公表資料

個人情報保護委員会
Personal Information Protection Commission

News Release

LINE ヤフー株式会社への勧告等に対する
改善状況の概要及び同社への対応方針について

令和７年４月 30 日

個人情報保護委員会は、LINE ヤフー株式会社への勧告に対する改善策の実施状況について、以下資料のとおり、取りまとめましたので、お知らせいたします。

【連絡先】
個人情報保護委員会事務局
監視・監督室
電話：03-6457-9680（代）

令和７年４月30日　個人情報保護委員会

LINEヤフー株式会社への勧告等に対する改善状況の概要及び同社への対応方針

- LINEヤフー株式会社（以下「LY社」という。）の業務委託先企業のPCがマルウェアに感染したことが契機となり、LY社の情報システムが不正アクセスを受け、コミュニケーションアプリであるLINEに関する個人データが漏えい等した事案について、個人情報保護委員会は、LY社に対し、令和６年３月28日、個人情報の保護に関する法律（平成15年法律第57号）第148条第１項の規定により勧告を行い、同法第146条第１項の規定により、令和７年３月31日を最終として３か月ごとに改善状況を報告するよう求めていた。
- 今般、LY社から令和７年３月31日に報告のあった改善状況について確認したところ、NAVERグループ及びNAVER Cloud社（以下「NC社」という。）との認証基盤やシステムの分離については、LY社本体については概ね完了し、国内及び海外子会社においても計画どおり進んでいるほか、NAVERグループ及びNC社への委託業務の終了や縮小等も計画どおり進んでいることが認められた。また、漏えい等事案に対応するための定期演習の実施や、ペネトレーションテストや振る舞い検知のテストの結果を踏まえた是正対応等についても進展が認められた。
- 当委員会としては、今後もLY社の改善策が計画どおり進むことを注視するとともに、LY社には、全ての改善策が完了する令和８年３月末まで利用者等のステークホルダーへの丁寧な説明等を期待したい。

	事実概要	勧告等の事項	LY社の改善策	実施状況及び今後の予定	
組織的安全管理措置	【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】 ⑴　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、NC社との共通認証基盤システムや、広範なネットワーク接続を許容するネットワーク構成を利用しており、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った。	組織的安全管理措置の不備を是正するために必要な措置として、NC社との共通認証基盤システムの利用、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及び重要度の高い個人データを保管する情報システムに対するアクセス者の識別と認証の方式に関するリスクや課題を適切に把握するために、安全管理措置が徹底される組織体制を整備し、また、漏えい等事案に対応する体制の整備並びに安全管理措置の評価、見直し及び改善を行うこと。	・NC社がシステム管理を担う認証基盤の利用停止と自社認証基盤への移行 ・NAVERグループ及びNC社とのシステム分離 ・NC社を含む業務委託先に対し、実効的な業務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 ・リスクの可視化、評価の新たな仕組みの構築	完了	LY社が管理するシステムについて、認証基盤の分離を優先的に実施し、NAVERグループと認証基盤及び認証情報を共通化している状態を解消した。
				令和８年３月末完了見込み	NAVERグループ及びNC社が管理するシステムについて、LY社が利用するシステムについては、令和７年３月末に認証基盤の利用を停止し分離が完了した。国内子会社及び海外子会社については予定した計画に沿って進行中。
				令和７年６月末完了見込み	LY社が利用しているシステムで、NAVERグループ及びNC社が管理するシステムについて、一部のシステムを除き（※）、令和７年３月末にシステムの切替え及び利用停止を完了した。 （※）会計監査と税務申告に利用するデータがあるシステムについては、業務上の必要性から、会計監査・税務申告の目的に限り、令和７年６月まで必要最低限の利用を行うこととなった。
				令和８年３月末完了見込み	国内子会社及び海外子会社については、予定した計画に沿って、システムの切替え及び利用停止を進行中。
				完了	NC社に対する実地監査を行い、本件事案発生の一因となったNC社の安全管理措置の実施状況の確認並びに是正の指摘及び要求を行った。また、今後のNC社における是正状況を主導的に確認するため、NC社に対する監査権等を定めた覚書を締結した。令和６年４月末及び６月末にNC社に対する監査を完了しており、今後、年１回の頻度で定期的に監査を継続していく。
				令和７年12月末完了見込み	NAVERグループ及びNC社へ委託しているサービス企画・機能・開発委託業務について、業務委託契約等の契約名に限定せず、継続的な役務やシステム等の提供関係にある全ての契約や取組を含めて確認、対応を進め、業務委託の終了・縮小計画を策定し、委託終了目標時期を踏まえ対応を進めている。予定どおり進行中。
				完了	業務委託先の管理について、セキュリティリスク評価基準を見直し、チェックシートを新設した。また、業務委託先に関わる体制及び運用方針について、令和６年６月26日のLY社取締役会にて、委託先管理に関する基本方針を決議し、同方針に沿った内部規程を施行した。
				完了	委託する業務の内容により業務委託先を類型化し、優先的な対応を要する業務委託先について、令和６年４月から６月にかけて実地監査及び書面監査を完了した。 LY社の委託先管理に関する規程（令和６年７月１日付け施行）に基づき、適切な委託先であるかを評価するサプライヤ評価及び案件として業務委託を行うことが適切であるかを評価する案件リスク評価を開始しており、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業務委託契約の締結や案件の発注をすることはできないこととし、支障のない運用が図られている。
				完了	NC社との関係に応じたリスクに対する問題意識が担当部門内にとどまり、組織全体の問題と捉えて対応することができていなかったことが課題であるとして、従業者が普段感じているリスクの可視化、評価のために、令和６年７月に全従業者向けにセキュリティに関するアンケートを実施した。アンケート結果に基づき、課題解決の取組を継続的に推進し、取組内容や成果については、経営層と従業者との対話集会等で従業者にフィードバックしている。 令和６年11月に全従業者向けにコンプライアンスの視点から「LINEヤフーグループ行動規範に関するアンケート」を実施。結果の分析を完了し、必要な対応の検討を進めている。今後も継続的に従業者の意見を吸い上げ、経営層及び関連部門に共有し、課題解決や改善を行う。

組織的安全管理措置	【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】 ⑵　令和３年行政指導後の対応に関する問題点 　LY社は、令和３年行政指導に対し、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への多要素認証の導入は見送られており、リスクの適切な評価や安全管理措置の見直し及び評価に問題があった。	組織的安全管理措置の不備を是正するために必要な措置として、NC社との共通認証基盤システムの利用、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及び重要度の高い個人データを保管する情報システムに対するアクセス者の識別と認証の方式に関するリスクや課題を適切に把握するために、安全管理措置が徹底される組織体制を整備し、また、漏えい等事案に対応する体制の整備並びに安全管理措置の評価、見直し及び改善を行うこと。	・従業者向けシステムに対する二要素認証の適用、リスクアセスメント ・重要システムの認証プロセスに対するセキュリティ診断と発見された脆弱性の修正	完了	LY社の従業者向けシステムに二要素認証を適用した。また、従業者向けシステムに対して、認証プロセスを迂回する試みや、認証要素を悪用できる方法がないかのセキュリティ診断を実施した。 旧ヤフー株式会社のデータセンターにある一部システムについても、令和６年10月末に二要素認証の適用を完了した。
				完了	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、ISO27001を活用したリスクマネジメントプロセスの中でリスクを把握、管理する仕組みの構築を令和６年６月に完了し、同年７月１日付けで情報セキュリティ規程として定めた。また、年次のリスクアセスメントとして、各システムのデータ保管の現状やセキュリティ対策、それに伴うリスクを把握し評価する業務の仕組みを構築した。 上記を踏まえ、重要システムを特定し、令和６年10月に重要システムの安全管理措置遵守状況の確認を行い、同年12月末に安全管理措置の未遵守箇所の是正を完了した。この取組は今後も定期的に実施していく。 さらに、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、その実施計画を定めた。
	【漏えい等事案に対応する体制の整備】 　LY社は、本件事案の事実関係及び原因の究明について、NC社やNAVERグループに頼らざるを得ない状況であり、本件事案の全容を把握するために約３か月半を要したことから、漏えい等事案に対応する体制の整備に問題があった。		・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	完了	漏えい等事案発生時のNC社との窓口を明確化した。また、LY社のログ保管期間ルールに従い、NAVERグループのシステムのログを１年間保管することとし、必要に応じてNC社から受領できるように覚書を締結した。
				完了	漏えい等事案発生時の調査範囲の判断プロセスについて改善点を洗い出し、必要なマニュアル及びルールの改善計画を立案し、外部機関の評価を得た上で確定した。漏えい等事案発生時の対応に関する以下の項目について、令和６年10月に対応を完了した。 ・初期行動フローの整備 ・速やかなシステム構成全体像の把握及び調査範囲判断プロセスの整備 ・ステークホルダーとの役割と責任の整備 また、上記の実行性を担保するため、令和６年12月から定期演習を開始しており、令和７年３月までに複数回実施した。また、令和７年４月以降も継続的に実施予定。
				完了	業務委託先に対して、LY社が管理するPCの貸与を完了した。さらに、追加措置として、PC貸与の対象を拡大させ、LY社の業務委託先か否かに関わらず、業務上、LY社のネットワークにアクセスすることが可能な関係先に対しては、LY社が管理するPCを貸与することとし、配付を完了した。 漏えい等事案発生の際には速やかにPCを回収し、フォレンジック調査を行う。
	【組織体制の整備】 　LY社においては、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、その組織体制が十分に機能していたとは言い難い。		・セキュリティガバナンス委員会の設置 ・LY社のグループ全般のセキュリティガバナンスについて抜本的見直しや高度化を行うため、主要グループ会社のCISO（Chief Information Security Officer：最高情報セキュリティ責任者）で構成する「グループCISO Board」を設置	完了	CISOを責任者として、個人データの取扱いレベルと安全管理措置を定義して、セキュリティ規程に定めるとともに、各部門にセキュリティ責任者を任命し、個人データが適切に取り扱われているかについてリスクアセスメントを実施している。また、令和６年４月、規程遵守状況をモニタリングするための監査部門を設置した。
				完了	令和６年４月、LY社社長CEOが委員長を務めるセキュリティガバナンス委員会を組成し、本件に関連する対応の一層の推進及びLY社の課題全般についての議論を継続している。令和７年１月から３月26日までに、「各改善策に係る方針議論、進捗確認、個別課題の確認」等を議題として、計29回の委員会を開催している。
				完了	令和６年４月、LY社CISO、LY社の主要なグループ会社CISO及びオブザーバーとしてのソフトバンク株式会社CISOで構成される「グループCISO Board」を設置し、LY社グループ内におけるセキュリティの統一ルールの策定と遵守の徹底や、それらを前提としたLY社グループ会社間での委託関係の整理等の議論と推進を行っている。令和７年１月から３月28日までに、「LY社が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」等を議題として、計５回の会議を開催し、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を行っている。

技術的安全管理措置	【アクセス制御】 LY社は、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から、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。	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適切なアクセス制御を行うこと。	・NC社との不必要な通信の遮断 ・社外とLY社データセンター間の接続経路の総点検	令和８年３月末完了見込み	NC社データセンターからLY社データセンターへのインバウンド通信について、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った。 NC社のインフラを利用しているLY社サービスの本番環境用のサーバとLY社データセンター内のサーバ間の通信について、関連するサーバの利用停止に伴い、全てのインバウンド通信を遮断した。 NAVERグループ及びNC社とのシステム分離や、NAVERグループ及びNC社への業務委託の終了に伴い、不要となったインバウンド通信を遮断した。 今後も、システム分離等に伴い不要となったインバウンド通信は順次遮断するとともに、３か月毎にファイアウォールポリシー設定のメンテナンスを継続する。
				完了	NC社以外でも、社外からLY社データセンターに専用線やVPN等を介して接続している経路（インバウンド及びアウトバウンド双方向の通信）に対して、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令和６年８月末に完了した。総点検の結果、ネットワークアクセス制御の適切性について、是正対象とした通信許可設定の修正及び削除を行い、インシデント対応の準備状況について、問題がないことを確認した（令和６年９月末是正完了）。
				完了	LY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、上記の接続経路の総点検の結果を踏まえ立案した計画に従って、令和６年10月末にファイアウォールポリシーの適用を完了し、同年12月末に不必要な通信の点検を実施した。点検結果を踏まえ、是正対象となったファイアウォールポリシーの修正・削除を令和７年２月に完了した。 また、NAVERグループ及びNC社とのシステム分離や業務委託の終了に伴い、不要となったアウトバウンド通信の遮断を令和７年３月末に完了した。 今後も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する。
		当委員会からの勧告等の事項に対するものではないが、改善策の実効性を担保する観点から、LY社において右記の改善策を実施する予定。	・サイバーセキュリティ対策及びセキュリティ監視に係る効果検証と抜本改善、強化	完了	実際にLY社のシステムがどのように攻撃され得るかを実証的に把握、評価することを目的として、ペネトレーションテストを実施し、段階的なサイバー攻撃を想定した脅威シナリオに対して効果的に分断できている仕組みや、これまで実施した再発防止策の効果及び本番環境の堅牢性について評価を得た。一方で、多層防御の観点から複数の発見事項が提示されたため、それらに対する是正計画を立案し、その計画に則った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令和７年３月末に完了した。今後も改善状況の定期的なモニタリングを実施する。 また、LY社の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について、疑似攻撃を行い、有効性をテストした。テストの結果を踏まえ、令和７年２月に全ての検知ルールをSIEM環境(※)に実装した。今後も継続的に検知ルールの見直しを実施する。 (※)SIEM：Security Information and Event Management。ネットワーク製品やセキュリティ製品を含むあらゆるIT機器から集積されたログを一元管理し、相関分析を行った上で、インシデントにつながる脅威を早期に検知する仕組み。

※令和７年１月29日付け公表資料から進展があったものは赤字で記載し、下線を引いている。