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（2015年版）改訂のポイント

東北大学大学院法学研究科
高等教育機関における情報セキュリティポリシー推進部会
金谷吉成 <kanaya@law.tohoku.ac.jp>

目次

1. 大学における情報セキュリティ対策
2. サンプル規程集 ―ポリシー・実施規程の雛形―
3. サンプル規程集の使い方
4. サンプル規程集（2015年版）改訂のポイント
   - A）改訂の概要
   - B）CSIRTの設置
   - C）クラウドサービスの利用
   - D）情報セキュリティ教育への取組み

1．大学における情報セキュリティ対策

大学の活動と情報セキュリティ

- 構成員
  - 役員、職員（事務、技術、準職員）、教員、派遣職員、受託業者
  - 学生（学部、大学院、研究生） ←構成員なのか、顧客なのか
  - TA・RA ←学生なのか、職員なのか
  - 研究員（学内、他大学、企業、外国……） ←権利と責任？
    - 多様な主体
- 大学で取扱う情報（3つの柱）
  - 教育：教務情報（履修、成績）、教材・講義資料、eラーニング
  - 研究：研究情報（原稿、データ、技術・設備）、発表論文、特許
  - 運営：経営情報（財務、人事、労務など）、広報
  - （医療）：医療情報（患者の個人情報など）
    - 多様な客体

情報セキュリティを考える上で、
民間企業や行政機関とは違った難しさがある

大学での情報セキュリティ対策

- 情報セキュリティへの要請
  - 情報システムの全体のセキュリティ（機密性・完全性・可用性）の維持・向上
  - 機密情報（入試・試験、未発表論文・特許技術、経営情報）
  - 社会や関係先に対する責任
  - 個人情報保護、安全保障貿易管理（、医事）からの要請との関連
  - （コンピュータソフトウェアの適正な管理）
  - 研究組織・研究者について、学問の自由との両立
  - 教育機関として、学生に対する情報セキュリティ教育

↓

- 大学の取組み
  - 情報セキュリティポリシーの策定
  - インシデント対応
    - 不正アクセス対策、情報漏えい対策、予防、利用者教育、自己点検
  - 政府機関統一基準への準拠
  - 情報セキュリティ対策に取組む体制の構築

具体的な取組み

- 情報セキュリティポリシーの策定
  - ポリシー、実施規程、啓発用テキストを各大学が独自に作成することは大変な労力を要する　→サンプル規程集
- インシデント対応
  - ネットワーク障害への対応や脆弱性攻撃、ウイルス感染への対応は民間企業や行政機関と同様
  - しかし、予算・人材・設備等の資源不足に悩む大学も多い
  - また、教育不足・管理の甘さなどに起因した、著作権侵害やソフトウェアライセンス違反等のインシデントが発生することもある
- 政府機関統一基準への準拠
  - 大学は「政府機関の情報セキュリティ対策のための統一基準」の適用対象ではないが、情報セキュリティ水準引き上げの要求に応えるため、事務情報システム等は準拠することが適当
- 組織・体制
  - CIO、CISO及び情報部門の再編
  - 各部局を含めた情報セキュリティ体制
  - ポリシー、実施規程の策定
  - 情報セキュリティ教育の実施

2. サンプル規程集

ポリシー、実施規程の雛形

サンプル規程集

- 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
  - 雛型となるセキュリティ関連の学内規程とその解説
  - 標準的かつ活用可能な大学向けのサンプル規程集
  - 各大学（および各種機関）でカスタマイズ
  - 政府機関統一基準とその考え方に準拠
    - 特に事務情報システム
  - 他の制度や規格との関係についても考慮
    - ISOやプライバシーマーク制度などの情報セキュリティの基準を含め、大学における情報セキュリティ対策のあり方を検討
  - 専門家集団による策定
    - 大学の研究者、民間企業の実務者、弁護士等
  - 2007年2月初版公開、2015年版は32編879頁
    - http://www.nii.ac.jp/csi/sp/　公開中
  - 引き続き改訂・推進の活動を継続中

推進部会

- 高等教育機関における情報セキュリティポリシー推進部会
  - 大学等への情報セキュリティポリシーの普及促進活動
    - PDCAサイクルを回して初めて有意義に
    - サンプル規程集の利活用の促進のためのコンテンツ作り
      - 教材開発
      - サンプル規程集の使い方に関する情報を提供
      - 各大学等における議論を支援（直接に策定の支援ではない）
      - 講演等の依頼があった場合に、その対応の調整
  - サンプル規程集に対する質問・要望への一次対応
  - サンプル規程集改訂に向けた準備作業
    - 状況の変化や要望等について整理
      - 政府機関統一基準の改訂、技術の進歩、サービスの変遷など
  - 次回の見直し活動に向けた情報収集
  - 2007年12月より設置

大学のポリシー策定に関する背景

- 背景
  - 大学における情報セキュリティレベルの向上は急務
  - ポリシー、実施規程、教育テキストの作成が必要
  - 大学における教育・研究との関係および組織・運営の考慮、など広範な専門知識が求められる
  - 政府機関統一基準との関係、法制度との関係（個人情報保護法、プロバイダ責任制限法等）、国立大学の法人化、セキュリティの高度化・専門化
- 要請
  - 雛型となる規程集（ポリシー、実施規程、教育テキスト）を策定すべき必要性
    - 専門家集団 ⇒ セキュリティの高度化・専門化に対応した作業（全国共同利用情報基盤センター群、電子情報通信学会）

大学におけるポリシー策定の動き

電子情報通信学会

ネットワーク運用ガイドライン
検討ワーキンググループ（一期）

2001.2～2003.4
「高等教育機関における
ネットワーク運用ガイドライン」
（ネットワークの健全な運用・利用の考え方、指針）

大学の情報セキュリティポリシーに関する研究会

2001.7～2002.5
「大学における情報セキュリティポリシーの考え方」
（情報セキュリティの基本方針、対策基準）

情報セキュリティセンター（NISC）
※内閣サイバーセキュリティセンター

2005.12　政府機関統一基準・個別マニュアル群

ネットワーク運用ガイドライン
検討ワーキンググループ（二期）

2006.8～2007.2
サンプル規程集とその解説の作成

合同

国立情報学研究所

国立大学法人等における
情報セキュリティポリシー
策定作業部会

2006.8～2007.2
・政府機関統一基準を踏まえた見直し
・標準的かつ活用可能なサンプル規程集の策定

2007.12～　高等教育機関における
情報セキュリティポリシー推進部会

推進部会の活動体制

- 検討内容と活動体制
  - 意見・質問に対応しつつ、規程やマニュアルの雛形を作成
  - サンプル規程集を提供・公開
    - 2007年2月に初版、その後2010年／2013年／2015年に改訂
  - 成果の普及のため、セミナー・ワークショップ等における説明の実施

（総論・体制）	情報セキュリティポリシーの考え方や規程体系の見直し
運用（運用総論、システム運用、情報管理）	情報格付け、外部委託・人事異動、例外措置 運用・管理、ウェブサーバ・メールサーバ リスク評価・リスク管理、非常時行動計画
利用（利用、自己点検）	ウェブブラウザ、ウェブ公開、自己点検
教育（利用者、管理者、役職者）	教育テキスト
事務（事務）	各種マニュアル類、責任者等の役割
認証（認証運用）	認証手順

サンプル規程集（2015年版）の構成

ポリシー	実施規程	手順等
C1000 情報システム運用基本方針 C1001 情報システム運用基本規程 C1101 情報セキュリティインシデント対応チーム（CSIRT）設置規程	C2101 情報システム運用・管理規程 C2102 情報システム非常時行動計画に関する規程 C2103 情報格付け規程	C3100 情報システム運用・管理手順の策定に関する解説書 C3101 例外措置手順書 C3102 インシデント対応手順 C3103 情報格付け取扱手順 C3104 情報システム運用リスク評価手順
	C2201 情報システム利用規程 C2202 全学認証基盤利用規程※	C3200 情報システム利用者向け文書の策定に関する解説書
		C3251 情報機器取扱ガイドライン C3252 電子メール利用ガイドライン C3253 ウェブブラウザ利用ガイドライン C3254 情報発信ガイドライン C3255 利用者パスワードガイドライン
	C2301 年度講習計画	C3300 教育テキストの策定に関する解説書 C3301 教育テキスト作成ガイドライン（利用者向け） C3302 教育テキスト作成ガイドライン（システム管理者向け） C3303 教育テキスト作成ガイドライン（CIO/役職者向け）
	C2401 情報セキュリティ監査規程	C3401 情報セキュリティ監査実施手順
	C2501 事務情報セキュリティ対策基準 C2502 事務情報セキュリティ対策基準策定のためのガイドライン	C3500 各種マニュアル類の策定に関する解説書 C3501 各種マニュアル類(**)
	C2601 全学認証基盤運用管理規程※ C2602 全学認証基盤接続規程※ C2603 全学認証基盤アカウント利用規程※	C3600 認証手順の策定に関する解説書 C3601 情報システムアカウント取得手順
	C2651 証明書ポリシー(*) C2652 認証実施規程(*)	

水色部分は、技術系の規程・手順書
(*) 外部文書の参照のみ,
(**) 各大学にて策定することを想定

※C2202, C2601, C2602, C2603は
2015年10月時点で内容調整中につき、公開対象外

サンプル規程集（2015年版）の分量

（計32編，879p）	ポリシー C10xx (24p)	実施規程 C2xxx (612p)	手順・ガイドライン等 C3xxx (216p)
総論 x0xx	2編，20p		
運用 x1xx	1編，4p	3編，212p	5編，64p
利用 x2xx		1編，12p	6編，54p
教育 x3xx		1編，8p	4編，56p
監査 x4xx		1編，6p	1編，26p
事務 x5xx		2編，366p	1編，4p
認証 x6xx		2編，8p	2編，12p

この枠内で　9編，262p（2007年版と比べると186pの増加）

サンプル規程集の改訂

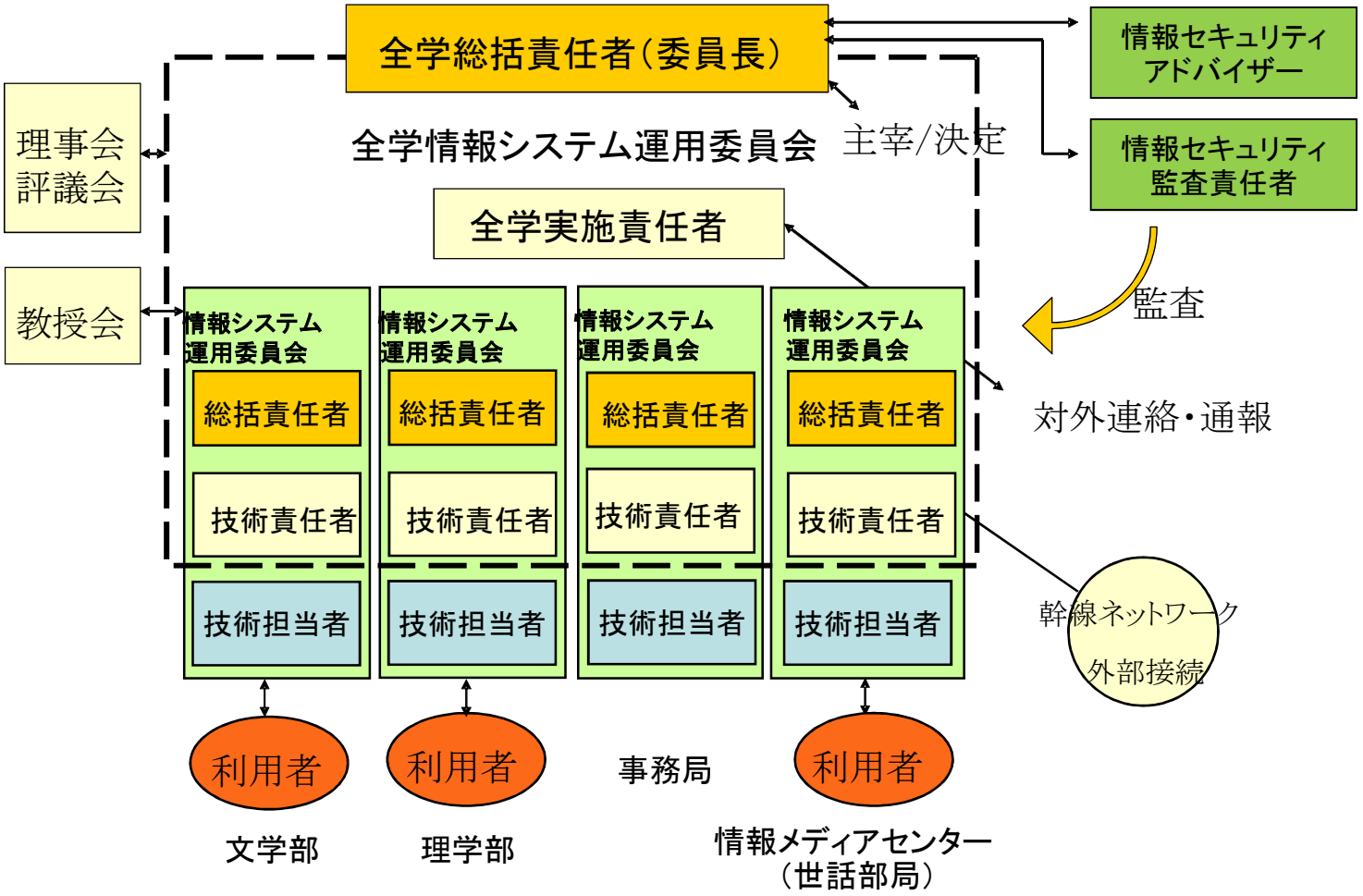
- 政府機関統一基準の改訂、技術の進歩、情報システムを取り巻く環境の変化等に応じて適宜改訂
- 2007年版（初版、18編308頁）
  - 政府機関統一基準（全体版初版）に部分的に準拠
  - 文書番号冒頭の記号をAとして策定（例：A1000、A1001）
- 2010年版の改訂（46編704頁）
  - 政府機関統一基準（第4版）に部分的に準拠
  - 3分冊化（①規程類　②手順・ガイドライン類　③用語集）
- 2013年版の改訂（13編421頁）
  - 政府機関統一基準（平成24年度版）に準拠
    - 平成23年度版より、「統一管理基準」と「統一技術基準」に分割され、大幅に構成変更
  - 文書番号冒頭の記号をAからBに変更（例：B1000、B1001）
- 2015年版の改訂（32編679頁）
  - 政府機関統一基準（平成26年度版）に準拠
    - 統一基準が再び一本化されるとともに、「府省庁対策基準策定のためのガイドライン」に相当する内容が分離されるなど、大幅に構成変更
  - 文書番号冒頭の記号をBからCに変更（例：C1000、C1001）

3. サンプル規程集の使い方

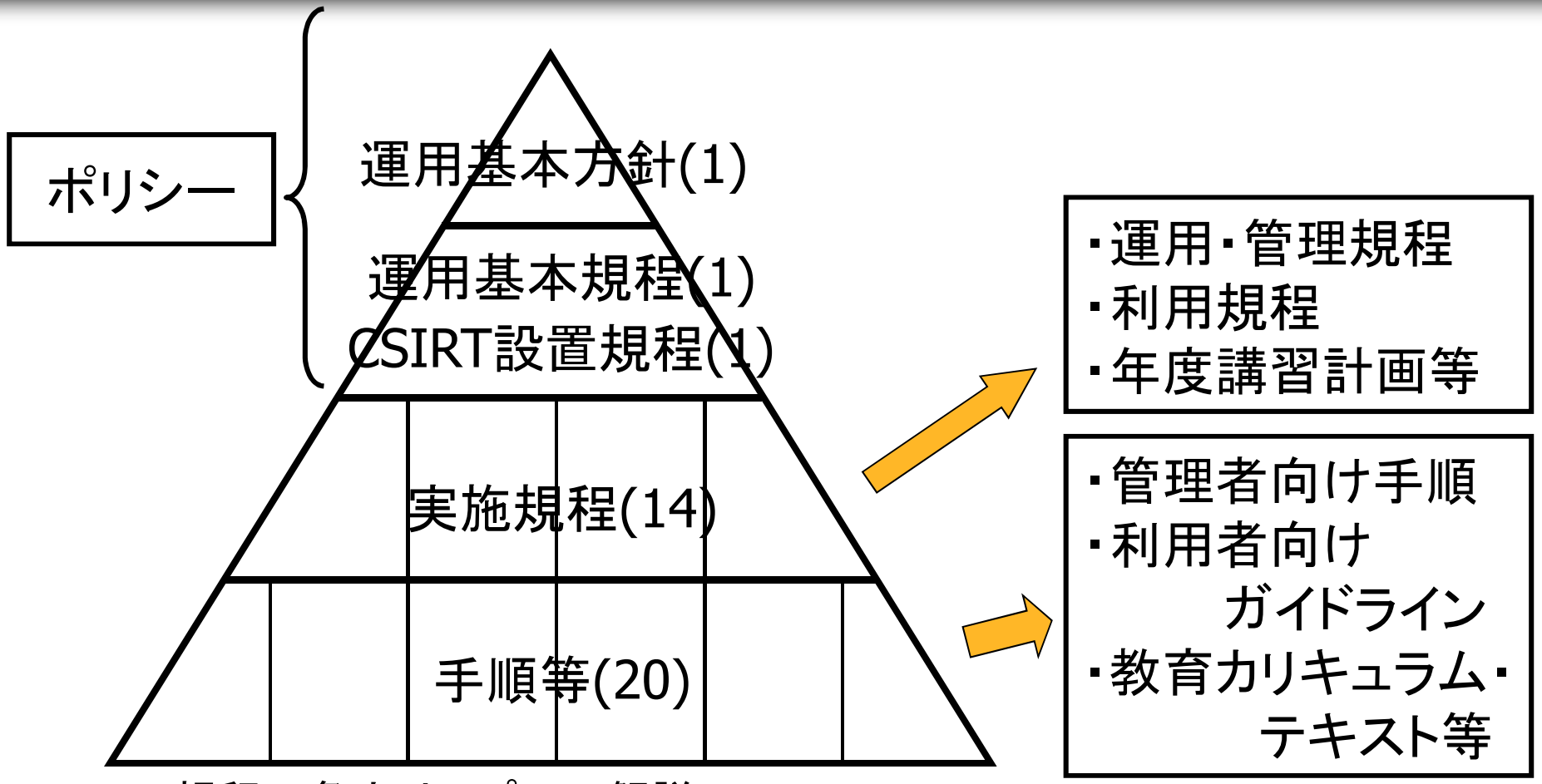
サンプル規程集における前提

- モデルとして仮想A大学を想定
  - 文学部と理学部の2学部で構成され、両学部とも在学生1,000人（1学年250名）ずつ
  - 学内共同利用施設として情報メディアセンター（図書館を含む）がある
  - 学内ネットワーク（事務系ネットワークを除く）や学内共同利用の情報システムは情報メディアセンターが担当
  - 副学長の一人が最高情報責任者（CIO）であり、最高情報セキュリティ責任者（CISO）の役も兼務
- 各機関の具体的な参考として策定
  - 大学の事情に合わせて可能な範囲で政府機関統一基準の考え方に準拠
  - サンプル規程集の対象は、「情報」、「情報システム」及び「これらを取り扱う者」とする。「情報」には、情報システムに関係がある限り、紙に記載された情報や情報システム外部の電磁的記録媒体に記録された情報を含むものとする。
    - 紙媒体文書の取扱い規程との整合（例：東北大学法人文書管理規程）

A大学の情報システム運用管理体制



ポリシー・実施規程・手順等の体系



- 規程の条文サンプル＋解説
  - 規定している内容が理解しにくい項目や、各大学で修正すべき項目、他の選択や議論の余地があるものについて、策定の参考のために解説

サンプル規程集の使い方①

- サンプル規程集は仮想のA大学について策定されたもの
- 従って、サンプル規程集を参考にしつつ、適切な置き換えや修正が必要
  - 学内委員会で必要な規程を選別＆修正して策定
    - （ほぼそのまま策定してようなケースも）
  - 各々の組織の運営方針や体制あるいは既存の規程との整合
    - 情報ネットワーク→情報システム→情報セキュリティ全体
    - 紙媒体文書の取扱い規程との整合
- サンプル規程集の将来の改訂への対応のため、対応付けを明確にしておく

サンプル規程集の使い方②

- A大学との差異
  - A大学は、部局の独立性を尊重しつつ、情報セキュリティ対策については全学総括責任者（CIOとCISOを兼務）を中心に全学的に取り組む体制をとる
  - A大学よりも規模の小さい大学や、逆に総合大学（附属病院を持つ）のように規模の大きな大学もあり、各大学の実情に合ったカスタマイズが必要
    - 大学によっては、歴史的な経緯などにより、部局の独立性が強かったり、情報システムが分散管理されていて統合・再編が難しい場合等がある
      - 例）東北大学は学部・大学院・附置研究所等を合わせて27部局、学生数は17,800人、教職員数6,400人

サンプル規程集の使い方③

- 段階的に策定
  - サンプル規程集は、初版18編308頁、2010年版46編704頁、2013年版13編421頁、2015年版32編679頁の分量があり、すべてを一括でカスタマイズして定めることは困難
  - 東北大学では

ポリシー
規程・細則

- 情報セキュリティポリシー（2009年3月）
- 情報システムの運用及び管理に関する規程（2009年3月）

} ポリシー

- 情報システムの運用及び管理に関する細則（2009年12月）
- 情報システムの利用に関する細則（2009年12月）
- 情報システムの非常時行動計画等に関する細則（2009年12月）
- 情報の格付け及び取扱制限に関する細則（2009年12月）

適宜改訂

手順
ガイドライン

利用者向け

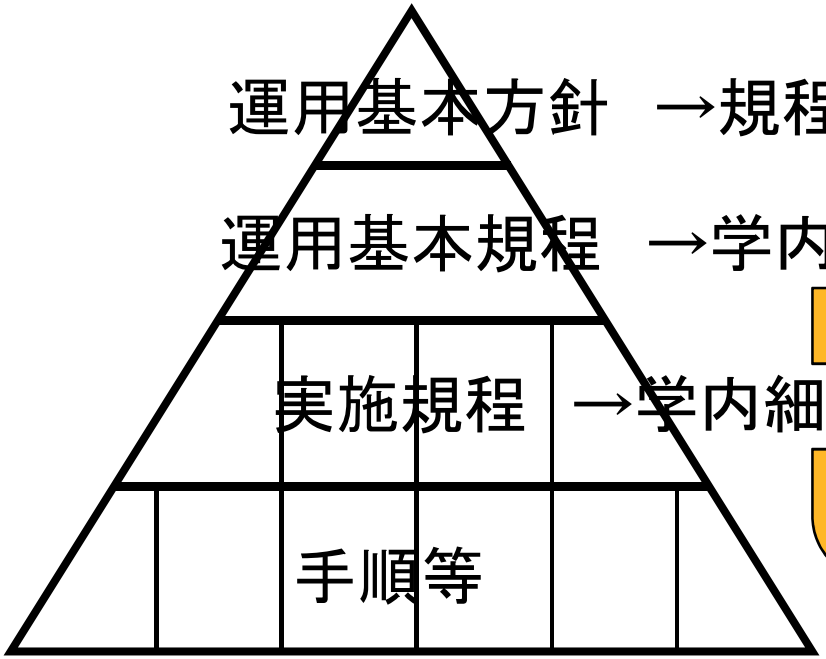
- アプリケーションソフトウェアの技術に関する細則（2014年3月）
- コンピュータネットワーク安全倫理に関するガイドライン（1999年、英語版あり）
- PC取扱ガイドライン（2013年2月）
- ウェブサービス利用ガイドライン（2013年2月）
- ウェブ公開ガイドライン（2014年10月）
- ソーシャルメディアの公式利用に関する情報セキュリティ対策ガイドライン（2014年10月）

管理者向け

- 情報システムにおける情報セキュリティ対策実施手順（2013年2月）
- 情報システムに関するインシデント対応手順（2013年2月）
- インシデント対応手順に基づくインシデント報告・承認要領（2013年2月）
- 機器等の購入における情報セキュリティ対策実施手順（2013年2月）
- 情報システムの調達における情報セキュリティ要件ガイドライン（2014年3月）

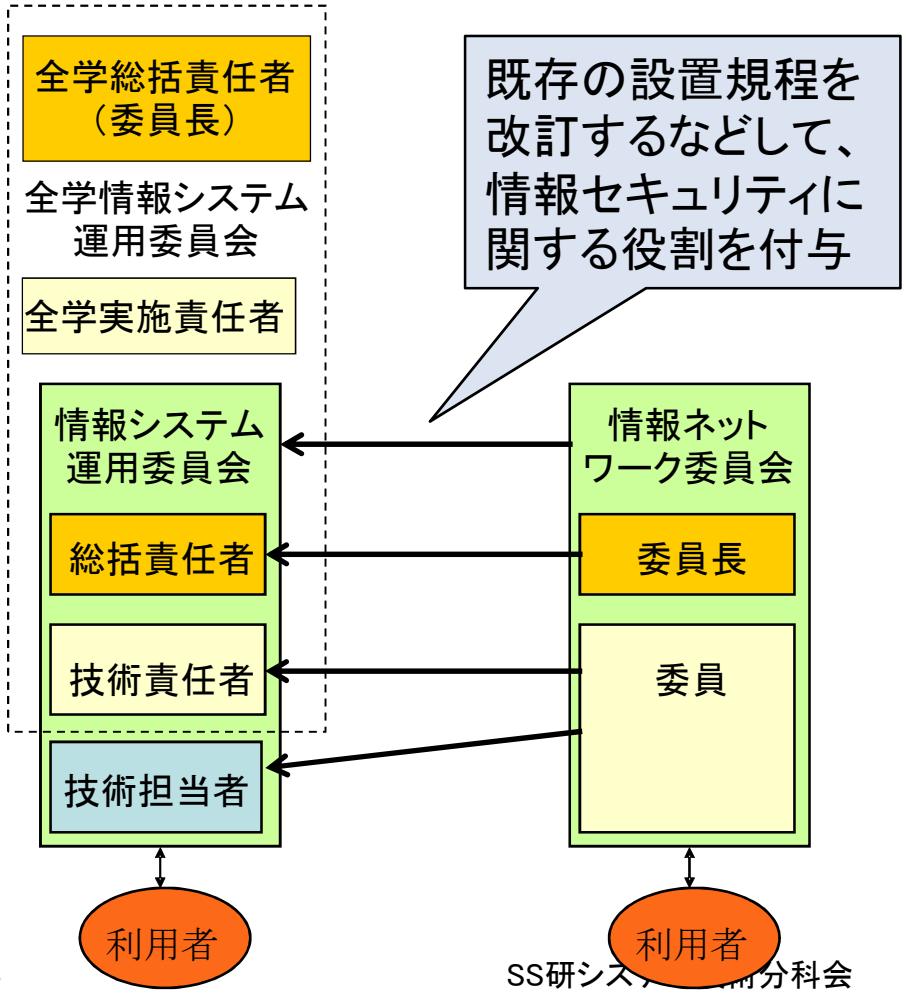
サンプル規程集の使い方④

- 学内規程体系にポリシーを位置付けしにくいケースもある
  - 規程～細則～内規のような体型への位置付けが難しい場合
    - 「基本方針」＝方針の骨子　→方向性の表明として規則体系の外
    - 「基本規程」＝組織体制を定める基準　→学内規程として策定
    - 基本規程の下の実施規程類も下方へスライド＝細則に位置付け



サンプル規程集の使い方⑤

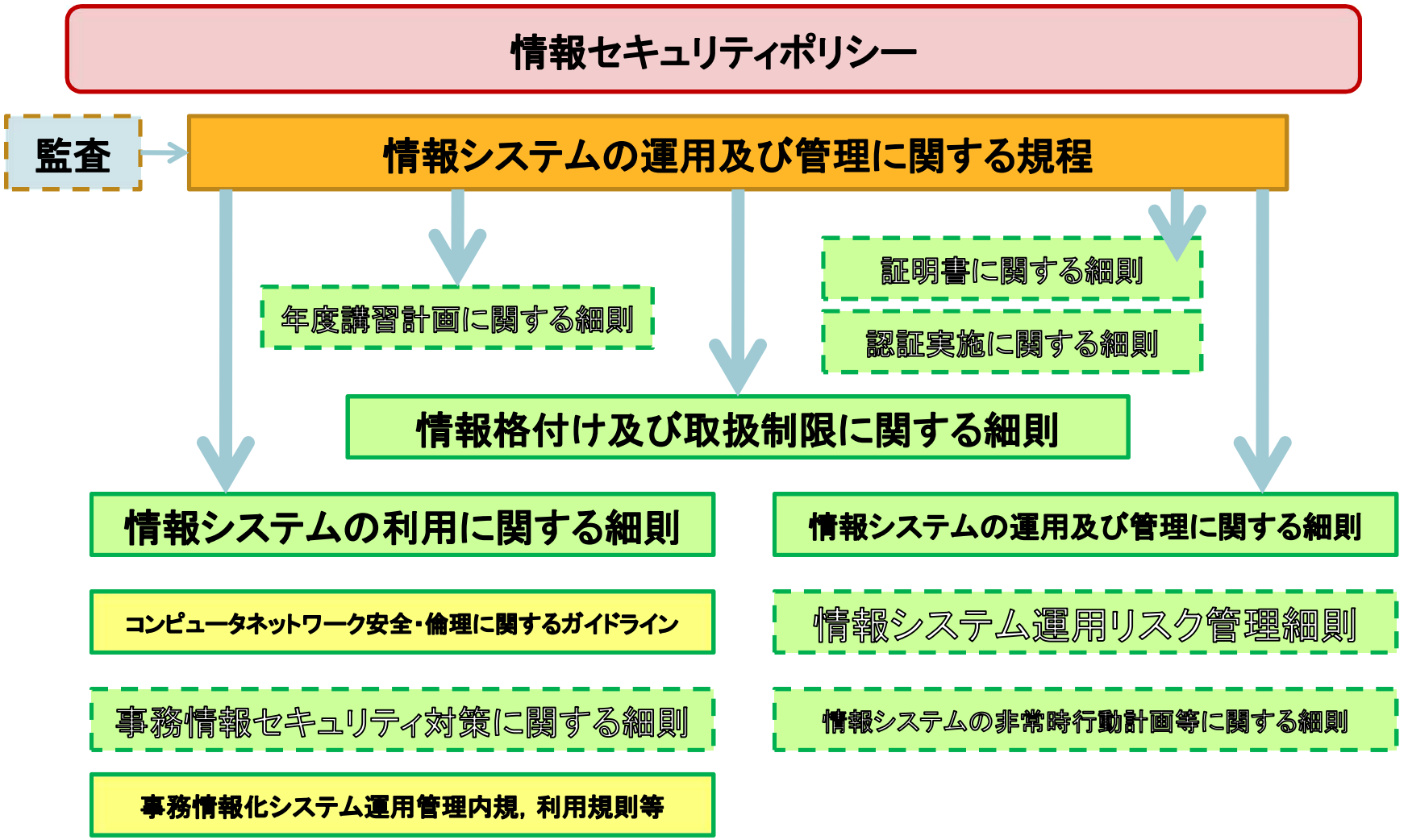
- 既存の運用管理組織や体制との関係
  - サンプル規程集の運用管理体制
    - 全学統括責任者
      全学実施責任者
      部局総括責任者
      部局技術責任者
      部局技術担当者
  - 既に情報ネットワークシステムの運用管理体制が整備済み



大学における策定の一例

- 検討範囲と方針
  - 取扱う範囲　→事務系情報についてはサンプル規程集のとおりとし、教員・研究者・学生等が取扱う情報は、情報を格付けした結果で取扱いを決定する。
  - 情報システムに計測器等を含むのか　→判断する基準を規程化し、より詳細な部分は各部局等で決定してもらう。
  - 文書管理規程　→格付けと取扱いのマッチングを図る。紙媒体については文書管理規程を遵守する。
- 運用基本方針、運用基本規程　→サンプル規程集に準拠した形で見直し
- 運用・管理規程　→現行規程との整合性を検討
- 利用規程　→現存する各システムの利用規程との整合

大学における策定の一例



4. サンプル規程集(2015年版)
改訂のポイント

A)改訂の概要

改訂内容

- 政府機関統一基準（平成26年度版）に準拠
  - 政府機関統一基準（平成24年度版）で「統一管理基準」と「統一技術基準」の2つに分割されていたものが一本化された
  - 他方、「府省庁対策基準策定のためのガイドライン」に相当する内容が分離されるなど、大幅に構成が変更された
  - 政府機関統一基準の構成が大きく変化していることに伴い、サンプル規程集の構成も変更された
- 大学における情報システムを取り巻く環境の変化等を踏まえ、内容を見直し
- 文書番号冒頭の記号をBからCに変更

改訂された文書①

文書番号・文書名	改訂内容
全体	文書番号冒頭の記号をBからCに変更。
C1001 情報システム運用基本規程	C2101の改定内容と整合をとるための用語定義等の見直し。
C1101 情報セキュリティインシデント対応チーム（CSIRT）設置規程	ニーズを踏まえて新規作成。
C2101 情報システム運用・管理規程	統一基準（平成26年度版）。 B2151～B2153に分離されていた内容を統合。
C2501 事務情報セキュリティ対策基準	統一基準（平成26年度版）をもとに全面改定。 解説に相当する内容をC2501に分離。
C2502 事務情報セキュリティ対策基準策定のためのガイドライン	統一基準（平成26年度版）に対応した「府省庁対策基準策定のためのガイドライン」をもとに新規作成。

改訂された文書②

文書番号・文書名	改訂内容
C3102 インシデント対応手順	刑法改正等への対応のための修正。
C3103 情報格付け取扱手順	情報システムの実態に合わなくなった箇所の修正。
C3104 情報システム運用リスク評価手順	情報システムの実態に合わなくなった箇所の修正。
C3251 情報機器取扱ガイドライン	情報システムの利用実態に合わなくなった箇所の修正。
C3252 電子メール利用ガイドライン	電子メールの利用実態に合わなくなった箇所の修正。
C3254 情報発信ガイドライン	ウェブ公開以外の情報発信を含めた形に修正。
C3255 利用者パスワードガイドライン	パスワードの最短文字数を修正（6文字→8文字）。
C3301 教育テキスト作成ガイドライン（一般利用者向け）	高等教育機関の実態に合わせた内容の見直し。
C3302 教育テキスト作成ガイドライン（システム管理者向け）	高等教育機関の実態に合わせた内容の見直し。
C3303 教育テキスト作成ガイドライン（CIO/役職者向け）	高等教育機関の実態に合わせた内容の見直し。

それぞれの大学での対応

- 特に大きく変わったのが
  - C2101 情報システム運用・管理規程
  - C2501 事務情報セキュリティ対策基準
    C2502 事務情報セキュリティ対策基準策定のためのガイドライン
- 構成は大きく変わったが、内容的に追加・変更になった部分はそれほど多くない
  - 改訂箇所を確認しながら、それぞれの大学のポリシー、実施規程、教育テキストに反映する

4. サンプル規程集（2015年版）改訂のポイント

B）CSIRTの設置

CSIRTに関する規定（C1001）

- サンプル規程集（2015年版）では、CSIRTについては、「体制を整備する」とあるのみ
  - C1001 運用基本規程
    - CSIRTの定義（情報セキュリティインシデント対応チーム）
    - 「全学総括責任者は、CSIRTを整備し、その役割を明確化する」
    - CSIRTの役割としては、以下のものを含む
      - 報告窓口からの情報セキュリティインシデント報告の受付
      - 情報セキュリティインシデントのCIO等幹部への報告
      - 対外的な連絡
      - 被害の拡大防止を図るための応急措置の指示又は勧告
    - CSIRT構成員は、情報セキュリティや情報システム等に関する専門的知識及び技能を持つ者とされる
      →実際に人材を確保することができるか？

CSIRTに関する規定（C1101）

- C1101 CSIRT設置規程
  - CIOは、CSIRTの活動が円滑に行えるよう、予算措置や適切な権限委譲を含めた環境を整備する
    - CSIRTに強制的な権限があるのか、ないのか？
      - ネットワークからの切り離し、システムの設定変更等
    - CSIRTによる事後対応（インシデント対応、脆弱性対応等）、事前対応（監視、監査、セキュリティツールの利用、情報集約等）、マネジメント（リスク分析、教育・啓発、訓練等）にはいずれもコストが発生
  - 組織＝委員長（CSIRT責任者）＋各部局の教職員から1名以上、必要と認められる者
    - CSIRT構成員の中から1名の連絡担当委員（PoC（Point of Contact））を指名
    - 既存の学内情報システム連絡会議や部局総括責任者、部局技術責任者のメーリングリストが使えないか？

CSIRTに関する規定（C2101）

- C2101 運用・管理規程
  - CSIRT構成員に対する教育
    - 学内でCSIRT構成員に対する教育を提供することは難しいのではないか？　→外部の専門事業者に委託することにより訓練を実施することも考える
  - インシデント認知時の報告・対処
    - 報告窓口はCSIRTが担うことが望ましい　→利用者への周知が必要
    - インシデント対応については、事前に策定された「C3102 インシデント対応手順」に従って対処する
    - CSIRTは、部局でのインシデント対応を支援（又は直接対応）するとともに、部局間の調整、学外との連絡調整を行う
    - インシデントの原因調査・再発防止についても、CSIRTが情報を集約し、他部局に水平展開することで、類似事案の発生を組織全体にわたって食い止めることが可能となる

具体的なCSIRTの構築

- 具体的なCSIRTの構築・運用マニュアルについては、JPCERT/CCや日本シーサート協議会の文書を参照しつつ、大学向けに利用可能かを推進部会で検討中
- CSIRTマテリアル（JPCERT/CC）
  https://www.jpcert.or.jp/csirt_material/
  - CSIRT構想フェーズ／構築フェーズ／運用フェーズの各段階毎に詳細な資料を提供
    - 企業向けの解説は、そのままでは大学に適用困難なものもある
      →大学向けのカスタマイズが必要か？　大学において、どこまで緻密にCIRSTの構築・活動ができるか？
    - 大学において参考になる資料も多い　→直接参照してもらう
    - 大学におけるCSIRTの事例紹介を盛り込むことができれば有用
- 日本シーサート協議会
  http://www.nca.gr.jp/
  - CSIRT人材の定義と確保
    http://www.nca.gr.jp/activity/training-hr.html

いくつかの疑問

- 情報システムの世話部局（情報メディアセンター）との関係は？
  - インシデント対応については、CSIRT責任者の判断で指示・勧告を行う
  - 情報メディアセンターは、CSIRT責任者の指示・勧告を支援する
    - CSIRTを情報メディアセンターの部内組織として位置付けるのが適当か？
- C2102 非常時行動計画に定める「非常時対策本部」との違いは？
  - 非常時行動計画は、BCP（事業継続計画）の中に位置付けられるもので、CSIRTとは役割が違う
    - CSIRTは事前に作られる組織
    - 非常時対策本部は事後に作られる組織

4. サンプル規程集(2015年版)
改訂のポイント

C)クラウドサービスの利用

学外への情報の提供

- 外部委託
  - 大学が保有する個人情報を委託先に預ける
  - 個人情報の取扱責任は大学（委託先の監督責任も）
  - 契約に基づく場合：外部委託における情報セキュリティ対策実施手順
    - 委託元としての責任者が遵守すべき手続き
  - 約款に基づく場合：約款による外部サービス
    - サービスを利用する上での要件が許容できるものであるか
- 第三者提供
  - 大学が保有する個人情報を大学以外の事業者が利用可能に
  - 個人の同意が前提

本学情報システムと約款による外部サービス

- （サンプル規程集が対象とする）
  本学情報システム
  - 本学が調達又は開発するもの（管理を外部委託しているシステムを含む）
    - 外部委託の場合、本学との契約あるいは他の協定に従って提供される
- 約款による外部サービス
  - 情報セキュリティ以外の契約内容については要求に基づいて用意される又は条件選択や修正ができる
  - 情報セキュリティに関する事項に条件選択の制限

外部委託における情報セキュリティ対策

- 必要な情報セキュリティ水準の確保（委託元としての責任者）
  - 可否の判断
    - 重要な情報を取り扱う情報処理業務は原則禁止
  - 調達：委託先の選定基準
    - 委託する情報処理業務に対する安定性
    - 求める情報セキュリティ対策等を遵守
      - その範囲を定め、対策を調達仕様として周知
      - 侵害時の対処、履行状況の確認
  - 契約
    - 実施させる情報セキュリティ対策の明示＋確認書
  - 実施中
    - 取り扱う情報の秘密保持等
    - 情報セキュリティ対策の履行状況の確認
  - 納品・検収

約款による外部サービスの利用

- 注意事項
  - 処理された結果生じる著作権等の権利の放棄や譲渡が利用条件となっている場合
  - 約款上データ消去等をサービス利用者側で直接実施できない場合
  - 利用したデータの削除についてサービス提供者が個別には応じないことや、情報の置き場所が特定の場所に固定されず、海外の法執行機関等による予期せぬアクセスが行われる場合
    - 準拠法に外国法が指定される場合
    - 管轄裁判所に海外の裁判所を指定される場合

無償で利用する外部サービスにも注意

- 無償で利用を開始できる場合であっても、外部委託に該当する場合があるので関連規則を遵守することが必要
  - 無償で提供されているメールサービスの利用
  - アンケート記入及び集計に係るウェブサービスの利用
  - オンラインストレージサービスの利用
- このようなサービスの利用者が調達に従事する教職員に限られたものではないため、当該留意事項について学内に広く周知する必要がある

4. サンプル規程集(2015年版)
改訂のポイント

D)情報セキュリティ教育への取組み

学生・構成員への啓発

- 新入生への教育
  - 入学時ガイダンスの中（履修登録システム操作の前）
  - 情報処理教育・演習の中（情報システム利用開始後）
- 職員への教育
  - 採用時
  - 周期的受講と評価？
- 学生・構成員向けの啓発資料・教材
  - 情報処理教育・演習のテキストの中
  - 情報セキュリティ・情報倫理教育のテキスト

情報セキュリティ・情報倫理の啓発教材の例

- 東北大学「コンピュータネットワーク安全・倫理に関するガイドライン」(1999年～)
  - 学生、教職員が利用時に守るべき注意事項(本文26ページ)
  - 第1部　利用心得編
    1. ネットワークを利用する前に
       - ネットワーク社会のルール
    2. 基本的な考え方
       - 言論の自由、学問の自由、他者の尊重
    3. ネットワークを気持ちよく利用するために
       - 情報発信／サービス利用の際の心構え、マナー
  - 第2部　利用手順編
    4. ネットワークを安全に利用するために
       - 情報セキュリティ
    5. ネットワークをスムーズに利用するために
       - 運用への協力、効率的利用
    6. ネットワークを正しく利用するために
       - 法令、規程、規則の遵守

情報セキュリティ教材

- 『ヒカリ＆つばさの情報セキュリティ3択教室』
  - 大学（高等教育機関）の学生を対象
  - Flash形式、全14話、2011年公開
  - 情報処理学会から表彰
- eラーニング教材
  - GakuNin®参加機関向けWebELSコンテンツ
  - 学生向け＋職員向け


表彰状

岡田 仁志 殿

あなたは 模範解答のできないセキュリティの問題において 学生自身に思考を促すなどの工夫を凝らし 授業外の自学自習を可能にした教材を開発し ネットワーク配信を行ってその普及と容易にした運用を行ってきました その教材は情報教育教材賞に値するものです よって ここに優秀教材賞選定規程により表彰し賞状ならびに賞金を贈呈いたします

2012年3月7日
一般社団法人 情報処理学会
会長 吉川 一夫

情報セキュリティ教材の開発

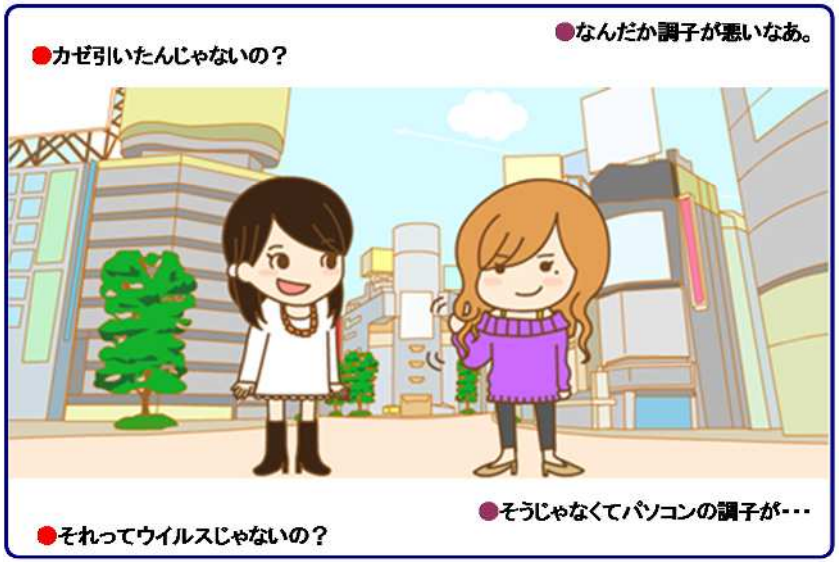
- 『ヒカリ＆つばさの情報セキュリティ3択教室』
  - サンプル規程集の考え方と、最新の問題への対応
    - 大学の状況に適応した、学生向け教育のガイドライン（14テーマ）
  - 学習しやすさ、自習可能
    - アニメ（紙芝居）＋わかりやすい解説
    - 3択問題
  - WebELSでも提供
    - 学認対応：学内の情報セキュリティ研修に利用可能
    - 状況管理も可能
  - 発展的学習
    - 学習ポイント、補足的コラム
    - 詳細な解説（4ページ）

3択教室～目次

話	テーマ	テーマの詳細	ページ
1	ウイルス	ウイルス対策はいつも忘れずに	・・・9
2	フィッシング詐欺対策	フィッシング詐欺	・・・15
3	匿名掲示板	匿名だったら何を書いても構わない？	・・・21
4	USBメモリ	USBメモリをなくしてしまったら	・・・29
5	ネット出会い	ネットで知り合った人と会ったら	・・・35
6	怪しいソフトウェア	怪しいソフトに近づくと危ない	・・・43
7	架空請求	ネット犯罪の被害にあわないように	・・・49
8	著作権	私設ファンクラブのサイトを開設する	・・・57
9	メールの添付ファイル	添付ファイル付のメールが届かない？	・・・63
10	無線LANは危ない？	無線LANが危ない。その対策は？	・・・71
11	パスワードの管理	安全で忘れないパスワードとは	・・・83
12	ＯＳ及びソフトウェアをアップグレード	OSとソフトウェアはいつも最新に保つ	・・・91
13	ネットショップで購入した商品が届かない	ネットショッピングで商品が届かない！	・・・99
14	パソコンの正しい捨て方	パソコンを捨てるときにも作法がある	・・・109

3択教室～問題例

ウイルス対策をしましょう



第１話

ウイルス対策は忘れずに！

ヒカリちゃんが，風邪をひいたうえに，パソコンの調子もイマイチのようで，しずかちゃんにこぼしています。パソコンも，ウイルスに感染したのでしょう。パソコンを買ったあと，ウイルス対策しないままだったようです。パソコンのウイルスもどこにでもいて，感染の機会をうかがっています。USB メモリを使って友達とレポートを交換しただけでもウイルス感染することがあります。このようにならないためのヒカリちゃんの選択は？

さて，ここで 3 択問題です。考えてみてください。

【問題】	ヒカリちゃんは，本当はどうすればよかったのでしょう？
A	ファイアウォールがあるから大丈夫。
B	パソコンにウイルスが侵入してから考える。
C	ウイルス対策ソフトを導入する。

この場合のヒカリちゃんの選ぶべき答えは

C	ウイルス対策ソフトを導入する。

です。

ありがとうございました

ご意見、ご要望等ありましたら、
お気軽にご連絡ください。

<kanaya@law.tohoku.ac.jp>

<sp-comment@nii.ac.jp>