令和６年●月●日　個人情報保護委員会

公表資料　資料３

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、定期的に改善状況を報告するよう求めていた。
- 令和６年６月28日、LY社から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。）とのシステム分離の前倒しや、NAVERグループ及びNC社へ委託している業務の終了・縮小計画の策定等について、進展が認められた。また、その他の改善策についても、対応が進んでいるものと評価できる。
- 実施状況が未了の改善策については、令和６年９月30日を期限として実施状況の報告を求めており、当委員会としては、引き続き、改善策の実施状況について注視していく。

	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。	－
				未了	NAVERグループ及びNC社が管理するシステムについて、認証基盤の分離を実施する。LY社の海外子会社については、システム及び認証基盤の移行の方法が明確化されたことで、先行して対応することとしていた国内子会社の移行と並行して作業を進めていくことが可能となったため、予定していた完了時期を令和８年12月から同年３月末に前倒しした。	LY社：令和７年３月末 国内子会社：令和８年３月末 海外子会社：令和８年３月末
				未了	LY社及びLY社子会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、その利用停止や別システムへの移行等を実施し、NAVERグループとシステムを分離する。LY社の海外子会社については、上記と同様の理由により、完了時期を令和８年３月末に前倒しして対応する。	LY社：令和７年３月末 国内子会社：令和８年３月末 海外子会社：令和８年３月末
				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。	（継続的な取組を予定している。）
				未了	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・縮小計画の策定が完了した。今後、策定した委託終了目標時期を踏まえ、順次対応を進める。	令和７年12月末
				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。	－
				未了	取引先及び業務委託先に対してセキュリティ面、信用面等の多角的なリスク評価を実施する社内ルールを策定し、定期的な監査を実施する。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～６月にかけて実地監査及び書面監査を完了した。未実施の業務委託先について、引き続き監査を実施していく。	順次監査実施予定
				未了	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、全従業者向けアンケートを実施する。	令和６年７月及び11月実施予定、順次改善取組を実施

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	未了	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は二要素認証の適用を令和６年12月までに完了するとしていたが、令和６年10月までを目標に、前倒しして対応する。	令和６年10月完了予定
				未了	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、①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、②安全管理措置未遵守箇所のリスクアセスメント、③時流等に応じた安全管理措置の見直し計画の策定を行う。 なお、上記①～③については、CISO（Chief Information Security Officer：最高情報セキュリティ責任者）及びセキュリティガバナンス委員会への報告や承認のプロセスを伴う。	①令和６年10月 ②令和６年12月末 ③令和６年12月末
	【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。	－
				未了	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整備を行い、外部機関の評価を得た上で確定した。また、その実行性を担保するために、演習の定期実施を行う。	令和６年下期に演習実施予定
				未了	業務委託先へは、原則LY社が管理するPCを貸与し、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。	令和６年９月貸与PC配布完了予定
	【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。	（継続的な取組を予定している。）
				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６年４月～６月21日までに計43回の委員会を開催している。	（継続的な取組を予定している。）
				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６年４月～６月21日までに計５回の会議を開催している。	（継続的な取組を予定している。）

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	完了	NC社データセンターからLY社データセンターへのネットワークアクセスについて、ファイアー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。 今後、システム分離や委託業務の終了に伴い、不必要となった通信は順次遮断するとともに、３か月毎にファイアーウォール設定のメンテナンスを継続する。	（継続的な取組を予定している。）
				未了	NC社以外で、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点検を実施する。	令和６年７月末完了予定
		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	未了	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、結果を踏まえ、是正計画を策定する。 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、既知の攻撃に加え、ゼロデイ攻撃等の未知の脅威に対する耐性や有効性等を、外部機関を交えて分析、検証し、結果を踏まえ、是正計画を策定する。	令和６年８月末是正計画策定完了予定

※令和６年５月22日付け公表資料から進展があったものや、追加したものは赤字で記載し、下線を引いている。