結果を図 9 に示す。この結果から、600 台の同時認証でも 1 秒以内に処理を完了できる性能を有することがわかる。

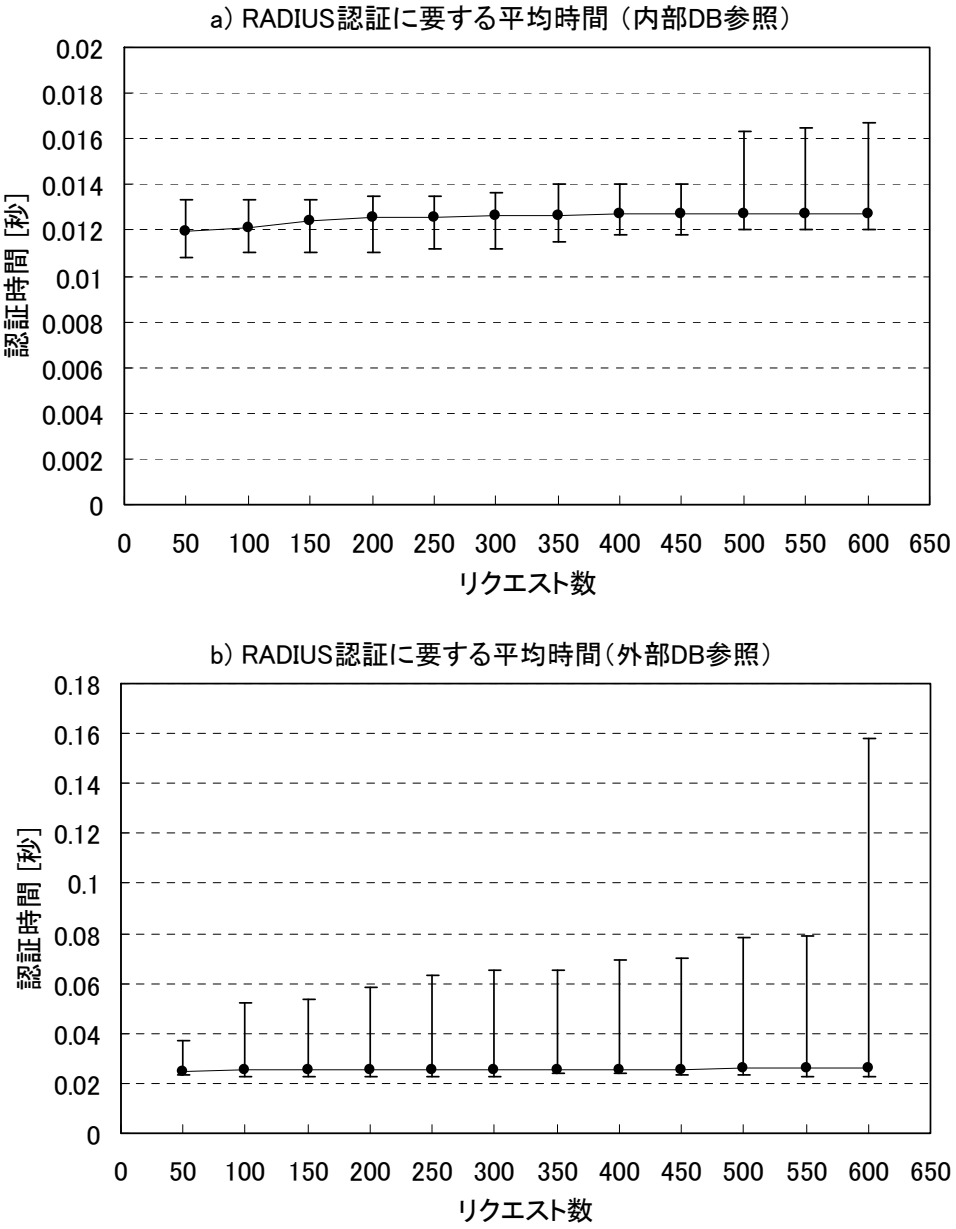


図 9 Radius サーバの応答時間

(3) 認証スイッチの同時認証性能

クライアントから http による外部 Web ページへのアクセス、フロアスイッチ内の認証ページへのリダイレクト、https(鍵長 2,048 ビット)による認証情報の送信、認証応答メッセージの受信までの時間の和を認証時間とし、同時認証セッション数を変化させて、すべての認証が完了するまでの時間(最小／平均／最大)を測定した。測定結果を図 10 に示す。この結果から、同時 100 セッションの認証要求に対しても最大 23 秒程度で処理が完了できることがわかる。

以上の評価結果から、事務用端末の一斉認証要求のような状況においても実用的な時間で認証処理を完了できることが確認できた。

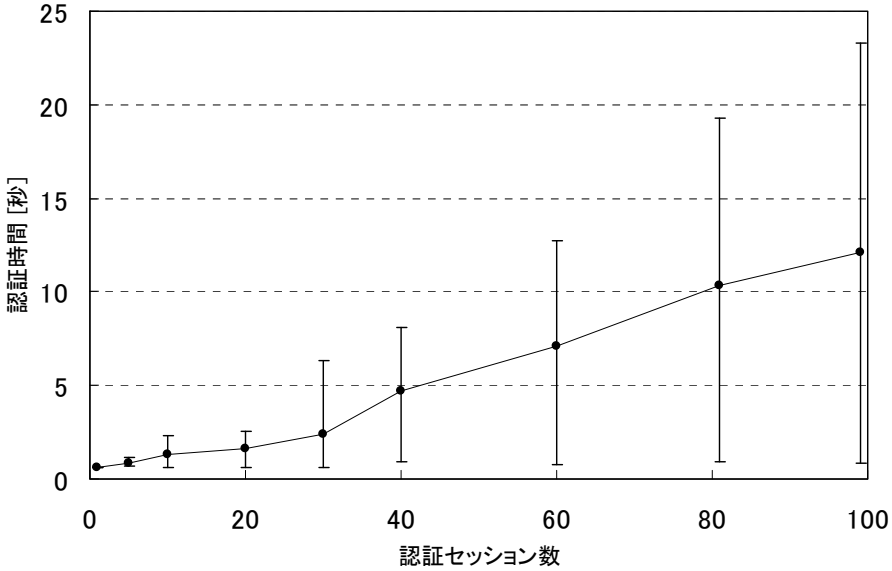


図 10　同時認証セッションに対する応答時間
（https 接続，鍵長 2,048 ビット）

5　移行の支援体制とシステム

5.1　申請手順

ゾーンＣを利用するには、コネクタ ID 申請、ゾーンＣ仮割当申請、ゾーンＣ本割当申請の３つが必要であり、図 11 のような手順で申請する[7]。HINET2007 では建物集約スイッチ、フロアスイッチの各ポートまでを一元的に管理するため、スイッチとポートにスイッチ ID とコネクタ ID と呼ぶユニークな識別番号を付している。利用者はコネクタ ID 申請において最寄りのスイッチ ID を指定するとポートが割り当てられ、コネクタ ID の通知と同時にコネクタ ID が印刷されたシールが送付される。利用者は指定されたポートに接続したフロア配線の情報コンセントにそのシールを貼り付け、以後のゾーンＣ本割当申請でポートを指定するために使用する。ゾーンＣ仮割当申請では VLAN ID の割当を行い、ゾーンＣ本割当申請ではコネクタ ID の VLAN ID への対応付けと、必要に応じて MAC アドレス認証をするためのホスト登録を行う。一方、ゾーン A,B はコネクタ ID 申請の後、ゾーンＣ本割当申請と同様な処理を行う。なお、ゾーン A,B は MAC アドレス認証のみである。

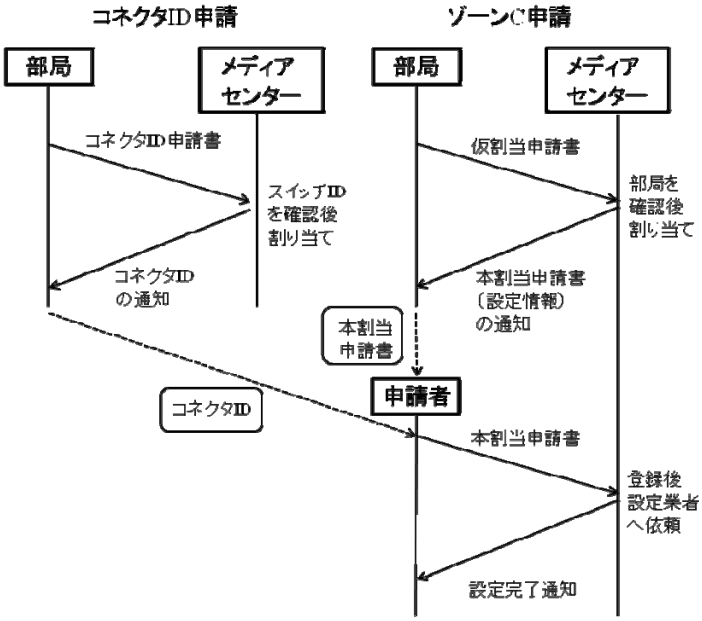


図 11　コネクタ ID とゾーンＣの申請手順

5.2 支援体制

これまで支線ネットワークの整備およびサブネットの管理はそれぞれの部局等で独自に行われてきたことから、移行段階においてはさまざまな例外処理が必要になることが予想されたため、人手による申請受付を行うこととした。コネクタ ID 申請およびゾーン申請は Excel で書かれた申請書に必要事項を記入し、電子メールで受付アドレスに送付する。メディアセンターでは教員 5 名が日替わりで受付処理を担当し、設定担当(外注業者)に指示している。申請書およびコネクタ ID やゾーンの管理台帳は WebDAV を利用して共有し、受付処理担当、設定担当および移行支援担当が常時参照できるようにしている。

設定が完了した後の HINET2001 から HINET2007 への接続変更、IP アドレスの変更は現場での作業となる。これらの作業は原則として申請者本人が行うこととしているが、申請者からの要請があった場合にはメディアセンターの職員のほか、技術センターの職員が支援を行う体制を構築した。技術センターには学内の全技術職員が所属し、派遣先の部局等でそれぞれの専門に基づいた技術支援業務を行う組織である。技術センター職員は全学に分散配置されており、派遣先の事情に詳しいため、彼らの力を有効活用することとした。HINET2007 の仕様が確定した約 1 年前から、技術センターの職員に対して新旧ネットワークの違い、新ネットワークの特徴、運用方針などの講習会を実施して移行開始に備えた。

5.3 ホスト登録システム

移行段階ではコネクタ ID の割当、ゾーンの割当などを集中的に行うため、人手による受付処理を行っているが、申請から完了までに最大 2 営業日かかる。そのため、ゾーン C 移行後の認証方式の変更(Web 認証から MAC アドレス認証へ)、ゾーン A,B のホストの入れ替え(MAC アドレスの変更)などの軽微な変更については、申請後すぐに変更が反映されるようホスト登録システムを構築した。管理者または副管理者は、利用者認証の後に自らが管理するゾーン C あるいはゾーン A,B のホストの属性(現在は MAC アドレスのみ)を変更できるようになっている。ホスト登録システムには、ゾーン C の申請を受け付け、VLAN ID や IP アドレスの割り当てを行い、コネクタ ID の対応付けを行って、設定担当に設定依頼を自動的に送付する機能も持たせているため、移行期間終了後は順次機能の提供を開始する予定である

6 おわりに

本稿では、広島大学で構築した新キャンパスネットワーク HINET2007 の特徴、運用・移行の方針、設計・構築のポイント、移行の支援体制とシステムについて概要を述べた。HINET2007 の構築手法は、教育研究を遂行する上での自由度を一定のレベルで維持しつつ、全体的なセキュリティレベルの底上げを図る現実的なひとつのモデルとなると考えている。最後に、2008 年 5 月(申請受付は 4 月)から開始した移行の状況は表 2 のようになっており、2008 年 12 月末現在でコネクタ ID 登録数は 3,798、ゾーン C 割当数は 832 である。一方、HINET2001 の残存ホスト数は図 12 のように推移しており、移行のペースが鈍ってきているため、2009 年 3 月末の HINET2001 停止に向けて各サブネットの管理者に残存ホスト(MAC アドレス)の一覧を送付し、ラストスパートを呼びかけているところである。

［謝辞］

HINET2007 の構築および移行、運用に尽力いただいている広島大学総務室情報化推進グループ、技術センターおよび情報メディア教育研究センターの関係者に感謝します。

表 2 HINET2007 の移行状況

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
申請メール受付数	28	126	100	140	173	183	110	100	126			
コネクタ登録数	-	520	95	1215	608	493	230	178	530			
コネクタ削除数	-	28	2	1	6	20	14	0	0			
アドレス登録数	-	290	215	1044	745	934	354	173	83			
アドレス削除数	-	8	11	16	9	32	34	10	2			
ゾーンC割当数	76	322	56	36	154	61	42	33	52			

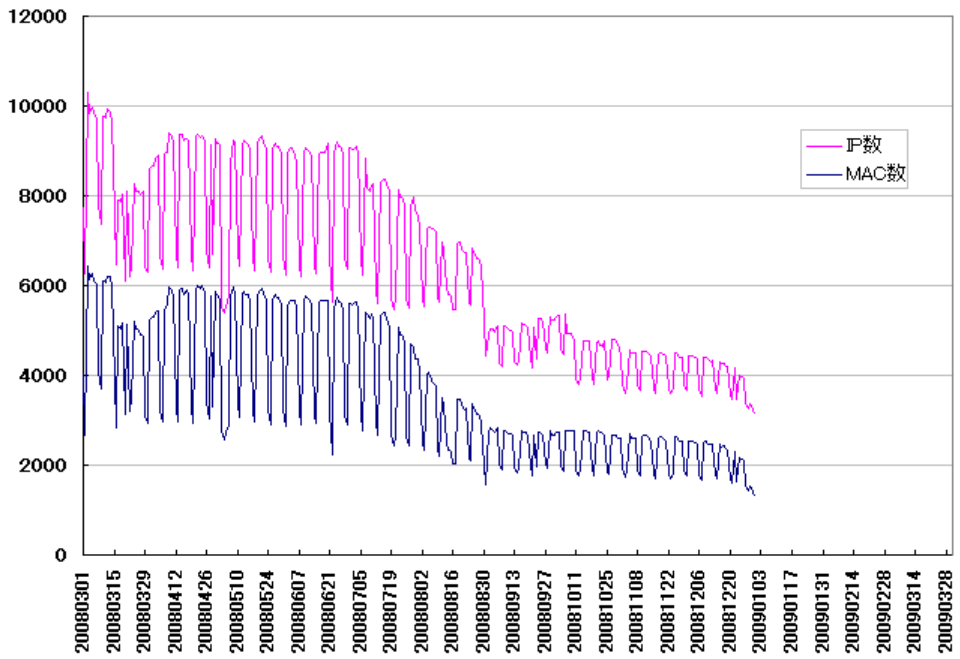


図 12　HINET2001 の接続ホスト数の状況

参考文献

[1] 広島大学情報メディア教育研究センター：
“HINET2007 情報”，http://home.hiroshima-u.ac.jp/infra/hinet2007info/.

[2] 相原 玲二，西村 浩二，岸場 清悟，田島 浩一，近堂 徹，“利用者認証機能を持つ大規模キャンパスネットワークの構築”，2008 年電子情報通信学会総合大会，BS-8-7，pp.S-116-S117（2008 年 3 月）.

[3] 相原 玲二，西村 浩二，近堂 徹，岸場 清悟，田島 浩一，“全教員に個別ファイアウォール機能を提供するキャンパスネットワークの構築”，情報処理学会研究報告，2008-IOT-2-6，pp.29-34（2008 年 7 月）.

[4] 西村 浩二，秋成 秀紀，野村 嘉洋，相原 玲二，“遠隔機器制御プロトコルを用いた有線／無線 LAN 用情報コンセントシステム”，情報処理学会論文誌，Vol.43，No.2，pp.662-670（2002 年 2 月）.

[5] 国立情報学研究所 UPKI イニシアティブ：サーバ証明書発行・導入における啓発・評価研究プロジェクト，http://upki-portal.nii.ac.jp/cerpj.

[6] 近堂 徹，田島 浩一，岸場 清悟，大東 俊博，岩田 則和，西村 浩二，相原 玲二，“利用者認証機能を備えた大規模キャンパスネットワークの性能評価”，情報処理学会第 1 回インターネットと運用技術シンポジウム（IOTS2008），pp.121-128（2008 年 12 月）.

[7] 大東 俊博，近堂 徹，岸場 清悟，田島 浩一，岩田 則和，西村 浩二，相原 玲二，“広島大学における新キャンパスネットワークへの移行手法”，情報処理学会研究報告，2008-IOT-3-6，pp.31-36（2008 年 9 月）.

2009年1月29日
サイエンティフィック・システム研究会
2008年度システム技術分科会第2回会合

日本最大規模のキャンパス認証ネットワーク ～HINET2007の構築と運用～

西村 浩二，相原 玲二，近堂 徹，大東 俊博，
田島 浩一，岸塲 清悟，岩田 則和

広島大学 情報メディア教育研究センター

広島大学

本報告の内容

- HINET2007の構築と運用
  - 導入の背景
  - 概要と特徴
  - 管理・運用・移行の方針
  - 設計・構築のポイント
  - 移行の支援体制とシステム
  - 移行の進捗状況

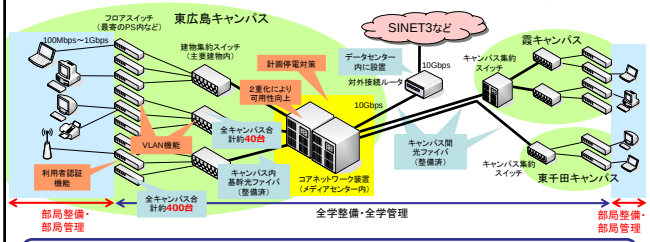
大学等のネットワークに対する要求

- 高度で柔軟なキャンパスネットワーク
  - 学部、学科、研究室等の単位でサブネット構築
  - 目的に応じて比較的自由な運用

ネットワークのライフライン化
セキュリティインシデントの多発

- 管理方針の根本的な見直し
  - 研究室は独立した企業活動（教員は社長）
  - しかし、外部からは同一組織とみなされる
  - さらに、経営の効率化を求められる

キャンパス情報ネットワーク HINET2007



- 2008年5月から本格移行開始
- 規模
  - 主要3キャンパス（東広島、霞、東千田）、附属学校、小規模遠隔部局（東京，福山，尾道，竹原，呉，宮島）
- 教員約1,800人、職員約3,300人、学生15,000人
- フロアスイッチ約400台（約14,000ポート）を全学整備

HINET2007の特徴

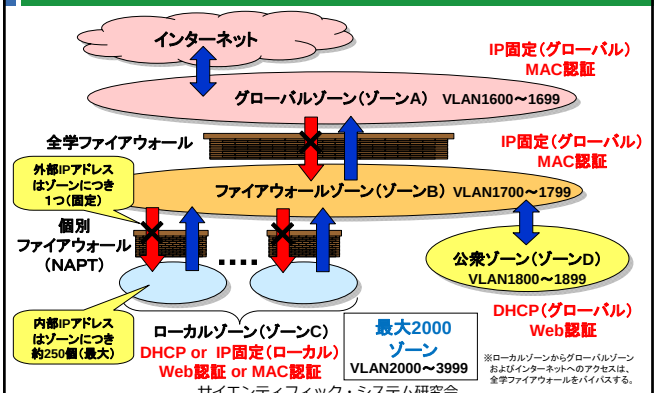
- 全学的な一元管理体制
  - ボランティアベースによるサブネット管理体制の破綻
  - 各フロアに設置するスイッチまで全学で一元管理
- VLANによる柔軟な仮想配線の提供
  - 同一研究室（グループ）が異なる建物等に分散する場合に対応
  - 学外向けサーバの設置、JGN2plusなどの利用に対応
- 個別ファイアウォール機能の提供
  - 全学ファイアウォール（対学外）のみでは不十分
  - ブロードバンドルータ相当の機能を教員数程度（約2,000個）提供
- すべての接続場所において利用者認証を要求
  - 多様な機器に対応するためWeb／MACアドレス認証を採用
  - 認証後はワイヤレートでの通信が必要

「ゾーン」の導入

ゾーン名略称	グローバルゾーン ゾーンA	ファイアウォールゾーン ゾーンB	ローカルゾーン ゾーンC	公衆ゾーン ゾーンD
主な用途	学外向けサーバ接続	学内共有サーバ接続	一般クライアント接続	オープンスペース
外部IPアドレス	グローバル　固定割当	グローバル　固定割当	グローバル　固定割当	グローバル　DHCP割当
内部IPアドレス	外部IPアドレスと同じ	外部IPアドレスと同じ	プライベート（NAPT）DHCPまたは固定割当	外部IPアドレスと同じ
ゾーン外からのアクセス	学内外とも制限なし	学外から不可 ゾーンAを除く 学内から可	同一ローカルゾーン以外から不可	学外から不可 ゾーンAを除く 学内から可
学外へのアクセス	制限なし	制限なし	原則制限なし（NAPTによる制限あり）	制限なし
端末認証	MACアドレス認証	MACアドレス認証	Web認証または MACアドレス認証	Web認証

これまでのサブネット構成とは異なる

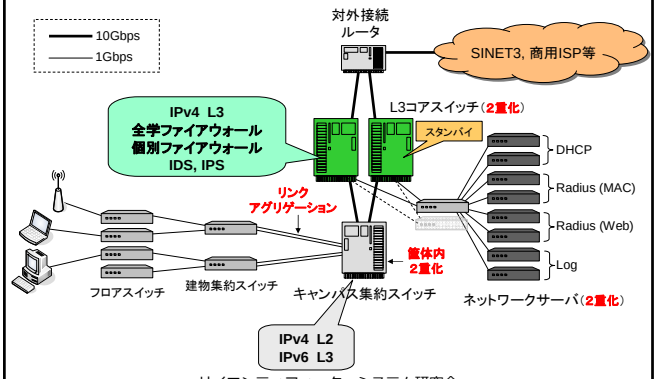
ゾーン種別とアクセス制限



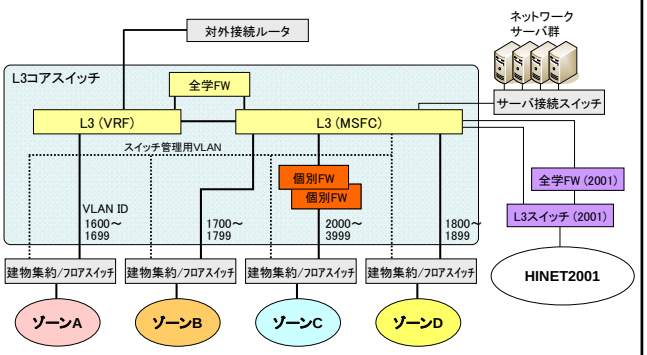
運用と移行の方針

- 運用方針
  - 個別ファイアウォールの例外設定は行わない
    - テレビ会議装置はグローバルゾーン（ゾーンA）に置く、など
    - 利用者が適切なゾーンを選択し、自己責任で守る
  - 個別ファイアウォールのローカル側／グローバル側のＩＰアドレスの希望は受け付けない
  - 希望すればスイッチの下流ポートへVLANをTaggedで提供（ただしVLAN IDはメディアセンターが指定）
    - 仮想ポート（1本の物理配線に複数のゾーンを載せることが可能）
- 移行方針
  - 移行期間は平成20年度末（2009年3月末）まで
    - 期間中はHINET2001とHINET2007を並行運用
  - IPアドレスのリナンバーが必要
    - 移行はポート単位で可能

基幹ネットワークの物理構成



L3コアスイッチの設定



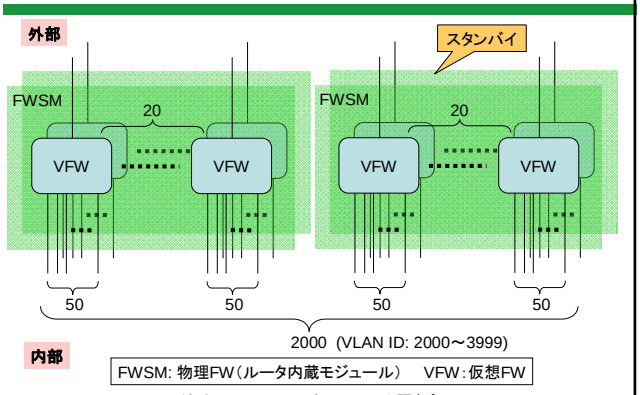
HINET2007 / HINET2001間のアクセス

X → Y 方向のアクセス可否　　△：同一ゾーンC内ではアクセス可、異なるゾーンC間ではアクセス不可

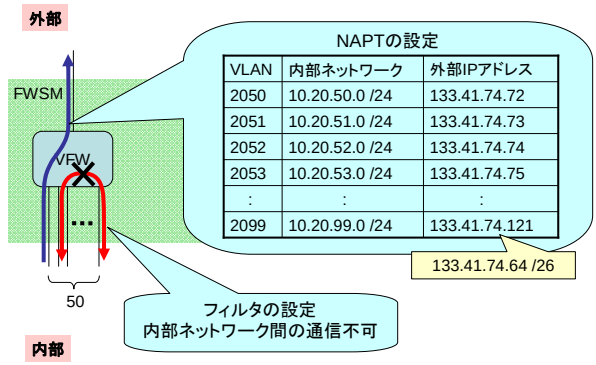
X ＼ Y	ゾーンA	ゾーンB	ゾーンC	ゾーンD	全学サーバ	2001 Global	2001 FW	学外
ゾーンA	○	×	×	×	○	○	×	○
ゾーンB	○	○	×	○	○	○	○	○
ゾーンC	○	○	△	○	○	○	○	○
ゾーンD	○	○	×	○	○	○	○	○
全学サーバ	○	○	×	○	○	○	○	○
HINET2001 Global	○	○	×	○	○	○	○	○
HINET2001 FW	○	○	×	○	○	○	○	○
学外	○	×	×	×	○	○	×	ー

全学サーバ：全学電子認証システムなど全学的サーバ接続用
HINET2001 Global：HINET2001の全学ファイアウォールに入っていないサブネット
HINET2001 FW：HINET2001の全学ファイアウォールに入っているサブネット

個別ファイアウォールの構成

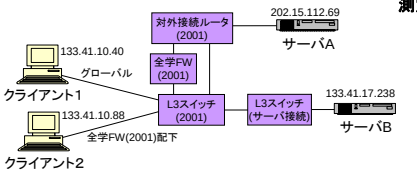


仮想ファイアウォールの設定



VLAN	内部ネットワーク	外部IPアドレス
2050	10.20.50.0 /24	133.41.74.72
2051	10.20.51.0 /24	133.41.74.73
2052	10.20.52.0 /24	133.41.74.74
2053	10.20.53.0 /24	133.41.74.75
:	:	:
2099	10.20.99.0 /24	133.41.74.121

移行前（HINET2001）の通信性能測定

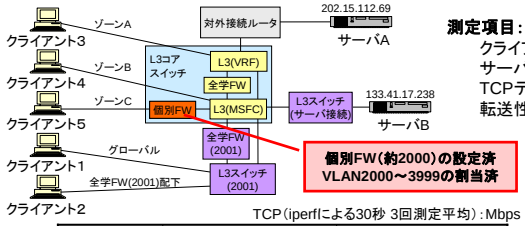


測定項目：
クライアント・サーバ間のTCPデータ転送性能

TCP（iperfによる30秒 3回測定平均）：Mbps

	サーバA		サーバB	
	送信	受信	送信	受信
クライアント1	505	444	672	620
クライアント2	--	360	680	645

HINET2007移行後の通信性能測定



測定項目：
クライアント・サーバ間のTCPデータ転送性能

TCP（iperfによる30秒 3回測定平均）：Mbps

	サーバA		サーバB	
	送信	受信	送信	受信
クライアント1	471	517	704	709
クライアント2	--	365	691	615
クライアント3	637	685	712	878
クライアント4	--	348	696	801
クライアント5	--	292	--	433

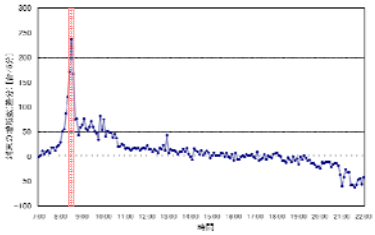
利用者認証機能に対する要件（1）

- ネットワークインフラとしての認証ネットワーク
  - 多様な機器に対応
    - 複数OSが混在（Windows, Linux, Mac OS X/9など…）
    - PC以外のネットワーク機器も認証
  - 既存の研究室内ネットワークとの親和性
    - ダムハブなども多数存在
  - 認証後でもワイヤスピードを確保
    - 認証を入れることによるパフォーマンス低下は×

最寄りのフロアスイッチにて利用者/機器認証
WEB（HTTPS）認証とMACアドレス認証をサポート

利用者認証機能に対する要件（2）

- 短時間での一斉認証要求への対応
  - 共同利用施設（演習用端末室）や事務職員用端末
    - 広島大学には事務職員用端末が約1,400台存在

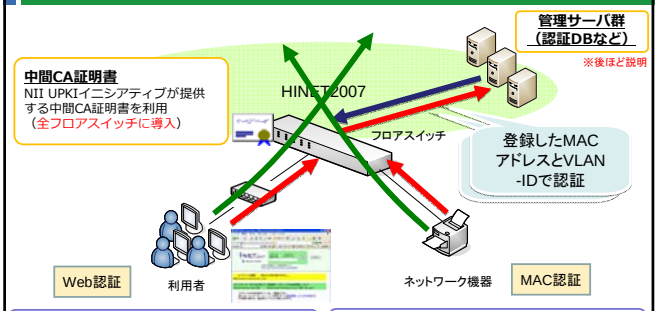


8時20分から35分（15分間）で約600台が稼働

100台からの同時認証を30秒以内で処理できることを条件

HINET2001における端末増減数（５分間隔）※2007年1月29日（月）に採取

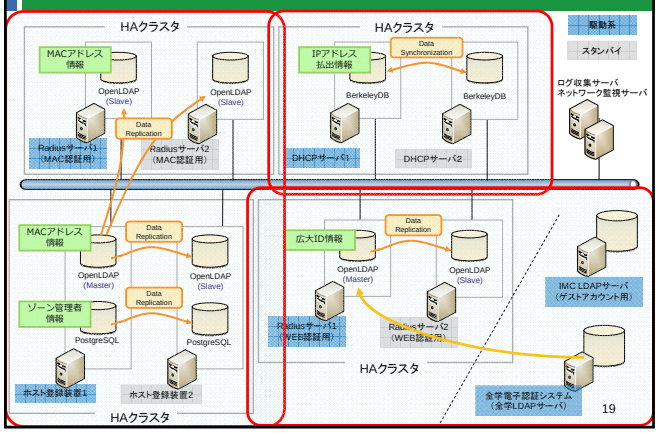
利用者認証の概要



httpsによる利用者認証
初回接続時に認証ページをリダイレクト表示
全学電子情報基盤で管理するIDを利用
ARPポーリング/リンクダウンによるログアウト

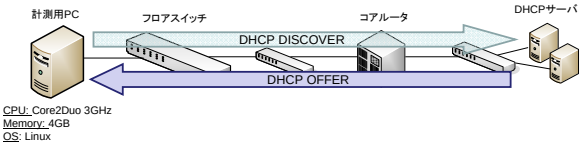
MACアドレスは事前登録（登録システムを利用）
Web認証が困難な機器を対象（プリンタ，NAS等）

HINET2007サーバ群の構成

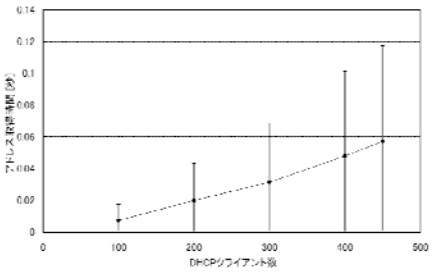


DHCPサーバのIPアドレス払い出し性能

- 実験概要
  - 計測用PCを稼働中のフロアスイッチに接続
  - 複数DHCPリクエストを同時に送信
    - PerlのDHCPクライアントライブラリを利用
    - 異なるMACアドレスでDHCP DISCOVERを送信
  - DHCPリクエストからアドレス取得時間までを計測
    - DHCP-DISCOVER から DHCP-OFFER
    - DHCPサーバのIP払出しDB更新を含む



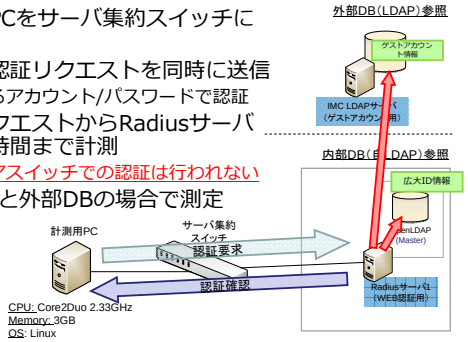
DHCPサーバのIPアドレス払い出し性能



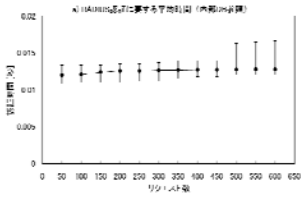
450台のDHCPアドレス取得要求に対して
最大0.12秒以内で処理が完了

Radiusサーバの同時認証性能

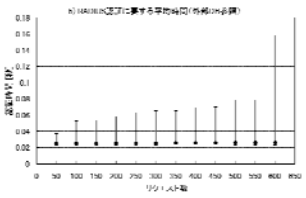
- 実験概要
  - 計測用PCをサーバ集約スイッチに接続
  - 複数の認証リクエストを同時に送信
    - 異なるアカウント/パスワードで認証
  - 認証リクエストからRadiusサーバの応答時間まで計測
    - フロアスイッチでの認証は行われない
  - 内部DBと外部DBの場合で測定



Radiusサーバの同時認証性能



内部DB参照（通常のWeb, MAC認証）

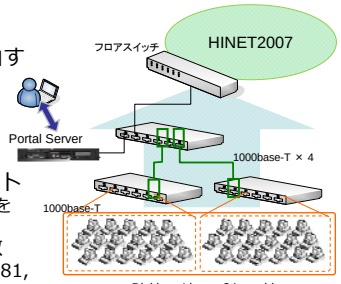


外部DB参照（ゲストのWeb認証）

600台からのRADIUS認証要求に対して
1秒以内に処理可能

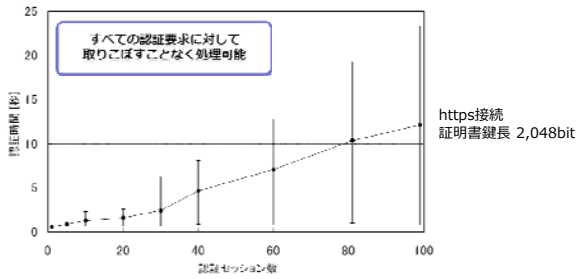
認証スイッチの同時認証性能

- 実験概要
  - フロアスイッチを経由する同時Web認証性能
  - リダイレクトと認証処理時間の和を計算
  - 100個の個別リクエスト
    - IMCゲストアカウントを利用
  - 同時接続セッション数
    - 1, 5, 10, 20, 30, 40, 81, 99
  - 認証リクエストは1秒以内で同期



近堂ら, "PCクラスタによる認証スイッチの認証評価システム", 2007-DSM-47(5), pp.25--30

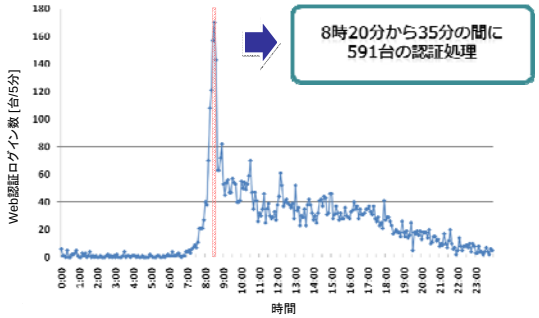
認証スイッチの同時認証性能



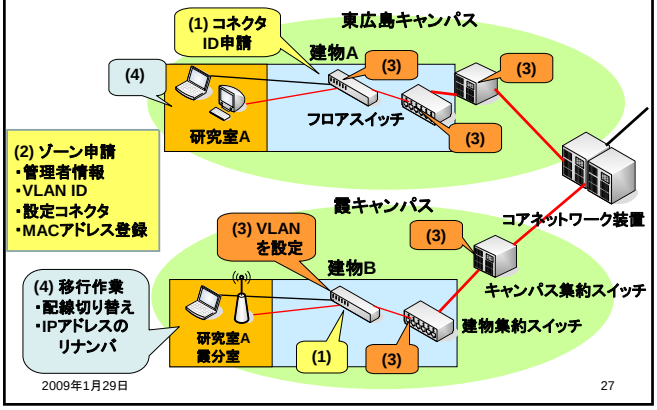
数セッションの同時認証では1秒
100セッションの同時認証でも最大23秒 で処理可能

現在の利用状況

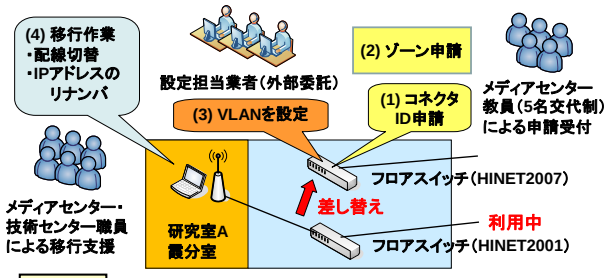
- Web認証の推移（5分間隔のログイン処理数）



ネットワーク移行の概要（移行手順）

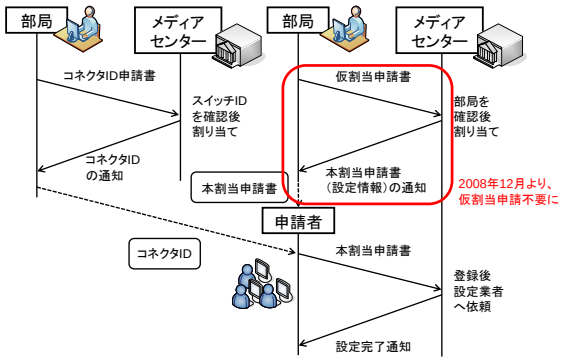


ネットワーク移行の概要（支援体制）



ポイント
HINET2001との並行運用
➡ 利用者の都合が良いタイミングで移行可能

コネクタIDとゾーンCの申請手順



ホスト登録システム

- Webによる移行申請受付、設定変更の自動化
  - 定常運用時での使用を想定
- 移行初期は人海戦術による手動申請受付
  - 部局で連続したグローバルIPアドレスを取得したい（電子ジャーナル対策）
- 2008年12月より
  一部機能開放
  - 副管理者登録・変更
  - ホスト情報登録・変更
    削除（ゾーンC）
  - MACアドレス登録・
    変更（ゾーンA,B）
  - 年度更新（ゾーンA,B）

ホスト登録システムの画面例

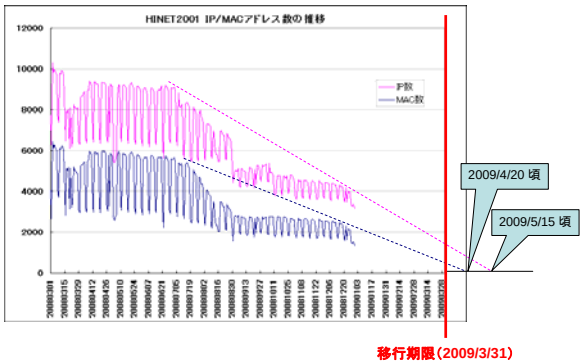
移行進捗状況（2008年12月末現在）

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
申請メール受付数	28	126	100	140	173	183	110	100	126				1086
コネクタID登録数	-	520	95	1215	608	493	230	178	530				3869
コネクタID削除数	-	28	2	1	6	20	14	0	0				71
MACアドレス登録数	-	290	215	1044	745	934	354	173	83				3838
MACアドレス削除数	-	8	11	16	9	32	34	10	2				122
ゾーンC割り当て数	76	322	56	36	154	61	42	33	52				832

コネクタID　最大14,000ポート ➡ 3,798ポート割当

ゾーンC　最大2,000ゾーン ➡ 832ゾーン割当

HINET2001 IP/MACアドレス数の推移



まとめ

- HINET2007の概要
  - 特徴
    - 全学的な一元管理体制
    - VLANによる柔軟な仮想配線の提供
    - 個別ファイアウォール機能の提供
    - すべての接続場所において利用者認証を要求
  - 管理・運用・移行の方針
  - 設計・構築のポイント
    - 個別ファイアウォール機能の実現
      - スループット測定
    - 利用者認証機能の実現
      - DHCPサーバのIPアドレス払い出し性能
      - Radiusサーバの同時認証性能
      - 認証スイッチの同時認証性能
  - 移行の支援体制とシステム
  - 移行状況

使用した機器の名称または仕様

装置	機器の名称または仕様
フロアスイッチ	Alaxala AX2430S
建物集約スイッチ	
サーバ集約スイッチ	
Radiusサーバ	CPU: Xeon X5355 2.66GHz x 2, Memory: 4GB FreeRADIUS 1.1.7, OpenLDAP 2.3.41
DHCPサーバ	CPU: Xeon X5355 2.66GHz x 2, Memory: 4GB ISC-DHCP 3.05
L3コアスイッチ（2007）	Cisco Catalyst 6509 w/ FWSM x 3, IDSM x 2
対外接続ルータ（2007）	Alaxala AX6304S
L3スイッチ（サーバ接続）	Cisco Catalyst 6506
L3スイッチ（2001）	Cisco Catalyst 6509
全学ファイアウォール（2001）	Alteon Switched Firewall Director/Accelerator Checkpoint Firewall-1
対外接続ルータ（2001）	Hitachi GR2000-BH
サーバA, B	CPU: Pentium4 3.06GHz, Memory: 512MB
クライアント1～5	CPU: Pentium4 2.8GHz, Memory: 512MB

システム技術分科会　選出
2008 年度 システム技術分科会 第 2 回会合 より

組織の壁を越える
利用者グループ概念の導入
～農林水産研究における新しい認証基盤～

農林水産技術会議事務局筑波事務所

宮坂　和孝

組織の壁を超える
利用者グループ概念の導入

～農林水産研究における新しい認証基盤～

農林水産技術会議事務局筑波事務所
(農林水産研究情報総合センター)
宮坂 和孝

本日の内容

- **内容は「情報共有サービス」と「認証基盤」です**
  - 利用者の所属組織の内部・外部を問わない、非常に柔軟な情報共有サービスの事例紹介を行います
  - サービス実現に不可欠な認証基盤についても、詳しく紹介します
- **発表の流れ**

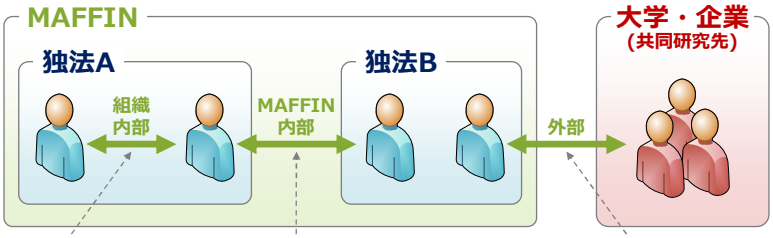
1. はじめに(情報共有サービスについて)
2. 農林水産研究情報総合センターについて
3. 情報共有サービスの改善
   1. 現行システムの問題点
   2. 次期システムのコンセプト
   3. 認証基盤の実装
   4. 認証基盤を活用するアプリケーションの整備
4. 今後の課題(認証連携時代に向けて)
5. まとめ

はじめに

情報共有サービスについて

情報共有サービスについて

- **産学官の連携はますます重要に**
  - 緊密な連携には情報共有が不可欠
  - どうすれば外部組織との情報共有がスムーズに行えるのか
    - カギは認証とアクセス制限
- **内部利用者の情報共有パターン**



同一組織内部の利用者と
- 独法側導入グループウェア
- 電子メール
- メーリングリスト
- 研究データ交換システム

MAFFIN内の他の組織の利用者と
- 電子メール
- メーリングリスト
- 研究データ交換システム

他の組織の利用者と
- 電子メール
- メーリングリスト
- 研究データ交換システム

農林水産研究情報総合センターについて

農林水産研究情報総合センターとは

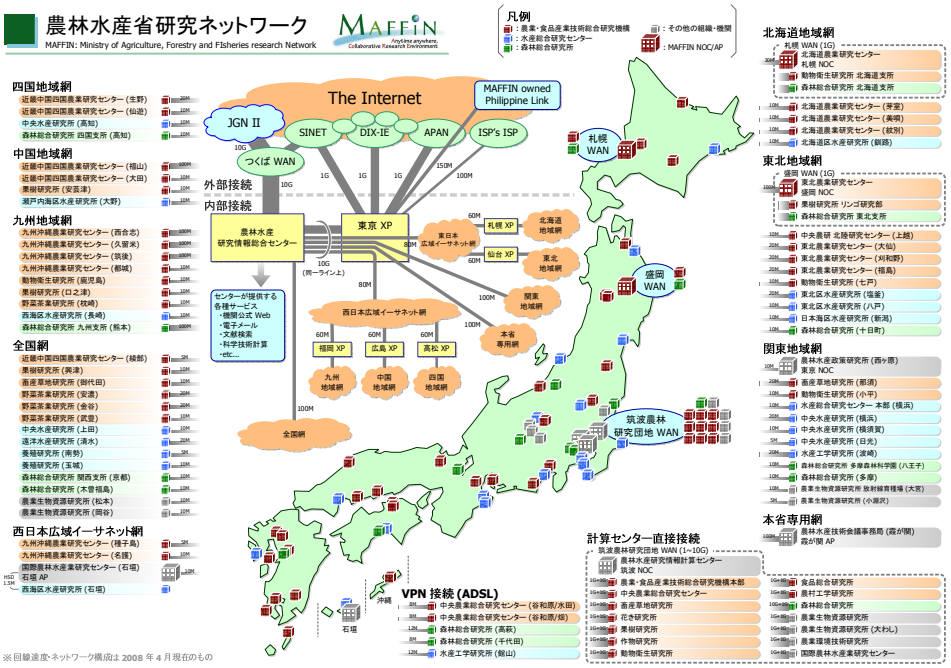
- **農林水産技術会議事務局筑波事務所が運営**
  - 国の機関、所在地つくば、30年以上の歴史(名称変更あり)
- **農林水産省研究ネットワーク(MAFFIN)を整備・運用**
  - 全国に展開する農林水産研究拠点を結ぶネットワーク
  - 「いつでも、どこからでも使える共同研究環境」の実現を目指す
    - "Anytime anywhere, Collaborative Research Environment"

ロゴにも記載

- **ネットワークから利用可能な各種サービスを運用**
  - 科学技術計算システム
  - ネットワークライブラリシステム
  - ネットワークサービスシステム
    - DNS、メール、利用者情報管理、情報共有サービス
  - AGROPEDIA(農学情報資源システム)など……

農林水産省研究ネットワーク

MAFFIN: Ministry of Agriculture, Forestry and FIsheries research Network



当センターの内部利用者

- **規模**
  - 約10,000人(うち研究者は約4,500人)
- **範囲**
  - 農林水産省の職員
  - 省の所管する独立行政法人の役職員と受け入れ職員
  - 省が推進する競争的資金による研究・プロジェクト研究等に参画する都道府県・大学・民間の研究機関の職員
  - etc…

※大学や企業の研究者でも当センターの「内部利用者」となることができます
参考: http://www.affrc.go.jp/PDF/news/pdf/news_no26.pdf
(ただし、一部のサービスは利用できない場合があります)

- **内部利用者特典**
  - 各種サービスが利用可能に
    - ネットワーク系サービス(メール、メーリングリスト、NAS、VPNなど)
    - 計算系サービス　(スパコン、アプリケーションなど)
    - 図書館系サービス　(文献複写依頼、オンラインジャーナルなど)

当センターの認証系システムの変遷

- **センター設立当初から認証情報は一元管理**
  - 古くはメインフレームの利用者管理から
  - 1993年に所属管理用の利用者管理データベースを作成
  - メールサーバが各地域に分散していた頃でも、認証情報はセンター側で集中管理して各サーバに反映
- **2000年度システムでの改善**
  - 利用者管理システムを導入
    - 利用者管理データベースのWebフロントエンド
  - LDAPを導入
    - メール、ネットワークストレージ(FTP/CIFS)などの認証を一元化
- **2004年度システムでの改善**
  - WebSSO(Cookie有効範囲内で利用可能なSSO)を導入
    - 各システムをシームレスに渡り歩けるようになった

2008年度システム更新

- **システム更新は4年に一度**
  - 稼働から2年が経過した時点で取りまとめる「中間評価報告書」の内容に基づいてシステム設計を行う
- **2008年度システムの更新経緯**
  - 2005.03 現行システム(2004年度システム)稼働
  - 2006.12 中間評価作業部会設置
  - 2007.04 中間評価報告書
  - 2007.09 システム設計作業部会設置
  - 2007.12 資料招請
  - 2008.05 意見招請
  - 2008.07 仕様書配布
  - 2009.03 新システム稼働(予定)

大まかなシステム構想は
2006年夏頃~2007年秋頃に

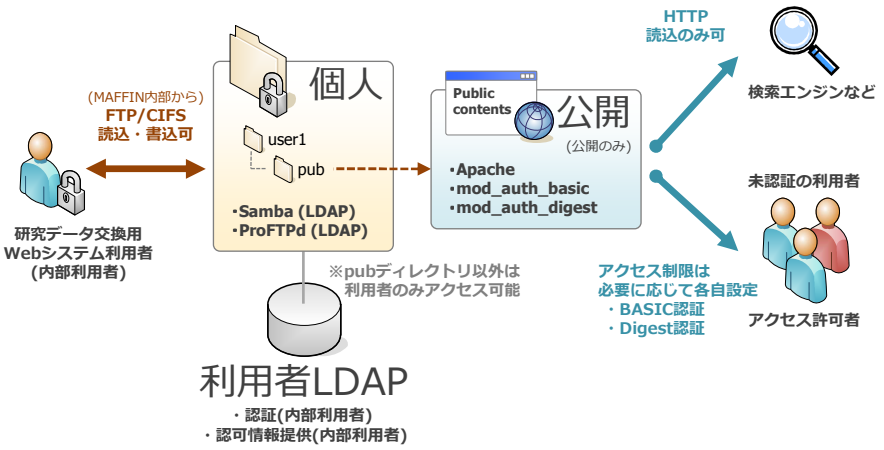
現行システムの問題点

情報共有サービスの改善(1)

個人向け情報共有サービス

- **研究データ交換用Webシステム**
  - 概要
    - 個人用ネットワークストレージと連携したWebスペースの提供
  - 利用ケース
    - 研究者プロフィール・業績などのWeb公開
    - メールでは送信できない大容量データの引き渡し
  - 詳細
    - ファイルのアップロードは、FTPおよびWindowsファイル共有経由で、MAFFIN内部からのみ可能
    - 容量上限10GB
    - 個人用フォルダ内の公開用フォルダが自動的にWeb公開される
      - http://cse.*所属組織サブドメイン*.affrc.go.jp/*アカウント名*/
    - CGI スクリプトなどの設置・実行は不可能
    - アクセス制限は自前でBASIC認証などを設定する必要あり
      - WebSSOとは連携していない(Cookie盗聴防止のため)

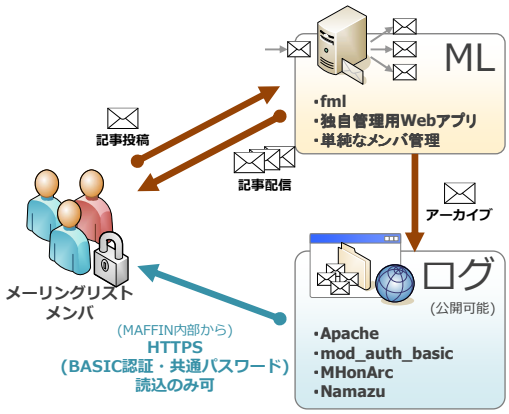
現行: 研究データ交換用Webシステム



グループ向け情報共有サービス

- **メーリングリストシステム**
  - 概要
    - 多人数による電子メールを介した共同作業を円滑に進めるためのメーリングリスト機能の提供
  - 利用ケース
    - 研究・業務グループ内での情報共有
    - 学会・シンポジウムの事務局連絡先
    - メールマガジン発行
  - 詳細
    - メーリングリストマネージャはfml
    - 独自作成の管理用Webインタフェース
    - 過去記事Webアーカイブ
      - アクセス制限は、共通アカウントと共通パスワードによるBASIC認証(パスワード設定はWebインタフェースから行える)
      - ただし、MAFFIN外部からのアクセスは不可能

現行: メーリングリストシステム



問題点1: アクセス制限

- **アクセス制限の設定が難しい**
  - htpasswdコマンド、htdigestコマンドを使えない利用者が多い
  - そもそも.htaccessという名前のファイルを作れない利用者も多い
- **簡単なパスワードを設定しがち**
  - 設定したユーザ名・パスワードをメールなどで相手に伝える必要があるため、「わかりやすいパスワード」を設定してしまう
  - 相手から見ると、自分自身で設定したパスワードではないため、パスワードを覚えにくい
- **多人数でファイルを供覧する場合でも、一対のユーザ名・パスワードで済ませがち**
  - 全員にパスワードを割り当てて全員に連絡するのは面倒すぎる
  - 相手から見ると、「全員知っているパスワード」であるため、パスワードの機密意識が低くなる

問題点2: ファイルのアップロード

- **外部からファイルをアップロードできない**
  - システム構成上、アップロードできるのは内部利用者だけ
    - 研究データ「交換用」Webシステムなのに、実は「交換」できない
    - アップロード不能とした理由
      - 適切なアクセス制限が困難である
      - 「誰々がアップロードした」というログを残せない
      - CGIを許可するとセキュリティ管理が困難
- **ファイルをアップロードできないのは外部だけではない**
  - 内部利用者間のファイルの交換でも、お互いのファイルスペースに直接アップロードすることはできない

問題点3: 情報公開管理

- **公開してはいけない情報をうっかり公開してしまう**
  - 研究データ交換用Webサービスの公開用フォルダ
    - システム構成の問題
      - 個人のフォルダの中に公開用フォルダを配置する現行の構成
      - 機密性の高いファイルをうっかり置いてしまう可能性
    - 利用者の意識の問題
      - 「誰もアクセスしないだろう」という思い込み
      - アクセス制限を掛けずに著作権を侵害するようなコンテンツを公開領域に置いてしまう可能性
- **公開したい情報を公開できない**
  - メーリングリストの過去記事アーカイブ
    - システム側でアクセスを「MAFFIN内からのみ」にIPアドレスで制限
    - インターネットの検索にも引っ掛からない
    - 貴重な農林水産研究情報が埋もれてしまう

次期システムのコンセプト

情報共有サービスの改善(2)

次期情報共有サービスのコンセプト

- **コンセプト**
  - 「認証・アクセス制限・管理の強化」を行い、より柔軟なサービスを
- **具体的には:**
  - 認証範囲を広げる　本日の発表の中心です
    - 外部組織の利用者でも認証可能な、懐の深い認証システムを提供
    - 各自が常に「自分のアカウントとパスワード」で認証できる環境づくり
      - 多人数へのアクセス許可時でも共通パスワードは不要とする
  - アクセス制限(認可)設定インタフェースを使いやすくする
    - 簡単にアクセス制限を設定できるようWebインタフェースを整備
    - 利用者／利用者グループを基本としたアクセス制限を徹底する
      - 権限さえあれば、誰でもファイルをアップロードできるように
  - 情報公開管理機能を導入する
    - 公開したい情報をきちんと公開できるように
    - 意図しない公開はある程度抑止できるように

認証可能な利用者の範囲拡大

MAFFIN Anytime anywhere, Collaborative Research Environment

■ ほぼ誰でも認証対象にできる下地を作る

- メールアドレスをIDとする「外部登録利用者」区分を新設する

信頼はできないが、認証はできるように

	内部利用者	外部登録利用者
利用者となる資格	必要(かなり限定)	不要
ID	英数字3~31文字	メールアドレス
利用者情報	正確な情報(公文書申請)	偽名も可能(本人独自申請)
管理DBの構造	複雑	単純

IDとしてメールアドレスを採用することについて

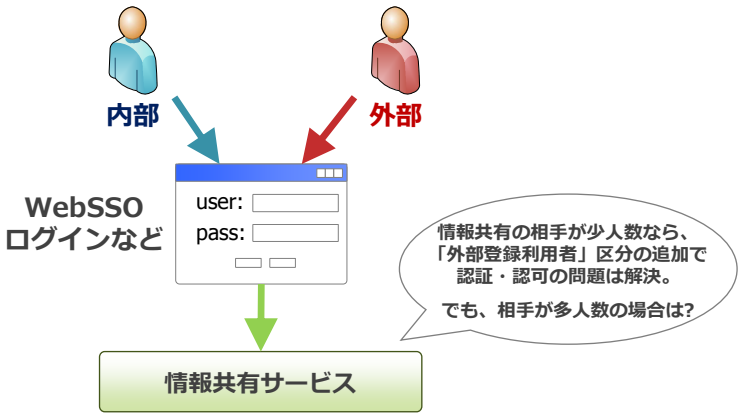
- ○ **電子メールは広く普及しており、誰でも登録できる**
- ○ **利用者が自分のIDを覚えやすい**
  - 独自の外部登録利用者IDを割り当てても、たいてい忘れられる
- × **IDに特殊記号が入るため、IDとして利用できないアプリもある**
  - ただし、最近のWebアプリなどでは考慮されていることも多い
  - 特殊文字含有ID→アプリ側でのローカルIDへのマッピングなど

認証サービスの拡大

MAFFIN Anytime anywhere, Collaborative Research Environment

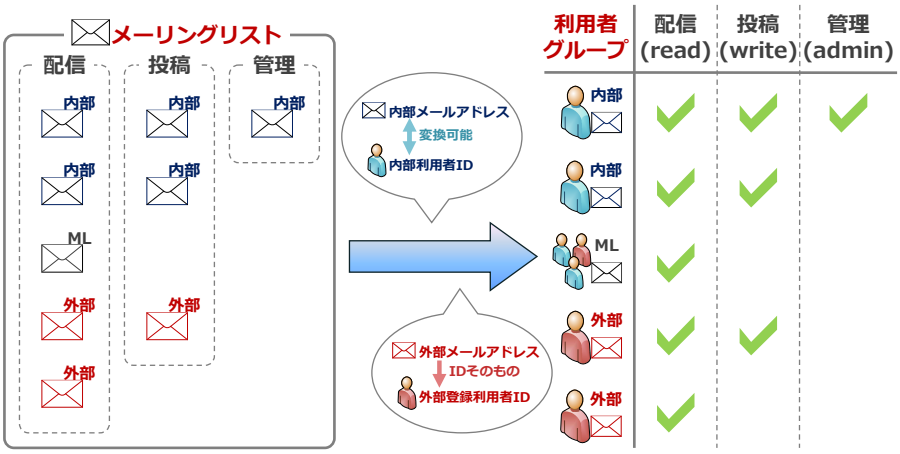
■ 内部利用者・外部登録利用者に同じ使い勝手を提供

- 内部利用者・外部登録利用者を区別せず同一のインタフェースでログインできる認証環境を整備する



利用者グループ概念の導入

- **既存のメーリングリストの捉え方を変える**
  - 「単なるメールアドレスの集合」から
    「認証可能な『利用者』の集合(利用者グループ)」へ



メーリングリストはグループとして優秀

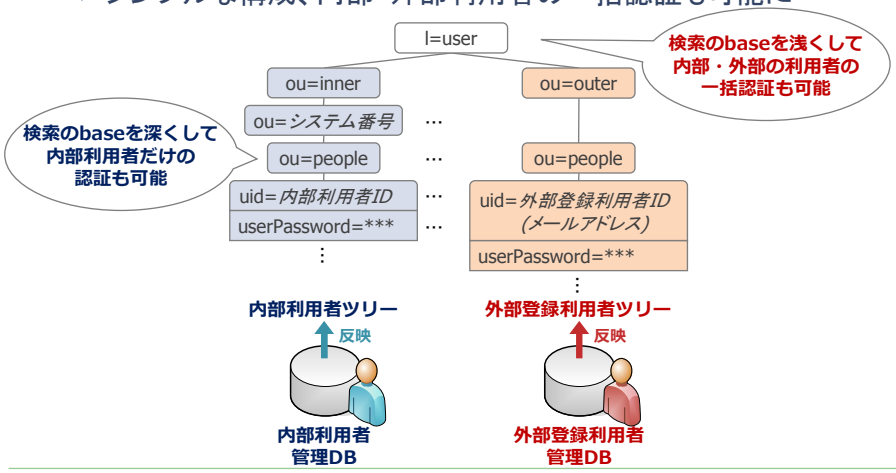
- **基本的な権限が明確**
  - グループの中での各メンバの役割が決まっている
    - 配信対象者(≒いわゆる読込権限を保持)
    - 投稿権限者(≒いわゆる書込権限を保持)
    - 管理者
  - この役割を他の情報共有ツールに当てはめることにより、非常に自然な形で情報共有サービスを拡充できる
- **その他の良いところ**
  - 情報共有したい、という目的で集まったメンバから構成される
    - 単なる組織階層情報から切り出したグループとは趣向が異なる
  - メンバ管理の方法が確立されており、利用者も慣れている
  - 管理者への連絡手段(専用メールアドレス)が用意されている
  - すでに約2,500個のメーリングリストがMAFFINに存在
    - 「農林水産系の研究者グループ」という財産の継承

認証基盤の実装

情報共有サービスの改善(3)

利用者LDAP

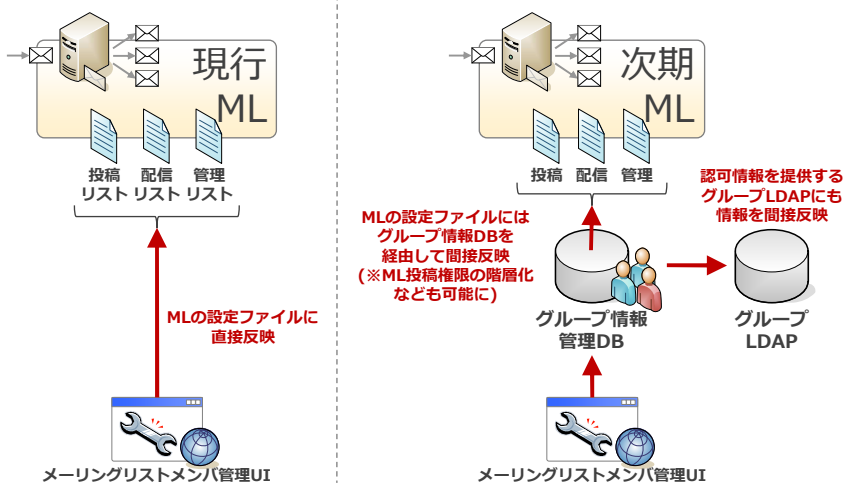
- **情報共有サービスの認証基盤として、利用者 LDAPを構築**
  - LDAPに登録する情報は各DBからの二次情報
  - シンプルな構成、内部・外部利用者の一括認証も可能に



グループ情報管理データベース

MAFFIN Anytime anywhere, Collaborative Research Environment

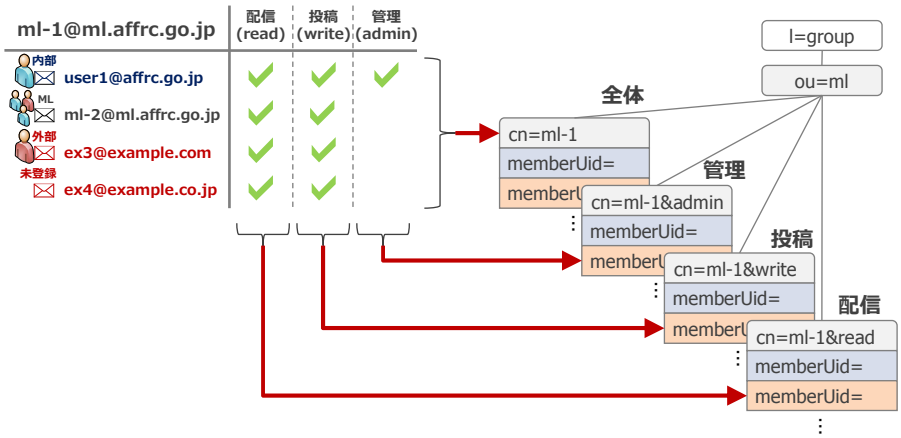
- **メーリングリストのメンバ情報を管理する**
  - メンバ情報を利用した二次情報の作成元となる



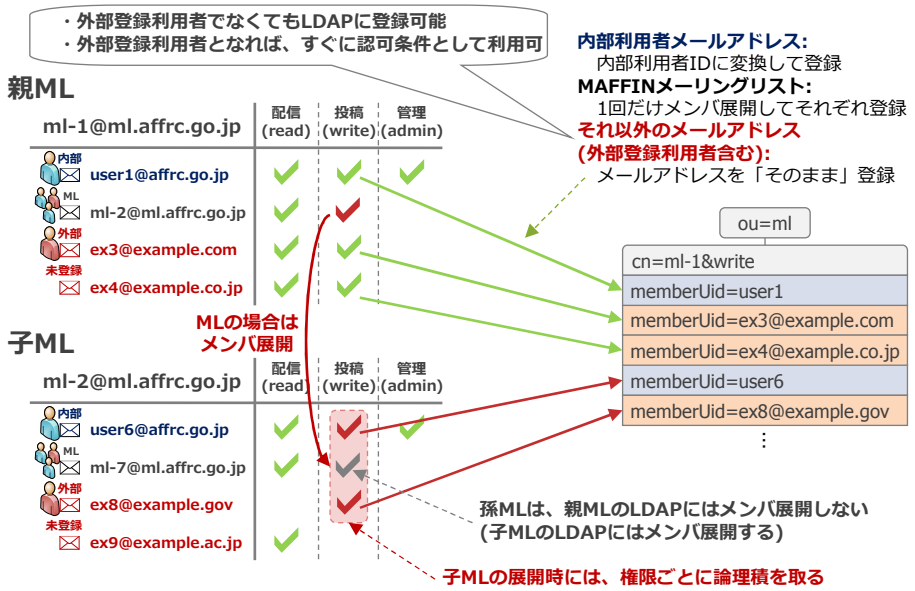
グループLDAP

MAFFIN Anytime anywhere, Collaborative Research Environment

- **情報共有サービスの認可基盤として、グループLDAPを構築**
  - 1つのメーリングリストから4つのグループを生成
    - ML全体グループと、権限ごとのグループ(配信・投稿・管理)

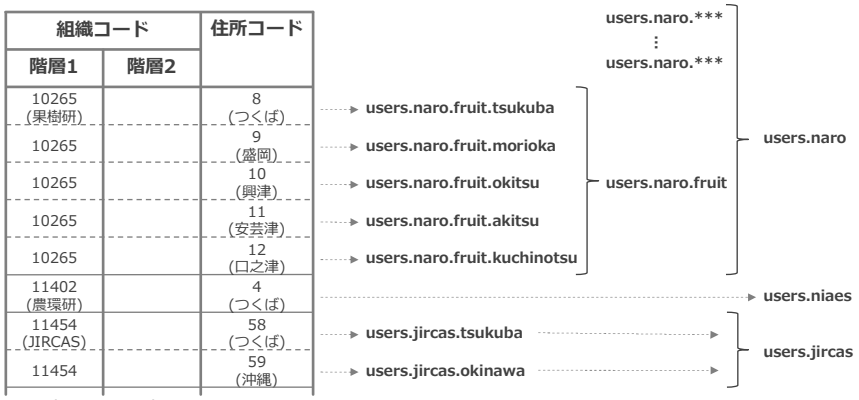


メンバ情報のグループLDAPへの登録



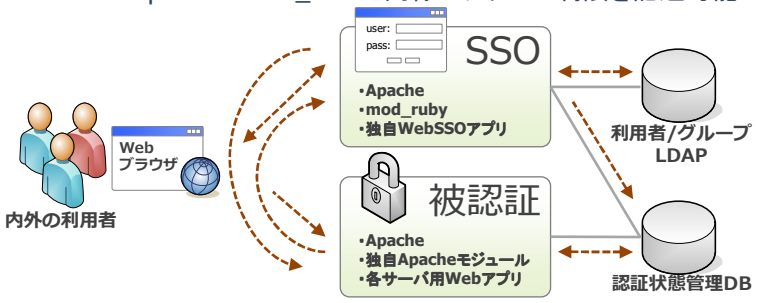
特殊グループ: プリセットグループ

- **ある拠点/組織の利用者に対応するグループを提供**
  - 組織コード・住所コードを元にバッチ処理でグループLDAPに登録
  - 従来の「IPアドレス(拠点サブネット)」によるアクセス制限を代替
    - ネットワーク中心ではなく、利用者中心のアクセス制限を身近に



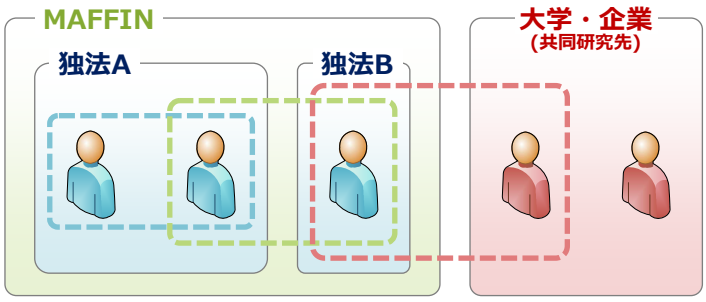
WebSSO

- **WebSSO機能も内部・外部の利用者に対応**
  - Cookieドメイン内で有効な独自方式のSSO
  - バックエンドは利用者/グループLDAP
    - 内部・外部の利用者を一括で認証可能
  - 被認証側のWebSSOクライアントはApacheモジュールとして提供
    - 認証・認可機能を含有
      - Apacheのmod_authと同様にアクセス制限を記述可能



ここまでのまとめ

- **この認証・認可基盤で実現できること**
  - 任意の利用者の認証
  - 任意の利用者のグループ化(組織の壁を超えても、何千人でも)
  - 利用者グループ情報の認可条件への利用



- **次は、認証基盤を利用する情報共有ツールの整備について**

認証基盤を活用する アプリケーションの整備

情報共有サービスの改善(4)

追加アプリケーションの選定

- **必要な機能の洗い出し**
  - 外部組織から接続できること
    - 現状ではHTTP上のサービス一択
  - MAFFINの認証基盤と連携できること
    - 可能な限りWebSSO、ダメならLDAPと連携
  - 権限として「アクセス不可」「読込」「書込」を設定できること
    - 「アクセス不可」権限は結構重要(実装していないWiki多し)
  - 権限として「誰でもアクセス可能」を設定できること
    - 「公開」は情報共有の延長線上に位置づけたい
  - アクセス制限設定インタフェースを統一できること
    - アクセス制限設定をPlain textで保存できるアプリだと都合がよい
- **DokuWikiとWebDAV(Apache+mod_dav)を選定**
  - DokuWikiは「ACL完備」「DBいらず」な優秀アプリ
  - WebDAVは大容量ファイルの交換に対応するため導入

権限とアクセス制限の連動

MAFFIN Anytime anywhere, Collaborative Research Environment

■ 初心者に優しく、上級者に便利に

- 初期設定で「安全、かつ十分便利に」使えるように

個人用
情報共有サービス

- 個人用Wiki
  - 読込: 本人のみ
  - 書込: 本人のみ
- 個人用共有フォルダ
  - 読込: 本人のみ
  - 書込: 本人のみ

グループ用
情報共有サービス

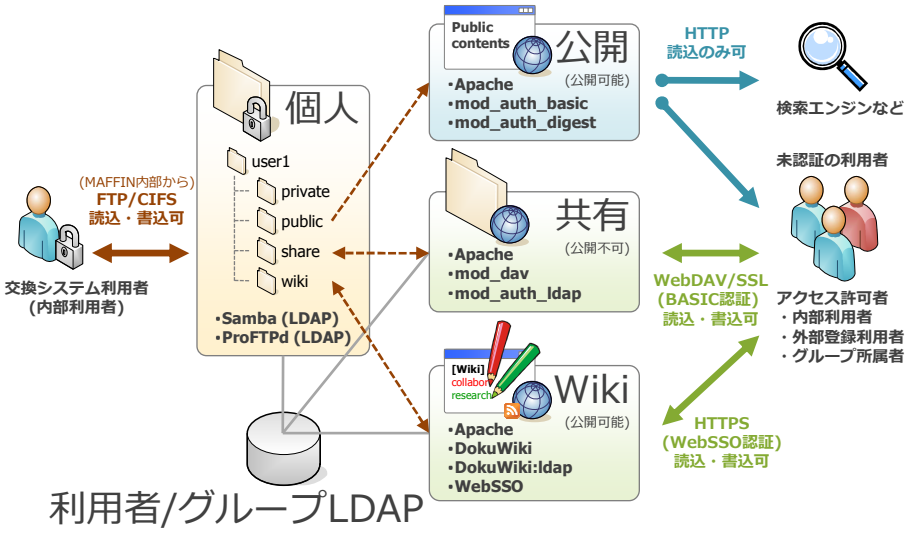
- ML用Wiki
  - 読込: 投稿グループ・配信グループ
  - 書込: 投稿グループ
- ML用共有フォルダ
  - 読込: 投稿グループ・配信グループ
  - 書込: 投稿グループ
- ML過去記事アーカイブ(読込のみ)
  - 読込: 投稿グループ・配信グループ

ML管理者グループは
いずれのサービスも
無条件で読込・書込可能

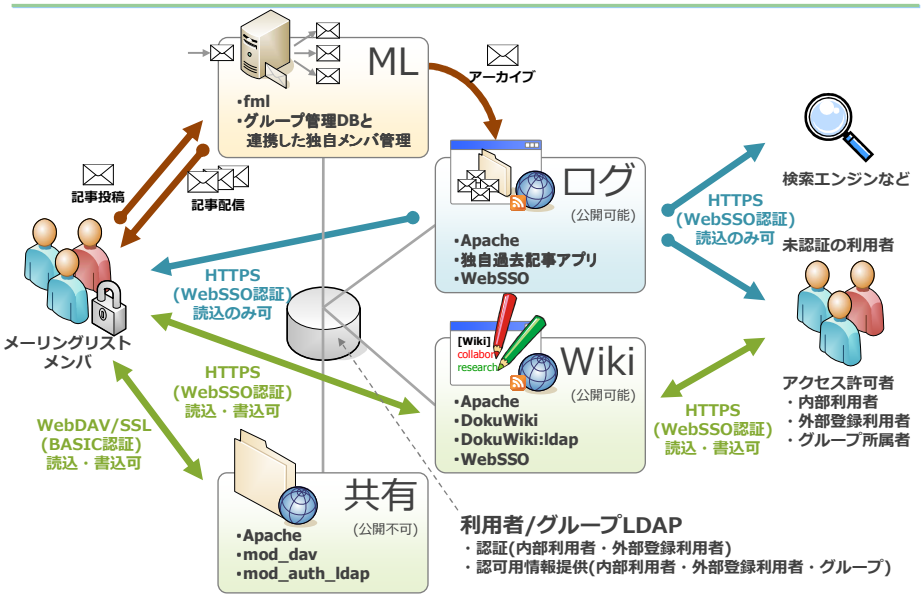
- Webから設定を行えば、どのようなアクセス制限でも可能に
  - 任意の利用者(内部利用者、外部登録利用者)
  - 任意のグループ(ML、プリセットグループ)

次期: 研究データ交換システム

MAFFIN Anytime anywhere, Collaborative Research Environment



次期: メーリングリストシステム



アクセス制限設定用インタフェース

- **Wiki、共有フォルダ、メーリングリスト過去記事アーカイブで、ほぼ同じ体裁のアクセス制限設定用インタフェースを用意**
  - このインタフェース以外からのアクセス制限設定は行えない

公開申請が承認されると、この「無効」が無くなる

アクセス許可する利用者・グループの設定

	フォルダ名	対象		権限	削除
	*	グループID	ml-1&配送者	読込	削除
	*	グループID	ml-1&投稿者	書込	削除
無効	*	any（誰でも）		読込	削除
	secret/*	ユーザID	user1	書込	削除
	secret/*	ユーザID	ex2@example.com	書込	削除
	secret/*	any（誰でも）		権限なし	削除
	ml-2/*	グループID	ml-2	書込	削除
	*	ユーザID		読込	追加

設定変更

- **組織の管理者による簡易公開制限が可能に**
  - 次期システムでの「公開」は、「不特定多数への閲覧権限付与」(未認証の利用者への閲覧許可)という意味
  - 上記以外は、「公開」ではないものとする
    - 人数の問題ではなく、認証の問題
    - 10,000人規模のグループへの閲覧権限付与は「公開」ではない

今後の課題

認証連携時代に向けて

OpenIDへの対応

- **OpenIDとは**
  - 簡易なWebSSO方式、URIがIDとなる
    - 世界的にIdP数が増加している
- **対応**
  - WebSSO機能にOpenIDのService Provider機能を組み込む
    - WebSSOに対応する全てのシステムがOpenID対応となる
- **実現できること**
  - MAFFINの情報共有サービス上でOpenIDをそのままIDとして利用するのは少し困難
  - パスワードをMAFFIN側に預けなくても良くなる効果はある
    - 外部登録利用者のパスワード管理の補助程度の効果
    - メールアドレスはOpenIDの属性情報から取得できるが、基本的に信頼できないため、メールアドレスの実在確認を行う必要がある
    - MAFFIN側ではOpenIDとメールアドレスの対応情報を保存

Shibboleth への対応

MAFFIN Anytime anywhere, Collaborative Research Environment

Shibbolethとは

- 組織間のID連携(フェデレーション)の一手段、SAMLベース
- 欧米の学術機関で実績あり、日本ではUPKI Initiativeで実験中

対応

- WebSSO機能にShibbolethのService Provider機能を組み込む

実現できること

- 属性情報として取得できるメールアドレス情報を信頼すると……
  - 得られたメールアドレスをMAFFIN認証のIDに設定することで、外部登録利用者と同様に取り扱える
  - ➔利用者登録作業が不要に

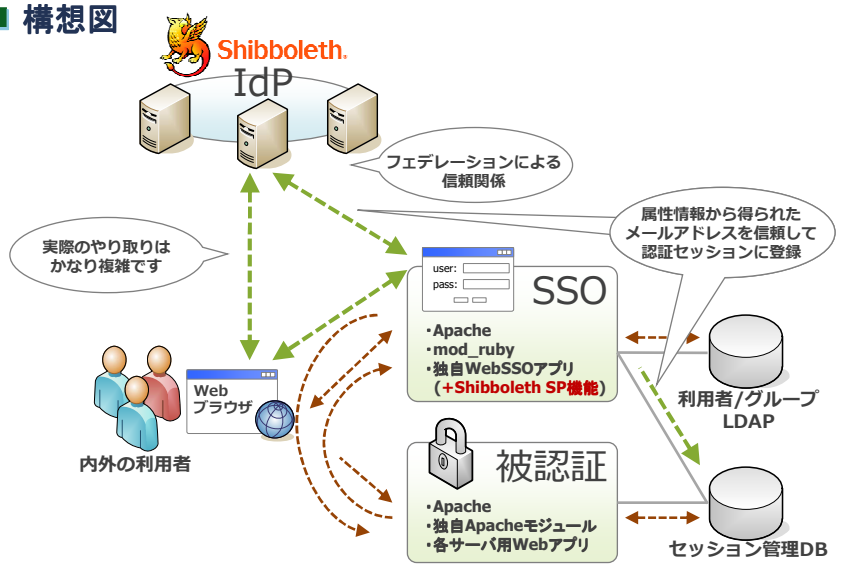
かなりイレギュラーな使い方ですが……

- もし学術系のフェデレーションに参加できれば……
  - この情報共有サービスのメインターゲットである学術系の利用者と、より手軽に情報共有を行うことが可能に
  - 組織間のID連携が実現した場合でも小回りの効くグループは有用

Shibboleth への対応

MAFFIN Anytime anywhere, Collaborative Research Environment

構想図



まとめ

まとめ

- **利用者の所属組織の内部・外部を問わない、非常に柔軟な情報共有サービスを構築した(2009.3稼働予定)**
  - メールアドレスをIDとする「外部登録利用者」という区分を設け、ほぼ誰でも認証できる環境を整備した
  - 既存のメーリングリスト資産を活用することにより、内部組織・外部組織の利用者を含む農林水産系の研究者グループをLDAP上に表現することができた(認証・認可バックエンドの構築)
  - メーリングリストメンバの権限情報を活用することにより、自然な形でグループ向けの情報共有サービスを拡充できた
  - 今後は認証連携への対応を検討している
- **農林水産系の研究情報交換が活発になることを祈念します**