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）「（別添１）特定個人情報に関する安全管理措置（事業者編）」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

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）（以下「マイナンバーガイドライン（事業者編）」という。）「（別添１）特定個人情報に関する安全管理措置（事業者編）」（以下「マイナンバーガイドライン（事業者編）別添１」という。）は、平成 26 年にマイナンバーガイドライン（事業者編）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、マイナンバーガイドライン（事業者編）別添１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番号利用事務等実施者による特定個人情報等の取扱いの態様は多岐にわたっている。また、近年、個人番号利用事務等実施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、特定個人情報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、個人番号利用事務等実施者においては、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、マイナンバーガイドライン（事業者編）別添１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「個人情報保護法」

---

[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

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、これに加えて、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「法」という。）第 12 条では、「個人番号利用事務実施者及び個人番号関係事務実施者（以下「個人番号利用事務等実施者」という。）は、個人番号の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために必要な措置を講じなければならない」と規定されている。

そして、マイナンバーガイドライン（事業者編）「第４－２－⑵　安全管理措置」では、法第 12 条又は個人情報保護法第 23 条の安全管理措置として「個人番号関係事務実施者又は個人番号利用事務実施者である事業者は、個人番号（生存する個人のものだけでなく死者のものも含む。）及び特定個人情報[4]（以下「特定個人情報等」という。）の漏えい、滅失又は毀損の防止その他の特定個人情報等の管理のために、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[5]。

マイナンバーガイドライン（事業者編）別添１は、上記の安全管理措置として、個人番号利用事務等実施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。マイナンバーガイドライン（事業者編）別添１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、マイナンバーガイドライン（事業者編）別添１では、「手法の例示」について「本例示は、これに限定する趣旨で記載したものではなく、事業者の規模及び特定個人情報等を取り扱う事務の特性等により、適切な手法を採用することが重要である」としている。

なお、中小規模事業者[6]については、事務で取り扱う個人番号の数量が少なく、ま

---

[4] 個人番号をその内容に含む個人情報

[5] 個人情報取扱事業者は、その取り扱う個人データについて安全管理措置を講ずる義務を負い（個人情報保護法第 23 条）、個人番号利用事務等実施者は、死者のものを含む個人番号について安全管理措置を講ずる義務を負う（法第 12 条）ため、個人データに該当する特定個人情報（個人番号をその内容に含む個人情報）については、個人情報取扱事業者兼個人番号利用事務等実施者は個人情報保護法第 23 条及び法第 12 条の安全管理措置を講ずる義務を負い、個人データに該当しない個人番号については、個人番号利用事務等実施者が法第 12 条の安全管理措置を講ずる義務を負うことになる。

[6] 「中小規模事業者」とは、事業者のうち従業員の数が 100 人以下の事業者をいう。ただし、次に掲げる事業者を除く。

・個人番号利用事務実施者

・委託に基づいて個人番号関係事務又は個人番号利用事務を業務として行う事業者

・金融分野（個人情報保護委員会・金融庁作成の「金融分野における個人情報保護に関するガイドライン」第１条第１項に定義される金融分野）の事業者

・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 を超える事業者

た、特定個人情報等を取り扱う従業者が限定的であること等から、特例的な対応方法として、「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、マイナンバーガイドライン（事業者編）別添１は、2－Ａ基本方針の策定、2－Ｂ取扱規程等の策定、2－Ｃ組織的安全管理措置、2－Ｄ人的安全管理措置、2－Ｅ物理的安全管理措置、2－Ｆ技術的安全管理措置及び2－Ｇ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２－３－２）

更新内容（案）について、マイナンバーガイドライン（事業者編）別添１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２－３－２である。

マイナンバーガイドライン（事業者編）別添１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、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。）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）の一部について、マイナンバーガイドライン（事業者編）別添１に追記する。当該追記による更新は、資料２－３－２において、青字で記載している。

(2)　更新理由

ガイドライン（通則編）別添は、個人情報保護法第 23 条の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として、「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。そして、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。ガイドライン（通則編）別添については、

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ている。

上記のとおりガイドライン（通則編）別添及びマイナンバーガイドライン（事業者編）別添１の構成、並びに、現行のガイドライン（通則編）別添及びマイナンバーガイドライン（事業者編）別添１で示している「講じなければならない措置」及び「手法の例示」の内容は共通している。

そこで、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は、マイナンバーガイドライン（事業者編）別添１にも追記することが適切であると判断した。

２　取扱規程等の策定について

(1)　2－Ｂ取扱規程等の策定の「手法の例示」について

ア　更新内容

マイナンバーガイドライン（事業者編）別添１2－Ｂ取扱規程等の策定の「手法の例示」として、源泉徴収票等を作成する事務においては「従業員等から提出された書類等の複製等を作成している場合に当該複製等の廃棄・削除方法」について手続を明確にしておくことが重要であることを追記する。

イ　更新理由

源泉徴収票等を作成する事務については、現行のマイナンバーガイドライン（事業者編）別添１2－Ｂ取扱規程等の策定の「手法の例示」で示される事務フローだけでなく、従業員等から提出された書類等を複製等することが考えられ、そして、当該複製等の廃棄・削除が適切に行われていないことが、漏えい等事案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　組織的安全管理措置について

(1)　2－Ｃ－ａ組織体制の整備の「手法の例示」について

ア　更新内容

①　マイナンバーガイドライン（事業者編）別添１2－Ｃ－ａ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「事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合」及び「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　現行のマイナンバーガイドライン（事業者編）別添１2－Ｃ－ａ組織体

制の整備の「手法の例示」では、「事務におけ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、個人番号利用事務等実施者においては、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、複数の部署で特定個人情報等を取り扱う等、特定個人情報等の取扱いが多岐にわたることが考えられ、このような場合に、責任者が各部署における特定個人情報等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、現行のマイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｃ－ａ組織体制の整備の「手法の例示」として示されている「特定個人情報等を複数の部署で取り扱う場合の各部署の任務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 法や個人番号利用事務等実施者において整備されている特定個人情報等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特定個人情報等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) $\boxed{2}$－Ｃ－ｂ取扱規程等に基づく運用及び同ｃ取扱状況を確認する手段の整備について

ア 更新内容

① 現行のマイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｃ－ｂ取扱規程等に基づく運用及び同ｃ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、同$\boxed{2}$－Ｃ－ｂ取扱規程等に基づく運用の「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[7]。

② マイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｃ－ｂ取扱規程等に基づく運用の「手法の例示」として「取扱規程等を明確化し、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、取扱規程等に基づく運用を確保するために「取扱規程等に従って特定個人情報等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、特

[7] これにより現行のマイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｃ－ｄが同ｃに、同$\boxed{2}$－Ｃ－ｅが同ｄとなる。

定個人情報等の取扱状況等の記録を「取扱規程等と照らし合わせること」を追記する。

イ　更新理由

①　現行のマイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｃ－ｂ取扱規程等に基づく運用では、取扱規程等に基づく運用を確保するために講じなければならない措置として、特定個人情報等の利用状況等を記録することを示し、手法の例として記録する具体的な項目を示している。くわえて、同$\boxed{2}$－Ｃ－ｃ取扱状況を確認する手段の整備では、手法の例として、取扱状況を確認するための記録等におい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、現行のマイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｃ－ｂ及び同ｃはいずれも、特定個人情報等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。そして、特定個人情報等の取扱状況等の記録等の取扱状況を確認する手段を整備し実際に確認することで、取扱規程等に基づく運用が確保されることからすれば、取扱状況を確認する手段の整備は、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　取扱規程等を明確化し、従業者に周知することが適切に行われていないことで、取扱規程等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。取扱規程等を明確化し、従業者に周知することについては、現行のマイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｃ－ｂ取扱規程等に基づく運用を確保するための具体的な手法の一つと考えられるが、同「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、マイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｄ人的安全管理措置では、同「ｂ　事務取扱担当者の教育」において、事務取扱担当者に、特定個人情報等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、取扱規程等を従業者に周知する点については、同「ｂ　事務取扱担当者の教育」を講ずる過程で実現されるとも考えられる。しかし、取扱規程等を従業者に周知するには、当該取扱規程等を、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、同「ｂ　事務取扱担当者の教育」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、同「ｂ　事務取扱担当者の教育」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い。

③　あらかじめ整備された取扱規程等に従って特定個人情報等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取扱規程等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)　2－Ｃ－ｄ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

マイナンバーガイドライン（事業者編）別添１2－Ｃ－ｄ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、「特定個人情報等の取扱状況、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が考えられる」ことを追記する。

イ　更新理由

特定個人情報等の取扱状況、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、現行のマイナンバーガイドライン（事業者編）別添１2－Ｃ－ｅ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「特定個人情報等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む」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。

４　人的安全管理措置について

(1)　2－Ｄ－ｂ事務取扱担当者の教育の「手法の例示」について

ア　更新内容

マイナンバーガイドライン（事業者編）別添１2－Ｄ－ｂ事務取扱担当者の教育の「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。

５　物理的安全管理措置について

(1)　2－Ｅ－ｄ個人番号の削除、機器及び電子媒体等の廃棄の「手法の例示」について

ア　更新内容

マイナンバーガイドライン（事業者編）別添１2－Ｅ－ｄ個人番号の削除、機器及び電子媒体等の廃棄の「手法の例示」における、特定個人情報等が記録された機器、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

特定個人情報等を削除する手法として、特定個人情報等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、特定個人情報等を利用不能にする論理的削除方法（暗号化消去）[8]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、追記する必要があると判断したため。

６　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「特定個人情報等を取り扱う情報システム」に統一する。

イ　更新理由

現行のマイナンバーガイドライン（事業者編）別添１2－Ｆ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「特定個人情報ファイル」、「特定個人情報ファイルを取り扱うことのできる情報システム端末等」、「情報システム」という用語が混在しているが、特定個人情報等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)　2－Ｆ－ａアクセス制御の「手法の例示」について

ア　更新内容

①　マイナンバーガイドライン（事業者編）別添１2－Ｆ－ａ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。

---

[8] 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

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、個人番号利用事務等実施者においては、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　現行のマイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｆ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)　$\boxed{2}$－Ｆ－ｂ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　マイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｆ－ｂ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「特定個人情報等を取り扱う情報システムを使用する者」とする。

②　マイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｆ－ｂ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、重要な特定個人情報等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、「事務取扱担当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　現行のマイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｆ－ｂ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、「事務取扱担当者」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特定個人情報等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、特定個人情報等を取り扱う情報システムにアクセスする者は事務取扱担当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、重要な特定個人情報等へのアクセス」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、特定個人情報等を取り扱う情報システムにアクセスする者は事務取扱担当者に限られず、顧客等がアクセスする場合も考えられ、事務取扱担当者が情報システムにアクセスする場合と同様に、事務取扱担当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)　2－Ｆ－ｃ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

マイナンバーガイドライン（事業者編）別添１2－Ｆ－ｃ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特定個人情報等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)　2－Ｆ－ｅ不正アクセス等の検知等について

ア　更新内容

①　マイナンバーガイドライン（事業者編）別添１2－Ｆ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「ｅ　不正アクセス等の検知等」を追記する。

②　マイナンバーガイドライン（事業者編）別添１2－Ｆ－ｅ不正アクセス等の検知等の「手法の例示」として、特定個人情報等を取り扱う情報システムの使用状況、特定個人情報等へのアクセス状況、特定個人情報等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特定個人情報等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、Ｆ技術的安全管理措置ａからｄの手法の例示も参照されたい」

ことを追記する。

⑤　マイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｆ－ｅ不正アクセス等の検知等の「中小規模事業者における対応方法」として「特定個人情報等を取り扱う情報システムの使用状況、特定個人情報等へのアクセス状況、特定個人情報等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　現行のマイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｆ－ｃ外部からの不正アクセス等の防止の「手法の例示」では、「ログ等の分析を定期的に行い、不正アクセス等を検知する」ことが示されている。しかし、現行のマイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｆの「ｃ　外部からの不正アクセス等の防止」という標題や、「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、適切に運用する」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、現行のマイナンバーガイドライン（事業者編）別添１において示されている前記「手法の例示」を、現行のマイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｆ－ｃ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、現行のマイナンバーガイドライン（事業者編）別添１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が手法の

例として示されているところ、かかる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、個人番号利用事務等実施者においては、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じ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、マイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｆ－ｅ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、マイナンバーガイドライン（事業者編）別添１$\boxed{2}$－Ｆ－ａからｄ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するため、中小規模事業者における特例的な対応方法として、「特定個人情報等を取り扱う情報システムの使用状況、特定個人情報等へのアクセス状況、特定個人情報等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