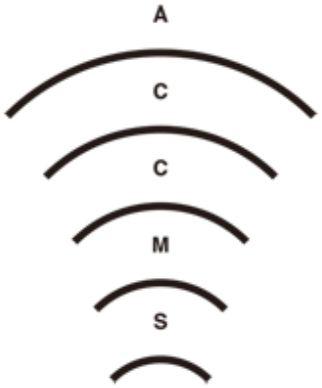


CAUA FORUM 2015
大学におけるサイバーセキュリティのこれから

大学における情報セキュリティ対策と情報セキュリティポリシーの浸透

岡部　寿男
京都大学 学術情報メディアセンター

2015年6月18日

あらまし

- 大学におけるキャンパスネットワーク運用の歴史はセキュリティインシデントへの対応の歴史でもあった。
- インターネットの導入が早期行われた大学ほど、キャンパスネットワークはオープンで、かつ草の根的な運用がなされ、セキュリティ対策は困難と言われてきた。
- 本発表では、そのような大学の典型例である京都大学でのこれまで事例をベースに、大学における情報セキュリティ対策と情報セキュリティポリシーの浸透について振り返りつつ、クラウド時代ともいわれる今日 に大学がとるべき対策について考えてみたい。

岡部寿男 : 自己紹介(1)

- 略歴
  - 1988.3　京都大学大学院工学研究科情報工学専攻修士課程修了
    - 並列計算の理論
  - 1988.4　京都大学工学部 助手
    - スパコンのコンパイラ
  - 1994.7　京都大学大型計算機センター 助教授
    - スパコンのソフト
  - 1998.4　京都大学大学院情報学研究科 助教授
    - 並列・分散アルゴリズム
  - 2002.4　京都大学学術情報メディアセンター 教授
    - ネットワーク研究部門

- 京都大学KUINSの動き
  - 1985
    - JUNETに接続
    - 学内UUCP
  - 1988
    - 基幹ループLAN
    - WIDEに接続
    - BITNETに接続
  - 1994
    - 補正予算によりサブネット化
  - 1996
    - ATMネットワークKUINS-II
  - 1999
    - ATMルータの増強
  - 2002
    - 安全なギガビットネットワーク KUINS-III

岡部寿男 : 自己紹介(2)

- 現在の肩書
  - 京都大学
    - 学術情報メディアセンター　センター長・教授
    - 大学院情報学研究科　知能情報学専攻・教授（兼担）
    - 情報環境機構　副機構長
    - 全学情報セキュリティ委員会常置委員会　委員
  - 国立情報学研究所
    - 客員教授（2005年より）
    - 学術情報ネットワーク運営・連携本部 委員
      - 認証作業部会 主査
      - 情報セキュリティポリシー推進部会 委員
    - 学術認証運営委員会 委員

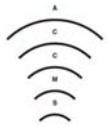
岡部寿男 : 自己紹介(3)

- CAUAでの発表
  - “京都におけるITを利用した大学の地域貢献”
    - CAUAシンポジウム2003京都　特別講演，2003年11月
  - “大学間連携のための全国共同電子認証基盤(UPKI)の現状と今後”
    - CAUA第6回合同研究分科会　～Look WEST : ICTは西に学ぶ～ 基調講演, 2007年11月

発表の流れ

- 京都大学における過去15年間のセキュリティ対策の事例を紹介

1. 京都大学の学内LAN KUINS-IIIにおけるセキュリティ対策の考え方
2. 無線LANサービスとセキュリティ
3. 京都大学の情報セキュリティポリシーと中期計画に基づくセキュリティ対策
   - サンプル規程に基づく政府統一基準準拠のポリシー（平成２１年度より施行）
   - 統合認証システム
4. 最近のインシデント例

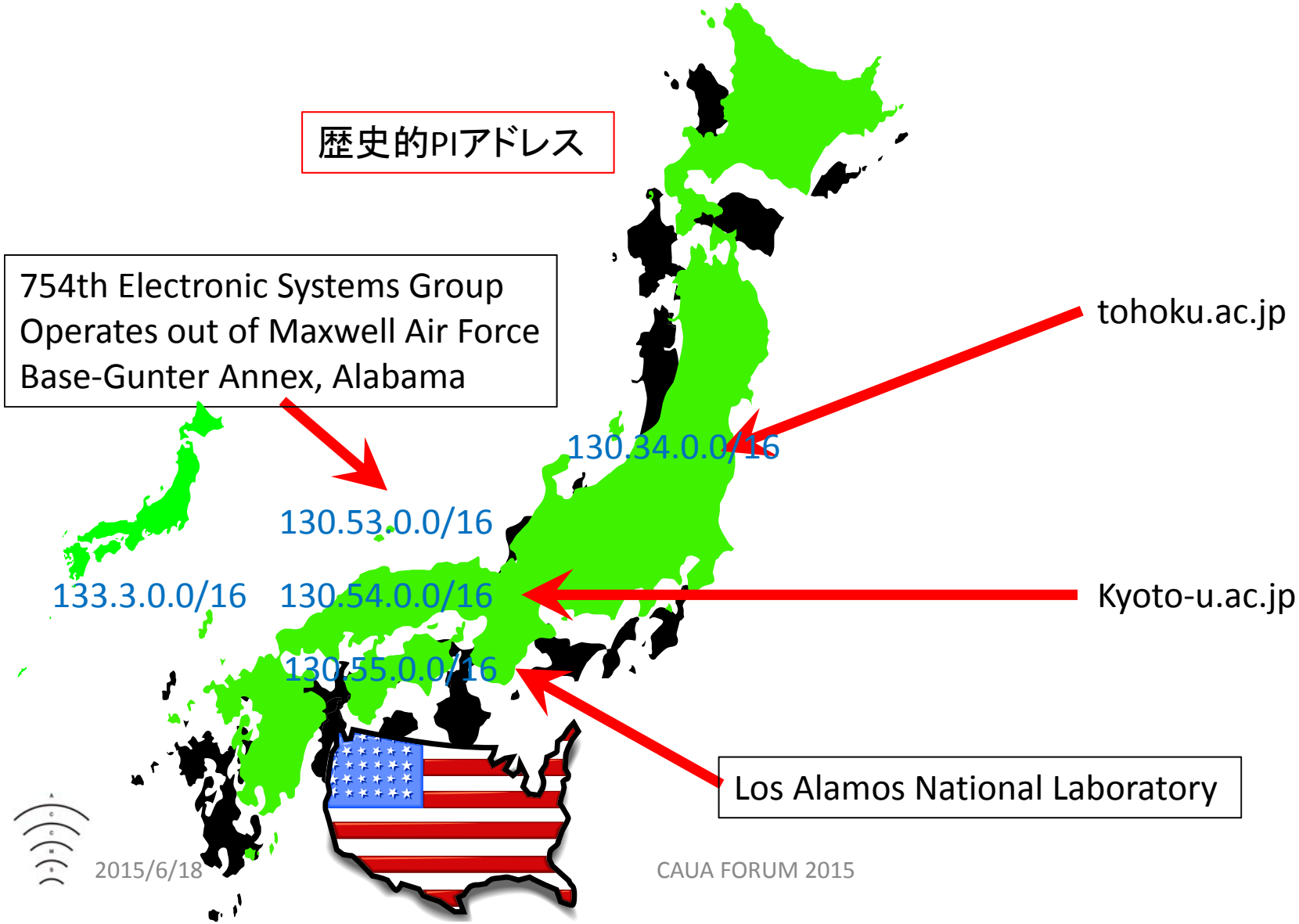


おことわり

- （立場上）サクセスストーリーとして話します。
  - 実際には、スライドに書けないことがいろいろあります。
    - 特に最近の話題…
- もし、京都大学でのセキュリティ対策が進んでいるように見えたら、それは錯覚です。
  - セキュリティポリシーの策定では歴史がありますが、その浸透、そしてそれに基づくPDCAサイクルは、依然（そしてますます）険しい道のりです。

京都大学の学内LAN KUINS-IIIにおけるセキュリティ対策の考え方

京都大学はどこにある？


歴史的PIアドレス
754th Electronic Systems Group
Operates out of Maxwell Air Force
Base-Gunter Annex, Alabama
tohoku.ac.jp
130.34.0.0/16
130.53.0.0/16
133.3.0.0/16
130.54.0.0/16
Kyoto-u.ac.jp
130.55.0.0/16
Los Alamos National Laboratory

平成13年頃の学内ネットワークの状況(1)

- 不正アクセスが頻発
  - グローバルIPアドレスを持つマシンが20,000台以上
  - 少なからぬマシンが甘い管理
    - ホームページ改竄、SPAM不正中継、踏み台、…
    - その筋では初級者向けクラッキングサイト？
  - IDS（不正アクセス監視装置）の警報が鳴りっぱなし
    - 平成11年運用開始（大学の入り口、FDDI 100Mbps）
      - Cisco NetRanger（元Hucom製）
    - 平成13年KUINS-III：全学10箇所に分散、1Gbps⇒警報数10倍

平成13年頃の学内ネットワークの状況(2)

- 学内ネットワーク（KUINS-II）の問題
  - KUINS機構の管理は建物の入りロルータ（全学百数十箇所）まで
    - NEC スーパーハブSH380、NEC ES100e/D4000
  - 建物内配線は部局任せ
    - トラブル・セキュリティ対応が困難
      - 「このIPアドレスを使っているマシンがどこにあるかわからない」
      - 「このネットワークケーブルの反対側がどこにつながっているかわからない」
    - 改組、耐震改修、キャンパス移転などに伴う学内移転
      - １サブネットにポリシーの異なる構成員が雑居

情報ネットワーク危機管理委員会

- 平成13年8月発足
- 最高情報セキュリティ責任者（＝情報担当理事）直属の特命委員会
  - 委員は匿名で参加
- 不正アクセス等の発生時のネットワーク緊急遮断権限
  - 第一段階は対外接続ルータでIPアドレス単位で遮断
    - 24時間365日の対応
  - 解除は部局長による申請が必要

（それまでは）

  - ネットワークの運用担当者の判断で遮断
  - 利用者からのクレームがあれば解除せざるを得ない

京都大学の
最高情報セキュリティ責任者(CISO)

法人化以前

- 総長特別補佐（情報基盤担当）
  - 土岐憲三（2001.4～2002.3）
- 副学長（情報基盤担当）
  - 西本清一（2002.4～2003.12）
  - 辻文三（2003.12～2004.3）

法人化後

- 理事・副学長（情報基盤担当）
  - 辻文三（2004.4～2005.9）
  - 松本紘（2005.10～2006.3）
  - 西村周三（2006.4～2008.9）
- 理事・副学長（情報担当）
  - 大西有三（2008.10～2010.9）
- 副理事・情報環境機構長
  - 美濃導彦（2010.10～2012.9）
- 理事・副学長（情報環境担当）
  - 江崎信芳（2012.10～2014.9）
- 理事・副学長（情報担当）
  - 北野正雄（2014.10～）

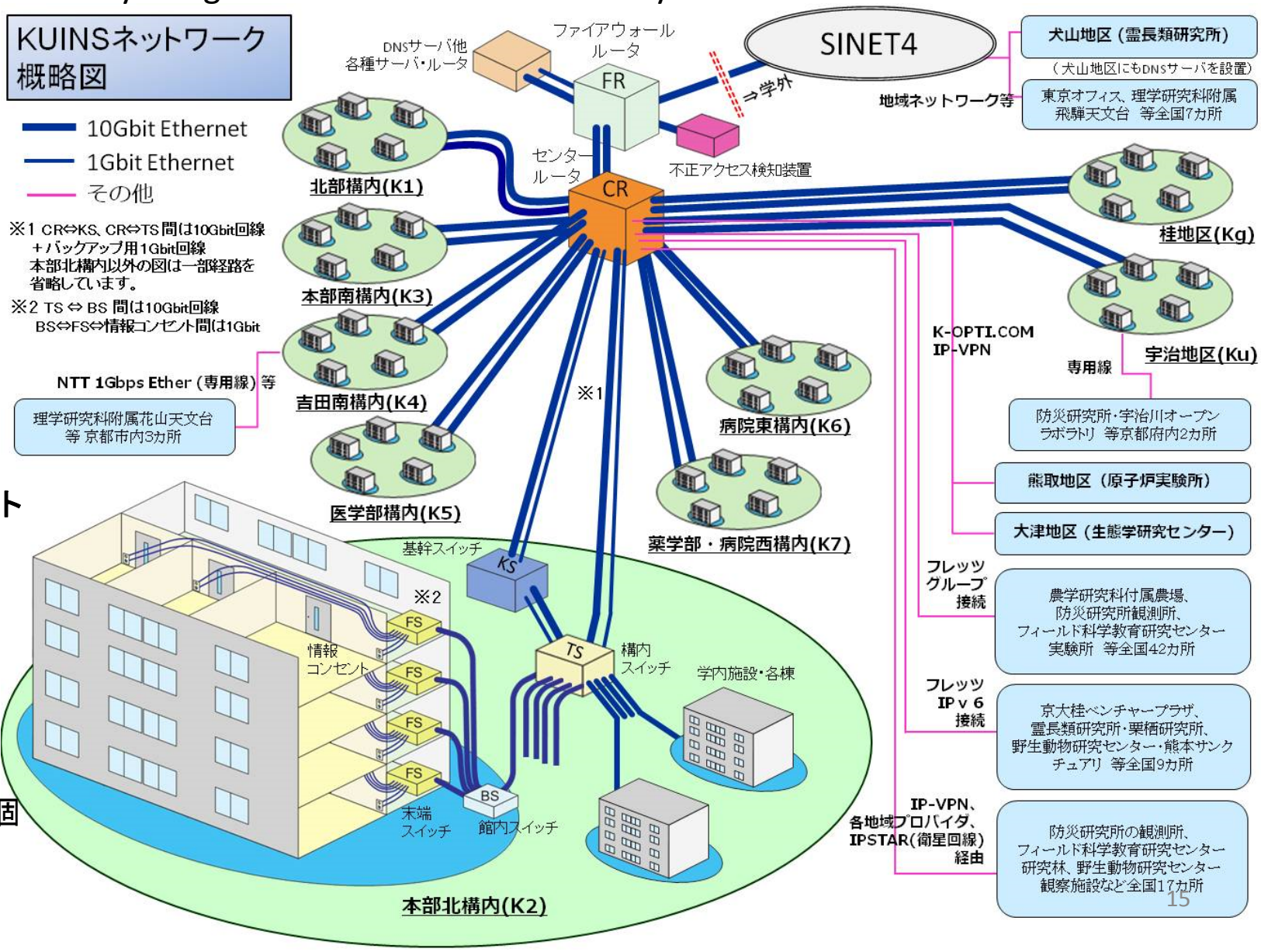
「安全なギガビットネットワークシステム」 KUINS-III

- 補正予算により平成１３年秋に導入
  - 平成11年度より概算要求準備
- KUINS-IIIの考え方
  - 新しいネットワークKUINS-IIIを新規に配線
    - 各部屋の情報コンセントまでKUINSが管理
    - ポリシーごとのVLAN
    - DHCPにより登録なしで使用できる
    - ファイアウォールを導入
      - 学外との直接の接続性はない
  - 従来のKUINS-IIは、厳格な登録制に移行
    - 計算機ごとの管理責任者を明確化
    - フィルタリングにより未登録端末からの利用を排除
      - DHCPの利用を制限

KUINSとは

京都大学の学内ネットワークの略称。（発音は「クインズ」）

Kyoto University Integrated Information Network System



情報コンセント

現在約32,000個

KUINSの規模

ネットワーク

グローバル IPアドレス： 約　2,500個
グローバル サブネット： 約　 500個
プライベート VLAN： 約　4,200個
情報コンセント： 約 21,000個
遠隔地接続： 83 箇所

ハードウエア

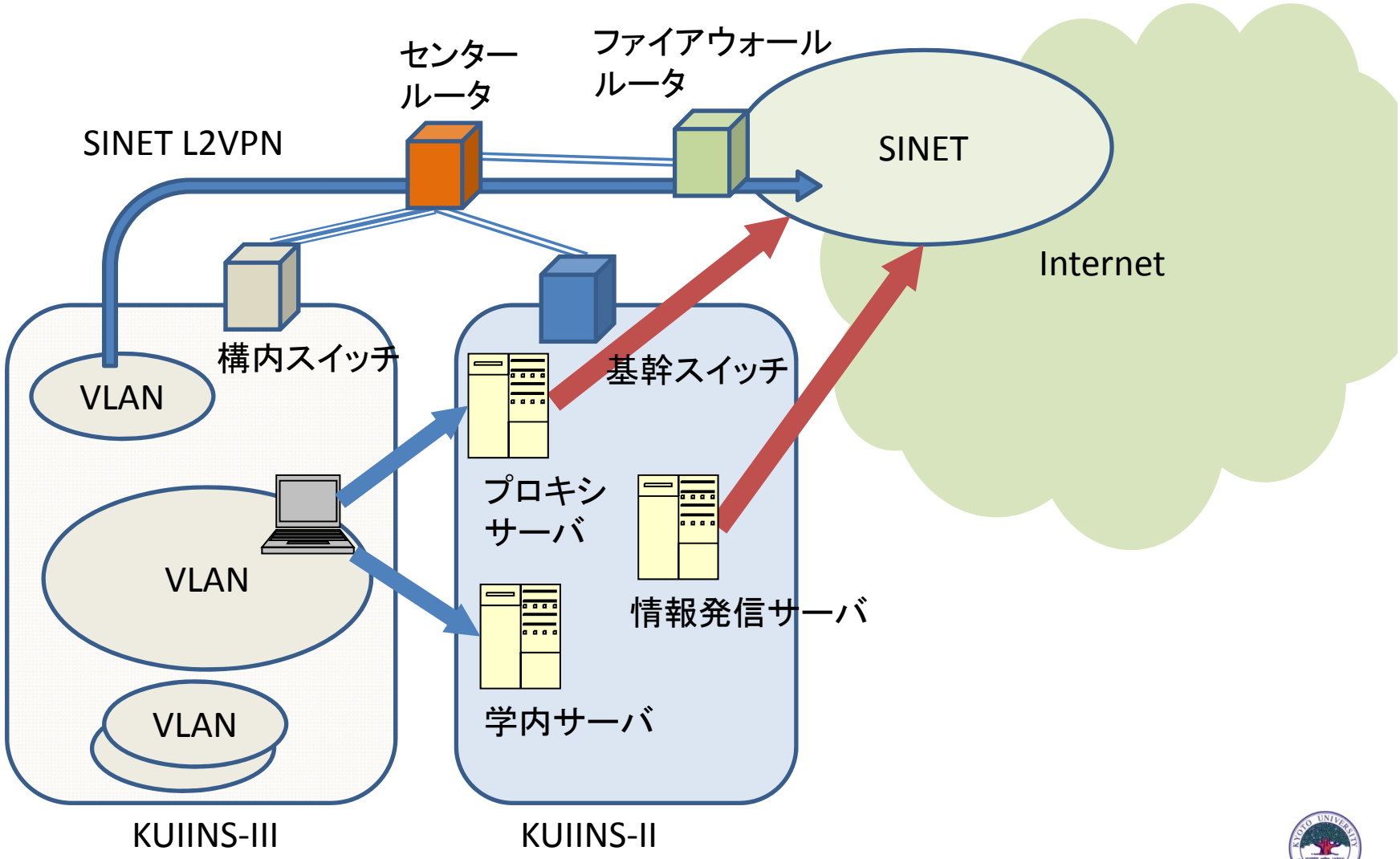
ルータ、スイッチ等

- メインルータ: 4台
（対外接続、学内接続）
- 構内スイッチ: 10台
- 基幹スイッチ:　4台
- サーバスイッチ: 3台
- 館内スイッチ: 約　250台
- 末端スイッチ: 約1,200台

サーバ類

- DHCPサーバ: 20台
- DNSサーバ: 4台
- NATサーバ: 10台
- VPNサーバ:1台
- メールー中継サーバ: 16台
- PPTPサーバ: 13台
- SSHポートフォワードサーバ: 1台
- 不正アクセス検知装置　1式
- 電子メールファイアーウオールサーバ: 2台
- SPAMメール検知サーバ: 4台
- ログ収集サーバ: 6台
- WEBプロキシサーバ: 20台

京都大学KUINSの論理構成



学術情報メディアセンター＆情報環境機構の発足

- 平成14年4月に学術情報メディアセンターが発足
  - 大型計算機センター
  - 総合情報メディアセンター〔旧・情報処理教育センター〕
  - **学術情報ネットワーク機構（学内措置）**

  の業務を引き継ぐ
- 平成17年4月に**情報環境機構**が発足
  - 学術情報メディアセンターの事務職員・技術職員を事務本部情報環境部 （旧・情報化推進部）に移管、改組
  - 学術情報メディアセンター情報サービス部の業務は、新設の全学機構である情報環境機構へ

KUINS利用負担金

- KUINS利用負担金（平成14年度より）
  - KUINS-II（グローバルIPアドレス）
    - IPアドレス1個につき月額1,500円
  - KUINS-III（プライベートIPアドレス）
    - 情報コンセントの端子あたり月額300円
  - 管理責任者（教職員）と支払責任者（教授等）の登録が必須
- なぜ負担金？
  - 責任分界点の移動による業務量の増加
    - 従来：建物の入り口まで（全学で約百数十箇所）
    - KUINS-III：各部屋のコンセントまで
      - 全学で一万六千ポート
      - VLANごとのポリシ設定
    - KUINS-IIも、端末ごとの厳格な登録性
  - セキュリティ対応業務の増加
    - IDS（侵入検知装置）による監視

  ⇒定員増では対応不可能、業務外注が前提
- 負担金制の効果
  - KUINS-IIからKUINS-IIIへの移行を推進
    - 約１年でKUINS-II登録台数は2000台強に減少、収束
  - 管理責任の明確化（研究室単位）

IPアドレス登録制の実装

【要請】
- 登録外のIPアドレスをルータで遮断（これは簡単）
- IPアドレスごとにホストのMACアドレスを登録
  →IP spoofingができない仕組み

（当初）
- サブネット外へのgatewayとなるルータのARP tableにIPアドレスとstaticに登録
  - サブネット外との双方向通信はできないが、送信元IPアドレスをspoofしたパケットが流出しDoS攻撃等の可能性は排除できない
  - 一つのIPアドレスで複数のMACアドレスの機器をつなぐ可能性がある場合には対応できない

（対応）調達時に以下の仕様を明記
「予め登録したIPアドレスとMACアドレスの組でフィルタできること」
- Cisco　Catalyst6500+ACE、Alaxalaが対応

KUINS接続機器登録データベース

1. メインメニュー
2. マニュアルメニュー
3. 承認を行う責任者に表示
4. VLANやホストの新規・変更・削除申請を行った際に表示
5. 管理責任者・支払責任者又は連絡担当者になっているVLANやホストの一覧
6. 管理責任者・支払責任者又は連絡担当者になっているドメインの一覧

セキュリティ関連業務の論文化

- 高倉弘喜，江原康生，宮崎修一，沢田篤史，中村素典，岡部寿男，**安全なギガビットネットワークシステム KUINS-III の構成とセキュリティ対策**, 電子情報通信学会論文誌 Vol.J86-B No.8 ,pp. 1494-1501, 2003年8月.
- 沢田 篤史, 高倉 弘喜, 岡部 寿男, **開放型大規模ネットワークのためのIDSログ監視支援システム**, 情報処理学会論文誌, Vol.44, No.8, pp.1861-1871, 2003年8月.

無線LANサービスとセキュリティ

MIAKOネットについて（歴史）

MIAKO　(Mobile Internet Access in KyotO)

- 2002年5月誕生
- 　～2005年3月31日　実証実験
- 2005年4月～2008年3月31日
  - 支援企業や団体や個人による運営
  - 実証実験時代の基地局は 京都アイネット株式会社が継承
- 2008年4月～　各団体による自律分散型運用の開始
  - **京都大学**
  - 国立病院機構 京都医療センター

http://www.miako.net/

MIAKOネット方式

外部からの訪問者に無料でネットワークを貸すことを前提とした
無線インターネットサービス方式

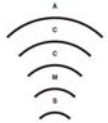
- **基地局提供者側からみると**
  - VPNプロトコル（暗号化＋認証）だけを通過させる無線基地局を一般に公開
    - MS PPTP
    - OpenVPN
    - SSH (secure Shell)
    - POP/SSL (TCP 995), IMAP/SSL (TCP 993), SMTP/SSL (465)
  - VPNプロトコル以外は通さないので、SPAM発信や掲示板荒らしなどはできない

  ⇒ 認証に伴うリスクや管理コストなし

- **利用者側からみると**
  - 基地局側での認証手続きなく直接自分の持っているVPNサーバに接続

  ⇒ VPNで暗号化されるので盗聴やなりすましのリスクなし

- **単に部外者が基地局に接続しただけでは何も出来ない。**
  - VPN接続していなければ、「みあこCAN（利用方法案内ページ）」にしか接続出来ない。



<u>VPNの普及が課題</u>

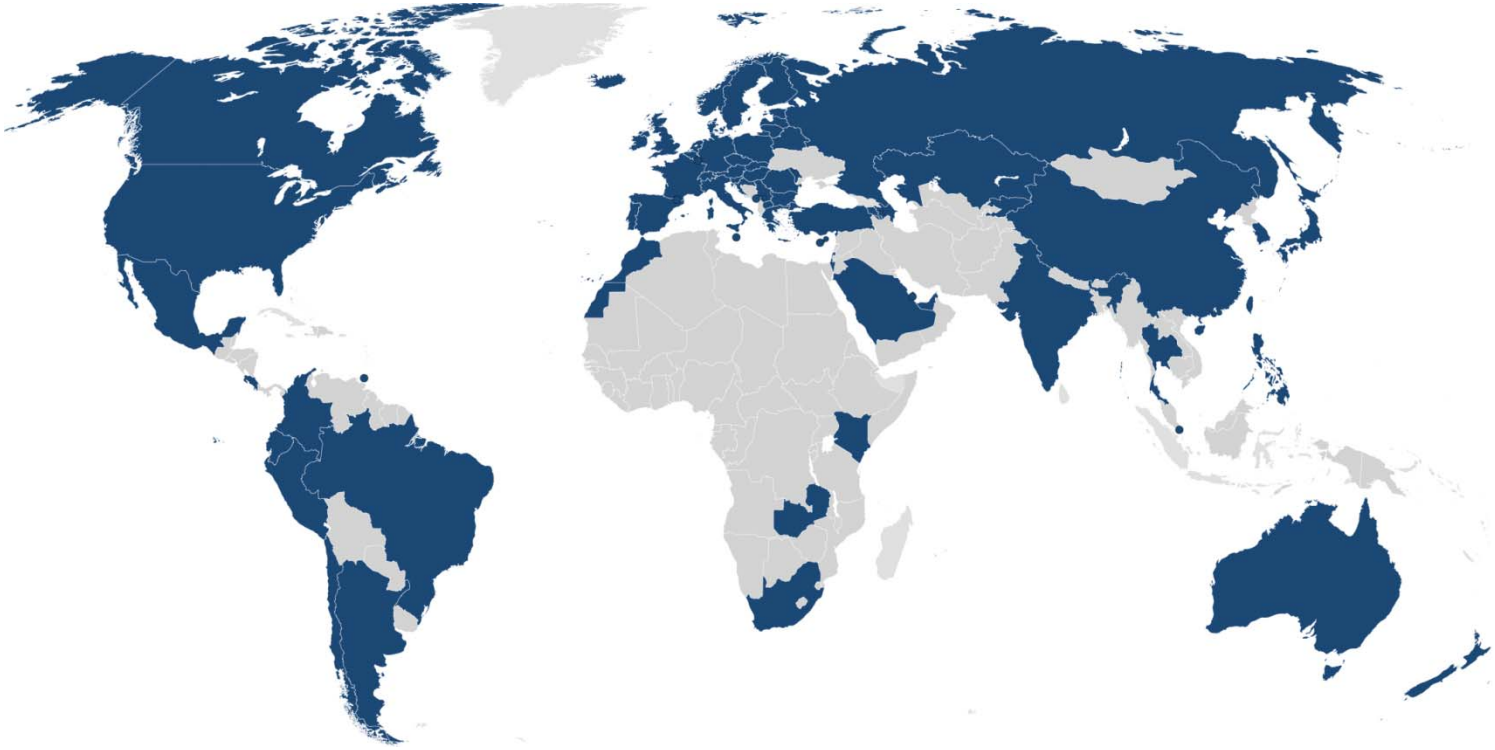
京都大学KUINSが提供する VPNサービス

MIAKOネット、eduroam、ならびに学外からの接続に利用

- MS PPTP
  - Windowsだけでなく、MacOS、iOS、Androidなども標準で対応
  - PPTP VLAN固定サービス
    - PPTP接続時に全学IDにVLAN管理番号を添えることで、当該VLAN内のリソース(プリンタやファイルサーバ)に直接アクセスできる
    - VLAN固定サービスで接続可能な利用者のリストはVLAN管理者がKUINS-DBで設定
- MS SSTP (*Microsoft* Secure Socket Tunneling Protocol)
  - MSが開発したPPP over HTTPSによるVPN
  - HTTPSが通れば使える。プロキシ越えも可
  - Windows Vista以降限定
- OpenVPN
  - Linux、MacOS、など幅広いプラットフォームに対応
- Port forward専用SSH
  - 特定のアプリのために特定のポートだけ学内にトンネル

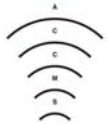
eduroam

- 欧州発祥の、学術研究機関間の無線LANローミングアーキテクチャ。
- 世界60か国で展開中
- IEEE802.1x (EAP-TTLS or EAP-PEAP)＋radius 連携



eduroam関連情報

- eduroam.jp
  - http://www.eduroam.jp/
  - 2015年6月現在、国内115機関（地域）がeduroamに参加
    - 京都大学KUINSのアクセスポイント（約1200台）はすべてeduroam対応
- eduroam 仮名アカウント発行システム
  - https://eduroamshib.nii.ac.jp/
  - 学術認証フェデレーションを利用して、所属機関の認証（京大生の場合はECS-ID）によりeduroamの仮名アカウント（最長1年有効）をオンラインで取得可能



eduroam仮名アカウント発行システム

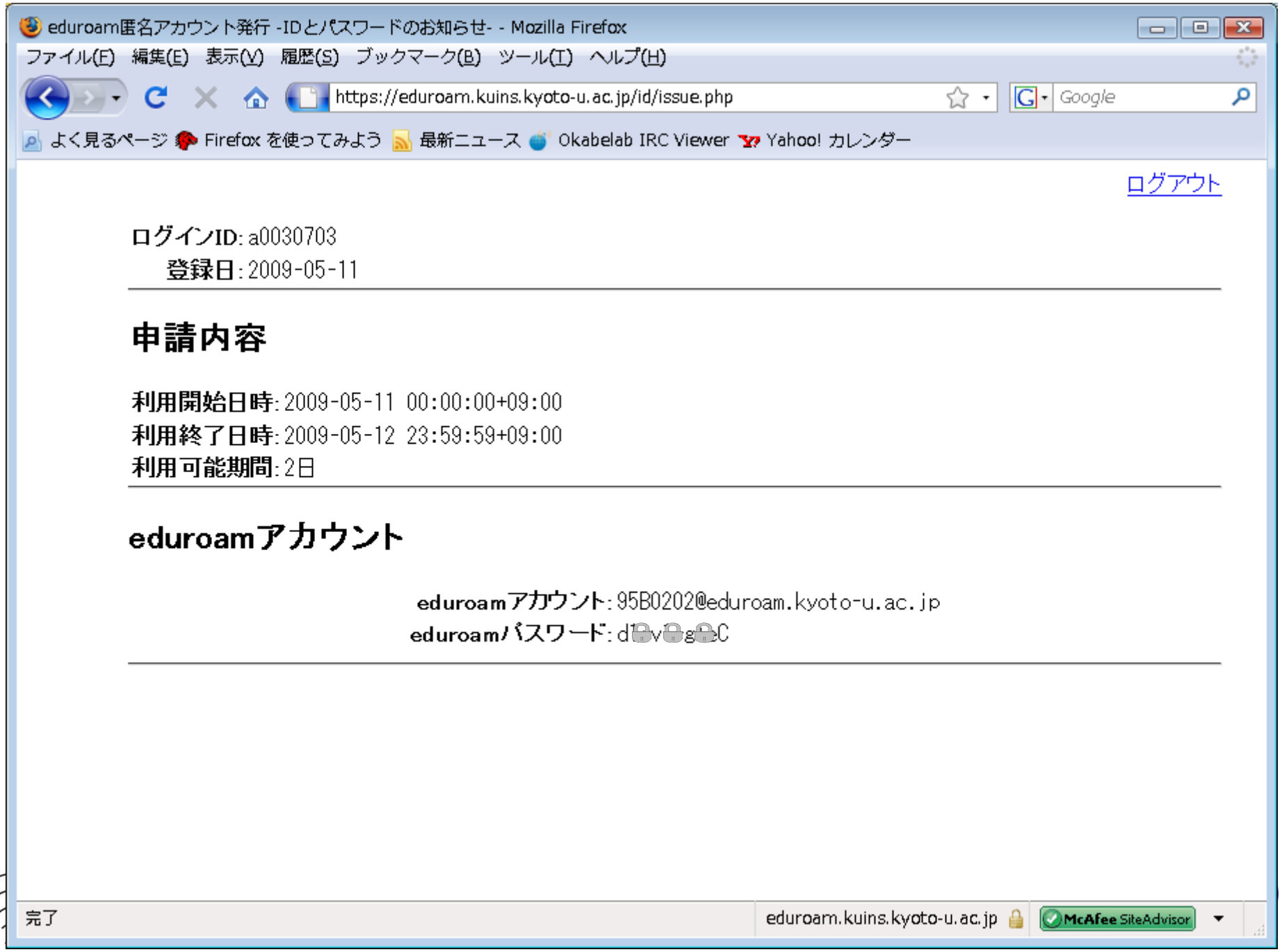
- ロケーションプライバシを守る eduroam用仮名アカウント発行システム
  - eduroamの認証に利用できるアカウントを発行
    - 学内IDとパスワードを安易に直接利用させない
  - 他大学のIdPとも連携
    - 学認のサービスとして他大学の利用者にもアカウント発行可能
  - アカウントに利用者を識別できる情報を含まない
    - 誰がどこで利用しているかのロケーションプライバシを所属機関と訪問先の双方から秘匿
  - アカウント発行時に有効期限を設定可能
    - １日～数ヶ月の範囲で選択可能
    - 出張時などに使い捨て利用を想定

仮名eduroamアカウント

ID体系: YMDSLNN@upkiroam.jp

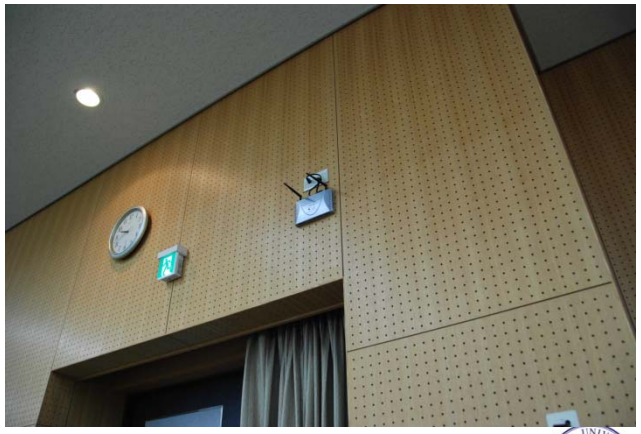
[Y]　発行年西暦下一桁 [0-9]
[M]　　発行月 [1-9a-c]
[D]　発効日 [1-9a-v]
[S]　利用開始日 (発効日からのオフセット) [0-9a-z]
[L]　　有効期間 [0-9a-z]
[NN] 同一発効日内での通し番号 [00 – zz]

- 各大学IdPで認証し、個人の識別情報を受け渡さずSSO連携
  - 本システムへ必要以上の情報を送らない
  - 本システムで発行したアカウントで不正なアクセスが行われた場合、ログから認証したIdPを抽出してIdPへ問い合わせ


eduroam匿名アカウント発行 -IDとパスワードのお知らせ- - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
https://eduroam.kuins.kyoto-u.ac.jp/id/issue.php
Google
よく見るページ Firefox を使ってみよう 最新ニュース Okabelab IRC Viewer Yahoo! カレンダー
ログアウト
ログインID: a0030703
登録日: 2009-05-11
申請内容
利用開始日時: 2009-05-11 00:00:00+09:00
利用終了日時: 2009-05-12 23:59:59+09:00
利用可能期間: 2日
eduroamアカウント
eduroamアカウント: 95B0202@eduroam.kyoto-u.ac.jp
eduroamパスワード: d
v
g
C
完了
eduroam.kuins.kyoto-u.ac.jp
McAfee SiteAdvisor

eduroam対応無線LAN アクセスポイントの展開

- 全学のアクセスネットワーク整備と連携して無線LANアクセスポイントを展開
  - アライドテレシス TenQ AT-TQ2403
  - 現在1000台以上稼働
  - Eduroam方式、MIAKOネット方式の併用
    - 学内学外者も利用可
      （学内LANとは別のアドレスブロックを割り当て）
  - KUINS Air（後述）にも対応（H27から）



新システムの導入

- 平成26年度から3年計画
  - BYODを想定した無線LAN環境の充実
  - IEEE802.11ac対応のAPを新たに導入
  - 集中管理
- 新サービス
  - KUINS Air
    - WPA-EAP (EAP-PEAP)により全学IDで直接利用可
    - 旧APにも展開
  - キャリアWi-Fi
    - 0000docomo, Wi2_club, mobilepoint

公衆無線LANサービス Captive Portalの問題

- 暗号化なし、あるいは暗号化にWEPを利用しているものが多い
  - WEPキーは契約者にのみ公開の建前でも検索すれば誰もが入手可
- キャプティブポータルにて認証
  - 盗聴あるいは偽基地局の設置によるパスワードの奪取が簡単
- 認証後はMACアドレスで端末を識別
  - MACアドレスを偽装すればセッションハイジャック可

京都大学の
情報セキュリティポリシー

京都大学における情報セキュリティポリシー

http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/regulation/index.html

情報セキュリティポリシー

- 京都大学における情報セキュリティの基本方針（H14年12月制定、H27年4月再制定）
- 京都大学の情報セキュリティに関する規程（H15年10月制定、H19年9月改正、H27年4月改正）
- 京都大学情報セキュリティ対策基準（H15年10月制定、H21年3月改正、H27年4月改正）
- 京都大学情報格付け基準（H21年3月制定）
- 京都大学情報セキュリティ監査規程（H21年3月制定）

情報倫理に関する規定

- 京都大学情報資産利用のためのルール（H16年3月制定、H19年9月改正、H27年4月改正）

実施手順

- 京都大学情報セキュリティポリシー実施手順書（標準版）
  （H15年10月以降、部局ごとに策定；雛型を全学に提供）
- 京都大学情報の格付け及び取扱い手順書
- 部局情報システム管理表（例）

全学情報システム利用規則

- 京都大学全学情報システム利用規則（H25年2月改訂）
- 京都大学全学情報システム利用者パスワードガイドライン
- 京都大学全学情報システム不正プログラム対策ガイドライン
- KUINSに接続する無線LAN設置のガイドライン（H24年2月制定）

京都大学における最初の情報セキュリティポリシー（平成15年版）の考え方

- 平成１５年度に制定（法人化直前）
  - 「 大学における情報セキュリティポリシーの考え方」（H.12）がベース
- 部局自治を基本
  - 部局情報セキュリティ責任者（＝部局長）に強い権限と重い責任
  - すべての部局が対等の立場
    - 学術情報メディアセンターやKUINSを特別扱いしない
  - 全学レベルでは「基本方針」・「規程」・「対策基準」・「利用のルール」のみを規定
    - 実施手順は部局ごと、ただし事務用実施手順については雛型を提供
- 重要事項は全学情報セキュリティ委員会で決定
  - 最高情報セキュリティ責任者＋全部局長で構成
- 全学情報セキュリティ幹事会
  - 部局情報セキュリティ幹事（＝セキュリティに関する実務を行う教員、事務職員、技術職員）の間の「連絡調整」

国立大学法人京都大学　中期目標・中期計画

http://www.kyoto-u.ac.jp/ja/profile/operation/medium_target/

<u>中期目標</u>

- Ⅵ その他業務運営に関する重要目標
- ３ 情報基盤の整備・活用に関する目標
- 3-1 **情報セキュリティに関する基本方針**
  - 大学が一体となって情報セキュリティ対策に取り組むための責任ある情報基盤組織を構築し、その機能と責任を明確化する
  - 情報システムを通じて取り扱う多様な情報について、重要度と公開性に応じた情報の分類に努めるとともに、情報の管理責任及び管理方法を明確化する
  - 情報セキュリティ対策の評価、情報システムの変更、新たな脅威の発生等を踏まえ、対策基準の点検・評価の定期的実施を通じて基本方針の見直しを図るための体制を構築する。

中期計画

Ⅴ　その他業務運営に関する重要目標を達成するためにとるべき措置

３ 情報基盤の活用・整備に関する目標を達成するための具体的な措置

3-1 情報セキュリティに関する具体的な施策

- 情報システムの設置場所に管理区域を設置するなど物理的なセキュリティ対策を講じる。
- 学内者による外部への不正アクセスを防止するために技術的な対策を講じるとともに、罰則規定を定める。
- 情報セキュリティに関する責任者とその権限の範囲を明確にし、全構成員に基本方針の内容を周知徹底するなど、十分な教育と啓発活動に努める。
- 学内情報資産への侵害が発生した場合における運用面での緊急時対応の計画を策定する。
- 学内情報基盤への接続に対する認証システムを構築し、セキュリティレベルの高い情報基盤活用サービスを全学に提供する。
- 各部局等における情報セキュリティの実施状況に関する監査体制を整備するとともに、管理担当者の育成と適正な配置に努め、大学全体として情報セキュリティレベルの向上を図る。
- 毎年全学版の「情報セキュリティの対策基準」及び各部局で取りまとめた「実施手順」の見直しを行い、情報セキュリティレベルの向上を具体的に図る。

中期計画に基づく具体的な施策

1. 「学内者による外部への不正アクセスを防止するために技術的な対策を講じるとともに、罰則規定を定める。」
   - 情報資産利用のためのルールの改正
   - 情報ネットワーク倫理委員会の設置
     - 倫理委員会による違反行為の停止命令・措置、調査
     - 違反行為者に対する措置に関する「意見」
2. 「情報セキュリティに関する責任者とその権限の範囲を明確にし、全構成員に基本方針の内容を周知徹底するなど、十分な教育と啓発活動に努める。」
   - 情報セキュリティeラーニングシステムの導入と義務化
3. 「学内情報基盤への接続に対する認証システムを構築し、セキュリティレベルの高い情報基盤活用サービスを全学に提供する。」
   - 個人認証検討委員会の設置
   - 職員証・学生証ICカード化を含む全学統合認証システムの導入
4. 「毎年全学版の『情報セキュリティの対策基準』及び各部局で取りまとめた『実施手順』の見直しを行い」
   - サンプル規程に基づくポリシーの改正

京都大学統合認証システム

- 情報環境機構が運用し全学で利用
- ID/passwordとICカードを併用
- 教職員系と学生系と2系統
  - 教職員(SPS-ID)：約11,000
    - yasuo123okabe（氏名のローマ字＋数字）
  - 学生等(ECS-ID)：約23,000
    - a0032109

統合認証システムで使うICカード

役員・認証カード(常勤教職員)

認証ICカード(非常勤教職員)

学生証

施設利用証(その他)

政府統一基準準拠に向けての情報セキュリティポリシーの改正（平成20年度）

- 「高等教育機関の情報セキュリティ対策のためのサンプル規程集」を活用
  - 「基本方針」（部局長会議了承）、「規程」（達示）は現行のものをもとに修正
  - 現「対策基準」（総長裁定）は一旦廃し、「情報システム運用・管理規程」を本学向けに読み替えて新「対策基準」（理事裁定）とする

    できるだけサンプル規程をそのまま活用する
- 平成21年4月より施行

サンプル規程を利用するにあたっての課題と解決（1）

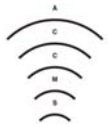
- モデルの違い
  - 本学の旧セキュリティポリシー
    - 部局自治の原則ならびにすべての部局が対等であるとの考え方の下に、全部局長からなる全学情報セキュリティ委員会が対策基準までを決定するが、対策の実施責任はそれぞれの情報システムを運用する部局が負う。
  - サンプル規程集
    - 「管理運営組織」（A大学の例ではメディアセンター）が「全学情報システム」の運用責任を持ち、全学のアカウント管理など一切を担う

サンプル規程を利用するにあたっての課題と解決（2）

- 現状と方向性
  - 本学では情報環境機構が全ての情報システムに責任を持つことは現状にそぐわない
  - しかし、徐々にその方向へと舵を切っていくべき
- 新ポリシーでの実装
  - 「管理運営組織」を情報環境機構とする。
  - 最高情報セキュリティ責任者は、全学の情報基盤として供される本学情報システムのうち、情報セキュリティが侵害された場合の影響が特に大きいと評価された情報システムを「全学情報システム」として指定する。
  - 「全学情報システム」として指定されたシステムの運用・管理は「管理運営組織」すなわち情報環境機構が行う。
  - 「全学情報システム」の利用規程は、全学レベルの規程として最高情報セキュリティ責任者が定める。
- 「全学情報システム」として以下を指定
  - 学内LAN（KUINS）
  - 統合認証システム

サンプル規程を利用するにあたっての課題と解決(3)

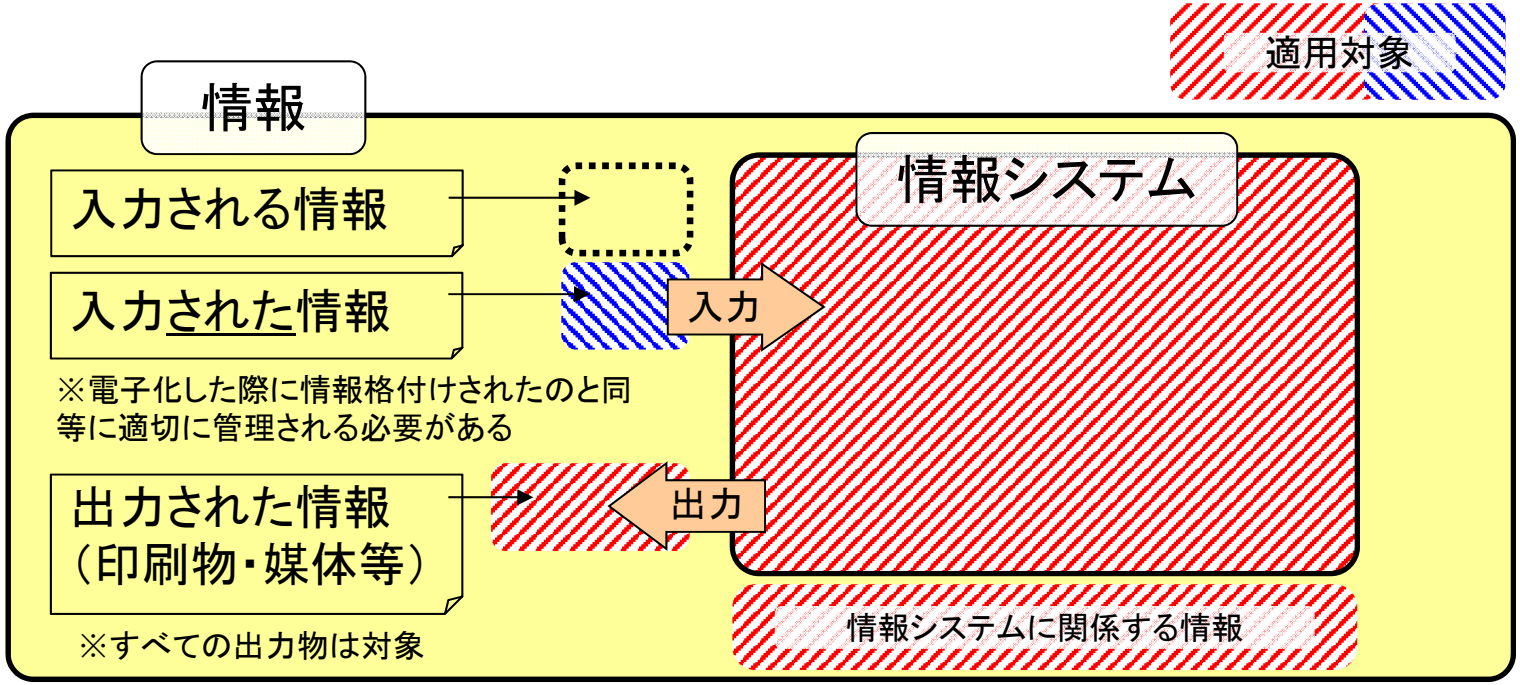
- 重要な情報の扱い
  - 旧ポリシーでは、重要な情報を(細かい格付けをせず一律に)「特定情報」として部局長が指定
    - 指定や管理のオーバヘッドが大きい
  - サンプル規程では、格付けを、情報を入手または生成した教職員が行う。
    - 指定や管理は容易だが、重要な情報がどこにどれだけあるかのリストを部局長が持つ保証がない？
- 以下の点を確認
  - 「文書管理規程」「個人情報保護規程」などでリストの作成が義務付けられている情報については、格付けと取扱い制限をそれらに準じたものとする。



情報とは

― 情報セキュリティ対策は、以下の情報に対して適用されます。

○ 情報システムに格納されている情報
○ 情報システム外部の電磁的記録媒体に記録された情報
○ 情報システムに関係がある紙に記載された情報



情報のライフサイクルにおける対策

情報のライフサイクル（情報の作成・入手から消去される間）のそれぞれにおいて発生する脅威に対して措置を講じることが必要です

【情報のライフサイクルにおける対策】

- ○ 情報の作成・入手 → 格付け及び取扱制限の明示
- ○ 情報の利用 → 持出し・複写・配付等の制限
- ○ 情報の保存 → 暗号化・アクセス制御の実施
- ○ 情報の移送 → 部局情報セキュリティ責任者への許可申請・届出
- ○ 情報の公表・提供 → 部局情報セキュリティ責任者への許可申請・届出
- ○ 情報の消去 → 抹消ソフト等の利用

情報の格付けと取扱制限

- 情報の作成者又は入手者が、当該情報の重要性や講ずべき情報セキュリティ対策を他の者に認知させ、明確化するための手段が「格付け」と「取扱制限」です。
  - 「格付け」は、京都大学共通の指標です。「取扱制限」は必要に応じて各部局で個別に採用・追加することができます。

格 付 け

情報の重要性や価値等を主体的にランク付けすることです。情報を作成又は入手し管理を開始する前に、機密性、完全性、可用性の観点から（書面については機密性のみ）定義に基づいて決定します。

すべての情報に必須

取扱制限

情報を取扱う際の制限事項です。機密性、完全性、可用性の観点から複製禁止、持出禁止、再配布禁止、暗号化、読後廃棄などと決定します。

情報に応じて任意

【機密性】 情報へのアクセスを許可された者だけがこれにアクセスできる状態を確保すること。

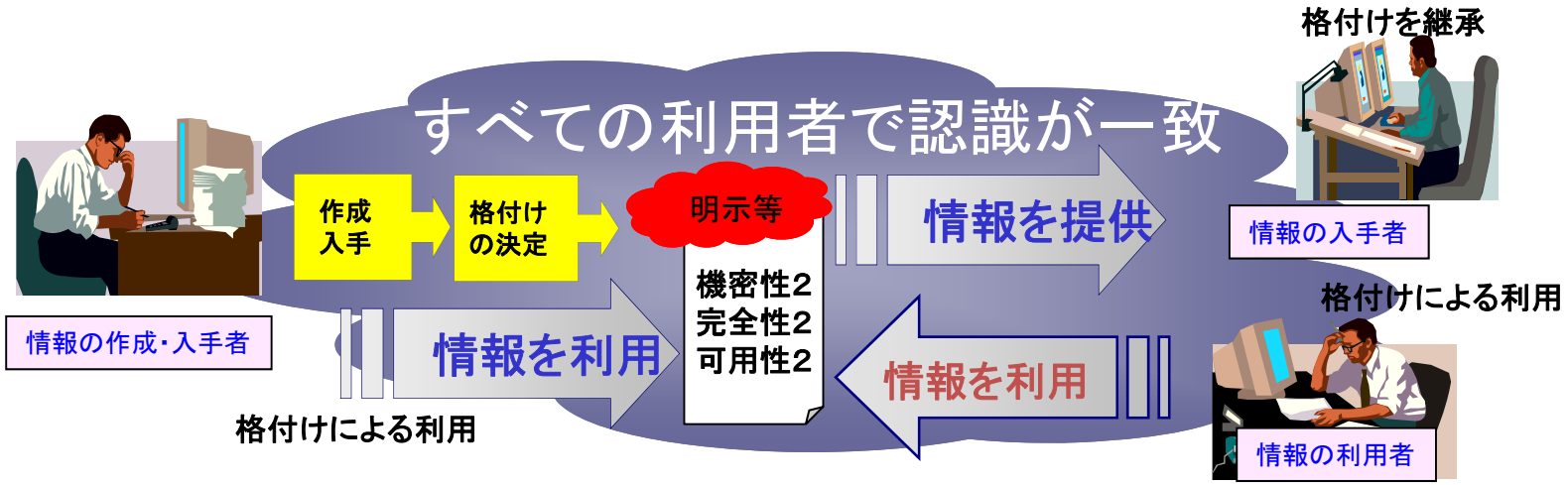
【完全性】 情報が破壊、改ざん又は消去されていない状態を確保すること。

【可用性】 情報へのアクセスを許可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること。

情報の作成と入手

教職員による格付け・取扱制限の決定・変更

- 情報を作成した時又は情報を入手しその管理を開始する時に、機密性・完全性・可用性の観点（書面については機密性のみ）から、格付け及び取扱制限の定義に基づき決定します。
- 情報の格付け及び取扱制限の変更には、大別して**再決定**と**見直し**があります。



情報の利用と保存

情報の利用

- 業務の遂行以外の目的で情報を作成、入手又は利用しないよう努めなければなりません。
- 教職員は、取り扱う情報に明示された格付けに従って、当該情報を取り扱って下さい。格付けに加えて、取扱制限の明示がなされている場合には、当該取扱制限の指示内容に従って当該情報を取り扱う必要があります。

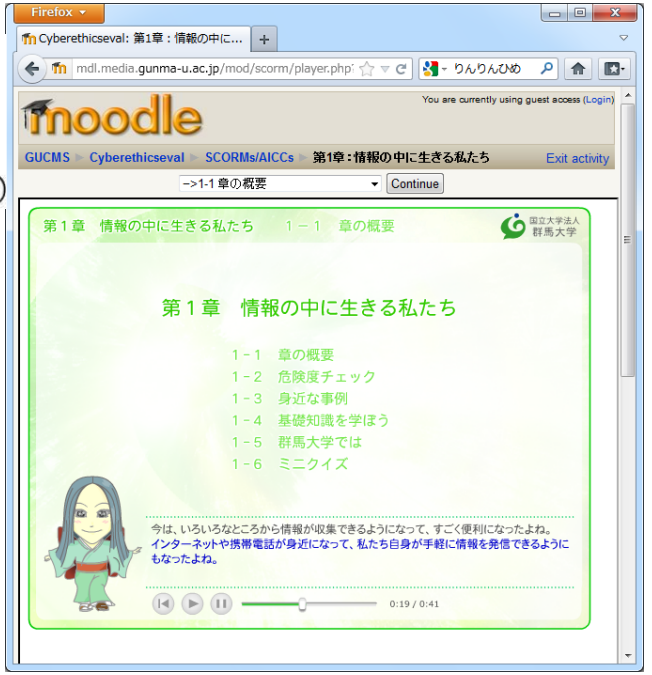
情報の保存

- 業務の遂行以外の目的で要保護情報を電磁的記録媒体に保存してはいけません。
- 電磁的記録媒体に保存された要保護情報について、保存の理由となった業務の遂行目的が達成された等、保存する理由がなくなった場合には、速やかに当該情報を消去して下さい。

…

情報セキュリティe-Learning

- 平成18年より本格運用
  - セキュリティポリシーにより、学生・教職員とも受講義務
    - ただし今のところ罰則なし
- 目的
  - 中期計画に基づき、全学全構成員にセキュリティポリシーを周知させる
- コンテンツ
  - Infoss情報倫理（H24年度まで）
    - 京大の要望で英語化
  - りんりん姫（H25年度～）
    - 4か国語対応
  - 京大オリジナルコンテンツ
    - NIIセキュリティポリシー推進部会作成のものがベース
- CMS
  - Moodle（H20～H23年度）
  - Sakai（H24年度）
  - 学認連携Moodle講習サイト（H25年度から）
- 課題
  - 受講率の維持
    - 受講者名簿を各部局長へ送付
    - 1回生時の授業での周知を推奨
    - 利用制限などの導入も検討
  - E-learningの適用が困難な部局の対応
    - 附属病院の看護師向けには別途講習会を開催

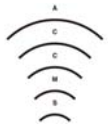


情報セキュリティ対策掛の活動

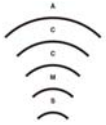
- 情報セキュリティ対策室が平成17年度に発足
  - 専任教員（教授）1名＋技術職員２名
- 学内のセキュリティ向上のための啓発活動、広報活動、支援活動、学内・学外連絡窓口
  ⇒情報セキュリティe-Learningの運用
- 情報セキュリティポリシー策定・改定等事務
- 不正アクセスの監視とインシデント対応
  - IDSの監視（24時間365日の監視を外注）
  ⇒外部からの攻撃を遮断することで侵害を防止、
  内部の問題については速やかに部局へ連絡
  - 関係省庁との折衝、報道機関対応
- 監査業務補助

BCP

- 東日本大震災を契機に、東南海地震への対応が求められる
  - 安否確認システム、…
- 具体策
  - DNS secondaryの犬山への設置
  - 学生用全学メールのOffice365へのアウトソース
  - 「汎用コンピュータシステム」、いわゆる“アカデミックプライベートクラウド”
    - 富士通（株）館林データセンターにシステムの一部（ラック1本）をハウジング
    - 教職員用全学メールを含む重要サーバをホスティング
  - 学術情報メディアセンター北館の“データセンター化”
    - 72時間対応の発電機を設置
    - 重要ネットワーク機器を電話庁舎から移設



最近のインシデント例



GhostShellによる国内大学への不正アクセス

- GhostShellと名乗るグループが2012年10月2日、全世界の有名大学へ不正アクセスして入手したとされるデータをインターネット(Pastebin)上に公開
  - 日本の大学は、東京大学、京都大学、東北大学、名古屋大学、大阪市立大学
- 各大学の状況
  - 東大:5サイト
    - 個人情報漏洩:メールアドレス約2,700名分、氏名1,300名分他
  - 名大:2サイト
    - 当初個人情報漏洩なしと発表(10/7)するも、後日(10/10)シンポジウム参加者名簿(193名分)、教員一覧(69名分)の情報漏洩の可能性を公表
  - 本学:2サイト
    - 個人情報漏洩なし

本省、捜査機関、報道機関への情報提供を一元化

フィッシングメール

- 2012年度1年で4回の大規模攻撃
  - 2012年5月、8月、12月、2013年1月
- 次第に巧妙化
  - 1月の攻撃では学生用メール(KUMOI)そっくりの画面でECS-IDとパスワードの入力を要求
  - パスワードを奪取された例はあるが、具体的な被害は未確認
    - 他大学ではパスワードを奪われSPAM発信などの踏み台に利用された事例も

京大バイト、生協バイト情報と称するスマートホンアプリ

- 学内において、「京大アルバイト情報リーダー」等と記載された掲示
  - 本学ならびに京大生協とは無関係
- GooglePlay（Androidスマートホンの公式アプリサイト）にアプリが登録されている
- 「利用時には京都大学の学内システムのメールアカウントが必要」
  - 実際にはWeb経由で学生メール(KUMOI)にアクセスに行き、アプリがECS-IDとパスワードを奪取しているわけではない模様

不正B-CASカード作成事件

- 2012年6月、京大職員が、有料テレビを無料で見られるように不正な「B-CASカード」を作成した等の疑いで、電磁的記録不正作出・同供用の疑いで京都府警に逮捕された。
  - 起訴→有罪
- 同職員は、自分のブログで不正カードの作成方法を公開、さらに「平成の龍馬」と名乗り、ネットに書き込み

  「カードの所有権がユーザーにあれば、改造しようがどうしようがユーザーの自由。刑事罰を科すことはできない」

その他の話題

- 2012/5
  - あるプロジェクトで取得していたドメインが、終了後、悪用されていたことが発覚
- 2012/12
  - 学生募集の説明会申込みサイト（外部委託）のプライバシーポリシーが、業者のもののまま公開されていた
- 2013/8,9
  - グループメールサービスの設定不備

などなど

まとめ

まとめ

- 京都大学における情報セキュリティ対策の取組の歴史と、それを支える情報セキュリティポリシー策定について紹介
- 情報セキュリティ対策は「人」中心
  - 技術だけではだめ
  - ポリシーを作っても飾っておくだけではだめ
  - ポリシーを構成員に理解させても、実施できる枠組みがなければだめ

    （京都大学でも…）
  - あえて一つポイントをあげるとすれば、最高情報セキュリティ責任者のリーダシップが重要

みなさまのご参考になれば幸いです。