# IRONKEY™ H200
# ユーザ ガイド

## 目次

# IRONKEY™ H200 の概要

IronKey™ H200 は、生体認証セキュリティ、データ暗号化、デジタル ID、および暗号サービスが組み込まれた USB（ユニバーサル シリアル バス）ポータブル ハード ドライブです。

図 1：IronKey™ H200


このガイドは、最低限の労力で IronKey™ H200 デバイスを設定できるように構成されています。

## 最小システム要件

IronKey™ H200 は、そのアプリケーション パーティション上に組み込みの ACCESS Standard™ ソフトウェアが搭載されています。以下のリストに、ACCESS Standard が組み込まれたデバイスを使用するために必要な要件を示します。

- コンピュータから供給可能な電力に応じて、1 ～ 2 つの USB ポート（タイプ A）
- USB 2.0 または 1.1 大容量記憶装置デバイスをサポートするオペレーティング システム

オペレーティング システム

- Microsoft Windows 7*
- Windows Vista* (Business, Enterprise, Home SP2)
- Windows XP Professional* SP3
- Windows XP Home* SP3
- Mac OS X 10.5 および 10.6

* 32 ビットと 64 ビットの両方

注意：ACCESS Standard は、アクセス重視の設計思想に基づき、Microsoft Active Accessibility (MSAA) を使用して開発されています。この製品は、ほとんどのスクリーン リーダーとの互換性があります。

# IRONKEY™ H200 の概要

## デバイスのアクセサリ

IronKey™ H200 パッケージには、双頭の USB ケーブルが同梱されています。このケーブルの使用方法については、4 ページの「デバイスの差し込み」を参照してください。システムの USB ポートにこのケーブルを接続すると、IronKey™ H200 はコンピュータから必要な電力を得ます。外部電源装置は提供されていません。また、使用の必要もありません。

## ドキュメント

IronKey™ H200 の使用および管理方法の詳細については、『ACCESS Standard ユーザガイド』に記載されています。

以下のトピックが記載されています。

- Imation デバイスに関する情報
- デバイスのカスタマイズ
- デバイスへのアクセス
- ユーザの管理
- デバイスの管理
- ウィルスからのデバイスの保護
- トラブルシューティング

オンライン ヘルプも、ACCESS Standard ソフトウェアとともに利用できます。

注意：ドキュメントを表示するには、Adobe® Reader® (http://www.adobe.com/acrobat) が必要です。

オンライン ヘルプを表示するには

- ACCESS Standard が開いているときに、詳細を表示するページの [ ヘルプ ] をクリックします。

# はじめに

デバイスを使用する前に、そのデバイスをコンピュータに正しく接続する必要があります。新しいデバイスを差し込んでから、認証およびプライベート パーティションの機能を使用する前に、そのデバイスをカスタマイズする必要があります。カスタマイズ プロセスについて案内するため、デバイスはプレインストールされている ACCESS Standard ソフトウェアを使用します。新しい（またはリサイクルされた）デバイスを差し込むと、カスタマイズ ウィザードが自動的に起動します。コンピュータで自動実行が構成されていない場合は、デバイス上のアプリケーション パーティションから ACCESS Standard を起動できます。

## デバイスの差し込み

本製品は、ホスト コンピュータに直接接続されている必要があり、同梱のケーブルのみを使用して、適切に接続する必要があります。中間ハードウェアを介した接続または代替のケーブルでは、製品の元の設計と認証外の電気放出が生じる可能性があります。IronKey™ H200 を使用するには、ホスト コンピュータによって供給される電力に応じて 1 ～ 2 個の USB コネクタが必要となる場合があります。

**IronKey H200 を 1 つの USB ポートを使用して差し込むには**

1. IronKey H200 デバイスの背面に小さい方（ミニ A）の USB コネクタを差し込みます。
2. 黒いタイプ A の USB コネクタをホスト コンピュータに差し込みます。
3. 灰色のタイプ A の USB コネクタは差し込まないでください。

   黄色の電源 LED がゆっくり点滅する場合は、2 つの USB ポートを使用する手順に従ってください。

**IronKey H200 を 2 つの USB ポートを使用して差し込むには**

1. IronKey H200 デバイスの背面に小さい方（ミニ A）の USB コネクタを差し込みます。
2. 灰色のタイプ A の USB コネクタをホスト コンピュータに差し込みます。
3. 黒いタイプ A の USB コネクタをホスト コンピュータに差し込みます。

   黄色の電源 LED がゆっくり点滅する場合、ホスト コンピュータが USB の仕様を満たさず、デバイスに必要な電力を供給できません。

注意 1：黒い USB コネクタを最初に差し込んでから灰色のコネクタを差し込むと、IronKey H200 の起動が数秒間遅くなる可能性があります。

注意 2：黄色の電源 LED が速く点滅する場合、電力検出がタイムアウトしています。USB 接続をすべて取り外して、ケーブルを再接続してください。

## デバイスのカスタマイズ

カスタマイズ プロセスでは、主に以下の 3 つの手順を実行します。

1 デバイス プロファイルの適用 ー プロファイルは、デバイスのデフォルト 優先順位を設定します。デバイス設定があらかじめ構成されている「 標準」プロファイルを選択、またはデバイス設定を自分で構成できる「 カスタム」プロファイルを選択できます。標準プロファイルには、以下のデバイス設定が含まれています。
   - 認証方法：生体認証またはパスワード

# はじめに

- デバイス ユーザ数: 1 ( 管理者を含まない )
- プライベート パーティションは使用可能な全ディスク領域を使用
- 2 要素認証: オフ
- 生体認証のセキュリティ レベル: 4,500 分の 1
- 最小パスワード長: 6
- パスワードの再試行制限回数: 10
- パスワードの再使用しきい値: 3
- ユーザのレスキュー: 有効
- データ破棄: オフ
- 管理者アカウント : 有効
- 生体認証の再試行制限回数: 無制限

2. 管理者アカウントの作成 ー 管理者だけが、ユーザの追加、削除、レスキューなど特定の操作をデバイス上で実行することができます。カスタマイズ プロセス中、管理者パスワードを設定すると、管理者アカウントが自動的に作成されます。カスタム プロファイルを選択して、管理者アカウントを無効にすると、管理者パスワードの入力が要求されなくなります。この場合、その後でアカウントを作成することができません。

   管理者パスワードを記憶、または安全な場所に保管しておくことが非常に重要です。

3. ユーザの作成 ー デバイス プロファイルに応じて、デバイス上で 1 人以上の一般ユーザを作成できます。

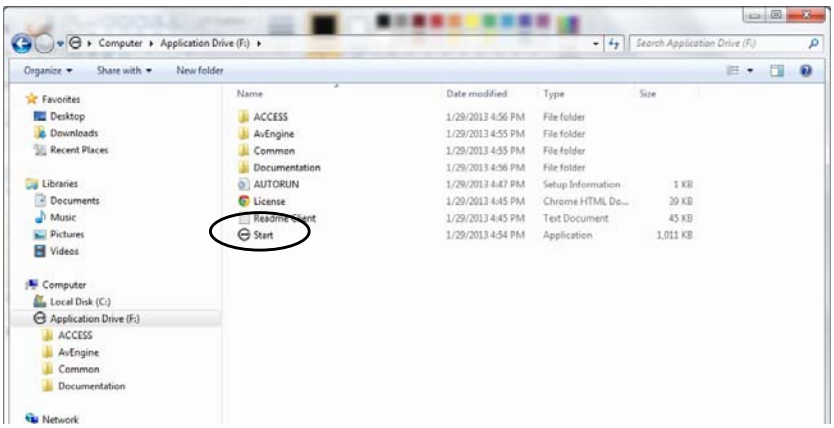
注意: 生体認証のみを使用するカスタム プロファイルは、FIPS 承認モードの動作と見なされません。パスワードの使用も強くお勧めします。生体認証は、パスワードの事実上の脆弱性を強化する 2 つ目の要素を提供します。生体認証のみを使用することは可能ですが ( 推奨されません )、設定した低誤合致率 (FMR) に関わらず、承認されていないユーザがデバイスに認証できる可能性が残ります。

# はじめに

デバイスをカスタマイズするには

1. デバイスをコンピュータの USB ポートに接続します。詳細については、4 ページの「デバイスの差し込み」を参照してください。

   自動実行により ACCESS Standard が自動的に起動しない場合は、アプリケーション パーティション上のルートディレクトリから **Start.exe** ファイルをダブルクリックします。( 必要に応じて、タスクバーの右端にある通知領域で IronKey アイコンをクリックし、メニューから **[** カスタマイズ **]** をクリックします )。




2. **ACCESS Standard** のメイン ページで、**[** デバイスのカスタマイズ **]** をクリックしてください。
3. **[** デバイスのカスタマイズ **]** ページで、デバイス プロファイル オプションの 1 つをクリックします。
4. 管理者パスワードを設定 ( 該当する場合 ) およびユーザを作成するには、その後に続くページの指示に最後まで従います。

注意 1: カスタマイズ プロセスを完了しない場合、次回デバイスに接続するときに上記の手順の一部を繰り返す必要がある場合があります。カスタマイズ プロセスの詳細については、『ACCESS Standard ユーザ ガイド』を参照してください。

注意 2: カスタマイズ プロセスが正常に完了すると、ファイル マネージャを使用してプライベート パーティションにアクセスできます。ログインして、プライベート パーティションにファイルを保存する方法、またはプライベート パーティションからファイルを開く方法については、7 ページの「デバイスのデータへのアクセス」を参照してください。

# デバイスのデータへのアクセス

デバイスをカスタマイズした後、登録済みユーザだけがそのデバイスに認証できます。認証には、パスワード、指紋、またはその両方を使用したデバイスへのログインが含まれます。使用する認証方法は、デバイスの機能およびデバイスへ適用されるプロファイルによって異なります。

ログインに成功すると、プライベート パーティションにファイルを保存したり、そのパーティションからファイルを開くことができます。コンピュータから離れている間、デバイスを接続したままにする必要がある場合は、そのデバイスをログアウトすることをお勧めします。ログアウトしない場合、不在中に他のユーザがそのプライベート パーティションにアクセスする可能性があります。また、デバイスを完全に切断することで、データを持って移動することもできます。

この章では、以下のトピックについて説明します。

- デバイスのログインとログアウト
- ファイルの保存および開き方
- デバイスの接続の取り外し

## デバイスのログインとログアウト

デバイスにログインするには

1. タスクバーの右端にある通知領域で、[IronKey] アイコン を右クリックして、[ ログイン ] をクリックしてください。
2. Mac OS X を実行しているコンピュータを使用している場合は、ファイル マネージャを開き、デバイスのアプリケーション ドライブをクリックします。[**ACCESS Standard**] アプリケーションをダブルクリックして、[ デバイスの管理 ] で、ACCESS Standard のメインページで [ ログイン ] をクリックしてください。
3. デバイスで正しく認証されるまで、認証ウィザードのプロンプトに従います。

ヒント：生体認証だけを使用するデバイスの場合は、指紋センサーに指をスワイプすることで、ACCESS Standard を起動することなくデバイスにログインできます。

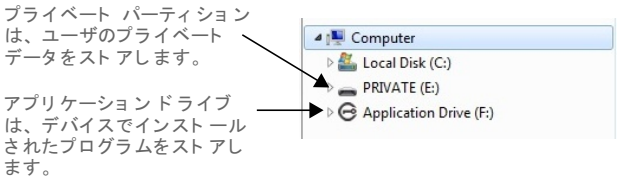
デバイスからログアウトするには

1. タスクバーの右端にある通知領域で、[IronKey] アイコン を右クリックして、[ ログアウト ] をクリックしてください。
2. Mac OS X を実行しているコンピュータを使用している場合は、ファイル マネージャを開き、デバイスのアプリケーション ドライブをクリックします。[**ACCESS Standard**] アプリケーションをダブルクリックして、[ デバイスの管理 ] で、ACCESS Standard のメインページで [ ログアウト ] をクリックしてください。

# デバイスのデータへのアクセス

## ファイルの保存および開き方

デバイスを差し込むと、Windows® エクスプローラなどのファイル マネージャに、アプリケーション ドライブおよびプライベート パーティションの両方が、各パーティションにドライブ文字が関連付けられた状態で表示されます。




デバイスにログインすると、適切なプログラムまたはファイル マネージャを使用してプライベート パーティションにあるファイルを開くことができます。プライベート パーティションにデータを保存すると、デバイスは 256 ビット の AES ハードウェア ベース暗号化機能を使用してデータを暗号化します。ファイルを開くとき、データは自動的に復号されます。

注意: アプリケーション パーティションにはデータを保存できません。

## デバイスの接続の取り外し

デバイスの接続の取り外し

- タスクバーの右端にある通知領域で、[IronKey] アイコン を右クリックして、[ デバイスの取り出し ] をクリックしてください。

ヒント : また、タスクバーの右端の通知領域にある [ ハードウェアの安全な取り外し ] アイコンをクリックしても、デバイスを切断できます。「 USB 大容量記憶装置デバイス - ドライブ (F:) を安全に取り外します」メッセージをクリックします。ここで、F はデバイスに関連付けられた、ファイル マネージャでのドライブ文字です。続いて「 USB 大容量記憶装置デバイスは安全に取り外すことができます」というメッセージが表示されたら、デバイスを切断します。

注意: Mac OS X を実行しているコンピュータを使用している場合は、デスクトップ上のデバイス ドライブを [ ごみ箱 ] にドラッグします。[ 取り出し ] プロンプト が表示されたら、マウスのボタンを離します。

注意: 適切な取り外し 操作を行わずに、誤って、または故意にデバイスを切断すると、デバイス上のデータが破損する可能性があります。

# トラブルシューティング

この『ユーザガイド』の指示に従っても、IronKey™ H200 の使用が難しい場合は、以下のトラブルシューティング情報をお読みください。

- USB ケーブルが正しく差し込まれていて、そのケーブルがデバイスに十分な USB 電力を供給していることを確認します。十分な電力を確保するために正しくデバイスを差し込む方法については、4 ページの「デバイスの差し込み」を参照してください。
- デバイスへの出力およびデバイスの状態を評価するため、IronKey H200 の発光ダイオード（LED）の状態を確認します。
- Imation.com/support の「FAQ」セクションを確認してください。

表 1: デバイスの LED の状態

| LED の状態 | 説明 |
|---|---|
| 認証およびデータ転送の状態 | |
| 緑色の点灯 | オープンな状態：認証メカニズムが設定されていない場合、すべてのユーザがデバイスを使用できます。<br>ユーザがデバイスにログインしている状態：ユーザが存在する場合、デバイスでユーザが認証済みであることを示します。 |
| 緑色の点滅 | 点滅の頻度は 1 秒間に約 1 回で、以下のいずれかの状況が原因でデバイスが指を待機していることを示します。<br>・デバイスが差し込まれたばかりで、ユーザが現在デバイスにログインしていない。<br>・ソフトウェアが生体認証または登録操作を開始した。<br>・ユーザが指の認証操作を開始した。例えば、デバイスが「アイドル状態」という指を待機している状態のときにデバイスに触れた。デバイスは、LED が赤色になってデバイスがロックされたことを示す前に、2 分間アイドル状態となります。 |
| 赤色で 1 回点滅 | 指紋認証試行に失敗した。デバイスは、失敗信号が終わったあと、指の待機状態（緑の通常点滅）に戻ります。 |
| 赤色と緑色が交互に点滅している LED | デバイスが認証する指を待機中。ただし、これは生体認証によるアクセスがブロックされる前の、最後の認証の機会でもあります。頻度は 1 秒に約 2 回です。 |

# トラブルシューティング

表 1: デバイスの LED の状態

| LED の状態 | 説明 |
|---|---|
| 赤色の点滅 | デバイスの電源が投入されたか、またはデバイスが完全にブロックされている。完全にブロックされている場合、ユーザがデバイスにログインできる認証方法はありません。つまり、これはデバイスをリサイクルする必要があることを示しています。 |
| 赤色の点灯 | デバイスがロックされている。 |
| 青色の LED | すべてのデバイスに対するデータの転送動作を示す。 |
| 赤色と青色の点滅 | 致命的なエラーが起きたことを示す。 |
| デバイスへの電力の状態 | |
| 黄色の点灯 | ホスト コンピュータから十分な電力が供給され、デバイスが正常に動作している。 |
| 黄色の点滅（遅い） | デバイスが動作するための電力が不足している。両方の USB コネクタをホスト コンピュータへ取り付けます。両方のコネクタがすでに差し込まれていても LED が点滅し続ける場合、ホスト コンピュータが USB 電力仕様を満たしていません。 |
| 黄色の点滅（速い） | 電力検出がタイムアウトしている。USB 接続をすべて取り外して、再接続してください。 |
| 黄色い LED の点灯なし | 電力が検出されない。デバイスは電源オフの状態です。 |

# 保証情報

限定保証：小売店から本製品を購入した日の 5 年以内に、材質や製造の欠陥が現れた場合、Imation の意向に応じて修理または交換されます。保証サービスを得るには、購入証明が必要です。この保証は、通常の摩耗、または同梱ソフトウェアには適用されません。Imation は、データの喪失や、その他の間接的、付随的、または結果的に生じる損害について、一切責任を負わないものとします。一部の管轄では付随的または結果的な損害の除外が許容されないため、上記の制限または除外が適用されない場合があります。この保証により、特定の権利が与えられます。国によって異なる他の権利を有する場合があります。

法規制のコンプライアンス：
FCC
本デバイスは、FCC 規則のパート 15 に準拠しています。使用にあたっては、以下の 2 つの条件が対象となります。(1) 本デバイスは有害な電波障害を引き起こしてはなりません。また、(2) 本デバイスは、望ましくない動作を引き起こす可能性のある電波障害を含め、受信したいかなる電波障害をも受け入れる必要があります。

住宅利用に関する説明：
注意：本機器は、FCC 規則のパート 15 に準拠した試験の実施により、クラス B のデジタルデバイスの制限に適合するものと認定されています。これらの制限は、住宅での設置で危険な妨害を防ぐための正当な保護を行うように設計されています。本機器は、無線周波エネルギーを生成、使用、ならびに放射する可能性があり、取扱説明書に従ってインストールおよび使用されない場合には、無線通信に有害な無線障害をきたす恐れがあります。ただし、妨害が特定の取り付けで発生しないという保証はありません。本機器が無線またはテレビの受信に対して有害な無線障害を生じさせる場合（機器のオフ / オンの切り替えで判断可能）、ユーザは以下の方法のうち 1 つまたは複数の方法で妨害の修正を試みることが奨励されます。

- 受信アンテナの方向を調整したり、移動します。
- 機器と受信機の間の距離を増やします。
- 受信機が接続されているコンセントとは異なる回路にあるコンセントに、機器を接続します。
- ディーラーまたは経験豊かな無線 / テレビ技術者に相談して、支援を受けてください。

注意：Imation Corp. によって明示的に許可されていない変更または改造は、ユーザの装置を使用する権限を無効にする可能性があります。

このクラス B 装置はカナダの ICES-003 に準拠しています。

以下の情報は、EU 各国だけに適用されます。
ご購入いただいた機器は、その製造において天然資源を抽出および使用する必要がありました。これらは、人の健康および環境に影響を与える可能性のある有害性物質を含んでいる場合があります。 印の付いている車輪付きゴミ箱の記号は、この製品を家庭廃棄物として処分できないことを表します。適切な回収システムでこの製品を処分することにより、環境への有害性物質の拡散を防ぎ、天然資源への影響を抑えることができます。これらのシステムは、寿命を迎えた機器のほとんどの素材を適切な方法で再利用またはリサイクルします。回収、再利用、およびリサイクルシステムに関する詳細については、お住まいの地域の廃棄物管理局にお問い合わせください。

Imation Enterprises Corp.
1 Imation Way
Oakdale, MN 55128-3414 USA

www.imation.com | info@imation.com

KCC-REI-IMN-H200

# 保証情報 続