資料３－２

令和6年8月〇日
個人情報保護委員会

令和6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6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

権限行使日	対象	権限行使の内容	法令	参照箇所
令和6年6月 27 日	東京電力パワーグリッド株式会社 東京電力ホールディングス株式会社 東京電力リニューアブルパワー株式会社	指導及び報告徴収	個人情報保護法	一般送配電事業者及び関係小売電気事業者等における顧客情報の不適切な取扱事案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-個人情報保護委員会-（https://www.ppc.go.jp/files/pdf/240627_01_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 142 件[1]

ア　民間事業者　計 110 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や、ファイアウォールが解除されていたことなど、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。このほか、サポート詐欺によるものもみられている。
- 指導等の内容として、特に技術的安全管理措置に関して、外部からの不正アクセス等の防止の不備が最も多く（44 件）、アクセス制御の不備（5件）もみられた。このほか、委託先に対する監督の不備（8件）、組織的安全管理措置の不備（7件）、人的安全管理措置の不備（2件）、物理的安全管理措置の不備（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、47 件の指導を行った。

	事案の概要	指導事項
1	事業者のサーバがランサムウェア[2]（Lockbit2.0 と類似した特徴を持つマルウェア）の攻撃を受け、個人データが暗号化され、漏えいのおそれが生じた事案。VPN ソフトの脆弱性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	事業者の顧客の個人データを管理するシステムが不正アクセスを受け、当該個人データが漏えいした事案。サーバの OS 及びソフトウェアに最新のセキュリティパッチが適用されておらず、また、管理者の ID・パスワードの	技術的安全管理措置（アクセス制御、外部からの不正アクセス等の

[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」の段階で数値等が改訂される可能性がある。
[2] 感染するとパソコン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。

	事案の概要	指導事項
	強度に問題があったことが原因と考えられる。	防止）
3	事業者の公開ウェブサイトで使用するコンテンツ管理システムの管理者IDとパスワードが窃取され、レンタルサーバに設置されたウェブサイトが不正プログラムによって改ざん、当該サーバに設置された5つのウェブサイトで管理される個人データに漏えいのおそれが生じた事案。コンテンツ管理システムの脆弱性を突かれ、管理者権限を窃取さ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	事業者のウェブサイトと同一のサーバ内で管理されていたテスト環境を通じて不正アクセスがなされ、個人データの漏えいのおそれが生じた事案。テスト環境のドメインを公開状態にしていたものの、アクセス制限を設けておらず、ID・パスワードの強度にも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）
5	事業者の職員が、廃棄のために、PC3台を一時的に屋外に置いていたところ、その後所在不明となり、当該 PC 内の個人データに漏えいのおそれが生じた事案。	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）
6	事業者が運営するウェブサイトの個人データを管理していたサーバに対して、不正アクセスがあり、個人データの漏えいのおそれが生じた事案。本件サーバで使用しているソフトウェアに脆弱性があり、その脆弱性を補完する機能を有する WAF（Web Application Firewall）を導入していたところ、特定の時期以降、同 WAF の設定が解除されており、それに気づかず脆弱性がある状態で本件ウェブサイトを運営してい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	事業者が従業員の個人データの取扱いをグループ会社である外国法人に委託していたところ、従業員データベースを管理するシステムが不正アクセスを受け、従業員の個人データが漏えいした事案。グループ会社の他国法人の従業員アカウントがパスワードスプレー攻撃 [3]を受け、第三者に認証情報を窃取されたことが原因と考えられる。	委託先に対する監督
8	事業者のウェブサイトに対して不正アクセスがあり、同サイトで使用していたプログラムに保存されていた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ウェブサーバに設置して使用していたところ、その脆弱性が放置されており、脆弱性が悪用さ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）
9	事業者が運営する EC サイトに不正アクセスがあり、顧客の個人データに漏えいのおそれが生じた事案。同 EC サイトには、クロスサイトスクリプティング攻撃 [4]に対する脆弱性が存在していたにもかかわらず、アップデート等の適切な対応を放置してい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）
10	事業者が運営する EC サイトに不正アクセスがあり、顧客の個人データに漏えいのおそれが生じた事案。同 EC	技術的安全管理措置（外部からの

[3] 多数のアカウントに対して、よく使われるパスワードでログインを試みることで、アカウントロックを回避しながら攻撃する手法。
[4] Web 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。

	事案の概要	指導事項
	サイトには、クロスサイトスクリプティング攻撃に対する脆弱性が存在していたにもかかわらず、アップデート等の適切な対応を放置していたことが原因と考えられる。	不正アクセス等の防止）
11	事業者が運営する EC サイトに不正アクセスがあり、顧客の個人データに漏えいのおそれが生じた事案。同 EC サイトはアプリケーションを使用していたところ、同アプリケーションの脆弱性情報及び同脆弱性に対応した新しいバージョンの公開がなされているにもかかわらず、同脆弱性がある旧バージョンのアプリケーションをそのまま用いて EC サイトを運営してい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）
12	事業者が使用している業務系サーバにランサムウェア攻撃があり、従業者の特定個人情報及び個人データ並びに顧客の個人データに漏えいのおそれ及び毀損が生じた事案。VPN 機器の脆弱性情報が公開されていたが、脆弱性情報の入手後の対応が遅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	事業者が運営・管理しているサーバに接続されたネットワーク機器の脆弱性を突かれて不正アクセスを受け、従業者及び採用応募者の個人データ並びに従業者の特定個人情報に漏えいのおそれが生じた事案。ネットワーク機器の脆弱性について、ウェブサイト上で公表されていたにもかかわらず、一定期間、脆弱性への対応としてパッチ適用などを行っておらず、最新ではない状態で使用を継続していたため、その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）
14	事業者が管理するサーバが不正アクセスを受け、同サーバに保存されていた従業者及び顧客の個人データに漏えいのおそれが生じた事案。本件サーバの管理者権限のアカウントは複数あったところ、その一部のパスワードが4桁の文字及び数字で構成されていたことから、パスワード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）
15	事業者のサーバが不正アクセスを受け、従業者及び取引先の個人データがランサムウェアにより暗号化され、毀損した事案。事業者が利用していた VPN 機器については、認証されていない遠隔の攻撃者によるブルートフォース攻撃 [5]を可能にする脆弱性が警告され対処が推奨されていたにもかかわらず、同脆弱性を放置していたため、VPN 経由で社内ネットワークに侵入され、社員の有効なアカウント情報が窃取さ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）
16	事業者が運営する EC サイトに不正アクセスがあり、顧客の個人データに漏えいのおそれが生じた事案。同 EC サイトには、クロスサイトスクリプティング攻撃に対する脆弱性が存在していたにもかかわらず、アップデート等の適切な対応をせずに放置していたこと、また、外部からの不正侵入を防止するシステム等のセキュリティ対策の	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] 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。

	事案の概要	指導事項
	不備があったことが原因と考えられる。	
17	事業者が利用するクラウドサービスにおいて、事業者環境に対し、攻撃者 PC の不正登録が発生。攻撃者は不正登録されたアカウントを利用してメールの同期を行い、メールボックスが閲覧可能な状態となったことから、アドレス帳に登録されていた個人データに漏えいのおそれが生じた事案。事業者環境に新規にデバイス登録する際の認証がユーザアカウント認証だけとなっており、必要な設定を看過し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）
18	事業者が提供する写真に関するアプリケーションにおいて、ユーザアカウントに対してリスト型攻撃がなされ、第三者に不正にログインされたことにより、個人データの漏えいのおそれが生じた事案。ユーザのパスワードの使い回し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）
19	地方公共団体から事業を委託されている事業者が業務上利用しているサーバに不正アクセスがあり、サーバに保存されていたデータがランサムウェアによって暗号化され、保有個人情報（個人データ）に漏えいのおそれ及び毀損が生じた事案。適切にログが保管されていなかったため、調査による原因特定ができなかったものの、事業者においては、少なくとも個人データの取扱いに係る規律に従った運用に問題が認められた。	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）
20	一定の要件を満たしている企業に対し認定する制度の審査業務を行っている事業者が、認定のための審査を、ある事業者に委託していたところ、委託先において、不正アクセスがあり、ランサムウェアの感染等により個人データの漏えいのおそれが生じた事案。真因は明らかとなっていないが、委託先において NAS（Network Attached Storage）の設定を誤って公開にしていたことにより外部からアクセスが可能な状態になっていたこと等が原因と考えられる。また、委託元である事業者においては、委託先における個人データ取扱状況の把握が適切に行われておらず、委託先に対する監督に不備が認められた。	委託先に対する監督 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）
21	一定の要件を満たしている企業に対し認定する制度の審査業務を行っている事業者が、認定のための審査を、ある事業者に委託していたところ、委託先において、不正アクセスがあり、ランサムウェアの感染等により個人データが暗号化され、漏えいのおそれが生じた事案。真因は明らかとなっていないが、委託先において NAS を誤って公開に設定していたことにより外部からアクセスが可能な状態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（アクセス制御及び外部からの不正アクセス等の防止）
22	委託元である事業者が、E ラーニングシステムの構築・保守・管理とともに個人データの取扱いを他の事業者に委託していたところ、委託先が管理する本件システムが不正アクセスを受け、個人データの漏えいのおそれが生じた事案。同システムで利用しているオープンソースのプラットフォームについては、コマンドインジェクションに対する脆弱性等複数の脆弱性の存在が公表されており、注意喚起や対応方法のリリースが行われていたにもかかわらず、平成 27 年以降アップデート等の適切な対応を行っていなかったことが原因と考えられる。また、委託元においては、委託先における個人データの取扱状況の把握が不十分であった。	委託先に対する監督

	事案の概要	指導事項
23	委託元である事業者が、E ラーニングシステムの構築・保守・管理とともに個人データの取扱いを他の事業者に委託していたところ、委託先が管理する本件システムが不正アクセスを受け、個人データの漏えいのおそれが生じた事案。同システムで利用しているオープンソースのプラットフォームについては、コマンドインジェクションに対する脆弱性等複数の脆弱性の存在が公表されており、注意喚起や対応方法のリリースが行われていたにもかかわらず、平成 28 年以降アップデート等の適切な対応を行っ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（外部からの不正アクセス等の防止）
24	事業者が運営するウェブサービスにおけるデータベースシステムに不正アクセスがあり、サービス利用者の個人データに漏えいのおそれが生じた事案。事業者による同システムの設定ミスにより、特定の操作を行うことで外部からデータベースにアクセスが可能な状態となっていたことが原因と考えられる。	技術的安全管理措置（アクセス制御）
25	一定の要件を満たしている企業に対し認定する制度の審査業務を行っている事業者が、認定のための審査を、ある事業者に委託していたところ、委託先において、不正アクセスがあり、ランサムウェアの感染等により個人データが暗号化され、漏えいのおそれが生じた事案。真因は明らかとなっていないが、委託先において NAS を誤って公開に設定していたことにより外部からアクセスが可能な状態になっていたこと等が原因と考えられる。また、委託元である事業者においては、委託先における個人データ取扱状況の把握が適切に行われておらず、委託先に対する監督に不備が認められた。	委託先に対する監督 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）
26	委託元である事業者が、自社の特定の事業の運営とともに同事業の参加者の個人データの取扱いを他の事業者に委託していたところ、委託先が管理するアカウントが不正アクセスを受け、アプリケーションに保存されていた個人データに漏えいのおそれが生じた事案。アカウントのパスワードが、同事業の名称を使用した簡単な文字列で構成されており、容易に推測されやすいものとなっていたこと等が原因と考えられる。 また、委託元である事業者においては、適切な委託先の選定、委託契約の締結及び委託先における個人データの取扱状況の把握が不十分であり、委託先に対する監督に不備が認められた。	委託先に対する監督
27	委託元である事業者が、自社の特定の事業の運営とともに同事業の参加者の個人データの取扱いを、他の事業者に委託していたところ、委託先が管理するアカウントが不正アクセスを受け、アプリケーションに保存されていた個人データに漏えいのおそれが生じた事案。アカウントのパスワードが、同事業の名称を使用した簡単な文字列で構成されており、容易に推測されやすいものとなっていたこと等が原因と考えられる。 また、委託元である事業者においては、適切な委託先の選定、委託契約の締結及び委託先における個人データの取扱状況の把握が不十分であり、委託先に対する監督に不備が認められた。	委託先に対する監督
28	委託元である事業者が、自社の特定の事業の運営とともに同事業の参加者の個人データの取扱いを、他の事業者に委託していたところ、委託先が管理するアカウントが第三者によって不正アクセスを受け、アプリケーショ	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
	ンなどに保存されていた個人データに漏えいのおそれが生じた事案。アカウントのパスワードが、同事業の名称を使用した簡単な文字列で構成されており、容易に推測されやすいものとなっていたこと等が原因と考えられる。	
29	事業者のサーバに対して不正アクセスがあり、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、管理者権限の窃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）
30	事業者が運営しているウェブサイトが不正アクセスを受けた結果、不審ファイルの設置等が行われるとともに、サーバ上のデータベースに保存されていた顧客の個人データに漏えいのおそれが生じた事案。事業者は、自らが管理するウェブサイトのウェブサーバにエスケープ処理を実装しておらず、SQL インジェクション [6]への対応が不十分であったこと又は管理者アカウントのユーザ名及びパスワードを脆弱なものに設定していたことから、攻撃者に認証情報が特定さ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）
31	委託元である事業者が、個人データの取扱いを含むシステム開発・運用業務を、他の事業者に委託していたところ、委託先が利用する仮想専用サーバ（Virtual Private Server 以下「VPS」という。）が不正アクセスを受け、顧客に関する個人データに漏えいのおそれが生じた事案。委託先がファイアウォールをデフォルトの設定（任意の IP アドレスから接続可能である状態）で利用していたこと、また本件 VPS のログイン ID とパスワードもデフォルトのまま利用していたことで、外部からブルートフォース攻撃にて認証を突破されたことが原因と考えられる。 また、委託元である事業者においては、委託契約の締結及び委託先における個人データの取扱状況の把握が不十分であり、委託先に対する監督に不備が認められた。	委託先に対する監督
32	委託元である事業者が、個人データの取扱いを含むシステム開発・運用業務を、委託先である事業者に委託していたところ、委託先である事業者が利用する仮想専用サーバ（VPS）が不正アクセスを受け、顧客に関する個人データに漏えいのおそれが生じた事案。委託先がファイアウォールをデフォルトの設定（任意の IP アドレスから接続可能である状態）で利用していたこと、また本件 VPS のログイン ID とパスワードもデフォルトのまま利用していたことで、外部からブルートフォース攻撃にて認証を突破さ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）
33	事業者のサーバに対して不正アクセスがあり、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、管理者権限の窃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、脆弱性が悪用さ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）

[6] Web アプリケーションの脆弱性を意図的に利用し、断片的な SQL 文をアプリケーションに不正に注入し実行させる攻撃手法。

	事案の概要	指導事項
34	事業者が運営する医療施設において、職員が、患者等の個人データが入った HDD を紛失した事案。事業者の規程に違反し、私物である外部電磁的記録媒体の利用や持ち帰り等が行われていたことが原因であると考えられる。	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） 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、電子媒体等を持ち運ぶ場合の漏えい等の防止）
35	事業者が運営する EC サイトに不正アクセスがあり、顧客の個人データが漏えいした事案。同 EC サイトについてクロスサイトスクリプティング攻撃に対する脆弱性が存在していたにもかかわらず、アップデート等の適切な対応をせず放置してい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）
36	事業者の基幹システムを含む情報システムへのランサムウェア攻撃により、顧客及び従業者の個人データに漏えいのおそれが生じた事案。事業者が使用していた VPN 機器には脆弱性があったが、当時、VPN 装置の保守契約が切れていたため、事業者自身でバージョンアップやアカウント管理をする必要があったものの、前任者からの引継ぎ等が不十分であったことにより、対応ができていなかった。その結果、VPN 装置内にセキュリティ設定の弱いテストアカウントが存在し続け、さらに、ロックアウト設定も適切に講じら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（外部からの不正アクセス等の防止）
37	クリニックの診療記録について、通院していた患者が個人情報保護法第 33 条第1項に基づき開示請求を行ったところ、クリニック側が開示も行わず、対象の個人データが存在しないことの通知も行わなかったため、同条第2項及び第3項の規定違反について指導を行った。	開示請求への対応
38	事業者の社内システムがランサムウェア攻撃を受け、サーバ内の顧客の個人データが暗号化され、漏えいのおそれが生じた事案。事業者が使用していた VPN 機器へのログオン認証用パスワードやサーバ管理者アカウント認証用パスワードが推測しやすいものであり、また、設定後のパスワード変更も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）
39	事業者が運営する顧客・契約管理システムをクラウド環境にて提供している事業者であるところ、顧客のデータ移行や保守において、クラウド上に顧客のデータを一時保管して作業を実施していた際、担当者のミスによりファイルが公開設定され、さらに当該公開状態が長期間継続したことにより、個人データの漏えいのおそれが生じた事案。設定ミスに加え、チェック体制が確立していなかったことが原因（最長5年間にわたり公開状態となっていたファイルがあった）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、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）

	事案の概要	指導事項
40	事業者が使用する PC 及びデータベースにランサムウェア攻撃があり、顧客の個人データに漏えいのおそれが生じた事案。インターネット上にデータベース管理システムのポートが解放されていたため、攻撃者がデータベース管理システムに接続可能な状態となってい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）
41	事業者がネットワーク監視機器の保守や技術支援に係る業務を委託しているA社及び事業者の子会社が UX・UI デザインやウェブ・モバイルサービスに係る業務を委託しているB社が使用している各メールサービスが不正アクセスを受けたことが契機となり、事業者の業務委託先用 VPN のパスワードが窃取され、同 VPN のアカウントに不正アクセスされた後、事業者が業務委託先に付与している事業者の社内システム用アカウントを悪用され、同社内システムが不正アクセスを受けた結果、従業員の個人データが漏えいした事案。業務委託先用 VPN や社内システムにおける多要素認証の導入、IP アドレスの制限等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）
42	事業者が利用している外部クラウドサービスが不正アクセスを受けた結果、従業員の個人データに漏えいのおそれが生じた事案。事業者が利用していた外部クラウドサービスは、初期仕様が公開設定となっていたため、事業者において設定変更を行わなければならないところ、その必要性の認識がなく、設定変更が行われていなかったことや、IP アドレス制限等のアクセス制御が実施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（アクセス制御）
43	事業者が利用するリモートアクセス装置経由で社内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ことで、顧客及び従業者の個人データ並びに従業者の特定個人情報について、漏えいのおそれが生じた事案。事業者がクラウド上で運用しているサーバの設定不備により任意の IP アドレスからアクセス可能であったこと、当該管理サーバを起点にラテラルムーブメント [7]をされた場合に早期検知する手段が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）
44	事業者が管理するサーバがランサムウェア攻撃を受け、同サーバに保存されていた従業者及び顧客の個人データに漏えいのおそれが生じた事案。事業者が使用する VPN 機器については、脆弱性情報が公開されているにもかかわらず、修正パッチの適用など基本的な脆弱性への対応が行わ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（外部からの不正アクセス等の防止）
45	事業者の従業者が、PC 閲覧中にサポート詐欺の被害に遭ったことが原因で、遠隔操作ソフトをインストールされた結果、個人データに漏えいのおそれが生じた事案。事業者においては、従業者に対し、情報セキュリティに関する研修等は行っており、社内 PC にデフォルトのソフト以外のインストールを原則禁止とする社内規程があっ	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] 攻撃者がシステムへの侵入に成功した後、ネットワーク内を横移動し、侵害範囲を拡大していく攻撃手法。

	事案の概要	指導事項
	たものの、許可のないインストール禁止について技術的・システム的な制限はなかったことが原因と考えられる。	
46	委託元である事業者が顧客の個人データの取扱いを他の事業者に委託していたところ、委託先事業者のサーバがランサムウェアの攻撃を受け、個人データが暗号化され、漏えいのおそれが生じた事案。VPN ソフトの脆弱性等が原因と考えられる。委託元である事業者においては、適切な委託先の選定及び委託先における個人データの取扱状況の把握が不十分であり、委託先に対する監督に不備が認められた。	委託先に対する監督
47	地方公共団体から個人データの取扱いの委託を受けていた事業者が管理していたメールアカウントに対し、第三者が不正になりすましてログインがなされ、委託されていた保有個人情報（個人データ）に漏えいのおそれが生じた事案。メールアカウントのパスワードについて、容易に推測できるものが使用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（外部からの不正アクセス等の防止）
48	事業者が管理するサーバが不正アクセスを受け、同サーバに保存されていた顧客の個人データに漏えいのおそれが生じた事案。事業者は、クーポン発行支援サービスを提供していたが、同サービスのシステムにおいて、ログイン画面にアクセスした者のウェブブラウザの表示をコントロールする Java Script ファイルに公開してはならない内部データである API エンドポイント一覧を誤って置いたままにしていたため、それを悪用さ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）
49	事業者が運営する EC サイトに不正アクセスがあり、顧客の個人データに漏えいのおそれが生じた事案。同 EC サイトには、クロスサイトスクリプティング攻撃に対する脆弱性が存在していたにもかかわらず、アップデート等の適切な対応をせずに放置してい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）
50	事業者のグループ会社である外国法人が不正アクセスを受けたことを発端に、日本法人である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、顧客及び従業者の個人データに漏えいのおそれが生じた事案。グループ会社が VPN 認証に脆弱なパスワードを使用していたこと、グループ内のネットワークにおいてオープンな運用がなされ、ファイアウォールを設置し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（外部からの不正アクセス等の防止）
51	事業者が管理・利用するネットワークシステムへのリモートデスクトップサービスのインターネット接続制限に不備があり、サーバに不正アクセスを受け、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。事業者は、クラウド環境上のサーバについて、取引先がアクセスするためのリモートデスクトップサービスを、接続制限を設けずに、外部インターネットに公開しており、また、リモートデスクトップ接続時の多要素認証及び接続試行失敗時のアカウントロックの未導入やアクセス監視など適切な認証管理を用いておらず、不正アクセスを遮断する措置を講じ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（外部からの不正アクセス等の防止）

	事案の概要	指導事項
52	事業者が運営するEC サイトに不正アクセスがあり、顧客の個人データに漏えいのおそれが生じた事案。事業者が Web サーバとして利用していた共有型レンタルサーバの公開領域に、本来削除すべき EC サイトインストールプログラムを誤って置いたままにしていたこと、また、ファイアウォールも設置していないなどのネットワークに関するセキュリティ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（外部からの不正アクセス等の防止）
53	行政機関等から保有個人情報の取扱いの委託を受けた事業者の派遣社員であり、補助金交付に係る書類のチェック業務に従事していた従業者が、当該保有個人情報を不正に持ち出し、漏えいのおそれが生じた事案。当該業務に使用するシステムにおいて、不適切な操作に対する検知システムを導入しておらず、定期的なログの分析や監査が実施されていなかったこと、また、業務上使用していたチャットツールにおけるファイル共有について、アクセス制御に問題があり、担当業務外のファイルを閲覧することが可能な状況であったこと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） 技術的安全管理措置（アクセス制御）
54	事業者のサーバに対して不正アクセスがあり、顧客の個人データに漏えいのおそれが生じた事案。事業者が利用するシステムの脆弱性に対する対策が十分に講じら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（外部からの不正アクセス等の防止）
55	事業者のサーバがランサムウェア攻撃を受け、顧客及び従業者の個人データに漏えいのおそれが生じた事案。VPN 機器の脆弱性対応が適時に行われていなかったこと、管理者アカウントの ID・パスワードが同じ5文字で構成されており容易に推測できるものであ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）
56	事業者のサーバがランサムウェア攻撃を受け、顧客及び従業者の個人データに漏えいのおそれが生じた事案。VPN 機器の脆弱性対応が適時に行われていなかったこと、管理者アカウントの ID・パスワードが同じ6文字で構成されており容易に推測できるものであ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）
57	事業者が運営する EC サイトに不正アクセスがあり、顧客の個人データに漏えいのおそれが生じた事案。同 EC サイトには、クロスサイトスクリプティング攻撃に対する脆弱性が存在していたにもかかわらず、アップデート等の適切な対応をせずに放置していたこと、また、同サイト管理画面の外部からのアクセス制御も行っ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（外部からの不正アクセス等の防止）
58	事業者の従業者である医師が、個人所有の PC を使用中にサポート詐欺の被害に遭い、同 PC に保存されていた要配慮個人情報を含む患者の個人データに漏えいのおそれが生じた事案。事業者においては、患者情報の持ち出しについて、一定のルールを定めていたが、同ルールが徹底されていなかったこと、また、点検や監査による個人データの取扱状況の把握が不十分であったこと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、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）
59	事業者の海外子会社の VPN 機器の脆弱性を突かれて攻撃者に侵入され、管理者アカウントを窃取されて横展開された結果、事業者の従業者等の個人データに漏えいのおそれが生じた事案。同海外子会社の VPN 機器の	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

	事案の概要	指導事項
	脆弱性対応が不十分であったこと、管理者アカウントの ID・パスワードの強度に問題があったことが原因と考えられる。	クセス等の防止）
60	事業者の VPN 機器を経由して社内ネットワークに侵入された後、認証サーバに不正アクセスされた結果、従業者の個人データに漏えいのおそれが生じた事案。事業者は、認証サーバに用いていたサーバ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、アップデート等の適切な対応をせずに放置していたこと、また、認証サーバに導入していたアンチウィルスソフトが最新の状態ではなか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）
61	事業者が利用していたメール管理システムの管理者アカウントが第三者に不正にログインされ、当該システムに構築した個人情報データベース等に保存されていたメールアドレスに、本件アカウントの認証情報が記載されたメールが一斉送信された結果、メール送信先から同システム内の個人データが閲覧可能な状態となり、漏えいが生じた事案。不正利用されたアカウントの認証情報を長期間にわたり変更しておらず、ID・パスワードの強度にも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）
62	行政機関等から業務委託された事業者の従業者が、業務用 PC で作業中にサポート詐欺に遭い、同 PC に保存中の保有個人情報（個人データ）に漏えいのおそれが生じた事案。事業者においては、サポート詐欺等、個人データ等の漏えい原因となる不正アクセスに関する従業者への教育研修が不十分であったことが原因と考えられる。	人的安全管理措置（従業者の教育）
63	事業者が業務上使用するレンタルサーバに第三者が不正アクセスし、同サーバに保存されていた顧客の個人データに漏えいのおそれが生じた事案。事業者がシステム構築する際に使用したサーバへの FTP 接続情報を、外部から閲覧可能な状態でウェブサーバに意図せず残置していたため、攻撃者は同 FTP 接続情報を読み取り、サーバに不正ログインしたことが原因と考えられる。	人的安全管理措置（従業者の教育）

▽ 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				技術的		
		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	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
指導等件数	1	4	1	2	3	5	3	44

指導等の内容	安全管理措置			委託先に対する監督	開示請求への対応
	人的	物理的			
	従業者の教育	機器及び電子媒体の盗難の防止等	電子媒体等を持ち運ぶ場合の漏えい等の防止		
指導等件数	2	2	1	8	1

※ 1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	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	3	9	9	1	14	1	2	1	4	9	10

※ 業種分類は、漏えい等報告の記載による。漏えい等報告の提出の遅延のみの事案は除く。

▽ 指導等対象の漏えい等した人数別件数

	1,000 人以下	1,001～10,000 人	10,001 人～50,000 人	50,001 人以上
指導等件数	1	35	14	12

※ 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。

イ　行政機関等　計 32 件　※

・　誤送付・紛失などのヒューマンエラー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。
・　保有個人情報の取扱いに関するルールの内容の不備や不徹底、監査・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。サポート詐欺によるものもみられている。
・　指導等の内容として、媒体の管理等の不備（4件）、保有個人情報の取扱状況の記録の不備（4件）、誤送付等の防止の不備（2件）、委託先に対する監督の不備（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、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	地方公共団体の職員が、自己の知人である第三者に保有個人情報の提供を依頼され、住民基本台帳から必要となる個人情報を抽出して渡したことで、保有個人情報の漏えいが生じた事案。ルールの不徹底及び保有個人情報へのアクセス状況の記録や監視の不備が原因と考えられる。	保有個人情報の取扱状況の記録、アクセス記録及びアクセス状況の監視の措置の不備
2	行政機関が要配慮個人情報を含む保有個人情報を、本来保存すべき期間より前に削除し滅失させた事案。職員において、電子媒体の行政文書の取扱いに関する理解不足があったため、保管期限に関する設定の誤りに気づくことができ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の措置の不備
3	地方公共団体のホームページ上にあるファイルを公開する際、誤って保有個人情報が記載されたファイルをアップロードしてしまい、保有個人情報の漏えいが生じた事案。同地方公共団体においては、ホームページに電子データを掲載する際のルール等は定められておらず、掲載時のダブルチェックも行われなかったことが原因と考えられる。	誤送付等の防止の措置の不備
4	地方公共団体が、ホームページに掲載すべきファイルについて、PDF 形式で掲載する予定だったところ、誤って PDF にする前の Excel ファイル（保有個人情報が記録されたシートを含む）を掲載したことにより、保有個人情報の漏えいのおそれが生じた事案。ホームページに資料等を掲載するルールはあったが、誤掲載を防止するためのルールとして不十分であり、PDF ではなく Excel ファイルが掲載されようとしていることを事前にチェックできなかったことが原因と考えられる。	誤送付等の防止の措置の不備
5	地方公共団体から事業を委託されている事業者が業務上利用しているサーバに不正アクセスがあり、サーバに	委託先に対する監督の不備

	事案の概要	指導事項
	保存されていたデータがランサムウェアによって暗号化され、保有個人情報（個人データ）に漏えいのおそれ及び毀損が生じた事案。適切にログが保管されていなかったため、調査による原因特定ができなかったものの、事業者においては、少なくとも個人データの取扱いに係る規律に従った運用に問題が認められた。また、地方公共団体においては、委託先における個人情報の管理の状況についての確認が不十分であったことが認められた。	
6	地方公共団体が、住民の保有個人情報を記録したフラッシュメモリーカードを紛失し、漏えいのおそれが生じた事案。記録媒体のルールの不徹底や取扱状況の記録等に問題があったことが原因と考えられる。	媒体の管理等、保有個人情報の取扱状況の記録の措置の不備
7	公立高校の教職員が、過去に勤務した高校の生徒の個人情報について、管理者の許可を得ずに、私用の PC に保存したまま、当該 PC を使用していたところ、サポート詐欺に遭い、当該 PC を遠隔操作されたことにより、保有個人情報の漏えいのおそれが生じた事案。当該教職員が勤務する高校を所管する教育委員会では、異動時に保有個人情報を返却すること等のルールが定められていたが、監査・点検等が適切に行われていなかったため、ルールに違反する行為について把握できていなかったことが原因と考えられる。	監査及び点検の実施に関する措置の不備
8	公立中学校において、生徒の個人データを校務用のサーバに保存するべきところ、誤って生徒用タブレットから閲覧可能な生徒用サーバに保存し、漏えいが生じた事案。同中学校を所管する教育委員会のルールでは、生徒用サーバに保有個人情報を保存しないことが規定されていたものの、同中学校においてはルールが徹底されておらず、また、同教育委員会は、監査・点検等によりそのルールの不徹底を把握していなかったことが原因と考えられる。	管理体制、教育研修、監査及び点検の実施の措置の不備
9	地方公共団体の庁舎内において、住民の特定個人情報及び個人情報が記載された申請書が所在不明となり、漏えいのおそれが生じた事案。同申請書は、本来、決裁終了後に月ごとのファイルに移して所定の場所に保管すべきところ、ファイルに綴らずに職員のデスク近くで保管していたことが原因と考えられる。	媒体の管理等の措置の不備
10	ある警察職員が、要配慮個人情報を含む保有個人情報が記録された資料を公私共用の鞄に入れたまま、私用の外出先で一時紛失したことにより漏えい及び漏えいのおそれが生じた事案（資料自体は、拾得者が警察署に届出済）。警察内にルールがあったものの、ルールが不徹底であったことが原因と考えられる。	媒体の管理等の措置の不備
11	ある警察署で保管されていた保有個人情報が記載された書類が、保存期間満了前に誤廃棄された事案。廃棄時に内規どおりの確認等が行われなかったことが原因と考えられる。	媒体の管理等の措置の不備
12	行政機関において、保有個人情報が記録されたファイルを紛失し、保有個人情報の滅失又は漏えいのおそれが生じた事案。文書の持ち出し簿が適切に記録されていなかったこと、監査・点検等に問題点があったことが原因と考えられる。	保有個人情報の取扱状況の記録、事案の報告及び再発防止措置、監査及び点検の実施の措置の不備

	事案の概要	指導事項
13	地方公共団体が運営する学校の学生に関する保有個人情報をとりまとめたデータファイルが、保存場所を誤ったことにより、本来アクセスできないはずの在校生等から閲覧可能な状態となっており、漏えいが生じた事案。同校内においては、個人情報の取扱いに関するルールが定められておらず、また、取扱状況を確認するための監査・点検等も内容が不十分であったこと等が原因と考えられる。	個人情報の適切な管理に関する定めの整備、監査及び点検の実施の措置の不備
14	地方公共団体の機関が業務を委託した先の従業者が、業務用 PC で作業中にサポート詐欺に遭い、同 PC に保存中の保有個人情報（個人データ）に漏えいのおそれが生じた事案。委託先である事業者においては、サポート詐欺等、個人データ等の漏えい原因となる不正アクセスに関する従業者への教育研修が不十分であったことが原因と考えられる。また、同地方公共団体は、委託先に対する監督に不備があった。	委託先に対する監督の不備

▽ 指導等の内容別の件数

指導等の内容	個人情報の適切な管理に関する定め	管理体制	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		個人情報の取扱いの委託	安全管理上の問題への対応	
				媒体の管理等	誤送付等の防止	保有個人情報の取扱い等の記録	アクセス記録	アクセス状況の監視		事案の報告及び再発防止措置	監査及び点検の実施
指導等件数	1	1	1	4	2	4	1	1	2	1	4

※ 1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

	国の行政機関等	地方公共団体等
指導等件数	2	12

※ 漏えい等報告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

	1,000 人 以下	1,001～ 10,000 人	10,001 人～ 50,000 人	50,001 人 以上
指導等件数	11	0	2	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（法第 156 条）　計 144 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6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、3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	事業者が使用している業務系サーバへのランサムウェア攻撃事案であり、従業者の特定個人情報及び個人データ並びに顧客の個人データに漏えいのおそれ及び毀損が生じた事案。VPN 機器の脆弱性情報が公開されていたが、脆弱性情報の入手後の対応が遅れたことが原因と考えられる。 ※p.4 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)
2	事業者が利用するリモートアクセス装置経由で社内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ことで、顧客及び従業者の個人データ並びに従業者の特定個人情報について、漏えいのおそれが生じた事案。事業者がクラウド上で運用しているサーバに関し、設定不備により任意の IP アドレスからアクセス可能であったこと、当該管理サーバを起点にラテラルムーブメントをされた場合に早期検知する手段がなかったこと等が原因と考えられる。 ※p.9 43 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	地方公共団体の庁舎内において、住民の特定個人情報及び個人情報が記載された申請書が所在不明となり、漏えいのおそれが生じた事案。同申請書は、本来、決裁終了後に月ごとのファイルに移して所定の場所に保管すべきところ、ファイルにつづらずに職員のデスク近くで保管していたことが原因と考えられる。 ※p.15 9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)

(2)報告徴収、立入検査(第 35 条第1項) 1件 ※

※ 上記の報告徴収、立入検査の件数は、定期的、計画的に行われた立入検査に伴うものを含まない。

以 上