

資料提供

令和6年3月28日
公益財団法人埼玉県健康づくり事業団
担当：健康管理課 小笠原、中村
TEL：0493-81-6089

X線画像読影システムへの不正アクセス攻撃について（第2報）

本事案（令和6年1月31日資料提供）につきましては、1月29日（月）に発覚後、2月3日（土）に当事業団において、埼玉県警、システム会社立会いのもと、専門の調査会社が侵入経路や個人情報の漏洩の有無などに関する調査（フォレンジック調査）を開始しました。

その後、約1か月の調査を行い、3月21日（木）に当事業団に最終報告書が提出されましたので、その概要を下記のとおり報告させていただきます。

今回の不正アクセス攻撃を厳粛に受け止め、再発防止に向けたセキュリティ対策の強化に取り組んでまいります。

記

1 侵入経路

攻撃者は、インターネットに接続しているVPNを経由して、1月27日（土）16時24分にX線画像読影システムの偵察活動に成功。

翌28日（日）18時36分に不正侵入、18時41分に探索活動、その後防御回避等を行い、サイバー攻撃を実行した。

2 個人情報漏洩の有無

個人情報については、データの窃取と漏洩の痕跡は確認されなかったが、RDP（リモートデスクトッププロトコル）を使用してもデータの転送ができることなどから、データ窃取の有無を完全に断定することはできない。

※RDPは、Windowsオペレーティングシステムで使用されるリモートデスクトップ接続のためのプロトコル。RDPを使用すると、ネットワーク経由で別のコンピュータに接続し、そのコンピュータのデスクトップを操作することが可能。

< X線画像読影システムに保存されていた個人情報 >

X線画像（胸部、胃部、乳部）及び超音波画像（腹部、乳部）と画像に付帯する情報（氏名、年齢、生年月日、性別、検査日、ID、撮影番号、問診、過去の所見と判定、今回の所見と判定）、モアレ検査画像（画像に付帯する情報は学校名、撮影番号）約94万人分。ただし、住所や電話番号、市町村名、事業所名は含まれておりません。

3 感染台数

サイバー攻撃の被害を受けた機器は、X線画像読影システムに関係する10台（サーバ8台、端末2台）※現在、ネットワークから切断しています。

4 現状の対応状況

X線画像読影システムを使用しない方法で事業を継続しています。

具体的には、健診センターや検診車で撮影したX線画像を専用のUSBメモリ（ウイルスチェック済）に保存し、X線画像読影システムとは別の独立した読影観察装置に取り込み、その画像を読影医が直接読影し、所見を読影簿に手書きします。その手書きした所見を結果処理システム（ウイルスチェック済）に手入力し、結果通知書を打ち出します。

X線画像の読影については、読影医が当事業団に来所する頻度を増やすことで、従前どおりの期間内で検診結果を提出いたします。

5 今後のセキュリティ対策

X線画像読影システムのバックアップデータ（暗号化はされなかった）を4月上旬までに読影観察装置に移行し、有識者の意見を踏まえながら、堅牢なセキュリティ対策を講じた新たなX線画像読影システムを令和6年12月までに構築する予定です。従来のX線画像読影システムについては、バックアップデータの新たなX線画像読影システムへの移行が終了した時点で廃棄し、再利用はしません。

併せて、健康づくり事業団のセキュリティ対策全般についても外部の有識者の意見を踏まえながら検証し、セキュリティ対策の強化に取り組んでまいります。