資料３－１

令和８年　月　日

個人情報保護委員会

令和８年度第１四半期における監視・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１四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 141 件[1]

①　民間事業者　計 98 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、ブルートフォース攻撃[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、15 件みられている。
・不正アクセスを原因とする漏えい等事案のほか、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、複数の漏えい等事態について漏えい等報告を行っていなかった事案等がみられた。
・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（21 件）、次いで、アクセス者の識別と認証の不備（14 件）が多かった。このほか、委託先に対する監督の不備（12 件）、情報システムの使用に伴う漏えい等の防止の不備（３件）などに対して指導を行った。

---

[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] 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。

・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、45 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、従業者及び顧客に関する個人データについて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、教職員、学生等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。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）
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、従業者及び顧客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。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）
４	保険会社等から鑑定業務を受託するに伴い、個人データの取扱いの委託を受け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、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）２番の事案と同じ。	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、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、従業者及び顧客等に関する個人データ並びに従業者に関する特定個人情報について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
	放置していたこと等が原因と考えられる。 ※Ⅱ２（１）４番の事案と同じ。	
６	事業者の社内ネットワークに対し、ＶＰＮ経由で不正アクセスがあり、攻撃者により当該ネットワーク内の管理者権限を持つアカウントが不正に利用され、従業者及び顧客等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。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、初期侵入に利用されたアカウントの認証情報が脆弱な設定となっていたこと等が原因と考えられる。 ※（ⅱ）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）
７	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、漏えいのおそれ及び毀損が生じた事案。事業者から機器の管理を委託されていた委託先において、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。事業者においては、ＶＰＮ機器等の脆弱性対応を含めた業務に伴い個人データの取扱いを委託先に委託していたところ、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についての把握に問題がある等、委託先の監督が不十分であることが認められた。 ※（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） 委託先の監督の不十分
８	委託元（上記事案（番号７）の事業者）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、漏えいのおそれ及び毀損が生じた事案。委託元から機器の管理を委託されていた事業者において、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）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、外部からの不正アクセス等の防止）
９	医療法人である事業者において、電子カルテシステム等を運用するためのサーバが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、従業者等に関する個人データについて漏えい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）
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、従業者及び顧客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	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
	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等が原因と考えられる。	防止）

(b)　ＥＣサイトの脆弱性

	事案の概要	指導事項
1	事業者は、ＥＣサイトの構築や運営を行う加盟店（委託元）に対し、クラウド上で通販システムをサービス提供していたところ、当該システムに対し、ＳＱＬインジェクション攻撃を受け、委託元の顧客に関する個人データについて漏えいのおそれが生じた事案。事業者においては、脆弱性対応が十分でなく、長年、ＳＱＬインジェクションに対する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 （情報システムの使用に伴う漏えい等の防止）
2	委託先（上記事案（番号１）の事業者）において、ＥＣサイトの構築や運営を行う加盟店（委託元）に対し、クラウド上で通販システムをサービス提供していたところ、当該システムに対し、ＳＱＬインジェクション攻撃を受け、事業者の顧客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。委託先においては、脆弱性対応が十分でなく、長年、ＳＱＬインジェクションに対する脆弱性が放置されていたこと等が原因と考えられる。 事業者については、本件事業者に対する個人データの取扱いの委託に当たり契約を締結しておらず、本件事業者における個人データの取扱状況についての把握に問題がある等、委託先の監督が不十分であることが認められた。	委託先の監督の不十分
3	委託先（上記事案（番号１）の事業者）において、ＥＣサイトの構築や運営を行う加盟店（委託元）に対し、クラウド上で通販システムをサービス提供していたところ、当該システムに対し、ＳＱＬインジェクション攻撃を受け、事業者の顧客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。委託先においては、脆弱性対応が十分でなく、長年、ＳＱＬインジェクションに対する脆弱性が放置されていたこと等が原因と考えられる。 事業者については、本件事業者に対する個人データの取扱いの委託に当たり契約を締結しておらず、本件事業者における個人データの取扱状況についての把握に問題がある等、委託先の監督が不十分であることが認められた。	委託先の監督の不十分
4	委託先（上記事案（番号１）の事業者）において、ＥＣサイトの構築や運営を行う加盟店（委託元）	委託先の監督の不十分

	事案の概要	指導事項
	に対し、クラウド上で通販システムをサービス提供していたところ、当該システムに対し、ＳＱＬインジェクション攻撃を受け、事業者の顧客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。委託先においては、脆弱性対応が十分でなく、長年、ＳＱＬインジェクションに対する脆弱性が放置されていたこと等が原因と考えられる。 事業者については、本件事業者に対する個人データの取扱いの委託に当たり契約を締結しておらず、本件事業者における個人データの取扱状況についての把握に問題がある等、委託先の監督が不十分であることが認められた。	
５	委託先（上記事案（番号１）の事業者）において、ＥＣサイトの構築や運営を行う加盟店（委託元）に対し、クラウド上で通販システムをサービス提供していたところ、当該システムに対し、ＳＱＬインジェクション攻撃を受け、事業者の顧客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。委託先においては、脆弱性対応が十分でなく、長年、ＳＱＬインジェクションに対する脆弱性が放置されていたこと等が原因と考えられる。 事業者については、本件事業者に対する個人データの取扱いの委託に当たり契約を締結しておらず、本件事業者における個人データの取扱状況についての把握に問題がある等、委託先の監督が不十分であることが認められた。	委託先の監督の不十分
６	委託先（上記事案（番号１）の事業者）において、ＥＣサイトの構築や運営を行う加盟店（委託元）に対し、クラウド上で通販システムをサービス提供していたところ、当該システムに対し、ＳＱＬインジェクション攻撃を受け、事業者の顧客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。委託先においては、脆弱性対応が十分でなく、長年、ＳＱＬインジェクションに対する脆弱性が放置されていたこと等が原因と考えられる。 事業者については、本件事業者に対する個人データの取扱いの委託に当たり契約を締結しておらず、本件事業者における個人データの取扱状況についての把握に問題がある等、委託先の監督が不十分であることが認められた。	委託先の監督の不十分
７	委託先（上記事案（番号１）の事業者）において、ＥＣサイトの構築や運営を行う加盟店（委託元）に対し、クラウド上で通販システムをサービス提供していたところ、当該システムに対し、ＳＱＬインジェクション攻撃を受け、事業者の顧客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。委託先においては、脆弱性対応が十分でなく、長年、ＳＱＬインジェクションに対する脆弱性が放置され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

	事案の概要	指導事項
	事業者については、本件事業者に対する個人データの取扱いの委託に当たり契約を締結しておらず、本件事業者における個人データの取扱状況についての把握に問題がある等、委託先の監督が不十分であることが認められた。	
8	事業者がＥＣサイトを運営していたところ、当該サイト内のファイル管理ツールの設定不備に起因する脆弱性を悪用した不正アクセスがあり、顧客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。当該管理ツールの管理者画面について適切なアクセス制御が行われておらず、第三者が管理者画面におけるファイルアップロード機能を利用できる状態と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。	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、ＥＣサイトを運営していたところ、当該ＥＣサイトが不正アクセスを受け、ＥＣサイト利用者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。事業者は、委託先との間で脆弱性対応に関する責任の所在を曖昧にしていたため、当該ＥＣサイト構築に利用されていたソフトウェアの脆弱性の対応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）
10	事業者は、ＥＣサイトを運営しているところ、当該サイトのデータベースサーバ等が、監視サーバ経由で不正アクセスを受け、従業者及び顧客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。監視サーバの管理者アカウントの認証情報が脆弱な設定となっていたこと、監視サーバの脆弱性対応が不十分であったこと等が原因と考えられる。 ※（ii）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）

(c)　その他の脆弱性

	事案の概要	指導事項
1	事業者が、委託を受けて構築・運用していた予約サイトのサーバが不正アクセスを受け、予約者に関する個人データが削除され、漏えいのおそれ及び滅失が生じた事案。当該予約サイトのデータベース管理システムについて、構築時からサポート切れのバージョンが使用されており、脆弱性が管理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 （情報システムの使用に伴う漏えい等の防止）
2	委託先（上記事案（番号１）の事業者）が、委託を受けて構築・運用していた予約サイトのサーバが不正アクセスを受け、予約者に関する個人データが削除され、漏えいのおそれ及び滅失が生じた	委託先の監督の不十分

	事案の概要	指導事項
	事案。当該予約サイトのデータベース管理システムについて、構築時からサポート切れのバージョンが使用されており、脆弱性が管理されていなかったこと等が原因と考えられる。 事業者においては、委託に当たり契約を締結しておらず、事業者における個人データの取扱状況についての把握に問題がある等、委託先の監督が不十分であることが認められた。	
3	事業者は、顧客向けのウェブサイトを運営していたところ、ＳＱＬインジェクション攻撃を受け、当該ウェブサイトに登録していた顧客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。事業者は、顧客がログインする画面について、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	事業者は、委託先に対し、医療機器等販売のためのウェブサイトの開設・管理等を委託していたところ、当該サイト構築のために使用されていたソフトウェアの拡張プログラムの脆弱性が悪用され、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のおそれが生じた事案。当該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。 委託元である事業者については、契約における安全管理措置に関する合意内容が不十分であり、委託先における個人データの取扱状況についての把握に問題がある等、委託先の監督が不十分であることが認められた。	委託先の監督の不十分
5	事業者は、委託元（上記事案（番号４）の事業者）から医療機器等販売のためのウェブサイトの開設・管理等の委託を受けていたところ、当該サイト構築のために使用されていたソフトウェアの拡張プログラムの脆弱性が突かれ、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のおそれが生じた事案。当該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）
6	事業者が管理する外部公開サーバが不正アクセスを受け、社内ネットワークに侵入され、従業者及び顧客に関する個人データについて漏えいのおそれが生じた事案。当該サーバについて定期的なパッチ適用を実施しておらず、既知の脆弱性を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）
7	事業者のウェブサイトがＳＱＬインジェクション攻撃を受け、サーバ内の顧客に関する個人データが改ざんされ、漏えいのおそれが生じた事案。当該サイトに使用されていたソフトウェアについては、ＳＱＬインジェクション攻撃に対する脆弱性を含む複数の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 （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

	事案の概要	指導事項
		（外部からの不正アクセス等の防止）

（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、事業者の職員、学生等に関する個人データについて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（ＩＤ及びパスワード）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）
2	保険会社等から鑑定業務を受託するに伴い、個人データの取扱いの委託を受け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、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の強度に問題が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。	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、外部からの不正アクセス等の防止）
3	事業者は、ＥＣサイトを運営しているところ、当該サイトのデータベースサーバ等が、監視サーバ経由で不正アクセスを受け、従業者及び顧客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。監視サーバの管理者アカウントの認証情報が脆弱な設定となっていたこと、監視サーバの脆弱性対応が不十分であったこと等が原因と考えられる。 ※（ｉ）(b) 10 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	事業者の社内ネットワークに対し、ＶＰＮ経由で不正アクセスがあり、攻撃者により当該ネットワーク内の管理者権限を持つアカウントが不正に利用され、従業者及び顧客等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。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、初期侵入に利用されたアカウントの認証情報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、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) ６番の事案と同じ。	
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、漏えいのおそれ及び毀損が生じた事案。事業者から機器の管理を委託されていた委託先において、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。事業者においては、ＶＰＮ機器等の脆弱性対応を含めた業務に伴い個人データの取扱いを委託先に委託していたところ、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についての把握に問題がある等、委託先の監督が不十分であることが認められた。 ※（ｉ）(a) ７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） 委託先の監督の不十分
６	委託元（上記事案（番号５）の事業者）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、漏えいのおそれ及び毀損が生じた事案。委託元から機器の管理を委託されていた事業者において、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 （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）
７	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、漏えいのおそれ及び毀損が生じた事案。ＶＰＮの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）
８	事業者は、情報インフラ基盤の運用・保守業務を行っており、複数社から従業者に関する個人データの取扱いの委託を受けていたところ、ＶＰＮ経由でネットワーク内のサーバに不正アクセスを受け、当該個人データについて漏えいのおそれが生じた。侵入に使用されたＶＰＮのアカウントは残置されたテスト用アカウントであり、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。 ※(iii) 11 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）
９	委託先（上記事案（番号８）の事業者）において、情報インフラ基盤の運用・保守業務を行っており、複数社から従業者に関する個人データの取扱いの委託を受けていたところ、ＶＰＮ経由でネットワーク内のサーバに不正アクセスを受け、当該個人データについて漏えいのおそれが生じた。侵入に使用されたＶＰＮのアカウントは残置されたテスト用アカウントであり、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。 事業者については、委託先に対する個人データの取扱いの委託に当たり契約を締結しておらず、委	委託先の監督の不十分

	事案の概要	指導事項
	託先における個人データの取扱状況についての把握に問題がある等、委託先の監督が不十分であることが認められた。 ※(ⅲ) 12 番の事案と同じ。	
10	委託先（上記事案（番号８）の事業者）において、情報インフラ基盤の運用・保守業務を行っており、複数社から従業者に関する個人データの取扱いの委託を受けていたところ、ＶＰＮ経由でネットワーク内のサーバに不正アクセスを受け、当該個人データについて漏えいのおそれが生じた。侵入に使用されたＶＰＮのアカウントは残置されたテスト用アカウントであり、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。 事業者については、委託先に対する個人データの取扱いの委託に当たり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についての把握に問題がある等、委託先の監督が不十分であることが認められた。 ※(ⅲ) 13 番の事案と同じ。	委託先の監督の不十分
11	事業者は、就職イベントを主催しているところ、イベント参加者の個人データを管理するシステムに不正アクセスがあり、当該個人データについて漏えいが生じた事案。本件システムに使用されていたデータベース管理ツールについて、アクセス制限をしないまま運用し、かつ、管理者アカウントの認証情報が脆弱な設定となっていたこと等が原因と考えられる。 ※(ⅲ) 14 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）
12	事業者の従業者の業務用ＰＣ端末から侵入されてサーバに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のおそれが生じた事案。当該ＰＣ端末においては、誤ってグローバルＩＰアドレスが設定されていた上、常用されていない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。 ※(ⅲ) 15 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）

（iii）アクセス制御の設定ミス

	事案の概要	指導事項
1	事業者は、宿泊施設向けの予約管理の一元化システムを利用していたところ、当該システムにおける本件ホテルのアカウントに不正アクセスがあり、顧客に関する個人データについて漏えいが生じた事案。事業者は、過去にも同様の不正アクセスによる漏えい等事案が生じていたにもかかわらず、当該システム運営者が推奨するＩＰアドレス制限等の措置を行わなかったこと等に不備が認められた。	技術的安全管理措置 （外部からの不正アクセス等の防止）
2	事業者の従業者がサポート詐欺に遭い、業務用ＰＣが遠隔操作されたことで、当該ＰＣに保管されていた顧客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。事業者においては、顧客の個人データが閲覧可能なＰＣ端末にログインする必要がない業務を行う従業者にも、当該端末のログイン権限を与え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）
3	事業者がプログラム管理システムの認証情報を外部から閲覧可能な状態にしていたことにより、攻撃者に当該認証情報を窃取・悪用され、当該管理システムに不正アクセスを受け、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事案。当該認証情報の保管方法や保管していたサーバの管理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）
4	事業者の顧客管理システムが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事案。当該システムのログイン画面を外部に公開する必要がないにもかかわらず、アクセス制限が適切になされておらず、また、認証ログインの試行回数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 （外部からの不正アクセス等の防止）
5	事業者がＥＣサイトを運営していたところ、当該サイト内のファイル管理ツールの設定不備に起因する脆弱性を突かれた不正アクセスがあり、顧客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。当該管理ツールの管理者画面について適切なアクセス制御が行われておらず、第三者が管理者画面におけるファイルアップロード機能を利用できる状態となっていたこと等が原因と考えられる。 ※（ｉ）(b) 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）
6	事業者のサーバが、グローバルＩＰアドレスが付与されたＳＩＭを搭載したＰＣ端末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のおそれが生じた事案。初期侵入されたＰＣ端末に対して、ブルートフ	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
	オース攻撃がなされたところ、事業者においては、認証ログインの試行回数制限が設定されていなかったこと等が原因と考えられる。	
7	事業者の事務局担当者が入会申込者に関する個人データを個人のクラウドストレージサービスに保管していたところ、当該担当者のアカウントに不正ログインされ、クラウドストレージサービス内の個人データについて漏えいのおそれが生じた事案。本事案発生時、個人データの取扱いに係る規律が整備されておらず、個人データの保管場所についてのルールが存在し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
8	事業者は、ファミリーレストランを全国展開する事業者から委託を受け、従業者のシフトのスケジュール等を管理するシステムについて、保守管理等していたところ、データベースサーバが不正アクセスを受け、委託元の従業者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。事業者は、委託業務を他の事業者に再委託する際に、ＶＰＮルータのポート開放を行った上、データベース管理システムの認証情報を脆弱な設定と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）
9	事業者のデータベースサーバが第三者から不正アクセスを受け、当該サーバ内の個人データが一部窃取又は削除されたことにより、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事案。ウェブサーバの設定に誤りがあり、外部からサーバの認証情報等を容易に取得できる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 （アクセス者の識別と認証）
10	事業者が利用する各種管理ツールに対し、不正アクセスがあり、当該ツールを利用する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。本来外部からアクセスできない環境で運用する予定であったため脆弱性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。	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	事業者は、情報インフラ基盤の運用・保守業務を行っており、複数社から従業者に関する個人データの取扱いの委託を受けていたところ、ＶＰＮ経由でネットワーク内のサーバに不正アクセスを受け、当該個人データについて漏えいのおそれが生じた。侵入に使用されたＶＰＮのアカウントは残置されたテスト用アカウントであり、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）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）
12	委託先（上記事案（番号 11）の事業者）において、情報インフラ基盤の運用・保守業務を行っており、複数社から従業者に関する個人データの取扱いの委託を受けていたところ、ＶＰＮ経由でネットワーク内のサーバに不正アクセスを受け、当該個人データについて漏えいのおそれが生じた。侵入に使用されたＶＰＮのアカウントは残置されたテスト用アカウントであり、認証情報が脆弱な設	委託先の監督の不十分

	事案の概要	指導事項
	定であったこと等が原因と考えられる。 事業者については、委託先に対する個人データの取扱いの委託に当たり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についての把握に問題がある等、委託先の監督が不十分であることが認められた。 ※（ⅱ）９番の事案と同じ。	
13	委託先（上記事案（番号 11）の事業者）において、情報インフラ基盤の運用・保守業務を行っており、複数社から従業者に関する個人データの取扱いの委託を受けていたところ、ＶＰＮ経由でネットワーク内のサーバに不正アクセスを受け、当該個人データについて漏えいのおそれが生じた。侵入に使用されたＶＰＮのアカウントは残置されたテスト用アカウントであり、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。 事業者については、委託先に対する個人データの取扱いの委託に当たり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についての把握に問題がある等、委託先の監督が不十分であることが認められた。 ※（ⅱ）10 番の事案と同じ。	委託先の監督の不十分
14	事業者は、就職イベントを主催しているところ、イベント参加者の個人データを管理するシステムに不正アクセスがあり、当該個人データについて漏えいが生じた事案。本件システムに使用されていたデータベース管理ツールについて、アクセス制限をしないまま運用し、かつ、管理者アカウントの認証情報が脆弱な設定となっていたこと等が原因と考えられる。 ※（ⅱ）11 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）
15	事業者の従業者の業務用ＰＣ端末から侵入されてサーバに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のおそれが生じた事案。当該ＰＣ端末においては、誤ってグローバルＩＰアドレスが設定されていた上、常用されていない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 番の事案と同じ。	技術的安全管理措置 （アクセス者の識別と認証）
16	事業者は、システム開発を受託し、これに伴い、委託元の従業者に係る個人データの取扱いの委託を受けていたところ、システム開発に利用していたサーバがＲＤＰ接続による不正アクセスを受	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
	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、委託元の従業者に係る個人データについて漏えいが生じた事案。ＩＰアドレス制限を行わずにＲＤＰ接続を利用し、また、サーバ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。	
17	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、従業者及び顧客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。何らかの原因によりサーバの全ポートが外部に公開された状態となっていたところ、これを検知する体制を整備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）

イ　その他の事案

	事案の概要	指導事項
1	事業者が他の事業者からコールセンター業務を受託して行うに当たり、顧客の個人データについて取扱いの委託を受けていたところ、事業者の元従業者が社内に侵入し、当該個人データを持ち出した可能性があり、これにより当該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、適切なアクセス制御や、個人情報データベース等を取り扱うサーバやコンピュータ等の情報システムを管理する区域について適切な管理が行われていなかったこと等が原因と考えられる。	物理的安全管理措置 （個人データを取り扱う区域の管理） 技術的安全管理措置 （アクセス制御）
2	事業者は、個別信用購入あっせん業者であるところ、ある加盟店の倒産リスクが高まったことから、当該加盟店に対し、システムで管理する顧客に関する個人データの提供（一括ダウンロード）を要請した。当該個人データには、事業者と契約する顧客に関する個人データと契約外顧客に関する個人データが混在していたところ、事業者は契約外顧客については本人の同意を得ずに第三者提供されたものであることを知りながら個人データを取得したものであるため、不正の手段による個人情報の取得に当たり、個人情報保護法第 20 条第１項について指導を行った。	適正取得（個人情報保護法第 20 条第１項）違反
3	事業者が、複数の漏えい等事態について、漏えい等報告（13 件）を行っていなかった事案（保健所による監査において指摘があり発覚）。個人情報保護法の理解不足及び漏えい等事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制の不備等が原因と考えられる。	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）
4	事業者が運営する病院において、事業者からビル管理業務を委託されている業者の従業者が廃棄予定のＰＣ端末及び端末に搭載されていたＳＳＤを不正の目的をもって持ち出したことにより、ＰＣ端末等に記録されていた患者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。事業者においては、廃棄予定として機械室に当該ＰＣ端末等を保管してから実際に廃棄作業を行うまでの約８か月間、データを削除せずに置いたままにしており、当該ＰＣの盗難又は紛失等を防止するために適切な管理が行われていなかったこと等が原因と考えられる。	物理的安全管理措置 （機器及び電子媒体等の盗難等の防止）
5	令和８年１月、東北地方の大雪に係る対応として、青森県等４県に対し、オンライン資格確認システムの災害時モードが有効化された。これにより、青森県内の医療機関においては、本人確認を行わずに本件システムから患者の情報を閲覧できる状況となったところ、青森県内のクリニックである事業者は、過去に貸与した医療機器が返却されないまま連絡がとれなくなった患者の住所を確認するために、本件システムを利用したという事案。このような当該システムからの個人情報の取得	適正取得（個人情報保護法第 20 条第１項）違反

	事案の概要	指導事項
	が偽りその他不正の手段による個人情報の取得であるとして、個人情報保護法第 20 条第１項について指導を行った。	
６	地方公共団体から受託した「物価高騰対策指定収集袋配布事業」について、配送方法の変更により宛名ラベルの貼り替え作業が必要になったところ、当該地方公共団体との合意とは異なり、元のラベルの上に、別人のラベルを貼るという方法により配送を行ったため、元のラベルに記載された個人データが配送先に漏えいしたという事案。事業者においては、個人データが漏えいすることを認識できたにもかかわらず、従業者に個人データの適正な取扱いについて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。	人的安全管理措置 （従業者の教育）
７	事業者は、クリニックから電子カルテシステム機器のリプレイス作業を委託されていたところ、廃棄の委託を受けて持ち帰った機器を事務室内で適切に管理せず紛失し、当該機器に保管されていたクリニックの患者に関する個人データについて漏えいが生じた事案。個人データを取り扱う機器の盗難等の防止のための適切な管理が実施できていなかったこと等が原因と考えられる。	物理的安全管理措置 （機器及び電子媒体等の盗難等の防止）
８	委託先（上記事案（番号７）の事業者）において、クリニックから電子カルテシステム機器のリプレイス作業を委託されていたところ、廃棄の委託を受けて持ち帰った機器を事務室内で適切に管理せず紛失し、当該機器に保管されていたクリニックの患者に関する個人データについて漏えいが生じた事案。個人データを取り扱う機器の盗難等の防止のための適切な管理が実施できていなかったこと等が原因と考えられる。 事業者については、契約における安全管理措置に関する合意内容が不十分であり、委託先における個人データの取扱状況についての把握に問題がある等、委託先の監督が不十分であることが認められた。	委託先の監督の不十分

▽　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			人的	物理的	
		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	従業者の教育	個人データを取り扱う区域の管理	機器及び電子媒体等の盗難等の防止
指導等件数	1	1	1	2	1	1	2

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	14	21	3	12	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
指導等件数	2	7	7	4	5

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	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	1	3	4	2	17

※　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	25	10	15

※　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 43 件　※

・マスキング処理が不十分であることや添付ファイル内の保有個人情報の削除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。
・指導等の内容として、媒体の管理等の不備（７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、31 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	廃棄予定であった心身障害児医療費関係書類の所在が不明となり（職員が誤って古紙回収用置き場に移動させたため、古紙回収業者が回収し、製紙工場で融解された可能性が高い）、要配慮個人情報を含む保有個人情報（個人番号も含む）について漏えいのおそれが生じた事案。廃棄置き場に運ぶ前に、事務室に一時的に保管していた間、行政文書の廃棄方法を知らない職員が古紙回収置き場に移動させたものであり、保有個人情報が記録された媒体の保管方法に問題があったこと等が原因と考えられる。 ※Ⅱ２（１）２番の事案と同じ。	媒体の管理等
２	地方公共団体が管理する障害児者サポートセンターにおいて、相談記録簿を誤廃棄し、要配慮個人情報を含む保有個人情報について滅失が生じた事案。保存期間が正しく管理されておらず、保存期間が異なる文書を同じファイルで管理していたこと等が原因と考えられる。	媒体の管理等
３	地方公共団体がインターネットで公開している例規集システムにおいて、不妊治療費助成交付要綱の中で不妊治療費助成事業台帳をエクセルファイルを用いて掲載していたところ、同ファイルの非表示シートの中に、本来公開すべきでない不妊治療費助成者名簿が含まれており、助成を受けた者の個人情報が閲覧可能な状態となっていたことで、漏えいが生じた事案。公開を予定している情報と非公開の助成者名簿を同じエクセルファイルで管理し、非表示シートの存在にも気づかなかった等、ウェブサイトへの誤掲載を防止するための確認体制に問題があったこと等が原因と考えられる。	誤送付等の防止
４	職業安定所において、２年度分の雇用保険被保険者離職証明書等を誤廃棄し、滅失が生じた事案。作業効率を優先するために、正規に作成した一覧表ではなく、職員が作成した誤った廃棄メモを用	媒体の管理等

	事案の概要	指導事項
	い、一人の職員で照合や箱詰めを行ったため、確認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、１年度分の被留置者診療簿が所在不明となり（誤廃棄の可能性が高い）、要配慮個人情報を含む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。当該警察署においては、業務上の利便性のために、名簿つづりから本件資料のみを取り出して保管していたところ、分冊登録をしておらず、ファイルの背表紙の記載も適切ではなかったこと等が原因と考えられる。	媒体の管理等
6	地方公共団体において、職員の預金口座振替による振込受付書の所在が不明となり（誤廃棄の可能性が高い）、職員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。当該文書の保存期間変更の際、背表紙の記載を更新せずに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	公立小学校において、児童の学籍に関する情報を取りまとめた指導要録が誤って廃棄され、児童に関する保有個人情報について滅失が生じた事案。保存年限を記載したラベルと実際の保存年限が一致していない状態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
8	行政機関は、民間事業者が提供する大容量ファイル転送システム（オンプレミス）を利用していたところ、攻撃者が同システムの保守用アカウントにログインし、本件システムの脆弱性を突いてＯＳコマンドインジェクション攻撃[5]を行ったことにより、職員及び国民に関する保有個人情報について漏えいのおそれが生じた事案。インターネットでアクセス可能な保守用アカウントの認証情報の強度や管理が不十分であったこと等が原因と考えられる。	アクセス制御
9	警察署において、物件事故捜査管理簿の所在が不明となり（誤廃棄の可能性が高い）、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。当該文書の保管の際、表紙や背表紙に保存期間を誤って記載し保管するなど保管方法に問題があったこと等が原因と考えられる。	媒体の管理等
10	元職員が、在職中に、鉱山が休止・廃止した際の鉱業権者の氏名が記載された名簿を機構が利用していたファイル転送サービスにアップロードした上で、私用アドレスを用いてダウンロードする等したことにより、保有個人情報について漏えいが生じた事案。当該保有個人情報が保管されているデータベースファイルへのアクセス状況に関する監査・点検が実施されていなかったこと等が原因と考えられる。	監査及び点検の実施

[5] 外部からの入力を介して不正にＯＳのコマンドを実行させるＯＳコマンドインジェクションへの脆弱性を突いた攻撃

	事案の概要	指導事項
11	情報公開制度に基づき文書を開示するに当たり、非開示とするべき保有個人情報に関する箇所については、マスキング処理して公開したところ、当該処理が不十分であったため、ＰＣ上で一定の操作を行うとマスキングを外すことができ、テキストデータが閲覧可能な状態となっていた。これにより保有個人情報（安全運転管理者選任事業、古物商、風俗営業等の一覧に記載された氏名及び電話番号）が漏えいした事案。開示に当たり、マスキング処理の確認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
12	特定検診業務において、職員が地方公共団体の福祉事業所に対し、当該事業所に関係する住民の保険証情報、がん検診無料クーポン情報等をエクセルファイルでメール送信する際、当該ファイルに、がん検診無料クーポンの対象となる町民リストが記録された別シートが含まれたまま送信したことにより、当該事業所とは無関係の町民に関する保有個人情報の漏えいが生じた事案。保有個人情報を含むファイルを電子メールで送信する際の確認に問題があったこと等が原因と考えられる。	誤送付等の防止

▽　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			監査及び点検の実施
	アクセス制御	媒体の管理等	誤送付等の防止	
指導等件数	1	7	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

組織区分	国の行政機関等	地方公共団体等
指導等件数	3	9

※　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	3	6	3	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 1 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、従業者に関する個人データ（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の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）
２	廃棄予定であった心身障害児医療費関係書類の所在が不明となり（職員が誤って古紙回収用置き場に移動させたため、古紙回収業者が回収し、製紙工場で融解された可能性が高い）、要配慮個人情報を含む保有個人情報（個人番号も含む）について漏えいのおそれが生じた事案。廃棄置き場に運ぶ前に、事務室に一時的に保管していた間、行政文書の廃棄方法を知らない職員が古紙回収置き場に移動させたものであり、保有個人情報が記録された媒体の保管方法に問題があったこと等が原因と考えられる。 ※Ⅱ１（１）②１番の事案と同じ。	物理的安全管理措置（機器及び電子媒体等の盗難等の防止）
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、従業者に関する個人データ（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のアカウント等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（アクセス制御、アクセス者の識別と認証）
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、従業者及び顧客等に関する個人データ並びに従業者に関する特定個人情報について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ず放置していたこと等が原因と考えられる。 ※Ⅱ１（１）①ア（ｉ）(a) ５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。

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

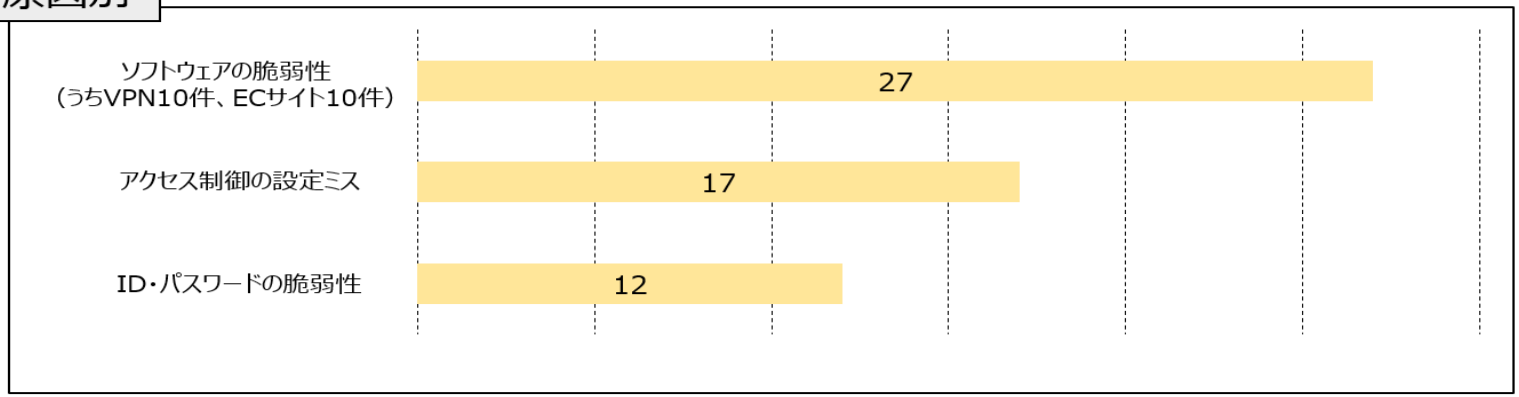
権限行使日 （参照箇所）	対象	改善策の実施状況
令和８年２月 25 日 （https://www.ppc.go.jp/files/pdf/260225_houdou.pdf）	埼玉県所沢市	・委員会は、所沢市の元職員が、①戸籍謄本等の公用申請、②住民基本台帳ネットワークシステム及び③統合宛名システムを不正に利用し、親族の個人番号を含む個人情報を不正に取得した事案に関して、所沢市に対し、令和８年２月 25 日に個人情報保護法第 157 条及びマイナンバー法第 33 条の規定による指導を行い、改善策の実施状況について、個人情報保護法第 156 条の規定による資料提出等及びマイナンバー法第 35 条第１項の規定による報告等を求めていた。 ・所沢市から、令和８年３月 31 日に報告書の提出を受け、改善策の実施状況等について確認したところ、市の担当部署がまとめて公用申請請求書を発送する場合、宛先それぞれの、対象者、本籍地、担当者名、用途を明記した管理簿を作成し、上司の決裁を受け、決裁を受けた管理簿を文書番号と紐づけて管理するなどの改善策が実施され、また、同改善策の形骸化を防ぐ制度や、職員がルールを守る仕組みの構築について、継続的に取り組んでいくことが確認された。 ・委員会としては、今後も、所沢市が改善策を確実に実施していくことを引き続き注視していく。

以　上

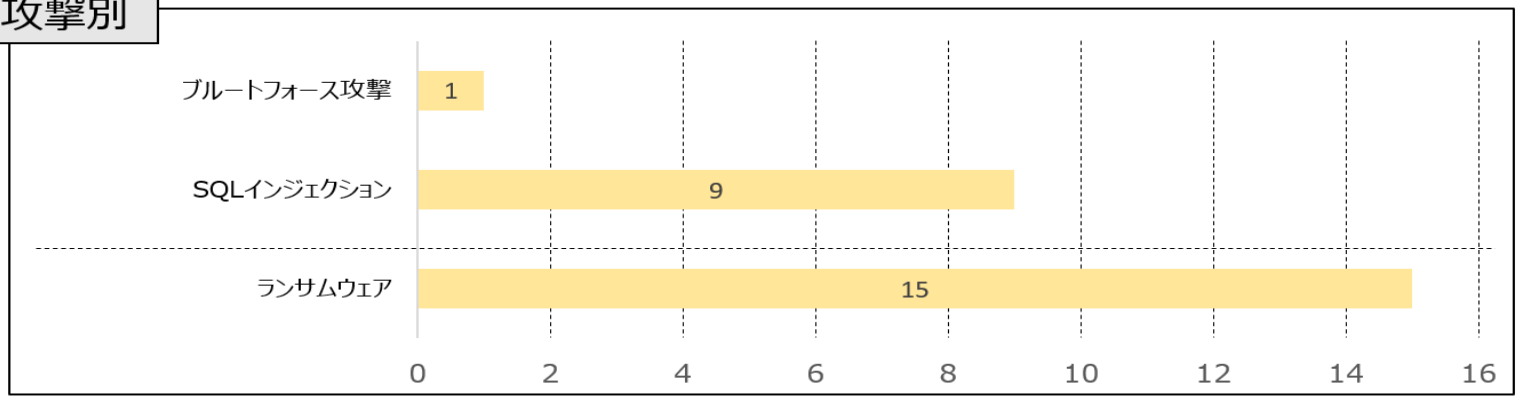
（参考）指導案件のうち不正アクセス事案の原因分析（令和８年度第１四半期）

（全体件数　45）

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（45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。