米国データセキュリティ法の課題と日本への示唆

2024.03.21.
小向　太郎 Taro KOMUKAI, Ph.D.
中央大学　国際情報学部　教授
大学院国際情報研究科　教授

1. データセキュリティ法とは
    1. 情報セキュリティに関する制度的アプローチ
    2. 情報漏洩に関する制度
    3. 日本における情報漏洩事例
2. 米国のデータセキュリティ法
    1. 米国における情報漏えい
    2. ターゲット事件
    3. 不法行為と「損害」の発生
3. データセキュリティ法の課題
    1. データセキュリティ法の迷走
    2. ソロブ=ハーツォグの提言
    3. 今後の課題と示唆

自己紹介：小向太郎

中央大学　国際情報学部　教授

情報通信総合研究所取締役法制度研究部長、早稲田大学客員准教授、日本大学教授等を経て、2020年より現職

【専門分野】

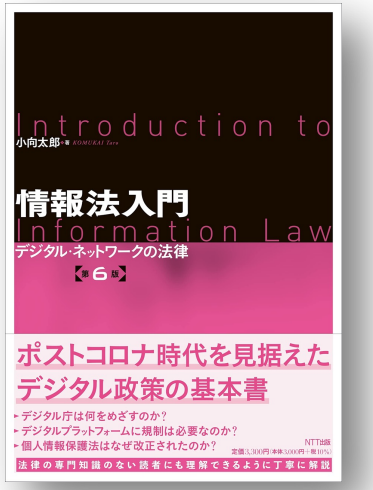
情報法、情報通信法

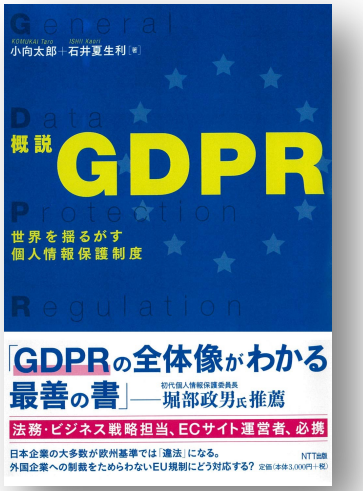
【主な著書・訳書】

『データセキュリティ法の迷走』監訳、勁草書房、2023年

『情報法入門（第6版）デジタル・ネットワークの法律』NTT出版、2022

『概説GDPR～世界を揺るがす個人情報保護制度』共著、NTT出版、2019





1.　データセキュリティ法とは

1-1. 情報セキュリティに関する制度的アプローチ

- データ侵害を防止するために、下記のようなアプローチが取られている
- このうち、「③情報漏洩の防止・救済」のための制度が、データセキュリティ法とよばれている

種類	概要	対象
①脅威となる行為の禁止	• 加害行為（情報の盗取、停止・破壊、無権限操作等）の禁止	侵害者
②政府による対策の強化	• 政府のセキュリティレベル向上 • 情報セキュリティのリソースの提供	政府機関等
③情報漏えいの防止・救済	• 安全管理措置義務等 • データ侵害通知 • 民事的責任：媒介者、漏洩等	情報管理者

（参考）脅威となる行為の禁止

種類	行為	罪名等
準備・手段	不正アクセス，フィッシング	不正アクセス禁止法違反
	マルウェア作成・頒布	不正電磁的記録作成等の罪
情報の盗取	営業秘密侵害	不正競争防止法違反
	特定秘密侵害	特定秘密保護法違反
停止・破壊	DDos攻撃，シャットダウン，データ身代金要求等	電子計算機損壊等業務妨害罪，業務妨害罪，脅迫罪　等
無権限操作	Webページの書き換え，データの改竄等	電磁的記録不正作出罪，業務妨害罪等
	不正送金，データ身代金奪取	電磁的記録不正作出罪，詐欺罪，窃盗罪　等
	設備や機械の無断操作	業務妨害罪　等

出典：小向太郎『情報法入門』（NTT出版、第6版、2022年）188頁

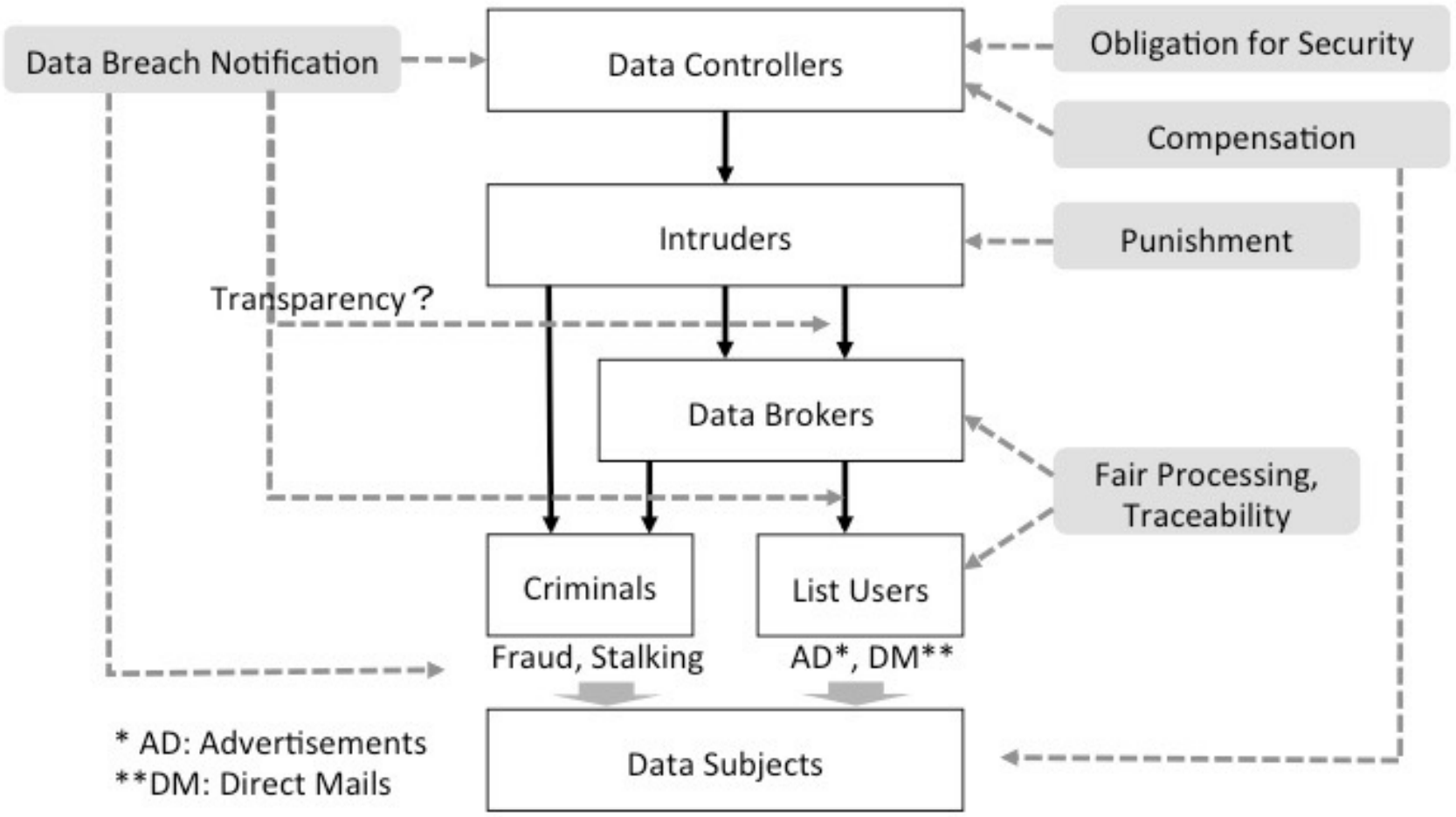
1-2. 情報漏洩に関する制度

- 不法行為責任は本来、損害を補償するためのものであり、副次的に抑止効果が期待される
- 情報セキュリティ対策のレベルを向上させるための制度としては、安全管理措置義務、データ侵害通知、トレーサビリティ等がある

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、補償等
②安全性の向上	情報セキュリティ義務：安全管理措置義務
③透明性の向上	データ侵害通知：監督機関、本人への通知 トレーサビリティ：情報の取得や提供の記録義務

出典：小向太郎「情報漏洩事案でデジタル・フォレンジックはどう使われるか」安冨潔・上原哲太郎編著『基礎から学ぶデジタル・フォレンジック』（日科技連、2019）115-118頁

（参考）法的アプローチの位置付け



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）.

1-3. 日本における情報漏洩事例

事件	事案概要	問題とされた点	賠償額（一人）	情報（件数）
2002年 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り決めなし，安易に社外での作業を承諾　等	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）
2007年 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（民法第709条，第710条）	ISPサービスの加入者の個人情報（合計約1,100万件）
2007年 TBCアンケート情報流出事件（東京高判平19.8.28）	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（民法第715条）	エステティックサロンのアンケート回答
2016年 ベネッセ顧客情報流出事件（大阪高判令元.11.20）	システム開発・運用を行っていた委託先の従業員（SE）が，顧客等の個人情報を不正に持ち出して販売	委託先企業にデータ書き出し制御の措置を講ずるべきなどの注意義務が果たされていない	慰謝料1,000円（民法第719条）	顧客情報（約3,504万件）

出典：小向太郎『情報法入門』（NTT出版、第6版、2022年） 168頁

2.　米国のデータセキュリティ法

2-1. 米国における情報漏えい

- 情報漏洩による被害は増加の一途をたどっており、当初から深刻な経済的被害が問題視されてきた
- 被害は深刻化しているが漏洩の要因にはあまり変化がない
  - 巨額の投資だけでは不十分
  - 人為的ミスが端緒になる
  - 多大なデータが（区分されずに）保持されている
  - デバイスは紛失されやすい
  - データが暗号化されていない
  - 全てがワンクリックで決まる
  - 教訓が活かされていない
  - 侵害はしばしば、不注意な単純ミスに起因する

出典：ダニエル・J・ソロブ、ウッドロウ・ハーツォグ『データセキュリティ法の迷走』（勁草書房、2023年）38-45頁

2-2. ターゲット事件（概要）

- 2013年の年末にサイバー攻撃を受け、約4,000万人の決済情報と約7,000万人の消費者の個人情報が流出、ハッカーが闇取引サイトでデータを販売
- 年末商戦の利益46%の落ち込みと、訴訟やセキュリティ対応費用（2016年3月の年次報告書では、損害を2億9100万ドルと推計）
- 消費者訴訟の和解金は、1,000万ドル（一人当たり数セント）
- 各州政府が調査を行っていたが、2017年5月にターゲットが、1850万ドルを支払うことで和解したと報じられている

出典：ダニエル・J・ソロブ、ウッドロウ・ハーツォグ『データセキュリティ法の迷走』（勁草書房、2023年）10-11頁

2-2. ターゲット事件（漏洩経緯）

- ターゲットには300人以上の情報セキュリティのスタッフがいた。ミネソタ州ミネアポリスに大規模なセキュリティ・オペレーション・センターがあり、バンガロールにはセキュリティ専門チームが置かれ、24時間365日コンピュータネットワークを監視していた
- 2013年5月、ハッキングのわずか六か月前に、ターゲットはサイバーセキュリティ企業のファイヤーアイ（Fire-Eye）から高価で高性能なマルウェア検出ソフトウェアを導入していた
- 数百万ドルの投資、最先端のセキュリティソフトウェア、数百人のセキュリティ担当者、24時間体制の監視。ターゲットのセキュリティには、いったいどこに問題があったのだろうか
- ターゲットの仕事をしているペンシルバニア州にある空調会社ファツィオ・メカニカル（Fazio Mechanical）の従業員が、ハッカーから送られた詐欺メールの添付ファイルを開いてしまい、そのメールに隠されていたマルウェアであるトロイの木馬が、ファツィオの管理者権限を奪取したのだ

出典：ダニエル・J・ソロブ、ウッドロウ・ハーツォグ『データセキュリティ法の迷走』（勁草書房、2023年）38-45頁

2-3. 不法行為と「損害」の認定①

- プロッサーの4類型
  - ① 他人の干渉を受けずにおくっている隔離された私生活への侵入
  - ② 他人に知られたくない事実の公表
  - ③ 一般の人に誤った印象を与えるような事実の公表
  - ④ 営利目的での氏名や肖像などの不正利用
- 原告適格（損害がなければ訴え却下）
  - 合衆国憲法第3条に基づき原告が訴訟を起こす資格
  - 事実上の損害：具体的かつ特定的で、「思い込みや仮定のものではなく、実際または差し迫ったもの」でなければならない
- 訴因（認められなければ請求棄却）
  - プロッサー4類型の典型的なケースでは、損害の存在を推定する傾向
  - それ以外の場合は、損害の認定がされない事が多い

出典：Daniel J. Solove and Danielle Keats Citron, Risk and Anxiety: A Theory of Data Breach Harms, 96 Texas L. Rev. 737 (2018).

2-2. 不法行為と「損害」の認定②

① 将来の損害リスク
- 単にデータが漏洩しただけでは、データを入手した者の動機は不明であり、ID 窃盗やその他の金融詐欺による「事実上の損害」が発生していない。
- ハッカーの悪意ある動機が推察されるようなケースでも、認識可能な損害とは認められない 。

② 予防コストの損害
- 情報漏えいによって生じうる将来の損害のリスクを事前に予防するために時間やコストがかかることを「事実上の損害」とは認められ難い.

③ 不安の損害
- 個人情報の盗取や悪用リスクの増加による原告の 恐怖，不安，精神的苦痛は，損害であると認めるには足りない

「被害が直感的で、目に見えるもので、定量的に測定可能なものであることが必要であり、物理的、金銭的、または財産的損害があるか、少なくとも差し迫っていなければ損害が認められない」

出典：Daniel J. Solove and Danielle Keats Citron, Risk and Anxiety: A Theory of Data Breach Harms, 96 Texas L. Rev. 737 (2018).

（参考）日本における情報漏えいと損害

- ベネッセ顧客情報流出事件
  - 大阪高裁「プライバシーの侵害による上告人の精神的損害の有無及びその程度等について十分に審理することなく，不快感等を超える損害の発生についての主張，立証がされていない」ことを理由に請求を棄却（大阪高判平28年6月29日判タ1442号48頁）
  - 最高裁「氏名，性別，生年月日，郵便番号，住所及び電話番号並びにBの保護者としての上告人の氏名といった上告人に係る個人情報」は，「上告人のプライバシーに係る情報として法的保護の対象となるというべき」であり，本件の漏えいによって侵害が生じている（最二小判平29年10月23日判タ 1442号46頁）
- 先行裁判例
  - 早稲田大学江沢民主席講演会名簿提出事件（最二小判平成15年9月12日）
  - Yahoo!BB顧客情報流出事件（大阪地判平成18年5月19日）

3.　データセキュリティ法の課題

3-1. データセキュリティ法の迷走

- データセキュリティ法は、情報漏洩を起こした企業の責任を厳しく追及すれば情報漏洩を根絶できるという、間違った考えに取り憑かれている

種別	概要	問題点
侵害通知法	情報漏洩等のデータ侵害があった場合に、規制機関や本人に通知することを義務付ける	侵害が起こったことを知るのには役に立つが、侵害を防いだり抑制したりする役には立たない
安全保護法	データを保有している組織に情報セキュリティ対策を義務付ける	義務付ける対策を具体化することは難しいし、法執行を迅速に行うことも難しい。 罰則等を課しても、被害者の救済に繋がらない
私的訴訟	被害者が漏洩企業に対して、損害賠償等を求めて訴訟を提起する（集団訴訟など）	データ侵害が被害者にもたらす危険や不安は「法的に認識可能な損害」と認められず、十分な補償が受けられないことが多い

出典：ダニエル・J・ソロブ、ウッドロウ・ハーツォグ『データセキュリティ法の迷走』（勁草書房、2023年）278-279頁

（参考）情報漏洩はなぜなくならないのか

- 第４章　全体像
  - 完璧なセキュリティを求めることは現実的ではないし、望ましいことでもない
  - 情報システムには、利便性も求められる。そして、多くの場合セキュリティ対策は利便性を損なう
  - 技術的に厳格な対応を無理に求めれば、現場では無視されてしまう
- 第５章　データエコシステム全体の責任
  - 情報漏洩のきっかけを作ってしまった不注意な人間や、それを防げなかった企業を責めたてても、漏洩はなくならない
  - 脆弱なソフトウェアやデバイスを提供する事業者、悪質な広告を掲載するアドネットワークやウェブサイト、アプリの審査が不十分なプラットフォーム、脆弱性を隠して取締りなどに使おうとする政府関係者、誤ったセキュリティ教育を行う組織など、情報漏洩を起こりやすくする関係者は他にもたくさん存在している

出典：ダニエル・J・ソロブ、ウッドロウ・ハーツォグ『データセキュリティ法の迷走』（勁草書房、2023年）279-281頁

（参考）情報漏洩はなぜなくならないのか

- 第６章　データ侵害による損害を軽減する
  - 現在のデータセキュリティ法が、損害の軽減という本来の使命を果たしていない
  - なりすましの被害にあってしまうと、そのダメージは延々と続き、いつまでももとの生活を取り返すことができない
  - 金銭を取られ、信用を毀損され、犯罪者と間違えられて逮捕されてしまうことさえある
  - なりすましは犯罪として禁止されているが、取締が積極的に行われることは少ない
  - クレジットカード発行の際の審査がずさんなことも、なりすましを容易にしている
  - 社会保障番号（ＳＳＮｓ）が本人確認のためのパスワードのように使われていることも被害に拍車をかけている

出典：ダニエル・J・ソロブ、ウッドロウ・ハーツォグ『データセキュリティ法の迷走』（勁草書房、2023年）279-281頁

（参考）情報漏洩はなぜなくならないのか

- 第７章　プライバシーとデータセキュリティの統合
  - 法律も実務も、プライバシーとセキュリティは別のものと考える傾向があり、多くの組織で別の部門が担当している
  - 情報システムを担当する部署はプライバシーやデータの保護を十分に考えない設計を行ってしまう
  - 例えば、誰にどのデータへのアクセスを許すべきかというプライバシーの基本が、セキュリティでは軽視されてしまう
  - ケンブリッジ・アナリティカの事件で、フェイスブックの幹部が、権限のある人間がアクセスしていたことを理由に「これはデータ侵害ではない」と抗弁したのはその典型例である
  - ランサムウェアの拡大で、こうした脅威は増大しており、プライバシーとセキュリティをトータルで考えることがより重要になっているとも指摘する。

出典：ダニエル・J・ソロブ、ウッドロウ・ハーツォグ『データセキュリティ法の迷走』（勁草書房、2023年）279-281頁

（参考）情報漏洩はなぜなくならないのか

- 第８章　人間という最大の弱点のためのセキュリティ設計
  - 人間は、怪しげなリンクをクリックしたり、ノートパソコンを紛失したり、認証情報をうっかり公開してしまったり、プログラムや証明書のアップデートをしなかったり、安易なパスワードを使い回したりしてしまう
  - 杓子定規にルールに従えと言っても人々は従わない
- 制度的に促すべきセキュリティデザイン例
  - ①　デフォルト設定の変更
    例：初期パスワードは強制的に変更させる
  - ②　相互の信頼の促進
    例：企業側にも本物であることの認証を義務付ける
  - ③　バランスのとれたセキュリティ対策の促進
    例：非現実的な対策ではなく現実的な対策を推奨する
  - ④　意味のある警告の発信
    例：本当に重要なシグナルだけを送るようにさせる

出典：ダニエル・J・ソロブ、ウッドロウ・ハーツォグ『データセキュリティ法の迷走』（勁草書房、2023年）279-281頁

3-2. ソロブ=ハーツォグの提言（抜粋）

- 事後対応よりも**事前対応**を重視すべきである
- データ・エコシステム内でデータ侵害の原因を起こしうる**すべての関係者に責任**を課すべきである
- データ侵害の**被害を軽減**することを目指すべきである
- 機械的な**チェックリストを推奨するのはやめる**べきである
- 法律における**プライバシーとセキュリティの統合**を進めるべきである
- システムにおける**人的要素を考慮**したセキュリティ・バイ・デザインを要求または奨励すべきである
- **統一的で負担の少ないセキュリティの基準**を促進して、人々が適正な期待と知識を持てるようにすべきである

出典：ダニエル・J・ソロブ、ウッドロウ・ハーツォグ『データセキュリティ法の迷走』（勁草書房、2023年）266-274頁

3-3.今後の課題と示唆

- 情報漏えいはなくならない
  - 情報管理者を責めるだけの制度は機能しない
  - 情報セキュリティ対策の動機を高めることが重要
  - 形骸化しないための工夫が必要
- 脆弱性を生み出すもとを少なくする
  - IoT機器を購入したユーザがセキュリティ対策をすると考えるのは、前提が間違っている
  - 情報システムやデバイスは、セキュリティを統合した形で、提供される必要がある
- 「侵害通知」を処罰にしてはならない
  - そもそも、データ状況の透明性を高めるためのもの
  - 被害拡大の防止に役立てることが重要
  - 対策に必要不可欠な情報共有が阻害されていないか