

SecurityUSB Manager

型番：HUD-SUMA

マニュアル

この度は SecurityUSB Manager (以下、本ソフトウェア) 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ソフトウェアの導入から使用方法までを説明しています。本ソフトウェアを正しくご利用いただくために、使用開始前に、必ずこのマニュアルを必ずお読みください。

1 ソフトウェア使用許諾契約書

本契約は、お客様（以下「お客様」とします）とハギワラソリューションズ株式会社（以下「弊社」とします）との間で弊社がお客様へ提供するソフトウェア（以下「許諾ソフトウェア」とします）の使用権許諾に関して次のように条件を定めます。

弊社は、お客様に対して、以下の条件に従って許諾ソフトウェアの使用を許諾いたします。お客様は、本契約書の内容をしっかりとお読みになり、本契約書の内容に同意できる場合に限り、お客様の責任で許諾ソフトウェアを使用してください。許諾ソフトウェアを使用することによって、お客様は本契約の各条項に同意したものとみなされます。本契約の各条項に同意されない場合、弊社はお客様に対し、許諾ソフトウェアのご使用を許諾できません。

第1条（総則）

許諾ソフトウェアは、日本国内外の著作権及びその他知的財産権に関する諸法令及び諸条約によって保護されています。許諾ソフトウェアは、本契約の条件に従い弊社からお客様に対して使用許諾されるもので、許諾ソフトウェアの著作権等の知的財産権は弊社に帰属し、お客様に移転いたしません。

第2条（使用権）

1. 弊社は、許諾ソフトウェアの非独占的な使用権をお客様に許諾します。
2. 本契約によって生ずる許諾ソフトウェアの使用権とは、お客様が取得または購入された許諾ソフトウェアがインストールされている電子機器上において、許諾ソフトウェアをお客様の機器等に対して使用する権利をいいます。
3. お客様は、許諾ソフトウェアの全部又は一部を複製、複写、並びに、これに対する修正、追加等の改変をすることができません。

第3条（権利の制限）

1. お客様は、許諾ソフトウェアを再使用許諾、譲渡、貸与又はリースその他の方法で第三者に使用させてはならないものとします。
2. お客様は、許諾ソフトウェアを用いて、弊社又は第三者の著作権等の権利を侵害する行為を行ってはならないものとします。
3. お客様は、許諾ソフトウェアに関しリバースエンジニアリング、逆アセンブル、逆コンパイル等のソースコード解析作業を行ってはならないものとします。
4. お客様は、本契約に基づいて、許諾ソフトウェアがインストールされている電子機器と一体としてのみお客様の許諾ソフトウェアに関する権利の全てを、譲受人が本契約の条項に同意することを条件に譲渡することができます。但しその場合、お客様は許諾ソフトウェアの複製物を保有することはできず、許諾ソフトウェアの一切（全ての構成部分、媒体、電子文書及び本契約書を含みます）を譲渡しなければなりません。

第4条（許諾ソフトウェアの権利）

許諾ソフトウェアに関する著作権等一切の権利は、弊社または、本契約に基づきお客様に対して使用許諾を行うための権利を弊社に認めた原権利者（以下原権利者として）に帰属するものとし、お客様は許諾ソフトウェアに関して本契約に基づき許諾された使用权以外の権利を有しないものとします。

第5条（責任の範囲）

1. 弊社及び原権利者は、第6条2項に定義するアップデートデータが正常にインストールできることを保証いたしません。また、弊社及び原権利者は、当該アップデートデータのインストールによってお客様に損害が発生しないことを保証いたしません。
2. 弊社及び原権利者は、許諾ソフトウェアにエラー、バグ等の不具合がないこと、若しくは許諾ソフトウェアが中断なく稼動すること又は許諾ソフトウェアの使用がお客様及び第三者に損害を与えないことを保証しません。また、弊社及び原権利者は、許諾ソフトウェアが第三者の知的財産権を侵害していないことを保証いたしません。
3. 許諾ソフトウェアの稼動が依存する、許諾ソフトウェア以外の製品、ソフトウェア又はネットワークサービス（第三者が提供する場合に限りならず、弊社又は原権利者が提供する場合も含みます）は、当該ソフトウェア又はネットワークサービスの提供者の判断で中止又は中断する場合があります。弊社及び原権利者は、許諾ソフトウェアの稼動が依存するこれらの製品、ソフトウェア又はネットワークサービスが中断なく正常に作動すること及び将来に亘って正常に稼動することを保証いたしません。
4. お客様に対する弊社及び原権利者の損害賠償責任は、当該損害が弊社又は原権利者の故意又は重過失による場合を除きいかなる場合にも、お客様に直接且つ現実に生じた通常の損害に限定され且つお客様が証明することのできる許諾ソフトウェアの購入代金を上限とします。
5. 弊社又は原権利者は、債務不履行及び不法行為等の理由の如何にかかわらず、如何なる場合においても、お客様に生じた逸失利益、結果的損害、間接損害、若しくは、データ消失及び破損における損害については、一切賠償する責を負わないものとする。
6. 弊社は、弊社ウェブページにて定めるお問合わせ窓口（許諾ソフトウェア購入ページからリンクしてご確認ください。）に限り、お客様が弊社から使用許諾を受けた許諾ソフトウェアに関する技術的サポートを提供します。但し、弊社は、お客様の同意を得ることなく、当該窓口の受付時間及び当該サポートの提供の有無について随時変更することができるものとします。なお、弊社は、お客様との間で、別途契約を締結しないかぎり、当該サポートをお客様に提供及び継続する義務を一切負うことはありません。

第6条（著作権保護及び自動アップデート）

1. お客様は、許諾ソフトウェアの使用に際し、日本国内外の著作権及びその他知的財産権に関する諸法令及び諸条約に従うものとします。
2. お客様は、弊社又は弊社の指定する第三者がウェブ上に、許諾ソフトウェアのセキュリティ機能の向上、エラーの修正、アップデート機能の向上等の目的で許諾ソフトウェアが適宜にアップデートデータ（以下「アップデートデータ」とします）を公開する場合は、アップデートデータ公開後 90 日以内に許諾ソフトウェアをアップデートしなければなりません。また、お客様は、アップデートデータ公開後 90 日を経過した場合は、旧許諾ソフトウェアを、アップデートをする目的以外で使用することができません。お客様は、(i)当該許諾ソフトウェアのアップデートに伴い、許諾ソフトウェアの機能が追加、変更又は削除されることがあること、及び(ii)アップデートされた許諾ソフトウェアについても本契約が適用されることに同意するものとします。

第7条（契約の解約）

1. 弊社は、お客様が本契約に定める条項に違反した場合、直ちに本契約を解約することができるものとします。
2. 前項の規定により本契約が終了した場合、お客様は契約の終了した日から 2 週間以内に許諾ソフトウェアの全てを廃棄するか、弊社に対して返還するものとします。お客様が許諾ソフトウェアを廃棄した場合、直ちにその旨を証明する文書を弊社に差し入れるものとします。
3. 本条 1 項の規定により本契約が終了した場合といえども、第 4 条、第 5 条、第 7 条第 2 項及び第 3 項並びに第 8 条第 1 項及び第 3 項乃至第 5 項の規定は有効に存続するものとします。

第8条（その他）

1. 本契約は、日本国法に準拠するものとします。
2. お客様は、許諾ソフトウェアを国外に持ち出して使用する場合は、適用ある条例、法律、輸出管理規制、命令に従うものとします。
3. 本契約に関連する一切の紛争については、弊社本店所在地の地方裁判所または簡易裁判所を第一審の専属管轄裁判所とします。
4. 本契約の一部条項が法令によって無効となった場合でも、当該条項は法令で有効と認められる範囲で依然として有効に存続するものとします。
5. 本契約に定めなき事項又は本契約の解釈に疑義を生じた場合は、お客様及び弊社は誠意をもって協議し、解決するものとします。
6. 本書の内容について、その正確性または完全性等について保証を行うものではありません。掲載内容については細心の注意を払っておりますが、万一、これらの情報に誤りがあっても、弊社は、一切責任を負いかねます。

2 同梱品の確認

本ソフトウェアのパッケージには、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。

- | | |
|---|------|
| <input type="checkbox"/> CD-ROM(SecurityUSB Manager Software 同封) ※1 | ×1 枚 |
| <input type="checkbox"/> シリアル番号用紙 | ×1 枚 |

※1：本 CD-ROM 内には次のソフトウェアが格納されております。

- SecurityUSB Manager
 - Local Updater(ウイルス対策 USB HUD-PUVS**GM*シリーズ用)
 - Local Updater(ウイルス対策 USB HUD-PUVM**GM*/H-PMPH***TM*シリーズ用)
- ※Local Updater につきましては LocalUpdater のマニュアルをご確認ください。

[重要]

コピーガード設定ソフトは ICManager は、SecurityUSB Manager へ組み込まれました。

コピーガードについてはタブ：実行制限/コピーガードにて設定できます。

それに伴い、ICManager for Device ライセンス ID 証書を同封しておりません。

3 本ソフトウェアについて

本ソフトウェアは、ウイルス対策 USB シリーズとセキュリティ HDD、パスワードロッカー（以下、対象デバイス）のパスワードポリシー設定、デバイスログ管理を行うためのシステム管理者用ソフトウェアです。

本ソフトウェアでできること

■ パスワードポリシー

- ・ ユーザによるパスワード変更の制限
- ・ ユーザによるパスワードヒント登録の制限
- ・ ユーザによるデバイスの初期化の制限
- ・ パスワードの最小登録文字数の設定（標準設定：8 文字）
- ・ パスワードのアルファベット 最小使用文字数設定（標準設定：0 文字）
- ・ パスワードの数字 最小使用文字数設定（標準設定：0 文字）
- ・ パスワードの記号 最小使用文字数設定（標準設定：0 文字）
- ・ パスワード再入力許可回数設定（標準設定：5 回）
- ・ 初期パスワード/ヒント登録
- ・ 初期パスワードの強制変更
- ・ パスワードの有効期間の設定
- ・ パスワード認証超過失敗時の強制デバイス初期化設定
- ・ 過去に登録したパスワードの再登録制限
- ・ 24時間以内のパスワード変更可能回数制限
- ・ パスワードロック機能の無効化
- ・ パスワード解除後のリムーバブルディスク画面表示

■ ネットワーク

- ・ ウイルス定義ファイルダウンロード方法設定

■ ウイルスソフト

- ・ ユーザによる起動時のウイルスチェック範囲設定
- ・ ウイルス検出時にウイルス削除の禁止設定
- ・ ユーザによるウイルス検出時の処理の設定変更制限
- ・ 自動ソフトウェアアップデートの表示制限
- ・ ウイルススキャンソフトのライセンス更新表示制限
- ・ ユーザによるログ閲覧・削除制限
- ・ ライセンス更新ページ(URL)設定変更
- ・ 製品初期化時の定義ファイル復旧設定
- ・ ウイルススキャン初期化中の進捗画面表示設定
- ・ 非通知ソフトウェアアップデート
- ・ プロキシ設定

■ デバイス

- ・ デバイスのリムーバブルディスク領域のボリュームラベル設定
- ・ デバイスの USB のプロダクトストリング設定
- ・ デバイスへのファイル書き込み制限(読み取り専用デバイス化)
- ・ 使用 WindowsOS 制限
- ・ MacOS X 使用設定
- ・ 貸し出し期限設定(有効期限再設定ソフトウェア追加)

■ 追加ファイル

- ・ デバイスの CD-ROM 領域/リムーバブルディスク領域へのファイル追加
- ・ パスワードロック解除時の自動実行ファイルの設定
- ・ リムーバブルディスク容量の変更
- ・ セキュリティ USB/HDD の実行制限設定

■ 特殊

- ・ 遠隔地にいるユーザが持っているデバイスのデータ救出(レスキューファイル/レスキュー番号)
- ・ 管理者の手元にあるデバイスのデータ救出
- ・ デバイス内のログ収集

■ 実行制限/コピーガード/操作ログ

- ・ コピーガード/実行制限の設定(自動パスワード解除・使用 PC 制限機能の設定)
- ・ ファイル操作/印刷ログ取得設定

■ ログ送信

- ・ Info Banker へのログ送信設定
※パスワードロッカーはウイルス検知ログの送信非対応
- ・ 機密情報送信設定
- ・ 認証付きログ機能

■ 配信

- ・ 遠隔消去設定

■ デバイス情報

- ・ デバイス情報の確認とコメントの設定

■ その他

- ・ 設定ファイルの出力、設定ファイルの読み込み
- ・ 遠隔設定 TOOL の出力
- ・ 認証キーの非表示機能

■ クラウド管理設定

■ セキュリティ SSD シリーズ(LMD-PBLxxxU3BS/ESD-PLxxxxGM) へ対応 **New!**

各製品によって本ソフトウェアでカスタムできる項目が異なります。
各製品の対応機能について別紙：[Function_Support.pdf](#) に記載しております。

製品仕様

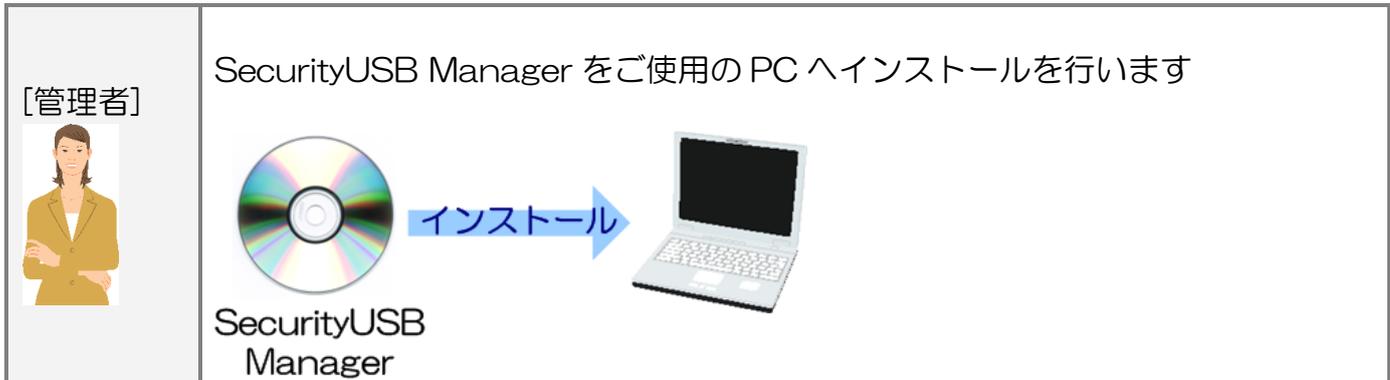
USB インターフェース	USB1.1 (Full Speed)/USB 2.0 (High Speed/Full Speed) USB3.0(Super Speed)
動作環境*1*2	USB インターフェース(USB2.0 必須)を搭載した DOS/V 機器 Pentium4 1.4GB 以上の CPU 物理空きメモリ容量 512MByte 以上 ハードディスク空き容量 500MB 以上
対応 OS	Windows10 Windows11 ※日本語 OS 場合、日本語表示になります。 ※日本語 OS 以外の場合、英語表示になります。
対応ユーザアカウント	コンピュータの管理者 (Administrator) ※制限ユーザには対応していません
対象デバイス	<ul style="list-style-type: none"> • USB2.0 版ウイルス対策 USB MF-PUVT**GM*シリーズ • USB2.0 版ウイルス対策 USB HUD-PUVS**GM*シリーズ • USB2.0 版ウイルス対策 USB HUD-PUVM**GM*シリーズ • USB2.0 版パスワードロッカー(HUD-PL**GM) シリーズ • USB3.0 版ウイルス対策 USB MF-PUVT3**GM*シリーズ • USB3.0 版ウイルス対策 USB HUD-PUVS3**GM*シリーズ • USB3.0 版ウイルス対策 USB HUD-PUVM3**GM*シリーズ • USB3.0 版パスワードロッカー(HUD-PL3**GM) シリーズ • パスワードロッカーHDD シリーズ(H-PLPH***TM*) • セキュリティ HDD Model-M シリーズ(H-PMPH***TM*) • セキュリティポータブル HDD(ELP-S***T*) • セキュリティ対策用外付け SSD(ESD-PLxxxxGM) • 暗号化機能付き外付け SSD(LMD-PBLxxxU3BS)

*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。

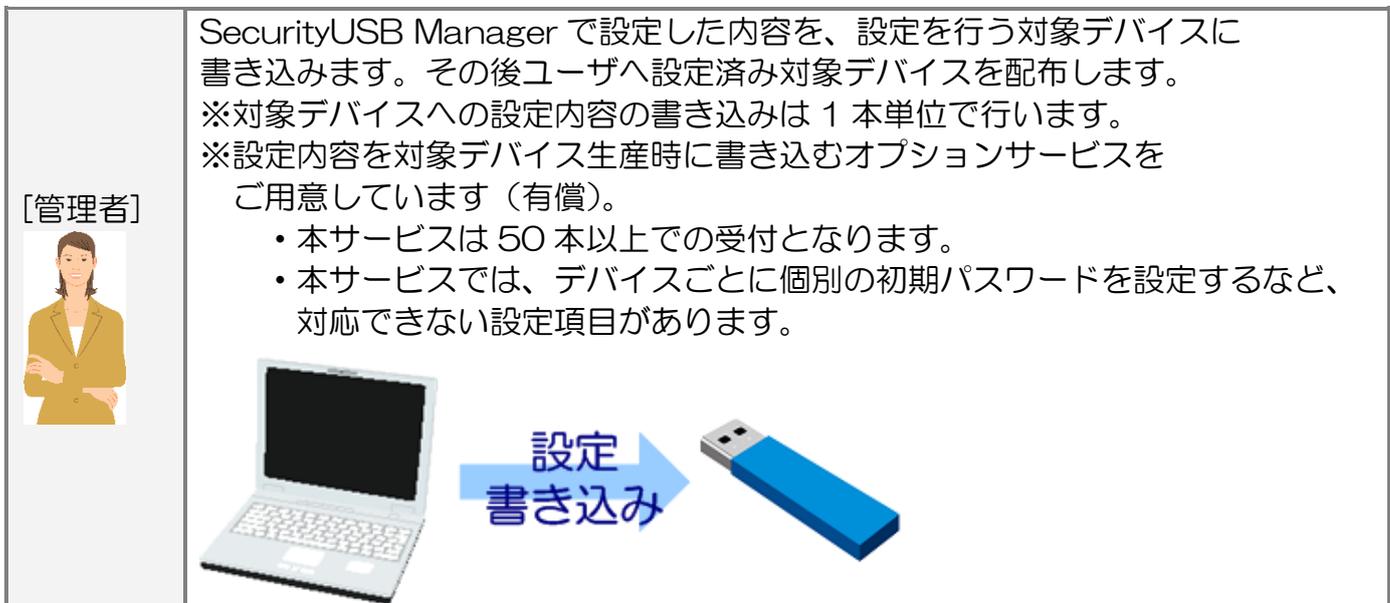
*2 USB Mass Storage Class ドライバ、HID Class ドライバ、CD-ROM ドライバがあらかじめ組み込まれている必要があります。

4 セットアップから運用開始までの流れ

<セットアップ>



<運用>



5 ご使用方法

本章では、本ソフトウェアの使用方法などを説明しております。

SecurityUSB Manager のインストール

CD-ROM のフォルダ [SecurityUSB Manager] 内にインストーラファイル「setup.exe」があります。
「setup.exe」を実行し、画面の指示に従い PC へ SecurityUSB Manager をインストールしてください。
インストール途中にシリアル番号入力画面が表示されますので、同封のシリアル番号用紙に記載されているシリアル番号を入力してください。

デバイス認証（対象デバイスへの認証キー登録・認証）

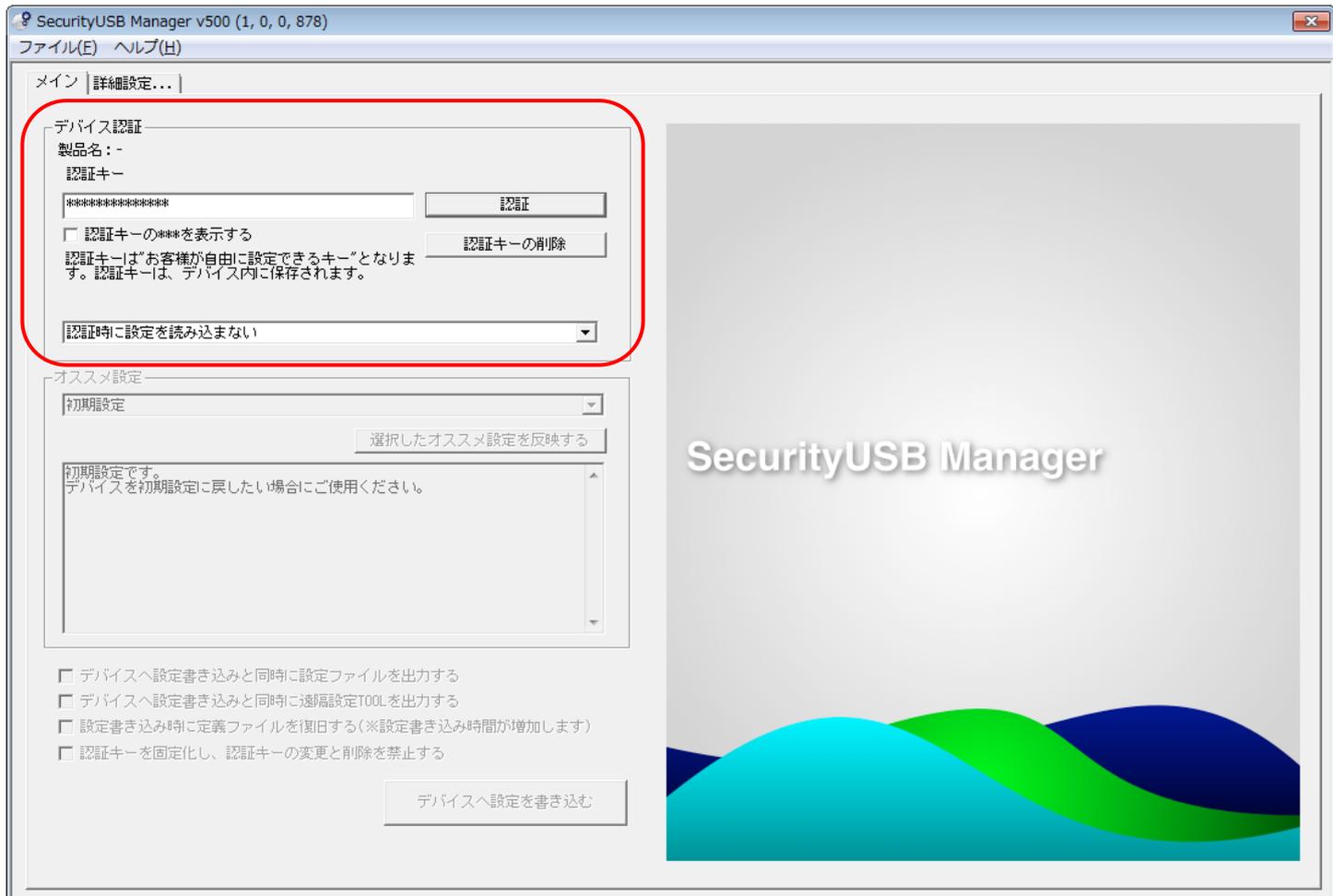
本ソフトウェアを使用し、対象デバイスへ設定を行う場合、始めに認証キーを対象デバイスに登録する必要があります。

登録した認証キーで認証処理を行うことで、設定の書き込みや対象デバイスからのデータ救出（パスワードのリセット）が可能になります。

認証キーは”お客様が自由に決定できるキー”となります。

推測されにくく、他のお客様と被らないような認証キーをご使用ください。

1.本ソフトウェアを起動し、タブ[メイン]を開いてください。



2.対象デバイスを PC に接続してください。

3.認証キーの登録/認証/認証キーの削除

○対象デバイスへ認証キーが未登録の場合

認証キーを決定し、認証キー入力欄へ認証キーを入力して[認証]ボタンをクリックしてください。

認証キーが対象デバイスへ登録され、対象デバイスへの設定が可能になります。

※認証キーを表示させたい場合は[認証キーの***を表示する]へチェックを入れてください。



本処理を行うと、対象デバイス内のパスワード、ヒント、設定、デバイス内のデータが初期化されます。解除される恐れのあるような簡単な認証キーを設定しないように注意してください。

○対象デバイスへ認証キーが登録済みの場合

登録済みの認証キーを入力欄へ入力し、[認証]ボタンを押してください。

認証キーが一一致した場合、対象デバイスへの設定が可能になります。

○対象デバイスから認証キーを削除する場合

[認証キーの削除]ボタンを押してください。



本処理を行うと、対象デバイス内のパスワード、ヒント、設定、デバイス内のデータが初期化されます。

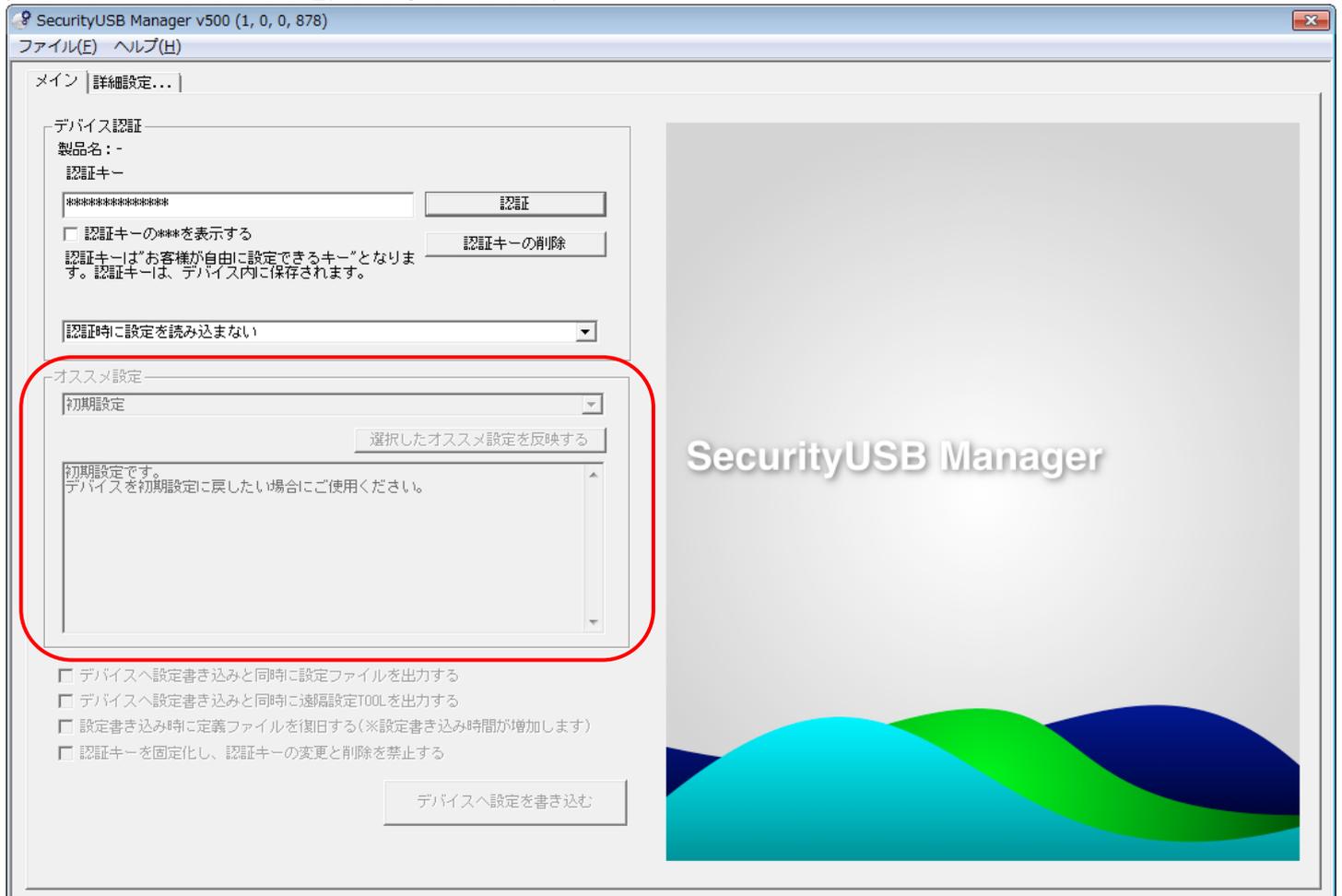
■設定読み込み機能

認証成功時に設定を読み込み、反映する機能があります。

設定	内容
認証時に設定を読み込まない	認証時に設定を読み込みません。設定項目へは初期値を反映します。 設定項目は維持されますので、同じ設定を複数の対象に連続で書き込む場合はこちらを選択してください。
認証時にデバイスの設定を読み込む	認証時に現在デバイスに書き込まれている設定を読み込み、設定項目へ反映します。
認証時に前回書き込んだ設定を読み込む	認証時に前回 SecurityUSB Manager が書き込んだ設定を読み込み、設定項目へ反映します。設定は自動保存されます。
認証時に設定ファイルを読み込む	認証時に設定ファイルを読み込み、設定項目へ反映します。 ※設定ファイル保存はデバイス書き込み時に[設定ファイルを出力する]へチェックを入れて行ってください。 ※認証キーが一致しない設定ファイルは読み込むことができません。

オススメ設定

弊社がオススメする設定を選択することができます。



オススメ設定をプルダウンメニューから選択し、[選択したオススメ設定を反映する]ボタンをクリックすると、本ソフトウェアに選択したオススメ設定が反映されます。

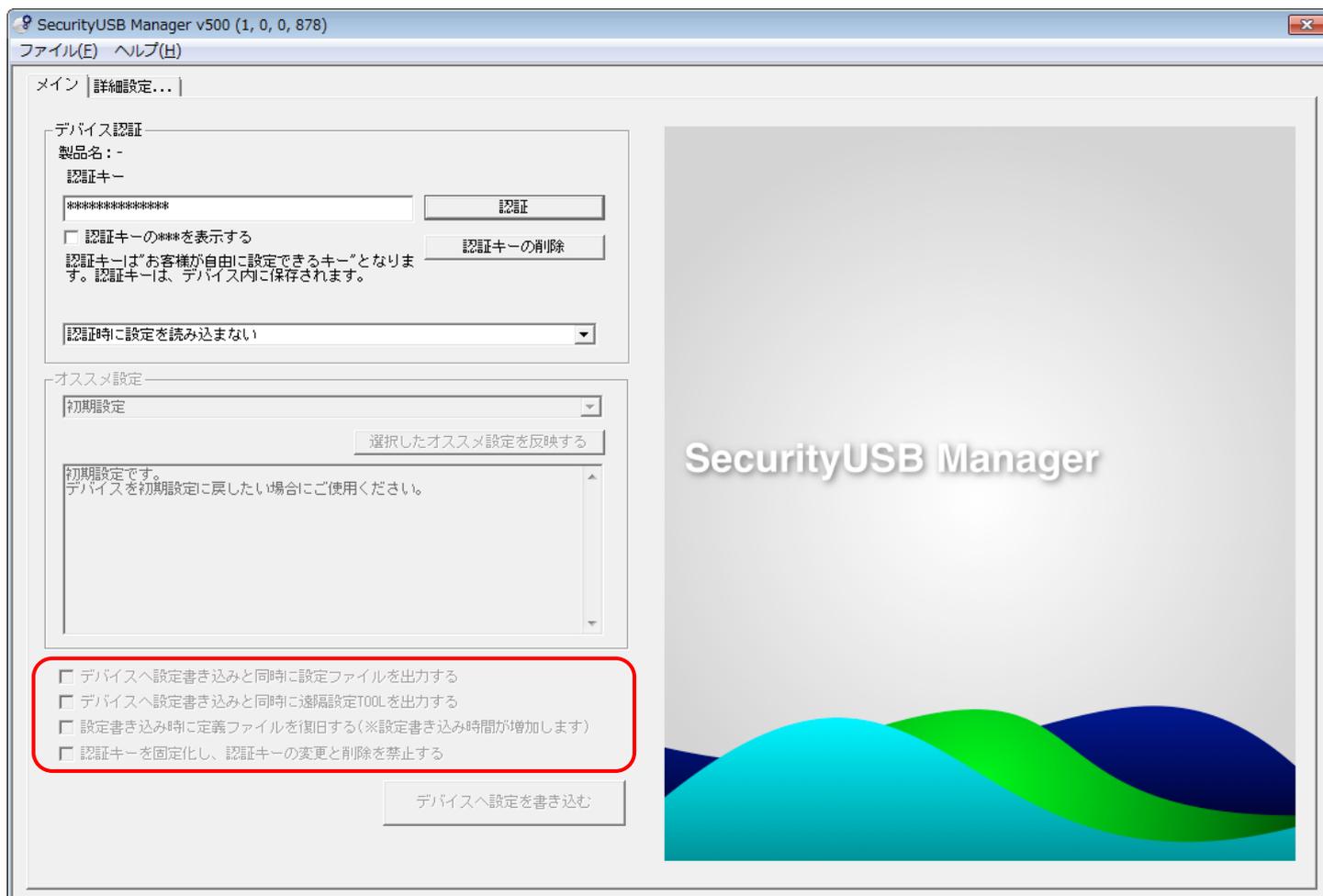
オススメ設定一覧

オススメ設定	内容
パスワード強固デバイス設定	パスワードを強固に設定し、紛失時のリスクを減らす設定です。 パスワードへ数字、記号を各1文字入力必須、30日毎に強制パスワード変更など、パスワードを強固にします。
貸し出し用デバイス設定	デバイスを貸し出す場合に最適な設定です。 30日間の使用制限により、サンプル貸し出し等に利用できます。
コンテンツ配布用デバイス設定	お客様のコンテンツ、ファイルを配布する時に最適な設定です。 書き込みが一切できないので、データの改ざんなどの心配がありません。
管理者ラクラクデバイス設定	管理者のユーザ管理を軽減する設定です。 ユーザがパスワードを忘れた場合のユーザデータの救出など、管理者のユーザサポート負荷を減らす設定になっています。
ウイルス持ち運びデバイス設定	ウイルスファイルであっても削除せずに持ち運びデバイス設定です。 証拠データなど、ウイルスファイルであっても持ち運ぶ必要がある場合にご使用ください。
初期設定	弊社の標準の設定です。 デバイスを初期設定に戻したい場合にご使用ください。

デバイスへ設定を書き込む

本ソフトウェアで設定した内容を対象デバイスへ書き込みます。

対象デバイスへの書き込みと同時に「設定ファイルの出力」、「遠隔設定 TOOL 出力」を行うことができます。



項目	内容
デバイスへ設定を書き込む	<p>本ソフトウェアで設定した内容を対象デバイスへ書き込みます。</p> <p>[設定方法]</p> <p>本ソフトウェアで各種設定を行い、「デバイスへ設定を書き込む」ボタンをクリックすると対象デバイスへ設定が書き込まれます。</p> <p> ご注意!</p> <p>本処理を行うと、対象デバイス内のパスワード、ヒント、設定、デバイス内のデータが初期化されます。</p>

<p>デバイスへ設定書き込みと同時に設定ファイルを出力する</p>	<p>本ソフトウェアで設定した内容を、設定ファイルおよび画面キャプチャとして保存することができます。</p> <p>以後、その設定ファイルを読み込むことで設定を反映することが可能になります。</p> <p> 設定ファイルを読み込むには、設定ファイル出力時と同じ認証キーが必要です。</p> <p>設定ファイル格納フォルダ；MpSUM***** *：日時情報 設定ファイル名：MpSUM.sum</p> <p>画面キャプチャフォルダ：png</p> <p>[設定方法] 「デバイスへの書き込みと同時に設定ファイルを出力する」へチェックを入れ、「デバイスへ設定を書き込む」ボタンをクリックします。</p>
<p>デバイスへ設定書き込みと同時に遠隔設定 TOOL を出力する</p> <p>※リムーバブルディスク・ドライブ+リムーバブルディスク・ドライブのデバイス構成 非対応項目</p>	<p>遠隔にいるユーザが持っている対象デバイスの設定を変更するソフトウェア「遠隔設定 TOOL」を出力します。そのソフトウェアをユーザへ渡し、実行するとユーザの手元で対象デバイスの設定を変更できます。</p> <p>注意：遠隔設定 TOOL は同じ認証キーを持つ対象デバイスに対してのみ使用できません。</p> <p>遠隔設定 TOOL ファイル格納フォルダ；SUMLite***** *：時刻情報 遠隔設定 TOOL ファイル名：SUM_Lite.exe/ Hagiwara_SDK_63.dll 等</p> <p>[設定方法] 「デバイスへの書き込みと同時に遠隔設定 TOOL を出力する」へチェックを入れ、「デバイスへ設定を書き込む」ボタンをクリックします。</p>
<p>設定書き込み時に定義ファイルを復旧する (※設定書き込み時間が増加します)</p>	<p>設定書き込みを行うと USB メモリ上から定義ファイルは削除されます。そのため次回ユーザが対象デバイスを使用してパスワード解除を行うと定義ファイルの復旧が始まります。</p> <p>デバイスへ設定書き込みと同時に定義ファイルを書き込み、初回定義ファイルの復旧を行わない設定を行うことができます。</p> <p>[設定方法] 「設定書き込み時に定義ファイルを復旧する」へチェックを入れ、「デバイスへ設定を書き込む」ボタンをクリックします。</p>

<p>認証キーを固定化し、認証キーの変更と削除を禁止する</p>	<p>この設定を有効にして書き込みを行った場合、以降の使用において認証キーの変更と削除ができなくなります。</p> <p>この設定を有効にするとセキュリティ USB の PID が変更されます。</p> <p>PC 側のシステム (SKYSEA Client View 等) で USB メモリの制限に VID, PID を使用している場合はシステム側の変更が必要です。</p> <p>次ページに各セキュリティ USB の VID, PID を記載します。</p>
----------------------------------	--

各セキュリティ USB/HDD の VID/PID について

各セキュリティ USB/HDD(管理者用ソフト対応モデル)の VID/PID について以下に記載します。

セキュリティ USB は PID を 2 つ持っている製品になります。

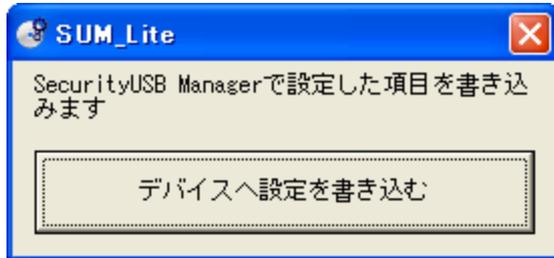
セキュリティ HDD は PID を 1 つ持っている製品になります。

製品	標準 VID/PID	認証キー固定後の VID/PID
USB3.0 版対応セキュリティ機能付き USB フラッシュメモリ (トレンドマイクロエディション/管理者用ソフト対応モデル)1 年モデル 型番: MF-PUVT3**GM1	VID:0x056E PID:0x6806/0xe806	VID:0x056E PID:0x6906/0xe906
USB3.0 版対応セキュリティ機能付き USB フラッシュメモリ (トレンドマイクロエディション/管理者用ソフト対応モデル)3 年モデル 型番: MF-PUVT3**GM3	VID:0x056E PID: 0x6807/0xe807	VID:0x056E PID:0x6907/0xe907
USB3.0 版対応セキュリティ機能付き USB フラッシュメモリ (トレンドマイクロエディション/管理者用ソフト対応モデル)5 年モデル 型番: MF-PUVT3**GM5	VID:0x056E PID: 0x6808/0xe808	VID:0x056E PID:0x6908/0xe908
USB3.0 版対応セキュリティ機能付き USB フラッシュメモリ (マカフィーエディション/管理者用ソフト対応モデル)1,3,5 年モデル 型番: HUD-PUVM3**GM*	VID:0x0693 PID:0x0093/0x0094	VID:0x0693 PID:0x0193/0x0x194
USB3.0 版対応セキュリティ機能付き USB フラッシュメモリ (シマンテックエディション/管理者用ソフト対応モデル)1,3,5 年モデル 型番: HUD-PUVS3**GM*	VID:0x0693 PID:0x0091/0x0092	VID:0x0693 PID: 0x0191/0x0x192
PasswordLocker4 型番: HUD-PL3**GM	VID:0x0693 PID:0x0095/0x0096	VID:0x0693 PID: 0x0195/0x0x196
USB2.0 版対応セキュリティ機能付き USB フラッシュメモリ (トレンドマイクロエディション/管理者用ソフト対応モデル)1 年モデル 型番: MF-PUVT**GM1	VID:0x056E PID:0x6801/0xe801	VID:0x056E PID:0x6901/0xe901
USB2.0 版対応セキュリティ機能付き USB フラッシュメモリ (トレンドマイクロエディション/管理者用ソフト対応モデル)3 年モデル 型番: MF-PUVT**GM3	VID:0x056E PID:0x6802/0xe802	VID:0x056E PID:0x6902/0xe902
USB2.0 版対応セキュリティ機能付き USB フラッシュメモリ (トレンドマイクロエディション/管理者用ソフト対応モデル)5 年モデル 型番: MF-PUVT**GM5	VID:0x056E PID:0x6803/0xe803	VID:0x056E PID:0x6903/0xe903
USB2.0 版対応セキュリティ機能付き USB フラッシュメモリ (マカフィーエディション/管理者用ソフト対応モデル)1,3,5 年モデル 型番: HUD-PUVM**GM*	VID:0x0693 PID:0x0057/0x0058	VID:0x0693 PID:0x0157/0x0158
USB2.0 版対応セキュリティ機能付き USB フラッシュメモリ (シマンテックエディション/管理者用ソフト対応モデル)1,3,5 年モデル 型番: HUD-PUVS**GM*	VID:0x0693 PID:0x0055/0x0056	VID:0x0693 PID:0x0155/0x0156
PasswordLocker3 型番: HUD-PL**GM	VID:0x0693 PID:0x0072/0x0073	VID:0x0693 PID:0x0172/0x0173
パスワードロッカーHDD 型番: H-PLPH***TM*	VID: 0x0693 PID: 0x00b2	-
セキュリティHDD Model-M 型番: H-PMPH***TM*	VID: 0x0693 PID:0x00b1	-
セキュリティポータブルHDD 型番: ELP-S***T*	VID:0x056E PID:0x7122	-
セキュリティ対策用外付けSSD 型番: ESD-PLxxxxGM	VID:0x056E PID:0x6A11	
暗号化機能付き外付けSSD 型番: LMD-PBLxxxU3BS	VID:0x0789 PID:0x0310	

遠隔設定 TOOL について

遠隔設定 TOOL は、遠隔地にいるユーザが持っている対象デバイスの設定を変更するためのソフトウェアです。認証キーが一致するデバイスのみ使用可能です。

※遠隔設定 TOOL の出力方法は本マニュアルの前項[デバイスへ設定を書き込む]をご確認ください。



(注)：遠隔設定 TOOL では以下の設定ができません。

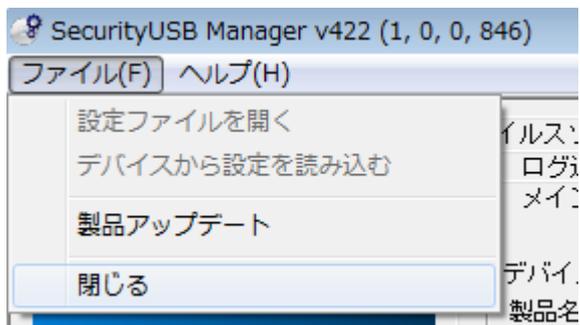
- リムーバブルディスク領域のボリュームラベルの設定
- CD-ROM 領域へのファイル追加
- リムーバブルディスク領域へのファイル追加
- パスワードロック解除後の自動実行ファイル設定
- リムーバブルディスク領域の容量変更
- ウィルススキャンソフトのライセンス更新案内表示設定
- コピーガード機能の設定

など

ツールメニュー

ツールメニューから以下のことができます。

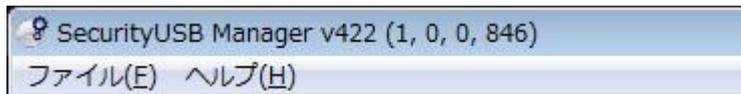
- 保存した設定ファイルを開く
- デバイスから設定を読み込む
- 製品アップデート
- マニュアルを見る



	項目	内容
ファイル	設定ファイルを開く	設定ファイル(ファイル名 : MpSUM.sum)を開きます。 本ソフトウェアでは設定した内容を設定ファイルとして保存することができます。その設定ファイルを読み込むことで、本ソフトウェアに設定した内容反映させることができます。
	デバイスから設定を読み込む	接続されている対象デバイスの設定を読み込み、本ソフトウェアにその設定を反映することができます。 (注):パスワードとヒントはセキュリティ上、読み出すことはできません。
	製品アップデート	弊社サーバに接続し、アップデートの有無を確認します。 アップデートがあった場合は、インターネット経由でソフトウェアアップデートを行います。
	閉じる	本ソフトウェアを終了します。
ヘルプ	マニュアル	本ソフトウェアのマニュアルを開きます。 マニュアルを開くには 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。

SecurityUSB Manager のバージョン確認

本ソフトウェアのバージョンは本ソフトウェアのキャプションに記載されております。



詳細設定を行う

より詳細な設定を行いたい場合は、[詳細設定。。]ボタンをクリックしてください。

パスワードポリシー設定

パスワード設定タブでは対象デバイスのパスワードに関するポリシー設定が可能です。
タブ[パスワード設定]を開いてください。

- ユーザによるパスワード変更の制限
- ユーザによるパスワードヒント登録の制限
- ユーザによるデバイスの初期化機能の制限
- パスワードの最小登録文字数の設定（標準設定：8文字）
- パスワードのアルファベット 最小使用文字数設定（標準設定：0文字）
- パスワードの数字 最小使用文字数設定（標準設定：0文字）
- パスワードの記号 最小使用文字数設定（標準設定：0文字）
- パスワード再入力許可回数設定（標準設定：5回）
- 初期パスワード/ヒント登録
- 初期パスワードの強制変更

パスワードポリシー（全製品対応）

- ユーザにパスワード変更を許可する
- ユーザにヒントの機能を許可する
- デバイスの初期化機能を有効にする

パスワードの最小文字数
（半角1～16文字）

アルファベットの最小文字数

数字の最小文字数

記号の最小文字数

パスワード再入力回数
（1～100回）

初期パスワード設定（全製品対応）

- 初期パスワードを設定する

パスワード（半角1～16文字）

パスワード(確認)

ヒント（半角0～32文字，全角0～16文字）

初期パスワードの強制変更

- パスワードを変更させない
- 強制的にパスワードを変更させる

項目	内容
ユーザにパスワード変更を許可する	<p>初期パスワード登録後のユーザによるパスワードの変更の[許可/禁止]設定ができます。</p> <p>[標準設定]許可 [設定方法]</p> <ul style="list-style-type: none"> ・パスワード変更を禁止する場合：チェックを外す ・パスワード変更を許可する場合：チェックを付ける
ユーザにヒントの登録を許可する	<p>パスワードのヒントの機能を[許可/禁止]設定ができます。</p> <p>[標準設定]許可 [設定方法]</p> <ul style="list-style-type: none"> ・ヒントの登録を禁止する場合：チェックを外す ・ヒントの登録を許可する場合：チェックを付ける
デバイスの初期化機能を有効にする	<p>製品の初期化の[許可/禁止]設定ができます。</p> <p>[標準設定]許可 [設定方法]</p> <ul style="list-style-type: none"> ・製品の初期化を禁止する場合：チェックを外す ・製品の初期化を許可する場合：チェックを付ける
パスワードの最小文字数	<p>対象製品のパスワード最小文字数を変更することができます。</p> <p>[標準設定] 8 文字 [設定方法]</p> <p>「パスワードの最小文字数」の入力欄に1～16を入力する。</p>
アルファベットの最小文字数	<p>パスワードに含むアルファベット数を設定することができます。</p> <p>[標準設定]0 文字 [設定方法]</p> <p>「アルファベットの最小文字数」の入力欄に0～16を入力する。 ※アルファベットによる制限を掛けない場合は「0」を入力してください</p>
数字の最小文字数	<p>パスワードに含む数字の数を設定することができます</p> <p>[標準設定] 0 文字 [設定方法]</p> <p>「数字の最小文字数」の入力欄に0～16を入力する。 ※数字による制限を掛けない場合は「0」を入力してください。</p>

記号の最小文字数	<p>パスワードに含む記号の数を設定することができます。</p> <p>[標準設定] 0文字</p> <p>[設定方法]</p> <p>「記号の最小文字数」の入力欄に0～16を入力する。 ※記号による制限を掛けない場合は「0」を入力してください。</p>
パスワード再入力回数	<p>パスワード再入力回数(間違えてもよい回数)を設定することができます。</p> <p>※ 無制限の設定はできません。</p> <p>[標準設定]5回</p> <p>[設定方法]</p> <p>「パスワード再入力回数」の入力欄に1～100を入力する。</p>
初期パスワード設定	<p>初期パスワード/ヒントを登録することができます。</p> <p>[標準設定] 初期パスワード/ヒント登録無し</p> <p>[設定方法]</p> <ul style="list-style-type: none"> ・初期パスワードを設定する場合 「初期パスワードを設定する」へチェックを入れ、パスワード、ヒントを入力する。 ※ヒントの登録は行わず、パスワードのみを登録することができます。 ・初期パスワードを設定しない場合 「初期パスワードを設定する」のチェックを外す。 <p>注意：ヒントに“ー”(長音記号)を使用することができません。</p>
初期パスワードの強制変更	<p>ユーザに初回起動時にパスワードを強制的に変更させることができます。</p> <p>共通の初期パスワードを登録した状態で配布し、ユーザによってパスワードを各自に変更させる場合にご使用ください。</p> <p>[標準設定]パスワードを変更させない</p> <p>[設定方法]</p> <p>ユーザに強制的に初期パスワードを変更させる場合、[強制的にパスワードを変更させる]を選択してください。</p>

- ・ パスワード有効期間の設定
- ・ パスワード認証超過失敗時の強制デバイス初期化設定
- ・ 過去に登録したパスワードの再登録制限
- ・ 24 時間内のパスワード変更可能回数設定
- ・ パスワードロック無効設定

パスワード有効期間設定 (全製品対応)

有効期間を設定しない

有効期間を設定する 日間毎に変更

パスワード認証超過失敗時の強制デバイス初期化 (全製品対応)

何も行わない

強制的に初期化を行う

パスワード履歴によるパスワード制限 (全製品対応)

制限しない

規定回数前までのパスワードの登録を制限する

回前までのパスワード

24時間以内のパスワード変更可能回数 (全製品対応)

制限しない

パスワードの変更回数を制限する

24時間以内に 回まで変更可能

パスワードロック無効化 (全製品対応)

パスワードロック有効(推奨)

パスワードロック無効

(注) : パスワードロックを無効にすると、リムーバブルディスクが常にアクセス可能な状態になります。

パスワード解除後のリムーバブルディスク画面表示を閉じる

リムーバブルディスク画面を開かない

リムーバブルディスク画面を開じる

項目	内容
パスワード有効期間設定	<p>パスワードの有効期間を設定でき、ユーザにパスワードを定期的に変更させることが可能です。</p> <p>[標準設定]有効期間を設定しない</p> <p>[設定方法]パスワード有効期間を設定する場合、[有効期間を設定する]を選択し、有効期間日数を設定してください。</p> <p>有効期間日数は 1 日～2000 日間で設定することができます。</p>
パスワード認証超過失敗時の強制デバイス初期化	<p>規定回数(通常 5 回)以上のパスワード認証失敗時にデバイスの初期化(デバイス内のデータ消去、パスワード初期化)を行うかを設定することができます。</p> <p>デバイスの紛失時のデータ流出のリスクを軽減することができます。</p> <p>[標準設定]何も行わない</p> <p>[設定方法]パスワード認証失敗時にデバイスの初期化を設定する場合、[強制的に初期化を行う]を選択してください。</p>

パスワード履歴によるパスワード制限	<p>過去に登録したパスワードの再登録を制限します。 最大過去の 10 回前までのパスワードの登録禁止が可能です。</p> <p>[標準設定]制限しない [設定方法]パスワード履歴によるパスワード制限を行う場合、[規定回数前までのパスワードの登録を制限する]を選択してください。 過去何回(1~10回)前までのパスワード登録を禁止するかを入力してください。</p>
24 時間内のパスワード変更可能回数	<p>24 時間の間に何回パスワードが変更できるかを設定します。 パスワード履歴によるパスワード制限と併用すれば、同じパスワードの入力制限をより強固にすることができます。</p> <p>例：パスワード履歴によるパスワード制限を過去 10 回に制限しても、 10 回入力が異なるパスワードを入力すると、10 回前と同じパスワードを入力することができます。 24 時間内のパスワード変更回数を 1 回に設定することにより、 同じパスワードを入力するまで最低 10 日必要になる設定ができます。</p> <p>[標準設定]制限しない [設定方法]制限を掛ける場合は[パスワードの変更回数を制限する]を選択し、 変更可能な回数(1~10回)を設定してください。</p>
パスワードロック無効化	<p>パスワードロック機能を無くすことができます。 パスワードロック機能を無くすため、常にデバイスのリムーバブルディスクが開いた状態で使用することができます。 Windows 以外の弊社ソフトウェアが動かない環境(Linux 等)とのデータ受け渡し時に本設定をご使用ください。 パスワードロック機能が無効な場合もウイルススキャンソフトウェアは起動します。 注意：本設定を行うと、パスワードロックが掛かっていないためデバイス紛失時データ流出が発生します。</p> <p>[標準設定]パスワードロック有効(推奨) [設定方法]パスワードロックを無効にするには、[パスワードロック無効]を選択してください。</p>
パスワード解除後のリムーバブルディスク画面表示を閉じる	<p>パスワード解除後にリムーバブルディスクの画面を自動で閉じることができます。</p> <p>[標準設定]リムーバブルディスク画面を閉じない [設定方法] リムーバブルディスク画面を閉じる場合は、 [リムーバブルディスク画面を閉じる]を選択してください。</p>

ウイルスソフト

ウイルスソフトタブではウイルススキャンソフトウェアの設定を行う事が可能です。本ソフトウェアを起動し、タブ[ウイルスソフト]を開いてください。

- ユーザによる起動時のウイルスチェック範囲設定
- ウイルス検出時にウイルス削除の禁止設定
- ユーザによるウイルス検出時の処理の設定変更制限
- 自動ソフトウェアアップデートの表示制限
- ウイルススキャンソフトのライセンス更新表示制限
- ユーザによるログ閲覧・削除制限
- ライセンス更新ページ(URL)設定変更
- 非通知ソフトウェア・アップデート設定
- パスワード解除後のリムーバブルディスク内のウイルススキャン範囲設定

ユーザによる起動時のウイルスチェック範囲設定 (マシテック、ホスト[®]、マカフィー)

- ウイルスチェック範囲変更を許可しない
- 変更を許可する

パスワード解除後のウイルススキャン範囲設定 (マシテック、ホスト[®]、マカフィー)

- 保存されているファイルを全てスキャンする
- 保存されているファイルをスキャンしない(マシテック、マカフィー)、一部スキャンする(ホスト[®])

ウイルス検出時の処理 (マシテック、マカフィー)

- ウイルスを削除する
- ウイルスを削除せず、デバイス内に保存する

ユーザによる[ウイルス検出時の処理]の設定変更の制限 (マシテック、マカフィー)

- 設定を制限する
- [ウイルス検出時の処理]の設定変更を制限しない

ソフトウェアアップデートの許可 (全製品対応)

- ソフトウェアアップデートを許可する 起動時に実施 毎月一度のみ
- ソフトウェアのアップデートを許可しない

ウイルススキャンソフトのライセンス終了の事前告知 (マシテック、ホスト[®]、マカフィー)

- 30日前から告知する
- ライセンス期間が終了するまで告知しない

ユーザによるログ閲覧・削除の制限 (全製品対応)

- 制限しない
- ログ閲覧・削除を制限する

ライセンス更新 (マシテック、マカフィー)

- 標準のライセンス更新ページを表示する
- 指定したライセンス更新ページを表示する

URL

非通知ソフトウェア・アップデート

- ソフトウェア・アップデートをユーザへ通知する
- ソフトウェア・アップデートをユーザへ通知せず、自動的にアップデートを行う

項目	内容
ユーザによる起動時の ウイルスチェック範囲設定	<p>ウイルススキャンソフトは起動時にデバイス内のファイルに対してのウイルスチェックを行います。</p> <p>ユーザがウイルススキャン範囲設定変更することを制限できます。</p> <p>ユーザ設定変更をさせたくない場合にご使用ください。</p> <p>[標準設定]変更を許可する</p> <p>[設定方法]</p> <p>ユーザによる設定変更を制限する場合、[ウイルスチェック範囲変更を許可しない]を選択してください。</p>
パスワード解除後のリムーバブルディスク内の ウイルススキャン範囲設定	<p>パスワード解除後のデバイス内に保存されているファイルに対してウイルスチェックする範囲を変更できます。</p> <p>[標準設定] 保存されているファイルを全てスキャンする</p> <p>[設定方法]</p> <p>全スキャンを行わない場合、[保存されているファイルをスキャンしない(マフィ、マソテック)、一部スキャンする(トレンド)]を選択してください。</p> <p>※トレンド版はリムーバブルドライブのルートにあるファイルのみウイルススキャンを実施します。</p>
ウイルスの検出時の処理	<p>ウイルスファイルを検出時、ウイルスの削除しない設定にできます。</p> <p>証拠ファイル、ウイルスに感染していても残す必要があるファイル等がある場合はご使用ください。</p> <p>ウイルス削除を行わない場合もウイルスの検出は行い、ウイルスがいることをユーザに知らせます。</p> <p>[標準設定]ウイルスを削除する</p> <p>[設定方法]</p> <p>ウイルスを削除しない場合、[ウイルスを削除せず、デバイス内に保存する]を選択してください。</p>
ユーザによる[ウイルス検出時の処理]の設定変更の制限	<p>ウイルス検出時にウイルスを削除するかをユーザに設定変更させる場合にご使用ください。</p> <p>[標準設定] 設定を制限する</p> <p>[設定方法]</p> <p>ユーザによって設定変更を可能にする、[ウイルス検出時の処理]の設定変更を制限しない]を選択してください。</p>

ソフトウェアアップデートの許可	<p>ソフトウェアアップデートを許可するか設定を行います。[標準設定]許可する</p> <p>[設定方法] ソフトウェアアップデートを許可しない場合は、[ソフトウェアのアップデートを許可しない]を選択してください。</p> <p>ソフトウェア・アップデートは製品起動時に毎回チェックを行います。1ヶ月に一度のみ、起動時にチェックしない、設定が可能です。</p>
ウイルススキャンソフトのライセンス更新案内表示	<p>ウイルススキャンソフトはライセンス製品で、有効期間間近になるとライセンス更新案内が表示されます。そのライセンス更新案内表示を制限することができます。</p> <p>[標準設定]表示する</p> <p>[設定方法] ウイルススキャンソフトのライセンス更新案内表示を制限する場合、[ライセンス更新案内を表示しない]を選択してください。</p>
ユーザによるログ閲覧・削除を制限	<p>本製品は使用した PC 情報、ウイルス定義ファイルバージョン等をログとして残し、ユーザはそのログを閲覧することができます。ユーザによるログの閲覧・削除を制限することができます。</p> <p>[標準設定]制限しない</p> <p>[設定方法] ユーザによるログの閲覧・削除を制限する場合、[ログ閲覧・削除を制限する]を選択してください。</p>
ライセンス更新設定	<p>セキュリティ USB/HDD はライセンスが切れる 1ヶ月前からライセンス更新を促すメッセージが表示され、弊社の更新説明ページへ移動できます。この移動先ページをお客様の用意したページへ設定することができます。お客様の管理者の連絡先がなど記載されているページなどにリンクするなどにご利用ください。</p> <p>[標準設定]標準のライセンス更新ページを表示する</p> <p>[設定方法] ライセンス更新ページを指定 URL へ変更する場合、[指定したライセンス更新ページを表示する]を選択し、URL を入力してください。</p>
非通知ソフトウェアアップデート	<p>ソフトウェア・アップデート通知画面を表示せず、自動的にアップデートをことができます。</p> <p>[標準設定]ソフトウェアアップデートをユーザへ通知する</p> <p>[設定方法] ソフトウェアアップデート画面をユーザへ通知しない場合は、「ソフトウェア・アップデートをユーザへ通知せず、自動的にアップデートを行う」を選択してください。 「ソフトウェア・アップデートをユーザへ通知せず、自動的にアップデートを行う」を選択してください。</p>

- 製品初期化時の定義ファイル復旧設定
- ウイルススキャン初期化中の進捗画面の表示有無設定
- プロキシ設定

製品初期化時の定義ファイル復旧 (シマンテック、マカフィー)

製品の初期化時に定義ファイルを復旧しない
 製品の初期化時に定義ファイルを復旧する

ウイルススキャン初期化中の進捗画面 (シマンテック、マカフィー)

ウイルススキャン初期化中の進捗画面を表示する
 ウイルススキャン初期化中の進捗画面を表示しない

プロキシ設定

Internet Explorerのプロキシ設定をインポートする
 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

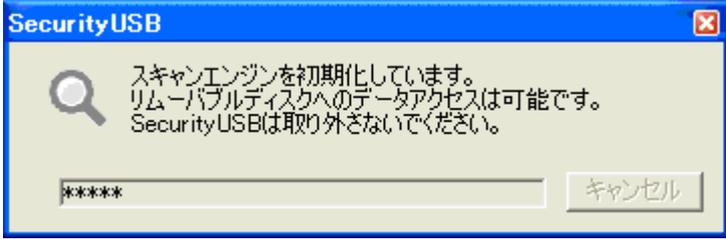
プロキシサーバ

ポート番号

プロキシサーバに資格情報が必要な場合は、以下の情報を入力してください。必要でない場合は何も入力しないでください。

ユーザ名

パスワード

項目	内容
製品初期化時の定義ファイル復旧	<p>製品初期化時に定義ファイルを復旧するか設定することができます。初期化時に復旧しない場合、初回パスワード解除後に復旧致します。</p> <p>[標準設定]製品の初期化時に定義ファイルを復旧しない [設定方法] 初回パスワード解除後に定義ファイルの復旧処理を行わず、すぐにご使用になられる場合、「製品の初期化時に定義ファイルを復旧する」を選択してください。</p>
ウイルススキャン初期化中の進捗画面	<p>ウイルス対策 USB(マカフィ・シマンテック)ではウイルススキャン初期化、定義ファイル更新時にタスクトレイの上部に進捗画面が表示されます。</p>  <p>その進捗画面を表示・非表示設定が可能です。</p> <p>[標準設定]ウイルススキャン初期化中の進捗画面を表示する [設定方法] 進捗画面を表示しない場合、[ウイルススキャン初期化中の進捗画面を表示しない]を選択してください。</p>

プロキシ設定	<p>ソフトウェア・アップデート時などにインターネットへアクセスを行います。</p> <p>プロキシで制限を掛けている環境で使用し、Internet Explorer 以外のプロキシを使用する場合本項目を設定してください。</p> <p>注意：定義ファイル更新には使用できません</p> <p>[標準設定] Internet Explorer のプロキシ設定をインポートする</p> <p>[設定方法] 「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」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。</p>
--------	--

・ ウイルス定義ファイルのダウンロード方法設定

ウイルス定義ファイルダウンロード設定 (シマンテック、マカフィー)

インターネット経由で定義ファイルをダウンロードする

インターネット経由またはLocal Updater経由でダウンロードする

Local Updater経由でダウンロードする

Local Updaterで設定したサーバの共有フォルダパスを入力してください

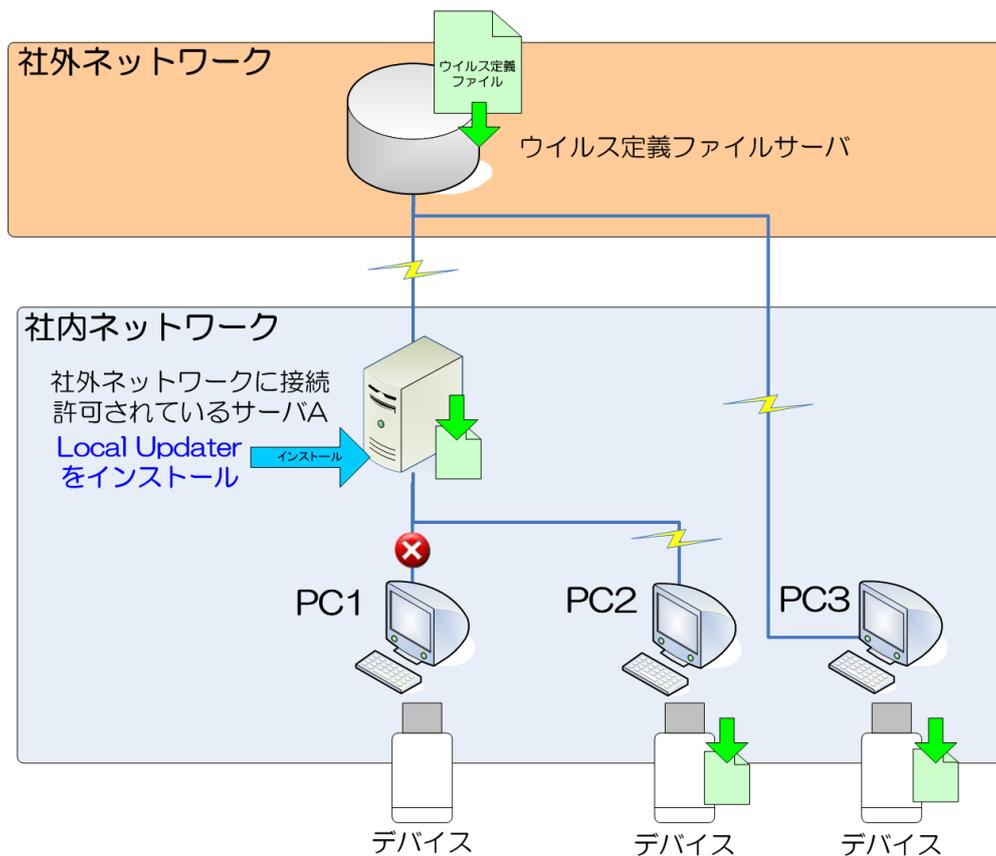
インターネット経由またはMcAfee VirusScan Enterpriseからダウンロードする

McAfee VirusScan Enterpriseからダウンロードする

項目	内容
ウイルス定義ファイルダウンロード設定	<p>ウイルス定義ファイルのダウンロード設定ができます。</p> <p>対象製品はウイルス定義ファイルをダウンロードする際、社外ネットワークのウイルス定義ファイルサーバへ接続する必要があります。</p> <p>SecurityUSB Manager と SecurityUSB Manager に同封されている Local Updater を使用することにより、社外ネットワークへ接続が許可されていない PC を使用し、ウイルス定義ファイルをダウンロードすることができます。</p> <p>[標準設定]インターネット経由 [設定方法]</p> <ul style="list-style-type: none"> ・インターネット経由のみでダウンロードする場合：[インターネット経由でダウンロードする]を選択 ・LocalUpdater 経由のみでダウンロードする場合：[LocalUpdater 経由でダウンロードする]を選択 ・インターネット経由または Local Updater 経由でダウンロードする場合、[インターネット経由または Local Updater 経由でダウンロードする]を選択 ・PC にインストールされている McAfee VirusScan Enterprise が持っている定義ファイルをダウンロードする場合、[McAfee VirusScan Enterprise からダウンロードする]を選択 ・PC にインストールされている McAfee VirusScan Enterprise が持っている定義ファイルをダウンロードするまたはインターネット経由でダウンロードする場合、 [インターネット経由または McAfee VirusScan Enterprise からダウンロードする]を選択 <p>※McAfee VirusScan Enterprise からのダウンロードはウイルス対策 USB HUD-PUVM**GM*シリーズのみ対応しております。</p> <p>※今後 McAfee VirusScan Enterprise の仕様が変わった場合、McAfee VirusScan Enterprise から定義ファイルをダウンロードできなくなる場合があります。</p> <p>そのような場合でもインターネット経由で定義ファイルのダウンロードが可能な [インターネット経由または McAfee VirusScan Enterprise からダウンロードする]の選択を推奨致します。</p>

Local Updater とは

Local Updater は社外ネットワークに接続されている社内サーバへウイルス定義ファイルをダウンロードし、社外ネットワークへ接続許可されていない社内 PC へ接続したウイルス対策 USB へ定義ファイルを配布するためのサーバソフトウェアです。



PC	PC 状態	Local Updater の対応可否
PC1	社外ネットワークに接続許可されていないローカルPC。 サーバAとネットワーク接続されていない。	サーバAとネットワーク接続してないため、 Local Updater 経由の定義ファイルダウンロードに 対応できません。
PC2	社外ネットワークに接続許可されていないローカルPC。 サーバAとネットワーク接続されている。	Local Updater 経由の定義ファイルダウンロードに 対応できます。
PC3	社外ネットワークに接続されているPC。	サーバAとネットワーク接続してないため、 Local Updater 経由の定義ファイルダウンロードに 対応できませんが、社外ネットワークに接続されてい るため、直接社外ウイルス定義ファイルサーバ からダウンロードを行います。

※本ソフトウェアをインストールしたサーバとローカル PC がネットワーク接続している必要があります。

※本ソフトウェアをインストールしたサーバとローカル PC がネットワーク接続してない場合、ローカル PC に接続した対象デバイス

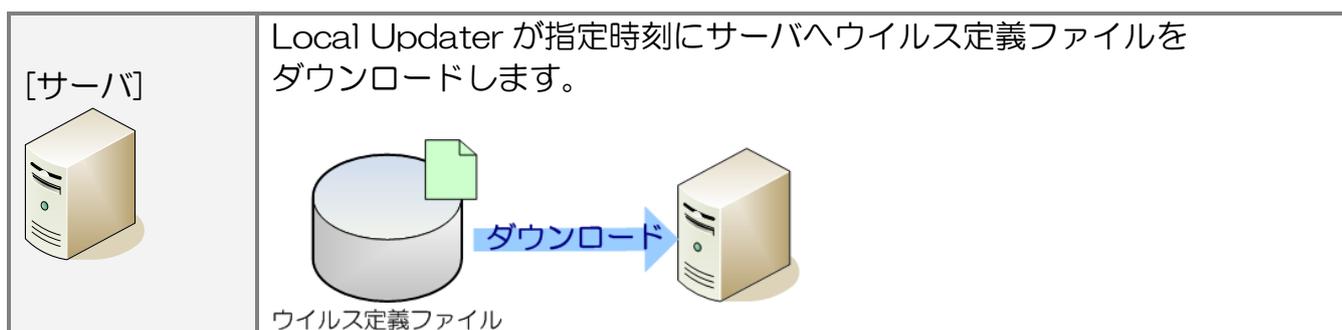
へウイルス定義ファイルを配布することはできません。

Local Updater の使用の流れ

<セットアップ>



<運用>



デバイス設定

デバイス設定タブではデバイスの貸し出し期限設定などの設定が可能です。
タブ[本体デバイス設定]を開いてください。

- ・デバイスのリムーバブルディスク領域のボリュームラベル設定
- ・デバイスの USB のプロダクトストリング設定
- ・デバイスへのファイル書き込み制限(読み取り専用デバイス化)
- ・使用 OS 制限
- ・Mac OS X 対応設定
- ・貸し出し期限設定

リムーバブルディスク領域のボリュームラベル設定 (全製品対応)

設定しない

設定する ボリュームラベル

USBプロダクトストリングの設定 (全製品対応)

設定しない

設定する プロダクトストリング

デバイスへのファイル書き込み制限(読み取り専用デバイス化) (全製品対応)

書き込み制限をかけない

書き込み制限をかける

使用OS制限 (全製品対応)

使用を制限するOSにチェックを入れてください

Windows2000 Windows7 Windows2003R2 Windows2008R2

WindowsXP Windows2003 Windows2008

WindowsVista Windows8/8.1 WindowsXP Embedded

Windows2012 Windows2012R2 Windows10

Mac OS X対応 (全製品対応)

Mac OS Xで使用しない 注: Mac OS X上で使用した場合、ウイルススキャンソフト、ログ収集機能、コピーガードソフトは動作しません。

Mac OS Xで使用する

MacOSやCD-ROMが制限された環境に最適化します

貸し出し期限設定 (全製品対応)

有効期限を設定しない

有効期限を設定する

有効期限日

有効期限日を過ぎた場合、強制的にデバイスを初期化する

項目	内容
リムーバブルディスク領域のボリュームラベル設定	<p>本体デバイスのリムーバブルディスク領域のボリュームラベルを変更することができます。英数字で最大 11 文字設定可能です。</p> <p>[標準設定]設定しない</p> <p>[設定方法] ボリュームラベルを変更する場合、[設定する]を選択し、ボリュームラベルを入力してください。</p>

USB プロダクトストリングの設定	<p>本体デバイスの USB プロダクトストリングを変更することができます。 英数字で最大 16 文字設定可能です。</p> <p>[標準設定]設定しない [設定方法] USB プロダクトストリングを変更する場合、[設定する]を選択し、プロダクトストリングを入力してください。</p>
デバイスへのファイル書き込み制限 (読み取り専用デバイス化)	<p>本体デバイスを読み取り専用を設定することができます。 デバイスへファイル書き込みを一切させたくない場合、本設定を行なってください。</p> <p>[標準設定]書き込み制限をかけない [設定方法] 本体デバイスへのファイル書き込みを制限する場合、[書き込み制限をかける]を選択してください。</p>
使用 OS 制限	<p>本体デバイスを使用できる Windows OS を制限します。 古い Windows OS で使用させたくない場合等にご使用ください。</p> <p>[標準設定]使用制限 OS 無し [設定方法] 使用する OS 制限の制限を掛ける場合、制限する OS 制限へチェックを入れてください。</p>
Max OS X 対応	<p>本体デバイスを Mac OS X 使用を設定します。 ウイルススキャンソフト、ログ収集機能、コピーガード機能等は Mac OS X では動作しないため、ご注意ください。Mac OS X ではパスワードロック機能のみ動作します。</p> <p>[標準設定]Mac OS X で使用しない [設定方法] Mac OS X で使用する場合、[Mac OS X で使用する]を選択してください。</p>
MacOS や CD-ROM が制限された環境への最適化	<p>MacOS や CD-ROM が制限された環境では、それらの環境で使用可能なモードでデバイスを再認識します。 この設定を有効にした場合、初めからそれらの環境で使用可能なモードとなり、デバイス再認識を行いません。</p>
貸し出し期限設定	<p>本製品の有効期間を設定します。 他社へ貸し出しを行う場合にご使用ください。</p> <p>[標準設定]有効期限を設定しない [設定方法] 有効期間を設定する場合、[有効期限を設定する]を選択し、有効期間日を選択してください。 有効期限日が切れた時に対象デバイスを初期化する場合、[有効期限日を過ぎた場合、強制的にデバイスを初期化する]へチェックを入れてください。</p>

書き出し期限設定：
有効期限再設定ソフトウェア

対象デバイスに対して設定した有効期限を再設定するための「有効期限再設定ソフトウェア」を追加しました。

試用期間が切れてしまった SecurityUSB を再度使用する場合にお使いください。

有効期限再設定ソフトウェアを使用する場合、[有効期限再設定ソフトウェアを開く] ボタンをクリックしてください。

- デバイスの CD-ROM 領域/リムーバブルディスク領域へのファイル追加
- パスワードロック解除時の自動実行ファイルの設定
- リムーバブルディスク容量の変更

The screenshot shows a settings window with the following sections:

- CD-ROM領域へのファイル追加 (全製品対応)**: Radio buttons for "ファイル追加しない" (selected) and "ファイル追加する". A text box contains "重要.txt". Buttons: "追加する", "削除する", "全て削除する".
- リムーバブルディスク領域へのファイル追加 (全製品対応)**: Radio buttons for "ファイル追加しない" and "ファイル追加する" (selected). A text box contains "key.txt". Buttons: "追加する", "削除する", "全て削除する".
- パスワードロック解除後の自動実行ファイル設定 (全製品対応)**: Radio buttons for "指定ファイルの自動実行を行わない" and "指定ファイルの自動実行を行う" (selected).
- 自動実行ファイル (全製品対応)**: "指定ファイル格納領域" with radio buttons for "CD-ROM" (selected) and "リムーバブルディスク". "指定ファイルのパス" with a list box containing "重要.txt".
- リムーバブルディスク容量の変更 (全製品対応)**: Radio buttons for "サイズ設定を行わない" (selected) and "サイズ設定を行う". A "サイズ" field shows "16" MByte.

項目	内容
CD-ROM 領域へのファイル追加	<p>本体デバイスの CD-ROM 領域へファイル追加を行うことが可能です。 管理者様が用意したユーザマニュアル等を追加する場合にご使用ください。 CD-ROM 領域へ追加したファイルの削除はユーザによって行うことはできません。</p> <p>[標準設定]ファイル追加しない [設定方法] ファイルを追加する場合、[ファイルを追加する]を選択し、[追加ボタン]を押して ファイル・フォルダを選択してください。</p> <p>(注)：追加されたファイルはソフトウェアのアップデート処理によって削除されます。</p>

<p>リムーバブルディスク領域への ファイル追加</p>	<p>本体デバイスのCD-ROM 領域へファイル追加を行うことが可能です。 管理者様が用意したユーザマニュアル等を追加する場合にご使用ください。</p> <p>[標準設定]ファイル追加しない [設定方法] ファイルを追加する場合、[ファイルを追加する]を選択し、[追加ボタン]を押して ファイル・フォルダを選択してください。</p> <p>(注)：追加されたファイルは、製品の初期化、ソフトウェアのアップデート処理に よってデータが削除されます。</p>
<p>パスワードロック解除後の 自動実行ファイル設定</p>	<p>パスワードロック解除後に、指定したファイルを自動実行することが可能です。 自動実行するファイルは[本体デバイスへのファイル追加]で設定したファイルから 一つ選択可能です。</p> <p>[標準設定] 指定ファイルの自動実行を行わない [設定方法] パスワードロック解除後に指定ファイルを自動実行する場合、[指定ファイルの 自動実行を行う]を選択してください。</p>
<p>自動実行ファイル</p>	<p>自動実行するファイルを選択します。</p> <p>※ パスワードロック解除後の自動実行ファイル設定で[指定ファイルの自動実行を 行う]を選択した場合に選択可能になります。</p> <p>自動実行するファイルが格納されているドライブを選択し、ファイルの選択を 行ってください。</p>
<p>リムーバブルディスク容量の変更</p>	<p>本体デバイスのリムーバブルディスク領域のサイズ変更ができます。 ユーザが使用できる容量を制限した場合にご利用ください。</p> <p>[標準設定]サイズ変更を行わない [設定方法] 本体デバイスのリムーバブルディスク領域のサイズ変更を行う場合、 [サイズ設定を行う]を選択し、サイズ(MByte 単位)を入力してください。</p>

特殊

特殊タブでは対象デバイスへの特殊処理が可能です。本ソフトウェアを起動し、タブ[特殊]を開いてください。

- ・ 遠隔地にいるユーザのデータ救出機能を有効化
- ・ 遠隔データレスキュー用の解除ファイル・解除番号生成
- ・ 手元にあるデバイスのデータレスキュー
- ・ デバイス内のログ収集

データ救出設定 (全製品対応)

- パスワードを忘れた時にデータ救出を許可しない
- レスキューファイルによるデータ救出を許可する
- レスキュー番号によるデータ救出を許可する
- レスキューファイル・レスキュー番号によるデータ救出を許可する

パスワードを忘れた場合でもセキュリティUSB内のデータを救出することができるようになります。ユーザがパスワードを忘れることが多々ありますので、本機能を有効にして頂くことを推奨します。
注：本設定が有効では無いセキュリティUSBはパスワードを忘れた場合、セキュリティUSB内のデータを救出することは一切できません。

遠隔地にいるユーザのデータ救出 (全製品対応)

遠隔地にいるユーザのデータ救出を行うため、解除番号/ファイルを生成します。ユーザへレスキュー番号/レスキューファイルを送付依頼をしてください。

ユーザからレスキューファイルが送付された場合は[ユーザ用 解除ファイル作成]へ進んでください。
ユーザからレスキュー番号が送付された場合は[ユーザ用 解除番号作成]へ進んでください。

ユーザ用 解除番号作成

ユーザ用 解除ファイル生成

データの救出 (全製品対応)

パスワードを忘れてしまったデバイス内のデータを救出します
お手元にデータ救出を行うデバイスがある場合、この救出方法を使用してください。
デバイス内のデータを保持し、パスワードを初期化します。

デバイスを接続し、[データ救出]ボタンを押してください。

データ救出

デバイス内のログ収集 (全製品対応)

デバイス内に保存されているログをPCへ保存します。

デバイス内のログを収集する

ログ収集後、デバイス内のログを削除する

項目	内容
データ救出設定	<p>遠隔地にいるユーザのデータ救出/データ救出機能を有効にすることができます。パスワードを忘れた場合でもセキュリティ USB/HDD 内のデータを救出することができます。セキュリティ USB/HDD 内のデータを保持したまま、パスワードだけを初期化することができます。ユーザがパスワードを忘れることが多々ありますので、本機能を使用して頂くことを推奨します。</p> <p>[標準設定]許可しない [設定方法] 遠隔地にいるユーザのデータ救出/データ救出機能を有効にする場合、チェックを入れてください</p>
遠隔地にいるユーザのデータ救出	<p>管理者から遠隔地にあるセキュリティ USB/HDD 内のデータを保持したまま、パスワードだけを初期化することができます。</p> <p>注意：データ救出は事前に(パスワードを忘れた時にデータ救出を許可する(推奨))を選択したセキュリティ USB/HDD のみ実行できます。</p> <p>使用法は本書の項「遠隔データレスキューの流れ」を確認ください。</p>
データの救出	<p>データ救出ボタンでパスワードを忘れてしまってセキュリティ USB/HDD 内のデータを保持したまま、パスワードだけを初期化することができます。</p> <p>注意：データ救出は事前にデータ救出設定欄で(***データ救出を許可する)を選択したセキュリティ USB/HDD のみ実行できます。</p> <p>[方法] 1：データ救出する対象デバイスを PC へ接続してください。 2：[データ救出]ボタンを押してください。 3：新しく登録するパスワード/ヒントを入力し、[登録]ボタンを押してください。データが保持されたまま、パスワードが初期化されます。</p>
デバイス内のログ収集	<p>デバイス内に保存されているログを収集します。保存するログは以下の3種類です。</p> <ul style="list-style-type: none"> •セキュリティ USB/HDD 標準ログ •ファイルアクセスログ※ •印刷ログ※ <p>※コピーガード設定ソフトで各ログを取得に設定している場合。 詳細はコピーガード設定ソフトマニュアルをご確認ください。</p> <p>※ファイルアクセスログ、印刷ログを救出する場合、データ救出機能が有効になっている必要があります。</p> <p>[方法] [デバイス内のログを収集する]ボタンを押してください。</p> <p>ログ収集後にデバイス内のログを削除する場合は、[ログ収集後、デバイス内のログを削除する]へチェックを入れてください。</p>

ログ収集機能について

ログ収集機能はセキュリティ USB/HDD 内に格納されているログを収集する機能です。収集できるログは以下です。

■ 収集できるログ

ログ	内容
セキュリティ USB/HDD 標準ログ	<p>セキュリティ USB/HDD が標準で取得するログです。パスワード解除の度に収集します。</p> <p>ファイル形式：テキスト</p> <p>ファイル名：2012_07_20_15_44_28.txt</p> <p>ログが取られた時刻がファイル名となっています。yyyy_mm_dd_hh_ss_mm.txt</p> <p>取得する情報：</p> <ul style="list-style-type: none"> ・セキュリティ USB/HDD を使用した PC 情報(OS 名、ユーザ名、MAC アドレス等)、 ・セキュリティ USB/HDD のデバイス情報(USB シリアル番号) ・ウイルススキャンソフトバージョン、定義ファイルバージョン ・駆除したウイルス名 <p>セキュリティ USB/HDD の種類によっては取れない情報もございます。各ログの詳細は各製品のマニュアルをご確認願います。</p>
ファイルアクセスログ※	<p>コピーガード機能を有効時に取得できるファイルアクセスログです。</p> <p>ファイル形式：XML</p> <p>ファイル名；0000000000000000/00000000000000001/00000000000000002...</p> <p>セキュリティ USB/HDD 内のファイルにアクセスする度にログを残します。</p> <p>取得する情報：</p> <ul style="list-style-type: none"> ・アクセスしたファイル名 ・ファイルへのアクセス動作(Open/Create/Access/Copy/Move/Execute/Delete) ・ファイルへアクセスしたプロセス名 ・ファイルへアクセスした時刻 等 <p>※ログの詳細は“コピーガード設定ソフトマニュアル”をご覧ください。</p>
印刷ログ※	<p>コピーガード機能を有効時に取得できる印刷ログです。</p> <p>ファイル形式：XML</p> <p>ファイル名；0000000000000000/00000000000000001/00000000000000002...</p> <p>セキュリティ USB/HDD 内のファイルを印刷する度にログを残します。</p> <p>取得する情報：</p> <ul style="list-style-type: none"> ・印刷したファイル名 ・印刷を実行したプロセス名 ・プリンタ名 ・ファイルを印刷した時刻 等 <p>※ログの詳細は“コピーガード設定ソフトマニュアル”をご覧ください。</p>

※コピーガード設定ソフトで各ログを取得に設定している場合。設定方法はコピーガード設定ソフトマニュアルをご確認ください。

収集したログのファイル・フォルダ構造は以下になります。

■ログのファイル・フォルダ構造

2012_07_20_17_56_30[フォルダ 1]

└device_log[フォルダ 2]

| └ 2012_07_20_15_44_28.txt

| └ 2012_07_12_11_24_15.txt

└iss_log_host[フォルダ 3]

| └ 000000000000000000

| └ 000000000000000001

└iss_log_print[フォルダ 4]

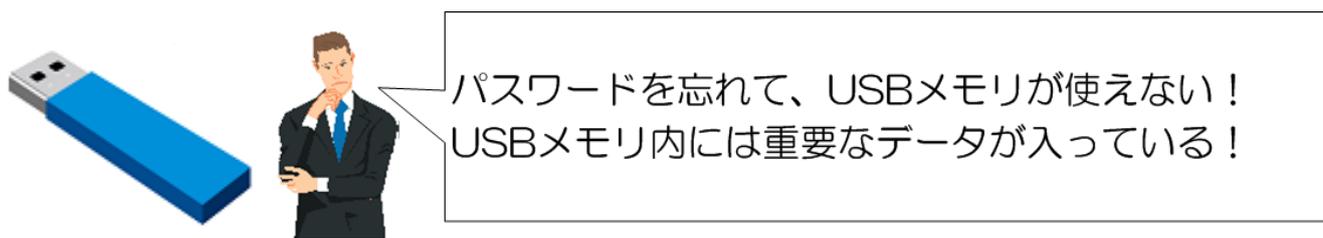
 └ 000000000000000000

 └ 000000000000000001

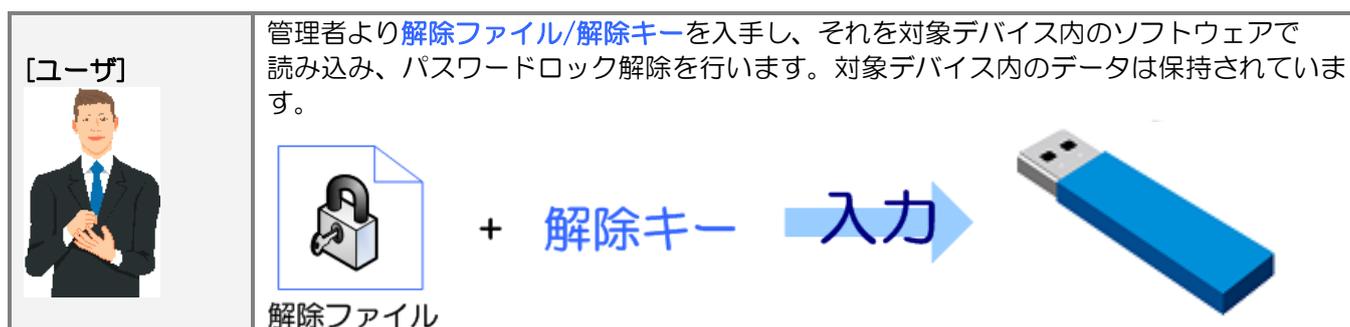
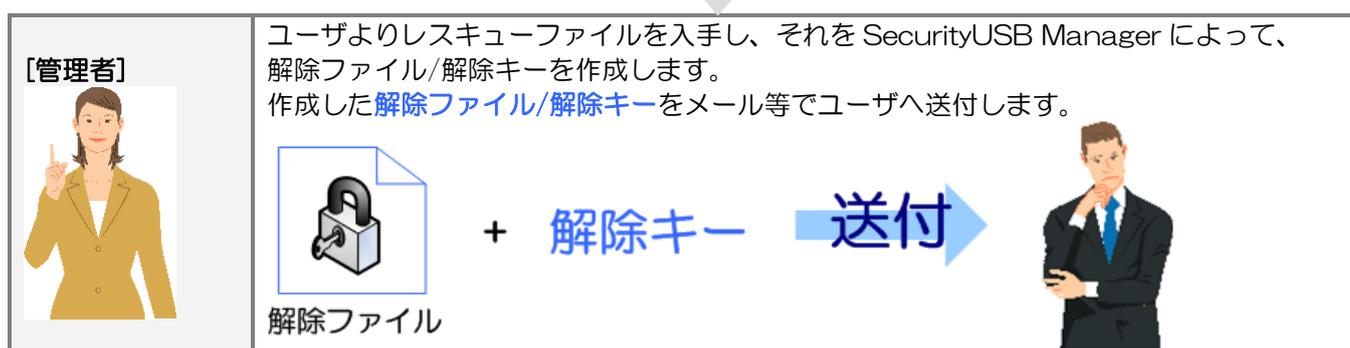
フォルダ	内容
フォルダ 1	ログ収集した時刻をフォルダ名にしたフォルダです。 フォルダ名のルール：yyyy_mm_dd_hh_ss_mm
フォルダ 2	セキュリティ USB/HDD が保存する標準のログを保存するフォルダです。 フォルダ名：device_log
フォルダ 3	ファイルアクセスログを保存するログフォルダです。 フォルダ名：iss_log_host
フォルダ 4	印刷ログを保存するログフォルダです。 フォルダ名：iss_log_print

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



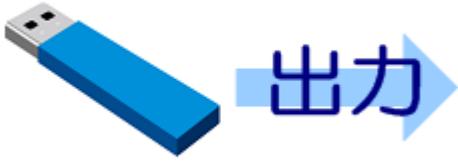
■レスキューファイルを使用した場合



■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。

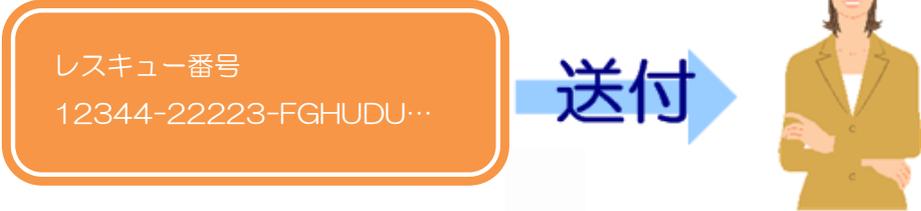


出力

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。



送付

レスキュー番号
12344-22223-FGHUDU...

[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

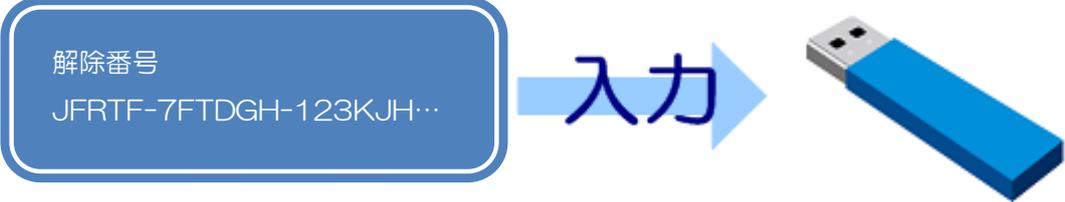


送付

解除番号
JFRTF-7FTDGH-123KJH...

[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。対象デバイス内のデータは保持されています。



入力

解除番号
JFRTF-7FTDGH-123KJH...

ログ管理

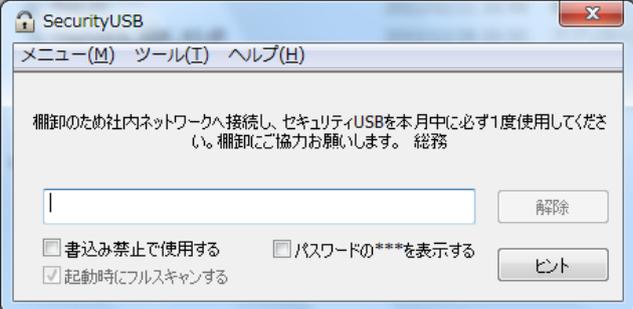
ログ管理タブではログ管理ソフト(Info Banker オンプレミス版・クラウド版)へのログ送信設定を行うことができます。

Info Banker オンプレミス版・クラウド版を両方使う場合、本タブで設定を行ってください。
本ソフトウェアを起動し、タブ[ログ管理]を開いてください。

- ・ ログ管理ソフト(Info Banker)へのログ送信設定

製品管理サービス (全製品対応)					
<input type="radio"/> 製品管理サービスを使用しない					
<input type="radio"/> Info Banker(オンプレミス)で管理する					
<input type="radio"/> Info Banker(クラウド)で管理する	※設定はタブ:クラウド管理で行えます。				
<input checked="" type="radio"/> Info Banker(オンプレミス・クラウド)で管理する	<input type="button" value="オンプレミス専用PC設定"/>				
※クラウドの設定も本画面で行えます。					
ホスト名(オンプレミスのみ)					
InfoBankerをインストールしたサーバのホスト名またはIPアドレスを入力してください					
ホスト名/IPアドレス1 例: 123.456.789.012	<input type="text" value="10.10.***.*"/>				
ホスト名/IPアドレス2 例: 123.456.789.012	<input type="text" value="10.11.***.*"/>				
通常ログ(全製品対応)					
<input type="radio"/> 通常ログを送信しない	<input checked="" type="radio"/> 通常ログを送信する				
ウイルス検知ログ(全製品対応)					
<input type="radio"/> ウイルス検知ログを送信しない	<input checked="" type="radio"/> ウイルス検知ログを送信する				
ファイルリストログ(全製品対応/オンプレミスのみ)					
<input checked="" type="radio"/> ファイルリストログを送信しない	<input type="radio"/> ファイルリストログを送信する				
棚卸ログ(全製品対応)					
<input type="radio"/> 棚卸ログを送信しない	<input checked="" type="radio"/> 棚卸ログを送信する				
送信月設定					
<input type="checkbox"/> 1月	<input type="checkbox"/> 2月	<input checked="" type="checkbox"/> 3月	<input type="checkbox"/> 4月	<input type="checkbox"/> 5月	<input type="checkbox"/> 6月
<input type="checkbox"/> 7月	<input type="checkbox"/> 8月	<input checked="" type="checkbox"/> 9月	<input type="checkbox"/> 10月	<input type="checkbox"/> 11月	<input type="checkbox"/> 12月
棚卸時に通知するメッセージを設定してください(最大全角120文字)					
<input type="text" value="棚卸しのため社内ネットワークへ接続し、セキュリティUSBを使用してください。"/> 情報ネットワーク部					
ファイル操作ログ(USB版対応)					
<input checked="" type="radio"/> ファイル操作ログを送信しない	<input type="radio"/> ファイル操作ログを送信する				
PC情報送信(全製品対応)					
<input type="radio"/> PC情報を送信しない	<input checked="" type="radio"/> PC情報を送信する				
認証機能(オンプレミスのみ)					
<input checked="" type="radio"/> 認証付きログを送信しない	<input type="radio"/> 認証付きログを送信する				

項目	内容
Info Banker へのログ送信可否設定	<p>対象デバイスからログ管理ソフト(Info Banker(オンプレミス)/クラウドへログを送信するか設定することができます。</p> <ul style="list-style-type: none"> • InfoBankerCloud へ送信する場合は、「InfoBankerCloud でログ管理する」を選択してください。詳細は項：クラウド管理で説明を致します。 • InfoBanker オンプレミス・クラウド両方へログ送信する場合は、「InfoBanker(オンプレミス・クラウド)で管理する」を選択してください。その場合、オンプレミスとクラウドの管理項目は共通となり、本タブで設定をしてください。 クラウドのアカウント情報のみタブ：クラウド管理で行ってください。 InfoBanker オンプレミス・クラウドで管理する場合に、オンプレミス専用 PC を設定することができます。詳細は項：オンプレミス専用 PC 設定で説明を致します。 <p>InfoBanker(オンプレミス)を2箇所へ導入している場合、2つのIPアドレスを入力してください。最初に見つかったIPアドレスのInfoBankerへログを送信します。</p> <p>[標準設定]Info Banker へログを送信しない [設定方法] Info Banker へログを送信する場合、[Info Banker へログを送信する]を選択し、Info Banker がインストールされているサーバのIPアドレスを選択してください。</p>
通常ログ	<p>対象デバイスからログ管理ソフト(Info Banker)へ通常ログを送信することができます。</p> <p>[標準設定]通常ログを送信しない [設定方法] Info Banker へ通常ログを送信する場合、[通常ロゴを送信する]を選択してください。</p>
ウイルス検知ログ	<p>対象デバイスからログ管理ソフト(Info Banker)へウイルス検知ログを送信することができます。</p> <p>[標準設定]ウイルス検知ログを送信しない [設定方法] Info Banker へウイルス検知ログを送信する場合、[ウイルス検知ロゴを送信する]を選択してください。</p>
ファイルリストログ (オンプレミスのみ)	<p>デバイスからログ管理ソフト(Info Banker)へファイルリストログを送信することができます。</p> <p>[標準設定]ファイルリストログを送信しない [設定方法] Info Banker へファイルリストログを送信する場合、[ファイルリストロゴを送信する]を選択してください。</p>

<p>棚卸ログ</p>	<p>対象デバイスからログ管理ソフト(Info Banker)へ棚卸ログを送信するか設定することができます。</p> <p>[標準設定]棚卸ログを送信しない [設定方法] Info Banker へ棚卸ログを送信する場合、[棚卸ロゴを送信する]を選択してください。</p> <p>棚卸ログは月に1度のみ送信するログです。送信する月を選択してください。 複数の月も選択可能です。また棚卸ログ送信を促すためのメッセージも表示可能です。 例：棚卸のため社内ネットワークへ接続し、セキュリティ USB を本月中に必ず1度使用してください。棚卸にご協力お願いします。 総務 →実際の表示は以下のようになります。</p> 
<p>ファイル操作ログ</p>	<p>ファイル操作ログを InfoBanker へ送信する設定を行います。</p> <p>[標準設定]ファイル操作ログを送信しない [設定方法]InfoBanker へファイル操作ログを送信する場合、「ファイル操作ログを送信する」を選択してください。</p>
<p>PC 情報送信</p>	<p>PC 情報を InfoBanker へ送信する・しないの設定を行います。 PC 情報：MAC アドレス/IP アドレス等</p> <p>[標準設定]PC 情報を送信する [設定方法] PC 情報を InfoBanker へ送信しない場合、「PC 情報を送信しない」を選択してください。</p>
<p>認証機能 (オンプレミスのみ)</p>	<p>認証キーを付けたログを InfoBanker へ送信する・しないの設定を行います。 InfoBanker 側で設定した認証キーとセキュリティ USB/HDD 側の認証キーが一致した場合のみ、InfoBanker でログを受信できます。 ※認証キー：セキュリティ USB Manager でセキュリティ USB/HDD に付けた認証キー ※InfoBanker 1.2.0.0 以上かつ、認証キー機能を有効にする必要があります。 InfoBanker 側の設定に付きましては InfoBanker マニュアルをご確認ください。</p> <p>[標準設定]認証付きログを送信しない [設定方法] 機密付きログを InfoBanker へ送信する場合、「認証付きログを送信しない」を選択してください。</p>

■ オンプレミス専用 PC 設定

InfoBanker(オンプレミス・クラウド)で管理する場合に、オンプレミス専用 PC を設定することができます。InfoBanker(オンプレミス・クラウド)で管理する場合、InfoBanker(オンプレミス・クラウド)の両方のサーバを確認するため、セキュリティ USB/HDD の起動が遅くなる場合があります。

指定した条件を満たす PC では、InfoBanker(オンプレミス)のみを確認することにより、セキュリティ USB/HDD の起動を高速化することができます。

※セキュリティ USB/HDD のソフトウェアバージョンが ver417 以上である必要があります。

□ オンプレミス専用 PC 設定運用イメージ

指定したファイル/フォルダ/レジストリキー/MAC アドレス/IP アドレス/ワークグループ/ドメインが存在する PC では、InfoBanker(オンプレミス)のみを確認し、InfoBanker(クラウド)を確認しません。

InfoBanker(オンプレミス)サーバの条件を設定しておくことにより、セキュリティ USB/HDD の起動を高速化することができます。

オンプレミス専用 PC 設定

オンプレミス専用PC設定

InfoBanker (オンプレミス)接続のみを使用するPCを設定します。
セキュリティUSB/HDDの起動を高速化するため
設定されたPCではInfoBanker(クラウド)にアクセスしません。

オンプレミス専用PC判定条件

AND方式 OR方式 AND + OR方式

ファイル/フォルダ/レジストリキー/IPアドレス(IP:)/MACアドレス(MAC:)/ワークグループ(DN:)/ドメイン名(DN:)を実行キーとして設定可能です
IPアドレス以降の実行キーを入力する場合、実行キーの前に()の値を追記してください。 例: MAC:11-22-33-44-55-66

AND方式

この設定項目がPC上に全て存在する場合、InfoBanker (オンプレミス)のみを使用します。設定値は99個まで設定可能です。

設定値		追加する	削除する
-----	--	------	------

OR方式

この設定項目の内一つでもPCに存在する場合、InfoBanker (オンプレミス)のみを使用します。設定値は99個まで設定可能です。

c:\¥12345.txt			
IP:128.1.105.1-128.1.105.3			
IP:192.168.1.220			
MAC:11-22-33-44-55-66			

設定値		追加する	削除する
-----	--	------	------

OK キャンセル

□ オンプレミス専用 PC 判定設定方法

1: オンプレミス専用 PC 判定条件とは設定値がどの様に存在した時にオンプレミス専用 PC と判定するかを決定する方式です。判定条件には以下の AND 方式、OR 方式、AND+OR 方式があります。お客様の都合のよい方法を選択してください。

方式	[1]AND 方式	[2]OR 方式
内容	<p>設定項目が”全て” PC に存在する場合に、InfoBanker(オンプレミス)のみを使用します。</p> <p>例： 設定 1 : C:\¥file1.bin・・・ファイル 設定 2 : C:\¥folder1・・・フォルダ 設定 3 : HKEY_CURRENT_USER¥Software¥TEST¥TEST1・・・レジストリキー</p> <p>PC 内に設定 1, 2, 3”全て”存在する場合、InfoBanker(オンプレミス)のみを使用します。</p>	<p>設定項目の中で1つでも該当設定が存在する場合に、InfoBanker(オンプレミス)のみを使用します。</p> <p>例： 設定 1 : C:\¥file2.bin・・・ファイル 設定 2 : C:\¥folder2・・・フォルダ 設定 3 : HKEY_CURRENT_USER¥Software¥TEST¥TEST2・・・レジストリキー</p> <p>PC 内に設定 1, 2, 3の内、“最低一つ”存在する場合、InfoBanker(オンプレミス)のみを使用します。</p>
設定項目	最大 99 個	最大 99 個
使用用途	特定のファイル、フォルダ、レジストリキーなどを設定できる場合。	IP アドレスなど、一定の範囲内のどれかを指定したい場合。

AND+OR 方式は AND 条件と OR 条件両方を満たす場合、InfoBanker(オンプレミス)のみを使用する方式です。

2: 方式を決定しましたら、設定値を登録します。[設定値]欄へ設定値を入力し、[追加する]ボタンを押してください。設定値は最大 99 個まで登録可能です。追加した条件を削除したい場合は、項目を選択し、[削除する]ボタンを押してください。

AND方式

この設定項目がPC上に全て存在する場合、InfoBanker (オンプレミス)のみを使用します。設定値は99個まで設定可能です。

設定値

OR方式

この設定項目の内一つでもPCに存在する場合、InfoBanker (オンプレミス)のみを使用します。設定値は99個まで設定可能です。

c:\¥12345.txt	
IP:128.1.105.1-128.1.105.3	
IP:192.168.1.220	
MAC:11-22-33-44-55-66	

設定値

□ 設定値について

設定値は以下を設定することができます。

- ファイル/フォルダの有無
- レジストリキーの有無
- MAC アドレス
- IP アドレス
- ドメイン
- ワークグループ

オンプレミス専用 PC 判定条件(AND 方式/OR 方式)に合わせて、[設定値]枠へ設定値を入力し、[追加する]ボタンを押してください。

AND方式
この設定項目がPC上に全て存在する場合、InfoBanker (オンプレミス)のみを使用します。設定値は99個まで設定可能です。

設定値		追加する	削除する
-----	--	------	------

OR方式
この設定項目の内一つでもPCに存在する場合、InfoBanker (オンプレミス)のみを使用します。設定値は99個まで設定可能です。

c:¥12345.txt	
IP:128.1.105.1-128.1.105.3	
IP:192.168.1.220	
MAC:11-22-33-44-55-66	

設定値		追加する	削除する
-----	--	------	------

■ **ファイル/フォルダ設定**

使用する PC 内に指定したファイル/フォルダが存在するかで判定します。

[設定例]

判定に使用するファイルを設定する場合、ファイル保存場所のフルパスを設定してください。

例：C:¥test¥test フォルダ下の test.bin ファイルを認証ファイルにする場合、設定項目へ以下を入力します。
C:¥test¥test¥test.bin

[上級者向け設定]

環境設定を使用し、設定することができます。ユーザ名などフルパス内のフォルダに入っている場合等にご使用ください。

例：C:¥Documents and Settings¥user1¥test¥test.bin を設定する場合
※ PC のログインユーザによって user1 が user2 などに変わります。

設定例：%USERPROFILE%¥test¥test.bin

■レジストリキー設定

使用する PC 内に指定されたレジストリキーが存在するかで判定します。レジストリキーをルートからすべて設定してください。

[設定例]

例：HKEY_CURRENT_USER¥Software¥TEST¥TEST2

■MAC アドレス設定

使用する PC の MAC アドレスが指定した MAC アドレスと一致するかで判定します。

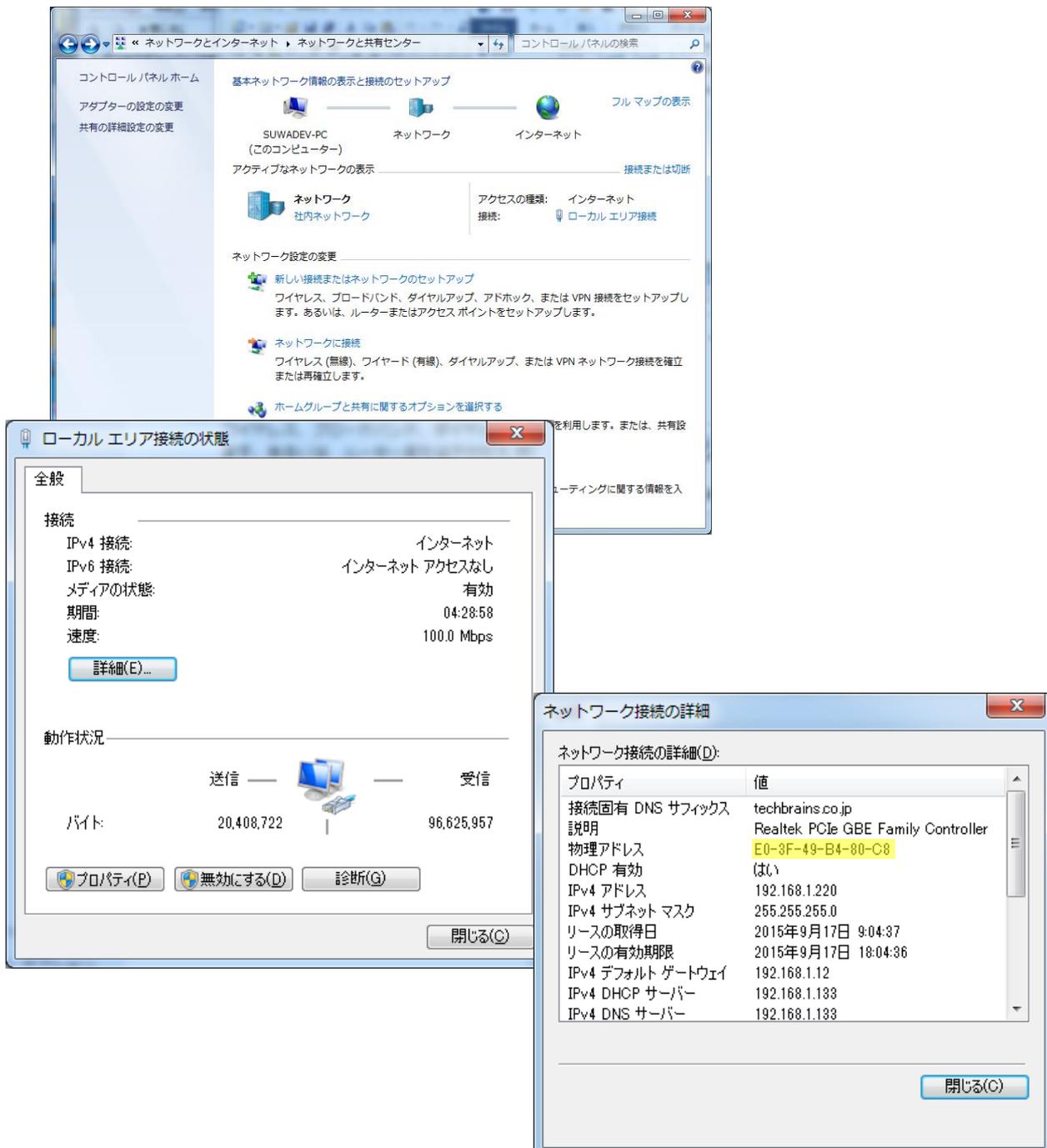
MAC アドレスの先頭に "MAC:" を付けて設定をしてください。

[設定例]

例 MAC:11-22-33-44-55-66

[PC の MAC アドレスの確認方法]

コントロールパネル→ネットワークとインターネット→ネットワークと共有センター→アクティブなネットワークの表示からローカルエリア接続を選択→詳細ボタン 物理アドレスとして表示されています。



■IP アドレス設定

使用する PC の IP アドレスが指定した IP アドレスと一致するかで判定します。

IP アドレスの先頭に "IP:" を付けて設定をしてください。

IPv4 のみ対応しております。IPv6 には対応しておりません。

[設定例]

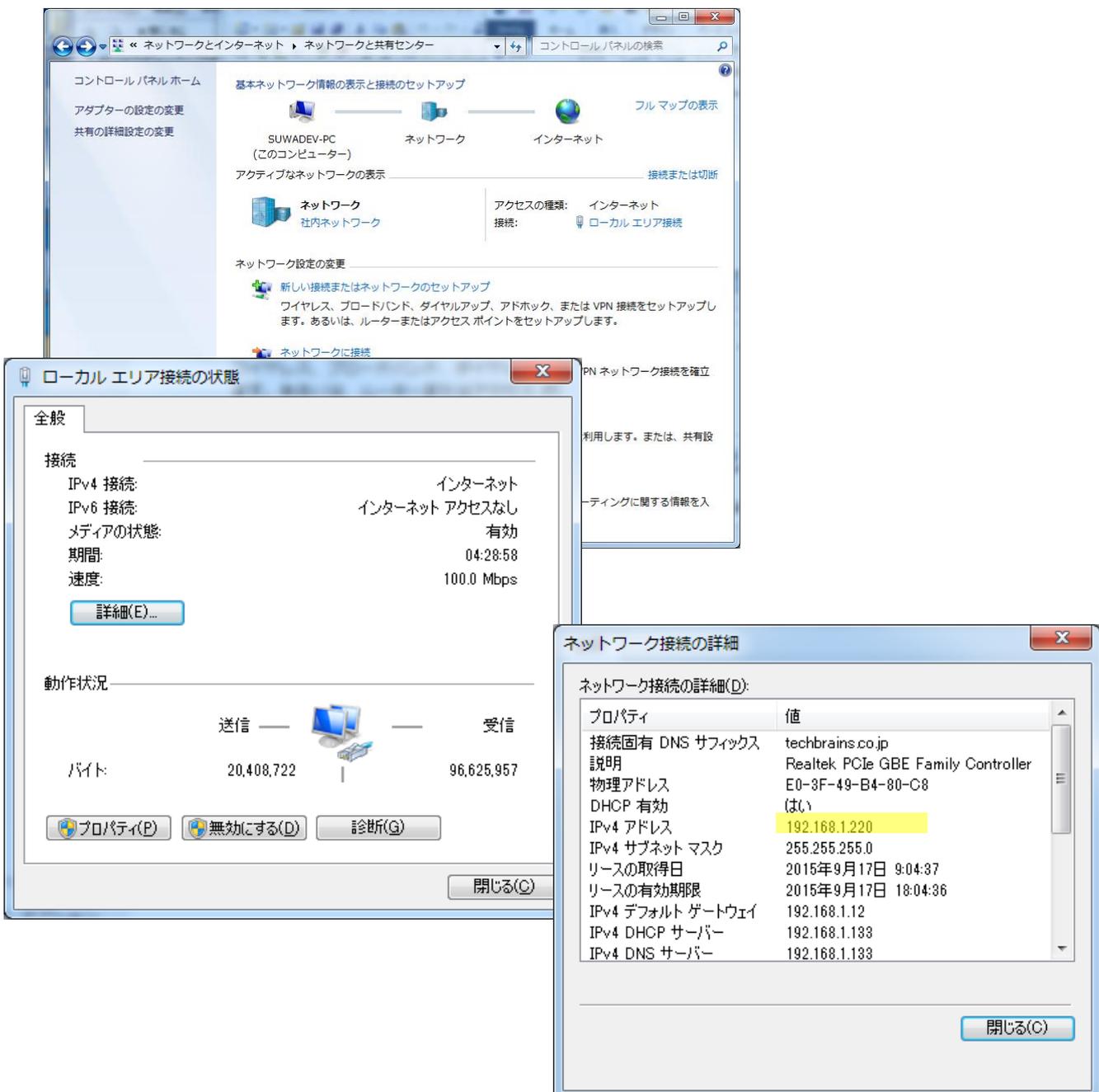
例 IP:192.168.1.220

範囲指定や、サブネットマスクでの設定も可能です。

- 範囲指定例：128.1.105.1-128.1.105.3 や 128.1.121.1-128.1.125.255
- サブネットマスク例：198.51.100.0/24

[PC の IP アドレスの確認方法]

コントロールパネル→ネットワークとインターネット→ネットワークと共有センター→アクティブなネットワークの表示からローカルエリア接続を選択→詳細ボタン IPv4 アドレスとして表示されています。



■ドメイン設定

使用するPCのドメインが指定したドメインと一致するかで判定します。
ドメインの先頭に "DN:"を付けて設定をしてください。

[設定例]

例 DN:hagisol.co.jp

[PCのドメインの確認方法]

コマンドプロンプトで、『nbtstat -n』と打ち込んで表示される、NetBIOS ローカルネームテーブルで、種類がグループとして表示されている行の名前の部分が、NetBIOS ドメイン名です。

■ワークグループ設定

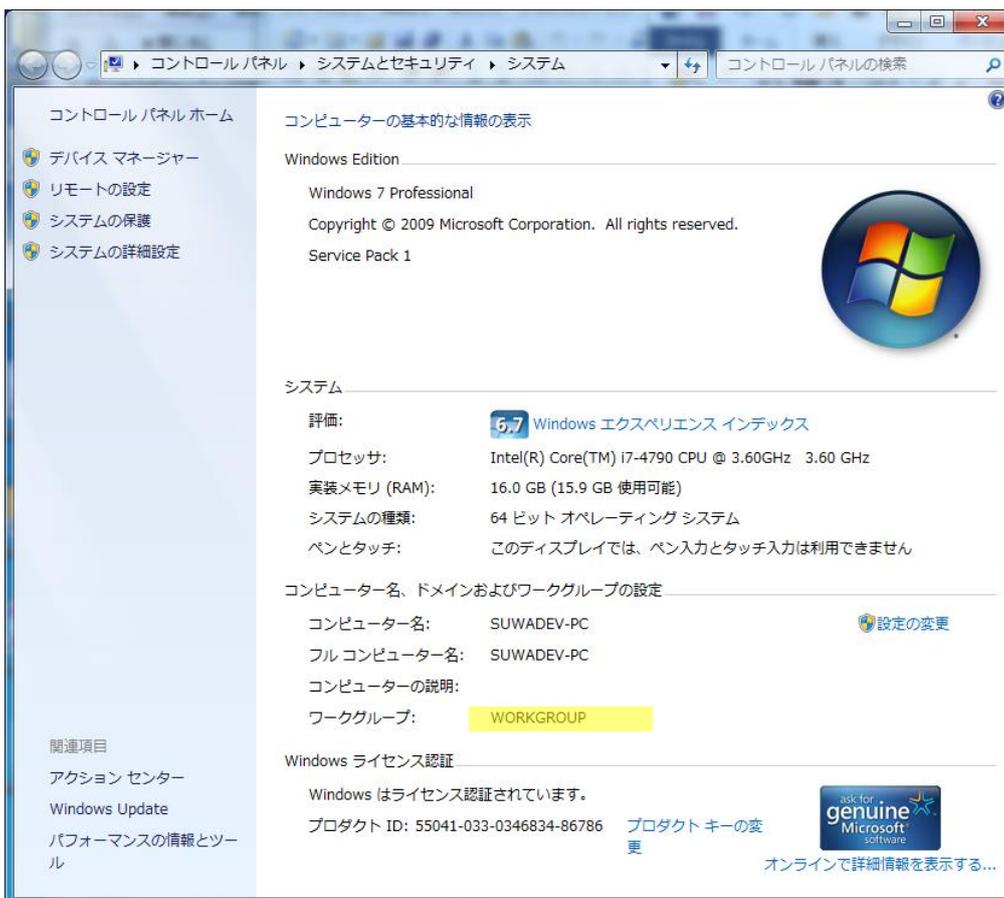
使用するPCのワークグループが指定したワークグループと一致するかで判定します。
ワークグループの先頭に "DN:"を付けて設定をしてください。

[設定例]

例 DN:WORKGROUP

[PCのワークグループの確認方法]

コントロールパネル→システムとセキュリティ→システムで表示されるワークグループ名



■ 認証機能の動作

認証機能を追加した場合の動作パターンを記載致します。お客様には 4-4 の設定をして頂く必要がございます。
 セキュリティ USB/HDD 側の設定と共に、InfoBanker 側の設定も必要となります。
 認証キー：セキュリティ USB Manager でセキュリティ USB/HDD に付けた認証キー

[1]

InfoBanker バージョン：1.1.0.1 以前(認証機能無し)
 セキュリティ USB/HDD：ver404 以前(認証機能無し)

No	InfoBanker 認証機能	InfoBaker 認証キー	セキュリティUSB/HDD 認証機能	セキュリティUSB/HDD 認証キー	InfoBanker ログ受信
1-1	機能無し		機能無し	X(何でも)	可

[2]

InfoBanker バージョン：1.1.0.1 以前(認証機能無し)
 セキュリティ USB/HDD：ver405 以降(認証機能有り)

No	InfoBanker 認証機能	InfoBaker 認証キー	セキュリティUSB/HDD 認証機能	セキュリティUSB/HDD 認証キー	InfoBanker ログ受信
2-1	機能無し		無効	X(何でも)	可
2-2	機能無し		有効	X(何でも)	不可 送信失敗でSecurityUSB/HDD 内にログ保持されます。

[3]

InfoBanker バージョン：1.2.0.0 以降(認証機能有り)
 セキュリティ USB/HDD：ver404 以前(認証機能無し)

No	InfoBanker 認証機能追加	InfoBaker 認証キー	セキュリティUSB/HDD 認証機能	セキュリティUSB/HDD 認証キー	InfoBanker ログ受信
3-1	無効	無し	機能無し	X(何でも)	可
3-2	有効	X(何でも)	機能無し	X(何でも)	不可 送信失敗でSecurityUSB/HDD 内にログ保持されます。

[4]

InfoBanker バージョン：1.2.0.0 以降(認証機能有り)
 セキュリティ USB/HDD：ver405 以降 S(認証機能有り)

No	InfoBanker 認証機能追加	InfoBaker 認証キー	セキュリティUSB/HDD 認証機能	セキュリティUSB/HDD 認証キー	InfoBanker ログ受信
4-1	無効	無し	無効	X(何でも)	可
4-2	無効	無し	有効	X(何でも)	可
4-3	有効	A	無効	X(何でも)	不可 送信失敗でSecurityUSB/HDD 内にログ保持されます。
4-4	有効	A	有効	A	可
4-5	有効	A	有効	B	不可 送信失敗でSecurityUSB/HDD 内にログ保持されます。

- Info Banker からの配信設定
- 遠隔消去設定
- ソフトウェア配信設定(オンプレミスのみ)

ホスト名(オンプレミスのみ)
InfoBankerをインストールしたサーバのホスト名またはIPアドレスを例のhostへ入力してください。

InfoBanker URL1
例: http://host/InfoBanker/

InfoBanker URL2
例: http://host/InfoBanker/

遠隔消去設定
InfoBankerを使用し、セキュリティUSBを遠隔からデータ消去/使用停止することができます。セキュリティUSBの不正利用時、退職予定者のセキュリティUSBに対してご利用ください。
※本機能を有効にした場合、MacOSX上でセキュリティUSBが使用できなくなります。

遠隔消去/停止機能を有効にする

定期接続確認
InfoBankerへ定期的に接続しない場合、セキュリティUSBの使用停止を行うことができます。使用停止後、再度InfoBankerへ接続すると、再利用することができます。セキュリティ強化する場合、ご使用ください。

InfoBankerへの定期接続確認をしない
 InfoBanker(オンプレ)への定期接続確認をする
 InfoBanker(オンプレミス及びクラウド)への定期接続確認をする

接続確認間隔 日

定期接続できない場合、製品を初期化する

ソフトウェア配信設定(オンプレミスのみ)
 ソフトウェア配信を有効にする

項目	内容
Info Banker のホスト名 (オンプレミスのみ)	<p>ログ管理ソフト(Info Banker)から送信するか設定することができます。 InfoBanker を2箇所へ導入している場合、2つのIPアドレスを入力してください。最初に見つかったIPアドレスのInfoBanker から配信を行います。</p> <p>[標準設定]Info Banker へログを送信しない [設定方法] Info Banker がインストールされているサーバのIPアドレスを選択してください。</p>
遠隔消去	<p>InfoBanker を使用し、遠隔からセキュリティUSB/HDD のデータ消去、利用停止を設定することができます。また定期的に InfoBanker への接続確認し指定間隔内に接続しない場合、使用停止、初期化するオプション[定期接続確認]もご用意しています。</p> <p>[標準設定]遠隔消去機能を使用しない [設定方法] 遠隔消去機能を使用する場合、「遠隔消去機能を有効にする」へチェックを入れてください。</p> <p>注意: 本機能を有効にすると仕様上 Mac OS X でセキュリティ USB/HDD の使用が制限されます。</p>
ソフトウェア配信設定 (オンプレミスのみ)	<p>InfoBanker からセキュリティ USB/HDD へソフトウェア配信をすることができます。 この設定を有効にした場合、InfoBanker のソフトウェア更新のみを確認し、インターネット上のソフトウェア更新は確認しません。</p> <p>[標準設定]ソフトウェア配信を有効にしない [設定方法] 機能を使用する場合、「ソフトウェア配信を有効にする」へチェックを入れてください。</p>

クラウド管理

クラウド管理タブでは Info Banker クラウドへのログ送信・管理設定を行うことができます。本ソフトウェアを起動し、タブ[クラウド管理]を開いてください。

注意；クラウド機能を使用する場合、クラウドサービスへの情報送信や情報取得は Windows10 以上の OS が必要です。

弊社推奨はタブ：デバイスで使用 OS 制限を掛けて頂くことになります。

制限を掛ける OS：Windows2000/XP/Vista/2003R2/2003/XP Embedded

・Info Banker クラウドのログ送信・管理設定

※本設定を有効にするには、タブ：ログ管理で「InfoBanker Cloud でログ管理する」を選択してください。

※セキュリティ USB/HDD のソフトウェアバージョンが ver410 以上である必要があります。

本設定を有効にするには、タブ：ログ管理画面で「InfoBanker Cloudでログ管理する」を選択してください。

InfoBanker Cloudアカウント設定

InfoBanker Cloudを使用するにはアカウント情報の登録が必要です。
InfoBanker Cloudの申込みを行い、アカウントファイルを手入力してください。

C:\IbcAccInfo.bin 参照...

アカウント設定状態： 未設定 設定保存

ログ設定

通常ログ/ウイルスログを送信しない 通常ログ/ウイルスログを送信する

欄卸ログ

欄卸ログを送信しない 欄卸ログを送信する

送信月設定

1月 2月 3月 4月 5月 6月
 7月 8月 9月 10月 11月 12月

欄卸時に通知するメッセージを設定してください(最大全角120文字)

ファイル操作ログ

ファイル操作ログを送信しない ファイル操作ログを送信する

PC情報送信

PC情報を送信する PC情報を送信しない

PC情報とはMACアドレス、IPアドレス等を含むPCを特定できる情報全てです。

遠隔消去設定

InfoBankerを使用し、セキュリティUSBを遠隔からデータ消去/使用停止することができます。セキュリティUSBの不正利用時、退職予定者のセキュリティUSBに対してご利用ください。
※本機能を有効にした場合、MacOSX上でセキュリティUSBが使用できなくなります。

遠隔消去/停止機能を有効にする

定期接続確認

InfoBankerへ定期的に接続しない場合、セキュリティUSBの使用停止を行うことができます。使用停止後、再度InfoBankerへ接続すると、再利用することができます。セキュリティ強化する場合、ご使用ください。

InfoBankerへの定期接続確認をしない InfoBankerへの定期接続確認をする

接続確認間隔 日

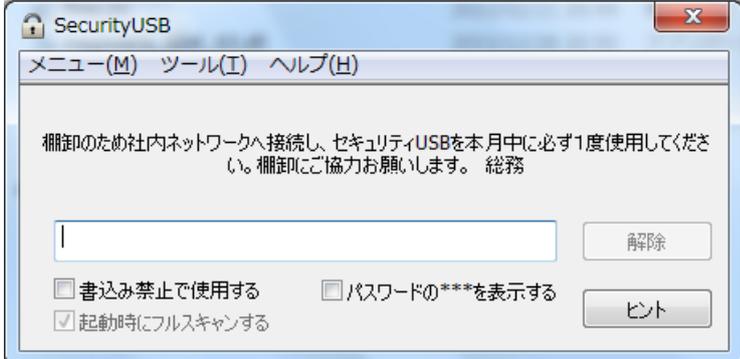
ポリシー配信設定

InfoBankerを使用し、遠隔からセキュリティUSBのポリシーをアップデートすることができます。セキュリティUSBに付けたポリシーバージョンより新しいバージョンがある場合、ポリシーは更新されます。よってポリシーの初期値は「000」推奨です。

遠隔ポリシー配信を有効にする

ポリシーバージョン

項目	内容
Info BankerCloud アカウント設定	InfoBanker Cloud へ申し込んで頂くと、弊社からお客様のアカウントと紐付いたアカウントファイル(lbcAccInfo.bin)をお送りします。 参照ボタンを押し、アカウントファイルを選択してください。設定保存ボタンを押すと、アカウント情報が SecurityUSB へ保存され、クラウドサービスで管理が可能になります。
ログ設定	デバイスから Info Banker Cloud へ通常ログ/ウイルスログを送信するか設定することができます。 [標準設定]通常ログ/ウイルスログを送信する [設定方法] Info BankerCloud へ送信しない場合、[通常ログ/ウイルスログを送信しない]を選択してください。

<p>棚卸ログ</p>	<p>デバイスからログ管理ソフト(Info Banker Cloud)へ棚卸ログを送信するか設定することができます。</p> <p>[標準設定]棚卸ログを送信しない [設定方法] Info BankerCloud へ棚卸ログを送信する場合、[棚卸ログを送信する]を選択してください。</p> <p>棚卸ログは月に1度のみ送信するログです。送信する月を選択してください。 複数の月も選択可能です。また棚卸ログ送信を促すためのメッセージも表示可能です。 例：棚卸のため社内ネットワークへ接続し、セキュリティUSB/HDDを本月中に必ず1度使用してください。棚卸にご協力をお願いします。 情報ネットワーク部</p> <p>→実際の表示は以下のようになります。</p> 
<p>ファイル操作ログ</p>	<p>ファイル操作ログを InfoBankerCloud へ送信する設定を行います。</p> <p>[標準設定]ファイル操作ログを送信しない [設定方法]InfoBankerCloud へファイル操作ログを送信する場合、「ファイル操作ログを送信する」を選択してください。</p>
<p>PC 情報送信</p>	<p>PC 情報を InfoBanker へ送信する・しないの設定を行います。 PC 情報：MAC アドレス/IP アドレス等</p> <p>[標準設定]PC 情報を送信する [設定方法] PC 情報を InfoBanker へ送信しない場合、「PC 情報を送信しない」を選択してください。</p>
<p>遠隔消去</p>	<p>InfoBanker を使用し、遠隔からセキュリティ USB/HDD のデータ消去、利用停止を設定することができます。</p> <p>[標準設定]遠隔消去機能を使用しない [設定方法] 遠隔消去機能を使用する場合、「遠隔消去機能を有効にする」へチェックを入れてください。</p> <p>注意：本機能を有効にすると仕様上 Mac OS X でセキュリティ USB/HDD の使用が制限されます。</p>

実行制限/コピーガード 設定

実行制限/コピーガードで対象デバイスの実行制限設定が可能です。

※コピーガード機能はセキュリティ USB でのみ使用可能です。セキュリティ HDD では使用できません。

■実行制限で出来ること

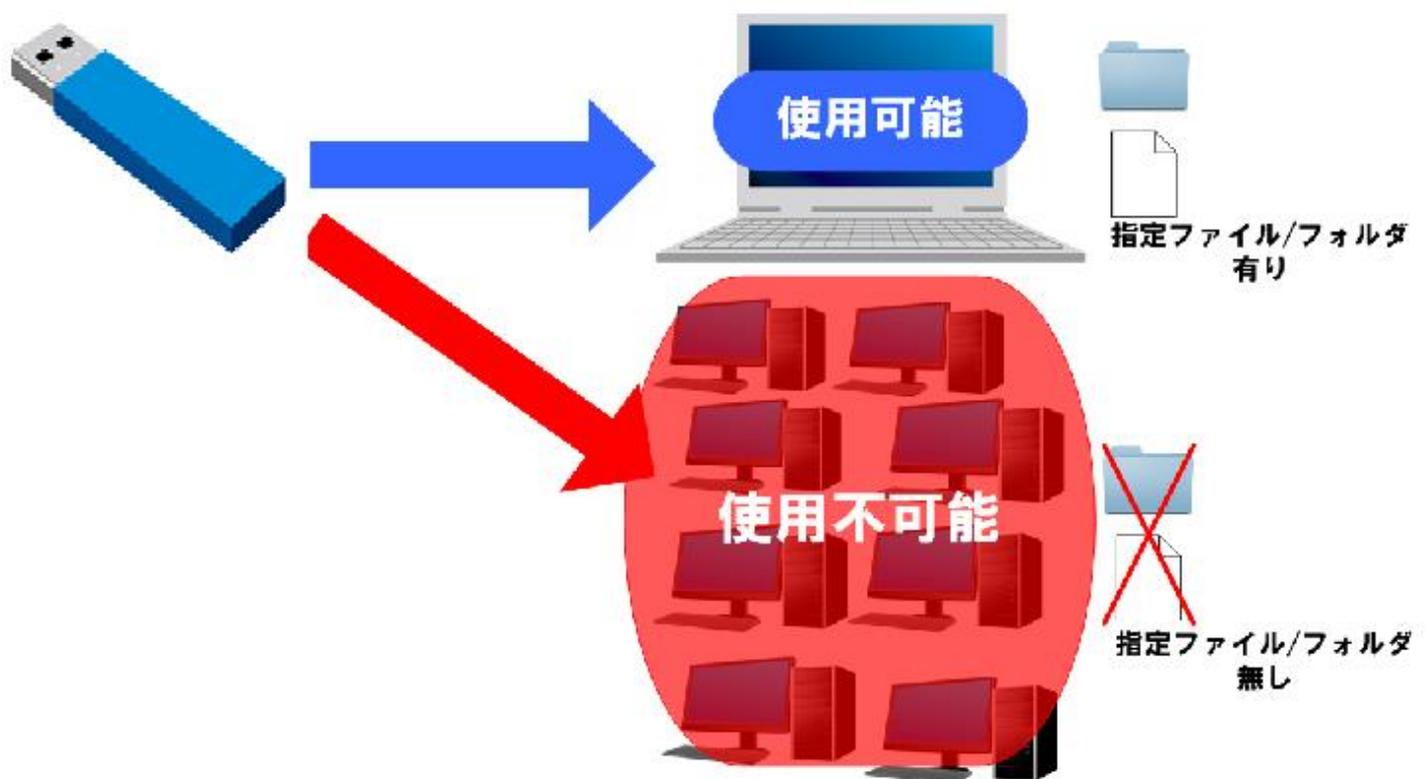
- セキュリティ USB/HDD の実行制限設定：ファイル/フォルダ/レジストリキー/MAC アドレス/IP アドレス/ワークグループ/ドメインの有無によってセキュリティ USB/HDD の実行を制限します。特定の PC のみセキュリティ USB/HDD を実行できる様に制限する時にご使用ください。

注意：本機能を有効にすると仕様上 Mac OS X でセキュリティ USB/HDD の使用が制限されます。

実行制限運用イメージ

指定したファイル/フォルダ/レジストリキー/MAC アドレス/IP アドレス/ワークグループ/ドメインが存在する PC のみ使用可能で、それ以外の PC では使用できません。

社内 PC のみにあるファイル/フォルダ/レジストリキー/MAC アドレス/IP アドレス/ワークグループ/ドメインを設定し、社内 PC のみ使用可能にするのが通常の運用方法となります。



■実行制限の流れ

[管理者]

① セキュリティ USB/HDD の利用を許可する PC を決定する。例；社内の PC、特定部署の PC

利用許可するPC



The illustration shows a manager on the left. In the center, there are several laptops. A blue-bordered box encloses six of these laptops, with the text '利用許可するPC' (PCs to be permitted for use) written above it. To the right of this box is a desktop computer.

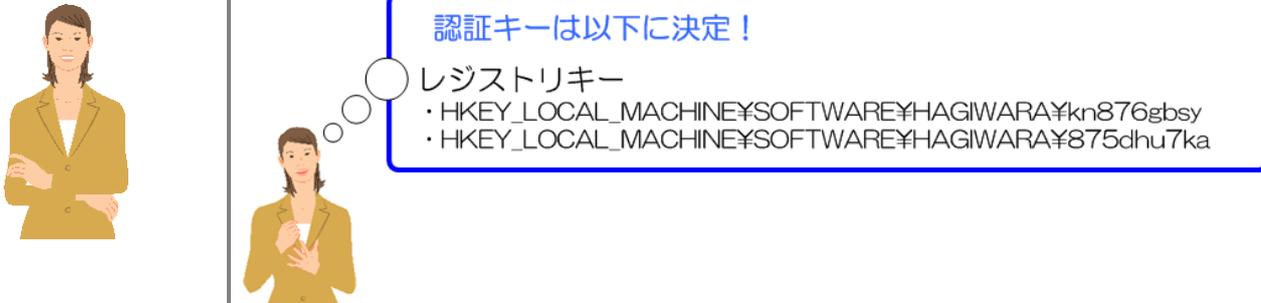
[管理者]

②：利用許可する PC に認証キーとして使用する固有のファイル/フォルダ/レジストリキー/MAC アドレス/IP アドレス/ワークグループ/ドメインを作成/登録する。

認証キーは以下に決定！

レジストリキー

- ・ HKEY_LOCAL_MACHINE¥SOFTWARE¥HAGIWARA¥kn876gbsy
- ・ HKEY_LOCAL_MACHINE¥SOFTWARE¥HAGIWARA¥875dhu7ka



The illustration shows a manager on the left. To her right is a thought bubble containing the text '認証キーは以下に決定！' (Authentication key is determined as follows!). Below the bubble, it says 'レジストリキー' (Registry key) and lists two registry paths: 'HKEY_LOCAL_MACHINE¥SOFTWARE¥HAGIWARA¥kn876gbsy' and 'HKEY_LOCAL_MACHINE¥SOFTWARE¥HAGIWARA¥875dhu7ka'.

[管理者]

② ②で決定した認証キーをセキュリティ USB/HDD の利用許可する PC へ登録/コピーしてください。登録/コピー方法はお客様が決定、実行願います。予め利用許可する PC に認証キーがある場合は登録/コピーを行う必要はありません。

認証キー

レジストリキー

- ・ HKEY,,,¥HAGIWARA¥kn876gbsy
- ・ HKEY,,,¥HAGIWARA¥875dhu7ka

登録

利用許可するPC



The illustration shows a manager on the left. In the center, there is a box labeled '認証キー' (Authentication key) containing the text 'レジストリキー' (Registry key) and the same two registry paths as in the previous step. A blue arrow labeled '登録' (Registration) points from this box to a blue-bordered box on the right labeled '利用許可するPC' (PCs to be permitted for use), which contains six laptops.

2：次に実行条件方式を決定します。実行条件方式とは認証キーをどの様に存在した時にセキュリティ USB/HDD の実行を許可するかを決定する方式です。実行条件には以下の AND 方式、OR 方式、AND+OR 方式があります。お客様の都合のよい方法を選択してください。

方式	[1]AND 方式	[2]OR 方式
内容	設定項目が”全て” PC に存在する場合にセキュリティ USB/HDD が使用可能になる設定です。 例： 設定 1：C:\¥file1.bin・・・ファイル 設定 2：C:\¥folder1・・・フォルダ 設定 3： HKEY_CURRENT_USER¥Software¥TEST¥TEST1・・・レジストリキー PC 内に設定 1, 2, 3”全て”存在する場合、セキュリティ USB/HDD が実行可能になります。	設定項目の中で1つでも該当設定が存在する場合にセキュリティ USB/HDD が使用可能になる設定です。 例： 設定 1：C:\¥file2.bin・・・ファイル 設定 2：C:\¥folder2・・・フォルダ 設定 3： HKEY_CURRENT_USER¥Software¥TEST¥TEST2・・・レジストリキー PC 内に設定 1, 2, 3の内、“最低一つ”存在する場合、セキュリティ USB/HDD が実行可能になります。
設定項目	最大 5000 個※	最大 5000 個※
使用用途	特定のファイル、フォルダ、レジストリキーなどを全 PC に設定できる場合。 例：全 PC をアクティブディレクトリで管理している、新規に PC を調達した場合など	PC 内のファイル、フォルダ、レジストリキー構成を変更できない、また共通のファイル等がない場合。 例：PC の回収が難しい場合など

※注意：USB2.0 モデルと USB3.0 モデルのバージョン 400 以前は最大 15 個まで対応となっております。

AND+OR 方式は AND 条件と OR 条件両方を満たす場合、セキュリティ USB/HDD が実行可能になる方式です。

3：方式を決定しましたら、認証キーを登録します。[設定値]欄へ認証キーを入力し、[追加]ボタンを押してください。

認証キーは最大 99 個まで登録可能です。

追加した条件を削除した場合は、項目を選択し、(削除する)ボタンを押してください。

[一括設定]からは認証キー情報を記載したファイルを一括で読み込ませることができます。最大 5000 個まで登録可能です。

AND方式

この設定項目がPC上に全て存在する場合、セキュリティUSBを実行できます。
または、この設定項目がPC上に全て存在する場合、オフィスモードで動作します。

設定値

OR方式

この設定項目の内一つでもPCに存在する場合、セキュリティUSBを実行できます。
または、この設定項目の内一つでもPCに存在する場合、オフィスモードで動作します。

c:\¥12345.txt

MAC:11-22-33-44-55-66

IP:128.1.105.1-128.1.105.3

IP:192.168.1.220

設定値

認証キーの設定

認証値としては以下を設定することができます。

- ファイル/フォルダの有無
- レジストリキーの有無
- MAC アドレス
- IP アドレス
- ドメイン
- ワークグループ

認証条件(AND/OR)に合わせて、[設定値]枠へ認証値を入力し、[追加する]ボタンを押してください。画面上では最大 99 個まで登録可能です。99 個以上登録する場合、[一括設定]ボタンを押して、テキスト形式で登録をしてください。最大 5,000 個まで登録可能です。

The screenshot shows two sections for setting authentication keys. The top section is titled 'AND方式' (AND mode) and contains the text: 'この設定項目がPC上に全て存在する場合、セキュリティUSBを実行できます。または、この設定項目がPC上に全て存在する場合、オフィスモードで動作します。' Below this text is a large empty text box for input. At the bottom of this section are three buttons: '設定値' (Setting value), '追加する' (Add), and '削除する' (Delete), along with a '一括設定' (Batch setting) button. The bottom section is titled 'OR方式' (OR mode) and contains the text: 'この設定項目の内一つでもPCに存在する場合、セキュリティUSBを実行できます。または、この設定項目の内一つでもPCに存在する場合、オフィスモードで動作します。' Below this text is a table with four rows of example values: 'c:\¥12345.txt', 'MAC:11-22-33-44-55-66', 'IP:128.1.105.1-128.1.105.3', and 'IP:192.168.1.220'. At the bottom of this section are three buttons: '設定値' (Setting value), '追加する' (Add), and '削除する' (Delete), along with a '一括設定' (Batch setting) button.

■ファイル/フォルダ設定

使用する PC 内に指定したファイル/フォルダが存在するかで判定します。

[設定例]

認証に使用するファイルを設定する場合、ファイル保存場所のフルパスを設定してください。

例：C:\¥test¥test フォルダ下の test.bin ファイルを認証ファイルにする場合、設定項目へ
C:\¥test¥test¥test.bin

[上級者向け設定]

環境設定を使用し、設定することができます。ユーザ名などフルパス内のフォルダに入っている場合等にご使用ください。

例：C:\¥Documents and Settings¥user1¥test¥test.bin を設定する場合

※ PC のログインユーザによって user1 が user2 などに変わります。

設定例：%USERPROFILE%\¥test¥test.bin

■レジストリキー設定

使用する PC 内に指定されたレジストリキーが存在するかで判定します。レジストリキーをルートからすべて設定してください。

[設定例]

例：HKEY_CURRENT_USER¥Software¥TEST¥TEST2

■MAC アドレス設定

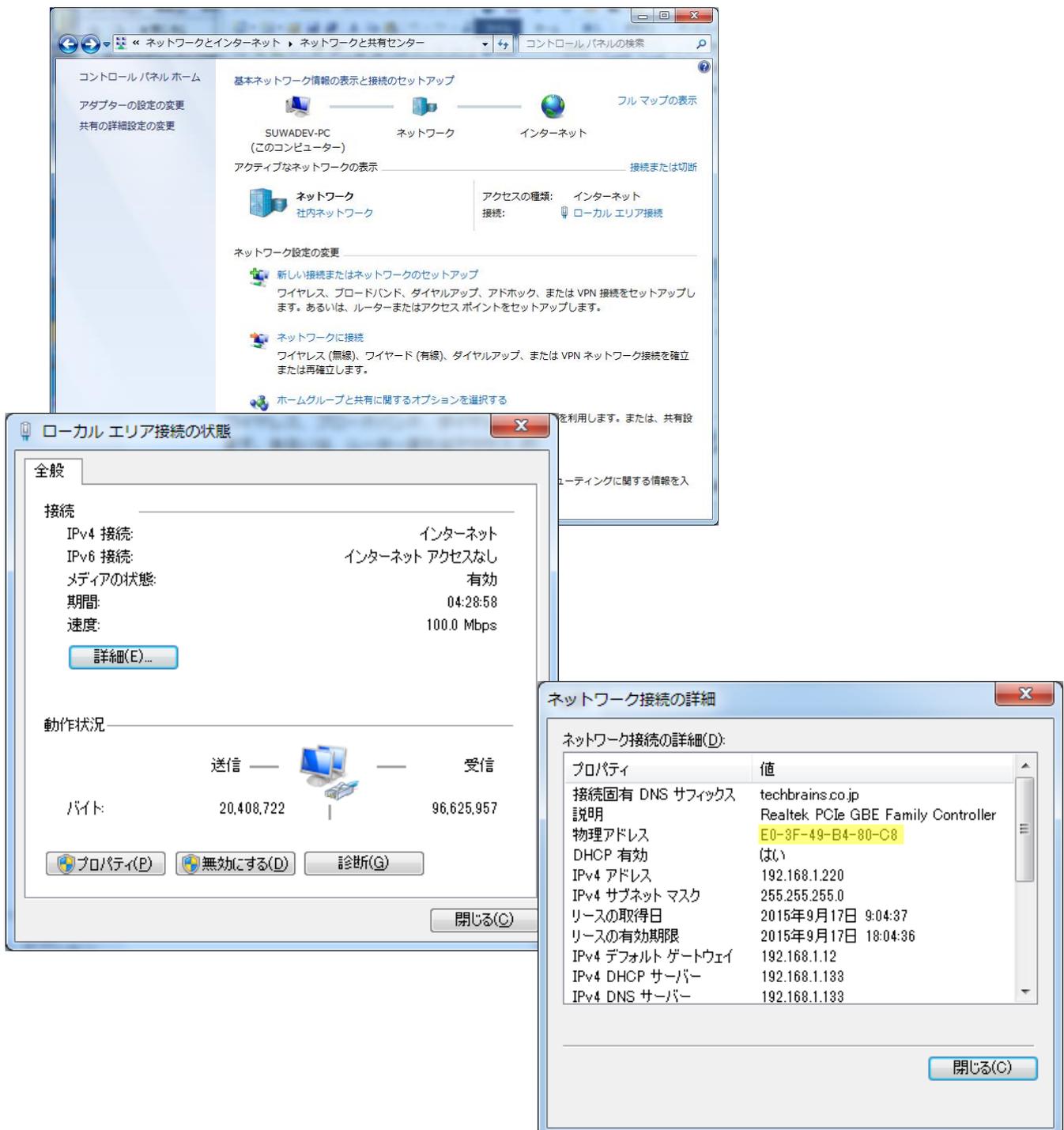
使用する PC の MAC アドレスが指定した MAC アドレスと一致するかで判定します。
MAC アドレスの先頭に "MAC:" を付けて設定をしてください。

[設定例]

例 MAC:11-22-33-44-55-66

[PC の MAC アドレスの確認方法]

コントロールパネル→ネットワークとインターネット→ネットワークと共有センター→アクティブなネットワークの表示からローカルエリア接続を選択→詳細ボタン 物理アドレスとして表示されています。



■IP アドレス設定

使用する PC の IP アドレスが指定した IP アドレスと一致するかで判定します。

IP アドレスの先頭に "IP:" を付けて設定をしてください。

IPv4 のみ対応しております。IPv6 には対応しておりません。

[設定例]

例 IP:192.168.1.220

範囲指定や、サブネットマスクでの設定も可能です。

- 範囲指定例：128.1.105.1-128.1.105.3 や 128.1.121.1-128.1.125.255
- サブネットマスク例：198.51.100.0/24

[PC の IP アドレスの確認方法]

コントロールパネル→ネットワークとインターネット→ネットワークと共有センター→アクティブなネットワークの表示からローカルエリア接続を選択→詳細ボタン IPv4 アドレスとして表示されています。

The image shows a Windows Control Panel window titled "ネットワークとインターネット" (Network and Internet) with the "ネットワークと共有センター" (Network and Sharing Center) selected. The "ネットワーク" (Network) section is active, showing "社内ネットワーク" (Corporate Network) as the active network. The "アクセスの種類" (Access type) is set to "インターネット" (Internet) and the "接続" (Connection) is "ローカル エリア接続" (Local Area Connection).

Overlaid on this are two smaller windows:

- ローカル エリア接続の状態** (Local Area Connection Status): Shows connection details for the active network. It indicates IPv4 is connected to the Internet, IPv6 is not, and the connection speed is 100.0 Mbps. It also shows a data transfer graph with 20,408,722 bytes sent and 96,625,957 bytes received.
- ネットワーク接続の詳細** (Network Connection Details): A table showing the configuration for the selected network connection.

プロパティ	値
接続固有 DNS サフィックス	techbrains.co.jp
説明	Realtek PCIe GBE Family Controller
物理アドレス	E0-3F-49-B4-80-C8
DHCP 有効	はい
IPv4 アドレス	192.168.1.220
IPv4 サブネット マスク	255.255.255.0
リースの取得日	2015年9月17日 9:04:37
リースの有効期限	2015年9月17日 18:04:36
IPv4 デフォルト ゲートウェイ	192.168.1.12
IPv4 DHCP サーバー	192.168.1.133
IPv4 DNS サーバー	192.168.1.133

■ドメイン設定

使用する PC のドメインが指定したドメインと一致するかで判定します。
ドメインの先頭に "DN:" を付けて設定をしてください。

[設定例]

例 DN:hagisol.co.jp

[PC のドメインの確認方法]

コマンドプロンプトで、『nbtstat -n』と打ち込んで表示される、NetBIOS ローカルネームテーブルで、種類がグループとして表示されている行の名前の部分が、NetBIOS ドメイン名です。

■ワークグループ設定

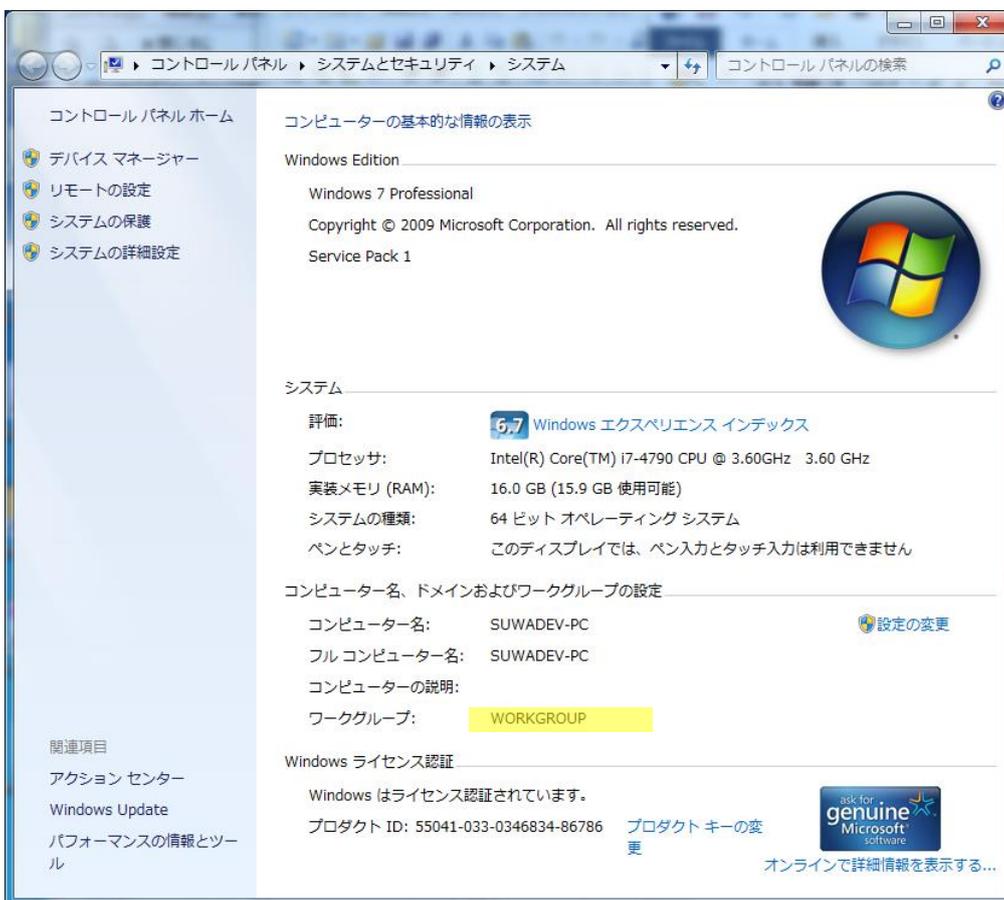
使用する PC のワークグループが指定したワークグループと一致するかで判定します。
ワークグループの先頭に "DN:" を付けて設定をしてください。

[設定例]

例 DN:WORKGROUP

[PC のワークグループの確認方法]

コントロールパネル→システムとセキュリティ→システムで表示されるワークグループ名



認証値についての説明は以上になります。

4.セキュリティ USB/HDD の実行条件を満たした PC 上でのパスワード解除方法の設定を行います。

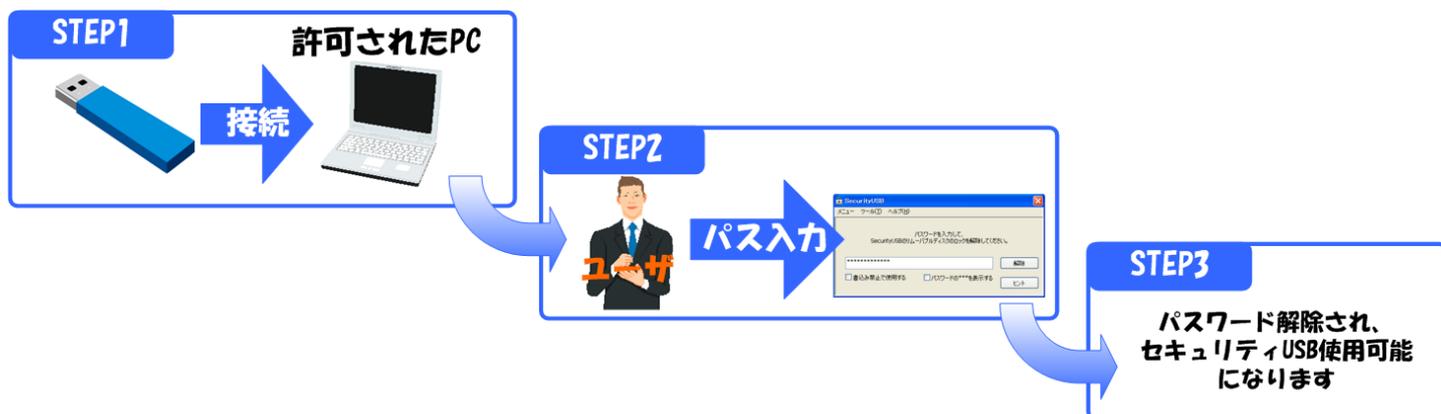
自動パスワード解除設定

自動パスワード解除を行わない 自動パスワード解除を行う

解除方法は2つから選択できます。

① : 自動パスワード解除を行わない

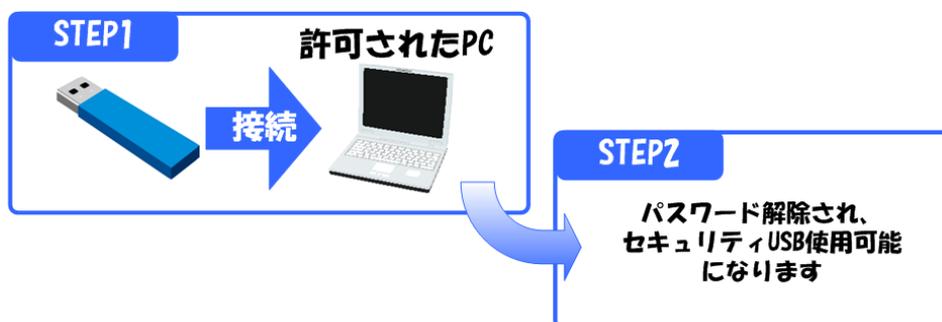
実行条件を満たす PC ではパスワード入力が可能になり、ユーザが毎回パスワードを入力し、セキュリティ USB/HDD を使用可能にします。



② : 自動パスワード解除を行う

実行条件を満たす PC ではセキュリティ USB 自身が自動でパスワード入力しセキュリティ USB/HDD を使用可能にします。ユーザによるパスワードの入力が不要になります。

※ 本設定を行っても、制限が掛かっている PC ではセキュリティ USB/HDD を使用出来ません。



5.セキュリティ USB/HDD の実行条件を満たしていない PC 上でのパスワード解除方法の設定を行います。

制限PCでの起動設定

制限PCでは一切使用させない

制限PCではパスワード入力画面を表示する
(パスワード認証で使用可能)

制限されている PC でパスワード入力を許可する設定ができます。自動パスワード解除設定を[制限 PC ではパスワード入力画面を表示する]へ設定しご使用ください。

※ 制限されている PC でセキュリティ USB/HDD を一切使用させたくない場合、本設定は行わないでください。

コピーガード 設定

タブ：実行制限/コピーガードでコピーガード設定が可能です。

※コピーガード機能はセキュリティ USB でのみ使用可能です。セキュリティ HDD では使用できません。

■コピーガードとは

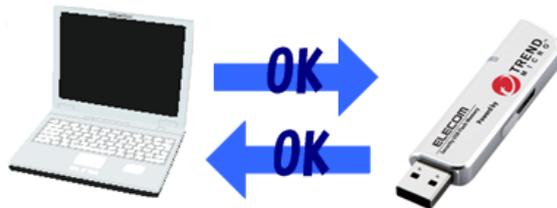
コピーガード機能とは自宅 PC 等で USB メモリ内のファイルを編集する際に、USB メモリから外部にファイル操作を制限する機能です。USB メモリ内であればファイルの編集は可能なため、データの不正流出を防ぎ、社外での作業を可能にします。

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答えします。



オフィスモードで動作

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



モバイルモードで動作

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！

■コピーガードでできること

- ・ 印刷禁止設定
- ・ スクリーンキャプチャ禁止設定
- ・ クリップボード使用禁止設定
- ・ ネットワーク共有フォルダへのアクセス禁止設定
- ・ インターネットアクセス禁止設定
- ・ エンドポイント監視設定
- ・ ファイル操作ログの取得設定※1
- ・ 印刷ログの取得設定

※1：コピーガード無効かつファイル操作ログを有効にした場合も、動作環境は以下のコピーガード動作環境になります。

■コピーガード動作環境

コピーガード機能を有効にした場合、セキュリティ USB とは異なる動作環境となるのでご注意ください。

対応 OS	・ Windows10 (日本語 32bit/64bit) ※1※2
CPU	動作させるために必要な最低 CPU です。さらに低速な CPU でも動作はしますが、使用に支障をきたすおそれがあります。 Intel Pentium M 1.0GHz 以上 (64bit OS の場合、Intel Core Duo 1.66GHz 以上)
メモリ	動作させるために最低必要なメモリ容量です。 1GB 推奨 1.5GB 以上 (64bit OS の場合、2GB 以上)
ハードディスクの空き容量	250MBi 以上
ソフトウェア	動作に必要なソフトウェアです。 Internet Explorer 9/10/11 (WEB アクセス、各種インターネット関連の制御はこのブラウザで動作を保証しています。)

※ 1：Windows ストアアプリは起動しません。

※ 2：モバイルモード終了時、デスクトップの壁紙が消える（黒くなる）ことがあります。

設定が消えてしまっているわけではなく再ログオンすると復旧します。

■コピーガード制限事項

1. コピーガード機能利用後、ログオフ・シャットダウン時にアプリケーションエラーが表示される場合があります。
通常、ユーザプロセスのエラーのため、システムやアプリケーションに重大な異常が発生するものではありません。引き続きご利用いただいても、問題はありません。
2. コピーガード機能利用時、SecurityUSB 以外のアプリケーションを終了させるときにアプリケーションエラーが表示される場合があります。アプリケーションに異常が発生するものではありません。
引き続き利用いただいても、問題はありません。
3. プリンタ・スキャナなどの周辺機器について
モバイルモード中はローカル HDD へのアクセスが制限されるため、プリンタやスキャナ等の周辺機器が正常に動作しない場合があります。
4. 日本語変換ソフトウェアについて
モバイルモードでサポートしている日本語変換ソフトウェアは、OS 付属の日本語変換ソフトウェア (MS-IME)、Microsoft Office (2007、2010、2013) 付属の日本語変換ソフトウェア、ATOK (2011~2013) となります。
ローカル HDD の書き込み制御の影響で、ユーザー辞書やオプションの辞書は利用できない場合があります。
 - Google IME、Baidu IME、ATOK スマイル等はサポートしていません。
ユーザー辞書機能が利用できないなど、動作に制限が発生する場合があります。
5. 「Windows ストアアプリ」の動作をサポートしていません。
拡張子に関連付けられたアプリケーションが Windows ストアアプリに設定されている環境ではファイルが実行されません。予め、拡張子の関連付けをデスクトップアプリケーションに設定してご利用ください。
(PDF の閲覧は Adobe Reader をご利用ください。)
6. ユーザー切り替えは、ご利用頂けません。
7. 一部のウイルス対策ソフトで、コピーガード機能の動作に対して警告と動作制限が加えられる場合があります。
SecurityUSB のプログラムモジュールを除外設定することで回避できる場合があります。
8. SecurityUSB メモリを利用中に Windows が休止/スリープ状態になると、休止/スリープ状態からの復帰時、専用 USB メモリが切り離されていて、動作中のアプリケーションなどが誤動作する場合があります。
SecurityUSB メモリの利用中は、休止/スリープ状態にならないようにしてください。
9. 他社の暗号化ソフトウェア・ログ取得ソフトウェア・デバイス制御ソフトウェアなどが動作している PC では、コピーガード機能が利用している基本技術と競合して、正常に動作しない場合があります。
10. USB 接続ケーブルや、USB ハブを経由して専用 USB メモリを接続すると、正しく動作しないことがあります。このような場合には、USB 接続ケーブルや USB ハブを取り外して、動作が改善するかご確認ください。
11. Office 2007 (IME 2007) を使用中に漢字変換すると Office 2007 が強制終了する場合があります (IME 2007 の不具合です)。
IME 2007 をご利用の場合は、IME 2010 にアップデートしてご利用ください。
(KB938574)
12. コピーガード機能の動作中は、アプリケーションのインストールが正常にできない場合があります。

インターネットアクセス禁止関連の注意・制限事項

1. インターネットアクセス制限を利用したとき、Internet Explorer コンポーネントを利用しているアプリケーションの動作が極端に遅くなる場合があります。
2. Internet Explorer 10 及びそれ以降のバージョンをご利用時に「この Web サイトのセキュリティ証明書には問題があります。」のメッセージが表示されるサイトで閲覧を続行するとページが表示されない場合があります。その際は Internet Explorer の保護モード機能を無効に設定してご利用ください。

モバイルモードでの注意・制限事項

1. モバイルモードは全てのシステム構成での動作を保証するものではありません。一般に利用されるアプリケーションでも、モバイルモードで正常に動作しない場合があります。また、セキュリティ上の理由から、コントロールパネルや管理ツール等の動作も抑止されます。
※ローカル HDD への書き込み制御だけでなく、レジストリや環境変数に対するアクセス制御や内容の一時的な入れ替え、OS システムコール等へのアクセス制御や介入を行っているため、アプリケーションの各種機能が通常通り動作しない場合があります。
2. 動作確認済みのアプリケーションは以下の通りです。括弧内のファイル形式以外のファイルは利用できない場合があります。
 - Microsoft Word 2007/2010/2013/2016 (.doc, .docx のみ)
 - Microsoft Excel 2007/2010/2013/2016 (.xls, .xlsx のみ)
 - Microsoft PowerPoint 2007/2010/2013/2016 (.ppt, .pptx のみ)
 - 一太郎 2011/2012/2013 (.jtd のみ)
 - メモ帳
 - ペイント
 - Adobe Reader 9/X/XI (ドキュメントの表示のみ)
 - Internet Explorer 9/10/11 (ページの閲覧のみ)※アプリケーションの起動・ファイルを開く・閉じる・ファイルの保存・文字の入力といった基本動作以外は、通常時と動作が異なる場合があります。
※上記アプリケーションが標準とは異なる場所にインストールされていると、正常に動作しない場合があります。
※各種アドインがインストールされている環境や、マクロが含まれるファイルの編集・利用時は、正常に動作しない場合があります。
※アドインやマクロの誤動作によって、利用中のファイルが破損・消失する可能性がありますので、適宜バックアップを行うなど、運用にはご注意ください。
※Office2007 以降は 32bit 版での動作確認を行っております。
3. プリンタ・スキャナなどの周辺機器について
モバイルモード中はローカル HDD へのアクセスが制限されるため、プリンタやスキャナ等の周辺機器が正常に動作しない場合があります
4. モード起動中に強制電源断などの方法でコンピューターの電源を落とした場合
コピーガード機能によってユーザー設定情報等が変更されたままになる場合があります。原則としては正規の手順でシャットダウンを行っていただくことを強く推奨いたしますが、予期せぬ問題等により強制的に電源断を行った場合は、再度モバイルモードの起動をしていただくことで、一時的に書き換えられたユーザー設定等が復旧します。
5. 「Windows ストアアプリ」の動作をサポートしていません。

そのため拡張子に関連付けられたアプリケーションが Windows ストアアプリに設定されている環境ではファイルが実行されません。予め、拡張子の関連付けをデスクトップアプリケーションに設定してご利用ください。

(PDF の閲覧は、Adobe Reader をご利用ください。)

6.Internet Explorer から Active X コンポーネントのダウンロード、インストールに失敗する場合があります。

モバイルモード移行前にダウンロード、インストールをお願い致します。

7.モバイルモードではローカル HDD への書き込みを行えないようにしていますが、アプリケーションによっては一時ファイルを書き込めないと不具合が発生する場合がありますため、これを防ぐために、書き込めないように振る舞います。このため、あたかもファイルが書けたようにみえる場合がありますが、モバイルモード終了後は、ローカル HDD に作成したファイルが残ることはありません。

Windows10 での制限事項

- 1.「Windows ストアアプリ」を利用することはできません。
(拡張子がストアアプリに関連付けられている場合は、デスクトップアプリケーションに関連付けてご利用ください。)
- 2.スタートメニューを利用することはできません。
- 3.MTP/PTP 接続したデバイス内のファイルを直接参照できません。
- 4.OneDrive のご利用はサポートしておりません。
- 5.画像ファイルをダブルクリックで開く場合に「レジストリに対する値が無効です」と表示されて開けない場合があります。
(拡張子の関連付けをストアアプリ以外のデスクトップアプリ (Windows フォトビューアー等) に設定してご利用ください。)
- 6.Microsoft Office ドキュメントファイルを右クリックし「保護ビューで開く」から ファイルを開くことはできません。
- 7.Microsoft Office 利用時にタスクバーを右クリックしてもメニューが表示されません。

■コピーガードの設定方法

1: コピーガードを設定するにはまず、上部にある[セキュリティ USB のコピーガードを有効にする]を選択してください。選択すると条件設定が行えるようになります。

実行制限 (全製品対応)

セキュリティUSBの実行制限/コピーガードを無効にする
 セキュリティUSBの実行制限を有効にする
 セキュリティUSBのコピーガードを有効にする

実行制限/コピーガードのヘルプ

※コピーガードの設定はタブ: コピーガード2/操作ログで行ってください。

実行条件

AND方式 OR方式 AND + OR方式

ファイル/フォルダ/レジストリキー/IPアドレス(IP:)/MACアドレス(MAC:)/ワークグループ(DN:)/ドメイン名(DN:)を実行キーとして設定可能です
IPアドレス以降の実行キーを入力する場合、実行キーの前に()の値を追記してください。
例: MAC:11-22-33-44-55-66

AND方式

この設定項目がPC上に全て存在する場合、セキュリティUSBを実行できます。
または、この設定項目がPC上に全て存在する場合、オフィスモードで動作します。

設定値		追加する	削除する	一括設定
-----	--	------	------	------

OR方式

この設定項目の内一つでもPCに存在する場合、セキュリティUSBを実行できます。
または、この設定項目の内一つでもPCに存在する場合、オフィスモードで動作します。

設定値		追加する	削除する	一括設定
-----	--	------	------	------

自動パスワード解除設定

自動パスワード解除を行わない 自動パスワード解除を行う

制限PCでの起動設定

制限PCでは一切使用させない
 制限PCではパスワード入力画面を表示する
(パスワード認証で使用可能)

2：次にオフィスモード実行条件方式を決定します。オフィスモード実行条件方式とは認証キーをどの様に存在した時にセキュリティ USB をオフィスモードで動作させるかを決定する方式です。オフィスモード実行条件には以下の AND 方式、OR 方式、AND+OR 方式があります。お客様の都合のよい方法を選択してください。

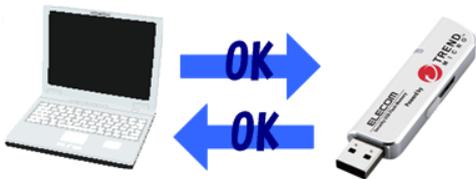
方式	[1]AND 方式	[2]OR 方式
内容	<p>設定項目が”全て” PC に存在する場合にセキュリティ USB がオフィスモード動作する設定です。</p> <p>例： 設定 1：C:\¥file1.bin・・・ファイル 設定 2：C:\¥folder1・・・フォルダ 設定 3： HKEY_CURRENT_USER¥Software¥TEST¥TEST1・・・レジストリキー</p> <p>PC 内に設定 1, 2, 3”全て”存在する場合、セキュリティ USB がオフィスモード動作します。</p>	<p>設定項目の中で1つでも該当設定が存在する場合にセキュリティ USB がオフィスモード動作する設定です。</p> <p>例： 設定 1：C:\¥file2.bin・・・ファイル 設定 2：C:\¥folder2・・・フォルダ 設定 3： HKEY_CURRENT_USER¥Software¥TEST¥TEST2・・・レジストリキー</p> <p>PC 内に設定 1, 2, 3の内、“最低一つ”存在する場合、セキュリティ USB がオフィスモード動作します。</p>
設定項目	最大 5000 個※	最大 5000 個※
使用用途	<p>特定のファイル、フォルダ、レジストリキーなどを全 PC に設定できる場合。</p> <p>例：全 PC をアクティブディレクトリで管理している、新規に PC を調達した場合など</p>	<p>PC 内のファイル、フォルダ、レジストリキー構成を変更できない、また共通のファイル等がない場合。</p> <p>例：PC の回収が難しい場合など</p>

※注意：USB2.0 モデルと USB3.0 モデルのバージョン 400 以前は最大 15 個まで対応となっております。AND+OR 方式は AND 条件と OR 条件両方を満たす場合、セキュリティ USB がオフィス動作する方式です。



オフィスモードで動作

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。

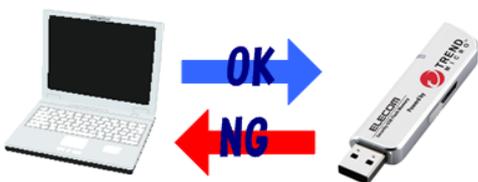


通常のUSBメモリの様に使用ができる



モバイルモードで動作

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！

- 3: 方式を決定しましたら、認証キーを登録します。[設定値]欄へ認証キーを入力し、[追加]ボタンを押してください。
認証キーは最大 99 個まで登録可能です。
追加した条件を削除した場合は、項目を選択し、(削除する)ボタンを押してください。
[一括設定]からは認証キー情報を記載したファイルを一括で読み込ませることができます。最大 5000 個まで登録可能です。

The screenshot shows two sections for setting authentication keys. The top section is titled "AND方式" (AND mode) and contains the text: "この設定項目がPC上に全て存在する場合、セキュリティUSBを実行できます。または、この設定項目がPC上に全て存在する場合、オフィスモードで動作します。" Below this text is an empty text input field. The bottom section is titled "OR方式" (OR mode) and contains the text: "この設定項目の内一つでもPCIに存在する場合、セキュリティUSBを実行できます。または、この設定項目の内一つでもPCIに存在する場合、オフィスモードで動作します。" Below this text is a table with four rows of example data: "c:\¥12345.txt", "MAC:11-22-33-44-55-66", "IP:128.1.105.1-128.1.105.3", and "IP:192.168.1.220". Both sections have a "設定値" (Setting value) input field and buttons for "追加する" (Add), "削除する" (Delete), and "一括設定" (Batch setting).

認証キーの設定

認証値としては以下を設定することができます。

- ファイル/フォルダの有無
- レジストリキーの有無
- MAC アドレス
- IP アドレス
- ドメイン
- ワークグループ

認証条件 (AND/OR) に合わせて、[設定値] 枠へ認証値を入力し、[追加する] ボタンを押してください。画面上では最大 99 個まで登録可能です。99 個以上登録する場合、[一括設定] ボタンを押して、テキスト形式で登録をしてください。最大 5,000 個まで登録可能です。

認証キーの設定方法は実行制限と同じですので、項：実行制限の項目をご確認ください。

4. セキュリティ USB の実行条件を満たした PC 上でのパスワード解除方法の設定を行います。

The screenshot shows a dialog box titled "自動パスワード解除設定" (Automatic password unlock setting). It contains two radio button options: "自動パスワード解除を行わない" (Do not perform automatic password unlock) which is selected, and "自動パスワード解除を行う" (Perform automatic password unlock).

解除方法は 2 つから選択できます。
次にモバイルモードでの動作制限について記載します。

■モバイルモードの動作制限

モバイルモードではファイルをPCへコピーする制限以外にさらに情報漏洩防止強化を行うことができます。設定は実行制限/コピーガードで行うことができます。

モバイルモード動作時の動作制限

コピーガード機能が有効になる環境(自宅等)で使用した時の制限設定を行います。データ流出対策をさらに強化することができます。

印刷禁止: する しない

スクリーンキャプチャ禁止: する しない

クリップボードの使用禁止: する しない

ネットワーク共有フォルダへのアクセス禁止: する しない

[ファイルサーバ設定](#)

インターネットアクセス禁止: する しない

[制限の詳細設定](#)

PCのエンドポイント監査※ 使用禁止 警告を表示 しない

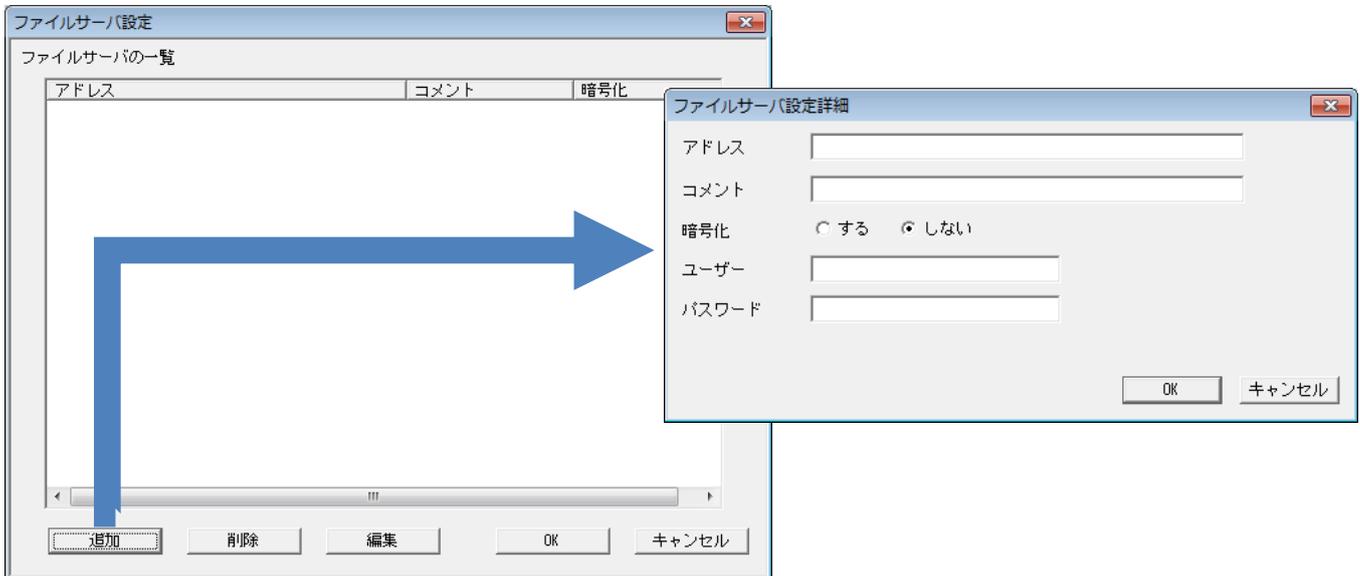
※セキュリティUSBを使用したPCIにウイルススキャンソフトが入っているかを確認し、そのPC上での動作を設定します。
例: ウイルススキャンソフトが入っていないPCでは使用禁止する

モバイルモード項目ではコピーガード機能を有効にしたPCでの動作設定を行うことが可能です。USBメモリへ設定できるポリシーは以下になります。

設定項目	説明	デフォルト値
印刷禁止	印刷を禁止するか選択します。禁止するときは、「する」を選択します	しない
スクリーンキャプチャ禁止	スクリーンキャプチャを禁止するか選択します。禁止するときは、「する」を選択します。	しない
クリップボードの使用禁止	クリップボードの使用を禁止するか選択します。禁止するときは、「する」を選択します。	しない
ネットワーク共有フォルダへのアクセス禁止	ファイルサーバー、NAS等のネットワーク共有フォルダへのアクセスを禁止するか選択します。禁止するときは、「する」を選択します。ネットワーク共有フォルダの暗号化・復号化を行うときは、「 ファイルサーバーの設定 」ボタンをクリックして個別に設定してください。	しない
インターネットアクセス禁止	インターネットのアクセスを禁止するか選択します。インターネットのアクセスを禁止するときは、「する」を選択します。インターネットのアクセスを禁止を「する」に設定したとき、「 制限の詳細設定 」で設定されるドメインのみアクセスを許可することができます。	しない
PC エンドポイント監査	USBメモリが挿入されたコンピュータのウイルス対策ソフトの状態・リムーバブルメディアの自動再生設定状態を監査します。ウイルス対策ソフトの状態は、Windowsのセキュリティセンターおよびアクションセンターの情報を参照しています。	しない
	※セキュリティセンター・アクションセンターの情報は、WMIの「root¥SecurityCenter」および「root¥SecurityCenter2」から情報を取得しています。	
	※SSOオプションを利用しているコンピュータでは利用できません。	
	使用禁止	
警告を表示	ウイルス対策ソフトが最新の状態で動作していないと警告のみ表示します。	
しない	エンドポイント監査をしません。	

■ファイルサーバの設定

ネットワーク共有フォルダの暗号化あるいは、アクセス禁止のときの例外設定を行います。「ファイルサーバー設定」ボタンをクリックすると、ファイルサーバー設定画面が表示されます



新規に、ネットワーク共有フォルダの設定を追加するときは、「追加」ボタンをクリックして次の項目を入力します。

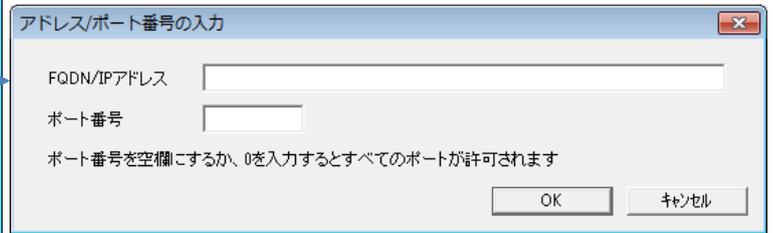
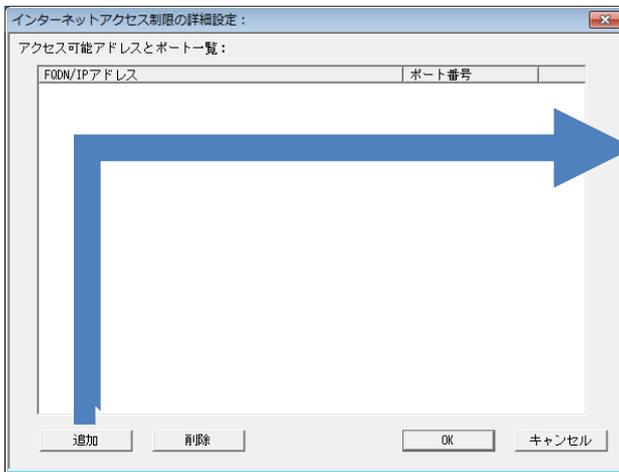
設定項目	説明
アドレス（必須）	ネットワーク共有フォルダを指定します。 書式は必ず、「¥¥ファイルサーバーアドレス¥共有フォルダ名」で指定してください。
コメント	一覧画面でわかりやすいようにコメントを入力します。
暗号化	暗号化するかどうか選択します。暗号化するときは、「する」を選択します。
アクセスユーザー名	ファイルサーバーへアクセスするためのユーザー名を指定します。
パスワード	ファイルサーバーへアクセスするためのユーザーに設定されているパスワードを指定します。

ネットワーク共有フォルダへのアクセスが禁止されているときでも、ここで設定されている共有フォルダにはアクセス可能となります。

■制限の詳細設定

インターネットアクセスが禁止されているときの、例外設定を行います。

「制限の詳細設定」ボタンをクリックすると、インターネットアクセス制限の詳細設定画面が表示されます。



新規に、インターネットアドレスの設定を追加するときは、「追加」ボタンをクリックして次の項目を入力します。

設定項目	説明
FQDN/IP アドレス（必須）	ドメイン名あるいはドメインの IP アドレスを指定します。 例) intelligent.jp 「 http://www.hagisol.co.jp/ 」を指定しても有効に働きません。サブドメイン名などは入力しないでください。同様に URL などを指定しても有効に働きません。
ポート番号	ポート番号を指定するときは、許可するポート番号を指定してください。 入力がないときは、すべてのポートに対してアクセス可能となります。

■コピーガード機能のウイルス対策ソフトとの共存について

ウイルス対策ソフトとの共存についての注意事項を説明します。

※各ソフトウェアで有効なライセンスをお持ちで、最新のものを利用されていることを前提としています。
※いずれの製品もデフォルト設定の状態を確認しています。

■利用開始時にメッセージが表示される、あるいは例外設定が必要なもの

メーカー	ソフトウェア名	表示されるメッセージ/設定など	32bit 版で確認済みバージョン	64bit 版で確認済みバージョン
F-Secure	エフセキュア インターネットセキュリティ	こちら を参照	2011/2012	2011/2012
Kingsoft	Kingsoft Internet Security	こちら を参照	2011	2011
AVG	AVG インターネットセキュリティ	こちら を参照	2011/2012	2011/2012

各ソフトウェアの「表示されるメッセージ/設定など」を参照して適切に操作してください。

■メッセージなどの表示はなく、そのまま利用できるもの

メーカー	ソフトウェア名	32bit 版で確認済みバージョン	64bit 版で確認済みバージョン
トレンドマイクロ	ウイルスバスター	2010※1/2011/2012	2010/2011/2012
シマンテック	ノートン インターネットセキュリティ	2011/2012	2011/2012
マカフィー	インターネットセキュリティ/ トータルセキュリティ	2011/2012	2011/2012
ESET	ESET Smart Security	4.2	4.2

ソースネクスト	ウイルスセキュリティ ZERO	2011/5	2011/5
カスペルスキー	Kaspersky Internet Security	2011/2012	2011/2012
G DATA	G DATA インターネットセキュリティ	2011/2012※2	2011/2012※2
マイクロソフト	Microsoft Security Essentials	2011/5_	2011/5
Avira	Avira Premium Security Suite	2011/5	2011/5
Avast	Avast! インターネットセキュリティ	2011/5_	2011/5
BitDefender	BitDefender インターネットセキュリティ	2011	2011

※1 必ず最新のものにアップデートしてください。一度もアップデートされていない環境では、起動できない場合があります。

※2 モバイルモード時、HDD ドライブもエクスプローラー上に表示されますがファイルの読み込み、書き込みはできません。

法人向けの対策ソフトについては、上記製品を参考にして管理者の方が検証および例外設定してください。それぞれの例外設定方法などは、各製品のマニュアルあるいは各メーカーにお問い合わせください。

エフセキュア クライアント セキュリティ/インターネット セキュリティ

専用 USB メモリ起動時に、次の設定をします。

■2011 の場合

2 種類の画面が表示されます。



システム変更の試行画面では、「プログラムを信頼しています。プログラムを許可します。」を選択して、「OK」ボタンをクリックします。

新しいサーバアプリケーション画面では、「今後、このプログラムでこのダイアログを表示しない」をチェックして、「許可」ボタンをクリックします。

2012 の場合

以下の画面が表示されます。



システム変更の試行画面では、「プログラムを信頼しています。プログラムを許可します。」を選択して、「OK」ボタンをクリックします。

※エフセキュア クライアント セキュリティの使用方法は、エフセキュア クライアント セキュリティの説明書をご覧ください

Kingsoft Internet Security

専用 USB メモリ起動時に、PersonalFirewall がメッセージを表示します。

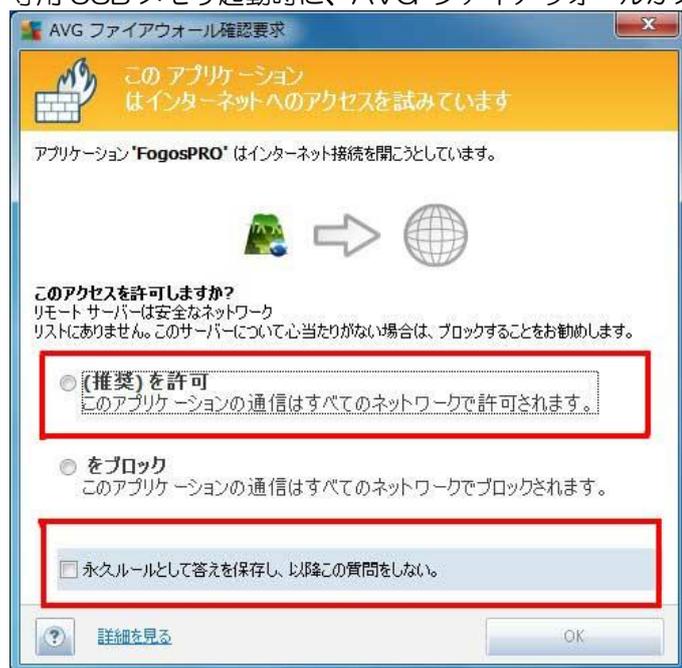


「いつでも許可」を選択して、「信用認証したプログラムのアクセスをいつも許可」にチェックをいれて「OK」ボタンをクリックします。

※Kingsoft Internet Security の使用方法は、Kingsoft Internet Security の説明書をご覧ください

AVG インターネットセキュリティ

専用 USB メモリ起動時に、AVG ファイアウォールがメッセージを表示します。



アプリケーションが「FogosPRO」とあるとき、「【推奨】を許可」を選択し、「永続ルールとして答えを保存し、以降この質問をしない」にチェックを入れて「OK」ボタンをクリックします。

※AVG Internet Security の使用方法は、AVG Internet Security の説明書をご覧ください

ファイル操作ログ/印刷ログ取得

セキュリティ USB メモリ内のファイル操作ログ(いつ、どこで、どのファイルが操作されたか)を取得、管理することができます。データ漏えい防止、データ漏えい時の原因追求などにご利用頂けます。ファイル操作ログは INFO BANKER により、ネットワーク経由で集中管理します。
※ファイル操作ログ/印刷ログは、セキュリティ USB のみ取得可能です。
※コピーガード有効時はモバイルモード時のみログを取得します。

■取得ログ内容

取得できるログ概要は以下になります。

[ファイル操作ログ]

- **ファイル操作した PC の情報**
(操作日時/コンピュータ名/ユーザ名/Mac アドレス/IP アドレス)
- **デバイスに関する情報**
(デバイスの USB シリアル番号)
- **ファイル操作情報**
(ファイル名、ファイルサイズ、ファイル操作したプロセス名、ファイル処理*)
*コピー、削除、リネーム等

[印刷ログ]

- **プリンタ情報**
(印刷日時/プリンタ名)
- **デバイスに関する情報**
(デバイスの USB シリアル番号)
- **ファイル情報**
(印刷されたファイル名、印刷したプロセス名)

■ファイル操作ログ/印刷ログ取得設定方法

ログ取得設定の[ファイル操作/印刷ログ取得]を「する」を選択してください。

ログ取得設定

ファイル操作/印刷ログの取得： **する** **しない**

ファイル操作ログをInfoBankerへ送信する場合、タブ：ログ送信で送信設定をしてください。
詳細はログ送信タブ内の[InfoBankerのヘルプを開く]でご確認ください。

■ファイル操作ログを InfoBanker へ送信する設定設定方法

ファイル操作ログは InfoBanker で一元管理することができます。設定方法はタブ：ログ送信へ移動し、「ファイル操作ログを送信する」を選択してください。その他項目については項：ログ管理をご確認ください。

ファイル操作ログ

ファイル操作ログを送信しない ファイル操作ログを送信する

■ファイルアクセスログ/印刷ログについて

項目	内容
ログファイル保存場所	<p>セキュリティ USB のリムーバブルディスク領域(パスワードロック)内の「a1fd5b43,\$\$\$」フォルダ下に保存されます</p> <pre> a1fd5b43,\$\$\$ ---iss_log_host --- 000000000000000000 --- 000000000000000001 ---iss_log_print --- 000000000000000000 --- 000000000000000001 </pre> <p>iss_log_host : ファイルアクセスログ格納フォルダ iss_log_print : 印刷ログ格納フォルダ</p>
ファイルアクセスログ	<p>コピーガード機能を有効時に取得できるファイルアクセスログです。</p> <p>ファイル形式 : XML</p> <p>ファイル名 ; 000000000000000000/000000000000000001/00000000000000002...</p> <p>セキュリティ USB 内のファイルにアクセスする度にログを残します。 詳細なログ内容については次ページを確認ください。</p>
印刷ログ	<p>コピーガード機能を有効時に取得できる印刷ログです。</p> <p>ファイル形式 : XML</p> <p>ファイル名 ; 000000000000000000/000000000000000001/00000000000000002...</p> <p>セキュリティ USB 内のファイルを印刷する度にログを残します。 詳細なログ内容については次ページを確認ください。</p>
保存されたログへのアクセス権	<p>セキュリティ USB 内へ保存されているログはアクセス制限が掛かっており、ユーザーは保存されているログの読み書き、削除することができません。</p> <p>ログの中身を確認するためには InfoBanker へ送信する設定にするか、SecurityUSB Manager の [デバイス内のログ収集]機能を使用してログを収集してください。</p> <p>注意 ; セキュリティ USB によって製品の初期化を行うとログを削除されてしまいます。ユーザーにログを消されたくない場合は SecurityUSB Manager によってデバイスの初期化機能を無効にしてください。</p>

■ファイルアクセスログ内容

項目	内容
time	ファイルアクセスが行われた時間(エポック時間)
localtime	ファイルアクセスが行われた時間(ローカル時間)
process	ファイルへアクセスを行ったプロセス名
function	ファイルへ行った処理 <ul style="list-style-type: none"> • Open : ファイルを開く • Create : ファイルを作成 • Access: : ファイルをアクセス • Copy : ファイルをコピー • Move : ファイルを移動 • Execute : ファイルを実行 • Delete : ファイルを削除
target	ファイル操作元のファイルパス/ファイル名
destination	ファイルコピー、移動などを行った際のコピー・移動先ファイルパス/ファイル名
serverSource※1	転送元サーバー名
serverDest※1	転送先サーバー名
flagSourceFile※1	転送元にファイル名が存在する場合「1」が記載。
flagDestFile※1	転送先にファイル名が存在する場合「1」が記載。
deviceId	製品の USB シリアル番号
loginName	PC のログインユーザ名
uniqID	ID 番号。1 ログ毎に異なる番号が割り当てられます。
fileByte	アクセスしたファイルのファイルサイズ[byte]
vendorID	PC に他の USB メモリから取得するベンダーID
productID	PC に他の USB メモリから取得するプロダクトID
deviceType	PC に他の USB メモリから取得するデバイスタイプ
Dup	弊社管理情報
userID	
fingerNumber	
ipAddress	
macAddress	
HostID	
operationMode	
accessType	

※1 : ファイル操作対象がネットワークドライブにある場合に記載されます。

■印刷ログ内容

項目	内容
Time	ファイル印刷が行われた時間(エポック時間)
localtime	ファイル印刷が行われた時間(ローカル時間)
process	ファイル印刷を行ったプロセス名
function	“print” 固定
target	印刷されたファイルのファイルパス/ファイル名
destination	プリンタ名
Dup	印刷枚数
loginName	PC のログインユーザ名
deviceID	製品の USB シリアル番号
uniqlD	ID 番号。1 ログ毎に異なる番号が割り当てられます。
HostID	弊社管理情報
userID	
fingerNumber	
operationMode	
vendorID	本項目は記録されません。
productID	
deviceType	
AccessType	
serverDest	

デバイス情報

デバイス情報タブではデバイスヘユーザの情報を設定することが可能です。持ち主の名前や部署名などを入れてご利用ください。

[デバイス情報で出来ること]

- ※ デバイス管理番号の設定（デバイス管理番号はパスワード解除画面に表示されます。）
- ※ デバイスのコメント情報の設定
- ※ USB 製品の USB ベンダーID、USB プロダクト ID、USB シリアル番号、製品シリアル番号の確認

デバイス情報 (全製品対応)

USBベンダーID	0x693
USBプロダクトID	0x95/0x96
USBシリアル番号	07000708485912CA7575
製品シリアル番号	E51301000001
デバイス管理番号	株式会社ABCDE

コメント

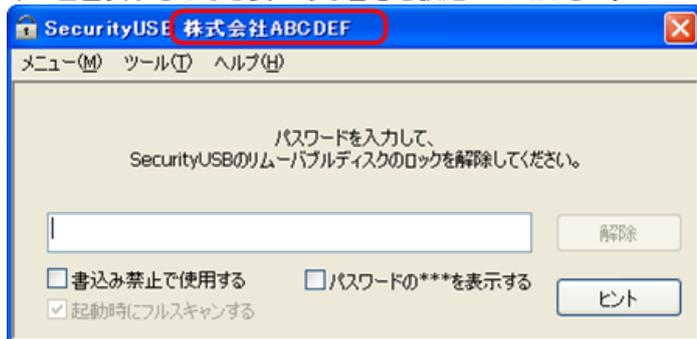
株式会社ABCDE
営業2課
2015年4月1日貸出

- ・ USBベンダーID、USBプロダクトID、USBシリアル番号：
USB製品を制限するシステム等にご使用ください。
- ・ 製品シリアル番号：
製品表面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(最大16文字)：
設定したデバイス管理番号はUSB製品使用時に常に画面上部に表示されます。
- ・ コメント(最大140文字)：
デバイスにコメントをつけることができます。ユーザも確認可能な情報です。
設定したコメントはUSB製品使用時のパスワード解除画面→[ヘルプ]→[デバイス情報]から確認することができます。

項目	内容
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	現在接続されている USB 製品の製品シリアル番号が表示されます。 製品シリアル番号は USB 製品の裏面に記載されている番号です。

デバイス管理番号

デバイス管理番号を設定できます。最大 16 文字です。ユーザも確認可能な情報です。設定したデバイス管理番号は USB 製品使用時に常に画面表示されます。常に画面表示させる必要がある番号を設定してください。

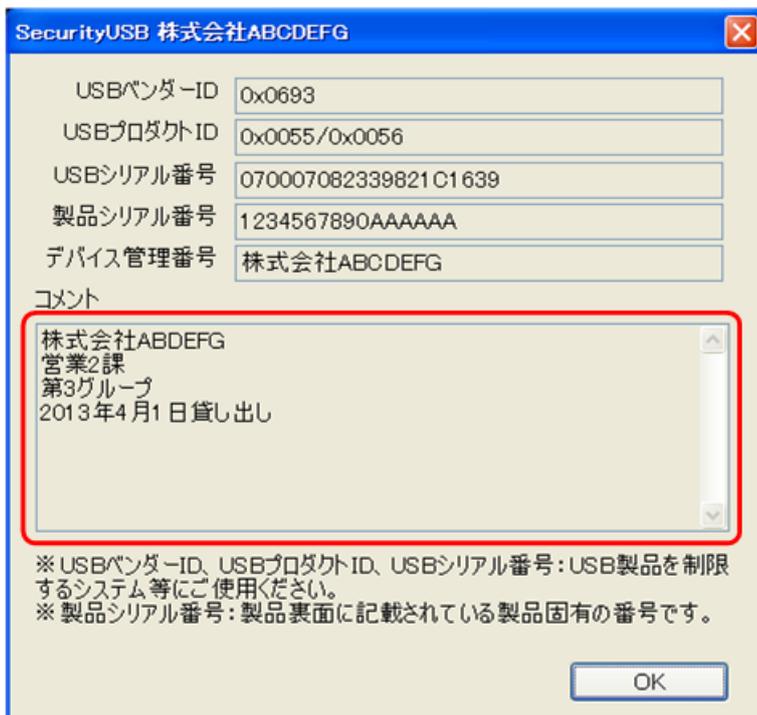


コメント

デバイスにコメントをつけることができます。最大 140 文字です。ユーザも確認可能な情報です。

設定したコメントは USB 製品使用時のパスワード解除画面→[ヘルプ]→[デバイス情報]から確認することができます。

コメントは管理番号 16 文字で足りない場合や、常に画面表示させる必要が無い情報を設定してください。



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。

• SecurityUSB Manager 起動

※SecurityUSB Manager 起動時に自動でソフトウェアアップデートを行わない場合は、SecurityUSB Manager の

ツールバーから

[ファイル]→[製品アップデート]でチェックを外してください。

• SecurityUSB Manager のツールバーから[ファイル]→[製品アップデート]実行

ソフトウェアアップデートがある場合、以下の画面が表示されます。



※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。

■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、SecurityUSB Manager メイン画面に移ります。

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。

弊社への設定書き込み生産依頼について

お客様が要望する設定を弊社で書き込み、設定を書き込んだ状態の製品をお客様へ納品するサービスをご用意しております。お客様からご提供頂くものは以下になります。

ご提供頂くもの	作成方法
設定ファイル	<p>管理者用ソフト「セキュリティ USB マネージャー」で各種設定完了後、メイン画面で『デバイスへ設定書き込みと同時に設定ファイルを出力する』にチェックを入れた上で [デバイスに設定を書き込む] をクリックすると、設定内容を設定ファイル（ファイル名：MpSUM.sum）として出力されます。</p> <div data-bbox="437 577 1471 887"><ul style="list-style-type: none"><input checked="" type="checkbox"/> デバイスへ設定書き込みと同時に設定ファイルを出力する<input type="checkbox"/> デバイスへ設定書き込みと同時に遠隔設定TOOLを出力する<input type="checkbox"/> 設定書き込み時に定義ファイルを復旧する（※設定書き込み時間が増加します）<input type="checkbox"/> 認証キーを固定化し、認証キーの変更と削除を禁止する<p style="text-align: right;"><input type="button" value="デバイスへ設定を書き込む"/></p></div>
認証キー	<p>設定ファイルを作成時に使用した認証キーです。</p> <div data-bbox="437 1003 1471 1447"><p>メイン 詳細設定...</p><p>デバイス認証</p><p>製品名：-</p><p>認証キー</p><p><input type="text" value="123451234512345"/> <input type="button" value="認証"/></p><p>認証キーは”お客様が自由に設定できるキー”となります。認証キーは、デバイス内に保存されます。</p><p><input type="button" value="認証キーの削除"/></p><p><input type="text" value="認証時に設定を読み込まない"/> ▼</p></div>

上記を用意して頂き、販売店もしくは営業担当にお申し付けください。

6 | トラブルシューティングと Q&A

質問		回答	
Q1	SecurityUSB Manager が動作しません。	A1	対象デバイスを接続してください。
Q2	パスワード入力ミス回数(通常 5 回)間違えた場合、どうすれば再度対象デバイスが利用可能になりますか？	A2	SecurityUSB Manager にて「データの救出」/「遠隔地にいるユーザのデータ救出」を行なってください。
Q3	複数台の対象デバイスに対して同時に SecurityUSB Manager を実行することは可能ですか？	A3	複数台同時に実行することはできません。必ず一台の対象デバイスのみ接続し、実行してください。
Q4	ネットワークドライブからの実行に対応していますか？	A4	ネットワークドライブからの実行には対応しておりません。
Q5	SecurityUSB Manager は対象デバイスの状態に関係なく実行できますか？ 例：Password 認証後のメモリ領域へアクセスできる状態	A5	対象デバイスのパスワード認証前に実行してください。 また対象デバイスのソフトウェアが起動している場合は終了させてください。

その他 QA につきましては QA サイトをご確認ください。

<http://qa.elecom.co.jp/> へ移動して頂きメモリ→ウイルス対策機能付き USB メモリへ移動してください。



お問い合わせ窓口

ご連絡先		受付
サポートセンター※	TEL : 0570-080-900	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。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「全国统一番号」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 ™ マークは明記していません。
- ◆本ドキュメント内容は、2023年3月時点のものです。今後、当該内容は予告なく変更される場合があります。

SecurityUSB Manager
型番：HUD-SUMA
マニュアル
2023年3月