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３四半期における監視・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３四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 136 件[1]

①　民間事業者　計 104 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、14 件みられている。
・不正アクセス以外の漏えい等事案では、元従業者が退職後に顧客の個人データを持ち出した事案のほか、利用目的を明示しない個人情報の取得（個人情報保護法第 21 条第２項違反）や本人の同意を得ていない個人データの第三者提供（同法第 27 条第１項違反）といった事案もみられた。

---

[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] 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。

・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（23 件）、次いで、アクセス者の識別と認証の不備（17 件）が多かった。このほか、組織的安全管理措置の不備（10 件）、人的安全管理措置の不備（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、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、特定個人情報を含む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ため、脆弱性を突かれたこと等が原因と考えられる。 ※Ⅱ２（１）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。事業者が利用していた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、特定個人情報を含む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。 ※Ⅱ２（１）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）
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	技術的安全管理措置

	事案の概要	指導事項
	暗号化され、事業者及び委託元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。事業者が利用していた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	（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。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）
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並びに事業者及び委託元の顧客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）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）
７	事業者のグループ会社である外国事業者のネットワークに設置されていたＶＰＮ経由で、事業者のサーバが不正アクセスを受け、事業者のサーバ内のデータが窃取され、事業者の従業者や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事案。当該ＶＰＮ機器には多数の脆弱性が存在していたにもかかわらず、事業者が当該外国事業者のネットワークから事業者のサーバへの広範なアクセスを許容していたことが原因と考えられる。 ※（ⅲ）５番の事案、Ⅱ２（１）４番の事案と同じ	技術的安全管理措置 （アクセス制御）
８	事業者のサーバがＶＰＮ経由で不正アクセスを受け、個人データを含むファイルが外部に送信され、漏えいが生じた事案。事業者が利用していた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）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）
９	事業者は、グループ会社のサーバを一括して管理していた（個人データの取扱いの委託を含む）ところ、当該サーバがＶＰＮ経由で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顧	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
	客、従業者等の個人データについて漏えいが生じた事案。事業者が利用していた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。	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、不正アクセスに利用されたアカウントについて適切に管理がされていなかったこと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）
2	事業者が開発し運用しているＥＣサイトが不正アクセスを受け、会員である顧客の個人データについて漏えい等が生じた事案。当該サイトには開発当時から、ログイン後にＨＴＭＬソースコードを書き換えることにより、ログインした会員とは別の会員のページを開くことができる設計上の不備が存在したこと、多数の会員に関する個人データを取り扱うシステムであるにもかかわらず、脆弱性診断等を実施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 （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）
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サイトが不正アクセスを受け、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サイトにおいては、問合せフォームから画像ファイル等のアップロードが可能であったところ、当該機能を悪用され、マルウェアをアップロードさ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）

（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、ランサムウェアに感染した結果、ファイルが暗号化され、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。当該サーバについてファイアウォール等の不正アクセス防止のためのセキュリティ対策を適切に講じていなかったこと、不正アクセスに利用された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）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）
2	事業者の運用終了後のサーバがＳＱＬインジェクション攻撃を受け、当該サーバと接続されていたシステムに保管されていた委託元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。当該サーバが不要となった後も廃棄せずシステムに接続したままとし、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 （情報システムの使用に伴う漏えい等の防止）
3	事業者のサーバが不正アクセスを受け、メールマガジンの配信先の登録情報に関する個人データが漏えいした事案。事業者はメールマガジン配信用プログラムを利用していたところ、管理者権限の奪取や任意コマンドの実行などの脆弱性が公表され、対応方法がリリース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）
4	事業者の顧客向けのウェブサイトがパスワードリスト攻撃[6]による不正アクセスを受け、多数の顧客のマイページに不正なログインがなされた結果、当該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、ログ等の定期的な分析等による不正アクセスの検知を十分に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）
5	事業者はグループ会社が利用するシステムの開発及び維持管理業務の委託（個人データの取扱いの委託を含む）を受けていたところ、事業者が開発等しているウェブサービスが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が生じた事案。事業者が当該サービスにおけるセキュアコーディングを徹底しておらず、ＳＱＬインジェクション攻撃に対する脆弱性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 （外部からの不正アクセス等の防止）
6	事業者は、顧客がインターネットを利用して注文できるサービスを提供していたところ、当該サービスに利用するシステム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等が生じた事	組織的安全管理措置 （漏えい等事案に対応する体

[6] パスワードリスト攻撃とは、流出したＩＤ・パスワードの組合せをリスト化し、そのリストを使って不正ログインを試みる攻撃手法である。

	事案の概要	指導事項
	案。事業者のサーバで利用されていた開発ツールに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。	制の整備） 技術安全管理措置 （外部からの不正アクセス等の防止）
7	事業者は顧客の個人データを管理していたシステムの開発等を委託（個人データの取扱いを含む）していたところ、当該システムが不正アクセスを受け、データが外部に送信され、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。不正アクセスを受けたサーバが誤設定により外部ネットワークから直接アクセス可能となっていたこと、当該サーバに設置されていたソフトウェアの脆弱性が対応されずに放置されていたこと等が原因と考えられる。 ※（iii）６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、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、情報システムの使用に伴う漏えい等の防止）
8	事業者（上記事案（番号７）の委託先）は委託元の顧客の個人データを管理していたシステムの開発等の委託（個人データの取扱いを含む）を受けていたところ、当該システムが不正アクセスを受け、データが外部に送信され、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。不正アクセスを受けたサーバが誤設定により外部ネットワークから直接アクセス可能となっていたこと、当該サーバに設置されていたソフトウェアの脆弱性が対応されずに放置されてい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 （アクセス制御）
9	事業者が開発、保守及び運営を行うウェブサイトが、ＳＱＬインジェクション攻撃による不正アクセスを受け、当該ウェブ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。当該ウェブサイトには開発当時から、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 （情報システムの使用に伴う漏えい等の防止）
10	事業者のウェブサーバが不正アクセスを受け、事業者のウェブ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。当該ウェブサイトの画像アップロード機能の一部に古いプログラムが残っており、画像ファイルに偽装した不正プログラムをアップロード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）

	事案の概要	指導事項
11	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、当該ウェブサイトが不正アクセスを受け、当該ウェブ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。事業者は当該ウェブサイトの開発を子会社等に委託及び再委託（個人データの取扱いの委託を含む）していたところ、当該ウェブサイトの構築のために利用されていたツールに存在した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 （情報システムの使用に伴う漏えい等の防止）
12	事業者が運営するＥＣサイトがパスワードリスト攻撃による不正アクセスを受け、当該ＥＣサイトの会員に関する個人データについて漏えいが生じた事案。事業者が設定するパスワードポリシーが十分な強度のパスワードを求めるものではなく、会員が脆弱なパスワードを設定可能であったこと、ログイン試行回数制限の措置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 （アクセス者の識別と認証）

（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（学校）の従業者（教職員）が利用するシステムが、本来アクセス権限のない生徒によって不正にアクセスされ、生徒及び教職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。当該システムにアクセス可能な端末を制限しておらず、生徒も利用可能な共用端末からもアクセスが可能となっていたこと、教職員のパスワードポリシーが定められておらず強度に問題があるパスワードが設定可能となっていたこと、生徒が閲覧可能な状況で教職員がＩＤ・パスワードを入力していたこと等が原因と考えられる。 ※（ⅲ）１番の事案と同じ	人的安全管理措置 （従業者の教育） 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）
2	事業者は、委託元（保険会社）から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ＮＡＳ（Network Attached Storage）が不正アクセスを受け、当該ＮＡＳ内のデータが削除されたことで、委託元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ＮＡＳが外部からアクセス可能であり、外部からのアクセスに必要な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）
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。事業者	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
	が利用していた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） ２番の事案と同じ	部からの不正アクセス等の防止）
４	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、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。当該サーバについてファイアウォール等の不正アクセス防止のためのセキュリティ対策を適切に講じていなかったこと、不正アクセスに利用された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）（c） 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）
５	事業者は、法人向けにサービスを提供し、当該サービスの利用法人から顧客の個人データについて取扱いの委託を受けているところ、当該サービスのメール配信機能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。事業者の従業者がフィッシングメールによって当該メール配信機能の認証情報を流出させ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）
６	事業者のサーバ等がＶＰＮ経由で不正アクセスを受け、事業者の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。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）
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、株主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。不要なアカウントが残置されていたこと、当該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 （アクセス制御、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、事業者及び委託元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。事業者が利用していた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） 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）
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、従業者の特定個人情報を含む個人データ並びに事業者及び委託元の顧客等に関する個	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
	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ため、脆弱性を突かれたこと、不正アクセスに利用された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) ６番の事案、Ⅱ２（１）４番の事案と同じ	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、個人データを含むファイルが外部に送信され、漏えいが生じた事案。事業者が利用していた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) 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）
11	事業者が利用する社内システムが、管理者アカウントを利用した不正アクセスを受け、当該システムに保管されていた取引先等に関する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アカウントの認証情報が適切に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 （アクセス者の識別と認証）
12	事業者が顧客管理のために利用しているシステム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が生じた事案。不正アクセスに利用された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）
13	事業者が顧客管理のために利用しているシステムに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。不正アクセスに利用された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）
14	事業者は、委託元（行政機関等）から指定を受け公共施設を管理等しており、当該管理業務等の限りで保有個人情報の取扱いの委託を受けていたところ、事業者のサーバが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、公共施設等の利用者に関する保有個人情報及び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。不正アクセスに利用されたＰＣ端末のＲＤＰ（Remote Desktop Protocol）ポートが制限なく公開されていたこと、不正アクセスに利用された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) 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）
15	事業者は、会員システムの開発等の業務を委託（個人データの取扱いの委託を含む）していたところ、当該委託先のＶＰＮサーバが不正アクセスを受け、事業者の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。委託先がＶＰＮサーバのＲＤＰポートを公開状態としていたこと、	委託先の監督の不十分

	事案の概要	指導事項
	不正アクセスに利用された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) ９番の事案と同じ	
16	事業者（上記事案（番号 15）の委託先）は、会員システムの開発等の業務の委託（個人データの取扱いの委託を含む）を受けていたところ、当該委託先のＶＰＮサーバが不正アクセスを受け、事業者の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。委託先がＶＰＮサーバのＲＤＰポートを公開状態としていたこと、不正アクセスに利用された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) 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）
17	事業者は、委託元（行政機関等）から、業務に利用するシステムの運用、保守等の委託（保有個人情報の取扱いの委託を含む）を受けていたところ、事業者が利用するクラウドサービス上の開発環境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、委託元の保有個人情報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アカウントの認証情報の強度に問題があったこと、当該開発環境でテストに利用された委託元の保有個人情報については本来削除するはずであったにもかかわらず、削除を失念したため残存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） 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（学校）の従業者（教職員）が利用するシステムが、本来アクセス権限のない生徒によって不正にアクセスされ、生徒及び教職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。当該システムにアクセス可能な端末を制限しておらず、生徒も利用可能な共用端末からもアクセスが可能となっていたこと、教職員のパスワードポリシーが定められておらず強度に問題があるパスワードが設定可能となっていたこと、生徒が閲覧可能な状況で教職員がＩＤ・パスワードを入力していたこと等が原因と考えられる。 ※(ii) １番の事案と同じ	人的安全管理措置 （従業者の教育） 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）
2	事業者は、委託元（保険会社）から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、	技術的安全管理措置

	事案の概要	指導事項
	事業者のＮＡＳが不正アクセスを受け、当該ＮＡＳ内のデータが削除されたことで、委託元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ＮＡＳが外部からアクセス可能であり、外部からのアクセスに必要な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	（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）
３	事業者の従業者が、ボイスフィッシングにより攻撃者の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ように誘導されたことで、顧客等に関する個人データについて漏えいが生じた事案。事業者の従業者が各自の判断で、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可能であり、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。	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	事業者の従業者が、ボイスフィッシングにより顧客管理システムの認証情報等を窃取され、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されたことで、当該顧客管理システムにおいて管理されていた顧客等の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。	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	事業者のグループ会社である外国事業者のネットワークに設置されていたＶＰＮ経由で、事業者のサーバが不正アクセスを受け、事業者のサーバ内のデータが窃取され、事業者の従業者や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事案。当該ＶＰＮ機器には多数の脆弱性が存在していたにもかかわらず、事業者が当該外国事業者のネットワークから事業者のサーバへの広範なアクセスを許容していたことが原因と考えられる。 ※（ｉ）(a) ７番の事案と同じ	技術的安全管理措置 （アクセス制御）
６	事業者は顧客の個人データを管理していたシステムの開発等を委託（個人データの取扱いを含む）していたところ、当該システムが不正アクセスを受け、データが外部に送信され、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。不正アクセスを受けたサーバが誤設定により外部ネットワークから直接アクセス可能となっていたこと、当該サーバに設置されていたソフトウェアの脆弱性が対応されずに放置され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 （個人データの取扱状況を確認する手段の整備、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、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
7	事業者（上記事案（番号６）の委託先）は委託元の顧客の個人データを管理していたシステムの開発等の委託（個人データの取扱いを含む）を受けていたところ、当該システムが不正アクセスを受け、データが外部に送信され、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。不正アクセスを受けたサーバが誤設定により外部ネットワークから直接アクセス可能となっていたこと、当該サーバに設置されていたソフトウェアの脆弱性が対応されずに放置されていたこと等が原因と考えられる。 ※（ｉ）（c）８番の事案と同じ	技術的安全管理措置 （アクセス制御）
8	事業者は、委託元（行政機関等）から指定を受け公共施設を管理等しており、当該管理業務等の限りで保有個人情報の取扱いの委託を受けていたところ、事業者のサーバが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、公共施設等の利用者に関する保有個人情報及び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。不正アクセスに利用されたＰＣ端末のＲＤＰポートが制限なく公開されていたこと、不正アクセスに利用された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）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、外部からの不正アクセス等の防止）
9	事業者は、会員システムの開発等の業務を委託（個人データの取扱いの委託を含む）していたところ、当該委託先のＶＰＮサーバが不正アクセスを受け、事業者の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。委託先がＶＰＮサーバのＲＤＰポートを公開状態としていたこと、不正アクセスに利用された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）15 番の事案と同じ	委託先の監督の不十分
10	事業者（上記事案（番号９）の委託先）は、会員システムの開発等の業務の委託（個人データの取扱いの委託を含む）を受けていたところ、当該委託先のＶＰＮサーバが不正アクセスを受け、事業者の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。委託先がＶＰＮサーバのＲＤＰポートを公開状態としていたこと、不正アクセスに利用された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）16 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。事業者によるファ	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
	イアウォール切替作業時の設定ミスにより、当該サーバが外部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。	の防止）
12	事業者はウェブサイトを運営していたところ、当該ウェブサイトの会員ページが不正アクセスを受け、会員等の個人データ及び事業者が一部の同サービス利用法人から取扱いの委託を受けた個人データについて漏えいのおそれが生じた事案。当該サービスにはログイン後、マイページのパラメータを操作することで他会員の情報を閲覧できるという設計上の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 （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	事業者による委員会に対する漏えい等報告の提出だけでなく、委託元への通知が著しく遅滞した事案。個人情報保護法の理解不足や漏えい等事案に対応す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）
2	事業者が、本人の同意を得ることなく、従業者の個人データが記載された名簿を第三者に提供した事案。また、事業者は、従業者から個人情報を取得するに当たり、利用目的として、当該名簿の作成について明確に示していなかった。そのため、個人情報保護法第 21 条第２項及び同法第 27 条第１項の規定違反が認められた。	取得に際しての利用目的の通知等（個人情報保護法第 21 条第２項の規定違反） 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	事業者が、委託元から取扱いの委託を受けた個人データをメールの誤送信により漏えいさせたが、委員会への漏えい等報告及び委託元への通知を長期間行っていなかった事案。個人情報保護法の理解不足によって事業者の個人情報保護管理責任者が誤った判断をしたこと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	事業者の元従業者が、退職日に顧客の個人データが記録された紙媒体を持ち出すとともに、退職後に、顧客の個人データを、ストレージサービスを利用してダウンロードしたことにより、顧客の個人データについて漏えいが生じた事案。退職時にデータの返還等の確認が行われていなかったこと、事業者が利用するストレージサービスのアクセス制限が行わ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） 技術的安全管理措置 （アクセス制御）
5	事業者は委託元から健康診断等の業務の委託（個人データの取扱いの委託を含む）を受けているところ、従業者が外出中に業務用ＰＣを一時紛失及び破損した。これにより、当該ＰＣ内に保存されていた、健康診断受診者等の特定個人情報を含む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。事業者においては、業務用ＰＣのローカルディスクにデータを保存しない運用としていたが、当該運用が徹底されていなかったこと、業務用ＰＣにおける個人データの保管状況等について把握でき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、取扱状況の把握及び安全管理措置の見直し）
6	事業者が、令和４年４月から令和７年７月までの間、多数の漏えい等報告を行っていなかった事案。事業者においては、個人情報保護法の理解不足等により、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ような体制が整備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 （漏えい等事案に対応する体制の整備）
7	事業者が提供するサービスにシステム上の不備があり、機能が有効に働かず、第三者から個人デー	技術的安全管理措置

	事案の概要	指導事項
	タが閲覧可能となっていたことで、利用者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。事業者において、システムやデータの連携を示す設計書の整備が不十分であったこと等が原因と考えられる。	（情報システムの使用に伴う漏えい等の防止）
８	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、業務用ＰＣの取扱いに係る規程が存在せず、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）
９	事業者が、令和４年４月から令和７年 10 月までの間、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）
10	事業者（教育機関）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、ＮＡＳに接続されたことで、当該ＮＡＳに保管されていた生徒や教職員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。事業者において、規程で禁止されていたにもかかわらず、ＮＡＳに個人データを保存し、当該ＮＡＳにおいて漏えい等を防止するための措置を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）
11	複数の歯科医院を運営する事業者が、本人の同意を得ることなく、患者の口くう内写真を事業者のウェブサイト上で公開することにより、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）

▽　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の整備	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	3	1	5	3	3

指導等の内容	安全管理措置				委託先の監督	取得に際しての利用目的の通知等	第三者提供の制限
	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	5	17	23	9	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	金融業、保険業	学術研究、専門・技術サービス業
指導等件数	7	1	9	1	9	5	1

業種	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	3	2	3	2	1	8

※　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	３	25	９	11

※　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 32 件　※

・ウェブサイトで公開していたファイルのマスキング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。
・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、誤送付等の防止の不備（７件）、媒体の管理等の不備（５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、18 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	高等学校の職員がサポート詐欺に遭い、業務用ＰＣに遠隔操作ツールをインストールされたことで、当該業務用ＰＣに保管されていた生徒、保護者等に関する保有個人情報（氏名、住所等）について漏えいのおそれが生じた事案。規程に従った教育研修が行われていなかったこと等が原因と考えられる。	教育研修
２	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たことにより、被害者・被疑者の氏名等の保有個人情報について漏えいのおそれが生じた事案（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、常時施錠まではされておらず、出し入れについて確認していなかったこと等が原因と考えられる。	媒体の管理等
３	地方公共団体の保有個人情報（職員の氏名や人事管理に関する個人情報等）が、経緯は不明であるが何者かによって持ち出され、報道機関等に流出していたこと等が発覚した事案。外部記録媒体等に情報が残存していたこと、保有個人情報にアクセスするための認証情報の管理が適切でなかったこと、保有個人情報へのアクセス履歴を記録していなかったこと等が原因と考えられる。	廃棄等 アクセス制御 アクセス記録
４	教育委員会が所管する図書館において、行政文書開示請求に対し、不開示情報をマスキング等して行政文書の一部公開を行ったところ、当該マスキング等が不十分であったことにより、図書館利用者に関する保有個人情報が漏えいした事案。マスキング等の手順が具体的に定めら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
５	地方公共団体が保管していた妊娠届の所在が不明となり、特定個人情報を含む保有個人情報（妊婦	媒体の管理等

	事案の概要	指導事項
	の氏名、生年月日等)について漏えいのおそれが生じた事案（誤廃棄の可能性が高い)。当該地方公共団体では、妊娠届について、保存期間の満期を迎えたものと保存期間中のものを明確に区別することなく保管していたこと等が原因と考えられる。 ※Ⅱ２（１）３番の事案と同じ	
６	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、保有個人情報を白地処理して公開したところ、当該白地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
７	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
８	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、保有個人情報を白地処理して公開したところ、当該白地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
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、保有個人情報を白地処理して公開したところ、当該白地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	警察署が保管していた道路使用許可申請書を誤廃棄したことにより、申請書に記載された氏名、住所等の保有個人情報が滅失した事案。当該申請書について、保存期間の満期を迎えたものと保存期間中のものを明確に区別することなく保管していたこと等が原因と考えられる。	媒体の管理等
11	地方公共団体が障害者控除対象者認定書を作成する過程において、氏名と住所等の間に行ずれが生	誤送付等の防止

	事案の概要	指導事項
	じたが、それに気付かず、他の対象者の住所や障害者区分が記載された認定書を送付したことにより、保有個人情報の漏えいが生じた事案。当該認定書の作成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。	
12	地方公共団体が管理するウェブサイトである統合基盤地理情報システム等において、道路現況平面図等のデータを、住民や建物所有者の氏名等の記載を削除することなく公開したことで、住民や建物所有者に関する保有個人情報が漏えい等した事案。当該地方公共団体は当該平面図等に個人情報が記載されている事実を明確に認識しておらず、県が、ウェブサイトで公開するに当たり、道路現況平面図等に個人情報が記載されているか否かについて確認し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
13	教育委員会が所管する図書館において、受理した個人貸出登録申込書等の所在が不明となったことにより、図書館の利用者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（誤廃棄の可能性が高い）。当該図書館では、当該申込書等を月末にまとめて保管していたが、所定の場所に保管されることなく事務室内に放置されていたこと等が原因と考えられる。	媒体の管理等
14	高等学校において、職員（臨時講師）が、要配慮個人情報を含む保有個人情報が記載された資料（欠席連絡表）を窃取したことにより、生徒に関する保有個人情報が漏えいした事案。当該資料に大量の保有個人情報が記載されているにもかかわらず、施錠設備のない場所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

▽　指導等の内容別の件数

指導等の内容	教育研修	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	廃棄等	アクセス制御	アクセス記録
指導等件数	1	5	7	1	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	0	14

※　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	10	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（第 156 条）　計９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、特定個人情報を含む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) 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、特定個人情報を含む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) 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）
３	地方公共団体が保管していた妊娠届の所在が不明となり、特定個人情報を含む保有個人情報(妊婦の氏名、生年月日等)について漏えいのおそれが生じた事案（誤廃棄の可能性が高い）。当該地方公共団体では、妊娠届について、保存期間の満期を迎えたものと保存期間中のものを明確に区別することなく保管していたこと等が原因と考えられる。 ※Ⅱ１（１）② ５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）
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、従業者の特定個人情報を含む個人データ並びに事業者及び委託元の顧客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（ｉ）(a) ６番の事案、Ⅱ１（１）①ア（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）
５	事業者のサーバがＲＤＰ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について漏えいのおそれ及び毀損が生じた事	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
	案。ＲＤＰポートが意図せず公開状態となっていたこと等が原因と考えられる。	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、従業者の特定個人情報を含む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。不正アクセスに利用されたアカウントが管理されておらず、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）
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、従業者の特定個人情報を含む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ため、脆弱性を突かれたこと、不正アクセスに利用された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）

（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。

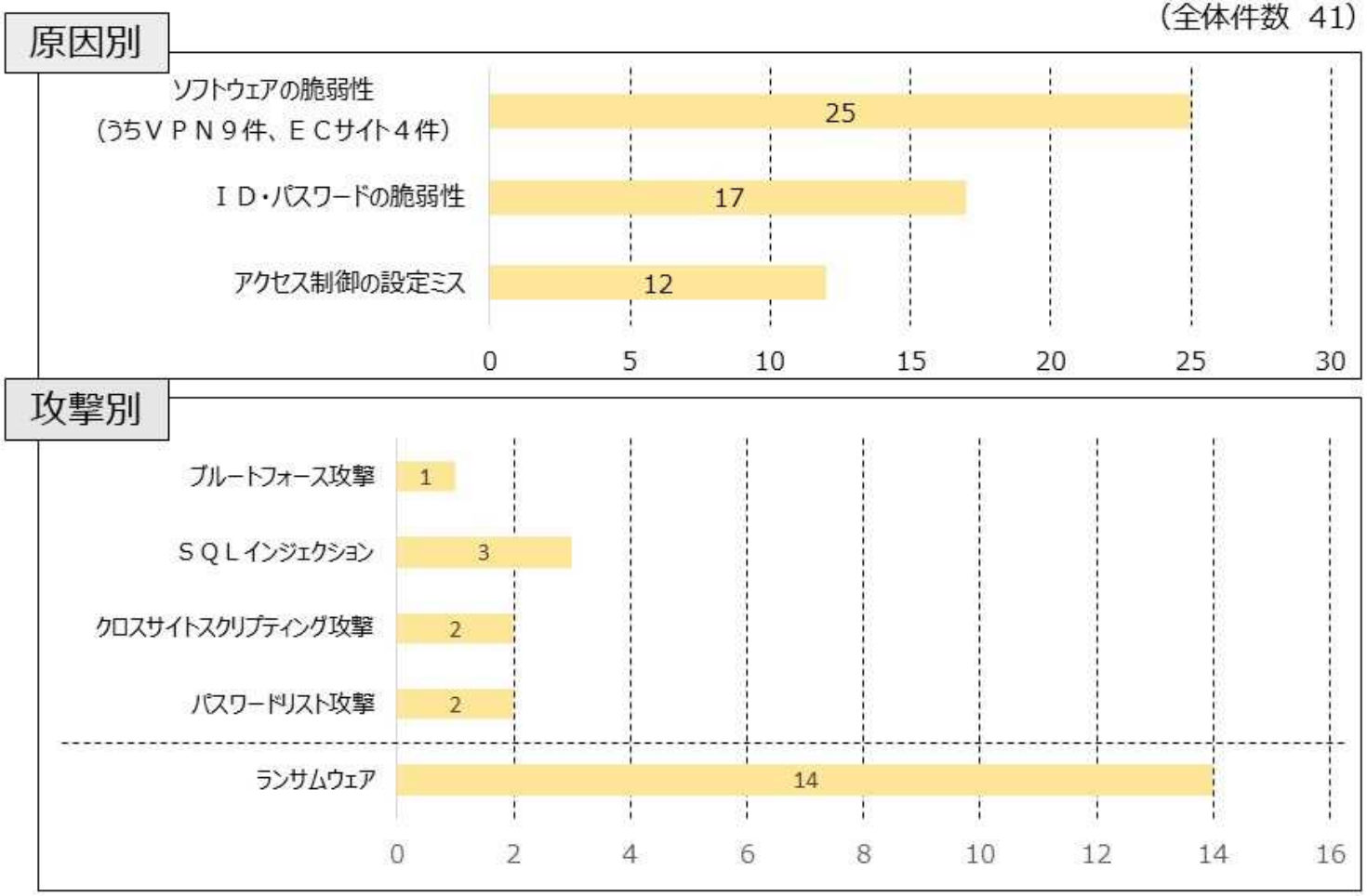
Ⅲ　公表事案に関する指導・助言等の対象先における改善策の実施状況

権限行使日 （参照箇所）	対象	改善策の実施状況
令和７年１月 30 日 (https://www.ppc.go.jp/files/pdf/250129_2_houdou.pdf)	株式会社ビーバーズ	・委員会は、令和７年１月 30 日、株式会社ビーバーズ（以下「ビーバーズ」という。）に対し、ビーバーズが建設会社等に架電し、架空の事業者名を名のった上で虚偽の事実を伝えるなどの方法により１万人以上の個人情報を不適正に取得していた件に関し、個人情報保護法第 148 条第１項の規定による勧告を行い、同法第 146 条第１項の規定により、再発防止策の実施状況等について報告するよう求めた。 ・ビーバーズは、委員会に対し、①前記勧告以降は適正に個人情報を取得していること及び②個人情報保護法第 20 条第１項の規定に違反して取得した個人情報を全て消去したことを、疎明資料を添えて報告するとともに、③再発防止策の策定・実施状況等を報告した。 ・委員会としては、今後も、ビーバーズにおける個人情報の取扱状況について、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７年度第３四半期）

（全体件数　41）



（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（41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。