個人情報漏洩に関する法制度の動向

2016.11.28.
小向　太郎 Taro KOMUKAI, Ph.D.
日本大学　危機管理学部　教授

1. デジタル・ネットワークと情報漏洩
   - 1-1.　デジタル・ネットワークと個人情報
   - 1-2.　個人情報漏洩
   - 1-3.　3つのアプローチ

2.　個人情報漏洩に関する法制度
   - 2-1.　日本
   - 2-2.　米国
   - 2-3.　EUと英国

3.　制度の比較と課題
   - 3-1.　制度比較
   - 3-2.　法的アプローチの位置付け
   - 3-3.　情報漏洩に関する制度の課題

IFIP TC9 Human Choice and Computers Conference（2016）

Comparative Legal Study on Data Breach among Japan, the U.S., and the U.K.

Kaori Ishii[1] and Taro Komukai[2]

[1] Faculty of Library, Information and Media Science, University of Tsukuba, Tsukuba, Japan
kaoriish@slis.tsukuba.ac.jp
[2] InfoCom Research, Inc., Tokyo, Japan
komukai@icr.co.jp

Abstract. This paper focuses on the liability and duties of data controllers regarding data leaks and compares the relevant legal schemes of Japan, the U.S., and the U.K. Data leaks can cause two types of concerning issues. One is the privacy risk caused by the wide circulation of personal data and the other is the risk of economic damage.

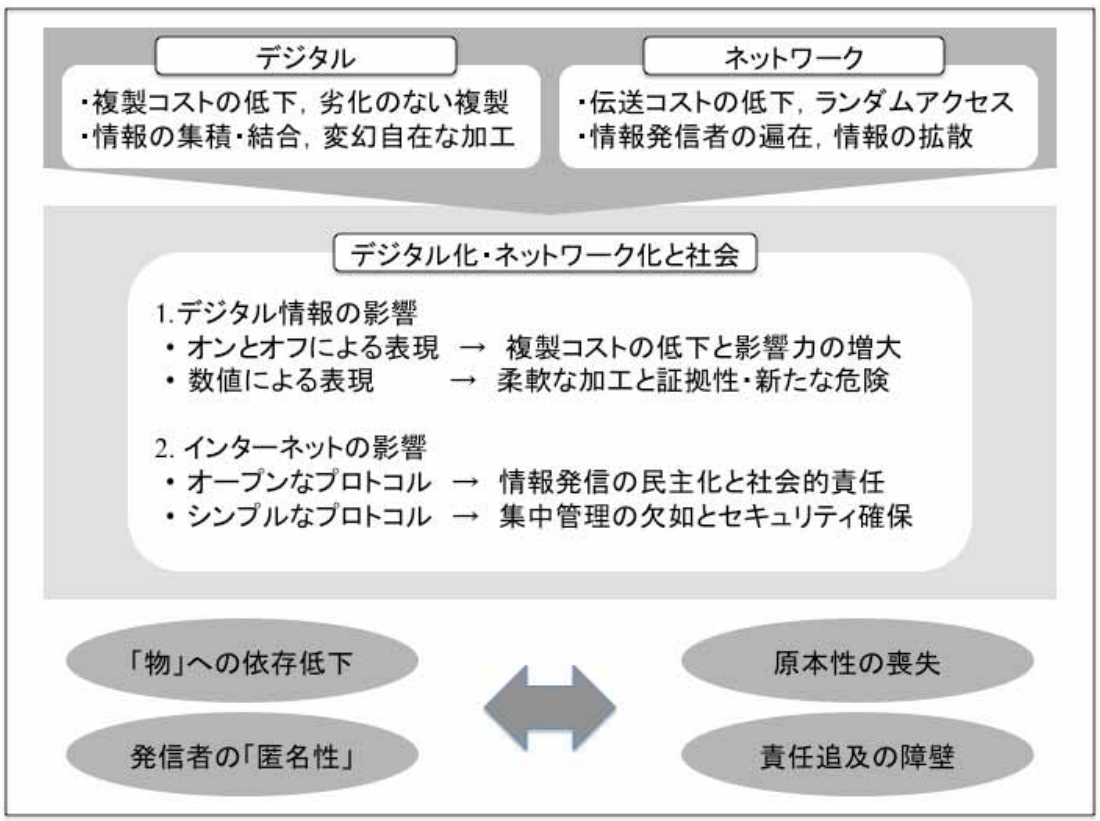
In Japan, rather than monetary compensation based on tort liabilities, companies confront severe condemnation regarding their leaks from the general public and mass media. In the U.S., there are many class actions seeking compensation for data leaks caused by hacking and malware and the compensatory amounts are generally high. In the U.K., there are not as many leaks as in the U.S., and few cases seem to lead to the economic damages that result from fraudulently using credit card information.

Currently, making the use of breached data for a criminal offense in Japan and the U.K. does not seem to be as pressing as in the U.S. It is expected that the introduction of a data breach notification rule in the U.K. will improve the transparency of data circulation. It will be necessary to review whether the data breach notification rule is not only effective for addressing the criminal use of breached data, but also it increases the transparency of data circulation and reduces inadequate data flows, especially during the reform process of the EU data protection framework.

http://hcc12.net

1. デジタル・ネットワークと情報漏洩

1-1. デジタル・ネットワークと個人情報



出典：小向太郎『情報法入門（第3版）デジタル・ネットワークの法律』NTT出版（2015）

1-2.　個人情報漏洩

- ベネッセ
  - 業務委託先元社員が、約3,504万件分の情報を名簿業者3社へ売却
  - 名前、性別、生年月日、郵便番号、住所、電話番号、出産予定日、メールアドレス
- 日本年金機構
  - 外部から送付された 不審メールに起因する不正アクセスにより、個人情報 (約 125 万件) が外部に流出
  - 基礎年金番号、氏名、生年月日、住所

ベネッセと日本年金機構

	ベネッセ	日本年金機構
セキュリティ体制	入退室管理、監視カメラ、ワイヤーロックによる施錠、持ち出し禁止、認証IDパスワードの定期更新、端末設定の変更禁止、外部ストレージの制御等	オフラインの基幹系システムでの管理、メール・アクセスログの採取
問題点	モニタリングとアラートの不足、書き出し制御のバグ、きめ細かなアクセス権限管理の不足	2010年以降LANシステムにコピー（アクセス制限のないデータ約55万件）、モニタリング、対応指針、決定権者の不在
特記事項	「具体的なリスクと想定した上での、二重、三重の対策を講じるといった徹底的な体制までは構築できていなかった」「社内の人間が悪意を持って大量の個人情報を持ち出すことはあり得ないという意識を持っていた可能性が高い」	「情報セキュリティアドバイザには、統括情報セキュリティ責任者が所属する部署内の、情報セキュリティスペシャリスト等の資格を有する職員1名が任命されていたが、この職員は役員や管理職などの判断件者に対して率直に進言できるような職位にはなかった」

アプローチ	概要
①被害者救済	• 損害賠償請求：不法行為責任、 法定の補償等
②安全確保	• 情報セキュリティ義務：安全管理措置義務
③被害把握	• データ侵害通知：監督機関、 本人への通知

2.　個人情報漏洩に関する法制度

情報漏洩に対する補償	不法行為責任 （民法709条、710条、715条）
安全管理措置義務	個人情報取扱事業者の義務 （個人情報保護法20条）
データ侵害通知	情報漏洩に関する報告の推奨 （内閣：個人情報の保護に関する基本方針）

我が国における係争事例

事件	事案概要	問題とされた点	損害賠償	情報（件数）
宇治市住民票データ流出事件（最決平14.7.11）	データの処理を委託していた事業者の再々委託先のアルバイトが、名簿業者に販売、インターネット上に流出	再委託を安易に承認、再委託先との間で秘密保持の取決めなし、作業が終了しなかっただけで安易に社外での作業を承諾し管理上特段の措置を取った形跡がない等	原告一人当たり慰謝料10,000円および弁護士費用5,000円（民法第715条）	京都府宇治市の住民基本台帳データ（約21万件）
Yahoo!BB顧客情報流出事件（最決平19.12.14）	ISPの業務委託先から派遣されて顧客データベースのメンテナンスを行っていた者が、業務終了後にリモートアクセスし、顧客情報を取得	リモートアクセスの危険性を考えれば、アクセス管理等の企業として果たすべき管理義務が十分果たされていない	原告一人あたり慰謝料5,000円および弁護士費用1,000円（民法709条、710条）	ISPサービスの加入者の個人情報（合計約1,100万）
TBCアンケート情報流出事件（東京高判平19.8.28）	サーバのメンテナンス時に、インターネットに接続されているサーバに、アクセス制限のない状態で保存	情報の性質からも精神的苦痛が大きい	慰謝料30,000円および弁護士費用5,000円（民法715条）	エステティックサロンのアンケート回答

出典：小向太郎『情報法入門（第3版）デジタル・ネットワークの法律』NTT出版（2015）

法執行の動向

主務大臣による法執行の動向

Fiscal year	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
Reports requiring (Article 32)	87	60	83	28	18	15	16	8	2	3
Advice (Article 33)	0	0	1	0	0	0	1	1	0	0
Recommend ations (Article 34)	1	4	0	0	2	0	0	0	0	1

（出典）消費者庁「「個人情報の保護に関する法律施行状況の概要」（平成17年～26年）

情報漏洩に関する政府への報告

「二次被害の防止、類似事案の発生回避等の観点から、可能な限り
事実関係等を公表することが重要（個人情報の保護に関する基本方針）」

年度	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
件数	1,556	893	848	538	490	413	420	319	366	338

出典：消費者庁「個人情報の保護に関する法律施行状況の概要」
（平成17～２６年年度）

情報漏洩に対する補償	不法行為責任（コモン・ロー）
安全管理措置義務	不公正または欺瞞的な行為または実務の禁止（FTC法5条）
データ侵害通知	司法長官への報告と情報の開示 （各州法、最初の制定はカリフォルニア州）

米国におけるハッキングによる大規模漏洩

日時	企業・団体名	業種	漏洩した情報	漏洩件数
April 27, 2011	Sony PlayStation Network (PSN), Sony Online Entertainment (SOE)	ゲーム販売	氏名、住所、性別、emailアドレス、生年月日、ログインネームとパスワード、電話番号、オンラインID、購買履歴、請求先住所、秘密の質問、クレジットカードおよび銀行のアカウント	約10,160万件(1,200万件の暗号化されないクレジットカード番号)
December 13, 2013	Target	流通	氏名、クレジット・デビットカード番号、有効期限、セキュリティコード	約4,000万件(最大11,000万件とも報じられる)
May 21, 2014	eBay	ネットオークション	emailアドレス、暗号化されたパスワード、生年月日、住所（ファイナンシャルデータ、ペイパルのデータベースは漏洩していない）	約14,500万件
August 28, 2014	JP Morgan Chase	金融保険	氏名、住所、電話番号、emailアドレス、（金融情報や銀行口座情報にはアクセスされていない）	約7,600万件
February 5, 2015	Anthem	金融保険	氏名、生年月日、医療ID、社会保障番号、住所、emailアドレス、雇用および収入の情報	約8,000万件

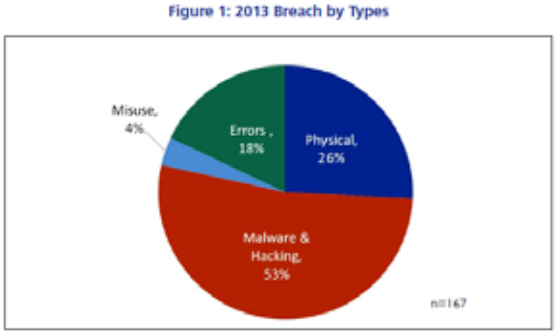
情報セキュリティに関するFTCの法執行例

	対象者 日付	問題とされた行為	エンフォースメント
1	Wyndham Worldwide Corp. 06/26/2012	ホテルチェーンが、情報システムのセキュリティ・ホールを放置したため、数百万ドルの詐欺による損失を生じた他、ペイメントカード情報がロシアドメインのサイトに流出した	違反行為の差止、被害者救済のための金銭的賠償、訴訟費用の支払等（司法法的措置→係争中）
2	Cbr Systems, Inc. 05/03/2013	大手臍帯血バンクが、自社システムにおいて適切な情報セキュリティ対策を取らなかったことで、SSNやクレジットカード、センシティブな健康情報等を危険にさらした	包括的な情報セキュリティプログラムを実施し、第三者によるセキュリティ・アセスメントを2年ごとに今後20年間行うこと等（行政的措置）
3	HTC America 07/02/2013	モバイル端末の脆弱性に対処せずに出荷した	セキュリティパッチの開発・提供、セキュリティプログラムの実施、今後20年間の年次第三者評価実施等（行政的措置）
4	TENDnet 02/07/2014	家庭用遠隔モニターカメラのシステムのセキュリティが不十分で、インターネット上でモニタ画面が公開された	セキュリティに関する事実隠蔽の禁止、顧客への情報提供の実施、包括的な情報セキュリティプログラムの実施、第三者によるセキュリティ・アセスメント（2年毎20年間）等（行政的措置）
5	Fandango, LLC Credit Karma 08/19/2014	提供するモバイルアプリが、保護手段を講じずにクレジットカード情報やSSNを晒していた送信しており、第三者に取得される危険に晒していた	包括的な情報セキュリティプログラムの実施、第三者によるセキュリティ・アセスメント（2年毎20年間）等（行政的措置）
6	GMR Transcription Services, Inc. 08/21/2014	医療情報のトランスクリプト会社が、委託先企業のセキュリティ対策が不十分だったために、顧客の医療履歴や検査結果等の情報がインターネット上に公開された	消費者のセキュリティとプライバシーに関する保護状況についての公表、包括的な情報セキュリティプログラムの実施、第三者によるセキュリティ・アセスメント（2年毎20年間）等（行政的措置）

小向太郎「米国FTCの消費者プライバシーに関する法執行の動向」
堀部政男編著『情報通信法制の論点分析』商事法務別冊NBLNo.153(2015年)

データ侵害通知に対する評価

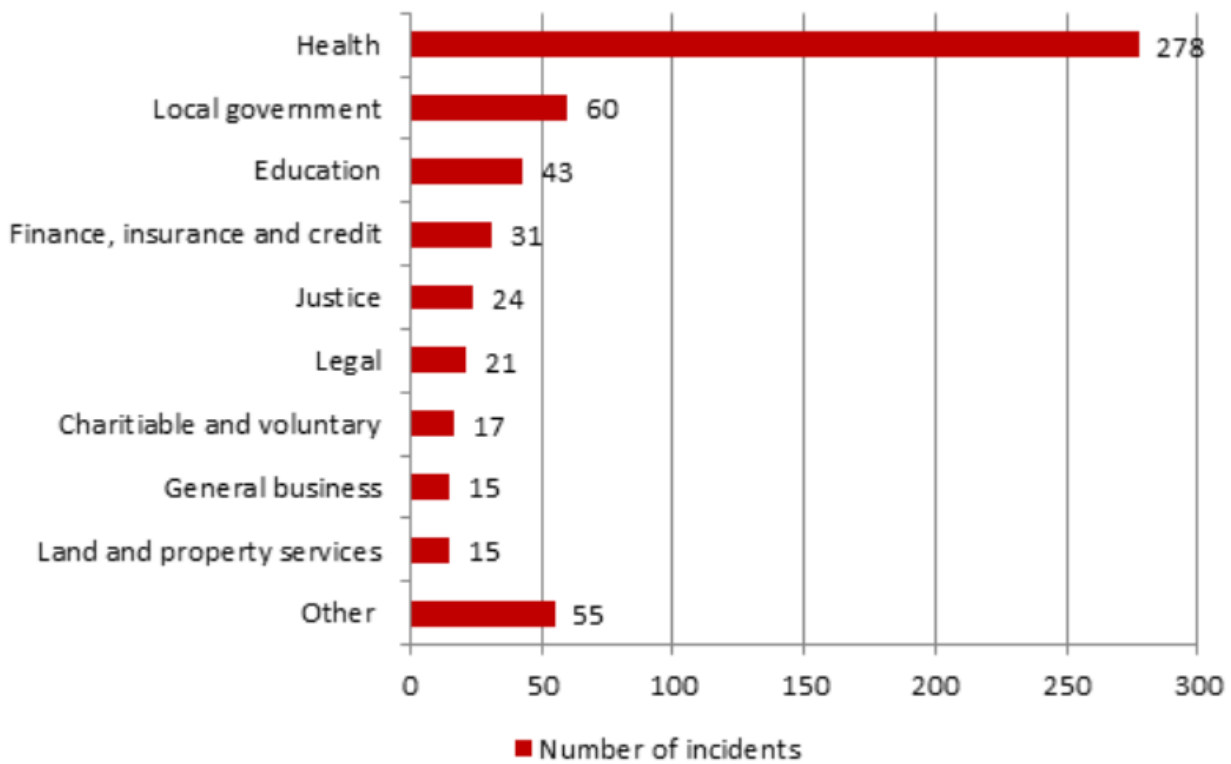
- 2012年に167件の侵害（500人超）が報告
- 具体的な犯罪を想定したペイメント・カード情報等への攻撃が過半
- 被害を防ぐ事後対策の重要性を強調



出典：Kamala D. Harris, California Data Breach Report 2014.

情報漏洩に対する補償	補償を受ける権利（データ保護法13条）
安全管理措置義務	個人データは公正に適法に処理されなければならない（第１原則） 適切な技術的および組織的な方法が取られなければならない（第７原則）
刑事罰	個人データの不正な取得と提供は処罰および押収命令の対象
データ侵害通知	監督機関と情報主体への通知（EU一般データ保護規則） 通信および医療分野におけるデータ侵害通知義務

データセキュリティに関するインシデントの動向（英国）



Source: ICO, Data security incident trends, https://ico.org.uk/action-weve-taken/data-security-incident-trends/

英国の情報漏洩事例

時期	企業・団体名	業種	漏洩情報	原因	件数
2007	HM Revenue & Customs	政府機関	児童手当の記録	CD-ROMの紛失	約2,500万件
2008	T-Mobile	電気通信	顧客情報	営業員がデータブローカーに売却	数百万件
2011	Sony Computer Entertain-ment Europe Limited	ゲーム会社	氏名、住所、 email アドレス、生年月日、パスワード、ペイメントカード情報	ハッキング	最大300万件
2012	Think W3 Limited	オンライン旅行代理店	クレジットカード、デビットカードの記録	ハッキング (SQLインジェクション攻撃)	1,163,996件
2014	Mumsnet	子育てネットワーク	ユーザ・アカウント	ハッキング	約150万件
2015	Moonpig	オンライン販売	顧客登録情報	ハッキング	約300万件

This chart was made with information from the case list of the ICO, https://ico.org.uk/action-weve-taken/enforcement/

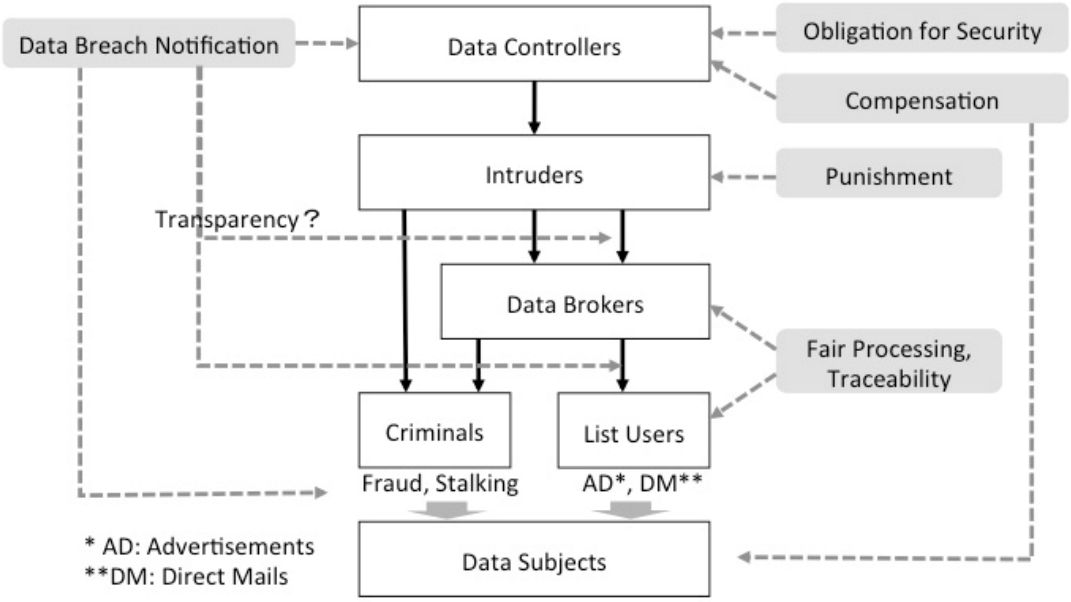
3. 制度の比較と課題

3-1. 制度比較

種類	日本	米国	英国
①被害者への補償	不法行為責任：民法710、715条等	不法行為責任：コモンロー（クラスアクションあり）	データ管理者の違反等への補償：データ保護法13条
②データセキュリティ義務	安全管理措置義務：個人情報保護法20条等	不公正または欺瞞的な行為または実務の禁止：FTC法第5条	技術および組織上の安全管理措置義務：第7原則
③データ侵害通知	報告の推奨(特別法、基本方針)	本人等への通知・公表、司法長官への報告：加州データ侵害通知法等	（監督機関、本人への通知：EU一般データ保護規則案)

3-2. 法的アプローチの位置付け

- データ侵害通知は二次被害の防止に一定の効果が認められる
- 拡散防止や透明性確保にも有効かどうかを評価する必要がある



出典：Kaori Ishii and Taro Komukai, *Comparative Legal Study on Data Breach among Japan, the U.S., and the U.K.,* 12th IFIP TC9 Human Choice and Computers Conference（2016）.

- 二種類のリスク
  - 情報の流通による心理的または潜在的リスク：英国、日本
  - 漏洩情報を利用した犯罪による現実的リスク：米国

- 被害を減らすために求められる取り組み
  - 個人情報を利用して行われる犯罪行為の防止における漏洩に関する情報の利用
  - 個人情報の取得・利用・提供に関する透明性の向上
  - データ侵害通知を促進させるような制度設計（過度な負担の回避、モチベーション等）　等