

公益財団法人東京都保健医療公社が運用する端末等に対する不正アクセス被害の発生による、メールアドレス等の個人情報の流出と対応について（第二報）

令和元年5月20日に報道発表した、公益財団法人東京都保健医療公社（以下、「公社」という。）が運営する多摩北部医療センターの医師の端末・メールアカウントに対する不正アクセス被害に関しましては、関係する皆さまに多大なご迷惑をおかけしましたこと、改めて深くお詫びいたします。報道発表後、原因究明と再発防止の取組を進めてきたところですが、その後の対応状況をご報告いたします。

1 不正アクセス被害の原因と被害の特定に関わる調査結果について

外部専門機関に委託し、当該職員の職務用パソコン端末及び個人用パソコン端末等を調査した結果、以下のことが判明しました。

- (1) ウイルス感染の原因は、5月1日に職務用パソコン端末へ送信された不正アクセスを意図したメールの添付ファイルを5月2日に当該職員が開封した結果によるものと特定しました。
- (2) ウイルスは、マルウェア「Emotet」亜種と推定されます。(注)
- (3) 不正アクセスの被害が確認されたのは、当該職員の職務用パソコン端末のメールボックスのみで、ハードディスクやファイルサーバに被害はありませんでした。
 - ① 職務用パソコン端末のメールボックスが不正にアクセスされた痕跡が認められましたが、流出した情報はメールボックス内の情報の一部に留まったことが推定されます。なお、ウイルスにより暗号化されていたため、流出した情報を特定することはできませんでした。
 - ② 職務用パソコン端末のハードディスクが不正にアクセスされた痕跡はありませんでした。
 - ③ 当該端末に接続しているファイルサーバが不正にアクセスされた痕跡はありませんでした。
 - ④ 当該職員の個人用パソコン端末については、ウイルスの感染はなく、個人情報の流出は確認されませんでした。
- (4) 多摩北部医療センターの全端末でウイルススキャンを実施し、感染及び感染疑いがあった18台の端末については、いずれも本件との関連はなく、個人情報の流出は確認されませんでした。

2 スпам攻撃の状況について

- (1) 6月6日時点で、公社や都庁のメールサーバ等に対し46件のスパム攻撃が確認されていますが、いずれもウイルススキャン機能や受信者による当該メールの削除などにより感染には至っておらず、現時点で具体的な被害の情報はありません。

(スパム攻撃の状況)

攻撃対象	第一報時点	第二報（累計）
公社メールサーバ	3件	30件
都立病院・院内LAN	0件	6件
都庁メールサーバ	4件	5件
その他不正アクセスの被害にあった職員とメールの送受信があった方	3件	5件
合計	10件	46件

(2) 被害の拡大を防止するため、公社及び当該病院のホームページにスパム攻撃時に送信されたメールの特徴を掲載し、広く注意喚起を図っています。

3 個人情報の流出について

(1) 5月20日の報道発表後、公社及び当該病院のホームページにおいてお詫びと注意喚起を掲載するとともに、当該病院内に同様の掲示をしました。

(2) 本件に対する問い合わせは、6月6日時点で、38件です。

(3) 患者情報等が記載されたメール24件（5月20日既報）の流出は確認されておられません。

(4) 本件に関する問い合わせは、多摩北部医療センターにおいて、引き続き対応してまいります。

〔お問い合わせ窓口：多摩北部医療センター庶務課（電話番号 042-306-3105）〕

4 再発防止について

(1) 不正アクセスを防止するための技術的な対応

- ・スパム攻撃をブロックする対策ツールの導入等の技術的な対策を実施しました。
- ・現在停止している外部から職務用パソコン端末に送信されたメールを閲覧する機能については、今後、ID、パスワードに加え、証明書の登録を必要とするなどセキュリティ対策を強化します。

(2) 公社職員の個人情報保護及び情報セキュリティに対する意識の徹底

- ・公社6病院、1センターの全院長等をメンバーとする「個人情報保護及び情報セキュリティ委員会」を緊急開催し、公社全体で本件事故の詳細を共有するとともに、個人情報の管理やセキュリティ対策の強化など再発防止に向けた取組を指示しました。
- ・今回の事故を受け、個人情報の管理や情報セキュリティ対策をまとめた緊急対策のリーフレットを作成し、公社全職員に周知徹底を図りました。
- ・さらに、個人情報や情報セキュリティの適正な取扱いを徹底するため、引き続き同委員会で検討し、必要な対策を実施していきます。

(注) マルウェア「Emotet」とは

「Emotet」は一般的に、Outlookに関する情報の窃取を行い、C&Cサーバ（マルウェアに感染した端末に指令を送り、詐取した情報の受け取り等を行うサーバ）にその情報をアップロードします。アップロードされた情報から得られたメールの宛先に対して、感染拡大を図ります（調査を委託した外部専門機関より）。

《問い合わせ先》

公益財団法人東京都保健医療公社事務局事業推進課 森田・小林
電話 03-5577-2149（直通）