YubiOn
WindowsLogon Standalone
設定マニュアル

2020/10/16 作成

2024/07/26 更新

株式会社　ソフト技研

目次

1． 注意事項

- **「YubiOn WindowsLogon Standalone」のインストールに必要な権限**

  「YubiOn WindowsLogon Standalone」(以下「本ソフトウェア」とします)のインストールには、コンピューターの管理者権限が必要です。

  管理者権限がないユーザーでインストールした場合、実行時に管理者アカウントの ID とパスワードの入力が必要です。

  ※ユーザーの権限の確認方法は、13.サポート情報「管理者権限の確認方法」を参照ください。

  ※ユーザーアカウント制御(UAC)を有効にする必要があります。(既定では有効設定になっています。)

- **Windows の最新アップデートを適用**

  本ソフトウェアをインストールする前に、最新の Windows Update を適用してください。

- **ライセンスファイルについて**

  本ソフトウェアを実行するためにはライセンス登録が必要です。販売元から、ライセンス登録を行うためのライセンスファイルを入手してください。ライセンスファイルが手元にない場合、販売元へお問合せください。

- **本ソフトウェアに使用できる認証器**

  ソフトウェアインストール後に設定できる認証器は、本ソフトウェアと一緒にご購入いただいた認証器のみに限定されます。使用する認証器の追加等が必要な場合、販売元へお問合せください。

  （お客様が独自に入手された認証器は、ご利用できません。）

- **ATKey をご利用の場合**

  ATKey を本ソフトウェアでご利用になる前に、指紋登録を完了している必要があります。また、キーをご利用の際は、OTP モード（黄色点灯状態）で認証を行う必要があります。

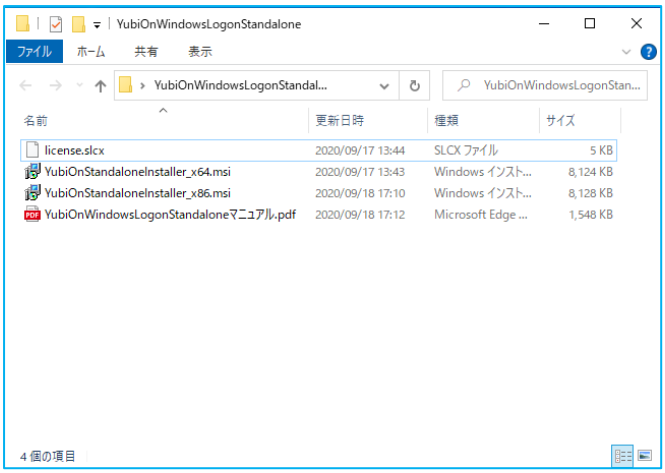
  （詳細は、ユーザーズマニュアルをご参照ください）

2. インストール方法

1. インストーラーとライセンスファイルを準備してください

任意のフォルダに本ソフトウェアのインストーラーとライセンスファイルを準備します。

YubiOnWindowsLogonStandalone マニュアル.pdf …本マニュアル
YubiOnStandaloneInstaller_x64.msi …64bitOS 用インストーラー
YubiOnStandaloneInstaller_x86.msi …32bitOS 用インストーラー
license.slcx …ライセンスファイル



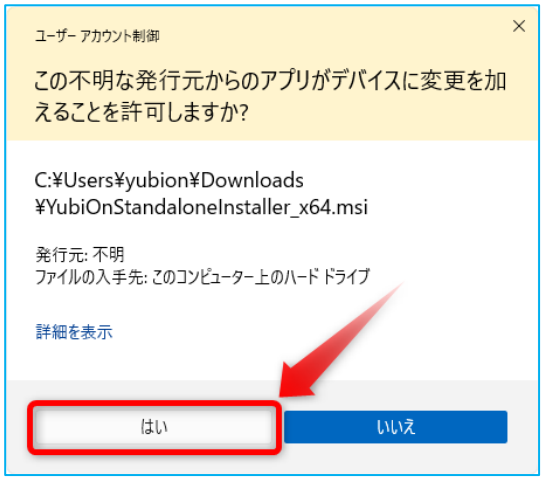
2. インストールする Windows OS のビット数の msi ファイルをダブルクリックしてください

msi ファイル	OS ビット数
YubiOnStandaloneInstaller_x64.msi	64 ビット
YubiOnStandaloneInstaller_x86.msi	32 ビット

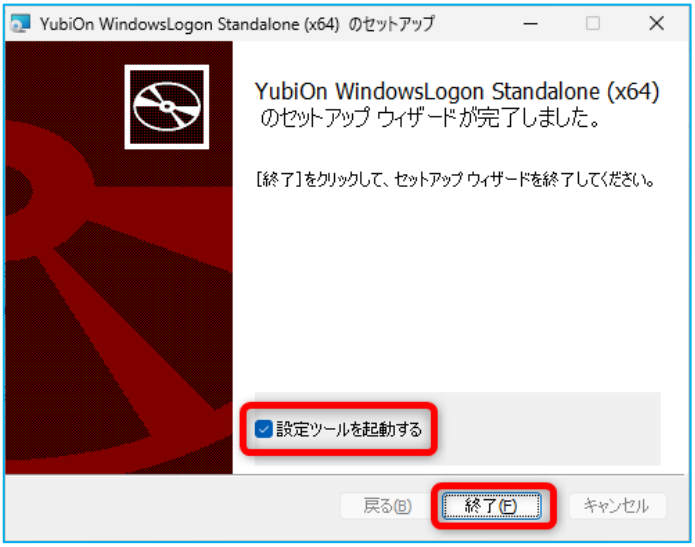
※お使いの環境が分からない場合は、13.サポート情報「OS 環境の確認方法」を参照してください。

3. インストール画面に従ってインストールを行ってください

ソフトウェアライセンス条項をお読みになり、同意してください。



ユーザーアカウント制御のメッセージが表示された場合は、「はい」をクリックしてください。



「終了」をクリックするとインストールが完了します。

スタートメニューに WindowsLogon Standalone 設定ツール(設定ツール)が追加されます。

「設定ツールを起動する」にチェックを入れておくと、続けて設定ツールが起動します。

3． 設定ツールの起動

YubiOn WindowsLogon Standalone を有効化するには、設定ツールを起動し、初期設定を行います。
まず、設定ツールを起動しましょう。

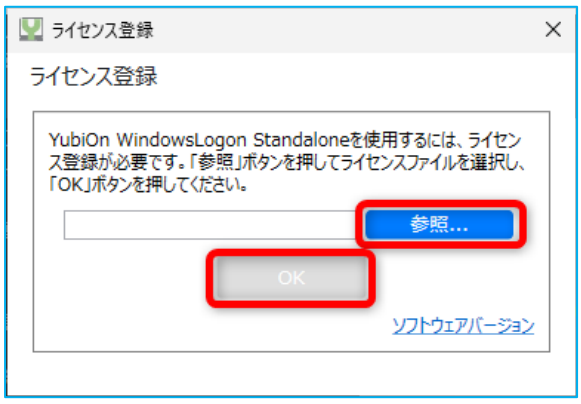
設定ツール内の名称表記変更
Ver.3.6.0 以降、ツール内の「YubiKey」表記を「認証器」に変更しました。

1. YubiOn 設定ツールを起動します

インストール完了時に「設定ツールを起動する」にチェックを入れていると、自動的に起動します。またはスタートメニューから「WindowsLogon Standalone 設定ツール」をクリックしてください。
※Windows10 の場合は、「YubiOn」フォルダの下にあります。
※設定ツールの実行は、管理者権限を持ったユーザーで実行してください。
※AD アカウントに割り当てを行う場合は、AD アカウントでログオンした状態で起動してください。

2. ライセンスファイルを読み込みます

初回起動時は、ライセンス登録ウィンドウが表示されます。参照ボタンをクリックし、ライセンスファイル(license.slcx)を読み込んで「OK」ボタンをクリックしてください。
※ライセンスファイルがない場合は本ソフトウェアを動作させることができません。手元にない場合は販売元にお問い合わせください。

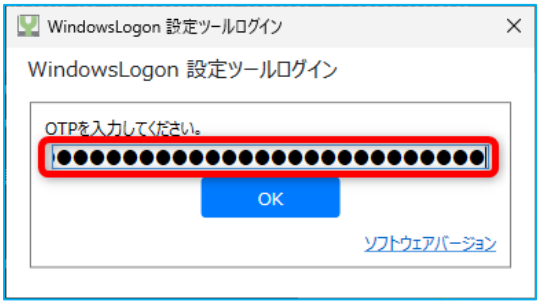


3. 認証器から出力した OTP を入力して設定画面を表示します

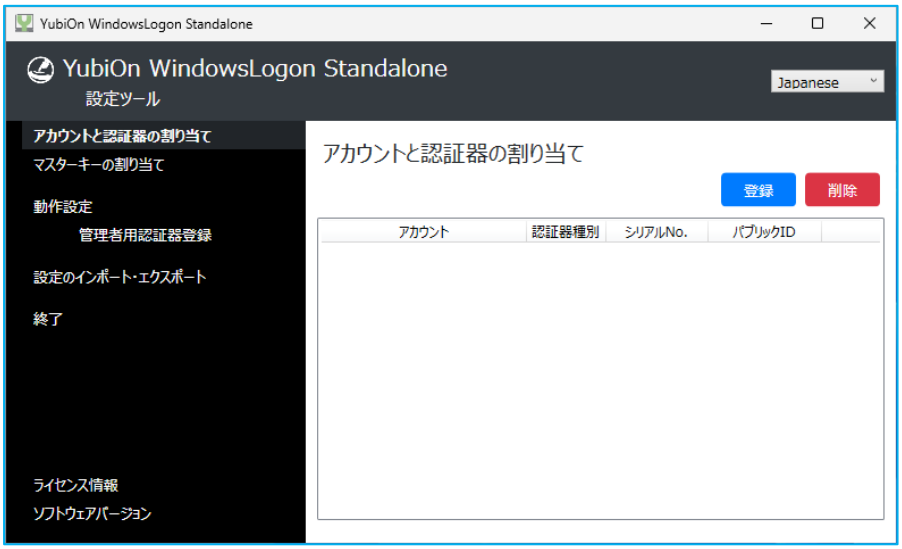
認証器を USB ポートに挿入し、ワンタイムパスワード(OTP)を入力します。

ATKey をご利用の場合

事前に、ATKey に指紋登録を行っておく必要があります。
※登録方法は、ユーザーズマニュアル（ATKey 版）をご参照ください。
また、ご利用の際、FIDO2 モード（青色点灯状態）になっている場合は、
本体側面のスイッチを押して、OTP モード（黄色点灯状態）に切り替えてください。
切り替えた後に、指紋登録した指でセンサー部をタッチし、OTP を出力します。



入力された OTP の入力値が正常の場合、設定ツールが起動します。



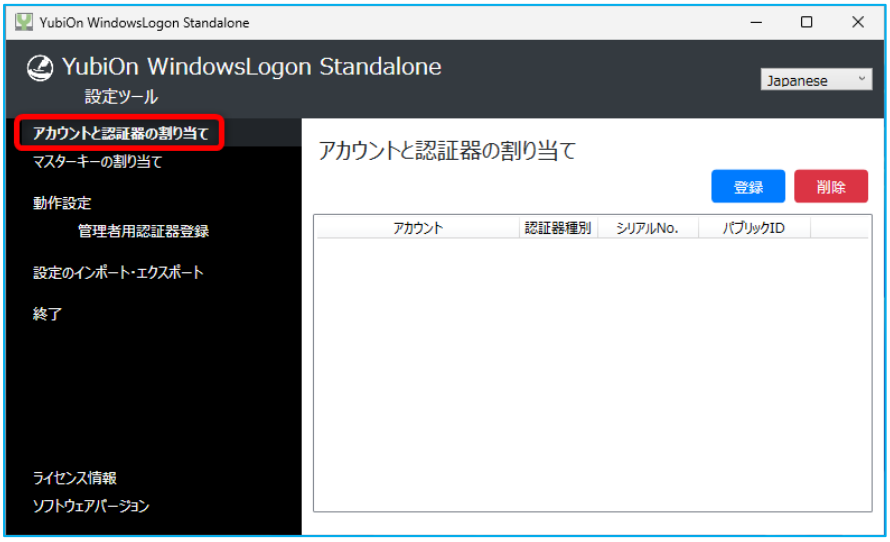
4． 認証器の登録と各種設定の流れ

認証器による二段階認証の設定の流れです。

1. 認証器を登録します

アカウントと認証器の割り当て画面で、使用する認証器とアカウントの割り当てを登録します。

登録方法は、「5.認証器の登録方法」を参照ください。



2. YubiOn 設定を有効にします

動作設定画面で、「認証器によるログオンを有効にする」をオンにします。設定方法は、「8． 各機能の設定方法」を参照ください。※YubiOn の動作確認をするまでは、セキュアモードを有効にしないでください。

3. YubiOn の動作を確認します

端末を一度スクリーンロック(Windows キー ＋ L)します。ログオン画面にて「Windows のパスワード」と「認証器のワンタイムパスワード(OTP)」でログオンできることを確認します。

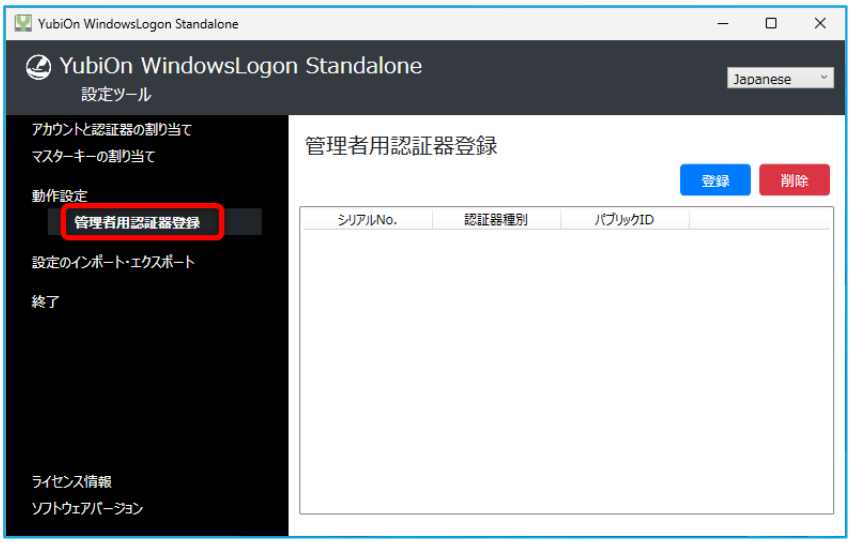
※ログオン方法の詳細については、別紙のユーザーズマニュアルを参照ください。

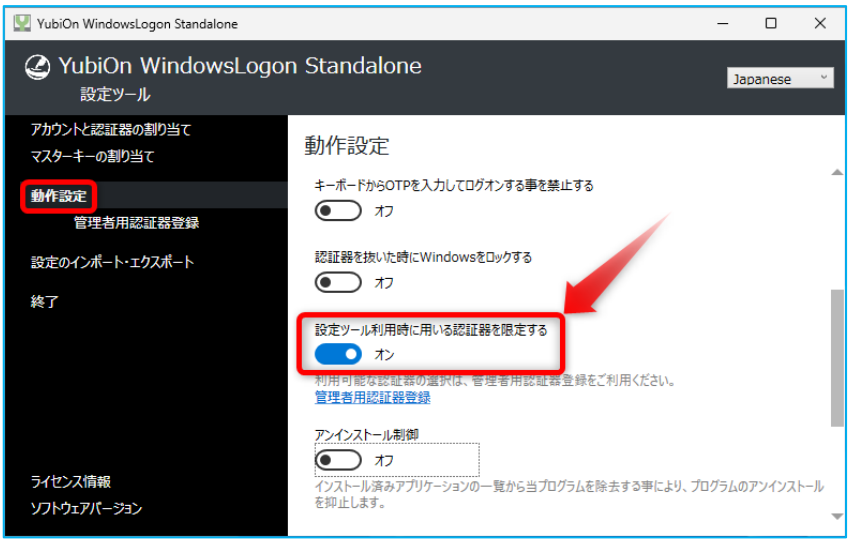
4. 認証器でのログオンを強制させる

認証器でのログオンを強制させるために、動作設定画面で「セキュアモードにする」をオンにします。その他、ロック機能、OTP 手入力制限、アンインストール制御もこちらで設定できます。設定方法は、「8. 各機能の設定方法」を参照ください。

5. その他の設定（管理者設定）

管理者用認証器の登録画面で、管理者用の認証器を登録し、動作設定画面で設定ツールの起動の制限を設定することができます。設定方法は、「9.管理者設定の方法」を参照ください。





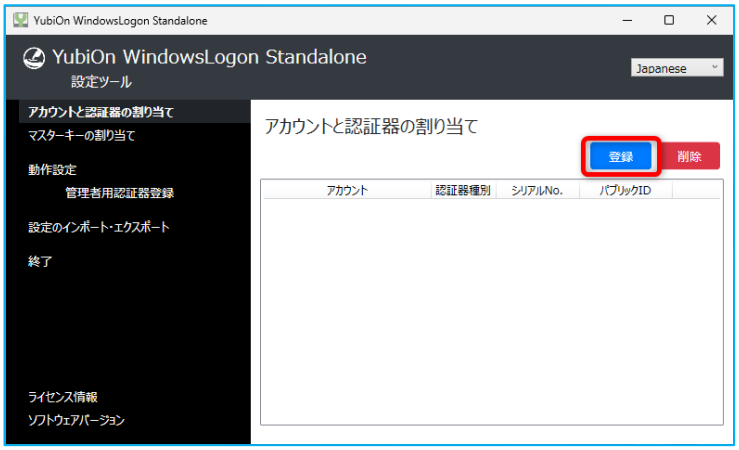
5． 認証器の登録方法

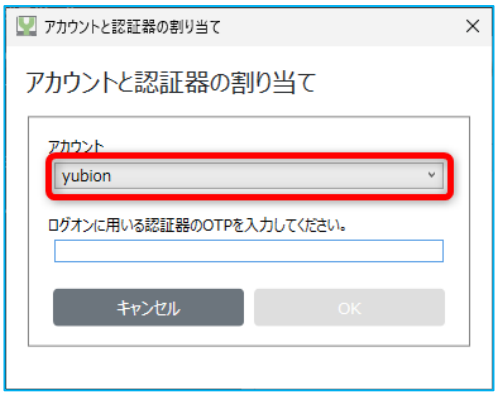
1. 「アカウントと認証器の割り当て」の「登録」ボタンをクリックします

2. 認証器と割り当てを行うアカウントを選択します

アカウントの選択項目で、ログオンで利用するアカウントを選択します。

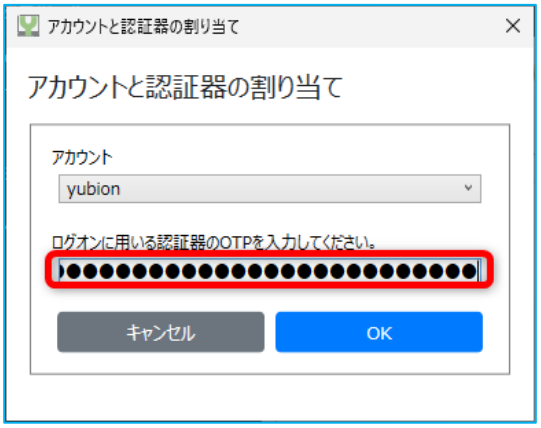
※アカウントの選択ボックスはその PC にログオン可能なアカウントのみ表示されます。その PC にログオンしたことがないドメインアカウントは表示されません。

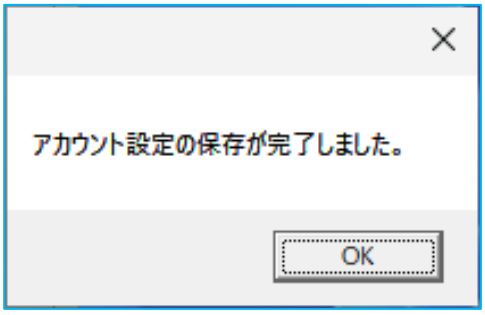




3. 認証器をタッチして登録します

OTP 入力欄にカーソルを合わせ、認証器を USB ポートに挿します。認証器のセンサー部分をタッチして（ATKey の場合は、側面のスイッチを押して OTP 出力モードに切り替える必要があります）、ワンタイムパスワード（OTP）を入力します。OTP を入力すると、割り当て登録が完了しますので「OK」をクリックしてください。





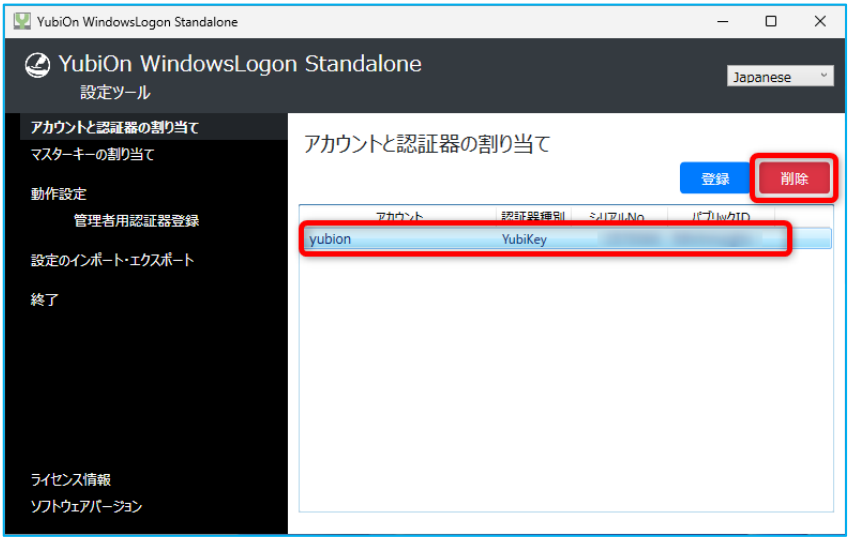
※初回登録時は、「認証器によるログオンを有効にする」をオンに変更するかの確認メッセージが表示されます。この設定は「動作設定」で後から変更することができます。

6． 登録情報の削除方法

登録したアカウントと認証器割り当ての削除を行えます。

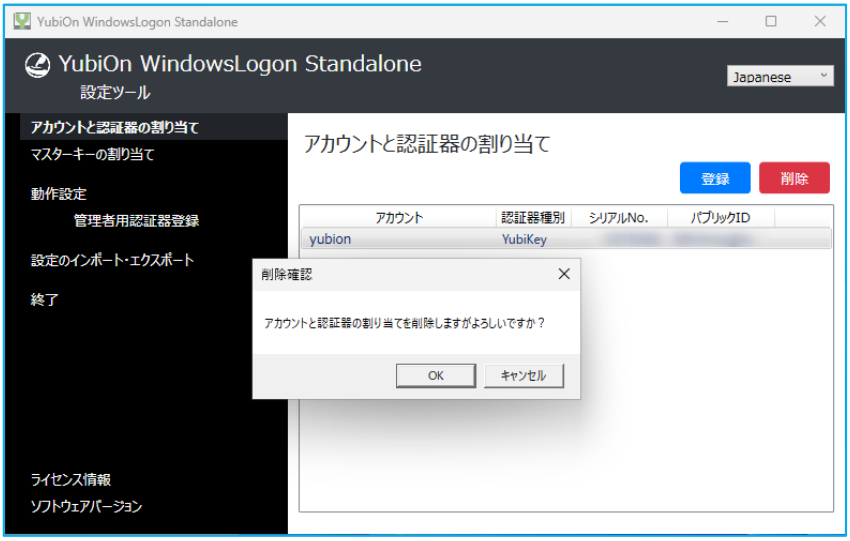
1. 削除したい割り当てを選択します

削除したいアカウントと認証器の割り当てを選択し、「削除」ボタンをクリックしてください。



2. 削除を実行します

確認ポップアップ画面で、「OK」ボタンをクリックして削除を実行します。

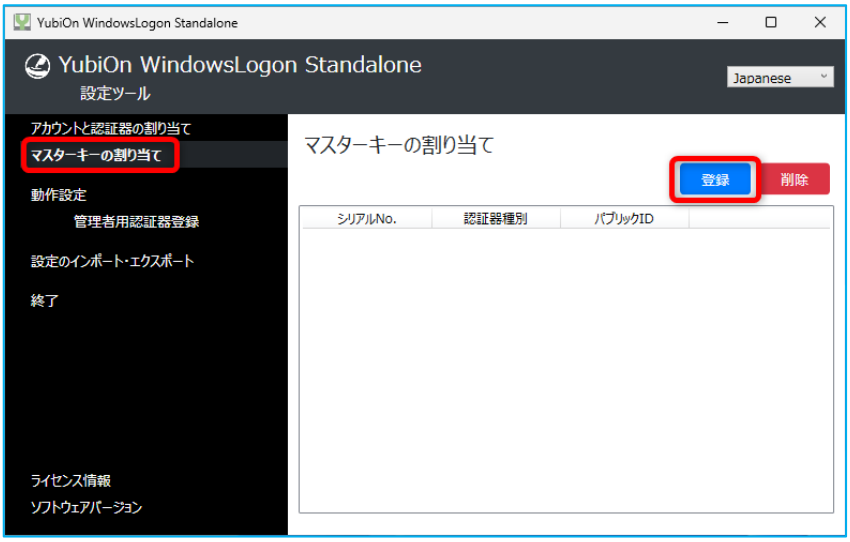


※削除した結果、マスターキー登録を含めたすべての割り当てが削除された場合、「認証器によるログオンを有効にする」が自動的にオフに切り替わります。

7． マスターキーの登録方法

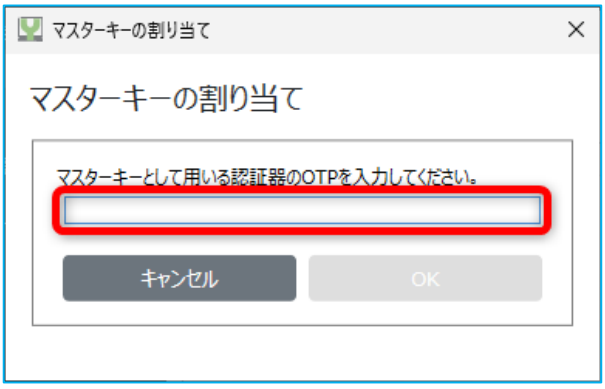
割り当てにかかわらず、すべてのアカウントのログオンに利用できる認証器(マスターキー)を登録することができます。

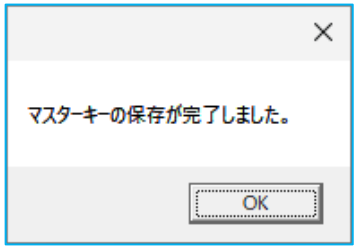
1. 「マスターキーの割り当て」の「登録」ボタンをクリックします



2. 認証器を登録します

OTP 入力欄にカーソルを合わせ、認証器を USB ポートに挿します。認証器のセンサー部分をタッチして（ATKey の場合は、側面のスイッチを押して OTP 出力モードに切り替える必要があります）、ワンタイムパスワード（OTP）を入力します。OTP を入力すると、割り当て登録が完了しますので「OK」をクリックしてください。





3. 一覧に登録した認証器が表示されます

マスターキーに登録した認証器は一覧に表示されます。

登録を削除する場合は一覧から対象の認証器を選択し、「削除」ボタンをクリックしてください。

8． 各機能の設定方法

動作設定画面で各機能の設定を行えます。

● 認証器によるログオンを有効にする

YubiOn の有効・無効を設定します。

「オフ」

YubiOn を無効にします。通常のログオン方法になります。

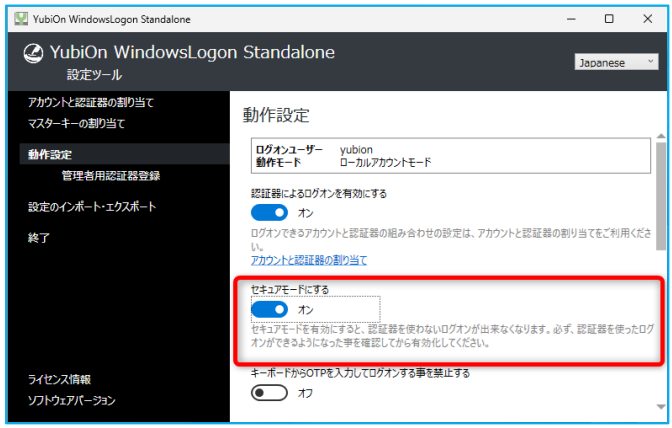
「オン」

YubiOn を有効にします。通常のログオンと認証器を使うログオンの両方が可能になります。

有効にすることで「セキュアモードにする」の項目が変更可能になります。

※「アカウントと認証器の割り当て」または「マスターキーの設定」が登録されていない場合は、有効にできません。

● セキュアモードにする



YubiOn の動作モードを選択します。

「オフ」

通常のログオンと認証器を使うログオンの両方でログオンが可能です。

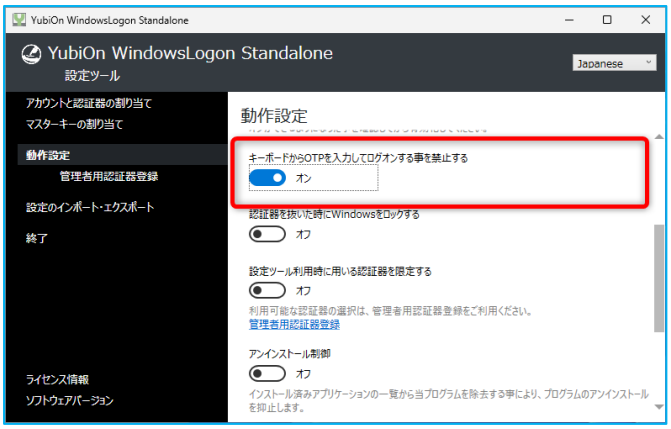
※この設定がオフの場合、認証器を使わない通常のログオンが可能なため、セキュリティの強化が十分ではありません。セキュリティを強化するため、セキュアモードの設定をおすすめします。なお、オンに設定する前に、認証器を使ってログオンできることを確認してください。

「オン」

認証器を使うログオンのみ可能になります。

ログオン時には必ず認証器が必要となるため、セキュリティが強化されます。

● キーボードから OTP を入力してログオンすることを禁止する



OTP の入力制限の設定を行います。

「オフ」

OTP 手入力を許可します。

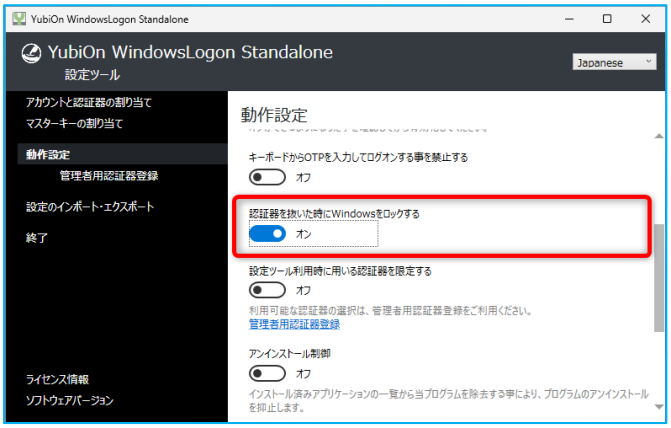
キーボードからの OTP 手入力が可能です。

「オン」

OTP 手入力を禁止します。

この状態では、認証器をタッチした入力のみ可能です。キーボードで OTP を手入力した場合はログオンできません。

● 認証器を抜いたときに Windows をロックする



認証器を抜いた時に自動的にスクリーンロックを行う機能(ロック機能)を設定します。

「オフ」

ロック機能を無効にします。

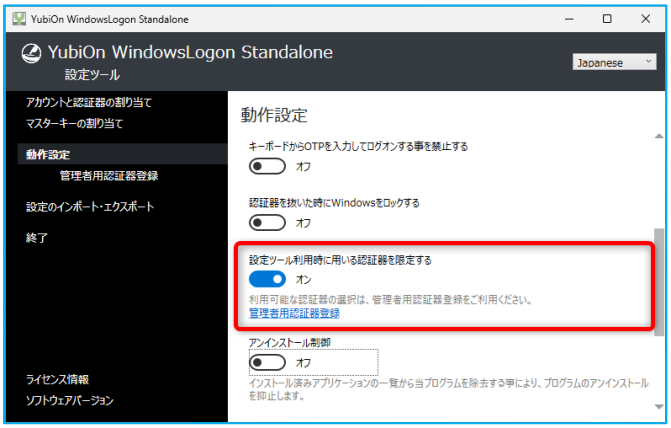
認証器を抜いてもログオン画面に切り替わりません。

「オン」

ロック機能を有効にします。

認証器を抜くと、自動的にログオン画面に切り替わります。

● 設定ツール利用時に用いる認証器を限定する



設定ツールを利用できる認証器を限定する設定を行います。

「オフ」

設定ツール起動時に利用できる認証器を限定しません。

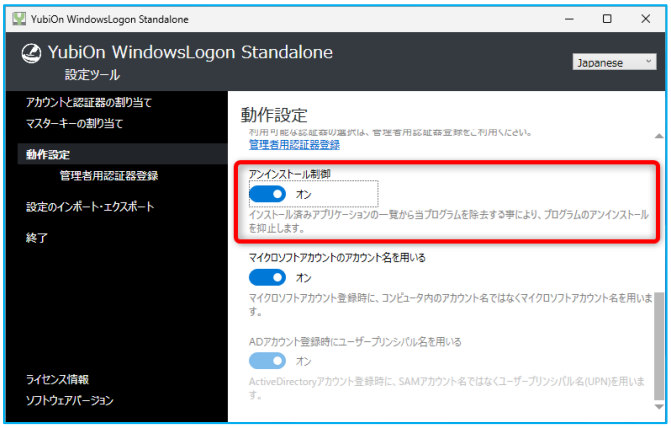
ライセンス許可されているすべての認証器で設定ツールが利用できます。

「オン」

設定ツール起動時に利用できる認証器を限定します。

この状態では、「管理者用認証器の設定」で登録した認証器のみ設定ツールを利用できます。

● アンインストール制御



ユーザーが本ソフトウェアをアンインストールしないように抑制する設定を行います。

「オフ」

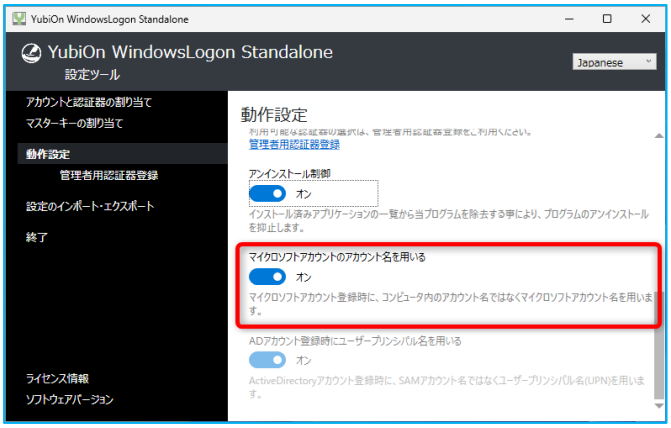
アンインストール制御を行いません。

「オン」

Windows のインストール済みアプリケーション一覧に、本ソフトウェアを表示しません。

この状態でアンインストールする場合は、本ソフトウェアインストール時に使用したインストーラーを実行して「削除」を選択します。

● マイクロソフトアカウントのアカウント名を用いる



マイクロソフトアカウントを「アカウントと認証器の割り当て」で割り当てする時の表示設定を行います。

「オフ」

マイクロソフトアカウントをローカルアカウント形式※で表示します。

※ローカルアカウント形式の例

user_000

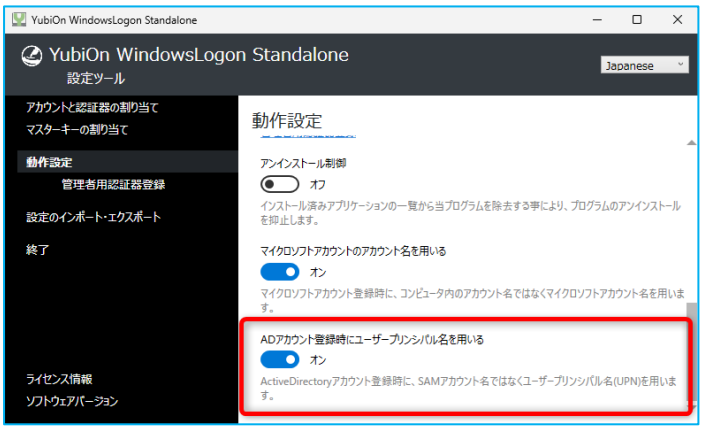
「オン」

マイクロソフトアカウントをマイクロソフトアカウント形式※で表示します。

※マイクロソフトアカウント形式の例

user@example.com

● AD アカウント登録時にユーザープリンシパル名を用いる



AD アカウントを「アカウントと認証器の割り当て」で割り当てする時の表示設定を行います。
この設定は AD アカウントでログオン中のみ設定可能です。設定は AD サーバーに接続可能な状態で行う必要があります。

「オフ」
AD アカウントを SAM アカウント形式※で表示します。

※SAM アカウント形式の例
domain¥user

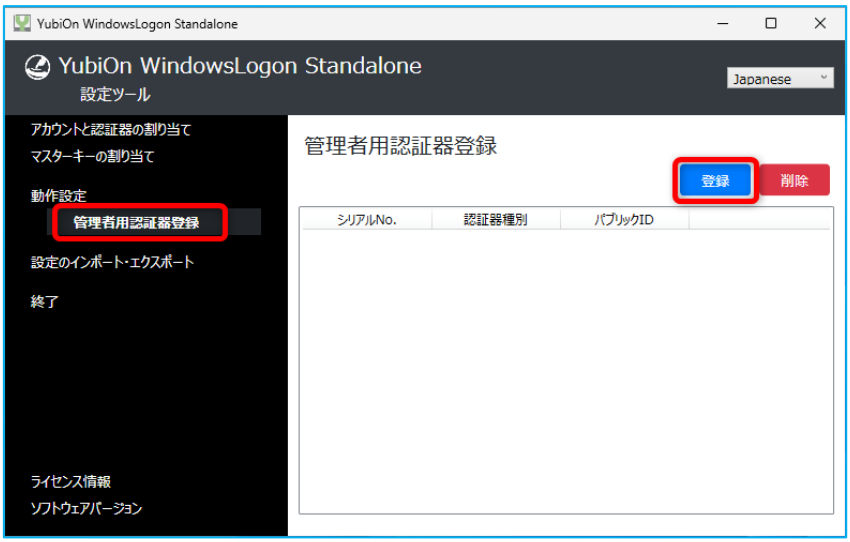
「オン」
AD アカウントをユーザープリンシパルネーム(UPN)形式※で表示します。

※ユーザープリンシパルネーム(UPN)形式の例
user@domain.com

9． 管理者設定の方法

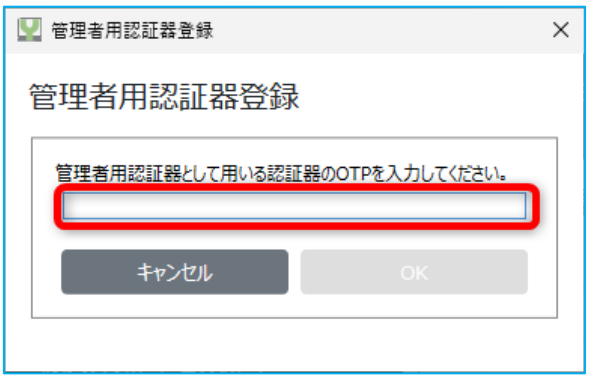
管理者用認証器登録より、設定ツール起動を許可する認証器を登録することができます。

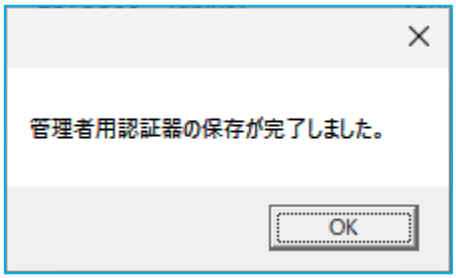
1． 「管理者用認証器登録」の「登録」ボタンをクリックします



2． 認証器を登録します

入力欄にカーソルを合わせ、認証器を USB ポートに挿します。認証器のセンサー部分をタッチして（ATKey の場合は、側面のスイッチを押して OTP 出力モードに切り替える必要があります）、ワンタイムパスワード（OTP）を入力します。OTP を入力すると登録が完了しますので「OK」をクリックしてください。

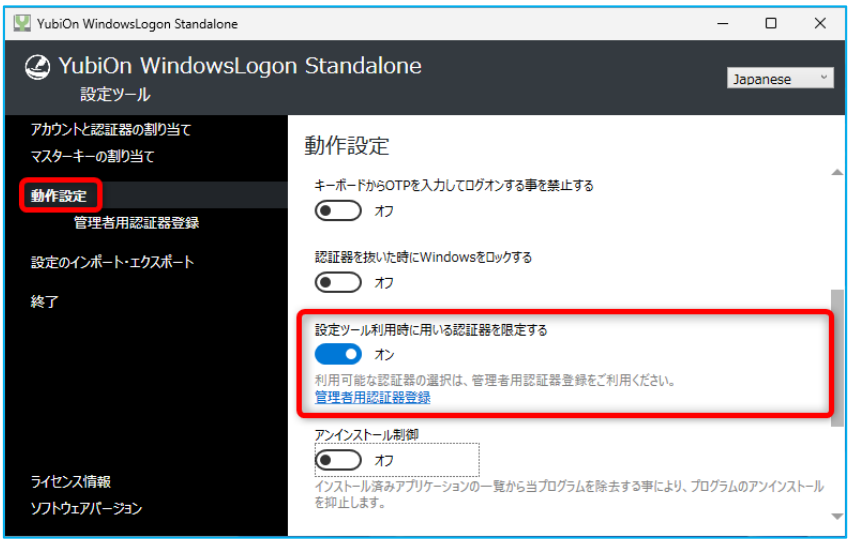




3. 「設定ツール利用時に用いる認証器を限定する」設定を有効にします

初回登録時、設定を有効化する確認メッセージが表示されますので、「はい」をクリックしてください。

この設定は、「動作設定」の項目で後から変更することができます。



4. 一覧に登録した認証器が表示されます

管理者用に登録した認証器は一覧に表示されます。

登録を削除する場合は一覧から対象の認証器を選択し、「削除」ボタンをクリックしてください。

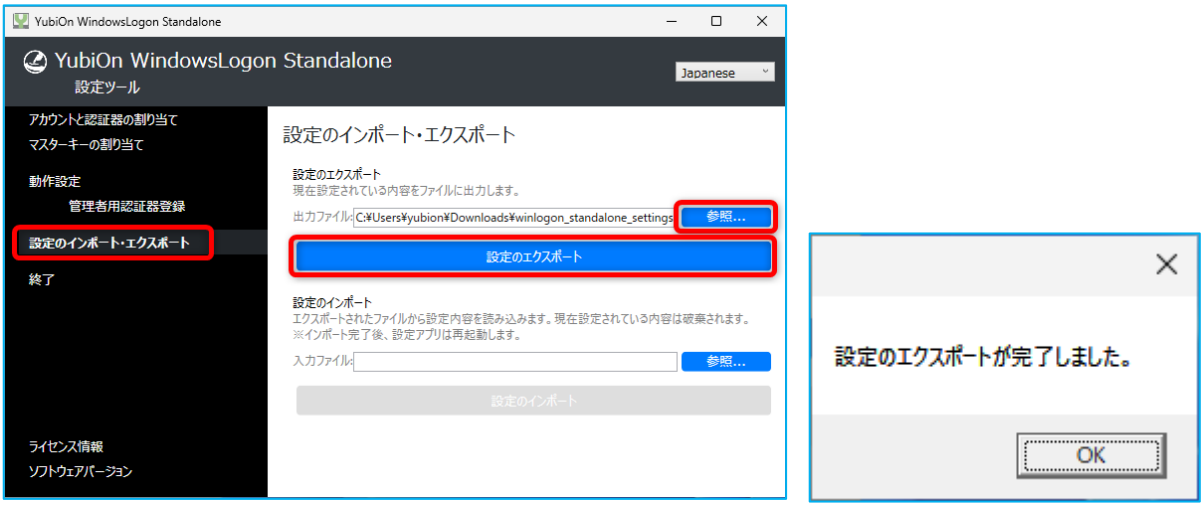
１０．　設定のインポート・エクスポート

設定のインポート・エクスポート画面で、割り当て情報や設定情報のエクスポートとインポートができます。同一の設定を他の PC に引き継ぎたい時などに使用します。

1. 設定のエクスポート

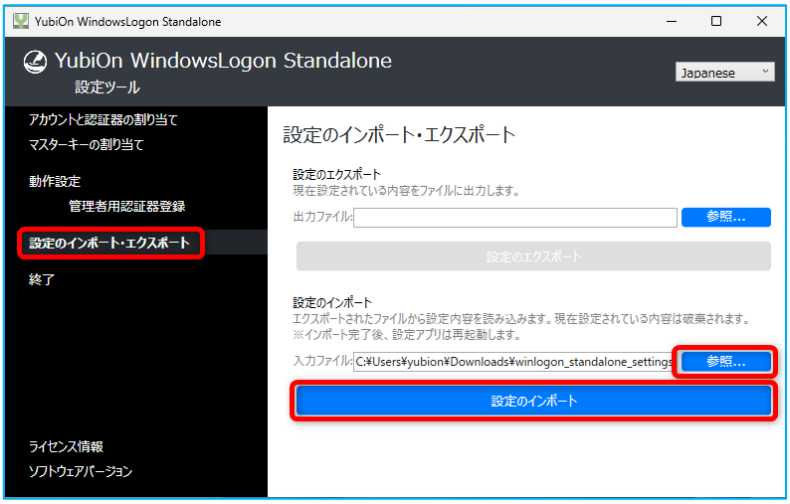
現在の「アカウントと認証器の割り当て」、「マスターキーの割り当て」、「動作設定」、「管理者用認証器登録」の各設定状態をファイルにエクスポートすることができます。

「参照」ボタンでファイルの保存先を指定し、「設定のエクスポート」ボタンでファイルをエクスポートします。



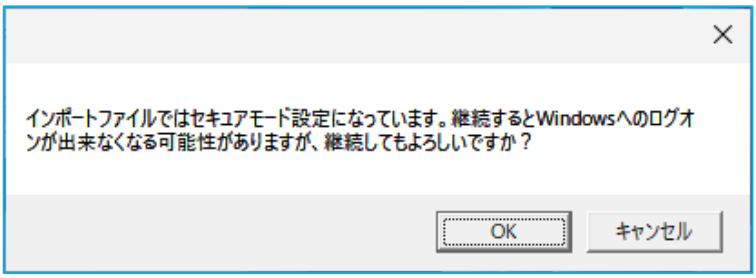
2. 設定のインポート

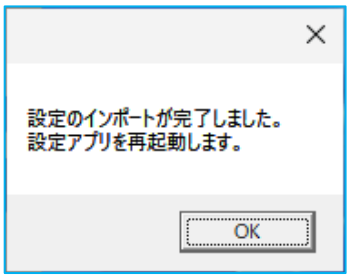
「参照」ボタンをクリックし、エクスポートした設定ファイル指定して「設定のインポート」ボタンをクリックします。「アカウントと認証器の割り当て」、「マスターキーの割り当て」、「動作設定」、「管理者用認証器登録」の各設定状態がエクスポート時の設定になります。現在の設定が上書きされますのでご注意ください。



エクスポート時の設定がセキュアモードになっていた場合は確認メッセージが表示されます。インポートした設定の割り当て状態によっては、PC のログオンが出来なくなる可能性がありますのでご注意ください。

インポート後、設定アプリが再起動します。インポート後の設定状態をご確認ください。





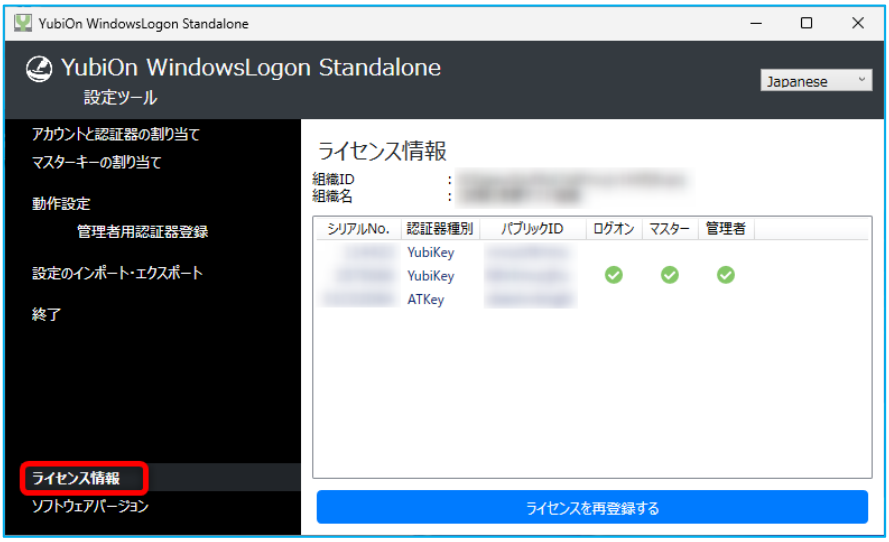
１１．　ライセンス情報

ライセンス情報画面で、利用可能な認証器の一覧が確認できます。

1. ライセンス情報

「ライセンス情報」をクリックすると、現在のライセンス情報が表示されます。

「組織 ID」はライセンスの固有 ID を表し、「組織名」登録の組織名を表します。一覧は利用可能な認証器をそれぞれ確認できます。



一覧の各項目は以下の通りです。

「シリアル No.」　…認証器のシリアルナンバーを表します。

「認証機種別」　…認証器の種別（YubiKey / ATKey）を表します。

「パブリック ID」　…認証器の OTP 先頭 12 文字を表します。

「ログオン」　…アカウントと認証器の割り当てで設定済みの場合にチェックが付きます。

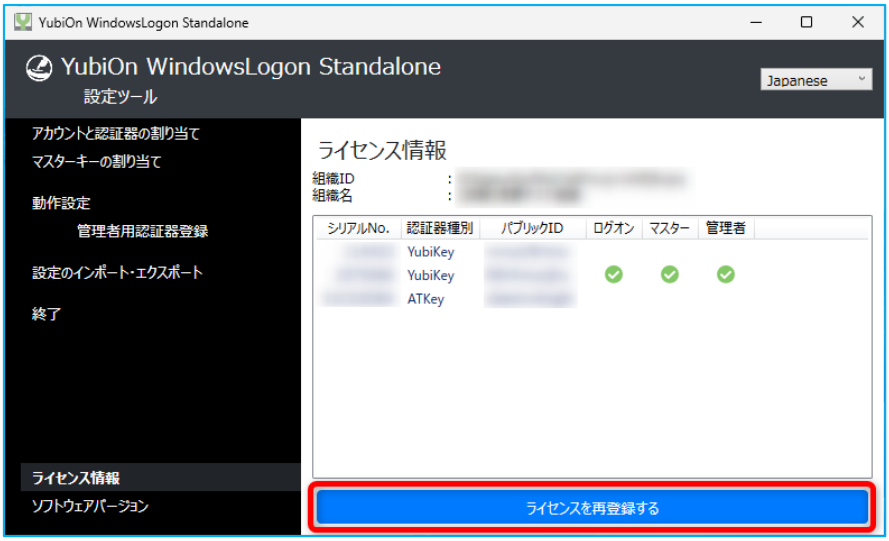
「マスター」　…マスターキーに登録済みの場合にチェックが付きます。

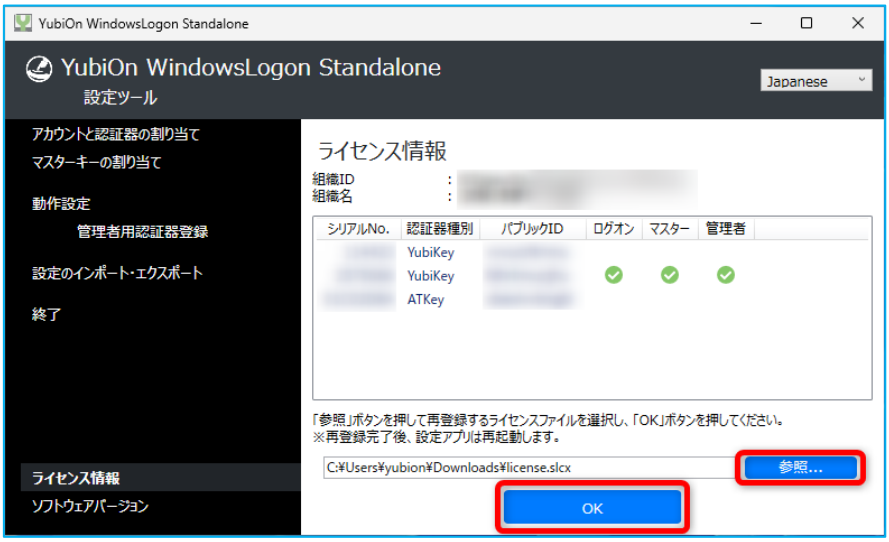
「管理者」　…管理者用認証器に登録済みの場合にチェックが付きます。

2. ライセンス再登録

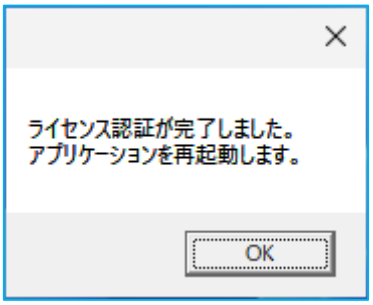
利用できる認証器の追加などで、ライセンスを再購入した時は、新しく入手したライセンスファイルを再登録してください。

「ライセンスを再登録する」ボタンをクリックし、「参照」ボタンをクリックして新しいライセンスファイルを読み込み、「OK」ボタンをクリックします。





ライセンスが正しく読み込まれると設定ツールが再起動します。「OK」をクリックしてください。



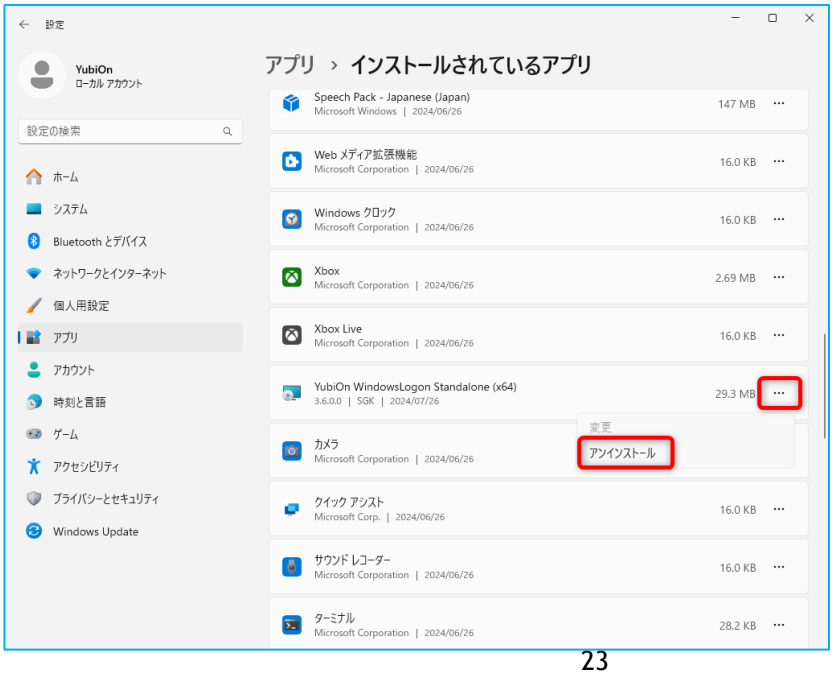
１２．　アンインストール方法

コンピューターから本ソフトウェアを削除します。

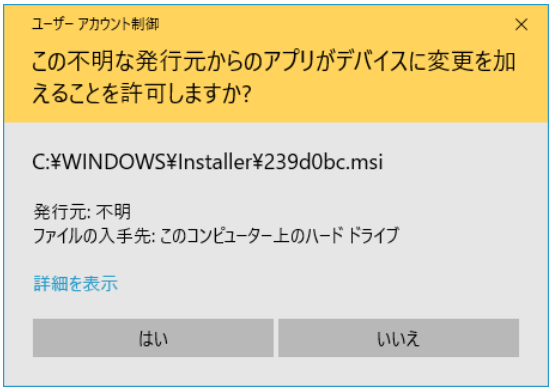
1. Windows の設定を表示し、[アプリ]から[インストールされているアプリ]をクリックします

2. アンインストールを実行します

「YubiOn WindowsLogon Standalone」の「…」をクリックし、「アンインストール」をクリックします。



確認ダイアログが表示された場合は「はい」をクリックし、アンインストールを開始します。



完了のメッセージが表示されるとアンインストールが完了です。

１３．　サポート情報

● 管理者権限の確認方法

1. Windows の設定を開き、[アカウント]を開いてください。
2. [ユーザーの情報]を選択し、クリックしてください。
3. 右側にあるあなたのユーザー名の下に「管理者」という表記があれば、管理者権限を持っています。

● OS 環境の確認方法

1. [スタート]ボタン > [設定] > [システム] > 「バージョン情報」の順に選択します。
2. [デバイスの仕様] > [システムの種類] で、実行中の Windows が 32bit か 64bit かを確認します。

● 動作環境

Windows 10※1 (32bit&64bit)
Windows 11※1

Windows Server 2016
Windows Server 2019
Windows Server 2022

CPU: 800MHz 以上の 32 ビットまたは 64 ビットプロセッサ (1GHz 以上を推奨)
メモリ: 512MB 以上(1GB 以上を推奨)
ハードディスク:100MB 以上のハードディスク空き容量

※1 Windows 10、11 の詳細バージョンのサポートはマイクロソフトのサポートライフサイクルに準じます。

● 必須ミドルウェア

.NET Framework 4.5.2 以上

● お問い合わせ先

販売代理店、または YubiOn サポートチームへお問い合わせください。
YubiOn サポートチーム　：　support@yubion.com

● 製造元

株式会社 ソフト技研　：　http://www.sgk.co.jp/

付録

●ログ出力について

イベントビューアーの Application ログに、当アプリケーションのログオンに関するログが出力されます。

●ログ出力の詳細

■イベントソース

イベントソース名	YubiOnWindowsLogonStandalone

■出力されるイベントの種類

イベント内容	レベル	イベントデータ内容
ログオンを行った	情報	Logged on. User:(ユーザー名)
ログオフを行った	情報	Logged off.
端末ロックを行った	情報	Screen is locked. User:(ユーザー名)
端末ロックを解除した	情報	Screen is unlocked. User:(ユーザー名)
認証に成功した	情報	Authentication by YubiOnWindowsLogon succeed. (認証パラメーター一覧) ※詳細は別表「認証パラメータ」参照
認証に失敗した	警告	Authentication by YubiOnWindowsLogon failed. (認証パラメーター一覧) ※詳細は別表「認証パラメータ」参照

■認証パラメータ

パラメータ名	型	説明
User	string	対象のユーザー名です。※Windows のログオンプログラムが認識するユーザー名のため、ユーザー表示名とは異なる場合があります。
PublicId	string	使用された OTP の Public ID(OTP 先頭 12 文字)です。 利用可能な OTP だと認識できなかった場合 null となります。
Key Type	string	認証器の種別です。 「YubiKey」か「ATKey」となります。 ※ver.3.6.0 以降
SerialNo	long	認証器の個体識別番号です。 ※認証器本体に刻印されています。
IsMasterKey	bool	使用された OTP がマスターキーだった場合 true となります。
IsValidOtp	bool	OTP の認証が成功した場合 true となります。
OtpCheckFailedReason	string	OTP 認証が失敗した場合の理由を表示します。成功した場合は null となります。 ※詳細は別表「OTP 認証失敗理由」参照
AuthenticationResultStatus	string	認証結果ステータスを表します。※詳細は別表「認証結果ステータス」参照

■OTP 認証失敗理由

出力メッセージ	(詳細部)	内容
Not assigned OTP.		アカウントに割り当てられていない OTP が使用されました。
The OTP was entered from the keyboard.		OTP がキーボードから入力されました。
Password is too short to check OTP.		入力されたパスワードが OTP より短いため OTP の認証が出来ませんでした。
The OTP is invalid. Detail:(詳細)	BadOtp	不正な OTP です。
	ReplayedOtp	過去に使用済みの OTP を入力されました。
	Unknown	その他、想定外のエラーです。

■認証結果ステータス

ステータス名称	内容
STATUS_SUCCESS	ログオンに成功しました。
STATUS_INVALID_INFO_CLASS	指定した情報クラスは指定したオブジェクトに対して有効な情報クラスではありません。
STATUS_NO_SUCH_USER	指定されたユーザーにはアカウントがありません。
STATUS_WRONG_PASSWORD	パスワードが無効です。
STATUS_PASSWORD_RESTRICTION	パスワードを更新しようとしたときに、一部のパスワード更新規則に違反しました。
STATUS_LOGON_FAILURE	ログオンに失敗しました。
STATUS_ACCOUNT_RESTRICTION	ユーザー名と認証情報は正しいが、一部のユーザー アカウント制限 (時間帯の制限など) によって認証が失敗しました。
STATUS_INVALID_LOGON_HOURS	ユーザー アカウントでログオン時間が制限されているため、現在はログオンできません。
STATUS_INVALID_WORKSTATION	ユーザーは、指定されたワークステーションにログオンすることを許可されていません。
STATUS_PASSWORD_EXPIRED	パスワードの有効期限が切れています。
STATUS_ACCOUNT_DISABLED	アカウントが無効になっています。
STATUS_INSUFFICIENT_RESOURCES	システム リソースが不足するため、API を終了できません。
STATUS_ACCOUNT_EXPIRED	アカウントの有効期限が切れています。
STATUS_PASSWORD_MUST_CHANGE	アカウントは、次回のログオン時にパスワードを変更する必要があります。
STATUS_ACCOUNT_LOCKED_OUT	アカウントはロックアウトされています。
その他数字	上記に当てはまらないエラーです。