

## ウイルス対策 USB 型番：HUD-PUVM3\*\*GM\* Windows マニュアル

この度はウイルス対策 USB HUD-PUVM3\*\*GM\*シリーズ(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。この取扱説明書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、必ずこの取扱説明書をお読みください。

本取扱説明書では本製品を Windows で使用した場合の動作を記載しております。Mac OS X で使用した場合のマニュアルは Mac OS X 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、米国 McAfee Co.,Ltd.(以下、McAfee 社と言います) 製エンジンを搭載したウイルススキャンプログラム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、お願いいたします。

#### 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

 <b>警告</b>	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。
 <b>注意</b>	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取扱説明書の使用方法、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のを御希望のときは、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從ってください。
- ・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いたします。
- ・本製品は、最新のウイルス定義ファイルに更新して使用してください。ウイルス定義ファイルは、お客様が本製品をPCに接続し、McAfee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。
- ・本製品は、最新のウイルスパターンファイルに更新することで、McAfee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。
- ・本製品のウイルススキャンプログラムは、発見したウイルスに感染したファイルを削除するものです。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削除しますので、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

1. 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

2. 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

3. 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。
4. 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。
5. 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。
6. 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。
7. 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

8. 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、本製品購入代金を上限とさせていただきます。
9. 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

10. 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 HUD-PUVM3\*\*GM\*(製品本体) ×1 個

## 3 本製品について

本製品は、McAfee 社製ウイルススキャンエンジンを搭載したウイルススキャンプログラムにより、ウイルスの検出及びウイルス感染したファイルを削除する機能をもつウイルス対策 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。

#### ✓ **McAfee 社製ウイルススキャンエンジンを使用したウイルススキャン機能**

本製品に書きこまれたファイルに対してウイルススキャンを行います。

本製品を PC に接続するとタスクトレイにウイルススキャン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。

#### ✓ **ウイルス定義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定義ファイルは、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。

#### ✓ **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き込み禁止機能**

リムーバブルディスク領域を書き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 X に対応

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

注意：Mac OS X 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	USB1.1 (Full Speed)/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	Windows XP with SP3 Windows XP Embedded with SP2 Windows VISTA with SP1 and SP2 Windows 7 with SP0 and SP1 Windows Server 2003 with SP2 *10 Windows Server 2003 R2 with SP2 *10 Windows Server 2008 with SP2 *10 Windows Server 2008 R2 *7 *10 Windows Server 2012 *7 *10 Windows 8 Windows 8.1 Mac OS X 10.4.11 以上 Mac OS X 10.5.8 以上 Mac OS X 10.6.8 以上 Mac OS X 10.7.5 以上 Mac OS X 10.8.5 以上 Mac OS X 10.9.3 以上  ※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。  ※Mac OS X：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。 ウィルススキャン機能及び、 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。  ※McAfee 社のサポート終了に伴い Windows 2000 のサポートは終了しました。  ※Windows XP のサポートは 2017 年末までを予定しています。
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。

64bit OS 上では「WOW64」機能を使用し、32bit 互換モードで動作します。

64bit OS 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 64bit OS 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 X は Intel CPU 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。



本製品にはソフトウェアがブ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 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解除を行ってください。
----------------------	-----------------------------------------------------------------------



本製品にデータ を書込む/読み込む	本製品のリムーバブルディスク領域にアクセスできるようになるので、リムーバブルディスク領域に保存するデータのコピーまたは移動をします。 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った、そのファイルを削除します。
----------------------	---------------------------------------------------------------------------------------------------------------------



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）」をクリック、もしくは「ハードウェアの安全な取り外し」アイコンをクリックしてください。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ます。
----------	--------------------------------------------------------------------------------------------------------------------------------------------------

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場合があります。
- ・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。




オペレーティングシステムの自動実行機能により本製品の使用許諾約款が表示されますので、内容を確認頂き、問題がなければ、[使用許可契約に同意します]を選択し、[OK]ボタンをクリックしてください。





 NOTE	<p>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。</p>
---------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

 NOTE	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul>
---------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 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

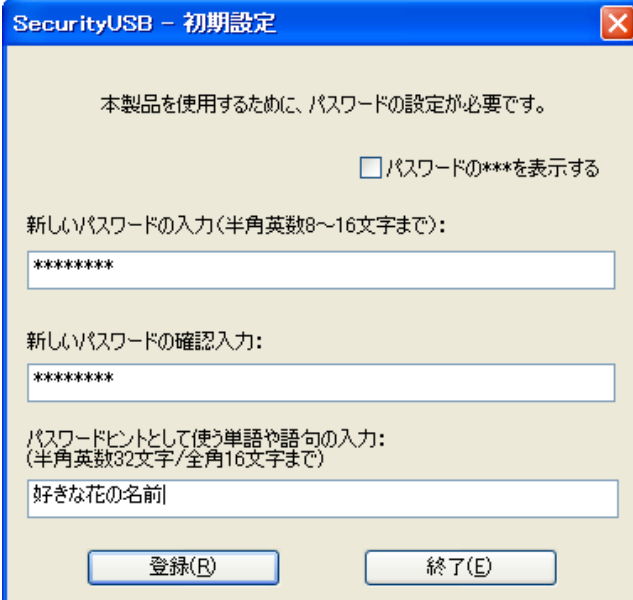
### 1. パスワードを入力します。


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。



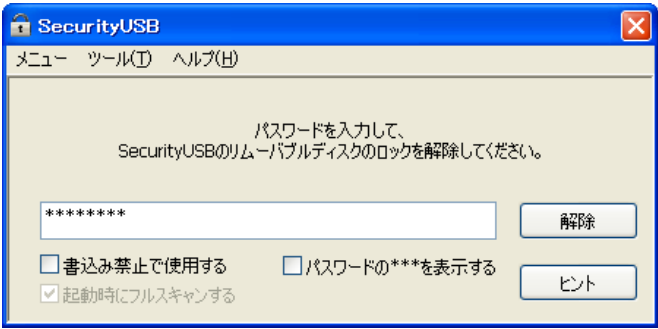
 NOTE	<ul style="list-style-type: none"> <li>・パスワードを設定しないと本製品のリムーバブルディスク領域は使用できません。</li> <li>・解除される恐れのあるような簡単なパスワードを設定しないように注意してください。</li> </ul>
-----------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------



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、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ブ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。
	<p>パスワードの紛失やパスワードの入力を 5 回以上間違えた場合、本製品の使用（リムーバブルディスク領域にアクセスすること）ができなくなります。本製品を再度ご使用になるには「本製品の初期化（パスワードの初期化）」が必要となり、その場合はパスワードやリムーバブルディスク領域に保存されたデータがすべて削除されます。パスワードの入力を 5 回以上間違えたことにより、リムーバブルディスク領域にアクセスできない、データの強制消去、データの内容確認ができないといった事態、その他に対して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。</p> <p>※パスワードの入力を 5 回以上間違えた本製品のリムーバブルディスク領域からデータを読み出すことは、弊社ではお受けできませんので、ご了承ください。</p>



## 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。

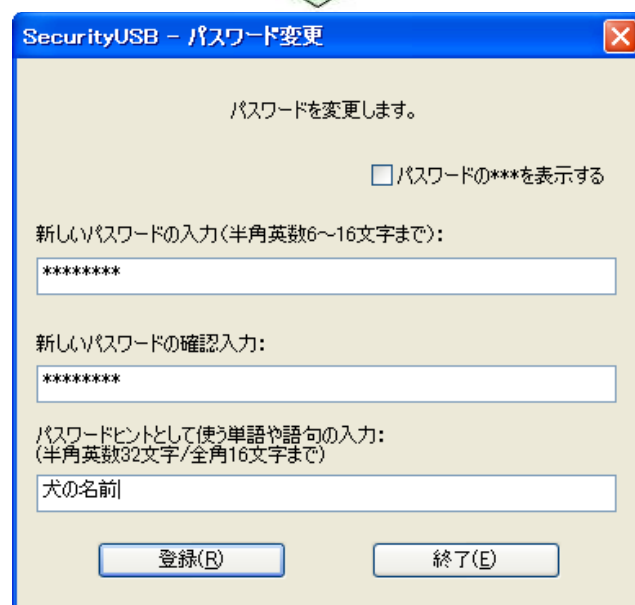
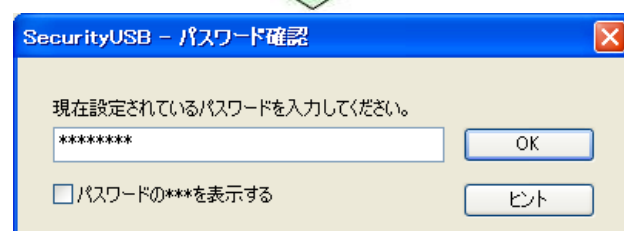
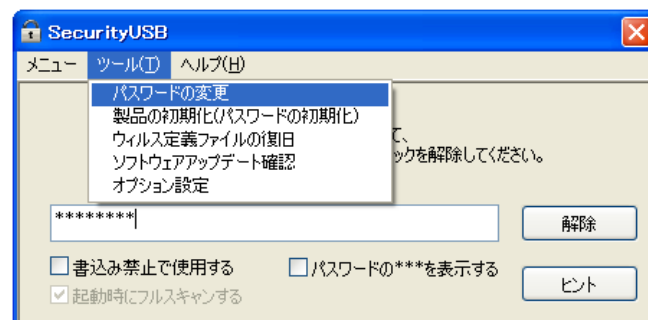
パスワード入力画面から「ツール」をクリックし「パスワードの変更」をクリックします。

現在設定しているパスワードを入力します。

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。






## 本製品の初期化（パスワードの初期化）

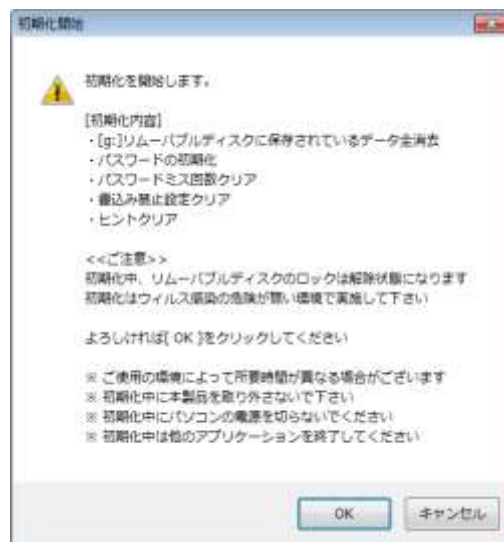
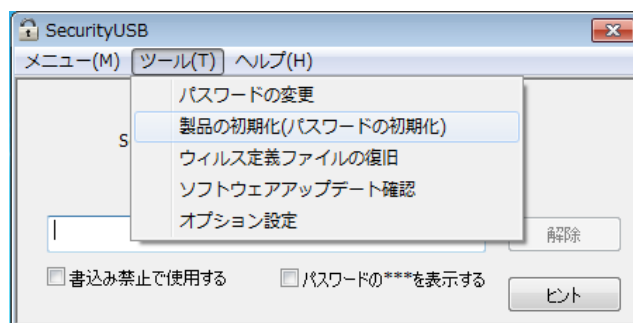
パスワードを紛失した場合、本製品を再度ご利用になるには初期化を行う必要があります。

	パスワードを初期化すると、パスワードとリムーバブルディスク領域に保存されているユーザデータ、ログは削除されますので、バックアップを取っておくことをおすすめします。
-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------

	<p>本製品の初期化（パスワードの初期化）を行うと、パスワードやリムーバブルディスク領域に保存されたデータがすべて削除されます。パスワードの紛失により、リムーバブルディスク領域にアクセスできない、データの強制消去、データ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。</p> <p>※パスワードを紛失した際、弊社では本製品のリムーバブルディスク領域からデータを読み出すことはお受けできませんので、ご了承ください。</p> <p>※本製品に保存するデータはバックアップを取っておくことをおすすめします。</p>
-----------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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。

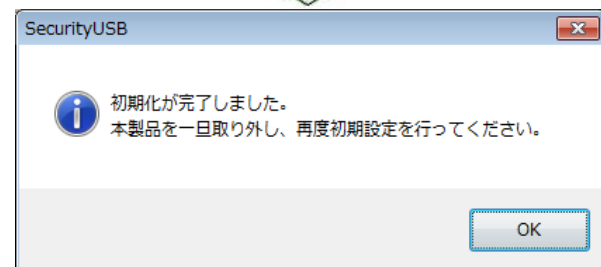
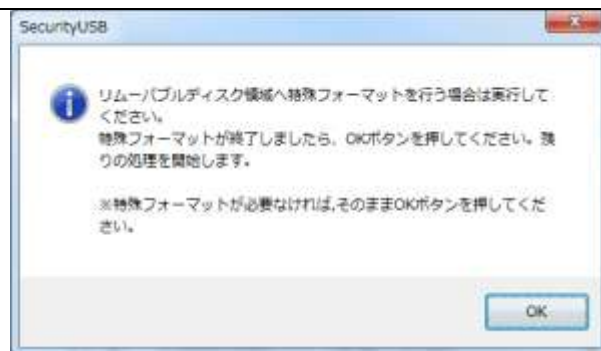




製品の初期化（パスワードの初期化）の途中、特殊フォーマットの確認画面が表示されます。  
お客様のシステム等で本製品に対して、特殊フォーマットが不要な場合は[OK]をクリックします。

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」等でリムーバブル ディスク領域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。

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。





## 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。

## 起動時のウイルススキャン範囲設定

本製品はパスワードロック解除後、リムーバブルディスク領域のファイルに対してウイルススキャンを行います。本設定では、そのウイルススキャンの範囲を設定することができます。

※[起動時のウイルススキャン範囲設定]は SecurityUSB Manager でユーザによる設定変更が有効の場合、設定可能です。

## 検知したウイルスの削除

本製品に書き込まれたファイルにウイルスが検知された場合、ウイルス情報を画面に表示し、標準設定ではそのファイルを削除します。

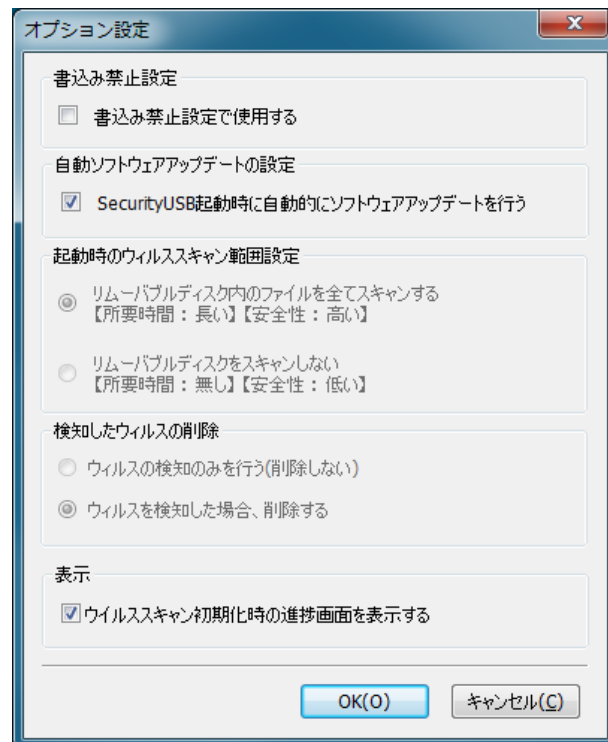
本設定では、ウイルスが検知されたファイルの処理方法について設定することができます。

※[検知したウイルスの削除]は SecurityUSB Manager でユーザによる設定変更が有効の場合、設定可能です。

## 表示設定

本製品のウイルススキャンプログラム初期化時に、初期化の進捗を画面に表示させる設定ができます。チェックを入れると、進捗が表示されます。

設定したら[OK]をクリックしてください。



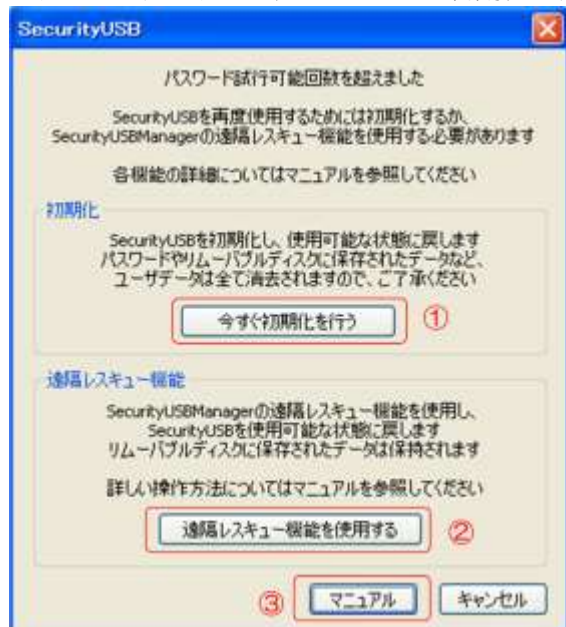


## パスワードを 5 回以上間違えた場合の動作について

パスワードを 5 回以上間違えた場合、本製品の使用ができなくなります。  
その後、本製品を PC に接続すると以下の画面が表示されます。

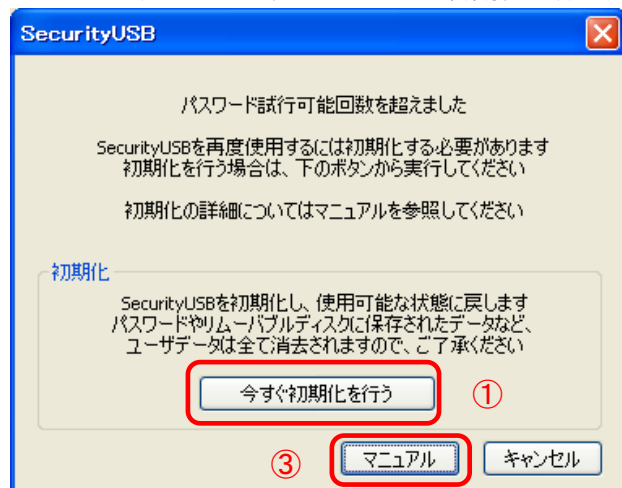
### ■SecurityUSB Manager によって[遠隔データレスキュー機能]が許可されている場合

- ・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[遠隔レスキュー機能を使用する]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[データ救出/遠隔データレスキュー機能]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。



No	項目	内容
①	今すぐ初期化を行う	本製品の初期化を行います。 詳細は本マニュアルの項：本製品の初期化（パスワードの初期化）を確認してください。
②	遠隔レスキュー機能を使用する	本製品内のデータを保持したまま、パスワードのみ初期化を行います。 詳細は本マニュアルの項：遠隔データレスキュー機能を確認してください。
③	マニュアル	本製品のマニュアルを開きます。 ※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。



	<p>本製品の初期化を行うと、パスワードやリムーバブルディスク領域に保存されたデータがすべて削除されます。パスワードを5回以上間違えたことにより、リムーバブルディスク領域にアクセスできない、データの強制消去、データの内容確認ができないといった事態、その他に対して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。</p> <p>※パスワードを紛失した際、弊社では本製品のリムーバブルディスク領域からデータを読み出すことはお受けできませんので、ご了承ください。</p> <p>※本製品に保存するデータはバックアップを取っておくことをおすすめします。</p>
-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


## 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。

本章では遠隔データレスキュー機能について記載します。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。

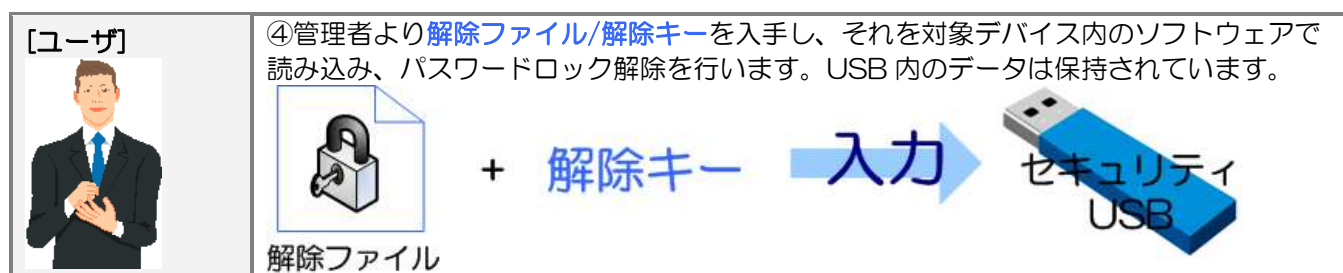
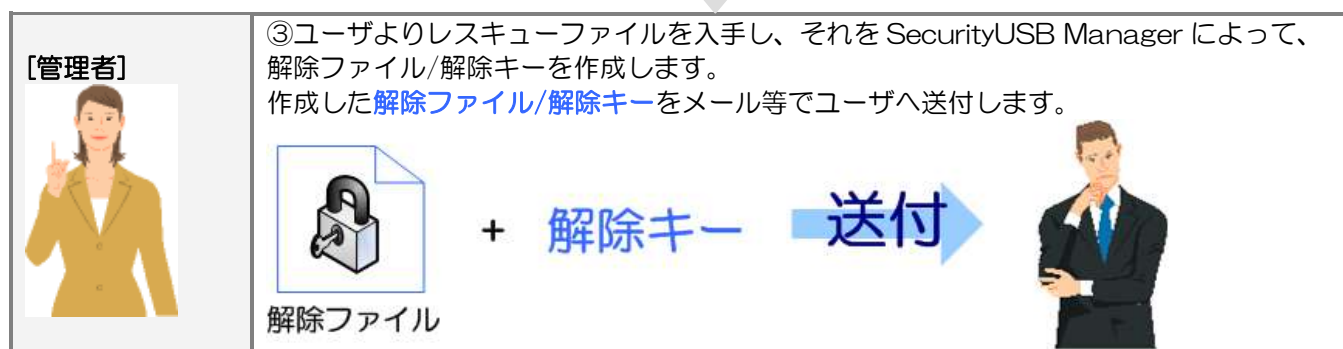
	<p>本機能を使用するには”事前”に SecurityUSB Manager によって遠隔データレスキュー機能を有効にする必要があります。パスワードを指定回数間違えた後に、デバイス内のデータを保持したまま、遠隔データレスキュー機能を有効にすることはできないので、ご注意ください。</p>
------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------

### ■ 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にしていることが前提の流れとなります。







## ■遠隔データレスキュー方法

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。

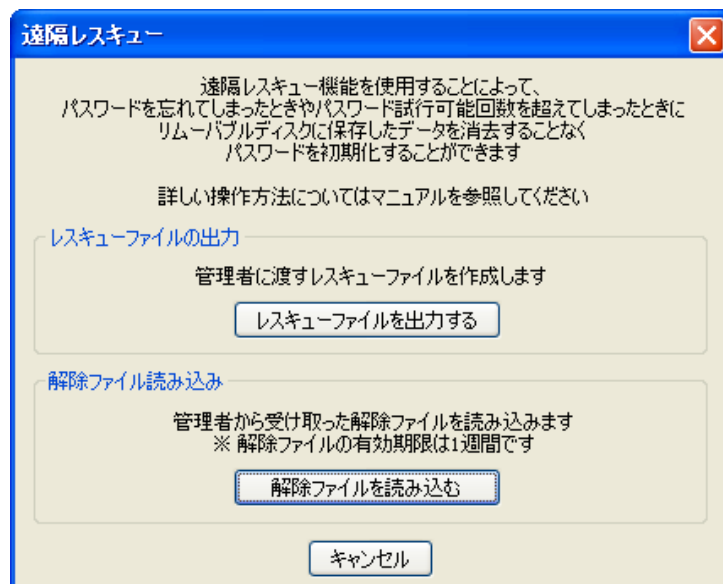
### ①レスキューファイル出力

パスワード入力画面から[ツール]をクリックし  
[遠隔レスキュー機能]をクリックします。

※ ツールの[遠隔レスキュー機能]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。





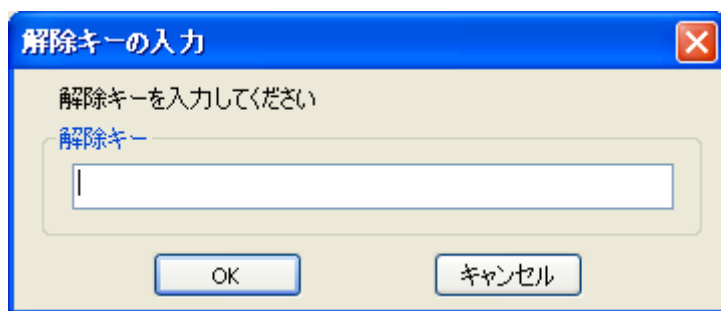
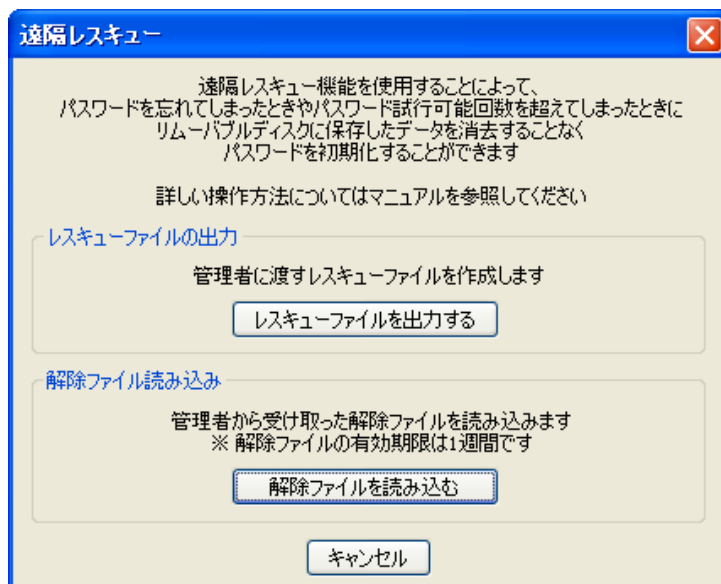
#### ④解除ファイル読み込み/パスワード初期化

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[遠隔レスキュー機能]をクリックします。

[解除ファイルを読み込む]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]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。

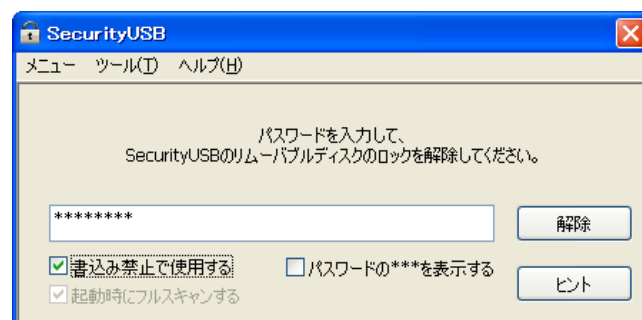


#### リムーバブルディスク領域への書き込みを禁止する

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。

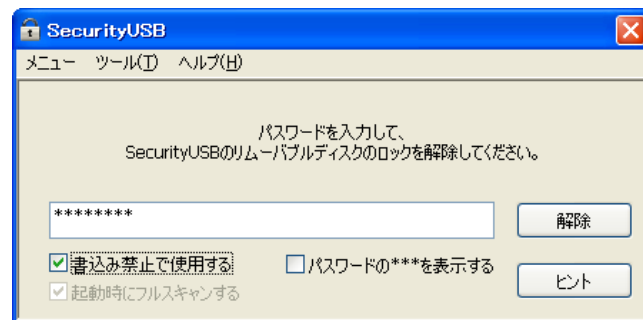




パスワードを入力し[解除]をクリックすると、リムーバブルディスク領域が書き込み禁止の状態が開きます。

※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

書き込み禁止を解除するには、次回のパスワード入力時に[書き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

本製品のマニュアルを参照することができます。

※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。

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。

※最新のマニュアルは Web ページをご確認ください。



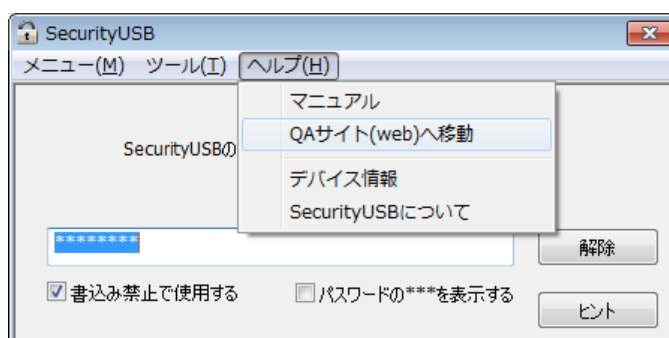
## Q&A サイト(web)へ移動

本製品の Q&A サイト(web)へ移動することができます。

※インターネットに接続できる環境が必要です。

※URL : [http://qa.elecom.co.jp/faq\\_list.html?category=404](http://qa.elecom.co.jp/faq_list.html?category=404)

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。





## 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。

本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：

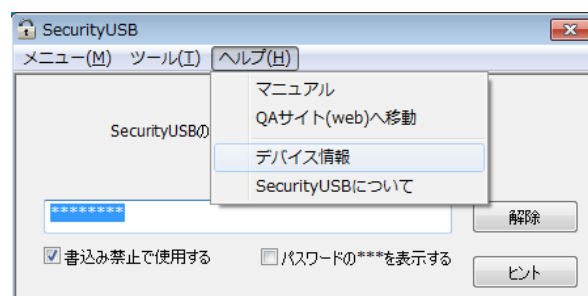
現在接続されているUSB 製品のUSB ベンダーID、USB プロダクトID、USB シリアル番号が表示されます。USB 製品を制限するシステム等にご使用ください。本製品は製品の性質上 PID を2つ持っております。システムへの2つのPID の登録をお願いします。

登録例：「VID：0x0693 、PID：0x0055/0x0056 USB、シリアル番号：0123456789012」の場合、以下の2つの情報をシステムへ登録してください。

- 登録 1:  
VID:0x0693  
PID:0x0055  
USB シリアル番号：0123456789012
- 登録 2:  
VID:0x0693  
PID:0x0056  
USB シリアル番号：0123456789012

※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。



## 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。

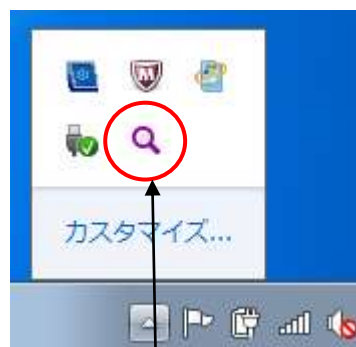





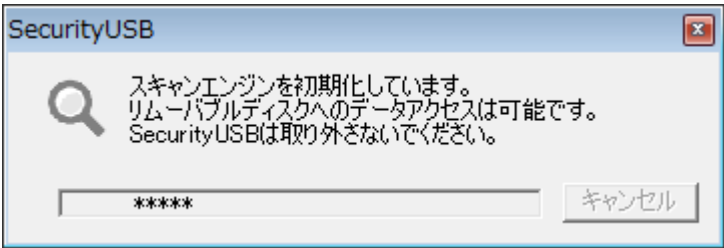

## ウイルススキャン機能

パスワードロックを解除するとウイルススキャンプログラムが起動し、本製品に対してのウイルス監視が開始されます。本製品を PC に接続するとタスクトレイにウイルススキャンプログラムの動作状態を示す右図のアイコンが表示されます。


以下にアイコンが示すウイルススキャンプログラムの状態について記載します。



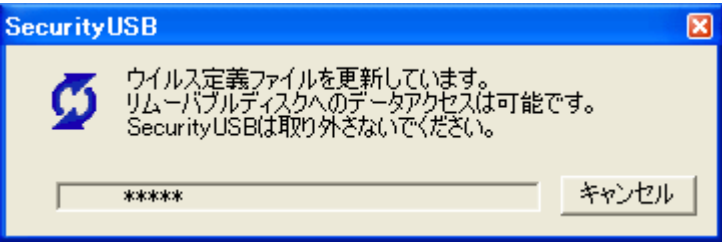

タスクトレイ上のアイコン

状態	アイコン表示	アイコンカラー	内容
ウイルススキャンプログラムの初期化中		黒	<p>ウイルススキャンプログラムの初期化を行っています。 初期化中には下記のポップアップが表示されます。</p> 
ウイルス定義ファイルの更新中		黒	<p>ウイルススキャンプログラムのウイルス定義ファイルの更新を行っています。 ウイルス定義ファイル更新中には下記のポップアップが表示されます。 ※タスクトレイ上のアイコンメニューからウイルス定義ファイルの更新を行った場合、下記のポップアップは表示されません。</p> 
本製品内ファイルをスキャン中		緑	本製品へ書き込まれたファイルをスキャンしています。
監視中		紫	本製品へ書き込まれるファイルを監視しています。



	<p>PC から本製品にファイルを書込む際にウイルススキャンを実行します。アイコン表示がどの状態でもファイルの書き込みは可能ですが、初期化中と更新中のときにファイルの書き込みを行った場合はウイルス定義ファイルの更新が完了するまでウイルススキャンは行われません。更新完了後にウイルススキャンを行います。</p> <p>※本製品は、PC に接続されるとウイルススキャンプログラムの初期化⇒ウイルス定義ファイルの更新⇒本製品内のウイルスチェック⇒本製品に書き込まれるファイルのウイルススキャン（監視）開始という順序でウイルススキャンプログラムが動作します。</p> <p>ご使用の環境により、本製品に書き込まれるファイルの監視が開始されるまでに時間がかかる場合がありますので、監視中のアイコンになるまでしばらくお待ちください。</p>
-----------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## ウイルス定義ファイルの更新

更新内容	更新方法	更新したファイルが有効になるタイミング
ウイルス定義ファイルの更新	<p>パスワードロック解除後にウイルススキャンプログラムが起動し、ウイルススキャンプログラムの初期化完了後にウイルス定義ファイルサーバにアクセス。ウイルス定義ファイルの更新を開始します。</p> <p>ウイルス定義ファイルサーバに新しいウイルス定義ファイルがあった場合、自動的に更新を行い、更新中は下記のウインドウが表示されます。</p> <p>※ウイルス定義ファイルの更新は、下記ウインドウで[キャンセル]をクリックすることでキャンセルすることができます。</p>  <p>また、ウイルススキャンプログラムのアイコン  のメニューから [ウイルス定義ファイルのアップデート] を選択することで、手動でウイルス定義ファイルの更新ができます。</p> <p>この場合、上記のウインドウは表示されません。</p>	更新直後

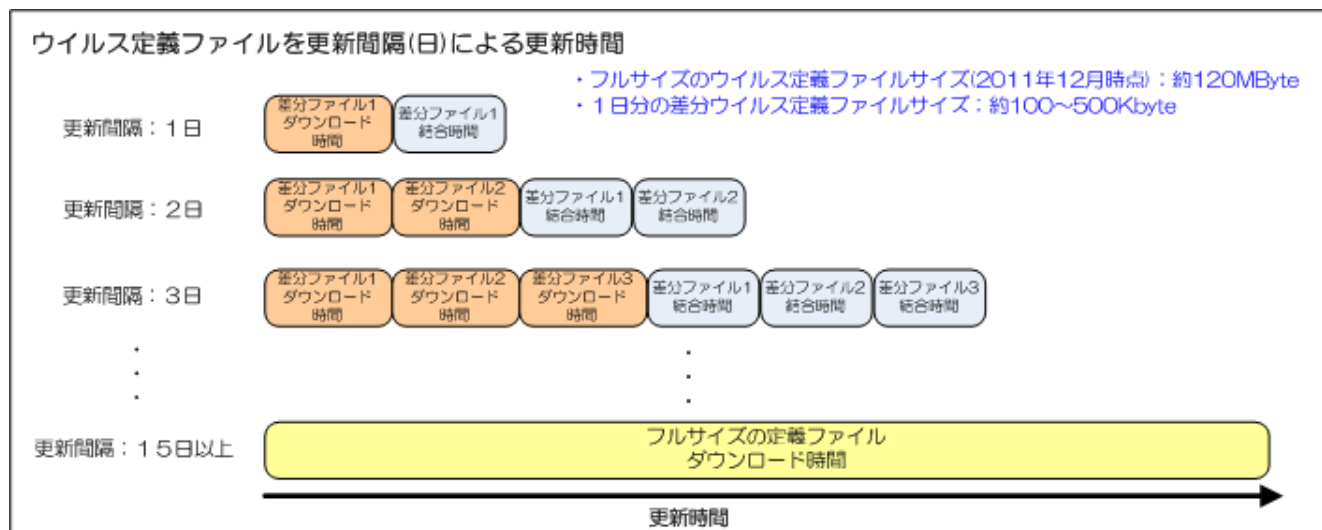
## ウイルス定義ファイルのダウンロード方式について

本製品ではウイルス定義ファイルのダウンロード方式に差分ダウンロード方式を採用しております。

この差分ダウンロード方式は、製品にダウンロードされているウイルス定義ファイルと新たにダウンロードするウイルス定義ファイルの差分だけをダウンロードする為、頻繁に本製品を使用することで、ダウンロードするファイルサイズが非常に小さく(約 100～500Kbyte)なり、ネットワーク回線速度が遅い環境でも短時間でダウンロードが完了します。

※ウイルス定義ファイルサーバのウイルス定義ファイルは1日に1回程度更新されます。





※15日以上ウイルス定義ファイルを更新していない場合は、フルサイズのウイルス定義ファイル(約120MB)をダウンロードします。

※差分ウイルス定義ファイル数が増えると結合時間が長くなり、ウイルス定義ファイルの更新に時間がかかる場合があります。

## ウイルスの検知

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。ウイルスに感染したファイルが検出されると右図のメッセージが表示され、ファイルを削除します。[閉じる]をクリックすると右図の画面を閉じます。ウイルス検知情報は、ログファイルで確認することができます。



## PC側のウイルスプロセスの検知

ウィルススキャンプログラム起動時にPC側で動作しているプロセスをスキャンします。

ウイルス感染しているプロセスがある場合、右図のメッセージが表示されますのでウイルス感染しているプロセスを停止する場合は[はい]を、停止しない場合は[いいえ]を押してください。



※ プロセスを停止することにより、PC側に問題が発生する可能性があります。

※ 本製品ではPC側のウイルス感染しているプロセスの削除は行いません。

プロセス停止後、PCの再起動等により、再度ウイルスが感染しているプロセスが動作する可能性があります。

※ ウィルス感染しているプロセスに対する処理結果はログに追記されます。





## ウイルスを起動させる Autorun.inf ファイル対策

USB メモリを経由して感染が広がるウイルスの挙動として、USB メモリのリムーバブルディスク領域に、ウイルスを起動させる 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、本製品のウイルススキャンプログラム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。




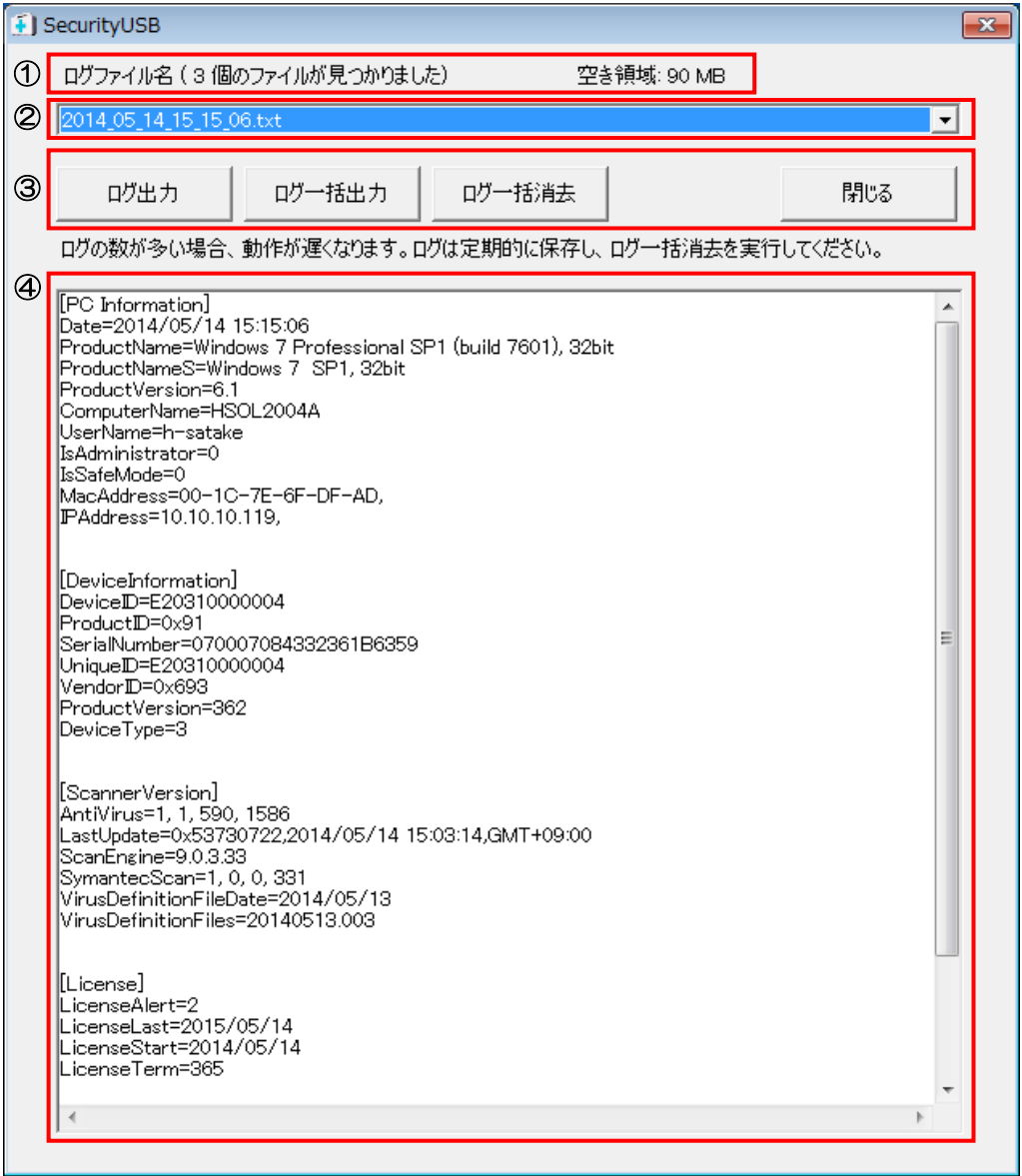
ログの閲覧方法

本製品を使用した PC 情報/デバイス情報/ウイルススキャンプログラム情報/ウイルス検知情報をログとしてデバイスへ保存します。

ログの収集は、ウイルススキャンプログラム起動後、自動的に行われます。

また、ログは OS から認識されない本製品の秘匿領域に保存されているため、誤って削除することはありません。

ログを閲覧するにはタスクトレイにある（紫）アイコンをクリックし、[ログフォルダを開く]を選択してください。



ログ閲覧画面説明

No	機能	内容
①	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領域を表示します。
②	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。
③	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。
	閉じる	ログ閲覧画面を閉じます。
④	ログ	選択されたファイルのログ内容を表示します。

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 サービスパックバージョン 例： Windows 7 Professional SP1 (build 7601), 32bit
ProductNameS	OS サービスパックバージョン（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：ScannerVersion ※起動時のウイルススキャンプログラムに関するセクション	
AntiVirus	アンチウイルスソフトバージョン 例： 1, 1, 0, 495
LastUpdate	最終更新日時 例： 0x4D0AAA59,2010/12/17 09:10:01,GMT+09:00
ScanEngine	スキャンエンジンバージョン 例： 5400.1158.353895558
McAfeeScan	アンチウイルスライブラリバージョン 例： 1, 0, 0, 111
VirusDefinitionFiles	ウイルス定義ファイルバージョン 例： 20111213.002
VirusDefinitionFileDate	ウイルス定義ファイルバージョン(日付) 例： 2011/12/13
セクション名：NewVersion* *：アップデート処理を行う度に 10 進で増加(例：1～10000～) ※ウイルス定義ファイルアプリのダウンロード結果	
AntiVirus	アンチウイルスソフトバージョン 例： 1, 1, 0, 502
LastUpdate	最終更新日時 例： 0x4D11D5B6,2010/12/22 19:40:54,GMT+09:00
SymantecScan	スキャンライブラリバージョン 例： 1, 0, 0, 111
ScanEngine	スキャンエンジンバージョン 例： 5400.1158.353895558
VirusDefinitionFiles	ウイルス定義ファイルバージョン 例： 20111213.002
VirusDefinitionFileDate	ウイルス定義ファイルバージョン(日付) 例： 2011/12/13
DefinitionPath	弊社管理情報
セクション名：UpdateDatResult* *：アップデート処理を行う度に 10 進で増加(例：1～) ※ウイルス定義ファイルのダウンロード結果	
TotalTime	アップデート時間 例： 198(s)
Result	アップデート結果 例： 0x0:Success




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 例： 0x29AA0025:Virus deleted
Result	ウイルススキャンの結果 例： 0x710F0003:KEY_AV_SUMMARY_INFECTED ※複数エラーがある場合は”,” 区切りで複数記載
InfectType	ウイルスの種類 例 Malware
Hash	ウイルスファイルの SHA1 ハッシュ 例： D27265074C9EAC2E2122ED69294DBC4D7CCE9141

セクション名：Error***      ***：スキャンにエラーがある毎に 10 進で増加(例：001～) ※ウイルススキャン時に失敗した場合の結果	
Path	ウイルスのフルパス 例： f:\eicar.zip
Result	ウイルススキャンの結果 例： 0x710F0003:KEY_AV_SUMMARY_INFECTED ※複数エラーがある場合は”,” 区切りで複数記載

セクション名：License ※ライセンス情報に関する情報	
LicenseAlert	ライセンス情報を表す情報 例 0：ライセンスが開始されていない状態 1：ライセンス有効期限切れ 2：ライセンス有効期限内（期限日から 90 日以上） 3：ライセンス有効期限内（期限日から 1 日～30 日以内） 4：ライセンス有効期限内（期限日から 31 日～90 日以内）
LicenseLast	ライセンス有効日 例：2015/12/26
LicenseStart	ライセンス開始日 例：2012/12/05
LicenseTerm	ライセンス日数 例：365
LicenseKey	更新ライセンス番号

 NOTE	<ul style="list-style-type: none"> <li>・スキャンログファイルは起動ごとに作成されます。</li> <li>・ウイルススキャンにより、ウイルスが発見されると[Virus***]の項目が追記されます。</li> <li>・ログ内容は予告無く変更される場合があります。</li> </ul>
-----------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------

## ウイルス定義ファイルの手動アップデート方法

タスクトレイにある （紫）アイコンをクリックし、  
[ウイルス定義ファイルのアップデート]をクリックします。  
ウイルス定義ファイルのアップデートが開始されます。

ログフォルダを開く
ウイルス定義ファイルのアップデート
セキュリティUSB内をスキャンする
ヘルプ
バージョン情報
終了 (取り外し)



## ヘルプ

本製品のマニュアルを参照することができます。

※ 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。


タスクトレイにある  (紫) アイコンをクリックし、  
[ヘルプ]をクリックします。

ログフォルダを開く  
ウイルス定義ファイルのアップデート  
セキュリティUSB内をスキャンする

ヘルプ  
バージョン情報  
終了 (取り外し)

## ウイルススキャンプログラムのバージョン情報/ライセンス有効期限の確認方法

本製品のバージョン情報/ライセンス有効期限を確認することができます。

タスクトレイにある  (紫) アイコンをクリックし、  
[バージョン情報]をクリックします。

- ①製品のバージョン
- ②ウイルス定義ファイルのバージョン (日付)  
ウイルススキャンエンジンのバージョン  
前回、ウイルス定義ファイルを更新した日付
- ③アクティベーション日  
ライセンス有効期限

ログフォルダを開く  
ウイルス定義ファイルのアップデート  
セキュリティUSB内をスキャンする

ヘルプ  
バージョン情報  
終了 (取り外し)





## ウイルススキャンプログラムのライセンスについて

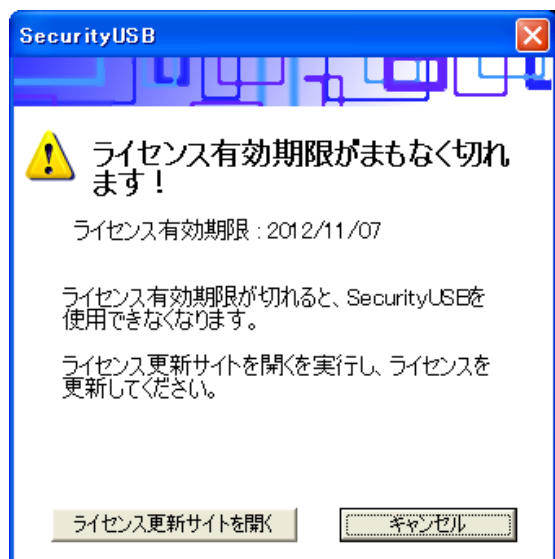
ウイルススキャンプログラムはライセンス製品です。初めてウイルス定義ファイルをアップデートした日からライセンスが有効になり、ライセンス期間内使用することができます。ライセンスが切れた場合、ウイルススキャンプログラムは起動しなくなります。

ライセンス有効期限はタスクトレイにあるアイコンをクリックすると表示されるメニューの[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 ヶ月前から起動毎に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[ライセンス更新サイトを開く]をクリックし、弊社ホームページでライセンス更新手順等の内容を確認頂き、ライセンスの更新を行なってください。有効期限が切れるまでは通常通り使用できます。

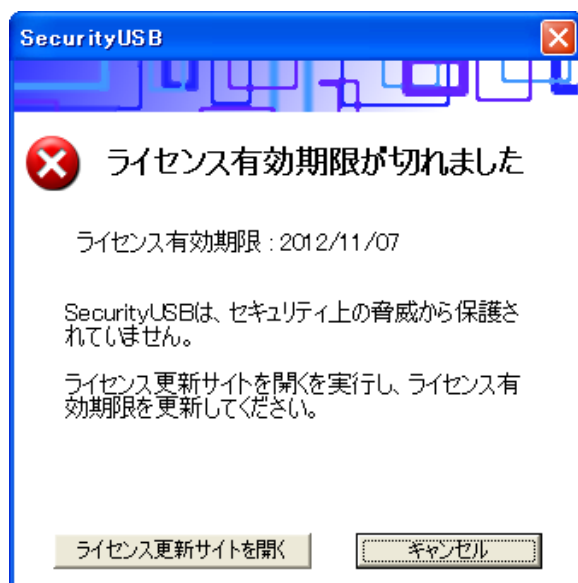


### ■ライセンス有効期限が切れた場合

ライセンス有効期限が切れた場合、ウイルススキャンプログラム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[ライセンス更新サイトを開く]をクリックし、弊社ホームページでライセンス更新手順の内容を確認頂き、ライセンスの更新を行なってください。



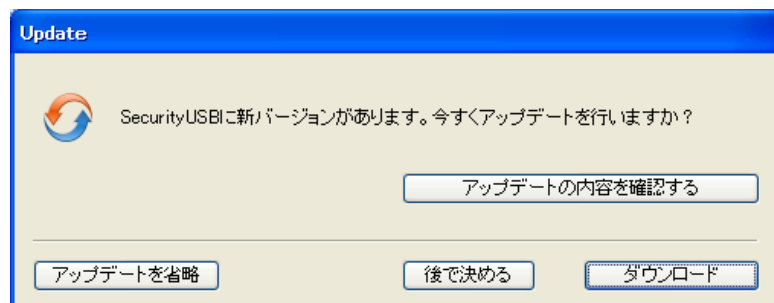


# ソフトウェアアップデート

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。

## 1. 本製品起動時に自動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

本製品起動時に自動でソフトウェアアップデート（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、Update 画面が表示されますので、処理を選択してください。



※本製品起動時に自動でソフトウェアアップデート（アップデート確認）を行わない場合は、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]を選択します。

「自動ソフトウェアアップデートの設定」で、「Security USB 起動時にソフトウェアアップデートを行う」のチェックを外してください。

## 2. 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、Update 画面が表示されますので、処理を選択してください。

※ソフトウェアのアップデートを行っても、リムーバブルディスク領域のユーザデータは削除されません。

※ソフトウェア アップデートはインターネットに繋がっている環境が必要です。

### ■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 Update 画面は表示されなくなります。

[アップデートを省略]を選択後に再度ソフトウェアアップデートを行う場合、次の操作を行ってください。

パスワード入力画面から「ツール」をクリックし[ソフトウェアアップデート確認]をクリックしてください。

ソフトウェアアップデート画面が表示されるので[ダウンロード]を選択してください。

### ■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]ボタンを押してください。

ソフトウェアアップデートを行わず、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。

### ■アップデートの内容を確認する

アップデート内容が記載してある WEB ページへ移動します。



## コピーガード機能有効時の動作について

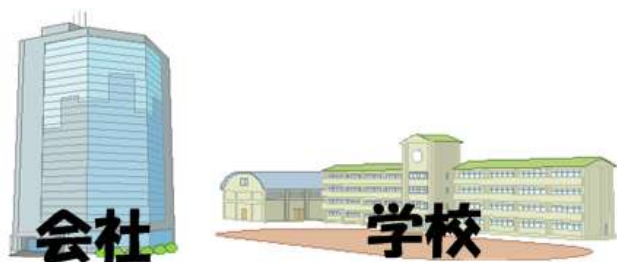
本製品は SecurityUSB Manager を使用し、コピーガード機能を有効にすることができます。

※コピーガードの運用開始方法については SecurityUSB Manager を管理している管理者にお問い合わせください。

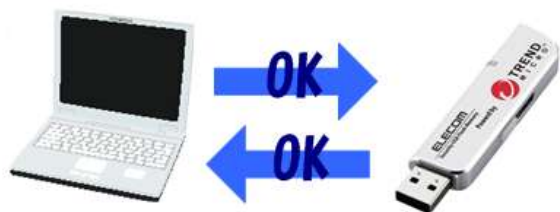
### コピーガード機能とは？

コピーガード機能とは自宅 PC 等で USB メモリ内のファイルを編集する際に、USB メモリ内のファイル操作を制限する機能です。USB メモリ内であればファイルの編集は可能なため、データの不正流出を防ぎ、社外での作業を可能にします。

ユーザ様の自宅でも仕事がしたいという要望と、管理者様のデータ流出を防ぎたいという要望にお応えします。



デバイスへ事前登録したPCではコピーガード機能が無効になり、通常のUSBメモリと同様にファイルの読み書きが可能です。



通常のUSBメモリの  
様に使用ができる



デバイスへ事前登録していないPCではコピーガード機能が有効になり、USBメモリのデータをUSBメモリ外にコピー/移動することはできません。USBメモリ内であればファイルの編集は可能なため、安全に職場の仕事が可能です



社外へのデータ流出  
の心配が無く、作業  
ができるから安心！



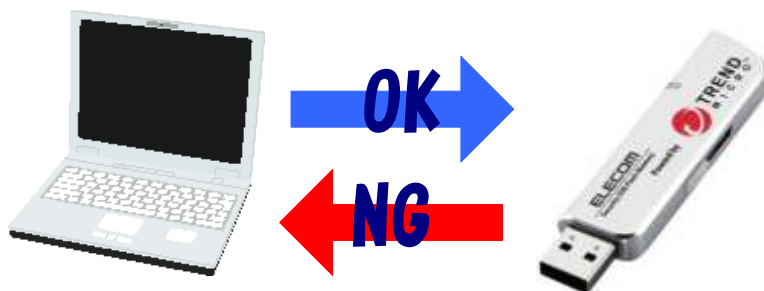
## コピーガード機能有効時の動作

コピーガードが有効な場合、本製品の動作が変わります。

### 1：許可されていないPC へのファイルコピー

コピーガードが有効な場合、許可されていないPC(自宅PC 等)へ USB 内のファイルをコピーすることができなくなります。USB 内であればファイルの編集は可能です。

**デバイスへ事前登録していないPCではコピーガード機能が有効になり、USBメモリのデータをUSBメモリ外にコピー/移動することはできません。USBメモリ内であればファイルの編集は可能なため、安全に職場の仕事が可能です**




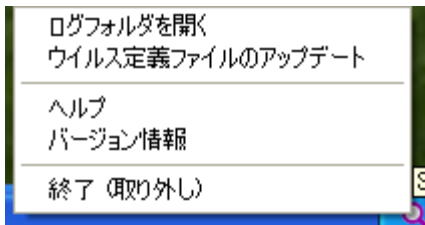
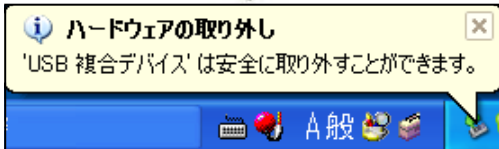
### 2：デバイス取り外し方法の変更

コピーガードが有効な場合、パスワードロック解除後 FogosPro というソフトウェアが起動し、タスクメニューへ常駐します。デバイスを取り外す時は FogosPro のタスクメニューの[終了]ボタンを選択してください。


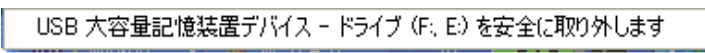
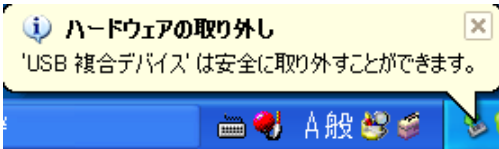



## 本製品の取り外し方法

### タスクトレイにがある場合

<p>タスクトレイにある（紫）アイコンを右クリックして、終了（取り外し）を選択します。</p> <p>右図のメッセージが表示されたら本製品を取り外してください。</p>	 
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### タスクトレイにが無い場合（書き込み禁止でを使用した場合）

<p>タスクトレイの「ハードウェアの安全な取り外し」アイコンをクリックします。</p> <p>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ます。</p> <p>右図のメッセージが表示されたら本製品を取り外してください。</p>	 
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------

 NOTE	<ul style="list-style-type: none"><li>・手順に従わずに本製品を取り外すと、データ破損及び故障の原因になります。</li><li>・本製品のリムーバブルディスク領域は、PC から取り外すとパスワードロックされます。PC から取り外さずに再起動/サスペンド/ユーザ切り替えを行うとパスワードロックがかからないことがあります。使用後は、必ず PC から取り外してください。</li></ul>
-----------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



質問	回答
<p>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。</p>	<p>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。</p> <p>※Windows Vista でオートラン機能を有効にするには以下の設定が必要となります。</p> <p>1. 「スタート」→「コントロールパネル」をクリックします。</p>  <p>2. 「ハードウェアとサウンド」から「CD または他のメディアの自動再生」をクリックします。</p>  <p>3. 「ソフトウェアとゲーム」より「プログラムのインストール／実行」を選択し、[ 保存 ] ボタンをクリックします。</p>  <p>以上でオートラン機能の設定は完了です。</p>



Q2	本製品を PC が認識しません。	A2	<p>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。</p> <p>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ク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。</p> <p>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。</p> <p>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。</p>
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	<p>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。</p> <p>※パスワードの文字数は 8～16 文字までです。</p> <p>※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。 ! # \$ % &amp; ' ( ) = ~   ` { + * } &lt; &gt; ? _ - ^ ¥ @ [ : ; , . /</p>
Q4	パスワードを忘れてしまいました。	A4	<p>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。</p> <p>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。</p> <p><b>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。</b></p> <p>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ってください。</p>
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	<p>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。</p>



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	本製品のウイルススキャンプログラムは 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	本製品のウイルススキャンプログラムは、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削除されます。
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	ウイルス定義ファイルはどのくらいの頻度で更新しますか？	A11	1 日 1 回程度です。
Q12	ウイルス定義ファイルの更新時間はどのくらいですか？	A12	更新間隔(日)、通信環境によりますが、更新間隔が1日、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	ウイルス定義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、ウイルス定義ファイルのダウンロードに時間がかかる場合があります。待機状態になるまでしばらくお待ちください。
Q14	本製品を PC 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	パスワードは Windows で設定したパスワードと共通ですか？	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](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) ライセンス期間	HUD-PUVM3**GM1 : 1 年 HUD-PUVM3**GM3 : 3 年 HUD-PUVM3**GM5 : 5 年 ※ハードウェア本体の保証期間は、本製品納品日起算となります。
-------------------------------	--------------------------------------------------------------------------------------------------------

### お問合せ窓口

ご連絡先		受付
サポートセンター※	TEL : 0570-080-900	9:00~19:00 (年中無休)

※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。ハギワラソリューションズ株式会社ホームページ : <http://www.hagisol.co.jp>

### 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てください。

- ◆掲載されている商品の仕様・外観、およびサービス内容等については、予告なく変更する場合があります。あらかじめご了承ください。
- ◆Microsoft 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。
- ◆その他掲載されている会社名・商品名等は、一般に各社の商標又は登録商標です。なお、本文中には®および ™ マークは明記しておりません。
- ◆本ドキュメント内容は、2015 年 2 月 19 日時点のものです。今後、当該内容は予告なく変更される場合があります。

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](http://www.7-zip.org)

License for use and distribution

7-Zip Copyright (C) 1999-2013 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: HUD-PUVM3\*\*GM\*  
 Windows マニュアル  
 2015 年 2 月 19 日