資料３－１

令和８年●月●日

個人情報保護委員会

令和７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７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８年２月 25 日	埼玉県所沢市	指導	個人情報保護法、マイナンバー法	埼玉県所沢市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に基づく行政上の対応について（https://www.ppc.go.jp/news/press/2025/260225/）

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 157 件[1]

①　民間事業者　計 115 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、23 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、本人の同意を得ずに個人データを第三者に提供した（個人情報保護法第 27 条第１項違反）事案、個人情報の取得が適正ではなかった（同法第 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（20 件）、次いで、委託先に対する監督の不備（19 件）が多かった。このほか、アクセス者の識別と認証の不備（10 件）、情報システムの使用に伴う漏えい等の防止の不備（８件）などに

---

[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。

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、55 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、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）
３	事業者は、委託先のホスティングサービス（サーバのレンタルサービス）を受け、同社のサーバを利用してホテル運営のためのシステムを構築し、委託先に対し、当該システムの保守・運用を委託していたところ、委託先のサーバ等が不正アクセスを受けた影響が当該サーバにも及び、ランサムウェアに感染した結果、ファイルが暗号化された。これにより、当該システムで管理されている顧客（宿泊者）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。	委託先の監督の不十分
４	事業者（上記事案（番号３）の委託先）は、自社のサーバ及びホスティングサービス（サーバのレンタルサービス）を利用して構築した運営のためのシステムの保守・運用の委託を受けていたところ、当該サーバ等が不正アクセスを受けた影響が、委託元のサーバにも及び、ランサムウェアに感染した結果、ファイルが暗号化された。これにより、当該システムで管理されている顧客（宿泊者）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	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
	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。	
５	事業者のサーバがＶＰＮ経由で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。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）
６	事業者のサーバが不正アクセスを受け（経路不明であるがＶＰＮ機器経由であった可能性もある）、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（他の事業者から取扱いの委託を受けて取り扱っていた個人データも含む）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、事業者が利用していたサーバの中にはサポートが終了していたものがあり、また、ハードウェアの保守契約の期限が切れていたこと、サーバ内に保管されていた個人データを適切に把握していなか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 （個人データの取扱状況を確認する手段の整備） 技術的安全管理措置 （外部からの不正アクセス等の防止）
７	委託先（上記事案（番号６）の事業者）のサーバが不正アクセスを受け（経路不明であるがＶＰＮ機器経由であった可能性もある）、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（他の事業者から取扱いの委託を受けて取り扱っていた個人データも含む）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、委託先が利用していたサーバの中にはサポートが終了していたものがあり、また、ハードウェアの保守契約の期限が切れていたこと、サーバ内に保管されていた個人データを適切に把握していなかったこと等が原因と考えられる。 ※Ⅱ２（１）２番の事案と同じ。	委託先の監督の不十分
８	委託先（上記事案（番号６）の事業者）のサーバが不正アクセスを受け（経路不明であるがＶＰＮ機器経由であった可能性もある）、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（他の事業者から取扱いの委託を受けて取り扱っていた個人データも含む）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、委託先が利用していたサーバの中にはサポートが終了していたものがあり、また、ハードウェアの保守契約の期限が切れていたこと、サーバ内に保管されていた個人データを適切に把握していなかったこと等が原因と考えられる。 ※Ⅱ２（１）３番の事案と同じ。	委託先の監督の不十分

	事案の概要	指導事項
９	委託先（上記事案（番号６）の事業者）のサーバが不正アクセスを受け（経路不明であるがＶＰＮ機器経由であった可能性もある）、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（他の事業者から取扱いの委託を受けて取り扱っていた個人データも含む）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、委託先が利用していたサーバの中にはサポートが終了していたものがあり、また、ハードウェアの保守契約の期限が切れていたこと、サーバ内に保管されていた個人データを適切に把握していなかったこと等が原因と考えられる。 ※Ⅱ２（１）４番の事案と同じ。	委託先の監督の不十分
10	委託先（上記事案（番号６）の事業者）のサーバが不正アクセスを受け（経路不明であるがＶＰＮ機器経由であった可能性もある）、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（他の事業者から取扱いの委託を受けて取り扱っていた個人データも含む）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、委託先が利用していたサーバの中にはサポートが終了していたものがあり、また、ハードウェアの保守契約の期限が切れていたこと、サーバ内に保管されていた個人データを適切に把握していなかったこと等が原因と考えられる。 ※Ⅱ２（１）５番の事案と同じ。	委託先の監督の不十分
11	委託先（上記事案（番号６）の事業者）のサーバが不正アクセスを受け（経路不明であるがＶＰＮ機器経由であった可能性もある）、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（他の事業者から取扱いの委託を受けて取り扱っていた個人データも含む）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、委託先が利用していたサーバの中にはサポートが終了していたものがあり、また、ハードウェアの保守契約の期限が切れていたこと、サーバ内に保管されていた個人データを適切に把握していなかったこと等が原因と考えられる。 ※Ⅱ２（１）６番の事案と同じ。	委託先の監督の不十分
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、従業者及び顧客等に関する個人データ（グループ会社から取扱いを委託されていた個人データも含む）及び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	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
	られる。 ※Ⅱ２（１）７番の事案と同じ。	
13	委託先（上記事案（番号 12）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、従業者及び顧客等に関する個人データ（グループ会社から取扱いを委託されていた個人データも含む）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。	委託先の監督の不十分
14	委託先（上記事案（番号 12）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、従業者及び顧客等に関する個人データ（グループ会社から取扱いを委託されていた個人データも含む）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。	委託先の監督の不十分
15	委託先（上記事案（番号 12）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、従業者及び顧客等に関する個人データ（グループ会社から取扱いを委託されていた個人データも含む）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。	委託先の監督の不十分
16	委託先（上記事案（番号 12）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、従業者及び顧客等に関する個人データ（グループ会社から取扱いを委託されていた個人データも含む）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。	委託先の監督の不十分
17	委託先（上記事案（番号 12）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、従業者及び顧客等に関する個人データ（グループ会社から取扱いを委託されていた個人データも含む）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。	委託先の監督の不十分
18	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	技術的安全管理措置

	事案の概要	指導事項
	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、ＶＰＮアカウントの認証情報（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。 ※（ⅱ）５番の事案と同じ。	（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、従業者に関する個人データ（特定個人情報も含む）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、ＶＰＮのゲスト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。 ※（ⅱ）６番の事案、Ⅱ２（１）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）
20	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（事業者のグループ会社等から取扱いの委託を受けていたものも含む）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。事業者は顧客に関するクレジットカード情報も保持していたが、取り扱う個人データの性質に見合った安全管理措置の見直しや改善が十分に実施できていなかったことにも問題点が認められた。 ※（ⅱ）８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 （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）
21	委託先（上記事案（番号 20）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（事業者のグループ会社等から取扱いの委託を受けていたものも含む）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。委託先は顧客に関するクレジットカード情報も保持していたが、取り扱う個人データの性質に見合った安全管理措置の見直しや改善が十分に実施できていなかったことにも問題点が認められた。	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） 委託先の監督の不十分
22	委託先（上記事案（番号 20）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（事業者のグループ会社等から取扱いの委託を受けていたものも含む）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。委託先は顧客に関するクレジットカード情報も保持していたが、取り扱う個人デー	委託先の監督の不十分

	事案の概要	指導事項
	タの性質に見合った安全管理措置の見直しや改善が十分に実施できていなかったことにも問題点が認められた。	

(b) ＥＣサイトの脆弱性

	事案の概要	指導事項
1	事業者及び委託元のチケット販売データを管理するデータベースサーバがＳＱＬインジェクション攻撃による不正アクセスを受け、チケットを購入した者に関する個人データが窃取されたことにより、漏えいが生じた事案。事業者が、運用が終了した旧ＥＣサイトの削除を忘れ、データベースサーバに接続したままにしており、旧ＥＣサイトに存在した脆弱性を攻撃者に突かれ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	事業者及び委託先（上記事案（番号１）の事業者）のチケット販売データを管理するデータベースサーバがＳＱＬインジェクション攻撃による不正アクセスを受け、チケットを購入した者に関する個人データが窃取されたことにより、漏えいが生じた事案。委託先が、運用が終了した旧ＥＣサイトの削除を忘れ、データベースサーバに接続したままにしており、旧ＥＣサイトに存在した脆弱性を攻撃者に突かれたこと等が原因と考えられる。	委託先の監督の不十分
3	事業者が運営するＥＣサイト等を管理するサーバに設置されていたシステム監視ツールの脆弱性を突かれた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及び漏えいのおそれが生じた事案。当該監視ツールについて、パッチ適用やアクセス制御の見直し等の必要な管理が実施されていなかったこと等が原因と考えられる。 ※(ⅲ) ７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	事業者がＥＣサイト構築のために利用していたプラットフォームに脆弱性があり、攻撃者から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。事業者において、当該プラットフォームの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）
5	事業者がＥＣサイトを運営していたところ、当該サイトを構築しているサーバが不正アクセスを受け、当該サーバにおいて保管されていた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。当該サイトにファイルアップロード機能が実装されていたところ、アップロー	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
	ド可能なファイルの容量や拡張子制限がされていなかったことから、攻撃者に不正ファイルをアップロードされたこと等が原因と考えられる。	

(c) その他の脆弱性

	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、事業者の従業者等の個人データ及び取引先の特定個人情報について、漏えい及び漏えいのおそれが生じた事案。リモートアクセスのために使用していた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	事業者のウェブサイトが不正アクセスを受け、ウェブサイトのデータベースに保存されていた顧客に関する個人データについて、漏えいが生じた事案。委託先において当該サイトのサーバ移設作業を行った際に、公開領域に設置したデータベースのダンプファイルが、作業完了後も削除されていなかったこと等が原因と考えられる。	委託先の監督の不十分
3	委託元（上記事案（番号２）の事業者）のウェブサイトが不正アクセスを受け、ウェブサイトのデータベースに保存されていた顧客に関する個人データについて、漏えいが生じた事案。事業者において当該サイトのサーバ移設作業を行った際に、公開領域に設置したデータベースのダンプファイルが、作業完了後も削除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）
4	婚活イベント事業を行っている事業者が、利用者のためのウェブサイトを開設し、ウェブアプリケーションで個人データを管理しており、当該ウェブアプリケーションの開発、保守及び運用については、他の事業者に委託していたところ、ウェブサイトがＳＱＬインジェクション攻撃を受け、データベースに保存されていた利用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。委託先における開発時にＳＱＬインジェクション攻撃に対する対策が不十分であったこと等が原因と考えられる。	委託先の監督の不十分
5	委託元（上記事案（番号４）の事業者）から、婚活イベント利用者のためのウェブサイトにおいて個人データを管理するためのウェブアプリケーションの開発、保守及び運用を委託されていたところ、ウェブサイトがＳＱＬインジェクション攻撃を受け、データベースに保存されていた利用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。事業者における開発時にＳＱＬインジェクション攻撃に対する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（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
6	事業者が運営している顧客向けウェブサイトが不正アクセスを受け、サーバ内に保存されていた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。事業者は、委託先に当該ウェブサイト及びウェブサーバの保守・管理を委託していたところ、CMS（Contents Management System）[5]のプラグインの更新について、委託先との間の責任分担を曖昧にしており、脆弱性対応ができ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	事業者が管理する職業紹介のためのウェブサイトがＳＱＬインジェクション攻撃による不正アクセスを受け、システム内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。システム改修の際に、ＳＱＬインジェクションに関する脆弱性を生じさせ、その後も適切な対策を講じられ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）
8	事業者が利用していたＮＡＳ（Network Attached Storage）が不正アクセスを受け、当該ＮＡＳで管理されていた従業者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。事業者は、当該ＮＡＳをインターネットに接続して使用していたところ、定期的なファームウェアのアップデートを行っておらず、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）
9	事業者のコーポレートサイトが不正アクセスを受け、当該サイトから問合せを行っ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、当該サイトの運用開始後から本件発覚まで、当該サイトを管理するために利用していたコンテンツ管理システムについて、セキュリティパッチの適用を実施しておらず、脆弱性が放置されていたこと等が原因と考えられる。	技術的安全管理措置（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	事業者が利用する宿泊・予約管理システムの管理者アカウントに、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事案。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（アクセス者の識別と認証）
2	事業者が運営するＥＣサイトの管理画面が不正アクセスを受け、当該ＥＣサイトの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。当該ＥＣサイトの構築・運用等を他の事業者	委託先の監督の不十分

[5] ＣＭＳとは、ウェブサイトを構築し、コンテンツ（ウェブページ、テキストや画像など）を統合的に管理するシステムである。

	事案の概要	指導事項
	に委託していたところ、管理画面に対するアクセス制限がなされていなかったこと、管理アカウント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。 ※(iii) １番の事案と同じ。	
３	事業者（上記事案（番号２）の委託先）は、委託元が運営するＥＣサイトの構築・運用等を委託されていたところ、当該ＥＣサイトの管理画面が不正アクセスを受け、当該ＥＣサイト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。管理画面に対するアクセス制限がなされていなかったこと、管理アカウント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。 ※(iii) ２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）
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のおそれ及び毀損が生じた事案。ＶＰＮアカウントの認証パスワードの強度に大きな問題があり、ブルートフォース攻撃により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）
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、ＶＰＮアカウントの認証情報（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。 ※(ｉ)(a) 18 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（特定個人情報も含む）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、ＶＰＮのゲスト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。 ※(ｉ)(a) 19 番、Ⅱ２（１）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、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。ＶＰＮアカウントの認証情報（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。	技術的安全管理措置 （アクセス者の識別と認証）
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、従業者及び顧客に関する個人データ（事業者のグループ会社等から取扱いの委託を受けていたものも含む）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	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）

	事案の概要	指導事項
	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。事業者は顧客に関するクレジットカード情報も保持していたが、取り扱う個人データの性質に見合った安全管理措置の見直しや改善が十分に実施できていなかったことにも問題点が認められた。 ※（ｉ）(a) 20 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	事業者が利用する顧客管理システムが不正アクセスを受け、当該システム上で管理されていた医療従事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。複数の従業者でテストアカウントを共用していたこと等の事情から、認証情報が漏えいしたこと等が原因と考えられる。また、事業者においては、不正アクセスを検知した当初の対応にも問題が認められた。	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） 技術的安全管理措置 （アクセス者の識別と認証）
10	事業者が動画配信サービスを会員向けに提供し、スマートフォン用アプリ等で利用可能なところ、アプリ向けサーバが不正アクセスを受け、会員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。当該アプリにおいては会員コードが記録されており、かつ、ある会員コードから他の会員の会員コードが推測容易なものであったこと、認証パラメータの再利用が可能であったことから攻撃者に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、情報システムの使用に伴う漏えい等の防止）

（iii）アクセス制御の設定ミス

	事案の概要	指導事項
１	事業者が運営するＥＣサイトの管理画面が不正アクセスを受け、当該ＥＣサイトの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。当該ＥＣサイトの構築・運用等を他の事業者に委託していたところ、管理画面に対するアクセス制限がなされていなかったこと、管理アカウント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。 ※（ⅱ）２番の事案と同じ。	委託先の監督の不十分
２	事業者（上記事案（番号１）の委託先）は、委託元が運営するＥＣサイトの構築・運用等を委託されていたところ、当該ＥＣサイトの管理画面が不正アクセスを受け、当該ＥＣサイト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。管理画面に対するアクセス制限がなされていなかったこと、管理アカウント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。 ※（ⅱ）３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）

	事案の概要	指導事項
３	攻撃者が事業者のカスタマーサービスセンターに架電し、担当者をだまして、当該担当者の端末にＡＰＩ（Application Programming Interface）をインストールさせ、攻撃者が利用する外部アプリケーションと事業者の顧客管理システムを接続するという手法により、当該顧客管理システムにおいて管理されていた顧客に関する個人データについて漏えいが生じた事案。事業者においては、アプリケーションの接続制限に関する対策が不十分で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） 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、カスタマーサポートサービスについて、カスタマーサポート管理システムを利用して問合せをした顧客に関する個人データを管理していたところ、攻撃者から当該システムのＡＰＩを悪用した不正アクセスを受け、当該個人データを窃取したことにより漏えい等が生じた事案。攻撃者に悪用されたＡＰＩが、任意のアカウントからアクセスできること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 （情報システムの使用に伴う漏えい等の防止）
５	事業者が行う研修事業に関し、研修受講者に関する個人データを管理していたシステムが第三者から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事案。事業者は、他の事業者に当該システムの開発、運用、保守等の委託に伴い個人データの取扱いを委託していたところ、委託先が、当該システムの新規アカウントを認証不要で登録することができる機能を有効にしていたため、第三者が管理権限のあるアカウントを作成し、不正ログインを行ったこと等が原因と考えられる。	委託先の監督の不十分
６	事業者（上記事案（番号５）の委託先）は、委託元が行う研修事業に関し、研修受講者に関する個人データを管理するシステムの開発、運用、保守等の委託に伴い個人データの取扱いを委託されていたところ、当該システムが第三者から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事案。事業者が、当該システムの新規アカウントを認証不要で登録することができる機能を有効にしていたため、第三者が管理権限のあるアカウントを作成し、不正ログインを行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）
７	事業者が運営するＥＣサイト等を管理するサーバに設置されていたシステム監視ツールの脆弱性を突かれた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及び漏えいのおそれが生じた事案。当該監視ツールについて、パッチ適用やアクセス制御の見直し等の必要な管理が実施されていなかったこと等が原因と考えられる。 ※（ｉ）(b) ３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）

	事案の概要	指導事項
８	事業者の従業者が業務で使用していた個人所有のＰＣが、認証情報窃取型マルウェアに感染した結果、攻撃者により個人データを含むファイルが窃取された可能性があり、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。事業者の社内規程においては、個人所有のＰＣを業務に利用すべきではない旨が規定されていたが、当該従業者だけでなくそれ以外の従業者も個人所有のＰＣを業務に使用してい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） 人的安全管理措置 （従業者の教育）
９	事業者のウェブサイトから問合せをした顧客の個人データを管理していたデータベースの認証情報が、インターネット上からアクセス可能な状態であったことから、認証情報を入手した攻撃者から当該データベース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のおそれが生じた事案。データベースの認証情報を記録したファイルの公開設定等を適切に管理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）
10	事業者が独立行政法人等から委託を受け、開発及び保守を行っていたイベント参加の応募者に関する受付システムにおいて、応募者の登録情報が外部から検索可能な状態であったことにより、応募者に関する個人データ（委託元の保有個人情報）について、漏えい及び漏えいのおそれが生じた事案。事業者が、応募者の登録情報の検索に関する設定を誤り、長期間にわたり、そのことに気付かなかったこと等が原因と考えられる。 ※イ　５番、②14 番の事案と同じ。	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）
11	事業者のウェブサーバが不正アクセスを受け、当該サーバのデータベース内に保管されていた顧客に関する個人データが削除されたことにより、当該個人データについて漏えいのおそれ及び滅失が生じた事案。当該データベースの接続情報がインターネット経由で外部から窃取可能な状態となっていたこと、データベース管理ツールの管理画面が不特定のＩＰアドレスから到達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 （外部からの不正アクセス等の防止）
12	事業者が会員の個人データを保管するシステムを管理するサーバが不正アクセスを受け、当該会員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、当該システムの保守・運用を他の事業者に委託していたところ、委託先におけるサーバの移行作業中に、当該システムの接続に関し、事業者の意向に応じた暫定的な対応を行う中で、委託先の設定ミス等によりインターネット経由で外部から当該システムにアクセス可能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
13	事業者（上記事案（番号 12）の委託先）は、会員の個人データを保管するシステムの保守・運用を委託されていたところ、当該システムを管理するサーバが不正アクセスを受け、会員に関する個人	組織的安全管理措置 （取扱状況の把握及び安全管

	事案の概要	指導事項
	データについて漏えいのおそれが生じた事案。事業者は、サーバの移行作業中に、当該システムの接続に関し、事業者の意向に応じた暫定的な対応を行う中で、設定ミス等によりインターネット経由で外部から当該システムにアクセス可能となっていたこと等が原因と考えられる。	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）
14	事業者は、地方公共団体から委託を受け、他の事業者とともに物価高騰対策賃上げ支援金の事務局を行っていたところ、事業者と他の事業者で構築していた情報共有のためのポータルサイトが外部から閲覧可能な状態となっており、同サイトで管理されていた、支援金申請事業者の担当者等に関する個人データ（委託元である地方公共団体の保有個人情報）について、漏えい及び漏えいのおそれが生じた事案。事業者が当該システムについて認証せずにアクセスできるような設定としていたこと等が原因と考えられる。 ※②18 番の事案と同じ。	技術的安全管理措置 （アクセス制御）

イ　その他の事案

	事案の概要	指導事項
1	事業者が、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。個人情報保護法の理解不足に起因した報告対応に関する不十分な体制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）
2	事業者が、本人の同意を得ることなく、従業者の前職に対し、当該従業者の氏名等の個人データを提供し、前職における在職期間等を確認した事案。個人情報保護法第 27 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）
3	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係る規程やマニュアルが存在せず、従業者に対する定期的な研修等が実施されてい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 人的安全管理措置 （従業者の教育）
4	事業者は定期的に講座を実施し、受講者からアンケートの回答等の個人データを取得していたところ、本人の同意なく当該アンケート回答を利用し、次回講座への勧誘等を行うために、アンケートに回答した受講者に関する個人データを第三者に提供した事案。個人情報保護法第 27 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）
5	事業者が独立行政法人等から委託を受け、開発及び保守を行っていたイベント参加の応募者に関する受付システムにおいて、応募者の登録情報が外部から検索可能な状態であったことにより、応募者に関する個人データ（委託元の保有個人情報）について、漏えい及び漏えいのおそれが生じた事案。事業者が、応募者の登録情報の検索に関する設定を誤り、長期間にわたり、そのことに気付かなかったこと等が原因と考えられる。 ※（ⅲ）10 番、②14 番の事案と同じ。	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）
6	地図の制作販売業者である事業者は、個人情報保護法第 27 条第２項の規定によるオプトアウト届出を委員会に提出しておらず、また、本人の同意を得ずに、地図上に居住者の氏を記載して住民に配布し、また、インターネット上で地図の販売を行っていた事案。個人情報保護法第 27 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）
7	事業者が運営するＥＣサイトにおいて、ＥＣサイト利用者が商品の注文画面で個人情報を入力したが、注文完了前に画面を閉じる等して注文手続を中止した場合にも、当該個人情報を取得し、後か	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
	ら、当該利用者に対しＳＭＳ等で購入を促す連絡等を行った事案。当該ＥＣサイトは、注文完了前に入力中の個人情報を取得することの記載はないこと、利用規約の同意欄のチェックは注文完了のボタンを押す際に行われること等の事実関係からすると、当該ＥＣサイトの利用者が、自己の個人情報を事業者に取得されることを認識又は予見することは難しく、かかる個人情報の取得は社会通念上、適正ではないことが認められた。	

▽　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
		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	従業者の教育
指導等件数	1	2	1	2	3	2

指導等の内容	安全管理措置				委託先の監督	第三者提供の制限	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	10	20	8	19	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	不動産業、物品賃貸業
指導等件数	5	9	4	2	9	1

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	医療、福祉	サービス業（他に分類されないもの）	分類不能の産業	不明
指導等件数	1	2	3	3	1	1	18

※　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	２	24	６	24

※　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 42 件　※

・メールの宛先誤り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（10 件）、誤送付等の防止の不備（４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、23 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	行政機関において、経営所得安定対策の支払のため、管轄地方公共団体内の加工用米等の届出数量について、複数の地域再生協議会に対し、エクセルファイルを協議会別に分けてメールで情報提供をしているところ、誤って、エクセルファイル内に当該地方公共団体内の全生産者の氏名、住所、出荷契約数量等が記載されたシートを含めたままメール送信したことにより、保有個人情報の漏えいが生じた事案。当時、エクセルファイルの作成部署とメールを送信する部署が異なっていたため、意思疎通や添付ファイルの内容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
２	行政機関が管理する資料（職員の個人情報が含まれるもの。一部に要配慮個人情報を含む）が、管理者の許可なく持ち出されたことにより、保有個人情報の漏えいが生じた事案。当該資料が保管されていた共有フォルダのアクセス制限に問題があったこと等が原因と考えられる。	アクセス制限
３	警察署において、約２年分の捜査関係事項照会書及び前科照会書の所在が不明となり、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が生じた事案。当該文書の保管の際、表紙や背表紙に定められた記載をしていなかったこと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
４	警察署において、自動車保管場所届出や緊急工事申請に関する書類の所在が不明となり、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事案。文書の保管方法に問題があり、保存期間を経過した廃棄予定の文書と保存期間満了前の資料の混同が生じたこと等が原因と考えられる。	媒体の管理等
５	地方公共団体の補助金申請業務について、職員が企業に対し、追加提出書類の作成例が入力されたエクセルファイルをメールで送信する際、当該ファイルに、過去の別業務で使用した保有個人情報が入力されたシートが含まれたまま送信したことにより、保有個人情報の漏えいが生じた事案。電	誤送付等の防止

	事案の概要	指導事項
	子メール送信の際の確認に問題があったこと等が原因と考えられる。	
6	警察署において、免許更新者の質問票等複数の種類の文書の所在が不明となり、保有個人情報について漏えいのおそれが生じた事案。保存する文書と廃棄予定の文書を明確に区別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
7	教育委員会が所管する小学校において、約 30 年分の卒業証書授与台帳が所在不明となったことにより、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事案。耐火書庫内に保管していたはずであったが、同書庫内の文書一覧は作成しておらず、また、同書庫内の文書の点検を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 監査・点検
8	地方公共団体の職員が年度切替えの文書引継ぎのため、文書のファイリング及び箱詰め作業を行い、作業中の行政文書を放置していたところ、誤って清掃業者によって回収され溶解されたことにより、保有個人情報について滅失が生じた事案。文書引継ぎ作業中の保管場所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
9	地方公共団体が地域農業経営基盤強化促進計画を、ウェブサイトにおいて公開するに当たり、保有個人情報を黒塗り処理して公開したところ、当該黒塗り処理が不十分であったため、当該文字部分をコピーして、文書作成ソフト等に貼付けを行うと閲覧可能な状態となっており、これにより保有個人情報（農業を担う者の氏名等）が漏えいした事案。ウェブサイトへの掲載に当たり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
10	地方公共団体の事務所において、業務上使用する必要がなくなったＰＣ端末３台の所在が不明となったことにより、地権者等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。不用決定をしてから廃棄するまでの端末の保管方法等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
11	地方公共団体の福祉事務所の職員が、休日夜間の緊急対応のために生活保護受給者等に関する個人情報が記載された資料を持ち出していたところ、電車の中に置き忘れたことにより、要配慮個人情報及びマイナンバーを含む保有個人情報について漏えいが生じた事案。当該福祉事務所では、持ち出しの際に記録が付けられておらず、また、持ち帰り用のファイルに必要以上の情報がつづられるなどの点に安全管理措置の不備が認められた。	媒体の管理等 保有個人情報の取扱状況の記録
12	自動車検査登録事務所において、継続検査申請関係書類を誤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。当該書類の保管方法に問題があり、廃棄すべき書類と保管すべき書類の混同が生じたこと等が原因と考えられる。	媒体の管理等

	事案の概要	指導事項
13	教育委員会が所管する中学校において、災害共済給付関係に必要な書類を誤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。誤廃棄自体について、組織としての安全管理措置の不備は認められなかったが、職員が誤廃棄による滅失に気付いてから校長に報告が上がるまでに２か月以上の時間がかかっており、漏えい等事態が生じた場合の対応に問題が認められた。	安全管理上の問題への対応
14	個人情報取扱事業者に開発及び保守を委託して行っていたイベント参加の応募者に関する受付システムにおいて、応募者の登録情報が外部から検索可能な状態であったことにより、応募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。事業者が、応募者の登録情報の検索に関する設定を誤り、長期間にわたり、そのことに気付かなかったこと等が原因と考えられる。 ※①ア（ⅲ）10 番、①イ５番の事案と同じ。	業務の委託等
15	行政機関の担当者は、源泉徴収票等作成事務を行うため、作業依頼を行うこととなり、各部局に職員及びその家族に関する個人情報をメールで送信するよう依頼した。その際、提出先メールアドレスとは異なる誤ったメールアドレスを伝達したところ、幾つかの部局が誤ったメールアドレスに送信したことにより、保有個人情報が外部に流出し、漏えいが生じた事案。 作業依頼をする際のメールアドレスの記載の確認、各部局がメールを送信する際の宛先の確認、ファイルのパスワード設定が不十分であったこと等が原因と考えられる。 ※Ⅱ２（１）９番の事案と同じ。	誤送付等の防止
16	行政機関の採用試験の不合格者の検査表（要配慮個人情報を含む）が所在不明となり、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事案。規程に従った保管場所以外の場所で保管する運用になっており、また、適切な背表紙が付されていないファイルにつづるなど廃棄文書と区別がつか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
17	警察署において、被保護者動静等確認票等の書類を誤廃棄したことにより、保有個人情報の滅失が生じた事案。数年前に当該資料等の保存期間を変更した際に保存方法の変更等を適切に行わなかったこと等が原因と考えられる。	媒体の管理等
18	地方公共団体から委託を受け、物価高騰対策賃上げ支援金の事務局を行っていた個人情報取扱事業者が構築していた情報共有のためのポータルサイトについて、外部から閲覧可能な状態となっており、同サイトで管理されていた、支援金申請事業者の担当者等に関する個人データ（当該地方公共団体の保有個人情報）について、漏えい及び漏えいのおそれが生じた事案。事業者が当該システムについて認証せずにアクセスできるような設定としていたこと等が原因と考えられる。	業務の委託等

	事案の概要	指導事項
	※①ア（iii）14 番の事案と同じ。	
19	地方公共団体の選挙執行期間中にＳＤカード６枚をケースに入れて執務室で保管していたところ、そのうち５枚がケースごと所在不明となり、保有個人情報（選挙人に関する個人情報）について漏えいが生じた事案。選挙執行期間中は施錠できない机の引き出しで保管するなど保管の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

▽　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			
	アクセス制限	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	10	4	2

指導等の内容	個人情報の取扱いの委託	安全管理上の問題への対応	監査及び点検の実施
指導等件数	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	6	13

※　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	2	14	1	2

※　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 12 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	事業者のサーバが不正アクセスを受け（経路不明であるがＶＰＮ機器経由であった可能性もある）、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（他の事業者から取扱いの委託を受けて取り扱っていた特定個人情報も含む）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、事業者が利用していたサーバの中にはサポートが終了していたものがあり、また、ハードウェアの保守契約の期限が切れていたこと、サーバ内に保管されていた特定個人情報を適切に把握していなかっ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。	組織的安全管理措置 （取扱状況を確認する手段の整備） 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	委託先（上記事案（番号１）の事業者）のサーバが不正アクセスを受け（経路不明であるがＶＰＮ機器経由であった可能性もある）、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（他の事業者から取扱いの委託を受けて取り扱っていた特定個人情報も含む）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、委託先が利用していたサーバの中にはサポートが終了していたものがあり、また、ハードウェアの保守契約の期限が切れていたこと、サーバ内に保管されていた特定個人情報を適切に把握していなかったこと等が原因と考えられる。 ※Ⅱ１（１）①ア（ｉ）(a) ７番の事案と同じ。	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）のサーバが不正アクセスを受け（経路不明であるがＶＰＮ機器経由であった可能性もある）、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（他の事業者から取扱いの委託を受けて取り扱っていた特定個人情報も含む）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、委託先が利用していたサーバの中にはサポート	委託先の監督の不十分

	事案の概要	指導事項
	が終了していたものがあり、また、ハードウェアの保守契約の期限が切れていたこと、サーバ内に保管されていた特定個人情報を適切に把握していなかったこと等が原因と考えられる。 ※Ⅱ１（１）①ア（ｉ）(a) ８番の事案と同じ。	
４	委託先（上記事案（番号１）の事業者）のサーバが不正アクセスを受け（経路不明であるがＶＰＮ機器経由であった可能性もある）、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（他の事業者から取扱いの委託を受けて取り扱っていた特定個人情報も含む）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、委託先が利用していたサーバの中にはサポートが終了していたものがあり、また、ハードウェアの保守契約の期限が切れていたこと、サーバ内に保管されていた特定個人情報を適切に把握していなかったこと等が原因と考えられる。 ※Ⅱ１（１）①ア（ｉ）(a) ９番の事案と同じ。	委託先の監督の不十分
５	委託先（上記事案（番号１）の事業者）のサーバが不正アクセスを受け（経路不明であるがＶＰＮ機器経由であった可能性もある）、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（他の事業者から取扱いの委託を受けて取り扱っていた特定個人情報も含む）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、委託先が利用していたサーバの中にはサポートが終了していたものがあり、また、ハードウェアの保守契約の期限が切れていたこと、サーバ内に保管されていた特定個人情報を適切に把握していなかったこと等が原因と考えられる。 ※Ⅱ１（１）①ア（ｉ）(a) 10 番の事案と同じ。	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）のサーバが不正アクセスを受け（経路不明であるがＶＰＮ機器経由であった可能性もある）、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（他の事業者から取扱いの委託を受けて取り扱っていた特定個人情報も含む）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、委託先が利用していたサーバの中にはサポートが終了していたものがあり、また、ハードウェアの保守契約の期限が切れていたこと、サーバ内に保管されていた特定個人情報を適切に把握していなかったこと等が原因と考えられる。 ※Ⅱ１（１）①ア（ｉ）(a) 11 番の事案と同じ。	委託先の監督の不十分
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	技術的安全管理措置

	事案の概要	指導事項
	ルが暗号化され、従業者及び顧客等に関する特定個人情報（グループ会社から取扱いを委託されていた特定個人情報も含む）及び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) 12 番の事案と同じ。	（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、従業者に関する個人データ（特定個人情報も含む）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、ＶＰＮのゲスト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。 ※Ⅱ１（１）①ア（ｉ）(a) 19 番、Ⅱ１（１）①ア（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	行政機関の担当者は、源泉徴収票等作成事務を行うため、作業依頼を行うこととなり、各部局に職員及びその家族に関する特定個人情報をメールで送信するよう依頼した。その際、提出先メールアドレスとは異なる誤ったメールアドレスを伝達したところ、幾つかの部局が誤ったメールアドレスに送信したことにより、特定個人情報が外部に流出し、漏えいが生じた事案。 作業依頼をする際のメールアドレスの記載の確認、各部局がメールを送信する際の宛先の確認、ファイルのパスワード設定が不十分であったこと等が原因と考えられる。 ※Ⅱ１（１）②15 番の事案と同じ。	漏えい等の防止
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、従業者に関する個人データ（特定個人情報も含む）について漏えいのおそれが生じた事案。事業者はサポートが終了したＶＰＮ機器を使用しており、脆弱性が存在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）
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、従業者及び顧客に関する個人データ及び従業者に関する特定個人情報について漏えいのおそれが生じた事案。ＶＰＮ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 （アクセス者の識別と認証）

(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

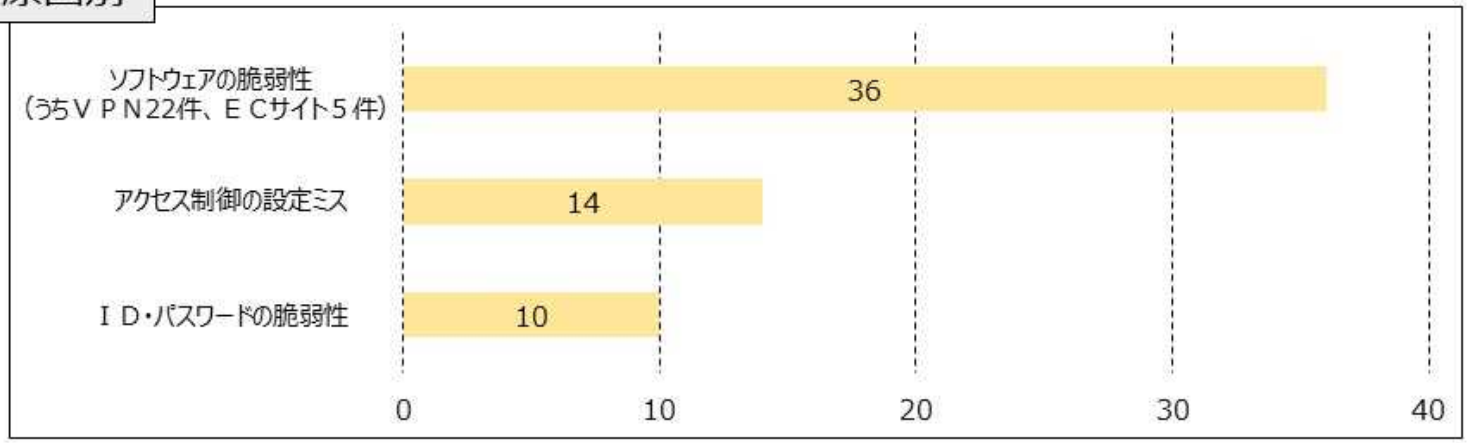
・なし

以　　上

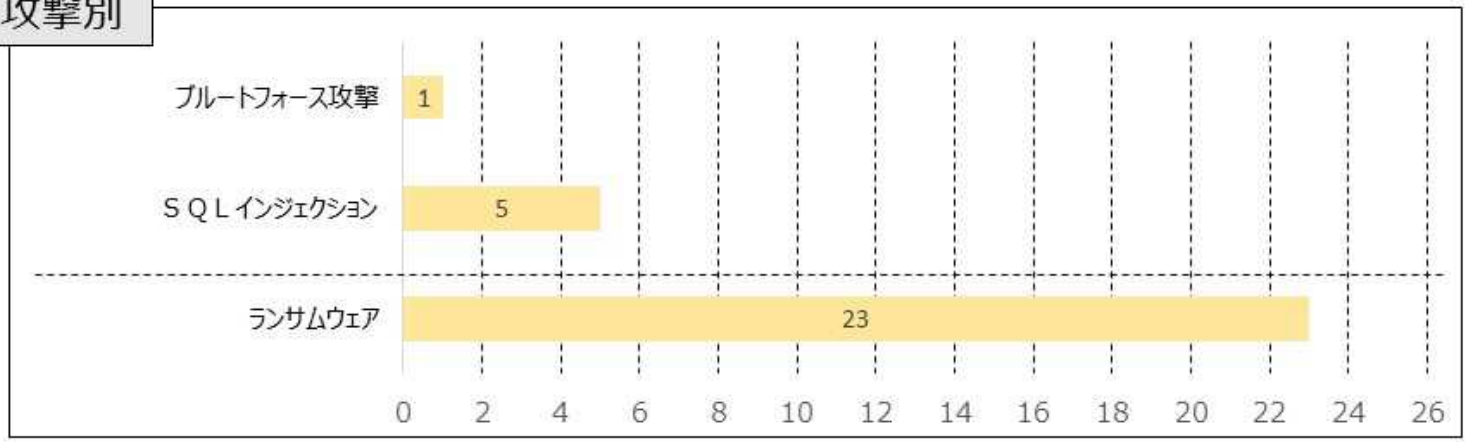
（参考）指導案件のうち不正アクセス事案の原因分析（令和７年度第４四半期）

（全体件数　53）

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（53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。