

サイバーセキュリティ講習会資料

医療情報システムの安全管理に関する ガイドライン 第 7.0 版

二要素認証とパスワード運用は、こう変わります

2026 年 6 月 厚生労働省が公開 | 対応期限 2027 年 4 月 1 日

対象：電子カルテ、レセプトコンピュータなどの診療・医事情報管理システム

本日おさえていただきたい 3 つのこと

いずれも、日々の業務のログイン操作に直接かかわる内容です。

1

期限

2027 年 4 月 1 日に稼働している医療情報システムは、原則として二要素認証が必要です。

2

中身

すでに導入済みでも、ガイドラインが求める形になっていなければ「導入済み」とは言えません。

3

影響

二要素認証があるかないかで、パスワードの桁数ルールが変わります。

なぜ今、認証の見直しが必要なのか

サイバー攻撃の狙い方そのものが変わってきています。

1

攻撃の狙い方が変わった

大きな組織を選んで狙うのではなく、インターネット上に公開された弱いシステムを機械的に探し出し、見つけた組織を次々に攻撃する形に変わってきました。

2

医療機関は狙われやすい

セキュリティ対策に制約を抱えることが多く、医療情報システムへのランサムウェア攻撃などの被害が後を絶ちません。

3

最初に狙われるのは「入口」

攻撃者が最初に狙うのはログイン情報です。だからこそ、認証の強化が最優先の対策になります。

**攻撃者が
最初に狙うのは
ログイン情報。**

入口である「認証」を固めることが、いちばん効果の大きい対策です。

ガイドライン第 7.0 版の基本情報

前回の改訂から約 2 年半ぶりの改訂です。

発行

厚生労働省

公開時期

2026 年 6 月（前回改訂から約 2 年半）

対象となるシステム

**電子カルテ、レセプトコンピュータなどの
診療・医事情報管理システム**

本日よりあげる箇所

**システム運用編
「認証・認可に関する安全管理措置」**

対応期限と、新しく加わった経過措置

第 7.0 版では、期限に間に合わない場合の取り扱いが新たに書き加えられました。

対応期限

2027

年 4 月 1 日

この日に稼働しているシステムが対象

原 則

2027 年 4 月 1 日に稼働している医療情報システムは、原則として二要素認証の導入が必要です。

経過措置（第 7.0 版で新設）

技術的な理由などで 2026 年度内の導入が難しい場合は、2027 年度以降に行う次期システム更新のタイミングでの導入が許容されます。

※ 経過措置は「導入しなくてよい」ではなく、「導入の時期をずらせる」というものです。

そもそも「二要素認証」とは

認証の要素は 3 種類あります。このうち異なる 2 種類を組み合わせるのが二要素認証です。

1

知識情報

本人だけが知っている

- ID・パスワード
- PIN（暗証番号）

2

所持情報

本人だけが持っている

- IC カード
- 証明書を入れた端末
- スマートフォン

3

生体情報

本人そのもの

- 指紋
- 顔
- 静脈

「パスワード+秘密の質問」は、どちらも知識情報なので二要素認証にはなりません。

ガイドラインが求めている実装

第 7.0 版（システム運用編）では、実装する場所まで踏み込んで示されています。

- 1 クライアント端末とサーバーの、いずれにも二要素認証を実装すること
 - 2 クライアント端末では、電子カルテなどアプリケーションのログイン時に実装すること
 - 3 サーバーについては、OS での二要素認証を実装すること
- 

よくある NG パターンと、OK の形

「二要素認証を入れている」つもりでも、数え方を誤っているケースがあります。



これは NG

- パソコンの OS ログインで 1 要素、電子カルテのログインで 1 要素と、分けて数えている
- 電子カルテのログイン時に、パスワードと秘密の質問など、同じ要素を 2 つ使っている



これが OK

- 電子カルテのログイン時に、パスワード（知識）と IC カードや証明書（所持）を組み合わせる
- サーバーは、OS のログイン時に二要素認証を行う

NG パターンに当てはまる場合、二要素認証を導入しているとは言えません。早急な見直しの検討が必要です。

二要素認証の有無で、パスワードのルールが変わる

職員の皆さんに、いちばん直接的に影響する部分です。

二要素認証 あり

8 桁以上

PIN であれば 4 桁以上

二要素認証 なし（未導入）

13 桁以上

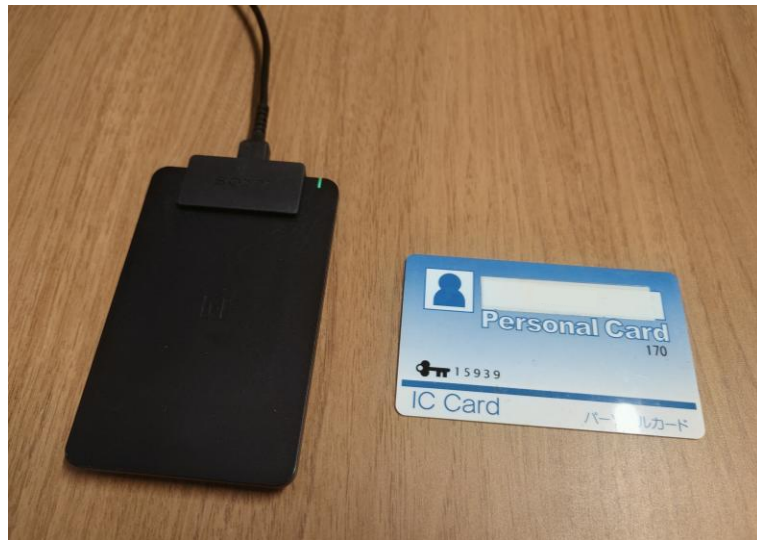
職員全員のパスワードが長くなります

どちらの場合も、大文字・小文字は問いませんが、英字と数字を混在させる必要があります。

当院では

2026年中の運用開始を目標に電子カルテ委員がカードリーダーを設置しています！

- 1 9月中にカードリーダー設置
- 2 10～11月中に全職員のカード登録
- 3 12月運用開始！



当院：ICカード + パスワード

職員一人ひとりが、今日からできること

仕組みを入れても、使い方が崩れると意味がなくなります。



パスワードは、院外のサービスなど他の場所と使い回さない



IC カードや証明書の入った端末を、他の人に貸したり共用したりしない



ID・パスワード・ワンタイムコードは、誰に聞かれても伝えない



メールやチャットのリンクから開いたログイン画面には入力しない



見覚えのないログイン通知や不審な動きに気づいたら、すぐ担当者へ連絡する

※ このページは講習会用に補足した実務上の注意点です。

本日のまとめ

1

2027 年 4 月 1 日が期限

経過措置はありますが、期限そのものがなくなるわけではありません。

2

同じ要素を 2 つ数えるのは NG

端末はアプリのログイン時に、サーバーは OS で二要素認証を実装します。

3

パスワードのルールが変わる

二要素認証があれば 8 桁以上（PIN は 4 桁以上）、なければ 13 桁以上です。

出典：厚生労働省「医療情報システムの安全管理に関するガイドライン 第 7.0 版」（2026 年 6 月公開）

参考：サイバートラスト株式会社 BLOG「二要素認証導入に経過措置？2026 年 6 月公開！医療情報システムの安全管理に関するガイドラインのポイント解説」（2026 年 7 月 23 日）