事　務　連　絡
令和８年10月28日

各都道府県衛生主管部（局）御中

厚生労働省政策統括官付医療情報連携担当参事官室
医政局医事課

オンライン診療システムにおける不正ログイン事案の発生に伴うセキュリティ対策強化のお願い

平素より厚生労働行政に対しご協力を賜り、厚く御礼申し上げます。

今般、国内のオンライン診療サービスを提供するシステムに対し、不正取得されたＩＤ・パスワードを用いた「リスト型アカウントハッキング（リスト型攻撃）」とみられる攻撃を受け、不正ログインされるという事案が発生しています。本事案では、医療機関側アカウント及び患者側アカウントの双方で不正ログインが確認され、患者の個人情報や診療情報等の閲覧被害が生じていることが確認されています。

医療機関及び医療情報システム事業者におかれましては、同様の手法による被害を防止・局所化するため、下記事項を確認し、必要な対応および利用環境の点検・対策の強化について早急に検討の上、実施いただきますようお願いします。また、SaaS 型サービスを提供する事業者におかれましても、予約システム、問診システム、業務効率化システム等関連するシステム・サービス全般について確認の上、対応をお願いします。

各都道府県におかれましては、内容を御了知の上、管内の医療機関及び医療情報システム事業者へ周知いただくとともに、その対応に遺漏がないようご協力をお願いします。

記

１　医療機関において対応・確認すべき事項

（１）多要素認証（二要素認証／パスキー）の必須化・有効化

オンライン診療や外部接続を伴うクラウド型医療システムにおいて、多要素認証（二要素認証、パスキー機能等）がシステム上利用できる状態だが利用していない場合には、有効化されているかどうかを直ちに確認ください。未設定の場合は速やかに導入・強制設定を検討・実施してください。

（２）パスワード管理の徹底（使い回しの排除）

院内で利用する医療情報システムや業務アカウントにおいて、私用サービスや他シス

テムと同一・類似のパスワードを使い回していないか点検を実施してください。

（３）アクセスログの緊急確認

直近において、深夜帯のアクセス、海外ＩＰアドレスからの接続、短時間の連続認証試行など、不審なログイン履歴がないか監査ログを確認してください。

（４）院内周知と警戒（二次被害の防止）

システム事業者や公式サポートを騙る不審な連絡（メール、SMS、電話）への警戒を周知してください（公式事業者がパスワードやワンタイムコードを個別に尋ねることはありません）。

２　医療情報システム事業者において対応・確認すべき事項

（１）認証基盤の強化

医療機関向け・患者向けの両インターフェースにおいて、多要素認証（MFA/2FA）やFIDO2/パスキーの導入を推進・標準化してください。

（２）不正ログイン試行の検知および防御機能の強化

同一ＩＰからの分散ログイン試行や、特定アカウントへの総当たり（パスワードスプレー）を検知し、自動遮断・アカウントロック・レートリミットを適用する仕組みを再点検・強化してください。

（３）リスクアカウントの保護措置

脆弱な認証設定（MFA 未設定など）のユーザーに対して、注意喚起やパスワードリセットの要請、セッションの強制無効化などのリスク低減措置を講じてください。

（４）監視体制の強化

異常なアクセス急増時のアラート基準や監視体制を見直し、インシデント兆候の早期検知体制を維持してください。

（５）緊急利用停止を含めた認証強化の対応

医療機関向け・患者向けのログインインターフェイスにおいて、メールアドレスや電話番号をＩＤに設定し、パスワード認証のみのシステムの場合や、外部流出情報によるリスト側攻撃を受けた場合に、正規の認証手段での不正ログインが容易に成立しやすいことが明らかとなっています。ついては、システムの緊急利用停止を含め、認証基盤の強化や認証手段の見直し等の措置を至急検討願います。

医療情報は極めて機微性の高い要配慮個人情報であり、万一それらの情報が漏洩等した場合には、患者のプライバシーや診療業務に重大な影響を及ぼします。各組織における安全管理措置の再確認と徹底を重ねてお願い申し上げます。

不正ログイン等のインシデントを検知された場合は、下記窓口まで速やかにご報告お願

いいたします。

政策統括官（情報政策担当）付医療情報連携担当参事官室
情報提供先　igishitsu@mhlw.go.jp