福県医発第2155号（地）
令和８年11月11日

各 医 師 会 長　　殿

福 岡 県 医 師 会
会 長 平 田 泰 彦
（公 印 省 略）

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

標記の件につきまして、厚生労働省より日本医師会並びに福岡県保健医療介護部医療指導課を通じて周知依頼がありました。

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攻撃を受け、不正ログインされる事案が発生しております。

本事案は、企業サーバが攻撃を受けた情報流出とは異なり、利用者アカウントが「リスト型アカウントハッキング（リスト型攻撃)」により不正ログインを受けたものです。

「リスト型アカウントハッキング（リスト型攻撃)」とは、他のサービスから流出したＩＤとパスワードを使い、別のＷＥＢサービスへの不正ログインを試みるサイバー攻撃のことで、複数のシステムで同じＩＤとパスワードのセットを使い回していると被害を受けやすくなります。

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され、患者の個人情報や診療情報等の閲覧される被害が生じているとのことです。

医療機関や医師会でシステムを提供している場合等におかれましては、今回の手法による被害を防止するため、次の事項（詳細は添付）を確認いただき利用環境の点検をお願いいたします。

つきましては、貴会におかれましても本件についてご了知いただくとともに、貴会会員への周知方よろしくお願いいたします。

なお、

１）「日本医師会サイバーセキュリティ支援制度」では、医療機関がサイバーセキュリティに取り組む際の、医療情報システムの安全管理に関するガイドラインや同チェックリスト対応するため、【日本医師会セキュリティガイドライン相談窓口】を設けられております。また、サイバーセキュリティに関連する日常の些細なセキュリティトラブルから重大トラブルまで幅広くご相談いただける【日本医師会サイバーセキュリティ対応相談窓口（緊急相談窓口)】を設置されております。本件にご対応いただく中で、ご不明な点等がございましたら、是非ご活用ください。

２）サイバーセキュリティ対策にかかる費用を医療機関が捻出するのは極めて難しいことから、日本医師会としては、国から医療機関への公的支援の拡充を引き続き強く要望していくとのことです。

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
（２）パスワード管理の徹底（使い回しの排除）
（３）アクセスログの緊急確認
（４）院内周知と警戒（二次被害の防止）

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
（２）不正ログイン試行の検知および防御機能の強化
（３）リスクアカウントの保護措置
（４）監視体制の強化
（５）緊急利用停止を含めた認証強化の対応

【日本医師会セキュリティガイドライン相談窓口】
TEL：0120-339-199　平日　９時～18 時（土日、祝日、年末年始は休業）

【日本医師会サイバーセキュリティ対応相談窓口（緊急相談窓口）】
TEL：0120-179-066　年中無休　６時～21 時

※詳細は日本医師会メンバーズルーム内専用ページをご確認ください。
https://www.med.or.jp/japanese/members/info/cyber_shien.html

日本医師会サイバーセキュリティ支援制度

日医発第1522号(情シ)(保険)
令和８年１０月３０日

都道府県医師会　担当理事　殿

公益社団法人　日本医師会
常任理事　長島　公之
常任理事　江澤　和彦
（公印省略）

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

平素より本会会務の運営に特段のご理解･ご支援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攻撃を受け、不正ログインされる事案が発生したとのことで、対策強化の周知依頼が参りました。

本事案は、企業サーバーが攻撃を受けた情報流出とは異なり、利用者アカウントが「リスト型アカウントハッキング（リスト型攻撃)」により不正ログインを受けたものとなります。

「リスト型アカウントハッキング（リスト型攻撃)」とは、他のサービスから流出したIDとパスワードを使い、別のWebサービスへの不正ログインを試みるサイバー攻撃のことで、複数のシステムで同じIDとパスワードのセットを使い回していると被害を受けやすくなるものです。

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され、患者の個人情報や診療情報等の閲覧される被害が生じているとのことです。

医療機関や医師会でシステムを提供している場合等におかれましては、今回の手法による被害を防止するため、次の事項（詳細は添付）を確認いただき利用環境の点検をお願いいたします。

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
（２）パスワード管理の徹底（使い回しの排除）
（３）アクセスログの緊急確認
（４）院内周知と警戒（二次被害の防止）

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
（２）不正ログイン試行の検知および防御機能の強化
（３）リスクアカウントの保護措置
（４）監視体制の強化
（５）緊急利用停止を含めた認証強化の対応

なお、「日本医師会サイバーセキュリティ支援制度」では、医療機関がサイバーセキュリティに取り組む際の、医療情報システムの安全管理に関するガイドラインや同チェックリスト対応するため、【日本医師会セキュリティガイドライン相談窓口】を設けております。

また、サイバーセキュリティに関連する日常の些細なセキュリティトラブルから重大トラブルまで幅広くご相談いただける【日本医師会サイバーセキュリティ対応相談窓口（緊急相談窓口）】を設置しております。

本件にご対応いただく中で、不明点等がございましたら、是非ご活用ください。

【日本医師会セキュリティガイドライン相談窓口】
TEL：0120-339-199 平日 9 時～18 時
（土日、祝日、年末年始は休業）

【日本医師会サイバーセキュリティ対応相談窓口（緊急相談窓口）】
TEL：0120-179-066　年中無休　6 時～21 時

日本医師会サイバーセキュリティ支援制度

※詳細は日本医師会メンバーズルーム内
専用ページをご確認ください。
https://www.med.or.jp/japanese/members/info/cyber_shien.html

つきましては、貴会におかれましても、本件についてご了知いただくと共に、貴会管下の郡市区等医師会ならびに会員への周知方につき、ご高配を賜りますようお願い申し上げます。

なお、サイバーセキュリティ対策にかかる費用を医療機関が捻出するのは極めて難しいことから、日本医師会として、国から医療機関への公的支援の拡充を引き続き強く要望してまいります。

【別添資料】
・【事務連絡】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

以上

公印省略

８医指第２３３７号
令和８年１０月２９日

公益社団法人福岡県医師会長
公益社団法人福岡県歯科医師会長
公益社団法人福岡県病院協会長
一般社団法人福岡県私設病院協会長
一般社団法人福岡県精神科病院協会長
公益社団法人全国自治体病院協議会福岡県支部長
殿

福岡県保健医療介護部長
（医療指導課）

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

本県の保健医療行政につきましては、平素から格別の御協力を賜り厚くお礼申し上げます。
標記について、厚生労働省から別添（写）のとおり事務連絡がありましたのでお知らせします。
つきましては、貴会会員に対して周知していただきますようお願いいたします。
なお、本通知については、県ホームページに掲載していますこと申し添えます。

通知掲載ホームページ
福岡県ホームページトップページから「健康・福祉・子育て」＞「医療提供体制」＞厚生労働省等からの通知」
https://www.pref.fukuoka.lg.jp/contents/kunituti2026.html

【担当】
医療指導係
TEL　092-643-3274
FAX　092-643-3277

事　務　連　絡
令和８年 10 月 28 日

公益社団法人　日本医師会御中

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。

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