令和７年 12 月 10 日
個人情報保護委員会

令和７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７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７年９月 10 日	株式会社中央ビジネスサービス	勧告及び報告徴収	個人情報保護法	株式会社中央ビジネスサービス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/250910_houdou.pdf）

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 136 件[1]

①　民間事業者　計 105 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]、ＥＣサイトへのクロスサイトスクリプティング攻撃[3]や、ウェブサイトのＳＱＬインジェクション攻撃[4]などがみられているほか、ランサムウェア攻撃[5]も、22 件みられている。
・不正アクセス以外の漏えい等事案では、従業者が、私的な目的で私物ＰＣから個人データをダウンロードした事案や本人の同意を得ていない個人データの第三者提供（個人情報保護法第 27 条第１項違反）といった事案もみられた。
・指導等の内容としては、特に技術的安全管理措置に関し、外部からの不正アクセス等の防止の不備が最も多く（29 件）、次いで、ア

---

[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] 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。

[5] 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。

クセス者の識別と認証の不備（18 件）が多かった。このほか、組織的安全管理措置の不備（５件）、委託先に対する監督の不備（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、53 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	事業者が管理するサーバがＶＰＮ経由で不正アクセスを受け、マルウェアに感染した結果、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。当該ＶＰＮ機器の認証情報の強度に問題があったこと、当該サーバのＯＳのサポートが切れてい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）
２	事業者はアルバムの制作業務の委託（個人データの取扱いの委託を含む）を受けていたところ、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、ファイルが暗号化され、委託元の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。当該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ため、脆弱性を突かれたこと、当該ＶＰＮ機器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）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）
３	事業者は、グループ会社から個人データの取扱いの委託を受けて、事業者及びグループ会社の従業者の個人データを同一のサーバで管理していたところ、当該サーバがＶＰＮ経由で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。当該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ため、脆弱性を突かれたこと、不正アクセスに利用された管理者権限を有するＶＰＮ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）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）
４	事業者は、グループ会社から情報システム全般の管理を委託（個人データの取扱いの委託を含む）されていたところ、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	技術的安全管理措置（アクセス者の識別と認証、外

	事案の概要	指導事項
	た結果、ファイルが暗号化され、グループ会社の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。初期侵入に利用されたＶＰＮアカウントの認証情報の強度に問題があったこと、当該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ため、脆弱性を突かれたこと等が原因と考えられる。 ※（ⅱ）14 番の事案と同じ	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、従業者の特定個人情報を含む個人データ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。当該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ため、脆弱性を突かれ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 （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、顧客等の個人データについて漏えいが生じた事案。不正アクセスに利用されたＶＰＮアカウントの認証情報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 （外部からの不正アクセス等の防止）
７	事業者が管理するサーバが、子会社（外国に所在）が利用していたＶＰＮ経由で不正アクセスを受け、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。当該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ため、脆弱性を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 （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、株主、従業者等の個人データについて、漏えい及び毀損が生じた事案。不正アクセスに利用されたＶＰＮアカウントの認証情報の強度に問題があったこと、当該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ため、脆弱性を突かれたこと等が原因と考えられる。 ※（ⅱ）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）

(b)　ＥＣサイトの脆弱性

	事案の概要	指導事項
1	事業者は、顧客企業の担当者向けにメールマガジンを配信するためのサイトを管理しており、当該管理に当たっては、委託先及び再委託先（いずれも個人データの取扱いの委託を含む）が提供する共有サーバを利用していたところ、当該サイトがクロスサイトスクリプティング攻撃による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。当該サイトを構築するソフトウェアの管理者権限を持つアカウントの認証情報の強度に問題があったこと、当該ソフトウェア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ため、脆弱性を突かれたこと等が原因と考えられる。 ※（ⅱ）２番の事案、（ⅲ）１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	事業者が運営するＥＣサイト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のおそれが生じた事案。当該ＥＣサイトの構築に使用していたソフトウェア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）
3	事業者が運営するＥＣサイトが、クロスサイトスクリプティング攻撃による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。事業者が利用するＥＣサイト構築システムに関し、脆弱性情報や対策等が公表されていたにもかかわらず対応を行わないまま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）
4	事業者が運営するＥＣサイトが、クロスサイトスクリプティング攻撃による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。事業者が利用するＥＣサイト構築システムに関し、脆弱性情報や対策等が公表されていたにもかかわらず対応を行わないまま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）

(c) その他の脆弱性

	事案の概要	指導事項
1	事業者は、配送業務等の委託（個人データの取扱いの委託を含む）を受けていたところ、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、委託元である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。当該サーバ上で稼働していたソフトウェア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ため、脆弱性を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（外部からの不正アクセス等の防止）
2	事業者は、会員向けアプリの開発、保守、点検等を委託（個人データの取扱いの委託を含む）していたところ、第三者に顧客情報等の一部が閲覧された結果、事業者の顧客の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。当該アプリには、リニューアルした時から複数の設定不備が存在し、これらが放置されていたことが原因と考えられる。	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、会員向けアプリの開発、保守、点検等を委託（個人データの取扱いの委託を含む）されていたところ、第三者に顧客情報等の一部が閲覧された結果、委託元である事業者の顧客の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。当該アプリには、リニューアルした時から複数の設定不備が存在し、これら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（情報システムの使用に伴う漏えい等の防止）
4	事業者は、ソフトウェアの開発等の委託等（いずれも個人データの取扱いの委託を含む）を受けていたところ、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、委託元である事業者の従業者の特定個人情報を含む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。侵入口となったサーバについて脆弱性が公表されていたにもかかわらず放置され、また、横展開されたサーバについてもサポート切れのまま放置されていたため、これらの脆弱性を突かれたこと等が原因と考えられる。 ※（ⅱ）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（外部からの不正アクセス等の防止）
5	事業者は、複数の委託元から、ウェブサイト等の開発、運用、保守等の業務の委託（個人データの取扱いの委託を含む）を受け、複数の委託元のウェブサイトを同一のサーバで管理していたところ、そのうち１つのウェブサイト経由で複数の委託元のウェブサイトが不正アクセスを受け、委託元の個人データについて漏えいのおそれが生じた事案。初期侵入されたウェブサイトを構築したソフトウェアの脆弱性を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（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	事業者は、グループ会社から従業員等の個人データの取扱いの委託を受け、事業者が管理するサーバに当該個人データを保存し、当該サーバの保守、運用等を他の事業者に再委託（個人データの取扱いの委託を含む）していたところ、当該サーバが不正アクセスを受け、事業者及び委託元であるグループ会社の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。当該サーバへの接続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ため、脆弱性を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 （外部からの不正アクセス等の防止）
７	事業者（上記事案（番号６）の委託元）は、グループ会社に従業員等の個人データの取扱いを委託していたところ、委託先である事業者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グループ会社の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。当該サーバへの接続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ため、脆弱性を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
８	事業者は、サーバの移行作業を委託（個人データの取扱いの委託を含む）していたところ、当該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、従業者等の特定個人情報を含む個人データについて漏えいが生じた事案。事業者の従業者がフィッシングメールから不正なサイトにアクセスしたこと、当該サーバ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ため、脆弱性を突かれ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） 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（上記事案（番号８）の委託先）は、サーバの移行作業の委託（個人データの取扱いの委託を含む）を受けていたところ、当該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、委託元の従業者等の特定個人情報を含む個人データについて漏えいが生じた事案。委託元である事業者の従業者がフィッシングメールから不正なサイトにアクセスしたこと、当該サーバ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ため、脆弱性を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 （外部からの不正アクセス等の防止）
10	事業者のウェブサイトの管理画面が不正アクセスを受け、当該ウェブサイトから問合せをした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。当該ウェブサイトの構築に使用していたソフトウェア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ため、脆弱性を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 （外部からの不正アクセス等の防止）
11	事業者のＮＡＳ（Network Attached Storage）等が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、顧客の個人データについて、漏えい及び漏えいのお	技術的安全管理措置 （アクセス者の識別と認証、外

	事案の概要	指導事項
	それが生じた事案。当該ＶＰＮ機器の認証情報の強度に問題があったこと、事業者が放置していたＯＳの脆弱性を突かれたこと等が原因と考えられる。 ※（ⅱ）10 番の事案と同じ	部からの不正アクセス等の防止）
12	事業者が運営するウェブサイトが、ＳＱＬインジェクション攻撃による不正アクセスを受け、顧客の個人データについて漏えいが生じた事案。当該ウェブサイトに存在したＳＱＬインジェクション攻撃に対する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）
13	事業者が使用するクラウドストレージサービスが不正アクセスを受け、ランサムウェアに感染した結果、当該ストレージ内の全データが削除されたことにより、顧客の個人データについて滅失及び漏えいのおそれが生じた事案。当該ストレージサービスでは、登録されたＩＰアドレスのみが利用可能な設定とすることができたが、事業者がＩＰアドレス制限等を実施していなかったことが原因と考えられる。 ※（ⅱ）13 番の事案、（ⅲ）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）
14	事業者が運営するウェブサイトが、ＳＱＬインジェクション攻撃による不正アクセスを受け、顧客の個人データについて漏えいが生じた事案。当該ウェブサイトに存在したＳＱＬインジェクション攻撃に対する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、情報システムの使用に伴う漏えい等の防止）
15	事業者は、ウェブサイトの開発、保守等について委託（個人データの取扱いの委託を含む）を受けていたところ、当該ウェブサイトが、ＳＱＬインジェクション攻撃による不正アクセスを受け、委託元の顧客の個人データについて漏えいのおそれ等が生じた事案。当該ウェブサイトに存在したＳＱＬインジェクション攻撃に対する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 （情報システムの使用に伴う漏えい等の防止）
16	事業者のサーバがＵＴＭ（Unified Threat Management[6]）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、従業者の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。当該ＵＴＭ機器が最新の状態ではなく、放置されていた脆弱性を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 （外部からの不正アクセス等の防止）

[6] 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。

（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	事業者がグループ会社と共に利用するサーバが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、事業者グループの従業者の特定個人情報を含む個人データ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。当該ＶＰＮ機器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。	技術的安全管理措置 （アクセス者の識別と認証）
2	事業者は、顧客企業の担当者向けにメールマガジンを配信するためのサイトを管理しており、当該管理に当たっては、委託先及び再委託先（いずれも個人データの取扱いの委託を含む）が提供する共有サーバを利用していたところ、当該サイトがクロスサイトスクリプティング攻撃による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。当該サイトを構築するソフトウェアの管理者権限を持つアカウントの認証情報の強度に問題があったこと、当該ソフトウェア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ため、脆弱性を突かれたこと等が原因と考えられる。 ※（ⅰ）(b) １番の事案、（ⅲ）１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）
3	事業者が管理するサーバがＶＰＮ経由で不正アクセスを受け、マルウェアに感染した結果、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。当該ＶＰＮ機器の認証情報の強度に問題があったこと、当該サーバのＯＳのサポートが切れていたこと等が原因と考えられる。 ※（ⅰ）(a) １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	事業者は、ソフトウェアの開発等の委託等（いずれも個人データの取扱いの委託を含む）を受けていたところ、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、委託元である事業者の従業者の特定個人情報を含む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。侵入口となったサーバについて脆弱性が公表されていたにもかかわらず放置され、また、横展開されたサーバについてもサポート切れのまま放置されていたため、これらの脆弱性を突かれたこと等が原因と考えられる。 ※（ⅰ）(c) 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 （外部からの不正アクセス等の防止）

	事案の概要	指導事項
5	事業者はアルバムの制作業務の委託（個人データの取扱いの委託を含む）を受けていたところ、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、ファイルが暗号化され、委託元の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。当該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ため、脆弱性を突かれたこと、当該ＶＰＮ機器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。 ※（ｉ）(a) ２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、顧客（投資家）の特定個人情報を含む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。侵入に利用された管理者権限を有するＶＰＮアカウントの認証情報を把握できていなかった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）
7	事業者は、システム開発、ネットワーク構築等の業務の委託（個人データの取扱いの委託を含む）を受け、委託元に成果物等を提出する際に事業者が管理するファイル送信ツールを使用していたところ、当該ツールがブルートフォース攻撃による不正アクセスを受け、委託元の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。当該ツール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。	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、グループ会社から個人データの取扱いの委託を受けて、事業者及びグループ会社の従業者の個人データを同一のサーバで管理していたところ、当該サーバがＶＰＮ経由で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。当該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ため、脆弱性を突かれたこと、不正アクセスに利用された管理者権限を有するＶＰＮ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。 ※（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、外部からの不正アクセス等の防止）
9	事業者はニュースの配信サービスを運営し、委託元となる配信依頼企業から、配信先の個人データの取扱いの委託を受けていたところ、事業者のサーバが不正アクセスを受け、配信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。事業者が当該サーバの管理者画面へのアクセスを許容するＩＰアドレスや同画面でのログインに必要な認証情報の棚卸しを実施していなかったこと等が原因と考えられる。 ※(iii)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
10	事業者のＮＡＳ（Network Attached Storage）等が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、顧客の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ＶＰＮ機器の認証情報の強度に問題があったこと、事業者が放置していたＯＳの脆弱性を突かれたこと等が原因と考えられる。 ※（ｉ）(c) 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、外部からの不正アクセス等の防止）
11	事業者は医療機関であり、複数の委託元から健康診断の実施等の委託（個人データの取扱いの委託を含む）を受けていたところ、事業者の電子カルテを管理等する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、事業者及び委託元の個人データについて漏えい、毀損及び漏えいのおそれが生じた事案。当該システムで利用されるアプリケーションのログイン画面が外部に公開されていたこと、当該アプリケーションの管理者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。	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）
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、事業者の従業者の特定個人情報を含む、事業者及び委託元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。当該ＶＰＮ機器のアカウントについて棚卸し等が実施されておらず、初期侵入に利用されたアカウントの存在を把握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）
13	事業者が使用するクラウドストレージサービスが不正アクセスを受け、ランサムウェアに感染した結果、当該ストレージ内の全データが削除されたことにより、顧客の個人データについて滅失及び漏えいのおそれが生じた事案。当該ストレージサービスでは、登録されたＩＰアドレスのみが利用可能な設定とすることができたが、事業者がＩＰアドレス制限等を実施していなかったことが原因と考えられる。 ※（ｉ）(c) 13 番の事案、（iii） 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）
14	事業者は、グループ会社から情報システム全般の管理を委託（個人データの取扱いの委託を含む）されていたところ、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、ファイルが暗号化され、グループ会社の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。初期侵入に利用されたＶＰＮアカウントの認証情報の強度に問題があったこと、当該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ため、脆弱性を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 （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) ４番の事案と同じ	
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、従業者の特定個人情報を含む個人データ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。不正アクセスに利用された管理者権限を持つアカウントについて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。	技術的安全管理措置（アクセス者の識別と認証）
16	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。不正アクセスに利用された管理者権限を有するＶＰＮ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。	技術的安全管理措置（外部からの不正アクセス等の防止）
17	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、顧客等の個人データについて、漏えい及び毀損が生じた事案。不正アクセスに利用されたＶＰＮ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。	技術的安全管理措置（アクセス者の識別と認証）
18	事業者が利用するクラウドストレージサービスが不正アクセスを受け、従業者等の特定個人情報を含む個人データについて漏えいが生じた事案。不正アクセスに利用された当該サービスの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。	技術的安全管理措置（アクセス者の識別と認証）
19	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、顧客等の個人データについて、漏えいのおそれが生じた事案。不正アクセスに利用された当該サーバの管理者権限を有する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。	技術的安全管理措置（アクセス者の識別と認証）
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、株主、従業者等の個人データについて、漏えい及び毀損が生じた事案。不正アクセスに利用されたＶＰＮアカウントの認証情報の強度に問題があったこと、当該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ため、脆弱性を突かれ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）

（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、顧客企業の担当者向けにメールマガジンを配信するためのサイトを管理しており、当該管理に当たっては、委託先及び再委託先（いずれも個人データの取扱いの委託を含む）が提供する共有サーバを利用していたところ、当該サイトがクロスサイトスクリプティング攻撃による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。当該サイトを構築するソフトウェアの管理者権限を持つアカウントの認証情報の強度に問題があったこと、当該ソフトウェア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ため、脆弱性を突かれたこと等が原因と考えられる。 ※（ⅰ）(b) １番の事案、（ⅱ）２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	事業者のサーバが不正アクセスを受け、株主、従業者等の個人データについて、漏えいが生じた事案。事業者が当該サーバの仕様を把握しておらず、攻撃者が当該サーバ上のファイル一覧を閲覧でき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	事業者はニュースの配信サービスを運営し、委託元となる配信依頼企業から、配信先の個人データの取扱いの委託を受けていたところ、事業者のサーバが不正アクセスを受け、配信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。事業者が当該サーバの管理者画面へのアクセスを許容するＩＰアドレスや同画面でのログインに必要な認証情報の棚卸しを実施していなか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）
4	事業者が使用するクラウドストレージサービスが不正アクセスを受け、ランサムウェアに感染した結果、当該ストレージ内の全データが削除されたことにより、顧客の個人データについて滅失及び漏えいのおそれが生じた事案。当該ストレージサービスでは、登録されたＩＰアドレスのみが利用可能な設定とすることができたが、事業者がＩＰアドレス制限等を実施していなかったことが原因と考えられる。 ※（ⅰ）(c) 13 番の事案、（ⅱ）13 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、従業者の特定個人情報を含む個人データ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。当該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	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

	事案の概要	指導事項
	たため、脆弱性を突かれたこと等が原因と考えられる。 ※（ｉ）(a) ５番の事案と同じ	止）
６	事業者が個人データを含むデータの移行作業の委託（個人データの取扱いの委託を含む）を受けていたところ、当該作業に利用していた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、委託元の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。事業者が、当該サーバを直接インターネットに公開していたこと、移行作業を依頼されたデータを、個人データを含むデータとして管理し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 （個人データの取扱状況を確認する手段の整備） 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（上記事案（番号６）の委託元）が個人データを含むデータの移行作業を委託（個人データの取扱いの委託を含む）していたところ、当該作業に利用していた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。委託先である事業者が、当該サーバを直接インターネットに公開していたこと、移行作業を依頼されたデータを、個人データを含むデータとして管理し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
８	事業者は予約管理システムを運営し、当該システムを利用する委託元から、予約をする顧客の個人データの取扱いの委託を受けているところ、当該システムのＡＰＩ（Application Programming Interface）に存在した不具合を第三者に利用され、委託元の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、当該システムを導入するに当たっての脆弱性テスト等によって、当該不具合を発見でき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）
９	事業者が運営するウェブサイトにおいて、ＡＰＩ経由で社内システムへのアクセスキーが取得可能な状態となっていたため、同システムに不正アクセスされ、当該ウェブサイトで登録した会員の個人データが漏えいした事案。当該ウェブサイト開発時の検証用プログラムに組み込まれていた社内システムにアクセスするためのアクセストークンが、開発終了後もそのまま残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）

イ　その他の事案

	事案の概要	指導事項
1	事業者は医療機関であるところ、事業者の代表者が、患者の氏名、診察内容等を、インターネット上のクチコミに投稿することで、本人の同意なく第三者に提供していた事案。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）
2	事業者は、委託元（独立行政法人）が運営する学校が利用するクラウドサービスを提供し、委託元から個人データの取扱いの委託を受けていたところ、当該サービス上で管理されている情報が第三者により閲覧可能な状態となったことで、学生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、当該状態となる可能性を考慮せず当該サービスの改修を行い、改修後も安全性の見直し等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 （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）
3	事業者が、本人の同意を得ることなく、個人データを含む契約関係情報を、電話で第三者（本人の家族を装う者等）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）
4	事業者の従業者がサポート詐欺に遭い、当該従業者が使用する業務用ＰＣに保存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。業務用ＰＣの取扱いについて明確なルールが周知されていないこと、個人データの取扱いについて定期的な研修を実施していなか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）
5	事業者が、約２年間、多数の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及び漏えい等事案が生じた際に責任ある立場の者へ速やかに報告がなされる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）
6	事業者（学校）の従業者（教員）が、最終出勤日以降、私的な目的で私物ＰＣから事業者のシステムにログインし生徒等の個人データをダウンロードしたことで、当該個人データについて漏えいが生じた事案。最終出勤日の時点で、当該私物ＰＣの利用状況を確認しなかったこと、私物ＰＣから自由に事業者のシステムにログイン可能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 （アクセス制御）
7	事業者はアプリケーションを活用してイベントを開催しているところ、イベント参加者が申込みをする際に、個人データの第三者提供の同意を求める文言に記載漏れがあり、その結果、本人の同意を得ることなく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）

	事案の概要	指導事項
8	事業者の従業者がテレワーク中にサポート詐欺に遭い、当該従業者が使用する業務用ＰＣに保存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。当該従業者が、事業者の規程に反して、個人データを保存したＰＣを取り扱っており、事業者において当該状況を把握し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 （取扱状況の把握及び安全管理措置の見直し）

▽　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
	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	2	1	1	1	2

指導等の内容	安全管理措置					
	技術的				委託先の監督	第三者提供の制限
	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	18	29	6	3	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	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	1	6	2	9	2	5	3

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	サービス業（他に分類されないもの）	不明
指導等件数	1	1	2	2	5	13

※　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	17	15	16

※　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 31 件　※

・ウェブサイトで公開していたファイルに個人情報が記載されたデータが残ってい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、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、19 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	地方公共団体の職員等の保有個人情報が記録された外付けハードディスクを紛失し、当該保有個人情報について漏えいのおそれが生じた事案。規程に従った管理ができていなかったこと、許可無く当該ハードディスクに保有個人情報が記録されていたこと等が原因と考えられる。	媒体の管理等 点検
２	独立行政法人（Ⅱ１（１）①イ その他の事案 ２番の委託元）が運営する高等専門学校においてクラウドサービスを利用し、当該サービスを提供する事業者に個人データの取扱いを委託していたところ、当該サービス上で管理されている情報が第三者により閲覧可能な状態となったことで、学生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が、当該状態となる可能性を考慮せず当該サービスの改修を行い、改修後も安全性の見直し等を実施していなかったこと等が原因と考えられる。	業務の委託等
３	地方公共団体の職員が当該地方公共団体のネットワークに不正にアクセスし、職員及び住民の情報を、私物のＵＳＢメモリにコピーして持ち出した事案。第三者への流出は確認されず、漏えいは生じていない。当該ネットワークの利用に当たり各職員に割り当てられるＩＤ及びパスワードの推測が容易であったこと等が原因と考えられる。	アクセス制御 アクセス状況の監視 記録機能を有する機器・媒体の接続制限
４	行政機関が有料会員に公開しているデータベースにおいて閲覧可能な情報の一部に、意図せず国民の氏名が記載されていたことで、保有個人情報の漏えいが生じた事案。当該データベースを作成するに当たり活用した資料に氏名が記載されていることを把握しないまま、データベースを作成したこと等が原因と考えられる。	誤送付等の防止

	事案の概要	指導事項
5	地方公共団体が、身体障害者の障害に係る保有個人情報が記録されたファイルを紛失し、当該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（誤廃棄の可能性が高い）。地方公共団体では、文書保存箱に廃棄年月等を記載し、保存箱毎に記録簿を作成等することになっていたが、当該規程に従った記録等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
6	地方公共団体が、新生児の情報等に係る保有個人情報が記載された紙のファイルを紛失し、当該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（誤廃棄の可能性が高い）。廃棄文書を保存する箱と廃棄しない文書を保存する箱を区別することなく同じ書庫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、ふるさと納税事業の委託先事業者との連絡手段として使用していたコミュニケーションツールについて、運用開始から第三者が閲覧可能な状態で使用を継続していたことにより、納税者等に関する保有個人情報が漏えいした事案。地方公共団体による当該ツールのアクセス制御の設定に不備があったことが原因と考えられる。	アクセス制御
8	地方公共団体が管理する文書管理箱が紛失したことにより、当該文書管理箱で保管されていた資料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（誤廃棄の可能性が高い）。地方公共団体では文書保管箱に保存期間等を記載したラベルを貼付けして管理することとしていたが、当該文書保管箱にはラベルを貼付けせず保管していたこと等が原因と考えられる。	媒体の管理等
9	地方公共団体が管理する届出書の一部が紛失し、当該届出書に記録された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（誤廃棄の可能性が高い）。地方公共団体では、当該届出書について、管理簿に記載することで管理していたにもかかわらずこれを怠っていたこと、当該届出書の管理を特定の職員に一任していたため点検ができ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 点検
10	地方公共団体のウェブサイトで公開していたファイルに、個人情報が記載されたデータが残っていたことにより、当該保有個人情報について漏えいのおそれが生じた事案。当該ファイルについては、ウェブサイトでの公開前に上長が確認することとなっていたにもかかわらず、当該確認が行われていなかったこと等が原因と考えられる。	誤送付等の防止
11	地方公共団体が管理する、投票結果等が記録された外付けＳＳＤ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。当該ＳＳＤについては、施錠可能な安全な場所に保管する等の規定が定められていたにもかかわらず、投票所においては、実質的に誰も管理していなかった状況であっ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
12	警察署において自主点検を実施したところ、犯罪事件受理簿の所在が不明となっていることが発覚した事案（誤廃棄の可能性が高い）。当該警察署では、当該犯罪事件受理簿を施錠設備のある倉庫の書棚に保管していたが、これを使用した者が元の保管場所に戻さなかったために、他の文書と紛れ込んだ可能性が高いことが原因と考えられる。	媒体の管理等 安全管理上の問題への対応

▽　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			情報システムにおける安全の確保等		
	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	アクセス制御	アクセス状況の監視	記録機能を有する機器・媒体の接続制限
指導等件数	5	2	2	2	1	1

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	1	1	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

組織区分	国の行政機関等	地方公共団体等
指導等件数	2	10

※　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	1	9	1	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７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	事業者がグループ会社と共に利用するサーバが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、事業者グループの従業者の特定個人情報を含む個人データ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。当該ＶＰＮ機器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。 ※Ⅱ１（１）①ア（ⅱ）１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	事業者は、ソフトウェアの開発等の委託等（いずれも個人データの取扱いの委託を含む）を受けていたところ、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、委託元である事業者の従業者の特定個人情報を含む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。侵入口となったサーバについて脆弱性が公表されていたにもかかわらず放置され、また、横展開されたサーバについてもサポート切れのまま放置されていたため、これらの脆弱性を突かれたこと等が原因と考えられる。 ※Ⅱ１（１）①ア（ⅰ）(c) ４番の事案、Ⅱ１（１）①ア（ⅱ）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 （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（投資家）の特定個人情報を含む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。侵入に利用された管理者権限を有するＶＰＮアカウントの認証情報を把握できていなかった等が原因と考えられる。 ※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）
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、事業者の従業者の特定個人情報を含む、事業者及び委託元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。当該ＶＰＮ機器のアカウントについて棚卸し等が実施されておらず、初期侵入に利用されたアカウントの存在を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（ⅱ）12 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
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、従業者の特定個人情報を含む個人データ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。不正アクセスに利用された管理者権限を持つアカウントについて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。 ※Ⅱ１（１）①ア（ⅱ）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）
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、従業者の特定個人情報を含む個人データ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。当該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ため、脆弱性を突かれたこと等が原因と考えられる。 ※Ⅱ１（１）①ア（ⅰ）(a) ５番の事案、Ⅱ１（１）①ア（ⅲ）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）
７	事業者が利用するクラウドストレージサービスが不正アクセスを受け、従業者等の特定個人情報を含む個人データについて漏えいが生じた事案。不正アクセスに利用された当該サービスの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。 ※Ⅱ１（１）①ア（ⅱ）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）

(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。

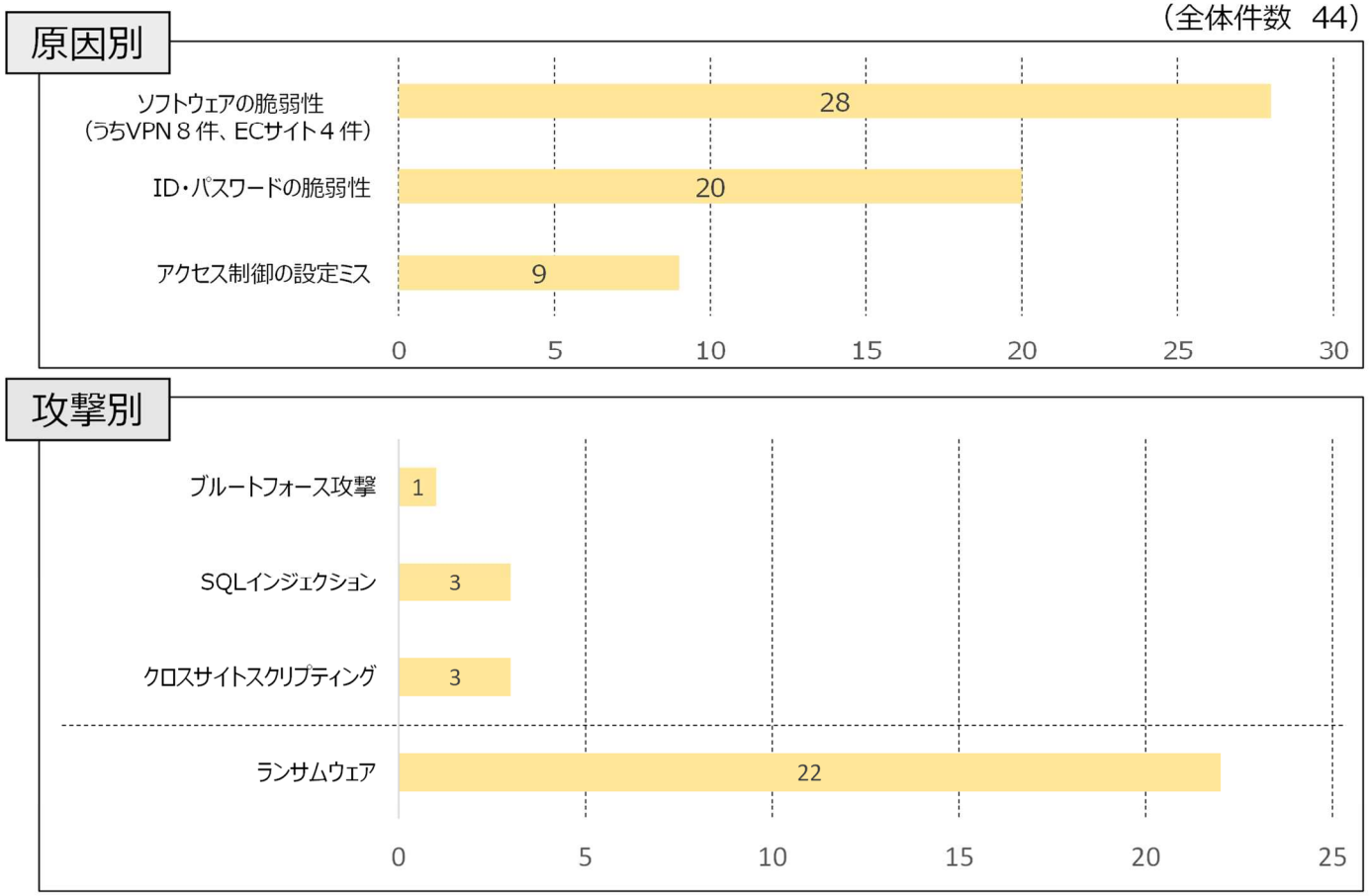
Ⅲ　公表事案に関する指導・助言等の対象先における改善策の実施状況

・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２四半期）

（全体件数　44）



（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（44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。