資料５－１

令和７年３月〇日
個人情報保護委員会

令和6年度第3四半期における監視・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3四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

・ なし

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 129 件[1]

ア　民間事業者　計 100 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[2]のほか、ECサイトのクロスサイトスクリプティングの脆弱性を突いた攻撃[3]などがみられている。ランサムウェア攻撃[4]は、20 件みられている。
・不正アクセス以外では、社用スマートフォンの入ったかばんの盗難、管理者 ID・パスワードの管理不備による元従業者のシステムへの不正ログインなどがみられている。
・指導等の内容として、特に技術的安全管理措置に関して、外部からの不正アクセス等の防止の不備が最も多く（25 件)、アクセス制御の不備（14 件）もみられている。このほか、委託先に対する監督の不備（14 件)、組織的安全管理措置の不備（14 件)、人的安全

---

[1] 本資料の計数は公表時点のものであり、「個人情報保護委員会年次報告」等の段階で数値等が改訂される可能性がある。
[2] 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。
[3] 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。
[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。

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、42 件の指導を行った。

	事案の概要	指導事項
１	事業者が運営する EC サイトにおいて、クロスサイトスクリプティング攻撃があり、顧客の個人データに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ついて、クロスサイトスクリプティングに対する脆弱性情報や対策等が公表されていたにもかかわらず、その内容の確認や適切な対応策を実施しないまま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）
２	事業者は、あるアプリのサービス提供事業を承継して運営していたところ、承継前の会社におけるアプリ開発の委託先である事業者へのアクセス権限を解除していなかった。これにより、委託先である事業者の従業者の PC からアプリの本番データベースに侵入できる状態であったところ、同従業者の PC が不正アクセスを受け、顧客の個人データが含まれていたアプリの本番データベースに攻撃者の侵入を許した結果、個人データの漏えい及び漏えいのおそれが生じた事案。事業承継の対象となったシステムのアカウントの棚卸しが実施されていなかったこと、ログの記録等が行われていなかったこと等が原因と考えられる。	組織的安全管理措置 （個人データの取扱いに係る規律に従った運用） 技術的安全管理措置 （アクセス者の識別と認証）
３	事業者が顧客とのファイル授受用に利用するファイル交換サーバが不正アクセスを受け、一部ファイルが窃取されたことで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。事業者がインターネット経由で任意にアクセス可能なサーバに導入されているソフトウェアについて、不正アクセスにつながり得る脆弱性を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）
４	事業者は、委託元である事業者が利用する従業者の安否を確認するシステムの運用・保守を委託されていたところ、同システムの管理者 ID・パスワードが不正利用され、同システムに登録されていた従業者情報が一括ダウンロードされた結果、従業者の個人データについて漏えいが生じた事案。事業者において、管理者アカウントの認証情報の ID・パスワードを担当者以外の者も閲覧できるフォルダで管理していたことが原因と考えられる。	技術的安全管理措置 （アクセス制御）
５	事業者は、自らが運営するモール型 EC サイトに出店している各店舗を運営する顧客が一括で商品の登録・更新を行うことができるシステムの管理を委託されていたところ、同システムの管理サーバが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。事業者における同システムの管理サーバに適切なアクセス制御が行われ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 （アクセス制御､情報システムの使用に伴う漏えい等の防止）
６	事業者は、予約受付サイトを運営していたところ、同サイトが稼働しているサーバ上のリモートアクセ	技術的安全管理措置

	事案の概要	指導事項
	スソフトウェアの脆弱性を突いた不正アクセスを受け、管理していた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。リモートアクセスソフトウェアのバージョンアップ等の対応が適切に実施されていなかったこと等が原因と考えられる。	（外部からの不正アクセス等の防止）
7	事業者の従業者が、社用スマートフォンが入ったかばんの盗難被害に遭い、社用スマートフォンに保存されていた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。社用スマートフォンのパスコード設定ルールが徹底されておらず、初期パスコードから変更されていない状態で社外へ持ち出して盗難された結果、パスコードが解除されたこと等が原因と考えられる。	組織的安全管理措置 （個人データの取扱いに係る規律に従った運用）
8	事業者の従業者が使用する PC が不正アクセスを受け、ランサムウェアに感染した結果、同 PC 内に保存されていた複数のファイルが暗号化され、従業者等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。ルータの設定不備及び設定不備につながった組織的な問題（PC が標準外 PC という研究用の特殊なものであると位置付けられており、導入時の審査や定期的なアセスメント等の対象から外れていた点）が原因と考えられる。	組織的安全管理措置 （個人データの取扱いに係る規律に従った運用） 技術的安全管理措置 （外部からの不正アクセス等の防止）
9	事業者は、委託元である独立行政法人から業務及びそれに伴う保有個人情報の取扱いの委託を受けていたところ、サポート詐欺の被害に遭い、業務に使用していた PC に、遠隔操作ができるソフトウェアをインストールする等したため、PC に保存されていた保有個人情報について漏えいのおそれが生じた事案。委託元である独立行政法人とのルールに反し、ファイルへのパスワード設定や業務終了後のデータ削除ができていなかったことが原因と考えられる。	組織的安全管理措置 （個人データの取扱いに係る規律に従った運用）
10	事業者は、シェアリングサービス業務の一部及びそれに伴う個人データの取扱いをグループ会社に委託していた。事業者と委託先であるグループ会社は、同業務のための運用システムを共同で利用し、同システム上で顧客である利用者の個人データを管理していたところ、同システムが事業者の元従業者から不正ログインを受け、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。IP アドレスの制限等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） 委託先の監督
11	事業者は、シェアリングサービス業務の一部及びそれに伴う個人データの取扱いを委託されていた。事業者と委託元であるグループ会社は、同業務のための運用システムを共同で利用し、同システム上で顧客である利用者の個人データを管理していたところ、同システムが委託元であるグループ会社の元従業者から不正ログインを受け、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。事業者におけるシステムの管理者 ID・パスワードの管理等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 （アクセス制御、アクセス者の識別と認証）

	事案の概要	指導事項
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、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。VPN 機器等のアップデートを実施しておらず、危険度の高い脆弱性が放置され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）
13	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に関する脆弱性が公表され、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ため、脆弱性を突かれ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）
14	外国事業者が管理・運用する業務システムにおいて、日本の顧客のものを含む個人データを管理していたところ、同システム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。事業者における設定不備により、外部からアクセスが可能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 （情報システムの使用に伴う漏えい等の防止）
15	事業者は、就労マッチングビジネスを行っているところ、就労マッチングを行うシステムが不正アクセスを受け、同システム上の就労希望者の個人データについて漏えいが生じた事案。適切なアクセス制御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 （アクセス制御）
16	事業者は、インターネット上で商品を販売するアプリを提供しているところ、本来公開が予定されていない商品購入者の個人データが、HTTP（Hypertext Transfer Protocol）レスポンス上に表示されたことにより漏えい及び漏えいのおそれが生じた事案。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。	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 （アクセス制御）
17	事業者が提供するウェブサービスのサーバが不正アクセスを受け、事業者及び委託先である事業者の従業者の個人データについて漏えいが生じた事案。同ウェブサービスの設計時に、管理画面の適切なアクセス制御が行われていなかったこと、管理画面にログインするための ID・パスワードが初期設定の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 （アクセス制御、情報システムの使用に伴う漏えい等の防止）
18	事業者のサーバが、RDP（Remote Desktop Protocol）接続による不正アクセスを受け、管理者権限を利用され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、顧客等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。初期侵入されたサーバに多数の脆弱性が存在していたこと、管理者アカウントについて設定さ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、外部からの不正アクセス等の防止）
19	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、取引先等の個人データ及び特定個人情報について、漏えい及び毀損並びに漏えいのおそれ	技術的安全管理措置 （外部からの不正アクセス等の

	事案の概要	指導事項
	が生じた事案。VPN 機器等のアップデートを実施していなかったこと、管理者アカウントについて設定さ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。	防止）
20	事業者の従業者が使用するクラウドサービスアカウントが不正アクセスを受け、多量のメールが、不正に登録されたメールバックアップソフトを経由し窃取されたことにより、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。アカウントの認証について推奨されている多要素認証を有効化していなかったこと、クラウドサービスへのアプリ登録制限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）
21	事業者の従業者が使用するクラウドサービスアカウントが不正アクセスを受け、なりすましメールが送付された。攻撃者によるアドレス帳閲覧の可能性が否定できず、取引先等の個人データについて漏えいのおそれが生じた事案。アカウントの認証について推奨されている多要素認証を有効化しておらず、どのデバイスからもアカウントにログイン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）
22	事業者が自らのイベントで使用する申請システム内のデータベースが不正アクセスを受け、申請者の個人データについて漏えいのおそれが生じた事案。同システムのデータベースに利用するポートが外部からも接続できる状態となっていたこと、管理者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）
23	事業者は、求人情報サービス等を、代理店を通じて企業等に販売しており、代理店向けのシステムを管理・運用していたところ、開発時の誤りにより、募集企業の担当者等の個人データが、企業の担当代理店以外にも長期間にわたり公開状態となっており、漏えいが生じた事案。適切なアクセス制御が行われていなかったこと、個人データの取扱状況の把握が適切に実施されていなかったこと等が原因と考えられる。	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 （アクセス制御）
24	事業者は、健康保険組合等の職員や、小学校・中学校・高等学校の生徒向けの健康診断等を実施していたところ、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、検査画像等の個人データが暗号化され、漏えいのおそれが生じた事案。VPN 機器に対する適切なアクセス制御が行われ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）
25	事業者の社内サーバが、インターネットから 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、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。事業者のリモートデスクトップがインターネットから直接アクセスできるように意図せず公開され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）
26	事業者の社内サーバが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、事	技術的安全管理措置

	事案の概要	指導事項
	業者及びグループ会社の従業者及びその家族並びに顧客の個人データ及び特定個人情報について、毀損及び漏えいのおそれが生じた事案。VPN 機器のテストアカウントを無効にすべきところを失念し攻撃者に利用されたこと、管理者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、アクセス者の識別と認証）
27	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、漏えいのおそれが生じた事案。VPN 機器のアップデートを実施していなかったこと、委託先である事業者のシステム保守用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） 委託先の監督
28	事業者のサーバが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。適切なアクセス制御が行われ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）
29	事業者は、行政機関から施設の運営及びそれに伴う個人データの取扱いを委託されており、同施設の予約システムの構築・運用等及びそれに伴う個人データの取扱いを再委託していたところ、同システムが不正アクセスを受け、同施設の利用者の個人データについて漏えいのおそれが生じた事案。再委託先である事業者について、セキュリティ設定が不適切であった状況で、システム移行作業のためにアクセス制限を解除したこと等が原因と考えられる。事業者においては、再委託先である事業者の監督に不備が認められた。	委託先の監督
30	事業者は、行政機関から施設の運営及びそれに伴う個人データの取扱いの委託を受けていた事業者から同施設の予約システムの構築・運用等及びそれに伴う個人データの取扱いの再委託を受けていたところ、同システムが不正アクセスを受け、同施設の利用者の個人データについて漏えいのおそれが生じた事案。セキュリティ設定が不適切であった状況で、システム移行作業のためにアクセス制限を解除し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）
31	事業者のサーバが VPN 経由で不正アクセスを受け、従業者、顧客等の個人データについて漏えいのおそれが生じた事案。VPN 機器等のアップデートを実施しておらず、脆弱性が放置されていたこと等が原因と考えられる。	組織的安全管理措置 （組織体制の整備、個人データの取扱いに係る規律に従った運用、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） 人的安全管理措置

	事案の概要	指導事項
		（従業者の教育） 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、情報システムの使用に伴う漏えい等の防止）
32	事業者は、複数の医療法人から委託を受け、患者の予約管理業務を行っており、その際、SMS（ショートメッセージサービス）配信ツールを使用していたところ、認証情報が窃取され、同ツールに不正に侵入されて患者の個人データが漏えいした事案。パスワードの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）
33	事業者は、独立行政法人及び他の事業者から、補助金申請業務に関し、保有個人情報及び個人データの取扱いを委託されていたところ、同業務を行っていた事業者のサーバが、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、補助金申請者の個人データ等について、毀損及び漏えいのおそれが生じた事案。VPN 機器等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）
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、ファイルが暗号化され、従業者、取引先等の個人データについて、漏えい及び毀損並びに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、管理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）
35	事業者は、模試等の発送業務及びそれに伴う個人データの取扱いを他の事業者に委託していたところ、委託先である事業者の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、ファイルが暗号化され、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、委託先である事業者に対し、発送業務終了後の指示を行っておらず、約５年間分の委託業務に関する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
36	事業者は、他の事業者から、賃貸不動産内覧サービスのシステム開発、運用・保守等及びそれに伴う個人データの取扱いを委託されていたところ、同システムに関し使用していたクラウドサービスが不正ログインを受け、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。クラウドサービスの適切なアクセス制御が行われ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 （アクセス制御）
37	事業者の海外グループ会社のネットワークから事業者のサーバが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、事業者及びグループ会社の従業者、顧客等の個人データについて漏えいのおそれが生じた事案。海外における最初の侵入の原因については不明であるが、事業者にお	組織的安全管理措置 （個人データの取扱いに係る規律に従った運用、取扱状況の把握及

	事案の概要	指導事項
	いては、管理者アカウントのパスワードの強度に問題があったこと、事業者のネットワーク内での端末間で適切なアクセス制御が行われていなかったことが原因と考えられる。	び安全管理措置の見直し） 技術的安全管理措置 （アクセス制御、外部からの不正アクセス等の防止）
38	事業者は、自社の顧客等の個人データをグループ会社で管理していたところ、海外グループ会社のネットワークからグループ会社のサーバが不正アクセスを受け、同サーバ等がランサムウェアに感染した結果、ファイルが暗号化され、事業者及びグループ会社の従業者、顧客等の個人データについて、漏えいのおそれが生じた事案。海外における最初の侵入の原因については不明であるが、グループ会社において、管理者アカウントのパスワードの強度に問題があったこと、グループ会社のネットワーク内での端末間で適切なアクセス制御が行われていなかったことが原因と考えられる。	組織的安全管理措置 （個人データの取扱いに係る規律に従った運用、取扱状況の把握及び安全管理措置の見直し）
39	事業者は、自社の顧客等の個人データをグループ会社で管理していたところ、海外グループ会社のネットワークからグループ会社のサーバが不正アクセスを受け、同サーバ等がランサムウェアに感染した結果、ファイルが暗号化され、事業者及びグループ会社の従業者、顧客等の個人データについて、漏えいのおそれが生じた事案。海外における最初の侵入の原因については不明であるが、グループ会社において、管理者アカウントのパスワードの強度に問題があったこと、グループ会社のネットワーク内での端末間で適切なアクセス制御が行われていなかったことが原因と考えられる。	組織的安全管理措置 （個人データの取扱いに係る規律に従った運用、取扱状況の把握及び安全管理措置の見直し） 委託先の監督
40	事業者は、自社の顧客等の個人データをグループ会社で管理していたところ、海外グループ会社のネットワークからグループ会社のサーバが不正アクセスを受け、同サーバ等がランサムウェアに感染した結果、ファイルが暗号化され、事業者及びグループ会社の従業者、顧客等の個人データについて、漏えいのおそれが生じた事案。海外における最初の侵入の原因については不明であるが、グループ会社において、管理者アカウントのパスワードの強度に問題があったこと、グループ会社のネットワーク内での端末間で適切なアクセス制御が行われていなかったことが原因と考えられる。	組織的安全管理措置 （個人データの取扱いに係る規律に従った運用、取扱状況の把握及び安全管理措置の見直し）
41	事業者は、自社の顧客等の個人データをグループ会社で管理していたところ、海外グループ会社のネットワークからグループ会社のサーバが不正アクセスを受け、同サーバ等がランサムウェアに感染した結果、ファイルが暗号化され、事業者及びグループ会社の従業者、顧客等の個人データについて、漏えいのおそれが生じた事案。海外における最初の侵入の原因については不明であるが、グループ会社において、管理者アカウントのパスワードの強度に問題があったこと、グループ会社のネットワーク内での端末間	組織的安全管理措置 （個人データの取扱いに係る規律に従った運用、取扱状況の把握及び安全管理措置の見直し） 委託先の監督

	事案の概要	指導事項
	で適切なアクセス制御が行われていなかったことが原因と考えられる。	
42	事業者が開発・運用していた人事労務管理に関するシステムが不正アクセスを受け、同システム内で管理していた、顧客である事業者から取扱いを委託されていた従業者の個人データ及び特定個人情報が、ダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。	組織的安全管理措置 （組織体制の整備、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 （アクセス制御、情報システムの使用に伴う漏えい等の防止）
43	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。	委託先の監督
44	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。	委託先の監督
45	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。	委託先の監督
46	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。	委託先の監督
47	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。	委託先の監督
48	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託	委託先の監督

	事案の概要	指導事項
	していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。	
49	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。	委託先の監督
50	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。	委託先の監督
51	事業者の従業者が使用する共用のメールアカウントが攻撃者により不正に利用され、同メールアカウントに保存されていたアドレス帳等で管理されていた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。不正ログインを受けたメール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 （アクセス制御）
52	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。VPN 機器のアップデートが適切に実施されておらず脆弱性が放置されていたこと、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、外部からの不正アクセス等の防止）
53	事業者は、グループ会社である複数の事業者から店舗の来店予約システムの管理及びそれに伴う個人データの取扱いを委託されていたところ、同システムに関する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。本来公開が予定されていない内部向けサイトを誤ってインターネット経由でアクセス可能な状態としたこと、管理画面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 （情報システムの使用に伴う漏えい等の防止）
54	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及び特定個人情報について、漏えいのおそれが生じた事案。VPN 機器のアップデートが適切に実施されておらず、脆弱性が放置されていたこと、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 （外部からの不正アクセス等の防止）

	事案の概要	指導事項
55	事業者が運営するウェブサイトにおいて、顧客の個人データを管理していたバックアップ管理用サーバが不正アクセスを受け、漏えいのおそれが生じた事案。何らかの理由により API（Application Programming Interface）キーが保管されていたサーバから、API キーの認証情報が流出し、不正アクセスに利用され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）
56	事業者が利用していたクラウドサービスにおいて、管理者アカウントに約１年３か月間、断続的に不正アクセスを受け、サービス上で管理されていた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。事業者は管理者アカウントを使用しておらず、業務に必要のないアカウントがクラウドサービスに放置されていたこと、ログの確認対象から外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）
57	事業者の教職員用クラウドサーバにおいて、教職員によるアクセス可能な共有サーバ内の個人データが不正にダウンロードされるとともに、共有サーバの学生、教職員等の個人データが暗号化され、漏えい及び毀損並びに漏えいのおそれが生じた事案。IP アドレスの制限なしに RDP 接続が可能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 （アクセス制御、外部からの不正アクセス等の防止）
58	事業者は、ユーザ同士で情報の共有等が行えるアプリケーションを開発しサービス提供していたところ、開発時から存在したセキュリティ上の脆弱性により、ユーザの個人データについて、漏えいのおそれが生じた事案。短期間での開発であったこと、開発時の組織的な問題があ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 （個人データの取扱いに係る規律に従った運用、漏えい等事案に対応する体制の整備、取扱状況の把握及び安全管理措置の見直し） 人的安全管理措置 （従業者の教育） 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）

▽ 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				
		組織体制の整備	個人データの取扱いに係る規律に従った運用	個人データの取扱状況を確認する手段の整備	漏えい等事案に対応する体制の整備	取扱状況の把握及び安全管理措置の見直し
指導等件数	1	2	11	1	1	10

指導等の内容	安全管理措置					委託先の監督
	人的	技術的				
	従業者の教育	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	2	14	9	25	7	14

※ 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	電気・ガス・熱供給・水道業	情報通信業	運輸業、郵便業	卸売業、小売業	不動産業、物品賃貸業	学術研究、専門・技術サービス業	生活関連サービス業、娯楽業	教育、学習支援業	サービス業（他に分類されないもの）	不明
指導等件数	2	8	2	8	1	9	1	5	1	6	3	12

※ 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

	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	20	16	22

※ 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 29 件 ※

・委託先へ提供するデータを誤ったこと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）、教育研修の不備（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、21 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	保有個人情報が記録された書類を警察職員が不正に持ち出し、外部に提供した事案。情報管理システムのアクセス制限に不備があったこと等が原因と考えられる。	教育研修 アクセス制限 複製等の制限 廃棄等
2	独立行政法人は、業務及びそれに伴う保有個人情報の取扱いを事業者に委託していたところ、委託先である事業者がサポート詐欺に遭い、業務に使用していた PC に、遠隔操作ができるソフトウェアをインストールする等したため、PC に保存されていた保有個人情報について漏えいのおそれが生じた事案。委託先である事業者が独立行政法人とのルールに反し、ファイルへのパスワード設定等や業務終了後のデータの削除等ができ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
3	地方公共団体が市民意識調査票を送付するに当たり、調査対象者を住民基本台帳システムから抽出する際に、本来 18 歳以上の住民の保有個人情報を抽出すべきところ、誤って対象ではない 18 歳未満の住民の保有個人情報を抽出し、指定管理者に提供したことにより、保有個人情報について漏えいが生じた事案。保有個人情報の誤送付等を防止するためのチェック機能に不備があったこと等が原因と考えられる。	誤送付等の防止
4	地方公共団体の職員が、庁舎外での会議の際に、無許可で私物 USB メモリに保有個人情報を記録して持ち出し、一時紛失したことにより、保有個人情報について漏えいのおそれが生じた事案。地方公共団体のセキュリティポリシーにおいて、媒体の管理、取扱状況の記録、監査・点検等について記載されていたが、形骸化していたこと等が原因と考えられる。	教育研修 媒体の管理等 保有個人情報の取扱状況の記録 監査及び点検の実施

	事案の概要	指導事項
5	行政機関において常用として保存すべきであった台帳を誤って廃棄したことにより、保有個人情報について滅失が生じた事案。保有個人情報に関する台帳の整備に問題があっ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
6	地方公共団体が運営する施設に勤務する職員が、部下と共同で 10 年以上の間、同施設利用者に関する保有個人情報を転記してリスト化し、第三者に交付したことにより、保有個人情報について漏えいが生じた事案。長年にわたり、同施設における保有個人情報の取扱いについて適切な監査・点検等を実施していなかったこと、職員に対する研修に不備があったこと等が原因と考えられる。	教育研修 複製等の制限 監査及び点検の実施
7	行政機関が施設の運営及びそれに伴う個人データの取扱いを事業者に委託しており、当該事業者が同施設の予約システムの構築・運用等及びそれに伴う個人データの取扱いを再委託していたところ、同システムが不正アクセスを受け、同施設の利用者の個人データについて漏えいのおそれが生じた事案。再委託先である事業者については、セキュリティ設定が不適切であった状況で、システム移行作業のためにアクセス制限を解除したこと等が原因と考えられる。行政機関に対しては、委託先である事業者の監督に不備が認められた。	個人情報の取扱いの委託
8	地方公共団体が実施している福祉事業に関する文書が紛失し、対象者等の保有個人情報について滅失が生じた事案。保有個人情報が記載されたファイルについて、保存文書閲覧・貸出簿を作成していなかっ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

▽ 指導等の内容別の件数

指導等の内容	教育研修	保有個人情報の取扱い						個人情報の取扱いの委託	監査及び点検の実施
		アクセス制限	複製等の制限	媒体の管理等	誤送付等の防止	廃棄等	保有個人情報の取扱状況の記録		
指導等件数	3	1	2	1	1	1	3	2	2

※ 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

	国の行政機関等	地方公共団体等
指導等件数	3	5

※ 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

	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	2	4	2	0

※ 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3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 15 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	事業者のサーバが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、従業者の個人データ及び特定個人情報並びに委託元である事業者の従業者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。RDP へのアクセス制御が適切に行われていなかったこと、RDP の認証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 （アクセス制御、アクセス者の識別と認証）
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、従業者の個人データ及び特定個人情報について、漏えいのおそれが生じた事案。VPN 接続のためのゲストユーザアカウントについて、本来は無効とすべきところ、設定・管理を失念していたこと、同アカウントに設定さ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 （アクセス制御、アクセス者の識別と認証）
３	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、取引先等の個人データ及び特定個人情報について、漏えい及び毀損並びに漏えいのおそれが生じた事案。VPN 機器等のアップデートを実施していなかったこと、管理者アカウントについて設定さ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。 ※P. ５ 19 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）
４	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、従業者の個人データ及び特定個人情報について、漏えいのおそれが生じた事案。VPN 機器等のアップデートを実施し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）
５	事業者の社内サーバが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、事業者及びグループ会社の従業者及びその家族並びに顧客の個人データ及び特定個人情報について、毀損及び漏えいのおそれが生じた事案。VPN 機器のテストアカウントを無効にすべきところを失念し攻撃者に利用されたこと、管理者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。 ※P. ６ 26 番の事案と同じ。	技術的安全管理措置 （アクセス制御、アクセス者の識別と認証）
６	事業者が開発・運用していた人事労務管理に関するシステムが不正アクセスを受け、同システム内で管理していた、顧客である事業者から取扱いを委託されていた従業者の個人データ及び特定個人情報が、	組織的安全管理措置 （組織体制の整備、取扱状況の把

	事案の概要	指導事項
	ダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。 ※P.10 42 番の事案と同じ。	握及び安全管理措置の見直し） 技術的安全管理措置 （アクセス制御､情報システムの使用に伴う個人データの漏えい等の防止）
7	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。 ※P.10 43 番の事案と同じ。	委託先の監督
8	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。 ※P.10 44 番の事案と同じ。	委託先の監督
9	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。 ※P.10 45 番の事案と同じ。	委託先の監督
10	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。 ※P.10 46 番の事案と同じ。	委託先の監督
11	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切	委託先の監督

	事案の概要	指導事項
	なアクセス制御が行われていなかったこと等が原因と考えられる。 ※P.10 47 番の事案と同じ。	
12	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。 ※P.10 48 番の事案と同じ。	委託先の監督
13	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。 ※P.11 49 番の事案と同じ。	委託先の監督
14	事業者は、人事労務管理に関するシステムの開発・運用をする他の事業者に個人データの取扱いを委託していたところ、不正アクセスを受け、委託先である事業者のシステム内で管理していた、従業者の個人データ及び特定個人情報がダウンロードされ、漏えい及び漏えいのおそれが生じた事案。開発時に適切なアクセス制御が行われていなかったこと等が原因と考えられる。 ※P.11 50 番の事案と同じ。	委託先の監督
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、ファイルが暗号化され、従業者及び顧客の個人データ及び特定個人情報について、漏えいのおそれが生じた事案。VPN 機器のアップデートが適切に実施されておらず、脆弱性が放置されていたこと、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。 ※P.11 54 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) O件 ※

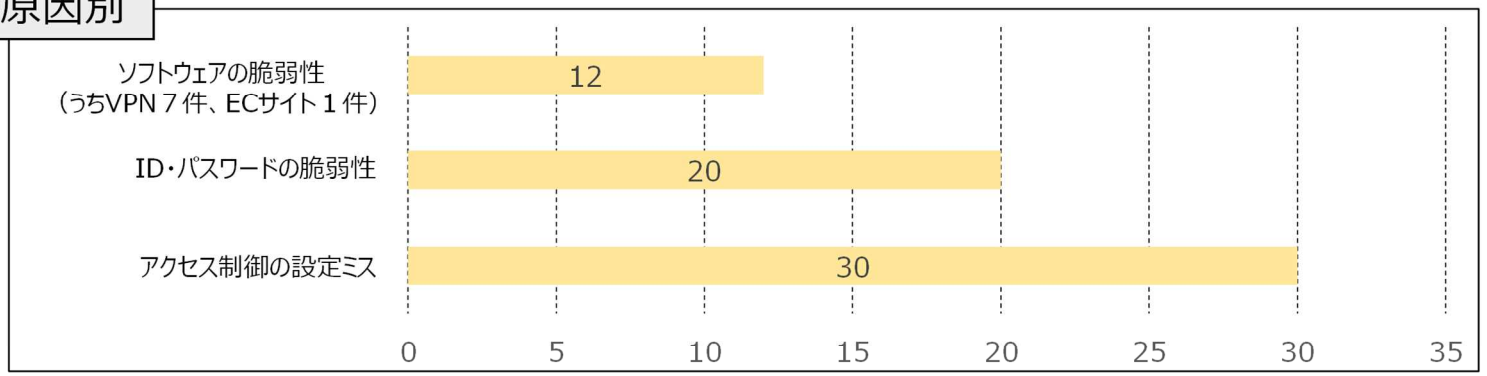
※ 上記の報告徴収、立入検査の件数には、定期的、計画的に行われた立入検査に伴うものは含まない。

以 上

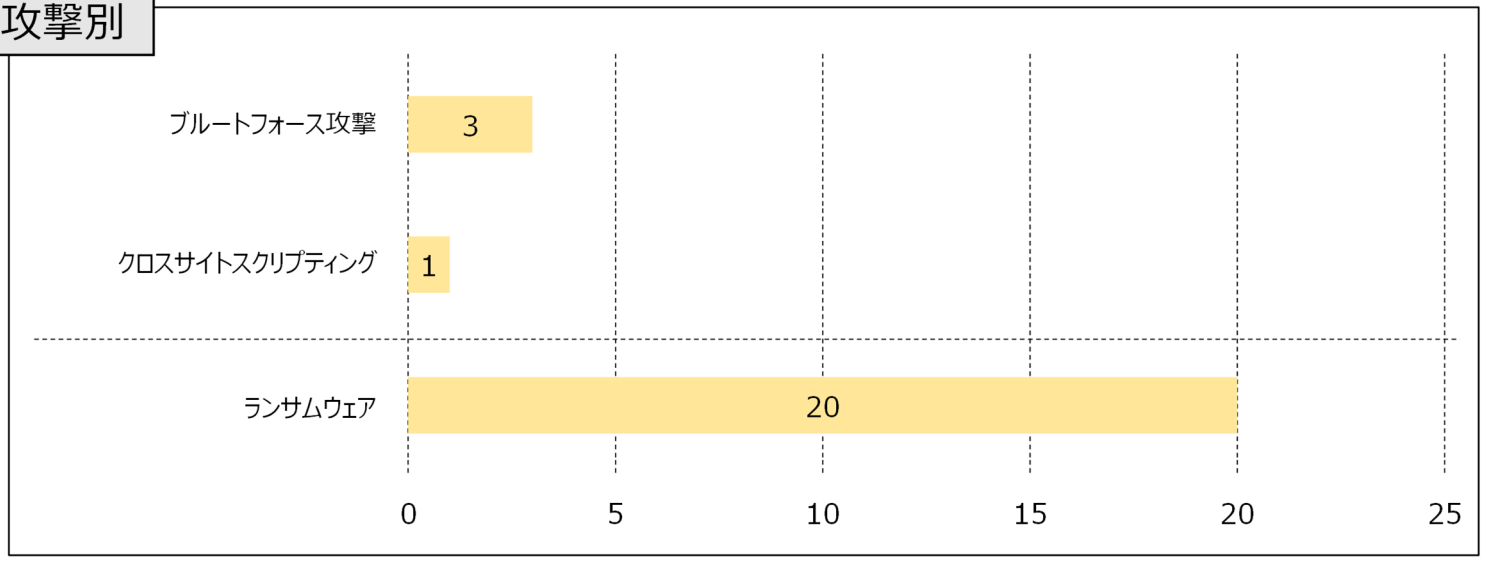
（参考）指導案件のうち不正アクセス事案の原因分析（令和６年度第３四半期）

（全体件数　52）

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（52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）一つの事案で複数の原因別・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。