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

2017年8月28日
デジタル・フォレンジック研究会
「法務・監査」分科会（第14期第2回）

セキュリティ侵害通知義務についてのEU及び米国の動き

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

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

EUの動き

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

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。

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

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。

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

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の通知義務についての考察

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

- ■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（？）

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

- ■制裁金
  - ■up to 2 % of the total worldwide annual turnover
  - ■「total worldwide」の解釈
  - ■売上高の挙証（？）
- ■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

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（Data Processing and Cybersecurity Notification Obligation 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

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

- Data breach nofiticationから、Cyber security notificatio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.

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

アメリカの動き

特色

- 個人に関する情報の漏洩は、アイデンティティ窃盗を引き起こすという観点から問題視
- 精神的・人格権的権利にかかわる問題であるからというよりも、経済的に大きな被害を生むアイデンティティ窃盗（identity theft）の原因となるため
- 特定領域連邦法規制
- 包括的州法規制
- 新たな連邦法化

連邦法

- 健康保険ポータビリティ及び説明責任法
  - Health Insurance Portability and Accountability Act, P.L. 104-191, 110 Stat. 1936 (1996), codified in part at 42 U.S.C. § § 1320d et seq.
- アメリカ復興・再投資法の一部である経済的・客観的な健康情報技術に関する法律
  - American Recovery and Reinvestment Act of 2009, P.L. 111-5, codified at 2 U.S.C. 661 et seq.
- グラム・リーチ・ブライリー法
  - Gramm Leach Bliley Act , Pub.L. 106-102, 113 Stat. 1338.

■アメリカ復興・再投資法

- ●健康保険ポータビリティ及び説明責任法のプライバシー基準及びセキュリティ基準を強化
- ●健康情報への侵害（breach）が発生した場合、または「保護される健康情報がセキュアでない（unsecured protected health information）」状態になった場合の通知・公表義務を明文で規定

■Sec. 13402

- ● (a)総則

本法の適用を受ける事業者であって、セキュアでない保護される健康情報（本条(h)項(1)号に定める）を、アクセス、保持、取得、修正、記録、保存若しくは廃棄その他の方法で保有、利用又は公開するものは、当該情報の侵害の発生が事業者によって発見されたときには、当該侵害の結果、セキュアでない保護される健康情報にアクセス、取得又は公開を受ける個人、若しくは受けることになると合理的に判断される個人に対して、当該侵害の通知を行わなければならない。

■個人に対する通知

- ●セキュリティ侵害の発生を事業者が知ったときから60日以内に原則として書面郵送
- ●個人が希望する場合は電子メールによる通知、個人の転居先が分からなくなっている場合等にはホームページへの掲載または主要なマスメディア等への掲載によって代えることもできる
- ●個人からの問い合わせを受ける無料電話を設置しなければならず、緊急性を有する場合には書面ではなく個人に電話で通知することも可

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

■通知内容

- ●侵害が発生した日時等の事案概要、侵害に含まれる項目（氏名、社会保障番号、生年月日、住所等）、侵害を受けた個人が被害に遭わないようにするための対処手段、侵害を受けた個人が被害を調査するための手段等

■このような通知を行った場合には、保健福祉長官にもその旨を報告

■保健福祉長官は、同省のホームページにセキュリティ侵害の通知に関する情報を掲載

州法

■カリフォルニア州法

- ●2002年に全米初のデータセキュリティ侵害通知法を制定
- ●個人情報の漏洩等のインシデントが発生した場合の公表義務と本人への通知義務を明文で規定
- ●漏洩等のセキュリティ侵害が発生した場合に公表・通知義務を負うことになる個人情報の種類を問わないこと、義務を負う者の業種等を問わない

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

- 1798.82(a)
  - いかなるカリフォルニアで事業を行う個人または団体であって個人情報を含むコンピュータ化されたデータを所有する又は権限を有するものも、カリフォルニアの居住者の暗号化されていない個人情報を含む又は含むと合理的に推定されるデータを権限のないものが取得してセキュリティ侵害が発生したときには、システムのセキュリティの侵害を公表するか、通知しなければならない。
- (b)
  - いかなる個人または団体であって当該個人又は団体が所有していない個人情報を含むコンピュータ化されたデータを運用するものも、カリフォルニアの居住者の暗号化されていない個人情報を含む又は含むと合理的に推定されるデータを権限のないものが取得してセキュリティ侵害が発生したときには、システムのセキュリティの侵害を公表するか、通知しなければならない。

■2017年4月時点
- ●48州で制定
- ●アラバマ州、サウスダコタ州が未制定
- ●コロンビア特別区、グアム、プエルトリコも制定

■クレジットカード情報漏洩時のsecurity freeze law
- ●全州で制定済

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

■対象となる「個人情報」、順守義務を負う者の範囲、何が侵害に該当するか、通知義務の内容、例外等にばらつき

■対象となる「個人情報」
- ●氏名と以下の情報の組合せで漏えいした場合
  - ◆ソーシャル・セキュリティ番号、運転免許証番号及び/又は
  - ◆暗証番号と共に口座番号、クレジット番号、デビッドカード番号

■侵害の定義

- ●暗号化又はreductされていない電子化されたデータのオーソライズされていない取得またはアクセスにより「個人情報」のセキュリティ、機密性又は完全性が損なわれること
- ●現実の危険性要件なし or 経済的損失やなりすまし、詐欺など、危害が起こりうる実質的レベルのリスクがあることなどの基準を伴っている

監督機関への届出の状況

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

■ニューヨーク州の場合

Data Security Breach Cause	Number of Breaches (% of Total)	NY Personal Records Exposed (% of Total)
External systems breach	519 (40.48%)	1,102,258 (69.05%)
Inadvertent disclosure	312 (24.34%)	304,277 (19.06%)
Other (i.e. skimming)	180 (14.04%)	50,313 (3.15%)
Insider wrongdoing	105 (8.19%)	7,300 (0.46%)
Loss of device or media	61 (4.76%)	9,607 (0.60%)
Merchant breach	38 (2.96%)	35,930 (2.25%)
Theft of device or media	19 (1.48%)	3,270 (0.20%)
Law enforcement recovery	18 (1.40%)	6,468 (0.41%)
Unauthorized access	13 (1.01%)	68,839 (4.31%)
Internal systems breach	10 (0.78%)	7,453 (0.47%)
Unknown	7 (0.55%)	492 (0.03%)
Total	**1,282**	**1,596,207**

https://ag.ny.gov/press-release/ag-schneiderman-announces-record-number-data-breach-notices-2016

日本法への影響

通知義務

■マイナンバーの場合

■マイナンバー法により委員会への報告義務

●（特定個人情報の漏えい等に関する報告）
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。

■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）

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

■検討課題

●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

●オランダ型はあり得るか（セキュリティ＋自己情報コントロール）

■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）

■ 本報告は、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