資　料　２

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）等における安全管理措置の手法の例示の追加等の検討について

１．検討の背景

近年、個人情報取扱事業者及び行政機関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。

このような情勢の中で、個人情報保護委員会（以下「当委員会」という。）は、データ関係省庁等との連携をより一層強化し、個人情報保護法上求められる各種の安全管理措置として講じ得る方策等について検討・把握するとともに、個人情報取扱事業者及び行政機関等に対する効果的な普及啓発の在り方等を検討する観点から、サイバーセキュリティ関係省庁・機関[1]との間で、個人情報保護法サイバーセキュリティ連絡会（以下「連絡会」という。）を令和６年 12 月から現在まで四半期ごとに７回開催している。連絡会では、不正アクセスによる個人データ等の漏えい等事案を踏まえ、個人データ等の漏えい等の対策や留意すべき点について検討するとともに、効果的な普及啓発の方法に係る情報交換を実施している[2]。

この連絡会で得た知見を踏まえ、平成 28 年 11 月の策定当時から内容が大きくは変わっていない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」（以下「ガイドライン（通則編）別添」という。）について、現代化を含めた見直しが必要との考えに至ったものである。具体的には、連絡会で得られた知見に加え、情報通信技術の進展、不正アクセスの脅威動向、当委員会が行政上の対応を行った個別の事案等を踏まえて、下記２．で挙げるような現時点における課題について検討を行うことが考えられる。

２．ガイドライン（通則編）別添の現時点における課題

⑴　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等による個人データ等の取扱いの態様が多岐にわたっていることを踏まえた内容とすることはできないか。

⑵　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

[1] 内閣官房国家サイバー統括室（ＮＣＯ）、警察庁サイバー警察局、独立行政法人情報処理推進機構（ＩＰＡ）、国立研究開発法人情報通信研究機構（ＮＩＣＴ）及び一般社団法人ＪＰＣＥＲＴコーディネーションセンター（ＪＰＣＥＲＴ／ＣＣ）

[2] なお、これまでに、連絡会で得られた知見を広く一般に普及する観点から、令和８年１月に個人データ等の漏えい等対策における留意点等をまとめた「不正アクセス発生時のフォレンジック調査の有効活用に向けた着眼点」（https://www.ppc.go.jp/files/pdf/260116_forensics_keypoints.pdf）を公表している。

リティモデルを念頭に置いたものであるが、ゼロトラストモデルの普及を踏まえ[3]、ゼロトラストアーキテクチャの考え方を取り込むことができないか。

⑶　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、侵入された後の横展開対策を示すことができないか。

⑷　ガイドライン（通則編）別添は、従わなかった場合、法違反と判断される可能性がある「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例を示した「手法の例示」で構成されているが、「講じなければならない措置」と「手法の例示」の対応関係、趣旨等をより明確なものとできないか。

３．上記２．の課題に対する対応の方向性（案）

⑴　情報通信技術の進展により個人情報取扱事業者等による個人データ等の取扱いの態様が多岐にわたっていることを踏まえた検討

ア　個人データ等の取扱いの態様が多岐にわたる個人情報取扱事業者等において講じなければならない組織体制、技術的な措置について、手法の例を明確にする。

イ　クラウドサービスでは、同サービス利用事業者からすると、個人データが記録された電子媒体それ自体は自ら管理しないこととなり、同サービス提供事業者からすると、同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があることとなる。以上の点を踏まえて、同サービスにおける個人データ等の取扱いに関して講じなければならない技術的な措置について、手法の例等を明確にする。

ウ　デバイスの高機能化により、生体認証や識別・認証手法を複数組み合わせる多要素認証の導入が比較的容易になっていることを踏まえて、これらの認証の手法の例を明確にする。

⑵　ゼロトラストアーキテクチャの考え方を取り込むことの検討

ゼロトラストアーキテクチャの考え方を取り入れた手法の例を明確にする。例えば、組織内・組織外のアクセスを問わず、アクセス要求ごとに、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こと等を手法の例として示すことが考えられる。

⑶　横展開対策を示すことの検討

横展開対策として講じなければならない技術的な措置について、手法の例等を明

[3] 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。

確にする。例えば、以下のような観点などが考えられる。

・　特権アカウントの利用等を最小限に限定すること。

・　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等、不正アクセス等が発生した場合でも被害が広がらないよう、必要な対策を講ずること。

⑷　「講じなければならない措置」と「手法の例示」の対応関係、趣旨等の明確化の検討

ア　以下の「講じなければならない措置」について、「手法の例示」の位置付けを整理し、再構成を検討する。

（ア）　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「手法の例示」は内容的に重複していると考えられるため、位置付けを整理し、再構成を検討する。

（イ）　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」ことなどが示されているが、「講じなければならない措置」の標題は「外部からの不正アクセス等の防止」であり、その内容は「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」とされている。現行のガイドライン（通則編）別添 10-6(3)の標題及びその内容から、前記の具体的な手法が考えられることを直ちに読み取れないため、同「手法の例示」等について位置付けを整理し、再構成を検討する。

イ　責任部署の設置、個人データの取扱いに係る規律の明確化と周知、安全管理措置の見直し、従業者の教育の実施方法等の見直し、その他の現行のガイドライン（通則編）別添の「講じなければならない措置」を実践するための手法の例として考えられるものの、「手法の例示」として示すことができていないものについて、当委員会が行政上の対応を行った個別の事案等を踏まえて、位置付けを整理し、追記を検討する。

ウ　「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における手法の例のうち、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はガイドライン（通則編）別添に記載を一本化する。

⑸　その他ガイドライン等について

なお、ガイドライン（通則編）別添の内容は、個人情報の保護に関する法律につ

いての事務対応ガイド（行政機関等向け）、特定個人情報の適正な取扱いに関するガイドライン（事業者編）、特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）、その他ガイドライン等で示される安全管理措置の内容と重複しているため、ガイドライン（通則編）別添の検討と合わせて、その他ガイドライン等で示される安全管理措置の内容も必要な見直しを検討する。

４．スケジュール（案）

令和８年９月頃	手法の例示の追加等の方向性の公表
令和８年 11 月頃	見直し案の委員会審議
令和８年 12 月頃	パブリックコメント開始
令和９年２月頃	パブリックコメントの結果を委員会で報告、改正事項の決定
令和９年４月	改正事項の施行

なお、上記改正事項の施行後も、情報通信技術の進展等を踏まえて、安全管理措置の手法の例示について不断の検討を行いたい。

以　上