

平成30年度産業経済研究委託事業
（経済産業政策・第四次産業革命関係調査事業費）
（データ流通秩序に係る技術及び法令に関する調査）
調査報告書

平成31年 3月

みずほ情報総研株式会社

目次

1. データ流出や流出時の被害を防ぐために	2
1.1 はじめに	2
1.2 データの種類	4
1.2.1 管理や利用の主体による分類.....	4
1.2.2 価値の源泉による分類	6
1.2.3 被害の影響による分類	9
1.3 データの保護方法	12
1.3.1 組織的対策	12
1.3.2 技術的対策	20
1.3.3 物理的対策	39
1.3.4 データ保護のための対策と契約との組合せ	40
1.4 データの保護に関してどのような対策をとるべきか	45
1.4.1 データ保護に関する方針策定の手順.....	45
1.4.2 データ保護に関する対策の考え方.....	49
1.4.3 データの特徴に応じた対策の選定.....	54
1.4.4 データの保護における利便性とのバランスの考え方.....	58
1.4.5 データ保護に関する方針を検討する上での参考情報.....	61
1.5 データ保護に用いる技術等の将来的な変化への対応	63
2. データ流出時の法的な救済について	66
2.1 データ保護に関する法律について	66
2.1.1 データの保護に関する法律の種類と役割.....	66
2.1.2 救済対象となる違法行為とその被害の分類	74
2.1.3 救済措置による分類.....	79
2.1.4 データに関する被害とそれに対応する法律との関係.....	81
2.2 法的救済に関する国内事例の紹介	83
2.2.1 データに係る事案数の推移	83
2.2.2 個別事案についての分析.....	83
参考文献.....	139

1. データ流出や流出時の被害を防ぐために

1.1 はじめに

(1) 背景

企業における IT の利活用が進むと同時に、企業における各種の業務で取り扱う情報も、従来の紙媒体主体から IT 機器や電子媒体で保存される電子データ（以下、「データ」という。）の形態で利活用される割合が増えている。データとして利活用することで、企業はより多くの付加価値を生じさせることが可能となることから、現在経済産業省による“Connected Industries”の提唱のもと、様々なつながりにより新たな付加価値が創出される産業社会を目指し、いっそうのデータ利活用を促進するための環境整備等のさまざまな取組がなされているところである。

反面、企業におけるデータが不正に利用されたり、データを利用する権利をもたない者に参照されたりするリスクは、情報が紙媒体に記録されている場合と比較して増大する。そこで、企業が安心してデータを利活用できるようにするためのデータの保護に関する取組の必要性は、企業において軽視できない経営課題となっている。インターネットにおけるマルウェア¹の蔓延やサイバー攻撃があらゆる企業にとって脅威として認識されつつある中で、ウイルス対策ソフトウェアの導入、ソフトウェアの更新、不正アクセスの監視、データの暗号化などの一連の情報セキュリティ対策を導入する企業が着実に増えてきている。一方、これまでの情報セキュリティ対策は、データの漏えいなどの事故を発生させないことを目標として整備されてきたが、現在のインターネットをはじめとするサイバー環境においては、ゼロデイ攻撃と呼ばれる未知、もしくは対処方法が確立していない脆弱性を悪用した攻撃や、発信者を巧みに偽装して行われる標的型攻撃など、適切な情報セキュリティ対策を講じていても完全に防御することが困難な場合も増えつつある。さらに、企業内での内部不正によるデータの流出事故なども生じており、こうした「事故前提社会」とも呼ばれる状況の中で、データの利活用を通じた企業における事業上のリスクを軽減するためには、個別の脅威に対処するための情報セキュリティ対策のみならず、データの不正利用を企図する者に対する刑事罰、差止請求、損害賠償請求などの法的措置の適用を可能とするための体制や環境の整備が欠かせない。

平成 30 年 5 月には、いわゆる「ビッグデータ」のような、従来の営業秘密の範疇で扱うことが難しい新しい流通形態で扱われるデータを不正利用から保護すること等を目的とする不正競争防止法²の改正、ならびに人工知能 (AI) の利活用に対応した著作権法³においても改正が実施されており、企業においてデータの利活用を事業の源泉として推進しつつ、それに伴う事業リスクを適

¹ 「悪意のあるソフトウェア (malicious software)」の略称。コンピュータウイルスに限らず、インターネットワームやランサムウェアなど、利用者の意図に反して動作し、利用者に不利益を与えるようなソフトウェアを総称するもの。

² 平成五年法律第四十七号。平成 30 年改正不正競争防止法における限定提供データ関連の改正内容の施行は 2019 年 7 月 1 日を予定している。

³ 昭和四十五年法律第四十八号

切に抑制していくためには、こうした法改正の趣旨を踏まえて、それぞれの要件を満たすような対策を導入することが極めて重要である。

(2) 本書の目的

本書は、前述の背景を踏まえ、企業におけるデータの流出や安全なデータの利活用を実現するために、企業において対策を講ずべき内容についてまとめたものである。これまで紙媒体に記録されていた秘密文書を安全に保管しようとする場合、施錠可能なキャビネット等に格納し、その鍵を安全な場所に保管するとともに、秘密文書として取り扱い規定や管理担当者を定めて、違反した場合に罰則を課すような対策が行われてきた。電子的に扱われるデータについてもこれらの対策に相当する措置を行うことが求められる。このとき、紙媒体をキャビネットに施錠して保管することに相当するのが、データの保護のための技術的対策である。紙媒体の場合と異なるのは、データの形態や役割が多様であり、それに応じて技術的対策にも多くの種類が存在するため、企業において自社での事業活動の特徴に怖じて選択する必要があることである。一方、データを保管するサーバ等を安全なところに設置するなどの物理的対策や、データの取り扱いに関するルールを設定し、管理担当者を定め、そのルールに違反した場合に罰則を課すような組織的対策については、紙媒体と同様に実施することが適切である。

本書では、こうした観点のもと、データの保護に関する方法を選択するために企業において知っておくべき事項として、データの種類と保護方法を紹介した上で、どのような方法を選択するかを選び方についての説明を行う。さらに、データが流出した場合の法的な救済措置として、関係する法律についてその種類と役割について説明するとともに、データの流出の状況と適用される法律との関係について整理する。

1.2 データの種類

企業において扱われるデータは、個人情報のように法律で保護が義務づけられているものもあれば、製品カタログのように不特定多数に公開しているものもあるなど様々である。一般に、データを厳重に保護しようとするほど、保護のためのコストが高くなったり、使い勝手が悪くなったりするため、すべてのデータを同じように保護することは合理的ではない。そこで、データをどのように保護するかを考えるにあたっては、保護対象となるデータにどのような特徴があるかについて把握した上で、その特徴に応じた保護のための対策について検討する必要がある。ここでは、データの特徴を把握するための視点として、「管理や利用の主体」「価値の源泉」「被害の影響」の3点について説明する。

1.2.1 管理や利用の主体による分類

データの保護を考える上で最も重要な要素は、データを利用できる範囲をどのように限定するかである。データの漏えいとは、予め定められたこの範囲の外部において当該データが利用できてしまうことに相当するものであり、データを利用するのは誰か、また管理するのは誰かを念頭に置いた上で保護の方法を考える必要がある。そこで、企業で扱うデータの利用者や管理者の違いでデータを分類してみると、次のような整理が可能である⁴。

(1) 自社単一部門で閉じて利用するデータ

企業のある部署で作成されたデータを、同一の部署のみで利用するものである。データの所有者である部署と利用者である部署とが同一であるため、後述するような管理上の問題が生じにくい。一方で、単一の組織内での利用に限定されていても、データの保管や移送などを通じて外部への漏えい等のリスクはある。よって部外者への流出によって事業上の損失が生ずる恐れのあるデータについては、他のデータと同様、保管時や移送時の暗号化などのデータ保護のための対策を講じる必要がある。しかしながら、部署外への提供を想定しないデータについては管理すべき対象から見落とされ、その結果データ保護がなされないままとなる可能性があることに留意する必要がある。

(2) 自社内で部門横断的に利用するデータ

ある企業内において、データを作成し、管理している部署と、そのデータを利用する部署とが異なる形態で用いられるデータである。この場合、データを扱う部署それぞれでデータの管理に関するルール（例：重要情報管理手続、データ利用手順等）を定めて利用される。それらのルールは共通のほうが管理は一般に容易であるが、部署で扱う業務の内容によっては異なるルールで

⁴ 利用者が自由に利用可能なデータであっても、データの管理者ないし著作権者が存在した上で自由な利用を許諾している場合が多い。ただし保護期間を超過した著作物や発明などは、「パブリックドメイン」として公有の状態にあるとされる。

運用したほうがよい場合もある。例えば、ある部署ではデータの更新作業を行うが、ある部署では参照するのみである場合、更新作業を行う部署のみにおいて、データの編集を許可するようなルールとすることで、全体の安全性が高まることが期待される。このように、データの利用形態に応じた最適なルールを策定し、そのルールに基づいて利用する仕組みを構築することが、この分類に相当するデータにおける対策の要となる。

(3) 自社と他社間で利用するデータ

自社で作成し、管理しているデータを他社に提供する場合、またはその逆のような場合がこれに該当する。このほか、他社との間で業務目的のコンソーシアムを形成し、そのコンソーシアムで作成されたデータを参加各社が利用する形態も含まれる。この場合、データを所有する企業ないしコンソーシアムにおいてデータの取扱に関するルール（例：秘密保持契約、コンテンツの利用許諾ポリシー等）を作成し、データを利用する企業がこのルールに従って利用するのが一般的である。どのようなルールを規定する必要があるかは、データの性質や利用方法に依存する。ルールに違反した場合の罰則の規定についても、ルールの実効性を高めるために有効である。

なお、現状において、機械学習システムをはじめとする人工知能（A I）は自らの意思のもとでデータを作成する主体とはみなされていない⁵ため、「A I が作成したデータ」という表現が用いられていても、A I 機能を提供するプログラム（ソフトウェア）が生成する出力データをどのように扱うかの問題に過ぎない。出力データの扱いについては、当該プログラムの利用に関してA I の提供元が定めているデータの取扱に関するルールに従う必要がある。

コラム：他社とのデータのやりとりにおける様々な形態⁶

以下の事例では他社との間で明示的なデータの移送が発生するわけではないが、実質的には自社のデータを他社が利用したり、他社のデータを自社で利用したりするデータ利活用の形態に相当する。したがって、こうしたデータを保護するためには、実態としてのデータの管理形態に応じてその保護方法を検討する必要がある。

- 自社サービスの API（アプリケーションプログラミングインタフェース）の公開（他社が API を用いて作成するシステム上で、自社のデータが扱われる）
- 自社サイトに広告を掲載する際の広告プラットフォーム提供事業者が用いる Cookie 情報の保存（自社サイトで他社データを扱う）
- 自社のサービス内でパートナー企業が独自のサービスを提供（同上）

⁵ 有識者ヒアリング調査結果による。

⁶ 企業ヒアリング調査による。

(4) オープンプラットフォームから情報取得して利用するデータ

公的な機関などが公表しているオープンデータ（例：国土地理情報、気象データ等）を取得し、それを自社で適宜加工して利用するデータに相当する。こうして加工され、新たに付加価値を加えられたデータは、データの提供者の許諾を得るなど一定の条件のもとで、自社の事業において有償で提供するなどの利活用が可能な場合もある。本項に分類されるデータの場合、オープンデータを用いていることに伴う取り扱い上の考慮が必要な場合を除けば、対策の考え方は（3）と同様である。

(5) 他社とオープンプラットフォームから情報取得して利用するデータ

(4) で取得したオープンデータ以外に、他社からもデータを取得して利用するようなデータである。この場合は、他社が定めるデータの利用条件に従う必要がある。具体的な事例としては、国土地理情報のほかに、鉄道事業者から時刻表データを取得することで公共交通利用のナビゲーションシステムを構築する場合などが当てはまる。本項についても、対策の考え方は（4）に準じる。

(6) 自社情報をオープンプラットフォームで共有して利用するデータ

自社で所有している情報を適切に加工した上で、オープンデータとして利用者を限定せずに利用可能な形で提供するデータに相当する。事例としては、株価や為替レート、貴金属の取引価格などが該当する。本項に相当するデータは、公表することが前提であるため秘密の保護に関する対策は不要であるが、不正に改ざんされないようにするための対策について考慮する必要がある。

1.2.2 価値の源泉による分類

データの保護に関して利用範囲に続いて着目すべきは、データの価値と利用方法の関係である。自分達だけが利用できるような状況に置くことで価値が産まれるデータもあれば、最新であることや、他者と共有することが価値を産むデータもある。このように、データがどのような状況のもとで利用されることで価値を産むかの違いを価値の源泉による分類としてとらえると、企業が扱うデータは次の5種類に整理される。

(1) 秘密にしておくことが価値を産むデータ

新製品の企画書や特許出願前の発明内容など、企業における営業秘密として扱うべきデータがこれに該当する。営業秘密は不正競争防止法において、「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」として定義されている。一般に営業秘密は秘密データである以上、企業内に閉じた形で取り扱わ

れることが原則であるが、企業コンソーシアムなど複数の企業等が連携して行う活動の内部において、共同の秘密データとして共有している場合についても同様に営業秘密として扱うことができる。こうした企業等にとっての秘密性を伴うデータは、攻撃側から見れば不正に入手することが自らの利益につながるため、サイバー攻撃などの不正アクセスの対象や、内部不正行為による持ち出しの対象となりがちである。

これに対して、個人データやマイナンバー等のデータは秘密として管理することそのものが価値を産むわけではないが、漏えいが生じかねないような状況で管理することが法律違反になるほか、データが漏洩することで社会におけるレピュテーションの低下等、負の効果を生じさせるため、結果的にデータを用いる際には必然的に秘密として扱う必要のあるデータであり、この分類に該当するものである。

これらのような秘密として扱う必要のあるデータを保護するための原則は、「Need to Know の原則」（知る必要のある人のみに情報を知らせる）として知られ、アクセス可能な利用者を限定する組織的対策と、データを保存するサーバ等におけるアクセス制御や暗号化などの技術的対策の組み合わせによって実現される。この具体的な対策方法について、1. 4. 2（1）にて詳細を示す。またこれらの対策とともに、不正競争防止法など、データを保護することを目的とする法律の適用を可能とするための要件を満たすことも重要である。

（2）更新されていることが価値を産むデータ

株価、為替レート、気象情報など、データの内容が最新であることが価値を産むものである。こうしたデータにおいては、古くなってしまったデータは価値をもたないことから、積極的な保護を行う必要がない場合も存在する。一方で、古くなったデータであっても、例えば「10年間の株価の経過」として集積されることで別の価値が認められるような場合があり、こうした活用を想定したデータの蓄積や管理方法についても考慮すべき状況が存在する。

こうしたデータの保護において重要なのは、「データをいかに正確な状態で管理し、確実に提供するか」であって、悪意によるデータの改ざんや消去、サービスの中断などを防ぐための保護対策が求められる。

（3）誰かと共有していることが価値を産むデータ

グループウェア上で管理されているデータなど、複数の関係者がアクセス可能な状態にあることに価値が存在するデータである。こうしたデータの保護においては、関係者以外からのアクセスを防ぐ一方で、関係者に対してはアクセスしたいときに負担なくアクセスできることが望ましく、グループウェアのようなこうした用途に対応した技術的手段を用いてデータを管理することが一般的に行われている。

こうしたデータの保護にあたっては、共有対象者以外による不正使用を防ぐための対策を実施することが重要である。具体的な対策方法については、（１）と同様であり、共有者のみデータにアクセスできるようにアクセス制御等の対策を用いるとともに、法的な保護が適用できるようにするための要件を満たすことが想定される。

（４）オープンデータ

自由に使えることに価値があるデータである。例として、法人番号は政府機関において法人番号データベースを提供することを通じて、法人の实在確認手段としての価値を創出している。GPS（Global Positioning System）や準天頂衛星システムで提供されるデータも、自由な利用が認められていることから、オープンデータ的一种とみることができる。

このほか、オープンソースソフトウェアのように、公開されていることでソフトウェアに脆弱性がないことを多くの目で確認されていることが価値を産むものもある。

こうしたオープンデータについては、厳密には「あらゆる人が対象のデータを自由に閲覧し、利用し、修正し、そして共有できる」⁷ようなデータのことを指す。誰もが常にアクセス可能なデータであることから利用者が積極的にその保護を考慮する必要はないが、一般にオープンデータに相当する扱いで用いられているデータには、一定の条件の範囲内でオープンな利用を認めているものが存在する。こうしたデータについてはその条件に違反するような利用を検出し、防止するような対策を講じる必要がある。このほか、オープンデータを加工して独自のデータを作成しているような場合は、オープンデータ由来であってもその加工したデータの特徴や用途に応じて（１）～（３）の対策を講じる必要がある。

（５）その他のデータ

（１）～（４）のいずれの条件も満たさないようなデータに相当する。具体的には、自社ウェブサイトで公開している、自社製品の利用方法に関する説明資料などは（１）～（４）のいずれにも当てはまらないデータである。このようなデータについては、前述のような「秘密にすること」「常に更新し続けること」「他社と共有すること」「オープン化されていること」といった要件を確保する必要はないが、例示した説明資料であれば、「製品の顧客から常にアクセスできるようにする」といった可用性を確保する必要性を考慮するなど、データの特徴に応じた保護等の対策が求められる。

⁷ Open Knowledge International の Open Definition プロジェクトにおける定義による。ただし、同プロジェクトにおいてもオープンデータとしての出自情報やオープンさの保持を目的とする制限は許容している。詳細は下記にて公開されている「オープン定義」を参照。
<http://opendefinition.org/od/2.1/ja/>

1.2.3 被害の影響による分類

データがどのような状態になった場合に、企業にとって損害が生ずるかは、データの保護方法すなわち対策を考える上で極めて重要な要素である。企業における被害がもたらす影響の違いによってデータを分類すると、次のように整理される。

(1) データが外部に漏えいすることで被害が生じるもの

1.2.2(1)に相当するデータと概ね対象範囲が重なるが、データの内容が外部に漏えいすることで、企業における被害を生じさせる場合である。外部への漏えいの経緯により、次のように分類される。

① 自社内からの流出

自社内で管理していたデータが、社外に漏えいする場合である。

ア) 自社従業員の過失に起因するデータの漏えい

標的型攻撃のように、自社従業員を欺くことでデータの漏えいが生ずる場合についてはウ)でまとめて扱うものとし、ここでは外部に不正を企図する者が存在しない状況で、データが漏えいする場合について扱う。具体的には、一般従業員による社外でのPCやUSBメモリの紛失・盗難、電子メールの宛先誤送信、システム管理者によるアクセス制御の設定ミスなどが含まれる。こうした漏えいに対する対策としては、「過失を生じにくくする」及び「過失が発生した場合の被害を最小限にする」の2種類の対策を併用することが有効である。

イ) 内部不正に起因するデータの漏えい

自社従業員や委託先など、本来はデータの保護に努めるべき要員が悪意で漏えい等の不正行為を行う場合である。米国の組織犯罪研究者であるドナルド・R・クレッシーによれば、不正行為が実施される背景には、次の3種類の要因からなる「不正のトライアングル」が存在するとされる⁸。

- 動機・プレッシャー（不正を行うことを欲する理由）
- 機会（不正行為を実施できる環境）
- 正当化（不正を正当化しようとする言い訳）

ゆえに、内部不正を防止するには、状況的犯罪予防の考え方にに基づき、次に示す5点の基本原則に従った対策を実施することが効果的である⁹。

- 犯行を難しくする（不正行為を実施しにくくする）
- 捕まるリスクを高める（監視強化などで不正を露見しやすくする）

⁸ Donald R. Cressey: Other People's Money: Study in the Social Psychology of Embezzlement, Wadsworth Publishing Company, 1972.

⁹ 内部不正対策の詳細については、独立行政法人情報処理推進機構（IPA）が公表している『組織における内部不正防止ガイドライン』にて説明されている。

<https://www.ipa.go.jp/security/fy24/reports/insider/>

- 犯行の見返りを減らす（利益を得にくく、割に合わないようにする）
- 犯行の誘因を減らす（不正を起こそうとする意識を生じさせにくくする）
- 犯罪の弁明をさせない（自らの行為の正当化理由を排除する）

ウ) 外部からの攻撃に起因するデータの漏えい

外部からの不正アクセスやマルウェアの感染など、サイバー攻撃を通じてデータが漏えいする場合である。発信者を詐称した電子メールを従業員が開封することで、マルウェアに感染して漏えいが生ずるなどの標的型攻撃もこの分類に含まれる。攻撃の動機としては、ブラックマーケットで販売できるデータを入手するといった金銭目的のものから、競合他社の営業秘密を入手しようとする明確な意図に基づくものまで多様であり、そうした動機に応じて攻撃方法も多様である。こうした攻撃への対策は、一般的なサイバーセキュリティ対策と共通なものとして考えることができる。

② 管理義務を負わせる態様でデータを提供した他社からの流出

提供先との間で提供したデータの管理義務を課すような形の契約を締結している状況において、その提供先からデータが漏えいした場合、提供先の契約違反として損害賠償請求等を行うことが一般的である。ただし、損害賠償請求による損害の補償よりも、データの流出によるレピュテーションリスクや、個人情報等が対象であった場合の法律違反等のほうが重大な問題となる場合は、契約を通じて適切な管理の実施を求めるだけでなく、提供先への立入検査などを通じて適切な対策が講じられていることを確認するなどの措置も併用される。

③ 売買契約等に基づきデータを提供した他社からの流出

データを販売もしくは使用許諾することによって、データを提供していた場合にその提供先から流出した状況に相当する。この場合、データの提供に伴って提供先との間で取り交わす売買契約等においては、データの保護に関して明示的な対策の実施義務を課すことは少ない。こうした売買契約等によって提供されたデータの不正利用を防ぐための対策として、電子透かし等のトレーサビリティ技術を用いてデータに自社のデータであることの証拠を付与し、これを活用することで不正利用の発見と差止等の措置を行うなどの方法が用いられている。

(2) データの改ざんや消失によって被害が生じるもの

(1) で示したデータは、機密性が損なわれることで企業における被害が生ずるものであるが、本項に相当するデータは完全性が損なわれることで被害が生ずるものである。具体的な例としては、ウェブサイト上の記載内容、商品の在庫に関するデータ、従業員の勤務状況に関するデ

ータ等、データの内容が不正確になることで、事業に影響が生ずるものである。

なお例示したデータのうち、ウェブサイトの記載内容については機密性を求める必要はないが、従業員の勤務状況などは完全性に併せて、機密性の確保についても同様に求められるなど、機密性との関係は一樣ではない。

1.3 データの保護方法

企業において、データの保護のために用いられる対策には、「組織的対策」「技術的対策」「物理的対策」の3種類が存在する。ここではそれぞれの概要と具体的な保護方法の違いについて説明する。

1.3.1 組織的対策

データの保護や管理に関する組織内のルールを定め、組織におけるデータの管理体制を整備した上で、そのルールに基づいた運用を行うことによって、データを保護する。技術的対策等の他の対策と組み合わせて実施することが原則である。

(1) 組織におけるデータ保護や管理のためのルールの策定

データの流出などの被害発生を防ぐために、データを取り扱う者が遵守すべき組織内ルールを策定する。ルールを策定するにあたって考慮すべきものを次に示す。

① データの保護に関する遵守事項を定める法律

企業で扱うデータの種類によっては、法律によりその取扱方法が定められているものが存在する。これらは必ず遵守することが求められる。以下にその例を示す。なお、法律の名称については、わかりやすさの観点から一般に用いられている通称にて表記し、初出時の脚注にて正式な名称を記載することとする。

ア) 個人情報

個人情報保護法¹⁰によって「個人データ」と定められているデータについては、その取扱事業者は次の措置を行うことが義務づけられている。

- 個人データに関する安全管理措置の実施（個人情報保護法第20条）
- 個人データを扱う従業員の監督（個人情報保護法第21条）
- 個人データの取扱を委託する場合の委託先の監督（個人情報保護法第22条）

イ) 特定個人情報（マイナンバー）

番号法¹¹により、マイナンバーが記載されたデータを利用した事務等を行う事業者は、次の措置を行うことが義務づけられている。

- マイナンバーが記載されたデータの漏えい、滅失又は毀損の防止その他の管理（番号法第12条）
- マイナンバーが記載されたデータを利用した事務等を委託する場合の委託先の監督（番号法第11条）

¹⁰ 個人情報の保護に関する法律（平成十五年法律第五十七号）

¹¹ 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号）

ウ) 匿名加工医療情報

次世代医療基盤法¹²において、医療情報及び匿名加工医療情報等の取扱いに関して、次の措置を行うことが義務づけられている。

- 管理する医療情報又は匿名加工医療情報の安全管理措置の実施（次世代医療基盤法第 20 条）
- 管理する医療情報又は匿名加工医療情報を取り扱う従業員の監督（次世代医療基盤法第 21 条）
- 管理する医療情報又は匿名加工医療情報の取り扱いを委託する場合の委託先の監督（次世代医療基盤法第 24 条）

エ) 事業で扱うデータの取扱

以下の各法において、データを扱う事業者に対し、データの取扱いについて定めている。

- 通信の秘密の保護（電気通信事業法¹³第 4 条）
- 有線電気通信における秘密の保護（有線電気通信法¹⁴第 9 条）
- 無線通信における暗号化されたデータの保護（電波法¹⁵第 109 条の 2）
- クレジットカード番号の適切な管理等（割賦販売法¹⁶第 35 条の 16 及び 17）

オ) 刑法で定める業務における守秘義務

刑法¹⁷（第 134 条）により、医師、薬剤師、医薬品販売業者、助産師、弁護士、弁護人、公証人又はこれらの職にあった者、ならびに宗教、祈祷若しくは祭祀の職にある者又はこれらの職にあった者は、業務上取り扱ったことについて知り得た人の秘密を正当な理由無く漏えいすることが禁じられている。

カ) 師法や士法において定める守秘義務

保健師、助産師、看護師、放射線技師、理学療法士、作業療法士については、それぞれ保健師助産師看護師法¹⁸（第 42 条の 2）、診療放射線技師法¹⁹（第 16 条）、理学療法士及び作業療

¹² 医療分野の研究開発に資するための匿名加工医療情報に関する法律（平成二十九年法律第二十八号）

¹³ 昭和五十九年法律第八十六号

¹⁴ 昭和二十八年法律第九十六号

¹⁵ 昭和二十五年法律第三百三十一号

¹⁶ 昭和三十六年法律第五百十九号

¹⁷ 明治四十年法律第四十五号

¹⁸ 昭和二十三年法律第二百三十三号

¹⁹ 昭和二十六年法律第二百二十六号

法士法²⁰（第 29 条）において、オ）と同様に業務上知り得た秘密の漏えいが禁じられている。

キ) 海外の法令等

欧州連合（EU）加盟国に国籍を有する人に関する個人データを取り扱う場合は、EU の一般データ保護規則（GDPR）を遵守する必要があるなど、事業の内容に応じて、海外の法制度への対応が必要となる場合もある。

② 事業分野に関連するガイドライン等

法的な拘束力はないものの、企業等の活動における望ましいデータ保護対策の考え方を示す文書として、公的機関等から各種のガイドラインが公表されている。具体的にどのようにデータを保護すべきかを検討する際には、こうしたガイドラインを参照することが有用である。

ア) すべての業種を対象とするもの

以下に業種に関わりなく、すべての企業において参考とすることのできるガイドラインの例を示す。

- 個人情報の保護に関する法律についてのガイドライン（個人情報保護委員会）²¹
- 特定個人情報の適正な取扱いに関するガイドライン（事業者編）（個人情報保護委員会）²²
- サイバーセキュリティ経営ガイドライン（経済産業省）²³
- 営業秘密管理指針（経済産業省）²⁴
- 中小企業の情報セキュリティマネジメントガイドライン（独立行政法人情報処理推進機構（IPA））²⁵

イ) 特定の業種を対象とするもの

業種ごとに関係機関や業界団体により策定されている。

- 重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（内閣サイバーセキュリティセンター）²⁶
- 国土交通省所管重要インフラにおける情報セキュリティ確保に係るガイドライン（鉄道分野、物流分野、航空分野、空港分野）（国土交通省）²⁷
- 建設現場における情報セキュリティガイドライン（一般社団法人日本建設業連合会）²⁸

²⁰ 昭和四十年法律第百三十七号

²¹ <http://www.ppc.go.jp/personal/legal/>

²² <https://www.ppc.go.jp/legal/policy/>

²³ http://www.meti.go.jp/policy/netsecurity/mng_guide.html

²⁴ www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf

²⁵ <https://www.ipa.go.jp/security/keihatsu/sme/guideline/>

²⁶ <https://www.nisc.go.jp/active/infra/siryou.html>

²⁷ http://www.mlit.go.jp/sogoseisaku/jouhouka/sosei_jouhouka9999.html

²⁸ https://www.nikkenren.com/kenchiku/ict/result/2015_02_guideline.html

- 金融機関等コンピュータシステムの安全対策基準（公益財団法人金融情報システムセンター）²⁹
- 医療情報システムの安全管理に関するガイドライン（厚生労働省）³⁰
- 教育情報セキュリティポリシーに関するガイドライン（文部科学省）³¹

③ 自社内の既存ルール

①②のほか、自社で策定している以下のような文書との整合を図る必要がある。カッコ内に具体的に参考にするべき内容を示す。

- 文書管理規程（文書管理責任者等の役割と体制）
- 事業継続計画（データのバックアップ方針等）
- セキュリティポリシー（セキュリティ確保のための社内体制）
- 個人情報保護ポリシー（個人情報の保護方針）
- プライバシーポリシー（プライバシー情報の保護方針）

コラム：従業員向けルールは適切な分量に抑制すべき³²

データを適切に保護するために考慮すべき事項は多く、一般にルールに相当する文書の分量は多くなりがちである。一方で実際にデータを扱う従業員にとっては、分量の多いルールを把握し、それに基づいて作業を行うのは多大な負荷となる。さらに、社内で扱うすべてのデータについてのルールを従業員向けに展開してしまうと、従業員は自分が扱うデータについての管理方法がどこに書いてあるかを探すのに時間を要してしまい、業務効率の低下につながりかねない。こうした事態を回避するため、従業員向けのルールは必要最低限になるように配慮し、事業部署ごとに、当該部署で扱う情報に絞ったマニュアルの形で整備するなどの工夫が考えられる。

（２）データ保護のためのルールの管理体制の構築

① データ保護のために必要となる機能

（１）で整備したルールを遵守させるための組織内体制を構築することになる。データ管理に関するルールを適切に遵守させるためには、社内体制（必要に応じて外部委託先を含む）において次表のような役割を担う機能を設ける必要がある。

²⁹ <https://www.fisc.or.jp/guideline/>

³⁰ <https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000027272.html>

³¹ http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm

³² 企業ヒアリング調査による。

表 1 データ保護に関する社内体制において担うべき機能と作業例

担うべき機能	機能の定義	機能に対応して実施する作業の例
企画機能	ルールの策定や環境変化(法律等の改正を含む)に応じた見直しを行う	<ul style="list-style-type: none"> ● 社内ルールの策定、見直し ● セキュリティサービスやクラウドコンピューティングサービス(以下、「クラウドサービス」という。)の選定 ● トレーサビリティの必要性についての検討
運用機能	従業員による対策実施を支援するとともに、サイバー攻撃や内部不正などの異常に関する監視、インシデント発生時の初動対応等を行う	<ul style="list-style-type: none"> ● 従業員向け ID とパスワードの発行、アカウント管理 ● 認証機能や暗号化機能を提供する機器の管理 ● セキュリティサービスベンダ、クラウドサービスベンダへの委託 ● アクセスログの監視 ● トレース結果の分析 ● 従業員による対策のサポート
監査機能	ルールが適切に運用されていることを確認する	<ul style="list-style-type: none"> ● 対策の実施状況の確認((4)①にて記述)

② 機能を提供するための体制の構築

①に示した機能を提供するための体制は、それぞれ次のように想定されるが、事業の形態や扱うデータの特徴に応じて、以下に示す内容とは異なる体制で実施することが適切な場合もある。

ア) 企画機能

情報セキュリティの観点では、「Security By Design」(設計段階までのセキュリティ対策の検討)を行うことが理想とされる。データに関するルールの策定や見直しは、一般に企業における総務部門やリスク管理部門等が行うことが一般的であるが、こうしたルールの検討を行う時点で、技術的な情報セキュリティ対策を検討する担当部署(システム企画部門や情報システム部門の企画担当者等)と連携して対策を検討することが望ましい。社内組織のみで適切な対策を検討することが困難な場合は、情報セキュリティサービスベンダやコンサルティングサービスベンダよりコンサルティングを受けることも想定される。

イ) 運用機能

データを保管または利用する情報機器やシステムの管理者が運用機能を担うのが一般的である。こうした運用を外部にアウトソーシングする場合は、アウトソーシング先の外部事業者も体制に含まれることとなる。データの保管先がクラウドサービスの場合は、クラウドサ

ービス事業者が運用機能の一部のアウトソーシング先に相当する。

ウ) 監査機能

自社内に監査を行う部署が存在する場合、当該部署が実施するのが一般的である。後述の(4)①にて示すように、自己点検を行う場合は運用担当部署、外部監査を実施する場合は外部の監査サービス事業者が体制を構成することとなる。

(3) データ保護に関する運用管理

(1) で策定したルールをもとに、(2) で構築した体制にて運用を行う。具体的な次のような作業が対象となる。

① 通常時の運用業務

②に示すようなトラブルの発生時以外に行うことを想定する運用業務を示す。

ア) データの利活用に伴う管理作業

業務の受発注や利用者の異動、役割の変更などが発生する都度、適切な保護が維持されるように行う作業である。以下にその例を示す。

- 利用者の登録、削除、属性変更（所属部署異動等）
- 業務毎のアクセス権の付与、削除
- 利用者によるパスワード失念等への対応

イ) 異常の監視

データを保管する情報システムやそれらに接続されるネットワークにおける操作や通信のログをもとに異常を監視する。また、情報システムに既知の脆弱性がないことを定期的を確認する。脆弱性がないことの確認方法の詳細については(4)②にて説明する。

ウ) 利用者の教育

利用者にデータ保護の重要性を認識してもらうとともに、保護のため利用者が実施ないし留意すべき事項についての教育を行う。教育は着任時のほか、重要事項の徹底や最新動向の周知を目的として、定期的に行う必要がある。

コラム：ルールに関する教育や確認を効率化する工夫

社内でデータの取扱に関するルールを策定しても、それが従業員に周知されていなければ、その効果を発揮することはできない。実施上の有効性の観点からは、集合研修を行い、終了時

に理解度テストを行うことで、実際にルールを理解しているかどうかを確認することが望ましいが、従業員にとっての負担も大きい。そこで、データ保護に関する従業員向けやシステム管理者向けの e ラーニング形式の教材を作成し、従業員が各自の都合のよい時間に受講できるようにする方法³³は、従業員の時間的拘束を抑制しつつ、受講履歴を電子的に確認できるなどの管理上の効果も期待できるため、優れた方法といえる。

このほか、従業員に対してルールを遵守する旨の誓約を求める場合も、その方法として e ラーニングに類似の環境で実施すると、従業員の手間も省け、エビデンスとしての有効性も確保できるなどメリットが多い。

② インシデント発生時または懸念時の初動対応

データの漏えいが懸念される事象が発生した場合、あるいは実際に漏えいが発生した場合、被害の拡大防止と被害範囲の特定のため、通常時の運用とは異なる活動を行う必要がある。このための体制は、一般に CSIRT (Computer Security Incident Response Team) と呼ばれる。企業内で CSIRT を構築し、運用する方法については、一般社団法人 JPCERT コーディネーションセンター³⁴や日本シーサート協議会³⁵等から参考資料が公表されている。

CSIRT が効果的に機能するためには、インシデント発生時または懸念時のみでなく、日頃からインシデント発生の予防や、発生に備えた準備を行っておくことが有用である。日本シーサート協議会が公表している資料³⁶では、CSIRT が提供すべき機能として次に示す 3 種類を提示している。同資料において示されている内容をもとに、CSIRT が保有すべき主要な機能とそれを構成する作業を次に示す。

ア) インシデント事後対応サービス

- インシデントハンドリング (インシデントの検知から対応、結果報告に至る一連の処理の総称)
- コーディネーション (複数部署によるインシデント対応を行う場合の調整作業)
- デジタル・フォレンジック (本書 1. 3. 2 (2) ⑦参照)
- インシデントレスポンス (インシデントによる被害の局限化し、復旧させるための対応作業)
- アーティファクトハンドリング (不審なプログラムの分析等)

³³ 企業ヒアリング調査にて実践事例を確認。

³⁴ https://www.jpcert.or.jp/csirt_material/

³⁵ <http://www.nca.gr.jp/>

³⁶ 『CSIRT スタータキット Ver2.0』(日本シーサート協議会)

<http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf>

イ) インシデント事前対応サービス

- 情報セキュリティに関する情報提供・アナウンスメント
- 脆弱性情報ハンドリング（ソフトウェアやハードウェアの脆弱性に関する情報を、影響する部署に適切に伝達する作業）
- インシデントの検知
- セキュリティ対策等に有用な技術動向調査の実施

ウ) セキュリティ品質向上サービス

- リスク分析・評価（対象となる情報システムのリスクとその影響度の分析作業）
- 事業継続／災害復旧計画の作成・見直し
- 情報セキュリティに関する教育・トレーニング・啓発活動
- 製品評価（利用する製品やサービスが安全かどうかの評価作業）

なお、これらの作業のうち、専門的な知識や技術を必要とする作業については、専門事業者への委託により対応することも一般的に行われている。

(4) データ保護対策に関する実施状況の確認

① 運用状況の確認方法

データ保護に関する対策の実施状況を確認する方法としては、一般に次の3種類の方法が利用される。

ア) 自己点検

データ保護に関する対策を実施する当事者が、対策実施状況に関するチェックリスト等をもとに対策実施状況の適切性について自己評価するものである。あくまで自己評価であるので、客観性は乏しいが、当事者に自覚を促す効果は期待できる。

イ) 内部監査

社内に専門の組織を設けて、その組織が対策の実施状況について監査を行う。監査人は業務とは独立した立場であるため、①と比較して客観性の高い確認効果が期待できる。

ウ) 外部監査

外部の情報セキュリティ監査サービス事業者等³⁷に、データ保護に関する対策実施の適切

³⁷ 独立行政法人情報処理推進機構（IPA）では平成30年度より、経済産業省が定めた情報セキュリティサービス基準を満たす情報セキュリティサービス事業者を以下のURLにて公表している（情報セキュリティサービス審査登録制度）。

性に関する監査を委託するものである。第三者による極めて客観的な視点からの確認が行われるため、確認の効果としては最も優れる反面、コスト的にも最も高価となる。一方で、専門家である情報セキュリティ監査サービス事業者による改善のアドバイス等も期待できるため、改善方策を得る方法として外部監査を利用することも考えられる。

② データ保護に関する技術的対策の実施状況の確認方法

①に示した対策状況とは別に、データを保管するサーバ等が適切に管理されていることを確認する手段として、脆弱性診断が用いられる。これは、診断対象となる機器に既知の脆弱性がないことを技術的に確認するものであり、脆弱性を悪用した不正なアクセスが不可能なことを客観的に確認するための手段として効果が期待できる。

このほか、脆弱性に限定せずに実際にサイバー攻撃で行われる手法等を擬似的に適用することで対策の適切性を確認するペネトレーションテストの実施も、重要度の高い情報システム等については考慮の対象となる。

コラム：サイバーセキュリティ関連保険

自動車保険や火災保険などと同様、個人情報の漏えいが発生した際の被害者への賠償や、不正アクセスによる損害など、サイバーセキュリティ関連の事故が生じたときの被害額が支払われるような保険制度が損害保険会社等から提供されている。本書に示すようなデータ保護のための対策を行っても、被害を完全に防ぐことは不可能であるため、保険に加入することで万一に備えることは有用である。こうした保険の場合、適切な対策を実施することによる保険料の割引制度があり、対策を行うことの経済的なインセンティブとして効果も果たしている。

1.3.2 技術的対策

データを保護するための技術的対策として、データを保護する技術及びトレーサビリティ技術について代表的なものを示す。

(1) データの外部への漏えいを防ぐための技術

データの外部への漏えいを防ぐことを、データの機密性の保護という。これに用いられる技術は、その特徴に応じて次のように分類される。

① 利用者の認証に基づくアクセス制御

データを参照する権限を有する利用者であることを認証の手続きによって確認し、認証が成功した場合にデータへのアクセス権限が提供される。認証の手続きには次のような方法が用い

られる。

ア) 知識による認証

データの利用者が有する知識の有無をもとに認証を行う。このときの知識とは、あらかじめ定めた符号のことを差し、その照合を行う方法が該当する。実際に利用されている方法には次の種類がある。

a) ID とパスワード

利用者ごとの ID と、それに対応するパスワードの組み合わせを、認証のための知識として照合の対象とする。現在、データを管理するための情報システムにおいて最も一般的に用いられている方法である³⁸。なお、複数名による ID とパスワードの共用（例：ある部署用の ID とパスワードを発行し、部署内メンバーで共用する）は、誰が操作を行ったかの特定ができないことで、内部不正の要因になりやすいことと、パスワードを知っているメンバーが異動などで担当から外れても引き続きアクセスできてしまう恐れがあるなどの問題があるため、避けるべきである。やむを得ず利用する場合は、共用するメンバーの構成が変わるたびにパスワードを変更することが必要である。

b) アクティベーション

ソフトウェアなどを有償で提供する場合に、その代金を支払った利用者に個別の符号（ライセンスキーなどと呼ばれ、英数字などで構成される一連の文字列であることが多い。）を提供し、利用者はソフトウェアを初めて利用するときその符号を入力することにより、権限を有する利用者であることが識別され、ソフトウェアの機能が利用できるようになる方法である。このほか、利用者が電気通信ネットワークにおいて用いる IP アドレスをもとに利用者を識別する「IP アドレス認証」と呼ばれる方法もこの一種である。

c) ワンタイムパスワード

a) に示す方法の特殊な形態であり、パスワードは認証のたびに使い捨てにして、毎回異なるパスワードを用いて認証する方法である。ネットワークを経由してデータを利用する際に、ネットワーク上での盗聴の恐れがある場合は通常のパASSWORDを用いた認証を行うと、悪意を有する者がパスワードを知り利用者をなりすまして不正を行うことができってしまう。ワンタイムパスワードを用いた認証はこうした環境において有用である。

イ) 所有物による認証

データの利用者が有する何らかの物の有無をもとに認証を行う。このときの物には次のような例がある。

³⁸ 安全なパスワードの利用方法については、内閣サイバーセキュリティセンター（NISC）が公表している『情報セキュリティハンドブック』にて解説されている。

<https://www.nisc.go.jp/security-site/handbook/index.html>

a) 電子証明書

公開鍵暗号方式と呼ばれる暗号化方式においては、秘密鍵と公開鍵の2種類の鍵が用いられる。このうち秘密鍵を第三者により利用者が所有するものであることを認証可能とした形式のデータのことを電子証明書と呼ぶ。電子証明書を証明書として電子計算機に保存することで、ア)におけるワンタイムパスワードと同様、悪意を有する者による利用者のなりすましを防ぐ形での認証を行うことができる。この場合、電子証明書の保存された機器からのアクセスのみを許すことで、委託先等外部とのデータ移送の安全性を高める用途への利用が可能である。

b) IC カード

IC カードは、カードの内部に集積回路 (IC) チップを内蔵しており、その IC チップに記録された情報をもとに認証を行う方法である。

c) USB ドングル

IC カードと同様、USB ドングル (いわゆる USB メモリと同様の形状の記録媒体であるが、USB メモリと異なり内容の書き換えができず、認証に特化したもの) 内部の情報をもとに認証を行う方法である。

ウ) バイオメトリクス認証

指紋など固有性の高い人間の身体的特徴をデータ化して本人確認に用いる認証方式である。認証に用いられる身体的特徴の例を次に示す。

- 指紋
- 虹彩
- 顔
- 指静脈

なお、バイオメトリクス認証を提供する製品の中には偽の認証手段 (例: タンパク質で偽造した人工指) で認証に成功してしまうものもあり、選定に際しては実際の認証機能としての有効性 (認証の精度等を含む) について調査することが重要である。

エ) 多要素認証

ア) からウ) に示した認証方式を複数種類組み合わせることにより、認証の強度を高める方式である。それぞれの弱点を補う効果があることから、高度なセキュリティを必要とする用途において利用価値が高い。

② データの暗号化

データの中身を暗号化することで、復号のための鍵に相当する符号を知らない利用者による利用を制限する技術である。暗号化に用いる鍵と復号に用いる鍵が同一の方法を共通鍵暗号、異なる鍵を用いる方法を公開鍵暗号と呼ぶ。暗号化の対象の違いにより、次の3種類に分類される。

ア) データやその保存場所の暗号化

名簿などの電子ファイルを暗号化したり、営業秘密に相当するデータが格納されたフォルダや記録装置（ハードディスク等）全体を暗号化したりするなどして、データにアクセスする権利を有する者以外の利用を防ぐ技術である。暗号化されたデータはそのままでは中身を読むことができないので、参照や編集等を行う場合は利用前の復号と利用後の暗号化を行う必要がある。これは利用者にとっては煩雑であるので、ハードディスクやストレージ機器の中には、自動的に暗号化して保存する機能をもったものが存在する。こうした機能をもった製品の中には、データを保存する際に鍵の入力を求められるものと、鍵の入力なしに暗号化が行われるものの2種類が存在する。このうち前者については、鍵の内容を必要な者のみが把握しておくことで、外部からの攻撃や内部不正への対策として利用することが可能である。後者については利用のたびに鍵を入力する手間が省ける一方で、利用者のアカウントが乗っ取られてしまうと暗号化の効果は失われてしまう。このような製品は、当該装置を社外で紛失した場合などに、当該装置にログインするためのパスワードを知らない、すなわちアクセス権限をもたない拾得者が、機器を分解した上でハードディスク等の中身を参照しようとした場合のデータの漏えいを防ぐことを目的としたものであり、こうした目的のためであれば導入の価値はある。こうした暗号化方式の特徴に応じた用途について、次表に整理したものを示す。

表 2 暗号化方式による特徴の違い

暗号化方式		特徴	適した用途の例
データやフォルダ単位で利用者が都度暗号化や復号操作を実施		<ul style="list-style-type: none"> ・利用者の利便性が大幅に低下する ・利用者アカウントを乗っ取られても暗号鍵を知らなければデータの不正取得は困難 ・データの提供先に応じて異なる暗号鍵を用いることが可能 	<ul style="list-style-type: none"> ・不定期に作成されるデータの保管時の保護 ・不定期な相手先とのデータの移送時の保護
暗号化と復号を自動で実施	利用時に暗号鍵の入力が必要	<ul style="list-style-type: none"> ・利用者の利便性がやや低下する ・利用者アカウントを乗っ取られても暗号鍵を知らなければデータの不正取得は困難 	<ul style="list-style-type: none"> ・社外に持ち出す USB メモリに格納するデータの保護
	利用時に暗号鍵の入力が不要	<ul style="list-style-type: none"> ・利用者の利便性は低下しない ・利用者アカウントを乗っ取られた場合は暗号化による保護の効果が失われる 	<ul style="list-style-type: none"> ・モバイル PC に格納されたデータの保護

なお、データの暗号化に用いた鍵を失念してしまうと、当然ながら当該データの復元が不

可能となる。利便性と漏えいのリスク、消失のリスクのバランスを考慮して、安全な場所に鍵の内容の控えを残しておくことが望ましい。

イ) ネットワークを介して通信するデータの暗号化

インターネット等の情報通信ネットワークを介してデータを移送する際に、外部からの不正な参照等を防ぐための暗号化に基づく技術として、次のようなものが利用されている。

a) VPN (Virtual Private Network)

通信路を暗号化することにより、あたかも専用線を利用して情報を移送している場合のように、外部への漏えいの懸念なしに通信できるようにする技術である。

b) TLS (Transport Layer Security)

SSL (Secure Socket Layer) とも呼ばれる。インターネットを経由した通信において、電子計算機相互間での通信内容の暗号化を行う方法のうち、現在最も広く普及している技術である。

c) WPA2 (Wi-Fi Protected Access)

無線 LAN 規格に基づく通信において、基地局及び端末間での通信内容を暗号化するための技術である。無線 LAN 向けの暗号化技術としては、これまでも WEP や WPA が用いられていたが、いずれも現在ではセキュリティの観点で脆弱とされ、利用しないことが推奨されている。

d) スクランブル放送

電波を介して送信される放送コンテンツを暗号化し、その解除機能を有する受信機においてのみ当該コンテンツを利用可能とする技術である。

e) 暗号化したファイルの電子メールへの添付

③の応用例として、文書等のファイルを暗号化した上で、電子メールに添付することで、電子メールの内容が外部に漏えいしても添付ファイルの中身が外部に漏えいすることを防ぐことができる。暗号化せずにデータを電子メールに添付して送付すると、誤送信などをきっかけに情報漏えいにつながりやすいことが指摘³⁹されている。国際標準化されている S/MIME (Secure / Multipurpose Internet Mail Extensions) は、これを公開鍵暗号方式

³⁹ 有識者ヒアリング調査による。S/MIME など、簡便に暗号化で保護する機能を利用できない場合は、電子メールに添付するよりも、クラウドサービス上で提供されるファイル授受サービスを利用するほうが、誤送信による被害が起きにくく、相手方での受信確認なども可能なため望ましいと指摘されている。

を用いて実現した規格であり、電子メール全体を暗号化する。S/MIME に従って電子メールを送る場合、利用者はファイルの暗号化等の作業を意識して行う必要がない。また、PGP (Pretty Good Privacy) や GPG (GNU Privacy Guard) などの暗号化ソフトウェアも、電子メール等でファイルを送受信する際の暗号化及び復号の手段として利用されている。

ウ) 特定の機器やソフトウェアのみに利用を制限する技術

暗号化技術を用いて、契約により特定の機器やソフトウェアにおいてのみ利用を許諾するデータ (例: 映画などの映像、音楽等のコンテンツ) を、契約で認められた機器やソフトウェア以外で利用できないように制限する技術であり、次のような事例が用いられている。

a) DRM (Digital Rights Management)

デジタルデータで構成される著作物の不正利用を制限する技術の総称として用いられる。現在利用されている仕様の例を次に示す。

- WindowsMediaDRM (米国 Microsoft 社が提供)
- FairPlay (米国 Apple 社が提供)
- Adobe LiveCycle (米国 Adobe 社が提供)

コラム: 暗号化に用いるアルゴリズムの選び方

共通鍵暗号、公開鍵暗号とも、暗号化や復号に用いるアルゴリズムには複数の方法があり、中にはコンピュータの計算処理速度の向上や攻撃方法の発見などにより安全性が確保できないアルゴリズムも存在する。日本では独立行政法人情報処理推進機構 (IPA) と国立研究開発法人情報通信研究機構 (NICT) が共同で運営している暗号アルゴリズムの評価を行う組織である CRYPTREC が「電子政府推奨暗号リスト」として現時点で十分な安全性が見込まれるアルゴリズムを公開⁴⁰しており、その最新のリストに基づいてアルゴリズムを選択することが望ましい。

③ ネットワーク上の不正な通信を検知・遮断する技術

社内に構築したネットワーク上で不正な通信が行われるのを防ぐための技術であり、⑦と組み合わせて利用されることも多い。

ア) ファイアウォール

ファイアウォールは、自組織内ネットワーク (LAN) とインターネットとの境界部分に設置し、自社で利用しているサービス (ウェブアクセス、電子メール、リモートアクセス等)

⁴⁰ <https://www.cryptrec.go.jp/list.html>

に必要な通信のみを通過させ、それ以外の不正な通信を遮断する機能をもった通信機器である。2000年代にはデータのセキュリティを確保するために欠くことのできない技術と考えられていたが、現在は次のような理由で重要性が低下している。

- ネットワークルーターやネットワークスイッチ等の通信機器にファイアウォールと同様の機能を持たせることが容易になり、セキュリティ対策においてファイアウォール単体で導入する事例が減少している。
- インターネット上のクラウドサービスに重要情報を保存する場合は、重要情報が組織内LANに保存されるわけではないため、防御の機能を果たさない。
- ウイルス対策ソフトの機能が強化される中で、パーソナルファイアウォール機能が実装され、ファイアウォールと同様の不正なアクセスの遮断機能を備えた端末が増えた。
- 攻撃者はファイアウォールを通過可能な通信を装って攻撃するため、「ファイアウォールがあれば大丈夫」とは言えなくなった

一方で、組織内で利用するネットワークカメラなどにはパーソナルファイアウォール機能は実装できないため、ファイアウォールがない環境では外部からの攻撃にさらされ、データの漏えいの原因になる恐れがある。こうしたリスクを考慮すると現状においてファイアウォールを設置する効果は依然として大きい。

イ) 不正侵入検知システム・不正侵入防御システム

不正侵入検知システム（IDS : Intrusion Detection System）は組織内ネットワークへの不正アクセスと見込まれる通信を検知した場合に警告を行い、不正侵入防御システム（IPS : Intrusion Prevention System）はIDSの機能に加えて当該不正アクセスを遮断する機能を有する。通信内容が不正アクセスかどうかの判断は過去の典型的な侵入実績に基づくパターンをもとに行われるが、これに類似した通信内容に対して誤警告を発生させたり、IDS/IPSを欺く方法で侵入する攻撃者の検知漏れが生じたりするなど、機械的に判断することによる限界が存在する。導入にあたってはこうした特徴を理解した上で実施することが望ましい。

④ 秘密分散技術

データを内容がわからない形式に変換した上で複数の断片に分割し、そのうち予め定めた個数の断片から元のデータを復元可能とする技術である。

⑤ コピーガード

著作物として扱われるコンテンツの不正な複製を防ぐための技術の総称であり、具体的に次のようなものが用いられている。

- ダビング 10（日本国内向けデジタル TV 放送で利用）
- AACS（Advanced Access Control System、ブルーレイディスクで利用）
- HDCP（High-bandwidth Digital Content Protection、HDMI（High-definition Multimedia Interface）対応機器で利用）

⑥ 強制アクセス制御

利用者のデータに対するアクセス権限を、当該データを保管している情報システムのシステム管理者が強制的にコントロールする技術である。これに対して、こうした機能をもたないアクセス制御方式を、任意アクセス制御と呼ぶ。こうした強制アクセス制御機能が提供された情報システムにおいては、利用者は自ら作成したデータに対し、あらかじめ定められた範囲よりアクセス権限を緩めて、すなわち許可されていない相手に対してアクセスを許すといった状況でデータを利用することができない。これにより、利用者の利便性がやや低下する一方で、過失や悪意によってデータに対する不正な利用が行われることを防止できるため、高い安全性が求められる情報システムにおいて用いられている。

⑦ 操作ログ・通信ログの取得及び異常な操作の検知

サイバー攻撃の検知だけでなく、従業員による内部不正の防止や、従業員の利用している PC が外部の攻撃者に乗っ取られた場合などを検知する手段としても、操作ログや通信ログ等のログファイルの取得は有用な手段である。現在は、利用者端末における攻撃や乗っ取りによる不審な挙動を検知する EDR（Endpoint Detection and Response）や、EDR が生成するものを含む各種のログを集約した上で、異常な操作を抽出する SIEM（Security Incident and Event Management）技術が注目されている。ただし、攻撃者が利用するマルウェアは必ずしもログに痕跡を残さないため、異常を必ず検出できるわけではない⁴¹ことに留意すべきである。

また、データの法的保護を考える場合、データそのものだけでなく、通信ログや操作ログについても保護する必要がある。これは、サイバー攻撃や内部不正等でデータの流出が発生した場合、いつ、どのアカウントから操作されたかのログファイルが訴訟において有力な証拠として扱われるためである。一方で、不正行為を行う者は、自らの行為の証拠を隠滅させる目的でログファイルの改ざんを行うことがある。こうした場合に、⑥に示した強制アクセス制御機能を備えたオペレーティングシステムであれば、仮にデータファイルの管理者権限が乗っ取られてデータが流出したとしても、ログファイルに関する管理者権限を分けて管理することで、ログファイルの改ざんを防ぐことが可能である。また、管理者であってもログを編集・消去することができないような形で記録を残せるデジタルフォレンジック関連製品も利用されている。

⁴¹ 有識者ヒアリング調査による。

⑧ その他

データの漏えいを防ぐための技術として、上述のほかに次のような技術も用いられる。

ア) 防犯カメラの設置

組織における内部不正の防止の観点からは、データにアクセス可能な空間や機器を対象とする防犯カメラの設置が考えられる。一般に、内部不正によるデータの不正取得は他人の目が届きにくい深夜や休日に行われることが多いことから、こうした時間に防犯カメラを稼働させる旨を社内でアナウンスすることは、内部不正の抑止効果が期待できる。一方、従業員を防犯カメラで常時監視することは、過剰なプライバシー侵害の印象を与え、従業員の士気の低下にもつながるとの指摘⁴²がある。

イ) ファイル授受システムの URL の複雑化

ID とパスワードを組み合わせて用いる代用として、データを保管する URL (Uniform Resource Locator) を構成する文字列を複雑化することで、外部から推測できないようにする方法も、アクセス制御技術の一種として、高度なセキュリティを要求されない条件のもとでのファイルの授受などの用途で用いられている。

(2) データの消失や改ざんを防ぐ技術

データが故意または過失により消失したり、改ざんされたりするなどの被害を防止することを、データの完全性の保護という。このための対策には、(1) に示した機密性の保護に関する技術とは異なる技術も利用される。以下にこれらの技術を整理する。

① アクセス制御に関する技術

データの機密性の保護に関する技術の項で示したアクセス制御技術は、データの完全性の保護にも有用である。機密性を目的とした保護との相違点は、機密性の場合はアクセスする権限をもたない利用者によるあらゆるアクセスを制限することに主眼が置かれるのに対して、完全性を目的とする場合はデータに対する「書き込み」や「削除」の権限を除いた状態で管理することで、データの改ざんや削除など、データの完全性に対する脅威から保護しようとするものである。この技術の重要な用途の一つとして、ログファイルの保護が挙げられる。データに不正にアクセスしようとする犯罪者（マルウェアなど不正なプログラムを含む）は、自らの不正の痕跡を抹消するためにログファイルの改ざんや削除を試みる場合が多いことから、そのような改ざんや削除を不可能とするために、ログファイルを編集したり削除したりする権限は、ログファイルへの書き込みを行う必要のあるアプリケーション等にものみ与えられる。これにより、

⁴² 有識者ヒアリング調査による。

サーバ等において一般的な利用者の権限が仮に犯罪者に乗っ取られたとしても、ログファイルの改ざんや削除を防ぐことができる。しかしながら、犯罪者がシステムの脆弱性等を悪用してサーバ等で用いられている OS の管理者特権を得た場合はアクセス制御の設定を自由に変更できるようになるため、効果は期待できない。このような場合にも対策を有効なものとするには、次項で示すような物理的に改ざんや削除が不可能な電子媒体を利用することが適切である。

② 改ざんや削除が不可能な電子媒体の活用

CD-R や DVD-R のように、物理的に内容を書き換えることができない特性を備えた電子媒体を用いることでも、①で示した改ざんや削除に関する権限を提供しないことによるアクセス制御と同等の機能を提供することが可能である。①で示したように、OS の管理者特権が奪われるような状況においても改ざんや削除を防ぐことができる利点を有する反面、いったん利用した電子媒体の再利用は不可能であり、書き込み済みの媒体の管理を含めて、運用コストが高価にならざるを得ないという欠点も有する。

③ データの改ざん等の検知に関する技術

データの完全性に関する対策技術としては、①及び②で示したような、データの改ざんや削除を防ぐ技術とは別に、次に示すようなデータが改ざんされたことを検知する技術も存在する。なお、こうした技術では意図的な改ざんだけでなく、運用上の障害等によるデータの損傷などの検出にも適用可能であることから、以下ではこれらを総称してデータの改変と呼ぶこととする。

ア) 電子署名の付与

公開鍵暗号方式を用いて、あるデータ（プログラムや PDF 形式の文書等）に付与される電子署名⁴³がその署名者のものであり、データそのものが改変されていないことを客観的に検証可能とする技術である。あるデータに対する電子署名を作成する場合、データが改変されていないと異なる電子署名が生成されるが、データが改変されていると異なる電子署名が生成されるため、改変されていることが検知できる。PDF や電子メールソフトウェアなど、広く使われている製品が電子署名に対応しており、国際的に標準化⁴⁴されているため、利用者は特別な対応を行うことなく電子署名が有効であることを確認できる。

なお、電子署名を付与した文書は、紙媒体で作成された文書における作成者による手書き

⁴³ 暗号化技術を用いて生成される一連の電子データのことであり、電子メールの末尾に記載する署名とは異なる。

⁴⁴ 電子メールにおける S/MIME (PDF Advanced Electronic Signatures, RFC 5751 ほか)、PDF における PAdES (PDF Advanced Electronic Signatures, ESTI EN 319 142) などとして国際規格になっている。

の署名や捺印がなされた文書に相当するものであり、電子署名に対してそれらと同様の法的効力を担保することを目的として、2001年に電子署名法⁴⁵が施行されている。同法に基づき、電子署名に用いられる署名者の公開鍵の真正性を証明する電子認証に関する業務を行う機関のうち、その安全性や信頼性に関する一定の要件を満たした電子認証サービスを特定認証業務として認定する制度が運用されている。

イ) ハッシュ値の取得

ハッシュ値とは、あるデータに対してハッシュ関数を適用することによって得られる、元のデータの特徴を表現し、より少ないデータ量で構成されるデータのことである。ハッシュ関数はこうした条件を満たすための数学的なアルゴリズムで実現される一方向性の関数である。前述の電子署名も、ハッシュ関数の一種である暗号学的ハッシュ関数を用いて実現されており、電子署名はハッシュ値を暗号化アルゴリズムを用いて加工したものである。これまで述べた通り、電子署名は標準化された技術であり、多くの製品で対応しているなどの利点を持つ反面、電子署名が有効であることを検証するための計算負荷が大きい欠点を有する。単にデータが改変されているかどうかを検知する目的であれば、必ずしも暗号学的ハッシュ関数を用いる必要はなく、より計算負荷の少ないハッシュ関数を用いることも可能である。こうした計算負荷の少ないハッシュ関数は、IoT (Internet of Things) デバイスのように、コストや消費電力等の制約から、計算能力の低いコンピュータを用いて実装される機器において、データの改変を検知するために利用される。

ウ) 元データとの比較

データの改変が生じているかどうかを検証するための方法としては、元のデータを改変のおそれのない場所や媒体等に保存しておき、そのデータと比較することでも可能である。電子データであれば、機械的に比較することで改変を確実に検出することができる。しかしながら、データの容量が大きい場合などは直接比較するよりも、予め元のデータのハッシュ値を得ておき、比較対象のデータのハッシュ値を計算することで改変の有無を調べるほうが一般に効率的である。

(3) データを必要なときに利用できるようにする技術

データが必要なときに利用できないことがないようにすることを、データの可用性の保護という。一般に、データの可用性を確保することは、そのデータを格納している情報システムやクラウドサービスの可用性を確保することに相当する場合が多く、関連する技術としては情報システ

⁴⁵ 電子署名及び認証業務に関する法律（平成十二年法律第百二号）

ムの可用性を高めるための技術に相当する。

① 情報システムの可用性を高めるための技術

情報システムの可用性が損なわれる可能性として、次のような要因が想定される。

- 情報システムの物理的な障害：情報システムを構成するサーバ等の物理的な故障等によって発生する障害である。
- 情報システムの運用上のトラブル：記録装置の空き容量不足や OS・アプリケーションの不具合等により、通常の稼働が困難になるものである。
- 不正アクセスやサイバー攻撃：情報システムの稼働を妨害するための攻撃、サービス妨害攻撃などによるものである。
- 情報システムの性能を超える過大な負荷：サイバー攻撃で類似の状況を生じさせるものを除き、悪意に基づくものではないが、利用者からみると情報システムの障害等で停止したり応答速度が低下したりするのと同様の可用性の低下に相当する状況に見える。
- 情報システムの保守のための一時停止：これは障害ではないが、情報システムを構成する OS やアプリケーションの更新、部品の交換等を行うために定期的にサーバ等の機器を停止させる必要がある。

こうした影響を避け、情報システムの可用性を高めるための手段として、以下の方法が利用される。

ア) 情報システムの構成要素の二重化

同様の機能を有するサーバや記録装置などを 2 系統以上設置し、主たるサーバ等に障害が発生した場合や保守を行う場合等にバックアップ用の機器による稼働に切り替えるものである。同じ構成の 2 系統の情報システムで運用されるものをデュプレックスシステム⁴⁶と呼ぶ。さらに障害等に備えてバックアップ系統の情報システムを常に動作させておく方法をホットスタンバイ方式、通常はバックアップ系統を停止させておき、障害等の発生時のみ稼働させる方法をコールドスタンバイ方式と呼ぶ。ホットスタンバイ方式のほうが稼働停止の期間を最小限に抑制することが可能であるが、その分通常の運用コストは高い。

上述した可用性が損なわれる要因のうち、情報セキュリティに起因するものと過大な負荷以外は本対策により概ね改善することが可能である。

なお、現在の PC やサーバ等で用いられている CPU（中央処理装置）の中には、マルチコアなどと呼ばれる複数の処理装置を内蔵するものが存在するが、これは OS などによる処理速度の高速化を目的としたものであり、可用性の向上手段としては有効ではない。

⁴⁶ 類似の用語としてデュアルシステムがあるが、こちらは同一の処理を 2 系統の情報システムで並行して実施し、両者の結果が一致することの確認を通じて処理の正確性を高めることを目的とするものである。

イ) 情報セキュリティ対策の実施

(1) においてデータの機密性を保護するための対策として紹介した各種の技術は、不正アクセスやサイバー攻撃等、情報システムの可用性が情報セキュリティに関する障害により低下するのを防ぐための対策としても有効である。

ウ) 情報システムの処理能力の増強

情報システムの性能不足による可用性の低下への対策としては、サービスの需要に見合った処理能力となるように情報システムの増強を行うことになる。しかしながら、負荷が高まるのがごく一時的な場合などは、情報システムを通じて提供するのではなく、次に示す②における対策であるクラウドサービスの利用が合理的となる場合も多い。

② サービスの可用性を高めるための技術

データの可用性を高める方法としては、データを扱う情報システムの可用性だけでなく、情報システムを用いて提供されるサービス全体の可用性についても考慮する必要がある。具体的な技術だけでなく、サービスの選定なども含めて考慮すべき事項を以下に示す。

ア) 複数拠点による同一サービスの提供

自然災害による情報システムの障害に対処しようとする場合、前述したようなデュプレックスシステム化では同一拠点にあるシステムが同時に被災する可能性があり、実効性の面で不十分である。そこで、データを保存する拠点を物理的に離れた複数の拠点（例：東京と大阪）に設けて、それらで同一のサービスを提供するようにするものである。このとき、複数の拠点間でデータの内容に相違が生じることのないよう、主たる拠点から他の拠点に対してデータの複製を送信し、それぞれのデータを同期させる必要がある。このための技術はレプリケーション技術と呼ばれる。拠点内での複製と異なり、大規模なデータの複製を送信するには大量のネットワークを介した通信が発生することから、差分のみを送信することで複製を効率化するような技術がレプリケーション技術の一部として工夫されている。

イ) ネットワーク回線の多重化

情報システムの可用性が高くても、情報システムとインターネットとを接続するネットワーク回線に障害が発生すると、その情報システムを通じて提供されるサービスの可用性は損なわれてしまう。そこで、高い可用性を必要とするサービスにおいては情報システムだけでなくネットワーク回線についても多重化を行っている。このとき、同一の方法や事業者（インターネットサービスプロバイダ）を通じた多重化では同時に障害が発生しやすいことから、

異なる回線を用いて多重化することが考えられる。具体的には、多重化の手段として次のような方法が想定される。

- 専用線とインターネット経由の接続の併用
- 異なる事業者が提供するインターネット接続の併用
- 光ファイバ接続と無線によるモバイルネットワーク接続の併用

こうしたネットワークの多重化方法の選定に際しては、想定されるネットワーク障害のシナリオと、そうしたシナリオ発生時のデータ利用やサービス提供に関する継続の必要性に応じて、代替効果が期待できる方法を選定することが望ましい。

ウ) クラウドサービスを用いた高可用性の確保

一般に、ビジネス向けに提供される著名な SaaS などのクラウドサービスでは、異なる地域に設置された複数の情報システムを用いてサービスが提供されており、インターネットへの接続回線についても多重化された高速の回線が用いられているのが一般的である。よって、こうしたクラウドサービスの可用性は、自組織で情報システムのハードウェアを運用する、いわゆるオンプレミスの場合と比較して高くなる。ただし、クラウドサービスにおいても保守のためのサービス停止は存在し、その停止のタイミングがクラウドサービス利用企業にとって都合の悪い状況となる可能性もあり得る。また、IaaS などで仮想サーバを利用する場合は、クラウドサービス上で同様に多重化を考える必要があり、実装方法によってはオンプレミスにおける可用性と大きくは変わらないこともある。

こうした状況のもとで、クラウドサービスの利用を前提に可用性を高めようとする場合、クラウドサービス事業者が提示する SLA (Service Level Agreement、サービス水準に関する合意事項) において、可用性ないし稼働率として提示されている値が高いものを選ぶ必要がある。ただし、SLA は提示されている可用性ないし稼働率を保証するものでなく、SLA を満たせなかった場合にはクラウドサービスの利用料金を返金するなどの補償が行われるのみで、稼働そのものを補償するわけではないことも珍しくない。よって、例えば中断が一切許されないようなサービスを IaaS を用いて構築する場合、SLA で高い可用性が提示されている異なる 2 社以上のクラウドサービスを組み合わせるなどの対策が考えられる。

(4) データのトレーサビリティを確保する技術

自社で作成ないし所有しているデータが外部で利用されていることを検知ないしその証拠を確保するための技術として、以下が利用されている。

① トレーサビリティ確保に用いられる技術や手法

ア) 電子透かし

暗号技術を応用し、偽造が困難な識別用の符号をデータの本来の用途に影響がない形でデータに書き込んでおき、後日それが有効なものであることを客観的に検証できるようにする技術である。電子透かしが記録されていることが明示される場合と、隠される場合の2種類があり、用途に応じて使い分けられている。具体例として次のものがある。

- Cinavia（ブルーレイディスクで利用）
- ソーシャル DRM（電子書籍等で利用）

イ) 電子署名

公開鍵暗号方式を用いて、あるデータ（プログラムや PDF 形式の文書等）に付与される電子署名がその署名者のものであり、データそのものが改ざんされていないことを客観的に検証可能とする技術である。ア) と異なり、電子署名が付与されていることを隠すことはない。国際的に標準化されており、PDF や電子メールソフトウェアなど、広く使われている製品が対応しているため、利用者は特別な対応を行うことなく電子署名が有効であることを確認できる。

ウ) タイムスタンプ

イ) の電子署名と用いている技術は同一であるが、タイムスタンプの対象となるデータがある時刻に生成されたことを保証する技術である。著作物に対する模倣による侵害などへの対策として効果がある。

エ) アクセス制御機能やトレース機能をもった文書アプリケーションの利用

クラウドサービスの利用を前提とするアプリケーションの中には、当該アプリケーションで作成した文書を利用する際には、クラウドサービスへのアクセスを必須とすることで、アクセスする権利が与えられていない利用者が参照しようとしても、暗号化が解除されなかったり、参照した時間が記録されたりするような機能を備えるものがある（例：マイクロソフト社 Office 365）。こうした機能を利用することで、別途トレーサビリティ機能を備えた製品等を利用しなくても同様の機能を活用することができる⁴⁷。

オ) ファイル送受サービスにおける履歴情報の利用

エ) のような機能を提供するアプリケーションを利用しなくても、クラウドサービスとし

⁴⁷ 有識者ヒアリング調査による。

て提供されるファイル送受サービスにおいては一般に、データの送付先がいつダウンロードしたかを送付元の利用者において確認することが可能である。データの送受信に関するトレースを行うことが目的であれば、電子メールへのファイル添付の代わりにこうしたサービスを利用することで、トレースの効果を得ることができる。

カ) ウェブビーコン

データの中にある URL へのアクセスを生じさせるコンテンツを潜ませおき、そのデータを利用したことがその URL へのアクセスを通じて判別できるようにする技術である。送付した電子メールの開封や、外部に提供した文書ファイルをいつ開いたかを把握する用途で用いられている。

キ) デジタル・フォレンジックサービスの利用

攻撃者や内部不正者は悪意のもとでデータの不正利用を行おうとする場合、その不正の痕跡を削除しようとする。そこで、コンピュータなどのデジタル機器に対する不正利用について、それらの機器上に残された不正利用の証拠を確保し、将来起こり得る裁判に備えるための技術や手順がデジタル・フォレンジックである⁴⁸。なお、デジタル・フォレンジックの知見やスキルをもたない利用者や管理者が同様の分析を行おうとしても、かえって痕跡を消してしまう結果につながりかねないため、法的措置を前提に不正の証拠確保を行おうとする場合は、できるだけ早期にデジタル・フォレンジックの専門サービス事業者にご相談することが望ましい⁴⁹とされる。

ク) ダミーデータの挿入

あるコンテンツの中に、検証用のダミーデータを忍ばせておく方法である。具体例として、地図データにおいて実在しないランドマークを記載しておくことが知られている。特殊な製品の導入が不要ながら、悪意による除去が困難であり、データの改変を伴う用途でも対応可能な利点を有する。

ケ) 流出データの検知・対応サービス

流出してしまったデータがどこで公開されているかを、インターネット全体を対象に検索することで、流出の実態について把握する商用サービスである。

⁴⁸ 文献[4]の定義による。なおデジタル・フォレンジックの定義は関係機関によって様々に定義されており、裁判を前提としないものも含まれる。

⁴⁹ 有識者ヒアリング調査による。

コ) その他

トレーサビリティ技術とは異なるが、電子データに限らない著作物について、公証役場での確定日付の取得は、模倣による著作権侵害に対するエビデンスとして有効である。同様に、ソフトウェアプログラムを対象に、一般財団法人ソフトウェア情報センターによるプログラム著作物登録制度⁵⁰が提供されている

このほか、ブロックチェーン技術のトレーサビリティへの応用が現在研究されている⁵¹。

② トレーサビリティ確保の目的との対応

これまで示したトレーサビリティ確保のための技術や手法について、トレーサビリティ確保の目的として次の2種類について、それぞれの目的での利用の適切性について整理した結果を次表に示す。

- データの不正流通をトレース
- データの保有者を明示

表 3 トレーサビリティの目的に応じた技術や手法の整理

	データの不正流通をトレース			データの保有者を明示		
	利用者による編集加工の可能性のないデータ			利用者による編集加工の可能性のあるデータ	利用者による編集加工の可能性のないデータ	利用者による編集加工の可能性のあるデータ
	映像・音楽等の著作物	アプリケーションソフトウェア	契約・約款等に基づく提供されるデータ			
電子透かし	◎	△	◎	△	△	△
電子署名	△	◎	◎	—	◎	—
タイムスタンプ	—	—	—	—	△	—
アクセス制御機能やトレース機能を持った文書アプリケーションの利用	—	—	◎	◎	◎	◎
ファイル送受サービスにおける履歴情報の利用	△	—	○	○	—	—
ウェブビーコン	—	△	○	○	—	—
デジタル・フォレンジックサービスの利用	△	○	△	△	—	—
ダミーデータの挿入	—	—	○	○	△	△
流出データの検知・対応サービス	△	△	○	○	—	—
確定日付の取得、著作物登録	—	—	△	—	○	○
ブロックチェーン技術の応用	△	△	△	△	△	△

記号凡例：◎＝目的に適している、○＝利用可能、△＝場合によっては利用可能、—＝利用不可

⁵⁰ <http://www.softic.or.jp/touroku/>

⁵¹ 有識者ヒアリング調査による。

このとき、最適な技術・手法は「データの種類」の違い及び「データに対する編集・加工の可能性」の有無によって変わってくる。

ア) データの不正流通をトレースする目的に適する技術や手法

この場合、対象とするデータが不正流出したデータであることを客観的に証明可能である必要がある。この要件を実現する手段としては、暗号化技術を用いた電子透かしや電子署名、トレース機能を持った文書アプリケーションの利用などが適している。ただし、このうち電子署名はデータを編集してしまうと効力を失うため、編集や加工を前提としないデータへの適用に限定される。一方、編集や加工を前提とした場合は、アプリケーションを通じて管理するか、ダミーデータの挿入等、技術以外による手法などの利用が考えられる。

イ) データの保有者を明示する目的に適する技術や手法

この場合、データの利用者がデータの保有者について確認できるようにする必要がある。不正を行おうとする者による偽造が困難で、かつ利用者による確認が容易なのは電子署名を用いることであるが、ア) に示したように電子署名はデータを編集してしまうと効力を失うため、編集や加工を前提としないデータへの適用に限定される。編集や加工を前提とした場合は、トレース機能を持った文書アプリケーションの利用が適切である。

(5) データの保護技術及びトレサビリティ確保技術の比較

これまで整理した、データ保護及びトレサビリティ確保に用いられる技術等の特徴について、次ページに一覧表の形で示す。

表 4 (5) データの保護技術及びトレサビリティ確保技術の比較

			セキュリティ機能の分類 (●=有効)			トレサビリティ機能の分類 (●=有効)		保護対象となるデータ例 (○=当該技術の利用可能性あり)			
			機密性	完全性	可用性	不正流通の把握	アクセス保有者の明	映像・音楽等の著作物	アプリケーションソフトウェア	秘密情報書類	
データの保護技術	利用者認証	知識による認証	IDとパスワード	●							○
			アクティベーション	●			●		○		
			ワンタイムパスワード	●						○	○
		所有物による認証	電子証明書	●						○	○
			ICカード	●						○	○
			バイOMETRICS認証	●						○	○
		多要素認証	●					○	○	○	
	アクセス制御	任意アクセス制御		●					○	○	○
		強制アクセス制御		●					○	○	○
		利用範囲の制限	DRM	●					○	○	
	データの暗号化	データやその保存場所の暗号化			●				○	○	○
		通信路暗号化	VPN	●					○	○	○
			TLS	●					○	○	○
			WPA2	●					○	○	○
			スクランブル放送	●					○	○	
		電子メール暗号化	S/MIME	●						○	○
	添付ファイル暗号化		●						○	○	
		秘密分散技術	●					○	○	○	
	不正の検知・遮断	ファイアウォール		●					○	○	○
		不正侵入検知システム (IDS)		●					○	○	○
		不正侵入防御システム (IPS)		●					○	○	○
		コピーガード		●					○	○	
		ハッシュ値の取得		●					○	○	○
		元データとの比較		●						○	○
		ログファイルの取得及び分析		●					○	○	○
	その他	ファイル授受システムURLの複雑化		●					○	○	○
		改ざんや削除が不可能な電子媒体の活用			●				○	○	○
		情報システムの構成要素の二重化				●			○	○	○
		処理性能の向上				●			○	○	○
		複数拠点による同一サービスの提供				●			○	○	○
ネットワーク回線の多重化					●			○	○	○	
クラウドサービスを用いた高可用性の確保					●			○	○	○	
トレサビリティ確保に用いられる技術や手法	電子透かし			●		●	●	○	○	○	
	電子署名			●		●	●	○	○	○	
	タイムスタンプ			●		●	●	○	○	○	
	アクセス制御機能やトレース機能をもった文書アプリケーションの利用	●	●			●	●			○	
	ファイル送受サービスにおける履歴情報の利用					●		○	○	○	
	ウェブビーコン					●		○	○	○	
	デジタル・フォレンジックサービスの利用					●		○	○	○	
	ダミーデータの挿入					●				○	
	流出データの検知・対応サービス					●				○	

1.3.3 物理的対策

紙媒体に記録されたデータを安全に保管する方法として、物理的に外部から隔絶された場所での保管は極めて有効な手段である。電子的なデータにおいても、次のような方法によって物理的な対策を講じることで、データの保護に関する安全性を向上させることが可能である。

- データが保管されているサーバを、システム管理者以外が入室できない場所に物理的に隔離して運用する（管理者特権はサーバ室からのアクセス以外は許可しない設定との組合せにより、脆弱性を悪用した攻撃が困難となる）。
- 暗号化に用いた鍵が保存されている電子媒体を、物理的に隔離した場所で管理する（簡単に復号ができなくなるため利便性が低下する反面、データの漏えいリスクを大幅に低下されることが可能となる）。

1.3.4 データ保護のための対策と契約との組合せ

データ保護技術で対処することができない部分を保護することを目的として、データの利用者との間で交わす契約において、データの利用者に対する要求事項等を対象となるデータの特徴に応じて整理する。

(1) 外部者との秘密保持契約

業務提携や受発注、共同研究などを行う際に、外部者に対して自社の秘密情報を提示する必要がある場合には、相手にその秘密保持を求めるための秘密保持契約を締結することが一般的である。JIS Q 27002:2014 において、こうした秘密保持契約や守秘義務契約を締結する場合にその内容に反映することが望ましい事項として、次表の内容が示されている。

表 5 秘密保持契約又は守秘義務契約において考慮することが望ましい要求事項⁵²

a) 保護される情報の定義（例えば、秘密情報）
b) 秘密を無期限に保持する場合も含めた、契約の有効期間
c) 契約終了時に要求する処置
d) 認可されていない情報開示を避けるための、署名者の責任及び行為
e) 情報、企業秘密及び知的財産の所有権、並びにこれらの秘密情報の保護との関連
f) 秘密情報の許可された利用範囲、及び情報を利用する署名者の権利
g) 秘密情報に関する行為の監査及び監視の権利
h) 認可されていない開示又は秘密情報漏えいの、通知及び報告のプロセス
i) 契約終了時における情報の返却又は破棄に関する条件
j) 契約違反が発生した場合にとるべき処置

なお、実際に秘密保持契約において扱うべき内容は、データに関する他者との共有の形態や、新たなデータの創出の可能性によっても異なる。経済産業省が平成30年6月に公表した『AI・データの利用に関する契約ガイドライン—データ編—』⁵³では、こうしたデータに関わる条件の違いをもとに、契約における考え方を次の3種類に区分し、うち「データ提供型」と「データ創出型」の2区分について、モデル契約書案を提示している。

① 「データ提供型」契約

取引の対象となるデータを一方当事者（データ提供者）のみが保持しているという事実状態について契約当事者間で争いが無い場合において、データ提供者から他方当事者に対して当該

⁵² JIS Q 27002:2014（情報技術—セキュリティ技術—情報セキュリティ管理策の実践のための規範）13.2.4項（秘密保持契約又は守秘義務契約）の実施の手引きより引用。

⁵³ <http://www.meti.go.jp/press/2018/06/20180615001/20180615001-2.pdf>

データを提供する場合を対象とするものである。

② 「データ創出型」契約

複数当事者が関与することにより、従前存在しなかったデータが新たに創出されるという場面において、データの創出に関与した当事者間で、データの利用権限について合意する場合を対象とするものである。

③ 「データ共用型（プラットフォーム型）契約

異なる企業グループに属する複数の事業者がデータをプラットフォームに提供し、プラットフォームにおいて当該データを集約・保管、加工または分析し、複数の事業者がプラットフォームを通じて当該データを共用または活用する場合を対象とするものである。

なお、経済産業省が平成28年2月に公表した『秘密情報の保護ハンドブック ～企業価値向上に向けて～』⁵⁴では参考資料2の第4において、業務提携の検討において取り交わす秘密保持契約書の事例を示しており、契約内容を検討する上での参考とすることが可能である。

(2) 従業員等に対する秘密保持契約

従業員の雇用に際しては、情報セキュリティ対策に関する実践の促進と内部不正防止の観点から、情報セキュリティに関する各自の責任及び組織の責任について当該従業員に伝え、同意を得ることが望ましい。JIS Q 27002:2014においては、新たに雇用する従業員に対して伝えるべき事項として、次表の内容が示されている。

表 6 従業員の雇用契約において明確にし、言及することが望ましい契約上の義務⁵⁵

a) 秘密情報へのアクセスが与えられる全ての従業員及び契約相手による、情報処理施設へのアクセスが与えられる前の、秘密保持契約書又は守秘義務契約書への署名
b) 従業員又は契約相手の法的な責任及び権利 [例えば、著作権法、データ保護に関連して制定された法律に関するもの]
c) 従業員又は契約相手によって扱われる情報の分類に関する責任、並びに従業員又は契約相手によって扱われる組織の情報、情報に関連するその他の資産、情報処理施設及び情報サービスの管理に関する責任
d) 他社又は外部関係者から受け取った情報の扱いに関する従業員又は契約相手の責任
e) 従業員又は契約相手が組織のセキュリティ要求事項に従わない場合にとる処置

⁵⁴ <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf>

(参考資料) <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/reference1-6.pdf>

⁵⁵ JIS Q 27002:2014 (情報技術—セキュリティ技術—情報セキュリティ管理策の実践のための規範) 7.1.2 項 (雇用条件) の実施の手引きより引用。

(3) 消費者等に対するコンテンツの利用制限

コンテンツの利用ライセンスの購入者に対して、ライセンスの範囲外での利用を禁じるような契約の締結や約款への同意を求める場合に、それらに盛り込むべき内容について、コンテンツの保護に用いる技術に応じて整理する。

① コンテンツの利用にアクティベーションを必要とする場合

アクティベーションを通じて同時に複数の機器や利用者のもとで利用することが不可能となっている一方、アクティベーションの方法によっては他者のアカウントを使ったアクティベーションによるコンテンツの不正利用は可能であるため、こうした使い方を契約や約款にて禁止することが考えられる。

② 複製等が困難な電子媒体で提供する場合

複製が困難な一方で、電子媒体そのものを他者に提供することが可能であることから、電子媒体の貸借や譲渡についての制限を契約や約款に盛り込むことが考えられる。

③ 契約等に違反した流通についてのトレースが可能な形態で提供する場合

①や②と異なり、トレースが可能であることは契約や約款で定める内容に反するような利用を制限できることには相当しない。しかし、トレースにより不正が発覚した場合の罰則を明示するなど、不正を抑止する効果を期待することができる。

(4) その他の契約

(1)～(3)以外に、データに関して次に例示するような保護が必要な場合に考慮すべき事項について整理する。

① データの所有者や著作権者を明示させる必要がある場合

データの利用者に対し、データの活用方法については自由に委ねる一方で、データの所有者や著作権者を明示させ、これら以外の者によるデータの所有権や著作権に関する詐称を防ぎたい場合に相当する。

ア) データを改変不可能な形態で提供する場合

CD-ROMなどの改変不能な電子媒体で提供したり、データそのものに電子透かしを付加することで改変が検知できるような形態で提供したりする場合は、データの所有者や著作権者に関する内容を改変してもオリジナルのデータとの照合が容易であるため、契約や約款等において、提供時の媒体に明示された所有者や著作権者に関する内容の改変を禁じる記載を行うことで一定の実効性を期待することが可能である。

イ) データを改変可能な形態で提供する場合

データの利用者において、データの所有者や著作権者に関する内容の改変が容易である。このような場合、契約や約款でデータの所有者や著作権者の明示を求めても実効性は限定的とならざるを得ないが、実際には逆にオリジナルのデータを公表に近い形で提供することで、第三者によるオリジナルとの照合を容易にし、改変を検出しやすくする取組が行われている。その一例として、Creative Commons が定めるライセンス制度⁵⁶の場合、原作者が自らの著作物に次図のような表記を行うことで、原作者のクレジット（氏名、作品タイトルなど）を表示することを主な条件として、改変のほか、営利目的での二次利用も許可することを規定することができる。



図 1 「表示」に関するマーク（Creative Commons）

② データの完全性を保護する必要がある場合

データを秘密にする必要はないが、データを提供したときの状態のまま利用すること、すなわち改変されていない状態で利用する場合を求める場合に相当する。

ア) データを改変不可能な形態で提供する場合

①と同様、CD-ROM などの改変不能な電子媒体で提供したり、データそのものに電子透かしを付加することで改変が検知できるような形態で提供したりする場合は、改変されたデータとオリジナルとの照合が容易であるため、契約や約款等において、提供時の媒体に明示された所有者や著作権者に関する内容の改変を禁じる記載を行うことで一定の実効性を期待することが可能である。

イ) データを改変可能な形態で提供する場合

データの利用者が意図をもって改変することが可能で、それがデータの提供者にとって望ましくない状況を生じさせる場合には、データの提供に伴う契約ないし約款において、相手に対してデータの改変を禁じ、データの完全性の保持義務を課す必要がある。なお、著作物の要件を満たすデータに関して、データの自由な流通を許可するが、完全性の保持を求める場合に向けて、前述の Creative Commons の定めるライセンスにおいて、著作者の表示とともに、著作物の改変を禁じるものが定められている。これは、次図のようなマークを表示す

⁵⁶ <https://creativecommons.jp/licenses/>

ることで、原作者のクレジット（氏名、作品タイトルなど）を表示し、かつ元の作品を改変しないことを主な条件に、営利目的を含む利用（転載、コピー、共有）を許可することを規定するものである。



図 2 「表示-改変禁止」に関するマーク（Creative Commons）

1.4 データの保護に関してどのような対策をとるべきか

以上の説明を踏まえて、企業においてデータの特徴に応じてどのような対策を選べば良いかの考え方について説明する。

1.4.1 データ保護に関する方針策定の手順

1.3.1において示した各種ルールの遵守ないし整合性の確保を図りつつ、次の手順でデータをどのように保護するかの方針を定める。

(1) 自社にどのようなデータがあるのかの把握

ルールを策定するに先立ち、自社でどのようなデータがあるかを把握する。このとき、1.2に示したデータの分類に応じて適した保護方法は変わってくることから、実際にデータがどの範囲で使われ、誰と共有されているかといったデータの特徴を併せて把握する必要がある。さらに、データを強固に保護することによって、漏えいに対する安全性は高まるが、同時にその運用コストが高価になったり、データの利活用に関する利便性が低下したりするなどの弊害が伴うことも多い。そこで、企業内で扱われるデータを、強固に保護する必要のあるものと、利便性を重視すべきものに分類し、それぞれの特徴に応じた対策が規定される。こうした分類作業は「データの格付け」⁵⁷と呼ばれる。具体的な手順について以下に示す。

① データの洗い出し（棚卸し）

社内にどのようなデータが存在するかのリストアップを行う。この際、次項以降における格付けの決定やアクセス制御を行う際の判断材料として、データに関する次のような特徴を把握することが望ましい。

- 個人情報やマイナンバーなど、法律で保護が義務づけられているデータか？
- 法律での保護が義務づけられていなくても、プライバシー保護や機微性の観点から、社会的に保護することが期待されているデータに相当するか？⁵⁸
- 当該データの流出が、企業における事業の継続やレピュテーション（評判）にどの程度影響を及ぼすか？（重大な影響、一定の影響、軽微な影響、影響しない）
- 公開されているデータ、あるいは管理する必要の無いデータか？
- 当該データを参照したり、編集したりする必要のある人（または役割）は誰か？
- 社外に提供する必要はあるか？
- データの保護が不要（公開可能）となる時期はあるか？

⁵⁷企業において秘密として管理すべきデータの洗い出しと分類、それに伴った管理方法に関する考え方は、『秘密情報の保護ハンドブック～企業価値向上に向けて～』（経済産業省、2016年）の第3章を参照。

<http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>

⁵⁸ この判断を画一的に行うことは一般に困難である。たとえば顧客の位置情報の場合、精度が低いデータであればプライバシー情報とは感じられにくいのが、高精度のデータであれば行動履歴が把握される恐れのあるプライバシー情報と感じられる場合がある。（企業ヒアリングにおける指摘による）

- データが不要（削除可能）になる時期はあるか？

② データの格付け基準の作成

①でリストアップされたデータ毎に、その取扱い方法について、「厳重に保護すべきもの」から「公開情報など、保護する必要がないもの」まで3～4段階程度に分類し、データの利用者がどのランクにあるデータなのかを識別できるようにする。このとき、格付けを決定する際には、自社におけるデータ保護における要件（①で洗い出したもの）のほか、データの提供や利用に関する各種の条件についても考慮する必要がある。こうした格付けの分類例を次表に示す。

表 7 データの格付け例（4段階に分類）

	格付けの定義	該当するデータの例	
レベル 4	最重要データ	<ul style="list-style-type: none"> ・個人情報、センシティブ情報、競合他社への漏えいが重大な損失となる情報 ・データの提供元から厳重な秘密保持を求められているデータ 	法律等で保護が求められているデータについては、レベル3または4のいずれかに格付け
レベル 3	重要データ	<ul style="list-style-type: none"> ・事業を営む上での営業秘密（製品図面、契約書等） ・データの提供元から営業秘密として提供されているデータ ・システムや通信に関するログファイル 	
レベル 2	要管理データ	<ul style="list-style-type: none"> ・厳重な保護を必要としないが、公開を前提としないデータ（出勤簿等） ・社外から提供を受けた、レベル3とレベル4以外のデータ 	
レベル 1	公開データ	<ul style="list-style-type: none"> ・自社ウェブサイトで公開しているデータ（製品カタログ等） 	

コラム：データの棚卸しを行う余裕がない場合

慢性的に人手不足の企業等においては、上述のデータの棚卸しを行った上で格付けを行う余裕がない場合も想定される。そうした場合でも、データの格付けを行うことなしにデータを保護しようとする、保護する必要のないデータまで保護してしまい、使い勝手が悪くなったり、厳重に保護すべきデータの保護が中途半端になって、データの漏えい事故が生じやすくなったりするなどの影響が生じる恐れがある。すべてのデータを把握することが難しい場合、次のような3段階の格付けを行い、上位レベルと下位レベルのデータのみをリストアップして、それらについてのみ異なる対策を講じるという方法⁵⁹もある。

表 8 データの格付け例（全データの棚卸しを行わない場合：3段階に分類）

	格付けの定義	該当するデータの例
レベル3	重要データ	個人情報、営業秘密など
レベル2	その他のデータ	レベル1,3に該当するもの以外のすべてのデータ (棚卸しをせず、すべてのデータに対して必要最低限の保護を行う)
レベル1	公開データ	保護する必要のないデータ(公開情報)

③ データの特徴に応じた格付けの実施

②で定義した基準をもとに、自社で扱うデータの特徴に応じて格付けを行う。1. 2にて分類した内容に応じた格付けの考え方を次表に示す。このとき安全性を考えると、高めのレベルに格付けするのが無難と考えられがちであるが、取り扱い上の効率化や情報の自由度の確保を考えると、必要以上に高いレベルに格付けることは避けるべきである⁶⁰。

表 9 データの特徴に応じた格付けの考え方

	データの分類	格付けの考え方
1. 管理や利用の主体による分類	(1) 自社単一部門で閉じて利用するデータ	データが漏えいしたり、消失・改ざんされたりした場合に自社が被ると見込まれる損失に応じて格付けを行うことが考えられる。(表3におけるレベル2~4)
	(2) 自社で部門横断的に利用するデータ	一般にデータの利用に関する契約を締結することが行われており、この契約においてデータの関する秘密保持が求められている場合、当該データは自社の営業秘密以上のレベルで扱うことが適切である。(表3におけるレベル3以上)
	(3) 自社と他社間で利用するデータ	加工した後のデータが漏えいしたり、消失・改ざんされたりした場合に自社が被ると見込まれる損失に応じて格付けを行うことが考えられる。(表3におけるレベル2~4)
	(4) オープンプラットフォームから情報取得して利用するデータ	他社との契約においてデータの関する秘密保持が求められている場合、当該データは自社の営業秘密以上のレベルで扱うこと
	(5) 他社とオープンプラットフォームから情報取得して利用するデータ	

⁵⁹ 有識者ヒアリング調査による。

⁶⁰ 有識者ヒアリング調査による。

		が適切である。(表 3 におけるレベル 3 以上)
	(6) 自社情報をオープンプラットフォームで共有して利用するデータ	公開情報に相当するものとして扱うことが適切である。(表 3 におけるレベル 1)
2. 価値の源泉による分類	(1) 秘密にしておくことが価値を産むデータ	秘密として管理する必要性が明らかであり、営業秘密以上のレベルで扱うことが適切である。(表 3 におけるレベル 3 以上)
	(2) 更新されていることが価値を産むデータ	更新や共有はデータを高度に保護することで実施しにくくなる場合が多いため、(1)と(3)の中間として扱うことが適切である。(表 3 におけるレベル 2)
	(3) 誰かと共有していることが価値を産むデータ	
	(4) オープンデータ	公開情報に相当するものとして扱うことが適切である。(表 3 におけるレベル 1)
	(5) その他のデータ	(1)と(4)のいずれにも該当しないことから、その中間として扱うことが適切である。(表 3 におけるレベル 2)
3. 被害の影響による分離	(1) データが外部に漏えいすることで被害が生じるもの	秘密として管理する必要性が明らかであり、営業秘密以上のレベルで扱うことが適切である。(表 3 におけるレベル 3 以上)
	(2) データの改ざんや消失によって被害が生じるもの	改ざんや消失を防ぐための管理の対象とすることが適切である。(表 3 におけるレベル 2 以上)

コラム：データの格付けを見直す必要がある場合

データの中には、蓄積されていくことではじめて価値を持つものがある。例えば、あるショッピングサイトのユーザの匿名化された購買履歴の場合、1 件のデータとしては漏えいしても事業への影響はないため、低い格付けを設定して何ら問題は無いが、何万人もの利用者による何年間にもわたる購買履歴であれば、マーケティング上の価値も高く、万一競合他社に漏えいするようなことがあれば自社事業へのダメージとなる恐れもあることから、適切に格付けした上で保護を行う必要がある。このような購買履歴であれば蓄積開始時点で高い格付けにする判断も可能かもしれないが、今後 AI によるデータの活用が展開されていく中で、新たに価値が見いだされるようなことも考えられる。

一方、これとは逆に、市場の縮小。消滅や事業からの撤退などを通じて、これまで価値があると考えられていたデータの価値が失われることもあり得る。

そこで、データを対象とする格付けについては定期的にその妥当性について確認し、必要に応じて見直すプロセスを導入することが考えられる。

なお、法律や契約で保護が求められているデータについては、自社における事業上の価値に関わらず、適切な保護を行う必要がある。

(2) 対策方針の選定

(1) で洗い出したデータそれぞれについて、格付けに応じた対策に関する方針を選定する。このとき、レベルに応じた方針の考え方は次の通りである。

① 最重要データ (表 7 におけるレベル 4)

このレベルに相当するデータについては、漏えいを防止する効果に相当するセキュリティレ

ベルの高さを優先することが求められる。ただし、その代償としてコストが高くなることや使い勝手が悪くなることなどのデメリットが生ずる場合が多いため、その受け入れ可能性を検討した上で方法を選択する。前述の通り、複数の方法を組み合わせることでセキュリティレベルを高めることが可能であり、例えば②で選択する認証方法に加えてデータの暗号化を行うことなどが考えられる。

なお、外部から提供されたデータ等の場合は、その扱いが提供元から指示されることもある。

② 重要データ（表 7 におけるレベル 3）

このレベルに相当するデータは、セキュリティレベル、使い勝手、コストの3点のバランスを考えて選定することが望ましい。このバランスは用途によっても変わってくるため、同じレベルのデータであっても用途に応じて異なる対策を採用することもあり得る。

③ 要管理データ（表 7 におけるレベル 2）

このレベルに相当するデータについては、セキュリティレベルとして高度な対策で保護する必要はなく、データの保護に関する必要最低限の対策を行うことを中心に選定することが考えられる。

④ 公開データ（表 7 におけるレベル 1）

このレベルのデータに対しては、公開が前提であるため漏えいからの保護のための対策は行わない。

1.4.2 データ保護に関する対策の考え方

1. 3にて示したように、データを保護するための対策には多くの方法があり、データの特徴に応じて適した方法も変わってくる。また1. 1で示したように、現在は適切な情報セキュリティ対策を講じていても、完全にデータを保護することが困難な場合が増えつつある。こうした状況の中で、データの利活用を通じた企業における事業上のリスクを軽減するためには、個別の脅威に対処するための技術的対策のみならず、データの不正利用を企図する者に対する刑事罰、差止請求、損害賠償請求などの法的措置の適用についても併せて検討する必要がある。

組織的対策、技術的対策、物理的対策を組み合わせ、データ保護のための具体的な対策方法について以下に説明する。なお、データ保護に関連して考慮すべき法律については、本書の第2章において詳述する。

（1）必要な人以外がデータを使えないようにする

データの流出の可能性を減らすためには、データを扱うことができる者の数を必要最小限とす

ることで、流出等の事故が発生する可能性をできるだけ下げることが有効である。この考え方は「Need to Knowの原則」（知る必要のある人のみに情報を知らせる）と呼ばれ、重要なデータを保護するための基本的な考え方として知られている⁶¹。ここでは「必要な人以外がデータを使えないようにする」ための手段として広く用いられている方法として、利用者認証に基づくアクセス制御とデータの暗号化の方法について説明する。

① 利用者の認証に基づくアクセス制御（1. 3. 2（1）①参照）

データを管理するサーバなどの機器において、ID とパスワードによる認証によって利用者を識別した上で、それぞれの利用者がサーバ内のどの範囲にアクセスしてよいかを設定する。

ア) 認証方式の選定

認証方式選択の参考として、下表にそれぞれの方式の特徴の違いを示す。データの格付けレベルの高いデータの認証には、よりセキュリティレベルの高い方法（多要素認証を含む）を用いることが望ましい。

表 10 認証方式による特徴の違い

認証方式		セキュリティレベル	使い勝手	コスト		備考
				導入コスト	運用コスト	
知識による認証	IDとパスワード	低	並	低	低	ほとんどの環境で利用可能であり追加投資が不要。
	ワンタイムパスワード	中	やや難	中～低	低	導入コストはワンタイムパスワード生成方法に依存。
所有物による認証	電子証明書	高	並	中～低	中～低	用途によっては無償の証明書の利用も可能。
	ICカード	高	並	中～やや低	中～やや低	低価格 IC カードリーダーと市販のフェリカカードで運用すると比較的 low コストで実現可能。
バイOMETRICS 認証		高～中	並 (方式による)	高～中	高～中	指紋などは低価格製品もあるが偽造も容易とされる。
多要素認証		中～高 (方式による)	難	中	中	2 種類以上の認証方式を併用するため、認証操作は煩雑になる。

イ) アクセス制御方式の選定

高いセキュリティレベルを求める場合、1. 3. 2（1）⑥に示した強制アクセス制御の利用が可能なオペレーティングシステムを用いてデータを扱う情報システムを構築することが考えられる。強制アクセス制御を用いることで、過失や悪意によるアクセス制御機能の無効化などの被害を発生させにくくすることができる。

次表は企業において扱うデータの種類に応じて、「Need to Know の原則」をもとにアクセス制御に関する設定を行った例である。

⁶¹ Need to Know の原則に基づくアクセス管理が行われていることは、裁判において営業秘密として管理されていたことの要件として主張可能である。(有識者ヒアリングによる)

表 11 社内におけるデータの種類に応じたアクセス制御設定の例

データの例		データの利用・管理部署					当該データのシステム管理者
		役員 経営企画部門	人事部門	総務部門 経理部門	事業部門	情報システム部門	
従業員 情報	氏名・所属・ 連絡先等	△	●	△	△	△	★
	上記以外の 個人情報	— (本人分 のみ●)	●	— (本人分 のみ●)	— (本人分 のみ●)	— (本人分 のみ●)	★
	給与関連情報	— (本人分 のみ△)	●	●	— (本人分 のみ△)	— (本人分 のみ△)	★
自社の事業戦略データ		●	—	—	—	—	★
顧客から提供された 営業秘密データ		—	—	—	担当部署 のみ●	—	★
製品販売情報、 受発注伝票等		●	—	●	●	—	★
社外秘の技術情報、 製造ノウハウ等		—	—	—	担当部署 のみ●	—	★

●＝読み取り／編集可、△＝読み取りのみ可、★＝管理者権限により全ての操作が可、—＝不可

上記の例では情報システム部門に設置されたサーバにすべての情報を保存する前提としており、情報システム部門に所属するサーバのシステム管理者がシステム管理特権をもつこととしている。このような場合、当該システム管理者が不正を働くことですべての情報を閲覧することができるほか、外部からの不正アクセスによりシステム管理者の管理者権限が奪われた場合は、攻撃者からもすべての情報が参照できてしまう。こうした被害を防ぐためには、アクセス制御を実施した上で次項に示す暗号化を施した状態で保管し、暗号化に用いた鍵はそれぞれのデータの管理部門で保管し、情報システム部門からアクセスできないようにすることが考えられる。

② データの暗号化（1. 3. 2（1）②参照）

データを暗号化することで、その復号のための暗号鍵をもたない利用者が、データの内容を閲覧できないようにする。個人情報など、厳重に保護する必要のあるデータについては、①のアクセス制御を行った上でさらにデータの暗号化を行うことも行われる。一般に、データの暗号化を行うと当該データを利用する前に復号を行う手間が発生するため、利便性の低下を招くことから、暗号化すべきデータは適切に選定することが望ましい。

（2）悪意をもつ者の活動を検知し、データから遠ざける

現在、サイバー攻撃による情報漏えい事故は、インターネットに接続された企業すべてにとっての脅威となっている。また、組織における内部不正によるデータの持ち出しも、競合他社等へ

のデータの漏えいのリスクも含め、事業に重大な影響を与える恐れがある。こうした悪意をもつ者が重要なデータに接したり、データを流出させたりさせないための対策として、(1)に示すアクセス制御の導入が有用であるが、このほかに次のような方法が利用できる。

① ファイアウォールや不正侵入検知システム・不正侵入防御システムの導入

一般に、サイバー攻撃はインターネットに接続された電気通信回線を通じて行われる。したがって、その経路上において不正な通信を遮断したり、監視したりすることによって攻撃による被害を抑制することが可能となる。1. 3. 2 (1) ③に示したファイアウォールや不正侵入検知システム・不正侵入防御システムは、社内のネットワークを防御することにより、データを保護するための対策として広く利用されている。

② 操作ログや通信ログの取得

正当なアクセスかサイバー攻撃かに関わらず、データに関する通信の履歴や利用者による操作履歴を通信ログや操作ログとして記録する方法である。これらのログを分析することで、次のような情報を得ることができる。

- どのデータに対して、いつ不正なアクセスがあったか（流出したのはどのデータか）
- 攻撃はマルウェアによって行われているか、あるいはログインした攻撃者によって行われているのか
- 誰の ID が不正使用されたか（あるいは誰が内部不正を行っているか）
- 攻撃者はバックドア（継続的な不正侵入のためのアクセス手段）を設置しているか

なお、操作ログや通信ログはデータの取扱状況が争点となる裁判においても証拠として扱われることがあるため、こうした事態に備えた対策としても有効⁶²である。

操作ログや通信ログは時間経過とともに蓄積されていくため、これを適切に管理するために次のような運用のサイクルを行うのが一般的であり、これを自動的に行うための設定の実施と、記録されたログの管理のための体制の構築についても、併せて検討する必要がある。

- 蓄積されたログを定期的に保管場所（アーカイブ）に移動する。
- 保管場所に移動したログについて、不正な改ざんを防ぐために変更が不可能となるようにアクセス設定を変更する。
- 保管場所内の一定の保存期間を超過したログを削除する。

(3) データが不正に使われたことがわかるようにする

1. 3. 2に示したトレーサビリティ技術のうち、用途に応じて次の①②に示すような方法が利用できる。また、□はデータが流出したことを外部サービスを通じて検知するものである。

⁶² 有識者ヒアリング調査による。

① 自社のデータが許可された範囲外で不正に利用されたことをリアルタイムで検知する

次のような技術が活用できる。このうち、ウェブビーコンを利用する場合は、あらかじめ外部に提供する文書ファイルにウェブビーコンと呼ばれる特殊なデータを埋め込んでおく準備が必要である。

- トレース機能をもった文書アプリケーションの利用（この場合は、ファイルを開けないようにすることも可能）
- ウェブビーコン

② 訴訟等の場面において、自社から流出したデータであることの証拠として利用する

次のような技術が活用できる。いずれも事前にこれらのトレーサビリティ技術を適用させておく必要がある。

- 電子透かし
- 電子署名
- ダミーデータの挿入

このほか、訴訟においては操作ログや通信ログについても証拠として利用される。

③ 流出データの検知・対応サービスの利用

1. 3. 2 (2) ⑨に示した商用サービスを利用することで、流出したデータが公開されているかどうかを把握することができる。

(4) 法的保護による抑止

データの利活用を通じた企業における事業上のリスクを軽減するためには、個別の脅威に対応するための情報セキュリティ対策のみならず、データの不正利用を企図する者に対する刑事罰、差止請求、損害賠償請求などの法的措置の適用についても併せて検討する必要がある。このとき、データの不正利用に対する法的措置を実効的なものとするためには、適用される法律それぞれが定める要件を満たす形でデータを管理する必要がある。例えば不正競争防止法を適用し、企業の営業秘密を不正に利用しようとする者に対する処罰を可能としようとする、営業秘密に相当するデータについて、次の3要件を満たすような形で管理する必要がある。

- 秘密管理性（データが秘密として管理されていること）
- 非公知性（データが公表されていないこと）
- 有用性（データの内容が公序良俗に反するものでなく、事業活動に何らかの形で資するものであること）

データを保護するために適用可能な法律の種類と特徴については、本書の2. 1. 1にて紹介

する。

1.4.3 データの特徴に応じた対策の選定

データを保護するためにどのような方法を選択すべきかは、1.2で整理したデータの分類やデータの特徴によって異なってくる。こうした方法の選択における考え方を整理した表を次ページ以降の表9～表11に示す。自社で扱うデータの特徴を把握した上で、本表に示す内容を参考に選択することが望ましい。なお、これらの方法は1つのみを導入すればよいのではなく、複数の方法を組み合わせることでより有効な対策となる。

(1) 管理や利用の主体による分類（表9）

データが利用される範囲に応じて、重要となる対策が変わってくる。データの利用者が自部署内等に限定される場合は、アクセス制限を厳重に実施することが最も重要な対策となる。一方、自社のルールを適用できないような社外の関係者に提供する場合は、提供先による不正利用を防止するための法的措置や、データの移送中の漏えい対策などが重要となる。

(2) 価値の源泉による分類（表10）

「秘密にしておくことが価値を産むデータ」の場合、その価値を保護するために、合理的な範囲で複数の対策を併用することが適切となる。「誰かと共有していることが価値を産むデータ」については、多くの場合はその共有の対象外の者へのデータの流出は価値の低下を生じさせる恐れがあるため、「秘密にしておくことが価値を産むデータ」に準じた対策を講じることが想定される。

(3) 被害の影響による分類（表11）

「データが外部に漏えいすることで被害が生ずるもの」については、自社からの流出か、他社からの流出にかかわらず、流出の防止のための対策を併用することが望ましい。これに対して、「データの改ざんや消失によって被害が生ずるもの」については、過失や悪意によるデータの改ざんや削除に備えるための対策を実施することが適切である。

表 12 データの特徴に応じた対策の考え方（その1：管理や利用の主体による分類）

分類	データ保護の基本的な考え方	実施することが望ましい対策			
		(1) 必要な人以外がデータを使えないようにする	(2) 悪意をもつ者の活動を検知し、データから遠ざける	(3) データが不正に使われたことがわかるようにする	(4) 罰則を課すことで抑止する
(1) 自社単一部門で閉じて利用するデータ	当該部門内で閉じた形で管理し、部門外からのアクセスを制限する。	◎関係範囲内にアクセス制限することが最も重要	○不正アクセスのリスク抑制のために重要	△適切に管理すれば外部流出のリスクは小さい	△適切に管理すれば外部流出のリスクは小さい
(2) 自社内で部門横断的に利用するデータ	社内の関係部署で共有し、社外からのアクセスを制限する。	○利用範囲による対象者が増えるほど効果は低下	◎社内への不正アクセス阻止の対策が最も重要	△適切に管理すれば外部流出のリスクは小さい	△適切に管理すれば外部流出のリスクは小さい
(3) 自社と他社間で利用するデータ	データの扱いに関する契約等を交わすとともに、移送時の保護方法について定める。社内での扱いは(1)(2)のいずれかに準じる。	◎移送時の暗号化を行うなどの対策が必須	◎不正アクセスにさらされる機会が多いため重要	◇流出時の早期検知が必要な場合はトレーサビリティ技術の利用が適切	◎契約に反する利用や不正競争行為への法的措置が重要
(4) オープンプラットフォームから情報取得して利用するデータ	加工済みデータの取扱いについて、(1)(2)に準じる。	○加工したデータの内容によるが標準的な対策は必要	○不正アクセスのリスク抑制のために重要	◇用途に依存 ⁶³	◇用途に依存 ⁶⁴
(5) 他社とオープンプラットフォームから情報取得して利用するデータ	加工済みデータの取扱いについて、(1)(2)に準じる。	○加工したデータの内容によるが標準的な対策は必要	○不正アクセスのリスク抑制のために重要	◇用途に依存 ⁶⁵	○他社との関係上一定の法的保護が必要と見込まれる
(6) 自社情報をオープンプラットフォーム上で共有して利用するデータ	機密性の確保が不要であるため、データの完全性と可用性を確保できるような提供方法に留意する。	△積極的な保護は不要	△攻撃のリスクは小さい	◇用途に依存 ⁶⁶	◇用途に依存 ⁶⁷

記号凡例:◎=重要、○=やや重要、◇=条件に応じて検討、△=不要な場合もあり

⁶³ 不正利用することで経済的なメリットが大きな用途では、対策が有用な場合がある。

⁶⁴ 加工したデータを契約に基づいて提供を行う場合などでは、法的措置を適用可能とすることが適切なものもある。

⁶⁵ (4)と同様の用途のほか、他者との契約状況に依存する。

⁶⁶ オープンデータに近い形で提供する場合は、トレーサビリティ機能を付加することはオープンデータの考え方からすれば不適切である。

⁶⁷ 著作物の要件を満たすデータをオープンに提供する場合など。

表 13 データの特徴に応じた対策の考え方（その2：価値の源泉による分類）

分類	データ保護の基本的な考え方	実施することが望ましい対策			
		(1) 必要な人以外がデータを使えないようにする	(2) 悪意をもつ者の活動を検知し、データから遠ざける	(3) データが不正に使われたことがわかるようにする	(4) 罰則を課すことで抑止する
(1) 秘密にしておくことが価値を産むデータ	データの利用権限をもつ人以外による不正使用を防ぐために、「Need to Know の原則」のもとで複数の対策を併用する。	◎漏えい防止のために重要	◎不正アクセス防止によるリスク抑制のために重要	◎データ漏えいを早期に検知するために重要	◎データの不正使用への法的措置のために重要
(2) 更新されていることが価値を産むデータ	悪意によるデータの改ざんや消去、サービスの中断などを防ぐための対策を実施する。	◇用途によるが重要性は低い	○改ざん等の不正への対策は必要	◇用途に依存 ⁶⁸	◇用途に依存 ⁶⁹
(3) 誰かと共有していることが価値を産むデータ	共有対象者以外による不正使用を防ぐための対策を実施する。	○共有対象者以外による不正利用の制限は必要	○共有対象者以外による不正利用の制限は必要	◇用途に依存 ⁷⁰	◎共有対象者以外による不正使用への法的措置のために重要
(4) オープンデータ	一定の条件のもとでオープンな利用を認めている場合はその条件に違反した利用を検出するための対策を講じる。	△不要（オープンデータの趣旨に反する）	△不要（オープンデータの趣旨に反する）	◇ルール違反の利用の検出には有用な場合あり	◇ルール違反の利用への適用には有用な場合あり
(5) その他のデータ	講ずべき対策はデータに関するその他の特徴に依存する。	◇用途に依存 ⁷¹	◇用途に依存 ⁷²	◇用途に依存 ⁷³	◇用途に依存 ⁷⁴

記号凡例:◎=重要、○=やや重要、◇=条件に応じて検討、△=不要な場合もあり

⁶⁸ データの提供先が加工して再版することを禁じるような用途の場合、その違反を検出するために有用である。

⁶⁹ データの提供先が加工して再版することを禁じるような用途の場合、その違反に法的措置を講じることができるようにするために有用である。

⁷⁰ 組織的・技術的なデータの保護対策が有効に機能しないことが懸念されるような場合に有用となる可能性がある。

⁷¹ 秘匿する意図ではなく、利用者の誤解や混乱を避けるために条件を満たす利用者だけにデータを提供したい場合などには有用である。

⁷² データを改ざんすることで不正な利益が見込まれる場合などに、改ざん等を目的とする攻撃を検知するための対策は有用である。

⁷³ データの提供先が加工して第三者に提供することで利益が見込まれるような用途の場合、その検出手段として有用である。

⁷⁴ 契約への同意を前提にデータの提供を行う場合などでは、法的措置を適用可能とすることが適切なものもある。

表 14 データの特徴に応じた対策の考え方（その3：被害の影響による分類）

分類	データ保護の基本的な考え方	実施することが望ましい対策			
		(1) 必要な人以外がデータを使えないようにする	(2) 悪意をもつ者の活動を検知し、データから遠ざける	(3) データが不正に使われたことがわかるようにする	(4) 罰則を課すことで抑止する
(1) データが外部に漏えいすることで被害が生じるもの	データの外部への漏えいを防止するために、複数の方法を併用する。	◎漏えい防止のために重要	◎不正アクセス防止によるリスク抑制のために重要	◎データ漏えいを早期に検知するために重要	◎データの不正使用への法的措置のために重要
(2) データの改善や消失によって被害が生ずるもの	データの完全性を確保するための対策を実施する	○過失や悪意による改ざんや削除を防ぐために重要	○悪意による改ざんや削除を防ぐために重要	△不要（被害に対して対策が有効に作用しない）	◇電磁的記録不正作出罪の適用には重要
記号凡例: ◎=重要、○=やや重要、◇=条件に応じて検討、△=不要な場合もあり					

1.4.4 データの保護における利便性とのバランスの考え方

前述の通り、データを保護することで安全性は高まるが、反面データの保護のための対策を講じることで、利便性が低下する場合が多い。そこで、両者のバランスを考える上で考慮すべき事項を以下に示す。

具体的な対策を選定する際の参考として、1.3.2(1)に示したデータの外部への漏えいを防ぐための技術的対策のうち、主に企業等でデータ保護に用いられるものについて、次の3つの観点との対応関係を整理した結果を次ページ表に示す。なお、本表は利便性への影響を比較するためのものであり、暗号鍵やパスワードの盗難などによる影響等はトラブルに含めていない。

- データの使い勝手への影響
- トラブル発生の際の影響
- コストの増大への影響

表 15 データ保護のための対策ごとの影響

		データの使い勝手への影響	トラブル発生時の影響	コストの増大への影響	
利用者の 認証に 基づく アクセス 制御	知識 による 認証	IDと パスワード	利用開始時のログインの手間を除けば使い勝手 への影響は小さい	パスワードを失念した場合などに作業ができなく なる	多くのシステムで対応しており、追加コストはIDと パスワードの管理を行うための人件費等に限ら れる
		ワンタイム パスワード	IDとパスワードを利用する場合と同様、使い勝手 への影響は小さい	ワンタイムパスワードを発行する装置(トークン) やワンタイムパスワード発行のためのアプリケー ションが利用できない場合は作業ができなくなる	IDとパスワードと比較して、ワンタイムパスワード の発行環境の運用コストが増加する
	所有物 による 認証	電子 証明書	利便性は ID とパスワードによる認証と同様であ り、用途によってはログイン操作なしで利用開始 させることもできる	電子証明書のデータが失われたり、有効期限が 失効したりすると作業ができなくなる	電子証明書を外部から購入する場合はその調達 コストが必要(有効期限に応じて定期的に発生す る)
		ICカード	使い勝手への影響は ID とパスワードを用いる場 合と同程度	ICカードを紛失したり、ICカードの有効期限が失 効したりすると作業ができなくなる	ICカードの調達及び運用コストが必要となる
	バイオメトリクス 認証	方法に依存するが、一般に使い勝手への影響は 小さい	負傷などで認証ができなくなる場合がある	認証に用いるバイオメトリクス情報の登録や管理 に伴うコストが必要となる	
	多要素認証	上述の認証方式1種類のみを利用する場合と比較 して、利用開始時の作業量は増える	利用する認証方式のうち、必要な要素数分の認 証ができなければ作業ができなくなる	組み合わせる認証方式に依存する	
データの暗号化		データを利用する機会ごとに復号する場合は使 い勝手が低下するが、一定の場所に保存すると 自動的に暗号化する機能を備えた製品も存在す る	暗号化に用いた鍵が不明となると、データの復号 が不可能となり、データが失われたのと同じ状態 となる	無料のツール等を利用する場合、コストの増大は 暗号化/復号の操作に要する作業コストの増大 分に限定される	
秘密分散技術		製品やサービスに依存するが、データの利用開 始までには追加的な操作が必要となる	運用方法に依存し、一部のデータが失われても 復元できるような形で利用することも可能	秘密分散技術に対応するツールやサービスの利 用コストが必要となる	
強制アクセス制御		利用者がアクセス権を変更することができないた め、データ管理上の使い勝手は悪くなる	(特になし)	強制アクセス制御を利用可能な OS を用いる必 要があるが、無料 OS もありコスト増になるとは限 らない	
ネット ワーク における 保護技術	VPN	VPNを利用開始するときにVPNへのログインの 手間がかかるが、データの利用時の使い勝手 には影響しない	(特になし)	VPN製品の調達コストが必要だが、運用におい て追加コストは発生しない	
	TLS	暗号化のみに利用する場合は、使い勝手への影 響はない(認証にも利用する場合は電子証明書 の項目と同様)	(特になし)	サーバに設定する電子証明書(要定期更新)の 調達コストが必要であるが、無料の電子証明書も あるため、TLSの管理コストのみに抑えることも 可能	
	WPA2	(特になし)	(特になし)	現在販売されている無線 LAN 関連機器では標 準対応しており、追加コストは発生しない	

		データの使い勝手への影響	トラブル発生の際の影響	コストの増大への影響
	暗号化したファイルの電子メールへの添付	電子メールの送受信の際に、データを暗号化及び復号する作業が必要となるため、使い勝手は低下するが、S/MIME に対応したメールアプリケーションを用いる場合には使い勝手の低下は生じない	暗号化に用いた鍵が不明の場合は、データの受信者においてデータを取得していないのと同じ状態となる	無料のツール等を利用する場合、コストの増大は暗号化／復号の操作に要する作業コストの増大分に限定される(S/MIME を利用する場合は暗号化に用いる電子証明書の調達コストが必要)
その他	操作ログ・通信ログの取得及び異常な操作の検知	(特になし)	(特になし)	システム管理における監視コストの増大(外部委託する場合はその委託費用として発生)
	ファイル授受システムの URL の複雑化	(特になし)	URL が不明となると、データの授受が不可能となる	(特になし)

1.4.5 データ保護に関する方針を検討する上での参考情報

データ保護に関する方針は、1.4.1及び1.4.2に説明した内容をもとに決定すべきであるが、サイバー攻撃による被害の経験がなく、またデータ保護対策製品やサービスに関する知見も不十分の場合は、自社でどのような対策を選定すべきかの判断は容易ではない。このような場合に、どのような対策を選定すべきかについての考え方を以下に示す。

(1) 基準となるものの選択

これまでデータの保護について意識していなかった企業が、新たに単独で保護の方針を定めるのは必ずしも容易ではない。そこで、次のような方法で行うことで、自社で検討する負荷を軽減させることが現実的と考えられる。

① サプライチェーンで連携する他社と共通のデータ保護に関する基準を利用

得意先が典型であるが、業務遂行において共通のデータもしくはデータの提供元となる企業等において実施している対策に合わせる方法である。近年ではサプライチェーンを通じたセキュリティ確保の観点から、委託先に自社と同レベルのセキュリティ対策を求める企業が増えており、導入上の支障がない限りにおいて合理的な方法である。

② 国内外の情報セキュリティ対策に関する基準・ガイドライン等を利用

国際標準や国内のセキュリティ対策推進機関、及び業界団体などで策定している基準やガイドラインで示されている内容に基づいて対策を定める方法である。複数の委託元から受託している関係で特定の1社の委託元が定める内容に従うことが難しい場合や、対外的に適切なデータ保護対策を行っていることをアピールしたい場合などに適している。後者の場合は、基準に準拠していることを認証する制度を活用することで、よりアピールの効果を高めることが可能である。

- 情報セキュリティマネジメントシステム (ISMS) 適合性評価制度 (一般財団法人日本情報経済社会推進協会) ⁷⁵
- Payment Card Industry Data Security Standard (PCI DSS) (Payment Card Industry Security Standards Council) ⁷⁶
- 中小企業の情報セキュリティマネジメントガイドライン (独立行政法人情報処理推進機構 (IPA)) ⁷⁷

なお、個人情報保護に関する国内規格 JIS Q 15001 に基づくプライバシーマークの取得も、対象となるデータが個人情報に限定されるものの、この方法の一例である。

⁷⁵ <https://isms.jp/isms.html>

⁷⁶ 日本カード情報セキュリティ協議会による参考資料
http://www.jcdsc.org/pci_dss.php

⁷⁷ <https://www.ipa.go.jp/security/keihatsu/sme/guideline/>

(2) 情報セキュリティサービスベンダによるコンサルティングサービスを利用

特殊なデータを扱っている場合などで、(1)の方法を用いることも難しい場合は、情報セキュリティベンダが提供するデータ保護対策に関するコンサルティングサービスを利用することが考えられる。この場合、ベンダに自社で扱っている情報の棚卸しを依頼し、これに基づいて情報の格付けを行うことも可能である。

1.5 データ保護に用いる技術等の将来的な変化への対応

これまでに示したデータ保護やトレーサビリティに用いられる技術等に関して、将来的な変化がどのような影響を及ぼすかを以下に示す。

(1) 将来的な計算能力の向上がもたらす影響

コンピュータの誕生から今日に至るまで、その処理性能は向上を続けており、現在の携帯電話に内蔵されている CPU の処理性能は、20 年前のスーパーコンピュータの処理性能をはるかに凌ぐものとなっている。こうしたコンピュータによる計算能力の向上は、データ保護に用いられる暗号化の強度に影響を及ぼす。現在、データの保護に用いられる暗号化技術は、その鍵を知らない者には暗号化されたデータを復号できないことを前提としているが、これは正確に言えば、「実用的な時間内に復号できない」ことを意味している。鍵に相当する可能性のある文字列のすべてのパターンを総当たりで試すことで、鍵を知らない者でも最終的には復号することができてしまう⁷⁸。以上の前提のもとで、データを扱う情報システムを構築した時点で実用的な時間内では復号できないと考えられていた暗号化が、その後の計算能力の向上や解読技術の発達を通じて復号可能となってしまう事態がこれまでに発生している。これを暗号の危殆化（きたいか）と呼ぶ⁷⁹。たとえば、1977 年に米国で標準暗号に選定された暗号アルゴリズム（鍵の長さは 56 ビット）である DES（Data Encryption Standard）は、1999 年に 22 時間で解読されるなど、暗号化が有効性を維持できる期間は決して長いとは言えない。

以上で示した暗号の危殆化により、データの保護に関する効果が損なわれることへの対策として、次の方法が想定される。

① 長くて複雑な鍵の利用

数字 4 桁を鍵として用いる場合、総当たり攻撃を行うための試行数は $10^4=10,000$ 回であるが、アルファベット大小文字と数字を組み合わせた 4 文字とした場合、 $(26 \times 2 + 10)^4=14,776,336$ 回となり、数字のみの場合より 1,477 倍の試行が必要となるため、安全性が高まることになる。さらに、鍵の長さを 5 文字とすると 4 文字の場合のさらに 62 倍、6 文字とすると 4 文字の場合の 3,844 倍となる。このように、長く複雑な鍵を用いることで、鍵の推定を難しくすることで、安全性を確保することができる。しかしながら、鍵の長さを長くすることは、利用者が鍵を覚えにくくなったり、処理に時間を要することになるなどのデメリットもあるため、安全性と利便性のトレードオフで鍵の長さや複雑性を定めることとなる。このとき、金融機関の ATM（現金自動預け払い機）のように一定回数間違った暗証番号を入力した場合は

⁷⁸ このような試行により鍵を推定する方法を、総当たり攻撃（ブルートフォースアタック）と呼ぶ。

⁷⁹ 暗号の危殆化に関する詳細については、次の文献が詳しい（DES の事例も同文献に記載がある）。

「暗号の危殆化に関する調査 報告書」（独立行政法人情報処理推進機構、2005 年 3 月）

<https://www.ipa.go.jp/files/000013736.pdf>

以後の試行を認めないのと同様な鍵の運用を行える場合は仮に数字4桁でも十分に実用的であるが、電子データを格納したファイルを暗号化して暗号鍵を知らない者に内容を見せないようにする場合のように、復号を試みる者が手元で何回でも試行できる環境では十分に長くて複雑な鍵を用いなければ安全性を担保できないなど、暗号を用いる環境によって適切な鍵の選び方は変わってくる点に留意が必要である。

② データの保護に用いる暗号アルゴリズムの変更を可能とする仕組みの整備

暗号化や電子署名など、データの保護やトレーサビリティの確保に用いられる技術は、データを流通させる上での互換性を担保する観点から、暗号アルゴリズムと鍵長の組合せで扱われることが多い。たとえばRSA1024というのは、鍵長1024ビットのRSA公開鍵暗号アルゴリズムを用いることを示す。IT機器やアプリケーションソフトウェアにおいて、こうした暗号アルゴリズムと鍵長を特定の方式に依存させた形で実装すると、その暗号アルゴリズムや鍵長が危殆化した場合にデータの保護やトレーサビリティの効果が失われてしまうことから、別の方式への変更が可能な形で実装することが望ましい。例えば世界中で幅広く利用されているウェブブラウザアプリケーションの場合、暗号化に関する処理を行うモジュールはアプリケーション本体とは独立して実装され、複数の暗号アルゴリズムや鍵長の方式を選んで利用することが可能となっている。これに対して、自組織向けに組織内で開発するアプリケーションの場合、開発のコストを抑えて簡便に開発しようとする、特定の方式に依存した形で実装されることも生じがちであり、長期的な利用を行っていく中でセキュリティ上の問題となる恐れがある。

なお、安全性の高い暗号アルゴリズムを選定するための参考情報として、総務省と経済産業省及びその関係機関が共同で運営するプロジェクトであるCRYPTREC⁸⁰が、データを扱う情報システム等で用いるべき推奨暗号のリスト（CRYPTREC暗号リスト。電子政府推奨暗号リストとも呼ぶ）を公表⁸¹するとともに、暗号の危殆化に関する注意喚起⁸²を行っている。

（2）データを扱う技術に関する将来の変化がもたらす影響

音楽や映像による著作物に相当するデータを例にとると、かつてアナログのレコードやビデオテープなどのメディアを通じて提供されていたものが、CDやDVD、インターネット経由のダウンロードを経て、現在はストリーミング配信やオンデマンド配信を通じて提供されるなど、インターネットを取り巻く技術の変化がデータの流通形態に影響を与えている。同様に、こうしたデータの保護方法についても、アナログのメディアにおいては利用者による許諾範囲を超えた不正な利用（複製等）を防ぐ手段はなかったが、一方で複製を通じて音楽や映像の質が劣化するため、

⁸⁰ Cryptography Research and Evaluation Committees

⁸¹ <https://www.cryptrec.go.jp/list.html>

⁸² <https://www.cryptrec.go.jp/er.html>

それが不正な利用の抑制効果を生んでいた。これに対し、データがデジタル化されたことで複製による劣化の恐れがなくなり、CD において不正な利用が実際に著作権者にとっての脅威となったことから、以降のメディアではコピープロテクトなど、複製を防ぐための技術が適用されるようになっていく。さらに現在では、インターネットなどのネットワークを介してデータを利用することが一般的になったことから、アクティベーションのように接続先の利用者がデータを利用する許諾を得ているかどうかを確認した上でデータを利用可能とする技術が普及している。このように、データを扱う技術の変化がその保護方法にも大きく影響を及ぼすことから、今後の技術動向の変化に応じて、本書で示したようなデータの保護技術の利用形態も変化していくことが見込まれる。

（3）不正な行為や攻撃の主体や方法の変化

インターネットが普及する以前、機密性の保護が必要なデータに対する不正な行為のうち、主たる脅威と考えられていたのは、内部不正、移送時の盗難などである。現在、これらは依然として脅威ではあるが、加えてインターネットを介したサイバー攻撃やマルウェアによる情報の漏えいが重要な脅威として考えられるようになっていく。

また、不正な行為や攻撃の主体についても、内部不正であれば関係者であり、物理的な盗難であればデータの近くに位置する者による犯行であるなど、ある程度対象が限定されていたが、現在はデータと直接の関係をもたない海外の組織などが、営利目的でデータを不正に取得して転売するといった犯罪がインターネットを介して行われるようになっていく。今後、データを取り巻く環境の変化に応じて、こうした不正な行為や攻撃の主体や方法が変化することについても、ある程度想定した上で対策を検討することが望ましい。

本書で扱っていないが今後懸念すべき脅威の例としては、偽のデータを混入させることによる業務等の妨害が想定される。具体的には、センサネットワークにおいて本物のセンサになりすまして不正なデータを送信したり、AI に偽のデータを学習させることで正しい判断を行えないようにしたりするなどの行為は、今後こうした技術が社会で占める役割が高まる中でデータの活用における脅威として対策の必要に迫られることが想定される。具体的な対策としては、機器の認証を通じたなりすましの防止等、技術に応じた方法を検討することになる。

2. データ流出時の法的な救済について

本章では、企業で扱うデータの保護に関連して、データが不正に流出した場合に、その不正に対する救済措置の適用手段として活用可能な法律について説明する。

なお、以降の記述に関しては、平成31年1月31日時点で成立した内容（未施行のものを含む）に準拠するものとする。

2.1 データ保護に関する法律について

2.1.1 データの保護に関する法律の種類と役割

データ保護に関連する法律の概要について示す。なお、以下では法律の名称について、わかりやすさの観点から一般に用いられている通称にて表記し、本章における初出時の脚注にて正式な名称を記載することとする。

(1) データ保護に関する法律

データ保護に関する法律は、その役割に応じて次のように分類される。

① 特定のデータに関する扱いを定めるもの

個人情報、マイナンバーなど、社会において高度な保護を実施すべきと考えられているデータについて、講じるべき安全管理措置を定めている法律である。個人情報保護法⁸³、番号法⁸⁴、次世代医療基盤法⁸⁵などがこれに相当する。

② 特定の対象者によるデータの扱いについて定めるもの

医師、薬剤師、医薬品販売業者、助産師、弁護士、弁護人、公証人、宗教、祈祷若しくは祭祀の職にある者又はこれらの職にあった者については、刑法⁸⁶（第134条）により、業務上取り扱ったことについて知り得た人の秘密を正当な理由無く漏えいすることが禁じられている。看護師や放射線技師、理学療法士などはそれぞれの師法／士法に同様の記載がある。国家公務員法、地方公務員法にも守秘義務が規定されている。また、特定の業種を対象とする法律の中には、それぞれの事業を行う際のデータの取り扱いについて定めているものが存在する（例：電気通信事業法⁸⁷、プロバイダ責任制限法⁸⁸、割賦販売法⁸⁹）。

⁸³ 個人情報の保護に関する法律（平成十五年法律第五十七号）

⁸⁴ 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号）

⁸⁵ 医療分野の研究開発に資するための匿名加工医療情報に関する法律（平成二十九年法律第二十八号）

⁸⁶ 明治四十年法律第四十五号

⁸⁷ 昭和五十九年法律第八十六号

⁸⁸ 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（平成十三年法律第百三十七号）

⁸⁹ 昭和三十六年法律第百五十九号

③ 著作物としてのデータを保護することを目的としたもの

法的に著作物として認められるデータについては、著作権法による保護規定が適用される。

④ データに関する不正行為に対する措置を定めるもの

平成 30 年改正不正競争防止法では、データのうち「営業秘密」⁹⁰及び「限定提供データ」⁹¹に相当するものについて、その不正取得及び不正使用等に対する法的措置を定めるとともに、データの不正使用や不正な複製を防止するための技術的制限手段を妨げる行為（解除装置やプログラム、アクティベーションのためのシリアルコードの譲渡や提供、並びにこれらを行うサービスの提供を含む）に対する刑事的措置を規定している。

また、電波法⁹²では暗号化された通信内容の漏えい及び不正目的での復元に対する刑事的措置を定めている。

⑤ その他

データを保存する情報システムに対する不正アクセスやマルウェアを感染させるなどの行為については、不正アクセス禁止法⁹³及び刑法において刑事的措置を規定している。また、電磁的記録としてのデータを不正に作出・供用したり、損壊したりする行為に関してはそれぞれ刑法に電磁的記録に関する罪として規定されている。

（２）一般的なデータを対象とする法律

前項に示した内容を法律毎に整理する。このうち一般的なデータを対象とする法律については次の通りである。

① 民法⁹⁴

第 709 条（不法行為）において、不法行為に対する損害賠償責任を定めている。本条はデータ保護に限らない幅広い不法行為を対象とするものであるが、データに関する不法行為の例としては、データ管理者の過失による漏えい事故などが相当し、被害者に対する損害賠償等は本条に基づいて実施される。

また第 415 条（債務不履行による損害賠償）において、データの取扱に関する契約違反に対する損害賠償責任を定めている。

⁹⁰ 不正競争防止法における「営業秘密」の定義：秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの。

⁹¹ 不正競争防止法における「限定提供データ」の定義：業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その他の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、及び管理されている技術上又は営業上の情報（秘密として管理されているものを除く。）

⁹² 昭和二十五年法律第百三十一号

⁹³ 不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）

⁹⁴ 明治二十九年法律第八十九号

② 著作権法

著作権法(第10条及び第12条)における例示によれば、著作物として扱われるデータには、次のようなものが該当する。

- 小説、脚本、論文、講演その他の言語の著作物
- 音楽の著作物
- 舞踊又は無言劇の著作物
- 絵画、版画、彫刻その他の美術の著作物
- 建築の著作物
- 地図又は学術的な性質を有する図面、図表、模型その他の図形の著作物
- 映画の著作物
- 写真の著作物
- プログラムの著作物
- 編集物のうち、素材の選択又は配列によって創作性を有するもの
- データベースのうち、その情報の選択又は体系的な構成によって創作性を有するもの

これらのデータに対する権利侵害について、差止請求、損害賠償請求、刑事罰が規定されている。特に「データベースの著作物」については、その性質から「編集著作物」とは別に規定している。

このほか、第113条第3項において著作権の権利関係情報に対する改変等の不正行為、第120条の2において、著作権保護を目的とするプロテクト等の技術的保護手段(いわゆるコピーコントロール)の回避若しくは技術的利用制限手段の回避を行うことを禁じている。

③ 不正競争防止法

平成30年改正不正競争防止法においては、データの保護に関して次の3種類を規定している。なお、不正競争防止法はデータについての不正競争行為に対する差し止め、損害賠償及び刑事罰を定めるものであり、②の著作権法と異なりデータ所有者の権利に対する侵害への保護を講じるものではない。

ア) 「営業秘密」の保護

次の3要件を満たすデータを「営業秘密」として、第2条第1項第4号から第10号までにおいて、その不正利用等の不正競争行為についての差止請求、損害賠償、刑事罰が規定されている⁹⁵。

⁹⁵ 営業秘密の詳細については、「営業秘密管理指針」(経済産業省、平成31年1月改訂)を参照。
<http://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf>

- 秘密管理性（秘密として管理されている）
- 有用性（生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報）
- 非公知性（公然と知られていないもの）

イ) 「限定提供データ」の保護

次の3要件を満たすデータを「限定提供データ」として、第2条第1項第11号から第16号までにおいて、その不正利用等の不正競争行為についての差止請求、損害賠償が規定されている⁹⁶。保護に関する規定における営業秘密との相違として、刑事罰が定められていない点と、不正に取得されたデータであることを知らずに転得した者によるデータの使用を禁止していない点が挙げられる⁹⁷。

- 限定提供性（契約等で対象者を限定して提供している）
- 電磁的管理性（ID とパスワードなどにより電子データとして管理されている）
- 相当蓄積性（相当の蓄積がある技術上又は営業上の情報）

ウ) 技術的制限手段の効果を妨げる行為の禁止

第2条第1項第17号から第18号までにおいて、映像、画像、音声、プログラム、データ（電磁的に記録された情報）を保護することを目的として、その視聴、実行、記録を制限するために提供されている技術的制限手段（ソフトウェアプロテクト、アクティベーション等）について、その効果を妨げる装置やプログラム、指令符号（シリアルコード等）の譲渡、提供ならびにその効果を妨げるサービスの提供⁹⁸を禁じている。

コラム：AIの学習モデルの法的保護

ディープラーニングに代表される現在の機械学習システム（以下、本項では「AI」と表記する。）で用いられる「学習済みモデル」はAIが作成するデータの一種であり、この活用がAIによる価値ある成果の創出に欠かせないが、その保護に関しては次のような課題があることが指摘⁹⁹されている。

① 学習済みモデル作成に用いた元データとの関係性の判断が難しい

⁹⁶ 限定提供データの詳細については、「限定提供データに関する指針」（経済産業省、平成31年1月公表）を参照。
<http://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pdf>

⁹⁷ 営業秘密についても不正競争防止法による保護対象となった当初は刑事罰の適用対象外であった。ゆえに不正競争防止法の将来的な改正において、限定提供データにおけるこれらの扱いの見直しが行われる可能性はある。

⁹⁸ 平成30年改正不正競争防止法より、不正競争行為の範囲が技術的制限手段を妨げるための機器等の提供だけでなく、技術的制限手段を妨げる行為に関する代行サービスの提供等を含むように拡大された（技術的制限手段に関する改正内容については、平成30年11月29日に施行）。

⁹⁹ 有識者ヒアリング調査による。

ディープラーニングに基づくAIでは、AIが示す結果がどのような過程を経て導き出されたかを明らかにすることが困難である。この結果、A社が利用する学習モデルが、B社の学習モデルを不正に取得した上で、わずかに追加学習をさせただけのものであっても、A社の学習モデルの不正利用であることを立証することが困難である。

② AIシステムを公開して利活用する場合の学習モデルの保護方法

AIシステムを一般による利用のために公開すると、そのシステムで用いる学習済みデータが営業秘密として保護するための非公知性の要件を満たさなくなると言われている。そこで、こうした学習済みデータは、平成30年改正不正競争防止法において新たに定義された「限定提供データ」として保護する必要がある。

④ 不正アクセス禁止法

不正アクセス禁止法では、第2条にて以下の2種類を「不正アクセス行為」と定義し、第3条にて当該行為の禁止を規定している¹⁰⁰。

ア) 他人のIDとパスワードを用いたアクセス

アクセス制御機能を有する電子計算機に対し、他人のIDとパスワード（識別符号）を入力することで、アクセス制限されている機能を利用することをいう（第1号）。

イ) 脆弱性の悪用

電子計算機の脆弱性（セキュリティホール）を悪用して、アクセス制限されている機能を利用するものである。本項に該当する不正アクセスは、データにアクセスする権利を有する利用者であることを認証するための機能が、データを格納する電子計算機（サーバ）に併設されているかどうかで次の2種類に区分される。

a) 認証機能を備えた電子計算機への不正アクセス

アクセス制御機能を有する電子計算機に対し、その機能による制限を免れることができるような情報または指令を入力することで、アクセス制限されている機能を利用することをいう（第2号）。

b) 他の電子計算機の認証機能を用いてアクセス制限を行っている電子計算機への不正アクセス

他の電子計算機（認証用サーバ等）によって利用制限がなされている電子計算機に対し、その制限を免れることができるような情報または指令を入力することで、アクセス制限さ

¹⁰⁰ 詳細は警察庁の公表している「不正アクセス行為の禁止等に関する法律の解説」にて説明されている。
https://www.npa.go.jp/cyber/legislation/pdf/1_kaisetsu.pdf

れている機能を利用することをいう（第3号）。

このほか、第4条において他人のパスワード等の不正な取得、第5条において他人のパスワードの不正な提供、第6条において不正アクセス目的での他人のパスワードの保管についてもそれぞれ禁止している。第7条においては、いわゆる「フィッシング行為」を禁止している。

⑤ 刑法

データの保護に関する内容は、大きく以下の3種類に分類される。

ア) 秘密漏示に関するもの

第134条において、医師、薬剤師、医薬品販売業者、助産師、弁護士、弁護人、公証人、宗教、祈祷若しくは祭祀の職にある者又はこれらの職にあった者に対し、業務上取り扱ったことについて知り得た人の秘密を正当な理由無く漏えいすることを禁じている。また、看護師や放射線技師、理学療法士などはそれぞれの師法／士法に同様の記載がある。国家公務員法、地方公務員法にも守秘義務が規定されている。

イ) 電子計算機を対象として実施される犯罪に関するもの

第161条の2（電磁記録不正作出及び供用）において、業務を誤らせる目的で実施される、電子データに対する不正行為を禁じている。

また第168条の2（不正指令電磁的記録作成等）において、正当な理由なく、他人の電子計算機における実行を目的としてマルウェアの作成、提供、供用を行うこと、第168条の3（不正指令電磁的記録取得等）において、取得、保管を行うことを禁じている。

さらに第234条の2（電子計算機損壊等業務妨害）において、電子計算機もしくはその用に供するデータを損壊したり、または虚偽の情報や不正な指令を与えたりすることで、電子計算機の本来の目的に即した動作をさせなかったり、業務を妨害したりする行為を禁じている。

このほか第247条の2（電子計算機使用詐欺）において、オンラインシステムにおける詐欺等、電子計算機に虚偽の情報もしくは不正な指令を与えることで不正な利益を得ようとすることを禁じている。

ウ) 内部不正による犯罪に関するもの

第247条において、他人のためのその事務を処理する者が、自己もしくは第三者の利益を図りまたは本人に危害を加える目的で、その任務に背く行為をし、本人に財産上の損害を加えることを背任として禁じている。なお、企業の役員等が内部不正として行う機密情報の持

ち出しについては、会社法¹⁰¹における「取締役等の特別背任罪」（会社法第 960 条）が適用されることも多い¹⁰²。

⑥ 電波法

第 109 条の 2（暗号通信の傍受等）において、暗号通信を受信した者が、その漏えいまたは窃用目的での復元を行うことを禁じている。

⑦ 有線電気通信法¹⁰³

第 9 条（有線電気通信の秘密の保護）において、有線電気通信における秘密を侵してはならない旨が定められている。

（3）特定のデータを対象とする法律

① 個人情報保護法

個人データ（個人情報データベース等を構成する個人情報）を取り扱う事業者に対して、次の各条においてその保護を定めている。

ア) 第 20 条（安全管理措置）

取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じることを求めている。

イ) 第 21 条（従業員の監督）

事業者において、その従業員に個人データを取り扱わせる場合に、当該個人データの安全管理が図られるよう、当該従業員に対する必要かつ適切な監督を行うことを求めている。

ウ) 第 22 条（委託先の監督）

事業者において、個人データの取扱いの全部又は一部を委託する場合に、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行うことを求めている。

② 番号法

第 12 条（個人番号利用事務実施者等の責務）において、マイナンバーに係る情報を利用する関係者に対し、当該情報の漏えい、滅失又はき損の防止その他適切な管理のために必要な措置

¹⁰¹ 平成十七年法律第八十六号

¹⁰² 有識者コメントによる。

¹⁰³ 昭和二十八年法律第九十六号

を講ずることが求められている。

コラム：情報漏えい対策を施した個人情報の扱い¹⁰⁴

平成 27 年改正の個人情報保護法では、新たに個人情報をもとに特定の個人を識別することができないように加工することによって作成される「匿名加工情報」が定義された。この匿名加工情報の条件を満たすデータについては個人データとして管理する必要はないが、情報漏えい防止を目的として個人データを暗号化した状態のデータについては、個人情報保護法では特段の規定をしていないことから、個人データと同様の安全管理措置を講じる必要がある。

また、暗号化と並んで情報漏えい防止のための技術的対策である秘密分散技術を用いてデータを保管する場合、保管されているデータの断片単独からは元のデータを復元することはできない。しかしながら対象となるデータが個人データであった場合、同様に個人情報保護法に規定がないことを踏まえ、元のデータへの復元ができないことをもって個人データとして扱う必要がなくなったわけではないことに留意する必要がある。

(4) データを扱う事業者に関する法律

① 電気通信事業法

第 4 条（秘密の保護）において、事業の提供を通じて通信の秘密を侵してはならないことが、業務従事者における秘密保持とともに求められている。

② プロバイダ責任制限法

インターネットサービスプロバイダ等が扱うデータについて、次の 2 条においてその取扱いを定めている。

ア) 第 3 条（損害賠償責任の制限）

事業者が提供するサービスを通じた情報の流通によって他人の権利が侵害され（侵害されていることを知ることができたと認めるに足りる相当の理由がある場合を含む）、かつ当該情報の不特定者への送信の防止が技術的に可能であるとき、サービス提供事業者はその事実を認識しつつ当該情報の送信防止措置を講じない場合に、権利の侵害に対する賠償の責任を負う。

¹⁰⁴ 有識者ヒアリング調査による。

イ) 第 4 条 (発信者情報の開示請求等)

事業者が提供するサービスを通じた情報の流通によって自己の権利が侵害された場合、権利の侵害に対する損害賠償請求に必要な範囲において、サービス事業者に対して発信者情報の開示を求めることができる。

③ 割賦販売法

第 35 条の 16 及び 17 (クレジットカード番号等の適切な管理等) において、クレジットカード番号等のデータを対象に、その漏えい、滅失又はき損の防止その他クレジットカード番号等の適切な管理のために必要な措置を講じることを求めている。適切な管理のための基準に適合していないと認められる場合は、クレジットカード番号等の取扱事業者に対し、業務の方法の変更等の是正措置が命じられる。

2. 1. 2 救済対象となる違法行為とその被害の分類

データに関する違法行為を適用法令別に不正競争行為、不正アクセス、著作権侵害、刑法の定める犯罪行為等に類型化し、それぞれの適用条件や救済措置について整理する。なお、行為の内容によっては複数の法律の定める違法行為に該当する場合がある。

(1) 不正競争行為

平成 30 年改正不正競争防止法では、2. 1. 1 で示した通り、次の①から③に該当する行為が不正競争行為として救済の対象となる。

① 営業秘密の要件を満たすデータに対する不正競争行為

「秘密管理性」「非公知性」「有用性」の 3 要件を満たすデータは営業秘密として、データにアクセスする権限をもたない者がデータを不正に取得したり、データを外部に漏えいさせたりすることで、これらの要件を損なわせるような行為が不正競争行為として損害賠償、差止請求及び刑事罰の対象となる(第 2 条第 1 項第 4～10 号、救済の規定は第 3 条～第 5 条、第 21 条)。

② 限定提供データに対する不正競争行為

平成 30 年改正不正競争防止法の施行後、前述の通り、「限定提供性」「電磁的管理性」「相当蓄積性」の 3 要件を満たすデータは限定提供データとして、その不正競争行為¹⁰⁵が損害賠償請求及び差止請求の対象となる(第 2 条第 1 項第 11～16 号、救済の規定は第 3 条～第 5 条)。

③ 技術的制限手段(いわゆるアクセスコントロール)の効果を妨げる行為及びその助長に関する

¹⁰⁵ このうち、限定提供データの不正取得については、経済産業省が平成 31 年 1 月に公表した「限定提供データに関する指針」において類型化されている。

<http://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pdf>

る行為

映像、画像、音声、プログラム、データ（電磁的に記録された情報）を保護することを目的として、その視聴、実行、記録を制限するために提供されている技術的制限手段（ソフトウェアプロテクト、アクティベーション等）について、その効果を妨げる装置やプログラム、指令符号（シリアルコード等）の譲渡、提供ならびにその効果を妨げるサービスの提供が不正競争行為に相当し、損害賠償請求、差止請求及び刑事罰の対象となる（第2条第1項第17,18号、救済の規定は第3条～第5条、第21条）。

（2）不正アクセス及びその助長に相当する行為

不正アクセス禁止法の定める不正アクセス及びその助長に相当する行為を、同法における規定内容をもとに以下に示す。なお、同法についての違反はいずれも刑事罰の対象となる（罰則の規定は第11条、第12条）。

① 他人の識別符号を用いた不正アクセス行為

他人の ID 及びパスワード等の識別符号を用いて行う行為が違法行為となる（第2条第4項第1号）。

② 識別符号以外の情報や指令を用いた不正アクセス行為

ID 及びパスワード等の識別符号を用いて認証等を行う代わりに、データが格納されている情報システムの脆弱性を悪用したり、マルウェアを感染させたりすることによってネットワークシステムに侵入し行う行為が違法行為となる（第2条第4項第2号）。

③ 外部からアクセス制限されている電子計算機における不正アクセス行為

データが格納されている情報システムとは別の認証用サーバ等を用いることによりアクセス制限を行っている場合において、当該情報システムに対する①②に相当する行為が不法行為となる（第2条第4項第3号）。

④ 他人の識別符号を不正に取得する行為

データが格納されている情報システム等を利用するための他人の ID 及びパスワード等の識別符号を不正に取得する行為そのものが不法行為となる（第4条）。

⑤ 不正アクセス行為を助長する行為

データが格納されている情報システム等に対する外部からの攻撃者の共犯行為として、他人の ID 及びパスワード等の識別符号の取得や不正アクセスの助長等の行為が違法行為となる（第

5条)。

⑥ 他人の識別符号を不正に保管する行為

データが格納されている情報システム等を利用するための他人の ID 及びパスワード等の識別符号を、不正な利用ないし提供の目的で保管する行為が違法行為となる（第 5 条）。

（3）著作権の定めるデータの流出に関する違法行為

著作権法の定める違法行為のうち、データの流出に関する違法行為を以下に示す（罰則の規定は第 120 条の 2 第 1, 2 号）。

① 技術的保護手段の回避を行う行為

平成 24 年の著作権法改正までは、著作権法ではいわゆるコピープロテクト等のコピーコントロール¹⁰⁶のみを技術的保護手段として、その回避を行う装置やプログラムの提供及び回避の実施を違法行為としていたが、同改正以降、暗号化等によるアクセスコントロールを用いて不正な複製を制限するもの¹⁰⁷も技術的保護手段として扱われるようになった（第 120 条の 2 第 1, 2 号）。

② 技術的利用制限手段の回避を行う行為

平成 30 年改正著作権法¹⁰⁸より、①で定める著作物データの不正な複製等による著作権等の侵害行為の制限のみでなく、データに関する利用の制限を行うためのアクセスコントロール機能等の回避を行う行為について、新たに技術的利用制限手段の回避を行う行為として違法行為の対象となった。なお、①の技術的保護手段の回避を行う行為に相当しない、技術的利用制限手段の回避を行う行為については、損害賠償請求及び差止請求の対象であるが、刑事罰は適用されない（第 113 条第 3 項）。

（4）刑法の定めるデータの流出に関する違法行為

刑法の定める違法行為のうち、データの流出に関する違法行為を以下に示す。なお、同法についての違反はいずれも刑事罰の対象となる。

① 秘密漏示罪

特定の業務に従事する者（医師、薬剤師、医薬品販売業者、助産師、弁護士、弁護人、公証人、宗教、祈祷若しくは祭祀の職にある者又はこれらの職にあった者）が、業務上取り扱った

¹⁰⁶ 同法の定義によれば、著作物等の利用に用いる機器が特定の反応をする信号を音や映像とともに記録媒体に記録または送信する方式をいう。

¹⁰⁷ 同法の定義によれば、著作物等の利用に用いる機器が特定の変換を必要とするよう著作物等を構成する音や映像を変換して記録媒体に記録または送信する方式をいう。

¹⁰⁸ 平成 30 年 12 月 30 日施行。

ことについて知り得た人の秘密を正当な理由無く漏えいすることが違法行為となる。具体的には次のような例が該当する（第 134 条第 2 項）。

- 上述の業務を通じて不正に入手したパスワード等の識別符号を用いて、暗号化されたデータを復元する行為
- 上述の業務を通じて入手したデータの不正な使用や開示

② 電磁的記録不正作出及び供用

業務を誤らせる目的で実施される、電子データに対する不正が不法行為となる。例として、脆弱性や他人の ID 及びパスワード等の識別符号の悪用により、本来は存在しないはずの偽りのデータを作り出して、データの所有者や利用権限を持つ者に損害を与える行為がこれに相当する（第 161 条の 2）。

③ 不正指令電磁的記録作成等

正当な理由なく、他人の電子計算機における実行を目的としてマルウェアの作成、提供、供用を行うことが違法行為となる。これは「ウイルス作成罪」とも呼ばれ、コンピュータウイルスをはじめとするマルウェアを他人の環境で実行することを目的とする作成、提供及び供用（つまり実行）ならびにその未遂に関する行為がこれに相当する（第 168 条の 2 第 1 項）。

④ 電子計算機損壊等業務妨害

電子計算機もしくはその用に供するデータを損壊したり、または虚偽の情報や不正な指令を与えたりすることで、電子計算機の本来の目的に即した動作をさせなかったり、業務を妨害したりすることが違法行為となる。具体例として、ドメインネームシステム（DNS）の設定を不正に変更等し、データが格納されている情報システムから、攻撃者の電子計算機にデータを送信させる行為等がこれに相当する（第 234 条の 2）。

⑤ 背任

他人のためのその事務を処理する者が、自己もしくは第三者の利益を図りまたは本人に危害を加える目的で、その任務に背く行為をし、本人に財産上の損害を加えることが違法行為となる。データの流出が損害となる場合、データの流出につながる行為は任務に反するものとなることから、①で例示した行為に相当するものとなる（第 247 条）。

⑥ 電子計算機使用詐欺

オンラインシステムにおける詐欺等、電子計算機に虚偽の情報もしくは不正な指令を与える

ことで不正な利益を得ようとするものが違法行為となる。具体例として、データが格納されている情報システムに対して金額や金利等の数値を不正に設定する等の操作を行うことにより、不正に財産上の利益を得る行為がこれに相当する（第 246 条の 2）。

（５）データ保護に関する義務違反に相当する行為

個人情報保護法、番号法、各種の業法等、データ保護に関する義務を課す法律について、それぞれの法律の定める罰則等の内容について整理する。

① 個人情報保護法

個人情報取扱事業者に所属する役員や従業員の内部不正により、業務で扱う個人情報データベースを自己または第三者の不正な利益を図る目的で提供ないし盗用した場合は、刑事罰の対象となる（第 83 条）。

② 番号法

個人番号利用事務等に従事する者が、業務で扱う個人の秘密に関する事項が記録されたデータを正当な理由なく提供したり、業務を通じて知り得た個人番号を自己または第三者の不正な利益を図る目的で提供ないし盗用したりした場合は刑事罰の対象となる（第 48 条、第 49 条）。

③ 電波法

暗号通信に相当するデータを傍受ないし受信した者が、当該暗号通信の秘密を漏らしたり、窃用する目的でその内容を復元したりした場合は、刑事罰の対象となる（第 109 条の 2）。

④ 有線電気通信法

有線電気通信の秘密を侵した者は、その未遂を含めて刑事罰の対象となる（第 14 条）。

⑤ 電気通信事業法

電気通信事業者の取扱中に係る通信の秘密を侵した者は、その未遂を含めて刑事罰の対象となる（第 179 条）。

⑥ プロバイダ責任制限法

インターネットサービスプロバイダ等の事業者が提供するサービスを通じた情報の流通によって他人の権利が侵害され（侵害されていることを知ることができたと認めるに足りる相当の理由がある場合を含む）、かつ当該情報の不特定者への送信の防止が技術的に可能であるとき、事業者はその事実を認識しつつ当該情報の送信防止措置を講じない場合に、権利の侵害に対す

る損害賠償の対象となる（第3条）。また、発信者情報の開示請求に対し、インターネットサービスプロバイダ等が故意または重大な過失に基づいて応じないことで、当該請求者に損害が生じた場合には、その損害賠償の対象となる（第4条）。

⑦ 割賦販売法

次のような条件に該当する場合に、刑事罰の対象となる（第49条の2）。

- クレジットカード番号等を取り扱う業務に従事する者が、業務を通じて知り得たクレジットカード番号等を自己または第三者の不正な利益を図る目的で提供ないし盗用した場合
- 他人を欺いてクレジットカード番号等を提供させた場合
- クレジットカード番号等が記載された書面等を、承諾を得ずに複製することでクレジットカード番号等を取得した場合
- 不正アクセス行為により、クレジットカード番号等を取得した場合
- 正当な理由なく、有償でクレジットカード番号等を提供ないし提供を受ける場合
- 正当な理由なく、有償で提供する目的でクレジットカード番号等を保管する場合

2.1.3 救済措置による分類

データに関する被害に対する救済措置の種類ごとに、適用される法令の種類を整理する。

(1) 損害賠償

不法行為に対する損害賠償請求が可能となる条件について、不法行為を通じたデータ所有者における損害と適用法令の関係を下表に示す。

表 16 データに関する損害賠償請求における損害と適用法令の関係

データ所有者における損害	適用法令
契約や約款に反するデータの利用による損害	民法
営業秘密や限定提供データを対象とする漏えいや改ざん、削除による損害	不正競争防止法
不正競争対策としての技術的制限手段の効果を妨げる機器やサービスの提供を通じた損害	
著作物の違法コピーによって生じた損害、著作物のコピープロテクトやアクセスコントロール等の技術的保護手段・技術的利用制限手段を回避する手段の提供を通じた損害	著作権法
インターネットサービスプロバイダが権利侵害の防止措置を講じないことによる損害	プロバイダ責任制限法
発信者情報の開示請求に対し、インターネットサービスプロバイダ等が故意または重大な過失に基づいて応じないことによる損害	

(2) 差止請求

違法行為に対する差止請求が可能となる条件について、差止の対象となる違法行為と適用法令の関係を下表に示す。データに対する違法行為による損害の拡大防止の観点から、データの保有者が差止請求を行うことは有効¹⁰⁹であるが、差止が可能な法令は不正競争防止法及び著作権法に限定されており、差止を行うためにはこれらの法律が定める営業秘密等の要件を満たす必要がある。

表 17 データに関する差止請求における違法行為と適用法令の関係

差止の対象となる違法行為	適用法令
営業秘密や限定提供データを対象とする漏えいや改ざん、削除等の違法行為	不正競争防止法
不正競争対策としての技術的制限手段の効果を妨げる機器やサービスの提供等の違法行為	
著作物の違法コピー、著作物のコピープロテクトやアクセスコントロール等の技術的保護手段・技術的利用制限手段を回避する手段の提供等の違法行為	著作権法

(3) 刑事罰

違法行為に対する刑事罰が可能となる条件について、刑事罰の対象となる違法行為と適用法令の関係を下表に示す。

表 18 データに関する刑事罰の対象となる違法行為と適用法令の関係

刑事罰の対象となる違法行為	適用法令
営業秘密を対象とする漏えいや改ざん、削除等の不法行為	不正競争防止法
不正競争対策としての技術的制限手段の効果を妨げる機器やサービスの提供等の違法行為	
著作物の違法コピー、著作物のコピープロテクトやアクセスコントロール等の技術的保護手段を回避する手段の提供等の違法行為	著作権法
他人の ID 及びパスワード等を用いた不正アクセス行為	不正アクセス禁止法
脆弱性を悪用したネットワーク経由の侵入による不正アクセス行為	
他人の ID 及びパスワード等の不正な取得行為	
不正アクセス行為を助長する行為 (ID 及びパスワードを不正に提供する行為)	
他人の ID 及びパスワード等の不正な保管行為	刑法
業務上の守秘義務を課せられた者による秘密の漏示	
業務を誤らせる目的で実施されるデータに対する違法行為	
他人の情報システム等で動作させる目的のマルウェアの作成、保管及び利用	
虚偽の情報や不正な指令を情報システムに与えることによる違法行為	

¹⁰⁹ 企業ヒアリング調査による。

刑事罰の対象となる違法行為	適用法令
他人のために事務を行う者がその任務に背いて損害を加える等の違法行為	
情報システムを用いた詐欺行為	
個人情報取扱事業者の業務で扱う個人情報データベースに対する違法行為	個人情報保護法
個人番号利用事務従事者による業務で扱う個人の秘密に関するデータ及び個人番号に対する違法行為	番号法
暗号通信の秘密についての侵害行為	電波法
有線電気通信の秘密の侵害行為	有線電気通信法
電気通信事業者による通信の秘密の侵害行為	電気通信事業法
クレジットカード番号等の取扱業務従事者による違法行為	割賦販売法
クレジットカード番号等の不正な取得行為	
正当な理由のない、クレジットカード番号等の有償による譲受及び有償提供目的での保管	

2.1.4 データに関する被害とそれに対応する法律との関係

データについて想定される被害について、上述のどの法律による救済措置が可能かについて、救済措置の種類とともに整理したものを次ページ表に示す。

2.2 法的救済に関する国内事例の紹介

ここでは、前項で示したデータ保護に関する法律が争点となった裁判例について、過去10年間にわたる傾向と具体例を紹介する。

2.2.1 データに係る事案数の推移

次表に過去10年間におけるデータに係る事案数の推移を示す。なお、刑事・民事事件数に関してはデータに係る事案数に限定した統計値が存在しないことから、事案総数を示す。このとき、平成20年時点で刑事事案総数に対するサイバー犯罪検挙件数が0.5%程度であったのに対し、平成29年には1%に近づくなど、データに係る事案の占める比率が増加していることがわかる。

表20 データに係る事案数の推移

		H20	H21	H22	H23	H24	H25	H26	H27	H28	H29
サイバー 犯罪 検挙 件数	総数	6,321	6,690	6,933	5,741	7,334	8,113	7,905	8,096	8,324	9,014
	うち不正アクセス禁止法 ¹¹¹ 違反	1,740	2,534	1,601	248	543	980	364	373	502	648
	うちコンピュータ・電磁的記録対象犯罪、不正指令電磁的記録に関する罪	247	195	133	105	178	478	192	240	374	355
	電子計算機使用詐欺 ¹¹²	220	169	91	79	95	388	108	157	281	228
	電磁的記録不正作出・毀棄等 ¹¹³	20	22	36	17	35	56	48	32	24	39
	電子計算機損壊等業務妨害 ¹¹⁴	7	4	6	6	7	7	8	6	11	13
	不正指令電磁的記録作成・提供 ¹¹⁵	—	—	—	0	4	8	9	8	4	29
	不正指令電磁的記録供用 ¹¹⁶	—	—	—	1	34	14	16	21	36	24
	不正指令電磁的記録取得・保管 ¹¹⁷	—	—	—	2	3	5	3	16	18	22
	うちネットワーク利用犯罪	4,334	3,961	5,199	5,388	6,613	6,655	7,349	7,483	7,448	8,011
詐欺	1,508	1,280	1,566	899	1,357	956	1,133	951	828	1,084	
著作権法 ¹¹⁸ 違反	144	188	368	409	472	731	824	593	586	398	
その他	2,682	2,493	3,265	4,080	4,784	4,968	5,392	5,939	6,034	6,529	
事案総数(データに係るもの以外も含む全数) ¹¹⁹											
	刑事事件数	1,238,800	1,215,143	1,158,443	1,105,826	1,099,009	1,050,716	1,018,673	1,032,799	999,059	959,545
	民事事件数	2,252,437	2,408,571	2,179,355	1,985,303	1,707,714	1,524,023	1,455,734	1,432,332	1,470,647	1,529,382

(注) —は統計値が存在しない。

2.2.2 個別事案についての分析

我が国における具体的な裁判例、事件例をもとに、技術内容や判決における判断の内容について

¹¹⁰ 出典：警察庁 サイバー犯罪対策プロジェクトにおける各種公表資料

<https://www.npa.go.jp/cyber/statics/index.html>

¹¹¹ 不正アクセス行為の禁止等に関する法律（平成十一年法律第二百二十八号）

¹¹² 刑法（明治四十年法律第四十五号）第247条の2

¹¹³ 刑法第161条の2

¹¹⁴ 刑法第234条の2

¹¹⁵ 刑法第168条の2

¹¹⁶ 刑法第168条の2

¹¹⁷ 刑法第168条の3

¹¹⁸ 昭和四十五年法律第四十八号

¹¹⁹ 出典：裁判所データブック2018

<http://www.courts.go.jp/about/databook/index.html>

ての分析を行う。

(1) 個別事案の一覧

平成25年以降に判決が示された事案のうち、データに係るものについて、結果、裁判要旨等を含めて整理した結果を示す。

① 刑事事件

ア) インターネットバンキングへの不正（不正アクセス行為の禁止等に関する法律違反、電子計算機使用詐欺、私電磁的記録不正作出・同供用、不正指令電磁的記録供用、電波法違反被告事件）

表 21 裁判例調査結果（その1）

事件番号	平26（特わ）927号・平26（刑わ）2373号・平26（刑わ）2564号・平26（刑わ）2942号・平26（刑わ）3265号・平27（刑わ）490号・平27（刑わ）934号・平27（特わ）1411号・平27（特わ）1558号・平27（特わ）1670号
裁判年月日	平成29年4月27日判決
裁判所名	東京地裁
結果	一部有罪、懲役8年
原審	—
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/009/087009_hanrei.pdf
裁判要旨	被告人が、フィッシングメールや遠隔操作ウイルス等を利用して複数企業のインターネットバンキングの識別符号を不正に取得し、不正ログインや不正送金を行い、その他、様々な手法を用いてサイバー攻撃を行っているとして罪に問われた事案において、WEP鍵は、無線通信の内容として送受信されるものではなく、無線通信の秘密にあたる余地はないから、WEP鍵の利用は犯罪を構成せず、結局前記公訴事実については罪とならないから、同部分につき、被告人を無罪とする一方、被告人は様々な手法を用いてサイバー攻撃を行っている上、犯行の発覚を免れるため、あらかじめ不正に取得した暗号化鍵を用いて他人の無線LANアクセスポイントへ接続し、ときには中継サーバも経由させて接続元を隠し、また、不正送金の前には連絡用メールアドレスを変更する等しており、本件犯行の態様は巧妙で悪質であり、不正送金による財産的被害は合計519万円余りと高額に上っており、その被害結果は大きく、同種前科による前刑の仮釈放後間もなく本件各犯行に及んでいるおり常習性顕著であるとして、被告人に

	懲役8年を言い渡した事例
--	--------------

イ) ETC への不正 (電子計算機使用詐欺被告事件)

表 22 裁判例調査結果 (その2)

事件番号	平成27(わ)188
裁判年月日	平成27年6月9日
裁判所名	横浜地裁判決
結果	懲役1年6月、執行猶予3年
原審	—
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/203/085203_hanrei.pdf
裁判要旨	運転手である被告人が、ETC システムに対して、特大車である連結車両で高速道路を通行するに当たり、これらの車軸のうち1車軸を一時的に上昇させることにより、3車軸であり料金車種区分上の大型車である旨の虚偽の情報を与えて高速道路の通行料金の一部の支払を免れようと企て、会社に1085円相当の財産上の不法の利益を得させた事件

ウ) ベネッセ顧客情報の漏えい (不正競争防止法違反被告控訴事件)

表 23 裁判例調査結果 (その3)

事件番号	平28(う)974号
裁判年月日	平成29年3月21日
裁判所名	東京高裁判決
結果	原判決破棄・有罪 (懲役2年6月、罰金300万円 (求刑 懲役5年及び罰金300万円))
原審	平成28年3月29日 東京地裁立川支部 判決 平26(わ)872号 不正競争防止法違反被告事件
公開 URL	
裁判要旨	通信教育等を業とする株式会社Aが株式会社Bに業務委託したAの情報システムの開発等の業務に従事し、営業秘密であるAの顧客情報 (以下「本件顧客情報」という。) を、これが記録されたAのサーバコンピュータ (以下「本件サーバ」という。) に業務用パーソナルコンピュータ (以下「業務用PC」という。) からアクセスするためのID及びパスワード等を付与されるなどして示されて

いた被告人が、不正の利益を得る目的で、その営業秘密の管理に係る任務に背いて、①2度にわたり、業務用PCを操作して、本件顧客情報が記録された本件サーバにアクセスし、合計約2989万件の顧客情報のデータをダウンロードして業務用PCに保存した上、これとUSBケーブルで接続した自己のスマートフォンの内蔵メモリ又はマイクロSDカードにこれを記録させて複製する方法により、上記顧客情報を領得し、②上記顧客情報のうち約1009万件の顧客情報について、インターネット上の大容量ファイル送信サービスを使用し、サーバコンピュータにこれらをアップロードした上、ダウンロードするためのURL情報を名簿業者に送信し、同人が使用するパーソナルコンピュータに上記データをダウンロードさせて記録させることにより、これらの顧客情報を開示した、という不正競争防止法違反の事案。

被告人は、平成25年7月頃、充電目的で自己のスマートフォンを業務用PCに接続したところ、スマートフォンへのデータの書き出しが可能な状態にあることに気づき、本件データベース内の本件顧客情報を自己のスマートフォンに書き出して名簿業者に売却する行為を繰り返すようになった。そして、被告人は、平成26年6月、業務用PCからバッチサーバを経由して本件データベースにアクセスし、コマンドを入力して本件顧客情報を業務用PCの画面上に表示させ、これを業務用PCに保存した上、USBケーブルで接続した自己のスマートフォンに本件顧客情報のデータを記録させて複製し、本件各犯行に及んだ。

不正競争防止法2条6項の秘密管理性の要件は、事業者の営業上の利益保護の観点から保護に値する情報を限定するとともに、当該情報を取り扱う従業者に刑事罰等の予測可能性を与えることを趣旨とすることから、①当該情報にアクセスできる者を制限するなど、当該情報の秘密保持のために必要な合理的管理方法がとられており、②当該情報にアクセスした者につき、それが管理されている秘密情報であると客観的に認識することが可能であることを要するが、可能な限り高度な対策を講じて情報の漏出を防止するといった高度な情報セキュリティ水準まで要するものではない。

まず、①の要件について、判断すると、A及びBでは、アカウントの管理により本件顧客情報にアクセスできる者を従業者の一部に限定するとともに、執務室への入退室の管理等により無権限者からのアクセス防止措置をとり、社内規程において、本件顧客情報を機密に位置づけ、研修等でアクセス権限のある従業者にその趣旨の浸透を図り、関係者以外に本件顧客情報を開示することを禁止

した上、その実効性を高めるため、私物パーソナルコンピュータの使用を禁止し、業務用PCの持ち出しや外部記録媒体への書き出しを原則として禁止し、業務用PCによる本件データベースへのアクセス記録を保存していた。なお、外部記録媒体に対する管理については、記録媒体を有する私物スマートフォンの執務室内への持ち込みや業務用PCに接続しての充電が許容され、実際には多くのスマートフォンについて書き出し制御が機能していなかったなど、十分でなかったことは否定できないが、Bにおける研修等により、従業者にはスマートフォンを含む外部記録媒体への書き出し制御が実施されている旨周知されていた。また、本件システムのアカウント等の情報が、顧客分析課の共有フォルダ内に複数蔵置されていたが、本来アクセス権限がないにもかかわらず、上記の情報を利用して本件データベース内の本件顧客情報にアクセスできた者の人数が8名以内であったことに照らすと、アカウントを用いた本件顧客情報へのアクセス制限の実効性が失われていたとはいえない。以上の事実を総合すると、本件当時、A及びBにおいて、本件顧客情報につき、アクセスできる者を制限するなど、当該情報の秘密保持のために必要な合理的管理方法がとられていたといえることができる。

次に、②の要件について、判断すると、本件顧客情報は、アカウント等によりアクセス制限が行われ、外部記録媒体への書き出しが制限されていたこと、Bでは、毎年、従業者全員を対象とした情報セキュリティ研修を実施し、個人情報や機密情報の漏えい等をしてはならない旨記載された受講報告書のほか、個人情報及び秘密情報の保秘を誓約する内容の同意書の提出を求めており、被告人も、Bでの業務開始時に加え、その後も毎年研修を受講し、上記受講報告書及び同意書を作成して提出していたこと、本件システムの内容及び目的並びにその中の情報の性質等から、本件データベース内に集積される本件顧客情報がAの事業活動に活用される営業戦略上重要な情報であって機密にしなければならない情報であることは容易に認識することができ、実際に被告人を含む従業者は、そのことを認識していたと認められることなどからすれば、本件顧客情報にアクセスする従業者において、それが管理されている秘密情報であることを客観的に認識することが可能であったと認められる。

Bでは、毎年、従業者全員を対象とした情報セキュリティ研修を実施し、個人情報や機密情報の漏えい等をしてはならない旨記載された受講報告書のほか、個人情報及び秘密情報の保秘を誓約する内容の同意書の提出を求めていた上、本件システムの内容及び目的並びにその中の情報の性質等から、本件データベ

一ス内に集積される本件顧客情報がAの事業活動に活用される営業戦略上重要な情報であって機密にしなければならない情報であることは容易に認識することができたといえる。そうすると、後記のとおり、本件顧客情報へのアクセス制限に様々な不備があったとはいえ、一定のアクセス制限の措置がとられていたことを併せ考慮すると、本件において、秘密管理性の要件は満たされていたといえることができる。

Bにおける本件顧客情報の管理体制については、①本件データベースには、アカウントを通じてアクセス制限が行われていたものの、そのアカウント情報がBの共有フォルダ内に蔵置されていて、閲覧可能であったこと、②私物のスマートフォンの執務室への持ち込みが禁止されていなかったこと、③本件データベースにはアラートシステムが導入されていたが、実際には機能していなかったことなどの点で、不備があったと認められ、これらの点は、本件の発覚後にA社内に設けられた個人情報漏えい事故調査委員会の調査報告においても、指摘されているところである。加えて、前記のとおり、Bにおいては、相当数の業務委託先会社に所属する従業員を、パートナーと称し、実態は派遣労働者として受け入れ、本件システムの開発等の業務に従事させていたものである。特に、被告人は、3次派遣の労働者に該当し、Bの上長においても、被告人の所属先会社を正確には把握していない状態であった。システムエンジニアリングの業界においては、変動する労働力の需要に対応するため、このような安易かつ脱法的な労働力の確保が常態的に行われていたことがうかがえるが、Aのような大手企業が子会社であるBを通じてこのような方法を採用し、同社にとって経歴等が詳らかでない者に、経営の根幹にかかわる重要な企業秘密である本件顧客情報へのアクセスを許していたということは、秘密情報の管理の在り方として、著しく不適切であったといわざるを得ない。したがって、A等がこのような労働者に本件顧客情報へのアクセスを許したからには、秘密漏えい対策を講じたとしても、それに伴って生じる危険もある程度甘受すべき立場にあったといえる。また、上記③のアラートシステムについても、これが正常に機能していれば、被告人が同種の情報漏えい行為を行った比較的早い段階で、Bがこれを察知し、更なる被害拡大に対する防止策を立てることが可能であったと思われるのに、アラートシステムが全く機能していなかったため、約1年間にわたって被告人の同種行為が放置され、外部からの通報によりようやく本件が発覚したのであって、被告人が同種行為を反復継続したことが責められるべきであるとしても、被害が拡大したことの原因の一端は、B側の対応にもあるというべき

	<p>である。</p> <p>以上のとおり、被告人が本件犯行に及んだ背景事情として、A及びBにおける本件顧客情報の管理に不備があるとともに、被害が拡大したことの要因として、同社等の対応の不備があると指摘できるのであり、これらの点で、本件における被害者側の落ち度は大きいというべきであって、本件の結果をひとえに被告人の責めに帰するのは相当でないというべきである。</p> <p>しかるに、原判決は、量刑の理由においてこれらの点に全く言及しておらず、これらの点を考慮することなく前記の刑を量定したものとみるほかない。これらの点は、被告人にとって有利な量刑事情に相当するところ、これらの点を考慮に入れていない原判決は、量刑判断として明らかにバランスを失するものであり、これらを正當に考慮に入れた場合と比較して、重きに失する判断に至ったものといわざるを得ない。</p>
--	--

エ) CAD ソフトのアクティベーション機能回避プログラム提供（商標法等違反被告事件）

表 24 裁判例調査結果（その4）

事件番号	不明
裁判年月日	平成 28 年 7 月 1 日
裁判所名	秋田地裁判決
結果	懲役 2 年 6 月（執行猶予 4 年）罰金 2 0 0 万円
原審	—
公開 URL	民事事件（東京地裁平成 30 年 1 月 30 日）から引用
裁判要旨	被告人は、他人の商標に類似する商標をヤフオク上に掲載し、インターネット端末を利用する不特定多数の者に閲覧させた（商標法 3 7 条 1 号違反）として起訴され、被告人は起訴事実を全て認めた。裁判所は、被告人に対し、他の起訴事実とあわせて、懲役 2 年 6 月（執行猶予 4 年）罰金 2 0 0 万円の有罪判決を言い渡した。民事（1 2）参照。

オ) 電子書籍（不正競争防止法違反被告事件）

表 25 裁判例調査結果（その5）

事件番号	平 2 8（う）5 9 8 号
裁判年月日	平成 29 年 12 月 8 日
裁判所名	大阪高裁判決

結果	有罪
原審	京都地裁 平成 28 年 3 月 24 日 平 2 6 (わ) 4 0 5 号
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/780/087780_hanrei.pdf
裁判要旨	<p>C社は電子書籍の映像を配信するにあたって暗号化を行い、同社が提供する映像表示・閲覧ソフト（以下「本件ビューア」という。）による復号を必要とするようにしていた。被告人らは、本件ビューアに組み込まれている映像等の記録・保存の防止機能を無効化する方法で、本件ビューア以外でも上記映像の視聴を可能とするプログラム「F 3」を、2名の者に提供した。</p> <p>本件において、C社が電子書籍の映像を配信するにあたり、その閲覧のために本件ビューアによる復号が必要になるようコンテンツを暗号化しているのが、技術的制限手段に該当することは明らかである。この技術的制限手段の効果は、本件ビューアがインストールされた機器以外の機器では暗号化されたコンテンツの表示ができないということである。復号されたコンテンツが記録・保存されれば、他の機器でも自由にコンテンツが表示できるようになり、他の機器ではコンテンツの表示ができないという効果が妨げられるのであるから、F 3 が、不正競争防止法 2 条 1 項 1 0 号の「技術的制限手段の効果を妨げることにより映像の視聴を可能とする機能を有するプログラム」に該当するとした原判決は正当であって、電気通信回線を通じて F 3 を他者にダウンロードさせて提供する行為は、不正競争行為にあたる。</p>

カ) 複製ゲーム（商標法違反、不正競争防止法違反被告事件）

表 26 裁判例調査結果（その 6）

事件番号	平 2 9 (わ) 4 8 号
裁判年月日	平成 29 年 4 月 17 日
裁判所名	岡山地裁判決
結果	懲役 1 年及び罰金 3 0 万円
原審	
公開 URL	
裁判要旨	<p>本件は、被告人が既製品の△△のプログラムを改造するなどして複製ゲームソフトを使用できるようにして、それを 3 名に売却したという商標法</p>

	<p>違反及び不正競争防止法違反の事案である。</p> <p>被告人は、△△プログラムを改変して、ライセンス情報等に基づく適正な認証、復号をすることなくゲームデータ等の実行を可能とするプログラムを作成した。被告人は、これに既製品の商標と同一の商標を付した「△△」を代金合計5万7500円で販売した。これらの行為は、指定商品についての登録商標と同一の商標の使用による商標権侵害にあたるとともに、営業上用いられている技術的制限手段により制限されているプログラムの実行を当該技術的制限手段の効果を妨げることにより可能とする機能を有するプログラムを記録した記録媒体を譲渡する不正競争行為にあたる。</p>
--	--

キ) カラオケ（商標法違反、不正競争防止法違反被告事件）

表 27 裁判例調査結果（その7）

事件番号	平27（わ）448号
裁判年月日	平成28年2月29日
裁判所名	岡山地裁判決
結果	懲役1年6月，執行猶予3年
原審	
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/789/085789_hanrei.pdf
裁判要旨	<p>使用権限のない登録商標に類似した商標を用いて、技術的制限手段が正常に働かないように改造した通信カラオケ装置を販売した事案。</p> <p>被告人は、株式会社Aの商標（以下「本件商標」という。）の使用に関して何ら権限がないのに、その販売する通信カラオケ機器にこれを使用した。同機器には、使用開始後一定の期間が経過した後は、A社と情報サービス契約を締結した者以外の者が影像及び音の視聴をすることを不可能とする機能があるが、被告人は同機器の時計機能を正常に機能させないようにして、一定の期間が経過した後も前記契約を締結しないまま影像及び音を視聴することを可能にする改造を施した。被告人らは、この通信カラオケ機器を、代金合計18万0600円で売却した。これは、指定商品についての登録商標に類似する商標の使用による商標権侵害であるとともに、技術的制限手段の効果を妨げることにより可能とする装置を組み込んだ機器の譲渡の不正競争行為にあたる。</p>

	<p>本件は、常習的な事件であり、社会的影響も大きいが、その一方で、高齢者等の個人向けに安価なカラオケをも利用してもらいたいためのものであり、利欲目的も希薄であるため、罰金刑を併科しない懲役刑とし、執行猶予を付した。</p>
--	--

ク) ウェブサイト (わいせつ電磁的記録記録媒体陳列, 公然わいせつ被告事件)

表 28 裁判例調査結果 (その8)

事件番号	平27(わ)920号
裁判年月日	平成29年3月24日
裁判所名	京都地裁判決
結果	懲役2年6月, 執行猶予4年及び罰金250万円
控訴審	平成30年9月11日大阪高裁判決 平29(う)635号 わいせつ電磁的記録記録媒体陳列, 公然わいせつ被告事件があるが, 控訴棄却のため原審概要を記載
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/681/086681_hanrei.pdf
裁判要旨	<p>被告人Aは、大阪市に本店を置き、インターネット・ホームページの企画、立案、制作並びにインターネットでのサーバの設置及びその管理業務等を目的とし、アメリカ合衆国所在のC社(代表者D)と共にインターネットサイト「E」を管理・運営するF社の実質的相談役、被告人BはF社の代表取締役である。被告人両名は、C社の代表者と共に、投稿者らと共に共謀して、被告人らがC社と共に管理するサーバコンピュータに、投稿者が送信した無修正わいせつ動画のデータを記録・保存させる等し、インターネット利用者が無修正わいせつ動画を閲覧できる状態を設定したわいせつ電磁的記録記録媒体陳列1件及び各配信者らと共に共謀して、各配信者らが配信サイトの映像配信システムを利用して無修正わいせつ動画を即時配信し、不特定の視聴者らに閲覧させた公然わいせつ2件からなる事案において、被告人らは、無修正わいせつ動画が相当数投稿・配信されていることを認識しながら、これに対する措置を講じることなく許容し、一部は増収の手段として利用したと判断された。</p> <p>弁護人らは、いずれの犯行についても、被告人らは無修正わいせつ動画の投稿・配信に関与しておらず実行行為を行っていないし、無修正わいせつ動画の投稿者・配信者と共謀したこともないから、被告人らには実行共</p>

同正犯も共謀共同正犯も成立しないと主張したが認められなかった。

E動画では、インターネットを通じて、C社が契約するサーバに動画データを投稿することができる。投稿された動画データは、C社が管理する配信サーバへ送られるところ、不特定多数の視聴者は、そのサーバにアクセスすることで、その動画の内容を視聴できるが、日本で視聴する場合には、アメリカ合衆国にある配信サーバから長距離通信をせざるを得ず、視聴までに時間がかかるため、有料会員については、動画データを日本にあるキャッシュサーバに一時的に保存し、そこから配信することで通信の高速化が図られている。有料会員になると、無料会員では視聴できない動画も視聴でき、1日当たりの視聴制限が無制限となり、高画質動画データの配信を受けられるなどの特典があり、視聴者に有料会員登録を促す措置が講じられている。

また、E動画では、視聴者が投稿動画を介して新規に有料会員登録をした場合には、投稿者は登録料の一定割合に相当するポイントを報酬として受け取ることができ、それを現金化できるなどの仕組み（動画アフィリエイト制度）や、投稿された動画を視聴者に評価させる仕組み（動画評価システム）など、投稿者により多くの動画を配信するよう促す措置が講じられている。

E動画の大半が日本からのアクセスとなっている。またF社におけるEに関する業務について検討すると、F社は、C社との間で業務委託契約を締結しているものの、F社の前身である有限会社Fの時代から、Eの商標登録を保有している上、F社従業員が仕事で使うメールアドレスのドメインは、「(E社の社名). us」や「(E社の社名) co. jp」を使用し、取引先に対してもC社の従業員を名乗るよう指示され、F社従業員がC社の代表者であるDを「社長」と呼ぶ等の事情がうかがえる。

本件が問題となる平成25年から平成26年にかけても、F社はE関連のWebサービスを事業の核とし、Eのブログ・無料ホームページ・動画・ライブのシステム開発、サーバの保守・管理、ユーザーサポート、その他広告枠の販売業務を行っていたことが認められる。

上記その他の事情から、D及び被告人らは、E動画アダルトやEライブアダルトにおいて相当数の無修正わいせつ動画が配信されることを認識した上で、C社やサーバが米国にあるとの理由から許容し、それらを利用してサイト利用者や有料会員を維持・増加させようとして、E動画アダルト

	<p>トやEライブアダルトを管理・運営していたと認められるとされた。</p> <p>なお、本件では、被告人らがDとともにE動画アダルトのサーバを管理・運営し、動画をサーバに記憶・保存させた行為がわいせつ電磁的記録記録媒体の実行行為の一部に該当するか否かも争われているが、仮にこれが実行行為に該当しないとしても、被告人らがサーバを管理・運営しなければ、投稿された無修正わいせつ動画を不特定多数の者が閲覧できる状態に置くことはできないから、被告人らがサーバを管理・運営した行為は、Gらによる実行行為の不可欠の前提を成すものであり、被告人らは正犯者といえる程度に重要な役割を果たしたといえるので、少なくとも共謀共同正犯が成立すると認められた。</p>
--	--

ケ) マイニングプログラムの自動実行（不正指令電磁的記録作成等，不正指令電磁的記録供用被告事件）

表 29 裁判例調査結果（その9）

事件番号	平30（わ）114号・平30（わ）179号
裁判年月日	平成30年7月2日
裁判所名	仙台地裁判決
結果	懲役1年，執行猶予3年
原審	
公開URL	
裁判要旨	<p>本件は、他人のコンピュータの処理能力を勝手に用いて仮想通貨のマイニングを行い、利益を得た事案である。</p> <p>被告人は、使用者に気付かれずにマイニングを行うプログラムを自動で実行する機能を有するプログラムを作成し、現にそのプログラムをインターネット上にアップロードして実行の用に供した。被告人の有するプログラミングの知識・技術を悪用した巧妙な犯行であるところ、現に被告人が作成したプログラムをダウンロードした者がおり、これにより被告人が仮想通貨上の5000円程度の報酬を得たことからすると、本件の社会的影響は軽視できない。被告人は、他人のパーソナルコンピュータの処理能力を利用して仮想通貨を得ようという利欲的な動機から本件各犯行に及んだものであって、電子計算機のプログラムに対する信頼を毀損する害悪の根源を作り出し、害悪を社会に拡散させた本件の犯情は相応に重い。</p>

	しかしながら、被告人のために酌むべき事情が認められることなども併せ考慮し、今刑の執行が猶予された。
--	---

コ) リベンジポルノ（強要未遂，私事性的画像記録の提供等による被害の防止に関する法律違反，わいせつ電磁的記録記録媒体陳列被告事件）

表 30 裁判例調査結果（その10）

事件番号	平29（う）136号
裁判年月日	平成29年6月30日
裁判所名	大阪高裁判決
結果	破棄自判・一部有罪（懲役1年，執行猶予3年），一部無罪
原審	第一審 平成28年12月15日 大阪地裁 判決 平28（わ）4148号 強要未遂，私事性的画像記録の提供等による被害の防止に関する法律違反，わいせつ電磁的記録記録媒体陳列被告事件
公開 URL	
裁判要旨	<p>被告人は、自宅のパソコンを使用して、インターネットを介し、元交際相手の女性（以下「被害者」という。）の顔を写した画像データと共に、その露出した胸部等を撮影した画像データ及び動画データを a 社が管理するサーバーコンピュータ内に開設された〇〇サービスに送信して記憶、蔵置させた。被告人は同時に自宅のパソコンを使用し、被害者が使用するメールアドレスに、被害者の裸体画像等と共に返信がなければばらまく旨記載した電子メールを送信して閲読させ、その要求に応じなければ被害者の名誉に危害を加える旨告知して怖がらせ、義務のないことを行わせようとしたが、被害者が応じず、その目的を遂げなかったという強要未遂の事実でも起訴された。</p> <p>上記各公訴事実の外形的事実に争いはなく、原審では本件データの内容が「公然と陳列」されたといえるか否かが争われた。原審ではいずれの罪も既遂に達したと判断された。しかし控訴審では、被告人が本件データを〇〇サービスに記憶蔵置し、その公開を設定して公開用のURLの発行を受けたというだけでは、いまだ、同データの内容を不特定又は多数の者が認識し得る状態に置いたとみることはできず、公然陳列罪は成立しないと判断された。具体的には、同サービスの利用者は、a 社から受け取った公開用のURLを他のユーザーに示して、これを受け取ったユーザーがデー</p>

	<p>タを閲覧する仕組となっている。公開用のURLを受け取らずに閲覧することは不可能ではないが容易なことではない。本件においては、被告人は公開URLを被害者以外には通知していなかった。このことから、控訴審では、不特定又は多数の者が閲覧できる状態にはなく、公然陳列罪は成立しないと判断された。</p>
--	---

サ) 電話帳データの抜き取りアプリ（携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律違反，特定電子メールの送信の適正化等に関する法律違反，不正指令電磁的記録取得等，不正指令電磁的記録供用被告事件）

表 31 裁判例調査結果（その11）

事件番号	平25（わ）1111号・平25（わ）1204号
裁判年月日	平成25年11月8日
裁判所名	千葉地裁判決
結果	<p>被告人株式会社A 罰金500万円</p> <p>被告人B 懲役3年及び罰金150万円，執行猶予5年</p> <p>被告人C 懲役2年，執行猶予3年</p> <p>被告人D 懲役4月，執行猶予3年</p>
原審	—
公開URL	http://www.courts.go.jp/app/files/hanrei_jp/976/083976_hanrei.pdf
裁判要旨	<p>被告人株式会社A（以下「被告会社」という）は広告代理業等を営むもの、被告人Bは被告会社の代表取締役としてその業務全般を統括管理するもの、被告人C、同D及びEは、被告会社の従業員である。</p> <p>被告人B及び同Cは、共謀の上、正当な理由がないのに、実行者の意図に基づかずにスマートフォンに記録された電話帳データをアメリカ合衆国フロリダ州内に設置されたサーバコンピュータに送信する指令を与える電磁的記録であるウイルス・プログラムを同サーバコンピュータの記憶装置にアップロードしてアクセス及びダウンロード可能な状態で蔵置し、福岡県宗像市所在のP方ほか2か所にいた同人ほか2名が使用する携帯電話機に、上記ウイルス・プログラムをダウンロードさせた。</p>

シ) Microsoft Word 等（不正競争防止法違反，商標法違反，犯罪による収益の移転防止に関

する法律違反被告事件)

表 32 裁判例調査結果 (その 1 2)

事件番号	平 2 7 (わ) 1 6 1 号 ・ 平 2 7 (わ) 2 1 8 号 ・ 平 2 7 (わ) 4 6 7 号
裁判年月日	平成 27 年 9 月 8 日
裁判所名	神戸地裁判決
結果	懲役 2 年及び罰金 2 0 0 万円, 執行猶予 5 年
原審	—
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/750/085750_hanrei.pdf
裁判要旨	<p>被告人は, 「Microsoft Office Professional Plus 2013」 のライセンス認証システムの効果を妨げるように改造したプログラムを, C 株式会社が管理するサーバコンピュータの記憶装置に記憶・蔵置させた上, 前記プログラムの蔵置先 URL 情報を記録した圧縮ファイル D の蔵置先 URL を, インターネットオークションの落札者である E に通知して提供した。これは, 営業上用いられている技術的制限手段により制限されているプログラムの実行を当該技術的制限手段の効果を妨げることにより可能とする機能を有するプログラムを電気通信回線を通じて提供する, 不正競争にあたる。被告人は, 単に落札者に認証回避プログラムの蔵置先 URL を通知しただけでなく, 自ら認証回避プログラムを自分が使用する登録名に割り当てられた記憶領域に記憶・蔵置させ, これを他のインターネット利用者が閲覧, 取得できるように設定しているから, 一連の行為が情報ないしノウハウの提供にとどまらないことは明らかであって, 不正競争防止法 2 条 1 項 1 1 号にいうプログラムの提供に該当する。</p> <p>被告人は, また, ネットオークションサイトにおける出品制限を回避するべく, 他人になりすまして特定事業者との間における預貯金契約に係る役務の提供を受けることを目的として, 姉である F から, 株式会社 G 銀行 H 支店に開設された同人及びその 2 人の子各名義の総合口座通帳 3 通及びキャッシュカード 3 枚を譲り受けた。これは犯収法に違反する。</p> <p>被告人はさらに, 株式会社ジャストシステムが電子計算機用プログラムを指定商品として商標登録を受けている「一太郎」の標準文字からなる商標に類似する商標を, 「一太郎 2 0 1 4 徹 スーパープレミアム (ダウンロード版)」 と称する電子計算機用プログラムに関する販売広告に利用</p>

	した。これは、株式会社ジャストシステムの商標権を侵害する行為とみなされる。
--	---------------------------------------

ス) B-CAS (私電磁的記録不正作出, 同供用被告事件)

表 33 裁判例調査結果 (その13)

事件番号	平26(う)121号
裁判年月日	平成26年5月22日
裁判所名	大阪高裁判決
結果	控訴棄却, 懲役2年及び罰金200万円, 執行猶予5年
原審	第一審 京都地裁平成25年12月3日判決
公開URL	http://www.courts.go.jp/app/files/hanrei_jp/527/084527_hanrei.pdf
裁判要旨	<p>原判決は、B-CASカードは、「権利、義務に関する電磁的記録」であり、B-CASカードを用いた「事務処理」も観念できるところ、被告人が各B-CASカードの電磁的記録を改変する行為は、私電磁的記録不正作出罪の構成要件を客観的に充足し、改変されたB-CASカードをテレビに接続された衛星放送受信可能な各チューナー内蔵レコーダーに挿入する行為も、不正作出私電磁的記録供用罪の構成要件を客観的に充足していると判断し、原判示の各事実を認定した上、私電磁的記録不正作出罪及び同供用罪の成立を認めた。</p> <p>控訴審は、原審の事実認定及び法令の解釈適用は、全て正当であり、その理由として説示するところもおおむね是認することができるとした上で、以下のように付言した。</p> <p>B-CASカードに記録された電磁的記録は、刑法161条の2第1項、3項所定の人の事務処理の用に供する権利、義務に関する電磁的記録に該当し、被告人がこれを改変する行為は、同条1項所定の、人の事務処理を誤らせる目的で人の事務処理の用に供する権利、義務に関する電磁的記録を不正に作ったこと(不正作出)に該当するほか、被告人が改変した上記電磁的記録を記録したB-CASカードをテレビに接続された衛星放送受信可能なチューナー内蔵レコーダーに挿入する行為は、同条3項所定の、人の事務処理を誤らせる目的で不正に作られた権利、義務に関する電磁的記録を人の事務処理の用に供したこと(供用)に該当すると認められる。</p>

	<p>すなわち、B-CASカード記載の情報は、衛星放送事業者との視聴契約に基づいて受信権限の有無を判定するために用いられるものであるから、衛星放送事業者の財産上又は社会的責務上の事務処理の用に供する電磁的記録であるとともに、衛星放送事業者との視聴契約に基づく受信権限に関する電磁的記録である。そして、B-CASカードの記録の改変は、被告人が、受信権限のない衛星放送を受信して視聴するため、上記電磁的記録を、あたかも被告人に当該受信権限があるかのように当該衛星放送事業者の許諾を得ることなく書き換えるものであるから、同事業者との視聴契約に基づく受信権限に関する電磁的記録の不正作出に当たる。</p> <p>さらに、被告人が、改変したB-CASカードを、チューナー内蔵レコーダーに挿入した行為は、被告人が受信権限のない衛星放送を受信して視聴するため、あたかも被告人に当該受信権限があるかのように装うために用いたこと（供用）に当たる。</p>
--	--

② 民事事件

ア) データ、ソースコードの不正開示を受けて製品製造・販売した事案（不正競争行為差止等請求控訴事件）

表 34 裁判例調査結果（その14）

事件番号	平29（ネ）10007号
裁判年月日	平成30年3月26日判決
裁判所名	知財高裁
結果	製品の製造・販売停止、廃棄、169万余の損害賠償
原審	東京地方裁判所立川支部平成26年（ワ）第1519号
公開URL	http://www.courts.go.jp/app/files/hanrei_jp/601/087601_hanrei.pdf
裁判要旨	<p>RF切替器に関して、回路図データ、部品リストデータ、基板データ、ソフトウェアのソースコードの不正開示を受けて取得し、取得した営業秘密を使用して製品を製造・販売したとされた事案。</p> <p>不競法2条6項所定の営業秘密に当たるか、不競法2条1項8号、10号所定の不正競争行為の成否等が争われた。</p> <p>不競法2条6項営業秘密該当性については、①就業規則を制定し、従業員に秘密保持義務を課していたこと、②前身会社時代にISO27001の要求事項に適合していると認証され、適合性審査を毎年更新しており、ISO規格の内</p>

	<p>部監査員養成セミナーを受けたシステム管理責任者らにより、従業員に対し、一般情報セキュリティ教育を行っていたこと、③資産台帳上、機器制御ソフトウェア、部品リストデータ、基板データ、回路図データは、公開レベル「秘密」と区分されていること、④被控訴人の社内ファイルサーバ内のデータのうち、アクセスを制限するものは、「会社資料S」、「仕様書原本S」、「開発技術S」、「栄幸電子S」、「営業部S」の5つのフォルダに分けられ、それぞれアクセスできる従業員を限定した上で、個々の従業員が特定の端末から、ユーザー名とパスワードを入力しなければアクセスできないように管理されていたこと、⑤原告部品リストデータは「栄幸電子S」フォルダに保管され、原告PCソースコードや原告マイコンソースコード、原告回路図データ、原告基板データは、「開発技術S」に保管されていたことから、従業員において秘密情報であると認識していたものであるとともに、秘密として管理していることを十分に認識し得る措置が講じられていたと認められるから、秘密管理性が認められるとされた。</p> <p>不正競争行為の成否についても、営業秘密である原告PCソースコードを、秘密保持義務に違反して不正に開示していることにつき、重大な過失により認識しないで営業秘密を取得した上、当該営業秘密を用いて被告PCソフトを作成した事実を認定することができることとされた。</p>
--	---

イ) 高級婦人靴（不正競争行為差止等請求、請求異議事件）

表 35 裁判例調査結果（その15）

事件番号	平26（ワ）1397号・平27（ワ）34879号
裁判年月日	平成29年2月9日
裁判所名	東京地裁判決
結果	第1事件一部認容、第2事件請求棄却
原審	—
公開URL	
裁判要旨	<p>原告と被告三國は、平成14年4月頃、継続的な婦人靴の製造委託契約（以下「本件製造委託契約」という。）を締結。小売価格は3万3000円程。被告三國は、原告から、本件製造委託契約に基づき、上記取引のために、原告の設計する高級婦人革靴のマスター木型（全ての木型の原型となる木彫りの木型。原告が企画開発する靴のマスター木型については、株式会社中田靴木型製作所</p>

	<p>〔以下「中田靴木型」という。〕が製作して保管していた。)に基づいて作成された本件オリジナル木型を預かっていた。被告A i は、本件オリジナル木型を被告三國の社外に持ち出し、これらを被告A iiiと共にハマノ木型に持ち込んで複製させることにより、本件複製木型を作成した。さらに、被告A iiiは、ハマノ木型に本件複製木型を改造させることにより、本件改造木型を作成した。</p> <p>被告三國は、原告に対し、本件製造委託契約に基づく個別取引による委託報酬等の支払を請求する別件訴訟を提起。原告は、損害賠償請求権等と相殺する意思表示をした。別件判決は、原告に被告三國に対し689万2144円及びこれに対する平成25年10月25日から支払済みまで年6分の割合による金員を支払うことを命ずるものであったが、本件相殺1の自働債権については、被告三國が原告に無断で被告A iiiに対して本件オリジナル木型を貸与しこれを不正に複製したことが、本件製造委託契約上の善管注意義務に違反すると判断し、この債務不履行に基づく合計112万3994円の損害賠償請求権を認め、それについて相殺の効果を認めた。</p> <p>本件訴訟では営業秘密性、不正行為該当性が一部認められた。すなわち、原告の①被告たくみ屋らに対する不競法3条1項に基づく本件複製木型及び本件改造木型の使用及び開示の差止請求、②被告A iiiに対する本件返却合意に基づく本件複製木型及び本件改造木型の引渡請求、③被告A iiiに対する債務不履行に基づく損害賠償請求として363万5640円及び遅延損害金の支払請求は理由があるとされた。</p>
--	---

ウ) 顧客への書簡送付 (損害賠償請求事件)

表 36 裁判例調査結果 (その16)

事件番号	平27(ワ)17716号
裁判年月日	平成29年1月26日
裁判所名	東京地裁判決
結果	一部認容
原審	—
公開URL	
裁判要旨	本件は、原告が、原告の元取締役である被告A及び被告B、後記本件財産処分行為の相手方等である被告並びに同被告らの各代表者である被告C及び被告Dに対し、被告Aによる原告の財産の処分等並びに被告による原告の顧客名簿の不

	<p>正使用及び書簡送付等が取締役の任務懈怠ないし不法行為、不正競争防止法2条1項7号、15号等所定の不正競争等に当たり、これにより9892万0867円の損害を被ったと主張して、①被告A及び被告Bに対し、会社法423条1項、430条に基づき、上記損害金及び遅延損害金の連帯支払、②被告A、被告、被告C及び被告Dに対し、民法709条、719条1項等に基づき、上記損害金及び遅延損害金の連帯支払（被告Aに対しては上記①と選択的請求）を求める訴訟である。</p> <p>原告の商標の使用許諾を受けた被告が、原告の顧客である幼稚園・保育園及び能力開発教室の会員である生徒の保護者らに対し、次の各書簡を送付した。</p> <p>① 平成24年6月吉日付け、幼稚園・保育園の理事長・園長宛の「〇〇式漢字教育は、原告に代わり、6月25日より被告が行うことになった。同被告に移行しても従前どおり絵本の配本や研修会、能力開発教室（恵比寿）、各園の課外教室の開催など、社員・講師も引き続き担当する。」旨の書簡</p> <p>② 同月吉日付け、会員・保護者宛の「原告に代わって、6月25日より被告ハートウィングが行うことになった。同被告が新しい教室の委託先になったことに伴い、授業料振込先も新しくなる。」旨の書簡</p> <p>③ 同年7月12日付け、幼稚園・保育園宛の「7月より被告との取引となった。」旨の書簡</p> <p>④ 同月吉日付け、幼稚園・保育園宛の「被告と会社が変わったので、振込先も変わった。」旨の書簡</p> <p>⑤ 同年9月11日付け、原告の旧教室の生徒の保護者宛の「ご子息が6月まで通っていた教室は、名称を改め、授業を再開した。」旨の書簡</p> <p>被告Aは平成16年頃から原告の代表取締役を務めていたが、原告は恒常的に資金不足の状態にあり、被告Aは、被告Aが代表取締役を退任する際に弁済するとの約定で、原告に対し合計数千万円に及ぶ貸付けをしていた。被告Aは、株主間の対立関係に鑑み、代表取締役を退任することは避けられないと判断した。また、原告の財務状況に照らし、貸付金（被告Aの計算では当時の残高は約2000万円であった。）の弁済を受けることは困難であると考えた。そこで、被告Aは、原告の保有する絵本等を被告に売却して弁済資金を調達すること、被告Aの退任後は被告に能力開発教室を運営させることを企図。</p> <p>原告は顧客名簿を作成し、電磁データの形で保存し、管理していた。このパソコンを起動するためにはパスワードが必要であったが、本件顧客名簿のデータにはパスワードの設定はなかった。そのため、営業秘密該当性が否定された。</p>
--	--

	<p>他方で、〇〇式国語教育に関する事業主体が原告から被告に変更されたとみることとはできず、本件書簡に記載された事実は虚偽であると解すべきである。そして、本件各書簡は、原告の顧客に対して被告との取引を勧誘するものであり、これが原告の営業上の信用を害することは明らかと解される。そうすると、本件各書簡を送付した者が原告と競争関係にあると認められれば、その送付行為は15号の不正競争に当たると判断すべきものとなる。</p> <p>以上によれば、原告は本件財産処分行為により合計498万2795円、本件書簡送付行為により100万円の損害を被ったと認められるので、被告Aは498万2795円、被告はこれらに弁護士費用を加えた658万2795円、被告Cは598万2795円の各損害金及び遅延損害金を原告に対し賠償すべきものであり、これらは同一の損害の賠償を目的とするものであるから、金額が重複する限度でいわゆる不真正連帯債務の関係となる。</p>
--	--

エ) 顧客別の売上情報（不正競争行為差止等請求事件）

表 37 裁判例調査結果（その17）

事件番号	平25（ワ）12149号
裁判年月日	平成28年6月23日
裁判所名	大阪地裁判決
結果	一部認容
原審	—
公開 URL	
裁判要旨	<p>臨床検査会社である原告は、原告を退職した幹部従業員であった被告P1が、不正の利益を得る目的又は原告に損害を加える目的で原告から開示を受けた営業秘密の本件情報を就職した競業会社である被告会社に開示し、使用した行為、並びに被告会社が被告P1の不正開示行為を知りながら本件情報を取得し、使用した行為は不正競争行為に該当するなどとして、被告らに対し、本件情報の使用の差止め及び同情報の保存された媒体等の廃棄、並びに損害賠償の連帯支払を求めるとともに、被告P1に対し、それらの行為が就業規則上の懲戒解雇事由に該当することを理由に退職一時金434万7000円の返還を求めた事案。</p> <p>本件情報、すなわち顧客別の売上情報及び顧客別の平均販売価率情報は、従業員しか閲覧することのできない社内ネットで管理されており、閲覧できる範囲についても従業員の所属部署、地位に応じて定められていて、従業員においてもそ</p>

<p>のような情報保護の規程があることを認識することができた状況にあったといえるとして、秘密管理性、そして営業秘密該当性が認められた。</p> <p>被告P 1は、原告から営業秘密である本件情報を含む情報の開示を受けた者であるが、これを利用して作成された「親密度ファイル」を用いて、同時期に原告から被告会社に転職する予定の者らと被告会社転職後の原告顧客に対する営業活動について協議し、その結果を「KM売上計画2012」にまとめ、そこには新たに臨床検査の委託を受ける際の諸条件のみならず原告との関係における売上実績が記載されていたものである。そして、被告P 1ら転職者は、被告会社転職後、原告の顧客を主たる対象として営業活動をしていたものであるが、医療機関に対する営業開始後直ちに見積書を当該医療機関に提示した場合もあり、通常割合以上に原告から被告会社に対して臨床検査の委託先を変更した顧客があり、その顧客の多くは被告P 1ら転職者が「KM売上計画2012」において被告会社との取引を、取引開始月まで見込んでいた医療機関であることからすると、本件情報の有用性も併せ考えれば、原告顧客に対する営業活動をするに当たり、被告P 1は、その余の転職者らとともに「親密度ファイル」又は「KM売上計画2012」を媒介にして本件情報を使用していた、すなわち、被告会社転職後にその余の転職者らとともに本件情報を被告会社に開示し、使用したと推認する方が自然であり、また合理的である。また、そのような原告との競業のための被告会社に対する開示、使用である以上、これが不正の利益を得、あるいは保有者である原告を害する目的でなされたことも容易に認定できるところである。</p> <p>被告P 1は、原告から示された営業秘密である本件情報を、図利加害目的で被告会社に開示し、使用したと認められるから、上記行為は不正競争防止法2条1項7号に該当する不正競争であるというべきである。被告P 1のみならず、その余の原告からの転職者も被告会社において、本件情報を使用して営業をしていたものと認められるから、被告P 1ら転職者が被告会社従業員としてした原告顧客に対する営業活動により、被告会社は、図利加害目的で開示された営業秘密であることを知って本件情報を取得して使用していたものということになり、この行為は不競法2条1項8号の不正競争に該当するというべきである。</p> <p>不競法3条に基づき、原告の被告らに対する本件情報の使用及び第三者への開示の差止め、並びに本件情報が記載された文書及び電磁的記録媒体の廃棄請求にはいずれも理由がある（ただし、本件情報と社会的同一性のある範囲を超えて、外延が無限定となりかねない本件情報から「生成された情報」についての廃</p>

	<p>棄請求は、侵害の予防に必要な行為としても認めることはできない。なお、無形の情報である本件情報の廃棄である以上、その廃棄は、本件情報が記載された文書及び電磁的記録媒体廃棄が第三者による使用が全く許されない形でされるべきことはいうまでもない。)</p> <p>なお、損害賠償額については、請求額から大幅に減額された。</p>
--	---

オ) 下請けからの一方的な業務打ち切り (損害賠償等請求事件)

表 38 裁判例調査結果 (その18)

事件番号	平26(ワ)3822号・平26(ワ)7205号・平26(ワ)27009号・平27(ワ)1901号
裁判年月日	平成28年6月2日
裁判所名	東京地裁判決
結果	一部認容
原審	—
公開 URL	
裁判要旨	<p>甲事件は、原告会社との間で業務委託契約を締結してその下請業務を遂行していた被告会社が、正当な理由なく上記契約を解約して一方的に業務の受託を打ち切り、原告会社の得意先との取引関係を奪取し、これにより原告会社の業務遂行が不可能となったとして、原告会社が、被告会社に対して、主位的には業務委託契約の債務不履行に基づいて、予備的には不法行為に基づいて、原告会社の被った損害の賠償を求めるものである。これに対し、乙事件は、被告会社が、原告会社に対して、業務委託契約に基づいて業務委託料の支払を求めるものであるが、原告会社は、甲事件請求に係る損害賠償債権を反対債権として対当額にて相殺したことで業務委託料債権は消滅しているとして争っている。</p> <p>また、丙本訴事件は、原告会社が、原告会社の元従業員であった被告Y2及び被告Y3に対して、上記両名が被告会社の専務取締役と共謀して、原告会社の得意先奪取行為に加担したことが共同不法行為となるとして、甲事件で請求する損害のうち一部の損害の賠償を求めるものであるところ、これに対する反訴が丙反訴事件であり、被告Y3が、原告会社による上記訴訟提起は、被告Y3に対する不当訴訟であるとして、慰謝料及び弁護士費用の支払を求めている。</p> <p>原告会社は、アパレルメーカー、卸問屋、商社等のベンダー等が各量販店に配送する商品の入出荷、加工、検品、梱包、保管、配送の手続等を行う物流加工代行</p>

業者たる株式会社である。被告会社は、衣料品、雑貨物等の入出荷、加工、検品、梱包、保管、配送手続等を行う物流加工代行業者たる株式会社である。被告 Y2, Y3 は原告会社元従業員である。

原告会社の物流事業においては、得意先ないしアパレル量販店からの発注に対し、オンラインで即時に対応し入出荷が行えるようにするため、入出荷連絡・入出荷予測、商品在庫状況、配送状況等を管理するシステム（以下「本件システム」という。）を設置し、顧客データ等を蓄積し、被告会社従業員も本件システムを共同利用する形で、作業の効率化を図るとともにコスト削減を実現していた。原告会社は、本件業務委託契約により、受託した物流業務のほぼ全てについて被告会社に業務委託していた。

原告会社は、a 社から当時 a 社にて使用されていたシステム（以下「旧システム」という。）を承継した後、旧システムの維持管理・保守だけではなく、システムのカスタマイズや開発に向けた投資を行い、その成果を原告会社の業務に取り込んでいた事実が認められる。また、被告会社も、被告会社が a 社と業務委託契約を締結していた段階で運用していた旧システムと比べると、本件システムについては、システム附属部分の改良がなされていることは認めている。そうすると、本件システム（具体的に何をどの範囲で含むのかについて、原告会社の主張は必ずしも明らかではないが、その点はしばらくおく。）について原告会社が所有権を有するといえるかはともかく、本件システムや、その中で蓄積された各種データの利用権が原告会社にあることは間違いないのであり、これらを原告会社の意思に反して持ち去ったり、消去したりすることは、その利用権を侵害することとなるので許されない。仮に、被告会社との共同利用が認められたものと評価できるとしても同様である。

次に、被告らの違法行為（原告得意先奪取行為）について。本件業務委託契約は、書面によらない契約合意であり、締結された契約の性質を検討すると、物流加工代行業を営む会社間の業務委託であり、商品の入荷、在庫管理、配送等を組織的効率的に実施して、利用企業の要請に応えることが求められるため、継続的な業務遂行が要求されるものである。そうであれば、解約事由としては、契約当事者間の信頼関係が維持できず、契約関係を解消してもやむを得ない事情が必要となると解される。加えて、解約手続面について検討すると、契約関係を終了させるに際して相手方に不測の損害を発生させないように配慮すべきであるから、一方的な解約通知をもって解約を認めるには、そうすることがやむを得ない重大な事情の存在が求められると解すべきであるが、本件通知解約には、解約につ

	<p>いての正当事由が認められないことになる。加えて、本件解約通知は、業務受託会社として被告会社が問題と捉える課題を解決するための具体的な交渉の呼びかけすらせずに、突然一方的に解約を通知したものであり、手続的にも正当性が認め難い。そして、本件解約通知により1か月後に解約すると一方的に通告され、その間に年末年始を挟む上に、事前の対応準備を欠いていた原告会社としては、その業務遂行を妨げられたものと認められる。</p> <p>そうであれば、被告会社は、本件業務委託契約を、正当事由なく一方的に解約したものであり、加えて、本件解約通知がなされた以降においても原告会社との交渉を実質的に拒絶していたのであるから、原告会社に対する契約関係の誠実履行義務に違反したものとして債務不履行責任を負うことになる。</p> <p>その他、原告従業者の一斉退社への関与、原告得意先業務に関する資料の持ち寄り・データの消去等が認められた。</p> <p>被告会社は、原告会社に対し、1239万6322円及び遅延損害金を、被告Y2及び被告Y3は、原告会社に対し、連帯して5000万円及び遅延損害金を支払うよう判決が下された。</p>
--	--

カ) 営業秘密性の否定（請負代金請求事件）

表 39 裁判例調査結果（その19）

事件番号	平25（ワ）3058号
裁判年月日	平成26年10月23日
裁判所名	大阪地裁判決
結果	請求認容
原審	—
公開 URL	
裁判要旨	<p>原告が被告に対し、サイト構築作業の請負契約に基づく代金の支払を求めたところ、被告は、請負契約の成立及び請負作業の完成の事実を争い、仮に被告の支払義務が存するとしても、不正競争防止法違反に基づく損害賠償請求権を自働債権として、対当額で相殺する旨の抗弁を主張した事案において、請求原因事実はすべて認められ、かつ、被告が主張する各情報は営業秘密と認められないから、被告の相殺の抗弁は理由がないとして、請求を認容した事例。</p> <p>原告は、ホームページ及びインターネットシステムの企画、研究、開発、制作、デザイン及び保守管理業務等を目的とする株式会社である。被告は、販売促進に</p>

	<p>関する宣伝用ツールの作成及び販売等を目的とする株式会社である。原告と被告は、平成24年2月ころ、被告が日本事務器から受注した本件業務を、原告が代金約560万円（見積書の記載は557万5500円）で請け負う契約を締結した（以下「本件請負契約」という。）。</p> <p>被告は、①文書アップロード、②文書自動変換、③文書保管・運用、④本棚・書類一覧、⑤デジタルビューワー方式の全てを1つのシステムとする、デジタルブック提供システムという発想そのものが営業秘密である旨主張したが、従来から他社が提供していたデジタルブック提供サービスと異なる有用性を基礎付ける事実を認めるに足りる証拠はないとされた。</p> <p>また被告が主張する外注先情報は、〇〇という企業が存在し、外注先として被告と取引していたという単純な事実を過ぎず、役員及び従業員において、秘密として保持しなければならない有用な技術上又は営業上の情報とは認められず、外注先情報が営業秘密にあたるということとはできないとされた。さらに被告が主張する顧客情報も、〇〇という企業が存在し、被告の得意先であったという単純な事実を過ぎず、役員及び従業員において、秘密として保持しなければならない有用な技術上又は営業上の情報とは認められず、顧客情報が営業秘密にあたるということとはできない不正競争防止法違反に基づく損害賠償請求権を自働債権として、対当額で相殺する旨の抗弁は認められなかった。</p>
--	--

キ) 業務移管の際の顧客情報の流出取得（損害賠償請求事件）

表 40 裁判例調査結果（その20）

事件番号	平23（ワ）22277号
裁判年月日	平成25年10月17日
裁判所名	東京地裁判決
結果	一部認容
原審	—
公開 URL	
裁判要旨	原告が、仕入先であった被告Y1の完全子会社である被告Y2に顧客対応業務を移管した際、被告Y1、被告A及び被告Bが共同して、不正の手段により当該顧客情報を取得し、被告Y2で使用して、これにより損害を被ったなどと主張して、被告らに対し、不正競争防止法4条、民法719条及び被告Y2について会社法350条に基づき、損害金合計1億2035万2200円及び遅延損害金

の連帯支払を求めた事案において、本件顧客情報は、営業秘密に当たるといふべきであり、また、被告A及び同Bは、共同して、E1が不正の手段により本件顧客情報を取得したことを知って、又は重大な過失により知らないで、本件顧客情報を取得し、若しくは使用したものとすべきであるなどとして、原告の被告Y2、被告A及び被告Bに対する請求の一部を認容した事例。

原告は、レジスター、計算機の製造及び販売等を業とする会社の販売会社として設立され、平成3年2月1日、同社を吸収合併した被告Y1の間で、売買取引契約を締結し、以来、被告Y1の製品を継続的に仕入れて販売していた。原告は、販売先の名称、住所、連絡先、販売した時期や製品、価格、リース期間及び契約番号等から構成される顧客情報（以下「本件顧客情報」という。）を本社3階にある管理部の専用パソコン1台（以下「顧客管理パソコン」という。）に集約して、パスワードにより管理していた。顧客管理パソコンのアクセス権者は、パスワードを知っている管理部所属の従業員4名だけであり、その他の従業員が本件顧客情報を必要とする場合には、所属先の長が管理部に書面で申請して、必要な情報のみを記録したCD等の記憶媒体の送付を受け、受領した旨の返信をする必要があった。原告は、被告Y2に対し修理や交換等の顧客対応業務を移管して（以下、この移管を「本件移管」という。）、営業活動を停止し、被告Y2に対し、工具や電光表示器変更パソコン等を引き渡した。

本件顧客情報は、平成22年3月当時、2万6378件の販売情報から構成されていたこと、顧客管理パソコンが置かれた原告の本社3階の管理部は、業務時間外には、本社1階と管理部の各出入口に取り付けられた錠と警備装置により、錠を開く各鍵と警備を解除するカードキーとを所持する役員及び管理部所属の正社員3名以外の立入りが制限され、業務時間内にも、常に管理部所属の従業員4名のうちの誰かが管理部か奥の役員室にいることにより、役員、管理部所属の従業員及びこれらの者に入室を認められた者以外の立入りが制限されていたこと、原告は、本件規定や本件就業規則で個人情報を含む本件顧客情報の守秘義務を従業員に課し、業務通達や社内研修で周知に努め、例えば管理部が営業のために営業部等に本件顧客情報を送付した場合には、送付先の長が個人情報管理責任者としてその責任の下に管理していたことが認められるなどとして、営業秘密性が認められた。

被告Bは、原告がいまだ顧客に対し顧客対応業務を被告Y2に移管する旨を通知していないことを知って、原告に代わり、通知書の文案を作成した。E1は、被告Bから通知書の文案を受け取り、顧客管理パソコンを用いて過去6年間

に取引があった顧客7529名の宛名印刷を始めたが、発送予定日に間に合わないおそれがあったので、元部下のE2に全ての本件顧客情報を顧客管理パソコンから処理の速い電光表示器変更パソコンにエクセルファイルの形式で複製させ、電光表示器変更パソコンをも用いて宛名印刷を行わせるなどして、本件通知書を発送した。Cは、平成22年3月27日ころ、原告内で行われた打合せにおいて、本件移管に伴って被告Y2に引き渡すべき物を協議し、工具等の引渡しに加え、E1等の提案により、電光表示器変更パソコンを引き渡すことを認めたが、この中に本件顧客情報が入っていることを知らず、E1もそのことに言及しなかった。E1は、平成22年3月31日、E2に全ての本件顧客情報を顧客管理パソコンから記憶媒体にアクセスファイルの形式で複製させて取得した。被告Y2は、平成22年4月の本件移管後、E1から本件顧客情報の開示を受け、本件顧客情報を顧客対応業務に使用したが、本件顧客情報以外の情報や原告の対応が必要になると、「サービスカード」という照会用紙に販売先の名称や連絡先、販売した製品、用件等を記載して、これを原告に送付し、原告に回答してもらったり対応してもらっていた。Cは、E1とE2が送付したサービスカードに契約番号など本件顧客情報を使用しなければ記載することができない情報が記載されていることに気付き、E1に電話を掛け、本件顧客情報を使用していないか問いただした。これに対し、E1は、初め使用していないと答えたが、後に使用していると認めた上で、被告Bに相談し、以後、サービスカードに契約番号など本件顧客情報を使用しなければ記載することができない情報を記載しなくなった。

前記認定の事実によれば、E1は、E2に全ての本件顧客情報を顧客管理パソコンから記憶媒体に複製させてこれを取得し、電光表示器変更パソコンの中に本件顧客情報が入っていることを知りながら、上記パソコンを原告から被告Y2に引き渡させて本件顧客情報を取得したのであるから、不正の手段により本件顧客情報を取得したといえることができる。

そして、原告のような販売会社における顧客情報は、通常、販売に役立つ営業上の秘密情報として管理されていることが多く、のれんの一部を構成するものであり、被告Aは、平成21年5月以降、Cとの間で、のれんを含めた原告の事業や資産等を被告Y2で譲り受けるための交渉を断続的に行い、被告Bも、平成22年3月以降、被告Y2による顧客対応業務の引受けに係る作業に従事していたところ、E1から開示された本件顧客情報は被告Y2が引き受けた顧客対応業務において有用なものであったにもかかわらず、本件移管において、原告が被

	<p>告 Y 2 に対し本件顧客情報を明示して開示する手続をしていないのであるから、被告 A と同 B は、本件顧客情報が原告の営業秘密に当たるものであり、E 1 が不正の手段によりこれを取得したことを知って、又は重大な過失により知らないうちに、E 1 から本件顧客情報の開示を受けたと認められる。なお、被告 A や同 B が E 1 から本件顧客情報の開示を受けたときに本件顧客情報が原告の営業秘密に当たることや E 1 が不正の手段によりこれを取得したことを重大な過失によることなく知らなかったとしても、被告 Y 2 で本件顧客情報が使用されていることについて、被告 A は C から問いただされ、また、被告 B は E 1 から相談を受けて、いずれも、本件顧客情報が原告の営業秘密に当たるものであり、E 1 が不正の手段で本件顧客情報を取得したことを知って、又は重大な過失により知らないうちに、本件顧客情報を使用したと認められる。</p> <p>したがって、被告 A 及び同 B は、上記不正競争によって生じた原告の損害を賠償する責任を負う。また、被告 A の上記不正競争は、被告 Y 2 の職務を行うについてされたことが明らかであるから、被告 Y 2 も、原告の損害を賠償する責任を負うとして、被告 Y 2、同 A 及び同 B は、原告に対し、連帯して 5 2 9 6 万 6 1 0 0 円及び遅延損害金を支払うよう判決が下された。</p>
--	---

ク) CAD ソフトのアクティベーション機能回避プログラム提供 (損害賠償請求事件)

表 41 裁判例調査結果 (その 21)

事件番号	平 2 9 (ワ) 3 1 8 3 7 号
裁判年月日	平成 30 年 1 月 30 日
裁判所名	東京地裁判決
結果	一部認容
原審	—
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/479/087479_hanrei.pdf
裁判要旨	<p>原告が、「建築 CAD ソフトウェア「DRA-CAD11」(以下「本件ソフトウェア」という。)について著作権及び著作者人格権を有し、また「DRA-CAD」との文字からなる商標に係る商標権を有しているところ、被告は、ヤフオクにおいて本件商品を入札して代金を被告に支払った顧客に対し、本件ソフトウェア及び B のプログラムのクラック版(いずれも原告の許諾がないもの)が蔵置されていたオンラインストレージサイト「C」の URL をダウンロード先として教示し、かつ当該 B のプログラムのクラック版の起動方</p>

	<p>法及び本件ソフトウェアの起動・実行方法を教示するマニュアル書面を提供していた。当該顧客は、上記ダウンロード先から本件ソフトウェア（無許諾品）及びセットアップCDの内容とクラックされたBVer. 11. 0. 1. 3を入手することができ、セットアップを行った後、クラック版のBを上書きすると、本件ソフトウェアで要求されるアクティベーション機能（正規品のシリアルナンバー等を入力しないとプログラムが起動・実行されないようにする機能をいう。）を回避することができた。かかる被告の行為は、原告の上記著作権（複製権、翻案権、譲渡権）及び著作者人格権（同一性保持権）を侵害するとともに、原告の上記商標権を侵害し、さらに平成27年法律第54号による改正前の不正競争防止法2条1項11号（現12号）所定の不正競争行為に該当する」と主張し、被告は、商標権侵害の事実を認めるが、著作権侵害及び不正競争防止法違反の各事実及び原告の損害額を争った事案。</p> <p>被告は、本件ソフトウェアの一部に原告の許諾なく改変（アクティベーション機能の回避）を加え（本件ソフトウェアの表現上の本質的な特徴の同一性を維持しつつ、具体的表現に修正、変更等を加えて新たな創作的表現を付加し）、同改変後のものをダウンロード販売したものと評価できるから、被告は、原告の著作権（翻案権及び公衆送信権）並びに著作者人格権（同一性保持権）を侵害したものと評価すべきであり、これに反する被告の主張は採用できない。なお、原告は、譲渡権侵害を主張しているが、有体物の譲渡ではなくソフトウェアのダウンロードが行われたものとして、公衆送信権が侵害されたものと解すべきである。</p> <p>また被告は、原告が営業上用いている技術的制限手段（アクティベーション）により制限されているプログラム（本件ソフトウェア）の実行を、当該技術的制限手段の効果を妨げることにより可能とする機能を有するプログラム（Bのクラック版）を、電気通信回線（インターネット回線）を通じて提供したものと評価できるから、被告は旧11号（現12号）所定の不正競争行為を行ったものと認められる。</p>
--	--

ケ) アプリケーションのプロダクトキー（損害賠償請求事件）

表 42 裁判例調査結果（その22）

事件番号	平27（ワ）36号
------	-----------

裁判年月日	平成 29 年 8 月 10 日
裁判所名	長野地裁
結果	一部認容
控訴審	知財高裁判決平成 30 年 3 月 29 日平 29 (ネ) 10082号・平 30 (ネ) 10005号があるが、控訴棄却であるため、原審を掲載する。 http://www.courts.go.jp/app/files/hanrei_jp/651/087651_hanrei.pdf
公開 URL	
裁判要旨	<p>被告は、「マイクロソフト」という標章（以下「被告標章」という。）を用いて、原告が著作権を有する OS 又はアプリケーションプログラムのソフトウェア製品（以下、まとめて「原告製品」という。）のプロダクトキー（プログラムを、コンピュータにインストールするに際し、入力求められるシリアルデータで、ユーザーが原告からライセンスの認証を受けるために必要なもの）（以下、被告が販売したプロダクトキーを、まとめて「被告商品」という。）を、販売するとの内容を被告ウェブサイトに掲載の上、購入者から商品代金の入金を確認した後、購入者に対して被告商品を提供した。これが原告商標権を侵害するとして、原告から、被告に対し、商標権侵害の不法行為による損害賠償請求権（商標法 38 条 1 項又は民法 709 条）に基づき、逸失利益 2 億 7 1 3 0 万 2 0 3 3 円及び弁護士費用 7 3 1 万円の一部請求として、2 7 0 0 万円及び遅延損害金の支払を求めた事案である。</p> <p>・争点 1（原告商標と被告標章の類否）について</p> <p>商標の類否は、対比される商標が同一又は類似の商品又は役務に使用された場合に、その商品又は役務の出所につき誤認混同を生ずるおそれがあるか否かによって決すべきである。</p> <p>原告商標と被告標章とを対比すると、いずれも同一の称呼及び観念を有するものであり、外観においても、文字のフォントに違いがあるものの、いずれも横書きで同じ語で構成されている。原告商標と被告標章が、原告製品又は原告製品のプロダクトキーという商品に使用された場合には、取引者・需要者において、その商品の出所について誤認混同を生ずるおそれがあると認められる。</p> <p>したがって、被告標章は、原告商標と社会通念上同一であるか、少なくとも類似するというべきである。</p> <p>・争点 2（原告商標の指定商品と被告商品の類否）について</p>

	<p>商標法上の「商品」には、無体物も含まれると解され、商標法施行規則別表第9類十五は「電子応用機械器具及びその部品」として「電子計算機用プログラム」を挙げているが、当該規定は例示であって、それ以外の無体物を含む部品を除外するものではない。</p> <p>そしてプロダクトキーは、原告製品をコンピュータ記憶装置内に物理的にインストールするために必要なものである上、原告製品として制限のないプログラムの使用を可能とするライセンス認証を得るために不可欠な情報鍵である。そうすると、プロダクトキーは、「電子応用機械器具」（「電子計算機用プログラム」）に相当する原告製品をコンピュータで利用するために必要不可欠な部品であり、電子応用機械器具の部品に該当する。</p> <p>したがって、原告商標の指定商品である「電子応用機械器具及びその部品」には、原告が著作権を有するOS又はアプリケーションプログラムのソフトウェア製品である原告製品のみならず、プロダクトキーが含まれるというべきであるから、被告商品は、原告商標の指定商品と同一のものといえることができる。</p> <p>・争点3（被告標章の使用が商標法2条3項8号又は同項2号に該当するか否か）について</p> <p>(1) 商標法2条3項8号該当性</p> <p>被告は、被告ウェブサイトにおいて、被告標章を用いて、被告商品を販売するとの内容を掲載し、顧客から購入申込みを受け、購入者から商品代金の入金を確認した後、購入者に対して被告商品を提供していたところ、被告の上記掲載行為は、「商品に関する広告を内容とする情報に原告商標と同一又は類似する被告標章を付して電磁的方法により提供する行為」といえることができるから、商標法2条3項8号の「使用」に該当する。</p> <p>(2) 商標法2条3項2号該当性</p> <p>被告が、被告ウェブサイトにおいて、被告標章を用いて、被告商品を販売するとの内容を掲載した行為は、有体物である商品のラベルやタグに標章を付する行為と同様とは認められず、商標法2条3項2号の「使用」に該当するとはされなかった。</p> <p>4 争点4（被告標章の使用は商標的使用に該当するか否か又は商標法26条1項6号に該当するか否か）について</p> <p>被告ウェブサイトの「マイクロソフトのプロダクトキーを扱っております。」等の記載に接した取引者・需要者は、被告商品が、原告が著作権を</p>
--	---

	<p>有する原告製品のプロダクトキーであって、被告商品の出所が原告であると理解するのが通常であり、単に被告商品の内容の説明や被告商品の適合関係を示すために被告標章が使用されていると理解するものではないとの理由から、被告標章の使用は商標的使用に該当し、商標法26条1項6号の「需要者が何人かの業務に係る商品又は役務であることを認識することができる態様により使用されていない商標」に該当するものではないと判断された。</p> <p>・争点5（被告標章の使用は商標法26条1項2号に該当するか否か）について</p> <p>被告ウェブサイトの「マイクロソフトのプロダクトキーを扱っております。」等の記載に接した取引者・需要者は、原告が著作権を有する原告製品のプロダクトキーを購入することができるかと理解するのが通常であって、これを、被告商品であるプロダクトキーが、その出所を原告とするものであるか否かにかかわらず、原告製品の用途に使用されるものであると理解するということはできないとされた。</p> <p>・争点6（被告商品の販売は真正商品の販売として実質的違法性を欠くか否か）について</p> <p>被告が、マニアが集めてインターネット上に掲載している適当なプロダクトキーを拾ってきて、これを被告商品として、これに関する広告を内容とする情報に原告商標と同一又は少なくとも類似する被告標章を付して電磁的方法により提供することは、当該プロダクトキーが真正商品ではない以上、原告商標権の出所表示機能及び品質保証機能を害し、実質的違法性を有することは明らかである。これらプロダクトキーが真正商品である証拠はないとされた。</p> <p>また、被告がT e c h N e t等によって発行を受けたプロダクトキーをいわば小分けをして被告商品として、これに関する広告を内容とする情報に被告標章を付して電磁的方法により提供することも、実質的違法性を欠くものということとはできないとされた。</p>
--	--

コ) アプリケーション製品不正ダウンロード（損害賠償請求事件）

表 43 裁判例調査結果（その23）

事件番号	平28（ワ）10425号
------	--------------

裁判年月日	平成 28 年 12 月 26 日
裁判所名	大阪地裁判決
結果	全部認容
原審	—
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/665/086665_hanrei.pdf
裁判要旨	インターネットオークションの落札者に、原告プログラムに付された技術的制限手段の効果を妨げる機能を有する被告プログラムを、電気通信回線を通じて提供した行為が不正競争防止法の禁止する不正競争に該当するとし、原告の損害額につき、原告は、被告プログラムの販売数量(ダウンロード数)に相当する数量の原告製品を販売する機会を失ったと認められた事案。

サ) カラオケ（損害賠償請求事件）

表 44 裁判例調査結果（その 24）

事件番号	平 2 6 (ワ) 2 7 6 1 7 号
裁判年月日	平成 27 年 10 月 15 日
裁判所名	東京地裁判決
結果	一部認容
原審	—
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/384/085384_hanrei.pdf
裁判要旨	<p>本件は、原告が、被告らに対し、原告が販売したカラオケ機器を被告らが改造して販売した行為が不正競争防止法（平成 27 年法律第 54 号による改正前のもの。以下同じ。）2 条 1 項 11 号（現 12 号）所定の不正競争及び商標権侵害に当たり、被告らは共同不法行為責任を負うと主張した事案である。</p> <p>被告会社はコンピュータ部品や周辺機器、テレビチューナーの販売等を営む株式会社であり、被告 A はその代表者、被告 B 及び被告 C は、被告会社の事務所内のスペースの提供を受け、業務を行っていた者である。被告 B は、原告が販売した正規品である DAM 端末の基盤等に演奏ロック機能を妨げる改造を行った。被告 A 及び被告 C は、インターネットオークションサイトを利用して、この改造された DAM 端末を複数販売した。被告らは、DAM シリーズの演奏ロック機能が不正競争防止法 2 条 7 項所定の</p>

	<p>「技術的制限手段」に当たること、被告商品の販売行為が同条1項11号（現12号）所定の不正競争及び本件商標権の侵害行為に当たるとを争っていない。争点は、(1)被告らによる共同不法行為の成否、(2)損害の有無及びその額（改造して販売した被告商品の台数、被告らの利益額等）であったが、共同不法行為の成立が認められ、被告会社、被告A及び被告Bに対し13万7848円及び遅延損害金の連帯支払、被告らに対し226万4646円及び遅延損害金の連帯支払が認められた。</p> <p>類似裁判例として、東京地判平成27年9月30日（事件番号平26（ワ）24118号）もある。</p>
--	---

シ) 米国人であるブログ管理者の削除義務（損害賠償請求事件）

表 45 裁判例調査結果（その25）

事件番号	平24（ワ）29003号
裁判年月日	平成28年6月20日
裁判所名	東京地裁判決
結果	棄却
原審	—
公開 URL	
裁判要旨	<p>イギリス領バージン諸島の法律に準拠して設立され、同地に登記上の主たる事務所を置く法人である原告X1社及びその代表者で中華人民共和国香港特別行政区に居住している原告X2が、ブログサービス等を提供する米国人である被告に対し、被告が提供するブログサービス上に掲載された原告らの名誉を毀損する表現を削除する義務を怠ったとして、各慰謝料及び原告会社につき同社の営業上の逸失利益等の支払を求めた事案。判決は、裁判管轄は日本の裁判所にあり準拠法は日本法であると認めたとうえで、被告の削除義務を否定した。以下、各論点についての判断を示す。</p> <p>・裁判管轄</p> <p>原告X1社の当事者能力及び本件訴えの国際裁判管轄を認めた。</p> <p>本件記事は、日本語で記載され、その内容も原告X2が販売する商品を日本人が購入する場合の扱いや原告会社に対する金融庁からの警告に関し記載するものであるから、本件記事が日本に居住する日本人の読者を主な対象としていると認めることができる。そうすると、本件記事による原</p>

告らの社会的評価の低下は日本国内で生じているといえるので、本件訴えに係る不法行為による結果の発生した地は日本国内にあり、その不法行為があった地は日本国内にあるといえることができる。

また、被告のウェブサーバは米国にあるが、原告らの社会的評価は本件記事により日本において低下され、かつ、本件記事が日本語で記載され、その内容も日本に関するから、被告において、日本国内における結果の発生が通常予見することのできないものとはいえず、また、日本の裁判所が審理及び裁判することが当事者の衡平を害するということができないので、民事訴訟法3条の9所定の「特別の事情」があったとはいえることができない。したがって、日本の裁判所は、本件訴えについて、管轄権を有する一方、特別の事情により本件訴えを却下すべきということとはできない。

・ 準拠法

原告会社は、ホームページやパンフレットを日本語で表記し、また、東京において日本人の顧客を相手に海外投資のためのセミナーを開催するなどして、日本人に香港における投資商品を紹介することを主たる事業としている。そして、本件記事は、日本語で記載され、その内容も原告X2において販売する商品を日本人が購入する場合の扱いや原告会社に対する金融庁からの警告に関し記載するものであるから、日本に居住する日本人の読者を主な対象としているといえることができる。

原告会社の事業が日本に密接に関連し、原告X2が原告会社の代表者である上、本件記事は原告らの日本における社会的評価に密接に関わるものといえるので、本件記事による最も重大な社会的な損害は日本において生じているといえるから、本件記事に関する不法行為によって生ずる債権の成否について、通則法20条所定の「密接な関連がある他の地」は日本であるといえることができる。

なお、被告は、他人の名誉を毀損する不法行為については、通則法20条の適用は制限されるべきである旨主張するけれども、通則法20条は、「前3条の規定にかかわらず」と規定しており、不法行為によって生ずる債権の成立及び効力の準拠法を定める通則法17条のみならず、名誉又は信用を毀損する不法行為に関する同条の特則である通則法19条についても、特則を定めていることは明らかであるから、被告のこの主張を採用することはできない。したがって、本件記事に関する不法行為の成否についての準拠法は、通則法20条の規定により、日本法であるといえるべきで

	<p>ある。</p> <ul style="list-style-type: none"> ・ブログ管理者の削除義務 <p>ブログの管理者においては、当該表現について不法行為が成立すると判断することができる場合に限り、当該表現を削除する義務を負うというべきであるところ、本件記事については、名誉を毀損する表現が含まれていたものの、真実性の抗弁や相当性の抗弁の成否につき、原告らと本件発信者との間で意見の対立があり、本件発信者が真実性の抗弁や相当性の抗弁についても一応の根拠が示されていたので、被告において、本件削除要求から本件削除までの間に、本件記事について不法行為が成立すると判断できる状況にあったとはいえない。</p> <p>したがって、被告には、本件削除要求から本件削除までの間に、本件削除義務があったということはできない。したがって、原告らの被告に対する本件記事に関する不法行為が成立するとは認められない。</p>
--	--

ス) マジコン (各不正競争行為差止等請求, 承継参加申立事件)

表 46 裁判例調査結果 (その26)

事件番号	平21(ワ)40515号・平22(ワ)12105号・平22(ワ)17265号
裁判年月日	平成25年7月9日
裁判所名	東京地裁判決
結果	一部認容
原審	—
公開URL	http://www.courts.go.jp/app/files/hanrei_jp/447/083447_hanrei.pdf
裁判要旨	<p>携帯型ゲーム機で実行されるゲーム等のプログラムが記録された記録媒体を販売している原告らが、被告B Iを除く被告らによる各製品の輸入、販売等が旧不正競争防止法2条1項10号(現11号に相当するが内容は変更されている)に掲げる不正競争に該当するとして、上記被告らに対し、上記被告らの行為が各製品の譲渡、輸入等の差止め及び廃棄を求め、また、原告X1が、被告らに対し、上記被告らによる行為が旧不正競争防止法2条1項10号(現11号に相当)に掲げる不正競争に該当するとして、損害賠償を求めた事案。</p> <p>本件DS用マジコンは、いずれもDS本体におけるプログラムの実行を</p>

	営業上用いられている技術的制限手段の効果を妨げることにより可能とする機能を有するプログラムを記録した記録媒体に当たると認められ、かつ、本件DS用マジコンに記録されているプログラムが上記機能以外の機能を併せて有するとは認められないなどとして、請求の一部を認容した。
--	---

セ) ツイッター（発信者情報開示請求控訴事件）

表 47 裁判例調査結果（その27）

事件番号	平28（ネ）10101号
裁判年月日	平成30年4月25日
裁判所名	知財高裁判決
結果	原判決変更・一部認容
原審	第一審 平成28年9月15日 東京地裁 判決 平27（ワ）17928号 発信者情報開示請求事件
公開URL	http://www.courts.go.jp/app/files/hanrei_jp/761/087761_hanrei.pdf
裁判要旨	<p>本件は、控訴人が、インターネット上の短文投稿サイト「ツイッター」において、控訴人の著作物である本件写真が、①氏名不詳者により無断でアカウントのプロフィール画像として用いられ、その後当該アカウントのタイムライン及びツイート（投稿）にも表示されたこと、②氏名不詳者により無断で画像付きツイートの一部として用いられ、当該氏名不詳者のアカウントのタイムラインにも表示されたこと、③氏名不詳者らにより無断で上記②のツイートのリツイートがされ、当該氏名不詳者らのアカウントのタイムラインに表示されたことにより、控訴人の本件写真についての著作権（複製権、公衆送信権〔送信可能化権を含む。〕、公衆伝達権。以下、これらを総称して「本件著作権」という。）及び著作者人格権（氏名表示権、同一性保持権、名誉声望保持権。以下、これらを総称して「本件著作者人格権」という。）が侵害されたと主張して、「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」（以下「プロバイダ責任制限法」という。）4条1項に基づき、上記①～③のそれぞれについて、別紙発信者情報目録記載の情報の開示を求める事案である。</p> <p>本件は、①～③の氏名不詳者を対象としているが、以下では③のリツイートを行った氏名不詳者に関して述べる。結論として、著作者人格権（同一性保持権、氏名表示権）侵害が認められた。なお、被控訴人ツイッター</p>

	<p> ジャパンについては全ての請求が棄却された他、最近のログイン時のIPアドレスの開示は認められなかった。以下、これら争点について述べる。 </p> <p> ・争点(1) (被控訴人ツイッタージャパンの発信者情報保有の有無) について </p> <p> 控訴人は、被控訴人ツイッタージャパンが、情報の削除等の窓口業務を含む、ツイッターのサポート業務を行っていること、控訴人が被控訴人ツイッタージャパンに対して控訴人撮影の写真について公衆送信の差止め等を求めた別件訴訟において、被控訴人ツイッタージャパンへの訴状送達後に画像が削除されたこと、本件についても、控訴人が被控訴人ツイッタージャパン宛てに本件写真の削除を申し出たところ、現実に削除がされたこと、被控訴人らの役員が共通していること、被控訴人米国ツイッター社は傘下にツイッター東京事務所を有すると表明しており、従業員の採用面接を同事務所で行っていることを主張するが、これらの事実が認められるとしても、これらの事実から、被控訴人ツイッタージャパンが発信者情報を開示する権限を有していると認められるものではないとして、控訴人の被控訴人ツイッタージャパンに対する請求をすべて棄却した。 </p> <p> ・争点(3) (本件リツイート行為による著作権等の侵害の明白性) について </p> <p> 本件リツイートにあたっては、リツイート者以外の者が管理するサーバにある本件写真が、本件リツイートにおいて指定された大きさ等で表示された。本件写真をリツイート者が公衆送信したとは認められず、受信装置を用いる公衆伝達を行ったとも認められない。しかし、本件画像が大きさ等を変更されて本件画像と異なるものとして表示されることについては、リツイート者の大きさ等の指定に係るものであるから、リツイート者による改変であり、同一性保持権侵害となる。また、本件リツイートにあたって位置や大きさを指定した結果、控訴人の氏名が表示されなくなったことから、氏名表示権侵害も認められる。 </p> <p> ・争点(4) (最新のログイン時IPアドレス等の発信者情報該当性) について </p> <p> 省令4号は「侵害情報に係るアイ・ピー・アドレス・・・及び当該アイ・ピー・アドレスと組み合わせられたポート番号」と、同7号は「侵害情報が送信された年月日及び時刻」とそれぞれ定めている。最新のログイン時IPアドレスは侵害情報に係るIPアドレスではないので、省令4号の「侵 </p>
--	--

	害情報に係るアイ・ピー・アドレス」には含まれない。また、当該侵害情報の発信と無関係な最近のログイン時タイムスタンプは同7号の「侵害情報が送信された年月日及び時刻」に当たらない。
--	--

ソ) ウェブサイトアップロード (損害賠償請求事件)

表 48 裁判例調査結果 (その28)

事件番号	平29 (ワ) 19660号
裁判年月日	平成30年3月29日
裁判所名	東京地裁判決
結果	一部認容
原審	—
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/721/087721_hanrei.pdf
裁判要旨	株式会社CAを吸収合併し、同社から本件各著作物の著作権及び本件各著作物の著作権侵害により発生した損害賠償請求権を取得した原告が、株式会社CAの許諾を得ることなく、本件各著作物をインターネット上の動画共有サイトである「FC2動画アダルト」のサーバー上にアップロードし、不特定多数の者が閲覧できる状態に置いた被告に対し、著作権侵害の不法行為に基づく損害賠償請求の一部請求を行った事案。 被告は、本件各著作物の一部を本件動画サイトにアップロードしたと認められ、この行為は、株式会社CAの本件各著作物に係る公衆送信権 (著作権法23条1項) の侵害に当たると認められる。

タ) 公衆送信権侵害のストリーミングの際の損害額 (損害賠償請求事件)

表 49 裁判例調査結果 (その29)

事件番号	平27 (ワ) 13760号
裁判年月日	平成28年4月21日
裁判所名	東京地裁判決
結果	一部認容
原審	—
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/883/085883_hanrei.pdf
裁判要旨	原告が著作権を有するデータを被告が動画共有サイトのサーバーにア

	<p>アップロードした行為が公衆送信権（著作権法23条1項）の侵害に当たるとされた。本件動画サイトは動画をストリーミング配信するウェブサイトであり、これを視聴する者のパソコン等に一時的に上記データが蓄積されるが、視聴すると直ちに消去されるので、データをダウンロードした場合のようにウェブサイトに再度アクセスせずに映像を再度視聴することはできない。公衆送信権侵害は争いにはならず、本件の争点は、原告の損害額である。</p> <p>1 著作権法114条1項に基づく損害額について</p> <p>原告は、①ストリーミングの再生回数が受信複製物の数量に当たること、②本件動画サイトにおけるストリーミングの再生回数はダウンロードの回数と同視できることなどからすれば、ストリーミングの再生回数が著作権法114条1項にいう受信複製物の数量となる旨主張した。</p> <p>裁判所は、当該映像を視聴しても、特殊なソフトウェアを使わない限り、受信複製物を保存することはできないので、再生回数とダウンロード数と同視できないとし、原告の主張をしりぞけた。</p> <p>2 著作権法114条3項に基づく損害額について</p> <p>本件著作物1の「再生数」は1万3292回、本件著作物2の「再生数」は2万4539回と本件動画サイトに表示されていた。この「再生数」には数秒間表示されるだけのサンプル動画の再生数も含まれる。本件著作物1及び2に係る「再生数」の内訳は不明である。</p> <p>「再生数」の正確性を裏付ける証拠はないが、サンプル動画の再生回数が多いであろうこと、本件著作物のストリーミング配信の正規の価格はおおむね1本当たり270～390円程度であること、原告自らが使用許諾をした場合の対価についての証拠が乏しいことなどの事情を総合して、被告による本件著作物の公衆送信権の侵害に対して原告が著作権の行使につき受けるべき金銭の額は、それぞれ50万円とされた。</p>
--	---

チ) 写真の違法アップロード（損害賠償等請求事件）

表 50 裁判例調査結果（その30）

事件番号	平26（ワ）21096号
裁判年月日	平成26年11月21日
裁判所名	東京地裁判決

結果	認容
原審	—
公開 URL	
裁判要旨	<p>原告は原告サイトでグラビア写真を閲覧者に有償で提供することを業とする株式会社であるが、原告が著作権を有する各写真（以下「本件各著作物」という。）を、被告が「〇〇.com」というドメインのウェブサイト（以下「被告サイト」という。）にアップロードして、被告サイトの閲覧者がそれらをダウンロードできるようにし、さらに、5個のドメインのウェブサイト等（以下「本件各ダウンロードサイト」という。）に本件各著作物をギャラリーごとアップロードして、当該サイトの閲覧者がギャラリーごとダウンロードできるようにしていた。さらに被告は、被告サイトに本件各ダウンロードサイトへのリンクを張っており、被告サイトの閲覧者に対し、本件各ダウンロードサイトでギャラリーごとグラビア写真をダウンロードするように誘導していた。</p> <p>被告は、上記行為により、原告が本件各著作物に対して有する著作権（複製権及び翻案権並びに自動公衆送信権及び送信可能化権）を侵害した。</p> <p>被告はこれまで、原告がダウンロードサイトに削除申請をしてグラビア写真が削除されると、すぐに別のダウンロードサイトにギャラリーごとグラビア写真をアップロードすることを繰り返してきた。</p> <p>被告の著作権侵害行為によって原告が被った損害については、ギャラリーごとの閲覧者のアクセス数が本件各著作物をダウンロードした数量とされ判断された。</p> <p>なお本件は、被告が口頭弁論期日に出頭せず、答弁書その他の準備書面を提出しないことから、自白したとみなされたもの。</p>

ツ) 自炊代行（著作権侵害差止等請求控訴事件）

表 51 裁判例調査結果（その31）

事件番号	平25（ネ）10089号
裁判年月日	平成26年10月22日
裁判所名	知財高裁判決
結果	控訴棄却

原審	<p>上告審 平成 28 年 3 月 16 日 最高裁第二小法廷 決定 平 2 7 (受) 1 6 7 号 著作権侵害差止等請求事件→上告不受理</p> <p>第一審 平成 25 年 9 月 30 日 東京地裁 判決 平 2 4 (ワ) 3 3 5 2 5 号 著作権侵害差止等請求事件</p>
公開 URL	<p>http://www.courts.go.jp/app/files/hanrei_jp/579/084579_hanrei.pdf</p>
裁判要旨	<p>本件は、小説家、漫画家又は漫画原作者である被控訴人らが、控訴人ドライブレッジは、顧客から電子ファイル化の依頼があった書籍について、著作権者の許諾を受けることなく、スキャナーで書籍を読み取って電子ファイルを作成し（以下、このようなスキャナーを使用して書籍を電子ファイル化する行為を「スキャン」あるいは「スキャニング」という場合がある。）、その電子ファイルを顧客に納品しているところ（以下、このようなサービスを依頼する顧客を「利用者」という場合がある。）、注文を受けた書籍には、被控訴人らが著作権を有する原判決別紙作品目録 1～7 記載の作品（以下、併せて「原告作品」という。）が多数含まれている蓋然性が高く、今後注文を受ける書籍にも含まれる蓋然性が高いから、被控訴人らの著作権（複製権）が侵害されるおそれがあるなどと主張し、①著作権法 1 1 2 条 1 項に基づく差止請求として、控訴人ドライブレッジに対し、第三者から委託を受けて原告作品が印刷された書籍を電子的方法により複製することの禁止等を求めた事案である。</p> <p>・控訴人による複製行為の有無</p> <p>本件サービスは、①利用者が控訴人ドライブレッジに書籍の電子ファイル化を申し込む、②利用者は、控訴人ドライブレッジに書籍を送付する、③控訴人ドライブレッジは、書籍をスキャンしやすいように裁断する、④控訴人ドライブレッジは、裁断した書籍を控訴人ドライブレッジが管理するスキャナーで読み込み電子ファイル化する、⑤完成した電子ファイルを利用者がインターネットにより電子ファイルのままダウンロードするか又は DVD 等の媒体に記録されたものとして受領するという一連の経過をたどるものであるが、このうち上記④の、裁断した書籍をスキャナーで読み込み電子ファイル化する行為が、本件サービスにおいて著作物である書籍について有形的再製をする行為、すなわち「複製」行為に当たることは明らかであって、この行為は、本件サービスを運営する控訴人ドライブレッジのみが専ら業務として行っており、利用者は同行為には全く関与していない。利用者から対価を得ており、控訴人ドライブレッジは、利用者</p>

	<p>と対等な契約主体であり、営利を目的とする独立した事業主体として、本件サービスにおける複製行為を行っているのであるから、本件サービスにおける複製行為の主体であると認めるのが相当である。</p> <p>・著作権法30条1項の適用の可否について</p> <p>控訴人ドライバレッジは、営利を目的として、顧客である不特定多数の利用者に複製物である電子ファイルを納品・提供するために複製を行っているのであるから、「個人的に又は家庭内その他これに準ずる限られた範囲内において使用することを目的とする」ということはできず、要件を欠く。また、控訴人ドライバレッジは複製行為の主体であるのに対し、複製された電子ファイルを私的使用する者は利用者であることから、「その使用する者が複製する」ということはできず、かかる要件も欠く。したがって、控訴人ドライバレッジについて同法30条1項を適用する余地はない。</p>
--	--

テ) P2P ネットワーク（発信者情報開示請求控訴事件）

表 52 裁判例調査結果（その32）

事件番号	平26（ワ）3570号
裁判年月日	平成26年6月25日
裁判所名	東京地裁判決
結果	認容
原審	—
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/311/084311_hanrei.pdf
裁判要旨	<p>本件は、レコード製作会社である原告らが、インターネット接続プロバイダ事業を行っている被告に対し、原告らが送信可能化権（著作権法96条の2）を有するレコードが氏名不詳者によって原告らに無断で複製され、被告のインターネット回線を経由して自動的に送信し得る状態に置かれたことにより、原告らの送信可能化権が侵害されたと主張して、被告に対し、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条1項に基づき、上記氏名不詳者に係る発信者情報の開示を求める事案である。</p> <p>G n u t e l l a ネットワークとは、ファイル共有ソフトである「G n u t e l l a」と称するソフトウェア及び同ソフトウェアと共通するプロ</p>

	<p>トコルを持つファイル共有クライアントソフトのユーザー同士が、互いのハードディスクにあるファイル（情報）を相互に交換することができるP2Pネットワークである。</p> <p>本件システムは、クロスワープ社が開発したインターネット上の著作権侵害検出システムであり、各種P2Pネットワークに接続し、流通するファイル及びダウンロード時の情報（送信元となったノードのIPアドレス、ポート番号、ファイルハッシュ値、ダウンロード完了時刻等）を収集、分析等するものである。クロスワープ社は、レコード会社等から依頼を受けて、同システムを使って、市販されているCDの音源が各種P2Pネットワーク上で公開されているかどうかを検索している。</p> <p>被告から「219.108.203.208」のIPアドレスの割当てを受けた者により、Gnutella互換ソフトウェアによって本件ファイル1及び2が自動的に送信し得る状態にされ、本件システムによりがダウンロードされたのであるから、上記IPアドレスを使用してインターネットに接続する権限を有していた契約者を本件ファイル1及び2に関する「侵害情報の発信者」と推認するのが合理的である。なお、契約者のIPアドレス等の不正利用や暴露ウィルスへの可能性などの一般的抽象的可能性の存在が、上記認定の妨げになるものとは認められない。これらにより、発信者情報開示の請求が認容された。</p>
--	--

ト) 動画サイトのリンク（損害賠償等請求事件）

表 53 裁判例調査結果（その33）

事件番号	平23（ワ）15245号
裁判年月日	平成25年6月20日
裁判所名	大阪地裁判決
結果	請求棄却
原審	—
公開URL	
裁判要旨	原告は、被告において、原告が著作者である動画を、自社の運営する「ロケットニュース24」と称するウェブサイトは無断で掲載し、これに原告を誹謗中傷する別紙記事記載の記事を掲載し、さらに本件記事下部のコメント欄に、読者をして原告を誹謗中傷する別紙コメント欄記載の書き込み

をさせ、これを削除しなかったことが、原告の名誉を毀損するとともに、原告の著作権（公衆送信権）及び著作者人格権（公表権、氏名表示権）を侵害するものであると主張。

原告が動画として、「ニコニコ生放送」にライブストリーミング配信し、原告以外の第三者（特定されていない。）がそのうち、の約15分間の部分を、動画共有サイト「ニコニコ動画」にアップロードしいつでも視聴し得るようにした。

被告は、本件動画に着目し、本件ウェブサイト内に本件記事を掲載するとともに、「ニコニコ動画」上の本件動画に付されていた引用タグ又はURLを本件ウェブサイトの編集画面に入力した。

・争点1-1（本件動画は映画の著作物に該当するか）について

被告は、本件動画は固定されていないので著作物に該当しないと主張したが、本件生放送は、その配信と同時にニワンゴのサーバに保存され、その後視聴可能な状態に置かれたものと認められ、「固定」されたものといえる（法2条3項）。したがって、本件生放送の一部である本件動画は、「映画の著作物」（法10条1項7号）に該当し、その著作者は原告と認められた。

・争点1-2（公衆送信権侵害の有無）について

被告は、「ニコニコ動画」にアップロードされていた本件動画の引用タグ又はURLを本件ウェブサイトの編集画面に入力することで、本件動画へのリンクを貼ったにとどまる。本件動画のデータを端末に送信する主体はあくまで「ニコニコ動画」の管理者であり、被告がこれを送信していたわけではない。したがって、本件ウェブサイトを経営管理する被告が、本件動画を「自動公衆送信」をした（法2条1項9号の4）、あるいはその準備段階の行為である「送信可能化」（法2条1項9号の5）をしたとは認められない。

本件動画にリンクを貼ることで、公衆送信権侵害の幫助による不法行為が成立するかについては、「ニコニコ動画」にアップロードされていた本件動画は、著作権者の明示又は黙示の許諾なしにアップロードされていることが、その内容や体裁上明らかではなく、このような著作物にリンクを貼ることが直ちに違法になるとは言い難い。そして、被告は、本件ウェブサイト上で本件動画を視聴可能としたことにつき、原告から抗議を受けた時点、すなわち、「ニコニコ動画」への本件動画のアップロードが著作権

	<p>者である原告の許諾なしに行われたことを認識し得た時点で直ちに本件動画へのリンクを削除している。</p> <p>このような事情に照らせば、被告が本件ウェブサイト上で本件動画へリンクを貼ったことは、原告の著作権を侵害するものとはいえないし、第三者による著作権侵害につき、これを違法に幫助したものでもなく、故意又は過失があったともいえないから、不法行為は成立しない。</p>
--	---

ナ) 動画サイトへのアップロード（損害賠償請求事件）

表 54 裁判例調査結果（その34）

事件番号	平25（ワ）1918号
裁判年月日	平成25年5月17日
裁判所名	東京地裁判決
結果	認容
原審	—
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/281/083281_hanrei.pdf
裁判要旨	原告が著作権を有する、総合格闘技競技である「Ultimate Fighting Championship」(UFC)の大会及び試合を撮影・編集した映像作品である本件各作品を、被告が「ニコニコ動画」にアップロードした行為により、被告は、著作権（公衆送信権）侵害の不法行為責任に基づく損害賠償義務を負うとされた事案。

ニ) 金融庁による調査不実施（金融庁不正アクセス禁止法違反調査不作為控訴事件）

表 55 裁判例調査結果（その35）

事件番号	平29（ワ）13420号
裁判年月日	平成29年11月8日
裁判所名	東京地裁判決
結果	請求棄却
原審	控訴審 平成30年4月19日 東京高裁 判決 平29（ネ）5168号 金融庁不正アクセス禁止法違反調査不作為控訴事件があるが、控訴棄却のため原審を記載
公開 URL	

<p>裁判要旨</p>	<p>本件は、原告が、原告が代表取締役を務めていた会社名義の朝日信用金庫の預金口座に対して不正アクセス行為の禁止等に関する法律に違反する不正なアクセス（識別符号提供、同使用）がされたことによって預金1500万円が失われたとして、関東財務局長宛てに同信用金庫に対する行政処分や違法の確認等を申し立てたが、調査が開始されたものの停止され、同局長が同信用金庫の調査や処分、違法の確認等をしないので、不作為の違法があるとして、行政不服審査法に基づき、金融庁長官に対して審査請求をしたのに対し、金融庁長官は、原告の上記申立ては行政手続法36条の3第1項に基づくもので、平成26年法律第68号による改正前の行政不服審査法（以下「旧行審法」という。）が適用されるどころ、同法7条の要件を満たさないから、補正の余地がない不適法な審査請求であるとして、却下する裁決をしたため、金融庁の不作為が続き、原告の損害が救済されない状態が続いているとして、国家賠償法に基づき、損害1500万円のうち一部である150万円の損害賠償を求めた事案である。</p> <p>行政手続法36条の3の処分等の求め及びこれを受けた行政庁等の対応についての制度は、一般人からの申出について、行政庁等の適正な規制・監督の端緒とするものであって、更に行政庁等において調査等の資料収集を行いこれに基づいて処分をするかについては、その要否も含めて行政庁等の広範な裁量に委ねているのであって、申出に基づいて一定の調査、処分等を行うことを行政庁等に義務付けるものではないことはもとより、申出をした者に対してその調査、処分等の行政庁等の対応の結果等を応答する義務を課したものでもない。</p> <p>したがって、行政手続法36条の3に基づく申出に関しては、そもそも旧行審法2条2項にいう「法令上に基づく申請」に当たらず、当該申出等に係る不作為は行審法7条の対象とはならないと解される。</p>
-------------	--

又) 理事長メールへの無断アクセスによる解雇（地位確認等請求事件）

表 56 裁判例調査結果（その36）

<p>事件番号</p>	<p>平26（ワ）10号</p>
<p>裁判年月日</p>	<p>平成26年3月30日</p>
<p>裁判所名</p>	<p>福井地裁判決</p>
<p>結果</p>	<p>請求棄却</p>

原審	控訴審 平成 28 年 9 月 14 日 名古屋高裁金沢支部 判決 平 2 8 (ネ) 8 6 号 地位確認等請求控訴事件があるが、控訴棄却のため原審を記載
公開 URL	
裁判要旨	<p>本件は、Y 1 信用金庫（以下「旧信金」という。）に雇用されて旧信金の業務に従事していた原告らが、職務上の必要も権限もないのに、旧信金の理事長らのメールファイルに無断でアクセスを行い、メールに添付されていた機密文書を閲覧した上で、当該機密文書を印刷する等不正アクセス禁止法に違反する行為をしたとして、旧信金が原告らに異動を命じた上、懲戒解雇したところ、原告らが、上記異動命令の発令等が不法行為に当たり、上記懲戒解雇は懲戒権を濫用してしたものであるから無効かつ原告らに対する不法行為に当たるなどと主張した事案。</p> <p>メールへアクセスする ID は、あらかじめ各職員に割り当てられている 5 桁の職員番号であり、パスワードは各職員が自ら設定するが、職員番号と同じ番号をパスワードとして設定する職員も多く、B 前理事長及び C 理事長もそのように設定していた。なお、個々の職員の職員番号は、職員番号表に掲載されており、旧信金の職員であれば、他の職員の職員番号を知ることができた。</p> <p>原告らは、次のような文書ファイルを印刷した。「一般貸倒引当金（日銀考査）10-26」、本件酒造会社以外の取引先の「保証人明細表」、「平成 23 年度決算シミュレーション（マル秘）」、「決意文の提出について」、「常勤役員意見交換会 230118」、「不振原因に係る反省と今後の取り組み方針」、本件酒造会社に関する 4 個のファイル等。原告らが印刷した文書には、本件酒造会社に対する融資に関するもののほか、旧信金職員の不祥事に関するもの、金融庁検査に関するものが大量に含まれていた。</p> <p>・争点 原告らは公益通報を目的として本件アクセス等を行ったか</p> <p>原告らは、本件アクセス等は、公益通報をするために旧信金の本件酒造会社への不正融資に関する資料を取得する目的で行ったものであると主張する。しかし、文書名やその内容に照らして、本件酒造会社とはおよそ無関係と思われるものが多く、不正融資とも全く関連性のないものさえ含まれている。さらに、原告らは、本件酒造会社への融資に関する資料を過去に遡って閲覧・印刷することは一切行っていない。加えて、原告らは、本件懲戒解雇に至るまで、警察からの求めがあっても、本件アクセス等によって取得した資料を警察等には一切提出していないなど、上記資料が公</p>

	<p>益通報の目的に供されたことを裏付ける客観的な事情や的確な証拠は見当たらない。したがって、公益通報をする目的で本件アクセス等を行ったとは認められない。</p> <p>・争点 本件懲戒解雇が社会通念上相当でないといえるか</p> <p>原告らは、顧客の信用情報その他の機密性の高い文書を、役員のメールアドレス等へ権限なくアクセスするという不正な手段を用いて、長期間・多数回にわたり、意図的に幅広く閲覧し、大量に印刷したのみならず、少なくともその印刷物の一部を外部に持ち出した。このような原告らの非違行為の態様及び結果は重大であると評価せざるを得ず、仮に原告らが旧信金の不正を糺すという正当な目的・動機を有していたとしても、そのことのみをもって正当化されるものではない。</p> <p>以上に指摘した諸事情を総合的に勘案すれば、本件懲戒解雇が社会通念上相当でないものとは認められない。</p>
--	--

ネ) B-CAS (損害賠償請求事件)

表 57 裁判例調査結果 (その37)

事件番号	平25(ワ)11826号
裁判年月日	平成25年7月31日
裁判所名	東京地裁判決
結果	認容
原審	—
公開URL	
裁判要旨	<p>原告は、B-CAS方式と呼ばれる限定受信システムを統括管理し、この方式を採用したカードをデジタル放送受信機に挿入することにより、有料放送などの個別視聴制御を行う「B-CASカード」を発行して、その管理及び放送事業者への利用提供等の事業を行っているところ、(1)被告が、原告が、有料衛星放送の契約者以外の者が同放送を視聴できないように制限するために営業上用いている技術的制限手段を妨げることにより、同放送の視聴を可能とする機能を有する不正なプログラムを、ファイル共有ソフト「○○」を作動させ、不特定多数のインターネット利用者へ送信し得る状態にして提供したこと、(2)被告が、ICカードリーダー・ライターを用いて「B-CASカード」に記録された電磁的記録を改変し、こ</p>

	<p>の不正に作出した「B-CASカード」を第三者に譲渡したことは、いずれも不正競争防止法（以下「不競法」という。）2条1項11号（現12号）に定める不正競争行為に該当するとして、損害賠償金を求めた事案。</p> <p>原告の管理する「B-CASカード」は、限定受信方式であるB-CAS方式により、カードチップに記録された電磁的記録を蔵置するカードをデジタル放送受信機に挿入することで有料放送などの個別視聴制御を行うものである。B-CAS方式においては、有料放送番組の映像や音等の映像信号は暗号化して発信されており、B-CASカードに設定された異なる固有の暗号鍵により、視聴契約者のみが有料放送番組の暗号を復号することができ、視聴が可能となる仕組みとなっている。したがって、原告のB-CAS方式は、不競法2条7項が定める「技術的制限手段」に該当し、また、不競法2条1項11号（現12号）が定める「他人が特定の者以外の者に影像若しくは音の視聴・・・をさせないために営業上用いている技術的制限手段」に該当する。</p> <p>そして、本件不正プログラムは、原告が、有料衛星放送の契約者以外の者が同放送を視聴できないように制限するために営業上用いている上記技術的制限手段を妨げることにより、同放送の視聴を可能とする機能を有するプログラムであるから、技術的制限手段回避プログラムに該当し、これを不特定多数のインターネット利用者に送信し得る状態にして提供した被告の行為は、不競法2条1項11号（現12号）に定める不正競争行為に該当する。</p> <p>また、被告が不正に作出したB-CASカードは、B-CASカードに記録された電磁的記録を改変し、視聴契約の権利、義務に関する電磁的記録を不正に作出し、原告が有料衛星放送の契約者以外の者が同放送を視聴できないように制限するために営業上用いている技術的制限手段を妨げることにより同放送の視聴を可能とする機能を有する装置であるから、技術的制限手段回避装置に該当し、これを譲渡した行為についても、不競法2条1項11号（現12号）に定める不正競争行為に該当する。</p> <p>なお被告は、本件口頭弁論期日に出頭せず、答弁書その他の準備書面も提出しないため、自白したものとみなされた。</p>
--	---

ノ) イラストの無断転載（損害賠償請求事件）

表 58 裁判例調査結果（その38）

事件番号	平30(ワ)12524号
裁判年月日	平成30年9月13日
裁判所名	東京地裁判決
結果	一部認容
原審	—
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/021/088021_hanrei.pdf
裁判要旨	<p>「A」という筆名のイラストレーターである原告のイラスト3点が、「A (@〇〇)」というツイッターアカウントで公開され、その後「Aさんの Twitter イラストまとめ-A. info」と題するウェブサイト等に掲載されたことに対し、原告の送信可能化権（著作権法23条1項）を侵害するものであると原告が主張して、送信可能化権侵害の不法行為に基づき、著作権法114条3項により損害賠償金及び遅延損害金の支払を求める事案。</p> <p>被告は、本件サイトについて、ドメインの設定及びブログ登録等の開設作業や、プログラム及びデザイン等のサポート業務を担当することとされていた。本件サイトのドメインは、被告名義で登録されている。被告は、本件サイトの管理並びに本件記事の作成及び投稿等について、不法行為責任を負う立場にあると認められた。</p>

ハ) 選挙公約のインターネット掲示板転載（発信者情報開示請求事件）

表 59 裁判例調査結果（その39）

事件番号	平29(ワ)21232号
裁判年月日	平成29年10月2日
裁判所名	東京地裁判決
結果	認容
原審	—
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/207/087207_hanrei.pdf
裁判要旨	<p>原告が、総極真の代表選挙における原告の公約文を何者かが2ちゃんねるに投稿したことにより著作権を侵害されたとして、経由プロバイダに発信者情報開示を求める事案。</p> <p>被告は、本件文書を構成する個々の表現は、公約としてありふれた表現であるとして、著作物性を争う旨主張する。しかしながら、本件文書には、</p>

	<p>総極真の代表選挙における原告の19個もの公約や信条に係る記載があり、全体として40以上の文章からなるまとまりのある文書であると認められるから、その内容や記載順序等において、原告の個性が表出されていると認められる。したがって、本件文書は、原告の思想又は感情を創作的に表現したものであると認められ、言語の著作物（著作権法10条1項1号）として著作物性を有し、原告は、その作成者として、その著作権を有するものと認められる。</p> <p>本件各記事は、末尾の部分を除いて40以上の文章からなる本件文書と同一であるから、氏名不詳者において、本件文書を分割して転載したものであると認められ、被告の提供するインターネット接続サービスを経由して本件掲示板に投稿されたことによって、公衆の求めに応じて自動的に公衆送信が行われる状態におかれている。したがって、少なくとも、原告が有する本件文書の著作権（送信可能化権）が侵害されたことは明らかであると認められる。</p>
--	--

ヒ) 楽曲の不正シェア（発信者情報開示請求事件）

表 60 裁判例調査結果（その40）

事件番号	平29（ワ）12582号
裁判年月日	平成29年6月26日
裁判所名	東京地裁判決
結果	認容
原審	—
公開 URL	http://www.courts.go.jp/app/files/hanrei_jp/471/087471_hanrei.pdf
裁判要旨	<p>本件は、レコードの送信可能化権を有する原告らが、氏名不詳者が上記レコードに収録された楽曲を複製してコンピュータ内の記録媒体に記録して蔵置し、被告の提供するインターネット接続サービスを経由して自動公衆送信し得る状態にした行為により送信可能化権を侵害されたと主張して、経由プロバイダである被告に対し、発信者情報の開示を求める事案である。</p> <p>氏名不詳者（1名に限られない。）は、レコードに収録された楽曲をmp3方式により圧縮して複製したファイルを、被告の提供するインターネット接続サービスを利用して、ファイル共有ソフトウェアを用いて上記複</p>

	<p>製に係るファイルを、不特定の他の利用者からの求めに応じて自動的に送信し得る状態に置いた事実が認められる。</p> <p>そして、上記送信可能化行為について、著作隣接権の権利制限事由（著作権法102条1項が準用する同法30条以下）があるとはうかがわれな いから、同行為により、原告らが有する本件各レコードの送信可能化権が侵害されたことが明らかであると認められるとされた。</p> <p>被告は、メールアドレスの開示には正当な理由がないと主張したが、権利行使の一環としての裁判外の交渉等を行うためには電子メールアドレスが必要だとされて、電子メールアドレスを含む情報の開示が認容された。</p>
--	---

フ) インターネットテレビ配信（損害賠償請求事件）

表 61 裁判例調査結果（その41）

事件番号	平25(ワ)23364号
裁判年月日	平成26年9月5日
裁判所名	東京地裁判決
結果	認容
原審	—
公開 URL	
裁判要旨	<p>韓国の放送事業者である原告は、本件テレビ番組を韓国の放送設備から放送していたが、インターネットを利用したテレビ番組配信サービス等を事業とする被告は、受信した本件番組をデジタルデータに変換（エンコード）して、そのデータファイルを日本国内にある被告サーバに保存し、日本に在住する利用者の操作に従って当該利用者宅に設置されたセットトップボックスに当該データファイルが送信されて、当該利用者が当該機器と接続したテレビで本件番組を視聴することができた。被告が提供した本件サービスは、少なくとも原告が有する本件番組についての著作隣接権（複製権及び送信可能化権）を侵害したことが認められるとされた。</p> <p>原告と被告はいずれも韓国の法人であるが、被告は受信した本件番組をデジタルデータに変換（エンコード）して、そのデータファイルを日本国内にある被告サーバに保存しており、被告がした不法行為の少なくとも一部が日本国内にあると認められるから、本件につき我が国の裁判所が管轄</p>

	権を有する（民訴法3条の3第8号）。
--	--------------------

（２）裁判例についての分析

前項の裁判例より、データの保護に関する対策の実施状況が裁判の結果等に及ぼす影響について、次のような傾向が判別される。

① 営業秘密における秘密管理性の要件の認定

（１）に示した裁判例において、営業秘密における秘密管理性の要件が成立するかどうか判断されたものについて、実施されていたデータ保護の対策と秘密管理性に関する要件の認定状況を整理すると次表のようになる。データをパスワード等で保護するだけでなく、不正競争行為を行う者に対して、当該データが秘密であることが認識されるような措置が講じられることが求められていることがわかる。

表 62 秘密管理性の認定状況の比較

分類	秘密として管理するために実施されていた対策
秘密管理性の要件を満たすと判断されたもの	以下の対策を組み合わせる実施 ● 営業秘密とするデータにアクセスできる者を従業者の一部に限定 ● 執務室への入退室の管理等により無権限者からのアクセス防止措置の実施 ● 社内規程において、営業秘密とするデータを機密に位置づけ、研修等でアクセス権限のある従業者にその趣旨の浸透を図り、関係者以外にデータを開示することを禁止 ● 私物パーソナルコンピュータの使用を禁止 ● 業務用 PC の持ち出しや外部記録媒体への書き出しを原則として禁止 ● 営業秘密とするデータを格納するデータベースへの業務用 PC によるアクセス記録を保存
	以下の対策を組み合わせる実施 ● 就業規則を制定し、従業員に秘密保持義務を課す ● ISO 27001 の要求事項に適合していると認証され、適合性審査を毎年更新しており、ISO 規格の内部監査員養成セミナーを受けたシステム管理責任者らにより、従業員に対し、一般情報セキュリティ教育を実施 ● 資産台帳上、営業秘密とするデータを、公開レベル「秘密」に区分 ● 社内ファイルサーバ内のデータのうち、アクセスを制限するものについて、フォルダ毎にアクセスできる従業員を限定した上で、個々の従業員が特定の端末から、ユーザ名とパスワードを入力しなければアクセスできないように管理
	以下の対策を組み合わせる実施 ● 営業秘密とするデータを従業員しか閲覧することのできない社内ネットで管理 ● 営業秘密とするデータを閲覧できる範囲を従業員の所属部署、地位に応じて限定 ● 従業員において情報保護の規程があることを認識
	以下の対策を組み合わせる実施 ● 営業秘密とするデータを管理部の専用パソコン 1 台に集約し、パスワードに

	<p>より管理</p> <ul style="list-style-type: none"> ● 専用パソコンのアクセス権者を、パスワードを知っている管理部所属の従業員4名のみ限定し、その他の従業員が営業秘密とするデータを必要とする場合には、所属先の長が管理部に書面で申請 ● 鍵と警備装置により、営業時間外を含めて、役員、管理部所属の従業員及びこれらの者に入室を認められた者以外の管理部への立入りを制限 ● 個人情報を含む営業秘密とするデータについての守秘義務を従業員に課し、業務通達や社内研修で周知に努めていた
秘密管理性の要件を満たすと判断されなかったもの	<p>以下の対策を組み合わせ実施</p> <ul style="list-style-type: none"> ● 営業秘密とするデータを保存するパソコンを起動するためにパスワードの入力を必要とするよう設定 ● 営業秘密とするデータにはパスワードを設定せず

② データの保護に関する適切な対策の実施状況に基づく影響

表 23 に示した刑事事件の裁判例においては、データの管理上の不備が、被告に対する量刑の軽減につながる結果となっている。具体的には、データの保護のための対策における次のような状況が管理上の不備と判断されており、データに対する法的な保護の実効性を高めるためには、単に対策を導入するだけでなく、適切な運用を行うことの重要性が示されている。

- 営業秘密を格納するデータベースに対してアカウントを通じたアクセス制限が行われていたが、そのアカウント情報が共有フォルダ内に蔵置されていて、アクセス権限を持たない者であっても閲覧可能となっていた。
- 私物のスマートフォンの執務室への持ち込みが禁止されていなかった。
- データベースに対する異常なアクセスに関するアラートシステムが導入されていたが、実際には機能していなかった。
- 脱法的な労働力確保を通じて、経歴等が詳らかでない者に、経営の根幹に関わる営業秘密データへのアクセスを許していた。

参考文献

- [1] AI・データの利用に関する契約ガイドライン, 経済産業省, 2018.
- [2] 証拠保全ガイドライン(第7版), 特定非営利活動法人デジタル・フォレンジック研究会, 2018.
- [3] 岡村久道: 情報セキュリティの法律 [改訂版], 商事法務, 2011.
- [4] 岡村久道: 著作権法 [第3版], 民事法研究会, 2014.
- [5] 佐々木良一(編著), 上原哲太郎・櫻庭信之・白濱直哉・野崎周作・八槇博史・山本清子: デジタル・フォレンジックの理論と実践, 東京電機大学出版局, 2017.
- [6] 町村泰貴・白井幸夫: 電子証拠の理論と実務—収集・保全・立証, 民事法研究会, 2016.
- [7] 秘密情報の保護ハンドブック～企業価値向上に向けて, 経済産業省, 2016.
- [8] 岡村久道: 個人情報保護法 [第3版], 商事法務, 2017.
- [9] 組織における内部不正防止ガイドライン(日本語版)第4版, 独立行政法人情報処理推進機構, 2017.