大学における情報セキュリティの取組み
～大学の情報セキュリティポリシー～

2018. 8. 31

東北大学　サイバーサイエンスセンター／
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
曽根秀昭

情報セキュリティ対策

(2005)

セキュリティへの脅威

- 種類
  - 不正アクセス攻撃
  - ウィルス，わな
  - 通信妨害（傍受，改変）
- 対策・取組み
  - 防犯，秘密保持，監視
  - 何を何から守るか
  - どのように守るか
  - どのくらいまで守るか
  - 設備整備＋運用＝効果
    - ポリシー，ルール，テキスト

不正アクセス対策

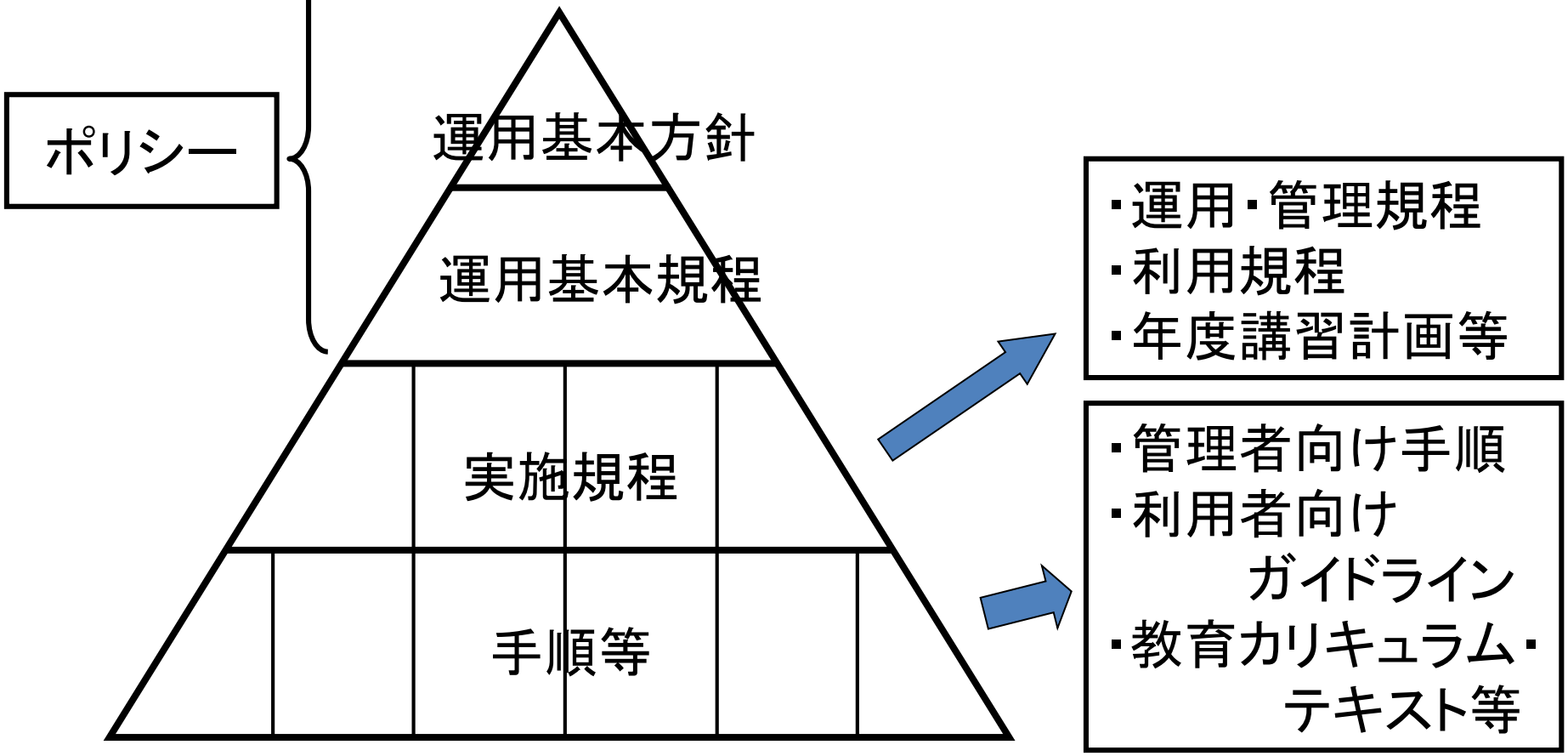
- アクセス制限の強化
  - ファイアウォール
  - パスワードの徹底
- セキュリティ対策
  - セキュリティホール，Update
  - セキュリティ管理
  - 暗号化通信
  - 不正アクセス検知
- 日常管理
  - トラブルの切り分け，対応
- 安全意識と正しい知識
- コンテンツの問題

コンテンツの問題

- 言論の自由の原則
- 他者危害の原則
- 他者の人格の尊重
- 法令，規程，規則の遵守
  - 知的財産権の侵害
    - （発明，考案，意匠，著作）
  - わいせつ罪，など
  - 違法行為の助長，誤認される行為
  - 目的外利用
  - 技術規程の遵守
- →利用の問題，情報安全・倫理の啓発

大学の情報セキュリティポリシー

サンプル規程集のポリシー･実施規程･手順等の体系



- 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

大学で扱う情報

【構成員】

•役員，　各種の職員，　教員，　派遣職員，　受託業者，　各種の研究員

•学生　←構成員なのか・顧客なのか（TA・RAは？）

【活動との関連】

•教育（学生へ）：　教務情報（履修，成績），教材・講義，eラーニング

•研究（学生とともに）：　研究情報（論文原稿，データ，技術・設備），発表論文

•運営：　経営（人事，財務，……），広報，

•（医療）

【情報セキュリティへの要請】

•情報システムの全体のセキュリティ（可用性・機密性・完全性）の維持・向上

•機密情報（入試・試験，未発表論文・特許技術，経営情報）

•社会や関係先へ対する責任

•個人情報保護，安全保障貿易管理（、医事）からの要請との関連

•（コンピュータソフトウェアの適正な管理）

•研究組織・研究者について，学問の自由との両立

•教育機関として，学生に対する情報セキュリティ教育

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

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

運用と管理に関する規則

- 情報システム運用規程
- 運用全般の根拠
  - 運用の組織： 役職の設定，権限の所在，指示系統
    - 下位規程で管理や利用等の規則を定める
- 情報システム管理規程
  - 管理に携わる者の遵守事項・項目別対策事項
- 情報の格付け
  - 機密性、可用性、完全性の観点から格付け
- 非常時行動計画
  - インシデント発生時の対応（非常時の組織）

利用に関する規則

- 情報システム利用規程
  - 情報システムの利用者の遵守事項
    - 利用にあたっての禁止事項、遵守事項
      - アカウント、情報機器の利用、メール、ウェブ、情報発信
- 情報機器取扱要領
  - PCやUSBメモリ等の利用時の遵守事項、注意事項
- メール利用要領
  - メールを利用するときの遵守事項、注意事項
      - HTMLメールの原則禁止、目的外使用の禁止、ToとCc等
- 情報発信要領
  - SNS等を利用するときの遵守事項、注意事項

クラウドサービスの導入と
セキュリティ関連規則

サンプル規程集におけるクラウド対応

政府機関統一基準の対応に準拠

解説の追加

- 管理基準
  - 外部委託に外部設備を利用したサービスが含まれる
  - 外部設備を利用する場合にデータの所在に留意
  - IT部門を通さずにITに相当する外部委託発注を想定
- 技術基準
  - 通信回線の用語定義に仮想ネットワークを想定
  - サーバの共用を想定

- クラウド対応として新たな規則の作成はなし

学外へ出せる情報と出せない情報

- 情報の格付けから考える
- 学外に出せる（かもしれない）情報と情報システム
  - 学外からアクセスできる情報やシステム
    - ホームページのコンテンツとサーバ
    - 安否確認システム
    - 図書館システム
- 情報を本学情報システムに置く理由
    - 学外だとどこにあるかわからない不安
    - 学外だと情報にアクセスするまでに経由する機器数が増える
    - （データの保存場所に制約のある）学外との研究に関する情報
    - 機微な情報（人事情報，入試問題，学生の属性）

本学情報システムと約款による情報処理サービスの違い

- （サンプル規程集が対象とする）本学情報システム
  - 情報処理及び情報ネットワークに係わるシステム
    （本学情報ネットワークに接続する機器を含む）
    - 本学により、所有または管理されているもの
    - 本学との**契約**あるいは他の協定に従って提供されるもの
- 約款による情報処理サービス
  - 情報セキュリティ以外の契約内容については要求に基づいて用意される又は条件選択や修正ができる
  - 情報セキュリティに関する事項に条件選択の制限

外部委託における情報セキュリティ対策実施手順

- 必要な情報セキュリティ水準の確保（委託元としての責任者）
  - 可否の判断
    - 重要な情報を取り扱う情報処理業務は原則禁止
  - 調達：委託先の選定基準
    - 委託する情報処理業務に対する安定性
    - 求める情報セキュリティ対策等を遵守
      - その範囲を定め，対策を調達仕様として周知
      - 侵害時の対処，履行状況の確認
  - 契約
    - 実施させる情報セキュリティ対策の明示＋確認書
  - 実施中
    - 取り扱う情報の秘密保持等
    - 情報セキュリティ対策の履行状況の確認
  - 納品・検収

「約款による情報処理サービス」の利用に際しての注意事項

- 処理された結果生じる著作権等の権利の放棄や移管が利用条件となっている場合
- 約款上データ消去等をサービス利用者側で直接実施できない場合
- 利用したデータの削除についてサービス 提供者が個別には応じないことや、情報の置き場所が特定の場所に固定されず、海外の法執行機関等による予期せぬアクセスが行われる場合
- 留意事項（運用・管理）と，確認事項（C, I, A）
- 無償で利用を開始できる場合であっても、外部委託に該当する場合がある
  - 無償のメールサービス，アンケートサイト，オンラインストレージ

ソーシャルメディアによる情報発信

ソーシャルメディアの公式利用

- 公式広報，情報発信、研究成果公開，社会連携の効果
  - 迅速な情報発信 （ただし利用者限定もある）
  - 詳細なウェブサイトや紙媒体への補完としての併用
- 公式広報と，それ以外の情報発信の区別
  - 公式プレスリリースと，「中の人」（個人的意見を含む）
- 公式の広報・情報発信の注意点
  - ネットワークサービスのユーザとしての利用
  - 文書など従来の広報との使い分け（あるいは置き換え）
  - 組織としてのアカウント運用ポリシーの表明（公式，返信）
  - 情報の貧富，情報弱者への配慮

情報拡散の特性への配慮(1・2/4)
話題の選び方・閲覧者の想定

- 意図しないコミュニケーションが生じるおそれ。
- 話題の選び方、表現に注意する。
  - 公開メディアでは多くの人に見られることを意識
- 悪気のない投稿内容が他人を不快にしてしまう場合がある。
  - さまざまな地域、立場、文化的背景、価値観の読者
  - 他人への中傷をしない・誹謗にも注意

- 多様な閲覧者を想定して投稿する。
- 公開になる投稿は、想定外の閲覧者の目にも触れる。
  - 内輪のつもりの投稿も、公開・再掲載の可能
  - 想定外の他人に閲覧され，誤解・批判される可能性

情報拡散の特性への配慮（3・4/4）匿名性は不確実・投稿の削除が困難

- 匿名にしていても、個人がわかることがある。
  - 後から閲覧者・投稿者がわかる可能性
    - 他の投稿やプロフィールを分析して特定
  - 実名・所属・住所などが暴露される可能性
- 個人を特定される可能性を想定しておく。
  - 実名がわかっても困らないように注意して行動
  - 想定外で実名が公開になることも想定

- 不用意な投稿を後で削除しても、ネット上から消えないことがある。
  - 連携サービスへの転送先では消えない可能性
  - 再掲載、アーカイブ、まとめに蓄積・保存されている可能性
- 将来まで責任をもてるかを考えて発言する。

情報発信・交流における留意点

- 相手を尊重し、不快にさせない
  - 過度な言い争い、反対意見主張、感情的発言
  - 友達以外への「友達申請」で当惑？
- 著作権・商標権
  - 著作物・商標の引用・転載に、許諾が必要
- 写真撮影時の肖像権
  - 撮影場所・対象について許可を得て撮影し掲載

トラブル発生時の対応

- 掲載内容による炎上（コンテンツインシデント）:
  - 想定外の批判、苦情、誹謗中傷の集中
  - 掲載内容が違法／不快／非常識； それぞれの対応
  - 公式／私的： それぞれの対応
    - 私的トラブルの場合に、所属先としての責任は？
    - 普段から安全とマナーの注意喚起は必要
- 公的アカウントの成りすまし（不正アクセス）
  - アカウント（パスワード）再設定
  - 掲載内容の一時閉鎖など