ウイルス対策 USB
型番：MF-PUVT3**GM*
Windows マニュアル

この度はセキュリティ USB (以下、本製品)をご購入いただき誠にありがとうございます。このマニュアルでは本製品の導入から使用方法までを説明しています。本製品を正しくご利用いただくために、使用開始前に必ずお読みください。
本マニュアルでは本製品を Windows で使用した場合の動作を記載しております。macOS で使用した場合のマニュアルは macOS で本製品を起動し、パスワード入力画面からメニューバーの[ヘルプ]をクリックし、[マニュアル]をクリックしてください。

1 ご使用になる前に

本製品は、トレンドマイクロ社のデバイス組み込み用ウイルス対策モジュール：Trend Micro USB Security 2.1 (TMUSB 2.1)が格納されたライセンス製品です。
本製品をご使用になる前に、本製品起動時に表示される使用許諾約款を必ずご確認、同意していただきますようにお願い申し上げます。
また TMUSB 2.1 の使用許諾契約に関しましては、別途 TMUSB 2.1 初回起動時に表示されますので、
必ずご確認、同意していただきますようにお願い申し上げます。

使用上の注意事項

本製品を正しくお使いいただくために、必ず下記に示す注意事項をお読みになり、内容をよく理解された上でお使いください。本製品を接続して使用する対象機器の故障、トラブルやデータの消失・破損、または誤った取り扱いのために生じた本製品の故障、トラブルは、保証対象外となりますので、あらかじめご了承ください。

警告表示の意味

⚠ 警告	この表示は、人が死亡または重傷を負う可能性が想定される内容を示しています。
⚠ 注意	この表示は、人が傷害を負う可能性が想定される内容や物的損害の発生が想定される内容を示しています

警告

・本製品を取り付けて使用する際は、取り付ける対象機器のメーカーが提示する警告、注意事項に従ってください。
・指定以外の電源電圧では使用しないでください。発火、火災、発熱、感電などの原因となります。
・本製品の分解や改造、修理等は絶対に行わないでください。火災、感電、故障の恐れがあります。
・濡れた手で本製品を使用しないでください。感電の恐れや故障の原因となります。
・小さなお子様や乳幼児の手の届くところに置かないでください。キャップ等を誤って飲み込むと窒息の恐れがあります。万一飲み込んだ時は、すぐに医師にご相談ください。
・本製品は水を使う場所や湿気の多い場所で使用しないでください。感電の恐れや、火災故障の原因となります。
・本製品や本製品を接続した機器に液体や異物が入った場合、または本製品や機器から煙が出たり、悪臭がした場合は、すぐに機器の電源を切り、電源ケーブルをコンセントから抜いてください。そのまま使用を続けると、感電の恐れや火災の原因となります。
・弊社は品質、信頼性の向上に努めておりますが、一般に半導体を使用した製品は誤作動したり故障したりする可能性があります。本製品を使用する場合は、事前に、本製品を使用する製品の誤作動や故障により、お客様または第三者の生命・身体・財産が侵害される可能性ことがないことを必ずご確認ください。

注意

・本製品に触れる前に、金属等に手を触れて身体の静電気を取り除いてください。静電気により破損、データ消失の恐れがあります。
・無理に曲げたり、落としたり、傷つけたり、上に重いものを乗せたりしないでください。故障の原因となります。
・本製品のコネクタに汚れ、ほこりなどが付着している場合、乾いたきれいな布で取り除いてください。汚れたまま使用すると故障の原因となります。
・本製品へのデータの書き込み・読み出し中に、本製品を機器から取り外したり、機器の電源を切ったりしないでください。データが破壊、または消去される可能性があり、本製品の故障の原因となります。
・本製品を取り付けて使用する際は、取り付ける対象機器のマニュアルの使用方法、注意事項に従ってください。
・本製品に保存するデータ、または保存されるデータは、必ずデータのバックアップを取ってください。本製品内に記録したプログラムやデータの消失、破損等の責任は負いかねますので予めご了承ください。
※弊社ではデータ復旧、回復作業は行っておりません。
・本製品はフラッシュメモリを使用している関係上寿命があります。長期間ご使用になると、データの書き込み・読み込みができなくなります。
・本製品は、お客様のシステムに組込むことを想定しておりません。組込む場合は、弊社は本製品に起因するか否かにかかわらず、一切の責任を負いません。
・弊社は、お客様が、日本国内において、本製品を使用する非独占的且つ移転不能な権利を認めます。本製品は、あくまで、お客様若しくはお客様が使用許諾約款に規定される監査を弊社に許可可能な国内関連会社での自己使用に限定されます。国内外を問わず、如何なる場合も、本製品の第三者へのレンタル、譲渡はできません。万一お客様が、本件製品を海外の関連会社で使用することを御希望のときは、事前に必ず弊社の書面による承諾を得てください。本製品を海外に輸出するときは、国内外の、関連するすべての輸出法規並びに手続きに完全に従ってください。
・本製品は、国内輸送を想定した梱包にてお届けしています。海外輸送される場合は、お客様にて海外輸送用に梱包いただきますようお願いします。
・TMUSB2.1 のウイルスパターンファイルは、お客様が本件製品をＰＣに装着して、トレンドマイクロ社のサーバからダウンロードすることで最新版に更新されます。
・TMUSB2.1 は、最新のウイルスパターンファイルに更新することで、トレンドマイクロ社が対応しているウイルスの検知が可能であり、すべてのウイルスを検知することを保証しているものではありません。なお、暗号化されているファイルやパスワード付きの圧縮ファイルなど、ウイルスを検出できない場合もあります。
・本製品に組み込まれた TMUSB2.1 は、発見したウイルスに感染したファイルを隔離するものです。お客様が本製品に格納していたファイルやアプリケーションプログラムが感染していた場合は、ファイルやプログラムのファイル自体を隔離しますので、重要なファイルは必ずバックアップを取っておいてください。

保管上のご注意

下記の場所では本製品を保管しないでください。製品に悪影響を及ぼしたり、感電、火災の原因になったりする場合があります。
- 直射日光があたるところ
- 水濡れの可能性のあるところ
- 暖房器具の周辺、火気のある周辺
- 高温（50℃以上）、多湿（85%以上）で結露を起こすようなところ、急激に温度の変化があるところ
- 平坦でないところ、土台が安定していないところ、振動の発生するところ
- 強い磁界や静電気の発生するところ
- ほこりの多いところ

製品保証規定

■保証内容

弊社が定める保証期間（本製品ご購入日から起算されます。）内に、適切な使用環境で発生した本製品の故障に限り、無償で本製品を修理または交換いたします。

■無償保証範囲

以下の場合には、保証対象外となります。

（1） 故障した本製品をご提出いただけない場合。
（2）ご購入日が確認できる証明書（レシート・納品書など）をご提示いただけない場合。
（3） (2)の証明書に偽造・改変などが認められた場合。
（4） 弊社および弊社が指定する機関以外の第三者ならびにお客様による改造、分解、修理により故障した場合。
（5） 弊社が定める機器以外に接続、または組み込んで使用し、故障または破損した場合。
（6） 通常一般家庭内で想定される使用環境の範囲を超える温度、湿度、振動等により故障した場合。
（7） 本製品を購入いただいた後の輸送中に発生した衝撃、落下等により故障した場合。
（8） 地震、火災、落雷、風水害、その他の天変地異、公害、異常電圧などの外的要因により故障した場合。
（9） その他、無償修理または交換が認められない事由が発見された場合。

■修理

修理のご依頼は、お買い上げの販売店もしくは弊社サポートセンターにお問い合わせください。

弊社サポートセンターへご送付いただく場合の送料はお客様のご負担となります。また、ご送付いただく際、適切な梱包の上、紛失防止のため受渡の確認できる手段（宅配や簡易書留など）をご利用ください。尚、弊社は運送中の製品の破損、紛失については一切の責任を負いません。

同機種での交換ができない場合は、保証対象製品と同等またはそれ以上の性能を有する他の製品と交換させていただく場合があります。

有償、無償にかかわらず修理により交換された旧部品または旧製品等は返却いたしかねます。

記憶メディア・ストレージ製品において、弊社サポートセンターにて製品交換を実施した際にはデータの保全は行わず、全て初期化いたします。記憶メディア・ストレージ製品を修理に出す前には、お客様ご自身でデータのバックアップを取っていただきますようお願い致します。

■免責事項

本製品の故障について、弊社に故意または重大な過失がある場合を除き、弊社の債務不履行および不法行為等の損害賠償責任は、本製品の購入代金を上限とさせていただきます。

本製品の故障に起因する派生的、付随的、間接的および精神的損害、逸失利益、ならびにデータ損害の補償等につきましては、弊社は一切責任を負いません。

■有効範囲

この製品保証規定は、日本国内においてのみ有効です。

補償の制限

如何なる場合であっても、弊社は、お客様に対して、本件製品に関連して生じた、利益の損失、使用の損失、データの損失、信用の損失、信頼の損失、ビジネスの中断若しくは他の一切の類似の損害を含む如何なる付随的な、間接的な、特別な、また派生的な損害、及び逸失利益の喪失に係る賠償の責任を負いません。

2 同梱品の確認

本製品のパッケージには、次のものが含まれます。はじめに、すべてのものが揃っているかご確認ください。
万一、不足品がありましたら、ご購入の販売店または弊社までお知らせください。

□ ウイルス対策 USB　MF-PUVT3**GM*（製品本体）　　×1 個

3 本製品について

本製品は、トレンドマイクロ社の TMUSB 2.1 及び弊社のアプリケーションプログラムを搭載し、ウイルスの検出及びウイルス感染したファイルを隔離する機能をもつ USB メモリです。

本製品は管理者用ソフトウェア「SecurityUSB Manager（型番：HUD-SUMA）」に対応しており、様々なポリシー変更、機能追加、管理を行うことができます。詳しくは SecurityUSB Manager マニュアルを確認ください。

本製品の特長

✓ *USB3.0 対応*

高速データ転送を実現する「USB3.0」に対応。
USB2.0/1.1 の環境でも使用することができます（転送速度は接続する USB ポートに依存します）。

✓ *管理者用ソフトウェア「SecurityUSB Manager」に対応*

SecurityUSB Manager に対応し、様々なポリシー設定、機能追加、管理を行うことができます。
詳しくは SecurityUSB Manager マニュアルを確認ください。

✓ *トレンドマイクロ社製 TMUSB 2.1 によるウイルス検索機能*

PC から本製品にファイルを書込む際にウイルス検出を実行します。
本製品を PC に接続するとタスクトレイにウイルス検索の状態を示すアイコンが表示されます。

✓ *パスワードロック機能*

本製品の紛失、盗難時の情報漏洩を防ぐためにパスワードによるロック（保護）機能を搭載しています。

✓ *ウイルスパターンファイルアップデート機能*

本製品に搭載されているウイルスパターンファイルは、インターネットに接続可能な PC に本製品を接続することでアップデートが可能です。
またウイルスバスターコーポレートエディション（ウイルスバスター Corp.）10.5/10.6 が保有するウイルスパターンファイルを使用し、アップデートすることが可能です。（ウイルスバスター Corp の設定が従来型スキャンになっている必要があります。）

✓ *ソフトウェアの自動アップデート機能*

インターネットに接続可能な PC に本製品を接続することで自動的にソフトウェアアップデートの有無を確認します。

✓ *リムーバブルディスク領域の書込み禁止機能*

リムーバブルディスク領域を書込み禁止に設定することができます。
保存したデータの改ざんや消去を防止するための機能です。

✓ *初期化・復旧機能*

本製品の初期化（パスワードの初期化）、リムーバブルディスク領域に保存してあるウイルス検索ソフトウェアを誤って消去した場合にウイルス検索ソフトウェアを復旧できる機能を有しています。

✓ *ハードウェア暗号化機能*

本製品はハードウェアによる自動暗号化機能を搭載しています。すべてのデータを強制的に暗号化してから書き込みますので、暗号化されていないデータが書き込まれることがなく、万一、紛失・盗難等があっても情報の流出を防ぐことができます。またデータの読み出しにおいても、自動的に復号化が行われるので、暗号化を意識することなく、直接本製品内のデータを読み書きすることができます。暗号化方式には、米国政府標準で日本政府も推奨している信頼性の高い「AES 方式(256bit)」を採用しています。

✓ *mac OS に対応*

macOS 上で本製品を使用することができます。macOS で使用するには SecurityUSB Manager で[macOS を使用する]へチェックを入れてください。

注意：macOS では Windows 上で動作する以下の機能がございません。

- ソフトウェアの自動アップデート機能
- ログ保存、出力、閲覧機能
- Autorun.inf 自動削除機能
- ウイルススキャン機能、ウイルス定義ファイル アップデート機能
- オプション設定
- SecurityUSB Manager の一部機能

製品仕様

USB インターフェース	USB 2.0（High Speed/Full Speed）/ USB3.0(Super Speed)
動作環境（*1*2*3*4*6）	USB インターフェースを標準搭載した DOS/V 機器 空きメモリ容量 600MB 以上(推奨 1GB 以上) CD-ROM ドライブが認識されること CD-ROM ドライブによるオートラン実行がされること USB マスストレージドライバがあること USB HID ドライバがあること インターネット環境に接続できること*8
対応 OS *5*9	Windows10 Windows11 Windows Server 2012/2012R2 *7*10 Windows Server 2016 *7*10 Windows Server 2019 *7*10 Windows Server 2022 *7*10 Windows Server 2025 *7*10 macOS 10.8.5 - 10.15 macOS 11,12,13,14,15 ※Windows：日本語 OS 以外では英語表示されます。 コピーガード機能の対応 OS は、上記と異なりますので、詳しくは SecurityUSB Manager のマニュアルを参照してください。 ※macOS：英語環境では英語で表示されます。日本語、英語環境以外では動作しません。 ソフトウェアの自動アップデート機能、ログ関連機能、Autorun.inf 自動削除機能、オプション設定、コピーガード機能を含む SecurityUSB Manager の一部機能が動作しません。
対応ユーザアカウント	コンピュータの管理者（Administrator） 制限ユーザ
外形寸法	全長 60.0mm×幅 20.8mm×高さ 7.8mm　（USB コネクタ収納時）
ハードウェア暗号化方式	AES 256bit
対応管理者用ソフトウェア	SecurityUSB Manager（型番： HUD-PUMMA）

*1　拡張ボードで増設した USB インターフェースには対応していません。
*2　USB Mass Storage Class ドライバ、HID Class ドライバ、CD-ROM ドライバがあらかじめ組み込まれている必要があります。
*3　オートランによるアプリケーション起動を行うには、OS 側でオートラン実行が有効となっている必要があります。
*4　Proxy サーバを経由してネットワークに接続する際にユーザ認証が必要になる場合は、モニタ及びキーボードが必要です。
*5　64bit OS の対応について
本製品のソフトウェアは 32bit アプリケーションです。
64bitOS 上では「WOW64」機能を使用し、32bit 互換モードで動作します。
64bitOS で 32bit アプリを動作させても自動的に「WOW64」機能を使用するため 、特別な作業は必要ありません。
※WOW64 を無効にしている 64bitOS では、本製品のソフトウェアは動作しません。

*6　下記のコンポーネントが必ず組み込まれている必要があります。
・Basic TCP/IP Networking
*7　対象 OS の制限ユーザ下では本製品は動作しません。
*8　ウイルス定義ファイルの更新、ソフトウェア更新の場合に必要となります。
proxy サーバを経由した環境でもウイルス定義ファイルのダウンロードが可能です。
ユーザ名/パスワード/プロキシサーバ/ポート番号
を入力するとインターネットへの接続が可能になります。
ユーザ名、パスワード、プロキシサーバ、ポート番号はネットワーク管理者にお問い合わせください。

*9　macOS は Intel CPU、Apple シリコン上での動作に限ります。

*10 コピーガードが有効な場合、本製品は動作しません。

NOTE	本製品にはソフトウェアがプレインストールされていますので、OS 上で表示されるリムーバブルディスク領域のメモリ容量は、製品ならびに製品パッケージに記載のメモリ容量より少なくなります。

4 セットアップから運用開始までの流れ

＜SecurityUSB Manager でポリシー設定を行う場合＞

［管理者］ SecurityUSB Manager によるポリシー設定	本製品をユーザに配布、展開される前に、SecurityUSB Manager を使用して本製品へ設定を書き込んでください。

▼

＜セットアップ＞

パスワードの登録	本製品をインターネットに接続されている PC に接続します。 自動実行でパスワードを登録する初期化設定画面が表示されます。 画面の指示に従いパスワードを入力して[登録]をクリックします。 登録後、パスワード入力画面に切り替わりますので、登録したパスワードを再度入力するとリムーバブルディスク領域にアクセスすることができます。

＜製品のご使用＞

PC に接続してパスワードを解除	本製品をインターネットに接続されている PC に接続します。 自動実行でパスワード入力画面が表示されますので、パスワードを入力してパスワードを解除してください。 パスワードを解除すると TMUSB 2.1 が自動実行し、本製品のリムーバブルディスク領域に対してウイルスの監視を開始します

▼

本製品にデータを書込む/読み込む	リムーバブルディスク領域に保存するデータをコピーまたは移動します。 このときコピーまたは移動したファイルにウイルス感染が見つかると、そのファイルを本製品内に隔離します。

▼

本製品を取り外す	本製品を取り外す場合タスクトレイまたは通知領域の PL モニタリングソフトウェアにある「デバイス取り外し機能」を使用する、または「ハードウェアの安全な取り外し」アイコンをクリックし、メッセージのポップアップが表示されたら、本製品のドライブ名を確認してクリックして取り外します。 ※「PL モニタリング ソフトウェア」については「PL モニタリングソフトウェア機能」の項をご確認ください。

NOTE	パスワード登録画面/パスワード入力画面が自動実行で表示されない場合は、下記の手順を実施してください。 ・マイコンピュータ上の「SecurityUSB」アイコンを右クリックして[開く]をクリックします。 開いたフォルダ内にある[Startup.exe]ファイルをダブルクリックするとパスワード登録画面/パスワード入力画面が表示されます。 ・マイコンピュータ上の「SecurityUSB」アイコンを右クリックし、[メディアからのプログラムのインストール/実行]をクリックします

NOTE	本製品にはソフトウェアがプレインストールされていますので、OS 上で表示されるリムーバブルディスク領域のメモリ容量は、製品ならびに製品パッケージに記載のメモリ容量より少なくなります。

5 ご使用方法

本章では、本製品の使用方法などを説明しております。ご使用前に「使用上の注意事項」、「ご使用にあたって」などを必ずお読みください。本マニュアルは標準設定に基づき作成しております。SecurityUSB Manager の設定によっては本マニュアル記載の動作と異なる箇所があることをご了承ください。

ご使用にあたって

- 本製品を接続した状態で PC を起動した場合、前回異常終了がなくてもスキャンディスクが自動的に行われる場合があります。
- 本製品を接続した状態で PC を起動した場合、これまでに接続したことのあるデバイスであっても新たにデバイスを認識する表示が出ることがあります。
- 本製品を接続してから認識されるまでに 5 分ほど時間がかかる場合があります。PC の再操作が可能になるまでお待ち
  ください。
- 本製品は著作権保護機能には対応しておりません。
- PC の電源が入った状態で、本製品を PC から取り外す際には、タスクトレイ（通知領域）上のウイルススキャンの状態を示すアイコンを右クリックして「終了（取り外し）」を選択、もしくは「ハードウェアの安全な取り外し」を行ってください。無理に取り外しますと、ファイルが消失したり、故障の原因になります。
- 消失・破損したデータに関しては、当社は一切の責任を負いません。
- 本製品は、正しい向きでまっすぐ抜き差ししてください。
- 本製品はスタンバイや休止状態、スリープ状態には対応しておりません。
- 本製品を湿気やホコリの多いところで使用しないでください。
- 本製品に強い衝撃を与えないでください。
- 本製品をお手入れの際には乾いたやわらかい布で軽く拭いてください。ベンジン、シンナー、アルコールなどは使用しないでください。
- 本製品を同時に複数台使用することはできません。

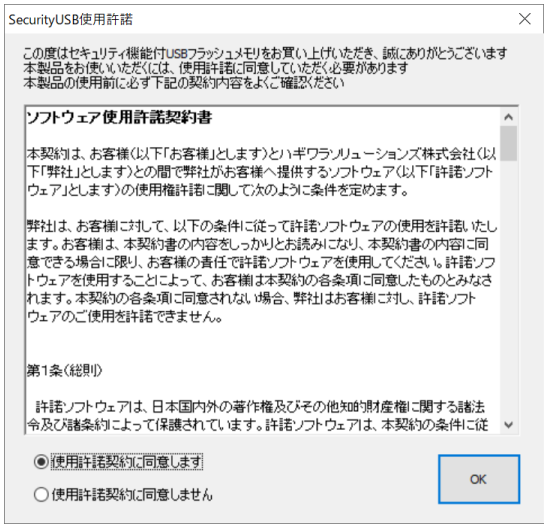
使用許諾約款の同意

本製品を PC の USB ポートに接続するとマイコンピュータ上に「SecurityUSB」と「リムーバブルディスク」のアイコンが表示されます。

※ご使用の PC によって、アイコン、ドライブ名、表示順が異なる場合があります。

「SecurityUSB」のアイコンをダブルクリック、もしくは「SecurityUSB」アイコンを右クリックして[開く]をクリックし、開いたフォルダ内にある「Startup.exe」ファイルをダブルクリックします。

初回起動時は使用許諾が表示されますので、ご確認いただき、問題がなければ、[…同意します]を選択し、[OK]ボタンを押してください。

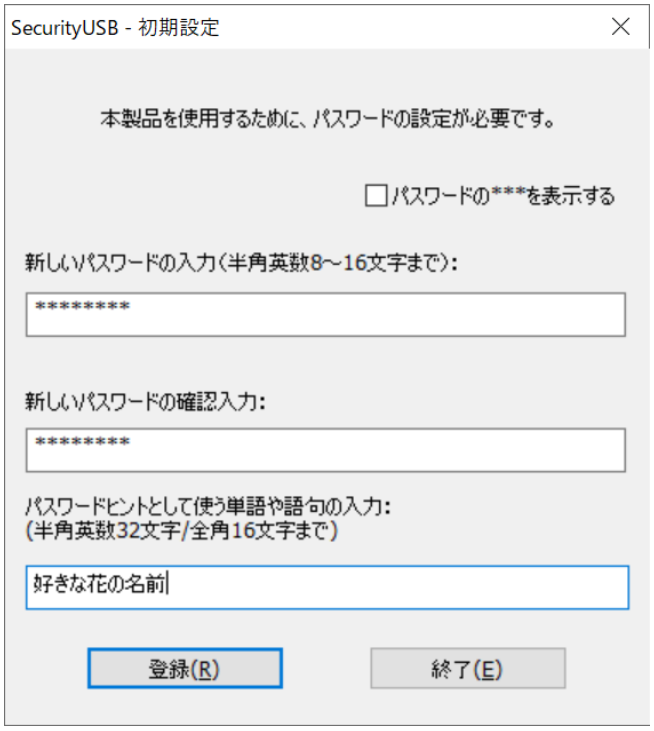


NOTE	使用許諾約款の画面が表示されない場合は、マイコンピュータ上の「SecurityUSB」アイコンを右クリックして[開く]をクリックします。開いたフォルダ内にある「Startup.exe」ファイルをダブルクリックします。 もしくは、マイコンピュータ上の「SecurityUSB」アイコンを右クリックし、[メディアからのプログラムの インストール/実行]をクリックします。

NOTE	• USB ハブやキーボードの USB ポートには接続しないでください。正常に動作しないことがあります。 • Windows 7 以降の場合、「パスワードロックの解除」を実行しないと、リムーバブルディスクのアイコンは表示されません。 • パスワードロック解除前のリムーバブルディスクドライブをクリックした場合、[ディスク挿入]画面が表示されます。 • 再起動メッセージが表示される事がありますが、再起動する必要はありません。 表示された場合は、再起動メッセージの[いいえ]をクリックしてください。

パスワードの初期設定

本製品をご利用になるには必ずパスワードの設定が必要です。



1. パスワードを入力します。
   パスワードは 8~16 文字までの半角英数字と以下の半角記号が使用できます。
   ! # $ % & ' ( ) = ~ | ` { + * } < > ? _ - ^ ¥ @ [; :] , . /
2. パスワードのヒントを入力後、[登録]をクリックします。

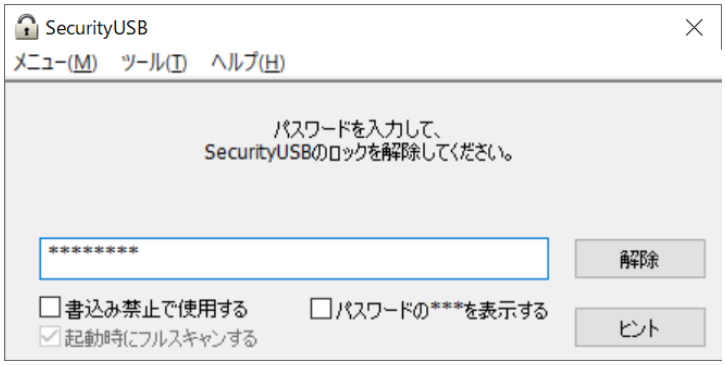
※パスワードヒントを設定しなくてもパスワードの設定は
可能です。パスワードヒントの登録は任意です。

※[パスワードの***を表示する]にチェックを入れた場合、
入力したパスワードを見ることができます。

NOTE	• パスワードを設定しないと本製品のリムーバブルディスク領域は使用できません。 • 解除される恐れのあるような簡単なパスワードを設定しないように注意してください。

パスワードロックの解除

パスワードの初期設定が完了すると続いてパスワードの入力画面が表示されます。
登録したパスワードを入力し、[解除]をクリックします。
パスワードロック解除後、本製品のメモリにアクセスすることができます。またウイルススキャンプログラムが起動し、ウイルス監視を開始します。



※パスワードの初期設定が完了すると、2 回目以降は本製品を PC に接続すると、右図のパスワードの入力画面を表示します。
※[パスワードの＊＊＊を表示する]にチェックを入れた場合、入力したパスワードを見ることができます。

NOTE	[解除]をクリックしてパスワードロックを解除すると、本製品を PC から取りはずすまでは、本製品のリムーバブルディスク領域にデータの読み書きができる状態です。本製品をいったん PC から取り外し、再度 PC に接続したときはパスワードロックのかかった状態になるので PC から取り外すときにパスワードロックを かけ直す必要はありません。

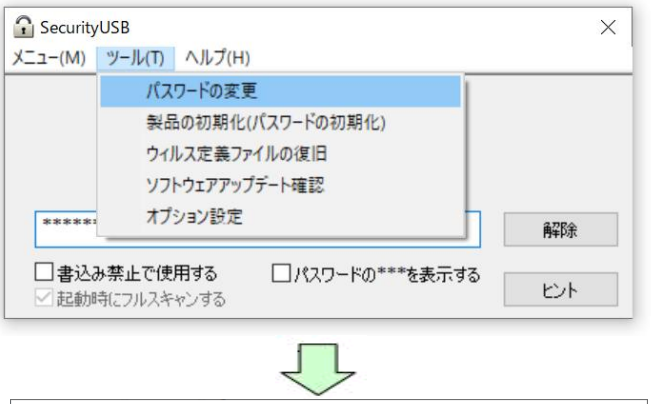
NOTE	本製品にはソフトウェアがプレインストールされていますので、OS 上で表示されるリムーバブルディスク領域のメモリ容量は、製品ならびに製品パッケージに記載のメモリ容量より少なくなります。

ご注意!	パスワードの紛失やパスワードの入力をセキュリティ解除できないまま 5 回以上間違えた場合、パスワード解除ができなくなり、本製品のメモリへアクセスできなくなります。 「本製品の初期化（パスワードの初期化）」を行うと、メモリへ保存したファイル、登録したパスワード、パスワードヒント等すべて削除されますので十分ご注意ください。 パスワードを 5 回以上間違えたことにより、メモリにアクセスできない事態に対して弊社は一切の責任を負いません。また、弊社では本製品のメモリからファイル救出をお受けできませんので、ご了承ください。

パスワードの変更

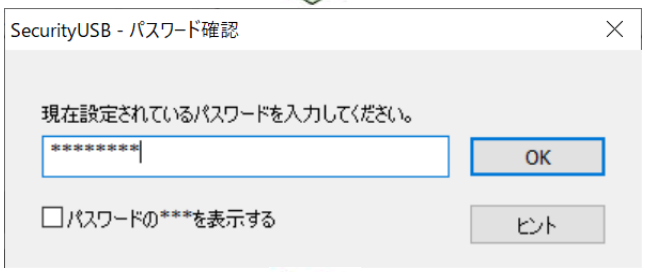
設定済のパスワードを別のパスワードに変更することができます。

パスワード入力画面から「ツール」をクリックし「パスワードの変更」をクリックします。



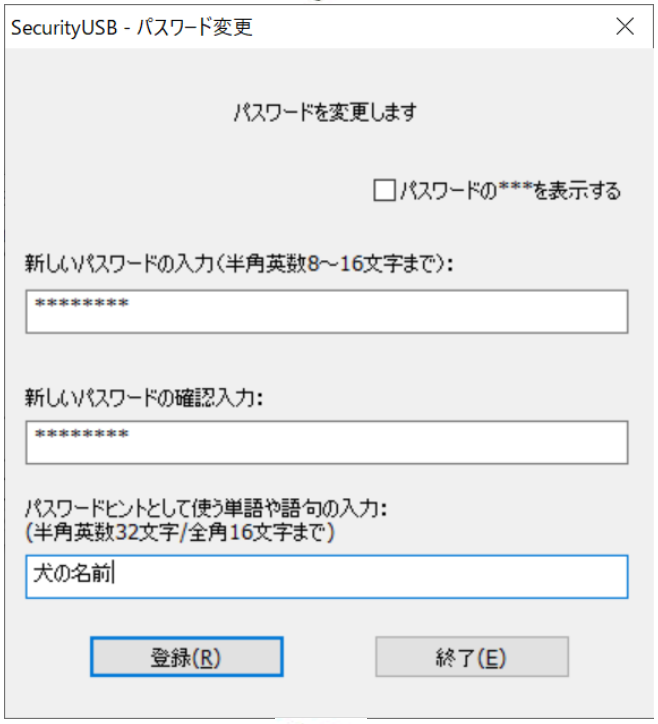
現在設定しているパスワードを入力します。

※5 回以上違えた場合、本製品のメモリへアクセスできなくなります。
※[パスワードの＊＊＊を表示する]にチェックを入れた場合、入力したパスワードを見ることができます。

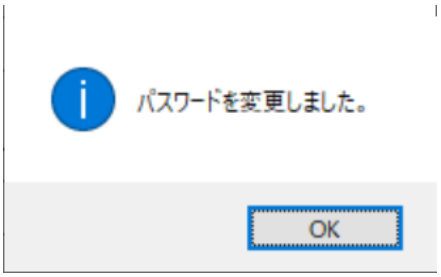


新しいパスワードとパスワードヒントを入力し、[登録]をクリックします。

※パスワードヒントを設定しなくてもパスワードの設定は可能です。パスワードヒントの登録は任意です。



登録が完了するとパスワード変更完了画面が表示されます。[OK]をクリックすると、パスワード入力画面へ戻ります。



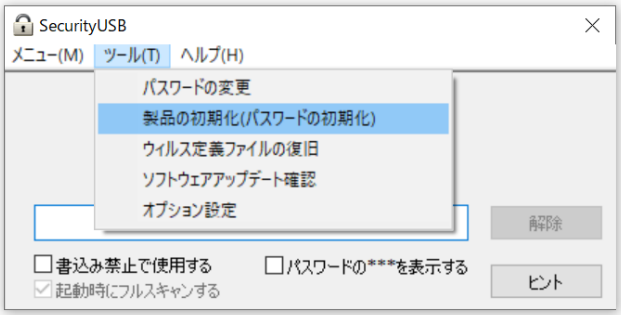
変更した新しいパスワードを入力しロックを解除してください。

本製品の初期化（パスワードの初期化）

パスワードを紛失した場合、本製品を再度ご利用になるには初期化を行う必要があります。

ご注意！	本製品の初期化を実施した場合、メモリへ保存したファイル、登録したパスワード、パスワードヒント等すべて削除されますので十分ご注意ください。 パスワードの紛失により、メモリにアクセスできない、保存ファイルの内容確認ができないといったパスワードを紛失したことに起因する事態に対し、弊社は一切の責任を負いません。また、一切の補償をいたしません。 パスワードを 5 回以上間違えたことにより、メモリにアクセスできない事態に対して弊社は一切の責任を負いません。また、弊社では本製品のメモリからファイル救出をお受けできませんので、ご了承ください。

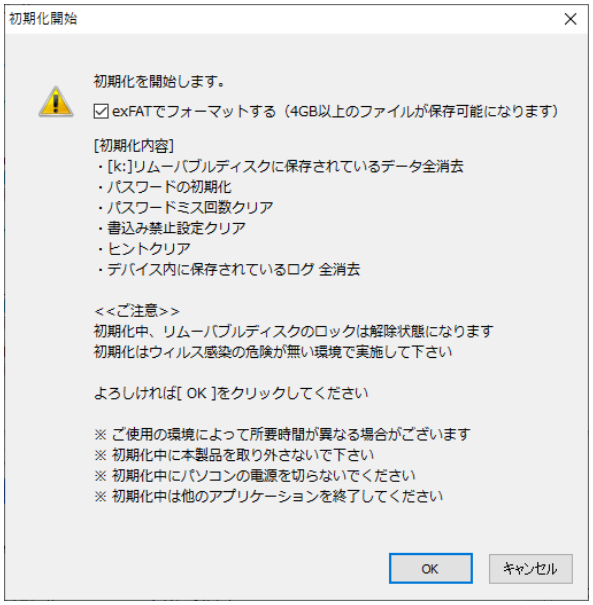
パスワード入力画面から[ツール]をクリックし[製品の初期化（パスワードの初期化）]をクリックします。



注意事項が表示されますので、内容を確認の上、問題が無ければ[OK]をクリックします。

4GB 以上のファイルを使用する場合は、[exFAT でフォーマットする]にチェックを入れてください。

製品の初期化（パスワードの初期化）の途中、特殊フォーマットの確認画面が表示されます。
お客様のシステム等で本製品に対して、特殊フォーマットが不要な場合は[OK]をクリックします。

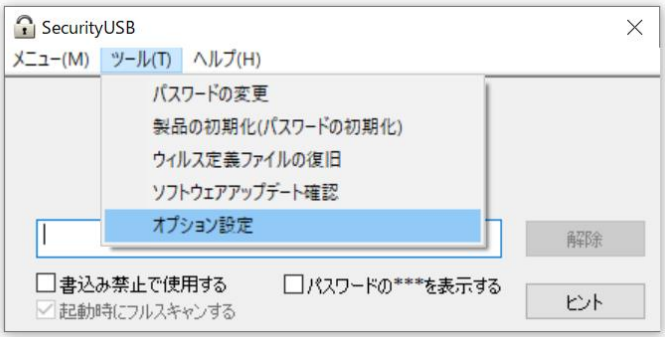


特殊フォーマットが必要な場合は、お客様のシステムにおける「専用のフォーマットソフト」等でメモリのフォーマットを行ってください。
フォーマットが完了したら[OK]をクリックしてください。

初期化完了画面が表示されますので[OK]をクリックします。

オプション設定

本製品のオプション設定ができます。パスワード入力画面から[ツール]をクリックし[オプション設定]をクリックします。
各項目を設定後、[OK]をクリックしてください。



オプション設定　内容

■書き込み禁止設定

本製品への書き込みを常に禁止することができます。書き込み禁止で使用する場合はチェックを入れてください。

■自動ソフトウェアアップデートの設定

本製品起動時に自動的にソフトウェアのアップデート(アップデート確認)を行うか設定ができます。
チェックを入れると起動時にソフトウェアアップデート(アップデート確認)を行います。
また「毎月一度のみ確認する」にチェックを入れると、毎月１度のみ確認し、使用時の起動時間が短縮できます。

■[製品の初期化]時に消去証明書(PDF)の作成

本製品の初期化時に消去証明書(PDF)を発行するか設定ができます。製品を破棄する際にご使用ください。
消去証明書はデスクトップへ保存されます。消去方式は暗号化消去です。

■起動時のウィルススキャン範囲設定（設定変更が禁止されている場合があります。）

パスワード解除直後にスキャンするリムーバブルディスクの範囲を指定することができます。

■ライセンス更新

ライセンスが切れる直前にライセンスサーバへの確認を行います。「ユーザー負担ゼロ更新」の場合、ライセンス延長が行われます。「ユーザー負担ゼロ更新」をご利用の場合は、チェックを入れてください。
このチェックを外すことにより、ライセンスサーバへの確認を行わなくなります。
このチェックを外した場合においても「通常ライセンス更新」、「同一キーライセンス更新」を行うことは可能です。

■InfoBanker（使用時のみ表示されます）

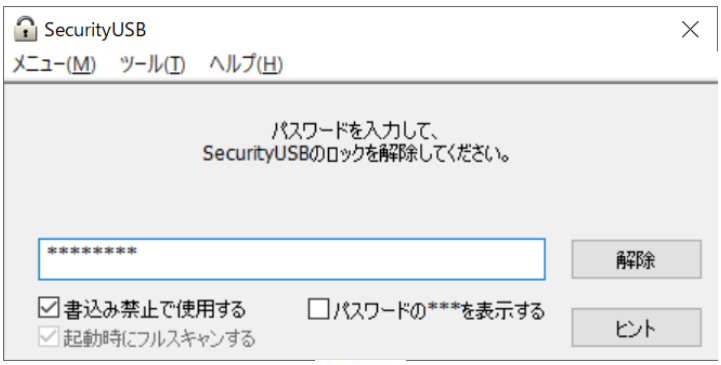
InfoBanker への送信テストを行います。「送信テスト」ボタンを押すことにより InfoBanker へのログ送信テストを実施します。InfoBanker へのログ送信ができない場合にご利用ください。
※[InfoBanker]は SecurityUSB Manager で InfoBanker 設定を有効にした場合に表示されます。

設定したら[OK]をクリックしてください。

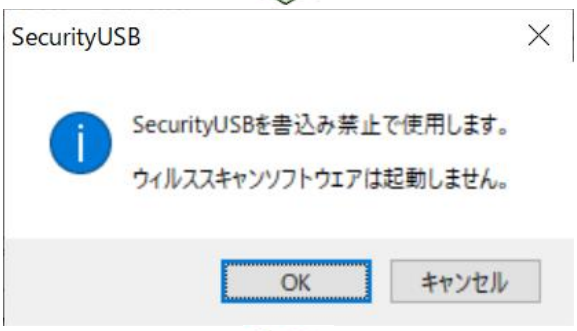
リムーバブルディスク領域への書込みを禁止する

リムーバブルディスク領域に保存されているデータの改ざんや誤消去、ウイルス感染を防止するための機能です。

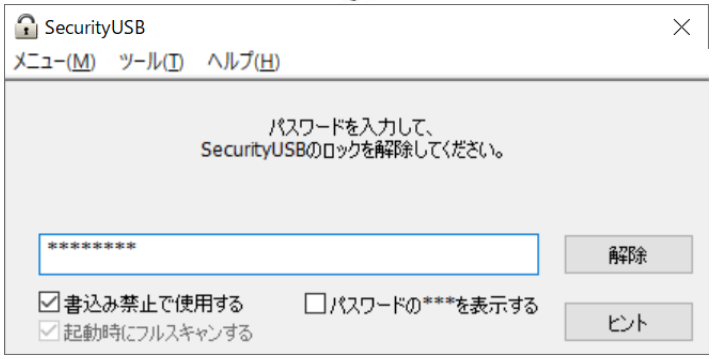
パスワード入力画面の[書き込み禁止で使用する]にチェックを入れます。



右図が表示されたら、[OK]をクリックします。



パスワードを入力し[解除]をクリックすると、リムーバブルディスク領域が書込み禁止の状態で開きます。



※書き込み禁止で使用した場合、ウイルススキャンプログラムは動作しません。

※本製品を取り外すにはタスクトレイから「デバイスの安全な取り外し」を行ってください。

NOTE	書込み禁止を解除するには、次回のパスワード入力時に[書込み禁止で使用する]のチェックを外し、パスワードを入力します。

マニュアル閲覧

パスワード入力画面から[ヘルプ]をクリックし、[マニュアル]をクリックします。弊社 WEB サイトへ移動し、
マニュアル(PDF)を開きます。
※マニュアルをご覧頂くには PDF ファイルを開くことができるソフトウェアが必要です。

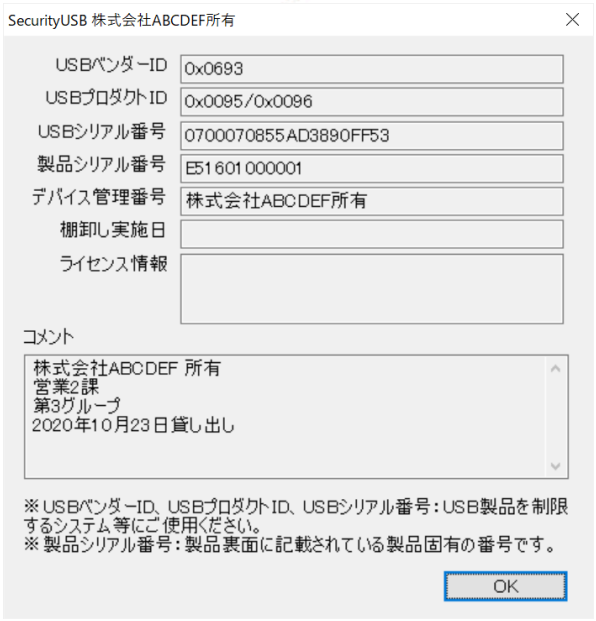
Q&A サイト(web)へ移動

パスワード入力画面から[ヘルプ]をクリックし、
[Q&A サイト(web)へ移動]をクリックします。

※インターネットに接続できる環境が必要です。
※Q&A サイト URL：
http://qa.elecom.co.jp/faq_list.html?category=404

本製品のデバイス情報確認

パスワード入力画面から
[ヘルプ]をクリックし[デバイス情報]をクリックします。



製品のデバイス情報を表示します。

※USB ベンダーID/USB プロダクト ID/USB シリアル番号：
本製品の USB ベンダーID、USB プロダクト ID、USB シリアル番号が表示されます。USB 製品を制限するシステム(デバイスコントロール)等にご使用ください。

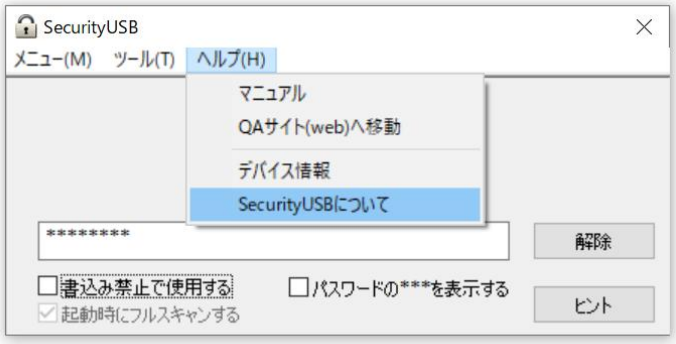
※製品シリアル番号は本製品裏面シールに記載されている製品固有の番号です。

※デバイス管理番号/コメントは、SecurityUSB Manager で設定するデバイスの管理番号およびコメントです。

※棚卸し実施日
INFO BANKER クラウド(有償)を使用し、棚卸しを実施した日

本製品のバージョン・更新履歴確認

パスワード入力画面から[ヘルプ]をクリックし
[SecurityUSB について]をクリックします。



本製品のバージョンが表示されます。
[更新履歴]をクリックすると本製品の更新履歴を表示することができます。

ウイルススキャン機能

パスワード解除すると自動的にウイルススキャンソフトウェア(トレンドマイクロ社 TMUSB2.1)がタスクバーに常駐します。TMUSB2.1 起動後、本製品に対してウイルス監視が開始されます。本製品のリムーバブルディスク領域へファイルがコピーされるとウイルス検索を行い、ウイルスが検知されたファイルを隔離します。

TMUSB2.1 起動直後に本製品のリムーバブルディスク領域に保存されている一部のファイルに対してウイルス検索を行います。

※TMUSB2.1 起動直後にウイルス検索を行うファイル

-リムーバブルディスク領域のルートにある全ファイル

-リムーバブルディスク領域のルートにある autorun.inf ファイル

TMUSB2.1 画面

ウイルススキャンソフトウェア(トレンドマイクロ社 TMUSB2.1)機能

■ウイルス隔離機能(自動実行)

本製品は、本製品のリムーバブルディスク領域へのファイルの書き込みを監視しています。監視はパスワード解除後に自動的に開始されます。ウイルスに感染したファイルが検出されるとファイルを隔離します。

■ウイルス定義ファイル更新機能(自動実行)

本製品は、ウイルス定義ファイルをダウンロードし、更新します。この処理はパスワード解除後に自動的に行われます。

本製品内ファイルのウイルス検索

本製品のリムーバブルディスク領域の全ファイルに対してウイルス検索を行います。
システムトレイの TMUSB2.1 アイコンをクリックし、メニューより[ウイルス検索開始]を選択してください。
ウイルス検索が開始されます。

ウイルス検索を途中で停止したい場合は、同メニューより[ウイルス検索停止]を選択してください。

ウイルスパターンファイルのアップデート

TMUSB 2.0 起動後、本製品内のウイルスパターンファイルより新しいウイルスパターンファイルがある場合、ウイルスパターンファイルのアップデートを行います。ウイルスパターンファイルのアップデート方法としては、以下の二通りの方法があり、自動的に最適な方法でダウンロードします。

1:トレンドマイクロ社のサーバよりウイルスパターンファイルをダウンロードする。

インターネットにつながっている環境が必要です。

2: ウイルスバスター コーポレートエディション(ウイルスバスター Corp.) 10.5/10.6 が保有するウイルスパターンファイルをコピーする。

インターネット接続が出来ない環境下で、本製品を接続している PC にインストールされているウイルスバスターコーポレートエディション(ウイルスバスター Corp.) 10.5/10.6 から、ウイルスパターンファイルをコピーします。

本機能は、エレコム株式会社より提供される機能であり、トレンドマイクロ社は、本機能に関する一切のサポートサービスおよび保証を行なっておりません。また、本機能の利用にあたり発生する損害等について一切の責任を負いません。
本機能は、「Trend Micro USB Security」のサポートサービス契約が有効期間内である必要があります。
本機能は、トレンドマイクロ社製品の「従来型スキャン」機能を有効とする必要があります。
本機能は、トレンドマイクロ社製品の仕様変更またはサポートサービス終了などにより、事前通知なく提供が終了する場合があります。

- Trend Micro Apex One 2019（※）
- ウイルスバスターコーポレートエディション XG（※）
- ウイルスバスタービジネスセキュリティ 9.0（※）、9.5（※）、10.0（※）

※これらの製品では、従来型スキャンを使用時のみローカルアップデートを利用可能。

任意のタイミングでウイルスパターンファイルをアップデートする

任意のタイミングでウイルスパターンファイルを
アップデートします。

システムトレイの TMUSB2.1 アイコンをクリックし、
メニューより[アップデート]を選択してください。
ウイルスパターンファイルのアップデートが開始されます。

隔離されたファイルを確認する

隔離されたファイルを確認します。

システムトレイの TMUSB2.1 アイコンをクリックし、
メニューより[隔離結果を表示]を選択してください。
隔離されたファイルが表示されます。

隔離されたファイルを復元する場合、ファイル選択後、
[復元]ボタンを押してください。

隔離されたファイルを削除する場合、ファイル選択後、
[削除]ボタンを押してください。

ログを確認する

ウイルス検索ログを確認します。
システムトレイの TMUSB2.1 アイコンをクリックし、
メニューより[メイン画面を起動.]を選択してください。
次に、タブで[ログ]を選択してください。

保護の履歴を表示します。保存期間が 30 日を過ぎた
項目は自動的に削除されます。

プロキシ設定を行う

プロキシ設定を行います。
使用するコンピュータがプロキシサーバ経由でインターネットに接続されている場合、設定を行なってください。

システムトレイの TMUSB2.1 アイコンをクリックし、メニューより[メイン画面を起動.]を選択してください。
次に、タブで[プロキシ設定]を選択してください。

プロキシサーバを使用する場合は、[プロキシサーバを使用してインターネットに接続する]にチェックを入れてください。

[Internet Explorer のプロキシ設定をインポートする]
Internet Explorer のプロキシ設定をインポートする場合、本項目を選択してください。

[次のフィールドに、必要なプロキシサーバ設定を入力する]
プロキシサーバ設定を独自に設定する場合、本項目を選択し、プロキシサーバ、ポート番号、ユーザ名、パスワードを入力してください。

プロキシサーバの設定項目につきましては、お客様のネットワーク管理者へ確認を行なってください。

ウイルス検索から除外するファイル、フォルダ設定を行う

ウイルス検索から除外するファイル、フォルダ設定を行います。

システムトレイの TMUSB2.1 アイコンをクリックし、メニューより[メイン画面を起動]を選択してください。
次に、タブで[除外リスト]を選択してください。
[ファイルの追加]もしくは[フォルダの追加]を選択し、本製品のリムーバブルディスク領域からファイルもしくはフォルダの選択を行なってください。

TMUSB2.1 の主要コンポーネントを確認する

TMUSB2.1 の主要コンポーネントを確認します。
ウイルス検索エンジン、ウイルス検索パターン、
TMUSB2.1 のバージョンの確認ができます。

システムトレイの TMUSB2.1 アイコンをクリックし、
メニューより[メイン画面を起動]を選択してください。
次に、タブで[コンポーネント]を選択してください。

TMUSB2.1 のアクティベーション日、有効期限を確認する

TMUSB2.1 のアクティベーション日、有効期限を確認
します。

システムトレイの TMUSB2.1 アイコンをクリックし、
メニューより[バージョン情報]を選択してください。

TMUSB2.1 のライセンスについて

TMUSB2.1 はライセンス製品です。アクティベーションを行なってからライセンス年数の期間、使用することができます。
ライセンス期間が終了すると TMUSB2.1 は起動しなくなるので、ライセンスの更新（有償）をご検討ください。
なお、ライセンス有効期限はメニューの[バージョン情報]より確認できます。

■ライセンス有効期限 1 ヶ月前

ライセンス有効期限の 1 ヶ月前から TMUSB2.1 が起動する時に以下の警告メッセージが表示されます。
ライセンス期間を延長する場合は[今すぐ更新]ボタンを押し、弊社ホームページで案内している手順に従い、ライセンスの更新(有償)を行なってください。

■　ライセンス有効期限が切れた場合

ライセンス有効期限が切れた場合、TMUSB2.1 が動作しないため非常に危険な状態になります。
また以下の警告メッセージが表示されます。
ライセンスを更新する場合は[今すぐ更新]ボタンを押し、弊社ホームページで内容を確認頂きライセンスの更新(有償)を行なってください。

TMUSB2.1 に問題が発生した場合

TMUSB2.1 で問題が発生した場合、トレンドマイクロ社で解析を行うための情報を取得するサポートツールを用意しています。

1:システムトレイの TMUSB2.1 アイコンをクリックし、メニューより[サポートツール]を選択してください。
2:以下の画面で[開始ボタン]を押し、その後問題が発生する処理を行なってください。
問題が発生したら[停止]ボタンを押し、[次へ]ボタンを押してください。

3:以下の画面で[情報の取得]ボタンを押してください。情報の取得が終了したら[次へ]ボタンを押してください。

4:以下の画面で[情報の表示]ボタンを押してください。取得した情報（診断情報ファイル）が保存された場所が表示されますので、診断情報ファイルを PC の任意の場所に保存し、[終了]ボタンを押してください。

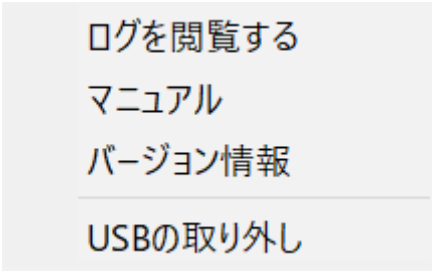
5:診断情報ファイルを症状と共に弊社サポートセンターへ送付してください。

ログの閲覧（PL モニタリング ソフトウェア）

パスワードロックを解除すると PL モニタリング ソフトウェアとウイルススキャンソフト：TMUSB2.1 が起動し、タスクトレーメニューへ格納されます。PL モニタリング ソフトウェア によって使用状況を把握することができるログを閲覧することができます。ログの保存は自動的に行われます。
また、ログは USB の見えない領域に保存されているため、誤って削除することもありません。

■左クリック：PL モニタリング ソフト起動
ニューリスト表示

■右クリック：メ



PL モニタリング ソフトウェア機能

■ログ収集、閲覧機能(別途詳細記載)
本製品の使用履歴ログの収集、閲覧ができます。

■Autorun.inf ファイル削除機能
現在 USB メモリへのウイルスの感染として、USB メモリのリムーバブルディスク領域へウイルスを起動する Autorun.inf をコピーする方法があります。この Autorun.inf の感染を防止するために、本ソフトウェアがリムーバブルディスク領域内の Autorun.inf ファイルを定期的に削除します。

※Autorun.inf 経由でのウイルス感染を防ぐための、簡易的な対策になります。
※Autorun.inf 以外のウイルス感染防止にはなりませんので、ご注意ください。

■USB の取り外し
ウイルス監視を停止し、本製品を OS から取り外しを行います。
取り外し後は、メモリへのアクセスができなくなります。

など

PL モニタリング ソフトウェア画面

全体メニュー(青枠)

項目	内容
ログ閲覧(メイン画面)	USB メモリ内に保存されているログ閲覧ができます。
USB の取り外し	本製品を取り外します。
更新	本画面を更新します。

ログ閲覧画面　説明(オレンジ枠)

機能	内容
ログファイル数 ログ保存領域空き容量	デバイスに保存されているログファイル数とログ保存領域の空き容量を 表示します。
ログファイル名	デバイス内に保存されているログファイルを選択することができます。
ログ出力	現在選択しているログをファイルとして出力します。
ログ一括出力	デバイス内に保存されている全てのログをファイルとして出力します。
ログ一括消去	デバイス内に保存されている全てのログを削除します。
ログ表示	選択されたファイルのログ内容を表示します。

メニューリスト 説明

項目	内容
ログ閲覧を閲覧する	PL モニタリング ソフトウェアを起動し、ログ閲覧画面を表示します。
マニュアル	弊社 WEB サイトへ移動し、マニュアル(PDF)を開きます。 ※マニュアルをご覧頂くには PDF ファイルを開くことができるソフトウェアが必要です。
バージョン情報	PL モニタリング ソフトウェアのバージョン情報が表示されます。
USB の取り外し	本製品を取り外します。

ソフトウェアアップデート

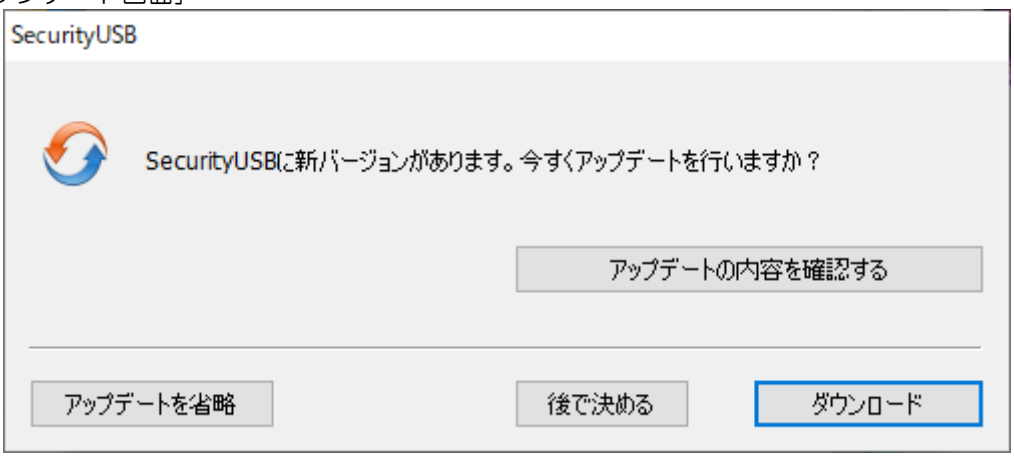
本製品のソフトウェアアップデートは、以下２つの方法で行うことができます。
※ソフトウェア アップデートはインターネットに接続できる環境が必要です。

■手動アップデート：手動でソフトウェアのアップデートを行う
パスワード入力画面のツールバーから[ツール]をクリックし[ソフトウェアアップデート確認]をクリックします。
ソフトウェアアップデートがある場合、アップデート画面が表示されますので、処理を実施してください。

■自動アップデート：本製品起動時に自動的にソフトウェアのアップデートを行う
本製品起動時に自動でアップデート確認を行い、ソフトウェアアップデートがある場合、アップデート画面が表示されますので、処理を実施してください。

※自動アップデートを無効にする場合、パスワード入力画面のツールバーから[ツール]をクリックし[オプション設定]を選択し、「自動ソフトウェアアップデートの設定]内の[セキュリティ対策外付けポータブル SSD 起動時にソフトウェアアップデートを行う」チェックを外してください。

[アップデート画面]



■ダウンロード
ソフトウェアアップデートを行う場合、[ダウンロード]ボタンを選択してください。
ソフトウェアアップデートが開始されます。

■アップデートを省略
本バージョンのアップデートを省略する場合、[アップデートを省略]ボタンを選択してください。
ソフトウェアアップデートを行なわず、パスワード入力画面に移ります。
以降は、次の新しいソフトウェアが公開されるまで、自動でアップデート画面は表示されなくなります。
※省略を選択後、省略したバージョンのアップデートを実施する場合、上記の[手動アップデート]を実施してください。

■後で決める
本バージョンのアップデートを一旦行わない場合、[後で決める]ボタンを選択してください。
ソフトウェアアップデートを行なわず、パスワード入力画面に移ります。
次回、本製品起動時に再度ソフトウェアアップデート画面が表示されます。

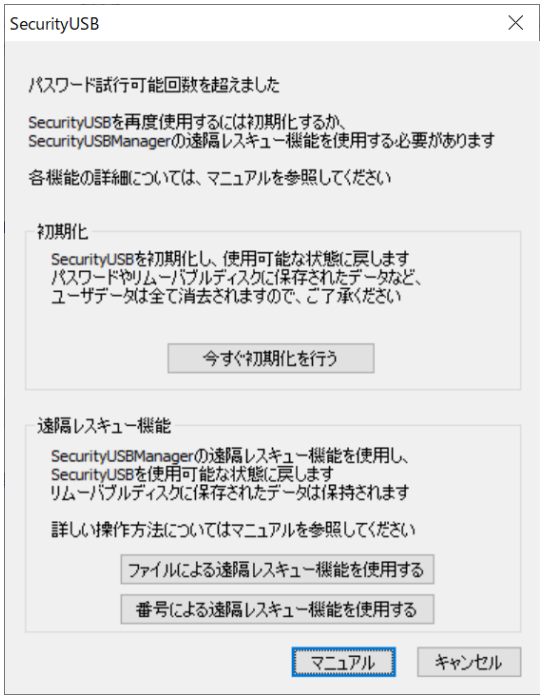
遠隔データレスキュー機能

パスワードを指定回数(標準:5回)以上間違えると、本製品が使用出来なくなります。
しかし、SecurityUSB Manager によって「データ救出設定（パスワードを忘れた時にデータ救出を許可する設定）を“有効”」にすることで、対象となる本製品内のデータを残したまま、パスワードの初期化を行うことができます。
パスワードの初期化には以下の２通りの方法があり、また、パスワードを指定回数間違える前でもパスワードの初期化は可能です。

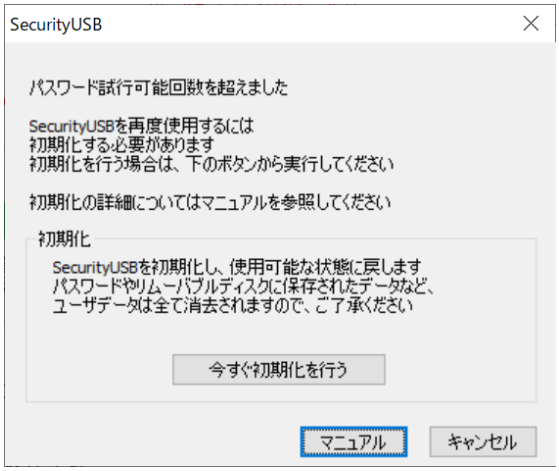
1．　ファイル、番号のやり取りを行うことで、遠隔地にある対象となる本製品のパスワードを初期化。
2．　対象となる本製品を管理者に送付してパスワードを初期化。

本章では１の遠隔地にいるユーザのデータ救出方法を記載します。データレスキュー機能の運用方法については管理者へお問い合わせください。

■SecurityUSB Manager によって「遠隔データレスキュー機能」が許可されている場合
・デバイス内のデータを保持したまま、パスワードのみ初期化を行う場合は[ファイルによる遠隔レスキュー]または[番号による遠隔レスキュー]をクリックしてください。
・デバイス内のデータ/パスワードの初期化を行う場合は[今すぐ初期化を行う]をクリックしてください。

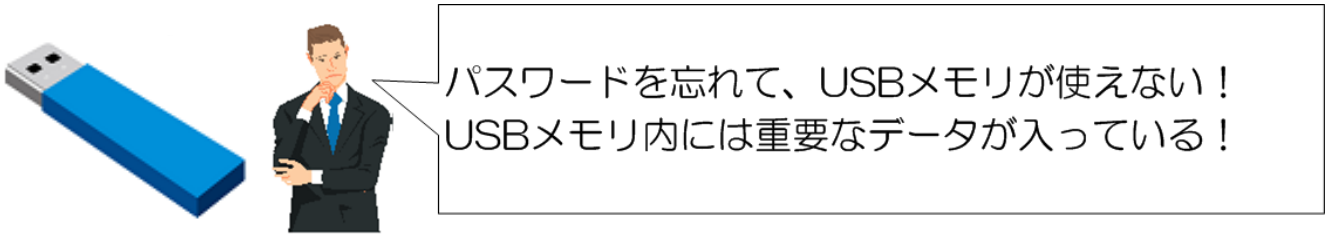


■SecurityUSB Manager によって遠隔レスキュー機能が禁止されている場合
・デバイス内のデータ/パスワードの初期化を行う場合は[今すぐ初期化を行う]をクリックしてください。



遠隔データレスキューの流れ

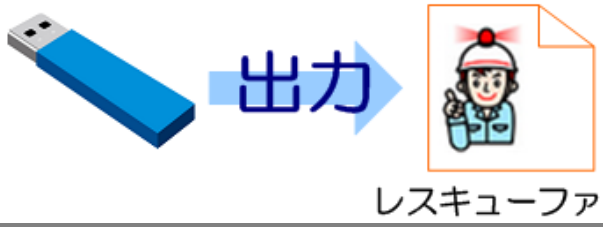
※　SecurityUSB Manager によって遠隔データレスキュー機能を有効している前提の流れです



■レスキューファイルを使用した場合

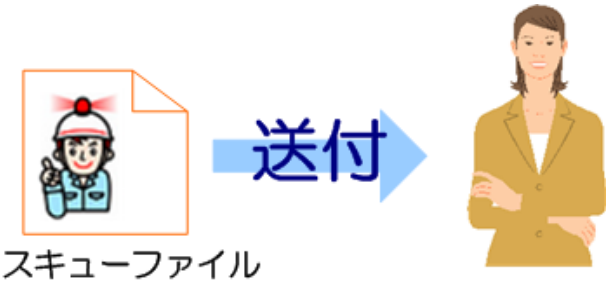
[ユーザ]

対象デバイスからレスキューファイルを出力します。

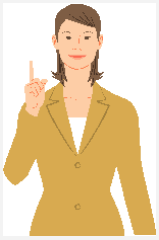


[ユーザ]

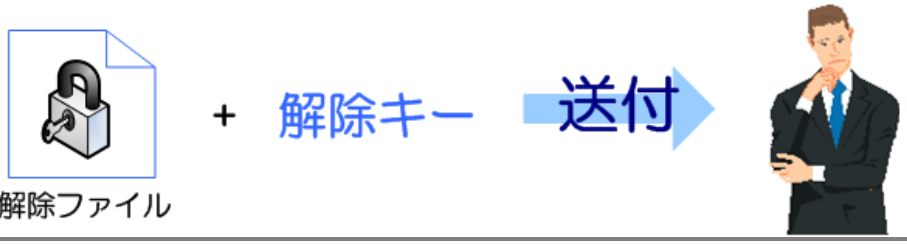
出力したレスキューファイルをメール等で管理者へ渡します。



[管理者]



ユーザよりレスキューファイルを入手し、それを SecurityUSB Manager によって、
解除ファイル/解除キーを作成します。
作成した解除ファイル/解除キーをメール等でユーザへ送付します。



[ユーザ]

管理者より解除ファイル/解除キーを入手し、それを対象デバイス内のソフトウェアで
読み込み、パスワードロック解除を行います。USB 内のデータは保持されています。

■レスキュー番号を使用した場合

[ユーザ]

対象デバイスからレスキュー番号を出力します。

出力

レスキュー番号
12344-22223-FGHUDU…

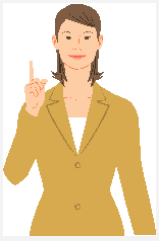
[ユーザ]

出力したレスキュー番号を電話等で管理者へ伝えます。

レスキュー番号
12344-22223-FGHUDU…

送付

[管理者]



ユーザよりレスキュー番号を入手し、それを SecurityUSB Manager によって、解除番号を作成します。作成した解除番号を電話等でユーザへ伝えます

解除番号
JFRTF-7FTDGH-123KJH…

送付

[ユーザ]

管理者より解除番号を入手し、それを対象デバイス内のソフトウェアへ入力、パスワードロック解除を行います。USB 内のデータは保持されています。

解除番号
JFRTF-7FTDGH-123KJH…

入力

■遠隔データレスキュー方法(レスキューファイル使用時)

遠隔データレスキューでユーザが行う処理（①、④）について説明をします。

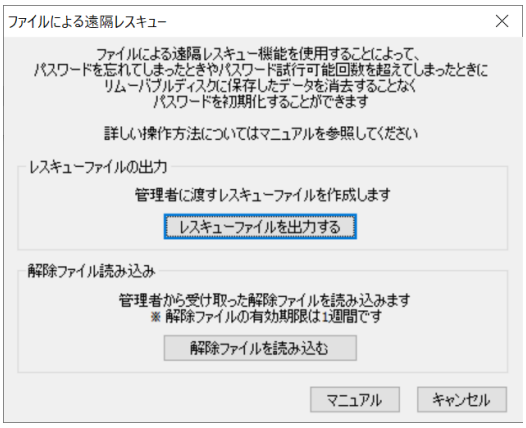
① レスキューファイル出力

パスワード入力画面から[ツール]をクリックし[ファイルによる遠隔レスキュー]をクリックします。

※ツールの[ファイルによる遠隔レスキュー]はSecurityUSB Managerで[データ救出/遠隔データ救出機能]を有効にした時のみ表示されます。

[レスキューファイルを出力する]ボタンをクリックし、レスキューファイルを出力します。

レスキューファイルを管理者へ送付してください。



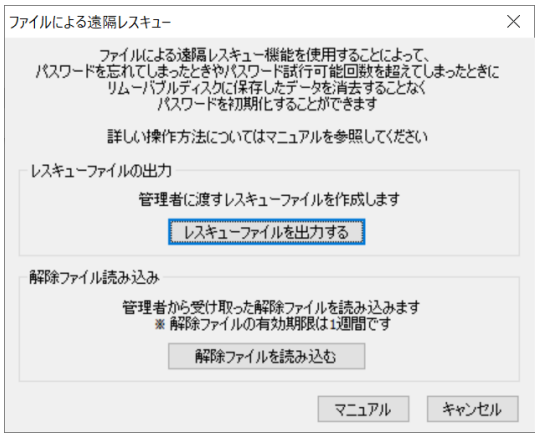
④解除ファイル読み込み/パスワード初期化

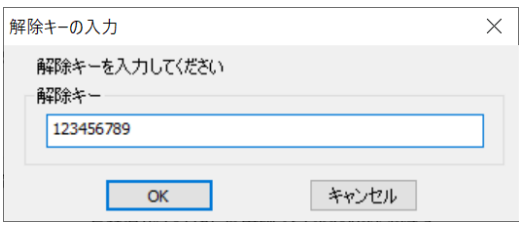
管理者より発行された解除ファイルと解除キーを入手し、パスワード入力画面から[ツール]をクリックし[ファイルによる遠隔レスキュー]をクリックします。

[解除ファイルを読み込む]ボタンをクリックし、管理者から発行された解除ファイルを選択してください。

解除ファイルが正常の場合、解除キー入力画面が表示されるので、管理者より発行された解除キーを入力し、[OK]ボタンをクリックしてください。

解除キーが正常の場合、デバイス内のデータを保持したまま、パスワードが初期化されます。





■遠隔データレスキュー方法(レスキュー番号使用時)

遠隔データレスキューでユーザが行う処理（①、④）について説明をします。

① レスキューファイル出力

パスワード入力画面から[ツール]をクリックし[番号による遠隔レスキュー]をクリックします。 ※ツールの[番号による遠隔レスキュー] は SecurityUSB Manager で[データ救出/遠隔データ救出機能]を有効にした時のみ表示されます。 レスキュー番号が表示されているので、その番号を覚えを管理者へ伝えてください。	

④解除ファイル読み込み/パスワード初期化

管理者より発行された解除番号を入手し、パスワード入力画面から[ツール]をクリックし[番号による遠隔レスキュー]をクリックします。 [解除番号入力欄へ解除番号を入力し、[解除番号の認証]ボタンを押してください。 解除番号が正常の場合、デバイス内のデータを保持したまま、パスワードが初期化されます。	

使用履歴ログ 内容

ログの内容は以下になります。

セクション名：PC Information ※PC 情報に関するセクション	
キー名	内容
Date	ログファイル作成日時　例：2010/12/16 18:06:17
ProductName	OS サービスバックバージョン 例： Windows 7 Professional SP1 (build 7601), 32bit
ProductNameS	OS サービスバックバージョン（短縮） 例： Windows 7　SP1, 32bit
ProductVersion	OS カーネルバージョン 例： 5.1
ComputerName	コンピュータ名 例： HSC
UserName	所有者 例： HAGIWARA TARO
IsAdministrator	ログインしたユーザ権限　0:制限ユーザ　　1:管理者
IsSafeMode	OS 起動モード　　0：通常起動　　1：セーフモード起動
MacAddress	MAC アドレス 例： 11-22-33-44-55-66,　※複数有る場合は”,”区切りで複数記載
IPAddress	IP アドレス　例；10.10.11.111
セクション名：DeviceInformation ※Device 情報に関するセクション	
DeviceID	デバイス ID
ProductID	デバイスの UBS　ProductID
SerialNumber	デバイスのシリアルナンバー
UniqueID	デバイスの固有 ID
VendorID	デバイスの UBS　vendorID
ProductVersion	製品のバージョン情報
DeviceType	弊社管理番号
セクション名：Capacity ※本製品に搭載されたメモリの容量情報に関するセクション	
Capacity_MB	製品に搭載されたメモリ容量(MB)
FreeCapacity_MB	製品に搭載されたメモリの空き容量(MB)
FreeCapacity_Percent	製品に搭載されたメモリの空き容量(%)
セクション名：Location ※本製品を使用した位置情報に関するセクション ※管理ソフトで位置情報取得を有効にした場合のみ	
Longitude、Latitude	本製品を使用した位置情報(緯度・経度)
Result	位置情報取得処理の実行結果
セクション名：License ※TMUSB2.1 のライセンス期間に関するセクション	
LicenseLast	ライセンス終了日
LicenseStart	ライセンス開始日
LicenseTerm	ライセンス期間（日数）
セクション名：ScannerVersion　※起動時の TMUSB2.1 に関するセクション	
AntiVirus	TMUSB2.1 例： 2, 1, 0, 1055
VirusDefinitionFiles	ウイルス定義ファイルバージョン 例： 10.809.00

セクション名：Virus*** ***：ウイルスファイルがある毎に 10 進で増加(例：001～) ※検出したウイルス詳細、及びそのウイルスに対してのウイルススキャンプログラムの処理結果	
Path	ウイルスのフルパス 例： f:¥eicar.zip
VirusName	ウイルス名 例： EICAR test file
CleanAction	ウイルスへの対処鳳凰 隔離処理失敗：「0：NoChange」 隔離処理：「2：Quarantine」
Result	成功：「0：Success」 その他：エラー表示

NOTE	・ログファイルは PL モニタリング ソフトウェア起動ごとに作成されます。 ・ログ内容は予告無く変更される場合があります。 ・InfoBanker に送信済みのログは表示されません。

6 トラブルシューティングと Q&A

質問		回答	
Q1	本製品を PC の USB ポートに接続しても ソフトウェアが自動起動しません。	A1	自動起動しない場合は「マイコンピュータ」または「コンピュータ」を開き、SecurityUSB アイコンを右クリックして[開く]を選択します。開いたフォルダにある「Startup.exe」をダブルクリックしてソフトウェアを実行してください。
Q2	本製品を PC が認識しません。	A2	1. PC に本製品が正しく挿入されているか確認してください。 2. ネットワークドライブをお使いの場合は、ドライブレター（マイコンピュータ上のドライブアイコンに割り当てられている文字）にご注意ください。Windows で本製品を使用する場合は、ネットワークドライブのドライブレターが本製品のドライブレターと重ならないようにネットワークドライブのドライブレターを変更するか、一時的にネットワークドライブの接続を解除してください。本製品を PC に接続すると、仮想 CD-ROM ディスク とリムーバブルディスクの 2 つのドライブが表示されます。お使いの PC の CD/DVD-ROM ディスクまたはハードディスの最終のドライブレターから 2 つ使用します。例えば、C ドライブがハードディスク、D ドライブが DVD-ROM をお使いの場合、本製品は E ドライブと F ドラ イブを使用します。 この状態でネットワークドライブを E ドライブや F ドライブに割り当てている場合、ネットワークドライブが優先されて表示されてしまうため、本製品で使用するドライブが表示されず、正しく動作できません。 3. USB ハブ経由では使用できない場合があります。その場合は直接 PC に接続してください。
Q3	パスワードを入力しても[登録]ボタンが押せないため、初期設定ができません。	A3	指定された文字数の範囲でパスワードを入力しているか確認の上、再度入力してください。 ※パスワードの文字数は 8～16 文字までです。 ※パスワードには半角英数字と以下の半角記号が使用できます。 ! # $ % & ' ( ) = ~ | ` { + * } < > ? _ - ^ ¥ @ [; :] , . /
Q4	パスワードを忘れてしまいました。	A4	1. 初期設定時にパスワードヒントを登録した場合、SecurityUSB の[ヒント]ボタンをクリックすると、お客様が登録したヒントを確認することができます。 2. パスワードを完全に忘れてしまった場合、SecurityUSB のメニューのツール→[製品の初期化]を選択してパスワードの初期化を行い、新たなパスワードを再設定してください。 注意；初期化を行うと、リムーバブルディスク領域に保存されて

			いるお客様のデータは全て削除されます。 3. データレスキュー/遠隔データレスキュー機能が許可されている場合、デバイス内のデータを保持したまま、パスワードを初期化できます。SecurityUSB Manager を管理している管理者へ問い合わせを行なってください。
Q5	パスワードロックを解除してもリムーバブルディスク領域が開きません。	A5	本製品を一旦、USB ポートから取り外し、再度接続してから、「SecurityUSB」を起動してください。
Q6	暗号化されたファイル、パスワードが掛かったファイルをウイルス検索できますか？	A6	暗号化されたファイル、パスワードが掛かったファイルのウイルス検索はできません。 本製品に書込むことは可能です。
Q7	“0”Byte のデータ、”0”Byte のデータを含む圧縮ファイルを本デバイスへ保存することはできますか？	A7	保存することができます。
Q8	TMUSB2.1 は PC 内へファイルを書込みますか？	A8	一時的に PC の temp フォルダ内にファイルをコピーして使用します。
Q9	ファイルが本製品に書き込まれる前にウイルス検索は行われますか？	A9	本製品の TMUSB2.1 は、本デバイスにファイルが書き込まれた後に、そのファイルに対しウイルス検索を行います。 ウイルス感染が発見されたファイルは隔離されます。
Q10	本製品に移動したファイルがウイルス感染していた場合、PC 上にあるファイルは残りますか？	A10	移動したファイルは PC 上には残りません。 コピーした場合、コピー元のファイルは残ります。
Q11	ウイルスパターンファイルはどのくらいの頻度で更新しますか？	A11	原則として 1 日 1 回です。月～金曜日に更新されます。
Q12	ウイルスパターンファイルの更新時間はどのくらいですか？	A12	通信環境によりますが、日本国内の標準的なネットワーク回線の場合、1 分程度掛かります。
Q13	ウイルスパターンファイルの更新状態が続いて、待機状態になりません。	A13	ご使用の環境により、ウイルスパターンファイルのダウンロード（更新）に時間がかかる場合があります。更新が完了するまでしばらくお待ちください。
Q14	本製品をパソコンの USB ポートに接続すると、タスクトレイまたは通知領域に次のメッセージが表示されます。 「さらに高速で実行できるデバイス」	A14	本製品は USB2.0 に対応していますが、接続した USB ポートが USB2.0 に対応していないために表示されるメッセージです。この場合、本製品は USB2.0 ではなく 1.1 の速度で動作します。
Q15	Windows で設定したパスワードは macOS でも共通ですか？	A15	共通です。
Q16	本バージョン(ver300)から自動パスワード解除が無くなっていますか？	A16	MAC アドレスをユーザ様が設定する方式の代わりに、 管理者様がファイル、フォルダ、レジストリキーを設定する方式を採用しました。そのためユーザ様が設定を行う必要が無くなりました。

その他の Q&A については以下の Web ページをご確認ください。
http://qa.elecom.co.jp/faq_list.html?category=404

7 サポート・メンテナンス・ライセンス

保証期間 （ハードウェア本体）	1 年；MF-PUVT3**GM1 3 年；MF-PUVT3**GM3 5 年；MF-PUVT3**GM5 ※本製品納品日から保証期間が有効になります。

お問合せ窓口

ご連絡先		受付
エレコム総合インフォメーションセンター	TEL：0570-084-465	平日　9:00～12:00 / 13:00～18:00 ※土日祝日、夏季ならびに年末年始の特定休養日を除く。

※内容を正確に把握するため、通話を録音させていただいております。個人情報に関する保護方針はホームページをご参照ください。http://www.elecom.co.jp/privacy/

ナビダイヤルについて

弊社ではサービスサポートお問い合わせ窓口にナビダイヤルを採用しています。
全国の固定電話から1分間10円の通話料（発信者のご負担）でご利用いただける「全国統一番号」で、NTTコミュニケーションズ（株）が提供するサービスのひとつです。
ダイヤルQ2などの有料サービスではなく、ナビダイヤル通話料から弊社が利益を得るシステムではありません。
※携帯電話からは20秒10円の通話料でご利用いただけます。※PHS・一部のIP電話からはご利用いただけません。
※お待ちいただいている間も通話料がかかりますので、混雑時はしばらくたってからおかけ直しください。

本製品にはオープンソースのファイルアーカイバ[7-Zip]を使用しております。
以下にライセンス情報を記載します。
◆ライセンス
7-Zip: www.7-zip.org

License for use and distribution
7-Zip Copyright (C) 1999-2016 Igor Pavlov.

Licenses for files contained in 7zip folder are:
1) 7z.dll: GNU LGPL + unRAR restriction
2) All other files: GNU LGPL

ウイルス対策 USB
型番：MF-PUVT3**GM*
Windows マニュアル
2024 年 12 月