【コーポレート】LINE、6月9日を「サイバー防災の日」記念日として登録

2017.05.23　コーポレート

インターネット上のトラブルから身を守る“サイバー防災訓練” 初実施

LINE株式会社（本社：東京都新宿区、代表取締役社長：出澤 剛）は、スマートフォンを筆頭にデジタルデバイスが普及した昨今、SNSアカウントの乗っ取りやハッキング、サービスの不正利用などインターネット上のトラブルが増加している背景をふまえ、毎年6月9日を「サイバー防災の日」として一般社団法人日本記念日協会（本部：長野県佐久市、代表理事：加瀬清志）へ申請し、正式に記念日として登録されたことをお知らせいたします。

「サイバー防災の日」は、スマートフォンやパソコンなどを通じてインターネットサービスを安心・安全に利用するために、インターネット上においても防災意識を持つ必要性を喚起する日です。記念日である6月9日は、6と9で“ロック（鍵）”の意味を込めています。

LINEでは、6月9日「サイバー防災の日」を中心に段階的にサイバーセキュリティ啓発施策を展開し、以下の取り組みを予定しています。

1.「セキュリティリテラシー実態調査」を実施（5月）
　・一般約2,000名に対し「セキュリティリテラシー実態調査」を実施
　・本調査結果データから、セキュリティリテラシーの現状と課題を発表

2.「サイバー防災訓練」の実施（6月9日）
　・LINEアプリ内にてサイバートラブルの一例としてLINE乗っ取りを無料疑似体験可能な動画キャンペーンを実施
　・LINE自主メディアにてLINE乗っ取りを含めたサイバーセキュリティ対策を特集
※1．2．詳細については、順次、プレスリリースにてご案内してまいります

LINEは、すべてのユーザーの皆さまのお役に立てるサービスであり続けるため、セキュリティ対策においても、LINEのサービス・インフラを活用した活動等も行ってまいります。また、今後は、本件の趣旨にご賛同いただける企業や各種団体、等との
連携を進め、サイバー犯罪の撲滅を目指してまいります。

ご参考：LINE株式会社のセキュリティに対する主な取り組みについて

LINEは、月間利用者数（MAU）2億人を超えるコミュニケーションアプリ「LINE」をはじめ、幅広いモバイルアプリ・サービスを提供しており、インターネット事業を行う企業の責任としてユーザー情報の保護を最重要視し、積極的に各種情報セキュリティの強化に取り組んでいます。主な取り組みを以下にご紹介いたします。LINEでは、今後も、ユーザーの皆様が、より安心・安全に利用できるサービスを目指し、プライバシー保護やセキュリティ強化に向けた取り組みや体制づくりを積極的に行ってまいります。

未来型インフラに向けた最新トレンドの共有と議論の場を提供
・第1回目「LINE and Intertrust Security Summit: Spring 2017 Tokyo」開催（開催：2017年5月17日）

AI、IoT、Biometricsといったテクノロジーが支える未来型インフラにおいて、信頼あるエンドポイント(Trusted End-point)および信頼あるサービス(Trusted Service)の実現を重要課題の１つであるという共通認識に立ち、LINE株式会社とIntertrust Technologies Corporationは、共同で「LINE and Intertrust Security Summit」を開催しました。本カンファレンスでは「Exploring Technologies for Trusted Apps and Services」というテーマのもと、東京とシリコンバレーにサイエンティストや業界ソートリーダーが一堂に会し、モバイルやIoTが直面するセキュリティおよびプライバシー保護に関わる最先端の研究、技術トレンド、サービス事例などについて討議しました。

FIDO標準の活用による認証の仕組みを提供し、より安全で便利なサービスの実現を目指す
・「FIDO（ファイド）アライアンス」へボードメンバーとして加盟（加盟：2017 年5月17日）
「FIDOアライアンス」＊1は、パスワードレス認証(生体認証、等)の技術仕様、認定仕様等の国際標準化を提唱する非営利団体で、インターネット企業、ソリューションベンダー、金融機関、クレジットカード事業者、通信事業者、などの幅広い業界の企業や団体が活動する国際標準化団体です。「FIDOアライアンス」が提唱する各種技術仕様は、汎用性、互換性、セキュリティが考慮されており、パスワードを入力せずに様々なインターネットサービスを安全で便利に利用することが出来るようになります。「FIDOアライアンス」が提唱する認証方式をLINE及びその他アプリケーションに導入する事によって、現在のパスワード認証に起因するセキュリティまたはプライバシーに関わる様々な問題（フィッシング、アカウント乗っ取り、サービス不正利用など）を解決していくことが期待できます。　＊1： FIDO = Fast IDentity Online

内外の専門家によるアプリケーションへの脆弱性対策
・LINEアプリのセキュリティに関する脆弱性の報告により報奨金を支払う
「LINE Security Bug Bounty Program」（常時運営：2016年6月2日～）
LINEアプリ（iPhone/Android/一部のWEBサイト）において、脆弱性の発見を公募し、LINE株式会社で確認・審査を行い、その内容が認められれば報告者名や脆弱性の概要を弊社公式サイト内の特設ページhttps://bugbounty.linecorp.com/ja/halloffame/ にて順次公表、その新規性・重要度に応じて報奨金を支払います。脆弱性の公表および報奨金の支払いは、該当脆弱性への対応が完了した後に行い、既にLINE株式会社にて把握しているものや他者によって先に発見・報告されているものは審査対象外になります。

ユーザー情報を保護するための取り組み
LINEでは、客観的な視点でユーザー情報保護を評価するため、セキュリティ・プライバシーに関する国際的な外部認証を取得・維持しています。
・内部統制の国際認証Service Organization Control（SOC）2、3取得（取得：2013年～2016年4年連続）
LINEは、個人情報関連サービスに関する内部統制の国際認証SOC（Service Organization Control）2、3（及びSysTrust）を世界で初めて2013年に同時取得したのに続き、2014年以降も毎年取得。LINEにおける内部統制および個人情報保護が国際基準を満たし、LINEは信頼できる優良サービスであることが改めて認められました。SOC2、SOC3認証は、顧客情報が第三者による不正アクセスから安全に保護されていることを証明するものであり、提供するサービスそのものの安全性だけでなく、運営する組織、管理システム、プロセスなど、総合的な内部統制について、ユーザーにサービスの信頼性を保証するものです。
＜SOC2およびSOC3認証とは＞
米国公認会計士協会（AICPA）とカナダ勅許会計士協会（CICA）が制定したTrustサービス原則（Trust Services Principles and Criteria）に準拠して、外部の監査機関が(1)サービスのセキュリティ性、(2)可用性、(3)処理の整合性、(4)機密性、(5)個人情報保護の5原則を基準に、合計127の領域において、監査を通じて提供するサービスの業務プロセスと統制環境が基準を満たしているかを検証し、該当基準を満たした場合にのみ取得可能な保証報告書です。

・ISO27001認証取得（取得：2007年1月10日）
LINE株式会社及び主要子会社では、国際的に最も広く活用されている情報セキュリティマネジメントシステム（ISMS）の国際規格である、ISO27001認証を取得しています。
＜ISO27001認証とは＞
JIS Q 27001（ISO/IEC 27001）は、組織が自社で保護すべき情報資産を洗い出し、各情報資産に対して機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）をバランスよく維持し、改善していくことを可能にする仕組みを
構築することを目的とした規格です。
