資料2－1

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

第24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
2025（令和7）年3月13日

令和7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
特定医薬品開発支援・医療情報担当参事官
Ministry of Health, Labour and Welfare of Japan

令和7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

・厚生労働省においては、令和５年４月から、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から特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）

・一部内容を改定し、**令和７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**及び**サイバーセキュリティ対策チェックリストマニュアル**を発出する予定。

主な修正点（案）

【追加項目】

・パスワードの桁数の規定、使い回しの禁止

・USBストレージ等の外部接続機器に対しての接続制限

・二要素認証の実装（令和９年度実装に向けた対応）

・運用管理規程等の整備

【その他修正】

・アクセス利用権限の設定について、管理者権限の対象者を明確化しているかを注記

・セキュリティパッチの項目等、端末PC・サーバ・ネットワーク機器等それぞれに求めていた項目を「医療情報システム全般」についての質問へ統合

※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記載する。

令和7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

令和７年度版
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

*立入検査時、本チェックリストを確認します。令和7年度中にすべての項目で「はい」にマルが付く
*「いいえ」の場合、令和7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	医療情報システム安全管理責任者を設置している。(1-①)	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。**	
	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。(2-①)	はい・いいえ （　/　）
	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。(2-②) ※事業者と契約していない場合には、記入不要	はい・いいえ （　/　）
	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。(2-③) ※事業者と契約していない場合には、記入不要	はい・いいえ （　/　）
	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(2-④)	はい・いいえ （　/　）
	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。(2-⑤)	はい・いいえ （　/　）
	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。(2-⑥)	はい・いいえ （　/　）
	パスワードは英数字、記号が混在した8桁以上とし、定期的に変更している。※二要素認証、または13桁以上の場合は定期的な変更は不要(2-⑦)	はい・いいえ （　/　）
	パスワードの使い回しを禁止している。(2-⑧)	はい・いいえ （　/　）
	USB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。(2-⑨)	はい・いいえ （　/　）
	二要素認証を実装している。または令和９年度までに実装予定である。(2-⑩)	はい・いいえ （　/　）
	サーバについて、以下を実施している。	
	アクセスログを管理している。(2-⑪)	はい・いい （　/　）
	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。(2-⑫)	はい・いい （　/　）
	端末PCについて、以下を実施している。	
	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。(2-⑫)	はい・いい （　/　）
	ネットワーク機器について、以下を実施している。	
	接続元制限を実施している。(2-⑬)	はい・いい （　/　）
3 インシデント発生に備えた対応	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。(3-①)	はい・いい （　/　）
	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、データやシステムのバックアップの実施と復旧手順を確認している。(3-②)	はい・いいえ （　/　）
	サイバー攻撃を想定した事業継続計画（BCP）を策定している。(3-③)	はい・いい （　/　）
4 規程類の整備	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。(4-①)	はい・いい （　/　）

※薬局用・事業者確認用においても同様に改訂
※目標日・備考欄を省略して表示

パスワードの適切な管理・設定について

背景

実際にサイバー攻撃の被害を受けた過去の事例においても、ネットワーク機器やサーバのパスワードが容易に推測可能なものや文字列が短かった例が繰り返し確認されている。
また、昨年発生したサイバー攻撃でもVPN装置をはじめとした医療機関内の**システム、ネットワーク機器、サーバ等のパスワードが共通（使い回し）にされていた**など、不適切なパスワードの設定・管理が被害拡大の要因であった事が判明した。

方針

- パスワードを強固なものに変更し、使い回しをしないよう適切な管理・設定を求める。
- 事業者確認用の項目においては、事業者側の管理のみではなく、医療機関に導入したサーバ、ネットワーク機器についても確認する。

〈強固なパスワードとは〉

- 長く、複雑で、推測困難
- 13 桁以上（桁数が多いほど、機械的な総当たりでの解析が困難）
- 英数字、大文字・小文字、記号が混在（組み合わせが多いほど解析が困難）
- ランダムな文字列（単語等の組み合わせによる解析を回避）
- 複数の機器や外部サービス等で、同一のパスワードを設定しない

〈危険なパスワード使い回し例〉

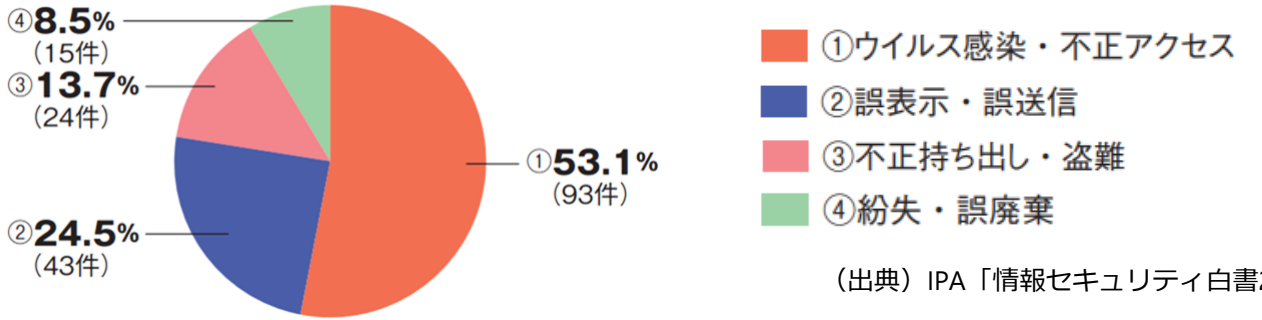
- 施設内のサーバ、ネットワーク機器等に同一のパスワードを用いている
- 事業者が契約している個別の施設に対して同一のパスワードを用いて管理している
- 出荷時のパスワードから変更を行っていない

USBストレージ等の外部接続機器に対しての接続制限について

背景

- **<u>部門システム等のPCにUSBストレージ経由でマルウェアが侵入</u>**し、他の部門の医療機器等にマルウェア感染が広がり、診療業務へ影響を及ぼす等の事例も過去に生じている。
- 医療従事者が臨床研究のために患者診療データの一部を保存したUSBストレージ等を紛失したり、USBストレージ等で持ち出したデータを保存した個人所有の端末PCがサイバー攻撃を受けることで、個人情報の漏えい事故が後を絶たない状況となっている。
- 情報漏えいの原因は外部からの不正アクセス、操作ミス等の過失、内部者の故意による持ち出し等の内部不正、不適切な情報の取り扱い等と続いており、半数程が職員の過失に起因している。（図１参照）

図１.個人情報漏えい・紛失事故の原因別内訳



（出典）IPA「情報セキュリティ白書2024」

方針

USBストレージ等の外部接続機器に対する接続制限に関する確認を求める。業務の必要性に応じて**<u>外部接続機器を利用する場合には、記録媒体及び記録機器の保管及び取扱い(※)について、適切に行う</u>**よう関係者に周知徹底するとともに、その利用にあたって教育を実施することが必要となる。

※ 例えば病院の情報システム部門が管理する特定の記録媒体以外の読み込みを不能とし、利用前の記録媒体のウイルススキャンや利用後の初期化を行う等の対策が想定される。

二要素認証の実装、規程類の整備について

二要素認証の実装に向けて

背景

医療情報システムの安全管理に関するガイドラインにおいて、**令和９年度時点で稼働していることが想定される医療情報システム**を、新規導入、又は更新するに際しては、**二要素認証を採用するシステムの導入**、又はこれに相当する対応を行うことを求めている。

方針

- 端末等への実装を促してきた二要素認証技術について、予定を確認して円滑に導入が進むよう項目に追加する。

〈認証に用いる要素〉
  - ID・パスワードの組み合わせのような利用者の「記憶」に よるもの
  - 指紋や静脈、虹彩のような利用者の生体的特徴を利用した「生体情報」によるもの
  - IC カードのような「物理媒体」によるもの

- 医療情報システムの次期更新時に向けて、二要素認証導入について確認を行う。
- 事業者においても、医療情報システムの次期更新に合わせた二要素認証導入について、医療機関等への情報提供を行う。

規程類の整備

医療情報システムの安全管理が適切に行われるためには、組織内において明文化されたルールを定めた運用管理規程の整備が重要である。サイバーセキュリティ対策チェックリストにおいても、運用管理規程の整備状況についても項目を追加する。