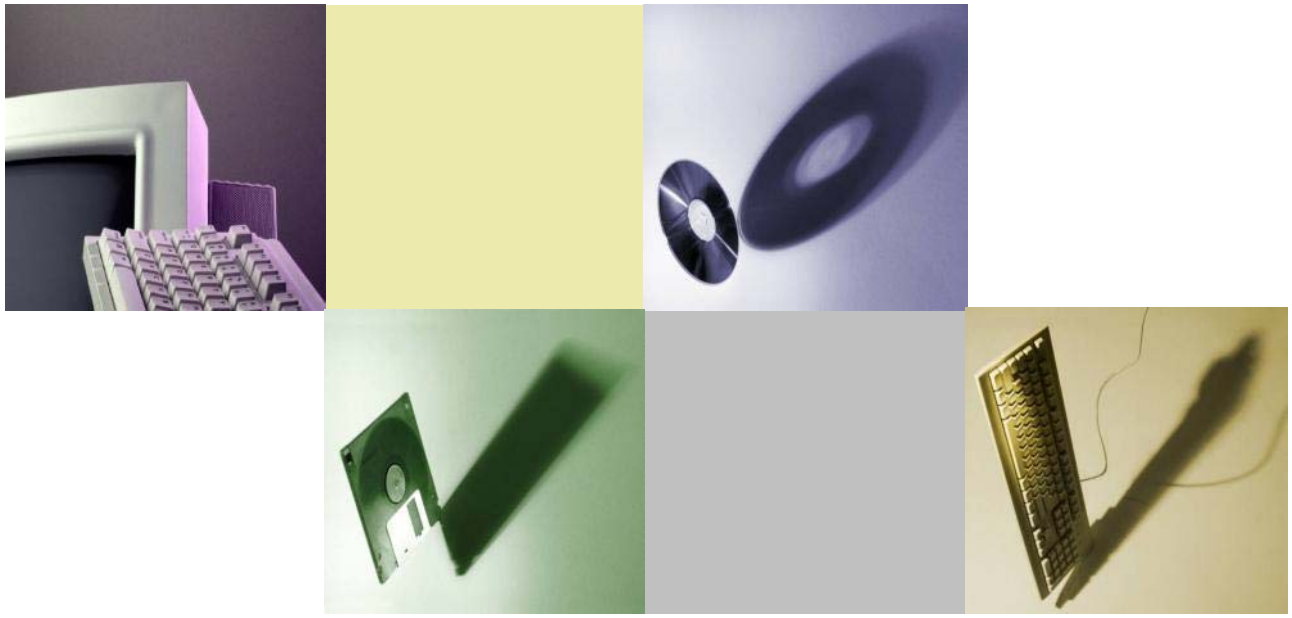
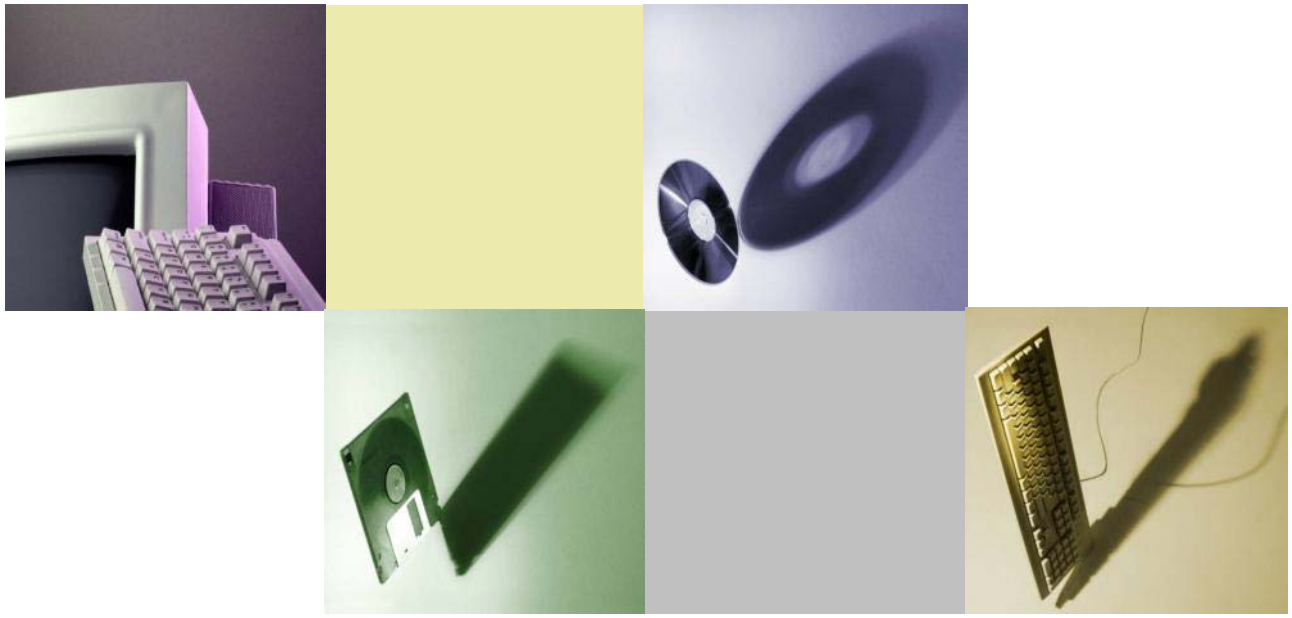
セキュリティポリシの話
（高等教育機関のための情報セキュリティ対策サンプル規程集）



東北大学　サイバーサイエンスセンター　曽根秀昭

大学の活動と情報セキュリティ



大学で扱う情報

【構成員】

•役員，　各種の職員，　教員，　派遣職員，　受託業者，　各種の研究員

•学生　←構成員なのか・顧客なのか（TA・RAは？）

【活動との関連】

•教育（学生へ）：　教務情報（履修，成績），教材・講義，eラーニング

•研究（学生とともに）：　研究情報（論文原稿，データ，技術・設備），発表論文

•運営：　経営（人事，財務，……），広報，

•（医療）

【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（可用性・機密性・完全性）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）

•社会や関係先へ対する責任

•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）

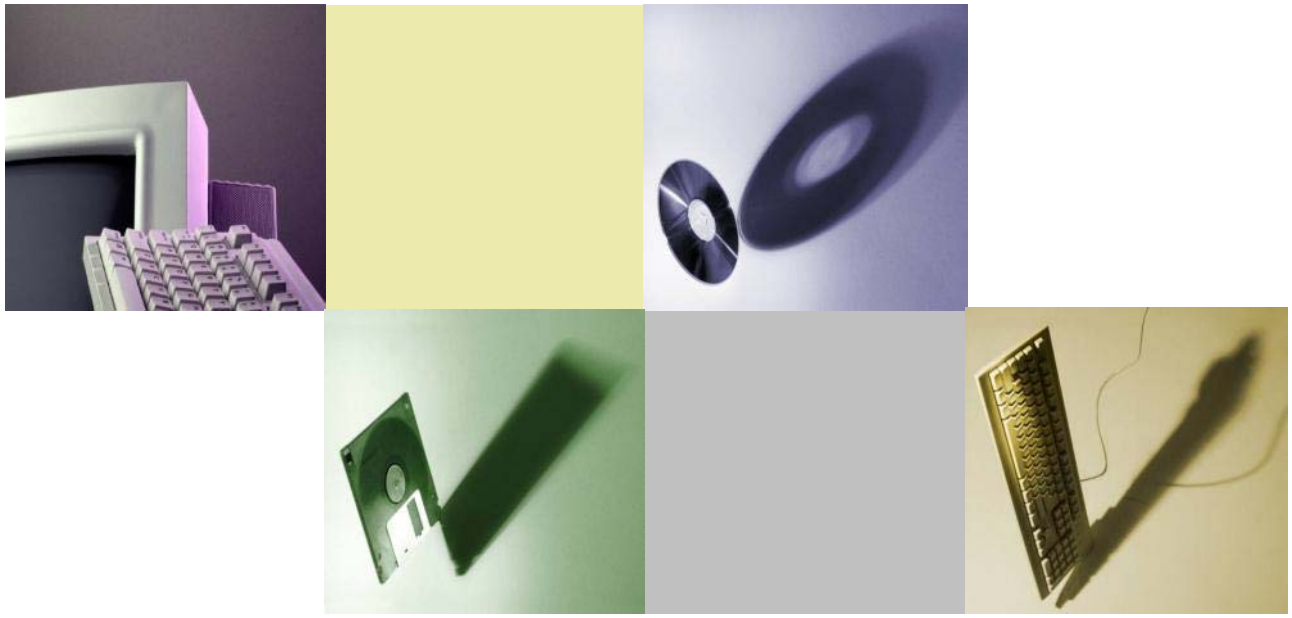
•研究組織・研究者について，学問の自由との両立

•教育機関として，学生に対する情報セキュリティ教育

（国立）大学の取り組みへの要求

- **情報セキュリティポリシーの制定**
  - 各大学において情報セキュリティポリシーを策定すること
- **情報セキュリティインシデント対策**
  - インターネットから／への不正アクセス等
  - 情報漏洩対策
  - 予防対策，　利用者教育，　自己点検
- **政府機関統一基準への準拠**
  - 「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向上の促進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であろう。
- **情報セキュリティ対策に取り組む体制の構築**
  - 各国立大学法人の第二期中期目標に必須
  - 「第2次情報セキュリティ基本計画」及び「セキュア・ジャパン2009」

情報セキュリティポリシー・規程の雛形



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

- **概要**
  - 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
  - 専門家集団による策定（合同）
    - 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
    - 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
  - 2007年10月公開
    - http://www.nii.ac.jp/csi/sp/ 公開中
  - ひきつづき，改訂・推進の活動を継続中

大学における情報セキュリティポリシーの策定の動き

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）

2001.2～2003.1
「高等教育機関におけるネットワーク運用ガイドライン」
（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

2001.7～2002.3
「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）

セキュリティポリシー政府機関統一基準

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～（2010.3）
サンプル規程集とその解説の作成

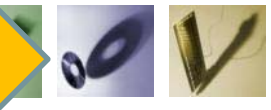
合同

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～（2010.3）
・「考え方」から 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

（2010–） 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



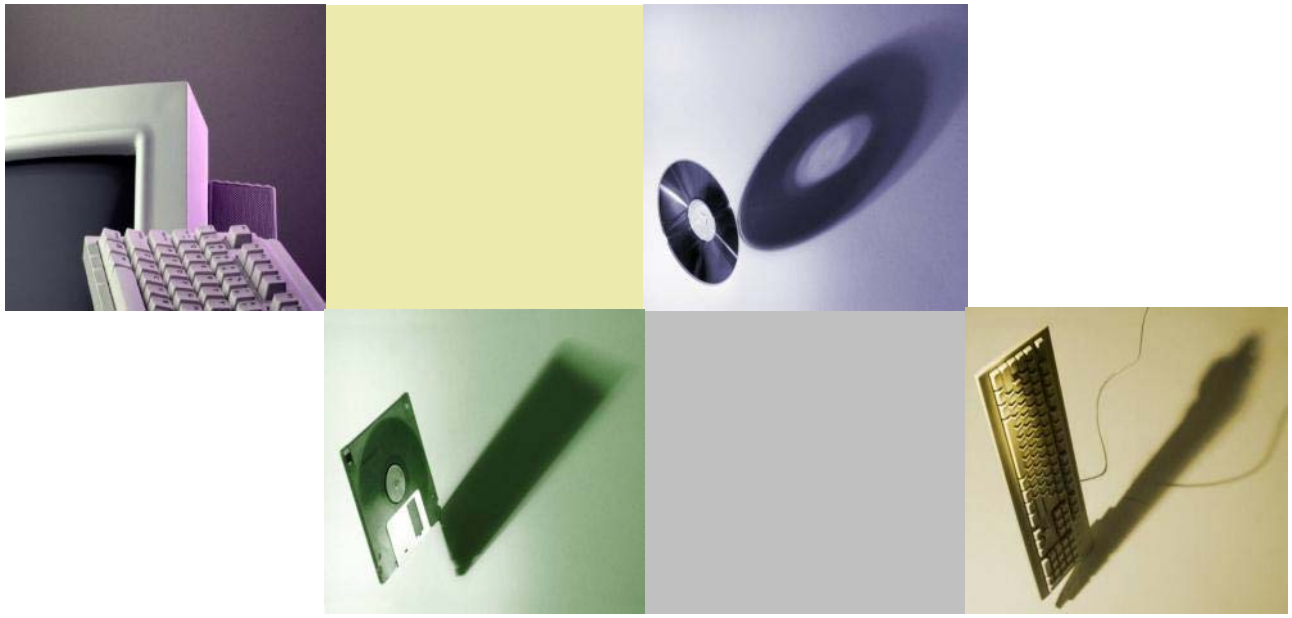
策定の活動体制

◆検討内容と活動体制

- 意見・質問に対応しつつ，規則やマニュアルのひな形の完成
- 平成19年8月に意見募集を実施
- 「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」（平成19年10月版）を提供・公開
- 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

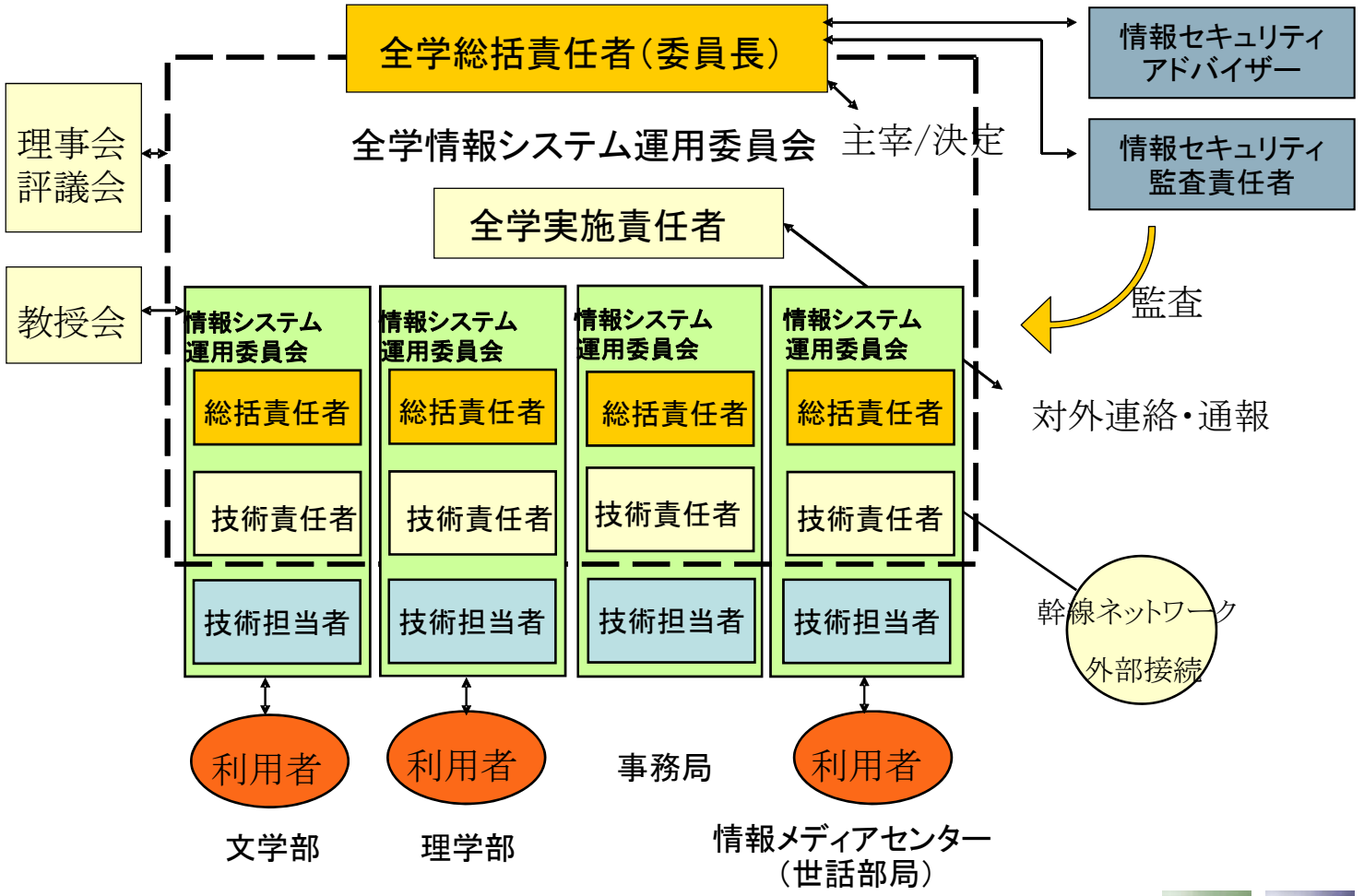
策定したサンプル規程集の体系



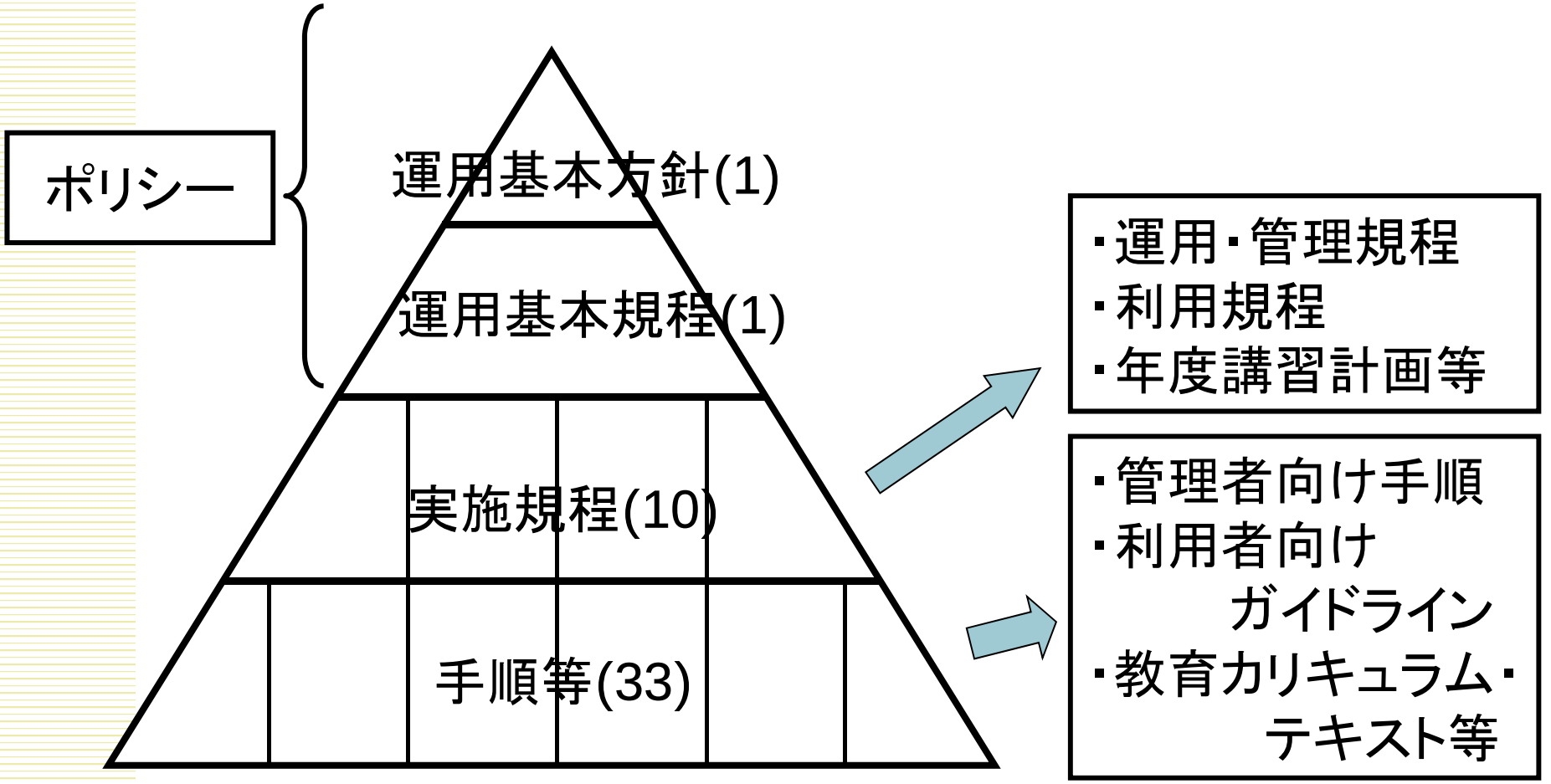
サンプル規程集における前提

- **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の担当
  - 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
  - 「ガイドライン」をベースとし，情報資産のセキュリティ確保を含めるため，対象を情報システム全体まで拡大

A大学の情報システム運用管理体制



サンプル規程集のポリシー・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

- **方針： 政府機関統一基準とその考え方に準拠**
  - とくに，事務情報システム
- **提供・公開： 2007年10月開始**
  - 以後改訂を継続
  - 46編，704p（2010年版）
  - インターネット出版 http://www.nii.ac.jp/csi/sp/
- **その後の改訂検討（～2010年度版・2011年3月）**
  - A2105 情報サービス運用・管理規程
  - 外部クラウドサービス利用の際にとるべき情報セキュリティ対策
    - A3111外部委託における情報セキュリティ対策として、実施手順

策定したサンプル規程集の構成(初期:2007-2010)

ポリシー	実施規程	手順等
A1000 情報システム運用基本方針 A1001 情報システム運用基本規程	A2101 情報システム運用・管理規程 A2102 情報システム運用リスク管理規程 A2103 情報システム非常時行動計画に関する規程 A2104 情報格付け規程	A3100 情報システム運用・管理手順の策定に関する解説書 A3101 情報システムにおける情報セキュリティ対策実施規程§ A3102 例外措置手順書； A3103 インシデント対応手順 A3104 情報格付け取扱手順； A3105 情報システム運用リスク評価手順 A3106 セキュリティホール対策計画に関する様式§ A3107 ウェブサーバ設定確認実施手順§ A3108 メールサーバのセキュリティ維持手順§ A3109 人事異動の際に行うべき情報セキュリティ対策実施規程 A3110 機器等の購入における情報セキュリティ対策実施規程§ A3111 外部委託における情報セキュリティ対策実施手順 A3112 ソフトウェア開発における情報セキュリティ対策実施手順§ A3113 外部委託における情報セキュリティ対策に関する評価手順 A3114 情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書(*) A3115 情報システムの構築等におけるST 評価・ST 確認の実施に関する解説書(*)
	A2201 情報システム利用規程	A3200 情報システム利用者向け文書の策定に関する解説書 A3201 PC取扱いガイドライン A3202 電子メール利用ガイドライン； A3203 ウェブブラウザ利用ガイドライン A3204 ウェブ公開ガイドライン； A3205 利用者パスワードガイドライン A3211 学外情報セキュリティ水準低下防止手順 A3212 自己点検の考え方と実務への準備に関する解説書
	A2301 年度講習計画	A3300 教育テキストの策定に関する解説書 A3301 教育テキスト作成ガイドライン(利用者向け) A3302 (部局管理者向け)； A3303 (CIO/役職者向け)
	A2401 情報ｾｷｭﾘﾃｨ監査規程	A3401 情報セキュリティ監査実施手順
	A2501 事務情報セキュリティ対策基準	A3500 各種マニュアル類の策定に関する解説書； A3501 各種マニュアル類(**) A3502 責任者等の役割から見た遵守事項
	A2601 証明書ポリシー(*) A2602 認証実施規程(*)	A3600 認証手順の策定に関する解説書 A3601 情報システムアカウント取得手順

§は策定手引書
(*) 外部文書の参照のみ,
(**) 各大学にて策定することを想定

サンプル規程集(2012年度版・2013年7月)の改訂

- 政府機関統一基準23年度版の構成の変更→「B系列」
  - 統一管理基準，統一技術基準への分割・改定への対応
- **学外認証連携に対応する規程等文書の作成**
  - 「認証基盤運用管理規程」
- 大学における情報システムを取り巻く環境の変化等
  - **外部委託・クラウド、モバイルなど、新しい運用・利用への対応**
- サンプル規程集の活用性の向上に関する検討
  - 重要度・活用度の低い文書を参考資料とするなどの整理
- 段階的提供：運用基本方針、運用基本規程、実施規程
- 全体
  - 文書番号冒頭の記号をAからBに変更。
  - 番号体系を変更（技術的内容を扱う文書の下2桁が、51～99）

新体系のサンプル規程集(2013)の提供

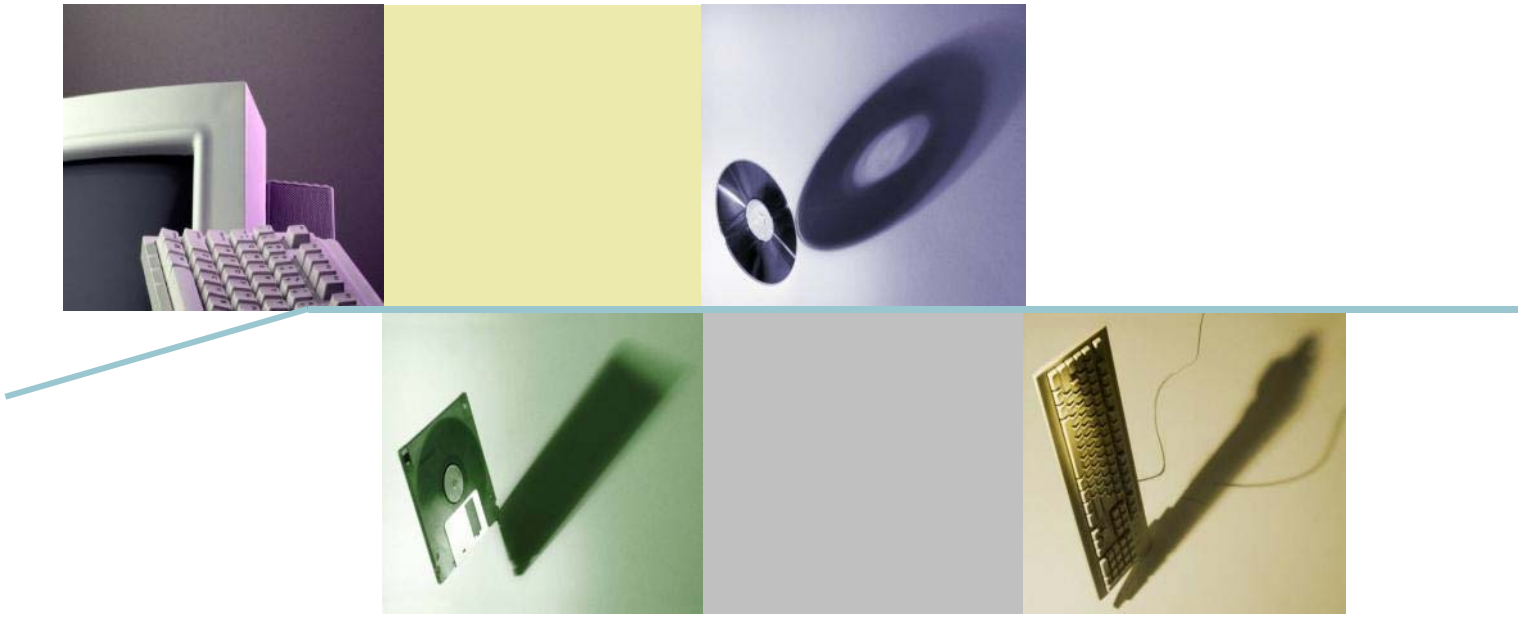
- B1000 情報システム運用基本方針
- B1001 情報システム運用基本規程

- B2101情報システム運用・管理規程
  - 平成24年度版までの統一基準群で追加、変更された内容を反映。
  - 技術的内容をB2151～B2153に分離。
- B2102 情報システム運用リスク管理規程
- B2103 情報システム非常時行動計画に関する規程
- B2104 情報格付け基準
- (B2151情報セキュリティ要件の明確化に関する技術規程)
  - 技術的なもののうち、B2152とB2153に含まれない内容
- (B2152情報システムの構成要素に関する技術規程)
  - 情報システムの構成要素に関する内容
- (B2153アプリケーションソフトウェアに関する技術規程)
  - アプリケーションソフトウェアに関する内容
- (B2201情報システム利用規程)
  - 情報システムの利用変化を踏まえた内容の見直し。
  - 取扱制限事項の追加・変更。
- B2202認証基盤利用規程
  - 学内認証基盤の利用のための規程
- B2301 年度講習計画
- B2401 情報セキュリティ監査規程
- B2501事務情報セキュリティ対策管理基準
  - 統一基準群平成24年度版に対応するため、全面改訂。技術的内容をB2551に分離。
- B2551事務情報セキュリティ対策技術基準
  - 「政府機関の情報セキュリティ対策のための統一技術基準」平成24年度版をもとに新規作成。
- (B2651 証明書ポリシー(CP)(外部文書))
- (B2652 認証実施規程(CPS)(外部文書))

サンプル規程集(2014年度版・2015年7月?)の改訂

- 政府機関統一基準(26年度版)の構成の変更→「C系列」
  - 統一管理基準，統一技術基準の統合への対応
- 情報システムに関わる環境，法律，制度，技術，利用形態の変化
  - **学外認証連携、外部委託・クラウド利用、インシデント対応**など
  - 「事務情報セキュリティ対策基準」
  - 「情報発信ガイドライン」(公式アカウント，SNS)
  - 「インシデント対応手順」
  - 「認証基盤運用管理規程，学外認証連携関連規程等」
    - 全学認証基盤運用管理規程，接続規程，アカウント利用規程
  - 「CSIRT設置規程」(大学におけるCSIRT構築支援)
  - (クラウド利用ガイドライン)
- サンプル規程集準拠教育コンテンツの電子書籍化
- サンプル規程集の活用性の向上に関する検討
- カスタマイズ支援(？)

クラウドサービスの導入とセキュリティポリシー



サンプル規程集でのクラウド対応

- 新たな規則制定は不要
- 現状の対策（規則体系）の検証は必要
  - 本学情報システム
  - 約款による情報処理サービス
- 外部委託の形態の一つとして対応
  - 約款による情報処理サービス（この項を追加）
- 情報の提供方法に応じた対応
  - 外部委託（契約と約款）
  - 第三者提供
  - その他



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：約款による情報処理サービス
    - 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
- **その他**

本学情報システムと約款による情報処理サービスの違い

- **（サンプル規程集が対象とする）本学情報システム**
  - 情報処理及び情報ネットワークに係わるシステム
    （本学情報ネットワークに接続する機器を含む）
    - 本学により、所有または管理されているもの
    - 本学との契約あるいは他の協定に従って提供されるもの
- **約款による情報処理サービス**
  - 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実施手順

- **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

「約款による情報処理サービス」の利用に際しての注意事項

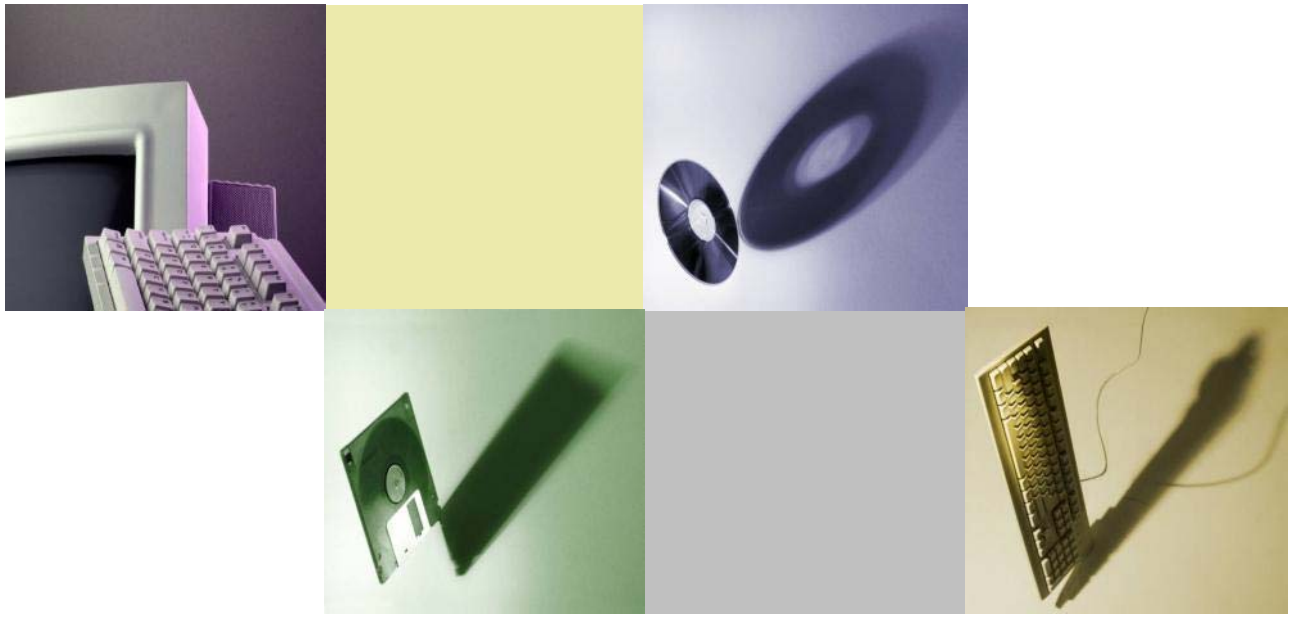
- 処理された結果生じる著作権等の権利の放棄や移管が利用条件となっている場合
- 約款上データ消去等をサービス利用者側で直接実施できない場合
- 利用したデータの削除についてサービス 提供者が個別には応じないことや、情報の置き場所が特定の場所に固定されず、海外の法執行機関等による予期せぬアクセスが行われる場合

無償で利用する情報処理サービスも外部委託にあたるかも

- **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**

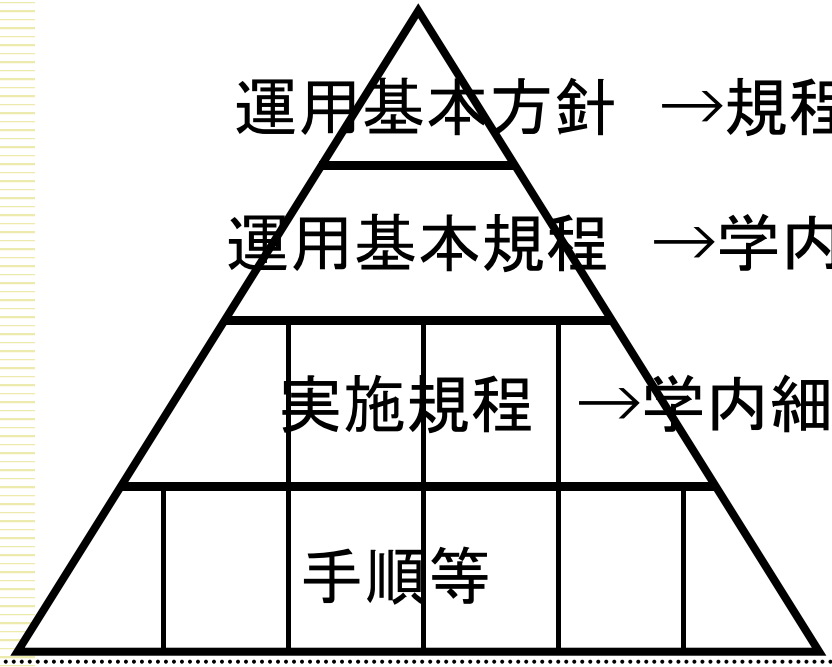


大学におけるサンプル規程集の利用



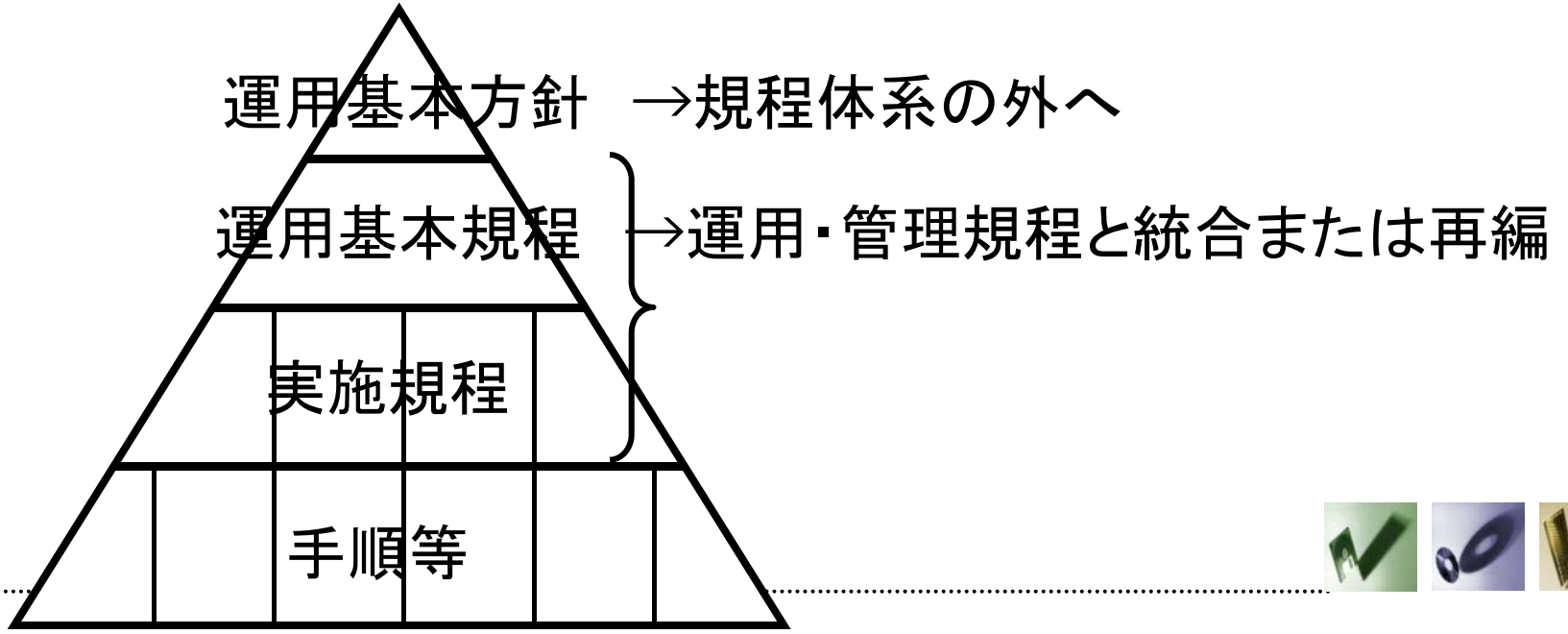
ポリシーの位置付け ― 案1

- 「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→学内規程として制定
- 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
  →内容の重要性や規範性，拘束性を考慮すると，適切とは言い難い



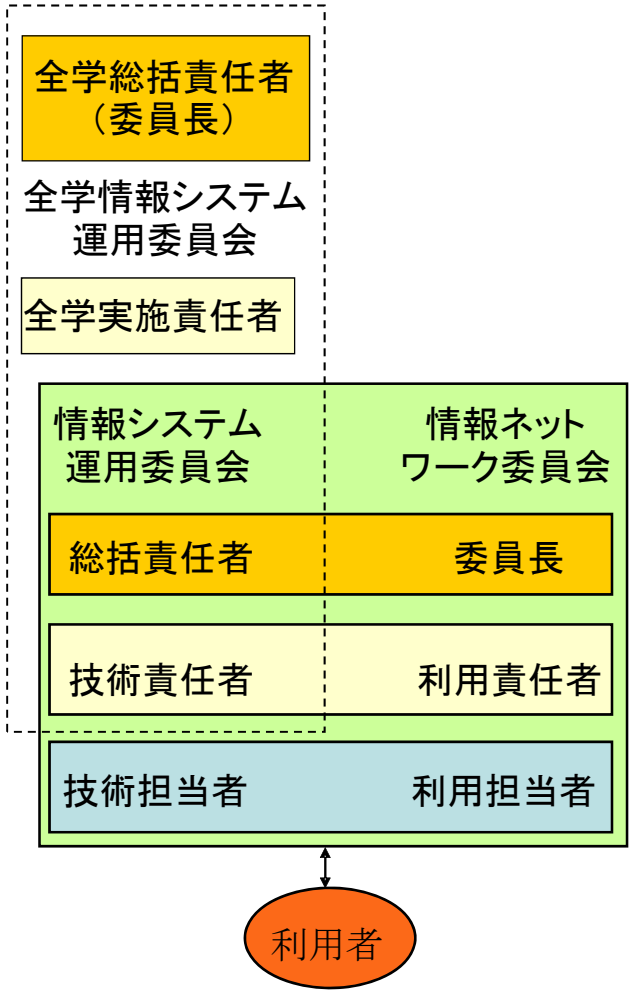
ポリシーの位置付け ― 案2

- 基本規程と実施規程類を学内規程で同列に位置づけ
- 案2－1 →運用基本規程と運用・管理規程を統合
- 案2－2 →これらを再編
  - 運用規程：組織体制の整備や担当者の役割等，運用にあたって必要な総則事項
  - 管理規程：担当者の行うべき事項や遵守事項等，適切に運用するために必要な管理業務



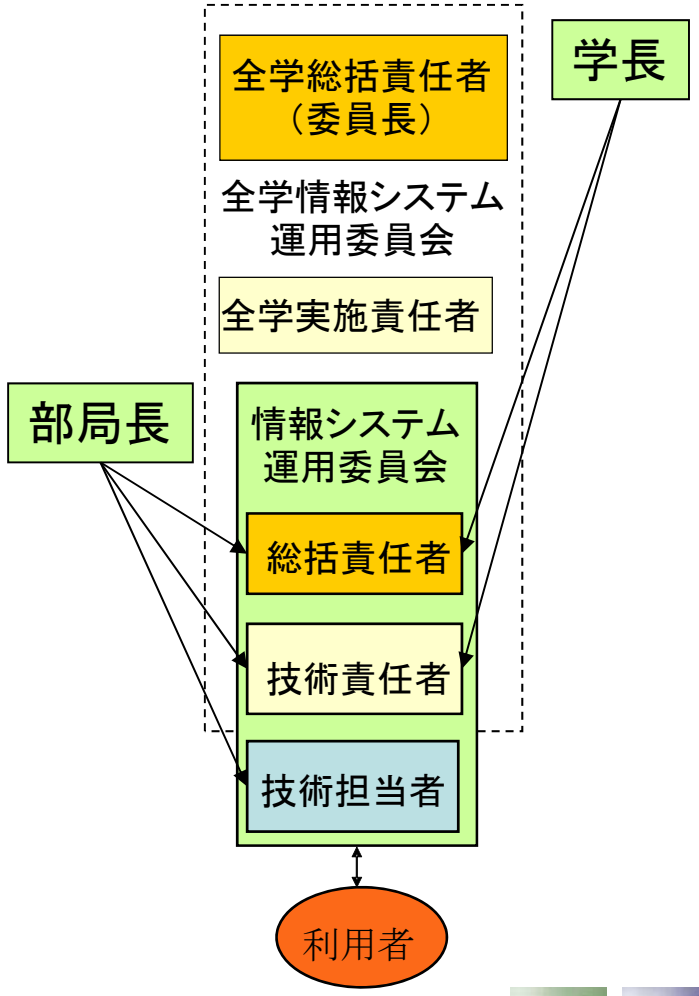
運用管理組織の見直し — 案1

- 既存の規程を改訂，または基本規程に統合
  - 情報ネットワーク・システムの運用管理・利用に，情報セキュリティ対策を追加
- 案１－１ →新たに情報セキュリティ委員会を置き既存の運用管理委員会とは別個に部局の責任者や担当者を任命
  - 機能性や合理性の点で問題
- 案１－２ →既存の組織の役割に情報セキュリティに関する事項を付加
  - このような改訂のほうが好ましいであろう



運用管理組織の見直し — 案2

- **部局の総括責任者や技術責任者などの任命**
  - サンプル規程集では部局で任命
  - 学長や全学総括責任者（CIO）が任命する体制もありうる
    - 大学の方針あるいは既存の組織制度などの事情による



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、研究者データ等はその研究成果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、運用基準　→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