

歯科医院向け セキュリティ対策実践ガイド

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」を踏まえ、院内で今すぐ取り組めるサイバーセキュリティ実務を分かりやすくまとめました。

対象：院長・歯科医師・歯科衛生士・受付スタッフ

難易度：初級～中級

所要目安：各項目5～15分

なぜ今、歯科医院にセキュリティ対策が必要なのか？

電子カルテ、Web予約、オンライン資格確認の普及に伴い、小規模診療所を標的にしたランサムウェアや情報漏洩インシデントが増加しています。日常の基本設定を適切に行うだけで、リスクの大部分を未然に防ぐことができます。

1 Wi-Fiルーターの型番確認と基本ソフト（ファームウェア）アップデート

Wi-Fiルーターは院内ネットワークの「玄関」です。古いルーターを放置すると、外部から不正侵入され、院内のPC全体がウイルス感染する足がかりになります。

■ 今すぐ実施する確認手順

- 1. 本体背面の型番シールの確認：**ルーター本体の背面または底面にある型番（例：WSR-xxxx、Aterm-xxxx等）を控えます。
- 2. サポート期限の確認：**メーカー公式サイトでその型番が「サポート終了（EOL）」になっていないか確認します。**※サポート終了品はセキュリティ更新が届かないため、即時買い替えが必要です。**
- 3. 自動更新（ファームウェア更新）の有効化：**管理画面にログインし、「ファームウェア自動更新」がONになっているか確認します。
- 4. 初期パスワードの変更：**ルーター管理画面のログイン用パスワードが初期値（admin / password等）のままの場合は直ちに変更してください。

参考（公的機関）：[総務省：Wi-Fi提供者向けセキュリティ対策の手引き](#) / [IPA：家庭・小規模オフィス用Wi-Fiルーターの安全な利用](#)

2 PCの点検（Microsoft公式ツールの活用）

Windows標準またはMicrosoft純正の無料ツールを用いて、院内端末の健全性とマルウェアの有無を定期点検します。

■ ツール1：Microsoft PC Manager（総合健全化ツール）

- **概要：**マイクロソフト公式の軽量化・セキュリティ支援アプリ（Microsoft Storeから無料入手可能）。
- **操作手順：**アプリを起動し、「Health check（ヘルスチェック）」を実行。不要なキャッシュ削除やスタートアップアプリの整理、Windows Defenderとの連携状態をワンクリックで診断できます。

■ ツール2：悪意のあるソフトウェア削除ツール（MRT）でスキャン

- **概要：**Windowsに標準搭載されている既知の危険なマルウェア（感染型ウイルス・ランサムウェア等）を駆除するツールです。
- **起動・実行手順：**
 1. キーボードの **Windowsキー** + **R** を同時に押し、「ファイル名を指定して実行」ウィンドウを開きます。
 2. 名前の欄に半角小文字で **mrt** と入力し、「OK」をクリックします。
 3. 「悪意のあるソフトウェアの削除ツール」が立ち上がったら、「次へ」を押し、「**クイックスキャン**」（月1回は「フルスキャン」推奨）を選択して実行します。

参考（公式）：[Microsoft サポート：悪意のあるソフトウェアの削除ツール \(MRT\) の使用方法](#)

3 Google セキュリティ診断の実施

予約管理、Gmail、Googleビジネスプロフィール（口コミ・医院情報管理）でGoogleアカウントを使用している場合、アカウント乗っ取りを防ぐ必須点検です。

■ 実施手順

1. 医院のGoogleアカウントにログインした状態で [Google セキュリティ診断ページ](#) にアクセスします。
2. 「お使いのデバイス」「最近のセキュリティ イベント」「2段階認証プロセス」「保存したパスワードの安全性」などを一覧確認します。
3. 黄色の「！」や赤色の警告が出ている箇所をクリックし、指示に従って解決します（すべての項目が緑色のチェックマークになれば安全です）。

診断URL： <https://myaccount.google.com/security-checkup>

4 2段階認証（多要素認証）の徹底

パスワードが万が一漏洩しても、手元のスマートフォンなどの「第2の鍵」がないとログインできない仕組みです。

■ 歯科医院での適用ポイント

- **対象サービス**：Google Workspace、クラウド型予約システム、クラウドカルテ・会計ソフト、公式LINEアカウント等。
- **推奨方式**：SMS（ショートメール）通知よりも、紛失・盗聴リスクが低い「**認証アプリ方式（Google Authenticator / Microsoft Authenticator）**」の利用を推奨します。

参考（公的機関）： [IPA：2要素認証（2段階認証）を設定しよう](#)

5 パスキー（Passkey）の活用

従来の「文字列パスワード」を廃止し、指紋認証・顔認証・端末PINコードを使ってログインする最新かつ最も安全な国際標準規格です。

■ メリットと導入手順

- **フィッシング詐欺に強い**：偽サイト（詐欺サイト）に誘導されても、認証情報が盗まれることが構造上ありません。
- **設定例（Googleアカウント）**：「Googleアカウントの管理」＞「セキュリティ」＞「パスキーとセキュリティ キー」を選択し、「パスキーを作成」をクリック。端末の指紋またはWindows Helloを登録します。

参考（公的機関）：[デジタル庁：安全な認証技術・パスキーの普及促進](#)

6 スマートフォンの連携アプリの確認・棚卸し

院内業務用スマートフォンや院長私物のスマホで、「Googleでログイン」「Appleでサインイン」した過去のアプリに権限が残ったままになっていないか確認します。

■ 棚卸しの手順

1. Googleアカウント管理の「データとプライバシー」＞「サードパーティ製のアプリとサービス」を開きます。
2. 現在使用していない古いアプリや、不要な権限（連絡先へのアクセス等）が付与されているサービスを探します。
3. 不要なものは「**アクセス権を削除**」して連携を解除します。

7 メール関連のセキュリティ対策（ヘッダー確認とブラックリスト設定）

医療機関を狙う攻撃の多くは「標的型攻撃メール（なりすましメール）」から始まります。

■ ① ヘッダー情報の確認（送信元の偽装を見抜く）

- **確認手順（Gmailの場合）**：メール画面右上の「その他（縦の3点リーダー）」＞「メッセージのソースを表示」を開きます。
- **確認箇所**：「SPF」「DKIM」「DMARC」という項目がすべて **PASS** になっているか確認します。
※ **FAIL** や **SOFTFAIL** の場合、差出人の名前が公的機関や取引先になっていても、偽装メールの可能性が極めて高いです。

■ ② ブラックリスト（ブロック）設定

- 不審な迷惑メールや詐欺メールが届いた場合、メールソフトの「ブロック」機能を使用し、送信元アドレスおよびドメイン単位（例：**@malicious-domain.com**）を受信拒否リストに追加します。
- Outlook等の場合は「迷惑メール」＞「受信拒否リスト」へ登録します。

参考（公的機関）：[IPA：標的型攻撃メールの分析と対策](#)

8 取引先（歯科技工所等）へのセキュリティ情報共有・連携

口腔内スキャンデータ（STLファイル）、患者の顔写真、指示書などをやり取りする技工所とのデータ共有経路は、サプライチェーン攻撃の標的になりやすい急所です。

■ 技工所と取り決めるべきセキュリティルール

1. **USBメモリの原則持ち出し禁止**：データの受け渡しに汎用USBメモリを使わない。利用が必要な場合はハードウェア暗号化機能付きUSBに限定する。
2. **無料フリーメールでの患者データ送信禁止**：一般の無料メールではなく、通信が暗号化（SSL/TLS）された専用ポータルやクラウドストレージを利用する。
3. **インシデント発生時の連絡窓口の決定**：万一どちらかのPCがウイルス感染した場合、直ちに相互連絡を行う連絡網を整備する。

参考（公的基準）：[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](#)

最新のシステムを導入しても、現場のスタッフが不審なリンクをクリックしてしまえば被害を防げません。定期的な意識合わせが肝要です。

■ 院内周知すべき基本ルール

項目	具体的な実践内容
不審な添付ファイル	「請求書」「納品書」を装った .zip .exe .iso 形式のファイルは絶対に開かず、管理者に確認する。
画面ロック（離席時）	受付や診察室から離れる際は、必ず Windowsキー + L で画面をロックする。
パスワードの管理	付箋にパスワードを書いてモニター周辺に貼る行為を禁止する。
私用機器の接続禁止	医院の業務用Wi-FiやPCに、個人のスマートフォンやUSBメモリを無断で接続させない。

参考（研修教材）： 厚生労働省：医療機関向けサイバーセキュリティ研修教材

※本レポートは歯科医院におけるサイバーセキュリティ対策の標準的な手順を示したものです。システム構成や使用ソフトに応じて適宜調整してください。

本資料の提供・監修元

株式会社シーエス24

全国の歯科医院および歯科技工所における医療情報セキュリティの標準化・啓発支援。

Webサイト：<https://cs24.biz>