YubiOn FIDO Logon Standalone

管理者向け クイックスタートガイド

株式会社 ソフト技研

2026年8月版

目次

このガイドについて

本書は、**YubiOn FIDO Logon Standalone**（以下、本製品）を **1 台の端末に導入し、認証器（YubiKey などの FIDO2 セキュリティキー）で Windows にログオンできる状態にする** までの手順を、最短の一本道でまとめたものです。

- **所要時間の目安:** 約 30 分（ライセンスファイルが手元にある場合）
- **対象:** これから本製品を初めて試す管理者
- **前提知識:** Windows の管理者権限での操作

分岐のある設定や運用設計、詳しい仕様は説明していません。詳細は別冊の「**管理者マニュアル**」を参照してください。本書の各 STEP の末尾に、対応する章を示しています。

全体の流れ

STEP	内容
STEP 1	インストールする
STEP 2	ライセンスを登録する
STEP 3	マスターキーを登録する
STEP 4	ユーザーに認証器を割り当てる
STEP 5	リカバリコードを発行する
STEP 6	認証器ログオンを有効にする
STEP 7	ログオンを試す
STEP 8	セキュアモードを有効にする

> **STEP の順序について**　STEP 3（マスターキー）と STEP 5（リカバリコード）を、ログオンを有効にする前に行います。認証器が 1 本もない状態では STEP 6 の有効化ができないこと、および認証器がすべて使えなくなったときにログオン手段を失わないようにするためです。**順番どおりに進めてください。**

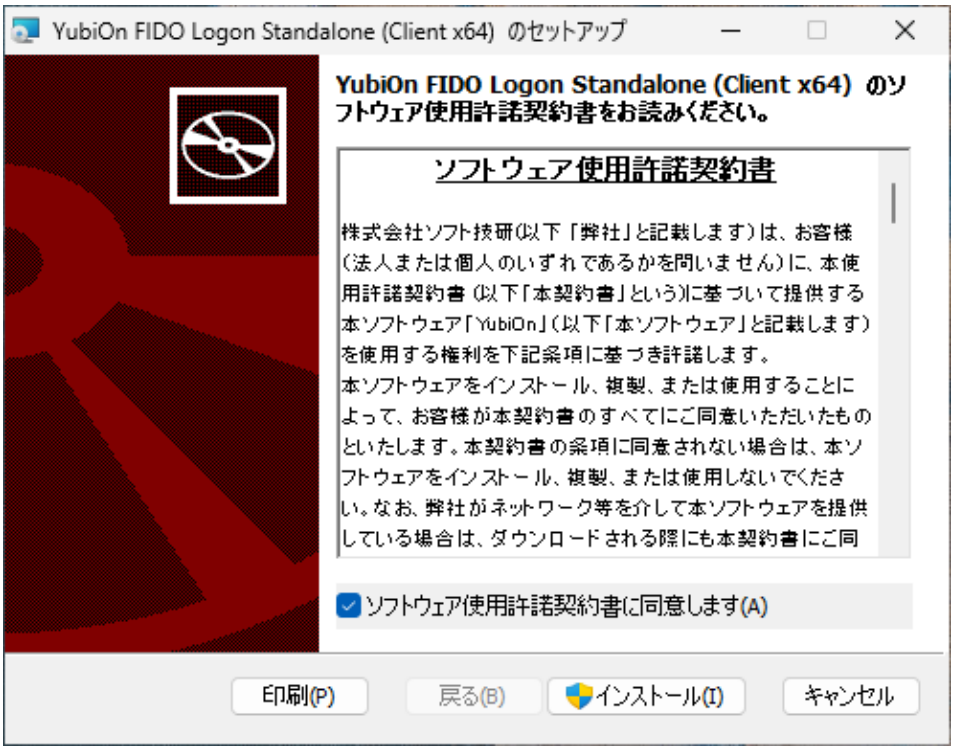
事前に用意するもの

用意するもの	補足
対応 OS の端末	Windows 10（20H2 以降）／Windows 11／Windows Server 2022 以降
MSI インストーラー	**サーバー用とクライアント用で別のファイル**です。端末の OS 種別に合ったものを用意します
ライセンスファイル	未入手の場合は STEP 2 でマシンコードを取得し、発行元へ依頼します
FIDO2 認証器	FIDO2 対応であれば YubiKey 以外も使用できます
管理者権限	インストール・設定ツールの操作に必要です

> **注記**　本書はローカルコンソール（端末に直接ログオン）での利用を前提にしています。RDP 経由での FIDO ログオンには追加の要件があるため、管理者マニュアル 第2章を参照してください。

STEP 1　インストールする

1. OS 種別に対応した **MSI インストーラー** を実行します。
2. 画面の指示に従ってインストールを進めます。
3. インストールが完了すると、Windows サービス `YubiOnFidoStandaloneService` が自動的に開始されます。



図：MSI インストーラーのウィザード画面

> **「Windows によって PC が保護されました」と表示されたら**　Microsoft Defender Smart Screen の標準的な確認画面です。「**詳細情報**」→「**実行**」の順に選択すると続行できます。

この時点では、まだ FIDO ログオンは有効になっていません。続けて STEP 2 に進みます。

> 詳細は管理者マニュアル 第3章「インストール」を参照してください。

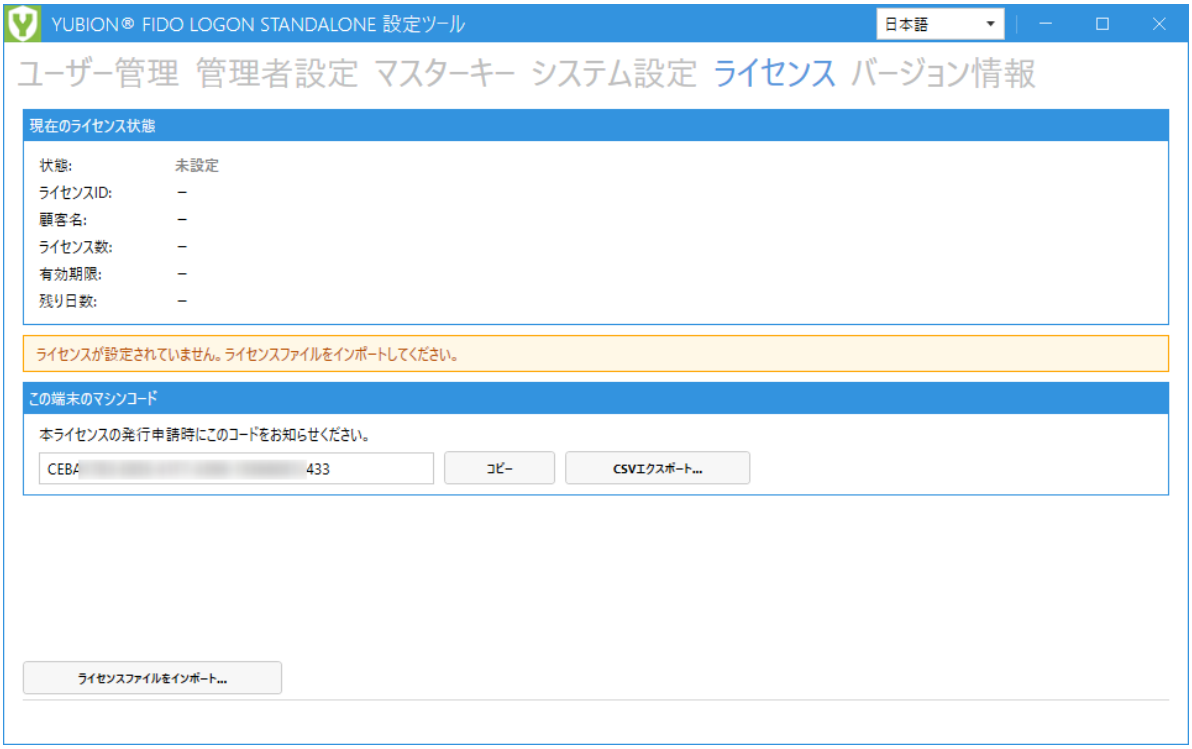
STEP 2　ライセンスを登録する

本製品の動作には有効なライセンスが必要です。ライセンスが有効でない間は、FIDO ログオンは動作しません。

設定ツールを起動する

STEP 2 以降の操作は、すべて **設定ツール** で行います。

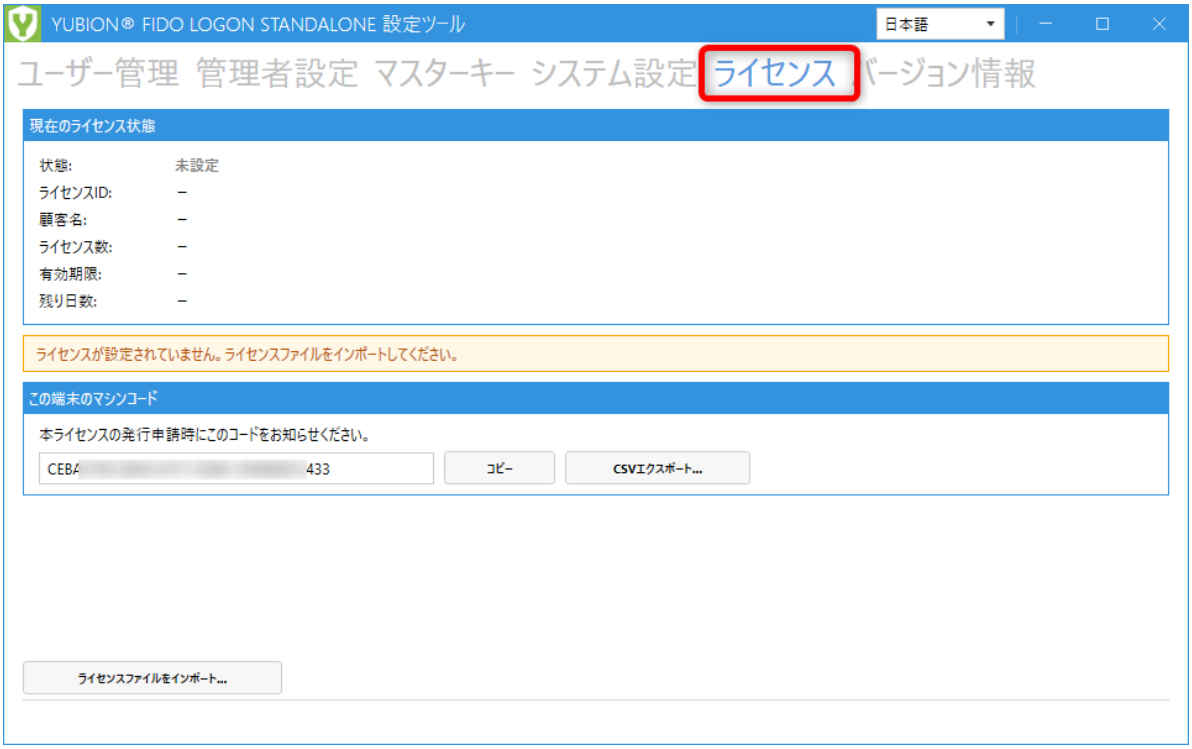
1. スタートメニューから「**すべてのアプリ**」を開き、「**YubiOn FIDO Logon Standalone Settings Tool**」を選択します。
2. ユーザーアカウント制御（UAC）の確認画面で「**はい**」を選択します。



図：設定ツールのメイン画面

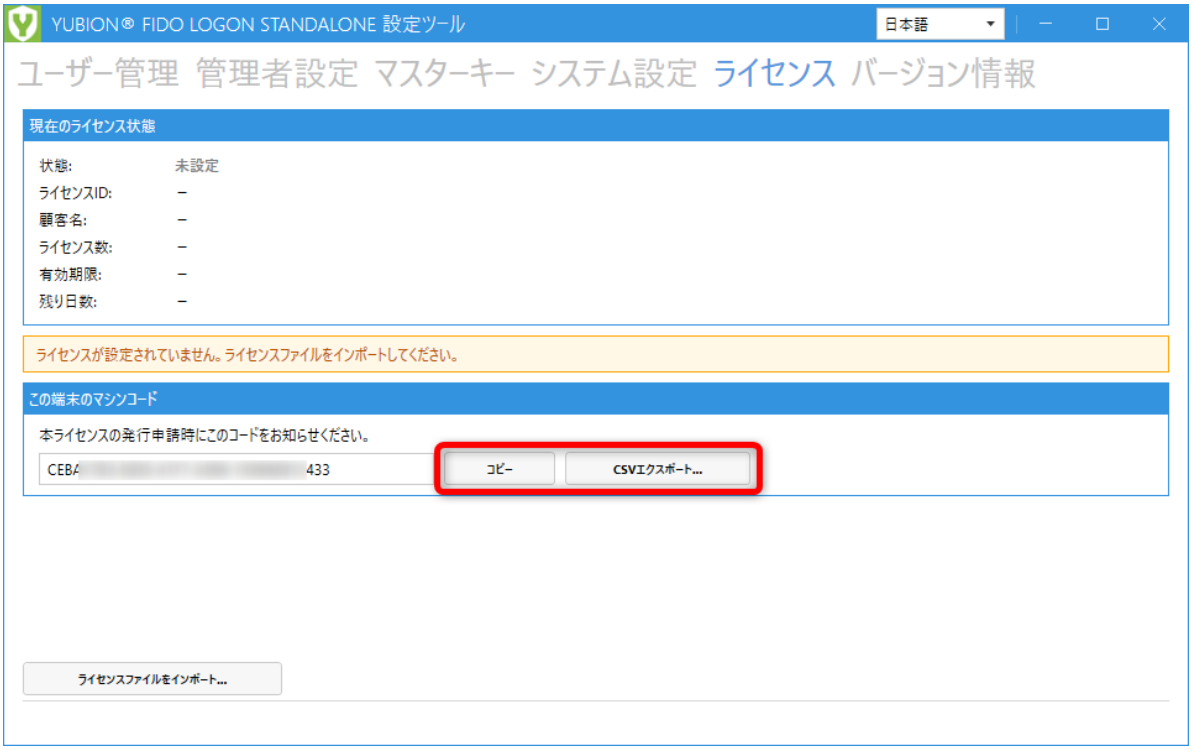
ライセンスファイルを登録する

1. **ライセンス** タブを開きます。



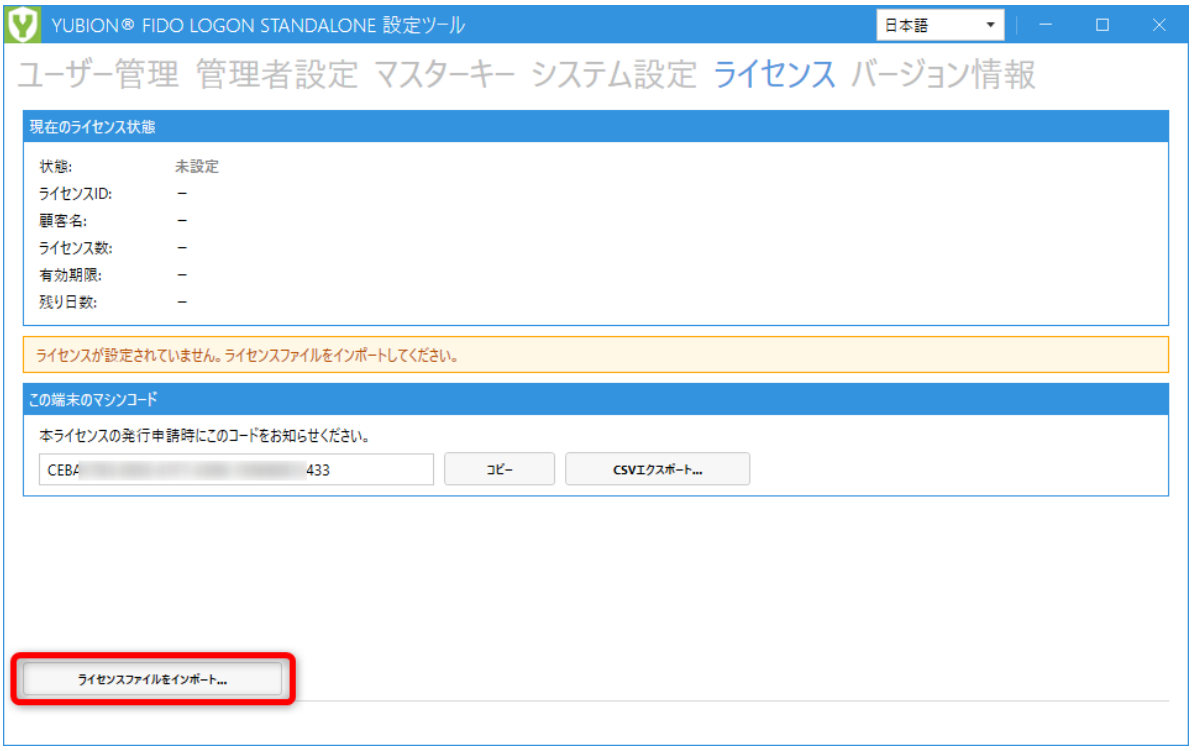
図：ライセンスタブ

2. ライセンスファイルが未入手の場合は、「**この端末のマシンコード**」欄の値を「コピー」で取得し、ライセンス発行元へ提出して発行を依頼します。



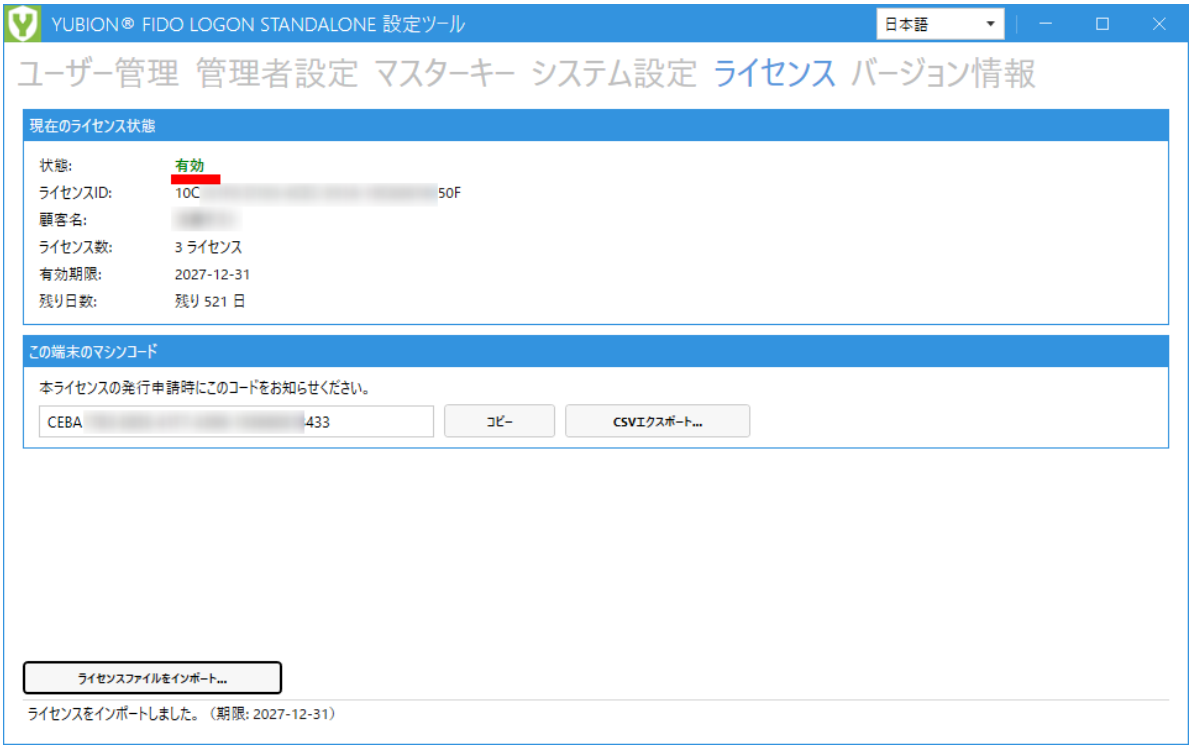
図：マシンコードのコピーボタン

3. 「**ライセンスファイルをインポート...**」を選択し、受け取ったライセンスファイルを指定します。



図：ライセンスファイルをインポートボタン

4. ライセンス状態が「**有効**」になったことを確認します。



図：ライセンスが有効化された状態

> **インポートできないとき**は　ライセンスは **端末（マシンコード）** と **OS 種別（サーバー／クライアント）** に紐づきます。「端末不一致」「OS 種別不一致」と表示された場合は、その端末向けに発行されたファイルか、OS 種別が合っているかを確認してください。

> 詳細は管理者マニュアル 第5章「ライセンスの登録」を参照してください。

STEP 3　マスターキーを登録する

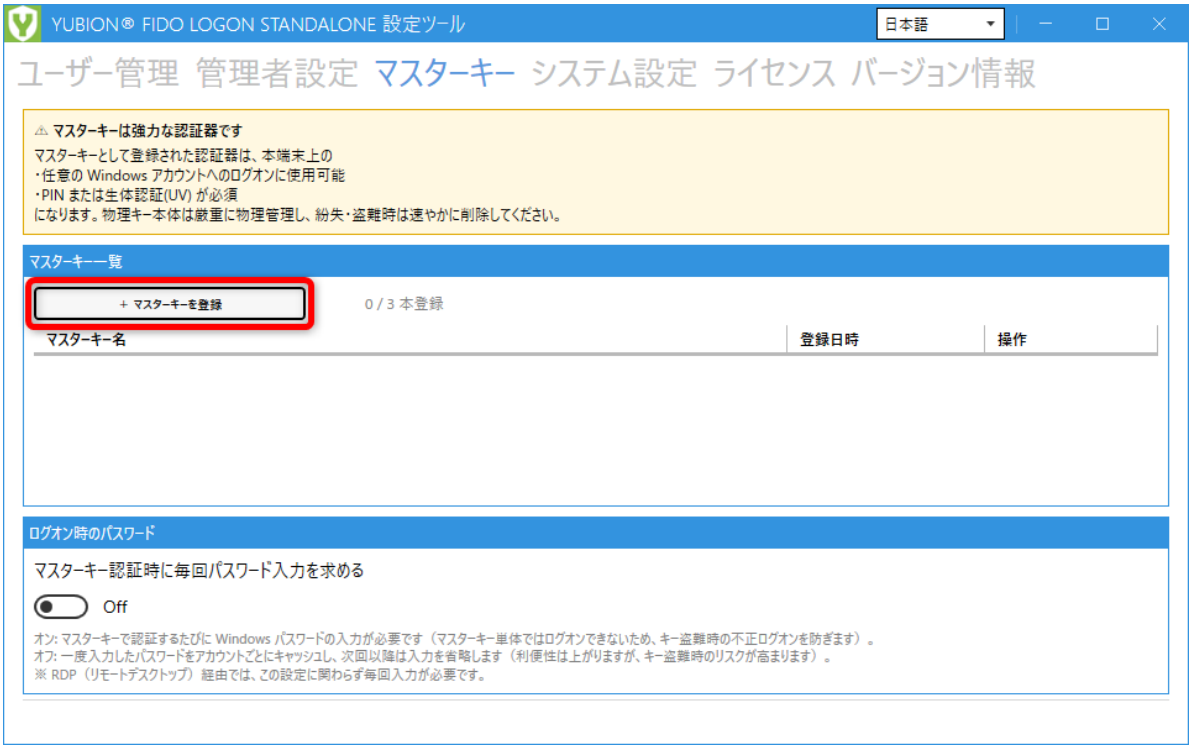
マスターキー は、割り当てを問わず **任意の Windows アカウントへログオンできる管理者用の認証器** です。ユーザーの認証器が故障・紛失・PIN ロックしたときの代行ログオン手段になります。

ここで 1 本登録しておくと、STEP 6 の「認証器ログオンを有効にする」の前提（ログオンに使用できる認証器が 1 本以上）も満たせます。

1. **マスターキー** タブを開きます。

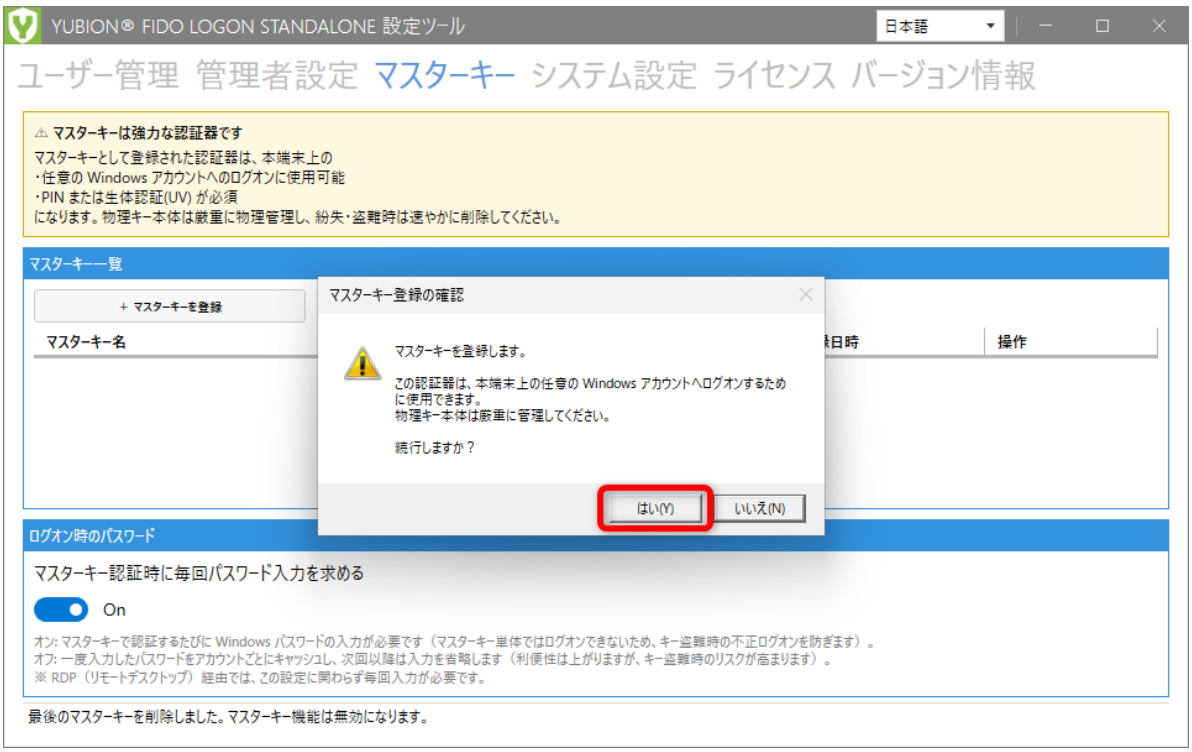
図：マスターキータブ

2. 「＋ **マスターキーを登録**」を選択します。



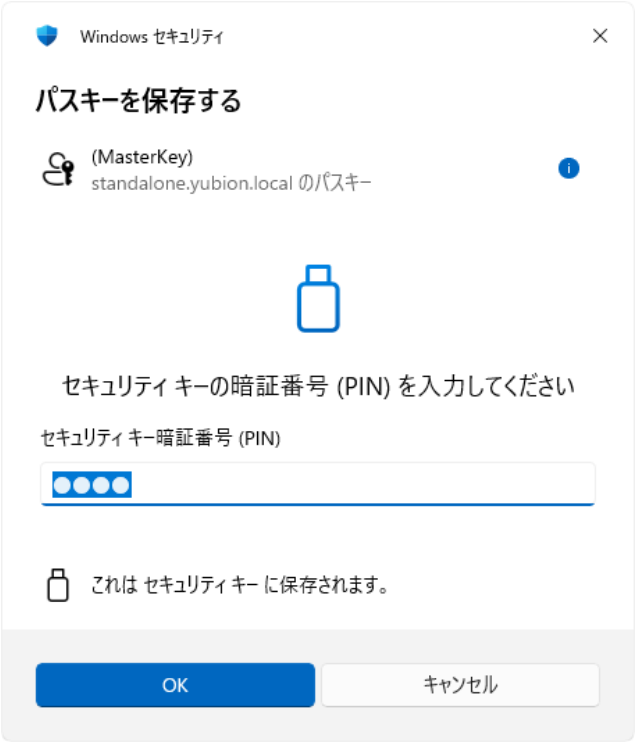
図：「＋ マスターキーを登録」ボタンを選択

3. 「任意の Windows アカウントへログオンできる」旨の確認ダイアログで「**はい**」を選択します。



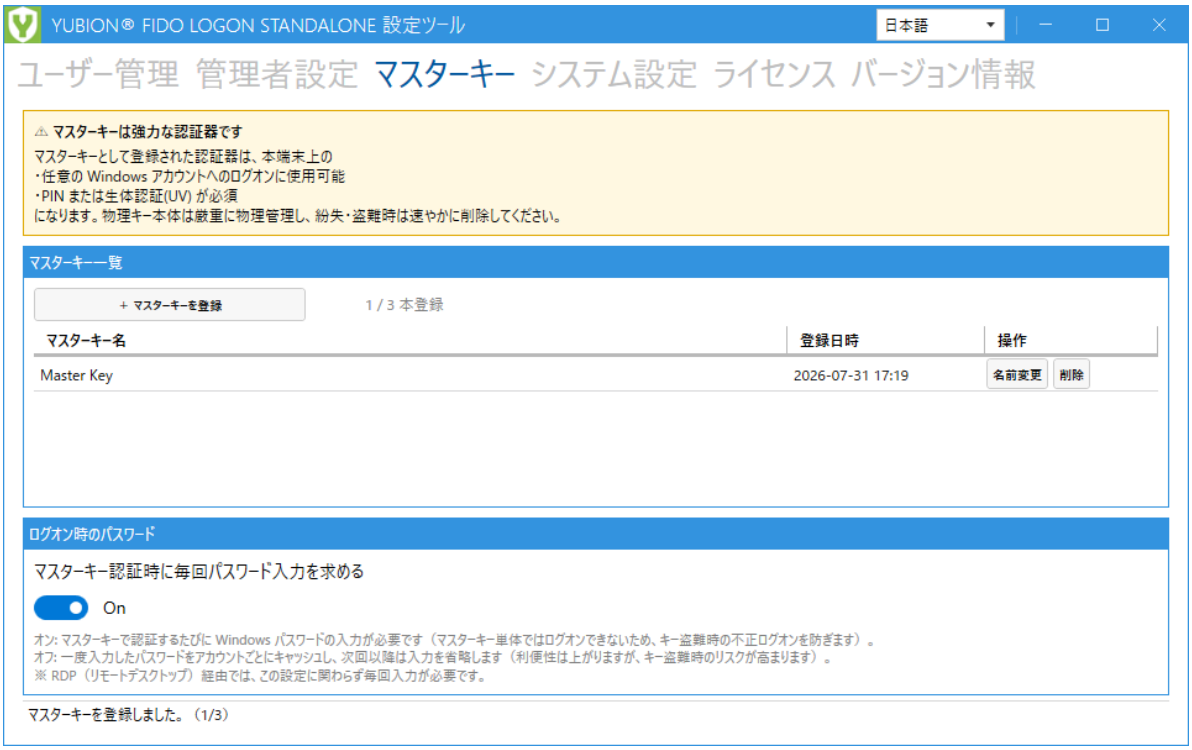
図：マスターキー登録の確認ダイアログ

4. 認証器を接続し、PIN（または生体認証）を入力して、認証器にタッチします。PIN が未設定の認証器では、ここで PIN の設定（最小 4 文字）を求められます。



図：PIN 入力ダイアログ

5. 名前の設定ダイアログで、管理しやすい名前（例: 管理者用YubiKey）を入力します。「マスターキー一覧」に追加されれば完了です。



図：マスターキー一覧に追加された状態

> **注意**　マスターキーは任意のアカウントにログオンできる強力な鍵です。**個人が物理的に管理し、共用しないでください。** 紛失した場合は、速やかに設定ツールから削除してください。

> 詳細は管理者マニュアル 第9章「マスターキーの管理」を参照してください。

STEP 4　ユーザーに認証器を割り当てる

ユーザーが FIDO ログオンに使う認証器を、管理者が事前に登録します。**まずは動作確認用に、ご自身のアカウントで 1 本登録** してみてください。

1. **ユーザー管理** タブを開きます。

図：ユーザー管理タブ

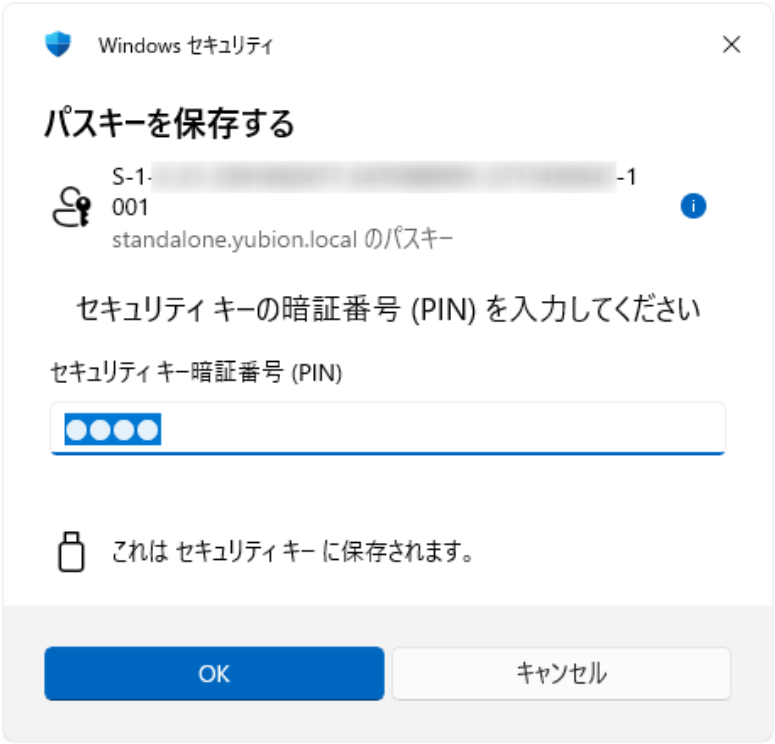
2. 対象の Windows アカウントを選択します。

図：対象の Windows アカウントを選択

3. 「**認証器を割り当て**」を選択します。

図：「認証器を割り当て」ボタンを選択

4. 認証器を接続し、PIN（または生体認証）を入力して、認証器にタッチします。



図：PIN 入力ダイアログ

5. 名前の設定ダイアログで名前（例: YubiKey5-NFC）を入力します。「登録済み認証器」の一覧に追加されれば完了です。

図：登録済み認証器の一覧に追加された状態

一覧に対象ユーザーが表示されないときは　一覧には、その端末に **ユーザープロファイルが作成済み**（一度でもログオンしたことがある）のアカウントのみが表示されます。先に本人が一度サインインしてください。

注記　一覧のアカウント名は、種類によって次の形式で表示されます。

- **ローカルアカウント:** 端末名¥アカウント名
- **Microsoft アカウント:** MicrosoftAccount¥アカウント名
- **Active Directory アカウント:** ドメイン名¥アカウント名
- **Entra ID（Azure AD）アカウント:** AzureAD¥メールアドレス

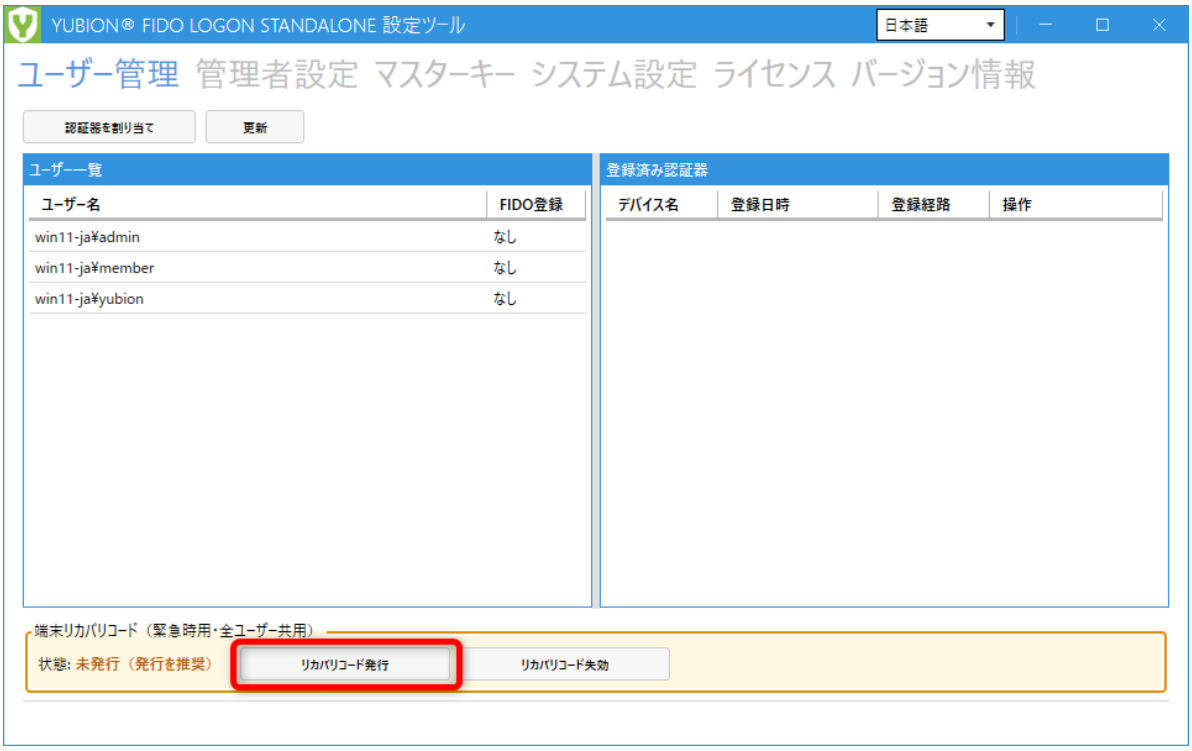
詳細は管理者マニュアル 第8章「認証器（ユーザー）の登録と管理」を参照してください。ユーザー自身に初回ログオン時に登録させる「自己登録」方式も同章で説明しています。

STEP 5　リカバリコードを発行する

リカバリコード は、**認証器を一切使わずに** 緊急ログオンできる唯一の手段です。認証器は PIN の連続入力ミスでロックしますが、本製品はこのロックを検知できません。登録済みの認証器とマスターキーがすべて使えなくなり、リカバリコードも未発行の場合、**ログオンできなくなり、設定変更では復旧できません。**

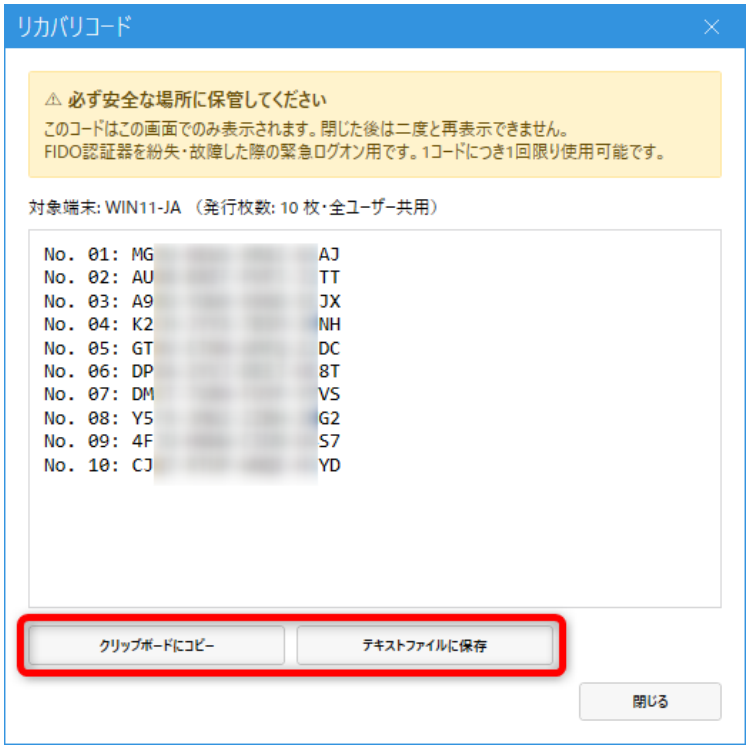
> **重要**　リカバリコードの発行は、**端末導入時の必須手順** として実施してください。

1. **ユーザー管理** タブ下部の「端末リカバリコード（緊急時用・全ユーザー共用）」欄で「**リカバリコード発行**」を選択します。



図：リカバリコード発行ボタン

2. 表示された 10 個のコードを「クリップボードにコピー」または「テキストファイルに保存」で **安全に保管** します。



図：リカバリコード発行ダイアログ

> **コードは発行直後に一度だけ表示されます。** 画面を閉じると再表示できません。必ずこの時点で保管してください。

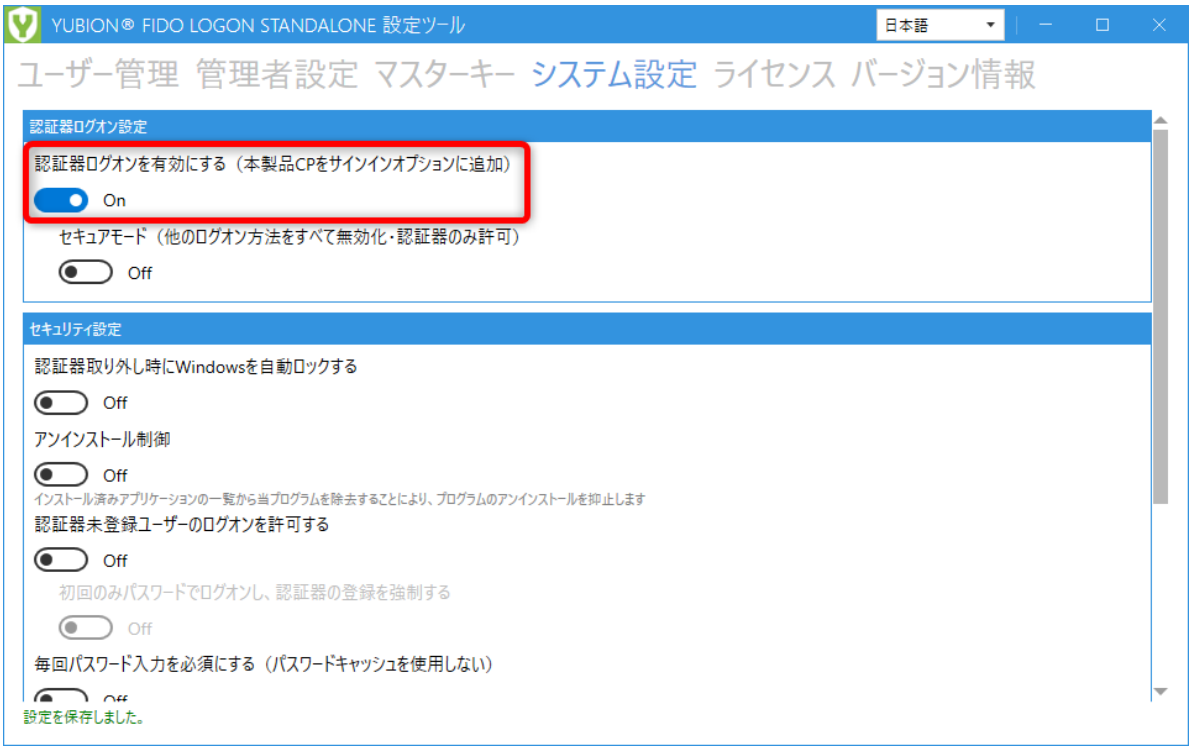
- リカバリコードは **端末単位（全ユーザー共用）** で、一括 10 枚発行されます。1 つのコードは 1 回だけ使用できます。
- リカバリコードだけではログオンできません。**Windows パスワードの併用が必要** です。

> 詳細は管理者マニュアル 第10章「リカバリコードの管理」を参照してください。

STEP 6　認証器ログオンを有効にする

ここまでの設定を、実際のログオン画面に反映します。

1. **システム設定** タブを開きます。
2. 「**認証器ログオンを有効にする（本製品 CP をサインインオプションに追加）**」を有効にします。



図：認証器ログオンを有効にする設定

これで、Windows のログオン画面に FIDO ログオンのタイルが表示されるようになります。

- ログオンに使用できる認証器が **1 本もない場合は有効にできません**（STEP 3・STEP 4 が完了していれば問題ありません）。
- 登録済みの認証器・マスターキーがすべて削除されて 0 本になると、この設定は自動的に無効へ戻ります。

> 詳細は管理者マニュアル 第7章「基本設定」を参照してください。

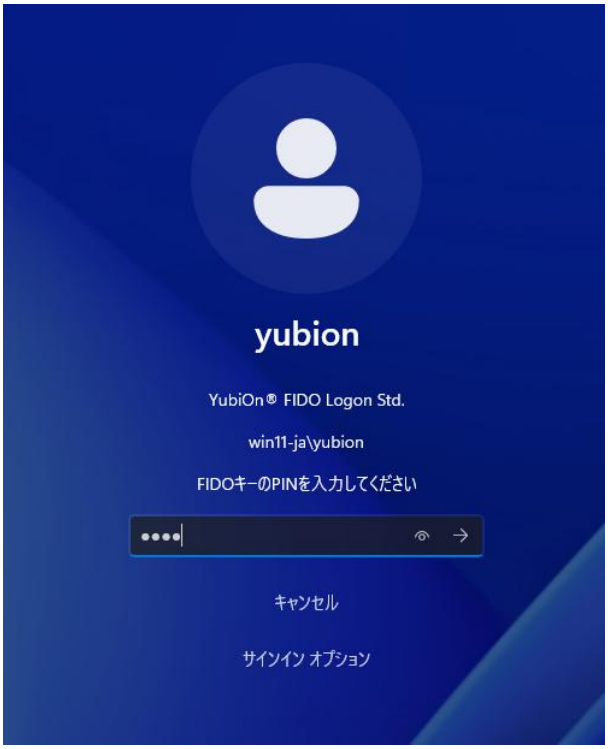
STEP 7　ログオンを試す

設定が反映されたか、実際にログオンして確認します。Windows からサインアウト（またはロック）してください。

1. ログオン画面で、本製品の **FIDO ログオン用タイル** を選択します。

図：FIDO ログオン用タイルを選択する

2. 認証器を接続し、**PIN** を入力します。



図：PIN を入力する画面

3. 認証器にタッチします。

図：認証器へのタッチを求める画面

4. **初回のみ**、Windows パスワードの入力を求められます。入力するとログオンが完了します。

図：Windows パスワードを入力する画面

入力したパスワードは端末内に暗号化して保存されるため、**2 回目以降は PIN 入力とタッチだけでログオン** できます。

> **この時点では、パスワードのみのログオンも引き続き可能です。** 認証器を使わないログオンを禁止するには、STEP 8 に進みます。

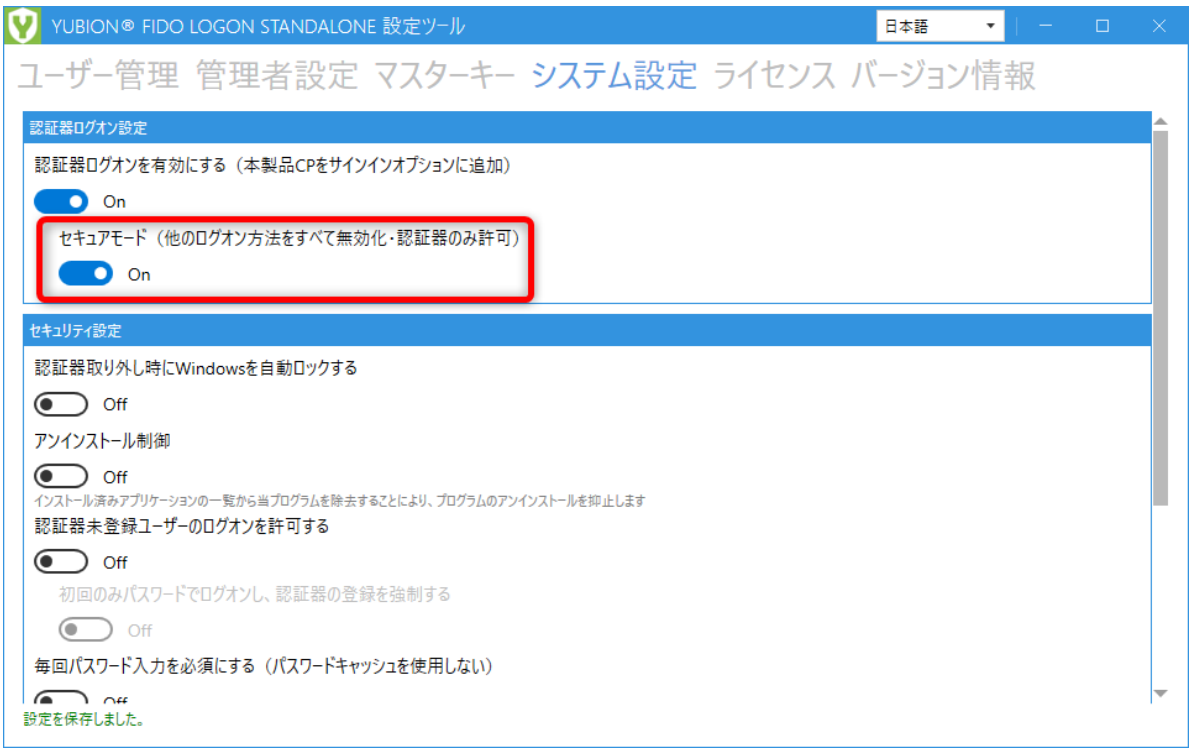
> ログオン時のユーザー向けの操作は、別冊「**エンドユーザー向け 操作マニュアル**」で説明しています。

STEP 8　セキュアモードを有効にする

セキュアモード を有効にすると、他のログオン方法（パスワードなど）がすべて無効化され、**認証器によるログオンだけに限定** されます。本番運用に移行する段階で有効にします。

> **警告**　セキュアモードを有効にすると、**認証器が未登録のユーザーはパスワードでログオンできなくなります。** 有効化する前に、次をすべて満たしていることを確認してください。
>
> - その端末を使う **全ユーザーの認証器登録が完了している**（STEP 4）
> - **マスターキーを登録済み**（STEP 3）
> - **リカバリコードを発行し、安全に保管済み**（STEP 5）

1. **システム設定** タブを開きます。
2. 「**セキュアモード（他のログオン方法をすべて無効化・認証器のみ許可）**」を有効にします。



図：セキュアモードを有効にする設定

3. サインアウトし、ログオン画面に FIDO ログオン以外のタイルが表示されないことを確認します。

- 有効にするには「認証器ログオンを有効にする」（STEP 6）が前提です。

- **RDP 経由のログオンにセキュアモードは必須ではありません。** ただし OFF の場合は RDP でもパスワードログオンが併用できるため、RDP でも FIDO 認証を必須にしたい場合は ON にしてください。

> 詳細は管理者マニュアル 第7章「基本設定」を参照してください。認証器がすべて PIN ロックした場合の備えについては、同 第8章「PIN の入力ミスによる認証器ロックへの備え」もあわせて確認してください。

うまくいかないときは

ログオン画面に FIDO ログオンのタイルが表示されない

次の順に確認してください。

1. ライセンス状態が「**有効**」か（STEP 2）。有効でない場合、タイルは表示されません。
2. 「**認証器ログオンを有効にする**」が有効か（STEP 6）。
3. 対象ユーザーに認証器が登録されているか（STEP 4）。

設定ツールで認証器を登録（割り当て）できない

1. **Windows の「パスキーアクセス」がオフになっていないか。** **設定** → **プライバシーとセキュリティ** → **パスキー** の「**パスキーアクセス**」が **オフ** だと、認証器・マスターキーの登録ができません。**オン** にしてから登録し直してください（この項目は比較的新しい Windows 11 にのみ存在します）。
2. **対象ユーザーが一覧に表示されているか。** プロファイル作成済みのアカウントのみ表示されます（STEP 4）。
3. **認証器が FIDO2 に対応しているか。** U2F（CTAP1）専用キーは既定では登録できません。

ライセンスが「端末不一致」「OS 種別不一致」になる

- 別の端末向けのライセンスファイル、または OS 種別（サーバー／クライアント）が異なるライセンスを登録していないか確認してください。
- **PC 本体の入れ替えやマザーボードの交換を行った端末** では、マシンコードが変わるため既存のライセンスは使用できません。新しいマシンコードで再発行を依頼してください。なお **OS の再インストールではマシンコードは変わりません。**

認証器を紛失した／PIN を忘れた・ロックされた

- ユーザーには **リカバリコード**（STEP 5）による緊急ログオンを案内してください。Windows パスワードの併用が必要です。
- 管理者は **マスターキー**（STEP 3）で代行ログオンできます。
- 紛失した認証器は、設定ツールの **ユーザー管理** タブから削除してください。

> ここに載せていない事象については、管理者マニュアル 第13章「トラブルシューティング」を参照してください。

次に読むもの

本書で扱わなかった機能・運用は、管理者マニュアルの以下の章で説明しています。

知りたいこと	参照先（管理者マニュアル）
RDP 経由でのログオンの要件	第2章 システム要件・動作環境
ライセンスの更新・多数端末への一括適用	第5章 ライセンスの登録
設定ツール起動時に FIDO 認証を要求する	第6章 設定ツールの起動認証（任意）
認証器の取り外しで自動ロック、アンインストール制御などの動作設定	第7章 基本設定
ユーザー自身に認証器を登録させる（自己登録）	第8章 認証器（ユーザー）の登録と管理
認証器の PIN ロックへの備え	第8章 認証器（ユーザー）の登録と管理
設定・認証情報の別端末への移送（エクスポート／インポート）	第11章 設定・認証情報の移送
イベントログの確認・サポート情報の収集	第12章 運用・保守
設定項目の一覧、イベント ID の一覧	付録B・付録C

エンドユーザー向けの操作説明は、別冊「**エンドユーザー向け 操作マニュアル**」を配布してください。

お問い合わせ先

本製品の導入・設定・運用に関するお問い合わせは、ご購入いただいた **販売代理店**、または **YubiOn サポートデスク（株式会社 ソフト技研）** へご連絡ください。