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6月28日提出報告書（概要）

2024年6月28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6月28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/

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　NC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

NC社インフラを利用した当社本番環境用のサーバーのうち日本のユーザーに係るサーバー・データの日本国内移転※1に伴ってファイアウォールのポリシーの見直し・設定変更を行いました。また、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の削除・ポリシーの見直しを行いました。**【2024年6月完了】**
今後は、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。
【2026年3月末※2完了目標として計画を前倒し】

(2) NC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

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ました。**【2024年6月完了】**

また当社が利用するNAVER社及びNC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、 NC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※2完了目標として計画を前倒し】

(3) NAVER社及びNC社のシステム分離

NAVER社及びNC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。対象システムごとにプロジェクト計画を策定完了し、分離プロジェクトを進行中です。
【従業員向けシステム※3については当社 2025年3月末※4、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※2完了目標として計画を前倒し】

国内・海外子会社に対して順次システム分離を進めていきますが、進行期間中のリスクに対しては、システムへの二要素認証の適用、アクセス範囲の精査や不必要な通信の遮断を継続的に行うことで対策してまいります。

※1 LINEのデータ移転に関するご説明：https://www.lycorp.co.jp/ja/news/announcements/000823/
※2 当初の完了時期は2026年12月末
※3 NAVER社及びNC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
※4 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

旧ヤフー社データセンターにある一部システムを除いて二要素認証のシステム適用を完了しています。**【2024年3月完了】**

追加策として、スマートフォンの持ち込みが禁じられている特定の制限エリアで利用可能な認証デバイスを配布し、制限エリアで業務を行う主な従業員アカウントに対する二要素認証の追加適用を完了しました。**【2024年6月末完了】**

また、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は、前段の作業となる当社統合Active Directory(以下、ADと記載)の新規構築を進めており、8月には当社統合ADへの移行作業と合わせて二要素認証の適用作業を開始する予定です。本対応においては計画の前倒しを検討中です。**【2024年10月末完了目標】**

(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月末完了】

重要システムへのセキュリティ診断を完了しています。

また、必要なセキュリティ診断の仕組みの構築及び重要システムの選定基準の定義や分類、これらシステムに要求するセキュリティ対策の基準等の実施状況については、P.13にて詳述いたします。

技術的安全管理措置の不備の是正 - 第3 (1/2)

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す。
【2024年7月末完了予定】

旧LINE社データセンターからNC社データセンターへのアウトバウンド通信についても適切にネットワークアクセス制御を行っていく方針とします。具体的なネットワークアクセス制御の考え方やポリシー、ファイアウォール等への適用について、上記総点検の結果を踏まえて計画を立案します。**【2024年8月末計画立案予定、以降計画に基づき実施】**

(2) 外部企業を交えた計画策定

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、外部企業の提言を踏まえた対策の立案・計画策定・是正策の推進を継続してまいります。当社データセンターでの対応が必要な項目の対応状況は次のとおりです。

- 旧LINE社データセンターのWindowsサーバーに対して、機能として利用しているサーバーを除き、管理共有機能を無効化**【2024年6月完了】**
- 社内システム上でのパスワード保存不可に関する注意喚起及び全従業員向けのe-Learningを実施**【2024年4月末完了】**

また、NC社データセンターでの対応が必要な項目については、対策が適切に実施されていることを確認しました。**【2024年5月末完了】**

技術的安全管理措置の不備の是正 - 第3 (2/2)

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

(3) 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

理論上のリスクだけでなく、実際に当社システムにおいてはどのように攻撃されうるかを実証的に把握・評価することを目的にペネトレーションテストを実施します。

- ペネトレーションテストの実施完了・結果分析**【2024年7月末完了予定】**
- テスト結果を踏まえた是正計画策定**【2024年8月末完了予定】**

また、既知の攻撃に加え、ゼロデイ等の未知の脅威に対する耐性や有効性等を外部機関を交えて評価・検証・改善することを目的に、現在当社データセンターにて運用されている振る舞い検知等の仕組みや相関分析ルール等を見直しています。

- 外部企業を交えた現状分析・有効性検証**【2024年7月末完了予定】**
- 検証結果を踏まえた是正計画策定**【2024年8月末完了予定】**

組織的安全管理措置の不備の是正 - 1 (1/5)

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 (2/5)

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　NC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セキュリティリスク評価基準の見直し【2024年3月チェックシートの新設完了、以降順次更新】
新設及び更新を実施したセキュリティチェックシートを活用し、監査の実施を行っております。

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及び基準の策定並びにその実施
【2024年7月運用開始準備完了、以降順次運用開始】

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月より順次運用を開始するにあたり、同年4月1日以降に新基準での運用の先行実施として、新基準での監査を実施し、また同年5月15日より一部業務委託先を対象としたトライアル運用を開始し、新基準での多面的リスク評価のテスト実施を行ってまいりました。
今後は、運用開始後に発生した個別事象等を踏まえて必要な追加措置を講じるほか、追加措置の検討にあたっては、基準策定時と同様に、外部企業の助言を受け、外部の客観的な目線も入れつつ委託先管理モデルの更なる高度化を検討していきます。

組織的安全管理措置の不備の是正 - 1 (3/5)

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　NC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

③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、当社がキッティングを実施した当社のPCでのみ業務の実施を認める方針としており、国内外ともに2024年9月末までのPC貸与を完了すべく計画どおり進捗させております。
【2024年9月末完了予定】

一方、追加措置として、PC貸与の対象を拡大させる計画を立てております。最終的には当社からの業務委託か否かに関わらず当社ネットワークにアクセスすることが可能な委託先に対しては、原則として、当社の、あるい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を貸与することといたします。その実施方針としては、当社の業務に関わる委託先に対するPC貸与を2024年9月末までに実施することとし、その他については、2024年度中にPC貸与の実施を完了させることを計画しております。
【グループ会社発番アカウントのうち当社業務を実施している委託先：2024年9月末完了予定】
【その他、上記以外で当社ネットワークにアクセスすることが可能な委託先：2025年3月完了予定】

組織的安全管理措置の不備の是正 - 1 (4/5)

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　NC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NC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

①NC社における対応

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、SOCに関する当社とNC社との業務委託関係については、2024年9月末をもって解消の予定です。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】**

②NC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

問題意識が担当部門内に留まり、組織全体の問題として対処できなかったことがリスク管理上の課題であると認識しています。この課題に対処するため、社員が普段感じている潜在的なリスクについて心理的安全性を担保した上で伝えられる仕組みを作るための改善活動の一環として、全従業員へのアンケートを実施する予定です。
【2024年7月及び11月実施予定】

※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 (5/5)

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　NC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NC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

②NC社との関係について

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

当社からNAVER社側への委託関係全般について検討を行うべく、継続的な役務やシステム等の提供関係にあると考えられるもの全てについて、その終了・縮小・残置の方針を決定しました。

委託関係は大きく「当社におけるNAVER社側技術及びシステム利用」と、「当社事業に関するNAVER社側へのサービス企画・機能・開発委託」に大別され、前者と後者の両方に対する取組を実施することにより、NAVER社側が当社に対して提供するシステムやサービスの利用全般について対象に含まれることになると理解しています。

当社とNAVERグループとの委託関係の取組一つ一つについて、具体的な計画（主要な委託内容、今後の具体的方針、最短での完了目標時期等の初期的見積もり等）の立案を実施したほか、それらのうち直ちに実施可能なものについて NAVER社側との協議・交渉を含む、終了・縮小等に向けた作業を開始しており、システム・ネットワークの運営委託及びサービス開発・運用委託については、原則として終了する方針としています。サービス企画・機能・開発委託について、委託関係ごとの最短終了（目標）時期は以下のとおりとなります。
【当社からNAVER社・NC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】

また、市販SaaSの利用、汎用類型APIの利用、海外事業、当社子会社とNAVER社側の間でのインフラ等利用・委託関係、さらには当社がNAVER社側に提供している役務やシステムに関する関係についても、今後の方針（終了・縮小・残置）を決定しました。今後は決定した方針に沿って実行してまいります。
【技術・システム利用及びサービス企画・機能・開発委託について2024年6月計画立案完了。順次終了・縮小に向けた作業開始済み】

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

令和３年行政指導後に改善する機会があったにも関わらず、個人データへのアクセスに対する多要素認証の導入が遅れていました。これは適用範囲と対象の具体的な定義が確立されていなかったこと、二要素認証を適用しない場合の判断基準やそのプロセスを適切に記録する仕組みが整っておらず、初期判断後の状況変化に対応するための再評価プロセスも設けられていなかったことが原因と考えております。

この問題に対する取組として、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定義したうえで、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、それに伴うリスクについて経営層も交えて全社的に把握・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る予定です。
【2024年6月末基準定義・仕組み構築完了、2024年7月1日規程化完了予定、以降定期的に見直し】

今後の実施計画は、下記のとおりです。

- 重要システムの特定及びそれらに対する安全管理措置遵守状況の確認**【2024年9月上旬特定、2024年10月上旬確認 完了予定】**
- 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】**

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

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に関する改善計画を立案します。計画について、外部機関の評価を得た上で改善を実施の上、その後定期的に演習を実施していきます。
【2024年6月末計画立案・外部評価完了、以後2024年度下期に定期演習予定】

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）

SOC Tier1業務について、現在、国内企業への業務トレーニングを実施しております。2024年7月より国内企業との仮運用を実施し実務経験を積んだ後に、予定どおり同年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します。
【2024年10月より運用開始予定】

※対応中の取組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。z

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　セキュリティ規程の遵守状況をモニタリングするための監査部門の設置

P.13　２記載の重要システムのリスクを把握・評価する仕組み構築にあたり、当社内部監査部門に加えてセキュリティ主管部門下にセキュリティ監査部門を設けました。このセキュリティ監査部門では、システム主管部門でのセキュリティ規程の遵守状況をモニタリングし結果をCISOへ報告します。また、内部監査部門においては、セキュリティ監査部門によるモニタリング活動を含めて監査の対象として、当社のセキュリティリスクマネジメント体制の監査を実施します。

２　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」では各種の社内議論・検討を行っています。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。

３　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おり、これまで特に二要素認証の適用、委託先管理に係る施策の議論・各社への展開を行っております。

LINEヤフー