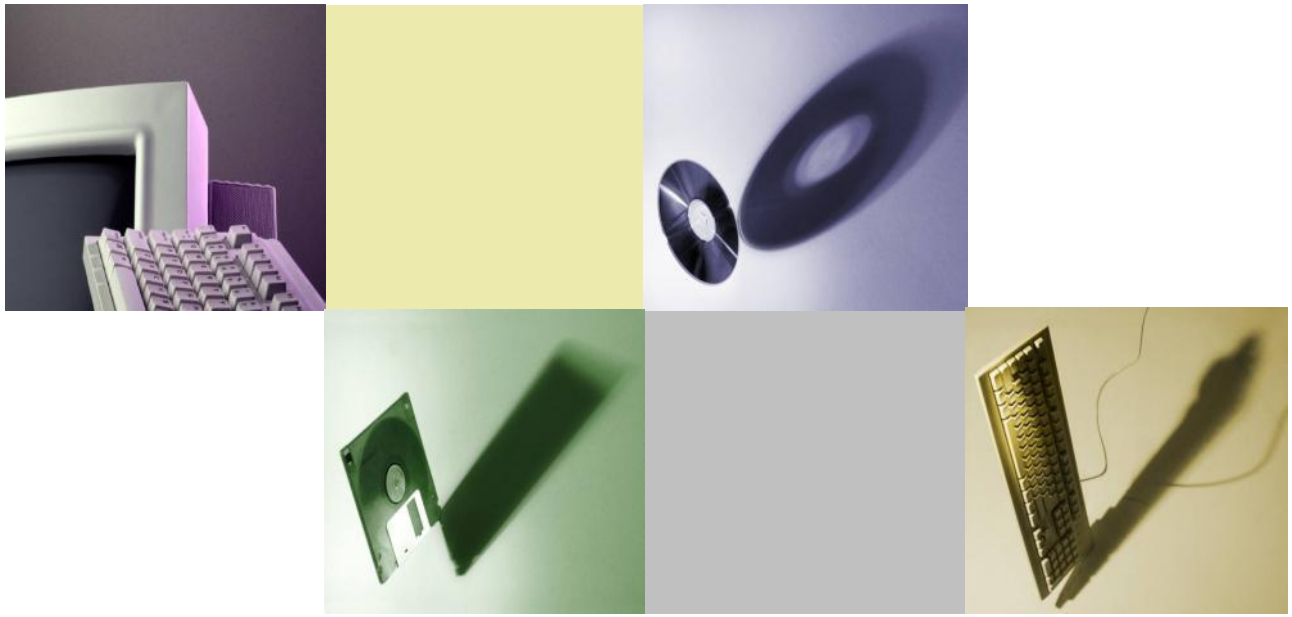
講演3：情報セキュリティポリシー推進部会より

「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」について



東北大学 サイバーサイエンスセンター 教授、
情報セキュリティポリシー推進部会 主査 曽根秀昭

2019.5.30 NIIオープンフォーラム

今北産業

（3行で）

- 大学の情報セキュリティサンプル規程集を提供してます。
- 継続して改訂していて，近くD系列を公表します。
- 各大学でカスタマイズしてください。

- www.nii.ac.jp/service/sp/

- 教材（りんりん姫、ヒカリ＆つばさ等）の報告は次の講演で。

（国立）大学の情報セキュリティ対策への要求

  - Since 2001
- **（情報セキュリティ対策の必要性 …… いまや当然）**
- **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
- **政府機関統一基準への準拠**
- **情報セキュリティインシデント対策**
  - 不正アクセス等, サービス継続性
  - 情報漏洩対策, 個人情報保護対策
  - 予防対策，　利用者教育，　自己点検
- **情報セキュリティ対策に取り組む体制の構築**
  - CISO
  - CSIRT

学内での情報セキュリティ対策を行う根拠規則

- **規則がないと対応したくても根拠がない**
- **規則体系**
  - 情報システム運用規則
  - 管理に関する規則
    - システム管理、リスク管理、非常時行動計画、情報の格付け
  - 利用に関する規則
    - 利用、情報機器、メール利用、情報発信
  - 教育に関する規則
  - 監査に関する規則
  - 事務システムに関する規則
- **規則を作らなければならない**

情報セキュリティポリシー推進部会
（情報犬ビットくん）

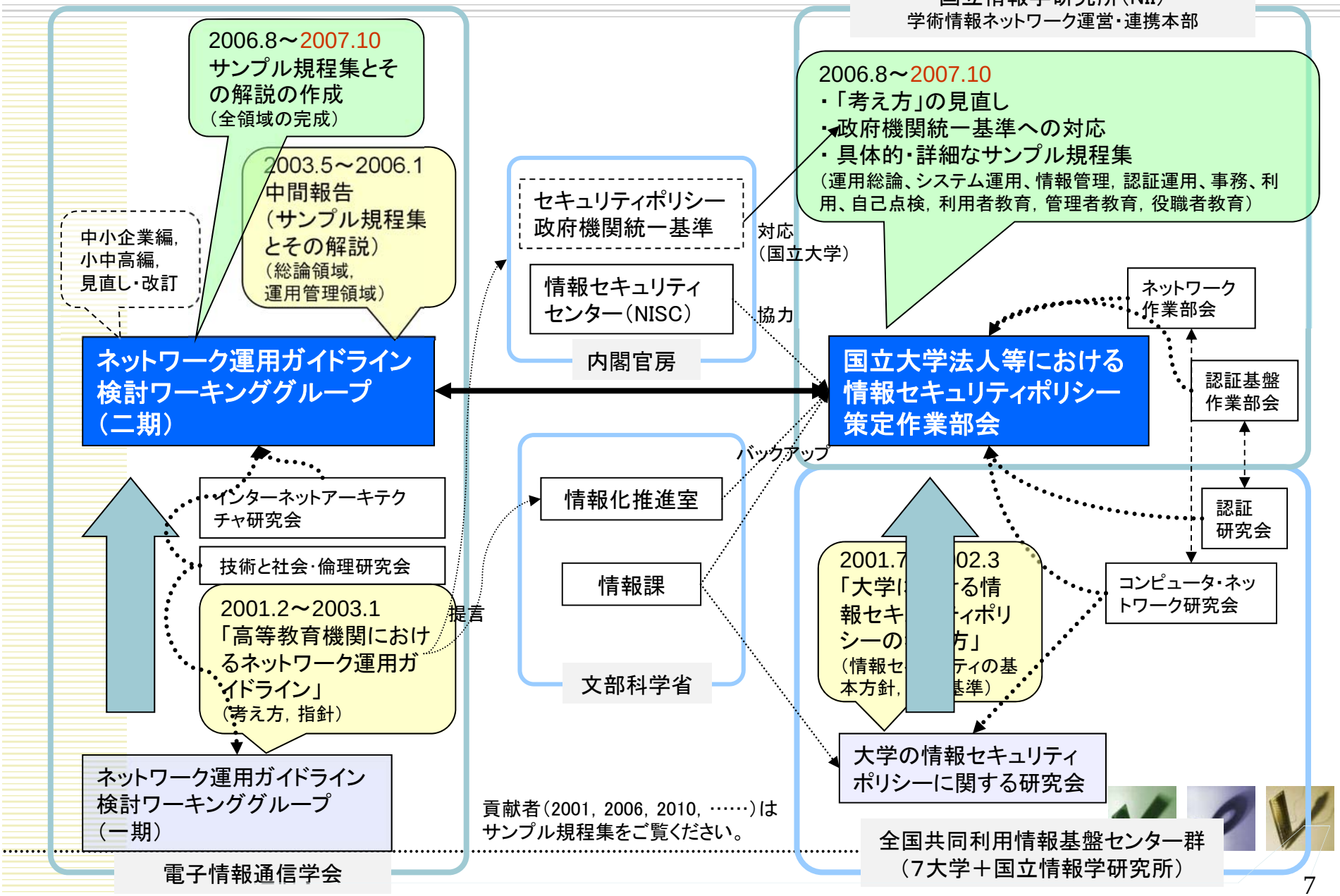
ビットくんメモ：高等教育機関における情報セキュリティポリシー推進部会は，2001年に電子情報通信学会が始めたのが最初なんだって．その後，NIIが中心となって取り組むようになったらしいよ．

5

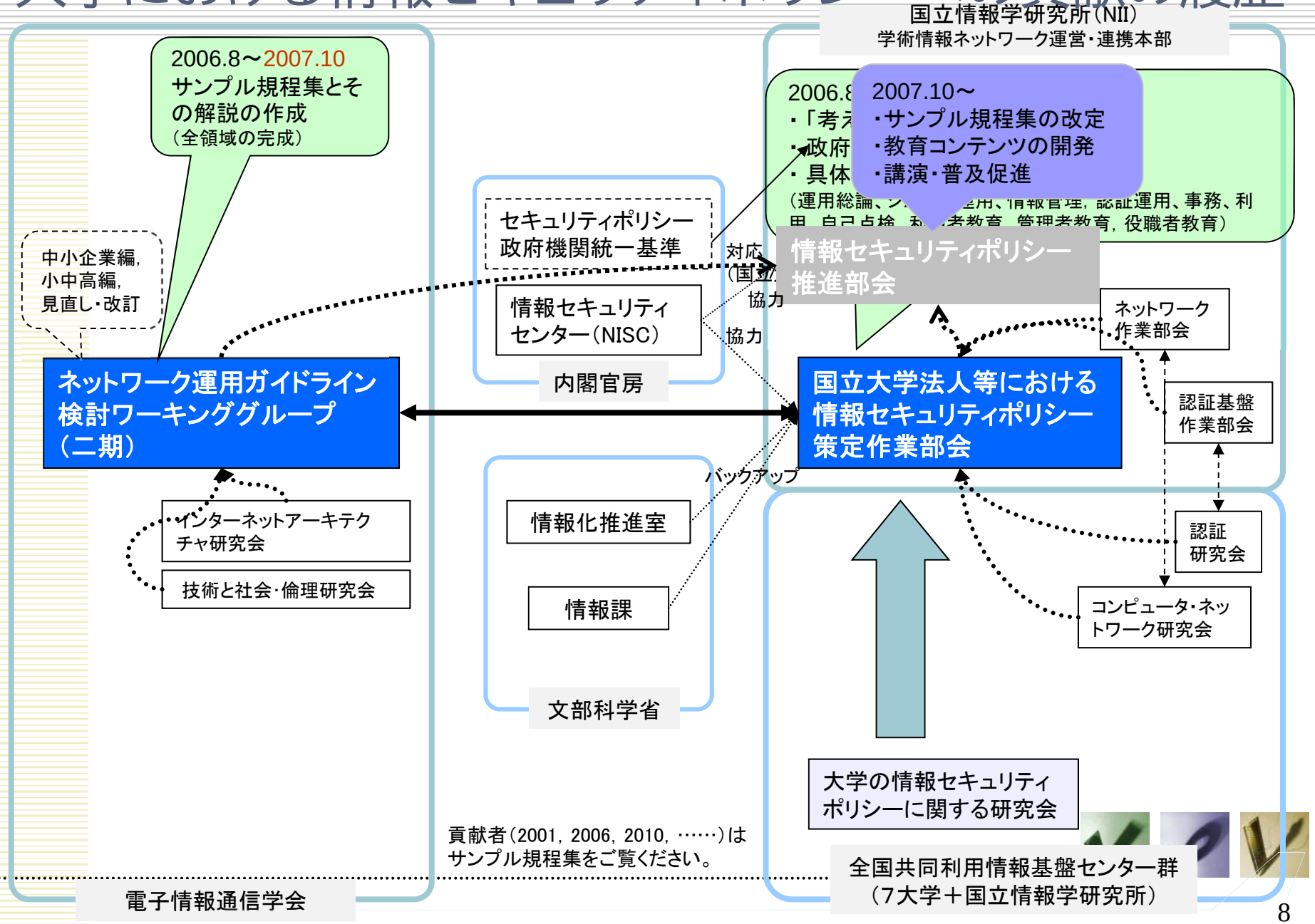
高等教育機関の情報セキュリティ対策のためのサンプル規程集

- **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
    - 2007年10月公開
  - 各高等教育機関でカスタマイズされることを想定
  - 当初、ネットワーク運用ガイドライン(2003)を踏襲
    - 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
  - 政府機関統一基準に準拠して改訂
    - 当初は特に事務情報システム → 徐々に全体へ
    - 高等教育機関による統一基準に準じたサイバーセキュリティ対策の実施を支援

大学における情報セキュリティポリシーへの貢献の履歴



大学における情報セキュリティポリシーへの貢献の履歴



策定したサンプル規程集における前提

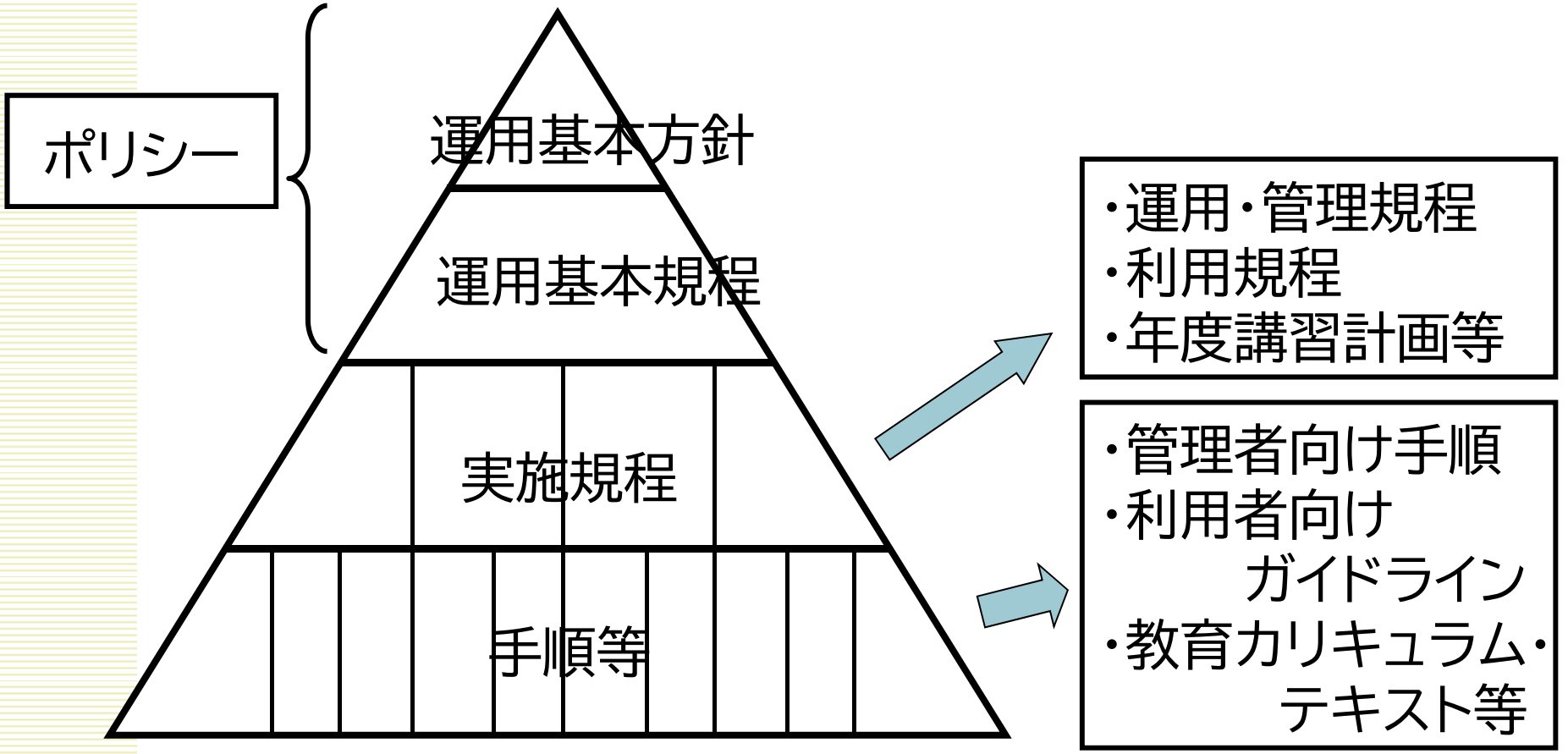
- **モデルとして仮想A大学を想定**
  - 文学部と理学部の2学部で構成され、両学部とも在学生1,000人(1学年250名)ずつ
  - 学内共同利用施設として情報メディアセンター(図書館を含む)がある
  - 学内ネットワーク(事務系ネットワークを除く)や学内共同利用の情報システムは情報メディアセンターの担当
  - 副学長の一人が最高情報責任者(CIO)であり、最高情報セキュリティ責任者(CISO)の役も兼務
  - ！ A大学以外では、組織/規程/文化によりカスタマイズが必要
- **各機関の具体的な参考として策定**
  - 大学の事情に合わせて可能な範囲で政府機関統一基準の考え方に準拠
  - 各大学の事情に合わせてカスタマイズ＋そのための解説

策定したサンプル規程集の領域

（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

- **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



- 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

策定したサンプル規程集の分量(2010)

(計45編, 586p)	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・C系列(2014年度版・2015年補訂)

- 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**など追加
  - 「事務情報セキュリティ対策基準」(新版)
  - 「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)
  - 外部委託の一形態として約款による情報処理サービス, 学外への情報提供
- 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

策定したサンプル規程集の分量(2017年版)

(計35編, 955p)	ポリシー C10xx	実施規程 C2xxx	解説・手順等 C3xxx
総論 x0xx	2編		
運用 x1xx	1編	3編	5編
利用 x2xx		1編	6編
教育 x3xx		1編	4編
監査 x4xx		1編	1編
事務 x5xx		2編	1編
認証 x6xx		5編	2編

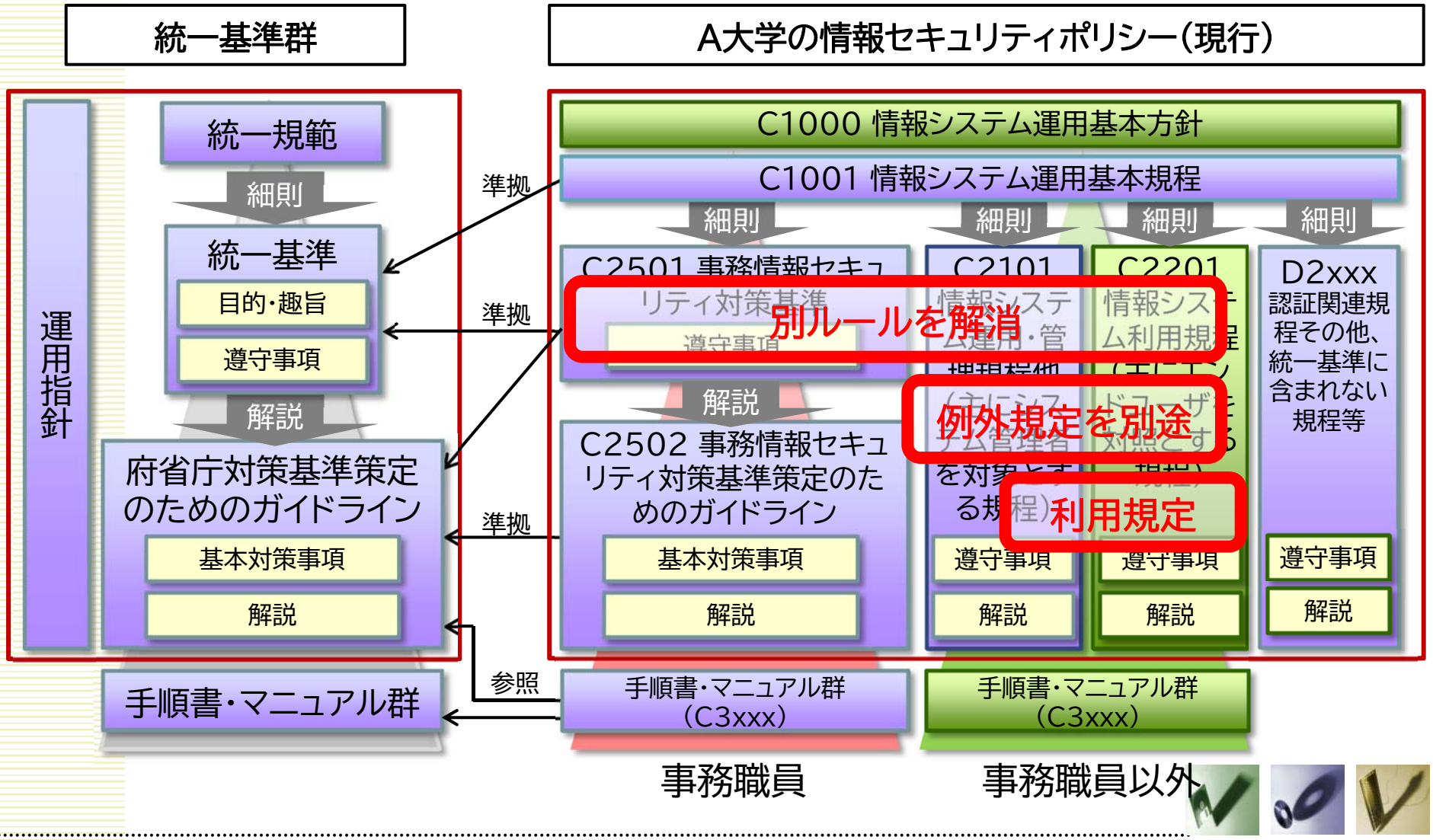
2018～2019年度の活動

- **サンプル規程集(D系列)の更新**
  - 統一基準(平成30年度版)の改訂内容を反映して更新
    - 統一基準の遵守事項への準拠性を高めるため、文書構成を見直し
  - クラウドサービス上で要機密情報を扱う場合について、解説書を作成
    - 将来は，情報システムや学内ネットワークの全外部委託も考えるか
  - 教育テキストガイドラインD330*について、規程や教育の環境変化に対応
  - 活用性(カスタマイズ)を高める方法について、解説等の検討
- **情報セキュリティ教材の整備**
  - 「ヒカリ＆つばさ……」に第18章「セキュリティ演習の課題」を追加
  - D2301(年度講習計画)，D3301(教育テキスト作成ガイドライン(一般利用者向け))の策定・修正の検討
  - 大学での情報の格付けと取扱制限の事例調査から、考え方を検討
  - ヒカつば，倫倫姫を含めたインタラクティブ教材の再構成
- **その他の活動**
  - 関連規程類の調査，講演依頼・NII OF対応，利用者問い合わせへの対応

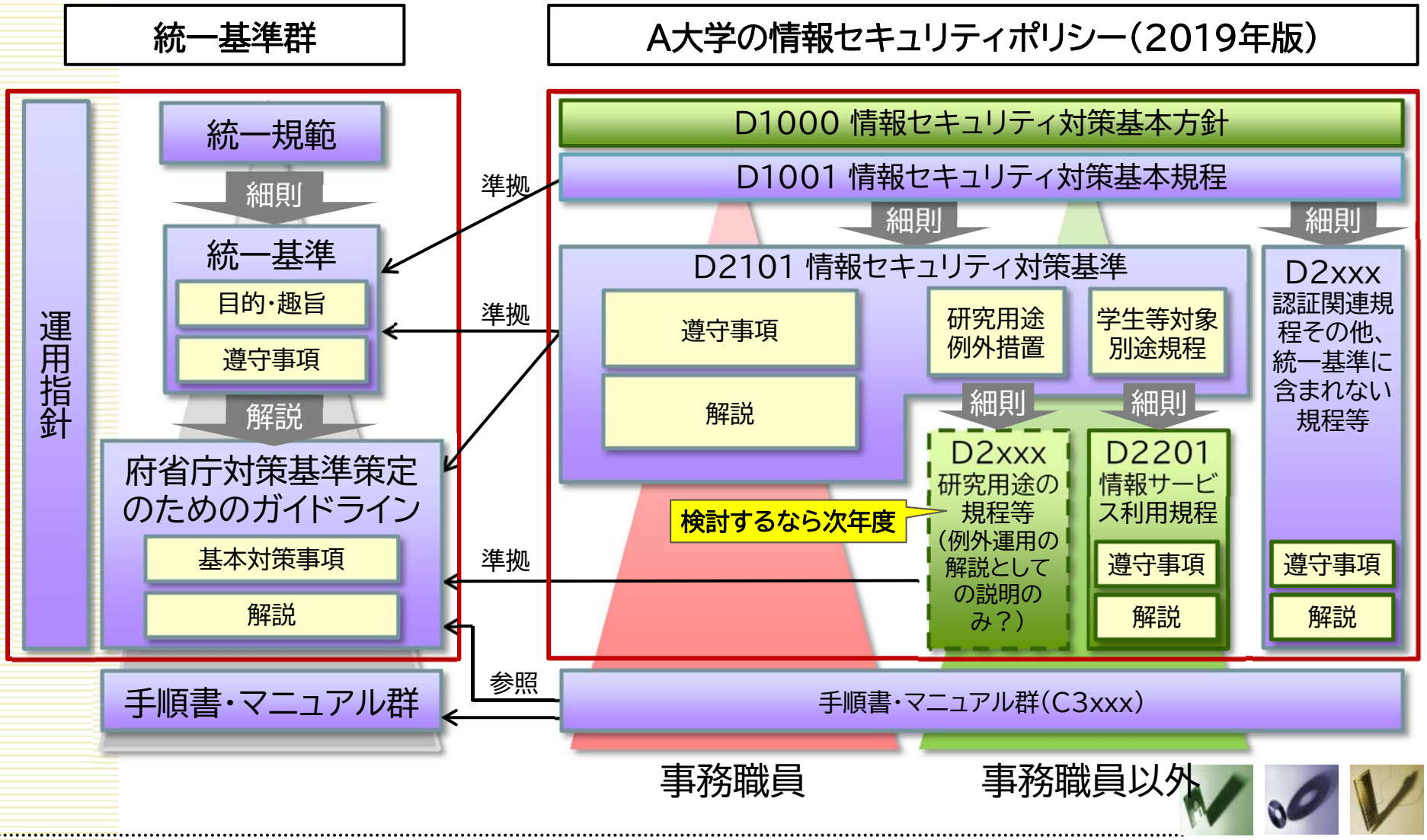
サンプル規程集(D系列)の考え方

- **規程体系を統一基準の考え方に合わせる**
  - 「高等教育機関におけるネットワーク運用ガイドライン」由来の「情報システム運用基本方針」を統一基準ベースに変更(「統一規範」は参照しない)
  - 同一目的の遵守事項が、事務職員向けとそれ以外向けとで別ルールになっているのを極力解消
    - 事務職員向け: 現行サンプル規程集と概ね変更なし
    - 教員向け: 基本的に事務職員向けを適用することを原則とした上で、適用困難な場面について例外規定で対応
    - 学生向け:「お客様」と「スタッフ」との両面性を考慮
- **規程の様式は既存の学内規程様式との整合性を維持**
  - 統一基準の「x.x.x(x)(x)」でなく、「条・項・号」形式を維持
- **規程体系は関係者別でなく、管理対象とする情報の種類別に整備**
- **大学病院は引き続き対象外**
  - 文部科学省管掌以外の規程等が適用される機関は扱わない

現行・C系列の規程体系


統一基準群
A大学の情報セキュリティポリシー（現行）
運用指針
統一規範
細則
統一基準
目的・趣旨
遵守事項
解説
府省庁対策基準策定のためのガイドライン
基本対策事項
解説
準拠
準拠
準拠
参照
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
細則
細則
細則
細則
C2501 事務情報セキュ
リティ対策基準
遵守事項
C2101
情報システム運用・管
C2201
情報システム利用規程
D2xxx
認証関連規程その他、統一基準に含まれない規程等
別ルールを解消
例外規定を別途
利用規定
解説
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
基本対策事項
解説
遵守事項
解説
遵守事項
解説
遵守事項
解説
手順書・マニュアル群
手順書・マニュアル群
（C3xxx）
手順書・マニュアル群
（C3xxx）
事務職員
事務職員以外

D系列(2019～)の規程体系の検討



サンプル規程集の改訂(D系列・検討中)

- D1000(情報セキュリティ対策基本方針)
  - 「情報システム」を対象とすることが前提なので、全面的に修正。
- D1001(情報セキュリティ対策基本規程)
  - 「クラウド」の定義や「情報サービス」に関する文言を追加?
  - 外部からの監査・監視の機能について想定しておく
  - CSIRTとBCPを定義 (C1101 CSIRT設置規程は運用規程へ)
- D2101 (情報セキュリティ対策基準)
- C2102(非常時行動計画に関する規程)
  - セキュリティの範囲外なので, サンプル規程でなく解説に?
- D2201(情報サービス利用規程)
  - 政府機関統一基準に対応するものがないが, 独自に書く
  - インシデント報告など, 利用者の義務はここに書いておく
  - 情報サービスの利用ルールを設けることなど

サンプル規程集(D系列)

- **情報セキュリティポリシーや基本規程を修正**
  - D1000(情報セキュリティ対策基本方針)
  - D1001(情報セキュリティ対策基本規程)
  - D2101 (情報セキュリティ対策基準)
  - 政府機関統一基準への準拠
  - クラウドサービスなどの利用, 外部からの監視などに対応
- **教育テキストガイドラインD330*を改訂**
  - サンプル規程集に準拠したインタラクティブ教材も準備中
- **この夏公表(予定)**
  - おまちください