

ACCESS STANDARD™
ユーザガイド

Copyright 2013 Imation Corp.

Imation、Imation ロゴ、IronKey と IronKey ロゴ、および ACCESS Standard は Imation Corp. の商標です。その他の商標は、それぞれの所有者の財産です。

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

www.imation.com

サポート : <http://www.imation.com/support>

目次

ACCESS Standard の概要	4
概要 Imation デバイス	4
セキュリティ	6
システム要件	6
はじめに	8
ACCESS Standard 起動	8
デバイスのカスタマイズ	9
1. デバイス プロファイルの選択および適用	9
2. 管理者アカウントの作成	10
3. 最初のユーザの作成	11
LED の状態	11
デバイスのデータへのアクセス	12
デバイスのログインとログアウト	12
ファイルの保存および開き方	13
デバイスの接続の取り外し	13
ユーザの管理	14
ユーザの種類	14
ユーザの作成	14
ユーザの削除	15
認証方法の管理	15
ユーザのレスキュー	15
ユーザ情報の表示	16
デバイスの管理	17
言語の選択	17
デバイス情報の表示	17
デバイスのリサイクル	17
ウイルスからのデバイスの保護	19
デバイスおよびホスト コンピュータのスキャン	19
ウイルス データベースの更新	19
ACCESS Antivirus Scanner イベントの記録	20
トラブルシューティング	21
デバイスを取り出せない	21
生体認証デバイスが指を認証しない	21
デバイスへのパスワードまたは生体認証アクセスがブロックされる	21
デバイスのドライブ マッピングが表示されない	21
アプリケーション パーティションに保存されたデータを使用できない	22
デバイス ポリシー設定付録	23
パスワード ポリシー	25
インデックス	27

ACCESS STANDARD の概要

Imation デバイスは、安全なポータブルストレージを提供する USB（ユニバーサルシリアルバス）デバイスです。ACCESS Standard™ ソフトウェアを使用することで、デバイスをカスタマイズおよび管理することができます。ACCESS Standard は、デバイスの設定および使用開始時に役立つ詳しい操作手順を提供します。

Imation デバイスを大規模展開する場合、カスタマイズからエンド ユーザへの配信、オプションのリサイクル、および新しいユーザによる再使用までのライフサイクルを通じてデバイスを制御できるようにする ACCESS Enterprise™ - のスケーラブルな管理ソリューションを使用します。ACCESS Enterprise の詳細については、Imation にお問い合わせください。

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。

この章では、以下の情報について説明します：

- ・ 概要 Imation デバイス
- ・ セキュリティ
- ・ システム要件

概要 IMATION デバイス

各デバイスに関する簡単な説明を以下の表に示します。ACCESS Standard は一覧表示されているデバイスをすべてサポートします。

表 1: Imation デバイス

デバイスのイメージ	名前	説明
	IronKey™ F200	<ul style="list-style-type: none"> ・ 生体認証、パスワード、および 2 要素セキュリティ ・ 組み込みの ACCESS Standard ソフトウェア（インストール不要） ・ プライベート およびアプリケーション ディスクパーティション
	IronKey™ F100	<ul style="list-style-type: none"> ・ パスワード セキュリティ ・ 組み込みの ACCESS Standard ソフトウェア（インストール不要） ・ プライベート およびアプリケーション ディスクパーティション

表 1: Imation デバイス

デバイスのイメージ	名前	説明
	IronKey™ F150	<ul style="list-style-type: none"> ・ パスワード セキュリティ ・ 組み込みの ACCESS Standard ソフトウェア (インストール不要) ・ プライベート およびアプリケーション ディスクパーティション
IronKey H100  IronKey H80 	IronKey™ H100 & IronKey™ H80	<ul style="list-style-type: none"> ・ 組み込みの ACCESS Standard ソフトウェア (インストール不要) ・ プライベート およびアプリケーション ディスクパーティション ・ 極めて大きな記憶域容量
	IronKey™ H200	<ul style="list-style-type: none"> ・ 生体認証、パスワード、および 2 要素セキュリティ ・ 組み込みの ACCESS Standard ソフトウェア (インストール不要) ・ プライベート およびアプリケーション ディスクパーティション ・ 極めて大きな記憶域容量
	MXI Stealth™ MXP (Gen I)	<ul style="list-style-type: none"> ・ 生体認証、パスワード、および 2 要素セキュリティ ・ 組み込みの ACCESS Standard ソフトウェア (インストール不要) ・ プライベート およびアプリケーション ディスクパーティション
	MXI Gen I Stealth MXP® Passport	<ul style="list-style-type: none"> ・ パスワード セキュリティ ・ 組み込みの ACCESS Standard ソフトウェア (インストール不要) ・ プライベート およびアプリケーション ディスクパーティション

表 1: Imation デバイス

デバイスのイメージ	名前	説明
	MXI Stealth™ Key M200	<ul style="list-style-type: none"> ・ パスワード セキュリティ ・ 組み込みの ACCESS Standard ソフトウェア（インストール不要） ・ プライベート およびアプリケーション ディスクパーティション
	MXI Outbacker MXP® (Gen1)	<ul style="list-style-type: none"> ・ 生体認証、パスワード、および 2 要素セキュリティ ・ 組み込みの ACCESS Standard ソフトウェア（インストール不要） ・ プライベート およびアプリケーション ディスクパーティション ・ 極めて大きな記憶域容量

ディスク パーティション

コンピュータは、各デバイスのパーティションを個別のドライブとして認識します。

- ・ **プライベート パーティション**：ユーザのプライベート データを保存します。ユーザはそれぞれ、デバイスへログイン後にアクセスできる自分のプライベート パーティションを持ちます。詳細については、13 ページの「ファイルの保存および開き方」を参照してください。
- ・ **アプリケーション パーティション**：ACCESS Standard などのプレインストールされたアプリケーションを含みます。このパーティションでデータを保存したり削除することはできません。

セキュリティ

セキュリティ オプションは、使用している Imation デバイスに応じて異なります。一般的に、各デバイスには以下の 2 つの主なセキュリティ形式があります。

- 1 **デバイスへのアクセス**：生体認証（指紋）、パスワード、および 2 要素を含む、デバイスに使用可能な認証メカニズムによって制御されます。2 要素認証では、デバイスをロック解除するために生体認証およびパスワードの両方を必要とします。生体認証だけを使用すると、FIPS 承認モードの動作と見なされません。詳細については、21 ページの「認証の種類」を参照してください。
- 2 **プライベート データの保護**：プライベート パーティションで各ユーザの情報を暗号化することにより提供されません。

Imation デバイスは、AES アルゴリズム (FIPS PUB 197) と 256 ビットのキーを使用することで、プライベート パーティションのデータを暗号化します。データはデバイスで転送されるときに自動的に暗号化または暗号化解除されます。暗号化キーは各ユーザに対して固有で、ユーザを作成するたびにデバイス上で生成されます。

注意：IronKey™ H80 は FIPS 認証ではありません。

システム要件

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の要件を示します。デバイスは、そのアプリケーションパーティション上に ACCESS Standard のプレインストールバージョンが組み込まれています。

- ・ 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 XP Professional SP3*
- Windows XP Home SP3*
- Windows Vista* (Home、Business、**および** Enterprise Edition SP2)
- Mac OS X 10.5 **および** 10.6

* 32 ビットと 64 ビットの両方

はじめに

ACCESS Standard は、新しいデバイスおよびリサイクルされたデバイスをカスタマイズできるアプリケーションです。また、ACCESS Standard を使用してユーザおよびデバイスを管理することもできます。新しいデバイスおよびリサイクルされたデバイスを最初に使用するときは、そのデバイスをカスタマイズする必要があります。

デバイス上の発光ダイオード (LED) を使用して、デバイスの現在の状態を識別することができます。例えば、緑色の点灯は、デバイスをカスタマイズする必要があるか、またはユーザが現在デバイスにログインしていることを表します。

この章では、以下のトピックについて説明します。

- ACCESS Standard 起動
- デバイスのカスタマイズ
- LED の状態

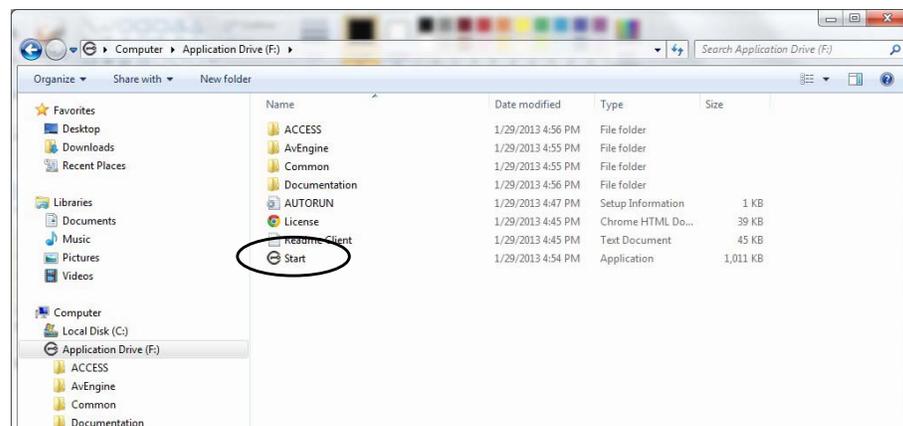
ACCESS STANDARD 起動

ACCESS Standard は、新しいデバイスまたはリサイクルされたデバイスを差し込むと、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ドライブから ACCESS Standard を起動できます。

ACCESS Standard を起動するには

1. デバイスが新しい、またはリサイクルされている場合は、そのデバイスをコンピュータの USB ポートに差し込みます。ACCESS Standard は自動的に起動します。

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 [デバイスのカスタマイズ] をクリックします)。



2. 9 ページの「デバイスをカスタマイズするには」の手順に従います。

3. デバイスがすでにカスタマイズされている場合は、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て、メニューから [デバイスの管理] を選択することで、ACCESS Standard を起動できます。

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、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ます。

デバイスのカスタマイズ

デバイスのカスタマイズ プロセスでは、デバイス プロファイルの適用、管理者アカウント の作成、およびユーザの作成という 3 つの主な手順を実行します。

デバイスをカスタマイズするには

1. ACCESS Standard を起動します (8 ページの「 ACCESS Standard 起動」を参照)。
2. [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。
3. 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、その後続く ページの指示に最後まで従います。

注意: 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、12 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。すべてのカスタマイズ 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一部の手順を繰り返す必要がある場合があります。

1. デバイス プロファイルの選択および適用

デバイス プロファイルは、使用する認証方法の種類 (例えば、生体認証、パスワード、または 2 要素)、および他のデバイス ポリシー (ユーザ数、パスワード 長、生体認証およびパスワード の再試行制限回数など) を決定します。デバイス プロファイルを適用する場合、以下の 2 つのオプションから選択できます: 標準およびカスタム。

標準

[標準] オプションは非生体認証デバイス および生体認証デバイスに対してパスワード 認証だけを使用するか、生体認証デバイスに対してパスワード だけを使用します。1 人のユーザだけがデバイスで許可されます (管理者アカウント は含まれません)。[標準] オプションは、以下のデフォルト の認証設定を適用します (該当する場合):

- ・ 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

カスタム

[カスタム] オプションでは、デバイスで使用する認証方法を選択したり、デバイス ポリシーをカスタマイズすることができます。使用可能なポリシーは、ご使用のデバイスの種類によって異なります。例えば、生体認証の再試行制限回数は生体認証デバイスだけに適用されます。作成するデバイス プロファイルが複数のユーザを許可する場合、デフォルトでプライベート パーティション領域が管理者アカウントを除くすべてのユーザに対して均等に分割されます。ユーザの作成時に、各ユーザに特定のプライベート パーティションのサイズを設定することができます。カスタム プロファイルで設定したデバイス ポリシーは、デバイス上のすべてのユーザに適用されます。

使用可能な認証方法は以下のとおりです：

- ・ パスワード または生体認証
- ・ パスワード および生体認証
- ・ パスワード のみ
- ・ 生体認証のみ

注意：生体認証だけを使用すると、FIPS 承認モードの動作と見なされません。生体認証を使用するデバイスの場合は、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。

使用可能なデバイス ポリシーは以下のとおりです：

- ・ 最大ユーザ数（管理者アカウントを除く、最大 10 人までのユーザを作成できます）。
- ・ 生体認証のセキュリティ レベル
- ・ 生体認証の再試行制限回数
- ・ パスワードの再試行制限回数
- ・ データ破棄 - ユーザ アカウント がブロックされる場合に行う 動作
- ・ パスワード ポリシー
- ・ デバイス管理コード
- ・ 管理者アカウントを無効にする機能

デバイス ポリシー設定の詳細については、21 ページの「デバイス ポリシーの設定」を参照してください。

注意：管理者アカウントが無効になるように選択すると、デバイス上で 1 人のユーザしか作成できません。後で管理者アカウントを作成することはできません。管理者アカウントがない場合、管理機能を実行する機能も禁止されます。例えば、ユーザがデバイスに認証できなくなった場合、ユーザをレスキューすることも、デバイスをリサイクルすることもできなくなります。

2. 管理者アカウントの作成

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。パスワードがないと、一部のデバイス設定を変更できなくなります。

管理者の詳細については、14 ページの「ユーザの種類」を参照してください。

3. 最初のユーザの作成

管理者パスワードを設定した後（該当する場合）、ユーザを作成して、指の登録、パスワードの作成、またはその両方による認証の資格情報を指定することを促すメッセージが自動的に表示されます。認証方法は、使用されるデバイスおよびプロフィールによって異なります。ユーザの作成の詳細については、14 ページの「ユーザの作成」を参照してください。

注意：この時点でユーザを作成しない場合、デバイスは入力済みのカスタマイズ情報（管理者パスワードを含む）を保存します。次にデバイスを差し込んだときに、ユーザ作成のタスクを完了させる必要があります。

LED の状態

すべての Imation デバイスは、デバイスの動作状態を示すために 1 つ以上の発光ダイオード（LED）を使用します。LED の状態は、使用しているデバイスによって異なります。

表 2: デバイスの LED の状態

状態	状態の説明
緑色の点灯	<p>オープンな状態：デバイスがカスタマイズされていません。また、認証メカニズムが設定されています。</p> <p>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。</p>
緑色の点滅	<p>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。</p> <ul style="list-style-type: none"> ・ 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。 ・ ソフトウェアが生体認証または登録操作を開始した。 ・ 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。
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。使用する必要がある認証方法は、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。読み取り専用モードでプライベートパーティションの内容を表示する場合は、[マルウェア耐性モードを使用] チェックボックスをオンにします。

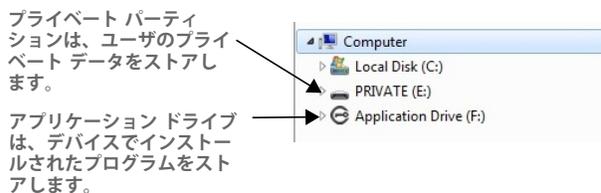
ヒント：生体認証だけを使用するデバイスの場合は、指紋センサーに指をスワイプすることで、ACCESS Standard を起動することなくデバイスにログインできます。

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。

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データを保存したり削除することはできません。

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。

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。

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：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、デバイスが破損し、使用不可能な状態になる可能性があります。

ユーザの管理

管理者は、ユーザを作成および削除したり、デバイスへ認証できなくなったユーザをレスキューすることができます。ユーザは、指を登録または削除、パスワードを変更、またはその両方を行うことで、自分の認証方法を管理することができます。

この章では、以下のトピックについて説明します：

- ・ ユーザの種類
- ・ ユーザの作成
- ・ ユーザの削除
- ・ 認証方法の管理
- ・ ユーザのレスキュー
- ・ ユーザ情報の表示

ユーザの種類

Imation デバイスは、デバイスに以下の 2 種類のユーザを登録できます：

- ・ **管理者**：このアカウントは、デバイスのカスタマイズ手順で管理者パスワードを入力すると自動的に作成されます。管理者アカウントだけがユーザを管理できます。管理者はデバイスへログインしません。代わりに、ユーザの追加または削除、およびユーザのレスキューなど、管理者権限を必要とするタスクをユーザが実行しようとした時、ACCESS Standard は管理者パスワードの入力をユーザに促すメッセージを自動的に表示します。

注意：管理者アカウントが無効となっているカスタム プロファイルを使ってデバイスがカスタマイズされている場合は、管理機能を実行できません。詳細については、21 ページの「デバイス ポリシー設定付録」を参照してください。

- ・ **一般ユーザ**：デバイスに認証したり、プライベートパーティションにデータを保存できる一般的なデバイスユーザです。ユーザは、自分のパスワードを変更したり、指登録を更新することができます。

ユーザの作成

管理者だけがユーザを作成することができます。最初のデバイスユーザは通常、管理者パスワードが設定された後、デバイスのカスタマイズプロセス中に作成されます。デバイスプロファイルが複数のユーザをサポートする場合、管理者はデバイスのカスタマイズ中または後に、続けてユーザを作成することができます。最大 10 人までのユーザと 1 人の管理者を追加できます。

ユーザの作成では、ユーザ名を作成したり、ユーザが認証の詳細（指の登録、パスワードの入力、またはその両方）を指定します。生体認証デバイスにユーザを追加する場合、最大 10 個の指紋テンプレートをすべてのユーザに対して登録できます。各ユーザは、少なくとも 1 つの指紋を登録する必要があります。生体認証のみを使用する場合、またはデータ破壊が有効な場合、最低 2 つの指紋が必要です。

ユーザを作成するには

1. ACCESS Standard のメイン ページで、[ユーザ管理] の下にある [ユーザの作成] をクリックします。
2. 管理者パスワードを求められた場合は、[パスワード] ボックスにパスワードを入力します。
3. ユーザおよび認証の資格情報を追加するには、[ユーザの作成] ページの指示に最後まで従います。

ユーザの削除

管理者だけがデバイスからユーザを削除できます。ユーザを削除すると、キー回復システムが存在する場合でも、ユーザのデータが完全に失われます。

ユーザを削除するには

1. ACCESS Standard のメイン ページで、[ユーザ管理] の下にある [ユーザの削除] をクリックします。
2. 管理者パスワードを求められた場合は、[パスワード] ボックスにパスワードを入力します。
3. ユーザを削除するには、その後続く ページの指示に最後まで従います。

認証方法の管理

ユーザが指登録の更新やパスワードの変更など、自分の認証の詳細を更新するには、まずデバイスに認証する必要があります。管理者は、一度設定された管理者パスワードを変更することはできません。

デバイスまたはユーザ アカウントに対して許可されている登録された指の総数に達すると、指をそれ以上登録することはできません。

指登録を更新するには

1. ACCESS Standard のメイン ページで、[ユーザ管理] の下にある [認証方法の管理] をクリックします。
生体認証だけを使用する場合は、ステップ 2 に進みます。
 2. [指登録を管理] をクリックします。指示に従って、指を登録または指登録を更新します。
許可されている指の最大本数を登録済みの場合、指登録を更新前に指紋を削除する必要があります。
- 注意：生体認証デバイスは、登録ごとに 5 本の指を個別にスワイプするようユーザに要求する場合があります。

パスワードを変更するには

1. ACCESS Standard のメイン ページで、[ユーザ管理] の下にある [認証方法の管理] をクリックします。
パスワード認証だけを使用する場合は、ステップ 2 に進みます。
2. [パスワードを管理] をクリックして、その後続く ページの指示に最後まで従って新しいパスワードを設定します。
2 要素認証を使用している場合は、[パスワードの設定] ページを開く前に、生体認証を使用して認証するようデバイスが要求します。

ユーザのレスキュー

ユーザをレスキューすると、指登録の削除、パスワードのリセット、またはその両方により、ユーザの認証方法がリセットされます。その後、ユーザは指を登録し、必要に応じてパスワードを設定することができます。詳細については、15 ページの「認証方法の管理」を参照してください。

ユーザがデバイスに認証できなくなった場合、管理者アカウントだけがユーザをレスキューできます。例えば、デバイスに許可されている認証試行回数を超えたか、または自分のパスワードを忘れた場合、そのユーザは認証できなくなる可能性があります。

ユーザをレスキューするには

1. ACCESS Standard のメイン ページで、[ユーザ管理]の下にある[ユーザのレスキュー]をクリックします。
2. [パスワード]ボックスに管理者パスワードを入力して、[次へ]をクリックします。
3. デバイス上に複数のユーザがいる場合、デバイスへ認証できないユーザを[ユーザ名]リストから選択して、[次へ]をクリックします。
4. 新しい認証情報を追加するには、その後続くページの指示に最後まで従います。

ユーザ情報の表示

許可されている指登録の数、パスワードおよび2要素の状態、プライベートパーティションのサイズなど、認証およびパーティションの詳細を含むデバイスユーザに関する情報を表示することができます。すべての情報は読み取り専用です。

ユーザ情報を表示するには

- ACCESS Standard のメイン ページで、[ユーザ管理]の下にある[ユーザ]をクリックします。

デバイスの管理

デバイス ソフトウェアの言語を設定したり、デバイスの構成、パーティション、およびバージョン情報を確認するためのデバイス情報を表示することができます。デバイスをリサイクルすると、デバイスからすべてのユーザおよびデータが削除されます。

この章では、以下のトピックについて説明します。

- ・ 言語の選択
- ・ デバイス情報の表示
- ・ デバイスのリサイクル

言語の選択

ACCESS Standard で使用する言語を選択することができます。

言語を選択するには

1. ACCESS Standard のメイン ページで、[言語の選択] をクリックします。
2. リスト から使用する言語をクリックします。

デバイス情報の表示

デバイスに関する情報を参照できます。すべての情報は読み取り専用です。

デバイス情報を表示するには

1. ACCESS Standard のメイン ページで、[ハードウェアおよびソフトウェア情報] をクリックします。
2. 以下のカテゴリのいずれか 1 つをクリックします：
 - ・ デバイス設定：再試行制限回数、セキュリティ レベル、デバイスのシリアル番号などの生体認証およびハードウェア情報が含まれています。
 - ・ ディスク パーティション：デバイスでのディスク領域の全体的な割り当てを示します。
 - ・ 製品バージョン：デバイスに関連付けられているすべてのソフトウェアおよびハードウェアのバージョンをリストします。

デバイスのリサイクル

デバイスをリサイクルすると、すべてのユーザおよび認証メカニズムが削除され、デバイスがデフォルトの状態に戻ります。データおよびセキュリティ キーはすべて回復不可能です。デバイスの管理コードを知る管理者およびユーザであれば、デバイスをリサイクルできます。デバイス プロファイルを再適用およびユーザを再作成するには、リサイクルされたデバイスをカスタマイズする必要があります。詳細については、9 ページの「デバイスをカスタマイズするには」を参照してください。

デバイスをリサイクルするには

1. ACCESS Standard のメイン ページで、[デバイスのリサイクル] をクリックします。
2. [デバイスのリサイクル] ページにある警告を読んでから、[管理コード] ボックスに管理コードを入力します。

3. [次へ]をクリックします。

ACCESS Standard は自動的にデバイスをリサイクルします。

ウィルスからのデバイスの保護

ACCESS Antivirus Scanner™ がライセンス済みの場合、デバイス上のデータの保護を強化できます。スキャナはホスト コンピュータおよびデバイスのプライベート パーティション上のウィルスを検索します。また、スキャナが確実に新しいウィルスの内容を確認できるように、ウィルス データベースを更新することもできます。侵入ログでは、発生するすべてのスキャン イベントを追跡できます。

この章では、以下の情報について説明します：

- ・ デバイスおよびホスト コンピュータのスキャン
- ・ ウィルス データベースの更新
- ・ ACCESS Antivirus Scanner イベント の記録

デバイスおよびホスト コンピュータのスキャン

デバイスへアクセスするたびにプライベート パーティションおよびホスト コンピュータを定期的にもスキャンしたり、必要に応じて手動でスキャンするように ACCESS Antivirus Scanner を設定できます。

プライベート パーティションをスキャンするには

1. タスクバーの右端にある通知領域で IronKey アイコンをクリックしてから、[Antivirus Scanner の管理] をクリックします。
2. [プライベート パーティション] 領域で、以下の操作のいずれかを実行します：
 - ・ デバイスへアクセスするたびにスキャナでプライベート パーティションをチェックするには、[オンアクセス スキャン] チェックボックスをクリックします。
 - ・ プライベート パーティションをすぐにスキャンするには、[スキャン] をクリックします。

ホスト コンピュータをスキャンするには

1. タスクバーの右端にある通知領域で IronKey アイコンをクリックしてから、[Antivirus Scanner の管理] をクリックします。
2. [ホスト システム] 領域で、以下の操作のいずれかを実行します：
 - ・ デバイスを差し込むたびにスキャナでホスト コンピュータをチェックするには、[起動時にホスト システムをスキャン] チェックボックスをクリックします。
 - ・ ホスト コンピュータをすぐにスキャンするには、[スキャン] をクリックします。

ウィルス データベースの更新

更新が入手可能になったときに、ウィルス定義ファイルを自動的に更新できます。ログインするたびに、必要に応じてスキャナがデバイスを更新します。また、必要に応じてデータベースを手動で更新することもできます。

ウィルス データベースを更新するには

1. タスクバーの右端にある通知領域で IronKey アイコンをクリックしてから、[Antivirus Scanner の管理] をクリックします。

2. [ウイルス データベース] 領域で、以下の操作のいずれかを実行します：

- ・ ウィルス定義ファイルを自動的に更新するには、[自動更新] チェックボックスをクリックします。
- ・ 強制的にファイルを更新するには、[更新] をクリックします。

ACCESS ANTIVIRUS SCANNER イベントの記録

有効な場合、ACCESS Antivirus Scanner はすべてのスキャン イベントのログを記録します。

侵入ログを有効にするには

1. タスクバーの右端にある通知領域で IronKey アイコンをクリックしてから、[Antivirus Scanner の管理] をクリックします。
2. [侵入ログ] 領域で、[有効] チェックボックスをクリックします。

ログファイルを表示するには

1. タスクバーの右端にある通知領域で IronKey アイコンをクリックしてから、[Antivirus Scanner の管理] をクリックします。
2. [侵入ログ] 領域で、[表示] をクリックします。

ヒント：侵入ログからすべての項目を削除するには、[消去] をクリックします。

トラブルシューティング

デバイスの使用中に問題が発生した場合、以下のシナリオのいずれかで解決する可能性があります。技術的な詳細については、Imation.com/support にお問い合わせください。

デバイスを取り出せない

ファイルマネージャからデバイスを取り出そうとすると、以下のエラーが発生する場合があります：

「ボリュームを取り出せません - 「リムーバブルディスク (F:)」を取り出そうとしてエラーが発生しました。開いているファイルまたはそのボリュームからのウィンドウが存在しないことを確認してください。」

コンピュータの管理者ではない場合、このメッセージが常に表示され、ドライブを取り出すことはできません。これは、以下の技術情報で Microsoft によって文書化されている制限事項です：

<http://support.microsoft.com/default.aspx?scid=kb;en-us;192785>。

ログアウト、ACCESS Standard を使用したデバイスの取り出し、またはタスクバーアイコンを使用したデバイスの安全な取り外し（13 ページの「デバイスの接続の取り外し」を参照）によって、この問題を解決できます。

生体認証デバイスが指を認証しない

生体認証センサーが破損、または指紋が期限切れか環境要因や怪我が原因で変化している場合、デバイスは指の認証に失敗する場合があります。予備の指登録がある場合、別の指を登録したり、既存の指紋を削除して新しい指紋を登録することができます。詳細については、15 ページの「認証方法の管理」を参照してください。センサーが壊れている場合は、管理者または Imation にお問い合わせください。

デバイスへのパスワードまたは生体認証アクセスがブロックされる

再試行制限回数に到達する前に、パスワードまたは生体認証による試行回数が 1 回しか残っていない場合、警告メッセージが表示されます。再試行制限回数を超えると、デバイスはその認証方法を使ったデバイスへのユーザの認証をブロックします。ユーザアカウントをブロック解除するには、管理者に問い合わせる必要があります。詳細については、15 ページの「ユーザのレスキュー」を参照してください。

デバイスのドライブ マッピングが表示されない

Imation デバイスのパーティションにドライブ文字がマッピングされないことがあります。この問題は、ネットワークドライブのマッピングが、ACCESS Standard のドライブの 1 つに通常割り当てられる文字を占有している場合に発生します。

ACCESS Standard に通常割り当てられるドライブ文字を使用してリソースにネットワークドライブをマッピングすると、デバイスの接続時にファイル マネージャ ウィンドウにデバイスのドライブが表示されなくなります。この問題は、デバイスがコンピュータから切断されている間にドライブをマッピングする場合のみ発生します。マッピングされたネットワークドライブを切断する必要があります。マッピングの問題を解決するには、例えば Z や Y など、アルファベットの終わりからドライブ文字を使用して、ネットワークドライブを再マッピングすることをお勧めします。この Microsoft のネットワークドライブの問題について詳しくは、以下の Microsoft の Web アドレスにアクセスしてください:

<http://support.microsoft.com/?kbid=830238>

アプリケーションパーティションに保存されたデータを使用できない

デバイスの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。プライベートパーティションにのみデータを保存してください。

デバイス ポリシー設定付録

「カスタム」カスタマイズ プロセス中に、デバイス ユーザの数、生体認証のセキュリティ レベル、パスワード ポリシーなどのデバイス ポリシー設定を構成することができます。使用可能なポリシー設定は、デバイスが使用する認証の種類に応じて異なります。デバイスのカスタマイズの詳細については 9 ページの「デバイスをカスタマイズするには」、デフォルトのデバイス設定のリストを表示するには 9 ページの「1. デバイス プロファイルの選択および適用」を参照してください。

各ポリシー設定およびこれらのオプションが適用されるデバイスを以下の表に示します。パスワード ポリシーの詳細については、23 ページの表 4 を参照してください。

表 3: デバイス ポリシーの設定

ポリシー設定	説明	適用可能なデバイス
認証の種類	<ul style="list-style-type: none"> パスワード または 生体認証 パスワード および 生体認証 パスワード のみ 生体認証のみ <p>* 生体認証のみを使用することは、操作の FIPS 承認モードを考慮していないことに注意してください。生体認証を使用するデバイスの場合は、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。</p> <p>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。</p>	<p>生体認証 / パスワードのオプション:</p> <ul style="list-style-type: none"> IronKey™ F200 IronKey™ H200 MXI Stealth™ MXP (GenI) <p>パスワード:</p> <ul style="list-style-type: none"> IronKey™ H100 & IronKey™ H80 IronKey™ F100 IronKey™ F150 MXI Stealth™ Key M200 MXI Stealth MXP MXI Gen I Stealth MXP® Passport MXI Outbacker MXP® (GenI)
最大ユーザ数	<p>デバイスへ追加できるユーザの総数 (最大 10 人)。この数に管理者アカウントは含まれません。</p>	<ul style="list-style-type: none"> すべてのデバイス

表 3: デバイス ポリシーの設定

ポリシー設定	説明	適用可能なデバイス
生体認証のセキュリティ レベル	<p>すべてのデバイス ユーザに適用されます。「10,000 分の 1」など、誤合致率 (FMR) として表されます。FMR とは、異なる指が間違っ て一致したとされる確率のことです。</p> <p>デバイスでは 2 つの指紋間でより高い一致率を必要とするため、低い FMR はセキュリティが高いことを表します。従って、「10,000 分の 1」は「1,000 分の 1」よりも安全です。</p> <p>ただし、低 FMR は、センサーがゴミ や指を適切に配置しないなど、小さい指紋の誤差を許容しないために、デバイスが正しいユーザを拒否する可能性があることも意味します。反対に、高 FMR は、デバイスが正しいユーザを拒否することは少ないが、2 つの異なる指紋を誤って一致させる可能性が高いことを意味します。ユーザが任意のセキュリティ レベルでうまく デバイスに認証できない場合は、ユーザにパスワードも割り 当てておくことをお勧めします。</p>	<ul style="list-style-type: none"> • IronKey™ F200 • IronKey™ H200 • MXI Stealth™ MXP (GenI)
生体認証の再試行制限回数	<p>再試行制限回数に達したら、生体認証がブロックされたユーザのみが生体認証を使用したデバイスへのアクセスが拒否されます。パスワード 認証は使用できます。例えば、再試行制限回数 1 の場合は、ユーザが 2 回認証に失敗したらブロックされます。再試行制限回数は、1 ~ 254 回、または無限に設定できます。</p> <p>生体認証エラーは、常にユーザの違反であるとは限らないため、生体認証の再試行制限回数を、パスワード の再試行制限回数よりも多く 設定することをお勧めします。ユーザがデータベースへの認証試行中に再試行制限回数を越えた場合、次の動作が起こります。</p> <p>注意: 生体認証誤拒否（登録された指を使用しても本物のユーザが認証試行中に検証されない）は、どの生体認証システムで発生する可能性があります。誤拒否率は、生体認証セキュリティ レベルが高くなると上がります。したがって、高い生体認証再試行制限回数を設定して誤拒否による生体認証ユーザのデバイスへのアクセスをブロックする可能性を最小限にすることをお勧めします。低い再試行制限回数を設定すると、特に低誤合致率 (FMR) が生体認証セキュリティ レベルに設定されている場合にはアクセスがブロックされる可能性が高くなります。「生体認証のセキュリティ レベル」も参照してください。</p>	<ul style="list-style-type: none"> • IronKey™ F200 • IronKey™ H200 • MXI Stealth™ MXP (GenI)
パスワードの再試行制限回数	<p>23 ページの表 4 を参照してください。</p>	
デバイス管理コード	<p>デバイスのリサイクルなど、デバイスの管理プロセスを実行するには、管理コード が必要です。</p>	<ul style="list-style-type: none"> • すべてのデバイス

表 3: デバイス ポリシーの設定

ポリシー設定	説明	適用可能なデバイス
データ 破棄	この設定は、ユーザ アカウント がブロックされる場合に行う動作を決定します。 [データ 破棄] をオンにすると、ユーザがデバイスに認証できなくなった場合に、データを回復したりデバイスをレスキューすることができません。 管理者アカウント が無効な場合、[データ 破棄] は自動的にオンになります。	・ すべてのデバイス
管理者のアカウントの無効化	デバイスをカスタマイズする時は、管理者アカウントを含めません。ただし、管理者アカウント なしでは、ユーザをレスキューしたり他の管理機能を実行することができません。また、1 人のデバイス ユーザしか作成することができません。	・ すべてのデバイス

パスワード ポリシー

パスワード の設定時にユーザが守らなければならない規則の複雑性を変更することで、パスワード の強度を高めることができます。複雑なパスワード 規則は、承認されていないユーザがパスワード 違反をしてデバイスにアクセスする可能性を低くすることによってセキュリティを向上します。次の表は、ACCESS Standard で利用可能なパスワード 規則を説明しています。

表 4: パスワード ポリシー

規則	定義
パスワード の再試行制限回数	ユーザがデバイスへのログインをブロックされるまでに許可された、パスワード 認証試行の失敗回数です。例えば、再試行制限回数 1 の場合は、ユーザが 2 回認証に失敗したらブロックされます。パスワード がブロックされたユーザだけが、デバイスへのログインにパスワード を使えません。ただし、生体認証の再試行制限回数を超えていない場合は、生体認証を使用できます（該当する場合）。再試行制限回数は、1 ~ 254 回、または無限に設定できます。
最小パスワード 長	パスワード に含めること有効文字 (4 ~ 40) の最低文字数。
最小特殊文字数	パスワード に含める必要がある特殊文字 (0 ~ 15) の最低文字数。有効な文字は次のとおりです: ~ ! @ # \$ % ^ * () _ - + = { } [] \ : ' " , . / ? & ; < > .
最小数字数	パスワード に必要な最小数字数 (0 ~ 15、例えば 1234567890)。
最小英字数	パスワード に含める必要がある英字 (0 ~ 15) の最低文字数 (大文字と小文字を含む)。
最小大文字数	パスワード に含める必要がある大文字 (0 ~ 15) の最低文字数。
最小小文字数	パスワード に含める必要がある小文字 (0 ~ 15) の最低文字数。
再使用しきい値	以前のパスワード を再使用できるようになるまでに、ユーザが設定する必要がある別のパスワード の最小数 (0 ~ 15)。

表 4: パスワード ポリシー

規則	定義
最小ライフタイム（分）	新しく変更されたパスワードを再び変更できるようになるまでに、ユーザが待機する必要がある最小分数（0 ～ 120）。この規則は、ユーザがパスワードを変更してからすぐに元のパスワードに戻して新しいパスワードの使用を避けることを防ぎます。
最大ライフタイム（日）	新しく変更されたパスワードの有効最大日数（1 ～ 1000 または無限）。ユーザは最大ライフタイムが期限切れになったらパスワードを変更する必要があります。

インデックス

数字

2 要素のプロファイル 9

A

antivirus scanner
コンピュータのスキャン 19
データベースの更新 19
デバイスのスキャン 19
ログファイルの表示 20

L

LED
赤色の点滅 11
緑色の点灯 11
緑色の点滅 11
青色 11
赤色の点灯 11
緑色の遅い点滅 11
緑色の通常の点滅 11

あ

アプリケーション パーティション
デバイス 22
一般ユーザ 14
ウィルス データベース
更新 19
エラー
ボリュームを取り出せません 21

か

管理コード 9
管理者
アカウントの無効化 14
管理者特権 14
管理者の作成 10
危険な取り出しイベントのダイアログ 21
技術サポート ii
言語
applicationsetting の設定
言語 17
更新
ウィルス データベース 19
誤拒否率
生体認証 24

さ

再試行制限回数
パスワード用の設定 25
削除
デバイス 12
ユーザ 15
作成
新しいパスワード 15
ユーザ 14
サポート
技術アシスタンス ii
侵入ログ
概要 20
スキャナ
イベントの記録 20
ウィルス データベースの更新 19
スキャン
ウィルスについてデバイスを 19
ホスト コンピュータを 19
生体認証
誤拒否 24
登録 15
生体認証のプロファイル 9
設定
パスワードの再試行制限回数 25
ソフトウェア バージョン 17

た

追加
最初のユーザ 11
ユーザ 14
指 15
データ 破棄 25
デバイス
アプリケーション パーティション 22
カスタマイズ手順
デフォルト 設定 9
プロフィールについて 9
ユーザの追加 14
ユーザのレスキュー 15
リサイクル 17
デバイスのカスタマイズ
デバイスの初期化
カスタマイズを参照
デバイスの切断 12
デバイスの取り出し
トラブルシューティング 21
デバイスの取り外し 12

- デバイスのリサイクル 17
- デバイスのログアウト 12
- デバイスのロック解除 12
- デバイスへのログイン 12
- デフォルト
 - デバイス設定 9
 - プロファイル設定 9
- 問い合わせ先
 - Imation ii
- 登録の特権 14
- トラブルシューティング
 - 危険な取り出しイベントのダイアログ 21
 - 失敗した指認証 21
 - デバイスの取り出し 21
 - デバイスへのブロックされたアクセス 21
 - ネットワークドライブの問題 21
 - 表示されないデータ 22
 - ブロックされたパスワード アクセス 21

な

- 認証方法 15
- ネットワークドライブ
 - マッピング 21
- ネットワークドライブのマッピング 21

は

- ハードウェアの安全な取り外し操作 12
- ハードウェアバージョン 17
- バージョン番号 17
- パーティション
 - アプリケーション 22
 - サイズの表示 17
 - ファイルの保存 13
 - ファイルを開く 13
- パスワード
 - 管理者 10
 - 再試行制限回数 25
 - 再試行制限回数について 25
 - 変更 15
- パスワードのプロファイル 9
- パスワードの変更 15
- 表示
 - デバイス構成 17
 - バージョン情報 17
 - パーティション情報 17
 - ユーザ情報 17
- 表示されないデータ
 - トラブルシューティング 22
- ファイルの保存 13
- ファイルを開く 13
- ブロックされた生体認証アクセス 21
- ブロックされる
 - 生体認証またはパスワード アクセス 21
- プライベートパーティションのサイズ 9
- プロファイル
 - 概要 9
- 編集
 - パスワード 15

ま

- マルウェア耐性モード 12
- 緑色の LED 11

や

- ユーザ
 - 一般 14
 - 数の表示 17
 - 管理者 14
 - 救出 15
 - 最初に追加 11
 - 削除 15
 - 追加 14
 - 定義 14
 - 認証方法の変更 15
- ユーザのレスキュー 15
- 指
 - 登録 15
- 指の登録 15
- 読み取り専用モード 12

ら

- リセット
 - ユーザの認証方法 15
- ログファイル
 - antivirus scanner の 20

ん

- 青色の LED 11
- 赤色の LED 11