個人情報の保護に関する法律についてのガイドライン（通則編）「10（別添）講ずべき安全管理措置の内容」の「手法の例示」等の一部更新（案）について

第１　安全管理措置の「手法の例示」等の一部更新の必要性

個人情報の保護に関する法律についてのガイドライン（通則編）（以下「ガイドライン（通則編）」という。）「10（別添）講ずべき安全管理措置の内容」（以下「ガイドライン（通則編）別添」という。）は、平成 28 年にガイドライン（通則編）が策定された当時から、内容が大きくは変わっていない。

個人情報保護委員会（以下「当委員会」という。）の監視・監督業務においては、ガイドライン（通則編）別添に記載の安全管理措置の項目に従い、権限行使の要否、その内容等を検討している。

この点、クラウドサービスの普及、デバイスの高機能化等、情報通信技術の進展により個人情報取扱事業者による個人データの取扱いの態様は多岐にわたっている。また、近年、個人情報取扱事業者等への機密情報等の窃取・破壊等を企図したサイバー攻撃が一層高度化・複雑化・巧妙化し、攻撃対象も拡大し続けており、個人データ等の漏えい等の大きな要因となっている。「情報セキュリティ 10 大脅威 2026」（独立行政法人情報処理推進機構（ＩＰＡ））[1]では、組織向けの脅威として「ランサム攻撃による被害」が 11 年連続、「システムの脆弱性を悪用した攻撃」が６年連続でランクインしており、当委員会が過去に指導を行った不正アクセスを原因とする漏えい等事案においても、主な攻撃手法としてランサムウェアによる攻撃[2]が多く確認されている[3]。

このように、個人情報取扱事業者においては、情報通信技術の進展への対応だけでなく、侵入型ランサムウェアを代表とする、ネットワークの奥深くまで侵入する攻撃を含む、情報システムに対する不正アクセス等を防止することが期待されているところ、ガイドライン（通則編）別添の内容を、このような最近の技術的な動向や事案の傾向に合わせて更新する必要性が高まっている。

第２　安全管理措置の全体像

個人情報の保護に関する法律（平成 15 年法律第 57 号）（以下「法」という。）第 23 条では、「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は

---

[1] 当年に発生した社会的に影響が大きかった情報セキュリティの事故や攻撃の状況などから、ＩＰＡが脅威候補を選定し、情報セキュリティ分野の研究者、企業の実務担当者などのメンバーからなる「10 大脅威選考会」が審議・投票を経て決定したもの。

[2] 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。

[3] 「監視・監督状況（四半期別）」（個人情報保護委員会）（URL：https://www.ppc.go.jp/personalinfo/activity/）参照

毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」と規定されている。

ガイドライン（通則編）別添は、同条の「個人データの安全管理のために必要かつ適切な措置」、すなわち、安全管理措置として、個人情報取扱事業者が具体的に講じなければならない措置や当該措置を実践するための手法の例等について示すものである。ガイドライン（通則編）別添は、「講じなければならない措置」と、当該措置を実践するための「手法の例示」で構成されており、「講じなければならない措置」は、これらに従わなかった場合、法違反と判断される可能性があるが、「手法の例示」は、文字どおり例を示したものであって、必ずしも例示の内容の全てを講じなければ、法違反と判断されるというものではなく、また、適切な手法は例示の内容に限られない。

この点、ガイドライン（通則編）別添では、「安全管理措置を講ずるための具体的な手法については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものである」としている。

なお、中小規模事業者[4]については、その他の個人情報取扱事業者と同様に、法第23 条に定める安全管理措置を講じなければならないが、取り扱う個人データの数量及び個人データを取り扱う従業者数が一定程度にとどまること等を踏まえ、円滑にその義務を履行し得るような手法の例として、「中小規模事業者における手法の例示」が示されている。

以上を前提に、ガイドライン（通則編）別添は、「10-1 基本方針の策定」、「10-2 個人データの取扱いに係る規律の整備」、「10-3 組織的安全管理措置」、「10-4 人的安全管理措置」、「10-5 物理的安全管理措置」、「10-6 技術的安全管理措置」及び「10-7 外的環境の把握」に関して、「講じなければならない措置」及び「手法の例示」を示している。

第３　個別の更新内容（案）（資料２－２－２）

更新内容（案）について、現行のガイドライン（通則編）別添からの変更内容を、色付きの文字（赤字又は青字）で示したものが資料２－２－２である。

現行のガイドライン（通則編）別添からの内容的な変更点及びその理由は以下のとおりである。

１　「個人情報の保護に関する法律についてのガイドライン」に関するＱ＆Ａにお

[4] 「中小規模事業者」とは、従業員の数が 100 人以下の個人情報取扱事業者をいう。ただし、次に掲げる者を除く。
・その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去６月以内のいずれかの日において 5,000 を超える者
・委託を受けて個人データを取り扱う者

ける手法の例について

(1)　更新内容

「個人情報の保護に関する法律についてのガイドライン」に関するＱ＆Ａ（以下「Ｑ＆Ａ」という。）のうち、ガイドライン（通則編）別添の「手法の例示」を示していると考えられるもの（資料２－２－３、下線部）について、ガイドライン（通則編）別添に記載を一本化する。当該一本化による更新は、資料２－２－２において、青字で記載している。

(2)　更新理由

Ｑ＆Ａには、ガイドライン（通則編）別添の「手法の例示」を示していると考えられるものが存在する。現行のガイドライン（通則編）別添とＱ＆Ａの対応関係を示したものが資料２－２－３であり、当該Ｑ＆Ａのうち、ガイドライン（通則編）別添の「手法の例示」を示していると考えられるものについて下線を付している。

当該下線部の内容について参照しやすくするため、ガイドライン（通則編）別添に記載を一本化することとした。

２　組織的安全管理措置について

(1)　10-3(1)組織体制の整備の「手法の例示」について

ア　更新内容

①　ガイドライン（通則編）別添 10-3(1)組織体制の整備の「手法の例示」として「責任部署の設置及び役割の明確化」を追記する。

②　同「手法の例示」の「法や個人情報取扱事業者において整備されている個人データの取扱いに係る規律に違反している事実又は兆候を把握した場合」及び「個人データの漏えい等事案の発生又は兆候を把握した場合」の報告連絡先として「責任部署」を追記する。

イ　更新理由

①　現行のガイドライン（通則編）別添 10-3(1)組織体制の整備の「手法の例示」では、「個人データの取扱いに関する責任者の設置及び責任の明確化」が示されている。しかし、個人情報取扱事業者においては、責任者だけでなく、責任者を支える部署として責任部署を設置し、責任部署が、実際の業務を行っている場合が見られている（個人情報保護委員会事務局「個人データの取扱いに関する責任者・責任部署の設置に関する事例集」（令和５年 11 月）参照)。そして、比較的大規模な事業者においては、複数の部署で個人データを取り扱う等、個人データの取扱いが多岐にわたることで各部署の役割分担や責任の範囲が曖昧になった結果、漏えい等事案発生や被害拡大が生じる場合が実際に見られている。このような場合に、

責任者が各部署における個人データの取扱いを全て把握することは実際上困難であり、事業者の規模に応じて、責任部署を設置すべき場合があるものと考えられる。なお、「責任部署」とは、コンプライアンス部等の、事業部における業務執行を監督等する部署を指しているのに対し、現行のガイドライン（通則編）別添 10-3(1)組織体制の整備の「手法の例示」として示されている「個人データを複数の部署で取り扱う場合の各部署の役割分担及び責任の明確化」における「複数の部署」とは、業務執行を担う事業部を含むものである。

② 法や個人情報取扱事業者において整備されている個人データの取扱いに係る規律に違反している事実又は兆候を把握した場合及び個人データの漏えい等事案の発生又は兆候を把握した場合、前記責任者だけでなく、前記責任部署に対しても報告をすることが適切と考えられるため。

(2) 10-3(2)個人データの取扱いに係る規律に従った運用及び同(3)個人データの取扱状況を確認する手段の整備について

ア 更新内容

① 現行のガイドライン（通則編）別添 10-3(2)個人データの取扱いに係る規律に従った運用及び同(3)個人データの取扱状況を確認する手段の整備の「講じなければならない措置」並びに「手法の例示」の内容を、10-3(2)個人データの取扱いに係る規律に従った運用の「講じなければならない措置」及び「手法の例示」として記載を一本化する[5]。更新後の 10-3(2)個人データの取扱いに係る規律に従った運用の「手法の例示」では、基本的に、現行の 10-3(2)個人データの取扱いに係る規律に従った運用に関する手法の例を「(個人データの取扱いに係る規律に従った運用の確保)」、現行の 10-3(3)個人データの取扱状況を確認する手段の整備に関する手法の例を「(個人データの取扱状況を確認する手段の整備)」として記載する。

② ガイドライン（通則編）別添 10-3(2)個人データの取扱いに係る規律に従った運用の「手法の例示」として「個人データの取扱いに係る規律を明確化し、従業者に周知する」ことを追記する。

③ 同「手法の例示」として、個人データの取扱いに係る規律に従った運用を確保するために「あらかじめ整備された個人データの取扱いに係る規律に従って個人データが取り扱われていることを、責任者又は責任部署が確認する」ことを追記する。また、当該確認の手段として、「あらかじめ整備された個人データの取扱いに係る規律と照らし合わせること」を追記する。

イ 更新理由

[5] これにより現行のガイドライン（通則編）別添 10-3(4)が同(3)に、同 10-3(5)が同(4)となる。

① 現行のガイドライン（通則編）別添 10-3(2)個人データの取扱いに係る規律に従った運用では、個人データの取扱いに係る規律に従った運用を確保するための手法の例として、「システムログその他の個人データの取扱いに係る記録の整備や業務日誌の作成等を通じて、個人データの取扱いの検証を可能とすること」を示している。くわえて、同 10-3(3)個人データの取扱状況を確認する手段の整備では、手法の例として、「例えば次のような項目をあらかじめ明確化しておくことにより、個人データの取扱状況を把握可能とすることが考えられる」として、あらかじめ明確化しておく項目を示している。このように、現行のガイドライン（通則編）別添 10-3(2)及び同(3)はいずれも、個人データの取扱いに係る記録の整備等を手法の例として示しているように読め、「手法の例示」の記載に重複感がある。

この点、10-3(2)個人データの取扱いに係る規律に従った運用及び 10-3(3)個人データの取扱状況を確認する手段の整備の「中小規模事業者における手法の例示」がいずれも「あらかじめ整備された基本的な取扱方法に従って個人データが取り扱われていることを、責任ある立場の者が確認する」こととされていることからして、いずれも個人データの取扱いに係る規律に従った運用を確保することが目的であり、個人データの取扱状況の確認やこの手段の整備は、当該運用を確保するための手段とも位置付けられるため。

② 個人データの取扱いに係る規律を明確化し、従業者に周知することが適切に行われていないことで、個人データの取扱いに係る規律に従った運用が確保されず、漏えい等事案発生の原因となっている場合が、実際に見られている。従来、このような事案においては、ガイドライン（通則編）別添10-3(2)個人データの取扱いに係る規律に従った運用に関する安全管理措置に不備があるとして指導等の権限行使を行ってきたが、個人データの取扱いに係る規律を明確化し、従業者に周知することについては、現行のガイドライン（通則編）別添 10-3(2)個人データの取扱いに係る規律に従った運用の「手法の例示」として明記されていないため、明確化のために追記が必要であると判断した。なお、ガイドライン（通則編）別添「10-4 人的安全管理措置」では、従業者に、個人データの適正な取扱いを周知徹底するとともに適切な教育を行わなければならないとされ、個人データの取扱いに係る規律を従業者に周知する点については、人的安全管理措置を講ずる過程で実現されるとも考えられる。しかし、個人データの取扱いに係る規律を従業者に周知するには、当該規律を、従業者が定常的に参照できるようにしておくこと等も考えられるところ、「10-4 人的安全管理措置」

では、定期的な研修等によって従業者に教育を行う場面を念頭に置いているため、定常的な措置等を含む観点については、人的安全管理措置とは別に、組織的安全管理措置を講ずるための手法の例として位置付けることが適切である。このように、本「手法の例示」の追記は、人的安全管理措置を実践するための手法の例を上乗せ的に追記するものではなく、組織的安全管理措置に関する当委員会の従来の運用を明確化するものである。

③　あらかじめ整備された個人データの取扱いに係る規律に従って個人データが取り扱われていることを、責任者又は責任部署が、あらかじめ整備された個人データの取扱いに係る規律と照らし合わせる等の方法で確認することが適切に行われていないことが、漏えい等事案の発生や被害拡大の原因となっている場合が、実際に見られているため。

(3)　10-3(4)取扱状況の把握及び安全管理措置の見直しの「手法の例示」について

ア　更新内容

ガイドライン（通則編）別添 10-3(4)取扱状況の把握及び安全管理措置の見直しの「手法の例示」として、「個人データの取扱状況、情報技術の進歩等を踏まえて、講じた安全管理措置について、定期的に評価及び見直しを行い、必要に応じて改善をする」ことを追記する。

イ　更新理由

個人データの取扱状況、情報技術の進歩等を踏まえた、安全管理措置の評価、見直し及び改善が適切に行われていないことが、漏えい等事案発生の原因となっている場合が、実際に見られている。そして、現行のガイドライン（通則編）別添 10-3(5)取扱状況の把握及び安全管理措置の見直しでは、「講じなければならない措置」として「個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない」ことを示しているが、「手法の例示」では自ら行う点検又は他部署、外部の主体等による監査が示されており、「講じなければならない措置」である安全管理措置の見直しを実践するための手法の例については、必ずしも明確にはされていないことから、当該手法の例について追記する必要があると判断した。

３　人的安全管理措置について

(1)　10-4〇従業者の教育の「手法の例示」について

ア　更新内容

ガイドライン（通則編）別添 10-4〇従業者の教育の「手法の例示」として、「従業者に対する定期的な研修等の内容、実施方法等を評価、見直し及び改善する」ことを追記する。

イ　更新理由

従業者に対する定期的な研修等の内容、実施方法等の評価、見直し及び改善が適切に行われていないことが、漏えい等事案発生の原因となっている場合が、実際に見られているため。

4　物理的安全管理措置について

(1)　10-5(4)個人データの削除及び機器、電子媒体等の廃棄の「手法の例示」について

ア　更新内容

ガイドライン（通則編）別添 10-5(4)個人データの削除及び機器、電子媒体等の廃棄の「手法の例示」における、個人データが記録された機器、電子媒体等を廃棄する場合の手法の例として「暗号化消去」を追記する。

イ　更新理由

後記５(5)のとおり。

5　技術的安全管理措置について

(1)　用語の統一

ア　更新内容

用語を「個人データを取り扱う情報システム」に統一する。

イ　更新理由

現行のガイドライン（通則編）別添「10-6 技術的安全管理措置」では、技術的安全管理措置を講ずる客体として「個人情報データベース等」、「個人情報データベース等を取り扱うことのできる情報システム」、「情報システム」という用語が混在しているが、個人情報データベース等を構成する個人データ及び個人情報データベース等から抽出した個人データについて安全管理措置を講ずることが求められるため。

(2)　10-6(1)アクセス制御の「手法の例示」について

ア　更新内容

①　ガイドライン（通則編）別添 10-6(1)アクセス制御の「手法の例示」として、「特権アカウントを割り当てる従業者、利用する端末、利用する場面等を最小限に限定する」ことを追記する。

②　同「手法の例示」として、「組織体制に変更が生じた場合（例えば、人事異動、従業者の退職等）等に、アクセス権限の変更を適切に行う」ことを追記する。

③　同「手法の例示」として、「組織内外からのアクセスについて、アクセス要求ごとにアクセス元の場所、アクセス時間、デバイスのセキュリティ

状態等の動的コンテキストを評価し、リスクに応じてアクセスの可否を判断する仕組みを導入する」ことを追記する。

イ　更新理由

①　近年の不正アクセスを原因とする漏えい等事案は侵入型ランサムウェアを代表として、ネットワークの奥深くまで侵入する事案が増えており、個人情報取扱事業者においては、侵入を防ぐための対策をとりつつも、侵入された場合に被害拡大を防止するための対策を講ずることが期待されている。この点、管理者権限を有するアカウントが侵害・利用された場合には、大規模な横展開につながるおそれがあり、管理者権限を有する特権アカウントの利用は厳格に制限されるべきであるため。

②　組織体制に変更が生じた場合（例えば、人事異動、従業者の退職等）等に、アクセス権限の変更を適切に行っていないことが、漏えい等事案発生の原因となっている場合が、実際に見られているため。

③　現行のガイドライン（通則編）別添「10-6 技術的安全管理措置」は境界型セキュリティモデルを念頭に置いたものである。しかし、他のガイドライン（ＮＩＳＴ「Cybersecurity Framework 2.0」（令和６年２月）等）によれば、ゼロトラストアーキテクチャ（組織内外を問わず何も信頼せず、全てを検証するというセキュリティ概念）の考え方が取り込まれていく傾向が確認された。従来の境界型セキュリティモデルでは、侵入を防ぐことに重点が置かれていたが、ゼロトラストモデルでは侵入を防ぐための対策をとりつつも、侵入され得ることを前提とし被害を最小化するために、いかに侵入を早期に検知するのかに重点が置かれている。

上記の技術的な動向を踏まえて、現時点で、全ての事業者に対してゼロトラストモデルの採用を求めるものではないが、今後、ゼロトラストアーキテクチャの考え方を導入する事業者が更に増加することを見据えて、ゼロトラストモデルの概念を念頭に置いた対策を、「手法の例示」として追記しておく必要があると判断したため。

(3)　10-6(2)アクセス者の識別と認証の「手法の例示」等について

ア　更新内容

①　ガイドライン（通則編）別添 10-6(2)アクセス者の識別と認証の「講じなければならない措置」における、アクセス者の識別と認証が求められる対象を「個人データを取り扱う情報システムを使用する者」とする。

②　ガイドライン（通則編）別添 10-6(2)アクセス者の識別と認証の「手法の例示」における、識別・認証手法の例として「指紋認証・静脈認証・顔認証」を追記する。

③　同「手法の例示」として、ユーザーＩＤ・パスワードを利用する場合の

「同一のユーザーＩＤ・パスワードの使い回しの原則禁止」を追記する。

④　同「手法の例示」として、「組織外ネットワークからのアクセスや、管理者権限でのアクセス、重要な個人データへのアクセスにおいては、識別・認証手法を複数組み合わせる多要素認証（フィッシングに耐性のあるものを含む。）を導入する」ことを追記する。

⑤　同「手法の例示」として、「従業者以外の者を適切に識別・認証する方法を採用する。例えば、同一及び類似パスワードの使い回しをしないよう周知、最低パスワード文字数の設定、一定回数以上ログインに失敗したＩＤの停止、多要素認証（フィッシングに耐性のあるものを含む。）の導入等が考えられる」ことを追記する。

イ　更新理由

①　現行のガイドライン（通則編）別添 10-6(2)アクセス者の識別と認証の「講じなければならない措置」では、アクセス者の識別と認証が求められる対象は、「個人データを取り扱う情報システムを使用する従業者」とされているが、クラウドサービス提供事業者がそのサービスとして個人データを取り扱う情報システムに外部の者がアクセスする場合等、個人データを取り扱う情報システムにアクセスする者は従業者に限られないため。

②　指紋や静脈、顔などの生体情報のデータを事前に登録しておき、認証時に照合して本人であるかどうか判断する方法を導入する事業者等が、増加しているため。

③　複数のアカウントの認証情報等において、ユーザーＩＤ・パスワードを使い回していることが、漏えい等事案発生の原因となっている場合が、実際に見られているため。なお、現行のＱ＆Ａ10-19 では、「同一又は類似パスワードの再利用の制限」とされているところ、同一のユーザーＩＤ・パスワードの使い回しについては原則禁止とすることを手法の例として示すものである。

④　認証を突破することによる不正アクセス事案においては、多要素認証の導入が有効な再発防止策の一つであると考えられることに加え、実際に多要素認証を導入する事業者等が、増加しているため。ただし、多要素認証は、ログイン手順増加による利用者の利便性低下と、機器調達・システム構築に関わる管理者側のコスト増につながるため、多要素認証を導入する対象として考えられるものを「組織外ネットワークからのアクセスや、管理者権限でのアクセス、重要な個人データへのアクセス」に限定して、手法の例として示すものである。

⑤　前記①のとおり、個人データを取り扱う情報システムにアクセスする者は従業者に限られず、従業者以外の外部の者がアクセスする場合も考えら

れ、従業者が情報システムにアクセスする場合と同様に、従業者以外の者が情報システムにアクセスする場合の識別・認証手法の例を追記する必要があるため。

(4) 10-6(3)外部からの不正アクセス等の防止の「手法の例示」について

ア 更新内容

ガイドライン（通則編）別添 10-6(3)外部からの不正アクセス等の防止の「手法の例示」として、「組織が許可し、セキュリティ基準を満たしたデバイスからのみ個人データへのアクセスを許可する」ことを追記する。

イ 更新理由

前記(2)イ③の技術的な動向を踏まえて、現時点で、全ての事業者に対してゼロトラストモデルの採用を求めるものではないが、今後、ゼロトラストアーキテクチャの考え方を導入する事業者が更に増加することを見据えて、ゼロトラストモデルの概念を念頭に置いた対策を、「手法の例示」として追記しておく必要があると判断したため。

(5) 10-6(4)情報システムの使用に伴う漏えい等の防止の「手法の例示」について

ア 更新内容

ガイドライン（通則編）別添 10-6(4)情報システムの使用に伴う漏えい等の防止の「手法の例示」として、「クラウドサービスのサーバ上に保管された個人データを消去する際は、クラウドサービス提供事業者が提供する方法、暗号化消去等、容易に復元できない手段を採用する」ことを追記する。

イ 更新理由

個人データを削除する場合に関しては、現行のガイドライン（通則編）別添「10-5 物理的安全管理措置」の「(4)個人データの削除及び機器、電子媒体等の廃棄」において手法の例が示されている。しかし、クラウドサービスを利用して個人データを取り扱う事業者においては、個人データが記録された電子媒体それ自体を自ら管理しているわけではなく、クラウドサービスのサーバ上に保管された個人データを消去する場合については、現行のガイドライン（通則編）別添 10-5(4)ではカバーできないため、クラウドサービスのサーバ上に保管された個人データを消去する場合の手法の例を追記する必要がある。

そして、クラウドサービスのサーバ上に保管された個人データを消去する手法としては、クラウドサービス提供事業者が提供する方法（例えば、Google Drive 上でゴミ箱に入れたデータをゴミ箱から削除すること等が考えられる。）を利用することだけでなく、個人データを暗号化して記録しておき、抹消が必要になった際に復号に用いる鍵を抹消することで復号を不可能に

し、個人データを利用不能にする論理的削除方法（暗号化消去）[6]を採用することが考えられ、さらに、当該方法は事業者にとっても簡易な手法であることを踏まえ、これらの手法について追記する必要があると判断したため。

なお、自らが管理する電子媒体に記録された個人データの削除においても、同様に暗号化消去の手法を採用することが考えられるところ、この点については物理的安全管理措置に記載するべきであるため、ガイドライン（通則編）別添10-5(4)個人データの削除及び機器、電子媒体等の廃棄の「手法の例示」として「暗号化消去」を追記する。

(6)　10-6(5)不正アクセス等の検知等について

ア　更新内容

①　ガイドライン（通則編）別添「10-6 技術的安全管理措置」の「講じなければならない措置」として「(5)不正アクセス等の検知等」を追記する。

②　ガイドライン（通則編）別添 10-6(5)不正アクセス等の検知等の「手法の例示」として、個人データを取り扱う情報システムの使用状況、個人データへのアクセス状況、個人データを取り扱う情報システムへの外部からのアクセス状況等のログについて「一定の期間保管する」ことを追記する。

③　同「手法の例示」として「不正アクセス等の発生又は兆候を早期に検知等するための仕組み（例えば、ＩＤＳ／ＩＰＳ、ＥＤＲ等）等を導入する」ことを追記する。

④　同「手法の例示」として「不正アクセス等が発生した場合でも個人データを取り扱う情報システムの被害が広がらないよう、必要な対策を講ずる。例えば、侵害を受けた又はそのおそれがある情報システムの停止・隔離、アカウントの無効化などの方法が考えられる。その他必要な対策については、10-6 技術的安全管理措置(1)から(4)の手法の例示も参照されたい」ことを追記する。

⑤　ガイドライン（通則編）別添 10-6(5)不正アクセス等の検知等の「中小規模事業者における手法の例示」として「個人データを取り扱う情報システムの使用状況、個人データへのアクセス状況、個人データを取り扱う情報システムへの外部からのアクセス状況等のログ等を一定の期間保管する」ことを追記する。

イ　更新理由

①　現行のガイドライン（通則編）別添 10-6(3)外部からの不正アクセス等の防止の「手法の例示」では、「ログ等の定期的な分析により、不正アクセス等を検知する」ことが示されている。また、現行のＱ＆Ａ10-20 では、

[6] 総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和８年３月版）」（令和８年３月27 日改定）参照

現行のガイドライン（通則編）別添 10-6(3)外部からの不正アクセス等の防止の手法の例として、「個人データを取り扱う情報システムの使用状況、個人データへのアクセス状況（操作内容も含む。）、個人データを取り扱う情報システムへの外部からのアクセス状況等の監視（個人データへのアクセスや操作の成功や失敗の記録及び不正が疑われる異常な記録の存否の定期的な確認（当該記録の漏えい、滅失及び毀損並びに改ざん及び不正消去等からの適切な保護も含む）も含む。）」が示されている。このように、現行のガイドライン（通則編）等において、「講じなければならない措置」である外部からの不正アクセス等の防止を実践するための具体的な手法として、ログ等の定期的な分析による、不正アクセス等の検知、及び個人データを取り扱う情報システムの使用状況、個人データへのアクセス状況、個人データを取り扱う情報システムへの外部からのアクセス状況等の監視が示されている。しかし、現行のガイドライン（通則編）別添 10-6 の「(3)外部からの不正アクセス等の防止」という標題や、「個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない」との記載から直ちに、前記の具体的な手法が考えられることを読み取れるものではない。したがって、現行のガイドライン（通則編）等において示されている前記手法の例を、現行のガイドライン（通則編）別添 10-6(3)外部からの不正アクセス等の防止より適切な、「講じなければならない措置」を実践するための具体的な手法として再構成する必要があると判断した。

くわえて、他のガイドライン（ＮＩＳＴ「Cybersecurity Framework 2.0」（令和６年２月）等）によれば、侵入を防ぐための対策をとりつつも、侵入され得ることを前提とし被害を最小化するために、いかに侵入を早期に検知するのかに重点が置かれた、ゼロトラストアーキテクチャの考え方が取り込まれていく傾向が確認され、また、不正アクセスを受けた事業者においては、再発防止策等として、ＩＤＳ（不正侵入検知システム）及びＩＰＳ（不正侵入防御システム）といった、ネットワークやサーバへの不正アクセスを監視・防御するセキュリティ技術並びにパソコンやサーバなどのエンドポイントを監視し、不正アクセスを検知・調査・対応するセキュリティ対策である EDR を導入する場合が確認された。そこで、現時点で、全ての事業者に対してゼロトラストモデルの採用を求めるものではないが、今後、ゼロトラストモデルを取り入れる事業者が更に増加することを見据えながら、現時点で事業者に「講じなければならない措置」として課したとしても過度ではないと判断したため、「不正アクセス等の検知等」を追記した。

② 前記①のとおり、現行のガイドライン（通則編）等において、ログ等の定期的な分析による、不正アクセス等の検知、及び個人データを取り扱う情報システムの使用状況、個人データへのアクセス状況、個人データを取り扱う情報システムへの外部からのアクセス状況等の監視が、手法の例として示されているところ、これらの具体的な手法の実現のためには、その前提として、ログ等を一定の期間保管することが必要となるため。

③ 不正アクセス等を適切に検知するには、ログ等の定期的な分析に加えて、ネットワーク等を常時監視することも有効と考えられるところ、前記①のとおり、不正アクセスを受けた事業者においては、再発防止策等として、ＩＤＳ及びＩＰＳといった、ネットワークやサーバへの不正アクセスを監視・防御するセキュリティ技術並びにパソコンやサーバなどのエンドポイントを監視し、不正アクセスを検知・調査・対応するセキュリティ対策であるEDRを導入する場合が確認されたため。

④ 近年の不正アクセスを原因とする漏えい等事案は侵入型ランサムウェアを代表として、ネットワークの奥深くまで侵入する事案が増えており、個人情報取扱事業者においては、侵入を防ぐための対策をとりつつも、侵入された場合に被害拡大を防止するための対策を講ずることが期待されていることを踏まえて、侵入された後の横展開対策について、「手法の例示」として示す必要があると判断したため。なお、ガイドライン（通則編）別添10-6(5)不正アクセス等の検知等では、不正アクセス等を検知した後の被害拡大を防止するための対策について記載しているが、ガイドライン（通則編）別添10-6(1)から(4)における「手法の例示」も、侵入された後の被害拡大を防止するための対策として有効であるため、他の「手法の例示」も参照されるべきである旨を記載している。

⑤ 不正アクセス等の検知等のためには、ログの保管が出発点であることに加えて、不正アクセスの発生原因を明らかにするためにもログの分析は基本である。他方で、ログが存在しないことから不正アクセスの原因が明らかにならず、適切な再発防止策の検討ができない事例も存在し、中小規模事業者が円滑に義務を履行し得るような手法の例として、「個人データを取り扱う情報システムの使用状況、個人データへのアクセス状況、個人データを取り扱う情報システムへの外部からのアクセス状況等のログ等を一定の期間保管する」ことを示すことが必要であると判断したため。

以　上