ICTフォーラム2018

SS研 学術情報機関のための サイバーセキュリティ・ガバナンスWG 報告

東京工業大学 学術国際情報センター
北口 善明

August 31, 2018

学術研究機関のためのサイバーセキュリティ・ガバナンスWG

東京工業大学 Tokyo Institute of Technology

- 活動方針
  - 多様化、悪質化が進むサイバーセキュリティの脅威に対し、学術研究機関単独でのセキュリティ対策は限界となりつつある。今後は各機関が情報やリソースを融通し合いながらオールジャパンで対策を行う、横連携を考慮した体制作り、制度作りを進める必要がある。国立情報学研究所においても作業部会を立ち上げ、検討を進めるという動きがある。
    本WGでは、この作業部会での検討状況を睨みつつ、この取組みをより実効性の高いものとすることを目的とする。具体的には、各機関で実行すべきこと、実行できることを中心に議論し、各機関における体制や環境の整備に関する意見交換等を通して提言の取りまとめを行いたい。
- 活動期間
  - 2016年4月～2018年3月

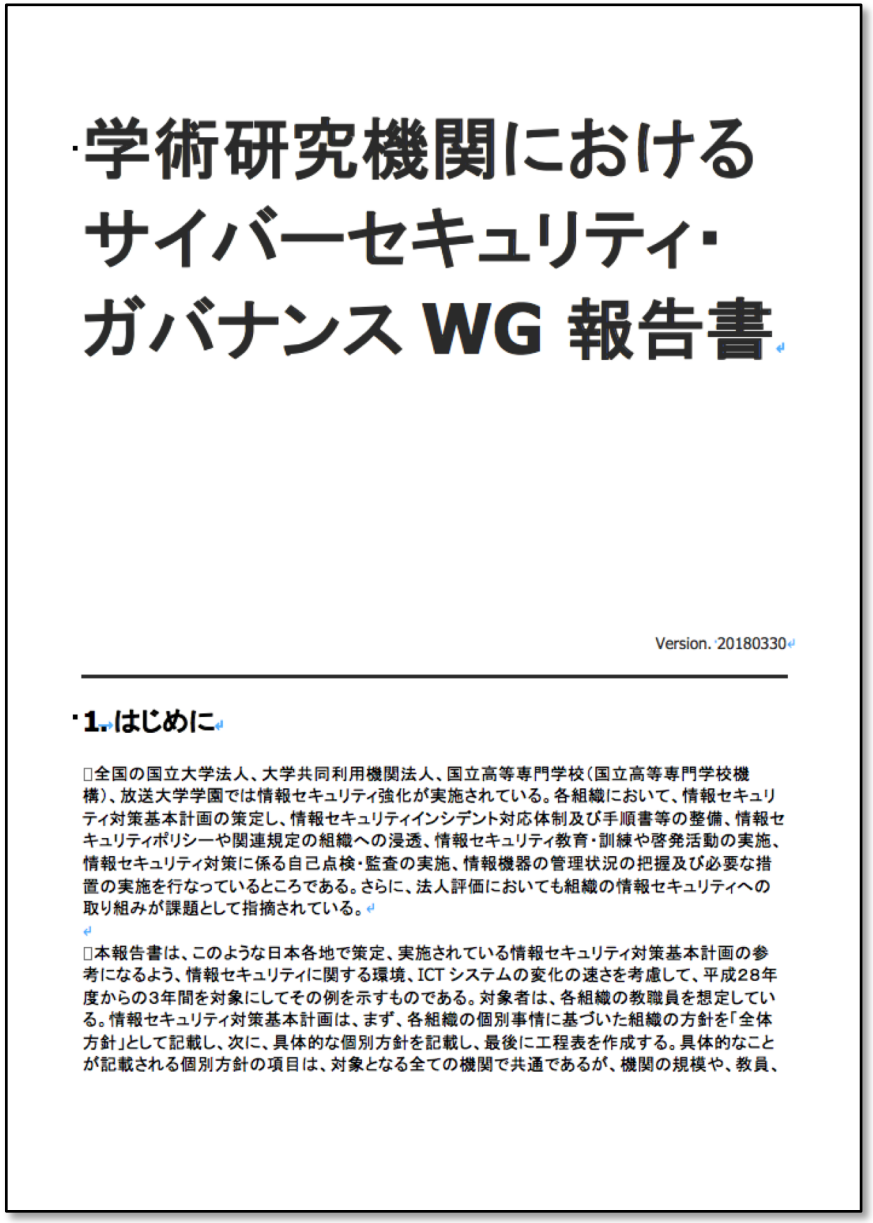
学術研究機関のためのサイバーセキュリティ・ガバナンスWG

東京工業大学 Tokyo Institute of Technology

- ワーキンググループ推進委員（五十音順）
  - 担当幹事
    西村 浩二（広島大）
  - まとめ役
    北口 善明（東京工業大）、武蔵 泰雄（熊本大）
  - WGメンバー
    井上 俊治（富士通）、岡村 耕二（九州大）、齋藤 彰一（名古屋工業大）、下園 幸一（鹿児島大）、園田 哲平（富士通）、只木 進一（佐賀大）、長谷川 明生（中京大）、山下 眞一郎（富士通）
  - オブザーバー
    高倉 弘喜（国立情報学研究所）
  - 事務局
    甲斐 友一朗（富士通）、西 一成（富士通）、松本 孝之（富士通）

成果物としての報告書

- 目的
  - 典型的な学術研究機関(大学)を例題として情報セキュリティ対策基本計画策定の参考情報となる資料の提示
    - 共通項の提示による策定工数低減
    - 平成28年度からの三年間程度を対象
- 検討項目
  - 情報セキュリティインシデント対応体制及び手順書等の整備
  - 情報セキュリティポリシーや関連規定の組織への浸透
  - 情報セキュリティ教育・訓練や啓発活動の実施
  - 情報セキュリティ対策に係る自己点検・監査の実施
  - 情報機器の管理状況の把握及び必要な措置



学術研究機関における
サイバーセキュリティ・
ガバナンス WG 報告書

Version. 20180330

1. はじめに

□全国の国立大学法人、大学共同利用機関法人、国立高等専門学校（国立高等専門学校機構）、放送大学学園では情報セキュリティ強化が実施されている。各組織において、情報セキュリティ対策基本計画の策定し、情報セキュリティインシデント対応体制及び手順書等の整備、情報セキュリティポリシーや関連規定の組織への浸透、情報セキュリティ教育・訓練や啓発活動の実施、情報セキュリティ対策に係る自己点検・監査の実施、情報機器の管理状況の把握及び必要な措置の実施を行なっているところである。さらに、法人評価においても組織の情報セキュリティへの取り組みが課題として指摘されている。

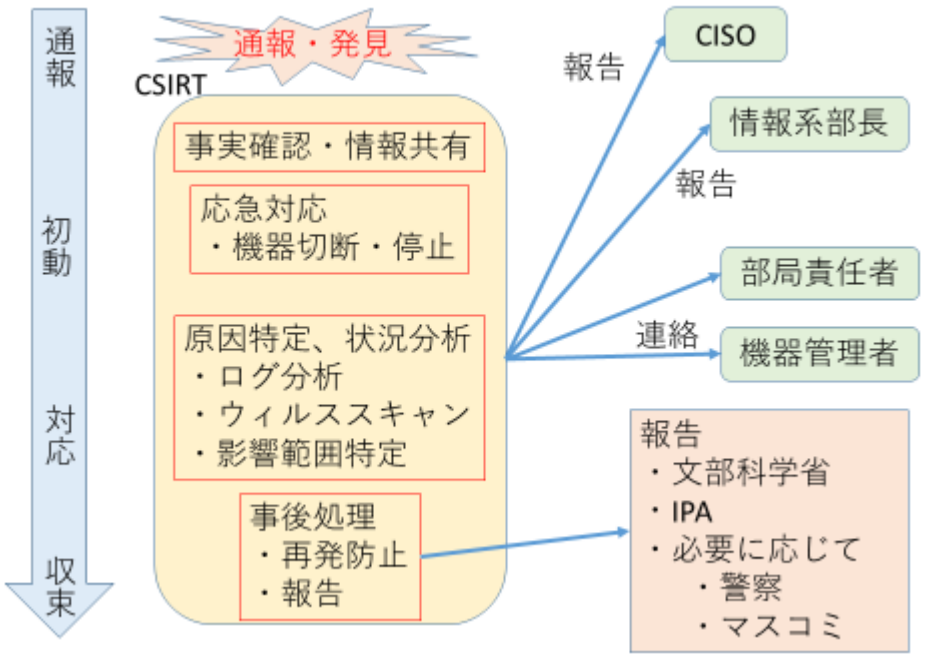
□本報告書は、このような日本各地で策定、実施されている情報セキュリティ対策基本計画の参考になるよう、情報セキュリティに関する環境、ICT システムの変化の速さを考慮して、平成28年度からの3年間を対象にしてその例を示すものである。対象者は、各組織の教職員を想定している。情報セキュリティ対策基本計画は、まず、各組織の個別事情に基づいた組織の方針を「全体方針」として記載し、次に、具体的な個別方針を記載し、最後に工程表を作成する。具体的なことが記載される個別方針の項目は、対象となる全ての機関で共通であるが、機関の規模や、教員、

情報セキュリティインシデント対応体制

東京工業大学 Tokyo Institute of Technology

- 高等教育機関におけるCSIRT
  - 人員・予算の制約上理想的なCSIRTは困難
  - どの程度まで実施できることが理想か検討
- 国立大学法人におけるCSIRTの任務
  - インシデント発生時の受付窓口
    - 電話番号やメールの公表・周知が必要
  - インシデントの重大性判定と発生源の特定
    - 被害拡大の防止（切断・停止）を第一に取り組む
  - 外部セキュリティ組織との連携
    - 高度なフォレンジックなどは外部の支援を利用
  - 重大性に応じて大学本部や外部へ報告
    - CISOや学長との非公式チャンネル形成が肝要

※セキュリティ対策の不備における責任を負う組織ではないという認識が必要

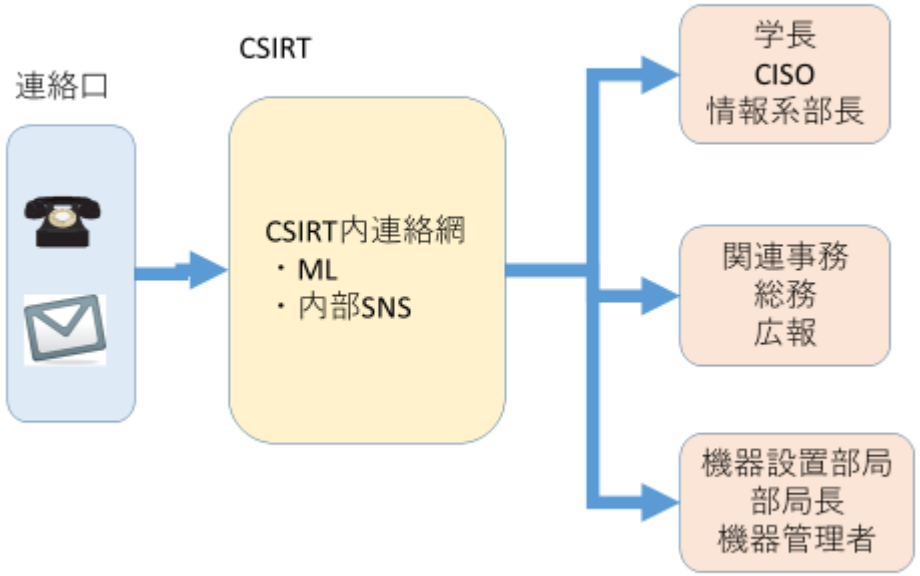


インシデント対応の処理手順例

情報セキュリティインシデント対応体制

東京工業大学 Tokyo Institute of Technology

- CSIRTの体制
  - 新たに人員を確保することは困難
  - 情報系センターだけでなく現場担当も組み込むことが肝要
    - 複数のキャンパスからなる場合は特に
  - 報告・通報・会見などの対応に事務局との窓口整備が必要
  - 組織的に学長や担当理事直下に配置
    - ある程度の強い権限が必要
- CSIRT体制維持のために
  - 閉じたSNS/グループウェアでの情報共有
  - 情報システムの管理者/担当者情報の収集



情報セキュリティインシデント対応体制

- CSIRTの制約と対策
  - 24時間365日対応することは事実上不可能
  - 勤務時間外のインシデント対応を少人数で稚拙に対応しない

  → 勤務時間外の対応手順・発動要件の定義が必須
  重大事案発生時に外部専門家を活用できる予算を確保
  事務職員や技術職員で初動対応できる準備も必要

  - 大学間連携による相互支援
- 対応手順の整備
  - インシデント対応のレベル設定が必要
    - 定期的にまとめて報告：迷惑メールや遮断できている攻撃　など
    - 簡単な報告を後日実施：PCのマルウェア感染や攻撃で被害が発生しなかった場合　など
    - 迅速な対応と外部報告の検討：機微情報の漏えいや外部に対する攻撃の検知　など

情報セキュリティ教育・訓練・啓蒙活動

- 情報セキュリティ向上のために
  - 構成員のセキュリティに対する意識向上が鍵
    - 構成員：学生、一般教職員、部局管理スタッフ、CSIRTスタッフ、CISO/役職者
- 学生への教育
  - 目的：マルウェアの被害者や意に反した加害者になることを防止
  - 時期：入学時に実施しアカウント発行条件にするなど
- 一般教職員への教育・訓練
  - 法令遵守の徹底やセキュリティポリシー・運用規則の理解が必要
    - 学生への教育内容に加え個人情報の取り扱いなどの情報取り扱い規定の理解が重要
    - 採用時および年一回程度のセミナーやe-Learning形式の教育
  - インシデント発生時の対応訓練による意識向上
    - インシデント発生の報告が遅れないよう不必要にペナルティを与えないことが重要

情報セキュリティ教育・訓練・啓蒙活動

- 部局管理スタッフに求められること
  - 大学として守るべき情報資産の理解
  - インシデント発生時の対応手順の理解とその実施能力
  - 部局が利用する大学システム・ネットワーク構成の理解
  - 部局内システム構成の理解
  - インシデント発生時にCSIRTと連携した対応が必要
    - インシデント対応の初期手順の整備
    - 訓練により対応手順やシステム停止の判断、CSIRTへの連絡方法を確認
  - 通常時のセキュリティ啓蒙活動が重要
    - システム管理者としての管理研修、インシデント対応訓練
    - 担当者交代における引き継ぎ不足防止に向けた各システムの設定状況確認
    - OSやアプリケーションの更新などの管理

情報セキュリティ教育・訓練・啓蒙活動

東京工業大学 Tokyo Institute of Technology

- CSIRTスタッフの心構え
  - 大学の情報資産とリスクマネジメント、関連法例の理解
  - インシデント発生時の対応方法の理解と実践能力の維持
  - 訓練により維持が必要なこと
    - 部局管理スタッフからのインシデント発生報告への対応能力
    - インシデント発生機器の停止・隔離の判断能力
    - CISO等への報告業務を円滑に行う能力
  - CSIRT訓練のためのツールやサービス例
    - TrendMicro インシデント対応ボードゲーム
    - 富士通セキュリティソリューションインシデント対応訓練サービス
- CISOや役職者の教育
  - 情報セキュリティの必要性（人・コスト）や学外への影響の理解を求める
  - インシデント発生時におけるリスクマネジメントの理解を求める
    - 優先事項や対外広報の方針決定が求められる

監査および自己点検

- 目的
  - 策定したセキュリティ確保の基準や規定の適切な運用の維持
  - 各種規定の準拠性・実効性・妥当性を定期的に確認し改善
- 監査の体制
  - 監査責任者
    - CISOにより任命され以下の役割を担う
      - 監査を行う監査実施者・監査チームの編成
      - 監査計画の策定
      - 監査結果報告書の作成とCISOへの報告
    - CISOとは独立させる考え方や既設の法人監査部門て対応する方法もある
  - 監査チーム
    - 監査責任者により任命された監査を実施する者（被監査者とは必ず別人物）
    - 倫理観や監査についての知識や技術が求められる
    - 外部の専門業者を含む体制も

監査および自己点検

- 監査計画
  - 監査は年1回以上行わないと実効性に問題
  - 監査対象が膨大となる場合、中・長期的な監査計画も必要
  - 監査対象に必ず含める事項
    - 前回の監査で指摘（不備・違反）があった箇所
    - 組織等の改変があった箇所
    - 規定が改定または追加された箇所
  - 監査計画策定において明確にする事項
    - 監査方針、監査の目的、監査対象、監査スケジュール、監査基準、監査業務の体制
  - 監査の指摘基準例
    - 重大な違反：単独又は他の違反と複合することで重大なリスク発生の可能性があるもの
    - 軽微な違反：重大な違反以外の違反
    - 改善の機会：違反ではないが改善の対応が望ましいもの

監査および自己点検

- 監査の実施
  - 監査調書を必ず作成し一定期間保存
    - 監査調書：判断の元となった監査証拠を明確にする
  - 違反等があった場合、指摘事項等報告書にて指摘事項をまとめる
    - 指摘事項の内容は被監査側の同意が必須
  - 全数調査が困難な場合はサンプリング調査
    - 機器の実態調査（脆弱性確認）などにツールを利用する方法も
- 監査の報告と対応
  - 監査責任者は監査報告書を作成しCISO/学長に報告
  - 監査報告書の指摘事項に対して改善を指示（CISO）
  - 被監査部門における対策例
    - 対応が困難なものにはリスク軽減対策と対応目標を提示
    - 教育や訓練で解決すべき事項には教育訓練の計画を提示

監査および自己点検

- 監査体制の整備
  - 監査体制がない場合には早急な整備が必要
  - 特定の人員に監査が集中しないよう監査可能な人員の教育が必要
  - 人員不足に対して
    - 外部機関への委託
    - 大学間での相互監査
- 自己点検
  - 構成員が自らの役割に応じて対策事項を実施できるか確認
  - 自己点検結果を踏まえ改善策を実施
  - 自己点検の流れ
    - CISOが年度自己点検計画を策定
    - 部局総括責任者が構成員毎に自己点検票や自己点検の実施手順を整備
    - 年2回以上実施し、部局総括責任者が分析・評価し、CISOに報告
    - CISOは報告を受け改善を指示

まとめ

- 学術研究機関向けの情報セキュリティ対策基本計画
  - 策定時の参考資料として報告書にまとめた
  - ICTシステムの変化が著しいため2,3年程度しか有効でないと想定
  - 組織毎に違いはあるが共通項を整理することで策定工数を低減
- 報告書内容
  - 大学におけるCSIRTの体制構築と維持
  - 構成員に対する情報セキュリティ教育・訓練・啓蒙活動
  - 監査や自己点検による実行性の維持と改善
  - 機器やIPアドレス管理に対する技術的手法の整理