＜セキュリティ政策・運営コース＞

B-2.「ベンチマークリストで先進的取組みをしている大学を参考に整備計画を考える」

立命館大学 沼 将博

本セッションの目的

- 本セッションでは、大学情報セキュリティベンチマーク(2017)の結果から、組織的情報セキュリティ対策に先進的に取り組んでいる大学の事例を参考として自大学の整備計画を振り返ります。

テーマ1　情報セキュリティポリシーと対策基準の策定
テーマ2　情報セキュリティルールの周知徹底
テーマ3　情報資産の把握とリスク対策

セッションの流れ

テーマ1

情報セキュリティポリシーと対策基準の策定

- 大学事例紹介
- グループワーク

テーマ2
テーマ3

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

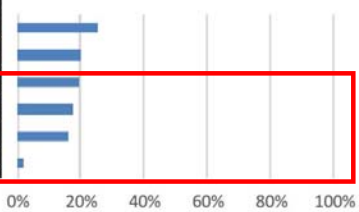
- 大学事例紹介
- グループワーク

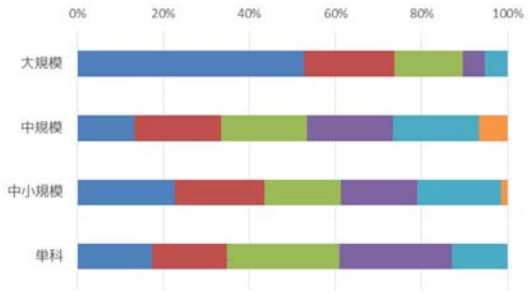
テーマ1：情報セキュリティポリシーと対策基準の策定

問２　経営執行部の方針により、情報セキュリティポリシーや情報セキュリティ管理に関する規程など学内ルールを策定し、周知徹底に努めていますか。

① 経営執行部の方針により、学内ルールの策定とその周知徹底を行っている。
② 経営執行部の方針により、学内ルールの策定を行っているが、周知徹底はできていない。
③ 経営執行部ではなく情報センター等部門により、学内ルールを策定し、その周知徹底を行っている。
④ 経営執行部ではなく情報センター等部門により、学内ルールを策定しているが、周知徹底はできていない。
⑤ 学内ルールの策定とその周知徹底を検討している。
⑥ 学内ルールの策定はしていない。

選択肢	選択数	割合	前年増減
①	30	25%	4%
②	24	20%	2%
③	23	19%	−8%
④	21	18%	2%
⑤	19	16%	−2%
⑥	2	2%	−1%





テーマ1：A大学様事例紹介(1/6)

本事例紹介の内容は、私情協情報セキュリティ研究講習会運営委員が2018年6月にA大学様にインタビューした内容に基づき作成したものです。

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制定。

- 背景
  - 10年以上前よりITセンターの内規としてのセキュリティポリシーは存在していたが、法人全体の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や、情報セキュリティ事故の発生などを踏まえ、法人全体としての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、大学間の合意にセキュリティポリシーが必要であった

テーマ1：A大学様事例紹介(2/6)

- ポリシー案作成の流れ
  - ITセンター所員会議およびITセンター委員会にて、国・公・私立他大学のポリシーを参考にしながら、当初OECDのセキュリティポリシーを参考としてポリシー案の作成に着手したが、本学や大学組織にそぐわない箇所が多かった
  - そのため、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)を参考に作り直しを行った
  - 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

テーマ1：A大学様事例紹介(3/6)

- 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絡みや人員体制を踏まえ、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，現状に合わない事項をそこから削除していくだけで，基本的には項目を追加する必要はない

テーマ1：A大学様事例紹介(4/6)

- 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)も含む内容のため、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IT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
  - ITセンター所長（CISO）より学長へ相談し、学長から理事長へ「何処に掛け合えばよいか」諮問いただいた。
  - たまたま同時期に法人で審議されていた文書管理規定のプロジェクトで，電子媒体の情報という観点から諮問があった。

テーマ1：A大学様事例紹介(5/6)

規程制定へ向けた学内調整(続き)

- 学長コーナー(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。ITセンター次長が事あるごとに状況を確認
- 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、学内で発生した情報セキュリティ事故が最後の後押しとなり、総務部が起案元となり規程として制定された
- 制定されたセキュリティポリシーは冊子化して学内へ配布した

テーマ1：A大学様事例紹介(6/6)

ポリシー制定時に考慮した点

- 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
- 通常、セキュリティポリシーには懲罰規程も含むが、これは大学教員に受入れられるとは思えない。そこで、「情報」かどうかにかかわらず、「大学に与える影響」で就業規則に基づき処罰が決まることとし、セキュリティポリシーからは除外した。
- ポリシーは緩い内容であっても存在することが重要。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する
- NIIサンプル規程集のように「基本方針」と「対策基準」の2つを策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。

テーマ1：B大学様事例紹介(1/5)

本事例紹介の内容は、私情協事務局が17年度ベンチマークテストの回答内容から、先進的な対応を実施されている大学に、具体的な取り組み内容をメール調査した内容に基づき作成したものです。

経緯

- 事務支援システム（業務システム）を全面再構築したことで、事務業務システム運用管理の体制が変わり、実際の運用管理と情報システム関連規程に乖離が目立つようになったことから、2015年に情報関連規程の改正に着手した。
- 同年6月の常務理事会（法人意思決定機関）にて、情報関連規程の改正について審議依頼をし、承認を受けた。改正した情報関連規程では、理事長の下に、本学情報環境整備運用管理を統括する「情報統括責任者」を配置し、理事長が常務理事の中から指名すると規定した。さらに、情報統括責任者の下に、本学情報環境整備運用管理推進体制の構築を規定した。この体制が、情報セキュリティ強化に繋がることとなる。
- 2015年に整備した情報関連規程の中では、情報セキュリティ確保について、情報セキュリティポリシーに従うことを規定したことから、情報セキュリティ体制確立の検討を開始した。

テーマ1：B大学様事例紹介(2/5)

情報セキュリティポリシーの策定

- 2015年9月、本学の情報セキュリティに詳しい教員に、情報セキュリティポリシーの策定に関する私案を相談。助言を受け、法人トップの情報セキュリティに対する理解を得る重要性を確認。その取組みに着手。はじめに、情報統括責任者（情報担当役員）に対し、本学常務理事に対する「情報セキュリティ勉強会」の開催を提案。その後、セキュリティに詳しい教員と勉強会の内容を検討、作成し開催に向け準備を進めた。
- 2016年1月、相談をした教員を講師に、理事長、常務理事を含む運営幹部に対するセキュリティ勉強会を開催。「情報セキュリティの現状と対策」と題し、情報セキュリティの一般的な話しと、サイバー攻撃の現状、ならびに本学の対策状況と課題について講義を行った。その中で、情報セキュリティ対応体制の構築と関連規程の整備を宣言し、役員の理解を得た。

テーマ1：B大学様事例紹介(3/5)

情報セキュリティポリシーの策定(続き)

- 2016年10月27日、大学NUA集合研修（セキュリティ対策）NEC主催に参加。情報セキュリティ体制構築のプロセスや役割分担等を学ぶ。この講習はCSIRTや情報セキュリティ体制検討に大変参考となった。
- 同じ時期に、文部科学省より、「文部科学省関係機関における情報セキュリティ対策の強化について（通知）」28文科政策第63号（平成28年10月12日）の通知を受け、まとめてきた「情報セキュリティ体制の原案」を情報統括責任者と検討、整理し、作成。
- 先に助言を頂いた教員にも確認いただき、2017年2月の常務理事会に「情報セキュリティポリシーの制定」、「情報セキュリティ対策本部と組織内CSIRTの設置」、「情報セキュリティ管理規程の制定」の3つを提案、審議を経て、全ての提案が承認され、2017年3月1日より施行となった。これにより本学情報セキュリティ体制の整備が完了したことになる。

テーマ1：B大学様事例紹介(4/5)

セキュリティポリシー策定後の活動状況

- 2017年3月15日第1回情報セキュリティ対策本部会議を開催、その後、年2回（9月、3月）本部会議を召集、開催している。インシデント発生の際には、臨時の対策本部会議を開催（開催実績あり）。
- 本学情報セキュリティの確保については、理事長の下に情報セキュリティ対策本部を置き、対策本部長に「情報統括責任者（情報担当役員）」を充て、情報セキュリティ啓蒙活動やインシデント対応方針などを情報セキュリティ対策本部で協議し、組織内CSIRTを兼務する情報システム部が実行部隊として対応にあたっている。
- また、9月開催の情報セキュリティ対策本部会議で次年度の情報セキュリティ確保に関する取り組み（計画）を情報システム部より提案、協議を経て、予算要求。その後、予算通知を受け、3月の本部会議で、次年度（4月）からの事業計画を報告し、事業実施という流れで、取組みを続けている。

テーマ1：B大学様事例紹介(5/5)

- セキュリティポリシー策定後の活動状況
  - 日々の活動としては、情報セキュリティに関する情報（関係省庁からの通達、IPAなど）に注意を払い、必要に応じて、学内情報共有のための全教職員に対しては学内情報共有グループウェアで、学生には本学ホームページ上で注意喚起等を実施している。
  - 情報セキュリティ対策本部は、統括、教学担当、事務担当、広報担当、附属校担当、情報担当の長で構成。少数にしている理由は、即時性、実働性重視の観点から。また、緊急時の対応は、さらにメンバーを統括者、事務担当、広報担当、情報担当に限定し、対応を協議、その結果により関係者への周知と理解を得て対応にあたることとしている。
  - 運営について、日常は、本部長とCSIRT（情報システム課）により情報セキュリティ確保にあたる。コラボレーションツールを活用し、本部員間の情報共有をする。本部会議として、定例会議は、原則年1回の開催（規定済み）。必要に応じて臨時会議を設ける。また、インシデント発生時には、緊急会議を招集する。

テーマ1：事例紹介(まとめ)

- トップダウンでセキュリティポリシーを策定することが理想であるが、現実には難しいため、CISOと情報部門が主体となり行動し、早い段階で経営層にセキュリティポリシーの必要性を理解してもらうことが重要
- ポリシーや規程は理想論ではなく大学ごとの実情に合わせた現実的な内容とする。理想論で作成すると、情報システム部門が管理を厳しくしたがっているという誤解を招き反対にあう場合や、仮に策定しても守られない意味のないポリシーとなってしまう
- ポリシーを策定して終わりではなく、その後の運用までポリシー策定時に考慮しておく必要がある
- 外部機関からの通知や、学内でのインシデントなどを後押しとすることも時に必要

テーマ1:グループワーク

(1) ペアワーク　5分×2回

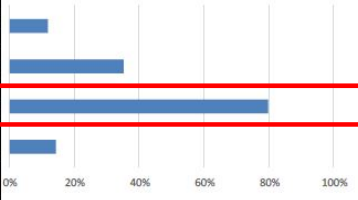
(2) グループ内シェア　10分（まとめを模造紙に記入を含む）

テーマ2:情報セキュリティルールの周知徹底

問５　経営執行部または部門単位で実施している危機意識の共有化、学内ルールの周知徹底・遵守の確認、攻撃に対する防御対策の内容について選択してください。（複数回答可）

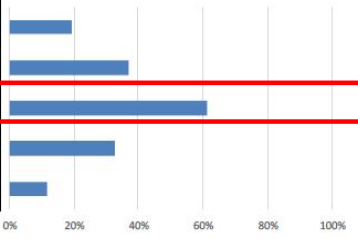
（１）危機意識の共有化

危機意識共有化の方法	選択数	割合	前年増減
① 学内外の情報セキュリティ研修会参加の義務化	14	12%	-6%
② FD・SD, 教授会, 職員会議などでの定期的な情報提供	42	35%	1%
③ Webサイトや学内文書による定期的な情報提供	95	80%	8%
④ その他（不定期な情報提供, 重大事象発生時に実施, 外部講師を招いた講習会開催, 情報セキュリティ委員会から各学部・各部署へ周知, 職員は入局時に実施し教員は実施していない, 教育計画中など）	17	14%	-3%



（２）学内ルールの周知徹底と遵守の確認

学内ルール周知徹底・遵守の方法	選択数	割合	前年増減
① 情報センター等部門によるルールの周知とアンケートでの点検・確認	23	19%	-2%
② 教授会、職員会議などでのルールの周知と遵守の確認	44	37%	-1%
③ Webサイトでのルールの紹介と遵守の呼びかけ	73	61%	3%
④ 説明会でのルールの紹介と遵守の呼びかけ	39	33%	-1%
⑤ その他（メール, 通達, 利用案内, 新入職員研修で周知, 教育計画中など）	14	12%	-3%



テーマ2：C大学様事例紹介

本事例紹介の内容は、私情協事務局が17年度ベンチマークテストの回答内容から、先進的な対応を実施されている大学に、具体的な取り組み内容をメール調査した内容に基づき作成したものです。

- 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）
- 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
- 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2016年9月に作成し、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

テーマ2：D大学様事例紹介

本事例紹介の内容は、私情協事務局が17年度ベンチマークテストの回答内容から、先進的な対応を実施されている大学に、具体的な取り組み内容をメール調査した内容に基づき作成したものです。

- 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。

テーマ2：E大学様事例紹介

本事例紹介の内容は、私情協事務局が17年度ベンチマークテストの回答内容から、先進的な対応を実施されている大学に、具体的な取り組み内容をメール調査した内容に基づき作成したものです。

- 各学科、事務部門から構成されるセキュリティ対策委員会により、定期的にセキュリティインシデントに対しての啓蒙活動を行っている。具体的には、昨今、急激に増加している標的型メールや実在する企業を騙ったフィッシングメール等の事例及び対策をまとめ全教職員に対して配信し、メールに対しての危機意識を高めている。
- また、ウイルス対策ソフトのインストールはもとより、更新状況等の調査・報告を義務化することにより、更新期限切れ等によるウイルス感染被害を防ぐようにしている。
- 個人情報保護に関する各種規程やセキュリティガイドラインにより新入教職員の入職前オリエンテーションにおいてセキュリティ対策委員会による周知を図っている。また、学生に関しても入学時に個人情報保護についての講習を開催し、注意喚起を行っている。

テーマ2：F大学様事例紹介

本事例紹介の内容は、私情協事務局が17年度ベンチマークテストの回答内容から、先進的な対応を実施されている大学に、具体的な取り組み内容をメール調査した内容に基づき作成したものです。

- JPCERT、IPA、文部科学省や県警等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。
- 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、現在、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。

テーマ2：G大学様事例紹介

本事例紹介の内容は、私情協事務局が17年度ベンチマークテストの回答内容から、先進的な対応を実施されている大学に、具体的な取り組み内容をメール調査した内容に基づき作成したものです。

- 危機意識の共有化については、経営部門については委員長である副学長から、部局長会（月1回）で報告するとともに、教員については、ネットワークセキュリティ委員会（定時：7月、臨時：随時）の委員による教授会での報告、職員については、事務部長会及び所属長会（ともに月1回）の報告、学生については、ポータルサイトによる告知を随時行っている為、日に1回以上のポータルサイトの確認義務を課している。
- また、本学のコンピュータ環境の使い方というWebページの、「知っておきたいICTセキュリティ」という項目に、ネットワークセキュリティポリシーを記載しており、危機意識の共有化を図っている。
- 学内ルールの周知徹底と遵守の確認については、ネットワークセキュリティ対策確認調査の実施（年1回1月）、コンピュータ環境の使い方の更新、作成、新規採用事務職員を対象としたパソコン研修会（年1回4月）の開催、また、新人等問わず教職員に対してeラーニング教材の「情報倫理」の受講を強く勧める等して、学内ルールの説明や呼びかけを行っている

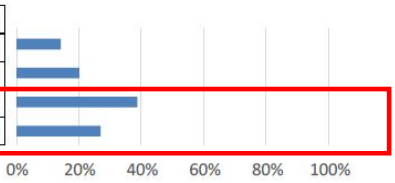
テーマ2：事例紹介(まとめ)

- 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大学が増えている
- 規程とは別に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ケースが多くみられる
- 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メール等で周知
- 一般教職員や学生への周知の他に、経営増への定期的な状況報告を行うことも重要

テーマ3：情報資産の把握とリスク対策

問1　重要な情報資産（金融資産情報を含む）の目録作成を実施。
① 実施しており、毎年見直しを行っている。
② 実施しているが、定期的な見直しは行っていない。
③ 検討している。
④ 実施していない。

選択肢	選択数	割合	前年増減
①	17	14%	−7%
②	24	20%	−2%
③	46	39%	9%
④	32	27%	0%



問2　重要な情報資産に対するアクセス制御及びリスク評価を行っていますか。
① 重要な情報資産に対するアクセス制御及びリスク評価を行っている。
② 重要な情報資産に対するアクセス制御を行っている。
③ 重要な情報資産に対するリスク評価を行っている。
④ 検討している。
⑤ 実施していない。

選択肢	選択数	割合	前年増減
①	10	8%	−5%
②	77	65%	5%
③	3	3%	1%
④	18	15%	0%
⑤	11	9%	−1%

公共社団法人 私立大学情報教育協会

テーマ3：H大学様事例紹介(1/5)

本事例紹介の内容は、私情協情報セキュリティ研究講習会運営委員が2018年8月にH大学様にインタビューした内容に基づき作成したものです。

情報資産の「機密レベル」、「保管場所」を定義し情報資産台帳で管理。定期的に管理検査を実施している。

※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)

- 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

    ※「管理窓口」は総務部門と情報システム部門の職員でチーム構成
  - 【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。

公共社団法人 私立大学情報教育協会

テーマ3：H大学様事例紹介(2/5)

■ 情報資産の保管場所の定義

- 大学共通オンプレファイルサーバ
- 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

■ 情報資産台帳の起票

- 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。

テーマ3：H大学様事例紹介(3/5)

■ 情報資産台帳例

□ 高リスクデータ

資産名（大分類）	資産名（中分類）	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	フォルダ	承認日	承認者

管理窓口届出日	管理窓口承認日

□ 制限データ（例外保管）

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	保管媒体	保管方法	承認日	承認者

管理窓口届出日	管理窓口承認日

□ 制限データ（オンラインストレージ保管）

資産名（大分類）	資産名（中分類）	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	フォルダ	承認日	承認者

□ 制限データ（持出）

資産名	持出日	持出終了予定日	持出終了日（削除日）	持出者	持出方法	持出目的	持出先	承認日	承認者

管理窓口届出日	管理窓口承認日

テーマ3：H大学様事例紹介(4/5)

管理検査の実施

- 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

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

テーマ3：H大学様事例紹介(5/5)

検査チームの管理検査内容(続き)

- 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
- 浮き彫りになった点で全学的に共通化できる点について、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、あまり厳格に行わず、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

本事例紹介の内容は、私情協事務局が17年度ベンチマークテストの回答内容から、先進的な対応を実施されている大学に、具体的な取り組み内容をメール調査した内容に基づき作成したものです。

テーマ3：I大学様事例紹介(1/3)

■ 組織体制

- 理事会のもと、情報資産セキュリティ委員会を設置。総務担当常任理事を委員長（情報資産統括責任者）に法人配下、大学、中学校、高等学校、幼稚園の部局責任者（部長級、学校長級役職者）を構成し、情報セキュリティに対する外部からの侵略、および情報資産の漏洩等への対応や情報セキュリティに関する啓蒙活動、情報セキュリティポリシー、関連規定等の検討精査等を所掌している。
- 所掌する具体的な対応作業等は、2014(平成27)年度から実施し、毎年度、法人配下の全事務組織から選出された「情報資産セキュリティ委員会作業部会リスク分析・評価WG」（WG：ワーキンググループの略）を編成し、更に情報資産洗出WG、関連規定等策定WGの2つのWGを組織し、情報資産台帳の整備・更新、リスク分析・評価に加え、ポリシー・関連規程・ガイドライン等の見直し、啓蒙等の素案・計画等の作業を実施し、現在は全学事務組織を対象に危機意識の共有化に努めている。

本事例紹介の内容は、私情協事務局が17年度ベンチマークテストの回答内容から、先進的な対応を実施されている大学に、具体的な取り組み内容をメール調査した内容に基づき作成したものです。

テーマ3：I大学様事例紹介(2/3)

■ 情報資産の管理

- 重要な情報資産に対するアクセス制御及びリスク評価は、部局毎に部局責任者（部局責任者・部長級）、同副責任者（副部局責任者・課長級）のもと、部局毎に情報資産台帳を整備し、リスク分析・評価作業を経て、改善計画等を作成することが定めされているが、実際には作業部会の選出されたメンバーがそれぞれの課内で中心となり、情報資産台帳の整備・更新、リスク分析・評価を実施しているのが現状。
- 具体的な情報資産台帳の作成・更新、リスク分析・評価、改善計画の手順については、総務省公開 「電子自治体の推進に関する懇談会（セキュリティワーキンググループ）検討結果の公表」（平成21年3月27日）（http://www.soumu.go.jp/menu_news/s-news/02gyosei07_000006.html）にて公開された資料・手引き・書式を流用し、事務局の庶務課担当者が手引き・書式を作成し、これを実状に合わせて改善利用している。

テーマ3：I大学様事例紹介(3/3)

本事例紹介の内容は、私情協事務局が17年度ベンチマークテストの回答内容から、先進的な対応を実施されている大学に、具体的な取り組み内容をメール調査した内容に基づき作成したものです。

実際の取り組み状況

- 平成27年度より実施し、重要情報＝個人情報に係る情報資産を洗出、平成28年度にはリスク分析・評価までを実施、2016(平成29）年度には改善計画を作成するなど、 年度毎に情報資産台帳の更新、リスク分析・評価、改善計画の着手までを実施している。
- 責任者・取扱者、取扱手順、処理の履歴・点検は、情報システム運用・管理規程の「第6章情報の取扱い」にて定められているが、具体的な関連規程・ガイドラインの整備が遅れており、定期的な確認までは行っておらず平成30年度検討課題の一つとしている。

テーマ3：事例紹介(まとめ)

- 情報資産の把握を具体的に推進するチームやWGを構成することが効果的。全学的に統一された観点や手順を示し対応する必要がある。
- 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る
- 情報資産の具体的な洗い出し作業については、学内の各部課(現場)で行うしかない。学内全体を巻き込んでの作業となるため、経営層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。

テーマ2/3：グループワーク

※テーマ2とテーマ3をまとめて実施

(1) ペアワーク　5分×２回

(2) グループ内シェア　10分（まとめを模造紙に記入を含む）

グループワークの成果発表

- 各グループ3分以内