資料６

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

第32回　健康・医療・介護情報利活用検討会

医療等情報利活用ワーキンググループ

2026（令和８）年５月29日

令和８年度版 医療機関等におけるサイバーセキュリティ対策チェックリストについて（案）

厚生労働省　医政局

医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

令和８年度版　サイバーセキュリティ対策チェックリスト

○　厚生労働省においては、令和５年４月から、医療法施行規則を改正して医療法に基づく医療機関に対する立入検査に、サイバーセキュリティ対策の項目を位置付けており、「医療情報システムの安全管理に関するガイドライン」（以下「ガイドライン」という。）のうち、優先的にに取り組むべき重要な項目を「医療機関におけるサイバーセキュリティ対策チェックリスト」等（以下「チェックリストという。）により示している。（薬局については同様に薬機法施行規則を改正して対応）

○　これまで、薬局確認用は別途作成していたところ、項目も一致しているため、本改定より「医療機関確認用」と「薬局確認用」を統合し、「医療機関等確認用」とした。

○　今般のガイドライン改定を踏まえ、チェックリストについて、必要な改定を行う。

○　また、システム・サービス供給事業者等に対するサイバー攻撃が続いており、医療の安定的な提供のため、サプライチェーンリスクに関連する事業者確認項目等も追加する。

主な修正点（案）

【ガイドライン改定に伴う変更】

・二要素認証の対象を明確化（サーバＯＳログイン・端末のアプリケーションログイン等）

・パスワード要件の見直し

- 英数字混在８桁以上。（二要素認証採用までの間は13桁以上）
- 記号混在要件と定期変更要件の撤廃

【その他の変更】

・事業者確認用に事業継続計画（ＢＣＰ）策定項目を追加（一部文言修正）

・事業者確認用の一部項目に「対象外」の選択肢を追加

（注）各項目の詳細についてはサイバーセキュリティ対策チェックリストマニュアル等を適宜修正。

令和８年度版　サイバーセキュリティ対策チェックリスト（医療機関確認用）

*立入検査時、本チェックリストを確認します。令和8年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*「いいえ」の場合、令和8年度中の対応目標日を記入してください。

	チェック項目	確認日
1 体制構築	①医療情報システム安全管理責任者を設置している。	はい・いいえ （　/　）
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**	
	①サーバ、端末~~PC~~、ネットワーク機器の台帳管理を行っている。	はい・いいえ （　/　）
	②リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。	はい・いいえ （　/　）
	③事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。	はい・いいえ （　/　）
	④利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。※管理者権限対象者の明確化を行っている	はい・いいえ （　/　）
	⑤退職者や使用していないアカウント等、不要なアカウントを削除または無効化している。	はい・いいえ （　/　）
	⑥セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ （　/　）
	⑦パスワードは英数字の混在した8桁以上としている。※二要素認証を採用するまでの期間は13桁以上としている	はい・いいえ （　/　）
	⑧パスワードの使い回しを禁止している。	はい・いいえ （　/　）
	⑨USBストレージ等の外部記録媒体や情報機器に対して接続を制限している。	はい・いいえ （　/　）
	⑩バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ （　/　）
	~~二要素認証を実装している。または令和９年度以降初回のシステム更新時に実装予定である。~~	はい・いいえ （　/　）
	端末~~PC~~について、以下を実施している。	
	⑪アプリケーションログイン時の二要素認証を実装している。または令和９年度以降初回のシステム更改時に実装予定である。	はい・いいえ （　/　）
	サーバについて、以下を実施している。	
	⑫OSログイン時の二要素認証を実装している。または令和９年度以降初回のシステム更改時に実装予定である。	はい・いいえ （　/　）
	⑬アクセスログを管理している。	はい・いいえ （　/　）
	ネットワーク機器について、以下を実施している。	
	⑭接続元制限を実施している。	はい・いいえ （　/　）
3 インシデント発生に備えた対応	①インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ （　/　）
	②インシデント発生時に診療を継続するために必要な情報を検討し、バックアップを確保のうえ、復旧手順を確認している。	はい・いいえ （　/　）
	③サイバー攻撃の想定を含む事業継続計画（BCP）を策定している。	はい・いいえ （　/　）
4 規程類の整備	①上記1-3のすべての項目について、具体的な実施方法を運用管理規程等に定めている。	はい・いいえ （　/　）

※目標日・備考欄を省略して表示

令和８年度版　サイバーセキュリティ対策チェックリスト（事業者確認用）

＊以下項目は令和8年度中にすべての項目で「はい」または「対象外」にマルが付くよう取り組んでください。

・「はい」：医療機関等との保守契約範囲に含まれる項目であり、事業者側の責任で対応できていることを指します。
・「いいえ」：医療機関等との保守契約範囲に含まれる項目であるが、事業者側が対応できていない項目となります。
　事業者としての令和8年度中の対応目標日を記入してください。
・**「対象外」：医療機関等との保守契約範囲外となり、当該項目の責任を医療機関等が負います。**
　医療機関等に対して、責任分界の認識齟齬がないか、事業者側から必ず確認して下さい。

	チェック項目	（日付） 確認日
1 体制構築	①事業者内に、医療情報システム等の提供に係る管理責任者を設置している。	はい・いいえ （　/　）
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**	
	②リモートメンテナンス（保守）している機器の有無を医療機関等に伝えた。	はい・いいえ （　/　）
	③医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出した。	はい・いいえ （　/　）
	④利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。※管理者権限対象者の明確化を行っている。	はい・いいえ・対象外 （　/　）
	⑤退職者や使用していないアカウント等、不要なアカウントを削除または無効化している。	はい・いいえ・対象外 （　/　）
	⑥セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ・対象外 （　/　）
	⑦パスワードは英数字の混在した8桁以上としている。※二要素認証を採用するまでの期間は13桁以上としている。	はい・いいえ （　/　）
	⑧パスワードの使い回しを禁止している。	はい・いいえ （　/　）
	⑨USBストレージ等の外部接続機器や情報機器に対して接続を制限している。	はい・いいえ・対象外 （　/　）
	⑩バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ・対象外 （　/　）
	~~二要素認証を実装している。または令和９年度までに実装予定である。~~	はい・いいえ （　/　）
	端末~~PC~~について、以下を実施している。	
	⑪アプリケーションログイン時の二要素認証を実装している。または令和９年度以降初回のシステム更改時に実装予定である。	はい・いいえ （　/　）
	サーバについて、以下を実施している。	
	⑫OSログイン時の二要素認証を実装している。または令和９年度以降初回のシステム更改時に実装予定である。	はい・いいえ （　/　）
	⑬アクセスログを管理している。	はい・いいえ・対象外 （　/　）
	ネットワーク機器について、以下を実施している。	
	⑭接続元制限を実施している。	はい・いいえ・対象外 （　/　）
3 インシデント発生に備えた対応	⑬サイバー攻撃の想定を含む事業継続計画（BCP）を策定している。	はい・いいえ （　/　）

※目標日・備考欄を省略して表示

令和８年度版　サイバーセキュリティ対策チェックリスト
その他の変更①　BCP策定の項目追加

背景

○　昨今、システム・サービス等の供給事業者へのサイバー攻撃によるサプライチェーンリスクが高まっており、サイバー攻撃は100%防ぐことが可能ものではない。

○　これを受け、医療の安定的な提供のためには、医療情報システムを提供する事業者においても、BCPを策定することでサービス提供レベルを担保すべきと考えられ、医療機関確認用のみならず、事業者確認用チェックリストにおいても、BCP策定の項目を追加した。

○　また、従来の「サイバー攻撃を想定した」という表現では、自然災害等に起因する事業継続計画（BCP）が含まれないと受け取られる可能性があるとのご指摘を受け、「サイバー攻撃の想定を含む」に変更した。

方針

○「サイバー攻撃の想定を含む事業継続計画（BCP）を策定している。」の項目を追加する。

令和８年度版　サイバーセキュリティ対策チェックリスト
その他の変更②　「対象外」の選択肢の追加

背景

○　これまでの事業者確認用チェックリストには「はい」、「いいえ」の2つの選択肢のみであった。しかし、例えば「退職者や使用していないアカウント等、不要なアカウントを削除している」のような、医療機関等が実施している場合もある項目が複数含まれている。

○　この場合、事業者がどのように記載すべきか不明確であるだけでなく、「事業者側が項目を遵守している」と医療機関等が誤認するリスクもある。

○　これらの問題を解消するため、事業者側の責任とならない可能性のある一部の項目について、「対象外」の選択肢を追加する。
　さらに、事業者側が「対象外」を選択した項目については、医療機関等が責任を負うことが明示され、事業者と医療機関等の間で責任分界の認識齟齬の発生を防ぐ効果も期待される。

方針

○　一部項目に「対象外」の選択肢を追加する。

- 2-④ アクセス利用権限の設定
- 2-⑤ 不要なアカウントの削除または無効化
- 2-⑥ セキュリティパッチの適用
- 2-⑨ 外部接続機器や情報機器に対する接続制限
- 2-⑩ 不要なソフトウェア及びサービスの停止
- 2-⑬ アクセスログの管理
- 2-⑭ 接続元制限の実施