

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

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7月1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

目次

01

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

02

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

03

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

「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

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。

「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

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】

追加策として、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NAVER Cloud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 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月末完了目標に前倒し検討中】

「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

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※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※3完了目標として計画を前倒し】※詳細は、補足資料をご参照ください。

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。

4 プライベートネットワーク完全分離

NAVER Cloud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※4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を削除しました。【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※3完了目標として計画を前倒し】

※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員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

※3 当初の完了時期は2026年12月末

※4 LINEのデータ移転に関するご説明：<https://www.lycorp.co.jp/ja/news/announcements/000823/>

「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

報告事項
(抜粋)

第2 認証基盤の分離

1 当社管理システムにおける認証基盤の分離に関する追加策

当社管理システムにおける認証基盤の分離を2024年3月末に完了したため、NAVER Cloud社から受領したログをもとに、NAVER Cloud社の認証基盤から当社管理システムへの認証連携設定が削除され、認証不可になっていることを確認しました。

【2024年6月完了】

2 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

運用面における分離として、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。

【2024年6月完了】

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引き続き進めてまいります。

【当社及び国内子会社 2025年4月、海外子会社 2026年4月完了予定】

なお、一部従業員情報等の残存に対するリスク対策としては、以下を実施済みです。

- ・ 当該従業員情報等 のうち、不必要な情報項目・認証情報の削除
- ・ NAVER社認証基盤が保有する認証情報を利用した当社データセンターのシステムがないことの再確認

3 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

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※1完了目標として計画を前倒し】

※1 当初の完了時期は2026年12月末

「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3

報告事項
(抜粋)

第3 SOC国内化・ログ取得

1 SOC業務の独立運営

NAVER Cloud社管理の監視ログについては、予定どおり国内化を完了し、すでに国内にあるログを利用した監視に移行済みです。
【2024年3月完了】

NAVER Cloud社に委託していたSOCのTier1監視業務を国内企業への委託に切り替え、当初計画どおり、品質と効果を担保しながら着実に遂行する所存です。【2024年10月より運用開始予定】

本施策により、ログデータ、分析システム、Tier1監視業務を国内に移管することで、SOC業務全般を国内で完結させることが可能となります。これにより、セキュリティインシデントに対するより迅速な対応が実現できると考えています。

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

上記計画と連携するものとして、セキュリティインシデントに対するより迅速な対応を実現するための取組として、インシデント対応態勢の改善を行います。

具体的には、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】

「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（1/2）

報告事項
（抜粋）

第4 安全管理措置の見直し

1 AD管理の是正に関する追加策

2023年12月にADに振る舞い検知ソリューションを導入し、当該ソリューションが再発防止として有効であることを検証するため、本事案で検知が不十分だった攻撃手法を模擬的に再現することで、適切に検知ができることを確認済みとなります。【2024年1月完了】

2 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

施策の効果検証を継続し、重要システムに対するセキュリティ水準を持続的に向上させるための追加策として、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決めました。【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、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月未完了予定】
- ・ 時流等に応じた安全管理措置の見直し計画策定【2024年12月未完了予定】

3 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月未完了】

また、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、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月未完了】

「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（2/2）

報告事項
（抜粋）

第4 安全管理措置の見直し

4 ペネトレーションテスト実施

本事案に関わる再発防止策の充分性や効果を検証するとともに、未知の脅威に対する態勢等も含めた包括的なリスク評価を実践的に行い、必要な追加策の特定やより効果的なセキュリティ対策や改善計画策定に繋げることを目的として、外部企業による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月未完了予定】
- ・ テスト結果を踏まえた是正計画策定【2024年8月未完了予定】

5 振る舞い検知等の仕組みや相関分析ルール等の見直し

「3 外部企業を交えた計画策定」（本資料8ページ参照）での外部企業による提言に基づき、当社データセンターで運用中の振る舞い検知システムや相関分析ルールを再評価します。

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

「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（1/2）

報告事項
（抜粋）

第5 委託先管理見直し

1 セキュリティリスク評価基準見直しに関する追加策

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。

【2024年3月チェックシートの新設完了、以降順次更新】

2 実効的な委託先管理実現のための監督方法の検討・基準策定に関する追加策

外部企業が活用するモデルを参考にしつつ、当社における委託先管理の高度化に向けた基準の策定を実施しました。これらの実際の運用を通じて、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。

【2024年3月基準策定完了、以後順次実施】

3 当社データセンターへのVPN接続時の二要素認証適用に関する運用状況

当社ネットワークにログイン又はアクセスする際の二要素認証の適用を完了しております。【2024年1月完了】

「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（2/2）

報告事項
（抜粋）

第5 委託先管理見直し

4 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。【2024年7月運用開始準備完了、以降順次運用開始】

5 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、当社がキitting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】

「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6

報告事項
(抜粋)

第6 当社によるNAVER Cloud社是正

1 NAVER Cloud社への当社・第三者企業による監査に関する追加策

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及び是正の指摘・要求を行いました。【2024年2月完了】

2 本件関係委託先企業への当社・第三者企業による監査・契約解除の状況

現地での実査を実施し、2024年3月末をもって契約関係を解消しております。【2024年3月未完了】

3 NAVER Cloud社に対する定期的な監査の継続

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NAVER Cloud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】

※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

「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

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・残置するか）を策定し、報告すること。

報告事項 (抜粋)

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・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】

※詳細は、補足資料をご参照ください。

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】

※詳細は、補足資料をご参照ください。

「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。

両社ともに協力的に対応いただいていますので、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ティで、2024年4月以降、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います。

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。

「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

当社コーポレートサイトに本事案の概要及び再発防止の進捗等について取りまとめた特設ページを2024年4月1日に公開いたしました。2024年3月5日付指導文書記載の「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」に関わる当社の各対応状況の進捗に関する情報提供を行っております。加えて、2024年4月16日付行政指導も踏まえ、「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」も含む進捗状況や、NAVER社への業務委託終了に向けた計画及び実施状況についても、報告書の提出にあわせ特設ページ上で公開しております。

第2 二次被害の発覚時の対応

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。

LINEヤフー