

I	C	T	フ	ォ		ラ	ム		選	出
SS 研 ICT フォーラム 2016 より										

「つながった機器」と「インシデント」

鹿野 恵祐
(一般社団法人
JPCERT コーディネーションセンター)

「つながった機器」と「インシデント」

2016年8月23日
 一般社団法人JPCERT コーディネーションセンター
 早期警戒グループ
 鹿野 恵祐

本日のお題目

1. JPCERT/CCの紹介
2. インシデント事例のご紹介
3. インターネットからの探索活動
4. JPCERT/CCからのおねがい

1. JPCERT/CCの紹介

「JPCERT/CCをご存知ですか？」

1. JPCERT/CCとは

一般社団法人 JPCERT コーディネーションセンター

Japan Computer Emergency Response Team Coordination Center
 シェアードサーバートコーディネーションセンター

- 日本国内のインターネット利用者やセキュリティ管理担当者、ソフトウェア製品開発者等（主に、情報セキュリティ担当者）がサービス対象
- コンピュータセキュリティインシデントへの対応、国内外にセンサをおいた「インターネット定点観測」、ソフトウェアや情報システム・制御システム機器等の脆弱性への対応などを通じ、セキュリティ向上を推進
- インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、我が国の窓口となるCSIRT（窓口CSIRT）

CSIRT: Computer Security Incident Response Team

※各国に同様の窓口となるCSIRTが存在する(米国のUS-CERT、CERT/CC、中国のCNCERT、韓国のKJCERT/CC、等)

- 経済産業省からの委託事業として、サイバー攻撃等国際連携対応調整事業を実施

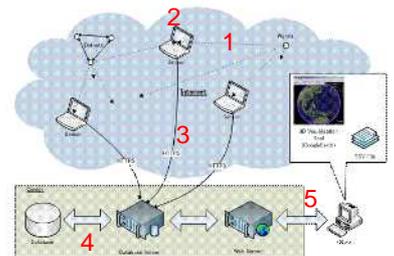
「JPCERT/CCをご存知ですか？」

1. JPCERT/CCの活動

インシデント予防	インシデントの予測と捕捉	発生したインシデントへの対応
脆弱性情報ハンドリング 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼 関係機関と連携し、国際的に情報公開日を調整 セキュアなコーディング手法の普及 制御システムに関する脆弱性関連情報の適切な流通	情報収集・分析・発信 定点観測 (TSUBAME) ネットワークトラフィック情報の収集分析 セキュリティ上の脅威情報の収集、分析、必要とする組織への提供	インシデントハンドリング (インシデント対応調整支援) マルウェアの接続先等の攻撃関連サイト等の隠蔽等による被害最小化 攻撃手法の分析支援による被害可能性の確認、犯行防止 再発防止に向けた関係各間の情報交換及び情報共有
早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信	
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援	
制御システムセキュリティ	制御システムに関するインシデントハンドリング、情報収集・分析発信	
アーティファクト分析	マルウェア (不正プログラム) 等の攻撃手法の分析、解析	
国内外関係者との連携	日本サーバート協議会、フィッシング対策協議会の事務局運営等	
国際連携	各種業務を円滑に行うための海外関係機関との連携	

1. 定点観測システムの仕組み

1. ワームやボットなどが送ったパケットをセンサが受信
2. センサ宛に届いたパケットをログに記録
3. ログファイルをサーバに送信
4. 受け取ったログファイルをデータベースに保存
5. 分析者はポータルにログインして分析等を実施



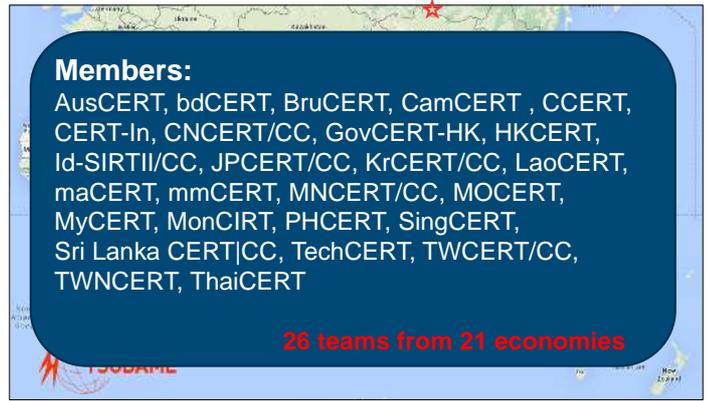
1. 本取組みに参加している組織

(2016年8月現在)



1. 本取組みに参加している組織

(2016年8月現在)



2. インシデント事例のご紹介

2.1 PLCがWANに露出していた事例

■ 事象の発見

—JPCERT/CC の分析官がパブリックモニタリング中に
 ブログ記事（中国語）を発見

■ キーワード

—国立大学
 —アクセス制御
 —認証不備
 —PLC

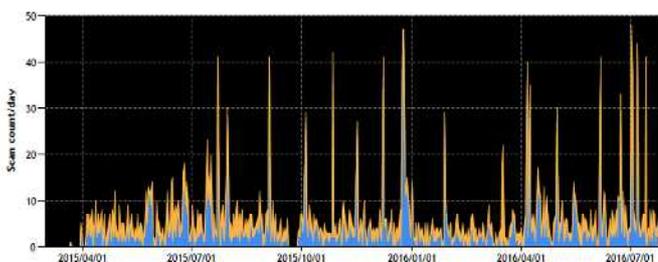


中国語のWebサイトで掲載されているブログ記事

■ 発生していた事象

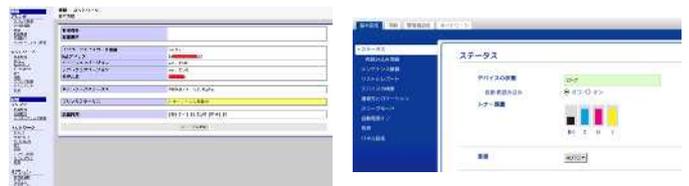
—Webインターフェースがインターネットからアクセス可能
 —PLCのポートにインターネットから到達可能

対象製品が使用する Port のパケット数の推移



- 2015年4月以降センサでパケットを継続して観測している
- セキュリティ研究者が調査目的に送ったと思われるパケットが多いが、それ以外のパケットも観測している

類似の例 | プリンタ、PCの画面など



プリンタ

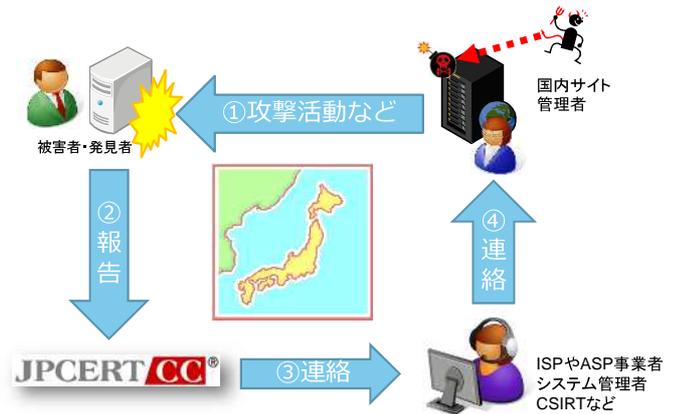


RDP/VNCなど

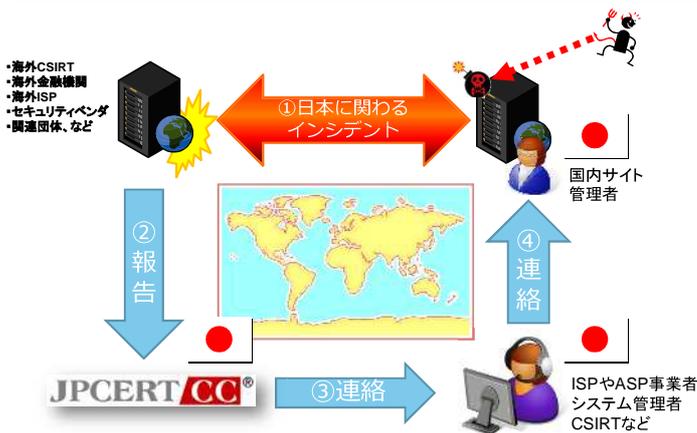
参考：

JPCERT/CCに報告された インシデント情報と連絡の流れ

対応ケース 1 | 国内→国内



対応ケース 2 | 海外→国内



対応ケース 3 | 国内→海外



2.2 Linux ボードが設置されていた事例

■ 事象の発見

- TSUBAMEセンサーに対し、Port22/TCP(SSH)のSYNパケットを送ってきた

Armadillo Default Page

Armadillo Series Features

- High Performance / Low power consumption
- The smallest IP camera (1000x1000 resolution) in the world
- High resolution (1080p) camera
- Research Ready
- It is the combination of the standard IP camera (1080p) and the smallest
- Small Form Factor
- It is the smallest IP camera in the world and the smallest form factor camera.



送信元IPアドレスで動作している
ネットワーク接続された Linux board の初期画面

■ キーワード

- 国立/私立大学等
- 組み込みLinux
- パスワード強度
- アクセス制御
- マルウェア感染
- 踏み台

■ 主な問題

- 攻撃者に辞書攻撃を受け、機器に侵入されていた (セットアップ後にデフォルトパスワードを変更していなかった)
- マルウェアが実行され第三者が探索や辞書攻撃等を行っていた

Port 22/TCP を対象としたパケット数の推移



- 定期的にパケットを観測している
- 観測パケット数 TOP5 にほぼ含まれる
- セキュリティ研究者だけではなく、マルウェア感染ホストなどもパケットを送信している

2.4 踏み台となるネットワーク機器

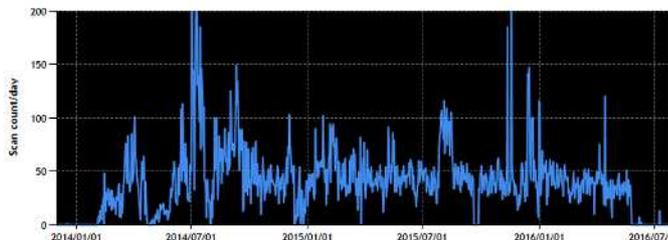
- 問題の発見
 - TSUBAMEにて送信元Port 53/UDP からDNSクエリに対する応答パケットを観測
- キーワード
 - 国立大学、企業、個人等
 - ネットワーク機器/DNSサーバ (国内機器ベンダ含)
 - オープンリゾルバ/フォワーダー
 - DDoS攻撃
 - 踏み台
- 主な問題
 - 設定不備
 - DNSコンテンツサーバが誤ってリゾルバとしても動作していた
 - WANからDNSクエリを受け付ける設定になっていた
 - DNS 水責め攻撃(DDoS)攻撃に参加していた
 - UDP Amp攻撃にも使用されていた可能性あり



DNS リゾルバ機能が動作しているネットワーク機器(イメージ)

Port 53/UDP からのパケット数の推移と特徴

```
■ User Datagram Protocol, Src Port: 53 (53), Dst Port: 5128 (5128)
■ Domain Name System (response)
  Transaction ID: 0x632d
  Flags: 0x8182 standard query response, Server failure
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    ■ irqjtf.www.epc[redacted].es.jp: Type A, class IN
      Name: irqjtf.www.epc[redacted].es.jp
      [Name Length: 24]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```



3.インターネットからの探索活動

3. サーチエンジンを使用した機器の検索

- インターネットに接続されたノード (IPアドレスを持つ機器) を検索するサービス
 - インターネットに対して、様々なプロトコルのリクエストを送信し、そのレスポンスをデータベース化している
 - 制御システム関連プロトコルなど広くにも対応している (Modbus、DNP3、Ethernet/IPなど)



検索サービスの例

類似の検索サービス

- ZoomEye
 - <https://www.zoomeye.org/>
 - 中国版SHODAN
- censys
 - <https://censys.io/>
 - 米国 Michigan 大学の研究チームが作成
- ICSfind
 - <http://icsfind.com/>
 - 中国の大学が作成 (現在はアクセスできない)

4. JPCERT/CCからのおねがい

JPCERT/CCからのおねがい

- ネットワークの状況を把握しましょう
 - どのIPアドレスが使用されているか、動的か静的か？
 - WHOIS など連絡体制の更新もおねがいします
- ログの取得や保存
 - ”高度サイバー攻撃への対処におけるログの活用と分析方法 (2015年11月公開)”では、1年以上の保存を推奨しています
- 機器をインターネットに接続する前に
 - WANとLAN接続口を間違えていませんか？
LANで使用を推奨する機器もあります
 - アンチウイルスの有無を確認する
 - ファイアウォールやルータのフィルタリングの設定を確認する
利用目的外の管理者 Web インタフェースやメンテナンス機能にも注意
ランダムPortを使用する製品もある

類似インシデントを防ぐための取り組み

- 注意喚起や早期警戒情報の発行
- 海外の National CSIRT との連携
 - 不審なパケットの送信元IPアドレスリストの提供
 - 推測される問題機器の情報
セキュリティ上の問題の共有
- 国内ISPや機器ベンダとの連携
 - 機器が設置されているIPアドレスの管理者への情報提供
 - 同様の問題を引き起こさないため製品ベンダにも情報提供

みなさまからの報告や情報を活用！！

* 悪者が特定されるような使い方は致しません

お問合せ、インシデント対応のご依頼は

JPCERT/CC®
安全・安心なIT社会のための、国内・国際連携を推進する
JPCERT/CC (Japan Computer Emergency Response Team / Coordination Center)

CERTコーディネーションセンター
— Email : pr@jpcert.or.jp
— Tel : 03-3518-4600
— <https://www.jpcert.or.jp/>

インシデント報告
— Email : info@jpcert.or.jp
— <https://www.jpcert.or.jp/form/>

制御システムインシデントの報告
— Email : ics-ir@jpcert.or.jp
— <https://www.jpcert.or.jp/ics/ics-form>

JPCERT/CC®
安全・安心なIT社会のための、国内・国際連携を推進する
JPCERT/CC (Japan Computer Emergency Response Team / Coordination Center)

ご静聴ありがとうございました

I	C	T	フ	ォ		ラ	ム		選	出
SS 研 ICT フォーラム 2016 より										

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

大森 幹之
(鳥取大学)

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

大森 幹之

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

ohmori@tottori-u.ac.jp

概要

鳥取大学は国内で唯一いわゆる「すなば」を敷地内に有し、時に大容量データ通信を必要とする乾燥地研究センターを擁する大学である。同時に、いわゆる「陸の孤島」とも呼ばれ、常に国内 1, 2 を争う過疎地域である地方の小規模大学でもある。本稿では、地方の小規模大学での事例の 1 つとして、鳥取大学でのセキュリティへの取り組みにおいて費用的、地理的、人的に限られた資源に起因する困難さを紹介する。その一方で、地方と小規模であることを生かした純朴で丁寧できめ細やかで迅速な取り組みを紹介する。

キーワード

セキュリティ、インシデント対応、費用対効果、中小規模、すなば、陸の孤島

1. はじめに

鳥取大学は国内で唯一いわゆる「すなば」（つまり砂丘）を敷地内に有し、時に大容量データ通信を必要とする乾燥地研究センターを擁する大学である。一方、鳥根県と共にいわゆる「陸の孤島」とも呼ばれ、常に国内 1,2 を争う過疎地域である山陰地方の鳥取県にある小規模大学である。小規模大学であるが故に費用的、地理的、人的な資源は非常に限られている。そのため、セキュリティへの取り組みへの投資も限られている。しかしながら、近年は学外からの攻撃も増加している。特に 2016 年からはウイルスが添付されたメールを多数受信しており、その数は例年と比較し凡そ倍以上になっている。しかもウイルス対策ソフトも未対応の新種のウイルスが添付されている例が増えており、攻撃も高度化している。

この様に、脅威が高度化し、その数も増加していることから、セキュリティへの取り組みがより求められている。そして、資源が非常に限られている状況で、高度な攻撃にも対応でき、かつ、効率的であることが求められている。加えて、近年では特に個人情報漏洩の防止が非常に強く求められており、インシデント発生時には個人情報が漏洩していないと判断するに足る証拠を求められることがある。これらの要求を全て完全に満たすことは、小規模大学にとってはほぼ不可能である。し

かしながら、鳥取大学では小規模であることの強みを生かし最善努力しているところである。

本稿では、上記の様にセキュリティに関して小規模大学が抱える課題と取り組みについて、鳥取大学を例に取り、紹介する。本稿の構成は以下のとおりである。まず、2 節で鳥取大学の規模やネットワーク構成を簡単に紹介する。3 節で鳥取大学の課題を紹介する。4 節では地方の中小規模大学であることの利点を述べ、5 節で鳥取大学での取り組みについて紹介する。最後に 6 節で結論を述べる。

2. 鳥取大学について

鳥取大学は教職員 2,235 名、学生 6,285 名（平成 27 年 5 月現在、附属学校の生徒数は除く。）しか有さず、地域活性化の中核的拠点を目指す小規模大学である。キャンパスは、大きく分けて鳥取市と米子市の 2 箇所にある。加えて、乾燥地研究センターや附属学校といった附属施設が点在している。

鳥取大学では、平成 15 年度より全学的にノート PC 必携化することで、PC 演習室の拡大といった追加投資なく、近年の情報通信技術を活用した講義への対応を試みている。

ネットワークに関しては、教育系、研究系、事務系の 3 種類のネットワークを Virtual Routing Forwarding (VRF) により仮想的に分離し、セキュリティを担保しつつ、費用を削減している。また、事務局を除く全ての PC でプライベート IP アドレスへ移行し、セキュリティの向上を図っている。そして、Intrusion Prevention System (IPS) を導入し、株式会社ラック[1]による監視サービスを契約しており、Critical 以上の緊急性を要するものをセキュリティインシデントとして対応している。

セキュリティインシデント対応のための体制としては、総合メディア基盤センターが全学 Computer Security Incident Response Team (CSIRT)として機能し、各部局においても部局 CISRT を置くこととし、各種規則、ガイドラインを設けている。

3. 地方の中小規模大学が抱える課題

3.1 限られた予算

ネットワーク機器やセキュリティ対策に投資する予算は中小規模大学では非常に限られている。特に鳥取大学ではこれまで概算要求により認められた予算でネットワーク機器を購入していた。そのため、ネットワーク機器のための定常的な予算を学内で確保していないという状況である。今後は、概算要求によりネットワーク機器の予算が中小規模大学に付与される可能性は低く、学内からの予算の捻出が必要となると予想される。

上記の様に予算が限られているにも係らず、鳥取大学では 2009 年に導入されていたネットワーク機器の老朽化に伴って、止むを得ずネットワーク機器のリプレースを計画している。削減された予算のため、冗長構成としなかったり、無線 LAN を取り止めたり、セキュリティ機器の削減といったことを視野に入れて計画している。

このような状況なため、新たにセキュリティ機器を購入することも出来ず、高度な攻撃に対応することも非常に難しいのが中小規模大学の現状である。

3.2 貧弱なネットワーク機器

上述の様に、鳥取大学では予算が十分ではないため、2009 年に導入した型遅れとも言える古いネットワーク機器を、可能な限り利用し続ける努力をしている。しかしながら、2009 年に導入されたファイアウォールのハードウェアの古い設計とコアスイッチのソフトウェアの脆弱な基本設計により、Simple Network Management Protocol (SNMP) の処理の実装の脆弱さに起因する学内ネットワークが停止する事象も発生した[2]。設定ミスによるコアスイッチの高負荷を誘発する SNMP を用いた Denial of Services (DoS) 攻撃や Distributed DoS (DDoS) 攻撃は有名であるが、今回の事象は明かに機器の設計が古過ぎることに起因した。

また、ネットワーク機器の性能が不十分なため、学内ネットワークでは、パケット損失を定常的に発生している。そのため、1 フロー当たりせいぜい 100Mbps しかスループットが得られないということが定常的に発生している。原因としてはファイアウォールもしくは IPS に起因すると考えられる。しかしながら、限られた予算ではファイアウォールや IPS を入れ替えることは容易ではなく、現在のところ致命的な障害には至っていないため、現状維持で運用しているというのが実態である。

3.3 陸の孤島

道路や公共交通機関の整備は人口といった費用対効果に基づいて実施されるため、鳥取県内の道路やバス、電車、自動車といった交通機関や施設、設備は必ずしも便利とは言えない。電車や自動車は 1 時間に 1 本あれば良い方である。そのため、島根県と鳥取県で構成される山陰地方は「陸の孤島」と揶揄される。そのためか各ベンダからの訪問の数は大都市に比較し少なく感じられる。

また、鳥取大学での障害時やインシデント時には大阪や広島といった大都市からベンダが人員を派遣することが多い。この場合に、本学から連絡して 4 時間以内に部品や人員が到着することは、まず、無い。加えて、近年では大都市に技術者を集中させる傾向がベンダに見られ、2015 年度から本学の担当者も広島へ移っている。

加えて、「陸の孤島」は大雨や大雪といった天候に非常にされ易く脆弱で、その様な天候時に障害が発生するとベンダからの部品や機器、人員が数日間到着しないことがある。特に冬季は鳥取では雪が定常的に積もっている期間もあり、その様な時季にはベンダも来学しながらない傾向が伺える。

上記の様な状況であるため、ベンダに運用や保守を頼るのは難しいと考えられ、技術者不足であるはずの地方の中小規模大学の方が大都市の大規模大学よりも高度な知識を持った構成員を必要としているのではないかと考えられる。

3.4 構成員の人数と知識、経験、意識

鳥取大学の総合メディア基盤センターには、ネットワークを始めとした基盤技術を担う ICT 基盤研究開発部門（教員 3 名）とその基盤上に構築されるシステムの構築や運用、管理を担う情報システム研究開発部門（教員 3 名）の 2 部門しかない。また、技術職員は 5 名であり、部門には属していない。つまり、他の大規模大学と異なり、セキュリティを担う専門の部門は無い。そのため、上記 2 部門と技術職員が協力してセキュリティに関する事案に対応している。このような状況であるため、システムの稼働に直接関係のある運用管理業務に比べ、インシデント発生時にしか重要視されない傾向にあるセキュリティに関する取り組みは後手後手になっているのが現状である。セキュリティは先手先手で防御していくのが望ましいがそのためには人員が不足していると言える。

そして、予算削減に伴い人員削減が叫ばれており、構成員の業務は増加の一步を辿っている。特に技

術職員においては年々事務処理が増加している。一方、高度化する外部からの攻撃への対応を求められており、年々業務の厳しさが増している。このような状況では高度な知識や経験を身に付け、業務の効率化を図ることが重要である。しかしながら、大都市に比較すると、地方都市では勉強会や研究会の機会も非常に少ないのが実態である。大都市への研修も実施しているが十分とは言えない。

加えて、地方の中小規模大学であるが故か、情報系センター業務として、最先端である必要は無いという雰囲気も感じられ、最先端的な取り組みを実施し難いとも感じられる。例えば、注意喚起にしても、英語での注意喚起を怠ったといったことが挙げられる。そのため、日本語を理解できない構成員がインシデントの発生源となるといった事例が見受けられる。

3.5 他大学との共同で設置している学科

地方の小規模大学である鳥取大学では、単独での設置が難しい研究科や学科を他大学と共同で設置していることがある。例えば、岐阜大学と鳥取大学が共同で設置している農学部の共同獣医学科が挙げられる。このような学科の場合、それぞれの大学に属する教員と学生がシームレスに講義を実施できる必要がある。しかしながら、現状では岐阜大学と鳥取大学では、採用している e-Learning システムが異なるため、講義をする教員に大きな負担を強いている。このような教職員への負担を軽減することが地方の中小規模大学の課題の 1 つとして挙げられる。

4. 地方の中小規模大学であることの利点

4.1 迅速さ

鳥取大学のキャンパスは大きく分けて鳥取市の湖山地区と米子市の米子地区があるが、大都市と比較するとそれぞれの規模は小さい。例えば、湖山地区においては、各部局の建物まで自転車で 5 分かからない。このような小規模さであるため、大規模な組織に比較すると柔軟で迅速に行動を起こせることがある。

例えば、小さな部局においては総合メディア基盤センターが部局 CSIRT としての役割を担っており、インシデント発生時には教員や技術職員が即座に自転車や徒歩で現場に数分以内に向かって初動を開始できる。また、小さな部局でない場合は、インシデント発生時には当該部局による対応を依頼しているが、重要なものや迅速性が求められる場

合には総合メディア基盤センターの教職員が直接対応することもある。

加えて、鳥取大学では 2014 年に Microsoft 社によるライセンス調査を受けたが、IT 担当副学長の指揮の元迅速に対応し、主にセンターの方で集計するなど部局の作業をセンターで担い、約 1 ヶ月で第一回の調査結果を提出できた。

4.2 柔軟さ

鳥取大学は小規模であるため、各部局の責任者や実務担当者として総合メディア基盤センターの教職員とが通常業務で連携する機会が多い。そのため、各員の技術的素養や性格といったことを相互に把握できており、柔軟で適切な会話と情報交換が可能となっている。

また、小規模のため、総合メディア基盤センターで実施しているサービスを全学に展開することが容易である。例えば、総合メディア基盤センターでは教職員向けにメールサービス (TU-Mail) を提供しているが、今や 2 学科を除き全ての学科の教職員は TU-Mail へ移行している。附属施設といった部局に関しては 2 部局を残して全て TU-Mail への移行している。TU-Mail ではメール向けの商用の Realtime Blackhole List (RBL) やウイルス対策ソフトを適用しているのに加えて、後述のとおり学外からの利用には二要素認証を実装している。この様にほぼ全学のメールシステムを総合メディア基盤センターで担うことで、セキュリティへの取り組みを一度に全学に柔軟に適用することも可能となっている。

4.3 きめ細やかさ

鳥取大学では主に学生が利用する教育用ネットワークで発生したインシデントは原則として総合メディア基盤センターが担っている。例えば、学生が携行しているノート PC がウイルスに感染し IPS により疑義のある通信を検出した場合には、総合メディア基盤センターが学生に直接メールや電話で連絡し必要な対応を取っている。具体的には当該ノート PC の学内ネットワークの隔離やウイルスの駆除、OS の再インストールの支援を行っている。

学生に限らず、他部局での教職員に起因するインシデント発生時にも必要に応じて総合メディア基盤センターの教職員が対応する。加えて、上司と部下といった関係の様にインシデントに関して報告や依頼をし難い様な状況で、総合メディア基盤センターの教職員が柔軟に対応することもある。

5. 鳥取大学での取り組み

5.1 認証技術

セキュリティの向上のため、鳥取大学では 2014 年から Shibboleth[3]による Single Sign-On (SSO)を導入した。学内システムへの展開の後、同年度に学認へ参加した。また、2014 年度に教育用有線 LAN における Shibboleth による認証を実装し、2016 年度から稼働させている。一方、無線 LAN では 2008 年度から WPA2-PEAP による認証を開始し、2015 年度から eduroam へ参加した。

学外からのアクセスには、アカウント情報による認証とマトリックスコード表やイメージングマトリクス、電子証明書などを用いた二要素認証に基づいて SSL-VPN によるアクセスを提供していた。しかし、SSL-VPN の不安定さと不便さから、2015 年度から各システムを Shibboleth による二要素認証に対応させてきた。メールやパッケージシステムの様なシステムでは Shibboleth に対応することが難しいため、“認証シャッター”[5]と呼ばれる Web による付加的な認証によって対応させた。また、実験的に Google Authenticator による認証も試みている。

5.2 メール経由のウイルス感染の防止

上述のとおり、鳥取大学ではいくつかの学科や部局を除き全学的にメールサービスとして TU-Mail を利用している。TU-Mail では既にメール用の商用のウイルス対策ソフトを適用しているが、2016 年に入り、新種のウイルスを添付したメールやフィッシングメールの受信を多数確認している。そこで、メールボックスを自動的に検査し添付ファイルの種類とその個数を検出するスクリプトを作成した。そして、疑義のある添付ファイルは、VirusTotal[6]での登録の有無とウイルスの振る舞いを手動で確認している。ウイルスである可能性が高い場合当該のメールを手動で全て隔離している。この様な取り組みによってウイルス感染を未然に防止することを試みている。

5.3 情報漏洩の有無の確認

前述のとおり個人情報の漏洩の有無が求められることがある。そのため、鳥取大学総合メディア基盤センターでは、ファイアウォールの通信ログを解析し、各 IP アドレスを持ったホストとの通信を算出するスクリプトを作成した。また、VirusTotal で疑義のある通信をした IP アドレスとして登録されたホストとの通信が無いかを自動的に確認するスクリプトを作成し、情報漏洩の可能性が極めて

低いことを示せる様に試みている。また、必要に応じて感染 PC を引き取り、個人情報を含むファイルへのアクセス時刻を確認することで情報漏洩の有無を確認する作業も試みている。

5.4 すなば

未知のウイルスの場合その振る舞いを把握しておかなければ対応が取れない。そのため、フリーのサンドボックスである Cuckoo[7]を実験的に運用している。既に、Cuckoo に対応したウイルスも確認されているが、その様なウイルスへの対応も模索中である。また、仮想環境ではない実機によるサンドボックス（すなば）を実験的に稼働させ、未知のウイルスの場合にはその振る舞いを確認することも試みており、実際に感染源の特定に大きな役割を果たしている。

6. おわりに

本稿では鳥取大学を例に取り、地方の中小規模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紹介した。小規模大学であるが故に予算が限られているにも関わらず、特に 2016 年からは非常に高度な対応を求められることが増加しており、対応の限界も迎つつある。小規模大学の現実的な対応を導き出すために、関係各位の広い見識を頂ければ幸いである。

7. 謝辞

鳥取大学総合メディア基盤センター教員並びに当該センターで業務にあたっている技術部技術職員各位に感謝の意を表す。

8. 参考文献

- [1] 株式会社ラック，“セキュリティ対策なら株式会社ラック”，available online: <http://www.lac.co.jp/>.
- [2] On a SNMP DoS Attack against Vulnerable Architecture of Network Equipment、Motoyuki OHMORI、IPSJ SIG Technical Report、2016-IOT-33 巻 4 号（頁 1～4）、2016 年 05 月。
- [3] The Shibboleth Consortium “Shibboleth,” available online: <https://shibboleth.net/>.
- [4] 国立情報学研究所，“学術認証フェデレーション 学認 Gaku Nin”，available online: <https://www.gakunin.jp/>.
- [5] 多田 充，“パスワード認証の強化策”，学術情報処理研究，No.19 2015，pp.40-49 2015 年 9 月。
- [6] VirusTotal，“VirusTotal - ウイルス、マルウェア、URL の無料オンラインスキャナ”，available online: <https://www.virustotal.com/ja>
- [7] Cuckoo Foundation，“Automated Malware Analysis - Cuckoo Sandbox,” available online: <https://www.cuckoosandbox.org/>.



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>



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



SS研ICTフォーラム2016 2016年8月23日

2



自己紹介



SS研ICTフォーラム2016 2016年8月23日

3

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



SS研ICTフォーラム2016 2016年8月23日

4



鳥取大学の規模と 鳥取大学ネットワークTUINS



SS研ICTフォーラム2016 2016年8月23日

5

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必修化

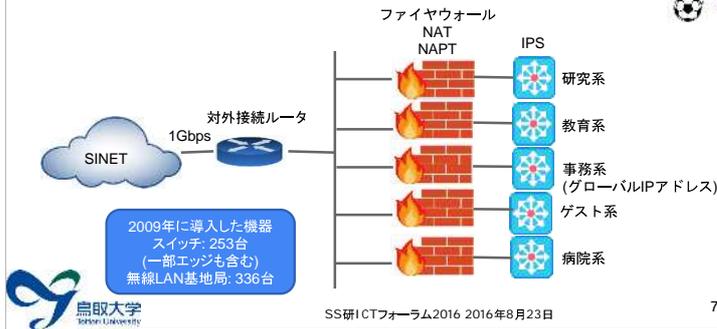


SS研ICTフォーラム2016 2016年8月23日

6



鳥取大学ネットワーク: TUI NS



7

鳥取大学におけるグローバルIPアドレス



- 原則N T N PT
 - 事務局を除く
 - 学外一学内だけでなく学内一学外へも通信可能とするポート番号を厳しく制限:
 - や 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1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



SS研ICTフォーラム2016 2016年8月23日

8

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CSI Tの役割を担う
- 部局CSI T
 - 部局毎にCSI T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
 - C社にネットワーク監視を委託
 - 学外と学内の 間の通信の監視を実施
- インシデント対応
 - C社や学外からの連絡を受け当該部局CSI Tに連絡し対応を依頼
 - 必要に応じて通信を遮断



SS研ICTフォーラム2016 2016年8月23日

9

地方の中小規模大学が抱える課題



SS研ICTフォーラム2016 2016年8月23日

10

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ら求められる
- 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…



SS研ICTフォーラム2016 2016年8月23日

11

インシデント発生時の当該PCの同定の難しさ



- 独自のN T N PTの設置
 - 学科で独自のN T N PTが設置されていることが多い
 - N T N PT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



SS研ICTフォーラム2016 2016年8月23日

12

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2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 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2程度)なファイアウォールのログからプライベートIPアドレスを求めのり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

SS研ICTフォーラム2016 2016年8月23日

13

陸の孤島



OpenStreetMap Japan, <https://openstreetmap.jp/>

SS研ICTフォーラム2016 2016年8月23日

14

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

SS研ICTフォーラム2016 2016年8月23日

15

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

SS研ICTフォーラム2016 2016年8月23日

16

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

SS研ICTフォーラム2016 2016年8月23日

17

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

- r 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

SS研ICTフォーラム2016 2016年8月23日

18



地方の中小規模大学であることの利点

鳥取大学
Tottori University

SS研ICTフォーラム2016 2016年8月23日

19

迅速さ

- 狭いキャンパス
 - 湖山では自転車ですぐに各部署の建物へ到達可能
 - 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



SS研ICTフォーラム2016 2016年8月23日

20

柔軟さ

- 顔が見え易い
 - 各部署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 M)を利用
 - 他に附属施設といった2部署のみがTU M を利用していない
 - やウイルスを含んだ添付ファイルの駆除を全学的に実施可能



SS研ICTフォーラム2016 2016年8月23日

21

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CSI Tの活動の支援
 - インシデント対応は部局CSI T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えることもある



SS研ICTフォーラム2016 2016年8月23日

22

鳥取大学でのセキュリティへの取り組み

鳥取大学
Tottori University

SS研ICTフォーラム2016 2016年8月23日

23

認証技術

- S によるSS の実現と学認への参加 (2 4年度)
- S による有線 N認証の実装 (2 4年度, 実運用は2 16年~)
- 無線 Nにおける P P Pの運用 (2 8年度)
- d r への参加 (2 5年度)
- 二要素認証とS の組み合わせによる学外アクセスの提供 (2 5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
- 認証シャッターによるS 未対応のシステムでの二要素認証の実現 (2 5年)
 - メールやパッケージのシステムなど



SS研ICTフォーラム2016 2016年8月23日

24

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を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 `rt`、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 `rt` 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の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ら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
- C 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聴こっこ
- 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

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UINS
- 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