データ保護と電子行政サービスに関する欧州調査ご報告資料

2014年8月28日

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

調査概要： 調査趣旨と日程

○調査趣旨

- パーソナルデータ検討会における検討やパーソナルデータの利活用に関する制度改正大綱（案）の策定を受け、「匿名化」「顔認識データ（準個人情報）」「マルチステークホルダープロセス」「プロファイリング」「第三者機関の役割」等、日本において論点となっている事項に対する欧州での考え方・方針について、現地のデータ保護監督機関（Data Protection Authority：DPA）を中心にヒアリング調査を実施した。調査国は欧州の中でも特に個人データ保護への積極的な取組みを行っているフランス、ドイツ、ポーランドの3ヶ国とした。
- また、併せて各国における電子行政サービス事例や番号制度について調査を行った。

○日程

- 2014年6月17日（火）～6月24日（火）

調査概要： 訪問先

国名	訪問先機関	概要
（1）データ保護関連		
フランス	①CNIL（Commission nationale de l'informatique et des libertés）	フランスのデータ保護監督機関
	②次世代インターネット財団（Fondation Internet Nouvelle Generation）	消費者に自己情報コントロールを与えるMesInfosﾌﾟﾛｼﾞｪｸﾄを実施
ドイツ	③連邦データ保護・情報自由監察官事務所	ドイツ連邦のデータ保護監督機関
	④ベルリン州データ保護・情報自由監察官事務所	ベルリン州のデータ保護監督機関
ポーランド	⑤個人データ保護監察官（Inspector General for Personal Data Protection）	ポーランドのデータ保護監督機関（監察官本人に面会）
	⑥Panoptykon財団	ポーランドのプライバシー保護団体
（2）番号制度・電子政府関連		
フランス	⑦首相府 法律・行政情報局（Direction de l'information legale et administrative）	mon.selvice-public（フランス版電子私書箱）を運営
ドイツ	⑧ベルリン州内務省（Senatsverwaltung fur Inneres und Sport）	eIDカードを用いた住民向けサービスを提供
ポーランド	⑨内務省	住民登録台帳やIDカード台帳を所管
(3)IT政策関連		
ドイツ	⑩経済エネルギー省	ドイツの新たなIT戦略（デジタルアジェンダ）を策定中

1. データ保護関連

全世界的なデータ保護制度見直しの動き

EU	・**1995年　EUデータ保護指令　採択** ・**2012年1月　EUデータ保護規則案　公表** ・2014年3月　EU規則案欧州議会修正案の採択（理事会は未決）
米国	・1974年　プライバシー法（連邦行政機関を対象）　制定 ・**民間分野は自主規制中心（医療、金融、教育等を除く）** ・**2012年2月　消費者プライバシー権利章典　公表** ・**2012年3月　FTCのプライバシー・フレームワーク　公表**
OECD	・1980年　プライバシーガイドライン　採択 ・**2013年7月11日　プライバシーガイドライン改定**
APEC	・2004年　APECプライバシー・フレームワーク　採択 ・2011年　越境プライバシールール（CBPR）　採択 ・2014年4月　日本のCBPRへの参加が認められる
日本	・2003年　個人情報保護法 制定 ・2013年12月 「パーソナルデータの利活用に関する制度見直し方針」 ・**2014年6月 「パーソナルデータの利活用に関する 制度改正大綱」**

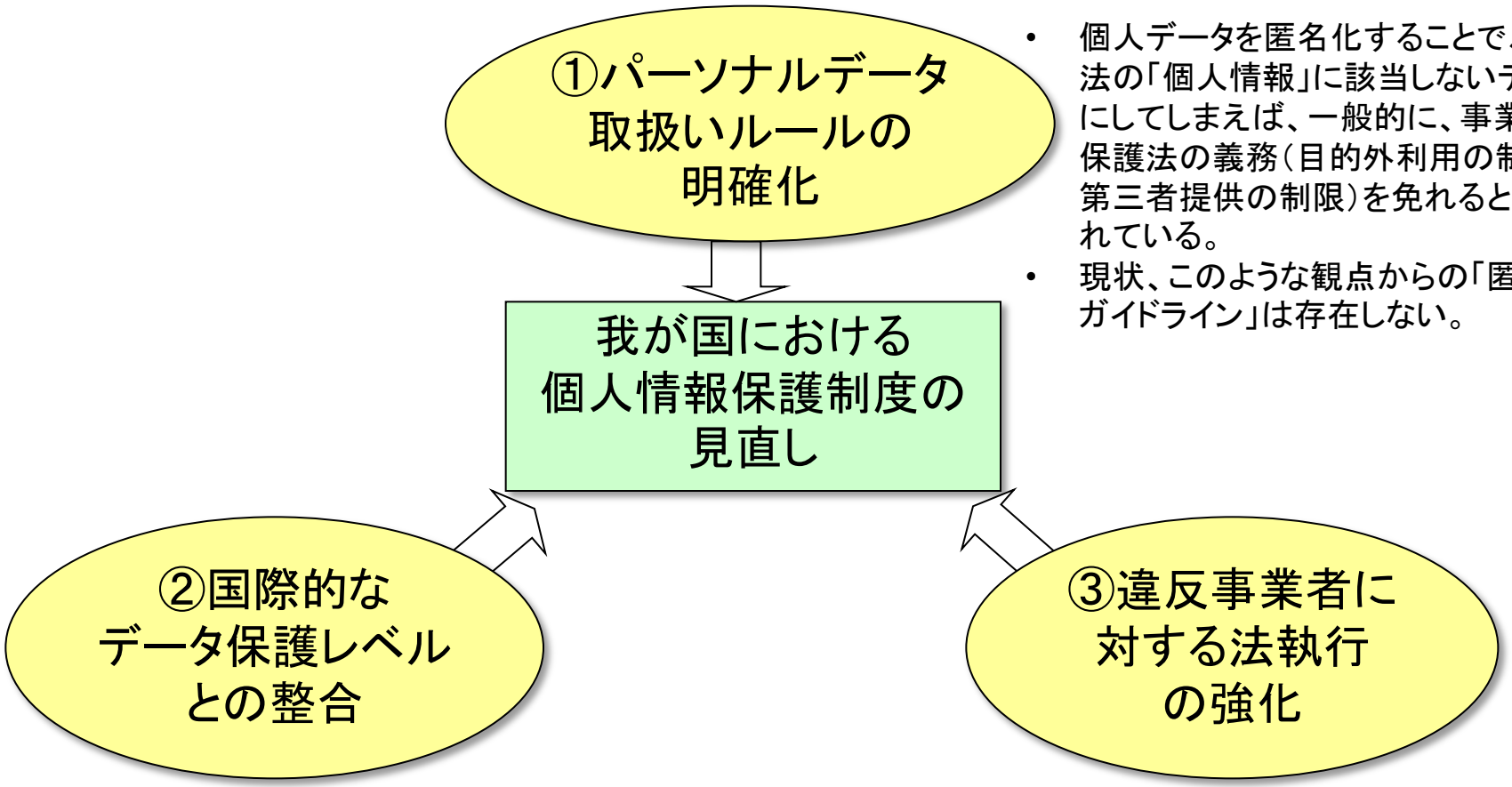
「忘れられる権利」など

Do Not Track など

FTC 3条件など

（出典：国際社会経済研究所）

日本における個人情報保護制度見直しの要因



- 個人データを匿名化することで、保護法の「個人情報」に該当しないデータにしてしまえば、一般的に、事業者は保護法の義務（目的外利用の制限、第三者提供の制限）を免れると考えられている。
- 現状、このような観点からの「匿名化ガイドライン」は存在しない。

- 日本のデータ保護法制は国際的には「十分なレベルにない」と見られている。
- EUはデータ保護指令において、十分な保護レベルにない第三国への個人データ移転を禁じているため、日本企業は特例的な方法を用いてデータ移転をしている。
- 第三国へのデータ移転禁止条項はシンガポールやマレーシア、台湾、香港等の保護法でも導入。

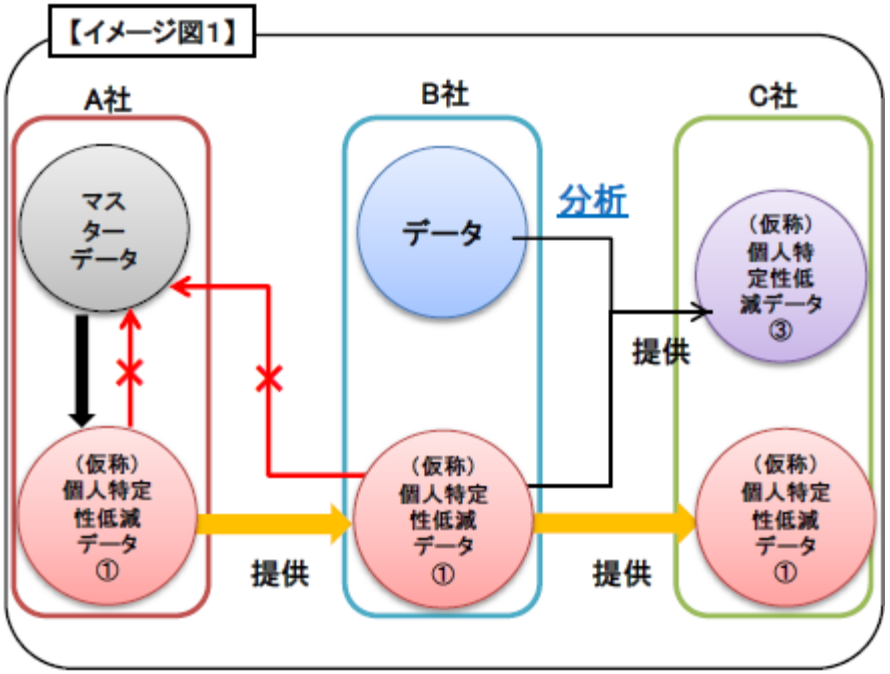
- 電話勧誘業者や名簿業者、スマホアプリ事業者、海外事業者等によって個人情報が濫用。
- 保護法には違反事業者に対する罰則規定があるが、これまで罰則適用は1件もない。
- 違反事業者に対する法執行の甘さは結果的に利用者の不安や不満を引き起こし、法令を遵守する大多数の事業者までが皺寄せを受ける羽目に。

（出典：国際社会経済研究所）

「大綱」における制度改正の柱

（1）個人特定性低減データの導入

- 特定個人が識別される可能性を低減するデータへの加工と、その適正な取扱い（再特定禁止等）を規定することで、本人同意のない第三者提供と目的外利用を可能とする。
- データの加工方法は一律に定めず、事業等の特性に応じた適切な処理を可能とする。また、当該加工方法等については、後述のように民間団体において自主規制ルールを策定し、第三者機関による認定を受けることが可能である。

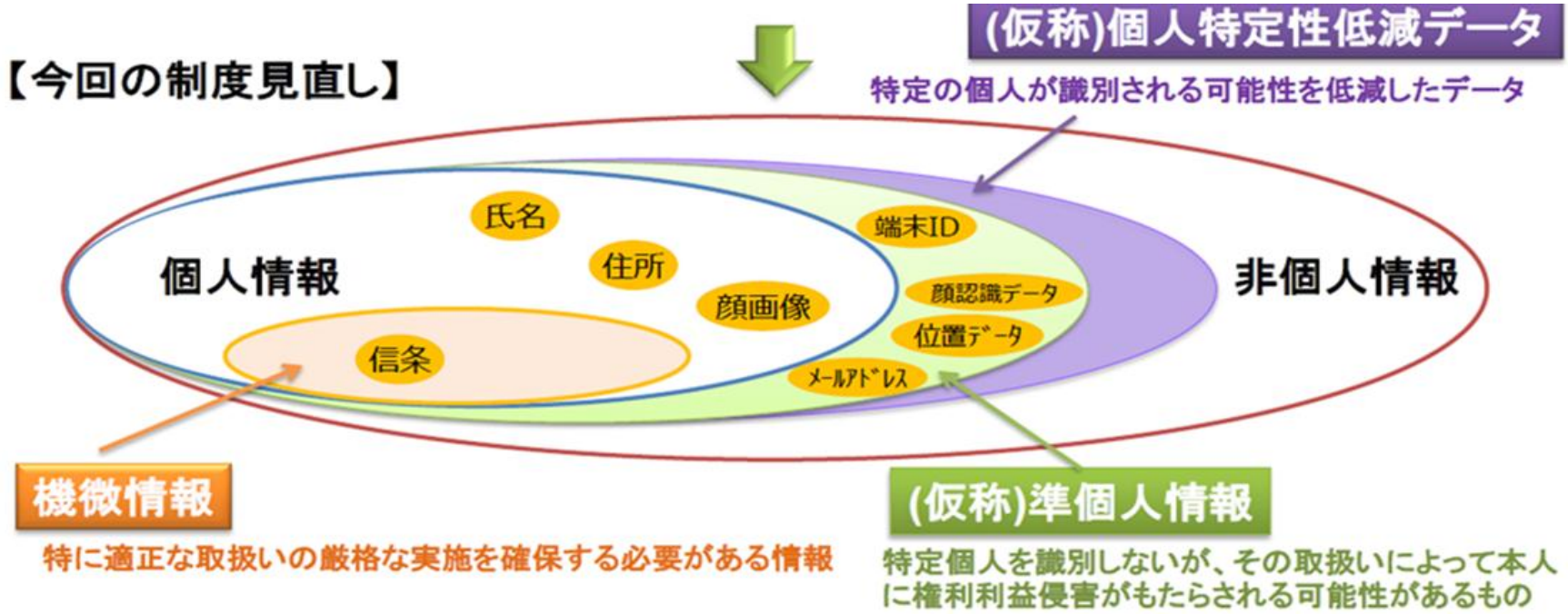


図の出典：パーソナルデータ検討会資料

「大綱」における制度改正の柱

（2）保護対象となるパーソナルデータの見直し

- パーソナルデータの中で、個人情報として保護対象となるものを明確化。
- 指紋認識データ、顔認識データ（特徴情報）等は保護対象に含める 。（「準個人情報」に相当）
- 個人情報等の定義への該当性判断は、第三者機関がガイドライン等を用いて解釈を明確化する。また、個別の事案に関する事前相談（第三者機関）等による迅速な対応を実施する。



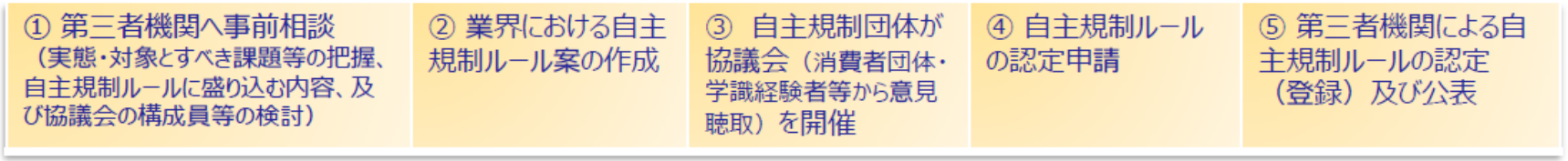
図の出典：パーソナルデータ検討会資料

「大綱」における制度改正の柱

（3）民間主導による自主規制ルール制度の創設（マルチステークホルダープロセス）

- 「マルチステークホルダープロセス」の考え方を活かした民間主導による自主規制ルールの枠組みを創設する。
- 「民間団体」（自主規制団体）が策定した自主規制ルールは、第三者機関の認定を受けることが可能に。

※マルチステークホルダープロセス： 国、事業者、消費者、有識者等の関係者が参画するオープンなプロセスでルール策定等を行う方法のこと。



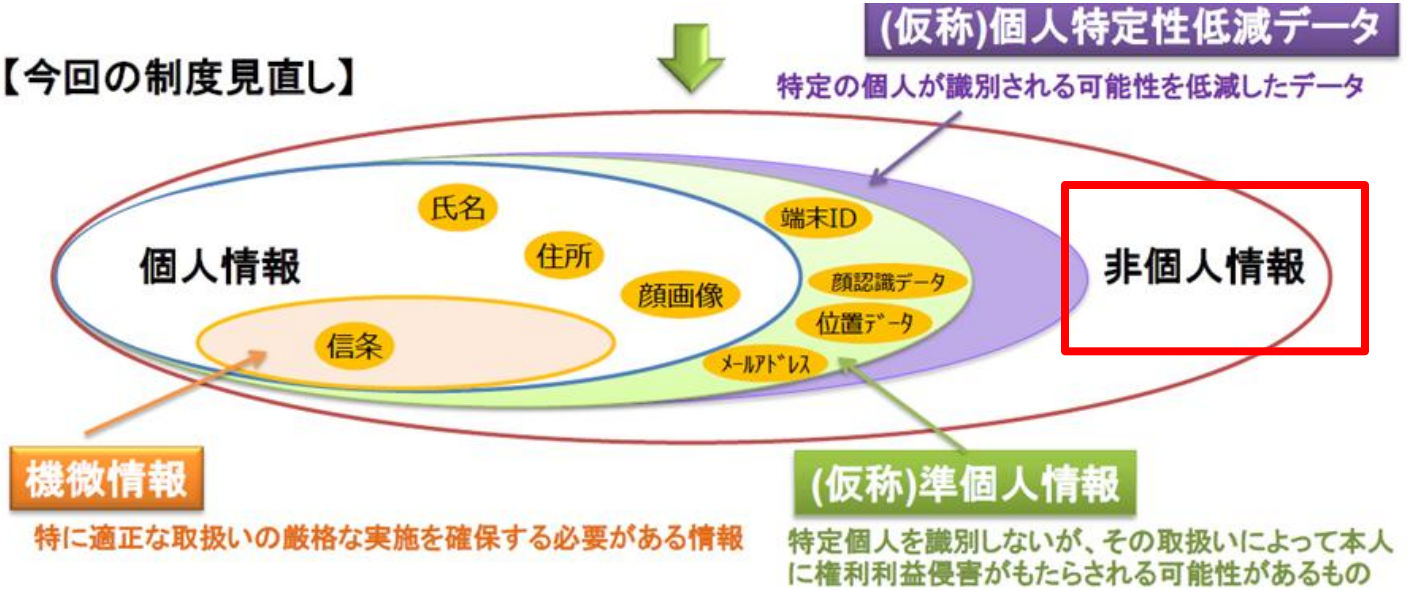
図の出典：パーソナルデータ検討会資料

（4）第三者機関の体制整備

- パーソナルデータの保護と利活用をバランスよく推進するため、独立した第三者機関を設置する。実際には、番号法で本年1月に設立された特定個人情報保護委員会 の所掌事務を拡大することで設置する。

①匿名化について： 概要

- 日本のパーソナルデータ検討会および大綱での検討状況
  - 保護法の対象外となる「匿名化」（Anonymisation＝非個人情報化）については大綱での言及なし。



図の出典：パーソナルデータ検討会資料を加工

- 他方、EUデータ保護指令やEUデータ保護規則案では、匿名化したデータは保護の対象外となることが明言されている。
- 2014年4月10日には、EU指令第29条作業部会から匿名化に関するガイドライン（WP216）が公表された。

①匿名化について： EUの指針

- EU指令第29条作業部会の文書
  - WP216：匿名化技術に関する意見書（2014年4月10日採択）
- WP216（Opinion 05/2014 on Anonymisation Techniques）
  - データ保護の観点から既存の匿名化技術の有効性と限界について分析し、個々の匿名化技術に固有の、特定化（identification）に関する残存リスクを考慮することにより、これらの技術を取扱う際の勧告を提供するもの。
  - 「有効な匿名化の3基準」を提示。
    - (i) Singling out：個人を識別（single out）できないこと
    - (ii) Linkability：同一人物の記録と連結（link）できないこと
    - (iii) Inference：ある個人に関する情報であると推定できないこと
  - この3基準に基づき、各匿名化技術の堅固性（robustness）について評価。

有効な匿名化の3基準 / 匿名化技術	個人を識別することが可能か	同一人物の記録と連結することが可能か	ある個人に関する情報であると推定することが可能か
仮名化	× 可能	× 可能	× 可能
ノイズ付加	× 可能	○ おそらく不可能	○ おそらく不可能
置換	× 可能	× 可能	○ おそらく不可能
アグリゲーションまたはk-匿名性	○ 不可能	× 可能	× 可能
l-多様性	○ 不可能	× 可能	○ おそらく不可能
差分プライバシー	○ おそらく不可能	○ おそらく不可能	○ おそらく不可能
ハッシュ化／トークナイゼーション	× 可能	× 可能	○ おそらく不可能

①匿名化について： 各国DPAの意見のまとめ

	フランスCNIL	ベルリン州データ保護監察官事務所	（参考）英国ICO（2013年7月調査）
匿名化したデータを第三者提供するに当たっての本人同意	本人同意不要	本人同意不要	本人同意不要
いわゆる連結可能匿名化されたデータの扱い	提供元が対応表を持つ場合、本人同意のない第三者提供は不可（提供元が対応表を持つ限りは匿名化と言えないため）	・提供元が対応表を持つ場合、本人同意のない第三者提供は不可 ・提供元が元データのみを持つ場合は、下記条件を満たせば、本人同意なく第三者提供可能 ・元データへの外部からのアクセス不可 ・匿名化に当たって一定レベルの集合化	対応表が提供元に残っていても、本人同意なく第三者提供可能
委託先（クラウド事業者等）における匿名データの扱い	委託元が匿名化したデータであっても、委託先が独自目的で匿名データを利用することはできない	委託元が匿名化したデータであっても、委託先が独自目的で匿名データを利用することはできない	委託先が、本人同意なく、匿名化して独自目的で利用することは、当該利用が公正で正当な場合には許される
匿名化へのDPAの関与	匿名データに対して、CNILはそれが適正な技術を用いた匿名化か否かを検査する権限を持っている。チェックするトリガーは3つあり、①市民からの苦情、②CNILの年間計画で規定された重点分野に対する検査、③マスコミ報道である	匿名化措置に関するリスク評価は、企業が自ら行う。ただし、企業のデータ保護担当官が自ら懸念を抱く場合や市民からの苦情があった場合には、DPAが検査・評価を行ったり、外部専門機関が評価をしたりする	匿名化措置に関するリスク評価や匿名化措置の適切性について、事前にICOに相談し、アドバイスを得ることが可能。ICOは監査人や調査チームを持っており、技術エキスパートも有している

①匿名化について： フランスCNILの意見（1/2）

- 第三者提供時の本人同意
  - 匿名化したデータにはフランスやEUのデータ保護法規が適用されなくなるため、第三者提供に当たって本人同意は不要である。ただ、どの段階で匿名化されたかがグレーゾーンとなっている。そのため、WP216（匿名化技術に関する意見書）を策定した。

- 「連結可能匿名化」について
  - データの提供元がいわゆる「対応表」を持っている場合には、匿名化とは言えない。（世の中のどこかに対応表が存在する限り、そのデータは匿名化データではない。）

- データ処理者（委託先）による匿名データ利用
  - データ管理者Aがデータ処理者B（クラウド事業者等）にデータ処理を委託している場合、委託元Aが匿名化したデータであっても、委託先Bが独自目的でデータを利用することはできない。
  - 上記のクラウド事業者Bが独自目的でデータを利用する場合には、Bはデータ管理者となる必要がある。この場合には、AとBが共同管理者として各々のデータ利用に責任を負う。

①匿名化について： フランスCNILの意見（2/2）

- 匿名化へのDPAの関与
  - 匿名化したデータを統計目的で利用する場合、CNILに申告する義務がある。
  - 医療データを匿名化する場合は、事前にCNILの承認が必要である。
  - 匿名データに対して、CNILはそれが適正な技術を用いた匿名化か否かをチェック（検査）する権限を持っている。チェックするトリガーは3つあり、①市民からの苦情、②CNILの年間計画で規定された重点分野に対する検査、③マスコミ報道である。

- WP216（匿名化技術に関する意見書）について
  - EU指令第29条作業部会の下のサブWPで作成した。イタリアのDPAがラポーターとなり、CNILと英国ICOが非常にアクティブに寄与した。基本的に、各国のコンセンサスを取っている。
- 匿名データのオープンデータとしての利用
  - 個人データ起源のオープンデータとしては2種類ある。
    - 匿名化されたデータ（統計法に基づく統計データ）
    - 法律上で情報公開が必要なデータ（公的機関の公務員名簿等）
  - 公共データの二次利用
    - 医療分野では、オープンデータではないが、SNIIRAM（Système National d'informations Inter Régions d' Assurance Maladie：疾病保険地方間全国情報システム）というDBがあり、二重の匿名化を行っている。このDBへのアクセス権限を得るためには、CNILの許可が必要である。

①匿名化について： ドイツのDPAの意見（1/3）

●ドイツ連邦データ保護監察官事務所

- WP216（匿名化技術に関する意見書）について
  - WP216にドイツの意見はかなり反映されている。匿名化、仮名化については明確な定義をすべきと考えている。

●ベルリン州データ保護監察官事務所

- 第三者提供時の本人同意
  - WP216に挙げたような有効な匿名化の条件が揃った時点で、そのデータは個人とは切り離されたものとみなされる。匿名化したデータは再特定が不可能なものという位置付けなので、第三者提供に当たって本人同意は不要である。
- 元データが残存する場合の匿名データの扱い
  - 元データの保存は一定の条件で許されており、その場合は匿名化したデータを本人同意なく提供できる。ただし、分野によって扱いが異なる。
  - 元データが残存する場合に匿名データを第三者提供できる条件は、元データに外部からアクセスできないことである。
  - さらに、元データと匿名データとの結合を再構築できないように、一定以上の防護の強度（一定レベルの集合化）が要求される。

①匿名化について： ドイツのDPAの意見（2/3）

●ベルリン州データ保護監察官事務所 （続き）

- データ処理者（委託先）による匿名データ利用
  - データ管理者Aがデータ処理者B（クラウド事業者等）にデータ処理を委託している場合、委託先Bが独自目的でデータを利用することはできない。クラウド事業者は、委託された時点の目的でしかデータを処理できない。
  - ただ、医療データの場合には、以下2つの場合に委託先が研究目的で使うことは許される。
    - 法の規定がある場合
    - データ処理委託の際に、元の医療機関が研究目的での利用に同意している場合
- 医療データの扱い
  - 医療データについては、匿名化・仮名化して研究目的で二次利用することが許されている。州によって若干、規定が異なる。
  - また、個人の権利利益に与える影響と公共の利益とを比較考量して後者の方が大きい場合には、匿名化しなくても二次利用できる。これはハードルが高く、DPAの承認が必要である。
  - 例えば、癌のDBには、関連する疾病も含め、全国の患者の氏名のデータが入っている。このDBを使う場合には、個人データと疾病データを併せて参照することも許されている。もちろん医療機関の全員がこのDBにアクセスできる訳ではなく、アクセス権限を持つ人も必要なデータにしかアクセスできない。

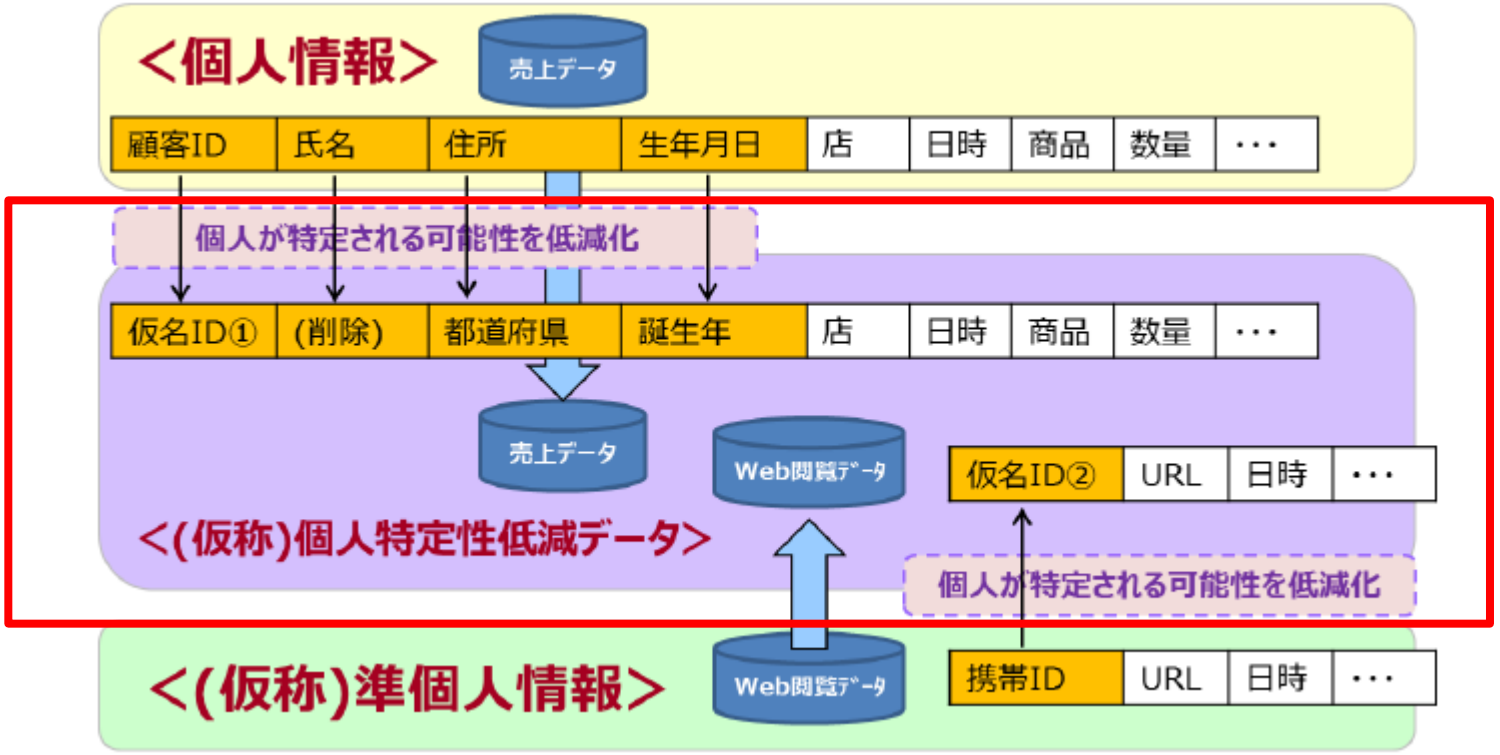
①匿名化について： ドイツのDPAの意見（3/3）

●ベルリン州データ保護監察官事務所 （続き）

- 匿名化へのDPAの関与
  - 匿名化措置に関するリスク評価は、企業が自ら行う。
  - ただし、一般的に、企業のデータ処理に懸念があれば、DPAが検査または評価を行ったり、外部専門機関が評価をしたりする。そのきっかけは市民による苦情申立てであったり、企業のデータ保護担当官が自ら抱く懸念であったりする。DPA等による評価の場合も、企業のデータ保護担当官は参加する。
  - 匿名化措置に関しては、再特定化が可能かどうかを評価する。そのため、一定の外部情報を持っている専門機関でないと評価できない場合がある。
  - このDPAによるリスク評価は第三者認証制度ではない。第三者認証制度としては、シュレースヴィヒ＝ホルシュタイン州のEuroPriSeがある。他州には無い。

②仮名化について： 概要

- 「仮名化」（Pseudonymisation）
  - 個人情報から個人を特定するデータ項目（氏名、住所等）を削除し、代わりに識別子を付加する処理。当該識別子は同一人物を識別（追跡）するために利用される場合がある。
- 前述の「個人特定性低減データ」は仮名データに近い概念。



図の出典：パーソナルデータ検討会資料を加工

【ご参考】EUデータ保護規則案の欧州議会修正案における仮名データの扱い

○ 第4条2a項

- 「仮名データ（pseudonymous data）」とは、以下のような条件において、追加情報の利用なくしては、特定のデータ主体に結び付ける（attribute）ことができない個人データを意味する。その条件とは、当該追加情報をデータ主体に結び付けないことを保証するために、当該追加情報が分離して保管され、技術的かつ組織的措置の下にあることである。

- ※**仮名データは個人データの1類型**であるが、管理者や処理者が仮名データの処理を行う場合には通常の個人データの処理を行う場合に比べて、**様々な義務が緩和**されている。
  - 仮名データに限った処理は、第6条にいう「データ処理の合法性」において、データ主体の合理的な期待に適合した処理とみなされる。【前文（38）】
  - 仮名データ処理に基づく「プロファイリング」は、データ主体の利益・権利等に重大な影響を与えるとはみなされない（ので、本人の明示的な同意等は必ずしも必要とされない）。【前文（58a）】
  - 仮名データに限った処理の場合、データ主体から自己データに関するアクセス請求等があった場合に、必ずしも管理者は請求に応じなくてよい。【第10条】

- ※その他、仮名データに関しては、以下のような規定がある。
  - 医師に代わって健康医療データを処理する処理者は、可能な限り匿名化されたデータ又は仮名化されたデータのみを受領し、処理するものとする。【前文（122a）】
  - データ保護影響評価の項目の一つとして、仮名化等の個人データ保護メカニズムのリストアップが挙げられている。【第33条】
  - 健康医療データを研究目的で、データ主体の同意なく処理する場合には、匿名化または仮名化が必要である。【第81条】

②仮名化について： フランスCNILの意見

- 仮名データの位置付け
  - 新たなEUデータ保護規則に仮名データの定義は必要ない。（2014年3月の欧州議会修正案では仮名データの定義が追加された。）
  - 仮名データには、作成元の企業に個人を特定できるデータ（対応表）が残っているため、匿名化データではなく個人データである。
  - 個人データの安全性を高める手段としての仮名データの利用は奨励するが、通常の個人データとは別に仮名データという別カテゴリを設けて管理者の義務を緩和することは、法の網の目に抜け穴を作るものなので、反対する。
  - もし仮名データの義務を緩めてしまうと、仮名データの量が非常に増えるのでリスクも増加する。トロイの木馬となってしまう。
  - EU指令第29条作業部会のリスクベース・アプローチに関する宣言書（WP218）でも、仮名化は重要な安全管理措置だが、仮名データに対する義務を緩和することには反対する旨が述べられている。

②仮名化について：ベルリン州データ保護監察官事務所の意見

- 仮名化の位置付け
  - EUレベルでは、第29条作業部会でEUデータ保護規則案（仮名データの扱い）に対する意見書を作るか議論中である。域内各国への影響を考えて出すかどうか決める。
  - ドイツでは、連邦データ保護法で仮名化をプロセスとして定義している。既存の法律に影響があるので、ドイツとしては意見を出そうとしている。
  - 仮名データをどのような目的で使うのか、仮名データの裏側に個人データがあるかどうかによって、プロセスは異なってくる。仮名化プロセスが異なる例としては、仮名データを第三者企業や関連会社に提供することが予定されている場合は、加工のレベルを上げなければならない。
  - （匿名化の基準を満たしていない）仮名データの第三者提供に当たっては、本人同意が必要である。個人の権利利益を考慮した上で、データ保有者にとって重大な利益がある場合には、本人同意のない第三者提供が認められる場合がある。

- 仮名データに対する開示請求や消去請求
  - データ主体には、仮名データに対する開示等の請求権がある。企業側で仮名データと元データの結合が可能ならば、請求に応じる必要がある。すなわち、企業側で仮名データのみならず個人特定データを利用できるか否かによって個別判断になる。
  - 個人データの仮名化を行う者と、仮名データを利用する者とが異なる場合には、仮名データと元データとを結合することが権利侵害になる場合もあるので、状況によって開示すべきかを判断する必要がある。

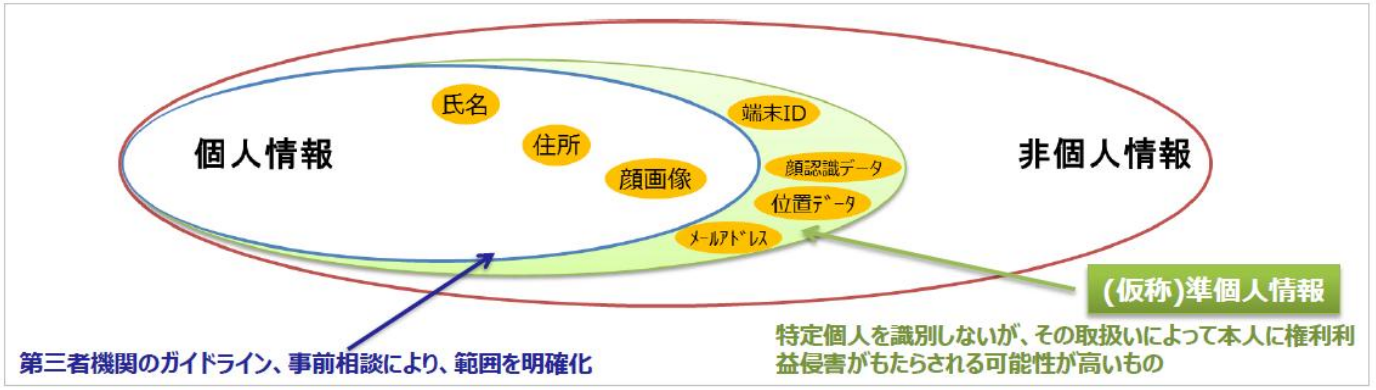
③個人情報の範囲： 日本における検討状況

- パーソナルデータ検討会では、従来からの保護対象である「個人情報」に加え、「（仮称）準個人情報」を新たな保護対象として検討してきた。
  - パーソナルデータ検討会での「準個人情報」の当初案は下記3類型。これらは、さらに技術検討WGで詳細検討された。

    ① パスポート番号、免許証番号、IPアドレス、携帯端末ID等の個人または個人の情報通信端末（携帯電話端末、PC端末等）等に付番され、継続して共用されるもの

    ② 顔認識データ、遺伝子情報、声紋並びに指紋等、個人の生体的・身体的特性に関する情報で、普遍性を有するもの

    ③ 移動履歴、購買履歴等の特徴的な行動の履歴
- 大綱に記載されたのは「指紋認識データ、顔認識データなど個人の身体的特性に関するもの等」のみ。



図の出典：パーソナルデータ検討会資料

③個人情報の範囲： フランスCNILの意見

- 境界的なデータの位置付け
  - IPアドレスは、ISPに聞けば誰が利用したIPアドレスか分かるので個人データである。
  - 携帯電話の端末ID、パスポート番号、メールアドレス、遺伝子情報、指紋情報については、EUでは全て個人データである。ISO/IEC29100でも個人データと定義されている。
    - 註：ISO/IEC29100「Information technology - Security techniques - Privacy framework」。ISO/IEC29100ではPIIとして、社会保障番号、パスポート番号、口座番号、電話番号、正確な位置情報、生体認証データが例示されている。
  - カルフールのサービスカードの顧客IDなど、企業ごとの顧客IDも、当該企業のDBで氏名につながるデータの場合には、個人データである。

④顔認識／監視カメラ：　日本におけるサービス事例

○JR東日本ウォータービジネスの次世代自動販売機　属性推定

– カメラの顔認識により推定した性別・年代や、時間帯・気温・天候を判定材料に、お薦めの飲料品を提示。

（図の出典：JR東日本ウォータービジネス資料）

○NECの「顔認証技術活用マーケティングサービス」

①「顔映像」の取得

②「特徴情報」に変換（＝数値化）

③「顔映像」の削除

④「特徴情報」の利用（リピート顧客の識別）

顔照合

○次世代コンビニ「ローソン パナソニック前店」　属性推定

– パナソニックのカメラを店内に6台配置し、棚の商品を手に取ったが元の棚に戻したときのような「顧客が買わなかった時のデータ」も取得。

– 「何月何日何時、30代後半の男性が、新商品のパンを買わなかった」といったデータが蓄積される。　（出典：THE PAGE 2014年2月15日記事）

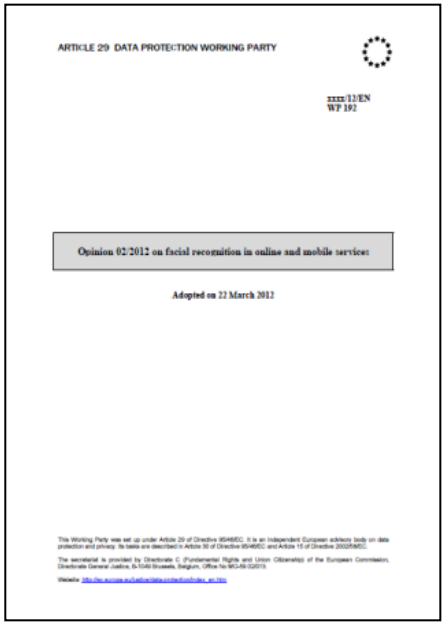
（図の出典：株式会社ローソンのHP）

④顔認識／監視カメラ： 日本の個人情報保護法上の扱い

- **「顔映像」は「個人情報」**に該当
  - 経済産業分野ガイドライン等において「防犯カメラに記録された情報等、本人が判別できる映像情報」は個人情報に該当すると例示。
- 「防犯カメラ」の扱い
  - 経済産業分野ガイドライン等において、一般に**防犯目的のためにビデオカメラを設置**し撮影する場合は、「**取得の状況からみて利用目的が明らかである**と認められる場合」（個人情報保護法第18条4項4号）に該当し、その**利用目的を公表等する必要がない**とされている。
  - ただし、**カメラを防犯以外の目的で利用する場合**には、「取得の状況からみて利用目的が明らか」とは認められない可能性が高いため、**当該利用目的を公表または本人に通知する必要**がある（経済産業分野ガイドライン）。
- 「特徴情報」の扱い
  - 「**特徴情報**」とは、後に顔照合や顔認証で用いるために、顔映像から抽出された個々人にユニークな特徴を示す数値データ。
  - 各省庁のガイドラインでは、「特徴情報」が**単体で個人情報なのか否かは記載されていない**。
    - ただ、IPAの「生体認証利用のしおり 」では「生体認証システムに登録する生体情報は、個人を特定できる情報」と記載されている。
  - 上述のように、大綱では、**「顔認識データ」（＝特徴情報）は新たな保護対象として例示**されている。

④顔認識／監視カメラ： EUと米国の指針

- EU指令第29条作業部会の文書
  - WP80：生体認証に関する作業文書（2003年8月1日採択）
  - **WP192**：オンライン及びモバイルサービスにおける顔認識に関する意見書（**2012年3月22日**採択）
  - **WP193**：**生体認証技術の発展に関する意見書**（**2012年4月27日**採択）
  - **特徴情報（biometric template/ reference template）も個人データ**である。なぜなら、特徴情報は個人の顔の顕著な特徴を含み、**特定個人に連結（link）される**ものであり、**将来的な特定や認証における照合のために蓄積されるものであるから**である。

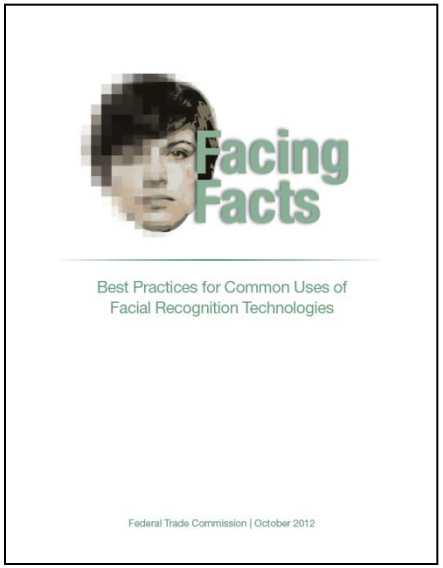

ARTICLE 29 DATA PROTECTION WORKING PARTY

xxxx/12/EN
WP 192

Opinion 02/2012 on facial recognition in online and mobile services

Adopted on 22 March 2012

- 米国FTCレポート “Facing Facts”
  - FTC（連邦取引委員会）では**2012年10月**にスタッフレポート“Facing Facts：Best Practices for Common Uses of Facial Recognition Technologies”を発行。
  - 顔認識技術を使用する企業は、顔検出や属性推定、顔照合などいかなる目的で使用するにせよ、消費者との関係のコンテキストにおいて適切なプライバシー保護を実施すべき。



④顔認識／監視カメラ： フランスCNILの意見

- 防犯目的での利用
  - 防犯目的での利用については、警察の前科情報処理システム（TAJ: traitement d'antécédents judiciaires）で顔照合技術を使用している。
  - 公道の監視カメラでは、顔照合技術は使っていない。かつて、スタジアムでフーリガンの暴動を防ぐ実証実験での使用をCNILが許可したことはある。
  - 監視カメラの画像は一定期間のみ保存できる。本人のアクセス（開示）請求権の規定もある。

- 商用目的での利用
  - フランスでは、顔画像から得られた性別や年齢層といった属性の利用に対しても法規制がある。CNILへの届出が必要であり、また、顔画像自体は消去しないといけない。最近はあまり届出がない（利用が少ない）。

- その他
  - フランスでは、生体認証データの利用にはCNILの許可が必要である。EUの他国では必ずしもそうではない。
  - EUデータ保護規則案の欧州議会修正案では、センシティブデータの1つとして生体認証データが含まれている。

④顔認識/監視カメラ:ベルリン州データ保護監察官事務所の意見(1/2)

- 防犯目的での利用
  - 防犯目的での顔照合技術の利用は、空港等でテロリストを認識する場合は、大多数の公共の利益になるという法益があり、また危険の回避なるので可能である。この場合、一般市民の顔画像を撮影し、Yes/Noの判断に顔画像を照合することは、後に顔画像を消去すれば適法である。ただ、誤認があると権利侵害になるので、ある程度の技術レベルがないといけない。
  - フーリガンのような一定の危険人物のDBを用いて顔照合することも、法的に問題ない。

- 商用目的での利用
  - フェイスブックなどSNSで使われている顔照合機能について、ハンブルクの裁判所が差し止め請求を出した。ベルリン州データ保護監察官は、ハンブルクの裁判所と同じ認識である。アップロードした写真からの顔照合について本人が包括的な同意をしている場合にはOKだが、他人の顔についても顔照合するのは問題である。
  - ドイツでは、(公道等において)マーケティング等の商業目的で顔照合を行うことは違法である。
  - デジタルサイネージ(看板)で、性別・年代に合わせて広告を出すような事例はドイツにはない。属性に合わせた広告を出すだけで、顔画像や顔認識データを保存せず、個人が再識別されないのであれば、よいのではないか。

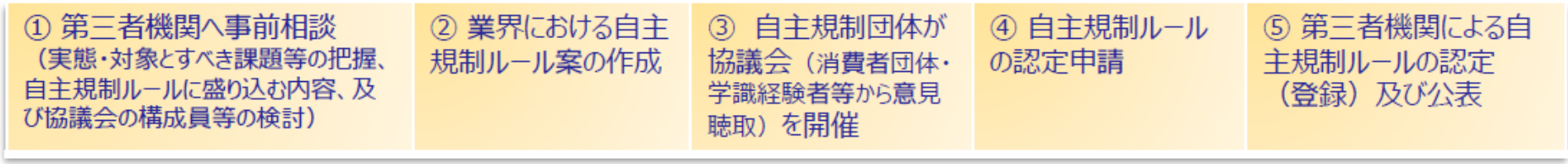
④顔認識/監視カメラ：ベルリン州データ保護監察官事務所の意見（2/2）

- 顔画像に対する消去請求
  - 一般に消去請求はできる。また、連邦データ保護法第6b条の規定により、必要なくなったデータは消去しないといけない。
  - データ保存期間については、DPAと防犯カメラ利用団体とで協定を作り、72時間で消去することとした。ただし、警察に録画データを渡す等の場合は例外である。

- WP192（オンライン及びモバイルサービスにおける顔認識に関する意見書）について
  - 第29条作業部会の意見書WP192に対しては、ベルリン州監察官は歓迎している。

⑤共同規制／マルチステークホルダープロセス：日本の検討状況

- 「マルチステークホルダープロセス」
  - 国、事業者、消費者、有識者等の関係者が参画するオープンなプロセスでルール策定等を行う方法のこと。
- 大綱における言及
  - 「パーソナルデータの利活用の促進と個人情報及びプライバシーの保護を両立させるため、消費者等も参画するマルチステークホルダープロセスの考え方を活かして、民間団体が業界の特性に応じた具体的な運用ルール（例：個人の特定性を低減したデータへの加工方法）や、法定されていない事項に関する業界独自のルール（例：情報分析によって生じる可能性のある被害への対応策）を策定した場合は、その認定等において、第三者機関が関与して実効性を確保する枠組みを創設する。」
  - 「自主規制ルールを策定する民間団体は、（・・・）業界・分野ごとの特性及び利害関係者の意見を踏まえてルールを策定し、当該ルールの対象事業者に対し必要な措置を行うことができることとする。また、第三者機関は当該ルール又は民間団体の認定等を行うことができることとする。」



図の出典：パーソナルデータ検討会資料

⑤共同規制／マルチステークホルダープロセス： ドイツのDPAの意見

●ドイツ連邦データ保護監察官事務所

- 業界レベルでルールを作れることは法律に規定されている。企業や業界団体が作った行動規範に対して、DPAは法律に適合しているかを判断できる。実際には両者で協議しながら行動規範作りを進めている。
- ただ、この枠組みで実際に作られた行動規範は2つしかなく、保険業界のものと、地理データの協会のものである。
- 行動規範は、企業が適法か否かを判断できるように規定を具体化したものである。行動規範を守っている限りは違反にならない。第三者機関が適法と判断しているので、安全である。

●ベルリン州データ保護監察官事務所

- 業界団体が作成した行動規範に対する認定制度はある。保険業界の行動規範はこれに当たる。
- 保険業界の行動規範の認定では2万ユーロの費用を業界側がDPAに払っている。これは工数等に応じて公共料金規定に則った料金である。高い金額に見えるが、保険業界側にも法に抵触しないことの保証というメリットがある。

⑤共同規制／マルチステークホルダープロセス：フランス・ポーランドDPAの意見

●フランスCNIL

- 各セクターで決める業界ルールは奨励されている。データ保護法（データ処理・データファイル及び個人の自由に関する法律）の第11条にも明記されている。CNILが業界ルールをチェックすることもある。
- CNILはセクターごとに適合性のパッケージを設けている。セクター側にも好感を持たれている。
- EUデータ保護規則案（第38条）でも、業界団体による行動規範の策定が奨励されている。

●ポーランド個人データ保護監察官

- 業界団体で作成した行動規範を評価してきている。ダイレクトマーケティング業界、保険業界、自動車販売業界、製薬業界などである。珍しい例として、カトリック教会やギリシャ正教の行動規範も評価した。
- 行動規範の例としては、昔は教会で結婚式を挙げるとき、1か月前から教会に新郎新婦の氏名や住所を掲示していた。これをマーケティング業者が収集して使っていた。氏名と教会の信者であることを掲示すれば十分なので、そのような行動規範とした。

⑥プロファイリング： 概要

- 「プロファイリング」
  - 個人データの自動処理（いわゆるビッグデータ分析）に基づき、一定の目的下で、個人をいくつかのカテゴリにセグメンテーション・分類すること。

- 大綱における言及
  - 「多種多量な情報を、分野横断的に活用することによって生まれるイノベーションや、それによる新ビジネスの創出等が期待される中、プロファイリングの対象範囲、個人の権利利益の侵害を抑止するために必要な対応策等については、現状の被害実態、民間主導による自主的な取組の有効性及び諸外国の動向を勘案しつつ、継続して検討すべき課題とする。」

- EUデータ保護指令／EUデータ保護規則案での扱い
  - 「profiling」は、「ある自然人に関する個人的側面を評価することを意図した自動処理、または、とりわけ当人の業務パフォーマンス、経済状況、位置、健康、個人的嗜好、信頼性若しくは行動を分析若しくは予測することを意図した自動処理」を意味する。（EU規則案）
  - プロファイリングに基づき、当人に対する法的効果を生み出すような措置または当人に重大な影響を与えるような措置は、規制されている。

⑥プロファイリング：ドイツ連邦データ保護監察官事務所の意見

- プロファイリングについては、データを収集すること自体は問題ない。ただし、プロファイリングによって直接的に本人が影響を被る場合は規制がかかる。データのセグメント化（構造化）を通じて、例えば銀行が融資の判断をすることは違法である。セグメント化（構造化）までを行うことは構わない。
- 自動的なセグメント化によって、事業者が本来持ってはいけないようなデータ（自動処理に基づく評価データ）を持つことは違法である。
- 例えば、Googleに対する2014年5月のEU司法裁判所の判決では、Webで収集したデータを構造化した時点で問題がある（検索結果への重み付けとして、本人に影響が及ぶため）。ドイツ連邦監察官として、判決に賛成する。構造化を通じてある時点を超えた時点で違法になる。

⑦第三者機関(DPA)の役割：日本における検討状況

- 大綱における記載内容
  - 「専門的知見の集中化、分野横断的かつ迅速・適切な法執行の確保により、パーソナルデータの保護と利活用をバランスよく推進するため、独立した第三者機関を設置し、その体制整備を図ることとする。」
  - 「番号法に規定されている特定個人情報保護委員会の所掌事務にパーソナルデータの取扱いに関する事務を追加することとし、内閣総理大臣の下に、パーソナルデータの保護及び利活用をバランスよく推進することを目的とする委員会を置くこととする。」
  - 「この第三者機関は、番号法に規定されている業務に加えて、パーソナルデータの取扱いに関する監視・監督、事前相談・苦情処理、基本方針の策定・推進、認定個人情報保護団体等の監視・監督、国際協力等の業務を行うこととする。」
  - 「第三者機関は、現行の主務大臣が有している個人情報取扱事業者に対する権限・機能(助言、報告徴収、勧告、命令)に加えて、指導、立入検査、公表等を行うことができることとするとともに、現行の主務大臣が有している認定個人情報保護団体に対する権限・機能(認定、認定取消、報告徴収、命令)を有することとする。」
  - 「また、第三者機関は、民間主導による個人情報及びプライバシーの保護の枠組みの創設に当たり、自主規制ルールの認定等を行う。さらに、国境を越えた情報流通を行うことを可能とする枠組みの創設に当たり、認証業務を行う民間団体の認定、監督等を行うこととする。」

⑦第三者機関(DPA)の役割：EU各国のDPAの意見

●フランスCNIL： 事前相談制度

– CNILにはアドバイザー機能がある。例えば、CNILに相談に来た中小企業に対して、法律にあったデータ処理ができるように、アドバイスや支援をしている。こうした企業を支援して、データ処理が法律に適合していることを保証する場合もある。

●ポーランド個人データ保護監察官： 事前相談制度

– 民間企業からの、自社のデータ処理が法律に適合するか否かに関する相談には、無料で応えている。prior consultationである。

– ただし、全ての相談に対応できないので、新たなデータ処理の方法や新たにデータ保護上のリスクが生じそうなサービスを導入しようとする企業を選んで対応している。

– 実際に、銀行が新たに生体認証ATMを導入しようとしたときには、DPAとして評価に参加した。しかし、銀行が通常のデータ処理をする場合に法に適合しているか否かの相談は断る。

●ドイツ連邦データ保護監察官事務所： DPAの責任

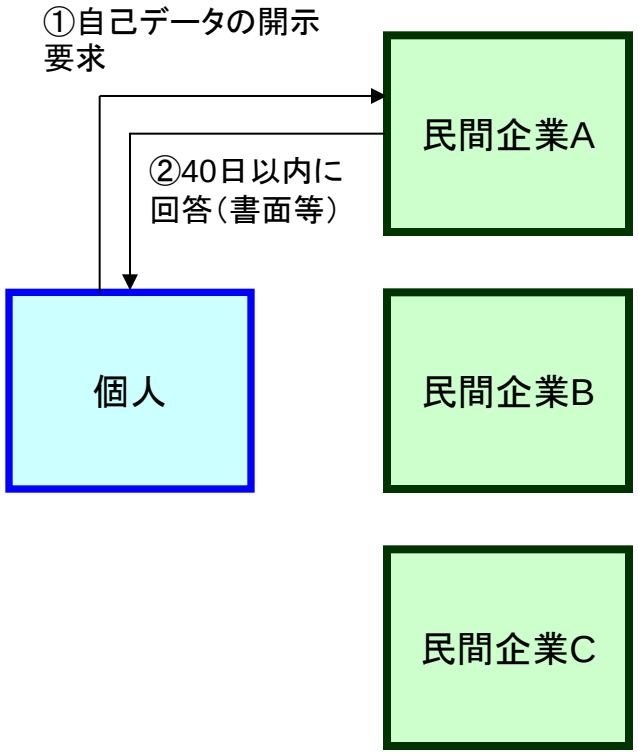
– DPAが監督する企業におけるデータ処理について、基本的にDPAが責任を負うことはない。データ処理に関する責任はすべて企業の側にある。DPAは、企業におけるデータ保持や処理を事前に許可しているわけではなく、事後的に監視するのみである。

– ただ、DPAに企業のデータ保護に関して責任を持たせるという議論は皆無ではなく、 DPAの判断に責任を持たせようという議論はある。連邦の監察官や州の監察官は反対している。コンプライアンスの責任は企業が負うべきである。

– BCR等は事前許可制なので、これに対してDPAが責任を取るのは理解できる。

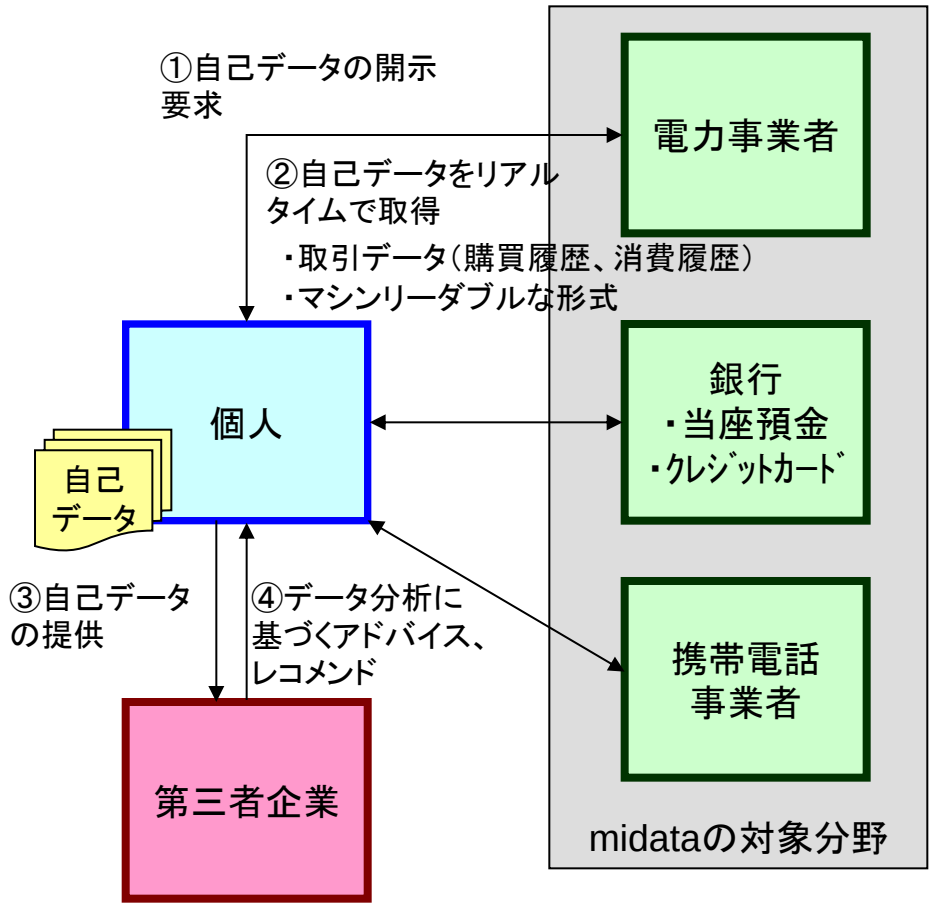
⑧消費者に自己情報コントロールを与える試み：英国midata（参考）

○従来の自己データ開示制度



- 企業に対する自己データの開示要求は法的権利として認められているが、取得に最大で40日間かかる（データ保護法の規定）
- 電子的形式で取得する権利は認められていない
- 国民の半数以上が開示要求権を知らない

○ midataの枠組み



- 個人が開示要求をした際、自己データをリアルタイムで取得することが可能になる
- 第三者企業も利用できるような、一定のマシンリーダブルな形式の電子データを取得可能

出典：国際社会経済研究所

⑧消費者に自己情報コントロールを与える試み：フランスMesInfos（1/2）

出典：http://mesinfos.fing.org/

⑧消費者に自己情報コントロールを与える試み：フランスMesInfos（2/2）

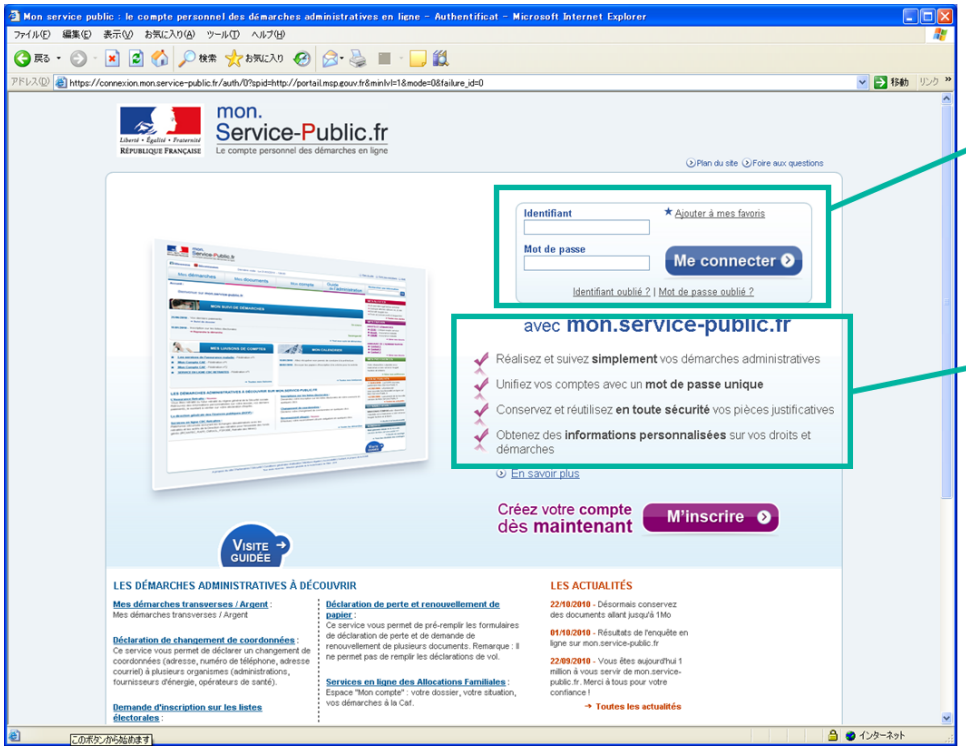
●フランス・MesInfosプロジェクト

- 政府や民間企業が保有する個人データを、データ主体の意思でパーソナルデータストア（クラウド）に預け、その利活用をデータ主体がコントロールできるようにするプロジェクト。英国のmidataに類似。
- フランスの次世代インターネット財団（FING）が主催。
- 2013年11月～14年4月まで実証実験を実施。ベンチャー企業が実証用アプリを開発。
  - 複数の銀行口座の利用明細をアグリゲートするアプリ
  - 利用者のカーボンフットプリントを算出して、改善をアドバイスするアプリ
  - 様々な製品の保証内容を比較してランキングを作るアプリ　等
- 実証実験には300人が参加。実証実験の分析結果は以下。
  - ①アプリ開発者の発想の転換が重要（企業向けサービスから個人向けサービスへ）
  - ②消費者は自分のデータを自分で管理し、自分で利活用するという理念には賛同するが、そのニーズを満たす具体的なサービス形態は今後の課題
  - ③企業における顧客データ形式の標準化が必要
  - ④複数のデータを組み合せることでデータの価値が増大する
- ビジネスモデルとしては、個人に課金することを想定。
- 今後は、ヘルスケア関連アプリの開発、大手銀行や行政機関との提携、基礎研究（技術的要素、ビジネスモデル、セキュリティ）の継続を図る。

２．番号制度・電子行政サービス関連

フランスMSP： mon.Service-Public.fr（MSP）の概要

- 国民に対して、オンライン行政サービスの単一のアクセス・ポイントを提供。
- 2008年12月から試験サービス、2009年10月に正式にサービス開始。首相府のDILA（法律・行政情報局）が運営。
- 利用者は2014年6月現在750万人（人口は約6600万人）。毎日4万5000件のアクセス。
- 2009年12月の閣議決定において、政府部門によって開発された新たなオンライン行政サービスは必ずMSPを通じて利用可能としなければならないとされた 。
- CNILの厳密なチェックの上での許可を受けて、MSPを開始している。



ID/PWによるログイン

MSPで何ができるかの説明

「あなたの行政手続きを簡便化します」

「あなたのアカウントを単一のパスワードに統合します」

「あなたのことを証明する文書を保管し、再利用できます」

「あなたの権利行使や手続き上で必要となるパーソナライズ情報を入手できます」

画像の出典：mon.Service-Public.frホームページ

フランスMSP： MSPの特徴

① ID連携（IDフェデレーション）:

- シングルサインオン機能を実装。リバティ・アライアンス標準に準拠。現状はID/PWでアクセス。
- 下記を含む15の全国レベルの機関と提携し、シングルサインオンが可能。
  - 全国医療保険金庫（CNAM）、全国年金保険金庫（CNAV）、家族手当金庫、預金・ローン金庫、農業相互保険金庫、社会保障家族手当保険料徴収連合（URSSAF）、法律・行政情報総局、公共財政総局　等
- MSP経由での手続き数が多いのは、家族手当、医療保険、税金。2014年には1200万件の所得税申告がMSP経由で実施
- 第一段階はこれら全国レベルの機関との提携。2011年以降、第二段階として県のレベルの機関との提携を進めている。

② 利用者向けのストレージスペース:

- 電子文書・所得税申告証明書等を保存したり、これらを行政機関等に送信することが可能。
- 個人データの登録により、フォーム入力を自動化できる。必ずしも全てのデータ項目を入力しなくてよい。自動入力機能を選択せずに、自分で入力することも選択可能。

③ 利用者によるコントロール、利用者視点:

- 自己決定権（アカウントの開設、ストレージスペースの利用、ストレージスペースでの公文書の受け取り等は全て任意）。
- ライフイベントに基づく、パーソナライズされた手続きの提供。自分が受けられる手続きの一覧が分かる。
- 手続きの進捗状況を確認できる。自分のインボックスや携帯電話で進捗状況を受信できる。この機能の実現には、提携機関からの情報提供が重要な点である。

フランスMSP： MSPへの利用者登録

- MSPに利用者登録（アカウント開設）し、ID/PWを取得する。MSPアカウントを作成すると、フォームへの個人データ自動入力が可能になる。また、他の機関のIDとのリエゾン（紐付け）を行うと、以降はシングルサインオンが可能になる。
- MSPから医療保険サイトへのアクセスは、①リエゾンでアクセスすることもできるし、②医療保険サイトで新たにログインすることも可能である。
  - ①の場合、リエゾンの登録に当たって、追加の情報が必要である。
  - ②の場合、その都度、NIR（国民登録番号）と医療保険サイト用のパスワードを入力する。
- 利用者登録に至るパターンとしては、行政手続きのページにアクセスするとMSPの案内が表示されるため、MSPに登録して、MSPから当該手続きを申請し、MSP経由で手続きの途中経過を確認する、というものである。
- 税申告のように毎年、定期的に利用する行政サービスでは、MSPに登録した方が便利。他方、引越しの手続きは単発のものであり、MSPへの利用者登録がブレーキになってはいけないので、MSPアカウントを作らずに手続きを進めることを認めている。
- MSPの利用者ターゲットは個人である。その他に、NPOや自営業者も利用できる。NPOの利用は多いが、自営業者の利用はそれほど多くない。

フランスMSP： MSPの提供サービス

- 前述の提携機関へのシングルサインオン、提携機関でのサービス
- 引越しワンストップ（Je change de coordonnees）
  - 現在、利用が最も多い手続きは引越しワンストップ（住所変更）である。
  - 公的機関以外にも、民間の電力会社やガス会社に通知することも可能。引越しする人の3人に1人がMSPを利用。
- 自治体サービス
  - 選挙有権者登録、兵役登録、住所変更（引越しワンストップ）、戸籍抄本・謄本の発行申請、国勢調査対象者登録（16歳以上）等
  - パリ警視庁のサービス：バカンスシーズンの自宅見回り、落し物登録
- 手続きのタイプは、1機関が手続き先の場合と、複数機関が手続き先の場合がある。例えば、新車購入時の手続きは内務省だけが対象だが、引越し時の住所変更手続きは15の提携機関が対象となる。ただし、どの機関に対して住所変更を行うかは個人が選択できる。

フランスMSP： 自治体との関係

- 自治体からの参加希望が多い。自治体は住民にとって最も身近なサービスを提供しているので、オンライン化による効率化の余地が大きい。
- MSP側から自治体に、こんなサービスが提供可能だというパッケージを見せる。戸籍抄本・謄本の発行申請や、住所変更届け、選挙有権者登録、兵役登録などである。
- 利用者は、郵便番号を入れるとその自治体でどんなサービスが使えるかを見ることができる。
- 有権者登録は毎年10月に登録が必要なので、利用頻度が高い。全3万6000のコミューンのうち、4500コミューンがMSPの有権者登録機能を利用。主に小規模の自治体がMSPの提供機能を利用しており、大都市の場合はMSPから当該自治体ポータルにリンクを張っている。
- 2012年以降、自治体との提携を強化している。既存の自治体ポータルへも、全国規模の提携機関と同様、MSPからシングルサインオンでログイン可能である。
- 自治体から見ると、医療保険などの利用者が多いので、MSPの利用者が自治体ポータルに流れることのメリットが大きい。自治体はeサービスの期待が大きい。MSPという国のサイトへの期待が大きいのは、フランスが中央集権国家であるため。
- MSPにとって、他機関や自治体と共存して繁栄することが目的。
- 有権者登録等、自治体のサービスがMSPの普及促進窓口ともなっている。

フランスMSP： MSPの課題

- 立ち上げ当初、広報が十分でなかった。
- 自治体が参加に積極的なのに対し、全国規模の機関は提携に難航する機関があった。
- 本人確認の問題。本人確認手段は色々な方針が検討されている。IDカードをチップ化する計画（電子IDカード：CNIE）はあるが、議論が進まず、頓挫している。CNIEを用いれば、本人確認の問題が解決される。
- 段階的に利用者数が増えているので、MSP側の人員確保が必要。

ドイツeIDカード： eIDカードの概要（1/2）

- 2010年11月から、既存の紙の身分証明書に替えて、順次発行。2014年6月現在、eIDカードの発行枚数は2000万枚（人口は約8000万人）。
- eIDカードは10年間有効。非接触型カード。16歳以上は身分証明書の所持義務あり。発行手数料は28.8ユーロ。
- eIDカードの3つの機能（それぞれチップ内で領域を分けている）

①実世界での身分証明書
  - 電子パスポート（2005年より発行）と同等の機能
  - 行政利用のみ（警察、入出国管理）・・・ただし電子行政サービスではない
  - 生体情報を格納（顔写真、指紋(オプション)）

②eID機能（オンラインでの身分証明書）： 認証機能
  - 氏名、学位、生年月日、出生地、住所、国籍、有効期限等の個人情報を格納
  - ID番号は格納しない。 生体情報は使用しない
  - 電子行政サービスやeビジネスで利用
  - 本人の希望でeID機能の有効化／無効化が可能

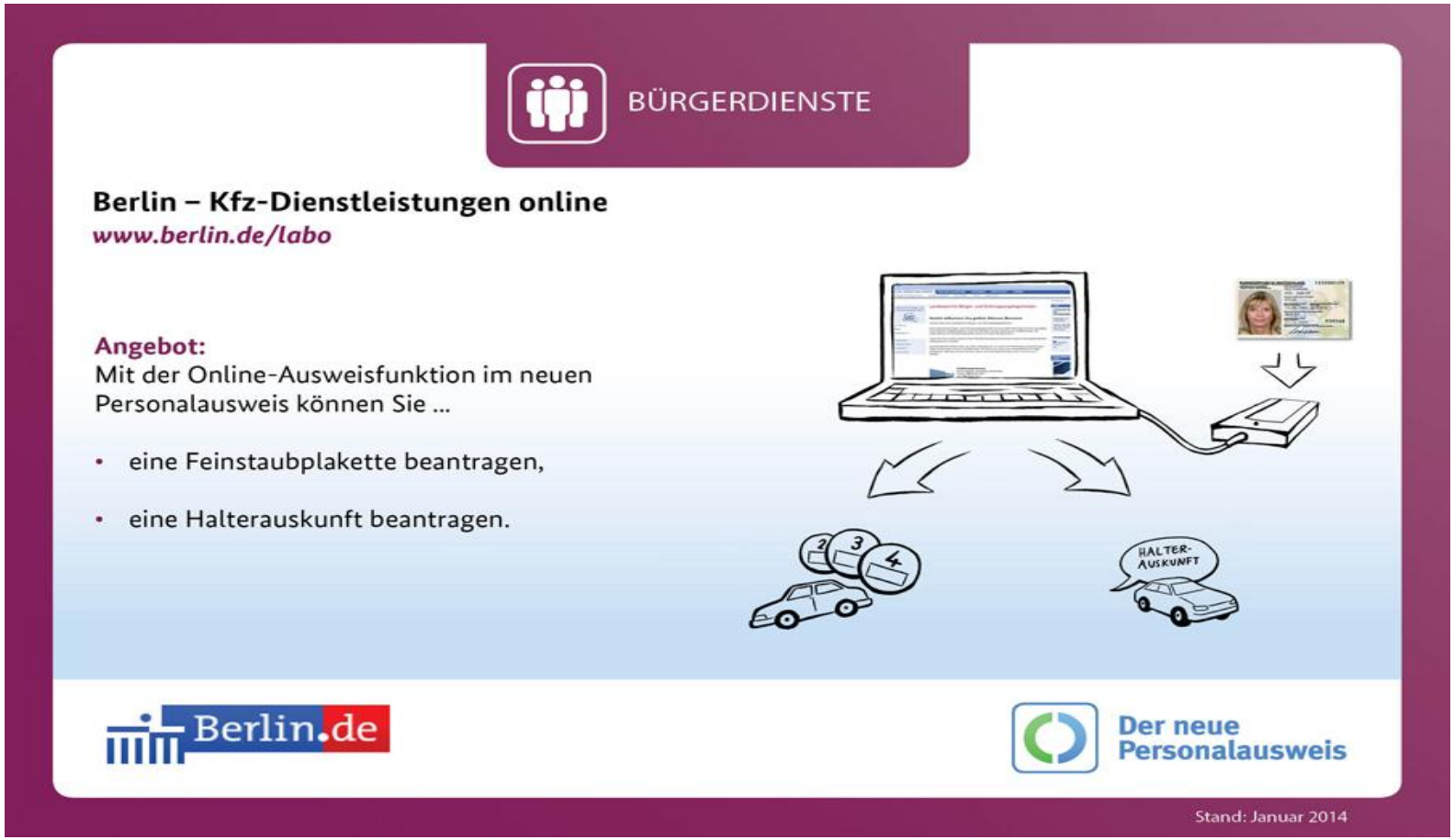
③電子署名（EU指令に準拠した適格な電子署名）
  - 本人の希望で搭載が可能

ドイツeIDカード： eIDカードの概要（2/2）

- eID機能（認証機能）をオンにしている人はあまりいない。eIDカード取得者のうち、eID機能をオンにしている人は4分の1である（約500万枚）。認証機能を何のために使うかが一般市民に伝わっていないため。
- バイエルン州のインゴールシュタット市では、eID機能をオンにしている利用者が多い。その理由は、eID機能を使えるサービスが多く、eID機能の認知度も高いためである。例えば、引越しサービスがある。完全に自動化はできないが、オンラインで届出ができるので、窓口で予めチップデータを用意しておいて、すぐにカード内容を変更することができる。また、eIDカードの券面には住所が書かれているので、住所変更時にはシールを貼っている。
- eID機能を用いた民間サービスとしては、eIDカード導入当初は、銀行、保険会社、債務情報サービスなどがサービス提供を始めたが、その後はあまり増えていない。

ドイツeIDカード： ベルリン州における取組み（1/2）

- 昨年から自動車関連の2つのサービスの実証実験を実施。
  - 車両ナンバーから自動車の所有者情報を検索するサービス
  - 排気ガス環境適合シール取得サービス：ベルリンなど大都市の市内に乗り入れるとき、排気ガス環境適合のシールがないと駐車できないが、その取得のためのサービス



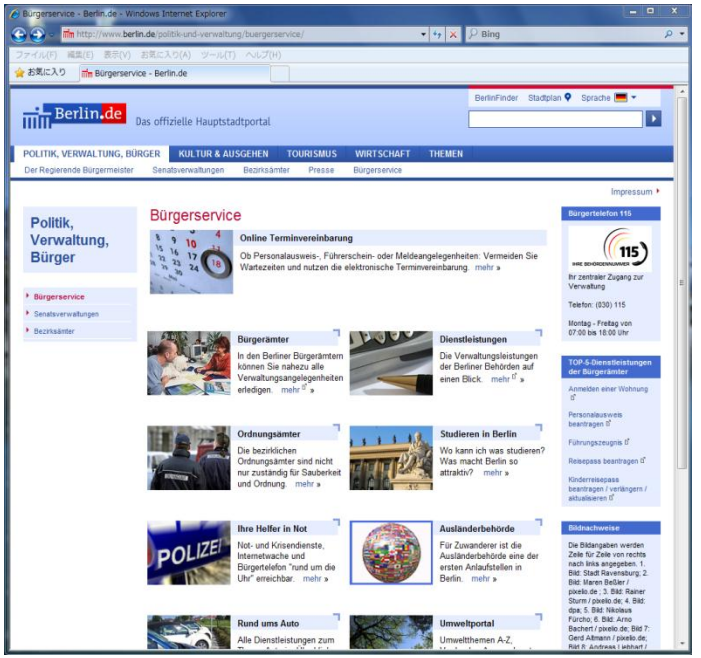
図の出典：http://www.personalausweisportal.de/

ドイツeIDカード： ベルリン州における取組み（2/2）

- ベルリン州（都市州）ではこれまでサービスが少なかったが、2014年7月1日から新たな法律が施行され、手書き署名の代わりに、電子署名を付した電子申請が利用可能になる。
  - また、この法律により、州の機関については州内務省がまとめて連邦行政管理庁にeIDカード内の個人情報へのアクセス許可申請を行い、許可をもらえることになった。従来、サービス提供者はeIDカードの中の氏名・住所・Pseudonymといったデータを使うために、個別に連邦行政管理庁の許可をもらう必要があった。同法によって、ベルリン州の全ての機関がeID機能を用いたサービスを提供できるようになった。
- 近い将来には、インゴールシュタット市のような半自動の引越しサービスの提供を希望。ただ、担当課の資金と人材が足りない。どの行政サービスから優先的にオンラインで提供するかは件数で判断するが、ベルリン州では引越しは年間60万件ある。
- これまでの行政手続きでは不要なデータまで申請書に記入させたり、手書き署名を要求したりしていたが、これを減らそうとしている。例えば民間企業のサービスでは登録手続きが煩雑だと利用者は離れる。手続きが簡単であれば、利用のハードルが下がり、それだけ利用のインセンティブが増えるとのこと。

ドイツeIDカード：ベルリン州ポータルberlin.deと「市民アカウント」

- ベルリン州ポータルberlin.deに7月以降、電子申請のためのメニューを付加する予定。
- また2014年9月以降、「市民アカウント」や「企業アカウント」を開設予定。
  - データ保存：税については既に同様なサービスが存在
  - 自分が申請した手続きの進捗状況の確認
  - シングルサインオン、ワンストップサービス
    - 医療保険組合（疾病金庫）等との連携を予定
    - 将来的には、他サービス間、地域間でも連携も計画



図の出典：http://www.berlin.de/

- ベルリン州が先行的にアカウントサービスを開設し、他の州との連携も予定。ただ、或る州から他州への引越し時にデータが移されるわけではない。フロントは1つの入り口にして利便性を高め、バックエンドで個別のサービスを提供するための共通仕様を策定する。
- 市民アカウントの認証にあたっては、eID機能、電子署名、De-mailの認証手段の3つから本人が認証手段を決められる。これらの認証手段を持たない利用者のために、最初はPINやTAN（ワンタイムパスワード）も用い、複数の選択肢から選べるようにする。

ドイツeIDカード： eIDカードの利用普及策

- 連邦では、以下の3つの利用普及策を実施
  - ①カードリーダーの普及による技術的利用可能性の拡大。展示会等でカードリーダーを無料配布。
  - ②システムに対する市民の信頼性向上。テストアプリケーションを配って、カードの中のデータを本人が見られるようにする。国でテストアプリを作ったが、やや失敗した。新しいOSに対応させるのに開発が間に合わなかった。
  - ③利用サービスの拡大。これら3つの要素のうち、最も大きいのは③の利用サービスを増やすことである。

- 連邦でのその他の検討
  - eIDカードにNFCを組み込むことにより、非接触で読み取り可能になる。現時点では搭載されていないが、今後の新世代カードに搭載されそうである。携帯端末でNFC機能を搭載しているものは少ないが、今後は増える見込み。
  - 職業上の公的資格を証明する機能をeIDカードに搭載することも検討されている。弁護士、公証人、医師、企業における役職等である。例えば、ある会社の役員に会社の署名をする権限があるか等を、eIDカードで確認できると便利である。まだ構想段階で、いつ実装されるか時期は分からないが、カードにこうした資格機能を組み込むことで利便性を高められる。

【ご参考】 EUのeIDAS規則案について

- 2012年6月4日、欧州委員会がeID・トラストサービス（eIDAS）規則案を公表。2014年4月3日に欧州議会が議会案を採択。同年7月23日に欧州連合理事会も議会案を採択。
  - eIDAS（アイダス）規則案の正式名称は「Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market」。
- eID（電子的な国民ID制度）と、トラストサービス（電子署名、電子シール、タイムスタンプ、電子送達サービス、サイト認証）に関するもの。
  - eIDの相互認証を通じて、EUの他国でも公共サービスにおいてeIDカード等が利用可能になる。この枠組みに参加するか否かは加盟国の任意だが、欧州委員会は多くの加盟国の参加を希望。加盟国にeIDの導入を強制したり、欧州規模のeIDやデータベースを導入するものではない。
  - また、従来の電子署名指令（1999年）を置き換える。電子署名指令に基づく各国の国内法が異なったため、EU域内で国境を越えた電子取引を行うことが困難だった。規則に格上げすることにより、電子署名を含むトラストサービスの共通ルールを設定する。
- eIDAS規則によって実現されるサービス事例は以下。
  - EUの他国の大学にオンラインで願書を提出できる。
  - EUの他国への引越し手続きや他国での結婚手続き、他国での税還付申告ができる。
  - EUの他国での診療が必要な場合、オンラインで医療記録を確認したり、医師に医療記録を閲覧させたりできる。
  - 企業は、EUの他国での公共調達にオンラインで入札できる。
  - EUの他国で起業したい人は、オンラインで会社登記を行える。

ポーランド pl.ID： pl.IDの概要

- pl.ID programmeは2013年2月に開始された電子政府プロジェクト。2009年～2012年のpl.ID projectの後継プロジェクトである。pl.ID projectのうちIDカードの電子化のみが中止になったが、他は継続。
- pl.ID programmeの内容
  - 中央住民登録台帳の構築
  - 住民基本データの連携基盤の構築
  - PKIの整備
  - IDカードのパーソナライゼーションの近代化（印刷機器の更改等）
  - 電子IDカード事業の中止
- pl.ID programmeの主たる目的は、住民登録台帳（出生登録）、IDカードの登録DB、結婚・死亡登録DBをPESEL番号（後述）で連携させることで、住民ステータスを確実に確認できるようにすることである。これら3つの基本DBは別々のDBであるが、オンラインで住民の基本データを照会可能となる。
- また、教育、医療、税等の登記簿（DB）についてもPESEL番号を利用可能とすることで、全ての行政機関や自治体が法律に従って基本DB上で住民ステータスを確認できるようになる。例えば、住民の基本データの更新時（姓変更等）にこれらのDBに異動情報が送信されるが、基本データ以外（納税データ、医療データ等）を他の機関がオンラインで照会できる訳ではない。（すなわち、PESEL番号に基づくバックオフィス連携の範囲は、住民の基本データに限定されている。）
- 住民の基本データの照会に当たっては、PESEL番号が利用される。

ポーランド pl.ID： IDカード

- 18歳以上のポーランド国民にはIDカードの取得義務がある。
- IDカードは10年間有効。
- IDカードの裏面には、PESEL番号（後述）も記載されている。
- 内務省のITプロジェクトセンターで2009年からpl.ID projectの一環としてIDカードの電子化が検討され、2013年末までに実用化する計画となっていたが、2012年4月に電子化計画が中止された。今後の電子化は未定。

図の出典：Wikipedia

ポーランド pl.ID： PESEL番号（1/2）

- PESEL（電子住民登録台帳）番号は1979年に導入。PESELは共産主義政権の下で住民の個人情報を追跡するためのシステムだったが、1989年の民主化以降もPESEL番号を利用。
- 出生時に付番される番号。IDカードの裏面にも記載される。子どもには、親にPESEL番号証明書が渡される。利用範囲は法律で定められている。
- 付番対象者
  - ①ポーランド国民　※在外ポーランド人がパスポート申請をする際にも必要
  - ②ポーランドに3か月以上在住する外国人
  - ③ポーランドの社会保障を受ける外国人
- PESEL番号は11ケタの番号。初めの6ケタは生年月日を表す。性別を表すケタもある。
- 公共機関がPESEL番号や個人データを利用したいときは、個人データ保護法を遵守しなければならない。保護法を遵守していれば、公共機関はこれらのデータを使うことができる。また、法の規定がなくても、本人同意があれば使うことができる。
- PESEL番号以外には、パスポート番号やIDカード番号がある。これらは、証明書に付された番号であり、更新時には別の番号になる。他に納税者番号（NIP）もあるが、一般的に使われるのはPESEL番号である。NIPは以前は所得税を払う全ての国民に付番されていたが、2011年以降は自営業者や法人のみに付番されている。一般の人はNIPの代わりにPESEL番号を用いる。
- パスポート、IDカード、教育、医療等の申請時にはPESEL番号を記入するので、これらのDBではPESEL番号を保有している。

ポーランド pl.ID： PESEL番号（2/2）

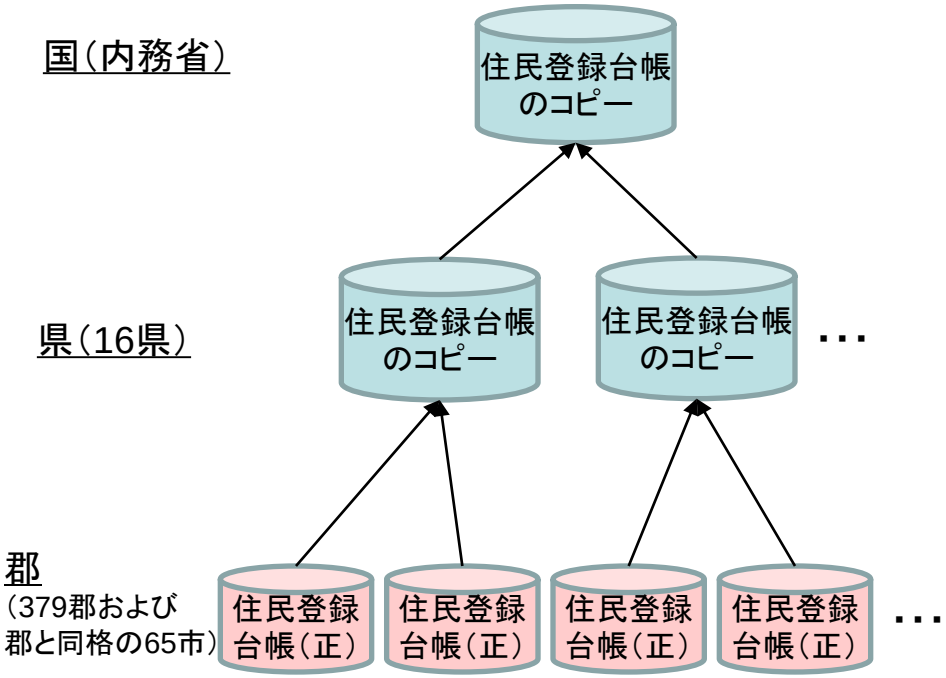
- PESEL番号の民間利用には以下の2通りがある。
  （1）法律の規定に基づき、民間企業にPESEL番号利用の必要性が認められ、内務省（大臣）が許可する場合。
  （2）本人同意の上でのPESEL番号の取得。銀行口座や電話の開設時に、IDカードをコピーする場合等。
- 民間企業は（2）の場合に、本人同意の上で取得したデータに基づき、住民基本データ（住民ステータス）の確認を行うことができる。内務省から民間企業に出向いてデータが正しいか否かを確認し、Yes/Noを回答する。民間企業から内務省にPESEL番号を送るのではない。
  - 例えば、ローンの申請時に提示されたIDカードのデータを、内務省で現在も有効なデータかどうかを確認し、Yes/Noを回答する。それ以外のデータを民間企業に提供することはない。
- 民間企業が内務省からPESEL番号利用の許可をもらう（1）は稀なケースであった。ただ、2015年1月以降は、銀行等は内務大臣の許可があれば、住民登録台帳をオンラインで照会できるようになる。この場合、必要なデータ項目のみ照会可能である。照会は有料であり、料金は法律上、1件当たり約30ズォティ（約1000円）である。

ポーランド pl.ID： 住民登録台帳の中央化（1/2）

- 住民登録（出生登録）は現在、郡で行っている。郡から県、県から中央政府へ登録内容のコピーが送信される。
- 住民登録の情報項目は住民登録・身分証明書法で決まっており、誰がこのデータを取得できるかも同法できまっている。PESEL番号も含まれる。
- 2015年1月からは郡で取得した住民登録データが直接、郡から中央政府に送信され、中央政府の台帳に登録され、中央政府で管理するようになる。すなわち、2015年1月以降は、内務大臣が住民登録台帳の管理者になる。県では中央政府の台帳を照会するようになる。
- 将来的には中央政府の住民登録台帳しか残らないが、2015年時点では郡の台帳が残る。これは郡に既存の行政機能があり、 住所登録の事務等があるためである。ただし、2016年から居住地（郡）での住所登録の義務自体を廃止するので、これに伴い、郡の住民登録台帳もなくなる。
- 住民登録台帳を中央化するのは、行政事務を簡素化・効率化するためである。従来は住民登録に郡→県→中央政府という3段階が必要であり、郡から県を経て中央政府にデータが届くまで2～4週間かかっている。今後は住民登録データが中央政府にすぐに届くように、また他の機関がそれをすぐに使えるようにする。
- 今回の中央化に伴い、新たに追加されるデータは、出生国、現居住国、最後のパスポートデータである。

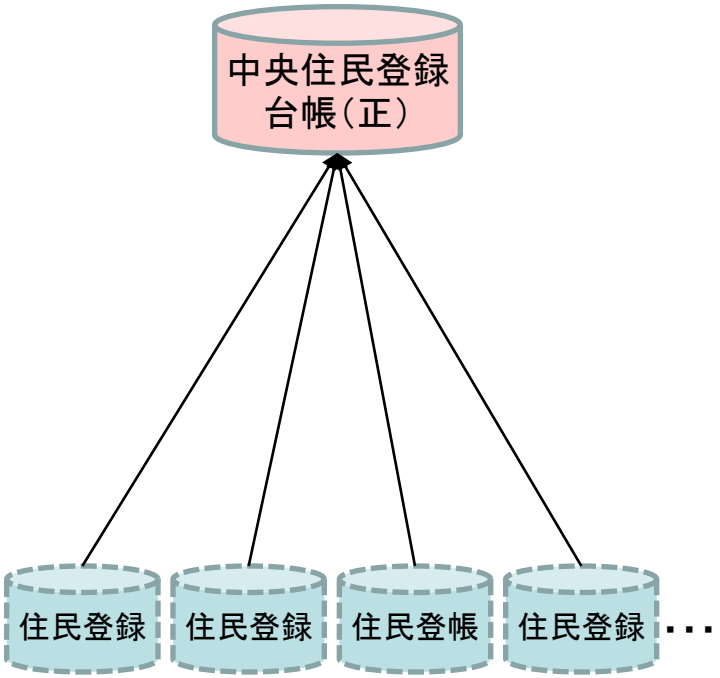
ポーランド pl.ID： 住民登録台帳の中央化（2/2）

○現状の住民登録



※郡の下に市町村（2479団体）あり。

○2016年以降の住民登録



※住民登録事務は引き続き郡が行うが、2016年以降は郡で台帳のコピーも保有しなくなる。