



2021年7月9日

不正アクセスによる個人情報流出の可能性に関する調査結果のご報告

株式会社エヌ・ティ・ティ・ロジスコは、当社への不正アクセス事案として7月2日に公表（「不正アクセスによる個人情報流出の可能性のお知らせとお詫びについて」）しましたが、その後の調査結果および対策についてお知らせいたします。

弊社は、この度の不正アクセスについて重く受け止め、セキュリティ対策をより一層強化してまいります。お客様をはじめ多くのご関係者の方々にご迷惑とご心配をおかけしておりますことを、深くお詫び申し上げます。

1. 不正アクセスに関する調査について

(1)調査内容・目的

不正アクセスの影響範囲の特定

(2)調査手法(当社及び外部専門機関による調査)

①不正アクセスを受けた同一ネットワークセグメント内の調査

- 全てのネットワーク機器のログ・状態の確認
- 全ての端末のログ・状態の確認
- 不正アクセスの痕跡のある端末のフォレンジック調査※1

②流出情報調査

インターネット上に該当する情報が流出していないかの調査

※1 フォレンジック調査とは、デジタル機器の記憶装置から証拠となるデータを抽出したり、サーバや通信機器などに蓄積された通信記録から違法行為の証拠となる活動記録を割り出し、記憶装置から証拠となるデータを割り出すなどの調査

(3)調査結果

①不正アクセスの影響を受けた範囲について

上記の調査の結果、不正アクセスの影響を受けた社数は2社のみということが判明しました。なお、現時点では2社とも個人情報の外部流出の痕跡は確認されておりません。

②影響範囲が大きいと公表したNTTぷららについて

前回の報道発表(7月2日発信)において、流出の可能性のある個人情報件数として最大数である800万件とお伝えしましたが、調査により可能性のある件数としては約500件まで絞られました。さらに、その後の調査により個人情報流出を示す明確な痕跡が確認されず、現時点において外部への流出の可能性は極めて低いと判断いたしました。

(4)原因

NTTロジスコがNTTぷららとは別に受託している業務において、ネットワークの設定不備および、既知の脆弱性を悪用され、外部からの不正アクセスを許してしまうこととなりました。

2. 対策

(1)これまでに実施した対策

今回の攻撃手法や範囲を踏まえて、以下の必要な対処を完了しました。

- ・全ネットワークのインターネット接続ポイントのセキュリティチェック
- ・全端末のパスワード確認及び必要に応じた変更

なお、外部機関を活用したさらなるネットワークの診断を早急に実施します。

(2)今後の対策及び再発防止策

従来からあるセキュリティ体制・権限の強化を目的として、2021年8月1日より社長直轄の「セキュリティ推進室」を設置し、情報セキュリティの更なる強化並びに再発防止策の徹底にあたります。

- ・セキュリティポリシーの再構築、実行・徹底
- ・高度なセキュリティ対策ソリューションの追加導入
- ・セキュリティ人材の確保と社員教育(セキュリティ・リテラシー教育含む)

3. その他

本件については、警察に相談し、必要な対処を要請中です。