別紙

（公印・契印省略）

総 基 二 第 61号
令和３年４月26日

LINE株式会社
代表取締役社長　出澤　剛　殿

総務省総合通信基盤局長
竹　内　芳　明
総務省サイバーセキュリティ統括官
田　原　康　生

社内システムに関する安全管理措置等及び利用者への適切な説明について（指導）

令和３年３月19日付けで発出した報告徴収に対して、同年４月19日付けで貴社より、事案の経緯や詳細、個人情報及び通信の秘密の保護等のために必要な体制の確保及びセキュリティ対策、利用者への周知や対応策等について報告書の提出があった。

今回の報告徴収は、同年３月17日に貴社が公表した事案について行われたもので、貴社の再委託先企業であるLINE China（Shanghai LINE Digital Technology Limited. Dalian Branch）の従業員による、社内システムの１つであるモニタリング支援システム（LMP：LINE Monitoring Platform）に対するアクセスのうち、特に通信の秘密又は個人情報に該当する可能性のある情報を含みうるLINEメッセンジャーに係るもの及び捜査機関対応業務従事者用システムに対するアクセスに関するものであり、貴社からの報告に基づく限りにおいては、通信の秘密の侵害又は個人情報の漏えい等があった旨は確認できなかった。

一方で、貴社の社内システムに関する安全管理措置等や利用者に対する説明に関して一部不十分なところがあったと認められること、また、貴社が提供する電気通信役務の利用者は約8,600万人に上っており、多くの利用者が多様な用途で利用していることに鑑みれば、今後とも利用者が安心して貴社が提供する電気通信役務を利用することができるよう、個人情報や通信の秘密の保護等に係る支障の発生の防止に万全を期すために必要な措置を講じることにより、貴社の電気通信事業に対する信頼を確保し、もって電気通信役務の円滑な提供の確保と利用者の利益の保護を図ることが求められる。

以上を踏まえて、下記の各事項のとおり実施されたい。また、下記の各事項を踏まえて講じた措置の状況について、令和３年５月31日までに報告されたい。なお、今後新たな懸念が生じた場合等には、追加的な報告及び調査や措置の実施を求める可能性がある旨を御承知おき願いたい。

記

1　社内システムに関する安全管理措置等に関する事項

（１）社内システムへのアクセス管理の徹底

社内システムへのアクセスを通じた利用者の個人情報や通信の秘密に該当する情報の漏えいが生じることのないよう、その万全を図るため、次のとおり、社内システムへのアクセス管理の強化徹底を図ること。

①　今回の報告において、LMPへのアクセス権限に関して、一部に適切なプロセスを経て付与されたものか否かが確認できないケースがあったと認められることを踏まえ、社内システムへのアクセス（外部向けサービスのためのシステムへの内部からのアクセスを含む。以下同じ。）の権限が、真に適切な者に対して、適切な範囲で付与されるプロセスになっているかについて、全般的に点検を行うとともに、その結果を踏まえて、必要に応じ、適切なプロセスを通じたアクセス権限の付与を確保するための措置を講じること。

②　今回の報告において、LMPへのアクセスのための通信について、不正の検知やログインしようとする者の認証の仕組みが、不正行為の防止や本人性の確認のための対策として必ずしも十分に厳格であるとはいえない部分があると認められることから、これらの対策について点検を行うとともに、その結果を踏まえて、必要に応じ、例えば、社内システムに対する不正・不審なアクセスの監視や監査、社内システムにアクセスする者の認証の強化等、内部からの不正・不審なアクセスやなりすましの防止に万全を図るための方策を検討し、具体的な措置を講じること。

（２）開発プロセス及び開発組織のガバナンスの強化

今回の報告において、内部向けシステムであるLMPの開発プロセスにおいて、権限管理やセキュリティチェックが適切に実施されていないケースがあったと認められることを踏まえ、LMPに限らずシステム開発全般について、適切な開発プロセスの下で実施されるよう確保することにより、利用者の個人情報及び通信の秘密に該当する情報の漏えいが生じることのないよう、その万全を図る観点から、次のとおり、開発プロセス及び開発組織のガバナンスの在り方を見直し、その強化を図ること。

①　内部向けシステムの開発プロセスについて、原則として電気通信役務の提供等の外部向けサービスのためのシステムに係る開発プロセスと同様の開発プロセスによることとするとともに、開発プロセス全般について再点検を行うこと。

②　適切な開発プロセスによる開発の実施や開発者に対するアクセス権限の適

切な付与、また、不適切なケースがあった場合の迅速な対応を図るため、開発組織のガバナンスの在り方の見直しを含めた検討を行い、その着実な確保を図ること。

（３）社内システムに関するリスク評価等を通じた透明性・アカウンタビリティの向上

社内システムからの利用者の個人情報及び通信の秘密に該当する情報の漏えいの防止に万全を期す上でリスク評価が十分ではなかったと認められることを踏まえ、次のとおり、社内システムに関するリスク評価等を行い、これらの情報の適切な取扱いに係る透明性・アカウンタビリティの向上を図ることにより、利用者からの信頼の確保に努めること。

① 上記（１）及び（２）を含め、外国の法的環境による影響等にも留意しつつ、委託先を含めた社内システムの開発・運用に当たっての情報の取扱いに係るリスク評価を実施し、必要に応じ所要の措置を講じること。また、これらの措置を講じた場合には、当該措置を適切に反映した内容になるようポリシーを見直すこと。なお、例外的なプロセスを適用する場合には、適用の範囲及びその判断の手続についても当該ポリシーにおいて明確にすること。

② 貴社においては、データセキュリティのガバナンス強化と情報保護の強化の観点から「米国NISTが定めた世界トップレベルのセキュリティ基準への準拠」を図ることとしていると承知しているところ、今後貴社において必要な体制の構築等を図ることにより、同基準への準拠に向けた取組の強化を図るなど、透明性・アカウンタビリティの向上に努めること。

２ 利用者への適切な説明に関する事項

トーク履歴等の通報機能使用に際して、利用者に示される文言が想定していたものと異なっていたケースがあったことを踏まえ、通信の秘密に関する情報の適切な取扱いを確保する観点から、トーク履歴の通報を行った際に、貴社に提供される情報の範囲、提供された情報の利用目的について利用者が分かりやすく理解できるようにするための措置を講じること。また、貴社に提供された情報が当該利用目的の範囲内で適切に取り扱われることを確保するための措置を講じること。

以上