

不正アクセスによる個人情報漏えいへの再発防止策に関するお知らせ

LINE ヤフー株式会社は、2023年11月27日に公表（※1）した不正アクセスを受け策定した再発防止策を以下のとおりお知らせいたします。

当社は、ユーザーおよび関係者の皆さまに多大なるご迷惑とご心配をおかけする事態となりましたことを、改めて心より深くお詫び申し上げますとともに、今回の事態を重く受け止め再発防止に努めてまいります。

■発生した事象

第三者による不正アクセスを受け、ユーザー情報・取引先情報・従業員等に関する情報の漏えいがあることが判明しました。当社関係会社である韓国 NAVER Cloud 社の委託先かつ当社の委託先でもある企業の従業員が所持する PC がマルウェアに感染したことが契機となります。（※1）

■原因と再発防止について

□原因

本事案の原因は、「委託先企業への安全管理措置」および「NAVER と旧 LINE 株式会社間（以下、旧 LINE 社）のシステム・ネットワークのあり方」、「旧 LINE 社における従業員システムのセキュリティ」に課題があったためと捉えており、主に以下の再発防止策を順次実施してまいります。

□再発防止

・委託先管理の強化

委託先のセキュリティリスク評価方法を見直すとともに、外部の第三者の協力も得て、より実効性を高めたモニタリングや管理・監督方法を策定します。当社外部委託先が当社社内ネットワークにアクセスする場合における、当社管理下の PC の利用および当社ネットワークに接続する際の二要素認証の徹底を進めてまいります。

また、NAVER Cloud 社含む本件の原因となった当社委託先に対して、本事案を踏まえた改善策について実施状況を確認し、必要に応じた管理の強化等を要請します。

・システム・ネットワークのリスク解消・強化（NAVER Cloud 社との認証基盤の分離含む）

NAVER Cloud 社と旧 LINE 社間のネットワークアクセスの管理を強化します。具体的には、ファイアーウォールの導入やセーフリスト化により、ネットワークへの異常な接続や攻撃を防ぎ、ネットワークを保護する仕組みを構築します。また、旧 LINE 社環境の従業員向けシステムで共通化している NAVER Cloud 社との従業員情報を扱う認証基盤環境を分離し、LINE ヤフー専用の認証基盤への移行を行います。

加えて、更なる対策として、NAVER 社および NAVER Cloud 社とのシステムのつながりによる不正アクセスのリスクを解消するため、従業員向けシステムおよびネットワークの分離も行います。

・従業員システムのセキュリティ強化

従業員向けシステムへのアクセス制御と制限を強化するため、二要素認証の適用を標準とする方針とします。

さらに、データ分析システム等の重要なシステムに対して、アクセス制御のメカニズムが適切に機能していることを検証する目的で、追加的なセキュリティ診断を実施します。

上記の再発防止策については、外部企業による計画の妥当性・有効性の客観的な評価を実施します。

また、上記の再発防止策に加え、原因の再分析およびリスクシナリオの再定義、再発防止策の妥当性検証、追加対策計画の策定等についても、今後検討を続けていく予定です。

改めまして、ユーザーおよび関係者の皆さまに多大なるご迷惑とご心配をおかけしましたことを、深くお詫び申し上げます。発生させてしまった事象について深く反省し、再発防止に努めてまいります。

※1) <https://www.lycorp.co.jp/ja/news/announcements/007712/>