令和7年度医療情報セキュリティ研修
及びサイバーセキュリティインシデント発生時初動対応支援・調査等事業

立入検査研修
準備コース

2025年7月9日

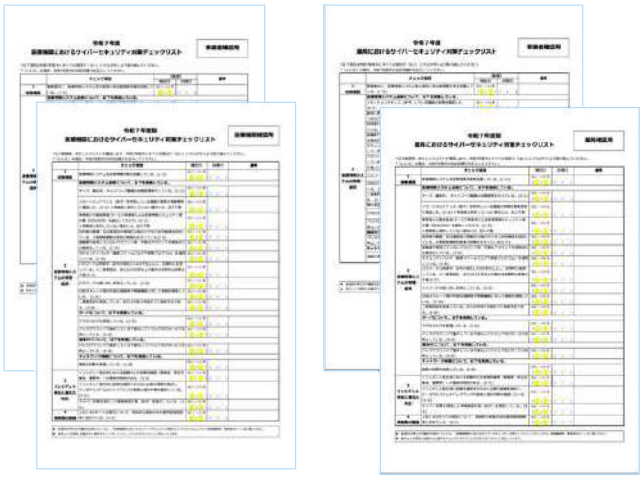
一般社団法人ソフトウェア協会

目次

チェックリスト概要

「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

1. 医療機関等におけるサイバーセキュリティ対策については、「医療情報システムの安全管理に関するガイドライン」を参照の上、適切な対応を行う必要があります。
2. このうち医療機関が**優先的に取り組むべき事項**をチェックリストとしてまとめられています。
3. このチェックリストによってサイバー攻撃を回避できると約束されるものではありません。
4. 令和５年度より、本チェックリストが医療法第25条第１項に基づく立入検査においてサイバーセキュリティ確保のために必要な取組を行っているかの確認に使用されています。



サイバーセキュリティの実効性を高める

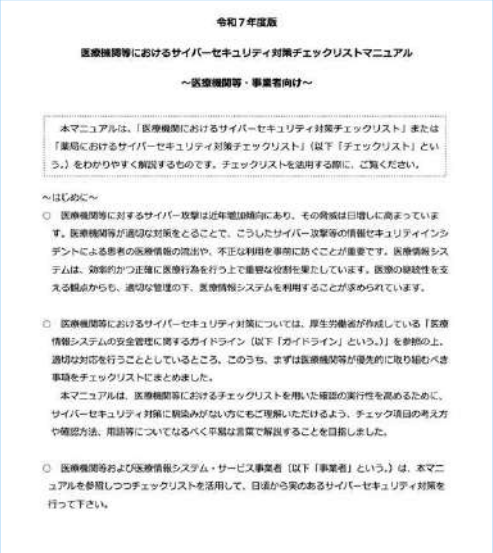
医療DX推進環境を整え医療の向上を図る

医療情報システムの安全管理に関するガイドライン
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
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

「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マニュアル」

1. 医療機関等におけるチェックリストを用いた確認の実効性を高めるために、チェックリスト マニュアルが作成、公開されています。
   医療機関、薬局及び関連する情報システム・サービス事業者は、本マニュアルを参照しつつチェックリストを活用して、サイバーセキュリティ対策を行ってください。

2. 令和7年度版でチェックリストおよびマニュアルが更新されていますので見落としが無いようご注意ください。



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マニュアル

～医療機関等・事業者向け～

本マニュアルは、「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」または「薬局におけるサイバーセキュリティ対策チェックリスト」（以下「チェックリスト」という。）をわかりやすく解説するものです。チェックリストを活用する際に、ご覧ください。

～はじめに～

○ 医療機関等に対するサイバー攻撃は近年増加傾向にあり、その脅威は日増しに高まっています。医療機関等が適切な対策をとることで、こうしたサイバー攻撃等の情報セキュリティインシデントによる患者の医療情報の流出や、不正な利用を事前に防ぐことが重要です。医療情報システムは、効率的かつ正確に医療行為を行う上で重要な役割を果たしています。医療の継続性を支える観点からも、適切な管理の下、医療情報システムを利用することが求められています。

○ 医療機関等におけるサイバーセキュリティ対策については、厚生労働省が作成している「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。）」を参照の上、適切な対応を行うこととしているところ、このうち、まずは医療機関等が優先的に取り組むべき事項をチェックリストにまとめました。
本マニュアルは、医療機関等におけるチェックリストを用いた確認の実行性を高めるために、サイバーセキュリティ対策に馴染みがない方にもご理解いただけるよう、チェック項目の考え方や確認方法、用語等についてなるべく平易な言葉で解説することを目指しました。

○ 医療機関等および医療情報システム・サービス事業者（以下「事業者」という。）は、本マニュアルを参照しつつチェックリストを活用して、日頃から実のあるサイバーセキュリティ対策を行って下さい。

医療情報システムの安全管理に関するガイドライン
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マニュアル
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

現物確認を求める文書等

マニュアルでも示されている通り、以下の文書は立入検査時に現物確認できるよう準備してください。

- 機器台帳　（２-①）
- インシデント発生時の連絡体制図　（３-①）
- 事業継続計画（BCP）　（３-③）
- 運用管理規程等の規程類　（４）

チェックリスト準備の進め方

チェックリストの準備対応、進め方（サマリー）

用意

- 医療機関は「医療機関確認用」を使用してください。薬局向けには「薬局確認用」が用意されています。
- 事業者には「事業者確認用」への記入を求め、回収してください。（１事業者で複数システム提供されている場合は総合してください。）
- 「事業者確認用」については、事業者との契約がない場合は不要です。

記入

- 「はい」または「いいえ」に〇をつけて確認した日を記入してください。
- もし「いいえ」の場合は、対策の実施にかかる令和７年度中の目標日を記入するようにしてください。
- チェック項目の対象となるものが無いことが明らかな場合は、「いいえ」とした上で、備考に対象外と明記してください。
- システムリプレースを要するなど、対策に数ヶ年を要する場合は、改善計画について説明できるものを準備し、備考に記入してください。

確認

- 回収した事業者向けの全てのリストを確認し、記入内容に相違が無いか確認してください。
- 医療機関確認用における回答は各項目それぞれについて施設全体を総合してください。
  （確認対象が複数システムあれば、1つでも満たさないものがあれば『いいえ』を選択してください）

提出

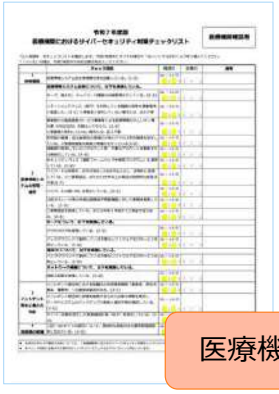
- 提出方法は書面現物か、デジタルデータとするか、所管保健所の指示に従い対応してください。
- 提出タイミングは、事前か、検査当日か、後日か、所管保健所の指示に従い対応してください。

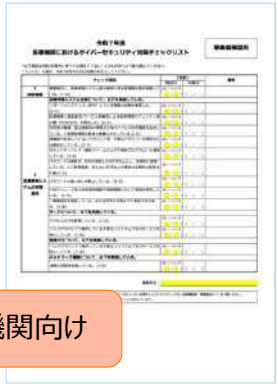
チェックリストの掲載先

医療情報システムの安全管理に関するガイドライン　第6.0版（令和5年5月）
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

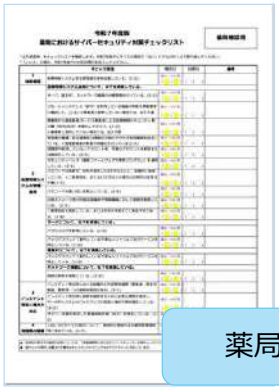
シートの用意

- 医療機関は「医療機関確認用」を、事業者は同ファイル２ページ目、「事業者確認用」を使用してください。
- 薬局は「薬局確認用」を、薬局向け事業者は同ファイル２ページ目に「事業者確認用」が用意されています。
- それぞれPDF版とExcel版が公開されていますので、使用、管理しやすい方をお使いください。





医療機関向け



薬局向け

システムを提供している事業者ごとに確認、協力を求めてください。

「事業者確認用」については、
製品購入の売買契約のみで、運用又は管理・保守に関する契約等がない場合は不要です。

事業者の皆様は医療機関からの協力要請に対してご協力をお願いします。

シートの記入

「はい・いいえ」を選択し、
確認日を記入してください。

対象となるものが無いことが明らかな場合は、「いいえ」とした上で、備考に対象外と明記してください。

システムリプレースを要するなど、対策に数ヶ年を要する場合は、改善計画について説明できるものを準備し、備考に記入してください。

「いいえ」の場合は、チェック項目内容を満たす「目標日」を記入してください。

各項目の対応状況を担当部門に確認し、総合して評価してください。

多数の事業者からシステム提供を受けている場合は、医療機関として全体を総合して評価してください。

確認

事業者確認用シート

事業者からの回収　記入内容の確認

医療機関確認用シート

薬局確認用シート

複数システムを総合した回答とする

証跡は必要か？

- 回答の根拠となる文書やデータを求められれば提示できるように準備しましょう。

一部のシステムで実施できていない場合は？

- 「はい」は、対象となる「医療情報システム」全てにおいて、網羅的に確認ができた状態を示します。**一部でも対応できていない場合は「いいえ」を選択**し、対応する期日を記載しましょう。
- 備考欄には「いいえ」となっている理由について記載してください。
- **前年度から合理的な理由なく改善が行われていないと認められる場合、口頭指導にとどまらず、文書指導や改善命令となる可能性があります。**

年度をまたぐ中長期対応が必要な場合

- **システム更改が不可欠になる場合など、長期間に渡る対応が必要になるものは、システム更改の中で予定する改善計画を説明できるよう準備してください。**

事業者から提出されてこない場合は？

- 回答が得られない理由をメールや文書などで求めてください。

提出

提出方法	提出タイミング
書面(紙)	事前
デジタルデータ	検査当日
	後日

所管保健所の指示に
従い対応してください

用語解説

医療情報システム
管理者権限　（2-④）
パスワードの安全性（2-⑦）
パスワードの使い回し（2-⑧）
二要素認証（2-⑦、2-⑩）
USBストレージ、外部記憶媒体（2-⑨）
運用管理規程（4-①）

令和6年度研修・準備コースにて解説した用語

医療情報システム安全管理責任者	サーバ　端末PC ネットワーク機器	リモートメンテナンス（保守）	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）
アカウント	アクセス利用権限	退職者、使用していないアカウント、不要なアカウント	アクセスログ
ソフトウェア脆弱性	セキュリティパッチ ファームウェア 更新プログラム	バックグラウンド	不要なソフトウェア及びサービス
接続元制限	インシデント	バックアップ	事業継続計画（BCP）

適宜アーカイブをご参考ください

医療情報システム

医療情報とは？

- 医療に関する患者情報（個人識別情報）を含む情報。

医療情報システムとは？

- 医療情報を保存するシステムだけではなく、医療情報を扱う情報システム全般
  サーバ、端末PC（≒エンドポイント,医療機器）、ネットワーク機器等を含む。

システムの例

1. レセコン
2. 電子カルテ
3. オーダリングシステム

マニュアルにも例示

4. 調剤システム、臨床検査システム等、各種部門システム
5. PDI作成装置、インポート装置
6. 各種撮影装置、検査装置（※）
7. レポートシステム、遠隔画像診断システム

医療情報が発生するもの
医療情報を参照するもの

8. オンライン資格確認端末
9. 医事会計システム
10. 予約システム
11. 受付機・精算機
12. 受付案内表示システム

患者の個人情報、
患者個人識別情報に紐づくもの

1. これらシステムを構成する機器およびそこで動作するソフトウェアは全て安全管理の対象です
   - PC
   - サーバ
   - ストレージ
   - テープ装置、外部ディスク装置
   - タブレット、携帯端末
   - モニター
   - ネットワーク機器
     （ファイアウォール、スイッチ、ルータ、VPNルータ　等）
2. インターネットへの接続の有無は関係ありません
3. 製品化されたシステムではなく、内製したシステムや、汎用のソフトウェアなどを使用して医療情報を扱う業務を行っている場合も対象となります

※薬機法上の「管理医療機器」であっても、サーバや他の端末等と連携して動作する情報システムの側面を持つものは対象として考える必要があります

アカウント

システムにおいて、アカウント管理は構成ごとに異なることが多くなります。
それぞれのアカウント情報の趣旨とあわせて、混同しないよう整理、管理する必要があります。

サーバのアプリケーション機能を利用する際の「アカウント」
→電子カルテ　メールサーバ　ECサイト　ネットバンク　など

サーバ/アプリケーション　アカウント登録状況

ID名	役割	アカウント種別	使用者
systemadmin	システム管理者	管理者	IT管理部門メンバー
d0200123	医師	医師	XX先生
n0220246	看護師	看護師	YYさん

PCへログインする「アカウント」
→　ユーザーID　利用者ID

端末PC/OS　アカウント

ID名	役割	Windows アカウント種別	使用者
Administrator	システム管理者	管理者	IT管理部門メンバー
user	一般利用者	標準ユーザー	一般職員

サーバ/OS　アカウント登録状況

ID名	役割	Windows アカウント種別	使用者
Administrator	システム管理者	管理者	IT管理部門メンバー
user	一般利用者	標準ユーザー	一般職員

サーバのOS機能を利用する際の「アカウント」
→　実際は端末PCからネットワーク越しに使用することが大半なので
サーバ自体に個別の利用者IDは登録されていないことが多い
ファイル共有サーバ　プリントサーバ　など

医療関係では端末OSへ「自動ログイン」することでOSのアカウントを意識させないシステムが多く存在します

アクセス利用権限

誰が、どの情報に、何ができるかを決めるルール

目的

- 誰がどの情報を操作したか、責任の所在を明確にする（真正性）
- 重要な情報に、関係のない人がアクセスしてしまうのを防ぐ（機密性）
- 不正な操作を防ぎ、システムやデータの正確性、トレーサビリティを確保する（完全性）

電子カルテをイメージした例	記事入力	病名	検査結果	処方オーダ
 システム管理者	○ 入力可能	○ 入力可能	△ 閲覧のみ	○ 入力可能
 医師	○ 入力可能	○ 入力可能	△ 閲覧のみ	○ 入力可能
 看護師	○ 入力可能	△ 閲覧のみ	△ 閲覧のみ	△ 閲覧のみ
 医事事務員	○ 入力可能	△ 閲覧のみ	△ 閲覧のみ	× 閲覧不可

医療情報システムにおけるイメージ

管理者権限　（2-④）

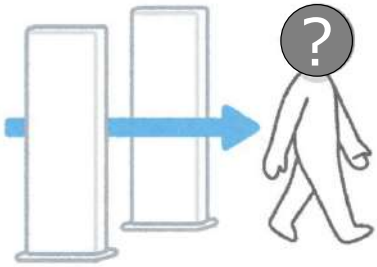
- 「アカウント」で許可される操作範囲や操作内容を「権限」という形で定義しています。
- 一般ユーザー権限では利用者自身のフォルダ、ファイルの操作や、許可されたシステム内のプログラム、機能等が利用可能です。
- 「管理者権限」はシステム内の操作に関して「全ての制御」可能なので、「特権」と言い換えることもできます。
  無知、悪意に関係なく誤った操作、不正な操作もできてしまうため、管理者権限付与は慎重であるべきものです。

管理者権限（特権）を必要とする主な操作	一般ユーザー権限での主な操作
• OS設定の変更（OSアップデート・セキュリティ設定変更）	• [不可] 管理者権限が必要な操作
• ユーザーアカウント管理（追加・削除）	• [不可] OSや他ユーザー設定の変更
• アプリ・ソフトのインストール／削除	• [不可] アプリ・ソフトのインストール／削除
• システムログの閲覧・変更	• ユーザー自身所有のファイルの操作（作成・編集）
• 全ファイル・全フォルダへのフルアクセス	• 共有、権限付与されたファイルの操作
	• 許可されたアプリの使用
	• 登録されたプリンタやネットワークの利用

管理者権限が設定されたユーザーで通常業務を行う設計のシステムは、
セキュリティレベルが低いため推奨されません。（医療システム等に多い問題です）

退職者、使用していないアカウント、不要なアカウント（2-⑤）

退職された方がそのままIDを保持していたら？



放置	• 入館ゲートを通過 • 不正侵入を誘発
削除	• 入館ゲートでブロック • 過去の記録との名寄せ確認ができない
無効化	•入館ゲートでブロック •過去の記録との名寄せ確認が可能になる •個人情報の保有期限に考慮が必要となる場合も

サーバアプリケーションの管理設定で、アカウントの削除や無効化する機能が備わっているはずです。

認証とパスワード

パスワードは何のため？

その人が本人かどうかを確かめる手法　＝　認証

認証は何のため？

本人識別の確実化

- 有効な利用者であることを確認できる
- 不正アクセス、なりすましを防止できる
- [例] ログイン・ATMでの引き出しなど

責任所在の明確化

- 誰が、いつ、何をしたか・・・記録をもって証明できる
- [例] 実施記録・通過記録

認証の条件

知識要素（記憶）

- 本人だけが知っていること
- [例] パスワードや秘密の質問など

所有要素（物理媒体）

- 本人だけが持っている物
- [例] ICチップ入りカード、マイナンバーカードや スマートフォンなど、電子証明書との関連付け

生体要素（生体計測）

- 本人固有の身体的特徴
- [例] 指紋、静脈、虹彩、顔など

パスワードの安全性（2-⑦）

安全ではないパスワード

簡単なパスワード

- 連番や繰り返し（123456　111111）
- 単語そのまま（admin　password）
- キーボードの配列 （qwertyuiop　qazwsx）
- 短い文字列（abc001　pw01）
- 生年月日や名前（19800501　taro）

特定されたパスワード

- パスワード解析で当てられたもの
- 外部に流出したもの

パスワードの安全性（2-⑦）

一般的に安全と言われるパスワード

簡単なパスワードを設定しない

- [NG] 規則的な数字、文字列
- [NG] 予測しやすいパスワード
- [NG] 複数サービスで同じパスワード

予測されない文字列を採用する

- 「安全ではないパスワード」を使わず、予測されない文字列を使用することが推奨されます
- 複雑化によって記憶しにくくなると、書き留めたり安全でない方法で記録する可能性が高まります

できるだけ長さを確保する

- パスワードの文字数が増えると解読が困難となり、長ければ長いほど良いとされています

定期的な変更をしない

- 以前は推奨されていましたが、頻繁に変更すると覚えやすい簡単な設定が増え危険なため、現在は推奨されていません
  - 前述の条件を全て満たすことが前提です
  - 不正アクセス等、漏えいがあった際には変更する必要があります

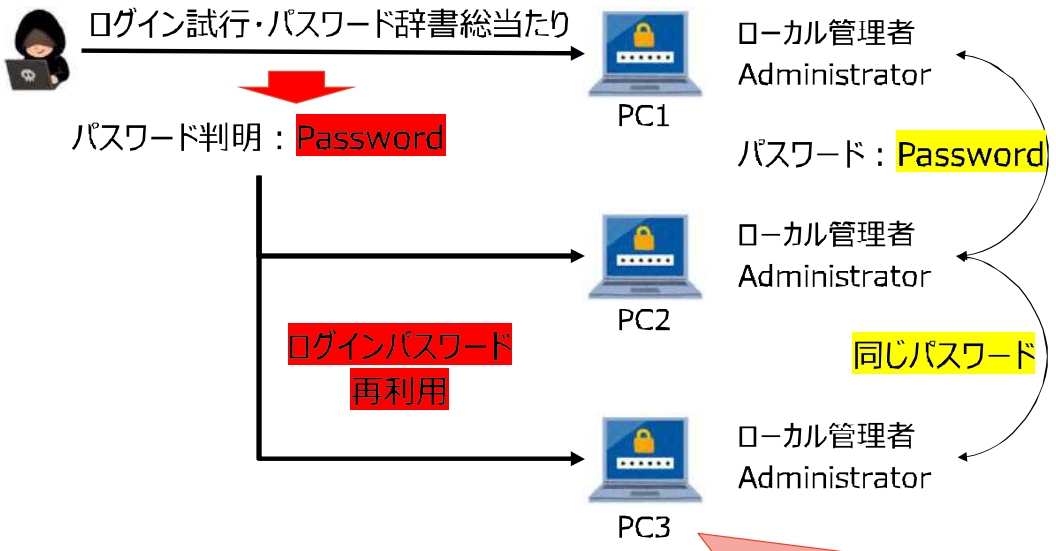
参考　NIST SP800-63B　Authentication and Lifecycle Management
付録 A―記憶シークレットの強度

パスワードの安全性（2-⑦）

本チェックリストのマニュアルで示されている強固なパスワードの例

- 英数字、記号を混在させた13 文字以上の推定困難な文字列
- 英数字、記号を混在させた８文字以上の推定困難な文字列を定期的に変更させる
- 二要素以上の認証の場合、英数字、記号を混在させた８文字以上の推定困難な文字列
- 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

パスワードの使い回し（2-⑧）

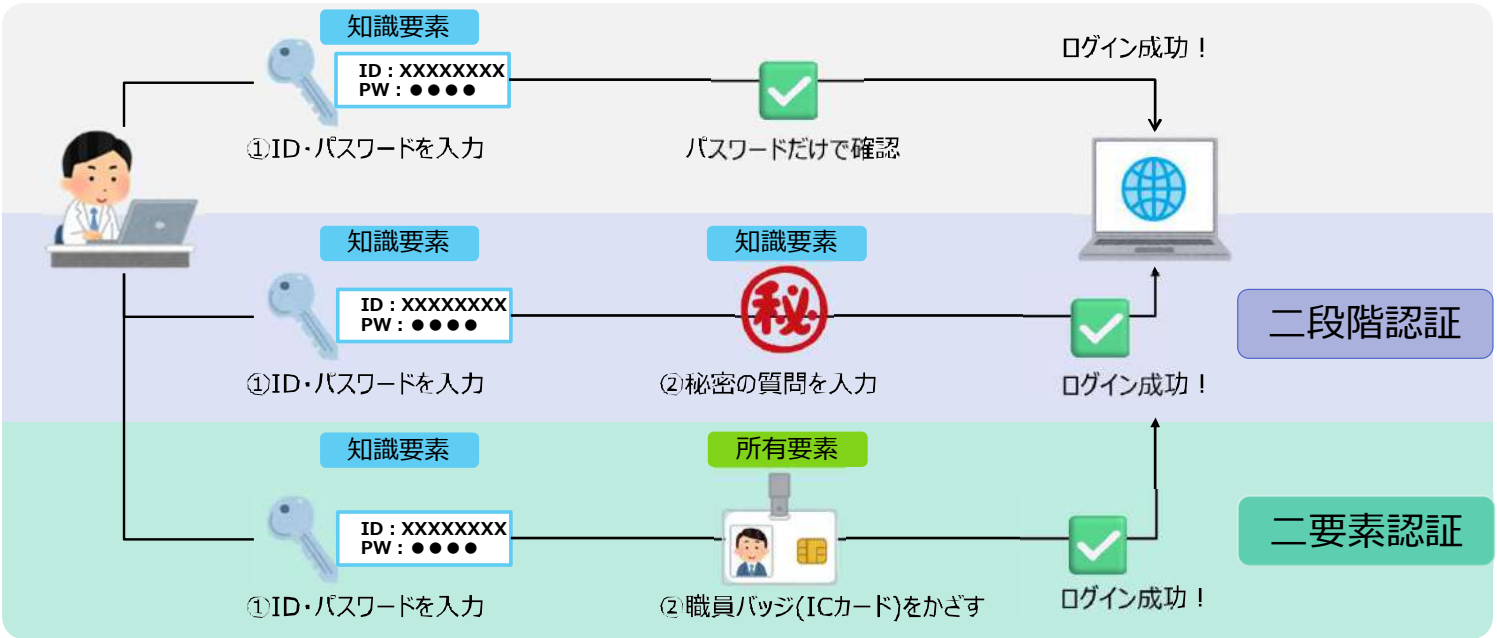


アクセス対象がWebサイトなどの外部サービスでも同様。
パスワード使い回しによる不正ログイン被害は多い。

同じパスワードを設定してしまう主な原因

- 同設定のPCを効率よく量産する
- 異なるパスワードを設定することで管理者のトラブルが増える

二要素認証（2-⑦、2-⑩）



USBストレージ、外部記憶媒体（2-⑨）

種類	例	特徴	主な用途
USBメモリ	フラッシュメモリ型USBスティック 	小型・軽量で持ち運びに便利。 書き換え可能。 セキュリティ機能付き(ウイルス対策機能、暗号化機能等)モデルもあり。	個人利用、 データの一時移動
外付けHDD （ハードディスク）	USB接続の外付けハードディスク 	大容量（TB単位）、衝撃に弱い。 比較的安価。 セキュリティ機能付きモデルもあり。	持ち運び、バックアップ、 映像・大量データ保存
外付けSSD	ポータブルSSD 	高速・静音・耐衝撃性に優れる 比較的高価。	持ち運び、 データ保存
光学ディスク	CD/DVD/BD（ブルーレイ） 	書き換え回数は少ないが 長期保存に向く。互換性に注意。	メディア配布、 アーカイブ保存
SDカード・ microSDカード	各種メモリカード 	小型でカメラ・スマホなどに利用。 転送速度や容量に差あり。	撮影データ保存、 カメラ/モバイル機器
磁気テープ	LTO（Linear Tape-Open） 	長期保存に強く大容量(TB～PB)。 読み書きに時間がかかる。	企業システムのバックアップ、 アーカイブ

運用管理規程（4-①）

- 運用管理規程は、システムを安全かつ安定的に運用するために、日常の管理業務や手順、責任分担を明確にすることを目的としています。内部監査などによる順守状況の確認や見直しを行うことで、継続的な運用改善が可能になります。

規程名※	想定される主な内容
組織規程	組織のセキュリティ基本方針
個人情報保護規程	個人情報の取扱いルール
運用管理規程	システム運用の実務ルール
人事・権限規程	アカウントや役職権限管理
情報管理に関する規程	情報資産の分類・取扱い
資産管理に関する規程	PC・サーバ・媒体の管理ルール
監査に関する規程	セキュリティ等規程の運用状況の定期点検と改善

※医療情報システムの安全管理に関するガイドライン企画管理編「４．２ 規程の整備」の規程名例示より引用

運用管理規程（4-①）

参考： 医療情報システム 運用管理規程テンプレート（例）

章番号	見出し	内容
第1章	総則	• 規程の趣旨、目的。 • 患者の安全、個人情報を含む機密情報の保護を前提とし、医療情報システムの安全かつ継続的な運用を確保するために、必要な管理手順および責任体制等を本規程で定める。
第2章	組織体制と責任	• 管理対象のシステムを定める。 • 医療情報システム管理責任者を明確にし、役割分担と権限を定める。 • 情報システム部門、各診療部門との連携体制を記載する。
第3章	機器・資産の管理	• 医療情報システムに使用する機器の導入・管理・廃棄に関する台帳を作成・管理する。 - 台帳には機器名称、管理番号、設置場所、導入日、使用部門等を記録する。 - 資産の定期点検と保守計画を明記する。
第4章	アカウント・アクセス権限の管理	• 利用者アカウントの登録・変更・停止・削除の手順を明記する。 - 権限付与の基準および管理者権限の管理方法を定める。 - 有効な利用者アカウントの定期的な整理について定める。
第5章	データ管理	• 電子カルテ等、保有データの機密性、保存年限、真正性の確保について定める。 - 機微な医療情報の暗号化・アクセス制御、アクセスログ管理の方針を記載する。 - データの保存・廃棄の手順を定める。 - データのバックアップの取得頻度・保存期間・保管場所を定める。 • 障害発生時の復旧手順・担当者責任体制を明記する。

運用管理規程（4-①）

章番号	見出し	内容
第6章	ネットワーク接続管理	• 有線LAN、無線LAN、インターネット接続、リモートアクセス等に関する制御方針と設定管理について定める。 - ネットワーク構成図を作成し、管理する。 - ネットワーク機器、リモートアクセス機器のログ保存、管理方法を定める。
第7章	外部記憶媒体の利用管理	• USBメモリ等の外部記憶媒体の使用制限・許可手順、記録義務を定める。
第8章	ソフトウェア管理と脆弱性対策	• OSのシステムログ保存、管理方法を定める。 • OSやソフトウェアの更新方針、パッチ適用手順を定める。 • 既知の脆弱性への対応方法、定期的な確認と通知体制を整備する。
第9章	保守・委託業務管理	• 保守業者との契約内容に基づく責任分界、作業範囲、記録管理を明記する。 • 外部事業者のアクセス制御、ログ記録義務などの委託管理を含む。
第10章	インシデント対応	• BCP縮退運転環境への移行手順を定める。 • 障害・セキュリティインシデント発生時の対応手順、通報・連絡体制を定める。 • 対応記録、再発防止策、インシデント報告書の作成手順を明記する。
第11章	教育・訓練	• システム利用者に対する定期的な研修を行うこと、実施頻度を定める。 • BCP訓練や操作演習の実施方針と記録方法を含む。
第12章	規程の見直し、監査	• 重大インシデントの発生、組織体制や技術の変化等に応じて随時見直し、改訂履歴を記録する。 • 運用状況の点検のため定期的に内部監査を実施し、必要に応じて是正対応と規程の更新を行う。

令和7年度医療情報セキュリティ研修
及びサイバーセキュリティインシデント発生時初動対応支援・調査等事業

立入検査研修
準備コース

終了

本日の研修の振り返り「修了テスト」をご用意しております。
アンケート内での回答形式となります。ご回答をお願いします