Dell Data Protection Console ユーザーガイド

暗号化ステータス / 認証登録 / Password Manager v8.13

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

Dell Data Protection Console ユーザーガイド

2017 - 04

Rev. A01

目次

1

DDP Console の概要

Dell Data Protection | Security Tools は、お使いのコンピュータのセキュリティを強化するための、使いやすく直感的なツールを提供します。

ワークステーションオペレーティングシステム上、DDP Console から次の機能が使用できます。

- Security Tools で使用する資格情報の登録
- パスワード、指紋、スマートカードを含む多要素資格情報の利用
- パスワードを忘れた場合にヘルプデスクや管理者のサポートなしでのコンピュータへのアクセス回復
- プログラムデータのバックアップおよび復元
- Windows パスワードの容易な変更
- 個人的なプリファレンスの設定
- 暗号化ステータスの表示（自己暗号化ドライブ搭載のコンピュータ上）

DDP Console

DDP Console は、資格情報の登録と管理、およびセルフリカバリ質問の設定が可能なインタフェースです。

次のアプリケーションにアクセスすることができます。

- Encryption Status ツールを使用して、コンピュータのドライブの暗号化ステータスを表示できます。
- 登録ツールでは、資格情報のセットアップと管理、セルフリカバリ質問の設定、および資格情報登録ステータスの表示を行うことができます。各資格情報のタイプに登録するためのユーザー機能は、管理者によって設定されます。
- Password Manager では、ウェブサイト、Windows アプリケーション、およびネットワークリソースにログオンするために必要なデータを自動的に入力し、送信することができます。また、Password Manager では、アプリケーションを使用してログオンパスワードを変更することも可能であり、Password Manager によって維持されているログオンパスワードがターゲットリソースのパスワードと同期化された状態であることを確実にします。

本書では、これらのアプリケーションそれぞれの使用方法を説明します。

マニュアルのアップデートについて、定期的に dell.com/support をチェックしてください。

Dell ProSupport へのお問い合わせ

Dell Data Protection 製品向けの 24 時間 365 日対応電話サポート（877-459-7304、内線 431003）に電話をかけてください。

さらに、dell.com/support で Dell Data Protection 製品のオンラインサポートもご利用いただけます。オンラインサポートでは、ドライバ、マニュアル、テクニカルアドバイザリー、よくあるご質問（FAQ）、および緊急の問題を取り扱っています。

適切なサポート担当者に迅速におつなぎするためにも、お電話の際はお客様のサービスコードをご用意ください。

米国外の電話番号については、Dell ProSupport の国際電話番号をチェックしてください。

2

DDP Console

DDP Console を使用すると、コンピュータのすべてのユーザーのセキュリティを確保するアプリケーションにアクセスして、コンピュータのドライブとパーティションの暗号化ステータスを表示および管理したり、管理者によって設定されたポリシーに基づいて、ウェブサイト、プログラム、およびネットワークリソースへのユーザーのログオンを管理したりすることができます。また、ユーザーの認証資格を簡単に登録することもできます。

DDP Console を開くには、デスクトップで **DDP Console** アイコンをダブルクリックします。

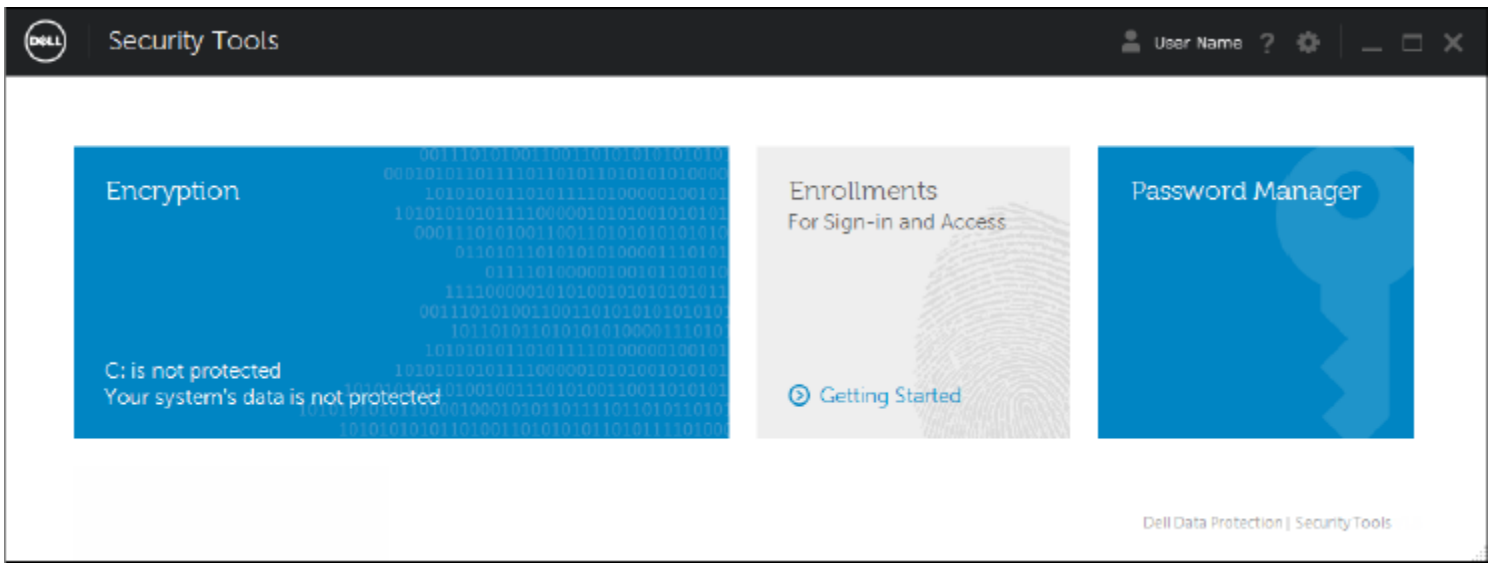
DDP Console が起動すると、ホームページに以下の Security Tools アプリケーションが表示されます。

- Encryption Status
- 登録
- Password Manager

  資格情報を初めて設定する場合は、登録 タイルの **はじめに** リンクを選択します。ウィザードが短い登録プロセスをガイドします。詳細については、「資格情報を初めて登録する」を参照してください。

ナビゲーション

アプリケーションにアクセスするには、適切なタイルをクリックします。



タイトルバー

アプリケーション内からホームページに戻るには、アクティブなアプリケーションの名前の横にある、タイトルバーの左端の 戻る 矢印をクリックします。

別のアプリケーションに直接ナビゲートするには、アクティブなアプリケーションの名前の横にある下矢印をクリックし、アプリケーションを選択します。

DDP Console を最小化、最大化、または閉じるには、タイトルバーの右端にある適切なアイコンをクリックします。

最小化後に DDP Console を復元するには、そのシステムトレイアイコンをダブルクリックします。

ヘルプを開くには、タイトルバーで **?** をクリックします。

DDP Console の詳細

DDP Console、ポリシー、実行中のサービス、およびログに関する詳細を表示するには、タイトルバーの左側にあるギアアイコンをクリックします。この情報は、管理者がテクニカルサポートを提供する場合に必要になることがあります。

メニューから項目を選択します。

メニュー項目	目的
バージョン情報	バージョンおよび著作権情報が記載されています。
情報の表示	次の情報が含まれます。 • 製品のバージョンと日付情報 • このコンピュータ上の DDP Console がエンタープライズまたはローカル管理者のどちらによって管理されているか • オペレーティングシステム、BIOS、マザーボード、および Trusted Platform Module (TPM) のバージョン番号
MS 情報	Microsoft Windows システム情報ユーティリティを実行して、ハードウェア、コンポーネント、およびソフトウェア環境に関する詳細情報を表示します。
情報のコピー	管理者または Dell ProSupport に送信する電子メールに貼り付けられるよう、すべてのシステム情報をクリップボードにコピーします。
フィードバック	この製品に関するフィードバックをデルに提供するためのフォームを表示します。(ドメイン以外のコンピュータでは、このオプションを常に使用できます。ドメインのコンピュータでは、このオプションを使用できるかどうかはエンタープライズポリシーによって異なります。)
ポリシー	このコンピュータに適用されるポリシーの階層を表示します。
サービス	実行中のサービスに関する詳細を表示します。
サポート	デルプロサポートのウェブサイトに接続します。
ログ	トラブルシューティングのため、ログされたイベントの詳細リストを表示します。
トレースの開始	トラブルシューティングのために、サインインアクティビティの記録を開始および停止することができます。

3

Encryption Status

暗号化 ページはコンピュータの暗号化ステータスを表示します。ディスク、ドライブ、またはパーティションが暗号化されていない場合は、ステータスが 未保護 となります。ドライブまたはパーティションが暗号化されている場合は、ステータスが 保護 と表示されます。

暗号化ステータスをアップデートするには、該当するディスク、ドライブ、またはパーティションを右クリックして、**更新** を選択します。

登録

登録ツールでは、管理者が設定したポリシーに基づいて、登録ステータスを登録、変更、およびチェックすることができます。

DDP Console に初めて資格情報を登録するときは、ウィザードがパスワード変更、リカバリ質問、指紋、モバイルデバイス、およびスマートカードの登録をガイドします。ポリシーに応じて、ユーザーは各資格情報を登録またはスキップすることができます。初期登録後は、登録 タイルをクリックして資格情報を追加または変更することができます。

資格情報を初めて登録する

初めて資格情報を登録するには、次の手順を実行します。

1 DDP Console のホームページで、登録 タイルの **はじめに** リンクをクリックします。
2 ようこそ ページで **次へ** をクリックします。
3 認証が必要 ダイアログで、Windows パスワードを使ってログインし、**OK** をクリックします。
4 Windows パスワードを変更するには、パスワード ページで新規パスワードを入力して確認し、**次へ** をクリックします。
パスワードの変更をスキップするには、**スキップ** をクリックします。ウィザードでは、資格情報を登録しない場合、その資格情報をスキップすることができます。前のページに戻るには、**戻る** をクリックします。
5 各ページの手順に従って、適切なボタン（**次へ**、**スキップ**、**戻る**）をクリックします。
6 サマリ ページで登録した資格情報を確認し、登録が完了したら **適用** をクリックします。
資格情報登録 ページに戻って変更を行うには、変更するページが表示されるまで **戻る** をクリックします。

資格情報の登録方法、または資格情報の変更方法の詳細については、「登録の追加、変更、表示」を参照してください。

登録の追加、変更、表示

登録を追加、変更、または表示するには、**登録** タイルをクリックします。

左ペインのタブには、利用可能な登録がリストされています。これは、お使いのプラットフォームまたはハードウェアのタイプに応じて異なります。

ステータス ページでは、サポートされている資格情報、それらのポリシー設定（必須または該当なし）、および登録ステータスが表示されます。ユーザーは、管理者によって設定されたポリシーに基づいて、このページから登録を管理できます。

- 資格情報を初めて登録する場合は、資格情報の行で **登録** をクリックします。
- 既存の登録済み資格情報を削除するには、**削除** をクリックします。
- 資格情報の登録または変更がポリシーによって許可されていない場合は、ステータス ページの **登録** リンクおよび **削除** リンクが非アクティブになっています。
- 既存の登録を変更するには、左ペインで該当するタブをクリックします。

  資格情報の登録または変更がポリシーによって許可されていない場合は、資格情報を変更することはポリシーで許可されていません というメッセージが資格情報の登録ページに表示されます。

パスワード

Windows パスワードを変更するには、次の手順を実行します。

1 **パスワード** タブをクリックします。
2 現在の Windows パスワードを入力します。
3 新しいパスワードを入力し、確認用にもう一度入力して、**変更** をクリックします。
パスワードの変更はただちに有効になります。

4 登録の成功 ダイアログで **OK** をクリックします。

メモ:
Windows パスワードは、Windows 上ではなく DDP Console でのみ変更する必要があります。Windows パスワードが DDP コンソール以外で変更された場合、パスワードの不一致が発生し、復元操作が必要になります。

リカバリ質問

リカバリ質問 ページでは、リカバリ質問と回答を作成、削除、または変更することができます。リカバリ質問は、たとえば、パスワードの期限が切れた、またはパスワードを忘れた場合に、ユーザーが Windows アカウントにアクセスするための質問および回答に基づく方法を提供します。

メモ:
リカバリ質問は、コンピュータへのアクセスの回復のみに使用されます。質問と回答は、ログオンには使用できません。

以前に登録したリカバリ質問がない場合は、次の手順を実行します。

1 **リカバリ質問** タブをクリックします。
2 事前定義された質問のリストから選択し、次に回答を入力して確定します。
3 **登録** をクリックします。

メモ:
リセット ボタンをクリックして、このページで選択内容を消去し、再起動します。

リカバリ質問がすでに登録されている

リカバリ質問がすでに登録されている場合、リカバリ質問の削除または再登録のいずれかを実行できます。

1 **リカバリ質問** タブをクリックします。
2 次の該当するボタンをクリックします。
- リカバリ質問を完全に削除するには、**削除** をクリックします。
- リカバリ質問と回答を再定義する場合は、**再登録** をクリックします。

指紋

メモ:
この機能を使用するには、コンピュータに指紋リーダーが必要です。

指紋を登録するには、次の手順を実行します。

1 **指紋** タブをクリックします。
2 指紋 ページで、登録する指をクリックします。
3 画面上の手順に従い、指紋を登録します。

メモ:
登録するには、指のスキャンが 4 回成功する必要があります。指紋登録を完了するために必要なスキャンの回数は、各スキャンの品質によって異なります。管理者が、指紋の最小および最大数を定義しました。

4 ポリシーによって必要とされる最少数の指紋を登録するまで、後続の各指をクリックします。
最少数の指紋を登録していないと、ダイアログがそれを通知します。**OK** をクリックして続行します。
5 必要な数の指紋のスキャンを終了したら、**保存** をクリックします。
スキャンした指紋を削除するには、指紋登録 ページでハイライト表示されている指紋をクリックして登録解除します。次に、**はい** をクリックして指紋の削除を確認し、**保存** をクリックします。

モバイルデバイス

モバイルデバイスを登録すると、ワンタイムパスワード (OTP) 機能を使用できます。OTP では、コンピュータとペアリングされているモバイルデバイスの Security Tools Mobile アプリによって生成されたパスワードを使用して Windows にログオンすることができます。また、ポリシーで許可されている場合は、パスワードの期限が切れた、またはパスワードを忘れたときのコンピュータへのアクセス回復のために OTP 機能を使用することもできます。

メモ:
DDP Console に モバイルデバイス タブが表示されない場合は、コンピュータの構成上サポートされていないか、管理者が設定したポリシーで許可されていません。

メモ:
OTP 機能の用途(パスワードの期限が切れた、またはパスワードを忘れた場合にお使いのコンピュータにログオンする、またはコンピュータへのアクセスを回復する) は、ポリシー設定によって決定されます。ログオンとリカバリの両方に使用することはできません。

OTP 機能を使用するには、お使いのモバイルデバイスを登録する、またはそれをコンピュータとペアリングする必要があります。複数のユーザーが存在するコンピュータでは、各ユーザーがそのコンピュータにそれぞれ 1 台のモバイルデバイスを登録することができます。モバイルデバイスは、複数のコンピュータに登録できます。

デバイスがすでに登録されている場合、新しいデバイスを登録することによって前のデバイスが自動的にペアリング解除されます。

モバイルデバイスの登録

1 DDP Console の 登録 ページで、**モバイルデバイス** タブをクリックします。
2 右上で、**登録** をクリックします。
ワンタイムパスワードの登録 ページが開きます。
3 これがペアリングする最初のコンピュータである場合は、**はい** を選択します。

a モバイルデバイスで、App Store から Dell Data Protection | Security Tools Mobile アプリをダウンロードします。
b コンピュータ上で、**次へ** をクリックします。

Security Tools Mobile のセットアップ

1 Security Tools Mobile アプリを開きます。

2 Security Tools Mobile アプリのアクセスに使う PIN を作成して入力します。

> **メモ:**
> モバイルデバイスがロックされていないときは、ポリシーによって PIN が必要となる場合があります。モバイルデバイスのロック解除に PIN を使用していなければ、Security Tools Mobile アプリにアクセスするための PIN が必要になります。

3 **コンピュータの登録** を選択します（必要な場合は、モバイル画面の左上隅をタップしてコマンドにアクセスしてください）。
モバイルデバイスにコードが表示されます。コードの長さと英数字の組み合わせは、管理者が設定したポリシーに基づきます。

モバイルデバイスとコンピュータのペアリング

1 コンピュータの DDP Console の モバイルコード ページで、次の手順を実行します。
   a モバイルデバイスからのコードをフィールドに入力します。
   b **次へ** をクリックします。
   c デバイスのペアリング ページで、次のいずれかを選択します。
   QR コード - QR コードが表示されます。

   または

   手動入力 - 24 桁のペアリングコードが表示されます。
2 モバイルデバイス：
   a **デバイスのペアリング** をタップします。
   b コンピュータ上で選択したものと同じペアリングオプション（**QR コードをスキャン** または **手動入力**）を選択します。
   c 次のいずれかを選択してください。
   - **QR コード**を使用する場合は、QR コードをスキャンできるようにコンピュータの画面の前にモバイルデバイスを配置します。
     モバイルデバイスに表示されている数字の検証コードをメモしてから、**次へ** をタップします。

     > **メモ:**
     > スキャンに問題がありますか? バーが表示された場合は、再試行するか、**手動入力** を選択します。

   - **手動入力**する場合は、コンピュータから 24 桁のペアリングコードを入力し、**完了** をタップします。
     モバイルデバイスに表示されている数字の検証コードをメモしてから、**次へ** をタップします。
3 コンピュータの DDP Console で、次の手順を実行します。
   a **次へ** をクリックします。
   b モバイルデバイスに表示されている検証コードを入力し、**次へ** をクリックします。
   c オプションとして、モバイルデバイスの名前を変更します。
   d **適用** をクリックします。
   デバイスがペアリングされます。
4 モバイルデバイス：
   a **続行** をタップします。
   b 必要な場合は、コンピュータの名前を変更し、**完了** をタップします。
   c **終了** をタップします。

別のモバイルデバイスの登録

新しいデバイスを登録すると、前のデバイスが自動的にペアリング解除されます。ペアリング解除には、別途手順は必要ありません。

コンピュータとモバイルデバイスのペアリング解除

別のデバイスを登録することなくコンピュータとモバイルデバイスのペアリングを解除するには、次のいずれかを選択します。

- DDP Console：登録ステータス ページで、モバイルデバイス資格情報の横にある **削除** をクリックします。
- モバイルデバイス：以下の手順を参照してください。

1 モバイルデバイスで、以下の手順を実行します。
   a Security Tools Mobile アプリを実行します。
   b 左上のメニューバーをタップし、ドロワーを開きます。
   c **コンピュータの削除** をタップします。
   d ペアリングを解除するコンピュータを選択します。
   e Android の場合は **削除** を選択します。iOS の場合は **完了** をタップします。
   確認メッセージが表示されます。
   f 登録されているすべてのコンピュータをデバイスから削除するには、**すべて削除** を選択します。
   すべて削除オプションは、複数のコンピュータを削除したとき、またはペアリングされているコンピュータのみを削除したときに表示されます。

   - 登録されているコンピュータと PIN を削除するには、**デフォルトの設定を復元** を選択します。デフォルト設定を復元すると、登録されているコンピュータ、および Security Tools Mobile アプリへのアクセスに使用する PIN がすべて削除されます。
   - コンピュータを登録されたままにするには、**キャンセル** を選択します。

ワンタイムパスワードを使用したログオン

メモ:
OTP 認証は、Windows ログオンのみで使用できます。

OTP は、リカバリ(ロックアウトされたコンピュータへのアクセスを回復する)、または Windows ログオンのいずれかに使用することができます。両方に使用することはできません。

ポリシーで許可され、OTP の記号 () がログオン画面に表示される場合、OTP で Windows にログオンできます。

OTP を使用してログオンするには、次の手順を実行します。

1 コンピュータの Windows のログオン画面で、OTP アイコン () を選択します。
2 モバイルデバイスで Security Tools Mobile アプリを開き、PIN を入力します。
3 アクセスするコンピュータを選択します。
   モバイルデバイスにコンピュータ名が表示されない場合は、次のいずれかの状態が存在する可能性があります。

   - モバイルデバイスがアクセスしたいコンピュータに登録またはペアリングされていない。
   - 複数の Windows ユーザーアカウントを持っている場合は、アクセスしようとしているコンピュータ上に Security Tools がインストールされていないか、コンピュータとモバイルデバイスのペアリングに使用したアカウントとは異なるユーザーアカウントにログオンしようとしているかのいずれかです。

4 **ワンタイムパスワード** をタップします。
   モバイルデバイス画面にパスワードが表示されます。

メモ:

必要であれば、更新シンボル  をクリックして新しいコードを取得します。最初 2 回の OTP 更新後、別の OTP を生成できるようになるまでに 30 秒の遅延が発生します。

コンピュータとモバイルデバイスは、両方が同時に同じパスワードを認識できるように同期化されている必要があります。パスワードを急速に連続して作成しようとすると、コンピュータとモバイルデバイスが非同期状態となり、OTP 機能が失敗する原因となります。この問題が発生した場合は、2 つのデバイスが再度同期化されるまで 30 秒程待ってから、再試行してください。

5 コンピュータの Windows ログオン画面で、モバイルデバイスに表示されているパスワードを入力し、**Enter** を押します。
リカバリに OTP を使用した場合は、コンピュータへのアクセスを回復した後、画面に表示される手順に従ってパスワードをリセットします。

Security Tools Mobile の管理タスク

これらのタスクは、モバイルデバイス上の Security Tools Mobile アプリを使用して実行します。

Security Tools Mobile アプリ PIN のリセット

Security Tools Mobile アプリ PIN をリセットするには、次の手順を実行します。

1 右上のメニューオプションをタップします。
2 **PIN のリセット** を選択します。
3 新しい PIN を入力して確認します。

Security Tools Mobile アプリのアンインストール

モバイルデバイス上で、次の手順を実行します。

1 デバイスとコンピュータのペアリングを解除します。
2 普段モバイルデバイスからアプリを削除するときと同じ手順で、Security Tools Mobile アプリを削除またはアンインストールします。

スマートカード

メモ:
この機能を使用するには、コンピュータにスマートカードリーダーが必要です。

スマートカードを登録するには、次の手順を実行します。

1 **スマートカード** タブをクリックします。
2 カードのタイプに基づいて、スマートカードを登録します。
   - カードリーダーにスマートカードを挿入します。
   - 非接触型カードの場合は、リーダーの上またはその近くにカードを配置して固定します。
3 カードが検知されると、緑色のチェックボックスと カードを登録 が表示されます。**カードを登録** を選択します。
4 登録の成功 ダイアログで **OK** をクリックします。

ユーザーに関連付けられているスマートカードの登録をすべて解除するには、スマートカード登録 ページで **アカウントから登録済みカードを削除** を選択します。

5

Password Manager

Password Manager では、ウェブサイト、Windows プログラム、およびネットワークリソースへの自動ログオンと、ログオン資格情報の管理を単一のツールで行うことができます。また、Password Manager では、ユーザーはアプリケーションを使用してログオンパスワードを変更することが可能になり、Password Manager によって維持されているログオンパスワードが対象リソースのパスワードと同期化された状態であることを確実にします。

Password Manager は、Internet Explorer および Mozilla Firefox でサポートされています。Password Manager は、Microsoft アカウント（旧 Windows Live ID）ではサポートされていません。

メモ:
Firefox 上で Password Manager を実行している場合は、Password Manager 拡張機能をインストールおよび登録する必要があります。Mozilla Firefox での拡張機能のインストール手順については、https://support.mozilla.org/ を参照してください。

メモ:
Mozilla Firefox での Password Manager アイコン（学習前および学習済みアイコンの両方）の使用は、Microsoft Internet Explorer での使用とは異なります。

- Password Manager アイコンでのダブルクリック機能が使用できない。
- ドロップダウンコンテキストメニューでデフォルトアクションが太字で表示されない。
- ページに複数のログオンフォームがある場合、複数の Password Manager アイコンが表示されることがある。

メモ:
ウェブログオンページの構造は常に変化し続けているため、Password Manager はすべてのウェブサイトを常時サポートできない場合があります。

Password Manager の使用開始

Password Manager は、ユーザーの作業に伴ってログオン資格情報を収集し、保管します。Password Manager は、Security Tools のインストール後、すぐに使用を開始することができます。ログオンページに資格情報を入力すると、Password Manager によって

ログオンフォームが検出され、Password Manager に資格情報を保存するかどうかを選択することができます。

これには、次の 3 つのオプションがあります。

- **ログオンを保存** をクリックして、Password Manager でログオン資格情報を保存します。
- ログオンを保存**しない**場合、ウェブサイトまたはプログラムにログオンするたびに、ログオン資格情報を保存するかどうかを尋ねるプロンプトが表示されます。このプロンプトを表示したくない場合は、**このサイトでは表示しない** を選択します。ウェブサイト除外 リストに記録が作成されます。詳細については、「除外するウェブサイト」を参照してください。
- 資格情報を保存しない場合は、**ログオンを保存しない** をクリックします。

このダイアログは、ウェブサイトまたはプログラムに対して以前保存した資格情報があるときに、それとは異なるユーザー名またはパスワードを入力した場合にも表示されます。新しいユーザー名を入力して **ログオンを保存** を選択すると、一組の新しい資格情報が保存されます。以前に保存したユーザー名と新しいパスワードを入力して **ログオンを保存** を選択すると、元の資格情報が新しいパスワードでアップデートされます。

ログオンの管理

Logon Manager は、ウェブサイト、Windows プログラム、およびネットワークリソースへのすべてのログオンの管理を簡素化し、一元化します。

Logon Manager を開くには、次の手順を実行します。

1 DDP Console のホームページで、**Password Manager** タイルをクリックします。
2 **ログオンマネージャ** タブをクリックします。

ログオンおよびカテゴリを追加して、それらを並べ替えたりフィルタリングすることができます。

ログオンの追加 - 一組の新しいログオン資格情報を追加できます。ポリシーによっては、ログオンを追加する際に、Security Tools に保管されている資格情報の入力が必要になる場合があります。

カテゴリの追加 - 並べ替えとフィルタリングで使用する新しいカテゴリ (電子メール、ストレージ、ニュース、コーポレートリソース、ソーシャルメディアなど) を追加できます。

並べ替え : アカウント、ユーザー名、またはカテゴリでログオンを並べ替えます。列見出しをクリックし、列順にソートします。

フィルタ : 表示 リストからカテゴリを選択すると、選択したカテゴリのログオンを除く、すべてのログオンが非表示になります。フィルタを削除するには、すべてを選択します。

ログオンは次のように管理することができます。

起動 - ウェブサイトまたはプログラムを開き、ユーザー設定に基づいてログオン資格情報を送信します。

編集 - ウェブサイトまたはプログラムの保管済みログオンデータを変更することができます。

削除 - Password Manager から保管済みのログオンデータを削除することができます。

追加 - 新規ログオン、カテゴリ、または新規ログオンデータを追加できます。

カテゴリの追加

ログオンを追加する前に、ログオンを作成するたびにそれらをカテゴリ化できるように、カテゴリ(電子メール、ストレージ、ニュース、コーポレートリソース、ソーシャルメディアなど) を作成します。この後、ログオンをカテゴリ別に並べ替えおよびフィルタリングすることができます。

カテゴリを追加するには、ログオンマネージャ ページで **カテゴリの追加** をクリックし、カテゴリ名を入力して **保存** をクリックします。

ログオンの追加

1 ログオンマネージャ ページで、**ログオンの追加** をクリックします。
ポリシーに基づいて、ログオンを追加するための認証が必要になる場合があります。
2 ログオン先のウェブサイトまたはプログラムを開きます。
3 ログオンの追加 ダイアログで、**続行** をクリックします。
4 次のダイアログで、以下を入力します。
- **カテゴリ** - 保存するウェブサイトまたはプログラムログオンのカテゴリを選択します。カテゴリを追加していない場合、このリストは空になります。
- **アカウント名** - 変更しないで、あらかじめ入力されている名前を受け入れるか、ウェブサイトまたはプログラムの名前を入力します。
- **未検知のタイトル** - これらは、Password Manager によって、ログオン情報を入力するログオンページ上のフィールドとして検知されたフィールドです。これらのフィールドには、通常、ユーザー名または電子メール、およびパスワードが含まれます。

5 フィールド名が未検知のタイトルになっている場合、または誤ったフィールドがログオンフィールドとして含まれている場合は、**その他のフィールド** ボタンをクリックして、フィールド名を編集するかフィールドを削除します。

6 その他のフィールド ダイアログで、**未検知のタイトル** をクリックして、各フィールドの正しい名前を入力します。
その他のフィールド ダイアログが表示されるときは、フィールドの名前変更に役立つように、ログオンの追加 ダイアログでアクティブであったフィールドがハイライト表示されます。

フィールドがログオンに不要な場合は、チェックボックスを選択解除してログオン情報から除外します。

7 変更を保存するには、**OK** をクリックします。
8 ログオンの追加 ダイアログで、ログオンに必要なフィールドを完了します。

メモ:
既存のログオンを保管しているため、パスワードは、ウェブサイトまたはプログラムの パスワードの変更 機能にアクセスしなければ変更できません。

9 Password Manager でログオン情報を自動的に入力して送信する場合は、**ログインデータを自動的に送信** を選択します。
10 **保存** をクリックします。
Logon Manager ページにウェブサイトまたはプログラムログオンが表示されます。

資格情報のインポート

ウェブブラウザに保管されている資格情報を Password Manager にインポートすることができます。

1 Password Manager ツールで、**資格情報のインポート** を選択します。
2 インポートするブラウザを選択し、**スキャン** をクリックします。
3 プロンプトが表示されたら、選択したブラウザのパスワードを入力します。

メモ:
インポートでパスワードをインポートできない場合は、確認のうえブラウザがインポートするデータを保存していないかどうかを判断してください。Firefox を使用している場合は、Sync にログオンします。資格情報のインポートを再試行してください。

アイコンコンテキストメニュー

ウェブサイトまたはプログラムにアクセスするときは、Password Manager アイコンが表示されます。

は、ログオンフォームに学習させることが可能なことを示しています。

がない場合、ログオンフォームにはすでに学習させています。アイコンをダブルクリックして、プログラムまたはウェブサイトにログオンします。

アイコンをクリックすると、ログオンフォームが学習済みか否かに応じて、コンテキストメニューに異なるオプションが表示されます。

現在のログオンフィールドが学習済みではない場合は、コンテキストメニューに次のオプションが表示されます。

Password Manager に追加 - ログオンの追加 ダイアログが開きます。

アイコン設定 - ユーザーに、学習可能なログオンページにおける Password Manager アイコンの表示設定を許可します。

Password Manager を開く - *Password Manager* 管理ツールが起動し、ログオンマネージャ ページが開きます。

ヘルプ - オンラインヘルプが開きます。

現在のログオンフィールドが学習済みの場合は、コンテキストメニューに次のオプションが表示されます。

ログオンデータを入力 - ログオンフォームに学習させたときの選択内容に応じて、自動ログオンするか、またはログオンデータを送信できるようにユーザー名とパスワードのフィールドに自動的に入力されます。

ログオンの編集 - ログオンの編集 ダイアログが開きます。

ログオンの追加 - ログオンの追加 ダイアログが開きます。

Password Manager を開く - ログオンマネージャ ページが開きます。

ヘルプ - オンラインヘルプが開きます。

Password Manager アイコンがログオンフォームと共に表示されない場合は、以下の手順を実行して、ブラウザのパスワード保存機能をオフにします。

- Mozilla Firefox の場合 : メニューアイコン、オプション、セキュリティ の順に選択して、**サイトのパスワードを保存する** チェックボックスをオフにします。
- Internet Explorer の場合 : 歯車アイコン、インターネットオプション、コンテンツ タブ、オートコンプリートの設定 の順に選択して、**フォームのユーザー名およびパスワード** チェックボックスをオフにします。

学習済みのログオン ページへのログオン

ウェブサイトまたはプログラムログオンを開くとき、Password Manager はそのページが学習済みであるかどうかを検知します。学習済みであれば、Password Manager アイコンがログオンエリアに表示されます。学習済みでなければ、学習済みでないフォームに対するプロンプトが無効化されている場合を除き、Password Manager アイコンが表示されます。

ログオンするには、次の操作のいずれかを選択します。

- 登録されている資格情報をスキャンします。指紋またはスマートカードを登録している場合は、登録されている指で指紋リーダーにタッチするか、登録されているカードをカードリーダーに提示します。
- Password Manager アイコンをクリックして、コンテキストメニューから **ログオンデータを入力** を選択します。
- Password Manager ホットキーの組み合わせ（ **Ctrl + Win + H** ）を押します。Password Manager のポップアップに学習したサイトが提示され、サイトを迅速に起動できます。

メモ:
ホットキーの組み合わせを変更するには、DDP Console、Password Manager、設定 の順に選択します。

サイトまたはプログラムに対して複数のログオンが保管されている場合は、使用するアカウントを選択するプロンプトが表示されます。

ウェブドメインのサポート

特定のウェブドメインのためにログオンページを学習させたが、異なるログオンページからそのウェブドメインのアカウントにアクセスしたい場合は、新しいログオンページに移動します。既存のログオンを使用するか、Password Manager に新しいログオンを追加するかを確認するためのプロンプトが表示されます。

- ログオンの使用 をクリックすると、エンドユーザーは以前に作成されたアカウントへログオンされます。次に新しいログオンページからそのアカウントにアクセスする時は、以前に作成されたアカウントに自動的にログオンされます。
- ログオンの追加 をクリックすると、ログオンの追加 ダイアログが表示されます。

Windows 資格情報の入力

一部のプログラムでは、ログオン用に Windows 資格情報の使用が許可されています。

ユーザー名とパスワードを入力する代わりに、ログオンの追加 ダイアログおよび ログオンの編集 ダイアログにあるドロップダウンメニューから Windows 資格情報を選択します。

ユーザー名については、次のタイプから選択してください。

- Windows ユーザー名
- Windows ユーザープリンシパル名
- Windows ドメイン\ユーザー名
- Windows ドメイン

パスワードについては、Windows パスワードを使用します。

これらのオプションは変更できません。

古いパスワードの使用

Password Manager でパスワードを変更したにも関わらず、新規パスワードがプログラムに拒否される場合があります。この場合、そのプログラムでは、最新のパスワードの代わりに以前のパスワード（このログオンページで以前に入力したパスワード）を使用することができます。

パスワード履歴 を選択します。認証後、パスワード履歴 リストから古いパスワードを選択するためのプロンプトが表示されます。リストには、7 つのパスワードが含まれます。

除外するウェブサイト

Password Manager がウェブサイトを管理しないようにするには、**ウェブサイト除外** タブをクリックします。

ウェブサイト除外には、以下の特徴があります。

- Password Manager アイコンを呼び出さない。
- ユーザーを自動的にログインしない。
- パスワードリマインダーを表示しない。

除外リストに新しいウェブサイトを追加するには、次の手順を実行します。

1 **ウェブサイト除外** タブをクリックします。
2 **ウェブサイトの追加** をクリックします。
3 除外するウェブサイトの URL を入力します。
4 **保存** をクリックします。

ウェブサイトが除外されると、そのウェブサイトは Password Manager によって管理されなくなります。除外を無効にするには、ウェブサイト除外 リストからウェブサイトを単に削除します。除外リストからウェブサイトを削除するには、X をクリックします。

複数のウェブサイトを追加した後は、次の操作を実行できます。

- ウェブサイトを昇順または降順で並べ替えるには、ウェブサイト列見出しをクリックします。
- リスト内で検索するには、URL の一部を検索フィールドに入力します。入力するに従って、リストもフィルタリングされます。

ログオンフォームに学習させるためのプロンプトの無効化

既存の学習済みログオンを維持しながら、新しいログオンフォームを学習させるためのプロンプトを無効にすることができます。

新規ログオンに対するプロンプトを無効にするには、次の手順を実行します。

1 DDP コンソールを開きます。
2 **Password Manager** タイルをクリックします。
3 **設定** タブをクリックします。
4 **ログオン画面のときにログオンを追加するプロンプトを表示** チェックボックスをオフにします。

Password Manager 資格情報のバックアップと復元

Password Manager では、Password Manager によって管理されているログオンデータをセキュアにバックアップすることができます。このデータは、Password Manager によって保護されている任意のコンピュータ上で復元できます。

メモ:
バックアップされている Password Manager データには、オペレーティングシステムや起動前認証 (PBA) ログオン資格情報、または指紋などの資格情報固有の情報は含まれません。

資格情報のバックアップ

資格情報をバックアップするには、次の手順を実行します。

1 **資格情報のバックアップ** タブをクリックして、バックアッププロセスを設定します。
2 **参照** をクリックし、目的のバックアップ場所に移動します。
データをローカルドライブにバックアップしようとすると、データをポータブルストレージまたはネットワークドライブにバックアップするための推奨が表示されます。
3 パスワードを入力し、確認します。バックアップしたこれらの資格情報を後ほど復元する必要がある場合は、このパスワードを使用する必要があります。
4 **バックアップ** をクリックします。
5 Windows パスワードを入力します。
6 成功 ダイアログで **OK** をクリックします。

メモ:
実行したバックアップ操作のテキストログを表示するには、 をクリックして、**ログ** を選択します。

資格情報の復元

資格情報を復元するには、バックアップの場所が使用可能である必要があります。

資格情報を復元するには、次の手順を実行します。

1 **資格情報の復元** タブをクリックします。
2 **参照** をクリックしてバックアップファイルに移動して、ファイルのパスワードを入力します。
3 **復元** をクリックします。

警告:
Password Manager データの復元により、すべての既存データが上書きされます。バックアップの作成後に追加されたログオンおよびその他のデータは失われます。

4 **次へ** をクリックします。

メモ:

復元操作のテキストログを表示するには、タイトルバーで アイコンをクリックし、**ログ** を選択します。

6

用語集

資格情報 - 資格情報とは、指紋または Windows パスワードなど、ある人物の身元を証明するものです。

ワンタイムパスワード（OTP） - ワンタイムパスワードは、一度しか使用できないパスワードで、有効時間が限定されています。OTP には、TPM が存在し、有効化され、所有されている必要があります。OTP を有効にするには、Security Console および Security Tools Mobile アプリを使用して、モバイルデバイスをコンピュータとペアリングします。Security Tools Mobile アプリは、Windows ログオン画面でのコンピュータへのログオンに使用されるパスワードをモバイルデバイス上に生成します。コンピュータへのログオンに OTP を使用しなかった場合は、ポリシーに基づき、パスワードの期限が切れたときに、またはパスワードを忘れたときに、OTP 機能を使用してコンピュータへのアクセスを回復することができます。OTP 機能は、認証またはリカバリのいずれかに使用できますが、両方には使用できません。生成されたパスワードが一度しか使用できず、短時間で失効するため、OTP セキュリティは他の認証手法よりも優れています。

起動前認証（PBA）- 起動前認証（PBA）は、BIOS または起動ファームウェアの拡張機能としての役割を果たし、信頼された認証レイヤとして、オペレーティングシステム外部のセキュアな耐タンパ環境を保証します。PBA は、ユーザーが正しい資格情報を持っていることを立証するまで、オペレーティングシステムなどをハードディスクから読み取ることができないようにします。

保護済み - 自己暗号化ドライブ（SED）の場合、コンピュータは、SED がアクティブ化され、起動前認証（PBA）が導入されると保護されます。

自己暗号化ドライブ（SED） - メディアに保存されるすべてのデータの暗号化とメディアから出力されるすべてのデータの復号化を自動的に実行する暗号化メカニズムが内蔵されたハードドライブです。このタイプの暗号化は、ユーザーに対して完全に透過的です。

シングルサインオン（SSO） - SSO は、起動前と Windows ログオンの両方で多因子認証が有効になっているとき、ログオン処理を簡素化します。有効になっている場合、認証は起動前のみで必要となり、ユーザーは Windows に自動的にログオンされます。有効ではない場合は、数回にわたる認証が必要となることがあります。

Trusted Platform Module（TPM） – TPM は、セキュアストレージ、測定、および構成証明という 3 つの主要機能を備えたセキュリティチップです。Encryption クライアントは、セキュアなストレージ機能のために TPM を使用します。TPM はまた、ソフトウェア資格情報コンテナ用に暗号化されたコンテナも提供できます。TPM は、ワンタイムパスワード機能の使用にも必須です。