

# 政府機関統一基準に準拠した国立大学法人 向け情報セキュリティポリシーの公開

平成19年2月26日

国立情報学研究所客員教授  
東北大学情報シナジーセンター 副センター長  
曾根 秀昭

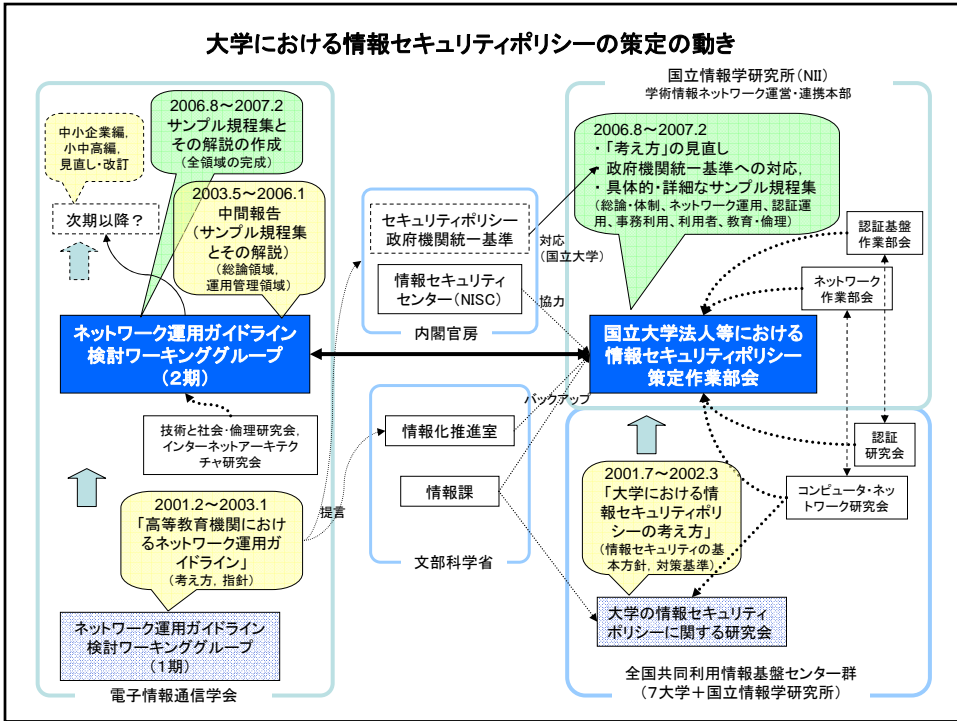
## 大学の情報セキュリティポリシー策定に関する背景

- 【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
  - ↓
  - 大学における教育・研究との関係および組織・運営の考慮や、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



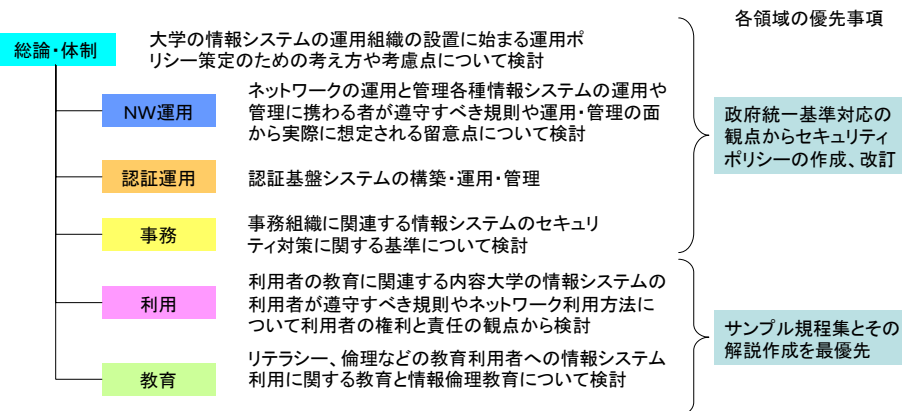
- 【要請】**
- 雑型となるポリシー規程集を制定すべき必要性
- 専門家集団 ⇒ セキュリティの高度化・専門化に対応した作業

## 大学における情報セキュリティポリシーの策定の動き



## サンプル規程集策定の活動

総論・体制、NW運用、認証運用、事務、利用、教育の6つの領域から構成  
各グループ、研究会などのメンバーによる横断的時限組織で、セキュリティポリシーを策定  
法律、統一基準への対応や情報システム運用に関連する規程集の取りまとめ



## 策定したサンプル規程集の構成

ポリシー	実施規程	手順	
A1000 情報システム 運用基本方針	A2101 運用・管理規程 A2102 リスク管理規程 A2103 非常時行動計画 A2104 情報格付け規程	A3101 運用・管理手順 A3102 情報システムリスク評価手順 A3103 インシデント対応手順 A3104 情報格付け手順 A3105 情報取扱い手順 A3106 外部委託における情報セキュリティ対策実施手順 A3107 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 A3111 ウェブサーバ設定確認実施手順 策定手引書 A3112 メールサーバのセキュリティ維持に関する規程 策定手引書	
		A2201 利用規程	A3201 PC取扱い手順 A3202 電子メール手順 A3203 ウェブブラウザ手順 策定手引書 A3204 Web公開手順 A3211 学外情報セキュリティ水準低下防止手順 A3212 自己点検についての解説書
		A2301 年度講習計画	A3301 教育テキスト
		A2401 監査規程	A3401 監査手順
		A2501 事務情報セキュリティ対策基準	A3501 各種マニュアル類
		A2601 証明書ポリシー A2602 認証実施規程	A3601 認証手順
		A3001 責任者等の役割から見た遵守事項 A3002 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 A3003 例外措置手順書	

青字は今年度の策定対象外とした文書

## 効果1. ポリシー策定の効率化

【従来】 各大学で個々に『政府統一基準』の論点を検討

人的資源：学内外から各領域の専門家を集める

基礎調査：  
・法令集の解釈  
・政府統一基準の解釈  
・他大学事例の理解

時間費用：委員10名 × 300時間 と仮定した場合、  
⇒ 人件費換算 3000時間相当/大学



【今回】 ポリシー規程集を活用した場合、

基礎調査：そのまま適用可能 → 不要  
あてはめ：カスタマイズが必要な部分 → 短時間

→ 想定削減効果：きわめて短期での作業を可能に

## 効果2. ポリシー策定の高品質化

**【従来】** 各大学で個々に『政府統一基準』の論点を検討

- 人的資源: 各領域の専門家は全国でも限られている  
⇒ 専門家を集められないおそれ
- 調査範囲: 多岐にわたる専門的領域の調査を要する  
⇒ 検討漏れ事項が生じるおそれ
- 検討期間: 基礎調査の作業に長期間を要する  
⇒ 喫緊の課題に対応できないおそれ

→全論点の検討には、2年程度の検討期間が必要



**【今回】** ポリシー規程集を活用した場合、

- 調査・検討: 全論点を各領域の専門家が検証済み

→効果: セキュリティ対策を早期かつ高品質で実現