【大学情報セキュリティ研究講習会】

大学における CIO/CISO の役割について

2018年 8月24日

JPCERT/CC
早期警戒グループ　洞田 慎一

目次

- 自己紹介
- 「CIO/CISO」に対する考え方
- インシデント対応に見る
  「CIO/CISO」と「CSIRT」の役割
- 【参考】大学等に求められる対策
- まとめ

自己紹介

自己紹介

- 洞田 慎一
  - 2006-2015年 総合研究大学院大学葉山情報ネットワークセンター
  - 2015年~ JPCERT コーディネーションセンター

- 外部委員等
  - 2016年 金融情報センター コンティジェンシープラン改訂に関する検討部会
  - 2017年 金融情報センター IT人材育成検討部会
  - 2017年 私立大学情報教育協会 情報セキュリティ対策問題小委員会
  - 2018年 日本学術振興会 契約等監視委員会
  - 2018年 国立大学法人 総合研究大学院大学 情報セキュリティアドバイザー

- 講演
  - 金融ISAC 名古屋ワークショップ 基調講演 “Open Source Intelligence のススメ”, 2018.
  - 民間放送連盟・放送セプター情報セキュリティ対策に関する説明会, “2017年度の放送におけるインシデントの振り返り”, 2018.
- 論文
  - S. Abe, Y. Tanaka, Y. Uchida, S. Horata, "Developing Deception Network System with Traceback Honeypot in ICS Network", SICE Journal of Control, Measurement, and System Integration, 2018.
  - 高等教育機関に対するサイバー攻撃の動向と情報セキュリティ対策の考え方, 大学と教育, 2018年3月号.

JPCERT/CCの活動全体像

世界各国144組織との連携
27か国の組織とMoU締結

研修やイベントでの講演等を通じて、CSIRTの構築・運用支援を実施

高度なマルウェアの解析

重要インフラ／制御システムのセキュリティ対策支援を2007年から実施

年間約4千件の脆弱性案件を調整し公表へ

年間1万件以上のインシデント情報に対応

アジア各国間連携によるインターネット観測網

重要インフラ事業者との情報共有（ISAC）等への活動支援

セプターカウンシル（13インフラ分野）

政府機関、専門機関、重要インフラ、各種メーカー等との連絡・連携

JPCERT/CCの活用

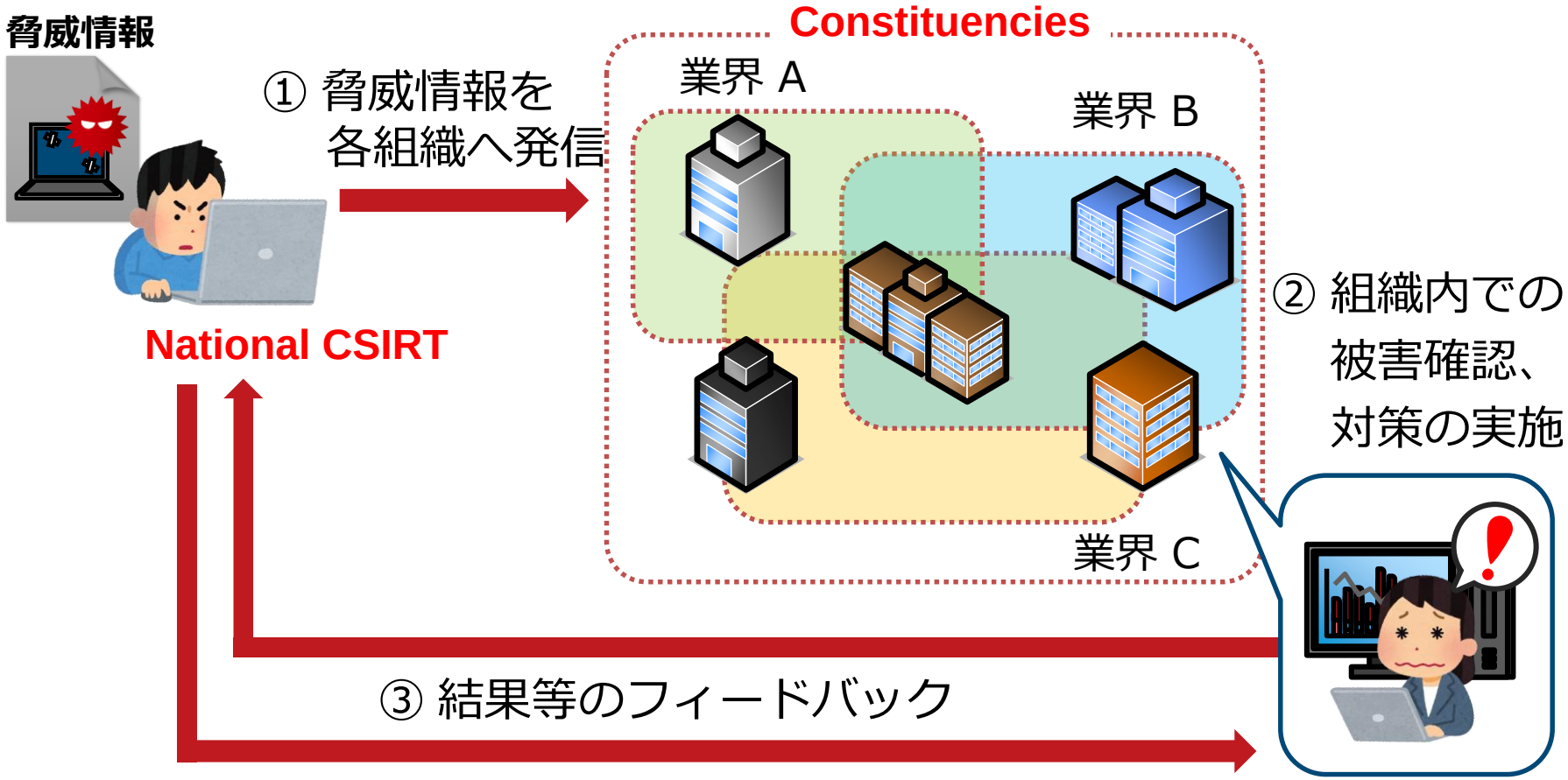
- **コーディネーションセンターの役割と活用**
  - インシデントレスポンス
  - 脆弱性・脅威情報に関する情報流通
    - 脆弱性情報 【JVN】
    - 脅威情報、注意喚起、早期警戒情報他
  - アーティファクト分析【検体解析など】
  - 国内外 のCSIRT 連携促進、コミュニティ推進

“インシデント”に沿った活動を展開しています

- **例えば、こんなときにお役立てください**
  - インシデントが発生し、初動対応での技術的な支援や情報が必要となるケース
  - 日々の対策を進める上で、脆弱性や脅威に関する情報が必要となるケース
  - その他、よろずお気軽にご相談ください

脅威情報の共有による防御

- サイバー攻撃などの脅威情報を共有することで、組織におけるサイバー脅威に対するリスクを軽減



【JPCERT/CC における情報共有・情報連携】

JPCERT/CC における情報提供の流れ (概念)

公開情報

注意喚起

脆弱性関連情報

レポート等

他

コミュニティへの情報

早期警戒情報 (WAISE)

制御システムセキュリティ情報共有ポータルサイト (ConPaS)

他

脅威度や内容に基づき判断

公開・周知することが適切なもの
(公開情報、レポート、
ソフトウエアの脆弱性・注意喚起)

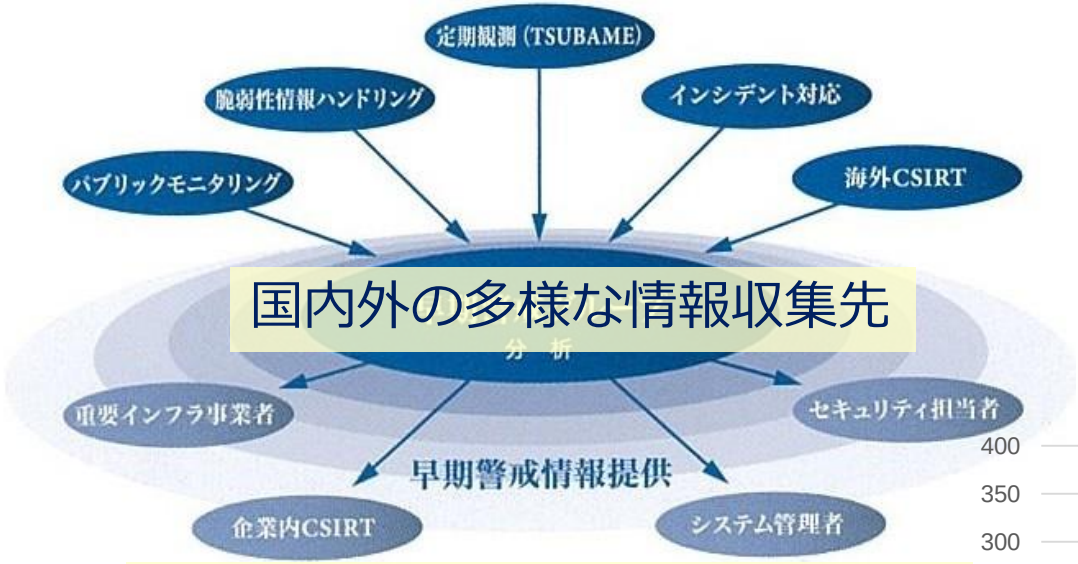
特定の組織やCSIRTに対策を促すことで
より有効に機能するもの
(未修正の脆弱性や攻撃情報等に関する早期警戒情報、 インディケータ情報、特定のグループ・コミュニティーに特化したセキュリティ情報)

分析

情報収集

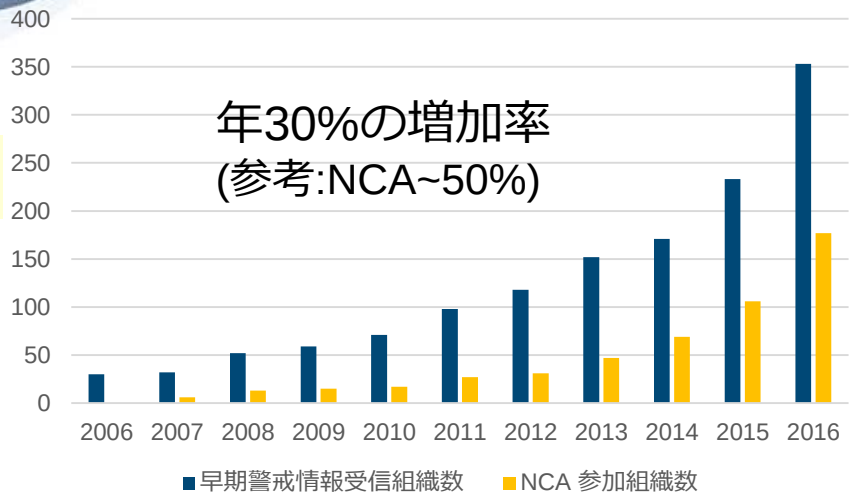
早期警戒情報の提供

- 情報セキュリティに関する情報の収集件数：約16,000件/年
- 早期警戒情報の発信数：約60,000件/年 (発行総数×ユーザ数)
- 早期警戒情報の受信組織数：500以上



国内外の多様な情報収集先

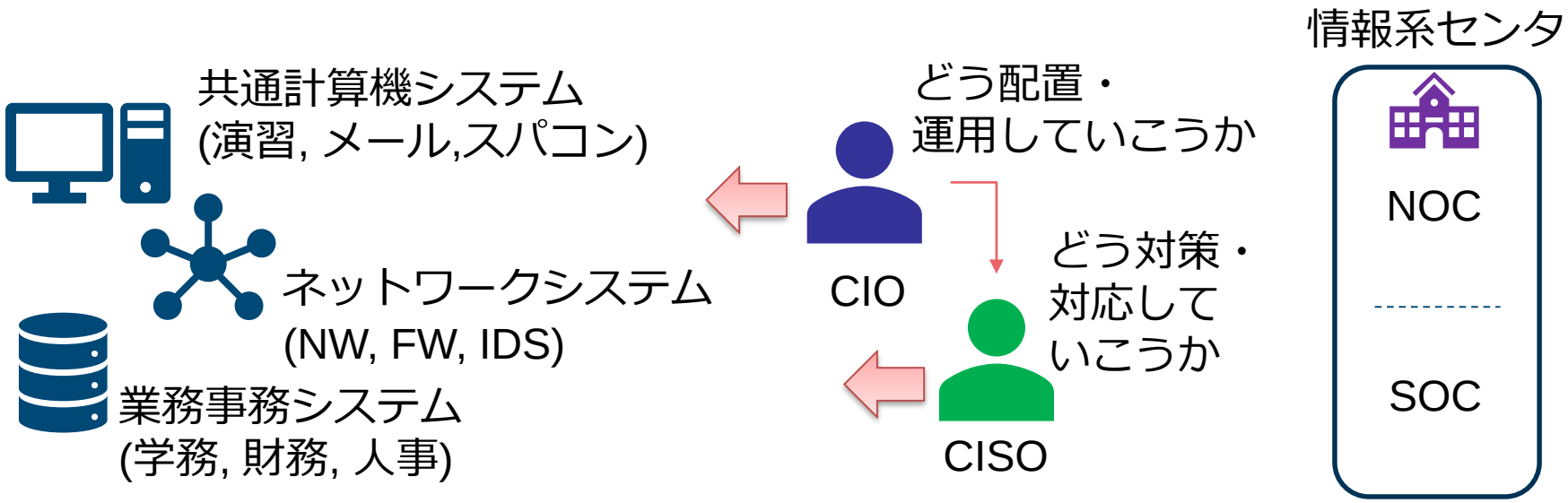
重要インフラを含む様々な配信先



「CIO/CISO」に対する考え方

CIO/CISO とは？

- CIO (Chief Information / Insights Officer)
  - 最高情報責任者, 情報担当理事 (役員)
  - 主に組織の情報システム、情報に対して統括
- CISO (Chief Information Security Officer)
  - 最高情報セキュリティ責任者, 情報セキュリティ担当理事
  - 主に組織の情報セキュリティ、情報管理に対して統括



どうして情報系センタの業務に担当理事？

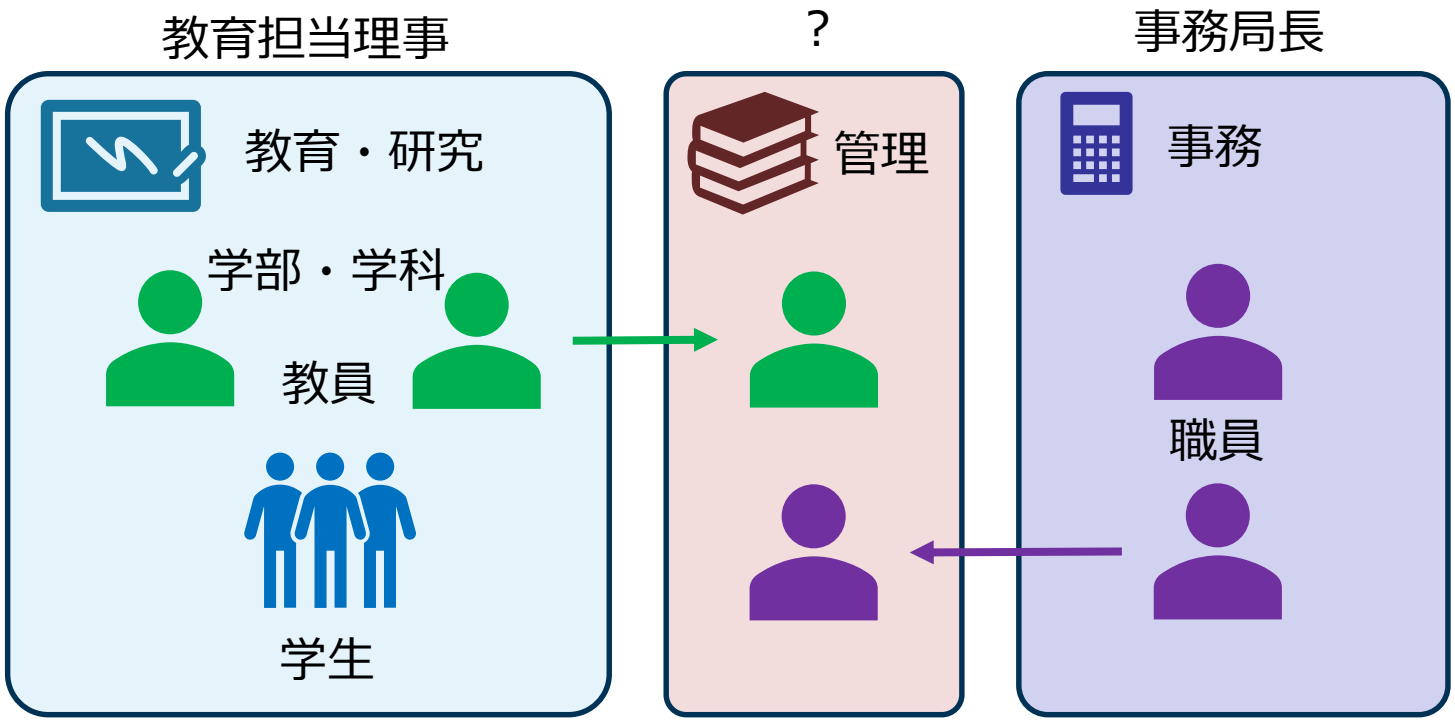
- **「設置すること」**がどうして望まれるのか？

- **決して安くはない IT 投資**
  - システム保守費、定期的なシステム更新にかかる費用
  - 各種ライセンス費
  - 運用のための人件費
  - などなど
- **投資対効果が見えにくい**
  - 出願者数が増加するわけでも、教育・研究効果にすぐに反映されるということでもない
- **問題が発生した場合の影響**
  - インシデント対応にかかる費用
  - 文部科学省や個人情報保護委員会などへの報告
  - プレスリリース・謝罪会見

- 情報系センタの業務は、地味な業務内容に対して、**「問題が発生した場合のリスクが高い」**部門ではないか？と考えられる
  - **方針などの重大な決定には、経営層の判断が不可欠**

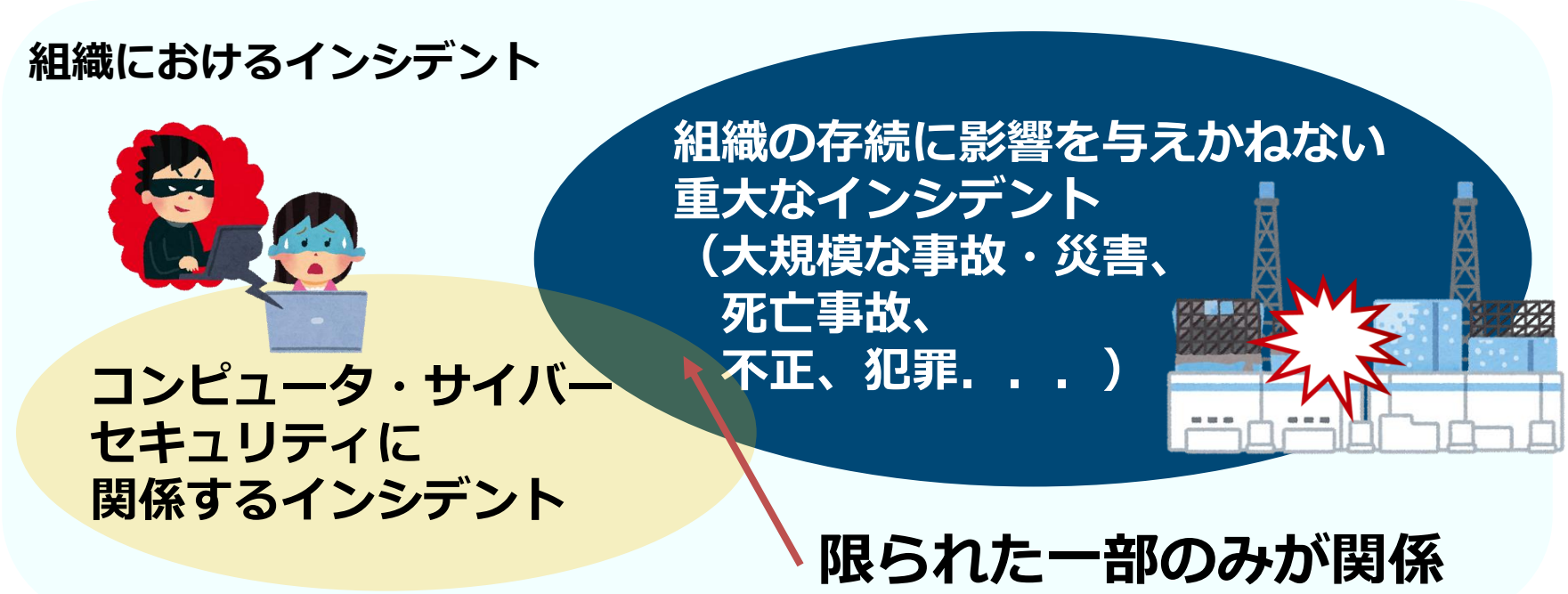
情報系センタの立ち位置

- 管理部門は、大学の「教育研究・事務」に置対してどのように機能しているか？どのような位置にあるか？



実際のインシデントにおいて

- **組織における重大なインシデント(事件・事故)**
  - コンピュータセキュリティインシデントは<u>**一部の問題**</u>でしかない



- **コンピュータセキュリティインシデントへの温度感**
  - <u>**所詮、PCのトラブルと考えがち**</u>ではありませんか？

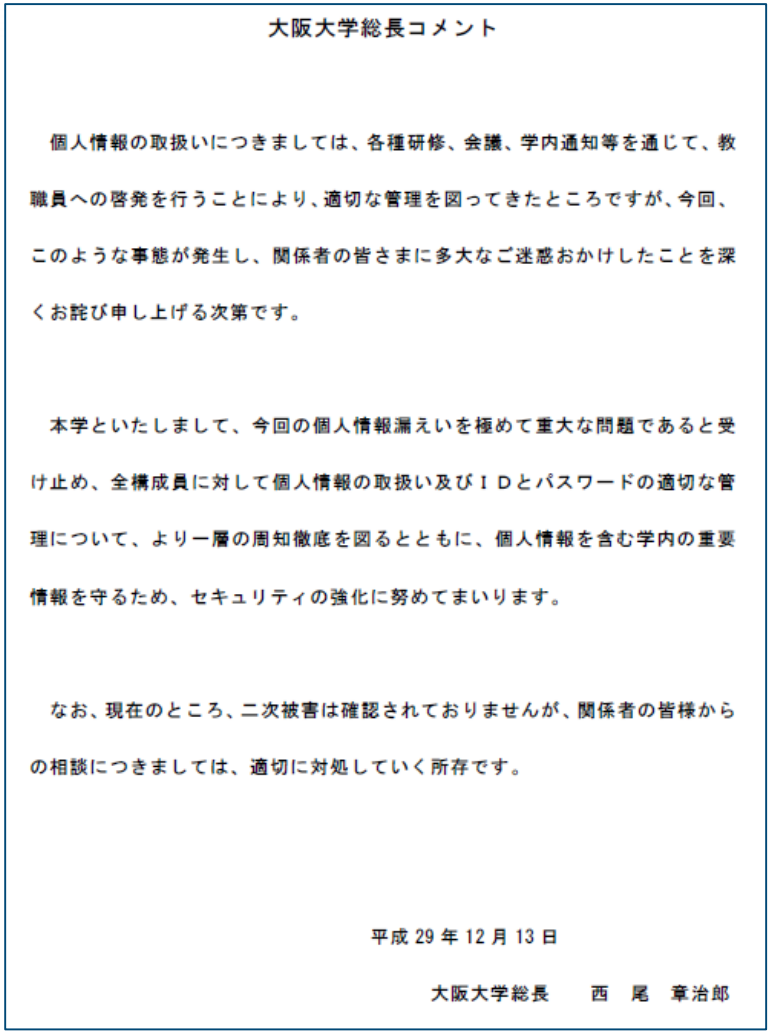
CIO/CISO の重要性

- ICT (Information and Communication Technology) の進展により、大学や教育・研究・事務をとりまく環境が急激に変化してきている
  - 時間・場所を超えた遠隔教育
  - 紙資料作成の手間や提出場所に依存しない電子申請
  - 高速な計算、シミュレーション
- 規模が大きくなるほどシステムにかかる様々な費用は大きくなる
- 使われていくほどシステムがトラブルを起こした場合の被害や問題も大きくなる
- 責任をすべて情報系センタに押し込めてよいか？

大阪大学にて発生した不正アクセス (2017年5月)

- **一人のIDを起点として大学全体の問題へ拡大**
  1. 何らかの方法で一人のID、パスワードが窃取され、悪用
  2. 不正なプログラムが設置され管理者のID,パスワードが窃取
  3. 利用者情報のさらなる取得
  4. 学内グループウェアなどへの不正アクセス

このようなケースの場合情報系センタのみで、対応や責任を議論してよいか？



大阪大学総長コメント

個人情報の取扱いにつきましては、各種研修、会議、学内通知等を通じて、教職員への啓発を行うことにより、適切な管理を図ってきたところですが、今回、このような事態が発生し、関係者の皆さまに多大なご迷惑おかけしたことを深くお詫び申し上げる次第です。

本学といたしまして、今回の個人情報漏えいを極めて重大な問題であると受け止め、全構成員に対して個人情報の取扱い及びＩＤとパスワードの適切な管理について、より一層の周知徹底を図るとともに、個人情報を含む学内の重要情報を守るため、セキュリティの強化に努めてまいります。

なお、現在のところ、二次被害は確認されておりませんが、関係者の皆様からの相談につきましては、適切に対処していく所存です。

平成 29 年 12 月 13 日

大阪大学総長　西　尾　章治郎

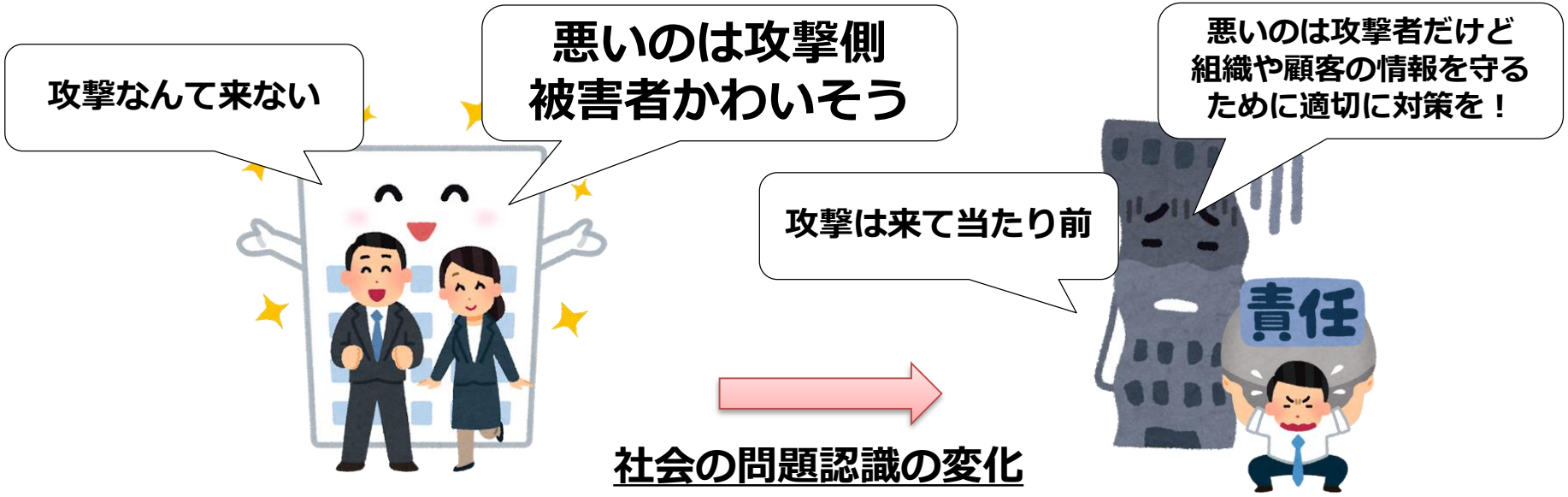
引用:
http://www.osaka-u.ac.jp/ja/news/topics/2017/12/13_01

サイバー経営ガイドライン

- 経済産業省「サイバー経営ガイドライン」

【引用】経済産業省，サイバー経営ガイドライン, http://www.meti.go.jp/policy/netsecurity/mng_guide.html

- IT の利活用は、(中略) 企業として必須の条件
- サイバー攻撃は、年々高度化、巧妙化している
- 経営者が適切なセキュリティ投資を行わずに社会に対して損害を与えてしまった場合、社会からリスク対応の是非、さらには経営責任や法的責任が問われる可能性がある



サイバー経営ガイドライン

- 重要10項目
  - サイバーセキュリティリスクの認識、**組織全体での対応方針の策定**
  - サイバーセキュリティリスク**管理体制の構築**
  - サイバーセキュリティ対策のための**資源確保**
  - サイバーセキュリティリスクの把握とリスク対応に関する**計画の策定**
  - サイバーセキュリティリスクに対応するための**仕組みの構築**
  - サイバーセキュリティリスク対策における**PDCAサイクルの実施**
  - インシデント発生時の**緊急対応体制の整備**
  - インシデントによる被害に備えた**復旧体制の整備**
  - ビジネスパートナーや委託先等を含めた**サプライヤーチェーン全体の対策及び状況把握**
  - **情報共有活動への参加**を通じた攻撃情報の入手とその有効活用及び提供

サイバーセキュリティ経営チェックシート

- 資料には「**チェックシート**」が含まれており、不足している点や改善を行った方がよい点などへの気づきや、会議・報告資料等の議題・項目整理にも活用できる

抜粋 指示１　サイバーセキュリティリスクの認識、組織全体での対応方針の策定

- ✓ 経営者がサイバーセキュリティリスクを経営リスクの一つとして認識している
- ✓ 経営者が、組織全体としてのサイバーセキュリティリスクを考慮した対応方針を策定し、宣言している
- ✓ 法律や業界のガイドライン等の要求事項を把握している

- **「すべてにチェックをつけないとダメ」ではなく**、なにがどうしてできていないか、改善をするにはどうしたらいいかをステークホルダーと議論し**「具体的な改善に向けて動く」**ことが重要

IPA 「企業のCISOやCSIRTに関する実態調査 2017」

- IPA 「企業のCISOやCSIRTに関する実態調査 2017」での調査から考えられること

【引用】IPA, 「企業のCISOやCSIRTに関する実態調査2017」報告書について,
https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html

  - CISOに対して、自社事業への理解を求めたり、実務経験を求めたりしていない→**誰でもいい？**
  - CISOは足りているが、情報セキュリティ技術責任者・担当者は足りていない→**役員ではなく手が動かせる人が欲しい？**

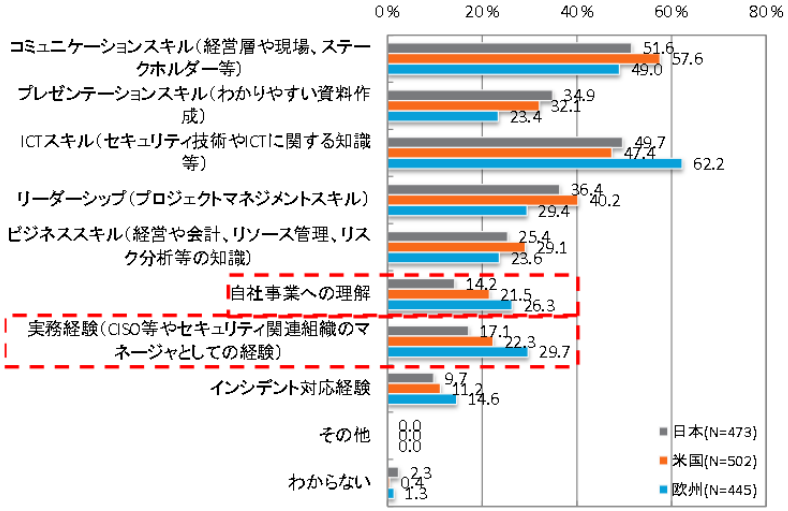


図 3.2-27 CISO等に求めるスキル・経験

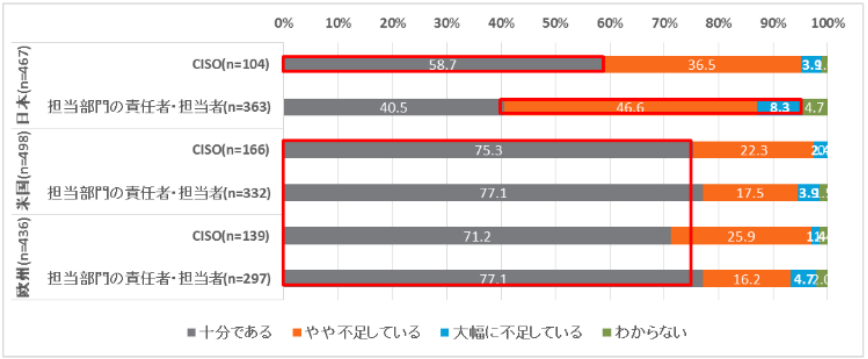


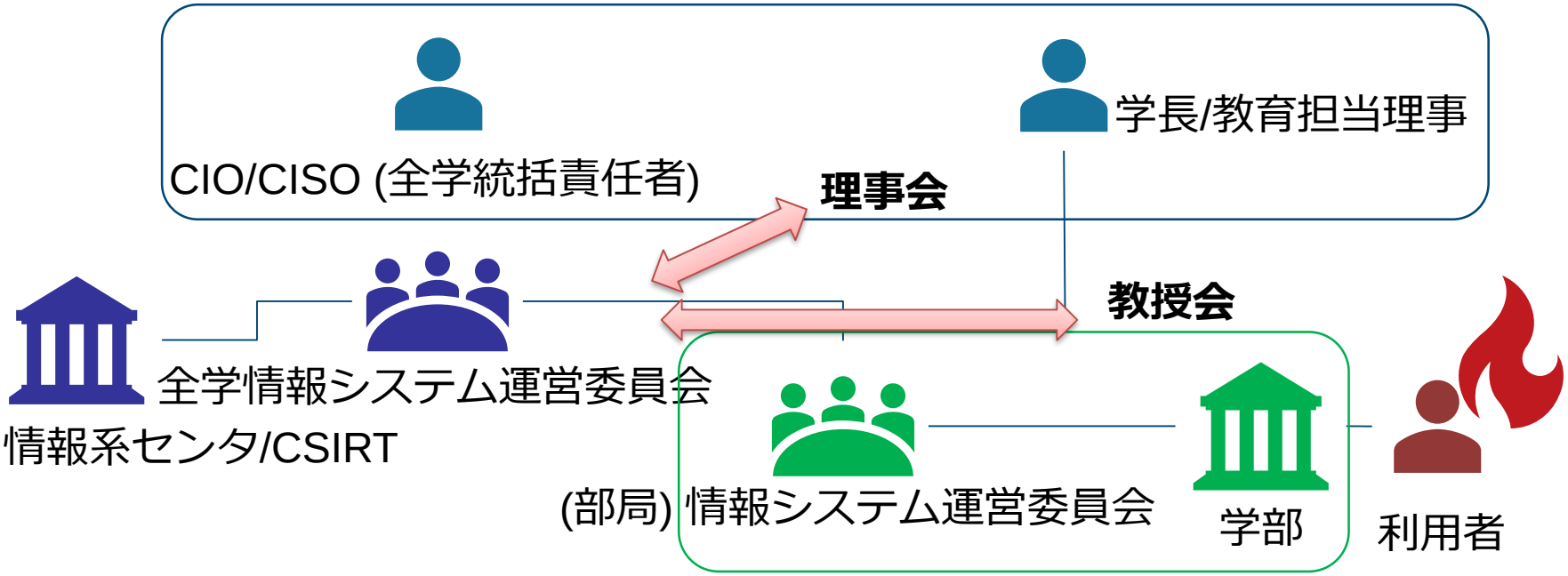
図 3.2-40 情報セキュリティ業務担当者の量的充足度（役職別）

大学での問題点を考えてみる

- CIO/CISO と情報系センタ間の相互理解・コミュニケーションの不足
  - CIO/CISO は、所掌する業務への理解があるか？
  - 情報系センターは、経営層からの期待に応えられているか？
- こんなことに陥っていませんか？
  - CIO/CISOが知らないところでシステム導入・更新、インシデントの処理が発生
  - 情報系センタが知らないところで人事計画の更新
  - などなど
- 情報系センタと他部署間、CIO/CISOと他理事間でもミスコミュニケーションは発生

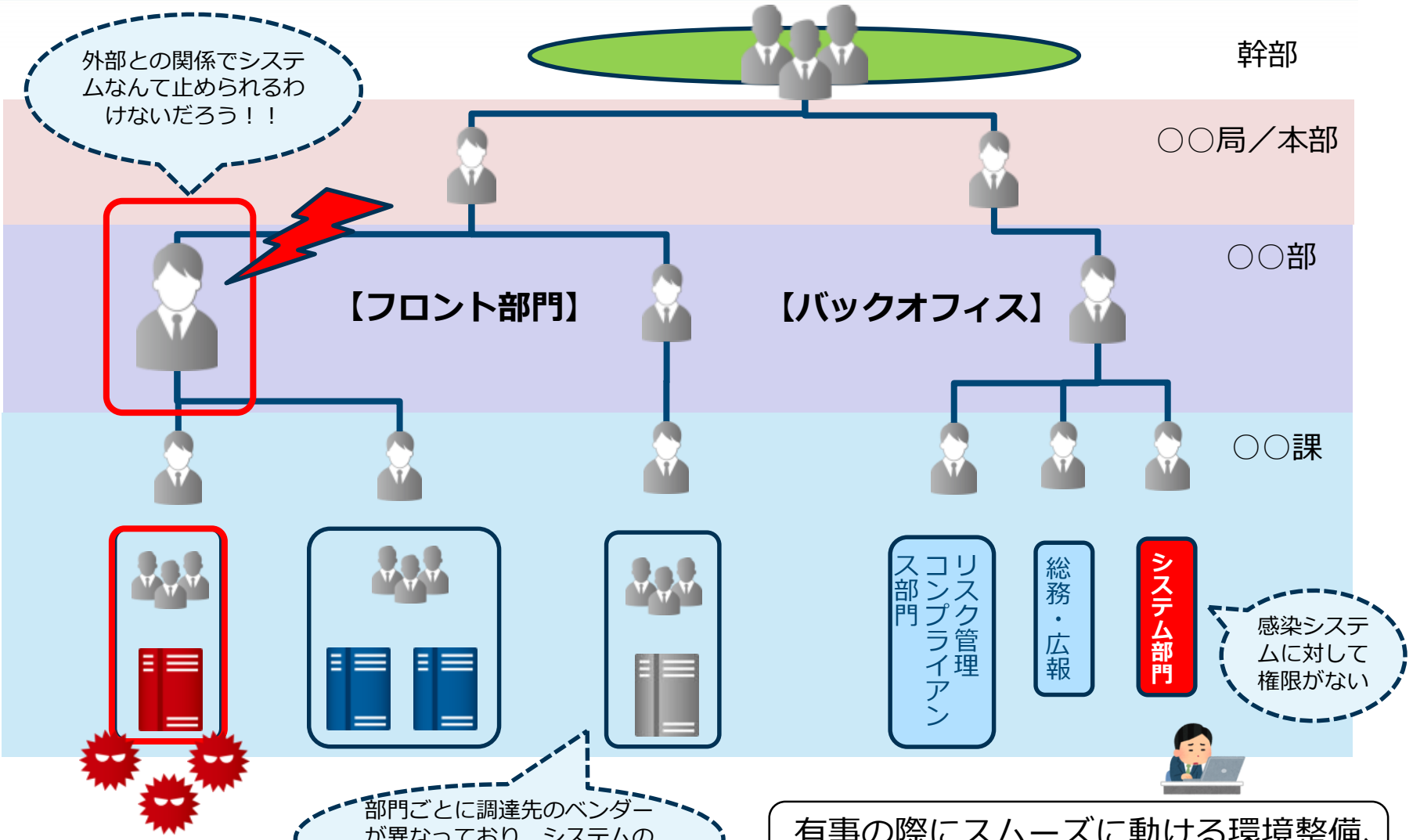
大学の自治とITガバナンス

- セキュリティポリシ・委員会がはまりやすいポイント
  - 一般的な構造 (参考：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)



- **利用者のインシデントに対して、CIO/CISO/CSIRT は、直接関与できない可能性？**
- **報告など文章においても、複数の会議を経ねばならない可能性？**

こんな構造になっていませんか？
～初動対応が進まない組織内の構造例～



注: ピラミッド構造が悪いわけではありません

有事の際にスムーズに動ける環境整備、コミュニケーションを図ろう！

陥りやすいコミュニケーションの問題

- **“縦”と“横”のコミュニケーション**
  - “縦”のコミュニケーション (エスカレーション・報告)
    - 丸投げ
    - **お互いの理解不足**
  - “横”のコミュニケーション (相談・オペレーション)
    - 利害の不一致
    - **お互いの理解不足**

- **事前対策を行うにあたって、既に実行できている分野と比較するとよい**
  - 物理的な事象など、既に実行できている問題を例に考えるとイメージしやすい
    - 災害、火災、事件、救急、避難　等

インシデント対応にみる CIO/CISO と CSIRT の役割

必要なのは専門技術か？それとも調整能力か？

- **こんなことで悩んでいませんか？**
  - CSIRT を作ったけれども、専門の知識をもった人間がいないので機能しない
  - 全学として取り組まなければならないことは分かっているけれども、個々の部門で運用や対策はバラバラ
  - 利用者が部局の理解が進まない
  - なんとなくインシデントも起きてないようだし、なんとなくうまくいっているような気がするけれど、これでいいのか漠然と不安
  - CIO/CISOが狙い通りに報告してくれない。理事会や評議会で常に批判されてしまい、会議が怖い
  - CSIRTがテクニカルタームを使っていて、何を言っているのか理解できない
- **「関係者全員が、正しい技術や知識が解れば解決できるはず」と思っていませんか？**
  - そもそも、これらの原因は「技術や知識」ですか？

必要な対策はテクニカルだけとは限らない

インシデント対応において重要なポイント

- 「その時に何が発生していたか、今何が発生しているのか」現状の問題や影響の範囲を正しく把握すること
- その規模に応じて適切にリスクを判断し、明確な戦略に基づく適切なリソースを決定・措置すること
- 第三者などからの技術的情報を活用し、客観的事実に基づいてインシデントマネージメントを行うこと
- モニタリングを実施し、実施可能で有効な再発防止策へフィードバックしていく

CIO/CISO と CSIRT の役割

- 適切な経営判断・・・CIO/CISO
- リスク・戦略の提示やインシデントへの実対応・・・CSIRT
- それぞれ必ずしも技術的な知見のみとは限らない

インシデント対応は組織の総力戦

- インシデント対応に必要なのは技術的な対応能力だけではありません。

  プレス発表や対外対応：広報

  関係各機関への報告：総務・企画

  行政サービスへの影響回避：各担当部門

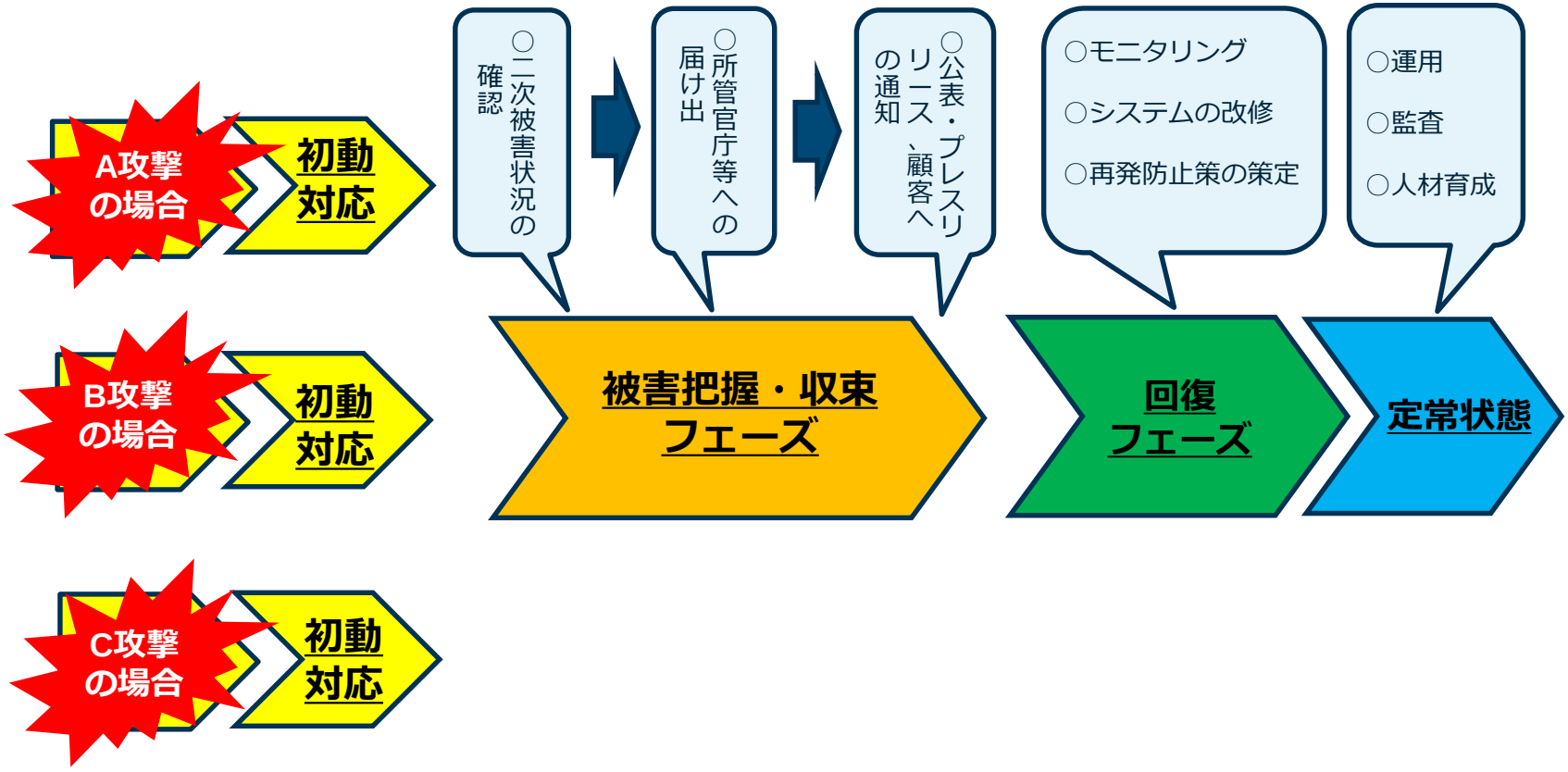
  緊急対処費用の調達：財務・経理

  緊急対応人員の確保：人事

  組織全体の統括：幹部

【参考】インシデント対応はフェーズに分けて考える

- **時中だけに注目しない～事後に向けた対応は不可避**
  - 発生している出来事への対応だけでなく、その後に必要なアクションを想像する必要がある

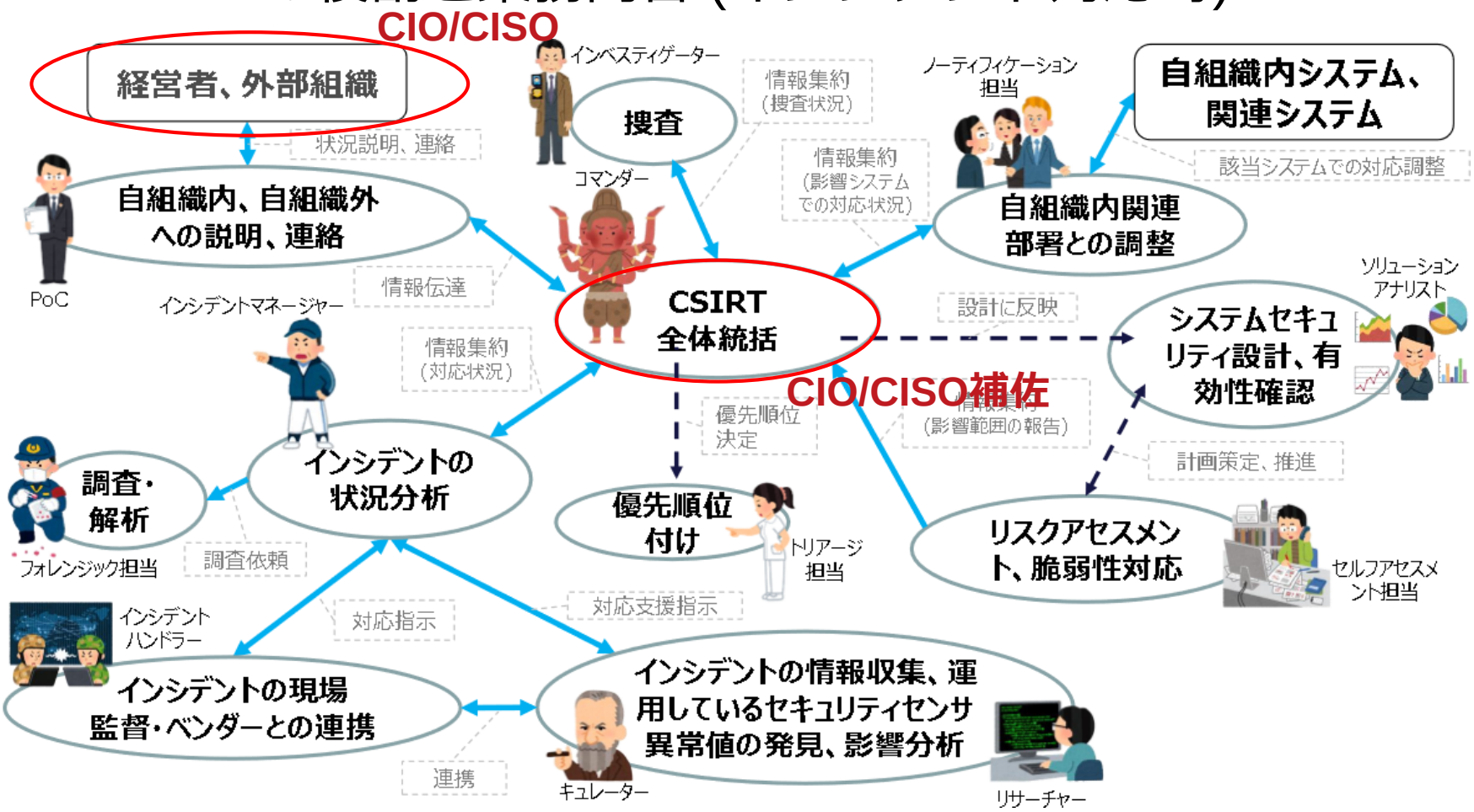


CIO/CISO と CSIRT が協力することが不可欠

- **ポリシやルール、計画の策定・体制の整備**
  - 戦略性や中長期をみたルールや計画の立案
  - 必要な情報を集められるようにする
  - CIO/CISO と CSIRT の相互信頼を築く最初のポイント
- **予算計画、マスタープランの立案・点検**
  - 他の部局や施設設備と違い、比較的短いスパン (3-6年) でシステムのリプレースが行われるからこそ、戦略性をもったマスタープランが不可欠
  - ランニングやコストを意識すること、させること
    - 例：一人当たりコストの算出と一人当たりインシデント対応拘束時間の算出→費用対効果の算出例
  - リスクマネーをどう確保するか？コスト部門であるからこそ、CFO や財務担当部門との良好な関係を心がける
- **適切な予算の執行・システムの運用**
  - ベンダに丸投げではなく、健全な運用を心がける
  - システムの正常動作と異常動作を肌感覚で理解することは、インシデントの早期発見にもつながる
  - 定期的なログ分析に基づいた委員会報告も重要
    - 監事や監査部門と普段からコミュニケーションを図り、システム監査を常に意識した健全なシステムの運用を心がける

CSIRTの様々な役割

■ CSIRTの役割と業務内容 (インシデント対応時)



様々な役割と業務があり、必要とされることで人員が増加される

引用:NCA
CSIRT 人材の定義と確保 Ver.1.5
http://www.nca.gr.jp/activity/training-hr.html

「CSIRT構築および運用における実態調査」から

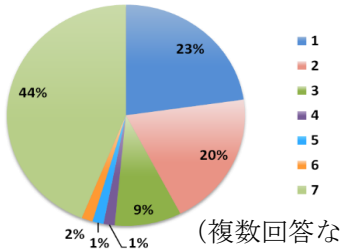
- NCA (日本シーサート協議会) 加盟の CSIRT の多くが設立後、CSIRT 要員の増加がみられる

【引用】JPCERT/CC, 「2015年度 CSIRT構築および運用における実態調査」, https://www.jpcert.or.jp/research/2015_CSIRTsurvey.html

  - 人員の追加 = CSIRTの業務が経営層に評価
  - CSIRTが成熟している一つの表れともいえる

2.3.2. 設立当初のメンバー数

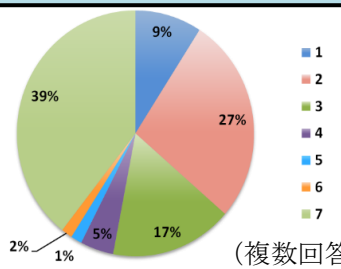
#	人数	回答数
1	5名未満	15
2	5名以上10名未満	13
3	10名以上20名未満	6
4	20名以上	1
5	バーチャルなので流動性あり	1
6	不明	1
7	未回答	29



（複数回答なし N = 66）

2.3.3. 現在のメンバー数

#	人数	回答数
1	5名未満	6
2	5名以上10名未満	18
3	10名以上20名未満	11
4	20名以上	3
5	5～20	1
6	バーチャルなので流動性あり	1
7	未回答	26



（複数回答なし N = 66）

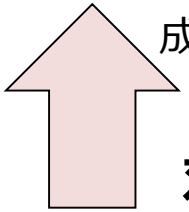
CSIRT構築時

現在の CSIRT

CIO/CISO や CSIRT 活動の成熟化と業務の明文化

- 大学での CIO/CISO の業務や、情報系センター (CSIRT含む) の業務において、**セキュリティポリシや関連規程に記載されないまま、なんとなく業務が遂行され、その場限りになっている**ものはありませんか？

最適化　⇒ ゴール
明文化　⇒ 組織全体で品質確保
ルール化　⇒ 一定の品質担保
その場限り ⇒ 対応品質はバラバラ



成熟度：高

対応の品質

- 情報・セキュリティに関する業務に限らず、その場限りや特定の個人のスキル・知識が業務を紐づくような対応はどこかで破綻します。
  - ポリシーや実施手順などの関連規程は何のために存在？
  - 実態に即していないことを背伸びをして書いても逆効果

- **規程としてまとめあげていくにも CIO/CISO と CSIRT の相互理解は不可欠**
  - CIO/CISO の情報系センター業務への理解
  - 情報系センターの業務成熟度の改善・対応品質の確保

明文化のメリット

- 必ずしも規程にする必要はありませんが・・・

明文化を行うためには、現状把握、実行プロセス、達成目標など様々な項目の洗い出し・検討が必要

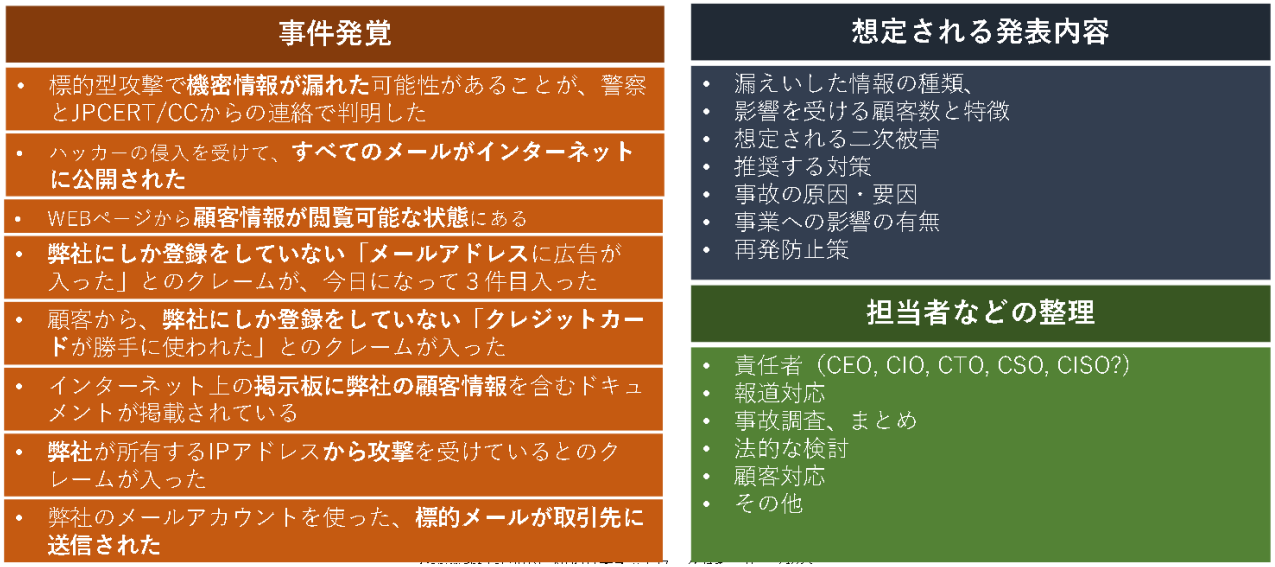
明文化を行うことで例えば次のようなメリットが

— 現状のセキュリティに対するレベルを把握できる
— 求めるセキュリティに対するレベルの目線を組織として合わせられる
— 各組織での役割の明確化（責任所在の明確化）
— インシデント対応が素早く可能
— システム計画やスキルアップ計画が立案しやすい
— 成果が定性的に加え定量的に測れる

など

演習のススメ

- JNSA 「CISO ハンドブック」
  【引用】JNSA, CISO ハンドブック, https://www.jnsa.org/result/2018/act_ciso/
  - インシデント対応ワークショップ



  - 組織で発生する可能性のある架空のインシデントを想定し、実対応を演習
    - 第１インシデント
      - インシデントへの対応と記者会見シミュレーション
    - 第２インシデント
      - 付加要因の設定
        - CIOが倒れた、出張中で連絡がつかない
        - 記者会見で失敗した
        - ジャーナリストに注目された

【参考】大学で考えたい
セキュリティ対策

【参考】大学等に求められる対策

(サイバーセキュリティ戦略本部第14回会合資料より)

⑤大学等における情報セキュリティ対策の向上

多岐に渡る情報資産、多様なシステムの利用実態といった大学等における多様性を踏まえ、当該特性に応じて、大学等の情報セキュリティ対策の強化を促進するとともに、大学等の相互の協力による自律的活動の向上に向けた取組を促す。

具体的には、**各大学等は、教育・研究等の多様性に配慮しつつ、中長期的な情報セキュリティ対策基本計画を策定し、マネジメント面及び技術面の取組を推進**する。また、**大学等の連携によるサイバー攻撃検知体制の整備や人材育成の取組を推進**する。なお、国は、これらの取組に対し、必要な支援に努める。

○ 大学等における自主的な取組

ア マネジメント面

・企画・法務・広報など関係部門と連携したインシデント対応体制の構築と対処能力の向上
・情報セキュリティポリシーや情報の取扱規程等の見直しや組織への浸透
・多様な構成員に対応した教育・訓練や啓発活動の実施
・構成員の役割に応じた自己点検や中立性を有する者による監査の実施

イ 技術面

・組織内の情報機器の把握と適切なアクセス制御の実施
・重要情報を扱う機器へのアクセス等を監視する機能等の実装
・組織内で利用しているソフトウェアの適切な更新が可能な仕組みの整備

○ 文部科学省等による支援

・大学等における自主的な取組の促進の観点から、**インシデント対応力の向上やセキュリティ監査手法に関する研修の実施及び機会の充実、情報システムの侵入耐性診断の実施に関する支援、諸会議における周知、啓発及びグッドプラクティスの共有並びに情報セキュリティ対策基本計画の進捗状況のフォローアップその他自主的な取組加速のための支援**を実施

○ 大学等の相互協力による取組

国立情報学研究所において、大学等と連携し、SINET におけるサイバー攻撃検知システムの運用や、同システムの実環境を用いた技術職員の実地研修の実施、脅威情報等の共有促進により、大学等のインシデント対処能力向上を図る。また、連携機関の拡大については、今後、運営上の課題を含めて検討する。

大学等共通の課題の検討や知見の共有等について、各大学等の枠を超えてCSIRT 担当者同士のコミュニティを形成し、脅威情報の共有や共通課題の検討等を実施予定。

https://www.nisc.go.jp/conference/cs/dai14/pdf/14gijishidai.pdf

今後の動向と大学への影響

- **マネジメント面**
  - 企画・法務・広報など**関係部門と連携したインシデント対応体制の構築と対処能力の向上**
  - 情報セキュリティポリシーや情報の**取扱規程等の見直し**や**組織への浸透**
  - 多様な構成員に対応した**教育・訓練や啓発活動の実施**
  - 構成員の役割に応じた自己点検や中立性を有する者による**監査の実施**
- **技術面**
  - 組織内の**情報機器の把握**と適切な**アクセス制御の実施**
  - 重要情報を扱う機器への**アクセス等を監視する機能**等の実装
  - 組織内で利用している**ソフトウェアの適切な更新**が可能な仕組みの整備

放置したら何が起こるのか？

- **「便利だからやってしまえばよい」、「トラブルを起こしたのは使い方が分かっていない人だから、自分は大丈夫」、「隣の人がトラブルにあったけれど、自分は関係ない」 – 独りよがりの考え方が続くと考えられること**
  - ルールがより厳格に・厳しくなる
  - 教育・研究・事務の活動などにも影響が生じる可能性

- **放置しても、よいことなど何もないです**
  - **異常なことがあったら隠さない。相談しあう**
  - **異常なことが起きても叱らない。解決を目指す**
  - **責任は逃れられません。覚悟を持ってください**
  - **人に責任を押し付けなでください。一人ひとりが注意深く行動することで防げることも少なくありません**

【参考】JPCERT/CC 早期警戒情報 CISTA にて提供している CSIRT へのサービス

- JPCERT/CC では、重要インフラや大規模組織、学術機関等への CSIRT の平時での活動への支援として早期警戒情報として情報提供を行っています
  - 早期警戒情報としての情報提供
    - ゼロディを含む脆弱性に関する対策情報
    - マルウエアなどの脅威に関する情報
    - サイバー攻撃 (予告等含む) に関する情報
  - 早期警戒情報提供ポータル CISTA 上での提供サービス
    - 情報提供機能
    - マルウエア検体分析機能 (2018年内公開を予定)
- 大学でのセキュリティ対策の一環として、ご興味・ご関心のある方はご相談ください

まとめ

大学におけるCIO/CISOの重要性

- **大学という特殊な環境下でのCSIRTの業務を正しく遂行する上で、経営層の関与は不可欠**
  - 情報系センタ (管理部門) の立ち位置や「兼務」スタッフ
  - 部局よりも弱い立場になりがち
    - 言うことを聞いてくれない、対応が見えない

- **CIO/CISO と情報系センタ (CSIRT) の間で適切にコミュニケーションできていますか？**
  - 経営層の思いは、現場に伝わっていますか？
  - 現場の思いは、経営層に伝わっていますか？
  - お互いに伝わらないのが普通。普段からの工夫が不可欠
    - 工夫は大学や、組織形態、担当者により異なる
  - お互いに相互信頼・相互信用を心がける

大学での CIO/CISO に求められる像

- **CIO/CISO と CSIRT の関係性は良好ですか？**

- **CIO/CISO に求められる像**
  - 経営層 (理事) として、大学の情報システム・セキュリティ関連業務を統括する
  - 適切な情報システム・セキュリティに対するプランを立案できる
  - 情報システムの更新や、インシデントが発生した場合など司令塔として責任を持つ
  - 適切な予算計画・人事計画を立案できる
  - 必要な学内調整（経営層間）で行える
  - 立案した計画やポリシの実行をCSIRTに指示できる

- **国内のCSIRTは、助言型機能を持つことが多い**
  - CSIRTは緊急時におけるオペレーションの実行を提案し、CIO/CISOはそれを決裁する立場にあると考えられる
  - 情報システム・セキュリティにおける学内の実際の業務フローを意識し、CIO/CISOの設置、CSIRTの設置を計画してください

高等教育機関で発生しているインシデント

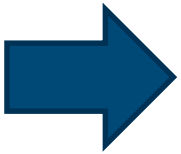
- **複雑なインシデントが複数の大学で発生**
  - 標的型メール攻撃などの高度サイバー攻撃
    - 科研費にまつわる標的型攻撃メール
    - 学会などの活動を囮文章にもつものも存在
  - 不正アクセス事案
    - 一つの ID から組織全体の問題につながるようなインシデントが発生

- **いつ、大学がインシデントに巻き込まれるかは予測がつかない**
  - その引き金が、誰なのかも予測がつかない

目的に応じた情報共有のススメ

- **「目的をもった攻撃」を意識する**
  - 様々な手段を用いて達成しようとする
  - 複数の攻撃先、繰り返される攻撃
  - 内部ネットワークまで到達できれば

- **「見えていないもの」に気付くための手段を確保する**
  - 各組織内においてデータを保全・共有する
    ログ / インシデント対応履歴 / 対処方法
  - 他組織との間でデータを突合させる
    これって、ウチだけ？？？



「知見の集約」がキーワード
経営課題としてのセキュリティを意識

組織内のインシデント対応体制(CSIRT)の活用

- **事業継続を意識していく**
  - セキュリティは**事業継続リスクの 1つ**
  - **BCM(事業継続マネジメント) / BCP(事業継続計画)との関連性**
  - 対応組織を作るのではなく、機能と組織を融合させる
  - 外からの攻撃だけではなく、中で暴れる攻撃も防ぐ意識

- **計画だけでなく、訓練も重要です**
  - インシデントは想定の範囲外まで対応が伸びることも
  - 決められたことが出来ない事は多々あります
  - 自組織でできないことは、他組織に相談してみるのも手

（ Face to Face での情報交換は、割と重要視されている… ）

おわりに

■ インシデントは確実に発生している

- ✓ JPCERT/CC では、多様なサイバー攻撃を確認しています
- ✓ 毎週のように**新しい脆弱性**や**事例**が報告されています

■ 脆弱性を悪用された攻撃の被害を防ぐには

- ✓ **悪用されやすい脆弱性は、数日のうちに悪用され、しばらく悪用が続く**こともあります
- ✓ 早期のうちにアップデートすることが望まれます

■ サイバー攻撃は、対岸の火事ではない

- ✓ **CISO/CSOは「ウチは狙われない」**という意識を捨てください。
- ✓ 攻撃を防止するだけでなく、**早期検知**、**復旧**、**追跡調査**ができる準備をしておくことも大切です

参考資料

- 洞田 慎一,高等教育機関に対するサイバー攻撃の動向と情報セキュリティ対策の考え方, 大学と教育, 2018年3月号.
- JPCERT/CC, CSIRT マテリアル構想編 “経営リスクと情報セキュリティ”, https://www.jpcert.or.jp/csirt_material/concept_phase.html
- 経済産業省, サイバー経営ガイドライン, http://www.meti.go.jp/policy/netsecurity/mng_guide.html
- IPA, 「企業のCISOやCSIRTに関する実態調査2017」報告書について, https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html
- IPA, 「CISO等セキュリティ推進者の経営・事業に関する役割調査」報告書について, https://www.ipa.go.jp/security/fy29/reports/ciso/
- JPCERT/CC, 「2015年度 CSIRT構築および運用における実態調査」, https://www.jpcert.or.jp/research/2015_CSIRTsurvey.html
- JNSA, CISO ハンドブック, https://www.jnsa.org/result/2018/act_ciso/
- NCA, CSIRT 人材の定義と確保 Ver.1.5, http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf
- NII,高等教育機関における情報セキュリティポリシー策定について, https://www.nii.ac.jp/service/sp/
- FISC, 金融機関等におけるコンティンジェンシープラン策定のための手引書（第3版追補3）

お問合せ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- Tel：03-3518-4600
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html