資料２－１

令和７年〇月〇日
個人情報保護委員会

令和６年度第４四半期における監視・監督権限の行使状況の概要

・個人情報保護委員会（以下「委員会」という。）は、漏えい等事案に関する報告の受理等による不断の監視のほか、報告徴収・立入検査等により収集した情報等に基づき、確認、調査及び分析を進めた上で、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）及び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 25 年法律第 27 号。以下「マイナンバー法」という。）に基づき、指導、勧告等を行う権限を有している。
・令和６年度第４四半期における委員会の監視・監督権限の行使状況の概要は、以下のとおり。

Ⅰ　公表事案

権限行使日	対象	権限行使の内容	法令	参照箇所
令和７年１月 30 日	株式会社ビーバーズ	勧告及び報告徴収	個人情報保護法	株式会社ビーバーズに対する個人情報の保護に関する法律に基づく行政上の対応について（https://www.ppc.go.jp/files/pdf/250129_2_houdou.pdf）
令和７年３月 19 日	株式会社イセトー	指導	個人情報保護法	株式会社イセトーに対する個人情報の保護に関する法律に基づく行政上の対応について(https://www.ppc.go.jp/files/pdf/250319_houdou.pdf）

Ⅱ　その他の権限行使

１ 個人情報保護法

(1) 指導・助言（第 147 条又は第 157 条）　計 116 件

ア　民間事業者　計 90 件

・不正アクセスを原因とする漏えい等事案を中心に、安全管理措置の不備等について指導を行った。
・不正アクセスによる漏えい等の原因として、①VPN（Virtual Private Network）機器の脆弱性やECサイトを構築するためのアプリケーション等の脆弱性が公開され、対応方法がリリースされていたにもかかわらず、事業者が放置していたこと、②ID・パスワードが容易に推測されやすいものとされていたこと、③設定ミスによりデータベースへのアクセス制御が不適切な状態になっていたことなど、安全管理措置に不備があったケースが多くみられている。
・攻撃種類としては、ブルートフォース攻撃[1]、ECサイトのクロスサイトスクリプティング攻撃[2]や、ウェブサイトのSQLインジェクション攻撃[3]などがみられているほか、ランサムウェア攻撃[4]も、13件みられている。
・不正アクセス以外の漏えい等事案では、生徒等の情報が保存されたハードディスクの紛失などがみられている。
・このほか、特定された利用目的の達成に必要な範囲を超えた会員の個人情報の利用（個人情報保護法第 18 条第１項違反）や、不適正な個人情報の利用（同法第 19 条違反）、本人の同意を得ていない個人データの第三者提供（同法第 27 条第１項違反）といった事案もみられた。

---

[1] ブルートフォース攻撃とは、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である。
[2] クロスサイトスクリプティング攻撃とは、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であり、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というものである。
[3] SQLインジェクション攻撃とは、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である。
[4] ランサムウェア攻撃とは、感染するとPC等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭や暗号資産）を要求する不正プログラムを用いた攻撃手法である。

・指導等の内容としては、特に技術的安全管理措置に関し、外部からの不正アクセス等の防止の不備が最も多く（32 件）、次いで、アクセス者の識別と認証の不備（12 件）が多かった。このほか、委託先に対する監督の不備（２件）、組織的安全管理措置の不備（２件）などに対して指導を行った。

・下表の事案対応のほか、漏えい等報告の提出の遅延に関し、45 件の指導を行った。

	事案の概要	指導事項
１	事業者が利用していた IT インフラが不正アクセスを受け、事業者の顧客、従業者及び取引先の個人データについて漏えいのおそれが生じた事案。当該 IT インフラのアクセス検証の際に用いたセキュリティが脆弱な検証用アカウントが削除されず残置され、当該アカウントから当該 IT インフラに侵入されたこと、事業者が当該 IT インフラの利用のため使用している NAS（Network Attached Storage）が、社内ネットワーク内ではユーザ認証を経ずにアクセス可能な状態であったこと等が原因と考えられる。	技術的安全管理措置（外部からの不正アクセス等の防止）
２	事業者が運営している施設のウェブサイトが SQL インジェクション攻撃による不正アクセスを受け、データベース内の個人データが窃取され、顧客の個人データについて漏えいが生じた事案。事業者による SQL インジェクション攻撃への対策が不十分であったことが原因と考えられる。	技術的安全管理措置（外部からの不正アクセス等の防止）
３	事業者が提供するクラウドサービスを構成するサーバが不正アクセスを受け、当該サーバに保存されていた、委託元である事業者の従業者及び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。事業者のファイアウォールの通信設定に不備があり、外部から制限なくアクセス可能な設定となっていたこと等が原因と考えられる。	技術的安全管理措置（外部からの不正アクセス等の防止）
４	事業者が販売する商品の発送業務及びそれに伴う個人データの取扱いを委託していたところ、委託先である事業者の倉庫管理システムが、不正アクセスを受け、ランサムウェアに感染した結果、事業者の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。事業者は、約７年間、委託先である事業者に個人データの取扱いを委託していたところ、発送に使用した顧客の個人データの保持状況（廃棄状況）について定期的な確認を一切しておらず、その結果、多数の顧客の個人データについて漏えいのおそれが生じたため、委託先の監督について不備が認められた。	委託先の監督
５	事業者のサーバが 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、ファイルが暗号化され、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。サポート切れの VPN 機器の利用を継続していたこと等が原因と考えられる。	技術的安全管理措置（外部からの不正アクセス等の防止）
６	事業者は SaaS（Software as a Service）を自ら開発し、顧客企業等に提供しているところ、当該 SaaS の顧客企業の担当者等に関する個人データが保管されていたサーバが、VPN 経由で不正アクセスを受け、	技術的安全管理措置（アクセス者の識別と認証、外部

	事案の概要	指導事項
	ランサムウェアに感染した結果、ファイルが暗号化され、当該個人データについて漏えいのおそれが生じた事案。VPN 機器の認証パスワード及び、当該サーバの AD（Active Directory）サーバの管理者権限に関する認証情報（ID・パスワード）の強度に問題があったこと等が原因と考えられる。	からの不正アクセス等の防止）
7	事業者は入会を希望する会員から個人情報を取得していたところ、当該個人情報を、利用目的である「会員管理」とは無関係の目的に利用していた。あらかじめ本人の同意を得ないで、個人情報保護法第 17 条第１項の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱っていたため、個人情報保護法第 18 条第１項の規定違反が認められた。	利用目的による制限 （個人情報保護法第 18 条第１項の規定違反）
8	事業者が運営する EC サイトに対し、クロスサイトスクリプティング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。事業者が利用する EC サイト構築システムに関し、脆弱性情報や対策等が公表されていたにもかかわらず対応を行わないままであったこと等が原因と考えられる。	技術的安全管理措置 （アクセス者の識別と認証、外部からの不正アクセス等の防止）
9	事業者が提供するクラウドサービス及び社内システムが、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、ファイルが暗号化され、委託元である事業者の顧客の個人データについて漏えいが生じた事案。当該クラウドサービスでは、仮想基盤ホストサーバを利用していたところ、同サーバの脆弱性の存在が公表されていたにもかかわらず対応ができていなかったこと、当該サーバの管理者アカウントについて、パスワードの強度に問題があったこと等が原因と考えられる。	技術的安全管理措置 （アクセス者の識別と認証、外部からの不正アクセス等の防止）
10	事業者の DB サーバで利用している CMS（Contents Management System）のログインページが、ブルートフォース攻撃による不正アクセスを受け、不正ファイルが設置されたことにより、学生の個人データについて漏えいが生じた事案。当該 DB サーバの認証に使われていたパスワードの強度に問題があったこと等が原因と考えられる。	技術的安全管理措置 （アクセス者の識別と認証）
11	事業者が運営する EC サイトで利用している CMS のログインページが、ブルートフォース攻撃による不正アクセスを受け、不正ファイルが設置されたことにより、顧客の個人データについて漏えいが生じた事案。CMS の管理画面への適切なアクセス制御を行っていなかったこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
12	事業者のサーバが 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、ファイルが暗号化され、患者の個人データについて漏えい、毀損及び漏えいのおそれが生じた事案。事業者が、VPN 機器の脆弱性が公表され、対応方法がリリースされていたにもかかわらず適切な対応をせず放置していたこと、VPN 機器の認証パスワード（管理者アカウントと共通）の強度に問題があったこと、VPN 機器のサポート終了から約 1 年が経過した時点においても、セキュリティリスクを適切に把握及び評価しなかったこと	組織的安全管理措置 （取扱状況の把握及び安全管理措置の見直し） 技術的安全管理措置 （アクセス者の識別と認証、外部

	事案の概要	指導事項
	等が原因と考えられる。	からの不正アクセス等の防止）
13	事業者が運営するECサイトが、クロスサイトスクリプティング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。事業者が利用するECサイト構築システムに関し、脆弱性情報や対策等が公表されていたにもかかわらず対応を行わないままであったこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
14	事業者のサーバが 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、ファイルが暗号化され、従業者及び顧客の個人データ(特定個人情報を含む)について漏えいのおそれが生じた事案。VPN機器の認証情報について、パスワードの強度に問題があったこと等が原因と考えられる。	技術的安全管理措置 （アクセス者の識別と認証）
15	事業者のサーバが 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、会員の個人データについて漏えいのおそれが生じた事案。VPN機器の認証情報についてパスワードの強度に問題があったこと、一部のシステムではパスワードが使い回されていたこと、VPN機器について危険度の高い脆弱性が複数残存していたこと等が原因と考えられる。	技術的安全管理措置 （アクセス者の識別と認証、外部からの不正アクセス等の防止）
16	事業者は自らが運営するECサイトの保守・点検及びそれに伴う個人データの取扱いを他の事業者に再委託していたところ、当該ECサイトがクロスサイトスクリプティング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。事業者が利用する EC サイト構築システムに関し、脆弱性情報や対策等が公表されていたにもかかわらず再委託先である事業者が対応を行わないままであったこと等が原因と考えられる。	委託先の監督
17	事業者が提供するアプリを管理するサーバが、ブルートフォース攻撃による不正アクセスを受け、当該アプリの利用者の個人データについて漏えいが生じた事案。事業者がアプリ利用者の認証に関して設定していたパスワードルールが十分なものでなかったこと、ブルートフォース攻撃への対策を講じていなかったこと等が原因と考えられる。	技術的安全管理措置 （アクセス者の識別と認証、外部からの不正アクセス等の防止）
18	事業者のウェブサイトに存在していたPHP（Hypertext Preprocessor）の脆弱性を突いた不正アクセスを受け、ランサムウェアに感染した結果、ファイルが暗号化され、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。当該 PHP はサポートが終了しており深刻な脆弱性を含んでいた可能性があること、適切なアクセス制御を行っていなかったこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
19	事業者が提供するサービスを運用するサーバが不正アクセスを受け、サービス利用者の個人データについて漏えいが生じた事案。事業者は、当初、運営管理システムの開発を第三者に委託していたが、委託業務終了後は、当該システムの管理アカウントを当該第三者から引き継ぎ、事業者自ら保守・運用を行って	技術的安全管理措置 （アクセス制御）

	事案の概要	指導事項
	いたところ、当該引継後、当該第三者の担当者が使用していた管理者アカウントについて、認証情報の変更を行うことなくそのまま使用していたこと等が原因と考えられる。	
20	事業者に勤務する教諭が、生徒等の情報が保存されたハードディスクを紛失し、生徒等の個人データについて漏えいのおそれが生じた事案。当該教諭は、業務に必要なデータを保存して持ち歩くことが長期に渡り常態化していたこと、事業者では従業者における個人データの具体的な安全管理について定めた規程を設けておらず、外部記録媒体の接続制限や接続を感知するシステムの構築などの対策がなかったこと等が原因と考えられる。	個人データの取扱いに係る規律の整備 組織的安全管理措置 （組織体制の整備､個人データの取扱状況を確認する手段の整備、取扱状況の把握及び安全管理措置の見直し）
21	事業者のサーバが 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、委託元である事業者の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。管理者権限を持つアカウントのパスワードの強度に問題があったこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
22	事業者は、業務に利用するサーバについて、業務委託先（個人データの取扱委託先ではない。）に対してアカウントを貸与していたところ、当該業務委託先が不正アクセスを受け、当該アカウントから、当該サーバに不正アクセスされた結果、従業者等の個人データについて漏えいが生じた事案。業務委託先のネットワーク環境からもアクセスを許可していたこと、業務委託先に貸与しているアカウントの権限で参照可能な範囲に、事業者の他のサーバ等に関する認証情報が保管されていたこと等が原因と考えられる。	技術的安全管理措置 （アクセス制御）
23	事業者は、行政機関等より委託を受け、当該行政機関等のふるさと納税特設サイトを開発、公開していたところ、当該サイトが不正アクセスを受け、寄附者の個人データ（保有個人情報）について漏えい及び漏えいのおそれが生じた事案。当該サイトにおいて、SQL インジェクションの脆弱性への対応を行っていなかったことが原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
24	事業者が運営する EC サイトが、クロスサイトスクリプティング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。事業者が利用する EC サイト構築システムに関し、脆弱性情報や対策等が公表されていたにもかかわらず対応を行わないままであったこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
25	事業者のサーバが不正アクセスを受け、メールマガジンの配信先の登録情報に関する個人データについて漏えいが生じた事案。事業者はメールマガジン配信用プログラムを利用していたところ、管理者権限の窃取や任意コマンドの実行などの脆弱性が公表され、対応方法がリリースされていたにもかかわらず	技術的安全管理措置 （外部からの不正アクセス等の防止）

	事案の概要	指導事項
	放置していたことが原因と考えられる。	
26	事業者が運営するECサイトが、クロスサイトスクリプティング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。事業者が利用するECサイト構築システムに関し、脆弱性情報や対策等が公表されていたにもかかわらず対応を行わないままであったこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
27	事業者が顧客に対して、クレジットカード決済の案内手段として利用しているシステムを管理するサーバがブルートフォース攻撃による不正アクセスを受け、従業者及び顧客の個人データについて漏えいが生じた事案。当該システムの認証について設定していたパスワードの強度に問題があったこと、試行回数の制限等のブルートフォース攻撃への対策が不十分であったこと等が原因と考えられる。	技術的安全管理措置 （アクセス者の識別と認証､外部からの不正アクセス等の防止）
28	事業者のサーバが不正アクセスを受け、顧客の個人データについて漏えいが生じた事案。事業者はメールマガジン配信用プログラムを利用していたところ、管理者権限の窃取や任意コマンドの実行などの脆弱性が公表され、対応方法がリリースされていたにもかかわらず放置していたことが原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
29	事業者が運営するECサイトが、クロスサイトスクリプティング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。事業者が利用するECサイト構築システムに関し、脆弱性情報や対策等が公表されていたにもかかわらず対応を行わないままであったこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
30	事業者が提供している配送状況確認サービスにおいて、いわゆる置き配の場合に表示される、事業者が撮影した画像（荷物の配送ラベルに表示された氏名、住所及び電話番号）が、外部から閲覧可能な状態となっており、顧客の個人データについて、漏えい及び漏えいのおそれが生じた事案。当該サービスのシステム設計に不備があったこと等が原因と考えられる。	技術的安全管理措置 （情報システムの使用に伴う漏えい等の防止）
31	事業者のサーバがRDP（Remote Desktop Protocol）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、ファイルが暗号化され、従業者及び顧客の個人データ（特定個人情報を含む。）について、毀損及び漏えいのおそれが生じた事案。RDP接続に関するセキュリティ対策が不十分であったこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
32	事業者のサーバが、なりすましログイン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。事業者が、正規ユーザとして社内ネットワークへログインした状態を管理するため発行していたCookie情報について、有効期限を90日間と設定しており、なりすましログインが容易な状態となっていたこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）

	事案の概要	指導事項
33	事業者が運営するECサイトが、クロスサイトスクリプティング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。事業者が利用するECサイト構築システムに関し、脆弱性情報や対策等が公表されていたにもかかわらず対応を行わないままであったこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
34	事業者のサーバが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、ファイルが外部に送信及び暗号化され、従業者及び取引先の個人データについて漏えい、毀損及び漏えいのおそれが生じた事案。退職済みの従業者のVPN機器のアカウントを管理できていなかったこと、オンプレミス環境のサーバのOSに既知の脆弱性が残存していたこと、複数のサーバの管理者アカウントのパスワードが同一であり、かつ、強度に問題があったことが原因と考えられる。	技術的安全管理措置 （アクセス者の識別と認証、外部からの不正アクセス等の防止）
35	事業者は、委託元である事業者から基幹システムの運用保守及びエンハンス業務を委託されていたところ、委託元である事業者のクラウド環境で構築しているサーバが不正アクセスを受け、取扱いの委託を受けていた個人データについて漏えいのおそれが生じた事案。当該クラウドに構築中の環境を、RDP接続でインターネットから直接アクセスできるよう公開していたこと、設定していた管理者権限のパスワードの強度に問題があったこと等が原因と考えられる。	技術的安全管理措置 （アクセス者の識別と認証、外部からの不正アクセス等の防止）
36	事業者のサーバが不正アクセスを受け、会員の個人データについて漏えいが生じた事案。事業者はメールマガジン配信用プログラムを利用していたところ、管理者権限の窃取や任意コマンドの実行などの脆弱性が公表され、対応方法がリリースされていたにもかかわらず放置していたことが原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
37	事業者のサーバが不正アクセスを受け、顧客の個人データについて漏えいが生じた事案。事業者はメールマガジン配信用プログラムを利用していたところ、管理者権限の窃取や任意コマンドの実行などの脆弱性が公表され、対応方法がリリースされていたにもかかわらず放置していたことが原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
38	事業者のサーバが不正アクセスを受け、顧客の個人データについて漏えいが生じた事案。事業者はメールマガジン配信用プログラムを利用していたところ、管理者権限の窃取や任意コマンドの実行などの脆弱性が公表され、対応方法がリリースされていたにもかかわらず放置していたこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
39	事業者は、顧客企業の採用候補者のバックグラウンド調査等の業務を行っており、具体的には、顧客企業から当該採用候補者の個人情報（個人データ）の提供を受け、これを取得し、当該個人情報を利用してバックグラウンド調査を実施し、調査結果を顧客企業に報告していた。調査・検討の結果、顧客企業において採用候補者の思想・信条等の個人情報を収集する特別な職業上の必要性が存在することその他業務の	不適正な利用の禁止 （個人情報保護法第19条の規定違反）

	事案の概要	指導事項
	目的の達成に必要不可欠である等の事情を十分に確認することなく、また、家の壁に貼ってあるポスターの内容等から採用候補者の思想・信条を断定して伝えるなどしており、顧客企業において正当な理由なく本人に対する違法な差別的取扱いを助長・誘発したものといえるとして、個人情報保護法第 19 条の規定違反が認められた。	
40	事業者のサーバが 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漏えいのおそれが生じた事案。VPN 機器のアカウントの認証情報及び社内サーバの管理者権限の認証情報の強度に問題があったこと等が原因と考えられる。	技術的安全管理措置 （アクセス者の識別と認証）
41	事業者が運営する EC サイトが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。当該 EC サイトは、マイページで過去の注文情報を表示できるところ、URL に含まれる注文番号を変更することで、他の顧客の情報を表示できる状態にあったというシステム設計の不備、脆弱性診断が不十分であったこと等が原因と考えられる。	技術的安全管理措置 （情報システムの使用に伴う漏えい等の防止）
42	事業者が運営する EC サイトが、クロスサイトスクリプティング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。事業者が利用する EC サイト構築システムに関し、脆弱性情報や対策等が公表されていたにもかかわらず対応を行わないままであったこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
43	事業者のサーバが、SQL インジェクション攻撃による不正アクセスを受け、生徒、卒業生、従業者等の個人データについて漏えいのおそれが生じた事案。事業者が利用していたウェブアプリケーションのサポートが終了しており、SQL インジェクションの脆弱性が放置されていたこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
44	事業者が運営する EC サイトが、クロスサイトスクリプティング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。事業者が利用する EC サイト構築システムに関し、脆弱性情報や対策等が公表されていたにもかかわらず対応を行わないままであったこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
45	事業者において、職務として外部に個人データを送信する権限のある従業者（管理職社員）が、業務遂行の一環で、業務委託契約等を締結していない外部の者（外国にある第三者）に対して、本人の同意を得ることなく、顧客の個人データを提供した事案。個人情報保護法第 27 条第 1 項及び同法第 28 条第 1 項の規定違反が認められた。	第三者提供の制限 （個人情報保護法第 27 条第 1 項の規定違反） 外国にある第三者への提供の制限 （個人情報保護法第 28 条第 1 項

	事案の概要	指導事項
		の規定違反）

▽　指導等の内容別の件数

指導等の内容	安全管理措置							
	個人データの取扱いに係る規律の整備	組織的			技術的			
		組織体制の整備	個人データの取扱状況を確認する手段の整備	取扱状況の把握及び安全管理措置の見直し	アクセス制御	アクセス者の識別と認証	外部からの不正アクセス等の防止	情報システムの使用に伴う漏えい等の防止
指導等件数	1	1	1	2	2	12	32	2

指導等の内容	委託先の監督	利用目的による制限	不適正な利用の禁止	第三者提供の制限	外国にある第三者への提供の制限
指導等件数	2	1	1	1	1

※　一つの事案で複数の内容に該当する場合は全て計上している。

※　漏えい等報告の提出の遅延のみの事案は除く。

▽　指導等対象の業種別件数

業種	建設業	製造業	情報通信業	運輸業、郵便業	卸売業、小売業	生活関連サービス業、娯楽業	教育、学習支援業	医療、福祉	サービス業（他に分類されないもの）	不明
指導等件数	1	6	10	2	12	1	5	1	1	6

※　業種分類は、漏えい等報告の記載による。漏えい等報告の提出の遅延のみの事案は除く。

▽　指導等対象の漏えい等した人数別件数

人数	1,000 人以下	1,001 人～10,000 人	10,001 人～50,000 人	50,001 人以上
指導等件数	0	18	12	12

※　漏えい等報告のあった事案に限る。漏えい等報告の提出の遅延のみの事案は除く。

イ　行政機関等　計 26 件　※

・閲覧及び公表の対象となる文書の黒塗りの不備による漏えいのほか、誤廃棄・紛失といったヒューマンエラーを原因とする漏えい等事案に対して、安全管理措置の不備等について指導を行った。
・保有個人情報の取扱いに関するルールは規定されていたが、運用の不徹底、点検の不徹底などにより、ヒューマンエラーが防止されていないケースが目立っている。
・指導等の内容として、保有個人情報の取扱状況の記録の不備（３件）、誤送付等の防止の不備（３件）などに対して指導を行った。
・下表の事案対応のほか、漏えい等報告の提出の遅延に関し、14 件の指導を行った。
※　上記の指導等の件数には、計画的に行われた実地調査等に伴うものを含まない。

	事案の概要	指導事項
１	地方公共団体がホームページ上で、外部の人も利用可能な公文書検索・閲覧システムを提供しているところ、当該システムにおいて、約 20 年間、個人情報が記録された文書を公開していたことで保有個人情報の漏えいが生じた事案。当該システムの設定について十分な確認を実施しなかったこと、当該文書を当該システムに連携する処理の際に、文書起案者以外の他の職員によるチェック等によって誤りを認識する機会がなかったこと等が原因と考えられる。	誤送付等の防止 監査及び点検
２	独立行政法人が寄付者の名簿を保有していたところ、当該名簿を紛失しており、誤廃棄した可能性が高いため、保有個人情報について漏えいのおそれ及び滅失のおそれが生じた事案。当該独立行政法人が事務所を移転する際に、法人文書ファイル管理簿と移転する文書の原本との突合を行う手順を実施せず、移転する文書と廃棄する文書を段ボール箱に仕分け、移転する文書を入れた段ボール箱の箱数を管理するにとどまっていたこと等が原因と考えられる。	保有個人情報の取扱状況の記録
３	地方公共団体において、法令に基づき、NPO 法人の事業報告書及び役員名簿記載の個人の住所については、閲覧及び公表の対象から除外されており、黒塗りすることとしていた。しかしながら、実際には、黒塗りに不備があり、個人の住所が当該地方公共団体の生活安全課等において閲覧可能な状況におかれ、また、ポータルサイトにおいて公開されたことで、保有個人情報が漏えいした事案。黒塗り対応について複数の職員で確認する体制が整備されていなかったこと等が原因と考えられる。	誤送付等の防止
４	地方公共団体が、受領した封筒内に自立支援医療（精神通院医療）利用者の名簿が保存された CD１枚が同封されていたことに気付かず、誤って封筒ごと廃棄してしまったことで、保有個人情報について漏え	媒体の管理等

	事案の概要	指導事項
	いのおそれ及び滅失のおそれが生じた事案。封筒の中身を確認していなかったこと、支払基金からの郵送物を受領後、速やかに定められた場所へ保管することを行っていなかったこと等が原因と考えられる。	
5	警察職員が、上司の許可を得ることなく、捜査資料を自宅に持ち帰るために、通勤用のリュックサックに入れて退庁し、当該リュックサックが盗難されたことで、保有個人情報の漏えいが生じた事案。当該職員は、業務のためとはいえ、保管責任者の許可を得ずに当該写真を持ち出すことが常態化しており、保有個人情報を適切に保管することが徹底されていなかったこと等が原因と考えられる。	職員の責務 媒体の管理等
6	警察本部においては、防犯活動に協力している企業及び団体に対し、毎月、県内の特殊詐欺等の犯罪発生状況を取りまとめたデータを PDF ファイルで送信して情報提供しているところ、誤って特殊詐欺被害者の個人情報が入力されたシートを付けたエクセルファイルのまま送信し、保有個人情報の漏えいが生じた事案。外部に保有個人情報を含むデータを送信する場合、複数人による確認等を実施すべきであったにもかかわらず、単独で送信作業を行っていたこと等が原因と考えられる。	誤送付等の防止
7	地方公共団体において、事業者に委託をして当該行政機関等のふるさと納税特設サイトを開発、公開していたところ、当該サイトが不正アクセスを受け、寄附者の保有個人情報（個人データ）について漏えい及び漏えいのおそれが生じた事案。事業者において当該サイトの SQL インジェクションの脆弱性への対応を行っていなかったことが原因と考えられる。	個人情報の取扱いの委託
8	地方公共団体が精神障害者保健福祉事務として、手帳台帳システムに登録された個人番号及び精神障害者保健福祉手帳情報を、本人がマイナポータルから閲覧できるよう情報連携したところ、紐付けに誤りがあり、精神障害者保健福祉手帳を所有する者のマイナポータルに、他者の手帳情報が表示され、保有個人情報の漏えい及び漏えいのおそれが生じた事案。紐付け作業の具体的な作業手順を規程等に明記することがないまま、担当職員が１名体制で作業を行い、登録データを複数の職員で確認する体制が整備されていなかったこと、作業前後の件数及び内容の照合等の確認作業が実施されていなかったこと等が原因と考えられる。	入力情報の照合等
9	行政機関において、緊急時対応業務のために担当職員に貸与している携帯電話の所在が不明となったことで、保有個人情報について漏えいのおそれが生じた事案。当該携帯電話の貸与・返却の手続について具体的に記載したマニュアルを定めていなかったこと、現物の返却を確認せずに記録上は返却があったものとして記録していたこと、当該携帯電話について、所在確認を含む定期的な管理（棚卸し）を行っていなかったこと等が原因と考えられる。	指針の意義 （規程の整備） 保有個人情報の取扱状況の記録
10	交番勤務の警察官が、前の所属部署で作成又は入手した被害届、供述調書、捜査メモ等の複写物を、業務	職員の責務

	事案の概要	指導事項
	の参考資料として、廃棄すること無く、必要な手続を経ずに所持し続けていたところ、事件現場（店舗）に臨場した際、当該複写物が入ったかばんを置き忘れたまま帰署したことで、保有個人情報の漏えいが生じた事案。なお、約４時間後に当該店舗から通報があり、当該複写物は回収された。当該警察官において、業務に必要な範囲を超えて、所属長の承認を得ないまま、要配慮個人情報を含む保有個人情報が記載された当該複写物を所持し、勤務中常に携行して勤務場所以外にも持ち出すなど、内部規定に反して携行することが常態化していたこと等が原因と考えられる。	複製等の制限
11	中学校教諭が学級編成資料をつづったファイルを体育館のステージ上に置き忘れたところ、複数の生徒及び保護者が閲覧したほか、当該資料を撮影した写真データが SNS に流出し拡散されたことで、保有個人情報の漏えいが生じた事案。当該教諭において、当該資料は執務室内のみで取り扱う資料であり、持ち出す必要があるときは管理者の許可が必要であることの認識がなかったこと、当該資料の執務室外への持ち出しについて管理簿が作成されておらず、管理体制が不十分であったこと等が原因と考えられる。	複製等の制限 保有個人情報の取扱状況の記録
12	地方公共団体において管理用のアカウントがブルートフォース攻撃により不正アクセスを受け、クラウドサービスに保管されていた公立小中学校の生徒及び職員の氏名、メールアドレス、授業の写真等の保有個人情報について、漏えいのおそれが生じた事案。パスワード等の管理に関する定めを整備していなかったこと、当該アカウントのパスワードの強度に問題があったこと等が原因と考えられる。	アクセス制御

▽　指導等の内容別の件数

指導等の内容	指針の意義	職員の責務	保有個人情報の取扱い			
			複製等の制限	媒体の管理等	誤送付等の防止	保有個人情報の取扱状況の記録
指導等件数	1	2	2	2	3	3

指導等の内容	情報システムにおける安全の確保等		個人情報の取扱いの委託	監査及び点検
	アクセス制御	入力情報の照合等		
指導等件数	1	1	1	1

※　一つの事案で複数の内容に該当する場合は全て計上している。

※　漏えい等報告の提出の遅延のみの事案は除く。

▽　指導等対象の行政機関等（組織区分）別件数

組織区分	国の行政機関等	地方公共団体等
指導等件数	2	10

※　漏えい等報告の提出の遅延のみの事案は除く。

▽　指導等対象の漏えい等した人数別件数

人数	1,000 人以下	1,001 人～10,000 人	10,001 人～50,000 人	50,001 人以上
指導等件数	7	3	1	1

※　漏えい等報告の提出の遅延のみの事案は除く。

(2)報告徴収、立入検査（第 146 条第１項）及び資料提出要求、実地調査等（第 156 条）　計２件　※

※　上記の報告徴収、立入検査の件数は、委員会実施分のみで委任先省庁実施分を含まず、資料提出要求、実地調査等の件数は、計画的に行われた実地調査等に伴うものを含まない。

２ マイナンバー法

(1) 指導・助言（第 33 条）　計３件　※

※　上記の指導等の件数には、定期的、計画的に行われた立入検査に伴うものは含まない。

	事案の概要	指導事項
１	地方公共団体が精神障害者保健福祉事務として、手帳台帳システムに登録された個人番号及び精神障害者保健福祉手帳情報を、本人がマイナポータルから閲覧できるよう情報連携したところ、紐付けに誤りがあり、精神障害者保健福祉手帳を所有する者のマイナポータルに、他者の手帳情報が表示され、保有個人情報の漏えい及び漏えいのおそれが生じた事案。紐付け作業の具体的な作業手順を規程等に明記することがないまま、担当職員が１名体制で作業を行い、登録データを複数の職員で確認する体制が整備されていなかったこと、作業前後の件数及び内容の照合等の確認作業が実施されていなかったこと等が原因と考えられる。 ※Ⅱ１（１）イ 行政機関等　８番の事案と同じ	取扱規程等の見直し等 組織的安全管理措置 （組織体制の整備）
２	事業者のサーバが、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、ファイルが暗号化され、特定個人情報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。当該 VPN 機器の脆弱性が残存していたこと等が原因と考えられる。	技術的安全管理措置 （外部からの不正アクセス等の防止）
３	事業者のサーバが RDP 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、ファイルが暗号化され、顧客及び従業者の個人データ（特定個人情報を含む。）について、毀損及び漏えいのおそれが生じた事案。RDP 接続に関するセキュリティ対策が不十分であったこと等が原因と考えられる。 ※Ⅱ１（１）ア 民間事業者　31 番の事案と同じ	技術的安全管理措置 （外部からの不正アクセス等の防止）

(2) 報告徴収、立入検査（第 35 条第１項）　０件　※

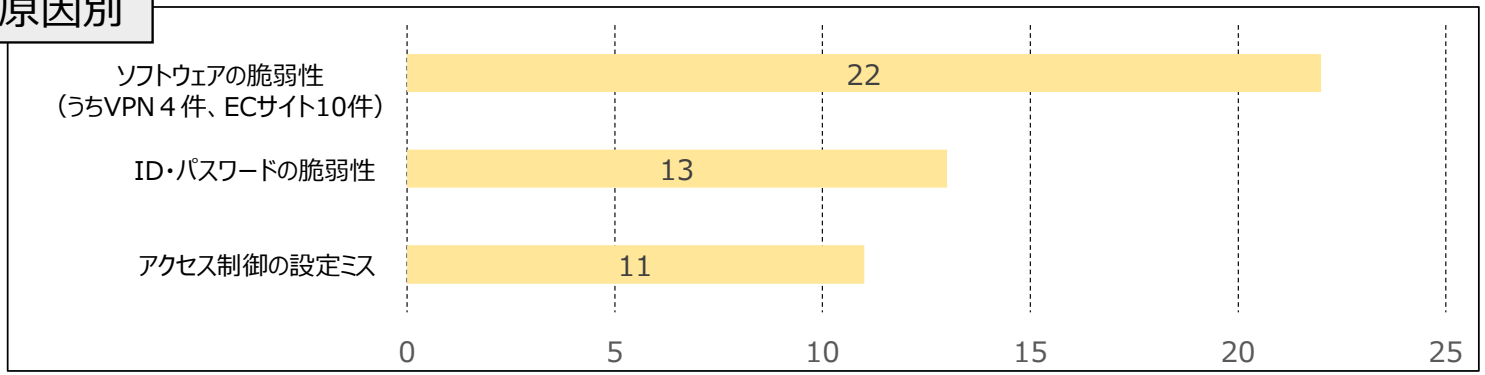
※　上記の報告徴収、立入検査の件数には、定期的、計画的に行われた立入検査に伴うものは含まない。

以　　上

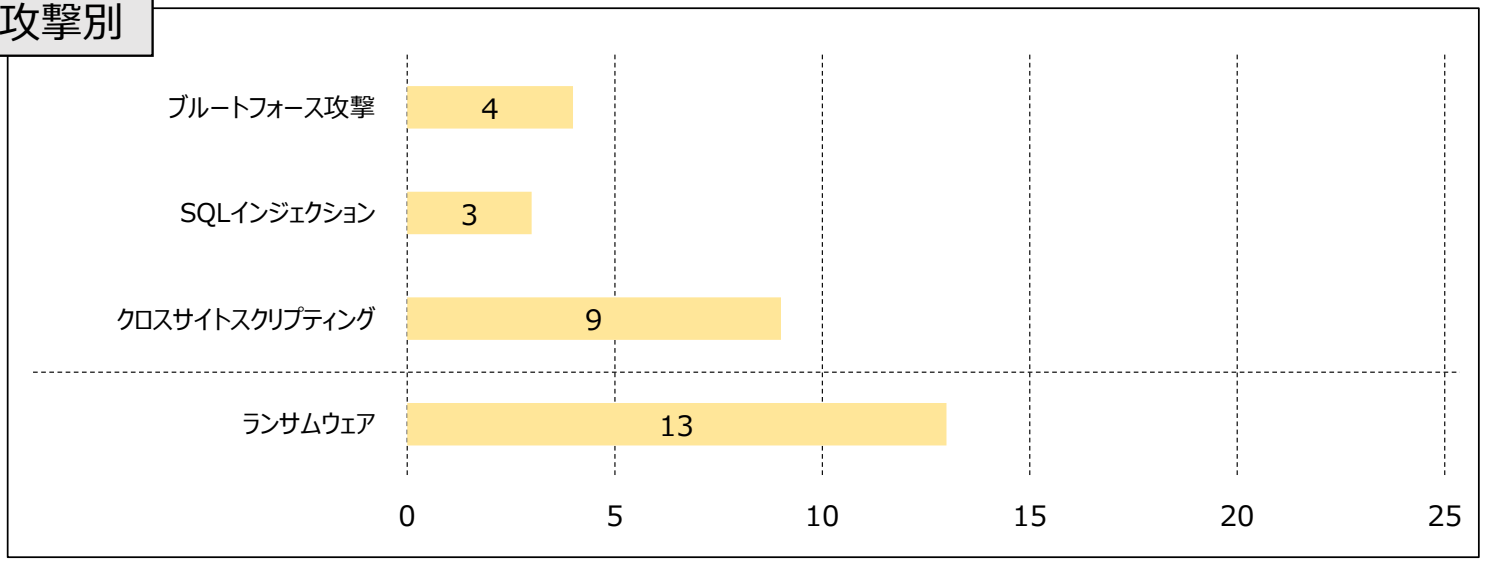
（参考）指導案件のうち不正アクセス事案の原因分析（令和６年度第４四半期）

（全体件数　40）

原因別



攻撃別



（注１）民間事業者に対する指導案件のうち、不正アクセスが原因となっている事案（40件）を抽出して分析したもの。なお、原因別・攻撃別の項目は、主なものに限り記載している。

（注２）一つの事態で複数の原因別・攻撃別の項目に該当する場合には全てに計上しているため、原因別・攻撃別の各項目の件数の合計は、全体件数を超えることがある。