# 第1章　序　論——予告された侵害の記録

探しているものが目の前にあるのに、それに気づかないことがある。ガブリエル・ガルシア＝マルケス（Gabriel Garcia Marquez）に『予告された殺人の記録』（*Chronicle of a Death Foretold*）というすばらしい小説がある。この話のなかでは、最初に主人公が刃物で刺されてひどい致命傷を負ってしまう。読み進めていくと、この殺人が起こる兆候を、誰でも目にすることができたのに、誰もそれに注意を払わなかったということが明らかになっていく。防ぐことのできた殺人であっても避けることは非常に難しく、その難しさは人間の本性に根ざすものだったのである。

データ侵害事例の多くは、これと似ている。私たちは、何千件ものデータ侵害を検討してみた。これらの事例からは、ほとんど同じ教訓が導き出される。「侵害は防ぐことができたが、人々がうっかりヘマをしてしまった」ということである。特に注目すべきなのは、この数十年間で進歩がみられないということだ。同じ間違いが何度も何度も繰り返されている。長い年月をかけて、データセキュリティを規制する法律が数多く制定されているのに、なぜ変わらないのだろう。

はじめに、すでに古典的な事例といえるターゲット（Target）のデータ侵害を取り上げたい。二〇一三年に起こった当時としては最大の侵害事例は、大変な注目を集めた。ターゲットの事例には、

データ侵害に共通する多くの要素が含まれているが、特に私たちを惹きつけるのは、それがダビデとゴリアテの物語の皮肉なバージョンだからである。ターゲットはいわば巨人ゴリアテであり、十分な防御を備えていた。豊富なリソースを駆使した防御策がとられ、他の組織よりもはるかに保護されていた。しかし、それでも守り切ることはできなかったのである。この事実は、私たちの背筋を凍らせる。

二〇一三年の一二月中旬、クリスマスセールの真っ只中に、ターゲットの幹部は恐ろしいニュースを知らされた。ターゲットがハッキングされたというのだ。皮肉なことに、全米第二位のディスカウントストア・チェーンであるターゲットのロゴは赤白の円で描かれた標的マークであり、文字どおりターゲット（標的）の看板を掲げていた。ハッカーは、その中心に矢を放ったのである。

ターゲットの経営陣は、このデータ侵害を、司法省の職員から知らされた。ターゲットから盗まれたデータがオンラインで公開されており、クレジットカードの不正請求の報告が出はじめていた。[1] 経営陣は、事態を深刻に受け止め、即座にフォレンジック会社に調査を依頼した。

調査の結果わかったことは、これが、大規模漏洩と表現してもまだ足りないような、歴史的巨大漏洩だということだった。[2] ターゲットは、小売業における米国史上最大のデータ漏洩という不名誉な事態に見舞われたのである。[3]

二〇一三年一一月から二週間にわたり、ハッカーは四〇〇〇万件のクレジットカードとデビットカードの口座に関する詳細な情報と、約七〇〇〇万人の顧客の個人情報を盗み出した。[4] そして、ハッカーたちは、その膨大なデータを闇取引の詐欺サイトで売りはじめていた。

ターゲットにとっては、最悪のタイミングだった。小売業者はクリスマスシーズンに、年間の二〇

～四〇％の売上を見込んでいる。[5] ターゲットの売上は、この時期に急落した。[6] これに対処するために、ターゲットは全店で一〇％の割引を行ったが、年末商戦の利益は四六％も落ち込み、ビジネスは壊滅的な打撃を受けた。[7]

ダメージはこれだけではない。利益が失われただけでなく、二月中旬には、このデータ侵害に関するコストは二億ドルを超えた。銀行からの払い戻し要求、規制当局からの罰金、直接的な顧客サービスの負担によって、コストは大幅に跳ね上がることになる。[8] 約九〇件の訴訟が提起され、多額の弁護士費用が発生した。[9]

誰もが不安に感じたのは、ターゲットが情報セキュリティにかなりの時間とリソースを割いていたことだ。ターゲットには三〇〇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、二四時間三六五日コンピュータネットワークを監視していた。二〇一三年五月、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（FireEye）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。[10]

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、二四時間体制の監視。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。

よくある説明は、この大惨事は、ハッカーの侵入を許したたった一人の人間が原因だというものだ。安手のアクション映画では、侵入先の内部にいる犯人の仲間がドアを開けっ放しにしておくといった手口が使われることがある。ただ、ターゲットの場合は、ハッカーたちを侵入させたのはターゲットの従業員ではなく、しかもその人にはなんの悪気もなかった。問題の人物は、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）の従業員である。彼が、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[11]。

トロイの木馬は、ZeuSと呼ばれるよく知られたマルウェアパッケージの亜種であり、企業向けの主要なアンチウイルス・ソフトウェアで容易に検出可能だった。全く目新しいものではない。しかし、ファツィオ・メカニカルにはターゲットのような立派なセキュリティ体制がなかったため、このマルウェアはファツィオのコンピュータで検出されないまま残っていた。そのためハッカーは、ファツィオが持っていたターゲットのシステムへのログイン認証情報を、まんまと入手することができたのである。

ハッカーたちは、ターゲットにアクセスすると、別のマルウェア・プログラムを放った。これは、ブラックマーケットでわずか数千ドルで購入したものだった[12]。マカフィー（McAfee）のディレクターであるジム・ウォーカー（Jim Walker）などの専門家は、このマルウェアを「全く素朴で面白みがないもの」と評している[13]。

当初、このマルウェアは検出されず、営業時間のピーク時に数百万件の記録を収集しはじめ、東欧にあるハッカーの拠点に転送できる状態になった。ただし、この直後には、ファイヤーアイがこのマルウェアを検知して、アラートを発している。バンガロールにあるターゲットのセキュリティチームはこのアラートに気づき、ミネアポリスのセキュリティ・センターに通知した。しかし、この警告は無視されてしまったのである。

ファイヤーアイが検知したのは、五つの異なるバージョンのマルウェアだった。このアラートをみ

れば、「踏み台（staging ground）」サーバーのアドレスがわかるはずだった。間抜けなことに、マルウェアのコードにはこれらのサーバーのユーザー名とパスワードが含まれていた。つまり、ターゲットのセキュリティ担当者がこの情報を使ってサーバーにログインしていれば、盗まれたデータをみることができたのである[14]。もっといえば、ターゲットのシステムから実際にデータが持ち出される前に何度も警告が出ていたのだから、ファイヤーアイの自動マルウェア削除機能が動いていれば、誰の手も煩わせずに攻撃を終了させることができただろう。しかし、ターゲットのセキュリティチームは、この機能をオフにしており、セキュリティに関する決定は最終的に手動で行うことになっていた[15]。

ファイヤーアイによるアラートが赤信号を激しく点滅させているなかで、ハッカーは一二月二日に盗んだデータの転送を開始した。マルウェアは、約二週間にわたって自由にデータを流出させ続けた。そして、一二日には、司法省の捜査官が、ターゲットに情報漏洩について連絡してきたのである。捜査官は、クレジットカードの不正請求の報告だけでなく、ハッカーが消去を怠っていたため中継サーバー（ダンプサーバー）に残されていた盗難データそのものを持っていた[16]。

この情報漏洩によって、ターゲットは莫大な金銭的損害を被った。正確な額は今も不明だが、二〇一六年三月のターゲットの年次報告書では、二億九一〇〇万ドルと推計されている[17]。会社の評判は損なわれ、CIOは辞職した。顧客にとっては、将来的に詐欺にみまわれるリスクが高まった。関係するアカウントの多くについて一日の利用限度額や引出限度額を設定したり、新しいクレジットカードを発行しなければならず、消費者はいたるところでカード情報を更新する時間と手間を強いられることになった[18]。

この情報漏洩は、歴史に残る記録的なものだ。しかし、この後すぐに起こるもっと大規模なデータ

侵害によって、その影は薄くなっていく。

## システムダウン

理屈の上では、ハッカーはターゲットに侵入することはできないはずだった。ハッカーが使っていたのは、最先端の技術ではなく、すぐに発見できるマルウェアなど、安直な方法だ。その上、とてもずさんで、不注意なミスも犯している。ターゲットには、ずっと優れた技術的ツールと大規模で洗練されたチームがあった。フィッシングに対応するテストを実施し、フォレンジック調査の専門家を採用していた。物量では、ハッカーより圧倒的に優っていた。しかし、ターゲットはそれでも敗北を喫した。

一見すると、ターゲットのアキレス腱は、サードパーティーベンダーの一人の従業員にあったようだ。ほとんどの大企業は、何百ものサードパーティーベンダーを抱えている。この人物がマウスを一回間違ってクリックするだけで、ハッカーにとっては十分だった。その人物がクリックさえしなければ、五億ドル以上の損失につながる情報漏洩は起こらなかったかもしれない。なんて高くつくマウスクリックだろう。

しかし、もっとよくみてみれば、システム的な脆弱性が山積みだったことがわかる。チェックリスト上では健全にみえていたターゲットが、ある重要な要素、つまり人間の行動を考慮していなかったために、損失を被ったのである。何百万ドルもかけてハイテク・ソフトウェアを導入しても、人間の致命的な失敗を防ぐことはできなかったのだ。

インターネット上の犯罪者として大成するためには、技術的卓越や優れたスキルが必要なわけではない。技術やデータエコシステムは非常に脆弱で不備があるものなので、ハッカーは、そうした素養がなくても簡単に侵入できる。闇市場には、サイバー犯罪のスタートアップ・キットがあふれている[19]。こうしたツールをダウンロードすれば、すぐにでも使うことができる。インターネット上の犯罪が追跡されたり取り締まられたりするのは、実際にはまれなケースなので、多くの詐欺師たちはそのまま逃げおおせる。

## 私たちが失うものは大きい

データセキュリティの危険性は恐ろしく大きい。私たちがデータ侵害といっているのは、企業や組織が、正当な権限なく個人情報を暴露、開示、紛失してしまうことである。こうしたデータ侵害は、数が増加しているだけでなく、危険度も増している。毎年、何百万人もの人々がなりすましの被害を受けている。パーソナルデータは、詐欺師が本人になりすますために利用される。被害者は、詐欺師による債務の不払いでクレジットカード情報が汚されてしまう。債権者は不払いの請求を支払ってほしいと被害者に言ってくるので、被害者は請求が自分のものでないことを苦労して証明しなければならない。メディカル・ケアを受けるためのＩＤが盗まれることもあり、健康保険が使えなくなってしまう。なかには、なりすまし犯によって警察の記録が書き換えられていたため、被害者が警察に逮捕されてしまったケースさえある。

ランサムウェアによる攻撃が激増している。ランサムウェアは、人々のコンピュータ上のファイル

を暗号化し、ファイルを解読不能にし、アクセスできなくしてしまう。データが人質にされてしまうのだ。データを取り戻すには、被害者はハッカーに身代金を支払わなければならない。ランサムウェアは、ハッカーに信じられないほどの利益をもたらす。文書、大切な写真や動画、音楽、とても大事な情報など、コンピュータに保存されているものであればどんなものでも人質になりうる。私たちは今、いつ誰に身代金が請求されるかわからない恐ろしい世界に住んでいる。ジョージア州アトランタ市は、二〇一八年に、約五万ドル相当の電子通貨ビットコインを要求するランサムウェア攻撃を受け、復旧するのに二六〇万ドルをかけている。[20]

いったんデータが侵害を受けると、悪質なハッカーは簡単に人を陥れることができる。[21] コンピュータに犯罪を犯したかのようなファイルを仕込んで警察に密告することができる。あなたのごくプライベートな写真や文章にアクセスし、それを世界中に公開することもできる。[22] 乗っ取ったコンピュータを通して、スパムを送ったり、犯罪を犯すパイプ役になったりすることもできる。

インターネットにつながる機器、家電、自動車が増えることで、物理的な安全が重大な脅威にさらされている。[23] ハッカーは、私たちの家庭用機器に侵入することができる。家庭用見守りカメラを通して私たちの子どもを覗きみることができる。私たちの自宅に設置された防犯カメラを通して様子を探ることもできる。ホームアシスタント機器を通じて、私たちの様子に聞き耳をたてることができる。自動車を勝手に操作することもできる。ペースメーカーやインスリンポンプなど、体内に埋め込まれている機器に侵入することも可能だ。

慎重に扱わなければならない情報は、私たちに関する大量の記録のなかで増え続けている。指紋、眼球スキャン、顔認証データ、ＤＮＡなどの生体情報も、収集・保存されるようになる。こうした情

報を企業や組織が安全に保つことができないとしたら、未来はどうなるのだろう。

フィリップ・K・ディック（Phillip K. Dick）の短編小説が原作の映画「マイノリティ・リポート」（二〇〇二年）では、主人公のジョン・アンダートンが当局から徹底的な追跡を受けて逃亡を続けている。映画の舞台は、政府や企業が大規模な監視技術を駆使している未来（二〇五四年）だ。常に存在する網膜スキャナーによる捕捉から逃れるために、ジョンは両目を交換する手術を受けなければならない。この手術はかなりぞっとするものだが、生体認証が行き渡ったこの物語の世界では、彼はそうしなければならなかったのだ。

未来のデータ侵害通知はこんなものになるかもしれない。

> ハッカーがあなたの網膜データを入手し、それを使ってあなたになりすまし、アカウントにアクセスすることが可能になった。将来的な被害から守るため、直ちに眼球を交換する手術を受けることをお勧めする。

私たちは、命にかかわる危険な未来に向かって突き進んでいる。企業や組織が収集するデータは増加を続け、その悪用がもたらす結果は悲惨なものになり、命にかかわることさえある。

## データセキュリティ法の登場

過去二〇年間、政策立案者たちは、増大するデータセキュリティの悪夢に対処するために、法体系

を急いで整備してきた。最も大きな成果は、データ侵害通知法の進展である。データ侵害が発生した組織に対して、規制当局、影響を受ける個人、時にはメディアに通知することを義務付けるものである。データ侵害通知はきわめて一般的で、米国各州や他の多くの国でこの法律が制定されている。ただし残念ながら、データ侵害通知は被害者にデータが侵害されたことを知らせるだけだ。被害を救済するわけではなく、危険性を知らせるだけだ。

そして、データ侵害通知によって、集団訴訟が発生する。情報漏洩が公表されてからわずか数時間後に、弁護士が情報漏洩の被害者に代わって企業を提訴することもある。こうした訴訟の多くは失敗に終わる。あるいは、企業が訴訟費用を節約するために和解金を支払うことで幕を閉じる。消費者はたいした利益や補償を受けられないことが多い。

ターゲットのケースでは、漏洩に対する消費者訴訟の和解金はわずか一〇〇〇万ドルであった。この和解金は、訴訟そのものによって得られたものではなく、事件を解決するために支払われたのだといってよい。ターゲットの不正アクセスは七〇〇〇万人から一億一〇〇〇万人の人々に影響を与えたとされるため、一人当たりにするとわずか数セントにすぎない[24]。被害者は、多額の賠償を受けることはなかった。和解金では、難解で評判の悪い「立証された損害」や「時間的損失」が補償の対象とされ、それらに認められる価値はわずかだったからである。

漏洩が発生すると、規制当局も法執行を行うことを検討するが、見送られることが多い。毎年あまりにも多くの漏洩があり、規制当局はそのごく一部を追及するためのリソースしか持ちあわせていない。もし規制当局が介入しても、その罰則は漏洩のコストをほんの少し、あるいはささやかに増加させるだけであることが多い。例えば、ある州の規制当局は、ターゲットと一八五〇万ドルで和解して

いる。[25] ターゲットの情報漏洩のコストは推定二億九一〇〇万ドルなので、この規制当局によるペナルティは、コスト全体の一〇％未満にすぎない。仮に規制当局や個々の訴訟当事者がより多くの罰金や損害賠償を得ようとしたとしても、事態が大きく変わるとは思えない。もちろん、データ漏洩による金銭的な痛みが大きくなれば、データの安全性を保つためのインセンティブが高まるかもしれない。しかし、企業や組織はすでに漏洩によって大きなコストに直面しており、さらにコストを上乗せしても、それがゲームチェンジャーになるとは思えないのだ。ターゲットはすでにセキュリティに真剣に取り組んでおり、かなりのリソースを投じていた。ターゲットが失敗したのは、セキュリティに対する配慮を欠いたからではなく、ミスを犯したからだ。

情報漏洩が生じたことによる法的な対応は、何年も尾を引いて、企業や組織は何百万ドルもの費用に悩まされることが多い。しかし、この時点では、遅すぎるのだ。すでに被害は生じてしまっており、法律は企業の出費を増やすだけになってしまっている。もちろん、企業や組織自身に、自分が作り出してしまったリスクを引き受けさせることは重要だ。しかし、これらの法律では、その企業以外にもリスクを生み出した主体がいることが見過ごされている。さらに悪いことに、こうした法律は、情報漏洩によってデータが流出した被害者本人を救済していないことが多い。

データセキュリティ法はデータ侵害を何とかすることに執着しているが、この法律によって、侵害の規模、重大性、件数が減少しているとは思えない。データ侵害は着実に増加している。[26] ニュースは、大きなコストや面倒な手間をかけなくても容易に防ぐことができたデータ侵害の話であふれている。なぜ、データ侵害は減らないのだろう。なぜ、法律は効果を発揮しないのだろうか。

## 本書の論点とロードマップ

本書は、データセキュリティに対する法律のアプローチを、どうすれば改善できるのかを、テーマとしている。私たちの目標は、個人情報を漏洩や悪用の危険にさらしてしまうシステムの構築や運用にかかわる全ての主体に対して、法律がよりよい効果を上げることができるような、新しい方法を提示することだ。

本書は、サイバーセキュリティ全般に関するものではない。広義のサイバーセキュリティには、インターネットを使用するシステムに関するあらゆる形態のセキュリティが含まれる[27]。本書が対象とするのは、データセキュリティである。サイバーセキュリティのなかでも、パーソナルデータに関して特に重要となるデータセキュリティに焦点を当てる。データセキュリティ法は、主としてプライバシー、データ保護及び消費者保護といった制度枠組みの一部として定められている。例えば、連邦取引委員会（FTC：Federal Trade Commission）による欺瞞的または不公正な行為に対する法執行、欧州連合（EU：European Union）の一般データ保護規則（GDPR：General Data Protection Regulation）、医療保険の相互運用性と説明責任に関する法律（HIPAA：Health Insurance Portability and Accountability Act）のような法制度がこれに当たる[28]。

最適なデータセキュリティのための規制と、最適なサイバーセキュリティのための規制には、重なり合う部分も多いが、両者には重要な違いもある。パーソナルデータに関する規制は、リスクの閾値、脅威のモデル化、影響を受ける主体、被害の種類と大きさなどの面で、サイバーセキュリティに関す

る規制とは違った特徴がある。特に、サプライチェーン、機械、またはインフラストラクチャに関する規制とは異なってくる可能性がある。したがって、データセキュリティをサイバーセキュリティと別扱いにすることが、背景や状況によっては理にかなっており、法律上もそうなっている。データセキュリティ法は、サイバーセキュリティ法よりも、プライバシー法のなかで定められることが多いのである。

残念ながら、データセキュリティ法は、現在、サイバーセキュリティとプライバシーにはさまれて、落ち着きの悪い状態にある。このような状態にあることによって、データセキュリティ法が、サイバーセキュリティとプライバシーの両方の長所を取り入れることを難しくしている場合が多い。プライバシー問題を扱う法律には、制度の一部としてデータセキュリティに関する規定が置かれていることが多い。この場合、立法目的はプライバシーであるため、立法者は通常、個人に焦点を当てる。データセキュリティについては、侵害通知を中心としたものになり、その他のセキュリティに関する規制は曖昧でまばらに置かれていることが多い。これとは対照的に、サイバーセキュリティ法には、システム的な観点に焦点を当てたセキュリティ枠組みに基づいて、より強固なセキュリティルールが頻繁に盛り込まれている。

とても皮肉なことに、プライバシー法におけるデータセキュリティに関する規定も、プライバシー法のよいところを取り入れられていない。データセキュリティは、ここでもプライバシーとは完全に切り離されている。プライバシー法の一部として定められているデータセキュリティに関する規定は、狭い範囲に限定されることが多い。プライバシー法は、単に秘匿性を維持するためではなく、人間の行動と人間価値の保護とを調和させることを目指すものであるが、データセキュリティ法は、こうし

た発展的な認識を十分に取り入れていない。さらに困ったことに、プライバシー法の保護規定は不十分で、セキュリティを確保するためには欠陥があることが多いのだ。

データセキュリティがプライバシー法の一部になっているのなら、その機会をメリットとして活かせるのに、そうしたことが見過ごされている。立法者は、プライバシー法のツールボックスから、パーソナルデータの安全性を確保するための、より豊かで繊細なアプローチを引き出すことができるはずだ。しかし、これまでのところ、彼らはそうしていない。

本書では、データセキュリティ法を、この「中間地帯」から救い出し、プライバシーとサイバーセキュリティの英知をかけ合わせて反映させることで、よりよいものにしたいと考えている。本書では主にパーソナルデータに焦点を当て、インフラセキュリティ、産業スパイ、サイバー戦争、コンピュータ犯罪、企業秘密や工業所有権、セキュリティ脆弱性の市場と開示をめぐる微妙な議論など、より一般的で重要なサイバーセキュリティの問題は取り扱わない[29]。これらの問題は、もちろんデータセキュリティの問題と重複している部分もある[30]。しかし、本書では、これらの問題全体のなかの一部である、データセキュリティにしぼって検証をしている。

また、技術者が情報を保護するために開発した既成の戦略を批判するものでもない。サイバーセキュリティの分野に新たな技術的アプローチを提案するわけでもない。むしろ、法学者として、法律がしばしば取り入れることのできない既存のセキュリティの知識を利用している。私たちは技術の専門家ではないので、データセキュリティの技術的な詳細について深く掘り下げることはしない。私たちの目標は、近い将来において法律を導くことができる原則と理論を構築することだ。本書では、パーソナルデータのセキュリティを向上させるために、法律家や裁判官がとりうる全般的なアプローチを

提案し、長い間、誤った方向に焦点を合わせてきた法制度に、一貫性と整合性をもたらすための幅広い原則の概要を示す。

私たちの議論は、一つの包括的なポイントを中心に組み立てられている。個人情報の安全性を高めるルールを改善するためには、政策立案者はその直観に反して、データ侵害以外の部分に、法律の焦点を当てるようにシフトしなければならない。現行のデータセキュリティ法では、情報漏洩や侵害を受けた主体だけをメインに据えているものがあまりにも多い。データセキュリティ法を「侵害の法」と言い換えると、侵害された主体の行為を過度に強調して、侵害に寄与している他の主体や要因を無視してしまうことになる。私たちは、説明責任、救済、技術設計の三つの領域において、既存のものに代わるデータセキュリティ政策の広範なビジョンを提示する。

企業や組織に対して「もっと安全性を高めろよ！」と言いたくなることはある。しかし、データセキュリティは非常に複雑であり、多くの調整が必要である。皮肉なことに、立法者や産業界がセキュリティを強化しようとすると、かえってシステムの脆弱性を高める場合がある[31]。セキュリティ対策にはコストと効果の難しいトレードオフが伴うため、どの方法をどれだけ使うかを選択することは非常に困難だ。

データセキュリティは、テクノロジーと人間の間の繊細なダンスである。理想的なデータセキュリティは、必ずしも可能な限りの安全性を確保し、何としてでも侵害を避けることではない。ほとんどの場合、トレードオフを無視することはできないため、企業や組織が可能な限り強力なセキュリティを持つことは、好ましくない選択肢となる。また、セキュリティ対策にかかるコストは、主に金銭的な面だけをみて、過小評価されることもある。多くのセキュリティ対策の最大のコストは、その対策

を入れることで機能が低下したり、業務にとって非効率的で不便なものになったり、やりにくくて時間のかかるものになってしまうことだ。

セキュリティの課題の一つは、完璧な答えは存在しないということだ。なぜなら、私たちが相手にしているのは、いつまでも終わらないリスクであり、攻撃者と防御者の間ではいたちごっこが続けられているからだ。政策の選択においては、リスクの評価だけでなく、そのリスクに対処するためのコストも考慮される。複雑なバランスを保たなければならないのだ。

現在のデータセキュリティのルールは、リスクのバランスをうまくとることができない。多くの場合、法律はリスクやバランスをほとんど考慮せずに漏洩に罰則を課している。一方で、企業や組織の行動が不当に大きなリスクを発生させたにもかかわらず、法律が何の罰則も課さない場合もある。

私たちは、もっとよい役割を法律に担わせるべきだと主張したい。本書で示す主な教訓は、データセキュリティに関する法と政策が、何度となく、大局を見失っているということだ。立法者は、「侵害された者を非難する」という従来の考え方にこだわらずに、データエコシステムにおいて、問題の発生に何らかの形で寄与している関係者全てに責任を負わせるべきだ。プライバシーとセキュリティの縦割りをなくすべきだ。そして、人々が実際にどのように考え行動するのかということに基づいた、人間中心のセキュリティを推進すべきだ。

本書の第1部では、データセキュリティの課題と、なぜ法律がこれらの課題に適切に対処できていないのかをテーマにしている。

第2章では、今世紀のデータセキュリティに関する歴史を簡単に紹介する。データ侵害が、なぜ、どのようにして、ニュースメディアの見出しを飾るようになったのか検討する。過去二〇年間を簡単

に振り返り、歴史的に重要な情報漏洩事件と、新たに発生したセキュリティ上の脅威を取り上げる。全体をみると、情報漏洩との戦いは、どれも負け続けている。データ侵害の事例から学ぶことは多い。なぜデータセキュリティが失敗しがちなのか、その理由を明確に示す共通の筋書きがあるからだ。

第3章では、データセキュリティに関する法と政策を概観し、その長所と短所を分析する。ちょっとした成功例は、ところどころにある。しかし、法と政策は、私たちが直面しているデータセキュリティの脅威に、全般的に有効に対処できていない。データセキュリティ法はあまりにも保守的だ。法律は、データ侵害のコストを増加させるだけで、データ侵害を防止するという点では役には立たないことが多い。さらに、データセキュリティの不備によってより大きなリスクにさらされている個人を保護することもできていない。

本書の第2部では、データセキュリティに対する別のアプローチ、すなわち私たちが「総体的データセキュリティ」と呼ぶアプローチを提案する。このアプローチの下では、法律はより早期に、より頻繁に、より多くの当事者と行動に適用されるであろう。

第4章では、私たちのアプローチである「総体的データセキュリティ」の内容を紹介する。このアプローチは、データエコシステム全体におけるリスクの軽減に焦点を当てる。データセキュリティ法は、個別の被害や特定の侵害のみに集中するのではなく、データエコシステムの健全性と回復力を確保することを目指すべきである。私たちのアプローチは、公衆衛生のような、システム全体の検討が不可欠な専門分野から知見を得ている[32]。データセキュリティに関するルールも、公衆衛生に関するルールも、どちらも、複雑でダイナミックなシステムを安全かつ発展的に保つことを目的としている。どちらも、複雑で不透明、かつ刻々と変化するリスクに対処する必要があるため、原因の特定や効果

的な法執行を、個人レベルで行うことが困難になっている。どちらの分野も、「ウイルス」の蔓延を緩和することを任務としているところまで同じだ。ただし、公衆衛生法では、全体的にリスクを低減するような活動を義務付けることによって、国民全体の健康を維持しようとする[33]。これに対して、データセキュリティ法は、ウイルスがどのように感染拡大したのかを考えるのではなく、その連鎖の最後の部分だけを問題視して、苦心惨憺している。

第5章では、立法者と裁判所が、どうすれば関係者に公平に責任を負わせることができるかを考える。データセキュリティの問題を引き起こすさまざまな関係者には、侵害の現場近くにいたかどうかだけではなく、より公平な観点で責任を負わせるべきである。情報漏洩は、データ侵害を受けた特定の組織だけが引き起こすものではない。データ侵害は多くの関係者によって生じるものであり、情報漏洩は、関係者全員がいてはじめて生まれるのだ。私たちは、このようなさまざまな関係者とその問題への寄与度について調査している。

残念ながら、法律はほとんどの関係者に責任を負わせていない。政策立案者は、直接侵害を受けた特定の組織に、近視眼的に焦点を当てることが多いからである。また、データセキュリティがシステマティックな問題であることを見落としていることも少なくない。

第6章では、政策立案者が、データ侵害の被害を拡大し、コストを増大させるような行為の多くに対して、適切な法的対処を行っていない場合が多いことを論じている。直接データ侵害を受けた企業や組織以外にも、データ侵害による被害の拡大に寄与している組織は存在する。全ての情報漏洩をなくすことはできないが、情報漏洩が引き起こす被害を大幅に減らすことは可能だ。

第7章では、プライバシーとセキュリティの関係を取り上げる。プライバシーは、データセキュリ

ティの重要な側面であるが、あまりそのように認識されていない。現在、企業ではプライバシーとセキュリティの間に分裂が起こっている。プライバシーについては、コンプライアンス部門や法務部門が担当し、セキュリティはＩＴ部門が担当するのが一般的だ。この二つの部門は分断され、互いに話すことがほとんどない。

データセキュリティとプライバシーの間の橋渡しをして、法や政策によって、両者が手を取り合えるようにする必要がある。強力なプライバシールールは、個人情報の収集、使用、拡散に関する説明責任を果たすように促し、個人情報の利用と保持を最小限に抑えることで、脆弱性とリスクを低減することができる。優れたプライバシーはセキュリティを強化する。

第8章では、データセキュリティの失敗の多くは人為的ミスが原因であるにもかかわらず、政策立案者が、人間を念頭に置いてセキュリティ対策を設計していないことを論じている。政策立案者は、人間が通常持ちうる認知の範囲を超えて対処することを期待してしまっている。データセキュリティにおける自分の役割について人々を教育することについても、あまりにも重点が置かれずリソースも割かれていない。その結果、彼らが策定する政策は、セキュリティ上の最大の脆弱性である人的要因に対処できていない。

ターゲットのデータ侵害についてもう一度考えてみよう。チェックリストを見れば、ターゲットは健全にみえる。優れた方針、大規模なセキュリティチーム、多大なリソース、強力なセキュリティソフトウェアを有していた。しかし、何百万ドルもかけてハイテク・ソフトウェアを導入しても、人間の不手際を防ぐことはできなかった。人間は、ソフトウェアをオフにし、赤信号の点滅を無視し、間違ったリンクをクリックした。

人間を中心に据えて法律を再検討することは、単なる再検討ではない。それは、データセキュリティに関する法や政策の根幹について考えるということなのだ。それが意味することは、既存の政策の多くに欠陥があり、多くの企業に広く受け入れられているセキュリティの取組みが、実は間違っていたということである。

■

本書では、政策立案者に新たな方向性、つまり根本的な転換を呼びかけている。その過程で、法律が求めるべき具体的な事柄をいくつか示唆しているが、特定の方策を列挙することが目的ではない。私たちが伝えたいことの核心は、その全体像である。私たちは、データセキュリティについてこれまでとは異なる考え方を提案し、法律がどのように異なるアプローチをとることができるのかについて、私たちのビジョンを示しているのである。

# 解説

小向太郎

本書は、米国の著名なプライバシー研究者であるダニエル・ソロブ教授とウッドロウ・ハーツォグ教授による『Breached! Why Data Security Law Fails and How to Improve It』を全訳したものである。

私は、二〇二二年三月にこの本が出版されたことを、ソロブ教授がプライバシー関係情報を提供しているメーリング・リストで知った。すぐに注文をしたが、当時はまだ新型コロナウィルス感染拡大の影響が残っており、海外から書籍が届くのには結構時間がかかった。しかし、著者たちがポッドキャストで紹介していた内容があまりに面白かったので、書籍がまだ手元に届く前に、情報セキュリティに関するシンポジウムでこの本のことを紹介したのを覚えている。

著者たちのデータ侵害とデータセキュリティ法に関する問題意識と、それに対する答えは、次頁掲載表のように非常にシンプルかつ明快なものである。要するに、現在のデータセキュリティ法が的外れだから、データ侵害が減らないということだ。

本書では、こうしたデータ侵害に関する現状の問題点を指摘するだけでなく、どうすれば問題解決につなげることができるのかについて具体的な提言をしている。すでに本書を読了された方には蛇足

| 本書の問題意識 | 著者たちの答え |
| --- | --- |
| （データセキュリティ法によって）、侵害の規模、重大性、件数が減少しているとは思えない。**データ侵害は着実に増加している**。ニュースは、大きなコストや面倒な手間をかけなくても容易に防ぐことができたデータ侵害の話であふれている。なぜ、データ侵害は減らないのだろう。**なぜ、法律は効果を発揮しないのだろうか**（12頁） | 現在のデータセキュリティ法は、**侵害通知法、安全保護法、私的訴訟**の三つに大別できるが、いずれもデータ侵害に重点を置きすぎている。**これらの法律は、情報漏洩の燃え殻を引っ掻き回すだけで、火消しの役には立たない**。データ侵害を防止したり、データ侵害による被害を軽減するには不十分だ（266頁） |

であるが、本書の概要を簡単に紹介してみよう。翻訳そのままではなく、私なりに咀嚼した表現になっていることをご了解いただきたい。

本書の第1部では、データ侵害の現状と、データセキュリティ法がどのように対応しようとしているのかについて、詳しく説明している。

まず、「第2章　データ侵害の蔓延」では、データ侵害の歴史を振り返ることで、データ侵害が増加の一途をたどっていることと、原因のほとんどがありふれた人為的ミスであることをあきらかにしている。この章に限らず、データ侵害事例についての、臨場感あふれる具体的な紹介が多いことが、本書の魅力の一つといえるだろう。

次に「第3章　データセキュリティ法の失敗」では、著者たちの最近のデータ侵害に関する法的な研究も踏まえて、データセキュリティ法の三つのアプローチ（侵害通知法、安全保護法、私的訴訟）が、それぞれ次のような理由で効果をあげていないと問題提起する。

まず、侵害通知法は、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もの

である。これは、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。

次に、安全保護法は、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ものである。しかし、どのような対策を義務付けるべきかを明らかにすることは難しいし、法執行を迅速に行うことも難しい。また、この規制で罰則等を課しても、被害を受けた人の救済に繋がらないことが多い。

最後に、特にアメリカではデータ侵害が生じると、被害者から私的訴訟が起されることが多い。しかし、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。

そして、データセキュリティ法が抱えている根本的な問題として、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からだという、非常に刺激的な指摘をしている。

第2部では、筆者たちが考えるデータセキュリティ法のあり方について、踏み込んだ提言をしている。

「第4章　全体像」で強調されているのは、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ということである。情報システムには、セキュリティの強化だけではなく、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のだ。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だろう。まず考えるべきなのは、どうすれば人間が過ちを起こさないようにすることができるのかということだ。

「第5章　データエコシステム全体の責任」では、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、決して漏洩はなくならないと指摘する。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のに、現状のデータセキュリティ法はこういった人たちに対して法的な責任を負わせていない。著者たちは、こうした多様なアクターにきちんと対応を促すような制度を構築すべきだと主張する。

「第6章　データ侵害による損害を軽減する」では、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と批判する。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。著者たちは、こうしたことを是正する法律を整備するべきであると主張する。

「第7章　プライバシーとデータセキュリティの統合」では、プライバシーとセキュリティが分断されていることの弊害を指摘する。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。そのため、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ことがある。ケンブリッジ・アナリティカの事件で、当初フェイスブックの幹部が「これはデータ侵害ではない」と抗弁したのはその典型的な例である。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。

最後に「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」で取り上げられているのは、最大の脆弱性である人為的ミスをどうしたら防げるかという問題である。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。そして、杓子定規にルールに従えと言っても人々は従わない。そこで筆者たちは、次のような方法でセキュリティデザインの改善を制度的に促すことを提案している。

① デフォルト設定の変更（例：パスワードを強制的に変更させる）
② 相互の信頼の促進（例：ユーザだけでなく組織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）

当然のことながら、本書が対象としているのは、米国のデータ侵害とデータセキュリティ法である。データ侵害の現状や、個人情報保護や情報セキュリティに関する制度は、日本と米国ではかなり異な

る。データ侵害による経済的被害は現在のところ日本よりも米国の方が深刻だと考えられるし、訴訟社会である米国ほど活発な訴訟提起は、日本ではなされていない。しかし、個人情報保護や情報セキュリティに関する制度がデータ侵害の予防や損害の軽減に対して効果を上げていないのは、日本も同様であろう。著者たちの問題意識は、日本にもほぼそのまま当てはまるものが多いはずである。

なお、本書では触れられていないが、情報漏洩を起こした企業の責任を厳しく追及すべきだという考えに取り憑かれているのは、サイバーセキュリティ法や法律家だけではないということも、指摘しておきたい。特に、日本では、情報漏洩をした企業や組織を叩いていれば事足りると思っている人が多い。マスメディアによる報道でも「情報漏洩はあってはならない」「情報漏洩したら大変だ」といった論調が決まり文句のように使われている。自分たちが思考停止に陥っていないか、本当に損害をなくすためにはどうしたらよいのか、本書を読んでぜひ考えてみていただきたい。

本書は、刺激的な示唆に溢れるだけでなく、わかりやすくユーモアにも富んだ素晴らしい本である。翻訳にあたっては、原著の読みやすさを損なわないように訳者一同できるかぎり努力をした。もちろん、原著のよさがどれだけ伝わるかは不安が残るが、できるだけ幅広い読者に読んでいただきたいと願っている。最後に、こうした思いを受け止めて、厳しい出版事情のなか、本翻訳書の出版を快く引き受けてくれた勁草書房と担当編集者の山田政弘氏に感謝する。