情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2018年1月25日
JNSA　クロスボーダー時代のアイデンティティ管理セミナー

改正個人情報保護法・GDPRとID情報

湯淺　墾道
情報セキュリティ大学院大学教授
yuasa@iisec.ac.jp

自己紹介

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 慶應義塾大学講師等をへて、2004年九州国際大学法学部専任講師、2005年助教授、2007年准教授、2008年教授、副学長・国際センター長、2011年情報セキュリティ大学院大学情報セキュリティ研究科教授、2012年学長補佐
- 総務省AIネットワーク化検討会議構成員
- 総務省投票環境の向上方策等に関する研究会構成員
- 総務省情報通信政策研究所招へい研究員
- 内閣官房日本経済再生本部裁判手続等のIT化検討会委員
- 一般財団法人日本データ通信協会電気通信個人情報保護推進センター諮問委員会委員長
- 神奈川県情報公開・個人情報保護審議会委員
- 埼玉県本人確認情報保護審議会会長
- 埼玉県特定個人情報保護評価委員会委員長
- 川崎市情報公開運営審議会副会長
- 渋谷区個人情報の保護及び情報公開審議会委員
- 情報ネットワーク法学会副理事長
- 株式会社ベネッセホールディングス情報セキュリティ監視委員会委員長代理

※E-Laws

- XML化対応
- 法令データ一括ダウンロード
- 法令API提供

改正個人情報保護法におけるIDの意義

改正のポイント

■個人情報保護法の改正ポイント

1. 個人情報の定義の明確化
2. 現行法のルールの適正化
3. 個人情報保護の強化
4. 新たな利活用ルール
5. 個人情報保護委員会の新設
6. グローバル化への対応

■2017年5月30日から改正法施行

個人情報の定義の明確化

■「個人識別符号」に該当するものを含める

① 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（個人情報保護法2条2項1号）

② 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、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方法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（同項2号）

■2項1号関係（施行令1条）

- 細胞から採取されたデオキシリボ核酸（別名DNA）を構成する塩基の配列
- 顔の骨格、皮膚の色並びに目、鼻、口その他の顔の部位の位置、形状によって定まる容貌
- 虹彩の表面の起伏により形成される線状の模様
- 発声の際の声帯の振動、声門の開閉並びに声道の形状、その変化
- 歩行の際の姿勢、両腕の動作、歩幅その他の歩行の態様
- 手のひら又は手の甲若しくは指の皮下の静脈の分岐、端点によって定まるその静脈の形状
- 指紋又は掌紋

■2項2号関係

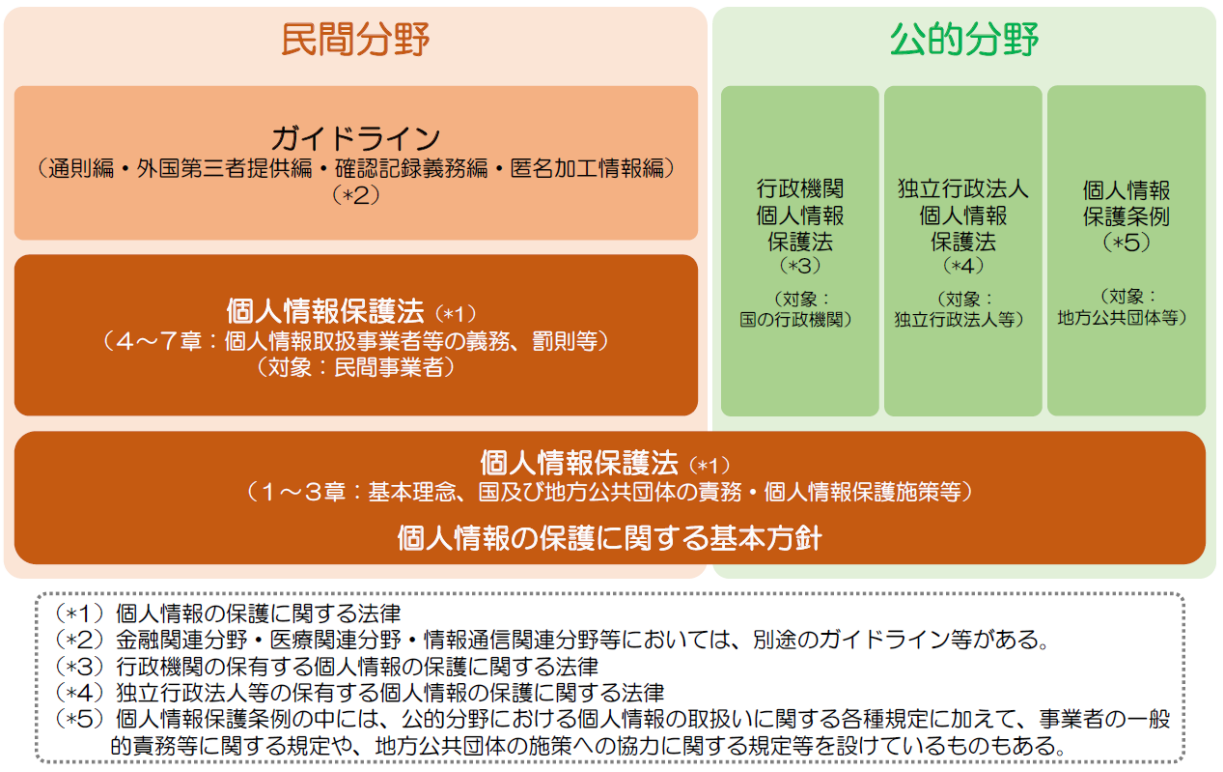
- ■ 旅券番号
- ■ 基礎年金番号
- ■ 運転免許証番号
- ■ 住民票コード
- ■ 個人番号
- ■ 国民健康保険の被保険者証の記号、番号、保険者番号
- ■ 後期高齢者医療制度の被保険者証の番号、保険者番号
- ■ 介護保険の被保険者証の番号、保険者番号
- ■ 健康保険の被保険者証の記号、番号、保険者番号
- ■ 高齢受給者証の記号、番号、保険者番号

- 船員保険の被保険者証の記号、番号、保険者番号
- 船員保険の高齢受給者証の記号、番号、被保険者番号
- 旅券番号（日本国政府が発行したもの以外）
- 在留カードの番号
- 私立学校教職員共済の加入者証の加入者番号
- 私立学校教職員共済の高齢受給者証の加入者番号
- 国民健康保険の高齢受給者証の記号、番号、保険者番号
- 国家公務員共済組合の組合員証の記号、番号、保険者番号
- 国家公務員共済組合の組合員被扶養者証の記号、番号、保険者番号
- 国家公務員共済組合の船員組合員証、船員組合員被扶養者証の記号、番号、保険者番号
- 地方公務員等共済組合の組合員証の記号、番号、保険者番号
- 地方公務員等共済組合の組合員被扶養者証の記号、番号、保険者番号
- 地方公務員等共済組合の高齢受給者証の記号、番号、保険者番号
- 地方公務員等共済組合の船員組合員証、船員組合員被扶養者証の記号、番号、保険者番号
- 雇用保険被保険者証の被保険者番号
- 特別永住者証明書の番号

ガイドライン

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■主務官庁ガイドライン　→　原則として個人情報保護委員会ガイドライン



https://www.ppc.go.jp/files/pdf/personal_framework.pdf

GDPR

GDPR

- 一般データ保護規則（General Data Protection Regulation：GDPR）
  - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
  - これまでEU加盟国に適用されてきた1995年データ保護指令（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指令」(Directive 95/46/EC)に替わり、新たに採択
  - 2018年5月施行予定

■データセキュリティ

●GDPRにより事業者に求められる要件

◆侵害発生前

➢仮名化・暗号化・システム復元力維持等の措置の実施、定期的な検査

◆侵害発生後

➢個人データ窃盗等の個人の権利・利益侵害の危険性が高い侵害に関する通知

■「個人データ侵害」

●「送信、格納、または処理される個人データについて、偶発的または違法な破壊、消失、変更、権限のない公開またはアクセスにつながるようなセキュリティ侵害を意味する。」（第4条第12号）

◆※訳文は、JIPDEC仮訳参照
https://www.jipdec.or.jp/library/archives/gdpr.html

ID漏洩が起きた場合

■日本

●マイナンバーは委員会への報告義務

◆第二十九条の四　個人番号利用事務等実施者は、個人情報保護委員会規則で定めるところにより、特定個人情報ファイルに記録された特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態が生じたときは、委員会に報告するものとする。

■アメリカ

- ●Security breach notification law
- ●医療、金融等の特定領域
  - ◆個別連邦法により通知及び報告義務
- ●州法
  - ◆カリフォルニア州法が契機
  - ◆2州を除いて、通知または報告を義務づける州法を制定

EUのGDPRでは？

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■個人データ侵害の監督機関への通知（第33条）

1　個人データの侵害が発生した場合、管理者は、不当な遅滞なしに、可能であれば、侵害に気が付いてから72時間以内に、第55条に従って個人データの侵害を管轄監督機関に通知しなければならない。ただし、個人データの侵害により自然人の権利又は自由に対するリスクが生じ得ない場合を除く。監督機関への通知が72時間以内になされない場合には、遅滞に関する理由と共に通知されなければならない。　※55条は、管轄権に関する規定

2　取扱者は、個人データの侵害に気付いた後、不当な遅滞なしに管理者に通知しなければならない。

3　第1項で定める通知は少なくとも次に掲げる事項が含まれなければならない。

(a)個人データ侵害の性質の記述。可能であれば、関連するデータ主体の種類及び概数並びに関連する個人データの記録の種類及び概数を含む。

(b)データ保護オフィサーの氏名及び詳細な連絡先又はより情報が入手できるその他連絡先の通知。

(C)個人データ侵害に関する起こり得る結果の記述。個人データ侵害に対処するために管理者によって取られている又は取られることが意図された対策の記述。適切な場合、個人データ侵害により起こり得る悪影響を軽減するための対策を含む。

4 通知と同時に情報を提供することが不可能である場合、情報はさらなる不当な遅滞なしに段階的に提供されてもよい。

5 管理者は、個人データ侵害に関わる事実、その影響及び取られた救済手段を含め、あらゆる個人データ侵害を文書で残さなければならない。当該文書は監督機関が本条の遵守を確かめられるようにしなければならない。

■データ主体への個人データ侵害の通知（第34条）

1　個人データ侵害が自然人の権利及び自由に対して高リスクを引き起こし得る場合、管理者は、不当な遅滞なしにデータ主体に個人データ侵害について通知しなければならない。

2　本条第1項で定めるデータ主体への通知はデータ侵害の性質について明白で平易な文章で記述され、少なくとも、第33条第3項(b)号、(c)号及び(d)号で規定された情報並びに推奨事項を含むものとする。

3　第1項で定めるデータ主体への通知は、次に掲げるいずれかの状況に合致するのであれば、要求されない。

◆(a) 管理者が適切な技術的及び組織的保護対策を実施しており、当該対策が個人データ侵害によって影響を受ける個人データに適用されている場合。特に、暗号化のように、当該個人データにアクセスが許可されていないあらゆる人に対して個人データが判読できないといった対策

◆(b)管理者が、第1項で定めるデータ主体の権利及び自由に対する高リスクがもはや実現し得ないことを確実にする後続の対策をとった場合

◆(C)通知が過度な労力を伴う場合。この場合、代わりとして、公表又はそれに類似する対策がなければならず、それによってデータ主体が等しく効果的手法で通知されること。

4　管理者が個人データ侵害をデータ主体に未だ通知していない場合、監督機関は、高リスクを起こし得る個人データ侵害の可能性を考慮し、管理者に通知することを要求するか又は第3項で定めるいずれかの条件に合致することを決定できる。

■罰則

- ●セキュリティ侵害を監督機関に通知しなかった場合
- ●データ主体に通知しなかった場合

- ●制裁金
- ●企業の前会計年度の全世界の売上高の2パーセント以下、または1000万ユーロ以下のいずれか高い方

GDPRの通知義務

- 監督機関への通知を、本人通知よりも優先
- 監督機関の裁量で本人通知省略も可
  - 事業者監督の性質強い
  - 自己情報の流通への自己情報コントロール権の保障という契機は薄い
- 「個人データの侵害に気付いた後」
  - 不正アクセス等の即時的検知までは義務づけず(?)
  - 注意義務が問われる可能性は(?)

- 制裁金
  - up to 2 % of the total worldwide annual turnover
  - 「total worldwide」の解釈(?)
- 文書保存義務と監督機関の調査（第33条第5号）
  - 結果的に、不正アクセスやマルウェア等の具体的侵害行為の報告義務
- 各国法による上乗せ、横出し

オランダの場合

- データ処理及びサイバーセキュリティ通知義務法義務法(Data processing and Cybersecurity Notification Act)
  - 2016年11月23日可決
  - イギリスのEU離脱とEUによる一般データ保護規則（GDPR）の施行を踏まえる
  - セキュリティに関する新たな国内法制度を制定し、オランダのサイバーセキュリティの競争力強化

- 第1章　総則
  - 第1条　定義
  - 第2条　必須事業者の義務
  - 第3条　個人データ
  - 第4条　データ提供要請
- 第2章　通知義務
  - 第5条　適用範囲
  - 第6条　必須事業者のセキュリティ侵害通知義務
  - 第7条　データ提供義務
  - 第8条　別の定め
  - 第9条　秘密データの取扱い
- 第3章　附則規定
  - 第10条　施行日
  - 第11条　法律名の略称

- Data breach notificationから、cyber security notificationへ
- 必須事業者（第1条）vital operator
  - 製品またはサービスの事業者であって、その可用性及び信頼性がオランダ社会にとって必須の重要性を有しているもの
  - マルウェア感染その他のインシデントの発生時に治安・法務省の下にある国家サイバーセキュリティセンター(NCSC)に届け出ると共に、必要なデータを提供することを義務づけ

■通知義務

a. the nature and size of the breach or loss;

b. the estimated time of the start of the breach or loss;

c. the possible consequences of the breach or loss;

d. a prognosis of the recovery time;

e. if possible, the measures taken or the measures to be taken by the vital operator to limit the consequences of the breach or loss or to prevent repetition thereof;

f. the contact details of the official responsible for the notification.

■導入の可能性

●「国際的に共通して導入されていることに鑑みると、データ侵害通知制度を個人情報保護法に取り入れることが考えられるが、これについても形式的な報告や通知に終始しないようにすることが重要である」（石井夏生利『新版個人情報保護法の現在と将来―世界的潮流と日本の将来像―』（2017年、勁草書房）」491頁）

ID漏洩の今後

■課題

- ●監督機関への通知重視（EU型）か、本人の権利利益侵害防止重視（アメリカ型）か
  - ◆セキュリティ重視であれば前者
  - ◆自己情報コントロール権の保障重視であれば後者
- ●対象の要件
- ●法的義務づけかガイドラインか

■参考

- ●湯淺墾道「 アメリカにおける個人情報漏洩通知法制に関する考察」『情報ネットワークロー・レビュー』11巻（2012年）72-87頁
- ●金子啓子・湯淺墾道「Security Breach Notification Lawの再検討」日本セキュリティマネジメント学会2017年度全国大会（2017年7月30日・情報セキュリティ大学院大学）

■ 本講演は、科学研究費補助金「行政におけるデータの取扱いに関する法的規制の比較研究」（26380153）及び「適応的セキュリティ制御とプライバシー保護支援を可能とするビッグデータ流通基盤」（15H02696）の研究成果の一部です