資料　31－2

電気通信事業ガバナンス検討会について

2021年5月

サイバーセキュリティタスクフォース事務局

LINE株式会社における情報管理の状況

- LINE株式会社が提供するLINEサービスに関するシステム**開発や運用の一部が中国企業や日本企業の中国拠点に委託**されていた。また、トークのテキストデータは国内のデータセンターに保管されている一方、**画像や動画等のデータは韓国のデータセンターに保管**されていた。
- LINEは国内で8,600万ユーザが利用するとともに、一部公共サービスにも利用されており、データの適正な取扱い、サイバーセキュリティ上のリスクに懸念がある。

データの保管場所

※LINE株式会社の公表資料及び同社から聴取した内容に基づき作成

サービス	データ	保管場所
LINEメッセンジャー（トーク）	テキスト	日本
	画像・動画・ファイル	日本・韓国
LINE公式アカウント（トーク）	テキスト	日本
	画像・動画・ファイル	韓国

国外での情報の取扱い

実施拠点	主な業務	主な取扱い情報
NAVER China	・公開タイムラインと通報コンテンツのモニタリング（日本・台湾・タイ・インドネシア以外） ・LINEゲームサービスのモニタリング、テスト	通報されたテキスト・画像・動画・ファイル
日系企業A社の中国拠点	・公開タイムラインとオープンチャットのコンテンツモニタリング ・タイムラインとオープンチャットで通報されたコンテンツのモニタリング	通報されたテキスト・画像・動画・ファイル
LINE Digital Technology（通称LINE China）	・通報モニタリングツールの開発保守 ・画像処理、モニタリングフィルター開発	通報されたトーク・タイムライン・公式アカウントのテキスト/画像/動画

LINE株式会社に対する行政指導

■ LINE株式会社の報告に基づく限りにおいては、通信の秘密の侵害等があった旨は確認できなかった一方で、**社内システムの安全管理措置等や利用者に対する説明等に関して一部不十分な点が認められた**。

■ このため、令和３年４月26日、同社に対し文書による**行政指導を実施**。指導を踏まえて講じた措置の状況について、同年５月末までの報告を求めている。

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（社内システムの１つであるモニタリング支援システム：LINE Monitoring Platform）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。

電気通信事業ガバナンス検討会

■ デジタル変革時代における安心・安全で信頼できる通信サービス・ネットワークの確保を図るため、電気通信事業者におけるサイバーセキュリティ対策及びデータの取扱いに係るガバナンス確保の今後の在り方について検討を行うことを目的として、令和３年５月より、「電気通信事業ガバナンス検討会」を開催。

検討事項

（１）電気通信事業者におけるサイバーセキュリティ対策及びデータの取扱いに係るガバナンス確保の今後の在り方
（２）上記（１）を踏まえた、政策的な対応の在り方
（３）その他

構成員

	相田　仁	東京大学大学院工学系研究科教授
	石井　夏生利	中央大学国際情報学部教授
	上沼　紫野	虎ノ門南法律事務所弁護士
（座長）	大橋　弘	東京大学公共政策大学院院長／大学院経済学研究科教授
（座長代理）	後藤　厚宏	情報セキュリティ大学院大学学長
	中尾　康二	一般社団法人ICT-ISAC顧問 国立研究開発法人情報通信研究機構サイバーセキュリティ研究所主管研究員
	中村　修	慶應義塾大学環境情報学部教授
	古谷　由紀子	公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会監事
	森　亮二	英知法律事務所弁護士
	山本　龍彦	慶應義塾大学大学院法務研究科教授

オブザーバ　内閣官房内閣サイバーセキュリティセンター、内閣官房IT総合戦略室、個人情報保護委員会