

LINEの個人情報保護、 問題の本質は どこにあるのか

LINE

文:西田宗千佳 フリージャーナリスト

3月14日に発覚したLINEの個人情報保護に関する問題は、誤解と懸念をはらんだまま、4月に入っても完全終息はしていない。日本全体で8,600万人が使い、官公庁のデジタル・トランスフォーメーションにとっても重要、とされているLINE。だが、今回の問題によって、その在り方も問われ始めている。では「LINEの抱えていた問題」の本質とは何であり、どうすべきなのか？ その点を深掘りしてみよう。



3月23日午後7時半から行ったLINEの記者会見

LINEは

「中韓から覗き放題」ではない。

だが……

3月14日、朝日新聞の記事から発した「LINEの個人情報取り扱い」に関する問題の本質はどこにあるのか？ それを考えるには、現実問題として「どんな懸念があるのか」という点だ。

LINEの出澤剛代表取締役CEOは会見で、「ユーザーの皆様にご迷惑とご心配をおかけしたこと、ユーザーの信頼を損なうことになったこととお詫びします」と謝罪した。だが、課題は本当に「ご迷惑とご心配をおかけしたこと」なのか？ 謝罪はあくまで「ご心配をおかけしたこと」と「信頼を損なったこと」への謝罪であり、データが漏れた、という話ではない点に留意していただきたい。

「そうではないのでは」と不信感を持った向

きもあるようだが、現実問題として、LINEはこう言うしかない。実際のところ、「一般的な利用者のLINEの中身を覗かれていた」とか、「一般的なLINEの会話が外部に流出した」ということは確認されていない。「LINEは海外、中国や韓国に覗かれ放題だ」というような誤解をしている人もいるが、それは誤解・曲解に近い。

ただし「懸念」はある。その懸念こそが、誤解を含めた問題の本質の一部ではある。それを理解するには、LINEでのデータの取り扱いがどうだったのかを知っておく必要がある。

LINEのメッセージや画像などのデータは、基本的に暗号化されてやり取りがされる。送った人のところで暗号化され、それは送られた人のところで展開される。基本的に、送った人と送られた人以外が暗号を展開することはできず、送信経路でデータを覗くことはできない。データの中身を見られない、というのはLINEの運営も例外ではなく、犯罪捜査や不具合の検

証といった特別な事情がないかぎり、メッセージ内容の閲覧などはできないし、していない。これを「エンド・トゥ・エンド暗号化」という。メッセージングサービスでは一般的な仕組みだ。

その上で、LINEならではの要素が、「データは送った側と送られた側が機器の中で保存している」点にある。別の言い方をすれば、LINEのサーバー内にすべてのデータが保存されていることは保証されていない……ということだ。そのため、スマートフォンの機種交換時などに、自分のタイムラインやメッセージが消えてしまうことがある。

ただし例外がある。送受信の作業やユーザー利便性向上のため、LINEのサーバーにも、メッセージなどのデータは一時的に残る。これは永続的なものではなく、時間がたてば消えていくものだという。LINE側の説明によれば、保存の期間は「サービスによって異なるが数年」。もちろんこのデータも暗号化されていて、

メッセージ同様、特別な事情がない限り中身が見られることはない。

現在のLINEはメッセージングサービスだけで成立していない。ペイメント(LINE Pay)から遠隔医療(LINEドクター)まで、さまざまなサービスの複合体で、サービスからの連絡や入口として、「メッセージサービスであるLINE」が使われる形になっている。

金融や医療など、それぞれ法制度などの違いもあり、個人情報の扱いについても条件が異なるのが実情だ。そこでは当然、通常のメッセージ以外にもサービスに必須となる情報を取得して保存していた。これらも一義的には運用ルールを守り、サービス外での利用や閲覧は行われていなかった、という。

軽く見られていた「中国リスク」

このような中身を見ると、「あれ、問題ってそんなにないのでは?」と思われるのではないだろうか。実際、現行法制度下という条件では、クリティカルな問題は発生していなかったと思われる。

だが、「100%適切であったか」「誤解を生まない状況であったか」というと、そうは言えない。

問題はいくつかある。

まず、直接的に問題だったのは、LINEの運用について、一部を中国企業に委託しており、その過程で、一部の情報が委託先側で閲覧可能になっていた、ということだ。具体的には、スパムを含めた迷惑行為の「通報」が行われた際、通報された情報の監視については、平文で扱われており、「エンド・トゥ・エンド暗号化」の原則を外れていた。

これは通報内容を認識して対処するには必要なことで、管理上で必要とされる範囲での利用と判断することができる。日本国内で業務のすべてと、システム開発が行われていたなら問題にはならなかっただろう。

だが、この管理システム開発の一部について、LINE Fukuokaを経由して中国法人に外

今後のデータ管理方針サマリ
 現在、日本国外で保管・管理している以下のデータは順次、日本国内に移転予定です。

データ種別		現在のデータ保管場所	今後のデータ保管場所*	データ移転完了時期
LINEメッセージ(トーク)	テキスト	日本	日本	21年6月予定
	画像/動画/ファイル	日本/韓国		21年8月予定
LINE公式アカウント(トーク)	テキスト	日本	韓国	国内保管で開始
	画像/動画/ファイル	韓国		21年9月予定
自治体向け コロナワクチン予約システム	テキスト	-	-	国内保管で開始
LINE Pay	決済情報	日本/韓国	日本	21年9月予定

※対象：日本国内のユーザー・LINE公式アカウント

会見で説明した「今後のデータ管理方針サマリ」

部委託されていたことが問題だ。その過程で通報されたトークの内容や関連情報も、開発企業側の担当者が閲覧可能だったという。

中国の場合、2017年に成立した「中華人民共和国国家情報法」の関係から、中国政府の判断により、中国国内にあるサーバーのデータはすべて中国政府の求めに応じて情報提供する義務を負っている。結果として、中国にあるデータについては、中国政府側がある程度自由に覗ける……と考えていい。

この関係から「LINEの情報は中国から見られていたのでは」という懸念につながる。だが前述のように、システムの構成を考えれば、そうしたことが起きるとは考えづらい。ただし、「中国の企業を個人情報に関わる業務に利用していた」という点において、リスクが存在したことは間違いない。

この点については、LINE側も非を認めている。出澤CEOは、「(中国の)国家情報法について、2017・18年頃の潮目の変化を見落としていた。情報としては把握していたが、感度が足りなかったと反省している」と答えた。

2017年当時から、国家情報法のリスクは関連業界では課題とされていたので、LINE側が認識していなかった、というのはお粗末な話ではある。

「韓国にデータが置かれていた」 このことの本質

もう1点は、データの保存場所についてだ。

前述のように、LINEは「個人のデータは個人が保管しているもので、LINEは永続的な保存をしていない」という立場で運営されている。だが、一時的なものとはいえ、個人データがサーバーに蓄積されているのは事実。中には個人認証などのために使われる保険証や医師免許などの画像データもある。

そうしたデータはどこにあったのか? これまで同社は「主たる情報は国内に保存している」と説明してきたのだが、実際には、「トークなどのテキストは日本に」「画像・動画などは韓国に」存在する形だったという。画像は主たるデータではない、という扱いだっただけだ。前述のように、遠隔医療や決済サービスでの個人認証の関係から、保険証や免許証などの画像データが取得されているわけだが、それらも韓国に保管されていた。

韓国に保存していた理由について、LINEの舛田淳CSMOは、「日本以外の国、台湾・タイ・インドネシア・ロシア・中東でもLINEは展開している。それらの国でも即応性と高いセキュリティが保てる場所はどこかと考えた場



「ユーザーの皆様にご迷惑とご心配をおかけした」と謝罪するLINE出澤剛代表取締役CEO

合、韓国だった」と話す。ただし、近年は「オープンチャットなど国内向けのサービスが増えてきたこともあり、2019年頃から順次日本へサーバーを移管していた」（舩田氏）と言う。

このことから「韓国にLINEの情報が筒抜けだったのでは」という指摘があるのだが、これも素直に考えると正しくはない。必要な人員以外はアクセスできない形であるからだ。日本での管理と同じ形態だったとするならば、そのことが直接的な問題とは言えない。

韓国は北朝鮮との戦時下であり、戦時法制によって、捜査礼状などを使わずにデータの提出を求めることも不可能ではない。だが、一般論として、他国のサービスが暗号化しているデータへと無差別にアクセスできる状況である、と考えるのは難しい。中国とは状況が異なる。

とはいえ、完全に問題がなかったか、というと、これもまた違う。

理由は、LINEが利用許諾でのポリシー明示の中で、具体的に「どの国にデータが置かれているのか」を明記していなかったからだ。「主たるデータは日本にあります」という説明と、「画像は韓国に置かれています」という説明とでは、受ける印象も判断も異なる。国内にデータがあるものだと思って利用していた側としては、「ちょっと話が違う」と思うのではないか。

結果的に、LINEは2021年中に、国内LINE関連事業のデータをすべて日本のサーバーに移行する。中国での開発・管理業務も3月の段階ですでに終了し、日本だけの体制

に変えている。プライバシーポリシー表記についても、3月31日付で、より現状に合わせた形へと改定している。

重要なのは 「日本にデータがある」ことではない

こうやって情報整理をすると、ようやくだが、LINEの本当の問題点が見えてくる。「日本にデータがあればいいのか」というと、これは違う。

本質として重要なのは「ちゃんと管理されている」ことだ。暗号鍵や情報閲覧ができる権利者の管理がちゃんとできていなければ、どの国にあってもデータは安全ではない。「他国からデータを覗かれていた」というのは正直濡れ衣に近い。その可能性はゼロではないが、それを言うなら、どの国だってあり得る話なのだ。そして、データが流出したり覗かれたりするときの一番の可能性は「管理の不適切さ」にある。

今回の場合、LINEは事態を以前からやんわりと把握していながら、記事で指摘されるまで大ごとにしなかった。確かに現行法制度上は問題ないし、データ移管は今回のことがなくても進める計画だったという。2022年施行の「改正個人情報保護法」への対応も進めてはいたようだ。だが、誤解なく利用者に運用状況が伝わるようであれば、問題は解決しないのだ。中国法人利用についての鈍感さもある。

これらのことは、LINE側が「厳密で透明な運用」について、どこか軽く見ていた部分がある……という証でもある。アメリカであろうが韓国であろうが、「その国にデータが置かれるサービスを使いたくない」と思う人がいるのは自由だし、そうした条件を元にサービスを選ぶのも自由だ。だが、記載がないということは、許諾するための条件が示されていないということであり、その状況は「不適切」だ。

政府自治体向けのサービスについても、画像が海外に置かれている事実を行政側・消費者は認識していただろうか？

そうした緩さが存在した以上、「管理体制を100%信じるのは難しい」と考える人がいても不思議ではない。

1社のサービスに依存する危険性

もう一つの課題は、LINEという1つのサービスに多くの人や行政が依存している、という事実だ。

もちろん、それは便利ではある。活用が悪い、ということでもない。だが、今回のような話が起きたときに、すぐに「別のサービスを選ぶことができない」ことはリスクだ。

このことは、日本だけの問題ではない。ネットでのメッセージングは、電子メール以降、「特定の企業が運用するサービス」に依存している。海外なら「WhatsApp」「Facebook Messenger」（ともにFacebook傘下）だし、中国なら「WeChat」や「QQ Mobile」の利用が多い。電子メールと違うのは、オープンにどの企業も使える仕組みではなく、特定企業が運営するものだ、ということだ。

携帯電話の世界では国際規格として「RCS」があるが、規格だけを使い、企業間で相互可用性のない形で使われている。NTTドコモ・KDDI・ソフトバンクが使う「+メッセージ」も、楽天モバイルが使う「Rakuten Link」も、RCSベースだが直接的な互換性はなく、携帯電話のショートメッセージサービスである「SMS」を介してのやり取りができるだけだ。

どの国にも、今のスマホ時代にあった「インスタント・メッセージングサービス」において、特定の企業に依存しないものはあまり広がっていない。そのことは認識しておく必要がある。

その上で、行政は、「複数のサービスに対応する」「利用する人の秘匿性レベルに応じて、使っているサービスを定める」などの対応が必要になる。そうした基本方針は定まっているわけではなく、判断が各自治体に委ねられている。国としての姿勢を示す必要があることが、LINEの不手際によってより明確に見えてきた、と言ってもいいのではないだろうか。 