

IoT時代のパーソナルデータの の活用と保護

国立情報学研究所
所長補佐／教授

佐藤一郎

Ichiro Satoh

自己紹介: 佐藤一郎

国立科学
博物館(上野)

- 国立情報学研究所・
アーキテクチャ科学研究系・教授
- 国立大学法人総合研究大学院大学・
複合科学研究科・情報学専攻・教授
- 内閣官房パーソナルデータに関する検討会
委員 & 技術WG主査、経済産業省産業構造審議会
商務流通分科会IT人材委員他

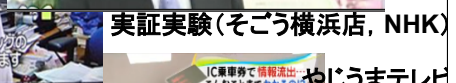
NHK週間ニュース深読み



ニュースゼロ(日テレ)



実証実験(そごう横浜店, NHK)



やじうまテレビ
(テレ朝)



実証実験(イトーヨーカドー, NHK)



o Satoh

自己紹介

- 本来は個人情報保護法よりも、組込向けのシステムソフトウェアの方が近い
- 軍艦島にセンサーネットワーク設営の手伝い



ESSと当方

10年ぶりに招待講演を
させていただきます

オブジェクト指向シンポジウム時代も
招待講演をさせていただいたはず

Ichiro Satoh: "A Testing Framework for Mobile Computing Software", IEEE Transactions on Software Engineering, Vol.29(12), Dec. 2003

ESS2005 (Embedded Software Symposium)

組込みソフトウェアシンポジウム2005

- 産学による組込みソフトウェア工学へのアプローチ -

日程: 2005年10月17日(月)~19日(水)

※ 17日は MDD ロボットチャレンジのみ実施(見学自由)

会場: 日本科学未来館: <http://www.miraikan.jst.go.jp/>

主催: 情報処理学会ソフトウェア工学研究会

■ 基調講演と討論

10月18日(火) 14:20-17:30

「モデル中心組込みソフトウェア開発 (MDD) が変える世界」

Branislav Selic (IBM)

-- UML2.0標準の父と呼ばれるリアルタイム組込みシステムエンジニア

Stephen Mellor (Mentor Graphics)

-- MDA の生みの親でトランスレーション技術界のリーダー

羽生田栄一 (豆蔵)

-- 情報処理学会 ソフトウェア工学研究会主査

■ 招待講演

10月18日(火) 12:30-14:00

「モバイル・ユビキタスコンピューティングのソフトウェア開発・試験手法」

佐藤一郎 (国立情報学研究所)

■ チュートリアル

・「低消費電力化ソフトウェア技術」

石原亨(九州大学), 富山宏之(名古屋大学)

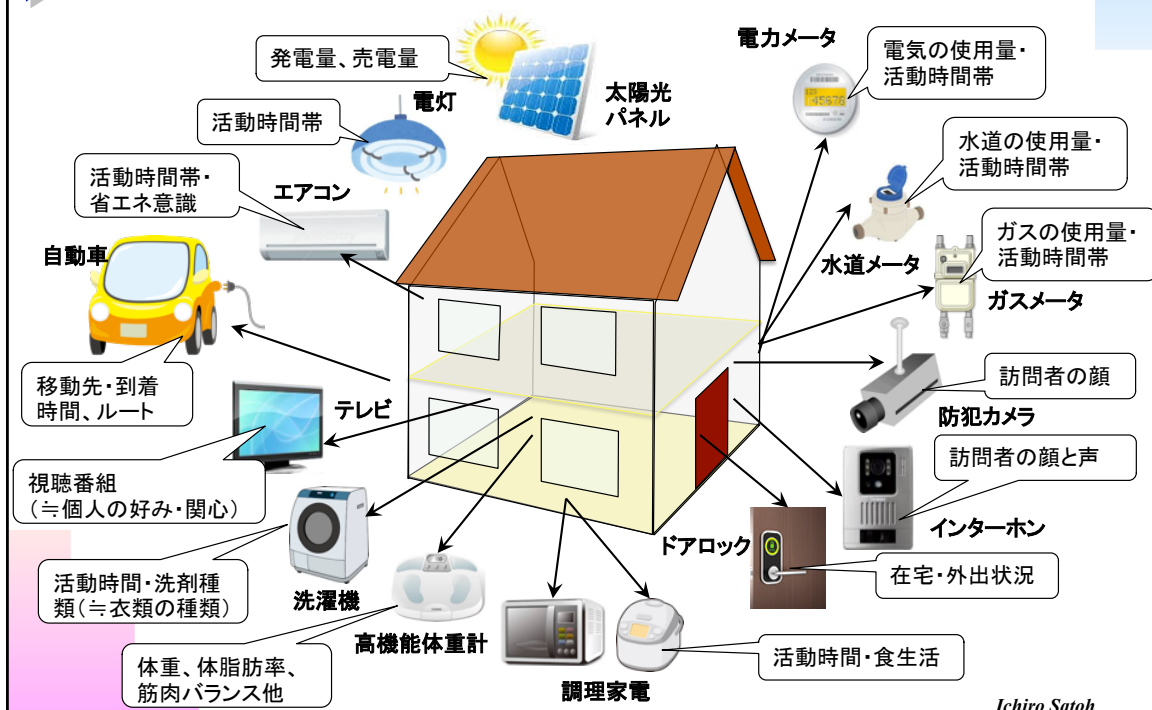
講演概要

1. IoTとパーソナルデータ
2. 用語整理
3. 個人情報保護法改正(2015年9月に可決成立しました)
4. 法改正とIoT
5. まとめ
6. 質疑応答

講演者の研究の話はしません

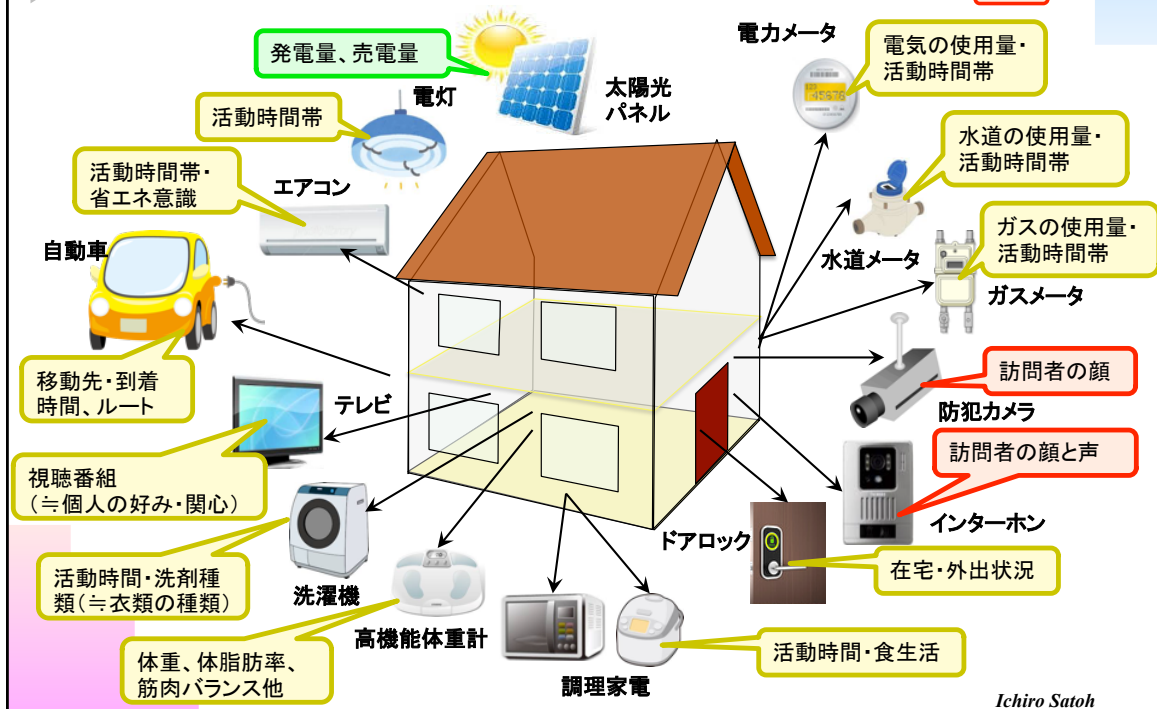
Ichiro Satoh

IoTで覗けるプライバシー(住宅)



Ichiro Satoh

IoTで覗けるプライバシー(住宅)



気がつくとプライバシー侵害

- IoTは多様な個人行動の捕捉や個人の識別を可能にする
 - 知らないうちにプライバシー侵害を引き起こすリスク
 - 例: 家電の利用履歴は場合によってはプライバシー
 - 法的、社会的な制約が生じる
 - 社会的批判根拠 ≠ 法律的問題
- 想定される問題
 - (結果としての)個人の特定と、それによる法的な問題
 - 情報による直接・間接のプライバシー侵害
 - 情報に関わるステークホルダー問題
- プライバシー侵害を含む、法的、社会的問題を解決しない限り、IoTの利用不可能
 - ひとつまちがうと顧客の信頼を失う
 - パーソナルデータは経営リスク



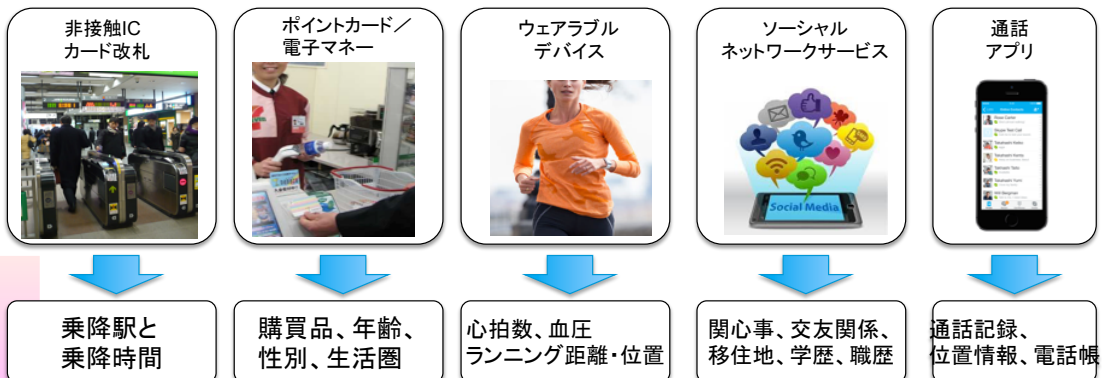
▶ 漏洩対策費として260億円特別損出計上



Ichiro Satoh

▶ ユーザ行動履歴の蓄積・活用

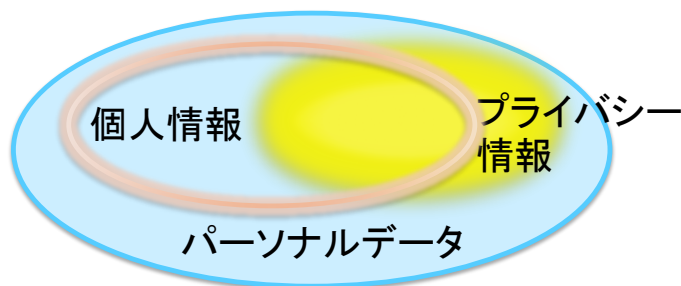
- ユーザ行動履歴から見てくること
 - 特定の個人の識別
 - 行動履歴から、どこに誰かがわかる(特定の個人の識別)
 - 個人のプライバシー
 - 個人の権利利益の侵害に関わる情報が見えてしまう



Ichiro Satoh

用語整理

- **パーソナルデータ**
 - 個人に関わる情報
- **個人情報**（個人情報保護法における定義）
 - 特定の個人を識別する情報（どこの誰なのかがわかる情報）
- **プライバシー情報**
 - 本人がプライバシーだと思う情報（明確な範囲は定義不能）



Ichiro Satoh

パーソナルデータの分類

- | | | |
|---|-----|--|
| <ul style="list-style-type: none"> ■ Volunteered data（自発的生成データ） <ul style="list-style-type: none"> ■ 個人が生成し、明示的に共有されるデータ <ul style="list-style-type: none"> ■ 例：ユーザ登録、SNSの書き込み | } → | 個人情報保護法の範囲
ただし、同法の対象は、特定の個人を識別する情報であり、プライバシーではない |
| <ul style="list-style-type: none"> ■ Observed data（観測データ） <ul style="list-style-type: none"> ■ 個人の過去の行動に基づくデータ <ul style="list-style-type: none"> ■ 例：乗降履歴、購買履歴 | } → | プライバシー侵害は個別対応
個人情報保護法改正では、観測データも個人情報の対象にはできなくはないが... |
| <ul style="list-style-type: none"> ■ Inferred data（推定データ） <ul style="list-style-type: none"> ■ 自発的生成データ及び観測データから、推定・プロファイリングされたデータ <ul style="list-style-type: none"> ■ 例：クレジットカードの与信情報 | } → | 法的には損害賠償による事後救済しかない。ただし、個人本人はデータの存在すら知らないで侵害が起きていても気がつかないことが多い |

法的な制約がなくても、社会的な批判を受ける可能性がある

Ichiro Satoh

▶ 現行法の問題：範囲の拡大・曖昧化

現行法の個人
情報の定義

- ①生存する個人に関する情報であり、
- ②当該情報に含まれる氏名、生年月日その他の記述等により、特定の個人を識別することができるものをいう（「識別性」）
- ③**他の情報と容易に照合**することができ、それにより特定の個人を識別することができるものも含まれる（「容易照合性」）
（個人情報保護法第2条第1項より）

- 技術進歩が個人情報の範囲を広げている
 - 照合対象の外部情報が増大、照合技術の高度化
 - 新しい情報が増えている
- 容易照合性の
範囲が拡大
(→個人情報の範囲の拡大)



政府見解 { 氏名到達は要件ではない(氏名不明でも特定の個人の情報とわかれば個人情報)
容易照合性は通常人による照合可能による個人の特定

Ichiro Satoh

▶ 個人情報の例

- 氏名や住所、電話番号など、直接、個人特定につながる情報
- 外部情報との突き合わせにより、個人特定につながりえる情報
 - 明確な基準はない
 - (誰かを知り得る人物が写った)顔画像
 - ある人物に関する深夜の位置情報
 - 氏名や組織名を含むメールアドレス
 - 履歴データも長期、詳細、最新なデータは個人情報になりえる
- 個人情報を利活用するには
 - 取得にあたって、目的、提供・利用する事業者を本人に示す
 - 目的外利用や第三者提供では本人同意が原則
 - 個人特定ができないように加工すれば、同意は不要
 - 法改正で、同意なしで第三者提供の枠組み導入

Ichiro Satoh

▶ 鉄道の乗降履歴から個人を特定できるか

- 乗降履歴
 - 利用者ID (ICカード番号)
 - 所定期間の乗車駅と時刻、降車駅と時刻
- 乗降履歴から個人を特定できるか
 - 同様履歴の個人が少数だと、外部情報照合による特定可能性は高まる
 - 乗降履歴で特定されるケース
 - 単体の情報から個人を特定
 - 同一の乗降区間の利用者が少数となる区間の利用
 - 長期的な履歴から個人を特定
 - ありふれた履歴でも長期になると該当者は少数化
 - 時刻情報は個人の特定に重要
- 利用者本人がプライバシー情報だと思えばプライバシー情報



Ichiro Satoh

▶ 購買履歴・ポイントカードから個人を特定できるか

- 日用品の購買履歴は個人の特定にならないが、特定できる場合も
 - 購入品の特殊性
 - 限定品などの購入と、購入に関する公開情報
 - 購入形態の特殊性
 - 購入数や時間に特殊性(毎週、決まった曜日に7個購入など)
 - 購入品の組み合わせの特殊性
 - 複数のありふれた商品でも、組み合わせに特徴がある
- 利用者本人がプライバシー情報だと思えばプライバシー情報
 - 思想信条に関する書籍など
 - 組み合わせにより、プライバシーは垣間見える
 - 例: カツラの購入と癌に関する書籍の購入→抗癌剤の服用

購買履歴は店舗名があるので、位置情報でもある

Ichiro Satoh

▶ 位置情報から個人を特定できるか

- ケースバイケースに判断すべき
 - 人口密度が低い地位域では位置情報は個人を特定されやすい
 - 都会と過疎地域では状況が大きく違う
 - 時間帯による人口変化に注意
 - 深夜の位置情報は自宅住所と考えられる(個人情報と扱うべき)
 - 新しい位置情報ほど、個人を特定されやすい
 - 現時点の位置情報は個人の特定につながりやすい
- 位置情報がプライバシーになるかは人による
 - 居場所を知られたくない人もいる
 - 例: DV被害から特定者から身を隠している

Ichiro Satoh

▶ ベネッセ漏洩問題

- 直接的被害
 - 漏洩した個人情報を直接利用した電話勧誘やダイレクトメールによる迷惑
- 間接的被害
 - 網羅的な個人情報は、部分情報の個人特定の突き合わせのベース
 - ベネッセからの漏洩情報には、1千万人分程度の子供の氏名、住所、生年月日、性別が含まれる

世間で注目されているのは直接的被害だが、
間接的被害の方が実害は大きいはず

Ichiro Satoh

ベネッセ漏洩問題の影響

- ベネッセからの漏洩情報
 - 1千万人分程度の子供の氏名、住所、生年月日、性別など
- ベネッセ情報の組み合わせを使うと、外部の部分情報から個人特定可能性が高まる
 - 80歳までの方がいたとして、生年月日と性別の組み合わせは
 - $365.25 \times 80 \times 2 = 58440$ 通り
 - ある地域の人数が上記より少なければ、**同一年月日と性別の持ち主は高々ひとりの可能性**が高くなる
 - 例: スーパーが顧客カードを配布し、登録時に生年月日と性別を記載
 - スーパーの顧客は特定地域に限定
 - 購買情報とリンクされていたら...
 - 例: ネットサービスで生年月日と性別を登録
 - ISP接続等で接続時にはIPアドレスには地域性
 - SNS上の匿名書き込みでも...
- 大量の個人情報漏洩により、個人特定可能性が高まる
 - 利活用できるパーソナルデータの範囲が狭まる

個人特定可能性は非常に高い

Ichiro Satoh

Appleのプライバシー重視戦略とその背景

あなたのプライバシーに関する
Appleの取り組みについて。
Tim Cookからのメッセージ

- Appleの声明(2014年10月)
 - プロファイリングしない、端末上の情報を売りにません、宣言

Appleにとって、あなたの情報は最も重要な資産です。だから私たちは、あなたのプライバシーを尊重し、強力な暗号化とすべてのデータの密い方を規定する厳格なポリシーによって、あなたのプライバシーを保護しています。

セグメント化プライバシーは、Appleのすべてのハードウェア、すべてのソフトウェア、そしてApple Payのような新しいものやCloudKitを含むすべてのサービスにわたって設計されています。そして私たちは常に改善を続けています。すべてのお客様におすすんでいる2ステップ確認は、あなたのApple IDのアカウント情報を保護します。しかもここ

私たちのビジネスモデルは明快です。素晴らしい製品を販売することです。私たちは、広告主に売るために、あなたのEメールの内容やネットサーフィンからプロフィールを作り上げることはしません。あなたのiPhoneや iCloudに保存されている情報を「換金」したりしないのです。あなたのEメールやメッセージを読んで、あなたに何かを売り込むための情報を集めることもありません。Appleのソフトウェアとサービスは、Appleのデバイスをより良いものにするためだけに作られています。わかりやすくシンプルです。

- GoogleのAndroidはGoogleにとって広告用看板であり、世の中を広告主に情報を売らない方向にむければ、Googleへの圧力
- 米国はパーソナルデータの取り扱いは、利活用から保護に急速に変化
 - 金が稼げるのは利活用より保護

Ichiro Satoh

▶ 個人情報保護法の改正(9月に成立)

■ 個人情報保護法の問題:

- 曖昧さ、技術進歩と合致しない、過度の萎縮、個人の不安……

■ ビッグデータ時代におけるデータ利活用の推進

- データ活用による新しいビジネスの創出
- プライバシー問題へ不安

■ データの国間流通の実現

- グローバルビジネスの推進
- 世界の標準にあったパーソナルデータ保護
- 安全管理措置

パーソナルデータに関する検討会と技術検討WGを設置

個人情報保護法の抜本改正

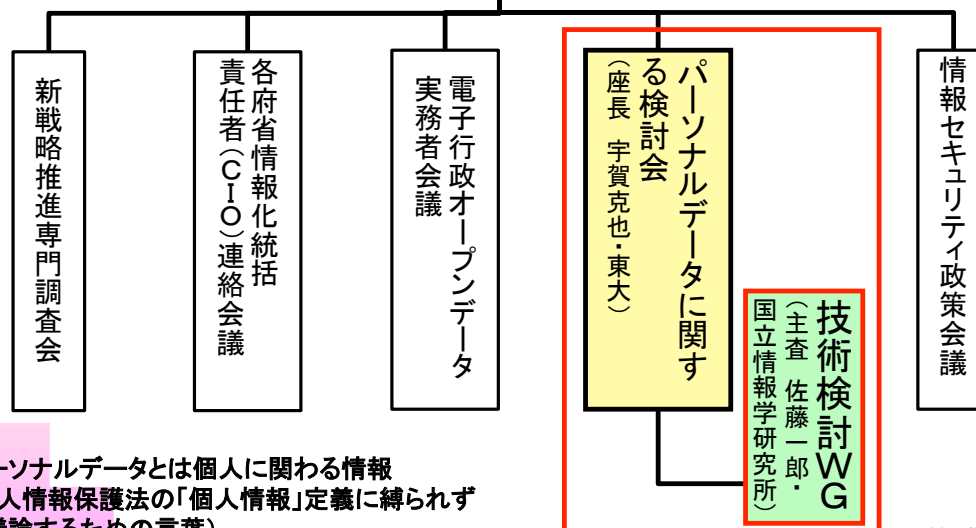
目標: 個人情報及びプライバシーの保護に配慮した
パーソナルデータの利用・流通を促進

- 透明性の確保と曖昧性の最小化
- 第三者機関の導入
- (同意不要な) 第三者提供
- 世界水準の保護

Ichiro Satoh

▶ パーソナルデータに関する検討会の体制

高度情報通信ネットワーク社会推進戦略本部
(IT総合戦略本部) (本部長: 内閣総理大臣)



Ichiro Satoh

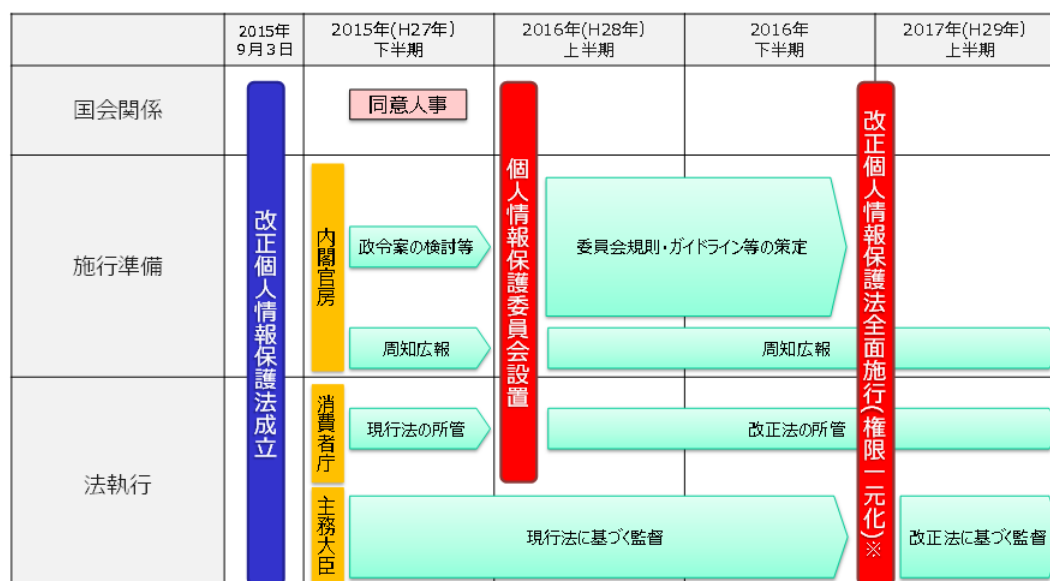
個人情報保護法改正の要点

(2015年9月3日に法改正成立)

- 個人情報の明確化
 - 従来の個人情報に「個人識別符号」を追加
- 要配慮情報を新設
 - 人種、病歴、犯罪歴などの記事情報は取得時に本人同意が必要
- 本人同意なく第三者提供するためのデータ類型を新設(匿名加工情報)
 - 個人の特定性が残っている情報を、提供元・先に個人の特定をしない条件で、本人に同意をとらなくても第三者提供可能にする
- 第三者機関による統一的な監視・監督
 - 所管府省庁に代わって個人情報保護委員会が事業者などの個人情報の取り扱いを監視・監督(立ち入り検査を含む)
- グローバル化への対応
 - 海外の個人情報の保護組織と捜査協力に必要な組織・制度

Ichiro Satoh

改正法の施行スケジュール(予想)

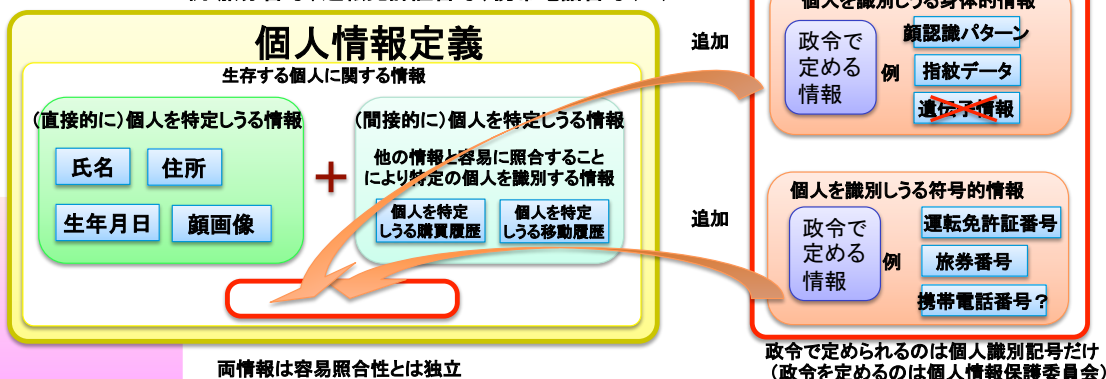


※「公布の日から起算して二年を超えない範囲内において政令で定める日」から施行。

出典：内閣官房 IT総合戦略室パーソナルデータ関連制度担当室作成資料を一部変更(2015年7月現在)

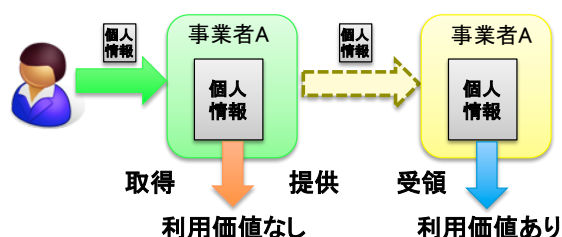
法改正：個人情報定義に個人識別符号を追加

- 従来の個人情報に、**政令で定める個人識別符号**を追加（容易照合性とは独立）
 - **身体的情報**：特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した符号であって、当該個人を識別することができるもの
 - 例：指紋データ、顔認識データ
 - **符号的信息**：個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、または個人に発行される書類に付される符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、または付されるもの
 - 例：旅券番号、運転免許証番号、携帯電話番号（？）



法改正：本人同意なく第三者提供するためのデータ類型を新設

- 個人情報を所有している事業者には利用価値のない情報でも、別の事業者には価値がある場合もある
 - 個人情報を第三者に売りたい（第三者提供）、しかし
 - 個人情報の第三者提供では、個人本人の同意が前提



- 一部事業者から、同意なしで提供したいという要望
 - 「第三提供＝利活用」という図式で法改正が進んだ部分も・・・
- 注意：業務委託と第三者提供の違いに注意

▶ ネットサービスのビジネスモデル

- **広告枠を広告クライアントに販売**(ユーザは広告の視聴者)
 - 広告を表示することで、広告主から広告料を稼ぐ
 - 例: 既存の多くの無料ネットサービス(Googleを含む)
- **サービスをユーザに販売**(ユーザが顧客)
 - 所定期間・回数・取得情報に応じてユーザから利用料をもらって稼ぐ
 - 例: ネットゲーム、新聞オンライン版、LINE(スタンプ)他
- **ユーザ情報を第三者に販売**(ユーザが商品)
 - サービスを通じてユーザに関する情報を収集し、その情報を売って稼ぐ
 - 例: Twitter、無料ヘルスケアサービス他

IoTで有効なビジネスモデルは？

Ichiro Satoh

▶ IoTとパーソナルデータの第三者提供

- 現状IoTではネット広告は成立しない
 - IoTにつながるのはデバイス
 - 広告効果はない
 - ネット広告を前提にした無償サービスに慣れきっている
 - IoTによるサービスにお金を払う人は少ない
- IoTで無償サービスを実現するには、
 - IoTサービスによる取得した情報を第三者に売るしかない
 - 高く売れる情報は、パーソナルデータ
- **ユーザ(の情報)を商品として売ることになる**
 - 高く売れるパーソナルデータは医療やヘルスケア
 - 高く売れるユーザしか、IoTサービスを利用できない可能性もある

Ichiro Satoh

ユーザが商品

- 例: 無料健康アプリの情報提供先
 - 保険会社などが含まれた場合、個人の権利・利益の侵害の恐れも
 - 就職活動で入社希望者の健康管理状況を事前把握も可能

事業者の要求

- 高く売れる情報が欲しい
 - 例: 医療など
- 高く売れることを阻害する規制はなくせ

個人にとって

- 自らの情報を事業者に渡すことで、結果としてサービスを得ている
- 如何に自分の情報を守りながら、サービスを楽しむか
- 如何に高い情報を提供できる個人になるか

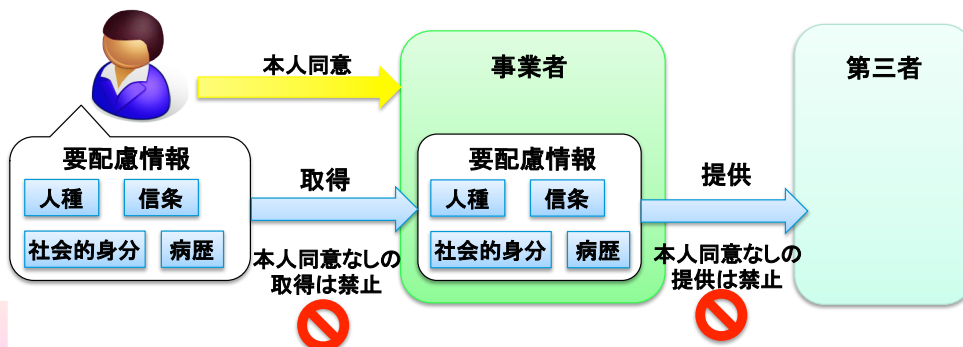


EVIDON
From : <http://www.evidon.com>



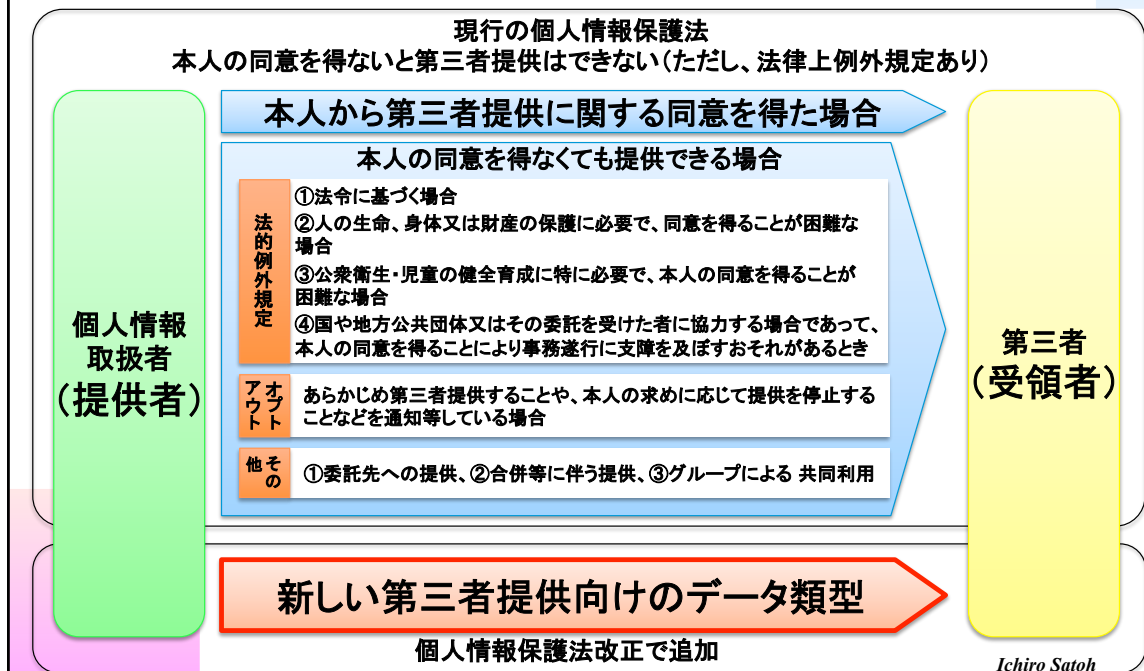
法改正: 要配慮情報の新設

- 本人に対する不当な差別又は偏見が生じないようにその取扱いについて特に配慮を要する記述等(例: 本人の人種、信条、社会的身分、病歴、犯罪被害を受けた事実及び前科・前歴) が含まれる個人情報に要配慮個人情報と定義
 - 要配慮個人情報の対象は政令により決める
 - 要配慮個人情報の取扱いでは、本人同意のない取得を原則として禁止

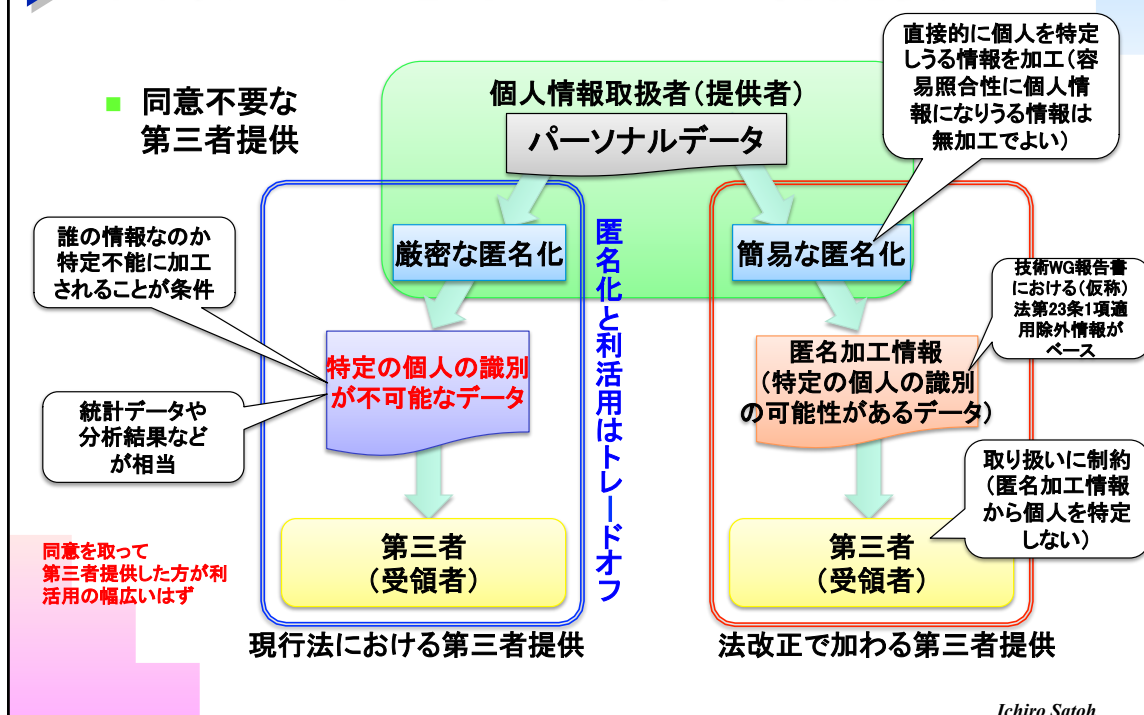


- 導入背景: EUデータ保護指令のSensitive Dataへの対応

▶ 現行法における個人情報の第三者提供



▶ 法改正：同意なしの第三者提供



匿名化とは

■ 個人を識別しにくくするデータ加工技術(あえてナイーブな定義)

- 匿名化より、識別困難化という方が適切

注)匿名化において利用している手法は非公開が望ましい(手法がわかると再特定
のリスクが高まる)

■ 代表的な匿名化手法

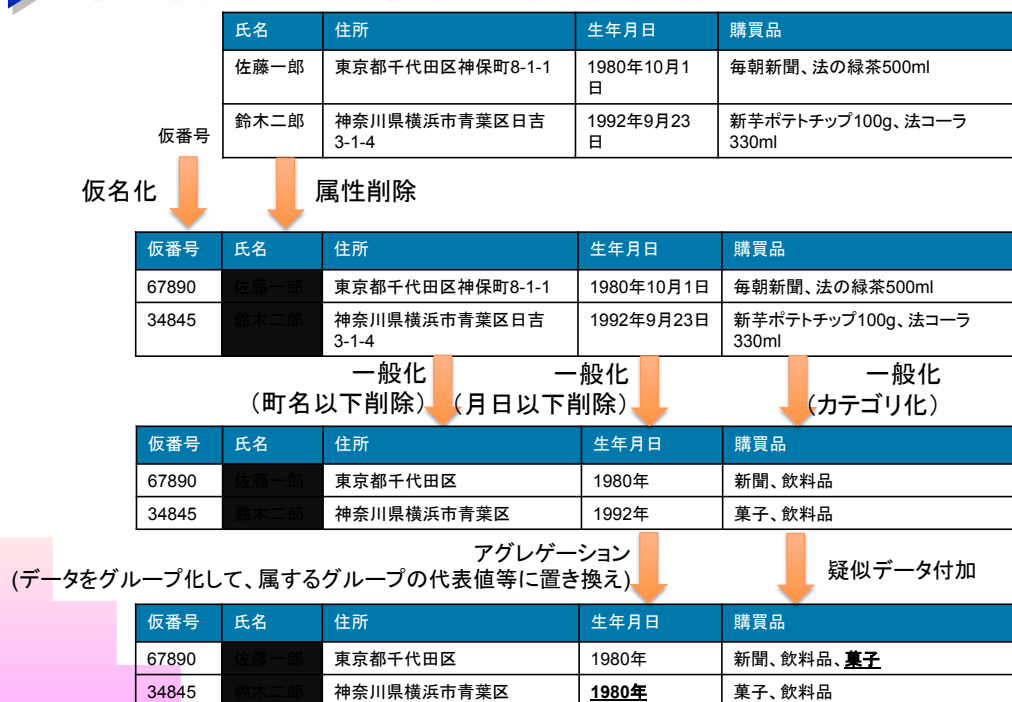
- 属性削除(Suppression)
- 仮名化(Pseudonymization)
- 一般化(Generalization)
- かく乱(Perturbation)

組み合わせる

- なお、**k-匿名性(k-anonymity)**とは、各種匿名化手法により、データ加工の結果、類似した属性をもつ複数人をひとまとめにする(k人未満に絞り込まれない)こと(注:本来、K-匿名化という用語はおかしい)

Ichiro Satoh

匿名化(代表的な手法)



Ichiro Satoh

属性の一般化や削除することで、
同じ保護属性の組み合わせ
を持つ個人が少なくともK人存在す
ることの指標

35

K匿名性

会員番号	住所	生年月日	年齢	好きな番組	購買品
10001	東京都千代田区神保町...	1980年10月1日	33	報道番組	ビール、新聞
10002	神奈川県横浜市緑区鴨居...	1992年9月23日	21	バラエティ	ポテトチップ、炭酸飲料
10003	東京都渋谷区神南...	1979年10月1日	35	ドラマ	コーヒー、タバコ
10004	東京都江東区牡丹...	1990年3月12日	24	ドラマ	化粧品、ヨーグルト
10005	神奈川県川崎市宮前区...	1985年7月28日	28	バラエティ	ポテトチップ、炭酸飲料
10006	神奈川県横浜市港北区日吉...	1987年4月18日	27	報道番組	コーヒー、新聞
10007	東京都港区白金...	1978年12月31日	34	ドラマ	おでん、ヨーグルト
10008	東京都品川区北品川...	1985年3月3日	26	バラエティ	おにぎり、お茶
10009	東京都文京区大塚...	1989年12月1日	23	ドラマ	コーヒー、おにぎり

同じ加工をしても、
所定のK匿名性を
満足するかはデータ
次第



K匿名性の判定は、
データ数に対して指
数的に組み合わせ
が増える

↓ 削除

↓ 一般化

↓ 削除

↓ 一般化

会員番号	住所	生年月日	年齢	好きな番組	購買品
10001	東京都	1980年10月1日	30代	報道番組	ビール、新聞
10003	東京都	1979年10月1日	30代	ドラマ	コーヒー、タバコ
10007	東京都	1978年12月31日	30代	ドラマ	おでん、ヨーグルト
10004	東京都	1990年3月12日	20代	ドラマ	化粧品、ヨーグルト
10005	東京都	1985年7月28日	20代	バラエティ	おにぎり、お茶
10008	東京都	1989年12月1日	20代	ドラマ	コーヒー、おにぎり
10002	神奈川県	1992年9月23日	20代	バラエティ	ポテトチップ、炭酸飲料
10009	神奈川県	1985年7月28日	20代	バラエティ	ポテトチップ、炭酸飲料
10006	神奈川県	1987年4月18日	20代	報道番組	コーヒー、新聞

K匿名性
(K=3)

住所と年齢
の該当者3名

住所と年齢
の該当者3名

住所と年齢
の該当者3名

Ichiro Satoh

匿名化は難しい

■ 某鉄道会社の乗車履歴の第三者提供

■ 各利用者に仮IDを割り当てる(仮名化)

- ユーザを直接特定する情報を排除

■ 仮IDは長期間割り当て

- 長期的に分析すればするほど特定リスクは高まる

■ 乗降駅名だけでなく、乗降時間(秒単位)で記録

- 乗降数が少ない駅ならば、改札前を観察してれば...

■ 匿名化対象を選ぶ

- 少数乗降者数の少ない駅の情報提供しないは一見、良さそうですが
- 乗車履歴は乗車駅と降車駅の組合せ

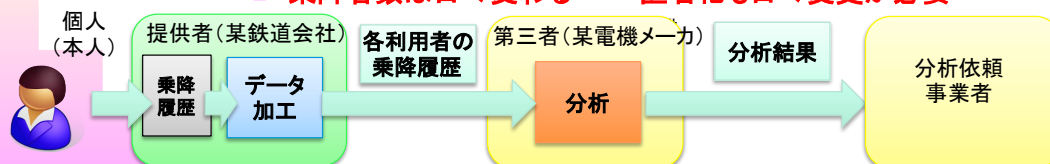
- 乗降客数が多い、二つの駅でも、その二つの駅を移動する人が一人ならば識別可能

- 乗降者数は日々変わる → 匿名化も日々変更が必要

技術力のあるされる某鉄道会社でも
匿名化ができていないことが問題

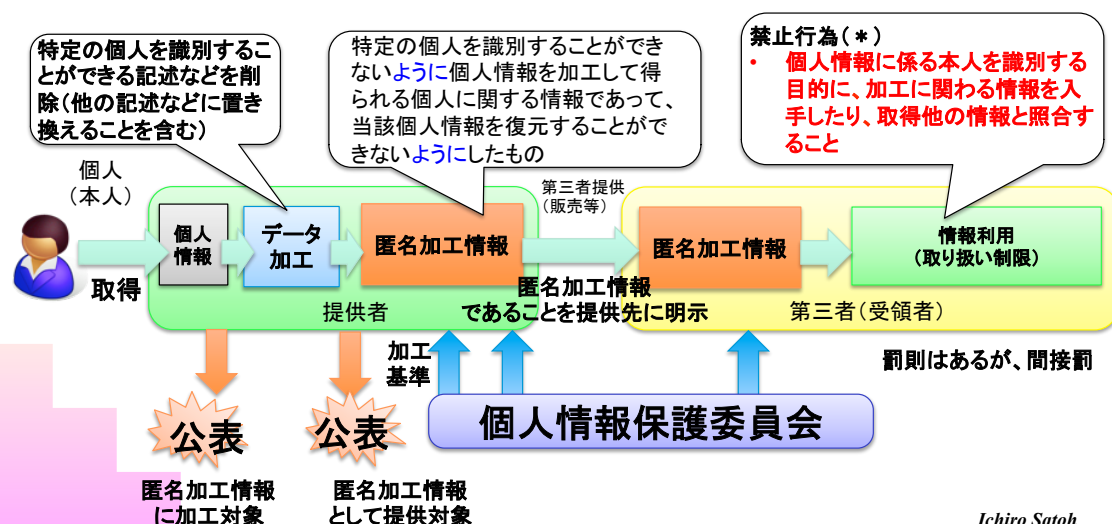
多くの会社には困難

困難を前提にして法制度を考える



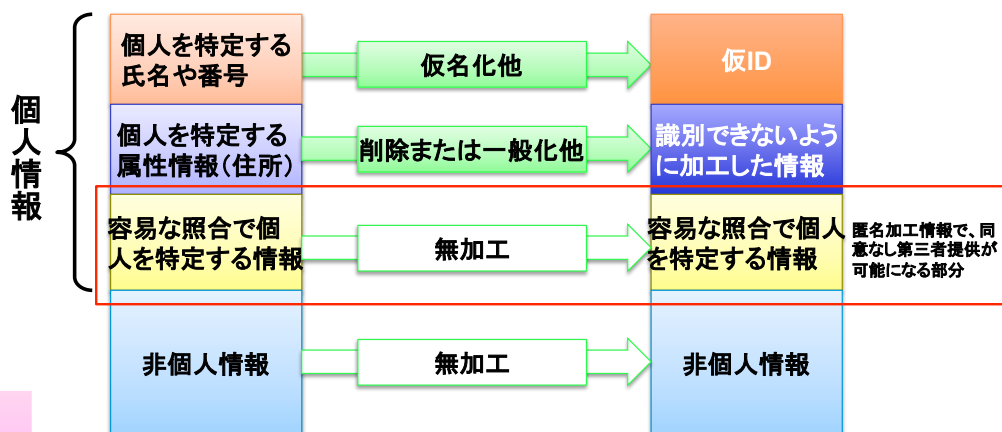
- 個人情報非個人情報化のような汎用的な方法はない個別対応をするしかない

- 匿名加工情報取扱事業者は、匿名加工情報を取り扱うに当たっては、当該匿名加工情報の作成に用いられたし、又は当該匿名加工情報を他の情報と照合してはならない。



匿名加工情報とは

- 個人情報から匿名加工情報への加工
 - 政令次第なので、現状ではなんともいえない
 - ただ、法律的な不備と思われる点もあるようなないような・・・



Ichiro Satoh

匿名加工情報への加工イメージ

- 統一的な加工方法は存在しない、個別で対応するしかない

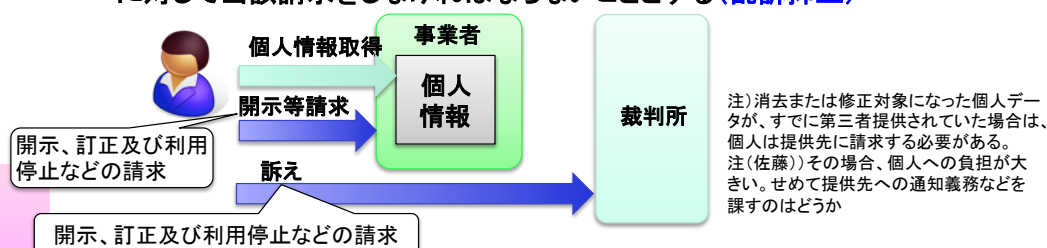
例：技術WGによる低減データ加工イメージ

パーソナルデータ	個人情報		個人情報	個人識別符号		個人に関わる情報	一品物
	氏名	住所	生年月日	旅券番号	指紋	購買品	
	佐藤一郎	東京都千代田区神保町8-1-1	1980年10月1日	THX1831		毎朝新聞(2014年4月22日)、シュワッコーラ 330ml(2014年4月21日)、...	コーラ
	鈴木花子	東京都中央区銀座9-1-4	1992年9月23日	TJP2014		オートクチュールドレス(2014年4月20日)、華香る紅茶250ml(2014年4月22日)、...	華香る紅茶
(技術WG) 個人特定低減データ	仮ID	住所	生年月日	旅券番号	指紋	購買品	
	8748160	東京都千代田区	1980年			毎朝新聞(2014年4月22日)、シュワッコーラ 330ml(2014年4月21日)、...	コーラ
	8045150	東京都中央区	1992年			華香る紅茶250ml(2014年4月22日)、...	華香る紅茶

Ichiro Satoh

法改正：個人情報保護に向けた規定整備

- 小規模事業者への対応
 - 取り扱う個人情報量が少量である事業者への除外規定を削除
(現行法は保有個人情報が5千件以下ならば除外)
- 個人データ消去
 - 個人情報取扱事業者は個人データを利用する必要性がなくなったら、**遅延なく消去**するように**努め**なければならない(**努力規定**)
- 開示請求の明確化
 - 個人情報の本人が、個人情報取扱事業者に対して開示、訂正及び利用停止などの請求を行う権利を有することを明確化(**訴訟**)
 - **ただし**、開示等の請求に関わる訴訟を提起する**前に**、個人情報取扱事業者に対して当該請求をしなければならないこととする(**乱訴抑止**)

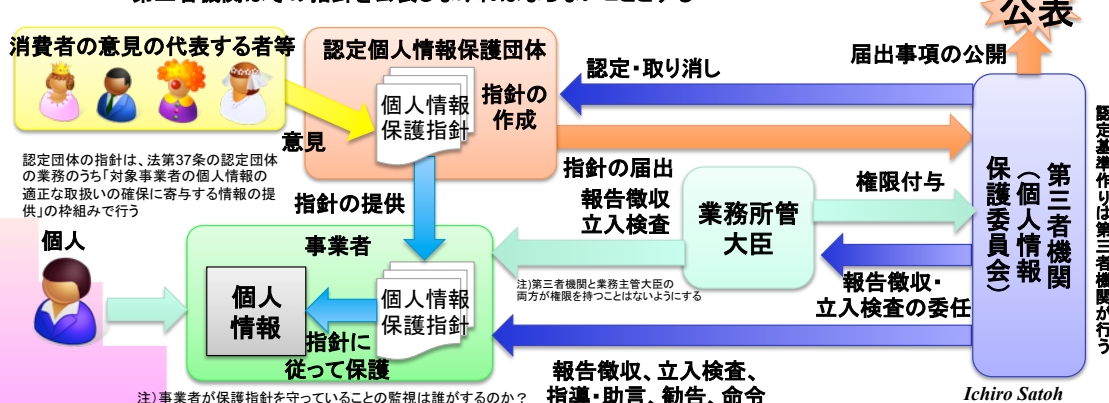


注) 行政機関個人情報は請求権があり、それをベースにする

Ichiro Satoh

法改正：第三者機関(個人情報保護委員会)

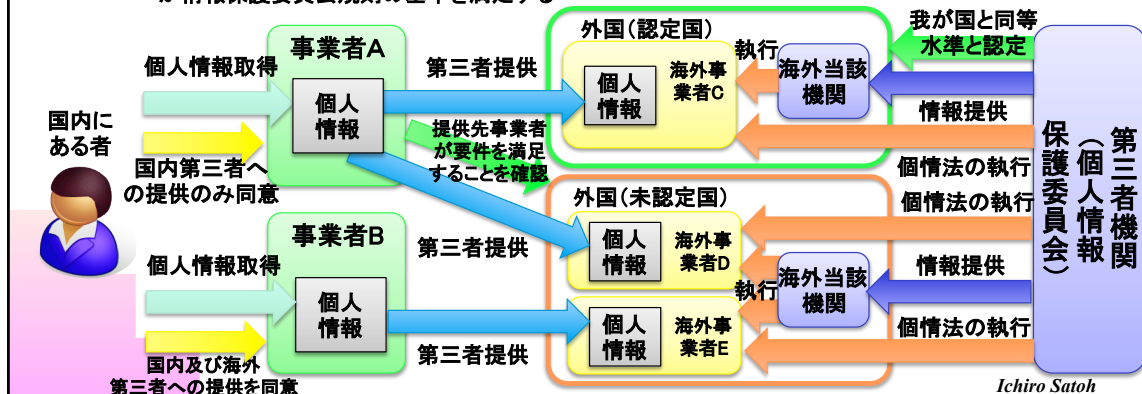
- 個人情報及び匿名加工情報の取扱いに関する監督等の事務をつかさどる第三者機関(名称:個人情報保護委員会)を内閣府の外局として新設(特定個人情報保護委員会(マイナンバー委員会)を改組)
 - 個人情報保護委員会に現行の主務大臣の有する権限(報告徴収、命令、認定個人情報保護団体の認定等)に加えて、**立入検査**の権限等を付与する
 - 個人情報保護委員会は、個人情報取扱事象者等に対する報告徴収及び立入検査の権限を事業所管大臣等に**委任**することができる
- 認定個人情報保護団体が、個人情報保護指針を作成する場合には、消費者の意見を代表する者等の意見を聴くように**努め**、第三者機関(個人情報保護委員会)に届け出なければならない
 - 第三者機関に、その指針の変更等を命じることができる現行の主務大臣の有する権限を付与する
 - 第三者機関はその指針を公表しなければならないこととする



Ichiro Satoh

▶ 法改正：グローバル化への対応

- 国内にある者に対する物品又は役務の提供に関連してその者を本人とする個人情報を取得した個人情報取扱事業者が、外国において当該個人情報を取り扱う場合についても個人情報保護委員会による命令に関する部分を除いて、適用する(域外適用、ただし海外事業者に命令はできない)
- 個人情報保護委員会は、本法に相当する外国の法令を執行する外国執行当局に対し、情報提供を行える(執行協力)
- 個人情報取扱事業者が個人データを外国にある第三者に提供する場合、当該提供についての本人同意を得るか、次のいずれかの要件を満たさなければならないこととする。
 - 提供先は同等の水準にあると認められる個人情報保護の制度を有している国として個人情報保護委員会が定める国にある第三者
 - 提供先は個人情報取扱事業者が講じなければならない措置相当を継続的に講じる体制等をもち、それが情報保護委員会規則の基準を満足する



▶ 単一種類データからはわからない

- 自宅の電力監視
 - Googleの推奨電力監視セットを入手、勝手に配電盤に取り付け

TED 5000 (Energy Inc.)



- 電力消費データだけで、ユーザ行動推測は難しいのでは？
 - 本人ですら電力消費と利用家電の相関が難しい
 - 粗いユーザ行動推定、例えば家に人がいるか、ぐらい
 - 結局、Googleも撤退した

▶ データの組み合わせとプライバシー問題

- 個別データで見えないユーザ行動が、相違なデータの組み合わせで見える
 - 実例：水道メータとガスメータの遠隔共同検針（2002年）
 - 某自治体水道局と某ガス会社
 - PHS回線及び電灯線を利用した遠隔検針
 - 実証実験（戸建住宅：100軒、集合住宅：60軒）
 - しかし、プライバシー問題の危惧から実証実験開始直後に中止
 - 水道とガスが同時利用がわかると
 - お風呂の準備をしていることがわかる
- 情報単体ではプライバシー侵害や個人特定がなくても、データの組み合わせによっては問題が起きうることに注意

Ichiro Satoh

▶ 知は誰のものか

- IoTによる情報の取得、分析、利用にはステークホルダーがいっぱい
 - データの対象、センサー所有者、分析者、分析結果の利用者他多数
- 例：米国保険会社Progressive
 - 保険会社が自動車取り付けようデバイスを契約者に無償提供
 - 運転頻度、速度、走行距離、運転時間帯等のデータを収集
 - 保険会社に携帯電話回線を通じて送信
 - 運転者のドライブ履歴を分析して、そのリスクを算定し、保険料率反映
 - 運転者を運転状況に見合った保険料
 - 運転習慣を見直し

写真は
PROGRESSIVE
社のWebページから



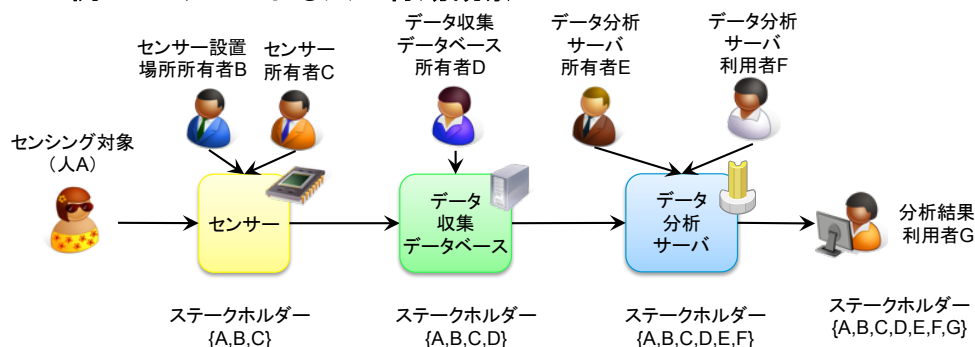
- デバイスが収集した運転情報は誰のものか？

Ichiro Satoh

マルチステークホルダー問題

■ 現実の知には多数のステークホルダーが登場

■ 例: センサーによる人の行動観察



■ パーソナルデータ/プライバシー問題は、個人本人とデータ利用者などの2者問題(マルチステークホルダー問題の一部にしか過ぎない)

IoTはステークホルダーが整理・利害調整ができれば絵に描いた餅

Ichiro Satoh

技術と社会問題

■ 技術には功罪が伴う

■ 知の集積・伝播・探索、予見・発見の促進は重要であるがそれが生み出す影響を考えておくべき

■ パーソナルデータ、プライバシー問題

■ ITの進化が誘発した問題

■ ITで抑制できる問題だけとは限らない

■ 人々が漠然と思う、ITへの不安

■ 思い過ごしとして一蹴できるのか

**強い薬ほど、大きな効用をもたらす同時に、大きな副作用をもつ
(副作用もない弱い薬では、状況は変えられない)**

Ichiro Satoh

▶ 技術と制度の一体化

- ITの進歩は、大きな効用をもたらしたが、一方で問題を生み出している
 - 例:個人情報およびプライバシーに関わる権利・利益の侵害
 - ウェアラブルカメラとプライバシー
- 問題によっては技術だけでは解決できない
 - 制度による補完が必要
- 技術と制度を一体化で考えるべき
 - 研究開発段階から、技術が引き起こす問題を予測し、それを抑止・最小化する制度設計を行うべき
 - プライバシー・バイ・デザイン
 - セキュリティファースト、プライバシーファースト

Ichiro Satoh

▶ 研究開発と制度設計は不可分



- 某社のウェアラブルカメラから学ぶ教訓
 - ウェアラブルカメラのプライバシー問題は知られていた問題
 - 製品発売と法制度の提案のセットでもよかったかも

Ichiro Satoh

▶ まとめ

- 組込／IoTでもプライバシー問題は無関係ではない
 - 人に関する情報を集める限りは、プライバシー侵害リスクがある
 - 一つ違ふと経営リスク
 - IoTではステークホルダー関係も複雑化
 - プライバシー保護を先送りせずに、設計段階から考慮すべき
 - プライバシー・バイ・デザイン
- 個人情報保護法の改正
 - パーソナルデータの利活用は容易になった部分と、厳しくなった部分
- 技術と法制度は不可分
 - 組込システムやIoT開発では、起きうる問題を予測し、その問題を解決する技術や法制度を検討すべき