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概要

令和８年10月
個人情報保護委員会事務局

スケジュール

令和８年９月16日に開催した第369回個人情報保護委員会では、以下のスケジュールとしていた。

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

しかし、近時、個人情報保護委員会は、国民に広く普及した、大量の個人情報を取り扱う個人情報取扱事業者が外部からの不正アクセスを受け、その取り扱う大量の個人データが漏えいし、又は漏えいのおそれが生じた漏えい等事案に接しており、このような動向を踏まえ、**施行を可能な限り前倒す**こととした。具体的には以下のとおり。

令和８年 ９月16日	今回	委員会決議 後１ヶ月	可能な限り 早く
手法の例示の追加等の方向性の公表	見直し案の委員会審議	パブリックコメント	パブリックコメントの結果報告、改正事項の決定、**改正事項の施行**

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う。

安全管理措置の全体像

個人情報保護法第23条

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。

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」

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について示す**。

講じなければならない措置

- **義務**
- 従わなかった場合、法違反と判断される可能性がある。

手法の例示

- **（義務ではなく）例**
- 具体的な手法については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因する**リスクに応じて、必要かつ適切な内容とすべき**

※ 保有個人情報の安全管理措置について、個人情報保護法第66条第1項
※ 個人番号の安全管理措置について、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第12条

現行の「10（別添）講ずべき安全管理措置の内容」

個人データの取扱いに係る規律の整備

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等の防止その他の個人データの安全管理のために、個人データの具体的な取扱いに係る規律を整備しなければならない。

組織的安全管理措置

講じなければならない措置

⑴組織体制の整備
⑵個人データの取扱いに係る規律に従った運用
⑶個人データの取扱状況を確認する手段の整備
⑷漏えい等事案に対応する体制の整備
⑸取扱状況の把握及び安全管理措置の見直し

物理的安全管理措置

講じなければならない措置

⑴個人データを取り扱う区域の管理
⑵機器及び電子媒体等の盗難等の防止
⑶電子媒体等を持ち運ぶ場合の漏えい等の防止
⑷個人データの削除及び機器、電子媒体等の廃棄

人的安全管理措置

講じなければならない措置

〇従業者の教育
（参考）従業者に個人データを取り扱わせる場合には、法第24条に基づき従業者を監督

技術的安全管理措置

講じなければならない措置

⑴アクセス制御
⑵アクセス者の識別と認証
⑶外部からの不正アクセス等の防止
⑷情報システムの使用に伴う漏えい等の防止

検討の方向性

令和８年９月16日　第369回 個人情報保護委員会

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。
- 個人情報保護委員会がサイバーセキュリティ関係省庁・機関との間で四半期ごとに開催している個人情報保護法サイバーセキュリティ連絡会で得られた知見、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、ガイドライン（通則編）別添の内容について検討を行い、下記①から④の課題を認識した。

① 取扱い多様化への対応

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への対応

② ゼロトラストモデルの導入

従来の境界型セキュリティモデル※1に加え、ゼロトラストモデル※2の考え方を導入

※1 インターネットと内部ネットワークの境界を防御するというセキュリティ概念
※2 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

③ 横展開対策

侵入型ランサムウェア等による、侵入された後の被害拡大防止の対策の提示

④ 記載の明確化

「講じなければならない措置」と「手法の例示」の対応関係、趣旨等の整理

※ ただし、「手法の例示」の追加等であり、新たな規律を設けるものではない。

本資料の対象

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。）

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）
（以下「マイナンバーガイドライン（事業者編）別添１」という。）

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）
（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。）

※ 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）についても同趣旨の改訂を行う。
※ 特定分野ガイドラインについても同様の検討を行い、必要な改訂を行う。

更新（案）の全体像

				ガイドライン（通則編）別添	マイナンバーガイドライン（事業者編）別添１	マイナンバーガイドライン（行政機関等編）別添１
① 取扱い多様化への対応	①-1	責任部署の設置等	組織	追記	追記	ー
		同一のユーザーID・パスワードの使い回しの原則禁止	技術	追記	追記	追記
		ログ等の保管	技術	追記	追記	追記
	①-2	アクセス者の識別と認証の対象	技術	変更	変更	(変更)
		暗号化消去等	技術 物理	追記	(追記)	(追記)
	①-3	指紋認証・静脈認証・顔認証	技術	追記	追記	追記
		多要素認証	技術	追記	追記	追記
② ゼロトラストモデルの導入		動的コンテキストの評価等	技術	追記	追記	追記
		許可デバイスからのアクセス限定	技術	追記	追記	追記
③ 横展開対策		特権アカウントの限定	技術	追記	追記	追記
		被害拡大の対策	技術	追記	追記	追記
④ 記載の明確化	④-1	組織的安全管理措置の再構成	組織	変更	変更	ー
	④-2	不正アクセス等の検知等	技術	追記	追記	追記
	④-3	規律の明確化等	組織	追記	追記	追記
		規律との照合	組織	追記	追記	追記
		安全管理措置の見直し等	組織	追記	追記	ー
		研修等の見直し等	人的	追記	追記	ー
		アクセス権限の変更	技術	追記	追記	追記
		早期検知等の仕組み等	技術	追記	追記	追記
	④-4	Ｑ＆Ａの一本化	組織 人的 技術	追記	追記	追記
	④-5	マイナンバーガイドライン固有の記載		ー	追記	追記

【凡例】
追記：記載の追加　（追記）：同様の追加（該当箇所が異なる）
変更：記載の変更　（変更）：同様の変更（理由が異なる）
ー：対象外

更新（案）の概要 ①-1 取扱い多様化への対応

①-1　**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。**

組織的安全管理措置

責任部署の設置
及び役割の明確化等

※ 左記の内容を、矢印右記の各ガイドラインに反映する。以下同じ。

追記

- ガイドライン（通則編）別添
  10-3⑴組織体制の整備
  手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-Ｃ-ａ組織体制の整備
  手法の例示

※ マイナンバーガイドライン（行政機関等編）別添１は該当箇所に「手法の例示」がないため対象外

技術的安全管理措置

同一のユーザーID・パスワードの
使い回しの原則禁止

追記

- ガイドライン（通則編）別添
  10-6⑵アクセス者の識別と認証　手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-Ｆ-ｂアクセス者の識別と認証　手法の例示
- マイナンバーガイドライン（行政機関等編）別添１
  2-Ｆ-ｂアクセス者の識別と認証　手法の例示

ログ等の一定期間の保管

追記

- ガイドライン（通則編）別添
  10-6⑸不正アクセス等の検知等※1　手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-Ｆ-ｅ不正アクセス等の検知等　手法の例示
- マイナンバーガイドライン（行政機関等編）別添１
  2-Ｆ-ｅ不正アクセス等の検知等　手法の例示

※1 「不正アクセス等の検知等」について、④-2記載の明確化参照。以下同じ。

更新（案）の概要 ①-2 取扱い多様化への対応

①-2　**クラウドサービス**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。**

技術的安全管理措置

アクセス者の識別と認証の対象を「個人データを取り扱う情報システムを使用する者」へ

変更

- ガイドライン（通則編）別添 10-6⑵アクセス者の識別と認証
  講じなければならない措置　手法の例示
- マイナンバーガイドライン（事業者編）別添１ 2-Ｆ-ｂアクセス者の識別と認証
  講じなければならない措置　手法の例示

※ マイナンバーガイドライン（行政機関等編）別添１の2-Ｆ-ｂアクセス者の識別と認証についても同様の変更を行うが理由が異なる。
※ 明確化であり新たな規律を設けるものではない（本資料５頁）。

暗号化消去等、容易に復元できない手段による消去

追記

- ガイドライン（通則編）別添 10-6⑷情報システムの使用に伴う漏えい等の防止
  手法の例示

※ マイナンバーガイドライン（事業者編）別添１及びマイナンバーガイドライン（行政機関等編）別添１は該当箇所がないため対象外
※ 以下の物理的安全管理措置について同様の追記を行う。
・ガイドライン（通則編）別添10-5⑷個人データの削除及び機器、電子媒体等の廃棄
・マイナンバーガイドライン（事業者編）別添１の2-Ｅ-ｄ個人番号の削除、機器及び電子媒体等の廃棄
・マイナンバーガイドライン（行政機関等編）別添１の2-Ｅ-ｄ個人番号の削除、機器及び電子媒体等の廃棄

更新（案）の概要 ①-3 取扱い多様化への対応

①-3　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る場合があることを踏まえて、**これらの認証の手法の例を明確にする**。

技術的安全管理措置

指紋認証・静脈認証・顔認証 → 追記

- ガイドライン（通則編）別添
  10-6⑵アクセス者の識別と認証
  手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-Ｆ-ｂアクセス者の識別と認証
  手法の例示
- マイナンバーガイドライン（行政機関等編）別添１
  2-Ｆ-ｂアクセス者の識別と認証
  手法の例示

多要素認証 → 追記

- ガイドライン（通則編）別添
  10-6⑵アクセス者の識別と認証
  手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-Ｆ-ｂアクセス者の識別と認証
  手法の例示
- マイナンバーガイドライン（行政機関等編）別添１
  2-Ｆ-ｂアクセス者の識別と認証
  手法の例示

更新（案）の概要 ② ゼロトラストモデルの導入

② **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。**

技術的安全管理措置

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。

追記

- ガイドライン（通則編）別添
  10-6⑴アクセス制御
  手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-Ｆ-ａアクセス制御
  手法の例示
- マイナンバーガイドライン（行政機関等編）別添１
  2-Ｆ-ａアクセス制御
  手法の例示

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個人データへのアクセスを許可する。

追記

- ガイドライン（通則編）別添
  10-6⑶外部からの不正アクセス等の防止
  手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-Ｆ-ｃ外部からの不正アクセス等の防止
  手法の例示
- マイナンバーガイドライン（行政機関等編）別添１
  2-Ｆ-ｃ不正アクセス等による被害の防止等
  手法の例示

更新（案）の概要 ③ 横展開対策

③　**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、手法の例等を明確にする。**

技術的安全管理措置

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。

追記

- ガイドライン（通則編）別添
  10-6⑴アクセス制御
  手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-Ｆ-ａアクセス制御
  手法の例示
- マイナンバーガイドライン（行政機関等編）別添１
  2-Ｆ-ａアクセス制御
  手法の例示

不正アクセス等が発生した場合でも個人データ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。

追記

- ガイドライン（通則編）別添
  10-6⑸不正アクセス等の検知等
  手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-Ｆ-ｅ不正アクセス等の検知等
  手法の例示
- マイナンバーガイドライン（行政機関等編）別添１
  2-Ｆ-ｅ不正アクセス等の検知等
  手法の例示

更新（案）の概要 ④-1 記載の明確化

④-1　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」の位置付けを整理し、**再構成**をする。

組織的安全管理措置

「個人データの取扱いに係る規律に従った運用」及び「個人データの取扱状況を確認する手段の整備」の記載を一本化

変更

- ガイドライン（通則編）別添
  10-3⑵個人データの取扱いに係る規律に従った運用
  講じなければならない措置　手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-C-b 取扱規程等に基づく運用
  講じなければならない措置　手法の例示

※ マイナンバーガイドライン（行政機関等編）別添１では同2-C-b 取扱規程等に基づく運用と同 c 取扱状況を確認する手段の整備で客体が異なるため当該変更を行わない。
※ 現行の内容の再構成であり新たな規律を設けるものではない（本資料５頁）。

更新（案）の概要 ④-2 記載の明確化

④-2　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」である、「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」等**について、位置付けを整理し、**再構成**をする。

技術的安全管理措置

不正アクセス等の検知等

追記

- ガイドライン（通則編）別添
  10-6⑸不正アクセス等の検知等
  講じなければならない措置　手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-Ｆ-ｅ不正アクセス等の検知等
  講じなければならない措置　手法の例示
- マイナンバーガイドライン（行政機関等編）別添１
  2-Ｆ-ｅ不正アクセス等の検知等
  講じなければならない措置　手法の例示

※ 現行の内容の再構成であり新たな規律を設けるものではない（本資料５頁）。

更新（案）の概要 ④-3 記載の明確化

④-3　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、**追記をする**。

組織的安全管理措置

個人データの取扱いに係る規律を明確化し、従業者に周知する。

追記

- ガイドライン（通則編）別添
  10-3⑵個人データの取扱いに係る規律に従った運用
  手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-C-b 取扱規程等に基づく運用
  手法の例示
- マイナンバーガイドライン（行政機関等編）別添１
  2-C-b 取扱規程等に基づく運用
  手法の例示

あらかじめ整備された個人データの取扱いに係る規律と照らし合わせる。

追記

- ガイドライン（通則編）別添
  10-3⑵個人データの取扱いに係る規律に従った運用
  手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-C-b 取扱規程等に基づく運用
  手法の例示
- マイナンバーガイドライン（行政機関等編）別添１
  2-C-b 取扱規程等に基づく運用
  手法の例示

更新（案）の概要 ④-3 記載の明確化

組織的安全管理措置

個人データの取扱状況、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。

追記

- ガイドライン（通則編）別添
  10-3⑷取扱状況の把握及び安全管理措置の見直し
  手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-C-d 取扱状況の把握及び安全管理措置の見直し
  手法の例示

※ マイナンバーガイドライン（行政機関等編）別添１では同2-C-e 取扱状況の把握及び安全管理措置の見直しにおいて同趣旨の内容が規定されているため当該追記を行わない。

人的安全管理措置

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。

追記

- ガイドライン（通則編）別添
  10-4○従業者の教育
  手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-D-b 事務取扱担当者の教育
  手法の例示

※ マイナンバーガイドライン（行政機関等編）別添１は該当箇所に「手法の例示」がないため対象外

更新（案）の概要 ④-3 記載の明確化

技術的安全管理措置

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。

追記

- ガイドライン（通則編）別添
  10-6⑴アクセス制御
  手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-Ｆ-ａアクセス制御
  手法の例示
- マイナンバーガイドライン（行政機関等編）別添１
  2-Ｆ-ａアクセス制御
  手法の例示

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。

追記

- ガイドライン（通則編）別添
  10-6⑸不正アクセス等の検知等
  手法の例示
- マイナンバーガイドライン（事業者編）別添１
  2-Ｆ-ｅ不正アクセス等の検知等
  手法の例示
- マイナンバーガイドライン（行政機関等編）別添１
  2-Ｆ-ｅ不正アクセス等の検知等
  手法の例示

更新（案）の概要 ④-4・④-5 記載の明確化

④-4　「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の「手法の例示」についてガイドライン（通則編）別添、マイナンバーガイドライン（事業者編）別添１及びマイナンバーガイドライン（行政機関等編）別添１に記載を一本化する。

④-5　マイナンバーガイドライン固有の記載の明確化

マイナンバーガイドライン（事業者編）別添１	2-B 取扱規程等の策定 手法の例示	源泉徴収票等を作成する事務において「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の追記
マイナンバーガイドライン（行政機関等編）別添１	2-B 取扱規程等の見直し等 手法の例示	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の追記
	2-C-b 取扱規程等に基づく運用 手法の例示	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の追記