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）「（別添１）特定個人情報に関する安全管理措置（行政機関等編）」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（行政機関等編）（以下「マイナンバーガイドライン（行政機関等編）」という。）「（別添１）特定個人情報に関する安全管理措置（行政機関等編）」（以下「マイナンバーガイドライン（行政機関等編）別添１」という。）は、平成 26 年にマイナンバーガイドライン（行政機関等編）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（行政機関等編）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行政機関等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、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、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、行政機関等においては、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（行政機関等編）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 66 条第１項では、「行政機関の長等は、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報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[4]。

そして、マイナンバーガイドライン（行政機関等編）「第４－２－⑵　安全管理措置」では、「行政機関等は、安全管理措置の検討に当たり、番号法及び個人情報保護法並びに本ガイドライン（「（別添１）特定個人情報に関する安全管理措置（行政機関等編）」を含む。）、個人情報保護法ガイドライン（行政機関等編）及び事務対応ガイドを遵守することを前提とする」と規定されている。

マイナンバーガイドライン（行政機関等編）別添１は、上記の安全管理措置として、行政機関等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（行政機関等編）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（行政機関等編）別添１では、「手法の例示」について「手法の例示は、これに限定する趣旨で記載したものではなく、また、個別ケースによって別途考慮すべき要素があり得るので注意を要する」としている。

以上を前提に、マイナンバーガイドライン（行政機関等編）別添１は、2－Ａ基本方針の策定、2－Ｂ取扱規程等の見直し等、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２-４-２）

更新内容（案）について、マイナンバーガイドライン（行政機関等編）別添１

[4] 行政機関の長等は、保有個人情報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 66 条第１項）、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、保有個人情報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、個人情報保護法第 66 条第１項及び法第 12 条の安全管理措置を講ずる義務が生じ、保有個人情報に該当しない個人番号については、法第 12 条の安全管理措置を講ずる義務が生じることになる。

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２－４－２である。

マイナンバーガイドライン（行政機関等編）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２－４－３、下線部）の一部について、マイナンバーガイドライン（行政機関等編）別添１に追記する。当該追記による更新は、資料２－４－２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２－４－３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（行政機関等編）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（行政機関等編）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（行政機関等編）別添１にも追記することが適切であると判断した。

2　取扱規程等の見直し等について

(1)　2－Ｂ取扱規程等の見直し等の「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（行政機関等編）別添１2－Ｂ取扱規程等の見直し等の「手法の例示」として、「特定個人情報等を含む書類等の複製等を作成している場合には、当該複製等を削除・廃棄する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

行政機関等における特定個人情報等を取り扱う事務においては、特定個人情報等を含む書類等を複製等することが考えられ、そして、当該複製等の削除・廃棄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－ｂ取扱規程等に基づく運用について

ア　更新内容

①　マイナンバーガイドライン（行政機関等編）別添１2－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。

②　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、保護責任者等が確認する」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。

③　同「手法の例示」として、特定個人情報等の取扱状況を把握可能とするため、特定個人情報等の取扱いに係る記録等において、あらかじめ明確化しておくべき内容を追記する。

イ　更新理由

①　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（行政機関等編）別添１2－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。

②　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、保護責任者等の責任を有する者や部署が、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　現行のマイナンバーガイドライン（行政機関等編）別添１$\boxed{2}$－Ｃ－ｂ取扱規程等に基づく運用の「手法の例示」では、特定個人情報等の利用状況等の記録として考えられる具体的な項目を示している。特定個人情報等の取扱状況等の記録においては、当該項目に加えて、現行のマイナンバーガイドライン（行政機関等編）別添１$\boxed{2}$－Ｃ－ｃ取扱状況を確認する手段の整備において「講じなければならない措置」として示している、特定個人情報ファイルの取扱状況を確認するために記録する項目についても、同様に記録をし、当該記録をもって特定個人情報等の取扱状況を把握することが重要であると考えられるため。なお、マイナンバーガイドライン（行政機関等編）別添１$\boxed{2}$－Ｃ－ｃ取扱状況を確認する手段の整備は、特定個人情報ファイルの取扱状況を確認する手段の整備について、「講じなければならない措置」を示すものであるが、マイナンバーガイドライン（行政機関等編）別添１$\boxed{2}$－Ｃ－ｂ取扱規程等に基づく運用は、特定個人情報等の取扱規程等に基づく運用の確保、特定個人情報等の取扱状況等の記録・保存・分析等について「講じなければならない措置」及び「手法の例示」を示すものである。

４　人的安全管理措置について

(1)　$\boxed{2}$－Ｄ－ｂ事務取扱担当者等の教育の「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（行政機関等編）別添１$\boxed{2}$－Ｄ－ｂ事務取扱担当者等の教育の「講じなければならない措置」として、特定個人情報等の適正な取扱い等に関する研修について、「おおむね一年ごと」に実施することを追記する。

イ　更新理由

現行のマイナンバーガイドライン（行政機関等編）別添１$\boxed{2}$－Ｄ－ｂ事務取扱担当者等の教育の「講じなければならない措置」では、特定個人情報ファイルを取り扱う事務に従事する者に対するサイバーセキュリティの研修について、おおむね一年ごとに実施することが示されているが、その他特定個人情報等の適正な取扱い等に関する研修についても、おおむね一年ごとに実施することが適切であると考えられるため。なお、これらの研修についておおむね一年ごとの実施が適切であることは、現行のマイナンバーガイドラ

イン（行政機関等編）別添１$\boxed{2}$－Ｄ－ｂ事務取扱担当者等の教育の「講じなければならない措置」で示される「必要な教育研修」に含まれているが、この点を明確化するものである。

５　物理的安全管理措置について

(1)　$\boxed{2}$－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（行政機関等編）別添１$\boxed{2}$－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）[5]を採用することが考えられ、さらに、当該方法は行政機関等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。

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（行政機関等編）別添１$\boxed{2}$－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)　$\boxed{2}$－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（行政機関等編）別添１$\boxed{2}$－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

[5] 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

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（行政機関等編）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、全ての行政機関等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行政機関等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（行政機関等編）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（行政機関等編）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に「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。

イ 更新理由

① 現行のマイナンバーガイドライン（行政機関等編）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、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行政機関等が、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行政機関等が、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。

(4) $\boxed{2}$－Ｆ－ｃ不正アクセス等による被害の防止等の「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（行政機関等編）別添１$\boxed{2}$－Ｆ－ｃ不正アクセス等による被害の防止等の「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、全ての行政機関等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行政機関等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)　$\boxed{2}$－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（行政機関等編）別添１$\boxed{2}$－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（行政機関等編）別添１$\boxed{2}$－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「不正アクセス等の被害に遭った場合であっても、特定個人情報等を取り扱う情報システムの被害を最小化する仕組み（ネットワークの遮断、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）を導入し、適切に運用する。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。

イ　更新理由

①　現行のマイナンバーガイドライン（行政機関等編）別添１$\boxed{2}$－Ｆ－ｃ不正アクセス等による被害の防止等の「手法の例示」では、「定期に及び必要に応じ随時にログ等の分析を行い、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（行政機関等編）別添１$\boxed{2}$－Ｆの「ｃ　不正アクセス等による被害の防止等」という標題や、

「情報システムを外部等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等を導入し、適切に運用する」等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（行政機関等編）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（行政機関等編）別添１$\boxed{2}$－Ｆ－ｃ不正アクセス等による被害の防止等より適切な、「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た。そこで、現時点で、全ての行政機関等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行政機関等が更に増加することを見据えながら、現時点で行政機関等に「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（行政機関等編）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、不正アクセスを受けた行政機関等においては、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を導入することが考えられるため。

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、行政機関等においては、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（行政機関等編）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（行政機関等編）別添１$\boxed{2}$－Ｆ－ａからｅ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。

以　上