DXにおける情報リスクとセキュリティ（法制度）

2022.03.17.
小向　太郎 Taro KOMUKAI, Ph.D.
中央大学　国際情報学部　教授

1. DXと情報セキュリティ
    1. DXと情報リスクの拡大
    2. 情報セキュリティに関する法制度
    3. 情報漏えいの防止義務
2. 情報漏えいに関する制度
    1. 被害者救済
    2. 安全管理措置義務
    3. データ侵害通知
3. 制度の課題
    1. 個人情報保護と情報セキュリティ
    2. Solove & Hartzog, “Breached!”
    3. 情報セキュリティ対策を促す制度

自己紹介：小向太郎

中央大学　国際情報学部　教授

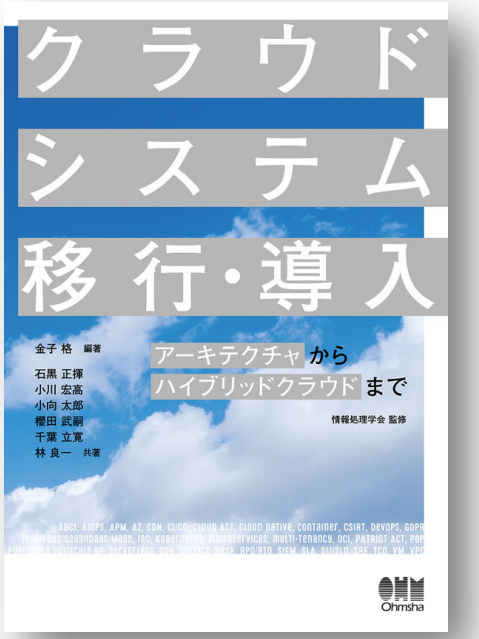
【専門分野】

情報法、情報通信法

【主な著書】

『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

『クラウドシステム移行・導入』共著、オーム社、2022



1.　DXと情報セキュリティ

1-1. DXの進展と情報リスクの拡大

Stolterman & Fors , *Information Technology and the Good Life*, Information Systems Research, IFIP, vol 143 (2004).

- 「私たちは日常生活の中で、情報技術がより一般的になり、私たちの行動のほぼすべての部分に存在するようになったことを経験している」
- 「私たちが目の当たりにしているのは、現在進行中のラディカルなデジタル・トランスフォーメーション（DX）なのである」
- それは「良い生活」の実現に資するものでなくてはならない

→生活への密着とリスクの深刻化

1-2. 情報セキュリティに関する法制度

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）情報漏えいの防止義務	• 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（第6版）デジタル・ネットワークの法律』（NTT出版）2022

（参考）サイバーセキュリティ基本法（2014年）

サイバーセキュリティ基本法案の概要　資料1－2（参考）

第Ⅰ章．総則

■目的（第1条）

■定義（第2条）

⇒「サイバーセキュリティ」について定義

■基本理念（第3条）

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について次を規定

① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応

② 国民1人1人の認識を深め、自発的な対応の促進等、強靱な体制の構築

③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築

④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施

⑤ IT基本法の基本理念に配慮して実施

⑥ 国民の権利を不当に侵害しないよう留意

■関係者の責務等（第4条～第9条）

⇒ 国、地方公共団体、重要社会基盤事業者（重要インフラ事業者）、サイバー関連事業者、教育研究機関等の責務等について規定

■法制上の措置等（第10条）

■行政組織の整備等（第11条）

第Ⅱ章．サイバーセキュリティ戦略

■サイバーセキュリティ戦略（第12条）

⇒ 次の事項を規定

① サイバーセキュリティに関する施策の基本的な方針

② 国の行政機関等におけるサイバーセキュリティの確保

③ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進

④ その他、必要な事項

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第Ⅲ章．基本的施策

■国の行政機関等におけるサイバーセキュリティの確保（第13条）

■重要インフラ事業者等におけるサイバーセキュリティの確保の促進（第14条）

■民間事業者及び教育研究機関等の自発的な取組の促進（第15条）

■多様な主体の連携等（第16条）

■犯罪の取締り及び被害の拡大の防止（第17条）

■我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第18条）

■産業の振興及び国際競争力の強化（第19条）

■研究開発の推進等（第20条）

■人材の確保等（第21条）

第Ⅲ章．基本的施策（つづき）

■教育及び学習の振興、普及啓発等（第22条）

■国際協力の推進等（第23条）

第Ⅳ章．サイバーセキュリティ戦略本部

■設置等（第24条～第35条）

⇒ 内閣に、サイバーセキュリティ戦略本部を置くこと等について規定

附則

■施行期日（第1条）

⇒ 公布の日から施行（ただし、第Ⅱ章及び第Ⅳ章は公布日から起算して1年を超えない範囲で政令で定める日）する旨を規定

■本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等（第2条）

⇒ 情報セキュリティセンター（NISC）の法制化、任期付任用、国の行政機関の情報システムに対する不正な活動の監視・分析、国内外の関係機関との連絡調整に必要な法制上・財政上の措置等の検討等を規定

■検討（第３条）

⇒ 緊急事態に相当するサイバーセキュリティ事象等から重要インフラ等を防御する能力の一層の強化を図るための施策の検討を規定

■IT基本法の一部改正（第４条）

⇒ IT戦略本部の事務からサイバーセキュリティに関する重要施策の実施推進を除く旨規定

内閣サイバーセキュリティセンターWebページ「サイバーセキュリティ基本法の概要」
https://www.nisc.go.jp/index.html

（参考）サイバーセキュリティの定義（第2条）

デジタル情報

「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう（第2条）」

ハッキングやマルウェア等による被害の防止

「デジタル情報の安全管理のために必要な措置（漏えい・滅失・毀損の防止等）と、情報システムと情報通信ネットワークの安全性と信頼性の確保のために必要な措置（※）が講じられ、その状態が適切に維持管理されていること」

（※）ハッキングやマルウェア等による被害の防止のために必要な措置を含む

1-3. 情報漏えいの防止義務

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

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

2.　情報漏えいに関する制度

2-1. 被害者救済（係争例）

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）

2-2. 安全管理措置

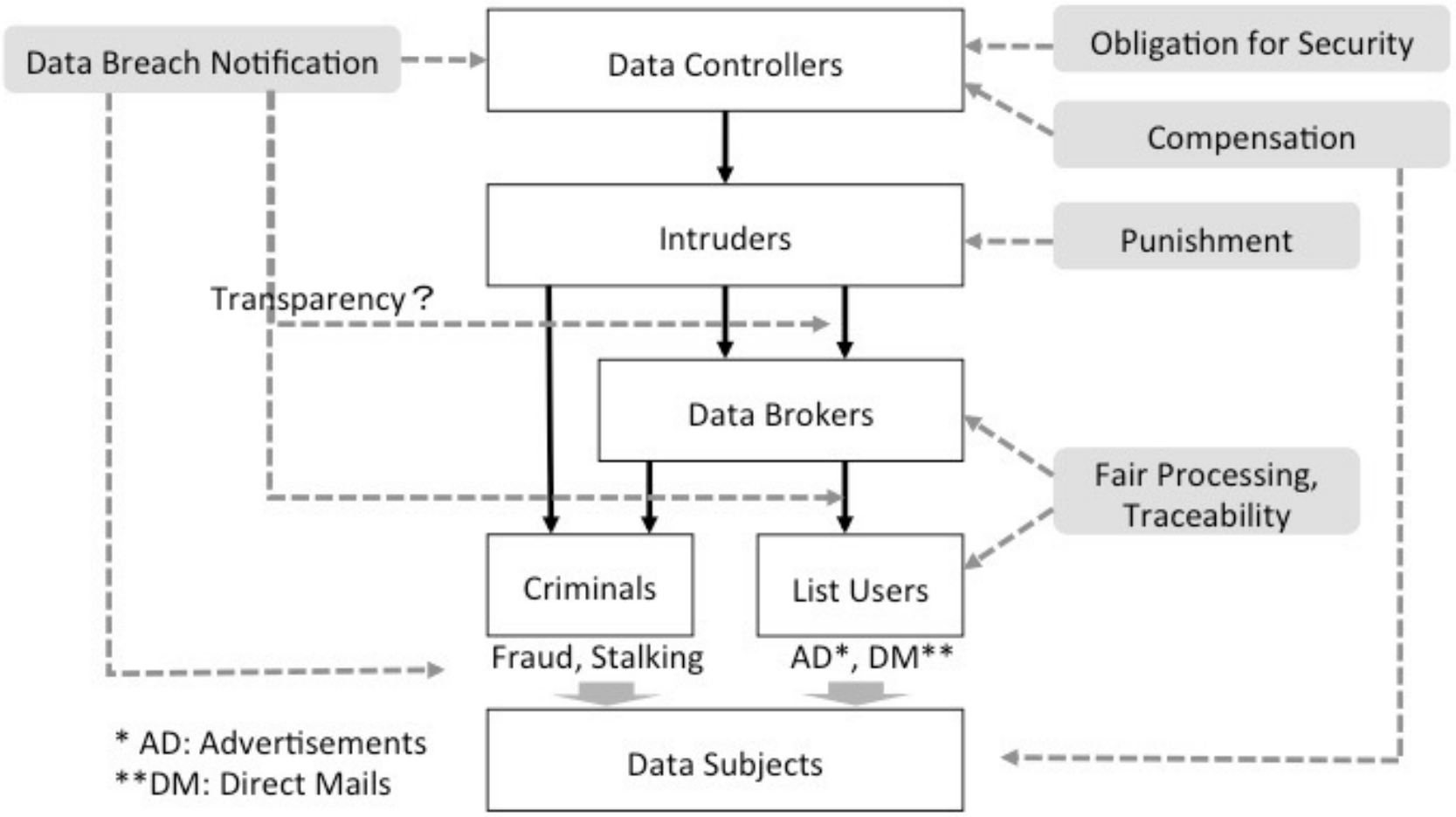
種類	講じなければならない措置
1. 規律の整備	個人データの取扱いに係る規律の整備
2. 組織的安全管理措置	(1)組織体制の整備、(2)個人データの取扱 いに係る規律に従った運用 、(3)個人データの取扱状況を確認する手 段の整備、(4)漏えい等の事案に対応する体制の整備、(5)取扱状況の把握及び安全管理措置の見直し
3. 人的安全管理措置	従業者の教育
4. 物理的安全管理措置	(1)個人データを取り扱う区域の管理、(2)機器及び電子媒体等の盗難等の防止、(3)電子媒体等を持ち運ぶ場合の漏えい等の防止、(4)個人データの削除及び機器、電子媒体等の廃棄
5. 技術的安全管理措置	(1)アクセス制御 、(2)アクセス者の識別と認証、(3)外部からの不正アクセス等の防止、(4)情報システムの使用に伴う漏えい等の防止

個人情報保護委員会「個人情報保護法ガイドライン(通則編) 」（別添）講ずべき安全管理措置の内容（2016年11月、2017年3月一部改正）

2-3.　データ侵害通知（2020年改正）

- 第二十二条の二　個人情報取扱事業者は、その取り扱う**個人データの漏えい、滅失、毀損その他**の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を**個人情報保護委員会に報告**しなければならない。ただし、当該個人情報取扱事業者が、他の個人情報取扱事業者から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を当該他の個人情報取扱事業者に通知したときは、この限りでない。
- ２　前項に規定する場合には、個人情報取扱事業者（同項ただし書の規定による通知をした者を除く。）は、**本人に対し**、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を**通知**しなければならない。ただし、本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

（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）.

3.　制度の課題

3-1. 個人情報保護法と情報セキュリティ

- 日本の個人情報保護制度は、内部利用を目的とする個人情報の取得・利用について、ほとんど制限がない。
- 一方で、事後的に第三者提供や利用目的変更を行うための条件は厳格であり、社会的に許容されるべき利用が制限される可能性がある（例：情報セキュリティ対策のための情報共有等）

<table>
<tr><th></th><th>個人情報保護法
（日本）</th><th>GDPR
（EU）</th><th>FTC法
（米国）</th></tr>
<tr><td>取得・
利用時</td><td>利用目的の特定、通知または公表等（原則自由）</td><td rowspan="2">(a)本人の同意
(b)契約等の履行への必要性
(c)法的義務
(d)生命に関する利益
(e)公共の利益・公的権限の遂行
(f)正当な利益の目的</td><td rowspan="2">不公正または欺瞞的な行為・実務は禁止

（参考）CCPA
消去・オプトアウトの義務等</td></tr>
<tr><td>利用目的の変更・第三者提供</td><td>• 本人の同意
• 法令の根拠
• その他（生命の保護等）</td></tr>
<tr><td>特徴</td><td>原則自由型</td><td>オプトイン型</td><td>オプトアウト型</td></tr>
</table>

（参考）GDPRにおける情報セキュリティのための情報共有

- **ネットワーク及び情報の安全性を確保する目的のために厳密に必要性であり、かつ、比例的な範囲内で行われる個人データの取扱い**、例えば、保存される個人データ若しくは送信される個人データの可用性、真正性、完全性及び機密性を阻害し、また、公的機関、コンピュータ緊急対応チーム(CERT)、コンピュータセキュリティインシデント対応チーム(CSIRT)、電子通信ネットワークのプロバイダ及び電子通信サービスのプロバイ ダ、並びに、セキュリティ技術及びセキュリティサービスの提供者によって、そのネットワーク及びシステムを介して提供され又はアクセス可能なものとされている関連サービスの安全性を阻害する事故、又は、違法な 行為若しくは悪意ある行為に対して、所与の機密性のレベルにおいて対抗するためのネットワークシステム又は情報システムの能力を確保することは、関係するデータ管理者の**正当な利益を構成する**。これには、例えば、電子通信ネットワークへの無権限アクセス及び悪意あるコード配布を防止すること、並びに、「サービス拒否」攻撃やコンピュータ及び電子通信システムの破壊行為を阻止することが含まれうる。（GDPR前文（49）個人情報保護委員会　仮日本語訳）

3-2. Solove & Hartzog, “Breached!”

Daniel Solove, Woodrow Hartzog: BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT, 2022/3/1.

- 現行制度の問題点

  ①データ侵害通知：過度な負担

  ②セキュリティ保護法：硬直的

  ③訴訟：侵害認定基準が曖昧
- 侵害のコストをデータエコシステムのすべての責任主体に適切に割り当てるべきである（ベンダー、ビッグデータ企業等）
- データ漏えいは避けられない。完全に防ごうとするのではなく漏洩した個人情報の危険を減らすことを考えるべきである
- 人は間違いを犯しやすく、リソースも限られている

3-3.　情報セキュリティ対策を促す制度

- 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
  - DXは、セキュリティを統合したソリューションとして、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