特集　情報セキュリティ

ベンチマーク評価で先進的取り組みをしている大学事例の紹介

立命館大学情報基盤課課長補佐
本協会情報セキュリティ研究講習会運営委員　沼　　将博

1．はじめに

本協会では、2015年度より毎年、加盟校に情報セキュリティベンチマーク評価をお願いしており、ベンチマーク評価の結果から課題を示してきました。本稿では、2017年度のベンチマーク評価結果から各大学が共通的にかかえる情報セキュリティ上の重点テーマについて、進んだ取り組みを行っている大学の事例を紹介します。

テーマ
・情報セキュリティポリシーと対策基準の策定
・情報セキュリティルールの周知徹底
・情報資産の把握とリスク対策

なお、本稿で紹介する事例は、情報セキュリティ研究講習会運営委員が大学を訪問しインタビューした内容、並びに本協会事務局によるメールでのヒアリング調査結果に基づき記載しています。

2．情報セキュリティポリシーと対策基準の策定

組織的な情報セキュリティ対策に取り組む上では、はじめに大学としての情報セキュリティに関する基本的な考え方を規定した情報セキュリティポリシーを制定することが重要とされています。昨今、情報セキュリティポリシーの必要性の理解は広がっており、ベンチマーク評価結果から80％以上の大学が何らかの学内ルールを定めていることが分かります。一方で、学内ルールが存在しない大学や、学内ルールは存在するが全学的

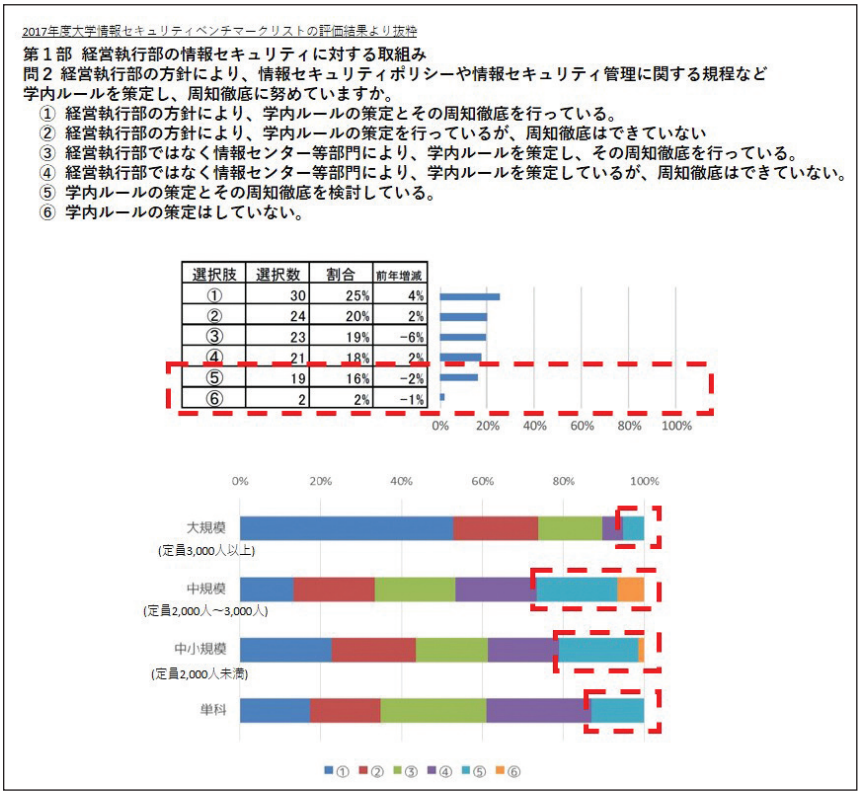

図１　情報セキュリティポリシーと対策基準の策定状況

なものではなく情報センター等部門の内規に留まっている大学が多数あることも分かります。

ここでは、2016年３月に学校法人全体の情報セキュリティポリシーを新たに作成された大学の事例を紹介します。

事例紹介（A大学）

（１）背景

- 定員3,000名以上の大規模大学で、併設校（幼稚園、小中高）が存在する
- 10年以上前より情報センターの内規としての情報セキュリティポリシーは存在していたが、学校法人全体の情報セキュリティポリシーは存在しなかった
- 社会的な情報セキュリティの重要性の高まりを踏まえ、学校法人全体としての情報セキュリティポリシーが必要な状況にあった
- 他大学との共同研究を進めていく上でも、大学間の合意に情報セキュリティポリシーが必要であった

（２）情報セキュリティポリシー案作成の流れ

- NIIが公開している「高等教育機関の情報セキュリティ対策のためのサンプル規程集」(以下、NIIサンプル規程集）を参考に情報センターでポリシー案の作成を行った
- NIIサンプル規程集を参考とすることで、他大学との共同研究時に大学間の情報セキュリティポリシーのレベルが概ね揃い、確認が容易になるというメリットも見込める

（３）NIIサンプル規程集に基づくポリシー案作成

- 学内の規程と形態が異なるため、学内の規程に合わせる形で形態を適宜修正
- 「セキュリティポリシー」という言葉自体が他規程とそぐわないため、「情報システム運用基本規程」という名称とした
- NIIサンプル規程集は膨大な量があるため、自大学に必要と考えられるところを順次取り入れていった
- 各条項に解説文がついているため、解説文を参考として、既存の就業規則との関係や組織・人員体制を踏まえ、現実的な内容になるよう不要な箇所(対応できない箇所)を削っていった
- NIIサンプル規程集は「完璧版」であるため、基本的には項目を追加する必要はない

（４）規程制定へ向けた学内調整

- 大学だけではなく併設校（幼稚園、小中高）も含む内容となるため、法人を巻き込んで調整する必要があった。したがって、CISOは、大学の担当副学長ではなく、ITサービス提供責任者である情報センター所長とした。なお、CIOは、法人規程で担当理事とかねてより定められていた
- 法人全体の規程とするために、法人内でどのようなルートで諮っていけばよいのかが、明確ではなかったため、情報センター所長（CISO）より学長へ相談し、学長から理事長へ確認いただいた
- 大学執行部より学部長会議、各学部教授会にて検討してもらったが、ポリシー案の具体的な内容ではなく、細かな文言への意見が大半であった（例：「ポリシー」という名称は規程の名称としてそぐわない）
- そもそも教授会で議論する内容ではない、と教授会での審議に諮られない学部もあった
- 学部長・研究科長会議が月２回、理事会が月１回であり毎回議題とするわけにもいかない状況。情報センター次長が事あるごとに状況を確認しフォローした
- 情報セキュリティポリシーの意義が理解されにくく、全学の危機管理の問題とは捉えられず、情報関係の問題として扱われる傾向があった
- 最終的には、総務部が起案元となり規程として制定された
- 制定された情報セキュリティポリシーは冊子化して学内へ配布した

（５）情報セキュリティポリシー制定時に考慮した点

- 情報セキュリティポリシー制定により新たな制限ができるのではなく、今まで良識を持って利用者が行ってきたことを明文化したもの、という位置づけとした
- 懲罰規程については「情報」かどうかにかかわらず、「法人に与える影響」で就業規則に基づき処罰が決まることとし、情報セキュリティポリシーからは除外した
- 情報セキュリティポリシーは緩い内容であっても存在することが重要。情報セキュリティポリシーがあることでその内容について議論が発生し、啓発につながる。一方で明文化されたポリシーがないと無法地帯になってしまう
- USBメモリ利用禁止など（当時）実現不可能な内容を定めると、ポリシーは守られず意味がない。USBメモリの管理をしっかりと行うこと、など現実的で啓発につながる内容とした
- NIIサンプル規程集のように「基本方針」と「対策基準」の２つの規程を制定するのは難しいので、１つの文書にまとめてしまったことも良かった点である

上記の事例より、CISOと情報センター等部門が主体となり行動し、早い段階で経営執行部に情報セキュリティポリシーの必要性を理解いただくことが重要と言えます。事例の大学では、情報セキュリティーポリシーや対策基準を策定する際

に、理想論ではなく大学の実情に合わせた現実的な内容とすることを心がけています。理想論で作成すると、情報センターが管理を厳しくしたがっているという誤解を招き学内での理解が得られない場合や、仮に制定しても守られない意味のないポリシーとなってしまいます。

3．情報セキュリティルールの周知徹底

情報セキュリティポリシーや対策基準は策定しただけでは効果がなく、構成員（学生、教職員等）に周知徹底し、一人ひとりが正しくその内容を理解することが重要です。一方で、周知徹底のための方策として、Webサイトや学内文書での情報提供のみに留まる大学が多いことが図２のベンチマーク評価結果から分かります。

ここでは、Webサイトや学内文書での情報提供以外に、危機意識の共有化や学内ルールの周知徹底のために、進んだ取り組みを行っている大学の事例を紹介します。

事例紹介（B大学）

- 教職員対象の情報セキュリティ講習会を毎年９月に実施し、義務化している。（2018年度からは、e-Learning形式で６～８月を受講期間として実施している）
- ルールの周知は、特に注意してほしいルールを抜粋した情報セキュリティガイドブックを作成し、学内の教職員専用Webサイトに掲載している。また、新任教職員には着任時に印刷して配布し、講習会などで情報セキュリティガイドブックの存在を周知している
- 定期的な情報提供は、長期休暇前の注意喚起など、IPAの呼びかけ内容を参考に毎月の報告資料に記載している。また、メールでの注意喚起を必要に応じておこなっている

事例紹介（C大学）

- 危機意識の共有化は、学内で確認された情報セキュリティインシデント事案の報告等を通じて、全学教職員にメール配信等により周知している。主に教学部門の長（学長、常務理事、副学長、学部長、学科長、委員会委員長）が参加する会議において報告し、所属長との情報共有を図っている。これらは全てインシデント発生の確認から１か月以内に実施するようにしている
- 学内ルールの周知徹底と遵守の確認は、「情報セキュリティ講習会」にて情報共有すると共に、隔年で全教職員を対象とした「情報セキュリティチェックシート」を用いた自己点検調査を通じて遵守確認を行っている。その自己点検調査の集計結果を次回の講習会等で取り上げることで全教職員へのフィードバックを行っている
- 自己点検調査の時期は、４月新規採用者の業務内容や学内ルール理解ならびにこれらへの順応状況等に配慮して、後期開始後の10月頃に実施するようにしている

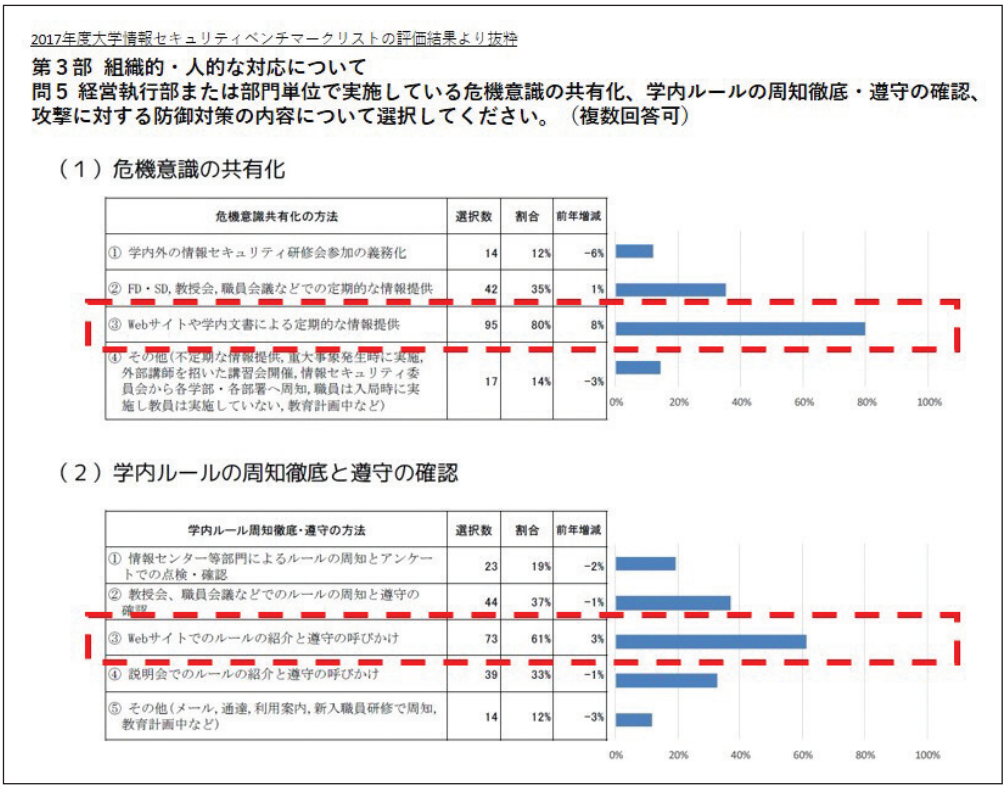

図２　情報セキュリティルールの周知徹底に関する状況

事例紹介（D大学）
- 年に数回、教職員や学生を対象とした情報セキュリティ研修を行っている。なお、セキュリティ研修会の参加については、ｅラーニングによる義務化を検討している
- 3,000名以上の教職員に学内ルールを周知するために、年度の始めに法人全職員に対して情報セキュリティハンドブック（冊子）を配付し、各自の責任と自覚、パソコンの管理、データの管理、インシデント発生時の対応手順、セルフチェック等を記載しており、注意する事項の確認や自身の状況が認識できる。なお、アンケートでの点検・確認、遵守状況の確認までは行っていない
- 学外組織からの情報セキュリティに関する情報提供やインシデント報告を受けた場合、学内での状況を確認するとともに、各種委員会や学内ポータルサイトで利用者に情報提供を行っている

上記の事例のとおり、危機意識の共有化や学内ルールの周知徹底のために進んだ取り組みを行っている大学では、
- セキュリティ講習会（e-Learning含む）の受講を義務付け定期的に実施する
- 規程とは別に、利用者に伝わりやすい形でセキュリティガイドライン、ハンドブック等を作成し配布する
- 危機意識の共有については、実際に学内で発生したインシデント事例やフィッシングメール文面を周知する
- 一般教職員への周知のほかに、経営執行部への定期的な状況報告を行う

といった対応が進められています。

４．情報資産の把握とリスク対策

情報セキュリティ対策を検討する上で、守るべき情報資産を正確に把握することは必要不可欠です。しかしながら、次ページ図３のベンチマーク評価結果から、半数以上の大学において、重要な情報資産の目録を作成できていないことが分かります。一方で、重要な情報資産へのアクセス制御を行っていると回答した大学は70％を超えています。守るべき情報資産が正確に把握できていない中で、一部の情報資産のみを対象にアクセス制御したとしても、十分な対策とは言えません。

情報資産の目録を作成し、作成した目録を継続的にメンテナンスしていくためには、大学全体を巻き込んだ取り組みが必要となりますが、可能な範囲から少しずつでも計画的に対応を進めていくことが重要です。

ここでは、重要な情報資産の把握とリスク対策について、進んだ取り組みを行っている大学の事例を紹介します。

事例紹介（E大学）

（１）概要
- 情報資産の「機密レベル」、「保管場所」を定義し各部署で情報資産台帳を作成し管理
- 情報資産台帳は定期的に管理検査を実施
- 情報資産の管理対象は法人業務を担う職員等、および職員等が利用するPC（教員は対象外）
- 総務部門と情報システム部門の職員のチーム体制で情報資産の「管理窓口」を担う

（２）情報資産の機密レベルの定義
- 【高リスクデータ】
  データの保護が法律、規則によって要求されているもしくは機密性、完全性、可用性の損失が大学に重大な影響を及ぼす可能性がある。当該データの保管に当たっては、個別に保管場所および取扱いを定めたうえで「管理窓口」に届出を行い、承認を得なければならない
- 【制限データ】
  データは一般に公開されておらず、機密性、完全性、可用性の損失は大学に悪影響を及ぼす可能性がある
- 【公開データ】
  高リスクデータ、制限データのいずれにも該当せず、すでに公開されているか、機密性、完全性、可用性の損失が大学に悪影響を与えないデータ

（３）情報資産の保管場所の定義
- 情報資産の保管場所として以下を定義
  - 大学共通オンプレミスファイルサーバ
  - 大学提供外部クラウドストレージ
  - 職員等利用PC
  - 大学情報システム
  - 例外的な保管場所
- 例外的な保管場所の利用並びに、データの持ち出し時には「管理窓口」への届出が必要

（４）情報資産台帳の起票目的
- 高リスクデータがどのような管理方法で保管・運用されているか。
- クラウドストレージや例外的な保管場所での運用が必要な制限データがどのような管理方法で保管・運用されているか。
- 情報資産を学外にどのような目的・方法で持ち出しているか。

（５）情報資産台帳例
- 情報資産の機密レベルごとに台帳を分け、各台帳では機密レベルに応じて必要となる項目を記録、管理する。
- 共通項目として、資産名、保管開始日、保管終了予定日、保管終了日(削除日)、取扱責任者、保管目的、保管場所、承認日、承認者を

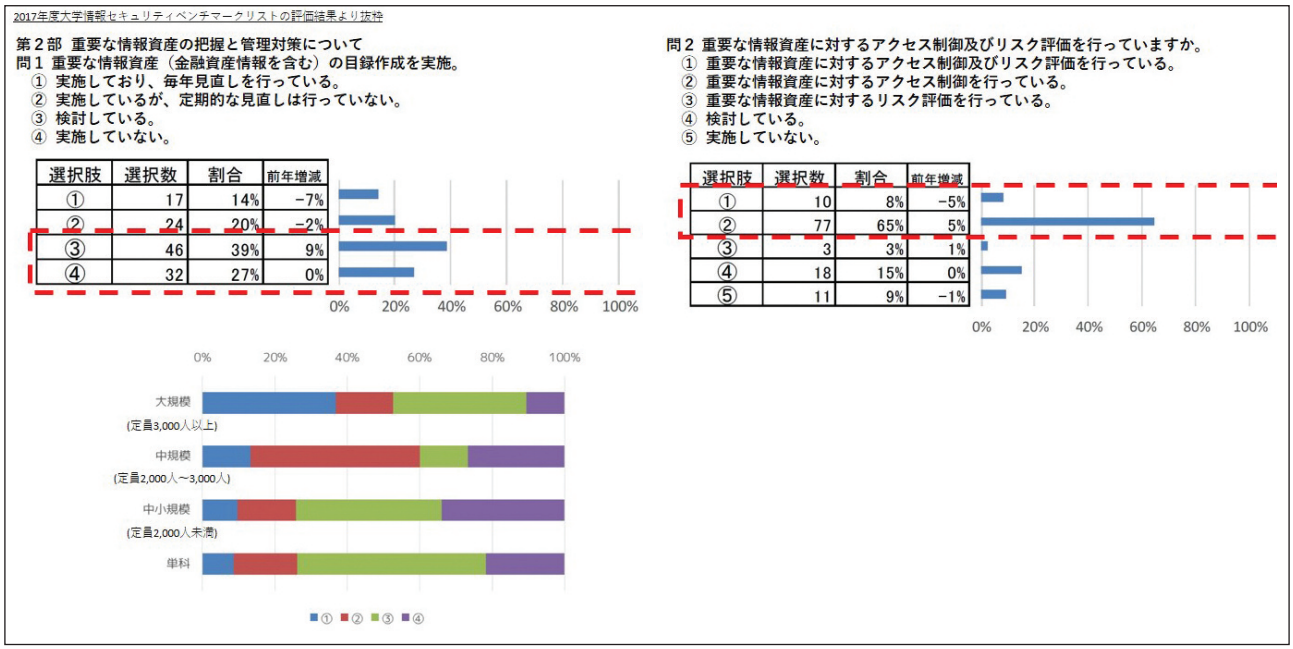

図３　情報資産の把握とリスク対策に関する状況

記録する。
- 高リスクデータの台帳については、共通項目に加え、管理窓口への届出日と承認日を記録する。
- 制限データのうち、例外的な保管場所に保管されるデータは、保管媒体と保管方法並びに、管理窓口への届出日と承認日を記録する。
- 制限データを持ち出す場合は、持出者、持出方法、持出目的持出先並びに、管理窓口への届出日と承認日を記録する。

（６）管理検査の実施
- 以下の４レベルで定期的に検査を実施する。
  - 担当者の随時のチェック
  - 担当管理職の隔月のチェック
  - 部署の年次のチェック
  - 検査チームの管理検査

（７）検査チームの管理検査内容
- 実施頻度は、20部署程度を検査対象として年１回。概ね３年かけて全部署を検査
- 検査チームは、管理窓口のチームが担当。管理職１名と一般職２名の計３名のグループを３グループ作り、検査にあたっている
- 検査内容は、事前に検査チームが検査対象部署の台帳から情報資産の内容を把握した上で、特に高リスクデータの保有の必要性や、その管理方法をヒアリング
- 検査の趣旨は、部署で情報資産の管理が正しくされていることの最低限のチェックと、各部署での情報資産の取り扱いに関して困っている点等、課題と部署独自の工夫等、グットプラクティスの抽出を目的としている
- 浮き彫りになった課題で全学的に共通化できるものについて、検査チームで検討し管理方法や台帳等の見直しを実施
- 各部署には、従来の業務に加え、情報資産台帳への記載など、新たな作業が生じることになるため、実施当初から、それなりの反発が予想された。そのため、検査という名称をとっているが、情報資産管理の必要性や情報セキュリティに係るリスクを説明し、理解してもらうことと、各部署の業務の特性や事情を聞いて、困っている点を一緒に考えるというスタンスをとっている

上記の事例から、情報資産の把握を具体的に推進するチームやワーキンググループを立ち上げ、統一された観点や手順を示し対応することが有効と言えます。情報資産の台帳管理を進める上では、整理完了後の定期的な点検の方法についても、合わせて検討しておく必要があります。情報資産の具体的な洗い出し作業については、学内の各部署（現場）で行うしかありません。大学全体を巻き込んでの作業となるため、経営執行部の理解を得るとともに、現場に作業の必要性を理解してもらう取り組みが必要です。

５．まとめ

本稿で取り上げたテーマは、多くの大学で課題認識され、対応を検討されていることと思います。事例紹介の内容が、各自の組織での情報セキュリティ対策上の課題解決に向けた対応の参考となれば幸いです。