弁護士法人外立総合法律事務所
HASHIDATE LAW
A PROFESSIONAL LAW CORPORATION
January, 2026

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. 18

個人情報の保護と利活用のすすめ　Vol. 10

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（Ⅱ）不正アクセスの実態とその具体的対策

7　最近の不正アクセスの実態とその傾向

前月号では、個情法上の不正アクセスに対する安全管理措置義務の制度的な内容について整理したが、今月号ではその具体的対策について、より踏み込んだ検討を行うこととする。

まず、最近の不正アクセスの実態および個情法上の指導等の状況について、直近の令和7年度上半期のデータを基に分析する[17]。

令和7年度上半期において、個情法第147条に基づく民間事業者に対する指導・助言（以下、「指導等」という。）は232件行われている。その原因として不正アクセスが130件（全体の約56％）と最多であり、漏えい等報告の遅延を理由とする92件（約40％）よりも多くなっている。（事項が重複するものもあり、合算して総計と一致しない場合もある（以下同じ）。）

17 データについては、委員会が四半期毎に公表している監視・監督権限の行使状況の概要
https://www.ppc.go.jp/files/pdf/250924quarter-report_kengenkoushi.pdf 及び
https://www.ppc.go.jp/files/pdf/251210quarter-report_kengenkoushi.pdf 使用

©HASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

不正アクセスの要因別件数も公表されているが、全体130件の不正アクセスのうち、

①ソフトウェア製品等の脆弱性の放置　　が66件と最も多く、
②推測されやすいID・パスワードの設定　　が47件、
③アクセス制御の設定ミス　　が15件となっている。

①ソフトウェア製品等の脆弱性の放置 については、その内訳として、前月号でも取り上げたVPNの脆弱性が23件、ECサイトの脆弱性が10件と多くなっている。

攻撃手法の内訳は、ランサムウェア攻撃が52件と突出して多く、その他、ECサイトへのクロスサイトスクリプティング攻撃[18]が7件、ブルートフォース攻撃[19]が6件、ウェブサイトへのSQLインジェクション攻撃[20]が2件などとなっている。

指導等の内容は、個情法第23条の安全管理措置義務違反に関するものが162件と大半を占める。その中でも、前月号で説明した技術的安全管理措置に関するものが140件と圧倒的多数である。更にその内訳は、前月号の5「不正アクセスに対する具体的安全管理措置」の ③外部からの不正アクセス等の防止 が71件、②アクセス者の識別と認証 が44件、④情報システムの使用に伴う漏えい等の防止 が14件、①アクセス制御 が11件となっている。なお、技術的安全管理措置に関する指導ではないが、安全管理措置義務違反に関する指導の内訳は、組織的安全管理措置を内容とするものが16件、人的安全管理措置が4件、物理的安全管理措置が2件と、技術面以外の違反にも及ぶものが一定数あることに留意が必要である。

各事業者においては、こうした最近の不正アクセス攻撃の具体的傾向や、委員会による指導等の対象となった安全管理措置区分の状況等を踏まえた、メリハリのある対応の検討が求められる。

8 不正アクセス事案の具体的内容

令和7年度上半期に報告された不正アクセス事案のうち、最近の特徴的な傾向を示すものとして、以下の4点について、具体的に説明する。

(1)VPNの脆弱性

【事案の概要】

事業者のサーバがVPN経由で不正アクセスを受け、顧客や従業者の特定個人情報[21]を含む個人データについて漏えいのおそれが生じた事案である。

18 ウェブサイトの脆弱性を悪用して、攻撃者が用意した悪意のあるスクリプトを利用者の元に送り込んで実行させる攻撃手法。典型的には、ECサイト上に不正なファイルを作成し、そこに利用者が入力したクレジットカード情報を含む個人データを蓄積の上、外部へ転送する形で窃取するもの。

19 前月号脚注 14 参照（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。）

20 利用者からの入力情報を基に組み立てられるデータベースへの命令文（SQL文）に対して適切な取扱いをしていないことに起因して、データベースを不正に操作されるSQLインジェクションの脆弱性を突いた攻撃。

21 マイナンバーを含む個人情報。

ⒸHASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

【発生原因】
①当該VPN機器には脆弱性が複数確認されていたにもかかわらず、事業者が保守業者（個人データの取扱いの委託関係ではない。）との間でアップデート等について取決めをしていなかったことから、当該脆弱性への対応が実施されていなかった
②当該VPN機器のパスワードの強度自体に問題があった
等である。

（2）ECサイトの脆弱性
【事案の概要】
ECサイトを運営している場合において、当該ECサイトを通じて事業者のデータベースがブルートフォース攻撃による不正アクセスを受け、顧客の個人データについて漏えいのおそれが生じた事案である。

【発生原因】
①当該ECサイトの管理画面に対する、IPアドレス等を用いたアクセス制限が設定されていなかった
②利用されたアカウントのパスワードの強度が不十分であった
等である。

（3）推測されやすいID・パスワードの設定
【事案の概要】
VPN経由で不正アクセスを受けてランサムウェアに感染し、ファイルが暗号化され、株主・従業者等の個人データについて、漏えい及び毀損が生じた事案である。

【発生原因】
①不正アクセスに利用されたVPNアカウントの、認証情報の強度が不足していた
②当該VPN機器の脆弱性が公表されていたにもかかわらず放置していたため、その脆弱性を突かれた
等である。

（4）アクセス制御の設定ミス
【事案の概要】
クラウドストレージサービスが不正アクセスを受け、ランサムウェア感染によって、当該ストレージ内の全データが削除され、顧客個人データについて滅失及び漏えいのおそれが生じた事案である。

【発生原因】
当該ストレージサービスでは、登録されたIPアドレスのみを利用可能とする設定ができたが、事業者がIPアドレス制限等を実施していなかったこと 等である。

ⒸHASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

9 不正アクセスに対する具体的セキュリティ対策の検討

ここまで、近時の不正アクセス事案の実態と傾向について具体事例も交えながら説明してきた。事業者としては、ランサムウェア攻撃を中心に、攻撃が巧妙化かつ組織化している現状を踏まえ、いかなる具体的セキュリティ対策を講じるべきか検討する必要がある。

そこで以下、令和6年12月に個人情報保護委員会より公表された「不正アクセスによる個人データ漏えい防止のための注意喚起[22]」の8類型

① 脆弱性が放置された事例
② 脆弱性への対応が遅れた事例
③ 不正ログインの事例
④ グループ会社や海外拠点が狙われた事例
⑤ グループ会社間のアクセス制御不備があった事例
⑥ 個人領域に保存していたデータの漏えい事例
⑦ グループ会社への監督が不十分な事例
⑧ 利用するクラウドサービスからの漏えい事例

の事例を参考として、特に重要と思われる5つの類型（①②③⑤⑥）についてその具体的対策を検討することとしたい。

① 脆弱性が放置された事例

【パターンの概要】

前月号のクイズ1でも取り上げ、また前述のとおり、最近の不正アクセス事案発生の傾向としても多いものである。事業者が個人データを取り扱うために導入した情報システムについて、定期的にソフトウェア等のアップデート等が行われず、さらに、脆弱性が公開され対処方法がリリースされていたにもかかわらず、対策を放置していたことにより、不正アクセスによる個人データの漏えい等を防ぐことができなかったパターンである。

【発生原因】

特に、

・インターネットの接続を制御する装置ともなるVPN機器について、そのバージョンアップが必要であるが、その更新がなされなかった

また、

・システム業者との間で、情報システム導入の業務委託契約しか締結しておらず、セキュリティ対策に関するシステム保守の業務委託契約を締結していないこと

もその要因の一つとされている。

22 https://www.ppc.go.jp/files/pdf/241211_warning.pdf

ⒸHASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

【具体的対応策】

まずは、VPN機器の重要性とその用途を正しく理解することが必要である。VPN機器は、サーバやストレージ等の、それ自体が明確に管理・利用される機器と異なり、ネットワークサービスの一部として提供されるケースがある。その場合、運用体制が不明確となることも多い。このことから、適切なシステム業者を選定し、情報システムの脆弱性対策等、セキュリティ対策も含めたシステム保守の業務委託契約を締結することが有効である。

また、管理対象となるIT資産の洗い出し、脆弱性情報の収集・分析、脆弱性への対処といった脆弱性対策プロセスの確実な実行も重要である。この点に関しては、本コラムの2025年5月号「まずは知るところから。データマッピングのすすめ」[23]で指摘したとおり、データマッピング手法も活用して、まずは経営層及び幹部社員が個人データの状況を可視化し、その在りかを知ることが重要ではないか。前号で紹介したとおり、そもそも個人データの漏えい自体に気付いていない不正アクセス事案も多いことを再認識すべきである。

② 脆弱性への対応が遅れた事例

【パターンの概要】

グループ会社全体の情報システムを管理する親会社が、グループの複数会社が使用する情報システムに脆弱性が公開された際、グループ会社にセキュリティパッチを適用するよう指示したが、一部の子会社が適時に対応できなかったため、脆弱性を悪用された不正アクセスを受けたものである。

【発生原因】

・一部の子会社にはシステム対応を行うための人員が十分におらず、リソースの問題から、すぐにセキュリティパッチ適用作業を行うことができなかった
・親会社において資産管理が適切に行われておらず、脆弱性情報が公開されていることに気づくのが遅く、対応が遅れてしまった

子会社も含めた共通基盤でシステムを運用するケースも多いが、攻撃者は、対策の弱い子会社を見つけ出し、そこを踏み台として、重要かつ膨大な個人データの入った親会社のデータへの侵入を試みるパターンが多発している。グループ会社全体の漏れのない対応が重要となる。

【具体的対応策】

グループ全体のセキュリティガバナンス向上のため、脆弱性情報収集・分析の一元管理のみならず、セキュリティパッチ適用等の対策状況を含めて一元管理することも重要である。

前述のとおり、子会社も含めた漏れのない対応が不可欠であり、人材的に不足している子会社の対応について、親会社としても管理・支援が必須となる。

23 Microsoft Word - HLO Newsletter May 2025_HP²（_0530_6jW.docx 4頁下段参照

ⒸHASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

③ 不正ログインの事例

【パターンの概要】

個人データを取り扱う情報システムにログインするための本人認証の際、利用者が正当なアクセス権を有する者であることについて、識別した結果に基づき認証しなければならないが、不十分な識別・認証による不正ログインを許し、個人データの漏えい等が発生するものである。

【発生原因】

・桁数が少ないなど推測されやすいID・パスワードを使用していた
・複数回以上のID・パスワードの入力ミス時はアカウントを一定時間ロックするなど、ブルートフォース攻撃に対する対策が未実施であった
・過去の脆弱性によりID・パスワードが漏えいしており、脆弱性に対するセキュリティパッチは適用していたものの、ID・パスワード初期化等の措置を未実施であった

が挙げられている。

【具体的対応策】

推測されにくい複雑なパスワードを利用するよう従業者を教育することが必要であるが、ID・パスワードの桁数や文字種類の組み合わせ数などについて、組織的なルール作りとそのシステム制御も重要であろう。

また、取り扱う個人データの量・機密性に応じて、多要素認証等の高い強度の認証方式を採用することも必要である。大規模な事案では、はじめに個人データへの管理者権限を有すると推測される者に対する攻撃を行い、そのID・パスワードを摂取するケースが多い。その場合でも、生体認証等を組み合わせた多要素認証を導入していればシステム侵入を阻止できる場合も多いので、リスクベースの多角的な検討が重要である。

また、脆弱性等によりID・パスワードが漏えいした可能性がある場合は、ID・パスワードの初期化・変更を案内することも挙げられている。攻撃の第一歩として、HP上の氏名等の公開情報を用いて管理者権限を有すると思われる経営者及び幹部社員を特定し、当該者のメールアドレスを推定する攻撃も多いことから、氏名のみでなく、ランダムの文字列等も取り入れたメールアドレスへの変更も、第一次防御として有効であると考えられる。

⑤ グループ会社間のアクセス制御不備があった事例

【パターンの概要】

親会社がグループ会社全体の情報システムを一括管理するデータセンターを保守・管理しているが、同データセンター内のアクセス制御が不十分であるケースにおいて、グループネットワークへの不正アクセス攻撃があり、グループ会社全体の情報システムにて個人データの漏えい等が発生したものである。

【発生原因】

・グループ会社の個人データを管理するデータセンターにおいて、業務上の利便性等の観点から、グループ会社間で相互にアクセス可能としていた
・親会社が管理するグループネットワークの管理者パスワードの強度が十分ではなかった

ⒸHASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

が挙げられている。

個人データの漏えい等事案が発生した場合において、その被害を最小限にとどめるためにも、個情法上の安全管理措置義務に規定されているアクセス制御、及びアクセス者の識別と認証の徹底が重要である。

【具体的対応策】

グループ会社であっても業務上の必要最小限の範囲でアクセス制御を行い、同一のデータセンターで一元管理していても各会社の業務システムを極力分離独立し、管理・運営することが必要である。

従業員情報などグループ全体での管理が必要な情報は、各社人事部門関係間のアクセスを認容するルールもあるかもしれない。しかし、例えば各社毎に保有している顧客情報など、グループ他社に直接関係のないものについては、的確なアクセス制御を実施して分散管理することが重要と思われる。

また、推測されにくい複雑なパスワードを利用すること、管理者権限等の不正利用された際の被害が大きいアカウントには、多要素認証等の高い強度の認証方式を採用することも重要である。

これらの対策は、当然コスト増にもつながるものでもある。リスクに対応した的確な検討と対策の選択が重要と考えるが、規模の大きな個人データを有する事業者においては、多要素認証導入が必須の状況に至っているのではないか。

⑥ 個人領域に保存していたデータの漏えい事例

【パターンの概要】

事業者の従業者が業務で使用する電子ファイル等（個人データを含む。）を個人が管理する領域に保存しており、事業者の情報システムが不正アクセスを受けた際、個人が管理する領域に保存されていた個人データについても漏えいが生じるものである。

【発生原因】

・従業者が業務で使用する電子ファイルが、組織として管理されていない
・各自のデスクトップ等で加工・保存される業務運用が慣例化してしまっており、管理状況について定期的な監査等の網にかからなかった

ものである。

組織として管理されていない個人データの中には、本来は消去すべき古いデータ等が含まれているケースがあり、漏えい被害の影響が拡大するおそれがある。

【具体的対応策】

事業者における個人データの取扱いは、あらかじめ整備された個人データの取扱いに係る規律・ルールに従うことが挙げられている。その前提として、個人データの取扱規定について、あらかじめ再点検等を行うことが重要であろう。

ⒸHASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

また、個人情報管理台帳等を整備し、定められた保存場所で個人データの作成・加工・保存を徹底すること、個人データを組織で管理し、取扱職員・管理媒体等を監査部門が把握した上で、定期的な監査等を行うことが必要である。

組織的安全管理措置義務に対応した、定期的かつ的確な監査の実施が重要である。

10 不正アクセス攻撃への対応の要諦

ここまで、個人情報保護法上の制度と最近の不正アクセスの実態・傾向について、二号にわたって、具体的事例を交えながら、理解を深めてきた。

不正アクセス攻撃は、それ自体が犯罪行為である可能性が高いものであり、攻撃を受けた事業者側としては、「自分たちは被害者である」という意識が強いかもしれない。しかしながら、結果として、個人データの漏えい等の被害が発生すると、

・当該個人データ本人個人の人権、財産権等の侵害
・企業の経営維持の困難性の問題
・企業と関係する顧客や関連事業者等への被害の連鎖

など、甚大な課題が発生する。

したがって、何らかの個人データを扱うことにより業を成している事業者においては、法に則り、個情法上の不正アクセスの防止等の安全管理措置義務を遵守することが必要である。

前月号冒頭のA大手ビール等販売グループ会社の事案のように、不正アクセスの攻撃自体が巧妙化かつ高度化しており、特に中小規模事業者においては、コスト面も含めて、対策がなかなか困難となりつつあるのも事実である。しかし、まずは**【パスワードの強化】**や**【OSやソフトウェアの適時のアップデート】**など、比較的実行が容易なものを確実に実施する[24]ことが肝要と考える。攻撃者は、必ず、多数の事業者を比較検討して、侵入容易なところを見付け出して攻撃する。この対応だけでも、一定程度被害を軽減することができる。

不正アクセス攻撃発生時には、初動対応が特に重要となる。近時最も多くなっているランサムウェア攻撃発生時の初動対応としては、

・感染端末及び感染が疑われる端末からLANケーブルを抜くとともに、無線LANを無効にすること。
・感染端末等の再起動や電源オフをしないこと。既に感染端末等の電源がオフの場合はオンにしないこと。
・ウイルス対策ソフトによる感染端末等のフルスキャンをしないこと。
・ネットワーク機器の再起動や電源オフをしないこと。
・ファームウェアやOSのアップデートをしないこと。

以上の5点が、前月号で紹介した政府のランサムウェア事案共通様式にも示されているので参考としてほしい。

24 https://www.ppc.go.jp/files/pdf/241205_chuushou_leaflet.pdf

ⒸHASHIDATE LAW A PROFESSIONAL LAW CORPORATION
All Rights Reserved

不正アクセス攻撃への対応準備としては、まずは日常的な取組として、どこに個人データがあり、どのようなリスクがあるかを、データマッピング手法も活用し、それを経営層も含めて可視化・共有化することが大前提かつ重要であると考えている。そもそも、自社のどこに個人データがあるかが分からなければ、不正アクセス攻撃を受け、個人データが漏えい等していることすら、気付くことができなくなってしまう。

次に、不正アクセスによる個人データ漏えい等事案の最小化を目標にするとともに、事案が発生した際の被害の最小化とその後のPDCAサイクルの迅速化も重要である。

大きな不正アクセス事案は、突然発生するものではなく、それを防げる可能性のあるいくつもの小さなヒヤリハット事例の積み重ねが事前にあるケースが多いと私は考えている。

不正アクセス事案発生時は、事案を極小化・極大化して対応するのではなく、経営層を中心として、事態の適正分析と迅速な対応が必要である。

そして、そのためには、日頃の研修や訓練の繰り返しが大事である。

私は、東日本大震災発生時に、総務省消防庁の救急企画室長として、東京電力福島第一原子力発電所での消火・放水、救急救助業務に携わったが、実際の事故・事案では、想定外の事象が発生するのは当然であり、想定外の事象にも迅速かつ的確に対応しなければならない。しかし、そこで強く感じたのは、それまで日々行ってきた様々な想定訓練・研修があったからこそ、想定外の事案にも一定の対応ができたのでは、ということである。

不正アクセス事案についても、防災訓練等と同様、日常的に研修・訓練をしっかりと行い、想定外の事案にも対応できる能力の開発に努めることが重要ではないだろうか。

どれだけシステムやセキュリティ対策に投資しても、最後は、それを扱う人の問題に帰結する。研修・訓練内容は、本コラムでの具体的検討事例、自社のヒヤリハット事例、他同業者の事案など実践的なものとし、繰り返し定期的に実施することが重要と考えている。

本コラムが、皆さんの企業での不正アクセス攻撃に対応した個人データ保護の取組強化の一助となれば幸甚である。

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