

中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）関連資料

設定解説資料 （LINE）

ver1.1 (2024.03)

本書は、総務省の調査研究事業により作成したものです。

本書に関する問い合わせ先（個別のシステムおよび環境に関する御質問については、製品の開発元にお問い合わせください。）

総務省 サイバーセキュリティ統括官室

Email telework-security@ml.soumu.go.jp

URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

目次

1 はじめに	3
2 チェックリスト項目に対応する設定作業一覧	4
3 利用者向け作業	5
3-1 チェックリスト 3-1 への対応	5
3-1-1 グループトークの設定.....	5
3-2 チェックリスト 6-1 への対応	14
3-2-1 Letter Sealing 機能の有効化	14
3-3 チェックリスト 9-1 への対応	19
3-3-1 パスコードロックの設定.....	19
3-3-2 LINE アプリからのみのログイン許可設定	21

1 はじめに

（ア）本書の目的

本書は、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目について、LINE を利用しての具体的な作業内容の解説をすることで、管理者が実施すべき設定作業や利用者が利用時に実施すべき作業の理解を助けることを目的としています。

（イ）前提条件

LINE を利用する場合には「iOS 用アプリ」「Android 用アプリ」「PC 利用」等の利用方法があります。**本資料では「iOS 用アプリ」「Android 用アプリ」の利用を前提としています。**

（ウ）本書の活用方法

本書は、中小企業のセキュリティ管理担当者やシステム管理担当者（これらに準ずる役割を担っている方を含みます）を対象として、その方々がチェックリスト項目の具体的な対策を把握できるよう、第 2 章ではチェックリスト項目に紐づけて解説内容と解説ページを記載しています。本書では第 3 章にて利用者向けに設定手順や注意事項を記載しています。

表 1. 本書の全体構成

章題	概要
1 はじめに	本書を活用するための、目的、本書の前提条件、活用方法、免責事項を説明しています。
2 チェックリスト項目と設定解説の対応表	本書で解説するチェックリスト項目と、その項目に対応する設定作業手順および注意事項の解説が記載されたページを記載しています。
3 利用者向け作業	対象のチェックリスト項目に対する利用者向けの設定手順や注意事項を解説しています。

（エ）免責事項

本資料は現状有姿でご利用様に提供するものであり、明示であると黙示であるとを問わず、正確性、商品性、有用性、ご利用様の特定の目的に対する適合性を含むその他の保証を一切行つものではありません。本資料に掲載されている情報は、2023 年 11 月 7 日時点の各製品の操作画面を基に作成しており、その後の製品仕様の更新、追加、変更、削除もしくは部分改廃により、画面表示等に差異が生じる可能性があります。本資料は、初期出荷状態の製品を単体動作させている環境を利用して設定手順を解説しています。本製品をご利用様の業務環境で利用する際には、本資料に掲載している設定により業務環境システムに影響がないかをご利用様の責任にて確認の上、実施するようにしてください。本資料に掲載されている製品仕様・設定方法について不明点がありましたら、製品提供元へお問い合わせください。

2 チェックリスト項目に対応する設定作業一覧

本書で解説しているチェックリスト項目、対応する設定作業解説および注意事項が記載されているページは下記のとおりです。

表 2. チェックリスト項目と利用者向け設定作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
3-1 アクセス制御・認可 許可された人のみが重要情報を利用できるよう、システムによるアクセス制御やファイルに対するパスワード設定等を行う。	・ グループトークの設定	P.5
6-1 通信暗号化 Web メール、チャット、オンライン会議、クラウドストレージ等のクラウドサービスを利用する場合（特に ID・パスワード等の入力を求められる場合）は、暗号化された HTTPS 通信であること、接続先の URL が正しいことを確認するよう周知する。	・ Letter Sealing 機能の有効化	P.14
9-1 アカウント・認証管理 テレワーク端末のログインアカウントや、テレワークで利用する各システムのパスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また、可能な限りパスワード強度の設定を強制する。	・ パスコードロックの設定 ・ LINE アプリからのみのログイン許可設定	P.19 P.21

3 利用者向け作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第2部に記載されているチェックリスト項目のうち、本製品の利用者が実施すべき対策の設定手順や注意事項を記載します。

3-1 チェックリスト 3-1 への対応

3-1-1 グループトークの設定

LINEにて指定されたメンバー間のみに限定して情報を共有する方法として、「グループトーク」があります。この「グループトーク」を利用することで、指定されたメンバー間でのみの情報共有が可能です。「グループトーク」ではグループメンバーとして指定されたメンバーによる参加承認が求められます。本項では、情報共有を必要なメンバーに限定した運用が容易と考えられる「グループトーク」の利用を推奨設定とし、「グループトーク」の作成方法を記載します。

グループトークの作成－方法①ホーム画面-グループからの作成

【手順①】

ホーム画面より「グループ」を選択後、「グループ作成」を選択します。



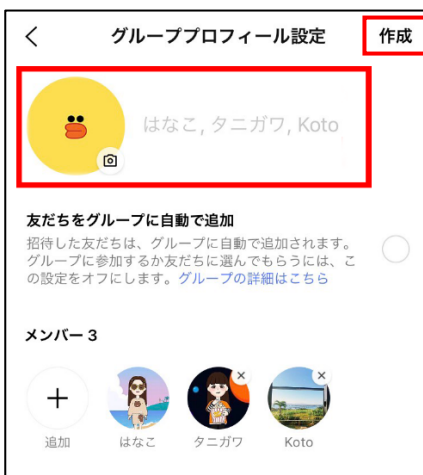
【手順②】

参加メンバー（追加したい友だち）を選択し、画面右上「次へ」を選択します。



【手順④】

「グループ名」にグループの名前を入力し、画面右上「作成」を選択します。



グループトークの作成－方法②トーク画面－トークルームでの作成

【手順①】

ホーム画面より「トーク」を選択し、画面右上「トークルーム作成アイコン」を選択します。



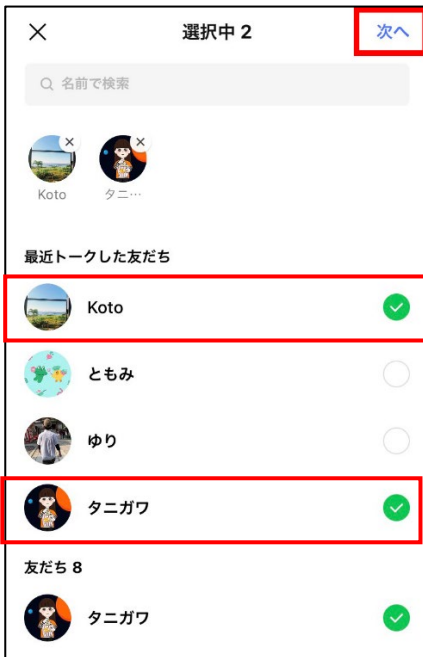
【手順②】

「グループ」を選択します。



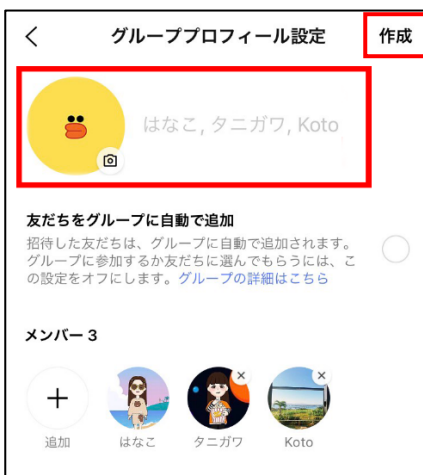
【手順③】

追加したい友だちを選択して、画面右上「次へ」を選択します。



【手順④】

「グループ名」にグループの名前を入力して、画面右上「作成」を選択します。

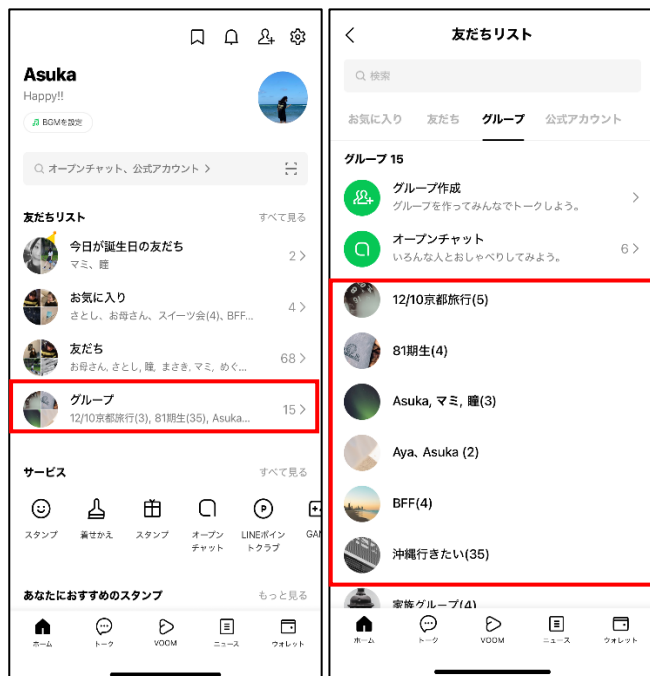


グループメンバーの追加

作成した「グループ」にメンバーを追加する手順を記載します。

【手順①】

ホーム画面の「グループ」より、メンバーの変更を行うグループを選択します。



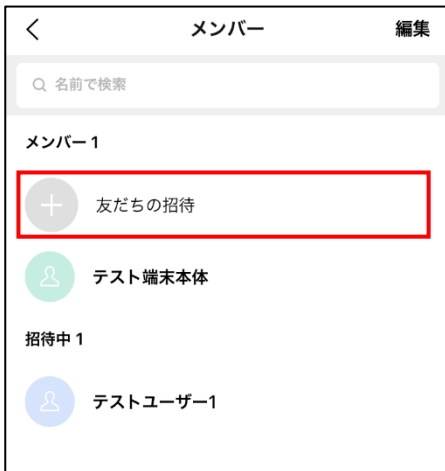
【手順②】

「設定（歯車ボタン）」を選択し、「メンバーリスト・招待」を選択します。



【手順③】

「友達の招待」を選択します。



【手順④】

「追加するメンバー（友だち）」を選択して「招待」を選択します。

招待されたメンバー側にて「参加」を行うことでメンバーとして追加されます。

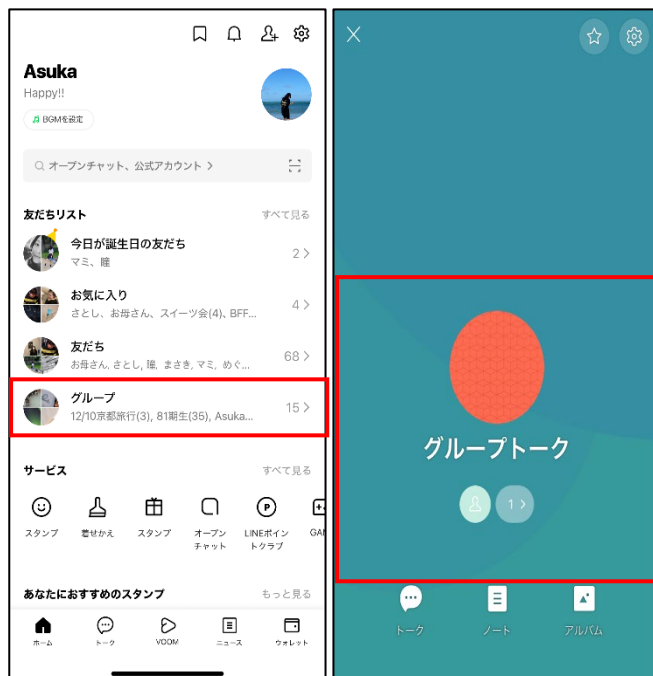


グループメンバーの削除

作成した「グループ」からメンバーを削除する手順を記載します。

【手順①】

ホーム画面の「グループ」より、メンバーの変更を行うグループを選択します。



【手順②】

「設定（歯車ボタン）」を選択し、「メンバーリスト・招待」を選択します。



【手順③】

「編集」を選択します。



【手順④】

削除するメンバーを選択して「削除ボタン」を選択します。

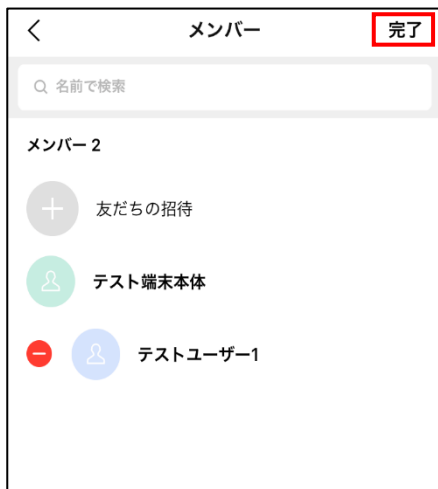


本当に削除するか確認画面にて「削除」を選択します。



【手順⑤】

「完了」を選択します。



3-2 チェックリスト 6-1 への対応

3-2-1 Letter Sealing 機能の有効化

LINE では、LINE クライアントとサーバー間の通信を保護する通信レイヤーの暗号化（LEGY 暗号、HTTPS）に加え、メッセージ通信を暗号化する Letter Sealing という機能が提供されています。この機能を有効化しておくことによって、**通信内容を盗み見られ、情報漏洩するリスクを低減することができます。**

初期設定においては、Letter Sealing は既に適用されている状態であるため、本項では本機能設定の確認手順、およびオフになっている場合にオンにする手順を記載します。なお、Letter Sealing は自身の設定だけでなく、やり取りをする相手も設定をオンしている場合のみ有効となるため、トーク相手の設定確認手順も合わせて記載します。

なお、Letter Sealing 機能は 50 名以下のグループのみに適用されます。

Letter Sealing 設定の有効化確認

【手順①】

ホーム画面より画面右上「設定アイコン」を選択します。



【手順②】

「プライバシー管理」を選択します。



【手順③】

「Letter Sealing」がオン（チェックマークが記載）になっていることを確認します。チェックが入っていない場合、チェックを入れ、有効化します。



トーク相手との通信の暗号化確認

トーク相手の Letter Sealing 設定が有効になっていることを確認します。本手順は、上記「Letter Sealing 設定の有効化確認」手順からの継続手順です。

【手順④】

「トーク」画面より送信する相手を選択します。



【手順⑤】

画面右上「メニュー」アイコンを選択します。



【手順⑥】

「このトークルームでは Letter Sealing が適用されています」をタップします。



【手順⑦】

暗号キー情報が表示されていることを確認します。



【手順⑧】

下図のように「このトークルームでは Letter Sealing が適用されています」の表示がない場合、相手の Letter Sealing が設定されていないため、相手側にも Letter Sealing を適用するように依頼をしてください。



3-3 チェックリスト 9-1 への対応

LINE の利用を制限する方法として、「パスコード」と「パスワード」による制限の 2 種類が存在します。

「パスコード」は、スマートフォン等にインストールする LINE アプリの利用時に入力を求められるパスワードで、第 3 者が LINE アプリを起動することを防ぐためのものです。

一方、LINE アカウントの「パスワード」は、パソコン等でブラウザから LINE を利用する際やスマートフォン端末を変更した場合に LINE アカウントを引き継ぐ際などに、メールアドレスと共に入力が求められるパスワードで、端末を問わず LINE アカウントにログインしようとしている人が確実に本人であることを認証するためのものです。

なお、メールアドレスと LINE アカウントの「パスワード」による設定について、LINE アカウントの「パスワード」は LINE アカウントの新規登録時に設定が必須となっていますが、「パスコードロック」は、初期状態では設定されていません。

本書では「パスコードロック」と LINE アカウント「パスワード」のそれぞれの設定方法と、他のデバイスから LINE にログインを許可/不許可をする設定を記載します。

3-3-1 パスコードロックの設定

パスコードロックを設定することにより、悪意のある第三者に LINE アプリを起動され悪用されるリスクを低減することができます。

【手順①】

ホーム画面より画面右上「設定アイコン」を選択します。



【手順②】

「プライバシー管理」を選択します。



【手順③】

「パスコードロック」を選択します。



【手順④】

設定したいパスコードを設定します。（4桁の数字固定）



3-3-2 LINE アプリからのみのログイン許可設定

本設定を行うことにより、設定した端末の LINE アプリからのみ LINE が利用可能となります。他の端末からだけでなく、端末のブラウザからも LINE を利用できなくなります。この設定により、悪意のある第三者に LINE アカウントのなりすまされるリスクを低減することができます。

【手順①】

ホーム画面より画面右上「設定アイコン」を選択します。



【手順②】

「アカウント」を選択します。



【手順③】

「ログイン許可」を「オフ」に設定します。

