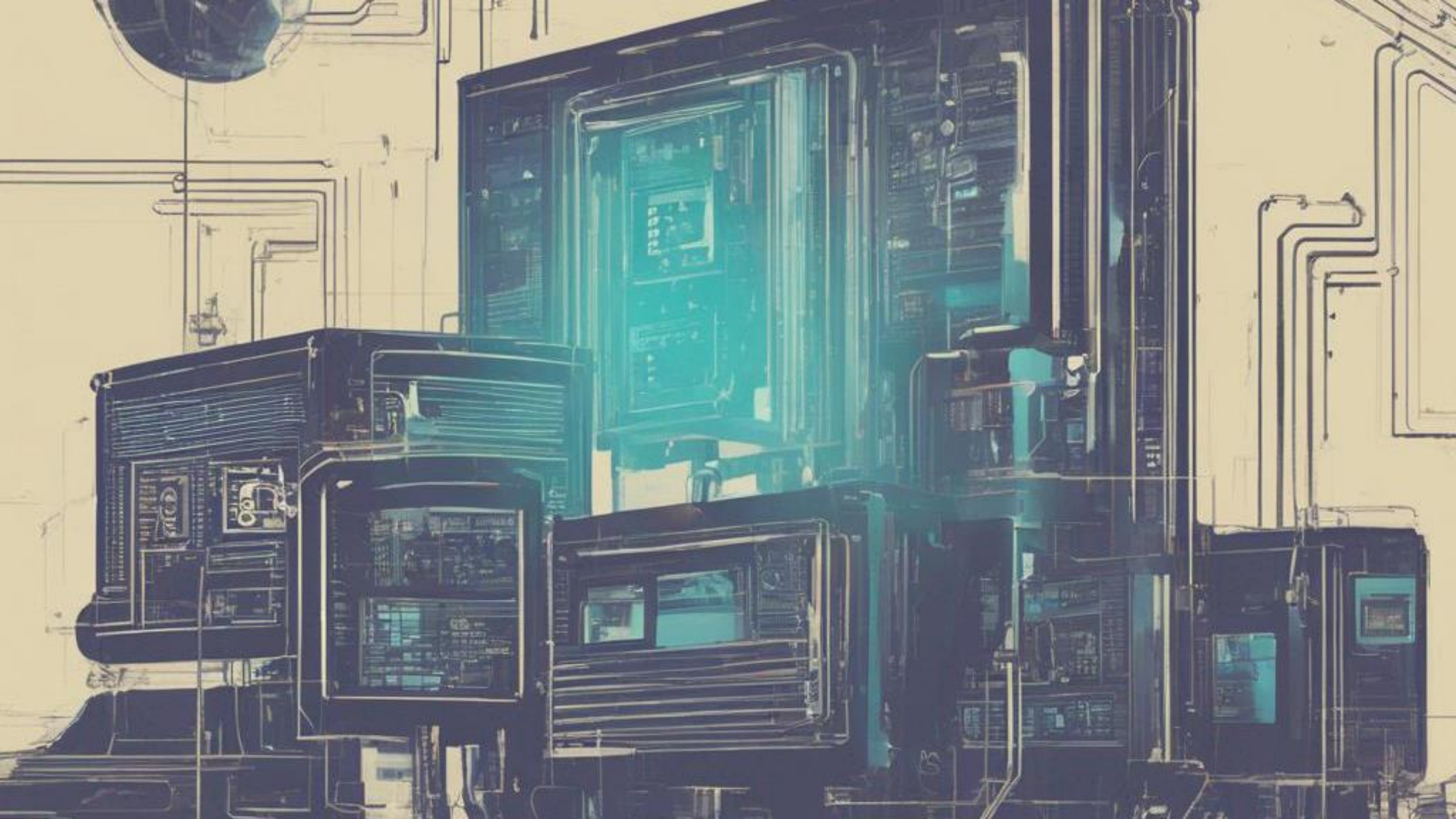


BaroPAM

Co., Ltd. ilsung



本人確認の現状

IDとパスワードのみで、
確認された情報が実際に
持っている人と一致するかを判断できない。

ログインの現状

既存のセキュリティでの限界点

- ・ 認証サーバ方式であるため、トラブルが発生した場合、システムの認証速度が低下し、利用不可能となる可能性
- ・ ハードウェアの購入と設置に伴う追加費用が発生
- ・ 認証サーバのハッキングの危険性が存在

1

ユーザーネーム＋パスワードでログイン

2

乗っ取りの原因になるため、弱規定の制限などが必要。

BaroPAM

BaroPAMとは

ワンタイムパスワード取り入れた
3段階認証方式のソリューション

3 段階認証方式とは？

生体認証

1

指紋、顔、瞳などの**生体情報**を使用

生体情報ユーザーID＋パスワード

2

既存に登録したIDとパスワードを入力

ワンタイムパスワード入力

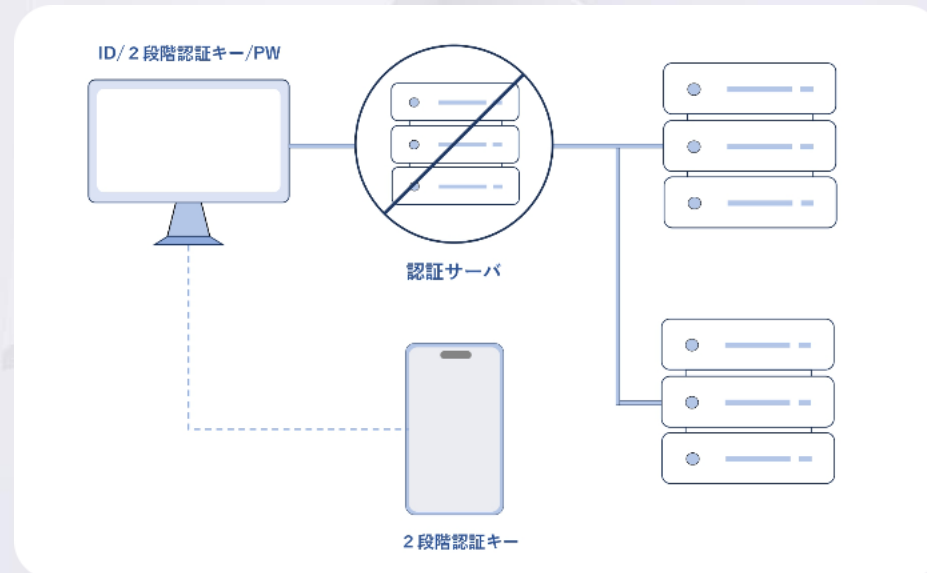
3

常に変わり続けるアルゴリズムによって生成された**ワンタイムパスワード**を入力

BaroPAMのメカニズム

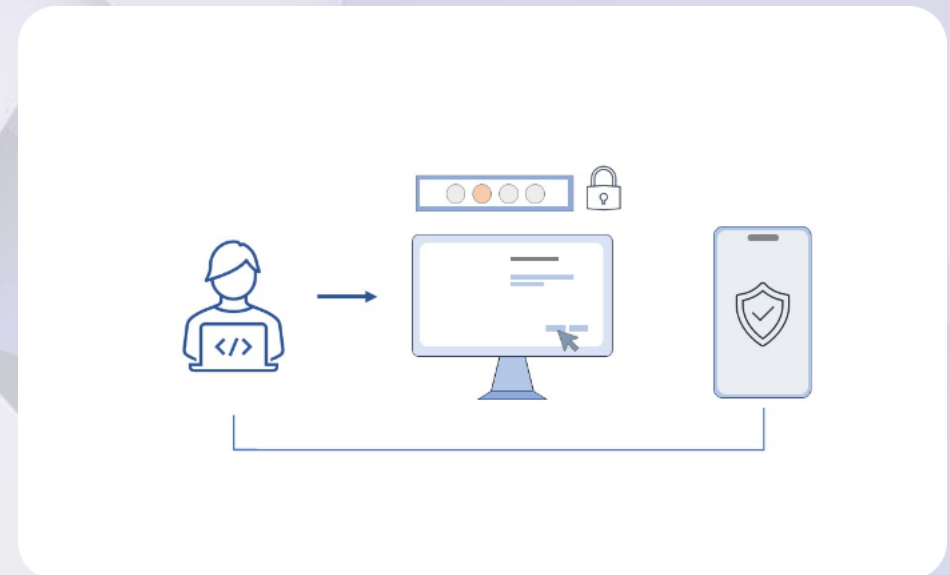
PAM方式(Pluggable Authentication Modules)を使っているため、

手軽に操作できてさらにセキュリティ強化が可能



認証サーバーを使わない

ソフトウェアモジュールを使っているため、
認証サーバーが不要ない。



スマートフォンでワンタイムパスワード

アルゴリズムにより、特定の時間ごとに変更される
パスコードをスマートフォンで確認可能

適用対象

- 1 Windows / Mac
- 2 Linux/Unix など
- 3 アプリケーションログイン
- 4 サーバー・ネットワーク

BaroPAMの機能

認証サーバーを
購入する必要が
ない
モジュール認証
方式

512Bit 標準Hash
関数を利用し
暗号化すること
によって
より強力的な
セキュリティ

C, Java
多様なOS
Windows, Linux,
MacOS
サーバー, アプリ
ケーションに適用
可能

画面保護機, ロック
防止, 解除機能
スマートフォン
紛失時アプリケー
ションLook機能.
OTP生成周期
細分化可能

BaroPAM 適用プロセスの仕組み



BaroPAM Manager - v1.0.20

制限回数(1~10 回):

制限時間(15~600 秒):

Key method:

サイクルタイム(3~60 秒):

Secure key:

ACL タイプ ☒ キャンセル ☐ 許可

中間者攻撃を防ぐには? ☒ はい ☐ いいえ

緊急用ワンタイムパスワード

追加

11111111
22222222
33333333
44444444
55555555

ACL ユーザー名

追加

追加機能

サーバー名 ユーザー名

環境設定 ☒ 共有 ☐ ユーザー名 ☐ BLE適用 ☐ 自動ログイン ☐ スクリーンセーバー

☐ データベース相互接続 ☐ BLE相互接続アプリケーション ☒ 生体認証相互接続

☐ HTTP相互接続 >>

閉じる ヘルプ 削除 ログ表示 コピー 更新 保存

制限時間内のログイン制限回数を1~10の中から入力。(5回推奨)

上記の制限時間を15~600の中から入力。(30秒推奨)

app512を選択。

サイクルタイムを3~60秒の中から入力。(20秒推奨)

購入時に頂いたセキュリティーを入力。

緊急用ワンタイムパスワードを最大5つまで登録できる。
(ワンタイムパスワードを生成できない場合に使用するもの)
1度使用したワンタイムパスワードは自動的に削除される。

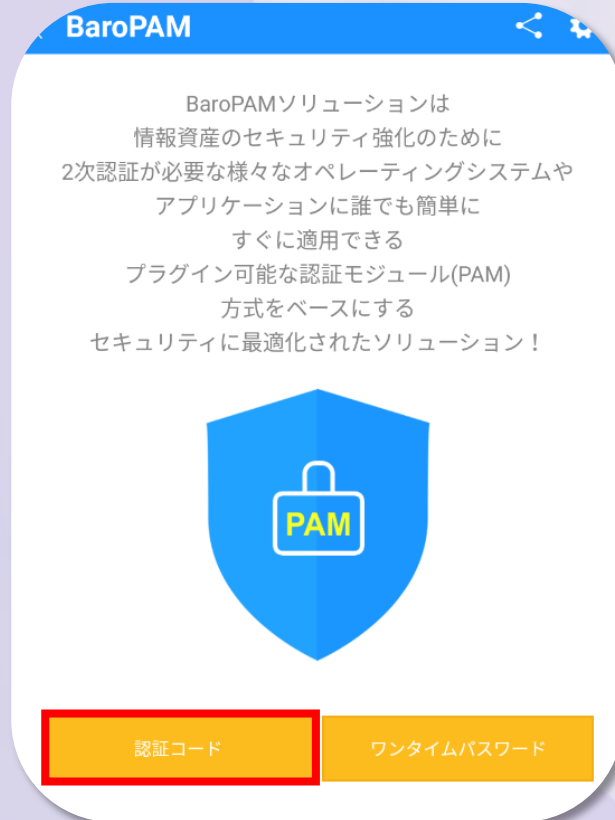
任意の名前を入力。

ユーザー名 + ¥ + ワークグループ名を書く

顔認証を設定

設定が終われば必ず保存を押す。

2 段階認証設定方法



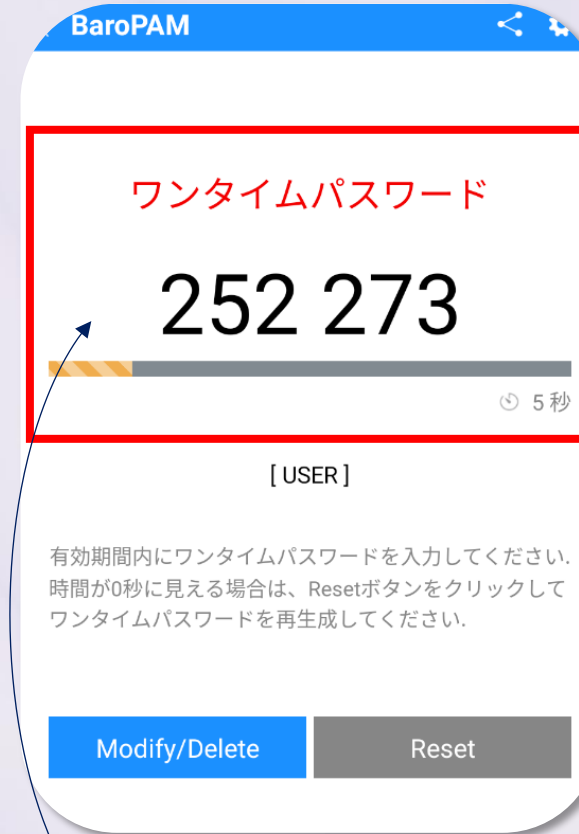
BaroPAMを適用したい
アプリケーション名を
入力する
(任意でも構いません)

購入時配布されたsecure keyを
入力する

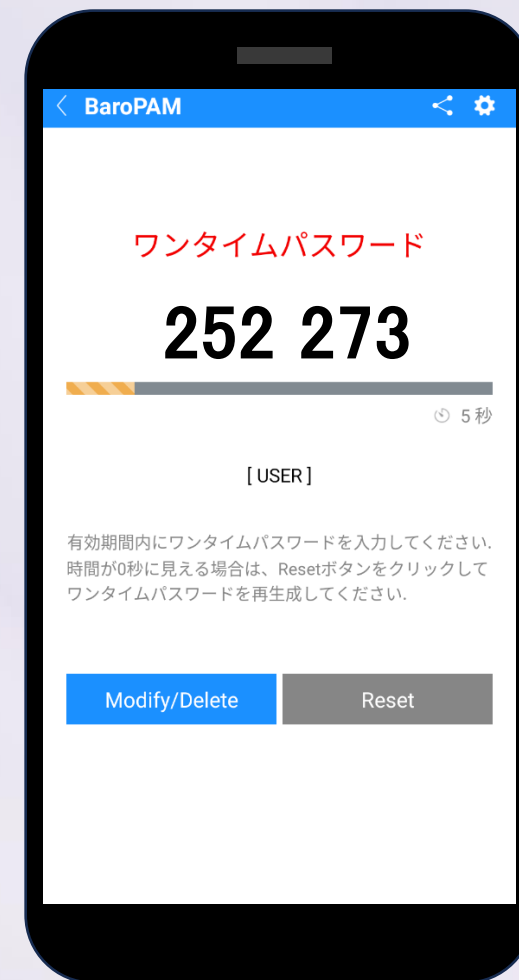
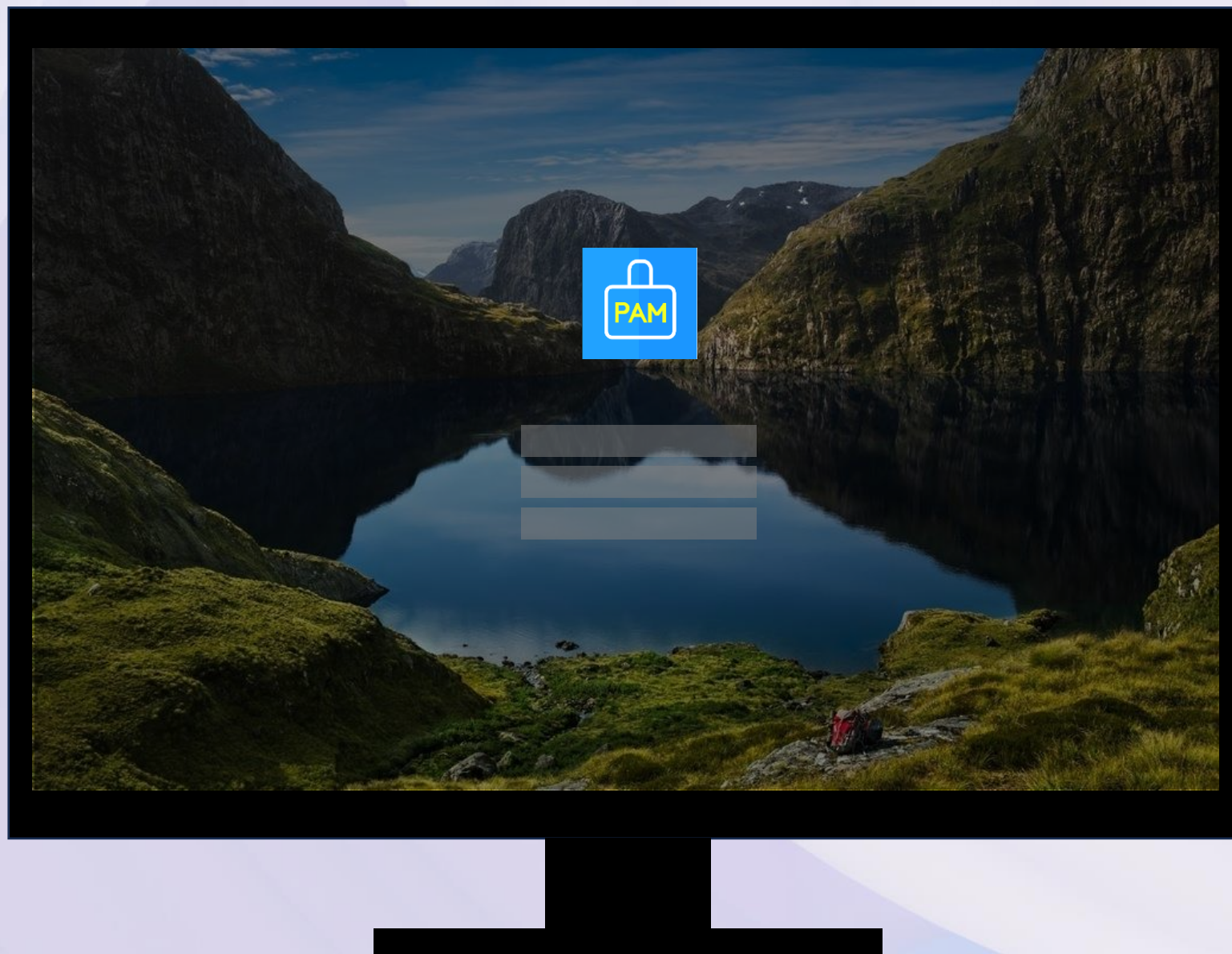
生成周期 (サイクルタイム) を
3~60秒の間で入力する

入力が終わったら
Saveを押す

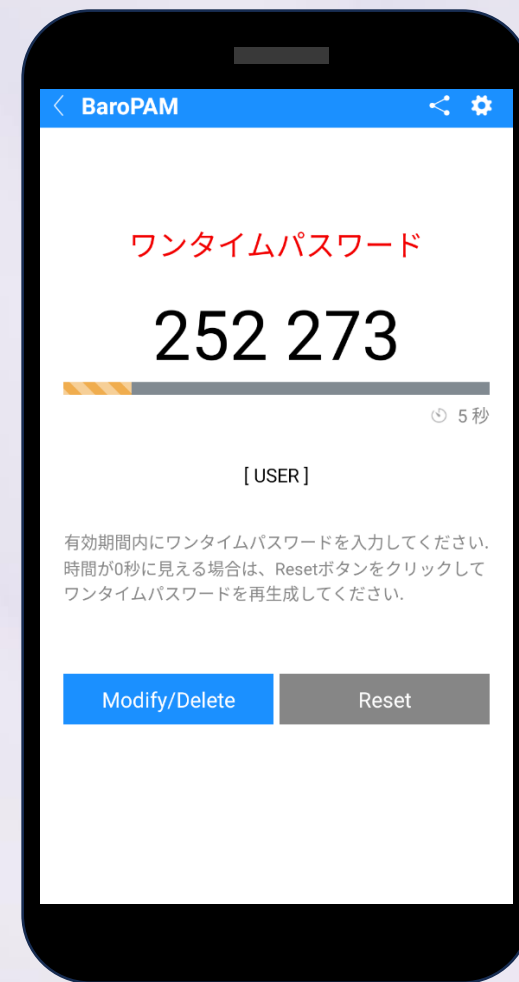
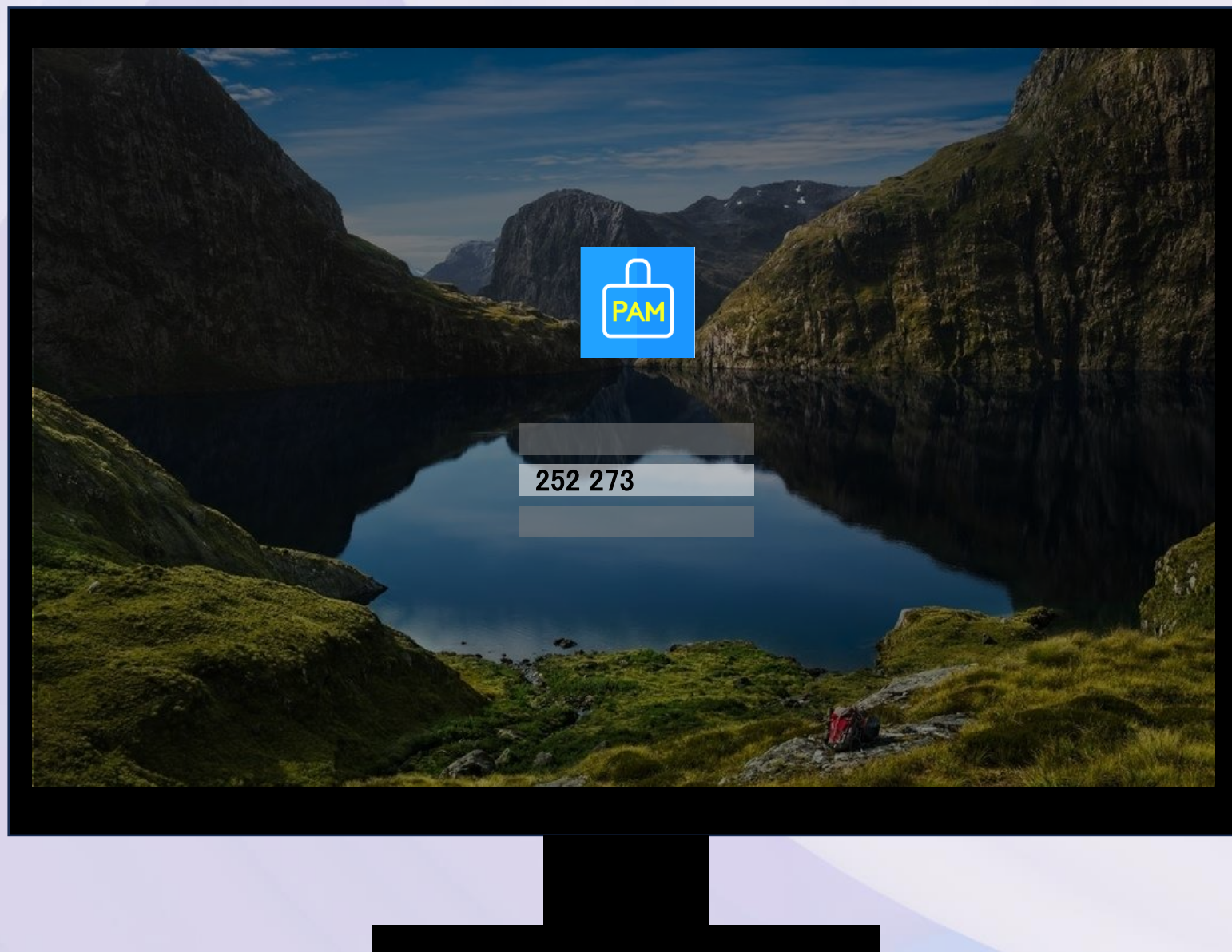
2 段階認証設定方法



ワンタイムパスワードが表示される



ワンタイムパスワードを入力



ワンタイムパスワードを入力

BaroPAM

株式会社日成情報