弁護士法人外立総合法律事務所
HASHIDATE LAW
A PROFESSIONAL LAW CORPORATION
December, 2025

Our Network : UK, China, USA (LA, NY, SF, Boston), Germany, Netherland, Brazil, Singapore, Vietnam, Philippines, Malaysia, Hong Kong, Korea, Indonesia, Thailand, Myanmar, India, UAE, Qatar, Oman

HASHIDATE LAW OFFICE NEWS LETTER

Vol. 17

個人情報の保護と利活用のすすめ　Vol. 9

執筆者

顧問　　松元　照仁　Matsumoto Teruhito
（前 個人情報保護委員会事務局長）
E-mail: kenjihashidate@hashidatelaw.com (代表)

TOPIC

不正アクセスと個人データ保護（Ⅰ）不正アクセスに対する安全管理措置義務

1 はじめに

2025年11月27日、A大手ビール等販売グループ会社（本メールマガジンでは、「A 社」とする。）より、「サイバー攻撃による情報漏えいに関する調査結果と今後の対応について」と題して発表があった[1]。

発表によると、攻撃者が、A社グループ内の拠点にあるネットワーク機器を経由してデータセンターのネットワークに侵入。ランサムウェア[2]が一斉に実行され、ネットワーク接続範囲で起動中の複数サーバーや一部パソコン端末のデータが暗号化されたとのことである。情報漏えいが発生、またはそのおそれがある個人情報は190万件超にのぼると報告された。

私自身も先日、孫のベビーフードを近所のスーパーで購入しようとしたところ、多くの商品が欠品しており、驚いた。調べると、この大手ベビーフード販売業者もA社のグループ企業であった。A社社長の発表コメントでは、「商品供給についても、システムの復旧状況に伴い段階的に出荷再開の対応を進めている。」との記載があった。

1 https://www.asahigroup-holdings.com/newsroom/detail/20251127-0104.html
2 ランサムウェアとは、不正プログラムのことで、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語であり、パソコンに保存されているファイルを暗号化し、元の状態に戻すことと引き換えに金銭を要求するパターンが多い。

©HASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

独立行政法人情報処理推進機構（以下、「IPA」という。）が公表した「情報セキュリティ脅威2025【組織編】」[3]でも、今回のA社でのランサムウェア被害が第1位となっている。ランサムウェア攻撃を受けた場合、情報漏えい等による直接被害にとどまらず、商品やサービス提供自体が長期停止となるリスクがあり、経営上の重大な脅威となっている。

そこで今月号及び次月号では、近年多発しているランサムウェア攻撃を中心とした不正アクセスと個人データ保護をテーマに取り上げる。内容は

・（Ⅰ）不正アクセスに対する安全管理措置義務（今月号）
・（Ⅱ）不正アクセスの実態とその具体的対策（次月号）

として、法的措置内容や具体的運用等も交えて、その理解を深めることとしたい。

まず、恒例のクイズで皆さんの理解を確認したい。正解は、後ほど発表する。

【クイズ１】
以下の記述は正しいでしょうか。それとも誤りでしょうか。

「Ｂ社のサーバーが、Ｃ社製ＶＰＮ[4]機器経由で不正アクセスを受け、ランサムウェアに感染した結果、従業者及び顧客の個人データ約２０万件について、毀損及び漏えいのおそれが生じた。
調査の結果、今回の不正アクセスは、Ｃ社製ＶＰＮ機器の脆弱性を突いたものであることが判明した。
Ｂ社は、当該ＶＰＮ機器について、脆弱性情報が半年前にＣ社から公開され、対応方法もリリースされていたが、未対応であった。
今回の不正アクセス事案発生原因は、ＶＰＮ機器製造業者であるＣ社の過失・脆弱性に起因するものであり、Ｂ社が個人情報保護法上の安全管理措置義務違反を問われることはない。」

2 ランサムウェア攻撃等の不正アクセスについて

皆さんの企業や事業所では、ランサムウェアをはじめとする不正アクセス攻撃を受けたことがあるだろうか。

2023年2月、個人情報保護委員会（以下、「委員会」という。）主催で、サイバー攻撃の高度化や不正アクセス脅威への対応をテーマとしたシンポジウムが開催された。

3 https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/setsumei_2025_soshiki.pdf
4 Virtual Private Network（仮想専用線）の略で、仮想的に専用の通路を作り、安全に通信を行う仕組みで、テレワークなどにも利用される。

©HASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

私も、基調講演[5]を行い、委員会に提出された漏えい報告のうち、第3号（不正アクセス）の発生原因の出現頻度の高い単語を大きな文字になるよう可視化した資料[6]を本コラムでも添付するので、参考としてほしい。

当該資料では、「メール」、「ファイル」、「アクセス」、「サーバー」といった基本用語に加え、「SSL_VPN」[7]、「Emotet」[8]、「ランサムウェア」等の個別の不正アクセスの攻撃形態と関連する単語も多く出現しており、様々なサイバー攻撃の脅威が迫っていることが分かる。

同時に行われた森井　昌克氏（神戸大学大学院教授（当時））の特別講演「サイバー攻撃による情報漏えい―脅威はランサムウェアだけではない！？―」[9]の内容は、大変示唆に富むものであった。

例えば、大阪市内の中小企業30社調査の結果、すべての企業がサイバー攻撃を受け、約半数が何らかの被害を受けていたにもかかわらず、それに気付いていないということが紹介された。これは、不正アクセス攻撃が、高度かつ巧妙化しており、データ漏えいの把握自体が困難であることを示している。

また、ランサムウェア攻撃は通常、突然発生するものではなく、
①調査（ポートスキャン等）
②侵入
③アンチウイルス無効化
④ログ消去
⑤情報スキャン・分析
⑥情報搾取・流出
⑦マルウェアアップデート
⑧踏み台（他サイト攻撃）
⑨ランサムウェア（暗号化・流出）（数値は筆者が付加）
という周到な準備を経るパターンが多く、「サイバー攻撃の本質は、認識できないことである」という説明[10]であった。

こうした発見・防御がなかなか困難となってきている不正アクセス攻撃にいかに対処し、また、攻撃を受けた場合でも、いかに被害を最小化するかが、多くの企業にとっても大変重要である。

5　ppc.go.jp/static/movies/230216Symposium02.mp4　（松元基調講演動画 20 分）
6　230216Keynote_lecture_2.pdf
7　暗号化の際にWeb上で用いられるSSL（Secure　Sockets　Layer）技術を利用したVPN方式。リモートワークなどで多く利用されている。
8　メールを使って拡がるウイルスで、メールに添付されたファイルやリンク先をクリックすること等により感染する。ランサムウェアなどの二次感染につながるケースも多い。
9　ppc.go.jp/static/movies/230216Symposium03.mp4　（森井氏特別講演動画 30 分）
10　230216Special_lecture.pdf

ⒸHASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

3 個人情報保護法上の安全管理措置義務

不正アクセスによる漏えい被害は、個人情報に限らず、企業の機密情報や秘密情報など多岐に渡っており、法的観点として個人情報保護法（以下、「個情法」という。）のみの問題ではなく、財産窃取目的や詐欺目的などの観点から犯罪行為として構成される可能性のあるものもある。

個人データの漏えい等報告の内容等については、本ニューズレター（2025年7月号）で詳報したが、2025年10月から、マルウェア事案については、事業者の負担軽減、対応迅速化等のため、委員会への報告についても、政府共通様式による報告が認められるようになった[11]。この共通様式をみても、対象となる手続きについて、個情法のみならず、電気通信事業法、放送法等の法律、航空分野等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ガイドライン等の各種ガイドライン及び監督指針、警察への相談など多数が記載されている。

しかしながら、不正アクセスによる被害においては、攻撃者が搾取するデータのほとんどに個人データが含まれるケースが多いことから、やはり個情法の法的義務に基づく対応が重要となる。

個情法第23条では、安全管理措置義務として、「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀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なければならない。」と規定されている。

本規定の解釈については、ガイドライン[12]に示されており、個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならないが、当該措置は、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならないとされている。

当然のことであるが、例えば、従業員100人の個人データと顧客10万人の個人データでは、個情法上の必要な安全管理措置の内容やレベルは、異なってくるということである。

4 不正アクセスに対する安全管理措置義務

それでは、多種多様な形態のある不正アクセス攻撃に対する個情法上の安全管理措置としては、企業は、具体的に何に取り組めば、その義務を果たせることとなるのであろうか。

具体的に講じなければならない措置や当該措置を実践するための手法の例等については、ガイドラインの「10（別添）講ずべき安全管理措置の内容」[13]に記載されている。

なお、ここで記載されている具体的な例示については、その全てを実行しなければならないものではなく、その一部での対応でも十分な措置として認められる場合もある。また、個人データの内容・量によっては、例示以外の、他

11 https://www.cyber.go.jp/policy/group/cyber/yoshikiichigenka.html
12 https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a3-4-2 3－4－2参照
13 https://www.ppc.go.jp/files/pdf/250601_guidelines01.pdf 168頁以下

ⒸHASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

の措置が必要な場合もあるので、リスクベースでの取組みが重要となる。

また、従業員100人以下の中小規模事業者については、その他の個人情報取扱事業者と同様に、同法第23条に定める安全管理措置を講じなければならないが、取り扱う個人データの数量及び個人データを取り扱う従業者数が一定程度にとどまること等を踏まえ、円滑にその義務を履行し得るよう、比較的実行容易な手法例が別に示されている事項がある。

ただし、最近では、中小規模の事業者においても、何十万人、何百万人といった個人データ量を扱うビジネスも容易に展開できるDX基盤の発達もある。そこで、従業員100人以下であっても、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去6月以内のいずれかの日において5,000を超える者や、委託を受けて個人データを取り扱う者は上記事項の適用が除かれているので、十分注意が必要である。

個情法上に基づく安全管理措置は、大きく
①組織的安全管理措置
②人的安全管理措置
③物理的安全管理措置
④技術的安全管理措置
⑤外的環境の把握
の5つの区分により規定されている。そして不正アクセスに対する対策の中心は、④技術的安全管理措置　である。

5 不正アクセスに対する具体的安全管理措置

個人情報取扱事業者は、情報システム（パソコン等の機器を含む。）を使用して個人データを取り扱う場合（インターネット等を通じて外部と送受信等する場合を含む。）、技術的安全管理措置として、
①アクセス制御
②アクセス者の識別と認証
③外部からの不正アクセス等の防止
④情報システムの使用に伴う漏えい等の防止
の4つの措置を講じなければならない。

もちろん、不正アクセス対策として直接有効なものは③外部からの不正アクセス等の防止であるが、①から④すべてが不正アクセス対策として重要である。

①アクセス制御

担当者及び取り扱う個人情報データベース等の範囲を限定し、不要なアクセス制御を行わなければならない。

不正アクセス対策関連においても、例えば、顧客の氏名、住所、電話番号等の個人情報を、商品発送部署等の担当部署以外の従業員も閲覧可能な状態であるとすると、その担当部署以外の従業員のパソコンが不正アクセスを受けた場合、顧客の個人データ全体に被害が及ぶリスクが拡大する。

ⒸHASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

ここでは具体的な対策の手法としては、以下が例示されている。

・個人情報データベース等を取り扱うことのできる情報システムを限定する。
・情報システムによってアクセスすることのできる個人情報データベース等を限定する。
・ユーザーIDに付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる従業者を限定する。

【中小規模事業者の手法例示】

個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する。

②アクセス者の識別と認証

個人データを取り扱う情報システムを使用する当該従業者が正当なアクセス権を有する者であることを、識別した結果に基づき認証（確認）しなければならない。

不正アクセス対策関連としては、例えば、ブルートフォース攻撃[14]の場合、比較的容易に類推されるようなID及びパスワードだと、すぐに個人データの漏えい等につながる。また、大量かつ重要な個人データを扱っている場合に、生体認証等を組み合わせた多要素認証を導入せず、一つのパスワードのみで対応していると、管理者一人のパソコンがマルウェア感染し、この一つのパスワードが窃取されるのみで、重要な個人データ全体が危機に晒される。

ここでは具体的な対策の手法としては、以下が例示されている。

・ユーザーID、パスワード、磁気・ICカード等の利用

【中小規模事業者の手法例示】

機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、個人情報データベース等を取り扱う情報システムを使用する従業者を識別・認証する。

③外部からの不正アクセス等の防止

個人データを取り扱う情報システムへの外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。

不正アクセス対策の関連としては、例えば、病院等において、自社のシステムはインターネットに繋がっておらず、クローズドなネットワークシステムとなっているので不正アクセスのリスクはないと捉えられていた具体的事例があるが、保守点検時に基本OSやソフトウェア等のバージョンアップ等でインターネットに繋ぐケースが想定され、それを狙った攻撃などが報告されているので、油断せず、同様の注意が必要である。

また、最近ではテレワーク等の導入が進んでいるが、その際にVPN機器の接続で対応としているケースが多い。しかし、このVPN機器の脆弱性を狙った不正アクセス攻撃が多発化している。

14 考えられる全てのパスワードを使って、総当たりでログインを試みる攻撃手法。

ⒸHASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

ここでは具体的な対策の手法としては、以下が例示されている。

・情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。
・情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入し、不正ソフトウェアの有無を確認する。
・機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。
・ログ等の定期的な分析により、不正アクセス等を検知する。

【中小規模事業者の手法例示】

・個人データを取り扱う機器等のオペレーティングシステムを最新の状態に保持する。
・個人データを取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。

ここでは、不正アクセス対策の態様毎の専門的かつ個別的な対応まで具体的に記載されている訳でないが、いずれも基本的な対策として記載された重要事項であり、留意が必要である。

④情報システムの使用に伴う漏えい等の防止

情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用しなければならない。

不正アクセス対策関連でも、通信経路や内容の暗号化など、ソフトウェアの基本機能の活用も含めて、被害軽減につながる重要事項である。

ここでは具体的な対策の手法としては、以下が例示されている。

・情報システムの設計時に安全性を確保し、継続的に見直す（情報システムの脆弱性を突いた攻撃への対策含む。）。
・個人データを含む通信の経路又は内容を暗号化する。
・移送する個人データについて、パスワード等による保護を行う。

【中小規模事業者の手法例示】

メール等により個人データの含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する。

6 クイズ1の解答

クイズ1の設例では、漏えい等した個人データの件数が約20万件にのぼり、VPN機器の脆弱性情報について、半年前から公開されていたにもかかわらず、未対応となっている。

個情法第23条の安全管理措置義務に対応したガイドラインからすれば、前述の技術的安全管理措置　③外部からの不正アクセス等の防止措置　の具体例として挙げられた「ソフトウェア等の最新状態への対応」の放置等が認められ、個情法上の安全管理措置義務違反となり得る。

ⒸHASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

実際に委員会が個情法第147条に基づく指導を行った事例において、事業者のサーバーがVPN経由で不正アクセスを受け、ランサムウェアに感染した結果、従業者及び顧客の個人データについて毀損及び漏えいのおそれが生じた事案において、事業者が当該VPN機器について脆弱性の情報が公開されていたにもかかわらず対応を行わないまま放置していたことが指摘されている[15]。

したがって、クイズ1の正解は、「誤り」ということになる。

ソフトウェア等の脆弱性については、自動更新による対応のものも多いと思われるが、一部ソフトウェア等については対応方法がリリースされているなど利用者の能動的な更新対応が必要なものもある。特に、顧客の大量の個人データを管理している企業においては、これらを放置せずに、迅速に対応することが重要である。

なお、情報セキュリティの脆弱性情報については、IPAからも随時情報が出されている[16]ので、活用願いたい。

（次号に続く）

15 https://www.ppc.go.jp/files/pdf/250924_shiryou-2-1.pdf 6頁24番
16 https://www.ipa.go.jp/security/vuln/index.html

本ニューズレターは、一般的な情報を提供する目的で作成されたものであり、特定の事実関係を前提とする具体的な法的アドバイスを提供するものではありません。本ニューズレターで紹介する法令又は判例の個別事案に対する適用可能性につきましては、具体的な事実関係に依拠することになりますので、弁護士等の専門家にご相談ください。また、本ニューズレターの記載のうち、意見もしくは見解にわたる部分は執筆担当者の個人的な見解であり、当事務所もしくは当事務所のクライアントの見解又はそれらの見解を代表するものではありません。

本ニューズレターの内容につきましてお問い合わせ等ございましたら、執筆担当者までご遠慮なくご連絡下さいますよう、お願い致します。また、本ニューズレターの配信の停止をご希望の場合には、newsletter@hashidatelaw.com(ニューズレター専用)までご連絡下さいますよう、重ねてお願い申し上げます。

Contact Information

弁護士法人外立総合法律事務所には、本ニューズレターでご紹介した事案以外も行政事件訴訟を担当しております。また、行政庁での勤務経験を有する弁護士を含め、複数の行政事件について経験・実績を有する弁護士が多数所属しており、行政事件業務の経験と実績を着実に積み重ね、あらゆる種類の行政事件案件につき、被告側として受任した事件は全て勝訴判決に導いており、最良のサービスを提供出来る体制を整えております。

弁護士法人外立総合法律事務所
HASHIDATE LAW A PROFESSIONAL LAW CORPORATION
〒100-0011 東京都千代田区内幸町 1-1-1 帝国ホテル本館 5 階
TEL: 03-3504-3800（代表） FAX: 03-3504-1009（代表）
URL: https://www.hashidatelaw.com/
Email: kenjihashidate@hashidatelaw.com

ADDLESHAW GODDARD LLP
Milton Gate, 60 Chiswell Street, London,
EC1Y 4AG, United Kingdom, DX 47 London
TEL: +44 (0)20 7606 8855 FAX: +44 (0)20 7606 4390
URL: https://www.addleshawgoddard.com/en/

ⒸHASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved