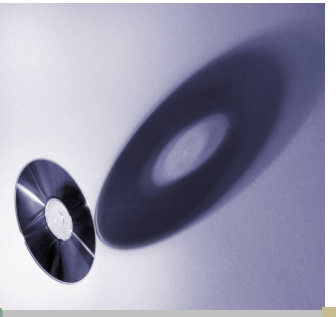
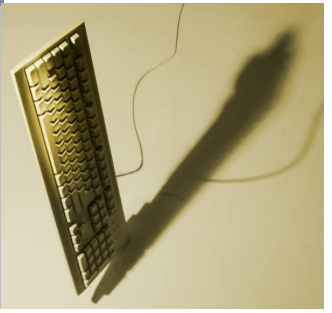
情報セキュリティポリシーの基本的な考え方
～サンプル規程集の利用について～

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



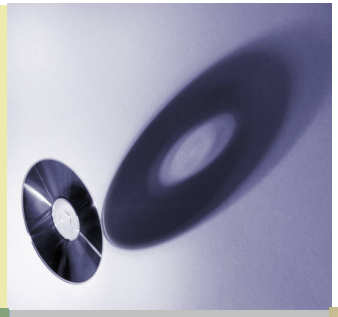
電子情報通信学会
ネットワーク
運用ガイドライン
検討ワーキング
グループ



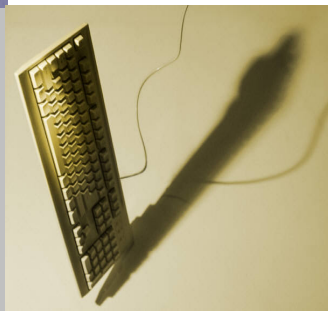
曽根秀昭
(国立情報学研究所 高等教育機関における情報セキュリティポリシー推進部会主査・東北大学教授)

サンプル規程集の策定活動

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



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



大学の情報セキュリティポリシー策定に関する背景

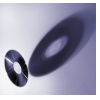
【背景】

- 大学における情報セキュリティレベルの向上は急務
- セキュリティポリシー、実施規程、教育テキストの作成が必要
- 大学における教学・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
- 情報セキュリティ対策の政府機関統一基準の制定、個人情報保護法の施行、国立大学の法人化、セキュリティ水準の高度化

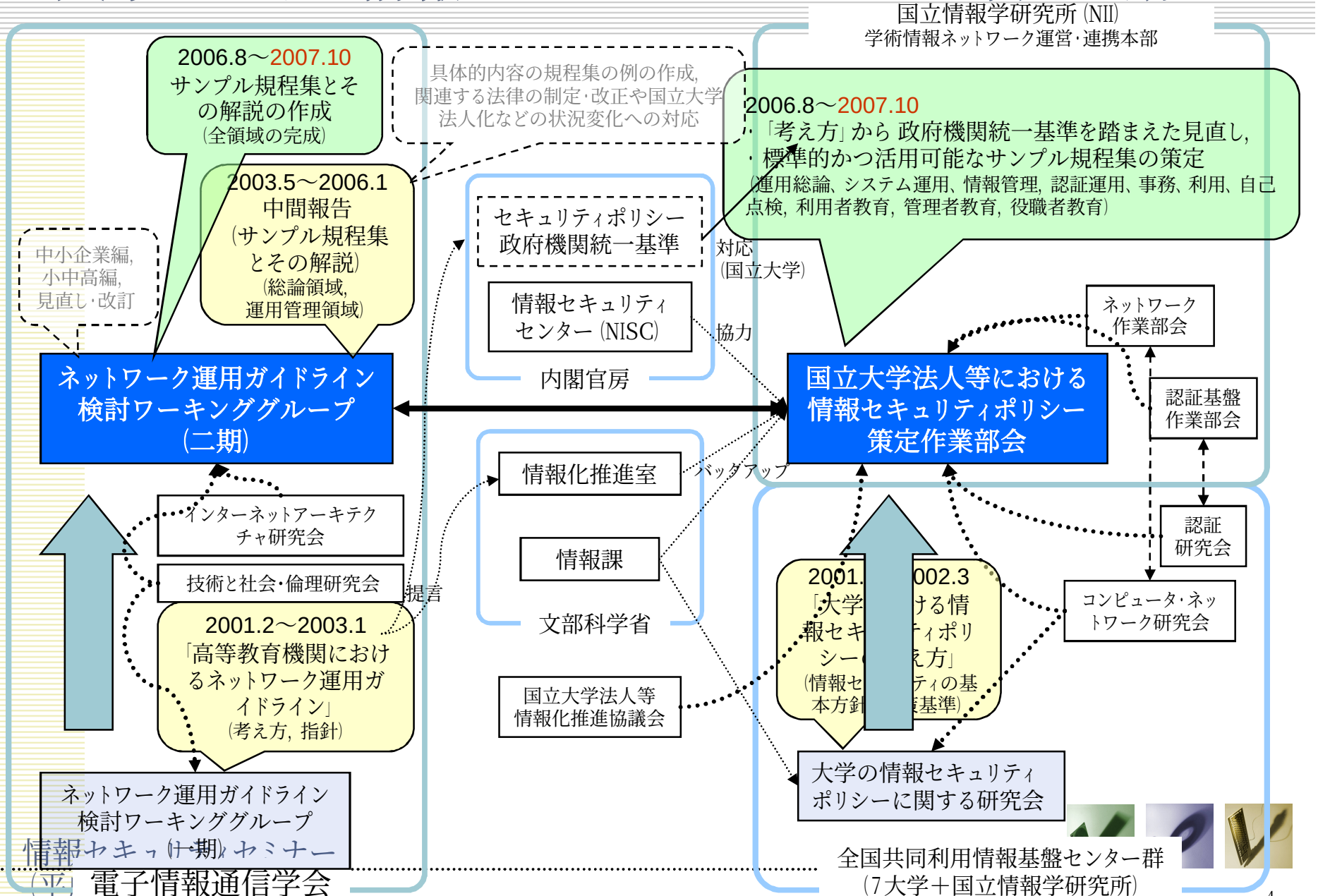
【要請】

雛型となるポリシー規程集を制定すべき必要性

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)


大学における情報セキュリティポリシーの策定の動き



策定の活動体制（2007年度）

◆検討内容と活動体制

- 意見・質問に対応し，前年度に公開に至らなかった未完の規則やマニュアルの完成
- 8月に意見募集を実施し10月に公開（10月までの設置）
- 「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
- 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

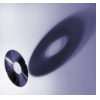
運用（運用総論、システム運用、情報管理）	情報格付け、外部委託・人事異動、例外措置 運用・管理、ウェブサーバ・メールサーバ リスク評価・リスク管理、非常時行動計画
認証（認証運用）	認証手順
事務（事務）	各種マニュアル類、責任者等の役割
利用（利用、自己点検）	ウェブブラウザ、ウェブ公開、自己点検
教育（利用者、管理者、役職者）	教育テキスト



策定したサンプル規程集の構成

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


策定したサンプル規程集の分量

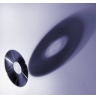
	ポリシー A10xx (12p)	実施規程 A2xxx (200p)	解説･手順等 A3xxx (374p)
総論 x0xx	2編, 12p		
運用 x1xx		4編, 47p	16編, 186p
利用 x2xx		1編, 8p	8編, 95p
教育 x3xx		1編, 5p	4編, 38p
監査 x4xx		1編, 4p	1編, 24p
事務 x5xx		1編, 134p	2編, 24p
認証 x6xx		2編, 2p	2編, 7p

この枠内で
9編，76p



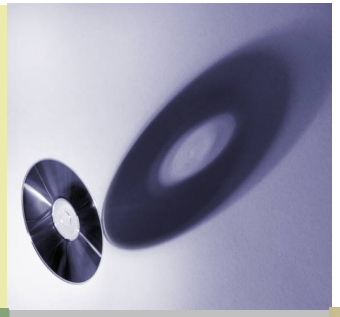
サンプル規程集の公開･配布

- インターネット出版
  - http://www.nii.ac.jp/csi/sp/
  - 10月31日公開 (11月16日目次訂正)
  - http://www.ieice.org/jpn/h191031.html からもリンク
- 「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」
  - PDFファイル, SJISテキスト圧縮ファイル
  - ＦＡＱ･お知らせ
- 意見･要望の募集 (平成19年8月実施) の結果
- 参考資料
  - 旧版
  - 「大学における情報セキュリティポリシーの考え方」(平成14年3月29日)

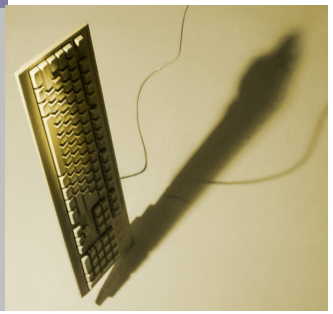




策定したサンプル規程集の体系

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

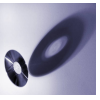


電子情報通信学会
ネットワーク
運用ガイドライン
検討ワーキング
グループ

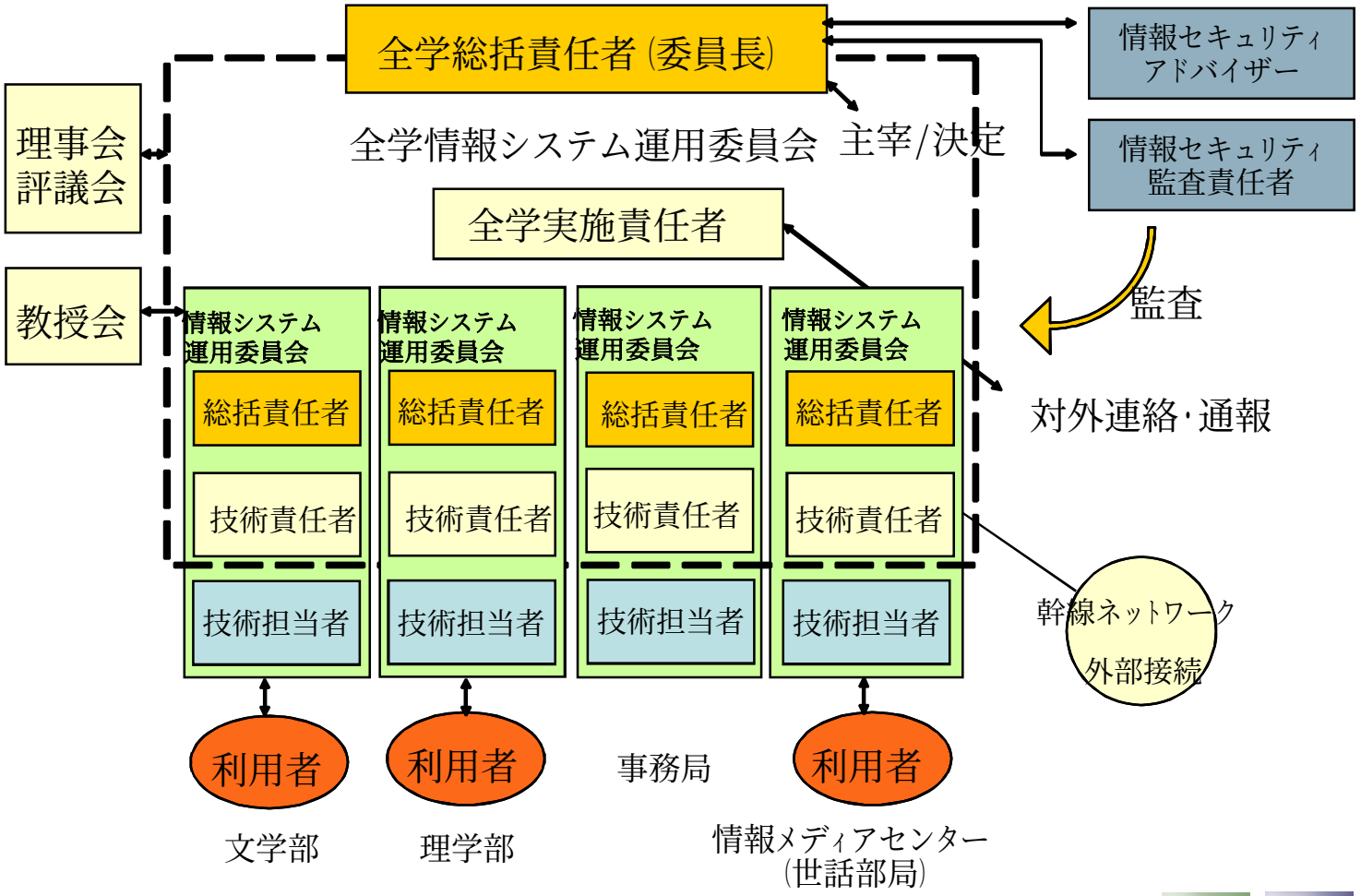


サンプル規程集における前提

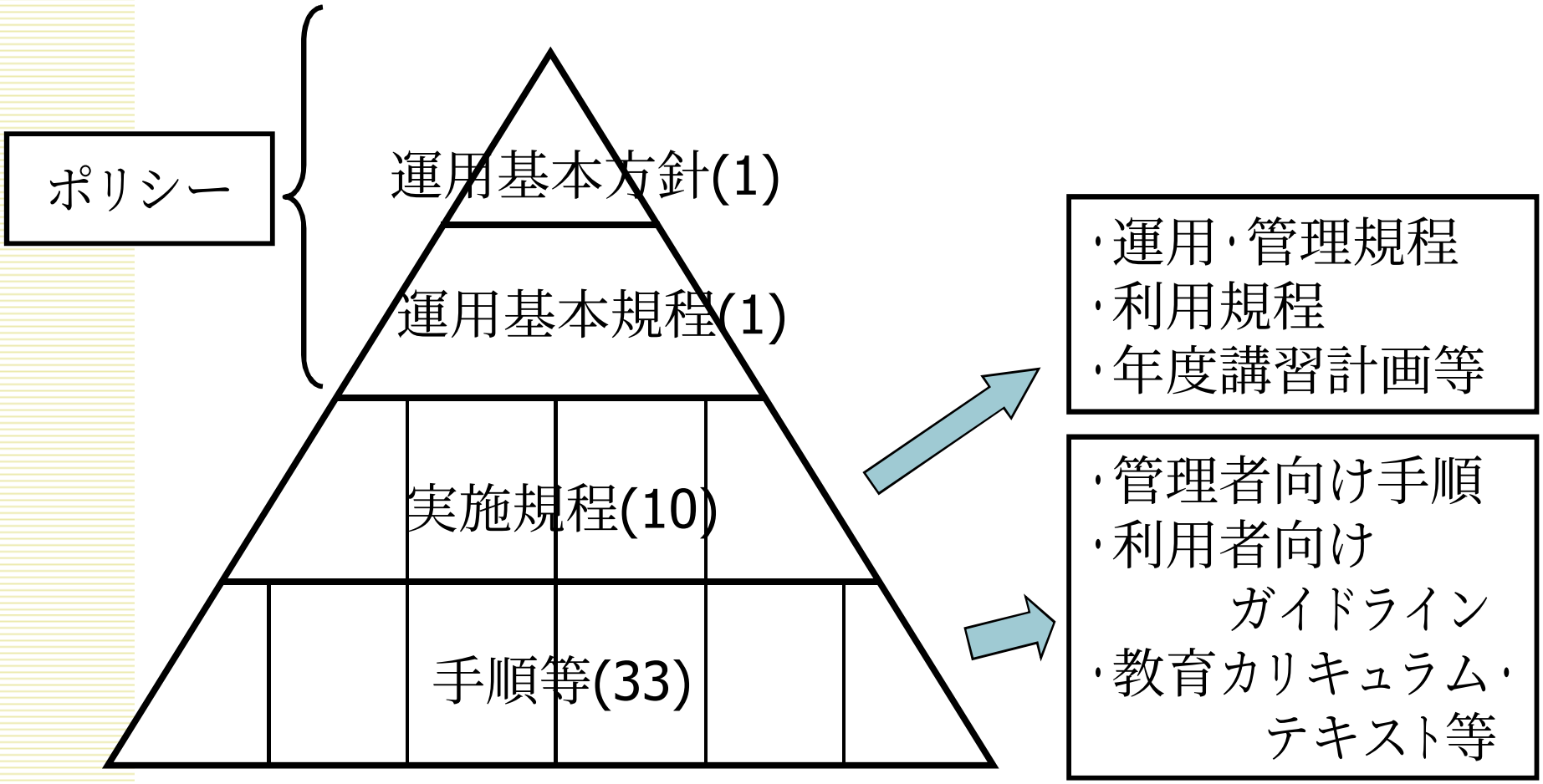
- モデルとして仮想A大学を想定
  - 文学部と理学部の2学部で構成され、両学部とも在学生1,000人（1学年250名）ずつ
  - 学内共同利用施設として情報メディアセンター（図書館を含む）がある
  - 学内ネットワーク（事務系ネットワークを除く）や学内共同利用の情報システムは情報メディアセンターの担当
  - 副学長の一人が最高情報責任者（CIO）であり、最高情報セキュリティ責任者（CISO）の役も兼務
- 各機関の具体的な参考として策定
  - 大学の事情に合わせて可能な範囲で政府機関統一基準の考え方に準拠
  - 「ガイドライン」をベースとし，情報資産のセキュリティ確保を含めるため，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

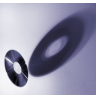


サンプル規程集のポリシー・実施規程・手順等の体系



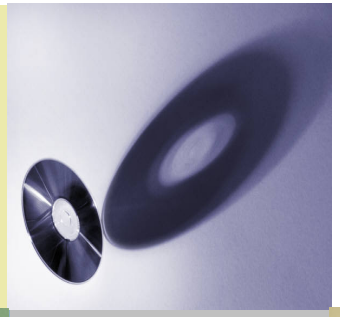
サンプル規程集に収録した範囲

- **ポリシー**
  - 情報システム運用基本方針，情報システム運用基本規程
- **実施規程**
  - （システム運用，情報管理領域）4
  - （利用者領域）1
  - （教育領域）1
  - （自己点検領域）1
  - （事務利用領域）1（基準）
  - （認証運用領域）2（外部文書の参照）
- **手順・ガイドライン等**
  - 33（外部文書参照と策定手引書を含む）
- **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

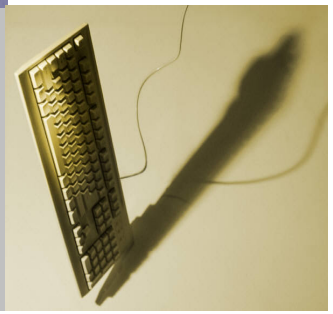




サンプル規程集の利用に関する考察

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

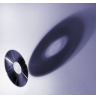


電子情報通信学会
ネットワーク
運用ガイドライン
検討ワーキング
グループ



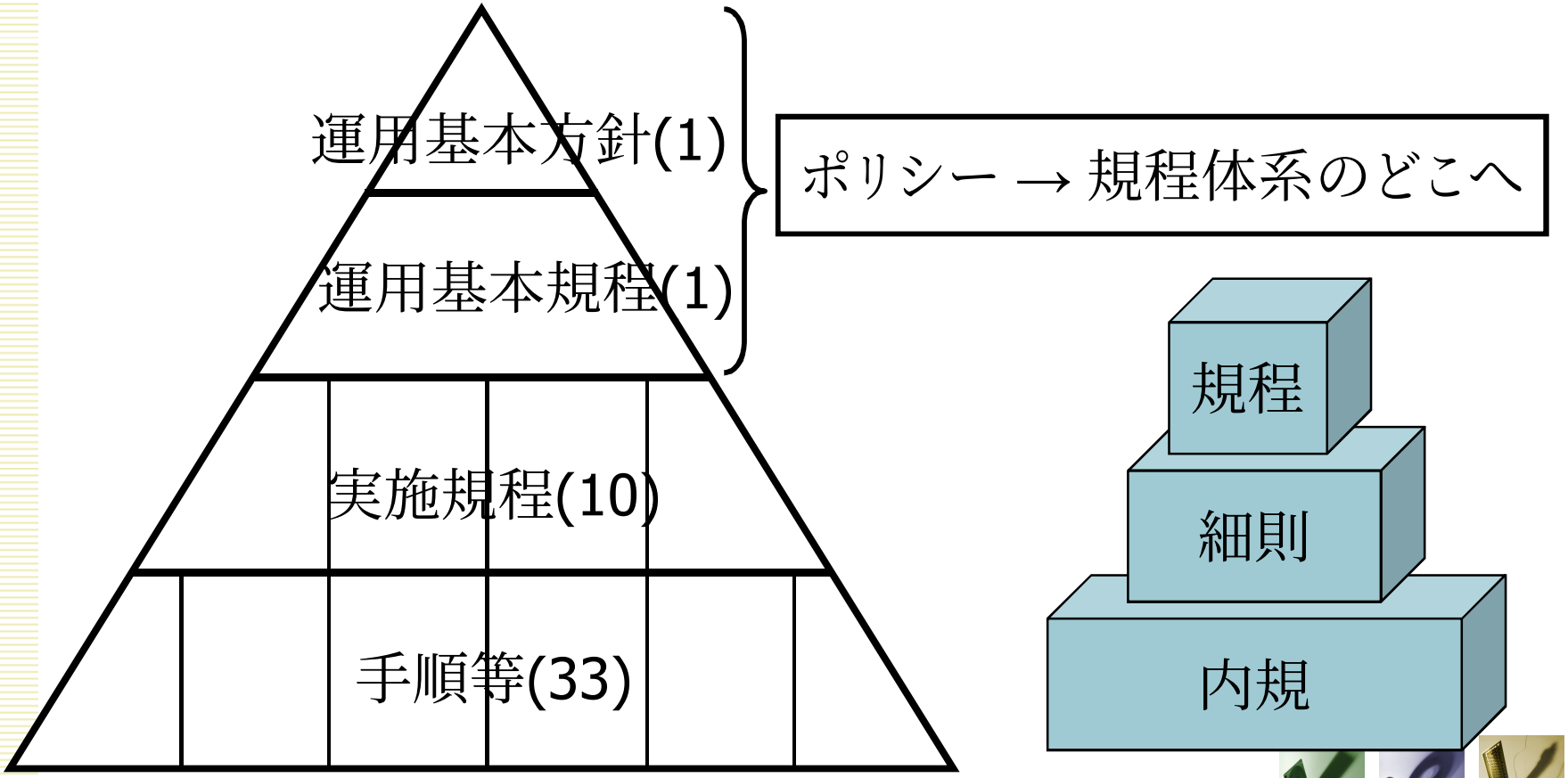
各機関における策定への注意点

- サンプル規程集は仮想の大学について策定されたもの
- これを参考にして具体的な規程を策定する場合
  - 各々の組織の運営方針や体制あるいは既存の規程に合わせて，適切な置換えや修正が必要
  - 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べき
- 以下，いくつかのケースで考察

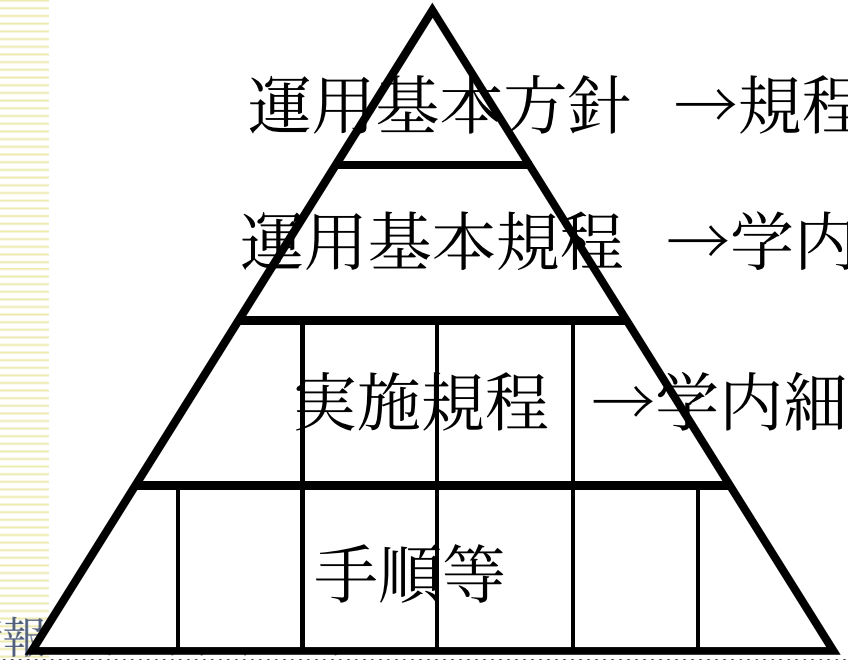

学内規則体系にポリシーを位置付けしにくいケース

- 学内規則の体系において，ポリシーの分類がないケース
  - 規程～細則～内規のような体系への位置付けは容易ではない



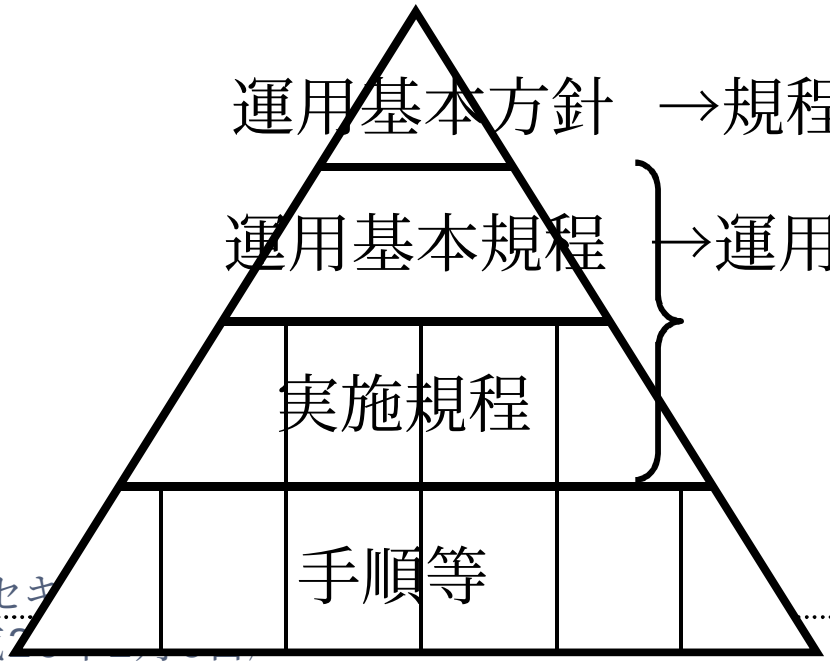
ポリシーの位置付け ― 案1

- 「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



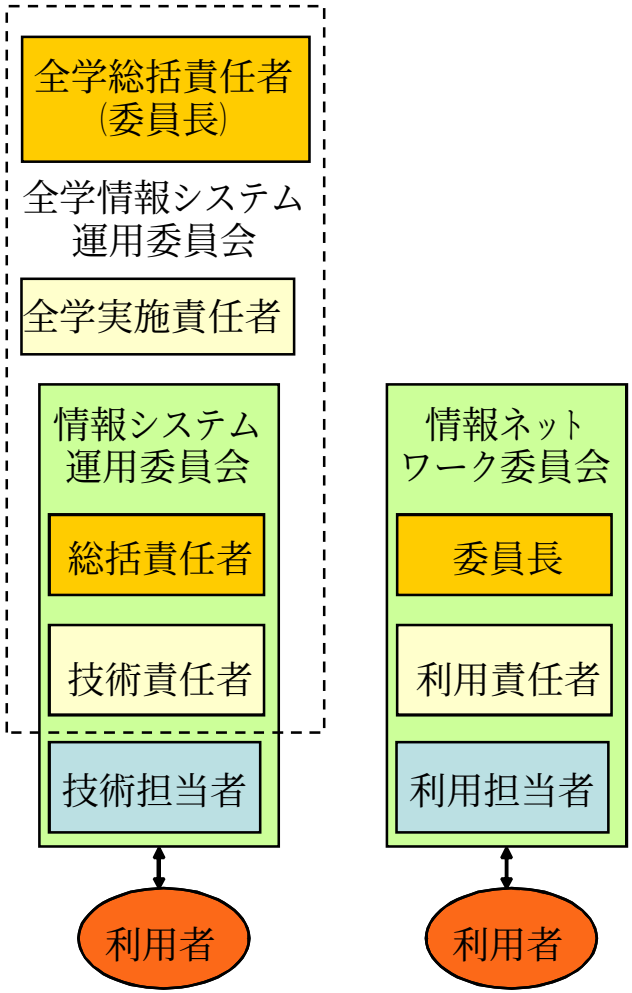
ポリシーの位置付け ― 案2

- 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



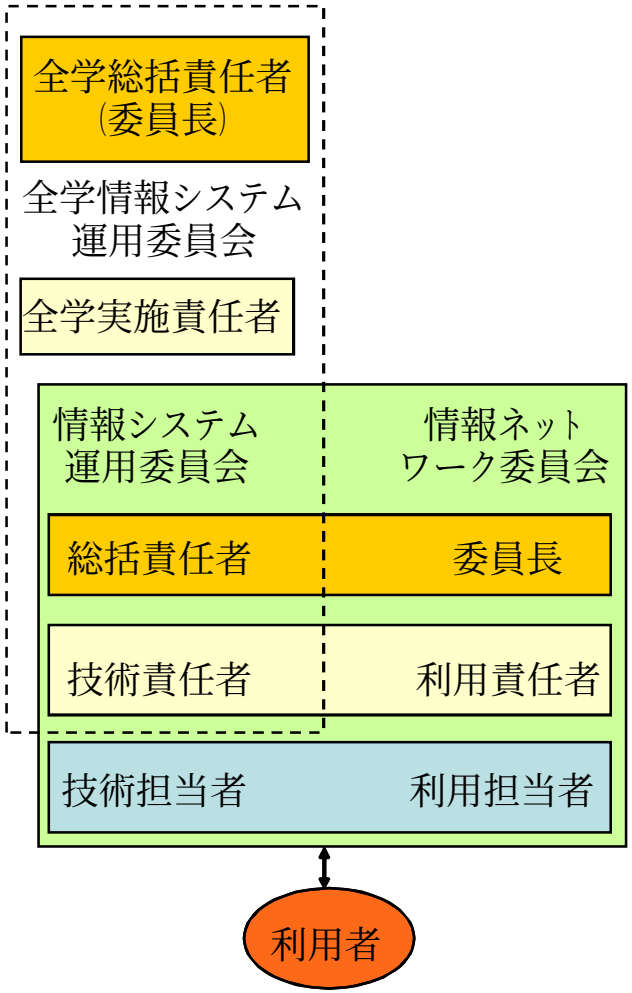
既存の運用管理組織や体制との関係を見直すケース

- **利用部局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**
  - 責任者や担当者が，サンプル規程集の全学委員会の体制と異なる位置づけで同様の機能
  - 役割を統合するなど何らかの整理が必要



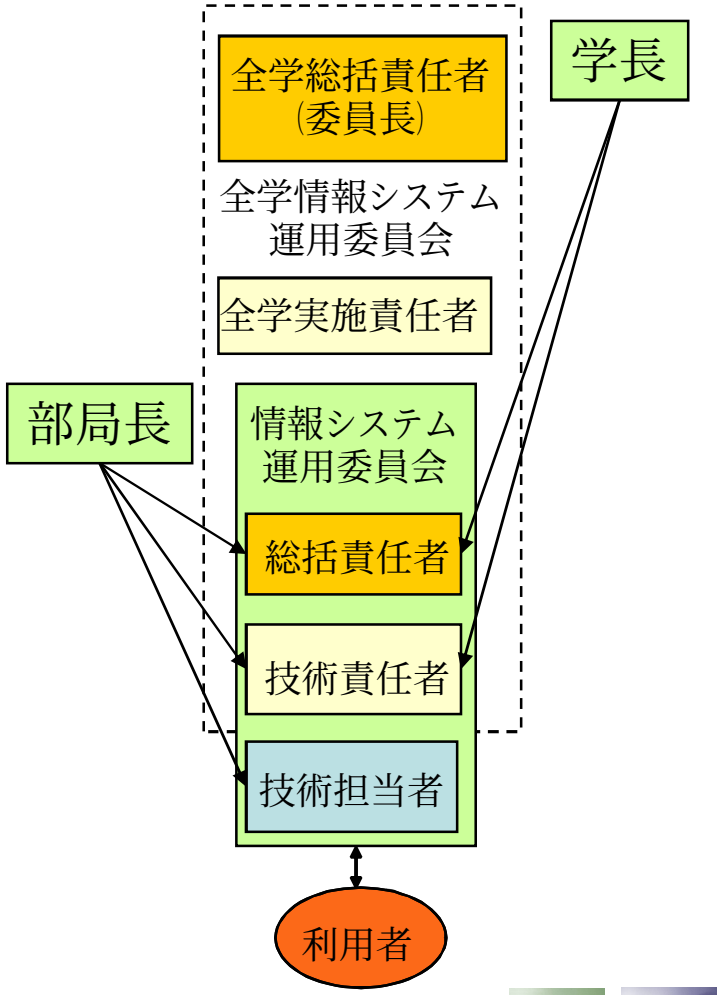
運用管理組織の見直し ― 案1

- 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



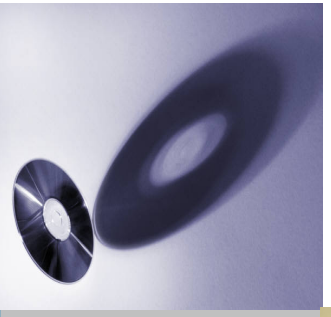
運用管理組織の見直し — 案2

- 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

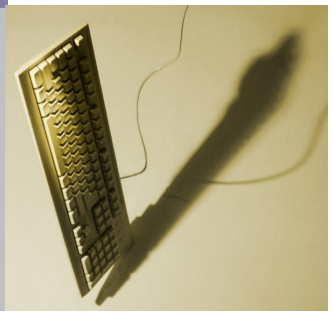


推進部会の今後の活動

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



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



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サイクルをまわ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
    - サンプル規程集の使い方に関わる情報を提供
    - 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**
  - サンプル規程集に対する問い合わせや要望への対応を検討
- **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し
  - 次回の見直し活動に向けた情報収集
- **2007年12月より設置**