龍谷大学理工学部におけるネットワーク運用(失敗)事例

龍谷大学理工学部
小島 肇

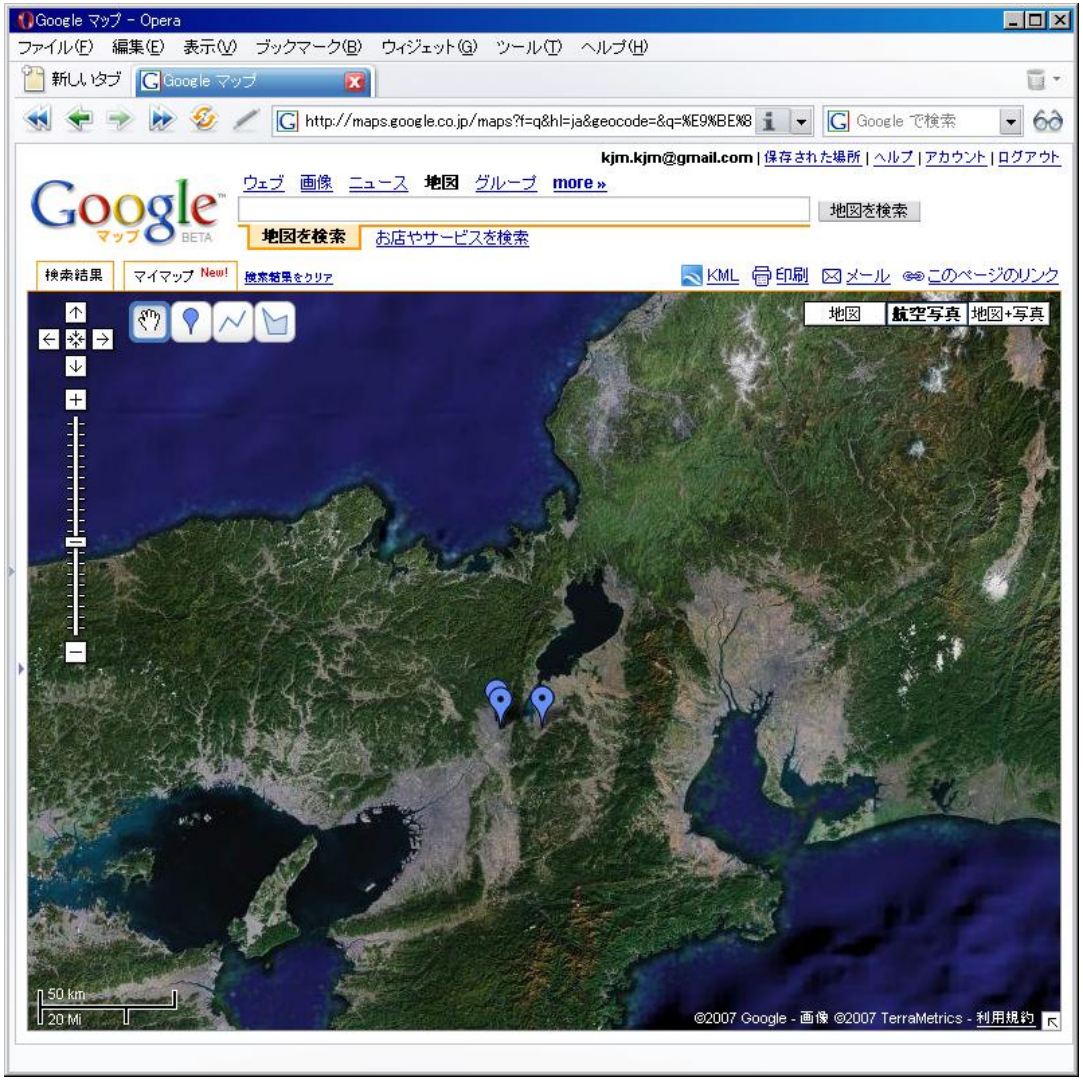
きょうのおはなし

- 対外接続系の話
- 界面系の話
- メール配送系の話
- 瀬田学舎教育系の話

組織の紹介

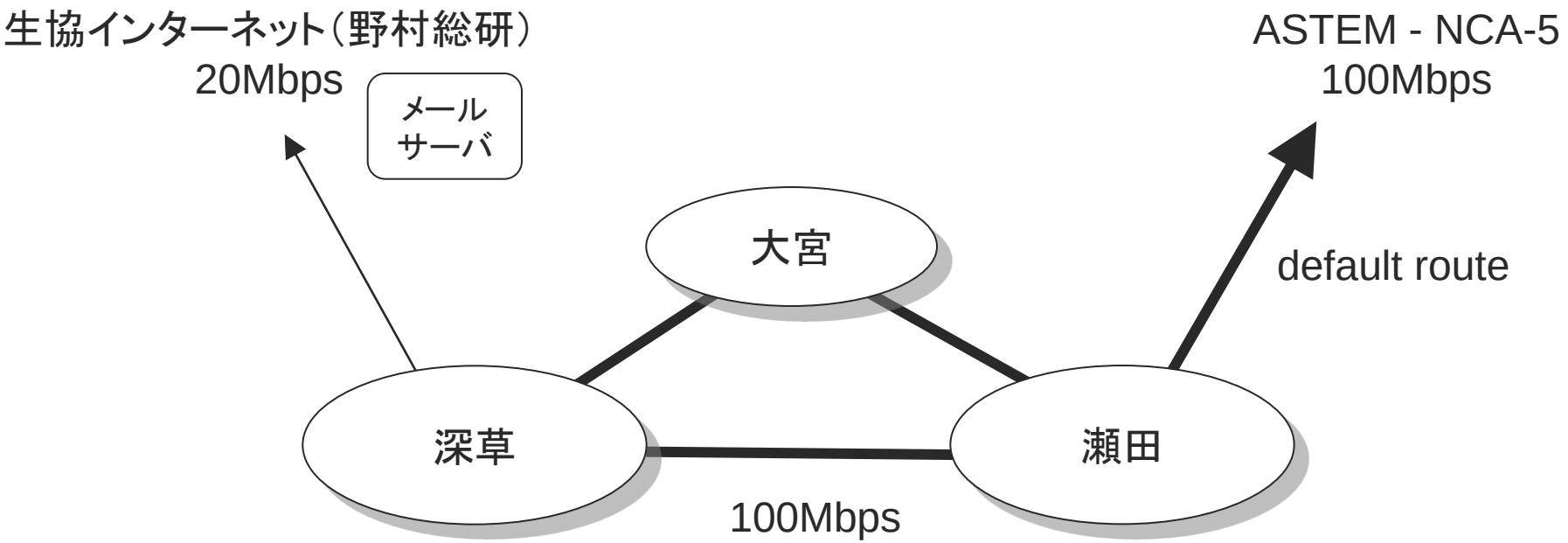
- RINS; Ryukoku Information Network System
  - 理工学部ネットワークの運営母体
  - 予算はあまりない
- 情報メディアセンター
  - 全学的な運営母体
  - 潤沢な予算

龍谷大学 瀬田学舎


Google マップ - Opera
ファイル(F) 編集(E) 表示(V) ブックマーク(B) ウィジェット(G) ツール(T) ヘルプ(H)
新しいタブ
Google マップ
http://maps.google.co.jp/maps?f=q&hl=ja&geocode=&q=%E9%BE%8
Google で検索
kjm.kjm@gmail.com | 保存された場所 | ヘルプ | アカウント | ログアウト
Google マップ BETA
ウェブ 画像 ニュース 地図 グループ more »
地図を検索
地図を検索 お店やサービスを検索
検索結果 マイマップ New! 検索結果をクリア
KML 印刷 メール このページのリンク
地図 航空写真 地図+写真
50 km
20 Mi
©2007 Google - 画像 ©2007 TerraMetrics - 利用規約

対外接続系の話

龍谷大学ネットワーク（2006.07）



ASTEM：京都高度技術研究所
NCA-5：第5地区ネットワークコミュニティ（主催：京都大学）

2006.07 までの状況

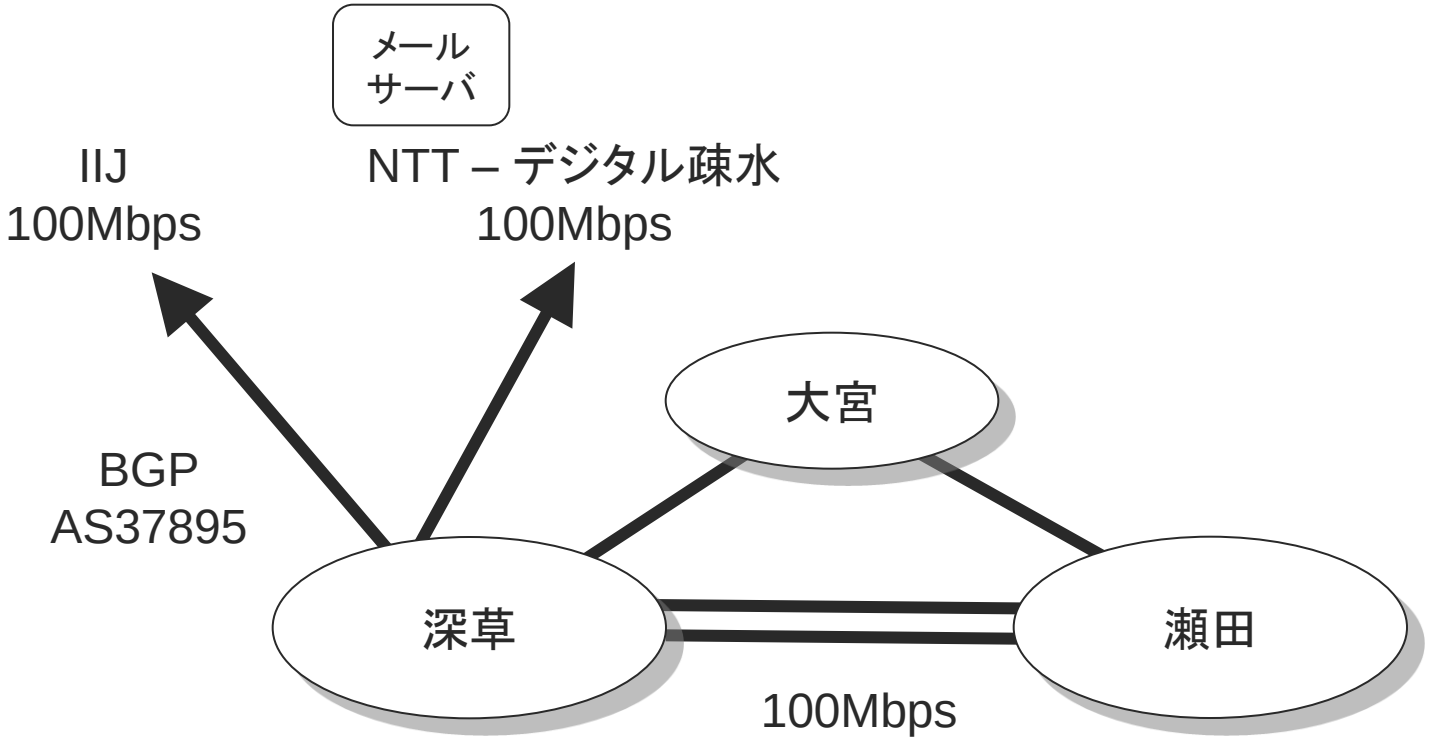
- 瀬田 – ASTEM – NCA-5 のラインがたびたび障害で停止
  - 生協側が生きていても対外接続は停止してしまう
- 京都大学が NCA-5 が手を引きたがっているという話
  - デジタル疎水（2003～）への移行

デジタル疎水：京都デジタル疏水ネットワーク。京都府主催の光基幹ネットワーク

BGP化の検討

- もともとはさくらインターネットからの持ち込み企画
  - 龍大 OB
- 各学舎をより独立的に運用する案も検討されたが、結局採用されず
  - NEC
- 深草学舎での一極集中接続案が採用される
  - single point of failure
  - 理工学部はバックアップ回線の必要性を訴えるも、いまいち通じず

龍谷大学ネットワーク（2006.08）

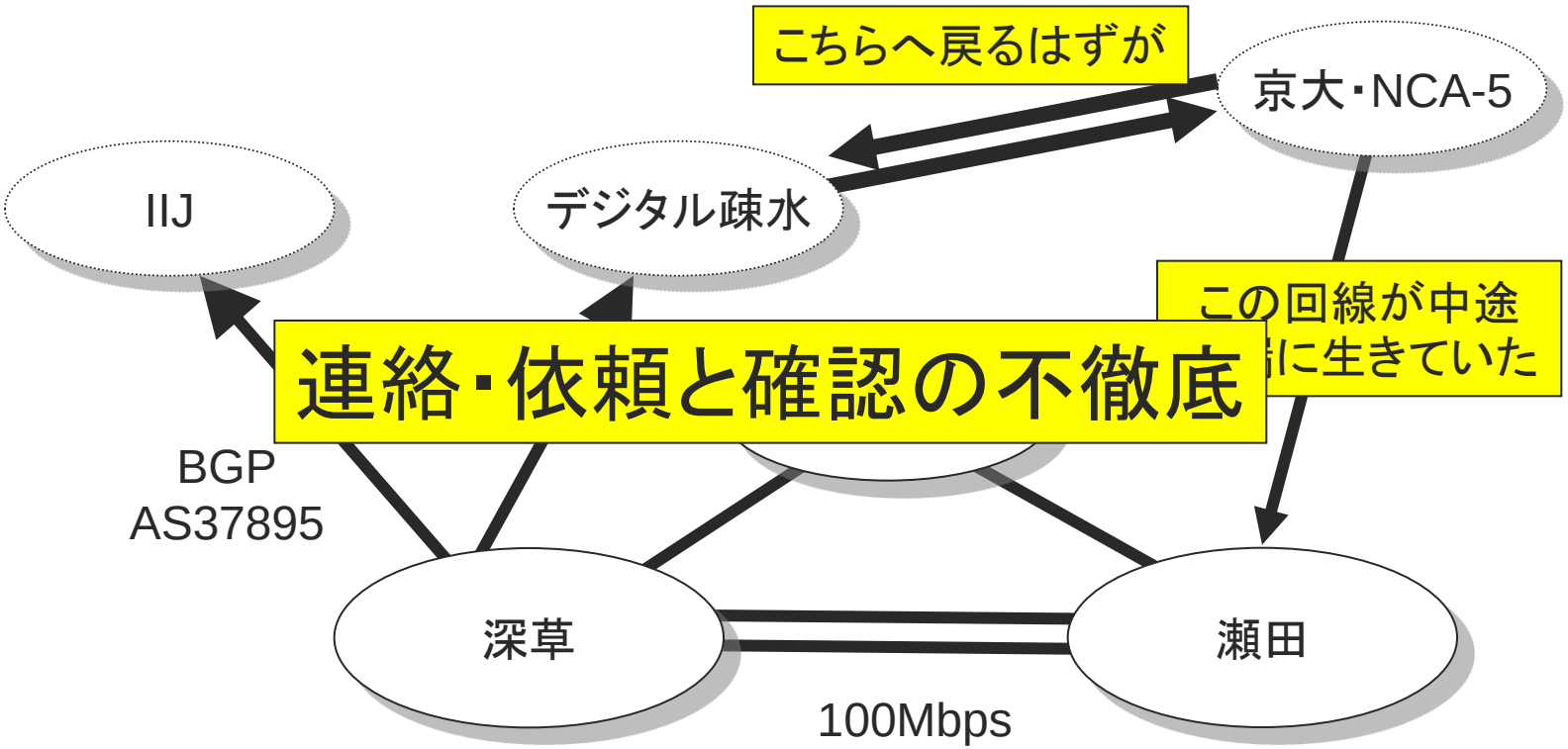


変更後の不具合

- 特定の組織との間の通信に障害が発生
  - 京都大学、生協インターネット、大学コンソーシアム京都、りそな銀行、……
- MTU を 1500 から 1470 に変更すると回避できる
  - 新規導入機器（BGP ルータなど）が悪さを？

MTU: Maximum Transmission Unit。Ethernet のデフォルト MTU は 1500 オクテット

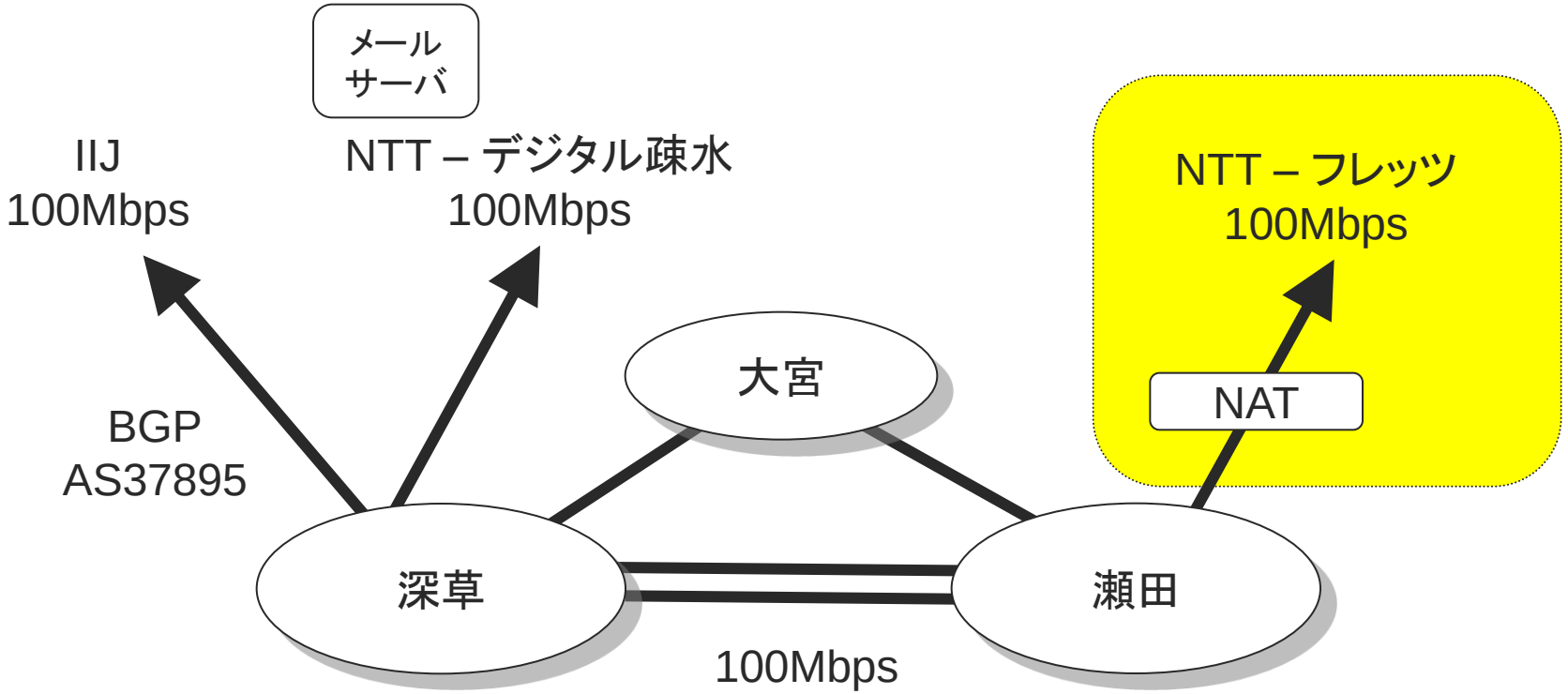
実は……
こうなっていたのが原因らしい



変更後の仕様

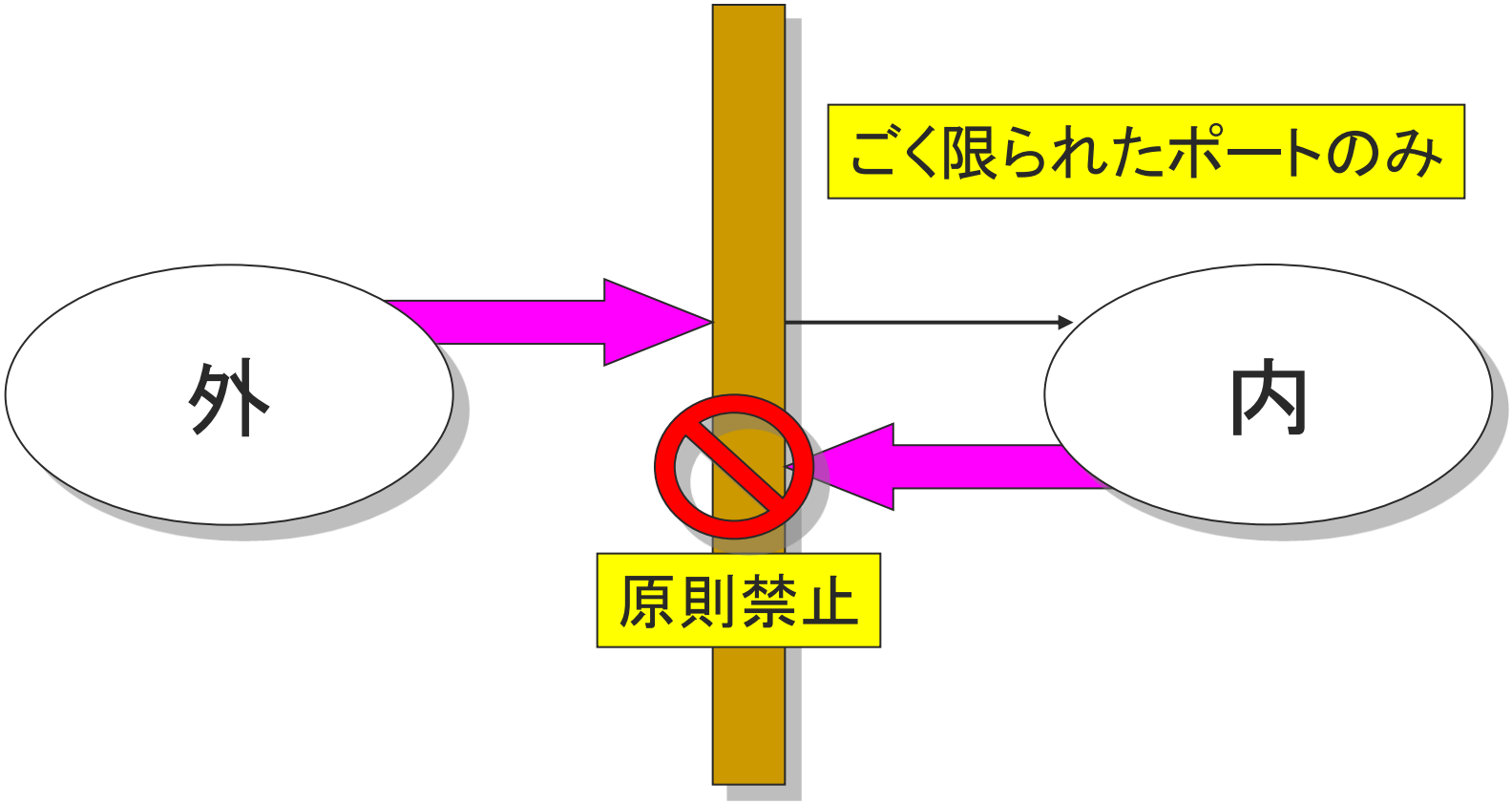
- 深草学舎が single point of failure
  - 瀬田学舎からすると、サービスが degrade したように見える
- 法定点検に伴う停電時にさっそく露呈
  - 「電源車により対応する」とされていたが、実際には機能せず
  - バックアップ回線の必要性がようやく理解される

龍谷大学ネットワーク（近未来）



界面系の話

ファイアウォールポリシー



ごく限られたポートのみ……

- 実は 80/tcp が解放されている
  - まずいじゃん！
  - プリンタやルータの Web 管理インターフェイスなど、イントラのつもりのサーバが見え見え……
  - 理工学部で使用している IP アドレス領域については 80/tcp も塞ぐように依頼

外に出るには proxy 必須

- 用意しているもの
  - http proxy
  - socks5 proxy（理工学部のみ）
  - rtsp proxy（理工学部のみ）
- 自動系のものは使わない
  - 透過型 proxy ではない
  - CARP（Cache Array Routing Protocol）は使わない
  - WPAD（Web Proxy Auto Discovery）は定義しない
- proxy はべんり
  - 内部で変なものが流行っても外に出ていきにくい（といいな）
  - やばそうなコンテンツについては proxy でアクセスを制限できる（かもしれない）

検出系

- IDS/IPS の類はなし
  - 全学設備にもない
  - つい最近のネットワーク導入に含めようとして失敗（予算不足　orz）
- ログを読む
  - 全学ファイアウォールには興味深いログがたくさんありそうだけど私には読む権限がない
  - 理工学部内の特定のサーバのログをしこしこ読んでJPCERT/CC に報告する日々

ログを読む話

- SSH や FTP への辞書攻撃がひどくてログが読み切れない
  - 一定以上のエラーが発生した場合にはアクセスを一時的に拒否するツールを使うようにした
    - http://www.st.ryukoku.ac.jp/~kjm/security/sshbook/hosoku.html#20061129
    - 手元のサーバでは iptables も pf も使えないので、/etc/hosts.allow を操作するように変更した
- apache のエラーログをまじめに読んでみたら attack がいろいろあるみたい
  - それっぽいものは syslog に吐き、再集計して JPCERT/CC にタレコミ

それっぽいものは syslog に吐き

```
<IfModule mod_setenvif.c>
    SetEnvIf Request_URI "/convert-date¥.php" worm
    SetEnvIf Request_URI "/crontab/" worm
    SetEnvIf Request_URI "/index.inc.php" worm
    SetEnvIf Request_URI "/modules/" worm
    SetEnvIf Request_URI "/phpmailer/" worm
    SetEnvIf Request_URI "/phpmyadmin/" worm
    SetEnvIf Request_URI "/pop3/core¥.php" worm
    SetEnvIf Request_URI "/replace/plugin¥.php" worm
    SetEnvIf Request_URI "/routines/" worm
    SetEnvIf Request_URI "/skin/" worm
    SetEnvIf Request_URI "/xmlrpc¥.php" worm
    SetEnvIf Request_URI "/ws/get_events¥.php" worm
    SetEnvIf Request_Method "SEARCH" worm
</IfModule>
.....
<VirtualHost 133.83.35.54:80>
    CustomLog "|/usr/bin/logger -t apache:133.83.35.54 -i -p security.info" combined env=worm
</VirtualHost>
```

課題

- socks があればかなりのことができる
  - Winny できます（笑）
  - socks = ssh の動的ポートフォワーディング
  - ログ……
- コネクション flood 系の攻撃に弱い
  - 意図しない「攻撃」が多い
  - 自動系は使わない点と諸刃
- Web を利用するマルウェアの増加
  - ICAP（Internet Content Adaptation Protocol）を利用したコンテンツフィルタとか
    - お金ない人も squid + c-icap + ClamAV とか

メール配送系の話

理工学部のメールまわり

- MTA: postfix 2.x
  - サーバ台数：3
  - Rgrey（**S25R + greylisting**）を使った spam 対策（2005～）
    - http://k2net.hakuba.jp/rgrey/
    - **S25R：Selective SMTP Rejection**
    - spam 数が 1/6 程度に減少（当社比）
    - ウイルスメール数が 1/10 程度に減少（当社比）
  - amavisd-new を使ってウイルスチェック
    - Sophos AntiVirus (Sophie – SAV Interface を利用する daemon)
      - http://www.clanfield.info/sophie/
      - Sophie を使わないとパフォーマンス悪すぎ
    - ClamAV
      - daemon 版標準添付

失敗事例

- 大量のメールによるメール配送遅延
  - Sophos AntiVirus によるウイルスチェックが負荷に
  - Sophie 化して対応
- 素の greylisting を使うと痛い目にあう
  - SMTP を無視するサイトからのメールが届かない
  - Rgrey 化して対応（動的 IP アドレスっぽいところにだけ greylisting を適用）
- ClamAV が phishing メールをうまく検出できないことがある
  - phishing ルールのいくつかはメールヘッダも見ているようだ
  - amavisd-new はメールを分解してボディだけをアンチウイルスに食わせているっぽい→よって検出できない
  - postfix 2.3 以降の milter 機能を併用して対応→clamav-milter を postfix で利用する

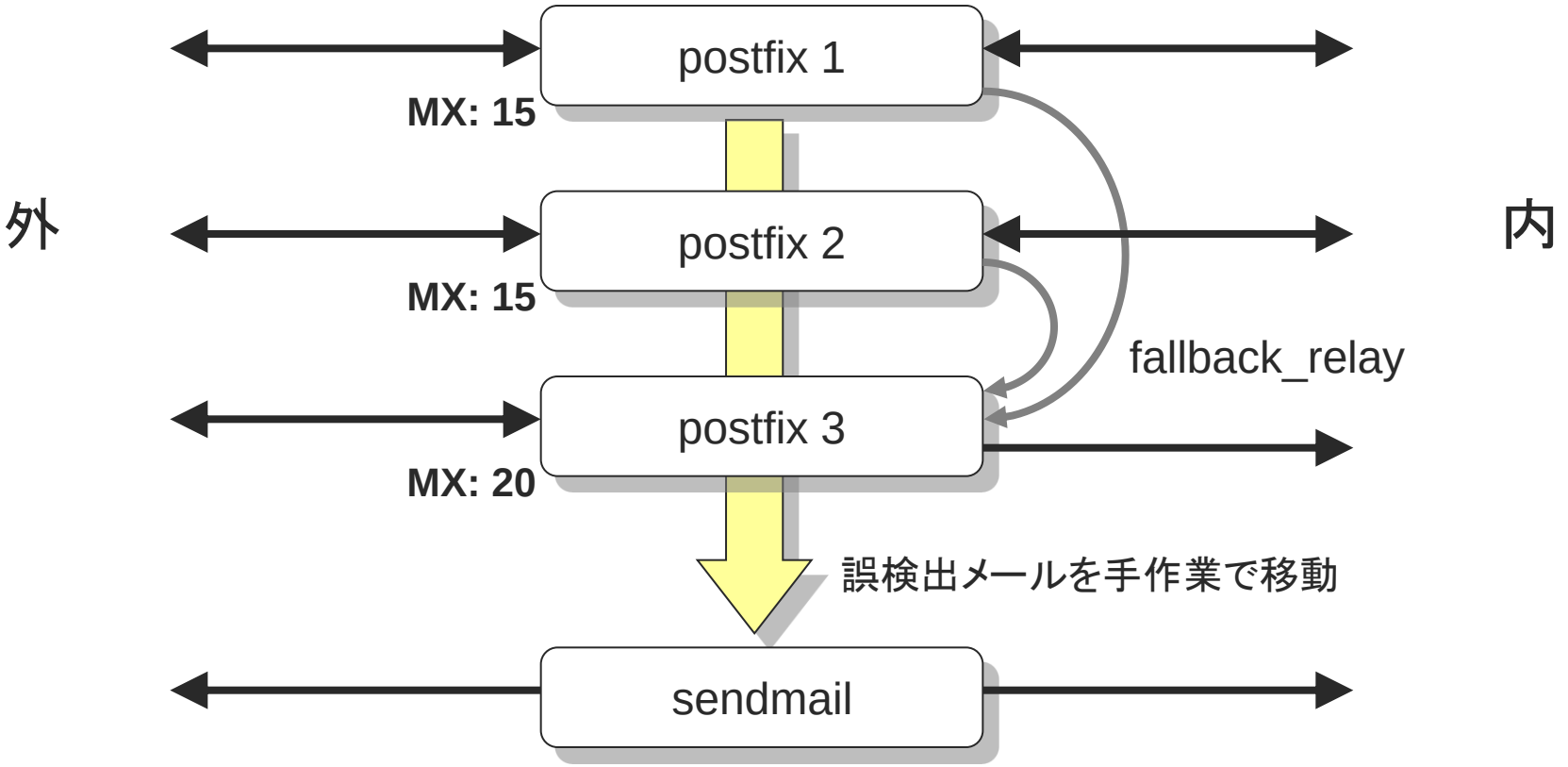
postfix と clamav-milter

- http://www.postfix.org/MILTER_README.html
- main.cf
  - smtpd_milters = unix:/var/run/clamav/clmilter.sock
  - milter_default_action = accept
- postfix から/var/run/clamav/clmilter.sock にアクセスできるように設定しておく
  - chgrp postfix /var/run/clamav/clmilter.sock
  - chmod g+rwx /var/run/clamav/clmilter.sock
- smtpd を chroot している場合は注意（master.cf）
  - chroot しないようにするか、あるいは chroot 先からアクセスできるように設定する

失敗事例

- メールの滞留状況がわかりづらい
  - MX が低位のサーバに fallback するようにした
    - fallback_relay = fallbackmx.st.ryukoku.ac.jp
  - queue を削除する場合も fallback 先だけで処理すればいいので楽
  - MX が上位のサーバの負荷低減にもなる
- 誤検出すると再送できない（再送するとまた誤検出するので）
  - アンチウイルスを通さないホストを用意する
  - 一時的に特定ホストの設定を変更する

こんな感じ


外
内
postfix 1
MX: 15
postfix 2
MX: 15
fallback_relay
postfix 3
MX: 20
誤検出メールを手作業で移動
sendmail

課題

- ウイルスを直接添付するメールの減少
  - Web ページ上に設置し、spam メールでそこへ誘導する形式が増加
    - ウイルス対策の意味での spam 対策の重要性
  - そろそろ **taRgrey を試してみるべきか……**
    - http://k2net.hakuba.jp/targrey/
    - Rgrey にタールピット機能（接続遅延）を追加
    - しかし 125 秒遅延って……
- コンテンツフィルタ系の spam 対策もの?

瀬田学舎教育系の話

概要

- 2003 年検討、2004 年導入。
  - 使用期間は 5 年
- クライアント: 約 1200 台
  - Windows / Linux デュアルブート：約 750 台
  - Windows のみ：約 500 台
  - Mac: 約 70 台
- ファイルサーバ
  - EMC Celerra NS7000GS / CX700 (ユーザ領域1.2TB)
- その他、ドメインコントローラ、PC 管理システム、教室用ネットワークなど

失敗事例

- PC管理システムの仕様
  - クライアント復旧インストールシステムの機能を可能とするもの
    - Windows / Linux のクライアントバックアップ・リストアができること
    - 教室単位・1 台単位でリストアできること
    - OS を指定してのクライアントのリモート起動・停止ができること
    - ……
  - マスター・メディアからのイメージ配布・インストールが容易であること。自動化されていることが望ましい
- 失敗：パーティション単位での操作が明記されていない
  - 導入されたもの（Altiris Deployment Server）は対応していなかった orz

失敗事例：Linux

- 採択業者が提案したのは Turbolinux 10 Desktop
  - 仕様では 5 年サポートを明記
  - 提案時に「Turbolinux でいいんですか?」と念は押した（ちょうどライブドア子会社になったあたりの時期）
  - 導入業者（富士通）としては、Turbolinux 10 Desktop の通常メンテナンス終了日（2007.10.16）までに、その時点の最新のデスクトップ製品に乗りかえて対応する予定だった
  - しかし Turbolinux FUJI 以降が続かない……
  - Turbolinux FUJI の通常メンテナンス終了日は 2008.11.24 なので、2009 年の夏まで使い続けるには足りない
  - 協議継続中……

質問？