Blentity - Data Protector with FIDO2

取扱説明書

バージョン 1.0 | 発行 2024 年 10 月

DOCUMENT CHANGE HISTORY

Date	Version	Change Description	Remark
2024.10.01	v1.0	First release	

目次

ようこそ

Blentity（日本での通称 SAMURAI Key と言います）のご購入、誠にありがとうございます。Blentityは、高度な個人情報保護を実現するために設計されています。コンピュータ内のデータ、USBメモリ内のオフラインデータ、そして日常的に利用するサービスのアカウントのログイン安全を確保します。

ハードウェアレベルの鍵保護でデータの安全を守る

従来の暗号化ソフトウェアは、鍵を安全でない環境に保存することが多く、万が一鍵が漏洩してしまうと、すべての暗号化データが危険にさらされることになります。Blentityは、CC EAL5+認証の高規格セキュリティチップを採用しており、あなたの暗号鍵を確実に保護します。物理的な侵入やサイドチャネル攻撃に対しても、鍵の盗難を防ぎ、常にデータの安全を確保します。

紛失のリスクを最小限に

物理的な鍵の盗用やデバイスの紛失に対応するため、BlentityはPINコード保護機能を備えています。PINコードを8回連続で誤入力すると、自動的にデバイスがロックされ、ブルートフォース攻撃を防ぎます。また、パスフレーす機能を使うことで、どのBlentityデバイスでも簡単に暗号化データを復元でき、データが失われる心配がありません。

日常のサービスのログイン安全性と利便性を強化

さらに、Blentityは二要素認証とパスワードレスのセキュリティキーとしても利用できます。Google、Microsoft、Facebook、Dropbox、AWSX、GitHubなど、数百のウェブサイトに対応しています（一つのデバイスで最大25サイトまで登録可能）。これにより、ソーシャルエンジニアリングやフィッシング攻撃といったパスワード漏洩のリスクからアカウントを守ります。パスワードレスのプロトコルに対応しているウェブサイトでは、パスワードなしでのログインが可能で、快適な体験を提供します。

本書には製品の使用方法が記載されていますので、使用前に必ずお読みください。また、使用許諾契約および安全に使用するための注意事項を確認し、正しく安全に本製品をご利用ください。

※ 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当に使用されたり、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。

2. クイックスタート

本製品を初期化するには、システム領域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。

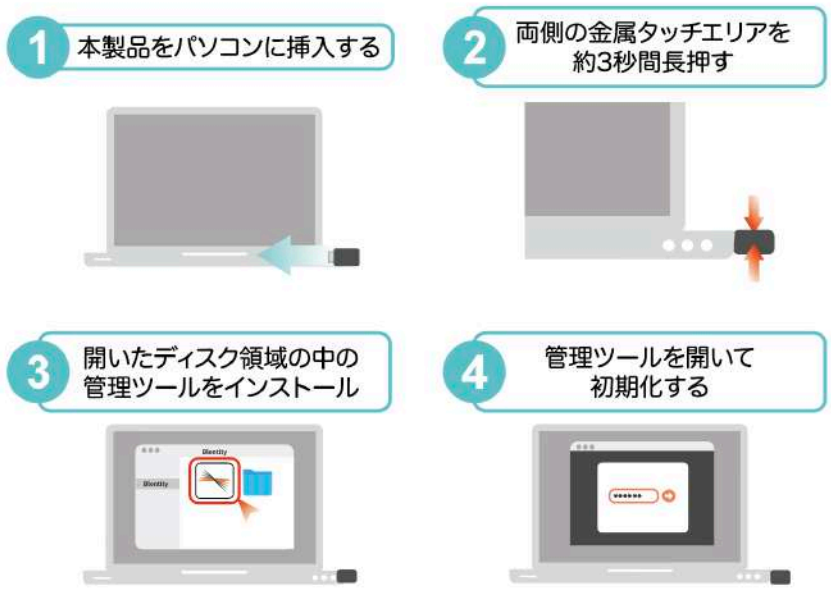
初期化が完了すると、PINコード（暗証番号）一つとパスフレーズ一つを受け取ります。これにより、認証機能、暗号化データの管理、暗号化USB機能を利用できるようになります。

1. デバイスのスイッチが**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の表示で確認できます。
2. コンピュータ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、システム設定画面にアクセスします。
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ますので、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

manOS Blentity/Mac/Blentity Manager Installer.pkg

Windows Blentity/Windows/Blentity Manager Installer.exe



PINコード（暗証番号）保護機能

PINコードは本製品の重要な保護機能です。デバイスの不正利用を防ぐための重要な仕組みです。デバイスを紛失または盗難に遭っても、PINを知らない限り、デバイスを使用することはできません。PINコードを8回連続で間違えると、デバイスは自動的にロックされ、ブルートフォース攻撃から保護されます。

PINコードは、いつでもBlentity Managerを使用して変更することが可能です。

パスフレーズ（Passphrase）復元機能

パスフレーズはランダムに生成された12個の英単語で構成されており、PINロックの解除やデバイスの安全な復元に使用されます。

1. パスフレーズを忘れないように、必ず記録して安全な場所に保管してください（製品のパッケージには記録用の紙カードが付属しています）
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され、**取り消すことができませんのでご注意ください。

セットアップ画面の参考

1. まずはPINコードを設定してください。

2. PINを設定した後、「次へ」をクリックします。初回のセットアップでは、「新しいパスフレーズを生成する」を選択してください。

3. 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。このページでコピーし、次の確認プロセスで直接貼り付けることも可能です。

4. 確認ページに進み、パスフレーズを貼り付けるか入力した後、「次へ」をクリックすると、暗号鍵の生成が始まり、初期化プロセスが完了します。

3. PCファイル暗号化（File Encryptor）

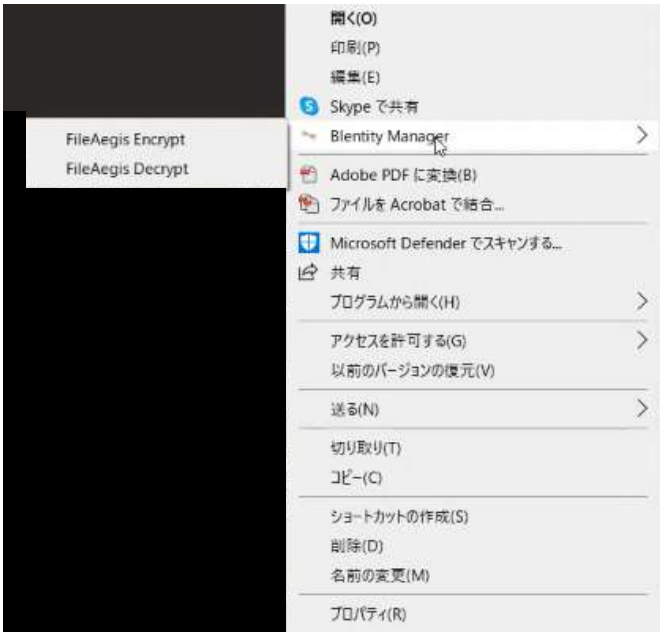
ファイルを暗号化する

ファイルまたはフォルダーを右クリックすると、メニューに「FileAegis Encrypt」を選択して、PINコードを入力したらファイルを暗号化されます。

暗号化されたファイルには自動的に「.btf」という拡張子が追加され、デフォルトでこのパス~/Documents/Blentity File Encryptor　に保存されます。

本製品を初期化した後、この機能が使用できない場合は、右クリックメニューの設定をご参考ください。

Windows



Mac

ファイルを復号化する

btf 拡張子ファイルの右クリックメニューに「FileAegis Decrypt」を選択して、PINコードを入力したら、同じ場所に復元されます。

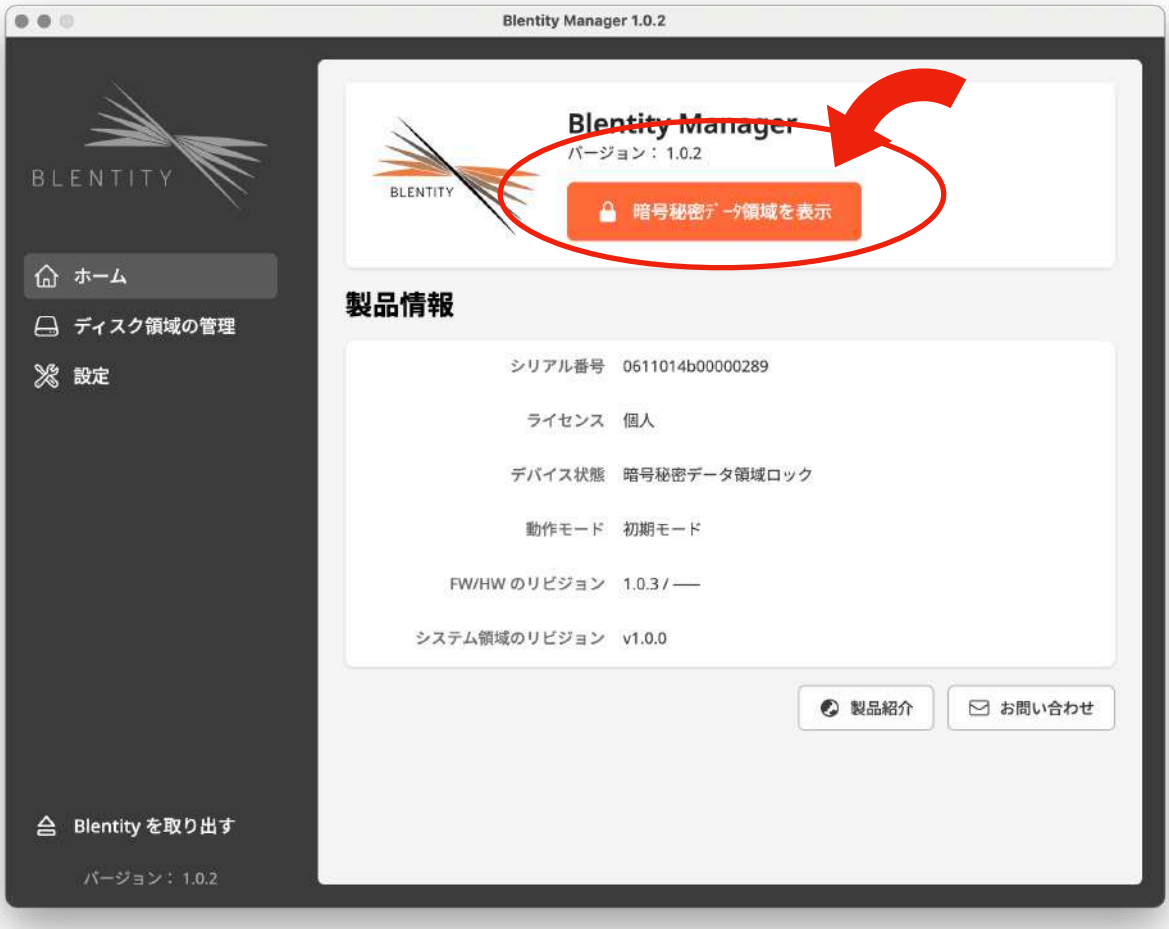
4. 暗号秘密データ領域

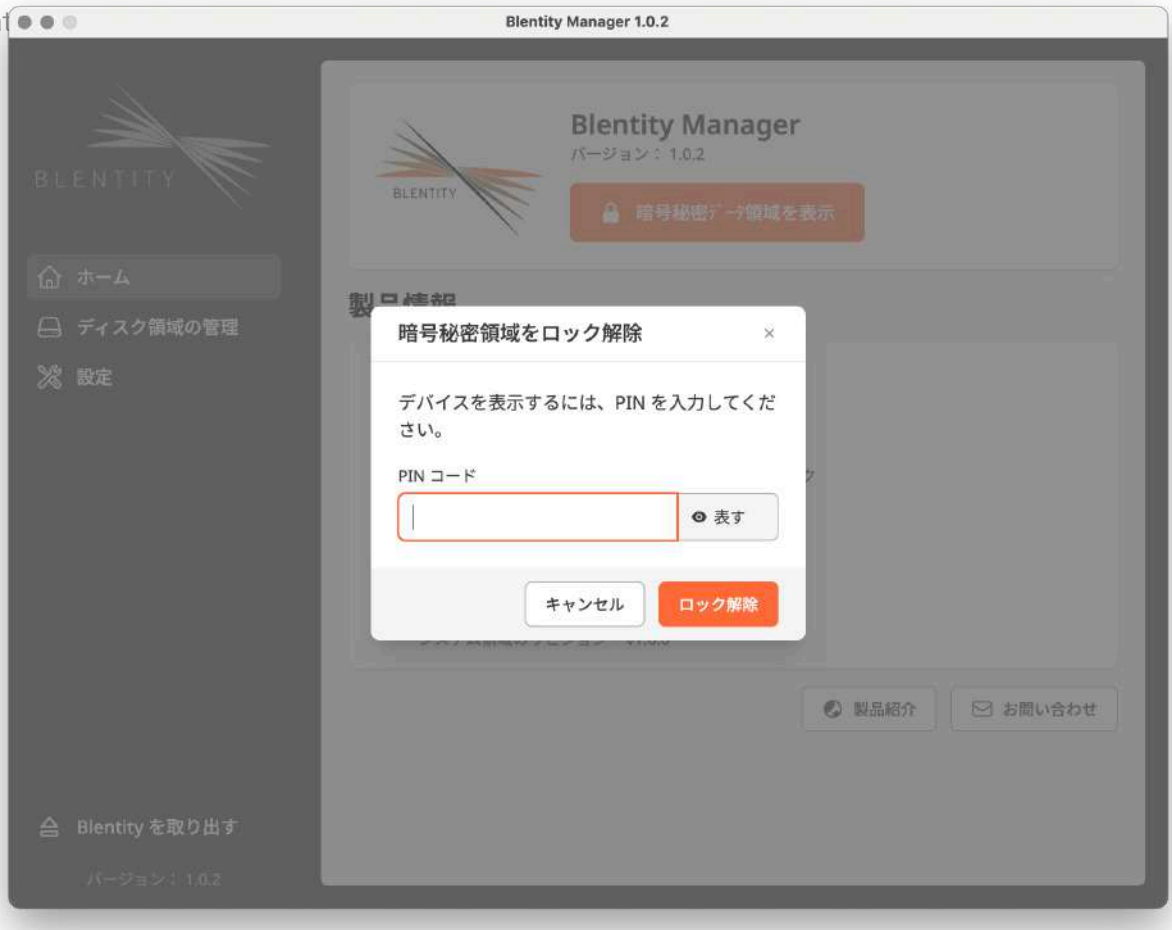
本製品は、ハードウェアベースの暗号化データ領域（AES-256 XTS）を提供しており、機密データの保護に適しています。開くには Blentity Manager でPINコード（暗証番号）の認証が必要です。

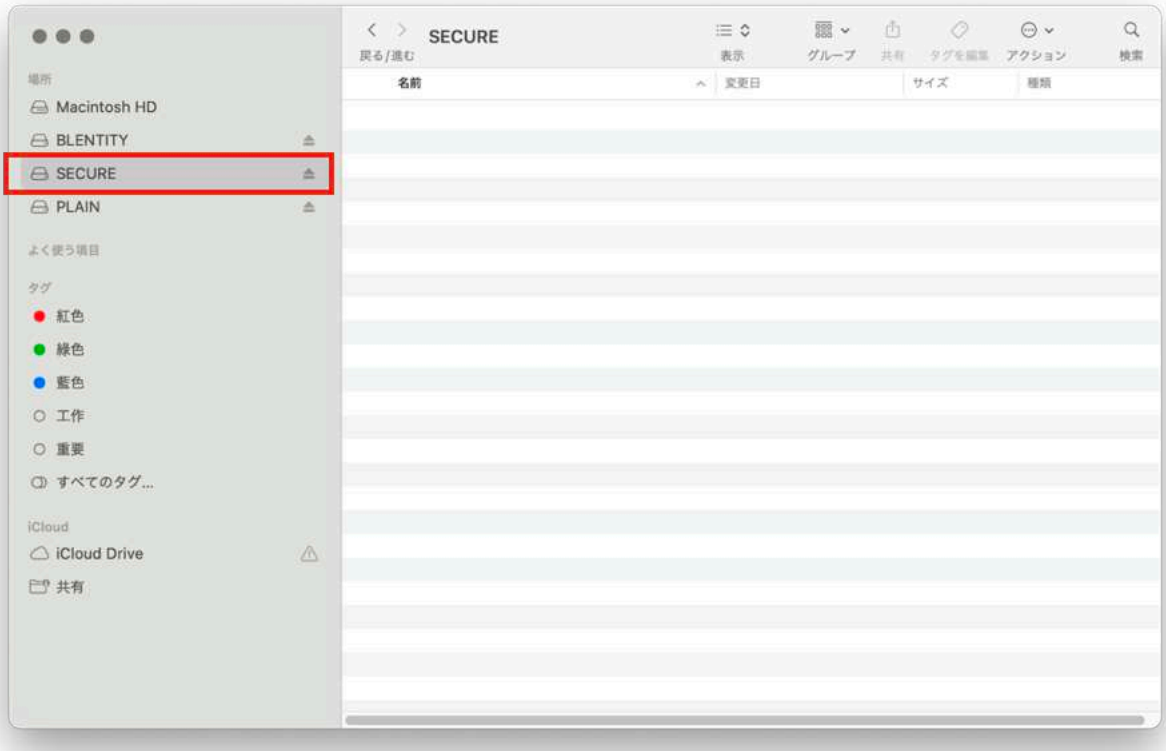
通常データ領域の機能を使用する場合は、ディスク領域の設定に従って容量を割り当ててください。

暗号秘密データ領域を開く手順

1. Blentity Managerを起動します。
2. 「暗号秘密データ領域を開く」をクリックします。
3. PINコードを入力して、暗号秘密データ領域が開きます。







また、システム領域内のライト版アプリケーションを使用して、暗号秘密データ領域を開くこともできます。

1. システム領域を開きます。
2. Blentity Manager Liteを起動します。
3. PINコードを入力して、暗号秘密データ領域が開きます。

5. 二要素認証とパスワードレス認証

本製品はFIDO2国際規格に基づいており、数百のウェブサイトで二要素認証やパスワードレス認証をサポートしています。最新の対応ウェブサイトのリストについては、FIDOアライアンスの公式ウェブサイトをご確認ください。以下は推奨される実行環境です：

Linux	Firefox
macOS	Safari
Windows	Chrome, Edge

! 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。

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アカウントにBlentityを追加する方法

1. Microsoftアカウントページにサインインし、[セキュリティ] > [その他のセキュリティオプション] > [サインインに使用する新しい方法を追加] を選択します。
2. [セキュリティキーを使用する] > [USB] を選択し、[次へ] をクリックします。
3. セットアップ画面が表示されたら、Blentityを挿入し、PINコードを入力します。
4. Blentityの両側にタッチします。
5. セキュリティキーの名前を入力して登録を完了します。

セキュリティキーの管理、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。

6. Blentity Manger について

6-1. バックアップと復元

暗号秘密データ領域のファイルや関連設定を安全にバックアップ・復元する機能です。

バックアップ

管理ツールのメニューから「バックアップと復元」>「バックアップ」を選択します。

1. パスフレーズを入力します。
2. バックアップファイルの保存先を選択します。
3. 暗号化されたバックアップファイルがエクスポートされます。
   ファイル名は「元ファイル名_BlentityBackup.bzb」となります。

復元

管理ツールのメニューから「バックアップと復元」>「復元」を選択します。

! 復元に使用するBlentityは、まず工場出荷状態に戻され、ディスク領域内の全てのデータは削除されます。重要なデータは必ず他の場所にバックアップしてください。また、そのデバイスが登録されていたサービスには再度ログインできません。再登録が必要となります。

1. バックアップファイル「ファイル名_BlentityBackup.bzb」を選択します。
2. 対応するパスフレーズを入力します。
3. バックアップファイルと関連設定が復元されました。
   （通常データ領域がある場合は、フォーマットする必要があります。）

6-2. PINの変更

管理ツールのメニューから「設定 > PINの変更」を選択します。

1. PINコードを入力して検証を行います。
2. 指示に従って新しいPINを設定します。

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。

6-3. PINを忘れた場合

管理ツールメニューから「設定 > PINを忘れた場合」を選択します。

1. パスフレーズを入力して検証を行います。
2. 指示に従って新しいPINを設定します。

6-4. ディスク領域の基本設定

管理ツールのメニューから「設定 > ディスク領域の設定」を選択します。

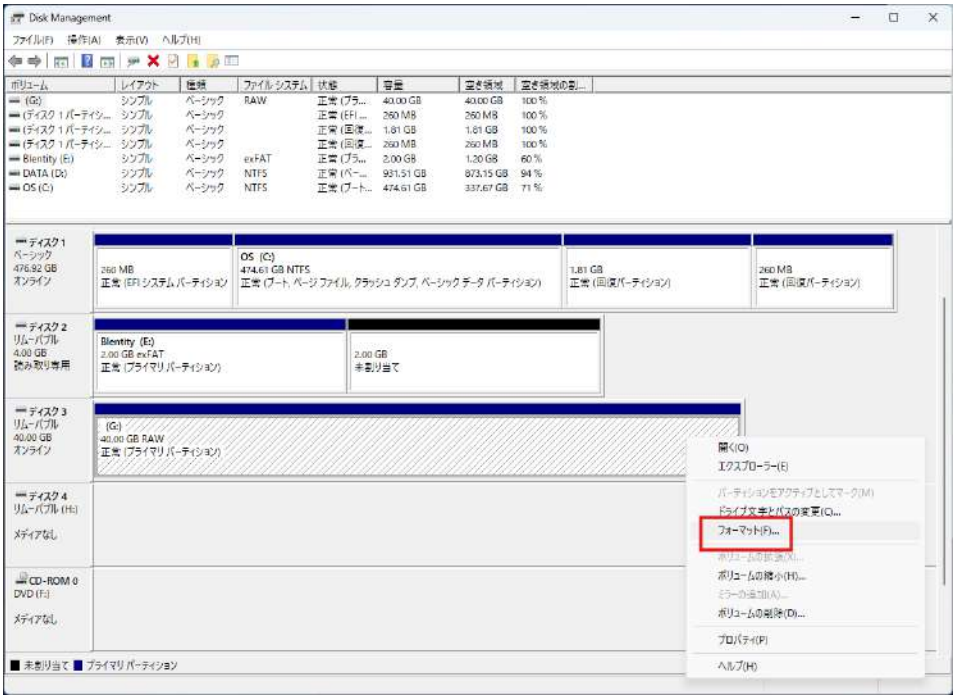
> ! この操作はディスク領域内の**すべてのデータを消去し、取り消すことができません**。操作を実行する前に必ずデータのバックアップを行ってください。

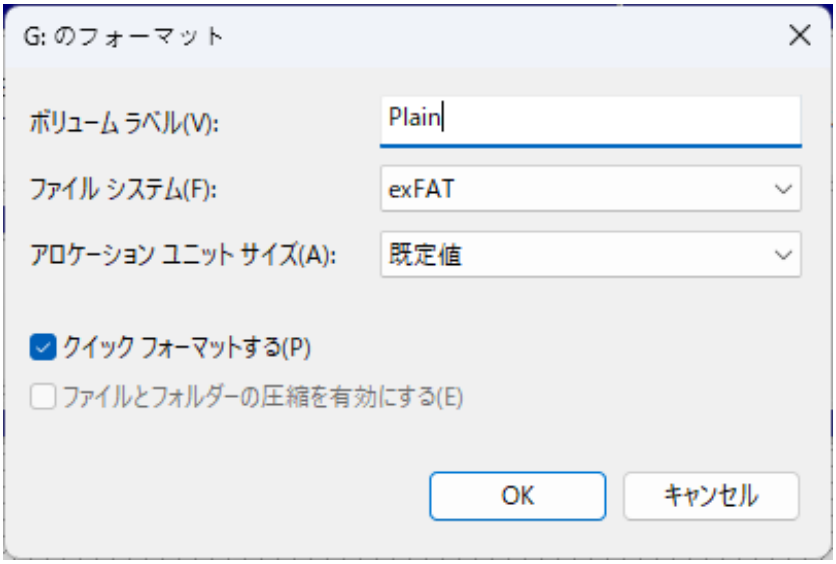
操作手順

1. ディスク領域の容量割り当て、「ディスクが読み取れません」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。
2. 続いて、管理者権限を取得するため、指示に従いシステム管理者のパスワードを入力してください。
3. ディスクの割り当てが完了したら、フォーマットが必要になります。「ディスクユーティリティを開く」をクリックしてください。
4. 対象ディスクを開いて、ディスクユーティリティ内で、対象のディスクを右クリックし、フォーマットをします。
5. ディスクの名前を再設定し、**exFAT** を選択してフォーマットを行ってください。

図: Macでフォーマットする

図: Windowsでフォーマットする





6-5. 動作モードの設定

本製品では、「動作モード」を設定することで、ディスク領域の開き方をニーズに応じて変更できます。管理ツールのメニューから「設定 > 運用モードの設定」を選択すると、以下のモードから選ぶことができます：

- **初期モード**：最も厳重なセキュリティが求められるモードです。すべてのディスク領域はデフォルトで隠され、ハードウェアスイッチをオンにし、タッチエリアを手動で長押しする必要があります。高度なデータ保護が必要な場合に適しています。
- **システム領域モード**：デバイスを挿入すると、「システムディスク領域」のみが自動で開きます。
- **簡易モード**：このモードでは、暗号秘密データ領域を除くすべてのディスク領域が、デバイスを挿入するだけで自動的に開きます。一般のデータを頻繁に使用する方に最適な便利さを提供します。

異なるモードにおける各ディスク領域の開き方

	暗号秘密データ領域（RW）	システム領域（RO）	通常データ領域（RW）
初期モード	管理ツールでの検証後に開く	手動で開く*	手動で開く*
システム領域モード	管理ツールでの検証後に開く	自動で開く*	
簡易モード	管理ツールでの検証後に開く	自動で開く*	自動で開く*

上の表に「*」が付いている場合は、スイッチをオンにして、オレンジ色が表示されるようにしてください。

RW： Read / Write　　RO： Read Only

6-6. 右クリックメニューの設定

File Encryptor 機能を使用するには、右クリックメニューの設定を有効にする必要があります。管理ツールのメニューから「設定 > 言語設定」を選択して、設定ページに進んでください。

MacOSを利用する場合

Finder の右クリックメニューに File Encryptor のオプションを表示するには、Mac 上で File Encryptor の拡張機能を有効にする必要があります。

1. 「システム環境設定」を開きます。
2. 「セキュリティとプライバシー」を選択します。
3. 「拡張機能」タブをクリックします。
4. 「暗号化 (FileAegis)」と「復号化 (FileAegis)」のチェックボックスをオンにします。

これらの設定が完了すれば、Finder の右クリックメニューで File Encryptor 機能を使用できるようになります。

6-7. 言語設定

Blentity Manager 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。

6-8. 工場出荷時設定へのリセット

管理ツールメニューから「設定 > 工場出荷時設定へのリセット」を選択します。

製品を未初期化の状態に戻すことができます。

! 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。

6-9. アップデート

本製品の品質と使用体験を常に最適な状態に保つため、管理ツールを通じてファームウェアの更新が可能です。

管理ツールメニューから「設定 > プログラム更新」を選択して、ソフトウェアおよびファームウェアの更新が可能です。

更新する前に、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。

! 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、取り消すことができませんので、**事前に必ずデータのバックアップを行ってください。

附録A：よくある質問 (FAQ)

Q: Blentityは私のファイルをどう保護しますか？

Blentityは内蔵のハードウェア暗号化技術を使用して、安全な暗号化ストレージとファイル暗号化機能を提供します。内蔵のCCEAL5+セキュリティチップは暗号鍵を保護し、ソフトウェア暗号化のように不安全なコンピュータに鍵を保存することはありません。物理的な侵入やサイドチャネル攻撃に対しても効果的に保護し、あなたのファイルの安全を確保します。

Q: Blentityは私のアカウントをどう保護しますか？

BlentityはFIDOセキュリティキー技術を利用し、非対称暗号化によりハードウェアトークンを持つ者のみが認証されます。これにより、パスワードが漏洩しても、攻撃者はあなたのアカウントにログインできません。フィッシング攻撃やパスワード盗用を防ぎ、アカウントに最高レベルのセキュリティを提供します。

Q: Blentityを紛失した場合、どのようなリスクがありますか？

BlentityはPINコードによる保護機能を採用しており、8回連続でPINコードを間違えるとデバイスが自動的にロックされ、ブルートフォース攻撃から保護されます。したがって、他者にデバイスを盗まれる心配はありません。また、パスフレーズ機能を提供しており、任意のBlentityデバイスでデータを簡単に復元できます。パスフレーズは安全に保管し、定期的に暗号化データのバックアップを行ってください。

Q: デバイスを紛失した場合、コンピュータ上の暗号化ファイルを解読することはできますか？

はい、パスフレーズを使用して別のBlentityデバイスで鍵を復元すれば、そのBlentityを通じて元の暗号化ファイルを解読できます。

Q: デバイスを紛失した場合、Blentityに保存した暗号化ファイルを復元することはできますか？

可能です。事前にバックアップ機能を使用して暗号化ファイルをエクスポートしておけば、パスフレーズを使用して別のBlentityデバイスにインポートし、復元できます。

Q: デバイスを紛失した場合、関連付けたサービスにログインすることはできますか？

サービスのサポート状況によります。FIDOをサポートするサービスは通常、独自のアカウント救済プロセスを提供します。例えば、一部のサービスでは、バックアップセキュリティキーを使用するか、他の本人確認手続きを経てアカウントに再ログインできる場合があります。具体的なアカウント回復手順については、関連サービスの公式説明を参照してください。

Q: 設定したPINは変更できますか？

いつでも管理ツールを使用して変更できます。他社のツールを使用してPINを変更しないでください。

Q: PINがロックされた場合、どうすればよいですか？

8回連続でPINを間違えたり、非公式な管理ツールを使用してPINを変更した場合、PINは自動的にロックされます。その際、状態LEDが赤く点灯しますので、Blentity Managerを開き、パスフレーズを使用してロックを解除し、PINをリセットしてください。

Q: PINを忘れた場合はどうすればよいですか？

PINを忘れた場合、「管理ツール＞設定＞PINを忘れた場合」でPINをリセットできます。

Q: どのような場合にパスフレーズが必要ですか？

- **PINのロック解除**
  PINの入力回数が上限を超えたり、非Blentity Managerのサードパーティツールを使用してPINを変更した場合、PINがロックされます。この場合、Blentity Managerにパスフレーズを入力してロックを解除し、PINをリセットする必要があります。

- **鍵の復元とバックアップファイルの復元**
  デバイスを紛失した場合、パスフレーズを使用して新しいデバイス上でデータを復元できます。この機能により、他のデバイスで簡単に暗号化されたバックアップファイルや暗号鍵を復元できます。

Q: パスフレーズを忘れた場合はどうすればよいですか？

パスフレーズを失うと、以後のバックアップデータを復元できなくなります。必ずパスフレーズを安全な場所に保管してください。パスフレーズを忘れたり失った場合は、データをバックアップした後、工場出荷時設定にリセットして再構築し、パスフレーズを保存することを強くお勧めします。PINがロックされて解除できず、強制的に工場出荷時設定に戻され、データが削除されることを避けるためです。

Q: データを復元するためのBlentityは新しいものでなければなりませんか？

パスフレーズで任意のBlentityでバックアップファイルを復元することができます。ただし、そのデバイスは工場出荷時設定に戻されるため、内部データや鍵は消去されてバックアップファイルのデータが暗号秘密データ領域に復元されます。また、登録していたサービスには再度ログインできません。再登録が必要となります。そのため、新しいBlentityに復元することをお勧めします。

Q: モバイルデバイス、Windows Server、Linuxはサポートされていますか？

これらのオペレーティングシステムはサポート対象外です。これらのシステムで本製品を使用する場合は、自己責任で行ってください。サポートされているオペレーティングシステムとブラウザについては、「附録：仕様とサポート環境」を参照してください。

Q: この製品を使用するにはソフトウェアのインストールが必要ですか？

初期化のために管理ツールをインストールする必要があります。初期化が完了した後は、そのツールをインストールしていないコンピュータでも、ディスク領域を開き、認証トークンとして使えます。

Q: なぜ暗号秘密データ領域の容量設定が、実際に設定された数値と異なるのですか？

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アカウントに登録すると、ブラウザによってはPasskeysまたはFIDO2セキュリティキーとして表示されますが、これは正常ですか？

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。ユーザー体験には違いがありません。

附録B：仕様とサポート環境

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。

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

- 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。

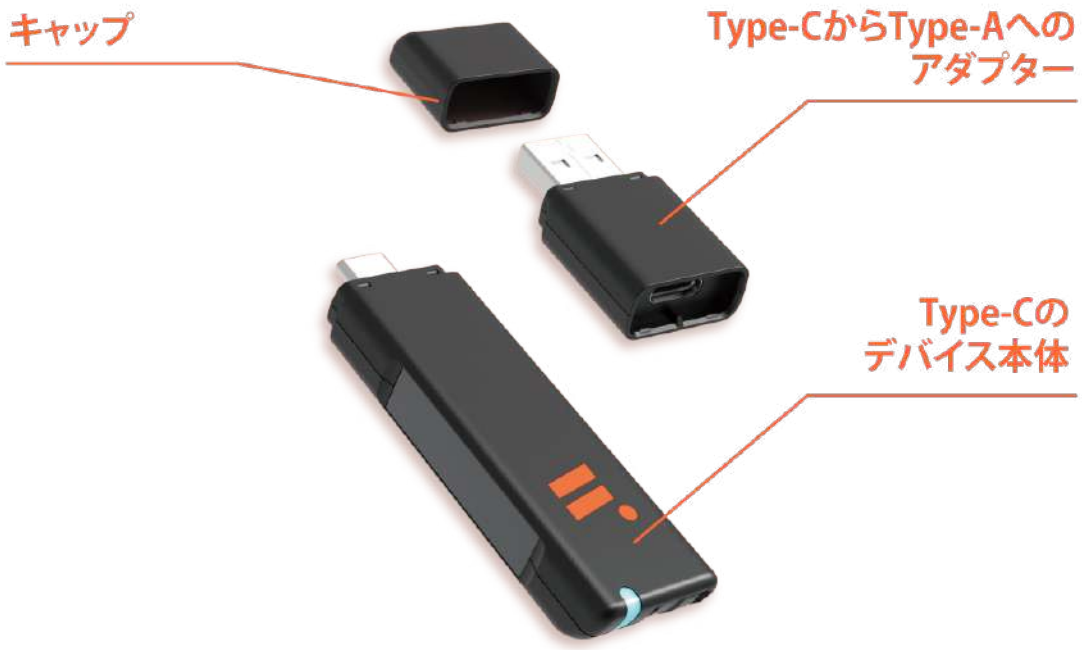
推奨される環境は以下の通りです：

Windows	ChromeおよびEdge
Linux	Firefox
macOS	Safari

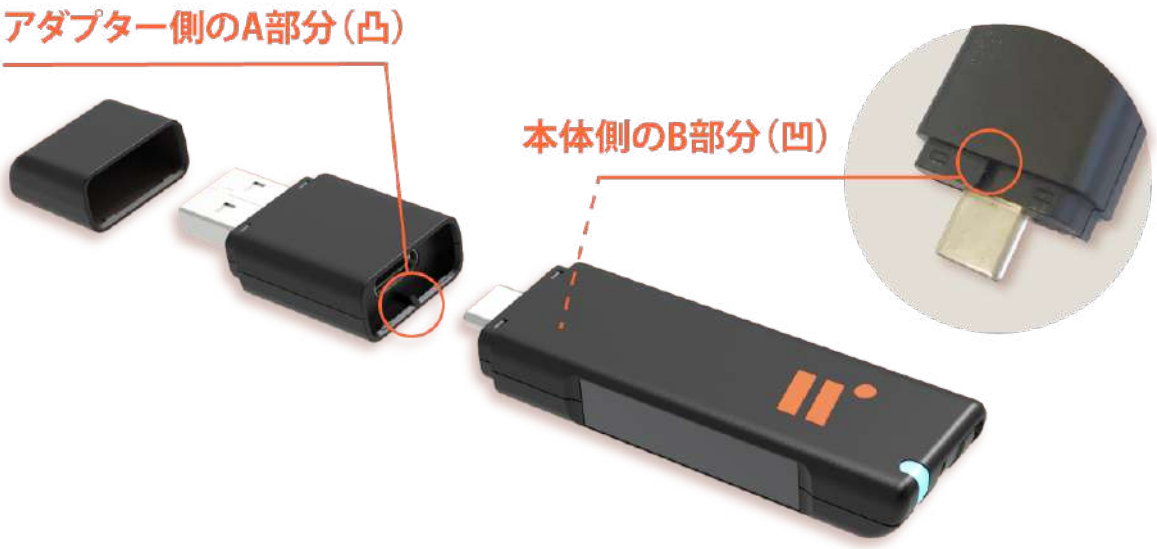
本製品は、FIDO認証機能を使用する前に必ず初期化を行ってください。

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向性があります。
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、操作が実際の人間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。

③ スイッチ

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。
- 動作モードの設定で、データディスクの開閉を自由に制御できます。

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。

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。

ステータスLED

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、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。

附録C：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、異音がするときは、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。

設置場所に関しての注意事項
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)
- 水気の多い場所(台所、浴室等)
- 腐食性ガスを含んだ大気中(Cl_2、H_2S、NH_3、SO_2、NOx 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。

附録D：トラブルシューティングとアフタサービスについて

万一「故障かな？」と思われる場合は、以下の対処方法をお試しください。

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。

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/
お問い合せメール：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ー17:00　月ー金曜日（祝祭日を除く）

Blentity - Data Protector with FIDO2

取扱説明書

バージョン 1.0 | 発行 2024年10月