令和６年４月１日
個人情報保護委員会事務局

「特定個人情報保護評価の実施手順」の更新

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）第 27 条第２項の規定に基づく特定個人情報保護評価指針（平成 26 年特定個人情報保護委員会告示第４号）の３年ごとの再検討による特定個人情報保護評価に関する規則（平成 26 年特定個人情報保護委員会規則第１号）及び特定個人情報保護評価指針の改正に伴い、特定個人情報保護評価の実施手順を更新しました。

主な更新箇所は、下記のとおりです。

記

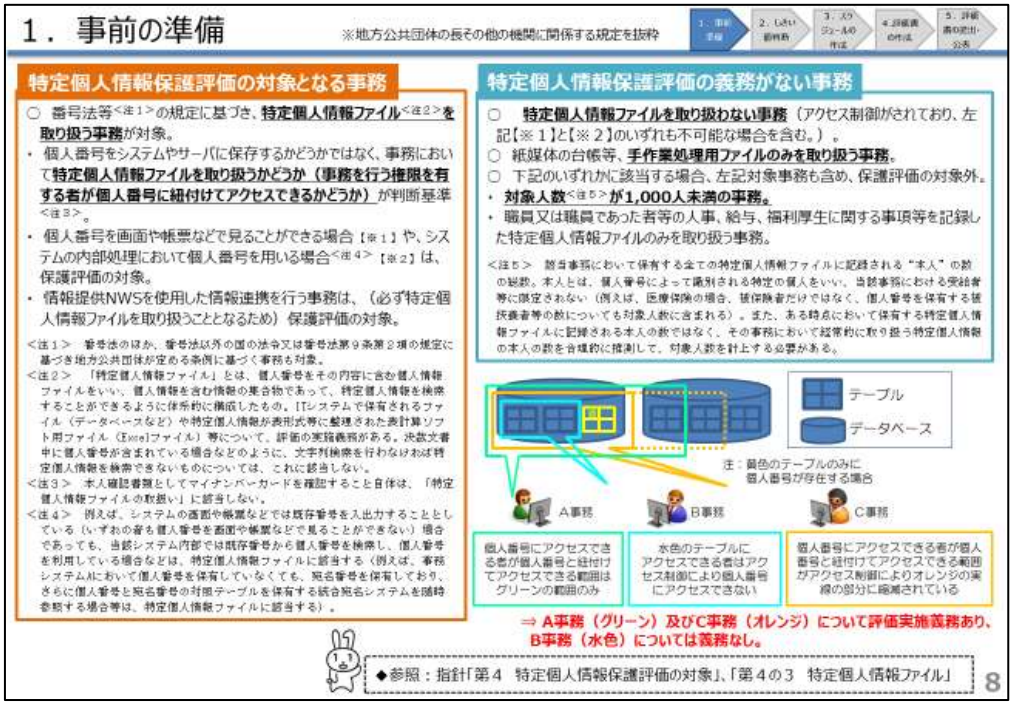
特定個人情報保護評価の実施手順の主な更新箇所		
p. 8	新規	１．事前の準備 特定個人情報保護評価の対象となる事務 （特定個人情報保護評価の義務がない事務）
p. 13	新規	３．スケジュールの作成 実施時期の特例（緊急時の事後評価）
p. 16	修正	４．（１）①基礎項目評価書 ①基礎項目評価書
―	削除	４．（１）①基礎項目評価書 マイナンバーガイドラインの参照箇所
pp. 17-20	新規	４．（１）①基礎項目評価書 「Ⅳ　リスク対策」において「２）十分である」を選択できる水準
p. 21	新規	４．（１）①基礎項目評価書 「Ⅳ　リスク対策」における措置状況の評価に係る判断の根拠
p. 22	修正	４．（１）②重点項目評価書 ②重点項目評価書
―	削除	４．（１）②重点項目評価書 マイナンバーガイドラインの参照箇所

p. 23	修正	４．（１）③全項目評価書 ③全項目評価書
―	削除	４．（１）③全項目評価書 マイナンバーガイドラインの参照箇所
p. 24	修正	４．（１）③全項目評価書 マイナンバーガイドラインを踏まえたリスク対策の記載例

新規 【p. 8】 1．事前の準備

特定個人情報保護評価の対象となる事務

（特定個人情報保護評価の義務がない事務）



新規 【p. 13】 3．スケジュールの作成

実施時期の特例（緊急時の事後評価）

修正 【p.16】４．（１）①基礎項目評価書

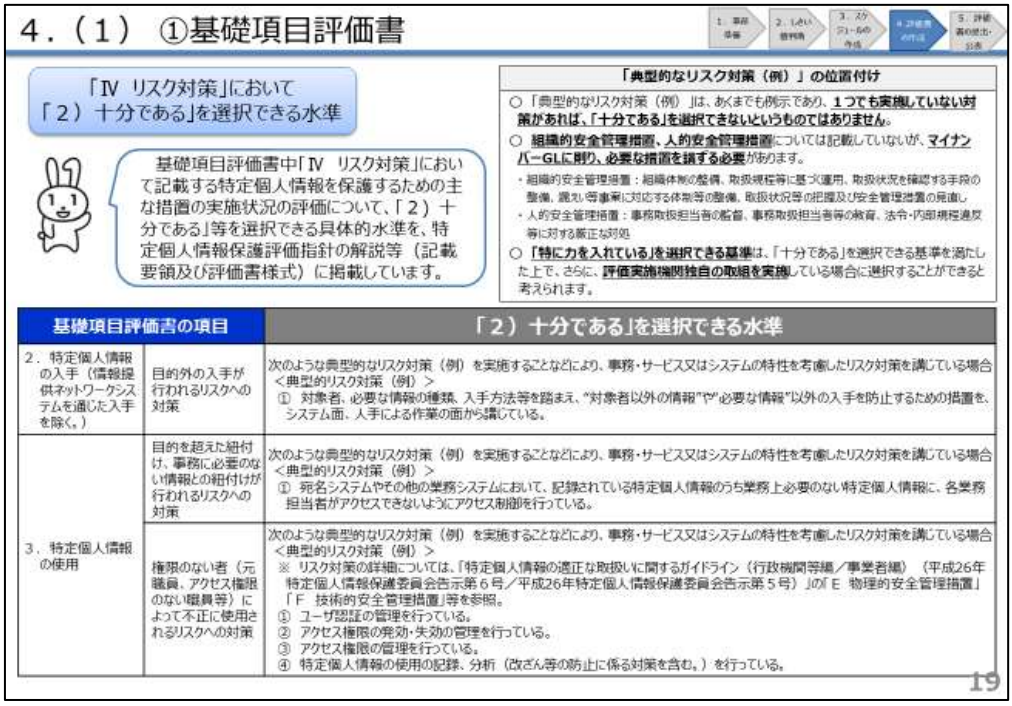
①基礎項目評価書

削除 【－】４．（１）①基礎項目評価書

マイナンバーガイドラインの参照箇所

新規 【pp. 17-20】 ４．（１）①基礎項目評価書

「Ⅳ　リスク対策」において「２）十分である」を選択できる水準



４．（１） ①基礎項目評価書

「Ⅳ リスク対策」において「２）十分である」を選択できる水準

基礎項目評価書中「Ⅳ リスク対策」において記載する特定個人情報を保護するための主な措置の実施状況の評価について、「２）十分である」等を選択できる具体的水準を、特定個人情報保護評価指針の解説等（記載要領及び評価書様式）に掲載しています。

「典型的なリスク対策（例）」の位置付け

- 「典型的なリスク対策（例）」は、あくまでも例示であり、**１つでも実施していない対策があれば、「十分である」を選択できないというものではありません。**
- **組織的安全管理措置、人的安全管理措置**については記載していないが、**マイナンバーGLに則り、必要な措置を講ずる必要**があります。
  - 組織的安全管理措置：組織体制の整備、取扱規程等に基づく運用、取扱状況を確認する手段の整備、漏えい等事案に対応する体制等の整備、取扱状況等の把握及び安全管理措置の見直し
  - 人的安全管理措置：事務取扱担当者の監督、事務取扱担当者等の教育、法令・内部規程違反等に対する厳正な対処
- **「特に力を入れている」を選択できる基準**は、「十分である」を選択できる基準を満たした上で、さらに、**評価実施機関独自の取組を実施**している場合に選択することができると考えられます。

基礎項目評価書の項目		「２）十分である」を選択できる水準
２．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	目的外の入手が行われるリスクへの対策	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 <典型的リスク対策（例）> ① 対象者、必要な情報の種類、入手方法等を踏まえ、"対象者以外の情報"や"必要な情報"以外の入手を防止するための措置を、システム面、人手による作業の面から講じている。
３．特定個人情報の使用	目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスクへの対策	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 <典型的リスク対策（例）> ① 宛名システムやその他の業務システムにおいて、記録されている特定個人情報のうち業務上必要のない特定個人情報に、各業務担当者がアクセスできないようにアクセス制御を行っている。
	権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスクへの対策	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 <典型的リスク対策（例）> ※ リスク対策の詳細については、「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／事業者編）（平成26年特定個人情報保護委員会告示第６号／平成26年特定個人情報保護委員会告示第５号）」の「Ｅ 物理的安全管理措置」「Ｆ 技術的安全管理措置」等を参照。 ① ユーザ認証の管理を行っている。 ② アクセス権限の発効・失効の管理を行っている。 ③ アクセス権限の管理を行っている。 ④ 特定個人情報の使用の記録、分析（改ざん等の防止に係る対策を含む。）を行っている。

19

４．（１） ①基礎項目評価書

基礎項目評価書の項目		「２）十分である」を選択できる水準
４．特定個人情報ファイルの取扱いの委託	委託先における不正な使用等のリスクへの対策	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 <典型的リスク対策（例）> ※ リスク対策の詳細については、「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／事業者編）（平成26年特定個人情報保護委員会告示第６号／平成26年特定個人情報保護委員会告示第５号）」の「第４－２－（１）委託の取扱い」等を参照。 ① 委託先における情報保護管理体制の確認を行っている。 ② 委託先における特定個人情報ファイルの閲覧者・更新者を制限している。 ③ 委託先における特定個人情報ファイルの取扱いの記録を行っている。 ④ 委託先から他者への又は委託元から委託先への特定個人情報の提供に関するルールを定めている。 ⑤ 委託先における特定個人情報の消去に関するルールを定めている。 ⑥ 委託契約において、特定個人情報ファイルの取扱いに関する規定を設けている。 ⑦ 再委託が行われる場合、再委託先による特定個人情報ファイルの適切な取扱いを確保するための措置を講じている。
５．特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）	不正な提供・移転が行われるリスクへの対策	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 <典型的リスク対策（例）> ※ リスク対策の詳細については、「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／事業者編）（平成26年特定個人情報保護委員会告示第６号／平成26年特定個人情報保護委員会告示第５号）」の「Ｅ 物理的安全管理措置」「Ｆ 技術的安全管理措置」を参照。 ① 特定個人情報の提供・移転に関するルールが定められている。 ② 特定個人情報の提供・移転の記録し、その記録を一定期間保存している。 ③ 当該記録を定期に及び随時に分析等するための体制を整備している。 ④ 当該記録について、改ざん、窃取又は不正な削除の防止のために必要な措置を講じている。
６．情報提供ネットワークシステムとの接続	目的外の入手が行われるリスクへの対策	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 <典型的リスク対策（例）> ① 自庁システム側において、必要最低限の人数、参照範囲となるよう、職員のアクセス権限を設定している。 ② アクセス権限の所有者は、ＩＤ、パスワード等を適切に管理するとともに、離席時のログアウトを徹底する。

◆参照：指針の解説「第９の２（１）基礎項目評価書」

20

4．（1） ①基礎項目評価書

基礎項目評価書の項目		「2）十分である」を選択できる水準
6．情報提供ネットワークシステムとの接続	不正な提供が行われるリスクへの対策	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞ ① 自庁システムの副本登録画面について、必要最低限の人数、情報の範囲となるよう、職員のアクセス権限を設定する。 ② アクセス権限の所有者は、ＩＤ、パスワード等を適切に管理するとともに、離席時のログアウトを徹底する。 ③ 副本登録を自動連携により行う場合は、サーバーにアクセス権限等を付与する。 ④ 住民基本台帳事務における支援措置対象者等については自動応答不可フラグを設定する等、必要な対応を行う。 ⑤「マイナンバー利用事務におけるマイナンバー登録事務に係るガイドライン」（令和５年12月18日デジタル庁）の次の留意事項等を遵守している。 （例） ・ 住基ネット照会によりマイナンバーを取得するのではなく、申請者からマイナンバーの提供を受け、その上で記載されたマイナンバーの真正性確認を行うこと。 ・ 申請者からマイナンバーが得られない場合にのみ行う住基ネット照会は、４情報又は住所を含む３情報による照会を原則とすること。 ・ 複数人での確認や上長による最終確認を行った上でマイナンバーの紐付けを行い、その記録を残すこと。 ・ 更新時には、本人からマイナンバーを取得し、登録されているマイナンバーに誤りがないか、確認すること。
7．特定個人情報の保管・消去	特定個人情報の漏えい・滅失・毀損リスクへの対策	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞ ※ リスク対策の詳細については、「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／事業者編）（平成26年特定個人情報保護委員会告示第６号／平成26年特定個人情報保護委員会告示第５号）」の（別添１）２「C 組織的安全管理措置」、「E 物理的安全管理措置」、「F 技術的安全管理措置」を参照。 ① 内閣サイバーセキュリティセンター（NISC）による政府機関等のサイバーセキュリティ対策のための統一基準群（「政府機関等のサイバーセキュリティ対策のための統一基準」中「第３部 情報の取扱い」、「第５部 情報システムのライフサイクル」、「第６部 情報システムの構成要素」、「第７部 情報システムのセキュリティ要件」、「第８部 情報システムの利用」等）及びそれに基づく各府省庁ポリシーを遵守している。（評価実施機関が政府機関の場合のみ） ② 地方公共団体においては、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等を参考に地方公共団体において策定した情報セキュリティポリシー等（第３編第２章中「２．情報資産の分類と管理」、「３．情報システム全体の強靭性の向上」、「４．物理的セキュリティ」、「６．技術的セキュリティ」等）を遵守している。 ③ 漏えい・滅失・毀損を防ぐために、物理的安全管理措置や技術的安全管理措置を実施している。 ④ 特定個人情報ファイルの滅失・毀損が発生した場合に復旧できるよう、バックアップを保管している。 ⑤ 過去の漏えい等事案を踏まえた、再発防止策を実施している。

◆参照：指針の解説「第９の２（１）基礎項目評価書」

19

4．（1） ①基礎項目評価書

基礎項目評価書の項目		「2）十分である」を選択できる水準
8．人手を介在させる作業	人為的ミスが発生するリスクへの対策は十分か	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞ ①「マイナンバー利用事務におけるマイナンバー登録事務に係るガイドライン」（令和５年12月18日デジタル庁）の次の留意事項等を遵守している。 （例） ・ 住基ネット照会によりマイナンバーを取得するのではなく、申請者からマイナンバーの提供を受け、その上で記載されたマイナンバーの真正性確認を行うこと。 ・ 申請者からマイナンバーが得られない場合にのみ行う住基ネット照会は、４情報又は住所を含む３情報による照会を原則とすること。 ・ 複数人での確認や上長による最終確認を行った上でマイナンバーの紐付けを行い、その記録を残すこと。 ・ 更新時には、本人から情報をマイナンバーを取得し、登録されているマイナンバーに誤りがないか、確認すること。 ② 特定個人情報の入手から保管・廃棄までの九セスで、人手が介在する局面ごとに人為的ミスが発生するリスクへの対策を講じている。 ※ 人為的ミス発生防止の着眼点等として、次の資料が参考となる（いずれも個人情報保護委員会ウェブページ公表資料：https://www.ppc.go.jp/legal/kensyuushiryou/）。 ・「特定個人情報を取り扱う際の注意ポイント」 ・「特定個人情報の漏えい等の防止について－地方公共団体における単純な事務ミスを防止するための着眼点－」
10．従業者に対する教育・啓発	従業者に対する教育・啓発	次のような典型的なリスク対策（例）を実施することなどにより、事務・サービス又はシステムの特性を考慮したリスク対策を講じている場合 ＜典型的リスク対策（例）＞ ※ リスク対策の詳細については、「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／事業者編）（平成26年特定個人情報保護委員会告示第６号／平成26年特定個人情報保護委員会告示第５号）」の「D 人的安全管理措置」を参照。 ① 研修計画を策定している。 ② 事務取扱者の適切な監督を行っている。 ③ 次の事務取扱者等への教育研修を行っている。 ・ 事務取扱者への研修 ・ 特定個人情報を取り扱う情報システムの管理に関する事務に従事する職員への研修 ・ 保護責任者への研修 ・ 事務取扱者へのサイバーセキュリティ研修（おおむね１年ごと）。 ※ 未受講者には、再受講の機会を付与する等の必要な措置を講じること。

◆参照：指針の解説「第９の２（１）基礎項目評価書」

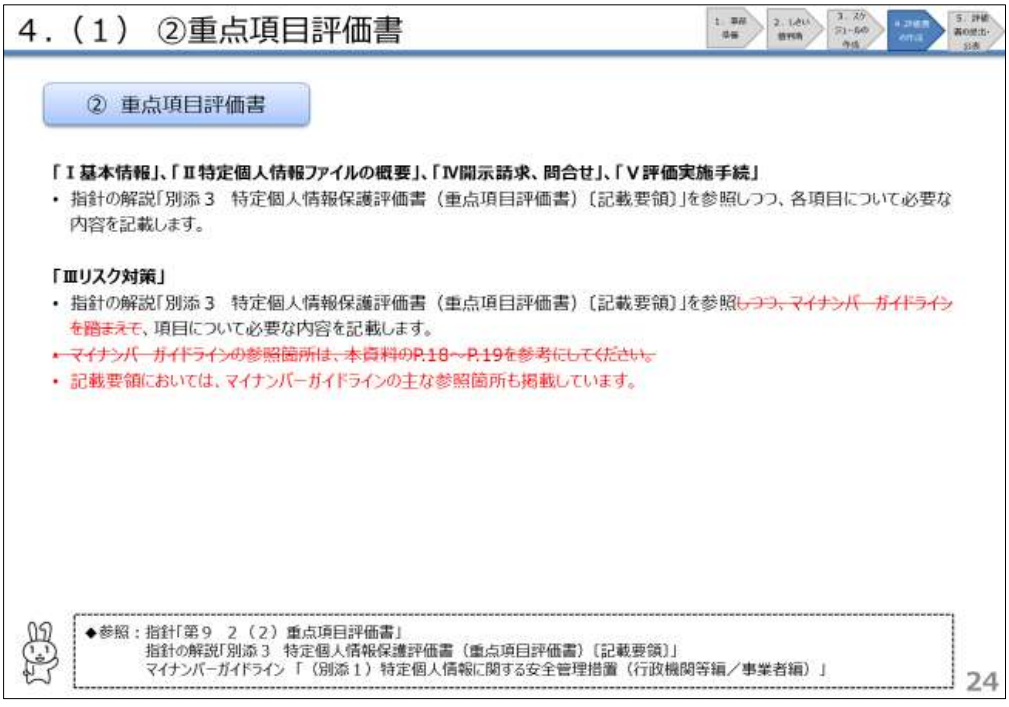
22

新規 【p. 21】４．（１）①基礎項目評価書

「Ⅳ　リスク対策」における措置状況の評価に係る判断の根拠

修正 【p. 22】４．（１）②重点項目評価書

②重点項目評価書

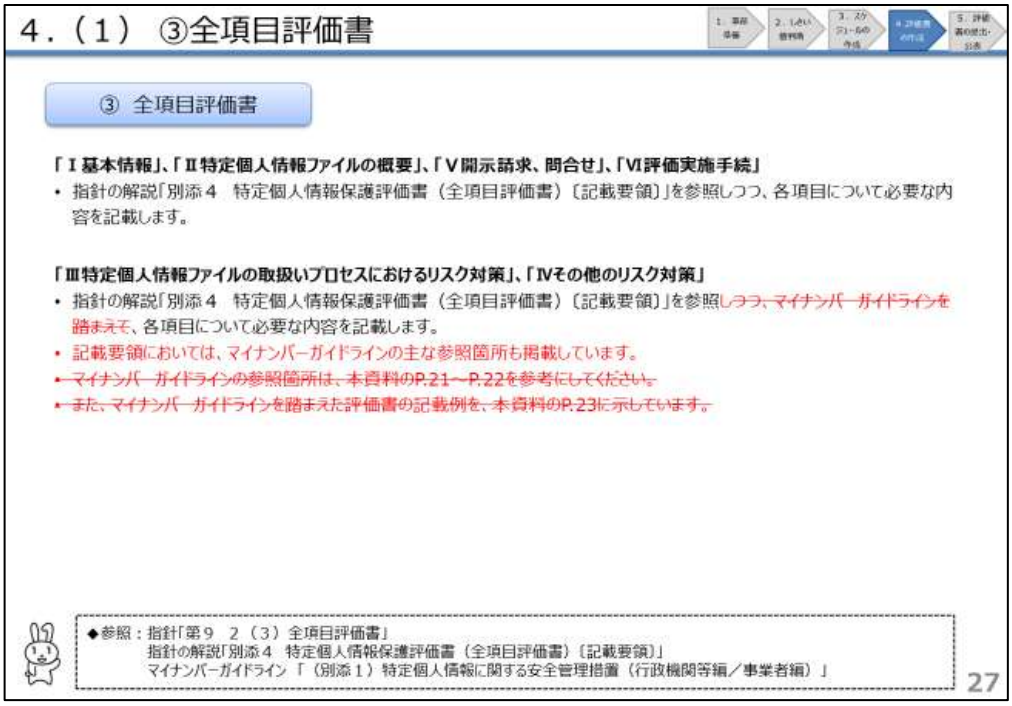


削除 【ー】４．（１）②重点項目評価書

マイナンバーガイドラインの参照箇所


修正 【p. 23】４．（１）③全項目評価書

③全項目評価書



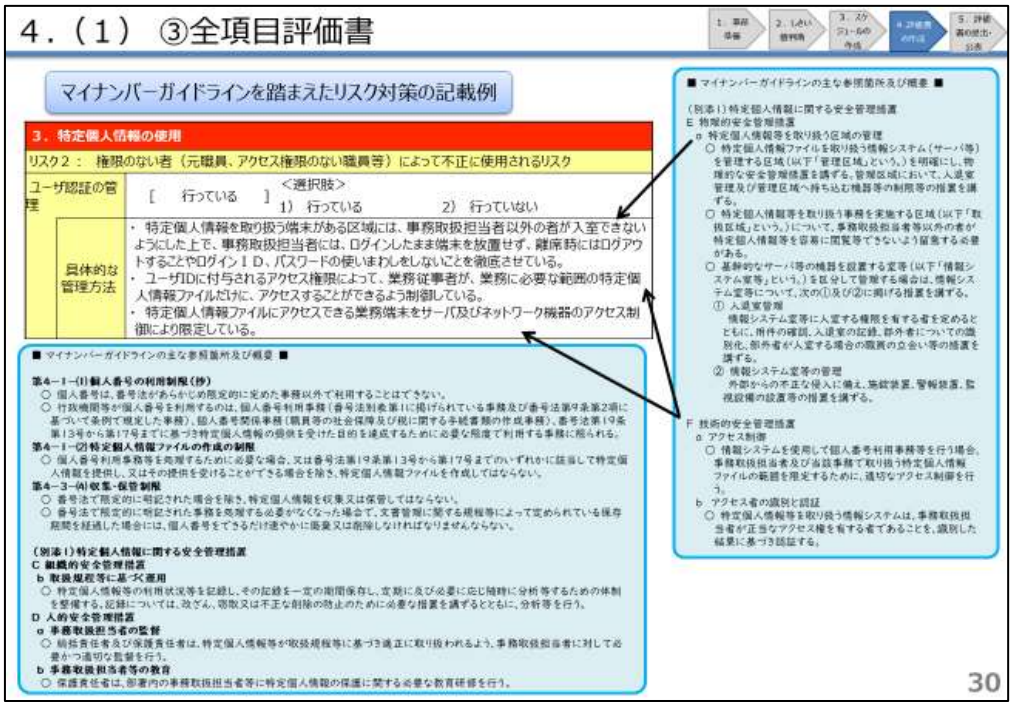
削除 【ー】４．（１）③全項目評価書

マイナンバーガイドラインの参照箇所


修正 【p. 24】４．（１）③全項目評価書

マイナンバーガイドラインを踏まえたリスク対策の記載例

⇒ マイナンバーガイドラインの参照箇所を記載要領に掲載することとなったことに伴い、記載要領に合わせる修正を行いました。



以　上