スマートフォンアプリのセキュリティ設定

© kaonavi, inc.

アプリ

スマートフォンアプリのセキュリティ設定

- パスコード/生体認証
- ログイン状態の保持設定
- スマートフォンアプリ/デバイスの利用許可設定
- スマートフォンアプリのアクセス設定
- ログイン端末の制限の利用
- その他セキュリティ設定

© kaonavi, inc.

アプリ

パスコード/生体認証

➢ **パスコード/生体認証**

パスコードを設定すると、アプリを起動するたびに（またはバックグラウンドから復帰するたびに）、パスコードの入力を求められるようになります。

なお、生体認証（Face IDまたは指紋認証）を設定し、ロックを解除することも可能です。

パスコード



Face ID



指紋認証



Point!

うっかり誰かに自身のスマートフォンを渡してしまったり、スマートフォンを紛失してしまったりしても、パスコードを設定しておけば**カオナビの情報を見られてしまう等のセキュリティリスクが低減できます。**

© kaonavi, inc.

アプリ

パスコード/生体認証

➢ パスコード/生体認証の設定方法

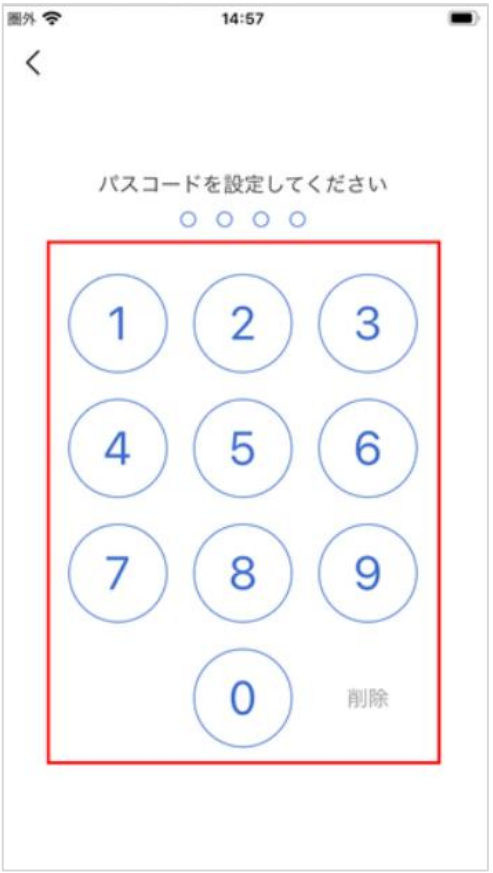
パスコードおよび生体認証の設定はユーザー自身でスマートフォンアプリ上から設定いただく必要があります。

設定はスマートフォンアプリTOPページの「アプリ設定」からパスコードや生体認証（Face ID、指紋認証）を設定できます。





Face ID/指紋認証を有効にしている端末の場合、
同画面から設定可能です



© kaonavi, inc.

アプリ

ログイン状態の保持設定

➢ ログイン状態の保持設定

「管理者メニュー＞スマートフォンアプリ管理＞基本設定＞ログイン状態の保持」より、アプリのログイン状態の設定をすることができます。

- **常に保持**：ユーザーがログアウトしない限り、ログイン状態を保持し続けます。
- **保持する時間を設定**：最終操作から設定した時間が経過すると、自動でログアウトされます。
  時間は最大336時間（14日）まで設定可能です。



Point!

- ”保持する時間を設定”に設定することで、一定時間経過後に自動ログアウトされるため、**スマートフォン紛失時に第三者がアプリにログインするリスクが低減**されます。
- 一方、ログイン状態を保持する時間が短い場合、頻繁にログインする必要があります。
  利便性向上のために**「ユーザーのログイン状態を保持」**しつつ、**「パスコードを設定」**することで
  セキュリティリスクを低減させる方法もございます。

© kaonavi, inc.

アプリ

スマートフォンアプリのアクセス設定

➢ スマートフォンアプリのアクセス設定

管理者メニュー＞アクセス管理に基づき、PCで利用可能な機能の中から、スマホアプリ側では利用させない機能を「管理者メニュー＞スマートフォンアプリ管理>スマートフォンアプリ管理＞アクセス設定」で個別に設定できます。
デバイスの特性に合わせた表示制御により、より安心してアプリを展開できます。

機能メニュー



Point!

・**アクセス管理で利用可能な機能のみ**、アプリ用アクセス設定で利用可/利用不可を設定できます。
・アクセス管理で利用不可の機能を、アプリ用アクセス設定で利用可にすることはできません。

© kaonavi, inc.

アプリ

ログイン端末の制限の利用

➢ ログイン端末の制限の利用

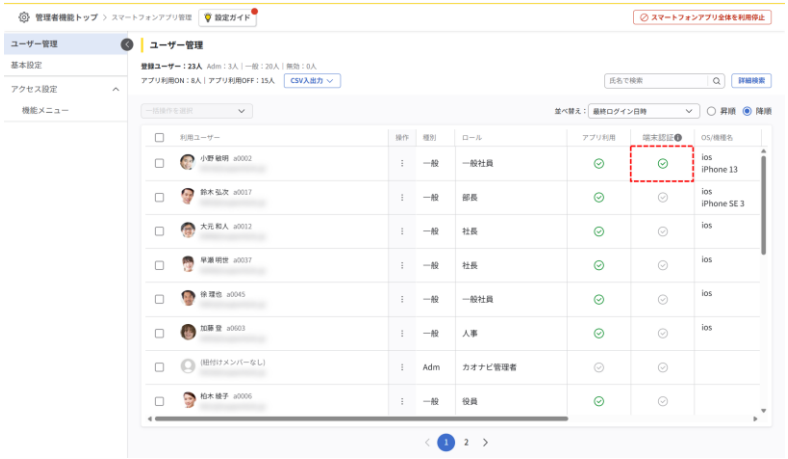
ログイン端末制限とは、ログインすることができる端末を制限、管理できる機能です。

「管理者メニュー＞スマートフォンアプリ管理＞基本設定＞ログイン端末制限機能の利用」から機能を有効にし、ユーザーがアプリからログインすると、利用している端末を今後ログインできる端末として登録し、登録以降はその端末でのみログインが可能になります。初回ログイン時に端末が認証されると、『利用ユーザーコントロール』の『端末認証』欄が有効となります。

ログイン端末制限機能の利用



ユーザー管理



Point!

・認証端末以外からアプリにログインすることができないようになるため、**不正ログインや未許可端末からのログインなどのセキュリティリスクの低減**を図ることができます。

© kaonavi, inc.

その他セキュリティ設定

➢ その他セキュリティ設定

・IPアドレス制限



「管理者メニュー＞IPアドレス制限」より設定いただけます。詳細設定方法はサポートサイトをご覧ください。

・ シングルサインオン（SSO）



「管理者メニュー＞シングルサインオン管理」より設定いただけます。詳細設定方法はサポートサイトをご覧ください。

※シングルサインオンによるログインは、IPアドレス制限の対象となります。
ただし、許可されているIPアドレスで、シングルサインオンによりログインをしたあとに許可されていないIPアドレスに移行した場合は、ログアウトするまで通常どおりアプリをご利用いただけます。



- シングルサインオン（SSO）とは、1つのIDとパスワードで認証を行い、複数のWebサービスやクラウドサービス、アプリケーションにアクセスする仕組みです。
- SSOを利用することで、**ユーザーの利便性の向上/パスワード漏洩リスクの低減/ID・PWの管理工数の削減**につながります。
- カオナビへのログインをSSO認証に限定することも可能です。詳細はサポートサイトをご覧ください。
- 既にSSOを社内でご利用の場合は、設定を追加することでカオナビでもご利用いただけます。

© kaonavi, inc.

アプリ

その他セキュリティ設定

➢ **その他セキュリティ設定**

・スクリーンショット・画面収録制限の利用

カオナビアプリ画面のスクリーンショットや動画収録を行った際、保存された画像や動画が自動的に黒い画面に置き換わります。

詳細設定方法はサポートサイトをご覧ください。

・ファイル保存制限の利用

カオナビアプリ内の添付ファイルに対して、「ブラウザで開く」「デバイスに保存」の操作ができないよう制御できます。

詳細設定方法はサポートサイトをご覧ください。

・ 外部ブラウザ起動制限の利用

カオナビアプリ内の外部リンクをタップしても、ブラウザで遷移できないよう制御できます。

詳細設定方法はサポートサイトをご覧ください。

Point!

- 本設定を行うことで、アプリ上で表示される情報の保護が可能です。
- スクリーンショット・画面収録制限の利用、ファイル保存制限の利用、外部ブラウザ起動制限の利用は「管理者メニュー＞スマートフォンアプリ管理>基本設定」から設定できます。

© kaonavi, inc.