Dell Data Protection | Access ホーム

Dell Data Protection | Access ホーム
ページは、このアプリケーションから各種機能を利用するための出発地点です。このウィンドウから、次の機能にアクセスすることができます。

System Access Wizard
アクセス オプション (Access Options)
Self-Encrypting Drive
詳細設定オプション (Advanced Options)

ウィンドウの右下隅には、クリックして詳細設定オプションにアクセスするための **[詳細設定]**リンクが存在しています。

詳細設定オプションからは、ウィンドウの右下にある **[ホーム]** リンクをクリックしてホームページに戻ることができます。

System Access Wizard

Dell Data Protection | Access アプリケーションを初めて起動した場合、System Access Wizard が自動的に起動されます。このウィザードは、システムへのログイン時期 (例:Windows、Pre-Windows、または両方) やログイン方法 (例:パスワードのみ、または指紋とパスワード) などを含め、システムの各種セキュリティの設定方法を案内するものです。また、システムに Self-Encrypting Drive が存在する場合は、それもこのウィザードで設定することができます。

管理者機能

システムに対する Windows 管理者権限を持つユーザは、**Dell Data Protection | Access**に関する次の機能を実行することができます。標準のユーザは、これらの機能を利用できません。

- システム (Pre-Windows) パスワードの設定／変更
- ハード ドライブ パスワードの設定／変更
- 管理者パスワードの設定／変更
- TPM 所有者パスワードの設定／変更
- ControlVault 管理者パスワードの設定／変更
- システムのリセット
- 資格情報のアーカイブと復元
- スマート カード管理者 PIN の設定／変更
- スマート カードの消去／リセット
- Windows への Dell セキュア ログインの有効化／無効化
- Windows ログイン ポリシーの設定
- 次のような自己暗号化ドライブの管理:
    - 自己暗号化ドライブのロックの有効化／無効化
    - WPS (Windows Password Synchronization) の有効化／無効化
    - Single Sign On (SSO) の有効化／無効化
    - 暗号的消去の実行

リモート管理

複数プラットフォーム上の **Dell Data Protection | Access** アプリケーションの機能を集中管理 (リモート管理) するように、環境を設定することができます。この場合、Active Directory などの Windows セキュリティ インフラを使って、**Dell Data Protection | Access** の特定の機能を安全に管理することができます。

コンピュータをリモート管理する場合 (例:リモート管理者が「所有」する)、**Dell Data Protection | Access** のローカル管理機能は無効になります。アプリケーションの管理ウィンドウにローカルからアクセスすることはできません。次の機能を、リモート管理することができます。

- Trusted Platform Module (TPM)
- ControlVault
- Pre-Windows ログイン
- システムのリセット
- BIOS パスワード
- Windows ログイン ポリシー
- Self-Encrypting Drive
- 指紋およびスマート カードの登録

リモート管理に Wave Systems 社の EMBASSY® Remote Administration Server (ERAS) を使用するための詳細情報については、Dell の営業担当者に問い合わせるか、または dell.com を参照してください。

アクセス オプション

[Access Options (アクセス オプション)]
ウィンドウでは、システムへのアクセス方法を設定することができます。

何らかの**Dell Data Protection | Access** のオプションを設定している場合、ホーム
ページにはそれらの利用可能なオプションが表示されます (例:Pre-Windows
ログイン用パスワードの変更)。この利用可能なオプションはショートカットです。このショー
トカットをクリックすると、その作業を行うためのウィンドウに移動します (例:Pre-Windows
パスワードの変更や他の指紋の登録など)。

全般
まず、ログイン時期 (Windows、Pre-Windows、または両方) やログイン方法
(例:指紋とパスワード) を指定できます。ログイン方法では 1 つまたは 2
つのオプションを選択することができます。たとえば、指紋、Smartcard、パスワードなどを組
み合わせて選択することができます。記載されるオプションは、お客様の環境に適用されている
ログイン ポリシーと、そのプラットフォームでのサポート内容に基づきます。

指紋
お使いのシステムに指紋リーダーがある場合は、指紋を登録または更新してシステムへのログイ
ンに使用することができます。指紋を登録したら、Windows、Pre-
Windows、または両方の時点でシステムの指紋リーダーに指紋を登録した指をスライドすること
で、システムにアクセスできるようになります (［全般アクセス
オプション］の設定内容による)。詳細は、「ユーザ指紋の登録」を参照してください。

Pre-Windows ログイン
Pre-Windows 時にユーザにログインを要求するように指定する場合、Pre-Windows
アクセス用にシステム パスワード (Pre-Windows パスワードと呼ばれることもある)
を設定する必要があります。いったんこれを設定したら、管理者はいつでもパスワードを変更す
ることができます。

また、この画面から Pre-Windows
ログインを無効にすることもできます。その場合は、現在のシステム
パスワードを入力し、そのパスワードが正しいことを確認してから [**無効**]
ボタンをクリックします。

スマート カード
ログイン時に Smartcard を使用させる場合は、従来の (接触型) または非接触型スマート
カードを登録する必要があります (複数登録できます)。［**他のスマート
カードの登録**］リンクをクリックして、スマート
カード登録ウィザードを起動してください。登録することは、ログインにスマート
カードを使用するように設定することを意味しています。

スマート カードを登録したら、[**スマート カード PIN の変更または設定**]
リンクを使ってそのカードの PIN を設定または変更することができます。

Pre-Windows ログイン

Pre-Windows ログインを設定すると、システムの電源を入れた後 Windows がロードされる前の時点で、認証 (パスワード、指紋、またはスマート カード) を行う必要があります。Pre-Windows ログイン機能はシステムに新たなセキュリティ手段を追加し、不正なユーザによる Windows の悪用やコンピュータへの不正アクセスを防止します (例:コンピュータ盗難の場合など)。

Pre-Windows ログイン ウィンドウでは、Pre-Windows ログインを設定したり、Pre-Windows (システム) パスワードを作成、変更することができます。また、Pre-Windows パスワードがすでに設定されている場合に、Pre-Windows ログインを無効にすることもできます。Pre-Windows ログインの設定時には、ウィザードが起動します。ウィザードでは、以下の作業を行います。

- システム パスワード:Pre-Windows アクセス用のシステム パスワード (Pre-Windows パスワードと呼ばれることもあります) を設定します。このパスワードは、ユーザが他の認証手段を利用している場合の、バックアップ手段として使用されることもあります (例:指紋センサーに問題が発生した時に、システムにアクセスするために使用)。
- 指紋またはスマート カード:Pre-Windows ログインで使用する指紋またはスマート カードを設定し、この認証手段を Pre-Windows パスワードの代わりに使用するのか、または Pre-Windows パスワードと併用するのかを指定します。
- Single Sign On:デフォルトでは、Pre-Windows 認証 (パスワード、指紋、またはスマート カード) により、Windows にも自動的にサイン インされます (Single Sign On)。この機能を無効にするには、[I want to login again at Windows (後で Windows にログインする)] チェック ボックスを選択します。
- Pre-Windows パスワードに加えて BIOS の ハード ドライブのパスワード設定されている場合、ハード ドライブのパスワードを変更したり、無効にすることもできます。

注意: Pre-Windows 認証に利用できない指紋リーダーもあります。互換性のないリーダーをご利用の場合、Windows ログイン用の指紋しか登録できません。指紋リーダーの互換性については、システム管理者に問い合わせるか、または support.dell.com でサポートする指紋リーダーの一覧をご確認ください。

Pre-Windows ログインを無効にする

このウィンドウから Pre-Windows ログインを無効にすることもできます。その場合は、現在の Pre-Windows (システム) パスワードを入力し、そのパスワードが正しいことを確認してから [無効] ボタンをクリックします。Pre-Windows ログインを無効にしても、登録している指紋やスマート カードはそのまま登録されていることに注意してください。

指紋の登録と削除

Windows ログインや Pre-Windows
ログイン時のシステム認証に、指紋を利用することができます。ユーザは、そのような目的で指紋を登録、更新することができます。[指紋]
タブで、指紋が登録されている場合は、どの指の指紋が登録されているかを示す手の画像が表示されます。**[他を登録]**
リンクをクリックすると、指紋の登録ウィザードが起動します。このウィザードが、登録のプロセスを案内します。「登録」とは、ログイン用に使用する指紋を保存することを意味しています。指紋を登録するには、有効な指紋リーダーを正しくインストールし、設定しておく必要があります。

注意: Pre-Windows ログインに利用できない指紋リーダーもあります。互換性のないリーダーで Pre-Windows ログイン用の指紋を登録しようとすると、エラー
メッセージが表示されます。デバイスの互換性については、システム管理者に問い合わせるか、または support.dell.com でサポートする指紋リーダーの一覧をご確認ください。

指紋の登録時には、正しいユーザであることを検証するために Windows
パスワードの入力が要求されます。ポリシーの設定によっては、Pre-Windows (システム)
パスワードの入力も要求されます。指紋リーダーに何か問題が発生した場合は、Pre-Windows
パスワードを使ってシステムにアクセスできます。

メモ：

- 登録プロセスでは最低でも 2 つの指紋を登録することをお勧めします。
- 指紋認識機能を有効にする前に、指紋が適切に登録されていることを確認してください。

- システムの指紋リーダーを変更した場合は、新しい指紋リーダーで指紋を再登録する必要があります。2
  つの異なる指紋デバイスを交互に切り替えながら使用することはお勧めできません。
- 指紋の登録時に「センサーはフォーカスを失いました」のようなメッセージが繰り返し表示される場合は、コンピュータが指紋リーダーを正しく認識していない可能性があります。外部指紋リーダーを使用している場合は、いったん指紋リーダーを取り外した後再接続することで、問題を解決できることもあります。

登録した指紋の消去
登録した指紋を削除するには、**[指紋の削除]**
リンクをクリックするか、または指紋登録ウィザードで登録した指紋の選択を解除します。

Pre-Windows
認証用に指紋を登録した特定ユーザの指紋を削除するには、管理者がそのユーザに対して登録されているすべての指紋を選択解除することができます。

注意:指紋登録プロセス時に何かエラーが発生した場合、wave.com/support/Dell
から他の参照情報や詳細を確認することができます。

スマート カードの登録

Dell Data Protection | Access では、従来型 (接触型) スマート カードや非接触型スマート カードを利用して、Windows アカウントへのログインや Pre-Windows 時の認証を行うことができます。 [スマート カード] タブで **[他のスマート カードを登録]** リンクをクリックすると、スマート カードの登録ウィザードが起動します。このウィザードが、登録のプロセスを案内します。登録することは、ログインにスマート カードを使用するように設定することを意味しています。

登録するには、有効なスマート カード認証デバイスを正しくインストールし、設定しておく必要があります。

注意:デバイスの互換性については、システム管理者に問い合わせるか、または support.dell.com でサポートするスマート カード リーダーの一覧をご確認ください。

登録

スマート カードの登録時には、正しいユーザであることを検証するために Windows パスワードの入力が要求されます。ポリシーの設定によっては、Pre-Windows (システム) パスワードの入力も要求されます。スマート カード リーダーに何か問題が発生した場合は、Pre-Windows パスワードを使ってシステムにアクセスできます。

登録時には、スマート カード PIN を要求するメッセージが表示されます (設定されている場合)。ポリシーで PIN が必要であると設定されているのに、まだ PIN が設定されていない場合は、PIN を作成するように要求するメッセージが表示されます。

注意:

- Pre-Windows で使用するスマート カードのユーザが登録されると、当該ユーザを削除することはできません。
- 標準のユーザはスマート カードのユーザ PIN を変更できます。管理者は、管理者 PIN とユーザ PIN の両方を変更することができます。
- 管理者はスマート カードをリセットすることもできます。リセットしたスマート カードは、再登録しない限り、Windows ログインや Pre-Windows の認証に使用することはできません。

注意:TPM 証明書認証の場合、管理者は Microsoft Windows スマート カード登録プロセスを通じて、TPM 証明書を登録することができます。このアプリケーションとの互換性を保つために、管理者は CSP (Cryptographic Service Provider.) として、Smartcard CSP の代わりに [Wave TCG-Enabled CSP] を選択する必要があります。また、クライアントの適切な認証タイプ ポリシーで、Dell セキュア ログインを有効にする必要があります。.

注意: Smartcard サービスが動作していない旨のエラー メッセージが表示された場合、以下の手順でサービスを開始／再開することができます。

- コントロール パネルの [管理ツール] ウィンドウから [サービス] を選択し、[Smartcard] を右クリックして [開始] または [再開] を選択します。
- 各エラー メッセージの詳細を知りたい場合は、wave.com/support/Dell を参照してください。

Self-Encrypting Drive の概要

Dell Data Protection | Access は、Self-Encrypting Drive のハードウェア ベースのセキュリティ機能を管理します。このドライブのハードウェアには、データ暗号化機能が組み込まれています。この機能は、権限のあるユーザのみが暗号データにアクセスできるようにする目的で用いられます (ドライブのロックが有効になっている場合)。

Self-Encrypting Drive ウィンドウにアクセスするには、下にある [**Self-Encrypting Drive**] タブをクリックします。このタブは、システムに 1 台以上の Self-Encrypting Drive (SED) が存在している場合にのみ表示されます。

[**設定**] リンクをクリックすると、Self-Encrypting Drive Setup Wizard が表示されます。このウィザードでは、ドライブ管理者 (Drive Administrator) のパスワードの作成、パスワードのバックアップの設定、ドライブ暗号化設定の適用を行います。Self-Encrypting Drive Setup Wizard は、システム管理者のみが利用できます。

重要: ドライブの設定が完了すると、データ保護とドライブのロックが有効になります。ドライブをロックすると、以下の処理が行われます。

- ドライブへの電源供給がオフになると、*ロック* モードに移行します。
- Pre-Windows ログイン画面で正しいユーザ名とパスワード (または指紋) を入力しない限り、ドライブが起動することはありません。ドライブ ロックが有効になる前は、コンピュータ上の任意のユーザがドライブ上のデータにアクセスすることができます。
- ドライブは、他のコンピュータにセカンダリ ドライブとして取り付けられた場合にも保護され、ドライブのデータにアクセスするには認証が必要になります。

ドライブの設定が完了すると、[Self-Encrypting Drive] ウィンドウに、ドライブおよびユーザが各自のドライブ パスワードを変更するためのリンクが表示されます。ドライブ管理者は、このウィンドウからドライブのユーザを追加、削除することもできます。設定されている外付けドライブがある場合は、それもこのウィンドウに表示され、ロックを解除することができます。

注意:セカンダリ
ドライブまたは外付けドライブをロックするには、ドライブの電源を個別にオフにする必要があります。

ドライブ管理者は、**[詳細設定] > [デバイス]** で、ドライブ設定を管理することができます。詳細は、「デバイス管理 - Self-Encrypting Drive」を参照してください。

ドライブの設定

Self-Encrypting Drive Setup Wizard は、ドライブの設定方法を案内します。この作業を行う際には、以下の概念を正しく把握しておいてください。

ドライブ管理者 (Drive Administrator)
システム管理者権限を持ち、最初にドライブ アクセス (およびドライブ管理者パスワード) を設定したユーザがドライブ管理者になります。ドライブ管理者のみが、ドライブ

アクセスの変更を行えます。最初のユーザがドライブ管理者になることを確認するために、この作業を続行するには [I understand (了解しました)] チェック
ボックスを選択する必要があります。

ドライブ管理者パスワード (Drive Administrator Password)
ウィザードは、ドライブ管理者のパスワード (Drive Administrator Password)
を作成し、パスワードの再入力を求めるメッセージを表示します。ドライブ管理者パスワードを作成するには、正しいユーザであることを確認するために Windows
パスワードを入力する必要があります。このパスワードを作成するユーザには、管理者権限が必要です。

ドライブ資格情報のバックアップ (Backup Drive Credentials)
ドライブ管理者資格情報のバックアップ
コピーを保存するために、バックアップ先を入力するか、隣にある [**Browse (参照)**]
ボタンをクリックしてバックアップ先を選択します。

重要**:**

- これらの資格情報を必ずバックアップすること、そしてプライマリ
  ハードディスク以外のドライブ (例:リムーバル メディア)
  にバックアップすることを強くお勧めします。そうしないと、ドライブへのアクセスを失った場合に、バックアップ データにアクセスできなくなってしまいます。
- ドライブの設定が完了したら、次回にシステムの電源を入れた時に、システムにアクセスするためには、Windows のロード前に正しいユーザ名とパスワード (または指紋)
  を入力する必要があります。

ドライブユーザの追加 (Add Drive User)
ドライブ管理者は、他の有効な Windows
ユーザをドライブに追加することができます。ドライブにユーザを追加する際には、ユーザの初回ログイン時に各自のパスワードをリセットさせるかどうかを指定することができます。Pre-Windows 認証画面でパスワードをリセットしないと、ドライブのロックは解除されません。

詳細設定 (Advanced Settings)

- *Single Sign On* - デフォルトでは、Pre-Windows
  時にドライブの認証を受けるために入力した Self-Encrypting Drive
  パスワードを使って、Windows へのサイン インが行われます (Single Sign On
  と呼ばれています)。この機能を無効にするには、ドライブ設定時に [I want to login again when Windows starts (Windows 起動時に再ログインする)] チェック
  ボックスを選択してください。
- *Fingerprint Login (指紋ログイン)* -
  対応しているプラットフォームでは、パスワードの代わりに指紋を使用して、Self-Encrypting Drive の認証を行うように指定することができます。
- *Sleep/Standby (S3) Support* (プラットフォームがサポートしている場合) -
  有効にすると、Self-Encrypting Drive は安全にスリープ／スタンバイ モード (S3
  モードとも呼ばれます) に移行できます。スリープ／スタンバイ
  モードから再開するには、Pre-Windows 認証が必要です。

注意:

- この S3 サポート オプションを有効にすると、ドライブ暗号化パスワードは、BIOS
  パスワード制限の影響を受けます。BIOS パスワードの制限に関する情報は、システム
  ハードウェア メーカーにお問い合わせください。

- S3 モードをサポートしていない Self-Encrypting Drive もあります。ドライブ設定時に、ドライブがスリープ／スタンバイ モードをサポートしているかどうかの情報が通知されます。このモードをサポートしていないドライブの場合、休止モードが有効になっていると、Windows のスリープ／スタンバイ要求は自動的に休止要求に変換されます (コンピュータの休止モードを有効にしておくことを強くお勧めします)。
- Single Sign On (SSO) オプションの設定後、最初にログインする場合、Windows ログイン プロンプトの時点でプロセスが一時停止します。この場合 Windows 認証に関する情報を入力する必要があります。これらの情報は、以降の Windows ログイン用に安全に保管されます。次回のシステム起動時には、Single Sign On により自動的に Windows にログインされます。ユーザの Windows 認証情報 (パスワード、指紋、スマート カード PIN) が変更された場合も、同じ手続きが必要になります。コンピュータがドメイン上に存在しており、このドメインのポリシーで Windows ログインに Ctrl+Alt+Del キーを押す必要があるように設定されている場合は、このポリシーが優先されます。

警告:**Dell Data Protection | Access** アプリケーションをアンインストールした場合は、Self-Encrypting Drive のデータ保護機能を無効にして、ドライブのロックを解除する必要があります。

Self-Encrypting Drive ユーザ機能

Self-Encrypting Drive 管理者は、ドライブ
セキュリティとユーザに関するすべての管理作業を行います。ドライブ管理者ではないドライブユーザは、次の作業のみを行えます。

- 自己のドライブ パスワードの変更
- ドライブのロック解除

これらの作業は、**Dell Data Protection | Access** の [**Self-Encrypting Drive**] タブから行えます。

パスワードの変更

登録ユーザは、新しいドライブ認証パスワードを作成できます。新しいパスワードを設定するには、現在のSelf-Encrypting Drive パスワードを入力する必要があります。

注意:

- このアプリケーションは、Windows のパスワード長とパスワードの複雑性ポリシーを採用しています (有効にしている場合)。Windows のパスワード ポリシーを有効にしていない場合、Self-Encrypting Drive パスワードの最大長は半角 32 文字になります。[S3 (Sleep/Standby)] を有効にしていない場合、最大長は 127 文字になります。
- ユーザの Self-Encrypting Drive パスワードは、Windows パスワードとは別のものです。ユーザの Windows パスワードを変更、リセットしても、Self-Encrypting Drive パスワードには影響ありません (WPS (Windows Password Synchronization) を有効にしている場合を除く)。詳細は、「デバイス:Self-Encrypting Drives」を参照してください。
- 英語版以外の一部のキーボードでは、Self-Encrypting Drive パスワードに利用できない制限文字が含まれている場合があります。Windows パスワードにこのような制限文字が含まれている場合、WPS (Windows Password Synchronization)を有効にすると、同期化は失敗し、その旨を知らせるエラー メッセージが表示されます。

ドライブのアンロック

ドライブのアンロックにより、ドライブの登録ユーザは、ドライブのロックを解除することができます。ドライブ
ロックが有効になっている場合、コンピュータの電源が切られるとドライブはロック状態になります。システムの電源を再びオンにした場合は、Pre-Windows
認証画面にパスワードを入力して、ドライブの認証を受ける必要があります。

注意:

- **コンピュータ上で複数の Self-Encrypting Drive ユーザ アカウントが同時にアクティブになっている場合は、節電モード (スリープ／スタンバイ／休止) に移行できないことがあります。**
- 中国語版、日本語版、韓国語版、およびロシア語版のアプリケーションでは、Pre-Windows 認証画面でドライブ ユーザ名にはユーザ 1 (User 1)、ユーザ 2 (User 2)... が使用されます：

詳細設定オプション

Dell Data Protection | Accessの [詳細設定]
オプションにより、管理者権限を持つユーザはアプリケーションに関する次の事項を管理することができます。

メンテナンス
パスワード
デバイス

注意:[詳細]
オプションは、管理者権限を持つユーザしか変更することはできません。標準ユーザもこれらの設定を表示することはできますが、設定を変更することはできません。

メンテナンスの概要

［メンテナンス］ウィンドウでは、Windows
ログインの設定、システムのリセット、システムのセキュリティ
ハードウェアに保管されているユーザ資格情報のアーカイブ／復元などの作業を行えます。詳細は、以下のトピックを参照してください。

アクセス初期設定
システムのリセット
資格情報のアーカイブと復元

アクセス初期設定

管理者は [Access Preferences (アクセス初期設定)] ウィンドウから、システムのすべてのユーザの Windows ログイン初期設定を指定することができます。

Dell セキュア ログインを有効にする
標準の Windows の Ctrl+Alt+Delete 画面を置換するオプションにより、Windows パスワードの代わりに (またはパスワードと一緒に) 他の認証手段を使って Windows にアクセスすることができます。Windows のログイン手続きにおけるセキュリティを強化するために、第 2 の認証手段として指紋を利用することができます。スマート カードや TPM 証明書などのその他の認証手段も、Windows へのログイン手段として利用することができます。

注意:

- Dell セキュア ログインを有効にすると、そのシステムのすべてのユーザに影響があります。
- このオプションは、ユーザが各自の指紋やスマート カードを登録した後に有効にすることをお勧めします。
- このオプションを設定した後最初にログインする時には、まず標準のポリシーに従って Windows への認証が要求されます。それ以降のスタートアップ時には、新しい認証手段を使用する必要があります。

Dell セキュア ログインを無効にする (Disable Dell Secure login)
このオプションは、Windows にログインするための、すべての **Dell データ プロテクション | アクセス**機能を無効にします。このオプションを選択すると、標準 Windows ログイン ポリシーに戻ります。

注意:

- ログイン時にセキュア Windows ログインに関するエラーが発生する場合は、Dell セキュア ログイン オプションをいったん無効にした後に、再度有効にしてください。
- 各エラー メッセージの詳細を知りたい場合は、wave.com/support/Dell を参照してください。

システムのリセット

システムのリセット (Reset System) 機能は、プラットフォーム上のすべてのセキュリティ ハードウェアから全ユーザのデータを消去するために用いられます。たとえば、コンピュータを他の用途で利用するために再設定する場合などに用いられます。このオプションでは、システム上のすべてのパスワード (Windows ユーザ パスワードを除く) が消去されます。また、ハードウェア デバイスにある全データも消去されます (ControlVault、TPM、指紋リーダーなど)。Self-Encrypting Drive の場合、この機能によりデータ保護も無効になるため、ドライブのデータには任意のユーザがアクセスできるようになります。

システムをリセットするとどうなるか理解していることを確認した上で、[次へ] をクリックしてください。システムをリセットするには、パスワードが設定されている各セキュリティ デバイスに対してパスワードを入力する必要があります。

- TPM 所有者
- ControlVault 管理者
- BIOS 管理者
- BIOS システム (Pre-Windows)
- ハード ドライブ (BIOS)
- Self-Encrypting Drive 管理者

注意: Self-Encrypting Drive の場合、ドライブ管理者のパスワードしか必要ありません。すべてのドライブ ユーザのパスワードが必要な訳ではありません。

重要:システムのリセットにより消去されたデータを復元する唯一の方法は、以前に保存したアーカイブからデータを復元することです。アーカイブがない場合、データを復元することはできません。Self-Encrypting Drive の場合は、設定データのみが削除されます。ドライブ上の個人データは削除されません。

資格情報のアーカイブと復元

資格情報のアーカイブと復元機能は、ControlVault と Trusted Platform Module (TPM) に保管されているすべてのユーザの資格情報 (ログインおよび暗号化情報) をバックアップ、復元するために用いられます。このようなデータのバックアップは、コンピュータの再プロビジョニングやハードウェア障害によるデータの復元時に重要になります。バックアップしておけば、保存してあるアーカイブ ファイルから新たなコンピュータに資格情報を復元するだけで済みます。

システム内の 1 人のユーザ、またはすべてのユーザの資格情報のアーカイブ、復元を行えます。

ユーザ資格情報は、登録された指紋データ、スマート カード データ、および TPM に保管されている鍵などの、Pre-Windows で用いられる情報から成り立っています。TPM はセキュア アプリケーションからの要求に応じて鍵を作成します。たとえば、デジタル証明書を生成すると、TPM に鍵が作成されます。

注意: Dell データ プロテクション | アクセス により TPM 鍵をアーカイブできるかどうかについては、ご使用のセキュア アプリケーションのマニュアルでご確認ください。一般的には、Wave TCG Enabled CSP を使用して鍵を生成するアプリケーションがサポートされています。

資格情報のアーカイブ

資格情報をアーカイブするには、以下の作業を行う必要があります。

- 自分の資格情報をアーカイブするのか、システムの全ユーザの資格情報をアーブするのかを指定します。
- システム パスワード、ControlVault 管理者パスワード、および TPM 所有者パスワードを入力して、セキュリティ ハードウェアに認証情報を提供します。
- 資格情報バックアップ パスワードを作成します。
- **[参照]** ボタンを使ってアーカイブ場所を指定します。ハード ドライブ障害から保護するために、USB フラッシュ ドライブやネットワーク ドライブなどのリムーバブル メディアをアーカイブの場所として指定する必要があります。

重要:

- 資格情報を復元するには、アーカイブ場所に関する情報が必要なため、正しく記録して安全に保管してください。
- データを確実に復元できるように、資格情報バックアップ パスワードは記録して安全な場所に保管してください。このパスワードは復元できないため、記録した情報は大切に取り扱ってください。
- TPM 所有者パスワードが分からない場合は、システム管理者に連絡するか、またはご使用のシステムの TPM セットアップ手順を参照してください。

資格情報の復元

資格情報を復元するには、以下の作業を行う必要があります。

- 自分の資格情報を復元するのか、システムの全ユーザの資格情報を復元するのかを指定します。

- アーカイブ場所に移動して、アーカイブ ファイルを選択します。
- アーカイブの設定時に作成されたバックアップ パスワードを入力します。
- システム パスワード、ControlVault 管理者パスワード、および TPM 所有者パスワードを入力して、セキュリティ ハードウェアに認証情報を提供します。

注意:

- 資格情報の復元に失敗したことを知らせるエラー メッセージが表示され、複数回再試行しても復元できない場合は、別のアーカイブ ファイルでの復元を試してください。それでも成功しない場合は、別の資格情報アーカイブを作成して、それの復元を試してください。
- TPM 鍵を復元できなかった旨のエラー メッセージが表示された場合は、資格情報アーカイブを作成した後に、BIOS で TPM を消去してください。TPM を消去するには、コンピュータを再起動してバックアップの開始時に **F2** キーを押し、BIOS 設定にアクセスします。次に[Security] > [TPM Security] に移動してください。その後、TPM の所有権を再確立してから、資格情報の復元を試みます。
- 各エラー メッセージの詳細を知りたい場合は、wave.com/support/Dell を参照してください。

パスワードの管理

管理者は [パスワード管理] ウィンドウで、システムのすべてのセキュリティ
パスワードを作成または変更することができます。

- システム (Pre-Windows)*
- 管理者*
- ハード ドライブ*
- ControlVault
- TPM 所有者
- TPM マスター
- TPM パスワード ボールト
- Self-Encrypting Drive

注意:

- 現在のプラットフォーム構成で利用できるパスワードのみが表示されます。そのため、お使いのシステム設定やステータスによって、このウィンドウの表示内容は異なります。
- 上記のパスワードで、隣に * が付いているものは BIOS パスワードで、システム BIOS から変更することもできます。
- BIOS 管理者が BIOS レベルのパスワードの変更を禁止している場合、BIOS レベルのパスワードの作成や変更を行うことはできません。
- Self-Encrypting Drive の **[設定]** リンクをクリックすると、Self-Encrypting Drive Setup Wizard が起動します。**[管理]** をクリックすると、Self-Encrypting Drive のパスワードを変更することができます。
- TPM パスワード ボールトの **[管理]** リンクをクリックすると、ウィンドウが表示されます。このウィンドウから、TPM 鍵を保護するパスワードを表示、変更することができます。パスワードが必要な TPM 鍵を作成すると、パスワードがランダムに生成され、ボールト内に保管されます。TPM パスワード ボールトを管理するには、TPM マスター パスワードを作成する必要があります。

Windows パスワードの構成規則

Dell Data Protection | Access は、以下のパスワードが Windows のパスワード複雑性規則に従っていることを保証します。

- TPM 所有者パスワード

コンピュータの Windows パスワード構成規則を確認するには、以下の手順に従ってください。

1. コントロール パネルを表示します。
2. [管理ツール] をダブル クリックします。
3. [ローカル セキュリティ ポリシー] をダブル クリックします。
4. [アカウント ポリシー] を開いて [パスワードのポリシー] を選択します。

デバイスの概要

[デバイス] ウィンドウは、システムにインストールされているすべてのセキュリティ
デバイスを、管理者が管理するために用いられます。各デバイスに対して、ファームウェアのバージョンなどの、ステータスや詳細情報を表示することができます。**[表示]**
をクリックすると各デバイスの情報が表示されます。**[非表示]**
をクリックすると、そのセクションが閉じられます。管理できるデバイスを次に示します。これは、お使いのプラットフォームに搭載されている機能によって異なります。

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive
認証デバイス情報

Trusted Platform Module (TPM)

Dell Data Protection | Access と TPM を使用するには、TPM セキュリティチップを有効にして、TPM 所有権を確立する必要があります。

[**デバイス管理**] の [Trusted Platform Module] ウィンドウは、お使いのシステムに TPM が検出された場合にのみ表示されます。

TPM 管理

これらの機能により、システム管理者は TPM を管理することができます。

ステータス (Status)

TPM のステータスを「active (アクティブ)」または「inactive (インアクティブ)」で表示します。ステータスが「Active (アクティブ)」の場合、TPM が BIOS で有効になっており、設定準備が完了していることを表しています (所有権を取得できる)。TPM がアクティブ (有効) でない場合、TPM を管理したりセキュリティ機能にアクセスすることはできません。

お使いのシステムで TPM が検出されたけれども、アクティブ (有効) になっていない場合は、このウィンドウで [**activate (アクティブ化)**] リンクをクリックすることで、システム BIOS に移動することなく TPM を有効にすることができます。この機能を使って TPM を有効にした場合、その後コンピュータを再起動してください。再起動時に、変更を受け入れるかどうかを確認するメッセージが表示される場合があります。

注意: このアプリケーションから TPM を有効 (アクティブ) にする機能がサポートされていないプラットフォームもあります。サポートされていない場合は、システム BIOS から有効にしてください。そのためには、システムを再起動した後 Windows がロードされる前に **F2** キーを押して BIOS 設定画面を表示し、[セキュリティ] > [TPM セキュリティ] に移動して、TPM をアクティブにしてください。

また、ここから [**deactivate (アクティブ化解除)**] をクリックして、TPM のアクティブ化を解除することも可能です。TPM のアクティブ化を解除すると、詳細セキュリティ機能が利用できなくなります。アクティブ化を解除しても、TPM 設定が変更されたり、TPM に保管されている情報や鍵が削除、変更されることはありません。

所有 (Owned)

所有権情報 (所有状態)を表示し、TPM 所有権を確立したり、TPM 所有者を変更することができます。TPM のセキュリティ機能を利用するには、TPM 所有権を確立する必要があります。所有権を確立するには、TPM を有効 (アクティブ) にする必要があります。

所有権の確立手続きは、ユーザ (管理者権限を持つ) による TPM 所有者パスワードの作成が関与します。 いったんこのパスワードが定義されると所有権が確立し、TPM の使用を開始することができます。

注記: TPM 所有者パスワードは、お使いのシステムの Windows パスワードの構成規則に準拠する必要があります。

重要:TPM 所有者パスワードは、**Dell Data Protection | Access** の TPM 詳細セキュリティ機能にアクセスするために必要なため、パスワードをなくしたり忘れないようにすることが大切です。

ロック (Locked)
TPM のステータスとして、[locked (ロック)] または [unlocked (ロック解除)]を表示します。ロックは TPM のセキュリティ機能です。TPM 所有者パスワードとして、一定回数を超えて誤ったパスワードが入力された場合、TPM はロック状態に移行します。TPM 所有者はここから TPM のロックを解除することができます。この場合、TPM 所有者パスワードの入力が必要になります。

注意:

- TPM の所有権を確立できない旨のエラー メッセージが表示された場合、システム BIOS で TPM を消去してから、もう一度所有権の確立を試みてください。TPM を消去するには、コンピュータを再起動してバックアップの開始時に **F2** キーを押し、BIOS 設定にアクセスします。次に [Security] > [TPM Security] に移動してください。
- TPM 所有者パスワードを変更できない旨のエラー メッセージが表示された場合は、TPM データをアーカイブし (資格情報のアーカイブ)、BIOS で TPM を消去してから、TPM の所有権を再確立して、TPM データを復元 (資格情報を復元) してください。
- 各エラー メッセージの詳細を知りたい場合は、wave.com/support/Dell を参照してください。

Dell ControlVault®

Dell ControlVault® (CV) は、Pre-Windows ログイン時に使用されるユーザ資格情報 (例:ユーザ パスワードや登録された指紋データなど)
を安全に保管するハードウェア保管庫です。[**デバイス管理**] の ControlVault
ウィンドウは、お使いのシステムに ControlVault が検出された場合にのみ表示されます。

ControlVault 管理

これらの機能により、システム管理者はシステムの ControlVault を管理することができます。

ステータス (Status)
ControlVault のステータスを「アクティブ (*active*)」または「
(インアクティブ*inactive*)」で表示します。ステータスが「インアクティブ
(Inactive)」の場合、お使いのシステムで ControlVault
をストレージとして利用することはできません。システムに ControlVault
が搭載されているかどうかについては、Dell システムのドキュメントを参照してください。

パスワード (Password)
ControlVault
管理者パスワードが設定されているかどうかを表しています。また、管理者パスワードを設定したり、パスワードを変更する (すでに設定されている場合)
ことができます。このパスワードは、システム管理者のみが設定、変更できます。以下の作業を行うためには、ControlVault 管理者パスワードを設定する必要があります。

- 資格情報のアーカイブまたは復元の実行。
- ユーザ データの消去 (すべてのユーザに対して)。

注意: ControlVault
管理者パスワードを設定していない状態でアーカイブや復元が試みられた場合は、パスワードを作成するように要求するメッセージが表示されます (それが管理者の場合)。

登録されているユーザ (Enrolled Users)
現在ログイン資格情報 (例:パスワード、指紋、またはスマート カード データ) が ControlVault
に保管されている、登録ユーザが存在しているかどうかを表しています。

ユーザ データの消去 (Clear User Data)
たとえば、ユーザが認証用の Pre-Windows
資格情報の使用や登録について問題がある場合など、ControlVault
のデータを消去しなければならないこともあります。このウィンドウから、ControlVault
に保管されている、1 人のユーザまたはすべてのユーザの全データを消去することができます。

プラットフォーム上のすべてのユーザ データを消去するには、ControlVault
管理者パスワードを入力する必要があります。Pre-Windows
資格情報が登録されている場合は、システム (Pre-Windows)
パスワードを要求するプロンプトも表示されます。すべてのユーザ
データを消去すると、ControlVault 管理者パスワードとシステム
パスワードがリセットされます。これが、ControlVault
管理者パスワードを消去する唯一の手段であることに留意してください。

注意:すべてのユーザ
データを消去すると、コンピュータの再起動を要求するメッセージが表示されます。システムが正常に機能するためには、再起動が重要です。

1 人のユーザの資格情報を消去する場合は、ControlVault 管理者パスワードは不要です。[**ユーザデータの消去**] をクリックすると、ControlVault
資格情報を消去するユーザの選択を要求するメッセージが表示されます。ユーザを選択すると、システム パスワードの入力を要求するメッセージが表示されます (Pre-Windows
資格情報が登録されている場合にのみ)。

メモ：

- ControlVault 管理者パスワードを作成できなかった旨のエラー
  メッセージが表示された場合は、自分の資格情報をアーカイブした後、ControlVault からすべてのユーザ
  データを消去して、コンピュータを再起動した後に、もう一度パスワードを再作成してください。
- 1 人のユーザの資格情報を ControlVault から消去できなかった旨のエラー
  メッセージが表示された場合は、自分の資格情報をアーカイブした後に、すべてのユーザ データの消去を試してから、当該ユーザのデータの消去をもう一度試みてください。
- すべてのユーザの資格情報を ControlVault から消去できなかった旨のエラー
  メッセージが表示された場合は、システム
  リセットの実行を検討してください。**重要:**システム
  リセットを実行する前には、システムのリセットに関するヘルプ項目を参照してください。この操作を行うと、すべてのセキュリティ データが消去されてしまいます。
- ControlVault および TPM データをバックアップできなかった旨のエラー
  メッセージが表示された場合は、システム BIOS で TPM
  を無効にしてください。このためには、コンピュータを再起動して、起動処理中に **F2** キーを押して BIOS 設定を表示し、[Security]>[TPM Security] を選択します。次に、TPM を再度有効にしてから、ControlVault データのアーカイブを試みてください。
- 各エラー メッセージの詳細を知りたい場合は、wave.com/support/Dell
  を参照してください。

Self-Encrypting Drive:詳細設定

Dell Data Protection | Access は、Self-Encrypting Drive のハードウェア
ベースのセキュリティ機能を管理します。このドライブのハードウェアには、データ暗号化機能が組み込まれています。この管理機能は、ドライブのロックが有効になっている場合に、権限のあるユーザのみを暗号データにアクセスさせる目的で用いられます。

デバイス管理の [Self-Encrypting Drive] ウィンドウは、お使いのシステムに 1 台以上の Self-Encrypting Drive (SED) が存在している場合にのみ表示されます。

重要:ドライブの設定が完了すると、Self-Encrypting Drive
データの保護とドライブのロックが有効になります。

ドライブ管理

これらの機能は、ドライブ管理者が、ドライブのセキュリティ設定を管理するために用意されています。ドライブ
セキュリティ設定の変更内容は、ドライブの電源をオフにした後に有効になります。

データ保護 (Data Protection)
Self-Encrypting Drive データ保護機能が有効 (enabled) かまたは無効 (disabled)
かを表示します。ステータスが有効 (enabled)
の場合、ドライブのセキュリティが設定されていることを表しています。ただし、ドライブのロック をオンにしないと、ドライブ アクセスのための Pre-Windows 認証は行われません。

Self-Encrypting Drive
のデータ保護機能は、ここで無効にすることができます。無効にすると、Self-Encrypting Drive の高度なセキュリティ機能がすべてオフになり、標準のドライブと同じように動作します。データ保護を無効にすると、ドライブ管理者やドライブ
ユーザの資格情報も含めて、すべてのセキュリティ設定が削除されます。ただし、ドライブ上のユーザ データが変更されたり、削除されることはありません。

ロック (Locking)
Self-Encrypting Drive のステータスが有効 (enabled) または無効 (disabled)
で表示されます。ロック時のドライブの動作については、「Self-Encrypting Drive」を参照してください。

一時的にドライブ
ロックを無効にする必要がある場合は、ここからその操作を行えます。ドライブ
ロックを無効にすると、ドライブへのアクセスに資格情報が不要になり、任意のユーザがドライブ
データにアクセスできるため、無効にすることはお勧めできません。ドライブのロックを無効にしても、ドライブ管理者やドライブユーザの資格情報およびドライブ上の任意のユーザデータも含め、セキュリティ設定が削除されることはありません。

警告:Dell Data Protection | Access アプリケーションをアンインストールした場合は、Self-Encrypting Drive
のデータ保護機能を無効にして、ドライブのロックを解除する必要があります。

ドライブ管理者 (Drive Administrator)

現在のドライブ管理者が表示されます。ドライブ管理者は、ここからドライブ管理者となるユーザを変更することができます。新しい管理者は、システムの管理者権限を持つ、有効な Windows ユーザでなければなりません。システムには、1 人のドライブ管理者しか存在することはできません。

ドライブ ユーザ (Drive Users)

登録されているドライブ ユーザ、および現在登録されているユーザ数が表示されます。サポートする最大ユーザ数は、Self-Encrypting Drive によって異なります (現在の所 Segate ドライブでは 4 ユーザ、サムスンの場合は 24 ユーザとなっています)。

Windows Password Sync

WPS (Windows Password Synchronization) 機能により、ユーザの Self-Encrypting Drive パスワードを Windows パスワードと同じに自動設定することができます。この機能は、ドライブ管理者には強制されません。ドライブ ユーザーにのみ適用されます。一定の期間 (例: 90 日) ごとにパスワードの変更を必要とするような環境に、WPS 機能を利用することができます。このオプションを有効にすると、ユーザの Windows パスワードの変更時に、全ユーザの Self-Encrypting Drive パスワードも更新されます。

注意:WPS (Windows Password Synchronization) を有効にした場合、ユーザの Self-Encrypting Drive パスワードを変更することはできません。Self-Encrypting Drive パスワードを変更するには、Windows パスワードを変更して、ドライブのパスワードを自動的に更新させる必要があります。

前回のユーザ名を保持 (Remember Last Username)

このオプションを有効にすると、デフォルトで Pre-Windows 認証画面の ［**Username (ユーザ名)**］ フィールドに、最後に入力されたユーザ名が表示されます。

ユーザ名の選択 (Username Selection)

このオプションを有効にすると、Pre-Windows 認証画面の ［**Username (ユーザ名)**］ フィールドに、すべてのドライブ ユーザ名が表示されます。

暗号的消去 (Cryptographic Erase)

このオプションを使って、Self-Encrypting Drive 上のすべてのデータを消去することができます。この処理では、実際にデータが消去される訳ではありません。データの暗号化に使われたキーを削除することで、データを利用不可能にします。暗号的消去を実施すると、ドライブのデータを復元することはできません。また、Self-Encrypting Drive のデータ保護機能が無効になり、ドライブを他の用途向けに再設定することができます。

注意:

- Self-Encrypting Drive 管理機能に関するエラー メッセージが表示された場合は、いったんコンピュータの電源を完全に切ってから (再起動ではない)、再び起動してください。
- 各エラー メッセージの詳細を知りたい場合は、wave.com/support/Dell を参照してください。

認証デバイス情報

[**デバイス管理**] の[認証デバイス情報] (Authentication Device Information) ウィンドウには、システムに接続されているすべての認証デバイス (指紋リーダー、接触型／非接触型スマート カード リーダーなど) の情報とステータスが表示されます。

テクニカル サポート

Dell Data Protection | Access ソフトウェアのテクニカル サポートについては、http://www.wave.com/support.dell.com を参照してください。

Wave TCG-Enabled CSP

Dell Data Protection | Access アプリケーションには、Wave Systems 社の TCG (Trusted Computing Group)-Enabled CSP (Cryptographic Service Provider) が含まれており、CSP が必要な場合にはアプリケーションから直接呼び出すことも、インストールされている CSP のリストから選択することもできます。可能な場合には [Wave TCG Enabled CSP] を選択し、TPM で鍵を生成し、**Dell Data Protection | Access** で鍵とパスワードを管理するようにしてください。

Wave Systems 社の TCG-Enabled CSP により、MSCAPI 経由で TCG 準拠プラットフォーム上で利用できる機能をアプリケーションで活用することができます。 TCG-Enhanced MSCAPI CSP モジュールは、Trusted Software Stack (TSS) プロバイダに関するベンダー固有の要件に関わらず、TPM 上の非対称鍵機能を提供し、TPM が提供する拡張セキュリティを活用します。

注意: Wave TCG-Enabled CSP により生成された がパスワードを必要としており、ユーザが TPM マスター パスワードを作成した場合、個別の鍵パスワードは無作為に生成され、TPM パスワード ボールトに保管されます。