長崎県立大学
UNIVERSITY OF NAGASAKI

システム設計における情報セキュリティ要求分析

長崎県立大学
情報セキュリティ学科
小松文子

自己紹介

- 日本女子大学　家政学部家政理学科　物理専攻卒（現理学部数物科学科）
  横浜国立大学大学院　博士課程（情報学）修了
- NECに勤務
  - 汎用OS開発，ネットワークプロトコル開発，国際標準化活動，セキュリティ評価・認証制度，主に，公開鍵暗号基盤を中心としたセキュリテイ製品・開発・研究・サービス・コンサルタント
- （独）情報処理推進機構（IPA）2008～
  - 情報セキュリティ分析ラボラトリー　ラボラトリー長
  - (独）経済産業研究所　コンサルティングフェロー（～2012）
- これまで，政府の有識者会議の構成員や委員，地方公共団体の審議会委員など多数，また複数の大学，大学院の非常勤講師を務める.
- 2014年3月　第10回情報セキュリティ文化賞受賞
- 長崎県立大学　情報システム学部情報セキュリティ学科　学科長，教授
- 内閣　サイバーセキュリティ戦略本部　研究開発専門調査会　委員
- 情報セキュリティ対策と人間との関係に焦点を当てた研究に興味を持つ

本日の内容

情報セキュリティを考慮したシステム設計について過去の経験を踏まえお話します

１．情報セキュリティの開発プロセス

２．事例：

マイナンバーシステム設計における情報セキュリティ要件定義

システムの開発プロセスにおける情報セキュリティ

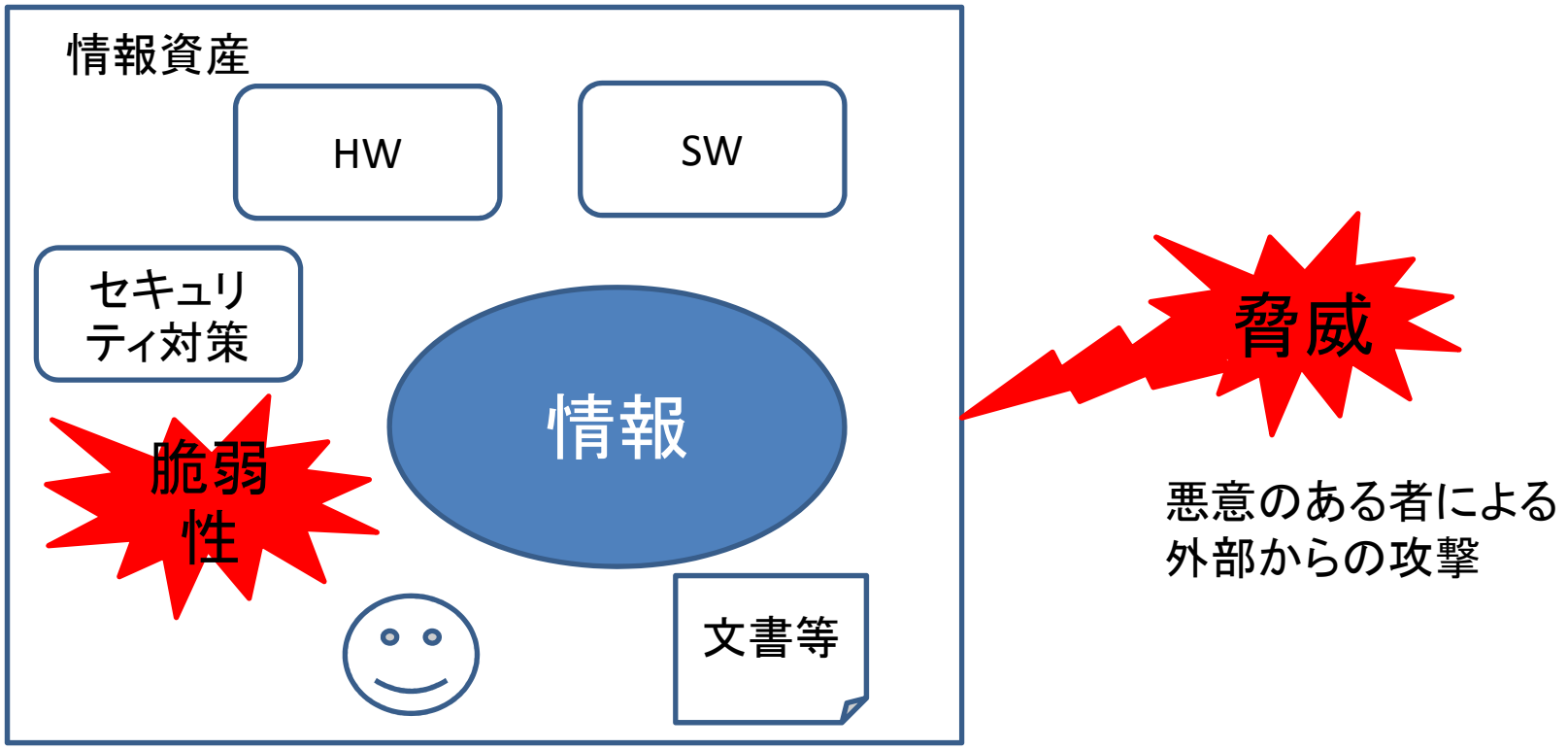
１．脅威・脆弱性と情報セキュリティリスク
２．システムのライフサイクルに沿ったセキュリティ対策
3.　セキュリティ要件定義

長崎県立大学
UNIVERSITY OF NAGASAKI

１．脅威・脆弱性と情報セキュリティリスク

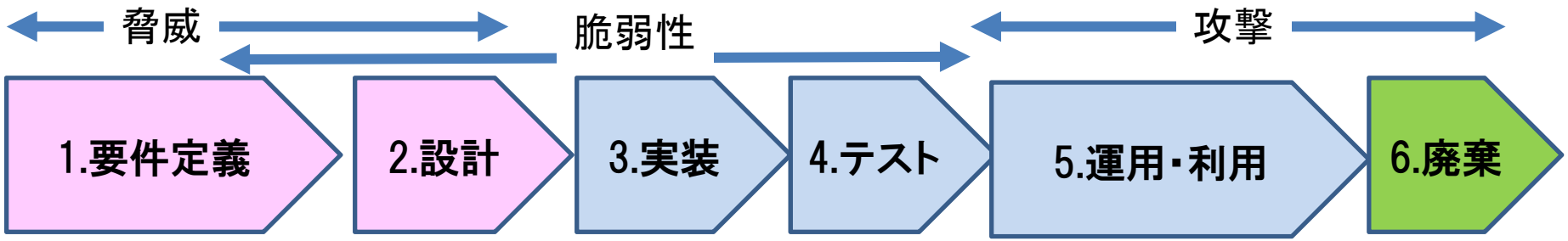
- **脅威（threat)**
  - ◆システム又は組織に損害を与える可能性がある，望ましくないインシデントの潜在的な原因
- **脆弱性（vulnerability）**
  - ◆1つ以上の脅威によって，付け込まれる可能性のある，資産または管理策の弱点
- **情報セキュリティリスク**
  - ◆**脅威**が情報資産の**脆弱性**または情報資産グループの**脆弱性**に付け込み，その結果，組織に損害を与える可能性に伴って生じる

情報セキュリティリスク≒ 事業方針×脅威×脆弱性



脆弱性：情報システム内部に潜む弱点の可能性

2. システムのライフサイクルに沿ったセキュリティ対策



■調査，動向把握
■開発方針・体制整備

■脅威分析・リスク分析・リスク評価

■テスト（ファジング）

■セキュア・プログラミング

■ソースコードセキュリティ検査

■脆弱性対策

■脆弱性診断（侵入テスト）

主な対策

■運用対策
■インシデント対策
■脆弱性対策

出典：IPA：「ソースコードセキュリティ検査」を元に作成

2.1　要件定義

- システムの目的や利用形態を明確にする
- 想定される脅威を洗い出す
- 脅威の事業に対する影響，対策方針，設計方針を決定する

2.2　設計

- 要件定義行程において検討した方針に従う
- 実装すべき機能や取り扱う情報の形式等を検討する
- ソフトウエアに脆弱性を作りこまないような，「コーディング規則」「セキュア・プログラミング技法」の周知
- 実装工程で，脆弱性を作りこまないための対策を事前に検討

2.3　実装

- ソースコードレベルの対策
- 脆弱性を発見するためのレビュー
- 脆弱性を機械的に発見するための検査

2.4　テスト

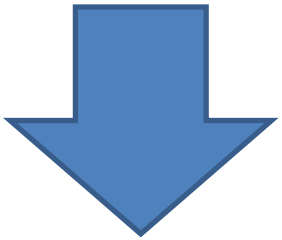
- ファジングや脆弱性診断等を用いてソフトウエアの脆弱性を摘出する
  - ◆脆弱性診断：検査対象のシステムやソフトウエアに対して，一般的に知られている攻撃を実施し，特徴的な応答を観察すること.

2.5　運用・利用

- 外部からの攻撃に備える
  - ◆脅威や脆弱性情報の収集
  - ◆定期的な脆弱性診断
    - ■アップデートプログラムの適用

3.セキュリティ要求定義

- システムの目的や利用形態を明確にする
- 想定される脅威を洗い出す
- 脅威の事業に対する影響，対策方針，設計方針を決定する



脅威分析・リスク分析・リスク評価

3.セキュリティ要求定義-2

- 守るべき資産の特定
- 資産に対する脅威は何か
- 事業に影響するリスクになり得る脅威はどれか
  - ◆受容可能なリスクレベルを決めておく
- リスクを回避・低減・保持するのはどれか
- 技術・運用・組織対策を決定

脅威分析の方法

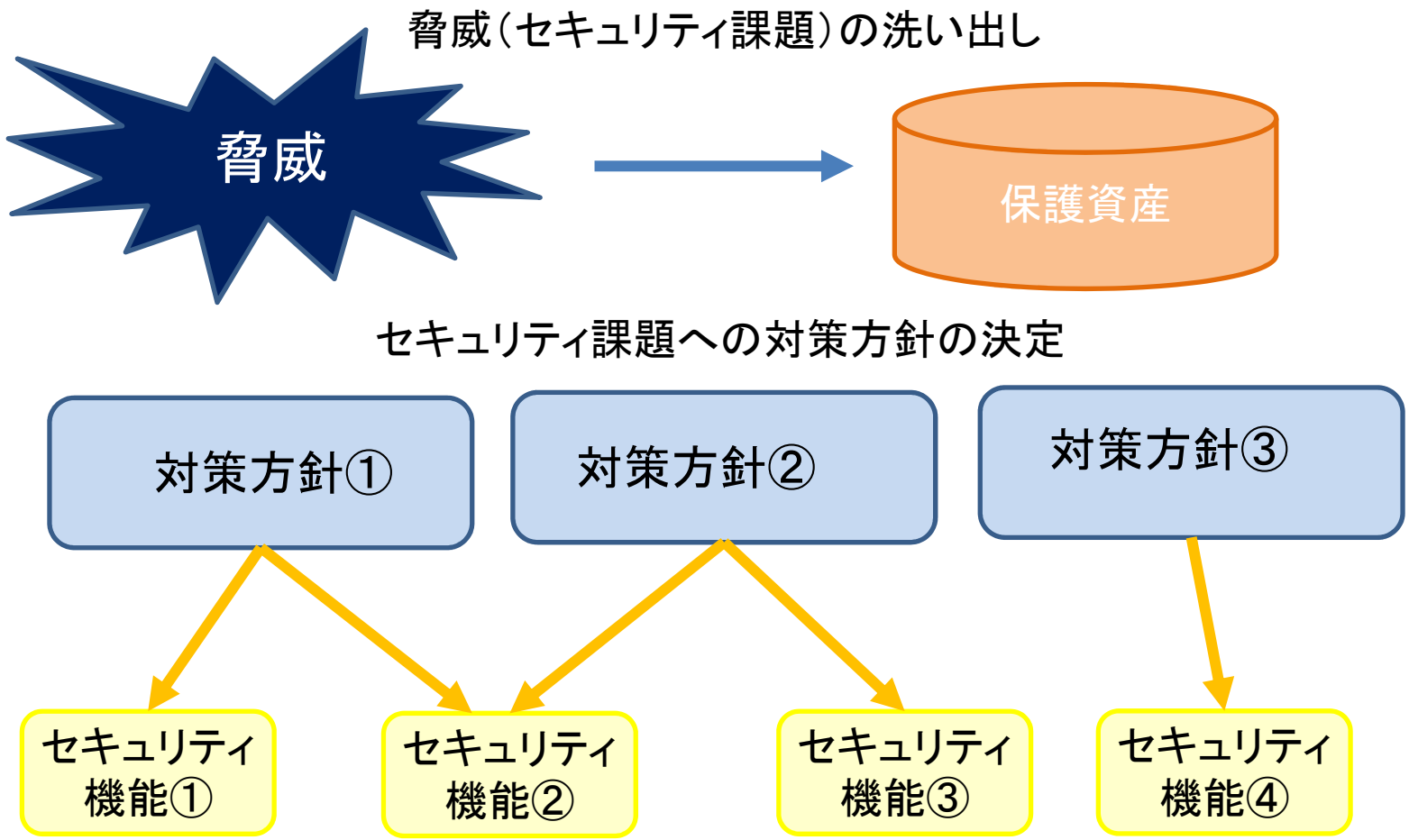
- 有名なのはSTRIDE
- STRIDE：マイクロソフト社
  - ■Spoofing（なりすまし）
  - ■Tampering（盗聴）
  - ■Repudiation(否認拒否)
  - ■Information Disclosure（情報漏えい）
  - ■Dos(Denial of Service)（サービス妨害）
  - ■Elevation of Privilege(権限昇格)

４．脆弱性対策

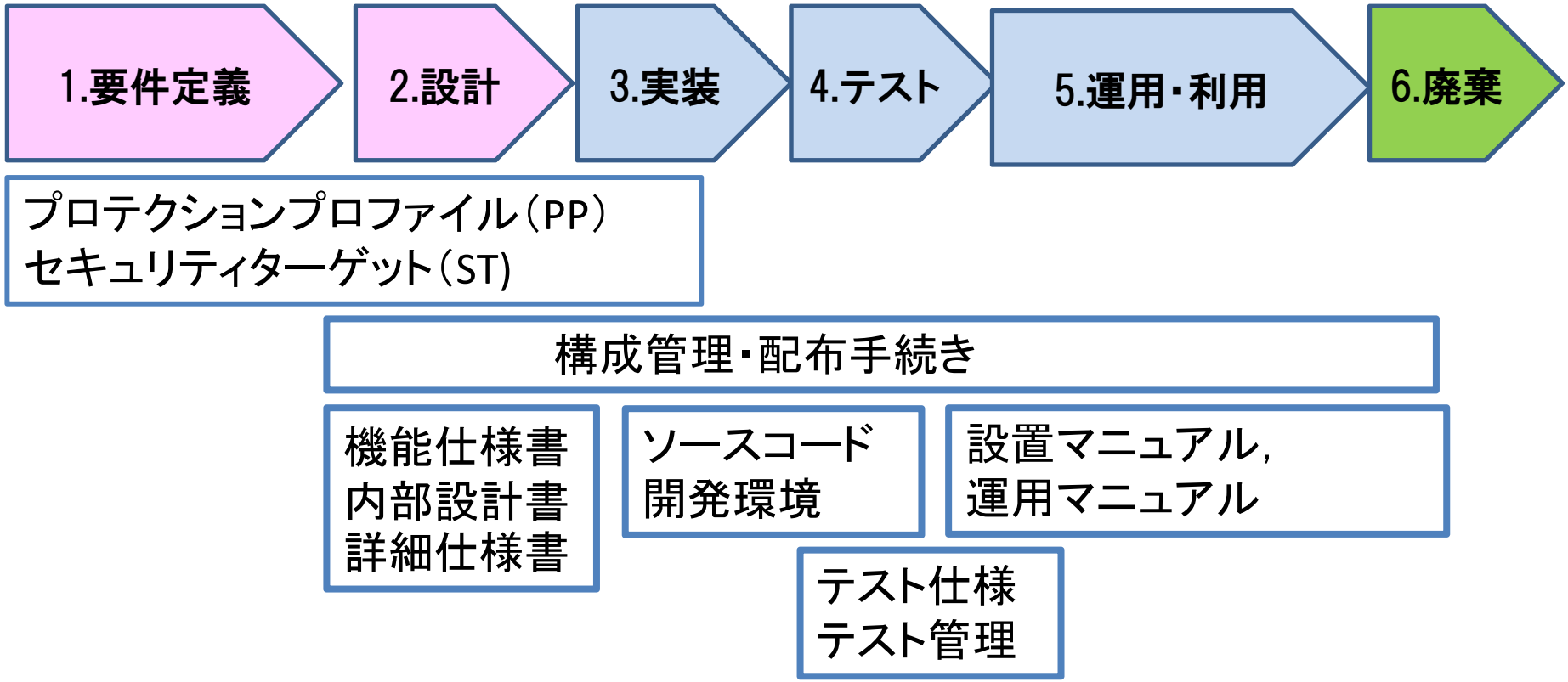
- ITセキュリティ評価・認証制度
  ①セキュリティ機能の必要十分性，及び

  ②それが正しく実装されていることを第三者が客観的に評価
  → 脆弱性を生み出さない仕組み

４・①　セキュリティ機能の必要十分性を確認



4. ②セキュリティ機能の正確性をライフサイクル全体で確認（脆弱性対策）



但し，本制度の対象は，政府系調達製品

出典：IPA

マイナンバーシステムのセキュリティ設計

「システム構成」を制度，セキュリティ上の脅威を考慮して検討した内容を紹介します

長崎県立大学
UNIVERSITY OF NAGASAKI

個人番号

- 番号
  - ◆住民基本台帳コードから生成する非可逆な値
- 要件　（大綱より）
  - ◆悉皆性
    - ■日本の国籍を有する者及び中長期在留者、特別永住者等の外国人住民が個人番号の対象
  - ◆唯一無二性
  - ◆民―民―官で利用可能で可視性がある
- 盗難・漏えいなどの申告に限り変更可能
- 符号・付番
  - ◆地方公共団体情報システム機構（JLIS）が主体となって実施

要綱より

検討プロセス

- 制度，技術をほぼ平行に検討
  - ◆パブコメによる合意形成
- 制度，司法からの技術への要件
  - ◆システム構成
  - ◆情報受け渡し方法
  - ◆データ保護の方法
  - ◆セキュリティ機能の保護

マイナンバーへの懸念

- 番号と同時に保管されている**関連情報が流出**し、番号をキーとして名寄せ・突合されてしまう（国家によるもの・悪意によるもの）
- 他人が番号を盗み**なりすまし**
- 番号システムへの**サイバー攻撃**
- 番号を扱う職員などによる**不正**

個人番号と関連情報を守る３つの観点の対策

1. **制度**
   - ◆利用範囲（事務・人）を限定
   - ◆罰則
2. **技術**
   - ◆複数の機関に保管された番号を安全に連携・管理する仕組み
3. **監視**
   - ◆第三者機関である個人情報保護委員会の設置
   - ◆自身の番号へのアクセスを監視できる仕組み（マイナポータル）
   - ◆特定個人情報保護評価（PIA)を導入

番号をキーとした名寄せ

- マイナンバーは12ケタの数
- マイナンバーをキーとして情報を一括管理できないシステム構成
- マイナンバーは変更可能
  - ◆流出などの懸念がある場合は変更できる

システム構成への要件1

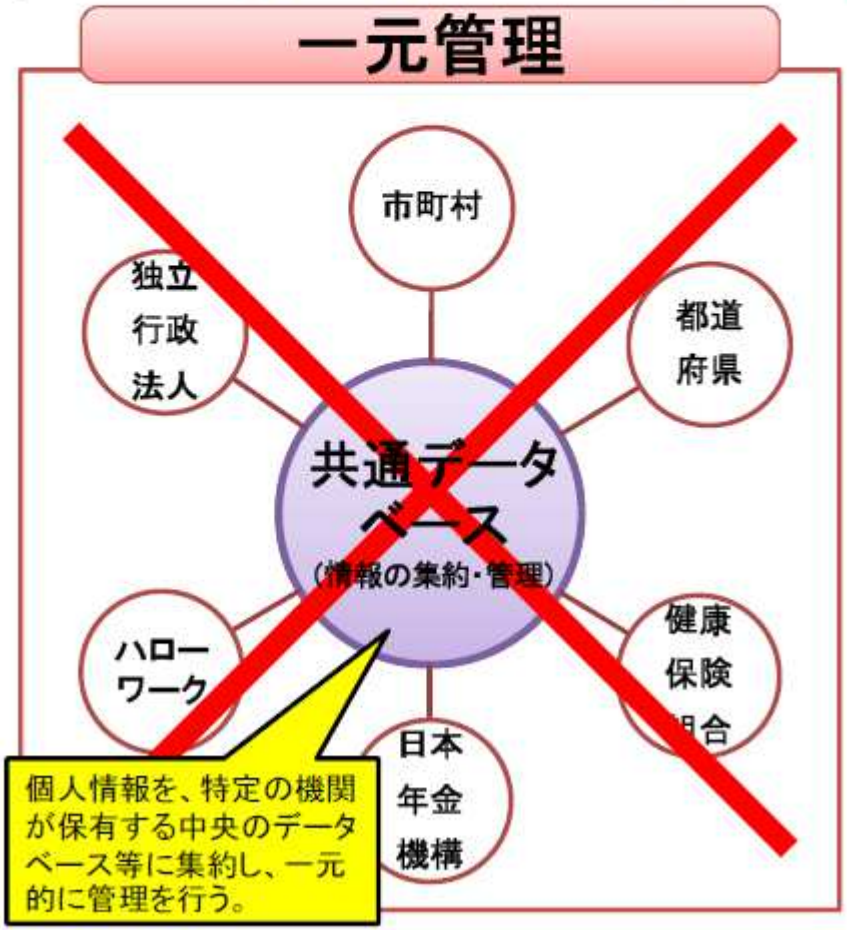
- 重要とされた要件:一元管理の回避
- 住民基本台帳ネットワークシステムの安全性について ～平成20年3月6日最高裁判決より～

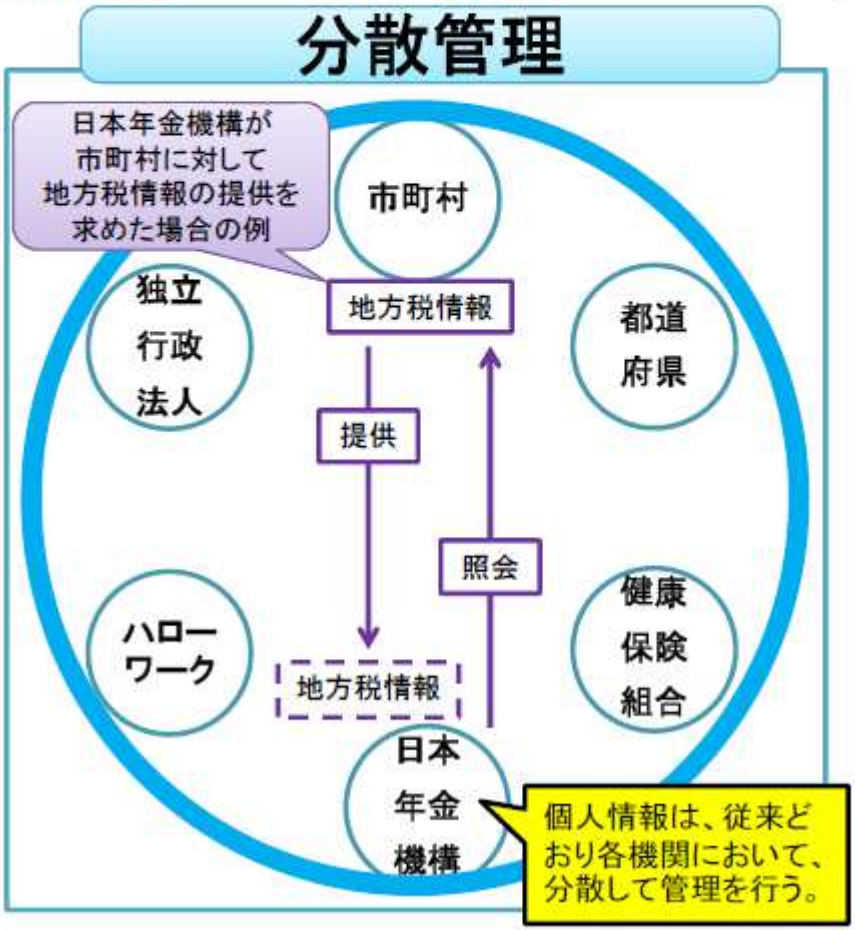
- 本人確認情報の漏えい防止等の安全確保の措置として、技術的側面では、住基ネットシステムの構成機器等について相当厳重なセキュリティ対策が講じられ、人的側面でも、人事管理、研修及び教育等種々の制度や運用基準が定められて実施されており、現時点において、住基ネットのセキュリティが不備なため本人確認情報に不当にアクセスされるなどして本人確認情報が漏えいする具体的な危険はない。
- データマッチングされ、本人の予期しないときに予期しない範囲で行政機関に保有され、利用される具体的危険については、刑罰をもって禁止されていること、個人情報を一元的に管理することができる機関又は主体は存在しないことなどにも照らせば、住基ネットの運用によって原審（大阪高裁判決）がいうような具体的な危険が生じているということはできない

分散管理をアピール

番号制度が導入されることで、各行政機関等が保有している個人情報を**特定の機関に集約**し、その集約した個人情報を各行政機関が閲覧することができる**『一元管理』**の方法をとるもの**ではない**。

番号制度が導入されても、従来どおり個人情報は**各行政機関等が保有**し、他の機関の個人情報が必要となった場合には、番号法別表第二で定められるものに限り、情報提供ネットワークシステムを使用して、情報の照会・提供を行うことができる**『分散管理』**の方法をとるもの**である**。





http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/250409kanrihou.pdf

マイナンバーシステム

複数の機関が保有している情報を各機関同士で連携させる仕組み

要件

「マイナンバーをキーとして情報を一括管理できない」システム構成

長崎県立大学
UNIVERSITY OF NAGASAKI

情報連携できても
情報収集できない
しくみが必要

年金事務所
マイナンバー
年金番号
名前・住所
支払い状況

税務署
マイナンバー
名前・住所
納税者番号
納税額・滞納状況

情報提供ネットワーク

健康保険組合
マイナンバー
名前・住所
健康保険
保険請求の内容

自治体
マイナンバー
名前・住所
住民税支払状況
国民保険情報

マイナンバー

：住所氏名：納税者番号：年金番号：住民税支払状況：健康保険情報

注：各機関内の情報は例である

情報提供ネットワークシステムへの要件2

- ビッグブラザーにならない
  ×偉大な兄弟があなたを見守っている（Big Brother is watching you）
  ジョージ・オーウェルの小説『1984年』
  ×誰かが番号や関連情報を盗み見することができない

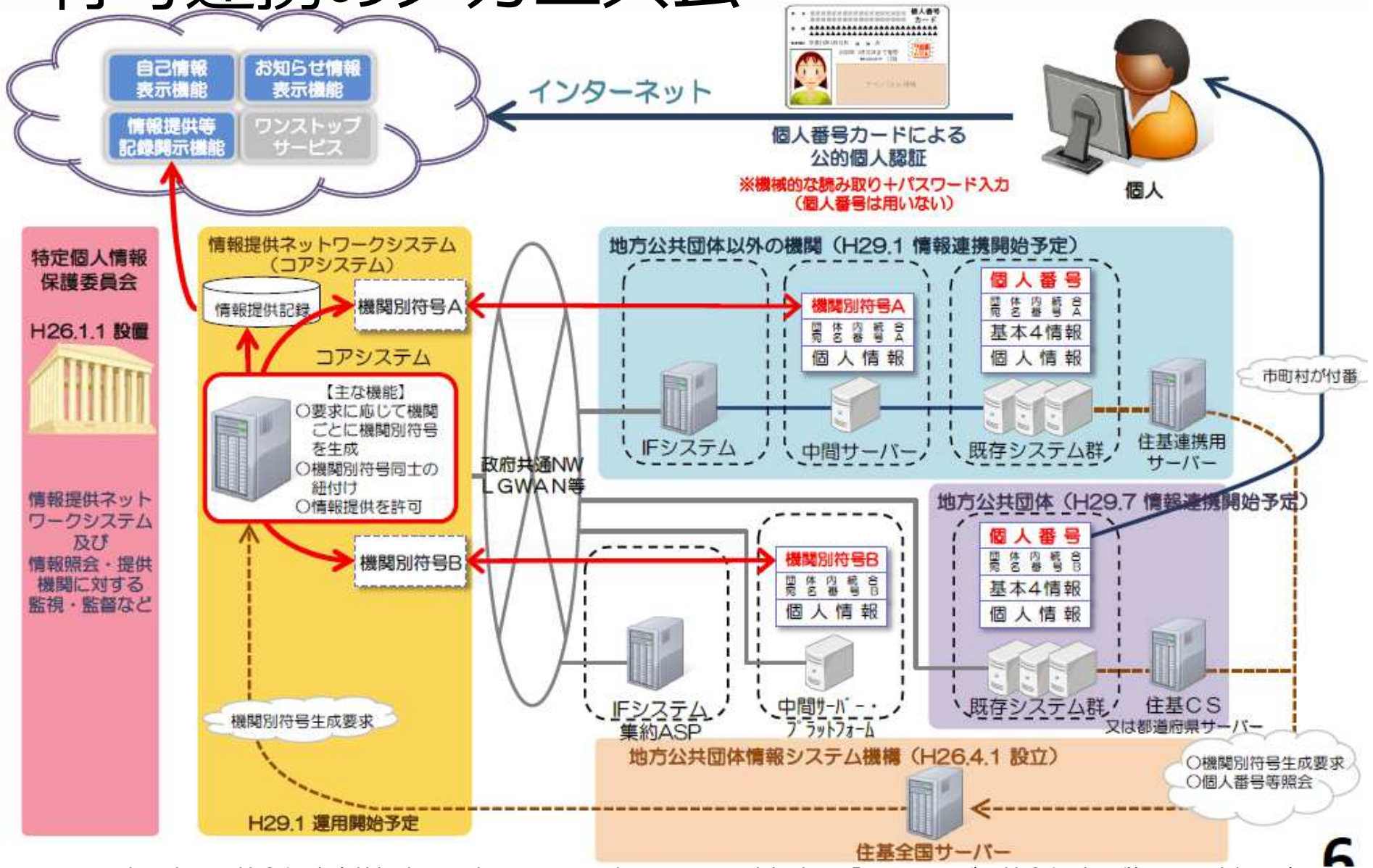
→記録（ログ）の取得
  ◆事後対策

→符号連携のメカニズム

→安全な符号管理のメカニズム

→安全なデータ転送のメカニズム

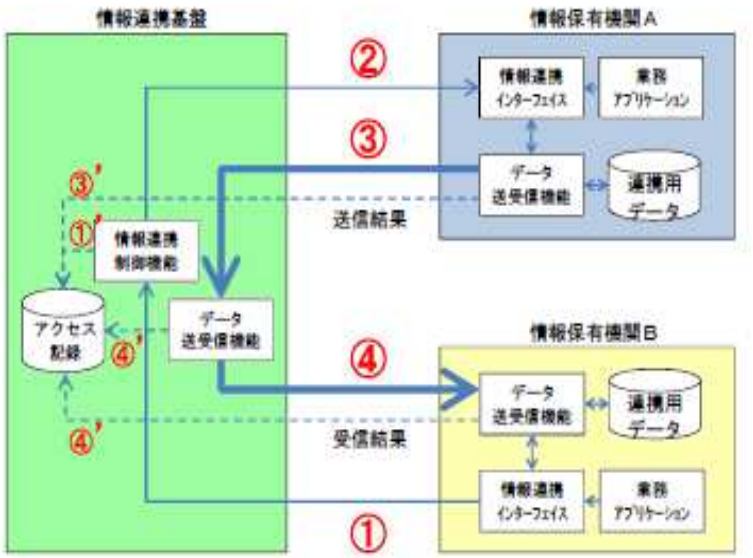
符号連携のメカニズム



（出典） 内閣官房　社会保障改革担当室、内閣府　大臣官房　番号制度担当室「マイナンバー社会保障・税番号制度概要資料」
http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/gaiyou_siryou.pdf

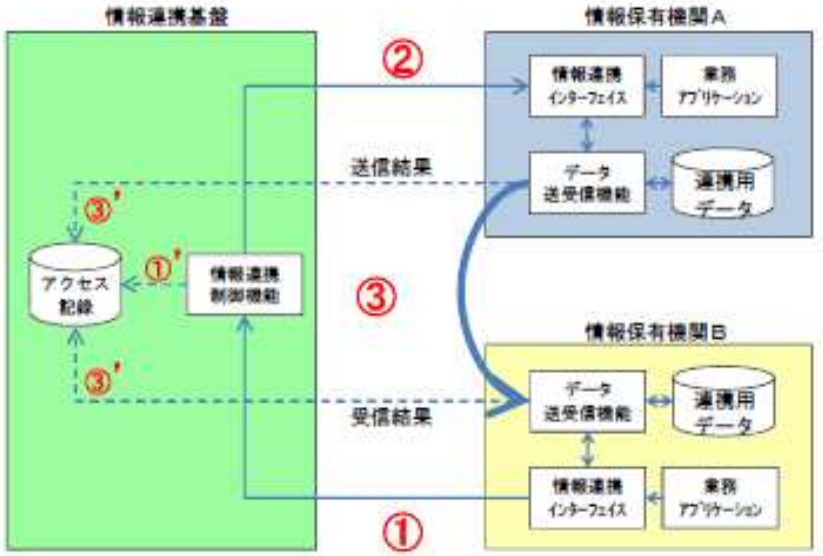
データ送受信のメカニズム

ゲートウエイ方式



すべてのデータ要求について情報連携基盤（情報提供ネットワークシステム）を経由する

トークン方式



データ要求についてトークンを取得し実際のデータ送受信は情報保有機関間で直接行う

情報連携（データ送受信）比較

開発費用	連携基盤システムはAが高額、保有機関はB方式が高額
連携対象の拡張性	両方式とも特に差異はない
稼働の安定性・運用性	Aでは、情報連携基盤に負荷大。Bでは情報保有機関の運用が複雑になる可能性があり
調達の透明・公正性	特に差異はない
障害発生時の影響度	Aでは、情報連携基盤の障害の影響が大
プライバシー影響度	Aでは監査に優れる。Bでは、監査が分散する。

A:ゲートウエイ方式　　B:トークン方式

なりすましを防ぐ

- (一般の人が）他人のマイナンバーを入手しても誰のものかを知る手段はない
- 事務等でマイナンバーを扱う場合は、マイナンバーカードなどにより本人確認が必須
- マイナンバーを利用する行政事務は法律で限定されており、収集、コピーは規定された手続以外は禁止
- オンラインでの手続では強い認証方法を採用

セキュリティ機能を守る

- 符号メカニズムを守る
  - ◆符号生成方法
  - ◆データベースに保持
    - ■データベースへの攻撃で影響範囲が大きい
  - ◆リアルタイムに生成
    - ■パフォーマンスを維持するためには，計算能力が必要
- 多くのシステムで，セキュリティ機能の暗号基盤を利用している場合，その鍵管理が重要となる

マイナポータルと
オンライン認証のしくみ

行政機関の間の情報連携は平成29年7月開始予定であり、マイナンバーの付いた自分の情報のやりとりの確認もこれ以降可能にする予定です。マイナポータル のその他の機能についても平成29年以降順次開始する予定であり、詳細が決まり次第、公表していきます。
（http://www.cas.go.jp/jp/seisaku/bangoseido/faq/faq6.html
2016年6月）

長崎県立大学
UNIVERSITY OF NAGASAKI

マイナポータル（附則第6条の2）

- 行政機関がマイナンバーの付いた自分の情報をいつ、どことやりとりしたのか確認できる
- 行政機関が保有する自分に関する情報を確認できる
- 行政機関から自分に対しての必要なお知らせ情報等を自宅のパソコン等から確認できる

例：各種社会保険料の支払金額や確定申告等を行う際に参考となる情 報の入手等が行えるようになる予定です。 また、引越しなどの際の官民横断的な手続のワンストップ化や納税などの決済をキャッシュレスで電子的に行うサービスも検討

（http://www.cas.go.jp/jp/seisaku/bangoseido/faq/faq6.html 2015年4月）

マイナンバーカード：2種類の電子証明書

- 署名用の電子証明書
  - ◆インターネット等で電子文書を作成・送信する際に利用：電子申請（e-Tax等）・民間オンライン取引（オンラインバンキング等）の登録など
  - ◆「**作成・送信した電子文書が、あなたが作成した真正なものであり、あなたが送信したものであること**」を証明できる

マイナポータルのセキュリティ

- 公開鍵暗号基盤方式を利用したオンライン認証
  - ◆暗号通信だけでなく、相手認証も行える
- マイナンバーカードの保持者認証
  - ◆マイナンバーカードを保持しているものしか使えない