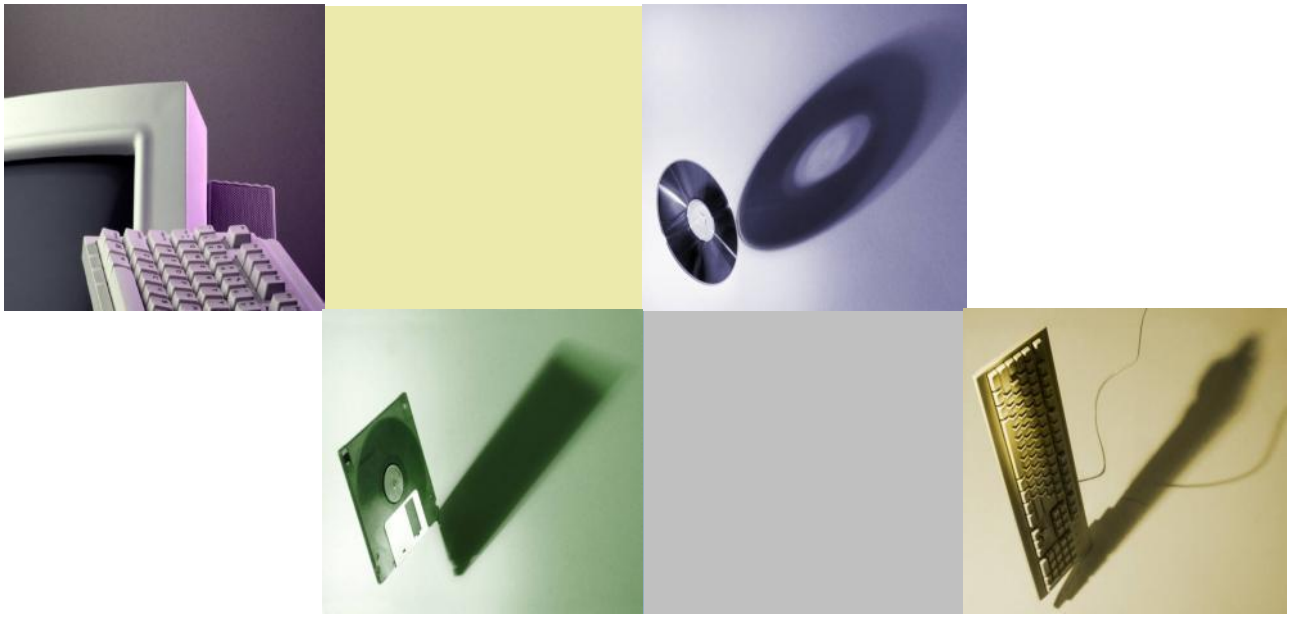
セキュリティポリシー推進部会　からの活動報告

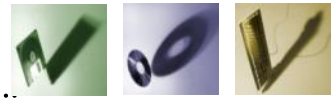


東北大学 情報シナジー機構 特任教授、
情報セキュリティポリシー推進部会 前主査　曽根秀昭
2021.7.8　NIIオープンフォーラム

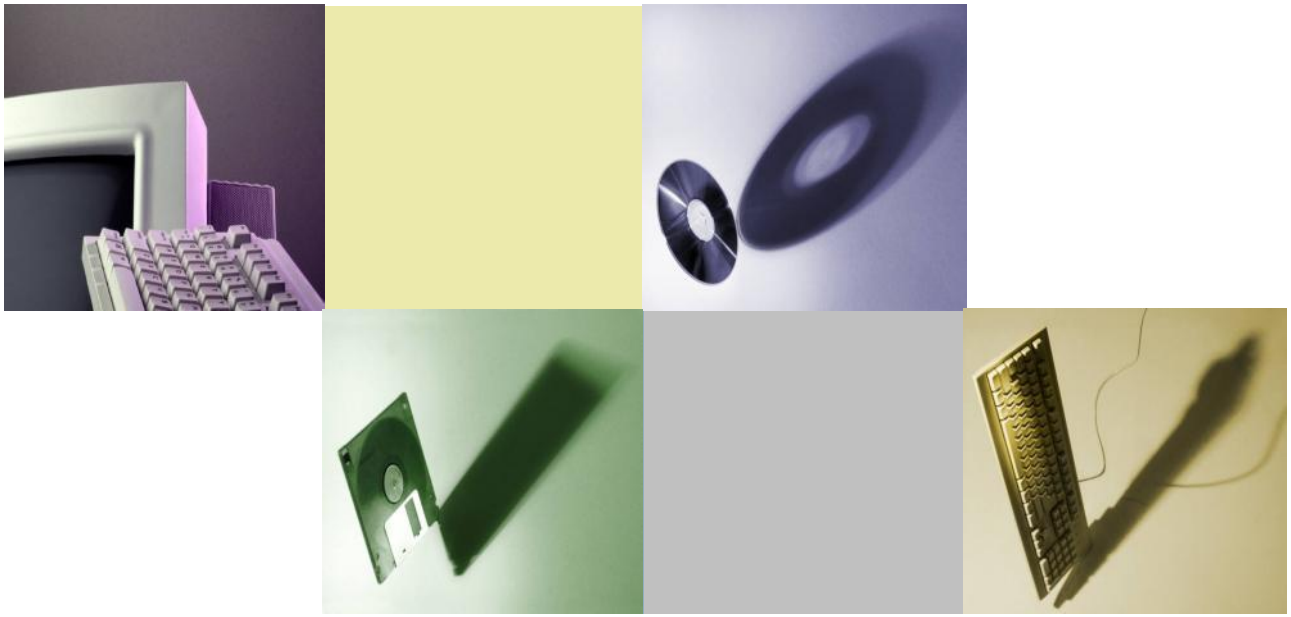
セキュリティポリシー推進部会

- 大学の情報セキュリティポリシーを制定しましょう。←Since 2000
- サンプル規程集を提供し、統一基準に準拠して改訂してます。 ←Since 2007
- サンプル規程集と教材の最新版をリリース。←イマココ

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

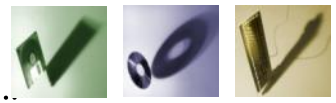


「政府機関等の情報セキュリティ対策のための統一基準群」の改定への対応の振り返り

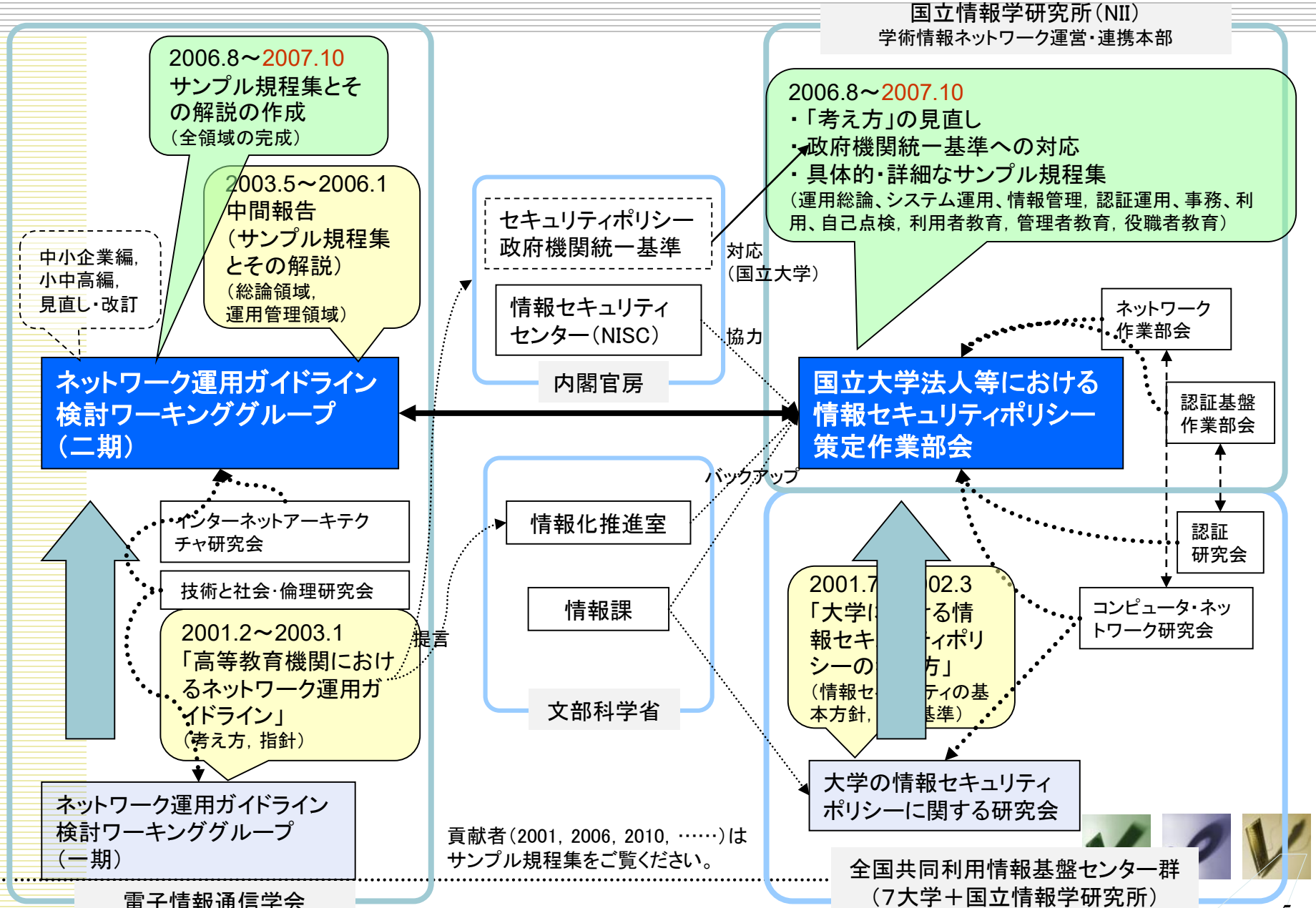


高等教育機関の情報セキュリティ対策のためのサンプル規程集

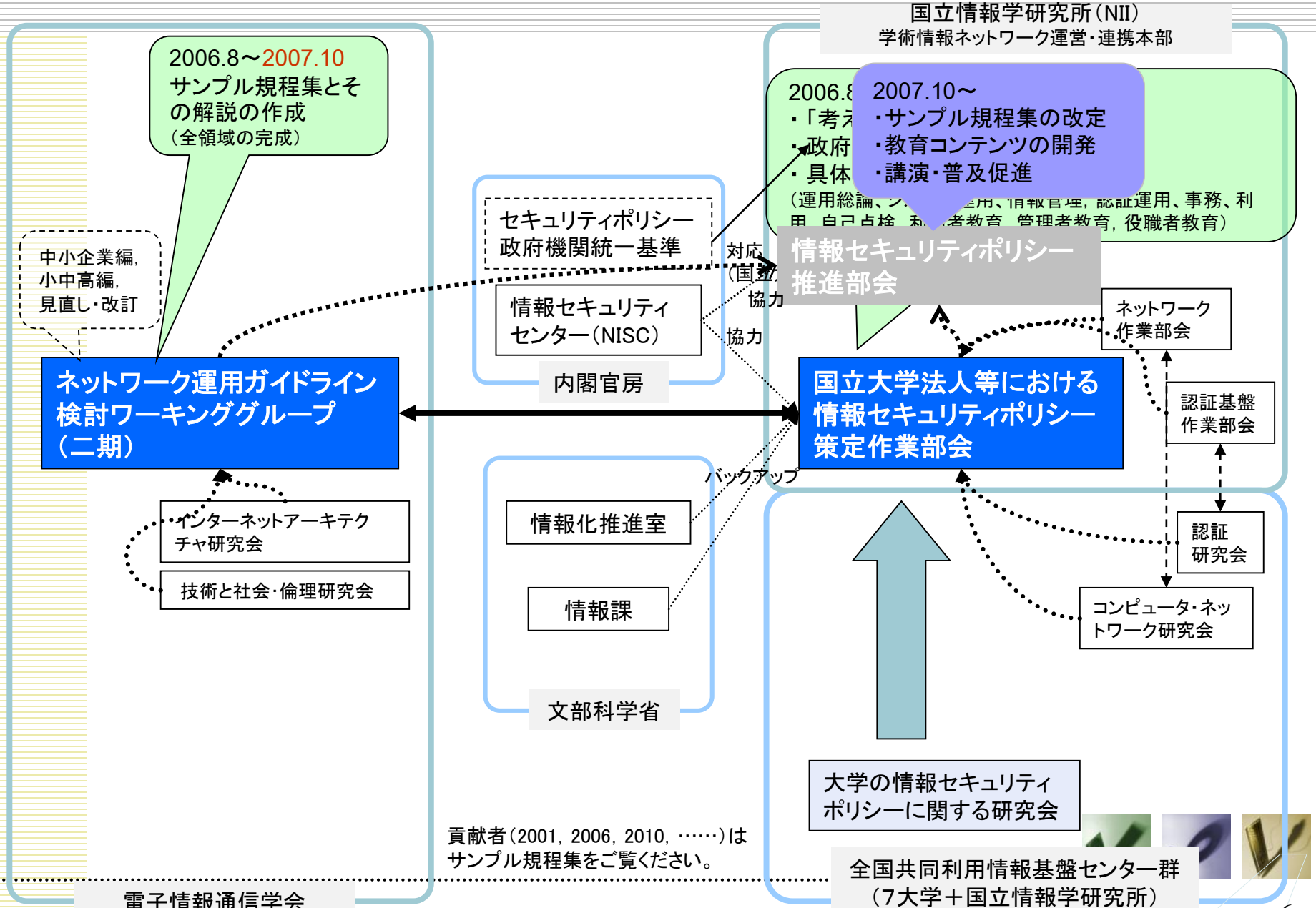
- **概要**
  - 雛型となるセキュリティ関連の学内規程とその解説
    - 仮想のA大学（２学部、学生１０００人程度）
    - 一定の想定状況で必要な規程類をフォロー
  - 標準的かつ活用可能な大学向けのサンプル規程集
    - 2007年10月公開、以後改訂、現在はD系列
    - 各高等教育機関でカスタマイズされることを想定
  - 当初、ネットワーク運用ガイドライン(2003)を踏襲
    - 電子情報通信学会ネットワーク運用ガイドライン検討ワーキンググループ
    - 国立情報学研究所　国立大学法人等における情報セキュリティポリシー策定作業部会
  - 『政府機関等の情報セキュリティ対策のための統一基準群』（以下、「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



統一基準に基づくサンプル規程集の策定までの経緯



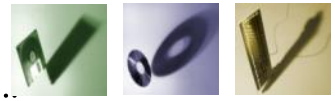
統一基準に基づくサンプル規程集の策定までの経緯



これまでの政府機関統一基準の改定状況

過去16年間で9回の改定を実施し、きのう10回目の改定

公表時期	版名	おもな改定内容
2005年2月	「政府機関の情報セキュリティ対策のための統一基準」(2005年項目限定版)	緊急度の高い対策のための基礎となる基準を中心に策定
2005年12月	「政府機関の情報セキュリティ対策のための統一基準」(全体版初版)	全体を網羅した初版
2007年6月	「政府機関の情報セキュリティ対策のための統一基準」(第2版)	IPv6、暗号モジュール試験及び認証制度等への対応、踏み台対策、情報システム台帳整備等の管理策の強化等
2008年2月	「政府機関の情報セキュリティ対策のための統一基準」(第3版)	DNS、ドメイン名の使用、異常の監視、成りすまし対策に関する管理策の強化等
2009年2月	「政府機関の情報セキュリティ対策のための統一基準」(第4版)	「基本編」と「情報システム編」に分離、最高情報セキュリティアドバイザーの設置義務化、ウェブ閲覧・送信時や電子メール、無線LAN等の管理策の強化等
2011年4月	「政府機関の情報セキュリティ対策のための統一基準群」(平成23年度版)	「技術基準」と「管理基準」に再編、クラウド技術への対応、不正アクセス対応及び教育・人材育成に関する管理策の強化等
2012年4月	「政府機関の情報セキュリティ対策のための統一基準群」(平成24年度版)	上位規定となる「管理規範」を策定、CSIRT体制の整備やIT-BCP策定を求める管理策の強化、強化遵守事項の廃止、モバイル端末の取扱を明確化等
2014年5月	「政府機関の情報セキュリティ対策のための統一基準群」(平成26年度版)	管理基準と技術基準の区分を改め、統一基準本体と「府省庁対策基準策定のためのガイドライン」の関係に見直し、標的型攻撃やサプライチェーンの管理策強化等
2016年8月	「政府機関等の情報セキュリティ対策のための統一基準群」(平成28年度版)	対象を独立行政法人等にも拡大、監査に係る規定整備、情報漏えい事案を踏まえた事案対応策の強化、クラウド対応等
2018年7月	「政府機関等の情報セキュリティ対策のための統一基準群」(平成30年度版)	不正プログラムの検知・実行防止等の管理策を強化、利用者側に立った追加的な対策、自律的なPDCAサイクルの循環促進、多様な業務形態への対応等
2021年7月	「政府機関等の情報セキュリティ対策のための統一基準群」(令和3年度版)	クラウドの利用拡大を見据えた記載の充実、境界型防御を補完する対策の推進、多様な働き方を前提とした管理策の整理等(~~パブコメ終了・近日公表予定~~)



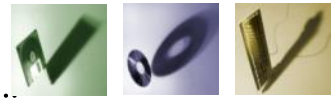
サンプル規程集の改定状況

統一基準公表の2年後より公表開始、14年間で3回の大規模改定（系列の変更）と5回の小改定を経て最新の統一基準(群)に随時対応

	公表時期	版名	おもな改定内容	準拠する統一基準（群）の版
A系列	2007年2月	（版番号なし）	● 策定に時間を要すると見込まれた文書を除いた初版	全体版初版
	2007年10月	2007年度版	● 統一基準の適用個別マニュアル群まで含む形で文書体系を整備	全体版初版
	2011年3月	2010年版	● 2分冊化し、用語集を追加 ● 「情報サービス運用・管理規程」を分離	第3版
B系列	2013年7月	2013年版	● 「管理基準」と「技術基準」に再編 ● 実施規程以上の文書に限定	平成23年度版
C系列	2015年10月	2015年版	● 「府省庁対策基準策定のためのガイドライン」の基本対策事項までを遵守事項として整備	平成26年度版
	2016年2月	2015年版補訂	● 学内認証関連規程の追加	平成26年度版
	2017年10月	2017年版	● CSIRT関連の遵守事項の強化・充実 ● パスワードに関する最新の考え方を反映	平成28年度版
D系列	2020年2月	2019年度版	● 学内の「事務従事者」と「それ以外の構成員」で主要規程を分けていたのを統合	平成30年度版
	2021年5月	2019年度増補版	● 利用者及び役職員向け各種ガイドラインのうち最新動向を踏まえた改定文書を追加	平成30年度版
	2021年度中（予定）	2021年度版（仮称）	● 統一基準（令和3年度版）の改定内容を反映（予定）	令和3年度版

「情報セキュリティの日」功労者表彰（2008年2月）

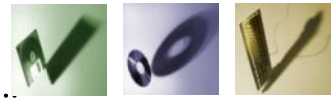
文部科学大臣表彰・科学技術賞（理解増進部門）（2020年2月）



サンプル規程集における各系列の比較

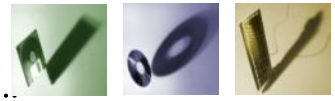
系列の変更は統一基準における大規模改定に対応

	供用期間	各系列の特徴
A系列	2007年～2013年	● 統一基準解説書と、電子情報通信学会ネットワーク運用ガイドライン検討WG成果物をもとに、事務職員向けと、他の学内構成員向けの2種類の規程体系が並立する形で構成される。 ● 統一基準全体版初版と同時期に公表された、「適用個別マニュアル群」のうち、高等教育機関での利用が見込まれる文書について、教育機関向けにカスタマイズしたものを構成に含む。
B系列	2013年～2015年	● 統一基準が「管理基準」と「技術基準」に分離されたのを踏まえ、サンプル規程集の構成文書のうち技術系の文書について、文書番号の十の位が0～4を管理系、5～9を技術系として識別が容易となるように配慮。 ● 当初はA系列と同規模の文書体系として整備する予定であったが、2014年に統一基準の構成が再度大きく変更されたため、主要文書の改定のみにとどまる。
C系列	2015年～2020年	● 統一基準が本体と「府省庁対策基準策定のためのガイドライン」に再編成され、統一基準解説書が廃止されたのを踏まえ、「府省庁対策基準策定のためのガイドライン」の基本対策事項までを遵守事項として再構成。 ● 強化遵守事項を廃止。 ● A系列で策定した「適用個別マニュアル群」に対応する文書のうち、統一基準で保守されていない文書を廃止。
D系列	2020年～	● C系列まで維持されていた、事務職員向けと、他の学内構成員向けの2種類の規程体系について、統一基準の対象が独立行政法人まで拡大され、大学教員等も事務職員相当の管理策を遵守することが適切であることから、事務職員向け体系で一本化し、学生や外部利用者に対する管理策は利用規程と関連ガイドライン等で規定することとする。 ● CISOやCSIRTの位置付けが機関毎に多様であることに配慮。

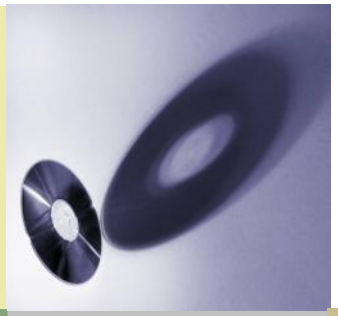


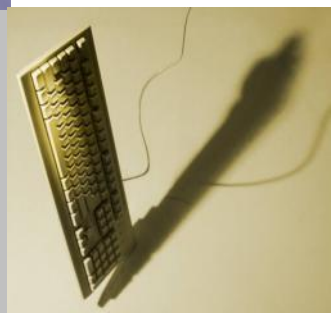
統一基準から何を変えているのか

- 役割名称の置換
  - 「最高情報セキュリティ責任者」→「全学総括責任者」、「情報システムセキュリティ責任者」→「部局技術責任者」等
  - 詳細はサンプル規程集「本文書について」の表1ご参照
- 利用者や利用環境の多様性に配慮
  - 学生、連携機関、外部利用者等の雇用関係にない利用者や、これらの関係者が用いる情報システムを対象とするガイドライン等を別途整備
  - 教員・研究者は当初の版では事務従事者と別扱いを想定していたが、統一基準が独法等を対象に含めたのに合わせ、事務従事者相当の遵守事項に一本化
  - CISO等の役職員向けを含む、多様な関係者に応じたセキュリティ教育の実施に有用な各種コンテンツを用意
  - 部局等の独立性の高い機関における利用も考慮
- 解説の充実
  - そのままでは統制としての効力を有さない遵守事項や、別途規定が必要なメタ規定であることを明記することで、サンプル規程集をもとに自組織の規程類を策定する担当者の負担を軽減



最近のリリースプロダクトの紹介

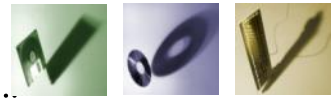





サンプル規程集（D系列）の構成文書一覧

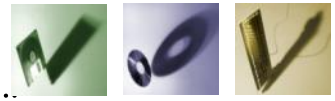
ポリシー（2文書）	実施規程（11文書）	手順・ガイドライン等（19文書）
D1000 情報セキュリティ対策基本方針 D1001 情報セキュリティ対策基本規程	D2101 情報セキュリティ対策基準 D2102 情報格付け基準 D2103 情報セキュリティインシデント対応チーム（CSIRT）設置規程	C3100 情報セキュリティ対策手順の策定に関する解説書 C3101 例外措置手順書 D3102 情報格付け取扱手順 D3103 インシデント対応手順策定に関する解説書 C3104 情報システム運用リスク評価手順 D3106 情報セキュリティ非常時行動計画に関する解説書
	D2201 情報サービス利用規程※	C3200 情報システム利用者向け文書の策定に関する解説書 D3251 情報機器取扱ガイドライン D3252 電子メール、メッセージング利用ガイドライン D3253 ウェブブラウザ利用ガイドライン D3254 情報発信ガイドライン D3255 認証情報管理ガイドライン
	D2301 年度講習計画	C3300 教育テキストの策定に関する解説書 D3301 教育テキスト作成ガイドライン(一般利用者向け) C3302 教育テキスト作成ガイドライン(システム管理者向け) D3303 役職員向け説明資料作成ガイドライン
	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
	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 C2651 証明書ポリシー(*) C2652 認証実施規程(*)	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

Dではじまる文書が2019年度増補版として公表済みの文書（※＝今後公表予定）
青字は、技術系の規程・手順書（より現場に近いレベルでの策定・運用を可能とするもの）
(*) 外部文書の参照のみ



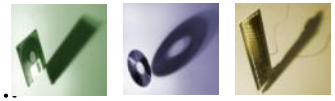
2019年度版増補におけるおもな改定内容

文書番号	文書名	改定内容
D1001	情報セキュリティ対策基本規程	● 他文書との整合のための調整 ● CISOとCSIRT関連の解説を実態を踏まえたものに修正
D2102	情報格付け基準	● 解説を微修正
D2103	情報セキュリティインシデント対応チーム運用規程	● 他規程と重複する内容を削除し、統一基準のみでは不足する内容のみで構成
D3101	例外措置手順書	● eduroam対応 ● その他微修正
D3102	情報格付け取扱手順	● 安全保障貿易管理の考慮等を追記
D3103	インシデント対応手順策定に関する解説書	● 他の関連ガイドライン等との整合を鑑み、解説書としての扱いに変更
D3106	情報セキュリティ非常時行動計画に関する解説書	● CSIRT関連の整合性を確保
D3253	ウェブブラウザ利用ガイドライン	● 現状にあわせて全面改定
D3254	情報発信ガイドライン	● 法改正（著作権法35条、51条など）を踏まえ、最新の内容を反映
D3301	教育テキスト作成ガイドライン（一般利用者向け）	● 著作権法改正等、最新の内容を反映 ● 犯罪統計を新しいものに更新
D3303	役職者向け説明資料作成ガイドライン	● 文書名変更（教育テキスト作成ガイドライン（CIO/役職者向け）より） ● 最新の内容を反映



統一基準（令和３年度版）/ サンプル規程集2021年度版におけるおもな改定内容（予定）

- クラウドサービスの利用拡大を見据えた記載の充実
  - クラウドサービスの利用者側として実施すべき対策や考え方に関する記載の追加
  - 政府情報システムのためのセキュリティ評価制度（ISMAP）を踏まえた記載の追加
  - 約款による外部サービスに係る考え方の再整理
- 情報セキュリティ対策の動向を踏まえた記載の充実
  - 情報セキュリティインシデント事例を踏まえた記載の追加
  - 従来からの境界型防御を補完するものとして、「常時アクセス判断・許可アーキテクチャ」の参照等、最新の考え方等の反映
- 多様な働き方を前提とした情報セキュリティ対策の整理
  - 急速に広まったテレワークや遠隔会議の経験も踏まえ、多様な働き方を前提とする場合に必要な情報セキュリティ対策について、参照すべき統一基準上の規定や解説を整理



大学の情報セキュリティ・情報倫理教育のための教材

- 「ヒカリ＆つばさの情報セキュリティ３択教室」
  - Flash動画15話＋解説本（2009）→改訂増補版：18話（2018）
  - Flash動画の公開を終了しました（2020）＋解説本PDFのみ提供
  - https://www.nii.ac.jp/service/sp/
- 「倫倫姫と学ぼう！情報倫理」
  - 2013～2022．3．31廃止予定
- 「倫倫姫の情報セキュリティ教室」
  - 前2件を合流し、「学認LMS」コンテンツとして提供開始（2020、2021改訂）
  - 日英中韓　4言語対応
  - – 電子メールを使ってみよう
  - – 取り扱い注意！ IDとパスワード
  - – 著作権はとても重要
  - + 電子メール，SMSによる詐欺に注意!
  - + 無線LANを安全に使おう
  - + 情報機器の持ち歩きに注意
  - 総合テスト
  - 教材に対する意見・コメント
  - https://lms.nii.ac.jp/auth/shibboleth/login.php