第14回民間利活用作業班
（令和6年11月28日開催）

資料４

PHR基本的指針の情報セキュリティ対策の項目整理について（案）

課題② 最新の情報セキュリティ対策への対応（最新のGL等への準拠）再掲

- 情報セキュリティ対策については、マイナポータル利用規約が、「中小企業における組織的な情報セキュリティガイドライン」(2008年IPA策定)を引用していたことを受けて、本指針においても、当該ガイドラインをほぼそのまま転記する形で作成している。そのため、最新の情報セキュリティ対策へ対応すべく、記載を見直す必要がある。

【対応方針】

- **関連ガイドライン（中小企業情報セキュリティGL※1、クラウドセキュリティGL※2、NISCハンドブック※3）等を参考に、現行指針に対して項目を追加する。**

最新の情報セキュリティ対策への対応を検討した項目

2.1 安全管理措置

(1)法規制に基づく遵守すべき事項
(2)本指針に基づく遵守すべき事項
① 情報セキュリティに対する組織的な取り組み
② 物理的セキュリティ
③ 情報システム及び通信ネットワークの運用管理
④ 情報システムのアクセス制御並びに情報システムの開発及び保守におけるセキュリティ対策
⑤ 情報セキュリティ上の事故対応
⑥ 外的環境の把握

2.2 第三者認証の取得

(1)法規制に基づく遵守すべき事項

詳細は **次頁以降**

※1 中小企業の情報セキュリティ対策ガイドライン第3.1（IPA） https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf
※2 クラウドサービス提供における情報セキュリティ対策ガイドライン第3版（総務省） https://www.soumu.go.jp/main_content/000771515.pdf
※3 インターネットの安心・安全ハンドブック（NISC）https://security-portal.nisc.go.jp/guidance/handbook.html

課題③ 無害化処理の要否

再掲

- 外部から受け取るファイルへの無害化処理（現行指針では「サニタイズ処理」に限定）について、過去に本指針の適用範囲を踏まえた議論が行われておらず、また、その必要性を十分に説明できていないことから、見直しを検討する。

（参考）２．１．安全管理措置　（２）　③ 情報システム及び通信ネットワークの運用管理 ＜抜粋＞

■外部から受け取るファイルに対して、無害化を実施する

➢ファイル無害化機器、無害化ソフトウェア又は無害化サービス等を導入し、外部からのファイルを受け取る際に、無害化を実施すること。

【対応方針】

- 未知のマルウエアに対応する必要性から無害化処理が求められているが、**技術的な選択肢は複数あり**、**PHRサービス提供者側が現状に適した技術を選択できる余地を残すべき**ではないか。
- **情報セキュリティ対策全体として必要な対策を規定することを前提に、無害化処理の記載は削除することとする。**

❶経産省の外部サイバーセキュリティ専門家からの意見

- 無害化処理以外にも、**アンチウイルスソフトでのファイルチェックや、機械学習モデルを使ってファイルの中をチェックすることも可能**であり、**無害化処理にこだわる必要はない。**
- まずは、守るべき対象を明確にした上で、必要な対策を検討すべき。その際、**無害化ありきではなく、情報セキュリティ対策全体として、必要な対策について包括的に議論すべき。**

❷事業者からの意見

- **ウイルススキャンでは、未知のウィルスへ対応できるものも含め、手法は様々存在し、技術の選び方の問題**である。一方で、完全に「無害化」することは技術的も費用的にも負担は大きい。
- 無害化は必要な処理であると思うが、なぜ**指針でこの技術だけを取り上げているのかが不明**である。
- **システム同士のやり取りでは、無害化の優先度は低い。**一方で、一般利用者がアップロードする場合は無害化の優先度が高いが、**システムの構成によってセキュリティの対応が異なるため、無害化は一手段に過ぎない。**

2．情報セキュリティ対策　2．１安全管理措置

（１）法規制に基づく遵守すべき事項

赤字：追加・修正点

大項目	中項目	対応方針
①個人情報保護法に基づく適切な取扱い	漏えい、滅失又は毀損の防止その他の安全管理のために必要かつ適切な措置	■ 従来の個人情報保護法に基づく規定を維持
②その他の法令等に基づく遵守事項		■ 事業者向けガイドラインという観点から、事業者にとして対応すべき情報管理に関する法令等（機密情報、知的財産等、その他法令又は契約上適切な管理等）の対応についての項目を追記

（２）本指針に基づく遵守すべき事項

大項目	中項目	対応方針
柱書	リスクアセスメント	■ セキュリティ対策の前提として、他のガイドライン等でリスクアセスメントを踏まえることが一般となっていることから、（２）本指針に基づく順守すべき事項における、前提となる考え方として追記
柱書	文書化の実施	■ 事業者のシステム管理に必要な文書化の実施（各種規程類、システム関連資料）に関する一般の項目がないので追記

【引用元ガイドライン】

※1 **中小GL：中小企業の情報セキュリティ対策ガイドライン第3.1版（IPA）**
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

※2 **クラウドGL：クラウドサービス提供における情報セキュリティ対策ガイドライン第3版（総務省）**
https://www.soumu.go.jp/main_content/000771515.pdf

※3 **NISC GL:インターネットの安心・安全ハンドブック（NISC）**
https://security-portal.nisc.go.jp/guidance/handbook.html

2．情報セキュリティ対策　2．1安全管理措置

（2）本指針に基づく遵守すべき事項
　① 情報セキュリティに対する組織的な取り組み

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
A)提供するサービスの目的・範囲等の明確化	サービス提供目的・範囲等の明確化	■ 事業者用のガイドラインという観点から、PHRのサービス目的を明らかにし、組織内の理解を促すことを追記		●	
B)情報セキュリティに関する経営者の意図の従業員への明示	経営者による情報セキュリティポリシーの策定の関与等	■ 例を追記	●	●	●
	情報セキュリティポリシーの定期的な見直し	■ 例を追記	●	●	
C)情報セキュリティ対策に関わる責任者と担当者の明示	情報セキュリティ及び経営を理解する責任者の任命	■ 例を追記		●	
	責任者による、各セキュリティ対策についての責任者及び担当者それぞれの役割の具体化	■ 例を追記	●	●	
	問い合わせ窓口	■ 事業者用のガイドラインという観点から、利用者に対する問い合わせ窓口について追記	●	●	
D)管理すべき重要な情報資産の区分	管理すべき重要な情報資産の区分	■ 例を追記	●	●	
	情報資産の管理者の指定	■ 例を追記		●	
	重要度に応じた情報資産の取扱指針の策定	■ 例を追記	●	●	
	健診等情報を取り扱う人の範囲の指定	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―

2．情報セキュリティ対策　2．1安全管理措置

（2）本指針に基づく遵守すべき事項

① 情報セキュリティに対する組織的な取り組み

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
E)情報資産の区分に基づいたリスク管理	保有する情報資産に対する脅威を想定したリスクの洗い出し	■ セキュリティ対策として、リスクアセスメントを踏まえたリスクマネジメントが一般的であることから追記	●		
	情報資産に対するリスク評価	■ セキュリティ対策として、リスクアセスメントを踏まえたリスクマネジメントが一般的であることから追記	●	●	
	情報資産のリスク評価に応じた方針を決定及びその方針を実現するための対策の実施	■ セキュリティ対策として、リスクアセスメントを踏まえたリスクマネジメントが一般的であることから追記	●		
	情報資産に対するリスク管理及びリスク対策の定期的な見直し	■ セキュリティ対策として、リスクアセスメントを踏まえたリスクマネジメントが一般的であることから追記		●	
F)個人情報の取扱状況を確認する手段の整備	個人情報の取扱状況を把握可能とするための項目の明確化	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―
G)健診等情報の入手、作成、利用、保管、交換、提供、消去及び破棄における取扱手順の策定	各プロセスにおける作業手順を明確化及び手順に基づいた決められた担当者による作業の実施	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―
	健診等情報に対して、漏えい及び不正利用を防ぐ保護対策の実施	■ 変更なし	●	●	
H)外部の組織と情報をやり取りする際の情報の取扱いに関する注意事項についての合意	契約書及び委託業務の際に取り交わす書面への情報の取扱いに関する注意事項の記載	■ 例を追記	●	●	

2．情報セキュリティ対策　2．1安全管理措置

（2）本指針に基づく遵守すべき事項
　① 情報セキュリティに対する組織的な取り組み

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
I)個人データの取扱いを委託する場合の委託先での安全管理措置の確保	個人データの取扱を委託する場合の安全管理措置の確保	■ 例を追記	●		●
	適切な委託先の選定	■ 事業者が個人データを取扱う委託を行う際に、リスク管理上、適切な体制や信頼性等を備えた事業者を選定する必要があることから追記。		●	●
	セキュリティ対策等を勘案した、導入するクラウドサービスの選定	■ クラウドサービスを利用して、サービス提供をする場合の事業者選定について追記		●	
J)外部の主体による監査等の実施	個人データの取扱状況に関する定期的な自己点検又は他部署等による監査の実施	■ 例を追記	●		
	外部の主体による監査の実施	■ 例を追記	●		
K)従業者（派遣を含む。）にする、セキュリティに関して就業上の義務の明示	従業者を採用する際の守秘義務契約又は誓約書の取り交わし	■ 変更なし		●	
	秘密保持に関する事項を就業規則等に盛り込むなど、 従業者が遵守すべき事項の明確化	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―
	違反に対する懲戒手続きの整備	■ 例を追記		●	
	在職中及び退職後の機密保持義務を含む誓約書の取得	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―

2．情報セキュリティ対策　2．1安全管理措置

（2）本指針に基づく遵守すべき事項
① 情報セキュリティに対する組織的な取り組み

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
L)情報セキュリティに関するルールの周知及び情報セキュリティに関わる知識習得の機会の提供	ポリシー及び関連規程の文書化による従業員への理解促進	■ 中項目の内容の明確化	●		
	従業員に対する必要な教育の定期的な実施	■ 中項目の内容の明確化 ■ 例を追記		●	●

2．情報セキュリティ対策　2．1安全管理措置

（2）本指針に基づく遵守すべき事項
② 物理的セキュリティ

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
A)健診等情報の保管、取扱場所の入退管理及び施錠管理	健診等情報の保管・取扱い区域の指定	■ 例を追記		●	●
	健診等情報を保管している部屋・フロアーへの侵入防止対策の実施	■ 例を追記	●		
	健診等情報を保管している部屋・フロアーへの入出者の制限及び入退の記録の取得	■ 変更なし		●	
B)重要なコンピュータ・配線についての地震等の自然災害等による重大な被害防止のための配置又は設置	建物・サーバルームにおける物理的セキュリティの確保	■ 災害等のリスク対策のため、システムの設置場所等に関する物理セキュリティ対策が重要性であることから追記		●	
	許可された人だけが入ることができる安全な場所への重要なコンピュータの設置	■ 例を追記		●	
	電源・通信ケーブル等への接触防止措置	■ 例を追記		●	
	重要なシステムについて、地震等による転倒防止、水漏れ防止、停電時の代替電源の確保	■ 例を追記		●	
	健診等情報を保管する重要なコンピュータ等の装置等の耐災害対策・盗難対策	■ 物理セキュリティとして、健診等情報を保管する重要なコンピュータ等の装置やラック等における耐災害対策や、盗難等への対策が重要であることから追記		●	

2．情報セキュリティ対策　2．1安全管理措置

（2）本指針に基づく遵守すべき事項
② 物理的セキュリティ

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
C)重要な書類及び記憶媒体等についての、整理整頓、盗難防止対策、紛失対策及び確実な廃棄	健診等情報を記載した書類について不要になった場合、シュレッダー又は焼却等による処分	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―
	健診等情報を記載した書類のキャビネットにおける施錠管理	■ 変更なし	●		
	健診等情報が存在する机上、書庫及び会議室等の整理整頓	■ 例を追記		●	
	（削除）~~郵便物、FAX及び印刷物等の放置禁止、重要な書類の裏面の再利用禁止~~	■ 「健診等情報が存在する机上、書庫及び会議室等の整理整頓」の例として移動	―	―	―
	使用しなくなった健診等情報の速やかな消去	■ 例を追記	●	●	
	（削除）~~クラウド上のデータを含めた不要データの確実な処分~~	■ 「使用しなくなった健診等情報の速やかな消去」の例として移動	―	―	―
	健診等情報を表示する画面の窃視対策	■ 個人情報の取扱いに際し、画面上のデータの保護を行う必要性が高いことから追記	●		
	データの不正持出し防止のための記憶媒体の管理	■ 物理的セキュリティにおいて、媒体全般を対象とするルールを明示する必要があることから追記		●	
	モバイルPC及び記憶媒体等の盗難防止対策・紛失対策	■ 例を追記	●		●
	許可のない私有PCの持ち込みや私有PCでの業務の禁止	■ 例としてBYOD端末使用時の対策及びルールについて追記			●

2．情報セキュリティ対策　2．1安全管理措置

（2）本指針に基づく遵守すべき事項
③ 情報システム及び通信ネットワークの運用管理

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
A)情報システムの運用に関して運用ルールの策定	システム運用におけるセキュリティ要求事項の明確化	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	ー	ー	ー
	情報システムの運用手順書（マニュアル）の整備	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	ー	ー	ー
	システムの運用状況の点検	■ 例を追記		●	
	システム操作、障害及びセキュリティ関連イベントについてログ（記録）の取得	■ 例を追記	●	●	
	設備（具体例）の使用状況の記録	■ 例を追記		●	
	取得したログ（記録）の定期的なレビューの実施	■ 例を追記		●	
	適切な運用のための管理策の実施	■ 事業者のシステム管理に必要なサービス提供に必要なシステムの運用監視に関する内容がないので追記 ■ 特にクラウドサービスの利用という観点から追記		●	
	サービスを提供するシステム等の環境の確保	■ サービス提供に必要なシステム等の環境確保に必要なシステムリソース監視に関する内容がないので追記 ■ 特にクラウドサービスの利用という観点から追記	●	●	
	クラウドサービスの特性に応じた運用	■ クラウドサービスの特性に応じた運用報告の方法や内容、運用関連情報の提供について示されていないので追記		●	

2．情報セキュリティ対策　2．1安全管理措置

（2）本指針に基づく遵守すべき事項
③ 情報システム及び通信ネットワークの運用管理

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
B)マルウエア対策ソフト等アプリケーションの運用の適切な実行	マルウエア対策ソフトの導入及び製品のバージョンや設定ファイル・定義ファイル等の定期的な更新の実施	■ 引用元ガイドラインでマルウエア対策が記載されていることにあわせ、中項目の内容を修正 ■ 例を追記	●	●	
	マルウエア対策ソフトの機能（ファイアウォール機能、スパムメール対策機能及び有害サイト対策機能）の活用	■ 引用元ガイドラインでマルウエア対策が記載されていることにあわせ、中項目の内容を修正		●	
	各サーバ及びクライアントPCの定期的なマルウエア検査の実施	■ 引用元ガイドラインでマルウエア対策が記載されていることにあわせ、中項目の内容を修正		●	
	組織で許可されていないソフトウェアのインストール及びサービスの利用の禁止・使用制限	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―
	PHRサービスの利用者に対する適切なセキュリティ対策済利用端末の利用啓発	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―

2．情報セキュリティ対策　2．1安全管理措置

（2）本指針に基づく遵守すべき事項
③情報システム及び通信ネットワークの運用管理

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
C)情報システムへの最新のパッチを適用等の脆弱性対策の実施	脆弱性の解消（修正プログラムの適用及びWindows update等）の実施	■ 例を追記	●	●	●
	脆弱性情報及び脅威に関する情報の入手方法を確認、定期的な収集	■ 例を追記	●	●	
	情報システム導入の際の、不要なサービスの停止等、セキュリティを考慮した設定の実施状況の確認	■ 例を追記		●	
	Webサイトの公開に際しての、不正アクセス又は改ざん等の防止のための設定又は対策等、脆弱性の解消	■ 例を追記	●		
	Webブラウザ・電子メールソフトのセキュリティ設定の実施	■ 変更なし	●		
D)重要なデータやファイルについて	TLS（version1.3）等を用いた通信データを暗号化	■ 例を追記 ■ 現時点での最新である1.3に修正及び1.2適用時の留意事項を追記	●	●	
	外部のネットワークから内部のネットワーク又は情報システムにアクセスする際のVPN等による通信路の暗号化	■ 変更なし	●		
	電子メールをやり取りする際に、健診等情報の暗号化等の保護策の実施	■ 変更なし	●		
	重要なデータやファイルに対する暗号化対策	■ データ交換の対象となるファイル等全般を対象とするルールの整備の重要性から追記	●	●	

2．情報セキュリティ対策　2．1安全管理措置

（2）本指針に基づく遵守すべき事項
③　情報システム及び通信ネットワークの運用管理

赤字：追加・修正点

大項目	中項目	対応方針	該当ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
E）モバイルPC、USBメモリなどの記憶媒体又はデータを外部に持ち出す場合の、盗難・紛失等に備えた適切なパスワード設定又は暗号化等の対策実施	モバイルPC又はUSBメモリ等の使用や外部持ち出し規程の策定	■ 例を追記		●	
	外部でのモバイルPC又はUSBメモリ等の紛失や盗難対策実施	■ 例を追記 ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―
	モバイルPC又はUSBメモリ等を外部に持ち出し、クラウド上のストレージに際しての、その使用者の認証の実施	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―
	保存されているデータの重要度に応じたHDD暗号化又はBIOSパスワード設定等の技術的対策の実施	■ 変更なし		●	
	モバイルPC又はUSBメモリ等の持ち出しにおける持出者並びに持出及び返却の管理施	■ 変更なし		●	
	持ち出し情報の一覧及び内容の管理	■ 変更なし 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―
F）システム外部から受け取るファイルに対して、ワクチンソフト等によるチェックを実施する	システム外部からファイルを受け取る際のワクチンソフト等によるチェックの実施	■ システム外部から受け取るファイルに対するチェックについて、無害化に限定しない記載へ変更	―	―	―

2．情報セキュリティ対策　2．１安全管理措置

（２）本指針に基づく遵守すべき事項
　④　情報システムのアクセス制御並びに情報システムの開発及び保守におけるセキュリティ対策

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
A)組織内利用者毎のID及びパスワード等の認証情報の管理等	組織内利用者（システム管理者を含む）毎へのID及びパスワード等割当て、当該ID及びパスワード等による識別及び認証の実施	■ システム管理者だけでなく、組織内の利用者一般に管理等の対象を拡大 ■ 例を追記	●		
	多要素認証の実施	■ 利用者認証の安全性向上に有効な多要素認証についてのルールの重要性から追記	●		●
	（削除）~~システム管理者のID管理~~	■ 「システム管理者IDに関する規程の整備と運用」に内容を統合	―	―	―
	システム管理者IDに関する規程の整備と運用	■ 管理者IDに関する規定に関する記載を統合して追記		●	
	組織内利用者のパスワード管理・ルールの策定	■ 利用者全般を対象とした一般的なパスワードのルールが必要であることから追記		●	●
	パスワードの定期的見直し及び複雑化	■ 中項目の内容の明確化 ■ 例を追記	●	●	
	離席する際のスクリーンセーバーによるパソコンの保護	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―
	（削除）~~管理者IDの削除~~	■ 上記の「システム管理者IDに関する規程の整備と運用」に統合	―	―	―

2．情報セキュリティ対策　2．１安全管理措置

（２）本指針に基づく遵守すべき事項
④　情報システムのアクセス制御並びに情報システムの開発及び保守におけるセキュリティ対策

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
B)健診等情報に対するアクセス権限の設定を行う	健診等情報に対するアクセス管理方針の策定による組織内利用者（システム管理者を含む）毎にアクセス可能な情報、情報システム、業務アプリケーション及びサービス等の設定	■ システム管理者だけでなく、組織内利用者一般に対象を拡大 ■ 例を追記	●	●	●
	職務の変更又は異動に伴う組織内利用者（システム管理者を含む）のアクセス権限見直し	■ システム管理者だけでなく、組織内利用者一般に対象を拡大 ■ 例を追記		●	
	システム管理者のアクセス権限の適切な管理	■ システム管理者のアクセス権限に管理について必要な事項を記載するため追記	●		
C) インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング及びIPSサービス等）を行う	外部との情報転送ルールの整備	■ 事業者と、外部（利用者や他の事業者）との情報転送（例えばAPI)は、ルールに基づき実施することが必要であるため追記		●	
	不正アクセスに対するネットワーク監視	■ 外部からの攻撃を速やかに検知し対策するため、ネットワーク監視全般を適切に実施する必要があることから追記	●	●	●
	なりすまし等の不正アクセスを防止するための、外部から内部のシステムにアクセスにおける認証の実施	■ 外部からのなりすましや、アクセス先のなりすましにより、不正アクセスが生じるのを防ぐのが重要であるため、なりすましの観点を追記 ■ 例を追記		●	●

2．情報セキュリティ対策　2．１安全管理措置

（２）本指針に基づく遵守すべき事項
　④　情報システムのアクセス制御並びに情報システムの開発及び保守におけるセキュリティ対策

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
C) インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング及びIPSサービス等）を行う	保護すべき健診等情報のデータベースに対する外部接続しているネットワークからの物理的な遮断・セグメント分割の実施	■ 例を追記		●	
	不正なサイトへのアクセスを遮断（フィルタリングソフトの導入等）措置の実施	■ 例を追記	●	●	●
	適切なセッション管理による不正アクセスやアクセス制御における脆弱性への対応	■ 不正なセッションによる接続や、サービスの可用性管理のためセッション管理が重要であることから追記		●	
D)無線LANのセキュリティ対策（WPA3等の導入等）	健診等情報の通信を行う際の無線LANの暗号化通信（WPA3等）の設定	■ 現時点での最新であるWPA3及びWPA2使用時の留意事項を追記	●		
	無線LANの仕様を使用する端末（MAC認証等）及びその使用者の認証	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	ー	ー	ー

2．情報セキュリティ対策　2．1安全管理措置

（2）本指針に基づく遵守すべき事項
④ 情報システムのアクセス制御並びに情報システムの開発及び保守におけるセキュリティ対策

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
E)ソフトウェアの選定及び購入、情報システムの開発及び保守並びにサービス利用に際して、情報セキュリティを前提とした管理	情報システム設計時の安全性（情報システムの脆弱性対策含む。）の確保と継続的な見直し	■ 例を追記		●	
	サービスを提供するためのシステム（ソフトウェア及び他者が提供するクラウド等のサービス）の導入及び変更に関する手順の整備及び本指針のセキュリティ対策の遵守状況の確認	■ 中項目の内容の明確化 ■ 例を追記	●	●	
	サービスを提供するためのシステム（ソフトウェア及び他者が提供するクラウド等のサービス）を構成するプログラム及びサービス等の、規定類等に基づいた管理及び更新	■ 事業者用ガイドラインのため、サービス提供に供するシステムの構成管理が重要であるため追記		●	
	システム開発時のレビューの実施、記録	■ 例を追記		●	
	外部委託によるソフトウエア開発における使用許諾及び知的財産等の取り決めの実施	■ 例を追記		●	
	サービスを提供するためのシステム（ソフトウェア及び他者が提供するクラウド等のサービス）の保守対応手順の策定	■ 事業者用ガイドラインのため、サービス提供に供するシステム・サービスの保守管理が重要であるため追記		●	
	開発又は保守の外部委託におけるセキュリティ管理の実施状況の把握	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―

2．情報セキュリティ対策　2．1安全管理措置

（2）本指針に基づく遵守すべき事項
⑤ 情報セキュリティ上の事故対応

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
A)情報システムに障害等が発生した場合のBCP対応としての業務再開手順の整理	情報システムの障害等における、最低限運用に必要な時間及び許容停止時間の明確化	■ 障害以外の事故も含む記載に変更 ■ 例を追記		●	
	障害等対策の仕組みについての組織としての検討の実施	■ 障害以外の事故も含む記載に変更 ■ 例を追記		●	
	障害等発生時のシステムの切り離し（即応処理）、必要なサービスを提供できるような機能（縮退機能）、情報の回復及び情報システムの復旧に必要となる機能等の確認	■ 障害以外の事故も含む記載に変更 ■ 例を追記		●	
	バックアップデータ及び運用の記録等の確保	■ 例を追記	●	●	●
	サービス提供におけるシステム（電源、通信等）の冗長化対策	■ 事業者用ガイドラインのため、サービス提供に供するシステム・サービスの全体的な冗長性が重要であるため追記		●	
	障害等発生時の報告要領、障害等対策の責任者と対応体制、システム切替え及び復旧手順並びに障害等発生時の業務実施要領等の準備	■ 障害以外の事故も含む記載に変更 ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―
	関係者への障害等対応要領の周知、必要なスキルに関する教育及び訓練等の実施	■ 障害以外の事故も含む記載に変更 ■ 例を追記		●	

2．情報セキュリティ対策　2．1安全管理措置

（2）本指針に基づく遵守すべき事項
⑤ 情報セキュリティ上の事故対応

赤字：追加・修正点

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
B)情報セキュリティに関連する事件又は事故等（マルウエア感染、情報漏えい等）のBCP対応としての緊急時対応手順の整理	マルウエア感染又は情報漏えい等の発生時の組織内の関係者への報告、緊急処置の適用基準及び実行手順、被害状況の把握、原因の把握、対策の実施、被害者ほか影響を受ける可能性のある本人への通知、外部への周知方法、個人情報保護委員会への報告、通常システムへの復旧手順並びに業務再開手順等の整備	■ 例を追記		●	●
	速やかな責任者への報告及び対応体制整備	■ 情報漏えいへの対応の記載から分割するとともに、情報漏えいに限定しない記載に変更 ■ 例を追記	●	●	
	対応についての判断を行うための、5W1Hの観点での調査及び情報の整理	■ 情報漏えいへの対応の記載から分割するとともに、情報漏えいに限定しない記載に変更 ■ 例を追記	●	●	
	対策本部による対応方針の決定、被害の拡大防止及び復旧のための措置の実施	■ 情報漏えいへの対応の記載から分割するとともに、情報漏えいに限定しない記載に変更 ■ 例を追記	●		
	情報漏えいにおける通知、個人情報保護委員会及び監督官庁等への報告、公表等の検討	■ 情報漏えいへの対応の記載から分割するとともに、情報漏えいに限定しない記載に変更 ■ 例を追記	●		●
	業務上の関係者との日常的なセキュリティ情報の共有及び最新情報の収集	■ サイバー攻撃時において対応策を含むセキュリティ情報の各機関、有識者、ベンダとの共有が重要であることから追記	●	●	●

2．情報セキュリティ対策

2．１安全管理措置

（２）本指針に基づく遵守すべき事項
⑥外的環境の把握

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
A)外国において個人データを取り扱う場合における、個人データの安全管理のために必要かつ適切な措置の実施	外国において個人データを取り扱う場合における、個人データの安全管理のために必要かつ適切な措置の実施	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―

2．２．第三者認証の取得

大項目	中項目	対応方針	引用元ガイドライン		
			中小GL※1	ｸﾗｳﾄﾞGL※2	NISC GL※3
(1)指針に基づく遵守すべき事項	標準規格（ISO又はJIS）等に準拠した対策の追加及び第三者認証（ISMS又はプライバシーマーク等）を取得義務	■ 変更なし ■ 最新の引用元ガイドラインに、対応する記載は明記されていないが、重要性から記載を維持	―	―	―