論　　文

大学の情報セキュリティに関する一考察

A Study On University Information Securities

西山　茂

概要

今日、企業の情報セキュリティに対しては多くの情報が提供されている。しかし、大学は事務職員、常勤教員、非常勤教員、学生など一般の企業とは異なる組織構成・組織特性を持っているため、情報セキュリティに関しては企業に対して提供されている対策などはそのまま適用できない部分がある。

そこで、本論文では、まず、情報セキュリティを取り巻く環境、大学の情報セキュリティの特異性を述べ、それらを踏まえて、大学の情報セキュリティに対する考察をおこなう。その結果に基づいて、それぞれの構成要素（事務職員、常勤教員、非常勤教員、学生など）に対する大学の情報セキュリティに関する考慮事項と対処を提案する。

キーワード：情報セキュリティ、大学、特異性、研究室、教職員

１．はじめに

今日、情報セキュリティに関しては企業に対しては多くの情報が提供されている。しかし、大学は一般の企業とは異なる組織特性を持っている。このため、情報セキュリティに関しては企業に対して提供されている対策などはそのまま適用できない部分がある。IPA に問い合わせたところ大学向けのセキュリティは検討していないとの回答を得ている。

そこで本論文では、大学における情報セキュリティの在り方について述べる。

２章では情報セキュリティを取り巻く環境、３章では大学の情報セキュリティの特異性、４章では大学の情報セキュリティに対する考察と提案を述べ、大学の情報セキュリティの在り方について提案をする。

２．情報セキュリティを取り巻く環境

現在の情報セキュリティを取りまく環境は、以下のような特性を持つ。

（1）　情報処理環境の高度化（ネットワークの高速化、コンピュータの高速化、モバイル環境の発達）

（2）　個人情報への意識の高まりと個人情報漏えい

（3）　個人情報暴露の高頻度化

（4）　情報不正取得手法・技術の高度化、大衆化

以下で各項目を詳述する。

２．１　情報利用環境の高度化

ここでは、情報利用環境の高度化とは次のことを指す。

① ネットワークの高速化
② コンピュータの高速化
③ モバイル環境の発達

以下、それぞれについて述べる。

２．１．１　ネットワークの高速化

ここでいうネットワークとは、加入者系のネットワーク（家から電話局、あるいは、移動通信機から基地局）を指す。

総務省の令和２年版情報白書［１］によれば、ブロードバンドの固定系ブロードバンド契約数は 4120 万契約、移動系ブロードバンド契約数は LTE と BWA を合わせて２億２千万契約である。日本の世帯数が約 5300 万世帯、人口が約１億２千万人である［２］ことを考えると、極めて高い普及率であると言える。

ネットワークが高速化するということは、大量の情報が伝送路上を流れるということであり、セキュリティ上の事故（インシデント）により大量の情報が流失することを意味する。

２．１．２　コンピュータの高速化

Moore の法則があたかも自然法則であるかの如く、LSI の集積度は 1965 年から１年半で２倍になるという成長を続けてきた。昨今はこの伸びが止まると言われているが、現状成長は続いている。

Intel© の Core™ i 9-10980XE プロセッサー エクストリーム・エディションは、クロック３－ 4.7GHz で動作する 64 ビットのコアを 18 個持ち、36 のスレッドを処理できるという極めて高速で動作し、情報の大量処理ができるコンピュータである［３］。

ネットワークと同様、コンピュータが高速・高機能であるということは、高速に大量の情報が処理されるということであり、セキュリティ上の事故（インシデント）により大量の情報が流失することを意味する。

２．１．３　モバイル環境の発達

前述の令和２年版情報白書によれば、スマホの保有率は表 2.1 のようになっている。

表２．１　スマホの年代別保有率

全年代	13～19 歳	20 代	30 代	40 代	50 代
56.8%	81.4%	94.2%	90.4%	79.9%	66.0%

これによれば、最も活動的な 10 最代後半から 40 歳代では、スマホの保有率は、ほぼ８割を超えている。

また、令和元年版情報通信白書によれば、タブレット端末の世帯保有率は 2018 年度で 40.1％になっている［４］。

モバイル端末は持ち歩くことが前提である。これにより情報セキュリティ上以下の問題を起こす可能性が高まる。

・ 端末を盗難・紛失する機会が多くなり、情報流出の頻度が高まる。警視庁によれば、令

和元年中の携帯電話類の拾得件数は 152,972 件に上っている［５］。

・ 電車やバス、コーヒー店などでの端末操作を第三者が傍で見ることにより、情報が流出する。

２．２　個人情報への意識の高まりと個人情報の漏えい

1990 年代頃からコンピュータとインターネットの発展により、行政や企業等が保有する膨大な個人情報が処理されるようになり、個人情報の取り扱いに関する意識が高まり、個人情報漏洩によるプライバシー侵害への危険性､不安が増大していった。これに対応するために､2003 年（平成 15 年）５月 23 日に個人情報保護法が成立し、一部規定を除き即日施行された。２年後の 2005 年（平成 17 年）４月１日には全面施行された。

この法律は施行当初は、極めて限られた特定の者しか個人情報が扱えないようにするなど過剰な反応も見られたが、現在では、個人情報を適正に扱うための重要な基盤となっている。

このような法律があるにも関わらず、個人情報の漏えいは止まっていない。

2020 年１月に東京商工リサーチ社が公開した「『上場企業の個人情報漏えい・紛失事故調査』［６］」による 2012 年から 2018 年までの上場企業の個人情報漏えいがあった企業数と漏えい件数を図２.１に示す。個人情報漏えい事故（インシデント）は 2013 年に大きくハンプがあるが、その後は企業数で 60 ～ 80 社、件数で 80 ～ 100 件の間で推移していて、毎年のように漏えいインシデントが起きていることを示している。2019 年には、個人情報の漏えい・紛失事故を公表した上場企業は 66 社 86 件、漏えいした個人情報は 903 万 1,734 人分に上っている。これは１企業当たり 17 万 6800 件の個人情報が漏えいした勘定になる。

個人情報の漏えいは、企業活動に深刻なダメージ（信頼の喪失）を与えるだけでなく、個人のプライバシーや財産権が侵害されることになり、その防止策は社会的に極めて重大な関心事・課題になっている。

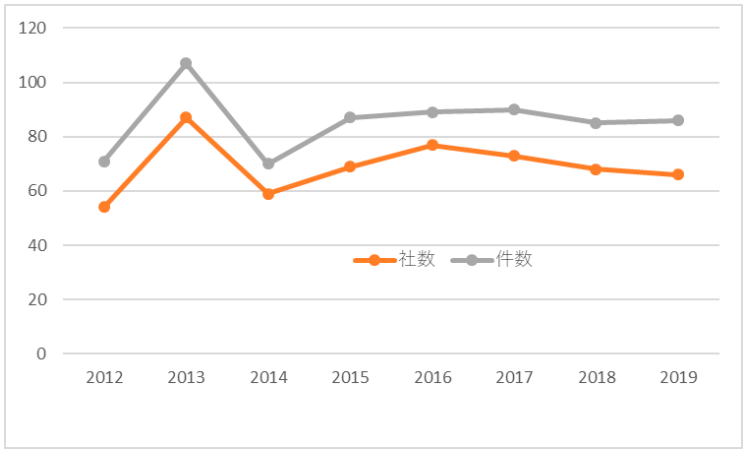

図２．１　上場企業の個人情報漏えい企業数と漏えい件数

２．３　個人情報暴露の高頻度化

インターネットは、商用化当初（日本では 1993 年ころ）は、情報の検索･取得が主であったが、現在は、生活のあらゆる局面で利用されるようになってきている。総務省統計局のデータ［７］によると、2005 年で５％程度であったインターネットショッピングの世帯利用率は 2018 年では約 40%にもなっている（図２）。世帯主の年齢が 40 歳未満である場合は、世帯利用率 62.4%、１ヵ月平均の支出額は 17,658 円であるとしている。支出額の全世帯平均は、12,610 円である。総務省統計局のデータによれば、2018 年の１世帯当たりの平均所得は 552 万円であり、月平均では 46 万円になる。したがって、世帯当たり全所得の 2.8%をインターネットショッピングにより消費していることになる。

インターネットショッピングにおける購入側の支払い方法や情報供与方法は多種多様であるが、クレジットカード情報、住所、氏名、年齢などがネット上を流れることになる。インターネットショッピングの利用率の増加は、個人情報の暴露の高頻度化につながる。

表２.２は、株式会社 UNIAD が集約して公表している SNS の利用者数を示したものである［８］。それぞれの利用者数の数字は当然重複している部分があると思われるが、それでも日本の人口が１億２千万人であることを考えると、極めて多く人が SNS を利用していることがわかる。SNS の利用は必然的に個人情報の暴露につながる。

２．４　情報不正取得手法・技術の高度化、大衆化

ここでいう情報不正取得とは、俗にハッキング、クラッキングと呼ばれる、不正に個人情報を取得する技術を指す。

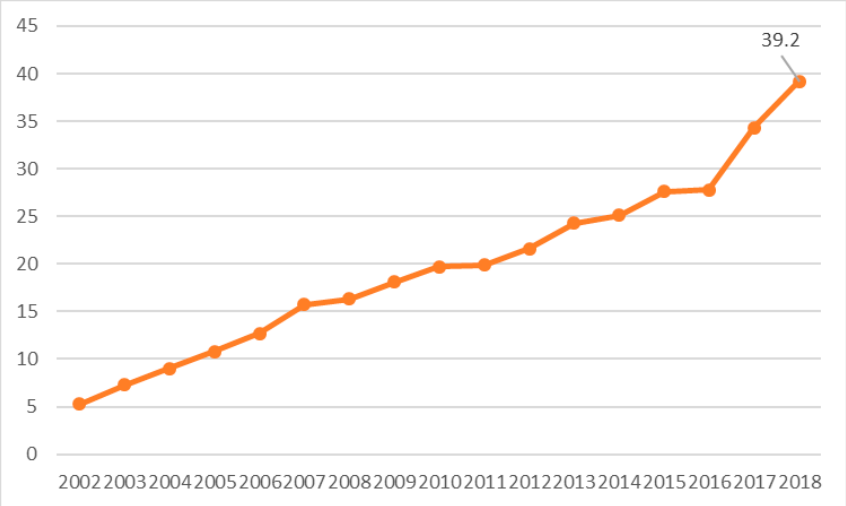

図２．２　世帯当たりのインターネットショッピング利用率

表２.２　各 SNS の利用者数

No	SNS 名	利用者数（万人）	各メディアの公表時期
1	LINE	8,400	2020 年 7 月
2	Twitter	4,500	2018 年 10 月
3	Instagram	3,300	2019 年 3 月
4	Facebook	2,600	2019 年 7 月
5	TikTok	950	2018 年 12 月
6	Pinterest	530	2019 年 8 月

ソーシャルエンジニアリング、ウィルス等を利用した情報の不正取得は日々巧妙さを増し、様々な被害を生み出している。

警視庁の資料［９］によれば、

- 従来から発生している犯罪に加え、新たな手口の犯罪が発生している
- 2019 年のサイバー空間における探索行為（脆弱性を探る行為）は、4,192.0 件／日・IP アドレスと、増加傾向にある
- 2019 年中の標的型メール攻撃の件数は 5,301 件である

として、懸念を示している。これらの事象は、不正情報取得の手法・技術の高度化がその一因になっていると考える。

一方、Windows の Edge で「ハッキング やり方 サイト　サイバー空間」をキーワードとして検索すると、約 44 万件がヒットする。この中には、ハッキングに備えてハッキングの知識の獲得を目的とするものも多いが、不正情報取得方法を教示するものもある。このようなサイトがあるということは、誰でもハッカー（不正情報取得者）になることができるということ（ハッキング手法の大衆化）であり、不正情報漏えいの被害の拡大に繋がると懸念される。

３．大学の情報セキュリティの特異性

本章では、大学の情報セキュリティ特徴について述べる。本章は、国内の複数の大学を調査した結果を集約したものではなく、本学の状況を念頭に述べる。しかし、かなり他の大学、殊に私学と共通する部分があると思われるため、情報共用になると考える。

３．１　大学の組織構成

新潟国際情報大学（以下、NUIS と呼ぶ）の組織図は大学 Web サイトで公開されている［10］。この組織図は機能を表現したものであり、セキュリティの観点からは不十分である。情報セキュリティの観点で考えた大学の組織図を図３.１に示す。

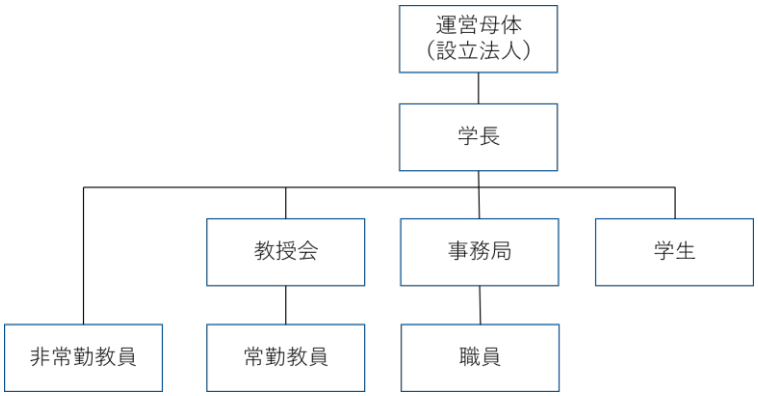

図３.１　セキュリティの観点から考えた NUIS の組織図

図３.１と大学が公表している組織図の大きな違いが、組織の中に学生と非常勤教員が組み込まれている点である。

学生は、企業組織であれば顧客に相当するものであるが、次のような特徴を持ち、大学組織の一部とみなす必要がある。

①　大学ではネットワークを教職員と共用する
②　ある程度自在に建物を利用する
③　学則で行動を拘束される（顧客を社内規則で拘束する企業などはない）

非常勤教員は、高度な知識・スキルを持った派遣社員的な性格の教員である。大学行政管理に携わることはなく、教授会の指示に従う必要はないが、以下のような特徴を持つため、学生と同様に大学組織の一部とみなす必要がある。

①　情報供与、情報共有のため学内システムにアクセスする
②　学生の氏名や成績情報など機密情報を持つ

３．２　情報セキュリティの観点から見た大学の組織の特徴

３．１節で述べた組織図の構成要素のうち、事務局及び職員は通常の企業の組織員（社員）などと業務の進め方も命令指示系統も大きく変わることはないため、世に喧伝されているセキュリティの体制、進め方を援用できる。しかし、学生及び（常勤、非常勤の）教員は企業組織の構成とはかなり異なる性格・行動パターンを持つ。このため、それに応じたセキュリティの進め方を取る必要がある。

本節では、各構成員の特徴を述べ、４章でそれぞれに対するセキュリティの進め方を提案する。

３．２．１　学生

学生は様々なガイドライン文書（テキスト）やガイダンス等により、大学の情報システムにアクセスする場合はセキュリティに注意するように指導を受ける。しかし、学生は当事者意識が薄く、ガイドライン文書に十分に目を通すこと、ガイダンスの話の内容に十分に耳を傾けることを

学生に期待することは難しい。したがって、大学の情報セキュリティに関するルールを守らせることはかなり難しく、実際にセキュリティ上問題のある行動をとることは多々ある。

３．２．２　非常勤教員

非常勤教員は、契約書あるいは別途用意されるNDA（Non-Disclosure Agreement：秘密保持契約）によって、大学の情報セキュリティルールの遵守を要請される。しかし、非常勤教員は、非常勤教員として勤務する大学を離れれば本務先の組織人であったり、場合によっては組織に属さない個人であったりする。このため、情報セキュリティに対する意識は本務先のものであったり、個人的なものであったりして、非常勤教員として勤務する大学のものとは異なることが考えられる。

また、非常勤教員は、個別の研究室が与えられておらず、学生の成績情報は自宅（あるいは本務先）に持ち帰って情報システムに投入することが多く、情報漏えいの機会が増す。

３．２．３　常勤教員

常勤教員の特性を以下で述べる。

（１）独立志向

常勤教員は、大学組織の一員ではあるが、通常の企業などの組織の所属員と違い、学問の自由などの観点を理由に、事務的な制約を回避する傾向がある。言い方を変えると組織の決めたルールに理解を示し、それに従うということを嫌う傾向がある。

（２）ルールを意識しない、ルールに縛られない／縛らない

理由は判然としないが、常勤教員は、組織のルールに関心が低いことが多い。このため、大学内の様々なルールを無意識のうちに破っていることも多い。

また、これも理由は判然としないが、事務職員は、常勤の教員にルールを強制することは少ないようである。

（３）居室（研究室）

常勤教員は、個人ごとに「研究室」と呼ばれる隔離された居室が与えられることが多い。研究室の使用法に関するルールはほぼなく、常勤教員は各自の好み、仕事（研究や学生指導等）のし易さに応じて自由にレイアウトして使用する。

通常の組織の場合、組織員は周囲から見える仕事机と場合によってはロッカー（書類棚）が与えられる。これらは周囲の目があるため、余り乱雑には使用されない。

しかし、研究室は周囲の目から隔離されており、整理整頓状況を第三者によってチェックされることもないため、乱雑に使用されることが多い（もちろん属人的ではある）。

研究室には様々な情報やものが置かれている。その一例を以下に示す。

- 授業資料
- 成績関連資料
- 研究資料（個人、共同）
- 学内委員会資料
- 学外活動（行政や地域の委員会等）資料
- 書籍・雑誌
- 授業用機材
- 研究実験用機材

・　電子機器（PC、プリンター等）
・　USB メモリ、可搬型外部メモリ（HDD 等）
・　他

これらの中には機密性の高い情報を含むものもあり（成績関連資料や研究資料等）、機密保護は重要であるが、その保護・管理は居住者（当該研究室の使用者）にほぼ委ねられている。

USB メモリは小型であり可搬性が良いため、非常によく利用されている。しかし、その中には成績情報などが含まれることもあり使用には細心の注意が必要であるが、その方法については所有者に任されていることが多い。

4．大学の情報セキュリティに対する考察と提案

セキュリティ、情報セキュリティは、施設を（盗難等に対して）堅固に作ることも重要であるが、最終的にはそれを扱う「人」依存する。本章では、３章で述べた大学組織に所属する人に着目して、それぞれどのようにすべきかを提案する。

また、ここでは大学には一定のセキュリティルール（ポリシーや運用規則など）が制定されていることを前提とする。

4.1節では、大学の構成員がアクセスできる情報及び情報機材について述べる。4.2節以降で大学構成員ごとの情報セキュリティに対する考慮事項を述べる。

4.1　アクセスできる情報と情報機材

大学の構成員がどのような情報、情報機材にアクセスできるかは、情報セキュリティを検討するうえで極めて重要である。表4.1にアクセスできる情報を表4.2にアクセスできる情報機材をまとめた。

表4.1　大学の構成員のアクセスできる情報

	大学行政管理情報	学生情報	授業関連情報	備考
常勤教員	○	○	○	
非常勤教員	×	○	○	
学生	×	×	○	
事務職員	○	○	○	部署によってアクセス権が異なる

表4.2　大学の構成員のアクセスできる情報機材

	PC（大学設備）	LAN	メールサーバー	授業支援サーバー	その他の学内サーバー	備考
常勤教員	○	○	○	○	○	
非常勤教員	△	△	×	○	×	△：限定的
学生	○	○	○	○	△	△：限定的
事務職員	○	○	○	○	○	部署によってアクセス権が異なる

４.２　事務職員

３.２節の冒頭でも述べたが、事務職員はその属性が企業などの社員と余り変わることはない。そのため、定められたセキュリティポリシーを遵守するように通達を出し、必要に応じて監査（チェック）を行えば、一般企業並みのセキュリティレベルは維持できると考える。すなわち、一般企業のセキュリティ運用と同様に考えればよい。

４.３　学生

（１）啓蒙

３.２.１節で述べたように、学生に対するガイドやガイダンスは、読まれない、聞き流されてしまう、である。このように学生をルールだけで縛ることはなかなか難しい。しかし、何事によらず、啓蒙は重要である。そこで、もう少し踏み込んだ啓蒙を提案する。

現在、多くの大学で新入学生に対して高大連携の授業を行ってる。この授業の１～２コマをセキュリティの授業とし、可能であれば、小テストを行い、学生への浸透を図るとともに理解程度を把握する。

また、ゼミなどで抜き打ち的にセキュリティルール遵守度などをチェックすることも効果があると考える。

（２）情報、情報機材アクセス

学生がアクセスできる情報は授業関連情報だけであり（表４.１）、学生が大学の機密情報を漏えいする不安はない。

一方、学生がアクセスできる情報機材は、大部分の学内サーバーにアクセスできないことを除けば、ほぼ常勤教員、事務職員並みである（表４.２）。このため情報機材に対して以下のような対策を講じておく必要がある。なお、筆者が所属する新潟国際情報大学では以下のセキュリティインシデント報告以外は概ね対策済みである。

- 学生がアクセスネットワークは教員･職員がアクセスするネットワークとは別ネットワークとする
- ウィルスソフトを常に最新バージョンにする
- 学内の共用 PC は、シャットダウン時に利用者が作成、または派生させたファイルをすべて消去する
- 書式を定め、セキュリティインシデントに遭遇した場合は直ちに担当部署に報告させる

４.４　非常勤教員

非常勤教員がアクセスできる情報、情報機材は限られている（表４.１、表４.２）。注意すべきは学生の成績などの個人情報である。

非常勤教員は、非常勤の勤務先ではなく、本務先あるいは自宅などで学生の成績（個人情報）に触れることが多と思われる。

これに対しては以下のようなルールを定め、非常勤教員に遵守してもらわなければならない。

- 個人情報を平文でメールを使って送受しない
- 暗号化された個人情報であってもこれをメールで送受することは原則しない
- 個人情報は必ず暗号化して PC、あるいは可搬型のメモリに格納する
- 個人情報が格納された PC、可搬型のメモリの移動は可能な限り少なくする

- 個人情報が格納されたPC、可搬型のメモリを紛失した場合は、直ちに非常勤勤務先の大学に報告する
- セキュリティインシデントに遭遇した場合は直ちに定められた書式で非常勤勤務先の大学に報告する
- 退職する場合は、すべての個人情報を適切に破棄または大学に渡す
- 学外で個人情報を扱う場合、周囲から見られないように配慮する

なお、非常勤教員を長年にわたって務められる方は多い。このような場合、学生の個人情報が、非常勤教員のPCやUSBメモリなどに蓄積してしまう可能性がある。PCやUSBメモリに格納された学生の個人情報は学期ごとに担当部署に渡し、非常勤教員の媒体からは削除するようなルールと仕組みを整備する必要があると考える。

紙媒体に残された個人情報は、次節で述べる常勤教員の場合と同じように取り扱う必要がある。

4.5　常勤教員

常勤教員の特性は3.2.3節で述べた。その特性考慮して、以下で対応を述べる。

（1）啓蒙

全大学的な取り組みを始めるときに、①セキュリティポリシーの確認、②情報セキュリティ対策の必要性、③情報セキュリティ対策、④具体的な情報の取り扱い方、等についてフルスケールの講習会を実施する。このときに使用する資料は、全般的な話はIPA（独立行政法人情報処理推進機構）の資料［11］が役に立つ。ただし、大学固有な状況や対策に対する資料は、大学で作成する必要がある。

常勤教員の流動性は高くないため、全常勤教員に対するフルスケールの講習会は取り組みを始めるときに1回だけ実施すればよい。ただし、年に1度は教授会などの場を利用して、過去1年の情報セキュリティの状況報告や再確認事項、新しく留意しなければならないこと等について、報告周知を行う必要がある。

また、新しく採用された常勤教員に対しては、採用時にフルスケールの講習会を実施する。

（2）個人情報の取り扱い

教員が日常的に扱う個人情報は主として当該教員が担当する授業を履修している学生の情報（氏名、成績等）であるが、これらは紙媒体で保存されたり、電子的に保存されたりしている。いずれも、各教員の居室（研究室）におかれていることが多いと考える。また、その取扱いについては各教員に任されていることも多い。これは情報セキュリティの観点からは極めて高リスクの状態である。

紙媒体で保存されている学生の個人情報は、施錠でき、入退室が管理できる倉庫の様なものを用意し、年代別、学期別、教員別に保管する必要がある。また、保管年限を明確に定め、保管期限を過ぎたものは、適切な方法で順次廃棄するようにする。

電子媒体で保存されている学生の個人情報については、前節で述べた非常勤教員に対する要請事項と同じことが要請される。

また、成績など個人情報の処理は、原則、研究室（居室）で行なうこととする。

（3）監査

本来であれば、セキュリティルールの遵守状況をチェックするために居室（研究室）に立ち入って監査をする必要がある。この方法はかなりの労力と時間がかかる。例えば、新潟国際情報大学

の場合、常勤教員は 40 名程度在籍している。1 研究室当たり監査時間 30 分としても全居室を監査するために、20 時間が必要である。

また、３.２.３節で述べた常勤教員の特性を考えると居室に立ち入る監査方法にはかなりの抵抗があると思われる。

そこで、監査用の所定の書式（紙、電子のいずれでもよい）を作り、全常勤教員に記入してもらい、それをセキュリティ担当者（常勤教員と事務局員のチーム）でチェックし、必要であれば是正勧告を出すという方法をとるのが良いと考える。この監査は各学期毎に学生の成績評価が終わった後に行うのが良いと考える。

監査書式は、各常勤教員がチェックを行ったことがわかり、虚偽の報告ができないように、記述方法の工夫が必要である。

５．おわりに

本論文では、情報セキュリティ取り巻く環境、大学の情報セキュリティの特異性述べ、それを踏まえて、大学の情報セキュリティに対する考察を行った。

大学は事務職員、常勤教員、非常勤教員、学生などそれぞれ極めて性格の異なる組織要素で構成されるため、それぞれの構成要素に対して大学の情報セキュリティに対する考慮事項と対処を提案した。

今後はこれらの対策に対する数値データを集め、その有効性や不足点を明らかにする。

謝辞

本論文を作成にするにあたり、種々のデータを提供してくださり、また、問い合わせに対応してくださった新潟国際情報大学情報センター課課長補佐丑田氏に感謝する。

参照文献

［1］ 総務省，“令和 2 年版情報白書 ,”総務省，2020 年 .
［2］ 総務省統計局，“日本の統計 2020,”総務省，2020 年 .
［3］ Intel，“Intel ホームページ ,”Intel, 2020.［オンライン］. Available: https://www.intel.co.jp/content/www/jp/ja/homepage.html.
［4］ 総務省，“令和元年版情報通信白書 ,”著：令和元年版情報通信白書，2018 年.
［5］ 警視庁，“遺失物取扱状況（令和元年中),”警視庁，2019 年.［オンライン］.
［6］ 東京商工リサーチ，“「上場企業の個人情報漏えい・紛失事故」調査 ,”［オンライン］. Available: https://www.tsr-net.co.jp/news/analysis/20200123_01.html.
［7］ 総務省統計局，“急拡大するネットショッピングと電子マネーの利用 ,”［オンライン］. Available: https://www.stat.go.jp/info/today/141.html.
［8］ 株式会社 UNIAD,“【2020 年 9 月更新】主要ソーシャルメディアのユーザー数まとめ ,”［オンライン］. Available: https://www.uniad.co.jp/260204.
［9］ 警視庁 ,“令和元年におけるサイバー空間をめぐる脅威の情勢等について ,”警視庁 , 2020 年 .
［10］ 新潟国際情報大学，“新潟国際情報大学 ,”［オンライン］. Available: https://www.nuis.ac.jp/pub/common/pdf/soshiki.pdf.
［11］ 独立行政法人情報処理推進機構，“IPA　情報セキュリティ ,”［オンライン］. Available:

https://www.ipa.go.jp/security/keihatsu/features.html.