令和６年 12 月４日
個人情報保護委員会

令和6年度第2四半期における監視・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2四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6年7月3日	宮崎県綾町	指導及び資料提出要求	個人情報保護法	宮崎県綾町における保有個人情報の取扱いについての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/240703_01_houdou.pdf）
令和6年7月3日	埼玉県熊谷市 株式会社アクト・ジャパン 株式会社アーバンシステム	指導	マイナンバー法	埼玉県熊谷市及び株式会社アクト・ジャパン等に対する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に基づく行政上の対応について（https://www.ppc.go.jp/

				files/pdf/240703_02_houdou.pdf）
令和6年7月 17 日	富士通 Japan 株式会社	指導及び報告徴収	個人情報保護法	高松市のコンビニ交付サービスにおける証明書誤交付事案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/240717_houdou.pdf）
令和6年9月 13 日	株式会社中央ビジネスサービス[1] ネクストステージ合同会社	指導及び報告徴収	個人情報保護法	株式会社 NTT マーケティングアクト ProCX 等における不正持ち出し事案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/240911_houdou.pdf）

[1] 株式会社中央ビジネスサービスに関しては、委員会が以前実施した個人情報保護法第 146 条第1項に基づく報告徴収に対し、虚偽の報告をした事実が確認されたため、刑事告発を実施した。

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 115 件[2]

ア　民間事業者　計 87 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[3]が目立っているほか、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[4]や、ウェブサイトの SQL インジェクションの脆弱性を突いた攻撃[5]などがみられている。ランサムウェア攻撃[6]は、21 件みられている。
- 不正アクセス以外では、メール誤送信、POS(Points of Sales)レジの処分時のデータ未消去、PC 端末の入ったバッグの盗難がみられている。
- 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(42 件)、アクセス者の識別と

---

[2] 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。

[3] 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。

[4] クロスサイトスクリプティング攻撃は、Web 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。

[5] SQL インジェクションの脆弱性とは、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脆弱性であり、この脆弱性を利用した攻撃のことが SQL インジェクション攻撃である。この攻撃により、ウェブサイト運営者が意図していないデータベースの操作が可能となり、データベースに格納されたデータの漏えい、改ざん等の被害が発生する。

[6] ランサムウェア攻撃とは、感染するとパソコン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。

認証の不備（8件）もみられている。このほか、委託先に対する監督の不備（3件）、組織的安全管理措置の不備（5件）、人的安全管理措置の不備（3件）、物理的安全管理措置の不備（1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、33 件の指導を行った。

	事案の概要	指導事項
1	事業者のウェブサイトに対し攻撃者が SQL インジェクションにより不正にアクセスし、管理者アカウントを乗っ取り、データベースにアクセスして顧客の個人データが漏えいした事案。侵入の端緒となったウェブサイトには、SQL インジェクションの脆弱性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）
2	大学等を運営する事業者において運用する情報ネットワークシステムに対し、不正アクセス（ランサムウェア攻撃）があり、主に学生の履修状況や進路情報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。RDP（リモートデスクトッププロトコル）ポートを、インターネットに意図せず公開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	事業者のサーバに不正アクセス（ランサムウェア攻撃）があり、従業者、取引先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 機器の脆弱性対応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（外部からの不正アクセス等の防止）
4	地方公共団体から委託を受けた業務に関し、保有個人情報を取り扱っていた事業者が、保有個人情報が記録されたエクセルファイルを誤ってメールに添付して第三者に送信し、漏えいが生じた事案。外部メール送信の際、添付ファイルの確認に不備があ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）
5	事業者のサーバに不正アクセス（ランサムウェア攻撃）があり、従業者及び顧客の個人データについて、漏えいのおそれ及び毀損のおそれが生じた事案。RDP が侵入経路となったところ、インターネットとサーバ間の適切なアクセス制御を行っていなかったこと、サーバにアクセスする際のログインパスワードの強度に問題があったことから、認証を突破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）
6	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があり、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）
7	事業者の海外子会社の社内ネットワークに不正アクセス（ランサムウェア攻撃）があったことを受け、海外と日本国内のネットワークとを切断したが、既に日本国内のサーバ及び端末に不正アクセスがなされた痕跡が判明し、グループ会社のサーバ等で管理されていた従業者の個人データについて、漏えい又は漏えいのおそれが生じた事案。事業者においては、国内のネットワーク上のサーバの管理者 ID が初期設定状態となっており、また、サ	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
	ーバに未対応の脆弱性が残存していたことから、特権アカウントの不正利用が容易な状態となっていたこと等が原因と考えられる。	
8	事業者の海外子会社の社内ネットワークに不正アクセス（ランサムウェア攻撃）があったことを受け、海外と日本国内のネットワークとを切断したが、既に日本国内のサーバ及び端末に不正アクセスがなされた痕跡が判明し、グループ会社のサーバ等で管理されていた従業者の個人データについて、漏えい又は漏えいのおそれが生じた事案。事業者においては、国内のネットワーク上のサーバの管理者 ID が初期設定状態となっており、また、サーバに未対応の脆弱性が残存していたことから、特権アカウントの不正利用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）
9	事業者の海外子会社の社内ネットワークに不正アクセス（ランサムウェア攻撃）があったことを受け、海外と日本国内のネットワークとを切断したが、既に日本国内のサーバ及び端末に不正アクセスがなされた痕跡が判明し、グループ会社のサーバ等で管理されていた従業者の個人データについて、漏えい又は漏えいのおそれが生じた事案。事業者においては、国内のネットワーク上のサーバの管理者 ID が初期設定状態となっており、また、サーバに未対応の脆弱性が残存していたことから、特権アカウントの不正利用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）
10	事業者の海外子会社の社内ネットワークに不正アクセス（ランサムウェア攻撃）があったことを受け、海外と日本国内のネットワークとを切断したが、既に日本国内のサーバ及び端末に不正アクセスがなされた痕跡が判明し、グループ会社のサーバ等で管理されていた従業者の個人データについて、漏えい又は漏えいのおそれが生じた事案。事業者においては、国内のネットワーク上のサーバの管理者 ID が初期設定状態となっており、また、サーバに未対応の脆弱性が残存していたことから、特権アカウントの不正利用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）
11	事業者の職員が執務室において業務用 PC を使用して作業を行っていたところ、サポート詐欺の被害に遭い、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。事業者においては、個人データの取扱いに関する研修の実施について不備があり、職員はサポート詐欺であることに気付か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） 人的安全管理措置（従業者の教育）
12	事業者が運営するクラウドメールサービスに関し、攻撃者は特定のユーザ ID についてブルートフォース攻撃を行い、ユーザのウェブメールページに対して不正にアクセスし、ユーザのアカウント情報の一部である個人データを窃取し、漏えいが生じた事案。事業者が、同サービスに係るアプリケーションの脆弱性を把握できていなかったこと、ユーザのアカウントに対するブルートフォース攻撃の対策を講じていなかったこと等が原因と考えられ	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
	る。	
13	事業者が利用するサーバに不正アクセスが行われ、従業者の個人データについて漏えいのおそれが生じた事案。侵入の入口となったのは海外現地法人の顧客向けサービスを提供しているウェブサーバであるところ、このような外部公開を前提とするウェブサイトに対する脆弱性診断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（外部からの不正アクセス等の防止）
14	事業者のサーバに不正アクセス（ランサムウェア攻撃）があり、従業者及び顧客の個人データ並びに従業者の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 機器の認証に使用するパスワードの強度に問題があったことから認証を突破され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	事業者の海外子会社が踏み台とされ、国内のネットワークに不正アクセス（ランサムウェア攻撃）がなされ、従業者の個人データについて漏えいのおそれが生じた事案。VPN 機器の脆弱性が残置されていたこと、海外拠点のセキュリティ対策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（外部からの不正アクセス等の防止）
16	事業者は、親会社である別事業者に EC サイトの保守・運用を委託していたところ、同 EC サイトに対し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。また、委託元である事業者においては、委託契約の締結がなされていなかったこと、委託先である事業者における個人データの取扱状況の把握に問題があったことから、委託先に対する監督に不備が認められた。	委託先の監督
17	事業者は、子会社である別事業者から EC サイトの保守・運用の委託を受けていたところ、同 EC サイトに対し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）
18	事業者のサーバに不正アクセス（ランサムウェア攻撃）があり、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。リモート端末のポートが意図せず解放されていたこと、リモート端末ログイン時のパスワードが使い回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があり、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）

	事案の概要	指導事項
20	事業者が管理・運用するクラウドサービスの開発用環境においてデータベース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。開発用環境における設定作業終了時に誤って IP アドレスの制限を解除したままにしたこと、開発用環境において作業後も個人データを含む作業用データが残置されてい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 人的安全管理措置（従業者の教育） 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	事業者及び複数の子会社の個人データを管理するサーバに不正アクセスがあり、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。事業者はサーバにアクセス制限を行っておらず、サーバがインターネットに公開された状態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）
22	事業者の医療用画像管理システムのサーバに不正アクセス（ランサムウェア攻撃）があり、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。システムの保守のため、IP アドレス制限なしにリモートデスクトップ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（アクセス者の識別と認証、外部からの不正アクセス等の防止）
23	事業者はシステム開発に関する業務を再々委託されていたところ、事業者の従業者が、委託元である事業者の取引先の個人データを個人利用のクラウド環境にアップロードし、さらに自己の私用 PC にダウンロードする等して、漏えいのおそれを生じさせた事案。再々委託先である事業者においては、外部へのアップロード行為を検知するシステムの導入及び検知された場合のルールの策定がされていたが、ルールどおりに運用がな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（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）
24	事業者は、委託元である事業者に対する仮想サーバサービスの提供に伴い個人データの取扱いを委託されていたところ、サーバに不正アクセスがあり、委託元である事業者の従業者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、ファイアウォール設定を適切に実施しておらず、不要な RDP 接続用のポートが解放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）
25	事業者が管理する顧客情報管理システムに不正アクセスがあり、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。事業者がシステムの改修を行うに当たり、誤って IP アドレスの制限を全て解除した状態としてしま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）
26	事業者が管理・運用する検索・予約システムに対し不正アクセスがあり、顧客の予約に関する個人データについて漏えいのおそれが生じた事案。同システムでは、一定のルールに基づき生成される暗号化トークンを予約情報ごとに個別に割り当てているが、暗号化トークンを生成する仕組みに脆弱性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）

	事案の概要	指導事項
27	事業者が管理・運用するサーバに対して、ブルートフォース攻撃による不正アクセスがあり、従業者の個人データが漏えいした事案。一般アカウントのパスワードの強度に関するポリシーは存在したが、運用が適切に行われておらず、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）
28	事業者のサーバに不正アクセス（ランサムウェア攻撃）があり、委託元である事業者から取扱いの委託を受けていたものを含む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 機器の認証に使用するパスワードの強度に問題があったことから認証を突破され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）
29	事業者の委託先である事業者のサーバに不正アクセス（ランサムウェア攻撃）があり、取扱いを委託していたものを含む従業者及び顧客の個人データについて、委託先である事業者において漏えいのおそれが生じた事案。VPN 機器の認証に使用するパスワードの強度に問題があったことから認証を突破されたこと等が原因と考えられる。委託元である事業者においては、委託先である事業者における個人データの取扱状況の把握に問題があったことから、委託先である事業者に対する監督に不備が認められた。	委託先の監督
30	事業者の業務システムサーバ並びに事業者及び子会社の PC 端末に対し不正アクセス（ランサムウェア攻撃）があり、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 機器の認証に使用するパスワードルールが徹底されておらず、強度に問題があるパスワードが利用され、認証を突破され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）
31	事業者のファイルサーバ及び従業者の PC 端末に対し不正アクセス（ランサムウェア攻撃）があり、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。リモート業務に使用している端末のリモートアクセス設定が有効に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）
32	事業者のサーバに不正アクセス（ランサムウェア攻撃）があり、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、毀損及び漏えいのおそれが生じた事案。事業者において、VPN 機器の脆弱性対応に不備があったこと、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。	技術的安全管理措置（外部からの不正アクセス等の防止）
33	事業者は、委託先である事業者にウェブサイトの開発・管理を委託していたところ、当該ウェブサイトが SQL インジェクションにより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。委託先である事業者においては、SQL インジェクション等に対する脆弱性対応に不備があったこと等が原因と考えられる。委託元である事業者においては、委託契約の締結がなされていなかったこと、委託先である事業者における個人データの取扱状況の把握に問題があったことから、委託先に対する監督に不備が認められた。	委託先の監督
34	事業者が委託元である事業者から委託を受けて開発・管理していたウェブサイトが、SQL インジェクションにより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。SQL インジェクション等に対す	技術的安全管理措置（外部からの不正アクセス等の防止、情報シス

	事案の概要	指導事項
	る脆弱性対応に不備があったこと等が原因と考えられる。	テムの使用に伴う漏えい等の防止）
35	事業者は、委託元である事業者が顧客に提供するクラウドサービスの開発・運用及び個人データの取扱いについて委託されていたところ、同サービスに係るサーバに対し不正アクセスがあり、委託元事業者の顧客の個人データについて漏えいのおそれ（一部については毀損もあり）が生じた事案。強権限のアクセスキーが残置されていたため、攻撃者に窃取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）
36	事業者を退職した元従業者が、在職中に顧客リストを不正に持ち出したことにより顧客の個人データについて漏えいした事案。元従業者が顧客リストを利用して転職先から営業目的のメールを送信したことにより、漏えいが発覚した。事業者においては、個人データの取扱いについて定期的な点検等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）
37	事業者の海外子会社が使用していたセキュリティ製品の管理者アカウントを利用されてウィルス検知ポリシーが改ざんされ、個人データ及び特定個人情報を保存していたサーバに対し不正アクセス（ランサムウェア攻撃）があり、従業者及び顧客の個人データ並びに従業者の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。仮想基盤のネットワークにファイアウォールが設置さ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）
38	事業者のサーバに不正アクセス（ランサムウェア攻撃）があり、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からブルートフォース攻撃により侵入を許したこと、各サーバの管理者権限の認証情報の強度にも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）
39	事業者のサーバに不正アクセス（ランサムウェア攻撃）があり、ネットワークシステムでつながっていたグループ全体に被害が広がり、従業者及び顧客の個人データ並びに従業者の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 機器の脆弱性対応に不備があったこと、VPN 接続のための認証アカウントの ID 及び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）
40	事業者は転職支援サイトを運営していたところ、Web サーバの脆弱性をついた不正アクセスがあり、サーバ内の個人データが外部に転送され、ユーザの個人データについて漏えい又は漏えいのおそれが生じた事案。Web サーバの脆弱性が公開されていることを認識していたものの、ミドルウェアの適時の更新対応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）
41	臨床検査事業を行う事業者のファイルサーバに不正アクセス（ランサムウェア攻撃）があり、検査を受けた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。リモートデスクトップがインターネットから直接ア	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
	クセスできるように公開されていたこと等が原因と考えられる。	
42	事業者のウェブサイトが SQL インジェクションにより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又は漏えいのおそれが生じた事案。SQL インジェクションの脆弱性対応に不備があったこと、ウェブサイトへのログインパスワードについて暗号化をせずデータベースに保管されてい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 技術的安全管理措置（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）
43	事業者のサーバに不正アクセス（ランサムウェア攻撃）があり、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。サーバが意図せずインターネットに公開された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）
44	事業者のアカウント情報管理システムに不正アクセスがあり、従業者の個人データが窃取され、漏えいが生じた事案。社内システム（ユーザがアクセスする際、サーバに保存されているユーザ情報を確認し、認証の可否を判断するシステム）の脆弱性対応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（外部からの不正アクセス等の防止）
45	事業者のサーバに不正アクセス（ランサムウェア攻撃）があり、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。サーバのログインパスワードを初期パスワードのまま使用し続けていたこと、ウィルス対策ソフトの定期的なアップデート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（外部からの不正アクセス等の防止）
46	事業者の社内システムに不正アクセスがあり、従業者の個人データについて漏えいのおそれが生じた事案。SSL-VPN の脆弱性対応に不備があったこと、攻撃者がログオンに成功したサーバにおいて、パスワードなしにサーバにアクセスできるゲストユーザが有効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）
47	事業者のサーバに不正アクセス（ランサムウェア攻撃）があり、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。サーバのログインパスワードを初期パスワードのまま使用し続けていたこと、ウィルス対策ソフトの定期的なアップデート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（外部からの不正アクセス等の防止）
48	事業者が運営する EC サイトに対し不正アクセスがあり、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。不正アクセスについては事業者が利用する EC サイト構築システムの脆弱性を突いたものではなく、個人データの外部流出の痕跡やクレジットカード情報等を窃取する不正ファイルは確認されていないものの、データベースへのアクセス自体は否定できないものであった。EC サイト構築に係るソースコードに存在する複数の脆弱性を検知する対策が講じら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）
49	病院を運営する事業者が、患者の要配慮個人情報が記録された POS レジを処分する際、個人データを消去せ	物理的安全管理措置（個人データ

	事案の概要	指導事項
	ずに処分を業者に委託したところ、処分業者が POS レジを流通させた結果、個人データの漏えい及び漏えいのおそれが生じた事案。POS レジに個人データが記録されていることについて認識不足があり、廃棄の方法に問題があったこと等が原因と考えられる。	の削除及び機器、電子媒体等の廃棄）
50	事業者の顧客の個人データを含むログデータが、本来保存することを予定していないサービス稼働状況を監視するための情報システムに保存される設定となっており、また、情報システムのアクセス権限が事業者の取引先である外部の者にも付与されていたことから、外部の者からも顧客の個人データが閲覧可能な状態となり、漏えいのおそれが生じた事案。ログ管理システム内に保存されるログデータに関するルール徹底に不備があ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、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（情報システムの使用に伴う漏えい等の防止）
51	事業者のサーバに不正アクセスがあり、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 機器の脆弱性について速やかな対応が実施されていなかったこと等が原因と考えられる。なお、事業者の VPN 機器から攻撃者が侵入したことが明らかとなってから約3か月後に漏えい等報告の速報が提出されたことから、漏えい等事案に対応する体制の整備についても問題点が認められた。	技術的安全管理措置（外部からの不正アクセス等の防止） 組織的安全管理措置（漏えい等事案に対応する体制の整備）
52	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があり、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）
53	事業者のサーバに不正アクセス（ランサムウェア攻撃）があり、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。UTM（Unified Threat Management[7]）のファームウェアの脆弱性を突いた不正アクセスであると認められるところ、事業者においては、UTM のファームウェアのバージョンアップ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）
54	事業者の従業者が海外出張中に、PC 端末の入ったバッグの盗難被害に遭い、端末内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。従業者に対する教育に不備があったこと等が原因と考えられる。	人的安全管理措置（従業者の教育）

[7] Unified Threat Management（統合脅威管理）とは、複数のセキュリティ機能を一つに集約することで、ネットワークを効率的かつ包括的に保護する管理手法である。

▽ 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		
		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	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	3	2	2	8	42	4

指導等の内容	安全管理措置		委託先の監督
	人的	物理的	
	従業者の教育	個人データの削除及び機器、電子媒体等の廃棄	
指導等件数	3	1	3

※ 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	卸売業、小売業	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	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	4	15	1	4	12	1	3	1	4	3	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

	1,000 人以下	1,001～10,000 人	10,001 人～50,000 人	50,001 人以上
指導等件数	0	20	15	19

※ 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 28 件　※

・ ウェブサイト掲載に際しての保有個人情報の削除失念のほか、誤送信・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、22 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	執務室内の施錠可能なロッカーに保管されていたはずの USB メモリーが紛失し、保有個人情報の漏えいのおそれが生じた事案。利用記録を記載する台帳が整備されていたものの、利用や貸出返却等の記録の記入がされていなかったことが原因と考えられる。	保有個人情報の取扱状況の記録
2	地方公共団体が運営するウェブサイトにおいて、当該地方公共団体が実施するトレーニング事業の登録団体一覧のファイルを公開する際に、誤って登録団体の代表者及び事務担当者の氏名、住所、電話番号及びメールアドレスを削除せずに、ウェブサイトに掲載し、保有個人情報が漏えいした事案。ウェブサイト掲載の際に、ダブルチェックが行われなかったこと等が原因と考えられる。	誤送付等の防止
3	入札公告資料の公示に際し、資料の一部に記載されていた受注業者の氏名、電話番号等の保有個人情報について、誤ってマスキング処理を行わずに公示したことにより、漏えいが生じた事案。入札事務のルールどおりにダブルチェックが行われなかったこと等が原因と考えられる。	誤送付等の防止
4	地方公共団体が組織する健康に関する部会の会員に対し、職員が会議資料をメール送信した際、誤って、後期高齢者被保険者向け健康診断の受診者等の氏名、生年月日、住所、電話番号、健康診断結果等の保有個人情報が記録されたファイルをメール送信し、要配慮個人情報を含む保有個人情報の漏えいが生じた事案。ダブルチェック等が行われなかったこと等が原因と考えられる。	誤送付等の防止
5	地方公共団体が管轄する小学校において、卒業生の個人情報を取りまとめた卒業証書授与台帳を誤って金庫ごと廃棄した結果、保有個人情報が滅失した事案。金庫内の文書について保管等の取扱状況の記録がなされ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、監査及び点検の実施

	事案の概要	指導事項
6	PC 用外付け HDD を紛失したことにより、独立行政法人が主催する事業への参加者及び職員の氏名、生年月日、電話番号等の保有個人情報について、滅失及び漏えいのおそれが生じた事案。決められた運用どおりに、管理台帳への記録がなされ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	保有個人情報の取扱い		安全管理上の問題への対応
	誤送付等の防止	保有個人情報の取扱状況の記録	監査及び点検の実施
指導等件数	3	3	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

	国の行政機関等	地方公共団体等
指導等件数	2	4

※ 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	1,001～10,000 人	10,001 人～50,000 人	50,001 人以上
指導等件数	2	3	1	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(法第 156 条) 計 15 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4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。

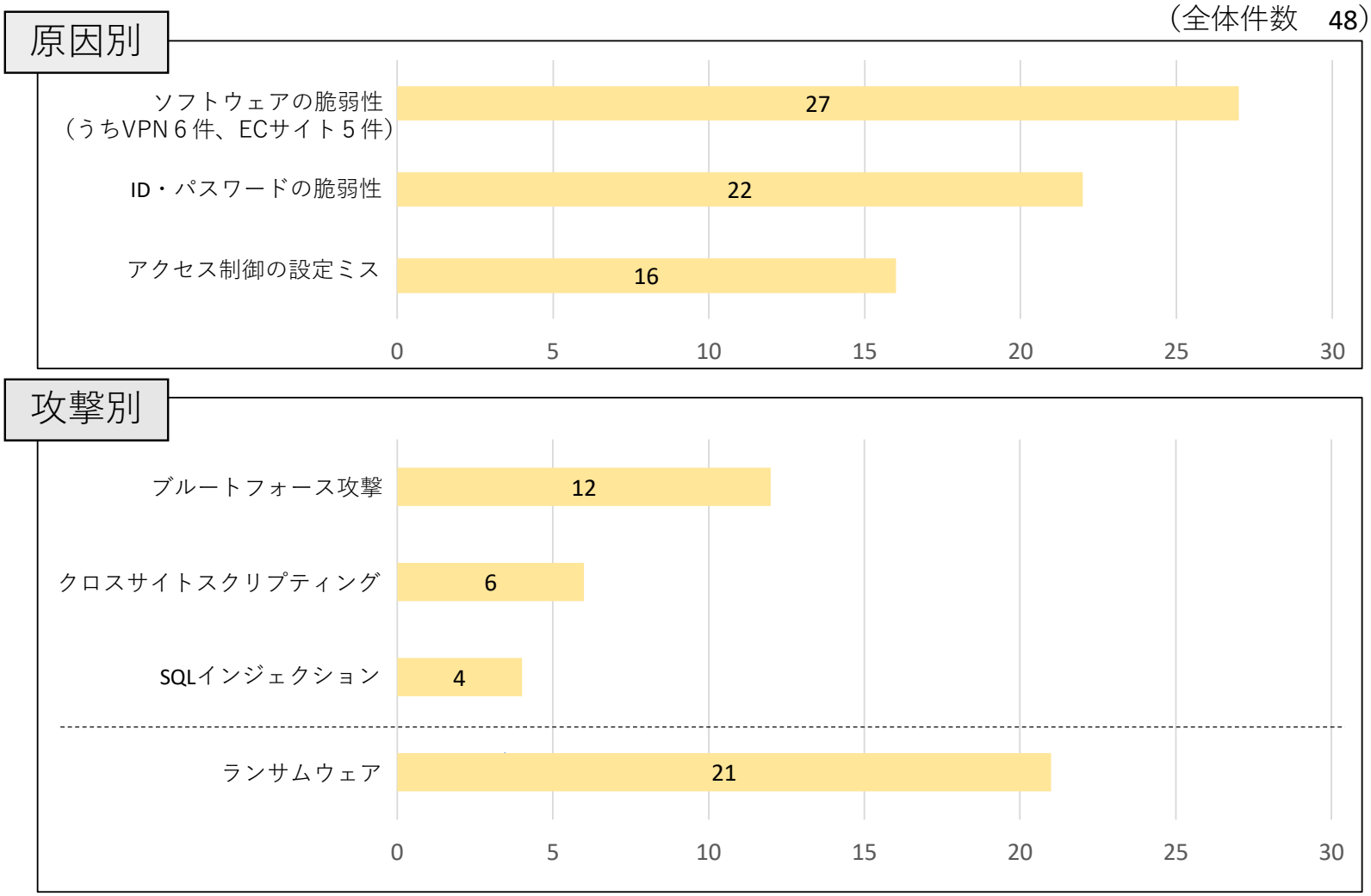
	事案の概要	指導事項
1	事業者のサーバに不正アクセス(ランサムウェア攻撃)があり、従業者及び顧客の個人データ並びに従業者の特定個人情報について、毀損及び漏えいのおそれが生じた事案。VPN 機器の認証に使用するパスワードの強度に問題があったことから認証を突破されたこと等が原因と考えられる。 ※p.6 14 番の事案と同じ。	技術的安全管理措置(アクセス者の識別と認証)
2	事業者のサーバに不正アクセス(ランサムウェア攻撃)があり、従業者及び顧客の個人データ及び特定個人情報について、毀損及び漏えいのおそれが生じた事案。事業者においては、VPN 機器の脆弱性対応に不備があったこと、管理者アカウント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.8 32 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)
3	事業者の海外子会社が使用していたセキュリティ製品の管理者アカウントを利用されてウィルス検知ポリシーが改ざんされ、個人データ及び特定個人情報を保存していたサーバに対し、不正アクセス(ランサムウェア攻撃)があり、従業者及び顧客の個人データ並びに従業者の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。仮想基盤のネットワークにファイアウォールが設置されていなかったこと等が原因と考えられる。 ※p.9 37 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	事業者のサーバに不正アクセス(ランサムウェア攻撃)があり、ネットワークシステムでつながっていたグループ全体に被害が広がり、従業者及び顧客の個人データ並びに従業者の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 機器の脆弱性対応に不備があったこと、VPN 接続のための認証アカウントの ID 及び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.9 39 番の事案と同じ。	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)

(2)報告徴収、立入検査(第 35 条第1項) 0件 ※

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

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２四半期）



（注１）民間事業者に対する指導案件のうち、不正アクセス事案（48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。