多目的･多階層ユーザーが共存する環境下でのセキュアでシームレスなネットワークの構築

～全国共同利用施設化に伴うネットワークのスムーズな移行～

大阪大学　レーザーエネルギー学研究センター

谷口　麻梨香、 福田　優子、 長友英夫

レーザーエネルギー学研究センター（ILE）の紹介

レーザーエネルギー学研究センター（ILE：Institute of Laser Engineering）は、高強度レーザーを用いたレーザー核融合をはじめ、「高エネルギー密度状態の科学を」開拓するとともに、最先端のレーザー技術により半導体製造技術などの先端産業の発展に貢献する多様な研究を行っています。

2006年4月より、全国共同利用施設となりました。

高性能計算機室の役割

レーザー核融合研究にはスーパーコンピュータを用いたシミュレーションが重要な役割をになっています。
高性能計算機室では、爆縮シミュレーションとそのデータ解析のための大規模シミュレーションシステム、実験データベースシステムから、メール、WEB、ネットワークシステムまで、多目的・多階層なシステムの構築・管理を行っています。

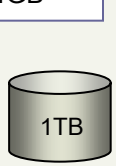
また、ベクトル化や並列化などのプログラミング技法やプログラム開発支援ツール・性能採取方法などについてのテキスト作成し、講習会・個別プログラム相談の実施など、利用者の支援にも力を入れています。

高性能計算機室管理システム

レーザープラズマ実験コンピュータシステム　2005/3～

SX-8/6A

6CPU
98GFLOPS
64GB



1TB

File Server

Laser DATA Server

Daily schedule Server

Experimental DATA Server

Programing Server

Graphic Server

Terminal Client

Login Server

Mail Server

EUVシミュレーション データ蓄積解析システム

4CPU
32GFLOPS
24GB

SX-6

Cybermedia Center
2007/1 ~

SX-8R　SX9

EUVシミュレーションGRID

EUV-GRID Server

データ管理サーバ

FACTDB　Database　Server

ネットワーク管理サーバ

DHCP Server ×2

Authentication Gateway

WEBサーバー

Public wwwServer

ILE wwwServer

collaboration wwwServer

レーザー研ネットワーク（ILE－NET）運用体制

大阪大学

レーザー研ネットワーク運用管理委員会

ILE-NET係 （10名）

・ネットワーク機器の管理　・接続マシンの登録作業
・IPアドレスの管理　　・ネットワーク接続の相談

各居室、実験室

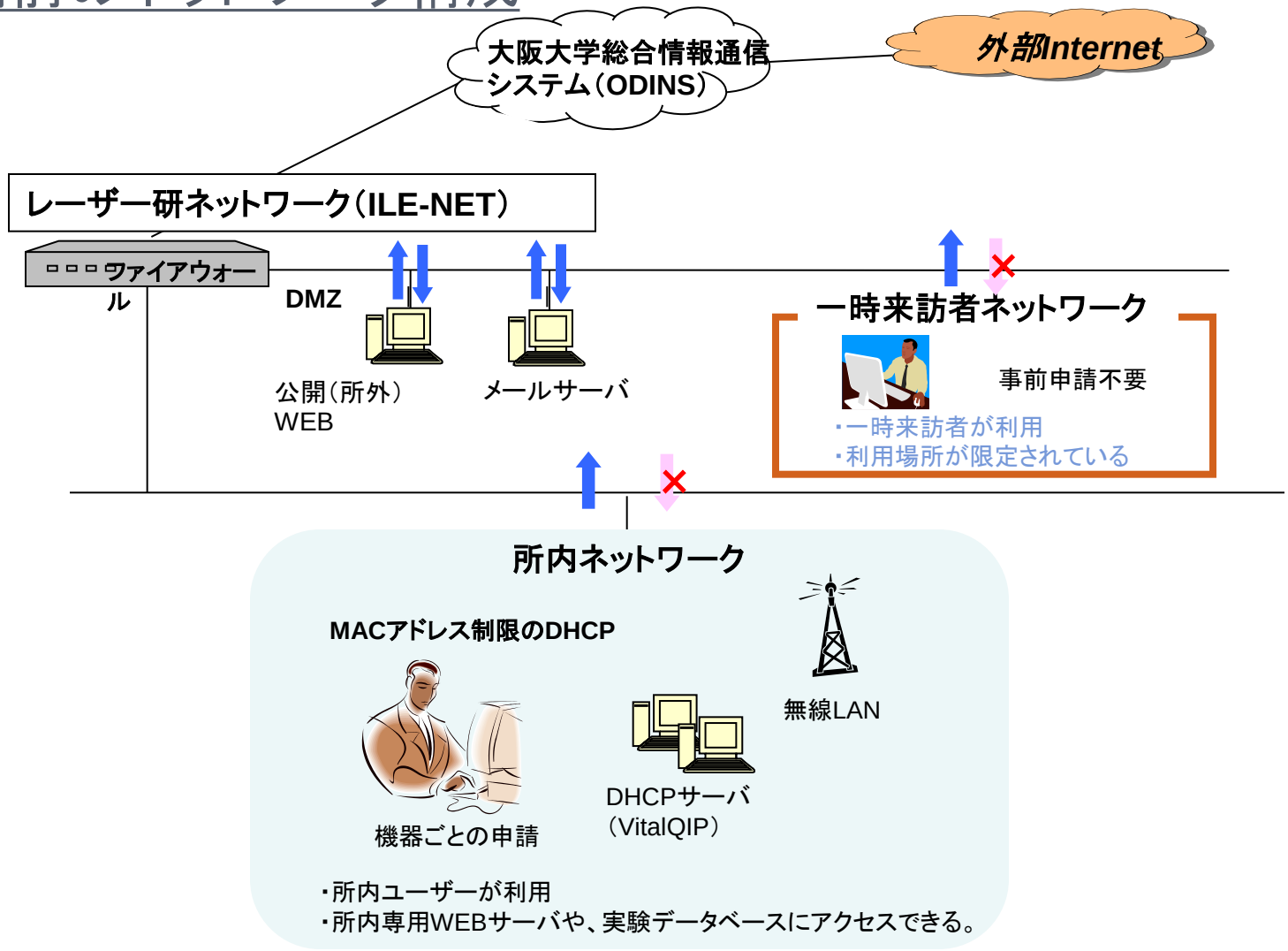
担当者の設置、配線図の提出

ユーザー数：約300名
マシン登録台数：約1000台

■用途に応じた4種類のネットワーク

全国共同利用施設化に伴う要求に応えるために…

整備前のネットワーク構成



全国共同利用施設化に伴う要求事項

- 共同研究者のネットワーク利用
  （実験室や居室でも利用したい。来てすぐ利用したい。）
- 無線でも利用したい。
- 外部の共同研究者とデータのやり取りをしたい。
- 実験計測機器にアクセスしたい。

指定の場所で利用できる一時来訪者ネットワークを整備していたが、使い勝手やセキュリティに問題あり。

- 利用場所を増設するのが困難
- 固定アドレスでの利用
- 使用履歴がファイルに記入するだけ

セキュリティの配慮も必要。

- 大阪大学ネットワーク利用ポリシーの遵守
- レーザー研内部ネットワークへのアクセス制限

無線ネットワークの問題点

会議室でもネットワーク利用したいという要望により、2002年10月に無線アクセスポイントを設置。
また、各グループの無線アクセスポイントが乱立してきていた。

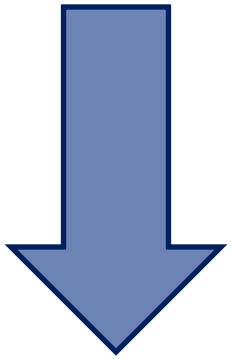
（問題点）

- 無線アクセスポイントが古くなり、トラブルが発生
- MACアドレスを登録する必要があるため各管理者の負担が大きい（サービス拡大が困難）
- 無線アクセスポイント乱立のため、チャネルの干渉

認証ネットワーク導入の検討

2006年5月より、大阪大学全学無線LAN試行が開始され、SSL-VPNを用いた認証でネットワーク利用ができるようになった。

大阪大学のアカウントを持っていれば利用できたが、共同研究者は利用できないため、これを参考にレーザー研の認証ネットーワークを検討。



認証ネットワーク導入を決定

認証ネットワークを導入したら

■認証ネットワークのテストと、今後のネットワーク検討を行う

1. レーザー研ユーザー用の認証ネットワークを構築し、まずはテスト的に運用

2. 共同研究者用の認証ネットワークを構築。
レーザー研内部ネットワークにはアクセスできないが、実験データベースなどにのみアクセスできるように設定。

3. 将来的なネットワーク管理システムを検討
既存DHCPサーバの保守サービス終了のため、今後のネットワーク運用を検討。

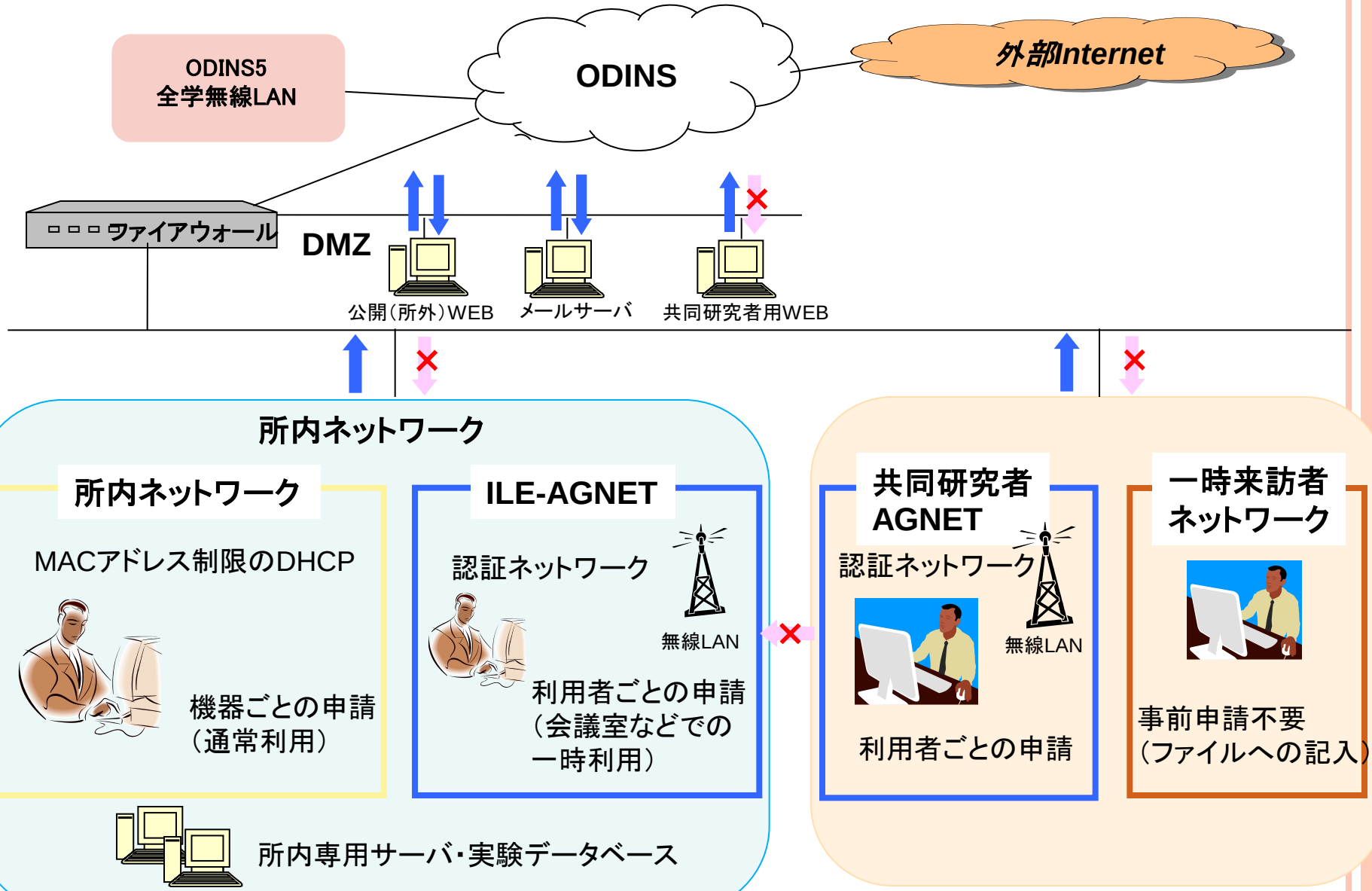
■無線ネットワークの整備が可能になる

無線アクセスポイントは全て認証ネットワークに移行

1. 認証のアカウントを持っていれば、MACアドレスを登録していなくても利用可能。

2. アクセスポイントの共有、整備が容易になる。

用途に応じた4種類のネットワークを検討



所内ネットワークとは

・所内ユーザーのための既存ネットワーク
・MACアドレス制限のDHCPで運用
（機器ごとの申請が必要）
・重要なデータや個人情報データのサーバも接続されている

所内認証ネットワーク（ILE-AGNET）とは

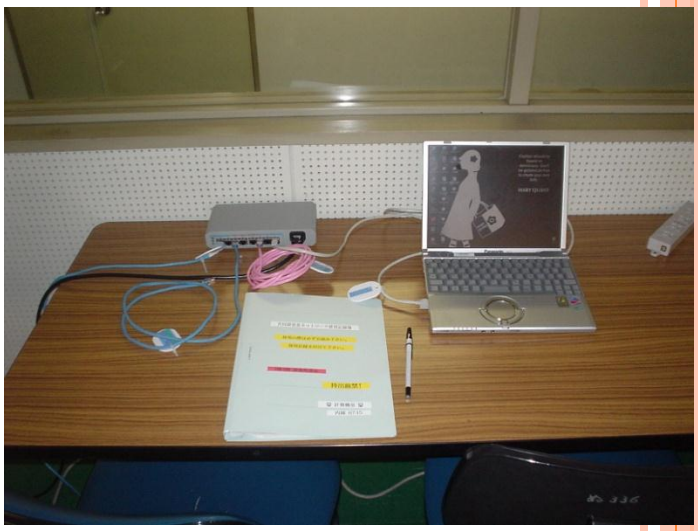
・所内ユーザーのための新ネットワークで、会議室などで一時利用される
・所内ネットワークと同じセキュリティレベルが求められる
・ユーザーごとの認証により利用できる
・無線アクセスポイントは全て移行

共同研究者用認証ネットワークとは

・共同研究者のための新ネットワーク
・ユーザーごとの認証により利用できる（事前申請が必要）
・無線や実験室での利用も可能
・所内ネットワークへのアクセスはできない。

一次来訪者用ネットワークとは

・以前からサービスしており、便利だと好評だったので移行
・事前申請は不要で、使用する際にはファイルへ記録
・限られた場所での利用
・所内ネットワークへのアクセスはできない。



整備の進め方

まずは新セグメントをつくり、認証サーバでILE-AGNETのサービスを開始

↓

共同研究者ネットワーク（認証＆一時利用）の整備

↓

既存ネットワークの整備（新DHCPサーバ導入）

■新セグメントの導入

- 認証ネットワークの導入
- 共同研究者用ネットワークの導入

認証ネットワーク導入検討

認証サーバの選定は下記の方針で行いました。

- ライセンス数が無制限であること
- クライアントソフトウエアが不要であること
- クライアントのOSが限定されないこと
- 利用履歴をログで残せること
- 認証サーバーのOSが、運用し慣れたLinuxで、管理しやすいこと

認証サーバ決定

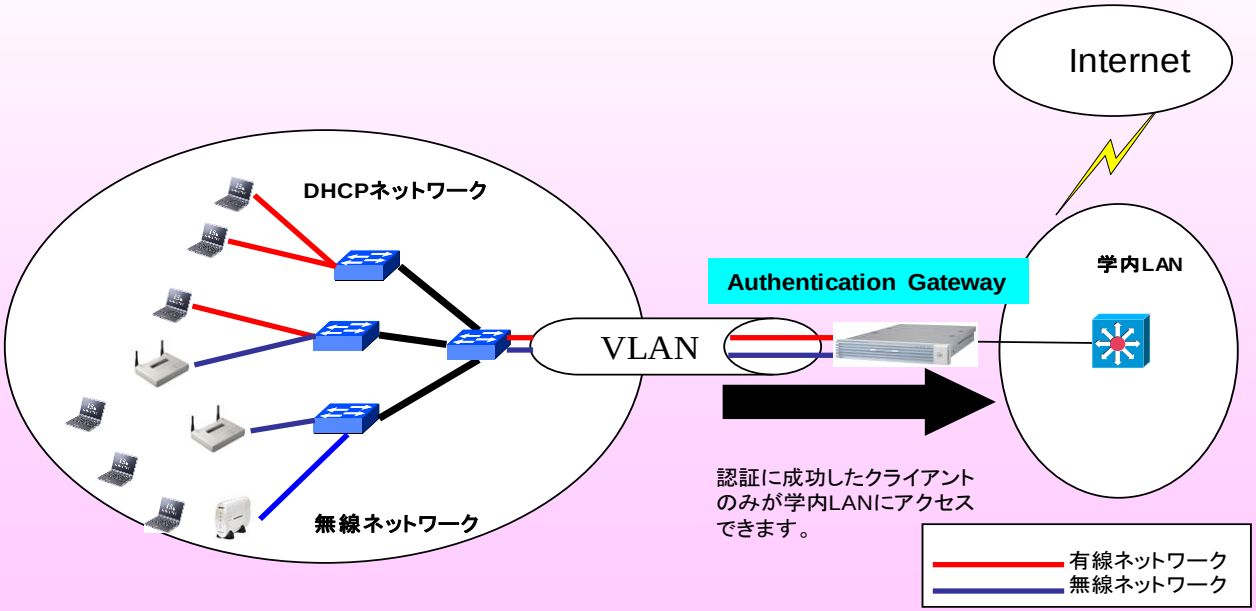
認証サーバは、NECシステムテクノロジー社製のSyntheuniv/AG（導入時はAuthenticationGateway）を導入しました。

ゲートウェイ型認証システム

AuthenticationGateway

AuthenticationGatewayでは、ゲートウェイ型認証VLANを採用しており、認証方式もWebとSSHによる認証に対応しておりますので、
- ユーザ認証（＋利用端末Macアドレス）による利用制限環境の構築
- プラットフォーム（OS/ブラウザ）の制約を軽減
- インフラ（無線LANアクセスポイント/無線LANカード）に依存しないサービス
- 利用端末間の通信制限

を実現します。



認証ネットワークポリシー策定

「新ネットワーク管理システムおよび無線LANの運用方針について」

2007年3月8日　ネットワーク運用管理委員会　決定事項

- 認証サーバへの登録については、ID・パスワードはメールサーバのアカウント、パスワードと同一とするが、申請が必要。学生は教員の責任での利用とする。

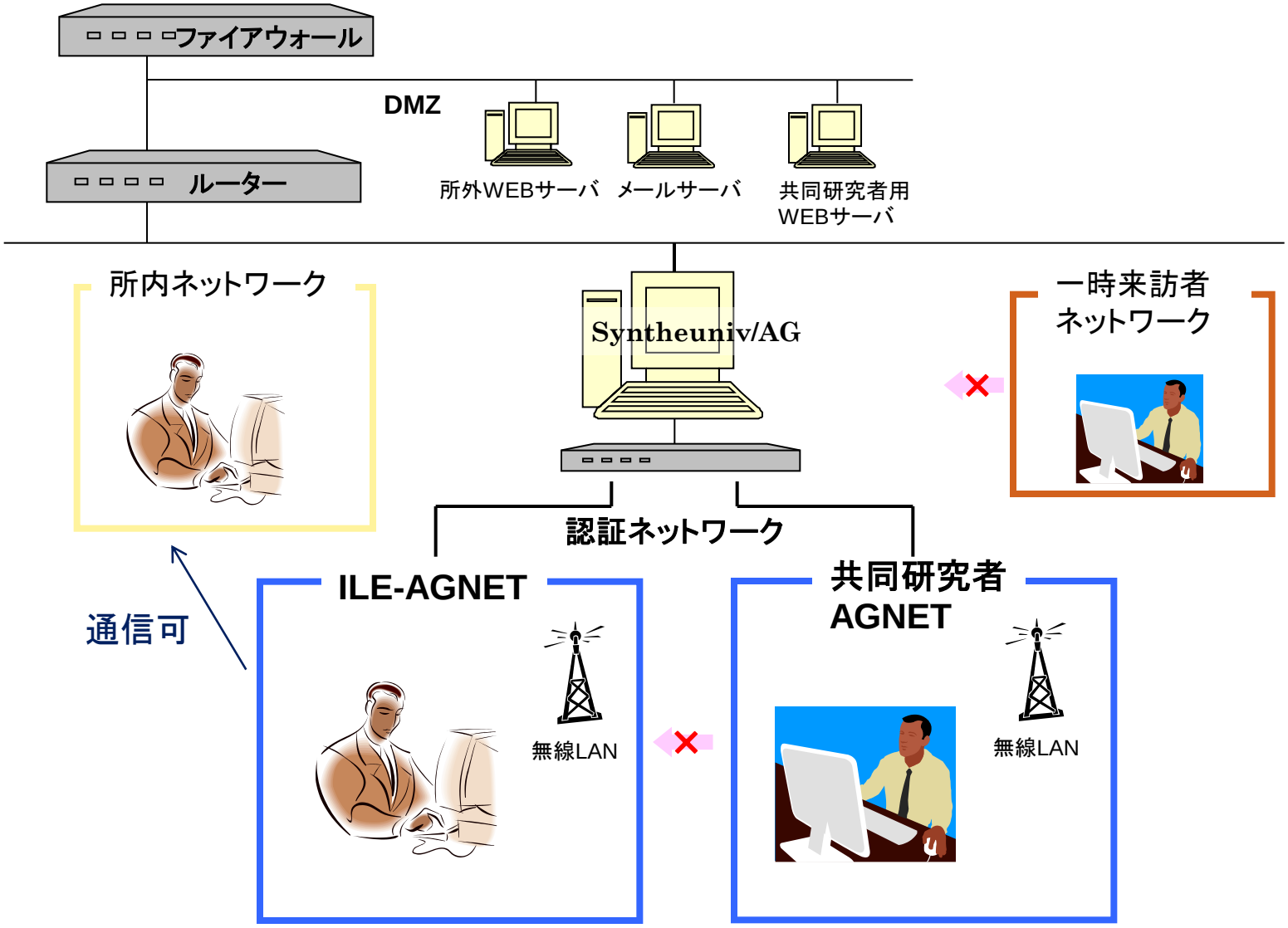
- パスワードレベルについては、現在のメールサーバの標準設定より厳格なもの（全学統一アカウントレベル）とし、パスワードが変更されなければ認証ネットワークに登録しないこととする。

- 共同研究者用ネットワークについてはILEユーザー用認証ネットワークとは別のネットワークとしてサービスする。ユーザーのグループによってレーザー研内部への通信を制限する機能が実装される2007年6月以降にサービス開始とする。

- ILENET管理の無線アクセスポイントは認証ネットワークに移行し、運用原則はよりセキュアになるように変更する。

- 個人無線アクセスポイントは廃止とする。
  ILENET管理のアクセスポイントの電波が届かない場合は、新認証ネットワークに接続する場所に限り許可する。

認証ネットワーク構成


ファイアウォール
DMZ
ルーター
所外WEBサーバ
メールサーバ
共同研究者用
WEBサーバ
所内ネットワーク
Syntheuniv/AG
一時来訪者
ネットワーク
認証ネットワーク
通信可
ILE-AGNET
無線LAN
共同研究者
AGNET
無線LAN

ILE-AGNET運用開始準備

- メールのパスワード変更レベルを厳格にする
- 申請があり、メールのパスワードを変更したユーザーのアカウントとパスワードを認証サーバーに持っていく自動ツールを作成
- 認証サーバの運用管理ツールを作成し、監視やセーブなどの運用定型作業準備
- 認証ネットワークセグメントを、各ネットワークスイッチに設定
- 無線アクセスポイントの設定と設置。　（既存のアクセスポイント移行も。現在、ILENET管理は7台、その他27台）
- 利用者ガイドライン、無線LAN利用要項を改定
- 利用方法のテキストやwebページを作成
- 申請書を作成・申請手順を決定（学生用）
- Webページ、メールなどによるアナウンス

2007年５月　ILE-AGNET運用開始

ILE-AGNET利用の流れ

1. **ILE-AGNETに接続します（無線、または有線）**
   マシンのネットワーク設定はDHCP
   （ほとんどのマシンが普段の設定のまま利用できます）

2. **IPアドレスが自動的に割り振られます　（※1）**
   （この時点で、ILE-AGNET内のみの通信は可能ですが、
   ILE-AGNET外には通信できません）

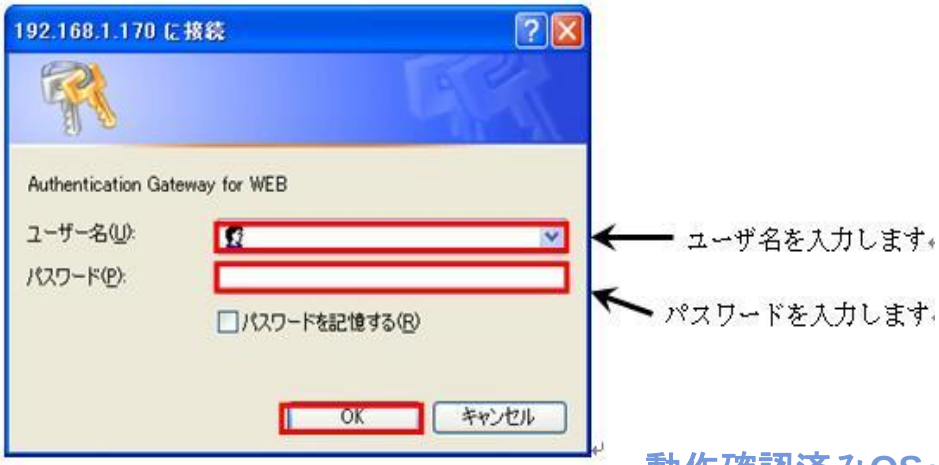
3. **認証作業　（二通りの方法があります）**
   ・webブラウザより認証を行う
   ・sshで認証を行う

4. ILE-AGNET外への通信が可能になり、メール、webなどができるようになります。

(※1)認証前でもILE-AGNET内の通信は可能であるため、必ず各自の責任でウイルス対策ソフトやパーソナルファイアウォールを導入のうえ、利用して下さいとアナウンスしています。

認証画面イメージ

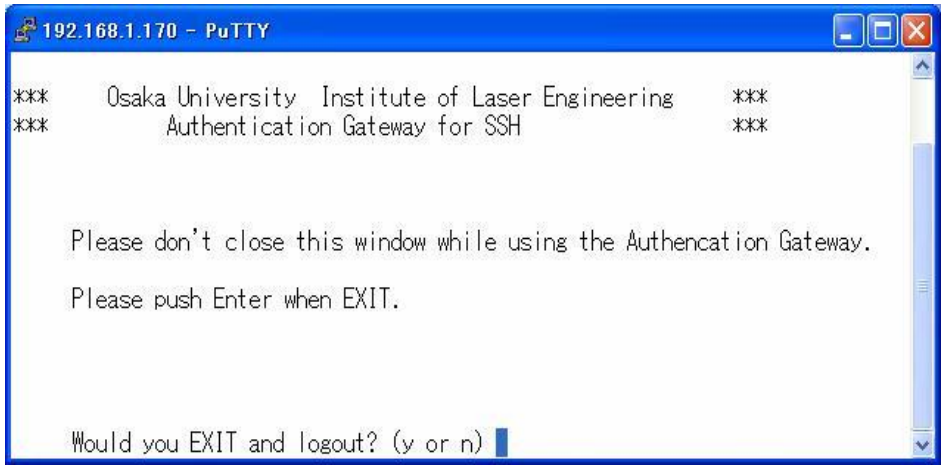
Web認証



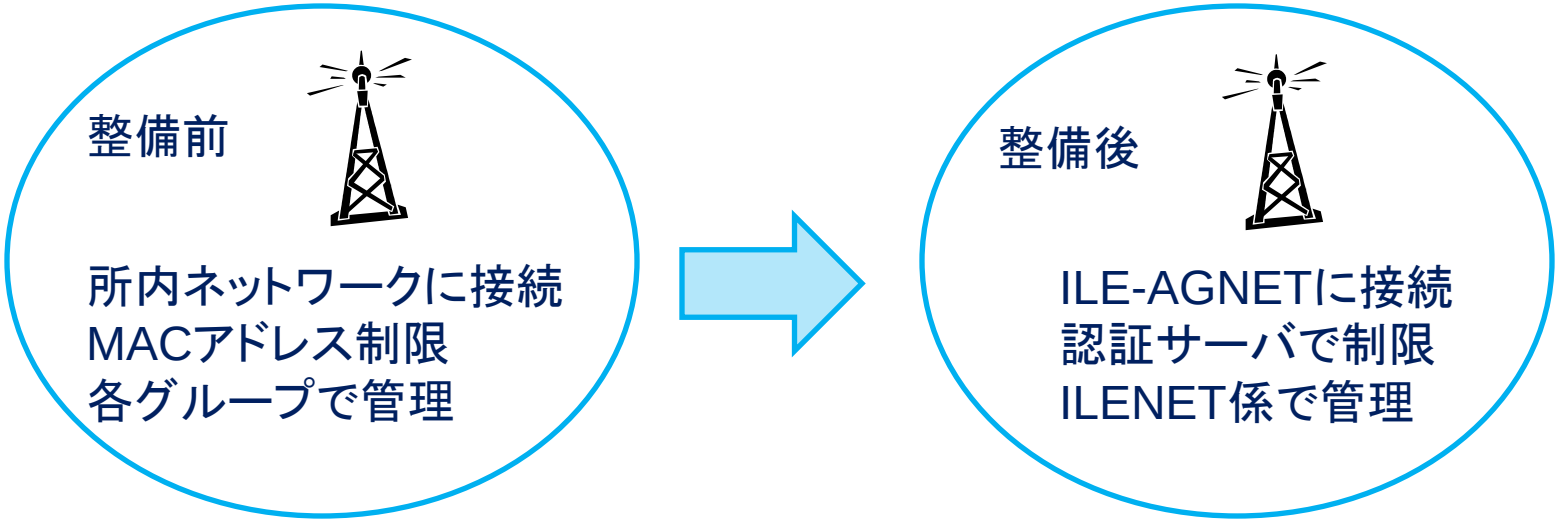
↑図は Internet Explorler の場合です。

動作確認済みOS:
Windows用→IE7、IE6.0、Firefox2.0、Netscape7.1、Opera9.10
Mac OS用➔Opera9.10、Saffari 1.3.2(ver312.6)、Firefox2.0

SSH認証



無線ネットワークの整備



導入効果

・無線アクセスポイントの乱立を防ぐことができた。
（11ケ所のうち、7ヶ所を廃止）

・無線アクセスポイントの増設・代替機への交換が容易になった。
（新たに、会議室に設置した。代替機は設定をしておけば、
おきかえるだけでよい。）

・全ての無線アクセスポイントが利用できるようになった。
（認証サーバのアカウントを持っていれば、どこでも利用できる）

ILE-AGNET運用開始後の状況

運用開始にあたって、利用説明会やwebなどでのアナウンスを行ったが、OSやwebブラウザによっての動作の違いにより、接続できないと相談に来るユーザーが多かった。

■WEB認証　-- ブラウザ対応、ポップアップブロック --

WEB認証のためには、ポップアップブロックを解除する必要があるが、ブラウザでのポップアップブロックのみでなく、YahooやGoogleツールバーでもブロックされているユーザーもいた。使えないと相談に来たユーザーの原因ではこれが一番多かった。

■SSH認証

WEB認証ができない場合は、SSH認証で対応してもらった。しかし、MacOSXでは標準でターミナルが利用できるが、WindowsではSSHソフトをインストールする必要があるため、普段SSHを利用していないユーザーには少し難しかったようだ。

■WEB認証　-- お気に入りに登録できない --

認証サーバ認証画面のURLは、お気に入りに登録できなかったため、煩雑だという声もあった。このため、別のhtmlファイルを認証サーバに作成し、認証画面URLへのリンクをはった。
これは、2008年3月のバージョンアップで、webブラウザを起動すると自動的に認証画面が表示されるようになった。

ILE-AGNET導入効果

- ユーザー認証では、一度申請すれば、新しいマシンを接続する場合、MACアドレス登録前でもネットワーク利用ができるため、ユーザーにも管理者にも負担軽減効果があった
- インシデント発生時にユーザーの特定が容易になった
- 無線LANの一元管理ができるようになった

- 認証前でも、ILE-AGNET内での通信は可能であるため、所内ネットワークよりのセキュリティレベルが低い
- 認証サーバは二重化などされていないため、トラブル時には認証ネットワークは全く利用できなくなる
- アカウントとパスワードの厳重な管理が必要

共同研究者用ネットワーク整備

従来の、一時来訪者用ネットワークは

・事前申請不要で利用できるため、非常に好評だった
・固定アドレスの設定を間違えると重大なトラブルを起こしかねなかった
・利用履歴がファイルの記入のみのため、インシデント時のユーザー特定が不確かだった
・利用場所の増設が困難であった

⇩

二種類のネットワークを準備

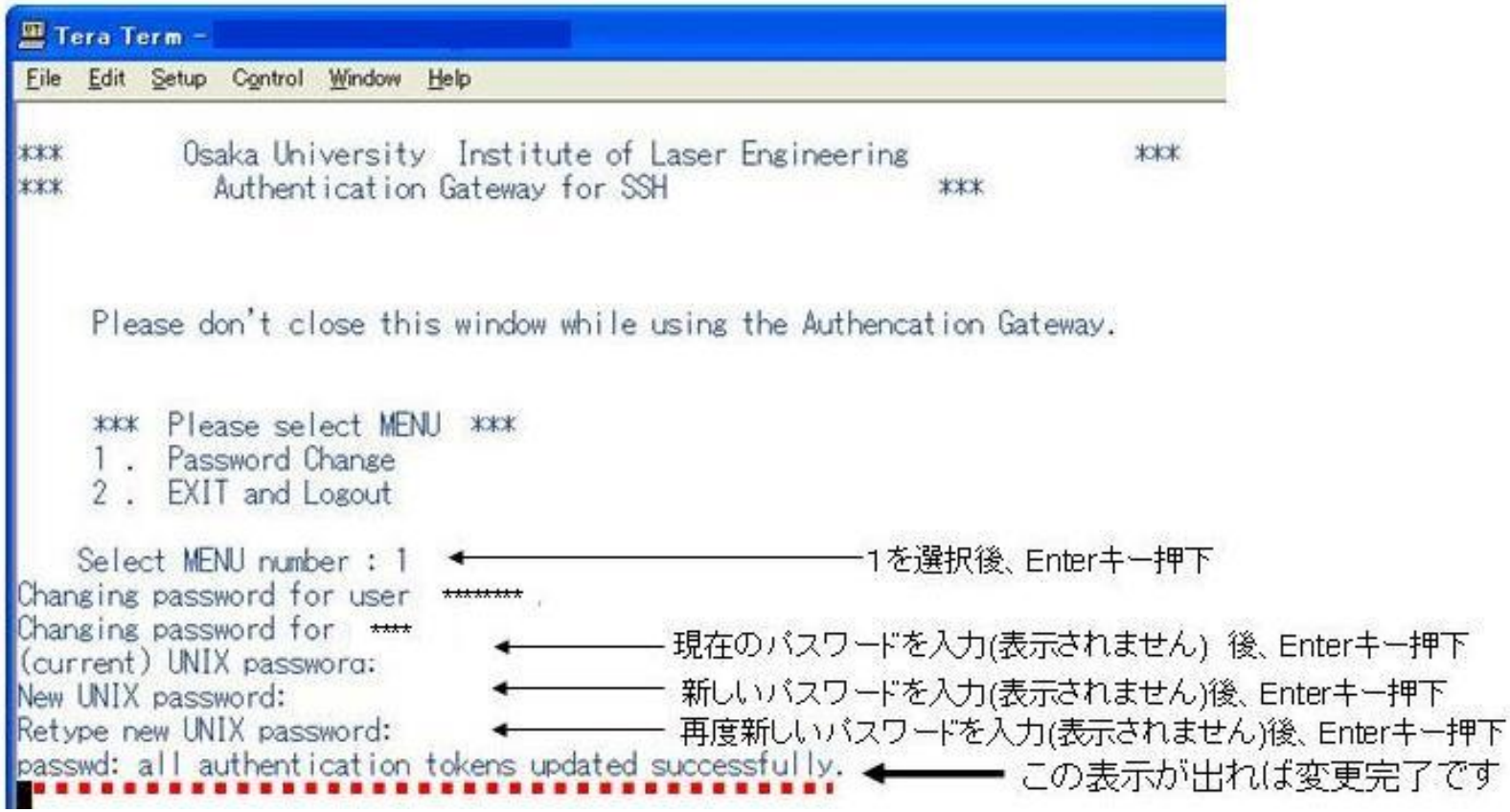
共同研究者AGNET（認証ネットワーク）	**一時来訪者用ネットワーク**
外部、及びDMZにアクセスできる。レーザー研内ネットワークにはアクセスできない。	
事前申請が必要（アカウントが必要）	申請不要（使用時にファイルへの記入が必要）
利用場所が多い	利用場所が限られている
実験スケジュールwebにアクセスできる	実験スケジュールwebにアクセスできない
利用には認証は必要	利用時にネットワーク設定変更が必要

共同研究者AGNET運用開始準備

ILE-AGNETと異なる点

- 共同研究者のアカウントには、最大で年度末までの有効期限をつけることとした。
- 共同研究者のみ、SSH認証の際にパスワード変更のメニューが表示されるようにした。
- 共同研究者アカウント申請方法の検討
- 共同研究者用のWEBサーバ運用開始

共同研究者AGNET　パスワード変更画面



共同研究者AGNET申請方法

◇来所前に申請する場合（一週間前までにご提出下さい）

共同研究者

申請書

サイン:

受け入れ担当者サイン:

内容を確認の上、必要事項を記入して下さい。
（※直筆サインの欄は空白）

メール、郵送などで、
受け入れ担当者に提出

受け入れ担当者

申請書

サイン:

受け入れ担当者サイン: ●●●●●

内容を確認の上、
直筆サインをして下さい。

CMPに提出

CMP

申請書

サイン:

受け入れ担当者サイン: ●●●●●

登録作業を行い、アカウントを
発行します

アカウントと申請書を
企画室に置いておきます

企画室担当秘書

来所時に、企画室にお越し下さい。
アカウントをお渡しいたします。
またその際、申請書のサイン欄に直筆サインをして下さい。

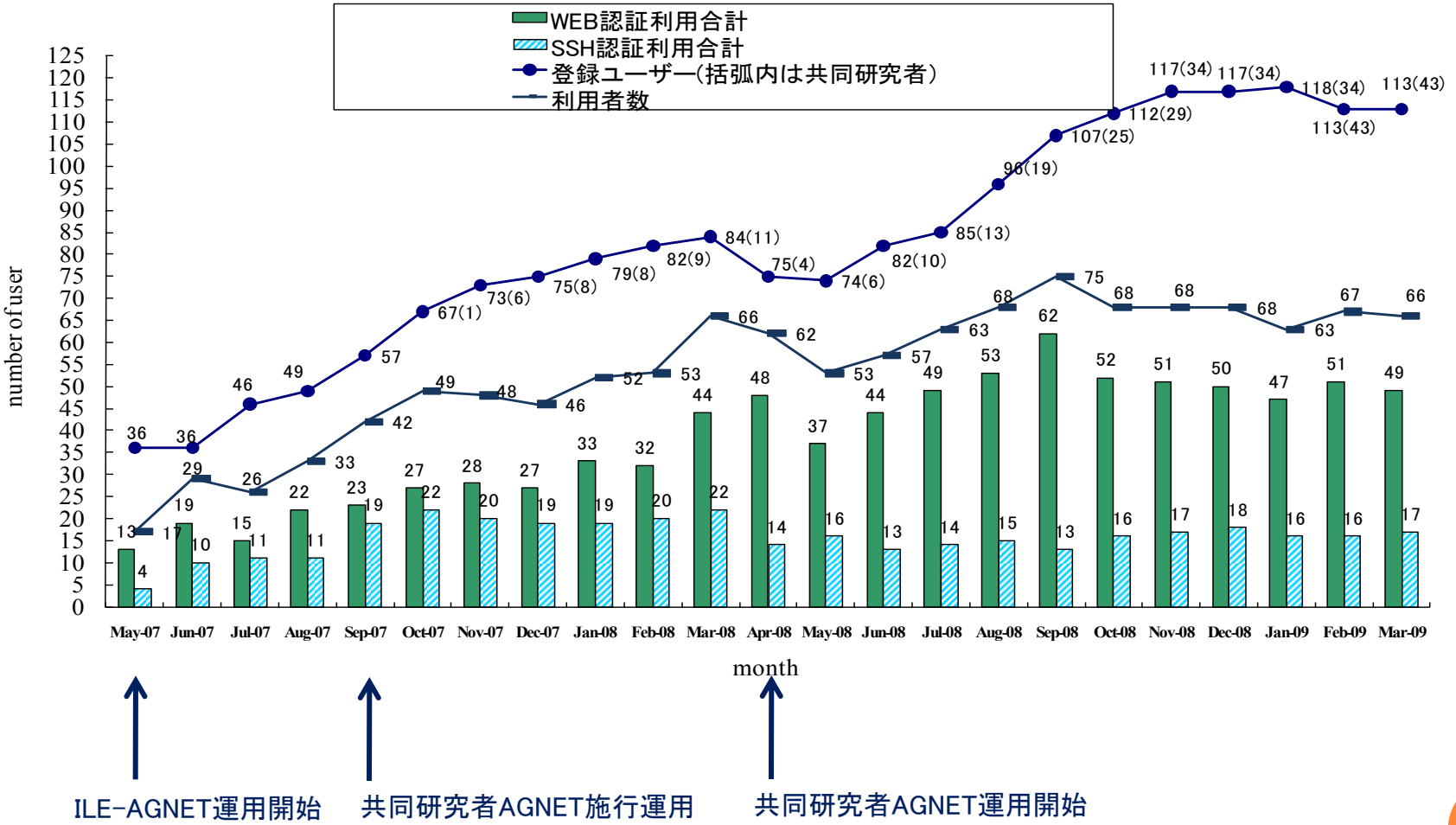
アカウント

申請書

サイン: ●●●●●

受け入れ担当者サイン: ●●●●●

認証ネットワーク利用者数の推移



共同研究者AGNET導入効果と問題点

- ILE-AGNETを先行して運用していたため、ノウハウも溜まっており、運用開始もしやすく、また、既に使っているレーザー研メンバーが各自、共同研究者の認証ネットワーク利用サポートをしてくれた
- ネットワーク利用の要望がある場所で利用できるようになった（利用可能場所が増えた）
- 無線LANでも利用できるように整備した
- 利用ログが確実に採取できるようになった

- 認証前でも、共同研究者AGNET内での通信は可能であるため、各マシンでのセキュリティ対策が必要
- 認証サーバは二重化などされていないため、トラブル時には認証ネットワークは全く利用できなくなる
- 認証サーバがILE-AGNETと同じものなので、ILE-AGNETに接続した場合でも認証され、利用できる。

■既存ネットワークの移行

・新DHCPサーバ運用開始

・IPアドレス大変更

新DHCPサーバ導入検討

既存DHCPサーバの機能で必要なもの

・MACアドレス制限によるDHCP払い出し
・フェイルオーバー機能
・利用ログを検索し、マシンを特定

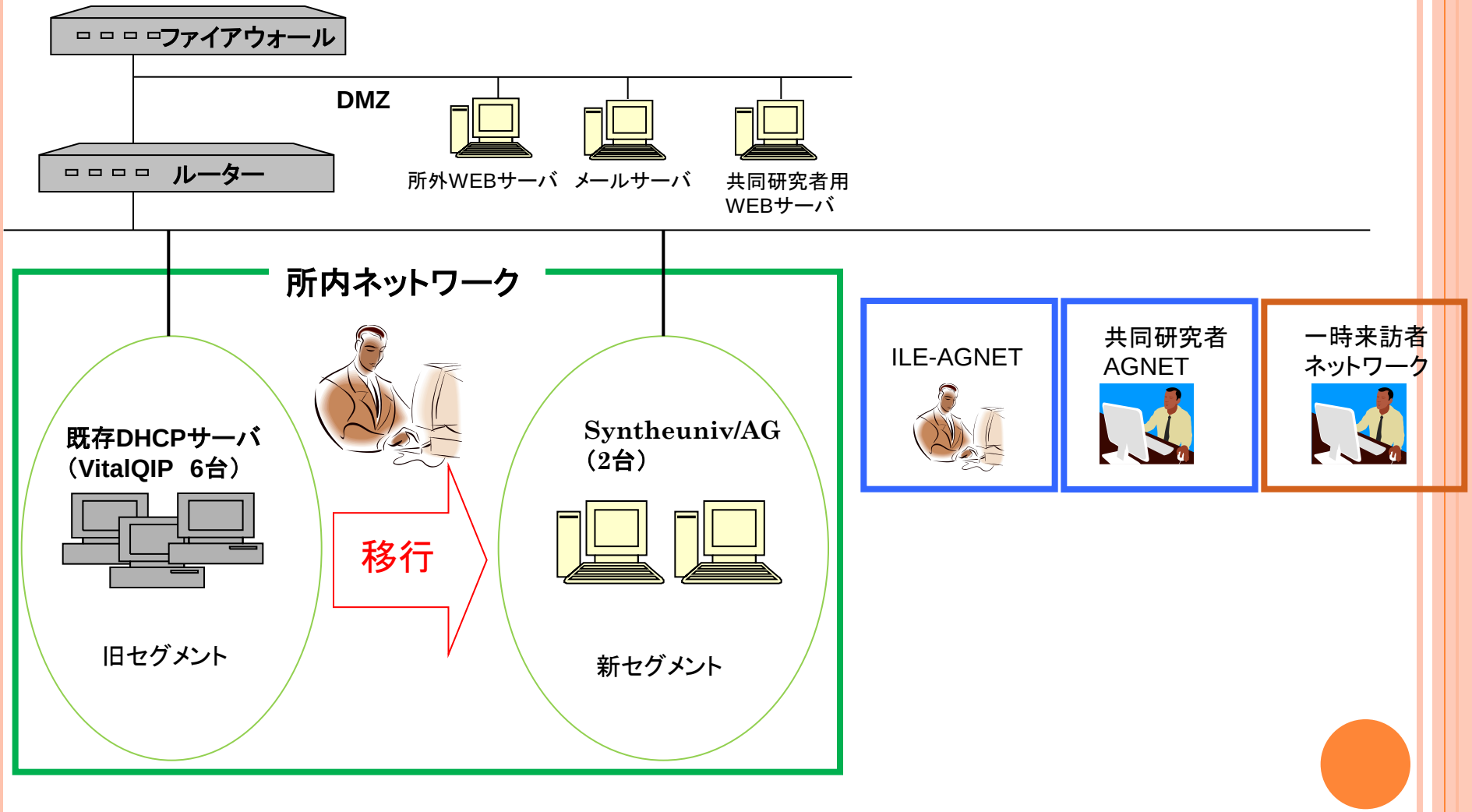
Syntheuniv/AGの機能（2007年5月～　認証ネットワークで運用中）

・MACアドレス制限によるDHCP払い出しが可能
・2台のサーバーがあれば、フェイルオーバー可能
・DHCPログより、マシンの特定が可能

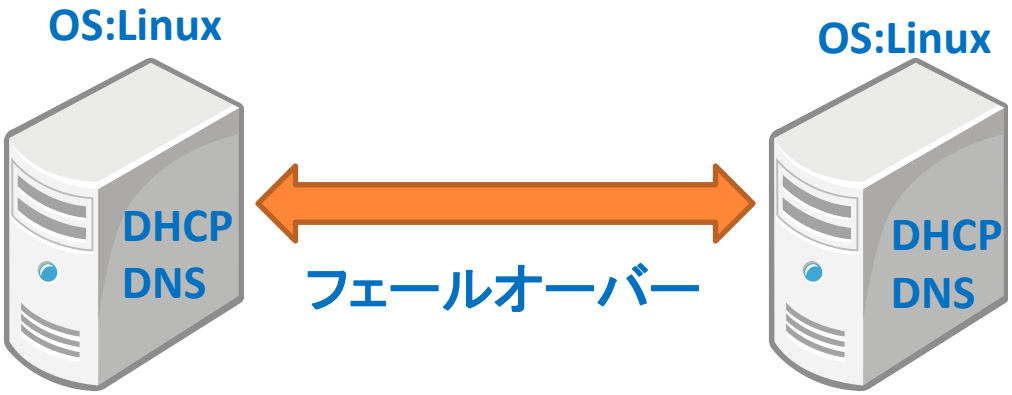
その他の背景

- 全てのネットワークを認証ネットワークにしてしまうのは、レーザー研の利用者には負担が大きすぎる（ブラウザが対応やポップアップブあロック問題、毎回認証するのが面倒など）
- 既存ネットワークの運用を継続したままの移行が可能
- PC検疫や、スイッチとの連携による申請外ホストの通信遮断までの機能までは不要
- サーバOSがLinuxであるため、扱いやすい

新DHCPサーバへの移行



新DHCPサーバ導入効果

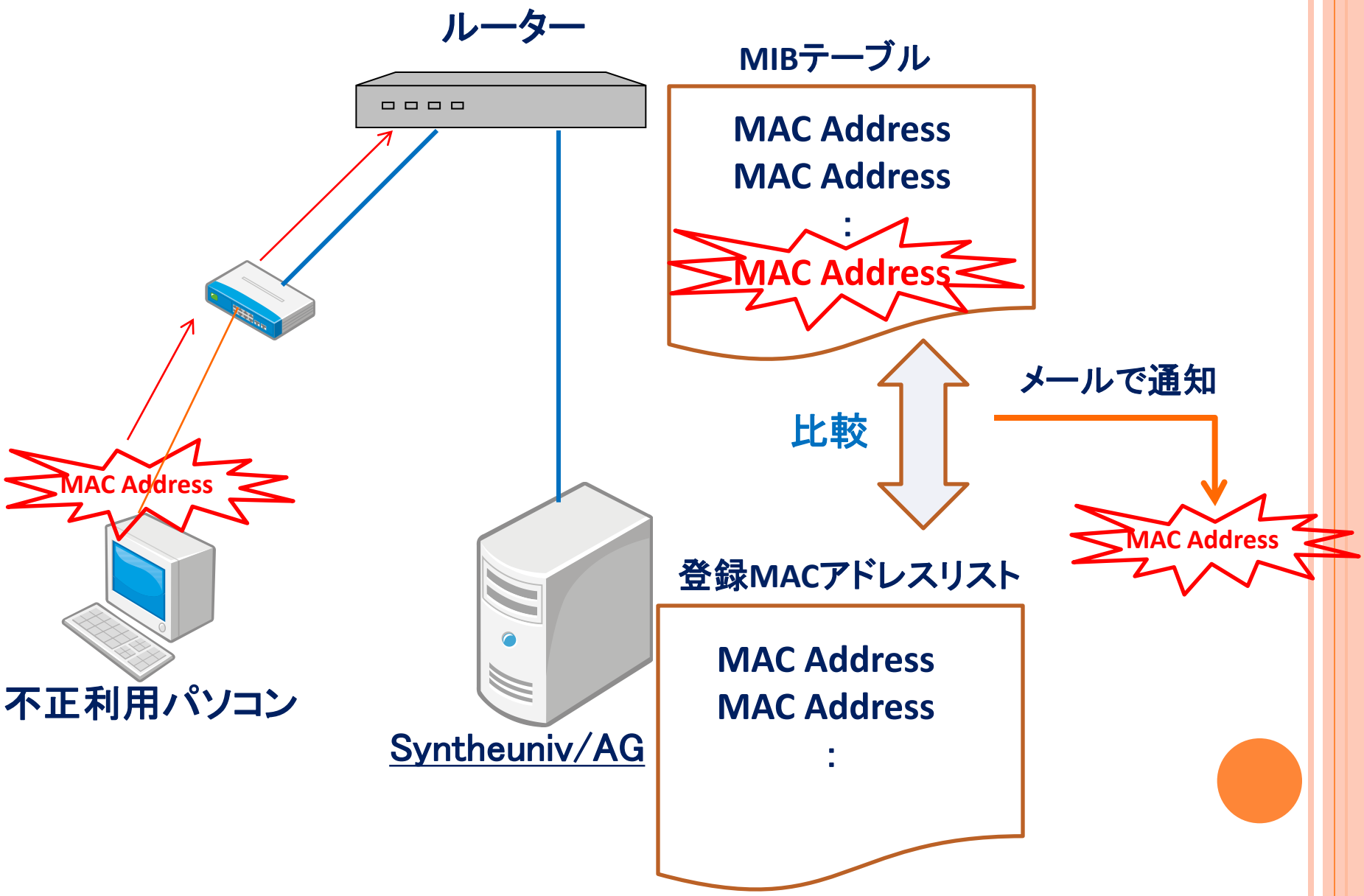


1. **不正利用MACアドレスの自動検知が可能に。**
   申請されていないMACアドレスで接続すると、検知メールが自動的に送信されるため、不正使用を見つけることができるようになった。

2. **OSがLinuxのため、ログ採取などの運用管理ツールの作成が容易に。**
   サーバー状態監視ツールだけでなく、DHCPのログ採取やIPアドレス払い出し数採取、エラーログ検知などのツールを作成し、運用している。

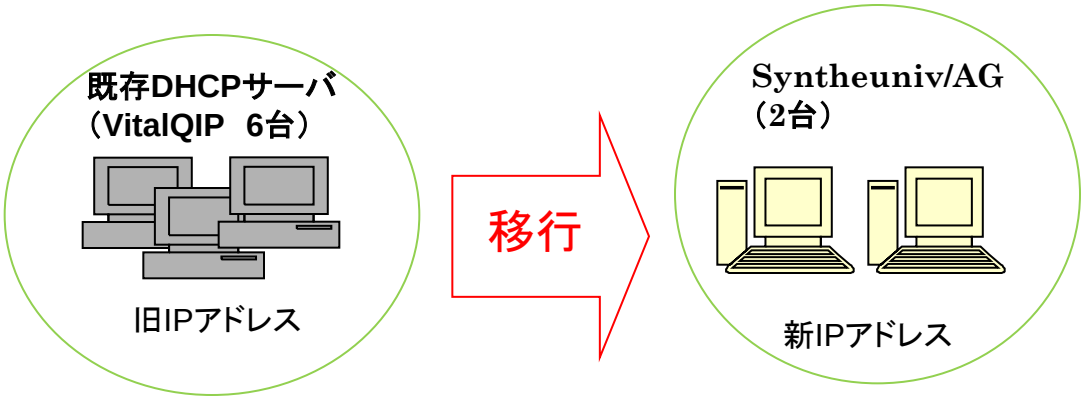
3. **CUI作業により、登録手順が簡易に。**
   以前のサーバはWindowsでGUIでの手作業が必要だったが、ツールを作成し、CUI作業が増えたため、ツールを作成し、自動化できた。

不正MACアドレス検知機能



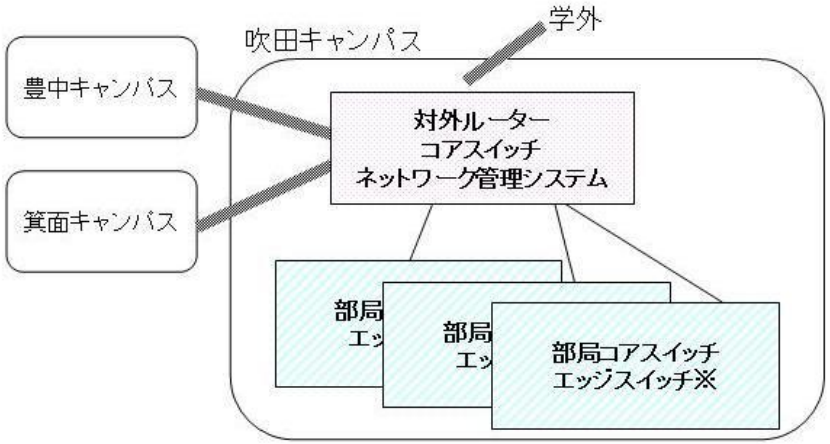
IPアドレス大変更

ODINS5導入に合わせて、長年の課題であったIPアドレス返却のため、
所内ネットワークのIPアドレスを全て変更することを決定



ODINS5とは・・

大阪大学総合情報通信システム、2008年4月より運用開始



ユーザーへのアナウンス

～～　IPアドレスが変更します！！　～～

- **固定アドレスのパソコンの設定変更をして下さい**

サーバーやネットワークHDなど、固定アドレスのパソコンはもちろん設定変更が必要です。
また、サーバーのファイアウォールなどで、IPアドレスでのアクセス制限の設定をしている場合、この設定変更も必要です。

- **プリンタの設定変更をして下さい**

プリンタの固定アドレス変更が必要です。滅多にしないと思いますので、今のうちに説明書などを探して、変更方法を確認しておきましょう。

- **各パソコンのプリンタ設定の変更をして下さい**

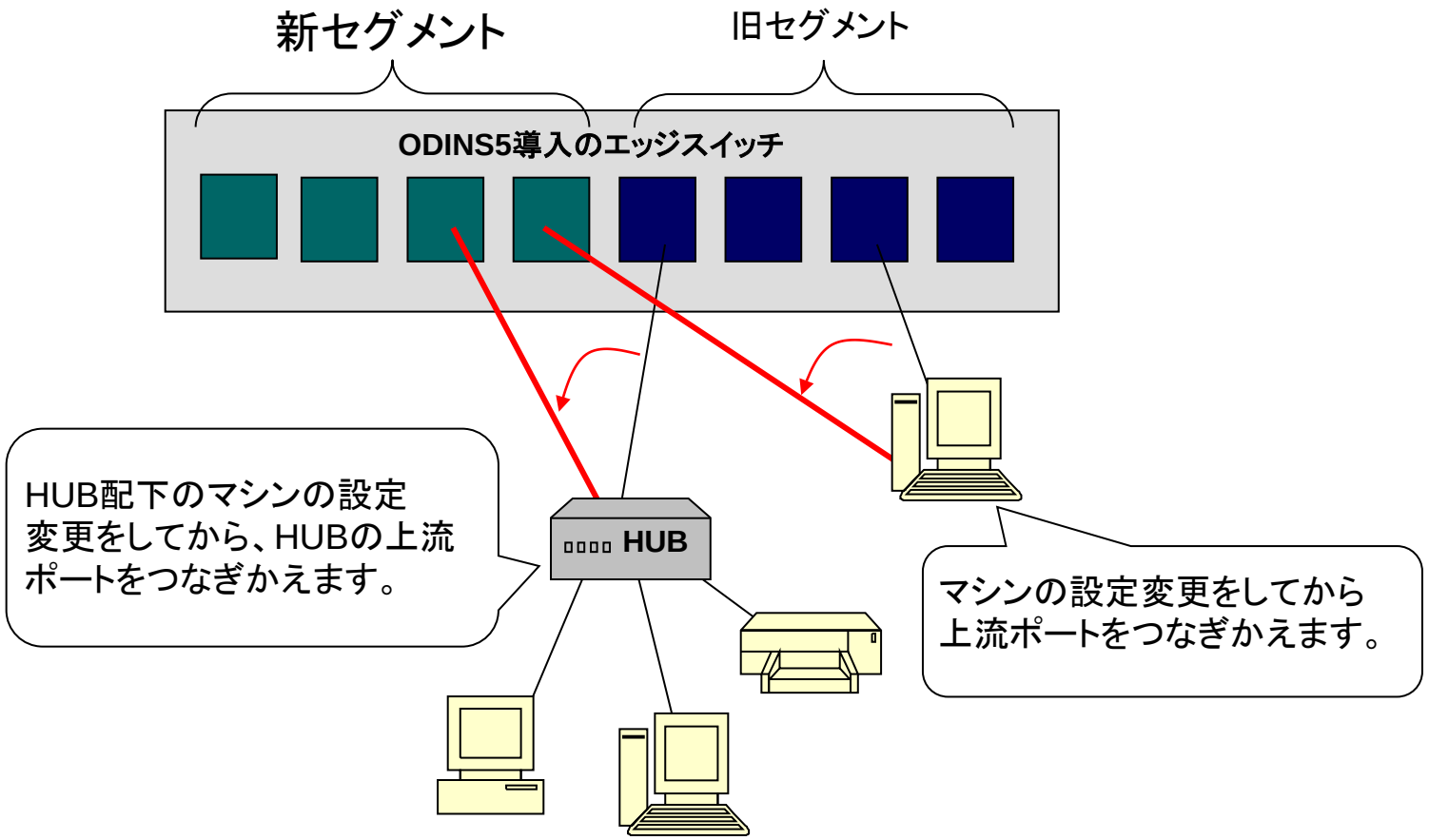
プリンタのアドレスを変更したので、パソコンのプリンタ設定も変更しなければいけません。
そのプリンタを使っている全パソコンが対象です。

- **DHCPで利用しているパソコンはネットワークの設定変更は必要ありません。**

ただし、上記のプリンタ設定の変更などは必要です。

- **配線状況によっては、部屋のマシンを一斉に変更する必要があります。**

ネットワーク移行手順


新セグメント
旧セグメント
ODINS5導入のエッジスイッチ
HUB
HUB配下のマシンの設定
変更をしてから、HUBの上流
ポートをつなぎかえます。
マシンの設定変更をしてから
上流ポートをつなぎかえます。

IPアドレス変更をしてみて

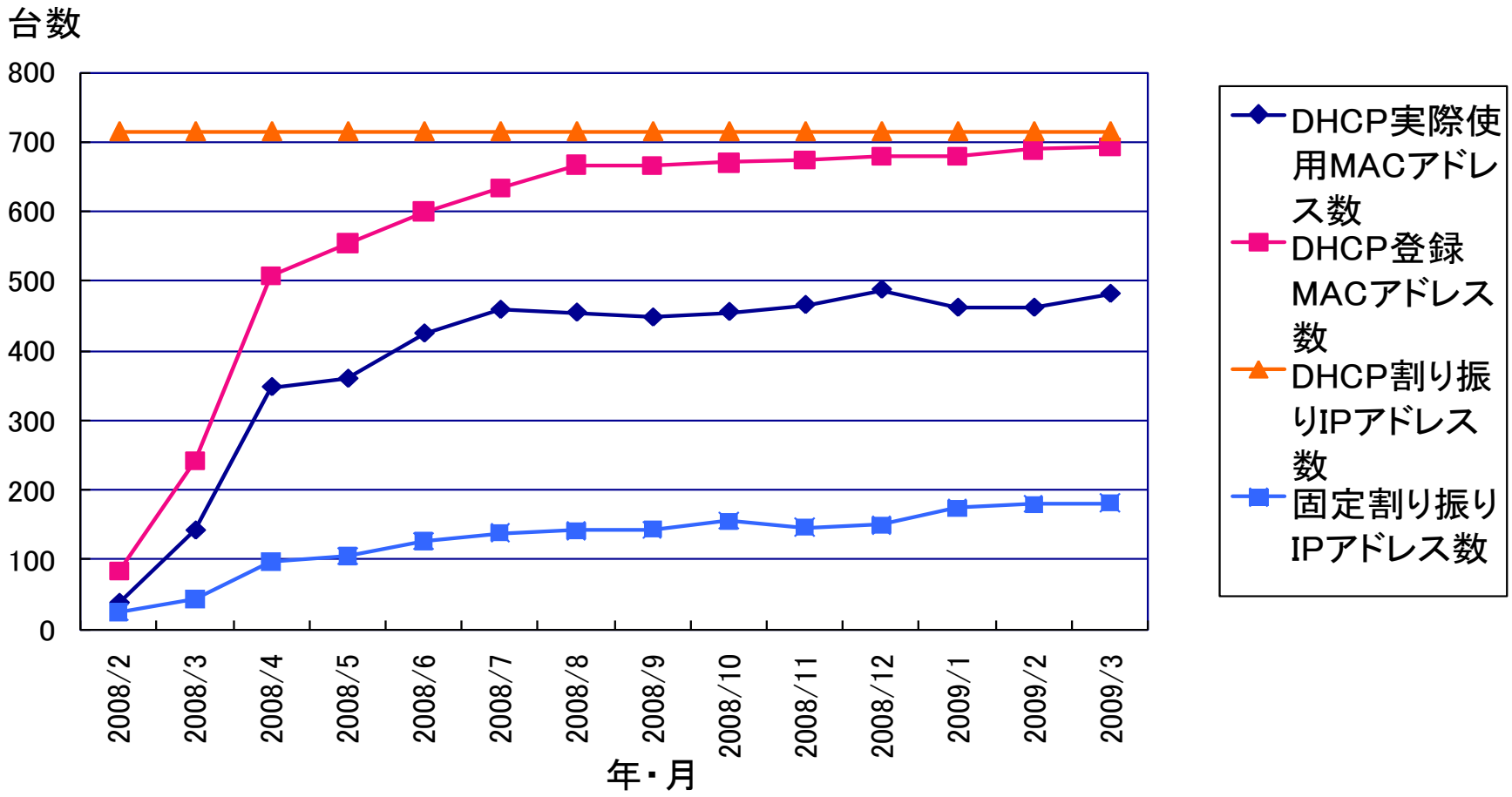
- 旧ネットワークと新ネットワークの共存が可能だったので、ユーザーは自分の都合のよい時に移行作業ができ、万一接続できない場合でも差し戻しが容易にできたため、余裕をもって移行ができた。
- 新ネットワークからは旧ネットワークのDNSサーバにはアクセスできないようにし、ユーザーの設定ミスを発見できるようにした。
- 1000台近くの登録マシンがあり、機種やOS、使い方も統一されていないため、移行には時間がかかると予想していたが、比較的スムーズに移行だった。ODINS5期の基幹ネットワークスイッチの入れ替えと同時期に作業したことや、新旧DHCPサーバの並行運用が可能だったことが大きい。

移行時のトラブル

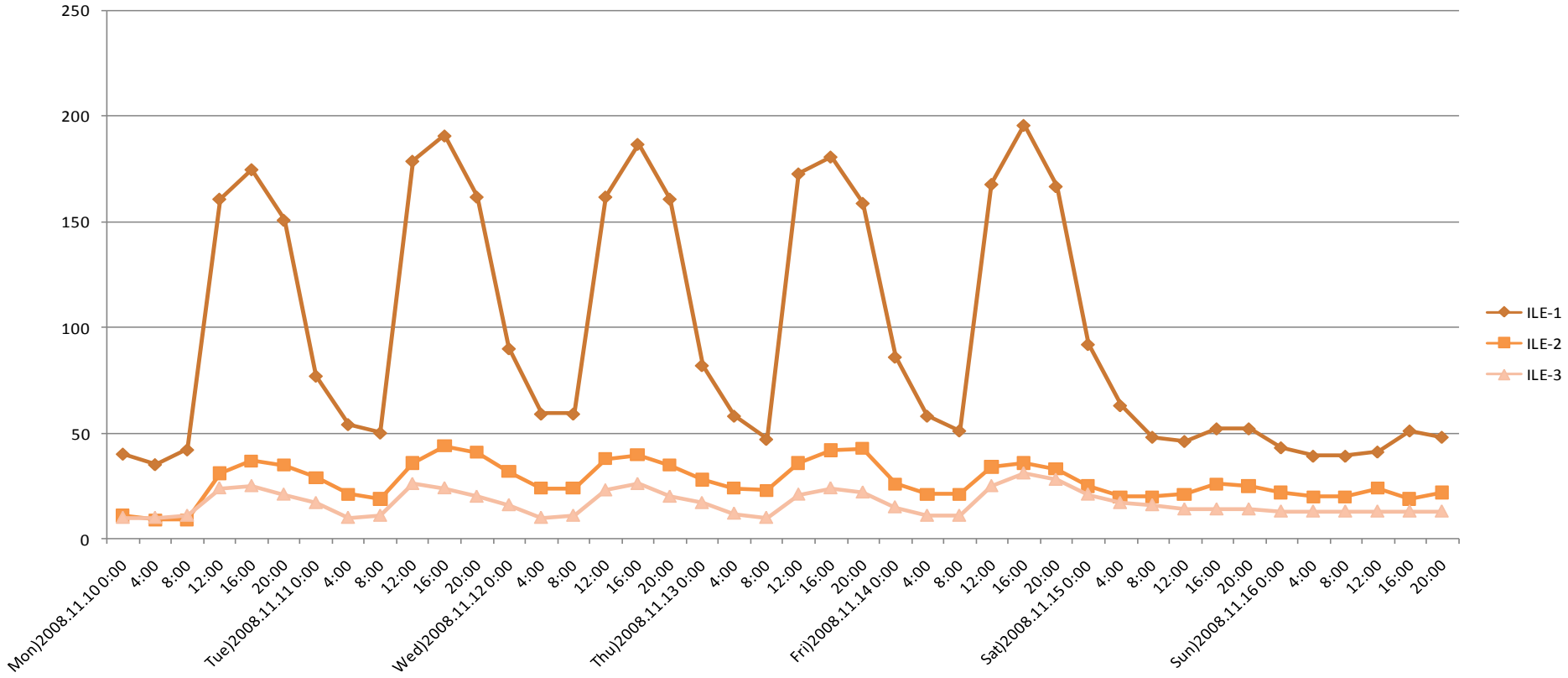
- 「ケーブルを繋ぎかえても接続できない！」
  →再起動すればOK
- 「Webやメールに接続できない！」
  →DNSサーバの設定
- 「サーバに接続できない！」
  →サーバのファイアウォール設定
- 「プリンタのIPアドレス変更！」
  →滅多にしないため手間取るユーザーが多数

新DHCPサーバ運用状況

登録MACアドレス、使用MACアドレス数やIPアドレス数の変移



一週間におけるIPアドレス使用推移



終わりに

このネットワーク整備は、長期的計画をたて、既存の運用に影響を与えぬよう、除々に行ってきた。

長年の課題だったIPアドレス返却や、全国共同利用対応などが解決し、多目的・多階層ユーザーが共存する環境下での、セキュアでシームレスなネットワークを整備することができた。

大学という環境下、様々なOSや機種などが混在し、使い方も多様なユーザーに対して理解を得るために、状況を時間をかけて説明し、できるだけ細やかな対応をすることで、理解・協力を得られたのも、スムーズな移行の要因の一つだと考えている。

日本電気株式会社・NECシステムテクノロジー株式会社・大阪大学総合情報通信システム情報推進部・レーザー研ネットワーク運用管理委員会・レーザー研ILENET係の皆さまに、感謝いたします

ご清聴ありがとうございました

大阪大学　レーザーエネルギー学研究センター

高性能計算機室

谷口　麻梨香　（たにぐち　まりか）

メールアドレス：ile-comp@ile.osaka-u.ac.jp

URL：http://www.ile.osaka-u.ac.jp