

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



RITSUMEIKAN

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

第1	はじめに.....	1
第2	用語の定義等.....	3
第3	総論.....	7
第3-1	目的.....	7
第3-2	本ガイドラインの適用対象等.....	7
第3-3	本ガイドラインの位置付け等.....	8
第3-4	番号法の特定期間に関する保護措置.....	8
第3-5	特定期間保護のための主体的な取組について.....	12
第3-6	特定期間の漏えい事案等が発生した場合の対応.....	12
第3-7	個人情報取扱事業者でない個人番号取扱事業者における 特定期間の取扱い.....	12
第3-8	本ガイドラインの見直しについて.....	12
第4	各論.....	13
第4-1	特定期間の利用制限.....	13
第4-1-1	個人番号の利用制限.....	13
第4-1-2	特定期間ファイルの作成の制限.....	18
第4-2	特定期間の安全管理措置等.....	19
第4-2-1	委託の取扱い.....	19
第4-2-2	安全管理措置.....	22
第4-3	特定期間の提供制限等.....	23
第4-3-1	個人番号の提供の要求.....	23
第4-3-2	個人番号の提供の求めの制限、特定期間の提供 制限.....	25
第4-3-3	収集・保管制限.....	30
第4-3-4	本人確認.....	33
第4-4	第三者提供の停止に関する取扱い.....	35
第4-5	特定期間保護評価.....	36
第4-6	個人情報保護法の主な規定.....	37
第4-7	個人番号利用事務実施者である健康保険組合等における 措置等.....	42
(別 添)	特定期間に関する安全管理措置(事業者編).....	47
(巻末資料)	個人番号の取得から廃棄までのプロセスにおける本ガイドライン の適用(大要)	

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

マイナンバーガイドライン入門

～特定個人情報の適正な取扱いに関するガイドライン（事業者編）の概要～



平成26年12月版
特定個人情報保護委員会事務局

はじめてのマイナンバーガイドライン （事業者編）

～マイナンバーガイドラインを読む前に～



特定個人情報保護委員会事務局

（留意事項）
○本資料は、「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」の概要をご理解いただくために、まとめたものです。
○特定個人情報の適正な取扱いを確保するための具体的な事務に当たっては、「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」を参照してください。
（特定個人情報保護委員会ホームページ <http://www.ppc.go.jp/legal/policy/>）

- 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/>

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

個人番号 123456789012	社員番号	氏名	生年月日	住所	給与 支給総額
----------------------	------	----	------	----	------------

属性情報(一部は単体でも個人情報)

改正後は
要配慮情報かも？

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
------	------------

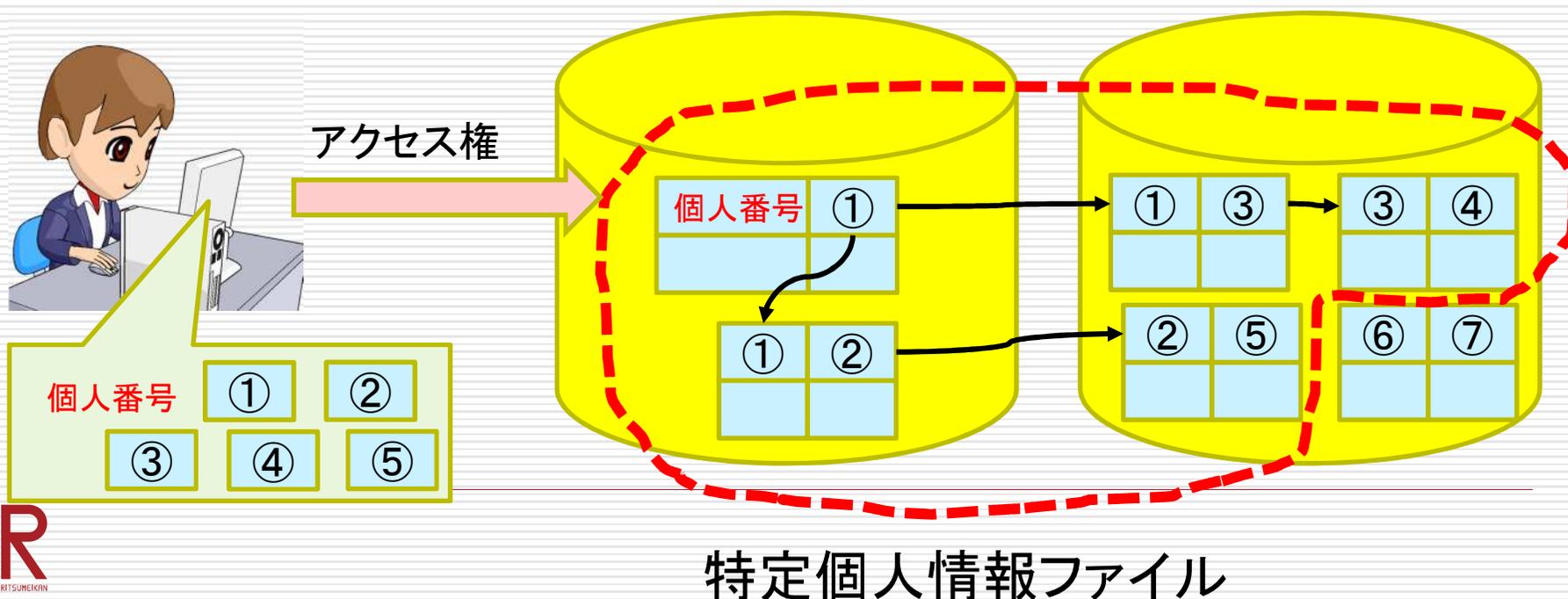
全レコードに
アクセス権を持つ者にとっては
全てが特定個人情報

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

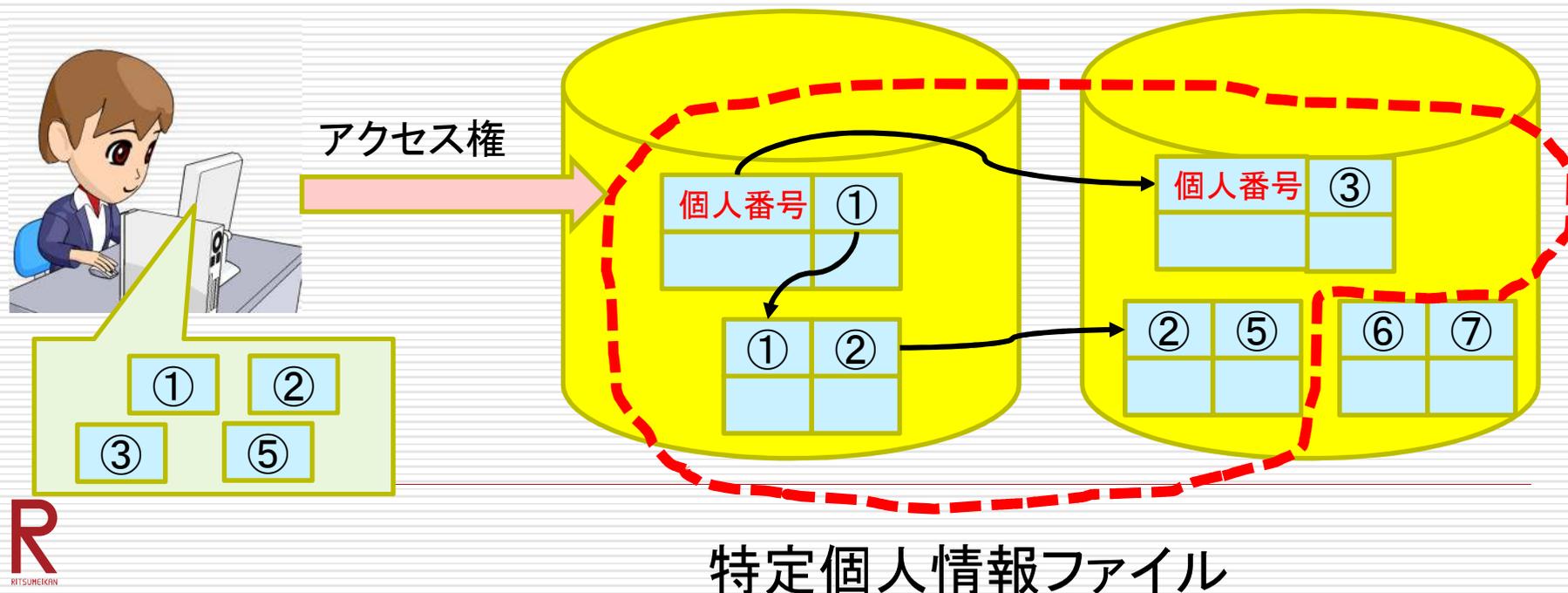
「個人番号をその内容に含む 個人情報ファイル」とは

- 「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)



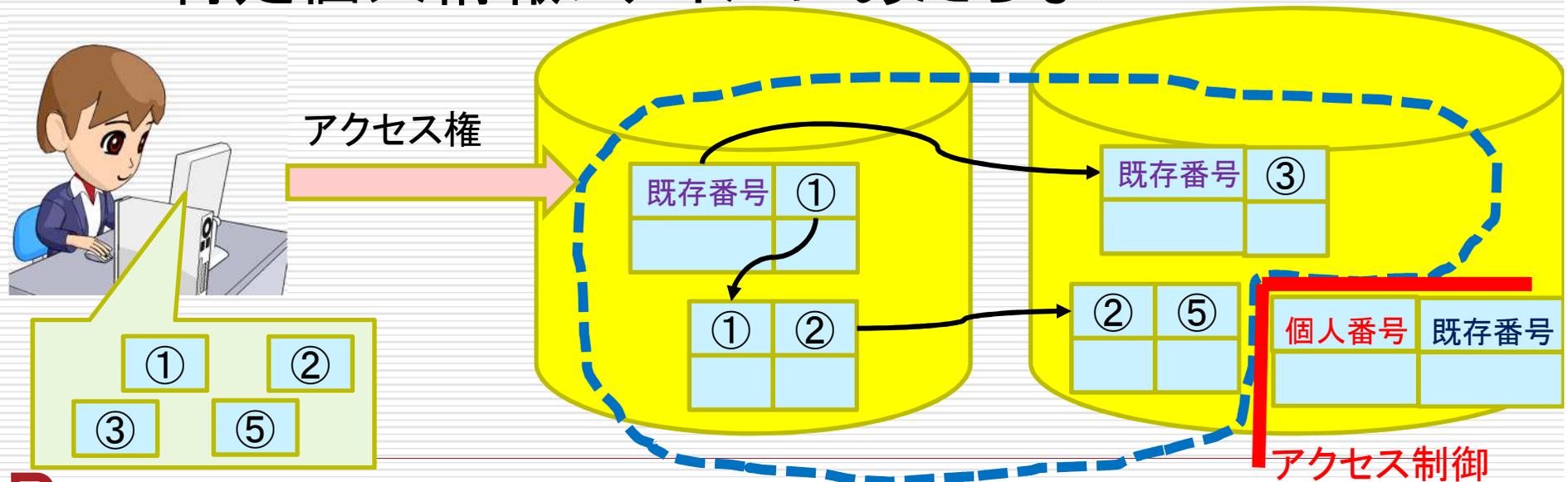
特定個人情報ファイルの わかりにくさ

- 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

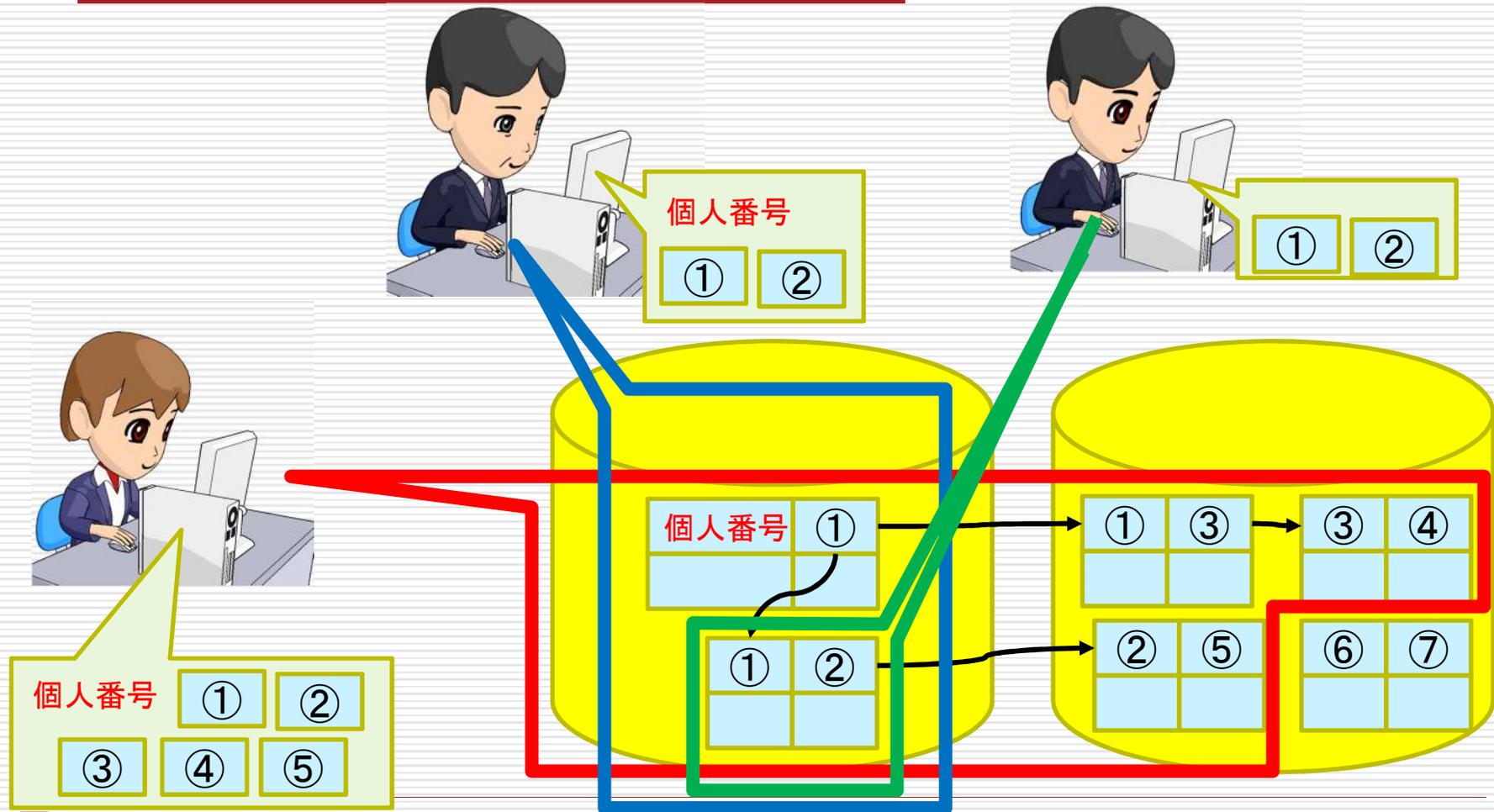
既存番号など「他の番号」の扱い

- 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

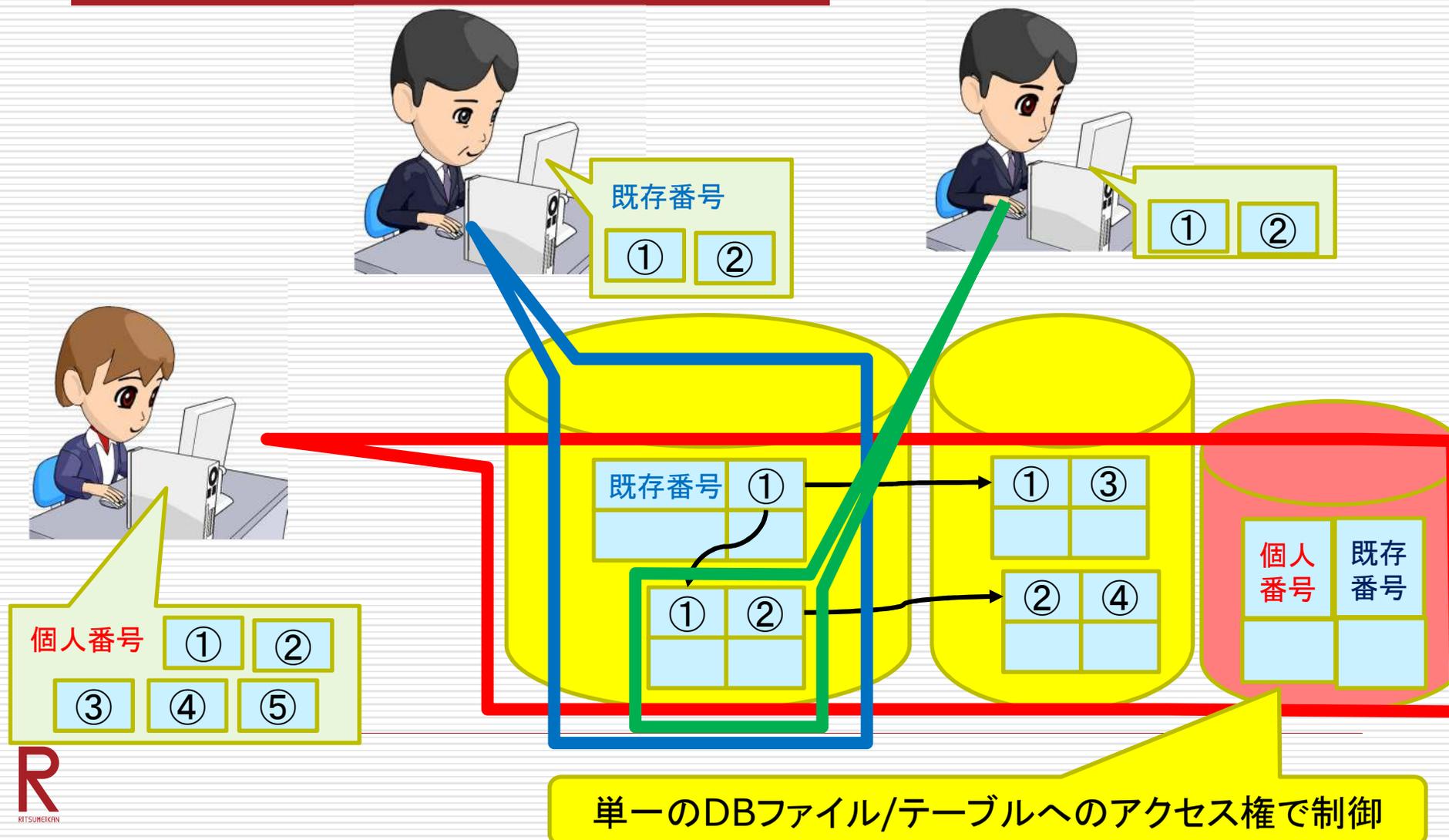
業務とシステムと 特定個人情報ファイル

- 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

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

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に記載しない(!)
 - 「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



わかるけど...
どこまで?!

必要な情報はここにまとまっています

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/>

特定個人情報保護委員会

Specific Personal Information Protection Commission

[> 本文へ](#) [> サイトマップ](#)

ENGLISH

文字サイズ変更 [標準](#) [大きめ](#)



検索

[ホーム](#)

[委員会の概要](#)

[お知らせ](#)

[委員会の活動](#)

[法令・ガイドライン](#)

[申請・お問合せ](#)

特定個人情報保護委員会 > [法令・ガイドライン](#) > [ガイドライン](#) > [ガイドライン資料集](#)

ガイドライン資料集

広報用資料

● [マイナンバー制度、はじまります。](#) (PDF: 654KB)

● [マイナンバー特集ページ](#) [New](#)
政府広報オンラインにて、マイナンバー特集ページを公開しました。
事業者向けのご案内はこちら

説明資料

<<事業者編>>

● [マイナンバーガイドライン入門（事業者編）](#)（平成26年12月版）（全16ページ）
(PDF: 3244KB)

<経営者向け>

● [社長必見「ここがポイント」マイナンバーガイドライン（事業者編）](#)（平成27年2月版）（全5ページ）
(PDF: 1186KB)

<マイナンバーガイドラインを読む前に>

● [はじめてのマイナンバーガイドライン（事業者編）](#)（平成27年2月版）（全8ページ）
(PDF: 1293KB)

● [中小企業向け はじめてのマイナンバーガイドライン](#)（平成26年12月版）（全8ページ）
(PDF: 1385KB)

法令・ガイドライン

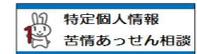
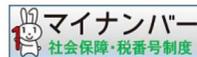
■ [関係法令一覧](#)

■ [ガイドライン](#)

● [ガイドライン資料集](#)

● [Q&A（回答）](#)

● [Q&A](#)



内閣官房

Cabinet Secretariat

● [マイナンバー制度のお問い合わせは0570-20-0178まで](#)

文字サイズの変更 [小](#) [中](#) [大](#)

マイナンバー 社会保障・税番号制度

国民生活を支える社会的基盤として、
社会保障・税番号制度を導入します。



マイナンバー



[トップページ](#) [社会保障・税番号制度とは](#) [事業者のみなさまへ](#) [地方公共団体のみなさまへ](#) [よくある質問\(FAQ\)](#) [関係法令](#) [個人情報の保護](#) [過去の経緯](#)

重要なお知らせ

- **DV・ストーカー行為・児童虐待等の被害者、東日本震災による被災者、一人暮らしで長期間、医療機関・施設に入院・入所されている方など、住民票の住所地で「通知カード」を受け取れない方は、居所に送付することが可能です。**
- **マイナンバー制度に便乗した不正な勧誘および個人情報の取得にご注意ください。通知前にマイナンバー制度関係で行政機関等から手続を求めることはありません。**

お知らせ

● [過去の掲載履歴](#)

平成27年9月10日 「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」を公表しました。 **NEW**

平成27年9月9日 「情報提供等記録開示システムに係る機器等の借入及び保守」の意見招請に関する公示につ

お問い合わせ

[聴覚障害者の方へ](#)

[視覚障害者の方へ](#)

[関係府省庁等へのリンク](#)

[国税庁特設サイト](#)

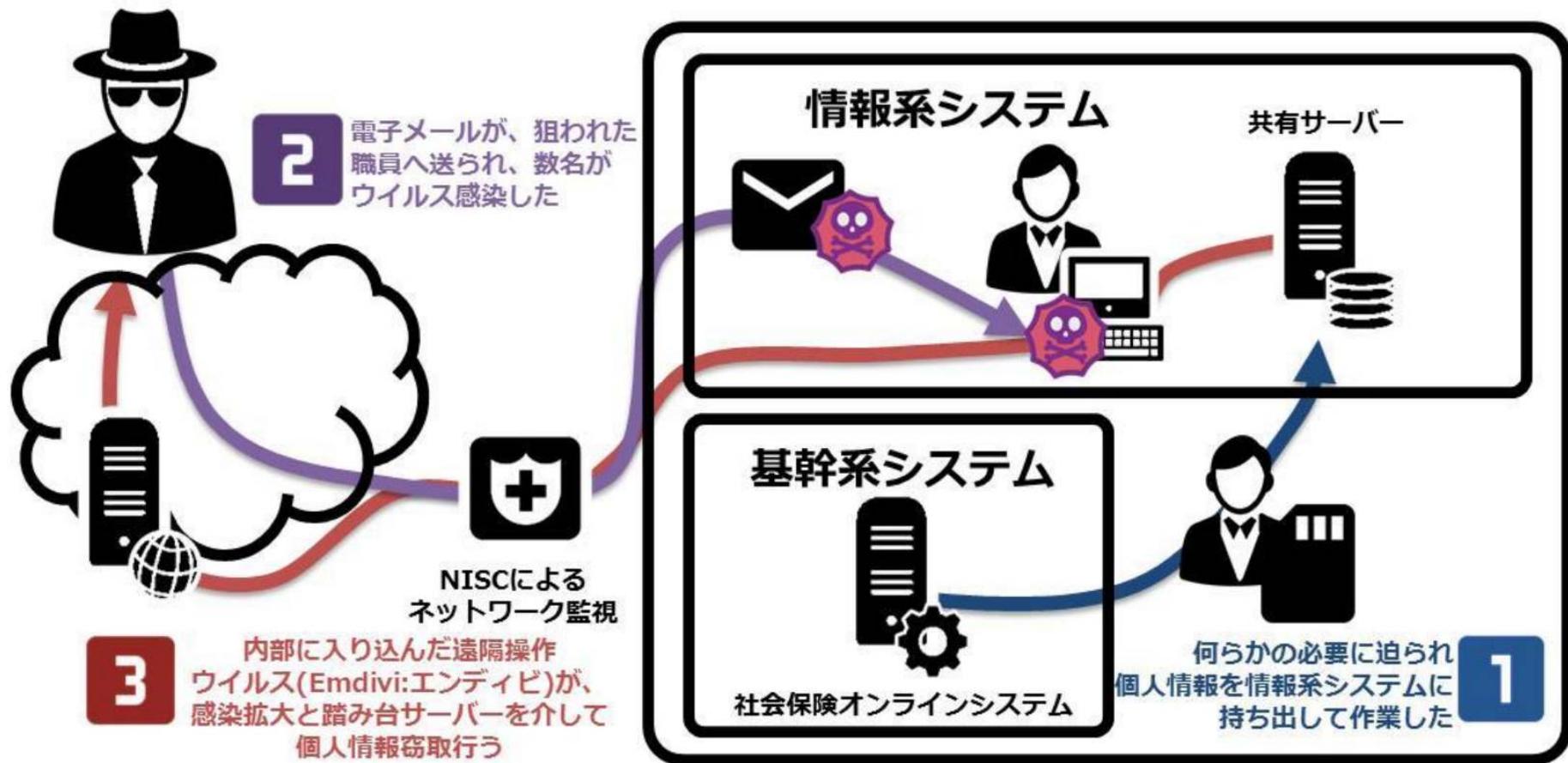
[総務省特設サイト](#)

[厚生労働省特設サイト](#)

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



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

もはや「入れないようにする」のは困難

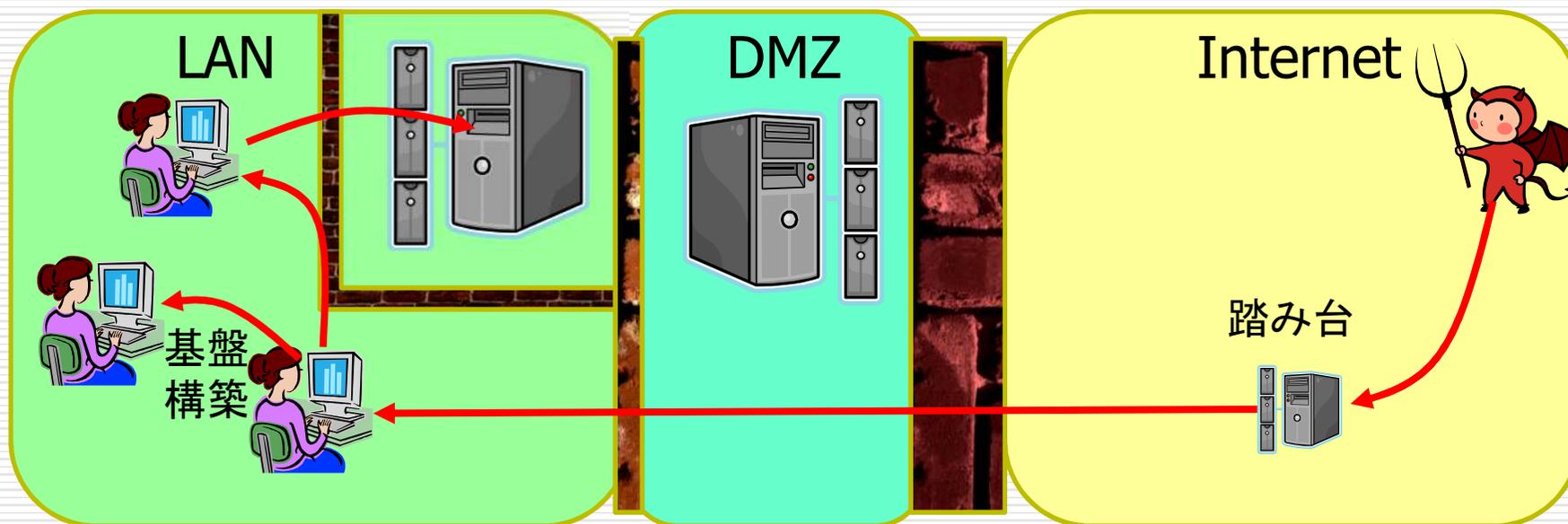
- 多層防御 多段階防御はもう常識
 - 入口対策＋出口対策＋「真ん中対策」
- 攻撃の各段階で可能な限り
攻撃者の手を縛る「意地悪セキュリティ」

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 外部サーバ
File,DB,Apps... Web,Mail,DNS...



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

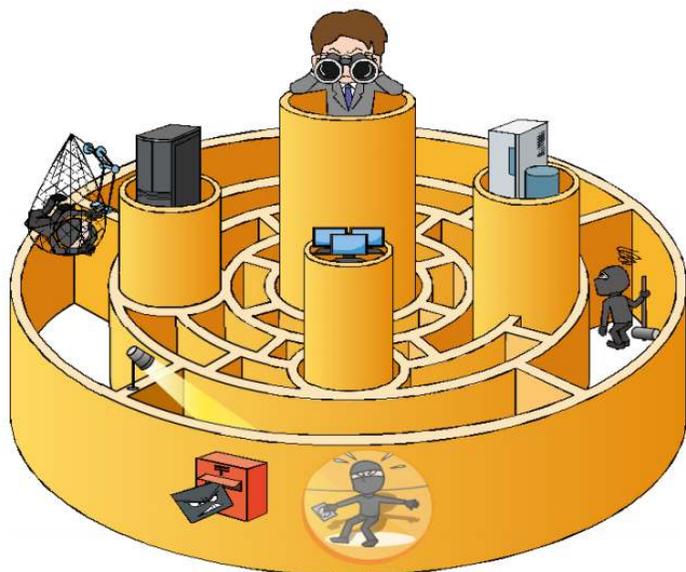
真ん中対策と
出口対策で対応

入口対策で対応

IPA「高度標的型攻撃」対策ガイド

「高度標的型攻撃」対策 に向けたシステム設計ガイド

～入口突破されても攻略されない内部対策を施す～



IPA 独立行政法人情報処理推進機構
セキュリティセンター

2014年9月

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」

IPA

組織における 内部不正防止ガイドライン



独立行政法人情報処理推進機構

- 「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

All Rights Reserved, Copyright © データベース・セキュリティ・コンソーシアム (DBSC) 2015

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！