3月5日付及び4月16日付
総務省からの行政指導に対する
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、総務省からの2024年3月5日付及び2024年4月16日付の行政指導に対し、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、安全管理措置及び委託先管理の抜本的な見直し及び対策の強化や、親会社等を含むグループ全体でのセキュリティガバナンスの本質的な見直し及び強化等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り組んでまいります。

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
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日公表）
https://www.lycorp.co.jp/ja/news/2024/20240401_appendix_ja.pdf

3月5日付及び4月16日付総務省からの行政指導に対する7月1日提出報告書（概要）　（2024年7月1日公表）
https://www.lycorp.co.jp/ja/news/2024/20240701_appendix1_ja.pdf

NAVER社側との委託関係等の今後の方針と計画等について（2024年7月1日公表）
https://www.lycorp.co.jp/ja/news/2024/20240701_appendix2_ja.pdf

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。

令和6年4月1日付報告書「一　本事案を踏まえた安全管理措置及び委託先管理の抜本的な見直し及び対策の強化について」記載の施策実施状況等

4月16日付総務省行政指導

（１） 本事案を踏まえた安全管理措置及び委託先管理の抜本的な見直し及び対策強化の加速化について

- 現段階において、明確な実施計画が策定されていない安全管理措置及び委託先の見直しについて、早期に計画を策定し提出するとともに、着実に推進すること（特に、貴社とNAVER社側との間で共通化されていたネットワークの分離措置について、明確な計画を早急に策定しこれを実施すること。）。
- 今後実施予定の対策について、着実にその内容を実施するとともに、可能なものについては、計画スケジュールを前倒しして実施すること。
- 現時点で実施済みの対策や今後１年以内に実施予定の計画（特に認証基盤の分離やSoC業務の独立運営）について、その内容が再発防止の観点から十分なものであるか、今後も計画の進捗及び効果検証を継続し、必要に応じて追加の対策を講じること。

令和6年4月1日付報告書「一　本事案を踏まえた安全管理措置及び委託先管理の抜本的な見直し及び対策の強化について」記載の施策の実施状況等 - 第1（1/2）

報告事項
（抜粋）

第１　NAVER Cloud社と当社のプライベートネットワーク分離

１　ネットワークアクセス管理の強化に関する追加策

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　従業員向けシステムに対する二要素認証の適用に関する追加策

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 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

令和6年4月1日付報告書「一　本事案を踏まえた安全管理措置及び委託先管理の抜本的な見直し及び対策の強化について」記載の施策の実施状況等 - 第1（2/2）

報告事項
（抜粋）

第１　NAVER Cloud社と当社のプライベートネットワーク分離

３　NAVER社及びNAVER Cloud社のシステム分離

2024年7月1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】

４　プライベートネットワーク完全分離

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】

※ 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

令和6年4月1日付報告書「一　本事案を踏まえた安全管理措置及び委託先管理の抜本的な見直し及び対策の強化について」記載の施策の実施状況等 - 第2・第3

報告事項
（抜粋）

第２　認証基盤の分離

１　NAVER社認証基盤からの従業員情報等の削除と当社認証基盤へのパスワード連携の停止

2024年7月1日付報告のとおり、NAVER社認証基盤から不要になった当社グループ従業員情報等の削除及び当社認証基盤へのパスワード連携の停止を実施済みです。

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】

２　NAVER社及びNAVER Cloud社が管理するシステムの認証基盤利用停止

2024年7月1日付報告のとおり、NAVER社及びNAVER Cloud社管理のシステムの認証基盤利用停止については下記のとおり実施します。
【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】

第３　SOC国内化・ログ取得

１　SOC業務の独立運営

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】

２　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】

※ 2024年9月30日時点の実施・検討状況です。

令和6年4月1日付報告書「一　本事案を踏まえた安全管理措置及び委託先管理の抜本的な見直し及び対策の強化について」記載の施策の実施状況等 - 第4

報告事項
（抜粋）

第４　安全管理措置の見直し

１　重要システムに対するアクセス管理強化に関する追加策

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】

２　ペネトレーションテスト実施

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。

３　振る舞い検知等の仕組みや相関分析ルール等の見直し

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。

令和6年4月1日付報告書「一　本事案を踏まえた安全管理措置及び委託先管理の抜本的な見直し及び対策の強化について」記載の施策の実施状況等 - 第5・第6

報告事項
（抜粋）

第５　委託先管理見直し

１　策定された基準に基づく委託先管理・監査の実施

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　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への当社PC貸与

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】

第６　当社によるNAVER Cloud社是正

１　NAVER Cloud社に対する定期的な監査の継続

2024年7月1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※2、及び2024年6月末※3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】

※ 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
※2　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
※3　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

令和6年4月1日付報告書「二　親会社等を含むグループ全体でのセキュリティガバナンスの本質的な見直し及び強化について」記載の施策の検討状況 - 第1・第2

4月16日付総務省行政指導

（２） 親会社等を含むグループ全体でのセキュリティガバナンスの本質的な見直しの検討の加速化について

- 報告書にある「NAVER社側への委託関係を順次縮小・終了していく方針」について、当該方針の対象となる「NAVER社側への委託」について、基本的な考え方とその具体的な対象範囲を報告すること。特に、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のか明らかにすること。
- その上で、「NAVER社側への委託関係を順次縮小・終了していく方針」について、実現に向けた具体的な計画（どの委託について、いつまでに、縮小・終了・残置するのか）を策定し、報告すること。

報告事項
（抜粋）

2024年7月1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。

令和6年4月1日付報告書「二　親会社等を含むグループ全体でのセキュリティガバナンスの本質的な見直し及び強化について」記載の施策の検討状況 - 第2

4月16日 付総務省 行政指導

（２） 親会社等を含むグループ全体でのセキュリティガバナンスの本質的な見直しの検討の加速化について

- 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め、委託先への適切な管理・監督を機能させるための経営体制の見直しについて、親会社等を含めたグループ全体での検討を早急に実施し、その検討結果を具体的に報告すること。

報告事項（抜粋）

第１　資本的な関係の見直しについて

2024年3月5日の行政指導以降、当社としては「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」のための方策の一つとして、親会社であるAホールディングス社の資本関係の見直しを同社株主であるソフトバンク社及びNAVER社に依頼しました。ただし、現状では両社の間で短期的な資本の移動には困難が伴うとの認識に至っていると共有を受けています。当社としては、これまでの経緯を踏まえ、当社としても議論が進展するよう、引き続き取り組んでいく方針です。

第２　当社経営体制の見直しについて

2024年7月1日付報告のとおり、 2024年6月開催の当社株主総会での承認を経て、本株主総会後の体制として当社は取締役6名体制、うち独立社外取締役・監査等委員が4名を占める体制となりました。これによって、ガバナンスの強化が図れるものと認識しております。

第３　セキュリティガバナンスの確保にかかる体制構築

当社及びNAVER社のCEOを構成員とするステアリングコミッティにて、引き続き委託終了に伴う協議を行っています。

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。

また、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。

※ 2024年9月30日時点の実施・検討状況です。

令和6年4月1日付報告書「三　利用者対応の徹底について」記載の施策の実施状況

4月16日 付総務省 行政指導

（３） 取組内容に係る進捗状況の定期的な公表等を通じた利用者対応の徹底について

- 引き続き、二次被害の発生把握や本事案に関する利用者への適切な情報提供を継続するとともに、上記（１）（２）の取組内容及びその進捗状況について、定期的にアップデートした情報を公表するなどして、利用者理解の確保に努めること。

報告事項 （抜粋）

第１　取組内容に関わる進捗状況の定期的な公表等を通じた利用者対応

2024年4月1日に当社コーポレートサイトにて公開した特設ページにおいて、引き続き再発防止の対応状況に関する情報提供を行ってまいります。

第２　二次被害の発覚時の対応

2024年7月1日付報告のとおり、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の一つとして、継続的にダークウェブ等のモニタリングを行っているところ、合理的な期間が経過するまでの間、当該モニタリングを強化し、二次被害の早期発見と拡大防止に努めるとともに、万一、情報の流出を確認した場合には、速やかに利用者へ通知を実施します。

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い、二次被害の発生を確認した場合には、必要な対応を適切に実施してまいります。

※ 2024年9月30日時点の実施・検討状況です。

LINEヤフー