

# Blentity - Data Protector with FIDO2

## 取扱説明書

バージョン 1.1 | 発行 2024 年 01 月



### DOCUMENT CHANGE HISTORY

Date	Version	Change Description	Remark
2024.01.10	v1.0	First release	
2024.01.12	v1.1	Update the URLs	

# 目次

ご使用前に

## 1. 製品情報

- 1-1. 製品仕様
- 1-2. ディスク領域と「Blentity Manager」
- 1-3. 対応環境
- 1-4. 各部の名称
- 1-5. ステータスLED一覧表

## 2. 使用方法

- 2-1. ご使用前に・安全上のご注意
- 2-2. 基本認証モード及び動作モード
- 2-3. 管理ツール「Blentity Manager」のインストール
- 2-4. 初期化
  - 2-4-1. PINコード（暗証番号）
  - 2-4-2. パスフレーズ（Passphrase）
  - 2-4-3. 初期化の操作手順
- 2-5. パスワードレス認証
- 2-6. ディスク領域の設定
- 2-7. 暗号秘密データ領域を開き方
- 2-8. 管理ツールの設定機能
  - 2-8-1. PINの変更
  - 2-8-2. 動作モードの設定
  - 2-8-3. 工場出荷時へのリセット
  - 2-8-4. 言語設定
  - 2-8-5. アップデート

## 3. トラブルシューティング

## 4. FAQ

## 5. アフターサービスについて

## ご使用の前に

このたびは「Blentity (SAMURAI Key)」をお買い上げいただき、まことにありがとうございます。本書には重要な注意事項や本製品のお取り扱い方法が記載されています。ご使用になる前に本書（ぜひ最新版のドキュメントを <https://wisecure-tech.jp/products/samurai-key/support/> でご確認ください）及び「[使用許諾条約](#)」をよくお読みください。その上、正しくご使用ください。

- ※ 本書の内容に関しましては、将来予告なしに変更することがあります。最新版のドキュメントを <https://wisecure-tech.jp/products/samurai-key/support/> でご確認ください。
- ※ 本書の内容は万全を期して作成しておりますが、万一ご不明な点や誤ったところがありましたら、弊社サポートセンターまでご連絡いただきますようお願いいたします。
- ※ Blentity、SAMURAI KeyはWiSECURE Technologies Corporationの登録商標です。その他本製品に記載した社名及び製品名は、一般に各社の商標または登録商標です。
- ※ イラストと実際の商品とは異なる場合があります。
- ※ 改良のため、予告なく仕様を変更することがあります。
- ※ 本製品がお客様により不適當に使用されたり、本書の内容に従わずに取り扱われたり、または当社指定のもの以外の第三者により修理・変更されたことなどに起因して損害などにつきましては、責任を負いかねますのでご了承ください。
- ※ 本製品はFIDO標準に基づいて、パスワードレス及び多要素認証の認証器として使います。FIDOの使用状況は各サービスの対応状況によって異なり、変更する可能性もあります。ご了承ください。
- ※ 本製品はセキュリティ上、PINコードとパスフレーズを忘れてしまった場合、保存したデータを閲覧することはできなくなります。データの救出等は弊社にて対応いたしかねますので、大事なデータは複数のバックアップを取る等の対策を行ってください。
- ※ WiSECUREは、本製品の操作が中断されないこと、またはエラーがないことを保証しません。説明書を遵守せず、対応コンピュータ上で本製品を使用することによって生じる一切のリスクは、ユーザーの責任とします。
- ※ 本製品はWiSECUREのネットワークに接続されていないため、WiSECUREは本製品を介して暗号化および保存されたデータを取得または復号化することができません。WiSECUREは、ユーザーによる本製品の使用、およびデータの損失について責任を負いません。

[目次に戻る](#)

# 1. 製品情報

## 1-1. 製品仕様

### 本体の仕様

製品名	Blentity – Data protector with FIDO2 (SAMURAI Key)
準拠した認証	FIDO2 Level 2, VCCI, CE, FCC
インターフェース	USB 3.2 Gen1
USBコネクタ形状	Type C
読み書き速度 (最速)	読み込み140MB/s、書き込み45MB/s
容量	128GB
フォーマット形式	exFAT、NTFS(Windows版のみ対応)
暗号化アルゴリズム	Hardware-based AES XTS 256
ケースの素材	プラスチック
外形寸法	76 x 20.5 x 10 mm
重量	13.6g

### アダプターの仕様

インターフェース	USB 3.2 Gen1
入力形状	Type C
出力形状	Type A
ケースの素材	プラスチック
外形寸法	37.5 x 20.5 x 10 mm
重量	5.6g

※ ストレージ容量の一部はシステム領域等で使用されているため、実際に使用できる容量は表記の容量より小さくなります。

※ 最大伝送速度は当社環境による実測値であり、全ての環境において保証するものではありません。

※ すべての対応環境での動作を保証するものではありません。改良のため、仕様、外観は予告なく変更する場合があります。

[目次に戻る](#)

## 1-2. ディスク領域と「Blentity Manager」

この製品は128GBの総ストレージ容量を持ち、三つの主要部分に分かれています：「システム領域」、「暗号秘密データ領域」および「通常データ領域」。

### システム領域 (System Partition)

デフォルトで設定され、読み込み操作のみ対応します。

内容ファイル：

- ・ Blentity Manager：フル機能を備えた管理ツールアプリ。インストールが必要です。使用するにあたり最初にインストールしてください。「[2-3. 管理ツールのインストール方法](#)」を参照ください。
- ・ Blentity Manager Lite：ライト版管理ツールアプリ。インストール不要で、共有のコンピュータでも暗号秘密データ領域に迅速にアクセス可能。
- ・ 取扱説明書 (PDF)：製品の仕様と操作手順の詳細を記載したガイド。

### 暗号秘密データ領域 (Secure Partition) と通常データ領域 (Plaintext Partition)

初期化後、Blentity Managerで自由に容量とフォーマットを設定可能です。設定方法は、「[2-6. ディスク領域の基本設定](#)」をご参照ください。

- ・ 暗号秘密データ領域：ハードウェアベースの暗号化 (AES256 XTS) で高度なデータ保護メカニズムを提供し、機密データの保存に適しています。必ず管理ツールでPINコードの検証に成功してから開きます。
- ・ 通常データ領域：一般データの保存や迅速なアクセスに適しています。必ず動作モードの簡易モードを基に開きます。



#### 重要な注意事項

- ・ データ領域の容量配置やフォーマットを行うと、**データが完全に消去されて、復元不可能**です。行う前に、重要なデータは必ずバックアップしてください。
- ・ システム領域への書き込みは不可能です。内容を変更しようとししないでください。
- ・ 二つの管理ツールを同時に開こうとししないでください。

[目次に戻る](#)

## 1-3. 対応環境

### ディスク領域と管理ツールの対応環境

#### 対応機種

本製品は、以下のシステム要件を満たすWindowsおよびMacでの使用が推奨されます：

- ・ USB3.0インターフェースの搭載された機種
- ・ メモリ容量は8GB以上の機種

#### 対応OS

Windows	Windows 10 (ver 21H2) 以上のバージョン
macOS	Ventura以上のバージョン

#### ！ ご注意ください

- ・ USB3.0インターフェイスカードやハブを経由して使用する動作は保証されません。
- ・ 各ホストコントローラのドライバーは、常に最新バージョンを使用してください。
- ・ すべての環境や機器の組み合わせでの動作を保証するものではありません。
- ・ Windows RT、Starter Edition、Embedded、Mobileサポート外となります。

### FIDO2認証の動作環境

本製品が提供する認証サービスの動作環境は、以下のFIDO2に対応ブラウザご参考ください：Microsoft Edge、Mozilla Firefox、Google Chrome、Apple Safari。最新の対応状況は、[FIDOアライアンス](#)の公式ウェブサイトでご確認ください。

推奨される環境は以下の通りです：

Windows	ChromeおよびEdge
Linux	Firefox
macOS	Safari

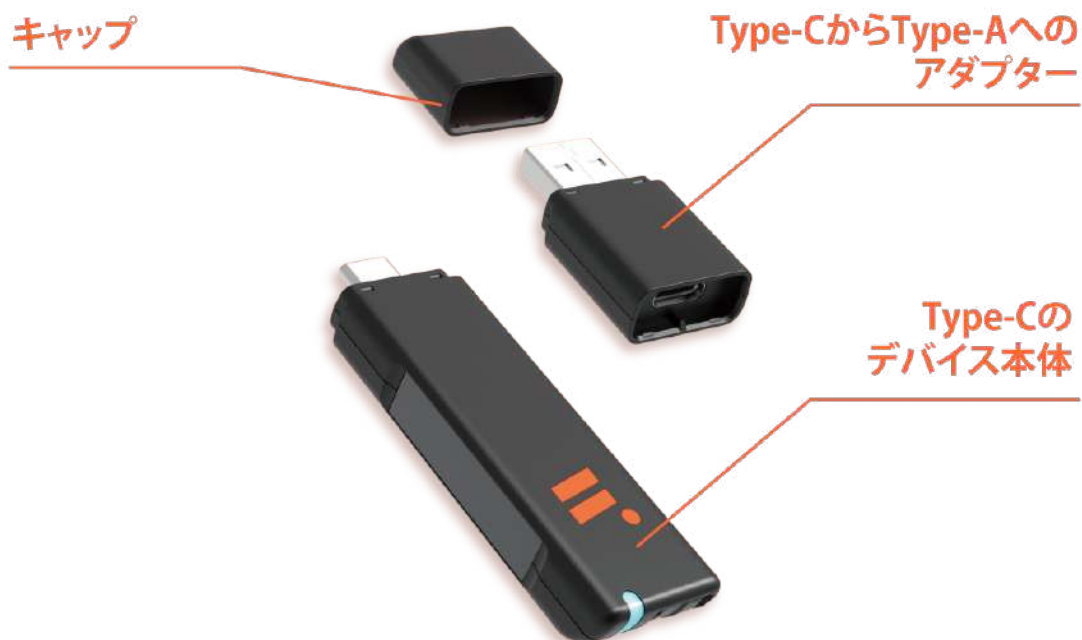
#### ！ ご注意ください

- ・ 本製品は、FIDO認証機能を使用する前に必ず[初期化](#)を行ってください。
- ・ MacでFIDO機能を使用する際には、管理ツールを閉じてください。これにより、機能が正常に動作します。

[目次に戻る](#)

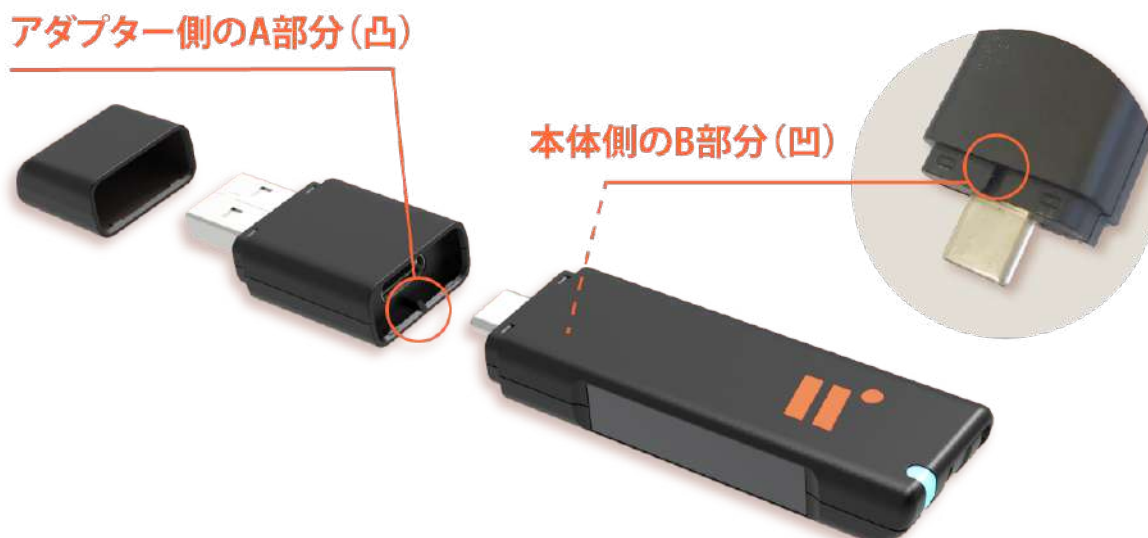
## 1-4. 各部の名称

### 製品構成



USB3.0の高速データ転送速度を確保するための設計が施されていますので、アダプターと本体の接続部分には特定の方角性があります。

正しく向きにして、アダプターのA部分（凸）と本体のB部分（凹）に合わせてはめ込んでください。逆にすると組み立てることができません。





## デバイス本体



### ① タッチエリア

本体の両側にある金属エリアはタッチセンサーを備えています。認証時には、このエリアに指を軽くタッチすることで、操作が実際の間人によって行われていることを確認できます。生体登録は不要で、指紋認証とは異なります。

### ② ステータスLED

暗号秘密データ領域のロック解除など、本体のさまざまな動作状況を、点灯や点滅のパターンで表示します。詳細は「[1-5. ステータスLED一覧表](#)」を参照してください。

### ③ スイッチ

スイッチをオンにすると、オレンジ色が表示され、デバイスは「動作モード」に入ります。動作モードでは、[設定に基づいて](#) デバイスを操作し、ディスク領域を開けることができます。オフの場合は「基本認証モード」になります。詳細は「[2-2. 基本認証モード及び動作モード](#)」をご参照ください。

### ④ ストラップホール

製品を落とさないように、ストラップホールを利用してストラップを取り付けることができます。

[目次に戻る](#)

## 1-5. ステータスLED一覧表

ステータスの優先度の高い順から低い順へ

LEDの状態	本体の動作状態
白色点灯	PC接続中の作動準備状態
赤色点灯	初期化未完成、PINのロック、デバイスのエラー状態
赤色点滅	タッチエリアを長押ししてディスク領域の操作を行う状態、タッチなどの操作待ち状態
緑色点灯	暗号秘密データ領域のロック解除されている状態
緑色点滅	暗号秘密データ領域にあるデータをアクセス中
青色点滅	通常待機状態（何のディスク領域も開いてない状態）
紫色点滅	通常待機状態（暗号秘密データ領域を除く他のディスク領域が開いている状態）

### 赤色点灯している状態の対処方法：

- ※ デバイスがまだ初期化されていない場合は、[2.4 初期化](#)の手順に従って初期化してください。
- ※ PINがロックされた場合、Blentity Managerを開き、ホーム上部の指示に従ってパスフレーズを入力し、PINをリセットしてください。
- ※ 上記の原因を排除しても赤色点灯している場合は、デバイスに異常がある可能性があります。[トラブルシューティング](#)を試すか、サポートセンターにお問い合わせください。

[目次に戻る](#)

## 2. 使用方法

### 2-1. ご使用の前に・安全上のご注意

ご使用の前に、安全上のご注意をよくお読みのうえ、正しくご使用ください。

記載しております注意事項、警告表示には、使用者や第三者への危害や財産への損害を未然に防ぐ内容を含んでおりますので、必ずご理解のうえ、守っていただくようお願いいたします。

警告と注意の表示区分では、表示内容を守らなかった場合に生じる危害、または損害程度を表します。

#### 警告

この表示で記載された文章を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性を想定した内容を示します。

#### **煙が出る、異臭がする、異音がする場合は使用しないでください**

煙が出る、異臭がする、異音がするとき、すぐにデバイスをコンピューターから抜いてください。異常状態のまま使用すると、故障、火災、感電の原因となり、差し込まれたコンピューター本体に障害を与える可能性もあります。

#### **分解・改造をしないでください**

デバイスの分解・改造をしないでください。故障、火災、感電の原因となり、差し込まれたコンピューター本体に障害を与える可能性もあります。

点検、調整、修理は、弊社サポートセンターまでご連絡ください。

#### **内部に水を入れるような環境での使用を避けてください**

デバイスの内部に水が入った場合は、すぐにコンピューターから抜いてください。

水が入ったまま使用すると、故障、火災、感電の原因となり、差し込まれたコンピューター本体に障害を与える可能性もあります。

#### **特殊なUSBポートでの使用しないでください**

モバイル電源や急速充電対応のUSBポートでの利用をしないでたします。これにより故障の可能性があり、挿入されたデバイスに損害を与えることがあります。

#### **本製品は精密部品です。以下の注意点を守ってご使用ください。**

- ・ 落としたり、衝撃を加えない
- ・ 本製品の近くで飲食・喫煙などをしない
- ・ 接続コードを無理に曲げる、ねじる、束ねる、はさむなどの行為をしないでください。

- ・ 接続コードの上に重い物を置かないでください。
- ・ ステープル、釘などで固定しないでください。
- ・ 無理に合わないコンセントやポートには接続しないでください。
- ・ 足を引っかけるおそれのある場所には設置しないでください。

### **ぬれた手で接続コードに触れないください**

ぬれたままの手で接続コードに触れないでください。感電や故障の原因になります。

### **体に異変が出たら使用しないでください**

体に異変が出た場合は、ただちに使用をやめて、医師にご相談ください。

本製品に使用されているプラスチックなどによって、かゆみやアレルギーなどの症状が引き起こされることがあります。

### **小さいお子様やペットを近づけない**

小さいお子様やペットをデバイスに近づけないようにしてください。

小さな部品の誤飲か誤嚥など、けがの原因になることがあります。

## **⚠ 注意**

この表示で記載された文章を無視して誤った取り扱いをすると、人が傷害ないし物的損害を負う可能性を想定した内容を示します。

### **設置場所に関する注意事項**

本製品を以下のような場所で保管・使用しないでください。

- ・ 振動や衝撃の加わる場所
- ・ 直射日光の当たる場所
- ・ 湿気やほこりが多い場所
- ・ 温度差の激しい場所
- ・ 熱の発生する物の近く(ストーブ、ヒーターなど)
- ・ 強い磁力電波の発生する物の近く(磁石、ディスプレイ、スピーカー、ラジオ無線機等)
- ・ 水気が多い場所(台所、浴室等)
- ・ 腐食性ガスを含んだ大気中(Cl<sub>2</sub>、H<sub>2</sub>S、NH<sub>3</sub>、SO<sub>2</sub>、NO<sub>x</sub> 等)
- ・ 静電気の影響の強い場所

### **長期間使用しない場合**

長期間使用しない場合は、コンピューターなどを外して、USBキャップを閉めて保管してください。

### **挿入している機器を移動するとき**

挿入しているコンピューターを移動する際は、必ずデバイスを外してください。接続したままの移動は故障の原因となります。

### **静電気にご注意ください**

デバイスに触れる際は、静電気にご注意ください。

本製品は精密電子機器ですので、静電気を与えると誤動作や故障の原因となります。

[目次に戻る](#)

## 2-2. 基本認証モード及び動作モード

本製品は、スイッチの状態によって二つのモードに切り替わります：

### 動作モード (Operation mode)

- ・ スイッチがオンの状態（オレンジ色が表示されている状態）です。
- ・ [動作モードの設定](#)に従い、デバイス进行操作することでディスク領域を開くことができます。

### 基本認証モード (FIDO-only mode)

- ・ スイッチがオフの状態です。
- ・ このモードでは、デバイスに操作しても（パソコンに挿入、タッチエリアを長押しするなど）ディスク領域を開くことはできません。ディスク領域が勝手に飛び出し、ログインを妨げることを防ぎます。

挿入している状態でスイッチしてから、デバイスを再挿入した後に有効になります。



どちらのモードでも、[暗号秘密データ領域を開く](#)ためには、管理ツールを通じて行う必要があります。



[目次に戻る](#)

## 2-3. 管理ツール「Blentity Manager」のインストール

本製品を初期化するため、システム領域の中にある管理ツールアプリ「Blentity Manager」をインストールしてください。

はじめて本製品を使用する際の手順は以下の通りです。

1. スイッチがオンになっていることを確認してください。オンの状態はオレンジ色が表示されます。
2. コンピューターにデバイスを接続し、本体の両側にあるタッチエリアを約3秒間長押しして、システム設定画面へアクセスします。
3. お使いのOSに応じて、表示されるディスク領域内から管理ツールをインストールしてください。ツールを開くと、初期化プロセスが自動的に開始され、画面の指示に従って進めてください。

### インストールファイルの場所

お使いのOSはWindowsの場合：

BLENTITY（システム領域）> Windows > Manager Installer.exe

お使いのOSはmacOSの場合：

BLENTITY（システム領域）> Mac > Manager Installer.pkg

[目次に戻る](#)

## 2-4. 初期化

初期化する前に、まず[管理ツールアプリをインストール](#)してください。  
初期化時には、PINコードとパスフレーズの設定が自動的にガイドされます。

### 2-4-1. PINコード（暗証番号）

PINコードは、デバイスの不正利用を防ぐための重要な仕組みです。デバイスが紛失または盗難に遭っても、PINコードがないと不正利用されません。

#### PINの構成

8文字から63文字の長さで設定でき、大文字・小文字の英数字と記号を含むことが可能です。

#### PINの使用

FIDO認証の実行、暗号秘密データ領域のロック解除、および管理ツールの特定機能の使用に際しては、PINコードの入力が必要となります。

#### PINの変更

「Blentity Manager」の「設定 > PINの変更」から行うことができます。

#### PINのロックとロック解除

PINの入力を8回間違えると、または、Blentity Manager以外のツールでFIDO PINコードを変更した場合、PINの非同期による本製品は自動的にロックされます。ロックされた場合、設定した「[パスフレーズ](#)」を使用してロック解除する必要があります。



## 2-4-2. パスフレーズ (Passphrase)

パスフレーズは、業界標準規格「BIP39」に基づく暗号資産のウォレットで広く使用されている仕組みです。初期化時には、12語の英単語からなるパスフレーズがランダムに生成されます。

### どんな状況でパスフレーズを使用しますか？

#### - PINロックの解除

PINの入力ミスが上限を超えて、また、Blentity Manager以外の方法でPINを変更してPIN非同期になってロックされた場合、パスフレーズを入力してロックを解除し、PINをリセットすることができます。

#### - バックアップファイルの復元 (将来提供予定)

もしデバイスを紛失してしまった場合でも、パスフレーズを利用して、新しいデバイス上でマスターキー（ファイルを暗号化するための基礎鍵）を再生成することが可能です。この機能により、バックアップファイルを他のデバイスへ簡単に復元することができるようになります。



#### 重要な注意事項

1. パスフレーズを正確に記憶するか、安全な場所に保存してください。製品パッケージには記録用のカードが含まれています。
2. パスフレーズを8回間違えて入力すると、デバイスは**工場出荷時の状態にリセット**されて、**すべてのデータを消去し、取り消すことができません。**
3. パスフレーズを忘れた場合は、ぜひデータをバックアップした後、デバイスを工場出荷時にリセットし、新しいパスフレーズを作成して保存してください。

### 2-4-3. 初期化の操作手順

初期化する前に、まず[管理ツールアプリをインストール](#)してください。

初期化時には、PINコードとパスフレーズの設定が自動的にガイドされます。以下の流れをご参考ください。

1. まずは、PINコードを設定してください。



2. PINコードを初期設定した後、以下のページに進みます。

新しいパスフレーズを生成するか、既存のパスフレーズでこのデバイスへマスタキーを復元するかを選択してください。



3. 「新しいパスワードを設定する」を選択して、12語のパスフレーズを自動的に生成します。コピーして安全な場所に保存するか、または手書きで記録して保管してください。

次のページでは、このパスフレーズを正確な順序で入力し、再確認を行う必要があります。パスフレーズのコピーとペーストも可能です。



4. 貼り付けた後、「次へ」をクリックすると、鍵の生成が開始されます。キー生成が完了次第、初期化のプロセスも完了します。



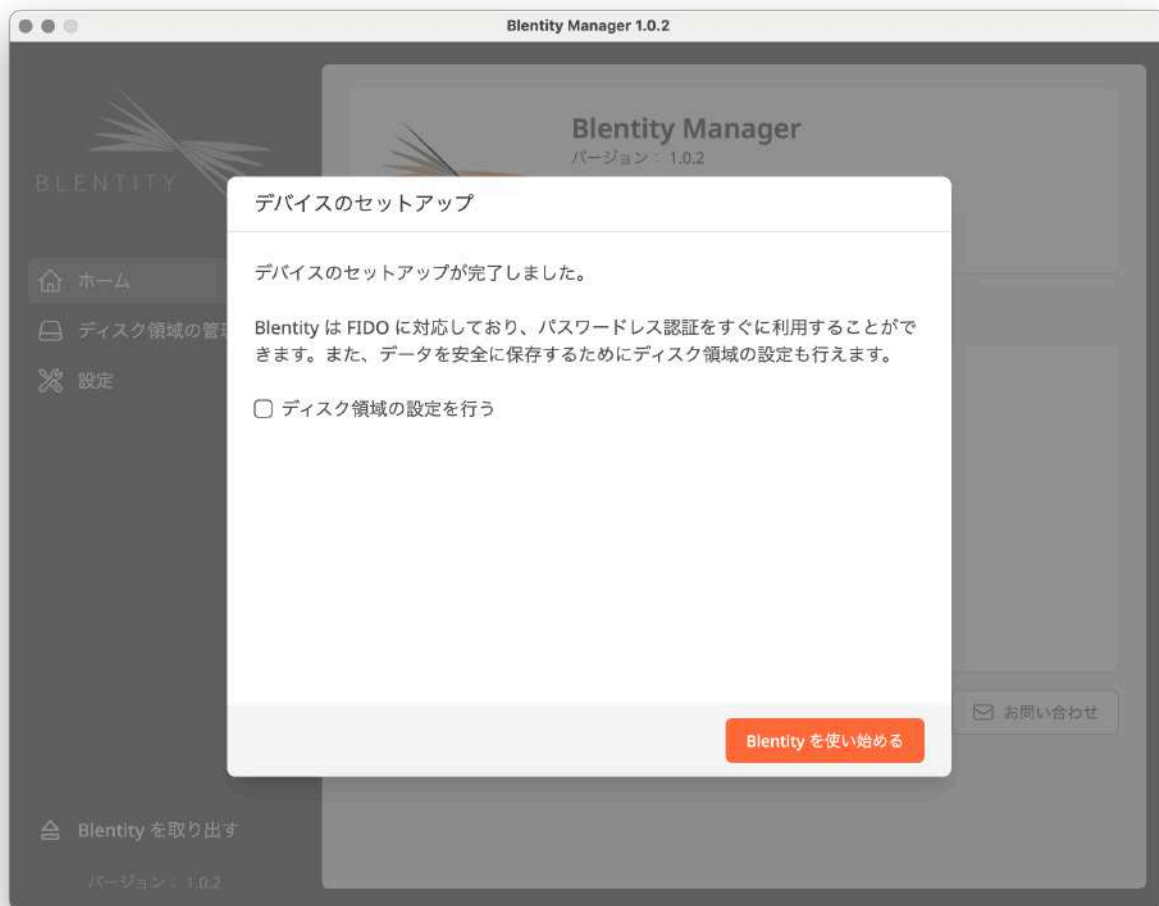
初期設定を完了した後、次の機能を使用することができます：

### FIDO認証機能の使用開始

初期設定完了後、本製品のFIDO認証機能を使用して、サポートされるサービスでのセキュリティ強化されたログインが可能になります。「[2-5. パスワードレス認証](#)」をご参照ください。

### データ領域の設定と使用開始

初期設定完了後、直ちに[ディスク領域の設定](#)に進むことができます。ここで、暗号秘密データ領域と通常データ領域の容量とフォーマットの設定を行ってから、データストレージの利用が可能になります。



### ご注意ください

ディスク領域の設定が行われていない場合、そのディスク領域は未フォーマット状態となります。そのため、正しい操作でロック解除してもディスクスロットで暗号化ディスク領域を表示することはできません。「ディスク領域の管理 > ディスク領域の設定」にて、容量の配置とフォーマットを行ってください。

[目次に戻る](#)

## 2-5. パスワードレス認証

本製品が提供する認証サービスの動作環境は、以下のFIDO2に対応ブラウザご参考ください：Microsoft Edge、Mozilla Firefox、Google Chrome、Apple Safari。最新の対応状況は、[FIDOアライアンスの公式ウェブサイト](#)でご確認ください。

BlentityのFIDO認証機能に推奨される環境は以下の通りです：

Windows	ChromeおよびEdge
Linux	Firefox
macOS	Safari

### ！ ご注意ください

- ・ 本製品は、FIDO認証機能を使用する前に必ず[初期化](#)を行ってください。
- ・ MacでFIDO機能を使用する際には、管理ツールを閉じてください。これにより、機能が正常に動作します。

Blentityをアカウントに登録・追加した後は、アカウントの安全性を強化になります。登録・追加方法はFIDO2に対応する各サービスの操作説明をご参照ください。

### 例：Microsoftアカウントのサインイン方法としてBlentityを追加する

1. [Microsoft アカウント ページ](#) に移動して、通常どおりサインインします。
2. [セキュリティ]>[その他のセキュリティ オプション]を選択します。
3. [サインインに使用する新しい方法を追加して確認]を選択します。
4. [セキュリティ キーを使用する]を選択します。
5. USBを選択して、[次へ]を選択します。
6. セットアップ エクスペリエンスのページが開いたら、Blentityを挿入またはタップします。
7. 既に作成済みのPINを入力します。（まだ作成してない場合は、ぜひBlentity Managerで[初期化](#)してください。）
8. 次に必要な操作を行います。Blentityの両側のタッチエリアにタッチします。
9. 他のキーと区別できるような名前を付けます。
10. サインアウトしてMicrosoft Edgeを開き、[Windows Helloまたはセキュリティ キーを使用する]を選択して、Blentityを挿入またはタップしてサインインします。

キーの管理、削除するには、[Microsoft公式サイト](#)の操作説明をご参考ください。

[目次に戻る](#)

## 2-6. ディスク領域の設定

本製品のストレージ機能を使用する前に、「ディスク管理 > ディスク領域の設定」を通じてディスク領域を割り当てまたはフォーマットする必要があります。暗号秘密データ領域と通常データ領域の作成が可能です。

**!** ご注意ください  
この操作には、コンピュータの管理者権限が必要です。

**!** 重要な注意事項  
この操作はディスク領域内の**すべてのデータを消去し、取り消すことができません**。  
操作を実行する前に必ずデータのバックアップを行ってください。

### 操作手順

1. 「ディスク領域の管理 > ディスク領域の基本設定」に進んでください。
2. 暗号秘密データ領域と通常データ領域の容量を設定してください。
3. ディスク領域の名前を設定してください。ここではアルファベットの大文字のみ設定可能ですが、後でコンピュータのファイルマネージャーを使用して名前を変更することができます。
4. ファイルシステムの形式を選択してください。
5. ディスクを読み取れないという警告が表示された場合は、[無視]を選択してください。
6. システムの指示に従い、コンピュータの管理員としてログインしてください。
7. ディスク領域の設定を完了します。**デバイスを取り出して、再挿入してください。**

### ディスク領域の利用方法

「[2-7. 暗号秘密データ領域の開き方](#)」と「[2-8-2. 動作モードの設定](#)」をご参照ください。

[目次に戻る](#)

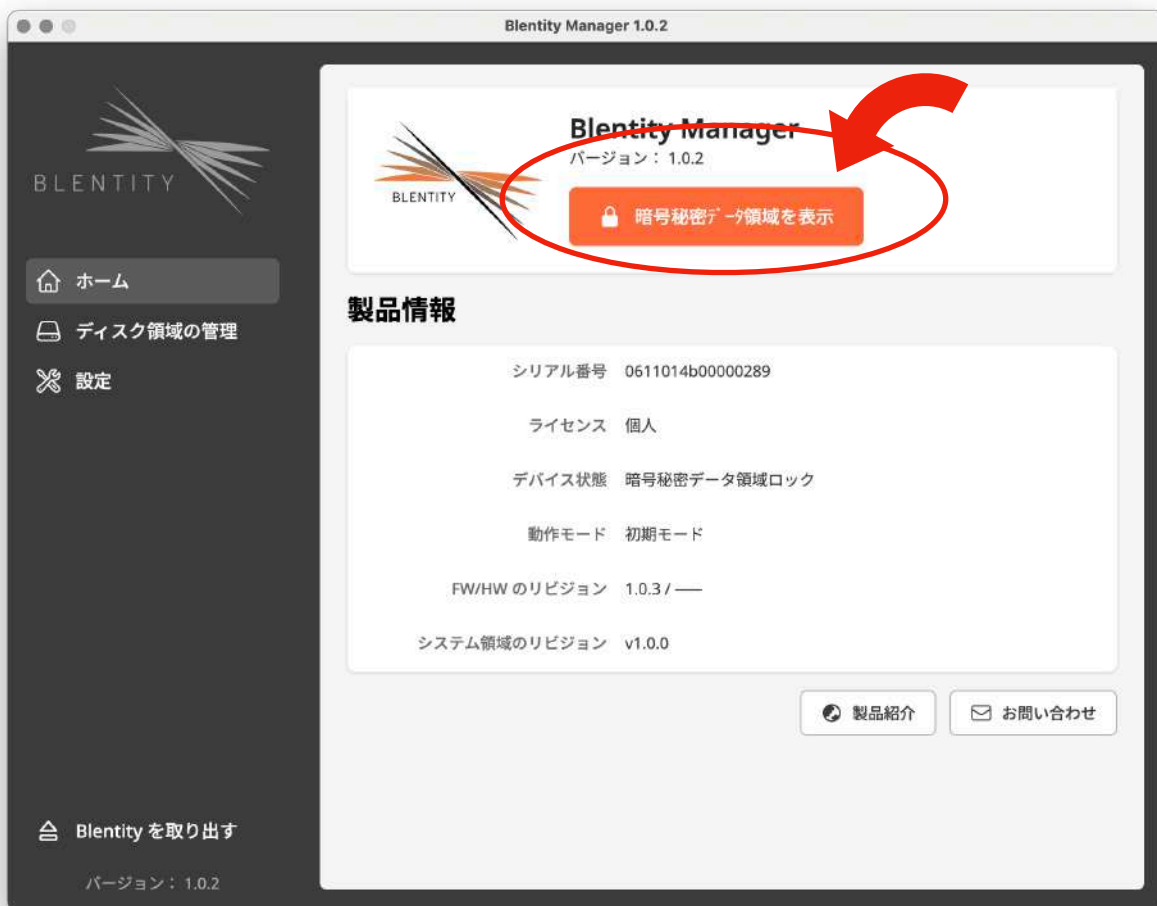


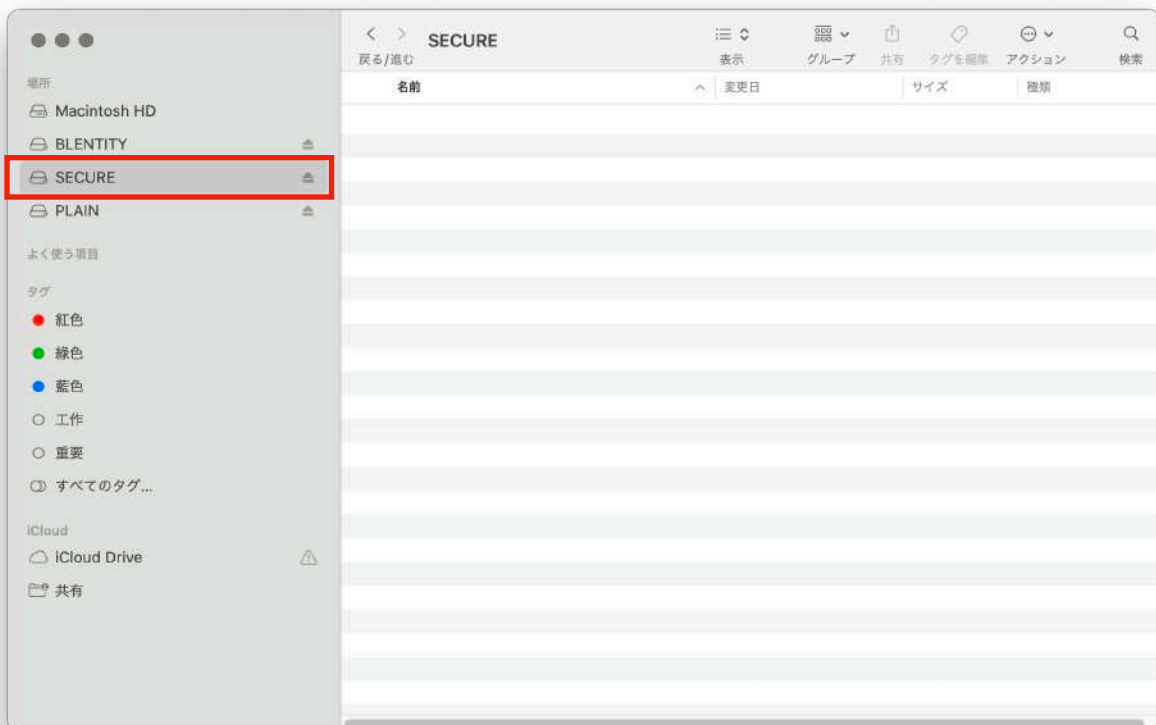
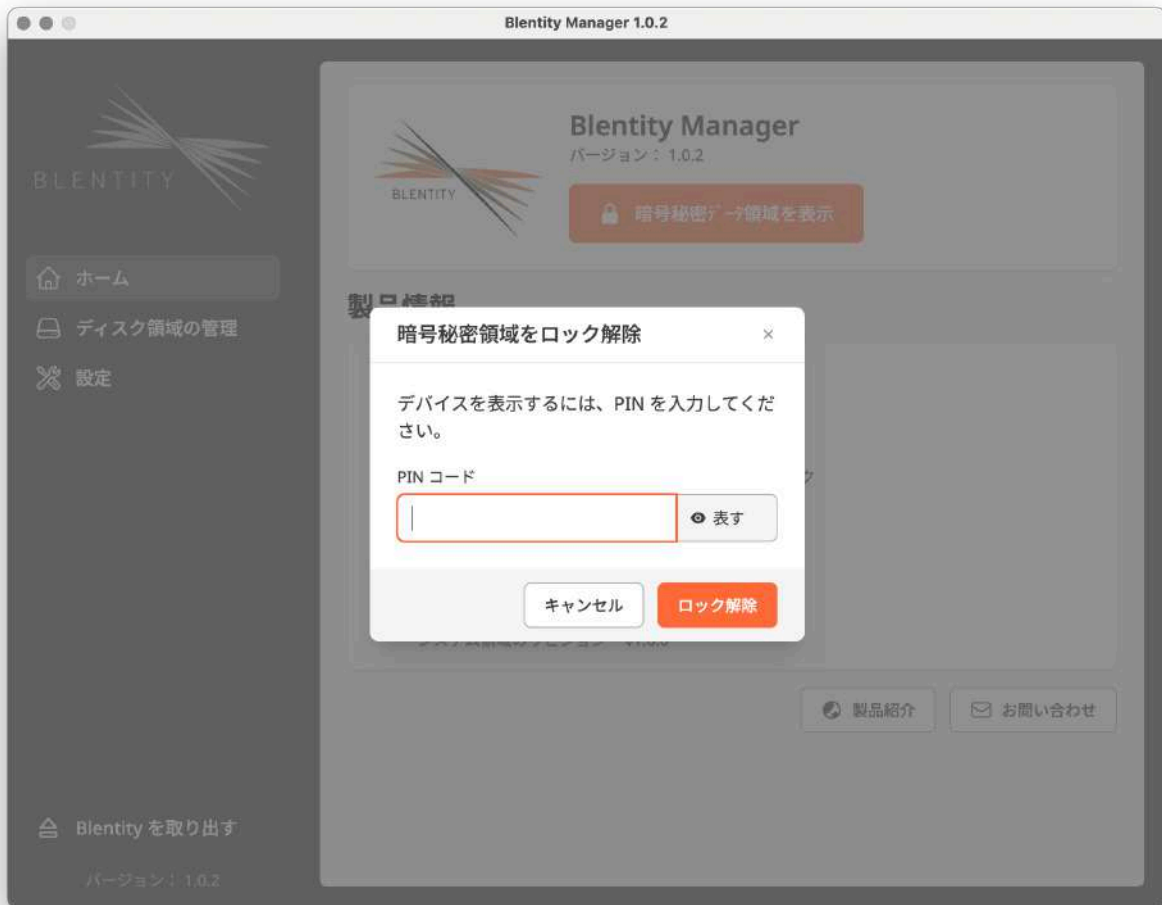
## 2-7. 暗号秘密データ領域の開き方

暗号秘密データ領域にアクセスするには、以下の方法があります：

### Blentity Managerを使用する方法

管理ツールアプリのホームで「暗号秘密データ領域を表示」ボタンをクリックしてPINを入力すると、暗号秘密データ領域が開きます。

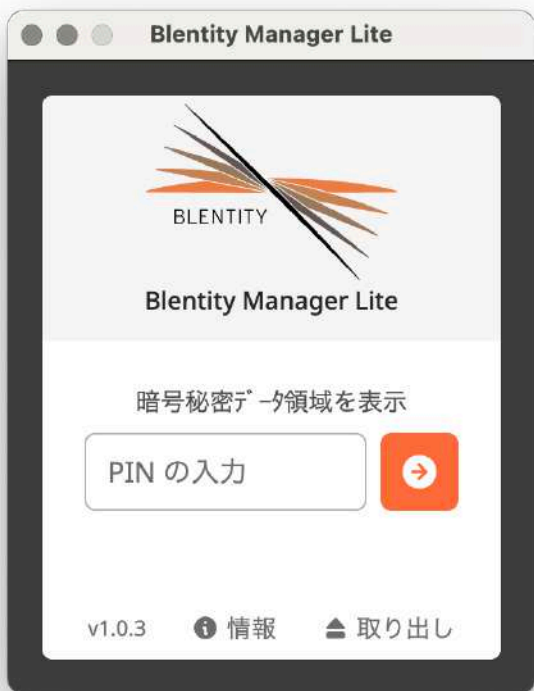




## Blenity Manager Liteを使用する

動作モードでシステム領域を開いて、Blenity Manager LiteにPINコードを入力すると、暗号秘密データ領域が開きます。

使用済みの際には、ツールの「終了と取り出し」をクリックすると、暗号秘密データ領域をロックされて、デバイスを安全に取り出して、アプリのウィンドウズも消します。



[目次に戻る](#)

## 2-8. 管理ツールのその他の機能

### 2-8-1. PINの変更方法

「設定 > PINの変更」からPINを変更できます。



ご注意ください

Blentity Manager以外のツールでFIDO PINを変更すると、PINをロックされます。この場合には、Blentity Managerでパスフレーズを使用して、PINをリセットしてください。

### 2-8-2. 動作モードの設定

本製品のスイッチをオンにすると（オレンジ色が表示される状態）、製品は「動作モード（Operation mode）」になり、システム領域や通常データ領域のアクセスが可能になります。「設定 > 動作モードの設定」から行ってください。モードの変更に成功した後、デバイスを再挿入した後に有効になります。

#### 利用可能な動作モード：

##### 初期モード

デバイスが接続された際には、自動的にはどのディスク領域も開きません。

デバイスの両側にあるタッチエリアを約3秒間長押しすることで、「システム領域」と「通常データ領域」が開きます。

また3秒ぐらい長押しすると、すべてのディスク領域を閉めます。

##### システム領域モード

デバイスを接続すると、「システム領域」のみが自動的に開きます。

##### 簡易モード

デバイスを接続すると、「システム領域」と「通常データ領域」が自動的に開きます。

	システム領域 (RO)	通常データ領域 (RW)	暗号秘密データ領域 (RW)
初期モード	デフォルトで閉じる 長押しすると開く*	デフォルトで閉じる 長押しすると開く*	デフォルト閉じる アプリで認証すると開く
システム領域モード	挿入すると開く*	閉じる	
簡易モード	挿入すると開く*	挿入すると開く*	

ディスク領域の動作モード

\*スイッチはオンにする必要があります。 RW : Read / Write RO : Read Only

### 2-8-3. 言語設定

本製品は中国語、英語、日本語のインターフェースを提供しています。「設定」メニューの「言語設定」オプションで言語を変更できます。

### 2-8-4. 工場出荷時へのリセット

「設定」メニューの「工場出荷時設定へのリセット」オプションで、製品を未初期化の状態に戻すことができます。



#### 重要な注意事項

この操作は**PIN、助記語、証明書、認証情報、データをすべて消去し、復元不可能です。**事前にデータのバックアップをとってください。

### 2-8-5. アップデート

管理ツールを通してソフトウェアおよびファームウェアの更新が可能です。これにより、最適な品質と体験が提供されます。

#### 更新前の準備

- ・ インターネット接続が安定していることを確認してください。
- ・ データをバックアップしてください。



#### 重要な注意事項

更新操作はディスク領域内の**データを消去する可能性があります、復元は不可能です。**事前に必ずデータのバックアップを行ってください。

#### 操作手順

1. 規格に合ったコンピュータにデバイスを接続します。
2. フル機能を備えたBlentity Managerを開き、約10分間待って更新ファイルを取得します。デバイスを抜くと取得が中断されます。
3. 取得後、管理ツールのホーム下部または「設定 > 更新」で表示される「更新」ボタンをクリックして更新を完了します。

[目次に戻る](#)

## 3. トラブルシューティング

万一「故障かな？」と思われる場合は、以下の問題を意識し、対処方法をお試してください。

### デバイスがPCに認識されない

- ・ USBハブを介さずに、直接PCのUSBポートにデバイスを接続してください。
- ・ 接続後にステータスLEDが点灯しているか確認してください。
- ・ USB3.0ポートの接続が確実であること、及びポートに損傷がないことを確認してください。
- ・ USB3.0インターフェイスカードのドライバが古い場合は、最新バージョンにアップデートしてください。

### スリープ、スタンバイ、休止状態から復帰時にファイルが損害する

- ・ 本製品はスリープ、スタンバイ、休止状態には対応していません。これらの状態にする前に、ファイルを保存し、デバイスを取り外してください。

### PINコードで認証に失敗する問題

- ・ 入力ミスがないか最初に確認してください。
- ・ PINコードを忘れたり、入力間違いの上限を超えるとPINがロックされます。この場合は、初期設定時に生成したパスフレーズを使用してPINコードをリセットしてください。
- ・ Blentity Manager以外のツールでFIDO PINコードを変更した場合、PINの非同期によるロックされます。この場合は、Blentity Managerを開き、ホームの上部にある指示に従って、パスフレーズによるロック解除してPINをリセットしてください。

### 暗号化秘密データ領域がディスクスロットで検出されない

- ・ 初期化が完了しているか、ディスク領域のフォーマットが行われているかをご確認ください。
- ・ 初期化後にフォーマットが行われていない場合、正しい操作でロック解除してもディスクスロットで暗号化ディスク領域を表示することはできません。「ディスク領域の管理 > ディスク領域の設定」にて、容量の配置とフォーマットを行ってください。

### パスフレーズを使用してPINをロック解除する際に画面が停止する

- ・ パスフレーズを入力後、キーを計算する時間は約10秒程度必要ですが、コンピューターによって時間が異なる場合がありますので、しばらくお待ちください。1分以上待っても反応がない場合は、サポートセンターにお問合せください。

[目次に戻る](#)

## 4. FAQ

Q： モバイル、Windows Server、Linuxでの動作はサポートされていますか？

A： これらのOSはサポート対象外です。動作は自己責任でお願いします。サポート対象OSは、「[1-3. 対応環境](#)」を参照してください。

Q： ソフトウェアのインストールは必要ですか？

A： 初期化するにはフル機能版の管理ツールをインストールする必要があります。初期化後、暗号秘密データ領域はLite版ツールで開けます。インストールしていないコンピュータでも使えます。

Q： PINコードを忘れた場合はどうすればいいですか？

A： 初期化時に生成した12語のパスフレーズでロック解除が可能です。パスフレーズも紛失した場合は、データを失うこととなりますので、定期的なバックアップとパスフレーズの安全な保管が重要です。

Q： PINコードの連続入力失敗後のデータはどうなりますか？

A： 8回連続で間違えると自動的にロックされ、パスフレーズで解除する必要があります。解除に成功すればデータは使用可能です。

Q： 設定したPINコードを変更することは可能ですか？

A： はい、「Blentity Manager」の「設定 > PINの変更」から行うことができます。保存したデータに影響を与えません。

Q： 一定時間操作がない場合、自動的にロックはされますか？

A： 自動ロック機能はありません。不在時はデバイスを取り外すか、暗号秘密データ領域を取り外してください。

Q： Azure ADと連携して使用する場合、PCから取り外すとWindowsは自動的にロックされますか？

A： 自動ロックはされません。ログイン時のみ使用して、その後は抜いても大丈夫です。

Q： ディスク領域に設定した容量は実際設定された数字が異なるのはなぜですか？

A： 設定完了の暗号秘密データ領域の容量は、設定画面で見た数値よりも「大きく」表示されます。これは、1GBが1024MBに等しく、余りが出るためです。設定値が1024で割り切れない余りがある場合、その余りは設定時には加算されませんが、最終的には暗号秘密データ領域に割り当てられます。設定完了後の完成画面でその変更が表示されます。

Q : BlentityをGoogleアカウントに二段階認証の手段として追加するには、ブラウザによってPasskeysとして追加されたことが問題ないでしょうか。

A : BlentityはEdgeとChromeに登録する場合、Passkeysに分類されますが、Firefoxに登録する際には FIDO2セキュリティキーになります。ただし、どのブラウザに追加しても、他のブラウザに同じ手順でサインインできます。ユーザーエクスペリエンスには違いがありません。

他のFAQをこちらへご参照ください :

<https://wisecure-tech.jp/products/samurai-key/support/>

[目次に戻る](#)



## 5. アフタサービスについて

お客様の権利を保護するために、領収書の日付を記入し、適切に保存してください。

### 保証範囲

製品には1年間の保証が提供されます。通常使用範囲外の製品保証は受けられません。初期不良が確認された場合、商品がお手元に届いた時点で破損していた場合、新品と交換させていただきます（包装の破損は含みません）。

### 修理について

修理の要望は、「管理ツールの「お問い合わせ」からメールで送信できます。保証期間後の修理は有償です。なお、修理・検査の際に認証情報・データが消去される可能性がありますので、事前のバックアップをしてください。

### お問い合わせ

WiSECURE Technologies Corporation

サポートページ：<https://wisecure-tech.jp/products/samurai-key/support/>

お問い合わせメール：[info@wisecure-tech.jp](mailto:info@wisecure-tech.jp)（デバイス情報を同時に得られるように、管理アプリBlentity Manager内の「お問い合わせ」を優先してご利用ください）

受付時間 10:00–17:00 月一金曜日（祝祭日を除く）

[目次に戻る](#)

# Blentity - Data Protector with FIDO2

## 取扱説明書

バージョン1.1 | 発行 2024年01月