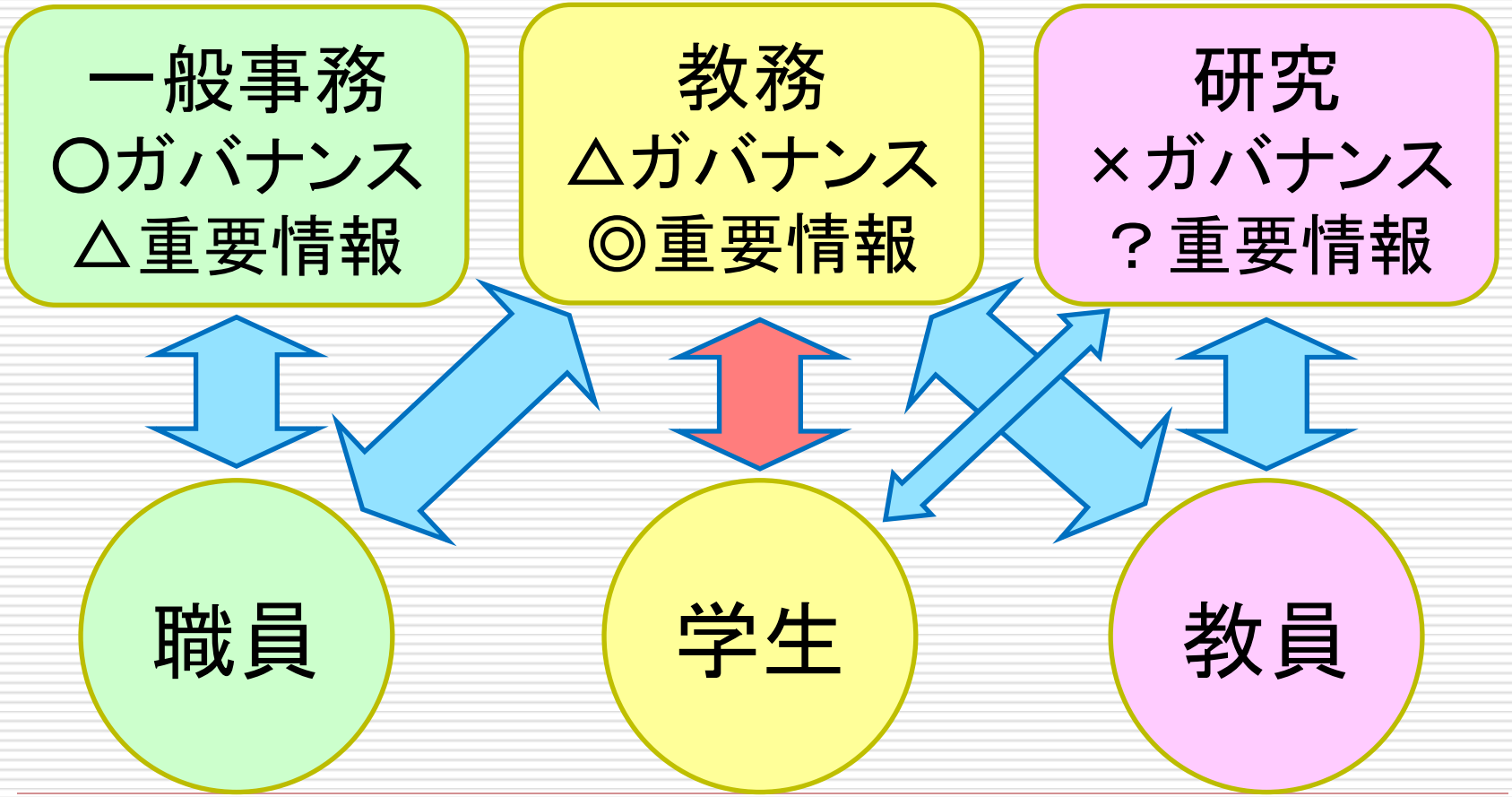
大学の情報セキュリティ

立命館大学
情報理工学部
情報システム学科
上原哲太郎

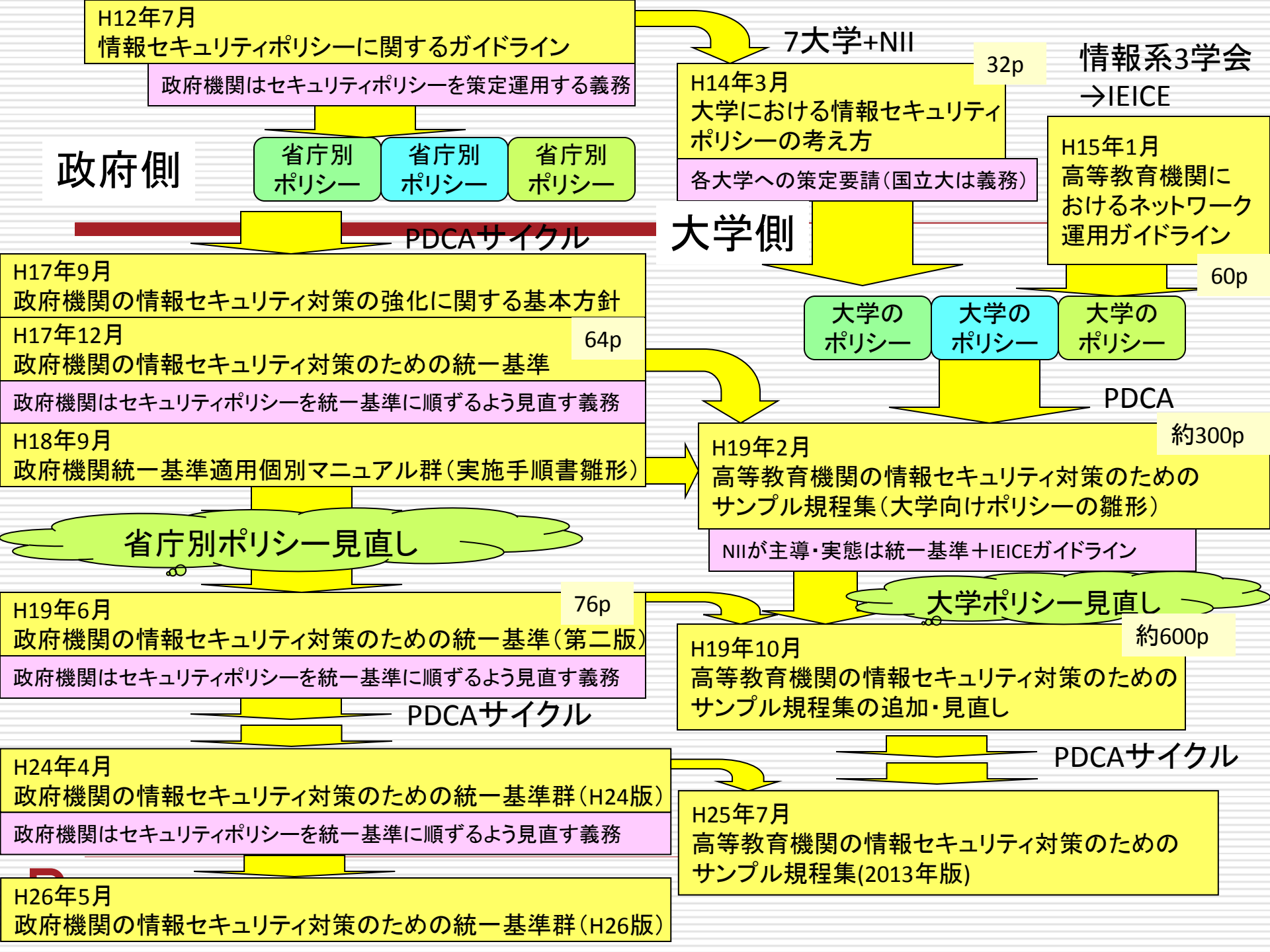
大学という組織の特殊性



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」
- その後、政府機関統一基準は改訂を繰り返す
  - 「高等教育機関の～サンプル規程集」も追随

RITSUMEIKAN


H12年7月
情報セキュリティポリシーに関するガイドライン
政府機関はセキュリティポリシーを策定運用する義務
7大学+NII
32p
情報系3学会
→IEICE
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
各大学への策定要請（国立大は義務）
H15年1月
高等教育機関におけるネットワーク運用ガイドライン
60p
政府側
省庁別ポリシー
省庁別ポリシー
省庁別ポリシー
大学側
PDCAサイクル
H17年9月
政府機関の情報セキュリティ対策の強化に関する基本方針
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
64p
政府機関はセキュリティポリシーを統一基準に順ずるよう見直す義務
大学のポリシー
大学のポリシー
大学のポリシー
PDCA
H18年9月
政府機関統一基準適用個別マニュアル群（実施手順書雛形）
約300p
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（大学向けポリシーの雛形）
NIIが主導・実態は統一基準＋IEICEガイドライン
省庁別ポリシー見直し
大学ポリシー見直し
約600p
H19年6月
政府機関の情報セキュリティ対策のための統一基準（第二版）
76p
政府機関はセキュリティポリシーを統一基準に順ずるよう見直す義務
H19年10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の追加・見直し
PDCAサイクル
PDCAサイクル
H24年4月
政府機関の情報セキュリティ対策のための統一基準群（H24版）
政府機関はセキュリティポリシーを統一基準に順ずるよう見直す義務
H25年7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(2013年版)
H26年5月
政府機関の情報セキュリティ対策のための統一基準群（H26版）

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？？？

かつてのリスク要因

- 「踏み台」
  - サーバ乗っ取り
    →他への攻撃
    SPAMばらまき
  - Bot植え付け
- 学生の「悪さ」
  - 著作権違反事案など
- 「個人情報漏洩」
  - 多くは事故
    （紛失＆盗難）
  - 被害実態はとにかく
    報道＆世論は
    漏洩件数に敏感
    →ブランド毀損を
    避けるために
    対策が必要

結局、あまり直接的被害ではなかった…

RITSUMEIKAN

しかし今はサイバー犯罪は「金になる」

- 2013年「リスト型アカウント攻撃」の急増
- ネットバンキング等を狙った不正送金激増
  - 2012年　64件　4800万円
    2013年　1315件　14億円　今年はそれ以上
  - 特に法人向け口座が狙われる
  - マルウェアの高度化
- 詐欺手口の多様化
  - SNSアカウント乗っ取りによる詐欺など

2011年頃から我が国において重要機関における事故が続く

- 2011年9月　三菱重工へのサイバー攻撃
  - 防衛関連機密が狙われたとみられる
- 2011年10～11月　衆参両院へのサイバー攻撃
  - 標的型メール攻撃を用いてサーバに侵入
    議員のメールが盗み見されるなどの被害
- 2011年11月　総務省に標的型メール攻撃
  - 詳細不明
- 2012年1月　JAXAでウィルス感染発覚
  - NASA関連技術を含む重要機密が漏洩
- 2012年7月　財務省でウィルス感染発覚
  - 過去2年にわたって継続的に情報漏えい？
- 2013年1月　農水省へのサイバー攻撃
  - 内部文書124点（うち機密性2が85点）流出
    TPP交渉に関わる記録など漏洩

RITSUMEIKAN

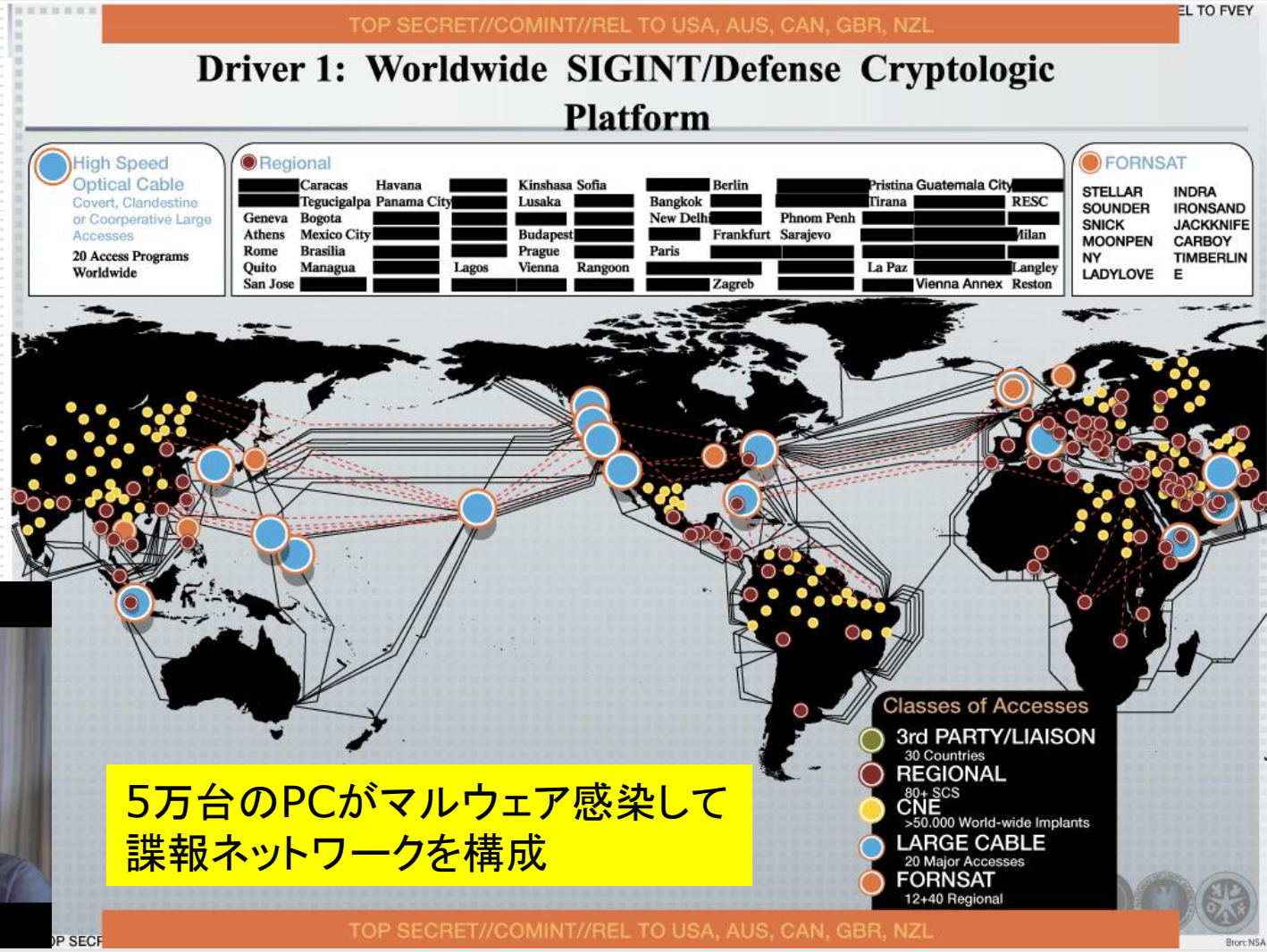
2013年
最高レベルの企業が次々に

- 2月　巨大ネット企業が相次いで被害
  - facebookにゼロデイ攻撃
  - Apple, Javaの脆弱性を突かれマルウェア感染
  - Microsoft Mac製品開発部門が被害
- 5月 Yahoo!Japanの認証サーバに攻撃
  - 最大2200万件のID＋PWハッシュが流出
  - 146万人分の「秘密の質問」流出
- 韓国では2波に渡る攻撃が
  - 3月　銀行やテレビ局に対する業務妨害
  - 6~7月　政府機関やメディアに対する妨害
  - 4年前から続く一連の攻撃の一部？

http://thenypost.files.wordpress.com/2013/10/snowden2.jpg

http://media2.mic.com/2025d8c2dd70ab46920521643da58d9f.jpg

そして大きな問題



5万台のPCがマルウェア感染して
諜報ネットワークを構成

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
- 破壊工作・諜報

さらに外部か内部かなど…

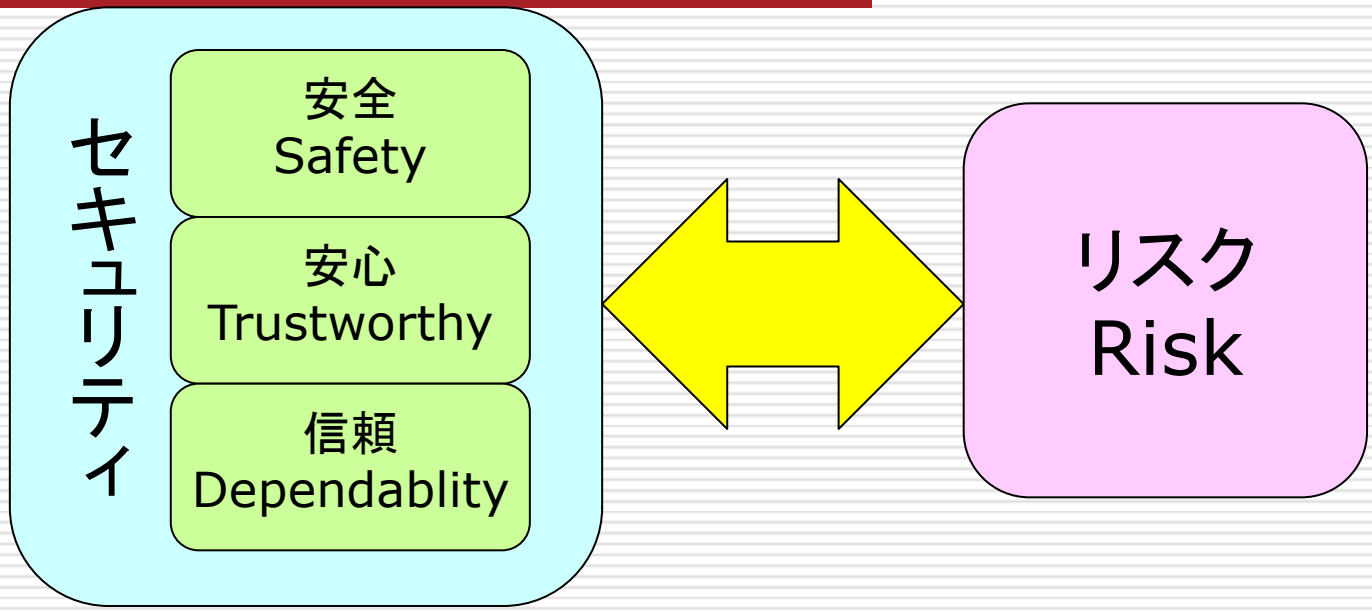
いま大学が本当に恐れるべきは…

- 「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…？

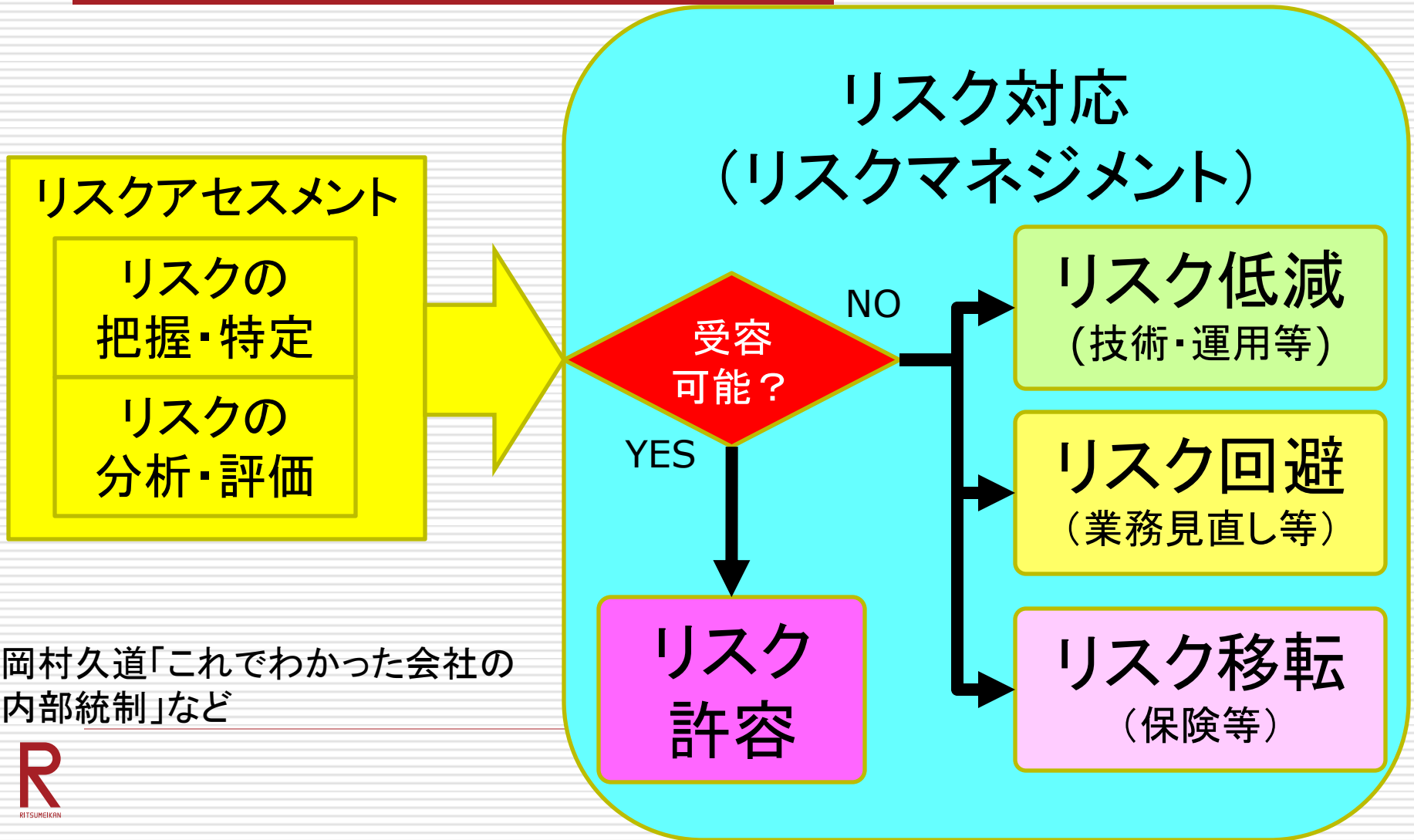
RITSUMEIKAN

「セキュリティ」と「リスク」は表裏一体



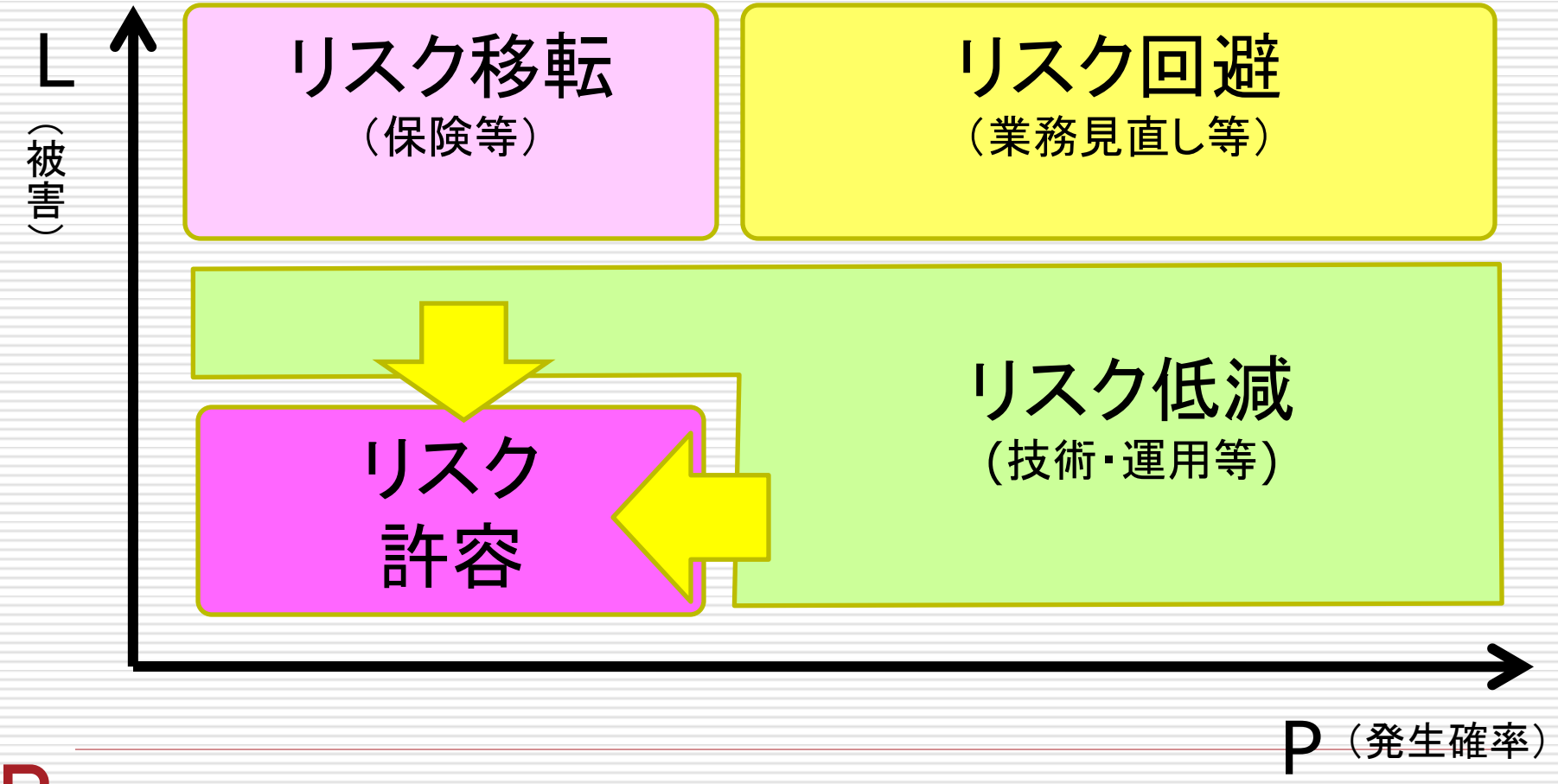
- セキュリティを高めるのが「セキュリティマネジメント」
  →それにより「リスク」が軽減する
  これに事故（インシデント）発生時対応を加えて
  「リスクコントロール」を実現する

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

ITリスクの特殊性

- ITが生む利便性は比較的見えやすいが
  同時に持ち込むリスクはなかなか見えない
  - 運用コストや情報セキュリティ上の危機の見えにくさ
- ITは複雑な技術：評価が難しい
  - たとえ利便性が見えても、必要性や費用対効果の即断は困難
- ITによるインシデントは発生確率が
  外的要因に激しく左右される
  - 脆弱性の発見、攻撃法の流行、見えない「攻撃者の意思」
  - 攻撃力は「資金」や「マンパワー」ではなく
    純粋に「技術」で決まる
- ITでは「生産者責任」がなかなか取られない歴史的経緯
  - いくらバグを出しても免責されるソフトウェア会社

経営層やシステム管理者に求められる常識・・・

- ITによる効率化は危機も呼び込むことになる
- 業者はリスクには責任を負わない・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

- 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も重要

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

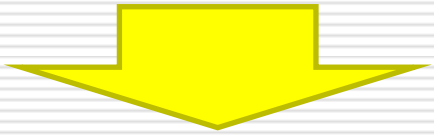
教員・職員

重要情報の
リスク対策

情報・情報機器

トップダウンのメリット

- 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

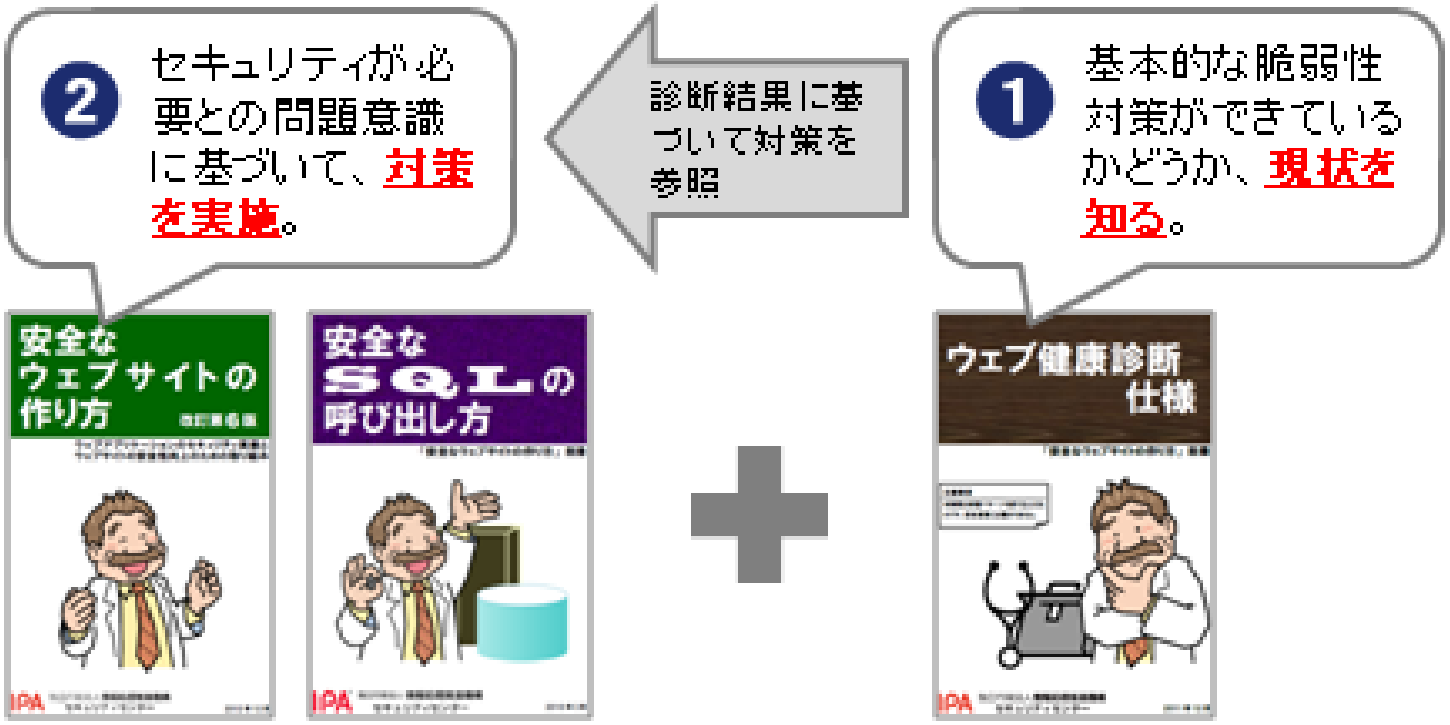
重要業務領域に対して…

- 情報セキュリティ対策を適切に講じる
  - まずは王道をしっかり＝入口対策
    - 「入口を狭く」ファイアウォール・多段proxy・認証強化・VPN
    - 「入口での検知」ウィルス対策・IDS・スパムフィルタ
    - 「入られないように」脆弱性対策・URLフィルタリング
  - 入られた後の被害を押さえる＝真中対策～出口対策（内部犯行対策も兼ねる）
    - 暗号化の適用・重要なデータの分離
    - ログ監視・分析・アノマリ検出
- インシデントレスポンス＆フォレンジックス
  - 被害拡大の防止
  - 正確な被害の特定→原因特定→再発防止
    何より事故は起こることを前提にする

堅牢なシステムはまず
堅牢なWebシステムから

- 発注時に「健康診断」を

例えば
IPAの
一連の
文書を
参照



安全なウェブサイトの作り方

[別冊]
安全なSQLの呼び出し方

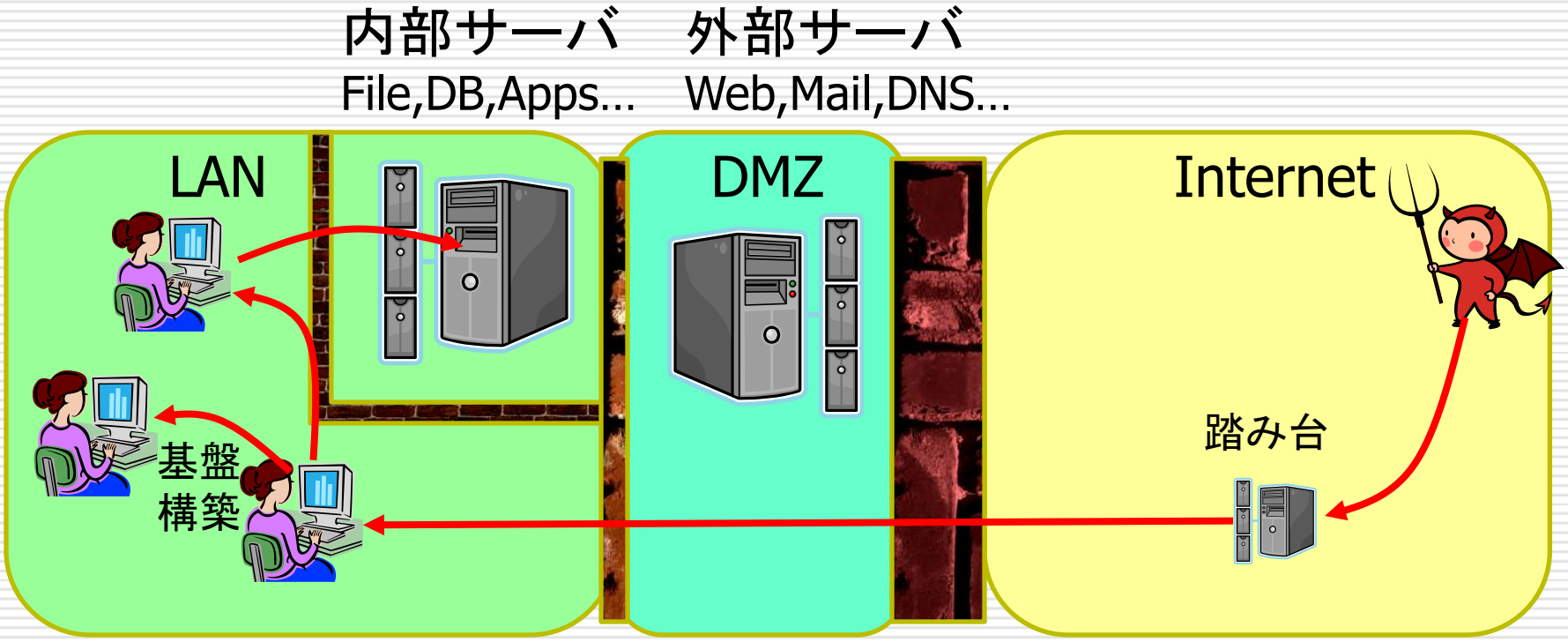
[別冊]
ウェブ健康診断仕様
（今回追加）

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」
- 攻撃の各段階で可能な限り
  攻撃者の手を縛る「意地悪セキュリティ」

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

侵入→基盤構築→目的達成


内部サーバ
File,DB,Apps…
外部サーバ
Web,Mail,DNS…
LAN
DMZ
Internet
基盤
構築
踏み台

IPA「高度標的型攻撃」に向けたシステム設計ガイド

IPA「高度標的型攻撃」対策ガイドにおけるシステム対策リスト（一部）

セット No	前版との対応*	対策セット名称	統制目標
対策セット A	断①	ネットワーク通信経路設計によるコネクトバック通信の遮断	ユーザ端末から直接インターネット上の C&C サーバへ接続するコネクトバック通信を遮断および検知する。
対策セット B	断③ ＋ 視①	認証機能を活用したコネクトバック通信の遮断とログ監視	ユーザ端末から認証機能を持たないプロキシを突破して C&C サーバへ接続するコネクトバック通信を遮断および検知する。
対策セット C	断② ＋ 視②	プロキシのアクセス制御によるコネクトバック通信の遮断と監視	CONNECT メソッドを利用してセッションを維持するコネクトバック通信を遮断および検知する。
対策セット D	断④ ＋ 断⑤	運用管理専用の端末設置とネットワーク分離と監視	ユーザ端末に保存されている重要情報（運用管理業務で使われている管理者情報や機微情報など）の窃取を防止し検知する。
対策セット E	断⑦ ＋ 視⑤ ＋ 新規視③	ファイル共有の制限とトラップアカウントによる監視	攻撃者によりリモートコントロールされたユーザ端末から、周囲のユーザ端末へファイル共有機能を悪用した内部侵害拡大を防止する。また、ファイル共有が業務上必要な場合は監視を強化し、不正なファイル共有機能の利用を検知する。
対策セット F	断⑥ ＋ 新規視④	管理者権限アカウントのキャッシュ禁止とログオンの監視	攻撃者に管理者権限のアカウント情報を窃取させない。および、万が一窃取されたときも管理者権限のアカウントの不正使用を検知する。

*対応 ： 前版にて記載したシステム設計対策セットとの対応　【凡例】 断: 遮断策　　視: 監視策

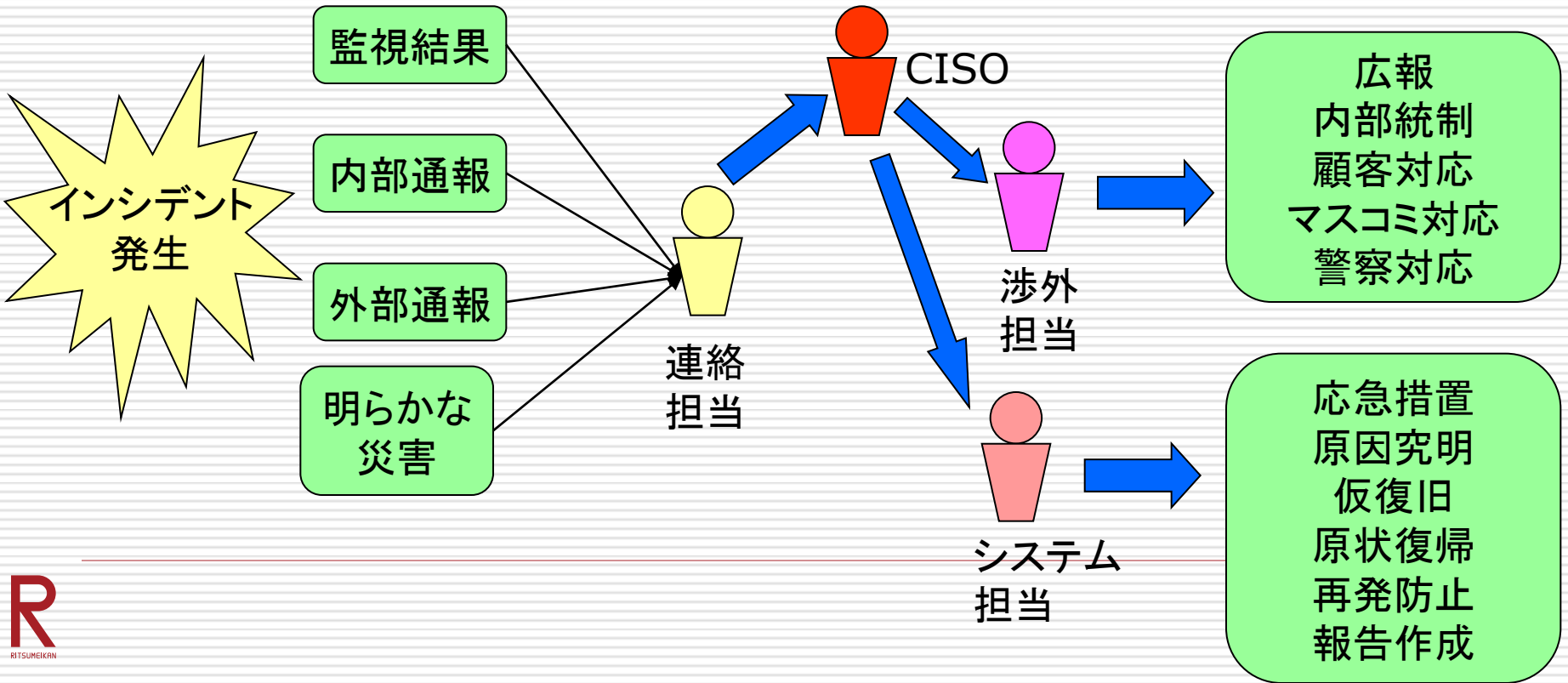
- 設定変更で可能な対策を中心に具体的に列挙

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
  - 営利企業では対処は経営判断に直結
  - 法的対応には法務部門等とのリンクが不可欠

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



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と仲良く♪
    - 信頼関係が必要　予算が必要な場合「お願い」も必要
    - 必要に応じてCISOを普段から「教育」しておく
- 渉外担当：情報を一元化
  - 勝手にそれぞれが応対すると混乱を招く（特にマスコミ相手）
  - 情報公開が遅れても批判の矢面　だから専従は必須
  - ただし独断で動いてはいけない
- システム担当
  - 実際のトラブルシューター
  - 必要に応じてCISOや渉外に情報をあげる

終わりに

- セキュリティポリシーの認知はもう上がらない？
- PDCAがあまり回ってる気がしない
  - 形骸化の危険

- 一方でリスク要因の変化は大きい
  - 特に内部犯行はあまりこれまで語られなかったが
    今後は怖いのでは…

- 結局、大きな事故が起きるまで
  現状は続くのでしょうか…

必要なリソース

- IPAがいくつもよい資料を作っています
  - https://www.ipa.go.jp/security/vuln/newattack.html
- インシデントレスポンスについては
  米国NIST SP800-61をIPAが日本語訳
  - https://www.ipa.go.jp/security/publications/nist/
- 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