LINE WORKS

Security System Guide

セキュリティシステムガイド

VER.3.9.0

line.worksmobile.com

国際認証の取得

LINE WORKS サービスは、厳格な審査規準が設けられた以下の国際認証を取得し、安全に運用されています。

ISO/IEC27001, 27017, 27018

情報資産の機密性(Confidential)、完全性(Integrity)、可用性(Availability)を確保・改善維持するシステムの確立のため、国際標準化機構（ISO）が制定した情報セキュリティ・マネジメントシステムに関する国際規格であり、各認証における規定内容は以下である。

ISO/IEC27001

組織の情報セキュリティ・マネジメントシステムを第三者認証するための要求規格

ISO/IEC27017

クラウドコンピューティングサービスの情報セキュリティマネジメント制御の実践のための規範

ISO/IEC27018

クラウドコンピューティングサービスの、データ（個人情報を含む）保護制御の実践のための規範

SOC2/SOC 3 (SysTrust)

情報システムの信頼性について公認会計士が保証を与えるにあたり、米国公認会計士協会とカナダ勅許会計士協会が定めた規格であり、日本においても、日本公認会計士協会が本規格の提供に関するライセンス契約を締結している。本規格への準拠性について、外部監査機関による監査を通じて検証し、該当基準をすべて満たす場合にのみ付与される。

SysTrust の検証では、以下の４つの必須原則に照らして、システムの信頼性を測定する。

可用性（Availability）/安全性（Security）/完全性（Integrity）/維持性（Maintainability）

インフラシステムのセキュリティ

データセンター

ファシリティー/システムの耐久性

LINE WORKS のデータセンターは、最新の物理セキュリティを備え、
想定できる様々な災害等の状況にも耐え得る堅牢な建物と、システム構成を採用しています。
また、多重構造によるデータ保護にて安全にバックアップを行ない、国際認証を取得した高いレベルの情報管理システムとワークフローにてサービスを提供しています。

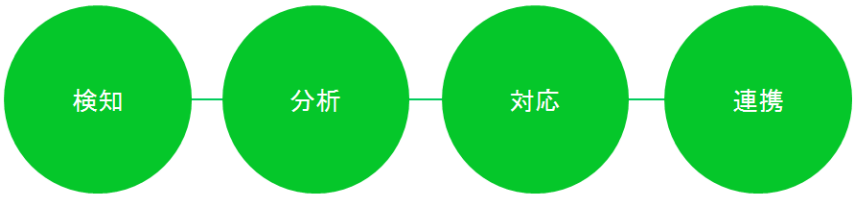
物理セキュリティ

データセンターの出入は、必要最小限の人員にのみ許可されており、認証スタッフ以外のデータセンターへの立ち入りは一切許可しておりません。
また、非認可アクセス、非認可資料の利用防止と監査はもちろん、データベースへのアクセスも別途承認を得たスタッフのみアクセス可能な経路に限定されており、情報利用の際には、それらの参照、照会、およびダウンロードの全てログ記録と監査を行なっています。

サービスシステム

情報セキュリティ

サービスのインフラは、他のコンシューマー向けサービスとは分離した環境で運用されており、
セキュリティ専門スタッフによる 24×7 の体制で、365 日すべてのアクセスをモニタリングしています。
リアルタイムでのウィルス検知、トレンドに合わせたマルウェア対策とスパムフィルタリングはもちろん、DoS・DDoS 攻撃に代表される外部からの脅威も常時監査され、セキュリティリスクを検知した場合には、それらの分析、対応、またその再発防止に向けた情報共有と必要な機関との連携を迅速に行っています。



なお、システムの点検では、SQL インジェクション、クロスサイトスクリプティング(XSS)、クロスサイトリクエストフォージェリ(CSRF)等の脆弱性、認証・セッション管理の脆弱性に対する様々なテスト、さらに専用のセキュリティ診断ツールを用いた自動診断と、チェックリストを用いた手動診断を並行して実施し、高いセキュリティレベルの維持に努めています。

セキュリティ機能の紹介

アカウント・アクセス

パスワードポリシーの設定 [管理者機能]

セキュリティ ＞ アカウント管理

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

各メンバーが LINE WORKS サービスへログインする際のパスワードは、難易度や有効期限など、
各企業のセキュリティポリシーに沿って設定が可能です。

パスワードの難易度	半角英数字 半角英数字と特殊文字の組み合わせ
パスワードの長さ	８～20 文字
パスワードの有効期限	制限なし、30 日、60 日、90 日、180 日、365 日
パスワードの再使用禁止	制限なし、 最近使ったパスワード 1 個まで使用不可（1～5 回で設定可能）
ログイン失敗時の アカウント一時停止	制限なし、 3 回連続で失敗した場合、アカウントを一時停止（3～10 回で設定可能）

2 段階認証ログイン [全メンバー対象]

環境設定 ＞ 2 段階認証

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

LINE WORKS サービスへのログインに、携帯番号または個人メールアドレスを使った 2 段階認証を設定できます。管理者は本機能のメンバー利用を「必須」または「選択」から設定します。

メンバーのパスワード変更 [管理者機能]

メンバー ＞ メンバー情報 ＞ セキュリティ設定

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

各メンバーのパスワードは、管理者により変更可能です。（各メンバーが設定したパスワードは確認不可）
パスワード情報やデバイス自体の紛失等の場合にも、アカウントを停止・削除することなく、不正アクセスのリスクを低減できます。

ID/パスワード確認時における本人認証 [全メンバー対象]

ログイン ＞ ID･パスワードの確認

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

第三者による不正な ID・パスワード確認のリスク対策として、LINE WORKS へのログイン ID・パスワードを忘れた場合の確認作業では、認証番号を用いた本人確認を採用しています。
認証番号はメンバー情報として登録されている電話番号、もしくはメールアドレスでのみ受取が可能です。

IP アドレス接続制限 [管理者機能]

セキュリティ ＞ ネットワーク管理

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

PC 版アプリ、またはブラウザを使用した LINE WORKS サービスへのアクセス、および Drive エクスプローラーからのアクセスを特定の IP アドレスのみに制限します。
第三者による不正アクセスなど、外部端末からのサービスへのアクセスを規制することで、セキュリティリスクを低減できます。（モバイル版アプリからのアクセスは制限の対象外です。）

アクセス状況の確認と強制接続解除 [管理者機能]

メンバー ＞ メンバー情報 ＞ アクセス状況

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

各メンバーによる 90 日間のアクセス状況を個別に確認できます。管理者が強制的に接続を解除することも可能なため、外部からの不正アクセスや、社内でのシャドーIT の監視にも有効です。

アカウント一時停止 [管理者機能]

メンバー ＞ メンバー情報 ＞ その他

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

企業ポリシーに沿って必要な場合には、アカウントの一時停止が可能です。

メンバーのアクセスブロック　[管理者機能]

メンバー ＞ メンバー情報 ＞ その他

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

特定メンバーの LINE WORKS PC 版/モバイル版 からのアクセスをブロックします。ブラウザ版からのアクセスは可能なため、端末の紛失等でアプリからのアクセスのみブロックする場合に有効です。

ファイル制限　[管理者機能]

セキュリティ ＞ ファイルセキュリティ

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

トーク/ノート/掲示板/メール/カレンダー/Drive/アンケートで使用されるファイル形式を制限できます。拡張子による制限が可能なためシャドーIT によるマルウェアの拡散や不正プログラムを含む可能性がある実行ファイルの送受信などを防止し、セキュリティリスクを低減します。
(本設定の制限有無に関わらず、ウィルススキャンはすべてのサービスに対し標準で行なわれています。)

利用状況　[管理者機能]

セキュリティ

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

LINE WORKS を利用しているメンバーのデバイス情報、使用アプリのバージョンなどを確認できます。
会社で許可していない端末によるログインの確認や、アプリのアップデート通知も可能なため、
セキュリティリスクに繋がる使用の有無を確認できます。

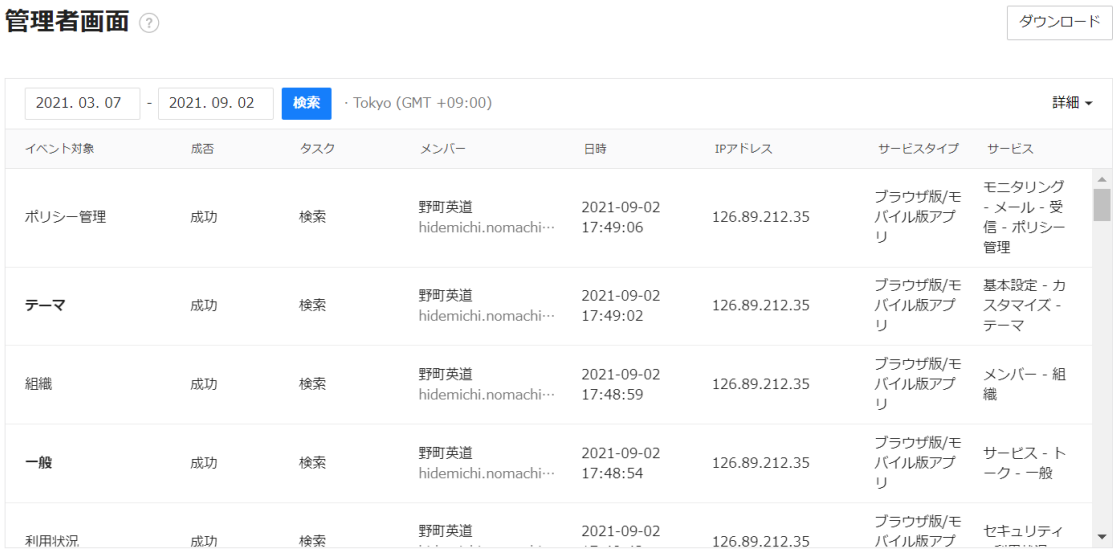
監査/モニタリング

監査/ログ 機能 [管理者機能]

監査

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

監査/ログ機能によって管理者画面での操作、およびメンバーによる各サービスの利用について確認できます。各操作内容の日時、内容、メンバー情報等が残るため、不正な管理や利用の防止に有効です。



監査/ログ機能によって確認できる内容は以下のとおりです。

管理者画面	管理者画面におけるすべてのタスク履歴と操作したメンバーを表示します。
ログイン	モバイル版/PC 版アプリ・ブラウザ版サービスへのログイン履歴を表示します。
掲示板	掲示板における投稿、編集、削除などの履歴を表示します。
Drive	Drive におけるアップロード、ダウンロード、削除などの履歴を表示します。
カレンダー	カレンダーにおける予定の登録、修正、削除などの履歴を表示します。
アドレス帳	アドレス帳における情報照会などの履歴を表示します。
タスク	タスクにおける作成、修正、完了、削除などの履歴を表示します。
アンケート	アンケートにおける作成、編集、削除などの履歴を表示します。
画面共有	画面共有における参加者と利用履歴を表示します。
ノート	ノートにおける投稿、編集、削除などの履歴を表示します。
メール	メールにおける送受信履歴を表示します。
トーク	モバイル版/PC 版アプリ・ブラウザ版でやり取りされたトークおよび音声・ビデオ通話の履歴を表示します。
テンプレート	トーク、ノート、掲示板で使用されたテンプレートの履歴を表示します。

メールの送受信ポリシー/モニタリング　[管理者機能]

モニタリング

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

メンバーによるメールの送受信に対して、ポリシーを設定しフィルタリングが可能です。
悪意あるメールの受信ブロックや、情報漏洩に繋がるファイルの送信もフィルタリングできます。

Drive ポリシー/モニタリング　[管理者機能]

モニタリング

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

メンバーの Drive 利用に対して、ポリシーを設定しモニタリングが可能です。
セキュリティリスクのあるファイルの保存など監査ができます。

トークポリシー/モニタリング　[管理者機能]

モニタリング

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

メンバーのトーク利用に対して、ポリシーを設定しモニタリングが可能です。

外部連携での情報漏洩の監査ができます。また、社内トークにおけるコンプライアンス監査にも有効です。

モバイルセキュリティ

遠隔デバイス管理(MDM) [管理者機能]

セキュリティ ＞モバイル管理

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

事前にデバイス登録されたモバイル端末の情報を遠隔で削除・初期化できる LINE WORKS MDM と、外部 MDM と連携し iOS/Android for Work/Android Enterprise 対応端末からのサービス利用を管理できる外部 MDM 連携が利用できます。
モバイル端末の紛失への対応や、不正な端末からのアクセスによる情報漏洩の防止にも有効です。

パスコードロック [管理者機能]

セキュリティ ＞モバイル管理

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

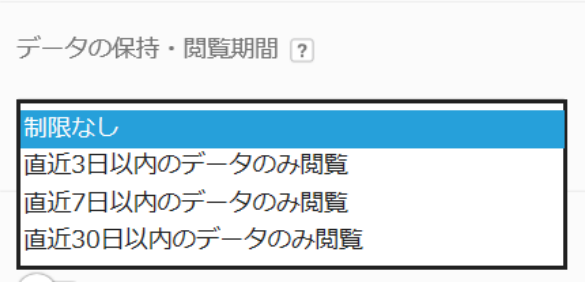
モバイル版アプリからの利用に対してパスコードロックの有無、パスコードの長さ、
入力回数制限を設定します。
メンバー以外の第三者によるモバイルからの操作を防止できます。

データの保持・閲覧期間　[管理者機能]

セキュリティ ＞モバイル管理

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

各サービス内のデータをモバイル端末から閲覧できる期間を設定します。
期間外のファイルのキャッシュデータは自動的に削除されるためデータ管理における安全性を高めます。



ファイルのアップロード制限　[管理者機能]

セキュリティ ＞モバイル管理

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

モバイル端末で保持しているファイルをサービス内にアップロードできないよう設定します。マルウェアなど悪意のあるファイル/データの拡散リスクを低減します。

テキストのコピー制限　[管理者機能]

セキュリティ ＞モバイル管理

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

各サービス内のテキスト情報をモバイル端末のクリップボードにコピーできないよう設定します。不正な情報取得や情報の誤送信のリスクを低減できます。

メールセキュリティ

ウィルスメール・スパムメール対策　[基本機能]

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

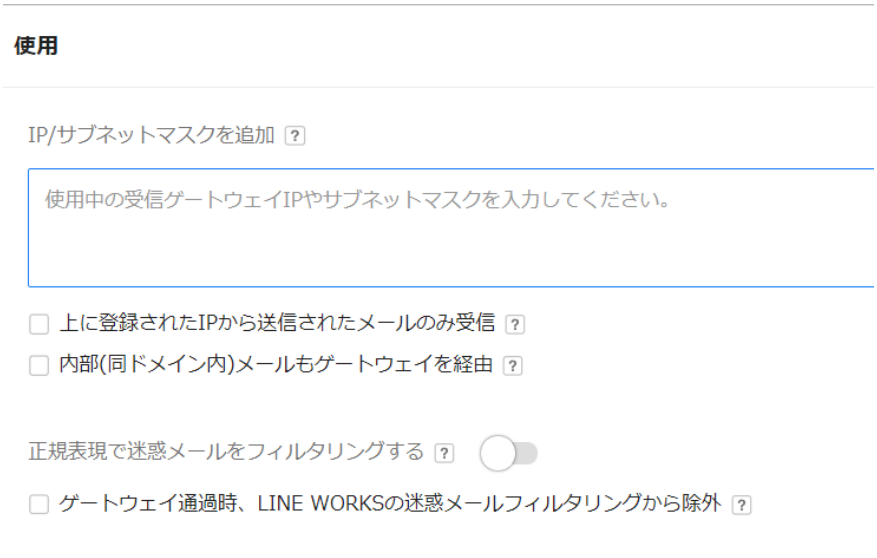
LINE WORKS では、違法性・犯罪性の内容を含むメールや、ユーザーの権益侵害を目的とした悪意のあるメール、また受信者の同意なく送られてくる広告メールなど、迷惑メール、スパムメールに分類されるメールに対して常時対策を行っており、メール利用者が快適に使用できるサービスの提供に努めています。また、迷惑メールを受信した場合も、その削除や受信拒否の設定等もメンバー自身で簡単に行えます。

受信ゲートウェイ設定　[管理者機能]

サービス ＞ メール ＞ 送受信設定

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

メールの監査やフィルタリング、アーカイブなどの理由により外部の受信ゲートウェイサービスを利用している場合も LINE WORKS メールで設定が可能です。



送信ドメイン認証（DKIM）　[管理者機能]

サービス ＞ メール ＞ 送受信設定

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

送信ドメイン認証 DKIM(DomainKeys Identified Mail)を設定し、メールが送信側で不正に改ざんされていないかを確認し安全に受信できます。

なりすましメール警告　[基本機能]

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

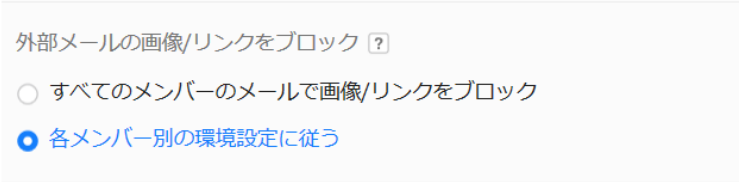
受信メールにおいて、メール送信者（差出人）として表示されているメールアドレスと、実際にメール送信で経由したメールサーバーが異なる場合に、「なりすましメール」の警告が受信者に表示されます。

外部受信メールの画像・リンク表示制限 ［管理者機能］

セキュリティ ＞ メール管理

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

受信メールに画像添付やリンク情報が含まれている場合、メール開封時にそれらの情報を直接表示しないよう制限が可能です。
これにより、万が一迷惑メールや、悪意のあるメールを開封した場合でも、添付ファイル、リンクへのアクセスによるセキュリティリスクを低減できます。



IP アドレスによる受信許可/拒否 ［管理者機能］

サービス ＞ メール ＞ 送受信設定

不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

特定の IP アドレスから送られるメールのみ受信許可または受信拒否するよう設定できます。
迷惑メールや、悪意のあるメールによるセキュリティリスクを低減できます。

社内メールのセキュリティレベル/有効期限設定 ［管理者機能］

セキュリティ ＞ メール管理

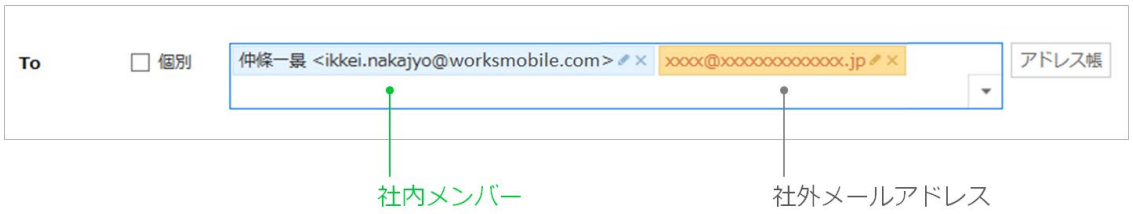
不正アクセス対策　情報漏洩対策　マルウェア対策　誤送信対策　紛失・盗難対策

社内メールの作成時にセキュリティレベルとメールの有効期限を設定可能です。期限を過ぎると自動的にメールが削除されるため情報保護に有効です。

宛先メールアドレス判定　[基本機能]

不正アクセス対策　**情報漏洩対策**　マルウェア対策　**誤送信対策**　紛失・盗難対策

メール作成において、宛先（CC、BCC 含む）に入力されたメールアドレスを判定し「社内メンバー」と「社外メールアドレス」を色別に表示します。これにより社外へのメール誤送信が減るため、情報漏洩のリスクも低減できます。



保留送信　[メンバーにより設定]

環境設定 ＞ 基本設定 ＞ メール作成/返信

不正アクセス対策　**情報漏洩対策**　マルウェア対策　**誤送信対策**　紛失・盗難対策

メール送信をクリック後、実際にメールが送信されるまでの時間を設定可能です。
誤送信は「送信」をクリックした直後に気付くことも少なくないため、設定した時間内であれば内容の誤りに気付いた場合も送信をキャンセルでき情報漏洩を防止できます。

保留送信	☐使用する　30秒　後に送信 「送信」ボタンをクリックして、設定した時間保留してから送信する機能で、 誤ってメールを送信した時に速やかに送信を取り消したり、修正することができます。 ※ ただし、保留送信を有効にする場合、送信取消後にメールを修正して再送信できるように、 設定に関係なく送信済みメールが保存されます。

送信前プレビュー　[メンバーにより設定]

環境設定 ＞ 基本設定 ＞ メール作成/返信

不正アクセス対策　**情報漏洩対策**　マルウェア対策　**誤送信対策**　紛失・盗難対策

メール送信の前にプレビューを表示します。
プレビューによる確認画面を一度表示することで誤送信のリスクを低減します。

送信前プレビュー	◯すべてのメール　◉重要なメール　◯使用しない メールを送信する前に内容を再確認できます。

導入相談

ライト/ベーシック/プレミアム 導入相談（専用窓口）

ライト/ベーシック/プレミアム導入相談の専用窓口です。
LINE WORKS の機能、およびフリープランに関するお問い合わせについては、対応できかねますのでご了承ください。

0120-907-570 (平日 10:00-18:00)