USB HARDLOCKER 5

ESCOMPUTER

販売元： 株式会社ライフボート
開発元： 株式会社エスコンピュータ

利用ガイド

LIFEBOAT
a megasoft company

注意
この利用ガイドに記載されている情報は、予告無しに変更されることがあります。
株式会社ライフボートは、本利用ガイドあるいはプログラムに記載されている内容に対していかなる誤りが含まれる場合にも、一切の保証を行いません。

EDITION
August 2023

Printed in Japan

PUBLISHED BY
株式会社ライフボート
東京都千代田区神田神保町 2-2-34
ホームページ： https://www.lifeboat.jp/

目　次

第1章　USB HardLocker 5の概要

第1節　USB HardLocker 5 について

『USB HardLocker5』はPCの不正使用防止、USBメモリーの使用制限、データの自動暗号化、操作ログの収集といったデータ流出防止に不可欠な機能を統合したセキュリティ対策ソフトです。

本利用ガイドは、『USB HardLocker 5』『USB HardLocker 5 Server』共用です。このページ以降、各製品に限定された機能を説明する場合、下記のように記載します。
USB HardLocker 5　→ クライアントOS版
USB HardLocker 5 ボリュームライセンス　→ ボリュームライセンス版
USB HardLocker 5 Server　→ サーバー版 シングル／ボリュームライセンス

■機能と特長

● USB機器、USB機器×パスワードによる鍵を設定可能

USB機器の鍵、USB機器だけでは解錠ができないUSB機器×パスワードによる鍵を選択することができます（パスワードによる合鍵の作成も可能）。

● コンピューターのロック

PCに鍵をかけて第三者による操作ができないようにします。施錠された状態(鍵非装着)でログオンすると、スクリーンがロックされPCの操作はできません。解錠(鍵を装着)するとスクリーンロックが解除されます。ロックの機能はセーフモードによる起動時にも動作します。

● 鍵を挿すだけでWindowsにログオン

USB鍵をWindowsのユーザーと連携させて、鍵を装着してロック解除と同時にWindowにログオンすることができます。

● 鍵の管理（管理者鍵、利用者鍵、合鍵）

鍵は管理者鍵と利用者鍵の2種類に分かれます。管理者鍵は、利用者鍵の権限を設定したり、ソフトウェア全般の設定をしたりするのに使われます。万が一鍵が壊れたり紛失したりしたときのために、登録済みのそれぞれの鍵に対して合鍵の登録が可能です。

● 暗号化領域（秘密領域）の作成
内蔵ディスク上の空き領域に、鍵がないと使用できない暗号化領域（秘密領域）を作成することができます。鍵が装着されたときにだけ、仮想ドライブとして暗号化領域にアクセスすることができます。隠したいファイルや外部に漏れては困るデータを暗号化領域に保存しておけば、鍵を持たない第三者にデータを読み取られる心配はありません。
※ 暗号化のアルゴリズムにはAES256ビットを使用しています。

● 秘密領域と鍵情報のバックアップ機能
万が一コンピューターがクラッシュした場合に備えて、設定情報、登録された鍵に関する情報、作成された秘密領域をバックアップすることができます。秘密領域は暗号化された状態でバックアップされ、リストアには管理者鍵が必要になりますので、セキュリティレベルを落とさずにバックアップを取ることができます。

● ネットワークロック
鍵を取り外すと、ネットワーク接続が切断されます。コンピューターのロックと組み合わせて、ロック時にネットワークを切断することもできます。

● 操作ログ収集・保存
USB HardLockerによる解錠と施錠、ログオンとログオフ、ハードウェアの追加と削除、ファイルアクセス、インターネットアクセス、キーボード操作、ウィンドウ、プロセス起動、ファイル操作、印刷、Webアップロードに関する事象をログファイルに記録できます。

● ストレージ追加禁止
許可されていないUSBストレージやドライブが接続されると、スクリーンロックがかかり、操作が一切できなくなります。そのデバイスを取り外すと、スクリーンロックが解除されます。

● Configurator 2 による設定情報作成／配布 （ボリュームライセンス版）
鍵のリストや動作に関する設定情報を作成して、他のPCに配布するための専用ツールです。複数のPCに導入する際、インストール作業を省力化することができます。

● サイレントインストールに対応 （ボリュームライセンス版）
Configurator 2で作成した設定を読み込み、サイレントインストールを実行できます。

● 設定情報の自動同期 （ボリュームライセンス版）
PCの起動時、指定先に最新の設定情報ファイルを検知すると、自動インポートして設定内容を更新することができます。

第2節　設定できる鍵の種類について

『USB HardLocker 5』の鍵には管理者鍵と利用者鍵の 2 種類があります。

■鍵の種類

鍵の種類	意　味
管理者鍵	管理者鍵により、『USB HardLocker 5』がインストールされたコンピューターの操作ポリシーを規定することができます。 管理者鍵自身を一つの利用者鍵として利用することができます。
利用者鍵	利用者鍵は、管理者（管理者鍵を保有するユーザー）によって作成されます。利用者鍵により、管理者が規定した操作ポリシーに従ってその利用者鍵が登録されたコンピューターの操作をすることができます。

■鍵の種類による機能の違い

	管理者鍵	利用者鍵
管理者鍵の合鍵登録	◎	×
利用者鍵の登録・変更・削除	◎	×
利用者鍵の合鍵登録	◎	×
コンピューターのロック設定	◎	×
コンピューターのロック・解除	◎	○
Windows ユーザーに関連付け	◎	○
秘密領域の作成・変更・削除	◎	×
秘密領域の利用	◎	○
秘密領域の有効化・無効化	◎	○
ストレージ追加禁止設定	◎	×
ネットワークロックの設定	◎	×
ネットワークのロック・解除	◎	○
ストレージ追加	◎	○
ログ閲覧（モニター表示）	◎	×
設定、アンインストール	◎	×
バックアップ	◎	×

注　○印は管理者により予め許可されている場合に限り可能であることを示します。

第3節　必要なシステム

＜本ソフトのご使用に必要なシステム＞

対応 OS ※1	**USB HardLocker 5** Windows 11/10/8.1/7
	USB HardLocker 5 Server Windows Server 2022/2019/2016/2012R2/2012
対応機種	上記 OS が正常に動作する PC(PC/AT 互換機)
CPU	1GHz 以上のインテル Pentium 互換 CPU
メモリー	4GB 以上
ディスク容量	100MB 以上（秘密領域作成時、およびログ保存時はそれぞれの分の空き領域が別途必要）
その他	鍵になる USB 機器 ※2、利用可能な USB ポート（2.0 以上）

※1 日本語版以外のOSには対応しておりません。

※2 鍵になるUSB機器について

デバイスマネージャーに表示される USB 機器（ハブを除く）を鍵にすることができます。

電源をとっているだけの機器（充電機、LED ライト等）、およびハブは鍵になりません。

鍵の識別情報として、USB 機器の ROM 領域に予め書き込まれている「ベンダー ID」、「プロダクト ID」、「シリアル番号」を鍵の情報として利用しています。USB 機器によってはシリアル番号が無かったり、同じ型番の製品すべてに同じシリアル番号がつけられていたりすることがあります。そのような USB 機器を鍵にした場合は、同じメーカーの同じ型番の USB 機器を装着すると、ロックが解除されます。

第4節　注意事項

＜USB接続機器の取り外しについて＞
USB機器をコンピューターから取り外す際には予め「ハードウェアの安全な取り外し」処理をしてください。
※　鍵専用デバイス『ROCKEY2』を使用する場合、「ハードウェアの安全な取り外し」処理をする必要はありません。

＜作成できる秘密領域について＞
秘密領域は、鍵1つにつき1つ作成可能です。
秘密領域の最大サイズは2TBとなります。

＜秘密領域のフォーマットタイプについて＞
秘密領域は、FATまたはFAT32で自動的にフォーマットされます。1ファイルのサイズが4GBを超えるデータを保存する場合は、ドライブのプロパティを開いて、ドライブをNTFSに再フォーマットしておく必要があります。
※　秘密領域の作成先は内蔵ハードディスク／SSD のみとなります。リムーバブルディスク等はサポート対象外となります。
※　秘密領域は仮想ドライブになりますので、別途パーティション操作ソフトなどを使ってフォーマットしたりサイズ変更したりすることはできません。
※　秘密領域への OS のインストールやアプリケーションのインストールはサポートしていません。

＜セーフモード起動時の制限ついて＞
セーフモードで Windows を起動した場合、『USB HardLocker 5』の使用可能な機能はスクリーンロック／スクリーンロックの解除、ネットワークロック／ネットワークロックの解除、ログの参照となります。設定を変更したり、他の機能を使用したりすることはできません。

＜鍵の管理＞
鍵およびパスワードはユーザー様の自己責任で厳重に管理してください。製品の性質上、鍵およびパスワードの紛失に関するサポートはご提供できません。

＜ハードウェアの破損に備えて＞
鍵に設定したUSB機器が故障したり、USBポートが破損したりすると、スクリーンロックを解除できず、PCを操作できなくなります（秘密領域やログへのアクセスもできません）。
故障等に備えて、管理者鍵の合鍵としてパスワードを設定しておくことをお勧めします。

＜USB ハブの利用について＞
USB ハブを経由して USB 鍵を利用する場合、鍵を設定する前に USB 機器のシリアル番号をハブ経由でも認識できることをご確認ください。

＜データのバックアップ＞
失っては困るデータを秘密領域に保存する場合は、必ず付属のバックアップツールまたは別の手段によりバックアップを取るよう強くお勧めします。

＜ご利用環境上の留意点について＞
仮想ドライブを扱うツール、資産管理ソフト、ログ収集ソフトを併用すると、動作が不安定になることがあります。

第5節　よくある質問(FAQ)

ライフボートのホームページ（ https://www.lifeboat.jp ）にて『USB HardLocker 5』の便利な利用方法や最新の注意情報等、よくある質問と回答を公開しております。

ホームページトップの上部にある「FAQ」をクリックし、「USB HardLocker…」をお選びください。

第2章　USB HardLocker 5 のインストール

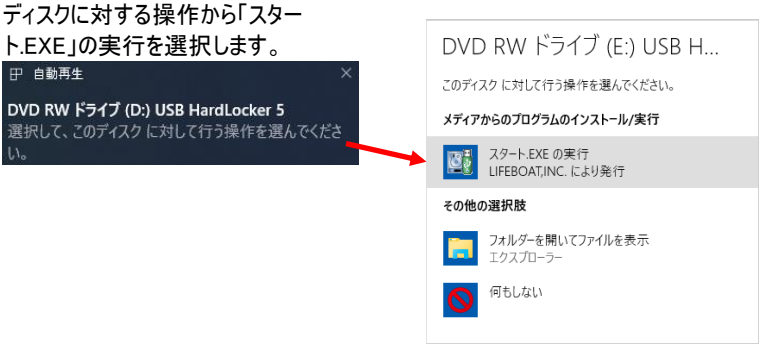
第1節　USB HardLocker 5 のインストール

インストールをするにはライセンスキーが必要です。事前にご用意ください。
（ライセンスキーはパッケージ製品の場合、同梱された「お客様控え」に記載されています。ダウンロード版は購入後に配信されるメールをご覧ください。）

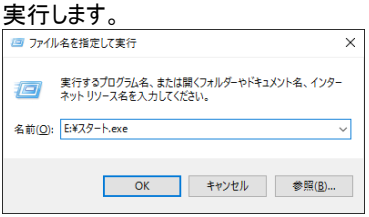
※ インストールは必ず管理者権限で Windows にログオンしてから実行してください。

1. 『USB HardLocker 5』のディスクをドライブにセットすると、自動再生のメニューが表示されますので、「スタート.EXEの実行」を選択してください。メニューが起動しない場合は、Windowsの「スタート」から「ファイル名を指定して実行」を選択して、「E:¥スタート.EXE」と入力して(CDドライブがEの場合)、「OK」をクリックします。

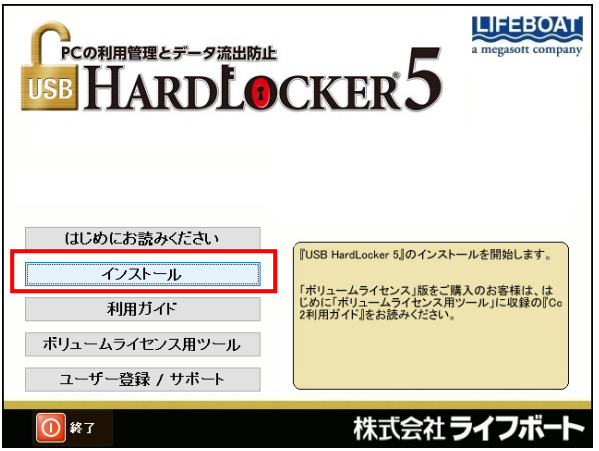
ディスクに対する操作から「スタート.EXE」の実行を選択します。



自動再生のメニューが表示されない場合は、ディスクを参照して「スタート.EXE」を実行します。



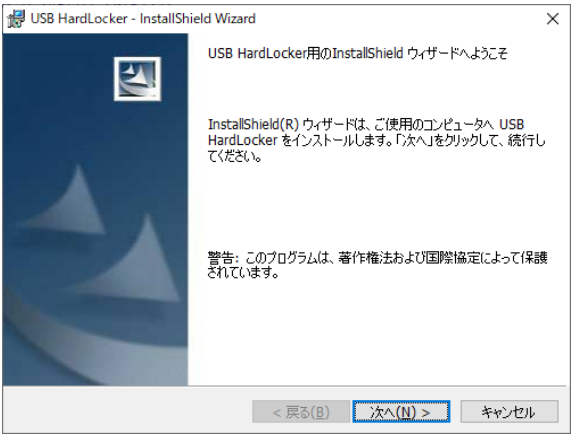
2. インストール用のメニューが表示されます。インストールを開始する場合は「インストール」をクリックしてください。



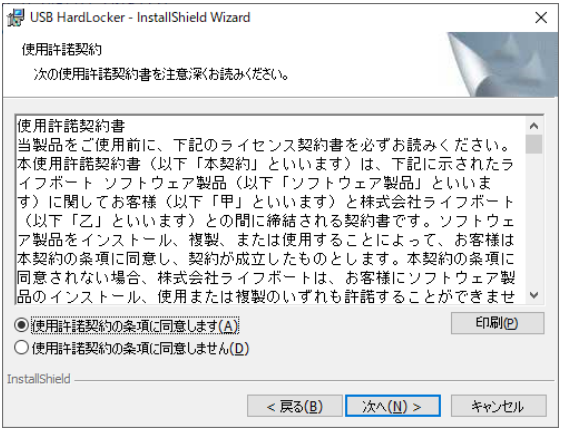
メニューの説明	
はじめにお読みください	Readme.txt を開きます。インストールを開始する前に必ずお読みください。
インストール	インストーラを起動して『USB HardLocker 5』のインストールを開始します。
利用ガイド	『USB HardLocker 5 利用ガイド』(PDF)を開きます。
ボリュームライセンス用ツール (ボリュームライセンス版のみ)	ボリュームライセンス版専用のツールを収録しています。(Configurator 2、サイレントインストール関連)
ユーザー登録 / サポート	オンラインユーザー登録ページへのリンク、サポートセンターの情報を表示します。

※ サーバー版はボタン配置が若干異なります。

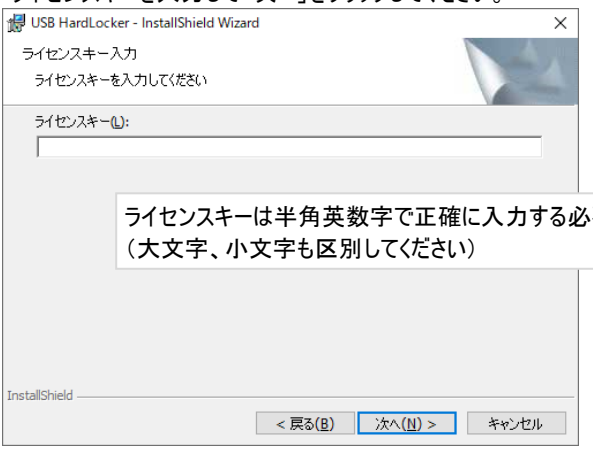
3. 『USB HardLocker 5』のセットアップ画面が表示されます。「次へ」をクリックしてください。



4. 「使用許諾契約」画面が表示されます。契約内容をよくお読みいただき、同意いただける場合は「使用許諾契約の全条項に同意します」をチェックして「次へ」をクリックしてください。同意いただけない場合には、インストールを中止します。

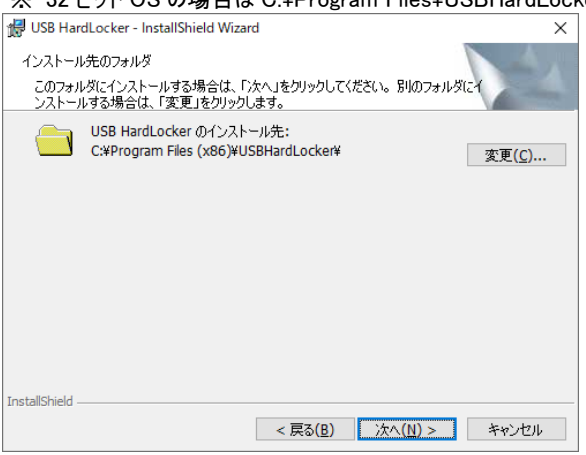


5. ライセンスキーを入力して「次へ」をクリックしてください。

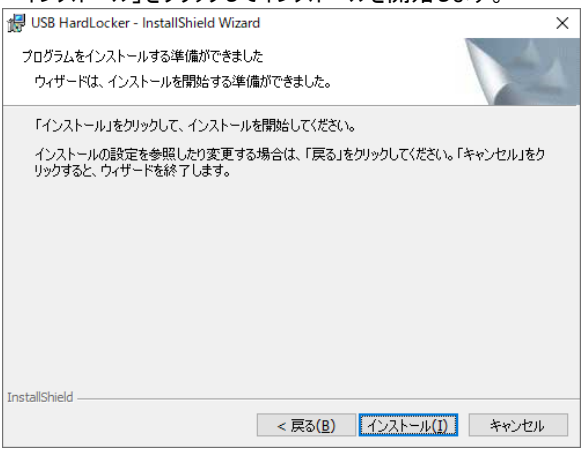


ライセンスキーは半角英数字で正確に入力する必要があります。
（大文字、小文字も区別してください）

6. 「次へ」をクリックします。インストール先を変更する場合は「変更」をクリックしてインストール先を指定することができます。
初期設定時のインストール先は C:¥Program Files(x86)¥USBHardLocker です。
※ 32 ビット OS の場合は C:¥Program Files¥USBHardLocker



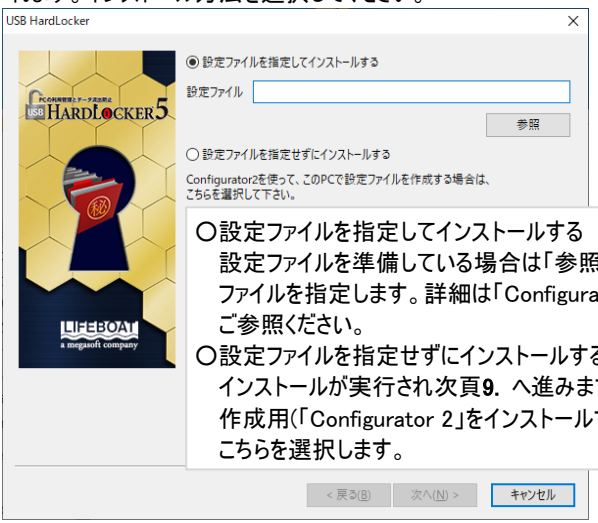
7. 「インストール」をクリックしてインストールを開始します。



「インストール」クリック後の動作は、ご購入製品により表示される画面が異なります。クライアントOS版／サーバー版はインストールが開始されます。完了後に **9.** (P17)の画面が表示されます。

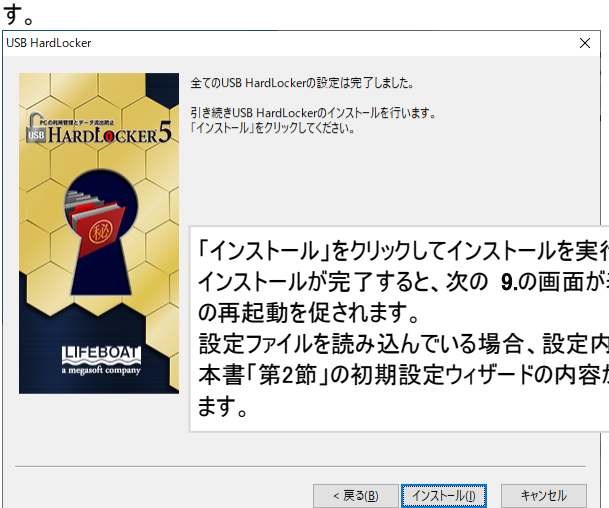
ボリュームライセンス版の場合、次頁の **8.** へ進みます。

8. ボリュームライセンス用のライセンスキーを使用している場合、以下の画面が表示されます。インストール方法を選択してください。



○設定ファイルを指定してインストールする
設定ファイルを準備している場合は「参照」をクリックしてファイルを指定します。詳細は「Configurator 2利用ガイド」をご参照ください。
○設定ファイルを指定せずにインストールする。
インストールが実行され次頁**9.** へ進みます。設定マスター作成用(「Configurator 2」をインストールする PC)の場合はこちらを選択します。

設定ファイルを読み込んで「次へ」をクリックした場合は、以下の画面が表示されます。

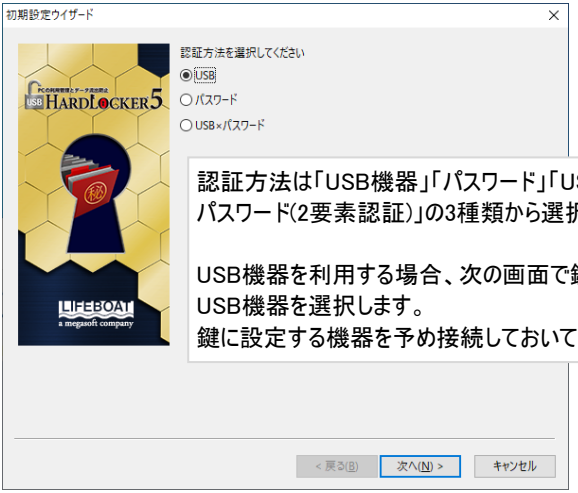


「インストール」をクリックしてインストールを実行します。
インストールが完了すると、次の **9.**の画面が表示されシステムの再起動を促されます。
設定ファイルを読み込んでいる場合、設定内容に依りますが、本書「第2節」の初期設定ウィザードの内容が一部省略されます。

9. 「InstallShield Wizardの完了」画面が表示されます。「完了」をクリックすると、システムの再起動を促す画面が表示されます。

第2節　初期設定ウィザード

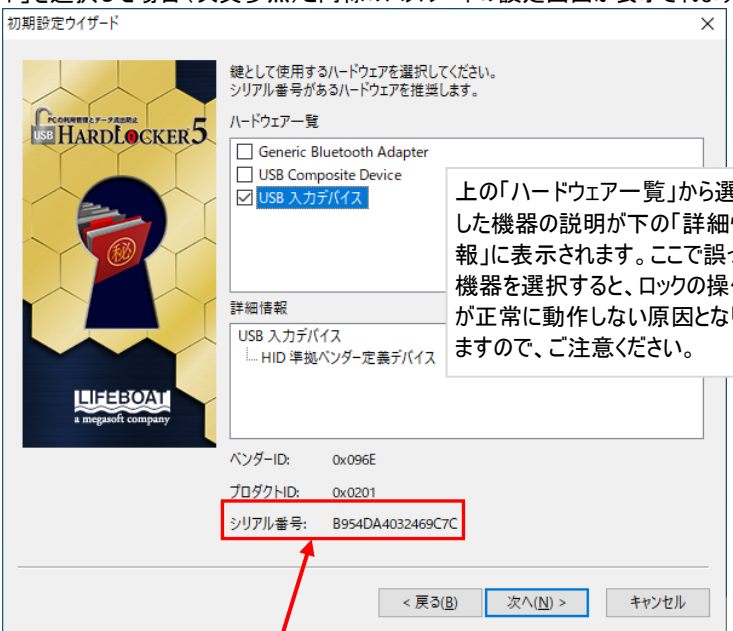
1. コンピューターを再起動すると、デスクトップ上に初期設定ウィザードが表示されます。最初に登録する鍵(管理者鍵)の認証方法を選択して「次へ」をクリックしてください。
   ※ 管理者鍵の作成後、利用者鍵や他の鍵を追加します。追加方法は「第 3 章　第 2 節」(P28)参照。
   ※ 鍵を Windows ユーザーに関連付けする場合は「USB」を選択してください。Windows ユーザーとの関連付けは「第 3 章　第 10 節」(P52)参照。
   ※ Windows 8.1 の環境では、Modern UI Style 画面からデスクトップ表示に切り替えた時点で初期設定ウィードが表示されます。



認証方法は「USB機器」「パスワード」「USB機器とパスワード(2要素認証)」の3種類から選択できます。

USB機器を利用する場合、次の画面で鍵にするUSB機器を選択します。
鍵に設定する機器を予め接続しておいてください。

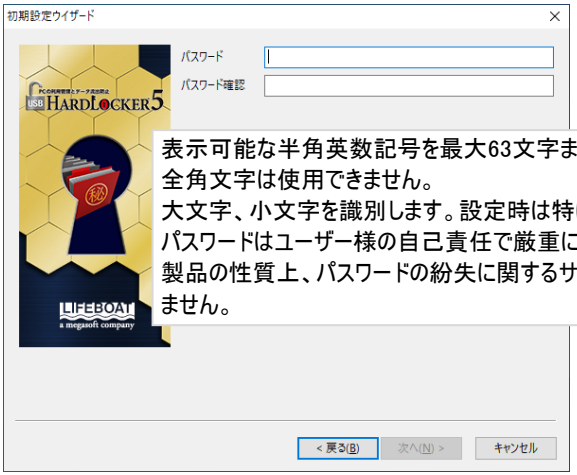
2. 「USB」または「USB × パスワード」を選択した場合はハードウェアの選択画面が表示されます。ハードウェア一覧に表示された USB 機器から鍵として使用したいものをチェックして「次へ」をクリックしてください（同時に複数の機器をチェックすることはできません）。「USB × パスワード」を選択した場合は、「次へ」をクリックすると「パスワード」を選択した場合（次頁参照）と同様のパスワードの設定画面が表示されます。



※ USBマウスやキーボードの多くは「ベンダーID」「プロダクトID」のみで、「シリアル番号」を持っていません(下図の例)。そのような機器は同じ型番のすべてが「合鍵」となってしまうので、鍵として適していません。鍵に設定する機器は上図のようにシリアル番号を持つものをご利用ください。

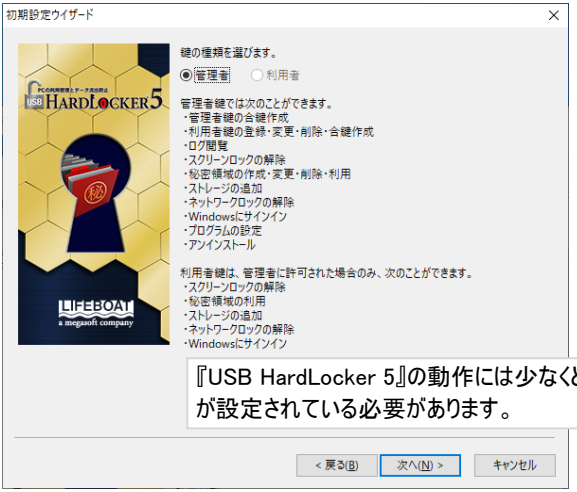
シリアル番号がない機器の例
（USB キーボード）

「パスワード」を選択した場合はパスワード入力画面が表示されるのでパスワードを入力して「次へ」をクリックしてください。



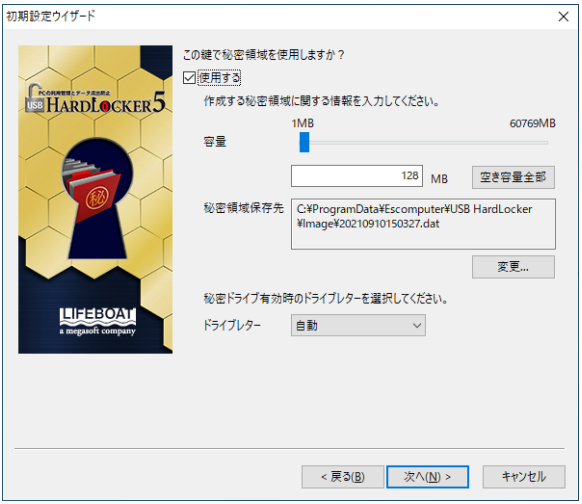
表示可能な半角英数記号を最大63文字まで設定できます。
全角文字は使用できません。
大文字、小文字を識別します。設定時は特にご注意ください。
パスワードはユーザー様の自己責任で厳重に管理してください。
製品の性質上、パスワードの紛失に関するサポートはご提供できません。

3. 鍵の種類を選択する画面が表示されます。初めて鍵を設定する際は管理者鍵が自動的に選択されるのでそのまま「次へ」をクリックしてください。

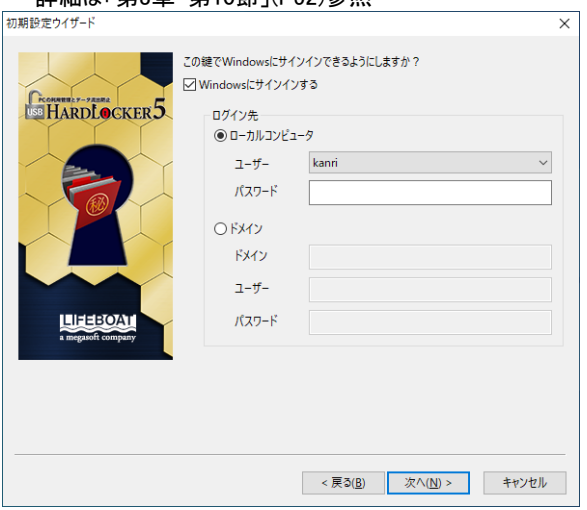


『USB HardLocker 5』の動作には少なくとも1つの管理者鍵が設定されている必要があります。

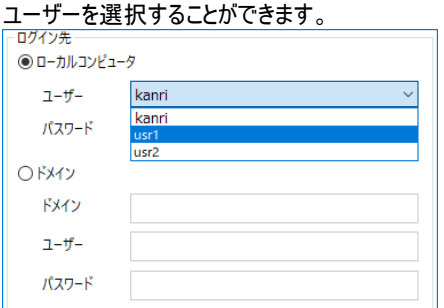
4. 秘密領域使用の有無を選択してください。秘密領域を使用する場合は、「使用する」をチェックして設定をします。
※ 秘密領域は鍵の作成完了後に追加することも可能です。初期設定ではチェックを外しておき、必要な場合に後から追加設定することをお勧めします。
（秘密領域の設定は P43 参照）。



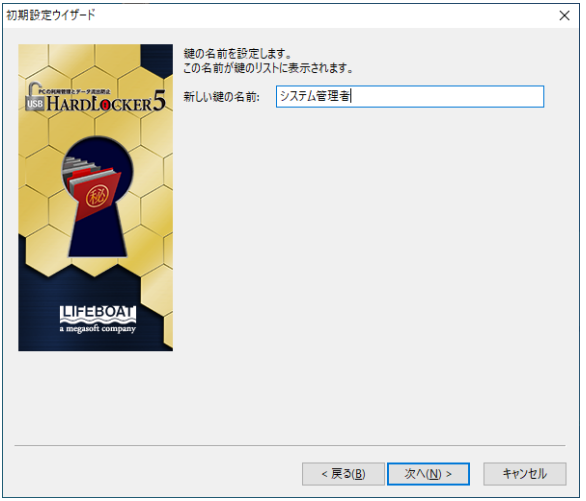
5. 鍵をWindowsユーザーと関連付ける場合 、「Windowsにサインインする」をチェック、ユーザー名とパスワードを入力して「次へ」をクリックします。
関連付けを行うと、鍵を装着してWindowsにログオン(同時に『USB HardLocker 5』のロック解除)することができます。
※ ユーザーとの関連付けをする場合はUSB鍵を選択してください。
※ ユーザーとの関連付けは鍵の作成完了後に追加することも可能です。
詳細は「第3章 第10節」(P52)参照



ローカルユーザー(含マイクロソフトアカウント)またはドメインユーザーを選択することができます。



6. 設定する鍵の名前を入力して「次へ」をクリックしてください。



7. 作成した鍵の内容が表示されます。内容を確認して「完了」をクリックしてください。
設定内容に問題があれば「戻る」で変更することができます。

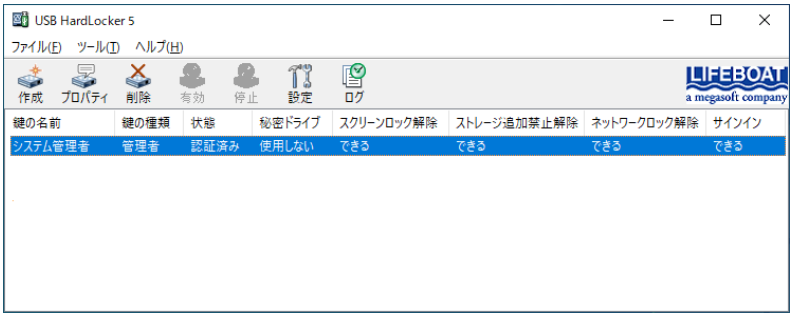
この画面では次の内容を確認することができます。

認証方法	USB、パスワード、USB × パスワードの区別を表示
ベンダーID	ハードウェアベンダーの ID 番号
プロダクト ID	製品の ID 番号
シリアル番号	製品のシリアル番号
秘密領域	秘密領域使用の有無
容量	秘密領域を使用する場合の容量
秘密領域保存先	秘密領域を使用する場合の保存先
ドライブレター	秘密領域に割り当てるドライブレター
スクリーンロック解除	スクリーンロック解除機能の有無
ストレージ追加解除	ストレージ追加禁止解除機能の有無
ネットワークロック解除	ネットワークロック解除機能の有無
Windows サインイン	鍵と Windows ユーザーの関連付けの有無
鍵の種類	管理者鍵、利用者鍵の区分
鍵の名前	鍵を設定する時に指定した名前

第3章　USB HardLocker 5 を使用する

第1節　ユーティリティ

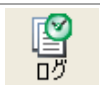
Windows の「スタート」から「USB HardLocker」-「USB HardLocker ユーティリティ」を選択するか、タスクトレイのアイコンをクリックすると「ユーティリティ」が起動します。『USB HardLocker 5』の主な操作はユーティリティ上のメニューボタンからすることができます。



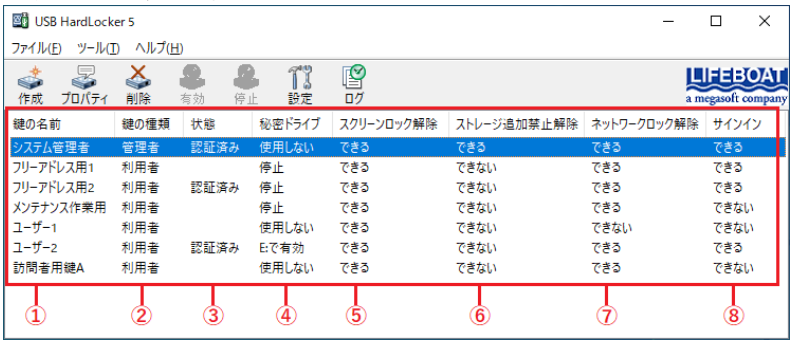
※　管理者鍵が装着されている場合と、利用者鍵のみ装着されている場合では、操作できる内容が異なります。
操作できる内容については、次のページの＜メニューボタンの説明＞をご覧ください。

※　Windows 8.1 の Modern UI Style の場合、「スタート」から「USB HardLocker ユーティリティ」を選択します。

＜メニューボタンの説明＞

	鍵作成ウィザードが起動します。新規に鍵を作成する時に使用します（P28 参照）。 （管理者鍵装着中の場合のみ操作できます。）
	選択した鍵の機能設定、秘密領域、認証方法の表示、変更ができます。
	選択した鍵を削除します。 ※ 設定されている管理者鍵が 1 つだけの場合、その管理者鍵を削除 することはできません。 （管理者鍵装着中の場合のみ操作できます。）
	選択した鍵に設定した秘密領域を使用可能にします。
	選択した鍵に設定した秘密領域を停止します。
	『USB HardLocker 5』の「全般設定」、「スクリーンロック」、「ストレージ追加禁止」、「ネットワークロック」、「ログ」の有効／無効、設定変更を行います。（管理者鍵装着中の場合のみ操作できます。）
	ログをリアルタイムに表示します。（P61）参照 （管理者鍵装着中の場合のみ操作できます。）

＜鍵ステータス表示の説明＞



①	鍵の名前	鍵を設定する時に指定した名前を表示します。
②	鍵の種類	管理者鍵、利用者鍵の識別を表示します。
③	状態	現在の鍵の状態を表示します。 認証済み ---鍵が装着されています。 空白 ---鍵は装着されていません。
④	秘密ドライブ	停止 ---秘密領域は停止中です。 「X:」で有効 ---秘密領域はドライブ「X」で使用可能です。 使用しない ---この鍵では秘密領域を作成していません。
⑤	スクリーンロック解除	スクリーンロック解除の可否を表示します。
⑥	ストレージ追加禁止解除	ストレージ追加禁止解除の可否を表示します。
⑦	ネットワークロック解除	ネットワークロック解除の可否を表示します。
⑧	サインイン	Windows ユーザー関連付けの可否を表示します。

①～⑧は項目名の部分をクリックしてソートすることができます。

※ 管理者鍵が装着されている場合、設定済みの鍵は装着されていないものも含めてすべて一覧に表示されます。

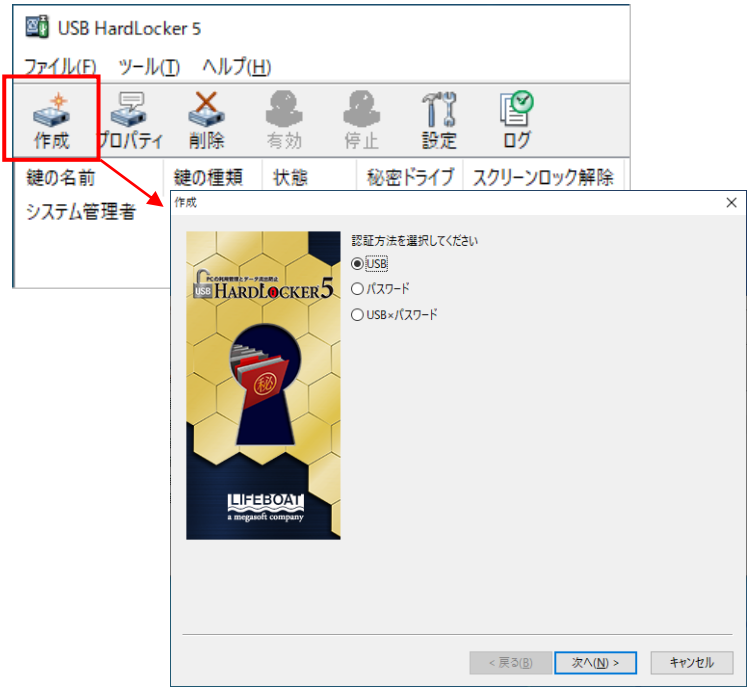
※ 利用者鍵のみ装着されている状態では、他の設定済みで未装着の鍵は一覧に表示されません。

第2節　鍵の作成と設定変更

ユーティリティ画面から鍵を作成する方法と設定済みの鍵を変更する手順について説明します。

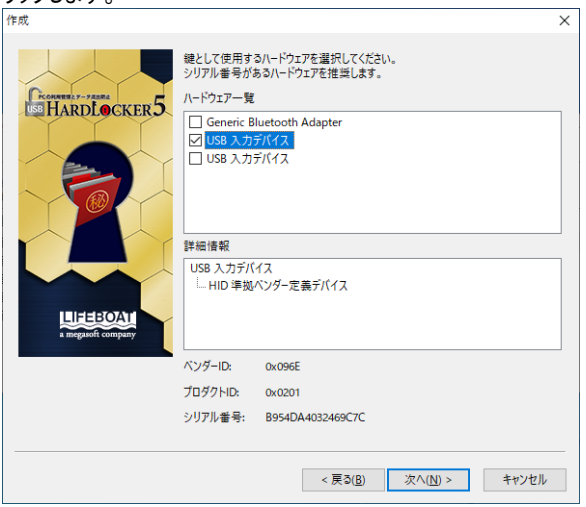
鍵の新規作成(追加)

1. ユーティリティから「作成」をクリックすると作成ウィザードが起動します。
   使用したい認証方法を選択して「次へ」をクリックします。



「パスワード」を選択した場合は次頁のパスワード設定画面が表示されます。
「USB × パスワード」を選択した場合は、使用するハードウェアを選択した後でパスワード設定画面が表示されます。

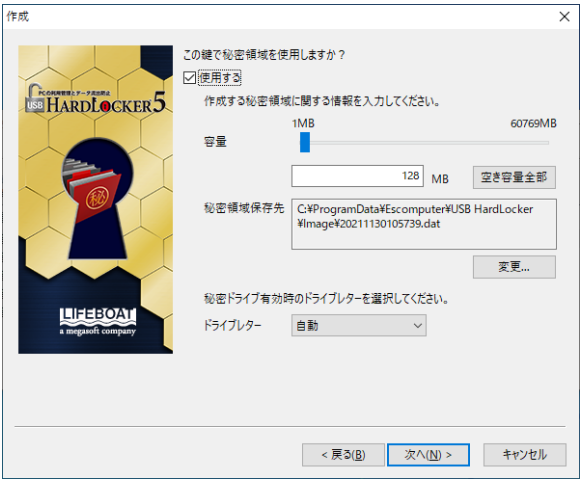
2. 「USB」、「USB × パスワード」を選択した場合はハードウェアを選択する画面が表示されるので、「ハードウェア一覧」から使用するハードウェアを選択して「次へ」をクリックします。



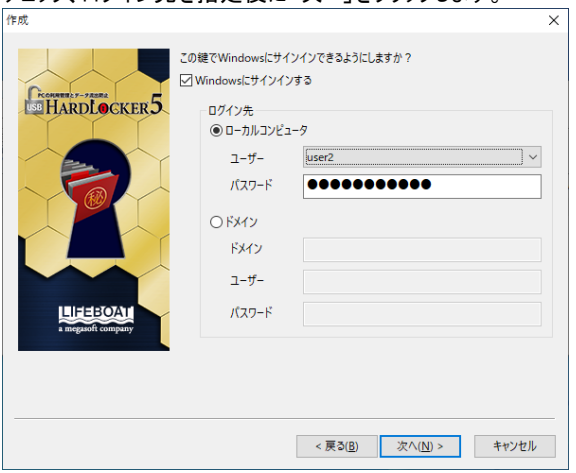
パスワード設定画面

3. 鍵の種類を選択して「次へ」をクリックします。
管理者鍵、利用者鍵の機能については、(P7)参照。

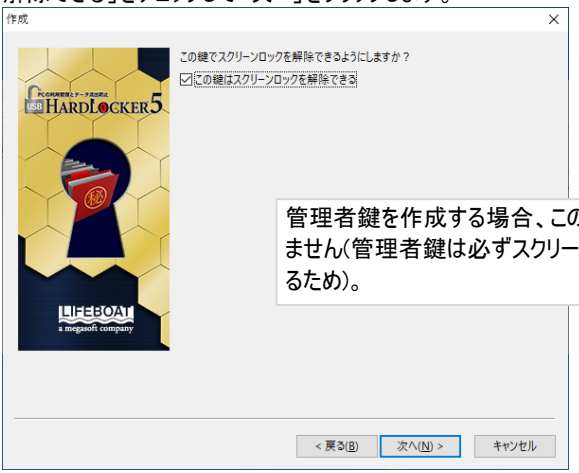
4. 秘密領域使用の有無を選択します。使用する場合は、「使用する」をチェックしてサイズを設定します（鍵の作成後に「プロパティ」から作成することも可能です）。



5. この鍵を Windows ユーザーに関連付けする場合は「Windows にサインインする」をチェック、ログイン先を指定後に「次へ」をクリックします。

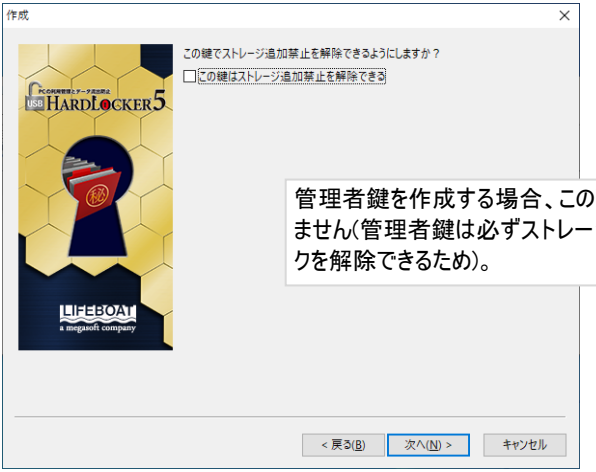


6. この鍵をスクリーンロックの解除用に使用したい場合は「この鍵はスクリーンロックを解除できる」をチェックして「次へ」をクリックします。



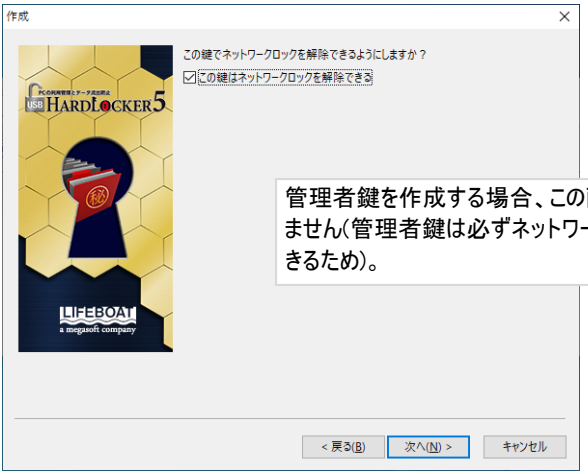
管理者鍵を作成する場合、この画面は表示されません(管理者鍵は必ずスクリーンロックを解除できるため)。

7. ストレージの追加禁止を解除できるようにしたい場合は「この鍵はストレージ追加禁止を解除できる」をチェックして「次へ」をクリックします。



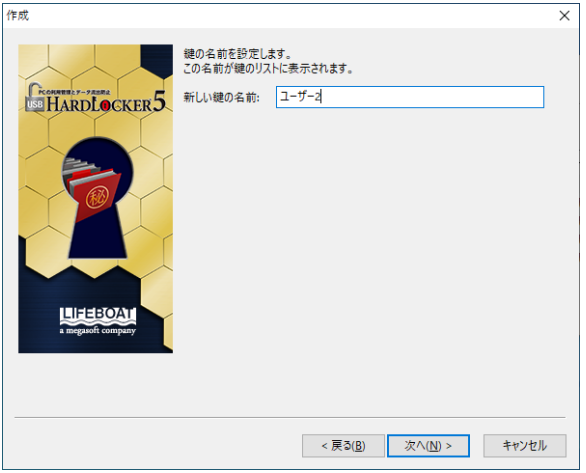
管理者鍵を作成する場合、この画面は表示されません(管理者鍵は必ずストレージ追加禁止ロックを解除できるため)。

8. ネットワークロックを解除できるようにしたい場合は「この鍵はネットワークロックを解除できる」をチェックして「次へ」をクリックします。

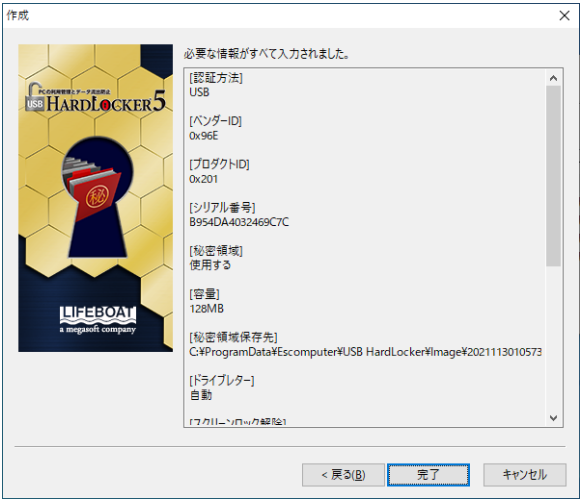


管理者鍵を作成する場合、この画面は表示されません(管理者鍵は必ずネットワークロックを解除できるため)。

9. この鍵を識別するための名前を入力して「次へ」をクリックします。
※ 特殊文字や記号は鍵の名前に使用しないでください。



作成した鍵の設定内容が表示されます（表示される内容は初期設定の設定確認画面で表示されるものと同様です）。内容を確認して「完了」をクリックします。
設定内容を修正したいときは「戻る」で変更することができます。

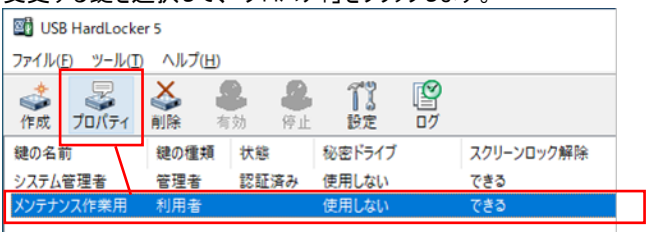


鍵の設定変更

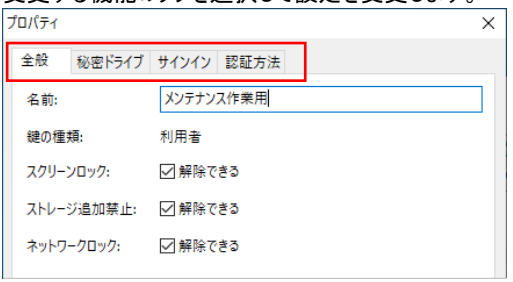
作成済みの「鍵」に対して、名前・各機能(秘密ドライブ・スクリーンロック解除・ストレージ追加禁止解除・ネットワークロック解除・サインイン)の設定を変更可能です。

※ 利用者鍵の設定変更時は「管理者鍵」を装着しておく必要があります。

変更する鍵を選択して、「プロパティ」をクリックします。



変更する機能のタブを選択して設定を変更します。



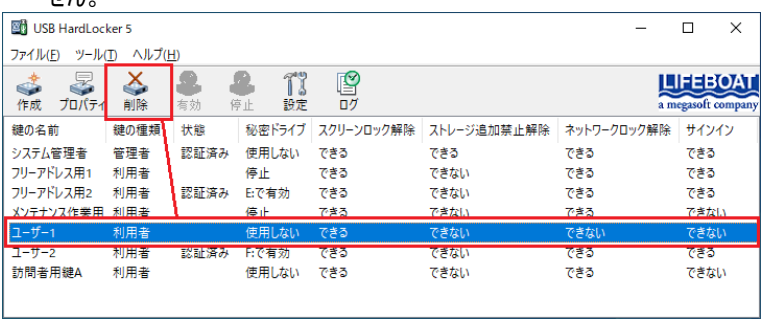
＜各タブの設定内容＞

全般	スクリーンロック、ストレージ追加禁止、ネットワークロックの可否を設定します。
秘密ドライブ	秘密ドライブの設定を変更します。「☑使用する」のチェックを外すと、作成済みの秘密ドライブは削除され復元することはできません。第 6 節(P43)参照
サインイン	Windows ユーザーとの関連付けを変更します(USB 機器を鍵に設定している場合のみ)。第 10 節(P52)参照
認証方法	鍵デバイスを変更・追加します。ここで鍵を追加して合鍵を設定することができます。第 4 節(P37)参照

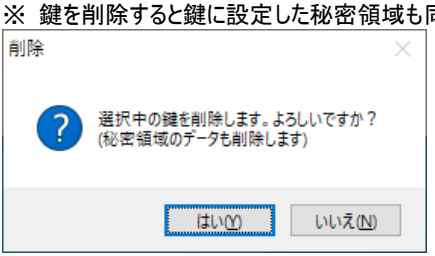
第3節　鍵の削除

設定した鍵を削除したい場合はユーティリティから削除します。

1. 削除したい鍵を選択して「削除」をクリックします。
   ※ 管理者鍵が一本だけの場合、削除することはできません。
   ※ 管理者鍵が装着されていない状態で、利用者鍵を削除することはできません。



2. 鍵を削除するための確認メッセージが表示されるので、よろしければ「はい」をクリックします。選択した鍵が削除されます。
   ※ 鍵を削除すると鍵に設定した秘密領域も同時に削除されます。

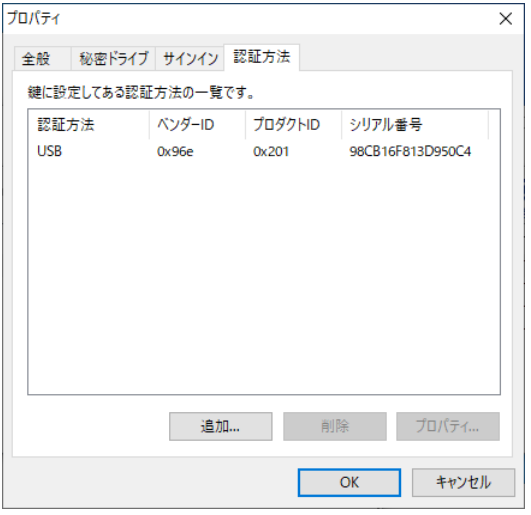


第4節　合鍵の設定

設定した鍵の破損や紛失に備えて合鍵を設定することができます。
※「USB 機器」「USB 機器×パスワード」「パスワード」のいずれも設定可能です。

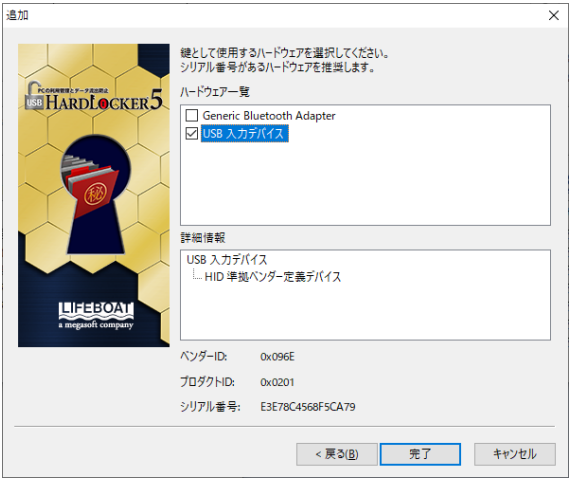
1. 合鍵を設定する鍵を選択して「プロパティ」をクリックします。

2. 「認証方法」タブから「追加」をクリックします。

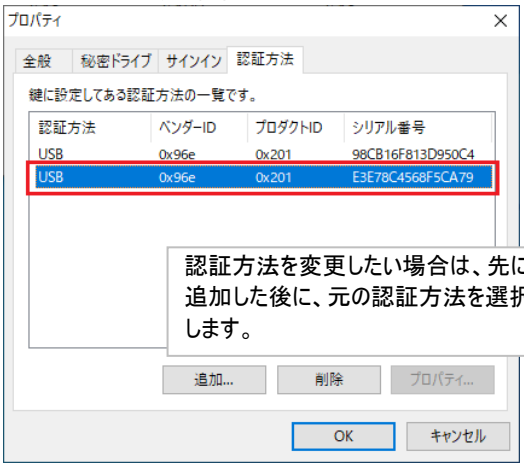


3. 設定したい認証方法を選択して「次へ」をクリックします。
ここでは合鍵として「USB」を設定する場合を例にして説明します。

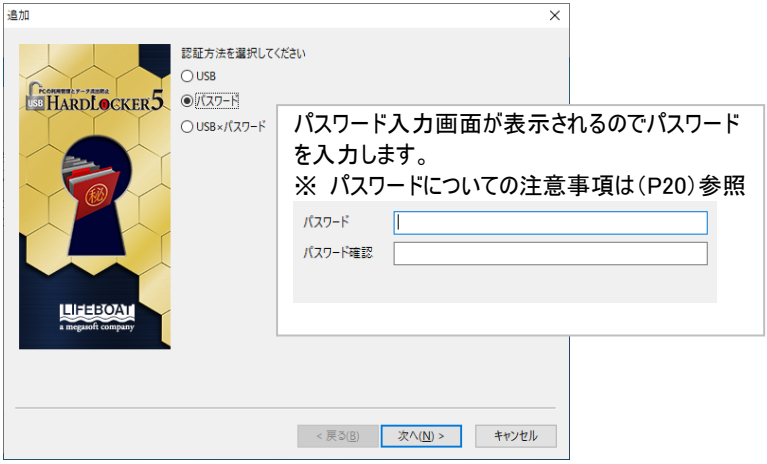
4. 設定可能なUSB機器が表示されるので、リストから1つ選択してチェック後「完了」をクリックします。複数の合鍵を設定したい場合は、**2.**– **4.**の操作を繰り返し実行してください。



5. 追加されたUSB鍵が認証方法リストに追加されます。

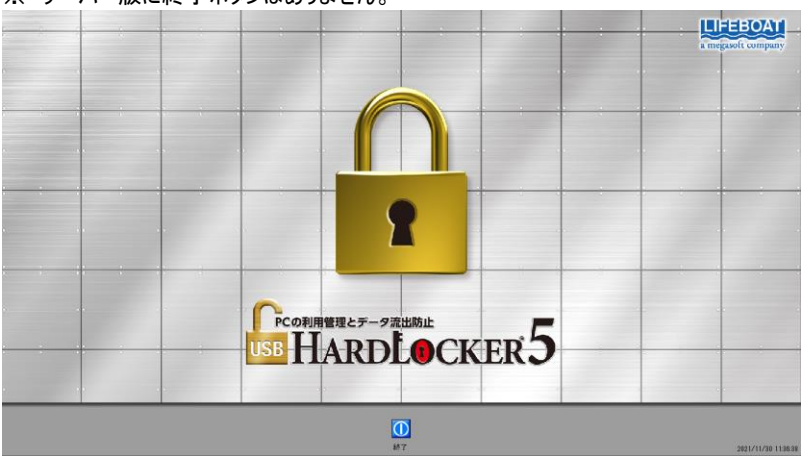


6. パスワードを追加する場合は5. の鍵の「プロパティ」-「認証方法」から「追加」をクリックして「パスワード」を選択します。



第5節　コンピューターのロックと解除

＜コンピューターのロック＞
スクリーンロックを使用する設定をした場合、以下の操作でスクリーンがロックされスクリーンロック画面が表示されます。ロックされた状態では、シャットダウン以外の操作は実行できません。シャットダウンはスクリーンロック画面下部の「終了」ボタン※をクリックします。
※ サーバー版に終了ボタンはありません。



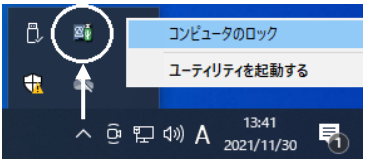
この他に、許可しないUSB機器やドライブが追加された時にスクリーンをロックする機能があります（P49参照）。

＜ロックするための操作方法＞

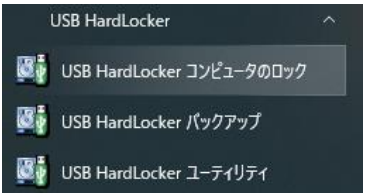
設定した鍵の種類	操作方法
USB	鍵を取り外します。
パスワード	「コンピューターのロック」操作（※）をします。
USB×パスワード	鍵を取り外します。

※ コンピューターのロック操作：　次の3通りの方法でコンピューターのロックの操作をすることができます。

ロック方法A. Windowsツールバーのアイコンを右クリックして「コンピューターのロック」を選択します。



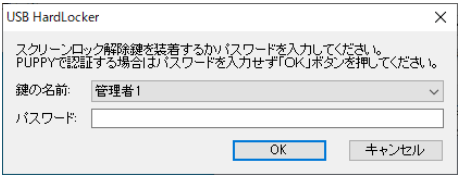
ロック方法B. 「スタート」から「USB HardLocker」-「コンピューターのロック」を選択します。



ロック方法C. ショートカットキー（「Ctrl」＋「Shift」＋「L」）を入力する。

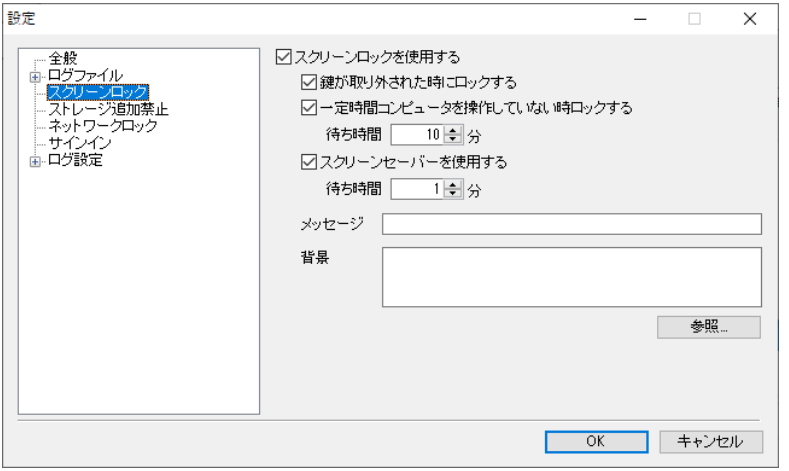
＜ロックの解除方法＞ 3 通りの方法いずれでも解除できます。

鍵の種類	操作方法
USB	鍵を装着します。
USB＋パスワード	鍵を装着後パスワード入力画面が表示されるのでパスワードを入力します。
パスワード	「Ctrl」+「Shift」+マウスの左クリックによりパスワード入力画面を表示してパスワードを入力します。



※ **鍵が装着された状態で「コンピューターのロック操作」をした場合**のロック解除は「Ctrl」+「Shift」+マウスの左ボタンをクリックします。

＜スクリーンロックの設定＞
ユーティリティから「設定」をクリックして「スクリーンロック」タブを選択します。スクリーンロックの設定画面が表示されます。



＜項目の説明＞

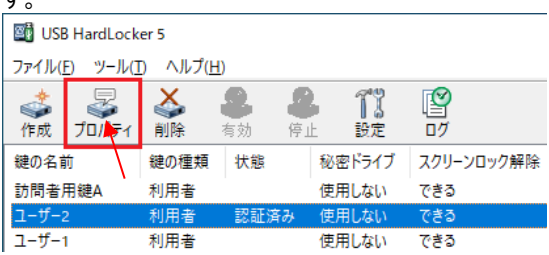
スクリーンロックを使用する	スクリーンロック機能を有効にします。
鍵が取り外された時にロックする	設定した鍵を取り外した時にスクリーンをロックします。
一定時間コンピュータを操作していない時ロックする	指定した時間、コンピューターを操作していないと、スクリーンがロックされます。
スクリーンセーバーを使用する	スクリーンのロック後、指定された時間が経過した後にスクリーンセーバーを起動します。
メッセージ	スクリーンロック画面（P40）の下部に、指定したメッセージを表示することができます。
背景	ロック画面を他の画像に変更することができます。「参照」をクリックして使用したい画像を指定します（形式はBMPのみ）。※

※ 初期設定時のサイズは 1280×800 ピクセルですが、1024×768、1366×768 の画像が用意されています。

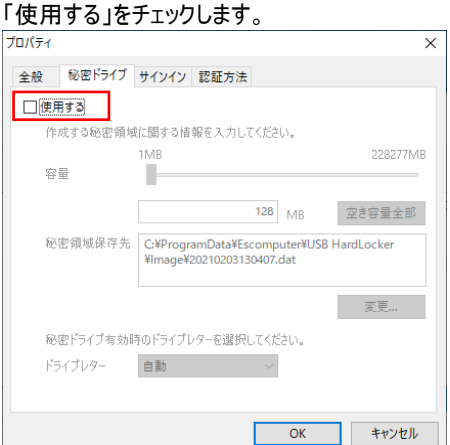
第6節　秘密領域の設定

秘密領域の設定には 2 通りの方法があります。
※ 秘密領域の作成先は内蔵ドライブ(ハードディスク、SSD)のみとなります。
リムーバブルドライブ等を指定することはできません。
A. 鍵の設定時に作成ウィザードから秘密領域を設定する。
B. 鍵を設定した後でユーティリティから鍵の「プロパティ」をクリックして秘密領域を設定する。
この節では「プロパティ」からの設定方法を説明します。鍵設定時の秘密領域の作成は「第 2 節」(P21)をご参照ください。

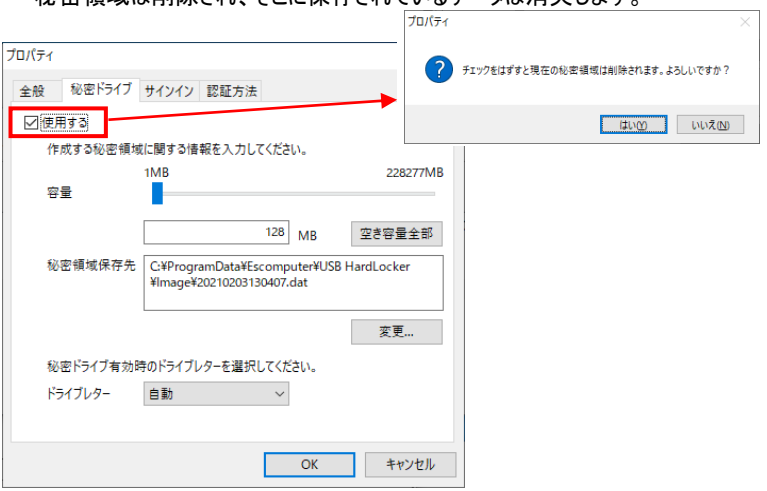
1. 「ユーティリティ」から鍵の「プロパティ」をクリックして「秘密ドライブ」タブを選択します。



2. 「使用する」をチェックします。



3. 「使用する」をチェックすると、秘密領域のサイズや保存先を指定できます。
※ 秘密領域が作成済みの場合にこのチェックをはずして「OK」をクリックすると、警告メッセージが表示されます。ドライブレター以外の変更をすると、既存の秘密領域は削除され、そこに保存されているデータは消失します。



4. 作成する秘密領域のサイズを指定します。「容量」のスライドバーを操作するか、入力ボックスにサイズ(MB)を正の整数で入力してください。
「空き容量全部」をクリックすると秘密領域保存先に指定したドライブの空き容量すべてを割り当てます。
※ システムがインストールされたドライブの場合は「空き容量全部」をクリックしないでください。

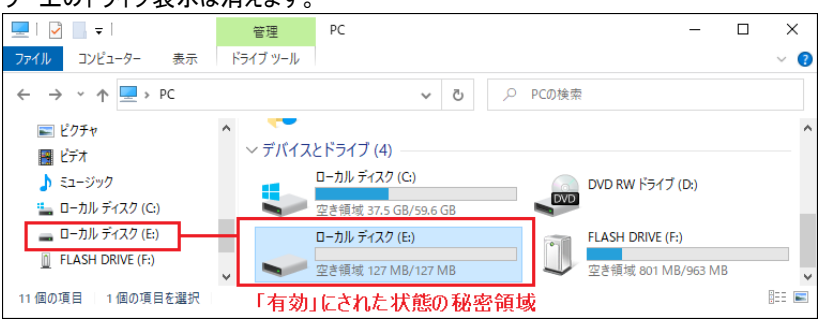
5. 秘密領域の保存先を指定します。「秘密領域保存先」に保存先のパスが表示されます。パスを変更する場合は「変更」でエクスプローラーが起動します。任意のパスを選択してください。
※ 秘密領域の保存先にドライブのルートを指定しないでください。

6. 秘密領域のドライブレターを指定したい場合はプルダウンリストから任意のドライブレターを指定します。自動を選択すると、空いているドライブレターが割り当てられます。

第7節　秘密領域の使用

ユーティリティ画面から、秘密領域を設定した鍵を選択して「有効」をクリックすると秘密領域がコンピューターのファイルシステムにマウントされ使用できるようになります。

「有効」状態の秘密領域はエクスプローラー上からは他のドライブと同じように表示され、ファイルの書き込み、読み取りが自由にできます。秘密領域を「停止」するとエクスプローラー上のドライブ表示は消えます。



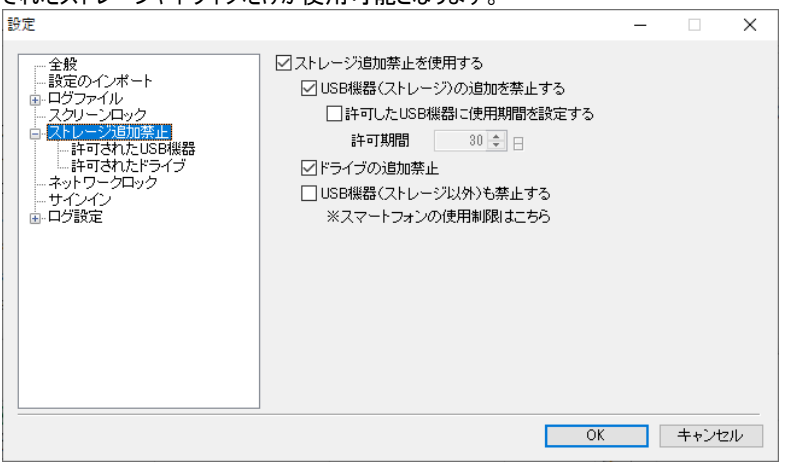
※ 秘密領域は自動的に FAT または FAT32 にフォーマットされます。

※ 1ファイルのサイズが4GBを超えるデータを保存する場合は、ドライブのプロパティを開いて、ドライブをNTFSで再フォーマットする必要があります。フォーマットは秘密領域にデータを保存する前に実行してください。データを保存した後でフォーマットを実行すると、保存したデータはすべて消失します。

※ バックアップツール（P91 参照）を使用して秘密領域のバックアップすることができます。

第8節　ストレージ追加禁止

使用できる USB ストレージやドライブ、その他 USB 機器の利用を制限するときに「ストレージ追加禁止を使用する」をチェックします。この設定を有効にすると、許可リストに登録されたストレージやドライブだけが使用可能となります。



＜チェックボックスの内容＞

USB機器(ストレージ)の追加を禁止する	USBストレージとのデータ読み書きを禁止します。
許可したUSB機器に使用期間を設定する	チェックして許可期間を入力すると使用期間を設定できます。ここで設定しない場合、後から機器ごとに期間を含めた設定をすることができます(次頁参照)。
ドライブの追加禁止	エクスプローラー上に新たなドライブレターを追加できないようにして新規ドライブの利用を禁止します。
USB機器(ストレージ以外)も禁止する	スマートフォンやメディアプレーヤー機器等とのデータ読み書きを禁止します。この設定をチェックするとマウスやキーボード等の利用も管理者の許可が必要になります。

※「USB 機器の追加を禁止する」と「ドライブの追加禁止」は利用者鍵ユーザーUSB 利用を制限するための機能です。
利用者鍵ユーザーにストレージ追加禁止ロックの解除機能を付与する場合は、鍵を選択して「設定」-「全般」の「ストレージ追加禁止： 解除できる」をチェックします。

＜USB 機器の登録方法＞

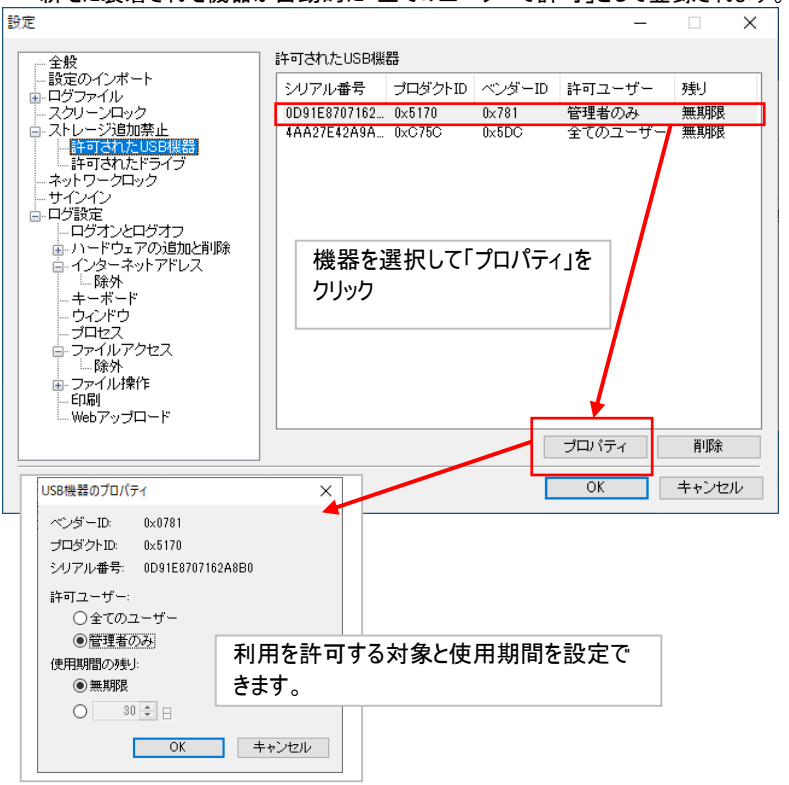
「ストレージ追加禁止を使用する」(前頁)をチェックした環境で、管理者鍵を装着します。(リストへの登録自体はストレージ追加禁止解除を許可されている利用者鍵も可能ですが、設定変更はできません)。

上記の鍵が装着された状態で接続された USB ストレージやドライブは、自動的に許可リストに登録されます。

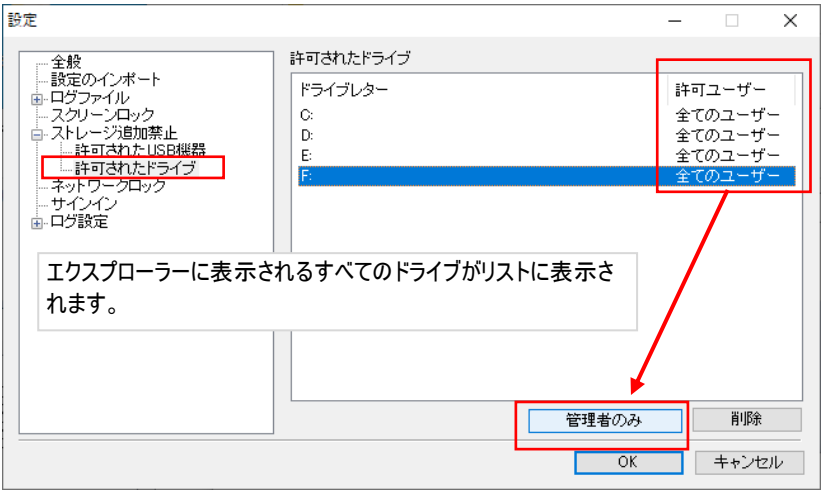
「許可された USB 機器」を選択すると、以下の機器リストが表示されます。許可ユーザーの変更ボタンで、機器の利用を許可するユーザーを変更できます(許可ユーザーの種類は「管理者のみ」と「全てのユーザー」の 2 種類です)

利用者鍵ユーザーに使用させない USB 機器は「管理者のみ」に変更してください。

※ 管理者鍵または「ストレージ追加禁止解除」を許可された利用者鍵の装着中は、新たに装着された機器が自動的に「全てのユーザーで許可」として登録されます。



＜ドライブの登録方法＞
「ストレージ追加禁止を使用する」をチェックした環境で、管理者鍵を装着します。
「許可されたドライブ」を選択すると以下の機器リストが表示されます。許可ユーザーの変更ボタンで機器の利用を許可するユーザーを変更できます。
利用者鍵ユーザーに使用させないドライブは「管理者のみ」に変更してください。

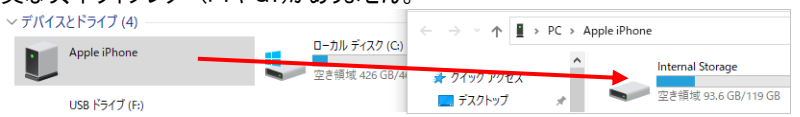


USB 機器の追加禁止(上記)と同様にリストを作成します。解除権限のない鍵だけが接続された状態で、ドライブの追加ができなくなります。

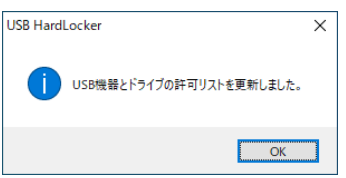
ローカル PC にマウントしたネットワークドライブもドライブの追加禁止対象に含まれます。
ネットワークドライブを使用する環境では、これらのドライブ(一般的に X、Y、Z 等のアルファベット末尾のドライブレター)も許可リストに加えておくことをお勧めします。

＜ストレージ以外の USB 機器も禁止する＞
スマートフォンや携帯音楽プレーヤー等は、データを書き込める状態でも、ストレージとして認識されないことがあります。このような機器やキーボード、マウス等の新規接続を禁止する場合にチェックします。

下図はスマートフォンを接続した例ですが、ハードディスクやUSBフラッシュメモリー等とは異なり、ドライブレター(F:やG:)がありません。

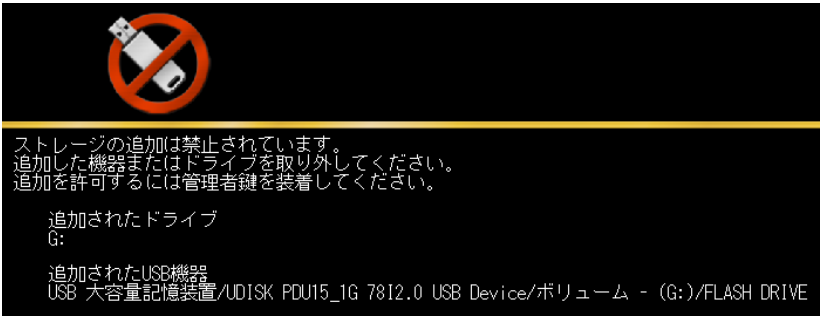


＜許可リストの更新＞
管理者鍵、またはストレージ追加禁止解除を許可する鍵が装着されている状態で新しいUSBストレージやドライブを接続すると、右のメッセージが表示され許可リストが更新されます。



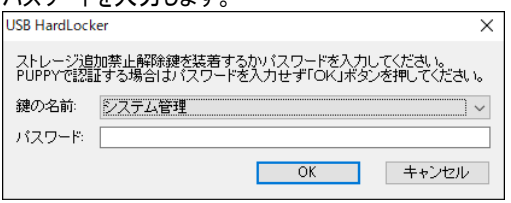
＜ストレージ追加禁止ロック＞
ストレージの追加権限のない状態で許可リストにない新しい USB ストレージを装着したり新しいドライブを追加したりすると、次のような画面が表示されてスクリーンがロックされます。この時、コンピューターの操作は、シャットダウン以外実行できなくなります。シャットダウンはロック画面下部中央の「終了」ボタン※をクリックします。
※ サーバー版に終了ボタンはありません

ロック画面には、接続された非許可の USB 機器名およびドライブ名が表示されます。



＜ストレージ追加禁止ロックの解除方法＞
ストレージ追加禁止ロックを解除するためには、禁止された機器を取り外す、またはストレージ追加禁止解除の権限を持つ鍵を装着する必要があります。

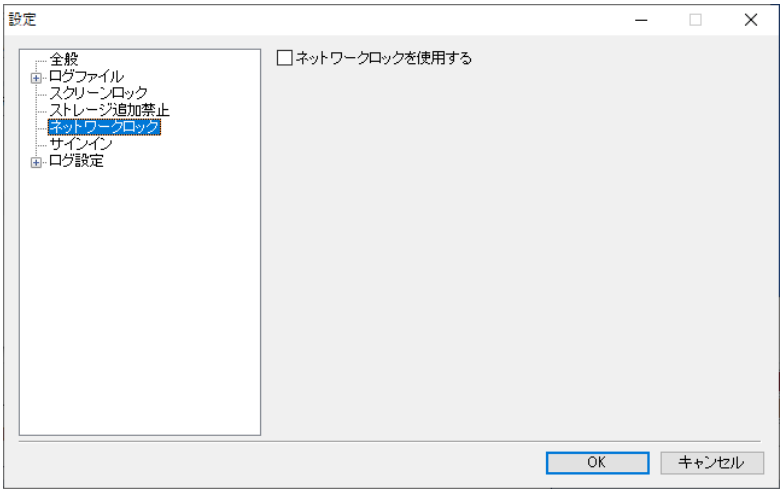
USB 鍵の場合は鍵を装着します。
パスワード鍵の場合は「Ctrl」+「Shift」+マウスの左クリックでパスワード認証画面を表示させ、パスワードを入力します。
USB×パスワード鍵の場合は USB を装着するとパスワード認証画面が表示されるのでパスワードを入力します。



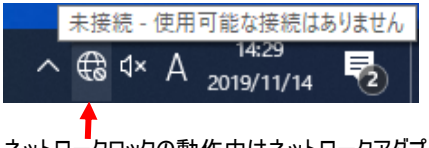
※ 鍵を取り外してスクリーンロックをかけている場合に許可されていない機器を追加すると、スクリーンロックが二重に動作している状態になります。

第9節　　ネットワークロック

鍵の取り外しにより、ネットワークの接続を遮断することができます。スクリーンロックと組み合わせて、ロック時に、外部からの不正アクセスを遮断することもできます。
※　スクリーンロックと組み合わせず単独で動作させることもできます。
※　ネットワークロックを使用する場合、ログの保存先をネットワーク上の共有ドライブにしないようご注意ください。保存先にアクセスできず、ログの保存ができなくなります。



「ネットワークロックを使用する」をチェックしていると、鍵が取り外された時、ネットワークへの接続ができなくなります。



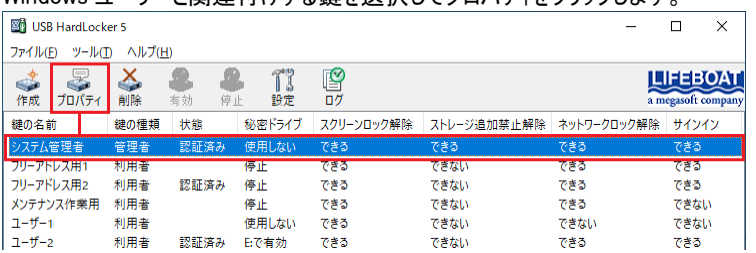
ネットワークロックの動作中はネットワークアダプターが無効になります。複数のネットワークアダプターが存在する環境ではすべてのアダプターが使用不可になります。
（上図はスクリーンロック機能を OFF にして、ネットワークロックのみ動作させた場合のタスクトレイの表示です。）

第10節　鍵と Windows ユーザーの関連付け

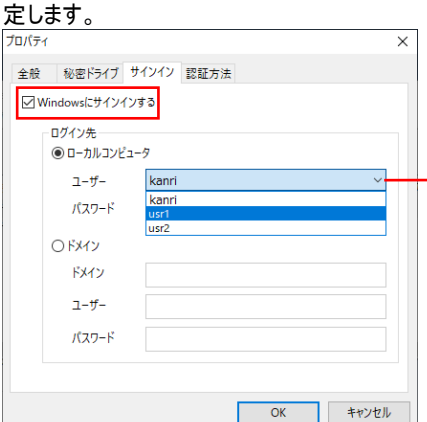
USB 鍵を Windows ユーザーに関連付けることで、鍵を装着して Windows のログオン(サインイン)と『USB HardLocker 5』のスクリーンロック解除を同時に実行することができます。

手順

1. Windows ユーザーと関連付けする鍵を選択してプロパティをクリックします。



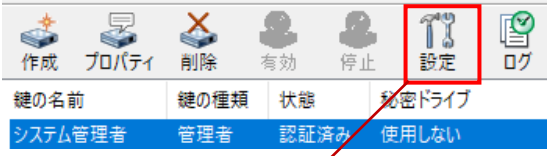
2. 「サインイン」タブから「Windows にサインインする」をチェックして、「ログイン先」を指定します。

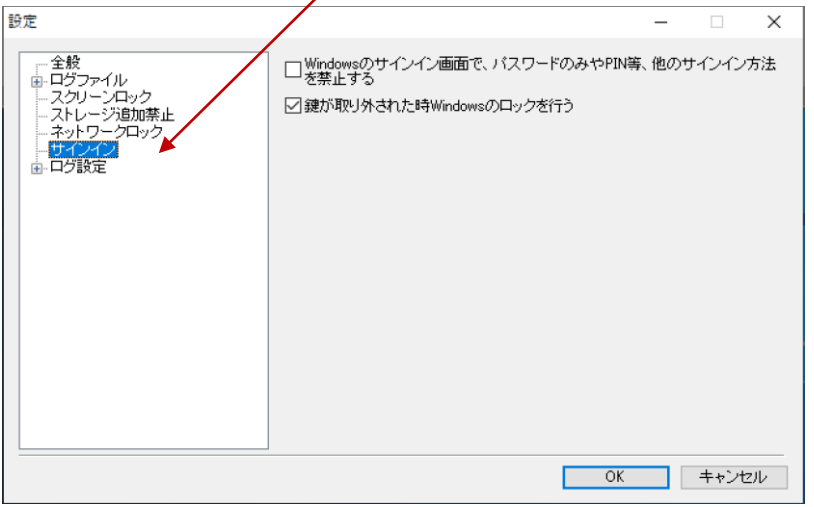


PC に登録済のユーザー名をプルダウンリストから選択してパスワードを入力します。

ドメインの場合は、「ドメイン名」「ユーザー名」「パスワード」を入力してください。

＜サインインオプション＞
鍵を Windows ユーザーに関連付けている場合のオプションを設定することができます。
ユーティリティの「設定」-「サインイン」を選択します。





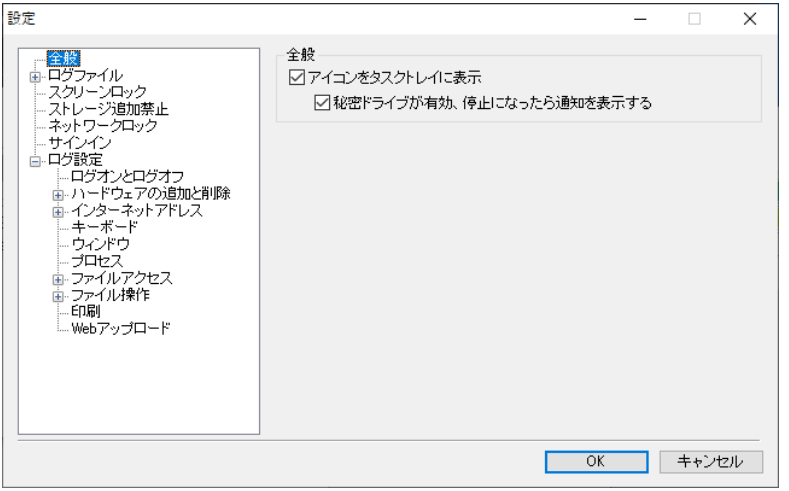
＜設定できる内容＞

Windowsのサインイン画面で、パスワードのみやPIN等、他のサインイン方法を禁止する
サインイン方法を『USB HardLocker 5』の鍵装着に限定します。

鍵が取り外された時 Windows のロックを行う
『USB HardLocker 5』のスクリーンロックと同時に、Windowsのロックが実行されます。
複数のWindowsユーザーアカウントを設定している環境や、単一のWindowsユーザーアウカウントを複数人で利用する場合はチェックすることをお勧めします。

第11節　その他設定

「設定」-「全般」を選択してタスクトレイアイコンの表示や通知を設定できます。



＜設定できる内容＞

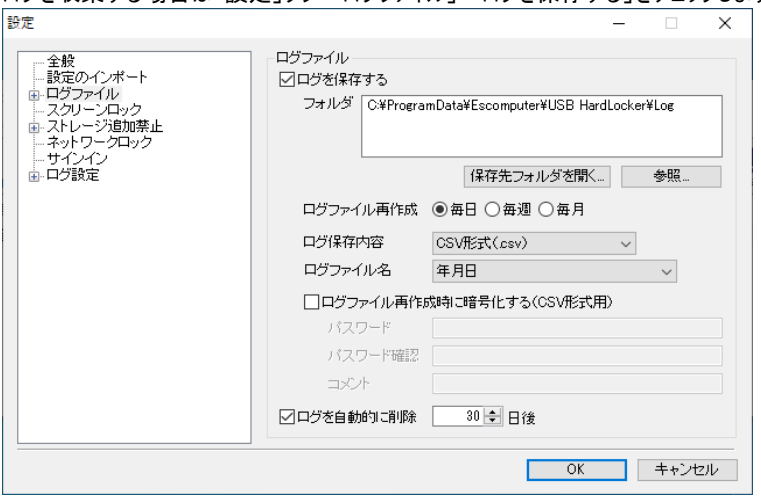
アイコンをタスクトレイに表示	チェックすると、タスクトレイ上にアプリケーションアイコン表示を設定します。 
秘密ドライブが有効、停止になったら通知を表示する	チェックすると、秘密領域の有効、停止時にポップアップで通知します。 

※ ログファイルに関する設定は「第 4 章」をご参照ください。

第4章　ログの収集と管理

第1節　ログの設定

＜ログ保存の選択＞
ログを収集する場合は「設定」タブ-「ログファイル」-「ログを保存する」をチェックします。

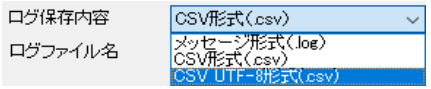


＜ログの保存先＞
初期設定時は以下のパスに保存されます（C: がシステムドライブの場合）。
「参照」から保存先を変更できます。
C:¥ProgramData¥Escomputer¥USB HardLocker¥Log

一切のログを記録したくない場合は「☑ログを保存する」のチェックをはずしてください。
記録する項目(P58)のチェックをすべてオフにしても「ロック」「ロック解除」「設定変更」等、USB HardLocker の動作に関するログは記録されます。

＜ログファイル再作成＞
ログは「毎日」、「毎週」、「毎月」の単位で記録することができます。初期設定値は「毎日」です。

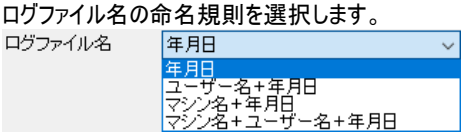
＜ログ保存内容＞
保存するログファイルの形式を選択します。



メッセージ形式（.log）	USB HardLocker独自の形式で記録され、暗号化されます。閲覧するためには、ユーティリティから「ログ」を起動するか、エクスポート(P63参照)する必要があります。
CSV形式（.csv）	Excelやメモ帳等を利用して開くことができます。解析等が必要な場合に選択することをお勧めします。
CSV UTF-8形式（.csv）	文字コードUTF-8のCSV形式ファイルです。

※ ログの形式を切り替えると、切り替えた時刻より、新しいファイルが生成され、以後のログが書きこまれます。記録が終了した切り替え前のログはそのまま保存されます。
※ UTF-8形式のログファイルは、kanri_211109_1u.csv　のように日付の後に「_u」の文字が挿入されます。

＜ログファイル名＞
ログファイル名の命名規則を選択します。



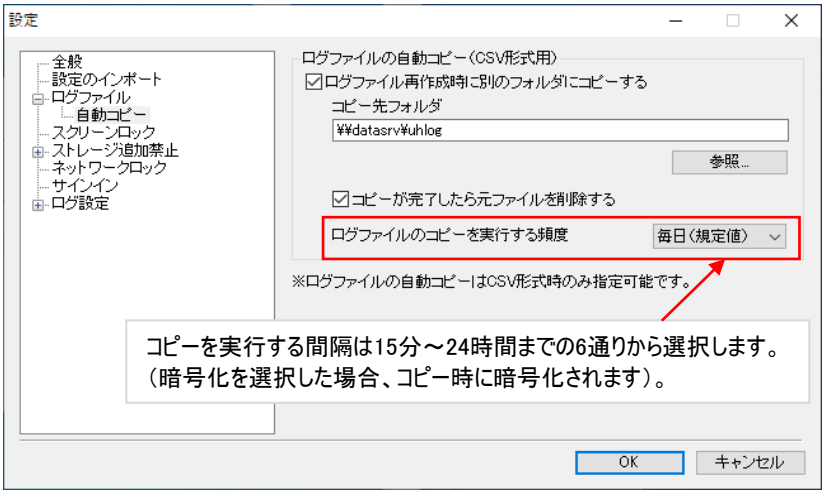
※ 選択により記録単位が変わります(ユーザー名を含めると、ファイルがユーザーごとに生成されます)。

年月日	20211212.csvのようなファイル名になります。1ファイルに複数のWindowsユーザーのログが記録されます。
ユーザー名＋年月日	LBuser20211212.csvのようなファイル名になります。Windowsのユーザー単位でログファイルが生成されます。
マシン名＋年月日	testpc20211212.csvのようなファイル名になります。1ファイルに複数のWindowsユーザーのログが記録されます。
マシン名＋ユーザー名＋年月日	testpc_LBuser_20211212.csvのようなファイル名になり、Windowsのユーザー単位でログファイルが生成されます。

＜ログファイル再作成時に暗号化する＞
CSV形式でログを記録する場合のみ選択できます。詳細は「第6節」（P66）参照。

＜ログを自動的に削除＞
チェックすると指定した日数を経過したログを自動的に削除します。ログのディスク消費量が問題となるような場合に使用すると便利です。

＜自動コピー＞
このオプションを選択すると、記録が終了したログを指定のフォルダーへコピーします（CSV形式を選択した場合のみ）。

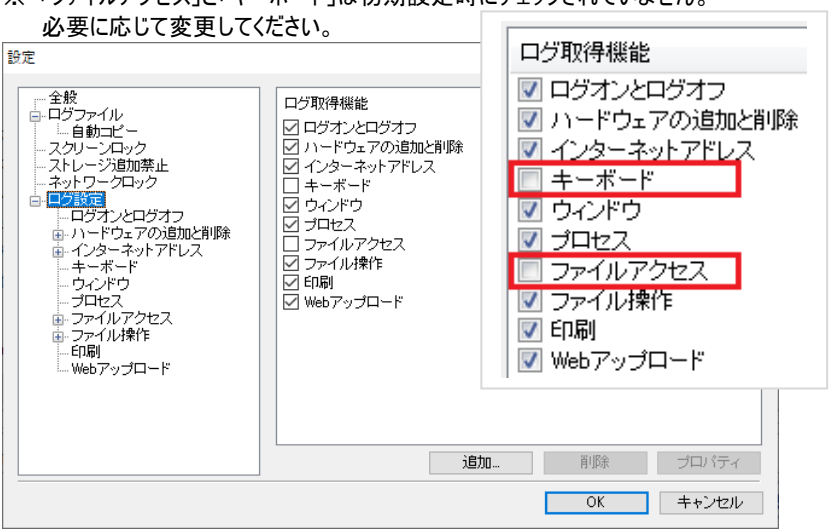


※ コピーが実行される時刻に、PC の電源が OFF の場合やコピー先のネットワークドライブに接続できない等の理由でコピーが実行できない場合、コピーが可能となった時点でコピーが実行されます。

自動コピーは、ネットワーク共有フォルダーにログを保存する場合に便利です。この場合、ログの保存先をローカルコンピューター上に設定し、次に自動コピーをチェックしてコピー先にネットワーク共有フォルダーを指定します。
ログの保存先をネットワークドライブ上に設定した場合、保存先に常時アクセスできないモバイル機ではログが記録されないケースが発生します。自動コピーを利用すると、ネットワーク切断時はローカル上にログを残せるため、記録漏れを回避することができます。

第2節　記録する項目の設定

「設定」タブ －「ログ設定」で記録できるログの一覧が表示されます。各項目のチェックのオン／オフでログ収集の有無を切り替えることができます。
各項目の詳細については、「第 7 節」(P68)参照
※「ファイルアクセス」と「キーボード」は初期設定時にチェックされていません。
　必要に応じて変更してください。



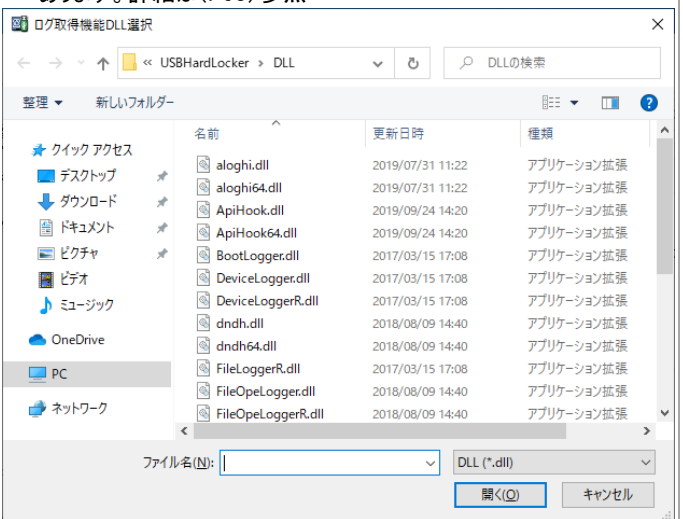
＜記録できるログの種類＞

ログオンとログオフ	「ログオン」、「スタンバイ」、「スタンバイからの復帰」、「ロック」、「ロックの解除」、「ユーザーの切り替え」、「ユーザーの切り替えからの復帰」、「ユーザーの切り替え(リモート)」、「ユーザーの切り替えからの復帰(リモート)」、「ログオフ」、「終了」を記録します。
ハードウェアの追加と削除	「ドライブレターの追加」、「ドライブレターの削除」、「デバイスの追加」、「デバイスの削除」を記録します。

インターネットアドレス ※1	Microsoft Edge、Internet Explorer、Google Chrome、Mozilla Firefox を使用してアクセスされた URL を記録します。
キーボード	キーボードの入力情報を記録します。
ウィンドウ	ウィンドウタイトルを監視し、「ウィンドウが開いた」、「ウィンドウが切り替えられた」の動作を記録します。
プロセス	プロセスを監視し、「すでに起動中のプロセス」、「プロセスの起動」、「プロセスの終了」のログを記録します。
ファイルアクセス	ファイルアクセスを記録します。
ファイル操作	ファイルの「コピー」、「移動」、「削除」、「リネーム」、「実行」を記録します。
印刷	ドキュメントの印刷、ページ数等を記録します。
Web アップロード	InternetExplorer を使用したファイルのアップロード（http、https）を記録します。
ネットワーク通信量 （サーバー版のみ）	ネットワークの通信量を監視し、通信量が設定値を超えた時のログを記録します。
フォルダ （サーバー版のみ）	指定したフォルダ内のファイル操作（「新規作成」、「削除」、「更新」、「名前の変更」）を記録します。
USB HardLocker ※2	『USB HardLocker 5』の動作に関する以下の内容を記録します。 「鍵の作成／削除」、「秘密領域の有効／停止」、「ストレージ追加禁止／追加禁止の解除」、「コンピューターのロック」、「コンピューターのロック／ロックの解除」、「ネットワークロック／ロックの解除」

※1　Modern UI 版 IE には対応していません。
※2　ログ取得機能一覧には表示されません。詳細は(P88)参照

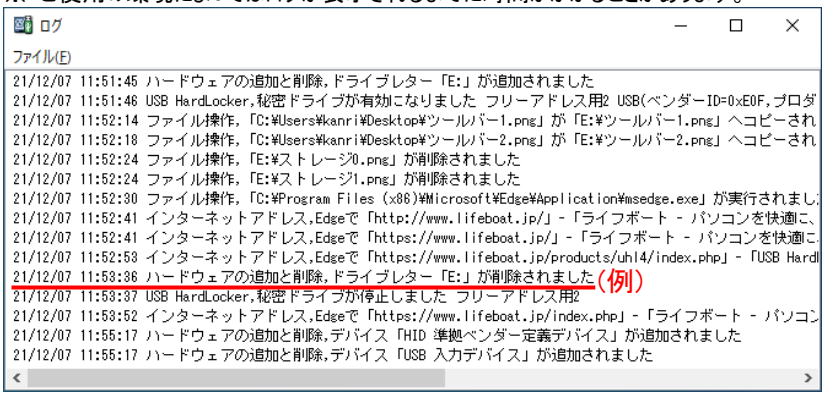
＜追加、削除、プロパティ＞

追加	ログ取得機能 DLL を追加したい場合にクリックします。ログの種類がリストに追加されます。 ※ 通常は使用しませんが、バックアップのリストア時に必要となる場合があります。詳細は（P93）参照 
削除	ログの種類をリストから削除したい場合にこのボタンをクリックします。
プロパティ	このボタンを押すと、選択したログの種類の情報が表示されます。

第3節　　ログの参照と保存

ログの形式はメッセージ形式（USB HardLocker独自の暗号化形式）または、CSVの2種類から選択できます（初期設定はメッセージ形式です）。CSV形式については、「第5節 CSV形式のログ」をご参照ください。

＜ログの参照＞
「ユーティリティ」から「ログ」をクリックすると、リアルタイムにログを参照することができます。
（「ログ」を閉じてもログの収集は継続されます。）
※ ご使用の環境によってはログが表示されるまでに時間がかかることがあります。



＜ログの表示例＞

21/12/07	11:53:36	ハードウェアの追加と削除	ドライブレター「E:」が削除されました
①日付	②時刻	③種類	④詳細

①「日付」 イベントの発生年月日を記録
②「時刻」 イベントの発生時刻を記録
③「種類」 「ログ設定」の「ログ取得機能」の項目（「ログオンとログオフ」、「ハードウェアの追加と削除」、「ファイルアクセス」、「インターネットアドレス」、「キーボード」、「ウィンドウ」、「プロセス」、「ファイル操作」、「USB HardLocker」）のいずれかが表示されます（ログ取得機能DLLを追加した場合は追加したものも表示対象となります）。
④「詳細」 イベントの詳細を記録

＜ログファイルについて＞
初期設定時は以下のパスに保存されます（C: がシステムドライブの場合）。

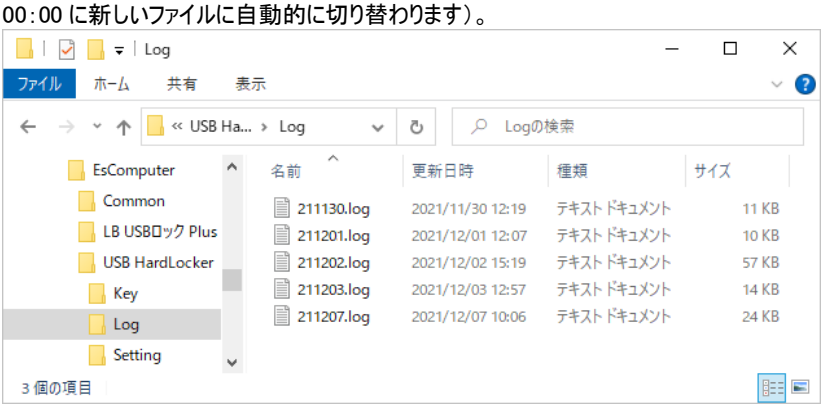
C:¥ProgramData¥Escomputer¥USB HardLocker¥Log

メッセージ形式のログは暗号化されており、ログを見るためには、ユーティリティから「ログ」を開く必要があります。他の PC で参照する場合はエクスポート(次節参照)する必要があります。
※ CSV形式の場合、暗号化の有無を指定できます。

メッセージ形式のログファイル名は初期設定で以下のようになります。
ログファイルの命名規則については(P56)もご参照ください。
例： 211130.log

211130	.log
日付(YYMMDD)	ファイル拡張子

初期設定時は 1 日に 1 ファイルのログが作成されます（コンピューターへログオン中は 00:00 に新しいファイルに自動的に切り替わります）。

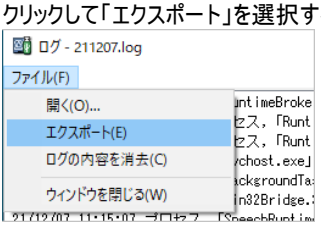


＜ログの保存と参照に関する注意事項＞
◎ ネットワーク共有フォルダーをログの保存先に指定することができますが、ネットワーク接続が切断されると、切断前と切断中のログが記録されないことがあります(ネットワークロックの動作中も同様です)。
◎ メッセージ形式でログを保存した場合、ログを生成したコンピューター以外からログの参照をすることはできません。
◎ 1 日あたりのログファイルのサイズは、記録する項目の設定内容やコンピューターの使用状況により大きく異なります。
◎ 必要に応じて以下のことを調整すると、ログのサイズを抑えることができます。
・プロセスやファイルのフルパス表示を選択しない。
・OS 関連のプロセスの動作やファイルアクセスを除外する。
・ウイルス対策ソフトの関連のプロセスやファイルアクセスを除外する。

第4節　ログのエクスポート(メッセージ形式)

メッセージ形式のログは暗号化されているため、「ログ」ボタン以外から開くことはできません。他のコンピューターからログを開く必要がある場合は、テキスト形式のファイルにエクスポートする必要があります。

＜ログのエクスポート方法＞
「ユーティリティ」から「ログ」を選択してログを表示した状態からメニューバーの「ファイル」をクリックして「エクスポート」を選択するとファイルの保存先を指定できます。



エクスポートしたログは
テキスト形式で保存されます。

ログの内容を消去
現在記録中のログを削除して、クリックした時点からの新しいログを生成します。
※　アクティブなログのみ削除されます。例えば、1日単位でログを再作成している場合、前日以前のログは削除されません。

第5節　CSV 形式のログ

ログの保存形式で CSV 形式を選択した場合、メッセージ形式より詳細な内容が記録されます。

	A	B	C	D	E	F	G	H	I	J	K
1	コンピュータ名	IPアドレス	ログイン名	年月日	時刻	ログ種類	ログ種類詳	タイトル	パス1	パス2	URL
2	DESKTOP-KQK5	192.168.0.33	kanri	2021/12/7	11:29:07	ファイル操作	コピー		C:¥Users¥kanri¥Desktop¥ドラ	E:¥ドライブ1.png	
3	DESKTOP-KQK5	192.168.0.33	kanri	2021/12/7	11:29:07	ファイル操作	コピー		C:¥Users¥kanri¥Desktop¥ス	E:¥ストレージ1.png	
4	DESKTOP-KQK5	192.168.0.33	kanri	2021/12/7	11:29:08	ウィンドウ	切り替え	ローカル ディスク (E:)			
5	DESKTOP-KQK5	192.168.0.33	kanri	2021/12/7	11:29:12	ファイル操作	コピー		C:¥Users¥kanri¥Desktop¥管理	E:¥管理者のみのポタ	
6	DESKTOP-KQK5	192.168.0.33	kanri	2021/12/7	11:29:12	ファイル操作	コピー		C:¥Users¥kanri¥Desktop¥ドラ	E:¥ドライブ管理者の	

上図は Excel を使用してファイルを開いています。

※「ツールバー」-「ログ」から起動するモニター画面の内容は、メッセージ形式、CSV形式どちらの場合も同じです。

※ CSV 形式の場合、暗号化オプション（P66）をチェックして暗号化を選択しておくと、不正な閲覧や改ざんを防ぐことができます。

例：

コンピュータ名,IPアドレス,ログイン名,鍵の名前,鍵の種類,VID,PID,SerialNo,年月日,時刻,ログ種類,ログ種類詳細,タイトル,パス1,パス2,URL,プリンタ名,プリンタIPアドレス,総ページ数,パラメーター,エラー値

PC520U,192.168.0.20,kanri,2012/2/7,8:40:45,ファイルアクセス

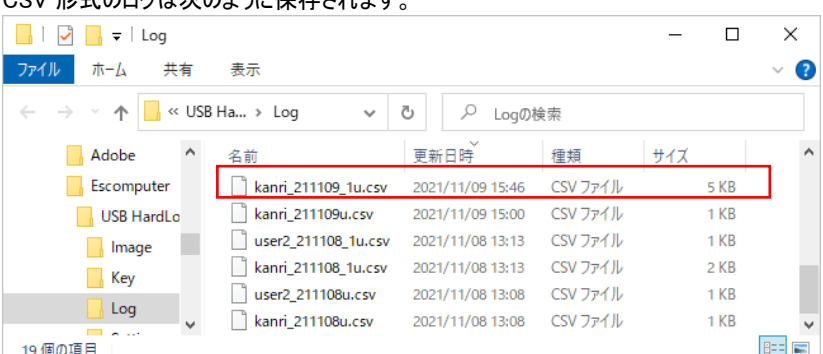
,,,SearchProtocolHost.exe,C:¥Users¥kanri¥Documents¥desktop.ini,,,,,,

項目	説明
コンピュータ名　※	イベントが発生したコンピューター名
IP アドレス　※	イベントが発生したコンピューターの IP アドレス
ログイン名　※	ログイン中のユーザー名
鍵の名前	ロック、ロックの解除に使用した鍵の名前
鍵の種類	ロック、ロックの解除に使用した鍵の種類（管理者/利用者）
VID	ロック、ロックの解除に使用した鍵のベンダーID
PID	ロック、ロックの解除に使用した鍵のプロダクト ID
SerialNo	ロック、ロックの解除に使用した鍵のシリアルナンバー
年月日	イベントが発生した日時
時刻	イベントが発生した時刻
ログ種類	ログの種類（ログオンとログオフ、ハードウェアの追加と削除、ファイルアクセス、プロセス等）

項目	説明
ログ種類詳細	ログの種類の詳細（ログオンとログオフの場合； ログオン、スタンバイ、ロック、ログオフ等）
タイトル	ウィンドウログのウィンドウタイトル
パス 1	ファイルの移動元、コピー時のコピー元、ファイルにアクセスしたプロセス
パス 2	ファイル移動先、コピー時のコピー先、プロセスがアクセスしたファイル
URL	インターネットアドレス、Web アップロードの URL
プリンタ名	印刷に使用されたプリンタ名
プリンタIPアドレス	ネットワークプリンタの IP アドレス
総ページ数	印刷されたドキュメントのページ数
パラメーター	実行ログ（ファイル操作）の実行パラメーター
エラー値	実行ログ（ファイル操作）のエラー

※ コンピューター名、IP アドレス、ログイン名は CSV 形式の場合のみ記録可能です。

CSV 形式のログは次のように保存されます。



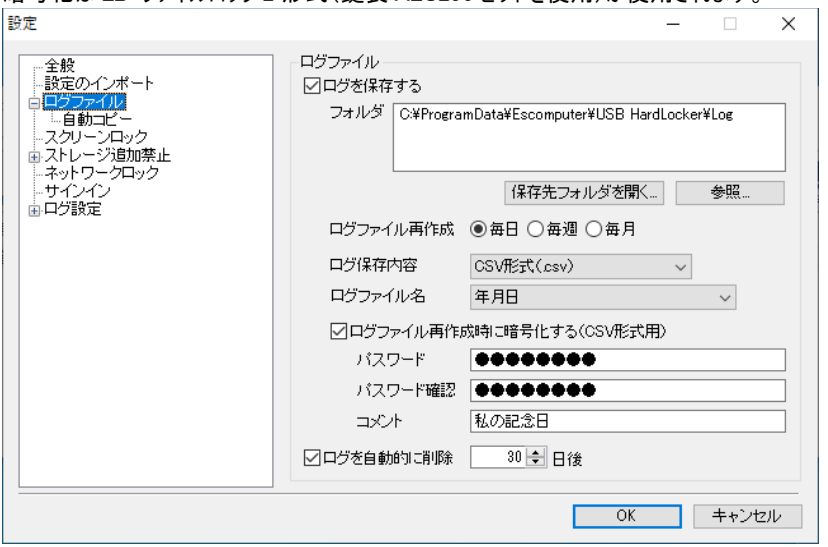
例： kanri_211109_1u.csv

kanri	211109	1u	.csv
ユーザー名	日付(YYMMDD)	UTF-8 形式	ファイル拡張子

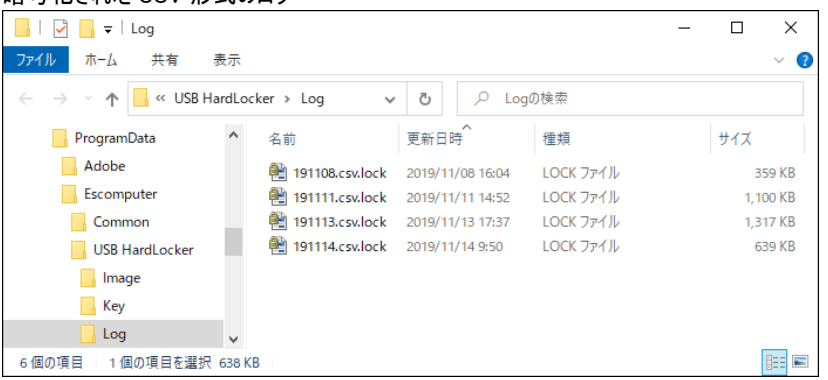
マシン名＋ユーザー名＋年月日をファイル名として指定した場合の例です。UTF-8 形式を選択した場合、日付の後に「_u」の文字が挿入されます。ファイル名については(P56)もご覧ください。

第6節　CSV 形式のログの暗号化

CSV 形式により保存されたログは、記録終了後、自動的に暗号化することができます。
暗号化は LB ファイルロック 2 形式（鍵長 AES256 ビットを使用）が使用されます。



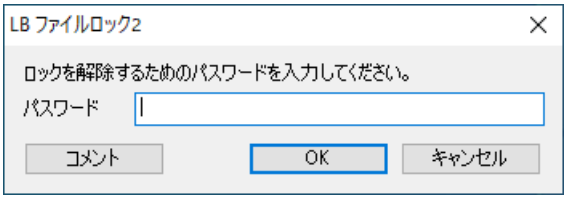
暗号化された CSV 形式のログ



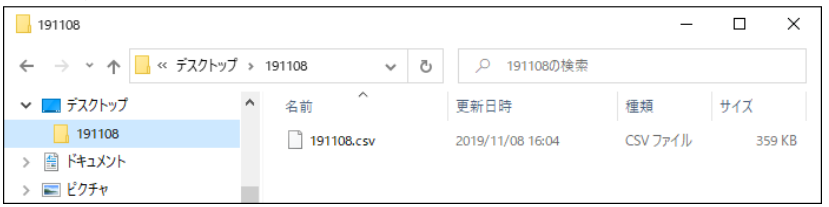
＜暗号化されたログファイルの復号化＞
暗号化されたログの復号化は 2 通りの方法があります。

方法 A.　『USB HardLocker 5』がインストールされた環境

暗号化されたファイルをダブルクリックすると、パスワードを入力するためのウィンドウが表示されます。

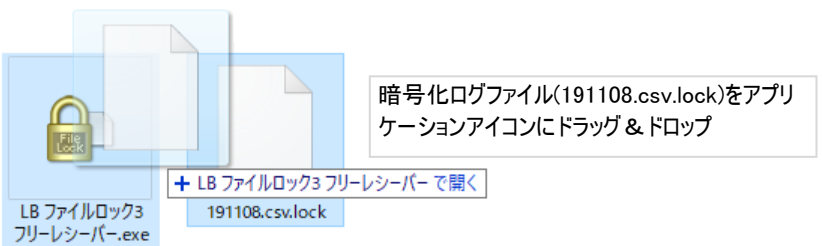


パスワードを入力して「OK」をクリックすると、デスクトップにフォルダー付きの状態で復号化されます。



方法 B.　『USB HardLocker 5』がインストールされていない環境

LB ファイルロックシリーズ(『LB ファイルロック2』以降)を使用して復号化します。
以下はLB ファイルロック3 フリーレシーバーを使用した例



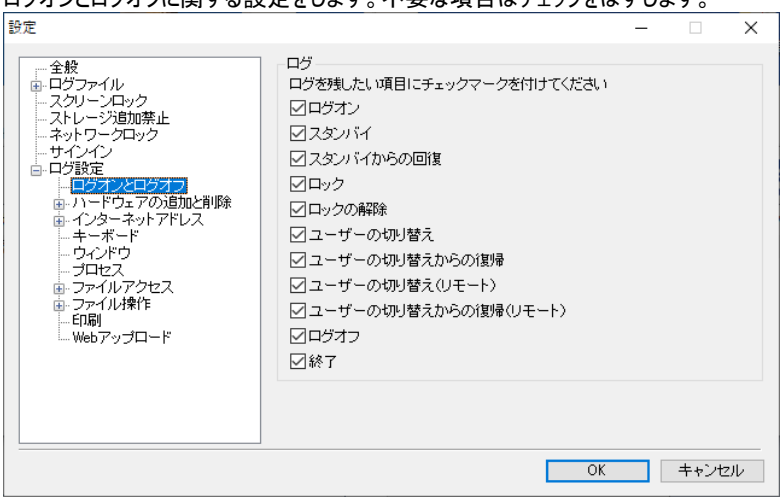
第7節　記録内容の詳細設定

本節は、ログに記録できる各項目の詳細な設定内容について説明しています。設定内容は項目ごとに異なります。

※ ファイルアクセスやファイル操作は、フィルターを使用して不必要なログを除外すると、ログのサイズを抑えることができます。

1. ログオンとログオフ

ログオンとログオフに関する設定をします。不要な項目はチェックをはずします。



＜項目の説明＞

ログオン	コンピューターへのログオンを記録します。
スタンバイ	スタンバイモードへ切り替えを記録します。
スタンバイからの回復	スタンバイモードからの復帰を記録します。
ロック	コンピューターのロックを記録します。
ロックの解除	コンピューターのロックの解除を記録します。
ユーザーの切り替え	ユーザーの切り替えを記録します。
ユーザーの切り替えからの復帰	切り替えたユーザーから元のユーザーへの復帰を記録します。

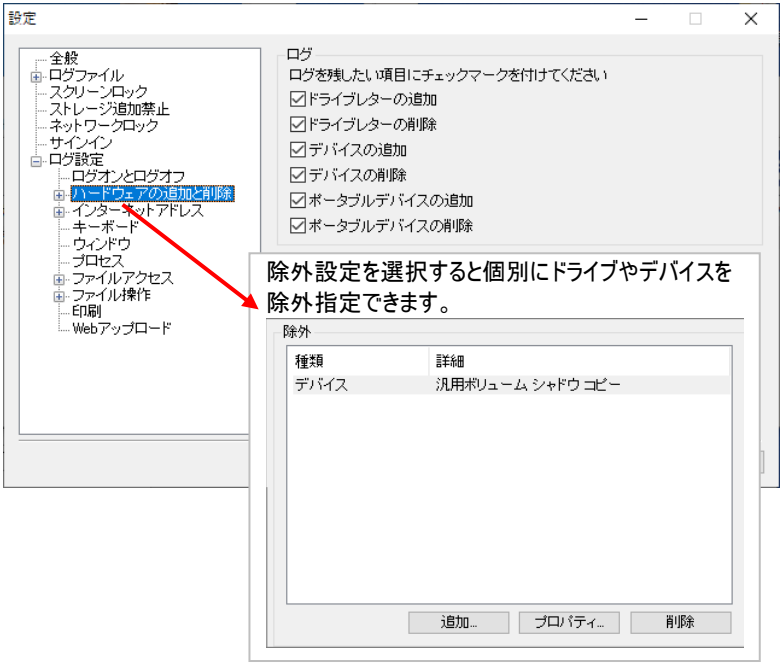
ユーザーの切り替え（リモート）	ユーザーの切り替え（リモートコンピューターからのログオン）を記録します。
ユーザーの切り替えからの復帰（リモート）	切り替えたユーザー（リモートコンピューターからのログオン）から元のユーザーへの復帰を記録します。
ログオフ	コンピューターのログオフを記録します。
終了	コンピューターの終了を記録します。

2. ハードウェアの追加と削除

ドライブの追加／削除や、デバイス(外付けディスクや各種機器)の追加／削除」に関する設定をします。

ログオフ時のハードウェアの状態を記録していますので、電源切断時、スタンバイ時に追加、削除されたハードウェアを検出することができます。

追加、削除されたハードウェアは、次回ログオン時にログに記録されます。



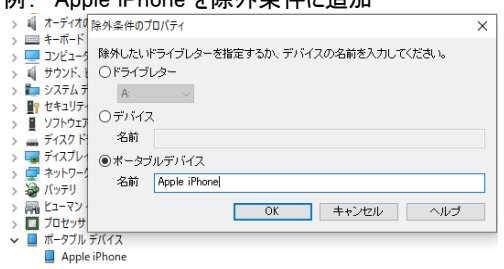
＜項目の説明＞

ドライブレターの追加	ドライブの追加（USB フラッシュメモリーの装着等）を記録します。
ドライブレターの削除	ドライブの削除（USB フラッシュメモリーの取り外し等）を記録します。
デバイスの追加	デバイスの追加を記録します。
デバイスの削除	デバイスの削除を記録します。
ポータブルデバイスの追加	ポータブルデバイスの追加を記録します。
ポータブルデバイスの削除	ポータブルデバイスの削除を記録します。

＜除外設定＞

ログから除外したいハードウェアは「除外」から「追加」をクリックして指定することができます。

例： Apple iPhone を除外条件に追加



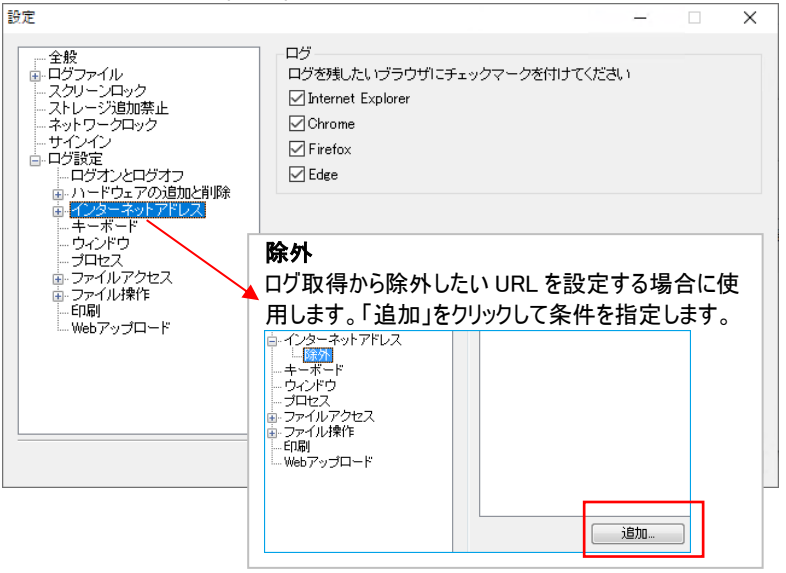
デバイス名やポータブルデバイスの名前は、タスクマネージャーで表示される名称と完全に一致する必要があります。

＜除外条件のプロパティ＞

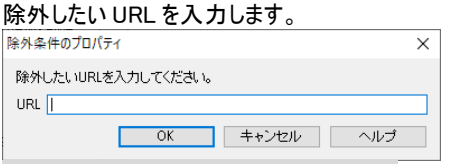
ドライブレター	プルダウンリストから除外リストに追加するドライブレターを選択します。指定したドライブレターは、ログに残らなくなります。
デバイス	指定したデバイスは、ログに残らなくなります。
ポータブルデバイス	指定したポータブルデバイスは、ログに残らなくなります。

3. インターネットアドレス

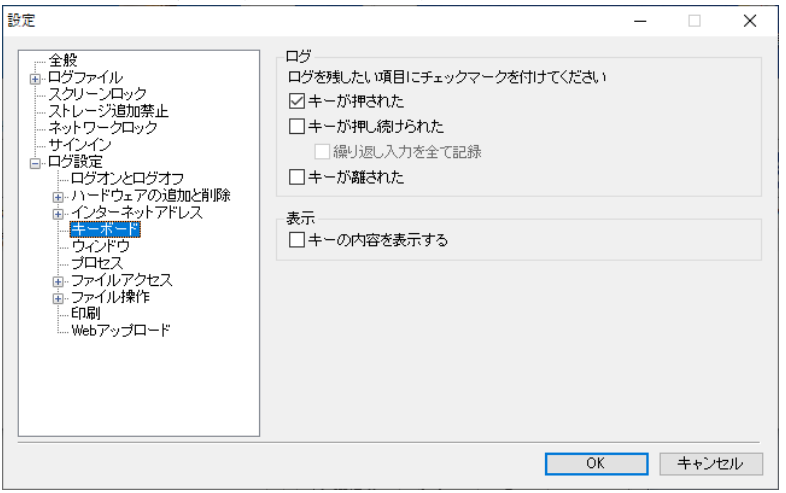
Microsoft Edge、Internet Explorer、Google Chrome、Mozilla Firefox を使用してアクセスしたURL(http、https)のログに関する設定をします。



＜除外条件の設定＞

除外条件のプロパティ	除外したい URL を入力します。  http://www.lifeboat.jp/　を入力した場合 http://www.lifeboat.jp/以下の全ての URL へのアクセスが除外されます。 http://www.lifeboat.jp/index.html　を入力した場合 指定した URL のみアクセスが除外されます。

4. キーボード（初期設定はチェックOFF）
キーボード入力のログに関する設定をします。 チェック後の初期設定は、「キーが押された」のみチェックされます。他のチェックを入れることで「キーが押し続けられた」、「繰り返し入力を全て記録」、「キーが離された」操作も記録することができます。
ログに残したくない項目は、チェックを外します。

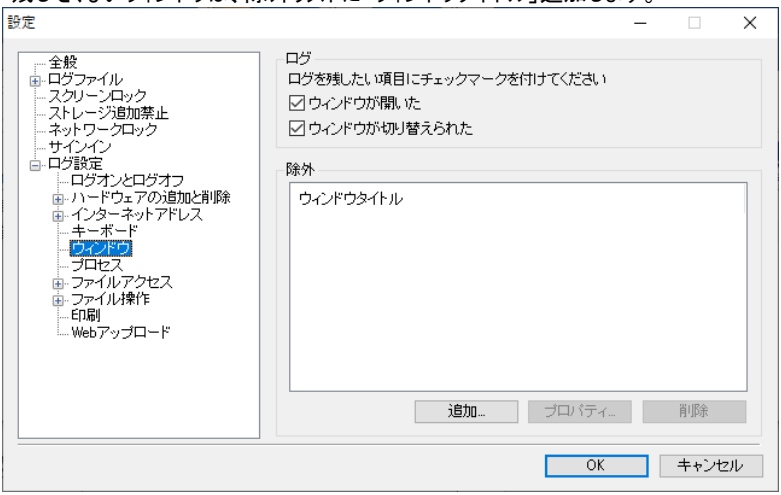


＜設定項目＞

キーが押された	キー押下を記録します（例： キーが離されました）。
キーが押し続けられた	キーが押し続けられた状態を記録します。 （例： キーが押し続けられています。）
キーが離された	キーを離した操作を記録します。（例： キーが離されました）。
キーの内容を表示する	チェックすると、キーの内容を記録します（例： 「A」が押されました）。 チェックを外すと内容は記録されません （例： キーが押されました）。

5. ウィンドウ

「ウィンドウのオープン」、「ウィンドウの切り替え」のログに関する設定をします。ログに残したくないウィンドウは、除外リストに「ウィンドウタイトル」追加します。

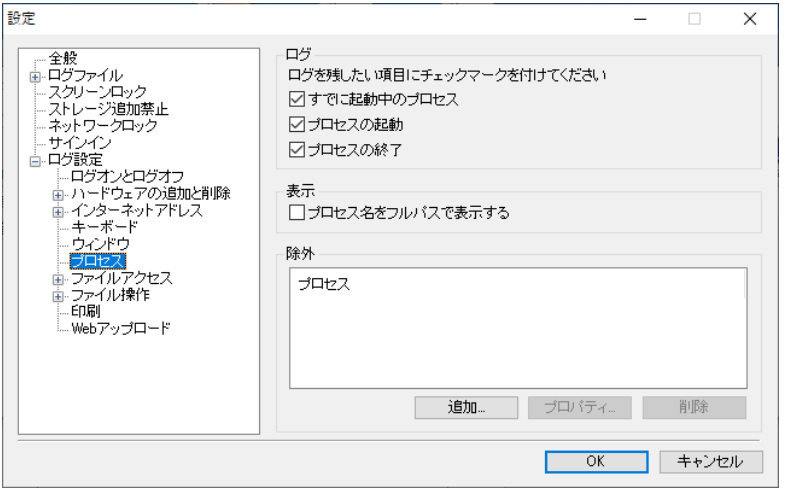


＜設定項目＞

ウィンドウが開いた	ウィンドウの開く動作を記録します。
ウィンドウが切り替えられた	アクティブなウィンドウを切り替えた時、ログに記録します。
追加	ログ取得から除外したいウィンドウタイトルを設定する場合には「追加」をクリックして設定します。
プロパティ	除外リストのウィンドウタイトルの情報を表示します。
削除	除外リストの設定を削除します。

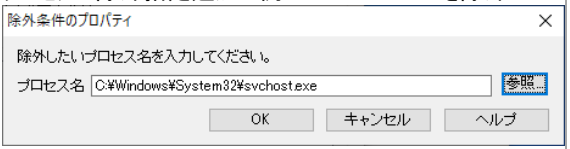
6. プロセス

プロセスのログに関する設定をします。「すでに起動中のプロセス」、「プロセスの起動」、「プロセスの終了」のログを記録することができます。



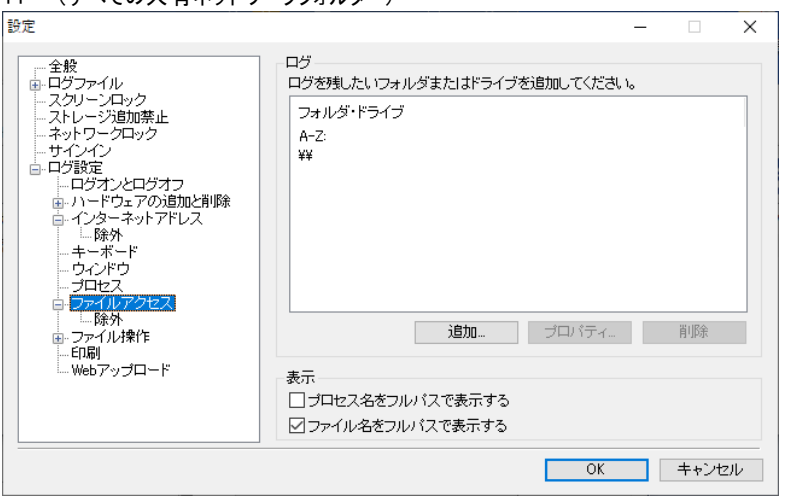
＜設定項目＞

すでに起動中のプロセス	Windows のログオン時、すでに起動しているプロセスを記録します。
プロセスの起動	プロセスの起動を記録します。
プロセスの終了	プロセスの終了を記録します。
プロセス名をフルパスで表示する	チェックするとフルパスのファイル名を、チェックを外すとファイル名のみを記録します。ログに残したくないプロセスは、除外リストに追加します。
追加	ログ取得から除外したいプロセスを設定する場合には「追加」をクリックして設定します。
プロパティ	除外リストのプロセスの情報を表示します。

削除	除外リストの設定を削除します。 プロセスの除外指定追加の例：　svchost.exe　を除外  ※ ウイルス対策ソフトの監視プロセス等、ユーザーが直接操作しないファイルに対してアクセスするプロセスは、ファイルアクセスが発生する都度、ログ記録の対象となり、ログサイズが肥大化する原因となります。ファイルアクセスのログ記録対象でドライブ全体を指定しているような場合、このようなプロセスは除外指定することをお勧めします。

7. ファイルアクセス（初期設定はチェックOFF）
ログを残したいフォルダーまたはドライブに関する設定をします。指定したフォルダー・ドライブ以下に、除外したいフォルダー・ファイルがある場合は「除外」を選択して設定します。

＜初期設定で指定されているフォルダー＞
A-Z：（A～Zまですべてのドライブ）
¥¥　（すべての共有ネットワークフォルダー）

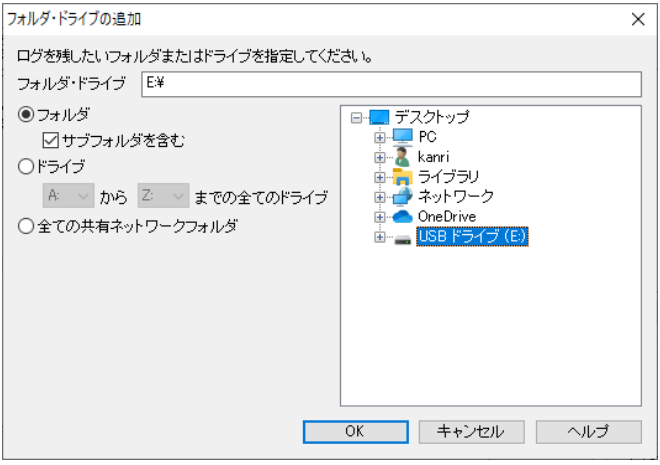


＜設定項目の説明＞

追加	ログを残したいフォルダーまたはドライブを設定する場合にクリックします。クリックすると「フォルダー・ドライブの追加」ウィンドウが表示されます。
プロパティ	設定済みのフォルダー・ドライブを選択してからクリックします。設定した内容の確認、変更をする場合に使用します。
削除	リストの設定を削除します。
プロセス名をフルパスで表示する	チェックを付けるとフルパスのプロセス名を、チェックを外すとプロセス名のみを記録します。
ファイル名をフルパスで表示する	チェックを付けるとフルパスのファイル名を、チェックを外すとファイル名のみを記録します。

＜フォルダー・ドライブの追加＞

ログを取得するファイルまたはドライブを指定します。



＜設定項目＞

フォルダー・ドライブ	右のツリー表示（「フォルダー」）、または左のチェック（「ドライブ」、「全ての共有ネットワークフォルダー」）で選択したフォルダー・ドライブが表示されます。
フォルダー	ログを残すフォルダーを右のツリーから指定します。
ドライブ	ログを残すドライブをプルダウンで選択して指定します。
全ての共有ネットワークフォルダー	このコンピューターから、共有ネットワークフォルダーへのアクセスログを残します。

※ フォルダー・ドライブの追加指定は直接パスを入力することも可能です。直接入力する場合はパス無し、相対パス、ファイル名等の細かい指定ができ、またファイル名には、一括して指定するためのワイルドカードを使用できます。ワイルドカードには、1文字の置き換えに使用する「?」と、複数文字の置き換えに使用する「*」があります。フォルダー名には、パス無し・フルパス・相対パスの指定をすることができます（フォルダー名にワイルドカードを使用することはできません）。

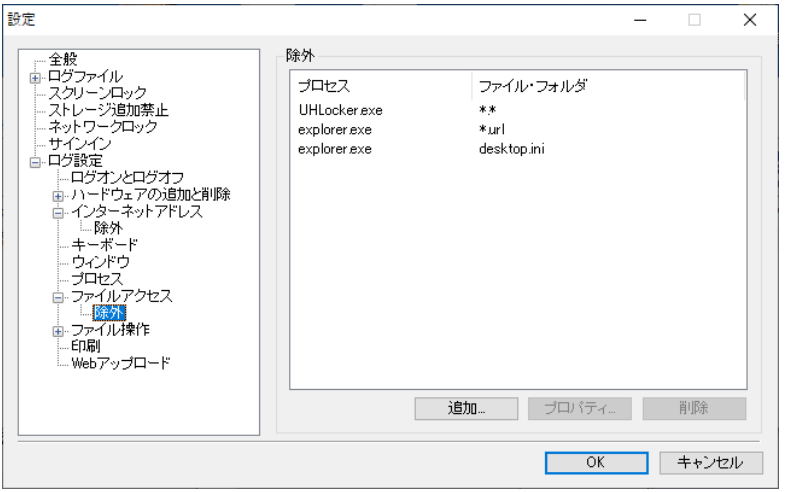
◇パス無しの例
sample.txt － ファイル名がsample.txtの全てのファイル
*.txt － 拡張子txtを持つ全てのファイル
a*.* － a で始まる全てのファイル
sample? － sample? の全てのファイル。 ?は任意の1文字

◇フルパスの例
C:¥dir¥test.exe － 指定されたファイルのみ
C:¥dir¥*.exe － C:¥dir¥フォルダー内で拡張子exeを持つ全てのファイル
C:¥dir¥*.* － C:¥dir¥フォルダー内の全てのファイル
C:¥dir¥ － すべてのサブフォルダーを含めた、C:¥dir¥内の全てのファイル

◇相対パスの例
dir¥test.exe － dir¥フォルダー内のtest.exe
dir¥*.exe － dir¥フォルダー内で拡張子exeを持つ全てのファイル
dir¥*.* － dir¥フォルダー内の全てのファイル
dir¥ － すべてのサブフォルダーを含めた、dir¥フォルダー内の全てのファイル

◇その他特別な文字列
D-Z: － Dドライブから、Zドライブの全てのドライブ
¥¥ － 全ての共有ネットワークフォルダー

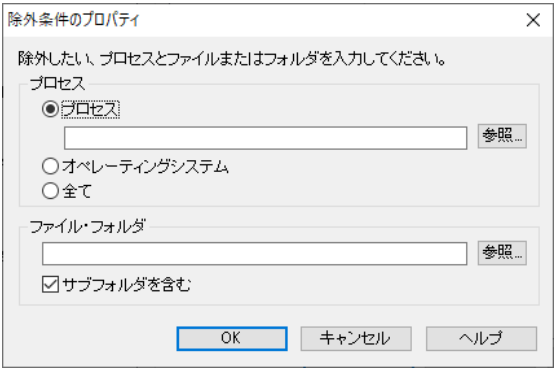
＜「除外」（ファイルアクセス）＞
ログに残したくないファイルアクセスは除外リストに追加します。



＜除外の説明＞

追加	ログ取得から除外したいファイルアクセスを設定する場合には「追加」をクリックして設定します。 ※　初期設定で除外されているプロセス（explorer.exe）を除外リストから削除しないようにしてください。削除するとログのサイズが非常に大きなものとなります。
プロパティ	除外リストのファイルアクセスの情報を表示します。
削除	除外リストの設定を削除します。

＜除外条件の追加の設定＞

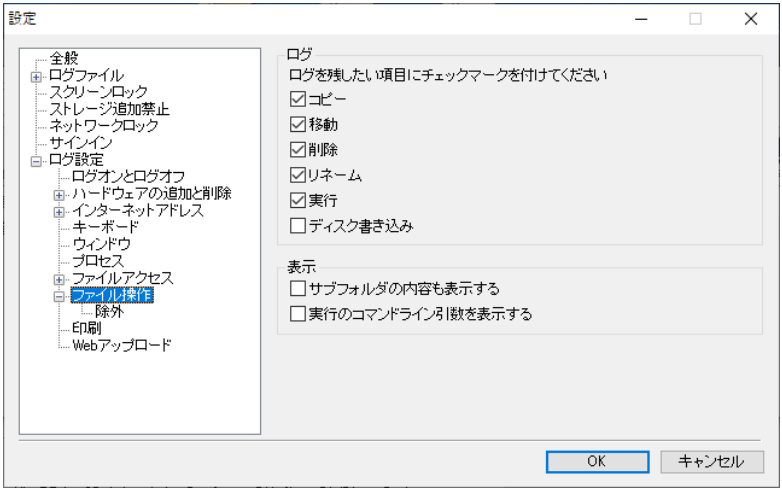


＜除外条件追加の説明＞

プロセス	参照をクリックして除外するプログラムのファイル名を追加します。
オペレーティングシステム	プロセスではなく、オペレーティングシステムによるファイルアクセスを指定します。「オペレーティングシステム」を選択する場合、同時に「ファイル・フォルダー」を指定する必要があります。
全て	全てのプロセスとオペレーティングシステムによるファイルアクセスを指定します。
ファイル・フォルダー	アクセスされるファイル名またはフォルダー名を入力します。 ※ ファイル名には、一括して指定するためのワイルドカードを使うことができます。ワイルドカードには、1文字の置き換えに使用する「?」と、複数文字の置き換えに使用する「*」があります。フォルダー名には、パス無し・フルパス・相対パスの指定をすることができます（フォルダー名にワイルドカードを使用することはできません）。

8. ファイル操作

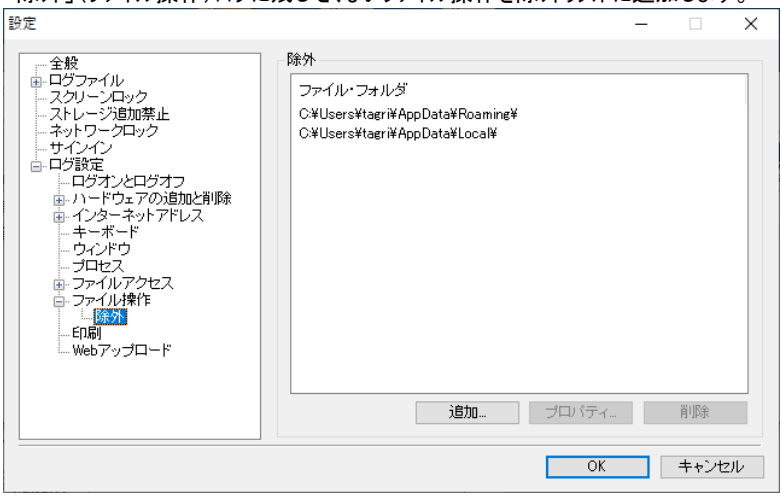
ファイル操作のログに関する設定をします。「コピー」、「移動」、「削除」、「リネーム」、「実行」のログを記録することができます。



＜設定項目＞

コピー	ファイルのコピーを記録します。
移動	ファイルの移動を記録します。
削除	ファイルの削除を記録します。
リネーム	ファイルのリネームを記録します。
実行	ファイルの実行を記録します。
ディスク書き込み	ディスク書き込み準備フォルダーへの、ファイル追加を記録します。
サブフォルダの内容も表示する	フォルダーに含まれるすべてのサブフォルダーのログが記録されます。チェックを外すと、フォルダーのログのみが記録されます。
実行のコマンドライン引数を表示する	チェックすると、実行ログの実行パラメーターを記録します。

「除外」(ファイル操作)ログに残したくないファイル操作を除外リストに追加します。

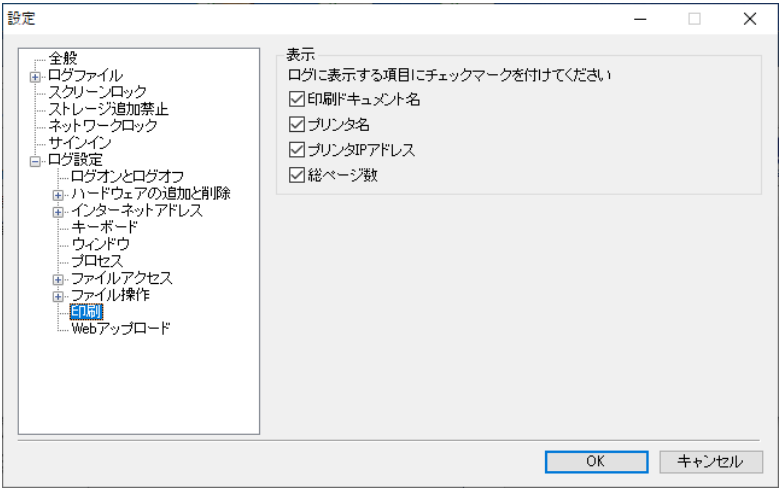


＜除外の設定項目＞

追加	ログ取得から除外したいファイル操作を設定する場合には「追加」をクリックして設定します。 ※ 初期設定で除外指定されているフォルダーを除外から削除しないようにしてください。削除するとログのサイズが非常に大きなものとなります。
プロパティ	除外指定したファイル・フォルダーの情報を表示します。
削除	選択した除外リストの設定を削除します。

9. 印刷

印刷のログに関する設定をします。「印刷ドキュメント名」、「プリンタ名」、「プリンタIPアドレス」、「総ページ数」のログを記録することができます。



＜設定項目＞

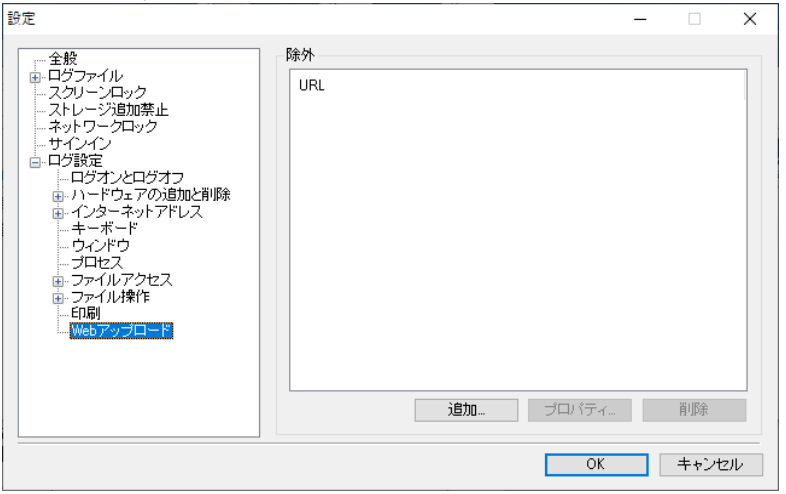
印刷ドキュメント名	印刷されたドキュメント名を記録します。
プリンタ名	印刷に使用されたプリンタ名を記録します。
プリンタ IP アドレス	ネットワークプリンタの IP アドレスを記録します。
総ページ数	印刷ドキュメントのページ数を記録します。

※ 共有プリンタ（他のコンピューターに接続したプリンタ）を使用した印刷には対応しておりません。

10. Webアップロード

Web上へのファイルアップロードに関するログを記録することができます。

※ InternetExplorerを使用してのアップロードのみに対応します。

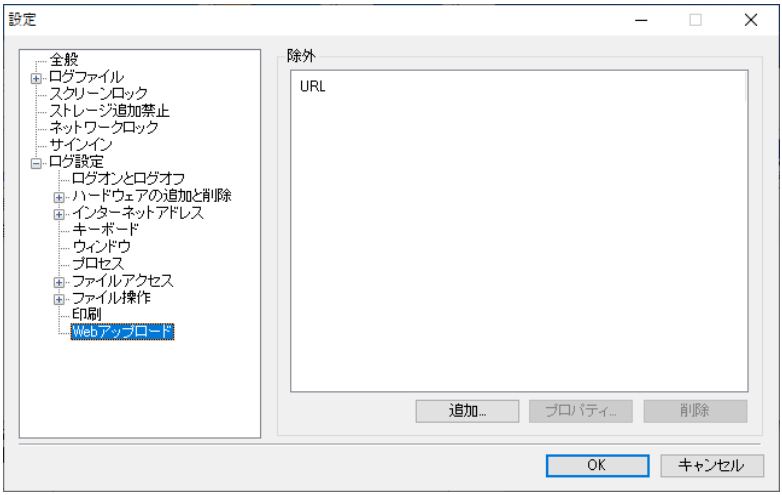


＜設定項目＞

追加	ログ取得から除外したい URL を設定する場合には「追加」をクリックして URL を追加します。
プロパティ	除外リストの URL 情報を表示します。
削除	プロセスの終了を記録します。

11. ネットワーク通信量（サーバー版のみ）

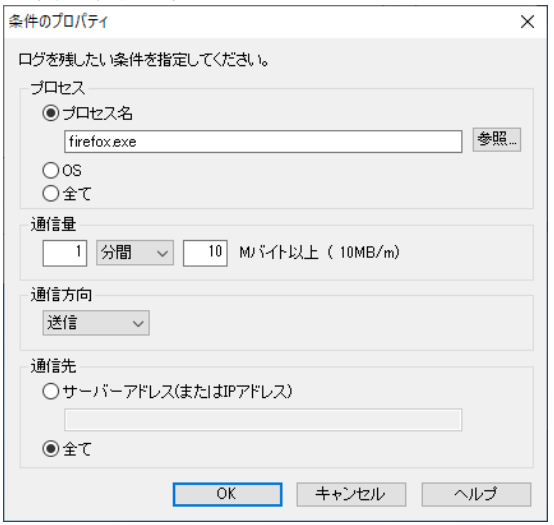
ネットワーク通信量が設定値を超えるとログに記録することができます。



＜設定項目＞

プロセス	設定したプロセスを表示します。
通信量	設定した閾値を表示します。
方向	送信／受信の表示がされます。
通信先	通信先のアドレスが表示されます。
通知	通知設定をした項目に〇印が表示されます。
添付	スクリーンショットの添付設定をした項目に〇印が表示されます。

＜条件の設定内容＞



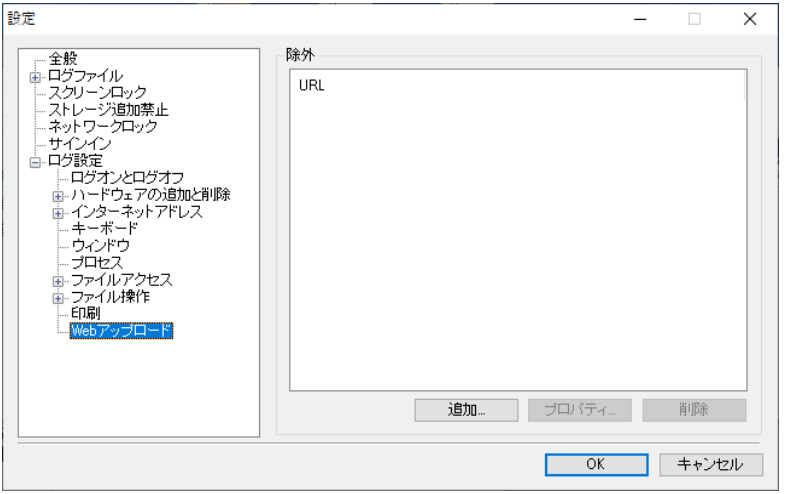
＜設定項目＞

プロセス名	監視対象のプロセスを入力します。特定のアプリを監視する場合は、プロセス名を個別に指定、システム全体を監視するような場合は「全て」を選択します。
通信量	閾値を入力します。ここで入力した通信量を超えた場合、ログに記録されます。
通信方向	送信／受信の区別を設定します。
通信先	通信先の IP アドレスまたはサーバアドレスを設定します。
通知	通知が必要な場合にチェックします。

上記の設定では以下のようなログが記録されます。

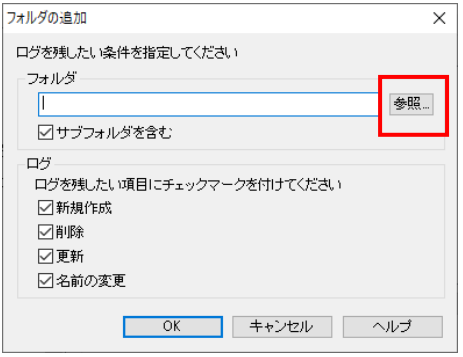
```
2023/07/24 13:35:35  ファイルアクセス      「CompatTelRunner.exe」が「C:¥Users¥kanri¥Desktop¥alog2_t
2023/07/24 13:36:03  ネットワーク通信量    firefox.exeが1分間に1MB(162Kbps)以上の送受信を行いました
2023/07/24 13:37:23  ファイルアクセス      「explorer.exe」が「C:¥Users¥kanri¥Desktop¥alog2_temp¥alo
2023/07/24 13:37:23  ファイルアクセス      「explorer.exe」が「C:¥Users¥kanri¥Desktop¥alog2_temp¥ス
```

12. フォルダー（サーバー版のみ）
指定したフォルダー内のファイル操作(「新規作成」「削除」「更新」「名前の変更」)を記録します。



＜設定項目＞

追加	監視するフォルダーをリストへ追加します。
プロパティ	追加したフォルダーを選択して設定内容を確認します。
削除	選択したフォルダーをリストから削除します。

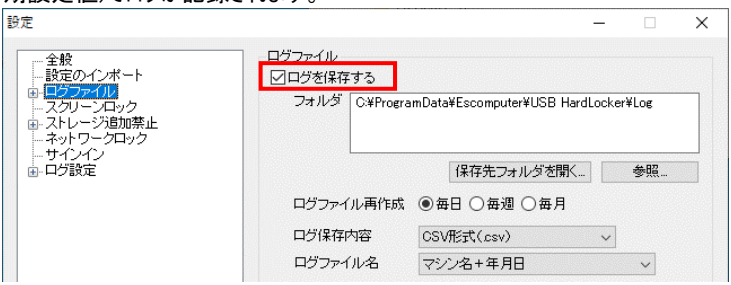


参照をクリックするとエクスプローラーが起動します。監視するフォルダーを選択してください。

13. USB HardLocker(※)

『USB HardLocker 5』の動作(鍵の作成、スクリーンロック等)についてログを記録します。

※ この項目は他と異なり「ログ設定」に設定画面が存在しません。ユーティリティの「設定」-「全般」-「ログファイル」で「ログを保存する」がチェックされた状態(初期設定値)でログが記録されます。



＜記録される項目＞

鍵の作成　/削除	鍵の作成と削除を記録します。
コンピューターのロック /ロックの解除	スクリーンロックとロックの解除を記録します。
ネットワークロック /ロックの解除	ネットワークロックの動作とその解除を記録します。
秘密領域の有効 /停止	秘密領域の有効化と停止を記録します。
ストレージ追加禁止 /追加禁止の解除	許可リスト以外のストレージが接続されたとき、とりはずされた動作を記録します。
USB 機器(ストレージ) 許可	権限のある鍵が装着された環境で、新しい USB 機器が装着された動作を記録します(次節参照)。
USB 機器(ストレージ) 使用期間変更	USB 機器の使用期間変更を記録します(次節参照)。
USB HardLocker の 起動	USB HardLocker の起動時に記録されます(システム起動時とアプリの復帰時)。

ログの例(CSV形式のログをExcelで表示しています。)

	A	B	C	D	E	F	G	H	I	J	K	L
1	コンピュー	IPアドレス	ログイン名	鍵の名前	鍵の種類	VID	PID	SerialNo	年月日	時刻	ログ種類	ログ種類詳細
2	DESKTOP	192.168.239.130	kanri						2019/11/12	11:35:52	USB HardLocker	起動
3	DESKTOP	192.168.239.130	kanri						2019/11/12	11:35:52	USB HardLocker	スクリーンロック開始
4	DESKTOP	192.168.239.130	kanri	ユーザー2	USB	0x96E	0x201	B954DA40	2019/11/12	11:38:34	USB HardLocker	スクリーンロック解除
5	DESKTOP	192.168.239.130	kanri	ユーザー2	USB	0x96E	0x201	B954DA40	2019/11/12	11:38:34	USB HardLocker	秘密ドライブ有効
6	DESKTOP	192.168.239.130	kanri	ユーザー2					2019/11/12	11:39:42	USB HardLocker	秘密ドライブ停止
7	DESKTOP	192.168.239.130	kanri	ユーザー2	USB	0x96E	0x201	B954DA40	2019/11/12	11:39:42	USB HardLocker	秘密ドライブ有効
8	DESKTOP	192.168.239.130	kanri	管理者1	USB	0x96E	0x201	98CB16F8	2019/11/12	11:41:48	USB HardLocker	ストレージ追加禁止解除
9	DESKTOP	192.168.239.130	kanri						2019/11/12	12:01:22	USB HardLocker	起動
10	DESKTOP	192.168.239.130	kanri						2019/11/12	12:01:22	USB HardLocker	スクリーンロック開始
11	DESKTOP	192.168.239.130	kanri	管理者1	USB	0x96E	0x201	98CB16F8	2019/11/12	12:02:22	USB HardLocker	スクリーンロック解除

14. ストレージの利用許可に関するログ

『USB HardLocker 5』の動作ログ(P88参照)にUSB機器の使用許可、使用期間の設定に関する履歴が追加されました。サンプルログの①

サンプルログ:

下図はCSV形式にて記録されたログファイルをMS Excelを利用して開いています。また、表示スペース確保のため一部の内容をカットしています。

C	D	E		K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
ログイン名	鍵の名前	鍵の種類		ログ種類	ログ種類詳細	タイトル	パス1								VID2	PID2	SerialNo2	使用期間
kanri	admin1	USB	13:25:57	USB HardLocker	USB機器（ストレージ）許可	USB 大容量記憶装置									0x781	0x5170	0D91E8707162	無期限
kanri			13:25:59	ハードウェアの追加と削除	デバイスの追加	SanDisk Cruzer Glide3.0 USB Device												
kanri			13:25:59	ハードウェアの追加と削除	デバイスの追加	ボリューム												
kanri			13:25:59	ハードウェアの追加と削除	デバイスの追加	USB 大容量記憶装置									0x781	0x5170	0D91E8707162	A8B0
kanri			13:25:59	ハードウェアの追加と削除	ドライブレターの追加	E:												
kanri			13:26:02	ハードウェアの追加と削除	デバイスの追加	BACKUPS												
kanri			13:26:02	ハードウェアの追加と削除	ポータブルデバイスの追加	BACKUPS												
kanri			13:27:48	USB HardLocker	USB機器（ストレージ）使用期間変更	USB 大容量記憶装置									0x781	0x5170	0D91E8707162	30
kanri			13:28:20	USB HardLocker	USB機器（ストレージ）使用期間変更	USB 大容量記憶装置									0x5DC	0xC75C	4AA27E42A9A(	無期限
kanri			13:28:52	ログオンとログオフ	ログオフ	kanri												

①

②

新規にUSB機器を許可リストへ追加した鍵と鍵情報(VID、PID、Serial No)、追加されたUSB機器の情報(VID、PID、Serial No)、使用期間が表示されます。

鍵の名前	鍵の種類	VID	PID	SerialNo	年月日	時刻	ログ種類	ログ種類詳細
admin	USB	0x96E	0x201	B954DA403246	2022/7/20	13:25:57	USB Hard	USB機器（ストレージ）許可

使用許可を与えたユーザーの鍵情報

下段へ続く

タイトル	VID2	PID2	SerialNumber2	使用期間
USB 大容量記憶装置	0x781	0x5170	0D91E8707162A7B5	無期限

許可リストに追加されたUSB機器情報

ログの種類「ハードウェアの追加と削除」にUSB機器の接続時に機器の「シリアルナンバー(VID、PID、Serial Number)」が追加されます。サンプルログの②

＜記録されるタイミング＞

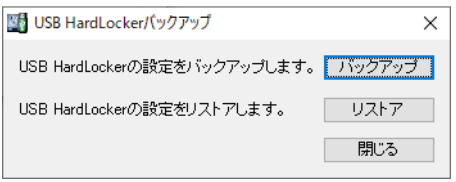
USB機器を接続して使用許可を設定した時は①② が記録されます。

設定完了後に許可済の機器が接続された時は ② が記録されます。

第5章　設定情報と秘密領域のバックアップ

第1節　バックアップツールについて

『USB HardLocker バックアップ』は『USB HardLocker 5』の設定情報をバックアップするためのツールです。



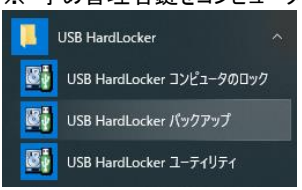
■主な機能
◎ 設定情報、秘密領域、ログのバックアップを取ることができます。
◎ バックアップした設定情報をリストアすることができます。

■注意事項
◎ 異なるバージョンのWindowsがインストールされた他のPC上で、バックアップをリストアすることもできますが、リストアできる内容が限られます。
リストア可能な内容:　鍵情報、秘密領域、ログ
※ 同じPC、OS環境でリストアする場合は、許可ストレージ、許可ドライブ、ログの設定もリストアされます。
◎ バックアップと復元は管理者権限で Windows にログオンしてから実行する必要があります。

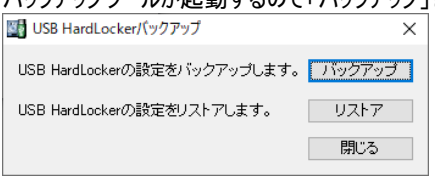
第2節　バックアップ

＜バックアップの手順＞

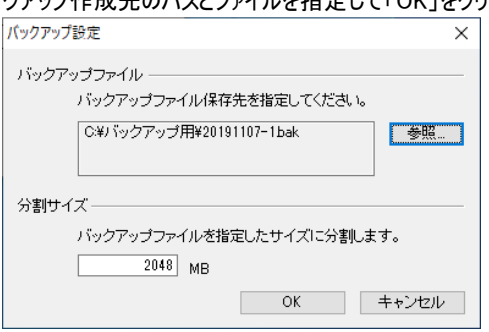
1. Windows の「スタート」から「USB HardLocker」-「USB HardLocker バックアップ」（Windows 8.1 は「スタート」または「すべてのアプリ」から「USB HardLocker バックアップ」）を選択します。
   ※ 予め管理者権限で Windows にログオンしておく必要があります。
   ※ 予め管理者鍵をコンピューターに接続しておく必要があります。



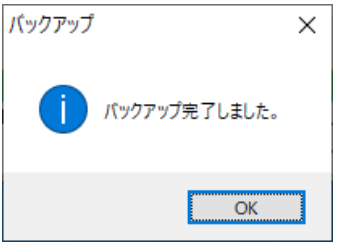
2. バックアップツールが起動するので「バックアップ」をクリックします。



3. バックアップの保存先となるパスとファイル名を指定します。「参照」をクリックしてバックアップ作成先のパスとファイルを指定して「OK」をクリックしてください。



4. バックアップが実行されます。完了すると「バックアップ完了しました」メッセージが表示されるので「OK」をクリックします。
※ バックアップの保存先に十分な空き容量が確保されていることをご確認ください。
※ バックアップの保存先となるファイルは指定されたサイズのアーカイブに分割されます（初期設定のサイズは 2GB）。バックアップ保存先のファイルフォーマットにより、分割サイズを 2GB 以上にするとバックアップできなくなる場合があります。

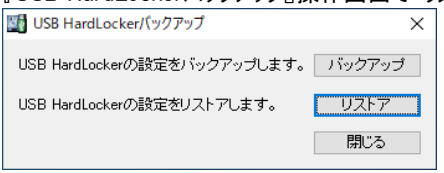


第3節　リストア

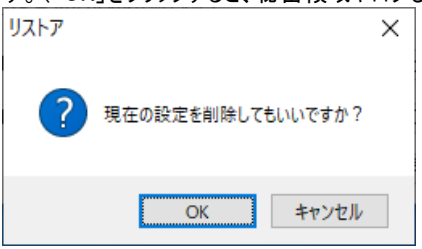
＜リストアの手順＞
『USB HardLocker 5』がインストール済みの環境に、バックアップファイルを用意します。
※ 予め管理者権限で Windows にログオンしておく必要があります。
※ 予め管理者鍵をコンピューターに装着しておく必要があります。

1. 「USB HardLocker バックアップ」を起動します。

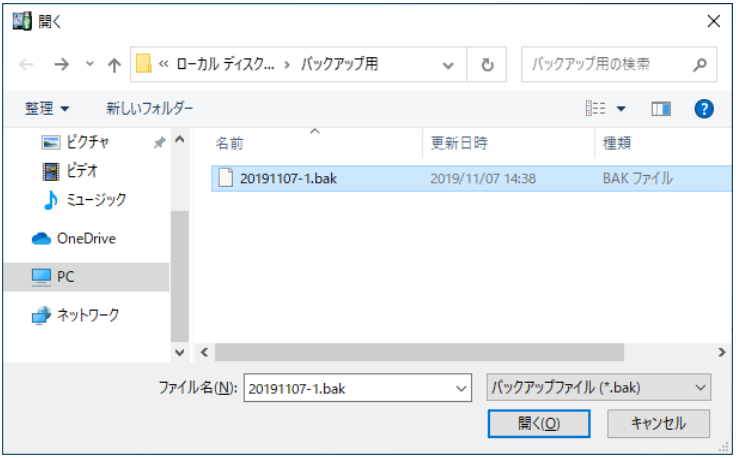
2. 『USB HardLockerバックアップ』操作画面で「リストア」をクリックします。



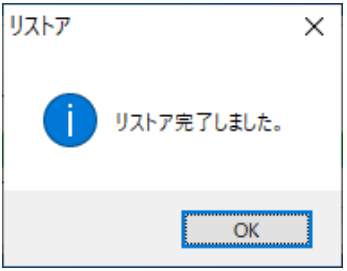
3. 初期設定完了済みの環境等、すでに鍵が設定されている場合、「現在の設定を削除してもいいですか？」という確認メッセージが表示されます。現在の設定を完全に削除してバックアップされている設定を上書きしたい場合は「OK」をクリックします。（「OK」をクリックすると、秘密領域やログも削除されます）。



4. バックアップファイルを選択して「開く」をクリックしてください。リストアが実行されます。
※ バックアップ時に複数のアーカイブに分割している場合は、すべてのファイルが揃わないとリストアを実行できません。

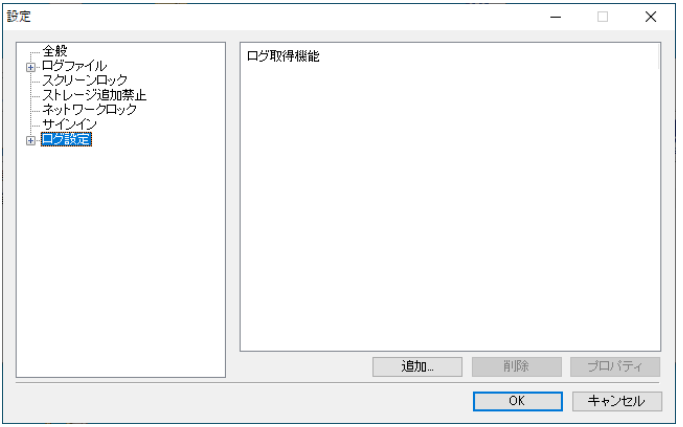


5. リストアが完了すると以下のメッセージが表示され、リストアされた内容に基づいて『USB HardLocker 5』が動作します。管理者鍵が装着されていない場合、設定内容によってはスクリーンロックがかかります。

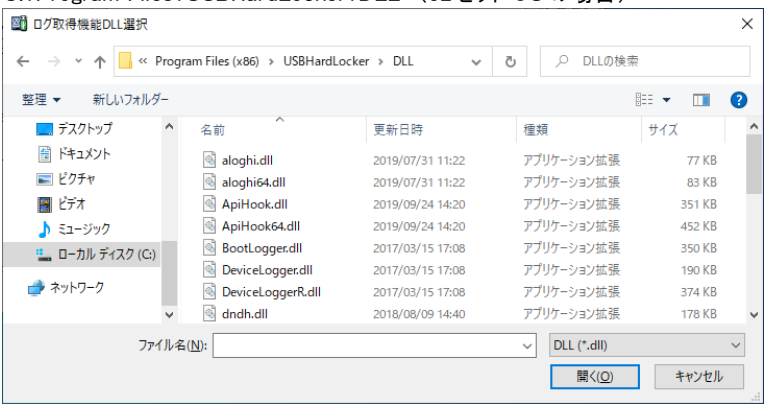


＜ログの再設定方法＞
32 ビット OS − 64 ビット OS の間でバックアップ − リストアを実行する場合、ログの設定がクリアされます。この場合、手動にて設定作業をする必要があります。

1. 「設定」アイコンをクリック−「ログ設定」を選択します。
この画面でログの取得設定が空白の場合は、「追加」をクリックしてログを取得する項目を追加します。



2. 「追加」をクリックするとエクスプローラーが起動して dll ファイルの一覧が表示されます。ここで、dll とログ項目の対応表を参考にして、必要な項目に対応した dll を選択して「開く」をクリックします。
下図のように dll ファイルが表示されない場合は、次のフォルダーを選択します。
C:¥Program Files (x86)¥USBHardLocker¥DLL （64 ビット OS の場合）
C:¥Program Files¥USBHardLocker¥DLL （32 ビット OS の場合）



＜dll の種類とログの項目＞

dll 名	ログの種類
BootLogger.dll	ログオンとログオフ
DeviceLoggerR.dll	ハードウェアの追加と削除
FileLogerR.dll	ファイルアクセス
FileOpeLoggerR.dll	ファイル操作
KeyLoggerR.dll	キーボード
PrintLoggerR.dll	印刷
ProcessLogger.dll	プロセス
URLLogger.dll	インターネットアドレス
WebUploadLoggerR.dll	Web アップロード
WindowTitleLoggerR.dll	ウィンドウ

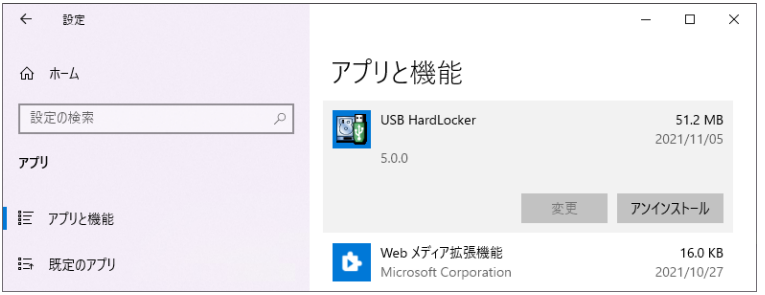
3. 上記 2.で BootLogger.dll を追加した場合、「ログオン」の項目が追加されます。この操作を繰り返して、必要なログの種類に対応する dll を追加していきます。

第6章　アンインストール

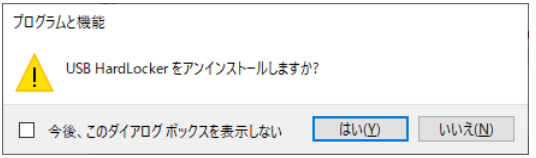
第1節　USB HardLocker 5のアンインストール

『USB HardLocker 5』のアンインストールについて説明します。
※ 管理者権限で Windows にログオンしてから実行する必要があります。
※ アンインストールするには管理者鍵の認証をする必要があります。予め管理者鍵を装着した状態でアンインストールを開始することをお勧めします。
※ アンインストールを実行すると秘密領域およびそこに保存されたファイル、鍵の設定情報、ログファイルはすべて削除されます。

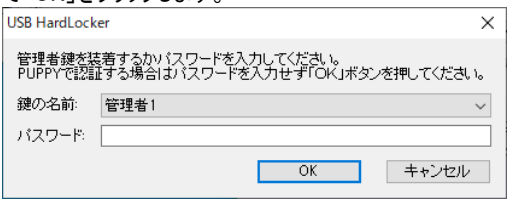
1. 「設定」－「アプリ」から「USB HardLocker」を選択して「アンインストール」をクリック、または「コントロールパネル」－「プログラムと機能」から「USB HardLocker」を選択して「アンインストール」をクリックします。



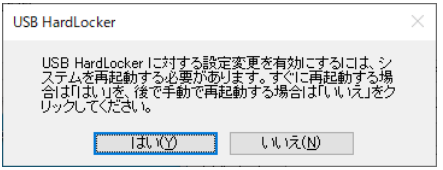
2. ウィザードが起動するので、「はい」をクリックします。



3. 管理者鍵が装着されていない場合は管理者の認証を要求するメッセージが表示されます。管理者鍵を装着するか、管理者鍵に設定しているパスワードを入力して「OK」をクリックします。



4. ファイルの削除終了後、再起動を促すメッセージが表示されます。
アンインストールを完了するためにはシステムを再起動する必要があります。すぐに再起動してよい場合は「完了」をクリックします。



使用許諾契約書

当製品をご使用前に、下記のライセンス契約書を必ずお読みください。本使用許諾契約書（以下「本契約」といいます）は、下記に示されたライフボート ソフトウェア製品（以下「ソフトウェア製品」といいます）に関してお客様（以下「甲」といいます）と株式会社ライフボート（以下「乙」といいます）との間に締結される契約書です。ソフトウェア製品を開封、インストール、複製、または使用することによって、お客様は本契約の条項に同意し、契約が成立したものとします。本契約の条項に同意されない場合、株式会社ライフボートは、お客様にソフトウェア製品のインストール、使用または複製のいずれも許諾できませんので、予めご了承ください。

第 1 条 定義

1. ソフトウェア製品
   本契約に基づき、乙が甲に提供するプログラムおよび関連資料を包括していい、改良版のソフトウェア製品が提供された場合には、当該改良版のソフトウェア製品をいう。
2. プログラム
   機械読取可能な形式で提供されるデータ処理プログラムをいう。
3. 関連資料
   プログラム以外の資料で、乙がプログラムの使用に関連して提供する、乙指定の資料をいう。

第 2 条 契約の目的

乙は甲に対しソフトウェア製品を非独占的に使用する譲渡不能な権利を許諾する。

第 3 条 契約期間

本契約は、本契約成立時から、甲または乙が本契約に従い解約するまで存続する。

第 4 条 使用権

1. 甲は、プログラムを1ライセンスに付き1台のコンピュータで使用することができる。また、印刷物の形で提供されたソフトウェア製品を本契約の目的に従って使用することができる。
2. 甲は、本契約に基づく使用権につき再使用権を設定し、またはソフトウェア製品もしくはその複製物を第三者に譲渡、転貸もしくは占有の移転をしてはならない。ただし、甲の管理の下で甲のためにソフトウェア製品を第三者に使用させる場合はこの限りでなく、甲の使用とみなすものとする。
3. 甲がマルチライセンスパックを購入した場合、本契約以外の書面（パッケージ等）において指定される許諾数だけのコンピュータにインストールできる。

第 5 条 複製権

甲は、ソフトウェア製品の一部または全部をバックアップコピー作成のためにのみ、複製及び複写することができる。甲は上記の目的以外のために、ソフトウェア製品の一部または全部を、メディアを問わず、転写、複製または複写してはならない。

第 6 条 危険負担

納入前に生じたソフトウェア製品および記録媒体の喪失または損傷は、甲の責に帰すべきものを除き乙の負担とし、納入以後に生じたこれらの損害は乙の責に帰すべきものを除き甲の負担とする。

第 7 条 保証

1. ソフトウェア製品の媒体及び関連資料に、物理的欠陥がある場合、甲がソフトウェア製品を購入してから90日間に限り、無償で乙より交換を受けることができる。
2. 乙は、ソフトウェア製品が甲の特定の使用目的に適合することを保証するものではない。また、前項において明示する場合を除き、本ソフトウェア及びサポートサービスに関して一切の保証を行わないものとする
3. 前各項の定めは、本契約に基づく法律上の瑕疵担保責任を含む、乙の保証責任のすべてを指定したものとする。

第 8 条 乙の責任および責任の制限

1. プログラムの不稼働を含む稼働不良のすべての場合において、乙の責任は誤りの訂正に合理的努力を尽すことに限られるものとする。
2. 法律上の請求の原因の種類を問わず、乙は、法律上許容される最大限において、本ソフトウェア製品の使用もしくは使用不能、サポートサービスの提供もしくは提供不能またはその他本契約書に関して生じる特別損害、付随的損害、間接損害、派生的損害、またはその他の一切の

損害（逸失利益、機密情報もしくはその他の情報の喪失、事業の中断、人身傷害、プライバシーの喪失、誠実義務または合理的な注意義務を含めた義務の不履行、過失、またはその他の金銭的損失を含むがこれらに限定されない）に関しては、乙の過誤、不法行為（過失を含む）、無過失責任、契約違反または保証違反の場合であっても、一切責任を負わないものとする。たとえ、乙がこのような損害の可能性について知らされていた場合でも同様である。

3. 本ソフトウェア又はサポートサービスに起因して、甲、もしくはその他の第三者に生じた結果的損害、付随的損害及び逸失利益に関して、乙は一切の責任を負わないものとする。本契約のもとで、理由の如何を問わず、乙が甲、又はその他の第三者に対して負担する責任の総額は、損害の原因となった本ソフトウェアに対して本契約のもとで甲が実際に乙へ支払った対価の100%を上限とする。

第 9 条 著作権等の侵害に関する損害賠償責任

1. ソフトウェア製品の使用が、第三者の著作権または工業所有権等の知的所有権を侵害したという理由で、甲が第三者より請求を受けた場合には、甲が次の各号所定のすべての要件を満たす場合には、乙の責任と費用負担で、当該請求を処理解決するものとし、甲に一切の損害を及ぼさないものとする。
   (1) 甲が第三者から請求を受けた日から速やかに、乙に対し請求の事実および内容を通知すること。
   (2) 甲が第三者との交渉または訴訟の遂行に関し、乙に実質的な参加の機会および決定の権限を与え、ならびに必要な援助をすること。
2. 乙は、甲が次の各号の一に該当する場合には、甲に対し前項所定の責任を負わない。
   (1) 甲が乙提供以外のプログラムと組合わせて使用したことに起因するとき。
   (2) 甲が本契約に違反してソフトウェア製品を使用したことに起因するとき。

第 10 条 ソフトウェア製品の変更または改作

甲は、自己の使用のため、必要な場合を除き「乙の許可なく」ソフトウェア製品を変更、または改作してはならない。

第 11 条 解約および解除

1. 甲は、乙に30日前の書面による通知をして、任意に解約することができる。
2. 甲または乙は、相手方に次の各号に掲げる事由の一が生じたときには、なんらの催告なしに直ちに本契約を解除することができる。
   (1) 支払いの停止または破産、和議開始、会社更正手続開始、会社整理開始もしくは特別清算開始の申立があったとき。
   (2) 手形交換所の停止処分をうけたとき。
3. 甲または乙は、本契約に違反すること等相手方の債務不履行が相当期間を定めてした催告後も是正されないときは、本契約を解除することができる。
4. 前各項の適用によりソフトウェア製品の使用権が消滅した場合には、甲は返還または破棄の手続きを行うものとする。

第 12 条 ソフトウェア製品の返還または破棄

1. 甲は、使用権の消滅後2週間以内にソフトウェア製品およびすべての複製物（変更または改作されたものを含む）を、乙に返還しまたは破棄するものとする。
2. 甲は、前項による返還または破棄と同時に、前項所定の事実を証明する書類を乙に提出する。

第 13 条 合意管轄

本契約に関し訴訟の必要が生じた場合には、乙本店所在地を管轄する裁判所を専属管轄裁判所とする。

第 14 条 協議

本契約に関して疑義が生じた場合には、両当事者は信義誠実の原則に従い協議するものとする。

USB HardLocker 5 利用ガイド

2023 年 8 月 9 日　　第 2 版

（非売品）

著作　　株式会社ライフボート

発行所　　株式会社ライフボート

東京都千代田区神田神保町 2-2-34