

多様なニーズに対応したネットワーク構築と運用ノウハウ

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、安原裕子、福田優子

レーザーエネルギー学研究センター 高性能計算機室

メンバー (3名)

福田	優子	(技術専門職員)
谷口	麻梨香	(特任技術職員)
安原	裕子	(技術補佐員)

スーパーコンピューターを用いたシミュレーションのため、レーザー核融合の研究に適したシステムと運用形態の開発や、研究の支援、データ解析のための可視化のサポートなどを行っています。

またネットワーク幹線や各種サーバの運用管理なども行っています。

スパコンを含め、100台以上のサーバーやネットワーク機器を管理しています。

目次

- ❁ 1. 用途に応じた4種類のネットワーク
～全国共同利用施設に対応したネットワーク整備～
- ❁ 2. 新DHCPサーバ導入とIPアドレス返却
- ❁ 3. ODINS5と全学無線LAN運用開始
- ❁ 4. 今後の予定

1. 用途に応じた4種類のネットワーク

全国共同利用施設に対応した
ネットワーク整備

ネットワークの経緯

全国共同利用施設化に伴い、ネットワークにも様々な要望が出てきました。

- ・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。
- ・実験機器にもアクセスしたい。

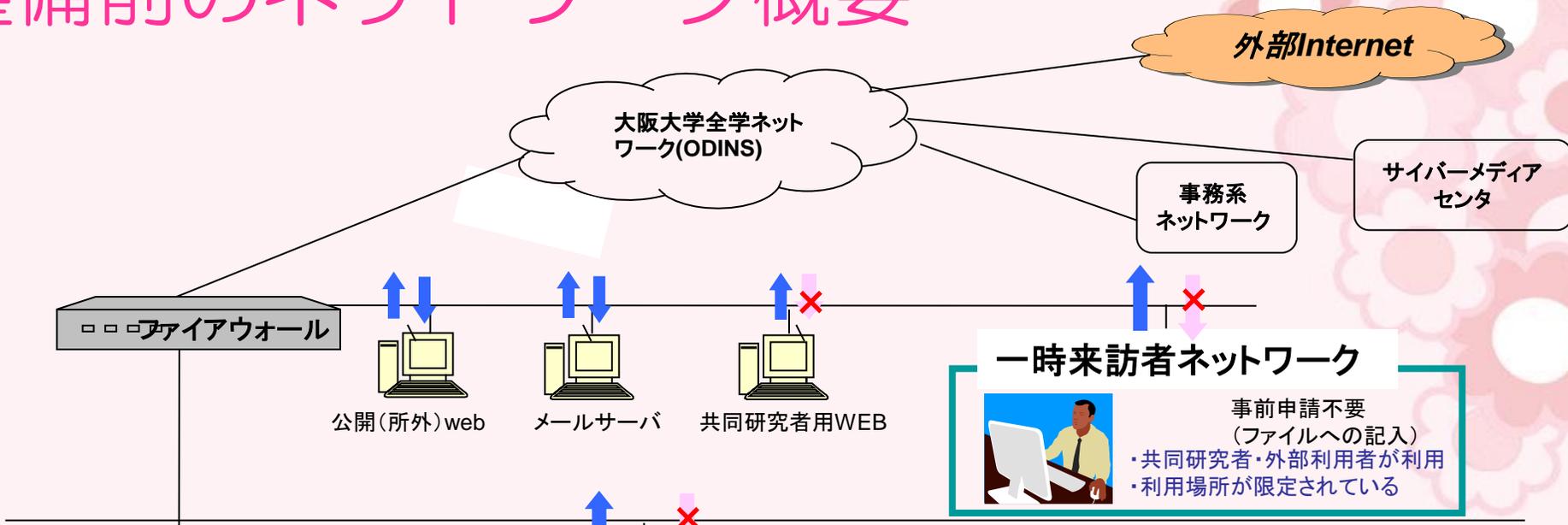


共同研究者用ネットワークの増強、センター内無線LANの整備として、認証ネットワークの導入をし、用途に応じた4種類のネットワークを整備



ODINS5サービス開始に伴い、新DHCPサーバ運用開始、IPアドレスの大幅な変更

整備前のネットワーク概要



レーザー研内NW

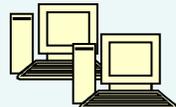
MACアドレス制限のDHCP



機器ごとの申請



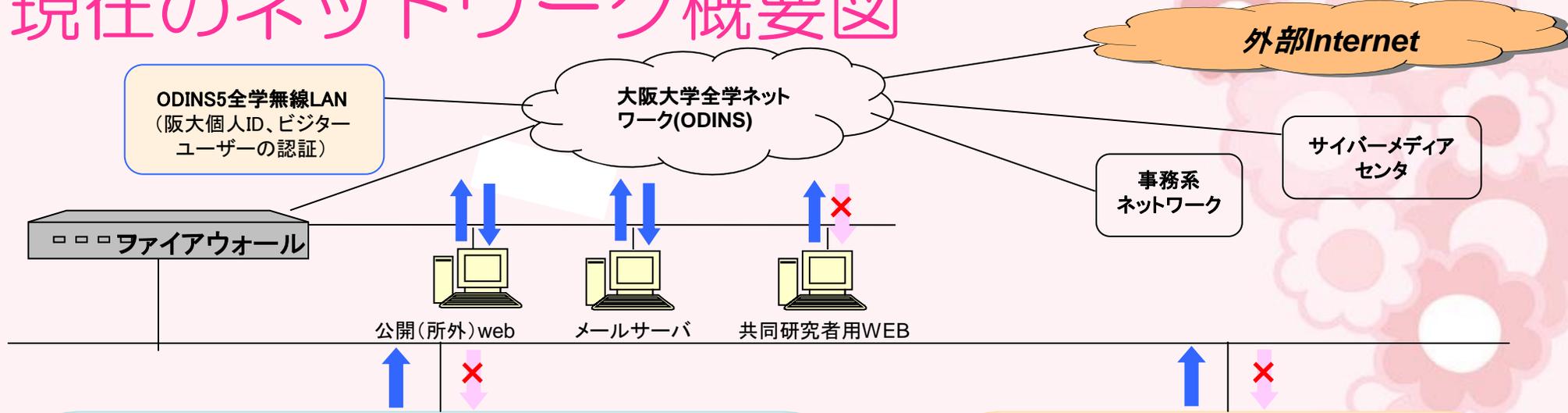
無線LAN



所内web、会議・出張DB、
実験DB など

- ・レーザー研メンバーが利用
- ・所内webや、会議・出張DB、実験DBなどにアクセスできる。

現在のネットワーク概要図



レーザー研内NW

ILE-NET (ILE-123)

MACアドレス制限のDHCP



機器ごとの申請
(通常利用)

ILE-AGNET

認証ネットワーク



無線LAN



利用者ごとの申請
(会議室などでの一時利用)

共同研究者AGNET

認証ネットワーク



無線LAN

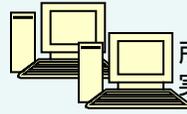


事前申請が必要(利用者ごと)
(一週間前までに)

一時来訪者ネットワーク



事前申請不要
(ファイルへの記入)

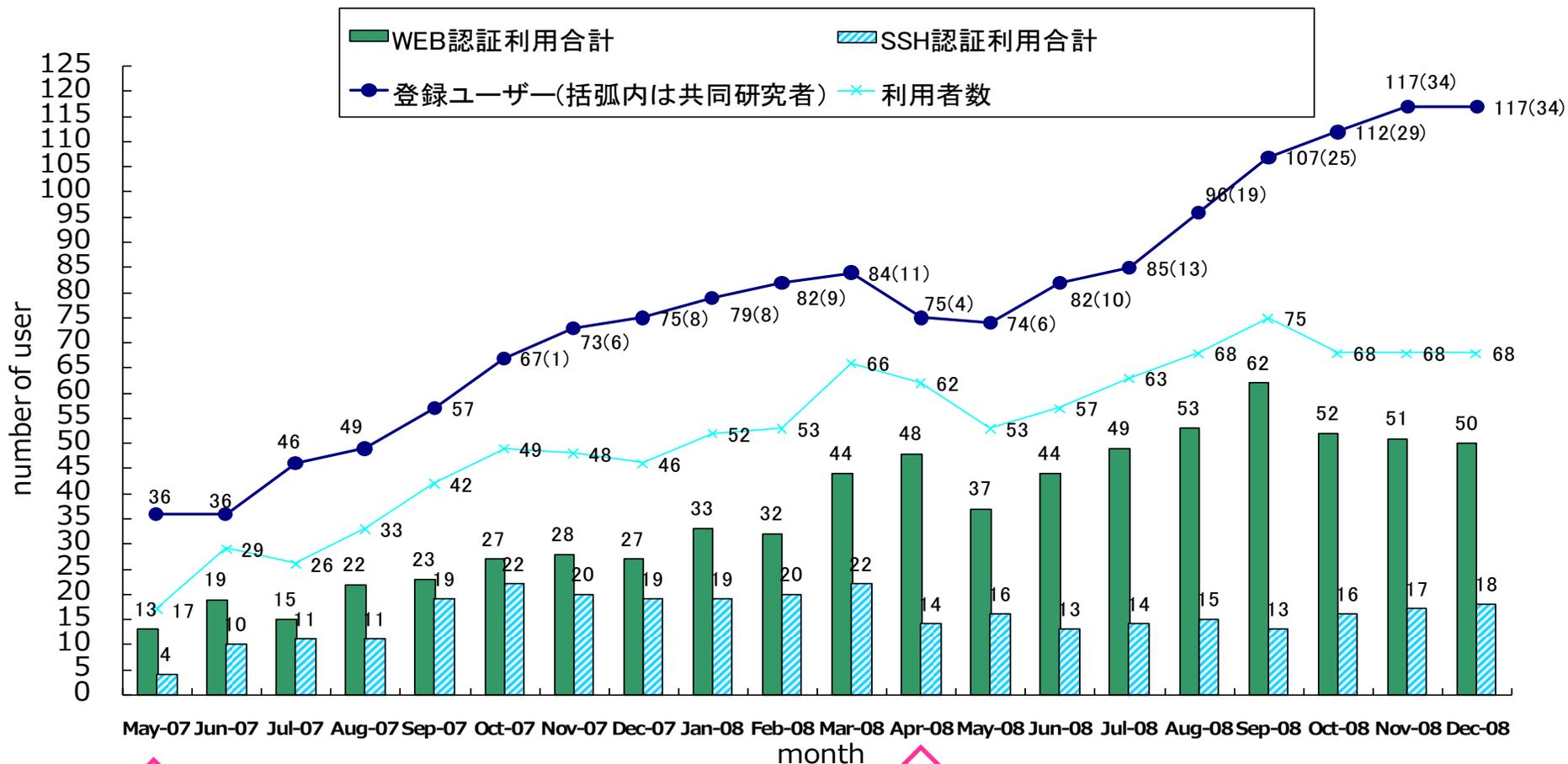


所内web、会議・出張DB、
実験DB など

- ・レーザー研メンバーが利用
- ・所内webや、会議・出張DB、実験DBなどにアクセスできる。
- ・このネットワーク内での通信制限は原則していないため、接続されている全ての機器にアクセス可能
(ただし、ILE-AGNET配下の機器への通信はできません)

- ・共同研究者・外部利用者が利用
- ・利用場所が限定されている(共同研究係が決定)
- ・レーザー研内NWにはアクセスできない
(ただし共同研究者AGNETはデイリースケジュールサーバにのみアクセス可能)

認証ネットワーク使用状況



↑
ILE-AGNET運用開始

↑
共同研究者AGNET運用開始

2. 新DHCPサーバ導入と IPアドレス返却



ネットワーク大変更への道

・2003年7月 DHCP導入

(レーザー研は人数に対してIPアドレスをたくさん使っているので返却してほしいという依頼あり)

・2003年10月 EUVシミュレーションGRID導入に伴い、小規模なFW構築

・2003年12月から2004年前半にかけて

上記のFWを用いて、レーザー研全体のネットワークに導入することをにらんだ様々なテスト&調査
2005年導入システムの仕様に反映

・2005年3月 新システム(レンタル)の一部としてFW導入

レーザー研ネットワーク大変更(NAT導入)

この時点で、IPアドレスを返却してほしいと言われたが、全スイッチ&サーバー、プリンタ、パソコンの設定変更が必要であり、とても 実現できないので、待ってほしいとお願いした

・2007年2月 認証ネットワーク導入

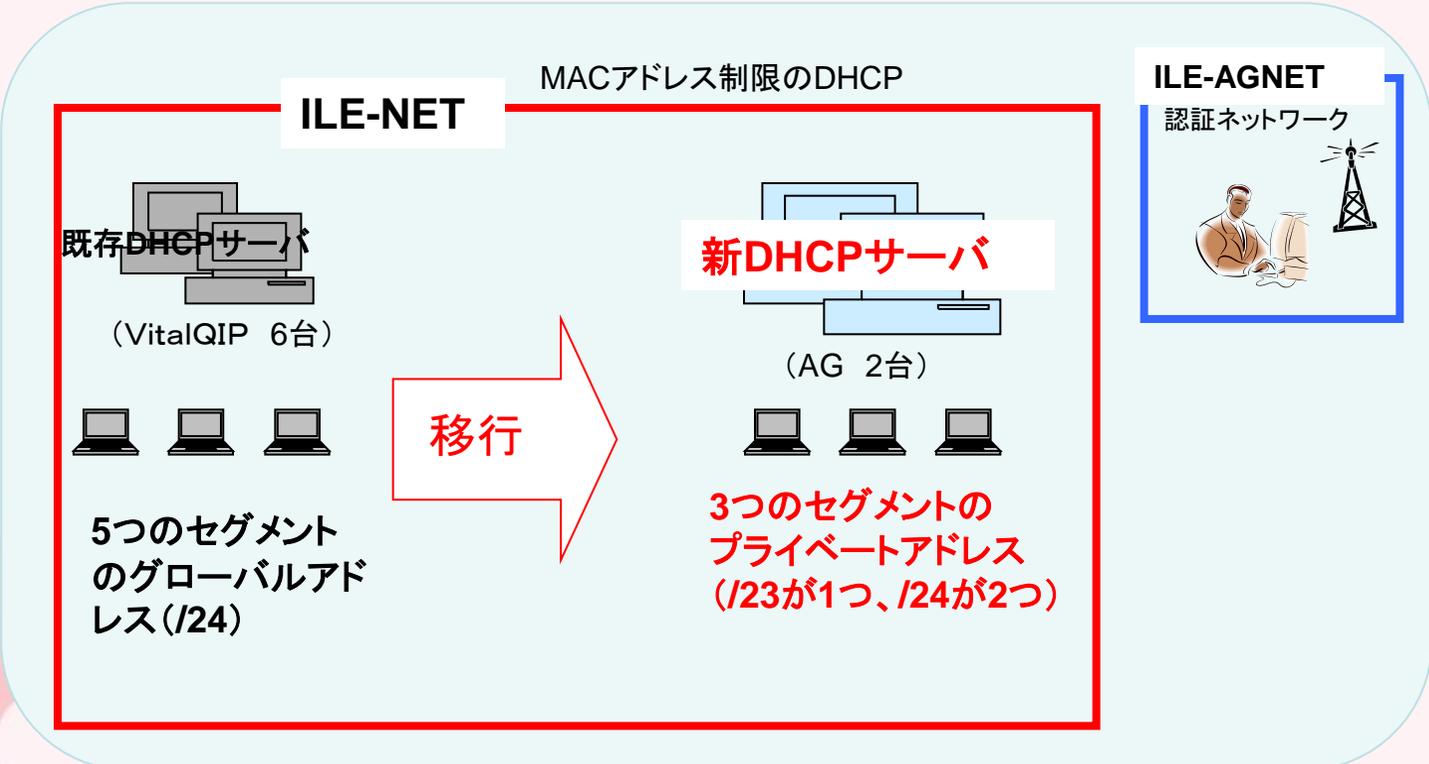
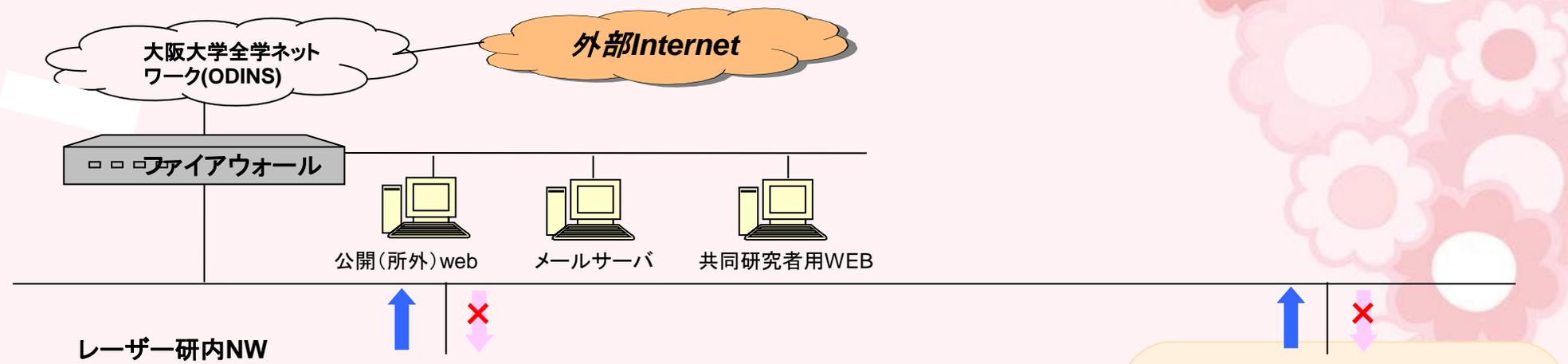
3月のネットワーク委員会で、新DHCPサーバー予算申請の方針決定

・2008年3月 ODINS5期整備 & 新セグメントのための新DHCPサーバーシステム導入

→2008年4月～順次、移行開始

(2008年3月末で、旧DHCPサーバーの保守切れ、今後のトラブル対応は不可能)

新DHCPサーバ導入



新DHCPサーバ 導入経緯

2007年 3月	ネットワーク運用管理委員会で、新DHCPサーバの導入方針決定 調査・見積もり依頼など
2007年 9月	会議で承認 調達手続きなど
2007年 11月	全登録マシン 再申請作業 (登録数 1082台 再申請により237台削除)
2008年 1月	DHCPサーバ納品 テスト、運用方針の検討など 新ネットワーク運用開始
2008年 1月～3月	ODINS4→ODIN5移行
2008年 4月	ODINS5運用開始
2008年 4月～	新ネットワークへ移行(徐々に)
2008年 6月	845台中、706台 移行完了 (移行未 139台)
2008年 7月	<u>3セグメント返却 (ネットワーク変更作業)</u>
2008年 8月	845台中、794台 移行完了 (移行未 51台)
2009年 1月	全ユーザーマシン 移行完了

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。
133.1.82.*** (テラヘルツ部門) は、現在固定アドレスのみなので、全てのパソコンが変更対象になります。
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。減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。

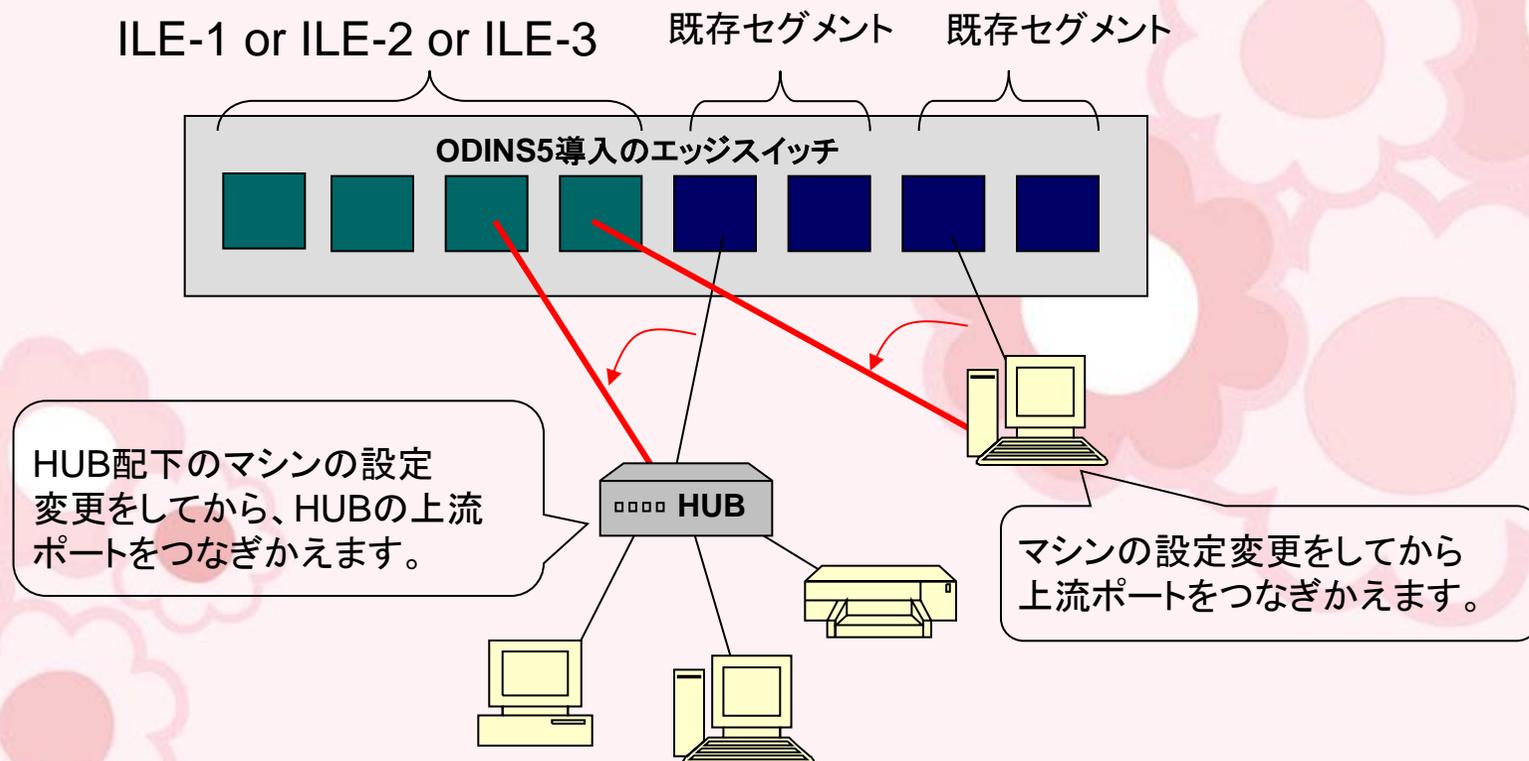
■ 配線状況によっては、部屋のマシンを一斉に変更する必要があるかもしれません。

担当のILENET係からご連絡いたします。

ユーザーへのアナウンス

～ 新ネットワークに移行するには ～

ODINS5のスイッチには、新ネットワークのポートが準備されています。
ILE-NET係から移行の連絡があり次第、マシンの設定変更をして、ケーブルをつなぎ換えてください。



IPアドレス変更の流れ

ネットワーク停止が伴わないような移行方法を検討しました。

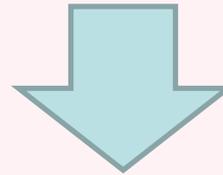
事前準備

ILENET係

移行する日程を決め、CMPに連絡。部屋のユーザーにアナウンス。
また、上流の線をどこに差し替えるかを決めておく(差し替えが出来ない場合は、ODINSに設定変更を依頼)

CMP

部屋のマシンを、新DHCPに登録、固定IPアドレスの割り振り、シールの発行



移行当日の作業

ILENET係

上流の線を差し替える

ユーザー

- ・DHCPのマシン : ネットワーク設定の変更はなし。サーバやプリンタの設定変更が必要(DNSでひっばっているものは変更しなくてもよい)
- ・固定のマシン : IPアドレスの変更。ファイアウォールなどの制限の変更も必要。

CMP

固定アドレスのサーバのDNSの変更

移行時トラブル

■ケーブルを差し替えてもつながらない！

- ・設定が反映されるまで時間がかかり、すぐには接続されなかった。
→ネットワークの再起動をしてもらうのが一番早かった。
(「ネットワークの修復」などでもよいが、結構時間かかった)
- ・昔のDNSサーバの設定が残っていた。

■サーバやプリンタのIPアドレス変更ができない！

- ・プリンタの設定変更は滅多にしないため、手間取る場合が多かった。
 - ・設定変更をする前にケーブルを差し替えてしまい、ネットワーク設定画面にアクセスできなくなってしまった。(または間違った設定にして差し替えてしまった。)
 - ・ファイアウォールの設定変更を忘れていて、接続できなかった。
 - ・デフォルトゲートウェイを設定していなくて、他セグメントからの通信ができなくなった。
- ※パソコン側でのプリンタ設定変更は、新規にプリンタ設定をしたほうが簡単だった。

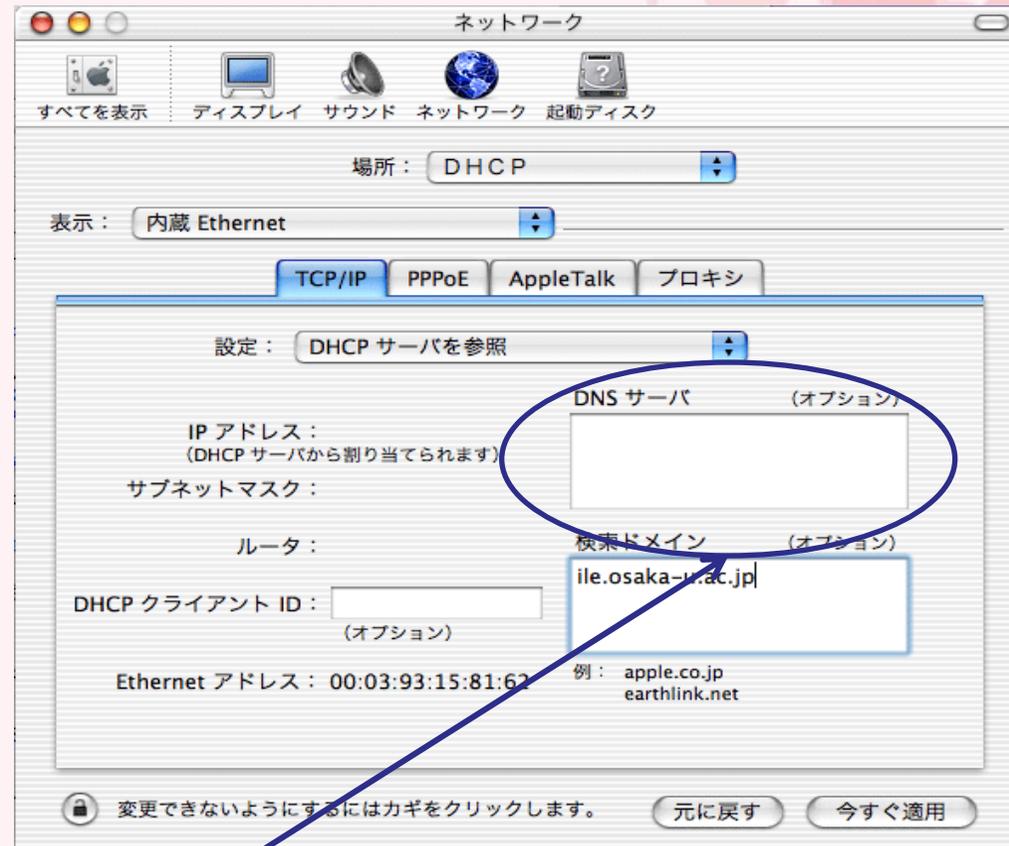
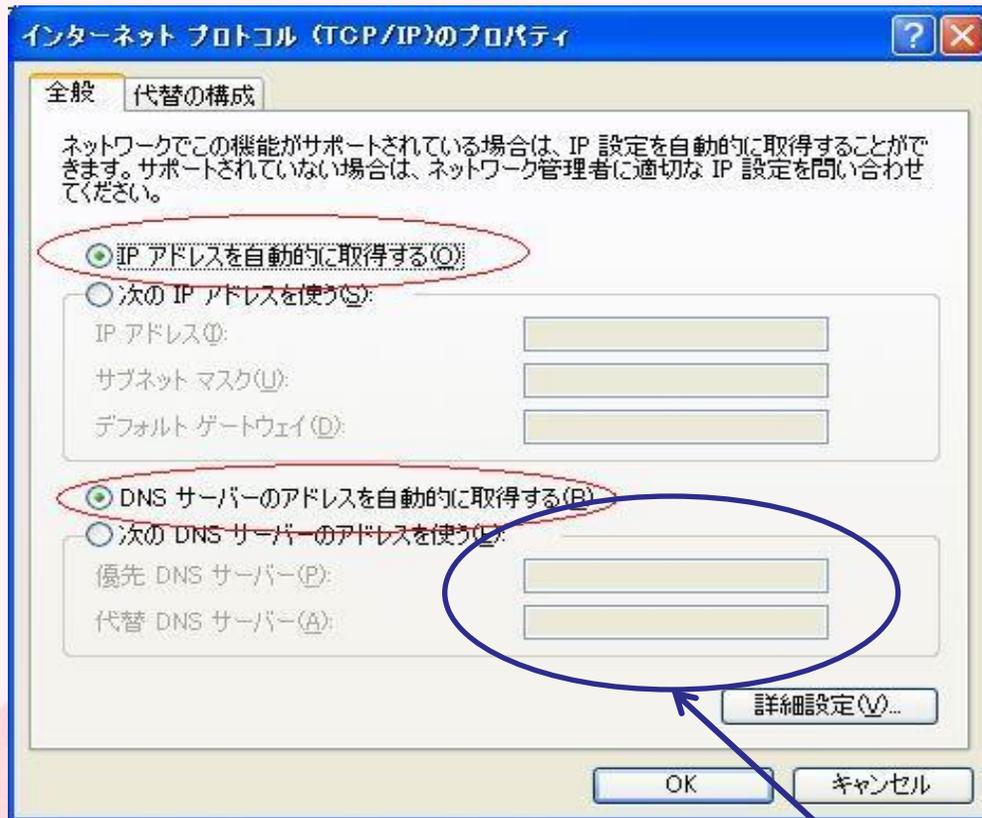
■WindowsネットワークやAppleTalkができない

- ・既存NWでは、他セグメント間でのWindowsネットワークやAppleTalkができるようにしていたが、新NWでは、同一セグメント内のみとしたため。
→IPアドレスでアクセスするか、同一セグメントにするかで対応。

【もう一度ご確認を！】DNSサーバの設定に注意

DHCPで利用しているパソコンに、DNSサーバの指定をしていませんか???

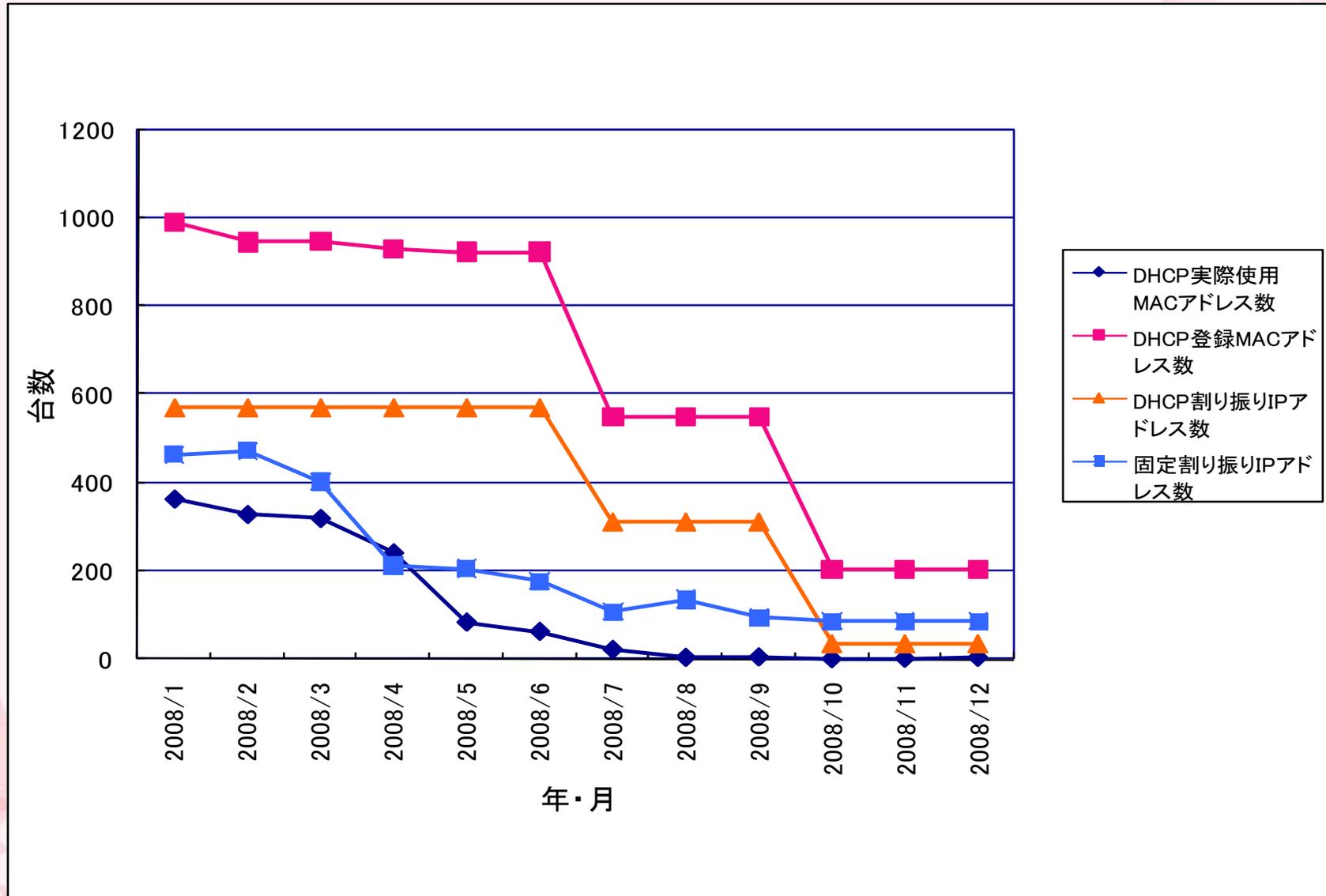
古い設定が残っているなど、間違った設定をしていると、レスポンスが遅くなります。



何も設定しないでください

旧ネットワーク運用状況

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



3セグメントをODINSに返却しました

■2008年7月 3セグメントのグローバルアドレスを返却しました。

< 返却日の作業 >

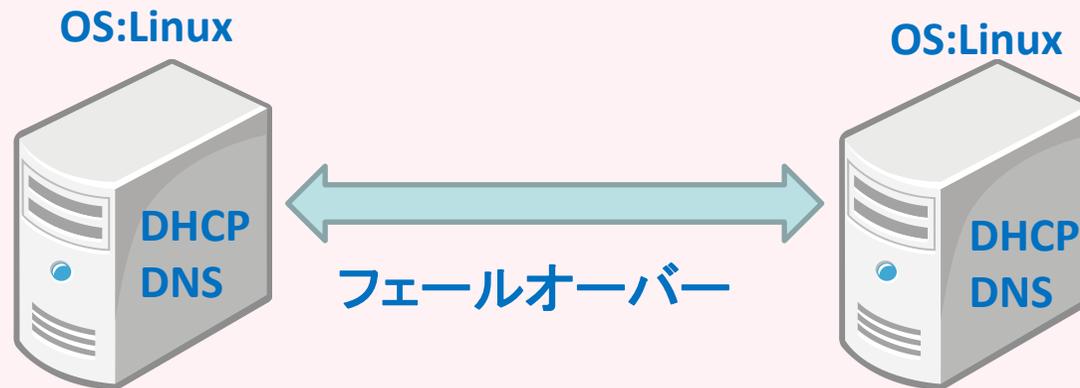
- ・ILEルーター 設定変更
- ・各スイッチ VLAN設定変更
- ・DNSサーバ変更

< 事前作業 >

- ・該当セグメントDHCPサーバ終了
(WindowsServerで、アクティブディレクトリや、フォレストなどもしていたので、
停止するのに苦労しました)
- ・AppleTalkルーター終了
- ・FWから設定削除(NAT設定など)
- ・各計算機やサーバなどのルーティングや、iptablesやhosts.allowやhttpd.conf...etcの
設定や、管理ツールから削除(数が多かったので、大変でした)

■2009年1月 全ての旧DHCPサーバ サービス終了しました。

新DHCPサーバを運用開始して



～ NECシステムテクノロジー社のAuthenticationGatewayを導入 ～

運用しやすくなりました！

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。

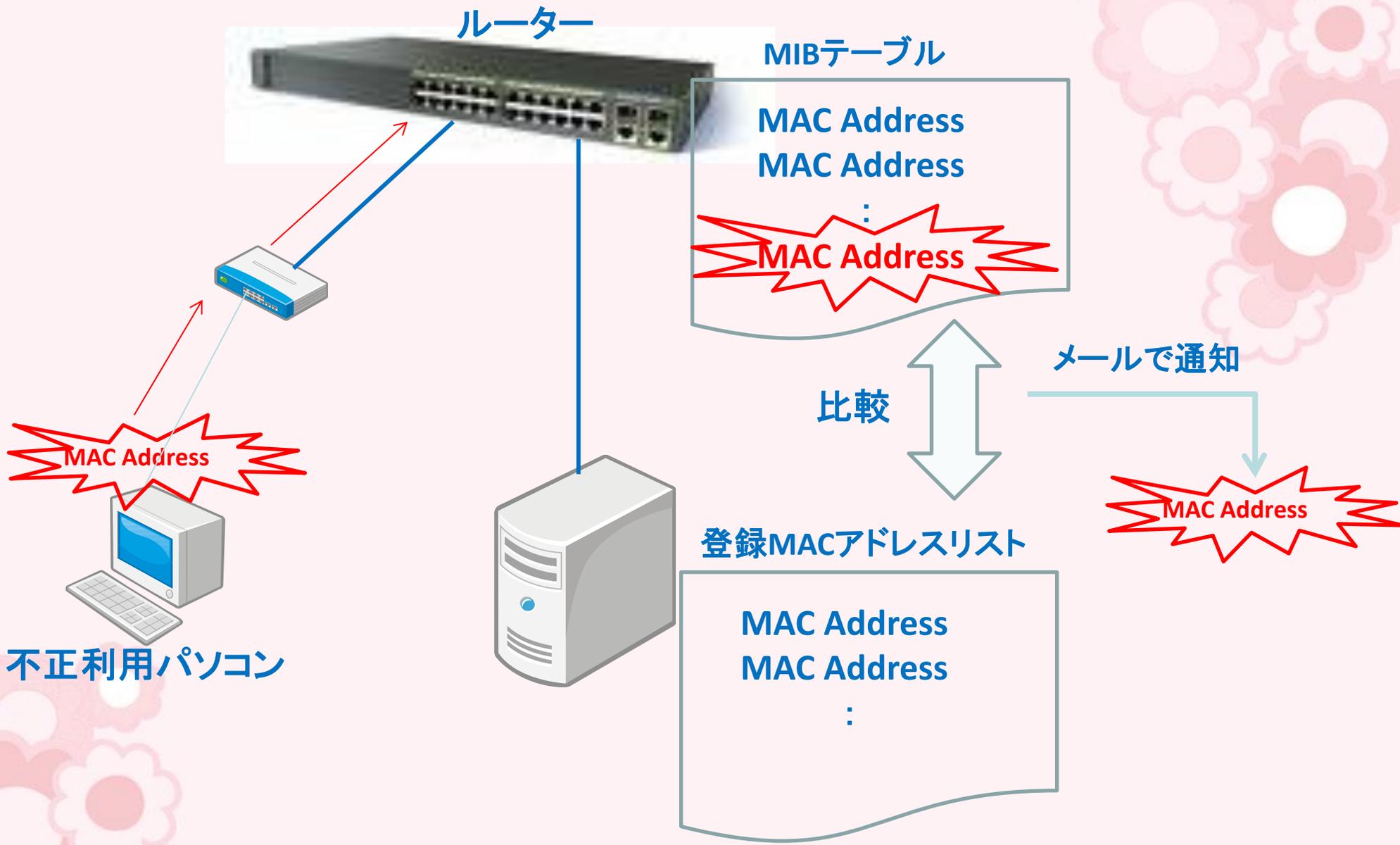
2. OSがLinuxのため、ログ採取などの運用管理ツールの作成が容易に。

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。

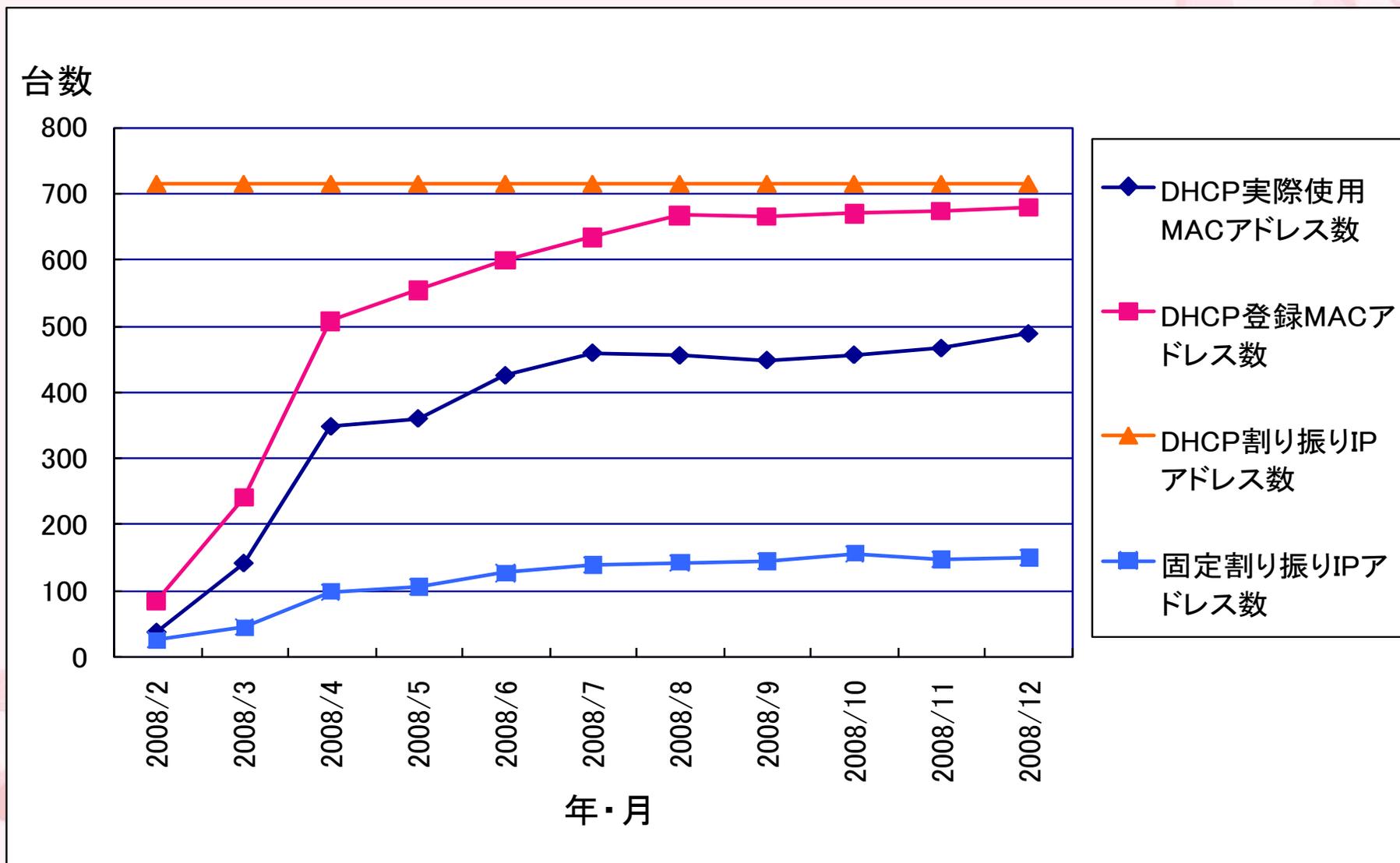
以前のサーバはWindowsでGUIでの手作業が必要だったが、ツールを作成し、CUI作業が増えたため、ツールを作成し、自動化できた。

不正MACアドレス自動検知



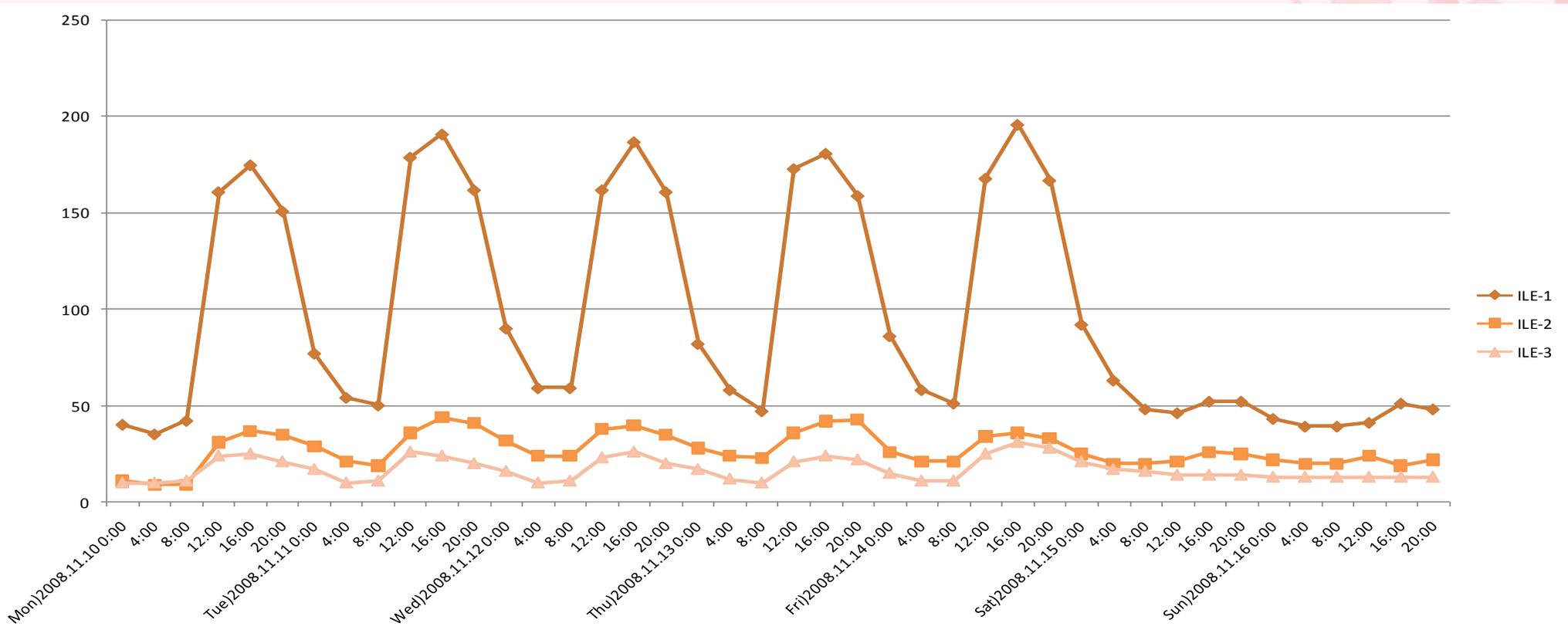
ILE-123ネットワーク運用状況

登録MACアドレス、使用MACアドレス数やIPアドレス数の推移



ILE-123ネットワーク運用状況

DHCPで実際に利用されているIPアドレス数の変移(2008年11月の一週間)

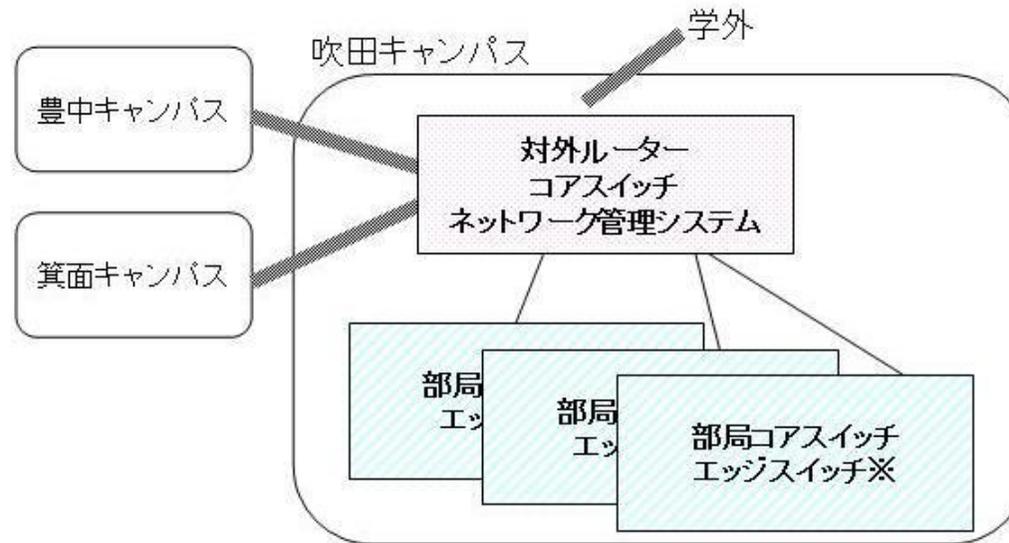


3. ODINS5と 全学無線LAN運用開始



全学ネットワーク ODINS5 運用開始

2008/4/1 運用開始



ODINS5の特徴

- ◆ 基幹ネットワークのセキュリティ向上・高速化
 - ・ブロードキャストストームの防止
 - ・バーチャルファイアウォールの導入
 - ・10Gbpsネットワークの導入
- ◆ 外大統合および、ODINS4期以降の建物のネットワーク整備
- ◆ 保守体制の強化、24時間365日の監視
- ◆ 全学無線LANの整備

全学無線LANビジターID

各部署長に任命された、無線LANビジターID発行者は、ビジターIDを発行できます。



無線LAN
ビジターID発行者

Webアクセス（阪大個人IDが必要）

- ・ビジターIDの新規発行
（cvsファイルによる一括発行
web画面による個別発行）
- ・発行済みビジターIDの照会
- ・ビジターID通知書・パスワードの再発行
- ・ビジターIDの一時停止・一時停止解除

認可システム



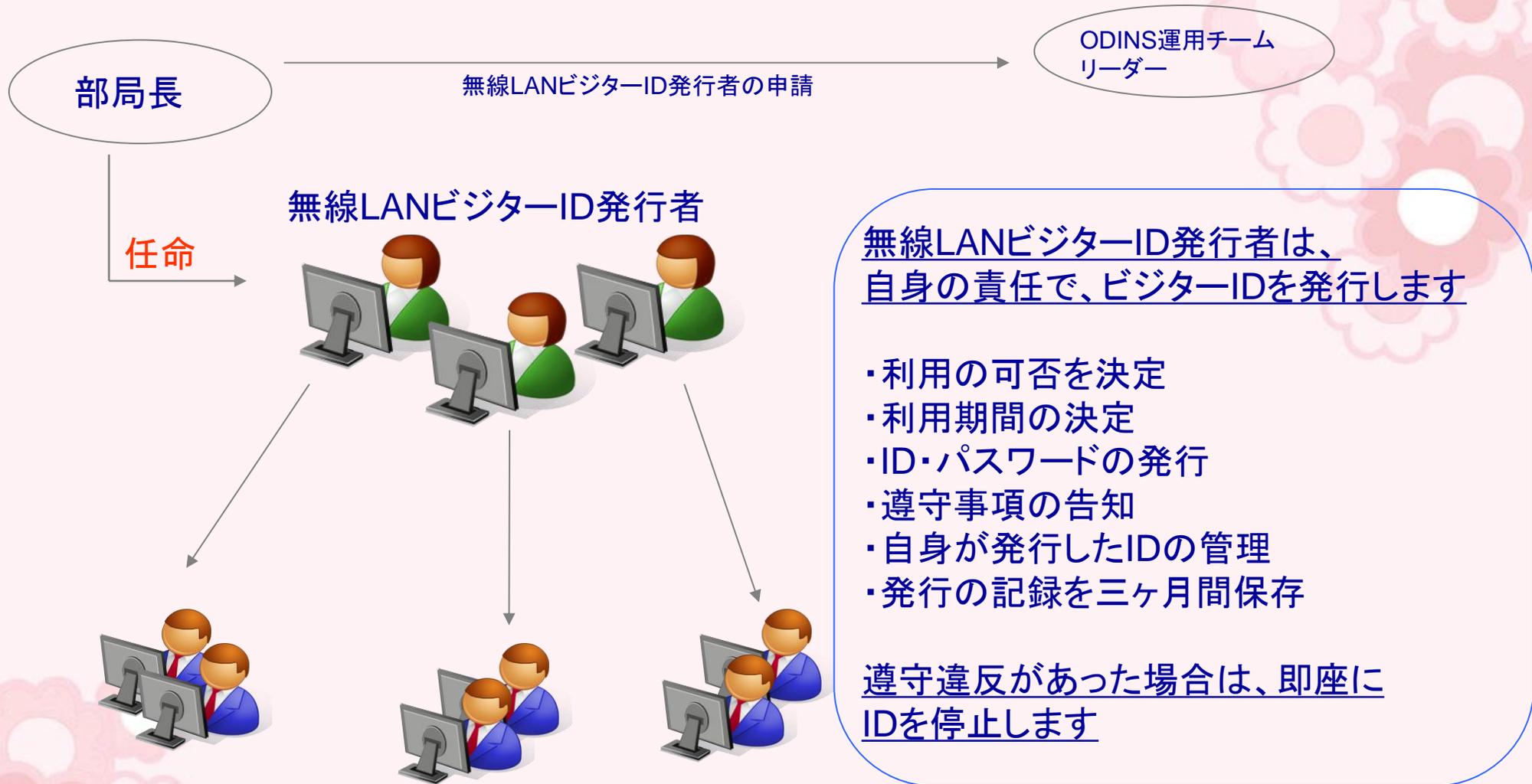
ビジターID通知書(pdfファイル)



ビジター

※ビジターIDの有効期限は、最長7日間です
※一つのビジターIDで、同時一台までの利用です

ビジターID運用細則



4. 今後の予定



今後の予定

◇全共化対応データベースシステム検討

全国共同利用施設として、実験データの共有・情報共有・文書管理を目的とした、データベースシステムを検討しています。

既存のデータベースシステムよりも、細やかなアクセス権や、変更にも柔軟に対応できるシステムを目指し、検討作業部会を発足し、検討を行っています。

◇次期システム導入に向けて準備をしています

平成22年2月末で、現システムのレンタル期間が終了します。
3月からの次期システムに向けて、準備をしています。

最後に

ネットワーク整備は、予算的な制限や、様々な利用者の意見もある中で、できる範囲で除々に行ってきました。

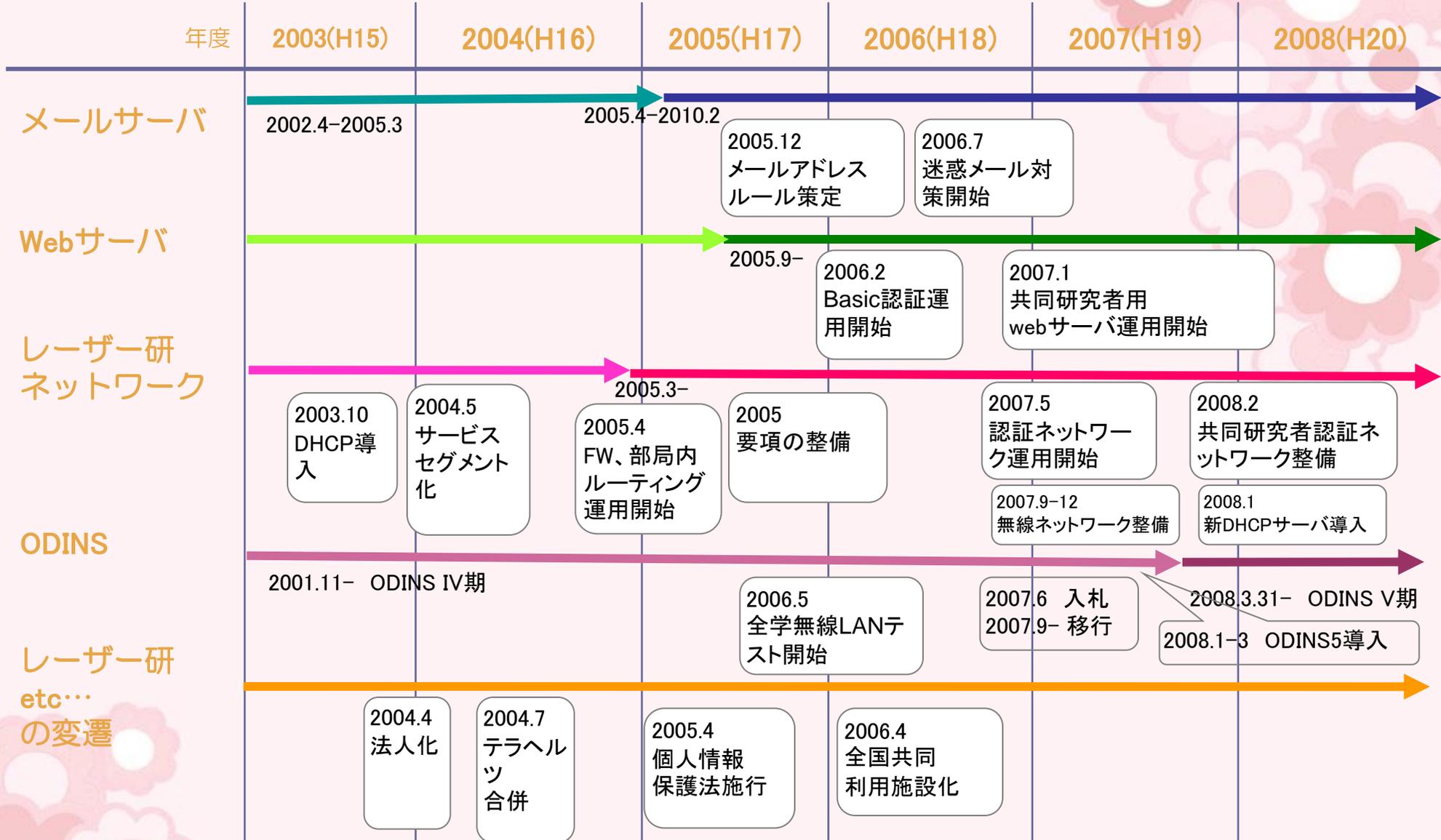
ネットワークは“動いていて当たり前”という感覚が利用者にあるため、既存の運用に影響を与えないようにサービスを開始したり、移行することが求められています。

他機関の皆様のお話も参考にし、これからも、できるだけシンプルなシステムを目指して、運用していきたいと思っておりますので、何かアドバイスなど頂ければ幸いです。

ご清聴ありがとうございました。

大阪大学サイバーメディアセンター、及びODINS事務室の皆様には大変お世話になっており、感謝いたします。

経緯



ODINS5 全学無線LAN

ODINS5より、全学無線LANが正式にサービス開始されました



- ・IEEE802.1x認証の導入(セキュリティの強化)
- ・アクセスポイントの運用・保守体制の強化
- ・コントロールサーバで、アクセスポイントを一括管理
- ・阪大個人IDで利用可能 また、ビジターIDの発行が可能

レーザー研の無線ネットワークとの違い

- ・全学無線LANは、レーザー研ネットワークから見ると、外部ネットワークと同じ。
- ・全学無線アクセスポイントが設置されている場所なら、全学どこでも利用できる。
- ・レーザー研に設置されているアクセスポイントで、すべての阪大個人ID、ビジターID所有者が利用できる
- ・ポート制限を設けている。