3月28日付個人情報保護委員会からの勧告及び報告等の求めに対する12月27日提出報告書（概要）

2024年12月27日

LINEヤフー

はじめに

本資料は、2024年3月28日付の個人情報保護委員会からの勧告及び報告等の求めに対し、2024年12月27日付で提出した報告書の概要です。本資料には、「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」に対する是正の進捗を記載しております。

当社は、引き続き再発防止に取組んでまいります。

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/

目次

上記について、2024年12月27日時点の実施・検討状況を次頁以降に記載しております。

技術的安全管理措置の不備の是正 - 第1 (1/3)

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 (2/3)

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社のインフラを利用している旧LINE社サービスの本番環境用のサーバーと旧LINE社データセンター内のサーバー間の通信について、ファイアウォールポリシーを継続的に見直しております。

- 3ヶ月に一度の設定メンテナンスにて不要と判断したファイアウォールポリシーを削除しました。【2024年12月完了】

今後もサーバー移転の完了や委託業務の終了に伴う不必要な通信の遮断の実施と3ヶ月に一度のファイアウォールポリシー設定のメンテナンスを実施してまいります。
【2026年3月末完了目標】

(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

NAVER Cloud社データセンターのNAVER社認証基盤に残る一部従業員情報等の削除は、予定どおりに進行中です。
【当社及び国内子会社 2025年4月末、海外子会社 2026年4月末完了予定】

また2024年6月28日付報告のとおり、当社が利用するNAVER社及びNAVER Cloud社が管理するシステムについても、2026年3月末までにシステム分離を完了し、NAVER Cloud社の認証基盤の利用停止が完了する予定です。
【当社 2025年3月末、国内子会社 2026年3月末に完了予定。海外子会社 2026年3月末完了目標】

※ 2024年12月27日時点の実施・検討状況です。

技術的安全管理措置の不備の是正 - 第1 (3/3)・第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

(3) NAVER社及びNAVER Cloud社のシステム分離

2024年6月28日付報告のとおり、NAVER社及び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。現在は、対象システムごとに策定したプロジェクト計画に則り分離プロジェクトを進行中です。
【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月末に完了予定。海外子会社 2026年3月末完了目標】

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

二要素認証が未適用だった旧ヤフー社データセンターにある一部システムについて、2024年10月末に二要素認証の適用を完了しました。
この対応により、当社従業者が利用するすべての社内システムへの二要素認証の適用が完了しました。【2024年10月末完了】

※ 2024年12月27日時点の実施・検討状況です。

※1 NAVER社及び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2025年1月にシステム分離、2025年3月ないし6月までに利用停止

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) 社外環境と旧LINE社データセンター間の接続経路の総点検

社外環境と旧LINE社データセンター間の接続経路におけるネットワークアクセス制御については、今後も定期的な点検や見直しを実施し、継続的な維持・改善に取り組んでまいります。

旧LINE社データセンターからNAVER Cloud社データセンターへのアウトバウンド通信制御は、立案した計画に従ってファイアウォールポリシーを順次適用し、2024年12月末に不必要な通信の点検を完了しました。併せて、アウトバウンド通信に対するファイアウォールポリシーの新規追加に備えた申請プロセスを構築しました。以降、継続的にファイアウォールポリシーのメンテナンスを実施していきます。
【アウトバンド通信に対するファイアウォールポリシーの適用を2024年10月に完了、2024年12月点検完了】

(2) サイバーセキュリティ対策及びセキュリティ監視にかかる効果検証と抜本改善・強化

- ペネトレーションテスト実施結果を踏まえた追加策
  2024年8月末に立案した是正計画に則り、本テストによる発見事項のうち優先度が高いものから順次対応を行っております。【2025年3月末完了予定】
- 振る舞い検知等の仕組みや相関分析ルール等の見直し結果を踏まえた追加策
  振る舞い検知や相関分析ルールの仕組みに関する効果検証の結果を踏まえ、2024年12月に一部の検知ルールを当社SIEM※1環境へ実装しました。
  今後も継続して、当社SIEM環境による検知能力向上に向け順次是正を行います。【2025年2月是正完了予定】

※ 2024年12月27日時点の実施・検討状況です。

※1　様々なログを集約・管理し相関した分析を行うシステム。セキュリティインシデントの早期発見に使用しています。

組織的安全管理措置の不備の是正 - 1 (1/4)

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 (2/4)

報告事項
（抜粋）

第４　個人データの取扱状況の把握並びに安全管理措置の評価、見直し及び改善について

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

①　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

2024年7月1日付で施行した委託先管理に関する基本方針及び委託先管理に関する基本規程に基づき、7月1日より新基準での運用として、サプライヤ評価及び案件リスク評価を開始し、その評価結果に応じたリスク管理を実施しています。また、これらのサプライヤ評価・案件リスク評価を終了しなければ契約締結及び発注を実施することはできないよう運用されております。【2024年7月運用開始済】

②　自社としての侵害の有無や範囲を把握すること

①当社発番アカウントを用いて当社ネットワークにアクセス可能な委託先、②その他の当社の業務に関わる委託先のうち、PC貸与が実施されていなかった委託先に対しては、PC貸与を完了し、かつ、当社貸与PC以外からのアクセス遮断及び不要と判断したアカウント自体の削除を実施しております。なお、貸与端末の持ち込みが制限されている等、委託先における業務全体のセキュリティ確保のためを理由として、当社CISOによる承認プロセスを経た委託先は貸与対象外となります※1。
【2024年9月末PC貸与完了、2024年10月アクセス遮断、その後不要と判断したアカウント自体の削除を完了】

一方、追加措置として、対象を拡大してPC貸与を実施するとした、上記①・②以外の当社ネットワークにアクセスすることができる委託先へのPC貸与については、対象の特定を完了させ、PC貸与プロセスの構築を進めております。【2025年3月末完了予定】

※ 2024年12月27日時点の実施・検討状況です。

※1　当社CISO承認プロセスを経た上での時限的な措置として貸与対象外としておりますが、委託業務の見直しを含め対応を見直しております。

組織的安全管理措置の不備の是正 - 1 (3/4)

報告事項
（抜粋）

第４　個人データの取扱状況の把握並びに安全管理措置の評価、見直し及び改善について

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

①NAVER Cloud社における対応

2024年6月28日付報告のとおり、現地での実査に加えて、業務委託の内容に応じた監査を2024年4月末※1、及び2024年6月末※2までに完了しております。
それらの監査等を通じて、是正要求事項に対しては是正済みとの確認が取れております。その後については、年に1回の頻度での監査を実施していくことを計画しております。
【2024年4月末及び6月末監査完了、以降年に1回の頻度で定期的に監査を実施予定】

②NAVER Cloud社との関係について

ア　リスク可視化・評価の新たな仕組みの設計

従業員が普段感じている表面化しないリスクを気軽に伝えられる仕組み作りの一環として、2024年7月に実施した全従業員へのセキュリティに関するアンケートの結果に基づき、課題解決に向けた取組を継続的に推進しております。取り組みの進捗については、社内イントラネットへの掲示や集会等を通して従業員に公開しております。

また、全従業員からコンプライアンス視点での意見を収集する活動として、LINEヤフーグループの行動規範に関するアンケートを2024年11月に実施しました。
【LINEヤフーグループ行動規範に関するアンケートを2024年11月に実施完了】

今後も、吸い上げた従業員の意見を経営層及び関連部門に共有し、課題解決や改善を行ってまいります。

※ 2024年12月27日時点の実施・検討状況です。

※1　経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律に基づく特定重要設備の供給元及び維持管理に関する業務委託先への監査
※2　当社が定める当社重要システムの保守運用に関する業務委託先への監査

組織的安全管理措置の不備の是正 - 1 (4/4)

報告事項
（抜粋）

第４　個人データの取扱状況の把握並びに安全管理措置の評価、見直し及び改善について

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

②NAVER Cloud社との関係について

イ　NAVER社側（NAVER社及びその子会社）・NAVER Cloud社への委託業務の終了・縮小計画策定

2024年6月28日付報告のとおり、NAVER社側が提供するシステムやサービスの利用が対象に含まれる形で、委託関係の終了・縮小の基本的な考え方とその具体的な対象範囲・方針を当社として検討・策定したほか、実現に向けた具体的な計画を策定して実際の終了・縮小の取組作業に着手しています。現在は遅延なく計画どおり進行中です。
なお、一部残置する業務についても、リスクアセスメント結果を踏まえた追加措置を計画に則り進行中です。
【当社からNAVER社・NAVER Cloud社への委託：2025年12月末まで目標】
【当社からその他NAVERグループへの委託：2025年3月末まで目標】
【技術・システム利用及びサービス企画・機能・開発委託：2026年3月末まで目標】

※ 2024年12月27日時点の実施・検討状況です。

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）

第４　個人データの取扱状況の把握並びに安全管理措置の評価、見直し及び改善について

２　令和３年行政指導後の対応に関する問題点の改善

当社セキュリティ規程に定める安全管理措置の中から確認項目を選定し、重要システムを対象に遵守状況の確認を行いました。【2024年10月完了】
確認された安全管理措置の未遵守箇所については、是正が完了しました。【2024年12月末完了】
上記一連の取り組みは、重要システムに対するセキュリティ向上のため、2025年4月以降も定期的に実施してまいります。

また、時流等に応じた安全管理措置の見直し計画として、12か月周期の安全管理措置の見直しプロセスを詳細化したうえで、その実施計画を定めました。
【2024年11月完了】

※ 2024年12月27日時点の実施・検討状況です。

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）

第５　漏えい等事案に対応する体制の整備についての改善

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

外部機関の評価を得た計画に基づき、インシデント発生時の初期行動フローや調査範囲判断プロセス、ステークホルダー及びその役割と責任の整備等の対応を完了しました。【2024年10月完了】

また、上記実効性担保のための定期演習については、2024年12月より開始しており、2025年3月まで複数回実施する予定です。2025年4月以降も継続的に実施してまいります。【2024年12月から2025年3月の間に定期演習を複数回実施予定】

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）

NAVER Cloud社に委託していたSOCのTier1監視業務について、当初計画どおり、2024年10月1日より国内企業との24時間365日体制の日本での運用を開始（NAVER Cloud社への委託は終了）しました。【2024年10月より運用開始】

※ 2024年12月27日時点の実施・検討状況です。

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）

第６　組織体制の整備等についての改善（安全管理措置が徹底される組織体制の整備）

１　セキュリティガバナンス委員会の組成

2024年4月に設置した「セキュリティガバナンス委員会」では、再発防止等を含む社内プロジェクトからの報告及び方針判断を含む当社セキュリティガバナンス全般について議論をしており、特に再発防止等に関連する各プロジェクトにおける進捗状況の確認・フィードバック等を継続しております。

２　グループCISO Boardの設置

2024年4月に設置した「グループCISO Board」では、引き続き当社の実施している再発防止策に関するグループ会社への共通的な適用を優先的な議題としている他、共通的なセキュリティ規程の適用等のグループ共通ルールに関する議論も継続実施し、これらを通じてグループとしてのセキュリティレベルの平準化及び底上げに努めてまいります。

※ 2024年12月27日時点の実施・検討状況です。

参考情報

※これまでの公表内容

個人情報保護委員会への報告書の提出等について　（2024年4月26日公表）
https://www.lycorp.co.jp/ja/news/announcements/008285/

2024年6月28日 個人情報保護委員会への報告書の提出について　（2024年6月28日公表）
https://www.lycorp.co.jp/ja/news/announcements/008728/

2024年9月30日 個人情報保護委員会への報告書の提出について　（2024年9月30日公表）
https://www.lycorp.co.jp/ja/news/announcements/009358/

LINEヤフー