3月5日付総務省からの行政指導に対する報告書（概要）

2024年4月1日

LINEヤフー

はじめに

LINEヤフー株式会社は、2023年11月27日、不正アクセスによる情報漏えいに関するお知らせを行いました。

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を契機として、2023年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が開始されました。また、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、2023年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。これにより、ユーザー情報・取引先情報・従業者等※に関する情報が漏えいしました。

本事案については、多数のユーザーを抱えるプラットフォーム事業者としての信頼を損なう重大な事態であると重く受け止め、今後このようなことが起こらぬよう真摯に再発防止に取り組んでまいります。

本事案に関して、2024年3月5日付で総務省より行政指導を受け、2024年4月1日にその指導を踏まえた報告書を提出いたしました。

本資料は、総務省への報告書の要旨になります。
対応状況や今後の予定等については、当社コーポレートサイト特設ページをご確認ください。

https://www.lycorp.co.jp/ja/privacy-security/recurrence-prevention/

※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

目次

安全管理措置の見直し等 - 1

指導事項
(1)-①ア

貴社の旧LINE社環境とNAVER Cloud社との間にネットワーク接続があり、NAVER Cloud社に対して旧LINE社環境のネットワーク及び社内システムへの広範なアクセスが許容されていたことにより、NAVER Cloud社のシステム・端末への侵入によって貴社のサーバやシステムにまで到達可能であったことが本事案発生の原因となったことを踏まえ、NAVER社側のシステムや端末から貴社のネットワークや社内システムに関して真に必要最小限度のアクセスのみを許容し、その他のアクセスを認めない仕組みを、ファイアーウォールの設置、不要ポートの閉鎖、プライベート通信の排除等を含めて構築するとともに、これに加えて、貴社のサーバ、ネットワークや社内システムの保護の万全を図るための方策を検討し、具体的な措置を講ずること。

報告事項
（抜粋）

(1) 不必要な通信の遮断

NAVER環境から旧LINE環境への広範囲にわたるネットワークアクセスが許可されていたことが、当社システムに対する本事案に係る不正アクセスの原因となったことを踏まえ、再発防止策の一環として、 NAVER環境から旧LINE環境へのネットワークアクセスについて、ファイアーウォールの設置を実施し、必要な通信のみを許可し、それ以外の通信は拒否する設定を行いました。【2024年3月完了】
今後、2024年6月までに策定予定の業務委託の見直し計画と、システム分離に合わせた段階的な通信の遮断を進めていきます。

(2) 二要素認証の適用

本事案に係る不正アクセスにおいて二要素認証が導入されていたサーバー、システム等については被害を免れていることから、当社の従業者が利用するサーバー、システム等の保護を目的とし、これらに対する二要素認証を適用することで、認証の強度を高め、不正アクセスのリスクを低減しました。【2024年3月完了】
なお、旧ヤフー環境にある一部システムの二要素認証適用は2024年12月末までの実施を予定しています。

(3) NAVER社およびNAVER Cloud社のシステム分離

NAVER社およびNAVER Cloud社とのシステム、ネットワーク的なつながりによる潜在的なリスクを排除するため、これらの企業が管理するシステムからの分離も実施します。
【従業員向けシステム※1については当社 2025年3月末※2、 国内子会社 2026年3月末、海外子会社 2026年12月 完了予定】

※1 NAVER社およびNAVER Cloud社が提供するNAVER環境ないし旧LINE環境にある当社及び当社グループ会社従業者が利用するシステム
※2 会計システムは24年11月までにシステム切り替えおよび利用停止時期を判断します。

安全管理措置の見直し等 - 2

指導事項
(1)-①イ

共通化している認証基盤（従業員アカウントの認証基盤に限らない。）や情報の同期を認めるシステム構成のセキュリティリスクについて貴社において改めて評価を行った上で、確実な再発防止を実現する観点から、NAVER Cloud社の認証基盤等と貴社の認証基盤等とを速やかに技術面及び運用面で完全に分離するため、貴社が管理する認証基盤等への移転や分離後の管理の在り方等を含めて計画を策定するとともに、これを着実に実施することにより具体的な対策を講ずること。

報告事項
（抜粋）

共通化されている認証基盤には、従業者アカウントに関連するもののみが含まれ（ユーザーの認証情報は含みません）、全部で3つのシステムがあります。それらの認証基盤に関連するシステム管理をNAVER Cloud社が担っている状況を踏まえ、当社が委託元として実施可能な安全管理措置だけではリスクを十分に低減できないと判断したため、これらのシステムの利用を停止し、下記のように当社の認証基盤への移行を進めることで、これらのリスクを原因とする不正アクセスを防止します。

認証基盤の分離については、当社側で認証機能の切替対応が可能な当社及びグループ子会社が管理するシステムにおける分離を最優先で実施し、NAVER社と認証基盤及び認証情報を共通化している状態の解消を実施します。
【2024年6月完了予定】

NAVER社およびNAVER Cloud社管理のシステムの認証基盤分離については下記の通り実施します。
【当社 2025年3月末、国内子会社 2026年3月末、海外子会社 2026年12月 完了予定】

安全管理措置の見直し等 - 3

指導事項
(1)-①ウ

旧LINE社環境のサイバーセキュリティ対策に関連して、SoCのTier 1 に係る業務をNAVER Cloud社に委託しているとのことであるところ、本事案の発生を踏まえ、貴社として、国内において、独立した形で認証情報を管理、運用するとともに、セキュリティ確保のために必要とされる各システム等のログ情報を自ら取得し、これら情報を集約した上で独立した形でSoC業務を行うことができる体制を早期に整えること。今後、セキュリティインシデントが発生した場合には、自社の中に保有されている証跡に基づき、事象の詳細を把握し、原因究明やそれに対応した再発防止策を自ら策定することができる体制を整えること。

報告事項
（抜粋）

本事案の発生を踏まえ、NAVER Cloud社に委託していたSOCのTier1に係る機能については国内企業への委託に切り替え、当社が当該国内企業と協力してSOCの運営を行なう体制を構築します。【2024年10月完了予定】

また、NAVER Cloud社が管理するシステムからの分離がなされるまでの期間において、NAVER Cloud社からのログを用いた分析を速やかに行えないリスクは残存するため、事象把握・原因究明に必要となるログ情報については全て取得できる体制を構築します。 【2024年3月完了】

安全管理措置の見直し等 - 4 （1/2）

指導事項
(1)-②

AD管理についてはその重要性に鑑みて厳重なふるまい検知の仕組み等の対策が取られてしかるべきであったにもかかわらず、これが行われておらず、セキュリティ監視レベルが不十分であったため、不正なアクセスを検知等できなかった。また、その他の重要サーバ等についても認証方式がIDとパスワードの組合せであるなどそのアクセス管理のレベルが不十分であった点があり、不正に取得された従業員アカウント等を用いたアクセスを防ぐことができなかった。これらを踏まえ、自社内のサーバ等の保護に向けて、高度な侵入検知システムの導入や多要素認証の導入を含めたアクセス管理の強化等を含む、実効的なサイバーセキュリティ対策の導入に向けた計画を策定し、その内容を報告するとともに、速やかに具体的な措置を講ずること。

報告事項
（抜粋）

(1) AD管理の是正 【2024年3月完了】
本事案ではAD管理者権限を持つアカウントを奪取されたため、AD管理者アカウントの運用変更を行いました。
また、新たに振る舞い検知ソリューションをADへ導入し、SOCによる監視を開始しました。
更に、これらの対策に加え、外部企業によるコンサルティングを踏まえ、AD管理の是正を実施しました。

(2) 重要システムに対するアクセス管理の強化 【2024年3月完了】
3ページ(2)記載のとおりの二要素認証の適用を行いました。
また、旧LINE環境の従業者向けシステムのうち重要なものに対して、脆弱性診断を専門とする部門のセキュリティエンジニアにより、認証プロセスを迂回する試みや、認証要素の悪用できる方法がないかのセキュリティ診断を行いました。

(3) 外部企業を交えた計画策定 【2024年5月末完了予定】
再発防止策の計画の妥当性・有効性・客観性の担保を目的として、外部企業の提言を受け、当社のシステムや業務環境における適用可能性の検討、対策の具体化、計画の策定等を行ないました。また、同社からの提言も踏まえ、NAVER Cloud社環境での対応が必要な項目については、NAVER Cloud社とともに提言内容を精査し、NAVER Cloud社にて既に実施した是正状況等も踏まえて、対策の具体化・計画の策定を行ないます。

安全管理措置の見直し等 - 4 （2/2）

指導事項
(1)-②

AD管理についてはその重要性に鑑みて厳重なふるまい検知の仕組み等の対策が取られてしかるべきであったにもかかわらず、これが行われておらず、セキュリティ監視レベルが不十分であったため、不正なアクセスを検知等できなかった。また、その他の重要サーバ等についても認証方式がIDとパスワードの組合せであるなどそのアクセス管理のレベルが不十分であった点があり、不正に取得された従業員アカウント等を用いたアクセスを防ぐことができなかった。これらを踏まえ、自社内のサーバ等の保護に向けて、高度な侵入検知システムの導入や多要素認証の導入を含めたアクセス管理の強化等を含む、実効的なサイバーセキュリティ対策の導入に向けた計画を策定し、その内容を報告するとともに、速やかに具体的な措置を講ずること。

報告事項
（抜粋）

(4) サイバーセキュリティ対策およびセキュリティ監視にかかる効果検証と抜本改善・強化 【2024年8月末完了予定】
より実効的・包括的なサイバーセキュリティの強化を目的とした具体的な計画を策定し、速やかかつ確実に是正措置を講じていきます。具体的には下記の対策を実施します。

ペネトレーションテストの実施
・2024年7月　テストの実施、結果分析、報告
・2024年8月　テスト結果を踏まえた是正計画策定

振る舞い検知等の仕組みや相関分析ルール等の見直し
・2024年7月　外部機関を交えた現状分析・有効性検証
・2024年8月　検証結果を踏まえた是正計画策定

委託先管理の見直し等 - 1

指導事項
(1)-③ア

通信の秘密に該当する情報の取扱い等を委託する場合（通信の秘密に該当する情報の取扱いを委託する場合及びこのような情報へのアクセスを許容する場合やアクセスが可能となる場合を含む。）における業務委託先管理の在り方について、セキュリティリスクの評価基準の見直しを行った上で、リスクに応じた実効的な委託先管理を実現するための監督方法の検討及び基準の策定並びにその実施を行うこと。
特に、本事案の内容に鑑みれば、情報の取扱いの委託の有無にかかわらず、重要な設備等に関する業務委託について、その委託先及び再委託先について特定した上で、安全管理措置ないしサイバーセキュリティ対策について適切な管理監督ができるように、令和６年３月末までに安全管理措置等の基準を策定し、実効性を高めたモニタリング・監督方法を検討・策定すること。あわせて、委託先の監督が委託先による分析結果や委託先から受領するログに依存しており、委託先からこれらが得られないと自社として侵害の有無や範囲も十分に把握できないという状況を見直すこと。

報告事項
（抜粋）

(1) **セキュリティリスク評価基準の見直し** 【2024年3月完了】
個人情報等の委託の際に適用されていたチェックシートをベースとして、より広く一般的な業務委託の管理にも活用することを意図して委託先チェックシートを新設しました。

(2) **実効的な委託先管理を実現するための監督方法の検討および基準の策定並びにその実施** 【2024年3月基準策定完了、以後順次実施】
個人情報等の委託に限定されない、新規の取引先・業務委託先に対してセキュリティ面、信用面等の多角的なリスク評価を実施する社内ルールを策定し、今後は、取引開始時及び契約更新時に加え、定期的な監査において多角的なリスク評価を実施してまいります。また、新評価基準での監督が一巡するまでの間は、委託先の対策不備に起因するリスクが残存するおそれがあるものの、かかるリスクへの対処として、 本事案の契機となった委託先等については、先行して監査等を実施してまいります。

(3) **安全管理措置/サイバーセキュリティ対策の策定** 【2024年1月完了】
当社発番のアカウントを用いた業務委託先が当社ネットワーク環境にアクセスをする場合、原則として二要素認証を経た場合にのみアクセスを許容する対応を実施しました。

(4) **自社としての侵害の有無や範囲を把握すること** 【2024年9月末完了予定】
当社のネットワークへログイン又はアクセスすることができる業務委託先に対しては、当社がキッティングを実施した当社のPCでのみ委託業務の実施を認める方針とします。上記貸与PCの配布が完了するまでの期間における委託先PCのマルウェア感染等のリスクは残存するものの、(3)記載の措置により、残存リスクの軽減措置を実施してまいります。

委託先管理の見直し等 - 2

指導事項
(1)-③イ

本事案における攻撃の端緒となったNAVER Cloud社における安全管理措置の強化について、委託元としてNAVER社側に対して適時に実施状況を確認するとともに、必要に応じて対策の強化を要請するなどし、実効的な再発防止策が策定されるよう、適切な管理監督を行うこと。
特に、貴社からの報告によれば、NAVER Cloud社は、貴社から指摘するまで侵害に気付かず、そのADサーバが侵害され、外部のC&Cサーバから直接接続された状況が相当期間にわたって継続していた等、その安全管理措置に問題があったとのことである。このことを踏まえ、委託や監督の在り方を見直すための、貴社としての計画を策定して提出すること。

報告事項
（抜粋）

NAVER Cloud社に対して、第三者企業も交えた現地での実査を実施いたしました。かかる実査においては、同社の再発防止策の履行状況を改めて確認するとともに、インシデントを引き起こすに至ったNAVER Cloud社における各種の安全管理措置の実施状況の確認および是正の指摘・要求を行っております。【2024年3月完了】

また、今後の是正対応等を当社として主導的に確認するため、 NAVER Cloud社に対する監査権等を定めた覚書を締結し、当社として上記の実効性を明確な形で担保していきます。【2024年3月完了】

今後、2024年9月末を目途にSOCに関する業務委託の解消を実施するほか、2024年6月までに策定予定の業務委託の見直し計画に基づき、関連する委託関係の終了・縮小により、委託範囲自体の縮小を進めてまいります。

上記の他、本件関係委託先企業への現地実査を実施し、契約の解除も行いました。【2024年3月完了】

グループ全体でのセキュリティガバナンスの見直し等

指導事項
(2)

貴社内におけるセキュリティガバナンス体制の抜本的な見直しや是正策の検討を行うことに加え、貴社の親会社等も含めたグループ内において、委託先への適切な管理・監督を機能させるための貴社の経営体制の見直し（委託先から資本的な支配を相当程度受ける関係の見直しを含む。）や、適正な意思決定プロセスの構築等に向けた、適切な検討がなされるよう、親会社等に対しても必要な働き掛けを行うこと。

報告事項
（抜粋）

(1) 当社委託先たるNAVER社側から資本的な支配を相当程度受ける関係の見直しに関して、当社として関係各社へ見直しを要請しております。

(2) 当社委託先NAVER社側への適切な管理・監督を機能させるための当社内における経営体制の見直しに関する議論を、当社指名報酬委員会にて議論を開始しております。今後、機関決定等が行われれば、必要な公表等を行います。

(3) 当社およびNAVER社側との間の、社内向けシステム・ネットワークの運用等の委託にとどまらない、サービス開発業務委託およびサービスインフラを含むシステム利用について終了・縮小する方針とします。一部継続する取り組み等がある場合は、その安全管理措置等を当社ガバナンス委員会で確認を行います。

また、2024年4月1日付で当社CISOおよびグローバルを含む当社の主要なグループ会社CISO並びにオブザーバーとしてのソフトバンク株式会社CISOで構成される「グループCISO Board」を設置し、当社グループ全般のセキュリティガバナンスについて抜本的見直しや高度化を図ってまいります。

上記に加え、社長直属の新組織を設置し、各種再発防止策の推進及びグループ全体でのセキュリティガバナンス確立を推進してまいります。

利用者対応の徹底

指導事項
(3)

本事案において、少なくとも、貴社の利用者の通信の秘密に該当する情報が２万件以上（推計値を含む。）漏えいしたことを踏まえ、利用者保護の観点から、今後も利用者に対する本事案に関する適切な情報提供を継続するとともに、二次被害が発覚した場合等には適切な支援、対応を実施すること。

報告事項
（抜粋）

(1) 利用者保護のための本事案に関する情報提供

当社においては、利用者保護の観点から、利用者に対する本事案に関する適切な情報提供を今後も継続します。
具体的には、当社コーポレートサイトに本事案の概要および再発防止の進捗等について取りまとめた特設ページを4/1付けで公開しました。特設ページでは、当社の各対応状況の進捗を掲載するほか、利用者保護の観点から公開すべき情報が新たに明らかになった場合には、本特設ページにて速やかに公開します。

(2) 二次被害が発覚した場合等の対応

当社においては、当社が未だ認識していない不正アクセスによる被害の発生やその可能性を認知するための取組みを、合理的な期間が経過するまでの間継続し、二次被害の早期発見と拡大防止に努めます。
また、本報告書提出時点において二次被害は確認されておりませんが、今後も、常設の顧客対応窓口に対してユーザーから二次被害の申告を受けた場合においては速やかに調査を行う等、必要な対応を適切に実施してまいります。

LINEヤフー