

マイナンバー法案における 個人情報保護とセキュリティ —問題検討の契機のために—

DBSCセミナー(2012年5月23)

東京電機大学(北千住キャンパス)

一橋大学名誉教授 堀部政男

自己紹介

- ① プライバシー・個人情報保護について半世紀
(50年)以上にわたり研究・実践
- ② 国の個人情報保護関係法のすべてに関与
- ③ 東京都・神奈川県等の地方公共団体の個人情報保護条例制定・運用に関与
- ④ 民間部門の個人情報保護ガイドライン策定等に関与
- ⑤ 国際的に活動

①プライバシー・個人情報保護について 半世紀(50年)以上にわたり研究・実践

- 1962年 東京大学大学院修士課程(基礎法学)修了
- 東京大学助手、一橋大学専任講師、助教授、教授、法学部長・法学研究科長等を経て、1997年3月一橋大学退官
- 1997年4月～2007年3月まで中央大学教授(うち2007年3月までの3年間中央大学法科大学院教授)
- 現在、一橋大学名誉教授
- 「アクセス権」(東京大学出版会、1977年)、「アクセス権とは何か」(岩波書店、1978年)、「現代のプライバシー」(岩波書店、1980年)、「情報化時代と法(NHK市民大学)」(日本放送出版協会、1983年)、「プライバシーと高度情報化社会」(岩波書店、1988年)、「情報公開・個人情報保護」(編著、有斐閣、1994年)、「自治体情報法」(学陽書房、1994年)、「情報公開・プライバシーの比較法」(編著、日本評論社、1996年)、「メディア判例百選」(長谷部恭男氏との共編著、有斐閣、2005年)、「インターネット社会と法(第2版)」(編著、新世社、2006年)、「地理空間情報の活用とプライバシー保護」(宇賀克也氏との共編著、地域科学研究会、2009年)、「プライバシー・個人情報保護の新課題」(編著、商事法務、2010)等著作多数。

②国の個人情報保護関係法のすべてに関与

- ○1970年前後に情報公開の制度化提唱、“生みの親”との評価
- ○個人情報保護関係では、1970年代前半にはその制度化を提唱、例えば、次のような個人情報保護の制度化等の検討にかかわる。
- 行政管理庁(当時)プライバシー保護研究会「個人データの処理に伴うプライバシー保護対策」(1982年7月)
- 総務省行政機関における個人情報の保護に関する研究会「行政機関における個人情報の保護対策の在り方について」(1986年12月)
- 高度情報通信社会推進本部個人情報保護検討部会「我が国における個人情報保護システムの在り方について(中間報告)」(1999年11月19日)(検討部会座長)
- 行政機関等個人情報保護法制研究会「行政機関等の保有する個人情報の保護に関する法制の充実強化について—電子政府の個人情報保護」(2001年10月26日)
- ○個人情報保護法に基づくガイドライン等策定関与多数(2003年以降)
- 社会保障・税に関わる番号制度に関する個人情報保護WG座長(2011年～)

③東京都・神奈川県等の地方公共団体の 個人情報保護条例制定・運用に関与

- 1970年代後半から多数の地方公共団体の個人情報保護条例等に関与
- 自治省個人情報保護対策研究会報告(1987年10月)(研究会座長)
- 「神奈川県の個人情報保護制度に関する提言」(1989年9月)(個人情報保護推進懇話会副会長)
- 東京都個人情報保護懇談会「東京都の個人情報保護制度のあり方についての提言」(1990年6月)
- 自治省第二次個人情報保護対策研究会報告(1990年7月)
- 東京都個人情報保護委員会委員(1991年～)
- 東京都情報公開・個人情報保護審議会会長(1999年～)
- 神奈川県個人情報保護審議会副会長(1990年～2010年)
- 神奈川県情報公開審査会会長(1997年～、1983年～1997年審査会職務代理)

④民間部門の個人情報保護ガイドライン 策定等に関与(1)

- 経済企画庁国民生活局データ・プライバシー保護研究委員会報告「民間部門におけるプライバシーの保護」(1986年3月)(研究委員会主査)
- (財)金融情報システムセンター「金融機関等における個人データ保護のための取扱指針」(1987年3月)(専門委員会委員長)
- (財)日本情報処理開発協会「民間部門における個人情報保護のためのガイドライン」(1988年3月)(委員会委員長)
- 国民生活審議会消費者政策部会報告「消費者取引における個人情報保護の在り方について」(1988年9月)
- 通商産業省機械情報産業局「情報化対策委員会個人情報保護部会報告」(1989年4月18日)(個人情報保護部会長)
- 郵政省電気通信局「電気通信事業における個人情報保護に関する研究会」報告(1991年8月)(研究会座長)
- 通商産業省機械情報産業局「プライバシー問題検討ワーキンググループ」報告(1996年4月)(ワーキンググループ座長)
- 大蔵省・通産省「個人信用情報保護・利用の在り方に関する懇談会」報告(1998年6月12日)(懇談会座長)

④民間部門の個人情報保護ガイドライン 策定等に関与(2)

- (財)日本情報処理開発協会「個人情報保護に係る環境整備検討委員会」プライバシーマーク制度提言(1998年)(委員会委員長)
- 高度情報通信社会推進本部個人情報保護検討部会「我が国における個人情報保護システムの在り方について(中間報告)」(1999年11月19日)(検討部会座長)
- 労働省「労働者の個人情報保護に関する行動指針」公表(2000年12月20日)(研究会委員)
- クレジット個人情報保護推進協議会会長(2001年～2009年)
- 一般財団法人日本情報経済社会推進協会(JIPDEC)プライバシーマーク制度委員会委員長(1998年～)

⑤ 国際的に活動

- 多数の国際会議等参加・スピーチ
- データ保護・プライバシー・コミッショナー国際会議（2011年第33回、その3分の2以上参加、スピーカー）
- 経済協力開発機構（Organisation for Economic Co-operation and Development, OECD）情報セキュリティ・プライバシー作業部会（Working Party on Information Security and Privacy, WPISP）副議長（1996年～2008年）
- カナダ・オンタリオ州・情報・プライバシー・コミッショナー（Information and Privacy commissioner, Ontario, Canada）のプライバシー・バイ・デザイン大使（Privacy by Design Ambassador）→世界で活躍しているプライバシー・個人情報保護関係の実務家・研究者等が任命されている
- デジタル啓蒙フォーラム（Digital Enlightenment Forum）名誉会員 *

* Digital Enlightenment Forum (1)

- The DIGITAL ENLIGHTENMENT FORUM stimulates and organises debate among representatives of science and technology, law and policy, with a view to providing guidance on the rapid changes in digital technologies and their perceived impact on society and its governance.
- It takes its inspiration from the 18th century Enlightenment period (also Age of Reason) as well as from transformations and evolutions that have taken place since then. It examines digital technologies and their application openly with essential societal values in mind.
- Founded in Luxembourg in 2011, the DIGITAL ENLIGHTENMENT FORUM aims to shed light on today's rapid technological changes and their impact on society and its governance.
- The FORUM stimulates debate and provides guidance.

* Digital Enlightenment Forum (2)

- Honorary Members (名誉会員)
- Sir Tim Berners-Lee – Professor at MIT, United States, Director of W3C and WWW Foundation
- Ann Cavoukian – Information and Privacy Commissioner, Ontario, Canada
- Masao Horibe – Emeritus Professor at Hitotsubashi University, Fellow at Chuo Law School, Tokyo, Japan
- Michael Kirby – The Hon Michael Kirby AC CMG, Australia
- Hamadoun Touré – Secretary-General of the International Telecommunication Union (ITU), Geneva, Switzerland

個人情報保護と情報セキュリティ

	個人情報	法人等情報
個人情報保護関係法令 例：個人情報保護法、行政機関 個人情報保護法、独立行政法 人等個人情報保護法、地方公 共団体の個人情報保護条例、 マイナンバー法案 (OECDプライバシー・ガイドライ ン、EUデータ保護指令)	○	×
情報セキュリティ関係法令 例：刑法改正(1987年、コン ピュータ犯罪処罰規定)、不正 競争防止法(1993年、営業秘 密)、不正アクセス禁止法(1999 年)、刑法改正(2011年、ウイル ス作成罪) (OECD2002年セキュリティ・ガイ ドライン)	○	○

マイナンバー法という名称(1)

- 2012年1月24日に召集された2012年の通常国会は、問題山積の多難な様相を呈している。今国会の最重要法案の一つは、社会保障・税の一体改革に関するもので、その改革を支える基盤となるのが社会保障・税に関わる番号制度である。番号制度については約2年前から議論が本格化し、その途中の昨年、番号制度の名称を公募したところ、約800件の応募があったと聞いている。その中から選ばれたのが、「マイナンバー」という名称である。番号制度を検討してきている「社会保障・税に関わる番号制度に関する実務検討会」は、2011年12月16日の会議で、「社会保障・税番号制度の法律事項に関する概要」をまとめ、番号制度の法律の名称を「マイナンバー法」とすることを決めた。
- **マイナンバー法案**は、正式には、「**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案**」という長い題名になっている。ここでも、適宜、「マイナンバー法」、「マイナンバー法案」と呼ぶことにする。

マイナンバー法という名称(2)

- マイナンバー法案は、関係法律の整備等法案とともに、2月14日に閣議決定され、国会に提出された。マイナンバー法案が成立した場合に、マイナンバーは税の分野でも利用されることになる。その利用に当たって、個人情報をどのように保護するかなどについて見ることにする。
- マイナンバー法案は、番号としては、**個人番号**と**法人番号**の二つを導入する。
- **個人番号**は、プライバシー・個人情報保護との関係で大いに論じられてきている。私は、社会保障・税に関わる番号制度に関する個人情報保護ワーキンググループ(WG)の座長を務めているが、2011年2月から6月にかけて、プライバシー・個人情報保護のあり方について大いに議論した。その成果は、2011年6月30日にまとめられた社会保障・税番号大綱で取り入れられ、今回の法案で条文化された。

マイナンバー法案の目次

第一八〇回

閣第三二号

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案

目次

第一章 総則(第一条—第三条)

第二章 個人番号(第四条—第十三条)

第三章 特定個人情報保護等

第一節 特定個人情報保護(第十四条—第十八条)

第二節 情報提供ネットワークシステムによる特定個人情報の提供(第十九条—第二十三条)

第三節 行政機関個人情報保護法等の特例等(第二十四条—第三十条)

第四章 個人番号情報保護委員会

第一節 組織(第三十一条—第四十四条)

第二節 業務(第四十五条—第五十条)

第三節 雑則(第五十一条)

第五章 法人番号(第五十二条—第五十五条)

第六章 個人番号カード(第五十六条)

第七章 雑則(第五十七条—第六十一条)

第八章 罰則(第六十二条—第七十二条)

附則

マイナンバー法案の概要(1)

第1章 総則(第1条～第3条)

- 目的(第1条)
- ○個人番号及び法人番号を活用した効率的な情報の管理、利用及び迅速な情報の授受
- ○手続の簡素化による国民の負担の軽減
- ○現行個人情報保護法制の特例を定め、個人番号その他の特定個人情報(個人番号を含む個人情報。以下同じ。)の適正な取扱いの確保

- 個人番号及び法人番号の利用の基本(第3条)
- ○行政事務の処理において、個人又は法人その他の団体に関する情報の管理を一層効率化するとともに、当該事務の対象となる者を特定する簡易な手続を設けることによって、行政運営の効率化及び国民の利便性の向上に資すること。
- ○情報提供ネットワークシステムその他これに準ずる仕組みを利用して迅速かつ安全に情報の授受を行い、情報を共有することによって、社会保障制度、税制その他の行政分野における給付と負担の適切な関係の維持に資すること。
- ○個人又は法人その他の団体から提出された情報については、これと同一の内容の情報の提出を求めることを避け、国民の負担の軽減を図ること。
- ○個人番号を用いて収集され、又は整理された個人情報法令に定められた範囲を超えて利用され、又は漏えいすることがないように、その管理の適正を確保すること。

マイナンバー法案の概要(2)

第2章 個人番号(第4条～第13条)

- **指定・通知、番号の生成(第4条、第5条)**
 - ○市町村長は、住民票コードを変換して得られる個人番号を指定し、書面により通知
 - ○市町村長は、個人番号の生成に係る処理を地方公共団体情報システム機構に要求
 - ○個人番号の漏えい等、一定の要件に該当した場合のみ、個人番号は変更可能
 - ○これらの市町村の事務は、法定受託事務とする。
- **再委託、個人番号利用事務実施者等の責務(第7条～第10条)**
 - ○個人番号を利用する事務等の全部又は一部の委託を受けた者は、当該事務の委託をした者の許諾を得た場合に限り、その全部又は一部の再委託が可能
 - ○個人番号を利用する事務等を行う者は、個人番号の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために必要な措置を講じなければならない。
 - ○同一内容の情報が記載された書面の提出を複数の番号関係手続において重ねて求めることがないよう、相互に連携して情報の共有及びその適切な活用に努める。
- **提供の要求、本人確認の措置、提供の求めの制限(第11条～第13条)**
 - ○個人番号を利用する事務等を行う者は、当該事務を処理するために必要があるときは、本人又は他の個人番号を利用する事務等を行う者に対し個人番号の提供、機構に対し個人番号、基本4情報の提供を求めることができる。
 - ○本人から個人番号の提供を受ける場合、個人番号カードの提示を受ける等の本人確認を義務付け
 - ○法定された場合を除き、個人番号の提供を求めることを禁止

マイナンバー法案の概要(3)

- 医療保険等の保険料徴収等の医療保険者における手続、福祉分野の給付、生活保護の実施等低所得者対策の事務等に利用。
- ・児童扶養手当法による児童扶養手当の支給に関する事務
- ・母子及び寡婦福祉法による資金の貸付け、母子家庭自立支援給付金の支給に関する事務
- ・障害者自立支援法による自立支援給付の支給に関する事務
- ・特別児童扶養手当法による特別児童扶養手当等の支給に関する事務
- ・生活保護法による保護の決定、実施に関する事務
- ・介護保険法による保険給付の支給、保険料の徴収に関する事務
- ・健康保険法、船員保険法、国民健康保険法、高齢者の医療の確保に関する法律による保険給付の支給、保険料の徴収に関する事務
- ・独立行政法人日本学生支援機構法による学資の貸与に関する事務
- ・公営住宅法による公営住宅、改良住宅の管理に関する事務等
- 国民が税務当局に提出する確定申告書、届出書、調書等に記載。当局の内部事務等に利用。
- 被災者生活再建支援金の支給に関する事務その他地方公共団体の条例で定める事務等に利用。

マイナンバー法案の概要(4)

別表第一

- 利用範囲(第6条)
- ○雇用保険等の資格取得・確認、給付を受ける際に利用。ハローワーク等の事務等に利用。
- ・雇用保険法による失業等給付の支給、雇用安定事業、能力開発事業の実施に関する事務
- ・労働者災害補償保険法による保険給付の支給、社会復帰促進等事業の実施に関する事務等
- ○年金の資格取得・確認、給付を受ける際に利用。
- ・国民年金法、厚生年金保険法による年金である給付の支給に関する事務
- ・国家公務員共済組合法、地方公務員等共済組合法、私立学校教職員共済法による年金である給付の支給に関する事務
- ・確定給付企業年金法、確定拠出年金法による給付の支給に関する事務
- ・独立行政法人農業者年金基金法による農業者年金事業の給付の支給に関する事務等

マイナンバー法案の概要(5)

第3章 特定個人情報の保護等(第14条～第30条)

- **特定個人情報ファイルの作成の制限、特定個人情報保護評価等(第14条～第18条)**
- ○個人番号情報保護委員会は、特定個人情報を適切に管理するために講ずべき措置を定めた指針を作成・公表
- ○行政機関の長等は、特定個人情報の漏えいその他の事態の発生の危険性及び影響に関する評価(以下「特定個人情報保護評価」という。)を実施
- ○マイナンバー法の規定によるものを除き、特定個人情報の収集・保管、特定個人情報ファイルの作成を禁止
- ○情報提供ネットワークシステムを使用して行う場合などを除き、特定個人情報の提供を禁止

- **情報提供ネットワークシステムによる特定個人情報の提供(第19条～第23条)**
- ○情報提供ネットワークシステムを使用して特定個人情報の提供を求められた場合、当該特定個人情報の提供義務あり
- ○情報提供の記録は情報提供ネットワークシステムに保存
- ○情報提供ネットワークシステムの運営に関する事務に従事する者には秘密保持義務あり

- **個人情報保護法等の特例(第24条～第30条)**
- ○情報提供ネットワークシステム上の情報提供の記録について、マイ・ポータル又はその他の方法により開示
- ○任意代理人による特定個人情報の開示請求等が可能
- ○本人同意があっても特定個人情報の第三者への目的外提供は原則禁止
- ○地方公共団体等は、特定個人情報の適正な取扱いの確認のための必要な措置を講ずる。

マイナンバー法案の概要(6)

第4章 個人番号情報保護委員会(第31条～第51条)

- **設置、所掌事務(第31条～第34条)**
- ○内閣府設置法第49条第3項の規定に基づく、いわゆる三条委員会として設置
- ○所掌事務
 - 特定個人情報の取扱いに関する監視又は監督
 - 特定個人情報保護評価に関することなど
- **組織、任期等(第35条～第51条)**
- ○組織・任期等
 - 委員長及び6人の委員をもって組織。任期は5年。(委員のうち3人は、非常勤)
 - 委員長及び委員は、両議院の同意を得て、内閣総理大臣が任命
 - 委員は、個人情報の保護に関する学識経験者、情報処理技術に関する学識経験者、社会保障制度や税制に関する学識経験者、民間企業の実務経験を有する者、地方公共団体の全国的連合組織の推薦する者等で構成
 - 委員長、委員、職員等の守秘義務、給与、政治運動等の禁止等を規定
- ○業務
 - 委員会は指導、助言、勧告、命令、報告及び立入検査の実施権限、委員会規則の制定権あり
 - 委員会は内閣総理大臣に対し、特定個人情報の保護に関する施策の改善についての意見を述べるができる
 - 委員会は毎年国会に処理状況を報告し、公表

マイナンバー法案の概要(7)

- 第5章 法人番号(第52条～第55条)

- ○国税庁長官は法人番号を指定、通知。法人等の名称、所在地等と併せて法人番号を公表。ただし、人格のない社団等の所在地等の公表は予め同意のあるものに限る。
- ○国税庁長官は法人番号の指定を行うために、法務大臣に商業登記法による会社法人等番号その他の登記簿に記録された事項の提供を求めることができる。
- ○行政機関の長等は、特定法人情報の授受の際、法人番号を通知して行う。
- ○法人番号については、利用範囲の制限等がなく、民間でも自由に利用できる。

マイナンバー法案の概要(8)

第6章 個人番号カード(第56条)

- ○市町村長は、申請により、個人番号カード(氏名、住所、生年月日、個人番号、顔写真等を記載)を交付しなければならない。
- ○カード記載事項に変更があったときは、その変更があった日から14日以内に、その旨をその者が記録されている住民基本台帳を備える市町村の長に届け出るとともに、当該個人番号カードを提出しなければならない。
- ○個人番号カードの交付を受けている者は、個人番号カードを紛失したときは、直ちに、その旨を住所地市町村長に届け出なければならない。
- ○上記の市町村の事務は、法定受託事務とする。
- ○市町村の機関は、条例で定めるところにより、個人番号カードを利用することができる。
- できる。

マイナンバー法案の概要(9)

第8章 罰則(第62条～第72条)

- **個人番号を利用する者に関する罰則(第62条～第64条、第66条)**
- ○正当な理由なく、特定個人情報ファイルを提供(個人番号利用事務等に従事する者等)
⇒4年以下の懲役若しくは200万円以下の罰金又は併科
- ○不正な利益を図る目的で、個人番号を提供又は盗用(個人番号利用事務等に従事する者等)
⇒3年以下の懲役若しくは150万円以下の罰金又は併科
- ○情報提供ネットワークシステムに関する秘密の漏えい又は盗用(情報提供ネットワークシステムの事務に従事する者)
⇒3年以下の懲役若しくは150万円以下の罰金又は併科
- ○特定個人情報記録された文書等を収集(国の機関等の職員)
⇒2年以下の懲役又は100万円以下の罰金

- **個人番号等を不正に取得する行為等に対する罰則(第65条、第70条)**
- ○人を欺き、人に暴行を加え、人を脅迫し、又は、財物の窃取、施設への侵入等により個人番号を取得
⇒3年以下の懲役又は150万円以下の罰金
- ○偽りその他不正の手段により個人番号カードの交付を受ける行為
⇒6月以下の懲役又は50万円以下の罰金

マイナンバー法案の概要(10)

- 個人番号情報保護委員会に関する罰則(第67条～第69条)
- ○職務上知り得た秘密を漏えい又は盗用(委員会の委員など)
 - ⇒2年以下の懲役又は100万円以下の罰金
- ○委員会の命令に違反(委員会から命令を受けた者)
 - ⇒2年以下の懲役又は50万円以下の罰金
- ○委員会による検査等の際し、虚偽の報告、虚偽の資料提出をする、検査拒否等(委員会による検査の対象者)
 - ⇒1年以下の懲役又は50万円以下の罰金
- ※上記については、必要に応じて国外犯処罰規定、両罰規定を設けている。

EUデータ保護指令による日本の評価(1)

- 日本は、個人の私生活にかかわる個人データ及び基本権に関して十分なレベルの保護を提供している国であるとは、EUによって未だ考えられていない。(Japan has not yet been considered by the EU as a country providing an adequate level of protection with respect to the protection of personal data and fundamental rights of the persons relating to their private life.)
- したがって、EU構成国から日本へのデータの移転は、EU構成国各国のデータ保護機関による事前の情報／権限付与 (prior information/authorization) を意味する指令95/46/EC第26条に従って行われなければならない。(2009年4月23日、ブルッセルで開催の「EUと日本におけるプライバシー・個人情報保護」(Privacy and Personal Data Protection between EU and Japan) 会議での欧州委員会データ保護担当官のプレゼンテーションによる。)

EUデータ保護指令による日本の評価(2)

- 日本は、OECD(経済協力開発機構)の加盟国(1964年加盟承認)であることもあり、そのプライバシー・ガイドライン(1980年)に準拠して、個人情報保護法制の整備を図ってきた。このガイドラインがなかったならば、日本の個人情報保護の整備は進まなかったであろう。
- しかし、今や、OECDプライバシー・ガイドライン(1980年)準拠のみでは、EUデータ保護指令の「十分性」基準を満たさない。
- 「十分性」が認められない場合、日本は、国際的恥辱を受けることになる。
- 日本におけるプライバシー・個人情報保護に関する最大の問題点の一つは、そのような認識すらほとんどないことである。

OECDプライバシー・ガイドライン(1980年)

- 経済協力開発機構 (Organisation for Economic Co-operation and Development, OECD)「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」(Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data) (1980年9月23日採択)
- プライバシー保護の8原則 : ①収集制限の原則(Collection Limitation Principle)、②データ内容の原則(Data Quality Principle)、③目的明確化の原則(Purpose Specification Principle)、④利用制限の原則(Use Limitation Principle)、⑤安全保護の原則(Security Safeguards Principle)、⑥公開の原則(Openness Principle)、⑦個人参加の原則(Individual Participation Principle)、⑧責任の原則(Accountability Principle)
- OECDの概要
 - 1960年 OECD条約
 - 1961年 設立(当初、20カ国で構成)
 - 1964年 日本の加盟承認
 - 2012年5月現在 加盟34カ国

EUデータ保護指令(1995年)

- 1990年 EC個人データ指令提案採択
- 1995年10月24日 欧州連合(European Union, EU)の「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」(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)採択→EUデータ保護指令
- 【2012年1月25日 欧州連合、個人データの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欧州議会及び理事会の規則(一般データ保護規則)の提案 (Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)→EU一般データ保護規則提案】

EUデータ保護指令第25条「十分性」(1)

- 第25条 諸原則(Principles)
- その第1項は、次のようになっている。
- 「構成国は、取扱い過程にある個人データ又は移転後取り扱うことを目的とする個人データの第三国への移転は、この指令の他の規定に従って採択されたその国の規定の遵守を損なうことなく、**当該第三国が十分なレベルの保護(adequate level of protection)を確保している場合に限って行うことができる**ということの規定しなければならない。」
- この十分性の評価がどのようになされるかについては、第25条第2項に規定されている。その第25条第2項は、次のようになっている。
- 「第三国によって保障される保護レベルの十分性は、一つのデータ移転の運用又は一連のデータ移転の運用に関するあらゆる状況にかんがみ評価されなければならない。特に、データの性格、予定されている取扱いの運用の目的及び期間、発出国及び最終目的国、当該第三国において有効である一般的及び分野別の法規範(the rules of law, both general and sectoral, in force in the third country in question)、並びに当該国において遵守されている専門的規範(professional rules)及び安全保護対策措置(security measures)が考慮されなければならない。」

EUデータ保護指令第25条「十分性」(2)

- 第25条の第3項以下の規定は、次のようになっている。
- 「3. 構成国及び委員会は、第三国が第2項の規定の意味における十分なレベルの保護を保障していないと考えられる事例について、相互に情報提供しなければならない。
- 4. 構成国は、第31条第2項に規定する手続に基づいて委員会が、第三国が本条第2項の規定の意味における十分なレベルの保護を保障していないと認定した場合には、当該第三国への同一タイプのデータの移転を阻止するために必要な措置を講じなければならない。
- 5. 委員会は、適切な時期に、第4項に基づく認定によってもたらされる状況を改善することを目的とする交渉を開始しなければならない。
- 6. 委員会は、第31条第2項に規定する手続に基づいて、第三国が私生活、個人の基本的な自由及び権利を保護するための当該第三国の国内法、又は特に本条第5項に規定された交渉の結果に基づいて締結した国際公約を理由として、第2項の規定の意味における十分なレベルの保護を保障していると認定することができる。
- 構成国は、委員会の決定を遵守するために必要な措置を講じなければならない。」]

EUデータ保護指令第26条「例外」(1)

- 第26条 例外(Derogations)
- 第25条につづく「第26条 例外」は、次のように規定している。
- 「1. 構成国は、第25条の適用を制約するものとして、及び特別な場合を規律する国内法に別段の定めがある場合を除いて、第25条第2項の規定の意味における十分なレベルの保護を保障しない第三国に対する個人データの移転又は一連の移転は、次の条件を満たした場合に行うことができることを定めなければならない。
- (a) データ主体が、予定されている移転に対して明確な同意を与えている場合、又は、
- (b) 移転が、データ主体及び管理者間の契約の履行のために、又はデータ主体の請求により、契約締結前の措置の実施のために必要である場合、又は、
- (c) 移転が、データ主体の利益のために、データ主体及び第三者間で結ばれる契約の締結又は履行のために必要である場合、又は、
- (d) 移転が、重要な公共の利益を根拠として、又は法的請求の確定、行使若しくは防御のために必要である場合、又は法的に要求される場合、又は、
- (e) 移転が、データ主体の重大な利益を保護するために必要である場合、又は、
- (f) 法律又は規則に基づいて情報を一般に提供し、及び公衆一般又は正当な利益を証明する者のいずれかによる閲覧のために公開されている記録から、閲覧に関する法律に規定された条件が特定の事例において満たされる範囲内で、移転が行われる場合。

EUデータ保護指令第26条「例外」(2)

- 2. 構成国は、第1項の規定に実体的な効果を持つことなく、管理者が個人のプライバシー並びに基本的な権利及び自由の保護、並びにこれらに相当する権利の行使に関して、十分な保護措置を提示する場合には、第25条第2項の規定の意味における十分なレベルの保護を保障しない第三国への個人データの移転又は一連の移転を認めることができる。当該保護措置は、特に適切な契約条項から帰結することができる。
- 3. 構成国は、第2項によって付与された許可を、委員会及び他の構成国に通知しなければならない。
- 一つの構成国又は委員会が、個人のプライバシー並びに基本的な権利及び自由の保護を含む正当な理由に基づいて異議申立てを行った場合には、委員会は、第31条第2項に規定された手続に基づいて適切な措置を講じなければならない。
- 構成国は、委員会の決定を遵守するために必要な措置を講じなければならない。
- 4. 構成国は、第31条第2項に規定された手続に従って、一定の標準契約条項が本条第2項によって要求される十分な保護措置を提供していると決定する場合には、委員会の決定を遵守するために必要な措置を講じなければならない。」

EUデータ保護指令と独立監督機関(1)

EUデータ保護指令の監督機関

EUデータ保護指令は、「第VI章 監督機関及び個人データの取扱いに係る個人の保護に関する作業部会」において、「第28条 監督機関」、「第29条 個人データの取扱いに係る個人の保護に関する作業部会」及び「第30条 【作業部会の所掌事項】」について規定している。そのうち、監督機関に関する第28条は、次のようになっている。

1. 各構成国は、一つ又は二つ以上の公的機関が、この指令に従って構成国が採択した規定の範囲内で、その適用を監視する責任を負うことを定めなければならない。

この機関は、委任された職権を遂行する上で、完全に独立して(with complete independence)活動しなければならない。

EUデータ保護指令と独立監督機関(2)

2. 各構成国は、個人データの取扱いに係る個人の権利及び自由の保護に関する行政措置又は規則を制定する際に、監督機関に諮ることを定めなければならない。
3. 各監督機関は、特に次の権限を与えられなければならない。
 - 取扱い作業の対象を構成するデータにアクセスする権限、及び監督職務の遂行に必要なすべての情報を収集する権限等の調査権限
 - 例えば、第20条の規定に従って取扱い作業の実施前に意見を述べ、及びこの意見の適切な公開を保障する権限、データのブロック、消去又は破壊を命じる権限、取扱いの一時的又は確定的な禁止を課す権限、管理者を警告又は懲戒する権限、中央議会又はその他の政治機関に問題点を照会する権限等の仲裁権限
 - この指令に従って採択された国内規定への違反があった場合に法的手続を開始する権限、又はこの違反を司法機関に通知する権限
 - 監督機関の決定に不服がある場合は、裁判所に対して訴訟を提起することができる。

EUデータ保護指令と独立監督機関(3)

4. 各監督機関は、個人データの取扱いに係る個人の権利及び自由の保護に関して、すべての者及びそれを代表する協会からなされる主張を聴取しなければならない。このような者は、主張の結果についての情報を提供されなければならない。
5. 各監督機関は、定期的に活動報告書を作成しなければならない。この報告書は、公開されなければならない。
6. 各監督機関は、当該取扱いに関してどの国の国内法が適用され得るかにかかわらず、当該構成国の領域内においては、本条第3項の規定に従って付与された権限を行使する資格を有する。各監督機関は、他の構成国からこの権限を行使することを要請される場合がある。

監督機関は、特にすべての有益な情報を交換する等、職務の遂行に必要な範囲内で、相互に協力しなければならない。
7. 構成国は、監督機関の構成員及び職員が、退職後であっても、アクセスした機密情報に関して職業上の守秘義務を負うことを定めなければならない。

欧州委員会の「十分性」認定の国・地域

- 欧州委員会が「十分性」を認定したのは、スイス、カナダ、アルゼンチン、アメリカ合衆国セーフ・ハーバー・スキーム、ガーンジー、マン島、ジャージー、フェロー島、アンドラ、イスラエル、ウルガアイ、ニュージーランドである。
- 日本は、欧州委員会によって「十分性」の認定を受けていない。

データ保護・プライバシー・コミッショナー 国際会議の「仲間はずれ」(1)

- 国民生活審議会「個人情報保護に関する取りまとめ(意見)」(2007年6月29日)
- VIII 第三者機関の意義
- (1) 現状
- ア 個人情報保護法において、第4章の個人情報取扱事業者の義務は、事業の用に供している個人情報の対象とされていることから、各事業等を所管する大臣が、主務大臣として、当該事業における個人情報の適正な取扱いについて、行政責任と権限を有するものとされている。
- イ 平成19年5月31日現在、事業等を所管する各省庁により、22分野について35のガイドラインが策定され、主務大臣制の下、事業者等に対する指導・監督が実施されてきている。
- ウ 平成19年5月31日現在、個人情報保護法第37条の規定に基づき、主務大臣が認定個人情報保護団体として認定した団体は、計34団体である。
- (2) 課題
- 諸外国には、中立的な第三者機関が個人情報保護法を執行している例も多い。

データ保護・プライバシー・コミッショナー 国際会議の「仲間はずれ」(2)

- (参考)国際的には、第三者機関として、次の要件を充足することを求める例がある注。自主性・独立性や、適切な範囲の機能及びその実施の法的な権限による担保の観点から、我が国の機関がこの要件を充足することは困難であると考えられる。
- ① 適切な法的根拠に基づいて設置された公的機関であること。
- ② 所掌事務の遂行のために適切な水準の自主性・独立性が保証されていること。
- 自主性については、第三者機関が、法的・実務的に、第三者の許可を得ずに適切な措置を講じる権限を付与されていることが求められる。独立性については、第三者機関が政治的・行政的干渉を受けずに活動し、既得権益の影響に耐えることができるために重要である。

データ保護・プライバシー・コミッショナー 国際会議の「仲間はずれ」(3)

- ③ 所掌事務を定めている法律が、データ保護やプライバシーに関する国際的な枠組みに準拠していること。
- ④ 適切な範囲の機能を有しており、その実施が法的な権限により担保されていること。
- データ保護の第三者機関は、法令順守、監督、調査、救済、指導及び公教育等の分野について、一連の機能を有する。第三者機関は、助言的な機能を有するだけでなく、法的・行政的な結果を伴う監督権限を有さなければならない。
- 注：「資格に関する委員会の基準及び規則並びに認定の原則」(2001年9月25日データ保護コミッショナー国際会議採択(2002年9月9日データ保護プライバシーコミッショナー国際会議改定))による。

資格に関する委員会の基準及び規則 並びに認定の原則

- 堀部政男による注

CRITERIA AND RULES FOR CREDENTIALS COMMITTEE AND THE
ACCREDITATION PRINCIPLES

Adopted on 25 September 2001 during the 23rd International Conference of Data Protection Commissioners held in Paris, 24-26 September 2001 and as amended on 9 September 2002 during the 24th International Conference of Data Protection and Privacy Commissioners held in Cardiff 9-11 September 2002

マイナンバー法案の個人番号情報保護委員会

第4章 個人番号情報保護委員会(第31条～第51条)

◆設置、所掌事務(第31条～第34条)

○内閣府設置法第49条第3項の規定に基づく、いわゆる三条委員会として設置

○所掌事務

- ・特定個人情報の取扱いに関する監視又は監督
- ・特定個人情報保護評価に関することなど

◆組織、任期等(第35条～第51条)

○組織・任期等

- ・委員長及び6人の委員をもって組織。任期は5年。(委員のうち3人は、非常勤)
- ・委員長及び委員は、両議院の同意を得て、内閣総理大臣が任命
- ・委員は、個人情報の保護に関する学識経験者、情報処理技術に関する学識経験者、社会保障制度や税制に関する学識経験者、民間企業の実務経験を有する者、地方公共団体の全国的連合組織の推薦する者等で構成
- ・委員長、委員、職員等の守秘義務、給与、政治運動等の禁止等を規定

○業務

- ・委員会は指導、助言、勧告、命令、報告及び立入検査の実施権限、委員会規則の制定権あり
- ・委員会は内閣総理大臣に対し、特定個人情報の保護に関する施策の改善についての意見を述べるができる
- ・委員会は毎年国会に処理状況を報告し、公表

毎日新聞1996年3月29日朝刊「住民番号」の導入 独立の監視機関を」①

- 「日本は「人権」後進国といわれる。国際会議などで「高度に情報化が進んでいる日本が、プライバシー保護になぜ目が向かないのか不思議だ」とよくいわれるが、諸外国の指摘を待つまでもなくプライバシー問題は今のうちに手を打っておかないと将来取り返しがつかない問題になることは間違いない。
- その点でいうと、今回提出された最終報告書は昨年三月の中間報告に比べ、①全国的な統一番号を付けない②民間への利用禁止③全国センターを連絡調整役にする④カード発行は本人申請による⑤審議組織の設置—などプライバシー保護にキメ細かく配慮した内容になっており、研究会の苦労の跡がうかがえる。
- だが、気になったのは、システムを監視していく機関を明確に打ち出していないこと。「審議機関の設置」とあっさり述べているが、プライバシーを真剣に保護していくには個人情報取り扱いを監視する独立機関が必要である。欧州では監督する専門スタッフのいる監督機関を設けることが常識になっている。

毎日新聞1996年3月29日朝刊「住民番号」の導入 独立の監視機関を」②

- ただこうした組織の設置は自治省のみが扱える問題ではない。ほかにも納税者番号や社会保険庁の年金番号制度など政府部内でいくつかの番号制度が検討されている状況を踏まえ、政府が一体になって取り組む時期にきたのではないか。役所の縄張り争いで実際はとても難しいという人もいるが、役所が限界なら政治家がリーダーシップを取ってやっていくべき課題だ。
- 心配された民間利用は禁止されたが、実際にはどう担保されるのか。法案要綱などを見ないと手放しては評価できない。信用情報機関、銀行、保険会社など民間事業者は顧客管理のため統一番号を求めており、あいまいなままスタートするとプライバシーが侵害される危険性があることを忘れてはならない。
- 報告書の案を導入するまでにはもう少し国民的議論が必要な気がする。自分の情報の流れを自ら決定できる「自己情報コントロール権」を能動的な権利として国民の共通認識として確立するとともに、自治体職員のプライバシー意識を高めなければならない。(談)」
-

「情報保護に監視機関を」(朝日新聞 1998年2月26日朝刊)

- 朝日新聞1998年2月26日朝刊は、「番号制、全体見すえ議論を 自治省が「住民票」法案提出方針」、「住民のメリットどこまで」、「税へ適用、厚生省と確執」の見出しで、住民基本台帳法の改正構想について報道し、その最後に堀部政男のコメントを含め、個人情報保護について問題点を指摘し、堀部のコメントから「情報保護に監視機関を」という見出しを掲げている。
- そのコメントの部分は、次のようになっている。
- 「堀部政男・中央大教授(情報法)は、自治省案の保護強化策を評価しつつも「情報漏れがあったり、目的外の使用があったりした場合は、行政側に意見を述べられる権限を明確にするなど、委員会や審議会をきちんとした監視機関とすべきだ」と注文している。」

共通番号制の導入計画と課題の指摘①

- 2010年2月初旬、朝日新聞記者から、共通番号制に関する政府の構想について、電話による取材ではなく、直接に会って意見を聞きたいという連絡があった。
- 日本におけるプライバシー論議、国民総背番号制の議論など、これまでに行われてきた議論について説明するとともに、政府の新たな構想については、プライバシー・個人情報保護の観点から、特に第三者機関設置の必要性を強調した。
- 朝日新聞2010年2月9日朝刊は、「納税者番号 格差是正狙い」という横見出し及び「閣僚検討会始動 5月までに複数案」という縦見出しとともに、「個人情報の保護論点」という縦見出しを掲げて、「税金と社会保障の個人情報を一つにまとめる『共通番号制』の検討が8日始まった」ことを報じた。その最後に私のコメントを次のように載せていた。

共通番号制の導入計画と課題の指摘②

- 「個人情報保護に詳しい堀部政男・一橋大学名誉教授(情報法)は『番号を使う範囲を明確化したうえで、目的外の使用を法律で禁じたり、不正利用を監視・規制する**第三者機関**を設置したりすることが必要だ』と話している。」
- この記事の前日の2月8日に、社会保障・税に関わる番号制度に関する検討会の第1回会合が開かれた。その配布資料4の「社会保障・税に関わる番号制度の目的・課題」の中の「検討に当たっての課題(案)」では、「利用する分野・番号などの特定」「個人情報保護する仕組みの構築」「その他」の3つが掲げられ、「一年以内を目処に結論」となっていた。
- ここには個人情報保護の具体的方策は示されていなかった。
- しかし、その後の検討会における議論では、個人情報保護のあり方に言及するものが出てきている。

「国境越える個人情報 守れ」①

(朝日新聞2012年4月1日朝刊)

- 朝日新聞2012年4月1日朝刊、平和博編集委員
- 見出し「国境越える個人情報 守れ」、「欧米で規制案 ネット進化に対応」、「『日本、世界で孤立』の懸念」
- 記事の一部 「EUが動けば米国も即座に呼応し、交渉しながらリーダーシップを強調する。言わばプライバシー外交だ。」 堀部政男・一橋大学名誉教授(情報法)はそう話す。
 グーグルが3月から、60以上のサービスの「プライバシーポリシー」(個人情報保護方針)を一本化し、各国の懸念を呼んだように、ネットの個人情報保護の問題は急速にグローバル化している。
 EUなどでは個人情報保護を担う独立監視機関がこうした

「国境越える個人情報 守れ」②

(朝日新聞2012年4月1日朝刊)

問題に対応してきた。

だが日本では「今のところ欧米のような議論をする政府機関もない」と堀部さん。

ようやく初の個人情報保護に関する独立監視機関「個人番号情報保護委員会」の創設が、政府の番号制度(マイナンバー)法案に盛り込まれたが、その範囲は税と社会保障の分野に限定される。「監視機関の設置はあくまで第一歩。日本でも早く議論を始めないとますます取り残される」と堀部さんは指摘する。

⇒朝日新聞2012年4月23日社説「個人情報保護 国境を超えた連携へ」のまとめ「言論・報道の自由などとの両立を図りながら、欧米並みの保護機関へとどう拡充していくのか、議論を深める時だ。」

独立監督機関の先輩たち

- プライバシー・個人情報保護における第三者機関（独立監視機関）は、ヨーロッパ諸国、カナダ、オーストラリア、ニュージーランドなどでは、早くから設置されてきた。アメリカの連邦取引委員会（Federal Trade Commission, FTC）もその中でプライバシー・個人情報保護を所管しており、独立監視機関であるにとらえることができる。
- 日本は、個人情報保護の独立監督機関を欠いているため、この分野では世界的に「仲間はずれ」の状況にある。残念ながら、そのような認識すらない。

独立監督機関の具体例

- アメリカ合衆国—連邦取引委員会 (Federal Trade Commission)、5人の委員、適用法令: 連邦取引委員会法 (Federal Trade Commission Act, FTC法5条 (不公正又は欺瞞的な行為又は慣行の禁止)、金融サービス現代化法 (Gramm-Leach Bliley Act)、公正信用報告法 (Fair Credit Reporting Act, FCRA)、児童オンラインプライバシー保護法 (Children Online Privacy Protection Act, COPPA)、スタッフ約40数人
- カナダ連邦—プライバシー・コミッショナー (Privacy Commissioner)、現在のコミッショナーは、Ms. Jennifer Stoddart、弁護士、スタッフ約86人 (2006年OECD調査)
- イギリス—情報コミッショナー (Information Commissioner)、現在の情報コミッショナーは、Mr. Christopher Graham で、BBC radio and TV journalist を皮切りに、Director General of the Advertising Standards Authority, Chairman of the European Advertising Standards Alliance, Secretary of the BBC を務めた。スタッフ約337人
- ドイツ—連邦データ保護・情報自由監察官 (Der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI))、初代のコミッショナー (1977-1983) は、Prof. Dr. iur. Hans Peter Bull, Universität Hamburg、スタッフ約90人 (2011/2)
- フランス—情報処理及び自由に関する国家委員会 (Commission nationale de l'informatique et des libertés (CNIL))、4代目の委員長 (1984-1999) Jacques Fauvet は、Le Monde の編集局長と聞いている。スタッフ約130人

先輩の一例としての英・情報コミッショナー

- イギリスの情報コミッショナー (Information Commissioner)
- その事務局は、Information Commissioner's Office (ICO)、Manchester郊外のWilmslow
- 1984年データ保護法 (Data Protection Act 1984) で女王陛下任命のデータ保護登録官 (Data Protection Registrar) として発足
- 現行法は、1998年データ保護法 (Data Protection Act 1998) で、2000年情報自由法 (Freedom of Information Act 2000) も所管
- 2011年4月 朝から夕刻まで、全体像を把握するために、Commissioner Christopher Graham, Deputy Commissioner David Smith及び各部門の責任者等からヒアリングを行った

Agenda for your day at the ICO:

- 09:30-10:00 - Welcome and ICO introduction, David Smith
- 10:00-11:00 - Strategic Liaison, David J Evans
- 11:00-12:00 - Complaints Resolution, Andy Laing
- 12:00-13:00 - Policy Delivery, Steve Wood
- 13:00-14:00 - Lunch
- 14:00-15:00 – HR, Bernadette McKnight
- 15:00-16:00 - Good Practice, Victoria Heath
- 16:00-17:00 – Enforcement, Sally-Anne Poole

ICO Key facts (1)

- 総員数 (Total staff headcount) 344 (うち、全時間就業者 (Full-time equivalent) 319)
- 2009-2010年度情報コミッショナー事務局予算 (ICO budget for 2009/10) 1ポンド150円として、約30億円 (c £20,172,000)
- 通知手数料 (Notifications fee income) 約20億円 (c £13,102,000)
- 通知する組織の数 (Number of organisations who notify with us) 約334,000 (c 334,000)
- ICOウェブサイトの閲覧数 (Visits to the ICO website) 約 2,293,800 (c 2,293,800)
- ICOの相談窓口への連絡 (Calls to the ICO's helplines) 212,134
- データ保護権の公衆の認識率 (Public awareness of data protection rights) 96%
- 情報自由権の公衆の認識率 (Public awareness of freedom of information rights) 85%

ICO Key facts (2)

データ保護 (Data protection)

- 受理件数 (Cases received) 33,234
- 終結件数 (Cases closed) 32,714
- 30日以内に終結した件数 (Cases closed in 30 days or less) 14,267 (43%)
- 訴追 (Prosecutions) 9
- 執行通知 (Enforcement notices) 15

情報自由 (Freedom of information)

- 受理件数 (Cases received) 3,734
- 終結件数 (Cases closed) 4,196
- 30日以内に終結した件数 (Cases closed in 30 days or less) 1,887
- 規制・執行措置 (Regulatory and enforcement actions) 3

ICO Key facts (3)

- データ保護の数字は、プライバシー・電子通信[規則]に基づく件数、また、情報自由の数字は、環境情報規則に基づく件数を含む (data protection figures include cases under privacy and electronic communications; freedom of information figures include cases under environmental information regulations.)。
- ほとんどの数字は、2009/10年の会計年度のものである (most figures are based on the 2009/10 financial year.)。

プライバシー・個人情報保護論議の注目概念

- プライバシー・バイ・デザイン (Privacy by Design, PbD)

PbDという言葉は、1990年代中葉から後半にかけて、カナダで開かれたプライバシー関係の国際会議の際などに、現在、オンタリオ州情報・プライバシーコミッショナーであるアン・カブキアン博士 (Dr. Ann Cavoukian) が使っているのを聞いたことがあった。また、アンが、PETs (privacy- enhancing technologies) [プライバシー強化技術] という概念をよく口にしていたのを記憶している。

- 忘れられる権利 (right to be forgotten)

2010年11月4日に公表された、EUデータ保護指令の見直し文書で使われているが、フランスでもその前に使われたり、関係者からも重要な概念になると聞いていた。

- 追跡拒否 (Do not track)

2010年12月にアメリカの連邦取引委員会スタッフ・レポートなどで使われている。

オンタリオ州情報・プライバシー・ コミッショナーのアン・カブキアン博士

- Dr. Ann Cavoukian
- トロント大学でPh.D.取得、刑事学と法を専攻
- 1980年代初頭 オンタリオ州司法省に勤務
- 1987年 情報・プライバシー・コミッショナー事務局に勤務、初代のコンプライアンス部長
- 1990年 副コミッショナーに任命
- 1997年 コミッショナーに任命、その後再任され、任期は2009年まで
- 2014年まで再任、3期務める最初のコミッショナー

プライバシー・バイ・デザインの7基本原則の要旨

プライバシー・バイ・デザインの7基本原則 (7 Foundational Principles) の要旨

1. 事後的ではなく、事前的; 救済的策でなく予防的
2. 初期設定としてのプライバシー
3. デザインに組み込まれるプライバシー
4. 全機能的 — ゼロサムではなく、ポジティブサム
5. 最初から最後まで — すべてのライフサイクルを保護
6. 可視性と透明性 — 公開の維持
7. 利用者のプライバシーの尊重 — 利用者中心主義を維持する

プライバシー・バイ・デザインの7基本原則(1)

- 7つの基本原則
- 1. 事後的ではなく、事前的; 救済的策でなく予防的
- プライバシー・バイ・デザイン(PbD)のアプローチは、受け身で対応するというより、むしろ先見的に対応することが特徴である。プライバシー侵害が発生する前に、それを予想し予防することである。PbDは、プライバシーの脅威が具体的に起きるのを待つものではなく、また、一旦それらが起こった場合に、プライバシー侵害を解決するための救済策を提供するものでもない。— それらの発生を防ぐことを目的としている。要するに、プライバシー・バイ・デザインは、事後ではなく、事前に作用する。
- 2. 初期設定としてのプライバシー
- われわれは、一つのことについて確信し得ている — 標準ルールである！ プライバシー・バイ・デザインは、所定のITシステムまたはビジネス・プラクティスにおいて、個人データが自動的に保護されることを確保することによって、最大級のプライバシー保護を提供することを目指している。個人が何もしなくても、彼らのプライバシーはそのまま保護される。彼らのプライバシーを保護するために、個別の措置は不要である。— それは、システムに最初から組み込まれているものである。

プライバシー・バイ・デザインの7基本原則(2)

- 3. デザインに組み込まれるプライバシー
- プライバシー・バイ・デザインは、ITシステムおよびビジネス・プラクティスのデザインおよび構造に組み込まれるものである。事後的に、付加機能として追加するものではない。これによって、プライバシーが、提供される中心的な機能の重要な構成要素になる。プライバシーは、機能を損なうことなく、システムに不可欠なものである。
- 4. 全機能的 – ゼロサムではなく、ポジティブサム
- プライバシー・バイ・デザインは、不要なトレードオフの関係を作ってしまう時代遅れのゼロサムアプローチではなく、ポジティブサムの「ウインーウイン」の方法で、すべての正当な利益および目標を収めることを目指している。プライバシー・バイ・デザインは、プライバシーとセキュリティの両方とも持つことが可能であることを実証し、プライバシー対セキュリティのような誤った二分法を回避する。

プライバシー・バイ・デザインの7基本原則(3)

- 5. 最初から最後までセキュリティ — すべてのライフサイクルを保護
- プライバシー・バイ・デザインは、情報の最初の構成部分が収集されるより前にシステムに組み込まれことから、関係するデータのライフサイクル全体を通じて安全に拡張する。— 強力なセキュリティ対策は、最初から最後まで、プライバシーに不可欠である。このことは、時期を逃さず、すべてのデータが安全に保持され、プロセスの終了時には確実に破棄されることを確保している。このように、プライバシー・バイ・デザインは、情報の安全なライフサイクル管理を、揺りかごから墓場まで、終始、全ライフサイクルにわたって確保している。
- 6. 可視性と透明性 — 公開の維持
- プライバシー・バイ・デザインは、どのようなビジネス・プラクティスまたは技術が関係しようとも、立の検証を受けることを条件に、決まった手続および目的に従って、実際には機能することをすべての関係者に保証することを目指している。その構成部分および機能は、利用者および提供者に一樣に、可視的で透明でありつづける。記憶し、信頼するが、検証すべきである。
- 7. 利用者のプライバシーの尊重 — 利用者中心主義を維持する
- 特に、プライバシー・バイ・デザインは、設計者および管理者に対し、強力なプライバシー標準、適切な通知、および権限付与の簡単なオプションのような手段を提供することによって、個人の利益を最大限に維持することを求めている。利用者中心主義を維持すべきである。

プライバシー・バイ・リデザイン(PbRD)

- プライバシー・バイ・リデザイン (Privacy by ReDesign, PbRD)
- 2011年にアン・カブキアン博士が提唱
- このプライバシー・バイ・リデザイン(PbRD)というコンセプトは、要約すれば、多数の組織が既存の情報システムに多額の投資をし、情報システム自体が成熟化していることから、新たなシステムをデザインし、実用化することは多くの場合、現実的ではないので、既存の情報システムにプライバシー・バイ・デザインを導入することであるということになる。
- The 3 R's of *PbRD* ; Rethink, Redesign, and Revive

個人情報保護と情報セキュリティ

	個人情報	法人等情報
個人情報保護関係法令 例：個人情報保護法、行政機関 個人情報保護法、独立行政法 人等個人情報保護法、地方公 共団体の個人情報保護条例、 マイナンバー法案 (OECDプライバシー・ガイドライ ン、EUデータ保護指令)	○	×
情報セキュリティ関係法令 例：刑法改正(1987年、コン ピュータ犯罪処罰規定)、不正 競争防止法(1993年、営業秘 密)、不正アクセス禁止法(1999 年)、刑法改正(2011年、ウイル ス作成罪) (OECD2002年セキュリティ・ガイ ドライン)	○	○