欧州におけるプライバシー影響評価（PIA）とEU指令改正の動向

2011年9月14日

（株）国際社会経済研究所
小泉　雄介
y-koizumi@pd.jp.nec.com

アジェンダ

Ⅰ．プライバシー影響評価（PIA）

１．PIAの概要

２．日本における検討状況

３．英国の状況

４．ドイツの状況

Ⅱ．EUデータ保護指令の改正動向

Ⅰ．プライバシー影響評価（PIA）

１．PIAの概要

PIA（Privacy Impact Assessment：プライバシー影響評価）とは

○ 「個人情報の収集を伴う情報システムの導入または改修にあたり、プライバシーへの影響を事前に評価し、問題回避または緩和のための運用的・技術的な変更を促す一連のプロセス」 －瀬戸・伊瀬・六川・新保・村上著『プライバシー影響評価PIAと個人情報保護』（中央経済社、2010年）より －

○ 「社会保障・税番号大綱」との関係

→ 「情報保護評価」に該当

※ 「社会保障・税番号大綱」（平成23年6月30日）

「第３ Ⅵ 「番号」に係る個人情報の保護及び適切な利用に資する各種措置

12. 情報保護評価の実施

（1）「番号」に係る個人情報の適正な取扱いを担保するため、「番号」に係る個人情報の保護に関する事前評価（以下「情報保護評価」という。）を実施し、情報システムの構築又は改修が「番号」に係る個人情報へ及ぼす影響を評価し、その保護のための措置を講じることとする。

（2）行政機関及び関係機関は、「番号」に係る個人情報を取り扱うシステムを開発又は改修する前に、情報保護評価を行政機関又は関係機関内で実施した上で、その結果をＸＩで後述する内閣総理大臣の下に置く、番号制度における個人情報の保護等を目的とする委員会に報告し、その承認を受けるものとする。

（3）ＸＩの委員会は、行政機関及び関係機関（義務付け対象者）向けガイドライン、並びに地方公共団体及び法令に基づき「番号」を取り扱い得る事業者（非義務付け対象者）向けガイドラインを作成するものとし、情報保護評価の実施についての助言を行うことができることとする。ガイドラインには、情報保護評価を実施しなければならない情報システムについての基準や、情報保護評価の実施方法、実施手順等を記載することとする。

（4）（略）」

※ なお、「社会保障・税に関わる番号制度についての基本方針」（1月31日）の時点では「プライバシーに対する影響評価」と呼ばれていた。

※ 「関係機関」とは日本年金機構や医療保険者等をいう。「法令に基づき「番号」を取り扱い得る事業者」とは金融機関や源泉徴収義務者・特別徴収義務者等たる事業者等をいう。

PIAとプライバシーマークの比較

	PIA（プライバシー影響評価）	プライバシーマーク
評価の対象、評価の単位	個人情報を取扱う特定のシステム、制度、プロジェクト （必ずしも組織毎に行う必要はない。ある制度が複数の組織に跨って導入・実施されるような場合には、1つのPIAで対処することも可能。）	個人情報を取扱う組織 （具体的には、当該組織の個人情報保護マネジメントシステム。）
評価実施のタイミング	事前 （システム・制度等を導入・改修する前。具体的にはシステム設計の前。）	事前・事後は特に問わない
評価の実施主体	当該組織による自主評価 （但し、日本では第三者機関による承認手続きも想定されている。）	審査機関による第三者評価 （当該組織による内部監査も実施。）
主に誰に対してアピールするためのものか	国民	消費者、委託元企業
準拠基準	第三者機関等が制定するガイドライン （日本では「行政機関及び関係機関向け情報保護評価ガイドライン」を策定予定。）	JIS Q15001「個人情報保護マネジメントシステム－要求事項」

各国のPIA導入状況

○ カナダ
  – 1990年代から自主的に実施。
  – 2002年にカナダ財政委員会事務局がPrivacy Impact Assessment Policyにおいて、個人情報を取り扱うITシステムを導入・改修する行政機関にPIA実施を義務化。
  – 上記Policyの付属文書としてガイドライン”PIA Guidelines: A Framework to Manage Privacy Risks”を発行。

○ 米国
  – 2002年電子政府法の第208条において、行政機関にPIA実施を義務化（報告書写しを連邦行政予算管理庁OMBの長官に提出する義務）。
  – 2003年9月にOMBがガイダンス ”OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002”を発行。
  – 2007年発行の国土安全保障省ガイドラインもあり。

○ オーストラリア
  – 2006年に連邦プライバシーコミッショナー局が行政機関向けのガイダンス”Privacy Impact Assessment Guide”を発行。
  – PIA実施は義務ではなく、ガイドラインにおける推奨。

※上記3か国については、瀬戸・伊瀬・六川・新保・村上著『プライバシー影響評価PIAと個人情報保護』（中央経済社、2010年）等を参照した。

○ ニュージーランド、香港でも実施

○ 英国（後述）
  – 先進諸国の取り組みを参考に、2007年頃に導入。
  – 2008年より、内閣府が中央省庁に対してPIA実施を義務化。法令化はされていない。
  – 2007年に情報コミッショナーオフィス（ICO）がPIAハンドブックを発行。

各国のPIA導入状況（続き）

○ その他のEU各国におけるPIA導入状況

– フィンランド
  - PIAの利用が一時検討されていた。

– アイルランド
  - データ保護コミッショナーが職場や学校における生体情報利用に関するガイドラインを策定し、その中でPIAの実施を推奨。

– オランダ
  - PIAを導入したが、成果が上がっていない。（英国ICOからの情報）

○ EUにおけるPIA類似の制度

– 欧州では、EUデータ保護指令（95/46/EC）第20条において「Prior checking」（事前評価）を規定。
  - PIAそのものではないが類似。
  - 国内法への反映状況等は国により様々。EU27カ国中、少なくとも16カ国で条文化。
  - 例：オーストリア（個人データ保護法第18条）、フランス（情報処理・データと自由に関する法律第25条）。

※EUデータ保護指令第20条　Prior checking（弊社訳）

1. EU加盟各国は、データ主体の権利や自由に対して明示的なリスクを提示するおそれのあるデータ処理を特定し、これらのデータ処理がその開始に先立って吟味されるように評価を行うものとする。
2. このような事前評価は、データ管理者からの通知の受領の後に監督機関によって、もしくはデータ保護職員によって実施されるものとする。データ保護職員は、疑義が有る場合には監督機関に相談しなければならない。
3. （略）

– ドイツ（後述）
  - データ保護法第4d条でPrior checking（事前評価）を規定。官民が対象。

２．日本における検討状況

日本政府の社会保障・税大綱の概要①

1.番号制度導入の趣旨

現在

背景

- 少子高齢化（高齢者の増加と労働力人口の減少）
- 格差拡大への不安
- 情報通信技術の進歩
- 制度・運営の効率性、透明性の向上への要請
- 負担や給付の公平性確保への要請

課題

複数の機関に存在する個人の情報を同一人の情報であるということの確認を行うための基盤がないため、

- 税務署に提出される法定調書のうち、名寄せが困難なものについては活用に限界
- より正確な所得・資産の把握に基づく柔軟できめ細やかな社会保障制度・税額控除制度の導入が難しい
- 長期間にわたって個人を特定する必要がある制度の適正な運営が難しい（年金記録の管理等）
- 医療保険などにおいて関係機関同士の連携が非効率
- 養子縁組による氏名変更を濫用された場合に個人の特定が難しい

等

番号導入

将来

理念

- より公平・公正な社会の実現
- 社会保障がきめ細やかかつ的確に行われる社会の実現
- 行政に過誤や無駄のない社会の実現
- 国民にとって利便性の高い社会の実現
- 国民の権利を守り、国民が自己情報をコントロールできる社会の実現

効果

- 番号を用いて所得等の情報の把握とその社会保障や税への活用を効率的に実施
- 真に手を差し伸べるべき人に対しての社会保障の充実
- 負担・分担の公正性、各種行政事務の効率化が実現
- IT化を通じ効率的かつ安全に情報連携を行える仕組みを国・地方で連携協力しながら整備し、国民生活を支える社会的基盤を構築
- ITを活用した国民の利便性の更なる向上も期待

2．番号制度で何ができるのか

(1)よりきめ細やかな社会保障給付の実現

- 「総合合算制度（仮称）」の導入
- 高額医療・高額介護合算制度の現物給付化
- 給付過誤や給付漏れ、二重給付等の防止

(2)所得把握の精度の向上等の実現

(3)災害時における活用

- 災害時要援護者リストの作成及び更新
- 災害時の本人確認
- 医療情報の活用
- 生活再建への効果的な支援

(4)自己の情報や必要なお知らせ等の情報を自宅のパソコン等から入手できる

- 各種社会保険料の支払や、サービスを受けた際に支払った費用（医療保険・介護保険等の費用、保育料等）の確認
- 制度改正等のお知らせ
- 確定申告等を行う際に参考となる情報の確認

(5)事務・手続の簡素化、負担軽減

- 所得証明書や住民票の添付省略
- 医療機関における保険資格の確認
- 法定調書の提出に係る事業者負担の軽減

(6)医療・介護等のサービスの質の向上等

- 継続的な健診情報・予防接種履歴の確認
- 乳幼児健診履歴等の継続的把握による児童虐待等の早期発見
- 難病等の医学研究等において、継続的で正しいデータの蓄積が可能となる
- 地域がん登録等における患者の予後の追跡が容易となる
- 介護保険被保険者が市町村を異動した際、異動元での認定状況、介護情報の閲覧が可能となる
- 各種行政手続における診断書添付の省略
- 年金手帳、医療保険証、介護保険証等の機能の一元化

3.番号制度に必要な３つの仕組み

付番 新たに国民一人ひとりに、唯一無二の、民-民-官で利用可能な、見える「番号」を最新の住所情報と関連づけて付番する仕組み

情報連携 複数の機関において、それぞれの機関ごとに「番号」やそれ以外の番号を付して管理している同一人の情報を紐付し、紐付けられた情報を活用する仕組み

本人確認 個人や法人が「番号」を利用する際、利用者が「番号」の持ち主であることを証明するための本人確認（公的認証）の仕組み

4.安心できる番号制度の構築

- 国家管理（一元管理）への懸念
- 名寄せ・突合により集積・集約された個人情報の漏えい等の危険性への懸念
- 不正利用による財産その他の被害発生への懸念

制度上の保護措置

- 第三者機関の監視
- 法令上の規制等措置（目的外利用の制限、閲覧・複写の制限、告知要求の制限、守秘義務等）
- 罰則強化 等

システム上の安全措置

- 「番号」に係る個人情報の分散管理
- 「番号」を用いない情報連携
- 個人情報及び通信の暗号化
- アクセス制御 等

住民基本台帳ネットワークシステム最高裁合憲判決（最判平成20年3月6日）を踏まえた制度設計

5.今後のスケジュール

番号制度の導入時期については、制度設計や法案の成立時期により変わり得るものであるが、以下を目途とする。

- H23年秋以降 可能な限り早期に番号法案及び関係法案の国会提出
- 法案成立後、可能な限り早期に第三者機関を設置
- H26年6月 個人に「番号」、法人等に「法人番号」を交付
- H27年1月以降 社会保障分野、税務分野のうち可能な範囲で「番号」の利用開始
- H30年を目途に利用範囲の拡大を含めた番号法の見直しを引き続き検討

出典：政府・与党社会保障改革検討本部

日本政府の社会保障・税大綱の概要②

○番号法の構成(イメージ)

Ⅰ　基本理念

Ⅱ　個人に付番する「番号」

- 「番号」の付番、変更、失効

Ⅲ　「番号」を告知、利用する手続

年金分野
- 国民年金及び厚生年金保険、確定給付年金及び確定拠出年金、共済年金、恩給等の被保険者資格に係る届出、給付の受給及び保険料に関する手続

医療分野
- 健康保険(国家公務員共済組合法及び地方公務員等共済組合法に関する短期給付を含む)及び国民健康保険法等の被保険者資格に係る届出、保険料に関する手続
- 母子保健法、児童福祉法等による医療の給付の申請、障害者自立支援法による自立支援給付の申請に関する手続

介護保険分野
- 介護保険の被保険者資格に係る届出、保険給付の受給、保険料に関する手続

福祉分野
- 児童扶養手当、特別児童扶養手当、特別障害給付金等の支給申請に関する手続
- 生活保護の申請や各種届出に関する手続
- 母子寡婦福祉資金貸付、生活福祉資金貸付の申請に関する手続

労働保険分野
- 雇用保険の被保険者資格に関する届出、失業等給付の受給、公共職業安定所への求職申込、労災保険給付の支給に関する手続

税務分野
- 国税又は地方税に関する法令若しくは地方税に関する法令に基づく条例の規定により税務署長等又は地方公共団体に提出する書類への記載及びこれに係る利用
- 国税又は地方税に関する法令若しくは地方税に関する法令に基づく条例の規定に基づき、税務職員等又は地方公共団体の職員等が適正かつ公平な国税又は地方税の賦課及び徴収のために行う事務に係る利用

その他
- 社会保障及び地方税の分野の手続のうち条例に定めるもの
- 災害等の異常事態発生時の金融機関による預金等の払戻し等に係る利用

Ⅳ「番号」に係る個人情報
- 番号
- 左記Ⅲに掲げる手続のために保有される個人情報

Ⅴ「番号」に係る本人確認等の在り方
- 本人確認及び「番号」の真正性確保措置
- 「番号」のみで本人確認を行うことの禁止

Ⅵ「番号」に係る個人情報の保護及び適切な利用に資する各種措置
- 「番号」の告知義務、告知要求の制限、虚偽告知の禁止
- 閲覧、複製及び保管等の制限
- 委託、再委託等に関する規制
- 守秘義務、安全管理措置義務
- 「番号」に係る個人情報へのアクセス及びアクセス記録の確認
- 代理の取扱い
- 情報保護評価の実施

Ⅶ「番号」を生成する機関
- 組織形態(地方共同法人)
- 市町村への「番号」の通知
- 情報保有機関との関係(情報保有機関は番号生成機関に対し、基本4情報(住所、氏名、生年月日、性別)の提供を求めることができること。)

Ⅷ　情報連携
- 「番号」に係る個人情報の提供等(情報連携基盤を通じて情報の提供が行われること。)
- 情報連携の範囲
- 住基ネットの基本4情報(住所、氏名、生年月日、性別)との同期化
- 情報連携基盤の運営機関

Ⅸ　自己情報の管理に資するマイ・ポータル
- 設置、機能、運営機関(情報連携基盤の運営機関と同一の機関とする)

Ⅹ　マイ・ポータルへのログイン等に必要なICカード
- 交付
- 公的個人認証サービスの改良

ⅩⅠ　第三者機関
- 設置等(内閣総理大臣の下に委員会を置く)
- 権限、機能(調査、助言、指導等)

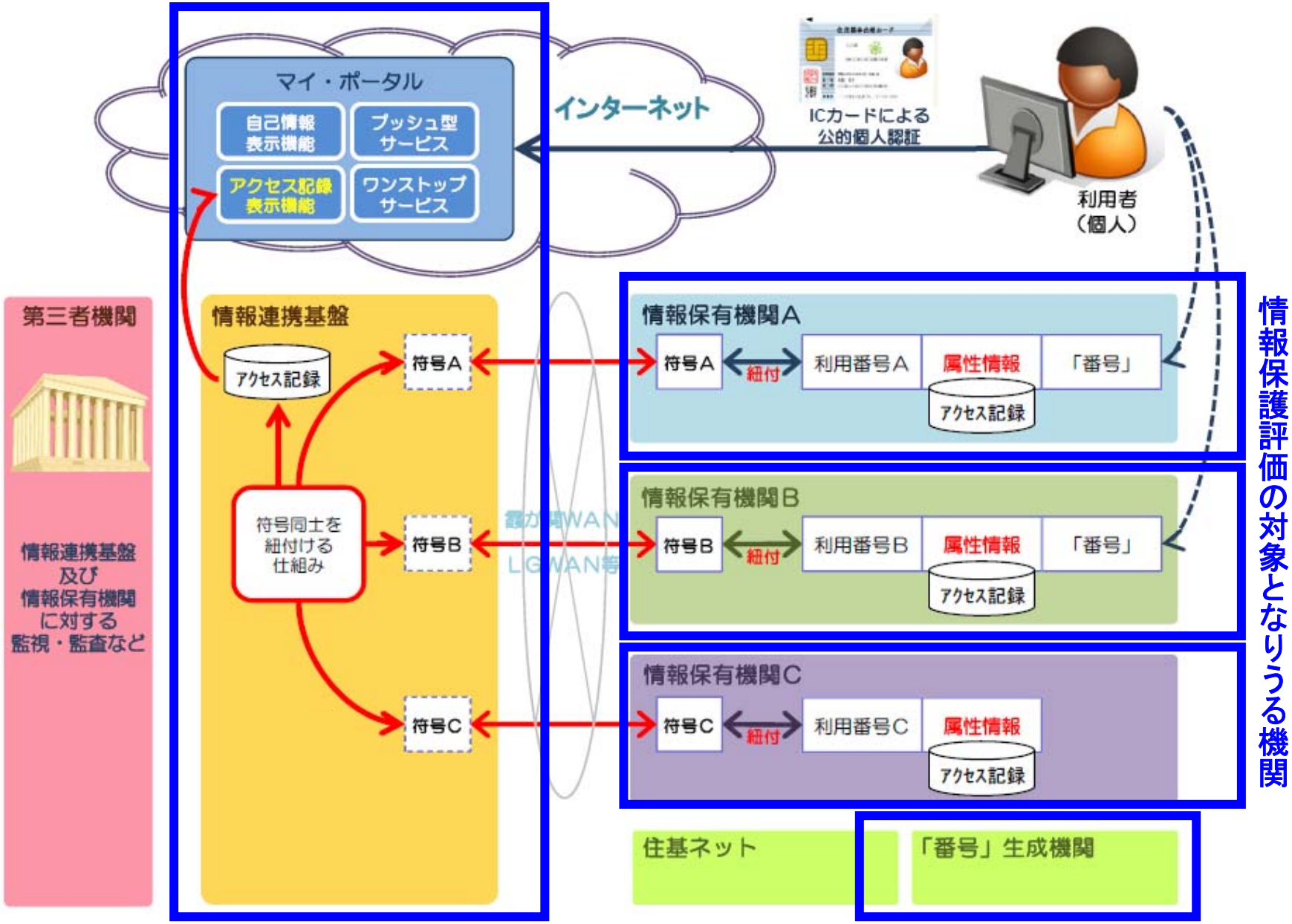
ⅩⅡ　罰則
- 行政機関、地方公共団体又は関係機関の職員等を主体とするもの
- 行政機関の職員等以外も主体となり得るもの
- 委員会の委員長等に対する守秘義務違反

ⅩⅢ　法人等に対する付番
- 付番、変更、通知
- 検索及び閲覧(法人等基本3情報(商号又は名称、本店又は主たる事務所の所在地、会社法人等番号)に係る検索、閲覧サービスの提供)
- 「法人番号」の適切な利用に資する各種措置
- 法人等付番機関(国税庁)

○情報の機微性に応じた特段の措置
- 医療分野等における個人情報保護法の特別法を整備(医療分野等の特に機微性の高い医療情報等の取扱いに関し、個人情報保護法又は番号法の特別法として、特段の措置を定める法制を番号法と併せて整備。)

出典:政府・与党社会保障改革検討本部

番号制度における符号連携のイメージ

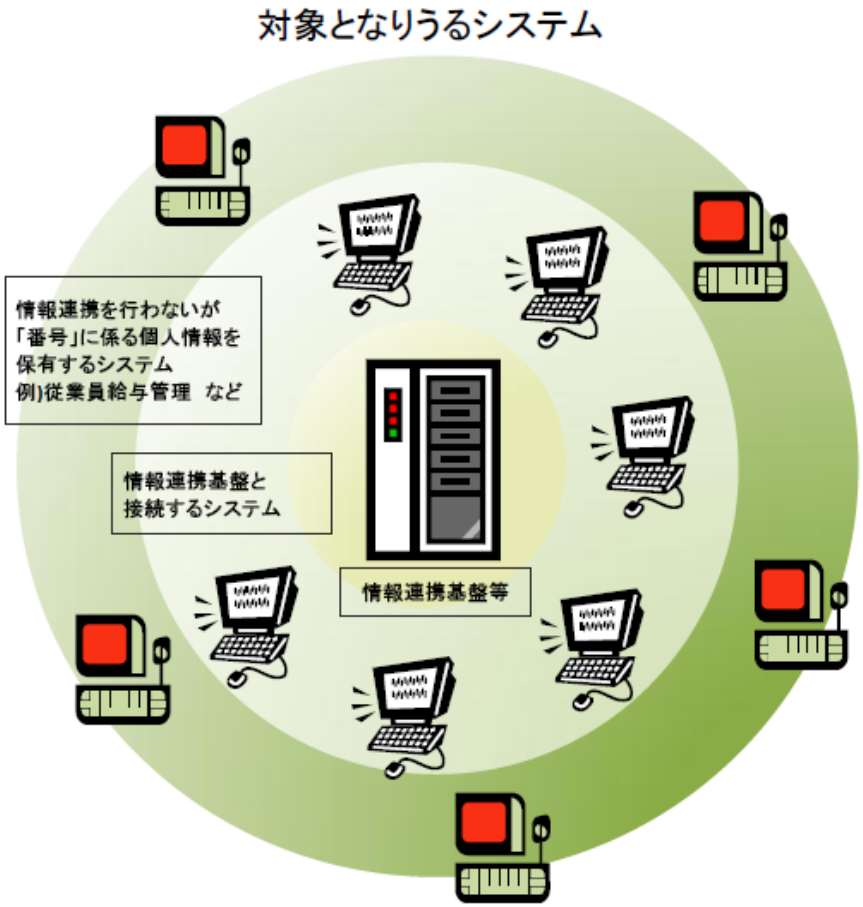


出典：情報連携基盤技術WG資料に加筆

情報保護評価の対象となりうる機関及びそのシステム

○対象となりうる機関

1	番号制度情報システム	
	1 運営機関(情報連携基盤・マイポータル)	
	2「番号」生成機関を担う地方共同法人	
2	社会保障分野	
	1 行政機関(厚生労働省ほか)	
	2 関連独立行政法人	
	3 地方公共団体	約1,800団体
	4 日本年金機構	1団体
	5 国民年金基金連合会	1団体
	6 国民年金基金	約70団体
	7 企業年金連合会	1団体
	8 厚生年金基金	約600団体
	9 企業年金基金(確定給付企業年金　基金型)	約600団体
	10 企業(確定給付企業年金・確定拠出年金)(規約型)	約13,000団体
	11 規約型企業年金信託の受託者たる信託銀行	
	12 石炭鉱業年金基金	1団体
	13 国家公務員共済組合(国家公務員共済組合連合会含む)	約20団体
	14 地方公務員共済組合(地方公務員共済組合連合会・全国市町村職員共済組合連合会含む)	約60団体
	15 日本私立学校振興・共済事業団	1団体
	16 日本鉄道共済組合	1団体
	17 日本たばこ産業共済組合	1団体
	18 NTT厚生年金基金	1団体
	19 農林漁業団体職員共済組合	1団体
	20 全国健康保険協会	1団体
	21 健康保険組合連合会	1団体
	22 健康保険組合	約1,450団体
	23 国民健康保険組合	約170団体
	24 後期高齢者医療広域連合	47団体
	25 社会保険診療報酬支払基金	1団体
	26 国民健康保険団体連合会	47団体
	27 国民健康保険中央会	1団体
	28 保険医療機関	約180,000団体
	29 保険薬局	約50,000団体
	30 介護サービス事業者	約260,000団体
	31 社会福祉協議会	約1,800団体
	32 適用事業所(健康保険・厚生年金保険)	約1,740,000団体
	33 適用事業所(雇用保険)	約2,000,000団体
	34 上記の他、公務員災害補償システムを保有するすべての行政機関・関係機関	
3	税務分野	
	1 国税庁	1団体
	2 地方公共団体	約1,800団体
	3 上記の他、公務員給与システムを保有するすべての行政機関・関係機関	約270団体
	4 源泉徴収義務者・特別徴収義務者(給与所得)	約3,637,000団体
	5 4以外の法定調書提出義務者	



(注1)上記機関は、「番号」に係る個人情報を保有する機関の例として大綱等に記載されているもの。
(注2)上記機関は、情報保護評価の非義務付け対象者(地方公共団体及び民間事業者)を含む。
(注3)地方公共団体については、上記の約1,800の都道府県及び市区町村のほか、厚生福祉に関わる一部事務組合・広域連合(939団体)、職員の退職手当や公務災害に関わる一部事務組合(91団体)、税務徴収に関わる一部事務組合・広域連合(23団体)等が存在する。(「地方公共団体間の事務の共同処理の状況調(平成22年7月1日現在、総務省自治行政局地町村体制整備課)」より、内閣官房社会保障改革担当室が集計したもの)

出典:情報保護評価SWG資料

現時点で想定されている情報保護評価のプロセス

- 情報保護評価の実施の仕組み（案）

出典：情報保護評価SWG資料

情報保護評価の必要性を判断する

(しきい値評価)

区分	情報保護評価	国民の意見	第三者機関の審査	公開
				
対象外	×	×	（論点）	（論点）
必要性が高くないもの	×	△ ※しきい値評価について各機関の裁量により意見聴取	△ ※しきい値評価をサンプリングチェック	○ ※しきい値評価を公開
必要性が高いもの	○	△ ※各機関の裁量により意見聴取	○ ※全件	○

情報保護評価サブワーキンググループ検討スケジュール

番号法（仮称）案が本年秋以降早期に国会に提出されることを前提に、以下のスケジュールを予定。

○ 第1回 日時：平成23 年 8月8日（月）
議題：論点の提示・整理
○ 第2回 日時：平成23 年 9月7日（水）
議題：論点に関する議論
○ 第3回 日時：平成23 年 9月30 日（金）
議題：論点に関する議論
○ 第4回 日時：平成23 年11 月
議題：論点に関する議論
○ 第5回 日時：平成23 年12 月
議題：中間とりまとめ

○ 平成23 年12 月～24 年1月頃
「行政機関及び関係機関向け情報保護評価ガイドライン」（仮称）の策定

○ 第6回 日時：平成24 年 1月
議題：地方公共団体向け及び法令に基づき「番号」を取り扱い得る事業者向けガイドラインについての論点の整理・議論
○ 第7回 日時：平成24 年 2月
議題：論点に関する議論
○ 第8回 日時：平成24 年 3月
議題：とりまとめ

○ 平成24 年4月頃
「地方公共団体向け情報保護評価ガイドライン」（仮称）及び
「法令に基づき「番号」を取り扱い得る事業者向け情報保護評価ガイドライン」（仮称）の策定

出典：情報保護評価SWG資料

3. 英国の状況

訪問時期：2011年4月中旬
訪問機関：
- ICO（情報コミッショナーオフィス）本部
- ICOスコットランド事務所
  （スコットランド政府Improvement Serviceと合同）
- BSI（英国規格協会）
- Ian Brown先生（オクスフォード大学）

英国におけるPIA導入状況

○ 導入の背景

- 情報コミッショナーオフィス（ICO）の「監視社会に関する報告書」（2006年）の中で、英国における監視社会（CCTV、IDカード等）の進展に対処するための手段としてPIAに言及。

○ その後の経緯

- 2007年5月頃、ICOがPIA国際調査（カナダ、オーストラリア、米国等）とハンドブック作成を公募。
- 2007年12月にICOがPIAハンドブック”Privacy Impact Assessment Handbook” を発行。
  - PIAの対象となるシステム（プロジェクト）は、個人データの処理を伴うもの全般（官民を問わない）。
  - 2009年6月に第二版発行。
- 2008年6月の内閣府の報告書“Data Handling Procedures in Government” において、中央省庁に対してPIA実施を義務化。
  - 2007年の歳入関税局での2500万人分のデータ入りCD-R紛失を受けたもの。
  - 法令化はされていないが、2010年1月までに中央省庁で270件の実施。
- 2010年8月、法務省が省庁向けPIAガイダンス“Undertaking Privacy Impact Assessments”を発行。
  - ICOハンドブックを簡易化。データ保護法への遵守に特化。

ICO（Information Commissioner‘s Office）の概要

- ○ データ保護（および情報公開）のための第三者機関
  - – EUデータ保護指令第28条で加盟各国に要請された「監督機関」に該当
  - – 官民におけるデータ保護法への遵守を監督することがミッション
  - – 活動内容
    - • ①個人や団体から法律違反に関する苦情を受け付け、対応する。
    - • ②団体に対して法律に従うためのベストプラクティスや教育を提供する。
    - • ③団体・個人に対して執行通知（データ取扱いの改善要求）を発行する（データ保護法第40条）。
  - – PIAは②の活動の一環である。
- ○ ICOの体制
  - – 現コミッショナーはグレイアム氏（2009年6月～）で4代目。
  - – 職員数は327名（2010年現在）。本部はマンチェスター郊外のWilmslow。
- ○ 独立機関であるが、法務省との結び付きが強い
  - – 情報コミッショナーは法務省が公募、法務省の国務大臣が選定、庶民院（衆議院）の委員会が承認、女王が任命。
- ○ 政府に対する発言権はそれほど強くない
  - – データ保護法違反の観点からデータ処理に対して意見表明可能（データ保護法第22条）。
  - – 2009年に、データ保護法に新たに55A条が追加され、データ侵害によって生じた損害に釣り合った罰金を官民の組織に課す新たな権限が付加された。
    - • 罰金の最高額は50万ポンド（約6600万円）に設定。

ICOがPIAにおいて果たす役割

○ ICOの役割はPIAの普及啓発のみ
  – ガイドライン（ハンドブック）の作成・提供。
  – 教育（トレーニング）・ワークショップ等。

○ PIAの実施方法は、実施機関の自主性に委ねられている
  – ICOは方法論を提供するのみで、PIAの実施方法について細かい指示はしない。
  – ICOとしては、PIAに関して新たに業務を増やすのではなく、既存の枠組み（ex.リスクマネジメント等）の延長上で実施することを推奨している。

○ PIA実施機関は、ICOにPIA報告書を提出したり、承認を得る義務はない
  – ただ、中央省庁に関しては、内閣府がPIA実施状況を管理。
  – PIA報告書の公開は義務ではないが、PIAハンドブックでは公表することを推奨している（セキュリティ・センシティブな情報は除いて）。
  – ICOは官民におけるPIAの実施状況を把握している訳ではないが、ICOへの問合せやイベントでの反応からPIAの浸透の度合いを見ると、行政分野では広範囲で利用されている。民間ではあまり利用されていない。

英国におけるPIAの特徴

○ 最大の特徴は「コンサルテーション・フェーズ」を重視していること
  – 「コンサルテーション」:
    利害関係者との話し合い・意見聴取。想定される影響やリスクの洗い出しが目的。
  – システムを利用する職員、システム開発に携わるIT企業・セキュリティ企業、プライバシーの影響を受ける市民・顧客などが対象。
  – コンサルテーションの方法は様々。ICOは特に方法を指定しない。
    • 市民に対するコンサルテーションの方法としては、フォーラムの開催、フォーカスグループの形成、市民団体への文書による照会、パブリックコメント等。
  – コンサルテーションの実施によって、プロジェクトの早期の段階で設計に変更を加えることが可能になるため、コンサルテーションは重要。
  – 市民に対しては、コンサルテーションで洗い出したリスクに対して、PIAを通じてこのように解決を図っていると説明することができるため、これによって反対意見を取り込むことが可能となる。

○ PIAの具体的方法はICOのPIAハンドブックにて規定

ICOのPIAハンドブックは、英国における「監視社会」の進展に対抗するICOの取組みの一環であり、カナダ・オーストラリアといった他国の取組みの研究に基づき、2007年12月に第1版が公表された。これは、英国で初めてのPIAに関するガイダンスである。第1版の公表後、「分量が長い」「繰り返しの箇所がある」といったいくつかの意見を受けて、2009年6月には第2版を公表した。以下の記述は第2版に基づく。

ICOのPIAハンドブックの概要①

○ なぜPIAを実施するか（PIAの目的）

（1）法令順守に留まらないプライバシー保護

PIAは、当該プロジェクトにおいて個人に対するプライバシーリスクを考慮に入れるためのプロセスであり、単に（英国の）データ保護法を順守するために必要となる措置よりもカバーする範囲が広い。

（2）ステークホルダーのコミットメントと一般市民の信頼の醸成

PIAは、関係するステークホルダーたちの見解を集め、適宜フィードバックを行う、透明でコンサルティブなプロセスである。そのため、PIAを実施することによって、一般市民を含むステークホルダーの理解やコミットメントを得ることができる。これによって、当該プロジェクトに対する一般市民のプライバシー保護面での信頼を醸成することが可能となる。

（3）事後の仕様変更やコスト発生の回避

PIAは当該プロジェクトの開始（設計等のフェーズ）に先立って、事前に実施するべきである。事前に行うことによって、PIAの実施組織が、起こりうる問題（プライバシーリスク）を予見したり、問題に対する解決策を事前に見出すことが可能となる。プロジェクトの中途や事後にPIAを実施することは避けるべきである。なぜなら、事後にシステムの仕様を変更したりエラーを直すことは、コストがかかるし、更なるエラーを引き起こす恐れがあるからである。

ICOのPIAハンドブックの概要②

○ PIAの実施プロセス

※例えば、システム改修時には、改修によって既存システムに新たな処理プロセスが追加される場合には、小規模版のPIAを推奨。

– Ⅰ．イニシャル・アセスメント
  - スクリーニング（質問表の利用）
    – PIAの実施が必要か否かの決定（さらに、フルスケール版か、小規模版※か）
    – 質問表への回答を全体的に検討して判断する
  - 利害関係者の特定
– Ⅱ．PIAの実施（下記はフルスケール版の場合）

①予備フェーズ（Preliminary Phase）
  – プロジェクト概要文書の作成

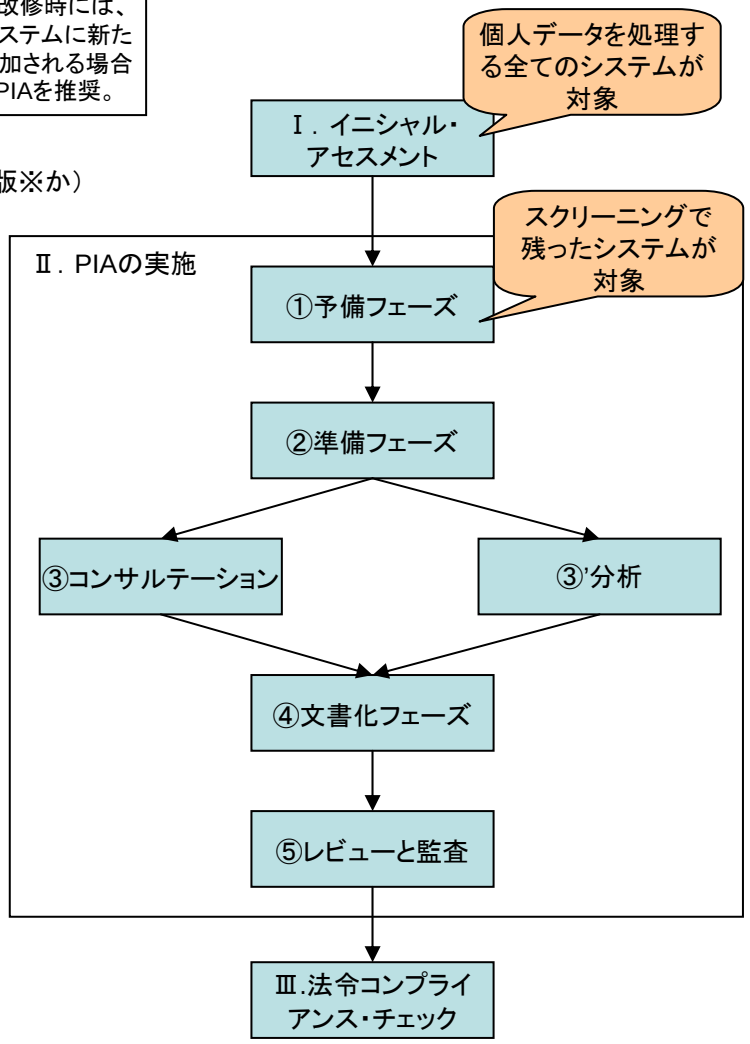
②準備フェーズ（Preparatory Phase）
  – 利害関係者とのコンサルテーション計画の作成
  – 諮問委員会の立ち上げ（利害関係者の代表者で構成）

③コンサルテーションと分析フェーズ（PIAの中核）
  – 利害関係者（市民を含む）とのコンサルテーションの実施
  – プライバシーリスクの特定
  – 個々のリスクに対する解決策（回避策または軽減策）の検討
  – 解決策の設計への組み込み（設計内容の変更）
  – 諮問委員会との相談

④文書化フェーズ（Documentation Phase）
  – PIA報告書の作成

⑤レビューと監査フェーズ（Review and Audit Phase）
  – 解決策が実装されていることのレビュー

– Ⅲ．法令コンプライアンス・チェック（チェックリスト利用）
  - プライバシー関連法令へのコンプライアンス・チェック
  - データ保護法へのコンプライアンス・チェック



出典：ICO"Privacy Impact Assessment Handbook"の図に筆者加筆

ICOのPIAハンドブックの概要③

○ プライバシーリスクの特定と解決策の検討

– コンサルテーション等を通じて特定したプライバシーリスクに対して、どのような解決策を実施するかを検討する必要があるが、取りうる解決策は、以下の3つに分類できる。
  - (a)リスク、影響、不利益を受容する。
  - (b)リスクを回避する方法を特定する。
  - (c)リスクを軽減する方法を特定する。

– (a)は、リスクが実現する可能性が極めて低いか、実現した際の影響が極めて少ない場合に取りうる選択肢であるが、あくまでもオプショナルな選択肢だと考えるべきである。この選択肢を取る場合には、リスクを受容することの理由付けを明確化する必要がある。

– (b)のプライバシー影響回避策（privacy impact avoidance measures）の例としては、以下の解決策が挙げられている。
  - 個人情報の収集を必要最低限のものに抑える。
  - 賛否両論のあるようなデータ項目を収集しない。
  - 意思決定において特定の情報の利用を取り止める（ex.就職活動時の履歴書における民族欄の削除）。
  - 個人の身体的自己を侵害するという論議を避けるために、生体情報は採用しない。

– (c)プライバシー影響軽減策（privacy impact mitigation/reduction measures）の例としては、以下の解決策が挙げられている。
  - 個人情報を記録しないことで、その保持を最低限に抑える。
  - 個人情報が必要なトランザクションが完了したら、速やかにそれを消去する。
  - 個人情報の消去スケジュールを定め、そのスケジュールを監査できるようにする。
  - 特定の目的で取得した個人情報の利用を、強力な法的・組織的・技術的安全手段によって制限する（目的外利用を防ぐ）： 苦情処理システムの導入・運用、厳格な罰則と執行能力による担保など。

イニシャル・アセスメントのスクリーニング質問表

11の質問（フルスケール版PIA用）　（弊社訳：一部抄訳）

（1）プロジェクトは、プライバシー侵害に実質的な可能性を持つ新たなもしくは追加的な情報技術を利用しているか？　ex. ICカード、RFID、バイオメトリクス、位置情報、監視カメラ等

（2）プロジェクトは、新たな識別子、既存の識別子の再利用、または侵害的な識別（identification）・アイデンティティ認証・アイデンティティマネジメントのプロセスを伴うものか？

（3）プロジェクトは、匿名性や偽名性を否定したり、従来は匿名・偽名で実施可能だったトランザクションを本人を特定するトランザクションに変更したりするものであるか？

（4）プロジェクトは、政府機関か民間企業かに関わらず、複数の組織を巻き込むものであるか？

（5）プロジェクトは、個人に特定の不安を与えるような個人データの新たな取扱いや、取扱いに関する重大な変更を伴うものであるか？　ex. 特定機微情報

（6）プロジェクトは、データベース内にある各個人に関する個人データのかなりの量について、新たな取扱いや、取扱いに関する重大な変更を伴うものであるか？

（7）プロジェクトは、大量の数の個人に関する個人データの新たな取扱いや、取扱いに関する重大な変更を伴うものであるか？

（8）プロジェクトは、複数のソースからの個人データの新たな連結や相互リンク（紐付け）、相互参照、マッチング、あるいはそれらの重大な変更を伴うものであるか？

（9）プロジェクトは、法令上のプライバシー保護の適用除外となるような仕方で、データ処理を行うか？

（10）プロジェクトの正当化理由は、公共のセキュリティ安全保護対策における寄与を含むものであるか？

（11）プロジェクトは、相当のプライバシー法制の影響下にない第三者への個人データの系統的な提供や、それらの第三者によるアクセスを伴うものであるか？

PIA実施プロジェクトの例①：スコットランド国民資格カード

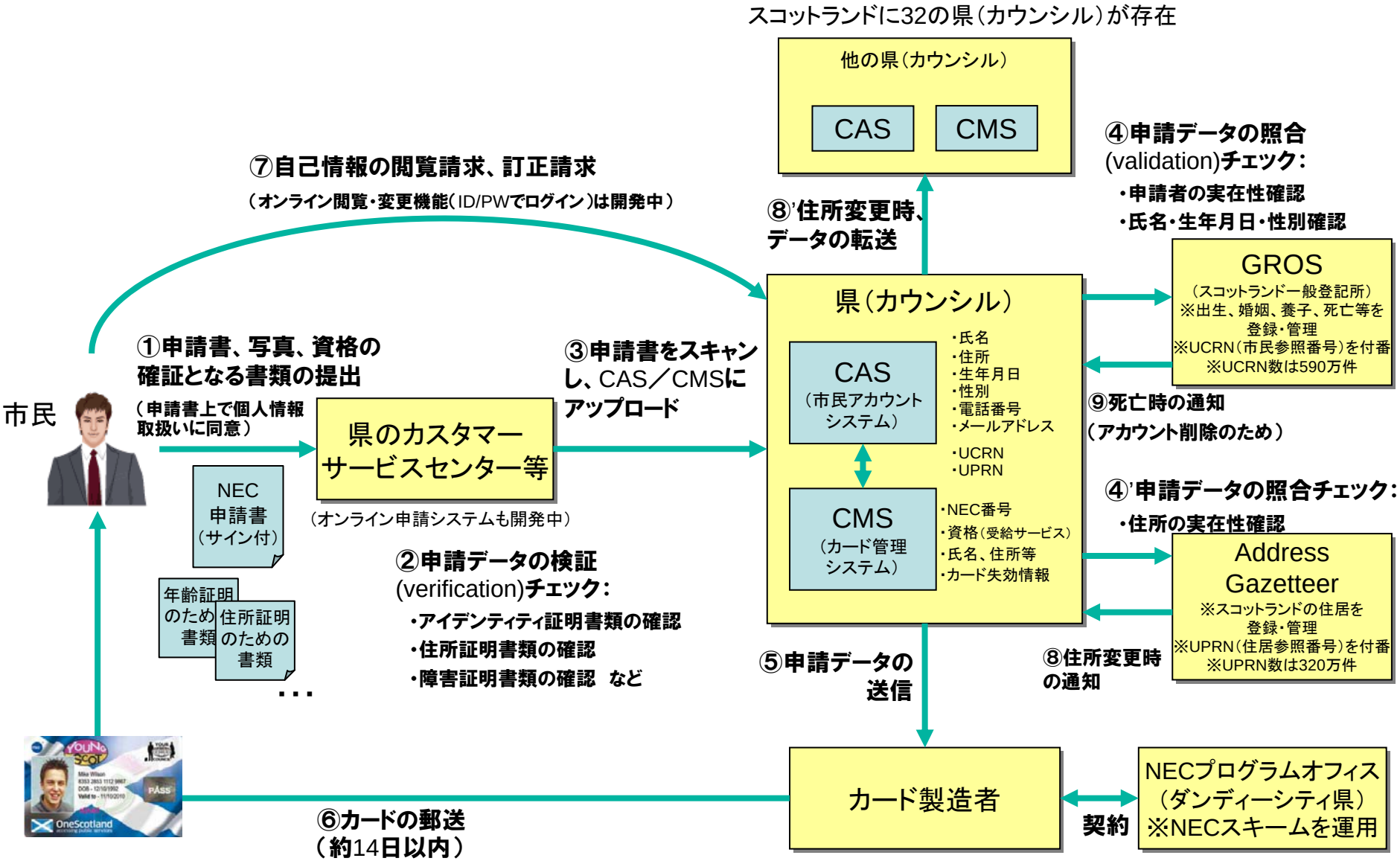
○ 国民資格カード（National Entitlement Card、NEC）の概要
  – 公共交通機関の割引乗車（高齢者、子ども、障害者）等、特定の公共サービスを受ける資格があることを示すカード。希望者のみに配布。
    2006年開始、160万人の利用者（cf. スコットランドの人口509万人）。

○ 券面記載情報
  – 氏名　　ー 生年月日
  – 写真　　ー NEC番号（16桁）
  – 有効期限　　ー PASSホログラム
  – ITSOやOneScotland、県のロゴ
  – 特定サービスの資格を示すロゴ
    （SPT、交通、Young Scot、sQuid（電子マネー）など）

○ ICチップ格納情報
  – ITSO用のセクション（乗車券情報）
  – 割引乗車券情報、民間の乗車券情報
  – 氏名・住所・生年月日・性別等
  – 図書館会員番号、スポーツジム会員番号等

○ 国民資格カードで利用できるサービス
  – 公共交通機関の割引乗車（子ども、高齢者、障害者）
  – 図書館やレジャー施設の会員カード
  – 商店での割引
  – 学校飲食施設での支払い　　ー　sQuid（電子マネー）等

スコットランド国民資格カードの運用



※上図のように様々な機関が関与しているが、各々の機関が個別にPIAを実施している訳ではない。

スコットランド国民資格カードのPIA

○ PIA実施概要

- コンサルテーション・フェーズ
  - 対象者：システム利用者（スコットランド政府・地方政府職員、公共サービス提供者の職員）、一般市民
  - 市民へのコンサルテーション内容（市民パネルに対して実施）
    - 「NECの導入によってどのような問題が懸念されるか？」
    - 「そのような懸念に対して、どのように対処したらよいか？」
  - 市民からの代表的意見
    - 「NEC管理システムに市民の情報が集積され過ぎるのではないか（政府がビッグブラザーになるのではないか）」
    - 「英国政府（特にIDカードシステム）と個人情報が共有されるのではないか」
    - 「カードのチップに個人情報を入れ過ぎるのはないか」
- 実施体制・期間
  - PIAチームは1名であり、セキュリティ会社に委託。スコットランド政府の担当者がPIAチームを監督
  - 約6ヶ月でPIA報告書ドラフトを作成し、スコットランド政府担当者が査閲・修正した。修正した報告書をシステム利用者（職員等）に提示し、フィードバックを受けた。正式なPIA報告書発行に至るまでのPIA実施期間は1年間程度だが、スコットランド政府担当者の多忙による遅延があった
- PIA報告書において市民にアピールしたこと
  - NECは（廃止になった）英国のIDカードとは別スキームであり、情報が共有されることもない。
  - NECにおいて市民の情報（特にカード利用履歴）を一元管理することはない。また、市民から取得する情報は、サービス提供に必要最小限なものである。
  - NECの利用は任意であり、公共サービス提供者への情報提供については必ず事前に本人の同意を取得する。

※ 作成時の苦労としては「PIA報告書を一般市民に読んでもらえるように極力簡潔なものとした」こと。

PIA実施プロジェクトの例②：警察全国データベース（PND）

- PNDの概要
  - 警察全国データベース（Police National Database）
  - イングランドとウェールズの43の警察機関でローカルに管理されている情報へのリンクを提供するDB。
- PIA実施概要、教訓等
  - 実施期間
    - 2008年2月　イニシャル・アセスメント（スクリーニング） → フルスケール版PIA
    - ～2008年4月　コンサルテーション（関連機関・団体への文書による照会）
    - （分析フェーズ後に、報告書ドラフトを用いて再度コンサルテーションを実施）
    - 2009年4月　PIA報告書の公表
- PIA実施後にシステムに加えた機能や運用
  - アクセス者の限定とトレーニング
  - 職務に必要なデータや機能のみにアクセス可能とすること（アクセスコントロール）
  - 利用ログの保存と監査
  - プライバシー要件（プライバシー原則）を考慮した機能設計
    - ex. PNDから警察機関へのデータ移転に対する一定の制限や安全保護措置　等
  - システムおよびデータ利用規則の策定

（ご参考）英国におけるその他の個人情報保護関連の動向

- PbD（Privacy by Design）については、ICOがデータ保護法に盛り込むことを提案。
  - PbDは「設計段階からプライバシー保護を組み込む」というシステム開発の1つの「哲学」であり、実践手段としてPIAやPET（Privacy Enhancing Technology：プライバシー強化技術）を伴う。
  - なお、EUデータ保護指令については2011年内に改正案が提出される予定であり、EU各国の国内法もそれに合わせて改正される見込み。

- BSI（英国規格協会）が2009年にBS10012を策定。
  - データ保護法を遵守した個人情報マネジメントシステムのための仕様。
  - 上記の歳入関税局など、漏えい事件が相次いだことが背景。
  - 現時点では、BS10012の第三者認証制度は存在しない。

PIAで守ろうとしている個人の権利利益(プライバシー)とは何か？

① 国家による不必要な個人情報収集や利用、提供を防ぐ側面

- 個人の権利に対する侵害を国家にどこまで認めるかという座標軸。
  - 一般的に、市民社会・民主主義が発展した先進国ほど人権(個人)寄りに傾き、新興国・途上国ほど国家寄りに傾く。

- 具体的には、政府機関が国民からどのような個人情報を取得でき、その情報をどのような目的で利用・提供できるかの範囲の狭さ(明確さ)⇔広さ(曖昧さ)。
  - 侵害性が高い個人情報の例: 特定機微情報、生体情報、位置情報、監視カメラ情報
  - 侵害性が高い利用目的の例: 個人の行動追跡、(思想統制、社会的差別)等

- 人権(が侵害されるリスク)と公共(共同体)の利益とを天秤にかけることが必要。
  (例) 個人の権利 ＜ 大災害時の対応(要援護者の避難支援のために自治体保有の情報を共有すること)
  (例) 個人の権利 ＞ 大災害時の対応(遺体確認のために全国民のDNAを事前登録すること)

② それ以外の、一般的な個人情報保護の側面

- 自己情報コントロール権を確保する。
  - 本人が利用目的に同意した上での個人情報取得
  - 本人情報の開示・訂正・利用停止等の請求権
- 行政職員による不正な個人情報取扱いを防ぐ。

４. ドイツの状況

訪問時期：2011年4月中旬
訪問機関：
・連邦データ保護監察官事務所
・ベルリン州データ保護監察官
・連邦情報セキュリティ庁

ドイツにおける「事前評価」

○ 連邦データ保護法の第4d条でデータ保護のためのPrior checking（事前評価）を規定

※連邦データ保護法　第4d条5項　（弊社訳）
自動化されたデータ処理が、本人（データ主体）の権利および自由に対する特別なリスクにつながる場合、そのようなデータ処理は開始に先立つ段階における評価（事前評価）の対象となる。事前評価は、特に以下のような場合に実施すること。
1. 特別な種類の個人データ（第3条9項）（＊註1）の処理を行う場合
2. 個人データの処理が、本人の能力を含む、個人的特徴、実績、または行動を評価するためのものである場合

ただし、以下のような場合は事前評価の対象とはならない：
法的な義務または本人の許可が存在し、もしくは本人との法的行為または法的行為に類する債務関係の証明、実行、または完了のために、（個人 データの）収集、処理もしくは利用が必要である場合。

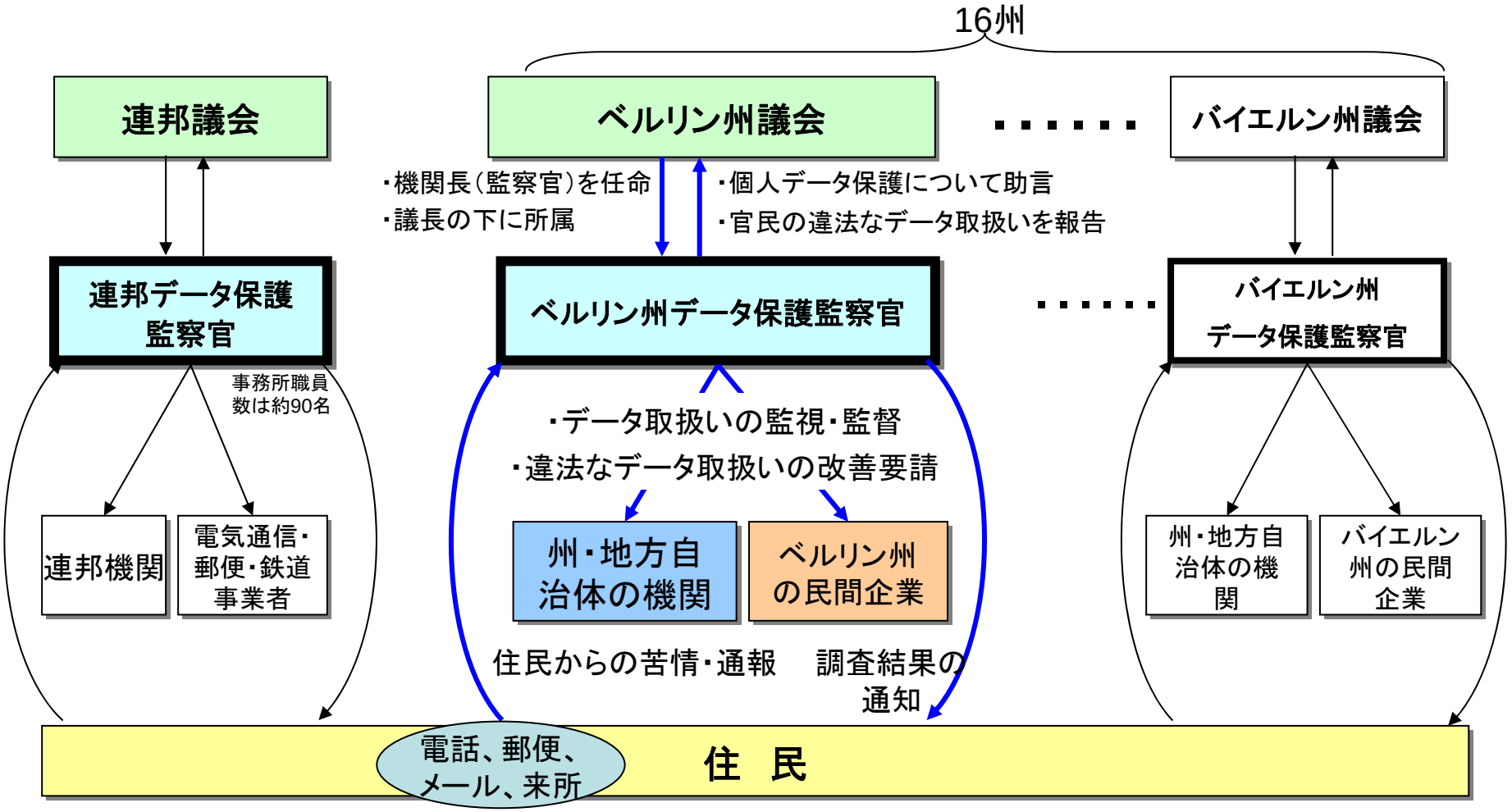
（＊註1）人種・民族、政治的見解、宗教・哲学的信条、労働組合への加盟、医療、性生活に関する個人データ

○ 官民の機関・組織が個人データの自動処理を行う場合には、事前評価が必要。
- 紙での取り扱いのみの場合は必要ない。
- 事前評価は、当該機関・組織によって自主的に実施される。
- 事前評価の実施責任者は、当該組織のデータ保護担当者である。
  - 個人データの自動処理を行う組織（官民）はデータ保護担当者を任命しなければならない（第4f条1項）。
- 事前評価結果をデータ保護監察官（データ保護のための監督機関）に報告する義務はない。
  - ただ、データ保護監察官による監査時に、事前評価の未実施が判明すると、罰金が課される。

○ 事前評価に関する詳細規定やガイドラインは存在しない
- データ保護担当者の資格基準があり、これによって各機関は事前評価の水準を担保。
- 事前評価のやり方や結果の妥当性について、データ保護担当者からデータ保護監察官への問合せは多い。

データ保護監察官の概要

・行政・民間における個人データの取扱いを監督する第三者機関。EU指令第28条の「監督機関」に該当。
・連邦、16の各州に存在。
・連邦監察官は、連邦政府が推薦し、連邦議会が選任し、連邦大統領が任命する。
・連邦監察官事務所のスタッフは内務省職員の出向。ただし、任期期間中は内務省の指示を受けない。



Ⅱ．EUデータ保護指令の改正動向

EUデータ保護指令の背景

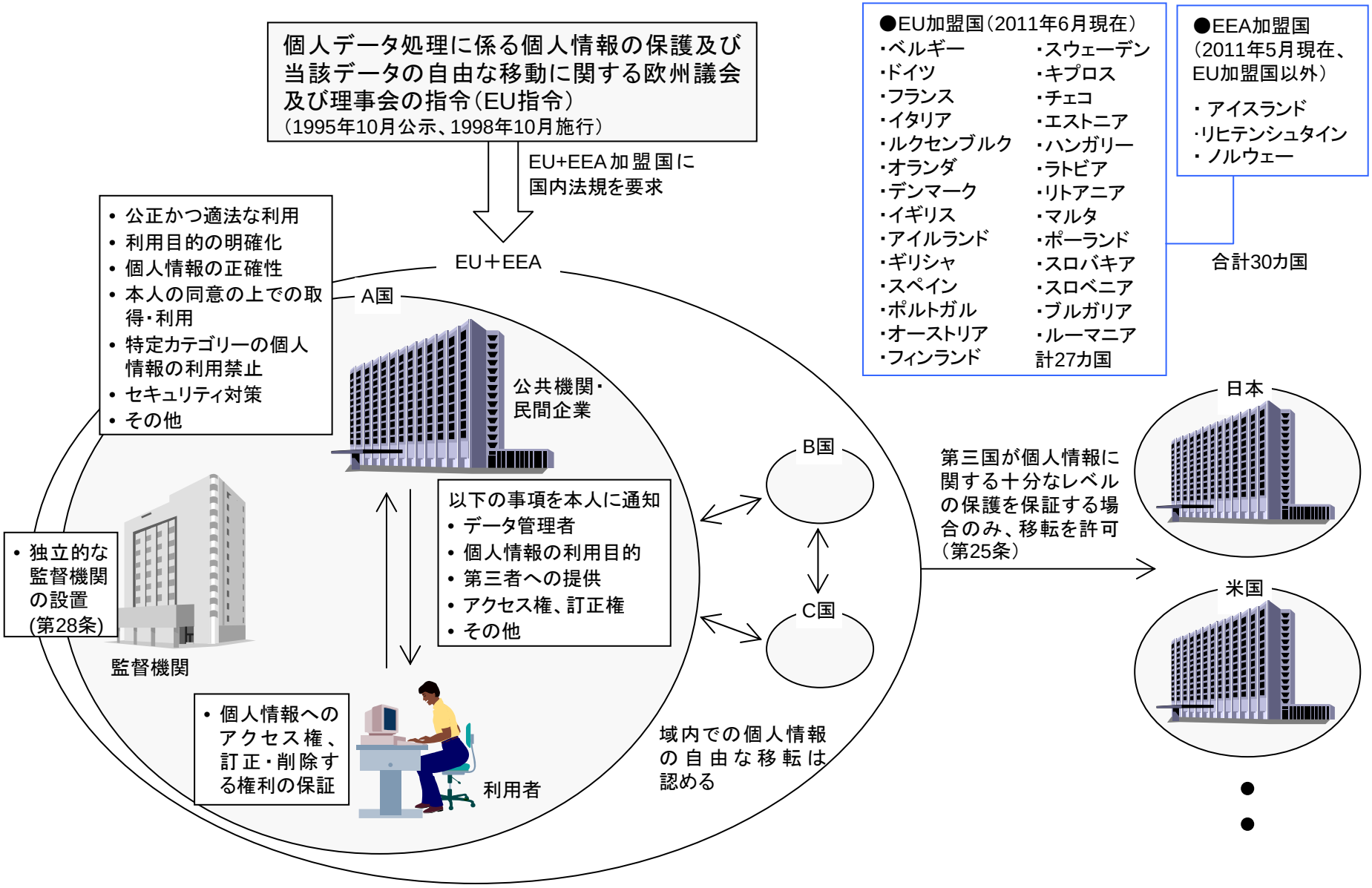
○ EUデータ保護指令（EU指令）制定の背景

- 1980年の欧州評議会「個人データの自動処理に係る個人の保護に関する条約」（CoE個人情報保護条約）がモデル
  - CoE条約はOECDプライバシーガイドラインとほぼ同時期に採択。
- 1990年　欧州共同体理事会「個人データ取扱いに係る個人の保護に関する理事会指令提案」
- 1992年　欧州共同体理事会「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する理事会指令の改正提案」
- 1993年　欧州連合（EU）発足
- 1995年　欧州議会及び理事会「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する1995年10 月24 日の欧州議会及び理事会の95／46／EC 指令」（EUデータ保護指令）の採択
- 1998年　EUデータ保護指令の発効

○ EU指令制定の目的

- 個人の基本的人権と自由（とりわけ個人データの処理に係るプライバシーの権利）を保護し、かつ加盟国間でのデータの自由な流通を妨げないことを目的としている。（EU指令第1条）
- 「1995 年のEU のデータ保護指令の目的は、できる限り高いレベルの統一的な個人情報保護の制度の構築を通じて、EU 域内及びヨーロッパ経済圏（EEA）における自由なデータ流通を一層促進しようというものであった。」（内閣府「国際移転における企業の個人データ保護措置調査報告書」より）

EU指令の概要



EU指令改正の背景

○ 2011年内に欧州委員会が改正案を提出する予定

○ EU指令改正の背景

出典：欧州委員会文書「欧州委員会から欧州議会、理事会、経済社会委員会、及び地域委員会への伝達：欧州連合における個人データ保護に関する包括的アプローチ」（2010年11月4日）

– 個人の基本的人権と自由（とりわけデータ保護の権利）を保護すると共に、個人データの自由な流通を促進するという当初からの目的は変わらない。
– 制定から15年が経ち、急激な技術的進歩とグローバル化が社会を変え、個人データ保護に新たな課題をもたらしている。
  - 個人が自分の行動や嗜好について他人と共有したり、全世界的に公開することが容易になった。SNSサイトが最も顕著な事例。
  - クラウドコンピューティングも個人データ保護に課題を投げかけている。他の場所のHWに個人データを保存するため、個人が自分の個人データに対するコントロールを失う恐れがある。
  - こうしたオンライン活動に関連し、プライバシーと個人データ保護に対するリスクは拡大。
– 個人データの収集方法はいっそう高度化し、容易に検知できないものとなっている。
  - 個人行動を監視するツールによって、企業が個人を容易にターゲッティング。
  - 電子交通チケット、電子道路通行料、位置情報端末により、個人の位置等が容易に把握。
  - 行政機関は個人データをより多様な目的で利用するようになった。
    伝染病発生時の個人の追跡、テロや犯罪の防止や対処、社会保障領域での利用、徴税目的での利用、電子政府アプリケーションでの利用など。

EU指令改正の背景（続き）

○ EU指令改正の背景（続き）

– これらの課題に対して既存のEU指令が適切に対処できるかを検討するために、欧州委員会は2009年5月にEU指令の見直しを初め、2009年末までパブリック・コンサルテーションも行った。

– この中で、以下のような事項はとりわけ大きな問題であると認識された。

① 新たな技術のインパクトに対処すること。

② 個人データ保護に関するEU域内市場の特質を強化すること。

– EU加盟国間でのデータ保護に関する法制度の整合が十分に取れていない。

③ グローバル化に対処し、国際データ移転を改善すること。

– EU域外へのデータ処理のアウトソーシングにおいて、当該処理に適用される法律等に関して問題が生じている。

– 国際データ移転に関しては、多くの企業が現行のスキームは不満足なものであり、単純化する必要があると見なしている。

④ データ保護規則の効果的な執行のために制度整備を強化すること。

– 監督機関の役割を強化する必要がある。

⑤ データ保護法的フレームワークの整合性を改善すること

EU指令改正の方向性

○ 上記2010年11月4日の欧州委員会文書に方向性が示されている
タイトル「欧州委員会から欧州議会、理事会、経済社会委員会、及び地域委員会への伝達： 欧州連合における個人データ保護に関する包括的アプローチ」

○ 目次

- 1. 個人データ保護に対する新たな課題
- **2. 個人データ保護に関する包括的アプローチの主要な目的**
  - **2．1 個人の権利の強化**
    - **2．1．1 あらゆる環境における個人の適切な保護の確保**
    - **2．1．2 データ主体に対する透明性の確保**
    - **2．1．3 自己のデータに対するコントロールの向上**
    - **2．1．4 意識向上**
    - **2．1．5 情報に基づく自由な同意（informed and free consent）の確保**
    - **2．1．6 センシティブ・データの保護**
    - **2．1．7 救済及び制裁の一層の効率化**
  - **2．2 域内市場特質の強化**
    - **2．2．1 法的確実性の増進、及びデータ管理者への公平な競争の提供**
    - **2．2．2 管理上の負担の軽減**
    - **2．2．3 準拠法と加盟国の責任に関する規則の明確化**
    - **2．2．4 データ管理者の責任の強化**
    - **2．2．5 自主規制イニシアティブの奨励、及びEU認証制度の探求**
  - **2．3 刑事事件における警察・司法協力分野のデータ保護規則の見直し**
  - **2．4 データ保護のグローバルな特質**
    - **2．4．1 国際データ移転のための規則の明確化と単純化**
    - **2．4．2 ユニバーサルな諸原則の促進**
  - **2．5 データ保護規則のよりよい執行のための制度整備の強化**
- 3. 結論：将来の方向性

EU指令改正に向けた検討項目

EU指令改正に向けた検討項目（主要論点）

○ ２．１．３　自己のデータに関するコントロールの向上

– データ最小化の原則（データ取得を必要最小限に留めること）の強化
– 個人のアクセス・訂正・削除・利用停止権を実現する手段を改善する
– いわゆる「忘れられる権利（right to be forgotten）」を明確化する
  - 個人データがもはや正当な目的では必要とされなくなったときに、個人が自分の個人データの処理を停止したり、削除したりする権利
  - SNSサイトでは、利用者が写真等の情報を削除しようとしても削除できないケースがある。「神は許し、忘れてくれるが、Webはそうしてくれない」
– 「データ・ポータビリティ」を保証することにより、データ主体の権利を補完する
  - 個人が或るサービスから自分の個人データ（写真、友人リスト等）を撤収し、他のサービスに移転したりすることを可能とする明示的な権利を提供する

○ ２．２．３　準拠法と加盟国の責任に関する規則の明確化

– 準拠法に関する規定（EU指令第4条※）を見直し、データ管理者の地理的な位置に関わらずEU市民が保護されるようにする
  - 現在、ネットによってEU域外の企業がサービス提供したりデータ処理することが容易
  - クラウドコンピューティングにおいては、或る時点での個人データの位置やデータ処理設備の位置を特定することが困難
  - EU市民を対象としたオンラインサービスを提供する企業はEU規則に従わなければならない。例えば、EUの利用者を持つ米国のSNS企業はEU規則に従う必要がある

※ EU指令第4条：EU域内のデータ管理者（企業等）には当該加盟国の法律が適用される。EU域外のデータ管理者であっても、EU域内の設備でデータ処理を行っている場合は、当該国の法律が適用される。

EU指令改正に向けた検討項目（主要論点）（続き）

○ ２．２．４　データ管理者の責任の強化
- 独立的なデータ保護オフィサーの任命を義務付ける
- 特定のケースにおけるデータ保護影響評価（＝プライバシー影響評価）の実施を法制度において義務付ける
  - センシティブデータを処理する場合、明示的なリスクを伴う処理の場合（とりわけ、特定技術を使用したり、プロファイリングや監視カメラを使用するような場合）
- プライバシー強化技術（PET）の使用を推奨する
- 「プライバシー・バイ・デザイン」の概念の具体的な導入の可能性を推奨する

○ ２．３　刑事事件における警察・司法協力分野のデータ保護規則の見直し
- この分野において、個人のデータ保護の権利（アクセス権や透明性の原則）に各国間で整合的な制限を設ける
- この分野において、遺伝子データの処理に係るデータ保護等について、整合的な規則を導入する

○ ２．４．１　国際データ移転のための規則の明確化と単純化
- 国際データ移転のための現行の手続き（標準契約条項やBCRを含む）を改善し簡素化する
  - 現状、標準契約条項は、非契約的状況や、行政機関間のデータ移転には使用できない
- 欧州委員会の「十分性認定」の手続きを明確化し、規準や要件を明示する

（ご参考）クラウドコンピューティングに関する論点：欧州でのヒアリング内容より

○ 英国規格協会（BSI）

– 「現在、データ保護に関してBSIで課題と認識していることは、他の企業に個人情報を委託する場合や、海外の企業に個人情報を委託する場合（オフショアリング。例えばインドのコールセンター会社に個人情報を委託する場合）である。いずれも個人情報の管理責任は、委託元企業にある。NHS（国民保険サービス）などでは、国際的な標準の導入とコミュニケーションによって、アウトソーシング先におけるデータ保護を担保するための方策を検討している。国際的な標準によって解決できる見込みはあるが、国によって保護のレベルが異なるので、英国のレベルを保てるかという課題は残る。」

○ ドイツ・連邦データ保護監察官事務所

– 「ドイツ国外の企業にアウトソーシングする場合、法律的な観点からは、アウトソーシング先がEU内の企業であれば、EU指令に基づき、EUのデータ保護水準が確保されるので問題ない。ただクラウドコンピューティングだと、まずデータがどこにあるかを特定できないので、データ保護法の保護水準には該当しないということで、最初の時点ではじかれる。委託する企業は、契約内で、どこでデータを保存するかを明記するようにしなければならない。

– 技術的な対策としては、委託元企業以外は処理できないように、クラウド上に保存するデータは暗号化する方法がある。ドイツでクラウドを使う企業は、データの処理自体はドイツ国内でという契約条項を設けることが多い。

– EU指令に定めるデータ保護水準を達成することは、日本にとっても利益になるだろう。」

（ご参考）クラウドコンピューティングに関する論点：欧州でのヒアリング内容より

○ ドイツ・ベルリン州データ保護監察官

– 「民間企業からクラウドコンピューティングにおけるデータ保護に関する問合せは多い。解決策までは見いだせていないが、特にサービス提供者に対するデータ保護の圧力がかかっている。企業のデータ保護の分野では一番の議論のテーマになっている。企業がデータを外部に保存する場合に、各企業の保護の基準にどう対応させていったらよいかということである。

  • 例：ベルリン州の学校がGoogleのストレージサービスに個人データを預けようとしているが、ドイツのデータ保護法やデータ保護監察官の立場からは、Googleはどこでデータを保管し、どこでデータを処理するかが明確でないため、認められない。データ保護監察官と当該学校の両者で議論しているところである。ちなみに、デンマークではオーデンセ（人口第三の都市）において、同様なケースにおいてGoogleへのデータ委託禁止の判定が出た。

– ベルリン州内でデータをクラウド化しているのは問題がない。EU域内で保管する分にも問題ではない。Googleの場合、世界のどこでデータを保管しているかが分からない。

– 米国では（愛国者法により）捜査機関が企業の保有するデータを利用することができるので、危険である。」

発表者の経歴

- 1998年（株）NEC総研入社。
- 電子政府・個人認証、個人情報保護、違法有害情報規制分野を中心に、情報技術が社会に与える影響についての調査研究に従事。
- 2008年7月より、日本電気（株）新IT戦略推進本部に出向。2010年7月に（株）国際社会経済研究所（旧NEC総研）に復帰。
- 2006年～2010年、日本セキュリティマネジメント学会理事。
- 著書
  - 『国民ID　導入に向けた取り組み』（共著、NTT出版、2009年）
  - 『デジタル・ツナガリ』（共著、NTT出版、2004年）
  - 『ブロードバンド国家戦略』（共著、NTT出版、2003年）
  - 『経営戦略としての個人情報保護と対策』（共著、工業調査会、2002年）
  - 『デジタル・デバイド』（共著、NTT出版、2002年）
- 論文
  - 「国民ID制度の概要と海外の最新事情」（共著、『CIAJ Journal』 2011年1月号）
  - 「将来を見据えた国民ID構築のための提言」（共著、日本セキュリティ・マネジメント学会第24 回全国大会研究報告書、2010年）
  - 「オーストリアの電子IDカードと市民カード」（共著、『情報化研究』、情報産業振興議員連盟、2008年）
  - 「諸外国におけるインターネットカフェ関連法制に関する調査」（共著、『季刊 社会安全』NO.68、社会安全研究財団、2008年）
  - 「諸外国におけるホットラインの実態調査」（『季刊 社会安全』NO.65、社会安全研究財団、2007年） など