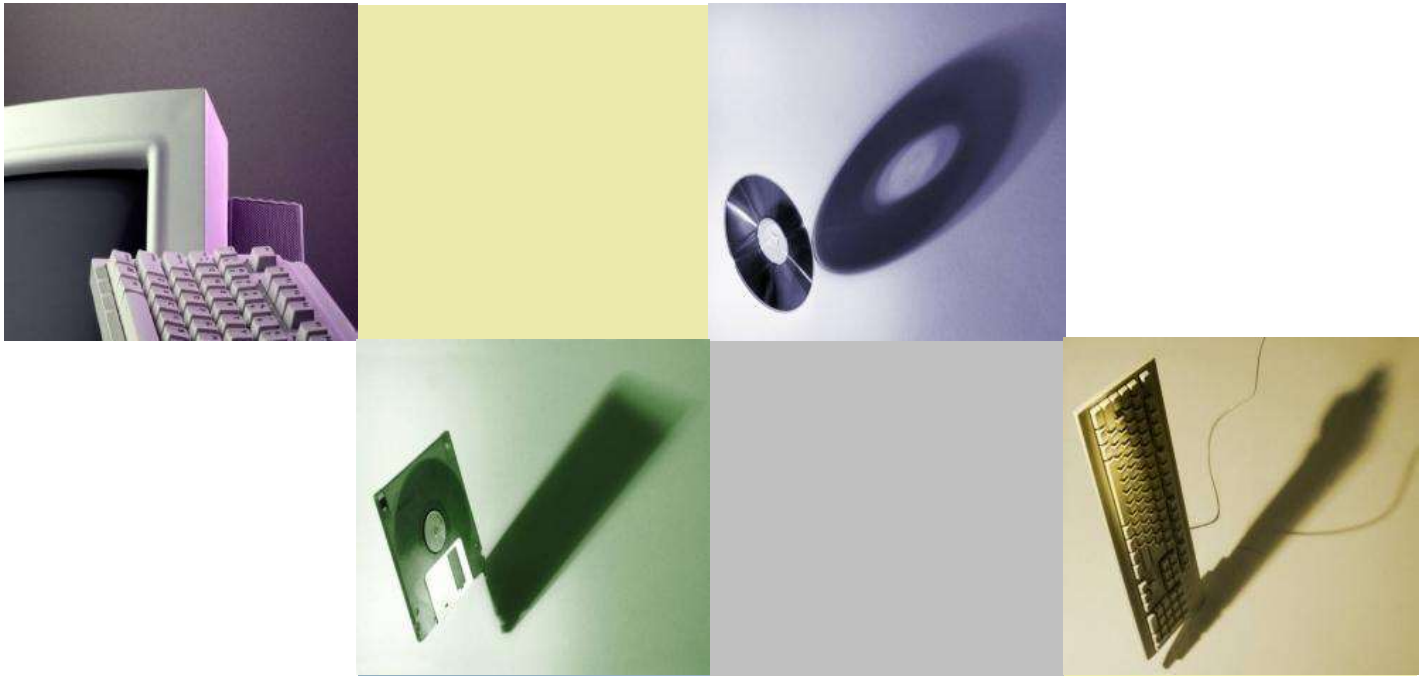
情報セキュリティポリシー推進委員会の活動概要



高等教育機関におけ情報セキュリティポリシー推進委員会 主査
中村素典（京都大学 情報環境機構）
2023.5.31　NIIオープンフォーラム2023

情報セキュリティポリシー推進委員会

本委員会の主な活動

- **「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」の提供**
  - 現在の最新は2022年度版（2023/3/17公開）

- **高等教育機関における情報セキュリティ教育のための教材の学認LMSによる提供**
  - 「倫倫姫の情報セキュリティ教室」

https://www.nii.ac.jp/service/sp/

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

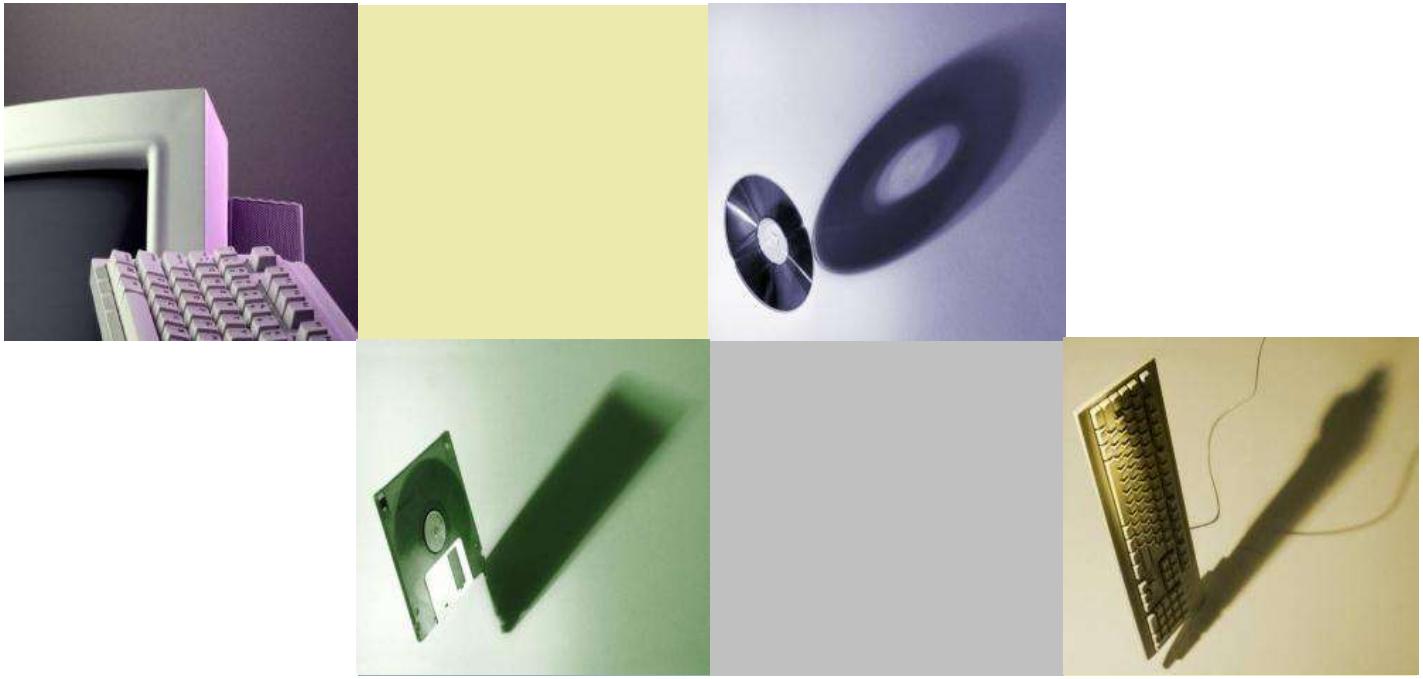
- **概要**
  - 雛型となるセキュリティ関連の学内規程とその解説
    - 仮想のA大学（２学部、学生１０００人程度）
    - 一定の想定状況で必要な規程類をフォロー
  - 標準的かつ活用可能な大学向けのサンプル規程集
    - 2007年10月公開、以後改訂、現在はD系列が中心
    - 各高等教育機関でカスタマイズされることを想定
  - 当初、ネットワーク運用ガイドライン(2003)を踏襲
    - 電子情報通信学会ネットワーク運用ガイドライン検討ワーキンググループ
    - 国立情報学研究所　国立大学法人等における情報セキュリティポリシー策定作業部会
  - 『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

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動画の公開終了（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公開終了
- 「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）
  - 全8話
    - 2022年3月に「安全にネットサーフィンを」を追加
    - 今後も随時追加予定
  - 日英中韓　4言語対応
  - 総合テストの提供
  - https://www.nii.ac.jp/service/rinrinhime/
  - https://lms.nii.ac.jp/



高等教育機関の情報セキュリティ対策のための サンプル規程集のアップデートと大学での活用に向けて



高等教育機関におけ情報セキュリティポリシー推進委員会 主査
中村素典（京都大学 情報環境機構）
2023.5.31　NIIオープンフォーラム2023

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系列が中心
    - 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

（参考）これまでの政府機関統一基準の改定状況

過去18年間で10回の改定を実施

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

(参考)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、16年間で3回の大規模改定（系列の変更）と6回の小改定を経て最新の統一基準に随時対応

	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
	2023年3月	2022年度版	● 統一基準（令和3年度版）の改定内容を反映	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）

(参考)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を参照

■ 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

(参考)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年度増補版以降に公表済みの文書　（Cではじまる文書は2017年版を参照）
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
◆＝2020年度改定文書 ●＝2022年改定文書

（参考）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2022年度版における主な改定内容

■ 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

サンプル規程集活用時の検討例

- ガバナンスの階層構造（責任体制）の整理
- 情報セキュリティ監査と業務監査
- 調達仕様書とサプライチェーンリスク
- アカウント発行と管理の責任体制
- 格付けの対象とする情報
- 個人情報保護

ガバナンスの階層構造（責任体制）の整理1/3

- **本サンプル規程は、CISO（最高情報セキュリティ責任者 / 全学統括責任者）の下での体制を定めているが、CIO（最高情報責任者）との関係も含めて検討する必要がある。**
  - 一般的に、CIOとCISOは利益相反の関係（利便性と安全性）だが、協力が不可欠
    - 同一人物で良いのか？
    - 部局では、部局長が部局のCIO兼CISO？部局技術責任者？
  - CIOの下でのICT戦略はどのように定めるのか？
    - サンプル規程の範疇外
  - アカウント発行やシステム利用規約などには、誰にシステムを利用させたいか（誰に利用する権利があるのか）、どのように利用させたいか、というCIOの立場から定めるべきポリシーも多く含まれる。

ガバナンスの階層構造（責任体制）の整理2/3

- **副CISO（全学統括副責任者）を置くかどうか**
  - CISOや全学実施責任者との役割分担は？
  - CISOが任命権者で良いのか？
- **情報セキュリティアドバイザーを置くかどうか**
  - 副CISOや全学実施責任者との役割分担は？
- **全学実施責任者**
  - CISOの役割の一部を担うとすると、部局総括責任者の中から選出するのは利益相反の可能性もある？（守る側と守らせる側）
  - CISOが任命権者で良いのか？

ガバナンスの階層構造（責任体制）の整理3/3

- **部局技術責任者（情報システムセキュリティ責任者）**
  - 部局に複数のシステムがある場合、システムごとに部局技術責任者を置くのか、部局総括責任者（部局長）を補佐する者として1人置くのか。
  - 技術面のみを補佐するのか、部局CISOとして補佐するのか。
  - 部局内に適当な人材がいない場合、部局総括責任者が兼任せず、
  - 部局外（学外）の者を充てても良いのか。
  - 部局技術担当者との役割分担はどうするのか。部局技術担当者の設置単位はどうするのか。
    - システムごとだとすると、PC 1台ごとに部局技術担当者を置くのか？（資産管理上の担当者？）
- **職場・区域情報セキュリティ責任者**
  - どのような単位で設置するのか。（人や建物と情報資産の関係）
  - 部局総括責任者や部局技術担当者との役割分担はどうするのか。
  - 部局内に設置された多数の「責任者」の統括はどうするのか。

情報セキュリティ監査と業務監査

- **情報セキュリティ監査責任者**
  - 監査の独立性を考えると学長が任命し、学長に報告すべき？
- **情報セキュリティ監査**
  - 情報資産に対するリスク評価・対策に関するPDCAの確認
  - NIST CSF: 特定、防御、検知、対応、復旧の5カテゴリ評価
- **業務監査の観点**
  - CISOが委員会に諮るべきものや、CISOの命により全学実施責任者や情報セキュリティ監査責任者が行うべき情報セキュリティ対策に関する意思決定手続きの証跡を残しているか？
    - 「全学情報セキュリティ委員会の審議を経て」
    - 監査実施計画の策定、監査実施体制の整備、監査の実施指示及び監査結果の全学総括責任者への報告

    など

サプライチェーンリスク

- **「サイバーセキュリティ対策等基本計画」（2019～）にも盛り込むこととされた**

  - リスクを軽減するための要求要件を調達仕様書に記載する等の対策が求められる

    - 仕様書記載事項のひな型の作成と学内周知
      - 業務の再委託に関する事項
      - 情報セキュリティを確保するための体制および環境の整備
        - 一貫した業務体制、不正の防止・検出体制
      - 情報資産の適正な管理
      - サイバーセキュリティ対策
      - 情報セキュリティが侵害された場合の対処
      - 情報セキュリティ監査の実施
      - 情報セキュリティ対策の改善（PDCA）

調達仕様書における情報セキュリティ対策

- **「本学が別途定める情報セキュリティポリシーを遵守すること」等と書いていないか？**
  - 一般に、「情報セキュリティポリシー」は組織に所属する職員等に求めている事項である。
  - 受注業者に 「情報セキュリティポリシー」をそのまま見せたとしても、 「情報セキュリティポリシー」は組織外の者に対して直接責任を課すものとはなっていない。
  - 職員等は「情報セキュリティポリシー」に基づいて、受注業者に提供する情報の取り扱い方法や、納入・構築させるシステムの情報セキュリティ対策等について、調達仕様書、契約書、その他で具体的に指示をする必要がある。

アカウント発行と管理の責任体制

- **アカウントは誰の責任で発行し、誰の責任で利用者を監督し、誰の責任で処罰（利用停止等）するのか。**
  - アカウントは教育・研究・業務に不可欠なものとなってきているため、情報メディアセンターだけでは対応できない場合がある。（CIOが定めるICT戦略に基づくべき？）
  - インシデント発生時の緊急対応については、情報メディアセンターに権限を与えておく必要があるが、それ以外の場合は、教育・研究・業務に責任を持つ者も含めた体制を構築しておくことが重要と思われる。
  - 学務DBや人事DBを学内で入手し、情報メディアセンターの裁量でアカウントを発行する時代ではなくなりつつある。
    - システム上で扱われる情報資産は部局が責任を持つべきもの
    - 情報メディアセンターが全ての利用者を監督することは不可能
- **情報システム（アカウント）利用規程**
  - 分かりやすく整理（ICT戦略（権利）の観点や教育的配慮の観点も含め）

対象とする情報

- ✓ 当該情報システムから出力された書面に記載された情報

及び

- ✓ 書面から情報システムに入力された情報

を含む。

- どこまで厳密に適用するのか。

- 対象となる情報は、格付け等、情報セキュリティポリシーに基づいた運用が求められる。

個人情報保護

- **取扱いの観点**
  - 組織内利用か第三者提供か
  - 利用目的についての事前同意
- **入学時、入職時にどこまで同意を得ているか**
- **個人情報の取り扱いについて厳守させられるか**
  - 特に学生に対する強制力は怪しい（第三者提供の可能性）

- **原則は「オプトイン」（事前に同意を得る）**
  - 特にグループウェアでは、名前や連絡先の一覧が取得可能
  - 入学時、入職時に同意が得られていないのであれば、グループウェア利用開始前に改めで同意を得る必要があると思われる。

令和3年改正個人情報保護法は令和５年４月１日全面施行

情報セキュリティ講習「テスト問題」問題

- 「サイバーセキュリティ対策基本計画」の中で「情報セキュリティ教育」の実施が求められている。
- 「倫倫姫の情報セキュリティ教室」の総合テストもあるけれど、教職員向けにもなる多様で全般的な設問を用意したい。
- 毎年同じ設問を実施するのは意味がないが、自分の大学で毎年異なる問題を作成して、検証するのは大変。
- 業者に外注しても、いまいち品質が良くない。

- 大学間で問題プールを共有できると嬉しいですか？
  - もちろん、ギブ＆テークの精神で！

おわりに

- サンプル規程やその関連事項についてのご意見
- 情報セキュリティ教育のための教材についてのご意見
- 情報セキュリティ教育のテスト問題についてのご意見
- 一緒に活動いただける方（いろんな疑問、コメント、アドバイス等を頂ける方）も募集中