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６年５月 22 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）

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

令和６年５月22日　個人情報保護委員会

- 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、改善状況を報告するよう求めていた。
- 令和６年４月26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、現時点において、LY社の従業者向けシステムへの二要素認証の適用や、NAVER Cloud社（以下「NC社」という。）のデータセンターとLY社のデータセンター間のファイアーウォールの設置等について一定の改善が認められた。
- しかしながら、現時点で、計画策定中や未了の取組も多く、LY社においても一部の取組について完了時期の前倒し、早期実施を検討しているが、引き続き、改善策の早期実施、完了等を求めるとともに、実施状況が未了の改善策については、令和６年６月28日を期限として実施状況の報告を求めている。

	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】 (1)　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	未了	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する。	令和６年６月完了予定
				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：令和７年３月末(※) LY社の国内子会社：令和８年３月末(※) LY社の海外子会社：令和８年12月(※)
				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：令和７年３月末(※) LY社の国内子会社：令和８年３月末(※) LY社の海外子会社：令和８年12月(※)
				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。	－
				未了	NAVERグループ及びNC社へ委託している業務について、業務委託の終了又は縮小を進める。	令和６年６月までに計画策定、順次実施予定(※)
				完了	個人データの取扱いの委託を行わない業務委託先の管理において、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。	－
				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。	令和６年３月社内ルール策定完了、順次監査実施予定

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】 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令和６年12月までに二要素認証の適用を完了する。	令和６年12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・管理する仕組みを構築する。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するとともに、規程として定める。さらに、これらを確実に実施するため、CISO（Chief Information Security Officer：最高情報セキュリティ責任者）直下にセキュリティ監査部門を設け、リスク対策の定期的なレビュー・評価の仕組みを構築する。	令和６年６月末完了、順次運用予定
	【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する。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５月計画立案、同年６月外部評価完了、順次実施予定
				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	未了	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月から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。	
				未了	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。	
				未了	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。	
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。	－
				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月完了予定

（※）LY社にて完了時期の前倒し、早期実施を検討している。