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，島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．

この様な状況なため，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，汽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．電車や汽車は 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た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も考えられる．

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．この様な状況であるため，システムの稼動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歩を辿っている．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．この様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．この様な学科の場合，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．この様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 分とかからない．この様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 年度から実稼動させている．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）を実験的に稼動させ，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，対応の限界も迎えつつある．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る．

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 Netw ork Equipment 、 Motoyuki OHMORI 、 IPSJ SIG Technical Report 、 2016-IOT-33 巻 4 号 （頁 1 ～ 4） 、 2016 年 05 月.

[3] The Shibboleth Consortium “Sibboleth,” 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/.