地方の中小規模大学である鳥取大学における セキュリティへの取り組みと課題について

鳥取大学
総合メディア基盤センター ICT基盤研究開発部門
大森 幹之
<ohmori@tottori-u.ac.jp>

鳥取大学
Tottori University

SS研ICTフォーラム2016 2016年8月23日

Table of Contents

- 自己紹介
- 鳥取大学の規模と鳥取大学ネットワークTUINS
- 地方の中小規模大学が抱える課題
- 地方の中小規模大学の利点
- 鳥取大学でのセキュリティへの取り組み
- まとめ

鳥取大学
Tottori University

自己紹介

鳥取大学
Tottori University

自己紹介

- 氏名: 大森 幹之 (おおもり もとゆき)
- 出身: 島根県 (鳥取県の隣)
- 勤務地: 鳥取県 (島根県の隣), 3年前に転職
- 出身大学: 九州大学
- 専門: インターネット, コンピュータネットワーク, モバイルネットワーク, 経路制御
  - 大学4年次には, 富士通製のICカードを用いた認証基盤といったセキュリティの研究に従事

鳥取大学 Tottori University

鳥取大学の規模と
鳥取大学ネットワークTUINS

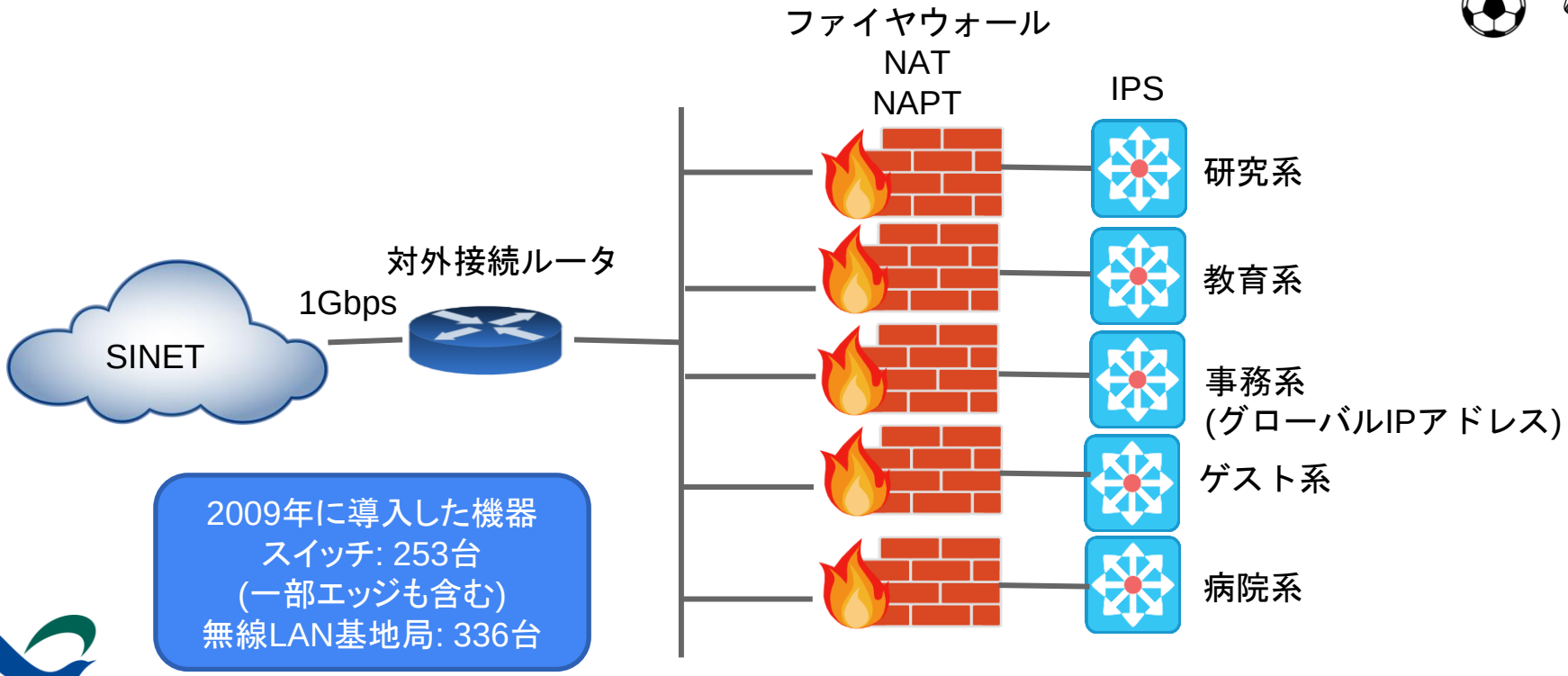
鳥取大学
Tottori University

鳥取大学

- キャンパス
  - 湖山(鳥取市)キャンパス，米子キャンパス（医学部，病院）
- 学部
  - 地域学部
  - 医学部
  - 工学部
  - 農学部
- 構成員（平成27年5月1日現在）
  - 教職員：2,235
  - 学生：6,285（学部: 5,287，修士: 657，博士: 341）
  - 中学校，小学校，幼稚園，特別支援学校の生徒数は除く
- 平成15年度より全学的にPC必携化

鳥取大学
Tottori University

鳥取大学ネットワーク: TUINS



2009年に導入した機器
スイッチ: 253台
(一部エッジも含む)
無線LAN基地局: 336台

鳥取大学
Tottori University

鳥取大学におけるグローバルIPアドレス

- 原則NAT/NAPT
  - 事務局を除く
  - 学外→学内だけでなく学内→学外へも通信可能とするポート番号を厳しく制限:
    - Gitやwhoisすら閉じられている
    - 申請によりポートを開放できる
- 申請に基づく学外公開
  - 約10年以前では申請が不要だったため，申請書が存在せず完全な把握ができていない
  - 内部監査を実施し，現在ファイアウォールの設定から棚卸を実施中

鳥取大学におけるインシデント対応体制

- 総合メディア基盤センター
  - 全学CSIRTの役割を担う
- 部局CSIRT
  - 部局毎にCSIRTがインシデントに対応する役割を担う
  - 必要に応じて総合メディア基盤センターも支援する
- ネットワーク監視
  - LAC社にネットワーク監視を委託
  - 学外と学内のVRF間の通信の監視を実施
- インシデント対応
  - LAC社や学外からの連絡を受け当該部局CSIRTに連絡し対応を依頼
  - 必要に応じて通信を遮断

地方の中小規模大学が抱える課題

鳥取大学
Tottori University

非常に限られた資源と求められる高度な対応

- 2016年から攻撃やインシデントが急増
- 個人情報の漏洩の有無について厳しく問われる
  - 個人情報が漏洩していない証拠を求められる
  - メールによる感染の場合は他に同様のメールが他の構成員に届いて開く可能性が無いかまで求められる
- 最新の機材も無く対応が難しい
  - 最新のファイアウォールやIPS，UTMなら対応可能と考えられるが…
- 中小規模大学で対応できる範囲を超越しつつある…

鳥取大学
Tottori University

インシデント発生時の当該PCの同定の難しさ

- 独自のNAT/NAPTの設置
  - 学科で独自のNAT/NAPTが設置されていることが多い
  - NAT/NAPTのログを全く取得しておらずPCを特定できないことがある
- スイッチのポート表の欠如
  - スイッチのポートの接続先が不明であることがある

非常に限られた予算

- 情報関連経費
  - ネットワークに関わらず全学のために申請ベースで支出する経費
  - とても最新のファイアウォールやIPS，UTMを導入する余裕は無い
- ネットワークリプレースの財源が無い
  - 前回は概算要求により予算を付与されたため問題無かった
  - 現在のネットワーク機器は2009年に導入され最早近年の脅威には対応できない
  - 情報関連経費を廃止し捻出することを検討
  - 冗長構成を廃止し耐障害性を犠牲にしてでも最新の機器への更新を検討中
- 潤沢に用意できない各種ログを蓄積するためのストレージ
  - 安価なHDDを利用したオブジェクトストレージを利用したストレージが限界
  - アクセス速度が非常に遅い
  - インシデント発生時に外部からの指摘のみだった場合には対応に時間を要する
  - 膨大（1日当たり20GB程度）なファイアウォールのログからプライベートIPアドレスを求めるのに数十分
  - インシデントの対応としては時間を要しすぎている

陸の孤島

OpenStreetMap Japan, https://openstreetmap.jp/

構成員の人数と知識，経験，意識

- 限られた総合メディア基盤センターの構成員
  - ICT基盤研究開発部門： 教員3名（全員湖山）
  - 情報システム研究開発部門: 教員3名（湖山: 2名，米子: 1名）
  - 技術職員: 5名（湖山3名，米子2名）
  - 事務職員: 情報基盤係3名，事務補佐員1名
  - 業者の常駐は無い
- 業務内容
  - ネットワークの整備と運用管理
  - 認証基盤の整備と運用管理
  - 仮想計算機基盤の整備と運用管理
  - 演習室端末の運用管理
  - インシデント対応
  - ソフトウェアライセンス管理

構成員の人数と知識，経験，意識（cont’d）

- セキュリティ専門部門の欠如
  - センターの部門にも技術職員にも事務職員にもセキュリティを担う専門部門は存在しない
  - 技術的な対応は教員と技術職員で実施

構成員の人数と知識，経験，意識（cont’d）

- 知識の習得，経験の蓄積をする場の少なさ
  - 大都市と比較し圧倒的に勉強会の機会が少ない
  - 情報も得られない
  - 研修によって情報を得ようとはするが生きた知識を得るのは難しい
- 構成員の意識
  - 地方の中小規模大学的な考えが染み付いていることが多い
  - 他大学の事例を追うことが多い
  - 独自の取り組みには消極的

他大学と共同で設置している学科や大学院

- 農学部共同獣医学科
  - 岐阜大学との共同設置
- 連合農学研究科
  - 山口大学との共同設置
- 教育環境の改善の必要性
  - e-Learningシステムの利用方法の改善が課題
  - 現状教員が各大学の学生のシステムに合わせて講義資料を用意

鳥取大学
Tottori University

地方の中小規模大学であることの利点

鳥取大学
Tottori University

迅速さ

- 狭いキャンパス
  - 湖山では自転車で5分以内で各部局の建物へ到達可能
  - インシデント発生時に現地に赴く必要がある場合に迅速に対応可能
  - 必要に応じて総合メディア基盤センターの教職員が直接対応
- 素早い意思決定と実施
  - IT担当副学長の指示の下，全学的なソフトウェアライセンス調査に1ヶ月で速報を提出した

柔軟さ

- 顔が見え易い
  - 各部局の責任者や実務担当者と連携する機会が多く，インシデント発生前に顔見知りであることが多い
  - 相互に技術的素養や性格が事前に明かなため，インシデント発生時のコミュニケーションが容易
- サービスの全学への展開が容易
  - 例: 2学科を除き全ての学科が鳥取大学メールサービス（TU-Mail)を利用
  - 他に附属施設といった2部局のみがTU-Mailを利用していない
  - RBLやウィルスを含んだ添付ファイルの駆除を全学的に実施可能

きめ細やかさ

- 学生の必携PCに起因するインシデントへの対応
  - 教育系ネットワークで発生したインシデントは原則総合メディア基盤センターが全て対応
  - 学生に直接メールや電話で連絡を取り対応を依頼
  - 対応が芳しくない場合には学内ネットワークからの遮断を実施
  - 必要に応じてウイルスの駆除，OSの再インストールを支援
- 部局CSIRTの活動の支援
  - インシデント対応は部局CSIRTでの対応を原則とする
  - 必要に応じて総合メディア基盤センターが現地に赴き対応をすることがある
  - 現場でインシデント当事者からは伝え難いことを総合メディア基盤センター教職員が代わりに伝言することもある

鳥取大学での
セキュリティへの取り組み

鳥取大学
Tottori University

認証技術

- ShibbolethによるSSOの実現と学認への参加（2014年度）
- Shibbolethによる有線LAN認証の実装（2014年度，実運用は2016年～）
- 無線LANにおけるEAP-PEAPの運用（2008年度）
- eduroamへの参加（2015年度）
- 二要素認証とShibbolethの組み合わせによる学外アクセスの提供（2015年度）
  - アカウント情報とマトリックスコード，イメージングマトリックス，電子証明書，Google Authenticator
- 認証シャッターによるShibboleth未対応のシステムでの二要素認証の実現（2015年）
  - メールやパッケージのシステムなど

メール経由のウイルス感染の防止

- 商用のメール用ウイルス対策ソフトの適用
  - 既知のウイルスは削除される
- ウイルスを含んだ添付ファイルの検査と隔離
  - 定期的にメールボックスを検査し添付ファイルの種類の統計を出力するシステムを作成
  - 独自の指針でウイルスの可能性が高い添付ファイルを自動検出
  - 特定の種類の添付ファイルの受信数が増加した場合には手動で確認
  - ウイルスの疑義がある場合には手動でRBL.jpやVirusTotal，サンドボックスによって確認
  - ウイルスであることが判明した場合には同様のメールを隔離を実施

個人情報漏洩の有無の確認

- 通信相手のIPアドレスをVirusTotalで調査し疑義のある通信の有無を確認
  - 近日中に疑義のある通信が観測されていた場合には情報漏洩の可能性があるものとして精査する
- ファイアウォールのログから通信相手との通信量を解析
  - 情報漏洩のために要する通信量に満たなかったものは情報漏洩の可能性が低いものとして考える
- 個人情報を含むファイルへのアクセス日時の確認
  - 必要に応じてPCを回収，もしくは，総合メディア基盤センターの教職員が確認
  - 個人情報を含むファイルへのアクセス日時を確認
  - アクセス日時がインシデント発生後でなければ情報漏洩の可能性が低いものとして考える

すなば

- ウイルスの振舞いを明かにするための取り組み
  - インシデントの原因を特定するため
  - インシデント発生時の情報漏洩の可能性の判断材料とするため
- Cuckooのサンドボックスによるウイルスの自動検出
  - 仮想環境を検出するウイルスとの鼬ごっこ
- 仮想環境でない実機によるウイルスの振る舞いの確認
  - 学外を攻撃する危険性がある
  - インシデントの原因の特定やウイルスの振る舞いの確認には非常に有用

すなば（鳥取砂丘）

まとめ

まとめ

- 自己紹介
- 鳥取大学の規模と鳥取大学ネットワークTUINS
- 地方の中小規模大学が抱える課題
- 地方の中小規模大学の利点
- 鳥取大学でのセキュリティへの取り組み
- まとめ

鳥取大学
Tottori University