

安全管理措置の比較

	個人情報	匿名加工情報等			マイナンバー関連	PIA関連	
	個人情報	匿名加工情報の加工方法等情報	匿名加工情報	非識別加工情報等	匿名加工医療情報	特定個人情報等	評価書と安全管理措置の対応
法令	個情法20条	個情法36条2項、規則20条	個情法36条6項、39条	行政機関個人情報保護法・独立行政法人等個人情報保護法44条の15第1項・行政機関非識別加工情報規則14条、独立行政法人等非識別加工情報規則14条	次世代医療基盤法8条3項3・4号、施行規則6条	番号法12条、個情法20条	番号法28条、以下全項目評価書の該当箇所の列記
対象	個人データ	匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号並びに加工の方法に関する情報	努力義務、匿名加工情報	行政機関非識別加工情報、行政機関非識別加工情報の作成に用いた保有個人情報から削除した記述等及び個人識別符号並びに加工の方法に関する情報	医療情報等及び匿名加工医療情報	個人番号、個人データ	特定個人情報等が対象だが、個人情報やパーソナルデータも対象にできる
該当情報であることの明示	△ (法令・ガイドラインでは明記されていないが望ましい)	△ (法令・ガイドラインでは明記されていないが望ましい)	○ (ガイドライン18頁)	△ (法令・ガイドラインでは明記されていないが望ましい)	△ (大臣認定事業者での安全管理措置であり自明ともいえるが、他の事業も実施している場合は、法令・ガイドラインでは明記されていないが望ましい)	△ (法令・ガイドラインでは明記されていないが望ましい)	—
事務・情報・人の明確化	△ (法令・ガイドラインでは明記されていないが望ましい)	△ (法令・ガイドラインでは明記されていないが望ましい)	—	—	○(ガイドラインⅡ5頁)	○ (ガイドライン49頁)	○ 事務：Ⅰ1・別添1、Ⅱ3⑧ 情報：Ⅰ3、Ⅱ1・2、 人：Ⅱ2⑥③⑦
基本方針の策定	△ プライバシー・ポリシー等を整備すると望ましい。	△ (法令・ガイドラインでは明記されていないが望ましい)	個人情報と同様の取扱いを求めるものではないが、例えば、法第20条から第22条までに定める個人データの安全管理、従業員の監督及び委託先の監督並びに法第35条に定める個人情報の取扱いに関する苦情の処理で求められる措置の例(※)を参考にすることも考えられる。	△ (法令・ガイドラインでは明記されていないが望ましい)	○(ガイドラインⅡ5頁)	△ プライバシー・ポリシー等を整備すると望ましい。	△ (明確な該当箇所はないが、備考欄等に追記すると望ましい)
規律の整備	○ 取扱規程の作成、取扱方法の周知等	○ 規則20条2号		△ (法令・ガイドラインでは明記されていないが望ましい)	○ (ガイドラインⅡ6頁、組織的安全管理措置に分類)	○ 取扱規程の作成、取扱方法の周知等	○ Ⅲ7リスク1③④
組織的安全管理措置							
組織体制の整備	○ 責任者・担当者等を決定等	○ 取り扱う者の権限・責任を明確に定める(規則20条1号)		○ 取り扱う者の権限・責任を明確に定める(行政機関非識別加工情報規則14条1号、独立行政法人等非識別加工情報規則13条1号)	○ 相当の経験・識見を有する責任者の配置、取扱者の権限・責務・業務明確化	○ 責任者・担当者等を決定等	○ Ⅲ7リスク1②
個人データの取扱いに係る規律に従った運用	○ ログ等	○ 規程類に従って適切に取り扱う(規則20条2号)		○ 規程類に従って適切に取り扱う(行政機関非識別加工情報規則14条2号、独立行政法人等非識別加工情報規則13条2号)	○(ガイドラインⅡ7頁)	○ ログ等	○ Ⅲ3リスク2特定個人情報の使用の記録、Ⅲ4特定個人情報ファイルの取扱いの記録、Ⅲ5リスク1特定個人情報の提供・移
取扱状況を確認する手段の整備	○ 台帳等	○(ガイドライン17頁)		○(ガイドライン18頁)	○ (情報のやり取り時のログについてガイドラインⅡ7頁)	○ 台帳等	○ 計画管理書
漏えい等の事案に対応する体制の整備	○ 連絡体制の決定等	△ (法令・ガイドラインでは明記されていないが望ましい)		△ (法令・ガイドラインでは明記されていないが望ましい)	○ 連絡体制の決定等	○ 連絡体制の決定等	○ Ⅲ7リスク1⑧

	個人情報		匿名加工情報等			マイナンバー関連	PIA関連
	個人情報	匿名加工情報の加工方法等情報	匿名加工情報	非識別加工情報等	匿名加工医療情報	特定個人情報等	評価書と安全管理措置の対応
取扱状況の把握及び安全管理措置の見直し	○ 点検、監査等	○ 取扱いの状況の評価、その結果に基づき改善を図るために必要な措置を講ずる(規則20条2号)		○ 取扱いの状況の評価、その結果に基づき改善を図るために必要な措置を講ずる(行政機関非識別加工情報規則14条2号、独立行政法人等非識別加工情報規則13条2号)	○ 運用評価及び改善	○ 点検、監査等	○ IV1
人的安全管理措置							
従業員の教育	○ 研修、守秘義務	○ (ガイドライン17頁)		○ (ガイドライン18頁)	○	○ 研修、守秘義務	○ IV2
従業員の監督	○ (個人情報21条)	△ (規則20条2号)		△ (行政機関非識別加工情報規則14条2号、独立行政法人等非識別加工情報規則13条2号)	○ (次世代医療基盤法21条)	○	○ III IV全般
その他	—	—		—	・欠格事由に該当しないことの確認 ・目的外取扱い防止 ・無権限者による取扱い防止	—	
物理的安全管理措置							
区域の管理	○ 間仕切り、入退室管理等	△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(規則20条3号)		△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(行政機関非識別加工情報規則14条3号、独立行政法人等非識別加工情報規則13条3号)	○ 間仕切り、入退室管理、常時監視カメラ等	○ 間仕切り、入退室管理等	
機器及び電子媒体等の盗難等の防止	○ 施錠、セキュリティワイヤー等	△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(規則20条3号)		△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(行政機関非識別加工情報規則14条3号、独立行政法人等非識別加工情報規則13条3号)	○ セキュリティワイヤー等	○ 施錠、セキュリティワイヤー等	△ III7リスク1⑤
電子媒体等を持ち運ぶ場合の漏えい等の防止	○ パスワード、封緘等	△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(規則20条3号)		△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(行政機関非識別加工情報規則14条3号、独立行政法人等非識別加工情報規則13条3号)	△ (提供時のダブルチェック等が人的安全管理措置にある。郵送時の書留等の利用は技術的安全管理措置にある(17ページ)。持運びはあまり想定されないか。)	○ パスワード、封緘等	
削除、廃棄	○ 復元不可能な方法で	△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(規則20条3号)		△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(行政機関非識別加工情報規則14条3号、独立行政法人等非識別加工情報規則13条3号)	○ 復元不可能な方法で	○ 復元不可能な方法で	
技術的安全管理措置							

	個人情報		匿名加工情報等			マイナンバー関連		PIA関連
	個人情報	匿名加工情報の加工方法等情報	匿名加工情報	非識別加工情報等	匿名加工医療情報	特定個人情報等	評価書と安全管理措置の対応	
アクセス制御	○ 権限管理等	△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(規則20条3号)		△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(行政機関非識別加工情報規則14条3号、独立行政法人等非識別加工情報規則13条3号)	○ 権限管理等	○ 権限管理等	△ Ⅲ7リスク1⑥	
アクセス者の識別と認証	○ ID/PWD、カード等	△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(規則20条3号)		△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(行政機関非識別加工情報規則14条3号、独立行政法人等非識別加工情報規則13条3号)	○ ID/PWD、カード等	○ ID/PWD、カード等		
外部からの不正アクセス等の防止	○ FW、セキュリティ対策ソフト等	△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(規則20条3号)		△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(行政機関非識別加工情報規則14条3号、独立行政法人等非識別加工情報規則13条3号)	○ 異常検知、異常制御、セキュリティ対策ソフト等	○ FW、セキュリティ対策ソフト等		
情報システムの使用に伴う漏えい等の防止	○ パスワード等	△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(規則20条3号)		△ 無権限者による取扱いを防止するために必要かつ適切な措置を講ずる(行政機関非識別加工情報規則14条3号、独立行政法人等非識別加工情報規則13条3号)	◎ 専用線、暗号化、サーバ構成、ネットワーク構成等	○ パスワード等		
その他	—	—		—	・動作記録 ・使用目的に反する動作をさせる機能の不存在確認	—		
ガイドライン	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) https://www.ppc.go.jp/files/pdf/guidelines01.pdf	個人情報の保護に関する法律についてのガイドライン(匿名加工情報編) https://www.ppc.go.jp/files/pdf/guidelines04.pdf	行政機関の保有する個人情報の保護に関する法律についてのガイドライン(行政機関非識別加工情報編) 独立行政法人等の保有する個人情報の保護に関する	医療分野の研究開発に資するための匿名加工医療情報に関する法律についてのガイドライン II. 安全管理措置編 https://www.kantei.go.jp/jp/singi/kenkouiryou/jiseda/kiban/pdf/h3005_guidelin	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) https://www.ppc.go.jp/files/pdf/my_number_guideline_ijgvoaha.pdf	特定個人情報保護評価に関する規則、特定個人情報保護評価指針 https://www.ppc.go.jp/enforcement/assessment/		
個人情報該当性	○	△ (加工方法等は個人情報でない場合も)	×	△ (加工方法等は個人情報でない場合も)	△ (医療情報は個人情報、加工方法等は個人情報でない場合も)	△ (死者の個人番号は個人情報でない場合も多い)	—	