

# HP Client Security

お使いになる前に

© Copyright 2013 Hewlett-Packard  
Development Company, L.P.

Bluetooth は、その所有者が所有する商標であり、使用許諾に基づいて Hewlett-Packard Company が使用しています。Intel は米国 Intel Corporation の米国およびその他の国における商標または登録商標であり、使用許諾に基づいて使用しています。Microsoft および Windows は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。

本書の内容は、将来予告なしに変更されることがあります。HP 製品およびサービスに関する保証は、当該製品およびサービスに付属の保証規定に明示的に記載されているものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。本書に記載されている製品情報は、日本国内で販売されていないものも含まれている場合があります。本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対して責任を負いかねますのでご了承ください。

初版：2013年8月

製品番号：735339-291

---

# 目次

<b>1 HP Client Security Manager の概要</b> .....	<b>1</b>
HP Client Security の機能 .....	1
HP Client Security 製品の説明と一般的な使用例 .....	2
Password Manager (パスワード マネージャー) .....	3
HP Drive Encryption (一部のモデルのみ) .....	3
HP Device Access Manager (一部のモデルのみ) .....	4
Computrace (別売) .....	4
主なセキュリティの目的の実現 .....	4
盗難からの保護 .....	5
機密データへのアクセス制限 .....	5
内部または外部からの不正なアクセスの防止 .....	5
強力なパスワード ポリシーの作成 .....	5
その他のセキュリティ対策 .....	6
セキュリティの役割の割り当て .....	6
HP Client Security パスワードの管理 .....	6
安全なパスワードの作成 .....	7
証明情報および設定のバックアップ .....	7
<b>2 お使いになる前に</b> .....	<b>8</b>
HP Client Security を開く .....	9
<b>3 HP ProtectTools for Small Business イージー セットアップ ガイド</b> .....	<b>10</b>
お使いになる前に .....	10
Password Manager (パスワード マネージャー) .....	10
Password Manager (パスワード マネージャー) に保存されている認証の表示および 管理 .....	11
HP Device Access Manager .....	11
HP Drive Encryption .....	11
<b>4 HP Client Security</b> .....	<b>12</b>
ユーザー認証の機能、アプリケーション、および設定 .....	12
指紋 .....	13
Fingerprints Administrative Settings (指紋の管理者設定) .....	13
Fingerprints User Settings (指紋のユーザー設定) .....	14

HP SpareKey : Password Recovery (パスワード復元) .....	14
HP SpareKey Settings .....	15
Windows password (Windows パスワード) .....	15
Bluetooth Devices (Bluetooth デバイス) .....	15
Bluetooth Devices Settings (Bluetooth デバイス設定) .....	16
Cards (カード) .....	16
Proximity, Contactless, and Smart Card Settings (近接型、非接触型、お よびスマート カード設定) .....	17
PIN .....	18
PIN の設定 .....	18
RSA SecurID .....	18
Password Manager .....	18
ログオン情報が作成されていない Web ページまたはプログラムの場合 .....	19
ログオン情報が作成されている Web ページまたはプログラムの場合 .....	19
ログオンの追加 .....	20
ログオンの編集 .....	21
HP Password Manager の[クイック リンク]メニューの使用 .....	21
ログオンをカテゴリ別に整理 .....	22
ログオンの管理 .....	22
パスワード強度の評価 .....	23
[Password Manager]アイコンの設定 .....	23
ログオンのインポートおよびエクスポート .....	24
設定 .....	25
詳細設定 .....	25
Administrator Policies (管理者ポリシー) .....	25
Standard User Policies (標準ユーザー ポリシー) .....	26
セキュリティ機能 .....	27
ユーザー .....	27
My Policies (マイ ポリシー) .....	28
データのバックアップおよび復元 .....	28
<b>5 HP Drive Encryption (一部のモデルのみ) .....</b>	<b>30</b>
Drive Encryption を開く .....	30
一般的なタスク .....	31
標準ハードドライブに対する Drive Encryption の有効化 .....	31
自己暗号化ドライブに対する Drive Encryption の有効化 .....	31
Drive Encryption の無効化 .....	32
Drive Encryption の有効化後のログイン .....	32
追加のハードドライブの暗号化 .....	33

高度なタスク .....	33
Drive Encryption の管理（管理者のタスク） .....	33
個々のドライブ パーティションの暗号化または暗号化の解除（ソフトウェアによる暗号化のみ） .....	34
ディスクの管理 .....	34
バックアップおよび復元（管理者のタスク） .....	34
暗号化キーのバックアップ .....	34
暗号化が有効になっているコンピューターでのバックアップ キーを使用したアクセスの復元 .....	35
HP SpareKey のリカバリの実行 .....	36
<b>6 HP File Sanitizer（一部のモデルのみ） .....</b>	<b>37</b>
シュレッド .....	37
空き領域ブリーチ .....	38
HP File Sanitizer の起動 .....	38
セットアップ手順 .....	39
シュレッド スケジュールの設定 .....	40
空き領域ブリーチのスケジュール設定 .....	41
ファイルがシュレッドされないように保護する .....	41
一般的なタスク .....	42
[File Sanitizer]アイコンの使用 .....	42
右クリック シュレッド .....	43
シュレッド操作の手動開始 .....	43
空き領域ブリーチの手動開始 .....	43
ログ ファイルの表示 .....	44
<b>7 HP Device Access Manager（一部のモデルのみ） .....</b>	<b>45</b>
HP Device Access Manager を開く .....	46
[ユーザー]ビュー .....	46
[システム]ビュー .....	46
ジャスト イン タイム認証の構成 .....	48
ユーザーまたはグループのジャスト イン タイム認証ポリシーの作成 .....	48
ユーザーまたはグループのジャスト イン タイム認証ポリシーの無効化 .....	48
設定 .....	49
管理されないデバイス クラス .....	49


<b>8 HP Trust Circles .....</b>	<b>51</b>
HP Trust Circles を開く .....	51
お使いになる前に .....	51
Trust Circle .....	52
トラスト サークルへのフォルダーの追加 .....	52
トラスト サークルへのメンバーの追加 .....	53
トラスト サークルへのファイルの追加 .....	53
暗号化されたフォルダー .....	54
トラスト サークルからのフォルダーの削除 .....	54
トラスト サークルからのファイルの削除 .....	54
トラスト サークルからのメンバーの削除 .....	54
トラスト サークルの削除 .....	55
設定の指定 .....	55
<b>9 盗難からの回復（一部のモデルのみ） .....</b>	<b>57</b>
<b>10 ローカライズされたパスワードの例外事項 .....</b>	<b>58</b>
パスワードが拒否された場合の対処方法 .....	58
電源投入時認証レベルおよび HP Drive Encryption レベルでの Windows IME の非サポート .....	58
サポートされている別のキーボード レイアウトを使用したパスワードの変更 .....	59
特別なキーの扱い .....	59
<b>用語集 .....</b>	<b>62</b>
<b>索引 .....</b>	<b>66</b>

# 1 HP Client Security Manager の概要

HP Client Security を使用すると、データ、デバイス、およびユーザー認証情報を保護して、お使いのコンピューターのセキュリティを強化できます。

コンピューターで利用可能なソフトウェア モジュールは、モデルによって異なる可能性があります。

HP Client Security ソフトウェア モジュールは、プリインストールまたはプリロードされている場合と、HP の Web サイトからダウンロードできる場合があります。詳しくは、<http://www.hp.com/jp/> を参照してください。

 **注記：** このガイドの操作手順は、該当する HP Client Security ソフトウェア モジュールがすでにインストールされていることを前提に書かれています。

## HP Client Security の機能


以下の表で、HP Client Security モジュールの主な機能を詳しく説明します。

モジュール	主要な機能
HP Client Security Manager	<p>管理者は、以下の機能を実行できます</p> <ul style="list-style-type: none"><li>• Windows®が起動する前のコンピューターを保護する</li><li>• 強力な認証を使用して Windows アカウントを保護する</li><li>• Web サイトやアプリケーションのログオン情報およびパスワードを管理する</li><li>• Windows オペレーティング システムのパスワードを簡単に変更する</li><li>• 指紋を利用してセキュリティと利便性を強化する</li><li>• 認証用のスマート カード、非接触型カード、または近接型カードをセットアップする</li><li>• 認証方法として Bluetooth®対応電話を使用する</li><li>• 認証を強化するための PIN を設定する</li><li>• ログオン ポリシーおよびセッション ポリシーを設定する</li><li>• プログラムのバックアップおよび復元を実行する</li><li>• アプリケーションを追加する (HP Drive Encryption、HP File Sanitizer、HP Trust Circles、HP Device Access Manager、HP Computrace など)</li></ul> <p>一般ユーザーは、以下の機能を実行できます</p> <ul style="list-style-type: none"><li>• 暗号化の状態の設定および Device Access Manager の設定を表示する</li><li>• Computrace を有効にする</li><li>• [オプション]および[バックアップおよび復元]オプションを設定する</li></ul>

モジュール	主要な機能
Password Manager(パスワードマネージャー)	<p>一般ユーザーは、以下の機能を実行できます</p> <ul style="list-style-type: none"> <li>• ユーザー名とパスワードを整理およびセットアップします</li> <li>• 強固なパスワードを作成して電子メールと Web アカウントのセキュリティを強化する。Password Manager は、この情報を自動的に入力して送信します</li> <li>• ユーザーの資格情報を自動的に記憶して適用するシングルサインオン機能を使用してログオン プロセスを効率化します</li> <li>• 安全性に疑問があるアカウントをマークし、同様の証明情報のあるアカウントを通知する</li> <li>• サポートされるブラウザーからログオン データをインポートする</li> </ul>
HP Drive Encryption (一部のモデルのみ)	<ul style="list-style-type: none"> <li>• ハードドライブをボリューム全体にわたって完全に暗号化します</li> <li>• データの暗号化解除やデータへのアクセスにブート前認証を強制します</li> <li>• 自己暗号化ドライブを有効にするオプションを表示します (一部のモデルのみ)</li> </ul>
HP Device Access Manager	<ul style="list-style-type: none"> <li>• IT 管理者が、ユーザー プロファイルに基づいてデバイスへのアクセスを制御できます</li> <li>• 不正なユーザーが外部のストレージ メディアを使用してデータを削除したり、外部のメディアからシステムにウイルスを侵入させたりできないようにします</li> <li>• 管理者が、特定の個人またはユーザーのグループに対して、通信デバイスへのアクセスを無効にできます</li> </ul>
HP Trust Circles	<ul style="list-style-type: none"> <li>• ファイルとドキュメントのセキュリティを提供する</li> <li>• ユーザーが指定したフォルダーに置かれたファイルを暗号化し、それらをトラスト サークル内で保護する</li> <li>• ファイルの使用および共有をトラスト サークルのメンバーに限定する</li> </ul>
盗難からの回復 (別売の Computrace)	<ul style="list-style-type: none"> <li>• 有効にするには、追跡契約およびトレース契約を別途購入する必要があります</li> <li>• フォルダーやファイルを安全に管理できます</li> <li>• ユーザー操作や、ソフトウェアとハードウェアの変更を監視します</li> <li>• ハードドライブが再フォーマットまたは交換されてもアクティブな状態を維持します</li> </ul>

## HP Client Security 製品の説明と一般的な使用例

HP Client Security 製品のほとんどは、パスワードを紛失したり、利用できなくなったり、忘れてしまった場合、または企業のセキュリティ部門が必要となった場合にコンピューターにアクセスするためのユーザー認証機能 (通常はパスワード) および管理バックアップ機能を搭載しています。

 **注記：** 一部の HP Client Security 製品は、データへのアクセスを制限するように設計されています。データの重要性が非常に高いためデータを紛失することより第三者の目に触れる危険にさらすことの方が懸念される場合には、データを暗号化する必要があります。すべてのデータは安全な場所にバックアップしておくことをおすすめします。



## Password Manager (パスワード マネージャー)

Password Manager は、ユーザー名およびパスワードを格納します。次の用途に使用できます。

- インターネット アクセスまたは電子メールのログイン名およびパスワードを保存する
- ユーザーを Web サイトまたは電子メールに自動的にログインさせる
- 認証を管理および整理する
- Web またはネットワーク資産を選択して、リンクに直接アクセスする
- 必要に応じて名前およびパスワードを表示する
- 安全性に疑問があるアカウントをマークし、同様の証明情報のあるアカウントを通知する
- サポートされるブラウザからログオン データをインポートする

**例 1:** ある大規模メーカーの購買担当者は、その企業の取引のほとんどをインターネットで行っています。また、ログイン情報が必要となるいくつかの人気 Web サイトにもよくアクセスします。この購買担当者は、セキュリティに十分注意しているため、アカウントごとに異なるパスワードを使用しています。購買部では、Password Manager を使用して、Web リンクごとに異なるユーザー名およびパスワードを設定することにしました。購買担当者が Web サイトのログオン画面にアクセスすると、Password Manager によって資格情報が自動的に提供されます。ユーザー名およびパスワードが表示されるようにしたい場合は、Password Manager で設定できます。

Password Manager は、認証を管理および編集するためにも使用できます。ユーザーは、このツールを使用して、Web またはネットワーク資産を選択し、リンクに直接アクセスできます。また、必要に応じてユーザー名およびパスワードを表示することもできます。

**例 2:** ある多忙な社員が、経理部全体を監督する立場に昇進しました。経理部では、多数のクライアントの Web アカウントに、それぞれ異なるログイン情報を使用してログオンする必要があります。このログイン情報は複数の社員で共有する必要があるため、機密保持が問題となります。そこで、すべての Web リンク、企業ユーザー名、およびパスワードを Password Manager 内で整理することにしました。整理を完了させ、Password Manager を他の社員に配布すれば、使用する資格情報を知らないでこれらの社員に Web アカウントを利用させることができます。

## HP Drive Encryption (一部のモデルのみ)

HP Drive Encryption は、コンピューターのハードドライブ全体またはセカンダリ ドライブ上にあるデータへのアクセスを制限するために使用できます。また、Drive Encryption は自己暗号化ドライブも管理できます。

**例 1:** ある医師が、自分のコンピューターのハードドライブにあるどのデータにも自分しかアクセスできないようにしたいと考えています。そこで、この医師は Drive Encryption を有効にし、Windows のログイン前にブート前認証が求められるようにしました。セットアップを完了すれば、オペレーティング システムの起動前にパスワードを入力しなければハードドライブにアクセスできなくなります。自己暗号化ドライブ オプションでデータを暗号化するように選択すれば、ドライブのセキュリティをさらに強化することもできます。

**例 2:** ある病院の経営者は、医師および承認されている人だけが、個人パスワードを共有することなく、自分たちのコンピューター内のデータにアクセスできるようにしたいと考えています。そこで、病院の IT 部門は、その経営者、医師、および承認されたすべての人を Drive Encryption ユーザーとして追加することにしました。これで、承認された人だけが個人のユーザー名およびパスワードを使用してコンピューターまたはドメインにログオンできるようになります。

## HP Device Access Manager（一部のモデルのみ）

HP Device Access Manager を使用すると、管理者は、ハードウェアへのアクセスを制限および管理できます。HP Device Access Manager を使用して、データのコピーが可能な USB フラッシュ ドライブへの不正なアクセスをブロックできます。また、CD/DVD ドライブへのアクセス、USB デバイスの制御、ネットワーク接続などを制限することもできます。たとえば、外部の業者が社内のコンピューターにアクセスできるようにすると同時に、その業者がデータを USB ドライブにコピーできないようにする必要がある場合が考えられます。

**例 1：**医薬品会社のあるマネージャーは、個人の医療記録と会社のデータを仕事でよく使用しています。他の社員もこのデータにアクセスする必要がありますが、そのデータが USB デバイスや他の外部ストレージ メディアによってコンピューターからコピーされないようにすることが大変重要です。ネットワークは安全ですが、コンピューターに CD ライターや USB ポートが搭載されているため、データがコピーされたり盗まれたりする可能性があります。そこで、このマネージャーは、HP Device Access Manager で CD ライターと USB ポートを無効にし、使用できないようにしました。たとえ USB コネクタをブロックしても、マウスおよびキーボードは引き続き動作します。

**例 2：**ある保険会社では、社員が自宅にある個人のソフトウェアをインストールしたり、個人のデータを読み込んだりできないようにしたいと考えています。ただし、一部の社員は、すべてのコンピューターで USB ポートにアクセスする必要があります。そこで、この会社の IT 管理者は、Device Access Manager を使用して、一部の社員に対してアクセスを許可すると同時に、その他の社員に対しては外部アクセスをブロックしました。

## Computrace（別売）

Computrace（別売）は、盗難されたコンピューターがインターネットに接続されればいつでもその所在地を追跡できるサービスです。Computrace を使用すると、コンピューターをリモートで管理および特定したり、コンピューターの使用状況やアプリケーションを監視したりできます。

**例 1：**ある学校の校長は、IT 部門に対し、学校にあるすべてのコンピューターを常時監視するように指示しました。そこで、学校の IT 管理者はコンピューターの保有状況を確認してから、すべてのコンピューターを Computrace に登録し、盗まれた場合に追跡できるようにしました。その後、この学校では、いくつかのコンピューターがなくなっていることに気づきました。そのため、IT 管理者は、警察に通報するとともに、Computrace の担当者に通知しました。これらのコンピューターは発見され、警察の手によって取り戻されて学校に返却されました。

**例 2：**ある不動産会社では、世界中にあるコンピューターの管理および更新が必要になりました。そこで、Computrace を使用して、IT 担当者を実際に現地に派遣しなくてもコンピューターの監視および更新が実行できるようにしました。

## 主なセキュリティの目的の実現

各 HP Client Security モジュールが連携して動作することによって、以下の主なセキュリティの目的を含む、さまざまなセキュリティの問題に対処するためのソリューションを提供できます。

- 盗難からの保護
- 機密データへのアクセス制限
- 内部または外部からの不正なアクセスの防止
- 強力なパスワード ポリシーの作成

## 盗難からの保護

盗難の例として、空港の検問所での、機密データや顧客情報を含むコンピューターの盗難が挙げられます。盗難からの保護には、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。
  - HP Client Security : [12 ページの「HP Client Security」](#)を参照してください。
  - HP Drive Encryption : [30 ページの「HP Drive Encryption \(一部のモデルのみ\)」](#)を参照してください。
- 暗号化は、ハードドライブが取り外されて、セキュリティ保護されていないシステムに取り付けられている場合でもデータにアクセスできないようにするために役立ちます。
- Computrace では、盗難の被害にあった後のコンピューターの場所を追跡できます。
  - Computrace : [57 ページの「盗難からの回復 \(一部のモデルのみ\)」](#)を参照してください。

## 機密データへのアクセス制限

契約監査官がオンサイトで作業していて、機密の財務データの確認のためにコンピューターへのアクセスを許可されているとします。ただし、この検査官がこれらのファイルを印刷したり、CD などの書き込み可能なデバイスに保存できるようにはしたくありません。データへのアクセスを制限するには、以下の機能が役立ちます。

- HP Device Access Manager を使用すると、IT 管理者は、機密情報をハードドライブからコピーできないように、通信デバイスへのアクセスを制限できます。[46 ページの「\[システム\]ビュー」](#)を参照してください。

## 内部または外部からの不正なアクセスの防止

セキュリティ保護されていないコンピューターへの不正なアクセスは、金融サービス、役員、または研究開発チームからのデータなどの社内ネットワーク リソースや、患者記録や個人の財務データなどの個人情報を非常に大きなリスクにさらすこととなります。不正なアクセスを防止するには、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。(30 ページの「[HP Drive Encryption \(一部のモデルのみ\)」](#)を参照してください)。
- HP Client Security は、不正なユーザーがパスワードを入手したり、パスワードで保護されたアプリケーションにアクセスしたりできないようにするために役立ちます。[12 ページの「HP Client Security」](#)を参照してください。
- HP Device Access Manager を使用すると、IT 管理者は、機密情報をハードドライブからコピーできないように、書き込み可能なデバイスへのアクセスを制限できます。[45 ページの「HP Device Access Manager \(一部のモデルのみ\)」](#)を参照してください。


## 強力なパスワード ポリシーの作成

いくつかの Web ベースのアプリケーションやデータベースに対して強力なパスワード ポリシーを使用する必要が生じた場合、Password Manager (パスワード マネージャー) で、パスワードやシングルサインオンのための保護されたリポジトリが提供されます。[18 ページの「Password Manager」](#)を参照してください。

# その他のセキュリティ対策


## セキュリティの役割の割り当て

コンピューターのセキュリティを（特に、大きな組織で）管理する上では、責任および権限をさまざまな管理者やユーザーに割り当てるのが重要な作業の1つです。


 **注記：** 小さな組織や個人で使用する場合は、一人の人がすべての役割を受け持つこともできます。

HP Client Security では、セキュリティの責任および権限を以下のように分けられます。

- セキュリティ統括責任者：企業またはネットワークのセキュリティ レベルを定義し、Drive Encryption などの配備するセキュリティ機能を決定します。

 **注記：** HP Client Security の機能の多くは、セキュリティ統括責任者が HP と協力してカスタマイズできます。詳しくは、<http://www.hp.com/jp/> を参照してください。

- IT 管理者：セキュリティ統括責任者によって定義されたセキュリティ機能を適用し、管理します。また、一部の機能を有効または無効にできます。たとえば、セキュリティ統括責任者がスマート カードの配備を決定した場合、IT 管理者はパスワード モードおよびスマート カードモードの両方を有効にできます。
- ユーザー：セキュリティ機能を使用します。たとえば、セキュリティ統括責任者および IT 管理者がシステムでスマート カードを有効にしている場合、ユーザーはスマート カードの PIN を設定し、そのカードを認証に使用できます。

 **注意：** 管理者は、エンド ユーザーの権限の制限や、ユーザー アクセスの制限に関して「ベスト プラクティス」に従うことをおすすめします。

権限のないユーザーには管理者権限を付与しないでください。

## HP Client Security パスワードの管理

HP Client Security の機能のほとんどは、パスワードによってセキュリティ保護されています。以下の表に、よく使用されるパスワード、そのパスワードが設定されるソフトウェア モジュール、およびパスワード機能の一覧を示します。

この表には、IT 管理者のみが設定して使用するパスワードも示されています。その他のすべてのパスワードは、一般のユーザーまたは管理者が設定できます。

HP Client Security パスワード	設定するモジュール	機能
Windows のログオン パスワード	Windows の[コントロール パネル]または HP Client Security	HP Client Security のさまざまな機能にアクセスするための手動ログオンまたは認証に使用できます
HP Client Security の[バックアップおよび復元]パスワード	HP Client Security (ユーザーごと)	HP Client Security の[バックアップおよび復元]ファイルへのアクセスを保護します
スマート カードの PIN	Credential Manager (資格情報マネージャー)	マルチファクター認証として使用できます Windows 認証として使用できます スマート カードが選択されている場合は、Drive Encryption のユーザーを認証します

## 安全なパスワードの作成

パスワードを作成する場合は、まず、プログラムで設定されている仕様に従う必要があります。ただし一般的には、強力なパスワードを作成し、そのパスワードが危険にさらされないようにするために、以下のガイドラインを参考にしてください。

- 文字数が6文字、できれば8文字を超えるパスワードを使用します。
- パスワード全体にわたって大文字と小文字を混在させます。
- 可能な場合は、常に半角アルファベットと半角数字を混在させ、さらに特殊文字と句読点を含めます。
- パスワード中の文字の代わりに特殊文字または数字を使用します。たとえば、アルファベットのIまたはLの代わりに数字の1を使用します。
- 2つ以上の言語から取った単語を組み合わせてみます。
- 単語またはフレーズを数字や特殊文字で分けます。たとえば、「Mary2-2Cat45」とします。
- 辞書に載っているような用語は使用しないでください。
- 名前やその他の個人情報（たとえば、誕生日、ペットの名前、母親の旧姓など）は、たとえ綴りを逆にしたとしても、パスワードには使用しないでください。
- パスワードは定期的に変更してください。いくつかの文字や数字を以下の値に変更するだけでも構いません。
- パスワードをメモした場合は、コンピューターのすぐ近くの、人目につきやすい場所に保管しないでください。
- パスワードを、電子メールなどのコンピューター上のファイルに保存しないでください。
- アカウントを共有したり、パスワードを誰かに教えたりしないでください。


## 証明情報および設定のバックアップ

インストール済みのいくつかの HP Client Security モジュールからのセキュリティ証明書をバックアップし、復元するための中心となる場所として、HP Client Security のバックアップおよび復元ツールを使用できます。




## 2 お使いになる前に

自分の資格情報を使用するように HP Client Security を設定するには、以下の方法で HP Client Security を起動します。一度ウィザードを完了してしまったユーザーは、以後、ウィザードを起動することはできません。


1. スタート画面またはアプリ画面で **[HP Client Security]** アプリケーションをクリックまたはタップします (Windows 8)。  
または  
Windows デスクトップで、**[HP Client Security]** ガジェットをクリックまたはタップします (Windows 7)。  
または  
Windows デスクトップで、タスクバーの右端の通知領域にある **[HP Client Security]** アイコンをダブルクリックまたはダブルタップします。  
または  
Windows デスクトップで、通知領域にある **[HP Client Security]** アイコンをクリックまたはタップしてから、**[Open HP Client Security]** (HP Client Security を開く) を選択します。
  2. HP Client Security セットアップ ウィザードが起動し、[ようこそ] ページが表示されます。
  3. [ようこそ] 画面の説明を読んでから、Windows パスワードを入力してユーザー認証を行い、**[次へ]** をクリックまたはタップします。  
Windows パスワードをまだ作成していない場合は、作成するよう求められます。お使いの Windows アカウントが第三者から不正にアクセスされないようにするために、また HP Client Security の機能を使用するためには、Windows パスワードが必要です。
  4. [HP SpareKey] ページで、セキュリティに関する質問を 3 つ選択します。各質問の回答を入力し、**[次へ]** をクリックします。ユーザー自身で質問を作成することもできます。詳しくは、[14 ページの「HP SpareKey : Password Recovery \(パスワード復元\)」](#) を参照してください。
  5. [指紋] ページで、最小限数以上の指紋を登録し、**[次へ]** をクリックまたはタップします。詳しくは、[13 ページの「指紋」](#) を参照してください。
  6. [Drive Encryption] ページで、暗号化を有効にし、暗号化キーをバックアップして、**[次へ]** をクリックまたはタップします。詳しくは、HP Drive Encryption ソフトウェアのヘルプを参照してください。
- 
-  **注記:** この作業が必要になるのは、ユーザーが管理者で、管理者がこれまで HP Client Security セットアップ ウィザードを実行したことがない場合のみです。
- 
7. ウィザードの最後のページで、**[完了]** をクリックまたはタップします。  
このページで、機能および資格情報の状態を確認します。
  8. HP Client Security セットアップ ウィザードによって、ジャスト イン タイム認証および HP File Sanitizer の機能が有効になっていることが確認されます。詳しくは、HP Device Access

Manager ソフトウェアのヘルプおよび HP File Sanitizer ソフトウェアのヘルプを参照してください。

 **注記:** この作業が必要になるのは、ユーザーが管理者で、管理者がこれまで HP Client Security セットアップ ウィザードを実行したことがない場合のみです。

## HP Client Security を開く

HP Client Security アプリケーションは以下のどれかの方法で開くことができます。

 **注記:** HP Client Security アプリケーションを起動するには、先に HP Client Security セットアップ ウィザードを完了する必要があります。

- ▲ スタート画面またはアプリ画面で **[HP Client Security]** アプリケーションをクリックまたはタップします。

または

Windows デスクトップで、**[HP Client Security]** ガジェットをクリックまたはタップします (Windows 7)。

または

Windows デスクトップで、タスクバーの右端の通知領域にある **[HP Client Security]** アイコンをダブルクリックまたはダブルタップします。

または

Windows デスクトップで、通知領域にある **[HP Client Security]** アイコンをクリックまたはタップしてから、**[Open HP Client Security]** (HP Client Security を開く) を選択します。

## 3 HP ProtectTools for Small Business イージー セットアップ ガイド

この章は、HP Client Security for Small Business 内の最も一般的で、かつ最も役立つオプションを有効にするための基本的な手順を示すように設計されています。このソフトウェアには、設定を微調整したり、アクセス制御を設定したりするために使用できる多数のツールやオプションが含まれています。このイージー セットアップ ガイドは、各モジュールを最小限の設定作業および時間で動作させることに重点を置いています。より詳しい情報を表示するには、対象のモジュールを選択し、右上隅にある[?]ボタンまたは[ヘルプ]ボタンを選択します。このボタンを選択した時に表示されているウィンドウでの作業に役立つ情報が自動的に表示されます。

### お使いになる前に

1. Windows デスクトップで、タスクバーの右端の通知領域にある[HP Client Security]アイコンをダブルクリックして HP Client Security を開きます。
2. Windows パスワードを入力するか、作成します。
3. HP Client Security セットアップを完了します。

Windows ログイン中に HP Client Security によって 1 回のみ認証されるようにする方法については、[27 ページの「セキュリティ機能」](#)を参照してください。

### Password Manager (パスワード マネージャー)

どのユーザーも多数のパスワードを使用します。定期的に Web サイトにアクセスしたり、ログオンの必要なアプリケーションを使用している場合は特にそうです。一般的なユーザーは、すべてのアプリケーションおよび Web サイトに同じパスワードを使用したり、パスワードの作成に凝っても、どのパスワードがどのアプリケーションのものかすぐに忘れてしまったりします。

Password Manager を使用すると、パスワードを自動的に記憶させるか、またはパスワードを記憶するサイトと省略するサイトをユーザーが識別できるようになります。コンピューターにサインオンした後は、登録されているアプリケーションまたは Web サイトのパスワードまたは資格情報が Password Manager によって提供されます。

資格情報が必要な任意のアプリケーションまたは Web サイトにアクセスすると、Password Manager がそのサイトを自動的に認識し、ユーザーの情報をソフトウェアで記憶するかどうかをユーザーに尋ねます。特定のサイトを除外したい場合は、ユーザーの情報を記憶するという要求を辞退できます。

Web の場所、ユーザー名、およびパスワードの保存を開始するには、以下の操作を行います。

1. 登録されている Web サイトやアプリケーションなどにアクセスして、Web ページの左上隅にある>Password Manager]アイコンをクリックし、Web 認証を追加します。
2. リンクに名前を付け (オプション)、Password Manager にユーザー名およびパスワードを入力します。
3. 完了したら、[OK]ボタンをクリックします。
4. Password Manager には、ネットワーク共有またはネットワーク ドライブの割り当てのためのユーザー名およびパスワードを保存することもできます。



## Password Manager (パスワード マネージャー) に保存されている認証の表示および管理

Password Manager を使用すると、中心となる場所から認証を表示、管理、バックアップ、および起動できます。また、Password Manager では、保存されているサイトの Windows からの起動もサポートされます。

Password Manager を開くには、**ctrl** キー + **Windows** ロゴ キー + **h** ホット キーを使用します。[**ログイン データの入力**]をクリックすると、保存されているショートカットがすばやく起動され、認証されます。

Password Manager の[**編集**]オプションを使用すると、名前とログイン名を表示および変更できるほか、パスワードを表示することもできます。

HP Client Security for Small Business では、すべての証明情報および設定を別のコンピューターにバックアップしたり、コピーしたりできます。

## HP Device Access Manager

HP Device Access Manager を使用すると、データがハードドライブ上に安全な状態で残り、会社の外部に持ち出されることがないように、さまざまな内蔵および外付けストレージ デバイスの使用を制限できます。たとえば、あるユーザーにデータへのアクセスは許可するものの、CD、個人用音楽プレーヤー、または USB メモリ デバイスへのコピーをブロックとします。

1. Device Access Manager を開きます ([46 ページの「HP Device Access Manager を開く」](#)を参照してください)。  
現在のユーザーのアクセスが表示されます。
2. ユーザー、グループ、またはデバイスのアクセスを変更するには、[**変更**]をクリックまたはタップします。詳しくは、[46 ページの「\[システム\]ビュー」](#)を参照してください。

## HP Drive Encryption

HP Drive Encryption を使用すると、ハードドライブ全体を暗号化することによってデータを保護できます。コンピューターが盗まれたり、ハードドライブが元のコンピューターから取り外されて異なるコンピューターに接続されたりしたとしても、ハードドライブのデータは保護されたままになります。

また、Drive Encryption を使用すると、オペレーティング システムを起動する前にユーザー名とパスワードを使用して適切な認証をすることが必要になるため、セキュリティが強化されます。このプロセスはブート前認証と呼ばれます。

作業が簡単に実行できるように、Windows ユーザー アカウント、認証ドメイン、HP Drive Encryption、Password Manager、HP Client Security などさまざまなソフトウェア モジュールでパスワードが自動的に同期されます。

HP Client Security セットアップ ウィザードによる初期セットアップ時に HP Drive Encryption を設定する方法については、[8 ページの「お使いになる前に」](#)を参照してください。

## 4 HP Client Security

HP Client Security の[ホーム]ページは、HP Client Security の機能、アプリケーション、および設定に簡単にアクセスするための中心となる場所です。[ホーム]ページは以下の 3 つのセクションに分かれています。

- **[データ]** : データのセキュリティを管理するためのアプリケーションにアクセスします。
- **[デバイス]** : デバイスのセキュリティを管理するためのアプリケーションにアクセスします。
- **[認証情報]** : 認証資格情報を登録および管理します。

アプリケーションのタイルの上にカーソルを置くと、そのアプリケーションの説明が表示されます。

ページの下部に、ユーザー設定および管理者設定へのリンクが表示されることがあります。ギアの絵の**[設定]**アイコンをタップまたはクリックすると、詳細設定および機能にアクセスできます。

### ユーザー認証の機能、アプリケーション、および設定

HP Client Security で提供されるユーザー認証の機能、アプリケーション、および設定を使用して、ユーザーのデジタル ID をさまざまな面から管理できます。HP Client Security の[ホーム]ページで以下のタイルのどれかをクリックまたはタップして、Windows パスワードを入力します。

- **[指紋]** : 指紋による資格情報を登録および管理します。
- **[SpareKey]** : HP SpareKey による資格情報を設定および管理します。この資格情報は、他の資格情報を紛失してしまった場合にコンピューターにログオンするために使用できます。また、パスワードを忘れてしまった場合にリセットするためにも使用できます。
- **[Windows Password]** (Windows パスワード) : Windows のパスワードを簡単に変更できます。
- **[Bluetooth Devices]** (Bluetooth デバイス) : Bluetooth デバイスを登録および管理できます。
- **[Cards]** (カード) : スマート カード、非接触型カード、および近接型カードを登録および管理できます。
- **[PIN]** : PIN による資格情報を登録および管理できます。
- **[RSA SecurID]** : RSA SecurID による資格情報を登録および管理できます (事前に適切にセットアップしておく必要があります)。
- **[Password Manager]** (HP Password Manager) : オンライン アカウントおよびアプリケーションのパスワードを管理できます。

## 指紋

HP Client Security セットアップ ウィザードでは、指紋の設定、つまり「登録」ができます。

[指紋]ページでは、指紋の登録のほかに削除もできます。[指紋]ページにアクセスするには、HP Client Security の[ホーム]ページで[指紋]アイコンをクリックまたはタップします。

1. [指紋]ページで、指紋が正常に登録されるまで指を滑らせます。  
このページには、登録する必要のある指の数が示されます。人差し指または中指の登録をおすすめします。
2. 以前に登録した指紋を削除するには、[削除]をクリックまたはタップします。
3. 指紋を追加登録するには、[Enroll an additional fingerprint]（追加の指紋の登録）をクリックまたはタップします。
4. [保存]をクリックまたはタップして、ページを閉じます。

**△ 注意：** ウィザードで指紋を登録するときは、[次へ]をクリックするまで指紋の情報は保存されません。コンピューターをしばらくアイドル状態にしていた場合や、プログラムを閉じた場合は、それ以前に行った変更が保存されません。

- ▲ [Fingerprints Administrative Settings]（指紋の管理者設定）では、管理者が登録、精度、その他の設定を指定できます。このページにアクセスするには、[Administrative Settings]（管理者設定）をクリックまたはタップします（管理者権限が必要です）。
- ▲ [Fingerprints User Settings]（指紋のユーザー設定）では、指紋認識の表示および動作に関する設定を指定できます。このページにアクセスするには、[User Settings]（ユーザー設定）をクリックまたはタップします。

### Fingerprints Administrative Settings（指紋の管理者設定）

管理者は、指紋認証システムの登録、精度、その他の設定を指定できます。操作には管理者権限が必要です。

- ▲ 指紋資格情報の管理者設定にアクセスするには、[指紋]ページで[Administrative Settings]（管理者設定）をクリックまたはタップします。
- [User enrollment]（ユーザー登録）：ユーザーが登録できる指紋の最小数および最大数を選択します。
- [Recognition]（認識）：スライダーを動かして、指紋認証システムでの指紋の読み取り感度を調整します。

指紋が認識されないことがある場合は、認識設定を低くしてみてください。この設定を高くすると指紋の読み取りの変化に対する感度が向上するため、誤って受け入れられる可能性が減ります。[中-高]に設定すると、セキュリティおよび利便性の適切な組み合わせが得られます。

## Fingerprints User Settings (指紋のユーザー設定)

[Fingerprints User Settings] (指紋のユーザー設定) ページでは、指紋認識の表示および動作に関する設定を指定できます。

- ▲ 指紋資格情報のユーザー設定にアクセスするには、[指紋]ページで[User Settings] (ユーザー設定) をクリックまたはタップします。
- [サウンド フィードバックを有効にする] : 初期設定では、指紋が読み取られたときに、サウンドによるフィードバックが返されます。プログラム イベントごとに異なるサウンドが再生されます。Windows の[コントロール パネル]にある[サウンド]設定の[サウンド]タブで、これらのイベントに新しいサウンドを割り当てることができます。サウンドのフィードバックを無効にする場合は、このチェック ボックスのチェックを外します。
- [スキャン品質のフィードバックを表示] : 品質に関係なくすべての読み取りを表示するには、このチェック ボックスにチェックを入れます。高品質の読み取りのみを表示するには、このチェック ボックスのチェックを外します。

## HP SpareKey : Password Recovery (パスワード復元)

HP SpareKey を使用すると、セキュリティに関する 3 つの質問に回答することによって、サポートされているプラットフォーム上のコンピューターにアクセスできます。

HP Client Security セットアップ ウィザードの初期セットアップ時に、個人用の HP SpareKey をセットアップするよう求めるメッセージが表示されます。

HP SpareKey をセットアップするには、以下の操作を行います。

1. ウィザードの[HP SpareKey]ページで、セキュリティに関する質問を 3 つ選択し、各質問の回答を入力します。  
あらかじめ定義されている質問を選択することも、独自の質問を作成することもできます。
2. [登録] をクリックまたはタップします。

HP SpareKey を削除するには、以下の操作を行います。

- ▲ [[HP SpareKey]の削除] をクリックまたはタップします。

HP SpareKey をセットアップした後は、電源投入時認証ログオン画面または Windows の[ようこそ]画面から HP SpareKey を使用してコンピューターにアクセスできます。

[SpareKey]ページでは、別の質問を選択したり、回答を変更したりできます。このページにアクセスするには、HP Client Security の[ホーム]ページで[Password Recovery] タイルをクリックまたはタップします。

[HP SpareKey Settings] (HP SpareKey 設定) では、管理者が HP SpareKey 資格情報に関する設定を指定できます。このページにアクセスするには、[設定] をクリックします (管理者権限が必要です)。

## HP SpareKey Settings

[HP SpareKey Settings]ページでは、HP SpareKey 資格情報の動作および使用に関する設定を指定できます。

- ▲ [HP SpareKey Settings]ページにアクセスするには、[HP SpareKey]ページで**[設定]**をクリックまたはタップします（管理者権限が必要です）。

管理者は、以下の設定ができます。

- 各ユーザーが HP SpareKey をセットアップするときに表示されるセキュリティに関する質問を指定する。
- ユーザーに表示されるセキュリティに関する質問の一覧に独自の質問を追加する（最大3つ）。
- ユーザーがセキュリティに関する質問を独自に作成できるようにするかどうかを選択する。
- HP SpareKey によってパスワードを復元できるようにする認証環境（Windows 認証または電源投入時認証）を選択する。

## Windows password (Windows パスワード)

HP Client Security を使用すると、Windows の[コントロール パネル]を使用するよりもすばやく簡単に Windows パスワードを変更できます。

Windows パスワードを変更するには、以下の操作を行います。

1. HP Client Security の[ホーム]ページで、**[Windows Password]**をクリックまたはタップします。
2. **[現在の Windows パスワード]**テキスト ボックスに、現在のパスワードを入力します。
3. **[新しい Windows パスワード]**テキスト ボックスに新しいパスワードを入力し、**[新しいパスワードの確認]**テキスト ボックスにそのパスワードを再度入力します。
4. **[変更]**をクリックまたはタップします。現在のパスワードが、入力した新しいパスワードにすぐに変更されます。

## Bluetooth Devices (Bluetooth デバイス)

管理者が認証資格情報として Bluetooth を有効にしている場合は、セキュリティ強化のために他の資格情報と組み合わせて Bluetooth 対応電話を設定できます。

 **注記：** Bluetooth 対応の電話デバイスのみがサポートされています。

1. Bluetooth 機能がコンピューターで有効になっていること、および Bluetooth 対応電話が検出モードに設定されていることを確認します。電話を接続するには、自動生成されたコードを Bluetooth デバイスで入力することが必要になる場合があります。Bluetooth デバイスの構成設定によっては、コンピューターと電話のペアリング コードを比較することが必要になる場合があります。
2. 電話を登録するには、その電話を選択して、**[登録]**をクリックまたはタップします。

[[16 ページの「Bluetooth Devices Settings \(Bluetooth デバイス設定\)」](#)]ページでは、管理者が Bluetooth デバイスに関する設定を指定できます。このページにアクセスするには、**[設定]**をクリックします（管理者権限が必要です）。

## Bluetooth Devices Settings (Bluetooth デバイス設定)


管理者は、Bluetooth デバイス資格情報の動作および使用に関する以下の設定を指定できます。

### Silent Authentication (サイレント認証)

- **[Automatically use your connected enrolled Bluetooth Device during verification of your identity]** (ユーザー認証時に接続されている登録済み Bluetooth デバイスを自動的に使用する): ユーザーがユーザー認証時に特に何も操作をしないで Bluetooth 資格情報を使用できるようにする場合は、このチェック ボックスにチェックを入れます。このオプションを無効にする場合は、チェック ボックスのチェックを外します。

### Bluetooth Proximity (Bluetooth の近接)

- **[Lock computer when your enrolled Bluetooth device moves out of range of your computer]** (登録済み Bluetooth デバイスがコンピューターとの通信範囲から出たときにコンピューターをロックする): ログイン時に接続されていた Bluetooth デバイスがコンピューターとの通信範囲から出たときにコンピューターをロックする場合は、このチェック ボックスにチェックを入れます。このオプションを無効にする場合は、チェック ボックスのチェックを外します。

 **注記:** この機能を使用するには、コンピューターに搭載されている Bluetooth モジュールでこの機能がサポートされている必要があります。

## Cards (カード)

HP Client Security では、幅広い種類の認証用カード (コンピューター チップが埋め込まれた小型のプラスチックのカード) がサポートされています。これには、スマート カード、非接触型カード、および近接型カードが含まれます。適切なカード リーダーをコンピューターに接続し、製造元から提供された対応ドライバーを管理者がインストールして、認証資格情報としてカードを有効にすることで、これらのカードを認証資格情報として使用できます。

スマート カードの場合は、通常、HP Client Security でセキュリティ アルゴリズムに使用されるセキュリティ証明書および PIN 管理機能のインストール ツールが製造元から提供されます。PIN として使用できる文字の数および種類は製造元によって異なります。スマート カードを使用するには、管理者が事前にスマート カードを初期化する必要があります。

HP Client Security では、以下の形式のスマート カードをサポートしています。

- CSP
- PKCS11

HP Client Security では、以下の種類の非接触型カードをサポートしています。

- 非接触型 HID iCLASS メディア カード
- 非接触型 MiFare Classic 1k、4k、および小型メディア カード

HP Client Security では、以下の近接型カードをサポートしています。

- HID 近接型カード

スマート カードを登録するには、以下の操作を行います。

1. スマート カード リーダーを接続してカードを挿入します。
2. カードが認識されたら、カードの PIN を入力して、**[登録]** をクリックまたはタップします。



スマート カードの PIN を変更するには、以下の操作を行います。

1. スマート カード リーダーを接続してカードを挿入します。
2. カードが認識されたら、カードの PIN を入力して、**[認証]**をクリックまたはタップします。
3. **[PIN の変更]**をクリックまたはタップして、新しい PIN を入力します。

非接触型カードまたは近接型カードを登録するには、以下の操作を行います。

1. カードを適切なリーダーの上またはすぐ近くに置きます。
2. カードが認識されたら、**[登録]**をクリックまたはタップします。

登録済みのカードを削除するには、以下の操作を行います。

1. カードをリーダーに認識させます。
2. スマート カードの場合は、カードに割り当てられた PIN を入力して、**[認証]**をクリックまたはタップします。
3. **[削除]**をクリックまたはタップします。

カードを登録すると、**[Enrolled Cards]**（登録済みカード）の下にそのカードの詳細が表示されます。カードを削除すると、この一覧からも削除されます。

[Proximity, Contactless, and Smart Card Settings]（近接型、非接触型、およびスマート カード設定）では、管理者がカード資格情報に関する設定を指定できます。このページにアクセスするには、**[設定]**をクリックまたはタップします（管理者権限が必要です）。

## Proximity, Contactless, and Smart Card Settings（近接型、非接触型、およびスマートカード設定）

カードの設定にアクセスするには、一覧でカードをクリックまたはタップしてから、表示される矢印をクリックまたはタップします。

スマート カードの PIN を変更するには、以下の操作を行います。

1. カードをリーダーに認識させます。
2. カードに割り当てられた PIN を入力して、**[続行]**をクリックまたはタップします。
3. 新しい PIN を入力し、確認のためにもう一度入力して、**[続行]**をクリックまたはタップします。

スマート カードの PIN を初期化するには、以下の操作を行います。

1. カードをリーダーに認識させます。
2. カードに割り当てられた PIN を入力して、**[続行]**をクリックまたはタップします。
3. 新しい PIN を入力し、確認のためにもう一度入力して、**[続行]**をクリックまたはタップします。
4. 初期化の実行を確認されたら**[はい]**をクリックまたはタップします。

カードのデータを消去するには、以下の操作を行います。

1. カードをリーダーに認識させます。
2. カードに割り当てられた PIN を入力して（スマート カードの場合のみ）、**[続行]**をクリックまたはタップします。
3. 削除の実行を確認されたら**[はい]**をクリックまたはタップします。

## PIN

管理者が認証資格情報として PIN を有効にしている場合は、セキュリティ強化のために他の資格情報と組み合わせて PIN を設定できます。

新しい PIN をセットアップするには、以下の操作を行います。

- ▲ PIN を入力し、確認のためにもう一度入力して、**[適用]**をクリックまたはタップします。

PIN を削除するには、以下の操作を行います。

- ▲ **[削除]**をクリックまたはタップし、削除の実行を確認されたら**[はい]**をクリックまたはタップします。


[PIN の設定]では、管理者が PIN 資格情報に関する設定を指定できます。このページにアクセスするには、**[設定]**をクリックまたはタップします（管理者権限が必要です）。

## PIN の設定

[PIN の設定]ページでは、PIN 資格情報に使用できる最小文字数および最大文字数を指定できます。

## RSA SecurID

管理者が認証資格情報として RSA を有効にし、以下の条件を満たしている場合は、RSA SecurID 資格情報を登録または削除できます。

 **注記：** 適切にセットアップしておく必要があります。

- RSA サーバーにユーザーが作成されている。
- ユーザーおよびコンピューターに割り当てられた RSA SecurID トークンが RSA サーバー ドメインに参加している。
- コンピューターに SecurID ソフトウェアがインストールされている。
- 適切に設定された RSA サーバーに接続できる。

RSA SecurID 資格情報を登録するには、以下の操作を行います。

- ▲ RSA SecurID のユーザー名およびパスコード（環境によって、RSA SecurID トークン コード、または PIN およびトークンコードが該当）を入力して、**[適用]**をクリックまたはタップします。

正しく登録されると、[Your RSA SecurID credential has been successfully enrolled] (RSA SecurID 資格情報が正しく登録されました) というメッセージが表示され、**[削除]**ボタンが有効になります。


RSA SecurID 資格情報を削除するには、以下の操作を行います。

- ▲ **[削除]**をクリックし、[Are you sure you want to delete your RSA SecurID credential?] (RSA SecurID 資格情報を削除してよろしいですか?) と尋ねるダイアログが表示されたら**[はい]**を選択します。

## Password Manager

HP Password Manager を使用すると、Web サイトおよびアプリケーションへのログオンがより簡単かつ安全になります。強固なパスワードを作成しておき、実際のログインは、指紋、スマートカード、近接型カード、非接触型カード、Bluetooth 対応電話、PIN、RSA 資格情報、または Windows パスワードを使用すればやく簡単に行えます。パスワードを書き留めたり覚えたりする必要もありません。



 **注記：** Web のログオン画面の構造は絶えず変化しているため、HP Password Manager で常にすべての Web サイトがサポートされるわけではありません。

HP Password Manager には以下のオプションがあります。

### [Password Manager] (HP Password Manager) ページ

- アカウントをクリックまたはタップして、自動的に Web ページまたはアプリケーションを開いてログオンする。
- アカウントをカテゴリごとに整理する。

### パスワード強度

- セキュリティ上のリスクがあるパスワードがあるかどうかを確認する。
- ログイン データの追加時に、Web サイトおよびアプリケーションに使用されている各パスワードの強度を確認する。
- パスワード強度は、赤色、黄色、または緑色の状態インジケータで表される。

[Password Manager] アイコンは、Web ページまたはアプリケーションのログオン画面の左上隅に表示されます。Web サイトまたはアプリケーション用のログオン情報が作成されていない場合は、プラス記号 (+) がアイコン上に表示されます。

▲ [Password Manager] アイコンをクリックまたはタップしてコンテキスト メニューを表示すると、以下のオプションを選択できます。

- [任意のドメイン] をパスワード マネージャーに追加
- [HP Password Manager] を開く
- アイコンの設定
- ヘルプ

### ログオン情報が作成されていない Web ページまたはプログラムの場合

以下のオプションがコンテキスト メニューに表示されます。


- [[任意のドメイン] をパスワード マネージャーに追加] : 表示中のログオン画面のログオン情報を追加できます。
- [[パスワード マネージャー] を開く] : HP Password Manager を起動します。
- [アイコンの設定] : [Password Manager] アイコンを表示する条件を指定できます。
- [ヘルプ] : HP Client Security のヘルプを表示します。

### ログオン情報が作成されている Web ページまたはプログラムの場合

以下のオプションがコンテキスト メニューに表示されます。

- [ログオン データの入力] : [ID の検証] ページを表示します。正しく認証されると、ログオン データがログオン用フィールドに入力され、ページが送信されます (ログオン データを作成または最後に編集したときに送信を指定していた場合)。
- [ログオンの編集] : 表示中の Web サイト用のログオン データを編集できます。
- [ログオンの追加] : アカウントを HP Password Manager に追加できます。

- **[パスワード マネージャー]を開く** : HP Password Manager を起動します。
- **[ヘルプ]** : HP Client Security のヘルプを表示します。

 **注記:** コンピューターの管理者によって、ユーザー認証時に複数の資格情報を入力するように設定されていることがあります。

## ログオンの追加

Web サイトまたはプログラム用のログオンは、ログオン情報を 1 回入力すれば、簡単に追加できます。以降は、HP Password Manager によって情報が自動的に入力されるようになります。該当する Web サイトにアクセスするかプログラムを開くと、追加したログオンを使用できます。

ログオンを追加するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. **[Password Manager]** アイコンをクリックまたはタップし、ログオン画面の種類（Web サイト用またはプログラム用）に応じて以下のどちらかをクリックまたはタップします。
  - Web サイトの場合は、**[[任意のドメイン]をパスワード マネージャーに追加]** をクリックまたはタップします。
  - プログラムの場合は、**[Add this logon screen to Password Manager]**（このログオン画面を Password Manager に追加） をクリックまたはタップします。
3. ログオン データを入力します。画面のログオン用フィールドおよびダイアログ ボックスの対応するフィールドが、オレンジ色の太い枠線で識別されます。
  - a. あらかじめフォーマットが用意された選択肢の 1 つを使用してログオン用フィールドに入力するには、フィールドの右側にある矢印をクリックまたはタップします。
  - b. このログオン用のパスワードを表示するには、**[パスワードの表示]** をクリックまたはタップします。
  - c. ログオン用フィールドの入力後に送信を実行しない場合は、**[ログオン データを自動的に送信する]** チェック ボックスのチェックを外します。
  - d. **[OK]** をクリックまたはタップして、使用する認証方法（指紋、スマート カード、近接型カード、非接触型カード、Bluetooth 対応電話、PIN、またはパスワード）を選択し、選択した認証方法を使用してログオンします。

**[Password Manager]** アイコンのプラス記号（+）が消え、ログオン情報が作成されたことが示されます。
  - e. HP Password Manager でログオン用フィールドが検出されない場合は、**[その他のフィールド]** をクリックまたはタップします。
    - ログオンに必要な各フィールドのチェック ボックスにチェックを入れ、ログオンに必要なフィールドのチェック ボックスのチェックを外します。
    - **[閉じる]** をクリックまたはタップします。

この Web サイトまたはプログラムにアクセスすると、そのたびに Web サイトまたはアプリケーションのログオン画面の左上隅に **[Password Manager]** アイコンが表示され、登録済みの資格情報を使用してログオンできることが示されます。

## ログオンの編集

ログオンを編集するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. ログオン情報を編集できるダイアログ ボックスを表示するには、[Password Manager]アイコン→[ログオンの編集]の順にクリックまたはタップします。

画面のログオン用フィールドおよびダイアログ ボックスの対応するフィールドが、オレンジ色の太い枠線で識別されます。

[Password Manager]ページからアカウント情報を編集することもできます。その場合は、ログオン情報をクリックまたはタップして編集オプションを表示し、[編集]を選択します。

3. ログオン情報を編集します。
  - アカウント名を編集するには、[アカウント名]フィールドに新しい名前を入力します。
  - [カテゴリ]名を追加または編集するには、[カテゴリ]フィールドで名前を入力または変更します。
  - [ユーザー名]ログオン フィールドであらかじめフォーマットが用意された選択肢の1つを選択するには、フィールドの右側にある矢印をクリックまたはタップします。  
あらかじめ用意されたフォーマットを選択できるのは、[Password Manager]アイコンのコンテキスト メニューで[編集]コマンドを選択してログオン情報を編集する場合のみです。
  - [パスワード]ログオン フィールドであらかじめフォーマットが用意された選択肢の1つを選択するには、フィールドの右側にある矢印をクリックまたはタップします。  
あらかじめ用意されたフォーマットを選択できるのは、[Password Manager]アイコンのコンテキスト メニューで[編集]コマンドを選択してログオン情報を編集する場合のみです。
  - 画面上の他のフィールドをログオン情報に追加するには、[その他のフィールド]をクリックまたはタップします。
  - このログオン用のパスワードを表示するには、[パスワードの表示]アイコンをクリックまたはタップします。
  - ログオン用フィールドの入力後に送信を実行しない場合は、[ログオン データを自動的に送信する]チェック ボックスのチェックを外します。
  - このログオンのパスワードが危険にさらされていることを示すマークを付けておく場合は、[このパスワードは安全性に疑問があります]チェック ボックスにチェックを入れます。  
変更内容の保存後、同じパスワードを使用する他のログオン情報でもパスワードが危険にさらされているというマークが付きます。これにより、後で該当するアカウントを簡単に見つけてパスワードを変更できます。
4. [OK]をクリックまたはタップします。

## HP Password Manager の[クイック リンク]メニューの使用

HP Password Manager では、ログオンを作成した Web サイトおよびプログラムをすばやく簡単に起動できます。HP Password Manager の[クイック リンク]メニューまたは HP Client Security の [Password Manager]ページから、プログラムまたは Web サイトのログオンをダブルクリックまたはダブルタップし、ログオン画面を表示して、ログオン データを入力します。

作成したログオンは、HP Password Manager の[クイック リンク]メニューに自動的に追加されません。

[クイック リンク]メニューを表示するには、以下の操作を行います。

- ▲ [HP Password Manager]のホットキー (ctrl + Windows ロゴ キー + h が工場出荷時の設定です)を押します。ホットキーを変更するには、HP Client Security の[ホーム]ページで[Password Manager]→[設定]の順にクリックまたはタップします。

## ログオンをカテゴリ別に整理

ログオンを整理するには、1つまたは複数のカテゴリを作成します。

ログオンをカテゴリに割り当てるには、以下の操作を行います。

1. HP Client Security の[ホーム]ページで、[Password Manager]をクリックまたはタップします。
2. アカウントをクリックまたはタップして、[編集]をクリックまたはタップします。
3. [カテゴリ]フィールドにカテゴリ名を入力します。
4. [保存]をクリックまたはタップします。

アカウントをカテゴリから削除するには、以下の操作を行います。

1. HP Client Security の[ホーム]ページで、[Password Manager]をクリックまたはタップします。
2. アカウントをクリックまたはタップして、[編集]をクリックまたはタップします。
3. [カテゴリ]フィールドでカテゴリ名を消去します。
4. [保存]をクリックまたはタップします。

カテゴリ名を変更するには、以下の操作を行います。

1. HP Client Security の[ホーム]ページで、[Password Manager]をクリックまたはタップします。
2. アカウントをクリックまたはタップして、[編集]をクリックまたはタップします。
3. [カテゴリ]フィールドでカテゴリ名を変更します。
4. [保存]をクリックまたはタップします。

## ログオンの管理

HP Password Manager を使用すると、ユーザー名、パスワード、および複数のログオン アカウントのログオン情報を、中心となる1つの場所から簡単に管理できます。

ログオン情報は[Password Manager]ページに一覧表示されます。

ログオンを管理するには、以下の操作を行います。

1. HP Client Security の[ホーム]ページで、[Password Manager]をクリックまたはタップします。
2. 既存のログオンをクリックまたはタップしてから、以下のオプションのどれかを選択し、画面の説明に沿って操作します。
  - [編集]：ログオンを編集します。詳しくは、[21 ページの「ログオンの編集」](#)を参照してください。
  - [ログイン]：選択したアカウントにログインします。
  - [削除]：選択したアカウントのログオン情報を削除します。

Web サイトまたはプログラムに他のログオンを追加するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. **[Password Manager]**アイコンをクリックまたはタップして、コンテキストメニューを表示します。
3. **[ログオンの追加]**をクリックまたはタップし、画面の説明に沿って操作します。

## パスワード強度の評価

証明情報を保護するには、Web サイトおよびプログラムに強固なパスワードを使用することが重要です。

HP Password Manager では、Web サイトおよびプログラムへのログオンに使用されている各パスワードの強度を自動的にすばやく分析することで、セキュリティを監視および強化できます。

HP Password Manager でアカウントのログオン情報を作成するときに、パスワードを入力すると、その下にパスワードの強度を色で示すバーが表示されます。各色は以下の強度を示します。

- 赤：弱い
- 黄：普通
- 緑：強い

## [Password Manager]アイコンの設定

HP Password Manager は、Web サイトおよびプログラムのログオン画面を識別します。ログオン情報が作成されていないログオン画面が検出されると、HP Password Manager によってプラス記号 (+) の付いた **[Password Manager]**アイコンが表示され、そのログオン画面用のログオンを追加するよう求められます。

1. ログオン可能なサイトでの HP Password Manager の動作方法をカスタマイズするには、アイコン→**[アイコンの設定]**の順にクリックまたはタップします。
  - **[ログオン画面へのログオンの追加を要求]**：ログオンがまだ設定されていないログオン画面が表示されたときに、HP Password Manager によってログオンの追加が求められるようにするには、このオプションをクリックまたはタップします。
  - **[この画面を除外する]**：HP Password Manager による、このログオン画面へのログオンの追加を求めるメッセージが以後表示されないようにするには、このチェックボックスにチェックを入れます。
  - **[ログオン画面のログオンを追加するかどうか確認しない]**：ラジオ ボタンを選択します。
2. 以前に除外した画面用のログオンを追加するには、以下の操作を行います。
  - a. 以前除外した Web サイトにログオンします。
  - b. このサイトのパスワードを HP Password Manager に追加するには、表示されるダイアログで**[記憶]**をクリックまたはタップしてパスワードを保存し、この画面のログオン情報を作成します。
3. HP Password Manager の詳細設定にアクセスするには、**[Password Manager]**アイコンをクリックまたはタップし、**[パスワード マネージャーを開く]**をクリックまたはタップして、**[Password Manager]**ページで**[設定]**をクリックまたはタップします。

## ログオンのインポートおよびエクスポート


HP Password Manager の[インポートおよびエクスポート]ページでは、Web ブラウザーによってコンピューターに保存されたログオン情報をインポートできます。また、HP Client Security のバックアップ ファイルからデータをインポートしたり、HP Client Security のバックアップ ファイルにデータをエクスポートしたりできます。

- ▲ [インポートおよびエクスポート]ページにアクセスするには、[Password Manager]ページで[インポートおよびエクスポート]をクリックまたはタップします。

ブラウザーからパスワードをインポートするには、以下の操作を行います。

1. パスワードをインポートするブラウザーをクリックまたはタップします（表示されるのはインストール済みのブラウザーのみです）。
2. パスワードをインポートしないアカウントがある場合は、そのチェック ボックスのチェックを外します。
3. [インポート]をクリックまたはタップします。

HP Client Security バックアップ ファイルを使用したデータのインポートおよびエクスポートは、[インポートおよびエクスポート]ページで[その他のオプション]の下にあるそれぞれのリンクから実行できます。

 **注記：** この機能では、HP Password Manager のデータのみインポートおよびエクスポートされます。その他の HP Client Security データのバックアップおよび復元については、[28 ページの「データのバックアップおよび復元」](#)を参照してください。

HP Client Security バックアップ ファイルからデータをインポートするには、以下の操作を行います。

1. HP Password Manager の[インポートおよびエクスポート]ページで、[Import data from an HP Client Security backup file]（HP Client Security バックアップ ファイルからデータをインポート）をクリックまたはタップします。
2. ID を検証します。
3. 以前に作成したバックアップ ファイルを選択するか、表示されているフィールドにパスを入力して、[参照]をクリックまたはタップします。
4. ファイルを保護しているパスワードを入力して、[次へ]をクリックまたはタップします。
5. [復元]をクリックまたはタップします。

HP Client Security バックアップ ファイルにデータをエクスポートするには、以下の操作を行います。

1. HP Password Manager の[インポートおよびエクスポート]ページで、[Export data from an HP Client Security backup file]（HP Client Security バックアップ ファイルにデータをエクスポート）をクリックまたはタップします。
2. ユーザー情報を認証して、[次へ]をクリックまたはタップします。
3. バックアップ ファイルの名前を入力します。初期設定では、このファイルはユーザーの[ドキュメント]フォルダーに保存されます。別の場所を指定するには、[参照]をクリックまたはタップします。
4. ファイルを保護するためのパスワードを入力し、確認のためにもう一度入力して、[保存]をクリックまたはタップします。



## 設定

HP Password Manager では、以下の個人設定を指定できます。

- **[ログオン画面へのログオンの追加を要求]** : Web サイトまたはプログラムのログオン画面が検出されるたびに**[Password Manager]**アイコンをプラス記号 (+) 付きで表示し、この画面のログオンを**[ログオン]**メニューに追加できることを示します。

この機能を無効にするには、**[ログオン画面へのログオンの追加を要求]**の横にあるチェックボックスのチェックを外します。

- **[Open Password Manager with Ctrl+Win+h]** (ctrl + win + h で Password Manager を開く) : HP Password Manager の**[クイック リンク]**メニューを開くための初期設定のホットキーは、ctrl + Windows ロゴ キー + h です。

このホットキーを変更するには、このオプションをクリックまたはタップして、新しいキーの組み合わせを入力します。ctrl、alt、shift、および任意の英数字キーを組み合わせることができます。

Windows または Windows アプリケーションで使用されている組み合わせは使用できません。

- 工場出荷時の設定に戻すには、**[初期設定に復元]**をクリックまたはタップします。

## 詳細設定

管理者は、HP Client Security の[ホーム]ページでギアの絵の**[設定]**アイコンを選択して、以下のオプションにアクセスできます。

- **[Administrator Policies]** (管理者ポリシー) : 管理者のログオン ポリシーおよびセッション ポリシーを設定できます。
- **[Standard User Policies]** (標準ユーザー ポリシー) : 標準ユーザーのログオン ポリシーおよびセッション ポリシーを設定できます。
- **[セキュリティ機能]** : 強固な認証や Windows 起動前認証を有効にすることによって Windows アカウントを保護し、コンピューターのセキュリティを高めることができます。
- **[ユーザー]** : ユーザーおよびユーザーの資格情報を管理できます。
- **[My Policies]** (マイ ポリシー) : 自分の認証ポリシーおよび登録状態を確認できます。
- **[バックアップおよび復元]** : HP Client Security のデータをバックアップおよび復元できます。
- **[About HP Client Security]** (バージョン情報) : HP Client Security のバージョン情報を表示します。

## Administrator Policies (管理者ポリシー)

このコンピューターの管理者のログオン ポリシーおよびセッション ポリシーを設定できます。ログオン ポリシーでは、ローカル管理者が Windows にログオンするために必要な資格情報を設定します。セッション ポリシーでは、ローカル管理者が Windows セッション内でユーザー認証するために必要な資格情報を設定します。

初期設定では、**[適用]**をタップまたはクリックした直後から、新しいポリシーまたは変更したポリシーが適用されます。

新しいポリシーを追加するには、以下の操作を行います。

1. HP Client Security の[ホーム]ページで、[設定]アイコンをクリックまたはタップします。
2. [詳細設定]ページで、[Administrator Policies]をクリックまたはタップします。
3. [Add new policy]（新しいポリシーの追加）をクリックまたはタップします。
4. 各下向き矢印をクリックして、新しいポリシーの第 1 資格情報および第 2 資格情報（オプション）を選択し、[追加]をクリックまたはタップします。
5. [Apply]（適用）をクリックします。

新しいポリシーまたは変更したポリシーを後で適用するには、以下の操作を行います。

1. [Enforce this policy immediately]（このポリシーを今すぐ適用）をクリックまたはタップします。
2. [Enforce this policy on the specific date]（このポリシーを特定の日に適用）を選択します。
3. ポリシーを適用する日付を入力するか、ポップアップ カレンダーで選択します。
4. 必要に応じて、新しいポリシーについてユーザーに通知するタイミングを選択します。
5. [Apply]（適用）をクリックします。

## Standard User Policies（標準ユーザー ポリシー）

このコンピューターの標準ユーザーのログオン ポリシーおよびセッション ポリシーを設定できます。ログオン ポリシーでは、標準ユーザーが Windows にログオンするために必要な資格情報を設定します。セッション ポリシーでは、標準ユーザーが Windows セッション内でユーザー認証するために必要な資格情報を設定します。

初期設定では、[適用]をタップまたはクリックした直後から、新しいポリシーまたは変更したポリシーが適用されます。

新しいポリシーを追加するには、以下の操作を行います。

1. HP Client Security の[ホーム]ページで、[設定]アイコンをクリックまたはタップします。
2. [詳細設定]ページで、[Standard User Policies]をクリックまたはタップします。
3. [Add new policy]（新しいポリシーの追加）をクリックまたはタップします。
4. 各下向き矢印をクリックして、新しいポリシーの第 1 資格情報および第 2 資格情報（オプション）を選択し、[追加]をクリックまたはタップします。
5. [Apply]（適用）をクリックします。

新しいポリシーまたは変更したポリシーを後で適用するには、以下の操作を行います。

1. [Enforce this policy immediately]（このポリシーを今すぐ適用）をクリックまたはタップします。
2. [Enforce this policy on the specific date]（このポリシーを特定の日に適用）を選択します。
3. ポリシーを適用する日付を入力するか、ポップアップ カレンダーで選択します。
4. 必要に応じて、新しいポリシーについてユーザーに通知するタイミングを選択します。
5. [Apply]（適用）をクリックします。



## セキュリティ機能

コンピューターを不正アクセスから保護するために役立つ HP Client Security 機能を有効にできます。

セキュリティ機能を設定するには、以下の操作を行います。

1. HP Client Security の[ホーム]ページで、**[設定]**アイコンをクリックまたはタップします。
2. [詳細設定]ページで、**[セキュリティ機能]**をクリックまたはタップします。
3. チェックボックスにチェックを入れてセキュリティ機能を有効にし、**[適用]**をクリックまたはタップします。選択する機能が多いほど、コンピューターのセキュリティは高くなります。

これらの設定はすべてのユーザーに適用されます。

- **[Windows へのログオンの保護]** : Windows アカウントへのアクセス時に HP Client Security の資格情報を要求することで、Windows アカウントを保護します。
  - **[Pre-Boot Security (Power-on authentication)]** (ブート前セキュリティ (電源投入時認証)) : Windows が起動する前のコンピューターを保護します。BIOS によってサポートされていない場合は、この機能を使用できません。
  - **[ワン ステップ ログオンを許可する]** : 電源投入時認証レベルまたは HP Drive Encryption レベルで認証が完了している場合は、Windows のログオンを省略できるようにします。
4. **[ユーザー]**をクリックまたはタップして、ユーザーのタイルをクリックまたはタップします。

## ユーザー

このコンピューターの HP Client Security ユーザーを監視および管理できます。

他の Windows ユーザーを HP Client Security に追加するには、以下の操作を行います。

1. HP Client Security の[ホーム]ページで、**[設定]**アイコンをクリックまたはタップします。
2. [詳細設定]ページで、**[ユーザー]**をクリックまたはタップします。
3. **[Add another Windows user to HP Client Security]** (他の Windows ユーザーを HP Client Security に追加) をクリックまたはタップします。
4. 追加するユーザーの名前を入力して、**[OK]**をクリックまたはタップします。
5. そのユーザーの Windows パスワードを入力します。

[ユーザー]ページに、追加したユーザーのタイルが表示されます。

HP Client Security から Windows ユーザーを削除するには、以下の操作を行います。

1. HP Client Security の[ホーム]ページで、**[設定]**アイコンをクリックまたはタップします。
2. [詳細設定]ページで、**[ユーザー]**をクリックまたはタップします。
3. 削除するユーザーの名前をクリックまたはタップします。
4. **[Delete User]** (ユーザーの削除) をクリックまたはタップし、削除の実行を確認されたら**[はい]**をクリックまたはタップします。

ユーザーに適用されているログオン ポリシーおよびセッション ポリシーの概要を表示するには、以下の操作を行います。

- ▲ **[ユーザー]**をクリックまたはタップして、ユーザーのタイルをクリックまたはタップします。

## My Policies (マイ ポリシー)

自分の認証ポリシーおよび登録状態を確認できます。[My Policies]ページには、[Administrators Policies] (管理者ポリシー) ページおよび[Standard User Policies] (標準ユーザー ポリシー) ページへのリンクも表示されます。


1. HP Client Security の[ホーム]ページで、**[設定]**アイコンをクリックまたはタップします。
2. [詳細設定]ページで、**[My Policies]**をクリックまたはタップします。  
現在ログオンしているユーザーに適用されているログオン ポリシーおよびセッション ポリシーが表示されます。

[My Policies]ページには、[25 ページの「Administrator Policies \(管理者ポリシー\)」](#)および[26 ページの「Standard User Policies \(標準ユーザー ポリシー\)」](#)へのリンクも表示されます。

## データのバックアップおよび復元

HP Client Security のデータは定期的にバックアップすることをおすすめします。バックアップの頻度は、データが変更される頻度によって決まります。たとえば、毎日のように新しいログオンを追加している場合は、データを毎日バックアップする必要があります。

また、他のコンピューターへの移行時にバックアップを使用することもできます。この作業は、インポートおよびエクスポートと呼ばれます。

 **注記：** この機能によってバックアップされるのは HP Password Manager のデータのみです。Drive Encryption には独自のバックアップ方法が用意されています。Device Access Manager および指紋認証の情報はバックアップされません。

バックアップ ファイルからデータを復元できるようにするには、バックアップ データを取り込むコンピューターに HP Client Security をインストールしておく必要があります。

データをバックアップするには、以下の操作を行います。

1. HP Client Security の[ホーム]ページで、**[設定]**アイコンをクリックまたはタップします。
2. [詳細設定]ページで、**[Administrator Policies]**をクリックまたはタップします。
3. **[バックアップおよび復元]**をクリックまたはタップします。
4. **[Backup]** (バックアップ) をクリックまたはタップして、ユーザー認証を行います。
5. バックアップに含めるモジュールを選択して、**[次へ]**をクリックまたはタップします。
6. ストレージ ファイルの名前を入力します。初期設定では、このファイルはユーザーの[ドキュメント]フォルダーに保存されます。別の場所を指定するには、**[参照]**をクリックまたはタップします。
7. ファイルを保護するためのパスワードを入力し、確認のためにもう一度入力します。
8. **[保存]**をクリックまたはタップします。

データを復元するには、以下の操作を行います。

1. HP Client Security の[ホーム]ページで、**[設定]**アイコンをクリックまたはタップします。
2. [詳細設定]ページで、**[Administrator Policies]**をクリックまたはタップします。
3. **[バックアップおよび復元]**をクリックまたはタップします。
4. **[Restore]** (復元) を選択して、ユーザー情報を認証します。

5. 以前に作成したストレージ ファイルを選択します。表示されているフィールドにパスを入力します。別の場所を指定するには、**[参照]**をクリックまたはタップします。
6. ファイルを保護しているパスワードを入力して、**[次へ]**をクリックまたはタップします。
7. データを復元するモジュールを選択します。
8. **[復元]**をクリックまたはタップします。


## 5 HP Drive Encryption（一部のモデルのみ）

HP Drive Encryption は、コンピューターのデータを暗号化することでデータを完全に保護します。Drive Encryption を有効にしている場合は、Windows®オペレーティング システムが起動する前に表示される、Drive Encryption のログイン画面からログインする必要があります。

Windows 管理者は、[HP Client Security]の[ホーム]画面から、HP Drive Encryption の有効化、暗号化キーのバックアップ、および暗号化するドライブやパーティションの選択または選択解除を行います。詳しくは、[HP Client Security]ソフトウェアのヘルプを参照してください。

Drive Encryption では、以下のタスクを実行できます。

- Drive Encryption の設定の選択：
  - ソフトウェアによる暗号化を使用した個々のドライブまたはパーティションの暗号化または暗号化の解除
  - ハードウェアによる暗号化を使用した自己暗号化ドライブの暗号化または暗号化の解除
  - Drive Encryption のブート前認証が常に要求されるようにスリープまたはスタンバイ状態を無効にすることによる、一層のセキュリティ強化

 **注記：** 暗号化できるドライブは内蔵 SATA ハードドライブおよび外付け eSATA ハードドライブのみです。

- バックアップ キーの作成
- バックアップ キーおよび HP SpareKey を使用した、暗号化されたコンピューターへのアクセスの復元
- パスワード、登録された指紋、または一部の対応するスマートカードの PIN を使用した Drive Encryption のブート前認証の有効化

### Drive Encryption を開く

管理者は[HP Client Security]を開いて HP Drive Encryption にアクセスできます。


1. スタート画面から、**[HP Client Security]**アプリをクリックまたはタップします (Windows 8)。  
または  
Windows デスクトップで、タスクバーの右端の通知領域にある**[HP Client Security]**アイコンをダブルクリックまたはダブルタップします。
2. **[HP Drive Encryption]**アイコンをクリックまたはタップします。

# 一般的なタスク


## 標準ハードドライブに対する Drive Encryption の有効化

標準ハードドライブはソフトウェアによる暗号化を使用して暗号化されます。ドライブまたはディスク パーティションを暗号化するには、以下の操作を行います。

1. HP Drive Encryption を起動します。詳しくは、[30 ページの「Drive Encryption を開く」](#)を参照してください。
2. 暗号化するドライブまたはパーティションのチェック ボックスにチェックを入れ、**[Backup Key]**（キーをバックアップする）をクリックまたはタップします。

 **注記：** セキュリティを強化するには、**[Disable sleep mode for increased security]**（スリープ モードの無効化によるセキュリティの強化）チェック ボックスにチェックを入れます。スリープ モードを無効にすると、ドライブのロック解除に使用される資格情報がメモリに保存されるリスクが完全になくなります。

3. 1つまたは複数のバックアップ オプションを選択してから、**[バックアップ]**をクリックまたはタップします。詳しくは、[34 ページの「暗号化キーのバックアップ」](#)を参照してください。
4. 暗号化キーがバックアップされている間も作業を続行できます。コンピューターを再起動しないでください。

 **注記：** コンピューターの再起動を求めるメッセージが表示されます。再起動すると、Drive Encryption のブート前認証画面が表示され、Windows が起動する前に認証を求めるメッセージが表示されます。

Drive Encryption が有効になりました。選択したドライブのパーティションの数やサイズによっては、パーティションの暗号化に数時間かかる場合があります。

詳しくは、HP Client Security ソフトウェアのヘルプを参照してください。


## 自己暗号化ドライブに対する Drive Encryption の有効化

自己暗号化ドライブの管理に関する Trusted Computing Group の OPAL 仕様に適合する自己暗号化ドライブは、ソフトウェアによる暗号化またはハードウェアによる暗号化を使用して暗号化できます。ハードウェアによる暗号化は、ソフトウェアによる暗号化よりもはるかに速く行われます。ただし、あるディスク パーティションを選択して暗号化することはできません。すべてのディスク パーティションを含むディスク全体が暗号化されます。


特定のパーティションを暗号化するには、ソフトウェアによる暗号化を使用する必要があります。必ず、**[自己暗号化ドライブ (SED) のハードウェアによる暗号化のみ許可]**チェック ボックスのチェックを外してください。

自己暗号化ドライブに対して Drive Encryption を有効にするには、以下の操作を行います。

1. HP Drive Encryption を起動します。詳しくは、[30 ページの「Drive Encryption を開く」](#)を参照してください。
2. 暗号化するドライブのチェック ボックスにチェックを入れ、**[Backup Key]**（キーをバックアップする）をクリックまたはタップします。

 **注記：** セキュリティを強化するには、**[スリープ モードの無効化によるセキュリティの強化]**チェック ボックスにチェックを入れます。スリープ モードを無効にすると、ドライブのロック解除に使用される資格情報がメモリに保存されるリスクが完全になくなります。

3. 1つまたは複数のバックアップ オプションを選択してから、**[バックアップ]**をクリックまたはタップします。詳しくは、[34 ページの「暗号化キーのバックアップ」](#)を参照してください。
4. 暗号化キーがバックアップされている間も作業を続行できます。コンピューターを再起動しないでください。


 **注記：** 自己暗号化ドライブの場合は、コンピューターをシャットダウンするように要求されません。

詳しくは、HP Client Security ソフトウェアのヘルプを参照してください。

## Drive Encryption の無効化

1. HP Drive Encryption を起動します。詳しくは、[30 ページの「Drive Encryption を開く」](#)を参照してください。
2. すべての暗号化されたドライブのチェック ボックスのチェックを外してから、**[適用]**をクリックまたはタップします。

Drive Encryption の無効化が開始されます。


 **注記：** ソフトウェアによる暗号化が使用されていた場合は、暗号化の解除が開始されます。暗号化されていたハードドライブ パーティションのサイズによっては、暗号化の解除に数時間かかることがあります。暗号化の解除が完了すると、Drive Encryption が無効になります。

ハードウェアによる暗号化が使用されていた場合は、ドライブの暗号化がすぐに解除され、数分後に Drive Encryption が無効になります。


Drive Encryption が無効になると、ハードウェアによる暗号化が使用されていた場合はコンピューターのシャットダウンを求めるメッセージが表示されます。ソフトウェアによる暗号化が使用されていた場合は、コンピューターの再起動を求めるメッセージが表示されます。

## Drive Encryption の有効化後のログイン

Drive Encryption が有効になり、ユーザー アカウントが登録された後でコンピューターを起動した場合、Drive Encryption のログイン画面からログインする必要があります。

 **注記：** スリープまたはスタンバイ状態から復帰するときは、ソフトウェアによる暗号化でもハードウェアによる暗号化でも、HP Drive Encryption のブート前認証画面は表示されません。ハードウェアによる暗号化では**[Disable sleep mode for increased security]**（スリープ モードの無効化によるセキュリティの強化）オプションが用意されていて、これを有効にするとスリープまたはスタンバイ状態が発生しないようにできます。

ハイバネーション状態から復帰するときは、ソフトウェアによる暗号化でもハードウェアによる暗号化でも、Drive Encryption のブート前認証画面が表示されます。


 **注記：** Windows 管理者が HP Client Security で BIOS ブート前セキュリティを有効にしている、ワンステップ ログオンが有効になっている場合（初期設定では有効）は、BIOS ブート前セキュリティで認証を行った直後にコンピューターにログインできます。HP Drive Encryption のログイン画面による再認証は求められません。

### 1 人のユーザーのログオン：

- ▲ **[ログオン]** ページで、Windows のパスワード、スマート カードの PIN、または HP SpareKey を入力するか、登録した指の指紋を認証システムで読み取らせます。


## 複数のユーザーのログオン：

1. [ログオンするユーザーの選択] ページで、ドロップダウン リストからログオンするユーザーを選択して、[次へ] をクリックまたはタップします。
2. [ログオン] ページで、Windows のパスワードまたはスマート カードの PIN を入力するか、または登録した指の指紋を認証システムで読み取らせます。

 **注記：** 以下のスマート カードがサポートされます。

## サポートされているスマート カード


- Gemalto Cyberflex Access 64k V2c

 **注記：** Drive Encryption のログイン画面で復元キーを使用してログインする場合、ユーザー アカウントにアクセスするには、Windows のログオン画面で追加の資格情報を入力するように求められます。

## 追加のハードドライブの暗号化

HP Drive Encryption でハードドライブを暗号化してデータを保護することを強くおすすめします。暗号化を有効にすると、追加したハードドライブや作成したパーティションを以下の手順で暗号化できます。

1. HP Drive Encryption を起動します。詳しくは、[30 ページの「Drive Encryption を開く」](#)を参照してください。
2. ソフトウェアによって暗号化するドライブについては、暗号化するドライブ パーティションを選択します。

 **注記：** これは、標準ハードドライブと自己暗号化ドライブが 1 台または複数台混在する場合にもあてはまります。

または

- ▲ ハードウェアによって暗号化するドライブについては、暗号化する追加のドライブを選択します。

## 高度なタスク

### Drive Encryption の管理（管理者のタスク）

管理者は HP Drive Encryption を使って、コンピューター上のすべてのハードドライブの暗号化の状態（[未暗号化]または[暗号化されている]）を表示および変更できます。

- 状態が有効の場合、Drive Encryption は有効にされ、設定されています。ドライブは、次のどれかの状態になっています。

### ソフトウェアによる暗号化

- 暗号化されていない
- 暗号化されている
- 暗号化を実行中
- 暗号化解除を実行中




## ハードウェアによる暗号化


- 暗号化されている
- 暗号化されていない（追加のドライブ）

## 個々のドライブ パーティションの暗号化または暗号化の解除（ソフトウェアによる暗号化のみ）

管理者は HP Drive Encryption を使用して、コンピューター上の 1 つまたは複数のハードドライブ パーティションを暗号化したり、すでに暗号化されているドライブ パーティションの暗号化を解除したりできます。

1. HP Drive Encryption を起動します。詳しくは、[30 ページの「Drive Encryption を開く」](#)を参照してください。
2. **[ドライブの状態]**で、各ハードドライブ パーティションの横にあるチェック ボックスに、暗号化または暗号化解除に応じてチェックを入れるか外すかし、**[適用]**をクリックまたはタップします。

 **注記：** ドライブ パーティションの暗号化または暗号化解除が行われている間、暗号化されているパーティションの割合が進行状況バーに表示されます。

 **注記：** ダイナミック パーティションはサポートされていません。パーティションが使用可能として表示されるが、選択しても暗号化できない場合、そのパーティションはダイナミック パーティションです。ダイナミック パーティションは、**[ディスクの管理]**で新しいパーティションを作成するためにどれかのパーティションを縮小した結果生成されます。

パーティションがダイナミック パーティションに変換される場合は、警告が表示されます。

## ディスクの管理

- **[ニックネーム]**：ドライブまたはパーティションに簡単に識別できる名前を付けることができます。
- **[Disconnected drives]**（切断されたドライブ）：コンピューターから取り外されたディスクを HP Drive Encryption で追跡できます。コンピューターから取り外されたディスクは自動的に **[Disconnected]**（切断済み）リストに入れられます。ディスクがシステムに戻されると、再び **[Connected]**（接続済み）リストに表示されます。
- 切断されたドライブの追跡や管理がこれ以上必要なくなったときは、その切断されたドライブを **[Disconnected]**（切断済み）リストから削除できます。
- HP Drive Encryption は、接続されているすべてのドライブのチェック ボックスのチェックが外され、かつ **[Disconnected]**（切断済み）リストが空になるまで、起動した状態を維持します。

## バックアップおよび復元（管理者のタスク）

Drive Encryption が有効な場合、管理者は**[暗号化キーのバックアップ]**ページを使用して暗号化キーをリムーバブル メディアにバックアップしたり、復元を実行したりできます。

## 暗号化キーのバックアップ


管理者は、暗号化されたドライブの暗号化キーをリムーバブル ストレージ デバイスにバックアップできます。



**△ 注意：** バックアップ キーを含むストレージ デバイスは必ず安全な場所に保管してください。パスワードを忘れた場合、スマート カードを紛失した場合、または、指紋を登録していない場合に、このデバイスがコンピューターにアクセスする唯一の方法となります。ストレージ デバイスを使用することで Windows にアクセスできるため、保管場所の安全も確保してください。

1. HP Drive Encryption を起動します。詳しくは、[30 ページの「Drive Encryption を開く」](#)を参照してください。
2. ドライブのチェック ボックスにチェックを入れ、**[Backup Key]** (キーをバックアップする) をクリックまたはタップします。
3. **[Create HP Drive Encryption recovery key]** (HP Drive Encryption の復元キーの作成) で、以下のオプションを 1 つまたは複数選択します。

- **[リムーバブル ストレージ]** : チェック ボックスにチェックを入れてから、暗号化キーが保存されるストレージ デバイスを選択します。
- **[SkyDrive]** : チェック ボックスにチェックを入れます。インターネットに接続されている必要があります。[Microsoft SkyDrive] にログインし、**[はい]** をクリックまたはタップします。

 **注記：** [SkyDrive] に保存されている HP Drive Encryption のバックアップ キーを使用するには、キーを [SkyDrive] からリムーバブル ストレージ デバイスにダウンロードし、次にストレージ デバイスをこのコンピューターに挿入する必要があります。

- **[TPM]** (一部のモデルのみ) : TPM (Trusted Platform Module) パスワードを使ってデータを復元できます。

**△ 注意：** TPM が消去されたり、コンピューターが損傷したりすると、バックアップにアクセスできなくなります。この方法が選択されている場合は、別のバックアップ方法も選択してください。


4. **[バックアップ]** をクリックまたはタップします。  
選択したストレージ デバイスに暗号化キーが保存されます。

## 暗号化が有効になっているコンピューターでのバックアップ キーを使用したアクセスの復元

管理者は、暗号化を有効にしたときにリムーバブル ストレージ デバイスにバックアップした Drive Encryption キー、または HP Drive Encryption の**[キーをバックアップする]** オプションを選択してバックアップした Drive Encryption キーを使用して、復元を実行できます。

1. バックアップ キーが保管されているリムーバブル ストレージ デバイスを装着します。
2. コンピューターの電源を入れます。
3. HP Drive Encryption のログイン ダイアログ ボックスが表示されたら、**[復元]** をクリックまたはタップします。
4. バックアップ キーを含むファイル名またはパスを入力して、**[復元]** をクリックまたはタップします。
5. 確認ダイアログ ボックスが表示されたら、**[OK]** をクリックまたはタップします。

Windows のログオン画面が表示されます。


 **注記：** Drive Encryption のログイン画面で復元キーを使用してログインする場合、ユーザー アカウントにアクセスするには、Windows のログオン画面で追加の資格情報を入力するように求められます。復元を実行した後は、パスワードを再設定することを強くおすすめします。

## HP SpareKey のリカバリの実行


HP Drive Encryption のブート前認証で HP SpareKey のリカバリを実行する場合は、セキュリティに関する質問に正しく答えないとコンピューターにアクセスできません。HP SpareKey のリカバリの設定について詳しくは、HP Client Security ソフトウェアのヘルプを参照してください。

パスワードを忘れてしまった場合に HP SpareKey のリカバリを実行するには、以下の操作を行います。

1. コンピューターの電源を入れます。
2. [HP Drive Encryption] ページが表示されたら、ユーザー ログオン ページに移動します。
3. **[SpareKey]** をクリックします。

 **注記：** HP Client Security で HP SpareKey が初期化されていない場合は、**[SpareKey]** ボタンを使用できません。

4. 表示された質問に対して正しい回答を入力し、**[ログオン]** をクリックします。  
Windows のログオン画面が表示されます。

 **注記：** Drive Encryption のログイン画面で HP SpareKey を使用してログインする場合、ユーザーアカウントにアクセスするには、Windows のログオン画面で追加の資格情報を入力するように求められます。復元を実行した後は、パスワードを再設定することを強くおすすめします。

## 6 HP File Sanitizer（一部のモデルのみ）

HP File Sanitizer を使用すると、コンピューターの内蔵ハードドライブ上のフォルダーやファイル（例：個人情報やファイル、履歴データや Web 関連データ、その他のデータ コンポーネント）を安全にシュレッドしたり、コンピューターの内蔵ハードドライブを定期的にブリーチ（漂白）したりすることができます。

HP File Sanitizer は、以下の種類のドライブのクリーンアップやブリーチには使用できません。


- SSD（Solid State Drive）。SSD デバイスにまたがる RAID ボリュームも含まれます
- USB、IEEE 1394、または eSATA インターフェイスで接続された外付けドライブ

SSD 上でシュレッド操作またはブリーチ操作の実行が試みられた場合は、警告メッセージが表示され、操作は実行されません。

### シュレッド

シュレッドは、Windows の標準の削除操作とは異なります。File Sanitizer を使用してフォルダーやファイルをシュレッドすると、意味を持たないデータがファイルに上書きされて、元のフォルダーやファイルを取り戻すことが事実上不可能になります。Windows のシンプル削除操作では、ファイル（またはフォルダー）がハードドライブ上にそのままの状態に残されるか、または電子情報の分析によって復元できる状態で残される可能性があります。


将来のある時点でシュレッドするようスケジュール設定したり、シュレッドを手動で実行したりするには、HP Client Security の[ホーム]画面にある **[File Sanitizer]** アイコンを選択するか、Windows デスクトップにある **[File Sanitizer]** アイコンを使用します。詳しくは、[40 ページの「シュレッド スケジュールの設定」](#)、[43 ページの「右クリック シュレッド」](#)、または [43 ページの「シュレッド操作の手動開始」](#) を参照してください。

 **注記：** .dll ファイルは、ゴミ箱に移動されている場合にのみ、シュレッドされてシステムから削除されます。

## 空き領域ブリーチ

Windows でフォルダーやファイルを削除しても、そのフォルダーやファイルの内容はハードドライブから完全に削除されません。Windows はフォルダーやファイルの参照情報、またはハードドライブ上のフォルダーやファイルに存在する場所の情報のみを削除します。他のフォルダーやファイルによってハードドライブの同じ領域を新しい情報で上書きしないかぎり、フォルダーやファイルの内容はハードドライブに引き続き残ったままとなります。

空き領域ブリーチを実行すると、削除されたフォルダーやファイルに対してランダムなデータを安全に上書きできるため、削除されたフォルダーやファイルの元の内容をユーザーは参照できなくなります。

 **注記：** 空き領域ブリーチを実行しても、シュレッドされたフォルダーやファイルにセキュリティが追加されることはありません。

将来のある時点に空き領域ブリーチを実行するよう設定したり、以前にシュレッドしたフォルダーやファイルの空き領域ブリーチを手動で実行したりするには、HP Client Security の[ホーム]画面にある **[File Sanitizer]** アイコンを選択するか、Windows デスクトップにある **[File Sanitizer]** アイコンを使用します。詳しくは、[41 ページの「空き領域ブリーチのスケジュール設定」](#)、[43 ページの「空き領域ブリーチの手動開始」](#)、または [42 ページの「\[File Sanitizer\] アイコンの使用」](#) を参照してください。

## HP File Sanitizer の起動

1. スタート画面から、**[HP Client Security]** アプリをクリックまたはタップします (Windows 8)。

または

Windows デスクトップで、タスクバーの右端の通知領域にある **[HP Client Security]** アイコンをダブルクリックまたはダブルタップします。

2. **[データ]** で、**[File Sanitizer]** をクリックまたはタップします。

または

- ▲ Windows デスクトップの **[File Sanitizer]** アイコンをダブルクリックまたはダブルタップします。

または

- ▲ Windows デスクトップにある **[File Sanitizer]** アイコンを右クリックするかまたはタップしたまま押さえてから、**[File Sanitizer を開く]** を選択します。

## セットアップ手順

[シュレッド] : File Sanitizer は、選択したカテゴリのフォルダーやファイルを安全に削除またはシュレッドします。

1. [シュレッド]で、シュレッドするファイルの種類をチェック ボックスにチェックを入れ、シュレッドしない種類のチェック ボックスのチェックを外します。
  - [ゴミ箱] : [ゴミ箱]の中のすべての項目をシュレッドします。
  - [一時システム ファイル] : システムの一時フォルダーにあるすべてのファイルをシュレッドします。以下の環境変数が以下の順に検索されて、最初に見つかったパスがシステムフォルダーであるとみなされます。
    - TMP
    - TEMP
  - [インターネット一時ファイル] : 表示の高速化のために Web ブラウザーに保存された Web ページ、画像、およびメディアのコピーをシュレッドします。
  - [Cookies] : Web サイトによってコンピューターに保存されたすべてのファイルをシュレッドして、ログイン情報などの設定を保存します。
2. シュレッドを開始するには、[シュレッド]をクリックまたはタップします。

[ブリーチ] : ランダムなデータを空き領域に書き込み、削除した項目を復元できないようにします。

▲ ブリーチを開始するには、[ブリーチ]をクリックまたはタップします。

[File Sanitizer のオプション] : 以下のオプションを有効にする場合はチェック ボックスにチェックを入れ、無効にする場合はチェック ボックスのチェックを外します。

- [Enable Desktop icon] (デスクトップ アイコンを有効にする) : Windows デスクトップに[File Sanitizer]アイコンを表示します。
- [Enable right-click] (右クリックを有効にする) : フォルダーやファイルを右クリックするかまたはタップしたまま押さえてから、[HP File Sanitizer]→[シュレッド]の順に選択できるようにします。
- [Ask for Windows password before manual shredding] (手動シュレッドの前に Windows パスワードを要求する) : 項目を手動でシュレッドする前に、Windows パスワードによる認証を要求します。
- [Shred Cookies and Temporary Internet Files on browser close] (ブラウザーを閉じるときに Cookies およびインターネット一時ファイルをシュレッドする) : Web ブラウザーを閉じるときに、ブラウザーの URL 履歴など、選択したすべての Web 関連のフォルダーやファイルをシュレッドします。

## シュレッド スケジュールの設定

自動的にシュレッドを実行するようにスケジュールを設定できます。またフォルダーやファイルをいつでも手動でシュレッドすることもできます。詳しくは、[39 ページの「セットアップ手順」](#)（英語サイト）を参照してください。

1. File Sanitizer を起動し、**[設定]**をクリックまたはタップします。
2. 選択されているフォルダーやファイルを将来のある時点でシュレッドするようにスケジュール設定するには、**[Shred Schedule]**（シュレッド スケジュール）で、**[なし]**、**[1 回]**、**[毎日]**、**[毎週]**、**[毎月]**のどれかを選択してから、日付と時刻を選択します。
  - a. 時間、分、または午前/午後のフィールドをクリックまたはタップします。
  - b. 他のフィールドと同じレベルに目的の値が表示されるまでスクロールします。
  - c. 時刻設定フィールドの周りの空白部分をクリックまたはタップします。
  - d. スケジュールが正しく選択されるまで、フィールドごとに操作を繰り返します。
3. 以下の 4 種類のフォルダーやファイルが表示されます。
  - **[ゴミ箱]**：[ゴミ箱]の中のすべての項目をシュレッドします。
  - **[一時システム ファイル]**：システムの一時的フォルダーにあるすべてのファイルをシュレッドします。以下の環境変数が以下の順に検索されて、最初に見つかったパスがシステムフォルダーであるとみなされます。
    - TMP
    - TEMP
  - **[インターネット一時ファイル]**：表示の高速化のために Web ブラウザーに保存された Web ページ、画像、およびメディアのコピーをシュレッドします。
  - **[Cookies]**：Web サイトによってコンピューターに保存されたすべてのファイルをシュレッドして、ログイン情報などの設定を保存します。


チェックを付けたフォルダーやファイルが、スケジュール設定した時刻にシュレッドされます。
4. シュレッドするフォルダーやファイルをカスタムで選択して追加するには、以下のように操作します。
  - a. **[Scheduled Shred List]**（スケジュール済みのシュレッド リスト）で、**[フォルダーの追加]**をクリックまたはタップし、目的のファイルまたはフォルダーまで移動します。
  - b. **[開く]**→**[OK]**の順にクリックまたはタップします。

[Scheduled Shred List]からフォルダーやファイルを削除するには、該当するチェック ボックスのチェックを外します。

## 空き領域ブリーチのスケジュール設定

空き領域ブリーチを実行しても、シュレッドされたフォルダーやファイルにセキュリティが追加されることはありません。


1. File Sanitizer を起動し、**[設定]**をクリックまたはタップします。
2. ハードドライブを将来のある時点でブリーチするようにスケジュール設定するには、**[Bleach Schedule]**（ブリーチ スケジュール）で、**[なし]**、**[1 回]**、**[毎日]**、**[毎週]**、**[毎月]**のどれかを選択してから、日付と時刻を選択します。
  - a. 時間、分、または午前/午後のフィールドをクリックまたはタップします。
  - b. 他のフィールドと同じレベルに目的の時刻が表示されるまでスクロールします。
  - c. 時刻設定フィールドの周りの空白部分をクリックまたはタップします。
  - d. スケジュールが正しく選択されるまで、操作を繰り返します。

 **注記：** 空き領域ブリーチ操作は、非常に長い時間がかかる場合があります。コンピューターが外部電源に接続されていることを確認します。空き領域ブリーチはバックグラウンドで実行されますが、プロセッサの使用量が大きくなるため、コンピューターの動作が遅くなる場合があります。空き領域ブリーチは、業務時間外またはコンピューターが使用されていない間に実行できます。

## ファイルがシュレッドされないように保護する

シュレッドからフォルダーやファイルを保護するには、以下の操作を行います。

1. File Sanitizer を起動し、**[設定]**をクリックまたはタップします。
2. **[Never Shred List]**（シュレッドしないリスト）で、**[フォルダーの追加]**をクリックまたはタップし、目的のファイルまたはフォルダーまで移動します。
3. **[開く]**→**[OK]**の順にクリックまたはタップします。

 **注記：** このリスト内のファイルは、リスト内に存在している限り保護されます。


この除外リストからフォルダーやファイルを削除するには、該当するチェック ボックスのチェックを外します。




## 一般的なタスク

File Sanitizer を使用すると、以下のタスクを実行できます。

- **[File Sanitizer]アイコンでシュレッドを開始**：ファイルを Windows デスクトップの **[File Sanitizer]** アイコンにドラッグできます。詳しくは、[42 ページの「\[File Sanitizer\]アイコンの使用」](#)を参照してください。
- **特定のフォルダーやファイルまたは選択されているすべてのフォルダーやファイルを手動シュレッド**：スケジュールされたシュレッド時刻の前に、フォルダーやファイルをいつでもシュレッドできます。詳しくは、[43 ページの「右クリック シュレッド」](#)または[43 ページの「シュレッド操作の手動開始」](#)を参照してください。
- **空き領域ブリーチを手動で実行**：空き領域ブリーチをいつでも実行できます。詳しくは、[43 ページの「空き領域ブリーチの手動開始」](#)を参照してください。
- **ログ ファイルを表示**：シュレッドまたは空き領域ブリーチのログ ファイルを表示できます。ログ ファイルには、最後のシュレッド操作または空き領域ブリーチ操作で発生したエラーや障害が記録されます。詳しくは、[44 ページの「ログ ファイルの表示」](#)を参照してください。

 **注記**： シュレッド操作および空き領域ブリーチ操作は、非常に長い時間がかかる場合があります。シュレッドおよび空き領域ブリーチはバックグラウンドで実行されますが、プロセッサの使用量が大きくなるため、コンピューターの動作が遅くなる場合があります。

## [File Sanitizer]アイコンの使用

 **注意**： シュレッドしたフォルダーやファイルは復元できません。手動でシュレッドするために選択するフォルダーやファイルについては、十分に検討してください。

シュレッド操作を手動で開始すると、[File Sanitizer]ビューの標準シュレッド リストがシュレッドの対象となります（[39 ページの「セットアップ手順」](#)を参照してください）。

手動のシュレッド操作は、以下のどちらかの方法で開始できます。

1. File Sanitizer を起動し（[38 ページの「HP File Sanitizer の起動」](#)を参照してください）、[シュレッド]をクリックまたはタップします。
2. 確認ダイアログ ボックスが開いたら、シュレッドするフォルダーやファイルにチェックが付いていることを確認してから[OK]をクリックまたはタップします。

または

1. Windows デスクトップにある **[File Sanitizer]** アイコンを右クリックするかまたはタップしたまま押さえてから、**[今すぐシュレッド]**をクリックまたはタップします。
2. 確認ダイアログ ボックスが開いたら、シュレッドするフォルダーやファイルにチェックが付いていることを確認してから**[シュレッド]**をクリックまたはタップします。

## 右クリック シュレッド

**△ 注意：** シュレッドしたフォルダーやファイルは復元できません。手動でシュレッドするために選択するフォルダーやファイルについては、十分に検討してください。

[File Sanitizer]ビューで[**Enable right-click shredding**]（右クリック シュレッドを有効にする）が選択されている場合は、以下の操作でフォルダーやファイルをシュレッドできます。

1. シュレッドするドキュメントまたはフォルダーに移動します。
2. 目的のファイルまたはフォルダーを右クリックするかまたはタップしたまま押さえてから、[HP File Sanitizer]→[シュレッド]の順に選択します。

## シュレッド操作の手動開始

**△ 注意：** シュレッドしたフォルダーやファイルは復元できません。手動でシュレッドするために選択するフォルダーやファイルについては、十分に検討してください。

シュレッド操作を手動で開始すると、[File Sanitizer]ビューの標準シュレッド リストがシュレッドの対象となります（[39 ページの「セットアップ手順」](#)を参照してください）。

手動のシュレッド操作は、以下のどちらかの方法で開始できます。

1. File Sanitizer を起動し（[38 ページの「HP File Sanitizer の起動」](#)を参照してください）、[シュレッド]をクリックまたはタップします。
2. 確認ダイアログ ボックスが開いたら、シュレッドするフォルダーやファイルにチェックが付いていることを確認してから[OK]をクリックまたはタップします。

または

1. Windows デスクトップにある[File Sanitizer]アイコンを右クリックするかまたはタップしたまま押さえてから、[今すぐシュレッド]をクリックまたはタップします。
2. 確認ダイアログ ボックスが開いたら、シュレッドするフォルダーやファイルにチェックが付いていることを確認してから[シュレッド]をクリックまたはタップします。

## 空き領域ブリーチの手動開始

ブリーチ操作を手動で開始すると、[File Sanitizer]ビューの標準シュレッド リストがブリーチの対象となります（[39 ページの「セットアップ手順」](#)を参照してください）。

手動のブリーチ操作は、以下のどちらかの方法で開始できます。


1. File Sanitizer を起動し（[38 ページの「HP File Sanitizer の起動」](#)を参照してください）、[ブリーチ]をクリックまたはタップします。
2. 確認ダイアログ ボックスが表示されたら、[OK]をクリックまたはタップします。

または

1. Windows デスクトップにある[File Sanitizer]アイコンを右クリックするかまたはタップしたまま押さえてから、[今すぐブリーチ]をクリックまたはタップします。
2. 確認ダイアログ ボックスが表示されたら、[ブリーチ]をクリックまたはタップします。

## ログ ファイルの表示

シュレッド操作または空き領域ブリーチ操作を実行するたびに、エラーのログ ファイルまたは障害のログ ファイルが生成されます。これらのログ ファイルは、最新のシュレッド操作または空き領域ブリーチ操作に従って常に更新されます。

 **注記：** 正常にシュレッドまたはブリーチされたファイルは、ログ ファイルには表示されません。

ログ ファイルには、シュレッド操作について作成されるファイルと空き領域ブリーチ操作について作成されるファイルがあります。これらのログ ファイルは、ハードドライブ上の以下のフォルダーにあります。


- C:\Program Files\Hewlett-Packard\File Sanitizer\[ユーザー名]\_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer\[ユーザー名]\_DiskBleachLog.txt

64 ビットのシステムでは、これらのログ ファイルは、ハードドライブ上の以下のフォルダーにあります。

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer\[ユーザー名]\_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer\[ユーザー名]\_DiskBleachLog.txt

## 7 HP Device Access Manager（一部のモデルのみ）

HP Device Access Manager は、データ転送デバイスを無効にすることによってデータへのアクセスを制御します。

 **注記：** マウス、キーボード、タッチパッド、指紋認証システムなどの一部のヒューマン インターフェイス デバイスや入力デバイスは、Device Access Manager によって制御されません。詳しくは、[49 ページの「管理されないデバイス クラス」](#)を参照してください。

HP Device Access Manager を使用すると、Windows®オペレーティング システムの管理者は、システム上のデバイスへのアクセスを制御し、不正なアクセスを防止できます。

- アクセスを許可または拒否するデバイスを定義するためのデバイス プロファイルが、ユーザーごとに作成されます。
- ジャスト イン タイム認証 (JITA) を使用すると、あらかじめ定義されたユーザーは、通常はアクセスできないデバイスにアクセスするために、自身を認証することが可能です。
- 管理者および信頼できるユーザーをデバイス管理グループに追加することで、HP Device Access Manager によるデバイスへのアクセス制限からこれらの管理者やユーザーを除外できます。このグループのメンバーシップは、[詳細設定]を使用して管理します。
- グループ メンバーシップに基づいて、または個々のユーザーに対して、デバイス アクセスを許可または拒否できます。
- CD-ROM ドライブや DVD ドライブなどのデバイス クラスの場合は、読み取りアクセスおよび書き込みアクセスを個別に許可または拒否できます。

HP Device Access Manager は、HP Client Security セットアップ ウィザードの実行過程で、以下の設定を用いて自動的に構成されます。

- ジャスト イン タイム認証 (JITA) を使用したリムーバブル メディアへのアクセスが Administrators および Users に許可されます。
- デバイス ポリシーで他のデバイスへのフル アクセスが許可されます。

## HP Device Access Manager を開く

1. スタート画面から、**[HP Client Security]**アプリをクリックまたはタップします (Windows 8)。  
または  
Windows デスクトップで、タスクバーの右端の通知領域にある**[HP Client Security]**アイコンをダブルクリックまたはダブルタップします。
2. **[デバイス]**で、**[デバイス権限]**をクリックまたはタップします。
  - 標準ユーザーは、現在の自分のデバイス アクセス権を確認できます ([46 ページの「\[ユーザー\]ビュー](#)」を参照してください)。
  - 管理者は、**[変更]**をクリックまたはタップしてから Administrator パスワードを入力することで、コンピューターに現在設定されているデバイス アクセス権を確認および変更できます ([46 ページの「\[システム\]ビュー](#)」参照してください)。

### [ユーザー]ビュー

**[デバイス権限]**が選択されると、**[ユーザー]ビュー**が表示されます。ポリシーによっては、標準ユーザーおよび管理者は、このコンピューター上のデバイス クラスまたは個々のデバイスへの自分自身のアクセス権を確認できます。

- **[現在のユーザー]** : 現在ログオンしているユーザーの名前が表示されます。
- **[デバイス クラス]** : デバイスの種類が表示されます。
- **[アクセス]** : デバイスの種類または特定のデバイスに対して現在設定されているアクセス権が表示されます。
- **[継続時間]** : CD/DVD-ROM ドライブまたはリムーバブル ディスク ドライブにアクセスできる時間制限が表示されます。
- **[設定]** : 管理者は、HP Device Access Manager によって制御されるアクセス権が設定されるドライブを変更できます。


### [システム]ビュー

**[システム]ビュー**では、管理者が Users グループまたは Administrators グループに対して、このコンピューター上のデバイスへのアクセスを許可または拒否できます。

- ▲ 管理者は、**[変更]**をクリックまたはタップして Administrator パスワードを入力した後、以下のオプションから選択することによって、**[システム]ビュー**を使用できます。
- **[Device Access Manager]** : HP Device Access Manager のジャスト イン タイム認証 (JITA) のオン/オフを切り替えるには、**[オン]**または**[オフ]**をクリックまたはタップします。
- **[このコンピューターのユーザーおよびグループ]** : 選択されたデバイス クラスへのアクセスを許可または拒否されている Users グループまたは Administrators グループが表示されます。
- **[デバイス クラス]** : デバイス クラス、およびシステムにインストールされているか以前にインストールされていた可能性のあるデバイスを表示します。リストを展開するには、**[+]**アイコンをクリックします。コンピューターに接続されているすべてのデバイスが表示され、

Administrators グループおよび Users グループが展開されてそのメンバーシップが表示されます。デバイスのリストを最新の内容にするには、丸い矢印（更新）アイコンをクリックします。

- 保護は、通常はデバイス クラスに対して適用されます。アクセスが[許可]に設定されている場合、選択されたユーザーまたはグループは、そのデバイス クラスの任意のデバイスにアクセスできます。
- 特定のデバイスに対して保護を適用することもできます。
- 選択されたユーザーが自身を認証して DVD ドライブや CD-ROM ドライブまたはリムーバブル ディスク ドライブにアクセスできるようにする、ジャスト イン タイム認証 (JITA) を構成します。詳しくは、[48 ページの「ジャスト イン タイム認証の構成」](#)を参照してください。
- リムーバブル メディア (USB フラッシュ ドライブなど)、シリアル ポートおよびパラレルポート、Bluetooth デバイス、モデム デバイス、PCMCIA/ExpressCard デバイス、1394 デバイス、指紋認証システム、スマート カード リーダーなど、その他のデバイス クラスへのアクセスを許可または拒否します。指紋認証システムおよびスマート カード リーダーへのアクセスを拒否した場合、認証資格情報としてはそれらを使用できますが、セッションポリシー レベルでは使用できません。


 **注記：** Bluetooth デバイスを認証資格情報として使用する場合は、Device Access Manager ポリシーで Bluetooth デバイスへのアクセスを制限しないでください。

- グループまたはデバイス クラスのレベルで設定値を選択すると、その設定値を子オブジェクトに適用するかどうかを尋ねられます。

[はい]：設定が継承されます。

[いいえ]：設定が継承されません。

- DVD や CD-ROM など一部のデバイス クラスでは、読み取りおよび書き込み操作のためのアクセスを個別に許可または拒否することによって詳細な制御を設定できます。

 **注記：** Administrators グループを[ユーザー一覧]に追加することはできません。

- **[アクセス]：** 下向き矢印をクリックまたはタップし、アクセスを許可または拒否する以下のアクセスの種類をどれかを選択します。
  - **[許可：フル アクセス]**
  - **[許可：読み取り専用]**
  - **[許可：ジャスト イン タイム認証が必要]：** 詳しくは、[48 ページの「ジャスト イン タイム認証の構成」](#)を参照してください。

このアクセスの種類を選択した場合は、[継続時間]で下向き矢印をクリックまたはタップして時間制限を選択します。
  - **[拒否]**
- **[継続時間]：** 下向き矢印をクリックまたはタップして、CD/DVD-ROM ドライブまたはリムーバブル ディスク ドライブにアクセスする際の時間制限を選択します ([48 ページの「ジャスト イン タイム認証の構成」](#)を参照してください)。

## ジャスト イン タイム認証の構成

ジャスト イン タイム認証の構成では、管理者はジャスト イン タイム認証 (JITA) を使用してデバイスへのアクセスを許可されるユーザーおよびグループの一覧を表示したり変更したりできます。

ジャスト イン タイム認証が有効なユーザーは、**[デバイス クラス構成]**ビューで作成されたポリシーが制限されている一部のデバイスにアクセスできます。

ジャスト イン タイム認証期間は、設定した時間 (分) の間または無制限に有効です。期間を無制限に設定されたユーザーは、認証されてからシステムからログオフするまで、デバイスにアクセスできます。

JITA 期間が制限されたユーザーの場合は、JITA 期間が切れる 1 分前に、アクセスを延長するかどうかを尋ねるメッセージが表示されます。JITA 期間は、ユーザーがシステムからログオフするか別のユーザーがログインした時点で切れます。次にユーザーがログインし、ジャスト イン タイム認証が有効なデバイスにアクセスしようとする、証明情報を入力するよう求めるメッセージが表示されます。

ジャスト イン タイム認証は以下のデバイス クラスに対して使用できます。

- DVD/CD-ROM ドライブ
- リムーバブル ディスク ドライブ

### ユーザーまたはグループのジャスト イン タイム認証ポリシーの作成

管理者は、ジャスト イン タイム認証 (JITA) を使用してユーザーまたはグループがデバイスにアクセスすることを許可できます。

1. **[HP Device Access Manager]**を起動し、**[変更]**をクリックまたはタップします。
2. ユーザーまたはグループを選択してから、**[リムーバブル ディスク ドライブ]**または**[DVD/CD-ROM ドライブ]**の**[アクセス]**で下向き矢印をクリックまたはタップし、**[許可: ジャスト イン タイム認証が必要]**を選択します。
3. **[継続時間]**で下向き矢印をクリックまたはタップして、ジャスト イン タイム認証アクセスの期間を選択します。

新しいジャスト イン タイム認証の設定が適用されるには、ユーザーはログアウトして再びログインする必要があります。

### ユーザーまたはグループのジャスト イン タイム認証ポリシーの無効化

管理者は、ジャスト イン タイム認証を使用してユーザーまたはグループがデバイスにアクセスすることを無効にできます。


1. **[HP Device Access Manager]**を起動し、**[変更]**をクリックまたはタップします。
2. ユーザーまたはグループを選択してから、**[リムーバブル ディスク ドライブ]**または**[DVD/CD-ROM ドライブ]**の**[アクセス]**で下向き矢印をクリックまたはタップし、**[拒否]**を選択します。

ユーザーがログインし、デバイスにアクセスしようすると、アクセスは拒否されます。



# 設定

[設定]ビューで管理者は、HP Device Access Managerによって制御されるアクセス権が設定されたドライブを表示および変更できます。

 **注記:** ドライブ文字の一覧が構成されている場合は、HP Device Access Managerが有効になっている必要があります (46 ページの「[システム]ビュー」を参照してください)。

## 管理されないデバイス クラス

HP Device Access Manager では、以下のデバイス クラスは管理されません。

- 入出力デバイス
  - CD-ROM
  - ディスク ドライブ
  - フロッピー ディスク コントローラー (FDC)
  - ハード ディスク コントローラー (HDC)
  - ヒューマン インターフェイス デバイス (HID) クラス
  - 赤外線ヒューマン インターフェイス デバイス
  - マウス
  - マルチコネクタ シリアル
  - キーボード
  - プラグ アンド プレイ (PnP) プリンター
  - プリンター
  - プリンター アップグレード
- 電源
  - Advanced Power Management (APM) サポート
  - バッテリー
- その他
  - コンピューター
  - デコーダー
  - ディスプレイ
  - Intel®統合ディスプレイ ドライバー
  - Legacard
  - メディア ドライバー
  - メディア チェンジャー
  - メモリ テクノロジ
  - モニター
  - 多機能

- ネット クライアント
- ネット サービス
- ネット転送
- プロセッサ
- SCSI アダプター
- セキュリティ アクセラレータ
- セキュリティ デバイス
- システム
- 不明
- ボリューム
- ボリューム スナップショット

## 8 HP Trust Circles

HP Trust Circles は、フォルダー ファイル暗号化とトラスト サークルに基づく便利なドキュメント共有機能とを組み合わせた、ファイルおよびドキュメント セキュリティ アプリケーションです。このアプリケーションは、ユーザーが指定したフォルダーに置かれたファイルを暗号化し、それらをトラスト サークル内で保護します。保護されたファイルは、その後、トラスト サークルのメンバーによってのみ使用および共有できます。保護されたファイルをメンバー以外のユーザーが受信しても、ファイルは暗号化されたままなので、メンバー以外のユーザーがファイルの内容にアクセスすることはできません。

### HP Trust Circles を開く

1. スタート画面で[HP Client Security]アプリケーションをクリックまたはタップします。  
または  
Windows デスクトップで、タスクバーの右端の通知領域にある[HP Client Security]アイコンをダブルクリックします。
2. [データ]で、[HP Trust Circles]をクリックまたはタップします。


### お使いになる前に

電子メール招待状を送信し、それらに返信する方法は2つあります。

- **[Microsoft®Outlook を使用する]** : HP Trust Circles で Microsoft Outlook を利用すれば、HP Trust Circle の招待状および他の HP Trust Circle ユーザーからの返信の処理を自動化できます。
- **[Gmail、Yahoo、Outlook.com などの他の電子メール サービスを使用する (SMTP) ]** : 自分の名前、電子メール アドレス、およびパスワードを入力すると、これらの電子メール サービス経由で、トラスト サークルに参加するよう選択したメンバーに電子メール招待状が送信されます。

基本プロフィールをセットアップするには、以下の操作を行います。

1. 自分の名前および電子メール アドレスを入力し、[次へ]をクリックまたはタップします。  
この名前は、トラスト サークルに参加するよう招待されたすべてのメンバーに表示されます。電子メール アドレスは、招待状の送信、受信、または招待状への返信に使用されます。
2. 電子メール アカウントのパスワードを入力し、[次へ]をクリックまたはタップします。  
電子メール設定が正しいかどうか確認するため、テスト メールが送信されます。

 **注記:** コンピューターがネットワークに接続されている必要があります。

3. [HP Trust Circle 名]フィールドにトラスト サークルの名前を入力し、[次へ]をクリックまたはタップします。
4. メンバーとフォルダーを追加して、[次へ]をクリックまたはタップします。選択したフォルダーを使ってトラスト サークルが作成され、選択したメンバーに電子メール招待状が送信されます。何かの理由で招待状が送信できない場合は、通知が表示されます。メンバーは[HP Trust Circle]

ビューからいつでも再招待できます。**[Your Trust Circles]**（自分のトラスト サークル）をクリックしてから、目的のトラスト サークルをダブルクリックまたはダブルタップしてください。詳しくは、[52 ページの「Trust Circle」](#)を参照してください。

## Trust Circle


トラスト サークルは、初期セットアップで自分の電子メール アドレスを入力した後か、[HP Trust Circle]ビュー上で作成できます。

- ▲ [HP Trust Circle]ビューから、**[Create Trust Circle]**（トラスト サークルの作成）をクリックまたはタップし、次にトラスト サークルの名前を入力します。
  - トラスト サークルにメンバーを追加するには、**[メンバー]**の横にある**[M +]**アイコンをクリックまたはタップし、画面の説明に沿って操作します。
  - トラスト サークルにフォルダーを追加するには、**[フォルダー]**の横にある**[+]**アイコンをクリックまたはタップし、画面の説明に沿って操作します。

### トラスト サークルへのフォルダーの追加


新しいトラスト サークルにフォルダーを追加するには、以下の操作を行います。

- トラスト サークルの作成中に、**[フォルダー]**の横にある**[+]**アイコンをクリックまたはタップし、画面の説明に沿って操作すればフォルダーを追加できます。  
または
- Windows の[エクスプローラー]で、現在トラスト サークルに含まれていないフォルダーを右クリックするかまたはタップしたまま押さえて、**[HP Trust Circle]**を選択し、次に**[Create Trust Circle from Folder]**（フォルダーからのトラスト サークルの作成）を選択します。

 **ヒント：** フォルダーは 1 つまたは複数選択できます。

既存のトラスト サークルにフォルダーを追加するには、以下の操作を行います。

- [HP Trust Circle]ビューから、**[Your Trust Circles]**（自分のトラスト サークル）をクリックし、既存のトラスト サークルをダブルクリックまたはダブルタップして現在のフォルダーを表示し、**[フォルダー]**の横にある**[+]**アイコンをクリックまたはタップして、画面の説明に沿って操作します。  
または
- Windows の[エクスプローラー]で、現在トラスト サークルに含まれていないフォルダーを右クリックするかまたはタップしたまま押さえて、**[HP Trust Circle]**を選択し、次に**[Add to existing Trust Circle from Folder]**（フォルダーからの既存のトラスト サークルへの追加）を選択します。

 **ヒント：** フォルダーは 1 つまたは複数選択できます。

フォルダーをトラスト サークルに追加すると、HP Trust Circles によってそのフォルダーと内容が自動的に暗号化されます。対象ファイルすべての暗号化が完了すると、通知が表示されます。さらに、暗号化されたすべてのフォルダー アイコンおよびフォルダー内のファイル アイコンに、完全に保護されていることを示す緑色のロック記号が表示されます。

## トラスト サークルへのメンバーの追加

トラスト サークルにメンバーを追加するには、以下の3つの手順が必要です。

1. **招待**：最初に、トラスト サークルの所有者がメンバーを招待します。招待の電子メールは、複数のユーザーまたは配布リスト/グループに送信できます。
2. **承認**：被招待者が招待を受信し、承認するか拒否するかを選択します。被招待者が招待を承認すれば、電子メールの返信が招待者に送信されます。招待状がグループ宛てに送信された場合、各メンバーが招待状を受信し、承認するか拒否するかを選択します。
3. **登録**：招待者が、個々のメンバーをトラスト サークルに追加するかどうかを最終的に決定します。招待者がメンバーの登録を決定すると、返信が了承されたことを通知する電子メールが被招待者に送信されます。招待者および被招待者はオプションで、招待の処理のセキュリティを確認できます。被招待者に検証コードが表示されますので、被招待者は招待者に電話でこのコードを読み上げる必要があります。コードの確認が完了すると、招待者は最終登録の電子メールを送信できます。

新しいトラスト サークルにメンバーを追加するには、以下の操作を行います。

- ▲ **トラスト サークルの作成中に、[メンバー]の横にある[M +]アイコンをクリックまたはタップし、画面の説明に沿って操作すればメンバーを追加できます。**
  - Microsoft Outlook を使用している場合は、Microsoft Outlook のアドレス帳から連絡先を選択し、**[OK]**をクリックします。
  - その他の電子メール サービスを使用している場合は、新しい電子メール アドレスを手動で HP Trust Circle に追加するか、HP Trust Circle に登録されている電子メール アドレスから取得されるように設定できます。

既存のトラスト サークルにメンバーを追加するには、以下の操作を行います。

- ▲ **[HP Trust Circle]ビューから、[Your Trust Circles]（自分のトラスト サークル）をクリックし、既存のトラスト サークルをダブルクリックまたはダブルタップして現在のメンバーを表示し、[メンバー]の横にある[M +]アイコンをクリックまたはタップして、画面の説明に沿って操作します。**
  - Microsoft Outlook を使用している場合は、Microsoft Outlook のアドレス帳から連絡先を選択し、**[OK]**をクリックします。
  - その他の電子メール サービスを使用している場合は、新しい電子メール アドレスを手動で HP Trust Circle に追加するか、HP Trust Circle に登録されている電子メール アドレスから取得されるように設定できます。

## トラスト サークルへのファイルの追加

トラスト サークルに、以下のどちらかの方法でファイルを追加できます。


- 既存のトラスト サークル フォルダーに目的のファイルをコピーまたは移動します。  
または
- Windows の[エクスプローラー]で、現在暗号化されていないファイルを右クリックするかまたはタップしたまま押さえて、**[HP Trust Circle]**を選択し、次に**[暗号化]**を選択します。そのファイルを追加するトラスト サークルを選択するよう求められます。



**ヒント：** ファイルは1つまたは複数選択できます。

## 暗号化されたフォルダー

トラスト サークルのメンバーは、そのトラスト サークルに属するファイルを表示および編集できます。


 **注記：** Trust Circle Manager/Reader は、メンバー間でファイルの同期を行いません。

ファイルは、電子メール、FTP、クラウド ストレージ プロバイダーなど既存の方法で共有する必要があります。トラスト サークルのフォルダー内にコピー、移動、または作成されたファイルはすぐに保護されます。

## トラスト サークルからのフォルダーの削除

トラスト サークルからフォルダーを削除すると、そのフォルダーおよびそのすべての内容の暗号化が解除され、保護されなくなります。

- [HP Trust Circle]ビューから、[Your Trust Circles]（自分のトラスト サークル）をクリックまたはタップし、既存のトラスト サークルをダブルクリックまたはダブルタップして現在のフォルダーを表示し、目的のフォルダーの横にある[ごみ箱]アイコンをクリックまたはタップします。  
または
- Windows の[エクスプローラー]で、現在トラスト サークルに含まれているフォルダーを右クリックするかまたはタップしたまま押さえて、[HP Trust Circle]を選択し、次に[Remove from trust circle]（トラスト サークルからの削除）を選択します。

 **ヒント：** フォルダーは1つまたは複数選択できます。

## トラスト サークルからのファイルの削除

トラスト サークルからファイルを削除するには、Windows の[エクスプローラー]で、現在暗号化されていないファイルを右クリックするかまたはタップしたまま押さえて、[HP Trust Circle]を選択し、次に[Decrypt File]（ファイルの復号化）を選択します。

## トラスト サークルからのメンバーの削除

完全に登録されたメンバーをトラスト サークルから削除する方法はありません。考えられる代替案は、その他のメンバーで新しいトラスト サークルを作成し、すべてのファイルおよびフォルダーを新しいトラスト サークルに移動してから、古いトラスト サークルを削除することです。これにより、古いトラスト サークルのメンバーは、削除されたメンバーが受信する新しいファイルにはアクセスできなくなりますが、以前から共有されていたすべての情報には引き続きアクセスできます。

完全には登録されていないメンバー（トラスト サークルに加わるよう招待されたメンバー、またはトラスト サークルへの招待をまだ承認していないメンバー）の場合は、以下のどちらかの方法でそのメンバーをトラスト サークルから削除できます。

- [HP Trust Circle]ビューから、[Your Trust Circles]（自分のトラスト サークル）をクリックまたはタップし、次に目的のトラスト サークルをダブルクリックまたはダブルタップして現在のメンバーの一覧を表示します。削除するメンバー名の横にある[ごみ箱]アイコンをクリックまたはタップします。
- [HP Trust Circle]ビューから、[メンバー]をクリックまたはタップし、次に目的のメンバーをダブルクリックまたはダブルタップして現在メンバーとなっているトラスト サークルの一覧を表示します。トラスト サークルの横にある[ごみ箱]アイコンをクリックまたはタップすると、そのトラスト サークルからそのメンバーが削除されます。

## トラスト サークルの削除

トラスト サークルを削除するには、オーナーシップが必要です。

- ▲ [HP Trust Circle]ビューから、[Your Trust Circles]（自分のトラスト サークル）をクリックまたはタップし、削除するトラスト サークルの横にある[ごみ箱]アイコンをクリックまたはタップします。

これによりページからそのトラスト サークルが消去され、そのトラスト サークルのすべてのメンバーにトラスト サークルが削除されたことを通知する電子メールが送信されます。削除されたトラスト サークルに含まれていたファイルやフォルダーはすべて暗号化解除されます。

## 設定の指定

[HP Trust Circle]ビューから、[Preferences]（設定）をクリックまたはタップします。3つのタブが表示されます。

- [Email Settings]（電子メール設定）

オプション	説明
[Username]（ユーザー名）	現在使用中のユーザー名が表示されます。変更する場合は、テキスト ボックスに新しいユーザー名を入力します。変更は自動的に保存されます
[Email Address]（電子メール アドレス）	現在使用中の電子メール アカウントが表示されます。変更する場合は、[Change Email Settings]（電子メール設定の変更）をクリックまたはタップし、画面の説明に沿って操作します
[New Member Confirmation]（新しいメンバーの確認）	以下のオプションから選択します <ul style="list-style-type: none"><li>◦ [Confirm Automatically]（自動的に確認する）：被招待者から承認を受信すると、それらの被招待者が手動入力なしで確認されトラスト サークルに追加されます。確認の電子メールが被招待者に送信されます</li><li>◦ [Confirm Manually]（手動で確認する）：被招待者から承認を受信すると、新しいメンバーをトラスト サークルに登録するために手動入力が必要になります。その後、確認の電子メールが被招待者に送信されます</li><li>◦ [Require Verification]（検証を要求する）：被招待者から承認を受信すると、被招待者を完全に登録するために検証コードが要求されます。トラスト サークルの所有者は、被招待者と連絡を取り、被招待者から検証コードを取得します。正しいコードが入力されると、確認の電子メールが送信されます</li></ul>
[Periodic Authentication]（定期認証）	Periodic authentication（定期認証）では、指定されたタイムアウト（分単位で記録）経過後に、ユーザーに Windows パスワードの入力を要求します。機密性の高い操作の実行中にも入力を要求します。この設定により、ユーザーは認証のオン/オフを切り替えることができます
[Authentication Timeout]（認証タイムアウト）	認証が要求されるまでの指定のタイムアウト期間（分単位で記録）を選択します
[Don't show confirmation message]（次回から確認メッセージを表示しない）	確認メッセージの表示を無効にするにはチェック ボックスにチェックを入れ、確認メッセージを表示するにはチェック ボックスのチェックを外します
[I'd like to help improve the HP Trust Circle through anonymous usage tracking]（匿名の使用追跡を通して HP Trust Circle の改善に寄与する）	このプログラムに参加するにはチェック ボックスにチェックを入れ、参加しない場合はチェック ボックスのチェックを外します



- **[Backup/Restore]** (バックアップ/復元)

オプション	説明
<b>[Backup]</b> (バックアップ)	<p>Trust Circle Manager/Reader アプリケーションのデータ (各設定値およびトラスト サークル) をバックアップ ファイルにコピーします。クラッシュやシステム障害が発生した場合は、このファイルを使用して、HP Trust Circles の新しいインストールをファイルに保存された状態にまで復元できます</p> <p><b>注記:</b> ご使用の HP Trust Circle のアプリケーション データ (トラスト サークル、各種設定、およびメンバー) のみが保存されます。トラスト サークル フォルダ内の実際のファイルはバックアップされません。それらのファイルは個別にバックアップしてください</p> <p>トラスト サークルの設定およびユーザー データをバックアップするには、以下の操作を行います</p> <ol style="list-style-type: none"> <li>1. <b>[バックアップ]</b> をクリックまたはタップします</li> <li>2. バックアップ ファイルのファイル名およびディレクトリを選択して、<b>[保存]</b> をクリックまたはタップします</li> <li>3. パスワードを入力し確認してから、<b>[OK]</b> をクリックまたはタップします。このパスワードは、このファイルを復元する場合に必要となります</li> </ol>
<b>[Restore]</b> (復元)	<p>バックアップ ファイルから各種設定値およびトラスト サークルを復元します。通常は、システム クラッシュや他のコンピューターへの移行の後にを行います</p> <p>Trust Circle Manager の設定およびユーザー データを復元するには、以下の操作を行います</p> <ol style="list-style-type: none"> <li>1. <b>[復元]</b> をクリックまたはタップします</li> <li>2. バックアップ ファイルのディレクトリおよびファイル名まで移動して、<b>[開く]</b> をクリックまたはタップします</li> <li>3. バックアップの作成中にセットアップされたパスワードを入力します</li> </ol>

- **[About]** (バージョン情報) : Trust Circle Manager/Reader ソフトウェアのバージョンが表示されます。HP Trust Circle Manager を Pro バージョンにアップグレードしたり、HP のプライバシーに関する声明を表示したりできるリンクが表示されます。

## 9 盗難からの回復（一部のモデルのみ）

Computrace（別売）を使用すると、コンピューターをリモートで監視、管理、および追跡できます。

Computrace を有効にすると、Absolute Software カスタマー センターからツールの設定が行われます。管理者は Absolute Software カスタマー センターから Computrace を設定し、コンピューターを監視または管理できます。システムの置き忘れや盗難が発生した場合、Absolute Software カスタマー センターはコンピューターを探索し取り戻すために地域当局に協力します。設定によって、ハードドライブが消去または交換された場合でも Computrace が動作し続けるようにすることができます。

Computrace を有効にするには、以下の操作を行います。

1. インターネットに接続します。
2. HP Client Security を開きます。詳しくは、[9 ページの「HP Client Security を開く」](#)を参照してください。
3. **[盗難からの回復]**をクリックします。
4. Computrace 有効化ウィザードを起動するには、**[開始]**をクリックします。
5. 連絡先情報とクレジットカードの支払い情報を入力するか、または事前に購入したプロダクトキーを入力します。

[有効化ウィザード]によって取引が安全に処理され、Absolute Software カスタマー センターの Web サイトにユーザー アカウントがセットアップされます。完了すると、カスタマー センターのアカウント情報を含む確認の電子メールが届きます。

以前に Computrace 有効化ウィザードを実行したことがあり、Absolute Software カスタマー センターのユーザー アカウントをすでに持っている場合は、サポート窓口にお問い合わせで追加ライセンスを購入できます。

カスタマー センターにログオンするには、以下の操作を行います。

1. <https://cc.absolute.com/>（英語サイト）にアクセスして、ドロップダウン リストから**[日本語]**を選択します。
2. **[ユーザー名]**フィールドおよび**[パスワード]**フィールドに、確認の電子メールで受信した資格情報を入力し、**[ログイン]**をクリックします。

カスタマー センターでは、以下の操作を実行できます。

- コンピューターの監視
- リモート データの保護
- Computrace で保護されているコンピューターの盗難の報告
- ▲ Computrace について詳しくは、**[詳細情報]**をクリックしてください。

## 10 ローカライズされたパスワードの例外事項

電源投入時認証レベルおよび HP Drive Encryption レベルでは、パスワードのローカライズのサポートに制限があります。詳しくは、[58 ページの「電源投入時認証レベルおよび HP Drive Encryption レベルでの Windows IME の非サポート」](#)を参照してください。

### パスワードが拒否された場合の対処方法

パスワードは、以下の原因で拒否されることがあります。

- サポートされていない IME をユーザーが使用している場合。これは、2 バイト文字言語（韓国語、日本語、中国語）ではよく起こる問題です。この問題を解決するには、以下の操作を行います。
  1. [コントロール パネル]を使用して、サポートされているキーボード レイアウトを追加します（[入力言語]の[中国語]の下で、[US/英語]キーボードを追加します）。
  2. サポートされているキーボードを初期の入力言語に設定します。
  3. HP Client Security を起動して、Windows パスワードを入力します。
- ユーザーがサポートされていない文字を使用している場合。この問題を解決するには、以下の操作を行います。
  1. サポートされている文字のみを使用するように Windows パスワードを変更します。サポートされていない文字について詳しくは、[59 ページの「特別なキーの扱い」](#)を参照してください。
  2. HP Client Security を起動して、Windows パスワードを入力します。


### 電源投入時認証レベルおよび HP Drive Encryption レベルでの Windows IME の非サポート

Windows では、IME（入力方式エディター）を選択することによって、日本語や中国語の文字などの複雑な文字および記号を、一般的な西洋言語用のキーボードを使用して入力できます。

Windows の IME は、電源投入時認証レベルおよび HP Drive Encryption レベルではサポートされていません。電源投入時認証または HP Drive Encryption のログイン画面では、IME を使用して Windows パスワードを入力することはできません。また、入力しようとする、ロックアウトが発生することがあります。場合によっては、パスワードの入力時に Microsoft® Windows によって IME が表示されないこともあります。


この問題を解決するには、以下のどれかのキーボード レイアウトに切り替えます。これらのキーボード レイアウトは、キーボード レイアウト 00000411 に変換されるため、電源投入時認証レベルおよび HP Drive Encryption レベルでもサポートされます。

- 日本語 Microsoft IME
- 日本語キーボード レイアウト
- Office 2007 IME（日本語）：Microsoft や他社が、IME または入力方式エディターという用語を使用している場合、その入力方式は実際には IME ではないことがあります。このため、混乱が生じることもありますが、ソフトウェアは 16 進表記を読み取ります。したがって、サポートされているキーボード レイアウトに IME がマッピングされている場合、HP Client Security はその設定をサポートできます。

 **警告！** HP Client Security を使用すると、Windows IME を使用して入力したパスワードは拒否されます。

## サポートされている別のキーボード レイアウトを使用したパスワードの変更

初期パスワードをあるキーボード レイアウト（たとえば、英語（米国）（409））を使用して設定し、後から、サポートされている別のキーボード レイアウト（たとえば、ラテン アメリカ言語（080A））を使用して変更すると、そのパスワードの変更は HP Drive Encryption では正常に認識されます。ただし、ラテン アメリカ言語に存在して、英語（米国）には存在しない文字（たとえば、é）を使用すると、BIOS では正常に認識されません。

 **注記：** 管理者はこの問題を解決できます。HP Client Security の[ホーム]ページでギアの絵の[設定]アイコンを選択し、[ユーザー]ページにアクセスして、HP Client Security からこのユーザーを削除します。その後、オペレーティング システムで目的のキーボード レイアウトを選択してから、同じユーザーに対して HP Client Security セットアップ ウィザードを実行しなおします。BIOS に目的のキーボード レイアウトが保存され、このキーボード レイアウトを使用して入力できるパスワードが BIOS 内に適切に設定されます。

もう 1 つ問題になる可能性があるのが、同じ文字を出力できる、異なるキーボード レイアウトを使用している場合です。たとえば、米国インターナショナル キーボード レイアウト（20409）とラテンアメリカ言語キーボード レイアウト（080A）は、どちらも文字 é を出力できますが、異なる順序でキーを操作しなければならないことがあります。最初にラテン アメリカ言語キーボード レイアウトを使用してパスワードを設定すると、その後に米国インターナショナル キーボード レイアウトを使用してパスワードを変更しても、BIOS にはラテン アメリカ言語キーボード レイアウトが設定されます。

## 特別なキーの扱い

- 中国語、スロバキア語、カナダ フランス語、およびチェコ語  
上記のキーボード レイアウトのどれかを選択してパスワードを入力した場合（たとえば、abcdef）、電源投入時認証および HP Drive Encryption では、同じパスワードを小文字の場合は **shift** キーを押しながら、大文字の場合は **shift** キーと **Caps Lock** キーを押しながら入力する必要があります。数字のパスワードは、**テンキー**を使用して入力する必要があります。
- 韓国語  
サポートされている韓国語キーボード レイアウトを選択してパスワードを入力した場合、電源投入時認証および HP Drive Encryption では、同じパスワードを小文字の場合は右 **alt** キーを押しながら、大文字の場合は右 **alt** キーと **Caps Lock** キーを押しながら入力する必要があります。

- サポートされていない文字は、以下の表のとおりです。

言語	Windows	BIOS	Drive Encryption
アラビア語	ﻻ, ﻻ, およびﻻキーは、2文字になります	ﻻ, ﻻ, およびﻻキーは、1文字になります	ﻻ, ﻻ, およびﻻキーは、1文字になります
カナダ フランス語	<b>Caps Lock</b> を押した状態で入力した ç, è, à, および é は、Windows では Ç, È, À, および É になります	<b>Caps Lock</b> を押した状態で入力した ç, è, à, および é は、電源投入時認証では ç, è, à, および é になります	<b>Caps Lock</b> を押した状態で入力した ç, è, à, および é は、HP Drive Encryption では ç, è, à, および é になります
スペイン語	40a はサポートされていません。ただし、ソフトウェアによって c0a に変換されるため、40a は正常に動作します。しかし、これらのキーボード レイアウトはわずかに異なるため、スペイン語を話すユーザーは、Windows のキーボード レイアウトを 1040a (スペイン語 (バリエーション)) または 080a (ラテン アメリカ言語) に変更することをおすすめします	- - -	- - -
米国インターナショナル	<ul style="list-style-type: none"> <li>◦ 一番上の行にある j, ð, ‘, ’, ¥, および × キーは拒否されます</li> <li>◦ 2 番目の行にある à, ®, および ò キーは拒否されます</li> <li>◦ 3 番目の行にある á, ð, および ø キーは拒否されます</li> <li>◦ 一番下の行にある æ キーは拒否されます</li> </ul>	- - -	- - -
チェコ語	<ul style="list-style-type: none"> <li>◦ ě キーは拒否されます</li> <li>◦ ě キーは拒否されます</li> <li>◦ ů キーは拒否されます</li> <li>◦ é, í, および z キーは拒否されます</li> <li>◦ ě, ě, ě, ů, および ě キーは拒否されます</li> </ul>	- - -	- - -
スロバキア語	ž キーは拒否されます	<ul style="list-style-type: none"> <li>◦ š, š, および š キーは、入力した場合は拒否されますが、ソフト キーボードを使用して入力した場合は受け入れられます</li> <li>◦ ť デッド キーは 2 文字になります</li> </ul>	- - -
ハンガリー語	ž キーは拒否されます	ť キーは 2 文字になります	- - -

言語	Windows	BIOS	Drive Encryption
スロベニア語	zž キーは Windows では拒否されます。また、alt キーは、BIOS ではデッド キーとなります	ú、Ú、û、Û、š、Š、ś、Ś、š、および Š キーは、BIOS では拒否されます	- - -
日本語	利用できる場合は、Microsoft Office 2007 IME を選択することをおすすめします。IME という名前は付いていますが、実際にはキーボード レイアウト 411 であり、サポートされています	- - -	- - -

# 用語集

## Bluetooth

無線伝送を使用することで、Bluetooth 対応のコンピューター、プリンター、マウス、携帯電話などのデバイス間で短距離の無線通信を実行できるようにした技術。

## Drive Encryption

ハードドライブを暗号化して、適切な権限のないユーザーが情報を読み取れないようにすることによってデータを保護します。

### Drive Encryption のブート前認証

Windows が起動する前に表示されるログイン画面。ユーザーは、Windows のユーザー名およびパスワードまたはスマート カードの PIN を入力するか、登録した指紋を認証システムで読み取らせる必要があります。ワンステップ ログオンが選択されている場合、Drive Encryption のログイン画面で正しい情報を入力すれば、Windows のログイン画面で再度ログインすることなく、直接 Windows にアクセスできます。

### Drive Encryption のログオン画面

「Drive Encryption のブート前認証」を参照してください。

## DriveLock

ハードドライブをユーザーにリンクして、コンピューターの起動時にユーザーに正しい DriveLock パスワードの入力を要求するセキュリティ機能。

## HP SpareKey のリカバリ

セキュリティに関する質問に正しく回答することでコンピューターにアクセスできる機能。

## ID

HP Client Security (HP クライアント セキュリティ) 内で、特定のユーザーのアカウントまたはプロファイルのように処理される、証明情報と設定の集合。

## ID カード

ユーザー名および選択された画像を使用してデスクトップを視覚的に識別するための、Windows デスクトップのガジェット。

## PIN

登録されたユーザーが認証に使用する個人識別番号 (Personal Identification Number)。

## PKI

資格情報および暗号化キーを作成、使用、および管理するためのインターフェイスを定義する、公開キー基盤の規格。

## Trust Circle

データを定義済みの信頼されるユーザーのグループに結合することで、データの封じ込めを実現します。これにより、過失、故意を問わず、データが権限のない第三者の手に渡ることを防止します。CryptoMill の Zero Overhead Key Management テクノロジーでセキュリティ保護され、データはトラスト サークルに暗号化されて結合されます。これにより、トラスト サークル外でドキュメントやその他の機密情報が暗号化解除されるのを防止します。

## Trust Circle Manager/Reader

Trust Circle Reader は、HP Trust Circle Manager のユーザーによって送信された招待状の承認のみが可能です。これに対し、HP Trust Circle Manager では、トラスト サークルを作成できます。電子メールでトラスト サークルに招待したり、トラスト サークルへの招待状を承認したりできます。トラスト サークルがメンバー間で確立されると、そのトラスト サークルによって保護されるファイルを安全に共有できます。



## **Trusted Platform Module (トラステッド プラットフォーム モジュール) 内蔵セキュリティ チップ**

TPM では、ホスト システムに固有の情報 (暗号化キー、デジタル署名、パスワードなど) が格納され、ユーザーではなくコンピューターが認証されます。TPM を使用すると、物理的な盗難や外部のハッカーによる攻撃によってコンピューター上の情報が危険にさらされるリスクを最小限に抑えることができます。

### **Windows 管理者**

アクセス権を変更し、他のユーザーを管理するすべての権限を持つユーザー。

### **Windows ユーザー アカウント**

ネットワークまたは個別のコンピューターへのログオンを承認されたユーザー。

### **Windows ログオンのセキュリティ**

アクセスのために特定の資格情報を使用するよう求めることで、Windows アカウントを保護できます。

### **空き領域ブリーチ**

削除されたフォルダー、ファイル、または未使用領域にランダムなデータを上書きすることです。この処理を実行すると、削除されたフォルダーやファイルが存在する可能性が少なくなり、元のフォルダーやファイルの復元がより困難になります。

### **暗号化**

権限のない受信者がデータを解読できないように平文を暗号文に変換するための、暗号法で使用されるアルゴリズムなどの手順。データの暗号化にはさまざまな種類があり、ネットワーク セキュリティの基礎として使用されます。一般的な暗号化には、データ暗号化規格 (DES) や公開キー暗号があります。

### **暗号化の解除**

暗号化されたデータを平文に変換するための、暗号法で使用される手順。

### **暗号化ファイル システム (EFS)**

選択されたフォルダー内のすべてのファイルおよびサブフォルダーを暗号化するシステム。

### **管理者**

「Windows 管理者」を参照してください。

### **緊急リカバリ アーカイブ**

他のプラットフォームの所有者キーを使用して基本ユーザー キーを再暗号化できる、保護された記憶領域。

### **近接型カード**

認証時のセキュリティ強化のために他の資格情報と組み合わせて使用できるコンピューター チップが内蔵されたプラスチック製のカード。

### **グループ**

デバイス クラスまたは特定のデバイスに対して同じレベルのアクセス許可またはアクセス拒否が設定されているユーザーのグループ。

### **自動シュレッド**

File Sanitizer でスケジュール設定したフォルダーやファイルをシュレッドすることです。

### **指紋**

指紋の画像をデジタルの形式で抽出したもの。実際の指紋の画像は、HP Client Security には保存されません。

### **ジャスト イン タイム認証**

HP Device Access Manager ソフトウェアのヘルプを参照してください。

### **手動シュレッド**

単一のフォルダーやファイルまたは選択されている複数のフォルダーやファイルに対して、シュレッド スケジュールを省略して実行されるシュレッド。

### **シュレッド**

フォルダーやファイルに含まれるデータを、意味を持たないデータで上書きするアルゴリズムを実行すること。

### **証明情報**

個々のユーザーを認証するために使用される特定の情報またはハードウェア デバイス。

#### **シングルサインオン**

認証情報を格納し、パスワード認証が必要なインターネットおよび Windows アプリケーションに HP ProtectTools Security Manager (HP ProtectTools セキュリティ マネージャー) を使用してアクセスできるようにする機能。

#### **スマート カード**

PIN と組み合わせて認証に使用できるハードウェア デバイス。

#### **セキュリティ ログオン方法**

コンピューターへのログオンに使用される方法。

#### **接続されたデバイス**

コンピューターのコネクタに接続されているハードウェア デバイス。

#### **ソフトウェアによる暗号化**

ソフトウェアを使用してハードドライブを 1 セクターずつ暗号化すること。このプロセスはハードウェアによる暗号化よりも低速です。

#### **デバイス アクセス制御ポリシー**

ユーザーがアクセスを許可または拒否されているデバイスの一覧。

#### **デバイス クラス**

ドライブなど、特定の種類にあてはまるすべてのデバイス。

#### **電源投入時認証**

スマート カード、セキュリティ チップ、パスワードなど、コンピューターの起動時に何らかの形式の認証を要求するセキュリティ機能。

#### **ドメイン**

ネットワークの一部であり、共通のディレクトリ データベースを共有するコンピューターの集合。ドメインには一意の名前が付けられ、各ドメインには一連の共通の規則および手順が設定されます。

#### **トラスト サークル フォルダー**

トラスト サークルによって保護されるフォルダーのこと。

#### **認証**

Windows パスワード、指紋、スマート カード、非接触型カード、または近接型カードなどの資格情報を使用して、自分が本来のユーザーであることを検証するプロセス。

#### **ネットワーク アカウント**

ローカル コンピューター上、ワークグループ内、またはドメイン上の Windows ユーザーまたは管理者のアカウント。

#### **ハードウェアによる暗号化**

自己暗号化ドライブの管理に関する Trusted Computing Group の OPAL 仕様に適合する自己暗号化ドライブを使用して、即座に暗号化を完了すること。ハードウェアによる暗号化は即座に行われ、数分しかかからない場合がありますが、ソフトウェアによる暗号化には数時間かかることがあります。

#### **バックアップ**

バックアップ機能を使用して、重要なプログラム情報のコピーをそのプログラムの外部の場所に保存すること。バックアップした内容は、後日、同じコンピューターまたは別のコンピューターに情報を復元するために使用できます。

#### **非接触型カード**

認証に使用できるコンピューター チップが内蔵されたプラスチック製のカード。

#### **フォルダー/ファイル**

個人の情報やファイル、履歴や Web 関連のデータなどを含むデータ コンポーネントのことで、ハードドライブ上に存在します。

## **復元**

以前に保存されたバックアップ ファイルから、プログラム情報をこのプログラムにコピーするプロセス。

## **[ホーム]ページ**

HP Client Security の機能および設定に対するアクセスや管理を行うことができる、中心となる場所。

## **有効化**

Drive Encryption の機能にアクセスする前に完了する必要があるタスク。管理者は、HP Client Security セットアップ ウィザードまたは[HP Client Security]を使用して HP Drive Encryption を有効にできます。有効化プロセスは、ソフトウェアの有効化、ドライブの暗号化、およびリムーバブル ストレージ デバイス上の初期バックアップ暗号化キーの作成で構成されます。

## **ユーザー**

Drive Encryption に登録された人。管理者以外のユーザーは、Drive Encryption での権限が制限されています。管理者以外のユーザーが実行できる操作は、登録（管理者の許可がある場合）とログオンのみです。

## **リブート**

コンピューターを再起動するプロセス。

## **ログオン**

Web サイトやその他のプログラムにログオンするために使用できるユーザー名とパスワード（またはその他の選択された情報）で構成される、HP Client Security 内のオブジェクト。

# 索引

- B**  
Bluetooth デバイス 15
- C**  
Computrace 57
- D**  
Drive Encryption  
開く 30  
無効化 32
- H**  
HP Client Security 12  
機能 1  
詳細設定 25  
セットアップ 8  
[バックアップおよび復元]パスワード 6  
開く 9  
HP Device Access Manager 45  
イージー セットアップ 11  
起動 46  
HP Drive Encryption 30, 33  
イージー セットアップ 11  
管理 33  
個々のドライブの暗号化 33  
個々のドライブの暗号化解除 33  
実行 31  
バックアップおよび復元 34  
無効化 31  
有効化後のログイン 31  
HP File Sanitizer 37, 42  
起動 38  
セットアップ手順 39  
HP ProtectTools for Small Business イージー セットアップガイド 10  
HP SpareKey 14  
設定 15  
リカバリ 36  
HP Trust Circles 51  
開く 51
- M**  
My Policies (マイ ポリシー) 28
- P**  
Password Manager (パスワード マネージャー) 18, 19  
イージー セットアップ 10  
保存されている認証の表示および管理 11  
PIN 18  
スマート カード 6
- R**  
RSA SecurID 18
- T**  
Trust Circle  
起動 51
- W**  
Windows のログオン パスワード 6  
Windows パスワード、変更 15
- あ**  
アイコン、使用 42  
空き領域ブリーチ 41  
開始 43  
アクセス  
制御 45  
不正の防止 5  
暗号化  
解除、ドライブ 30  
ソフトウェア 31, 32, 34  
ドライブ 30  
ハードウェア 31, 32  
フォルダー 54  
暗号化キーのバックアップ 34
- お**  
お使いになる前に 10, 51  
主なセキュリティの目的 4
- か**  
カード 16  
管理  
ドライブ パーティションの暗号化または暗号化の解除 34  
パスワード 18, 19  
管理されないデバイス クラス 49  
管理者設定  
指紋 13, 14
- き**  
起動  
HP Device Access Manager 46  
HP File Sanitizer 38  
機能、HP Client Security 1
- く**  
[クイック リンク]メニュー、HP Password Manager 21
- こ**  
構成  
デバイス クラス 46  
異なるキーボード レイアウトを使用したパスワードの変更 59  
コンピューターへのログイン 32
- し**  
[システム]ビュー 46  
指紋  
管理者設定 13  
登録 13  
ユーザー設定 14  
ジャスト イン タイム認証の構成 48  
ジャスト イン タイム認証ポリシー  
ユーザーまたはグループに対する作成 48  
ユーザーまたはグループに対する無効化 48

シュレッド  
手動 43  
スケジュールの設定 40  
操作の手動開始 43  
フォルダーやファイルの保護  
41  
プロファイル 40  
右クリック 43  
詳細設定 49

## す

スマート カード、PIN 6

## せ

### 制限

機密データへのアクセス 5  
デバイス アクセス 45

### セキュリティ 6

主な目的 4  
機能 27  
役割 6

### 設定 55

Bluetooth デバイス 16  
HP SpareKey 15  
Password Manager 25  
PIN 18  
アイコン 23  
近接型、非接触型、およびスマート  
カード 17  
シュレッド スケジュール 40  
ブリーチ スケジュール 41

## そ

ソフトウェアによる暗号化 31,  
32, 34

## て

ディスクの管理 34

### データ

アクセス制限 5  
バックアップおよび復元 28

デバイス アクセスの制御 45

デバイス クラス

管理されない 49

## と

### 盗難

対策 5  
取り戻す 57

登録、指紋 13  
特別なキーの扱い 59  
トラスト サークルの削除 55

## は

ハードウェアによる暗号化 31,  
32  
ハードドライブの暗号化 33  
ハードドライブ パーティション  
暗号化 34  
暗号化の解除 34

### パスワード

HP Client Security 6  
安全な 7  
ガイドライン 7  
管理 6  
強度 23  
拒否された場合 58  
復元 14  
ポリシー 5  
例外事項 58

### バックアップ

HP Client Security 証明情報  
7  
暗号化キー 34  
データ 28

バックアップ キーを使用したアク  
セスの復元 35

## ひ

表示、ログ ファイル 44

## ふ

### ファイル

トラスト サークルからの削  
除 54  
トラスト サークルへの追加  
53

### フォルダー

トラスト サークルからの削  
除 54

### フォルダー

トラスト サークルへの追加  
52

### 復元

HP Client Security 証明情報  
7  
データ 28

不正アクセス、防止 5

## ブリーチ

開始 43  
手動 43  
スケジュール 41

## ほ

### ポリシー

管理者 25  
標準ユーザー 26

## み

右クリック シュレッド 43

## め

### メンバー

トラスト サークルからの削  
除 54  
トラスト サークルへの追加  
53

## も

目的、セキュリティ 4

## ゆ

### 有効化

自己暗号化ドライブに対する  
Drive Encryption 31  
標準ハードドライブに対する  
Drive Encryption 31

[ユーザー]ビュー 46

## ろ

### ログオン

インポートおよびエクスポー  
ト 24  
カテゴリ 22  
管理 22  
資格情報の追加 20  
編集 21

ログ ファイル、表示 44