

2025年12月25日

各 位

会 社 名 株式会社 ウイルコホールディングス  
代表者名 代表取締役社長 松浦 昌宏  
(コード: 7831 スタンダード市場)  
問合せ先 取締役 鈴木 正守  
(TEL. 076-277-9811 (代表))

連結子会社における不正アクセスの発生及び個人情報漏えいの可能性に関するお知らせ  
(第二報)

2025年10月31日に公表した「連結子会社における不正アクセスの発生及び個人情報漏えいの可能性に関するお知らせ」の続報の件で、現時点において、本件に関わる個人情報の外部漏えい事実や、漏えいに伴う二次被害はなかったことを確認いたしましたのでお知らせいたします。

記

1. 対応経緯

本事象の認知後、当社は速やかに緊急対策本部を設置し、事態の把握、影響範囲の特定と原因調査を開始するとともに、個人情報保護委員会へ報告を行いました。

本日までの対応経緯は以下のとおりです。

- 2025年10月29日(水) 不正アクセスを検知、対象サーバーを物理的に遮断
- 2025年10月31日(金) 緊急対策本部設置、フォレンジック調査決定、個人情報保護委員会へ報告及び外部に対する公表(第一報)
- 2025年11月4日(火) 対策本部会議(第2回)開催
- 2025年11月10日(月) 調査会社による対象サーバーの保全作業を実施
- 2025年11月13日(木) 調査会社へ調査対象サーバー(保全完了)のHDDを提出
- 2025年12月10日(水) 調査結果(速報)受領
- 2025年12月24日(水) 調査会社より正式報告書受領
  - (注1) フォレンジック調査: 不正や情報漏えいの原因を特定するためのデータ解析
  - (注2) HDD: ハード・ディスク・ドライブ(データ記録媒体)

2. 調査結果

- 攻撃手法: SSHサーバーに対するブルートフォース攻撃
- 調査結果: 攻撃者によるシステム情報の閲覧は確認されたが、外部へのデータ転送及びウェブコンテンツやデータベースへのアクセス痕跡はありませんでした。
  - (注3) SSHサーバー: 暗号化通信で安全な遠隔操作を行うサーバー機能
  - (注4) ブルートフォース攻撃: 多数のパスワードを試行し不正侵入を狙う攻撃手法

### 3. 再発防止策

本件の調査結果を踏まえ、以下の対策を実施しております。

#### [予防対策]

- (1) 被害サーバーの初期化と再構築
- (2) 外部アクセス制限（認証方式見直し、海外からのアクセス遮断）
- (3) パスワードポリシー強化
- (4) 脆弱性診断の定期実施
- (5) 監視体制強化による早期発見

#### [発生時対策]

- (1) 定期作業手順の見直しと訓練による担当者間の連係強化
- (2) 調査会社との連係強化

### 4. 当社及び他の子会社の対応

当社及び他の子会社においては外部委託による 24 時間監視体制をとっておりますが、  
本日までに各社のサーバーに対する不正アクセスは確認されておりません。

### 5. 今後の対応

引き続き、強化した監視体制の継続及び再発防止策の実施を徹底いたします。  
重要な進捗があれば速やかに開示いたします。

以上