# 公的機関の調査から見た大学等のセキュリティ状況と対策

石坂徹† 刀川眞† 石田純一† 早坂成人†

†室蘭工業大学
050-8585 北海道室蘭市水元町 27-1
Email: {ishizaka, tachikaw, ishida, hayasaka}@mmm.muroran-it.ac.jp

**あらまし** 本論文では，情報処理推進機構，日本ネットワークセキュリティ協会及び警察庁による調査・集計結果を用いて，大学等の情報セキュリティ対策の特徴を分析した．分析により大学が分類される業種「教育機関」では，他の業種と比較して情報セキュリティ対策が不十分であることが示された．不十分である要因は，業務のIT依存度の低さ，ルールの不備，ガバナンスの不明確さにあると我々は考えた．そこで，ルールの徹底，技術的対策，不明瞭なガバナンスの解消を大学等におけるセキュリティ対策として提案した．

# Study on the security situation and countermeasures for university using researches by public institutions

Tohru Ishizaka† Makoto Tachikawa† Jun-ichi Ishida† and Narihito Hayasaka†

†Muroran Institute of Technology
27-1 Mizumoto, Muroran, Hokkaido 050-8585, JAPAN
Email: {ishizaka, tachikaw, ishida, hayasaka}@mmm.muroran-it.ac.jp

**Abstract** In this paper, we analyzed the characteristics of information security countermeasures for universities, using results of survey from Information-technology Promotion Agency (IPA), Japan Network Security Association (JNSA), and Japan National Police Agency. The "educational institutions" university industry belongs, that information security is insufficient compared to other industries has been shown. We estimated the factors that low dependencies of IT, and unclear governance. Then we proposed strict execution of the rule, technical measures, and resolving ambiguous governances as the information security countermeasures for universities.

## 1 はじめに

企業をはじめとする組織では，業務の IT への依存度が高くなるにつれて，情報セキュリティ対策およびそれを推進するマネジメントの必要性が高まってきている．組織のセキュリティ体制の規格としては，JIS Q 27001 または ISMS(Information Security Management System)として知られる認証規格がある．大学もまた組織のひとつであり，相応の情報セキュリテ

ィ対策が求められている. しかし, ISMS に準拠している大学は 2012 年 8 月現在7校と少ない[1]. 上原は大学のセキュリティの問題点をITガバナンスの視点から考察している[2]. また, セキュリティインシデント予防, セキュリティ意識向上のため, 教職員に対する教育も行われている[3][4].

組織における情報セキュリティに関する調査は, 独立行政法人情報処理推進機構(以下, IPA という. )や NPO ネットワークセキュリティ協会(以下, JNSA という. )などにより行われている. これらの調査から, 組織においては, 業務の内容, 体質, または風土など様々な要因により, それぞれの業種に適切なセキュリティ対策が必要なことが推測される.

本研究では, 大学等の組織全体でどの程度情報セキュリティ対策が実施されているか調べるため, 公的機関の調査を用いた. 公的機関による情報セキュリティに関する調査は, 教育機関に対して文部科学省, 一般の企業については経済産業省で情報基盤とセキュリティに関する調査を行っているが, 調査項目に違いがあるため「教育機関」という業種として, 他の業種と比較はできない. そこで, 統一の調査内容で, 業種ごとに分類されて集計されている IPA「セキュリティ対策ベンチマーク」[5], JNSA「情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」[6]及び警察庁「不正アクセス行為対策等の調査」[7]を分析した. さらに分析に基づいて大学における問題点と対策を考察した.

# 2 IPA 情報セキュリティ対策ベンチマーク

## 2.1 概要

IPA は、技術・人材の両面から日本の IT 戦略を推進するために設立された独立行政法人である[8]. IPAでは事業の一つとして,「社会基盤としての IT の安全性・信頼性の向上」を掲げており, その一部として自己申告型の診断ツールである情報セキュリティ対策ベンチマークを公開している. 本研究では, 2011 年 5 月 31 日に公表されたベンチマークの集計結果を用いた. 集計数は延べ 1654 件である.

ベンチマークの質問は合計 40 個あり, 情報セキュリティ対策に関する 25 個の質問(ベンチマーク)と事業内容に関する 15 個の質問(業種分類)で構成される. ベンチマークの質問は「できていない」～「できている」の1～5の選択式で, 回答した番号がその質問のスコアとなる. スコアが高い方がより良好または十分な対策を行っていることになる. トータルスコアはすべての質問のスコアの総計を整数に切り上げたものである. トータルスコアは 120 点が満点となる. また, 業種分類の回答内容により, 同一の業種, 規模及び情報セキュリティ指標によるグループにより比較することができる. この情報セキュリティ指標によるグループ分けは従業員数, 売上高などから総合的に算出される値で, 企業が抱えるリスクを示す指標である. この指標により, 組織は,

- GⅠ:高水準のセキュリティレベルが要求される層
- GⅡ:相応の水準のセキュリティレベルが望まれる層
- GⅢ:情報セキュリティ対策が喫緊の課題でない層

の 3 個のグループに分類される.

## 2.2 医療・福祉、教育・学習支援業の傾向

IPA 情報セキュリティ対策ベンチマークにおいて, 大学は「医療・福祉、教育・学習支援業」の業種として集計されている. 表 1 にベンチマークの質問項目とこの業種の平均スコアを示す. 各項目のスコアを見ると多くが2点台で中間値 3 よりも大きい値を示している質問は(6), (14), (20)の 3 個しかなく, 全体的に情報セキュリティ対策が充分でないことを示している.

もっとも高いトータルスコアの業種は「情報・サービス業」で 92, 続いて「金融・保険業」で 89 となっている.「医療・福祉、教育・学習支援業」のトータルスコアは全業種で最も低い値である.

表 1:情報セキュリティ対策ベンチマークの質問内容と「医療・福祉、教育・学習支援業」のスコア

| 項番 | 質問内容 | スコア |
|---|---|---|
| (1) | 管理規定 | 2.646 |
| (2) | 推進体制 | 2.708 |
| (3) | 資産分類 | 2.375 |
| (4) | 情報の工程毎安全対策 | 2.417 |
| (5) | 業務委託契約 | 2.813 |
| (6) | 従業者との契約 | 3.042 |
| (7) | 従業者への教育 | 2.521 |
| (8) | 建物等のセキュリティ | 2.833 |
| (9) | 第三者アクセス | 2.479 |
| (10) | 機器の設置 | 2.792 |
| (11) | 書類・媒体の管理 | 2.833 |
| (12) | 実稼働環境 | 2.708 |
| (13) | システム運用 | 2.646 |
| (14) | 不正プログラム対策 | 3.313 |
| (15) | 脆弱性対策 | 2.688 |
| (16) | 通信ネットワーク保護策 | 2.917 |
| (17) | 媒体の紛失・盗難対策 | 2.375 |
| (18) | データへのアクセス | 2.875 |
| (19) | 業務アプリへのアクセス | 2.875 |
| (20) | ネットワークのアクセス制御 | 3.229 |
| (21) | 開発時のセキュリティ | 2.396 |
| (22) | ソフトウェアの管理 | 2.417 |
| (23) | 障害対策 | 2.896 |
| (24) | 事故対応手続き | 2.458 |
| (25) | 事業継続 | 2.729 |
| トータルスコア（整数に切り上げ） | | 68 |

また，情報セキュリティ指標による各グループの平均トータルスコアはＧⅠで 86，ＧⅡで 84，そしてＧⅢで 78 である．筆者らが所属する大学で情報セキュリティ指標を算出したところ，ＧⅢに分類される数値であった．この数値は従業員数や予算に依存する数値であるため，大学によってはＧⅠやＧⅡに分類される場合もある．ここでは，大学組織の情報セキュリティ対策が充分でないことを鑑み，比較対象としてＧⅢを選び，「医療・福祉、教育・学習支援業」との各項目のスコアの差を考察した．差分のグラフを図1に示す．

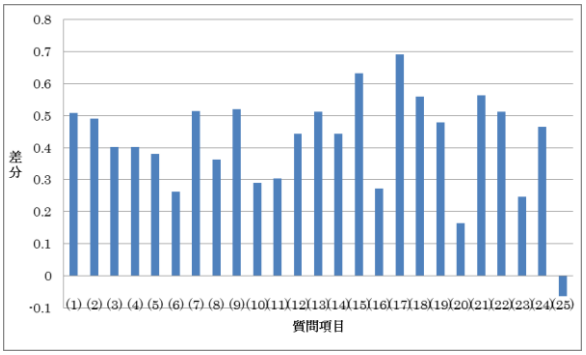


図 1:各質問項目スコアの差分
ＧⅢ－「医療・福祉、教育・学習支援業」

(25)事業継続以外でＧⅢのスコアが高く，「情報セキュリティ対策が喫緊の課題でない層」としても対策が充分に行われていないことがわかる．

## 3　JNSA 情報セキュリティインシデントに関する調査報告書

JNSA は，情報セキュリティレベルの維持・向上及び情報セキュリティ意識の啓発、情報提供などを行うことを目的として設立された特定非営利活動法人である[9]．本研究では「2010 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」を用いた．この報告書は JNSA が独自に，新聞などで報道された個人情報インシデントの情報を集計し，分析を行ったものである．この調査においてもインシデントは業種別に分類されている．表 2 に大学が業種として分類される「教育・学習支援」について，JNSA による集計及び分析を抜粋して掲載する．

## 4　警察庁不正アクセス行為対策等の調査

### 4.1　概要

この調査は警察庁により 2011 年 11 月 2 から 12 月 2 日にかけて行われた，無作為抽出によるアンケート調査である．発送数 3000 に対して 827 の回答が得られている．調査項目は業種，

表 2: JNSA による集計及び分析（抜粋）

| 分析項目 | データと傾向 | JNSA による分析 |
|---|---|---|
| (ア)インシデント数 | 業種全体インシデント数の 11 %を占める，経年変化ではほぼ横ばい | 業種別での順位は 2007 年以降上がってきており，インシデントを積極的に公表する傾向が浸透してきている. |
| (イ)1 件当たりの被害件数(人数) | 全被害件数のうち 2.4%と少ない | 扱う個人情報はクラス単位などが多いため，1 件当たりの 被害件数は数十人と他の業種に比べて少ない. |
| (ウ)原因別 | 「不正な情報持ち出し」の比率が高い | 業務特性と個人情報の持ち出しルールがかい離し，形骸化している可能性がある. |

情報システムの利用環境から始まり，セキュリティ対策，セキュリティインシデントの対応など 62 項目に及ぶ.

## 4.2 業種「教育」の傾向

ここでは，調査報告書に基づいて，業種「教育」に関する集計結果を抜粋した. また，一部比較のため，大学と同様に公共性の高い行政または差が顕著な金融，及び全業種の結果を示す.

(a)外部からの接続目的のうち，”基幹業務システムのアクセス”と回答

教育 : 20.7%
行政 : 13.0%
全業種 : 33.5%

(b)セキュリティ対策の必要性 : “「非常に」，「ある程度」感じている”と 98.7%が回答

(c)必要性の理由のうち,“顧客等との取引を万全なものとするため”と回答

教育 : 22.0%
行政 : 25.3%
全業種 : 41.2%

(d)セキュリティポリシーの策定状況 : “策定済”及び ”策定中”の合計

教育 : 61.2%
行政 : 97.6%
全業種 : 81.9%

(e)インシデント発生時の対応策 : ”策定済”及び”策定中”の合計

教育 : 44.0%
行政 : 77.3%
全業種 : 55.5%

(f)ISMS，専門家等によるチェックの実施

教育 : 9.9%
行政 : 29.4%
全業種 : 24.7%

(g)監査の実施頻度，短い期間(3～6 か月)で行っている大学はほとんどない(2.7%).

(h)外部からの接続時の ID/パスワードによる認証の利用

教育 : 81.9 %
行政 : 38.2%
全業種 : 65.4%

(i)セキュリティ投資 : 両極尺度“必要最低限”または”積極的投資”で” 必要最低限”傾向の回答

教育 : 38.9%
金融 : 28.9%
全業種 : 38.4%

(j)事後対応と予防 : 両極尺度“事後”または”予防”で” 事後”傾向の回答

教育 : 30.3%
金融 : 12.1%
全業種 : 23.4%

(k)非技術的対応 : 両極尺度“教育”または” 罰則”で” 教育”傾向の回答

教育 : 66.5%
金融 : 48.9%
全業種 : 52.6%

(l)従業員（教職員）のプライバシー（モニタリングなど） : 両極尺度 “業務上やむを得ない”または” プライバシーはある程度考慮す

べき”で” プライバシーはある程度考慮すべき”傾向の回答

| | |
|---|---|
| 教育 | : 32.3% |
| 金融 | : 11.1% |
| 全業種 | : 37.0% |

## 5　状況・調査から見る大学の特徴

まず，IPA 情報セキュリティ対策ベンチマーク「医療・福祉、教育・学習支援業」のスコアは 25 項目中 24 項目で GⅢよりも低く，セキュリティ対策全般にわたって低いことがわかる．また，警察庁の調査における(e),(k),(l)など予防的なセキュリティ対策を後回しにしている傾向がうかがえる．これは大学ではセキュリティインシデントにより直接的に売り上げ（受験者数）などいった消費者・市場の評価を受けにくいためだと考えられる． また，(25)事業継続のみ「医療・福祉、教育・学習支援業」のスコアが GⅢより大きい値を示している．さらに警察庁の調査(a)(c)でも業務としての情報システム利用が少ない．これはセキュリティ対策が不十分であっても事業としては成り立つという IT 依存度の低さを示していると考えられる．

警察庁の調査(k),(l)から，大学という組織では，特に教員のガバナンスが明確でない場合もあり[2],積極的（強硬）なセキュリティ対策を導入できていない．これは IPA による調査(1)(2)など組織全体としての取り組みで GⅢとの差が比較的大きいことからも見て取れる．しかし，JSNA の調査（ア）から，発生（報告）件数が年々上昇していること，また，警察庁の調査で(b)セキュリティ対策の必要性をほとんどの回答者が感じていることから，セキュリティに対する意識向上あるいはルールの適正運用の浸透が推測される．

また，多くの大学には情報センターや情報系担当事務などの全学組織としての情報系部署が設置されている．IPA 情報セキュリティ対策ベンチマークのスコアにおいて「医療・福祉、教育・学習支援業」と GⅢとの差が小さい，すなわち比較的良いスコアである(16)通信ネットワークの保護策,(20)ネットワークアクセス制御,(23)障害対策は，主として情報系部署などが行う対策であることが多い．一方，(15)脆弱性対策や(18)データへのアクセスのスコアは GⅢとの差が大きい．これら対策はそれぞれのシステムで行う対策である．情報系担当部署の職員と異なり，運用担当者が必ずしも情報セキュリティに明るいとは限らないため，十分な対策が行われていないことも考えられる．

## 6　大学の状況を考慮した提案

警察庁の調査において，(d)セキュリティポリシーや(e)インシデント発生時の対応策の策定が他の業種に比べて不十分であることから，先ずはルール自体の施行が急がれる．JNSA の調査において最も発生件数が多い「不正な情報持ち出し」に着目すると，IPA 情報セキュリティ対策ベンチマークにおいて，「医療・福祉、教育・学習支援業」の(6)従業者との契約，(11)書類・媒体の管理のスコアは，GⅢとの差が他の項目に比べて小さい．それに対して，(17)媒体の紛失・盗難対策はすべての項目の中で，GⅢとの差が最も大きい．この違いが「不正な情報持ち出し」を引き起こしていることの要因の一つであると推測される．「不正な情報持ち出し」を行なわせないためには，(6) 従業者との契約，(11) 書類・媒体の管理，そして(17) 媒体の紛失・盗難対策の間で齟齬や抜け穴のないルール作りが必要である．

技術的な対策もまた有効であると考えられる．例えば，「不正な情報の持ち出し」に対しては, USB メモリ等の利用をできなくなる仕組みや，通信の監視による制御などが挙げられる．さらに，業務形態の見直しも対策の一つであろう．「不正な情報の持ち出し」の要因の一つに自宅での業務が推測される．こ

のような行為が行われないような業務改善等を行うことも重要なセキュリティ対策になると考える.

また，大学におけるガバナンスが不明瞭な点を解決することにより，セキュリティ向上につながると考えられる．これには組織全体の取り組みのスコアが低いことから，策定したルールを組織構成員に浸透させることが効果的であると思われる.

個々のシステムの対策が不十分な点に関しては，システムを情報系担当部署へ移管することによる一元管理なども有効な対策である.これにより，人的なセキュリティコストを削減することも考えられる.

## 7　おわりに

本研究では，IPA「セキュリティ対策ベンチマーク」，JNSA「情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」及び警察庁「不正アクセス行為対策等の調査」を用いて，大学における情報セキュリティの状況を分析した．これらから，大学における情報セキュリティ対策はまだ不十分であることが示された．また，分析によって明らかになった問題への対策を提案した.

大学における情報セキュリティ対策の向上のためには，大学組織の特異性，特に教員組織あるいは教員個人の独立性とのバランスをうまく保ってマネジメントを行う必要がある.

そもそも大学本来の業務は IT 依存度が低い.そのため，IT による統制も行われず，それに伴い IT に対する統制も不十分になっていると我々は考える．しかし社会環境における IT 利用は今後増大し，それに伴って大学の業務自体も IT 依存度が高まることが推測される．それに追随したセキュリティ対策ではなく，先を見越した対策が望まれる.

## 参考文献


[1] ISMS 認証取得組織検索,
http://www.isms.jipdec.jp/lst/ind/

[2] 上原哲太郎，”大学のセキュリティ～IT ガバナンスの視点から～”，CTC アカデミックユーザアソシエーション，2011 年

[3]山之上卓，辰己丈夫 他，“情報倫理ビデオの製作と大学の情報セキュリティへの応用”，信学技報．ICM，情報通信マネジメント 108(24), 71-76, 2008-05-01

[4]石坂徹， 早坂成人他．“小規模大学における教職員向け情報セキュリティ教育の実践”，大学情報システム環境研究 13，31-36，2010-03

[5] 情報セキュリティ対策ベンチマーク
http://www.ipa.go.jp/security/benchmark/benchmark_tokuchover34.html

[6]日本ネットワークセキュリティ協会，2010 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～,2011

[7]警察庁，不正アクセス行為対策等の調査，2011

[8]独立行政法人 情報処理推進機構
http://www.ipa.go.jp

[9] 日本ネットワークセキュリティ協会
http://www.jnsa.org