YubiOn FIDO Logon Standalone

管理者向け 導入マニュアル

株式会社 ソフト技研

2026年8月版

目次

第1章　はじめに

1.1　本書の目的

本書は、**YubiOn FIDO Logon Standalone**（以下、本製品）を Windows 端末に導入・設定する管理者を対象に、システム要件の確認からインストール、初期設定、日常運用までの手順を説明する導入マニュアルです。

エンドユーザーが実際に認証器でログオンする際の操作方法については、別冊の「**エンドユーザー向け 操作マニュアル**」を参照してください。

1.2　対象読者

本書は、次のような方を対象としています。

- 社内の Windows 端末に本製品を展開する **IT 管理者・情報システム担当者**
- 本製品のライセンス管理・認証器（FIDO2 デバイス）管理を行う運用担当者

Windows の管理者権限、およびグループポリシーやレジストリに関する基本的な知識を前提としています。

1.3　製品概要

本製品は、Windows のログオン（サインイン）に **FIDO2 認証器（YubiKey 等）** による認証を組み込み、パスワードのみのログオンよりもセキュリティを強化するスタンドアロン型の Credential Provider 製品です。

主な特徴は次のとおりです。

- **サーバー通信を一切行いません。** FIDO2 の検証、認証情報（Credential）の保管、パスワードキャッシュのすべてを端末ローカルで完結させるため、インターネット非接続の閉域環境でも単体で動作します。
- 認証情報（公開鍵・credentialId 等）は、**DPAPI（LOCAL_MACHINE）** により端末固有の鍵で暗号化してローカルに保存します。別の端末では復号できません。
- **ローカルアカウント／Active Directory ドメイン／Entra ID（Azure AD）／Microsoft アカウント** のいずれにも対応します。1 台の PC に複数ユーザー、各ユーザーが複数の認証器を登録できます。
- 認証器の登録は、**管理者による事前登録** と **ユーザーによる初回自己登録** の両方に対応します。

> **注記**　本製品の動作には有効なライセンスが必要です。ライセンスの登録手順は「ライセンスの登録」を参照してください。

1.4　本書の構成

章	内容
第1章 はじめに	本書の目的・製品概要
第2章 システム要件・動作環境	導入前に確認すべき要件
第3章 インストール	MSI インストーラーによる導入
第4章 設定ツールの概要	設定ツールの起動と画面構成
第5章 ライセンスの登録	ライセンスの登録とマシンコード
第6章 設定ツールの起動認証（任意）	設定ツール起動時の FIDO 認証と管理者認証器
第7章 基本設定	認証器ログオン・セキュアモード等の設定
第8章 認証器（ユーザー）の登録と管理	ユーザーの FIDO 認証器の管理
第9章 マスターキーの管理	管理者用の代行ログオン認証器
第10章 リカバリコードの管理	緊急ログオン用コードの発行
第11章 設定・認証情報の移送	エクスポート／インポート
第12章 運用・保守	サポート情報収集・ログ確認
第13章 トラブルシューティング	よくある問題と対処
付録A 用語集	用語の定義
付録B 設定項目一覧	設定項目のリファレンス
付録C イベントログ一覧	監査用イベントの一覧

1.5　関連マニュアル

マニュアル	対象読者	内容
管理者向け 導入マニュアル（本書）	IT 管理者	導入・設定・運用
管理者向け クイックスタートガイド	IT 管理者	導入から初期設定・動作確認までの最短手順

マニュアル	対象読者	内容
エンドユーザー向け 操作マニュアル	一般利用者	認証器でのログオン操作

第2章　システム要件・動作環境

本製品を導入する前に、対象端末が以下の要件を満たしているか確認してください。

2.1　対応 OS

区分	対応バージョン
クライアント OS	Windows 10（20H2 以降）／ Windows 11
サーバー OS	Windows Server 2022 以降

> **注記**　上記は RDP 経由ログオン（WebAuthn リダイレクション）にも対応できる構成を基準としています。**Windows Server 2019 および Windows 10 20H2 より前のバージョンは WebAuthn リダイレクションに対応していないため、サポート対象外** です（詳細は本章「リモートデスクトップ（RDP）経由でログオンする場合の要件」）。

> **重要**　本製品はサーバー用と通常（クライアント）用でインストーラーが分かれています。ライセンスも端末の OS 種別（server / client）に紐づくため、OS 種別に合ったインストーラーとライセンスを使用してください。種別が一致しない場合、ライセンスは「OS 種別不一致」として拒否されます。

2.2　実行環境

項目	要件
CPU	**1 GHz 以上の 64 ビットプロセッサ**（本製品は 64 ビット版のみ提供しています）
メモリ	**4 GB 以上**
ストレージ	**200 MB 以上の空き容量**（プログラム約 40 MB ＋ ログ・設定・認証情報の領域）
ソフトウェア	**.NET Framework 4.7.2** 以上
USB	FIDO2 認証器を接続するための **USB ポート**（RDP 経由で利用する場合は接続元 PC 側に必要）

> **注記**　上記の CPU・メモリは、対応 OS（Windows 11／Windows Server 2022 など）自体が求める要件に合わせた値です。本製品が追加で必要とするリソースはわずかで、常駐するサービスのメモリ使用量は数十 MB 程度です。実運用では OS とその他の業務アプリの要件を満たす構成であれば問題ありません。

> **注記（ログ領域について）**　動作ログは `%ProgramData%¥YubiOn¥FidoStandalone¥logs` に出力され、**日付単位でファイルが切り替わります。90 日を過ぎた古いログはサービスが自動的に削除** するため、ログが無制限に増え続けることはありません（第12章「ログの確認」）。

2.3　FIDO2 認証器の要件

- **FIDO2 に対応した認証器** であれば、YubiKey に限らず登録できます。
- 認証器には **UV（User Verification：PIN または生体認証）** への対応が必要です。PIN が未設定の場合、初回登録時に PIN 設定（最小 4 文字）を求めます。
- **U2F（CTAP1）専用キーは、既定では登録・ログオンできません。** 設定「UV 非対応キー（U2F）の使用を許可する」を有効にした場合のみ利用できますが、この場合は hmac-secret 拡張が使えないためパスワードキャッシュが作成されず、**ログオンのたびに Windows パスワードの入力が必要** になります。

2.4　リモートデスクトップ（RDP）経由でログオンする場合の要件

RDP 経由で FIDO ログオンを利用する場合は、次の要件をすべて満たす必要があります。**いずれかを満たさない環境はサポート対象外** です（パスワードログオンへの自動フォールバックは行いません）。

- **接続元 PC（RDP クライアント）と接続先（ホスト）の両方** が、WebAuthn リダイレクションに対応した次のいずれかであること。

OS	必要な更新
Windows 11	2022-10 累積更新（KB5018418）以降
Windows 10（20H2 以降）	2022-10 累積更新（KB5018410）以降
Windows Server 2022 以降	2022-10 累積更新（KB5018421）以降

重要　**Windows Server 2019 は WebAuthn リダイレクションに対応していません**（この機能のプロトコル自体が 2022 年に追加されたものです）。グループポリシーの項目が存在する場合でも機能しないため、Server 2019 では RDP 経由の FIDO ログオンは利用できません。同様に、Windows 10 の 20H2 より前のバージョンも対応していません。

- グループポリシー「**WebAuthn 要求のリダイレクト**」を有効化（「WebAuthn リダイレクトを許可しない」を **無効** または **未構成** に設定）
- FIDO 認証器は **RDP クライアント側の PC に接続** すること（ホスト側に挿しても認識されません）
- 接続先の端末で「**認証器ログオンを有効にする**」が有効であること（第7章「認証器ログオンを有効にする」）

注記　RDP 経由の FIDO ログオンに **セキュアモードは必須ではありません。** セキュアモードが OFF の場合は、RDP でも従来のパスワードログオンが併用できます。RDP 接続でも FIDO 認証を必須にしたい場合は、セキュアモードを ON にしてください（第7章「セキュアモード」）。

補足　RDP 接続先が Windows 10 の場合、WebAuthn リダイレクションの仕様上パスワードキャッシュの作成方法が一部異なりますが、ログオン自体は利用できます。

2.5　動作に関する補足

- **RP ID**（FIDO2 の Relying Party 識別子）は `standalone.yubion.local` に固定されており、変更できません。
- **FIDO 認証のタイムアウト時間** は 120 秒（2 分）固定です。
- 認証情報などのデータは `%ProgramData%¥YubiOn¥FidoStandalone` 配下に保存されます。

2.6　インストールされるコンポーネント

インストーラーを実行すると、次のコンポーネントが導入されます。

コンポーネント	役割
Credential Provider	Windows ログオン画面に FIDO ログオン方式を追加します
Windows サービス（YubiOnFidoStandaloneService）	FIDO2 検証・認証情報の保管・復号を集約します（LocalSystem で動作）
設定ツール（管理者用 GUI）	ライセンス・認証器・各種設定を管理します

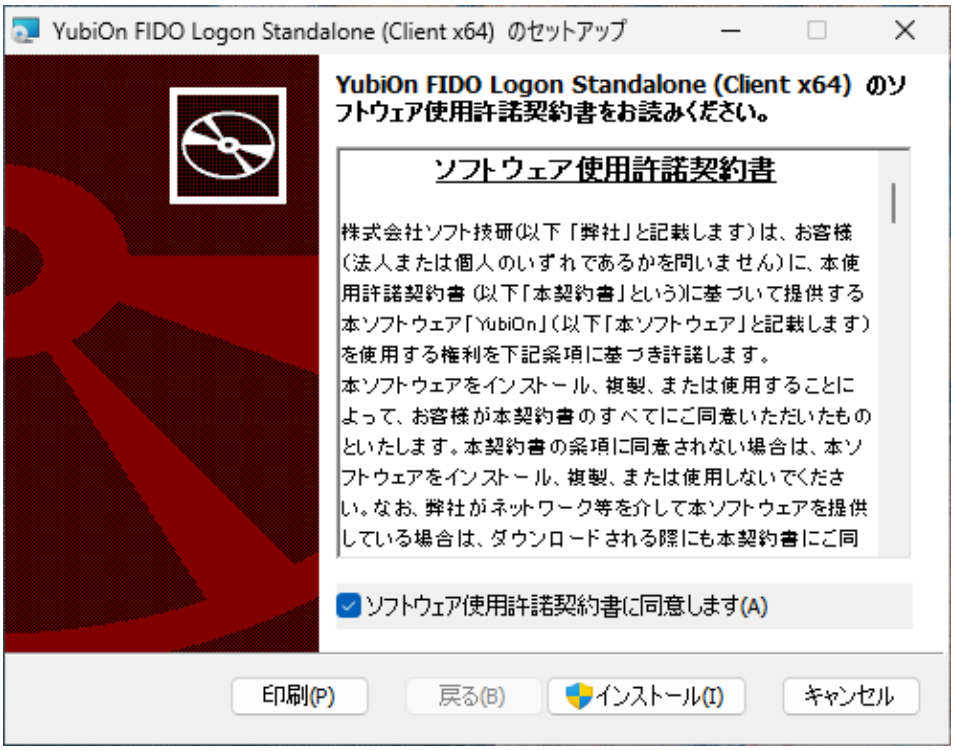
第3章　インストール

3.1　インストール前の確認

- 対象端末が「システム要件・動作環境」を満たしていること
- **端末の OS 種別（サーバー／クライアント）に対応したインストーラー** を用意していること
- インストールを実行するユーザーが **管理者権限** を持っていること
- 発行済みの **ライセンスファイル**（本製品の動作に必要）を用意していること

3.2　インストール手順

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

> **注記　Microsoft Defender SmartScreen が表示された場合**
>
> インストーラーを実行したときに「Windows によって PC が保護されました」という青い画面が表示されることがあります。これはインターネットから入手した実行ファイルに対する Windows の標準的な確認画面で、次の操作でインストールを続行できます。
>
> 1. 「**詳細情報**」を選択します。
> 2. 表示された「**実行**」を選択します。

インストール時に、データ保存先 `%ProgramData%¥YubiOn¥FidoStandalone` が作成され、アクセス権（ACL）が保護された状態に設定されます。

3.3　インストール後の確認

インストール直後の状態では、まだ FIDO ログオンは有効になっていません。続いて次の作業が必要です。

1. **ライセンスの登録**（第5章）
2. **認証器の登録**（第8章）
3. **認証器ログオンの有効化・各種設定**（第7章）

3.4　アンインストール

本製品は Windows の「アプリと機能」からアンインストールできます。

> **注意**　設定「アンインストール制御」を有効にしている場合、アプリ一覧に表示されないため、事前に設定ツールで無効化してからアンインストールしてください。

第4章　設定ツールの概要

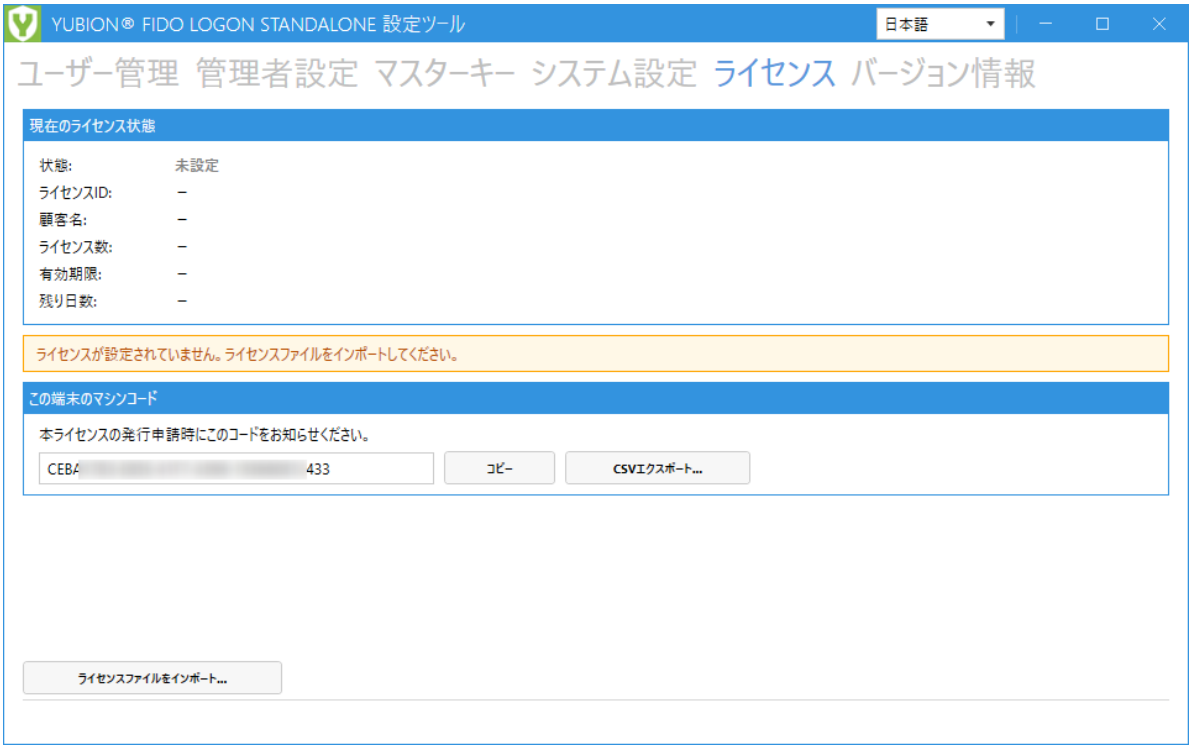
本製品の管理は、管理者用 GUI である **設定ツール** から行います。

4.1　起動

1. スタートメニューを開き、「**すべてのアプリ**」を選択してアプリケーション一覧を表示します。
2. 一覧から「**YubiOn FIDO Logon Standalone Settings Tool**」をクリックします。
3. ユーザーアカウント制御（UAC）の確認画面が表示されるので、「**はい**」を選択します。

設定ツールは管理者権限（UAC 昇格）で動作するため、手順 3 の確認画面は毎回表示されます。管理者権限を持たないユーザーでは起動できません。

> **補足**　ショートカットは名前の先頭が「Y」のため、アプリケーション一覧では末尾付近の「Y」の並びにあります。OS のバージョンによっては「**YubiOn**」フォルダーの下に表示されます。



図：設定ツールのメイン画面

4.2　画面（タブ）構成

設定ツールは以下のタブで構成されます（画面に表示される順序）。

タブ	主な機能	本書の該当章
ユーザー管理	認証器の登録／削除、リカバリコード管理	第8章・第10章
管理者設定	起動認証の切替、管理者 Credential 管理	第6章
マスターキー	マスターキーの登録／削除／名称変更	第9章
システム設定	各種動作設定、設定の移送	第7章・第11章
ライセンス	ライセンス状態表示・登録、マシンコード表示	第5章
バージョン情報	バージョン確認、サポート情報収集	第12章

> **参考**　ライセンスタブとバージョン情報タブは、ライセンスが有効でない状態でも常時操作できます（マシンコードの確認・ライセンス登録・サポート情報収集のため）。

第5章　ライセンスの登録

本製品の FIDO ログオン機能を利用するには、有効なライセンスが必要です。ライセンスは設定ツールの **ライセンス** タブで管理します。

5.1　ライセンスの種別

種別	説明
本ライセンス	登録した端末でのみ動作します。端末の識別情報（マシンコード）に紐づきます。
仮ライセンス	端末紐づけなしで一定期間動作します。トライアルや移行期間に使用します。

5.2　マシンコードの確認

本ライセンスの発行には、対象端末の **マシンコード** が必要です。マシンコードは、端末の **BIOS（SMBIOS）システム UUID** を、次の形式に正規化した値です。

- **大文字・ハイフンあり・36 文字**（8-4-4-4-12 形式）
- 例: 4C4C4544-0042-3010-8051-B7C04F503233

5.2.1　マシンコードが変わる場合・変わらない場合

マシンコードのもとになる BIOS システム UUID は、**マザーボード（システム基板）のファームウェアに記録された値** です。OS はこれを読み出しているだけなので、**OS の再インストールでは変わりません。**

端末に対する操作	マシンコード	ライセンス
OS の再インストール・初期化・アップグレード	**変わらない**	**そのまま使用できます**（再発行は不要）
ディスク（HDD／SSD）の交換・増設	変わらない	そのまま使用できます
メモリー・周辺機器の増設や交換	変わらない	そのまま使用できます
BIOS／UEFI の設定変更・アップデート	原則変わらない	通常はそのまま使用できます

端末に対する操作	マシンコード	ライセンス
マザーボードの交換（基板修理を含む）	**変わる**	**再発行が必要**
PC 本体の入れ替え（新しい端末への更新）	**変わる**（別の端末になるため）	**再発行が必要**

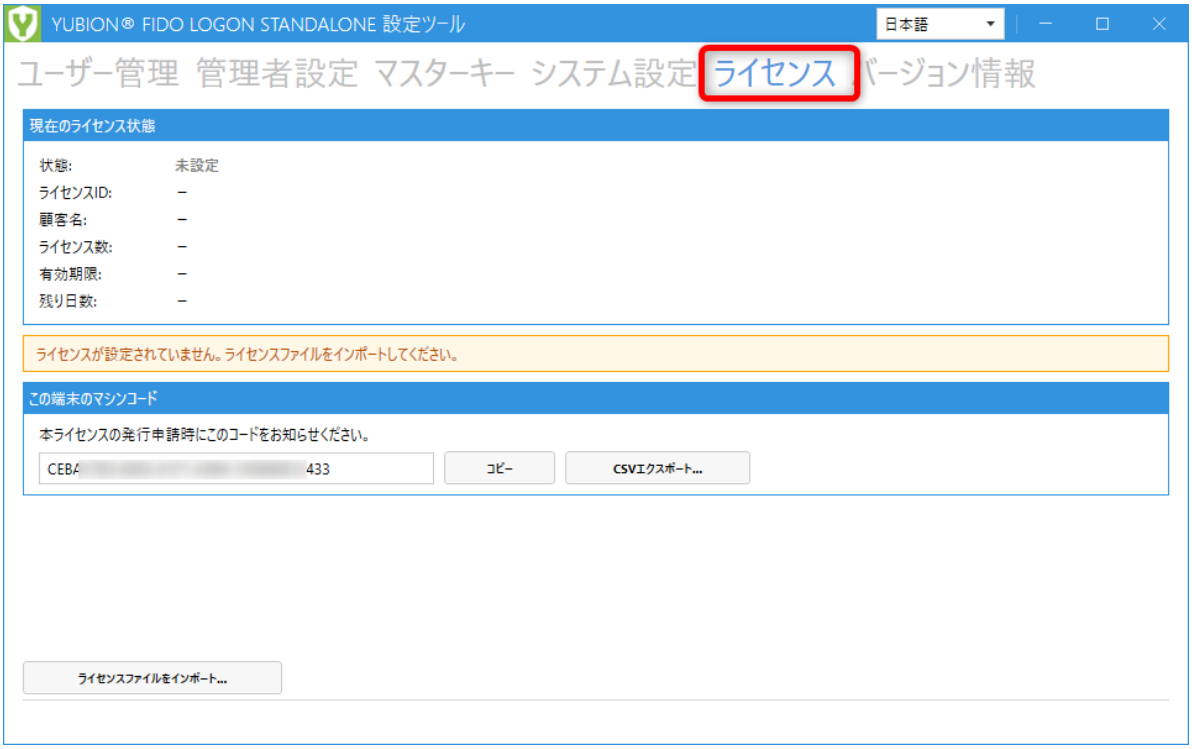
> **重要（PC を入れ替えたとき・マザーボードを交換したときはライセンスの再発行が必要です）**　本ライセンスは登録されたマシンコードの端末でのみ動作します。**新しい PC に入れ替えた場合や、マザーボードを交換した場合は、その端末のマシンコードが以前と異なるため、既存のライセンスでは動作しません**（設定ツールのライセンス状態は「**無効（端末不一致）**」と表示されます）。新しい端末のマシンコードを本節の手順で取得し、**ライセンスの再発行を発行元へ依頼** してください。
>
> - 入れ替え後すぐに運用を開始する必要がある場合は、端末に紐づかない **仮ライセンス**（本章「ライセンスの種別」）を一時的に登録して運用し、本ライセンスの再発行を待つ運用も可能です。
> - 入れ替えで**使用しなくなった端末**のマシンコードは、次回の再発行時に申請対象から外してください（契約台数の管理のため）。
> - 一方、**OS の再インストールや初期化ではマシンコードは変わらないため、ライセンスの再発行は不要** です。バックアップしておいたライセンスファイルを再登録するだけで、そのまま利用できます。

> **注記**　仮想マシン（VM）の場合、UUID は仮想化基盤側の構成に由来します。VM のクローン作成や再作成では値が変わることがあるため、その場合も再発行が必要になります。

5.2.2　設定ツールで確認する

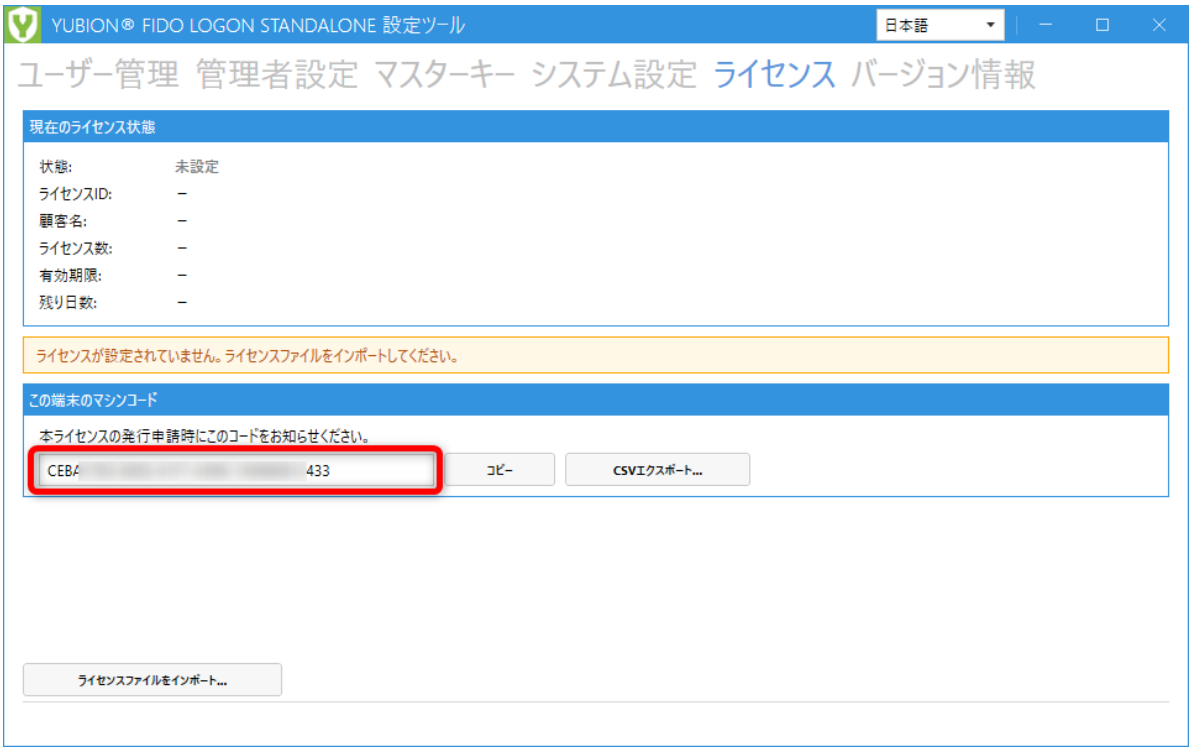
本製品をインストール済みの端末では、設定ツールから確認できます。

1. 設定ツールの **ライセンス** タブを開きます。



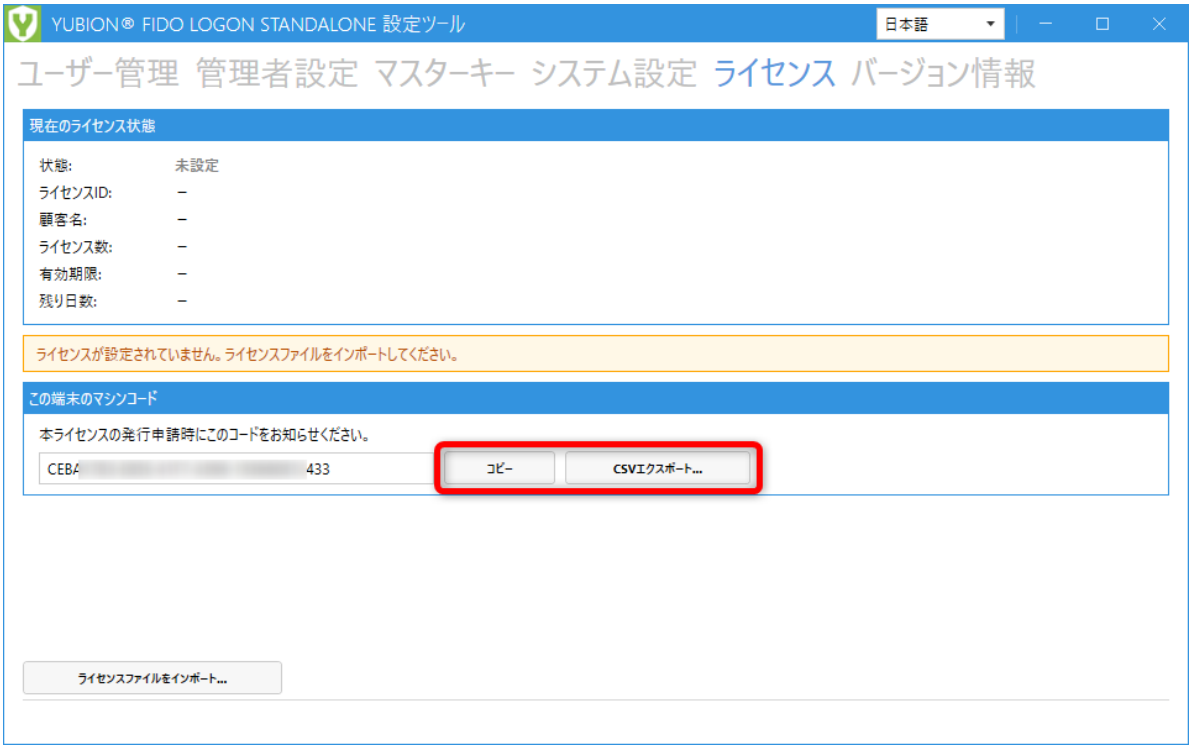
図：ライセンスタブ

2. 「**この端末のマシンコード**」欄に表示された値を確認します。



図：ライセンスタブのマシンコード表示

3. 「コピー」または「CSV エクスポート...」で値を取得し、ライセンス発行元へ提出します。



図：マシンコードのコピーボタン

複数端末を一括で発行する場合は、各端末でマシンコードを CSV エクスポートし、まとめて発行元へ提出してください。

5.2.3　本製品をインストールせずに取得する

本製品を導入する前でも、マシンコードのもとになる BIOS システム UUID は OS の標準機能や資産管理製品で取得できます。導入前に多数の端末分をまとめて申請したい場合などに利用してください。

方法1：PowerShell（推奨）

PowerShell で次のコマンドを実行します。

```
Get-CimInstance Win32_ComputerSystemProduct | Select-Object -ExpandProperty UUID
```

方法2：コマンドプロンプト（旧 OS 向け）

```
wmic csproduct get uuid
```

> **注意**　wmic コマンドは Windows 11 24H2 以降では既定で削除されています。新しい OS では方法1（PowerShell）を使用してください。

方法3：資産管理製品を利用する

Microsoft Configuration Manager（SCCM）、Microsoft Intune、その他のインベントリ／資産管理製品でも、端末の SMBIOS UUID を収集できます。製品によって項目名は異なり、「**UUID**」「**SMBIOS UUID**」「**System UUID**」「**BIOS GUID**」などと表示されます。

> **重要（提出前の確認）**　本製品はマシンコードを **大文字・ハイフンあり** に正規化して照合します。外部で取得した値が小文字の場合は **大文字に変換** して提出してください。また、次のような無効な値（一部の端末で設定されている既定値）はマシンコードとして使用できません。該当する場合は端末側の設定をご確認ください。
>
> - `00000000-0000-0000-0000-000000000000`（すべて 0）
> - `FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF`（すべて F）
> - `03000200-0400-0500-0006-000700080009`（一部マザーボードの既定値）

5.2.4　提出用ファイルの形式

複数端末分をまとめて提出する場合は、設定ツールの CSV エクスポートと同じ形式のテキストファイルにすると、そのまま利用できます。

- **文字コード:** UTF-8（BOM なし）
- **区切り:** カンマ（`,`）
- **ヘッダー行:** なし
- **1 行 = 1 台**、列は次の順序

列	内容	例
1	マシン名（コンピューター名）	`PC-001`
2	マシンコード（UUID）	`4C4C4544-0042-3010-8051-B7C04F503233`
3	OS 種別（`client` または `server`）	`client`

記入例:

```
PC-001,4C4C4544-0042-3010-8051-B7C04F503233,client
PC-002,9A8B7C6D-5E4F-3A2B-1C0D-EF1122334455,client
SRV-01,1122AABB-CCDD-EEFF-0011-223344556677,server
```

OS 種別について　本ライセンスは端末の OS 種別（サーバー／クライアント）にも紐づきます。PowerShell では次のコマンドで判別できます（1 がクライアント、それ以外はサーバー）。

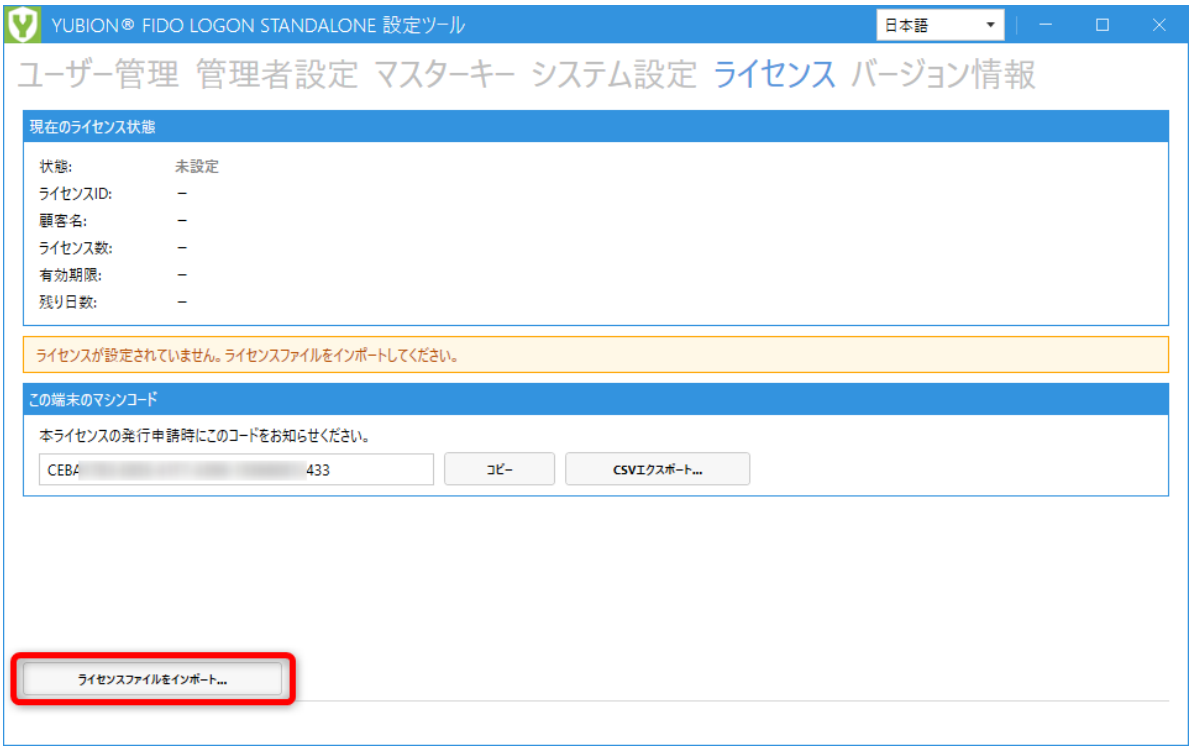
```
(Get-CimInstance Win32_OperatingSystem).ProductType
```

上記の 1 行形式（マシン名・UUID・OS 種別）をまとめて出力するには、次のように実行します。

```
$uuid = (Get-CimInstance Win32_ComputerSystemProduct).UUID.ToUpper()
$os = if ((Get-CimInstance Win32_OperatingSystem).ProductType -eq 1) { 'client' } else { 'server' }
"$env:COMPUTERNAME,$uuid,$os"
```

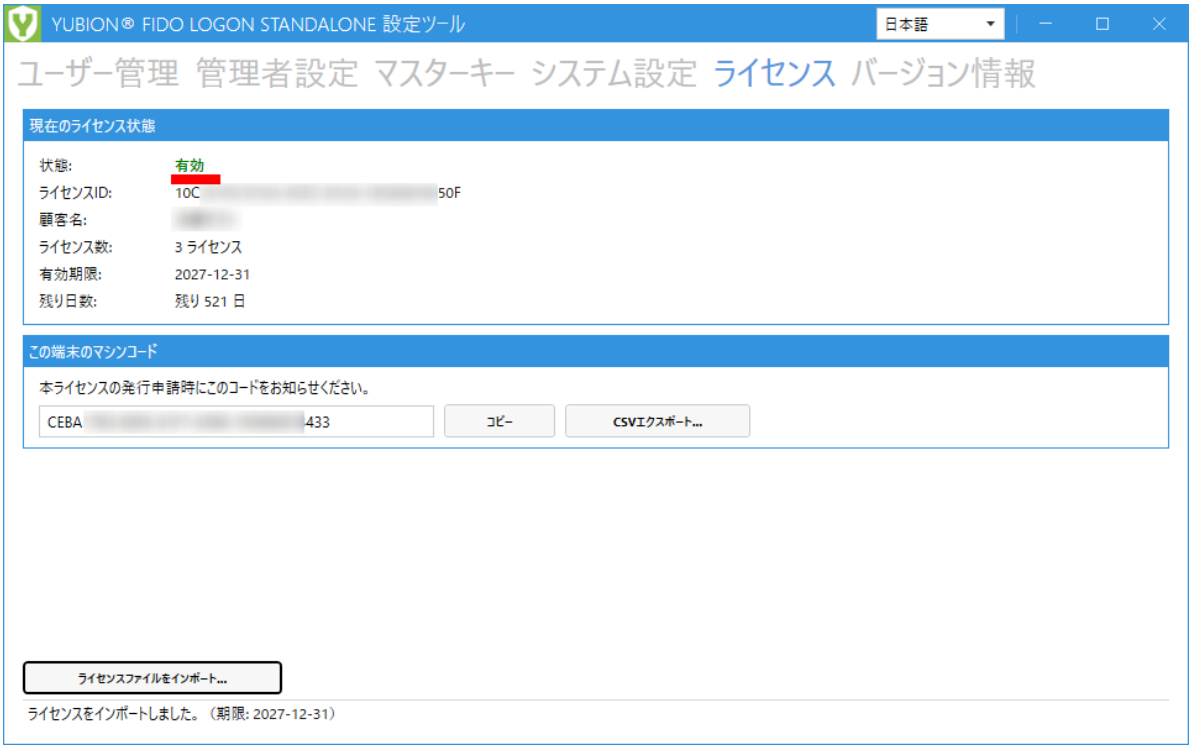
5.3　ライセンスファイルの登録

1. 発行された **ライセンスファイル** を端末に用意します。
2. ライセンスタブ下部の「**ライセンスファイルをインポート...**」を選択し、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

3. ライセンス状態が「有効」になることを確認します。



図：ライセンスが有効化された状態

5.4　ライセンスの更新

有効期限の延長、仮ライセンスから本ライセンスへの切り替え、契約台数の追加などでライセンスファイルを再発行してもらった場合は、**新しいライセンスファイルをインポートし直すだけ** で更新できます。古いライセンスを削除する操作や、本製品の再インストールは必要ありません。

5.4.1　更新の手順

1. 発行元から新しいライセンスファイルを受け取ります。
2. 設定ツールの **ライセンス** タブを開き、「**ライセンスファイルをインポート...**」を選択して新しいファイルを指定します（本章「ライセンスファイルの登録」と同じ操作です）。
3. 「ライセンスをインポートしました。（期限: yyyy-mm-dd）」と表示され、状態と有効期限が新しい内容に更新されたことを確認します。

既存のライセンスファイルは自動的に上書きされます。更新は端末ごとに行う操作で、認証器・マスターキー・リカバリコード・各種設定には影響しません。

> **注記**　ライセンス状態はログオンのたびに判定されるため、更新後にサービスや端末を再起動する必要はありません。次回のログオンから新しいライセンスで動作します。

5.4.2　更新のタイミング

- **期限が切れる前でも更新できます。** 本ライセンスは有効期限まで 30 日以内になると状態が「**有効・期限間近**」に変わり、ライセンスタブに残日数と更新を促す警告が表示されます。この表示が出たら更新を検討してください。更新すると状態は「**有効**」に戻ります。
- **期限が切れた後でも同じ手順で更新できます。** 期限切れの間は設定ツールの一部のタブが操作できなくなりますが、**ライセンスタブは引き続き操作できる** ため更新は可能です。更新すると各タブがその場で操作可能に戻り、FIDO ログオンも次回のログオンから自動的に復帰します（本章「有効期限が切れたときの動作」）。
- 本ライセンスの更新では、端末の **マシンコードは変わりません。** マシンコードを再提出する必要があるのは、PC 本体の入れ替えやマザーボードの交換を行った場合だけです（本章「マシンコードが変わる場合・変わらない場合」）。

5.4.3　更新できない場合

インポートは保存前に検証され、次のいずれかに該当するファイルは受け付けられません。この場合 **現在のライセンスファイルは置き換えられず、更新前の状態がそのまま維持されます**（イベント ID 3701 が記録されます）。

表示されるメッセージ	主な原因と対処
ファイルが見つかりません。	指定したパスにファイルがありません。ファイルの場所を確認してください。
ライセンスファイルが無効です（署名検証失敗または XML 形式エラー）。	ファイルが破損しているか、内容が改変されています。発行元から取得し直してください。
このライセンスファイルは既に期限切れのためインポートできません。	古いライセンスファイルを選んでいます。新しい有効期限のファイルを指定してください。
このライセンスにはこの端末のマシンコードが登録されていないためインポートできません。	別の端末向けのファイルです。本章「マシンコードの確認」で取得したマシンコードで再発行を依頼してください。
このライセンスはこの端末とは異なる OS 種別（サーバー／クライアント）で登録されているためインポートできません。	サーバー用とクライアント用を取り違えています。この端末の OS 種別に合わせて再発行を依頼してください。

5.4.4　多数の端末をまとめて更新する場合

設定ツールを使わず、各端末のライセンスファイルを新しいファイルで直接置き換える方法でも更新できます。配布スクリプトやグループポリシーによる一括更新に利用できます。

- 配置先は `%ProgramData%¥YubiOn¥FidoStandalone¥license.slcx` です。このフォルダーはアクセス権が保護されているため、**管理者権限で書き込む** 必要があります。
- サービスがファイルの置き換えを検知し、有効なライセンスであればイベント ID **2910** を記録します。サービスや端末の再起動は不要です。
- 誤って無効なファイル（破損・別端末向け・期限切れ）で置き換えてしまった場合は、サービスが直前の有効なライセンスのバックアップから **自動的に復元** します（イベント ID **2911**）。復元できるバックアップが無い場合は復元されず、イベント ID **2912** が記録されます。

> **注意**　ライセンスファイルを削除した場合は復元されません（意図的な撤去と区別できないため）。状態は「未設定」となり、FIDO ログオンは動作しなくなります。

5.5　ライセンス状態の一覧

状態	意味	動作
有効（Valid）	正常	動作します
有効・期限間近（ExpiringSoon）	有効期限まで30日以内	動作します
仮ライセンス（TemporaryValid）	仮ライセンスで有効	動作します
未設定（NotConfigured）	ライセンス未登録	動作しません
無効（Invalid）	ファイルが不正	動作しません
端末不一致（MachineMismatch）	別端末向けのライセンス	動作しません
OS 種別不一致（OsTypeMismatch）	サーバー／クライアントの不一致	動作しません
期限切れ（Expired）	有効期限超過	動作しません

> **ロックアウトは発生しません**　ライセンスが有効でない場合でも、FIDO ログオンが強制されて締め出される（ロックアウトする）ことはありません。この場合はパスワードによる通常ログオンが可能な状態となり、ライセンスを登録し直すと自動的に FIDO ログオンへ復帰します。

5.5.1　有効期限が切れたときの動作

有効期限はライセンスファイルに記載された日付の **当日いっぱい（23:59:59）** まで有効です。翌日以降は「**期限切れ（Expired）**」となり、次のように動作します。

ログオン画面

- 本製品の **FIDO タイルが表示されなくなります。**認証器でのログオンはできません。
- **セキュアモードを有効にしている場合も、期限切れになると他のログオン方法の抑止が行われなくなります。** 認証器を登録済みのユーザーもパスワードで通常どおりログオンでき、画面ロックの解除も同様です。なお、期限切れによってセキュアモードの設定が書き換わることはありません。ライセンスを更新すると、設定を変更しなくても次回のログオンから抑止が復帰します。
- RDP 接続でも本製品は介入しません。

> **参考**　ライセンス状態はログオンのたびに判定されます。期限が切れても、ログオン中のセッションがその場で中断されることはありません。次回のログオン・ロック解除から上記の動作になります。

設定ツール

- ライセンスタブの状態表示が赤字の「**期限切れ（yyyy-mm-dd）**」に変わり、残日数欄が「**期限切れ（n 日超過）**」になります。あわせて「ライセンスは yyyy-mm-dd に期限切れになりました。新しいライセンスをインポートしてください。」という警告が表示されます。
- 設定ツールを起動すると、**ライセンスタブが選択された状態** で開きます。
- **ユーザー管理・管理者設定・マスターキー・システム設定** の 4 タブが操作できなくなります（**ライセンス** タブと **バージョン情報** タブは引き続き使用できます）。

- 「**設定ツール起動時に FIDO 認証を要求する**」を有効にしている場合、**期限切れでも起動時の管理者認証は要求されます。**管理者認証器を紛失している場合はライセンスを更新しても設定を変更できなくなるため、注意してください。

4 タブが操作できないため、期限切れの間は次の操作が行えません。

操作	タブ
認証器の割り当て（登録）・削除・名称変更、リカバリコードの発行	ユーザー管理
管理者認証器の登録・削除、起動認証の切替	管理者設定
マスターキーの登録・削除・名称変更	マスターキー
各種システム設定の変更、設定・認証情報のエクスポート／インポート	システム設定

登録済みの情報

- 登録済みの認証器・管理者認証器・マスターキー・リカバリコード・各種設定は、期限切れになっても **削除されません。**
- 有効なライセンスをインポートすると、設定ツールの各タブがその場で操作可能に戻り、FIDO ログオンも次回のログオンから自動的に復帰します。**登録や設定をやり直す必要はありません。**

> **注意**　期限切れのライセンスファイルは **インポートできません**（「このライセンスファイルは既に期限切れのためインポートできません。」と表示されます）。新しい有効期限のライセンスファイルを発行元から取得してください。

期限切れを未然に防ぐには

- 本ライセンスは有効期限まで 30 日以内になると「**有効・期限間近**」に変わり、ライセンスタブに残日数と更新を促す警告が表示されます。定期的にライセンスタブを確認してください。
- **仮ライセンスは「期限間近」表示になりません。** 代わりに「仮ライセンスで動作中です。yyyy-mm-dd までに本ライセンスをインポートしてください。」という案内が常時表示されます。
- サービス開始時のイベントログ（イベント ID **2900**）にライセンス状態が記録されます。期限切れの端末では `License: Expired (yyyy-mm-dd)` と出力されるため、複数端末の状況をイベントログから確認できます。

第6章　設定ツールの起動認証（任意）

セキュリティを高めるため、設定ツール自体の起動に FIDO 認証を要求できます（**管理者設定**タブの「**設定ツール起動時に FIDO 認証を要求する**」、既定は無効）。

> **注記**　本章の操作は、ライセンスの登録（第5章「ライセンスファイルの登録」）が完了してから行ってください。

- 有効にすると、起動時に「管理者認証」ダイアログが表示され、**管理者認証器（管理者 Credential）** による FIDO 認証を求められます。「認証する」を選択して認証器をタッチしてください。

図：設定ツール起動時の FIDO 認証ダイアログ

- 管理者認証器は **Windows ユーザーには紐づきません**。一度登録した認証器は、どのユーザーでログオンしていても使用できます。
- 有効にする前に、管理者認証器を **1 本以上登録** しておく必要があります（未登録のままでは有効にできません）。
- 登録済みの管理者認証器をすべて削除すると、この設定は自動的に無効へ戻ります（締め出し防止）。

6.1 管理者認証器の登録

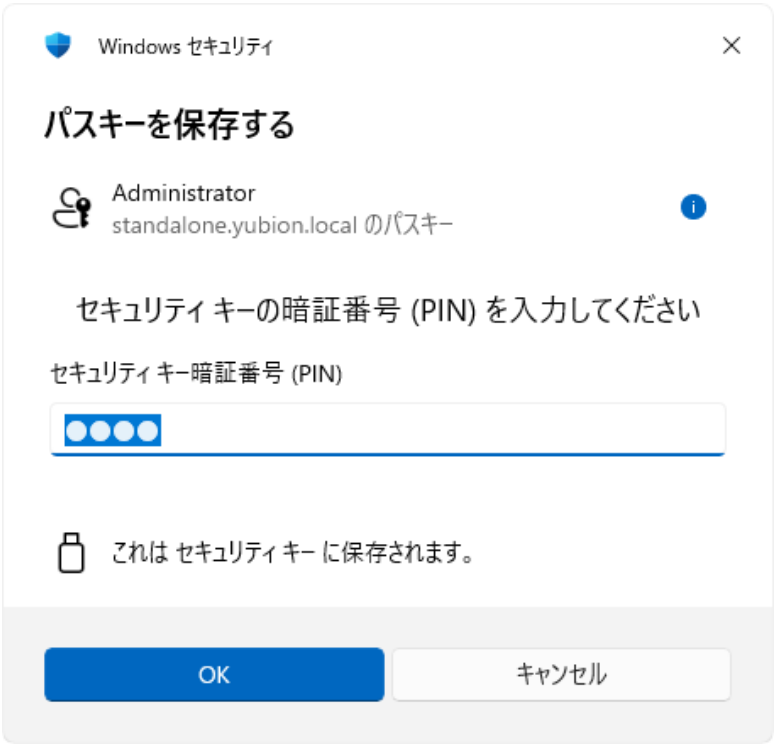
1. **管理者設定** タブを開きます。

図：管理者設定タブ

2. 「＋ **管理者キーを登録**」を選択します。

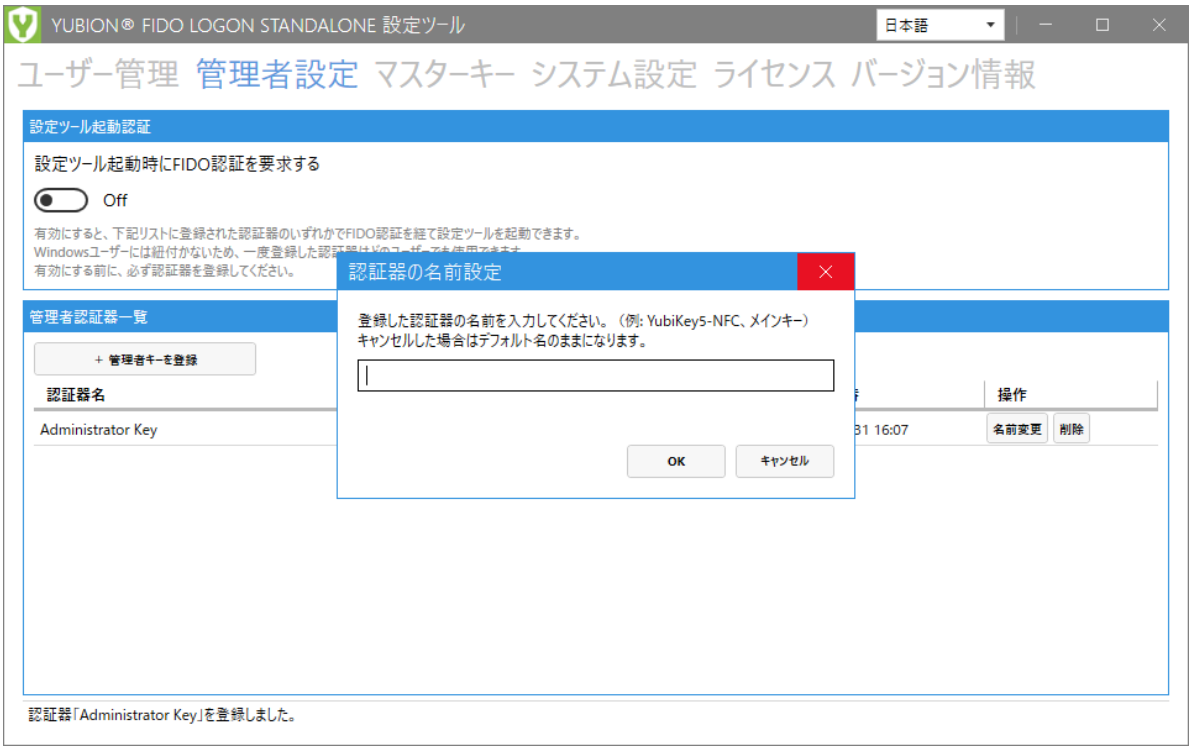
図：「＋ 管理者キーを登録」ボタンを選択

3. 認証器を接続し、PIN（または生体認証）を入力し、タッチします。



図：PIN 入力ダイアログ

4. 登録が完了すると、**認証器の名前設定** ダイアログが表示されます。名前を入力します（キャンセル時は既定の名前のままになり、後から「名前変更」で変更できます）。



図：認証器の名前設定ダイアログ

5. 「管理者認証器一覧」に追加されたことを確認します。

図：管理者認証器一覧に登録された状態

登録済みの認証器は、一覧の「操作」列にある「名前変更」「削除」で管理します。

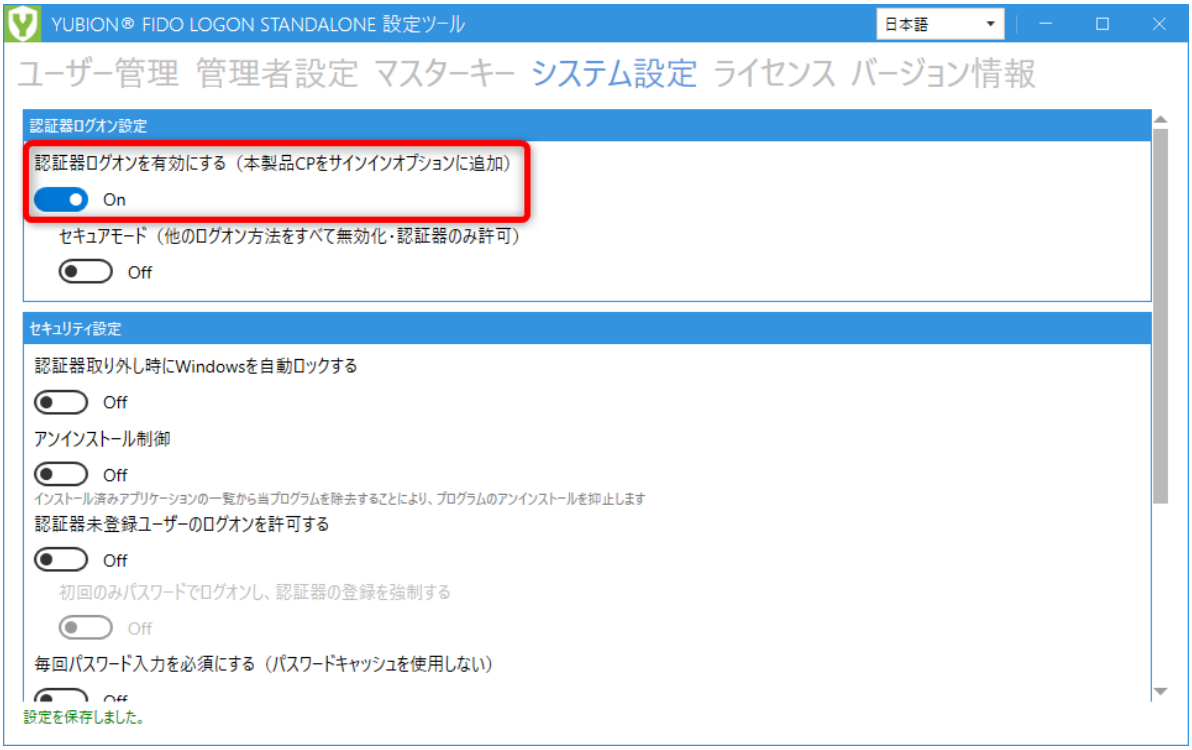
第7章　基本設定

FIDO ログオンを有効にし、運用ポリシーに合わせて動作を調整します。設定は主に **システム設定** タブで行います。

> **前提**　これらの設定を有効にする前に、ログオンに使用できる認証器（ユーザーの認証器またはマスターキー）を **1 本以上登録** しておく必要があります（第8章・第9章）。

7.1　認証器ログオンを有効にする

システム設定タブの「**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）**」を有効にすると、本製品の Credential Provider が Windows に登録され、ログオン画面に FIDO ログオンのタイルが表示されます。



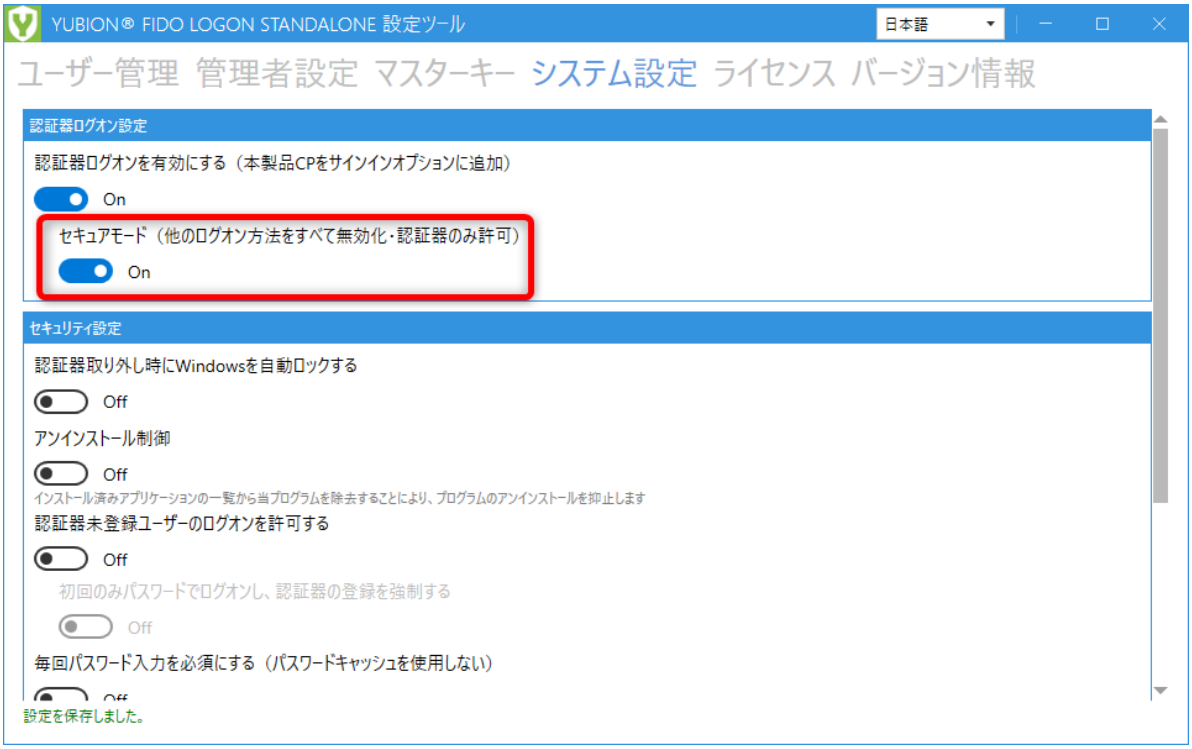
図：認証器ログオンを有効にする設定

- 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。
- ユーザーの認証器・マスターキーがいずれも 0 本になると、自動的に無効へ戻ります。

7.2　セキュアモード

「**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）**」を有効にすると、

他の Credential Provider を無効化し、本製品の FIDO ログオンのみに限定します。これにより、認証器によるログオンを強制します。



図：セキュアモードを有効にする設定

- 有効にするには「認証器ログオンを有効にする」が前提です。
- RDP 経由のログオンにセキュアモードは必要ありません。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。

> **注意**　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。全対象ユーザーの認証器登録が完了してから有効化してください。緊急時に備え、**マスターキー**（第9章）と **リカバリコード**（第10章）の準備を推奨します。

7.3　その他の動作設定

システム設定タブでは、以下の動作も設定できます。設定名は設定ツールに表示される名称です。

設定名	既定	説明
認証器取り外し時に Windows を自動ロックする	無効	認証器を抜くと自動的に Windows をロックします
アンインストール制御	無効	アプリ一覧に表示させず、不用意なアンインストールを防ぎます
毎回パスワード入力を必須にする（パスワードキャッシュを使用しない）	無効	有効にすると、認証器での認証成功後もキャッシュを使わず、毎回 Windows パスワードの入力を求めます
UV 非対応キー（U2F）の使用を許可する	無効	有効にすると U2F（CTAP1）キーの登録・ログオンを許可します（パスワードキャッシュ不可・毎回パスワード入力）

7.3.1　認証器未登録ユーザーの扱い

認証器が未登録のユーザーの扱いは、次の 2 つの設定で調整します。

- **認証器未登録ユーザーのログオンを許可する:** 有効にすると、認証器を登録していないユーザーもパスワードでログオンできます。
- **初回のみパスワードでログオンし、認証器の登録を強制する:** 有効にすると、未登録ユーザーは初回のみパスワードでログオンでき、その際に認証器の登録を促します。


YUBION® FIDO LOGON STANDALONE 設定ツール
日本語
ユーザー管理 管理者設定 マスターキー システム設定 ライセンス バージョン情報
認証器ログオン設定
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）
On
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）
On
セキュリティ設定
認証器取り外し時にWindowsを自動ロックする
On
アンインストール制御
On
インストール済みアプリケーションの一覧から当プログラムを除去することにより、プログラムのアンインストールを抑止します
認証器未登録ユーザーのログオンを許可する
On
初回のみパスワードでログオンし、認証器の登録を強制する
On
毎回パスワード入力を必須にする（パスワードキャッシュを使用しない）
On
認証器での認証成功後も、キャッシュされたパスワードを使わず必ず Windows パスワードの入力を求めます。
UV非対応キー（U2F）の使用を許可する
On
PIN や指紋などのユーザー検証（UV）に対応しない U2F キーでのログオンを許可します。OFF（既定）では UV を必須とし、より安全です。マスターキーは本設定に関わらず常に UV 必須です。
※ U2F キーは HMAC Secret に対応しないためパスワードキャッシュを利用できず、ログオンのたびに Windows パスワードの入力が必要です。
設定の移送
システム設定とCredential登録情報をファイルに書き出して、別の端末で読み込めます。改ざん検知用のHMAC署名が付与されます。
エクスポート...
インポート...
設定を保存しました。

図：システム設定タブ

第8章　認証器（ユーザー）の登録と管理

ユーザーが FIDO ログオンに使用する認証器は、設定ツールの **ユーザー管理** タブで管理します。

8.1　登録方式

認証器の登録には 2 つの方式があります。運用に合わせて選択してください。

1. **管理者による事前登録:** 管理者が設定ツールから、対象ユーザーの認証器を登録します（本章「認証器の登録（管理者による事前登録）」）。
2. **ユーザーによる自己登録:** ユーザーが初回ログオン時に、自分で認証器を登録します（本章「ユーザー自身に登録させる（自己登録）」）。対象ユーザーが多く、管理者が一台ずつ事前登録するのが難しい場合に適しています。

8.2　認証器の登録（管理者による事前登録）

1. **ユーザー管理** タブを開きます。

図：ユーザー管理タブ

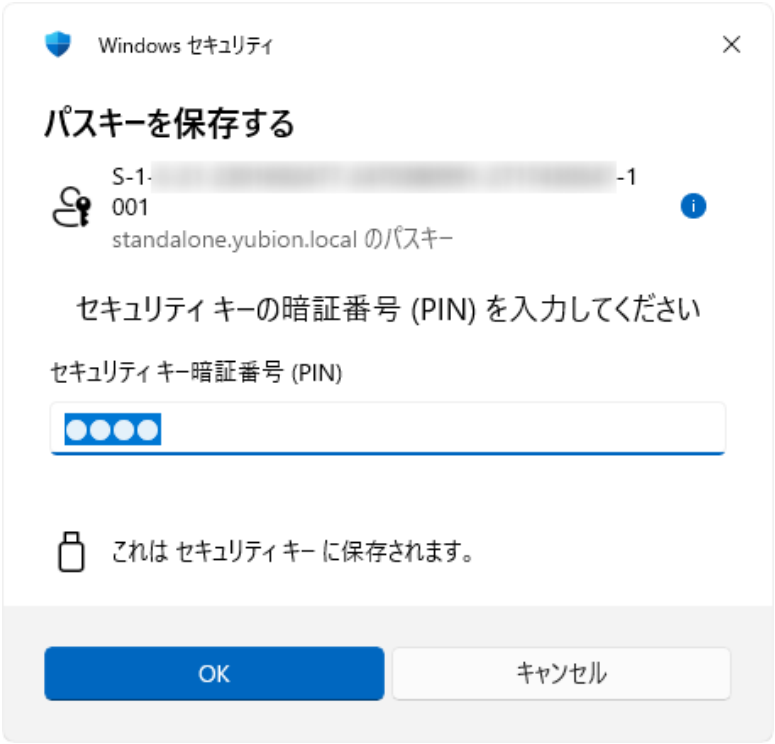
2. 対象の Windows アカウントを選択します。

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、タッチします。



図：PIN 入力ダイアログ

5. 登録が完了すると、**認証器の名前設定** ダイアログが表示されます。名前（例: YubiKey5-NFC、メインキー）を入力します。キャンセルした場合は既定の名前のままになり、後から「名前変更」で変更できます。

図：認証器の名前設定ダイアログ

6. 「登録済み認証器」の一覧に認証器が追加されたことを確認します。

図：登録済み認証器の一覧に追加された状態

注記　ユーザー一覧のアカウント名は、アカウントの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

重要　設定ツールのユーザー一覧には、その端末に **ユーザープロファイルが作成済みのアカウント**（＝これまでに一度でもその端末にログオンしたことのあるアカウント）のみが表示されます。一度もログオンしたことのないユーザーは一覧に表示されず、認証器を割り当てできません。対象ユーザーに事前登録を行う場合は、先に本人が一度その端末にサインインし、プロファイルを作成しておく必要があります。

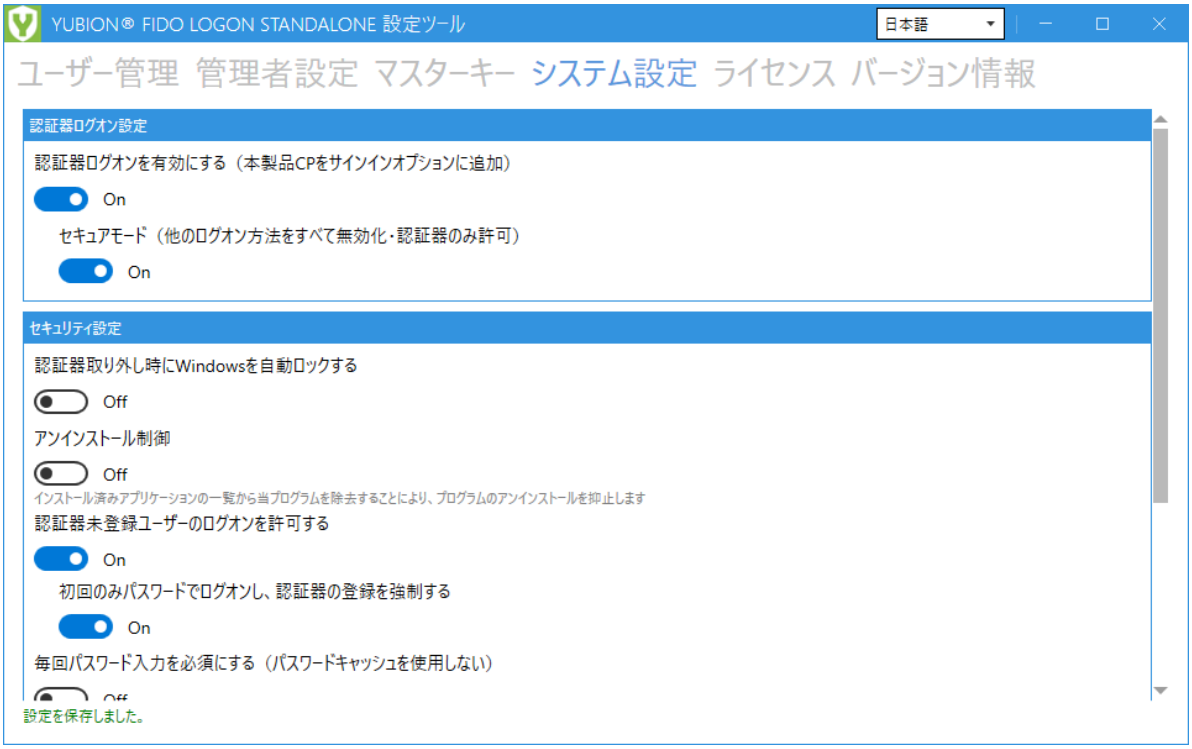
> **重要（Windows の「パスキーアクセス」設定）**　Windows の **設定** → **プライバシーとセキュリティ** → **パスキー** にある「**パスキーアクセス**」が **オフ** になっていると、**認証器の割り当て（登録）ができません。**本製品の設定ツールは認証器の登録に Windows の WebAuthn 機能を使用するため、この設定でブロックされます。登録前に「パスキーアクセス」を **オン** にしてください。
>
> この設定は端末（サインインユーザー）ごとの設定です。オフのままだと、設定ツールの次の操作がいずれも失敗します。
>
> - 認証器の登録（本節）
> - マスターキーの登録（第9章）
> - 管理者 Credential の登録、および起動認証（第6章「設定ツールの起動認証（任意）」）
>
> なお、この設定項目は比較的新しい Windows 11 にのみ存在します。設定画面に「パスキー」の項目が見当たらない場合は、この制限は該当しません。

8.3　ユーザー自身に登録させる（自己登録）

管理者が事前登録するのではなく、**各ユーザーに初回ログオン時に自分で認証器を登録させたい** 場合は、以下の設定を行います。これにより、認証器が未登録のユーザーは初回だけパスワードでログオンし、その際に認証器の登録を求められます。

8.3.1　必要な設定

システム設定 タブで、次のように設定します（各設定の詳細は第7章を参照）。



図：自己登録に必要なシステム設定

手順	設定名	値
1	認証器ログオンを有効にする	ON
2	認証器未登録ユーザーのログオンを許可する	ON
3	初回のみパスワードでログオンし、認証器の登録を強制する	ON
4（推奨）	セキュアモード	ON

- 手順 3 は、手順 2（許可）が ON のときにのみ設定できます。
- **手順 4（セキュアモード）を推奨する理由:** セキュアモードが OFF のままだと、ログオン画面に Windows 標準のパスワードタイルも並んで表示され、ユーザーが認証器を登録せずにログオンできてしまいます。セキュアモードを ON にすると他のログオン方法が隠れ、確実に自己登録へ誘導できます。

> **初期展開時の前提**　手順 1（認証器ログオンを有効にする）は、ログオンに使用できる認証器が 1 本もない状態では有効化できません。まだ誰も認証器を登録していない初期展開では、先に管理者が **マスターキー**（第9章）を 1 本登録しておくと、この条件を満たせます。

8.3.2　設定の組み合わせと挙動

「許可」と「強制」の組み合わせによって、認証器が未登録のユーザーの挙動が変わります。

認証器未登録ユーザーのログオンを許可する	初回のみ…登録を強制する	未登録ユーザーの挙動
OFF	–	パスワードでログオンできません（セキュアモード ON 時は案内タイルのみ表示）
ON	OFF	パスワードのみでログオンできます（**認証器の登録は求められません**）
ON	ON	初回はパスワードでログオンし、その際に **認証器の自己登録を求められます**

> **注意**　「許可」だけを ON にして「強制」を OFF にした場合、ユーザーはパスワードのみでログオンでき、認証器の登録は促されません。ログオン後に任意のタイミングで登録する画面は用意されていないため、**自己登録させたい場合は「許可」と「強制」の両方を ON** にしてください。

8.3.3　ユーザー側の操作の流れ

自己登録が有効な状態で、認証器が未登録のユーザーが初めてログオンすると、次のように進みます。

1. パスワードを入力してログオンします。

図：パスワード入力画面

2. 認証器の登録を求められます。認証器を接続します。

図：認証器の接続要求画面

3. PIN が未設定の場合は、PIN を設定します。

図：PIN の設定画面

4. 認証器にタッチして登録を完了します。

図：認証器へのタッチ画面

5. そのままログオンが完了します。2 回目以降は通常の FIDO ログオンになります。

具体的な画面操作は、別冊「**エンドユーザー向け 操作マニュアル**」の「認証器を登録する」を

参照してください。

8.3.4　留意点

- **ドメイン／Entra ID アカウント:** これらのアカウントは通常ログオン画面にタイルとして表示されないため、ユーザーは「**その他のユーザー**」からアカウント名を手入力して自己登録します。
- **マスターキーとの関係:** 自己登録の対象となる未登録ユーザーに対しては、マスターキーによる代行ログオンは提示されません（本人に登録させることを優先するため）。

8.4　認証器の削除・名称変更

- **ユーザー管理** タブの「登録済み認証器」一覧の「操作」列にある「**削除**」で、認証器の割り当てを削除できます。
- 同じ「操作」列の「**名前変更**」で、認証器に識別しやすい名称を付けられます。

> **注意**　ユーザーの認証器とマスターキーがいずれも 0 本になると、「認証器ログオン」および「セキュアモード」は自動的に無効化されます。

8.5　PIN の入力ミスによる認証器ロックへの備え

FIDO2 認証器は、**PIN を連続して間違えるとロックされ、最終的にはリセット（初期化）しないと使用できなくなります。**これは認証器側の仕様であり、**本製品からロックを解除することはできません。**また、リセットすると認証器内の資格情報はすべて消えるため、**本製品への再登録が必要**になります。

ロックは 2 段階で進行します。

段階	状態	ログオン画面のメッセージ	復旧方法
一時ブロック	PIN を数回連続で間違えた（一般的な認証器では 3 回）	「PIN 認証がブロックされました。キーを抜いて再挿入してください」	認証器を抜いて再挿入すれば、再度 PIN を入力できます
完全ブロック	さらに誤入力を続け、残り試行回数が 0 になった（一般的な認証器では合計 8 回）	「PIN がブロックされています。キーをリセットしてください」	**認証器のリセットが必要。**資格情報は失われ、再登録が必要です

> **注意**　試行回数の上限は認証器の製品仕様により異なります。また、**ログオン画面に残りの試行回数は表示されません。**ユーザーが「あと何回試せるか」を判断できないため、気付かないうちに完全ブロックに至る可能性があります。

このため、**認証器 1 本だけに依存する運用は避け、次の備えを事前に用意してください。**

備え	概要	参照
予備の認証器を登録する	同じユーザーに 2 本以上の認証器を登録できます（本数の上限はありません）。1 本がロックしても、もう 1 本で通常どおりログオンできます。ユーザーの利便性を損なわない **最も確実な備え** です。	本章「認証器の登録（管理者による事前登録）」
マスターキーを登録する	管理者が任意のアカウントへ代行ログオンできます。ユーザーの認証器がロックした際の復旧手段になります。	第9章
リカバリコードを発行する	**認証器を一切使わずに** 緊急ログオンできます。認証器のロックによる影響を受けません。	第10章

> **重要**　マスターキーも PIN を持つ FIDO2 認証器であり、同じくロックし得ます。マスターキー 1 本だけに頼らず、**リカバリコードの発行を併せて行ってください。**認証器を使わずにログオンできるリカバリコードは、認証器ロックに対する最終手段として最も有効です。

> **警告**　本製品は **認証器が PIN ロックされたことを検知できません。**「認証器ログオン」「セキュアモード」の自動無効化（前節の注意）は、設定ツールでの削除などによって **登録本数が 0 本になった場合** の動作であり、登録されたままロックした認証器は依然「登録済み 1 本」として数えられます。したがって、**セキュアモードが有効な状態で、登録済みの認証器・マスターキーがすべて PIN ロックし、リカバリコードも未発行の場合は、その端末にログオンできなくなります（ロックアウト）。** この状態は本製品の設定変更では復旧できないため、**上記の備えを必ず事前に用意してください。**

第9章　マスターキーの管理

マスターキー は、Windows アカウントへの割り当てを問わず、**任意のアカウントへログオンできる管理者用の FIDO 認証器** です。設定ツールの **マスターキー** タブで管理します。

9.1　用途

- 退職者アカウントなどへの一時的なアクセス
- ユーザーの認証器が故障・紛失した、または **PIN ロックで使用不能になった** 際の代行ログオン
- 管理作業のためのログオン

9.2　特徴と制約

- 端末あたり **最大 3 本** まで登録できます。
- 登録は **設定ツール経由でのみ** 行えます（ユーザーによる自己登録はできません）。
- **UV（PIN または生体認証）は、登録時・認証時ともに常に必須** です（設定に関わらず）。

9.3　登録手順

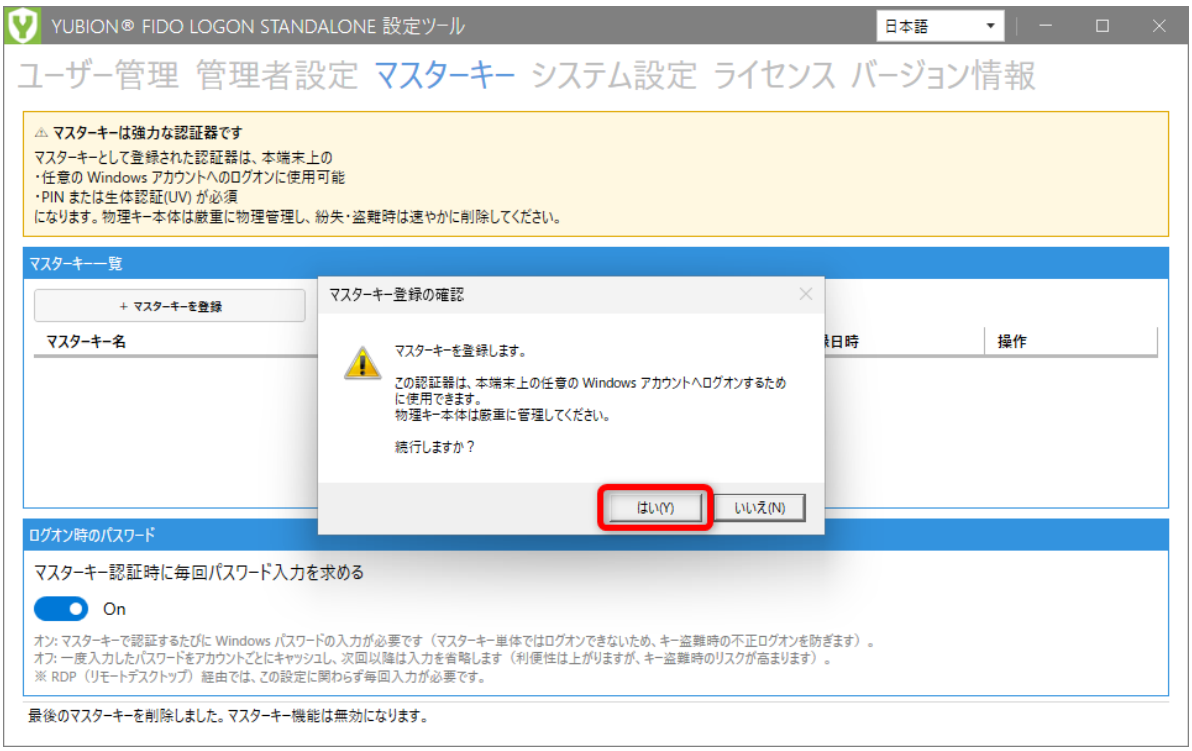
1. **マスターキー** タブを開きます。

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。

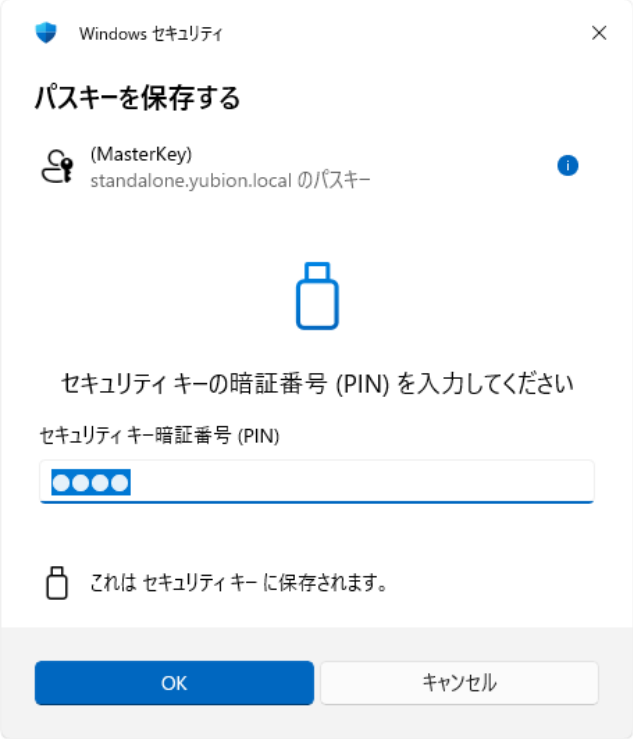
図：「+ マスターキーを登録」ボタンを選択

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が表示されます。内容を確認し、「はい」を選択します。



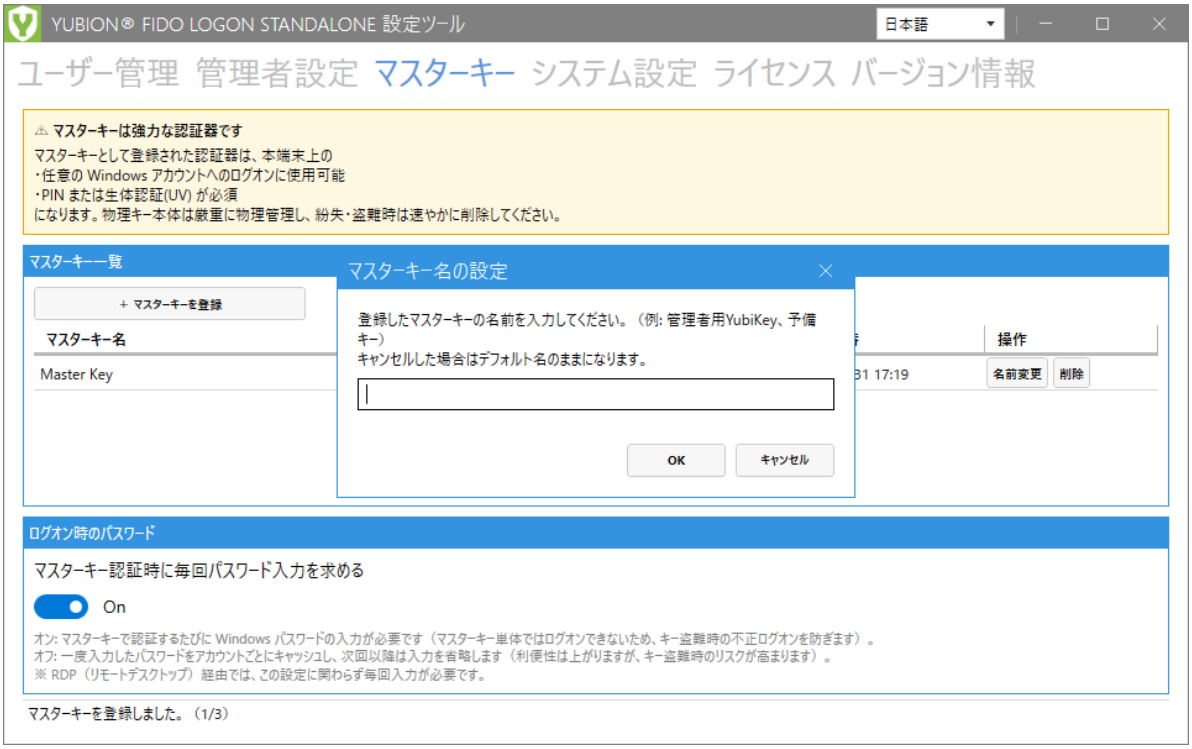
図：マスターキー登録の確認ダイアログ

4. 認証器を接続し、PIN（または生体認証）を入力し、タッチします。



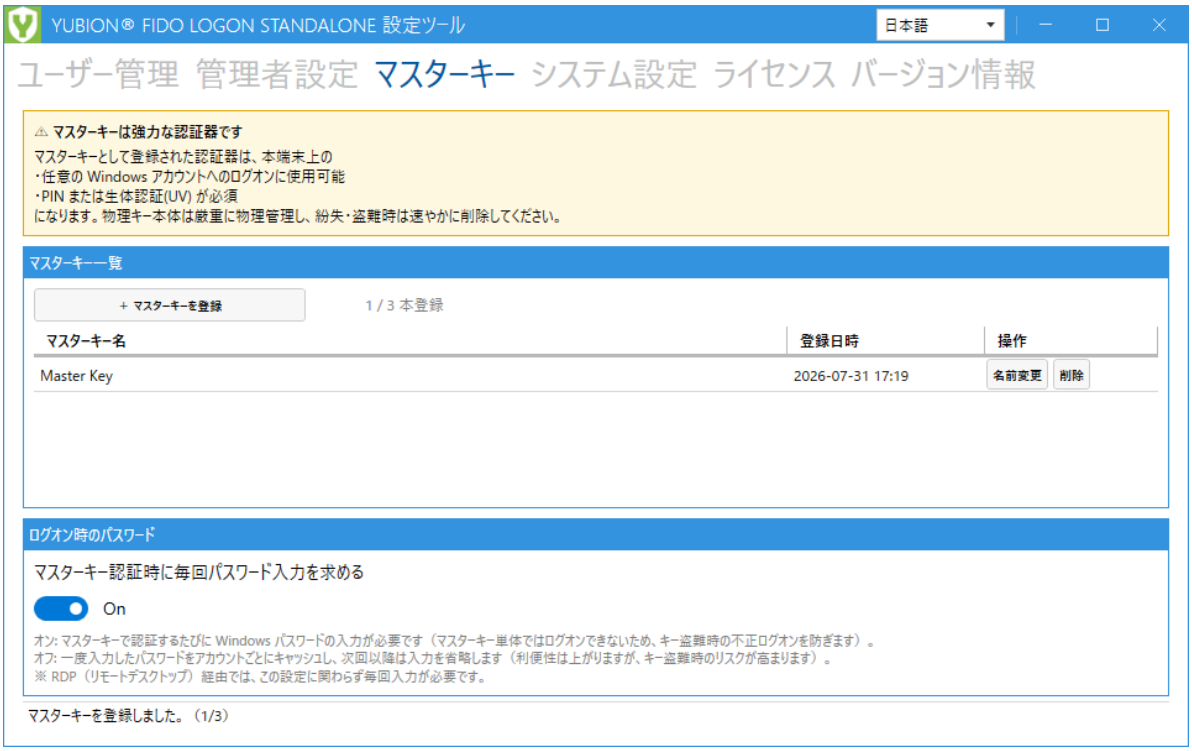
図：PIN 入力ダイアログ

5. 登録が完了すると、**マスターキー名の設定** ダイアログが表示されます。名前（例: 管理者用YubiKey、予備キー）を入力します。キャンセルした場合は既定の名前のままになり、後から「名前変更」で変更できます。



図：マスターキー名の設定ダイアログ

6. 「マスターキー一覧」に追加されたことを確認します。

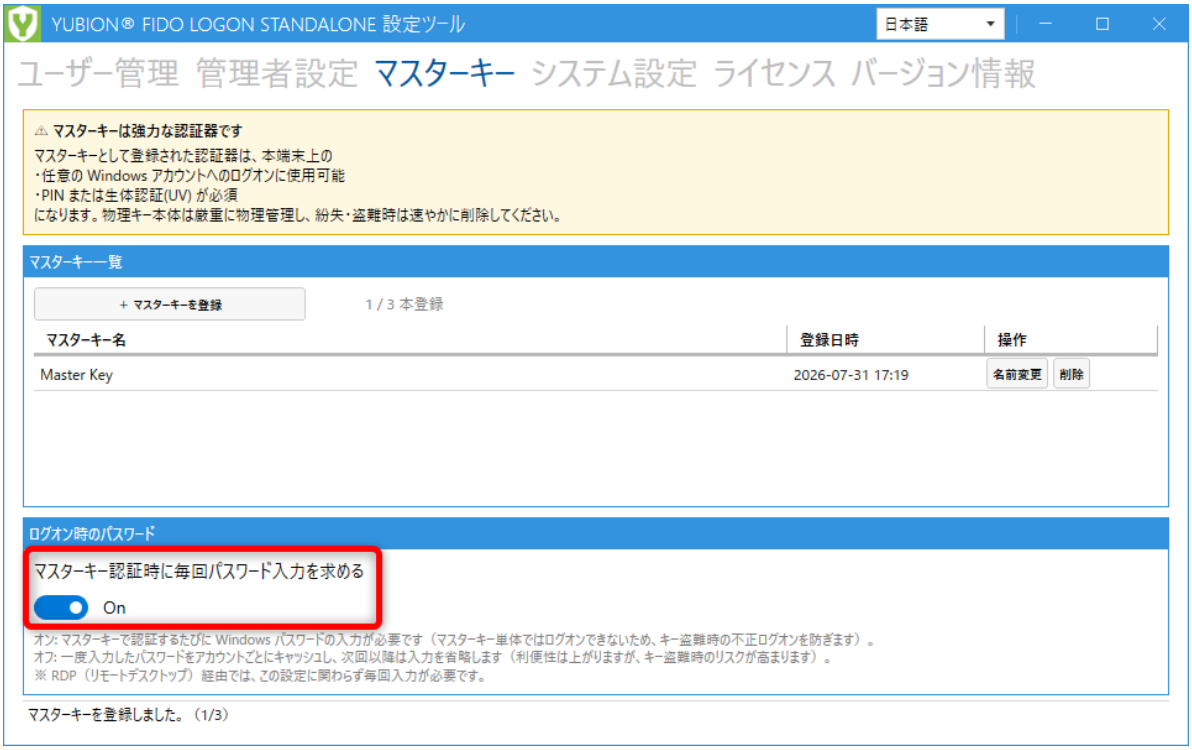


図：マスターキー一覧に追加された状態

> **注意**　Windows の **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 の場合、マスターキーを登録できません（第8章「認証器の登録（管理者による事前登録）」の注意を参照）。

9.4　運用上の注意

- マスターキーは **個人が物理的に管理し、共用しない** でください。
- マスターキーを **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。削除するまでは、そのキーで任意アカウントへログオンできてしまいます。紛失時は、あわせて全ユーザーのパスワード変更を検討してください。
- マスターキー認証時に毎回パスワード入力を求めるかどうかは、**マスターキー** タブ下部の「ログオン時のパスワード」欄にある「**マスターキー認証時に毎回パスワード入力を求める**」で設定できます（既定は無効＝キャッシュ使用）。



図：「マスターキー認証時に毎回パスワード入力を求める」設定

第10章　リカバリコードの管理

リカバリコード は、認証器が使えないときの緊急ログオンに使う使い切りのコードです。設定ツールの **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）**」欄で管理します。

> **重要（原則としてすべての端末で発行してください）**　リカバリコードは **認証器を一切使わずに** 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、リセットするまで使用できなくなりますが、**本製品はこのロックを検知できないため「認証器ログオン」の自動無効化も働きません。**登録済みの認証器・マスターキーがすべてロックし、リカバリコードも未発行の場合、セキュアモードが有効な端末では **ログオンできなくなり、本製品の設定変更では復旧できません。**予備の認証器やマスターキーを用意する場合でも、それらも同様にロックし得るため、**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**（詳細は第8章「PIN の入力ミスによる認証器ロックへの備え」）。

10.1　特徴

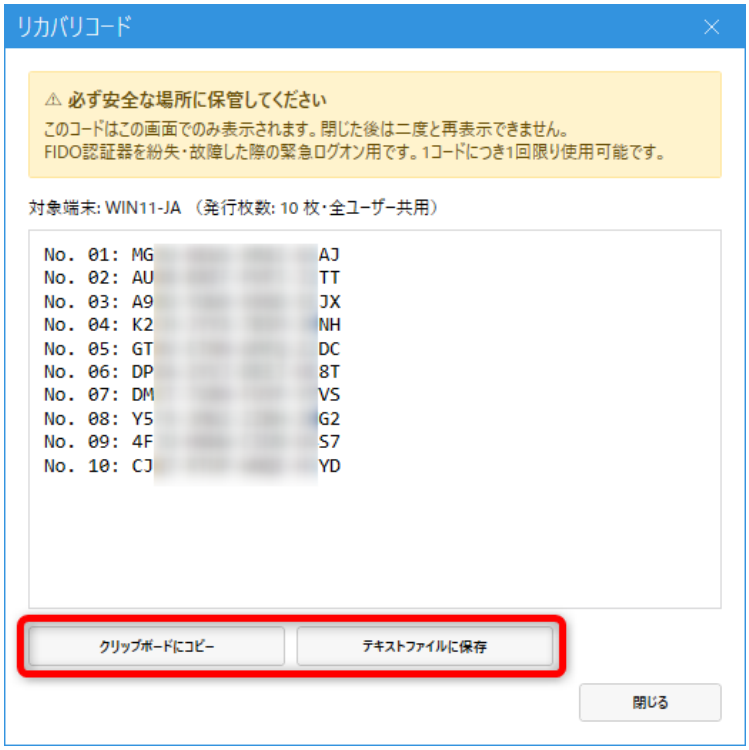
- **端末単位（全ユーザー共用）** で発行します。端末上のどのユーザーでも使用できます。
- **一括 10 枚固定** で発行します。
- 1 つのコードは **1 回だけ** 使用できます。
- コード形式は英数字 16 文字（4 桁ごとにハイフン区切り）で、十分な強度（約 78 ビット）を持ちます。
- リカバリコードだけではログオンできず、**必ず Windows パスワードの併用が必要** です。

10.2　発行手順

1. **ユーザー管理** タブを開きます。
2. 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

3. 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。

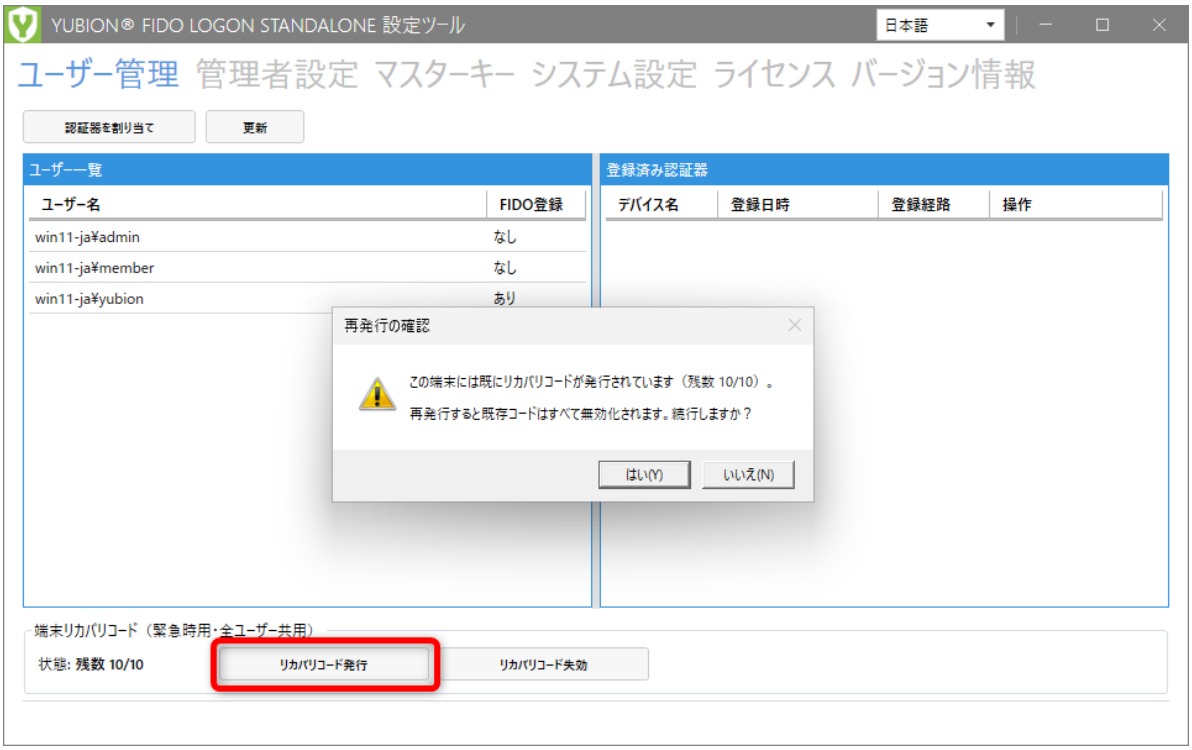


図：リカバリコード発行ダイアログ

重要　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。端末内にはコードそのものではなく、検証用のハッシュのみが保存されます。

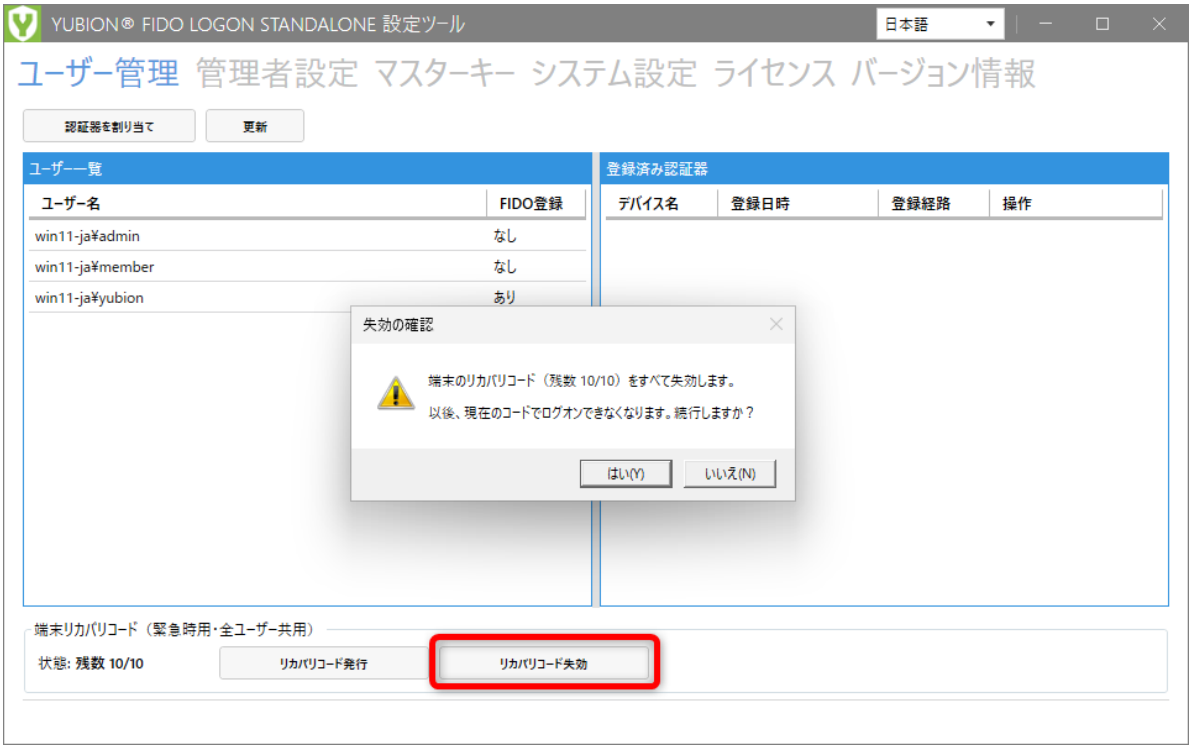
10.3　再発行・失効

- **再発行:** 発行済みの状態で「**リカバリコード発行**」を選択すると、再発行の確認ダイアログが表示されます。続行すると既存のコードをすべて無効化してから、新しく 10 枚を発行します。



図：リカバリコード再発行の確認ダイアログ

- **失効:** 「**リカバリコード失効**」を選択すると、発行済みのコードをすべて無効化します。



図：リカバリコード失効の確認ダイアログ

10.4　状態表示

リカバリコードの状態は「状態:」の右に表示されます。未発行の場合は「**未発行（発行を推奨）**」と表示され、欄全体が警告色で強調されます。発行済みの場合は「残数 X/10」のように表示されます。

図：リカバリコードの状態表示

第11章　設定・認証情報の移送（エクスポート／インポート）

設定と認証情報を別の端末へ移送したり、バックアップしたりするために、エクスポート／インポート機能を利用できます。**システム設定** タブの下部で操作します。

11.1　移送されるもの／されないもの

移送対象:

- 各種システム設定
- ユーザーの認証情報（Credential）
- 管理者 Credential
- マスターキー

移送対象外:

- ライセンスファイル、マシンコード
- リカバリコード
- パスワードキャッシュ
- ログ

> **重要（移送先端末ではリカバリコードを発行してください）**　リカバリコードは移送されないため、インポートした端末では **未発行の状態のまま** です。リカバリコードは認証器を一切使わずにログオンできる唯一の手段であり、認証器の PIN ロックによるロックアウトを防ぐ最後の備えになります。インポート後に、移送先端末で必ずリカバリコードを発行してください（第10章「発行手順」）。

11.2　エクスポート

1. **システム設定** タブ下部の「**設定の移送**」欄で「**エクスポート...**」を選択します。

図：エクスポートボタン

2. 保存先を指定してエクスポートファイル（拡張子 `.fidocfg.json`）を保存します。

> **セキュリティ**　エクスポートファイルには認証情報が含まれます。認証情報は移送元端末で復号し、移送先端末で再暗号化される仕組みです。ファイルの完全性は保護されていますが、取り扱いには十分注意し、安全な経路で受け渡してください。

11.3　インポート

1. 移送先端末の設定ツールで、**システム設定** タブ下部の「設定の移送」欄の「**インポート...**」を選択し、エクスポートファイルを指定します。

図：インポートボタン

2. **インポート確認画面** で、取り込まれるアカウントの一覧を確認します。
3. 内容を確認して実行します。

図：インポート確認ダイアログ

締め出し防止　インポート結果としてログオン可能な認証器が 0 本になる場合、「認証器ログオン」「セキュアモード」は自動的に無効化されます。

第12章　運用・保守

12.1　サポート情報の収集

障害調査のため、端末の設定・ログ等をまとめて収集できます。

1. **バージョン情報** タブを開きます。

図：バージョン情報タブ

2. 「**サポート情報の収集**」欄の「**ZIP で保存...**」を選択します。

図：ZIP で保存ボタン

3. 保存ダイアログで保存先とファイル名を指定します（初期の保存先はデスクトップです）。
4. 生成された ZIP ファイルを、サポート窓口へ安全な経路で送付します。

> **セキュリティ**　ZIP には認証情報ファイルが暗号化された状態で含まれます。別端末では復号できませんが、アカウント名や公開鍵などのメタデータは参照可能です。安全な経路で送付してください。

12.2　ログの確認

本製品の動作ログは **Windows イベントビューアー** に出力されます（イベントソース名 `YubiOnFidoLogonStandalone`）。設定ツール内にログ閲覧画面はありません。

- ログオンの成否、認証器の登録・削除・名称変更、ライセンス関連、サービス開始などが記録されます。
- 出力されるイベントの全一覧（イベント ID・レベル・内容）は「付録C イベントログ一覧」を参照してください。

12.2.1　詳細な動作ログ（ファイル）

イベントログとは別に、障害調査用の詳細ログがファイルとして出力されます。通常の運用で

参照する必要はありません（サポート窓口から依頼された場合や、前節「サポート情報の収集」で収集される対象です）。

項目	内容
出力先	%ProgramData%¥YubiOn¥FidoStandalone¥logs 配下（Service / CredentialProvider / AdministrateTool / CliTool の各フォルダー）
ローテーション	**日付単位**（例: Svc_Trace.log.20260427）
保持期間	**90 日**。これより古いファイルは **サービスが自動的に削除** します

> **注記**　自動削除はサービスが動作しているときに 1 日ごとに実行されます。サービスを長期間停止していた端末では、次回の起動後に古いログがまとめて削除されます。書き込み中のログファイルは削除対象になりません。

12.3　セーフモードでの動作

セキュアモードとセーフモードを併用してもロックアウトしないよう、サービスはセーフブート時にも起動するよう登録されます。

> **注記**　セーフモード（Minimal）で WebAuthn が認証器を列挙できるかは環境に依存します。運用前に実機でご確認ください。

第13章　トラブルシューティング

13.1　ログオンできない・FIDO タイルが表示されない

- ライセンスが「有効」であるか確認してください（第5章）。ライセンスが有効でない場合、FIDO タイルは表示されず、パスワードログオンが可能な状態になります。
- 対象ユーザーに認証器が登録されているか確認してください。
- 「認証器ログオンを有効にする」が有効か確認してください。

13.2　RDP 経由でログオンできない

- クライアント・ホストの OS バージョン、グループポリシー「WebAuthn 要求のリダイレクト」、認証器の接続先（クライアント側）を確認してください（第2章）。
- 接続先の端末で「認証器ログオンを有効にする」が有効か確認してください（セキュアモードの ON／OFF は RDP 経由でログオンできるかどうかには影響しません）。

13.3　ライセンスが「端末不一致」「OS 種別不一致」になる

- 別端末向け、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。
- マシンコードを再確認し、正しい端末向けのライセンスを取得してください。
- **PC 本体を入れ替えた、またはマザーボードを交換した端末では、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ライセンスの再発行を依頼してください（第5章「マシンコードが変わる場合・変わらない場合」）。なお **OS の再インストールではマシンコードは変わらない** ため、この事象の原因にはなりません。
- マシンコードが取得できない端末（既定値の無効な UUID が設定されている場合など）でも「端末不一致」になります。設定ツールのライセンスタブでマシンコードが表示されているか確認してください（第5章）。

13.4　認証器を紛失した／PIN を忘れた

- **リカバリコード**（第10章）による緊急ログオンを案内してください。
- 管理者は **マスターキー**（第9章）で代行ログオンできます。
- 紛失した認証器は、設定ツールから削除してください。

13.5　設定ツールで認証器を登録（割り当て）できない

次の順に確認してください。

1. **Windows の「パスキーアクセス」設定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** の場合、認証器の登録が行えません。設定ツールは登録に Windows の WebAuthn 機能を使用するため、この設定でブロックされます。**オン** にしてから登録し直してください。マスターキーの登録・管理者 Credential の登録・起動認証も同様に失敗します。設定画面に「パスキー」の項目がない Windows バージョンでは、この制限は該当しません。
2. **対象ユーザーが一覧に表示されているか。** その端末にユーザープロファイルが作成済み（一度でもログオン済み）のアカウントのみ表示されます（第8章）。
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（第2章「FIDO2 認証器の要件」）。
4. **PIN がブロックされていないか。** ブロックされている場合は下記「PIN を連続して間違えて認証器がロックされた」を参照してください。

13.6　PIN を連続して間違えて認証器がロックされた

ログオン画面のメッセージで状態を判別してください。

- 「**PIN 認証がブロックされました。キーを抜いて再挿入してください**」（一時ブロック）
  認証器を抜いて再挿入すれば、再度 PIN を入力できます。正しい PIN が分かっている場合はそのまま再試行してください。
- 「**PIN がブロックされています。キーをリセットしてください**」（完全ブロック）
  その認証器は **リセット（初期化）しないと使用できません。**リセット手順は認証器の製造元の案内に従ってください。**リセットすると認証器内の資格情報はすべて消えるため、設定ツールから当該認証器を削除し、あらためて登録し直してください。**

当該ユーザーをログオンさせる手段は次のとおりです。

1. そのユーザーに **予備の認証器** が登録されていれば、それでログオンできます。
2. **リカバリコード**（第10章）で緊急ログオンできます（Windows パスワードの併用が必要）。
3. 管理者が **マスターキー**（第9章）で代行ログオンできます。

> **警告**　上記のいずれも使えない場合（登録済みの認証器・マスターキーがすべて PIN ロックし、リカバリコードも未発行）、セキュアモードが有効な端末ではログオンできなくなります。本製品は PIN ロックを検知できないため「認証器ログオン」の自動無効化も働きません。この状態は本製品の設定変更では復旧できないため、下記の事前の備えを必ず用意してください。

事前の備えについては、第8章「PIN の入力ミスによる認証器ロックへの備え」を参照してください。

13.7　オフライン環境（AD ドメイン）での注意

- AD 参加端末がドメインコントローラーに到達できない場合でも、過去にその端末でログオン済みのユーザーは FIDO ログオンできます。
- 一度もログオンしたことのないユーザーを手入力でログオンさせることはできません（OS のキャッシュログオンと同じ制約）。

付録A 用語集

用語	説明
FIDO2	公開鍵暗号ベースのパスワードレス認証規格。
認証器（Credential / FIDO2 認証器）	YubiKey 等の FIDO2 デバイス。秘密鍵はデバイス内にあり、本製品が保存するのは公開鍵と credentialId のみ。
Credential Provider（CP）	Windows ログオン画面に組み込まれるログオン方式のプラグイン。
セキュアモード	他の CP を無効化し、本製品の FIDO ログオンのみに限定するモード。
認証器ログオン	本製品の CP を Windows に登録し、FIDO ログオンを利用可能にする設定。
hmac-secret	FIDO2 認証器の拡張。パスワードキャッシュの暗号化に使用し、認証器を接続しないと復号できない。
マスターキー	任意の Windows アカウントへログオンできる管理者用 FIDO 認証器（端末最大 3 本、UV 常時必須）。
管理者 Credential（管理者認証器）	設定ツールの起動認証（「設定ツール起動時に FIDO 認証を要求する」）に使う認証器。Windows ユーザーには紐づかない。マスターキーとは別概念。
リカバリコード	認証器が使えないときの緊急ログオン用の使い切りコード（10 枚・Windows パスワード併用必須）。
DPAPI（LOCAL_MACHINE）	Windows のデータ保護 API。端末固有鍵で暗号化し、別端末では復号できない。
RP ID	FIDO2 の Relying Party 識別子。本製品では `standalone.yubion.local` 固定。
UV（User Verification）	PIN や生体認証による本人確認。

用語	説明
マシンコード	ライセンスの端末紐づけに使う、正規化した BIOS UUID。

付録B 設定項目一覧

本文では設定を設定ツールに表示される **設定名（日本語）** で記載しています。以下は、設定ツールで設定できる項目の一覧です。

設定名（設定ツールの表示）	既定	概要
認証器ログオンを有効にする	無効	本製品 CP の登録／解除
セキュアモード	無効	他 CP を無効化し FIDO ログオンを強制
認証器取り外し時に Windows を自動ロックする	無効	認証器を抜くと自動ロック
アンインストール制御	無効	アプリ一覧に非表示
認証器未登録ユーザーのログオンを許可する	無効	未登録ユーザーのパスワードログオンを許可
初回のみパスワードでログオンし、認証器の登録を強制する	無効	未登録ユーザーに初回登録を強制
毎回パスワード入力を必須にする	無効	キャッシュ不使用・毎回入力
UV 非対応キー（U2F）の使用を許可する	無効	U2F キーの許可（キャッシュ不可）
設定ツール起動時に FIDO 認証を要求する	無効	設定ツール起動時に FIDO 認証を要求
マスターキー認証時に毎回パスワード入力を求める	無効	マスターキー認証時に毎回パスワード入力

設定ツールに表示されない内部仕様

以下は動作仕様として固定されており、設定ツールの画面には表示されません（変更できません）。

項目	値
RP ID（Relying Party 識別子）	`standalone.yubion.local`（固定）
キャッシュ有効日数	無制限

付録C イベントログ一覧

本製品は、ログオンや管理操作などの監査情報を **Windows イベントログ** に出力します。監査やトラブル調査の際にご利用ください。

出力先・ソース情報

項目	値
出力先ログ	アプリケーション（Application）ログ
イベントソース名	YubiOnFidoLogonStandalone
カテゴリ	使用しません（既定）

> **確認方法**　Windows の「イベント ビューアー」→「Windows ログ」→「Application」を開き、ソースが YubiOnFidoLogonStandalone のイベントを参照してください。

イベント ID の採番体系

番号帯	用途	主な出力元
1100–1199	FIDO 認証の結果	Credential Provider
1200–1211	ログオンの結果（FIDO／パスワード）	Credential Provider
1300–1301	自己登録（CP 経由）での認証器登録	Credential Provider
1400–1401	リカバリコードによるログオン	サービス
1500–1521	マスターキーによる認証・ログオン	Credential Provider
1600–1601	アカウント ID 手入力ログオンの入口エラー	Credential Provider

番号帯	用途	主な出力元
2100–2103	セッション（ログオン／ログオフ／ロック）	サービス
2200	認証器取り外しによる自動ロック	サービス
2900–2912	サービス状態・ライセンスファイル監視	サービス
3100–3201	設定のエクスポート／インポート	設定ツール
3300–3302	リカバリコードの管理	設定ツール
3400–3401	サポート情報の収集	設定ツール
3500–3502	マスターキーの管理	設定ツール
3600–3602	ユーザー認証器（Credential）の管理	設定ツール
3700–3701	ライセンスのインポート	設定ツール

> **メッセージ本文の主な項目**　User（ユーザー名）、SID、Session ID（セッション）、Client（接続元。ローカル／RDP クライアント名）、Authenticator（認証器名）、Device ID、NTSTATUS（ログオン結果コード）など。EntraID アカウントは AzureAD¥{UPN} 形式で記録されます。

ログオン・認証（Credential Provider）

FIDO 認証の結果（1100–1199）

ID	レベル	内容	発生タイミング
1100	情報	FIDO 認証成功	認証器の assertion 検証に成功したとき
1110	警告	FIDO 認証失敗：PIN 間違い／PIN ブロック	誤った PIN 入力、または PIN がブロックされたとき
1111	情報	FIDO 認証失敗：キャンセル	ユーザーが認証を中止したとき
1112	警告	FIDO 認証失敗：タイムアウト	認証が時間切れになったとき
1113	警告	FIDO 認証失敗：未登録の認証器	登録されていない認証器が使用された／検証が拒否されたとき
1114	エラー	FIDO 認証失敗：サービス未起動・通信不能	サービスへのチャレンジ要求／検証通信に失敗したとき
1199	エラー	FIDO 認証失敗：その他	上記以外の例外（CTAP エラー、デバイス取り外し、PIN 未設定 等）

ログオンの結果（1200–1211）

ID	レベル	内容	発生タイミング
1200	情報	ログオン成功（FIDO 経由）	FIDO タイルからの Windows ログオン成功
1201	警告	ログオン失敗（FIDO 経由）	FIDO 認証成功後の Windows ログオン失敗（パスワード不一致 等）
1210	情報	パスワードログオン成功	パスワード単独タイルからのログオン成功
1211	警告	パスワードログオン失敗	パスワード単独タイルからのログオン失敗

自己登録での認証器登録（1300–1301）

ID	レベル	内容	発生タイミング
1300	情報	自己登録による認証器登録成功	CP の自己登録フローで認証器の登録に成功したとき

ID	レベル	内容	発生タイミング
1301	警告	自己登録による認証器登録失敗	同フローで登録に失敗したとき（キャンセル・PIN 関連・通信失敗 等）

リカバリコードによるログオン（1400–1401）

ID	レベル	内容	発生タイミング
1400	警告	リカバリコードログオン成功	リカバリコード検証後にログオン完了したとき（残数も記録）
1401	警告	リカバリコードログオン失敗	コード不一致・使用済み・未発行のとき

> リカバリコードは認証器の紛失・故障などの緊急時のみ使われるため、成功も「警告」レベルで記録し、監査で目立つようにしています。

マスターキーによる認証・ログオン（1500–1521）

ID	レベル	内容	発生タイミング
1500	警告	マスターキー認証成功	マスターキーによる認証に成功したとき（対象アカウント・キー名を記録）
1520	警告	マスターキー経由ログオン成功	マスターキー認証後の Windows ログオン成功
1521	警告	マスターキー経由ログオン失敗	マスターキー認証成功後の Windows ログオン失敗

> **注記**　マスターキーは任意アカウントへログオンできる強力な権限のため、成功も「警告」レベルで記録します。
> マスターキー認証の **失敗**（PIN 間違い・キャンセル・タイムアウト 等）は、専用イベントではなく通常の FIDO 認証失敗（**1110〜1199**）として記録されます。

アカウント ID 手入力ログオンの入口エラー（1600–1601）

ID	レベル	内容	発生タイミング
1600	警告	手入力アカウントが見つからない	「その他のユーザー」で入力した ID が解決できないとき
1601	情報	手入力アカウントに認証器が未登録	解決できたが認証器が未登録のとき（以降の動作も記録）

サービス

セッション通知（2100–2103）

ID	レベル	内容	発生タイミング
2100	情報	ログオン（セッション開始）	セッションのログオンを検知したとき
2101	情報	ログオフ	セッションのログオフを検知したとき
2102	情報	端末ロック	画面ロックを検知したとき
2103	情報	端末ロック解除	ロック解除を検知したとき

自動ロック（2200）

ID	レベル	内容	発生タイミング
2200	警告	認証器取り外しによる自動ロック	認証器取り外しで自動ロックを実行したとき

サービス状態・ライセンス監視（2900–2912）

ID	レベル	内容	発生タイミング
2900	情報	サービス開始	サービス開始時（セキュアモード状態・ライセンス情報を記録）
2901	情報	サービス停止	サービス停止時
2910	情報	ライセンスファイル更新	有効なライセンスファイルの更新を検知したとき
2911	警告	不正なライセンスを検知・自動復元	不正なライセンスファイルを検知し、バックアップから復元したとき
2912	警告	不正なライセンスを検知（復元不可）	不正を検知したがバックアップから復元できなかったとき

設定ツールでの管理操作

> これらのイベントには、操作者（Operator / 〜 by）が記録されます。

設定のエクスポート／インポート（3100–3201）

ID	レベル	内容	発生タイミング
3100	情報	設定エクスポート成功	設定・認証情報のエクスポート完了時
3101	警告	設定エクスポート失敗	エクスポート失敗時
3200	情報	設定インポート成功	設定・認証情報のインポート完了時
3201	警告	設定インポート失敗	インポート失敗時

リカバリコードの管理（3300–3302）

ID	レベル	内容	発生タイミング
3300	情報	リカバリコード発行	新規にリカバリコードを発行したとき
3301	警告	リカバリコード再発行	既存を破棄して再発行したとき

ID	レベル	内容	発生タイミング
3302	警告	リカバリコード失効	リカバリコードを失効させたとき

サポート情報の収集（3400–3401）

ID	レベル	内容	発生タイミング
3400	情報	サポート情報収集 実行	サポート情報（ZIP）の生成完了時
3401	警告	サポート情報収集 失敗	収集に失敗したとき

マスターキーの管理（3500–3502）

ID	レベル	内容	発生タイミング
3500	情報	マスターキー登録	マスターキーを登録したとき
3501	警告	マスターキー削除	マスターキーを削除したとき
3502	情報	マスターキー名称変更	マスターキーの名称を変更したとき

ユーザー認証器（Credential）の管理（3600–3602）

ID	レベル	内容	発生タイミング
3600	情報	認証器の登録	設定ツールからユーザーの認証器を登録したとき
3601	警告	認証器の削除	ユーザーの認証器を削除したとき
3602	情報	認証器の名称変更	認証器の名称を変更したとき

ライセンスのインポート（3700–3701）

ID	レベル	内容	発生タイミング
3700	情報	ライセンスインポート成功	ライセンスのインポート完了時（ライセンス情報を記録）
3701	警告	ライセンスインポート失敗	インポート時の検証で拒否されたとき

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**、または下記の **YubiOn サポートデスク** へご連絡ください。

サポート窓口

項目	内容
窓口名称	YubiOn サポートデスク（株式会社 ソフト技研）
受付時間	平日 9:00〜17:00（土日・祝日および弊社休業日を除く）
メール	support@yubion.com
製品情報	https://www.yubion.com/

お問い合わせの際は、第12章「サポート情報の収集」で取得した ZIP ファイルを添付いただくと、調査がスムーズに進みます。

製造元

項目	内容
製造元	株式会社 ソフト技研
Web サイト	https://sgk.co.jp/