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9月30日提出報告書（概要）

2024年9月30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9月30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/

※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/

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/

目次

上記について、2024年9月30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9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9月30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どおりに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

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対応については、下記のとおり対応を進めています。**【2024年10月末完了目標】**

- 前段の作業となる当社統合Active Directory（以下、ADと記載）をリリース**【2024年8月完了】**
- 対象システムに対して個別に技術検証を実施し、移行方式と対応スケジュールを確定**【2024年9月完了】**

※ 2024年9月30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いて、ネットワークアクセス制御の適切性、及びインシデント対応の準備状況に関する総点検を行いました。

- ネットワークアクセス制御の適切性について、点検に基づく是正対象に対し、不必要な通信許可ルールの修正及び削除を行いました。
  【2024年8月末点検完了※1、9月末是正完了】
- インシデント対応の準備状況について、問題なく対応済であることを確認いたしました。**【2024年7月末完了】**

また、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2024年10月末までにファイアウォールポリシーを順次適用し、2024年12月末までに上記総点検を踏まえた不必要な通信の点検を行います。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。
【2024年8月末計画立案完了、2024年12月末点検完了予定】

(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

外部企業のホワイトハッカーにより、旧LINE環境における管理・運営系環境や本番環境に対するペネトレーションテストを行いました。テストを通じて、サイバーキルチェーンを効果的に分断できている点やこれまで実施した再発防止策の効果および本番環境の堅牢性について評価をいただいたものの、多層防御の観点から複数の発見事項を提示いただき、それらに対する是正計画を立案しました。**【2024年8月末完了】**
今後は是正計画に則り、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まいります。**【2025年3月末完了予定】**
また、ペネトレーションテストを年に一度実施することで、変化していく脅威にも対応可能なセキュリティレベルの維持・向上サイクルを実現することを目指します。

外部企業のホワイトハッカーが本事案で使用された攻撃手法や当社の業種業態で頻繁に用いられる攻撃手法から疑似攻撃を行い、振る舞い検知や相関分析ルールの仕組みがどれだけ効果的に対応できるかを検証しました。**【2024年8月末完了】**
本テストで未検知となった疑似攻撃項目については、当社SIEM環境による検知能力向上を主軸に順次是正を行います。**【2025年2月是正完了予定】**
なお、上記是正を実施した後も、検知ルールの最適化や被害影響度に基づいた改善について、SOCによる通常のルール維持活動の一環として取り扱い、継続的な改善を実施していきます。

※ 2024年9月30日時点の実施・検討状況です。

※1 点検対象ポリシーの設定の複雑さに伴い、詳細調査に当初想定以上の時間を要することが判明したため、完了期限を7月末から8月末に延期の上、対応完了いたしました

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

委託先管理の高度化に向け策定された基準に基づく監査について、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、同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ております。**【2024年7月運用開始準備完了、以降順次運用開始】**

②　自社としての侵害の有無や範囲を把握すること

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に対して、当社の、または当社と同水準のセキュリティソフトウェアを導入していることが確認・担保できているグループ会社のPCでのみ業務の実施を認める方針としております。

一部の個別事象として、委託先の業務全体のセキュリティ確保のため貸与端末の持ち込みが制限されている等を理由として当社CISOによる承認プロセスを経た委託先を除き※1、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、および②①以外で当社の業務に関わる当社ネットワークにアクセス可能な委託先のうち、PC貸与が実施されていなかった委託先に対するPC貸与を完了しております。**【2024年9月末完了】**

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、2024年10月より開始してまいります。**【2025年3月末完了予定】**

※ 2024年9月30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確認したところ、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

社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を作るための改善活動の一環として、全従業員へのセキュリティに関するアンケートを実施しました。
【2024年7月実施完了、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月実施予定】

アンケートを実施した結果、回答率は98%、自由記載の意見が約1,500件集まりました。これらの意見はマネジメントにも共有し、課題解決の取組や検討を開始しております。
これらの取組や成果については、従業員にも公表していく予定です。

※ 2024年9月30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。

【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】

また、残置する業務に関するリスクアセスメントは2024年7月から着手し、同年9月末時点で当社における評価を完了しています。**【2024年9月末完了】**
なお、当社セキュリティ部門から行った評価の結果、追加での措置を要するものについては、各業務の関係者と協議の上で実行計画（追加措置の内容決定および完了期限の設定）を策定しております。

※ 2024年9月30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

重要システムの定義及び重要システムに対する追加の安全管理措置について、当社情報システムの各ライフサイクルステージにおけるセキュリティ要求事項を定めた細則に追加し、定義に沿って重要システムを特定しました。**【2024年7月1日細則追加完了、同年9月重要システムの特定完了】**
今後の実施計画は、下記のとおりです。

- 重要システムに対する安全管理措置遵守状況の確認**【2024年10月上旬完了予定】**
- 重要システムに対する安全管理措置未遵守箇所のリスクアセスメント**【2024年12月末完了予定】**
- 時流等に応じた安全管理措置の見直し計画策定**【2024年12月末完了予定】**

※ 2024年9月30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進めています。**【2024年10月完了予定】**

また、上記実効性担保のための定期演習については、予定どおりに準備を進めています。**【2024年10月から2025年3月の間に定期演習予定】**

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、国内企業への業務トレーニングが完了し、2024年7月から仮運用を実施しております。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日体制の運用を開始（NAVER Cloud社への委託は終了）します。**【2024年10月より運用開始予定】**

※ 2024年9月30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、同年7月以降は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。議論の状況等は、当社執行役員に定期的に共有すること等を通じて、全社で再発防止やセキュリティガバナンスの向上に向けた意識を共有するように努めています。

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開始しており、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9月30日時点の実施・検討状況です。

LINEヤフー