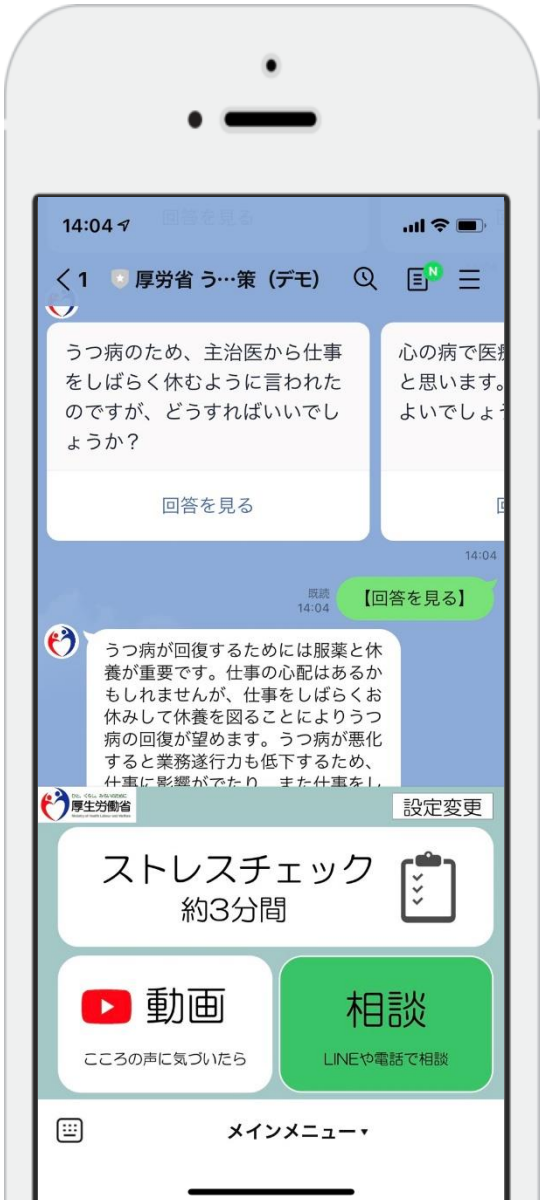
KOMEITO
公明党

厚労省うつ対策 LINE内アプリ （デモ版）

スマホで
お試しください →



機能①

厚労省
ストレス
チェック

機能②

動画
厚労省動画


14:04
厚労省 う…策（デモ）
もあてはまるものにチェックを付けてください。
回答する
14:04
厚生労働省 動画
こころのサインに気づいたら①
一般編
こころの悩みに気づいて…
悩んでいる人が安心する…
14:04
厚生労働省
設定変更
ストレスチェック
約3分間
動画
こころの声に気づいたら
相談
LINEや電話で相談
メインメニュー


14:05
厚労省 う…策（デモ）
もあてはまるものにチェックを付けてください。
こころのサインに気づいたら②（…
m.youtube.com
YouTube
ログイン
こころのサインに気づいたら②（2）家族編
1559 回視聴
高評価
低評価
共有
保存
報告
厚生労働省 / MHLWchannel
チャンネル登録者数 5.21万人
チャンネル登録
次の動画
自動再生
自殺
考えている人を見分ける
14の方法
【心理】自殺を考えている人を見分ける14の方法【アニメーション】
サイコ2ゴージャパン

機能③

相談

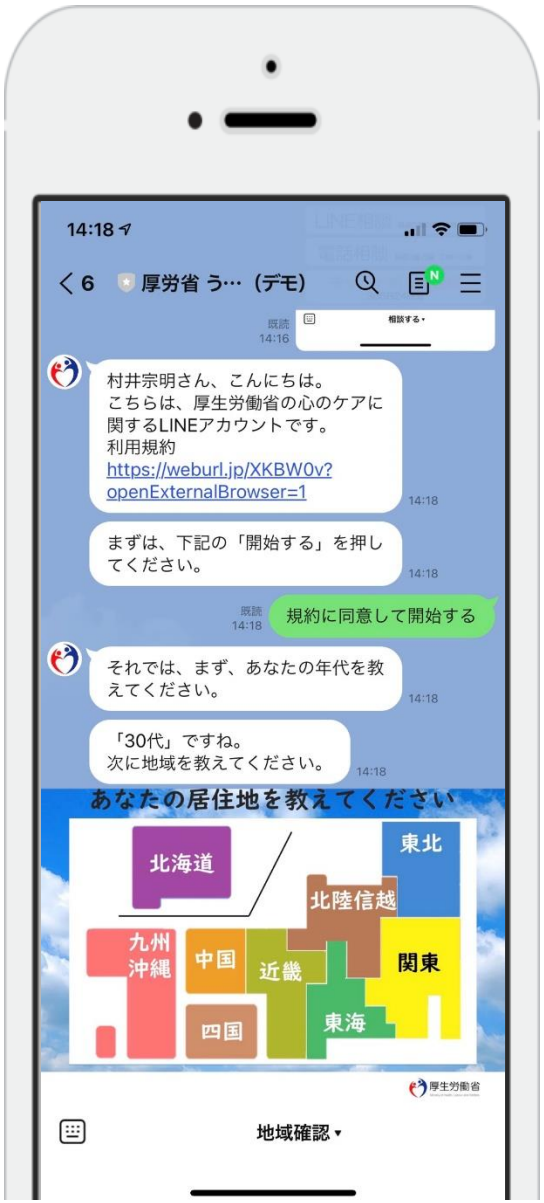
- 電話相談
- LINE相談
- AIチャットボット相談

機能④

情報発信

- 年代別
- 地域別

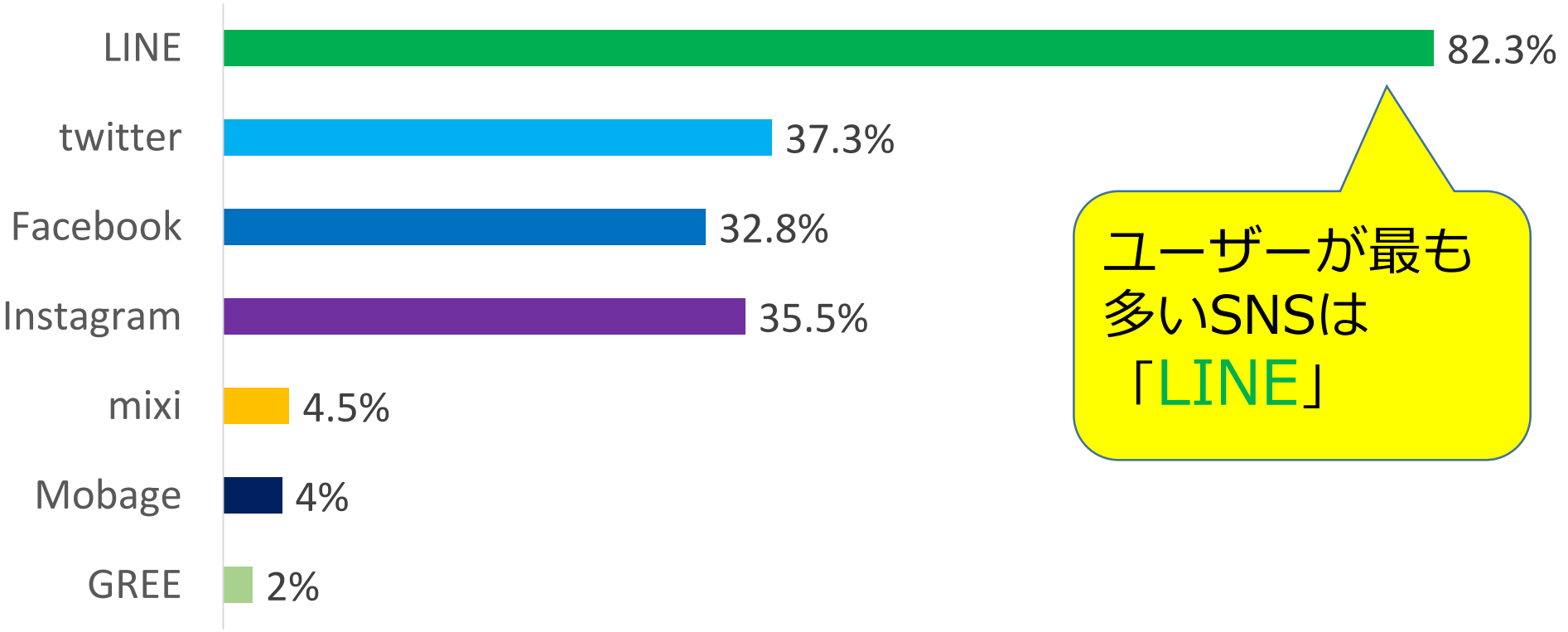
LINEでの一斉配信



参考資料

国内SNSのユーザー数　（総務省統計）

平成30年　全世代(N=1500)



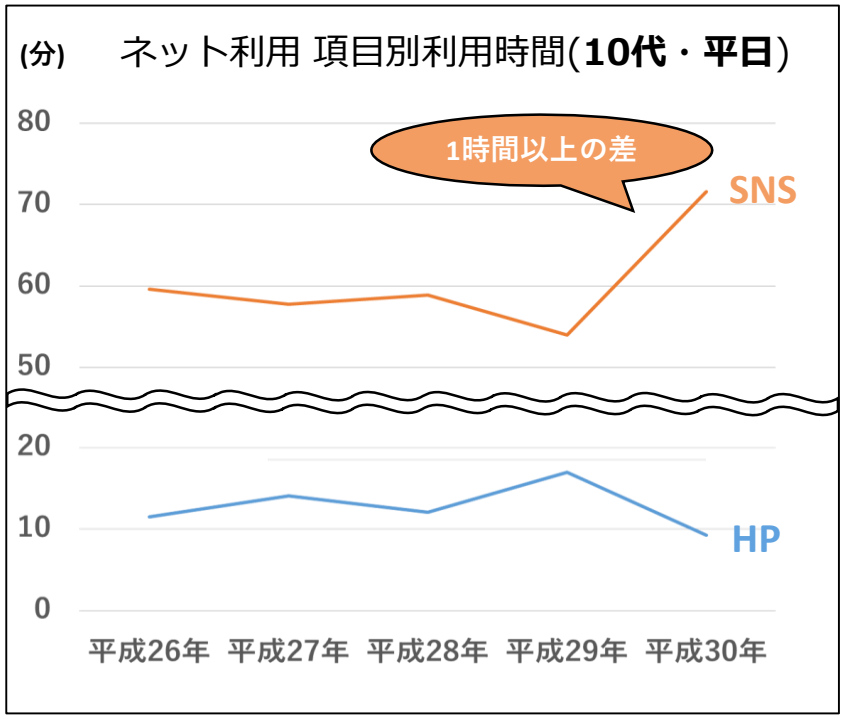
ユーザーが最も多いSNSは「LINE」

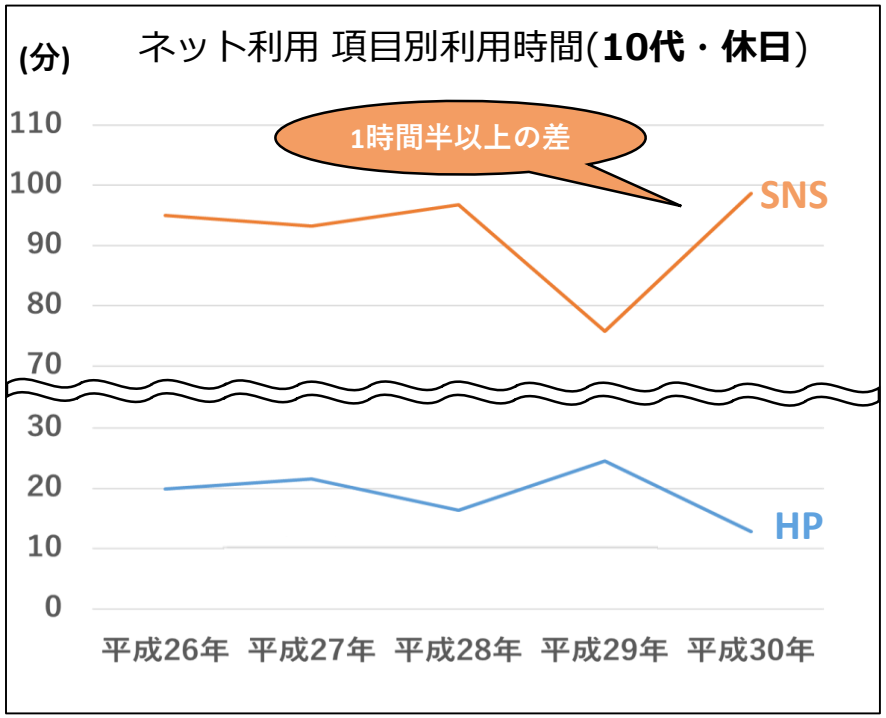
総務省　平成30年度情報通信メディアの利用時間と情報行動に関する調査報告書概要 15Pより引用
https://www.soumu.go.jp/main_content/000644166.pdf

デジタル化 成功のポイントは、国民の「HPからSNSへ」の変化に対応する事

①１０代

10代のネット利用の時間は、**圧倒的にSNSの利用時間が多い。**
パソコンを持たず、スマートフォンのみの利用者も多く、
顕著に利用時間の差が開いていく。



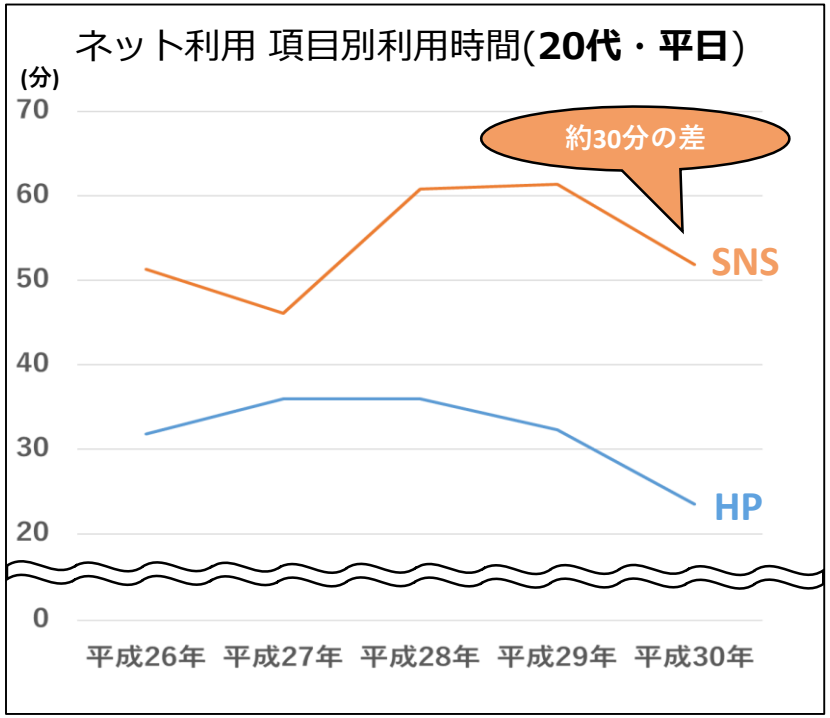


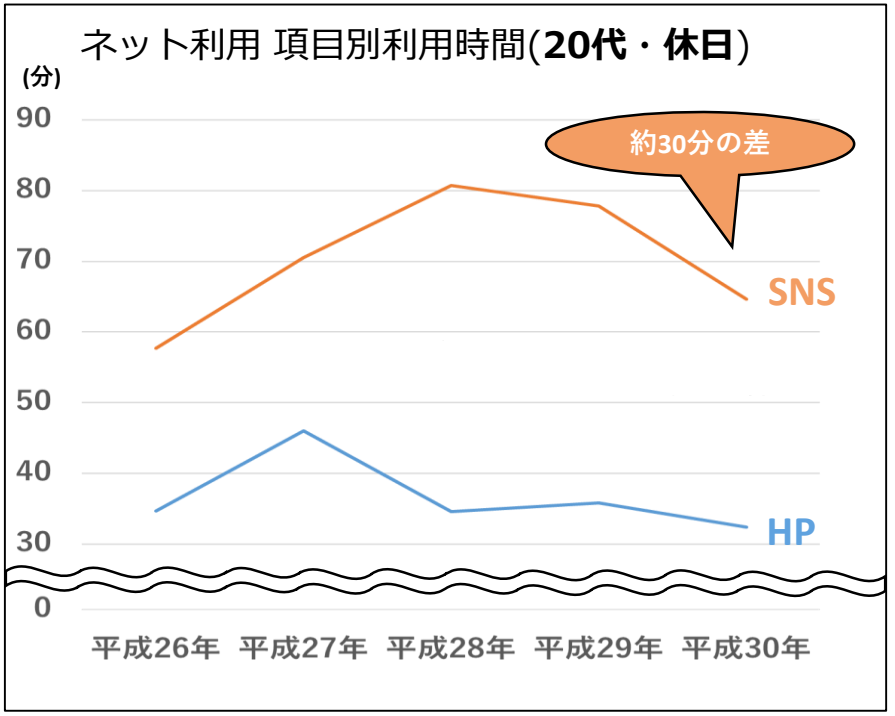
参考：**総務省**「情報通信メディアの利用時間と情報行動に関する調査(平成26年～30年)」
https://www.soumu.go.jp/iicp/research/results/media_usage-time.html

デジタル化 成功のポイントは、国民の「HPからSNSへ」の変化に対応する事

②２０代

20代のネット利用の時間は、**SNSの利用時間が多い**。
今後は、**子育て世代**においても**SNSが主要な情報収集のツール**となる。



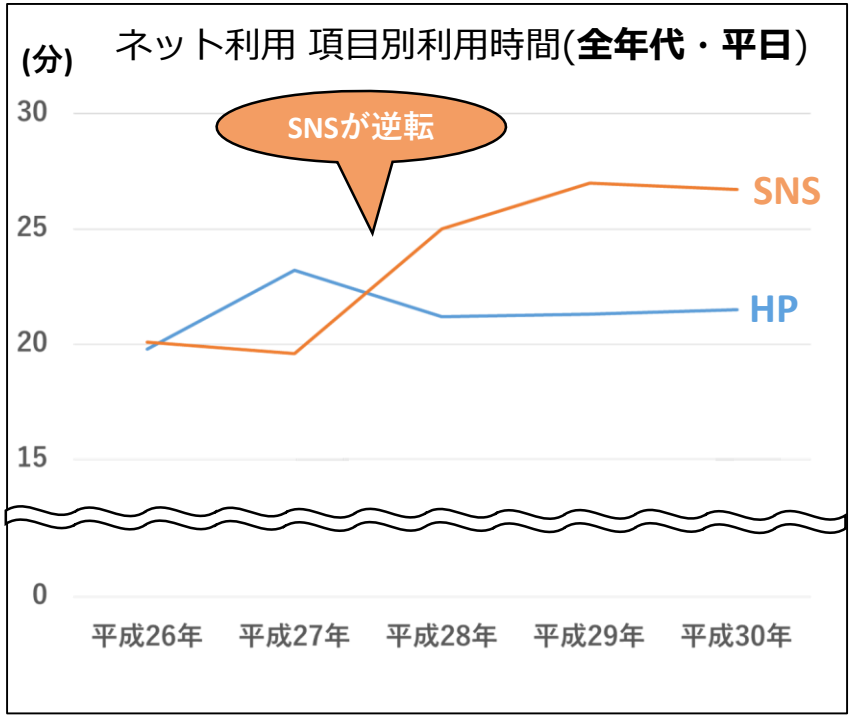


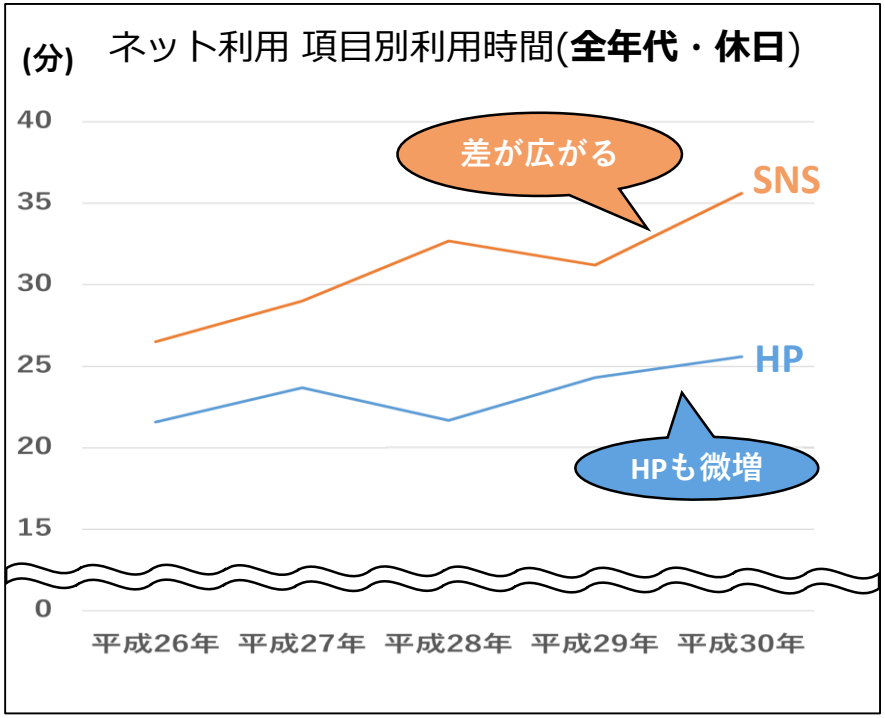
参考：**総務省**「情報通信メディアの利用時間と情報行動に関する調査(平成26年～30年)」
https://www.soumu.go.jp/iicp/research/results/media_usage-time.html

デジタル化 成功のポイントは、国民の「HPからSNSへ」の変化に対応する事

③全世代

ネット利用の時間は、毎年ホームページより**SNSの利用時間が増加**している。
若者に限らず**全年代に当てはまる事象**であり、今後**更に利用時間の差が開く**と推測。





参考：**総務省**「情報通信メディアの利用時間と情報行動に関する調査(平成26年～30年)」
https://www.soumu.go.jp/iicp/research/results/media_usage-time.html

LINEのセキュリティ　①「LINE」を支える環境

「LINE」を運営するLINE株式会社は日本に本社を置く企業であり、日本国の法規法令に則りユーザーの個人情報を管理しています。また、「LINE」で提供するメッセージ通信サービスは「電気通信事業」に該当し、当社は総務省に対し電気通信事業者として届け出ております。通信内容については「通信の秘密」として厳格なルールを設けて保護しております。

日本の最先端のデータセンター

「LINE」の個人情報を取り扱う主要なサーバーは、2018年10月現在、日本のデータセンターで管理しています。このデータセンターでは世界最高水準のセキュリティ設備を組み込んでいます。

厳格なアクセス管理

データセンター内では、警備員による常時監視やICカード及び生体認証での入退制限、監視カメラでのモニタリング等が行われています。同データセンターは厳格なアクセス統制を行い、LINE社内でも最低限の人員のみアクセスが許可されます。合理的な理由に基づく事前許可が無い場合、アクセスが許可されることはありません。

セキュリティ監視

専任のセキュリティチームがデータセンター内で24時間365日物理的、論理的な監視を行っています。このセキュリティチームはネットワーク上のトラフィックを常時監視し、LINEの安全性を脅かす可能性のある全ての動きの分析を実施し、即座に必要な対応を行います。

責任者と専門組織

CPO（最高プライバシー責任者）およびCISO（最高情報セキュリティ責任者）を任命し、組織におけるプライバシー保護やセキュリティ対策の責任と権限を明確化しています。CPOおよびCISOはCEO等の他の経営陣を含めた社内委員会を運営し、LINEのプライバシー保護やセキュリティ対策に係る方針を決定し、施策の実行状況のモニタリングや評価を行うとともに、情報事故の予防と発生時の対応を行います。

また、これらの方針の実働部隊として、当社ではITセキュリティや情報セキュリティ、政策や法務など、さまざまな部門における専門家による組織横断的な社内委員会を構成しています。これらの組織ではそれぞれの専門分野におけるプライバシー保護やセキュリティ対策を行うとともに、トレンドの把握・調査や、業務の現場からみえてくる潜在的な問題の把握を通して改善の提議・提案等を担当しています。

その他、技術的なセキュリティ対策、戦略、情報の取扱い、運用監視など、各分野において専門スタッフで構成される専任組織を構成し、より安全なサービスの実現を目指しております。

LINEのセキュリティ　②「LINE」のプライバシー保護やセキュリティ対策

LINEではプライバシー保護やセキュリティ対策を徹底するため、技術的なセキュリティを検証する専門組織や、個人情報保護法や電気通信事業法などの適用される法律の遵守状況を確認する専門組織を設置しています。サービスを公開するにあたっては設計や構築の段階からこれらの専門組織が関与し、高いプライバシー保護や安定したセキュリティ水準を提供し、変化するリスクに柔軟に対応する体制やプロセスを確立しています。

セキュリティ設計

LINEでは、サービスを公開/アップデートする前に専任のセキュリティチームによる徹底したセキュリティ検証を行っています。これには、暗号化強度の適切性の確認や第三者によるアカウント乗っ取りなどへの対策状況の検証、サービスが提供する機能に対して過剰なパーミッションを取得していないかの検証などが含まれます。また、「LINE」の安全性を担保するため、セキュリティチームや外部企業による定期的な模擬ハッキングを実施しています。これによりセキュリティホールの有無を検証し、社内外からの不正アクセスへの予防対策を行っています。

プライバシー設計

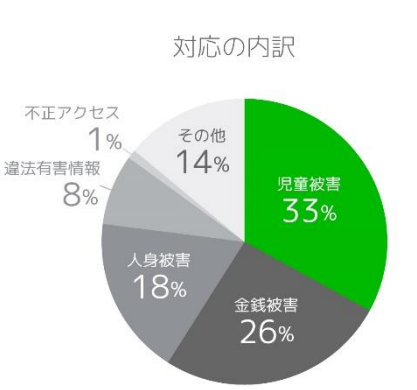
LINEで提供されるサービスは全て法務担当部門及び個人情報保護担当部門による審査を経ない限り公開されることはありません。取得する個人情報が必要最低限であること、利用目的の適切性、取得プロセスの適切性、重要情報の暗号化や保存期間の適切性、アクセス制御の適切性等の観点から確認や検証を行い、必要な場合の改善指示を行っています。

廃棄

LINEが取得した個人情報は、退会時などプライバシーポリシーに明記した利用目的達成後に社内規定に従って削除されます。削除は復号不可能な方法で行われ、サーバー廃棄時は廃棄IDC内にて物理破壊を行い、データ復元が不可能な状態にして廃棄しています。

透明性報告書

LINEはユーザーの許可なく第三者にユーザーの情報を提供することは原則ありませんが、例外として捜査機関による犯罪捜査のため、情報開示請求に応じることがあります。捜査機関から情報開示の要請を受領した場合、関係法令に基づいて開示することが適切と判断される状況と範囲に限り、当社では捜査に必要な情報を提供する場合があります。当社では2016年7月以降、捜査機関の開示請求に応じた件数を公開しております。



出典：LINE Transparency Report 2018.10.16版
https://linecorp.com/ja/security/transparency/2018h1

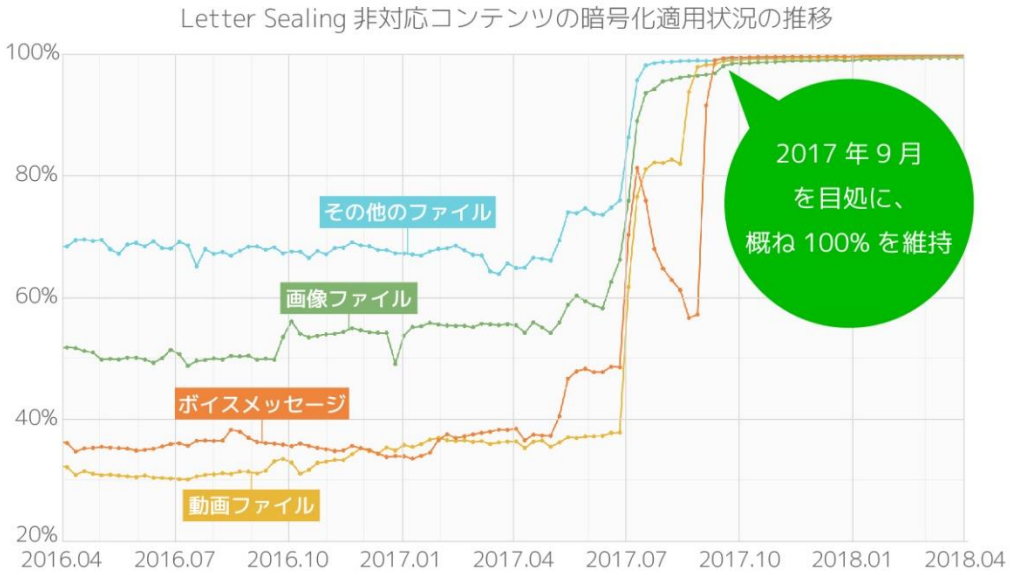
LINEのセキュリティ　③トーク内容の暗号化対策

LINEではユーザ間のトークにおいて通信経路での暗号化を実施しています。ユーザ間のトーク内容のうち、テキストメッセージ、位置情報、1対1のVoIPのメディアストリーム(音声とビデオ）は、Letter Sealing エンドツーエンド暗号化 (end-to-end encryption, E2EE)を用いてデフォルトで暗号化されています。Letter Sealing は、第三者のみならず当社のサーバー管理者であっても、通信上及びサーバー上でのメッセージ内容を閲覧することは出来ないことを保証します。通信経路の暗号化とLetter Sealing は、標準的な暗号化アルゴリズムを採用しています。

また、LINEのユーザー情報のうち、当社の定める主要な個人情報（電話番号、メールアドレス、パスワード等）は全て暗号化の上保管され、その管理状況を定期的に点検しています。

暗号化状況	2015年	2016年	2017年9月	2018年4月
テキスト	○	○→◎	◎	◎
位置情報	○	○→◎	◎	◎
スタンプ	△	△	○	○
画像ファイル	△	△	○	○
ボイスメッセージ	×	×	○	○
動画ファイル	×	×	○	○
その他のファイル	△	△	○	○
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	ー	○	○	○

凡例
- ◎ デフォルトでLetter Sealing暗号化が適用されている
- ○ 通信経路上での暗号化あり
- △ 部分的な保護
- × 暗号化無し or 不十分な暗号化
- ー 機能未実装



出典：LINE 暗号化状況レポート　2018.04.24版
https://linecorp.com/ja/security/encryption_report

LINEのセキュリティ　④外部との連携

LINEでは、プライバシー保護やセキュリティ対策に対して客観的な評価を確認したり、設計に外部の知見を取り入れたりするため、外部専門家と積極的な連携を図っています。

外部審査団体による客観的なセキュリティ評価

LINEでは、ユーザー情報を保護するための取り組みを内部ポリシーとして厳格に定め運用しており、客観的な視点でこれを評価するため、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。
LINEおよび主要子会社では、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認証を取得しております。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。
また、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（およびSysTrust）を世界で初めて同時に取得しています。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。

外部知見の取り入れ

LINEは、FIDO、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「FIDO（ファイド）アライアンス」へ、2017年5月17日よりボードメンバーとして加盟しています。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しています。

バグ報奨金制度

「LINE」および当社サービスに存在する脆弱性（バグ）を早期に発見し、ユーザーに、より安全なサービスを提供することを目的としたプログラム「LINE Bug Bounty」を常設しています。外部のセキュリティ専門家（バグハンター）が当社サービス内でバグを見つけ報告頂いた場合、「賞金」をお支払いするバグ報奨金制度を設けています。このプログラムを通じ今までに116件の脆弱性報告について、累計で205,500ドル支払っています。

支払った報奨金	報奨金対象の脆弱性件数	報奨金対象者の国数	参加者
205,500 ドル	116 件	21 カ国	283 人