マイナンバーに対応した情報システム設計とセキュリティ対策

立命館大学
情報理工学部

上原哲太郎

情報システムと「法」

- 情報システムが法的義務を満たす必要がある例が増えてきている
  - 特定電子メール法や特定商取引法における表示義務
  - 割賦販売法におけるクレジット番号の安全管理措置
  - 個人情報保護法における安全管理措置
  - 不正競争防止法における営業秘密管理指針 etc.
- これにマイナンバー法（番号法）が加わる
  - 対象となる事業者が大変広範に
  - しかもわかりにくい

目次

何をやらねばならぬのか？

（特定）個人情報保護委員会のガイドライン事業者編がバイブル

H26.12.11版は総ページ数61ページ

だが「わかりにくい」

わかりやすくする工夫はある

- 特定個人情報保護委員会のWebページに分かりやすい資料がいっぱい
  http://www.ppc.go.jp/legal/policy/document/

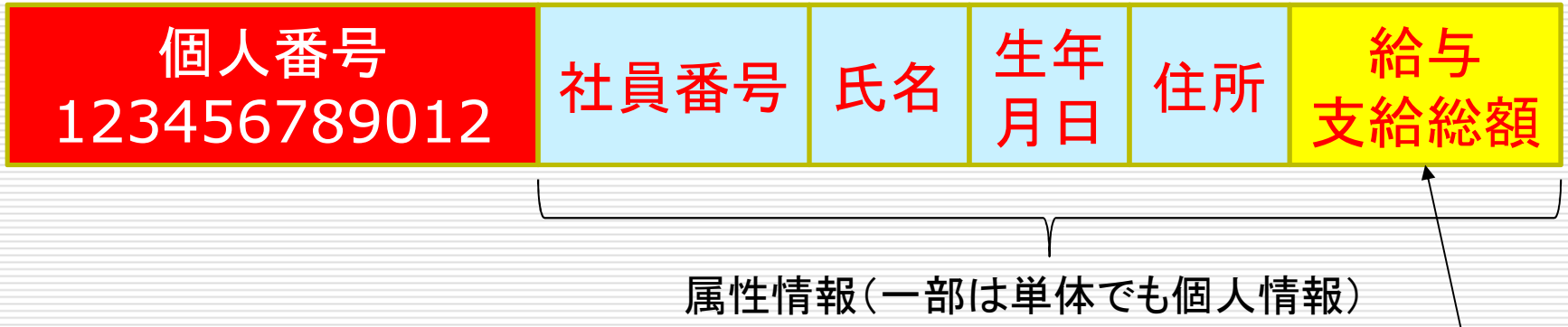
RITSUMEIKAN

それでも難しい…何故か？

- 「個人情報保護法」を理解していないと…
  - 法の「理念」「建て付け」
  - 個人情報の定義、個人情報ファイルの定義など
- 五月雨式に法改正が待っている
  - 改正個人情報保護法の施行もある
  - 適用範囲拡大に伴う細かい改正が追いかける
- 基本を押さえることが大切

特定個人情報とは何か

- 「個人番号を含む個人情報」
  - 個人番号＝番号法における個人番号
  - 個人情報＝個人を識別できる情報を含む情報
    （ただし特定個人情報においては死者を含む）
  - 個人番号∈個人情報



どこまでいっても特定個人情報

- 正規化してあっても…

社員番号	個人番号 123456789012

社員番号	氏名	生年 月日	住所	性別

社員番号	給与 支給総額

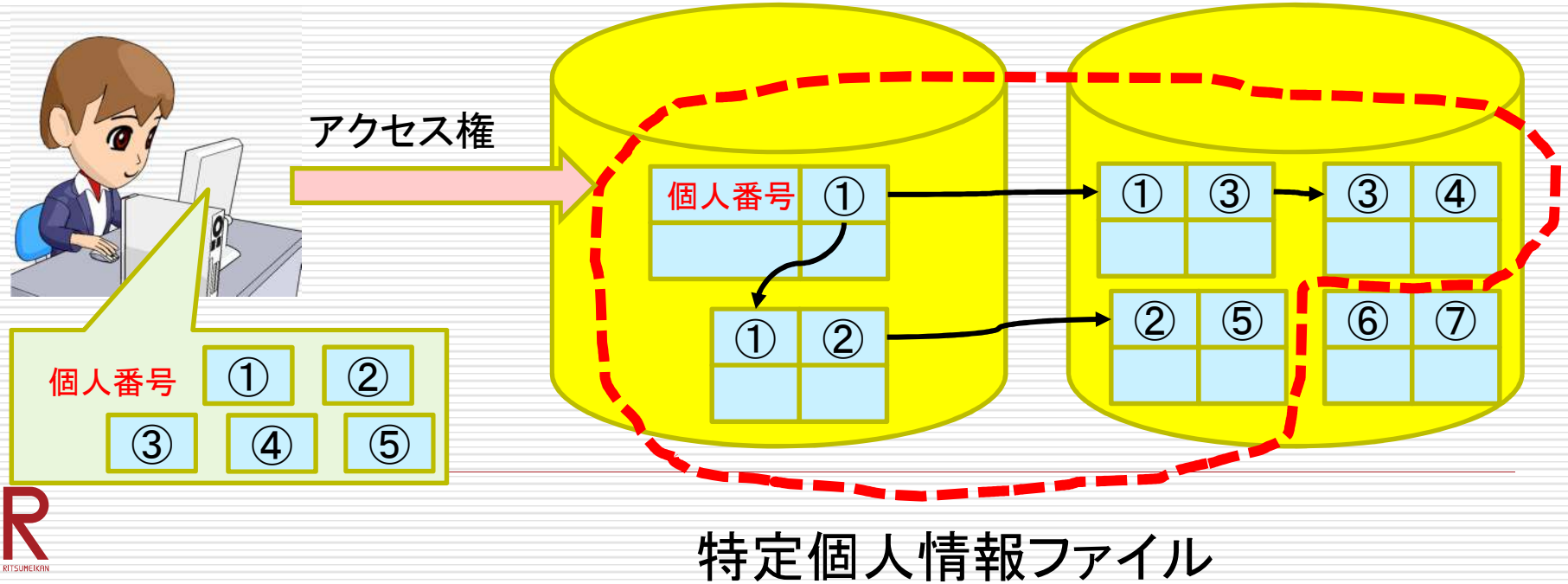
全レコードに
アクセス権を持つ者にとっては
全てが特定個人情報

特定個人情報ファイルとは何か

- 個人番号をその内容に含む個人情報ファイルまたは個人情報データベース等をいう
  - 個人情報ファイルとは個人を含む情報の集合体であって、個人情報を検索できるように体系的に構成したもの（行政機関個人情報保護法および独法等個人情報保護法における定義）
  - 個人情報データベース等は個人情報保護法における定義で条文は同じ
- 「ファイル」「データベース」に引きずられると理解を誤る

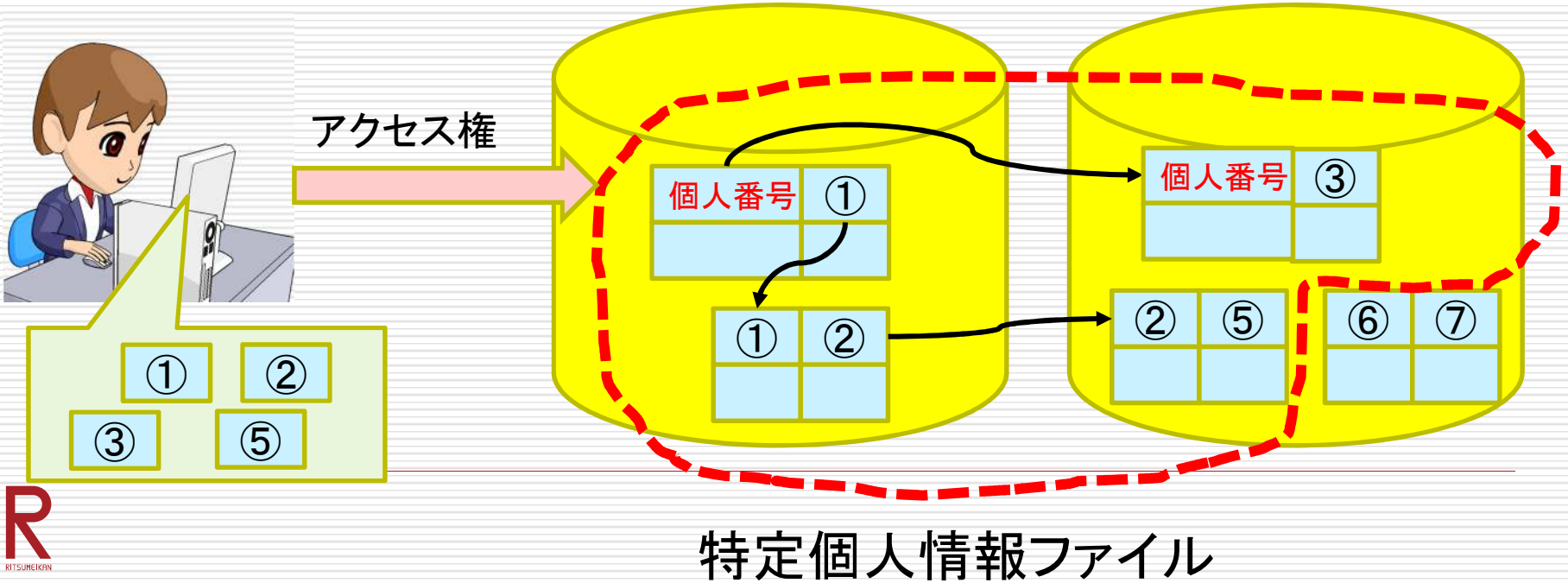
「個人番号をその内容に含む個人情報ファイル」とは

- 「個人番号にアクセスできる者が、個人番号と紐付けてアクセスできる情報」
  - 単なるファイルやテーブルを指していない（データベース正規化を意識）



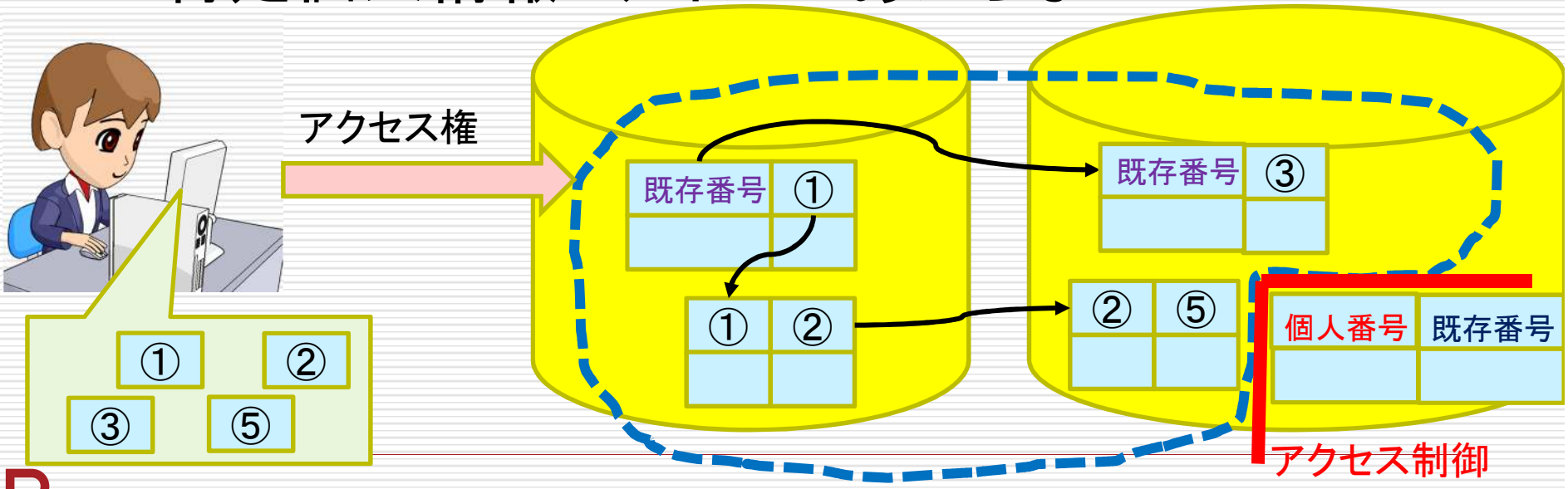
特定個人情報ファイルの
わかりにくさ

- 内部で検索キーとして個人番号が利用され
  紐付けてアクセスできるなら
  画面上に見えなくとも特定個人情報ファイル



既存の番号で連携してるDBは？

- 既存の番号で紐付けが行われていても
  個人番号そのものにアクセスできないよう
  アクセス制御がなされていれば
  特定個人情報ファイルにあたらない



特定個人情報ファイルではない

既存番号など「他の番号」の扱い

- 個人番号から「一定の法則により」
  生成される番号は個人番号と同等に扱う
  - 「ハッシュ化」「暗号化」も同じ扱い

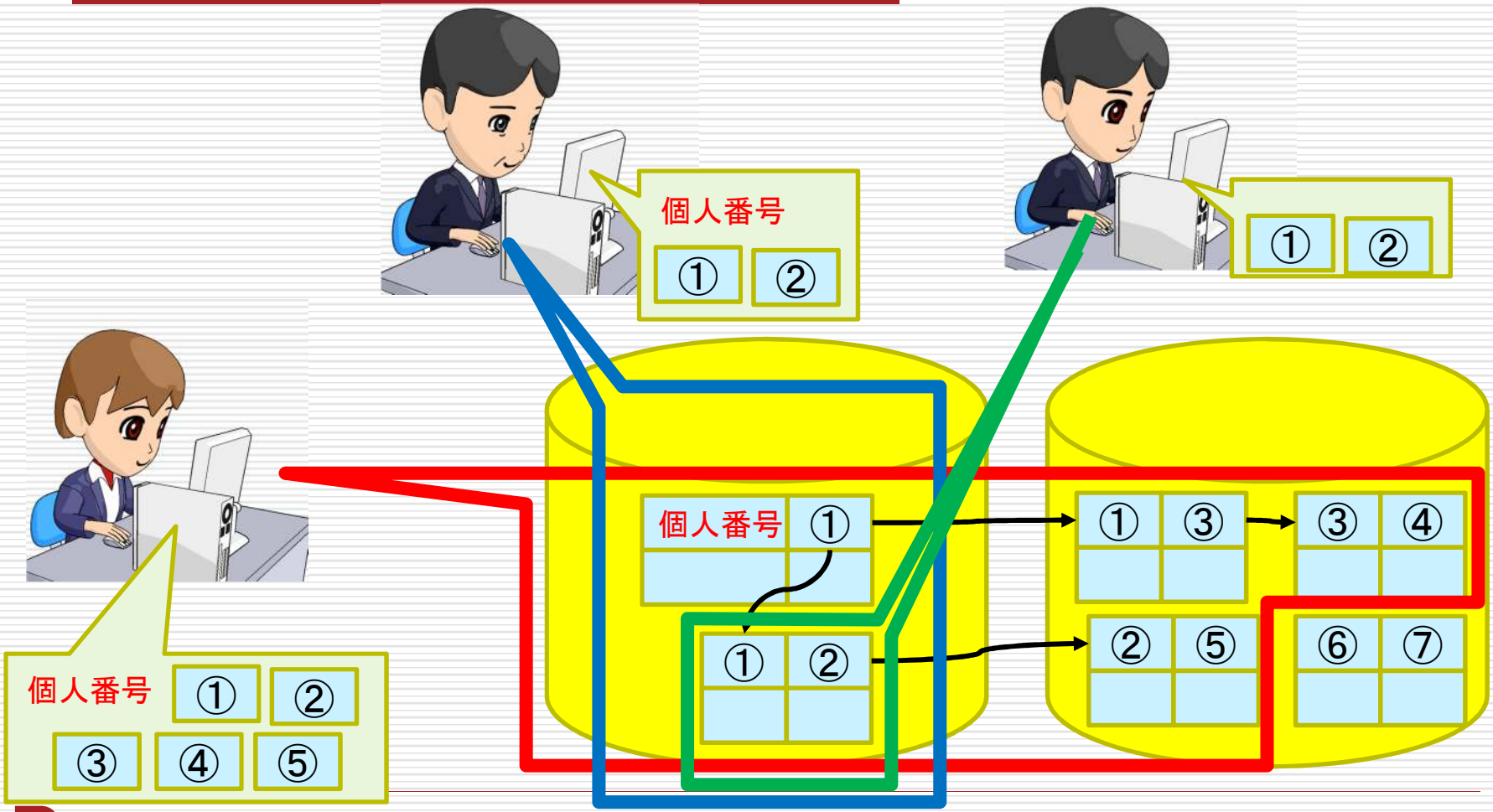
- 個人番号と無関係の番号が
  個人番号と紐付けされている場合は
  対応表へのアクセス制御で
  特定個人情報ファイルになるか否か変わる

業務とシステムと
特定個人情報ファイル

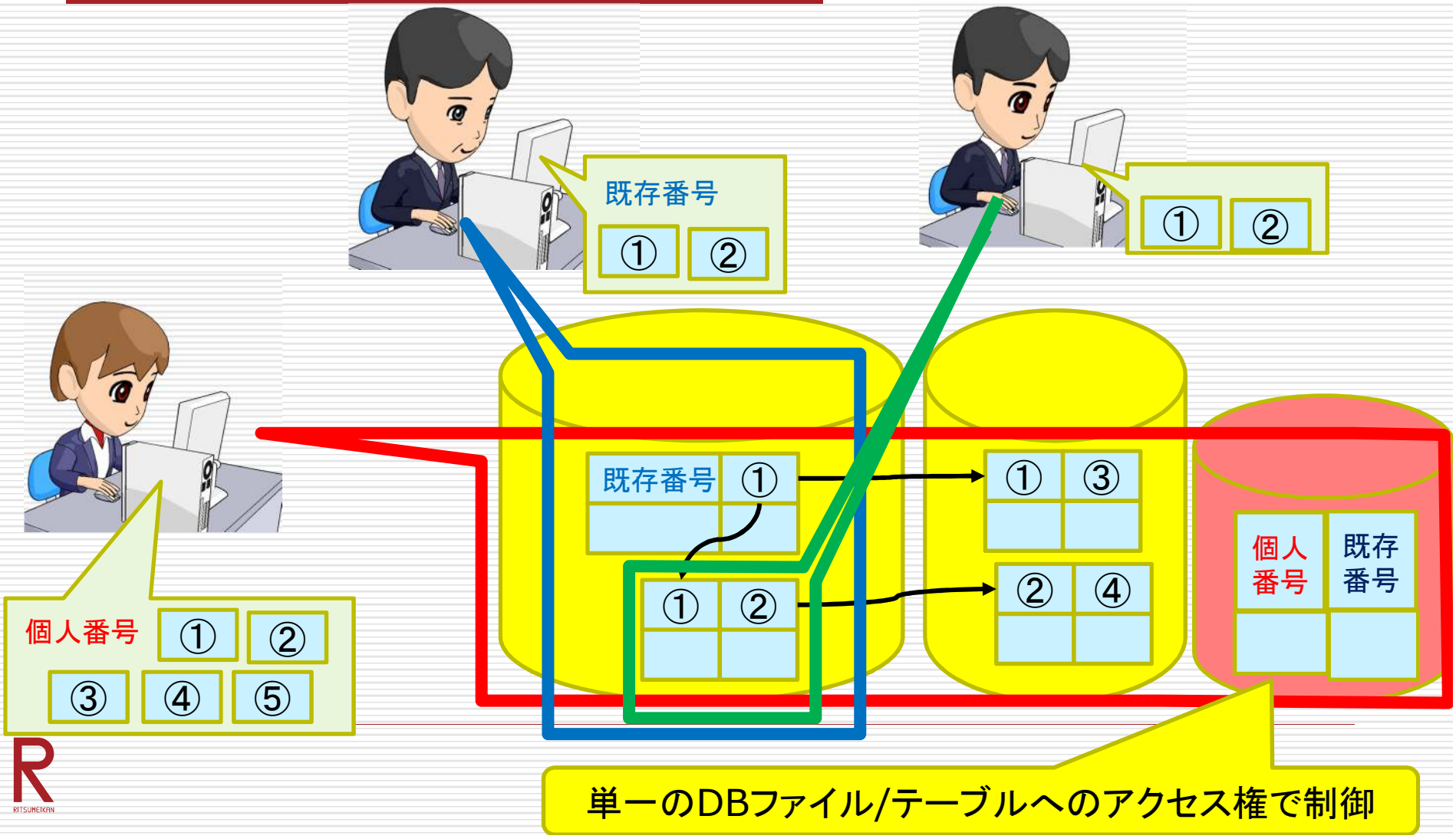
- 各業務において求められるのは…
  - 業務従事者の限定と適切なアクセス権付与
- システムに求められるのは…
  - 業務に応じたアクセス権においてアクセスできる
    データを最小限に
- これがシステムとして設計できて初めて
  「特定個人情報ファイル」が定義できる
- 同一システムを複数業務で使うと
  「特定個人情報ファイル」が複雑に

R
RITSUMEIKAN

アクセス制御されている範囲が特定個人情報ファイルの定義に反映



アクセス権制御を単純にする



特定個人情報の取扱いとシステム上の義務

- 取得時は「利用目的を通知」義務
  - どの事務に利用するのか示せば良い（税申告etc）
    →システムで取得するなら表示した方が良い
- 取扱い時は「実施者」のみが参照可能に
  - アクセス制御の厳格化・ログなど取扱い履歴の取得
  - バックアップ等のシステム管理上の参照はどうする?
- 保管は認められた期間のみ
  - 法定の年限が来たら個人番号だけ消去などのシステム化が必要（特にバックアップ問題）

安全管理措置

- 考慮すべきは番号法＋個人情報保護法
  ＋番号ガイドライン＋主務大臣ガイドライン
- 手順
  1. 個人番号を取り扱う事務の範囲の明確化
  2. 特定個人情報等の範囲の明確化
  3. 事務取扱担当者の明確化
  4. 基本方針の策定
  5. 取扱規程等の策定
- ワークフロー整理→ルール化→システム化

R
RITSUMEIKAN

安全管理措置はガイドラインの別添

- その内容はISMS的
  - 基本方針の策定
  - 取扱規程の策定
  - 組織的安全管理措置
  - 人的安全管理措置
  - 物理的安全管理措置
  - 技術的安全管理措置

組織的安全管理措置とは

- 組織体制の整備
  - 責任者・担当者の明確化
  - 事故時の連絡体制の整備など
- 取扱規程に基づく運用
  - システムログや利用実績の記録
- 取扱状況を確認する手段の整備
  - ログには特定個人情報は記載しない（！）
    - 「既存番号」の活用
- 情報漏えい等事案に対応する体制の整備
- 取扱状況の把握及び安全管理措置の見直し

物理的安全管理措置とは

- 特定個人情報等を取り扱う区域の管理
  - 要するに壁を仕切るなどしてくれということ
  - 入退室管理も例示されている（！）
- 機器及び電子媒体等の盗難等の防止
  - 金庫に入れたりワイヤー付けたり
- 電子媒体等を持ち出す場合の漏えい等の防止
  - 暗号化やパスワードを入れる
- 個人番号の削除・機器及び電子媒体等の廃棄
  - 特に媒体の復活防止

技術的安全管理措置とは

- アクセス制御
- アクセス者の識別と認証
- 外部からの不正アクセス等の防止
  - ファイアウォール
  - マルウェア対策
  - 脆弱性管理
  - ログ解析
- 情報漏洩の防止
  - 外部送信時の暗号化と認証など

こういうときは「リスクポイント」が大事

R
RITSUMEIKAN

必要な情報はここにまとまってます

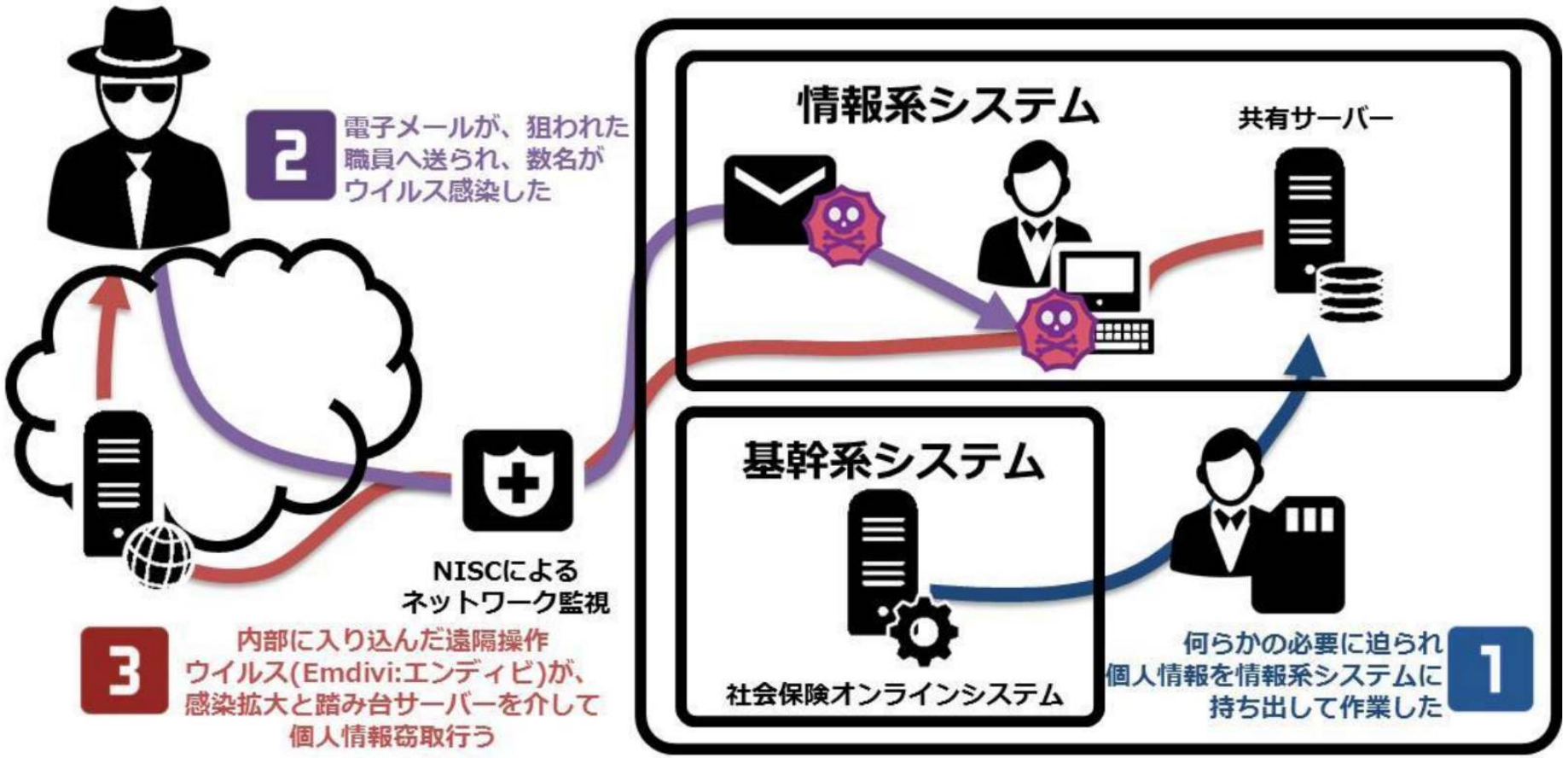
特定個人情報保護委員会
ガイドライン資料集
http://www.ppc.go.jp/legal/policy/document/

内閣官房
マイナンバーHP
http://www.cas.go.jp/jp/seisaku/bangoseido/

しかし昨今の状況は厳しい

- 外部からの攻撃
  - 標的型攻撃に代表される「サイバー企業スパイ」
  - 特に中小企業を狙ったネットバンキングへの攻撃
  - 広がるランサムウェア：「データを人質に」
  - 業務妨害としてのDDoS攻撃⇒脅迫
- 内部犯罪の広がり
  - 顧客情報や技術情報の故意の持ち出し
- 内部では事故にも注意
  - 減らない情報の紛失や誤送信

年金機構事件の大きな構図

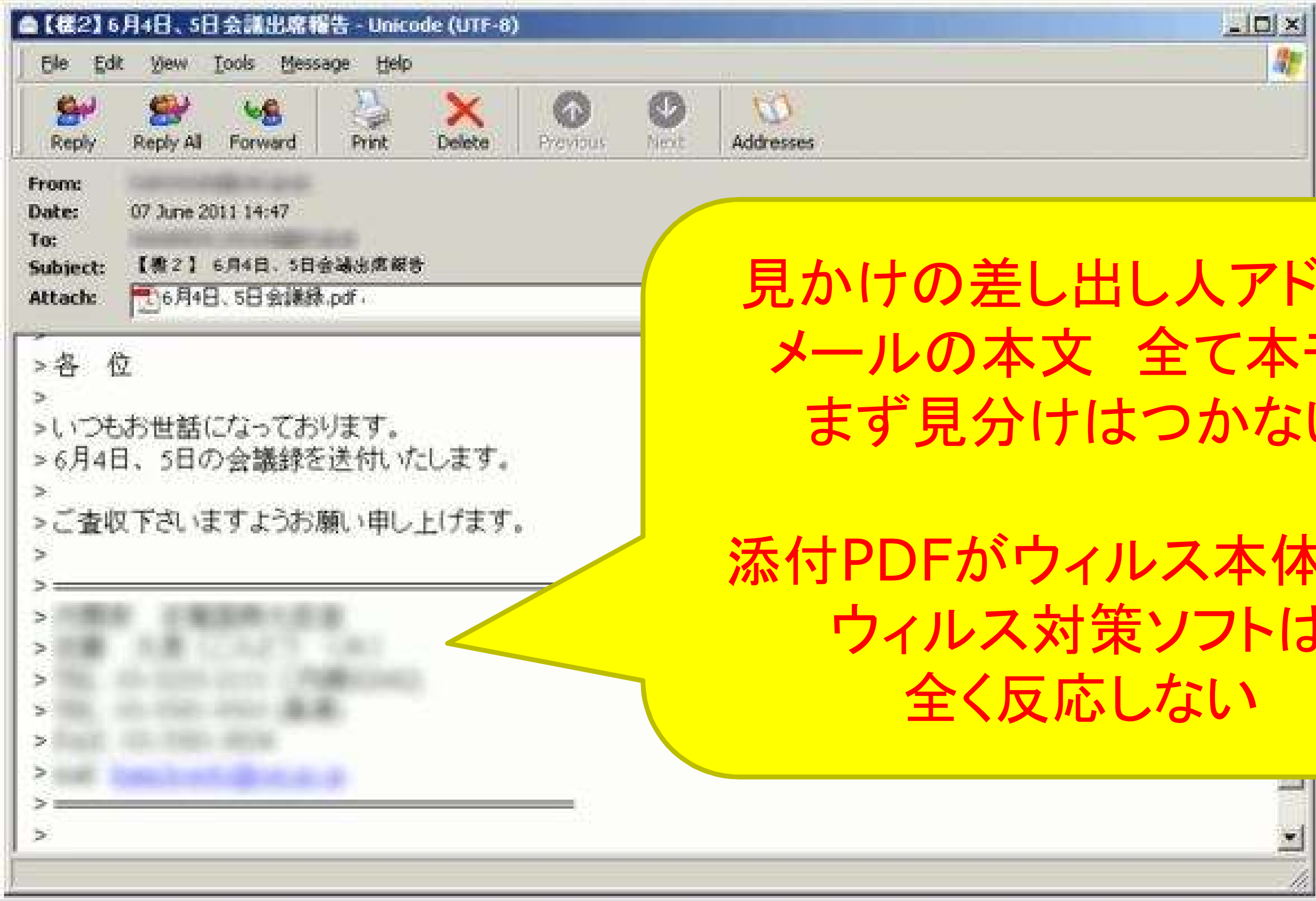


LAC「日本年金機構の情報漏えい事件から、我々が得られる教訓」より

標的型攻撃：
静かなる敵による産業スパイ行為

- マルウェアを用いて侵入・データを盗む
  1. まず攻撃先サイトのどれかのPCをマルウェアを用いて遠隔操作可能にし、機器構成やネットワーク構成の情報を盗む
  2. その情報を用いて重要な情報のありかを知る
  3. 重要な情報を持っているシステムへ侵入するための特製のマルウェアを作成、既に乗っ取ったPCを用いて感染させる
  4. 遠隔操作またはbot的手口で重要な情報を引き出す
- マルウェアは攻撃先向けにカスタマイズ→
  マルウェア対策の効きが悪い

「怪しいメールは開かない？」



見かけの差し出し人アドレス
メールの本文　全て本モノ
まず見分けはつかない

添付PDFがウィルス本体だが
ウィルス対策ソフトは
全く反応しない

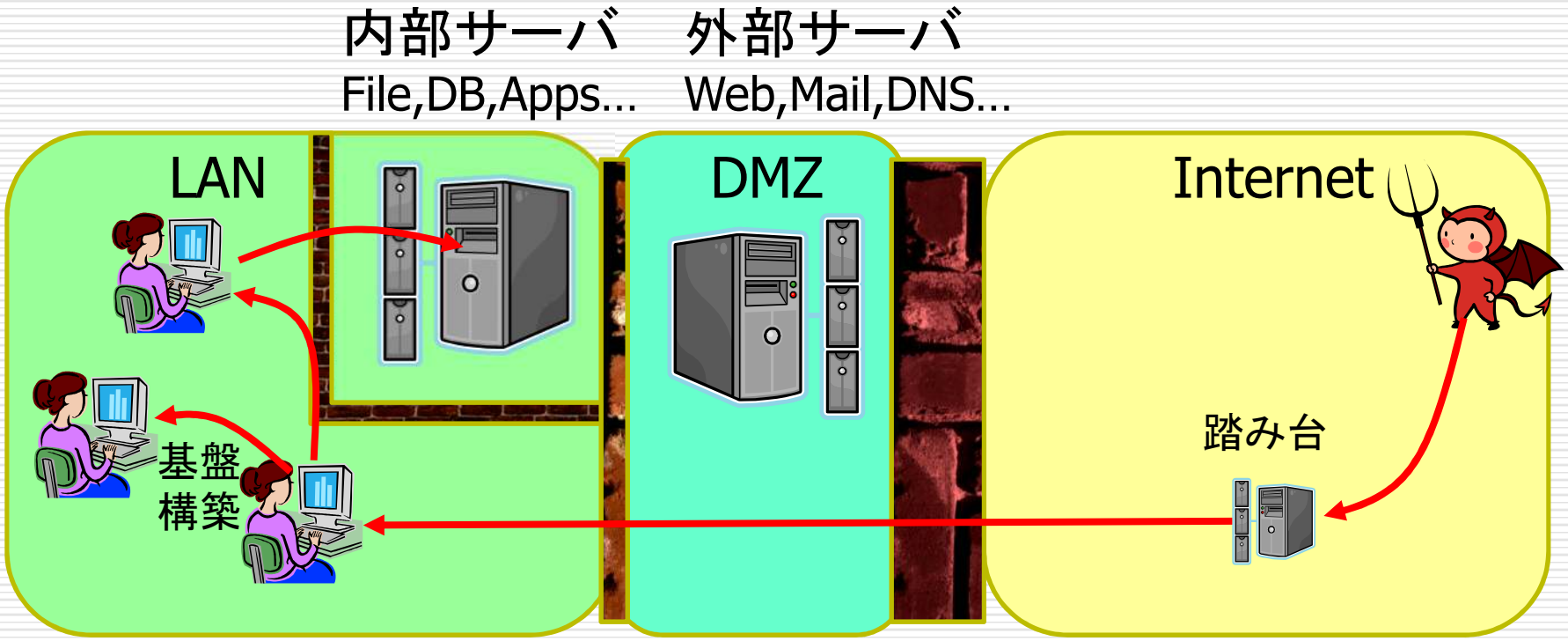
もはや「入れないようにする」のは困難

- 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

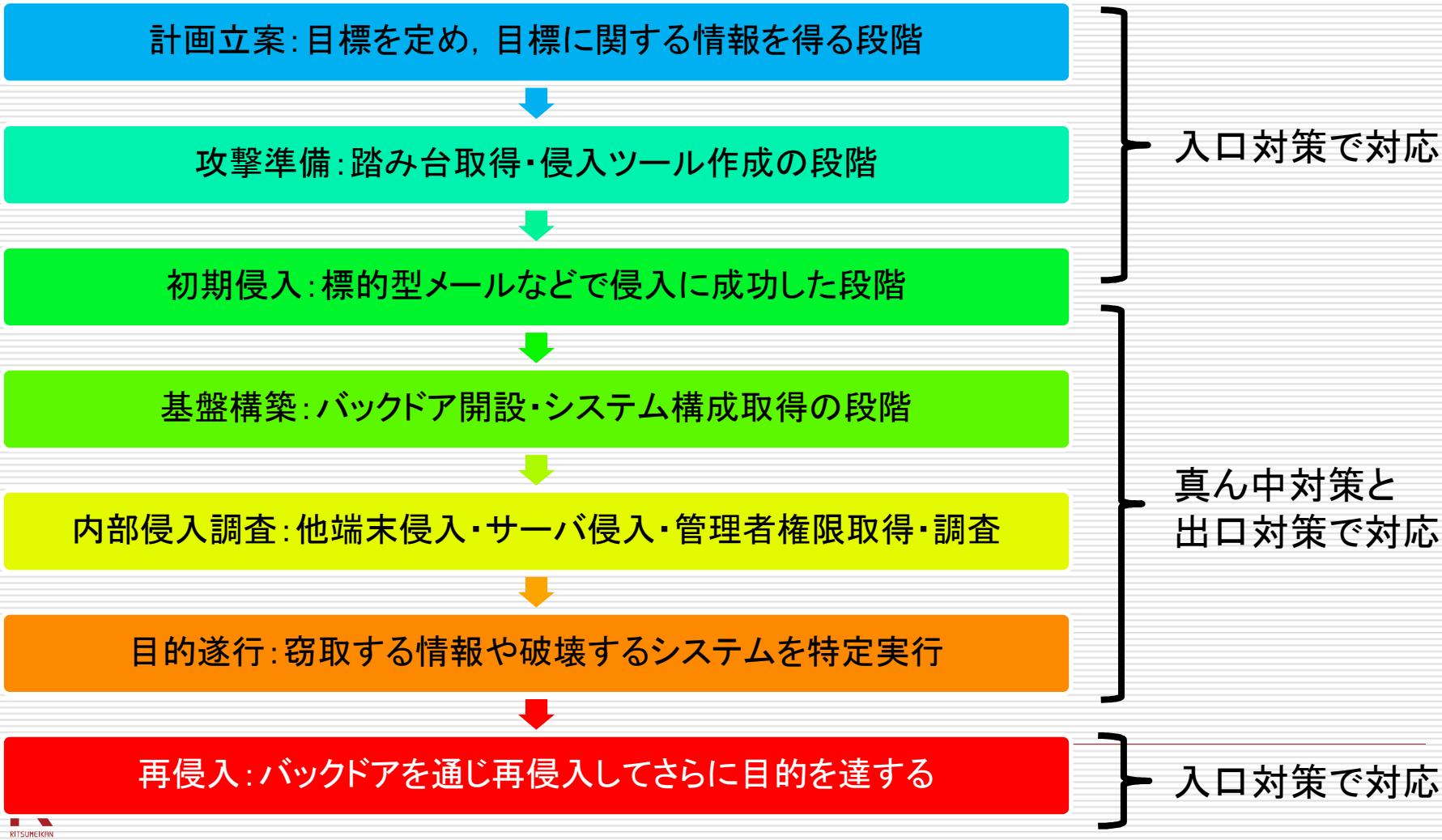
R
RITSUMEIKAN

侵入→基盤構築→目的達成



サイバー「産業スパイ」行為は段階を追って行われる
最初の攻撃は防ぎきれなくても本丸に辿り着くまでに気づけば…

攻撃の各段階


計画立案：目標を定め，目標に関する情報を得る段階
攻撃準備：踏み台取得・侵入ツール作成の段階
初期侵入：標的型メールなどで侵入に成功した段階
基盤構築：バックドア開設・システム構成取得の段階
内部侵入調査：他端末侵入・サーバ侵入・管理者権限取得・調査
目的遂行：窃取する情報や破壊するシステムを特定実行
再侵入：バックドアを通じ再侵入してさらに目的を達する
入口対策で対応
真ん中対策と
出口対策で対応
入口対策で対応

IPA「高度標的型攻撃」対策ガイド

このところ
ほぼ毎年改訂されてきた
システム設計ガイドの集大成

ポイントは
「侵入されないこと」
ではなく
「侵入されたことを
　発見しやすい」
「侵入されても被害が
　大きくなりにくい」
こと

IPA対策ガイドにおける システム対策リスト(一部)

(2) 内部侵入・調査段階

内部侵入・調査段階における、対策目標は下記2点となります。

① 攻撃者による内部侵入の拡大防止

② ユーザ端末におけるアカウント窃取防止

表 2.2-2 内部侵入・調査段階におけるシステム設計策一覧

分類	No.	対策タイトル	概要	対象機器
防御遮断策	断④	運用管理端末とユーザ端末のネットワーク分離設計 (2.2.6 参照)	ユーザ端末と運用管理端末を分離し、ユーザ端末から運用管理端末へアクセスできないようにネットワークを分離する	・ユーザ端末 ・運用管理端末
	断⑤	ネットワークの分離設計とアクセス制御 (2.2.7 参照)	適切なネットワークセグメントの分離設計とネットワークセグメント間のアクセス制御を実施する	・ネットワーク機器
	断⑥	高い管理者権限アカウントのキャッシュ禁止 (2.2.8 参照)	高い管理者権限を有するアカウント(Domain Admins 等)のキャッシュ禁止	・ユーザ端末
	断⑦	ユーザ端末間のファイル共有の禁止 (2.2.9 参照)	端末間でのファイル共有や管理共有を禁止(無効化)し、ファイルサーバなど必要最低限の対象とだけファイル共有を許可する	・ユーザ端末
監視強化策	視⑤	トラップアカウントによる認証ログの監視と分析 (2.2.10 参照)	ユーザ端末にトラップアカウントを仕込み、当該アカウントを用いた攻撃者のログイン攻撃を検知する	・ユーザ端末 ・認証サーバ (AD)
	視⑥	Listen ポート開設の監視	新たに開設されたコネクトバック通信の Listen ポートを監視する【継続検討中】	・サーバ
	視⑦	ハッキングコマンドの監視	普段の運用管理に使用せず、ハッキングで使用されることの多いコマンド群の使用状況を監視する【継続検討中】	・サーバ

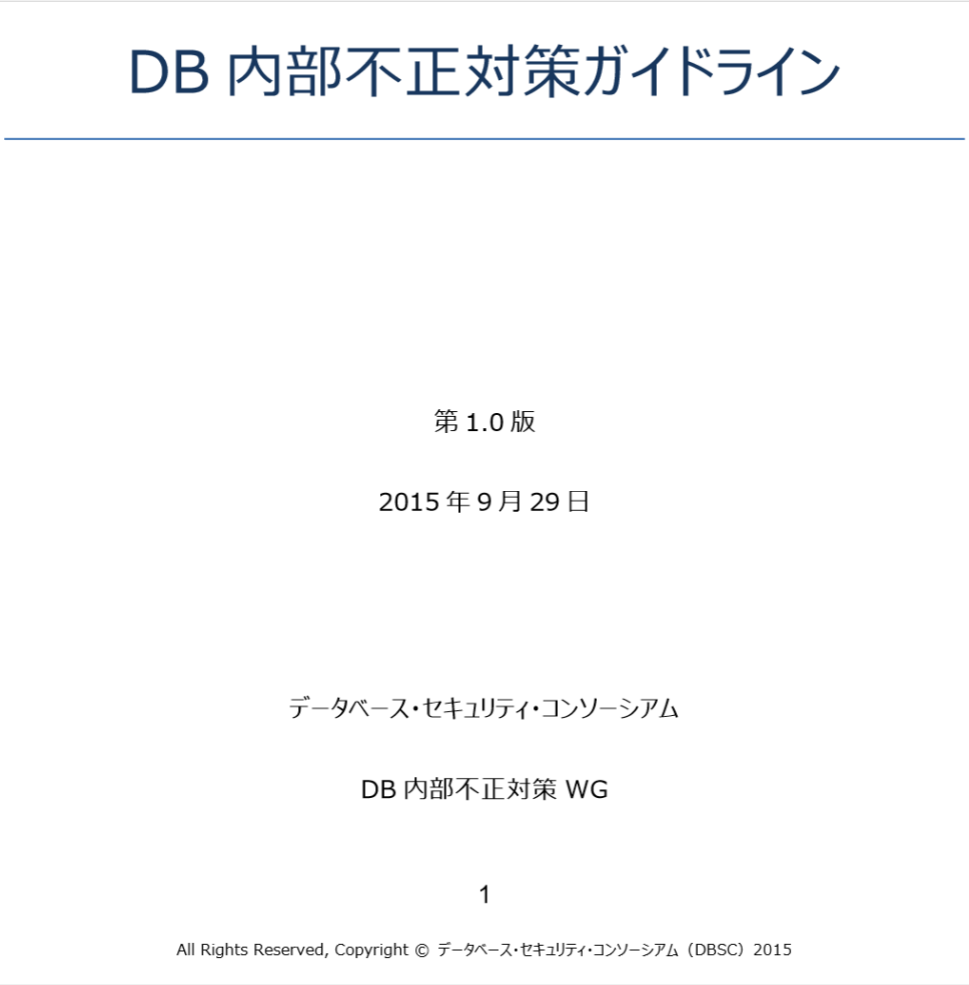
- 設定変更で可能な対策を中心に具体的に列挙
- コストは最小で済むはず
- 監視体制が重要

IPA「内部不正防止ガイドライン」

- 「情報の管理」
  - 格付け
    所在の確認
    管理者の任命と委任
- 監視体制の構築
  - 人的にも技術的にも
- 内部通報制度の
  確立など

DBSC内部不正対策ガイドライン

- DBのアクセス権を基に誘引分析
  多くは
  一般の内部不正に適用可能な内容
- チェックリストがわかりやすい


DB 内部不正対策ガイドライン

第 1.0 版

2015 年 9 月 29 日

データベース・セキュリティ・コンソーシアム

DB 内部不正対策 WG

1

RITSUMEIKAN

おわりに

- 年金機構事件をきっかけにして
  サイバー諜報戦の一端が少しは
  社会に知られるように
- しかしマイナンバー騒ぎが
  社会不安を煽っている一面も

- 状況は厳しいが…やれることをやろう！