

HP Client Security Gen3 ご紹介資料

株式会社 日本HP
2017年2月



HPのセキュリティにおけるリーダーシップ



✓多層防御

OSの下位から上位レイヤまでを網羅した防御機能を提供

✓追加費用不要

プリインストールもしくは無償ダウンロードにて提供

✓管理可能なセキュリティ

セキュリティポリシーをリモートから徹底

これらを

世界で最初のイノベーションと共に提供

自己回復型BIOS、内蔵プライバシースクリーン、モバイルデバイスによる自動ログインなど業界初のセキュリティ機能



HPのセキュリティイノベーション



- HP Sure Start Gen3 : BIOSへの攻撃を検知し自動復旧、OS起動前の
- **HP Client Security Suite** : デバイスアクセス制限、Windowsパスワード復元、パスワード管理を多要素認証で実現
- HP WorkWise : スマートフォンの距離情報に基づくログイン、PCの異常(不正アクセス、温度の上昇、バッテリー残量低下)をスマートフォンに通知
- HP Sure View : 公共の場におけるビジュアルハッキングから保護、内蔵プライバシースクリーン
- HP Manageability Integration Kit : ユーザーもしくはマルウェアによりセキュリティ機能をOffにさせない、リモートからの資産管理
- HP Sure Click : マルウェアやウイルスに感染したWebサイトからPCを守る、ハードウェアベースのブラウジングセキュリティ

世界で最も安全で、管理性に優れたビジネスPC¹



HP Client Security Gen3

手間をかけずにセキュリティを向上

The screenshot displays the HP Client Security Gen3 interface. At the top, there is a blue header with the HP logo and the text 'HP Client Security'. Below the header, the main content area is titled 'ユーザー認証情報、デバイス、およびデータの保護' (User authentication information, device, and data protection). This area is divided into two sections: 'ユーザー認証情報のセキュリティ' (User authentication information security) and 'デバイス セキュリティ' (Device security). The 'ユーザー認証情報のセキュリティ' section includes icons for 'HP Password Manager', '指紋' (Fingerprint), 'カード' (Card), 'HP SpareKey', and 'PIN'. The 'デバイス セキュリティ' section includes an icon for 'Bluetooth' and '仮想カード' (Virtual card). Below this, there is a section for 'デバイス 権限' (Device permissions) with a gear icon.

デバイスへの不正アクセスや、権限のないユーザーによるデータの持ち出しを防止します。

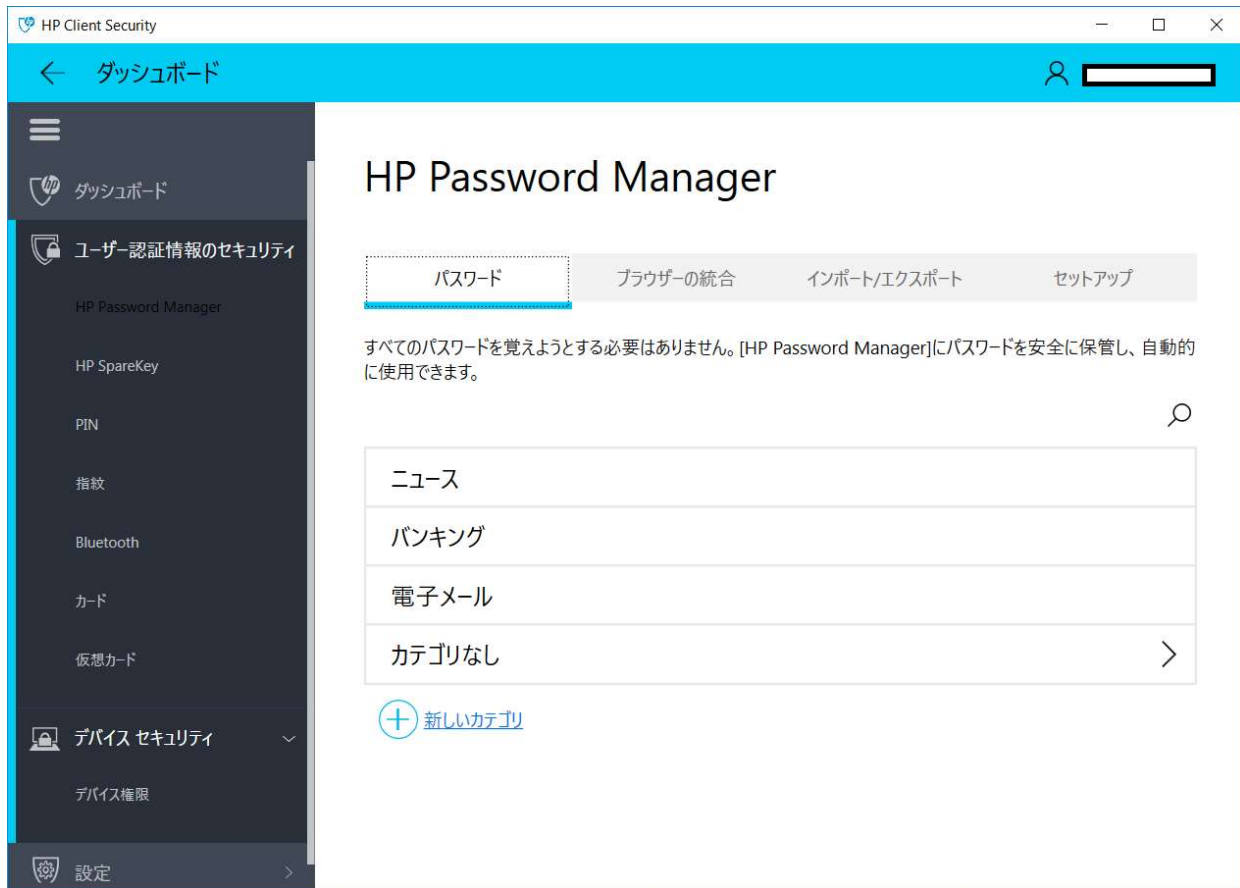
機能

- **HP Password Manager:** システムやWebサイトでのログオン情報をセキュアに管理、入力をサポートする機能
- **HPマルチファクタ認証:** 7つの認証要素から同時に2つの要素で認証する事でユーザーの本人確認を強化
- **HP SpareKey:** パスワードの自己復旧機能
- **HP Device Access Manger:** USB、プリンタ、CD/DVD、SD Microなどのリムーバブルメディアを介したデータの持ち出し防止機能・ジャストインタイム認証、およびポリシーによるポート制御が可能。

メリット

- **ITコストの削減:** 追加のセキュリティソフトウェア購入にかかるコストを削減。HP SpareKeyではサポートへの問い合わせと復旧にかかるダウンタイムを最小化することが可能。
- **セキュリティのカスタマイズ:** ポリシーに合わせてセキュリティレベルをカスタマイズ可能。また、Microsoft SCCMなどによりセキュリティ設定を配布し、徹底することが可能。

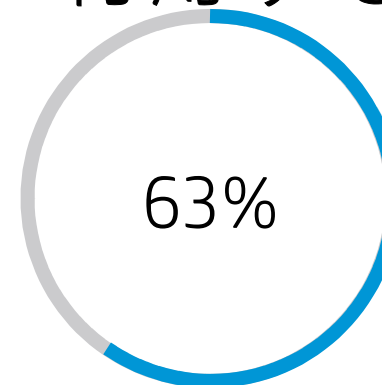
HPパスワードマネージャー



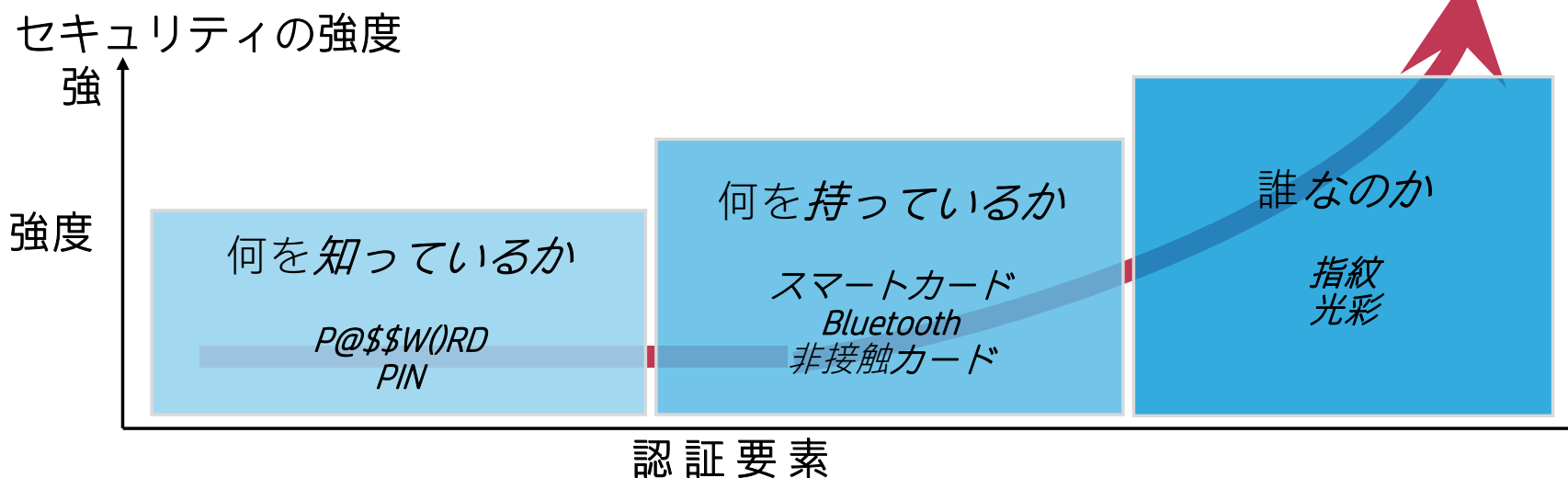
ウェブサイトやアプリケーションのIDとパスワードをセキュアに管理し、HP Client SecurityのパスワードのみでIDとパスワードの入力をサポートします。

WINDOWS 10をさらにセキュアに利用する

- ✓ **パスワード単独**では今日の脅威が必要とするセキュリティのレベルを提供することはできない
- ✓ ユーザーはパスワード確認の手間を省くために**ショートカット**を用いることが多い



パスワードの弱さによる
サイバー攻撃発生



マルチファクタ認証(多要素認証)の設定



7つの認証要素から1つないしは、2つの要素で認証する事でユーザーの本人確認を強化します。

認証の要素

- Windowsパスワード
- パスワード
- PIN
- 指紋
- スマートカード
- Bluetooth
- 非接触カード

HP SpareKeyの設定

パスワードを忘れてしまった際に事前登録した最大3つの質問に回答することで本人確認をしてPCへのログオンを許可します。

HP Device Access Managerの設定



PCに内蔵の各種ポートまたは接続された周辺機器に対して、どのユーザーがどのようなアクセス権限を持つかを定義します。

設定可能なデバイス

- 取り外し可能な記憶メディア
- 光学ドライブ
- Bluetoothデバイス
- IEEE 1394インターフェース
- COM/LPTポート
- 追加デバイス(生体認証デバイス、ネットワークアダプターなど)

設定可能なアクセス権

- フルアクセス
- 読み込みのみ
- ジャストインタイム認証で許可されたアクセスのみポリシーに基づきアクセス可能

ワンステップログオン・電源投入時認証



電源投入時の1回の認証でWindowsにログオンすることでセキュリティを保ちながら、利便性を向上します。

- Windowsログオンのセキュリティ
OSログオンの際のパスワード要求の設定
- 電源投入時認証
Windows起動前の認証の設定により、安全にOSを起動
- ワンストップログオン
「電源投入時認証」とこの機能を有効にすることで電源投入時認証の承認により、Windowsパスワード入力不要でOSへのログオン

Disclaimers & endnotes

1. HP独自の追加費用不要で包括的なセキュリティ機能とHP Managability Integration kitによる資産管理、MicrosoftのSCCMと連携したBIOS/ソフトウェアの管理を指し、2016年11月時点で年間100万台以上販売しているベンダーのモデルと、HP Elite製品のIntel第7世代プロセッサを搭載しているIntelアーキテクチャーモデルとの比較。