野村総合研究所

第2回情報法制研究会

国際標準化の現場から見た日本の個人情報保護法改正

～情報セキュリティ／プライバシーと国際標準～

2015年06月28日

株式会社野村総合研究所　上席研究員
ISO/IEC SC27/WG5 アイデンティティ・アクセス管理とプライバシー保護技術国内小委員会主査

崎村　夏彦

〒100-0005
東京都千代田区丸の内1-6-5 丸の内北口ビル

国際標準化団体で策定される任意規格

- 強制規格　⇔　任意規格
- 国際標準化団体の条件
  - WTO TBT協定（http://j.mp/wto-tbt ）で定義(Annex 1, 2, 3)
  - 参加に地域制限が無いこと（オープン参加）
  - 策定された規格にはだれでもアクセス可能であること
  - コンセンサスベースであること
  - 規格策定にあたっては、60日以上のコメント期間を設けること
  - Etc.
- 代表例：ISO, IEC, (ISO/IEC JTC1), ITU
- 他の例：IEEE, ETSI, OASIS Open, OpenID Foundation など
- 「地域標準」：ANSI, JIS
- 「フォーラム標準」「オープン標準」: IETF, W3C

ISO/IEC JTC 1/SC 27/WG 5
Identity management and privacy technologies

SC27

Participating countries: 51
Observing countries: 20

- ISOは本来産業界のあつまりだが、SC 27/WG 5は、当局からの参加も多い。
  - フランス：CNIL
  - カナダ：Office of the Privacy Commissioner
  - 英国：Cabinet Office
  - 米国：NIST
  - NZ: Ministry of Interior
  - 29条委員会 … etc.

官民の
コンセンサス形成

プライバシー関連規格

規格化済	ISO/IEC 29100 プライバシー・フレームワーク
	ISO/IEC 29101 プライバシー・アーキテクチャ・フレームワーク
	ISO/IEC 27018 PII処理組織としてのパブリック・クラウドにおけるPII保護行動指針
策定中	ISO/IEC CD 29134 PIA フレームワーク
	ISO/IEC CD 29151 PII保護行動指針
準備中	NP xxx プライバシー強化のための非識別化技術
	SP オンライン通知と同意
	SP プライバシー・エンジニアリング・フレームワーク
	SP 匿名属性確認
	SP プライバシー強化アイデンティ管理方式

日本の産業界は何を要求しているのか？わかってないんじゃないか？
国際的なところからずれてるんじゃないか？

（出所）鈴木正朝教授twitterプロフィール画像

ISO/IEC 29100 のPII（個人情報）の定義

- **2.9**
- **personally identifiable information PII**
- any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal
-
- その情報が(a) 関係する本人を識別するのに利用可能か、(b) 直接・間接的に本人に結び付けられる任意の情報

- **2.6**
- **identify**
- establish the link between a personally identifiable information (PII) principal and PII or a set of PII

- 本人と個人情報（PII）の結びつきを確立する

⇒　かなり広い定義

4.4 個人情報（PII）の認識（見つけ方）

保護の対象となる個人情報をあぶり出すやりかた～何に気をつけて探すか。

- 4.4.1 識別子
  - 個人に与えられた識別子（例：マイナンバー）を含むかそれに結び付けられた情報
  - 個人に関係する識別子（例：パスポート番号、口座番号）を含むかそれに結び付けられた情報
  - 個人に連絡をつけることができる識別子（例：地理的位置、電話番号）を含むかそれに結び付けられた情報
  - 上記の識別子に結びつけることができるような参照を含む情報
- 4.4.2 その個人を他の個人から区別し得る性質
  - テクニカルには、これも（準）識別子
  - 例：生体情報、基本4情報、行動履歴 etc.
- 4.4.3 本人にリンクされた、あるいはリンクされ得る情報
  - たとえ個人を識別できなくても（$k > 1$）、その情報が自然人について何か語っている場合、個人情報として取り扱うべき。
  - （例えば、その母集団の8割ががん患者という集合に当該個人がその母集団に入っているということが分かるだけで、プライバシーインパクトが有る～いわゆる l 多様性の問題。）
  - 例：医療記録、金融プロファイル、インターネット利用記録から生成した趣味嗜好。
- 4.4.4 仮名データ
- 4.4.5 メタデータ
  - 例：MS Officeのメタデータ、写真のEXIFデータ
- 4.4.6 （頼んでないのに送りつけられた）個人情報
- 4.4.7 より注意を要する（sensitive）個人情報

欧米の個人情報の定義はもともとかなり広い

- EU Data Protection Regulation案/Article 4/(2)
  - 'personal data' means any information relating to a data subject;

（出所）http://j.mp/eu-dp-reg-2015 (2015/6/26取得)

- 米国消費者プライバシー権利章典法案(2015)/SEC.4/(a)/(1)
  - In General.—“Personal data” means any data that are under the control of a covered entity, not otherwise generally available to the public through lawful means, and are linked, or as a practical matter linkable by the covered entity, to a specific individual, or linked to a device that is associated with or routinely used by an individual, including but not limited to— ..

（出所）http://j.mp/us-cpbor2015 (2015/6/26取得)

リスクベースアプローチの徹底

4.7 プライバシー制御

- 情報セキュリティコントロールに関しては、すべてのPII処理が同じレベルやタイプの保護を必要としているわけではないことに留意することが重要である。（中略）リスクマネジメントはこのプロセスの中核をなす。また、プライバシー・コントロールの識別は、組織の情報セキュリティマネジメントフレームワークの欠かせない一部であるべきである。
  - （出所）ISO/IEC 29100 4.7 Privacy Controls Paragraph 3

- ちなみに、OECDプライバシー・ガイドライン(2013)も「RECOGNISING the importance of risk assessment in the development of policies and safeguards to protect privacy; 」などに現れるようにリスクベースアプローチ。今年の秋出る予定のセキュリティガイドラインも同様。

リスクベースアプローチ

- EUデータ保護規則案/Section 2 data SECURITY/Article 30 Security of processing
  - 1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.

（出所）http://j.mp/eu-dp-reg-2015 (2015/6/25)

  - 1. コントローラとプロセッサは、個人データの性質と処理によって出現するリスクに応じて、適切な技術的および組織的手段を、最新の技術とその実装コストを勘案した上で実装しなければいけない。（崎村訳）

- 米国消費者権利章典法案（2015）/SEC.105/(b)/(1)
  - (1) The degree of the privacy risk associated with the personal data under the covered entity's control;

（出所）http://j.mp/us-cpbor2015 (2015/6/25)

- 個人情報保護法
  - （安全管理措置）
  - **第二十条**　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

処理が許可される条件

- 処理が許可される条件の規定が日本法と違う。
- **ISO/IEC 29100「5.3 処理の目的の正当性(legitimacy)と特定」**
  - 英国:
    - Conditions for Processing (Data Protection Act (1998))
  - EU Regulation案:
    - Article 6 Lawfulness of processing [1]
  - 米国プライバシー権利章典法案:
    - コンテキスト

必要

(a) 本人同意がある場合
(b) 処理が以下の理由で必要である場合
- **本人が結んだ契約を実施するのに**
- **本人が契約を結ぶにあたって要求したことを実施するのに**

(c) 法順守のために必要な場合
(d) 個人の身体生命を守るのに必要な場合
(e) 法執行に必要な場合
(f)「正当な利益(Legitimate Interest)」条件にしたがって処理する場合

- **ISO/IEC CD 29134 PIAフレームワーク**

[1] http://j.mp/eu-dp-reg-2015 accessed June 26, 2015

サイバーセキュリティ関連情報の除外：日本での実現方法は？

- サイバーセキュリティ情報交換推進大統領令
  - http://j.mp/us-eo-2015-is
  - OASIS CTI WG
    - 米国政府が中心になって組成。MITREのSTIX, TAXIIなどを標準化
  - OIDF RISC WG
    - Google, Facebook, Microsoft, Linkedin, Paypal, twitter, etc. が組成。
    - 特にアカウント情報についてリアルタイムで共有・対処する
- 当然、明示的同意なしに個人情報を交換・共有することになるが…
- 米国消費者権利章典法案（2015）/SEC.4/(a) Personal Data/(2) Exceptions/(D)
  - Cybersecurity data.—The term “personal data” shall not include cyber threat indicators collected, processed, created, used, retained, or disclosed in order to investigate, mitigate, or otherwise respond to a cybersecurity threat or incident, when processed for those purposes.

（出所）米国消費者プライバシー権利章典法案 http://j.mp/us-cpbor2015 (2015/6/25)

- EU:「**本人が結んだ契約を実施**」「**Legitimate Interest**」で対処？
- **日本は？**
  - **アカウント内にたまっている情報は「財産」にはならないから、23条第1項二は適用できないのではないか？**

匿名加工情報～De-identified Data?

- 今回の改正のもう一つの目玉
- 米国消費者プライバシー権利章典法案では、De-identified DataはPersonal Dataから除外
  - /SEC.4 DEFINITIONS/(a) Personal Data/(2) Exceptions.—

(A) De-identified data.—The term “personal data” shall not include data otherwise described by paragraph (1) that a covered entity (either directly or through an agent)—

(i) alters such that there is a reasonable basis for expecting that the data could not be linked as a practical matter to a specific individual or device;

FTC法5条との関係

(ii) publicly commits to refrain from attempting to identify with an individual or device and adopts relevant controls to prevent such identification;

(iii) causes to be covered by a contractual or other legally enforceable prohibition on each entity to which the covered entity discloses the data from attempting to link the data to a specific individual or device, and requires the same of all onward disclosures; and

(iv) requires each entity to which the covered entity discloses the data to publicly commit to refrain from attempting to link to a specific individual or device.

（出所）米国消費者プライバシー権利章典法案 http://j.mp/us-cpbor2015 (2015/6/25)

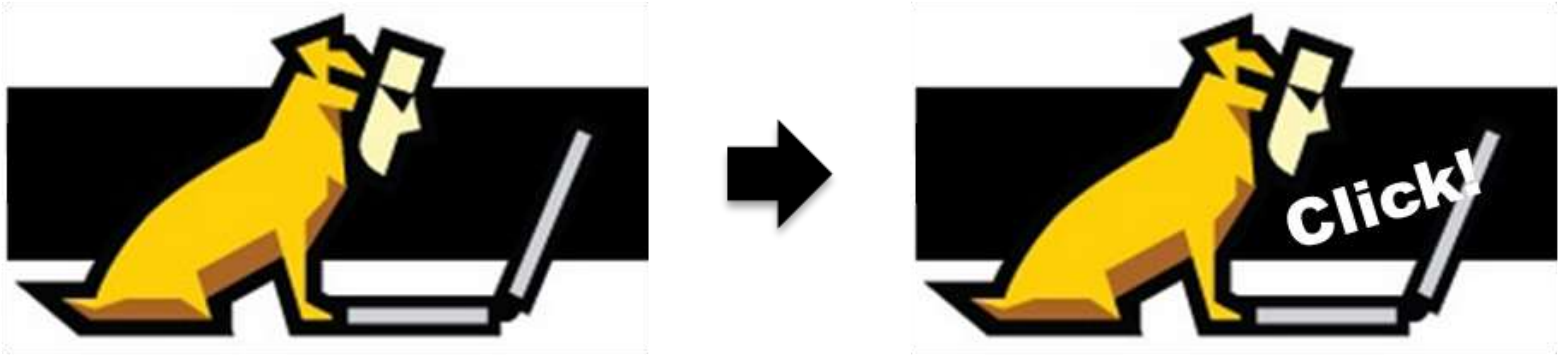
個人情報保護委員会規則で定める基準

V.S.

ISO/IEC NP XXXXXX プライバシー強化のための非識別化技術

同意取得の課題

- 処理に対する同意をどのように取っていくのか？
- わかりやすさの問題
- 「インターネット犬」→「パブロフの犬」転換問題



（出所）http://nat.sakimura.org/2013/03/01/explicit-consent-turning-internet-dog-into-pavlovs-dog/

- 同意取得タイミングの問題
  - IoT時代の「取得してしまう情報」に対する同意の問題
  - MACアドレス etc.

SP オンライン通知と同意

最後に…

規格化では無いが、エコシステムで欠けているものとして気になっているものが…

- 個人情報不正処理保険 （事業者向け）
  - 個人情報漏洩保険はあるが、限度額が低い
  - 例：東京海上日動「個人情報漏えい保険」

項目	支払限度額	免責金額
賠償責任部分	1請求・保険期間中[*1] 500万円～10億円	1請求 0円～1,000万円
費用損害部分	1事故・保険期間中[*2] 100万円～1億円 （ただし、賠償責任部分の支払限度額と同額以下での設定となります。）	1事故 0円または10万円

20万人以上の漏洩はカバーされていない

（出所）http://www.tokiomarine-nichido.co.jp/hojin/baiseki/roei/ 2015/6/26取得

- なりすまし被害(Identity Theft)保険 （個人向け）
  - クレジットカードの不正利用対策の保険などはあるが…。

まとめ

- 個人情報の範囲は広く取るのがトレンド。その処理に対してはリスクベースアプローチをとって適切な保護を行う。
- 産業界的には、個人情報の範囲を狭くするのではなく、処理が許される範囲を求めて行ったほうが良かったのでは？
- Legitimate Interest を求めていくには、先送りにしたPIAの導入が不可欠。
- サイバーリスク対応の個人情報の共有を、日本法の中でどう立てつけるのかは問題。
- 匿名加工情報の作り方は、国際的な整合性も必要。ISOで規格化が始まるので、個人情報保護委員会も参加を！
- 同意の取り方は、表示、通知、タイミング等、もっと工夫が必要。
- 残存リスクの共有～保険がきちんと機能するように、政策的に善導していくことが必要。