

改正個人情報保護法に係る 情報セキュリティへの影響

ビッグデータ・IoT時代における 個人情報の利活用と保護

2015 年 6 月 9 日

松本 泰 セコム（株） I S 研究所



Copyright (c) 2000-2015 NPO 日本ネットワークセキュリティ協会 ,

1

改正個人情報保護法による情報セキュリティへの影響 ビッグデータ・IoT時代における個人情報の利活用と保護

- 情報セキュリティ、および情報セキュリティビジネスに多大な影響を与えた個人情報保護法が、10数年ぶりの改正に向かっていきます。今回の改正の大きな目的の一つは、個人情報の保護と利活用の両立になります。
- 今後の社会において、IoTにより広く大量に集められたパーソナルデータを如何に活用し、かつ保護するかということが、日本だけではなく世界的な課題となっています。
- 本パネルディスカッションでは、改正個人情報保護法案の背景と概要を説明するとともに、IoT/ビッグデータの時代において、個人情報の利活用と保護を両立するための制度、技術、ビジネスの在り方や、情報セキュリティの関係者が社会に提言していくべき内容について議論します。

プロローグ？

What, Why

改正案の1条

- この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。

現行法：「個人情報の有用性に配慮しつつ」

- 個人情報保護と情報セキュリティ
 - 2005年全面施行の個人情報保護法
 - 情報セキュリティビジネスに多大な影響を与えた
 - 個人情報の「利活用」という視点では、個人情報を金庫にしまっておき利活用しない方向へ??
 - 今回の改正案の大きな目的ひとつ??
 - ビッグデータ利活用による新事業・新サービス創出の促進
 - そのための「個人情報の**利活用**と保護」
- 情報セキュリティ的にはどう変化するのか?
 - 「個人情報を金庫に閉じ込めておくための情報セキュリティ」から「個人情報を利活用するための情報セキュリティ」へ
 - 企業の競争力のための個人情報利活用と、そのための個人情報保護
 - ー> 企業の競争力のため情報セキュリティ投資
 - 個人情報を利活用する + 顧客との信頼関係を築く情報システム
 - そのための「セキュリティ・バイ・デザイン」、「プライバシー・バイ・デザイン」

パネルディスカッション

- 前半
 - 改正個人情報保護法（案）の理解
- 後半
 - ビッグデータ・IoT時代の情報セキュリティ
 - ビッグデータ・IoT時代を妄想??して個人情報の利活用と保護を両立するための制度、技術、ビジネスの在り方を議論する
- モデレータ
 - 松本 泰（セコム株式会社 IS研究所）
- パネリスト：
 - 宮内 宏 氏（五番町法律事務所 弁護士）
 - 福田 尚弘 氏（パナソニック株式会社）

(前半) 改正個人情報保護法案の概要

- ・「個人情報の定義」と
- ・「匿名加工情報の扱い」を
中心に説明

Copyright (c) 2000-2015 NPO日本ネットワークセキュリティ協会

7

個人情報保護法の改正のポイント

個人情報保護法の改正のポイント

1. 個人情報の定義の明確化	・個人情報の定義の明確化（身体的特徴等が該当） ・要配慮個人情報（仮称、いわゆる機微情報）に関する規定の整備
2. 適切な規律の下で個人情報等の有用性を確保	・匿名加工情報（仮称）に関する加工方法や取扱い等の規定の整備 ・個人情報保護指針の作成や届出、公表等の規定の整備
3. 個人情報の保護を強化（名簿屋対策）	・トレーサビリティの確保（第三者提供に係る確認及び記録の作成義務） ・不正な利益を図る目的による個人情報データベース提供罪の新設
4. 個人情報保護委員会の新設及びその権限	・個人情報保護委員会を新設し、現行の主務大臣の権限を一元化
5. 個人情報の取扱いのグローバル化	・国境を越えた適用と外国執行当局への情報提供に関する規定の整備 ・外国にある第三者への個人データの提供に関する規定の整備
6. その他改正事項	・本人同意を得ない第三者提供（オプトアウト規定）の届出、公表等厳格化 ・利用目的の変更を可能とする規定の整備 ・取扱う個人情報が5,000人以下の小規模取扱事業者への対応

出典: <http://www.kantei.go.jp/jp/singi/keizaisaisei/wg/innovation/dai5/siryou1.pdf>

Copyright (c) 2000-2015 NPO日本ネットワークセキュリティ協会

基本的な用語の理解 その1 データ、情報（などの定義）



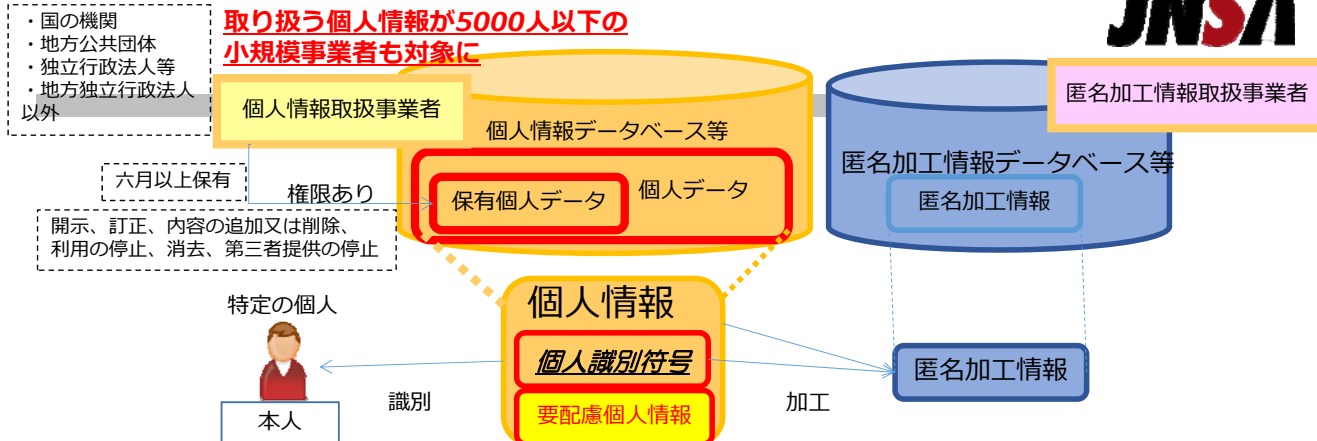
- 個人情報（2条）
 - 定義に一部変更がある **要注意
 - 個人情報の定義の明確化（のはず）
- 個人識別符号（2条2項）
 - 個人情報の定義における新規用語 **要注意
 - 個人識別符号が含まれると個人情報
- 要配慮個人情報（2条3項）
 - いわゆるセンシティブ情報
- 保有個人情報
 - 6ヶ月以上保有する個人データ
- 匿名加工情報（2条9項） **要注意
 - ビッグデータ、2次利用のための新類型
 - 「個人情報」ではないが「非個人情報」でもない??

基本的な用語の理解 その2 エンティティ - 関係者・組織等の定義



- 本人
- 個人情報保護委員会（50条-65条）
 - 一番重要な変更（追加）
 - 「特定個人情報保護委員会」が「個人情報保護委員会」へ
- 個人情報取扱事業者
 - 「個人情報」の安全管理措置義務等 現行法の20条
- 匿名加工情報取扱事業者
 - 「匿名加工情報」の提供先事業者
 - 「匿名加工情報」の安全管理措置の努力義務等
- 認定個人情報保護団体
 - 現行法にもあるが「匿名加工情報」の取り扱い等における指針（個人情報保護指針）の作成、マルチステークホルダープロセスの取りまとめなどを期待されている。
- 外国個人情報取扱事業者
 - 国内法の海外事業者への適用等

基本的な用語の理解 - 情報、取扱い事業者の関係



第二条一項

一 氏名、生年月日その他の記述等（中略）により特定の個人を識別することができるもの（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こととなるものを含む。）

二 個人識別符号が含まれるもの

第二条二項

一 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文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの

二 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カードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号、その他の符号であって、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、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

第二条三項

（中略）本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報という。

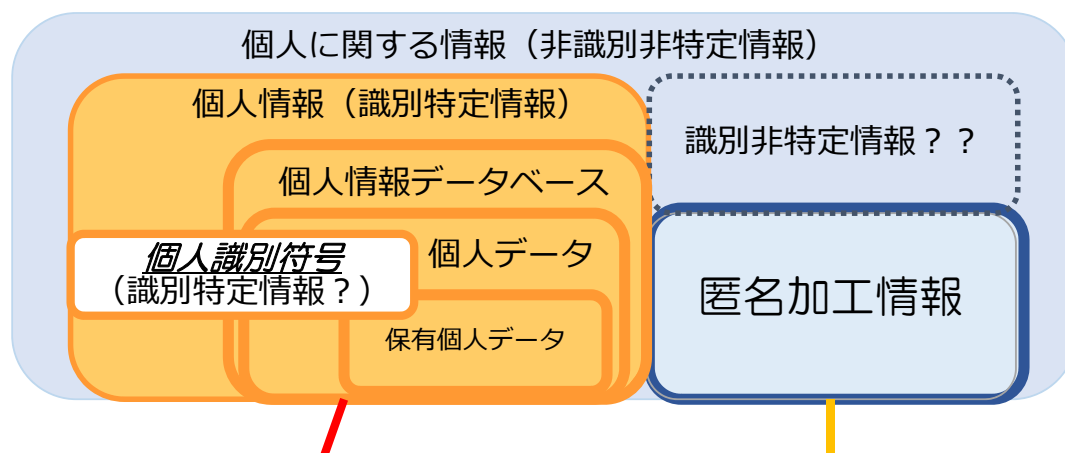
第二条九項

（中略）特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものという。

一（中略）個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）

二（中略）個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。） 11

情報の種別と安全管理措置の関係



•20条 安全管理措置義務
（現行法と同様）

•39条
安全管理措置努力義務

第二条一項 — この法律において「個人情報」とは

一 氏名、生年月日その他の記述等（中略）により 特定の個人を識別 することができるもの（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こととなるものを含む。）

二 個人識別符号が含まれるもの

第二条二項 — この法律において「個人識別符号」とは

一 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 変換した文字、番号、記号その他の符号であって、当該 特定の個人を識別することができるもの

二 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カードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号、その他の符号であって、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、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

Copyright (c) 2000-2015 NPO日本ネットワークセキュリティ協会

13

匿名加工情報の定義

• 第二条九項

- この法律において「匿名加工情報」とは、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて 特定の個人を識別することができないように個人情報 を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。
- 一 第一項第一号に該当する個人情報当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。
- 二 第一項第二号に該当する個人情報当該個人情報に含まれる 個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

Copyright (c) 2000-2015 NPO日本ネットワークセキュリティ協会

14

JNSA**JNSA**

- 個人情報保護委員会



- （宣言）ビッグデータ利活用による新事業・新サービス創出の促進
 - 第3者提供において利用者の同意を不要とした「匿名加工情報」の活用
- （報告書）どの程度データの加工等を実施すれば個人情報保護法の制限を受けることがなくなるのかを明確化
 - 「どの程度データの加工」
 - 委員会規則へ先送り？
 - 認定個人情報保護団体による個人情報保護指針等
 - マルチステークホルダープロセスへの期待？
 - 「個人情報保護法の制限を受けることがなくなる」
 - 「匿名加工情報」は、改正個人情報保護法（案）の制限は受ける
 - 加工したデータは「匿名加工情報」になる
 - 提供先での再識別禁止義務 **ここは要注意**
 - 提供先での安全管理措置努力義務

Q&A

後半 （妄想??） ビッグデータ・IoT時代の情報セキュリティ

ビッグデータ・IoT時代を妄想??して個人情報の利活用と保護を両立するための制度、技術、ビジネスの在り方を議論する

（妄想??） ビッグデータ・IoT時代の情報セキュリティ

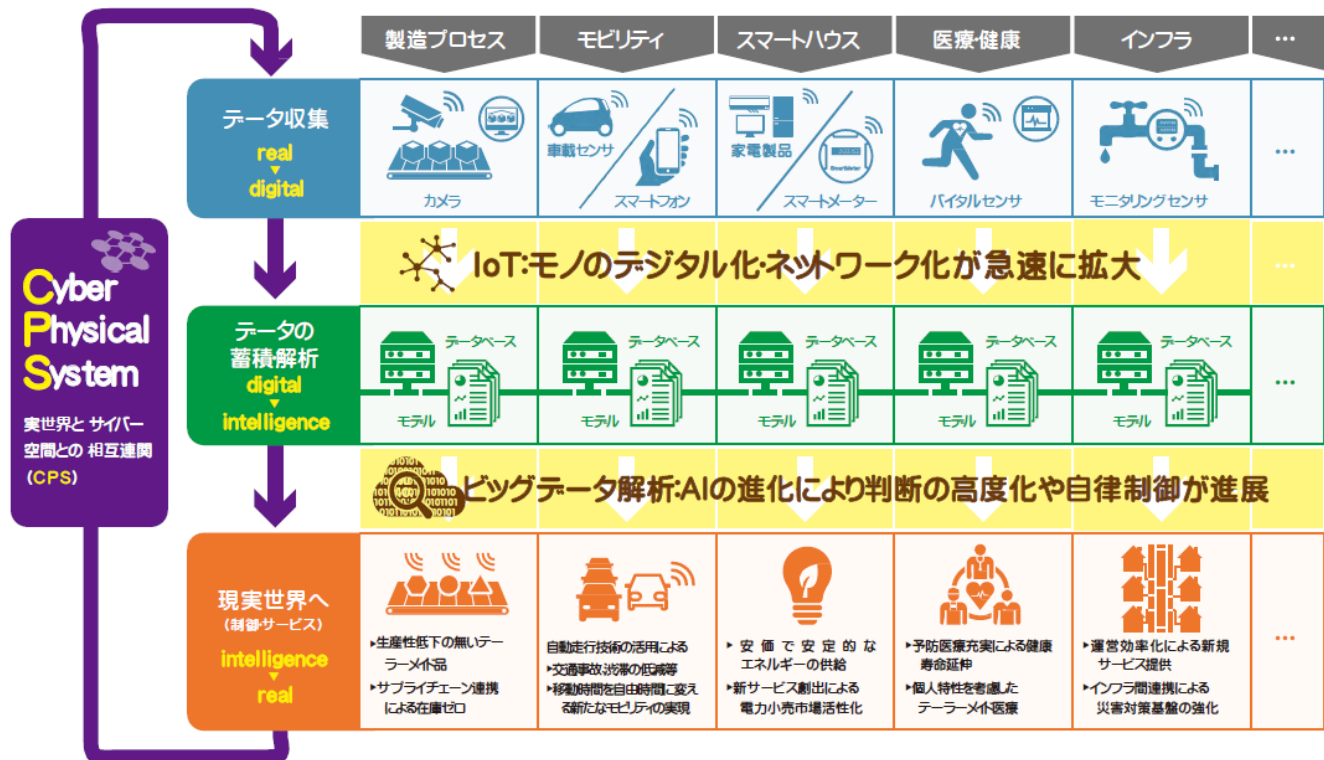


- なぜ**妄想**??
 - 世の中にあふれるパスワード - 成長戦略等の後押し?
 - ビッグデータ、M2M、IoT、CPS(Cyber-Physical System)
 - これらのパスワードを元に様々な**妄想**が語られている
 - #「妄想二ホン料理」並に
 - 「CPSの深化を見通した**効率的かつ集中的な要素技術開発の成否**が、今後の**産業競争力及び社会変革を大きく左右**すると考えられる」(経済産業省報告書より***)
 - これらの**成否**に — 保護の視点では「妄想」は少ない?
 - (情報セキュリティの関係者であれば) 誰が考えても「セキュリティ」「プライバシー」に関する課題解決が必要だけど
 - ありきたりの議論しかなされていないのでは??
 - 報告書の「コアテクノロジーの研究開発強化」では、プライバシー保護技術の様な「両立」を目指した技術の話は出てこない。
 - ここを**妄想**したい!!

社会全体がCPSにより変革される「データ駆動型社会」

CPSによるデータ駆動型社会

▶実世界とサイバー空間との相互連関（Cyber Physical System）が、社会のあらゆる領域に実装され、大きな社会的価値を生み出していく社会



出典: 経済産業省 ～CPSによるデータ駆動型社会の到来を見据えた変革～

http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/pdf/report01_02_00.pdf

ビッグデータ・IoT時代の制度、技術、ビジネス

JNSA

- 法案でのふたつの大きな論点
 - 個人情報 の定義
 - 匿名加工情報
- CPS (Cyber-Physical System) とパーソナルデータ の関係
 - モビリティ、スマートハウス、医療・健康等の分野
 - 本質的にパーソナルデータ 満載
 - かつ、個人の便利・快適等にフィードバックしたい (はず)
 - CPSにおけるデータ (パーソナルデータ?) の循環
 - データの収集 「個人識別符号」との関係
 - データの蓄積・解析 「匿名加工情報」との関係
 - 現実世界へ (制御サービス) 個人へフィードバック??
- CPSにより産業競争力の向上、社会変革を促すためには
 - 本質的に「個人情報 (パーソナルデータ) の利活用と保護の両立」に関する課題を解決する必要がある。
 - これは単に「個人情報の定義」で解決できる問題ではない??

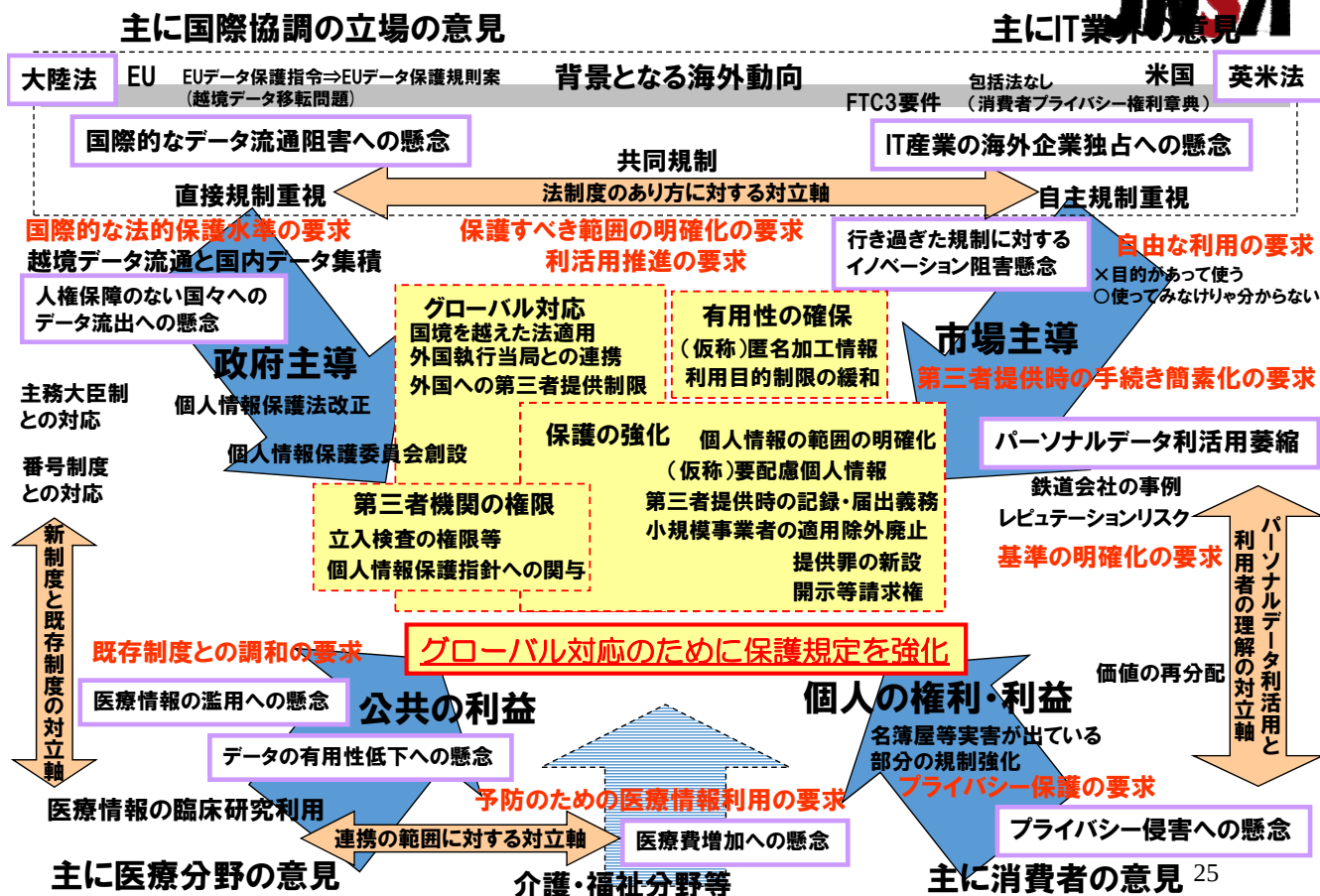
- 個人情報の明確化は、正しい方向性なのか？
- MAC address
 - 通信のためには「識別子」が必要という問題
 - 元々は有線LANを想定した昔々の仕様??
- 「匿名加工情報」は、使えるのか？
 - 利活用と保護を両立させる匿名化幻想??
- PIA (Privacy Impact Assessment) は、有効か？
 - 番号制度の特定個人情報保護評価
- プライバシー保護技術
 - データを金庫にしまっておく方向に向かわせた現行法の施行の元では、プライバシー保護技術は、まったく注目されなかった？
 - 欧州のF P 7では多くのプライバシー保護技術に関連するR&Dプロジェクトが実施された。
- PPDM (privacy-preserving data mining)
 - 「匿名加工情報」とは違うアプローチ

Copyright (c) 2000-2015 NPO日本ネットワークセキュリティ協会

23

参考スライド

複雑な背景???? 様々な論点、対立点



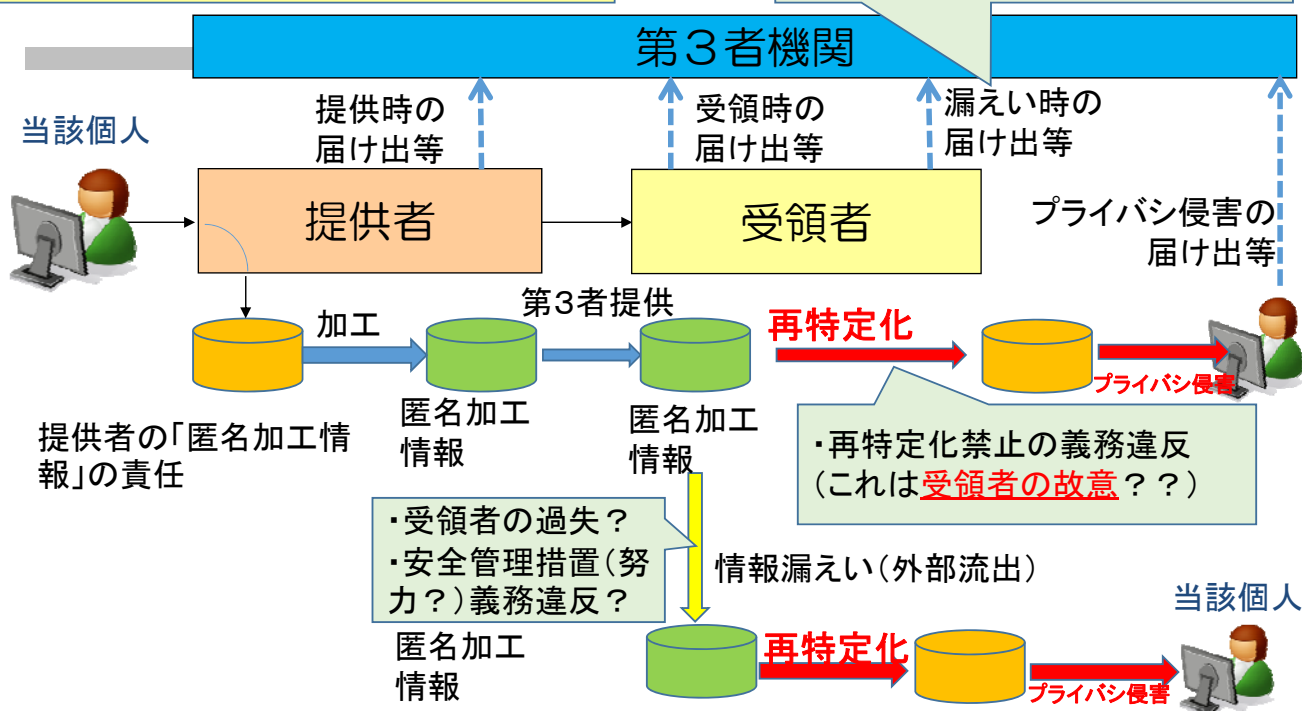
データセキュリティのドメインに対応した (暗号技術の) ガイドラインの例

ドメイン	ガイドラインの例	対象、備考
移動中のデータ (Data in Motion)	NIST SP800-52	TLS
	NIST SP800-77	IPsec VPNs
	NIST SP800-113	SSL VPNs
保管データ (Data at Rest)	NIST SP800-111	Storage Encryption for End user
使用中のデータ (Data in Use)	なし	「暗号化状態処理技術」などの応用が期待される
データの処分 (Data Disposed)	NIST SP800-88 **	電子メディアの破壊

** NIST SP800-88 rev.1 draft 2012年9月 このDraftには、暗号技術による消去 Cryptographic Eraseが記述されている。

そのままのプライバシー侵害との関係

第2回技術検討WG提出資料を一部修正



- ・ 事前規制としての第3者提供の公表、届け出の管理等
- ・ 情報漏えい時の、被害拡大などを最小化等のための迅速な対応
- ・ プライバシー侵害発生時の、責任の明確化等のための証拠の保存(証拠保存による抑制)
- ・ プライバシー侵害発生時の、被害拡大などを最小化等のための迅速な対応

「匿名加工情報」のふたつの考え方

第2回技術検討WG提出資料を一部修正

JNSA

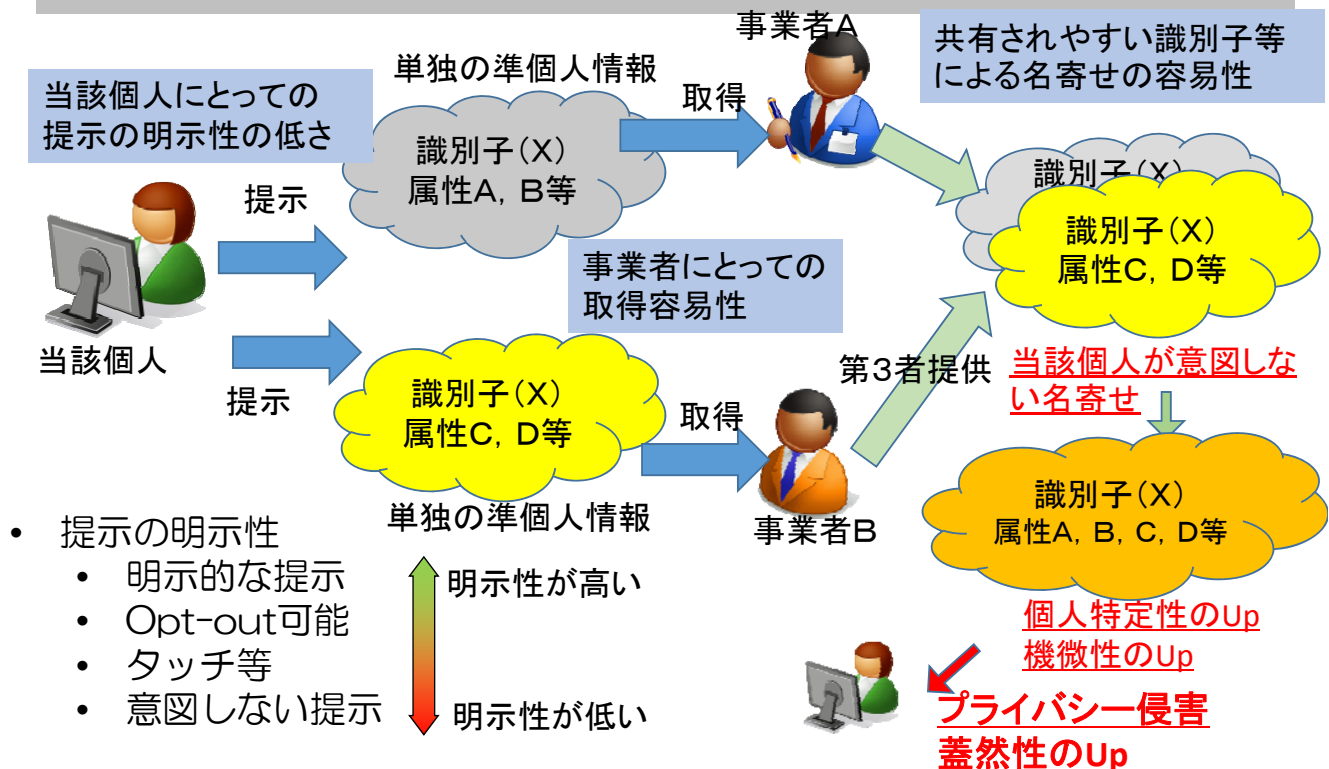
匿名加工情報	提供者	受領者	備考・課題
特定性低減のレベルが低い (利活用性が高い)	・ 提供者としては安心できる受領者に提供したい(受領者のお墨付きが欲しい?) ・ 提供者の責任は低い	・ 受領者の責任が重要 ・ 利活用がより可能になる。 ・ 受領者の安全管理措置等がより求められる。 ・ 第3者機関による「受領者」の登録制度等による許認可が理想?	・ 登録制度等を運用するのは難しいかもしれないが利活用は行いやすい。 ・ 受領者側がより専門性の高い事業者を想定される ・ 定量評価が難しい。
特定性低減のレベルが高い (利活用性が低い)	・ 提供者の責任が重要 ・ 提供者は、「匿名加工情報」の特定性・識別性の低減のレベルに責任を持つ必要がある	・ 利活用は、低減性の高いレベルのデータに制約を受ける。 ・ 受領者が持つべき責任は少ない	・ 提供者に、より多くのスキルが要求される。 ・ 提供者からの公表、届け出などが有効。 ・ 「匿名加工情報」の性質・レベル(k-匿名性)等が重要

「データの利活用における有用性と当該データ内の個人の特定性や識別性を低減させることはトレードオフの関係」。利活用の観点からは、「匿名加工情報」の加工方法以外の観点の検討も必要ではないか?

「準個人情報」の規制の重要性 「準個人情報」に含まれる識別子の性質・特性の考察

第2回技術検討WG提出資料を一部修正

JNSA



提示の明示性の低さは、利便性も提供していることが多い。

29

改正法案・匿名加工情報の雑感

JNSA

- 「匿名加工情報」というネーミングのミスリーディング？
 - 魔法の「匿名化データ」という幻想が残っている？
 - 技術検討WG報告書の「個人特定性低減データ」が、比較の実体を表したネーミング（だと思う）。
 - プライバシー侵害リスクが残存するデータ
 - 「匿名加工情報」の「利活用性」と「特定性低減」のレベルのトレードオフが理解されていない？
- 法制度と、実体（利活用、プライバシー侵害）が乖離しないためには、もっとユースケースに基づいた検討が必要ではないか？
 - 成長戦略や社会の効率化のための利活用のユースケース
 - ユースケース・ビジネスモデルの利活用にあった法制度
 - 実体的なプライバシー侵害のユースケース
 - ユースケースのリスクを低減するための法制度

- 議論の履歴
 - 従来の個人情報 + 準個人情報 → 扱いに差を付ける
 - 従来の個人情報の拡張 → 準個人情報ではなく、個人情報の拡張
 - 個人情報の明確化と「個人識別符号」 → 法案（拡張は避けた？）
- 技術検討ワーキンググループ報告書の記述
 - 従来からの容易照合性の議論はしない
 - 「何が個人情報に該当するのかの判断は、技術の進歩や社会環境の変化に応じてなされることが重要であると考えられる」
- 個人情報の定義、匿名加工情報の議論の背景??
 - 実現したい研究開発が進むほどに（進めたいと思う程に）プライバシーの課題が浮上する
 - ex.
 - ビッグデータ解析の研究・開発が進むほどに個人が特定できる
 - 顔画像認証の精度やGPS等の位置精度が高くなる程に個人が特定できる
 - ビッグデータ時代になる程に、背景知識（ネット上の情報）豊富になり個人が特定できる
 - ジレンマ?
 - ビッグデータを活用したい → 個人情報保護利用の規制を緩和する → ビッグデータの活用研究が促進される → 個人の特定がより可能になりプライバシー侵害の可能性も高くなる