北海道大学

セキュリティ対策におけるCISOの役割

国立情報学研究所　学術情報基盤オープンフォーラム2023
セキュリティトラック

北海道大学
情報基盤センター　サイバーセキュリティ研究部門 /
情報環境推進本部　情報セキュリティ対策室長（副CISO）

南　弘征（みなみ　ひろゆき）/ min@iic.hokudai.ac.jp

（おことわり）

- 本発表ならびにスライドの内容は、
  発表者個人の意見、見解、経験等に基づく私見、
  もしくは話題提供としてデフォルメした仮想例であり、
  所属組織・関与団体等との関連は一切ございません。

- 従って、本発表内容に係る、
  過度に具体なお問い合わせには対応致しかねる旨、
  ご理解を賜りたく、冒頭でお願い申し上げます。

- （NII-SOCSとしての、参加機関との意見交換は、
  別途実施予定です。）

（本日の仮想聴講者層）

- 高等教育機関・研究機関のCISOクラス
  - （いてほしいが、概してご多忙で少数と推察）
- 同　現場を預からさせられている職員・教員の方々
- 同　事務的補佐をしなければならない職員の方々
- 同　上記以外の機関構成員の方々

- これら機関にアプローチしたい関連企業等の方々

- その他一般

CISOに求められるらしい役割（私見）

下記各項　＋　バランス感覚

- 組織経営面での役割
  - インシデント・情報漏洩に係るリスクの認識と評価
  - セキュリティ対策に関する｛人、技術｝的コストの認識と評価
- 組織運営面での役割
  - 技術的リソースの確保・維持・性能向上
  - 対外（組織外）的対応
  - 組織内でのセキュリティレベル維持・向上、意識啓発
  - （丸投げの忌避）
- 司令塔としての役割
  - 任務、業務に係る正しい認識
  - セキュリティ技術、関連法令等に係る正しい認識
  - 社会情勢に係る正しい認識

高等教育機関・研究機関におけるCISOとは？（私見）

（前スライド以外の留意点）

- 不統一なIT環境との折り合い
  - 利用目的、必須使用環境、他機関との折り合い
- 「学問の自由」との折り合い
  - 利用者視点での「過剰な」制限との折り合い
- 「レガシー」との折り合い
  - インターネット黎明期からの運用との折り合い
  - 過去の歴史的経緯との折り合い

（極端なCISOの仮想例）

- 外部機関からの情報提供に対する針小棒大な反応
  - 組織防衛としてもマイナスに触れる場合あり
- 自身による全対応
  - 組織規模によってやむなき場合も
  - コントロール機能は必要
- 「Not My Business」丸投げ
  - 組織規模によってやむなき場合も
  - 技術に長じることは必須ではない

あらためて望みたいCISO理想像（私見）

- 提供リソースに関する「正しい」理解
  - 例：
    NII-SOCSは無作為抽出・情報提供サービス
  - 「〇〇さえ入れておけば安心」は常に不成立
  - 「使用上の注意をよく読み、正しくお使い下さい」
  - 「仏作って魂入れず」とならぬよう
    - サンプル規程集は
      自組織に応じたカスタマイズ必須
      - （CISOに関する記載　ほとんどなし）

あらためて望みたいCISO理想像（私見）

- 自組織保有リソースに関する「正しい」理解
  - 特有事情も認識した人的資源の育成は
    超高コスト
  - 単なる上意下達でなく、相互理解・認識が必須
  - 適時適確な認識と指示が肝要
    - 「事件は現場で起こっている」
  - 最終的責任の再認識
    - "The buck stops here."
  - 現有資源の最大限活用
    - 隣の芝生はよく見えがち
    - （不幸な内容でも）経験で得られるものあり

あらためて望みたいCISO理想像（私見）

- 根気強い 組織内「啓発」の実践
  - 「暖簾に腕押し」と思っていても継続的に
  - 事案発生時の責任に関連
  - 実践のためのリソース確保、支援

- 「悲観的備え」と「楽観的対応」

※関連企業のみなさまへ（私見）

- セールス先の概況を
  的確にご認識頂いた上でご提案を
- （できれば協働を）

（参考資料など ＋ 私見）

- 経済産業省
  「サイバーセキュリティ経営ガイドラインと支援ツール」
  https://www.meti.go.jp/policy/netsecurity/mng_guide.html
  ※（高等教育機関・研究機関へ直截に適用しにくい内容あり）

- 各種研修など
  - 可能な限り、指定された参加者属性の方が参加すべき
    （代理では実感が伴いにくい）