不正アクセスによる、情報漏えいに関するお知らせとお詫び（12/27更新）

2023年11月27日お知らせ

2023年12月27日追記および修正：継続している調査により、「ユーザーに関する情報の漏えい（369件*。可能性も含みます）を新たに確認」「不正アクセス開始日を10月9日から9月14日に変更」。

*増加分：370件（うち日本ユーザー294件）、減少分：1件（うち日本ユーザー1件）の合算値。なお、本増加分内に法人企業等の取引先に関する情報は含まれておりません。

※追記および修正箇所は下線を引いております。

LINEヤフー株式会社は、このたび、第三者による不正アクセス（以下、本事案）を受け、ユーザー情報・取引先情報・従業者等*1に関する情報の漏えいがあることが判明しましたのでお知らせいたします。

本件につきまして、以下の通り報告いたしますとともに、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、心より深くお詫び申し上げます。

なお、後述の当社へのアクセスの経路となったと推測される当社関係会社のシステムからは、当社の各サーバーに対するアクセスを遮断しております。11月27日時点でユーザー情報や取引先情報を利用した二次被害の報告は受けておりませんが、引き続き影響調査を進め必要な対応が発生した場合は速やかに対応してまいります。

■発生した事象

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者が所持するPCがマルウェアに感染したことが契機となります。9月14日に当社サーバーの社内システムへの不正アクセス開始、その後NAVER Cloud社と当社の従業者情報を扱う共通の認証基盤で管理されている旧LINE社の社内システムへネットワーク接続を許可していたことから、NAVER Cloud社のシステムを介し、10月9日、当社のシステムへ第三者による不正アクセスが行われました。

10月17日に当社システムへの不審なアクセスを検知し分析をしていたところ、10月27日に外部からの不正アクセスによる蓋然性が高いと判明したものです。当社では被害状況の把握と拡大の抑止の対応を実施しています。

また、関係省庁には適宜状況の報告を行っております。

■本事案の影響（詳細は別添を参照ください）

12月27日時点で、本件により漏えい（可能性も含みます）が確認できた個人情報は以下のとおりです。

〈ユーザーに関する情報〉

・ユーザーに関する個人情報　**302,938件**（うち日本ユーザー130,187件）

推計値49,751件を含む（うち日本ユーザー15,454件）：LINEユーザー内部識別子*2に紐づくサービス利用履歴など

　うち、通信の秘密*3に該当する情報　22,239件（うち日本ユーザー8,982件）

　推計値3,573件を含む（うち日本ユーザー31件）

口座情報、クレジットカード情報、LINEアプリにおけるトーク内容は上記に含まれません。

〈取引先等に関する情報〉

・取引先等に関する個人情報　**86,105件**：取引先等のメールアドレス等

　・取引先等のメールアドレス*4　86,071件

　・取引先等の従業者の氏名、所属（会社、部署）、メールアドレス等　34件

〈従業者等に関する情報〉

・従業者等に関する個人情報　**51,353件**：氏名、社員番号、メールアドレス等

　・ドキュメント管理システム内の従業者等に関する個人情報　6件

・認証基盤システム内の従業者等に関する個人情報*5　51,347件

・当社および当社グループ会社　　30,409件

・NAVER社およびグループ会社　　20,938件

*1　当社、当社グループ会社、NAVERグループにおける従業員、業務委託先および派遣元等の従業者

*2　LINEのアプリケーション内部で機械的にユーザーを識別するためのものであり、友だち追加のためのID検索に用いるLINE IDとは異なります。

*3　メッセージのように特定者間のやり取りに関連する情報

*4　当社メーリングリストに含まれていた当社（当社グループ会社を含む）ドメイン以外のメールアドレス

*5　提供しているシステムに応じて会社を区分。本件数は、アカウント数であり重複がある。従業員数とは一致しない。

■時系列対応（日本時間）

2023/09/14：当社サーバーの社内システムへ不正アクセス開始*6

~~2023/10/09：当社関係会社のサーバーを経由して当社サーバーに不正アクセス開始~~

2023/10/17：当社セキュリティ部門がシステムにて不審なアクセスを検知し調査開始

2023/10/27：外部からの不正アクセスである蓋然性が高いと判断

不正アクセスに使用された可能性のある従業者のパスワードをリセットし、当社関係会社から当社へのアクセスの経路となったと推測される当社関係会社のシステムから、当社の各サーバーに対するアクセスを順次遮断

2023/10/28：従業者の社内システムへの接続について再ログインを強制実施

2023/11/27：ユーザーおよび従業者等への通知を開始

*6　9月14日の不正アクセスにおいても、11月27日に公表した内容と同様、当社委託先企業の従業者が所持するPCがマルウェアに感染したことを契機としたものです。また、漏えい件数の追加は、不正アクセス開始日が10月9日から9月14日に変更になったことに伴うものではございません。

■対象者へのお知らせおよび今後の方針について

二次被害のおそれがあると評価したユーザーの皆さまには、個別にご連絡いたします。それ以外の、取引先の皆さまを含むご連絡可能なお客様に対しても個別のご連絡を実施予定です。該当の既存ユーザーおよび現時点で退会されているユーザー、取引先の皆さまには、ご登録いただいたメールアドレス、またはLINE公式アカウント「LINE Official Account」を通じた「LINE」アプリへのメッセージの通知機能等を通じて個別にご案内いたします。また、該当する当社従業者につきましても、本事案の説明を行います。なお、個別にご連絡ができない皆さまには、本発表を以て、通知とさせていただきます。

当社にてアクセス遮断などの処置を実施しており、該当するユーザーの皆さまにご対応いただく事項はございませんが、当社を装ったメッセージにご注意くださいますようお願い申し上げます。また、巧妙な詐欺やフィッシングの可能性があるため、十分にご注意くださいますようお願い申し上げます。

今後、当社は旧LINE株式会社環境の社内システムで共通化しているNAVER Cloud社との従業者情報を扱う認証基盤環境の分離を実施するとともに、ネットワークアクセス管理を一層強化していく予定です。加えて、事象の契機となった、委託先の安全管理措置の是正に取り組みます。また、これらの再発防止策については、計画の妥当性・有効性・客観性の担保を目的として外部企業を交えた計画策定を実施していきます。

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。

■本件に関する問い合わせ

本件に関するユーザーからの問い合わせは、下記窓口で受け付けています。

URL：https://support.yahoo-net.jp/formly/s/dirlycorporateinfo

■別添

本事案の影響の詳細

11月27日に公表した内容はこちらをご参照ください。