情報漏えい対策ツール

USB HARDLOCKER 4 Server

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

USB HardLocker 4 利用ガイド

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
December 2014

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: http://www.lifeboat.jp/

目　次

第1章　USB HardLocker 4 Serverの概要

第1節　USB HardLocker 4 Server について

『USB HardLocker 4 Server』はWindows Serverの不正操作防止、USBストレージの使用制限、データの自動暗号化、操作ログの収集といったデータ流失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。

■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

コンピューター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。施錠された状態でログオンすると、スクリーンロックが直ちにかかり操作が一切できなくなります。解錠するとスクリーンロックが直ちに解除されます。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。

● 暗号化領域の作成

内蔵ハード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。予め登録された鍵により開錠されたときにだけ、仮想ドライブとして暗号化領域にアクセスができるようになります。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。

● ネットワークロック

鍵を取り外すことで、ネットワーク接続を切断して、外部からの不正アクセスを防ぐことができます。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保存します。

● 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の接続を検出すると、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。

● 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。

● 鍵情報と暗号化領域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、暗号化領域をバックアップすることができます。リストアには管理者鍵が必要となるため、セキュリティのレベルを落とさずにバックアップをとることができます。

● 64ビットOSに対応
64ビットOS（Windows Server 2012/2012 R2、Windows Server 2008/2008 R2、Windows Server 2003）に対応しました。

第2節　　設定できる鍵の種類について

『USB HardLocker 4 Server』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 4 Server』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	◎	○
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	◎	×
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＞
■対応機種： 各社 DOS/V 機（NEC PC-9800、PC-9821 シリーズ、Macintosh では動作しません）
■対応 OS： Windows Server 2008/2008 R2、 Windows Server 2003/2003 R2、Windows Server 2012/2012 R2
※ ここに記載されていない OS、日本語版以外の OS には対応しておりません。
■CPU： Intel Pentium 互換 300MHz 以上（Windows Server 2008/2008 R2 /2012 は 1.4GHz 以上）
■ハードディスクの空き容量： 20MB 以上（暗号化領域作成時、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）
■必要メモリ： 512MB 以上（1GB 以上を推奨）

■その他： 鍵になる USB 機器、利用可能な USB ポート（2.0 以上）、CD-ROM ドライブ（インストール時）

＜鍵になるUSB機器について＞
『USB HardLocker 4 Server』は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（扇風機、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。

＜Windows Server 2012/2012 R2環境のご注意＞
Modern UI画面の表示中は鍵を取り外してもロックが動作しません。デスクトップに表示に切り替えてください。

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。

＜作成できる暗号化領域について＞
暗号化領域は、鍵1つにつき1つ作成可能です。
暗号化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 4　Server』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。

＜ご利用環境上の留意点について＞
仮想ドライブを扱うソフトウェア、スクリーンロック機能を持つソフトウェアとの併用はサポートしておりません。

＜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。

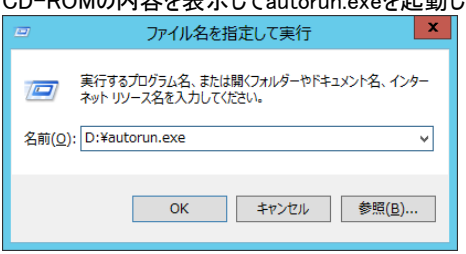
＜USB HardLocker for Server Version 3.0 からのアップデート＞
バージョン 3.0 がインストールされている場合、バックアップツールを使用して『USB HardLocker 4 Server』に鍵の設定情報を引き継ぐことができますが、プログラムの上書きインストールによるアップデートをすることはできません。

第2章　USB HardLocker 4 Server のインストール

第1節　USB HardLocker 4 Serverのインストール

注意！　:インストールをするにはライセンスキーが必要です。
（ライセンスキーはライセンス証書またはユーザー登録はがきに記載されています。ダウンロード版の場合はメールに添付されます。）事前にご用意ください。
※　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。

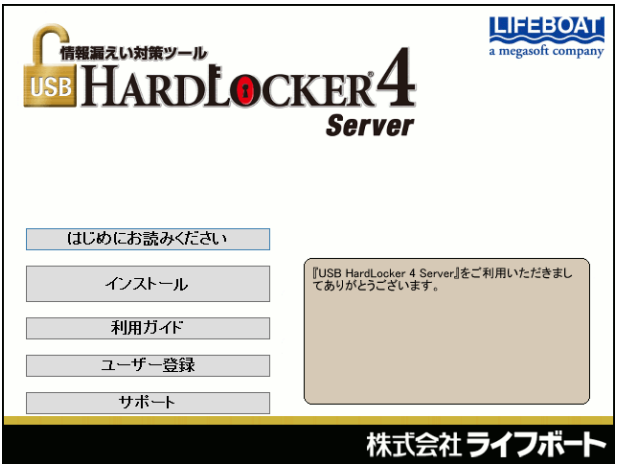
1. 『USB HardLocker 4 Server』CD-ROMをドライブにセットすると、インストールのためのメニューが起動します。自動的に起動しない場合は、エクスプローラーからCD-ROMの内容を表示してautorun.exeを起動してください。



Windows Server 2012 の Modern UI Style 環境に CD-ROM をセットした場合

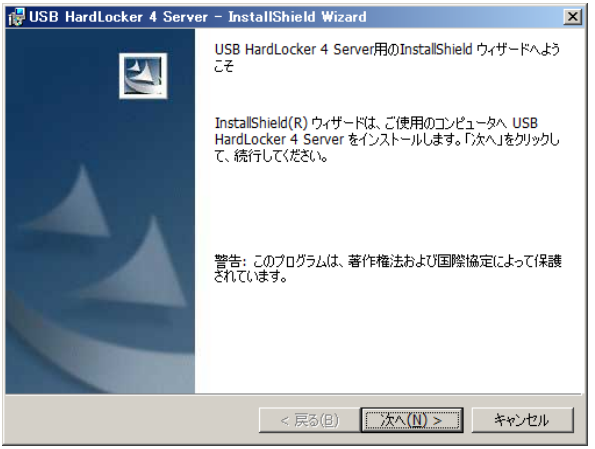
ディスクに対する操作から「autorun.exe」の実行を選択すると、画面がデスクトップに切り替わり、『USB HardLocker 4 Server』のインストールメニューが表示されます。

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。

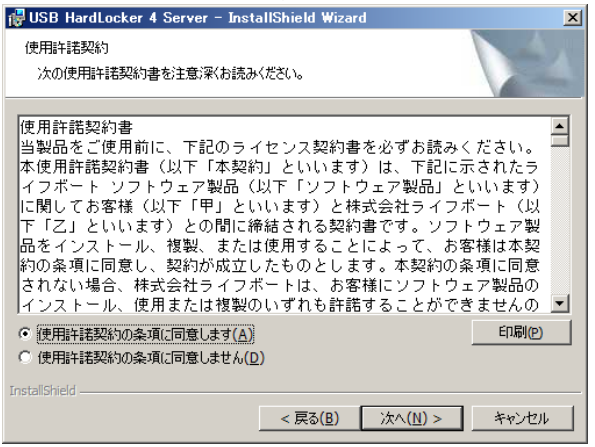


メニューの説明	
はじめにお読みください	最新の更新情報等を掲載していることがあります。インストール前にお読みください。
インストール	『USB HardLocker 4 Server』のインストールを開始します。
利用ガイド	『USB HardLocker 4 Server 利用ガイド』(PDF)を開きます。
ユーザー登録	Adobe Readerがコンピューターにインストールされていない場合にクリックします。
サポート	メニュー画面の2ページ目を表示します。サポートセンターのご利用方法やライフボートの製品ページへのリンクを表示します。

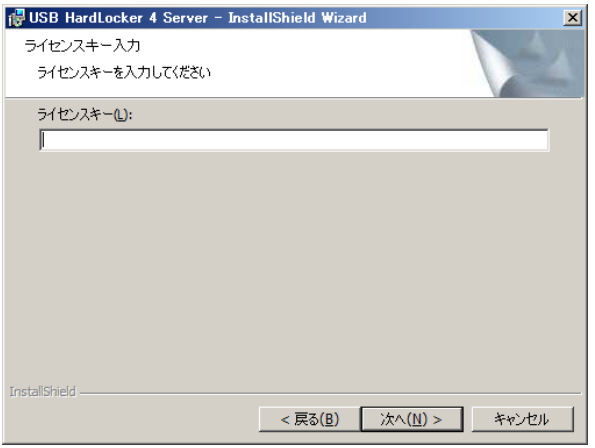
3. 「インストール」をクリックすると、インストールウィザードが起動します（インストールの完了後にシステムの再起動が必要となるので他のプログラムはあらかじめ終了しておいてください）。「次へ」をクリックしてください。



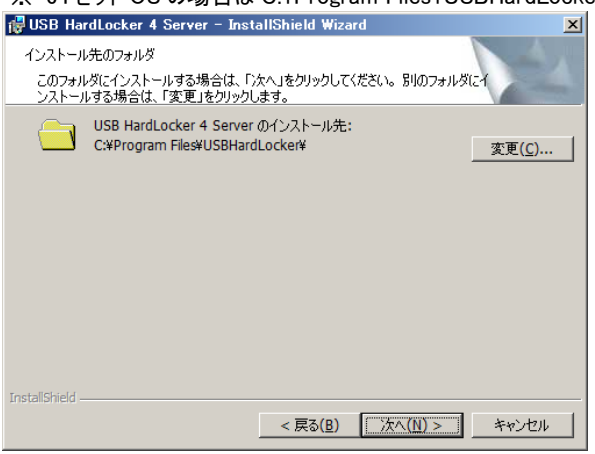
4. 「ライセンス」画面が表示されます。契約内容をよくお読みいただき、同意いただける場合は「使用許諾契約の全条項に同意します」をチェックして「次へ」をクリックしてください。同意いただけない場合には「使用許諾契約の条項に同意しません」を選択してインストールを中止します。



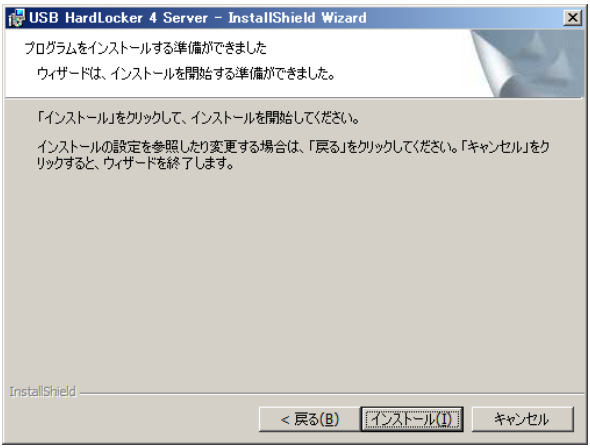
5. ライセンスキーを入力して「次へ」をクリックしてください。
※ ライセンスキーは半角英数字で正確に入力する必要があります。



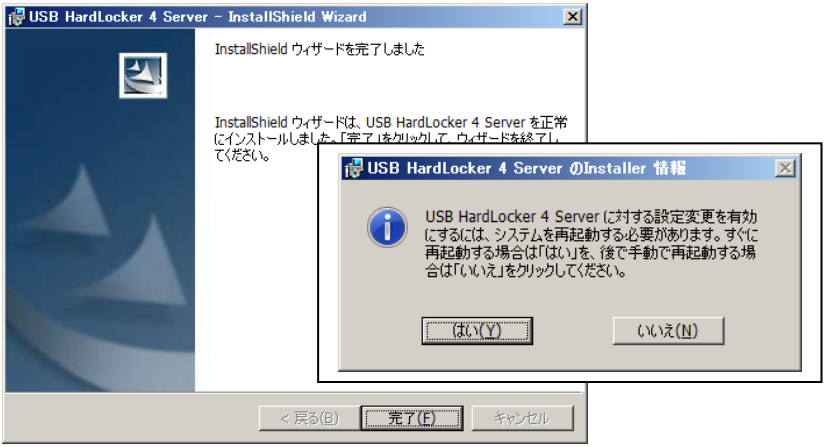
6. 「インストール」をクリックします。インストール先を変更する場合は「変更」をクリックしてインストール先を指定することができます。
デフォルトのインストール先は C:¥Program Files¥USBHardLocker です。
※ 64 ビット OS の場合は C:¥Program Files¥USBHardLocker(x86)



7. 「InstallShield Wizardの完了」画面が表示されます。インストールを完了するためには「完了」をクリックしてコンピューターを再起動する必要があります。



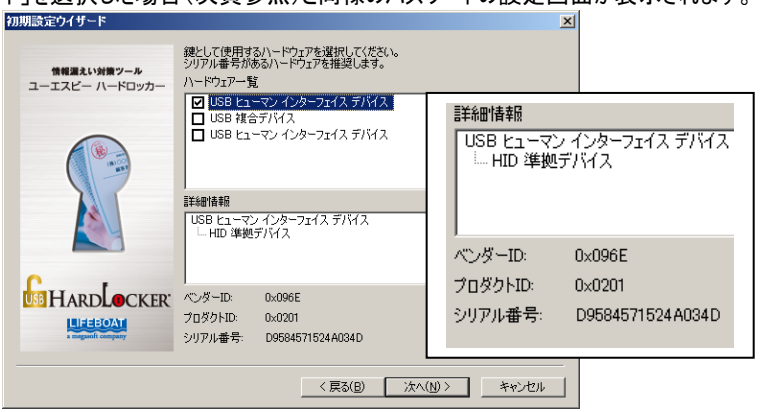
8. 「InstallShield Wizardの完了」画面が表示されます。インストールを完了するためには「完了」をクリックしてコンピューターを再起動する必要があります。



第2節　初期設定ウィザード

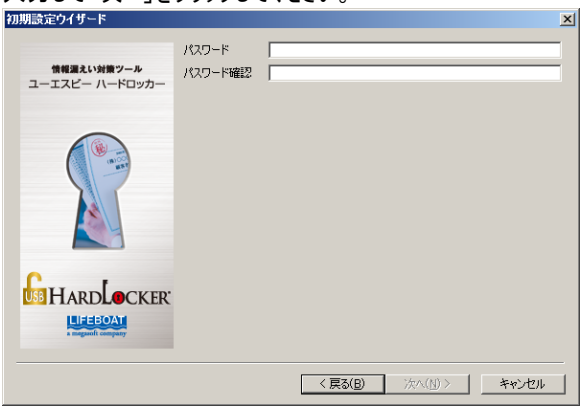
1. インストール完了後、コンピューターを再起動すると初期設定ウィザードが表示されます。最初に登録する管理者鍵として採用したい認証方法を選択して「次へ」をクリックしてください。

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シリアル番号を持っていません。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、鍵には設定しないでください。鍵に設定する機器はシリアル番号を持つものを推奨します。

「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。



＜パスワード設定に関する注意＞

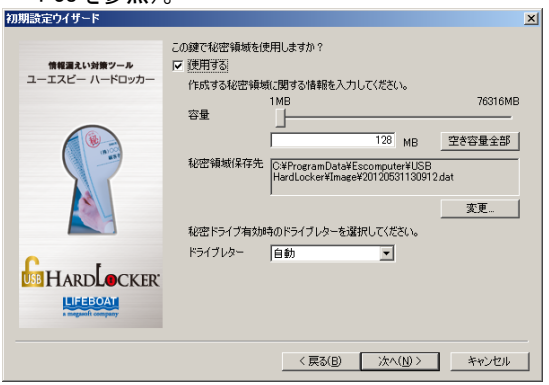
※ 表示可能な半角英数記号を最大 63 文字まで設定可能です。全角文字は使用できません。

※ 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 4 Server』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ます。秘密領域を使用する場合は、「使用する」をチェックして容量の指定や保存先の設定をして「次へ」をクリックします。
※ 秘密領域は鍵の作成完了後に作成することも可能です（秘密領域の設定は P38 を参照）。



5. 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。
※ 特殊文字や記号は鍵の名前に使用しないでください。

6. 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。

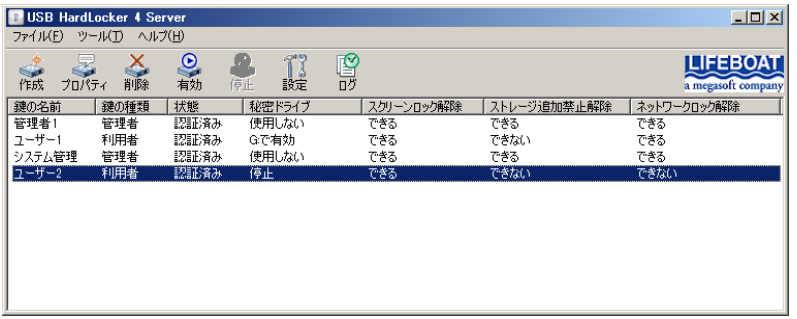
この画面では次の内容を確認することができます。

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
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 4 Server を使用する

第1節　ユーティリティの起動

1. Windows の「スタート」メニューから「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 4 Server』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。

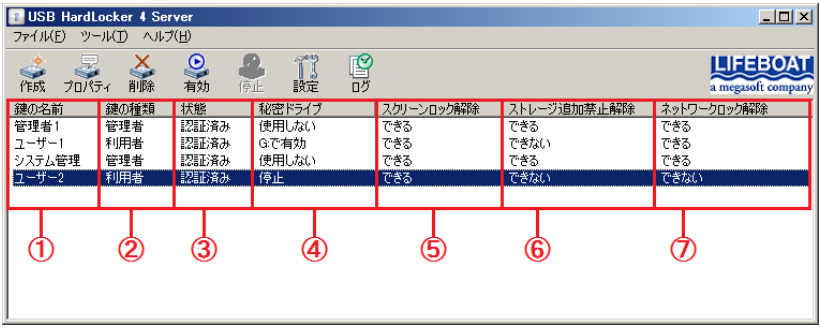


※　管理者鍵が装着されている場合と、利用者鍵のみ装着されている場合では、操作できる内容が異なります。
操作できる内容については、＜メニューボタンの説明＞をご覧ください。

＜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（P24 参照）。（管理者鍵装着中のみ操作できます。）
	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。
	「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」、「ログの設定」を変更します。 （管理者鍵装着中のみ操作できます。）
	ログをリアルタイムに表示します（P52 参照） （管理者鍵装着中のみ操作できます。）

＜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	スクリーン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。

①～⑦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。

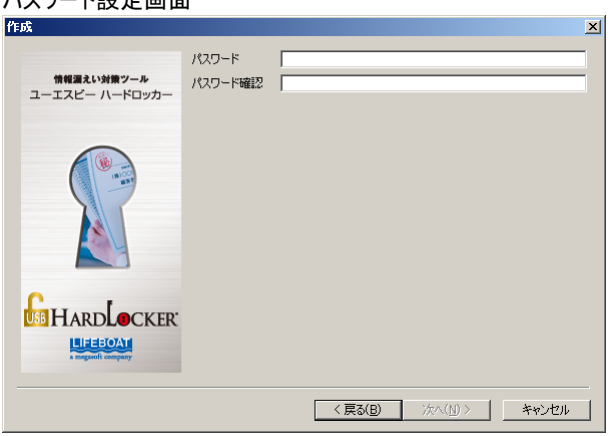
第2節　鍵の設定

ユーティリティ画面から鍵を新規に作成する方法について説明します。

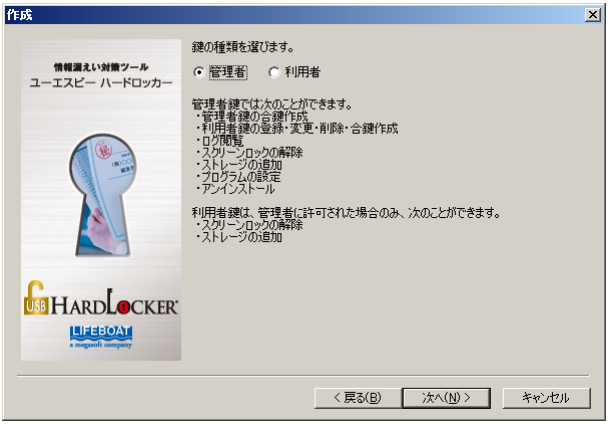
1. ユーティリティから「作成」をクリックすると作成ウィザードが起動します。
使用したい認証方法を選択して「次へ」をクリックします。

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」を選択した場合は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。

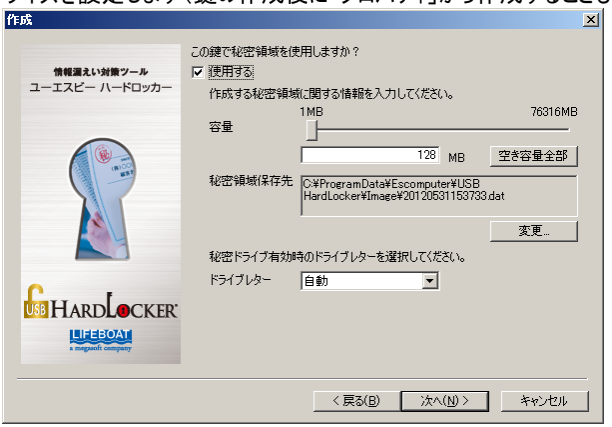
パスワード設定画面



3. 鍵の種類を選択して「次へ」をクリックします（初期設定ウィザードで管理者鍵を設定した後は利用者鍵を設定することができるようになります）。管理者鍵、利用者鍵の機能については、（P7）を参照してください。



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）。

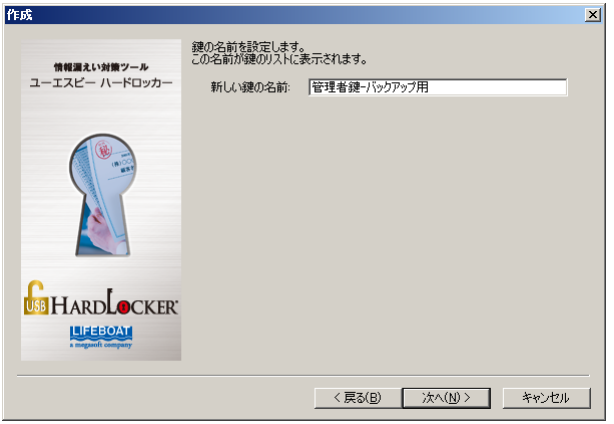


5. この鍵をスクリーンロックの解除用に使用したい場合は「この鍵はスクリーンロックを解除できる」をチェックして「次へ」をクリックします。
（管理者鍵を作成する場合、この選択画面は表示されません。）

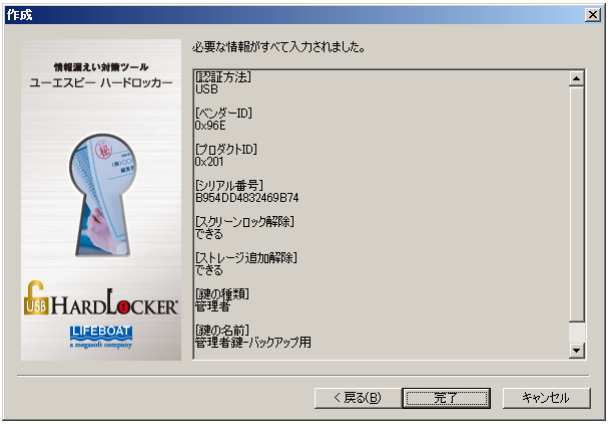
6. ストレージの追加禁止を解除できるようにしたい場合は「この鍵はストレージ追加禁止を解除できる」をチェックして「次へ」をクリックします。
（管理者鍵を作成する場合、この選択画面は表示されません。）

7. 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、この選択画面は表示されません。）

8. 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。



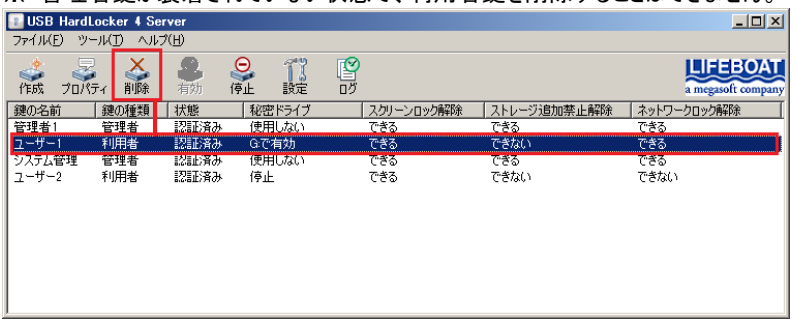
作成した鍵の設定内容が表示されます（表示される内容は初期設定の設定確認画面で表示されるものと同様です）。内容を確認して「完了」をクリックします。
設定内容を修正したいときは「戻る」で変更することができます。



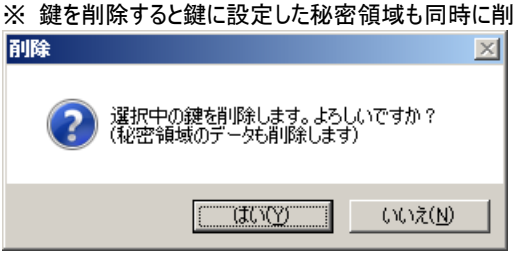
第3節　鍵の削除

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。



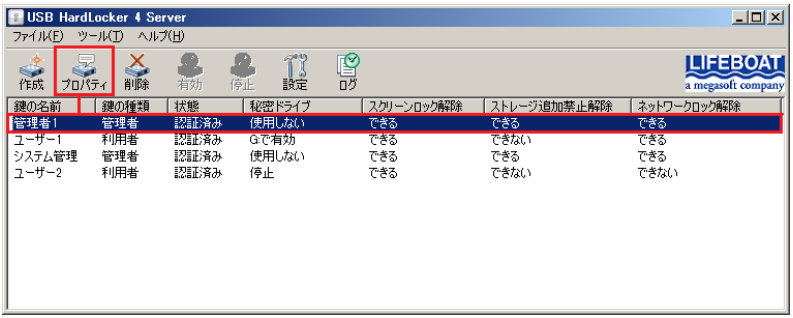
2. 鍵を削除するための確認メッセージが表示されるので、よろしければ「はい」をクリックします。選択した鍵が削除されます。
   ※ 鍵を削除すると鍵に設定した秘密領域も同時に削除されます。



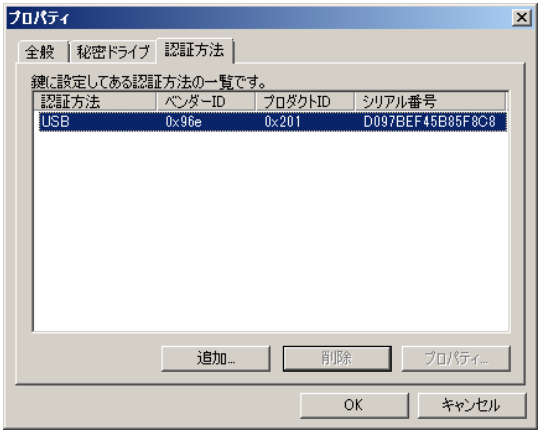
第4節　合鍵の設定

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。

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。

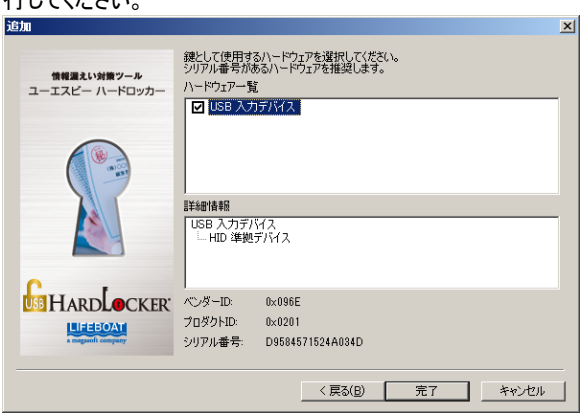


2. 「認証方法」タブから「追加」をクリックします。

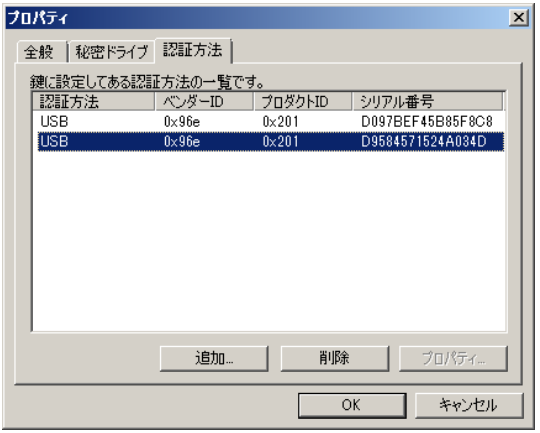


3. 設定したい認証方法を選択して「次へ」をクリックします。
ここでは合鍵として「USB」を設定する場合を例にして説明します。

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、前頁2.～の操作を繰り返し実行してください。



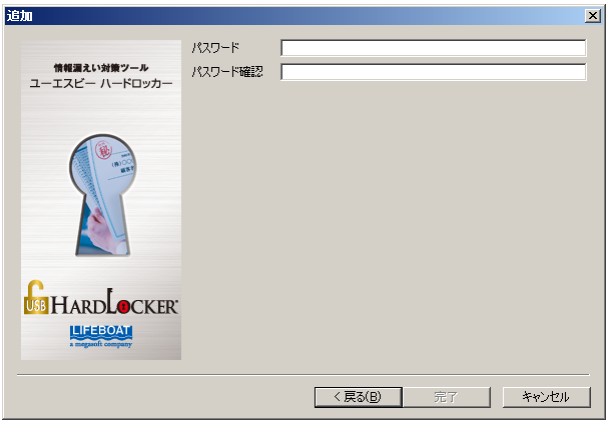
5. 追加されたUSB鍵が認証方法リストに追加されます。



※ 認証方法の変更をしたい場合は、先に新しい認証方法を追加した後に、元の認証方法を選択して「削除」をクリックします。

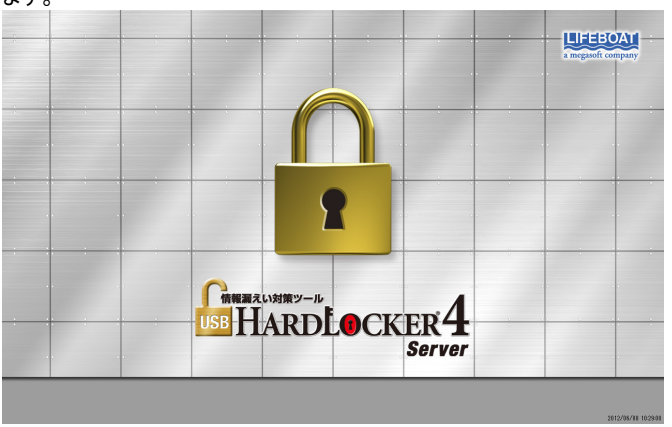
6. パスワードを追加する場合は 5.の鍵のプロパティ-「認証方法」から「追加」をクリックして「パスワード」を選択します。

7. 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。
※ パスワードについての注意事項は（P17）をご参照ください。



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、コンピューターの操作ができなくなります。



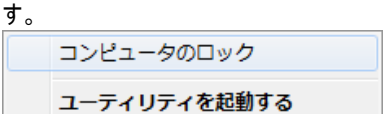
※ この他に、許可しないUSB機器やドライブが追加された時にスクリーンをロックする機能があります。（P43参照）

＜ロックするための操作方法＞

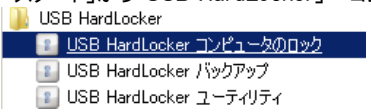
設定した鍵の種類	操作方法
USB	鍵を取り外します。
パスワード	「コンピューターのロック」操作（※）をします。
USB × パスワード	鍵を取り外します。

※ 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。

1. Windowsの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。



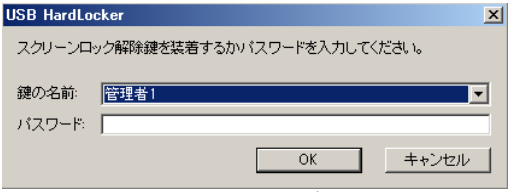
2. 「スタート」から「USB HardLocker」-「コンピューターのロック」を選択します。



3. 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＞

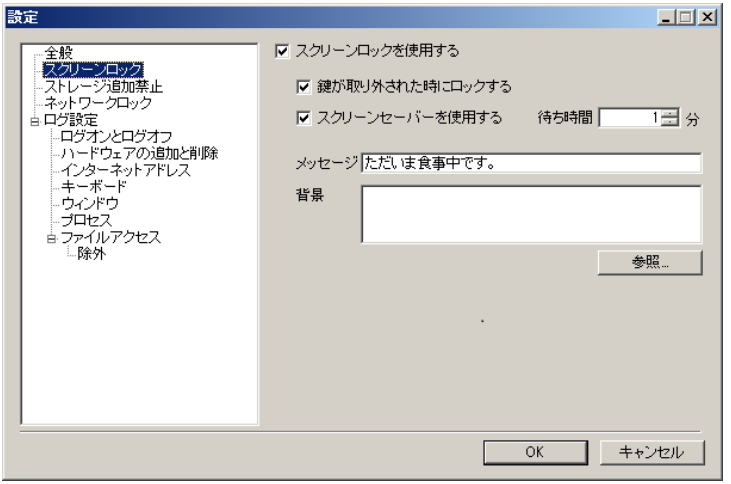
鍵の種類	操作方法
USB	鍵を装着します。
USB×パスワード	鍵を装着後パスワード入力画面が表示されるのでパスワードを入力します。
パスワード	「Ctrl」+「Shift」+マウスの左クリックによりパスワード入力画面を表示してパスワードを入力します。



※ **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」+マウスの左クリックをします。

＜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＞

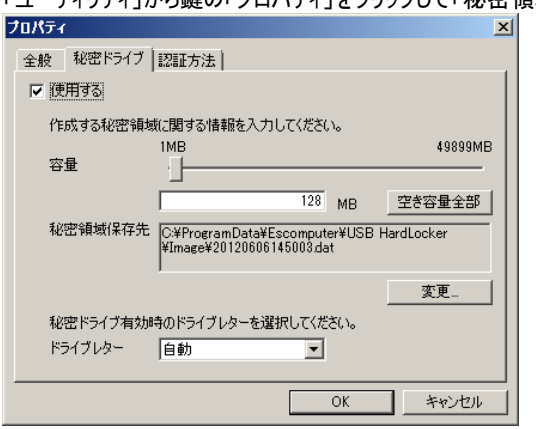
スクリーンロックを使用する	スクリーンロック機能を有効にします。
鍵が取り外された時にロックする	設定した鍵を取り外した時にスクリーンをロックします。
スクリーンセーバーを使用する	スクリーンのロック後、指定された時間が経過した後にスクリーンセーバーを起動します。
メッセージ	スクリーンロック画面（P35の図）に指定されたメッセージを表示することができます。
背景	ロック画面を他の画像に変更することができます。 「参照」をクリックして使用したい画像を指定します（形式はBMPのみ）。※

※ デフォルトのサイズは 1280×800 ピクセルですが、1024×768 の画像が用意されています。

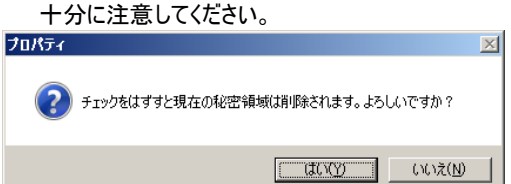
第6節　秘密領域の設定

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ハードディスクのみとなります。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」(P24)をご覧ください。

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

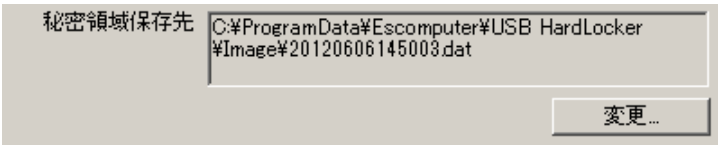


2. 「使用する」をチェックします。
※ 秘密領域が作成済みの場合にこのチェックをはずして「OK」をクリックすると次の警告メッセージが表示されます。ドライブレター以外の変更をすると、既存の秘密領域は削除され、そこに保存されているデータは消失します。変更時は十分に注意してください。

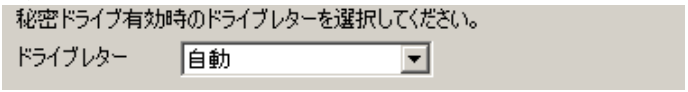


3. 作成する秘密領域のサイズを指定します。「容量」のスライドバーを操作するか、入力ボックスにサイズ(MB)を正の整数で入力してください。
「空き容量全部」をクリックすると秘密領域保存先に指定したドライブの空き容量すべてを割り当てます。
※ システムがインストールされたドライブの場合は「空き容量全部」をクリックしないでください。

4. 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。保存先のドライブやパスを変更する場合、「変更」をクリックしてください。
※ 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。



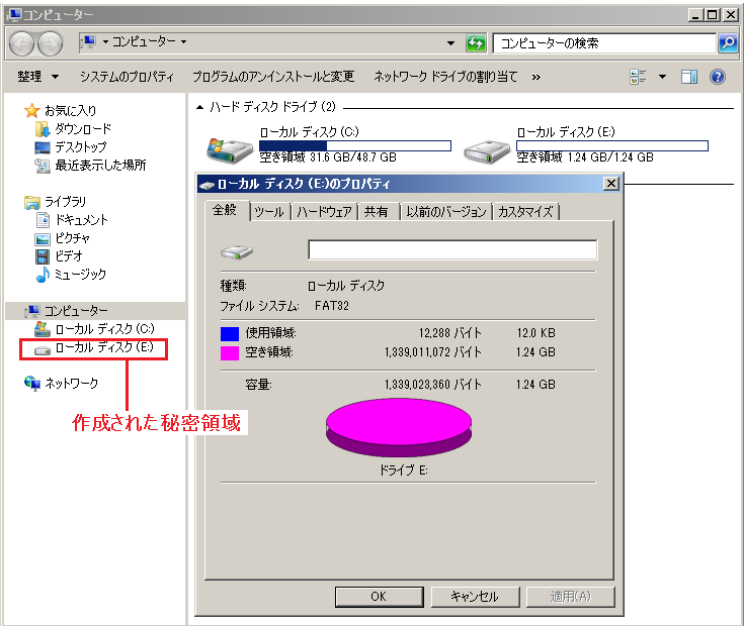
5. 秘密領域のドライブレターを指定したい場合はプルダウンリストから任意のドライブレターを指定します。自動を選択すると空いているドライブレターが割り当てられます。



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。



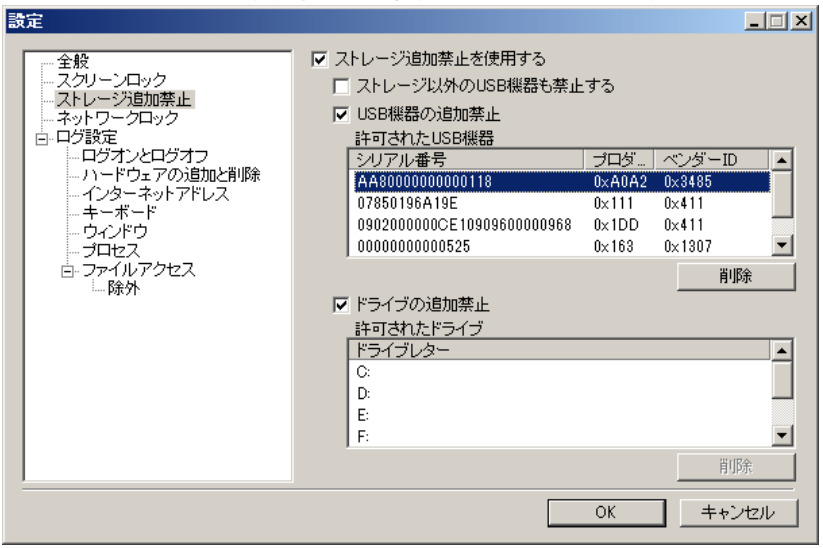
※ 秘密領域はデフォルトで FAT または FAT32 にフォーマットされています。

※ 秘密領域に 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。

第8節　ストレージ追加禁止

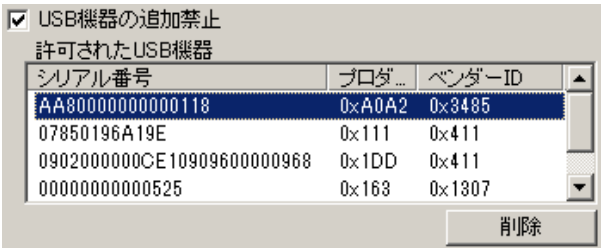
ストレージ追加禁止機能を使用するには 2 通りの方法があります。
A. 鍵の設定時に作成ウィザードで「ストレージ追加禁止を使用する」をチェックする。
B. 鍵の作成後にユーティリティから「プロパティ」で設定する。
ここではプロパティからの設定方法を説明します。

ユーティリティから「設定」をクリックして「ストレージ追加禁止」を選択します。ここで「ストレージ追加禁止を使用する」をチェックしてください。
※ ストレージ追加禁止は、鍵毎に異なる設定をすることはできません。



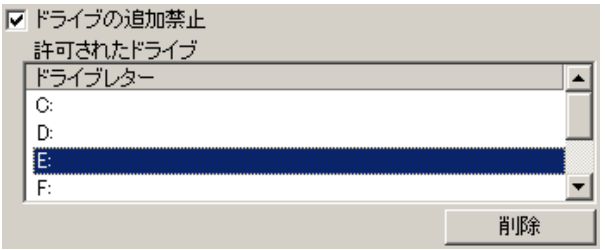
＜ストレージ以外の USB 機器も禁止する＞
スマートフォン、携帯音楽プレーヤーの一部の製品は、Windows 上で「ポータブルデバイス」と表示されます。「ポータブルデバイス」は USB 大容量記憶装置とは異なり、エクスプローラーやメディアプレイヤーからアクセスできますが、ドライブレターが表示されず『USB HardLocker 4 Server』のストレージ追加禁止の対象外となります。
「ポータブル デバイス」も禁止対象に含めたい場合にこのオプションをチェックします。

＜USB 機器の追加禁止＞
現在接続を許可されている機器が一覧にリストされます。



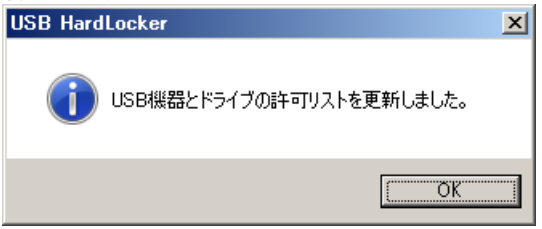
許可したくない機器がリストにある場合は、「削除」でリストから削除してください。許可リストが更新されます。解除権限を持つ鍵が装着されていない状態で、リストにない機器が接続されると、ストレージ追加禁止ロックが動作します。

＜ドライブの追加禁止＞
現在接続を許可されているドライブが一覧にリストされます。

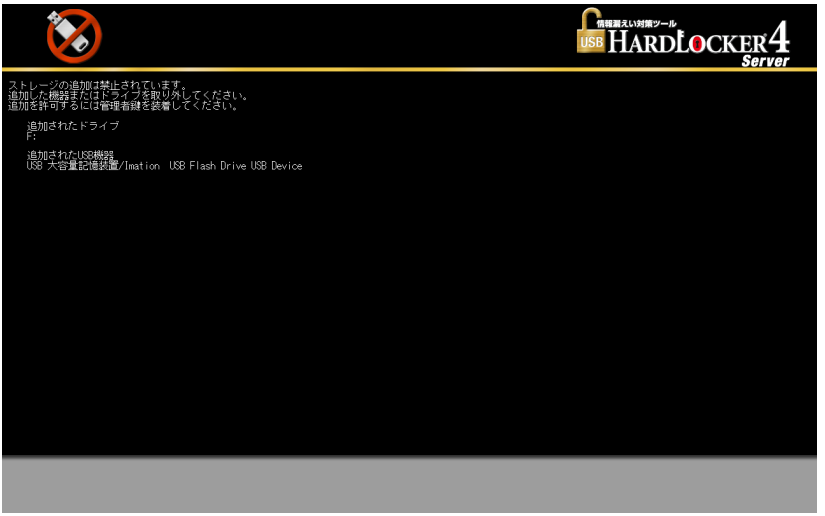


許可したくないドライブは「削除」をクリックしてリストから削除してください。許可リストが更新されます。解除権限を持つ鍵が装着されない状態でリストにないドライブが追加されると、ストレージ追加禁止ロックが動作します。

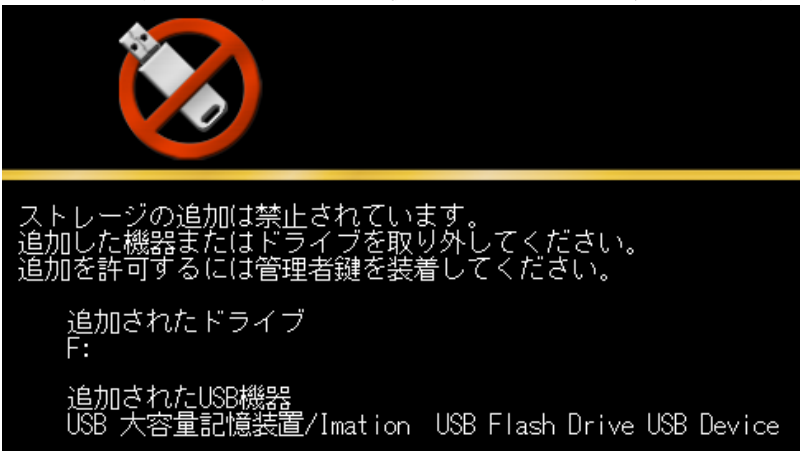
＜許可リストの更新＞
ストレージ追加禁止解除を許可する鍵が装着されている状態で新しい USB ストレージを装着したり新しいドライブを追加したりすると、次のメッセージが表示され許可リストが更新されます。



＜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。ロックされた状態では、コンピューターを操作することができません。



ロック画面には、追加された非許可 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では、ネットワークのロックは動作しません。

＜ストレージ追加禁止ロックの解除方法＞

ロックを解除するためには禁止された機器を取り外すか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 の場合は鍵を装着します。

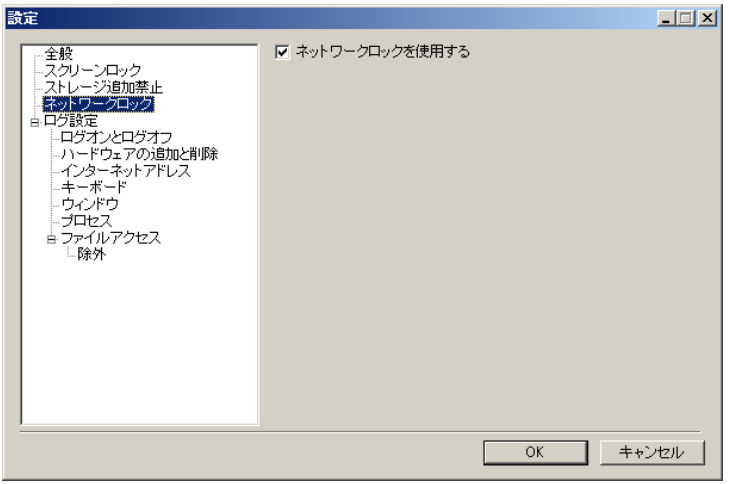
パスワードの場合は「Ctrl」+「Shift」+マウスの左クリックでパスワード認証画面を表示させ、パスワードを入力します。

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時に、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かかります。

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。
※ ネットワークロックはスクリーンロックと組み合わせずに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。

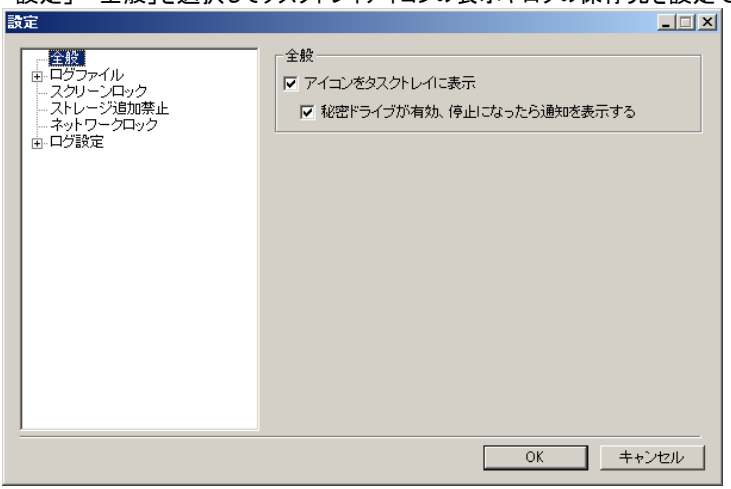


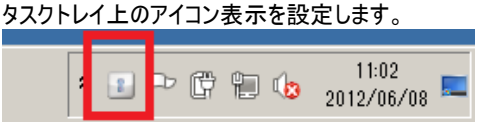
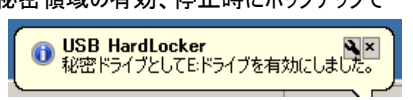
「ネットワークロックを使用する」をチェクしていると、鍵が取り外された時、ネットワークへの接続ができなくなります。

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を OFF にして、ネットワークロックのみ動作させている例です。）

第10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ログの保存先を設定できます。



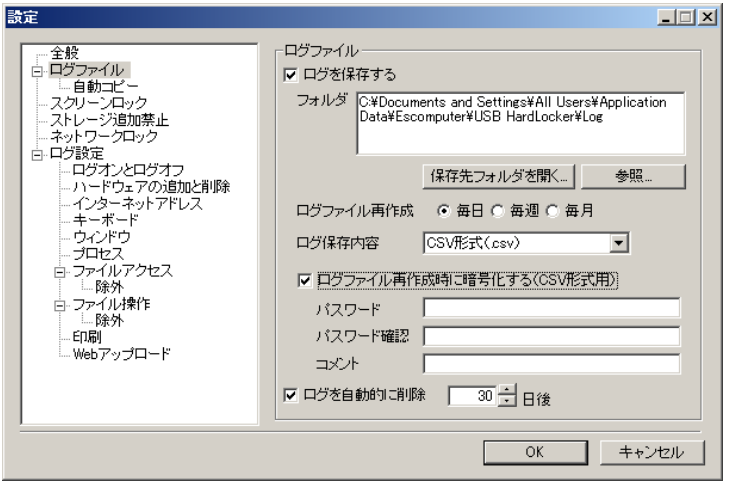
アイコンをタスクトレイに表示	タスクトレイ上のアイコン表示を設定します。 
秘密ドライブが有効、停止になったら通知を表示する	チェックすると秘密領域の有効、停止時にポップアップで通知します。 

※ 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

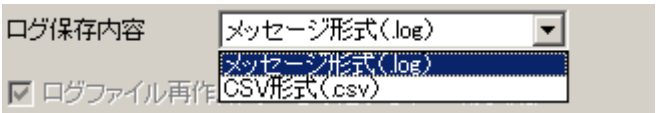
＜ログ保存の選択＞
ログを収集・保存する場合は「設定」タブ-「全般」-「ログを保存する」をチェックします。



＜ログの保存先＞
ログは初期設定で以下のパスに保存されます。「参照」から保存先を変更できます。
C:¥ProgramData¥Escomputer¥USB HardLocker¥Log

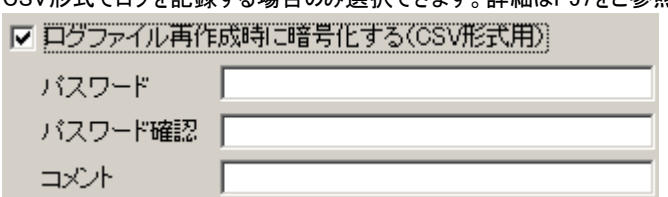
＜ログファイル再作成＞
「毎日」、「毎週」、「毎月」の単位でファイルを生成します。初期設定は「毎日」です。

＜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。



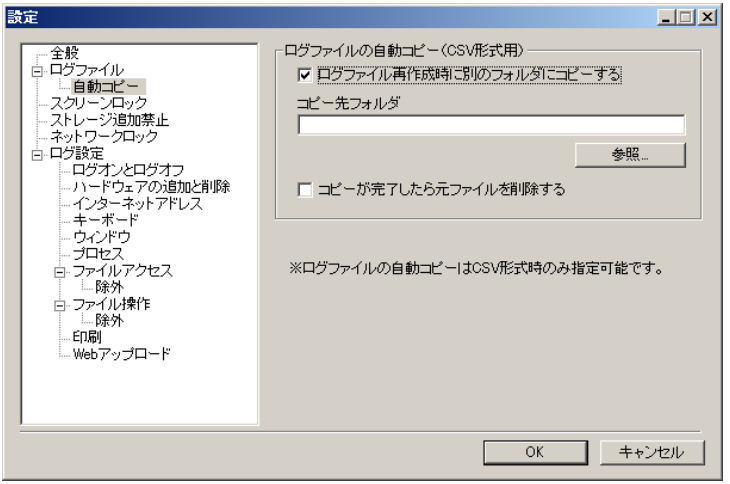
メッセージ形式(.log) (初期設定)	USB HardLocker 独自の形式で記録され、暗号化されます。閲覧するためには、ログを記録した USB HardLocker のユーティリティから「ログ」を起動するか、「ログ」画面からエクスポートをする必要があります。
CSV 形式(.log)	Excel やメモ帳等を利用して開くことができます。解析等が必要な場合に選択することをお勧めします。ように入力する必要があります。

＜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P57をご参照ください。



＜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毎日コピーします（CSV 形式を選択した場合のみ）。

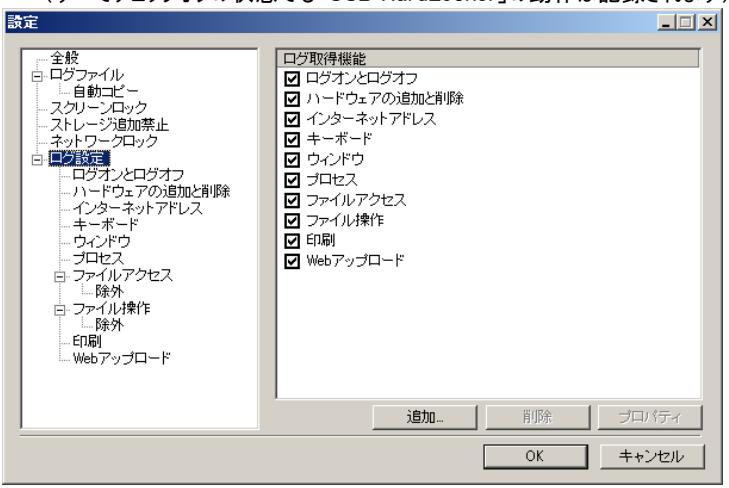


コピー先をネットワーク共有フォルダー等に指定して、ネットワークの切断等により自動コピーが実行できない場合は、コピー先のパスが有効になった時点で未コピー分のログのコピーが実行されます。

自動コピーは、ログの保存先をネットワーク共有フォルダーに設定したい場合に便利です。この場合、はじめにログの保存先をローカルコンピュータ上に指定します。次に自動コピーをチェックしてコピー先をネットワーク共有フォルダーに設定します。
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、ネットワーク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。
ネットワークロックを使用する環境では、ネットワーク共有フォルダーをコピー先に指定しないでください。

第2節　記録する項目の設定

「設定」タブ －「ログ設定」で取得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。
※ 初期状態ではすべてのチェックを外しています。必要に応じてチェックを入れてください。
（すべてチェックオフの状態でも「USB HardLocker」の動作は記録されます）



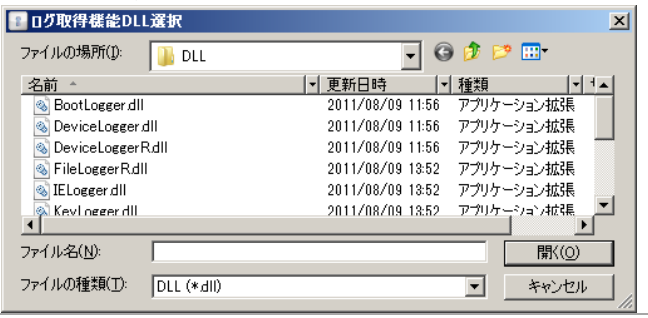
＜記録できるログの種類＞

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	Internet Explorer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、印刷した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。
USB HardLocker ※	USB HardLocker 4 Server 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／ロックの解除」、「ネットワークロック／ロックの解除」

※ USB HardLocker はログ取得機能一覧には表示されません。P47 の設定画面「ログを保存する」がチェックされていれば、自動的に記録されます。

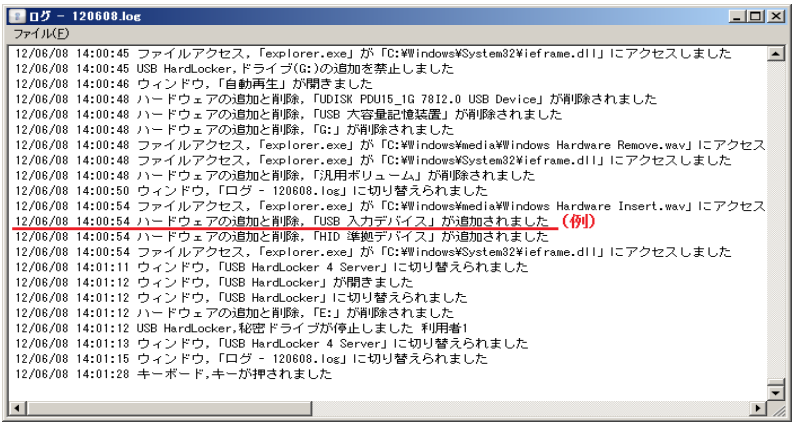
＜追加、削除、プロパティ＞

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。 
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。CSV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」をクリックしてログを参照することができます。ログを閉じてもアクセスログは常に保存されます。
※ ご使用の環境やログを取得する項目の設定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。



＜ログの表示内容＞

12/06/08	14:00:54	ハードウェアの追加と削除	「USB 入力デバイス」が追加されました
①日付	②時刻	③種類	④詳細

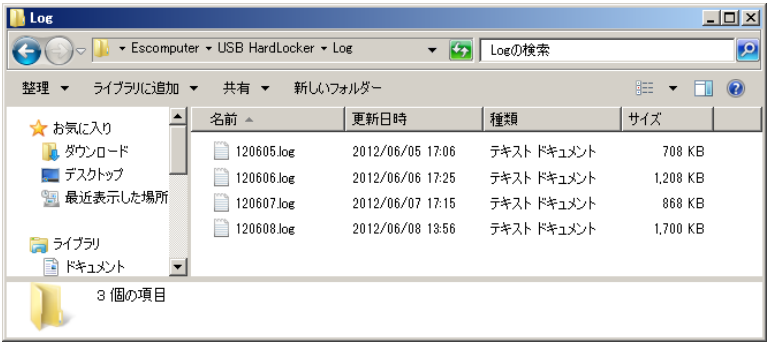
①「日付」 イベントの発生年月日を記録
②「時刻」 イベントの発生時刻を記録
③「種類」 「ログ設定」の「ログ取得機能」の各項目（「ログオンとログオフ」、「ハードウェアの追加と削除」、「ファイルアクセス」、「インターネットアドレス」、「キーボード」、「ウィンドウ」、「プロセス」、「USB HardLocker」）のいずれかが表示されます（ログ取得機能DLLを追加した場合は追加したものも表示対象となります）。
④「詳細」 イベントの詳細を記録

＜ログファイルについて＞
初期設定時は以下のフォルダーに保存されます（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」を開くか、エクスポートの処理を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。

ログファイル名はメッセージ形式の場合、以下のように自動的に命名されます。
例： 120608.log

120608	.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）。



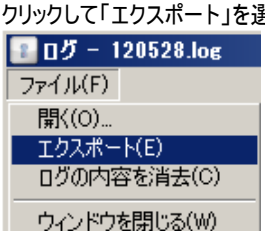
＜ログの保存と参照に関する注意事項＞

- ログはネットワーク共有フォルダーに保存することもできますが、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設定をしている場合、ネットワーク共有フォルダーをログの保存先にしないでください。ネットワークロックが動作時にログを記録できません。
- ネットワーク共有フォルダーに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、ログを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。

〇ログの内容を消去
クリックすると、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

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	ログ種類詳細	タイトル	パス1	パス2	URL
2	PC520	127.0.0.1	kanri	2012/1/21	11:51:04	ファイル操作	コピー		C:¥Users¥k	C:¥Users¥kanri¥Desk	
3	PC520	127.0.0.1	kanri	2012/1/22	11:51:03	ファイル操作	コピー		C:¥Users¥k	C:¥Users¥kanri¥Desk	
4	PC520	127.0.0.1	kanri	2012/1/22	11:51:03	ファイル操作	コピー		C:¥Users¥k	C:¥Users¥kanri¥Desk	
5	PC520	127.0.0.1	kanri	2012/1/22	11:51:03	ファイル操作	コピー		C:¥Users¥k	C:¥Users¥kanri¥Desk	
6	PC520	127.0.0.1	kanri	2012/1/22	11:51:03	ファイル操作	コピー		C:¥Users¥k	C:¥Users¥kanri¥Desk	

上図は MS 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（P57）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：

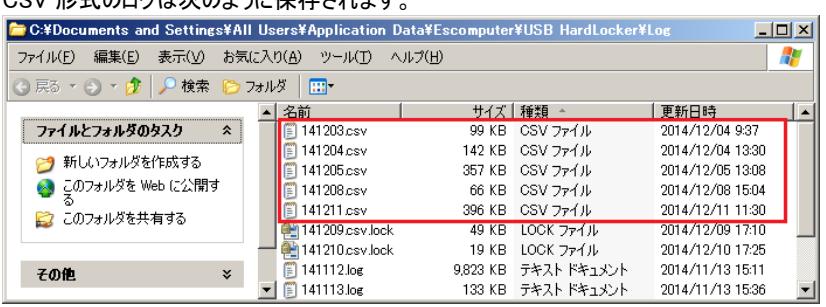
コンピュータ名,IPアドレス,ログイン名,鍵の名前,鍵の種類,VID,PID,SerialNo,年月日,時刻,ログ種類,ログ種類詳細,タイトル,パス1,パス2,URL,プリンタ名,プリンタIPアドレス,総ページ数,パラメーター,エラー値
PC520U,192.168.0.20,kanri,2012/2/7,8:40:45,ファイルアクセス
,,,SearchProtocolHost.exe,C:¥Users¥kanri¥Documents¥desktop.ini,,,,,,

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。

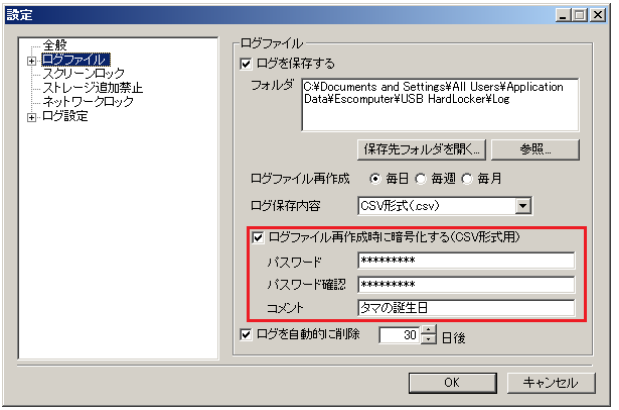


例： 141203.csv

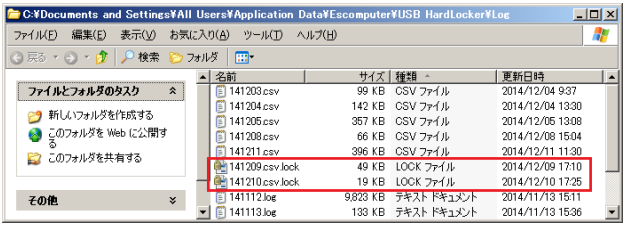
141203	.csv
日付(YYMMDD)	ファイル拡張子

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。



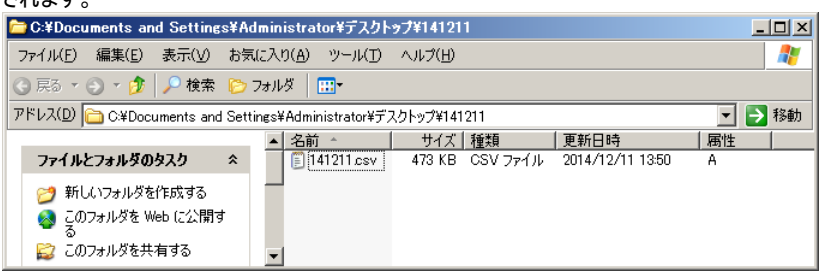
141209.csv.lock、141210.csv.lock　暗号化された CSV 形式のログ



＜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 4 Server』※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。 ※ Version 4.2.0以降がインストールされている必要があります。

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。



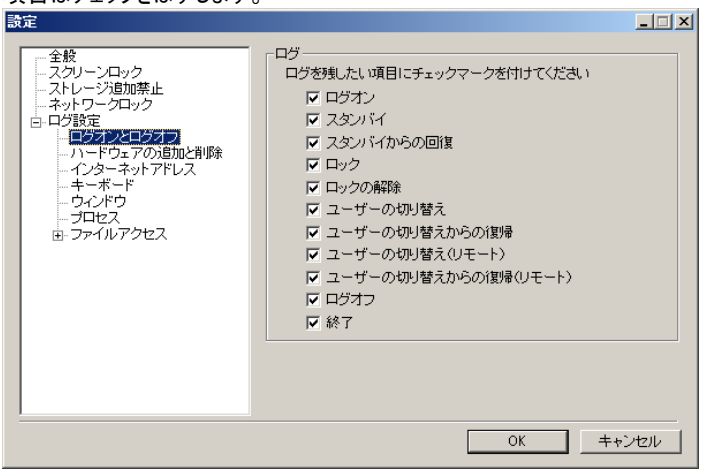
方法 B. 『USB HardLocker 4』がインストールされていない環境

『LB ファイルロック2』を使用して復号化します。
（暗号化されたログファイルを『LB ファイルロック2』にドラッグ＆ドロップします。）

第7節　　記録内容の詳細設定

1. ログオンとログオフ

ログオンとログオフについて、チェックした項目のログを記録します。ログに残したくない項目はチェックをはずします。



＜項目の説明＞

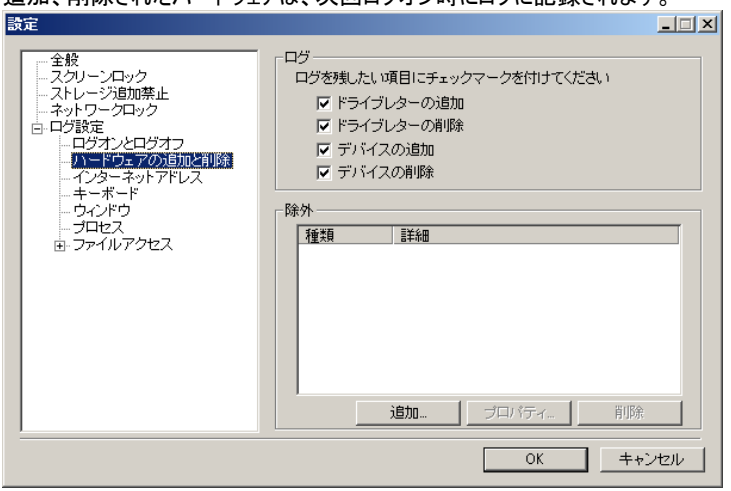
ログオン	コンピューターへのログオンを記録します。
スタンバイ	スタンバイモードへ切り替えを記録します。
スタンバイからの回復	スタンバイモードからの復帰を記録します。
ロック	コンピューターのロックを記録します。
ロックの解除	コンピューターのロックの解除を記録します。
ユーザーの切り替え	ユーザーの切り替えを記録します。
ユーザーの切り替えからの復帰	切り替えたユーザーから元のユーザーへの復帰を記録します。
ユーザーの切り替え(リモート)	ユーザーの切り替え(リモートコンピューターからのログオン)を記録します。
ユーザーの切り替えからの復帰(リモート)	切り替えたユーザー(リモートコンピュ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

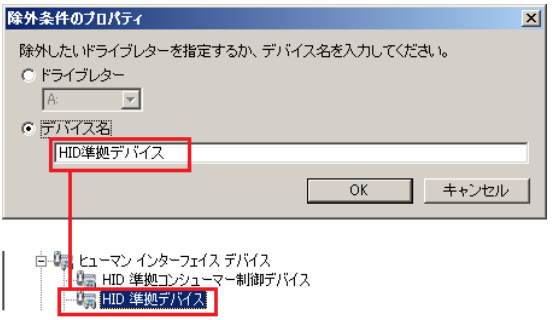
追加、削除されたハードウェアは、次回ログオン時にログに記録されます。



＜項目の説明＞

ドライブレターの追加	ドライブの追加をログに記録します（USB フラッシュメモリの装着等）。
ドライブレターの削除	ドライブの削除をログに記録します（USB フラッシュメモリの取り外し等）。
デバイスの追加	デバイスの追加をログに記録します。
デバイスの削除	デバイスの削除をログに記録します。
追加	ログ取得から除外したいハードウェア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	除外リストのハードウェア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。

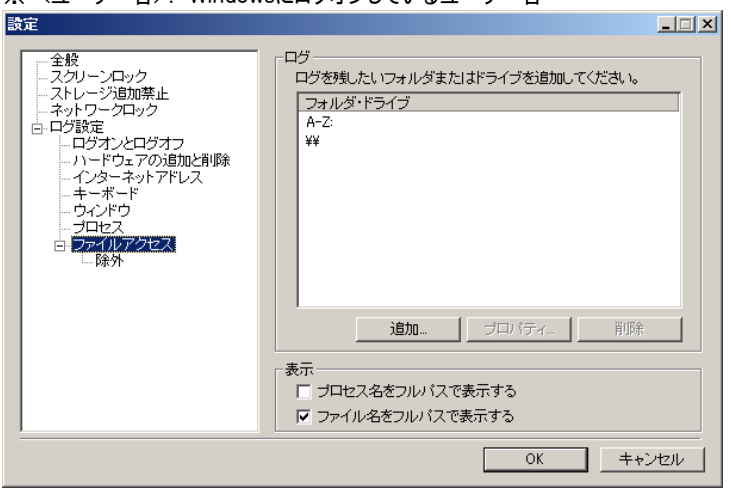
＜「追加」をクリックして表示される「除外条件追加」画面＞
例：　HID準拠デバイスを除外条件に追加



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。ここで指定したドライブレターは、ログに残らなくなります。
デバイス名	ここで指定したデバイスは、ログに残らなくなります。デバイス名はデバイスマネージャーで表示される名前を完全一致するように入力する必要があります。

3. ファイルアクセス
ファイルのアクセスを記録します。ログを残したいフォルダーまたはドライブを「追加」をクリックして指定します。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」を選択して設定することができます。

初期設定で指定されているフォルダー
¥Users¥<ユーザー名>¥Desktop¥
¥Users¥<ユーザー名>¥Documents¥
※ <ユーザー名>: Windowsにログオンしているユーザー名

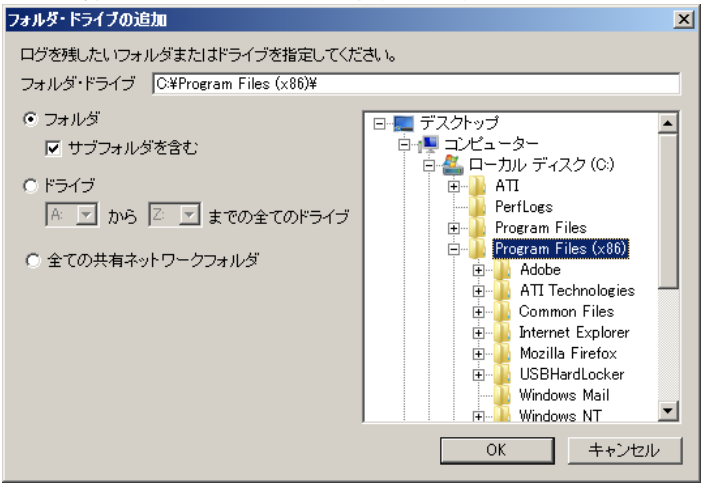


＜設定項目の説明＞

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	チェックす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。

＜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を記録します。

※ 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や相対パス、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）。

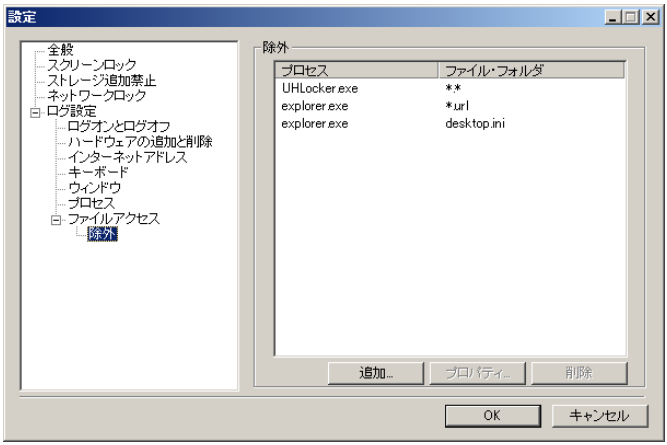
◇パス無しの例
sample.txt – ファイル名がsample.txtの全てのファイル
*.txt – 拡張子txtを持つ全てのファイル
a*.* – a で始まる全てのファイル
sample? – sample? の全てのファイル。 ?は任意の1文字

◇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

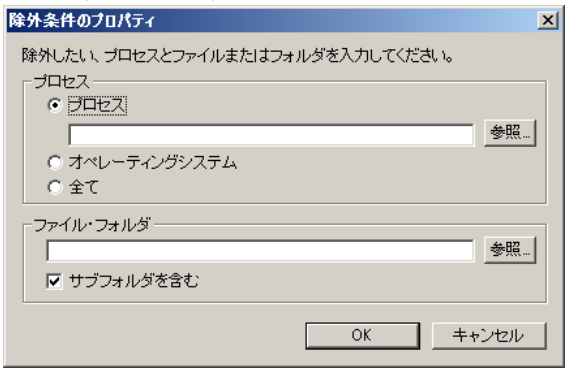
＜「除外」（ファイルアクセス）＞
ログに残したくないファイルアクセスは除外リストに追加します。



＜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。 ※　デフォルトで除外されているプロセス（explorer.exe）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＞

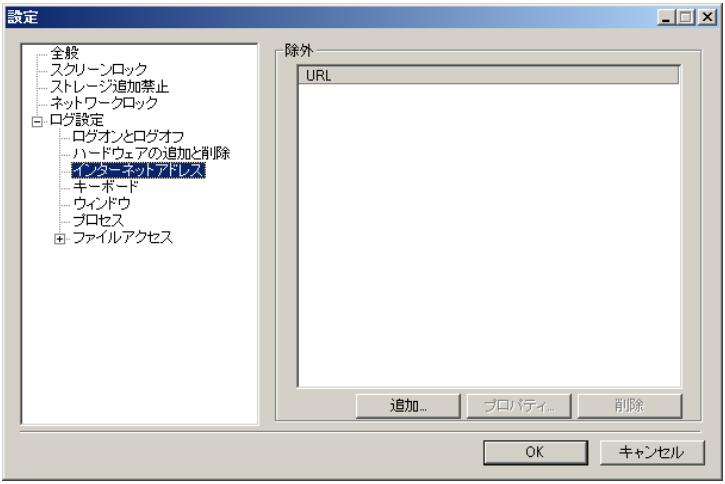


＜除外条件追加の説明＞

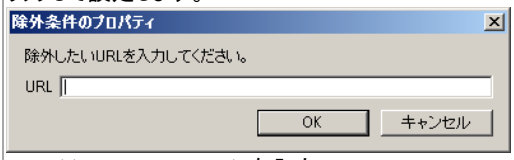
プロセス	参照をクリックして除外するプログラムのファイル名を追加します。
オペレーティングシステム	プロセスではなく、オペレーティングシステムによるファイルアクセスを指定します。「オペレーティングシステム」を選択する場合、同時に「ファイル・フォルダー」を指定する必要があります。
全て	全てのプロセスとオペレーティングシステムによるファイルアクセスを指定します。
ファイル・フォルダー	アクセスされるファイル名またはフォルダー名を入力します。 ※ ファイル名には、一括して指定するためのワイルドカードを使うことができます。ワイルドカードには、1 文字の置き換えに使用する「?」と、複数文字の置き換えに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

4. インターネットアドレス

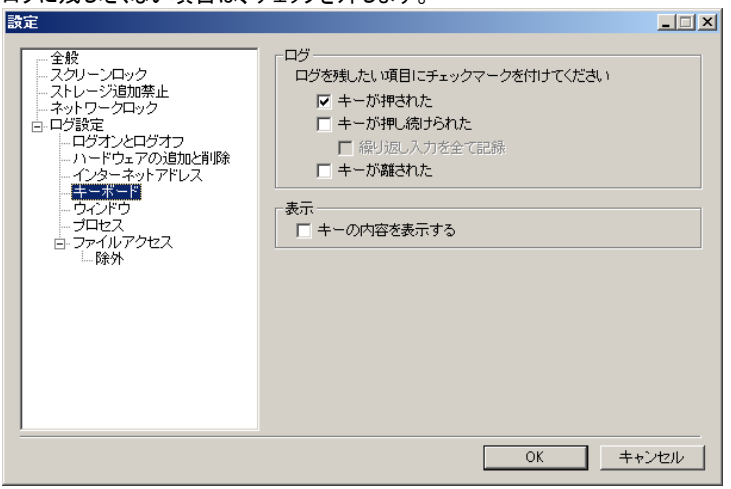
Internet Explorer を使用してアクセスしたURL(http、https)の記録に関する設定をします。



＜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」をクリックして設定します。  http://www.lifeboat.jp/　を入力 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 指定した URL のみアクセスが除外されます。
プロパティ	除外リストの URL 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。

5. キーボード（デフォルト設定はチェックOFF）
キーボード入力に関する設定をします。 デフォルトは、「キーが押された」のみチェックされています。項目に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。

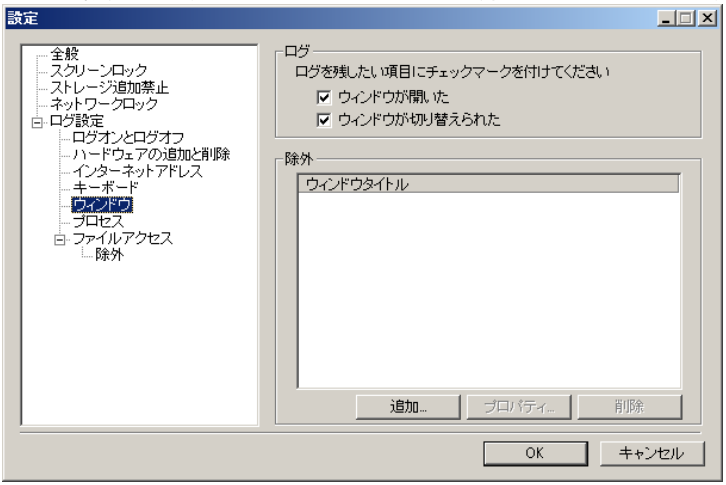


＜設定項目＞

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）。

6.　ウィンドウ

ウィンドウタイトルを監視し、「ウィンドウのオープン」、「ウィンドウの切り替え」に関するログを設定します。ログに残したくないウィンドウは、除外リストに追加します。

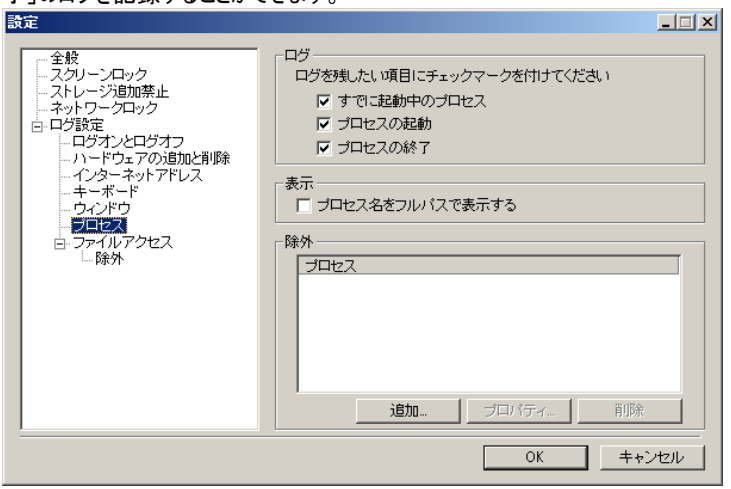


＜設定項目＞

ウィンドウが開いた	ウィンドウのオープンを記録します。
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。

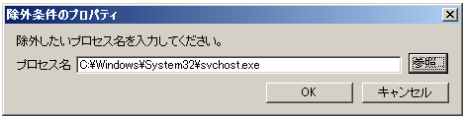
7. プロセス

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。



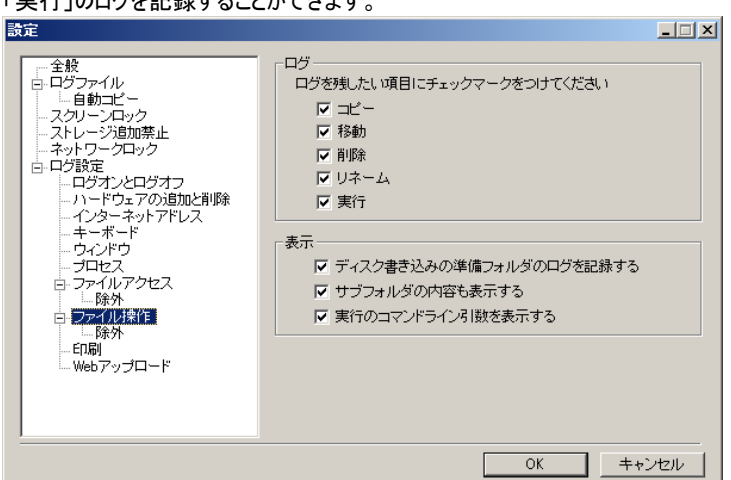
＜設定項目＞

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。

8.　ファイル操作

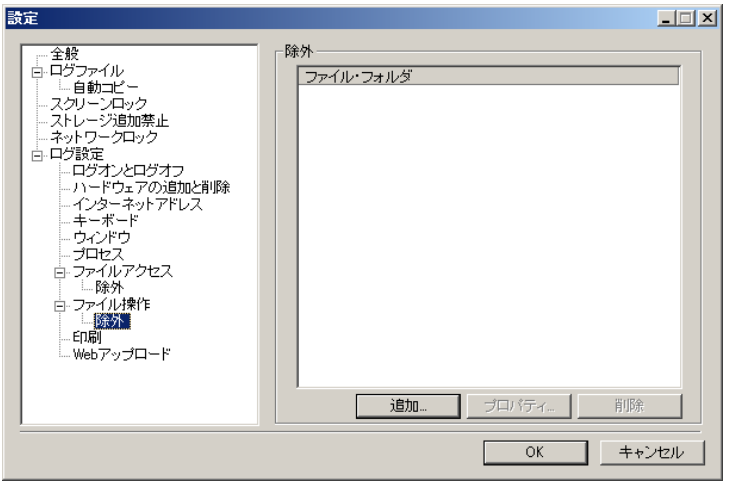
ファイル操作のログに関する設定をします。「コピー」、「移動」、「削除」、「リネーム」、「実行」のログを記録することができます。



＜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。
ディスク書き込みの準備フォルダのログを記録する	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。チェックをはずすと、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	実行ログの実行パラメーターが記録されます。

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

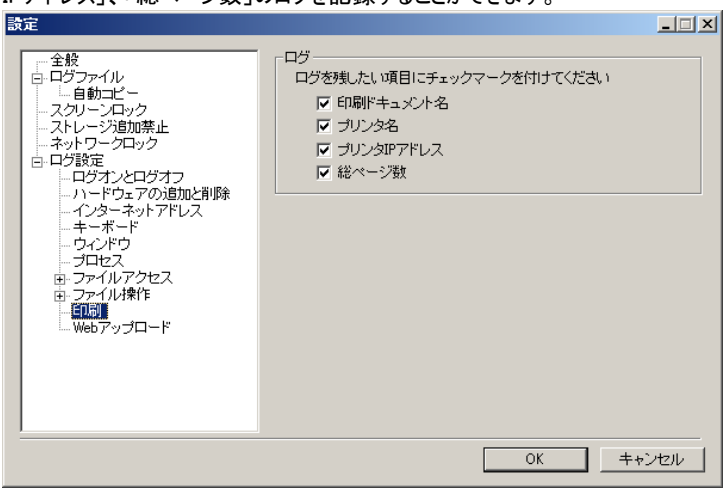


＜除外の設定項目＞

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」、「プリント名」、「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＞

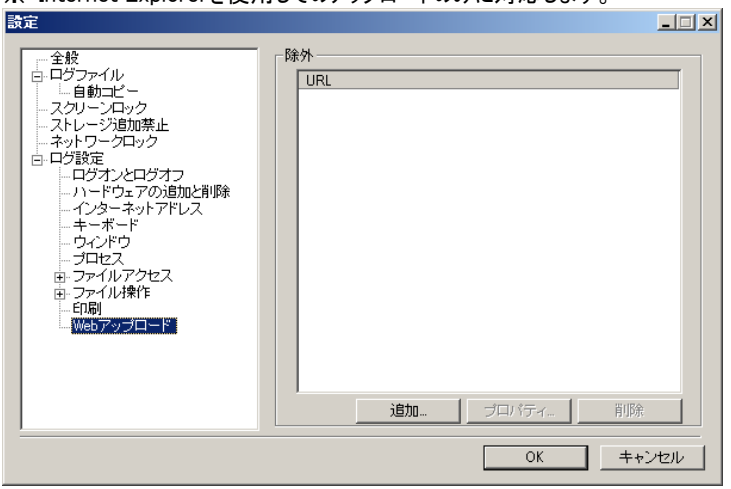
印刷ドキュメント名	印刷されたドキュメント名を記録します。
プリンタ名	印刷に使用されたプリンタ名を記録します。
プリンタ IP アドレス	ネットワークプリンタの IP アドレスを記録します。
総ページ数	印刷ドキュメントのページ数を記録します。

※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。

※ Internet Explorer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. USB HardLocker（※）

『USB HardLocker 4 Server』の以下の動作についてログを記録します。

※ この項目は他と異なり、ユーティリティの「設定」-「全般」で「ログを保存する」をチェックするとログが記録されます。

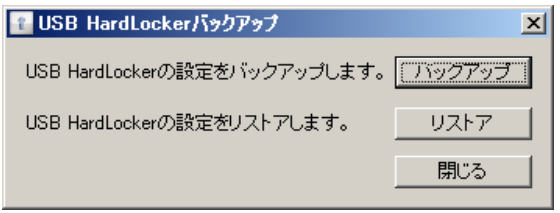
記録される内容：

「鍵の作成」、「鍵の削除」、「秘密領域の有効」、「秘密領域の停止」、「ストレージ追加禁止」、「ストレージ追加禁止の解除」、「コンピューターのロック」、「コンピューターのロックの解除」、「ネットワークロック」、「ネットワークロックの解除」

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 4 Server』の設定情報をバックアップするためのツールです。



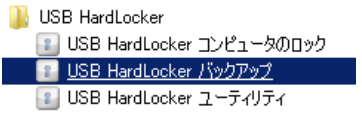
■主な機能
◎ 設定情報、秘密領域、ログのバックアップを取ることができます。
◎ バックアップした設定情報をリストアすることができます。

＜注意事項＞
- USB HardLocker for Server Version 3.0のバックアップをリストアすることもできますが、この場合にリストアできる内容は鍵の設定情報のみとなります。
  （ストレージ追加禁止、ネットワークロック、ログ記録は再設定が必要となります）
- バックアップを異なるOSがインストールされた他のPC上で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
  例） Windows Server 2003からWindows Server 2008 R2へ入れ替える場合等
  ※ 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。

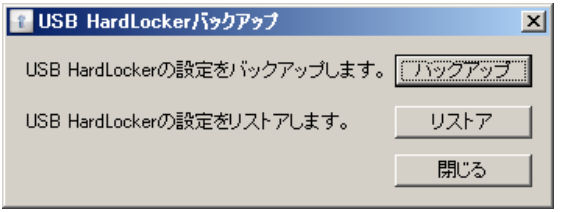
第2節　バックアップ

＜バックアップの手順＞

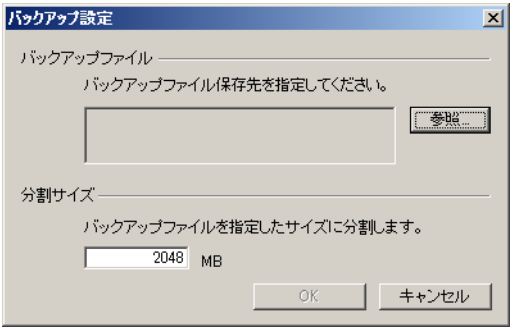
1. Windows の「スタート」から「USB HardLocker」-「USB HardLocker バックアップ」を選択します（Windows Server 2012 は Modern UI Style から「USB HardLocker バックアップ」を選択）。
   ※ 予め管理者権限で Windows にログオンしておく必要があります。
   ※ 予め管理者鍵をコンピューターに接続しておく必要があります。



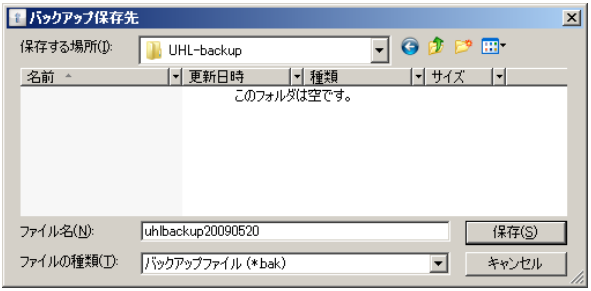
2. バックアップツールが起動するので「バックアップ」をクリックします。



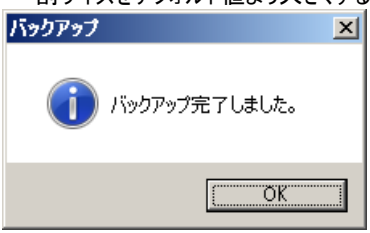
3. バックアップの保存先となるパスとファイル名を指定します。「参照」をクリックしてバックアップ作成先のパスとファイルを指定して「OK」をクリックしてください。



4. 保存先のパスとファイル名を指定して「OK」をクリックします。



5. 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（デフォルトは 2GB）。バックアップ保存先のファイルフォーマットによっては、分割サイズをデフォルト値より大きく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

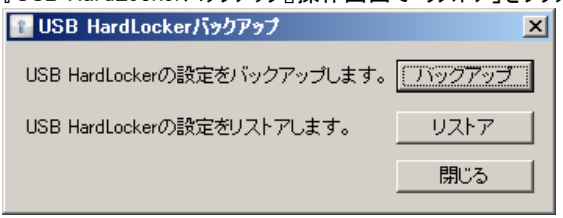
＜リストアの手順＞

『USB HardLocker 4 Server』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。

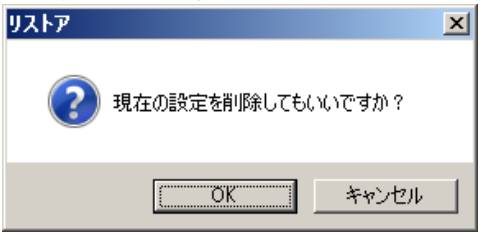
※ 予め管理者権限で Windows にログオンしておく必要があります。
※ 予め管理者鍵をコンピューターに装着しておく必要があります。

1. Windows の「スタート」から「USB HardLocker」-「USB HardLocker バックアップ」を選択します（Windows Server 2012 は Modern UI Style から「USB HardLocker バックアップ」を選択）。

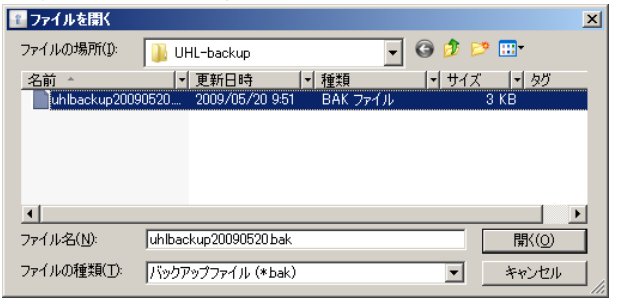
2. 『USB HardLockerバックアップ』操作画面で「リストア」をクリックします。



3. 既に鍵の設定が済んでいる環境では、「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。よろしければ「OK」をクリックしてください。



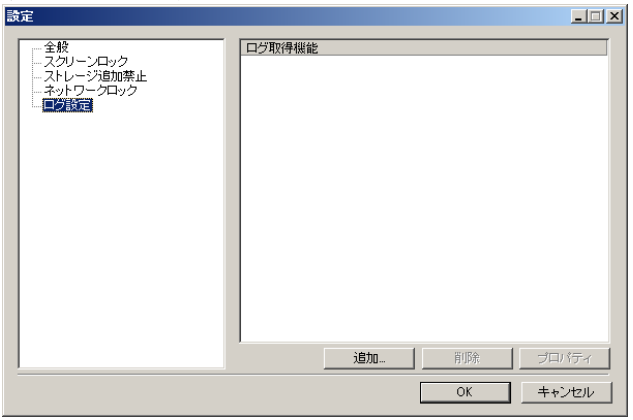
4. バックアップファイルを選択して「開く」をクリックするとリストアが実行されます。
※ バックアップ時に複数のアーカイブに分割している場合は、すべてのファイルが揃わないとリストアを実行できません。



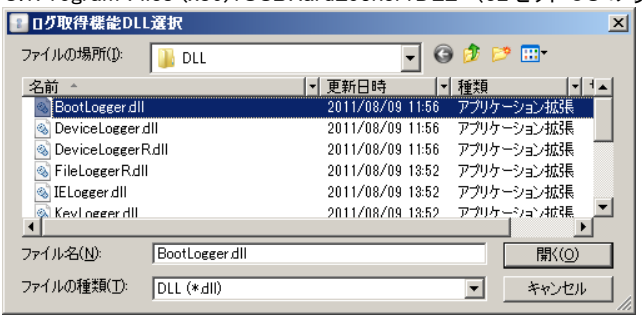
5. リストアが完了すると以下のメッセージが表示され、リストアされた内容に基づいて『USB HardLocker 4 Server』が動作します。管理者鍵が装着されていない場合、設定内容によってはスクリーンロックがかかります。

＜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¥USBHardLocker¥DLL （64 ビット OS の場合）
C:¥Program Files (x86)¥USBHardLocker¥DLL （32 ビット OS の場合）



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
KeyLoggerR.dll	キーボード
ProcessLogger.dll	プロセス
URLLogger.dll	インターネットアドレス
WindowTitleLoggerR.dll	ウィンドウ

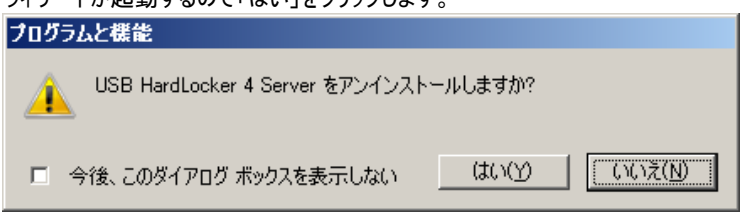
3. 上記 2.で BootLogger.dll を追加した場合、「ログオン」の項目が追加されます。
この操作を繰り返して、必用な項目の dll を追加していきます。

第6章　アンインストール

第1節　USB HardLocker 4 Serverのアンインストール

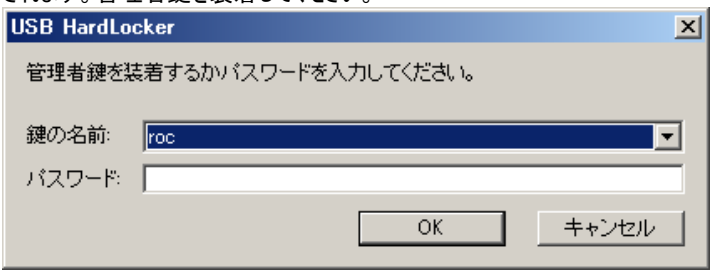
『USB HardLocker 4 Server』のアンインストールについて説明します。
※ 管理者権限で Windows にログオンしてから実行する必要があります。
※ アンインストールするには管理者鍵の認証をする必要があります。予め管理者鍵を装着した状態でアンインストールを開始することをお勧めします。
※ アンインストールを実行すると秘密領域およびそこに保存されたファイル、鍵の設定情報、ログファイルはすべて削除されます。

1. 「コントロールパネル」 - 「プログラムと機能」、「プログラムのアンインストール」から「USB HardLocker 4 Server」を選択します。
ウィザードが起動するので「はい」をクリックします。

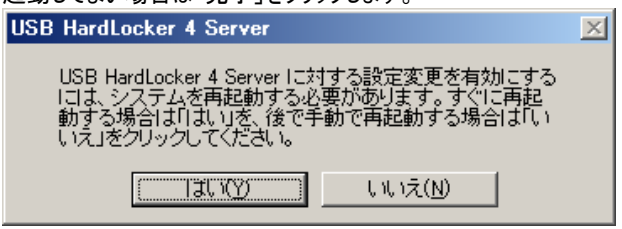


2. ユーザーアカウント制御の確認メッセージが表示されたら、「はい」をクリックします。

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。管理者鍵を装着してください。



4. ファイルの削除終了後「InstallShield Wizardの完了」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。



USB HardLocker 4 Server 利用ガイド

2014 年 12 月 22 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

Printed in Japan　　落丁、乱丁はお取替えいたします。

LIFEBOAT
a megasoft company