

# LINE WORKS

## 管理者トレーニング

### 4. セキュリティ管理

Ver 4.1.0

2018年6月版

# 4.セキュリティ管理

---

4.1 セキュリティ機能

4.2 ネットワークセキュリティ

4.3 アカウントセキュリティ

4.4 モバイルセキュリティ

4.5 ファイルセキュリティ

# 4.1 セキュリティ機能

# 管理画面のセキュリティ設定

**LINE WORKS Admin** 山坂一智 さん ログアウト

基本設定 メンバー サービス **セキュリティ** 監査 統計 購入 ヘルプ パートナー

**セキュリティ機能** メンバーのアカウントとデバイスを保護するセキュリティ機能を実行します。

組織図 **アクセスブロック** | 0人

写真	名前	職級	部署	アカウントステータス
	瓜原江美 emi.unihara@works1.jp	職級1	商品管理部/部長	使用中
	橋川尚征 naoyuki.hashikawa@works1.jp	職級1	マーケティング部/部長	使用中
	古澤桐畦 kirio.furusawa@works1.jp	職級1	経営支援部/部長	使用中
	仲條一景 nakajyo.ikkei@works1.jp			
	城木結菜 yuina.shiroki@works1.jp			
	本郷克馬			

**メンバーセキュリティ**

**セキュリティ情報**

アクセス状況

使用中のデバイス

パスワード変更

**瓜原江美**  
フリハラ エミ  
商品管理部 | 部長  
emi.unihara@works1.jp

使用中

直前の接続時刻 2018-04-06 11:22:27  
Chrome (Mac OS)  
Unknown (10.56.89.61)

最後にパスワードを変更した日 61日前 (2018-04-05 21:03:53)

一時停止

アクセスブロック

# セキュリティ機能（1）

[セキュリティ] - [セキュリティ機能]

- メンバーのアクセス状況を確認し、ブロックや一時停止などの利用管理を行います。
  - 一時停止：すべてのサービスからログアウト / 利用禁止
  - アクセスブロック：LINE WORKSモバイル版、PC版アプリ及びドライブエクスプローラーへのアクセスをブロックします。PC WEBでは正常にご利用いただけます。

The screenshot shows the LINE WORKS Admin interface. The top navigation bar includes icons for settings, members, services, security, monitoring, statistics, purchase, help, and partners. The left sidebar lists various security and management options. The main content area is titled 'セキュリティ機能' (Security Function) and includes a description: 'メンバーのアカウントとデバイスを保護するセキュリティ機能を実行します。' (Execute security functions to protect member accounts and devices). Below this, there is an '組織図' (Organizational Chart) showing a hierarchy of departments: '株式会社ワークスワン・コーポレーション' (Works One Corporation) with '本社' (Headquarters) at 18, '店舗' (Stores) at 12, and '新しい組織' (New Organization) at 0. A '写真' (Photo) section shows a list of member avatars, with a red starburst and arrow pointing to the first member. A modal window titled 'メンバーセキュリティ' (Member Security) is open, showing details for a member named 瓜原江美 (Emi Urihara). The modal includes a 'セキュリティ情報' (Security Information) section with tabs for 'アクセス状況' (Access Status), '使用中のデバイス' (Devices in Use), and 'パスワード変更' (Change Password). The 'アクセス状況' tab is active, showing the member's name, title (商品管理部 部長), and email (emi.urihara@works1.jp). It also displays '直前の接続時刻' (Last Connection Time) as 2018-04-06 11:22:27 on Chrome (Mac OS) and '最後にパスワードを変更した日' (Last Password Change Date) as 61 days ago (2018-04-05 21:03:53). At the bottom of the modal, two buttons are visible: '一時停止' (Suspend) and 'アクセスブロック' (Block Access), both highlighted with a red box.

- メンバーのセキュリティに関する項目を確認・設定することができます

The screenshot displays the LINE WORKS Admin console. The top navigation bar includes icons for settings, members, services, security, monitoring, statistics, purchase, help, and partners. The main content area is titled 'セキュリティ機能' (Security Function) and includes a sub-header 'メンバーのアカウントとデバイスを保護するセキュリティ機能を実行します。' (Execute security functions to protect member accounts and devices). On the left, there is an '組織図' (Organizational Chart) showing a hierarchy with '株式会社ワークスワン・コーポレーション' (Works One Corporation) at the top, '本社 18' (Headquarters 18), '店舗 12' (Stores 12), and '新しい組織 0' (New Organization 0). The main area shows a list of members under 'アクセスブロック' (Access Block) with 0 members. A red arrow points to the profile of '瓜原江美' (Emi Urihara). A modal window titled 'メンバーセキュリティ' (Member Security) is open for her profile, showing security information, access status, devices, and password change options. The modal also displays her profile picture, name, department, and contact information.

**LINE WORKS Admin**

基本設定    メンバー    サービス    **セキュリティ**    監査    統計    購入    ヘルプ    パートナー

・セキュリティ機能

・利用状況

・インストール状況

・ネットワークセキュリティ

・アカウントセキュリティ

・モバイルセキュリティ

・ファイルセキュリティ

**セキュリティ機能**    メンバーのアカウントとデバイスを保護するセキュリティ機能を実行します。

組織図    アクセスブロック | 0人

株式会社ワークスワン・コーポレーション

- 本社 18
- 店舗 12
- 新しい組織 0

写真

nao

ki

r

y

**メンバーセキュリティ**

セキュリティ情報

- アクセス状況
- 使用中のデバイス
- パスワード変更

一時停止

アクセスブロック

瓜原江美  
ウリハラ エミ  
商品管理部 | 部長  
[emi.urihara@works1.jp](mailto:emi.urihara@works1.jp)

使用中

直前の接続時刻    2018-04-06 11:22:27  
Chrome (Mac OS)  
Unknown (10.56.89.61)

最後にパスワードを変更した日    61日前 (2018-04-05 21:03:53)

- セキュリティ情報：メンバーの利用実績やパスワード変更の、状況を把握する

The screenshot shows the 'Member Security' page for a user named Emi Urahara. The page is divided into a left sidebar and a main content area. The sidebar contains a 'Security Information' section with sub-items: 'Access Status', 'Devices in Use', and 'Password Change'. The main content area displays the member's profile picture, name, department, title, and email address. Below this, it shows the current status as 'In Use'. A table lists the 'Previous Connection Time' with details: '2018-04-06 11:22:27', 'Chrome (Mac OS)', and 'Unknown (10.56.89.61)'. At the bottom, it shows the 'Last Password Change Date' as '61 days ago (2018-04-05 21:03:53)'. At the bottom left of the page, there are two buttons: 'Temporarily Stop' and 'Access Block'. Four callout boxes on the right point to specific elements: 'Member Information' points to the profile picture and name; 'Status' points to the 'In Use' status; 'Previous Usage Time' points to the connection time table; and 'Last Password Change Date' points to the password change date.

直前の接続時刻	2018-04-06 11:22:27
	Chrome (Mac OS)
	Unknown (10.56.89.61)

最後にパスワードを変更した日 61日前 (2018-04-05 21:03:53)

一時停止

アクセスブロック

メンバー情報

ステータス

直前の利用時間

最後にパスワードを変更した日

# メンバーセキュリティ：アクセス状況

[セキュリティ] - [セキュリティ機能]

- アクセス状況：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。アクセス時間やOS/ブラウザの環境を把握し、管理者が強制的に接続を「切断」する事もできます。外部からの不正アクセスなどの監視に利用します。

メンバーセキュリティ

セキュリティ情報

アクセス状況

直近90日間のすべてにアクセス状況

すべてのアクセス

アクセス時間	アクセス環境	位置(IPアドレス)	管理
06-05 18:13	モバイル版アプリ / iOS	JAPAN(111.239.60.152)	切断
04-06 11:22	Chrome / Mac OS	Unknown(10.56.89.61)	切断
04-06 10:53	Chrome / Mac OS	Unknown(10.56.89.61)	切断
04-05 22:38	Chrome / Mac OS	Unknown(10.56.89.61)	切断
04-05 22:13	Chrome / Mac OS	Unknown(10.56.89.61)	切断
04-05 21:04	Chrome / Mac OS	Unknown(10.56.89.61)	切断

一時停止

アクセスブロック

アクセス時間

## セッションの強制切断

モバイル版アプリ / iOS  
JAPAN(111.239.60.152)

接続されたセッションを終了します。

OK キャンセル

位置 (IPアドレス)

アクセス環境  
(OS/ブラウザ)

# メンバーセキュリティ：使用中のデバイス

[セキュリティ] - [セキュリティ機能]

- メンバーが使用しているデバイスの情報やインストールアプリのバージョン番号などを確認することができます。

メンバーセキュリティ

セキュリティ情報 **瓜原江美のすべてのデバイス合計1台** すべてのデバイス

モデル(デバイス名)	デバイス OS (バージョン)
iPhone	iOS (11.3)

ユーザー: 瓜原江美

モデル: iPhone

デバイス OS: iOS (11.3)

Vendor ID: A80AED0E-668C-014B-0000-000000000000

インストール済みアプリ: モバイル版アプリ (2.3.2)

初回接続時刻: 2018-04-18 01:36:54

直前の接続時刻: 2018-06-05 18:13:41

一時停止

アクセスブロック

デバイスのモデル / OSバージョン

インストール済アプリ

初回アプリインストール時刻

直前の接続時刻

# メンバーセキュリティ：パスワード変更 [セキュリティ] - [セキュリティ機能]

- 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）  
パスワード情報は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。

The screenshot displays the 'メンバーセキュリティ' (Member Security) settings page. The left sidebar contains a menu with 'セキュリティ情報', 'アクセス状況', '使用中のデバイス', and 'パスワード変更' (highlighted). Below the menu are buttons for '一時停止' and 'アクセスブロック'. The main content area is titled 'パスワード変更' and includes two options: 'パスワード強制変更' (highlighted with a red box) and 'パスワードの変更を要請' (highlighted with a red box). A red arrow points from the 'パスワード強制変更' option to a dialog box titled '新しいパスワードに変更します。' (Change to a new password). This dialog box contains two input fields for '新しいパスワード' and '新しいパスワード(確認)', and 'OK' and 'キャンセル' buttons. Another red arrow points from the 'パスワードの変更を要請' option to a dialog box titled '次回ログインする際にパスワードを強制変更するように設定しますか?' (Do you want to set up password forced change at the next login?). This dialog box has 'OK' and 'キャンセル' buttons.

- LINE WORKSモバイル版アプリとPC版アプリのインストール状況を把握することができます。未インストールのメンバーへ「インストール案内を送信」することもできます。

インストール状況 LINE WORKSモバイル版アプリとPC版アプリのインストール状況を把握することができます。

組織図

メンバー検索

インストール案内を送信 (1) 全員にインストール案内を送信 すべて | 28人 [インストール案内送信履歴](#)

<input type="checkbox"/>		本郷克馬 katsuma.hongo...	職級3	営業部/リーダー		未インストール	未インストール
<input checked="" type="checkbox"/>		立原真紀 maki@works1.jp	職級2	情報システム部/社員	wj90016@worksmobile.com	未インストール	未インストール
<input type="checkbox"/>		下平慶人 keito.shimohira...	職級3	マーケティング部/社員		未インストール	未インストール
<input type="checkbox"/>		石咲媛莉 airi.ishizaki@w...	職級4	マーケティング部/社員		未インストール	インストール済み

注) 「インストール案内を送信」はメンバー情報にメールアドレスが設定されている場合に送信することができます

## 4.2 ネットワークセキュリティ

# セキュリティ：ネットワークセキュリティ

- LINE WORKSのブラウザ版 および PC 版 アプリ、Drive エクスプローラー、POP3/SMTP、CalDAVサービスに接続できる グローバル IP アドレスを制限できます。
- **管理者画面およびモバイル版 LINE WORKS は制限されません。**
- IP アドレスはサブネットでの指定も可能です。

・セキュリティ機能

・利用状況

・インストール状況

・**ネットワークセキュリティ**

・アカウントセキュリティ

・モバイルセキュリティ

・ファイルセキュリティ

## ネットワークセキュリティ

●  すべてアクセス許可    ●  特定IPのみアクセス許可       

※ 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。

※ 「特定IPのみ許可」を選択した場合、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。

アクセスIP制限

許可済みIPアドレスリスト

192.165.1.1

  

### LINE WORKS

LINE WORKSアカウントを入力してください。

  

.....

現在接続中のIPではサービスをご利用いただけません。詳細については、内部の管理者にお問い合わせください。

ログイン保持     ID・パスワードの確認

他のグループ名またはドメインでログイン

## 4.3 アカウソトセキユリテイ

# セキュリティ：アカウントセキュリティ

- パスワードの複雑さや有効期限など、管理ルールを設定します。

<ul style="list-style-type: none"><li>・セキュリティ機能</li><li>・利用状況</li><li>・インストール状況</li><li>・ネットワークセキュリティ</li><li>・<b>アカウントセキュリティ</b></li><li>・モバイルセキュリティ</li><li>・ファイルセキュリティ</li></ul>	<b>アカウントセキュリティ</b>	
	<b>パスワード管理</b>	
	パスワードの難易度	<input type="text" value="半角英数字"/> <small>パスワードで使用する文字を「半角英数字」または「半角英数字と特殊文字の組み合わせ」で設定します。</small>
	パスワードの長さ	<input type="text" value="最小文字数 8"/> <small>使用できるパスワードの長さを設定します。パスワードの長さは8~20文字（半角英数字基準）以内で設定することができます。</small>
	パスワードの有効期限	<input type="text" value="365日"/> <small>パスワードを設定した日から選択した有効期限を過ぎると新しいパスワードを設定するようにします。</small>
	パスワードの再使用禁止	<input type="text" value="制限なし"/> <small>パスワードの再設定時に過去に使用したパスワードの再使用可否を設定します。</small>
ログイン失敗時のアカウント一時停止	<input type="text" value="制限なし"/> <small>設定した回数以上、連続してログインに失敗した場合にアカウントを一時停止します。</small>	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

パスワードの難易度

パスワード難易度を2段階（半角英数、半角英数+特殊文字）で設定します。

パスワードの長さ

8~20 文字でパスワード長を設定します。

パスワードの有効期限

パスワードの有効期限を設定します。

パスワードの再使用禁止

最近使ったパスワードを最大 5 個まで利用禁止にできます。

ログイン失敗時の  
アカウント一時停止

一定回数以上のログイン失敗時にアカウントを一時停止できます。  
一時停止の解除は「メンバー」メニューから行います。

## 4.4 モバイルセキュリティ

# セキュリティ：モバイルセキュリティ

- モバイルアプリに対するセキュリティ設定を行います。

The screenshot shows the LINE WORKS Admin interface. The top navigation bar includes icons for 基本設定 (Basic Settings), メンバー (Members), サービス (Services), **セキュリティ** (Security), 監査 (Audit), 統計 (Statistics), 購入 (Purchase), ヘルプ (Help), and パートナー (Partners). The left sidebar lists various security features, with **モバイルセキュリティ** (Mobile Security) highlighted in red. The main content area is titled 'モバイルセキュリティ' and contains two sections: 'パスコードロック' (Passcode Lock) and 'モバイルアプリ機能' (Mobile App Features).

## モバイルセキュリティ

### パスコードロック

パスコードロックの使用	<input type="radio"/> 有効にする <input checked="" type="radio"/> 無効にする ※ メンバーがモバイル版アプリ起動時にパスコードの入力を必須にするよう設定します。
パスコード形式	<input checked="" type="radio"/> 数字4桁 <input type="radio"/> 英数字6字以上10字以下 <input type="radio"/> 英数字8字以上10字以下
パスコード入力回数制限	<input type="text" value="5回"/> <input type="button" value="▼"/> ※ 連続してパスコードの入力に失敗した場合、アプリからログアウトするよう設定できます。

### モバイルアプリ機能

ログイン状態保持期間	<input type="text" value="30日"/> <input type="button" value="▼"/> ※ 上記設定は、モバイル版アプリで操作を行わない場合に自動ログアウトされるまでの期間です。 ※ 期間を変更した場合もメンバーが再ログインするまでは変更内容は適用されませんのでご注意ください。
データの保持・閲覧期間	<input type="text" value="制限なし"/> <input type="button" value="▼"/> ※ 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。 ※ 設定した期間を過ぎたファイルは自動的に削除されます。
ファイルのアップロー	<input checked="" type="radio"/> 許可 <input type="radio"/> 制限

- モバイルアプリの起動や切り替え時に、パスコードロックを強制できます。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
  - パスコードを一定回数間違えた場合に強制ログアウトさせる設定も可能です。
  - パスコードの複雑さも設定できますが、複雑なパスコードは利便性を大きく損ねるので設定は慎重に検討してください。

・セキュリティ機能 ・利用状況 ・インストール状況 ・ネットワークセキュリティ ・アカウントセキュリティ ・ <b>モバイルセキュリティ</b> ・ファイルセキュリティ	<b>モバイルセキュリティ</b>	
	<b>パスコードロック</b>	
	パスコードロックの使用	<input type="radio"/> 有効にする <input checked="" type="radio"/> 無効にする ※ メンバーがモバイル版アプリ起動時にパスコードの入力を必須にするよう設定します。
	パスコード形式	<input checked="" type="radio"/> 数字4桁 <input type="radio"/> 英数字6字以上10字以下 <input type="radio"/> 英数字8字以上10字以下
パスコード入力回数制限	<input type="text" value="5"/> 回 ※ 連続してパスコードの入力に失敗した場合、アプリからログアウトするよう設定できます。	

## パスコードロックの使用

モバイルアプリケーション利用時にパスコード設定を強制します。

## パスコード形式

パスコードの複雑さを 3 段階で設定します。

## パスコード入力回数制限

パスコード入力を一定回数以上間違えた場合に強制的にログアウトします。

- モバイルアプリでのログイン期間や、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などを設定します。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。

モバイルアプリ機能	
ログイン状態保持期間	<input type="text" value="30日"/> <span>▼</span> ※ 上記設定は、モバイル版アプリで操作を行わない場合に自動ログアウトされるまでの期間です。 ※ 期間を変更した場合もメンバーが再ログインするまでは変更内容は適用されませんのでご注意ください。
データの保持・閲覧期間	<input type="text" value="制限なし"/> <span>▼</span> ※ 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。 ※ 設定した期間を過ぎたファイルは自動的に削除されます。
ファイルのアップロード	<input checked="" type="radio"/> 許可 <input type="radio"/> 制限 ※ 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。
テキスト情報のコピー	<input checked="" type="radio"/> 許可 <input type="radio"/> 制限 ※ 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。

## ログイン状態の保持期間

モバイル版アプリが無操作状態で自動ログアウトされるまでの期間を設定します。(30日、6ヶ月、1年)

## データ保持/閲覧期間

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

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に設定します。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。

## テキスト情報のコピー

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に設定します。不正な情報取得や情報のご送信のリスクを低減できます。

# デバイス管理 (MDM)

[セキュリティ] - [モバイルセキュリティ]

- LINE WORKS MDMを利用することで、モバイル端末を紛失した際に、遠隔からデータを削除したり、端末を初期化することができます。
- OS の制約から管理プロファイルを 2つ同時に利用することはできません。すでに他社製の MDMを運用中の場合は、LINE WORKS MDMを有効にしないことを推奨しています。
- 外部MDMと連携し、利用するモバイルアプリを、MDMから配布したアプリに限定し、BYODのモバイル端末の利用を制限するなどの制御が可能です。

デバイス管理 (MDM)

---

**LINE WORKS MDM**

必須にする     個別設定する     無効にする    [例外管理](#)

※ LINE WORKS MDMを利用すると、モバイル版LINE WORKSアプリのデータ削除またはデバイスの初期化を遠隔操作で行なえます。

※ 本機能による各デバイスの識別番号取得、およびモバイル版LINE WORKSアプリのデータ削除またはデバイスの初期化は、これらに該当する社内規定やセキュリティポリシーに基づき合法的に行なってください。

---

遠隔デバイス管理

**外部MDM連携**

有効にする     無効にする

※ 「外部MDM連携」を有効にすると、外部MDMでConfiguration Keyを設定し配信したモバイル版LINE WORKSアプリからのログインのみ許可します。

※ Android端末との外部MDM連携は、LINE WORKSモバイル版アプリv2.3以降かつAndroid for Work/Android Enterprise対応端末でご利用になれます。

デバイス管理	説明
LINE WORKS MDM	事前にデバイス登録されたモバイル版LINE WORKSアプリのデータ削除またはデバイスの初期化を遠隔操作で行えます。
外部MDM連携	3rd PartyのMDMを利用して、iOS/Android for Work/Android Enterprise対応端末からのサービスを管理することができます。

## 4.5 ファイルセキュリティ

# セキュリティ：ファイルセキュリティ

- ファイルの拡張子でフィルタリングし、特定のファイル形式を添付または送信できないよう制限します。サービス上で利用可能なファイル形式をブラックリストで制限します。(最大 200 個)
- トーク/ノート/ホーム/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のためシャドー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。)

### ファイルセキュリティ

#### ファイル形式制限 ?

制限対象のファイル形式

拡張子を入力

制限するファイル形式を選択

bat  cmd  com  cpl  exe  scr  js  
 vbs  wsf

制限するファイル形式を追加 (0/200)

適用サービス

トーク  
 ノート  
 ホーム  
 メール  
 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)  
 アンケート

※ ファイル制限がDriveに適用されていない場合でも、Driveと連携しているサービスのいずれかにファイル制限が適用されている場合は、Driveからのファイル添付やDriveへのファイル保存などが制限されます。  
※ マルウェア/ウイルスによる被害および拡散を防止するため、[制限するファイル形式を選択]の拡張子は、全て制限することを推奨します。  
※ [監査>モニタリング>メール>受信>IP管理]で受信許可IPに登録されたIPから送信されたメールは、設定されたファイル形式が添付されている場合にも受信します。  
※ ファイル制限の変更内容は、サービスへ反映されるまで最大で1時間程度かかる場合があります。

# LINE WORKS