LINE 暗号化状況レポート

日本語 2020年 11月

2020.11.11

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、暗号化の適用状況を情報公開すること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。LINE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、HTTPS)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 は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。

暗号化適用状況

(1)メッセンジャー機能

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、以下いずれかの状況においてLetter Sealingによってend-to-end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1対nトーク(50人以下)
全てのユーザーがLetter SealingをONにした状態のグループトーク(50人以下)

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、位置情報以外に送受信される画像、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 HTTPS により通信レイヤーで暗号化されます。以下の図は2019年11月から2020年9月の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。

*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は鍵交換と暗号化に標準的な暗号化アルゴリズムを用いています。

* 2019年10月以前の暗号化適用の推移については、**去年のレポート**を参照してください。

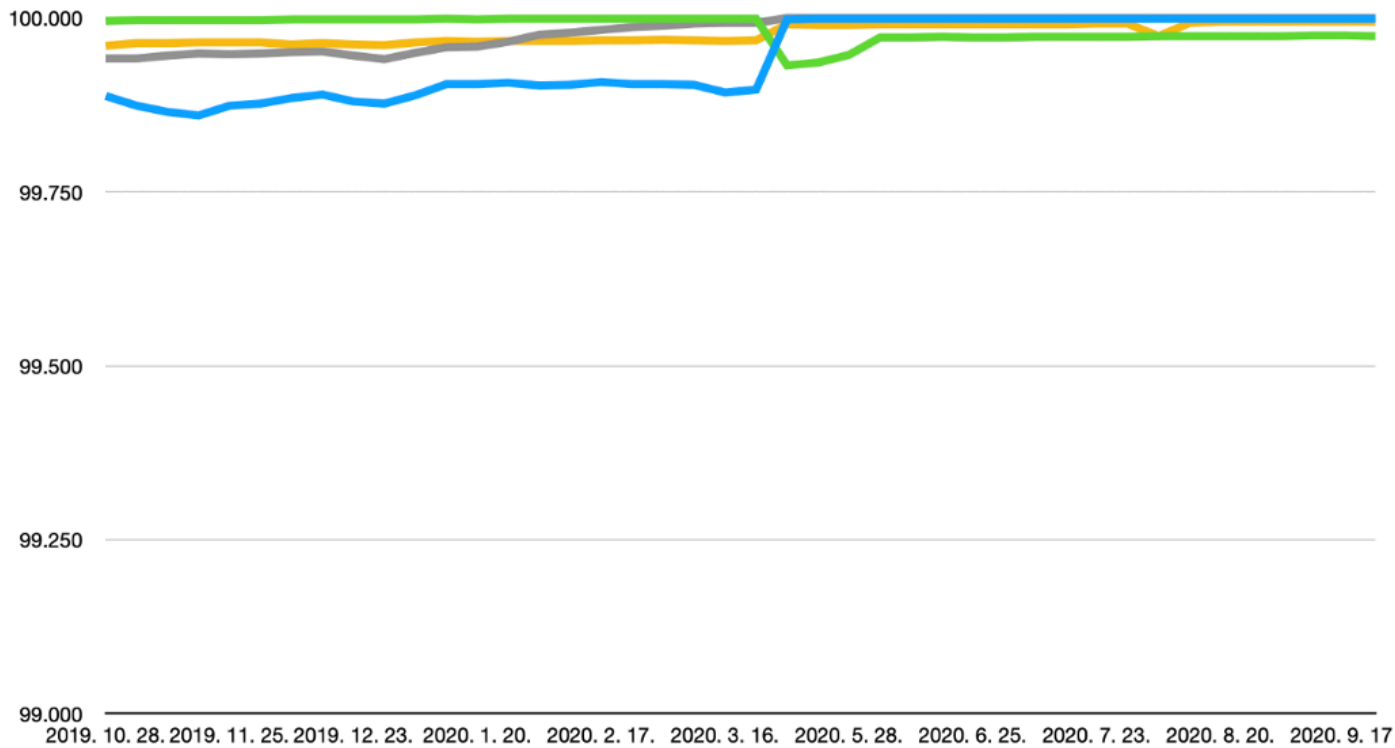

図1: 暗号化適用状況の時系列推移

なお、これまで以下のいくつかの要因によって、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ませんでしたが、2017
9月以降は概ね100%の適用率を維持しております。

- 暗号化適用に関わ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
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, HTTPS)をまとめると以下のようになります。

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
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	△	△	○	○	○	○

凡例: ◎ Letter Sealing対応 / ○ 通信経路上での暗号化あり / △ 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が行われています。
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)によっては暗号化を行わない。

*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う。

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の通話機能において、「音声通話 (1対1通話)」「ビデオ通話 (1対1通話)」は、以下の状況においてLetter Sealingによってend-to-endで暗号
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、通信路上の暗号化が適用されています。

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
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対応 / ○ 通信経路上での暗号化あり / - 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の実装です。 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暗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年中に主要な利用環境で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、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

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のサーバーに送られることがあります：

・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のみにおいて利用されます。ユーザーは設定画面からこの機能を無効化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このようなメッセージはサーバーに送信されます。

■機能別の適用状況の概要

E2EE	部分的なE2EE	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	テキスト、位置情報以外のメッセージ スタンプ カスタムスタンプ OpenChat グループ通話 LINE Meeting LINEソーシャルプラグイン

*5 ユーザーが好きな言葉を入れたスタンプを生成するため、ユーザーのクライアントは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E2EEで保護されています。一方、生成されたスタンプは通信レイ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。Letter Sealingが無効化されている場合、通信経路上での暗号化のみが行われます。

■Letter Sealing バージョン

2016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バージョンを Letter Sealing バージョン1 (v1) と呼んでいます。Letter Sealing v1 は、1-to-1 とグループチャットのエンドツーエンド暗号に対応してる一方で、メッセージ改ざんやユーザー乗っ取りに使えるプロトコルレベルの問題があります。その問題につては、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)が報していただきました。報告された問題は、プロトコルレベルの問題で、LINE メッセージサーバーで実装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 環境で実行できないことを確認しました。LINE ユーザーのセキュリティを向上し、将来的に発生しうる Letter Sealingへの攻撃を防ぐため、報告者と協力し、E2EE v2 を開発しました。E2EE v2 について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。

E2EE v2 は、2019年10月にLINEの主要なクライアントに対してリリースしました。各 LINE クライアントのE2EE v2 対応に必要な最低バージョンを以下のテーブルに示しています。

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

■E2EE v2 利用状況

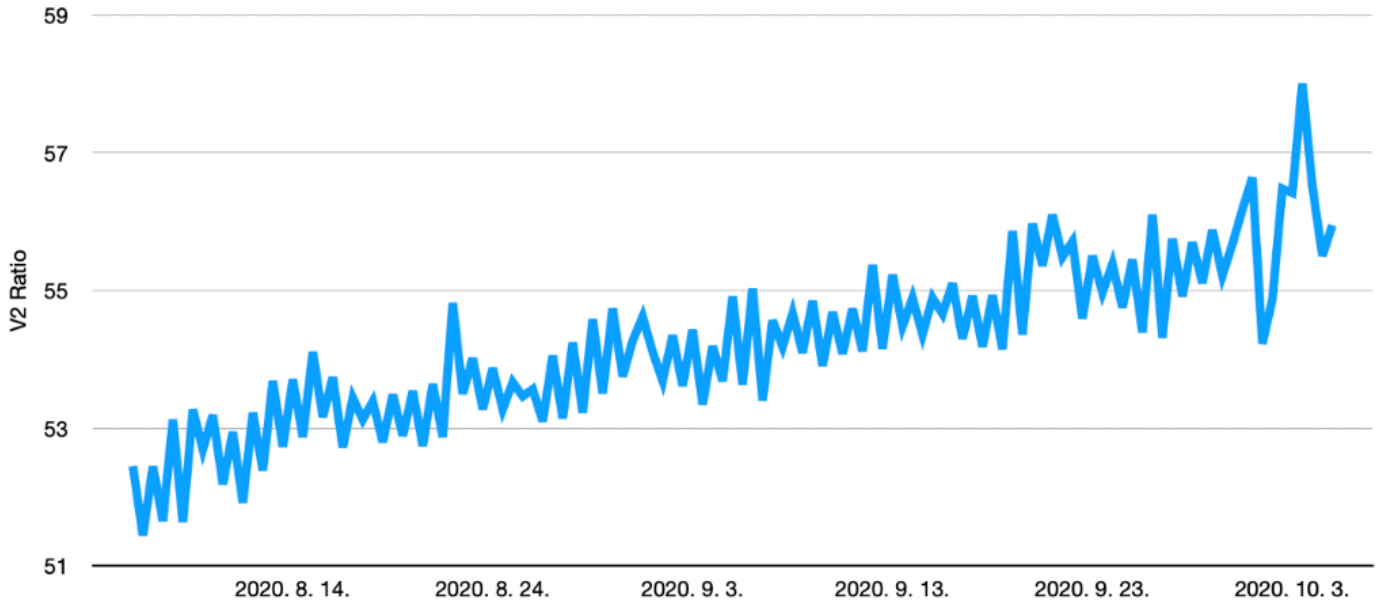

図2: 全E2EEトラフィックに占めるE2EE v2の割合

1年前にE2EE v2が適用されて以降、徐々にE2EE v1からv2への置き換えが進んでいます。上の図は全てのE2EEトラフィックにおけるE2EE v2が占る割合を示しています。現在は半分以上のE2EE通信がv2であり、この割合は増加しています。

(4)Forward Secrecyへの対応状況

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。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Forward Secrecyは保証します。 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)

2017年9月 ○ 主要な利用環境において対応 *6

2016年 △ 部分的に対応 *7

*6 OSやLINEクライアントのバージョンによっては非対応 / *7 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)

非対応