（公印・契印省略）

総基用第４６号

令和６年３月５日

LINEヤフー株式会社

代表取締役社長 CEO　出澤　剛　殿

総務省総合通信基盤局長

今川　拓郎

総務省サイバーセキュリティ統括官

山内　智生

通信の秘密の保護及びサイバーセキュリティの確保の徹底について（指導）

１．事案の概要

本事案の不正アクセスに係る具体的な経路は、貴社が他社にセキュリティ管理を委ねていた事情もあり、現時点では厳密に特定することが困難となっているが、貴社から提出のあった令和５年11月28日付け報告書並びに報告徴収に対する令和６年１月30日付け及び同年２月６日付けの各報告書等によれば、これまでに判明している事案内容は次のとおりである。

貴社のITインフラの運用に係る業務委託先であるNAVER Cloud社[1]及び貴社が、それぞれセキュリティに係るメンテナンス業務を委託していた会社（以下単に「業務委託先会社」という。）においてマルウェア感染が生じたことを契機として、NAVER Cloud社のADサーバ[2]がマルウェアに感染し、同社の管理者権限が奪取されるとともに、同社のADサーバに保存されていた貴社のADサーバへのアクセスに係る認証情報等が悪用され、NAVER Cloud社とネットワーク接続のあった貴社の旧LINE株式会社（以下「旧LINE社」という。）環境内の各種サーバやシステ

[1] NAVER Cloud社はNAVER社の100%子会社である。NAVER社及び同社配下のグループ企業により、貴社の持株会社であるAホールディングス社の株式の半数が保有されている。以下NAVER社とNAVER Cloud社を併せて「NAVER社側」ということがある。

[2] Active Directoryサーバ。Active Directoryとは、組織内のコンピュータやユーザを集中的に管理するためにMicrosoft社が提供しているディレクトリ管理サービスである。

ムに対して不正アクセスが行われ、これにより、旧LINE社環境内に保存されていた、貴社の提供する「LINE」サービスに係る利用者の通信情報が外部に流出等した[3]とのことである。

これは、電気通信事業法（昭和59年法律第86号）第４条第１項に規定する通信の秘密の漏えいであると認められる。

２．事案発生の要因

（１）システムやネットワーク構成等に係るNAVER社側への強い依存

そもそも旧LINE社の前身企業（NHN Japan社）がNAVER社の子会社であった当時から、貴社の旧LINE社環境においてはNAVER Cloud社のプラットフォームが利用されてきた経緯もあって、本事案発生当時、貴社の旧LINE社環境とNAVER Cloud社環境との間にはネットワーク接続があり、貴社からNAVER Cloud社に対して旧LINE社環境への広範なネットワークアクセスが許容されていた。法的な契約上は、貴社は、NAVER Cloud社に対して、物理的なサーバ及びソフトウェアなどのインフラの構築や運営業務を委託しており、その委託業務を行わせるために、旧LINE社環境への広範なアクセスを許容していたとのことである[4]。

また、このようなネットワーク接続がある背景として、上記の経緯もあり、貴社とNAVER社側との間では従業員アカウントの認証基盤についても共通化されており、旧LINE社従業員のIDやパスワード等の情報がNAVER Cloud社側の従業員管理システムにて管理・保存されていた状態であった（認証機能に付随して該当の従業員の氏名、社員番号及び所属等についても認証連携したシステムから参照可能であった。）。これにとどまらず、これまでの貴社からの報告によると、NAVER Cloud社のADサーバ内に、NAVER Cloud社内に設置されている旧LINE社サーバの開発・保守のために発行された旧LINE社従業員のアカウント情報が保存されていたこと、同一ドメインによって認証基盤が共通化されていた範囲内だけでなく、旧LINE社従業員のアカウント情報につい

[3] ファイルのダウンロード等の痕跡が確認されたものに限らず、該当のサーバ等に対して不正アクセスがなされた痕跡があるものも含む。

[4] この点に関し、これまでの貴社からの報告によれば、NAVER社の日本向けサービス提供用のネットワーク機器が貴社のデータセンター内に設置されており、同機器についてNAVER Cloud社から貴社のネットワークを介してアクセスがなされ、その保守管理が実施されていた事実も確認されている。

ては、旧LINE社の人事システムによって結びついたサーバ間で同じ情報が同期される仕様となっていた。

このように、貴社からNAVER社側に対して、旧LINE社環境に係るシステムやネットワーク構成、旧LINE社従業員のアカウント情報の取扱いについて、相当に強い依存関係が存在していたものと認められる。

本事案は、そうした貴社と密接な技術的・資本的な関係があるNAVER Cloud社、及び業務委託先会社の情報セキュリティに係る安全管理措置に不備があったことを起点として、攻撃者にNAVER Cloud社のADサーバ等へ不正に侵入された上、NAVER Cloud社のネットワークを介して、貴社に対して不正アクセスがなされ、貴社のサービスに係る利用者の通信情報が漏えいしたものである。

（２）不十分な技術的安全管理措置

本事案に係る不正アクセス及び情報漏えいに至った貴社側の主な原因としては、貴社は、NAVER Cloud社に対して、従業員アカウントの認証情報を共通基盤や情報の同期を認めるシステム構成によって共有するなどしており、そのために貴社のネットワーク及び社内システム等への広範なアクセスを許容していたところ、これらの経路や認証情報等が悪用された場合には、貴社のサーバやシステムが侵害されるリスクが高かったにもかかわらず、貴社のサーバ、ネットワーク及び社内システムを保護するために十分な技術的安全管理措置ないしサイバーセキュリティ対策を行っておらず、貴社内のADサーバを含む数々のサーバやシステムに対して不正アクセスを許した点が挙げられる。具体的には、NAVER Cloud社から貴社のネットワークに対して特定のポートに係る通信を除いて広くアクセスが許容されており、厳格なアクセス制御がなされていなかったこと、重要な社内システムへのログインに当たって多要素認証等が求められていなかったこと、不正を検知するための適切な仕組みも導入されていなかったこと等、様々な技術的不備が存在した。

（３）業務委託先の不適切な管理監督

これに加え、貴社のサーバやシステムの侵害に至る端緒として、NAVER Cloud社や業務委託先会社の安全管理措置ないしサイバーセキュリティ対策にも不備があり、外部からのマルウェア感染を許した上、ADサーバへの侵入

や管理者権限の奪取等を許した結果、貴社のネットワークへの不正アクセスにつながったものであるが、このような事態を防ぐための安全管理措置ないしサイバーセキュリティ対策をNAVER Cloud社や業務委託先会社は十分に実施しておらず、また、貴社との業務委託契約上も、定期的な評価や基準遵守に関する定めが存在していないなど、適切な業務委託先の管理監督が実施されていなかったことも認められる。

（４）セキュリティガバナンスの不備

以上に述べた貴社自身の安全管理措置ないしサイバーセキュリティ対策が不十分であったことや、業務委託先の不適切な管理がなされ、委託先を通じたサイバー攻撃に対する適切な安全管理措置ないしサイバーセキュリティ対策が取られていなかったことの背景には、まず、組織的・技術的な問題として、これまでの旧LINE社における社内ネットワークやシステム構築がNAVER社側による技術的支援を大きく受けて複雑に形成され、現在でも、その保守運用等をNAVER社側に頼らざるを得ないという関係が存在している。また、貴社からみるとNAVER社側は委託先として委託元である貴社から管理監督を受ける立場であるにもかかわらず、現在でも、貴社の親会社であるＡホールディングス社資本の半数をNAVERグループが保持しているなど、貴社とNAVER社側との間には資本的な支配を相当程度受ける関係が存在している[5]。こうした関係が存在するため、貴社側からNAVER社側に対して安全管理のための的確な措置を求めることや、適切な委託先管理を実施することが困難であったという事情も影響しているものと考えられる。

３．注意事項

貴社の前身企業であり、本事案により不正アクセスを受けた各種サーバやシステム等を有する旧LINE社に対しては、当省から令和３年４月26日付けで社内システムに関する安全管理措置の一環としてアクセス管理の徹底等も含めて行政指導を行っていたにもかかわらず、なおもアクセス管理の不備を一因とする本事案を招いたものである。加えて、貴社が提供する「LINE」サービスが我が国

[5] LINEヤフー社とNAVER社側との間に認められる、組織的・技術的にNAVER社側に頼らざるを得ない関係と、資本的な観点から支配を相当程度受ける関係を総称して、「組織的・資本的な相当の支配関係」と呼ぶことがある。

の国民の大多数が日常的に利用しているサービスであることにも鑑みれば、本事案の発生によって、貴社の提供する電気通信役務、ひいては電気通信事業全体に対する利用者の信頼を大きく損なう結果となったものであり、当省として極めて遺憾である。

貴社に対しては、今後、電気通信事業法の趣旨を踏まえ、通信の秘密の保護及び電気通信事業に係るサイバーセキュリティの確保が徹底されるよう、組織的・人的・技術的な各側面から安全管理措置や委託先管理の在り方等について抜本的な見直しを行った上で、必要とされる具体的な措置を講ずるとともに、親会社等[6]を含むグループ企業全体でのセキュリティガバナンスの在り方についても根本的な見直しを行い、その強化を図ることにより再発防止に努めるよう、厳重に注意する。

４．指導事項

以上を踏まえて、下記の（１）ないし（３）の事項について、必要な措置を実施されたい。ついては、その取組方針及び実施状況について、令和６年４月１日までに報告するとともに、今後、このような事案が再発しないよう、同報告から少なくとも１年間は、四半期に一度、今後の取組状況について定期的に報告されたい。なお、今後新たな懸念が生じた場合等には、追加的な措置を求める可能性がある旨御承知おき願いたい。

記

（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の強化について

２．で述べた貴社とNAVER社側との密接なネットワーク構成やそれに基づく貴社の情報の取扱い等を前提とすれば、NAVER社側に何らかのセキュリティインシデントが発生した場合、NAVER社側のネットワークを介して旧LINE環境下に保存された情報へ容易にアクセスすることが可能であり、NAVER社側のネットワークを通じて旧LINE社が取り扱う利用者の情報が侵害されるリスクが常態化していたというべきであるが、貴社からの報告によれば、それにもかかわらず、貴社において十分な安全管理措置はとられず、貴社からNAVER社側に対

[6] 以下「親会社等」とは、LINEヤフー社の親会社や親会社の議決権の半数以上を保有する企業グループをいう（会社法上の「親会社」、「親会社等」とは必ずしも同義ではない。）。具体的には、Aホールディングス社、NAVERグループ、ソフトバンクグループが該当する。

しても、これまで定期的な安全管理措置の実施状況の確認やセキュリティリスクの評価等はなされていなかったというのであって、本事案は正にこのようなリスクが顕在化した事案であるというべきである。

また、本事案の解明に際して、当省からも貴社に対して複数回にわたって報告を求めるなどしたが、貴社からは調査未了を理由として回答期限内に十分な回答がなされなかったり、回答がなされてもその内容に不明瞭な点が多々含まれたりするなどしていた。これは貴社が情報セキュリティに係る安全管理をNAVER社側に強く依存していたため、アクセスログ等の必要な情報の多くがNAVER社側に存在しており、その収集や分析に支障を来したからであると推察される。このように、サイバーセキュリティ事案において、自社として、委託先の監督や原因特定を速やかにできないこと自体、大きな問題であると言わざるを得ない。

ついては、貴社の安全管理措置やサイバーセキュリティ対策、業務委託先管理の在り方について、本事案と同様のインシデントの再発を確実に防止するよう、以下のとおり抜本的な見直しを行い、実効的かつ十分な対策を講じられたい。

① NAVER Cloud社とのネットワーク分離による安全管理措置の見直しについて

ア 貴社の旧LINE社環境とNAVER Cloud社との間にネットワーク接続があり、NAVER Cloud社に対して旧LINE社環境のネットワーク及び社内システムへの広範なアクセスが許容されていたことにより、NAVER Cloud社のシステム・端末への侵入によって貴社のサーバやシステムにまで到達可能であったことが本事案発生の原因となったことを踏まえ、NAVER社側のシステムや端末から貴社のネットワークや社内システムに関して真に必要最小限度のアクセスのみを許容し、その他のアクセスを認めない仕組みを、ファイアーウォールの設置、不要ポートの閉鎖、プライベート通信の排除等を含めて構築するとともに、これに加えて、貴社のサーバ、ネットワークや社内システムの保護の万全を図るための方策を検討し、具体的な措置を講ずること。

イ 本事案発生当時、貴社とNAVER社側との間では従業員アカウントの認証基盤が共通化され、旧LINE社従業員のアカウント情報がNAVER Cloud

社側の従業員管理システムにて管理、保存されていた状態であったと認められ、貴社からの報告によれば、このように従業員アカウントの認証基盤を共通化していたことが情報漏えい被害の拡大に寄与したとのことである。また、貴社のADサーバに保存されていた従業員のアカウント情報について、貴社の人事システムを介して貴社内の各種サーバやドメインが異なるNAVER Cloud社のADサーバ等とも、必要な範囲で情報が同期される仕様となっていたとのことである。十分な安全管理措置が施されていたとは認められない状況のもと、従業員のアカウント情報が他者であるNAVER Cloud社に対しても共有され、同社のサーバ内に保存されていたことは、貴社としての極めて重大なセキュリティリスクであったと認められる。

以上を踏まえ、共通化している認証基盤（従業員アカウントの認証基盤に限らない。）や情報の同期を認めるシステム構成のセキュリティリスクについて貴社において改めて評価を行った上で、確実な再発防止を実現する観点から、NAVER Cloud社の認証基盤等と貴社の認証基盤等とを速やかに技術面及び運用面で完全に分離するため、貴社が管理する認証基盤等への移転や分離後の管理の在り方等を含めて計画を策定するとともに、これを着実に実施することにより具体的な対策を講ずること。

特に、移行計画の概要については、報告徴収に対する令和６年１月30日付け報告書等の中でも言及があるが、具体的なシステムの内容ごとに詳細な計画を策定し、その移行が完了するまで、定期的にその実施状況を報告すること。なお、完全に分離が行われる前も、認証基盤等に対するNAVER社側からの接続が必要最小限の範囲に留まるよう適切に管理されているかについて、状況を報告すること。また、運用面では、貴社の従業員のアカウント情報は貴社内で管理することとし、本事案発生当時になされていたNAVER社側への同期は中止すること。

ウ　貴社からの報告によれば、旧LINE社環境のサイバーセキュリティ対策に関連して、SoCのTier１に係る業務をNAVER Cloud社に委託しているとのことであるところ、本事案の発生を踏まえ、貴社として、国内において、独立した形で認証情報を管理、運用するとともに、セキュリティ確保のために必要とされる各システム等のログ情報を自ら取得し、これら情報を集約した上で独立した形でSoC業務を行うことができる体制を早期に整えること。今後、セキュリティインシデントが発生した場合には、

自社の中に保有されている証跡に基づき、事象の詳細を把握し、原因究明やそれに対応した再発防止策を自ら策定することができる体制を整えること。その際、APTは既知の脆弱性だけではなく、ゼロデイ等を用いた攻撃を行うことも想定されることを踏まえ、ふるまい検知等を含め、最新の対策手法を取り入れた体制を検討すること。

② 貴社内において取るべき安全管理措置の見直しについて

本事案では、貴社内のADサーバを含む、各種の重要サーバやシステムに対して不正アクセスがなされ、重大な情報漏えい被害が生じたものである。AD管理についてはその重要性に鑑みて厳重なふるまい検知の仕組み等の対策が取られてしかるべきであったにもかかわらず、これが行われておらず、セキュリティ監視レベルが不十分であったため、不正なアクセスを検知等できなかった。また、その他の重要サーバ等についても認証方式がIDとパスワードの組合せであるなどそのアクセス管理のレベルが不十分であった点があり、不正に取得された従業員アカウント等を用いたアクセスを防ぐことができなかった。これらを踏まえ、自社内のサーバ等の保護に向けて、高度な侵入検知システムの導入や多要素認証の導入を含めたアクセス管理の強化等を含む、実効的なサイバーセキュリティ対策の導入に向けた計画を策定し、その内容を報告するとともに、速やかに具体的な措置を講ずること。

③ 委託先管理の見直しについて

ア 本事案において、NAVER Cloud社等の業務委託先の安全管理措置に係る貴社からの管理監督が不十分であったことを踏まえ、通信の秘密に該当する情報の取扱い等を委託する場合（通信の秘密に該当する情報の取扱いを委託する場合及びこのような情報へのアクセスを許容する場合やアクセスが可能となる場合を含む。）における業務委託先管理の在り方について、セキュリティリスクの評価基準の見直しを行った上で、リスクに応じた実効的な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並びにその実施を行うこと。

特に、本事案の内容に鑑みれば、情報の取扱いの委託の有無にかかわらず、重要な設備等に関する業務委託について、その委託先及び再委託

先について特定した上で、安全管理措置ないしサイバーセキュリティ対策について適切な管理監督ができるように、令和６年３月末までに安全管理措置等の基準を策定し、実効性を高めたモニタリング・監督方法を検討・策定すること。あわせて、委託先の監督が委託先による分析結果や委託先から受領するログに依存しており、委託先からこれらが得られないと自社として侵害の有無や範囲も十分に把握できないという状況を見直すこと。

イ　本事案における攻撃の端緒となったNAVER Cloud社における安全管理措置の強化について、委託元としてNAVER社側に対して適時に実施状況を確認するとともに、必要に応じて対策の強化を要請するなどし、実効的な再発防止策が策定されるよう、適切な管理監督を行うこと。

特に、貴社からの報告によれば、NAVER Cloud社は、貴社から指摘するまで侵害に気付かず、そのADサーバが侵害され、外部のC&Cサーバから直接接続された状況が相当期間にわたって継続していた等、その安全管理措置に問題があったとのことである。このことを踏まえ、委託や監督の在り方を見直すための、貴社としての計画を策定して提出すること。

（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及び強化について

（１）でも述べたネットワーク構成上の重大なリスクが存在していたにもかかわらず、これが是正されずに本事案の発生に至った背景には、貴社からみるとNAVER社側が委託先として委託元である貴社から管理監督を受ける立場であるにもかかわらず、NAVER社側と貴社の間で組織的・資本的な相当の支配関係が存在することもあり、貴社からNAVER社側に対して安全管理のための的確な措置を求めることや適切な委託先管理を実施することが困難であったという事情も影響しているものと考えられる。

本事案を受けて、貴社からの報告によれば、貴社ネットワークへのアクセスのホワイトリスト化やファイアーウォールの設置等を通じてNAVER社側と旧LINE社環境との間のネットワーク管理を強化し、共通化していた従業員アカウント認証基盤やNAVER社側と連携していた従業員向けシステムについても分離や切替えを進めることで、一定程度、NAVER社側との繋がりを解消する予

定であるとのことである。しかしながら、本事案の発生に直接寄与したシステムを含む複数の重要システムについて、現時点の計画では、その構成の複雑性から分離に相当の期間を要する見込みであること、上記の貴社からの報告に基づく取組が実施された後においても、一部のシステムの開発・運用・保守業務については依然としてNAVER社側への委託が予定されているとみられること、また、本事案の影響範囲に含まれない、エンドユーザ向けサービスの本番環境（エンドユーザ向けサービスが実際に稼働する環境）その他のシステムについてNAVER社側への委託の見直しがなされるのか明確でないこと等からすると、委託先管理の困難性は十分解消されておらず、本事案と同様のインシデントを招来するリスクが解消されているとは認められない。

（１）において実施を求めた貴社における安全管理措置ないしサイバーセキュリティ対策等を実効性のあるものとし、本事案と同様のインシデントの再発を確実に防止するためには、単に一部のシステムやネットワークの技術的な分離措置等を講ずるのみでは不十分というべきであって、セキュリティリスクを的確に把握し、リスクを踏まえた実効的な対策を実現できるガバナンス体制を、親会社等を含むグループ全体で構築することが必要である。

上記を踏まえ、実効的なセキュリティガバナンスの確保に向け、貴社内におけるセキュリティガバナンス体制の抜本的な見直しや是正策の検討を行うことに加え、貴社の親会社等も含めたグループ内において、委託先への適切な管理・監督を機能させるための貴社の経営体制の見直し（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む。）や、適正な意思決定プロセスの構築等に向けた、適切な検討がなされるよう、親会社等に対しても必要な働き掛けを行うこと。

（３）　利用者対応の徹底について

本事案において、少なくとも、貴社の利用者の通信の秘密に該当する情報が２万件以上（推計値を含む。）漏えいしたことを踏まえ、利用者保護の観点から、今後も利用者に対する本事案に関する適切な情報提供を継続するとともに、二次被害が発覚した場合等には適切な支援、対応を実施すること。

（以上）