令和７年９月 24 日
個人情報保護委員会

令和７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７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７年４月 30 日	東京海上日動火災保険株式会社 損害保険ジャパン株式会社 三井住友海上火災保険株式会社 あいおいニッセイ同和損害保険株式会社	指導及び報告徴収	個人情報保護法	損害保険会社及び保険代理店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/250430_02_houdou.pdf）
令和７年５月 16 日	有限会社ビジネスプランニング	緊急命令、勧告及び報告徴収	個人情報保護法	有限会社ビジネスプランニング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/250516_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 166 件[1]

①　民間事業者　計 127 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]やECサイトのクロスサイトスクリプティング攻撃[3]などがみられているほか、ランサムウェア攻撃[4]も、30 件みられている。
・不正アクセス以外の漏えい等事案では、個人データが保存されたPCやUSBメモリの入ったかばんの盗難などがみられている。
・このほか、不適正な個人情報の利用（個人情報保護法第 19 条違反）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。
・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（42 件）、次いで、アクセス者の識別と認証の不備（26 件）が多かった。このほか、組織的安全管理措置の不備（９件）、委託先に対する監督の不備（３

---

[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] 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。

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、39 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

	事案の概要	指導事項
1	事業者が、ウェブサイトの開発等の業務及びそれに伴う個人データの取扱いの委託を受けていたところ、委託元である事業者のサーバが不正アクセスを受け、委託元である事業者の個人データについて漏えいが生じた事案。事業者は、当該ウェブサイトにおいて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。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攻撃者による任意のコマンドの実行を可能とする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、地方公共団体から、システムの保守管理業務及びそれに伴う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 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、個人データ（保有個人情報）について漏えいのおそれが生じた事案。侵入口となった VPN アカウントの認証情報が脆弱であったこと等が原因と考えられる。	技術的安全管理措置（アクセス制御、アクセス者の識別と認証）
4	事業者が提供するサービスが不正アクセスを受け、サービスの利用者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、当該サービスに関する認証情報の管理が適切に行われていなかったこと等が原因と考えられる。	技術的安全管理措置（アクセス者の識別と認証）
5	事業者は EC サイトプラットフォームサービスを提供しており、当該サービスによって委託元である事業者の EC サイトが構築等されていたところ、当該 EC サイトが不正アクセスを受け、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 EC サイトが稼働するサーバにおいては、委託元以外の他の事業者の EC サイトも稼働していたところ、事業者による同サーバ内のアクセス設定に問題があり、攻撃者に横展開を許し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）
6	事業者は、ウェブサイトの開発等の業務及びそれに伴う個人データの取扱いの委託を受けていたところ、当該ウェブサイト経由でサーバが不正アクセスを受け、委託元である事業者の顧客等の個人	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
	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管理者権限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。	
7	事業者のサーバが RDP（Remote Desktop Protocol）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。初期侵入に利用されたアカウントにパスワードが設定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）
8	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、顧客の個人データ及び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。事業者において、VPN 機器やサーバ機器等に対するパッチ適用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 （外部からの不正アクセス等の防止）
9	事業者は EC サイトを運営しているところ、当該 EC サイト経由で事業者のデータベースがブルートフォース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 EC サイトの管理画面に対する IP アドレス等を用いたアクセス制限が設定されていなかったこと、利用された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 （アクセス制御、アクセス者の識別と認証）
10	事業者の PC 及び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毀損及び漏えいのおそれが生じた事案。従業者が不審なメールを開封したことによりランサムウェアに感染し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）
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 機器には、脆弱性が複数確認されていたにもかかわらず、事業者がアップデートやパッチ適用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 （外部からの不正アクセス等の防止）
12	事業者及びグループ会社が利用するサーバ等が、PC へのなりすましログインにより不正アクセスを受け、事業者及びグループ会社の個人データについて漏えいが生じた事案。事業者が、VPN を用いたネットワーク接続において通信制限を行っていなかったこと、VPN 機器の脆弱性に係るパッチ適用を実施していなかったこと、一部のサーバにおいてサポートが切れた古い OS の利用を継続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 （アクセス制御、外部からの不正アクセス等の防止）
13	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アカウ	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
	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。	
14	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に関する個人データについて漏えいが生じた事案。事業者は、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攻撃者による任意のコマンドの実行を可能とする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UTM（Unified Threat Management[5]）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、事業者及び委託元である事業者（事業者のグループ会社）の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が生じた事案。事業者が当該UTM機器の脆弱性への対応を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）
16	事業者が利用する社内システムが、ネットワーク設定の不備により一時的に外部からアクセス可能な状態となり、この間に不正アクセスされたことで、従業者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。事業者がファイアウォールの設定を誤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、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、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。事業者が、当該VPN機器について、複数の脆弱性情報が公開されていたにもかかわらず、アップデート等の対応をしていなかったこと、退職済み従業者のVPNアカウントを把握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 （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）
18	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）
19	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）
20	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、	技術的安全管理措置

[5] 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。

	事案の概要	指導事項
	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。事業者が、当該サーバ上で稼働しているアプリケーションについて、脆弱性対応をしていなかったこと等が原因と考えられる。	（外部からの不正アクセス等の防止）
21	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。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）
22	事業者は、システムの保守等の業務及びそれに伴う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、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のおそれが生じた事案。委託先である事業者においてポートの設定に不備がありアクセス制限がされていなかったこと等が原因と考えられる。	委託元： 委託先の監督
23	事業者（上記事案（番号 22）の委託先）は、システムの保守等の業務及びそれに伴う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、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。事業者においてポートの設定に不備がありアクセス制限がされていなかったこと等が原因と考えられる。	委託先： 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。事業者が当該 VPN 機器について脆弱性の情報が公開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）
25	事業者がクラウドサービス上で管理するサーバが不正アクセスを受け、サーバ上で運用していたシステムの登録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。当該サーバには脆弱性が存在していたところ、事業者が当該脆弱性に対する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）
26	事業者は、ウェブサイトの制作及びそれに伴う個人データの取扱いを委託していたところ、当該ウェブサイトが不正アクセスを受け、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。事業者は委託先である事業者との間で委託業務の具体的な内容を取り決めておらず、この結果、当該ウェブサイトの制作等に利用されているソフトウェア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。	委託先の監督
27	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	技術的安全管理措置

	事案の概要	指導事項
	号化され、従業者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。事業者が当該 VPN 機器について脆弱性の情報が公開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。	（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）
28	事業者のサーバが不正アクセスを受け、メールマガジン配信先に関する個人データに漏えいが生じた事案。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攻撃者による任意のコマンドの実行を可能とする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）
29	事業者のサーバが VPN 経由で不正アクセスを受け、顧客の個人データ及び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が生じた事案。当該 VPN 機器には、脆弱性が複数確認されていたにもかかわらず、事業者が保守業者（個人データの取扱いの委託はない）との間で、アップデート等について取決めをしていなかったことから、当該脆弱性への対応が実施されていなかったこと、当該 VPN 機器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、外部からの不正アクセス等の防止）
30	事業者は設備の施工等の業務及びそれに伴う個人データの取扱いの委託を受けていたところ、当該業務に使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、事業者の従業者及び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 VPN 機器には脆弱性の情報が公開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）
31	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）
32	事業者のサーバが VPN 経由でブルートフォース攻撃による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毀損及び漏えいのおそれが生じた事案。事業者が当該 VPN 機器にログインするためのパスワード及びサーバにアクセスするため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）
33	事業者の外国子会社がフィッシング攻撃による不正アクセスを受けた。その後、横展開により事業者の本社ネットワーク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	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
	され、従業者及び顧客の個人データについて漏えい、滅失及び毀損が生じた事案。当該ネットワーク内の複数の機器で OS の保守期間が終了しており、脆弱性が残置されていたこと等が原因と考えられる。	の防止）
34	事業者はアプリの開発等の業務及びそれに伴う個人データの取扱いの委託を受けていたところ、当該アプリの設定不備を利用され、顧客情報がダウンロードされたことで、委託元である事業者の個人データについて漏えいが生じた事案。事業者が、当該アプリの設定不備を放置し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）
35	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にダウンロードしていたツールにセキュリティ上の脆弱性が存在したこと、社内規程に従った個人データの取扱いがな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 （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）
36	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、従業者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。不要なアカウントが放置され初期侵入に利用されたこと、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、外部からの不正アクセス等の防止）
37	事業者の社内システムが 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、顧客の個人データ及び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が生じた事案。利用された管理者権限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 （外部からの不正アクセス等の防止）
38	事業者がグループ会社から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 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、事業者及びグループ会社の顧客の個人データ並びに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。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）
39	事業者が運営するウェブ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。事業者が、当該ウェブサイトに使用されていたアプリケーションについて脆弱性情報が公開されていたにもかかわらず、対応を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）

	事案の概要	指導事項
40	事業者が運営するウェブサイトが不正アクセスを受け、顧客の個人データが漏えい等した事案。当該ウェブサイトで利用するCMS（Contents Management System）について脆弱性が存在していたところ、当該脆弱性に対する対応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）
41	事業者は、顧客向けのアプリの開発等の業務及びそれに伴う個人データの取扱いを委託していたところ、当該アプリで利用されるAPI（Application Programming Interface）に脆弱性が存在し、当該脆弱性を利用され、サーバが不正アクセスを受けたことで、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。委託先である事業者においては当該脆弱性の対応が実施できていなかったところ、事業者と委託先である事業者との間で当該アプリにおける個人データの安全管理措置についての責任分担が曖昧となっていたこと、安全管理措置の評価や見直しを適切に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）
42	事業者は、顧客向けのアプリの開発等の業務及びそれに伴う個人データの取扱いの委託を受けていたところ、当該アプリで利用されるAPIに脆弱性が存在し、当該脆弱性を利用され、サーバに不正アクセスを受けたことで、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。事業者においては当該脆弱性の対応が実施できていなかったところ、事業者と委託元である事業者との間で当該アプリにおける個人データの安全管理措置についての責任分担が曖昧となっていたこと、安全管理措置の評価や見直しを適切に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 （情報システムの使用に伴う漏えい等の防止）
43	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）
44	事業者のサーバ及びPC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、顧客の個人データ並びに従業者及び取引先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。当該VPN機器について脆弱性情報が公開されていたにもかかわらず対応を行っていなかったこと、利用された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、外部からの不正アクセス等の防止）
45	事業者はメールシステムの開発等の業務及びそれに伴う個人データの取扱いの委託を受けていたところ、当該メールシステムが不正アクセスを受け、委託元である事業者の個人データについて漏	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
	えいのおそれが生じた事案。事業者が設置したファイアウォール機器について脆弱性情報が公開されていたにもかかわらず対応していなかったこと等が原因と考えられる。	の防止）
46	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、委託元である事業者の顧客等の個人データ及び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。事業者が、当該 VPN 機器について脆弱性情報が公開されていたにもかかわらず対応を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）
47	事業者が利用しているコミュニケーションツールの外国子会社の従業者のアカウントがなりすましログインされたことで、当該ツールに保存されていた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。事業者が定めるセキュリティ規程のとおりに従業者の PC が取り扱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、取扱状況の把握及び安全管理措置の見直し）
48	事業者の PC 及びサーバがブルートフォース攻撃による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、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 PC の RDP が外部インターネットから直接アクセスできるよう公開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）
49	事業者及びグループ会社が利用するサーバが 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、事業者及びグループ会社の従業者及び顧客並びにグループ会社の委託元である事業者の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）
50	事業者及びグループ会社が利用するサーバが 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、事業者及びグループ会社の従業者及び顧客並びに委託元である事業者の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）
51	事業者の委託先である事業者の従業者のアカウントが不正利用され、事業者の顧客管理データベースが不正アクセスを受けたことで、従業者及び顧客の個人データについて漏えいが生じた事案。事業者が当該委託先の従業者に対して、必要以上の権限を与えていたこと等が原因と考えられる。	技術的安全管理措置 （アクセス制御）
52	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及び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が生じた事案。侵入口は事業者の外国子会社のシステムであるところ、事業者がグループ会社間のアクセスについ	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
	て、十分なセキュリティ対策を講じていなかったこと等が原因と考えられる。	
53	事業者が運営するECサイトに対し、当該ECサイトの構築システムの脆弱性を突いた不正アクセスがあり、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）
54	事業者のサーバ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。事業者が当該サーバにインストールしていたウェブサイト構築用アプリケーションについて脆弱性情報が公開されていたにもかかわらず、対応を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）
55	事業者は、多数の委託元から顧客情報（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UTM経由でブルートフォース攻撃による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UTM機器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（アクセス者の識別と認証）
56	事業者は取引先から依頼（個人データの取扱いの委託を含む）を受けて設備の販売を行っているところ、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、顧客の個人データ及び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。利用されたアカウントのパスワードの強度に問題があったこと、当該サーバのサポートが切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（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	事業者は地方公共団体からシステム開発等の業務及びそれに伴う個人データ（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、当該個人データ（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（アクセス制御、アクセス者の識別と認証）
58	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、顧客の個人データ及び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のおそれが生じた事案。当該VPN機器について、脆弱性情報が公開されていたにもかかわらず対応していなかったこと、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、外部からの不正アクセス等の防止）
59	事業者は、会員システムの制作等の業務及びそれに伴う個人データの取扱いを委託していたとこ	委託先の監督

	事案の概要	指導事項
	ろ、当該システムが不正アクセスを受け、会員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において、当該システムの脆弱性が放置されていたこと、当該システムの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。	
60	事業者（上記事案（番号 59）の委託先）は、会員システムの制作等の業務及びそれに伴う個人データの取扱いの委託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、会員の個人データについて漏えいのおそれが生じた事案。事業者において、当該システムの脆弱性が放置されていたこと、当該システムの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、外部からの不正アクセス等の防止）
61	事業者のサーバが不正アクセスを受け、顧客の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	事業者のサーバが会員向けウェブサイト経由で不正アクセスを受け、会員の個人データについて漏えいのおそれが生じた事案。当該ウェブサイトの設計ミスにより、第三者が会員情報を呼び出す API にアクセス可能な状態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 （情報システムの使用に伴う漏えい等の防止）
63	事業者は、多数の委託元から担当者の連絡先及び顧客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 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、委託元である事業者の従業者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）
64	事業者のサーバが VPN 経由でブルートフォース攻撃による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が生じた事案。当該 VPN 機器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）
65	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、顧客の個人データ及び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及び毀損が生じた事案。当該 VPN 機器の脆弱性について、事業者が十分な対応を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）
66	事業者のサーバ及び端末が 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、当該 VPN 機器	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
	について脆弱性情報が公開されていたにもかかわらず、対応をしていなかったこと等が原因と考えられる。	の防止）
67	事業者は委託元である事業者に対し、業務用システム及びシステムを利用するための PC を提供しているところ、当該 PC が不正アクセスを受け、委託元である事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、リモート接続用ソフトを利用して当該 PC のリモート保守を実施していたところ、当該ソフトの認証情報を他の委託元のものと同一にしていたこと等が原因と考えられる。	技術的安全管理措置 （アクセス制御、アクセス者の識別と認証）
68	事業者に所属する医師がサポート詐欺に遭い、患者の個人データについて漏えいのおそれが生じた事案。当該医師は個人 PC を業務に使用していたところ、当該 PC には、事業者が定める個人 PC を使用する場合の規律に従った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。	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）
69	事業者は、地方公共団体からウェブサイトの構築等の業務及びそれに伴う個人データの取扱いの委託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[6]による不正アクセスを受け、当該ウェブサイトに登録した者の個人データについて漏えいのおそれが生じた事案。当該ウェブサイトを運用するウェブサーバに SQL インジェクション攻撃に対する脆弱性が存在し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）
70	事業者のサーバが不正アクセスを受け、サーバ内に保管されていた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、不正アクセスに利用されたアカウントの認証情報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。	個人データの取扱いに係る規律の整備 技術的安全管理措置 （アクセス者の識別と認証）
71	事業者の従業者がサポート詐欺に遭い、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。事業者が、サポート詐欺による不正アクセス等について、従業者に情報提供や注意喚起の実施等を行っ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）
72	事業者のサーバが VPN 経由で不正アクセスを受け、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。事業者が、当該 VPN 機器について脆弱性情報が公表されていたにもかかわらず、対応を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）

[6] 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。

	事案の概要	指導事項
73	事業者は住宅管理等の業務及びそれに伴う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VPN経由で不正アクセスを受け、ランサムウェアに感染し、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）

イ　その他の事案

	事案の概要	指導事項
1	事業者が、インターネットメディア及び新聞から性犯罪に関する報道記事を集め、性犯罪の加害者として報道された者に関する個人情報を収集し、個人情報データベース等を構成し、その一部である個人データをウェブサイトで公開するマップに掲載することで、個人データを第三者に提供していた事案。事業者は、当該マップの公開に当たりあらかじめ本人から同意を得ておらず、個人情報保護法第 27 条第１項の規定違反が認められた。また、事業者は、性犯罪の加害者として報道された者に対する不当な差別が、不特定多数の者によって誘発されるおそれがあることが予見できるにもかかわらず、性犯罪の加害者として報道された者の個人情報を集約してデータベース化し、インターネット上で公開しており、同法第 19 条の規定違反が認められた。	不適正な利用の禁止（個人情報保護法第 19 条の規定違反） 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）
2	教員が、海外出張中に個人データが保存された PC を入れたかばんを盗まれたことにより、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。事業者においては、個人データの取扱いに係る規律は整備されていたものの、情報セキュリティ責任者でもあった当該教員は、当該規律における取扱手順を遵守しておらず、個人情報の管理が徹底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 （個人データの取扱いに係る規律に従った運用）
3	事業者が、採用活動を行う会社からリファレンスチェックのための照会を受け、元従業者の個人データを本人の同意を得ることなく、第三者である当該会社に提供した事案。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	事業者が個人情報保護法の規定に基づく請求、保有個人データの取扱いに関する苦情の申出先として公開していたメールアドレスが使用できず、外部からの請求、申出等を受け付けることができない状態が長期間継続していた事態が発覚した事案。当該事態は個人情報保護法第 32 条第１項の規定に沿うものではなく、改善が必要であることが認められた。	保有個人データに関する事項の本人への周知（個人情報保護法第 32 条第１項）
5	事業者２社（番号５及び６の事業者）は、健康保険組合等から委託（個人データの取扱いの委託を含む）を受け、患者の情報を医療機関等に提供するシステム及び当該システムを利用するためアプリを共同運用し、当該システム等の運用・保守を、番号７の事業者（委託先）に委託していたところ、当該システム等のプログラムに誤りがあったことにより、一部の患者の情報が、誤って医療機関等に流出し、個人データに漏えいが生じた事案。システム開発時における当該プログラムのテストや確認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）
6	上記案件（番号５）の事業者のうちの１社は、健康保険組合等から委託（個人データの取扱いの委	技術的安全管理措置

	事案の概要	指導事項
	託を含む）を受け、患者の情報を医療機関等に提供するシステム及び当該システムを利用するためアプリを共同運用し、当該システム等の運用・保守を、番号７の事業者（委託先）に委託していたところ、当該システム等のプログラムに誤りがあったことにより、一部の患者の情報が、誤って医療機関等に流出し、個人データに漏えいが生じた事案。システム開発時における当該プログラムのテストや確認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）
７	事業者は、上記案件（番号５）の委託先から、患者の情報を医療機関等に提供するシステム及び当該システムを利用するためアプリの運用・保守の委託を受けていたところ、当該システム等のプログラムに誤りがあったことにより、一部の患者の情報が、誤って医療機関等に流出し、個人データに漏えいが生じた事案。システム開発時における当該プログラムのテストや確認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）
８	事業者は、複数の委託元からシステム運用等の業務及びそれに伴う個人データの取扱いの委託を受けていたところ、当該システムにおいて、委託元である事業者が他の委託元である事業者の情報を閲覧できる設計ミスがあったことにより、委託元である事業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。当該システムは委託元である事業者も利用していたが、事業者が、当該システムのテスト項目に、委託元が利用した場合の検証を含めておらず、設計ミスが放置されたこと等が原因と考えられる。	技術的安全管理措置 （アクセス制御、情報システムの使用に伴う漏えい等の防止）
９	事業者が、個人データが保存されたUSBメモリを入れたかばんの盗難に遭い、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USBメモリを施錠できないかばんに入れ、施錠していない社用車に放置したことが原因と考えられる。	物理的安全管理措置 （機器及び電子媒体等の盗難等の防止、電子媒体等を持ち運ぶ場合の漏えい等の防止）
10	事業者が、約４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）
11	事業者が、約４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）
12	事業者が提供するアプリケーションのAPIに設定ミスがあったことにより、一定の条件を満たす場合に、個人データを含む通知が他のユーザーに送信され、本人以外の者が閲覧可能な状態が生じ、	技術的安全管理措置 （情報システムの使用に伴う

	事案の概要	指導事項
	当該個人データについて漏えいのおそれが生じた事案。事業者においてAPIに制限を設け、当該通知が本人以外に送信されないような設定ができていなかったこと等が原因と考えられる。	漏えい等の防止）
13	事業者の元代表者が在職中に、利用者等の個人データが記載された名簿を、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）
14	事業者は、予約受付等のために委託先である事業者が運営する予約管理サイトを利用しているところ、当該サイトにおける事業者の管理画面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。事業者は速報の提出後、当委員会から何度も確報の提出を求めたにもかかわらず、発覚日から一定期間が経過してもなお確報を提出していないため、安全管理措置の不備が認められた。	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）
15	事業者が官報等に掲載された個人情報を取りまとめ、検索可能なデータベースを構築し、本人の同意を得ることなくウェブサイトで公開していた事案。個人情報保護法第21条第1項及び同法第27条第1項の規定違反が認められた。	利用目的の通知又は公表（個人情報保護法第21条第1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）

▽　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	物理的	
	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	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	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
指導等件数	1	5	3	3	2	1	1

指導等の内容	安全管理措置				委託先の監督	不適正な利用の禁止	取得に際しての利用目的の通知等	第三者提供の制限	保有個人データに関する事項の公表等
	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	9	26	42	8	3	1	1	4	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	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	不動産業、物品賃貸業
指導等件数	2	15	1	9	5	14	1	2

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	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	2	3	4	5	20

※　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	4	30	21	26

※　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 39 件　※

・ウェブサイトに掲載している文書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、アクセス制御の不備（４件)、媒体の管理等の不備（３件）などに対して指導を行った。
・下表の事案対応のほか、漏えい等報告の提出の遅延に関し、26 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	地方公共団体が、システムの保守管理業務を委託していたところ、委託先である事業者のサーバが 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、保有個人情報について漏えいのおそれが生じた事案。地方公共団体において、委託契約を締結してから２年以上の間、実地確認やチェックシート等での確認を実施していなかったことが原因と考えられる。	個人情報の取扱いの委託
2	行政機関がホームページに掲載した資料の様式に誤りがあったことで、保有個人情報を含む元データが閲覧可能な状態となっていたこと、また、第三者により、当該資料がウイルスチェックサイトにアップロードされたことで漏えいが生じた事案。当該資料を掲載する際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
3	行政機関の職員が、個人情報が記載された行政文書（書面）及び PC を、これらを入れたかばんごと紛失し、保有個人情報について漏えいのおそれが生じた事案。保護管理者との間で安全確保のための移送方法について確認が行われておらず、また当該職員は当該行政文書等を持ったまま飲酒を伴う会合に参加しており、行政機関が定める規定に即した対応ができていなかったこと等が原因と考えられる。	媒体の管理等
4	公立小学校において、いじめに関するアンケートがクラウドサービス上で実施されたところ、教職員が設定を誤ったことで全生徒が当該アンケートに含まれる保有個人情報を閲覧可能となっており、保有個人情報の漏えいが生じた事案。教育委員会では、規程上、いじめに関する情報をクラウドサービスに登録してはならないこととしていたが、当該規程の定めに従った保有個人情報の取扱	アクセス制御

	事案の概要	指導事項
	いがなされていなかったこと等が原因と考えられる。	
5	公立小学校において、教職員がコミュニケーションツールに保存した、生徒の保有個人情報を含むファイルへのアクセス権限の設定を誤ったことで、地方公共団体内の児童、生徒及び教職員等が、当該保有個人情報を閲覧することが可能な状態となっており、保有個人情報の漏えいが生じた事案。教育委員会では、規程上、当該保有個人情報については、コミュニケーションツールへの格納を禁止、又はアクセス制限を設定することとしていたが、当該規程の定めに従った保有個人情報の取扱いがなされていなかったこと等が原因と考えられる。	アクセス制御
6	地方公共団体がウェブサイトに掲載している文書について、個人情報のマスキングが不十分であったため当該情報が外部から閲覧可能な状態となり、保有個人情報の漏えい等が生じた事案。当該ウェブサイトに当該文書を掲載する際、マスキングについての確認や、ダブルチェックが実施さ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
7	公立高校で、学習支援システムが不正アクセスを受け、職員、生徒等の保有個人情報の漏えいが生じた事案。当該システムの管理者アカウントの認証情報の管理が適切ではなかったこと、当該認証情報が長期間変更されていなかったこと等が原因と考えられる。	アクセス制御
8	地方公共団体は、指定管理者である事業者に対して保有個人情報の取扱いを委託していたところ、当該個人情報が、指定期間の満了後も地方公共団体に返還されず、事業者において指定管理業務の範囲を超えて利用された事案。地方公共団体が指定期間満了後、約１年２か月の間、当該個人情報の返還を求めなかったことについて、安全管理措置の不備が認められた。	廃棄等
9	地方公共団体において、行政文書ファイルが決裁のために担当課に持ち込まれたところ、当該ファイルが職員の机上に放置されたことにより紛失し、漏えいのおそれ及び滅失のおそれが生じた事案。地方公共団体において、保有個人情報が記録されている媒体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。	媒体の管理等
10	公立中学校の職員がクラウドサービスの設定を誤り、生徒の保有個人情報について漏えいが生じた事案。当該職員が当該サービスの操作方法等に関する研修を受講していなかったこと等が原因と考えられる。	教育研修 アクセス制御
11	公立中学校の職員が、無断で私物の USB メモリに要配慮個人情報を含む生徒の保有個人情報を保存し、持ち帰り、当該 USB メモリを紛失したことで、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。当該中学校の規程では、当該保有個人情報の複製や持ち出しの制限等がされていたにも	複製等の制限

	事案の概要	指導事項
	かかわらず、当該規程が遵守されていなかったこと等が原因と考えられる。	
12	行政機関において、保有個人情報が記録された文書を紛失し、保有個人情報の滅失及び漏えいのおそれが生じた事案。廃棄用の文書箱と廃棄しない文書箱が同じ書庫で保管されており、かつ、整理されていなかったこと等が原因と考えられる。	媒体の管理等 廃棄等
13	地方公共団体の職員が、会議資料等を自宅に持ち帰った後、投棄し、住民に発見されたことで、要配慮個人情報を含む保有個人情報の漏えいが生じた事案。当該職員は、これまでに度々許可なく文書を自宅に持ち帰っており、溜まった書類の処分に困り投棄したものであるところ、地方公共団体においては、保有個人情報が記録されている媒体の外部への持ち出しの制限に関する措置について、不十分な状態であったこと等が原因と考えられる。	複製等の制限

▽　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	個人情報の取扱いの委託
		複製等の制限	媒体の管理等	誤送付等の防止	廃棄等	アクセス制御	
指導等件数	1	2	3	2	2	4	1

※　一つの事案で複数の内容に該当する場合は全て計上している。

※　漏えい等報告の提出の遅延のみの事案は除く。

▽　指導等対象の行政機関等（組織区分）別件数

組織区分	国の行政機関等	地方公共団体等
指導等件数	3	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	6	7	0	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７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　※

※　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、顧客の個人データ及び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が生じた事案。当該 VPN 機器の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）
２	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、顧客の個人データ及び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。事業者において、VPN 機器やサーバ機器等に対するパッチが未適用であったこと等が原因と考えられる。 ※Ⅱ１（１）①ア 不正アクセスを原因とする漏えい等事案 8 番の事案と同じ	技術的安全管理措置（外部からの不正アクセス等の防止）
３	事業者のサーバが UTM 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、事業者及び委託元である事業者（事業者のグループ会社）の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が生じた事案。事業者が当該 UTM 機器の脆弱性への対応を行っていなかったこと等が原因と考えられる。 ※Ⅱ１（１）①ア 不正アクセスを原因とする漏えい等事案 15 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、顧客の個人データ及び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が生じた事案。当該 VPN 機器には、脆弱性が複数確認されていたにもかかわらず、事業者が保守業者（個人データの取扱いの委託はない）との間で、アップデート等について取決めをしていなかったことから、当該脆弱性への対応が実施されていなかったこと、当該 VPN 機器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 不正アクセスを原因とする漏えい等事案 29 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	事業者の社内システムが VPN 経由で不正アクセスを受け、ランサムウェアに感染し、ファイルが暗号化され、顧客の個人データ及び従業員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が生じた事案。利用された管理者権限アカウントのパスワードが十分な強度を有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）

	事案の概要	指導事項
	※Ⅱ１（１）①ア 不正アクセスを原因とする漏えい等事案 37 番の事案と同じ	
６	事業者がグループ会社から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 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、事業者及びグループ会社の顧客の個人データ並びに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。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。 ※Ⅱ１（１）①ア 不正アクセスを原因とする漏えい等事案 38 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）
７	事業者のサーバ及び PC 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、顧客の個人データ並びに従業者及び取引先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。当該 VPN 機器について脆弱性情報が公開されていたにもかかわらず対応を行っていなかったこと、利用された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 不正アクセスを原因とする漏えい等事案 44 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）
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、ファイルが暗号化され、委託元の顧客等の個人データ及び従業員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。事業者が、当該 VPN 機器について脆弱性情報が公開されていたにもかかわらず対応をしていなかったこと等が原因と考えられる。 ※Ⅱ１（１）①ア 不正アクセスを原因とする漏えい等事案 46 番の事案と同じ	技術的安全管理措置 （外部からの不正アクセス等の防止）
９	事業者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及び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が生じた事案。侵入口は事業者の外国子会社のシステムであるところ、事業者がグループ会社間のアクセスについて、十分なセキュリティ対策を講じていなかったこと等が原因と考えられる。 ※Ⅱ１（１）①ア 不正アクセスを原因とする漏えい等事案 52 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）
10	事業者は取引先から依頼（個人データの取扱いの委託を含む）を受けて設備の販売を行っているところ、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、顧客の個人データ及び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。利用されたアカウントのパスワードの強度に問題があったこと、当該サーバのサポートが切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 （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
	※Ⅱ１（１）①ア 不正アクセスを原因とする漏えい等事案 56 番の事案と同じ	
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、顧客の個人データ及び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のおそれが生じた事案。当該 VPN 機器について、脆弱性情報が公開されていたにもかかわらず対応していなかったこと、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 不正アクセスを原因とする漏えい等事案 58 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）
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、顧客の個人データ及び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及び毀損が生じた事案。当該 VPN 機器の脆弱性について、事業者が十分な対応を行っていなかったこと等が原因と考えられる。 ※Ⅱ１（１）① ア 不正アクセスを原因とする漏えい等事案 65 番の事案と同じ	技術的安全管理措置 （外部からの不正アクセス等の防止）

(2) 報告徴収、立入検査（第 35 条第１項）　０件　※

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

Ⅲ　公表事案に関する指導・助言等の対象先における改善策の実施状況

権限行使日 （参照箇所）	対象	改善策の実施状況
令和６年３月 28 日 (https://www.ppc.go.jp/files/pdf/240328_houdou.pdf)	LINE ヤフー株式会社	・LINE ヤフー株式会社（以下「LY 社」という。）の業務委託先企業の PC がマルウェアに感染したことが契機となり、LY 社の情報システムが不正アクセスを受け、コミュニケーションアプリである LINE に関する個人データが漏えい等した事案について、委員会は、LY 社に対し、令和６年３月 28 日、個人情報保護法第 148 条第１項の規定により勧告を行い、同法第 146 条第１項の規定により、令和７年３月 31 日を最終として３か月ごとに改善状況を報告するよう求めていた。 ・今般、LY 社から令和７年３月 31 日に報告のあった改善状況について確認したところ、NAVER グループ及び NAVER Cloud 社（以下「NC 社」という。）との認証基盤やシステムの分離については、LY 社本体については概ね完了し、国内及び海外子会社においても計画どおり進んでいるほか、NAVER グループ及び NC 社への委託業務の終了や縮小等も計画どおり進んでいることが認められた。また、漏えい等事案に対応するための定期演習の実施や、ペネトレーションテストや振る舞い検知のテストの結果を踏まえた是正対応等についても進展が認められた。 ・委員会としては、今後も LY 社の改善策が計画どおり進むことを注視するとともに、LY 社には、全ての改善策が完了する令和８年３月末まで利用者等のステークホルダーへの丁寧な説明等を期待したい。
令和６年６月 27 日 (https://www.ppc.go.jp/files/pdf/240627_01_houdou.pdf)	東京電力パワーグリッド株式会社、東京電力ホールデ	・本件は、東京電力パワーグリッド株式会社（以下「東京電力 PG」という。）が利用し顧客情報等が管理されている「接点情報システム[7]」及び「要請応対システム[8]」（以下併せて「本件システム」という。）において、東京電力 PG の親会社である東京電力ホールディングス株式会社（以下「東京電力 HD」という。）及び東京電力 HD の子会社である東京電力リニューアブルパワー株式会社（以下「東京電力 RP」という。）に対し、本件システムのアクセス権限が誤って設定されていたことから、本件システム上の東京電力 PG の顧客の個人デー

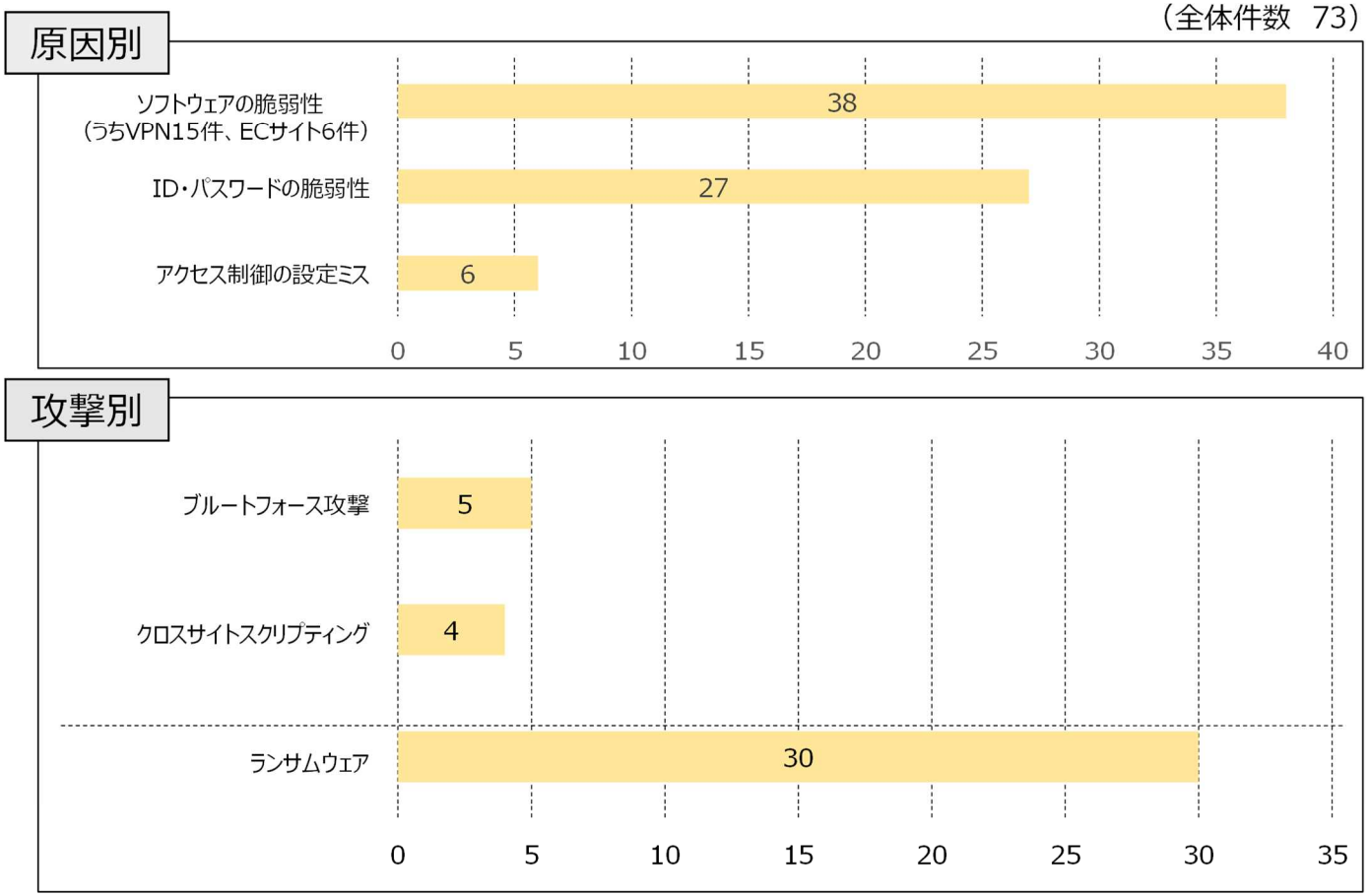
[7] 東京電力 PG と東京電力エナジーパートナーが、顧客と接点を有する業務における顧客情報や顧客との接触に関する情報を集約するシステム
[8] 東京電力 PG と東京電力エナジーパートナーが、顧客からの意見・要望、対応状況や結果を共有するシステム

権限行使日 （参照箇所）	対象	改善策の実施状況
	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	タが、東京電力 HD 及び東京電力 RP から閲覧できる状態となっていた事案である。 ・委員会は、令和６年６月 27 日、東京電力 PG、東京電力 HD、東京電力 RP（以下「東京電力グループ３社」という。）に対し、個人情報保護法第 147 条の規定による指導を行うとともに、再発防止策の実施状況及び個人情報の適正な取扱いに関する全社的総点検の結果について、同法第 146 条第１項の規定による報告を求めた。 ・今般、委員会は、東京電力グループ３社からそれぞれ報告を受け、再発防止策の実施状況や総点検の結果について確認を行ったところ、再発防止策について一定の取組が認められた。 ・また、個人情報の取扱いに関する全社的総点検の結果については、電気事業法上の非公開情報を他社が閲覧していたというような重大な事例は認められず、また、一部の取扱いに軽微な問題点が認められたものの、それらの問題点は速やかに是正され、総点検の成果が認められていることから、重ねての指導は行わないこととする。 ・委員会は、東京電力グループ３社が再発防止策を確実に実施すること等を引き続き注視していく。
令和６年７月 17 日 (https://www.ppc.go.jp/files/pdf/240717_houdou.pdf)	富士通 Japan 株式会社	・委員会は、高松市のコンビニ交付サービスにおける証明書誤交付事案に関して、富士通 Japan 株式会社（以下「富士通 Japan」という。）に対し、令和６年７月 17 日に個人情報保護法第 147 条の規定による指導を行い、同法第 146 条第１項の規定により、改善策の実施状況について報告するよう求めていた。 ・富士通 Japan から、令和６年９月 30 日及び令和７年１月 31 日、報告書の提出を受け、かかる報告に記載の改善策の実施状況について確認したところ、前記指導時点で確認された安全管理措置の不備に対する改善策が実施され、また、同社の提供するコンビニ交付サービスを利用する全ての地方公共団体に出力異常検出機能を適用完了する等、策定された再発防止策に沿った改善の取組が認められるものであった。 ・委員会としては、今後も、富士通 Japan において改善策が確実に継続され、同種の証明書誤交付事案が再発しないことを、引き続き注視していく。

権限行使日 （参照箇所）	対象	改善策の実施状況
		・なお、コンビニ交付サービスの年間稼働ピークが毎年３月末～４月頭であるところ、令和７年３月末及び４月頭において、証明書誤交付事案は１件も発生していないことを確認している。
令和７年４月 30 日 （https://www.ppc.go.jp/files/pdf/250430_02_houdou.pdf）	東京海上日動火災保険株式会社、損害保険ジャパン株式会社、三井住友海上火災保険株式会社、あいおいニッセイ同和損害保険株式会社	・複数の損害保険会社の保険商品を取り扱う一部の損害保険代理店が、損害保険会社から保険契約の締結等の業務を委託されることに伴って取扱いを委託されていた、保険契約者の個人データ（契約者氏名、証券番号、保険料、契約した損害保険会社名等）を本人の同意なく、他の損害保険会社に提供等した事案（代理店事案）及び、損害保険会社から損害保険代理店に出向している従業者が、出向先の保険代理店が管理する、他の損害保険会社の保険契約者に関する個人データ等（契約者氏名、証券番号、保険料、契約した損害保険会社名、保険期間等）を、出向先保険代理店に無断で、かつ、本人の同意を得ることなく、出向元の損害保険会社に対し、メール等により送付していた事案（出向者事案）について、委員会は、東京海上日動火災保険株式会社、損害保険ジャパン株式会社、三井住友海上火災保険株式会社及びあいおいニッセイ同和損害保険株式会社（以下これらをまとめて「大手損保４社」という。）に対し、令和７年４月 30 日、個人情報保護法第 147 条の規定による指導を行い、同法第 146 条第１項の規定により再発防止策の実施状況について、報告等の求めを行った。 ・今般、大手損保４社から報告等を受け、再発防止策の実施状況について検討したところ、現時点において委員会の指導事項を踏まえた一定の取組が認められた。委員会としては、大手損保４社が再発防止策を確実に実施すること等を、引き続き注視していく。

以　上

（参考）指導案件のうち不正アクセス事案の原因分析（令和７年度第１四半期）



（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（73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。