セキュリティＵＳＢフラッシュメモリ

PicoDrive Secure

ピコドライブ・セキュア

GH-UFD*SRM シリーズ 取扱説明書 Ver.1.0　管理ツール対応

はじめに

この度は本製品をお買い上げいただき、誠にありがとうございます。本製品を正しくご利用いただく為、本取扱説明書をよくお読みください。

安全に正しくお使いいただくために

⚠警告 下記事項を守らないと、死亡したり、重症を負うおそれがあります。

- ●発煙、発熱、異臭、異音が発生したら、すぐにパソコンなどの電源を切り、パソコンなどから取り外してください。
- ●ふんだり、のったり、投げたり、落としたりしないでください。
- ●落雷のおそれがある場合、触れないでください。
- ●異物や液体を付着させないでください。
- ●高温多湿や直射日光を避けてください。
- ●分解や改造をしないでください。
- ●子供や乳幼児の手の届くところで使用しないでください。
- ●パソコンなどへは、しっかり差し込んでください。

⚠注意 下記事項を守らないと、ケガをしたり、ものに損害を与えるおそれがあります。

- ●水分や静電気を帯びた手で触れないでください。
- ●使用しないときは、パソコンなどから抜いて保管してください。
- ●保管するときは、静電気や電磁波の発生するところを避けてください。
- ●データ転送中は、パソコンなどから取り外さないでください。

❗データについて

- ●誤操作や製品の故障によって消失する可能性があります。
- ●磁気や電磁妨害によって消失する可能性があります。
- ●温度や湿度、日射の影響によって消失する可能性があります。
- ●大切なデータは、他の記憶媒体へのバックアップをお勧めします。
- ●データが消失した場合、弊社は一切の責任を負いかねますので、あらかじめご了承ください。

■制限事項

- ●対応 OS 以外での動作は保証いたしかねます。
- ●他の USB 機器との同時使用についての動作は保証いたしかねます。
- ●省電力モード時での動作は保証いたしかねます。
- ●接続機器の制限により転送速度が USB1.1 規格値になる場合があります
- ●本製品を接続時の機器の起動や終了についての動作は保証いたしかねます。
- ●「Windows Ready Boost」には対応していません。

同梱物

- □PicoDrive Secure 本体
- □GH-UFD*SRM 取扱説明書 (本書)
- □1 年間保証書

本製品について

各部名称

■USBポートに接続すると、アクセスランプは「点滅」状態となり、パソコンで認識が完了すると「消灯」状態になります。

※データの読み書き時は「点滅」状態です。

⚠注意

アクセスランプ点滅中は絶対に本製品を USB ポートから抜かないでください。保存データが破損するおそれがあります。

特長と機能

●管理ツールに対応

管理ツール「GH-MNG-VS」(別売り) を使用することで、管理者がセキュリティポリシーの設定をすることができます。

●ハードウェアレベルでのデータ暗号化を実現。専用ソフトのインストール不要

コントローラにデータ暗号化エンジンを搭載しているので、専用ソフトのインストールなしで、すべて信頼性の高い AES256bit で暗号化されます。AES256bit で暗号化された保存データはハードウェアレベルで暗号化されますので、たとえ本製品を分解して別基板に組み込んだとしても、データを参照することはできません。

●紛失による情報漏洩からデータを護る、パスワードロック機能付き

紛失しても安心のパスワードロック機能が付いているので、万一、製品を紛失してしまっても中身を第三者に見られることはありません。AES256bit での暗号化と組み合わせて、強固なセキュリティを実現します。

●Autorun.inf ファイルチェック機能搭載

USB フラッシュメモリを介して感染する「Autorun ウイルス」をチェックする機能が搭載されています。「Autorun.inf」ファイルの内容をチェックし、不正な書き換えの可能性がある場合は、警告を表示して、「Autorun.inf」ファイルの削除や名前の変更ができます。

●リードオンリー (読み取り専用) 機能搭載

USB フラッシュメモリ内のデータを参照するだけなら、リードオンリー (読み取り専用) で開くことでウイルスの侵入を防ぐことができます。

●デバイス初期化機能搭載

設定したパスワードを忘れてしまった場合に、USBフラッシュメモリを初期状態に戻すことができ、再度ご利用することができます。※内部のデータは削除されます。

●ファイル・フォルダ暗号化

ファイル・フォルダの暗号化・復号化、および自己復号化形式の暗号化ファイルを作成することができます。簡単な操作により暗号化・復号化を行うことができ、機密情報流出防止に役立てることができます。

●ファイル完全削除

信頼性の高いファイル削除機能を簡単な操作により行うことができます。WindowsOS では、保存されているファイルを「データ管理情報」と「データ本体」に分けて保存しているため削除やフォーマットではデータを完全に消去することはできません。重要な社内機密や個人情報ファイルを完全に消去して、データ復元ソフトや残留磁気の解析でのデータ復元を不可能にします。

●パソコンロック

パソコンのロックキーとして使用することができます。本製品が接続されていない場合、自動的にログアウトし、パソコンをロックします。

●ユーザー権限動作対応

ソフトウェアのインストールなしで、管理者権限だけではなくユーザー権限でも使用できます。

●メモリの後ろに取り付けられる、紛失防止キャップ採用

●鉛等の含有量を抑えた環境にやさしい、RoHS 指令対応

「マイコンピュータ」上での認識

本製品 は、下図のように、PicoDrive Secure のプログラムの入ったプログラム領域とデータの読み書きができるデータ保存領域の、2 つの領域がマイコンピュータに認識されます。

●PicoDrive Secure のプログラムの入ったプログラム領域

※データの読み書きはできません。

●データの読み書きができるデータ保存領域

※ログイン後、データの読み書きができます。

※ドライブ名は、「SECURE」もしくは、「リムーバブルディスク」と表示されます。

※Windows 7 では、ログイン前は「PicoSRM」ドライブのみ表示されます。

※ご使用環境によっては、PicoDrive Secure のアイコン表示が異なる場合があります。

対応 OS

Windows 7 / Vista / XP (SP2 以降 /32bit)

※以降の内容は、初期設定に基づいた説明です。管理ツールにより本製品の設定が変更されている場合は、本書の内容と異なる動作になることがあります。設定内容については、管理者にお問い合わせください。

初めてお使いになる場合

パスワードとヒントの設定

本製品をご使用いただく為には、本製品をパソコンの USB ポートに接続し、最初に表示されるパスワードの登録画面でパスワードの設定をします。

※パスワードの登録画面が表示されない場合は、トラブルシューティングをお読みください。

①新しいパスワードの入力

ログイン時のパスワードを入力します。

※半角英数記号で4～16文字の範囲で入力してください。

※大文字と小文字は区別されます。

②パスワードの確認入力 (確認)

新しいパスワードと同じ文字を入力します。

③ヒントの入力

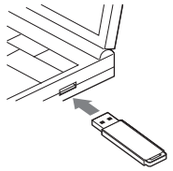
ログイン時に表示されるヒントを入力します。

※入力しなくともご使用いただけます。

※パスワードと同じヒントは登録できません。

PicoDrive Secure の基本的な使い方

1. パソコンに接続する



●本製品をパソコンの USB ポートに接続します。

※本製品のアクセスランプが点滅しているときは、本製品を抜かないでください。

※USBメモリを接続したときに、再起動要求がでることがありますが、再起動は必要ありません。

2.「ログインメニュー」の起動

●本製品をパソコンに接続するとログインメニュー画面が表示されます。

※ログインメニュー画面が表示されないときは、マイコンピュータ上の「PicoDriveSecure」ドライブをダブルクリックするか、「タスクトレイメニュー」から「ログインメニュー」を選択してください。

※「ログインメニュー」の選択方法は「タスクトレイメニュー」をお読みください。それでもログインメニュー画面が表示されない場合は、トラブルシューティングをお読みください。

3. ログイン

●ログインメニュー画面で「ログイン」ボタンをクリックするとログイン画面が表示されます。

ここで、最初に設定したログインパスワードを入力し「OK」ボタンをクリックます。

※「ヒントを表示」にマウスのポインタをあわせると、ヒントが表示されます。

※連続で 10回間違ったパスワードを入力するとログインできなくなります。この場合は初期化をしてください。

4.Autorun.inf チェックを使用しないでログイン

●Autorun.inf チェック機能を使用せずに本製品をご使用の場合は、ログインメニュー画面で「Autorun.inf チェックを使用しない」にチェックをいれてログインします。

5. 読み取り専用で開く

●読み取り専用で本製品をご使用の場合には、ログインメニュー画面で「読み取り専用モードで開く」にチェックをいれてログインします。

※読み取り専用モードは、「Autorun.inf チェックを使用しない」のチェックが入っていないと選択できません。

6. パスワードの変更

●パスワードを変更するときは、ログインメニュー画面から「パスワードの変更」ボタンをクリックし、パスワードの変更画面を表示します。

ここで、現在のパスワード、新しいパスワード (パスワードの確認入力を含む)、ヒントを入力し「OK」ボタンをクリックします。

7. オプション

●メニュー画面から「オプション」ボタンをクリックすると、オプション画面が表示されます。オプション画面では、USB メモリの初期化、プログラムのアップデート、リモートロック解除ができます。

7－1．初期化

●パスワードを忘れてしまったときや、USB メモリを初期化したいときは、オプション画面から「USBメモリの初期化」タブを選択して、「初期化実行」ボタンをクリックします。初期化を実行しない場合は、「戻る」ボタンをクリックし、メニュー画面に戻ります。

※初期化を実行すると、本製品内の保存データとログインパスワードが消去されます。よくご確認の上、実行してください。

7－2．アップデートの確認

●PicoDrive Secure プログラムのアップデートの確認と更新をするには、オプション画面から「アップデートの確認」タブを選択して、「アップデートの確認」ボタンをクリックします。アップデートプログラムがある場合は、ダウンロードをしてインストールすることができます。

アップデートの確認を実行しない場合は、「戻る」ボタンをクリックし、メニュー画面に戻ります。

7－3．リモートロック解除

●パスワードを忘れてしまった場合に、管理者が発行した認証キーでログインできます。

詳しくは、管理者にお問い合わせください。

8. ログアウト

●ログアウトするときは、ログイン中にログインメニュー画面を表示します。

次に「ログアウト」ボタンをクリックします。

※ログインメニューは、「タスクトレイメニュー」から選択します。タスクトレイメニューの表示方法は、「タスクトレイメニュー」をお読みください。

※管理者権限以外ではログアウトできません。この場合は、次項「9. 取り出し」を実行して、一旦、USB メモリを取り外してください。

9. 取り外し

●本製品の取り外しには、タスクトレイメニューから取り外しをクリックします。

●「コンピュータから安全に取り外しができます」という表示を確認してから本製品を取り外してください。

※タスクトレイメニューの表示方法は、「タスクトレイメニューの表示方法」をお読みください。

タスクトレイメニュー

1. タスクトレイメニューの表示方法

●タスクトレイメニューを表示するには、タスクトレイにある、PicoDriveSecure のアイコンを右クリックします。

PicoDriveSecureのアイコン

2. ログインメニュー画面の表示

●「ログインメニュー」を選択すると、ログインメニュー画面が表示されます。ログインメニューについては「PicoDrive Secure の基本的な使い方」をお読みください。

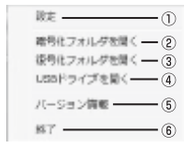
ファイル・フォルダ暗号化・復号化の操作方法

1. ファイル・フォルダ暗号化復号化ソフトウェアの起動方法

●「タスクトレイメニュー」から「ファイル･フォルダ暗号」を選択します。
起動すると、「ファイル･フォルダ暗号」ソフトウェアのアイコンがデスクトップ上に表示されます。
※タスクトレイメニューを表示方法は、「タスクトレイメニューの表示方法」をお読みください

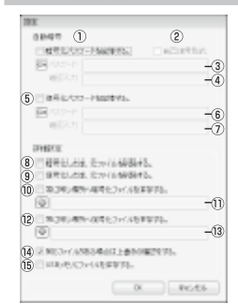
2. ファイル・フォルダ暗号メニュー

●「ファイル･フォルダ暗号」のアイコンを右クリックすると、ファイル･フォルダ暗号メニューが表示されます。



①各種設定画面を開きます。
②「設定」画面で暗号化フォルダを設定した場合、そのフォルダを開きます。
③「設定」画面で復号化フォルダを設定した場合、そのフォルダを開きます。
④PicoDrive Secureのデータ保存領域を開きます。
⑤「ファイル･フォルダ暗号」ソフトウェアのバージョン情報を表示します。
⑥ファイル･フォルダ暗号メニューを終了します。

3. 各種設定



●ファイル・フォルダ暗号メニューから設定を選択すると設定画面が開きます。
●設定完了後、「OK」ボタンをクリックすると、設定が有効になります。

[自動暗号]
暗号化・復号化のときに入力するパスワードの自動入力設定や、常に自己復号形式での暗号化をする設定をおこないます。
①暗号化パスワードを記憶する場合にチェックをいれます。
②常に自己復号形式で自動暗号化する場合にチェックをいれます。※①にチェックがある場合に選択できます。
③暗号化パスワードを入力します。※①にチェックがある場合のみ入力できます。
④暗号化パスワードを再入力します。※①にチェックがある場合のみ入力できます。
⑤復号化パスワードを記憶する場合にチェックをいれます。
⑥復号化パスワードを入力します。※⑤にチェックがある場合のみ入力できます。
⑦復号化パスワードを再入力します。※⑤にチェックがある場合のみ入力できます。

[詳細設定]
暗号化・復号化時の詳細な動作設定をおこないます。
⑧チェックを入れた場合、暗号化した後、元のファイルを削除します。
⑨チェックを入れた場合、復号化した後、元のファイルを削除します。
⑩チェックを入れた場合、常に⑪で指定したフォルダに暗号化ファイルを保存します。
⑪暗号化ファイルを保存するフォルダを指定します。※⑩にチェックがある場合に指定できます。
⑫チェックを入れた場合、常に⑬で指定したフォルダに復号化ファイルを保存します。
⑬復号化ファイルを保存するフォルダを指定します。※⑫にチェックがある場合に指定できます。
⑭暗号化・復号化後に同じファイルがある場合の上書き確認をする場合にチェックをいれます。
⑮PicoDrive Secureのデータ保存領域に保存する場合にチェックをいれます。

4. 暗号化・復号化の実行

1. デスクトップ上に表示されている、「ファイル･フォルダ暗号」アイコン(図①)に、暗号化･復号化をするファイルをドラッグ&ドロップします。
2. 暗号化するときは、図②の画面が表示されます。ここで、暗号化パスワード(確認パスワードを含む)を入力します。
※自己復号形式で暗号化ファイルを作成する場合は、自己復号形式オプション (図③) にチェックをいれます。
※自己復号形式で作成したファイルは、PicoDrive Secure なしで復号化できます。
3. 暗号化後、拡張子が sfb のファイルが、暗号化したファイルのあるフォルダ、または「3.各種設定」で指定したフォルダに作成されます。
4. 復号化するときは、図④の画面が表示されます。ここで、暗号化するときに設定した、暗号化パスワードを入力します。
5. 復号化されたファイルが、暗号化ファイルのあるフォルダ、または「3. 各種設定」で指定したフォルダに作成されます。

ファイル完全消去

1. ファイル完全消去の起動方法

●「タスクトレイメニュー」から「ファイル完全消去」を選択します。
起動すると、「ファイル完全消去」ソフトウェアのアイコンがデスクトップ上に表示されます。
※タスクトレイメニューの表示方法は、「タスクトレイメニューの表示方法」をお読みください。

2. ファイル完全消去メニュー

●「ファイル完全消去」のアイコンを右クリックすると、ファイル完全消去メニューが表示されます。

①Windowsのごみ箱の中身を完全消去します。
②ファイル完全消去の「設定」画面を開きます。
③「ファイル完全消去」ソフトウェアのバージョン情報を表示します。
④ファイル完全消去メニューを終了します。

3. 設定

●ファイル完全消去メニューから設定を選択すると、設定メニューが開きます。
●設定完了後、OK ボタンをクリックすると、設定が有効になります。

①ファイルの削除方式レベルを設定します。レベルが高いほど、セキュリティレベルが上がりますが、多くの処理時間を必要とします。
②ランダムデータの上書き回数を設定します。上書き回数が多いほど、セキュリティレベルは上がりますが、多くの処理時間を必要とします。
③削除ファイルの詳細を表示したい場合にチェックをいれます。
④削除の確認メッセージを表示しない場合にチェックをいれます。

4. ファイル完全消去の実行方法

●表示されている「ファイル完全消去」アイコンに、完全消去したいファイルまたはフォルダをドラッグ& ドロップします。
※消去したファイルは復元できませんので、よくご確認してから実行してください。

パソコンロック

1. パソコンロックの設定画面の表示方法

●「タスクトレイメニュー」から「パソコンロック」を選択します。
選択するとパソコンロックの設定画面が開きます。
※タスクトレイメニューを表示方法は、「タスクトレイメニューの表示方法」をお読み下さい。

2. 設定

①チェックを入れるとパソコンロックが有効になります。
②本製品を取り外した後、パソコンをロックするまでの時間を画面に表示する場合にチェックをいれます。
※①にチェックが入っていないときは、選択できません。
③テキストボックスの上下ボタンを使用して「パソコンがロックされるまでの時間」を3~30秒の間で設定します。
※①にチェックが入っていないときは、選択できません。

3. パソコンロックの起動方法

●設定メニューで「デバイスを取り外し後、パソコンをロックする。」にチェックを入れて「OK」ボタンをクリックします。
設定後、本製品を取り外すと自動ロックが実行されます。
※パソコンロックは、パソコンロックの設定をしたログインユーザーでのみ有効です。

4. パソコンロックの解除方法

●本製品をパソコンに接続後、Windowsにログインし、パソコンロックの設定で「デバイスを取り外し後、パソコンをロックする。」のチェックを外して「OK」ボタンをクリックします。
※本製品を失くした場合は、トラブルシューティングをお読みください。

トラブルシューティング

1. 初期化、ログイン等で、操作のやり直しを要求されたら

●OSの状態によって、稀に、初期化、ログイン等のときに、「USBを挿し直して再度初期化を実行してください」と表示されることがあります。このときは、一旦、USBメモリを取り外して、操作をやり直してください。

2. パスワード登録画面・メニュー画面が表示されない

●本製品をパソコンに接続しても画面が表示されない場合は、「PicoSRM」ドライブをダブルクリックしてください。表示されない場合は、「PicoSRM」ドライブを「右クリック」→「開く」→「StartupPD」アイコンをダブルクリックしてください。それでも表示されない場合は、一旦、USBメモリを取り外してやり直してください。

3. パソコンロック状態で、本製品を失くしたとき

●コンピュータ自動ロックの状態で、本製品を紛失した場合は、セーフモードで、Windowsを再起動し、スタートアップに登録されているSCKJAutoLockPCを削除してください。

4. 制限ユーザー環境でファイルの削除・保存ができない

●Windowsの仕様により制限ユーザー環境において、管理者権限が必要なフォルダ内ではファイルの削除・保存ができません。

仕様

型番	GH-UFD*SRM
容量	2GB ～ 16GB
重量	約 11g
外形寸法	W65 x D19 x H8 (mm)
USB 規格	USB 2.0/1.1
データ転送速度	最大 480Mbps(理論値)
電源	5 V ±10% (USB バスパワー)
消費電流	240mA(動作時最大)
電源管理	Windows スタンバイ・休止対応
使用温度範囲	0 ～ 60℃
使用湿度範囲	10 ～ 90%(結露なきこと)
保証期間	1 年間 (USB フラッシュメモリ本体)
その他	RoHS 指令準拠
対応機種	USB インターフェース搭載の DOS/V(OADG 仕様) パソコン、NEC PC98-NX シリーズ
対応 OS	Windows7 / Vista / XP(SP2 以降 / 32bit)

※管理ツール「GH-MNG-VS」は付属しておりませんので、別途ご用意ください。
※製品のデザイン、仕様は改良等により、予告なしに変更する場合があります。
※記載されている会社名、製品名は各社の登録商標または商標です。

テクニカルサポート情報

サポート窓口	グリーンハウス テクニカルサポート
テクニカルサポートダイヤル	03-5421-0580
受付時間	10 : 00 ～ 12 : 00 / 13 : 00 ～ 17 : 00 (土日祝日をのぞく弊社営業日)
FAX	03-5421-2266 (24 時間受付)
住所	〒150-0013 東京都渋谷区恵比寿 1-19-15 ウノサワ東急ビル 5 階
ホームページ	http://www.green-house.co.jp

・故障やご使用上のご質問は、テクニカルサポートダイヤルへお電話いただくか、弊社ホー ムページにあるサポート「各種お問い合わせ」やFAXでお問い合わせください。
・弊社ホームページにあるサポート「各種お問い合わせ」からお問い合わせの場合、ユーザー登録が必要になります。
・お問い合わせの前に、取扱説明書「トラブルシューティング」や弊社ホームページにあるサポート「よくあるご質問」をご活用ください。
・テクニカルサポートダイヤルの受付時間は、予告なしに変更する場合があります。