情報セキュリティ事故に緊急対応するための体制組織化への取り組み

立命館大学
情報理工学部
セキュリティ
＆ネットワークコース

上原哲太郎

今日ではどんな組織も多様なセキュリティ事故に備えが必要

- 外的要因＝「外からの攻撃」への備え
  - サイバー諜報が当たり前になった世の中で何をどのように守るのか

本日はこちら

- 内的要因
  - 「事故」への備え
    ＝システム障害がもたらすセキュリティ危機
  - 「事件」への備え
    ＝「内部不正」への備え

こちらは
本日は
触れません

多様化する攻撃者像

愉快犯→思想犯

- 技術誇示目的
- 思想信条の表現
- 「集団暴走」

明確な目的

- 怨恨
- 金銭目的（無差別攻撃）
- 破壊工作・諜報（標的型攻撃）

無差別攻撃よりも標的型攻撃が厄介な問題…

いま大学が本当に恐れるべきは…

- 「サイバー諜報」
  - 不正アクセスやマルウェアをきっかけにした高度な諜報戦
  - 攻撃の高度化により従来の対策では検知が困難に
- 「内部犯罪」
  - 業務の電算化が進み効率化と引き替えにリスクは高まる
  - 定員外職員の増加アウトソーシング増加ロイヤリティに頼った人的セキュリティは無理

どんな情報でも換金出来る時代になり潜在的脅威は高まっているはず…？

年金機構事件を契機にして大学も標的であることが明確に

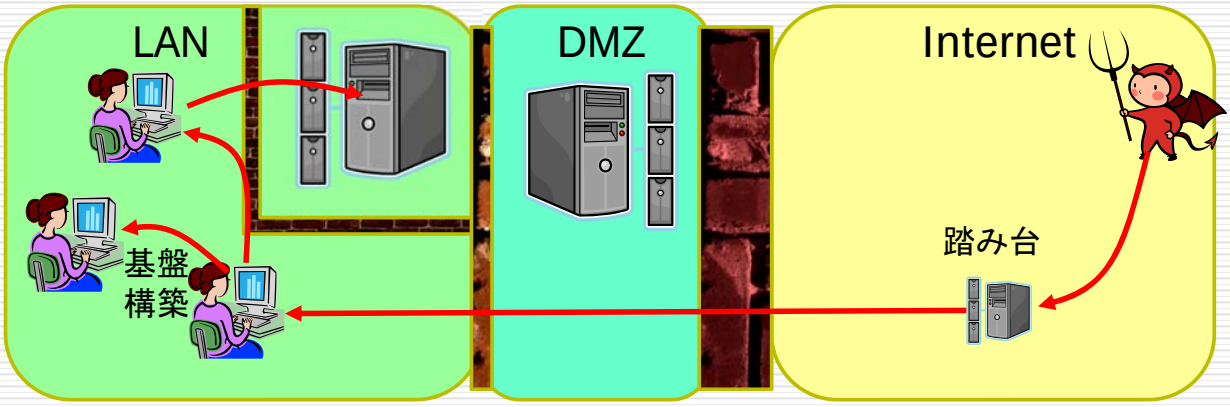
- 2015年11月　富山大学水素同位体科学研究センターに標的型攻撃
  - 2016年10月10日に各紙報道
  - 実際の経緯は…
    - 2015年11月5日　第1の不審メール
    - 2015年11月17日　第2の不審メール
    - 2015年11月24日　第3の不審メール
      （留学生を装い研究の相談メール）
      これを非常勤職員が開封して感染
    - 2015年11月26日～2016年3月ごろまで情報流出と思われる活動が継続
    - しかし富山大自身がそれを把握したのは2016年6月14日の外部通報による

長期にわたり気づかない

自分で気づくことができない

侵入→基盤構築→目的達成

内部サーバ　外部サーバ
File,DB,Apps…　Web,Mail,DNS…



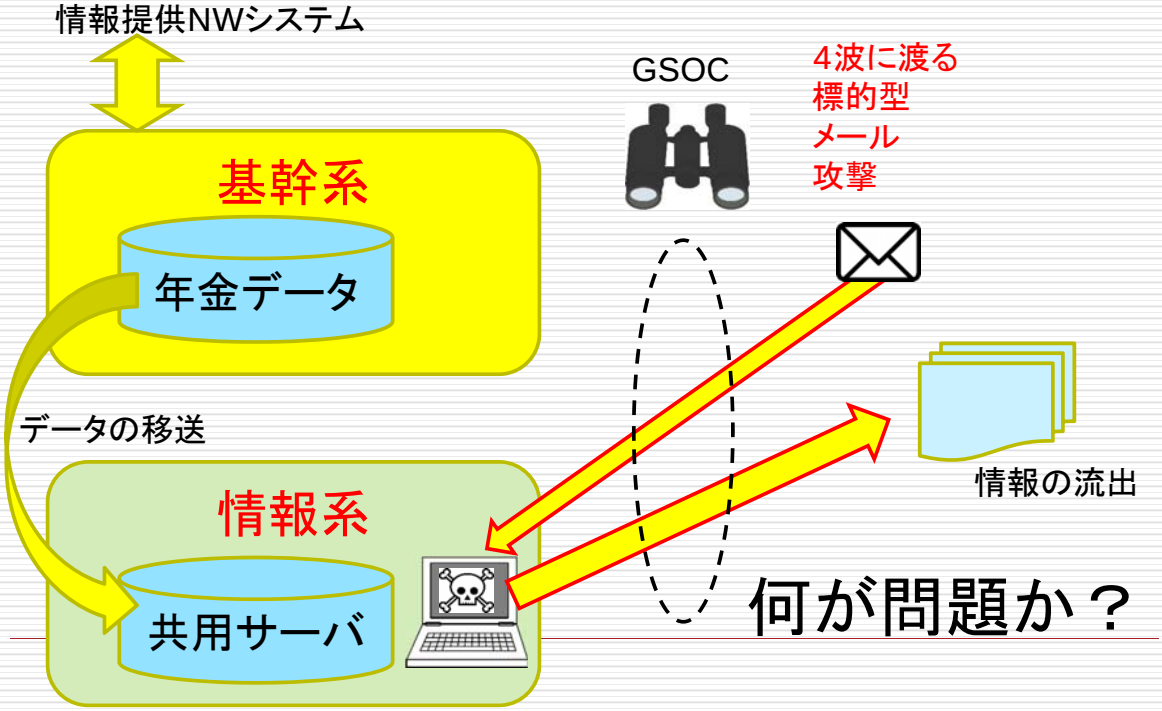
マルウェアを植え付け、遠隔操作しながら諜報活動を行う
ここ10年以上攻撃者の定石手

初期侵入は検出できるか？

- 手口にはパターンがあるとはいえ多彩
  - メール、水飲み場、クラウドサービス…
- マルウェア対策があまり役立たない
  - パターンファイル系は無理
  - ふるまい検知は精度が課題

- 何より相手は
  「成功するまで諦めない」

例えば年金機構事件では…



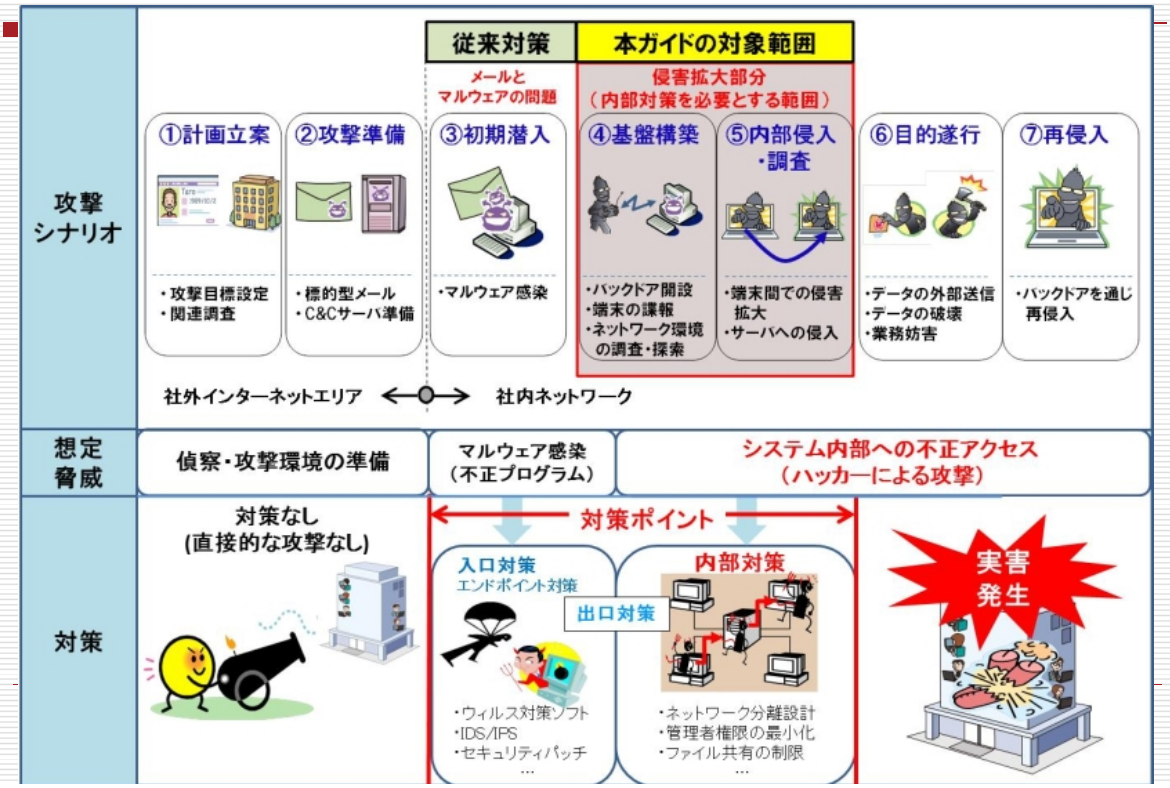
何が問題か？

もはや「入れないようにする」のは困難

- 多層防御　多段階防御はもう常識
  - 入口対策＋出口対策＋「真ん中対策」
- 攻撃者の手を縛り、時間を稼いで
  攻撃検出の機会を少しでも増やす

初期侵入から目的達成までは
時間がかかっているはず
時間を稼げる対策をして
その間に発見することを期待

IPA「高度標的型攻撃」に向けた
システム設計ガイド

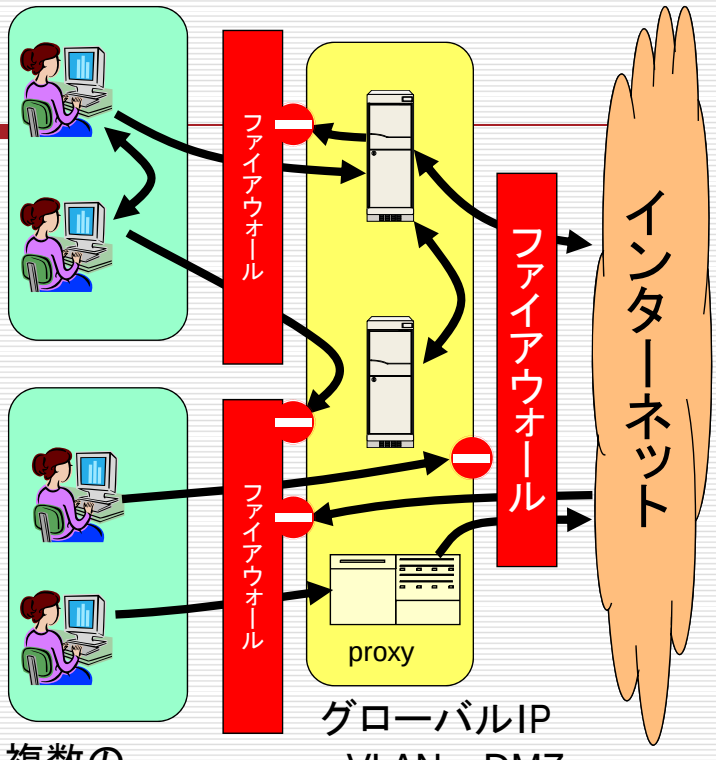


IPAシステム設計ガイドの基本思想

- 組織内システムそのものを「迷路」にする
  - 部課単位にネットワークを細かく切って
    相互の直接通信を禁止する
    →攻撃者のマルウェア拡散活動を防止し、
    検出も容易になる
  - 各ネットワークからインターネットへの通信の
    手段をできるだけ絞ってログ検出を容易にする
    →可能な限りHTTP Proxy経由でのアクセスのみ
    そのログも取得しておき定期的に監査
- こうして時間稼ぎしてる間に検出する
  ＝「検出できる体制を整える」

「細切れ」LAN

- クライアント類を
  部課単位で
  細かいVLANに
  閉じ込めて、
  被害拡大を防止
- FWやProxyは
  ログを取る
- 取ったログは
  定期的監査
  - SIEM活用など



優先順位をよく考えるべき

事故を減らす

事故検出能力向上

事後対応を迅速化

実際には事故は防げない…
長期にわたり気づかないと問題

しかし…大学という組織の特殊性

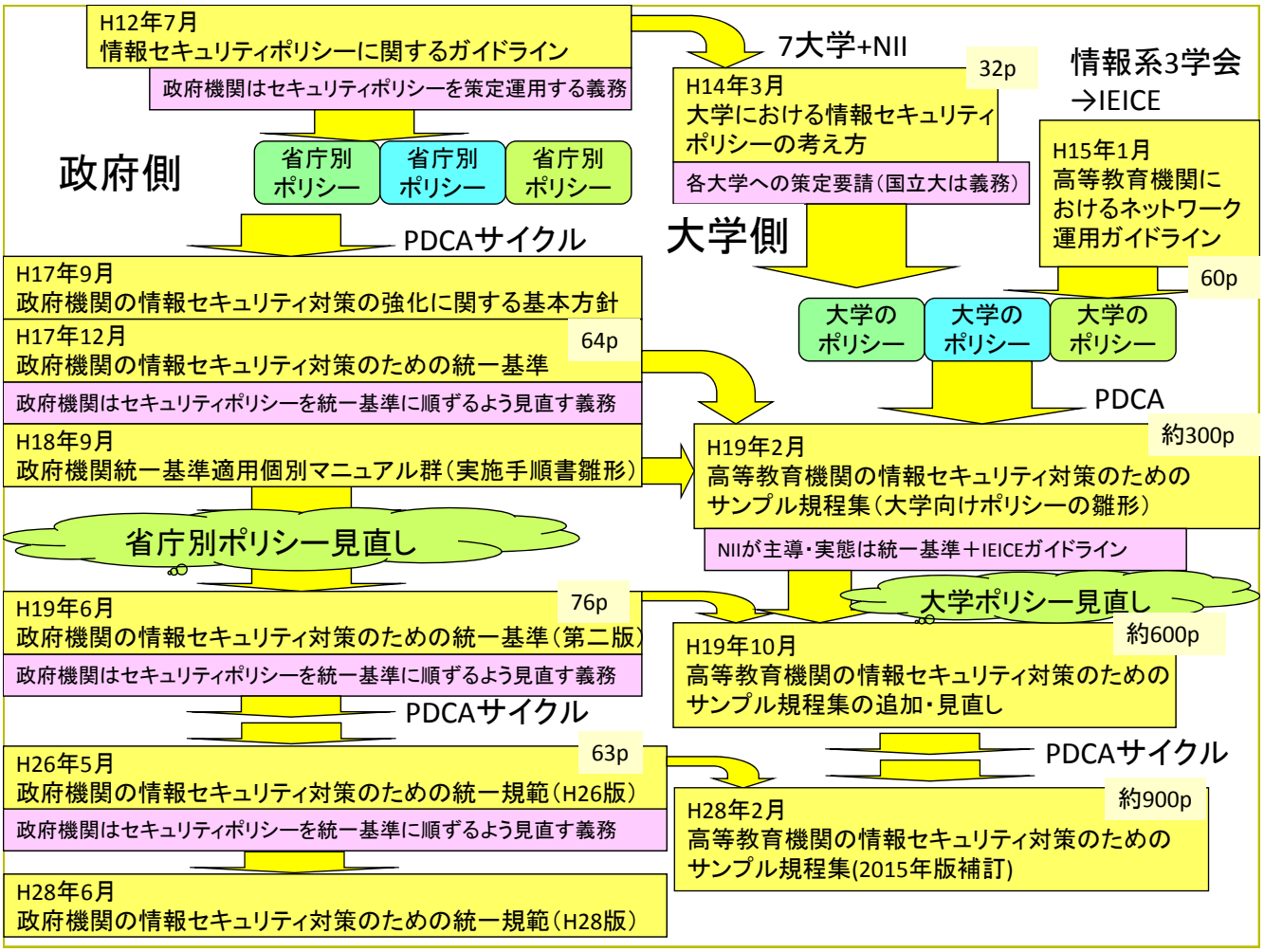
一般事務	教務	研究
○ガバナンス	△ガバナンス	×ガバナンス
△重要情報	◎重要情報	？重要情報
職員	学生	教員
ルールに従う時に官僚的	「お客様」だったり構成員だったり	組織の一員だったり個人事業主的だったり非常勤の人もいたり

何をするべきか？

- まずセキュリティポリシーをきちんと作る
  - 責任の所在とルールを明らかにし
    ガバナンスを確立する
- その上で実際の運用は重点領域から順に
  優先順位を決めて行うべきだが
  恐らく多くの組織にとって重要なのは
  「緊急時対応体制の確立」≒CSIRT設立
  - 特にSINET加入組織にとってはNII-SOCとの
    PoCを作る必要があるため

セキュリティのカナメ:
高等教育機関の情報セキュリティポリシー

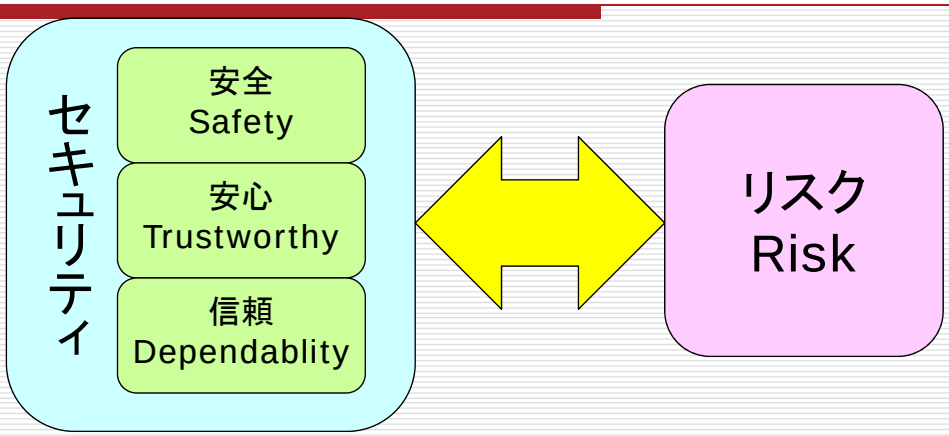
- H12年7月政府の「情報セキュリティポリシーに関するガイドライン」で大枠が決定
  - H14年3月「大学における情報セキュリティポリシーの考え方」
- H17年12月「政府機関の情報セキュリティ対策のための統一基準」を受けてサンプルが作られる
  - H19年2月「高等教育機関の情報セキュリティ対策のためのサンプル規程集」がNIIで作られる
- その後、政府機関統一基準はPDCAに従い
  改訂を繰り返し、サンプル規程集も追随



大学での情報セキュリティーポリシーは機能しているか

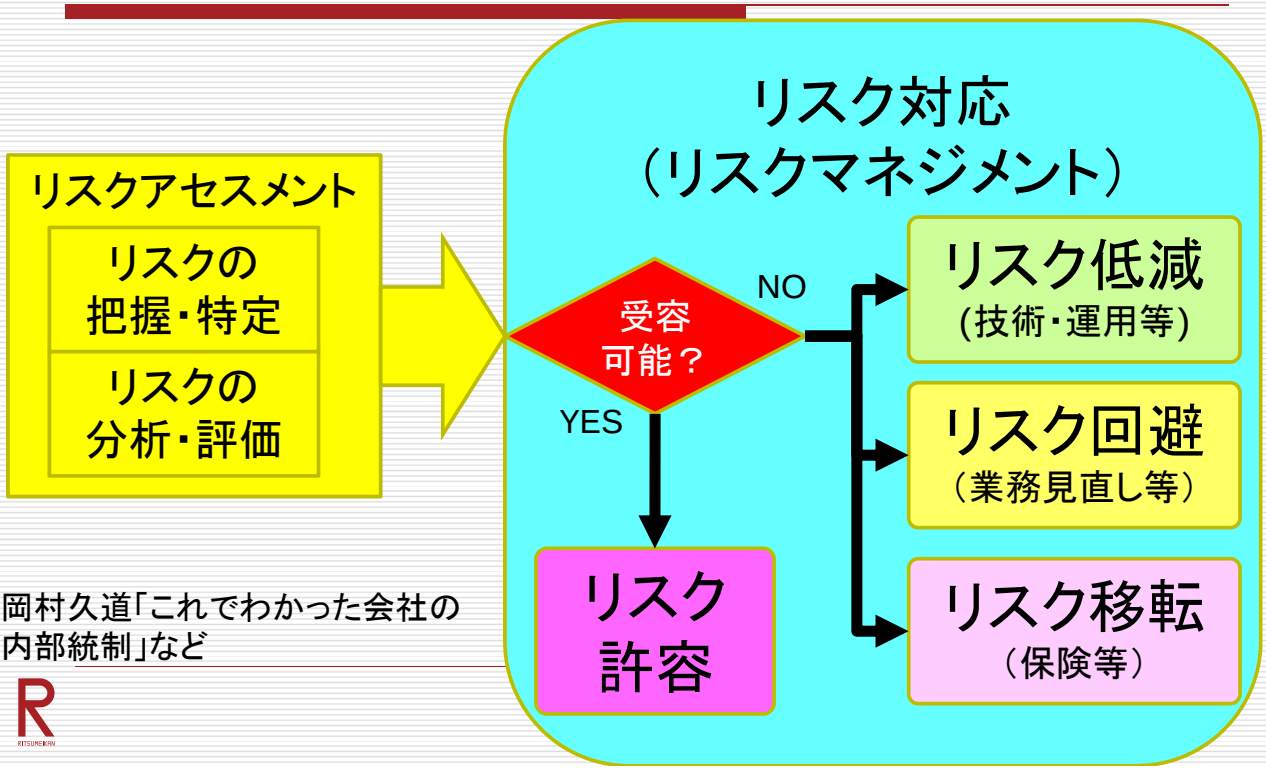
- 政府統一基準はほぼ毎年変更
- サンプル規定集は少し遅れて変更
- 各大学のレベルではどうか
  - PDCAが機能するためには組織にメスが必要
  - 国公立に比べて私学は…？
- そもそも大学はより「セキュア」になったか？
  - 変化する外的要因に対し
    リスクの見直しは出来ているか？？？

「セキュリティ」と「リスク」は表裏一体



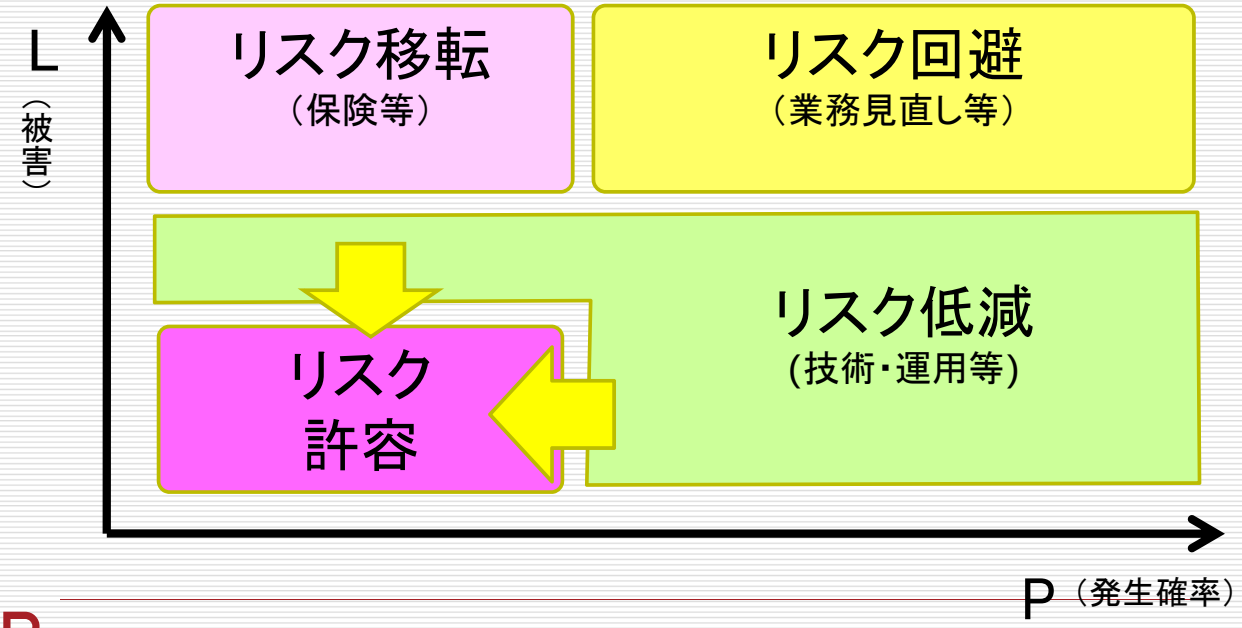
- セキュリティを高めるのが「セキュリティマネジメント」
  →それにより「リスク」が軽減する
  これに事故（インシデント）発生時対応を加えて
  「リスクコントロール」を実現する

リスクを評価し対応する



岡村久道「これでわかった会社の内部統制」など

リスクの大きさ・確率と対応の関係



佐々木良一：「ITリスクの考え方」より

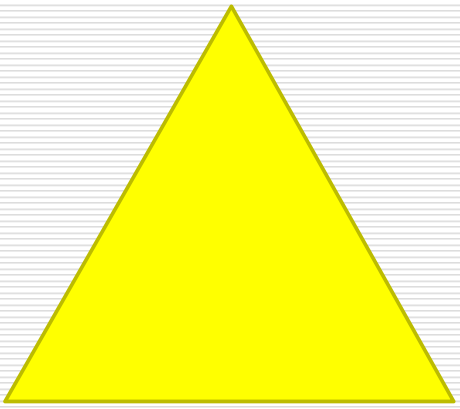
経営層とシステム管理者との間には まず「常識」の共有が必要・・・

- ITによる効率化は危機も呼び込むことになる
  （ブレーキのない車に人は乗せられない）
- システム調達の業者に全責任は負えない
  →事故発生時の被害は経営層が評価すべき
  →業務単位のリスク評価は経営層の責任
- リスク対策の勘所は「運用現場」にこそ見えている
  →細部のリスク対策は現場から上に上げるべき
  経営層はそのリスク対策の妥当性を評価し
  リソースを配分する
- 事故の発生確率は0にできない
  - だからこそ事故の予防策だけではなく
    事後対策が重要

リスク評価はトップダウン
リスク対策はボトムアップ

学長

重要業務の
リスク評価



教員・職員

重要情報の
リスク対策

情報・情報機器

執行部・経営層に求められること

- 重要な情報（機密）の保護にはコストがかかる
  - リソースの配分に権限がある人は
    細部のどこに重要な「情報」があるか
    理解が及ばない
  - 一方、重要な「業務」は把握しやすい
    リスクも想像が及びやすい

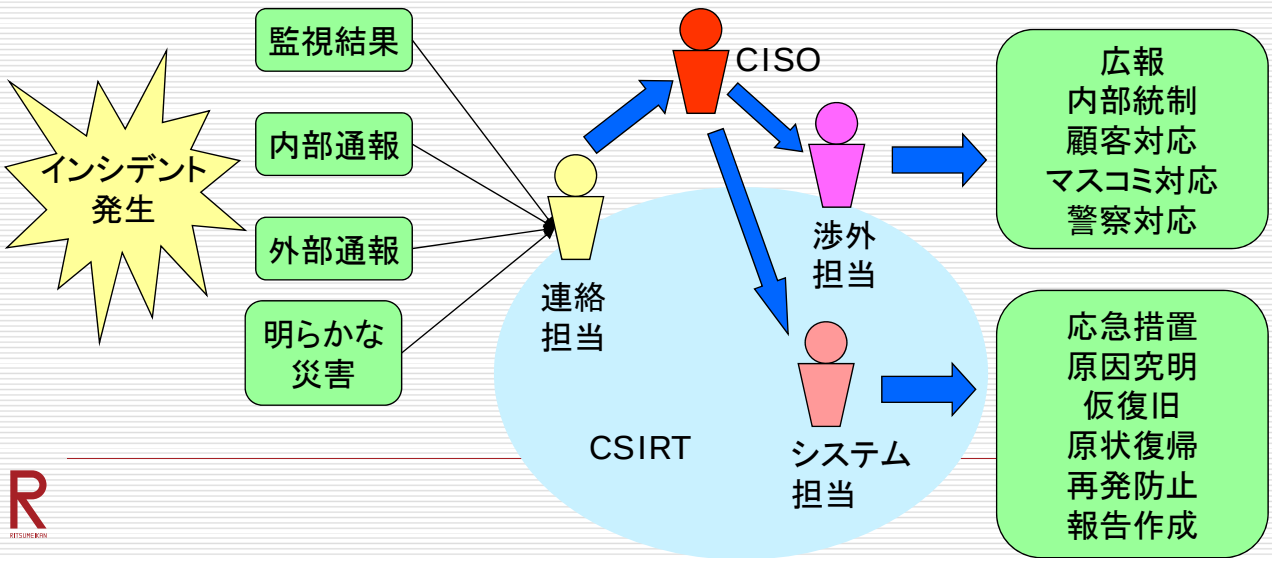
- 決定の迅速化、対策のメリハリ
  - 但し適切なリソース配分には
    結局細部のリスク評価が欠かせないことに注意
  - それを現場から「リスク対策案」とともに吸い上げる

インシデントレスポンスは どうあるべきか

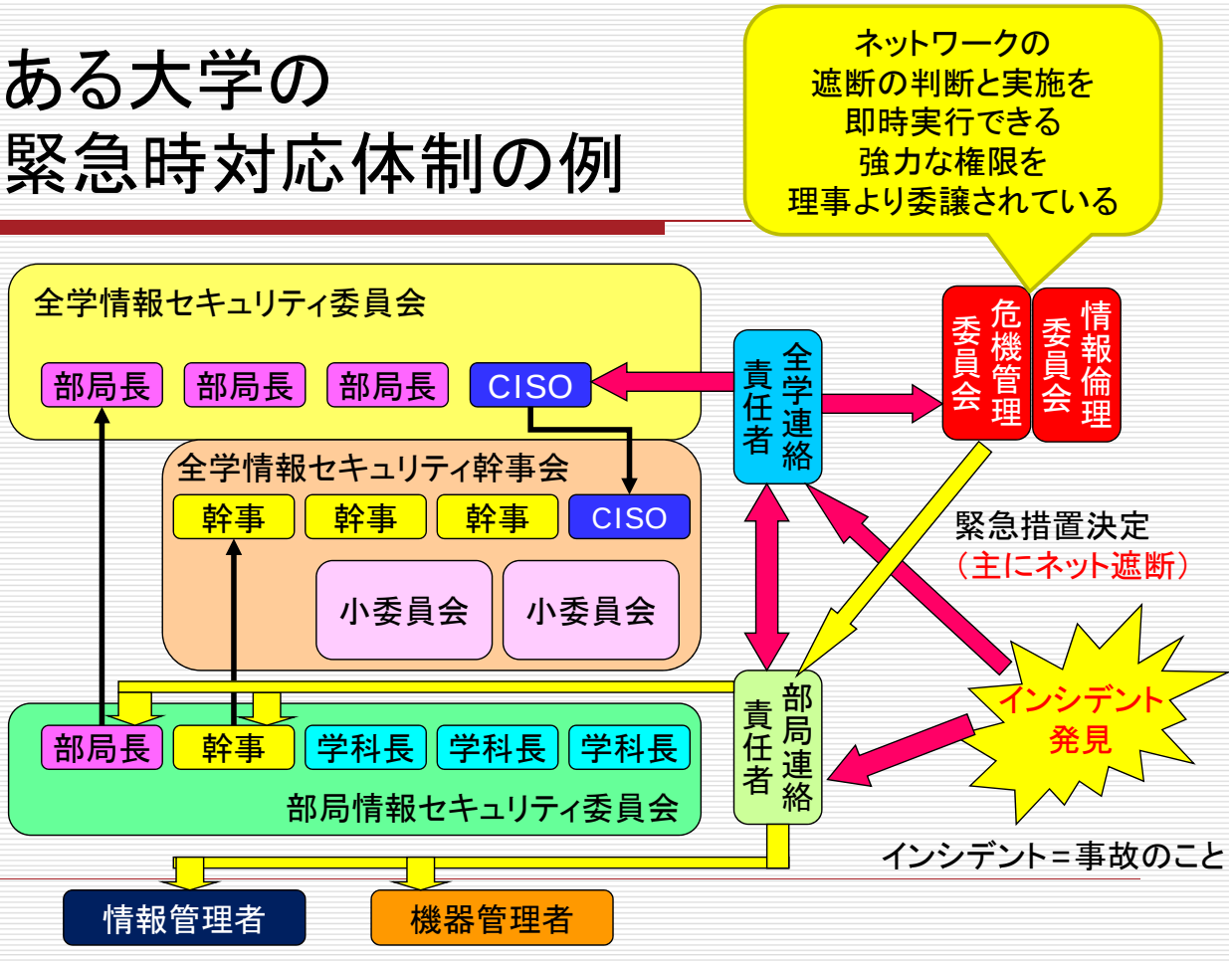
- 組織内体制の整備（CSIRT）が必要
  - シーサート（CSIRT: Computer Security Incident Response Team）とは、コンピュータセキュリティにかかるインシデントに対処するための組織の総称です。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をします。（日本シーサート協議会HPより）
- IRは技術だけでは不十分
  - 対処によっては教学に影響　経営判断にも直結
  - 法的対応には法務部門等とのリンクが不可欠
- セキュリティポリシーはマニュアル化が要だが IRは事前のマニュアルだけに頼れない
  - やや属人的になることは覚悟

緊急時対応計画の策定法

- イメージとしては「火災時の計画」
  - ただ、「消火」と「再発防止」まで自分でやる必要



ある大学の緊急時対応体制の例



役割分担

- CISO：権限を与え、対策を指示し、責任を負う
  - 緊急時の分限の範囲は予め決めておくべき
  - システム管理者は普段からCISOと密に連絡を
    - 信頼関係が必要　予算が必要な場合「お願い」も必要
    - 平時CISOがどれだけ理解しているかが事故時の対応の差
- 渉外担当・連絡担当（PoC）：情報を一元化
  - 外部組織と連携する必要がある時ことが多いので重要な任務
  - 情報公開が遅れても批判の矢面　事故時は専従が望ましい
  - 普段から同業他組織と交流があるとなおよい
- システム担当：CSIRTの実働部隊
  - 情報収集共有＆実際のトラブルシューター
  - 普段からリスクに関する情報収集をして共有
  - 必要に応じてCISOや実務部門に情報をあげる

大学におけるCSIRT

- NIIの「サンプル規程集」でも特に定義はない
  もともとそれほど定義に拘る必要はないはず
- CSIRTが「内部」に期待される機能
  - 脆弱性情報や攻撃トレンドなどの情報共有
  - インシデント対応のトレーニング
  - 非常時のインシデント対応支援
- CSIRTとして「外部」に期待される機能
  - インシデント観測時の連絡窓口
  - 他大学と連携したインシデント対応の調整役

大学CSIRT固有の機能

- そもそも情報機器に関した組織的管理体制が作りにくい
  - 特に教員や学生の存在
  - 事故発生時の連絡先が組織内でも把握しにくい
- 大切なのは…
  - 普段からの情報収集と共有を行うこと
    - そのためにも「アンテナの高い人」を確保しておく
  - その活動を通じて、普段から
    「重要なシステムにかかる情報を握るキーマンは
    それぞれ誰であるか？」を把握すること
- 構築のヒントとしては…普段から風通しを良く！
  - メーリングリスト、SNSなどを活用したら？

立命館におけるCSIRT構築

- そもそもセキュリティポリシーの改訂が遅れており、非常時対応体制も不明瞭
- 2015年4月　立命館情報基盤整備委員会発足
  - 常任理事会の下という位置づけ
  - 目的は情報基盤整備の推進と、クラウドや情報セキュリティなど専門化する整備に関しての共通化
  - 委員構成
    - 委員長：学術情報担当の副総長
    - 委員　：教学部長、一貫教育部長、総務部長、財務部長、APU事務局長、専門委員
    - 事務局：情報システム部

立命館におけるCSIRT構築

- 2015年4月　立命館情報基盤整備委員会のもとに情報セキュリティ専門部会を設置
  - 情報セキュリティ専門部会にてセキュリティポリシーと関連規程の見直し並びに緊急時対応体制(CSIRT)の検討に着手
- しかし…
  - 運営体制は委員長上原＋事務局
  - 緊急時対応体制の構成や規程の見直しについては学内での議論において何度も揺れ戻しがあり、検討から成立までに2年間を要する（今年4月ようやくまとまり、6月に常任理事会議決、7月にガイドライン制定）
  - 緊急時対応体制をCSIRTの名称を与えることは学内理解に時間がかかる→先送り

CSIRTに構築に役立つリソース

- NIIサンプル規程集
- 日本シーサート協議会の一連の資料
  - CSIRTスターターキットv2.0など
- JPCERT CSIRTマテリアル
- 米国NIST SP800-61
  「コンピュータインシデント対応ガイド」
  - IPAが日本語訳
- デジタルフォレンジック研究会が
  証拠保全についてガイドライン
  - http://www.digitalforensic.jp/
  - ただしこれはかなりシビアな（外部の専門家による調査が入るような）状況が想定されている