3月28日付個人情報保護委員会からの勧告および報告の求めに対する報告書（概要）

2024年4月26日

LINEヤフー

はじめに

LINEヤフー株式会社は、2023年11月27日及び2024年2月14日に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。

具体的には、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。

当社は、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28日付で個人情報保護委員会より、「技術的安全管理措置の不備」及び「組織的安全管理措置の不備」について速やかに是正するよう勧告を受けるとともに、実施状況について報告を行うよう求められました。この勧告及び報告の求めに基づき、当社は2024年4月26日に報告書を提出いたしました。

本資料は、個人情報保護委員会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

技術的安全管理措置の不備の是正 - 第1 (1/2)

委員会
公表資料
第5 - 1

1 技術的安全管理措置の不備

本件の攻撃者による NC 社（※NAVER Cloud社のこと。以下同じ。）のデータセンターから LY 社（※当社のこと。以下同じ。）のデータセンターへの接続方法は、通常の業務として想定されている接続方法とは異なるものであったにもかかわらず、NC社とLY社のネットワーク間において導入・運用している侵入検知システムは、本件の攻撃者による不正アクセスを防止及び検知することができなかった。これは、LY社が、NC社に対し、 LY社のネットワーク及び社内システムへの広範なアクセスを許容していたにもかかわらず、サーバ、ネットワーク及び社内システムを保護するための十分な措置を講じておらず、特定のポートに係る通信をブロックするのみで、それ以外の通信は広く許容されていたことが一因であったものと認められる。

LY 社が、このような広範なネットワーク接続によるリスクを理解し、NC 社のシステムや端末から LY 社のネットワークやシステムに関して、真に必要な通信のみを許容し、その他のアクセスを認めない仕組み等の措置をとっていれば、不正アクセスを防止又は検知できた可能性がある。

技術的安全管理措置の不備の是正 - 第1 (2/2)

報告事項
（抜粋）

第 1 NAVER Cloud社データセンターと当社データセンターとのネットワーク接続に関する是正

(1) 不必要な通信の遮断

NAVER Cloud社データセンターから旧LINE社データセンター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、NAVER Cloud社データセンターから旧LINE社データセンター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・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) NAVER Cloud 社がシステム管理を担う認証基盤の利用停止と当社認証基盤への移行

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、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ます。

- 当社側で認証機能の切替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認証基盤の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】**

(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】**

また、(1)に記載の業務委託の見直し、(2)認証基盤の分離、(3)システムの分離についてはより早期に実施完了できるよう、計画の策定または見直しを継続して行ってまいります。

※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。

技術的安全管理措置の不備の是正 - 第2

報告事項
（抜粋）

第２ 重要度の高い情報システムへのアクセス管理に関する是正

(1) 従業員向けシステムに対する二要素認証の適用、リスクアセスメント

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、旧ヤフー社データセンター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。また、本事案で不正アクセスがなされたデータ分析システム等は本来であれば二要素認証が適用されていてしかるべき重要なシステムであったことを踏まえ、重要システムとそれに対して求める安全管理措置基準を2024年6月末までに定義したうえで、ISO27001を活用したリスクマネジメントプロセスの中でリスクを把握・管理する仕組みとします。
加えて、年次のリスクアセスメントとして、各システムのデータ保管の現状、施されているセキュリティ対策、それに伴うリスクを全体的に把握し、評価する業務の仕組みを構築するとともに、これらについて当社規程として定めます。
これらを確実に実施するため、CISO直下にセキュリティ監査部門を設け、リスク対策の定期的なレビュー・評価の仕組みを構築します。
【2024年6月末完了、以降順次実施】

(2) 重要システムに対するアクセス管理強化（MFA+認証プロセスセキュリティ診断）【2024年3月完了】

5ページ(1)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社データセンターにおける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、認証要素を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) Active Directory（以下、ADと記載）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。

※対応中の取り組みは完了時期の前倒しを検討しております。

技術的安全管理措置の不備の是正 - 第3

報告事項
（抜粋）

第３ その他の技術的安全管理措置の是正策

(1) 社外と旧LINE社データセンター間の接続経路の総点検【2024年7月末完了予定】

NAVER Cloud社データセンターから旧LINE社データセンター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、旧LINE社データセンターのシステムに対する不正アクセスを許す原因となったことを踏まえ、NAVER社と同様に社外から旧LINE社データセンターに専用線やVPN等を介して接続している経路に対して、ネットワークアクセス制御の適切性、およびインシデント対応の準備状況に関する点検を2024年7月末までに行います。

(2) 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、計画の策定等を行いました。また、同社からの提言も踏まえ、NAVER Cloud社データセンター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・計画の策定を行います。

(3) 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

※対応中の取り組みは完了時期の前倒しを検討しております。

組織的安全管理措置の不備の是正 - 1 (1/3)

委員会
公表資料
第5 - 2

(1) 個人データの取扱状況の把握及び安全管理措置の評価、見直し及び改善について

ア NC社との関係に応じたリスク管理に関する問題点

LY社は、個人データの取扱いに関し、自らの判断でガイドラインに則した安全管理措置を講じなければならないところ、旧L社の沿革に起因するNC社との共通認証基盤システムやNC社との広範なネットワーク接続を許容するネットワーク構成の利用を継続してきた。また、LY社は、NC社に対して本件個人データの取扱いの委託は行っていないと整理していたため、実際にNC社に対して自らの安全管理措置と同等の措置が講じられるよう監督を行うことはなく、結果として、NC社に業務委託し構築させたシステムが侵入経路及び漏えい原因となり、本件個人データが漏えいした。

すなわち、LY社は、その安全管理のために必要かつ適切な措置を講ずる責任の所在と手段の検討及び把握が曖昧なまま、ユーザーの個人データを含む大量の個人データを取り扱っていたものである。

LY社は、このようなリスクや課題を認識すべきであったにもかかわらず、共通認証基盤システムの共同利用や、NC社に対する重要なシステムの構築及び運営の業務委託を継続してきたものであり、個人データの取扱状況の把握及び安全管理措置の評価、見直し及び改善に問題があると言わざるを得ない。

組織的安全管理措置の不備の是正 - 1 (2/3)

報告事項
（抜粋）

1 NAVER Cloud社との関係に応じたリスク管理に関する問題点の改善

(1) 委託先の監督方法の是正

A) 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。

B) 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いくとともに、当社環境へのVPN接続時における二要素認証の適用や当社発番のアカウントに対するPC貸与等の対応を通じてリスク低減を図ってまいります。

C) 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。

D) 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、 上記Cに記載の措置により、残存リスクの軽減措置を実施してまいります。

※対応中の取り組みは完了時期の前倒しを検討しております。

組織的安全管理措置の不備の是正 - 1 (3/3)

報告事項
（抜粋）

1 NAVER Cloud社との関係に応じたリスク管理に関する問題点の改善

(2) その他NAVER Cloud社との関係に応じたリスク管理に関する問題点の改善施策について

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】**

さらに、各部門の組織のリスクを洗い出し、管理する従来からの全社的なプロセス(ERM)によるリスク管理の徹底に加えて、従業員一人ひとりの声を集めることで、より多角的な視点から幅広いリスクを可視化し評価する新たな仕組みの導入を検討してまいります。
【2024年6月制度設計完了、以後順次実施予定】

※対応中の取り組みは完了時期の前倒しを検討しております。

組織的安全管理措置の不備の是正 - 2

委員会公表資料
第5 - 2

(1) 個人データの取扱状況の把握及び安全管理措置の評価、見直し及び改善について

イ 令和３年行政指導後の対応に関する問題点

委託先における個人データの取扱いに関して適切な監督等を実施するよう求めた令和３年行政指導に対し、LY社は、再発防止策の一つとして、重要度の高い個人データにアクセス可能な権限のログインには多要素認証を導入するとしたが、本件事案で不正アクセスを受けたデータ分析システム等において保管されているユーザーの情報の機微性が、他のシステムと比較して相対的に低いと判断し、多要素認証の導入を見送ってきた。

しかしながら、本件個人データのうち、データ分析システムに保管されている個人データは、ユーザーのLINE各種サービスの利用履歴に関する個人データであるところ、これらのサービス利用履歴は、個人の行動範囲、経済状況、趣味・嗜好等のプライバシーに関するデータであり、本人の権利利益の保護の観点からは、機微性の低い情報と分類することはできない。

そもそも、LY社においては、①NC社との共通認証基盤システムの利用及び②NC社との広範なネットワーク接続という点において、安全管理措置に関わる特殊性が存在していたものであるから、これらに起因するリスクを適切に評価し、ユーザーのサービス利用履歴等の個人データについても、多要素認証導入を積極的に判断するべきであった。

以上から、LY社においては、令和３年行政指導後の安全管理措置の評価、見直し及び改善が十分ではなかったものと認められる。

報告事項
（抜粋）

２ 令和３年行政指導後の対応に関する問題点の改善

ユーザーのサービス利用履歴等の個人データへのアクセスに対する多要素認証の導入について、令和３年行政指導後の当社対応および令和5年10月1日の経営統合（合併）に際する検討の中で、見直し、改善する機会があったにも関わらず導入が遅れていた点に関しまして、「技術的安全管理措置の不備の是正 - 第2」に記載のとおり、当社の従業員が利用するサーバー、システム等に対する二要素認証の導入を行っており、その対応を概ね完了しているところです。

当社としての安全管理措置全般について、当社経営の前提となっているような事項そのものについて議論検討を行うセキュリティガバナンスの体制についての改善も必要と考えており、本事案に関連する対応の一層の推進および当社課題全般についての議論を行う社長直属のセキュリティガバナンス委員会を設置したほか、当社グループとしてのセキュリティガバナンス全体を議論する、グループCISO Boardを設置しております。（「組織的安全管理措置の不備の是正 - 4」にて詳述いたします。）

組織的安全管理措置の不備の是正 - 3

委員会公表資料
第5 - 2

(2) 漏えい等事案に対応する体制の整備について

不正アクセスの原因や侵害範囲等の全容を明らかにするに当たっては、A社PC及びサーバを調査し、また、NC社に構築及び運営を業務委託するシステムのアクセスログを調査する必要があった。

しかしながら、LY社は、自らの判断でガイドラインに則した安全管理措置を講じなければならず、漏えい等事案の発生時には事実関係の調査及び原因の究明が実施できるような体制を整備すべきであるところ、事実関係の調査及び原因の究明については、NC社やNAVERグループに頼らざるを得ない状況であり、LY社が本件事案の全容を把握するために約３か月半という時間を要した。

このように、LY社は、自社の漏えい等事態に関する事実関係の調査及び原因の究明が速やかになされなかったものであり、漏えい等事案に対応する体制の整備の観点からも不備が認められる。

報告事項
（抜粋）

1 事実関係の調査・原因究明等、漏えい等事案に対応する態勢の整備

下記2点に起因する要因があったと認識しており、事案発生時に迅速に対応するための体制構築を進めてまいります。

1) 当社における漏えい等事案に対応する体制の未整備【2024年5月計画立案、同年6月外部評価完了、以後順次実施】

- 事案発生時の調査範囲の判断プロセスについて改善点を洗い出し、必要なマニュアル・ルールの整備を行います。また実施に当たっては、外部機関の評価を得た上で確定するものとし、実行性を担保するために、演習の定期実施を行います。
- 委託先については原則PC貸与の方針として、事案発生の際には速やかに回収、フォレンジック調査を行うこととします。

2) NAVER Cloud社や NAVERグループに依存度が高かったこと【2024年3月完了】

- 事案発生時のNAVER Cloud社との窓口の明確化を実施しました。
- 当社のログ保管期間ルールに従いNAVERグループのシステムのログを１年間保管するものとし、必要に応じてNAVER Cloud社から受領できるように個別覚書を締結しました。

2 ログを自社で取得し、分析できる態勢の整備（独立したSOC業務体制の構築）

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の運営を行う体制を構築します。**【2024年10月完了予定】**

※対応中の取り組みは完了時期の前倒しを検討しております。

組織的安全管理措置の不備の是正 - 4

委員会公表資料
第5 - 2

(3) 組織体制の整備等について

旧L社に対する令和３年行政指導後も、他社との広範なネットワーク接続を継続しているにもかかわらず、アクセス制御等の技術的安全管理措置が講じられていなかったこと、個人データの取扱状況の把握及び安全管理措置の評価、見直し及び改善に問題が認められること、漏えい等事案への対応を速やかに行うことができなかったことから、その組織体制が必ずしも十分に機能していたとは言い難い。

令和５年10月に経営統合が行われ、事業規模が拡大し、今後とも、大量かつ重要度の高い個人データの取扱いが想定されるところ、その取扱いに万全を期すために、個人データの取扱いに関する責任者（DPO 等）が中心となって、安全管理措置が徹底される組織体制を整備し、その実効性のある運用の確保に注力すべきである。

報告事項
（抜粋）

(1) 旧LINE社と旧ヤフー社等が合併をした令和5年10月1日以降の当社においては、個人データを取扱う上でのセキュリティ面での安全管理措置はCISOが全社のセキュリティ責任者として責任を持って実施しております。具体的には個人情報を含むすべてのデータの取り扱いレベルと安全管理措置を定義して、セキュリティ規程に定めるとともに、各部門にセキュリティ責任者を任命して、データが適切に取り扱われているかリスクアセスメントを実施しています。
加えて、2024年4月から規程遵守状況をモニタリングするための監査部門を設置しています。

(2) 当社において個人データを取扱うに際しては、プライバシー関連の専門組織による評価を行う会議体において、複眼的に、潜在的なプライバシーへの影響を評価、リスクや必要な行動の洗い出しを行って、方針の決定を行うほか、必要に応じて当社経営会議へのエスカレーションを行っております。同会議体にはDPO部門も参加し、執行側からは一線を画した独立した立場で、ユーザー目線で執行側による活動に対する監視・助言を行っております。

(3) 経営層および当社グループ全体においてセキュリティガバナンス、安全管理措置の強化を行うための組織体制を新設しています。
具体的には、2024年4月より当社社長CEOが委員長を務めるセキュリティガバナンス委員会を組成し、本事案に関連する対応の一層の推進および当社課題全般についての議論を行っております。
また、同じく2024年4月より、当社CISOおよびグローバルを含む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、当社グループ内におけるセキュリティの統一ルールの策定と遵守の徹底や、それらを前提とした当社グループ会社間での委託関係の整理等の議論と推進を行って参ります。

LINEヤフー