令和８年 11 月 25 日
個人情報保護委員会

令和８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８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８年８月 19 日	ＫＤＤＩ株式会社及びインターネットサービスプロバイダ	指導	個人情報保護法	「ＫＤＤＩ株式会社及びインターネットサービスプロバイダ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並びにメールサービス利用者に対する注意喚起について」の公表（https://www.ppc.go.jp/news/press/2026/260819_01_houdou/）

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 117 件[1]

①　民間事業者　計 95 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適切なアクセス制御を行っていなかったことなど、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、パスワードリスト型攻撃[2]、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、16 件みられている。
・不正アクセス以外の漏えい等事案では、個人情報の取得が適正ではなかった（個人情報保護法第 20 条第１項違反）事案、従業者が退職に際して個人情報を不正に持ち出した事案などがあった。
・指導等の内容としては、外部からの不正アクセス等の防止の不備が最も多く（23 件）、次いで、アクセス者の識別と認証の不備（11 件）が多かった。このほか、情報システムの使用に伴う漏えい等の防止の不備（４件）、取扱状況の把握及び安全管理措置の見直し

---

[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] パスワードリスト型攻撃とは、過去の情報漏えいや不正取得によって入手された「ＩＤとパスワードの組み合わせ（認証情報リスト）」を使い、複数のサービスへのログインを試みる攻撃手法である。

[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手法である。

[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。

（３件）などに対して指導を行った。

・下表ア及びイの事案対応のほか、漏えい等報告の提出の遅延に関し、52 件の指導を行った。

ア　不正アクセスを原因とする漏えい等事案

（ｉ）ソフトウェア製品等の脆弱性の放置

(a)　ＶＰＮの脆弱性

	事案の概要	指導事項
１	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、顧客、従業者等に関する個人データ（従業者については個人番号を含む。）について漏えい及び漏えいのおそれが生じた事案。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こと、脆弱性対応についての組織体制の整備（社内の責任分担の明確化等）が不十分であったこと等が原因と考えられる。 ※Ⅱ２（１）１番の事案と同じ。	組織的安全管理措置 （組織体制の整備） 技術的安全管理措置 （外部からの不正アクセス等の防止）
２	事業者は、サーバの管理を委託していたところ、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、顧客、従業者等に関する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。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こと、取り扱う個人データが保管されているデータセンター等のＩＴ環境を適切に把握できておらず、リスク評価の見直しも適切に行われていなかったこと等が原因と考えられる。 ※（ⅱ）２番の事案と同じ。	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 （外部からの不正アクセス等の防止）
３	事業者（上記事案（番号２）の委託先）が管理していたサーバが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、顧客、従業者等に関する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。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こと、取り扱う個人データが保管されているデータセンター等のＩＴ環境を適切に把握できておらず、リスク評価の見直しも適切に行われていなかったこと等が原因と考えられる。 また、事業者においては、特権アカウントのパスワードを脆弱な設定にしていたという問題点が	技術的安全管理措置 （アクセス者の識別と認証）

	事案の概要	指導事項
	認められた。 ※（ⅱ）３番の事案と同じ。	
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、従業者及び顧客に関する個人データについて漏えいが生じたおそれがある事案。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こと、ＶＰＮアカウントのパスワードが脆弱な設定であったこと等が原因と考えられる。 ※（ⅱ）５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）
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、従業者及び顧客に関する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。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こと、ＶＰＮのアカウントのパスワードが脆弱な設定であったこと等が原因と考えられる。 ※（ⅱ）９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）
６	事業者が管理する販売管理システム及びサーバが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、顧客、取引先、従業者等に関する個人データ（取引先については個人番号を含む。）について漏えいが生じたおそれがある事案。事業者はサポート切れのＶＰＮ機器の使用を継続しており、複数の脆弱性が残存していたこと等が原因と考えられる。 ※Ⅱ２（１）２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）
７	事業者のサーバがＶＰＮ経由で不正アクセスを受け、ファイルを閲覧された可能性があることから、従業者及び顧客に関する個人データについて漏えいが生じたおそれがある事案。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）
８	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、顧客に関する個人データについて漏えいが生じたおそれがある事案。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こと等が原因と考えられる。 ※（ⅱ）11 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）
９	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、従業者及び顧客に関する個人データ（従業者の個人番号を含む。）について漏えい、漏えいのおそれ及び毀損が生じた事案。ＶＰＮ機器の脆弱性が公表されていたにもかかわら	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
	ず放置していたこと等が原因と考えられる。	
10	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、顧客、従業者等に関する個人データ（従業者及び取引先の個人番号を含む。）について漏えいが生じたおそれがある事案。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こと、ＶＰＮアカウントの認証情報が脆弱な設定であったこと等が原因と考えられる。 ※（ⅱ）12 番の事案、Ⅱ２（１）３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）

(b)　ＥＣサイトの脆弱性

	事案の概要	指導事項
1	事業者が運営するＥＣサイト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、顧客に関する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。当該サイトを構築するために使用されていたソフトウェアについて、長期間アップデートがなされておらず、複数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 （アクセス制御、外部からの不正アクセス等の防止）
2	事業者は、食品販売業を営んでおり、ＥＣサイトを運営していたところ、攻撃者から不正アクセスを受け、顧客に関する個人データについて漏えいが生じたおそれがある事案。当該サイトを構築していたソフトウェアに脆弱性が残存していたこと等が原因と考えられる。事業者は、委託先にアップデートを委託していたにもかかわらず、不正アクセス発生までアップデートを行っておらず、また、委託先との間で正式な委託契約を締結しておらず、委託先における個人データの取扱状況の把握にも問題が認められた。	委託先の監督の不十分
3	事業者（上記事案（番号２）の委託先）は、ＥＣサイトの運営を委託されていたところ、攻撃者から不正アクセスを受け、顧客に関する個人データについて漏えいが生じたおそれがある事案。当該サイトを構築していたソフトウェアに脆弱性が残存していたこと等が原因と考えられる。また、事業者は、委託元からアップデートを委託されていたにもかかわらず、不正アクセス発生までアップデートを行っていなかった。	技術的安全管理措置 （外部からの不正アクセス等の防止）

(c) その他の脆弱性

	事案の概要	指導事項
1	事業者の取引先向けポータルサイトが不正アクセスを受け、当該サイトを構成するサーバに保存されていた取引先の従業者に関する個人データについて漏えいが生じたおそれがある事案。当該サイトの構築・運営のために利用していたソフトウェアの拡張プログラムに複数の脆弱性があっ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）
2	事業者は、寄付申請を管理するクラウドサービスを提供していたところ、当該サービスのファイルアップロードページに存在した脆弱性が悪用され、不正ファイルがアップロード及び実行されたことにより、寄付申請者に関する個人データ及び寄付金を受ける他の事業者から取扱いの委託を受けた個人データについて、漏えいが生じたおそれがある事案。ファイルアップロード機能で使用していたソフトウェアに深刻な脆弱性があったにもかかわらず、対応を怠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）
3	事業者は、占いを中心としたデジタルコンテンツを配信するウェブサイトを運営していたところ、ＳＱＬインジェクションの脆弱性を悪用した不正アクセスを受け、サーバに保存していたサービス利用者に関する個人データについて漏えいが生じたおそれがある事案。事業者は、開発時から、ログイン画面についてＳＱＬインジェクション攻撃への対策を実施しておらず、当該ウェブサイトは、外部からＳＱＬ文の実行が可能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）
4	事業者のウェブサイト上に設置していた申込フォームから、ＳＱＬインジェクション攻撃等の不正アクセスを受け、サーバに保存していた申込者等に関する個人データについて漏えいが生じたおそれがある事案。当該ウェブサイトにおいては、申込フォームの入力欄に送信された文字列をそのままサーバやデータベースへの命令として処理してしまう状態にあったこと等が原因と考えられる。また、事業者は、長期間、当該サーバの定期的な保守や脆弱性診断等の点検を実施していなかった。 ※（iii）２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）
5	事業者が運営する研究センターのサーバ管理を行っていた教員のアカウントに不正ログインがなされ、サーバに保存されていた教職員及び学生に関する個人データについて漏えいが生じた事案。不正ログインがなされたアカウントについてパスワードルールがなかったこと、サーバのＯＳ等に脆弱性が残存していたこと等が原因と考えられる。 ※（ⅱ）８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）

	事案の概要	指導事項
６	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、組合員に関する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ＯＳやミドルウェアがサポート切れ又は古いバージョンとなっており、脆弱性対応も長期間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）
７	事業者が管理するスキー場のゲートシステムに関するサーバが、リモートデスクトップ接続による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、スキー場利用者に関する個人データについて漏えいが生じたおそれがある事案。事業者は、５年以上システムに関する脆弱性診断を実施していなかったため、比較的容易に把握することが可能なＲＤＰ（Remote Desktop Protocol）ポートの公開について長期間認識することができず、インターネット上の全てのＩＰアドレスからＲＤＰ接続を試行することができる状態になっていたこと等が原因と考えられる。 ※（iii）５番の事案と同じ。	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）
８	事業者（上記事案（番号７）の委託先）が管理するスキー場のゲートシステムに関するサーバが、リモートデスクトップ接続による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、スキー場利用者に関する個人データについて漏えいが生じたおそれがある事案。事業者は、５年以上システムに関する脆弱性診断を実施していなかったため、比較的容易に把握することが可能なＲＤＰポートの公開について長期間認識することができず、インターネット上の全てのＩＰアドレスからＲＤＰ接続を試行することができる状態になっていたこと等が原因と考えられる。また、事業者においては、システムメンテナンスの際、ＲＤＰ接続の設定を誤り、設定後の検証も不十分であったこと等について、技術的安全管理措置の不備が認められた。 ※（iii）６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）
９	事業者は、イベント等で撮影された写真の販売を行うための写真販売システムを運営していたところ、攻撃者がシステムに利用されていたフレームワークに存在していた脆弱性を悪用して侵入し、システムにおいて管理されていた会員（写真購入者）に関する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。当該フレームワークについては、サポート切れとなっており、脆弱性対応が実施でき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 （外部からの不正アクセス等の防止）
10	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、	技術的安全管理措置

	事案の概要	指導事項
	顧客に関する個人データについて漏えいが生じたおそれがある事案。事業者は、システムで使用していたソフトウェアの脆弱性対応を実施し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）
11	事業者は、ビデオ通話サービスを運営していたところ、システムで使用されていたエラー検証用アプリがインターネット上から直接アクセス可能かつ認証設定がない状態で運用されていたことから、不正アクセスを受け、サービス利用者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、当該システムについて脆弱性診断等を行っておらず、上記の状態を認識せずに運用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 （情報システムの使用に伴う漏えい等の防止）

（ⅱ）推測されやすいＩＤ・パスワードの設定

	事案の概要	指導事項
1	事業者の顧客管理システムが、攻撃者により不正にログインされ、顧客に関する個人データがダウンロードされて漏えいが生じた事案。攻撃者により利用されたアカウントの認証情報が脆弱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）
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、顧客、従業者等に関する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。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こと、取り扱う個人データが保管されているデータセンター等のＩＴ環境を適切に把握できておらず、リスク評価の見直しも適切に行われていなかったこと等が原因と考えられる。 ※（ⅰ）(a) ２番の事案と同じ。	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 （外部からの不正アクセス等の防止）
3	事業者（上記事案（番号２）の委託先）が管理していたサーバが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、顧客、従業者等に関する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。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こと、取り扱う個人データが保管されているデータセンター等のＩＴ環境を適切に把握できておらず、リスク評価の見直しも適切に行われていなかったこと等が原因と考えられる。また、事業者においては、特権アカウントのパスワードを脆弱な設定にしていたという問題点が認められた。 ※（ⅰ）(a) ３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）

	事案の概要	指導事項
４	事業者が管理するレンタカー管理システムに対してブルートフォース攻撃が行われ、管理者権限アカウントの認証が突破され、当該システムにおいて保存されていた顧客等に関する個人データについて漏えいが生じたおそれがある事案。当該システムの管理者権限アカウントについては数字４桁という脆弱なパスワードが設定されており、ログイン試行回数制限も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）
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、従業者及び顧客に関する個人データについて漏えいが生じたおそれがある事案。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こと、ＶＰＮアカウントのパスワードが脆弱な設定であったこと等が原因と考えられる。 ※（ｉ）(a) ４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）
６	事業者の海外拠点に所在するサーバに対して、システムアカウントを悪用した攻撃がなされ、攻撃者が窃取した認証情報を利用してサーバに不正アクセスした結果、サーバ内に保存されていた従業者に関する個人データについて漏えいが生じたおそれがある事案。当該システムアカウントの認証情報が脆弱な設定となっており、また、アカウントが委託先従業者も含む複数の者で共用されていたなど、認証情報の管理体制が不十分であったこと等が原因と考えられる。 ※（iii）４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）
７	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、取引先担当者及び従業者に関する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接続に関する認証が脆弱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（アクセス者の識別と認証）
８	事業者が運営する研究センターのサーバ管理を行っていた教員のアカウントに不正ログインがなされ、サーバに保存されていた教職員及び学生に関する個人データについて漏えいが生じた事案。不正ログインがなされたアカウントについてパスワードルールがなかったこと、サーバのＯＳ等に脆弱性が残存していたこと等が原因と考えられる。 ※（ｉ）(c) ５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）
９	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、従業者及び顧客に関する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。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こと、ＶＰＮのアカウントのパスワードが脆弱な設定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）

	事案の概要	指導事項
	※（ｉ）(a) ５番の事案と同じ。	
10	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、取扱いの委託を受けていた他の事業者の顧客等に関する個人データについて漏えい、漏えいのおそれ及び毀損が生じた事案。ＶＰＮアカウントの認証情報が脆弱な設定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）
11	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、顧客に関する個人データについて漏えいが生じたおそれがある事案。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こと等が原因と考えられる。 ※（ｉ）(a) ８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）
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、顧客、従業者等に関する個人データ（従業者及び取引先の個人番号を含む。）について漏えいが生じたおそれがある事案。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こと、ＶＰＮアカウントの認証情報が脆弱な設定であったこと等が原因と考えられる。 ※（ｉ）(a) 10 番の事案、Ⅱ２（１）３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）
13	事業者は転職情報サービスを運営し、スマートフォン向けアプリを会員に提供していたところ、パスワードリスト型攻撃による不正ログインがなされ、会員に関する個人データについて漏えいが生じたおそれがある事案。会員に求めるパスワードルールが不十分であり、また、不正アクセスの検知も遅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）
14	事業者は転職情報サービスを運営し、スマートフォン向けアプリを会員に提供していたところ、パスワードリスト型攻撃による不正ログインがなされ、会員に関する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。会員に求めるパスワードルールが不十分であり、また、不正アクセスの検知も遅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）

（iii）アクセス制御の設定ミス

	事案の概要	指導事項
1	攻撃者が、事業者の業務用ＳＩＭカード内蔵型ＰＣにリモートデスクトップ接続し、社内ネットワークに侵入した結果、事業者のサーバが不正アクセスを受け、取引先担当者及び従業者等に関する	技術的安全管理措置（外部からの不正アクセス等

	事案の概要	指導事項
	個人データについて漏えいが生じたおそれがある事案。事業者は、ＰＣについてリモート接続の必要がないにもかかわらず、ポートの開放によりＰＣに外部からアクセス可能な状態のまま業務に使用していたこと等が原因と考えられる。	の防止）
２	事業者のウェブサイト上に設置していた申込フォームから、ＳＱＬインジェクション攻撃等の不正アクセスを受け、サーバに保存していた申込者等に関する個人データについて漏えいが生じたおそれがある事案。当該ウェブサイトにおいては、申込フォームの入力欄に送信された文字列をそのままサーバやデータベースへの命令として処理してしまう状態にあったこと等が原因と考えられる。また、事業者は、長期間、当該サーバの定期的な保守や脆弱性診断等の点検を実施していなかった。 ※（ｉ）(c) ４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	事業者の端末がリモートデスクトップ接続を悪用し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、委託元である他の事業者の顧客に関する個人データについて漏えいが生じたおそれがある事案。事業者は、ＯＳのバージョンアップ作業の際、ネットワーク接続に関する設定を適切に行わ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）
４	事業者の海外拠点に所在するサーバに対して、システムアカウントを悪用した攻撃がなされ、攻撃者が窃取した認証情報を利用してサーバに不正アクセスした結果、サーバ内に保存されていた従業者に関する個人データについて漏えいが生じたおそれがある事案。当該システムアカウントの認証情報が脆弱な設定となっており、また、アカウントが委託先従業者も含む複数の者で共用されていたなど、認証情報の管理体制が不十分であったこと等が原因と考えられる。 ※（ⅱ）６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）
５	事業者が管理するスキー場のゲートシステムに関するサーバが、リモートデスクトップ接続による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、スキー場利用者に関する個人データについて漏えいが生じたおそれがある事案。事業者は、５年以上システムに関する脆弱性診断を実施していなかったため、比較的容易に把握することが可能なＲＤＰポートの公開について長期間認識することができず、インターネット上の全てのＩＰアドレスからＲＤＰ接続を試行することができる状態になっていたこと等が原因と考えられる。 ※（ｉ）(c) ７番の事案と同じ。	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）
６	事業者（上記事案（番号５）の委託先）が管理するスキー場のゲートシステムに関するサーバが、リモートデスクトップ接続による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	技術的安全管理措置 （外部からの不正アクセス等

	事案の概要	指導事項
	が暗号化され、スキー場利用者に関する個人データについて漏えいが生じたおそれがある事案。事業者は、５年以上システムに関する脆弱性診断を実施していなかったため、比較的容易に把握することが可能なＲＤＰポートの公開について長期間認識することができず、インターネット上の全てのＩＰアドレスからＲＤＰ接続を試行することができる状態になっていたこと等が原因と考えられる。また、事業者においては、システムメンテナンスの際、ＲＤＰ接続の設定を誤り、設定後の検証も不十分であったこと等について、技術的安全管理措置の不備が認められた。 ※（ｉ）(c) ８番の事案と同じ。	の防止）
7	事業者の元従業者が、退職直前に顧客等に関する個人データをクラウド型グループウェアから個人端末に一括ダウンロードした可能性があり、当該個人データについて漏えいが生じたおそれがある事案。事業者においては、クラウド型グループウェアへのアクセス権限の付与について明確な取決めがなく、個人端末からのアクセス制限等の措置も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 （アクセス制御）
８	事業者は、クラウド型ＰＯＳレジシステムのアプリケーションを開発・運用し、他の事業者（委託元）にサービス提供していたところ、当該アプリケーションで使用されていたデータベースが不正アクセスを受け、委託元の顧客に関する個人データについて漏えい及び滅失が生じた事案。当該データベースで使用されていたツールが外部公開されていたことやデータベース管理システムのポートの一部が開放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 （情報システムの使用に伴う漏えい等の防止）
９	事業者は、委託先（上記事案（番号８）の事業者）からクラウド型ＰＯＳレジシステムのアプリケーションの提供を受けていたところ、当該アプリケーションで使用されていたデータベースが不正アクセスを受け、委託元の顧客に関する個人データについて漏えい及び滅失が生じた事案。事業者においては、委託先に対する監督が十分に実施できておらず、当該データベースで使用されていたツールが外部公開されていたことやデータベース管理システムのポートの一部が開放された状態となっていたこと等が原因と考えられる。	委託先の監督の不十分
10	事業者がクラウドストレージにおいて顧客のデータを管理していたところ、不正アクセスを受け、顧客に関する個人データについて漏えいが生じたおそれがある事案。事業者は、使わなくなったアクセスキーを有効な状態で放置していたため、攻撃者により悪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 （アクセス者の識別と認証）
11	事業者は、グループに加盟するホテルにウェブベースアプリケーションを提供しており、各加盟ホテルが、当該アプリケーションにおいて顧客データを管理していたところ、ある加盟ホテルの従業	技術的安全管理措置 （情報システムの使用に伴う

	事案の概要	指導事項
	者がフィッシング詐欺に遭い、攻撃者が当該加盟ホテルのアカウントを不正に利用したことにより、顧客に関する個人データについて漏えいが生じた事案。当該アプリケーションにおいては、一つの加盟ホテルのアカウントから、他の加盟ホテルのデータへのアクセスを可能とするアクセス制御の不備が存在していたこと等が原因と考えられる。	漏えい等の防止）
12	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、事業者の学生に関する個人データについて漏えいが生じたおそれがある事案。ハードウェア交換時に当該サーバにグローバルＩＰアドレスを付与したところ、その状態が作業後も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）

イ　その他の事案

	事案の概要	指導事項
1	事業者の顧客情報管理システムの認証情報が、従業者に送られたフィッシングメールの添付ファイルの実行により窃取され、当該システムで管理されていた従業者及び顧客に関する個人データがダウンロードされたことにより漏えいが生じた事案。事業者においては、個人データの取扱いに係る規律の整備や従業者教育が不十分で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 人的安全管理措置 （従業者の教育）
2	事業者の職員（教員）が、電車内でリュックサックを網棚に置いて作業をしていたところ、リュックサックの盗難に遭い、収納していたＳＳＤに記録されていた学生等に関する個人データについて漏えいが生じたおそれがある事案。事業者においては、個人データが記録された電子媒体の取扱いや学外への持ち出しについて明確なルールを定めておらず、また、教育研修も実施していなかった点について不備が認められた。	物理的安全管理措置 （電子媒体等を持ち運ぶ場合の漏えい等の防止）
3	事業者から他の事業者に出向していた従業者が、出向先から個人情報を不正に持ち出し、事業者もそのような不正な持ち出しにより取得されたものであることを知り、又は容易に知ることができたにもかかわらず、個人情報を取得していた。さらに、事業者の別の従業者が、出向先の従業者に関する個人データを外部にメールで送信し、漏えいを生じさせた。個人データの取扱いについて、従業者への周知徹底が不十分であったこと等が原因と考えられる。	適正取得（個人情報保護法第 20 条第１項）違反 人的安全管理措置 （従業者の教育）
4	事業者の複数の元従業者が、それぞれ（計３事案）、退職に際して私的な目的で、従業者、取引先関係者等に関する個人データを持ち出し、漏えいが生じた事案。事業者においては、従業者による個人データの不正持ち出しを防止するため、外部記録媒体の利用等についてルールを定めていたものの、実際の運用上はルールが徹底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）

▽　指導等の内容別の件数

指導等の内容	安全管理措置				
	組織的			人的	物理的
	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	取扱状況の把握及び安全管理措置の見直し	従業者の教育	電子媒体等を持ち運ぶ場合の漏えい等の防止
指導等件数	1	1	3	2	1

指導等の内容	安全管理措置				委託先の監督	適正取得違反
	技術的					
	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	11	23	4	2	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	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
指導等件数	4	1	9	2	3	2

業種	学術研究、専門・技術サービス業	宿泊業、飲食サービス業	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	2	1	1	3	1	4	10

※　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	20	10	13

※　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。

② 行政機関等　計 22 件　※

・マスキング処理が不十分である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。
・指導等の内容として、媒体の管理等の不備（５件）、誤送付等の防止の不備（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、13 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	教育委員会が所管する高等学校において、保管文書の点検をしたところ、３か年度分の入学者選抜関係文書の所在が不明となっていることが判明。同委員会が県内の他の学校に点検を指示したところ、当該高校を含め合計 23 の県立学校において、同じ資料の所在が不明となっていることが判明した。保存期間を誤認する等して誤廃棄した可能性が高く、志願者等に関する保有個人情報について漏えいのおそれ及び滅失が生じた事案。当該資料をつづっていたファイルの背表紙に文書名や保存期間を記載しておらず、適正に保存されていなかったこと等が原因と考えられる。	媒体の管理等
２	地方公共団体が内閣府ポータルサイトにおいて公開するＮＰＯ法人の事業報告書及び役員名簿について、個人の住所は、閲覧及び公表の対象から除外されており、黒塗りすることとされていたところ、当該地方公共団体は、ＰＤＦ上の黒塗り処理に不備があり、個人の住所が閲覧可能な状況に置かれ、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。黒塗り対応についての手順や確認体制が不十分であったこと等が原因と考えられる。	誤送付等の防止
３	警察署において、保存文書の点検を実施した際、道路使用許可申請書等の所在が不明となっていることが判明。紛失時期は不明であるが誤廃棄の可能性が高く、これにより、保有個人情報について漏えいのおそれ及び滅失が生じた。警察署においては、保存すべき文書と保存期間が満了した廃棄予定の文書が混在する状況であったこと等が原因と考えられる。	媒体の管理等
４	地方公共団体が内閣府ポータルサイトにおいて公開するＮＰＯ法人の事業報告書及び役員名簿について、個人の住所は、閲覧及び公表の対象から除外されており、黒塗りすることとされていたところ、当該地方公共団体は、ＰＤＦ上の黒塗り処理に不備があり、個人の住所が閲覧可能な状況に置かれ、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。黒塗り対応についての手	誤送付等の防止

	事案の概要	指導事項
	順や確認体制が不十分であったこと等が原因と考えられる。	
５	警察署において、保存文書の点検を実施した際、古物及び風俗営業等の申請等受理一覧表や令状請求簿等の所在が不明となっていることが判明。紛失時期は不明であるが令和８年２月の文書廃棄の際に誤廃棄した可能性があり、これにより、保有個人情報について漏えいのおそれ及び滅失が生じた。警察署においては、保存すべき文書と廃棄承認を得た文書が混在する状況であったこと等が原因と考えられる。	媒体の管理等
６	行政機関において、行政文書等に係る廃棄数量調査のため帳簿等保存簿を確認したところ、各種証明書発行手続に係る請求書をつづったものを誤廃棄したことが判明。これにより保有個人情報について滅失が生じた。当該資料は段ボールに入れて保管していたが、廃棄承認済みのものとそうではない段ボールを区別することなく書庫内の同じ場所で保管していたこと等が原因と考えられる。	媒体の管理等
７	地方公共団体が、民生委員法第 14 条に規定する職務（一人暮らしの高齢者宅の定期訪問等）のために、民生委員・児童委員に避難行動要支援者名簿等を渡していたところ、複数の名簿が所在不明となっていることが判明。これにより、保有個人情報について漏えいが生じたおそれがある事案。当該地方公共団体では、名簿の交付時の記録はなく、返却や廃棄についても記録していなかったなど、名簿の管理体制が不十分で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
８	地方公共団体が、開示請求を受けたところ、開示請求を受けてから 30 日以内に開示決定をすることなく、また、その後一部開示の決定をした際、個人情報保護法第 82 条第１項に係る、個人情報の保護に関する法律施行令（平成 15 年政令第 507 号）第 24 条が定める事項を記載した書面による通知を行うこともしなかった。	個人情報保護法第 82 条第１項（開示請求に対する措置）及び個人情報保護法第 83 条第１項（開示決定等の期限）違反
９	選挙管理委員会が、保存期間が満了していない選挙関連書類（選挙人名簿抄本、投票所入場券等）を誤廃棄した結果、保有個人情報について滅失が生じた事案。保存期間が異なる衆議院議員総選挙と最高裁判所裁判官国民審査を混同するなど、保存期間の誤認等が原因と考えられる。	媒体の管理等

▽　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			個人情報保護法第 82 条第 1 項（開示請求に対する措置）及び個人情報保護法第 83 条第 1 項（開示決定等の期限）違反
	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	5	2	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	1	8

※　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	4	3	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 41 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５件　※

・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、１件の指導を行った。

※　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、顧客、従業者等に関する特定個人情報（従業者の個人番号を含む。）について漏えい及び漏えいのおそれが生じた事案。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こと、脆弱性対応についての組織体制の整備（社内の責任分担の明確化等）が不十分であったこと等が原因と考えられる。 ※Ⅱ１（１）①ア（ｉ）(a) １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	事業者が管理する販売管理システム及びサーバが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、顧客、取引先、従業者等に関する特定個人情報（取引先の個人番号を含む。）について漏えいが生じたおそれがある事案。事業者はサポート切れのＶＰＮ機器の使用を継続しており、複数の脆弱性が残存していたこと等が原因と考えられる。 ※Ⅱ１（１）①ア（ｉ）(a) ６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、顧客、従業者等に関する特定個人情報（従業者及び取引先の個人番号を含む。）について漏えいが生じたおそれがある事案。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こと、ＶＰＮアカウントの認証情報が脆弱な設定であったこと等が原因と考えられる。 ※Ⅱ１（１）①ア（ｉ）(a) 10 番、Ⅱ１（１）①ア（ii）12 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）
４	事業者の従業者が業務用ＰＣでニュースサイトを閲覧中にサポート詐欺に遭い、攻撃者の指示に従って遠隔操作ソフトウェアをインストールした結果、当該ＰＣを遠隔操作され、保存されていたデータが削除される等により、従業者（退職者を含む。）に関する特定個人情報について	人的安全管理措置 （事務取扱担当者の教育）

	事案の概要	指導事項
	滅失及び漏えいのおそれが生じた事案。事業者においては、規程で定めていた従業者への教育・研修を実施していなかったこと等が原因と考えられる。	

(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。

Ⅲ　公表事案に関する指導・助言等の対象先における改善策の実施状況

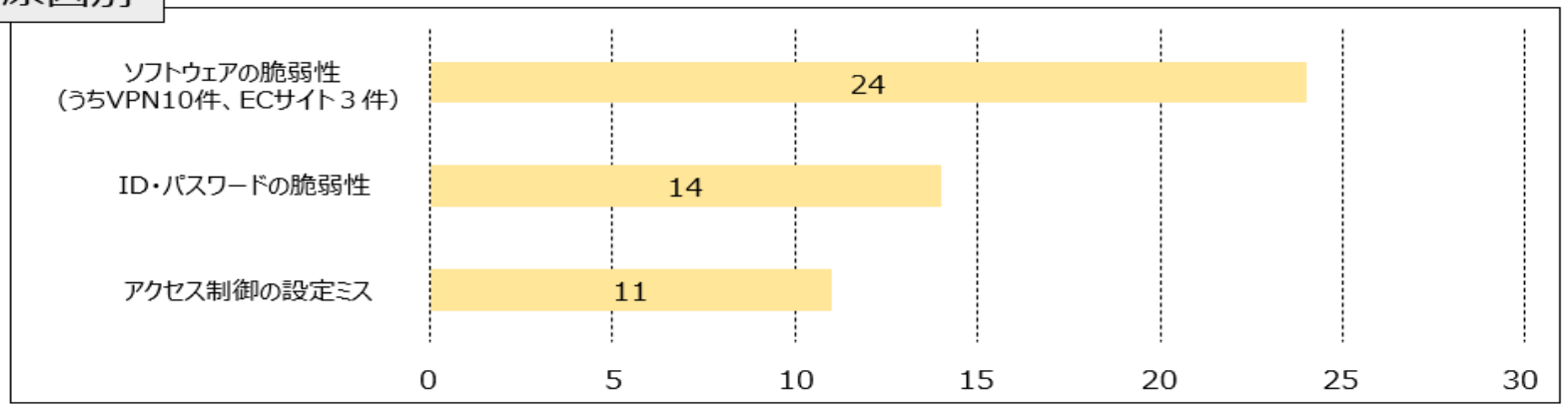
・なし

以　　上

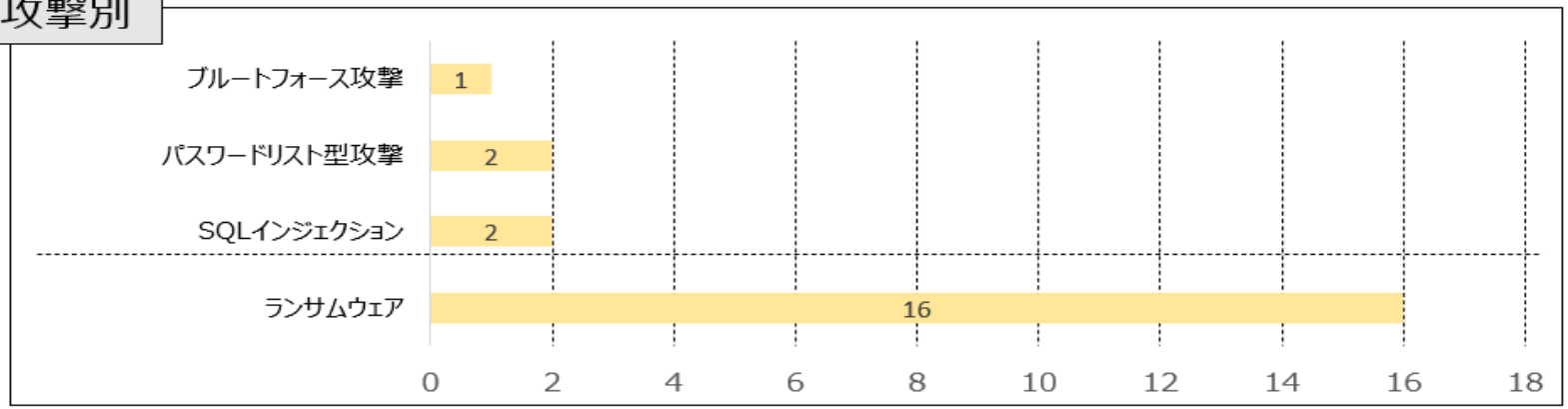
（参考）指導案件のうち不正アクセス事案の原因分析（令和８年度第２四半期）

（全体件数　39）

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（39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。