LINE 暗号化状況レポート

日本語 2022年 12月

2022.12.14

本レポートの目的

このレポートは、LINEの各機能で提供される暗号化方式の種類、保護対象及び、暗号化の適用状況の公開を目的としています。

LINEが提供する暗号化

LINEではユーザーの情報を保護するため、様々な方式の暗号化を行っています。クライアントとサーバー間の通信を保護する通信レイヤーの暗号化(LEGY暗号、TLS)に加えて、対応しているメッセージタイプや通話タイプにおいては Letter Sealing による暗号化が行われます。 Letter Sealing LINEの開発したエンドツーエンド暗号化(End-to-end encryption: E2EE)プロトコルです。

LINEで利用されている暗号化方式、及びアルゴリズムの詳細については**暗号化ホワイトペーパー**を参照してください。

暗号化の適用状況

(1)メッセンジャー機能

■Letter sealing (End-to-end encryption)

LINEのメッセンジャー機能で送受信される「テキスト」及び「位置情報」は、以下のいずれかの状況において Letter Sealing で暗号化されます。

両者のユーザーが Letter Sealing をONにした状態の1対1トーク

全てのユーザーが Letter Sealing をONにした状態の50人以下のグループトーク

チャットルームが Letter Sealing で保護されているかどうかを確認したい場合には、**こちら**のガイドをご覧ください。テキスト、位置情報以外に送信される画像、動画、ファイル、音声メッセージなどのコンテンツは、LEGY暗号*1または TLS により通信レイヤーで暗号化されます。以下の図(Figure 1)は、2021年8月から2022年8月までの期間における通信レイヤーでのコンテンツ別の暗号化の適用状況を示しています。

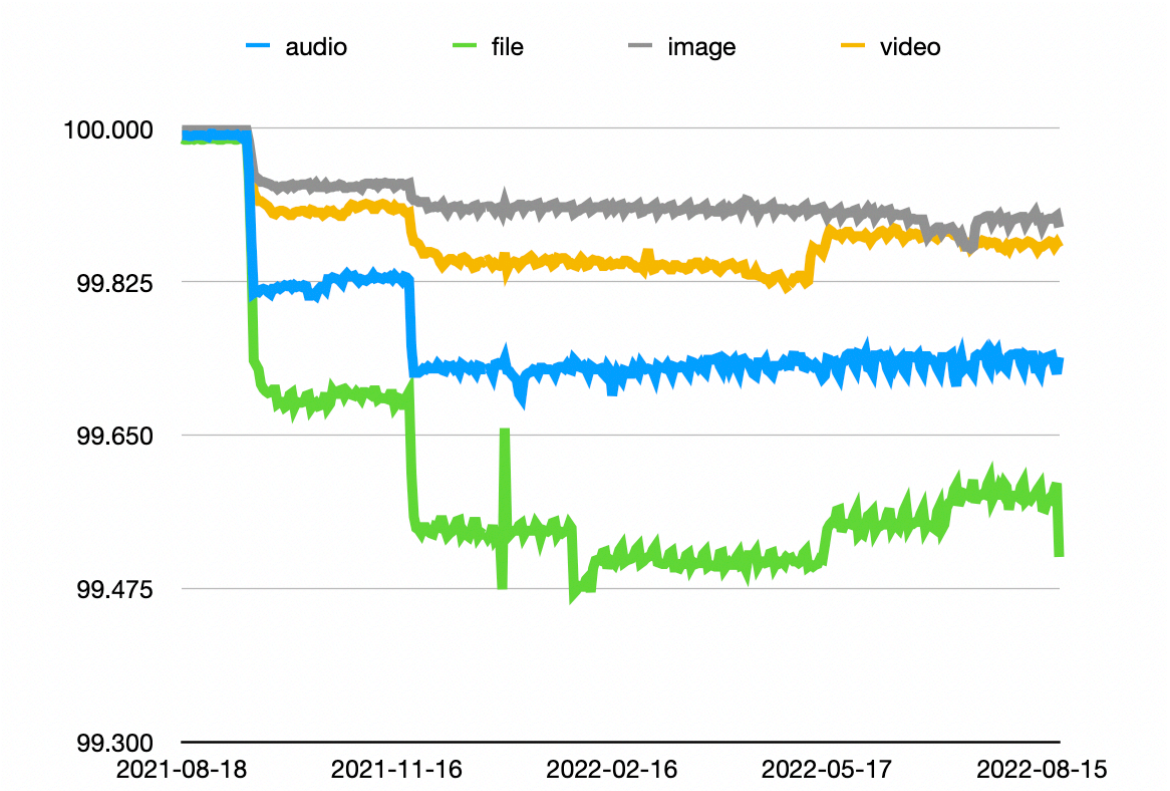

Figure 1: 暗号化適用状況の時系列推移

*1 LEGYとはLine Event-delivery GatewaYの略称で、カスタムで構築されたAPIゲートウェイサーバーを指します。LEGYでは鍵交換と暗号化に標的な暗号化アルゴリズムを用いています。

* 2021年8月以前の暗号化適用状況の推移については、**去年のレポート**を参照してください。

■通信レイヤーの暗号化

通信レイヤーの暗号化について、以前はLEGY暗号が使用されていましたが、現在はTLSに移行しておりTLSがデフォルトの暗号化プロトコルとなっています。TLS1.2および1.3が現在サポートされており、前方秘匿性(Forward Secrecy)を確保するために、鍵交換にDHEまたはECDHEのいずれかが使用されます。

また、これまでいくつかの技術的もしくは環境的な要因によって、通信レイヤーの暗号化が特定の種類のコンテンツに対し十分に適用されていない状況がありましたが、2017年9月以降は概ね100%の適用率を維持しております。

- 暗号化によるパフォーマンスの問題により適用を見送った時期がありました。
- 一部の国家のモバイルネットワーク接続環境において、HTTPS が利用できない時期がありました。現在は、接続環境に関係なく暗号化を適用しています。
- 2017年7月、音声ファイルの暗号化適用範囲を拡大した際に発生した不具合を解決するため、約2ヶ月の期間、暗号化適用範囲を縮小しましたが、2017年9月に再度、暗号化適用範囲を拡大いたしました。

各コンテンツタイプ別の暗号化状況(Letter Sealing, LEGY暗号, TLS)をまとめると以下になります。

コンテンツタイプ	2015年	2016年	2017年9月	2018年4月	2019年10月	2020年9月	2021年9月	2022年8月
テキスト	○	○ → ◎	◎	◎	◎	◎	◎	◎
位置情報	○	○ → ◎	◎	◎	◎	◎	◎	◎
スタンプ *2	△	△	○	○	○	○	○	○
画像ファイル *3	△	△	○	○	○	○	○	○
ボイスメッセージ *4	X	X	○	○	○	○	○	○
動画ファイル *4	X	X	○	○	○	○	○	○
その他のファイル *3	△	△	○	○	○	○	○	○
リアクション	-	-	-	-	-	-	○	○

凡例: ◎ Letter Sealing (End-to-end encryption) / ○ 通信レイヤーの暗号化 / △ 部分的な保護 / X 暗号化無し or 不十分な暗号化

■補足説明

◎は主要な利用環境において、Letter Sealing による暗号化がデフォルトで有効化されていることを示しています。
○は主要な利用環境において、当時の判断における十分な水準の通信経路上での暗号化を行っていることを示しています。
△は部分的な保護ですが、当時及び当レポート公開時点での判断において、概ね問題がないと考えられる水準での暗号化を行っていることを示してます。
Xは当レポート公開時点での判断において、十分な保護ではなかったと考えられるものを示しています。

*2 △の時期において、スタンプのパッケージダウンロード時に HTTP を利用、スタンプ送信のメッセージ自体は暗号化が適用。
*3 △の時期において、HTTP/HTTPS を併用、利用環境(OS, 地域, 回線種類など)によっては暗号化が適用されない状況があった。
*4 Xの時期において、WiFi利用時かつアップロード時のみ暗号化を行っていた。

OSやLINEクライアントのバージョンが古い場合は、上記に記載されている通りの暗号化が適用されなかったり、古い暗号化方式での通信が行われるなど、十分な保護が得られない場合があります。

(2)LINE通話機能（音声通話、ビデオ通話）

LINEはいくつかのタイプの通話機能をサポートしています。LINEの通話機能において「音声通話(1対1)」と「ビデオ通話(1対1通話)」は、Letter Sealing によってエンドツーエンドで暗号化されます。「グループ通話」「グループビデオ通話」および「LINEミーティング」においては、通信レ

ヤーのみの暗号化が適用されます。各時期における暗号化の状況は以下のテーブルを参照ください。

通話タイプ	2015年	2016年	2017年9月	2018年4月	2019年10月	2020年9月	2021年9月	2022年8月
1対1音声通話	○	○ → ◎	◎	◎	◎	◎	◎	◎
1対1ビデオ通話	○	○ → ◎	◎	◎	◎	◎	◎	◎
グループ通話	○	○	○	○	○	○	○	○
グループビデオ通話	-	○	○	○	○	○	○	○
LINE ミーティング	-	-	-	-	-	○	○	○

凡例: ◎ Letter Sealing (End-to-end encryption) / ○ 通信レイヤーの暗号化 / - 機能未実装

(3)Letter Sealing (End-to-end encryption) 適用状況

Letter Sealing はLINEによるエンドツーエンド暗号化プロトコルです。 Letter Sealing が有効化されたメッセージは、LINEクライアント内で予め号化された状態で送信され、LINEサーバー側でも内容を解読することは出来ません。Letter Sealing は2015年8月よりオプション機能として提供され、2016年に主要な利用環境においてデフォルトで有効化されました。

現時点では Letter Sealing による暗号化に対応しているメッセージタイプは限定されています。 Letter Sealing はデフォルトで有効化されており、オフに設定することはできません。

■Letter Sealingによる保護対象

- テキストメッセージ (1対1トーク、50人以下の1対nトーク及びグループトーク)
- 位置情報メッセージ (1対1トーク、50人以下の1対nトーク及びグループトーク)
- 音声通話 (1対1通話)
- ビデオ通話 (1対1通話)

* ファイルとして送信されたビデオ(動画)、音声は、現時点では Letter Sealing の対象外となります。

■Letter Sealingの例外

例外として、以下のケースではユーザーのコミュニケーションの一部がLINEサーバーに送られます。

・ウェブサイトのプレビュー機能(PagePoker): チャットルーム内でウェブサイトのプレビューを生成するためにURLがPagePokerサーバーに送信されます。送信されたURLはプレビューを生成する目的においてのみ利用されます。ユーザーは設定画面からこの機能を無効にすることができます。(設定 → トーク → URLプレビュー)

・スパムの通報: ユーザーがスパム行為を通報する場合、スパム行為が疑われるチャットメッセージの一部が調査のためサーバーに送信されます。報告者が同意する場合に限り、指定されたメッセージの一部がサーバーに送信されます。

・メッセージのアナウンス: 送受信したメッセージ、作成した投票、イベントなどを「アナウンス」して、チャットの上部に永続的に表示することができます。アナウンスは新しく参加したメンバーにも表示する必要があるため、ユーザーによりアナウンスに設定されたメッセージはサーバー送信されます。

・スタンプキーワード: LINEクライアントは、適切なスタンプをおすすめするためにメッセージ内の特定のキーワードをチェックします。一致するものがある場合は、匿名でサーバーに送信されます。

また、AppleやGoogleのような第三者が提供するクラウドバックアップ機能を用いる場合には、メッセージはエンドツーエンドで暗号化されませんこのような場合にはクラウドストレージ上に暗号化されていないコンテンツが保存されます。

■機能別の適用状況の概要

Letter Sealing	部分的なLetter Sealing	通信レイヤーの暗号化
テキスト、位置情報 1対1通話 次世代Googleアシスタント	メッセージスタンプ*5	メディアファイルメッセージ スタンプ カスタムスタンプ Open chat 公式アカウントとのトーク グループ通話

LINE Meeting
LINEソーシャルプラグイン
リアクション
メッセージのアナウンス
LINE災害連絡サービス
イメージマップメッセージ
テンプレートメッセージ
Flex Message
Story message

*5 LINEクライアントはユーザーが入力したテキストをスタンプに描画するためにレンダリングサーバーと通信する必要があります。クライアントとレンダリングサーバー間のテキストの通信は Letter Sealing で保護されています。一方、レンダリングサーバーで生成されたスタンプは通信レヤーの暗号化でのみ保護されています。

■Letter Sealingに関する補足

Letter Sealing によるメッセージの暗号化は、通信を行う双方(グループの場合はグループ参加者全員)のクライアントが Letter Sealing に対応し、Letter Sealing を有効にしている必要があります。もし通信を行うクライアントのいずれかが Letter Sealing を無効にしていた場合、通信レイヤーでの暗号化のみが行われます。

■Letter Sealing のバージョン

2015年にリリースされたLINEエンドツーエンド暗号化プロトコルの最初のバージョンをLetterSealing バージョン1 (v1) と呼んでいます。 Letter Sealing v1 は、1対1のトークとグループトークにおいてエンドツーエンド暗号化に対応しました。

Letter Sealing v1 のリリース後、LINE Bug Bounty プログラム経由で、五十部孝典氏(兵庫大学)と峯松一彦氏(NEC 中央研究所)により、メッセー改ざんやユーザー乗っ取りに利用されうるプロトコルレベルの問題が報告されました。調査の結果、報告された問題はLINEメッセージサーバーで実されたメッセージ検証や制限によってブロックされており、実際のLINE環境では実行できないことが確認されましたが、将来的に発生しうる Lette Sealing への攻撃を防ぐため、報告者と協力し、その問題を修正した Letter Sealing バージョン2 (v2) を開発しました。 Letter Sealing v2 の詳細情報については、**暗号化ホワイトペーパー**を参照してください。

Letter Sealing v2 は、2019年10月にLINEの主要なクライアントに実装されました。各LINEクライアントの Letter Sealing v2 対応に必要なバージョンを以下のテーブルに示します。

LINEクライアント	バージョン
LINE for iOS/iPad OS	8.15.0
LINE for Android	8.17.0
LINE for Mac/Windows	5.12.0
LINE Chrome Extension/ChromeOS	2.2.0
LINE Lite for Android	2.6.0

■Letter Sealing v2 の利用状況

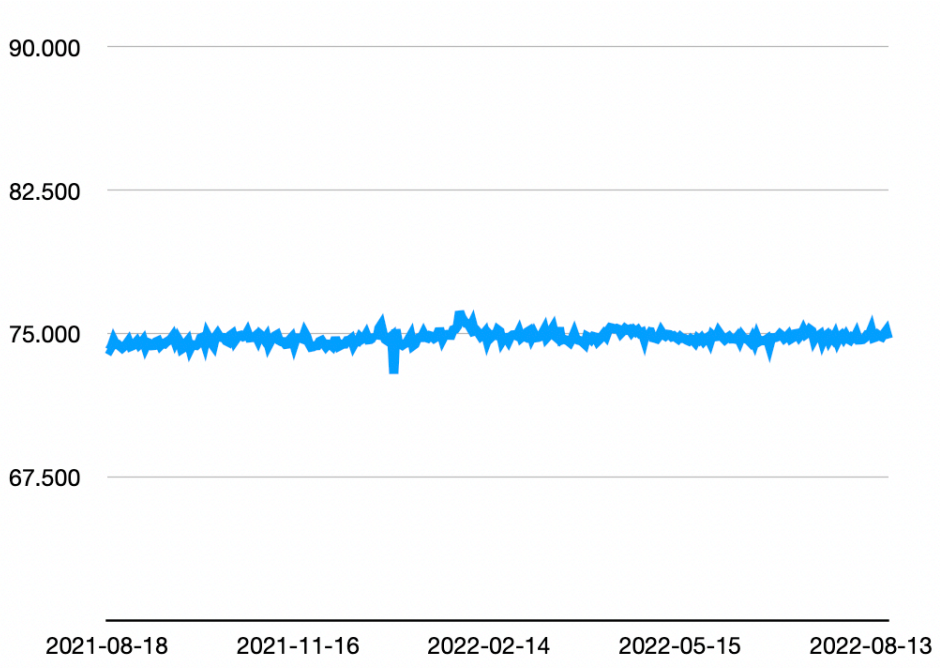

Figure 2: 全LetterSealing トラフィックにおける Letter Sealing v2 が占める割合

Letter Sealing v2 は2019年から適用されています。上の図(Figure 2)は全ての Letter Sealing トラフィックにおける Letter Sealing v2 が占める合を示しています。2021年8月以前のデータについては、**去年のレポート**を参照してください。

■アカウントの引き継ぎ

アカウント引き継ぎを行う場合、以前のメッセージを復号するために Letter Sealing の鍵を移動させる必要があります。まだ引き継ぎ前の端末が手にある場合は鍵を新しい端末へ転送できます。詳細についてはこちらの**オフィシャルガイド**を参照ください。

安全のために、我々は Letter Sealing の鍵の転送においてもエンドツーエンドでの暗号化を行なっています。引き継ぎ前の端末と新しい端末はお互の端末でそれぞれ一時的なECDH鍵ペアを生成します。暗号化された通信路を確立するために必要な引き継ぎ前の端末のECDH公開鍵は、QRコード使用してインターネットを介さずに新しい端末へ送信されます。 Letter Sealing の鍵はECDH鍵共有から生成した鍵を用いてAES256-GCMにより暗号化され、引き継ぎ前の端末から新しい端末へ送信されます。

■鍵のバックアップ

LINEでは Letter Sealing の鍵を安全にバックアップすることができます。もし万が一端末を無くした場合でも、無くした端末の鍵で暗号化されたメッセージにアクセスできます。バックアップを有効にするためにはこちらの**オフィシャルガイド**を参照ください。

機密性を確保するため、鍵は6桁のPINコードから生成されたキーにより、Client-Side Encryption (CSE) を用いて暗号化しています。さらに暗号化された鍵はSGXサーバーにより保護されており、またエンドツーエンドで暗号化されています。

(4)Forward Secrecyの対応状況

一部のLINEの利用環境は Forward Secrecy(前方秘匿性) に対応しています。 Forward Secrecy とは、もしも一方当事者の秘密鍵が漏洩した場合でも漏洩以前に暗号化されたメッセージが保護されることを保証する暗号方式です。現時点では Forward Secrecy の性質を持つ暗号化通信は限定されています。

■LINEサーバーとの通信暗号化における Forward Secrecy (LINEサーバー内の秘密鍵が漏洩した場合の前方秘匿性)

2021年 主要な利用環境において一部のデータが非対応*6

2017年9月 主要な利用環境において対応 *7

2016年 部分的に対応 *8

*6 TLS1.3の0-RTT(Zero Round Trip Time)機能有効化により一部のデータ(Early Data)が非対応。
*7 OSやLINEクライアントのバージョンによっては非対応。
*8 一部の地域、クライアントでのみ対応。

■Letter Sealingにおける Forward Secrecy (ユーザーの端末内の秘密鍵が漏洩した場合の前方秘匿性)

未対応