# セキュアプログラミング

2015.08.05

LINEでは、専任組織によるセキュリティ検証の実施等、内外の専門家によるアプリケーションへの脆弱性対策を実施しています。

### セキュリティ・バイ・デザイン

LINEでは、アプリケーション が公開／アップデート する前に様々な専門部署による検証を必ず行っており、そのうちのひとつとして専任のセキュリティチームによるアプリケーションのセキュリティ検証があります。検証内容は以下のとおりです。

**脆弱性検証**

・プログラム検証、自動、または手動による模擬攻撃実施によるセキュリティホール有無の検証

**過剰なパーミッション※の検証**

・アプリケーションが提供する機能に対して、過剰なパーミッションを取得有無の検証

※ここでは、iOSやAndroidOS等に対してアプリケーションが要求する権限を指します。

**セキュリティ設計検証**

・暗号化強度の適切性、第三者によるアカウント乗っ取りやサービス不正行為等の対策の検証

LINEでは、このようにセキュリティ対策をシステムの設計・構築の段階から組み込むことで、セキュリティ・レベルの安定性や拡張性を高め、変化するリスクに柔軟に対応するセキュリティ体制を確立しています。

### 外部専門家との連携と最新の情報収集

LINEでは、セキュリティチームを中心とした組織横断的なインシデントレスポンスチーム（LINE-CSIRT）を構築し、セキュリティに対する事前対策と対処を行っています。また、セキュリティに関する脅威は日進月歩のため、常に外部の最新の情報の入手および連携のため以下の団体に加盟し、継続的な技術動向の把握に取り組んでいます。

日本シーサート協議会：**http://www.nca.gr.jp/member/line-csirt.html**

FIRST：**https://www.first.org/members/teams/line-csirt**

### 脆弱性報告制度の実施

LINEでは、アプリケーションの安全性をより強固にするため、社内だけでなく社外のナレッジも率先して取り入れています。その一環として外部の方がLINEアプリケーションに対する脆弱性を発見した場合に報奨金をお支払いするプログラム「LINE Bug Bounty Program」を実施しています。脆弱性報告制度の詳細は**こちら**をご覧ください。