第４節　法制度上の課題

日本大学危機管理学部　教授　小向　太郎

Ⅰ　情報セキュリティに関する法制度

1　サイバーセキュリティ基本法

我が国における情報セキュリティに関する法制度として、まず、国家としての情報セキュリティ政策の基本法である「サイバーセキュリティ基本法」がある。この法律は、社会活動におけるサイバー空間の重要性が高まりサイバー攻撃等による被害のリスクが深刻化していること等を踏まえ、サイバーセキュリティ強化のための推進体制機能を確立することを目的として制定された（2014 年 11 月成立）。

この法律では、サイバーセキュリティに関する施策を総合的かつ効果的に推進するために、官房長官を本部長とする「サイバーセキュリティ戦略本部」が設置され、国家としてサイバーセキュリティの確保に取り組む体制の整備と、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その他の事業者・教育研究機関について、それぞれのサイバーセキュリティ確保のための責務が定められている[1]。

2　脅威となる行為を禁止する法律

情報セキュリティを確保するための法制度としては、情報セキュリティを脅かすような行為を法律で禁止することも重要である。このような法律としては、図表 1 のようなものがある。

図表 1　情報セキュリティを脅かす行為の禁止規定

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*

* 無断操作の対象や内容によっては、殺人罪・傷害罪・往来を妨害する罪（刑法第 124-129 条）等にあたることも考えられる。

出典：小向太郎（2018 年）『情報法入門（第 4 版）デジタル･ネットワークの法律』（NTT 出版）、169 頁。

3　被害者の法的救済

情報セキュリティが侵害されることで何らかの損害が発生した場合には、被害が拡大しないように差止めを求めたり、損害に対して賠償を請求したりすることが考えられる。問題となる行為が民法上の不法行為に当たるような場合には、行為の差し止めや損害賠償の請求が認められる。

しかし、インターネット上で民事上の不法行為責任を問われるような行為が行われた場合には、発信者が誰かがわからず、行為の差し止めを求めたり、損害賠償を請求したりすることが難しい場合がある。このような場合に、その情報を媒介している ISP（Internet Service Provider）等の媒介者に情報の削除等を求めたり、発信者情報の開示を請求したりするための制度として、プロバイダ責任制限法（特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律）が制定されている。

また、インターネット上で行われた犯罪の捜査についても、コンピュータやネットワーク上のデータに対する捜査手続が法定されていないと、捜査機関は強制的な捜査を行うことができない。ISP 等の協力義務や捜査権限の拡大についても法整備の必要がある。このような要請に応えるため、2011 年 6 月には「情報処理の高度化等に対処するための刑法等の一部を改正する法律（いわゆるサイバー刑法）」によって刑事訴訟法の一部が改正され、コンピュータに対する差押えや電気通信事業者に対する通信記録の保全要請に関する規定が整備されている。

Ⅱ　情報セキュリティを確保する義務

1　法的義務

情報システムのセキュリティ対策が不十分だと、そのシステムを運用している主体以外のものにとっても脅威となる。情報セキュリティ対策を怠った事によって生じた損害に対して、損害賠償等の責任を問われる場合がある。また、企業にこのような行為を防止する契約上の義務があるにもかかわらず、これを怠ったために損害が生じたのであれば、債務不履行責任を問われる可能性がある。

個人情報取扱事業者に関しては、個人情報保護法が安全管理措置義務を課しているが、特に社会的な影響が大きい事業者に対しては、個別の事業法が対策を求めている例もある。例えば、電気通信事業者に対しては、電気通信事業法第 41 条第 1 項が電気通信設備の維持義務を課しており（「電気通信回線設備を設置する電気通信事業者は、その電気通信事業の用に供する電気通信設備を総務省令で定める技術基準に適合するように維持しなければならない」）、これに基づいて、総務省が「電気通信設備の技術基準」を定めている。また、銀行については、金融庁の監査において情報システムの安全性についても対象とされており、監査指針においてシステム障害への対応等について十分な体制が取られているかどうかといった項目がある。

2　通信基盤

ネットワークを支える電気通信設備に障害が発生すると、現在では社会的にも大きな影響が生じる。2018 年 12 月 6 日午後に、ソフトバンクの 4G（LTE）携帯電話サービス等が、3 時間以上全国で利用不可または利用困難になったとされており、3G サービスに輻輳が発生し、利用困難な状況となった。ソフトバンクの発表によれば、影響規模は約 3,060 万回線である。障害の原因はパケット交換機のソフトウェアに異常が発生したことであるとされている。

この障害では、スマートフォンで交通系 IC カードや、QR コードを用いた決済やチケットを利用しているユーザに、広く支障が生じた。また、集荷や再配達に同社の回線を利用している宅配事業者の業務に影響が出たことも報じられている[2]。

電気通信事業者のサービス提供に関する約款では、一般に、障害が生じた際の損害賠償の範囲を制限しており、こうした波及損害については責任の対象としていない。損害賠償の責任を負うのは、「事業者の責に帰すべき理由によって提供をしなかった場合」で「24 時間以上その状態が連続したとき」に限定されており、損害額は基本料と通信料に相当する額に限定されている（ソフトバンク「4G 通信サービス契約約款（令和元年 9 月 13 日現在）」第 51 条（責任の制限）https://www.softbank.jp/mobile/legal/articles/）。

なお、電気通信事業者の設備の障害による波及損害については、電気通信事業に自由化が行われる前の日本電信電話公社に関する事例であるが、裁判で争われた例がある（世田

谷ケーブル火災事件)。この事案では、当時の公衆電気通信法が損害賠償額を通信回線使用料の5倍を上限にしていることについて、広く国民に対して低廉な通信料による通信サービスの提供を実現する必要性から、妥当であるという考え方が示されている（東京高判平成2年7月12日)。

3　クラウド事業者

現在では、様々な形態のクラウドサービスが提供されており、こうしたクラウド事業者のシステムに障害が生じた場合には、業務の停滞やデータの消失等、利用企業等に深刻な損害が生じる可能性が高い。クラウドサービス事業者の利用規約においても、障害発生時の責任は限定されていることが多く、こうした波及損害は基本的に補償されない。

一方で、クラウドサービスの重要性は高まっており、政府は、情報システムに関する調達において基本的にクラウドサービスの利用を第一に考える方針を打ち出している。しかし、重要なシステムにクラウドサービスを利用した場合に、クラウドサービスの提供にトラブルが生じると業務へのダメージは深刻になる。十分な情報セキュリティ対策が行われているかどうかを判断する基準もないため、クラウドサービスの導入が進んでいないという指摘もあり、総務省と経済産業省が2019年4月に「クラウドサービスの安全性評価に関する検討会」を立ち上げ、2019年内の最終取りまとめと制度立ち上げを目指している(2019年10月31日現在)。

Ⅲ　情報漏えいと法的責任

1　被害者救済

情報漏洩に対する法制度的な対応としては、図表2のようなものが考えられる。

図表2　情報漏えいに対する法制度的対応

種類	概要	根拠等
①被害者救済	漏洩によって生じた精神的な損害等について損害賠償の請求を認める	民法： 不法行為責任
②安全性の向上	個人情報取扱事業者に対して安全性を確保することを義務付ける	個人情報保護法： 安全管理措置義務
③透明性の向上	個人情報漏洩が生じた際の監督機関や本人への通知を義務付ける	個人情報保護法： 漏洩報告
	データの取得や提供に際して、利用目的等の確認や記録を義務付ける	個人情報保護法： トレーサビリティ

出典：小向太郎「情報漏えい事案でデジタル・フォレンジックはどう使われるか」安富潔・

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 年）117 頁。

まず、「①被害者救済」に関しては、個人情報が漏洩した場合にその個人情報の本人から、情報を保有していた事業者等に対して、損害賠償請求等が請求されうる。事業者の安全管理措置が不十分であったために、個人情報を漏洩された本人に損害が発生した場合には、当該事業者に対して不法行為責任が問われることがある。また、企業にこのような行為を防止する契約上の義務があるにもかかわらずこれを怠ったために損害が生じたのであれば、債務不履行責任を問われる場合もある。

図表 3　情報漏えいに関する我が国の係争事例

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（使用者責任: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（不法行為責任: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 万件）
TBC アンケート情報流出事件	サーバのメンテナンス時に、インターネットに	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	エステティックサロンのアンケート回答

（東京高判平19.8.28）	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		5,000円（使用者責任：民法715条）	
ベネッセ顧客情報流出事件（東京高判令1.6.27）	システムの開発・運用を行っていた委託先の従業員が、顧客情報を不正に持ち出して名簿屋に販売	業務用パソコンからMTP対応スマートフォンへのデータの書き出し（持ち出し）を制御する措置について、委託先に適切な監督をすべき注意義務を怠った	慰謝料2,000円（共同不法行為：民法719条）	大手教育産業企業の顧客情報（3,504万件）

出典：判決文をもとに作成。

2　安全性の向上

次に、「②安全性の向上」については、個人情報保護法 第20条が、個人情報取扱事業者に安全管理措置義務を課している。講じなければならない措置の具体的な内容については、個人情報保護委員会が図表4のような指針を示している。

図表 4　講ずべき安全管理措置の内容

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

出典：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）をもとに作成

3　透明性の向上

最後に「③透明性の向上」のための制度としては、「漏洩報告」や「トレーサビリティ」の制度が考えられる。

このうち、漏洩報告については、個人情報保護委員会のガイドライン（個人情報保護委員会「個人データの漏えい等の事案が発生した場合等の対応について（平成 29 年個人情報保護委員会告示第 1 号）」）が、漏洩等の事案が発生した場合には、早急に対策を講ずるとともに、事案の性質に応じて「本人への情報提供」「事実の公表「個人情報保護員会への報告」等を実施することを推奨している。なお、漏洩報告等を義務付ける制度が、カリフォルニア州をはじめとして米国のほとんどの州で導入されている。また、同種の制度は、EU が 2018 年 5 月に導入した一般データ保護規則（GDPR）にも盛り込まれており、個人データの侵害を所轄監督機関等に通知することと、特定の場合に 侵害により個人データが影響を受けている個人に通知することが求められている。

次に、わが国の個人情報保護法では、2015 年改正で、トレーサビリティのための制度が導入されている。個人情報の第三者提供を行う者には、「当該個人データを提供した年月日、当該第三者の氏名又は名称その他の個人情報保護委員会規則で定める事項に関する記録」の作成と一定期間の保存が義務付けられる（第 25 条）。そして、第三者から提供を受け取

る者にも、提供者の氏名・名称および住所（法人の場合は代表者の氏名）と当該個人データの取得の経緯を確認し、記録・保存することが義務付けられている（第 26 条）。これらは、個人情報のトレーサビリティを高めることで、本人から正当な手続きを踏んで収集されていない個人データが名簿事業者等によって流通されないようにするための制度である。

Ⅳ　今後の課題

情報セキュリティに関する制度は、悪意によってもたらされる脅威の抑止と減少を図るとともに、情報システムやネットワークを運営する事業者の情報セキュリティに対する取り組みを促すことが、その主要な目的である。最近では、これらに加えて、情報システムやネットワークに対する脅威が高度化、深刻化している現状から、情報共有を図る制度的な枠組みや、より積極的なセキュリティ対策を実施する制度の整備も重要になってきている。

情報共有に関しては、サイバーセキュリティ基本法が 2018 年 12 月に改正され、サイバーセキュリティ協議会（重要インフラにおける情報セキュリティへの脅威に対応するために情報共有と対策の協議を行う協議会）、の設置を定め、参加者に秘密保持義務を課すとともに、情報提供等を求める規定をおいている。

また、急速に増加している IoT 機器において、積極的な対策を行うための法整備もなされている。IoT 機器の中には、パスワード管理等がきちんとなされておらず、容易にハッキングがされてしまう危険な状態で放置されているものも多い。そこで、国立研究開発法人情報通信研究機構（NICT）の業務にサイバー攻撃に悪用されるおそれのある機器の調査等を 5 年間の時限措置として追加し、NICT がインターネット上の IoT 機器にアクセスして容易に推知されるパスワードを入力することでアクセスできる機器を特定して、電気通信事業者を通じて注意喚起を行っている。そして、こうした活動が不正アクセス（不正アクセス禁止法）等に当たらないことを「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律（2018 年 11 月施行）」によって明確にしている。

これ以外にも、例えば、個人情報漏洩に関する被害の情報は、情報漏洩後の対応にも有効に活用できる可能性がある。どのような情報が漏洩した可能性が高いのか、攻撃者としてどのような者が想定されるかといった情報は、情報セキュリティ対策や犯罪被害防止に役立てることも重要である。当該企業や漏洩情報の本人だけでなく、それ以外の関連業界や関連団体が活用することで、有効な事後対策につながる可能性がある。しかし、具体的な情報は個人情報に該当するものも多く、個人情報保護法が原則として本人同意を求めている第三者提供に当たるため、活用が難しい場合が多い[3]。

情報セキュリティ対策の高度化のための情報共有は、制度的なバックアップが必要なものが多く、こうした観点からの政策の検討が必要であると考えられる。

◆さらに学ぶための参考文献

・小向太郎（2020 年）『情報法入門（第 5 版）デジタル・ネットワークの法律』（NTT 出版）
・安富潔・上原哲太郎編著（2019 年）『基礎から学ぶデジタル・フォレンジック』（日科技連）
・岡村久道（2011 年）『情報セキュリティの法律（改訂版）』（商事法務）

---

[1] 小向太郎（2018 年）『情報法入門（第 4 版）デジタル・ネットワークの法律』（NTT 出版）、58-59 頁。

[2] 原田要之助（2019）「IoT 社会に適した社会基盤のあり方」『情報処理学会研究報告電子化知的財産・社会基盤（EIP）』2019-EIP-83:2019-2-15、（10）。

[3] 小向太郎（2019 年）「情報漏えい事案でデジタル・フォレンジックはどう使われるか」安富潔・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）121 頁。