2024年3月5日付及び2024年4月16日付総務省からの行政指導に対する2025年3月31日提出報告書（概要）

2025年3月31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、2025年3月31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。
なお、現在取り組んでいる再発防止策の進捗については、今後も総務省へ報告してまいります。

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、2025年3月31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

2024年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

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　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。
当社利用システムについては、全システムの切替及び会計監査・税務申告に利用するデータがあるシステム以外の利用停止を2025年3月末に完了いたしました。
国内子会社利用システム・海外子会社利用システムについては、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月末切替完了※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】

2　NAVER Cloud社データセンターから旧LINE社データセンターへのプライベート通信完全分離

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】
その後も下記のとおり、不要となった通信の遮断を実施しております。

- 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※3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。【2024年6月完了】
- 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、関連するサーバーの利用停止に伴い、全ての通信を遮断いたしました。【2025年3月末完了】
- NAVER社及びNAVER Cloud社が管理する当社利用システムの分離やNAVER社またはNAVER Cloud社への委託業務の終了に伴い、不要となった通信を遮断いたしました。【2025年3月末完了】

今後も国内子会社利用システム・海外子会社利用システムの分離等に伴う不必要な通信の遮断と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】

※ 2025年3月31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 会計監査・税務申告に利用するデータがあるシステムは2025年6月に利用停止
※3 LINEのデータ移転に関するご説明：https://www.lycorp.co.jp/ja/news/announcements/000823/

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

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 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、 点検に基づく是正対象に対して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、2024年9月末是正完了】

旧LINE社データセンターからNAVER Cloud社データセンターへの通信制御は、上記総点検を踏まえた不必要な通信の点検を2024年12月末に完了し、是正対象となったファイアーウォールポリシーの修正・削除を実施いたしました。【2025年2月完了】
また、NAVER社及びNAVER Cloud社が管理する当社利用システムの分離やNAVER社またはNAVER Cloud社への委託業務の終了に伴い、不要となった旧LINE社データセンターからNAVER Cloud社データセンターへの通信を遮断いたしました。【2025年3月末完了】

今後も、ファイアーウォールポリシーの見直しを継続していきます。

４ 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適用を完了しました。【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】

最後に、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】

※ 2025年3月31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2・第3

報告事項
（抜粋）

第２　認証基盤の分離

２　当社管理システムにおける認証基盤の分離に関する対策

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】

３　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

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】

４　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社管理の当社利用システムについては、2025年3月末のシステム分離により認証基盤の利用を停止いたしました。
国内子会社利用システム・海外子会社利用システムについても、2026年3月末のシステム分離によって認証基盤の利用を停止する予定です。
【当社 2025年3月末完了。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業務の独立運営について

当社データセンターにてログ収集・分析システムの構築及びログの取得を行い、NAVER Cloud社に委託していたSOCのTier1監視業務について、2024年10月1日より国内企業との24時間365日体制のもと、日本での運用を開始（NAVER Cloud社への委託は終了）しております。【2024年10月より運用開始】

なお、上記ログ収集・分析システムに取り込んでいない、NAVER Cloud社環境におけるログ情報についても取得する体制・環境を構築しております。【2024年3月末完了】

２　事実関係の調査・原因究明等、漏えい等事案に対応する体制の整備

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ております。【2024年10月完了】
また、上記実効性担保のために2024年12月より定期演習を開始し、2025年3月までに複数回実施いたしました。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完了】

※ 2025年3月31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　AD管理の是正

本事案ではAD管理者権限を持つアカウントを奪取されたため、AD管理者アカウントの運用変更を行いました。また、2023年12月にADに振る舞い検知ソリューションを導入し、SOCによる監視を開始しました。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、本事案で検知が不充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】

更に、これらの対策に加え、外部企業によるコンサルティングを踏まえ、AD管理の是正を実施しました。【2024年3月完了】

２　重要システムに対するアクセス管理の強化

旧LINE環境における当社従業者が利用する各システム従業者のうち、個人情報をはじめ重要な情報を扱うシステム、侵害されるとこれらのシステムへの不正アクセスのリスクが増大するシステムを重要システムとして定義しました。

旧LINE環境における重要システムのうち、WEBインターフェースを有するシステムを対象に認証プロセスを迂回する試みや、認証要素を悪用する方法がないことを確認するセキュリティ診断を2024年3月末までに行い、発見された脆弱性の修正を完了しました。【2024年3月末完了】

３　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ました。【2024年7月1日規程化完了】

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】

※ 2025年3月31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

4　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・是正策の推進を行いました。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、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月末完了】

5　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】

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。

6　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月末に立案した計画に則り、本テストによる発見事項の是正対応及び是正に向けた仕組みの検討や運用プロセスの改善を行いました。【2025年3月末完了】
今後も策定した仕組みの導入や改善状況の定期的なモニタリングを実施してまいります。

7　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】

8　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て計画した全ての検知ルールを当社SIEM※1環境へ実装しました。【2025年2月是正完了】
今後も継続的に検知ルールの見直しを実施してまいります。

※ 2025年3月31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。

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

報告事項
（抜粋）

第５　委託先管理見直し

２　セキュリティリスク評価基準見直しについて

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1月チェックシートの新設完了、2024年3月チェックシートの強化完了】

３　実効的な委託先管理実現のための監督方法の検討・基準策定について

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】

４　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】

５　策定された基準に基づく委託先管理・監査の実施

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運用となっております。新基準での運用開始後、特段の支障なく運用が図られております。【2024年7月運用開始済】

６　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

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するPC貸与を2024年9月末までに完了しており、追加措置とした上記①・②以外の当社ネットワークにアクセス可能な委託先へのPC貸与についても、2025年3月末までに完了いたしました。PC貸与の完了に伴い、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も完了しております。なお、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はリスク低減策を講じたうえでアクセス遮断の対象外となります。
【委託先①・②へのPC貸与 2024年9月末完了、①・②以外の当社ネットワークにアクセス可能な委託先へのPC貸与 2025年3月末完了】

※ 2025年3月31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社への第三者企業を交えた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第三者企業を交えた監査・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月末完了】

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、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】

※ 2025年3月31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

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

2024年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）

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※1】
【当社からその他NAVERグループへの委託：2025年3月末完了】
【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】

※ 2025年3月31日時点の実施・検討状況です。

※1 国内子会社・海外子会社が2026年3月末まで利用継続する従業員向けシステムにおける当社からNAVER社及びNAVER Cloud社への委託業務については、2026年3月末のシステム分離に伴って終了いたします。

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3

2024年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）

（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、1年にわたって継続的な働きかけを行いました。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変更はない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。

（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。

（3）セキュリティガバナンスの確保にかかる体制構築について

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。

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、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。

※ 2025年3月31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

2024年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

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。

※ 2025年3月31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

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

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日公表）
https://www.lycorp.co.jp/ja/news/2024/20240930_1_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12月27日提出報告書（概要）（2024年12月27日公表）
https://www.lycorp.co.jp/ja/news/2024/20241227_1_appendix_ja.pdf

LINEヤフー