

LINE WORKS



Security System Guide

セキュリティシステムガイド

VER.3.9.0

- **国際認証の取得 1**
 - ISO/IEC27001, 27017, 27018 1
 - SOC2/SOC 3 (SysTrust) 1
- **インフラシステムのセキュリティ 2**
 - データセンター 2
 - ファシリティ/システムの耐久性 2
 - 物理セキュリティ 2
 - サービスシステム 2
 - 情報セキュリティ 2
- **セキュリティ機能の紹介 3**
 - アカウント・アクセス 3
 - パスワードポリシーの設定 [管理者機能] 3
 - 2段階認証ログイン [全メンバー対象] 3
 - ID/パスワード確認時における本人認証 [全メンバー対象] 4
 - IP アドレス接続制限 [管理者機能] 5
 - アクセス状況の確認と強制接続解除 [管理者機能] 5
 - アカウント一時停止 [管理者機能] 5
 - メンバーのアクセスブロック [管理者機能] 6
 - ファイル制限 [管理者機能] 6
 - 利用状況 [管理者機能] 7
 - 監査/モニタリング 8
 - 監査/ログ 機能 [管理者機能] 8
 - メールの送受信ポリシー/モニタリング 9
 - Drive ポリシー/モニタリング [管理者機能] 9
 - トークポリシー/モニタリング [管理者機能] 10
 - モバイルセキュリティ 11
 - 遠隔デバイス管理(MDM) [管理者機能] 11
 - パスコードロック [管理者機能] 11
 - データの保持・閲覧期間 [管理者機能] 12
 - ファイルのアップロード制限 [管理者機能] 12
 - テキストのコピー制限 [管理者機能] 12
 - メールセキュリティ 13
 - ウィルスメール・スパムメール対策 [基本機能] 13
 - 受信ゲートウェイ設定 [管理者機能] 13
 - 送信ドメイン認証 (DKIM) [管理者機能] 14
 - なりすましメール警告 [基本機能] 14
 - 外部受信メールの画像・リンク表示制限 [管理者機能] 15
 - IP アドレスによる受信許可/拒否 [管理者機能] 15
 - 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] 15
 - 宛先メールアドレス判定 [基本機能] 16
 - 保留送信 [メンバーにより設定] 16
 - 送信前プレビュー [メンバーにより設定] 16

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/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。

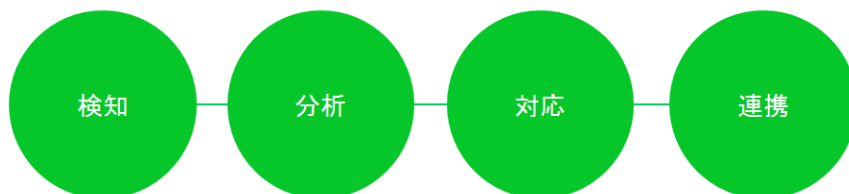
物理セキュリティ

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いません。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。

ログイン設定

2段階認証 (2-step verification) [?]

- 必須 - すべてのメンバーで2段階認証が必要
- 選択 - メンバーが個別に選択

2段階認証

2段階認証 [任意]



携帯番号または個人メールアドレスを使った2段階認証でログインします。

[認証方法の設定](#)

2段階認証の認証方法を確認してください。

次回ログイン時に携帯番号または個人メールアドレスを使った2段階認証が必要となります。

個人メールアドレス naoyuki.hashikawa@xxxxxxxx.xxxxx

携帯番号 +81 070-0000-0000

確認

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。

パスワード変更

強制変更
変更を要請

サンプルユーザー102さんの新しいパスワードを入力してください。

✓

✓

ID/パスワードを変更すると、5分以内にすべてのサービスからログアウトされ、再ログインには変更後のID/パスワードが必要です。

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認証を採用しています。

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。

IDの確認
パスワードの確認

パスワードの確認

正しい情報を入力すると、パスワードを再設定することができます。

携帯番号で確認

1079 : LINE WORKSの認証番号です。

個人メールで確認

LINE WORKS
認証番号は [0149] です。

アカウント

id@company.com または id@group

携帯番号

+81 (-)なしで、数字のみ入力

認証番号

認証番号を入力してください。

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IP制限 ^

すべてのIPからのアクセスを許可

指定したIPからのみアクセスを許可

- ・ LINE WORKSのブラウザ版 サービス、PC版アプリ、Driveエクスプローラー、POP3/SMTP、IMAP/SMTP、CalDAVに適用されます。モバイル版 LINE WORKSアプリは、IPに関わらずアクセス可能です。
- ・ 安定したサービス管理のために、管理者は設定に関係なくLINE WORKSサービスにアクセスすることができます。

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。

アクセス状況 ×

すべてにアクセス ▾ 直近90日のログイン履歴

アクセス時間	アクセス環境	位置(IPアドレス)	管理
09-03 13:11	Edge / Windows	Unknown (192.184.XX.XX)	ログアウト
09-02 13:46	モバイル版アプリ / iOS	JAPAN (121.115.XX.XX)	ログアウト
09-02 13:39	Edge / Windows	Unknown (192.184.XX.XX)	ログアウト

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。

一時停止しますか？

一時停止したメンバーはLINE WORKSのサービスを以後は利用できなくなります。

メンバーのアカウントとデータは削除されず、[一時停止の解除]から一時停止を解除できます。

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、ウイ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。)

制限対象のファイル形式

制限するサービス

掲示板/ノート トーク

カレンダー (チーム/グループ 予定)

Drive (チーム/グループフォルダ)

タスク (グループタスク)

アンケート

制限する拡張子 [?](#)

ファイル形式制限は、特に実行ファイル等によるマルウェア/ウイルス被害の防止に有用です。 [詳しく見る](#)

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。

モバイル PC

ダウンロード

直近30日以内にアクセスしたモバイルデバイス 2					
<input type="checkbox"/>	デバイス・Vendor ID	OS	インストール済みアプリ	ユーザー	最終アクセス↓
<input type="checkbox"/>	iPhone 11 58924F-xxxxxxxx-545421...	iOS 13.6.1	モバイルアプリ 2.9.2 最新	橋川尚征 naoyuki.h@worksmobile.com	2020-09-03 11:03:05
<input type="checkbox"/>	iPhone XS 7TFEW1-xxxxxxxx-874588 ...	iOS 13.6	モバイルアプリ 2.8.6 アップデートが必要	野町英道 hidemichi.n@worksmobile.com	2020-08-18 11:04:56
<input type="checkbox"/>	PAR-LX9 未登録 5c89479845xxxx	Android 9	モバイルアプリ 2.8.5 アップデートが必要	水平園子 sonoko.mizuhira@worksmobile.com	2020-08-18 15:26:16

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。

管理者画面 ?

ダウンロード

イベント対象	成否	タスク	メンバー	日時	IPアドレス	サービスタイプ	サービス
ポリシー管理	成功	検索	野町英道 hidemichi.nomachi...	2021-09-02 17:49:06	126.89.212.35	ブラウザ版/モバイル版アプリ	モニタリング - メール - 受信 - ポリシー管理
テーマ	成功	検索	野町英道 hidemichi.nomachi...	2021-09-02 17:49:02	126.89.212.35	ブラウザ版/モバイル版アプリ	基本設定 - カスタマイズ - テーマ
組織	成功	検索	野町英道 hidemichi.nomachi...	2021-09-02 17:48:59	126.89.212.35	ブラウザ版/モバイル版アプリ	メンバー - 組織
一般	成功	検索	野町英道 hidemichi.nomachi...	2021-09-02 17:48:54	126.89.212.35	ブラウザ版/モバイル版アプリ	サービス - トーク - 一般
利用状況	成功	検索	野町英道 hidemichi.nomachi...	2021-09-02 17:48:54	126.89.212.35	ブラウザ版/モバイル版アプリ	セキュリティ

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。

タイトル <input type="text" value="受信制限 (転職)"/>	<p>LINE WORKS</p> <p>メール受信ポリシーによるモニタリングで以下が検知されました。</p> <hr/> <p>メール受信ポリシー 3 の条件に該当するメールが検知されました。</p> <p>送信日時：2017-09-08 PM 04:00 (GMT +09:00) 送信元アドレス：mitsuhiro.suzuki@worksmobile.com 送信先アドレス：ikkei.nakajyo@worksmobile.com 件名：XXXXXXXXXX 適用ポリシー番号：受信ポリシー 3</p> <p>詳細はLINE WORKS管理者画面 [監査] で確認してください。</p>
条件設定	
メール受信 <input checked="" type="checkbox"/> メンバーからの受信 <input checked="" type="checkbox"/> 外部からの受信	
送信者 <input type="checkbox"/> 設定	
受信者 <input type="checkbox"/> 設定	
コンテンツフィルタリング <input checked="" type="checkbox"/> 設定	
コンテンツ <input type="text" value="件名"/> <input type="button" value="転職"/>	
<input type="checkbox"/> 大文字・小文字区分	
URL <input type="text" value="URL入力時に、http://は入力しないでください。"/>	
添付ファイル <input type="checkbox"/> 一般添付	

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。

タイトル <input type="text"/>	<p>LINE WORKS</p> <p>Driveポリシーによるモニタリングで以下が検知されました。</p> <hr/> <p>Driveポリシー2の条件に該当するファイルが検知されました。</p> <p>日時：2017/09/08 17:08:07 [GMT+09:00(Tokyo, Fukuoka)] メールアドレス：仲塚一景(ikkei.nakajyo@worksmobile.com) ファイル名：XXXXXXXXX.XXX 保存場所：/ 適用ポリシー番号：2</p> <p>詳細はLINE WORKS管理者画面 [監査] で確認してください。</p>
条件設定	
基準 <input checked="" type="radio"/> ファイル容量 <input type="text" value="1"/> GB以上 <input type="radio"/> ファイル数 <input type="radio"/> コンテンツフィルタリング	
メンバー指定 <input type="checkbox"/> 設定	
適用期間の設定	
期間 <input type="text" value="2020. 09. 03"/> - <input type="text"/> <input checked="" type="checkbox"/> 満了日指	
時間帯 <input type="text" value="東京, 日本 (GMT+09:00)"/>	
通知設定	

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。

タイトル	<input type="text"/>
条件設定	
トークを送信	<input type="checkbox"/> メンバー内トーク <input checked="" type="checkbox"/> 外部に送信
送信者 <small>?</small>	<input type="checkbox"/> 設定
受信者 <small>?</small>	<input type="checkbox"/> 設定
コンテンツフィルタリング	<input type="checkbox"/> 設定
添付ファイル	<input type="checkbox"/> 設定
Botのトーク	<input type="text" value="Botのトークを除く"/>
通知設定	
検知周期	<input type="text" value="1時間ごと"/>

LINE WORKS

トークポリシーによるモニタリングで以下が検知されました。

トークポリシー1の条件に該当するトークが検知されました。

モニタリング期間: 2017/09/08 13:00 ~ 2017/09/08 14:00

検知されたトーク数: 6

適用ポリシー番号: 1

詳細はLINE WORKS管理者画面【監査】で確認してください。

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。

遠隔デバイス管理 (MDM)

LINE WORKS MDM

無効にする

例外管理 0 >

外部MDM連携

外部MDM連携

他のドメインアカウントでのログインを制限する

Configuration Key 「LineworksAuthCode」と発行したKey Valueの値を、連携する外部MDMのApp Configuration機能で設定してください。

Configuration Key

Value Type String

Key Value 自動作成 その他の色

再発行

15文字の英字(大文字・小文字区分)、または数字を入力してください。

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。

画面ロック

画面ロックの使用

必須 - メンバー全員が必ず画面ロックを設定

選択 - メンバーの選択によって自由に設定

パスコード形式

数字4桁

英数字6字以上

英数字8字以上

パスコード設定

パスコード設定

設定したいパスコードを入力してください。

1	2	3
4	5	6
7	8	9
0		✖

パスコードを入力

パスコードを入力してください。

“LINE WORKS”でTouch IDを使用

LINE WORKSロックを解除

キャンセル

4	5	6
7	8	9
0		✖

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。

データの保持・閲覧期間 ?

- 制限なし
- 直近3日以内のデータのみ閲覧
- 直近7日以内のデータのみ閲覧
- 直近30日以内のデータのみ閲覧

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。

迷惑メール
未読
移動 ▾
リマインダー ▾
その他 ▾

迷惑メールを報告する
 選択したメールの迷惑メール処理方法を設定してください。

迷惑メールに送る 完全に削除

選択したメールアドレスを受信拒否する
(0 個 / 1000 個)

選択したメールアドレスから届いた既存のメールもあわせて迷惑メールとして処理

※ 迷惑メールとして報告されたメールは、迷惑メールタイプ分析に利用されます。
 ※ 完全に削除したメールは復旧できません。
 ※ 受信拒否に指定したメールアドレスから届いたメールは、迷惑メールフォルダに移動されます。

次回から表示しない

キャンセル
OK

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。

使用

IP/サブネットマスクを追加 [?](#)

使用中の受信ゲートウェイIPやサブネットマスクを入力してください。

- 上に登録されたIPから送信されたメールのみ受信 [?](#)
- 内部(同ドメイン内)メールもゲートウェイを経由 [?](#)

正規表現で迷惑メールをフィルタリングする [?](#)

- ゲートウェイ通過時、LINE WORKSの迷惑メールフィルタリングから除外 [?](#)

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。

認証状態	未認証	
セレクト	<input type="text" value="lineworks"/>	<input type="button" value="生成"/>
ホスト名	<input type="text" value="lineworks_domainkey"/>	<input type="button" value="コピー"/>
公開鍵 (TXTレコード)	メール認証を利用する場合は、新しいレコードが必要です。 セレクト右側の生成を選択してください。	<input type="button" value="コピー"/>

・ 認証を開始する前にこのドメインに対するDNS(ドメインネームサーバー)のレコードをアップデートしてください。
 ・ ドメインプロバイダーのDNS設定ページで上記のホスト名とTXTレコードを登録してください。

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。

返信 全員に返信 転送 削除 未読 移動 🔄 ⋮ 翻訳

☆ 先日はお世話になりました。📧

From VIP 市川勇二郎 <yujiro@worksmobile.com> [トーク](#)

! このメールは[worksmobile.com]を経由して送信されていません。[差出人]のアドレスは、実際の送信元アドレスとは異なる可能性がありますのでご注意ください。 [詳しく見る](#)

To 橋川尚征 <naoyuki.hashikawa@worksmobile.com>

お疲れ様です。

お話ししたプロジェクトの情報は以下となります。

ご確認お願いします。

<http://xx>

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。

外部メールの画像/リンクをブロック [?](#)

- すべてのメンバーのメールで画像/リンクをブロック
- 各メンバー別の環境設定に従う

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。

IP追加 ×

適用範囲 株式会社XXXXXXXXXXXX

IP

単一IP形式で追加します。複数のIPを一度に入力する場合は
コンマ(,)/エンター(Enter)/ブランク(Blank)で区別してください。

備考

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。

情報レベルの設定 [?](#)

公開 有効期限 未設定 転送 可能

社外秘 1週間 転送 可能

機密 1ヶ月 転送 可能

宛先メールアドレス判定 [基本機能]

不正アクセス対策

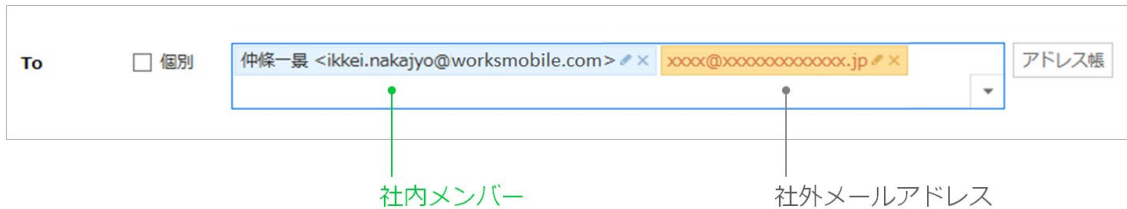
情報漏洩対策

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。

<p>保留送信</p>	<p><input type="checkbox"/> 使用する <input type="text" value="30秒"/> 後に送信</p> <p>「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。</p> <p>※ 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。</p>
--------------------	---

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。

<p>送信前プレビュー</p>	<p><input type="radio"/> すべてのメール <input checked="" type="radio"/> 重要なメール <input type="radio"/> 使用しない</p> <p>メールを送信する前に内容を再確認できます。</p>
------------------------	---

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)

