System and Organization Controls (SOC) 3 Report

セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに関連した LINE メッセンジャーサービスシステム係る SOC3 Report

2018 年 1 月 1 日から 2018 年 12 月 31 日まで

Ernst & Young Han Young
Taeyoung Bldg.,
111,Yeouigongwon-ro
Yeongdeungpo-gu, Seoul,
Seoul 07241 Korea
Tel: +82 2 3787 6600
Fax: +82 2 3787 4671
ey.com/kr
※ Ernst & Young Han Young is the global network firm of Ernst & Young

独立受託会社監査人の報告書

LINE 株式会社御中

範囲:
私たちは、LINE 株式会社（以下、「LINE」という。）の「受託会社確認書」を評価しました。当該「受託会社確認書」は、2018 年 1 月 1 日から 2018 年 12 月 31 日までにわたって LINE メッセンジャーサービスシステムに対する会社の内部統制が有効であり、セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーにおいて会社が提供するサービスとシステムの要求事項が AICPA の TSP Section 100 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy（以下、「Trust サービス」基準という。）を充足しているかに対して合理的な保証を提供するという事実を含んでいます。

経営陣の責任
「受託会社確認書」に対する責任は、LINE の経営陣にあります。「受託会社確認書」の根拠となる Trust サービス分類および関連項目の選択、また当該「受託会社確認書」に対する合理的な根拠の提供と共に次の事項における責任も経営陣にあります。

- LINE メッセンジャーサービスシステムの識別およびシステム環境に対する記述
- LINE が提供するサービスとシステム要求事項また、サービスおよびシステム要求事項の目標充足に脅威となるリスクの識別
- サービスおよびシステム要求事項の充足に脅威となる様々なリスクを緩和するために LINE メッセンジャーサービスシステムと関連した有効な内部統制の識別、デザイン、構築、運用とモニタリング

私たちの責任
私たちの責任は、私たちの評価結果に基づいて「受託会社確認書」に対する意見を提示することです。私たちの評価は AICPA の認証基準に基づいて実施されました。当該基準は、「受託会社確認書」が重要な点において公正に記述されたかどうかについて合理的な保証を得るための監査を計画し、実施することを求めます。私たちの評価は「受託会社確認書」に関する証拠の獲得手続を含んでおり、ここには、（1）LINE メッセンジャーサービスシステムのセキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに関連する政策、プロセスと統制に関する理解(2) 統制の運用効果に対するテストおよび評価 (3) そして、評価目的によって必要と判断される手続の実施を含んでいます。私たちは、不正または誤謬によって記述書が公正に表示されないリスクに対して評価などの手続を通じて監査手続の性質、時期、範囲を選定しました。監査期間中に獲得した証拠は、私たちの意見に対して合理的な根拠を提供すると考えます。

私たちの評価は、LINE のサイバーセキュリティリスク管理プログラムを評価する目的として実施されていないため、サイバーセキュリティリスク管理プログラムに対するいかなる保証は提供しません。

受託会社の内部統制の固有限界

統制の固有な制約事項によって間違って記述された内容の一部を予防、摘発または訂正できない場合があります。そして、未来の期間における効果の評価予測または、LINE のサービス提供とシステム要求事項が充足されるための統制デザインの適合性に関する結論は、統制が状況の変化によって不適切に変わること、統制の遵守水準の低下、システムまたは統制環境に対する変化、システムまたは統制に対する適切な変更の失敗によってその評価もしくは適合性に対する妥当性が変更される可能性があるリスクの水準によって変わる場合があります。セキュリティに関連した内部統制の固有限界の例として、(a)製造会社および開発が設計した IT 機器の脆弱性(b)供給会社およびビジネスパートナの内部統制の失敗(c)進化した技術および社会工学的な手法を利用した継続的な攻撃などが挙げられます。

意見

私たちの意見は、2018 年 1 月 1 日から 12 月 31 までにわたって LINE メッセンジャーサービスシステムの統制が有効に運用されており、LINE のサービスおよびシステム要求事項が Trust サービス基準を充足することに対して合理的な保証を提供することです。

Ernst & Young Han Young

2019 年 6 月 30 日

Trust サービス規準の
セキュリティ、可用性、処理のインテグリティ、機密保持およびプライバシーに関連した
LINE メッセンジャーサービスの有効な内部統制に関する受託会社確認書

2019 年 6 月 30 日

LINE 株式会社の経営陣（以下、LINE という。）は次の責任があります。

- LINE メッセンジャーサービスに対する記述書に含まれている LINE メッセンジャーサービスシステム（以下、システムという。）の識別および関連システム環境に対する記述
- サービスおよびシステムの要求事項の識別
- サービスおよびシステム要求事項の目標充足に脅威となり得るリスクの識別
- サービスおよびシステム要求事項の充足に脅威となるリスクを緩和するために LINE メッセンジャーサービス関連の効果的な内部統制の識別、デザイン、構築、運用とモニタリング
- 「受託会社確認書」の根拠となる Trust サービス分類および関連項目の選択

LINE は、2018 年 1 月 1 日から 12 月 31 までにわたって LINE メッセンジャーサービスシステムの統制が有効であり、サービスおよびシステム要求事項が Trust サービス基準を充足することに対して合理的な保証を提供すると主張します。

LINE 株式会社

LINE 株式会社の LINE メッセンジャーサービスに対するシステム記述書

組織の概要

LINE 株式会社（以下、「当社」という。）は、モバイルメッセンジャーLINE をサービスするインターネットサービス企業です。

当社のサービスは、一般的にスマートフォンアプリケーションおよび PC 版ソフトウェアを通じて提供されます。このようなサービスを提供するために、多様な IT システムとセキュリティ設備、独自に開発したサービス管理システムを使用しています。本システム記述書に含まれるサービスは次の通りです。

- **LINEメッセンジャー**

  LINEの代表サービスとして、1：1トーク、エンドツーエンド暗号化チャット（Letter Sealing）、グループトーク、無料通話（音声通話、ビデオ通話）、画像および動画の共有などの機能をモバイル、PCで提供します。

サービス利用者は、当社のサービスを安全かつ正しく利用するために、利用規約の「お客様の責任」を順守する義務があります。また、お客様ご自身のデータを保護するためにパスワードを定期的に変更し、他人に公開しないなど、一般的にサービス利用者本人がプライバシーのために行うべき活動を認識して実行する必要があります。

インフラストラクチャー

当社は、当社が提供するサービスを利用するためにサービス利用者が入力するデータおよびサービス提供のために処理される全ての情報を重要な情報として取り扱っており、個人情報においては、関連法令に従って定義、識別しています。このように収集および処理される個人情報とそれを処理するシステムを管理するための内部プロセスが整備されており、識別された情報の重要度に応じて、さらに強化された情報保護統制を適用しています。利用者のメッセージングデータの機密保持のためにデータを暗号化しており、退会時の利用者の個人情報は、利用者が同意し、法律上許容される期間内に削除されています。

データ

当社は、サービス利用者が当社から提供されるサービスを利用するために入力するデータとサービス提供のために処理されるすべての情報を重要な情報として取扱っており、個人情報の場合、関連する法規制に沿って定義し、識別しています。そのように収集および処理される個人情報とそれを処理するシステムを管理するための内部手続が定められており、識別された情報の重要度よりも強化した情報セキュリティ統制を適用しています。利用者のメッセージデータの機密保持のためにデータを暗号化しており、退会時の利用者の個人情報は、利用者が同意し、法律で定められている期間内に削除しています。

要員

システムを開発して管理する IT システム関連業務は、サービス提供を行うための主要な機能です。安定したサービスを提供するためにサービスに関連するプログラムを開発する業務と、関連システムを運営する業務を分離しています。サービスを支援、メンテナンス、モニタリング、監督する中心的な業務は次の通りです。

- **サービス企画**

当社が提供する多様なサービスの企画、設計及び運営を担当します。サービスの企画・運営部署は、進行中のサービスの変更及び新規サービスの開発のために、プログラム開発部署、テスト部署、情報保護部署と緊密に協力し、より便利かつ安全なサービスを提供するための取り組みを続けています。

- **開発**

サービスに必要なシステムを開発し、継続的なサービス改善および供給のために関連プログラムのメンテナンスを行い、関連事項を記録・管理します。プログラムの開発および変更は運営環境から分離された開発・テスト環境で行われます。開発担当部署は開発および変更に係る進捗状況や進行中に発生する問題について、グループウェアを通じて継続的なコミュニケーションを行っています。

- **テスト**

開発されたサービスの品質を確認し、改善を要求する業務を担当します。開発が完了したプログラムおよびシステムを顧客サービスに最終的に適用する前に、全ての企画および開発が適切に行われているかを確認します。また、開発されたプログラムおよびシステムに対するテストの結果を検討し、データが問題なく処理されていることを確認します。

- **インフラ運用**

サービスに必要なデータセンターのインフラ構築、ネットワーク、サーバーおよびデータベース運用を担当しており、サービスを円滑に提供するため、各分野の専門家がインフラの設計・構築・運用に取り組んでいます。

- **情報保護**

当社は顧客のプライバシーおよびサービスの安定性のために情報保護組織を運営しています。情報保護担当部署は、全社レベルの情報セキュリティリスク管理と情報保護規程およびポリシーの管理を担当しており、これに対して遵守しているかどうかを周期的にチェックする業務を遂行しています。また、各部署において業務上必要な権限を検討し、定期的にチェックを行い、必要のない権限に対する削除も行っています。

- **ITセキュリティ**

サービス提供のために必要なサーバーシステムと、ハードウェアの運営安定性および継続性を保障するための多様な活動を担当しています。また、セキュリティ専門家が24時間365日体制でお客様のサービス保護に向けたセキュリティオペレーションおよびチェックを実施しています。このために、サービスを脅かす各種のイベントに対してモニタリングし、その結果をもとにインシデント分析、対応、および予防対策などに取り組んでいます。

LINE

可用性

データセンターは火災に備えて、消火設備、警報設備、避難設備を備えています。また、冷房施設および恒温恒湿器を備え、環境の脅威からデータセンターを保護しています。また、停電に備えて非常電力を提供するための UPS（Uninterruptible Power Supply）および非常発電機を備えています。

データセンター内の電力・恒温恒湿・消火・セキュリティ設備に対する環境セキュリティチェックを定期的に実施しています。

サービスデータが保存されたデータベースはクラスタの二重化を通じてリアルタイムでバックアップされているので、データ複製本が常時維持されています。また、クラスタモニタリングシステムを通じてデータベースクラスタおよびサーバーの状態を常時検査してクラスタの二重化が正常に作動しているかをモニタリングしています。

データベースの正常な運用失敗に備えるため、年1回、データベースの可用性分析および対応策を立て、復旧シミュレーションテストを実施しています。

処理のインテグリティ

当社は、システムの開発および変更の際に必要なデータ処理に関するシステム連動構造やデータ構成基準などを識別して管理しています。

データベースのデータは暗号化され保存されているので、直接的な修正が制限されています。また、当社はインフラ統合管理ツールを通じてデータベースサーバーにアクセスしたユーザーの履歴を記録し、モニタリングしています。

当社は、システムデータ処理に関する完全性およびセキュリティを検証するため、システムの開発および変更の際にコードレビュー手続を作って運用しています。

サービスアプリケーションに入力できる入力値の種類と入力値の範囲を定め、システムに実装して入力値を検証しています。また、メッセージ状態コードを設定してメッセージデータのプロセッシングが正常に行われなかった場合、エラーメッセージが表示されるようにしています。

機密保持

- **ポリシー**

  当社は、機密情報の区分、開示の範囲などを定めた機密情報分類表を定義し、社内ツールを通じて分類情報を共有しています。

- **利用、保管および廃棄**

  当社は、機密情報の定義および機密情報別の保管期間を定めたポリシーがあり、保管期間が経過した機密情報を周期的に廃棄しています。また、サービス機密情報に対する保管期間の要求事項を定め、要求事項に従って機密情報を廃棄しています。

LINE

当社は、メールシステムに外部メールへの伝送禁止機能を設定して、機密情報が含まれた電子メールが外部メールに伝送されることを遮断しています。また、メールシステム内で情報等級別に電子メールの保管期間を設定し、設定した保管期間が経過した電子メールはシステムから自動で削除しています。

- **技術的保護措置**

  当社は、インフラ統合管理ツールを通じて開発環境サーバーと運用環境サーバーにアクセスしたユーザーの履歴をログで記録し、モニタリングしています。

  当社は、安全な暗号化通信のための要求事項を定め、要求事項に従って当社の内部システムおよびサービスウェブサイトにSSL（Secure Sockets Layer）認証書を通じて暗号化通信をしています。また、サービスアプリにエンドツーエンドの暗号化（end-to-end encryption）を適用してデータを暗号化し、暗号化キーに対する保護措置を取っており、ディスク暗号化を適用した業務用PCを役員および職員に支給して機密情報が漏えいされるのを防止しています。

- **外部委託先の管理**

  当社は、機密情報漏えい禁止条項を明示した業務委託契約書を外部委託先から受け取っており、個人情報を取り扱う外部委託先との契約時に外部委託先の情報セキュリティ状況をチェックしています。また、年1回、外部委託先の情報セキュリティ状況を更新しています。

  当社は、個人情報の保護に関する法律および当社の機密保持要求事項の変更を周期的に見直し、必要なときは業務委託契約に変更事項を反映させています。

プライバシー

- **告知および伝達**

  当社は、個人情報の管理対象、組織および責任、個人情報の取扱、収集、委託、利用、廃棄およびセキュリティ事項を含んだプライバシー保護に関する全般的な内部ポリシーと手続を、個人情報保護方針に明示しています。また、プライバシーポリシー内に個人情報の収集に対する選択と同意、利用、保有、廃棄、業務委託、セキュリティ事項を明示しています。

  当社は、年 1 回、個人情報保護方針等を定期的に検討してアップデートしています。サービス変更時はプライバシーポリシーを随時にアップデートし、変更されたバージョンは CPO（Chief Privacy Officer）の承認を得ます。また、社内グループウェアを通じて変更された個人情報保護方針等を告知しています。

  当社は、実施中のプライバシー保護活動をサービスウェブサイトおよびモバイルアプリ内のプライバシーポリシーおよび利用規約に告知し、プライバシーポリシーおよび利用規約の変更時にウェブサイトおよびモバイルアプリを通じて告知して、変更されたプライバシーポリシーおよび利用規約をユーザーが閲覧することができるようにします。

LINE

当社は、日本語、韓国語、英語を含む 7 つの言語でプライバシーポリシーおよび利用規約を作成して、サービスウェブサイトおよびモバイルアプリに告知しています。利用規約は日本語を原本とし、プライバシーポリシーは各サービス国の当該プライバシー保護に係るコンプライアンス要求事項に合わせて情報を提供しています。

当社は、ユーザーが提供したもの以外に収集されたクッキーや他の類似トレース技術に関する個人情報の収集の種類および方法と、収集拒否時に制限される内容についてプライバシーポリシーを通じてユーザーに告知しています。

- **選択と同意**

当社は、サービスウェブサイトおよびモバイルアプリに掲示したプライバシーポリシーと利用規約を通じて、ユーザーが個人情報の収集、利用、保有、提供、および廃棄に対して選択的に同意できることを告知しています。

個人情報の選択的収集項目に対する明示およびサービス提供に必要な個人情報の収集に同意しない場合に拒絶する方法についてもプライバシーポリシーおよび利用規約に告知しています。

当社は、サービスを最初に利用するユーザーに、個人情報の収集、利用、保有、提供、および廃棄に対する同意を得ています。

- **収集**

当社は、サービスウェブサイトおよびモバイルアプリに掲示したプライバシーポリシーを通じて、個人情報の収集項目および目的を告知し、サービスユーザーに同意を求めます。また、内部監査を通じて、収集された個人情報が明示された目的でのみ利用されているかを確認します。

当社は、ユーザーから要配慮情報を収集しません。

当社は、サービス提供の目的でクッキーまたは他の類似した電子装置を通じて個人情報を収集する場合、個人情報の収集に関する同意を求めており、拒否した場合にはサービス利用に制限があることを案内します。

- **利用、保存、廃棄**

法規制による強制の場合を除き、個人情報はユーザーの同意を得た目的に限って利用し、年 1 回、内部監査を通じて、収集された個人情報の目的および利用業務を確認します。

当社は、個人情報の保管時、重要な個人情報の場合は暗号化してデータベースに保存して管理しています。

当社は、個人情報の定義および個人情報の類型別の保管期間を定めたポリシーおよび文書を保有しており、保管期間が経過した個人情報を周期的に廃棄しています。また、サービス個人情報に対する保管期間の要求事項を定め、要求事項に従って個人情報を廃棄しています。

LINE

- **アクセス**

  当社は、ユーザーが自分の個人情報にアクセスおよび修正することができる機能を提供しています。ユーザーは、サービスアプリを通じて認証を受けた後、自分の個人情報にアクセスすることができます。

  当社は、カスタマセンターを通じてユーザーが自分の個人情報の確認または変更を要請する場合、ユーザー本人を識別できる情報を検証した後に情報を提供し、自主的に個人情報を変更しません。

  当社は、外部委託先がユーザーの個人情報を外部に共有しないようにし、内部システムを通じてのみ照会するようにします。

- **提供及び通知**

  当社は、個人情報を外部委託先に提供する場合、法規による強制の場合を除き、告知した目的に合わせて内·外的な同意があるときにのみ提供することを、プライバシーポリシーを通じて知らせています。会員登録（サービス利用）の際、事前に個人情報の提供に対する同意を得ています。

  当社は、個人情報の照会に関する記録を残しており、個人情報関連のインシデントや無断伝送などを確認するため、内部情報漏えい防止ソリューションおよびサービス管理システムへのアクセス履歴に対してモニタリングしています。また、インシデント検知および防止システムなどを通じて、サービス運用に脅威を与える可能性のあるセキュリティイベントをモニタリングし、セキュリティイベントの発生時は、定められているイベント別の対応手続、対応レベルに従って対応担当者がセキュリティイベントに対応しています。セキュリティオペレーションモニタリングの結果は、担当者が検討しています。また、セキュリティインシデントの発生時は、インシデント分類対象、対応指揮体制、対応プロセスを定めたインシデント対応マニュアルに従ってインシデントに対応しています。

  当社は、アウトソーシング会社のセキュリティチェックリストを通じて、アウトソーシング会社の職員から機密保持誓約書を受け取るようにし、事象およびインシデントが発生した場合にはアウトソーシング会社から当社に報告するようにしています。

  当社は、個人情報を取り扱うアウトソーシング会社との契約時、アウトソーシング会社の情報セキュリティ現況をチェックしています。また、年 1 回、アウトソーシング会社の情報セキュリティ現況をアップデートしています。

  当社は、インシデント管理規程およびセキュリティインシデント対応指針に個人情報関連のインシデントおよび違反管理事項について記述しています。また、モニタリングを通じて、インシデントが発生したときは、ポリシーに従って処理し、そのインシデントの内容をデータ主体および関連機関に通知し、再発防止策を講じています。

- **品質**

  当社は、ユーザーが正確かつ完全な個人情報を当社に提供しなければならないことや、情報の修正が必要な場合には当社に知らせる責任があることをサービスウェブサイトおよびモバイルアプリの利用規約を通じてユーザーに知らせています。

  当社は、ユーザーの個人データ主体の権利および個人情報の最新性を保障するため、加入および再認証時に携帯電話認証手続を通じて本人であることを実施した後、個人情報の修正ができるように統制しています。

LINE

当社は、サービス変更が発生した場合、ユーザー情報収集項目に対する妥当性を検討して適切な個人情報が収集され、維持されるようにします。また、内部監査を通じて、個人情報の収集項目、目的の適切性に対してチェックし、その結果を代表取締役に報告しています。

- **モニタリング及び執行**

  当社は、個人情報に係るユーザーの問い合わせおよび苦情事項を受け付けることができる手続および機能をユーザーに知らせています。また、ユーザーが提起した意見および苦情事項は、サービスウェブサイトおよびモバイルアプリの問い合わせ機能によって処理することができるようにします。

  当社は、ユーザーの問い合わせおよび苦情事項については、お問い合わせフォームを通じて受け付けており、顧客処理システムを通じてユーザーの問い合わせおよび苦情事項を確認しています。また、必要なときは関連担当者が検討して電子メールを通じてユーザーに回答します。

  法律変更を周期的にモニタリングして、個人情報保護方針等に反映させます。その反映内容は、経営陣および関連責任者の承認を得ます。

  当社は、内部監査を通じて、プライバシーポリシーを遵守しているかどうかや、プライバシーポリシーおよび個人情報保護方針等に対して検討し、その結果を経営陣に報告します。また、必要なときは違反事項に対する校正および懲戒規定を設けて実施しています。