LINE 暗号化状況レポート

日本語 2017年 9月

2017.09.13

本レポートの目的

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経路上での暗号化に加えて、 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。 このレポートは、LINEの各機能において適用される暗号化方式の種類と保護対象を明確にすることを目的としています。

LINEにおける主要なメッセージタイプの暗号化状況

	2015年	2016年	2017年9月
テキスト	○	○ → ◎	◎
位置情報	○	○ → ◎	◎
スタンプ ※1	△	△	○
画像ファイル ※2	△	△	○
ボイスメッセージ ※3	x	X	○
動画ファイル ※3	x	X	○
その他のファイル ※2	△	△	○

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。

※1 △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
※2 △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。
※3 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。

音声通話、ビデオ通話の暗号化状況

	2015年	2016年	2017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	-	○	○

凡例: ◎ Letter Sealing対応 / ○ 通信経路上での暗号化あり / - 機能未実装

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。

Forward secrecyへの対応状況

LINEの利用環境によってはForward secrecy に対応しています。Forward secrecyに対応した通信では、万が一秘密鍵が漏洩した場合でも、それ以前に暗号化されたメッセージは保護されます。 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 ※1

2016年 △ 部分的に対応 ※2

※1 OSやLINEクライアントのバージョンによっては非対応 ※2 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

更新履歴

2017年9月13日 公開