御堂筋監査法人ニュースレター Aug 2026

医療機関における退職者 ID 等のリスクと管理

公認会計士　川中 敏史
大手監査法人を経て 2022 年から御堂筋監査法人にて勤務。主に医療法人の内部統制指導、監査業務に従事。
保有資格：公認会計士/医療経営士

医療機関に限らず、ランサムウェアなどのサイバー攻撃が続いています。「うちには関係ない」「高度なハッキング技術なんて防ぎようがない」と思われがちですが、高度なセキュリティシステムの脆弱性だけではなく、退職した職員の「放置 ID（休眠アカウント）」もサイバー攻撃者から狙われやすいポイントの一つです。

今回は、監査の現場視点から、医療機関で起こりがちな「退職者 ID 管理」の落とし穴と、明日からできる対策をお伝えします。

1. 退職者IDの管理とは

退職者 ID の管理とは、職員が退職（または休職・異動）した際に、電子カルテ、グループウェア、財務システムなどへのアクセス権限を「速やかに」かつ「確実に」無効化することです。

ID 管理は情報セキュリティ対策の基本中の基本であり、退職者の ID が有効なまま維持されていることは、退職した職員がいつでもシステムに出入りすることが可能な状態を放置していることになります。

2. 退職者 ID が放置される原因と解決策

退職者の有効 ID が放置される原因として現場でよく聞く主なものは以下の通りです。

✧　非常勤医師は次にいつ来るか分からない！

【対策案】

- 「有効期限」をシステム側で初期設定する
- 最終ログインから 6 ヶ月経過で自動ロック
- 定期的にログイン履歴をチェックし、6 ヶ月以上ログインが無い場合は手動で無効化

✧　人事部からシステム担当へ退職者の情報共有が漏れる！

【対策案】

- 月次での「退職者リスト（人事）」とシステムの「有効 ID リスト」の突合

✧　電子カルテの仕様上、ID を削除すると過去の診療記録の署名者名が消えてしまう！（※）

【対策案】

- ID の「削除」ではなく、ログインのみを不可能にする「無効化」処理

※診療記録の署名者名は消えない

厚生労働省が定める「医療情報システムの安全管理に関するガイドライン第５版」では、電子カルテの真正性・見読性・保存性の確保が厳格に求められています。

そのため、現在稼働している標準的な電子カルテシステムでは、過去の署名を消さないために、そもそもユーザーIDを「削除」できない仕様になっており、代わりに、退職フラグを立てる、あるいはログイン権限を外す「無効化・非有効化」を行うボタンが用意されています。

3. 外部ハッカーによるサイバー攻撃のリスク

休眠アカウントは、持ち主がすでにいないため「パスワードが定期変更されない」「不審なログインがあっても本人が気づけない」という特徴があり、ハッカーにとって最も狙いやすい格好の侵入口（バックドア）となります。

① 医師のIDが乗っ取られた場合（システム停止の危機）
医師のIDは電子カルテや各種システムに対して広範な権限を有しています。このIDを外部から奪取されると、病院ネットワークの中枢に深く入り込まれ、ランサムウェア（身代金要求型ウイルス）の感染や、電子カルテの暗号化による「病院機能の完全停止」という最悪の事態に直結します。

② 看護師のIDが乗っ取られた場合（被害拡大の踏み台）
看護師のIDは、権限こそ医師より限定的ですが、人数が多く異動も激しいため「放置」が最も発生しやすい層です。ハッカーは権限の低いIDであっても、まずはそこから院内ネットワークに侵入し、時間をかけてシステム内を巡回して権限の昇格（より強いIDの奪取）を狙う「足場」として悪用します。

4. 退職者および現役職員による不正アクセスのリスク

「いつでもシステムに入れる状態」が放置されていると、本来は真面目な職員であっても、ふとしたきっかけで魔が差してしまう（内部不正のトライアングルが完成する）危険性もあります。

① 退職者本人による放置IDの悪用（転職先への「お土産」と覗き見）
有休消化期間中や退職後にアクセス権が残っていると、医師や研究者が次の職場で使うために、「患者の症例データ」や「研究資料」を持ち出すリスクが高まります。また、個人的な興味から「有名人のカルテ」や「元同僚の給与情報」を覗き見するといった、重大なプライバシー侵害も引き起こします。

② 現役職員による「退職者ID」の悪用（なりすましと責任転嫁）
元同僚のパスワードが漏れていた場合、現役職員が放置された退職者IDでシステムへログインして不正操作を行うリスクがあります。
カルテの改ざんや横領などを行っても、システム上のログ（証跡）には退職者の名前が残るため、犯人の特定が極めて困難になります。
※「共用ID」に重要な権限を付与した場合も同様に不正操作の追跡が困難となります。

5. 退職者による不正アクセス方法

「退職時に貸与のパソコンやスマホを回収しているから大丈夫」と思っていませんか？
アクセス権（ID）自体を削除（又は無効化）しない限り、院内システムに入られる可能性は残り続けます。

① 自宅の私物パソコンからの「VPN アクセス」
働き方改革で導入が進んだ VPN ですが、退職時に「VPN 接続用 ID」を消し忘れた結果、退職後も自宅の私物パソコンから、まるで院内にいるかのようにシステムにアクセスし放題となります。

② 待合室や駐車場での「職員用 Wi-Fi への自動接続」
個人のスマホに職員用 Wi-Fi を設定している場合、退職者が後日「患者」として来院した際、駐車場や待合室に入った途端に個人のスマホが自動で院内ネットワークに繋がります。
ID が有効であれば、個人のスマホから Web 版電子カルテなどを簡単に覗き見できてしまいます。

③ 個人のスマホで鳴り続ける「クラウドサービスの通知」
業務連絡用に個人のスマホに仕事用アプリ（メールやチャット等）を入れることを許可している場合、ID を無効化しない限りアプリはログイン状態を維持します。
退職者のスマホに、院内の機密情報や患者に関するやり取りがポップアップ通知され続けるという重大なインシデントに直結します。

④ 職員フロアへの不正侵入
職員と顔なじみであることを利用し、「忘れ物を取りに来た」「〇〇さんと面談」等のもっともらしい理由をつけて職員フロアへ侵入し、隙をみて専用端末から電子カルテシステムへアクセスされてしまいます。

6.「今すぐできる」セルフチェックリスト

人事・システム部門等の皆様で共有していただきたいチェックリストです。1 つでも「いいえ」があれば、早急な見直しや代替となるセキュリティ対策の検討をお勧めします。

確認	チェック項目	ポイント
□	**【毎月の棚卸し】** 毎月、人事部の「退職・休職者リスト」と、システムの「有効IDリスト」の突合を行っている。	部署間の「連絡漏れ」を防ぐ唯一の手段です。
□	**【無効化のタイミング】** 「退職日」を基準にすると数週間～数ヶ月に及ぶ有休消化期間中にアクセス権が残ったままとなるため、退職・休職・異動者のID無効化のタイミングが、「退職日」ではなく「最終出勤日」の業務終了後に速やかに実施されるルールとなっている。	人事部からシステム部へ提出する「退職・異動連絡書（または申請フォーム）」の項目に「最終出勤日（＝システム停止日）」を必須項目とすることや、「アカウントの有効期限」機能を活用することでタイムリーな無効化処理が実現できます。
□	**【非常勤・外部スタッフ】** 非常勤医師、派遣スタッフ、保守ベンダーのIDに、無期限ではなく「年度末」などの有効期限が設定されている。	「いつの間にか来なくなった職員のID」こそが、最もサイバー攻撃者に狙われやすい格好の「休眠アカウント」になります。
□	**【リモート・クラウド環境】** 電子カルテだけでなく、VPN接続、クラウドメール（Microsoft 365等）、職員用Wi-Fiへの接続権限も無効化対象としてリスト化されている。	個人のスマホに残ったセッションや、職員用Wi-Fiの自動接続から情報が漏れる可能性があります。
□	**【共用IDの禁止】** 「2階病棟用」「外来受付用」など、誰が操作したか個人を特定できない共用ID・共通パスワードを使用していない。	インシデント発生時に追跡が不可能になります。 電子カルテシステムのログインは「個人ID」を必須とすることや、共用IDの権限を閲覧のみ等に限定することでリスクは最小限に抑えられます。
□	**【不要IDの削除】** 「テストID」など、明らかに業務上不要と思われるIDは存在しない。	インシデント発生時に追跡が不可能になります。 退職者や休職者以外の視点でも定期的にIDの棚卸を行うことで「放置ID」を防止することができます。

以上