Network Controller

ユーザーズ・マニュアル

目　　次

ご利用いただけるシステム環境（システム要件）

HD 革命 /WinProtector Ver.6 with Network Controller（本マニュアルでは以降「Network Controller」といいます）の管理 PC としてご利用いただくには、次のコンピューターハードウェアおよびオペレーティングシステムが必要です。

コンピューターシステム環境

オペレーティングシステム（OS）（いずれも日本語版）	Windows 10 Creators Update（バージョン 1703）32bit/64bit 版 Windows 8.1 Update 32bit/64bit 版 Windows 7 SP1 32bit/64bit 版 Windows Server 2016 64bit 版 Windows Server 2012/2012 R2 64bit 版 ※ Windows RT/RT 8.1 には対応していません。 ※アドミニストレーター権限（管理者権限）が必要です。 ※ 2017 年 10 月 1 日現在の対応 OS となります。Windows 10 の大型アップデートについての最新情報は、弊社 Web サイトでご確認ください。 ※マイクロソフトがサポートを終了したオペレーティングシステムは、弊社製品のサポートも終了とさせていただきます。
コンピューター	上記の OS が稼働するコンピューター（PC/AT 互換機のみ） ※ Macintosh（Mac）には対応していません。
メモリー	Windows 10/8.1/7 64bit 版：4GB 以上（8GB 以上を推奨） Windows 10/8.1/7 32bit 版：2GB 以上 Windows Server 2016 64bit 版：4GB 以上（8GB 以上を推奨） Windows Server 2012/2012 R2 64bit 版：4GB 以上（8GB 以上を推奨）
CD/DVD ドライブ	DVD を読み込めるドライブ
ハードディスク SSD	100MB の空き容量（本製品のインストール用として）
モニター	画面解像度が 1,024 × 768 ピクセルのモニター
その他	データベースサーバーとして SQL Server 2012/2016 Express Edition FTP サーバーとして、Internet Information Service（IIS7 以上） 管理 PC およびクライアント PC には「.Net Framework 4.5」以上

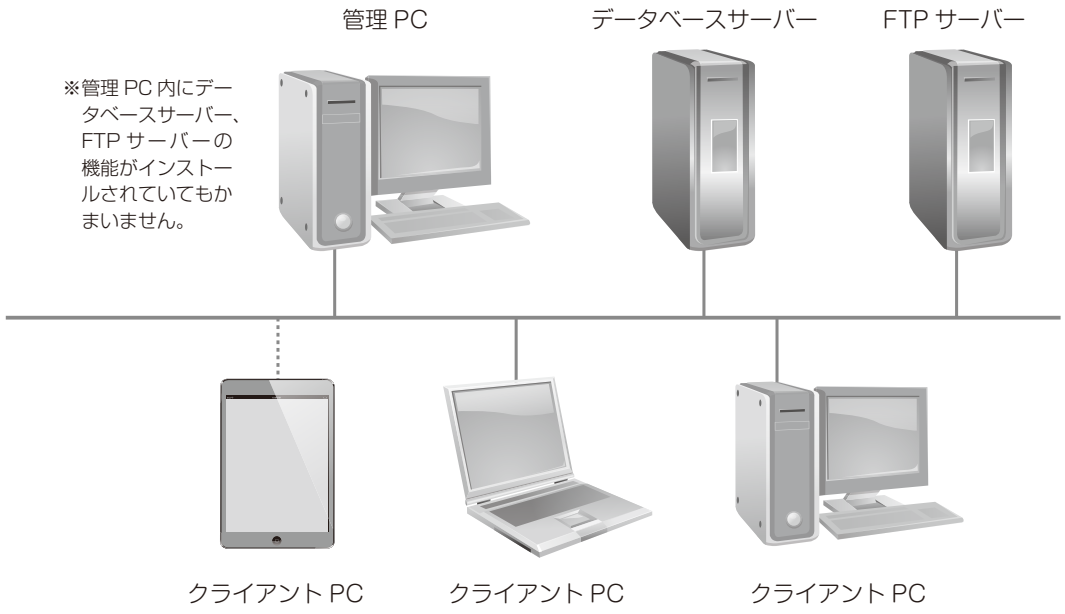
Network Controller について

Network Controller は、環境復元ソフト「HD 革命 /WinProtector」およびファイル抹消ソフト「HD 革命 /Eraser ファイル抹消」をリモート環境で制御することができるシステムです。その他にも、Network Controller では管理 PC 上で以下の機能が利用できます。

① PC のグループ管理……ネットワーク上の PC を一元管理することができます。
②電源管理……クライアント PC の電源オン／電源オフができます。
③ PC 操作……ファイルの送付やサイレントインストールを行うことができます。
④デバイスロック……マウス／キーボードや CD/DVD、USB メモリーのアクセス制御ができます。
⑤ファイル抹消……「HD 革命 /Eraser ファイル抹消」の機能でファイルを抹消できます。
⑥環境復元……「HD 革命 /WinProtector」の機能で環境復元（環境保護）ができます。
⑦連続実行機能……上記①～⑥の操作を組み合わせ処理できます。
⑧スケジュール実行……上記操作をスケジュール設定して実行できます。

Network Controller の構成

Network Controller は、管理する PC（管理 PC)、データベースサーバー、FTP サーバーおよび管理対象 PC（クライアント PC）で構成されます。



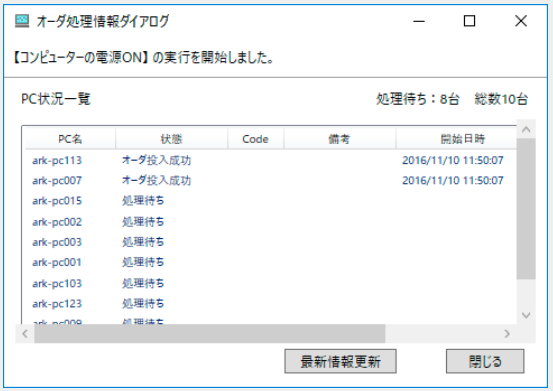
管理 PC の構成について

管理 PC は以下のプログラム（サービス）で構成されています。

① Network Controller
管理者が利用する GUI アプリケーションで、クライアント PC への処理依頼やスケジュール登録などを行うことができます。
②オーダー実行プログラム
タスクスケジューラに登録されたオーダーを、オーダー処理サービスに処理依頼を行うプログラムです。
③状態監視サービス
クライアント PC の状態を取得し、処理依頼したオーダーの結果を受け取る常駐型のサービスです。
④オーダー処理サービス
Network Controller からの処理を受け付け、対象となるクライアント PC に処理依頼を行う常駐型のサービスです。

Point

オーダーとタスク
Network Controller で、依頼する**1 つの処理を「オーダー」**といいます。ここでいう「処理」とは、シャットダウン、再起動、資料再配布、HD 革命 /WinProtector の保護開始などの動作を指します。処理の対象となる PC は 1 台、複数、または 1 つ以上のグループです。オーダーを、対象となる**個々の PC に割り当てた処理を「タスク」**といいます。
オーダーを実行すると、「オーダー処理情報ダイアログ」が表示され現在の状態を確認することができます。



クライアント PC の構成について

クライアント PC は以下のプログラム（サービス）で構成されています。

①クライアントエージェント
管理 PC からのオーダー受付をし、クライアント PC の状態を管理 PC に送信する常駐型のエージェントです。
②ＰＣ起動サービス
受け付けたオーダーを実行する常駐型サービスです。
③ PC 監視サービス
PC の状態を監視し変更があると、クライアントエージェントに変更報告を行う常駐型サービスです。
④ HD 革命 /WinProtector
クライアント PC に「HD 革命 /WinProtector Ver.7」がインストールされていると、環境復元（環境保護）を行うことができます。HD 革命 /WinProtector のバージョンが古い場合は正常に動作しませんので、Ver.7 がインストールされているか確認してください。
⑤ HD 革命 /Eraser ファイル抹消
クライアント PC に「HD 革命 /Eraser ファイル抹消」がインストールされていると、ファイル抹消を行うことができます。

注意事項・制限事項

Network Controller の使用開始に当たっての注意事項

・Windows の休止状態／サスペンド、スタンバイ／スリープなどになると正しく動作しない場合があります。管理対象の PC は、電源管理（電源オプション）で「コンピューターをスリープ状態にする」は「なし」としてください。
・セキュリティソフトウエアがインストールされている場合には管理 PC との通信がブロックされる場合があります。その場合はセキュリティソフトウエアのファイアフォールで、アプリケーションの許可設定をしてください。
・異なるサブネット間で管理する場合は、サブネット間にあるルータで利用する通信ポートの送受信を許可してください。デフォルト値は、10001, 10002, 10003 番ですが、別の番号での運用も可能です。その他、FTP サーバー（21 番）の送受信の許可が必要です。
・異なるサブネット間でWOLを利用するには、ルータで BroadCast (IPv4 の場合) を許可する必要があります。
・IPv6 での通信機能は含んでいますが、サポート対象外となります。IPv6 運用でも、IPv4 との相互運用している場合などは運用方式がいくつかあるので、導入についてはお客様環境で動作検証などを実施する必要があります。

デバイスロック機能における注意事項

・マウス / キーボードロック時に、クライアント PC で CTL+ALT+DEL キーを押すと、タスクマネージャが起動します。ただし、タスクマネージャの EXE を監視しており、起動したらそのプロセスを終了します。起動から終了まで多少のタイムラグがあります。
・マウス/ キーボードおよびデスクトップのロックは、ログアウト (シャットダウンも）されると解除されます。
・USB および CD/DVD のアクセス制御は、ログアウト（シャットダウンも）しても有効です。利用を再開するには、アクセスの許可が必要です。なお、設定／解除を行っても有効にならない環境がありますので、そのときはクライアント PC の再起動を行ってください。
・アクセス制御が可能なデバイスは、Media Transfer Protocol（MTP）規格で通信を行うデバイスとなります。そのため、Media Transfer Protocol（MTP）規格で通信を行うデバイスであれば、スマートフォン（スマホ）のほかにも、タブレットやデジタルオーディオプレイヤーもアクセス制御が可能となります。ただし、iPhone や iPad などの iOS デバイスには対応していません。

「HD 革命 /WinProtector」機能を使用する場合の注意事項

・対応ファイルシステムは NTFS と FAT32 となります。仮想ディスク（.VHD）をマウントしたドライブには対応していません。
・暗号化機能は、「BitLocker」に対応しています。「BitLocker」以外の暗号化ソフトウェアとの併用はできません。なお、「BitLocker」により暗号化されたディスクに対して保護を行う場合、「除外フォルダ（ファイル）の設定」を行うことはできません。
・Network Controller の「WinProtector 詳細設定」画面では、「リアルモードから保護を開始する」と「継続保護の設定」は選択できません。クライアント PC で直接設定を行うことは可能です。

・保護するドライブに断片化（フラグメンテーション）やエラーがある場合、レジストリの書き込みエラーや自動ログインの失敗、ブルースクリーンなどの現象が発生します。運用を開始する前に、クライアント PC の「エラーチェック」や「最適化とデフラグ」を行うことを推奨します
・保護を行うドライブは、「一時ファイル」の作成を行うために最低 4GB の空き容量が必要です。空き容量不足により「一時ファイル」を作成できない場合は、保護を行うことができません。一般的に「一時ファイル」は 10 ～ 15GB 程度の容量を指定することが推奨されますので、それ以上の空き容量を確保してください。なお、「一時ファイル」の保存先は保護を行うドライブとは別のドライブに指定することができます。
・「アップデート連携」で、WSUS サーバーの設定を行うと、クライアント PC の Windows グループポリシーにおける WSUS サーバーの設定が変更されます。そのため、HD 革命 /WinProtector を介さない Windows Update を行う場合も、設定した WSUS サーバーに接続しにいくようになります。また、WSUS サーバーの設定をしたままクライアント PC の HD 革命 /WinProtector をアンインストールしてもグループポリシーの WSUS サーバーの設定は残ったままとなります。
・「アップデート連携」で PROXY サーバーの設定を行う場合、Windows 10 の環境では認証つきプロキシは指定できません。

「HD 革命 /Eraser ファイル抹消」機能を使用する場合の注意事項

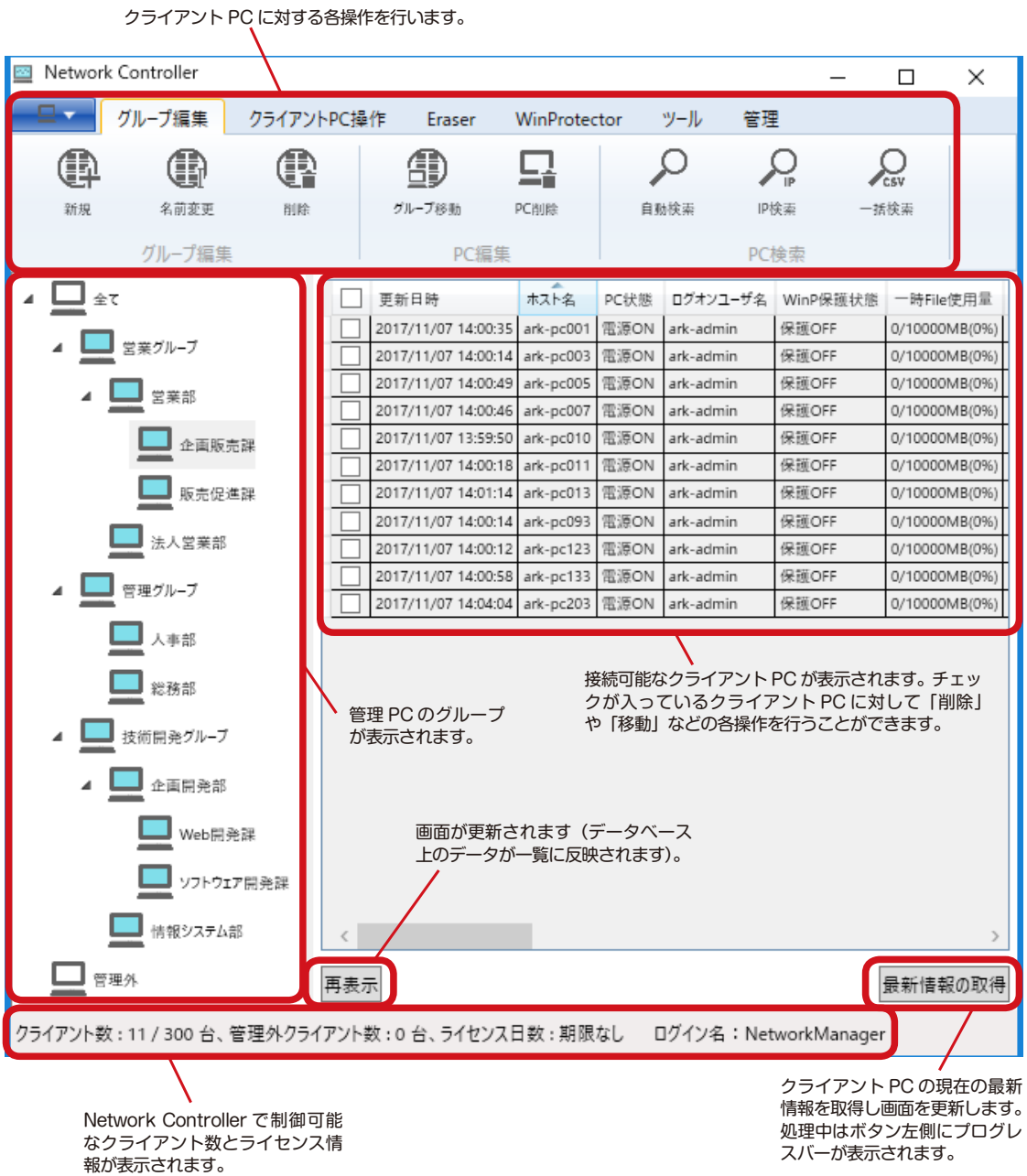
・ファイルを誤って抹消しないように、抹消前に必ず抹消してはいけないファイルが含まれていないかどうかを確認してください。
・抹消時間はクライアント PC のコンピューター環境や選択した抹消方式によって異なります。ファイルの容量、ハードウェアの速度によっては抹消に大変時間がかかることがあります。
・対応ファイルシステムは、NTFS、FAT32（1 セクターのバイト数が 512 バイトのみ）となります。FAT12、FAT16、exFAT など、他のファイルシステム上のファイルを抹消することはできません。
・ダイナミックディスク上のファイルを抹消することはできません。
・512 バイトエミュレーションを行っていない 4K セクター（4K ネイティブ）フォーマットのハードディスク上のファイルを抹消することはできません。
・NTFS の機能（代替データストリーム、リパースポイント、スパースファイル）が施されたファイルは抹消できません。
・暗号化されたファイルは抹消できません。
・他のアプリケーションによって使用中（ファイルが開かれた状態）のファイルを抹消することはできません。
・ネットワークドライブ上のファイルは抹消できません。

Network Controller 運用に際しての注意事項

・Network Controller を使用する環境において、データベースの定期的なバックアップを推奨します。
・資料配布などに FTP サーバーを利用していますが、基本的に FTP サーバーにアップしたファイルは削除していません。よって、利用可能なハードディスク容量が少ない場合はファイルの整理をする必要があります。ただし、オーダーやタスクを再実行する場合において、FTP サーバーに対象となるファイルがないとエラーとなりますので注意してください。
・スケジュール実行は、Windows タスクスケジューラで行っています。1 度しか実行しない場合も Windows タスクスケジューラに登録されています。これらは、「ツール」タブ→「作業履歴」と選択し、「オーダー一覧」に登録されたオーダーを右クリック→「スケジュール削除」と選択することで削除が可能です。

Network Controller のメイン画面

Network Controller は、クライアント PC の状態を表示し、各操作を一元管理することができます。本マニュアルでは以降「メイン画面」といいます。



グループ編集（「グループ編集」タブ）

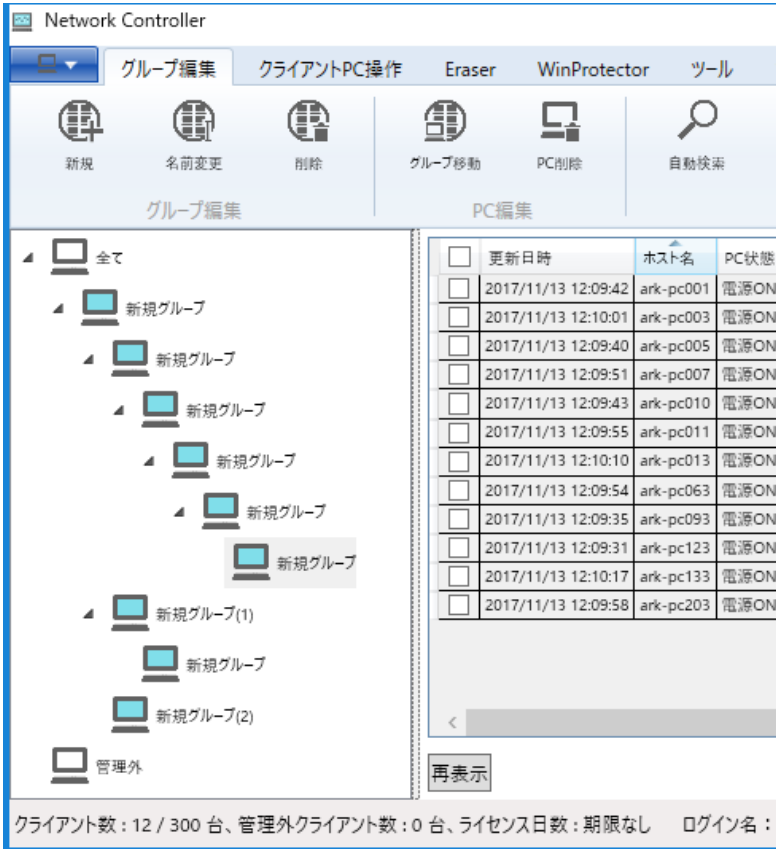
「グループ編集」タブでは、クライアント PC が所属するグループの作成や、クライアント PC の削除などの操作を行うことができます。

グループ編集

■新規

クライアント PC が所属する新しいグループを作成します。

グループはメイン画面左側のペインにツリー表示されます。グループは 7 階層まで作成できます。

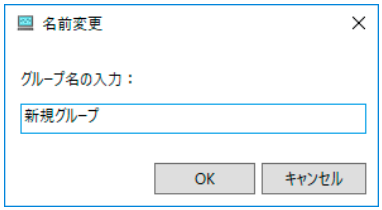


Point

12 ページのいずれかの方法でクライアント PC を追加すると、最初に管理外の下に入ります。管理外に登録されたクライアント PC を作成したグループに移動（11 ページ）することで操作ができるようになります。

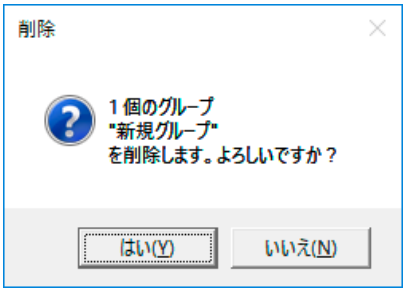
■名前変更

登録されているグループ名を変更できます。次の画面で新しいグループ名を入力します。



■削除

メイン画面右側のペインで削除したいグループを選択して「削除」をクリックすると、次の画面が表示されます。グループ名が表示されますので、削除するグループに間違いがないか確認してください。「全て」と「管理外」は削除できません。



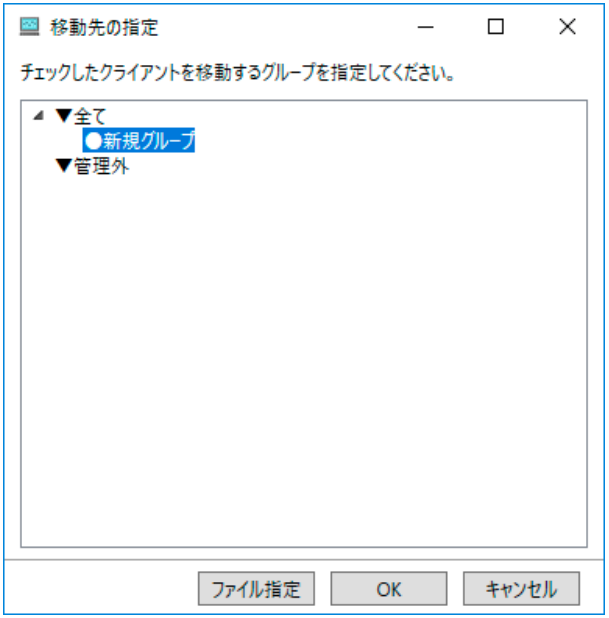
Point

グループにクライアント PC が登録されている場合は、グループを削除できません。クライアント PC を別のグループに移動するか、管理外に登録してから削除を行うようにしてください。
また、削除するグループの下層にグループが存在すると、同様に削除ができません。下層のグループを下から順に削除してください。

PC 編集

■グループ移動

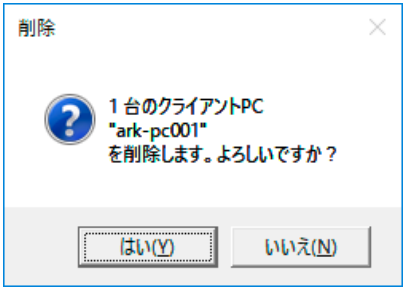
任意のクライアント PC を別のグループに移動できます。メイン画面右側のペインで移動したいクライアント PC を選択し、次の画面で移動先のグループを指定します。また、編集した CSV ファイルを指定して移動することもできます。



■ PC 削除

メイン画面右側のペインで削除（所属を解除）する PC を選択して「PC 削除」をクリックすると、次の画面が表示されます。

PC 名が表示されますので、削除するクライアント PC に間違いがないか確認してください。



PC 検索

■自動検索

ネットワークを検索し、接続可能なクライアント PC を検索します。クライアント PC の数が多い場合は、すべてのクライアント PC の情報が登録されるまで時間がかかる場合があります。

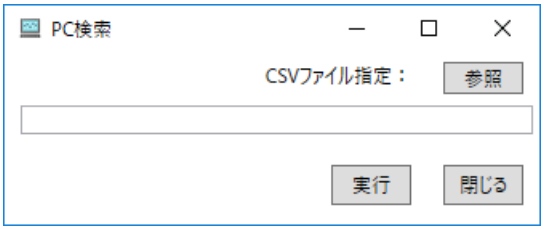
自動検索を行うクライアント PC は、BroadCast が届くネットワーク内にあることが条件となります。

■ IP 検索

IP を指定して PC を検索することができます。次の画面で IP を入力してください。

■一括検索

あらかじめクライアント PC の IP 番号が記載された CSV ファイルを作成しておくことで、クライアント PC を一括で登録することができます。



CSV ファイルの書式

グループ移動および一括検索で指定する CSV ファイルは以下の書式で作成します

1 フィールド目　IP アドレス（IPv4）
2 フィールド目　MAC アドレス
3 フィールド目　グループ名

例）192.168.0.1,A1B2C3D4E5F6, アーク学校 /1 年生 /1 組

〈注意事項〉

※フィールド間は「, 」（カンマ）区切りとなります。
※MACアドレスは、HEX表示で「-」（ハイフン）なしの12文字となります。
※グループ名は、「全て」以下からの絶対パスを区切り文字「/」で記載します。
※「管理外」グループへの移動はできません。
※「グループ移動」の場合には、移動対象のPCの一致条件はIPアドレスを優先し、IPアドレスが未記入の場合に、MACアドレスで検索します。「一括検索」の場合は、MACアドレスは必須となります。
※ CSV ファイルに記載するグループ名は既に登録されているグループとなり、未登録のグループ名は処理の対象外となります。
※ DHCP 環境では IP 番号が変更される場合があるので、登録が正しくできない場合は変更された IP 番号を CSV ファイルに記入してください。
※ NIC が複数ある PC の場合には、MAC アドレスも NIC ごとに存在するので、MAC アドレスが変更されることがあります。自動振り分けを行う場面で設定されている MAC アドレスを CSV ファイルに記入してください。

クライアント PC 操作（「クライアント PC 操作」タブ）

「クライアント PC 操作」タブでは、クライアント PC の電源管理、メッセージ送信、デバイスロックなどクライアント PC を管理する上で必要な機能が集約されています。

PC 電源操作

■電源 ON

メイン画面で選択したクライアント PC の電源を ON にします。クライアント PC は、Wake On LAN（WOL）機能に対応して BroadCast が届くネットワーク内にあることが条件となります。その他の注意事項は 6 ページを参照してください。

■シャットダウン

メイン画面で選択したクライアント PC をシャットダウンします。

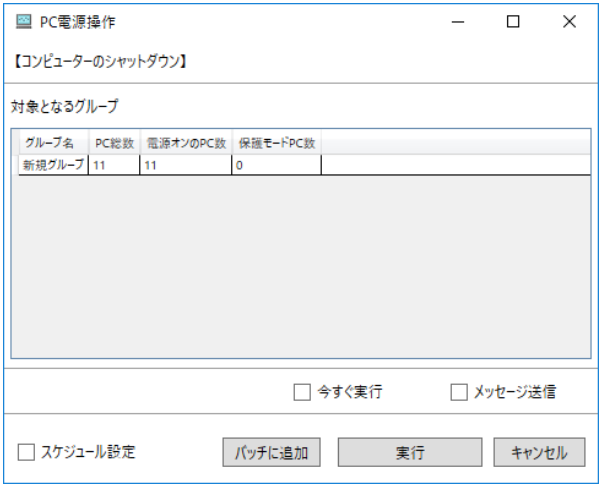
■再起動

メイン画面で選択したクライアント PC を再起動します。

■強制ログオフ

メイン画面で選択したクライアント PC を強制的にログオフ（サインアウト）します。

※上記の各 PC 電源操作実行時には、下の画面が表示されます。



Point

「今すぐ実行」オプション

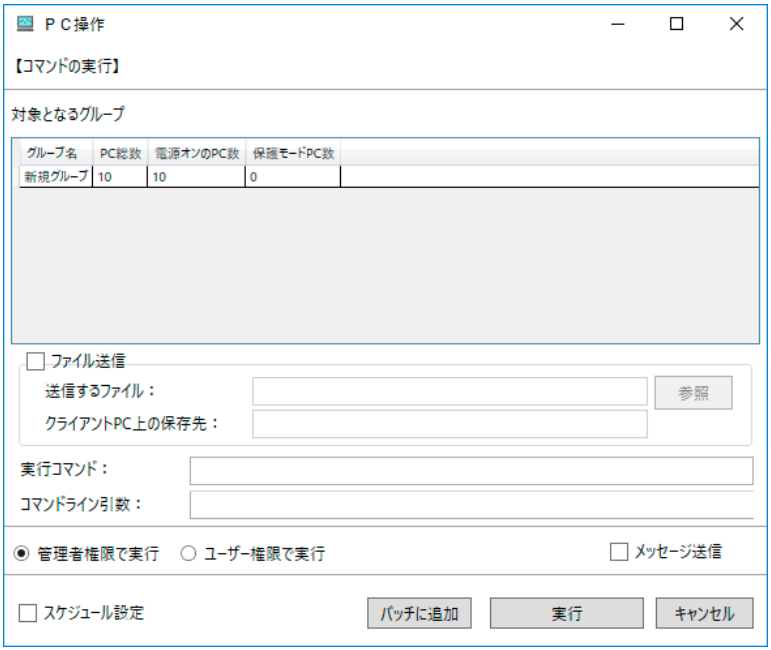
クライアント PC は、１つのオーダーが終了してから次のオーダー処理をしていますが、前のオーダーが実行中または待機中であると、次のオーダーを実行できません。クライアント PC 操作タブの「シャットダウン」または「再起動」には、「今すぐ実行」オプションがあり、実行中や待機中のオーダーを無視して処理を実行することができます。オーダーの応答がないような場合に選択してコンピューターを一度再起動してください。

なお、「今すぐ実行」オプションを選択して「シャットダウン」または「再起動」を行うと、処理中や待機中のオーダーもキャンセルされてしまいますので注意が必要です。

PC 操作

■コマンド実行

メイン画面で選択したクライアント PC をコマンドラインにより操作します。次の画面が表示されますので、実行する操作を指定します。ファイルを送信してそのファイルを実行することもできます。



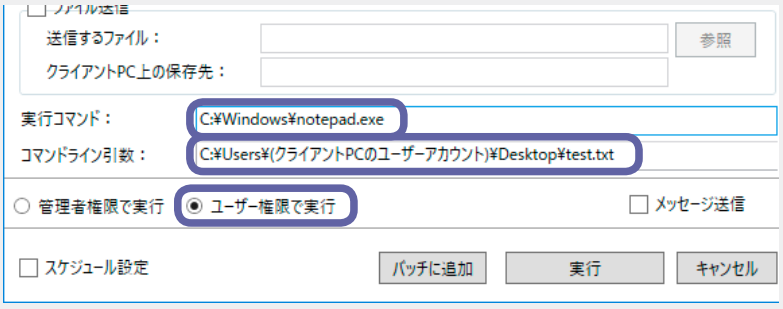
Point

コマンド実行の例

「コマンド実行」では、例えばインストール用の実行ファイルをクライアント PC に送信し、サイレントインストールを行うようなことができます。クライアント PC で実行するコマンド（アプリケーション）が管理者権限を必要とする場合は、「管理者権限で実行」を選択してください。

それ以外にも、クライアント PC でメモ帳を起動してテキストファイルを開く、などを実行することも可能です。コマンド実行を行うには、以下の例を参考にしてください。

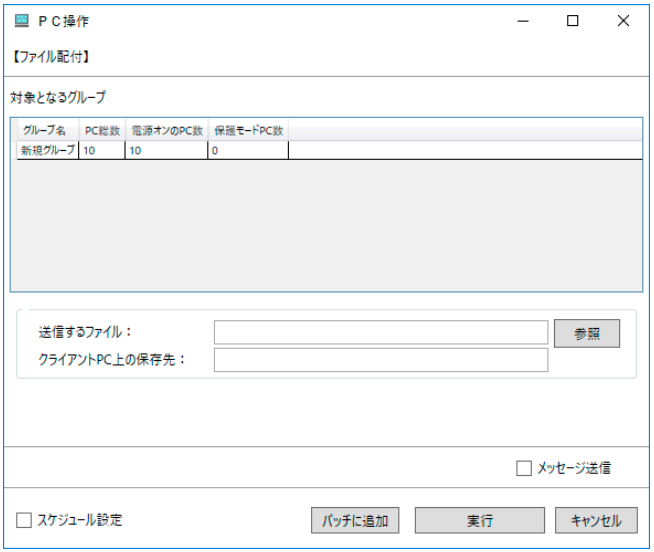
（例）「ユーザー権限」でメモ帳（notepad.exe）を起動してテスクトップの「test.txt」を開く



コマンド実行を行う場合、クライアント PC はいずれかのユーザーでログオンした状態で実行してください。
また、実行する権限は、通常「ユーザー権限で実行」を選択してください。
「管理者権限で実行」は、インストーラーやアップデータなどを実行する場合において選択してください。

■資料配付

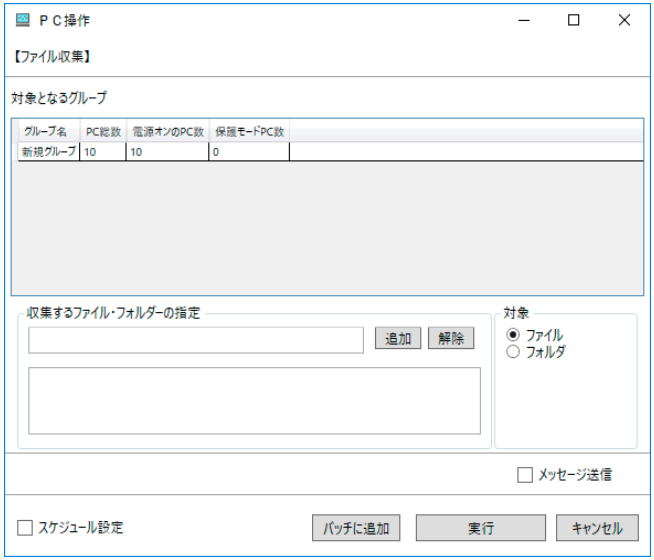
メイン画面で選択したクライアント PC に対してファイルを配布します。「クライアント PC 上の保存先：」は、フルパスで入力してください。



■資料収集

メイン画面で選択したクライアント PC 上にある任意のファイル、フォルダーを収集します。

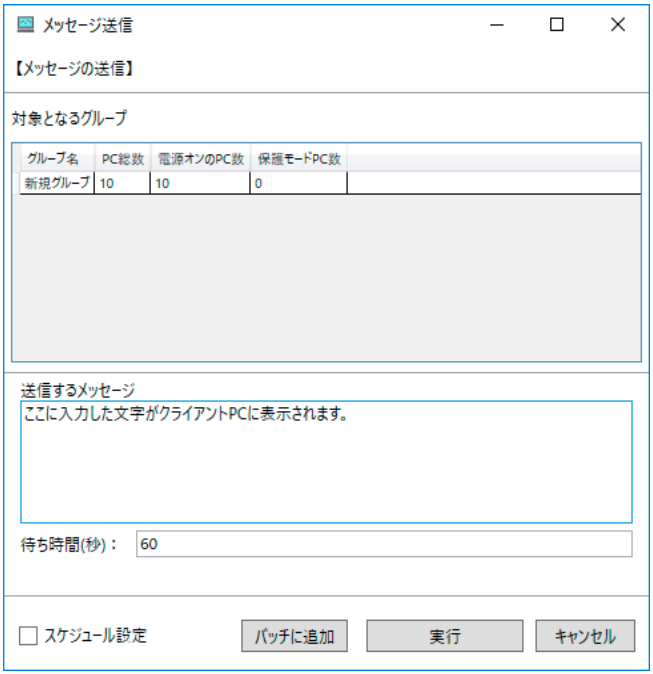
収集するファイルは、FTP サーバーに保存されます。「収集するファイル・フォルダーの指定」はフルパスで入力してください。なお、フォルダーを指定した場合は、指定フォルダー直下の全てのファイルがアップロード対象となります。FTP サーバーからファイルをダウンロードするには、54 ページの操作を行ってください。



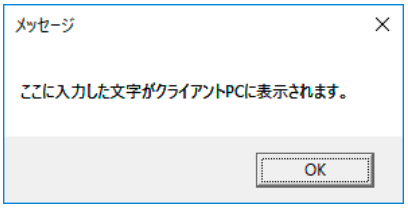
■メッセージ

メイン画面で選択したクライアント PC に対してメッセージを送信します。

「送信するメッセージ」欄に入力した文字が、クライアント PC においてメッセージウィンドウで表示されます。



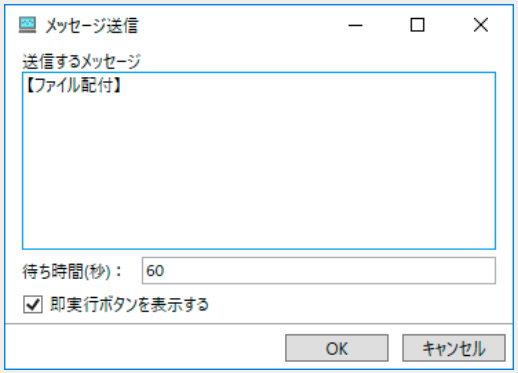
クライアント PC には次の画面が表示され、指定した秒数が経過すると自動的に閉じます。



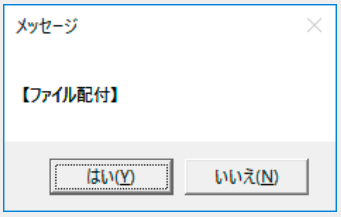
クライアント PC に表示されるメッセージウィンドウ

各操作画面での「メッセージ送信」

各操作画面で「メッセージ送信」にチェックを入れると次の画面が表示されます。
この画面では、メイン画面で「メッセージ」をクリックしたときと同様にクライアント PC にメッセージを表示します。

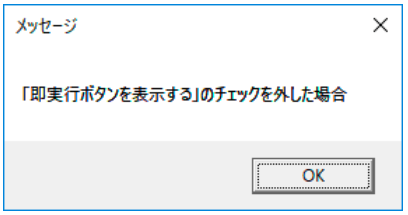


「即実行ボタンを表示する」にチェックが入っている場合、クライアント PC には選択式のメッセージウィンドウが表示され、「はい」をクリックするとすぐに指定した動作が行われます。
例えば、「資料配付」を実行している場合は、「はい」をクリックすると指定した場所にすぐにファイルが送信され、「いいえ」をクリックすると「待ち時間」で指定した秒数が経過してからファイルが送信されます。



Point

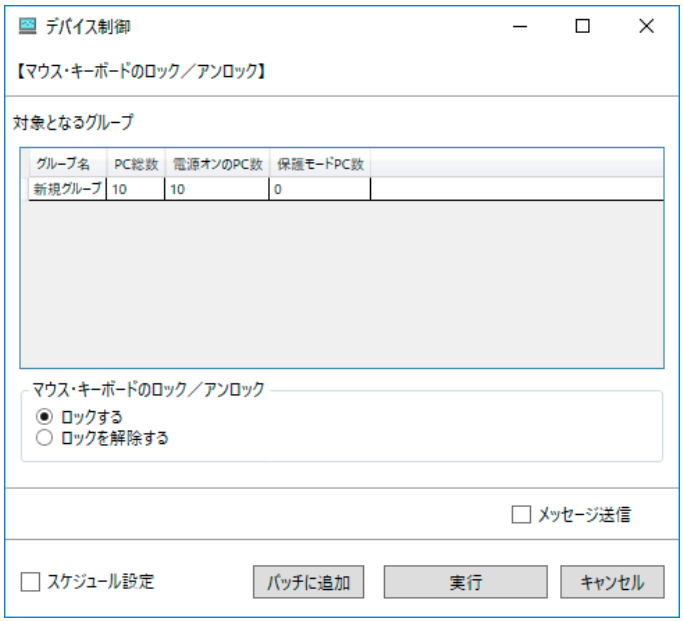
「即実行ボタンを表示する」のチェックを外した場合は、選択式のメッセージではなく「OK」ボタンのみとなります。



デバイスロック

■マウス／キーボード

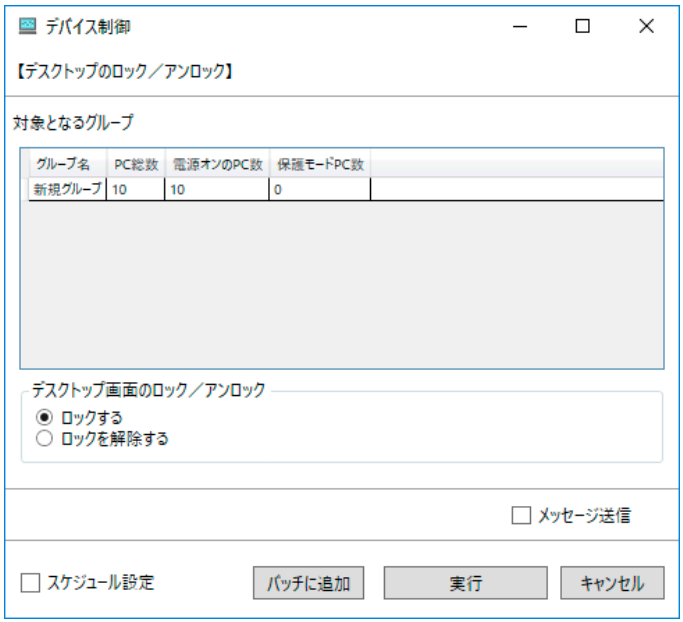
メイン画面で選択したクライアント PC のマウスとキーボードをロックして入力ができないようにします。



キーボードがロックされた状態であっても「Ctrl」＋「Alt」＋「Delete」」キーは無効になりません。

■デスクトップ

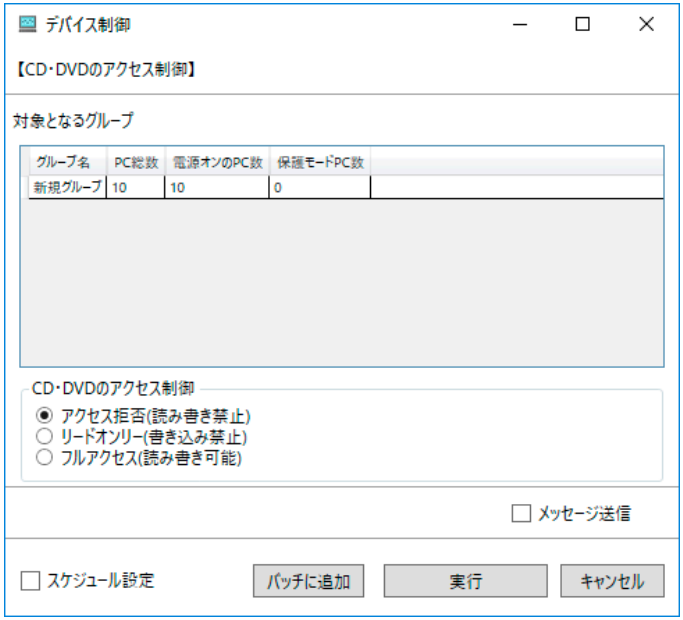
メイン画面で選択したクライアント PC のデスクトップ画面をロックして入力ができないようにします。



最前面に表示する設定のウィンドウは、ロックされた状態であっても表示されたままとなります。

CD/DVD

メイン画面で選択したクライアント PC の CD/DVD ドライブの制御を行います。



Point

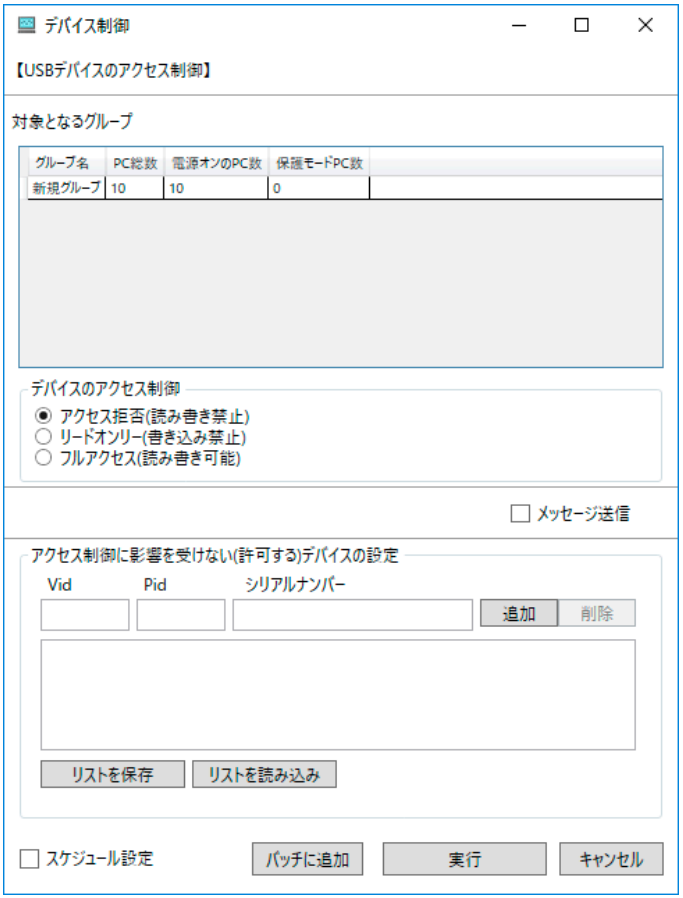
クライアント PC の状態を確認

各クライアント PC に対するデバイスロックの状態や、後述の「HD 革命 /WinProtector」における保護の状態はメイン画面で確認することができます。クライアント PC の設定を変更しても、すぐにメイン画面に状態が反映されないことがありますので、右下の「最新の情報に更新」ボタンを押して情報を更新してください。

更新日時	ホスト名	PC状態	ログオンユーザ名	WinP保護状態	一時File使用量	USB	MTP	CD/DVD	Mouse/Keyboard	Desktop	アン
2016/11/07 11:39:31	ark-pc001	電源ON	ark	保護OFF	0/10000MB(0%)	Read,Write	Read,Write	Read,Write	Lock/Lock	-	カス
2016/11/07 11:39:25	ark-pc002	電源ON	ark	保護OFF	0/10000MB(0%)	Read,Write	Read,Write	Read,Write	Lock/Lock	-	カス
2016/11/07 11:39:50	ark-pc003	電源ON	ark	保護OFF	0/10000MB(0%)	Read,Write	Read,Write	Read,Write	Lock/Lock	-	カス
2016/11/07 11:39:30	ark-pc007	電源ON	ark	保護OFF	0/10000MB(0%)	Read,Write	Read,Write	Read,Write	Lock/Lock	-	カス
2016/11/07 11:39:34	ark-pc009	電源ON	ark	保護OFF	0/10000MB(0%)	Read,Write	Read,Write	Read,Write	Lock/Lock	-	マカ
2016/11/07 11:40:04	ark-pc015	電源ON	ark	保護OFF	0/10000MB(0%)	Read,Write	Read,Write	Read,Write	Lock/Lock	-	Sym
2016/11/07 11:39:47	ark-pc103	電源ON	ark	保護OFF	0/10000MB(0%)	Read,Write	Read,Write	Read,Write	-/-	Lock	Sym
2016/11/07 11:40:37	ark-pc113	電源ON	ark	保護OFF	0/10000MB(0%)	Read,Write	Read,Write	Read,Write	-/-	Lock	ウイル
2016/11/07 11:39:43	ark-pc123	電源ON	ark	保護OFF	0/10000MB(0%)	Read,Write	Read,Write	Read,Write	-/-	Lock	マカ
2016/11/07 11:40:08	ark-pc133	電源ON	ark	保護OFF	0/10000MB(0%)	Read,Write	Read,Write	Read,Write	-/-	Lock	マカ

USB

メイン画面で選択したクライアント PC の USB デバイスの制御を行います。

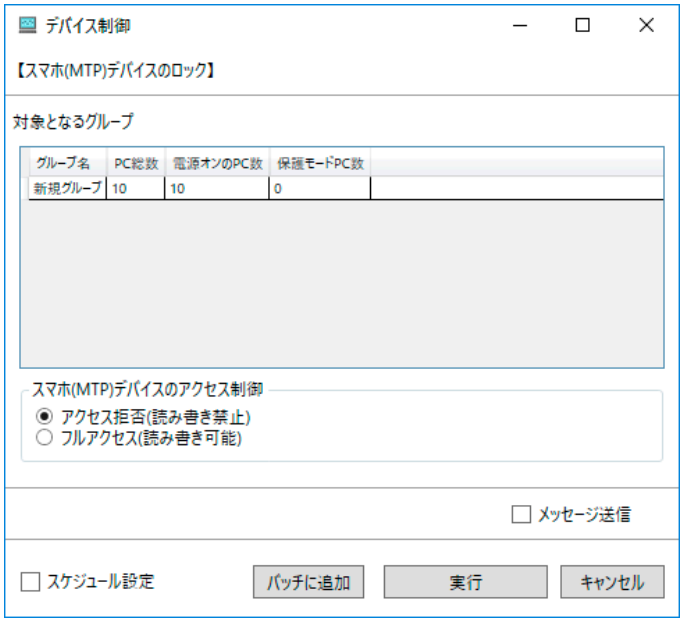


Point

ある特定の USB デバイスのみアクセスを許可したいような場合は、画面下の Vid（ベンダー ID）、Pid（プロダクト ID）を直接指 定することで例外処理を行うことができます。このとき、Vid と Pid はペアで入力する必要があります。また、Vid と Pid を入力しただけでは同じメーカーで同じ機種の USB デバイスが全て許可されてしまいますが、シリアルナンバーを追加することで、アクセスを許可する USB デバイスを限定することができます。許可する USB デバイスの設定数は最大で 16 となります。

■スマホ

メイン画面で選択したクライアント PC に接続するデバイスに対するアクセス制御を行います。



アクセス制御が可能なデバイスは、Media Transfer Protocol（MTP）規格で通信を行うデバイスとなります。そのため、Media Transfer Protocol（MTP）規格で通信を行うデバイスであれば、スマートフォン（スマホ）の他にも、タブレットやデジタルオーディオプレイヤーもアクセス制御が可能となります。ただし、iPhone や iPad などの iOS デバイスには対応していません。

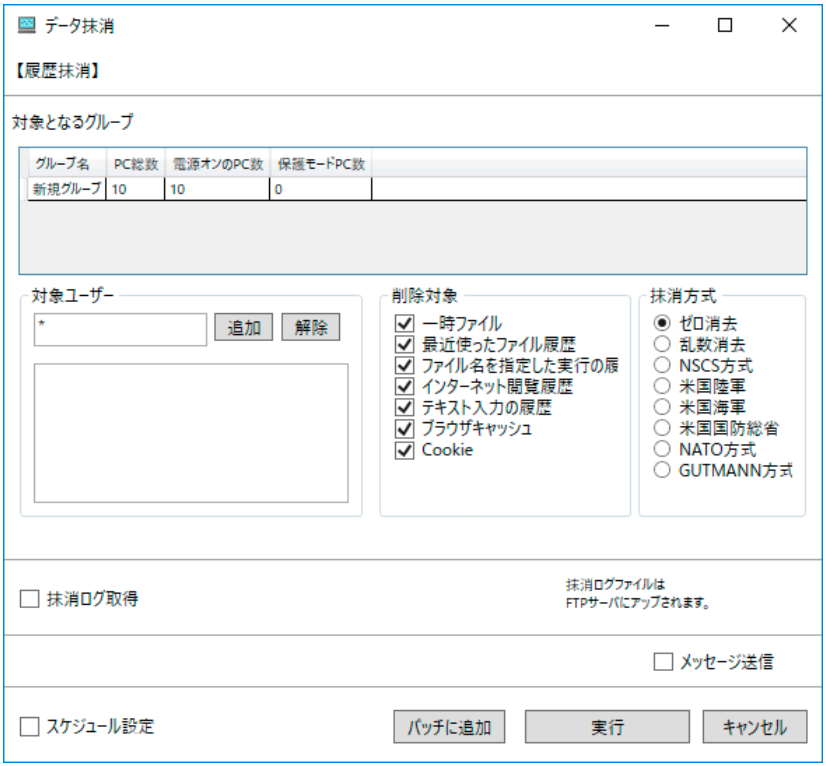
HD 革命 /Eraser の制御（「Eraser」タブ）

「Eraser」タブでは、各クライアント PC にインストールされている「HD 革命 /Eraser ファイル抹消」の動作を制御します。

データ抹消

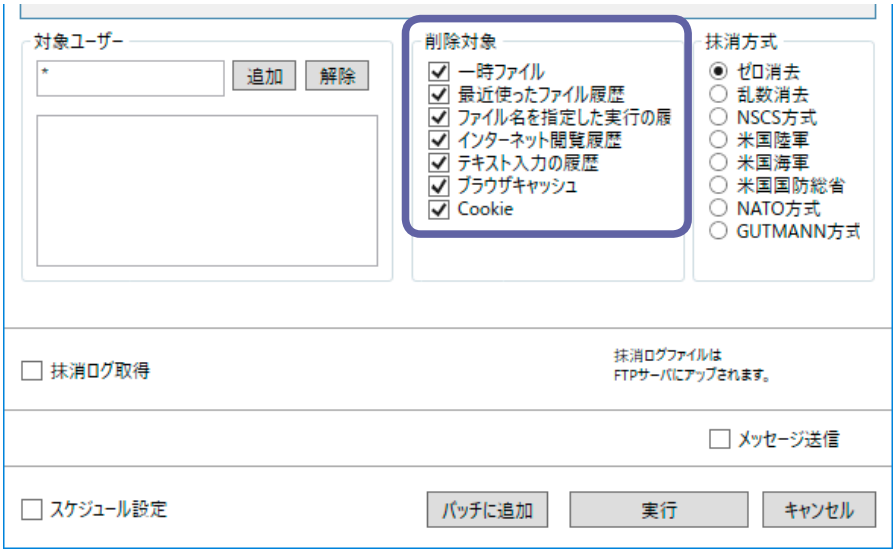
■履歴抹消

「履歴の抹消」では、メイン画面で選択したクライアント PC において「対象ユーザー」で追加したユーザーのデータを抹消します。対象ユーザーにはワイルドカード（＊と？）を使用することができます。削除する項目は右側の「削除対象」の中から選択します。



Point

「抹消ログ取得」にチェックを入れると、抹消完了後にログが FTP サーバーにアップ（保存）されます。
出力するファイルの形式は、PDF（.pdf）と TEXT（.txt）が選択可能です。アップ（保存）されたファイルを閲覧するには、ファイルを FTP サーバーからダウンロードする必要があります。操作については 27 ページを参照してください。



●一時ファイル

Windows やアプリケーションが一時的に作成するファイルの保存先フォルダー（一時フォルダー）の中を抹消します。Windows の環境変数「TEMP」「TMP」で指定されているフォルダー（標準では「C:/Users/[ログオン中のアカウント名]/AppData/Local/Temp」）が抹消対象となります。」

●最近使ったファイル履歴

Windows の「スタート」メニューなどに表示される最近使ったファイルの履歴を抹消します。

●ファイル名を指定して実行の履歴

Windows の「ファイル名を指定して実行」で「名前」欄に入力された履歴を抹消します。

●インターネットの閲覧履歴

「Internet Explorer」「Mozilla Firefox」「Google Chrome」「Microsoft Edge」の閲覧履歴を抹消できます。複数のインターネットブラウザをインストールされている場合、選択した項目が全てのインターネットブラウザにおいて抹消されます。

●テキスト入力の履歴

Web サイトのテキストボックスに入力したユーザー名や住所などのテキストで、インターネットブラウザに保存されている履歴を抹消します。抹消を行うと、過去に入力した内容が表示されなくなるため、再度入力が必要となります。

●ブラウザのキャッシュ

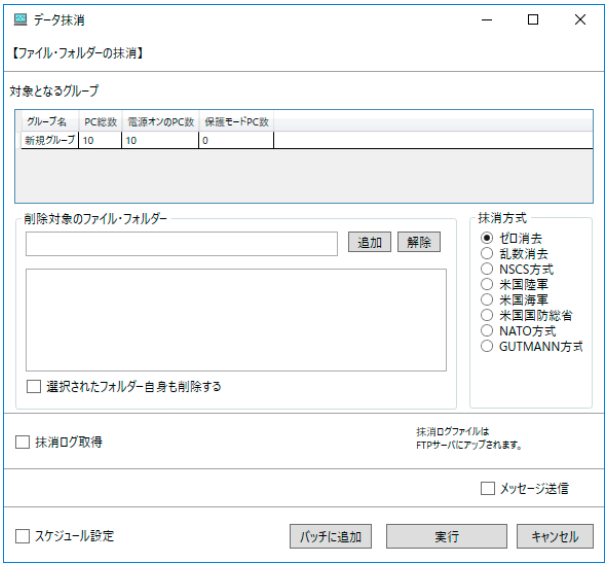
インターネットブラウザが保存している Web サイトの表示を高速化するためのテキストや画像データのキャッシュを抹消します。抹消を行うと、ページのデータを改めて読み込むため、表示に時間がかかります。

● Cookie

通販サイトなどで利用されている、Web サイトの閲覧者の情報をコンピューターに一時的に記録するための Cookie（情報ファイル）を抹消します。Web サイトで使用するためのユーザー名やパスワードが Cookie に保存されていた場合は、再度入力が必要となります。

■ファイル抹消

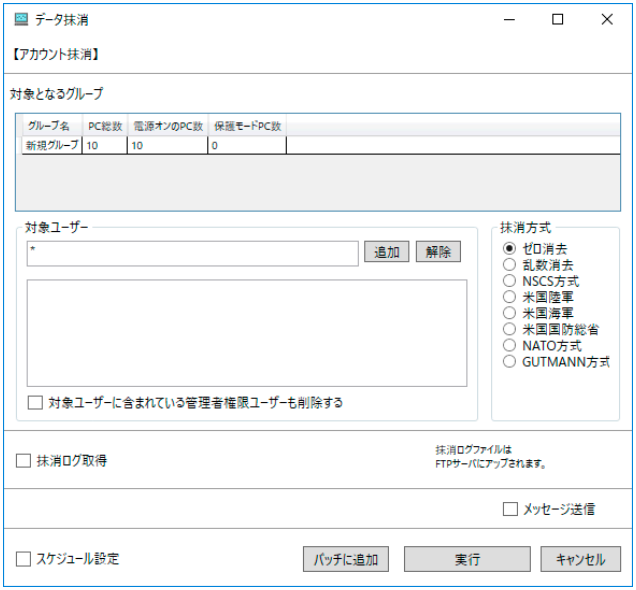
「ファイル抹消」では、メイン画面で選択したクライアント PC のファイル、フォルダーを抹消します。「削除対象のファイル・フォルダー」はフルパスで入力してください。なお、ファイル名にはワイルドカード（＊と？）を使用することもできます。



「選択されたフォルダー自身も削除する」のオプションを選択すると、抹消対象として追加したフォルダーの中に存在するファイル、フォルダーを抹消した後に追加したフォルダー自身も削除されます。スケジュールを設定して定期的に追加したフォルダーの中のファイル、フォルダーのみ抹消するような場合は、このオプションを選択しないようにしてください。

■アカウント抹消

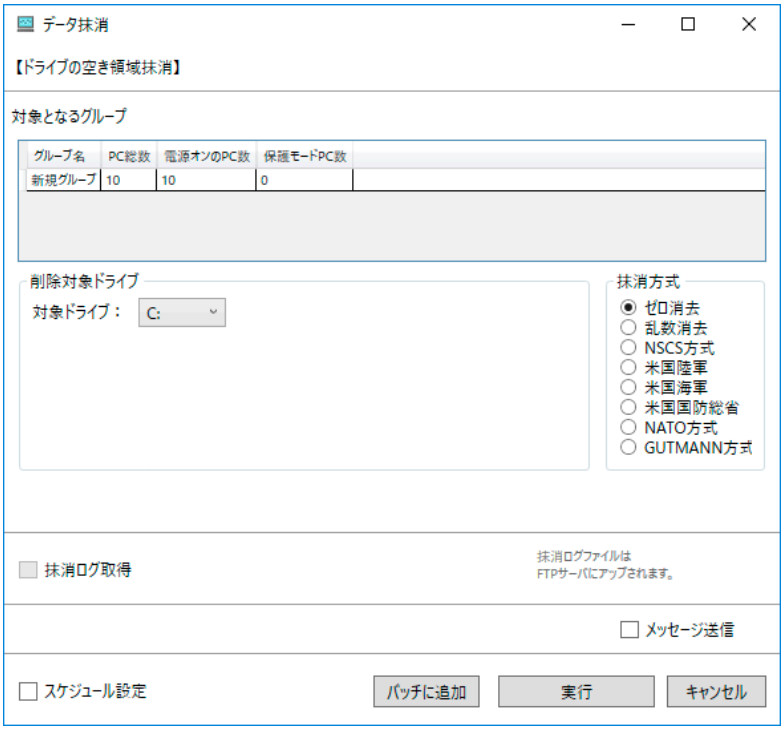
「アカウント抹消」では、メイン画面で選択したクライアント PC に登録されているユーザーアカウントを抹消します。「＊」を指定した場合は、全てのユーザーアカウントを抹消します。ただし、「Administrator」、「Guest」、「DefaultAccount」、現在ログオン中のユーザーアカウントは抹消できません。

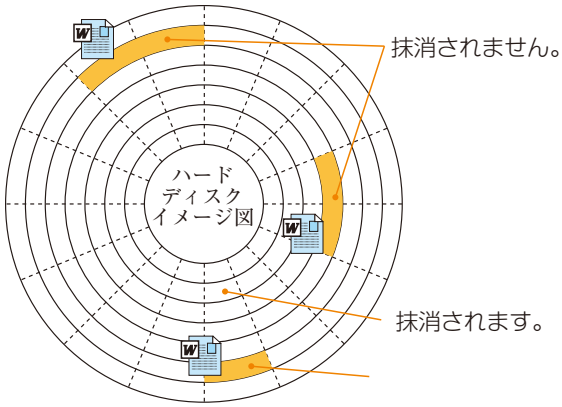


オプションを選択することで「管理者権限ユーザー」（管理者権限を持つユーザーアカウント）も削除することができますが、クライアント PC の「管理者権限ユーザー」をすべて削除してしまうとクライアント PC での操作（アカウントの追加など）ができなくなります。「管理者権限ユーザー」を削除する際は注意してください。

■空き領域抹消

「空き領域の抹消」では、メイン画面で選択したクライアント PC において、「削除対象ドライブ」で指定したドライブの空き領域（ハードディスクの中でファイルが存在しない領域）を抹消します。下のイメージ図のように、ファイルが置かれている領域以外の領域が「空き領域」となります。





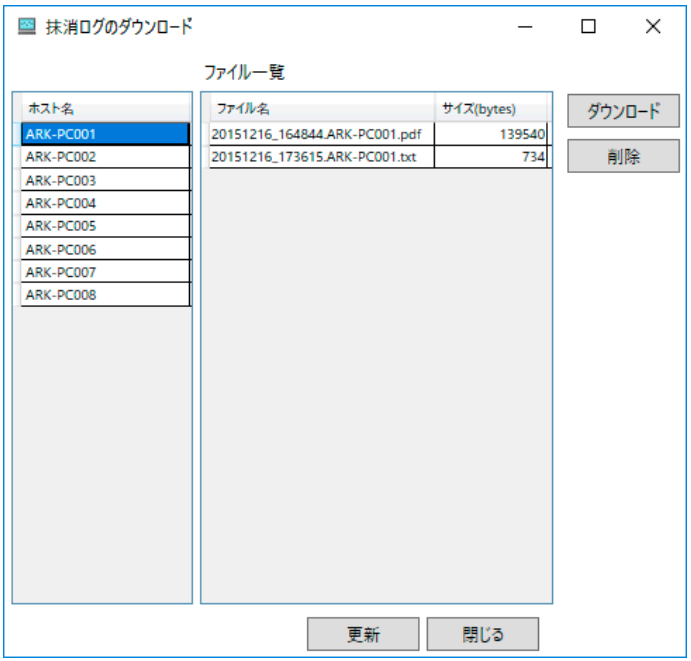
設定したスケジュールの時刻になったときに他のスケジュール抹消が実行されている場合は、スケジュールによる抹消は実行されません。

FTP

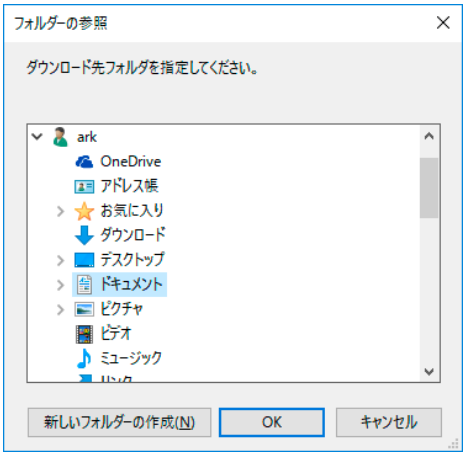
■抹消ログ取得

「データ抹消」の各操作画面で「抹消ログ取得」にチェックを入れると FTP サーバーに抹消ログが保存されます。メイン画面の「抹消ログ取得」をクリックすると下の画面が表示されますので、この画面から FTP サーバーに保存されている抹消ログをダウンロードします。

抹消ログをダウンロードするには、画面左側に表示されているホスト名（クライアント PC）のリストの中で１つまたは複数選択し、次に画面右側のファイル名を選択して「ダウンロード」をクリックします。



保存先を指定して「OK」をクリックします。



抹消方式について

クライアント PC にインストールされた「HD 革命 /Eraser ファイル抹消」では次の抹消方式でデータの抹消を行うことができます。

● 0（ゼロ）で抹消

書き込み回数：1 回、抹消レベル：低

各クラスタに 0（ゼロ）を書き込みます。抹消レベルは低くなりますが、抹消時間は最も速くなります。

●乱数値で抹消

書き込み回数：1 回、抹消レベル：低

各クラスタに乱数を書き込みます。「0（ゼロ）で抹消」より少し抹消レベルが高く、比較的短時間で抹消することができます。

● NCSC 方式

書き込み回数：3回、抹消レベル：中

NCSC（米国コンピュータセキュリティーセンター）で定められた方式です。最初に各クラスタに固定値 1（0x00）を書き込み、次にその補数（0xFF）で上書きし、最後に固定値 2（0x77）で上書きします。

●米国陸軍方式

書き込み回数：3回、抹消レベル：中

米国陸軍で定められた抹消方式です。最初に各クラスタに乱数を書き込み、次に固定値（0xFF）で上書きし、最後にその補数（0x00）で上書きします。

●米国海軍方式

書き込み回数：3回、抹消レベル：中

米国海軍で定められた抹消方式です。最初に各クラスタに固定値（0x88）を書き込み、次にその補数（0x77）で上書きし、最後に乱数で上書きした後に書き込み検証を行います。

●米国国防総省方式

書き込み回数：3回、抹消レベル：中

米国国防総省（ペンタゴン）で定められた抹消方式です。最初に各クラスタに固定値（0xFF）を書き込み、次にその補数（0x00）で上書きし、最後に乱数で上書きした後に書き込み検証を行います。

● NATO 方式

書き込み回数：7回、抹消レベル：高

NATO（北大西洋条約機構）で定められた抹消方式です。固定値 1（0x00）→固定値 2（0xFF）→固定値 1（0x00）→固定値 2（0xFF）→固定値 1（0x00）→固定値 2（0xFF）→乱数値で上書きします。

● Gutmann 方式

書き込み回数：35 回、抹消レベル：高

コンピューター科学者グートマン（PeterGutmann）博士によって提唱された抹消方式です。乱数値で 4 回→固定値（0x55 や 0xAA など）で 27 回→乱数で 4 回上書きします。最も安全な消去方式ですが、書き込み回数が計 35 回と多いため、非常に時間がかかります。

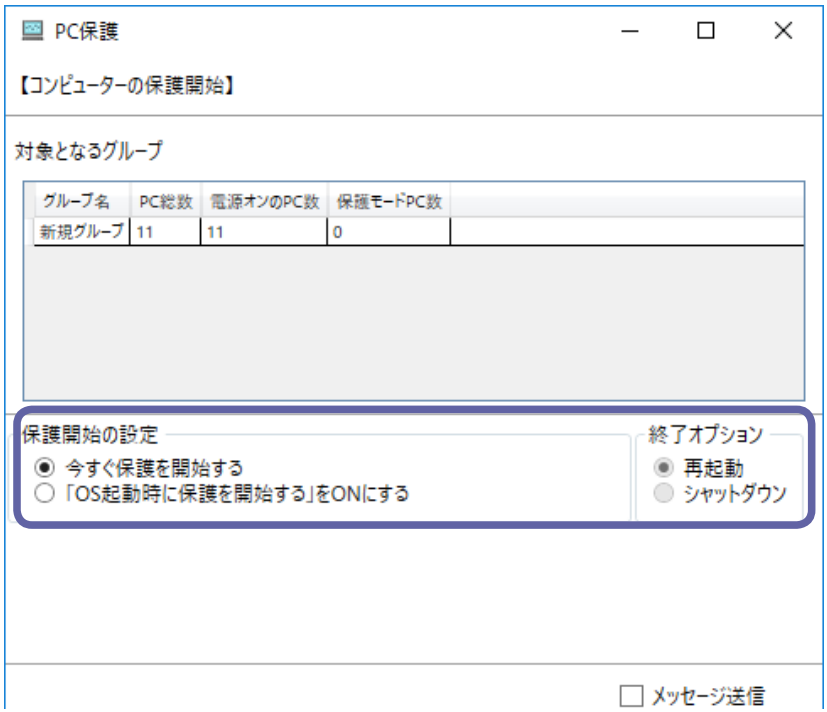
HD 革命 /WinProtector の制御（「WinProtector」タブ）

「WinProtector」タブでは、各クライアント PC にインストールされている「HD 革命 /WinProtector」の動作を制御します。

PC 保護

■保護開始

メイン画面で選択したクライアント PC の保護を開始します。



●保護開始の設定

「今すぐ保護を開始する」を選択するとオーダー投入後にすぐにクライアント PC の保護が開始します。

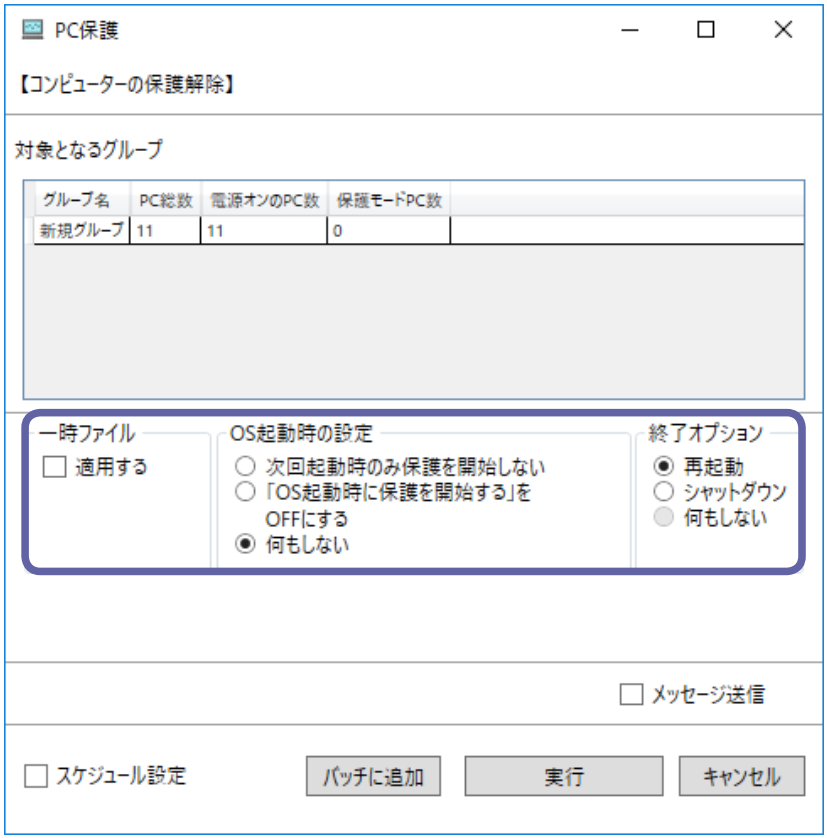
「「OS 起動時に保護を開始する」を ON」を選択すると、クライアント PC のオプション設定が変更され、毎回 OS 起動時から保護が開始されるようになります。

●終了オプション

「「OS 起動時に保護を開始する」を ON」を選択したときに、クライアント PC の動作を選択します。

■保護解除

メイン画面で選択したクライアント PC の保護を解除します。



●一時ファイル

「一時ファイル」は、保護を開始してから変更された内容をドライブに書き込みます。

● OS 起動時の設定

OS 起動時に保護を開始する設定になっている場合、そのオプション設定を指定した動作に変更します。OS 起動時に保護を開始する設定になっていない場合は指定しても無効となります。

Point

「一時ファイル」について

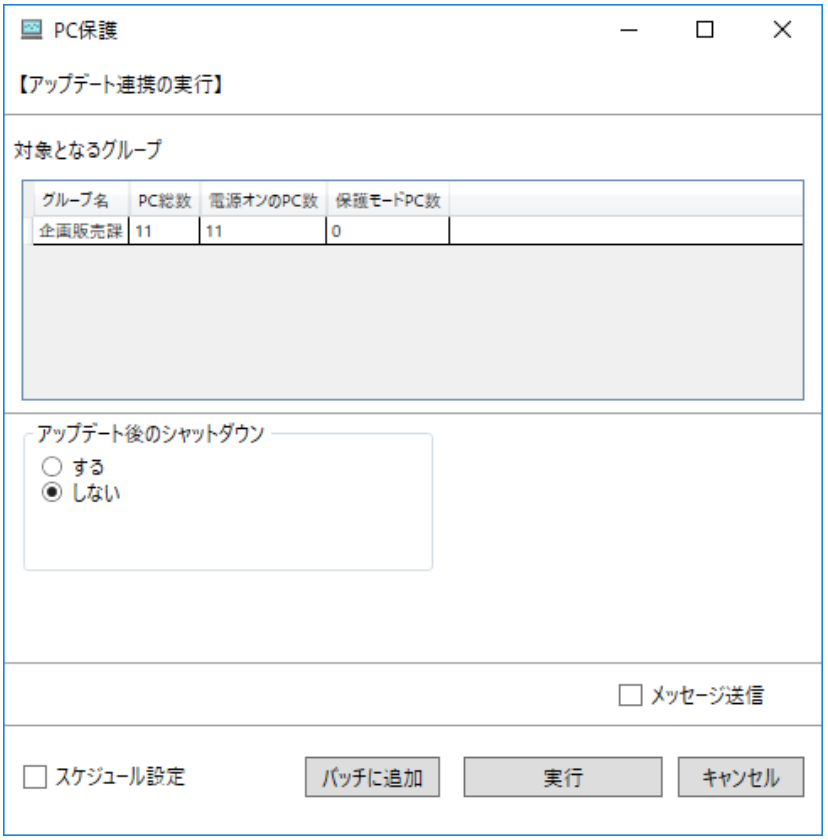
一時ファイルは、保護されたドライブに対して行われた書き込みをキャッシュするファイルとなり、ドライブに書き込みが行われるデータが多いほど増加します。そのため、システムユーティリティやインデックスを作成するようなソフトウェアが存在すると、一時ファイルの使用容量は通常の場合よりも早く増加することがあります。

●終了オプション

終了時の動作を選択します。「一時ファイル」で「適用する」を選択することで、「何もしない」が選択できるようになります。クライアント PC は、変更内容をドライブに適用した後に保護が解除されたままの状態となります。

■アップデート連携

詳細設定の「■アップデート連携」タブ（37 ページ）で設定した内容で「Windows Update」とアンチウィルスソフトウェアのアップデートを行います。



Point

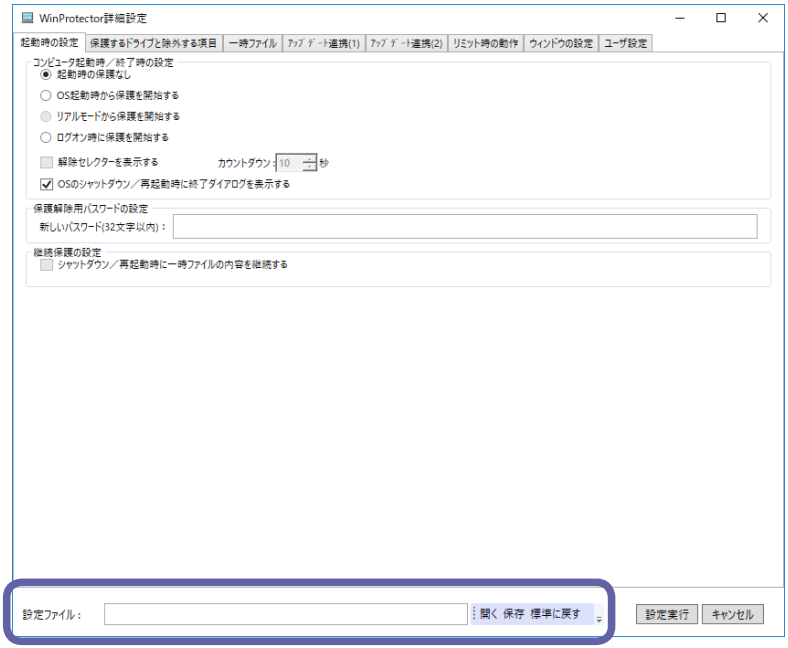
「アップデート連携」タブでの設定について

「■アップデート連携」タブ（37 ページ）で更新処理が有効になっていないとアップデート連携を実行できませんので、最初に設定を行うようにしてください。なお、「スケジュールで実行する」、「シャットダウン時に実行する」を選択していても、この画面からアップデート連携を即時実行することができます。この場合、実行するタイミングで設定した「制限時間」に関係なくアップデートが最後まで実行されます。

■詳細設定

「詳細設定」をクリックすると「WinProtector 詳細設定」画面が表示されます。この画面の各タブで、メイン画面で選択したクライアント PC に対する HD 革命 /WinProtector のオプションを設定します。「設定実行」をクリックすると設定ファイルが更新されクライアント PC の再起動が行われます。

設定した内容は、画面下の「設定ファイル」より xml、ini ファイルで保存ができます。保存したファイルを読み込ませることで、各タブのオプション設定を一度に変更できます。ただし、Network Controller Ver.1 で作成した xml ファイルは読み込めません。「標準に戻す」をクリックすると、HD 革命 /WinProtector のオプションが規定値に戻ります。



■詳細設定―「起動時の設定」タブ

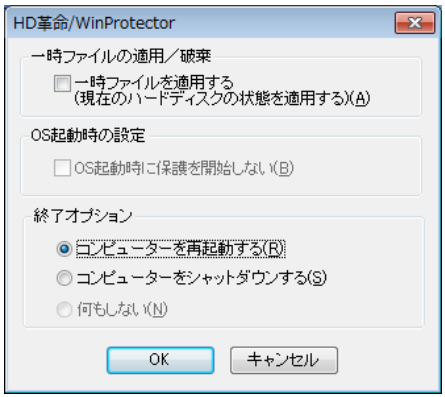
保護を行うタイミングと解除時のセレクター、ダイアログを設定します。

●コンピューター起動時／終了時の設定

・起動時の保護なし
　起動時の保護は行われません。
・OS 起動時から保護を開始する
　Windows の起動時から保護を行います。
・リアルモードから保護を開始する（Network Controller では選択できません）
　コンピューターの起動時から保護を行います。クライアント PC が GPT ディスク環境の場合は使用できません。
・ログオン時に保護を開始する
　ユーザーのログオン時から保護を行います。
・解除セレクターを表示する
　OS が起動するときに保護を解除するためのセレクターを表示するかどうかを設定します。

```
Press [ESC] key to cancel protection
Press another key to start protection ...   3
```

・OS のシャットダウン／再起動時に終了ダイアログを表示する
　OS のシャットダウン／再起動時に次の画面が表示され動作を選択できます。



「保護しないレジストリキーの設定」（35 ページ）を行っている場合は、「一時ファイルを適用する」のオプションは選択できません。

●保護解除用パスワードの設定

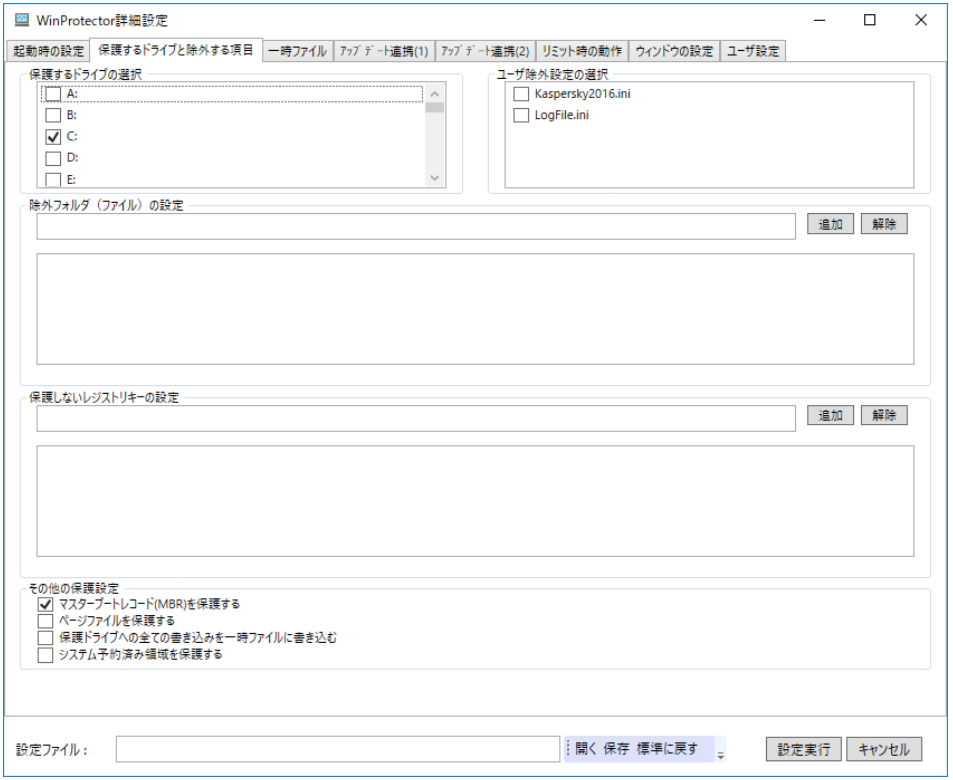
　クライアント PC 上で HD 革命 /WinProtector の保護を解除するためのパスワードを設定します。パスワードは、半角英数 32 文字まで設定可能で、記号の ! # $ % - ; , . < > / ? が使用可能です。ただし、クライアント PC 側で「リアルモードから保護を開始する」を選択して使用している場合は、半角英数字で 8 文字に制限されます。

●継続保護の設定

・シャットダウン／再起動時に一時ファイルの内容を継続する（Network Controller では選択できません）
　一時ファイルを破棄せずに継続して使用します。これにより、インストール後に再起動を行うようなアプリケーションでも、変更を適用することなく継続して使用できるようになります。このオプションを使用するには、「リアルモードから保護を開始する」を選択する必要があるため、クライアント PC が GPT ディスク環境の場合は使用できません。

■詳細設定―「保護するドライブと除外フォルダ」タブ

HD 革命 /WinProtector で保護するドライブおよびフォルダーを設定します。



●保護するドライブの選択

表示されているドライブの中から、クライアント PC で保護したいドライブ文字を選択します。保護できるドライブはローカルのハードディスクドライブに限られ、リムーバブルドライブ、ネットワークドライブ、CD/DVD ドライバなどは保護できません。また、クライアント PC に存在しないドライブを選択しても効果はありません。

●ユーザー除外設定の選択

保護中に除外する（保護しない）フォルダーやファイル、レジストリを記述した ini ファイルを作成し、ここで選択することで除外設定が有効となります。除外設定を有効にする場合、「保護ドライブへの全ての書き込みを一時ファイルに書き込む」を有効にする必要があります。

なお、標準で、「Kaspersky 2016.ini」が登録されていますが、こちらを選択することで「Kaspersky2016 / 2017」が使用しているフォルダーやレジストリ設定を除外することができます。これにより、アップデート連携で「アンチウィルスソフトウェアの更新処理を行う」を選択しなくても定義データベースを更新することができるようになります。「Kaspersky 2016 / 2017」を使用している場合のみ有効な除外設定です。ini ファイルの書式については、47 ページを参照してください。

●除外フォルダ（ファイル）の設定

クライアント PC で特定のフォルダーやファイルを除外する（フォルダーやファイルを保護しない）場合は、そのパスを入力し「追加」をクリックします。ここにリストされたフォルダー、ファイルは、保護を解除して

も、保護中に書き込まれたデータはそのまま削除されずに残ることになります。
　なお、「ユーザー除外設定の選択」の「Kaspersky 2016 / 2017.ini」は、特別な除外設定となり、除外するフォルダー、ファイルは自動的に設定され、リストに表示されません。

⚠ BitLocker により暗号化されたディスクに対して保護を行う場合、「除外フォルダ（ファイル）の設定」を行うことはできません。

●保護しないレジストリキーの設定
　クライアント PC で特定のレジストリキーを除外する場合は、レジストリキーを入力し「追加」をクリックします。ここにリストされたレジストリキーは、保護を解除しても変更された各値は保護中の状態のまま残ることになります。レジストリキーの入力の際、先頭に必ず「HKEY_LOCAL_MACHINE」を付けてください。

●その他の保護設定
・マスターブートレコード（MBR）を保護する
　マスターブートレコードを保護の対象とするかを設定します。特別な理由がなければ通常は ON の状態で使用してください。
・ページファイルを保護する
　Windows のページファイルを保護の対象とするかを設定します。一時ファイルの使用容量は、保護しないときよりも増加します。
・保護ドライブへの全ての書き込みを一時ファイルに書き込む
　空き領域も含め全てのドライブを全て保護の対象とするかを設定します。一時ファイルの使用容量は、保護しないときよりも増加します。
・システムで予約済み領域を保護する
　システムドライブの前にある「システムで予約済み」領域を保護の対象とするかを設定します。

Point

「保護ドライブへの全ての書き込みを一時ファイルへ書き込む」オプションについて
HD 革命 /WinProtector では、ドライブの保護中に使用領域（保護を開始した時点でファイル・フォルダーが存在する領域）の変更が行われると、その変更は「一時ファイル」に書き込まれます。新規に作成するファイル·フォルダーにおいては通常「空き領域」に書き込まれますが、この「空き領域」を保護するかどうかで、一時ファイルの使用量に次のような違いがあります。
●オプションを使用しない（「空き領域」への書き込みはそのまま書き込む）
ドライブの「空き領域」への書き込みは、実際のファイル・フォルダーは「空き領域」に書き込み、ファイル・フォルダーの登録情報のみ一時ファイルに書き込みます。これにより、一時ファイルの使用量を節約することができます。
●オプションを使用する（「空き領域」への書き込みを「一時ファイル」に書き込む）
ドライブの「空き領域」も保護の対象となり、保護中のドライブへの書き込みは、空き領域への書き込みも含めすべて一時ファイルに書き込まれます。このオプションを使用すると、保護中のドライブへの書き込みは行わないので、一時ファイルの使用量は増加しますがセキュリティは向上します。

■詳細設定―「一時ファイル」タブ

「一時ファイル」と「インデックス」の保存場所とサイズを設定します。

●一時ファイル保存場所

「一時ファイル」の場所を設定します。「メモリー＋ハードディスク」を設定した場合は、最初にメモリーが消費されます。

●インデックスの場所

「インデックス」は、保護するドライブのどのセクターが使用されたかを記録するものです。一時ファイルとは別に場所を指定します。「OS 管理外メモリー」は 64bit 版の Windows では使用できません。

●一時ファイル（ハードディスク）

「一時ファイル」をハードディスクに保存する場合に、どのドライブに保存するかを指定します。

●サイズの設定

「一時ファイル」をハードディスクに保存する場合にサイズを指定します。必要以上に大きくするとハードディスクの容量を圧迫しますので、適切なサイズを指定してください。

●一時ファイル（メモリー）

「一時ファイル」をメモリーに保存する場合にサイズを指定します。「OS 管理外メモリー」は 64bit 版の Windows では使用できません。

●使用するメモリー領域の選択

「一時ファイル」をメモリーに保存する場合に、どのメモリーを使用するかを選択します。「OS 管理外メモリー」は 64bit 版の Windows では使用できません。

> ⚠ 一時ファイル（メモリー）のサイズを大きくしても、実際に使用できるメモリーが不足している場合、保護を行うことはできません。また、システムメモリーを使用する場合、サイズを大きくすると Windows が使用できるメモリー容量が少なくなります。
> 保護を行うことができないときや動作が遅くなる場合は、サイズを小さくするかハードディスクのみを使用するようにしてください。

■詳細設定―「アップデート連携（1）」タブ

「Windows Update」、またはアンチウィルスソフトの更新処理について設定します。

● Windows Update 設定

・Windows Update の更新処理を行う

クライアント PC において、Windows Update を行うように設定します。更新処理を行うには 32 ページの「OS 起動時から保護を開始する」を選択してください。

・適用する更新プログラムの種類

更新プログラムの種類を設定します。適用しない更新プログラムは、KB 番号または文字列で除外できます。更新処理を行うには 32 ページの「OS 起動時から保護を開始する」を選択してください。

●アンチウィルスアップデート設定

・アンチウィルスソフトウェアの更新処理を行う

クライアント PC にインストールされているアンチウィルスソフトウェアのプログラムや定義ファイルの更新を行います。更新処理を行うには 32 ページの「OS 起動時から保護を開始する」を選択してください。

●実行するタイミング

アップデート連携を実施するタイミングを指定します。スケジュールで実行する場合は、右側の「間隔：」「開始時刻：」を設定します。なお、「制限時間：」は、アップデート連携を行う時間を制限するもので、指定した時間が経過するとアップデート連携が途中であっても処理を終了します。「制限時間：」は、シャットダウン時、または任意のタイミングで実行する場合も有効となります。シャットダウン時に実行する場合は、クライアント PC がログオン状態にある時のみ有効となります。

・前回更新されなかった場合は、起動／ログオン時に開始する

指定したタイミングで更新が行われなかった場合、次の起動時またはログオン時に更新が開始します。

・アップデート連携終了後、シャットダウン

アップデート連携終了後にコンピューターをシャットダウンできます。アップデート連携中はコンピューターが何回か再起動することがありますが、アップデートが完了するまではシャットダウンは行われません。

・遅延時間

アップデート連携時に、自動ログオンしてから実際に処理を開始するまでの遅延時間（待機時間）を 0 ～ 10 分の範囲で設定できます。

●更新処理を実行するアカウント

Windows Update やアンチウィルスソフトによりコンピューターの再起動が行われた場合、自動的にログオンして更新処理を行います。

ここでは、自動的にログオンするアカウントのユーザー名とパスワードを入力します。設定するパスワードは 64 文字以内としてください。入力された内容が間違っていると更新処理が行われません。

● WSUS サーバーを利用する

Windows Update において、WSUS サーバーを使用する場合にチェックを入れます。「WSUS サーバー」と「統計サーバー（通常は WSUS サーバーと同じ）」欄にサーバー名を入力します。

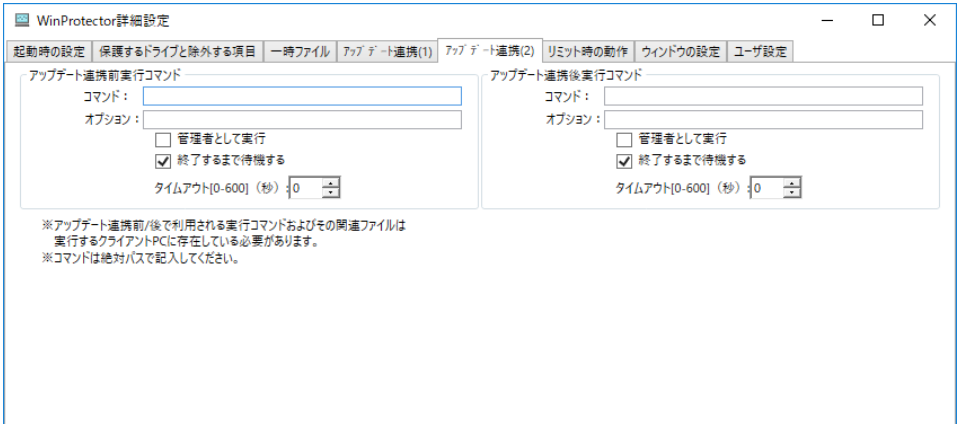
> ⚠
> WSUS サーバーの設定を行うと、クライアント PC の Windows グループポリシーにおける WSUS サーバーの設定が変更されます。そのため、HD 革命 /WinProtector を介さない Windows Update を行う場合も、設定した WSUS サーバーに接続しにいくようになります。
> また、WSUS サーバーの設定をしたままクライアント PC の HD 革命 /WinProtector をアンインストールしてもグループポリシーの WSUS サーバーの設定は残ったままとなります。

● PROXY サーバーを使用する

Windows Update において、PROXY サーバーを使用する場合にチェックを入れます。サーバー名とポート番号欄に PROXY サーバーの設定を入力します。認証付きプロキシの場合には、ユーザー名、パスワードも入力します。Windows 10 の環境では認証つきプロキシは指定できません。

■詳細設定―「アップデート連携（2）」タブ

アップデート連携前／後に実行するコマンドを設定します。

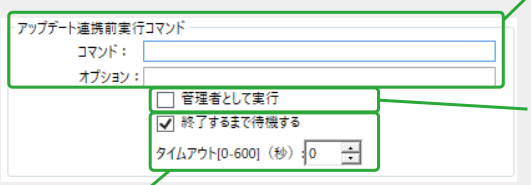


●アップデート連携前実行コマンド／アップデート連携後実行コマンド

アップデート連携の開始前、またはアップデート連携の終了後に、任意のコマンド（例：「.exe」、「.bat」）を実行することができます。コマンドを実行するには、「Windows Update の更新処理を行う」または「アンチウィルスソフトウェアの更新処理を行う」のチェックが ON になっている必要があります。

コマンドの設定とオプションスイッチの指定

「アップデート連携前／実行後コマンドの設定」の「設定」ボタンをクリックし、コマンドの設定とオプションスイッチを指定します。



実行するコマンドとコマンドに渡す引数（パラメーター）を指定します。
例：コマンド：D:\Execute\Setup.exe
　　オプション：/silent

このオプションが ON の場合は、指定したコマンドを管理者として実行します。Windows 上でエクスプローラーを右クリックして「管理者として実行」を選択した場合と同様の操作となります。

このオプションを ON にすると、「タイムアウト」で指定した時間だけ次のアップデート連携処理に進まずに待機します。なお、コマンドが実行中であっても「タイムアウト」で指定した時間が経過した場合は、次のアップデート連携処理が開始されます。0 秒を指定した場合、タイムアウトは行われません。オプションが OFF の場合は、コマンドの実行とともに次のアップデート連携処理に進みます。

アップデート連携時にコマンドを実行する場合、「終了するまで待機する」が ON でタイムアウトに 0 秒（タイムアウトなし）を設定する場合は、そのコマンドが確実に終了することを確認してから設定してください。例えば、コマンドに「notepad.exe」を指定して実行した場合、開いたウィンドウが閉じられるまでは先に進まなくなります。
なお、コマンドが実行中であってもアップデート連携を行う「制限時間」が指定した時間経過した場合は、アップデート連携が終了しコンピューターが再起動されます。

■詳細設定―「リミット時の動作」タブ

「一時ファイル」の消費に関する動作や告知方法を設定します。

●アラームの設定

・一定量が使用されるたびにメッセージで知らせる

一時ファイルが何%まで使用されたときにメッセージを表示するかを設定します。

・使用済み容量が設定値に達したときにアラームで知らせる

一時ファイルの使用済み容量が設定した値を超えたときにどのような方法で警告するかを指定します。

・アラームで知らせる使用済み容量

一時ファイルをどの程度消費したときに上記のアラームによって知らせるかを選択します。

●動作の設定

・使用済み容量が規定値に達したときの動作選択

「アラームの設定」とは別に、一時ファイルが設定した値を超えたときの動作を設定します。「現在の状態をシステムに適用後、保護を継続する」を選択した場合は、一時的に保護を解除して一時ファイルに保存された内容をドライブに書き込み、その後再度保護を行います。

・動作を実行する使用済み容量

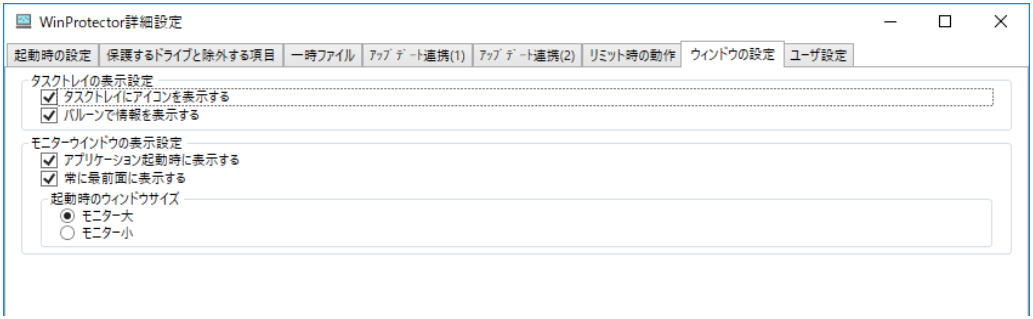
一時ファイルが何%まで使用されたときに、上記で設定した動作を行うかを設定します。

「現在の状態をシステムに適用後、保護を継続する」オプションを選択する場合、34 ページの「保護するドライブと除外フォルダ」タブで「保護するドライブの選択」のドライブを 1 つだけ選択し、かつ 36 ページの「一時ファイル」タブで「一時ファイル保存場所」に「メモリー」を選択する必要があります。

また、他のアプリケーションから強制的に再起動が行われると、一時ファイルの内容が適用されずにシャットダウン／再起動が行われるため、タイミングによっては内容に不整合が起こり OS やアプリケーションの動作に支障が出る場合があります。

■詳細設定―「ウィンドウの設定」タブ

アイコンやウィンドウに関する表示方法を設定します。



●タスクトレイの表示設定

・タスクトレイにアイコンを表示する

タスクトレイにアイコンを表示するかどうかを設定します。

・バルーンで情報を表示する

「リミット時の設定」タブの「アラームの設定」内容を基にバルーンで情報を表示します。

●モニターウィンドウの表示設定

・アプリケーション起動時に表示する

HD 革命 /WinProtector を起動したときに、下のモニターウィンドウを表示するかどうかを設定します。

・常に最前面に表示する

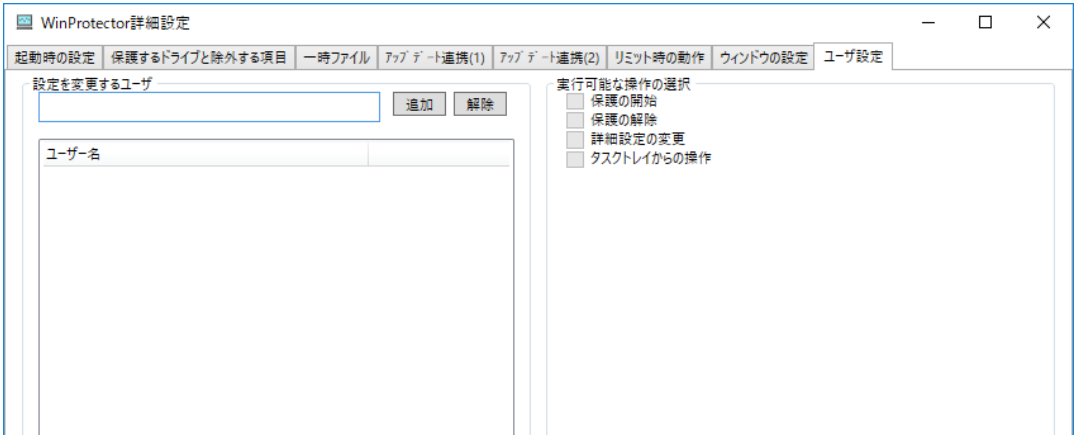
モニターウィンドウを表示する際に、常に最前面に表示するかどうかを設定します。

・起動時のウィンドウサイズ

モニターウィンドウには、大きいウィンドウと小さいウィンドウがありますので、どちらのサイズで表示するかを指定します。

■詳細設定―「ユーザー設定」タブ

ログオン可能なユーザーごとの動作を選択することができます。



●設定を変更するユーザー

クライアント PC にログオン可能なユーザー名を追加します。ユーザー名には、「＊」によるワイルドカード指定ができます。

●実行可能な操作の選択

「ユーザー名」の欄に登録されたユーザー名を選択し、実行を許可する操作にチェックを入れます。

クライアント PC で操作されたくない場合は、チェックをすべて外しておくことで誤操作を防ぐことができます。ユーザー名を確認してから設定を行うようにしてください。

・保護の開始

保護の開始を許可します。保護の開始が不許可になっているときでも、オプション設定で「OS 起動時からの保護を開始する」または「リアルモードから保護を開始する」が有効になっている場合は、OS 起動時に保護が開始されます。

・保護の解除（適用して解除）

「一時ファイル」を適用して保護を解除することを許可します。

・詳細設定の変更

「詳細設定」画面を開いて設定を変更することを許可します。パスワードが設定されている場合は、パスワードの入力が必要です。

・タスクトレイからの操作

タスクトレイのアイコンを右クリックしたときに表示されるメニューからの動作を許可します。

Point

特定ユーザーのログオン時に保護を開始する（しない）動作の設定

「起動時の設定」タブの「ログオン時に保護を開始する」と「保護の開始」の許可、不許可の設定を組み合わせることで、特定のユーザーがログオンした場合だけ、保護を開始する（または、保護を開始しない）という動作を設定することができます。

例えば、Administrator がログオンした場合は保護を開始せず、それ以外のユーザーのログオン時に保護を開始するようにしたい場合、

①「ログオン時に保護を開始する」オプションを ON

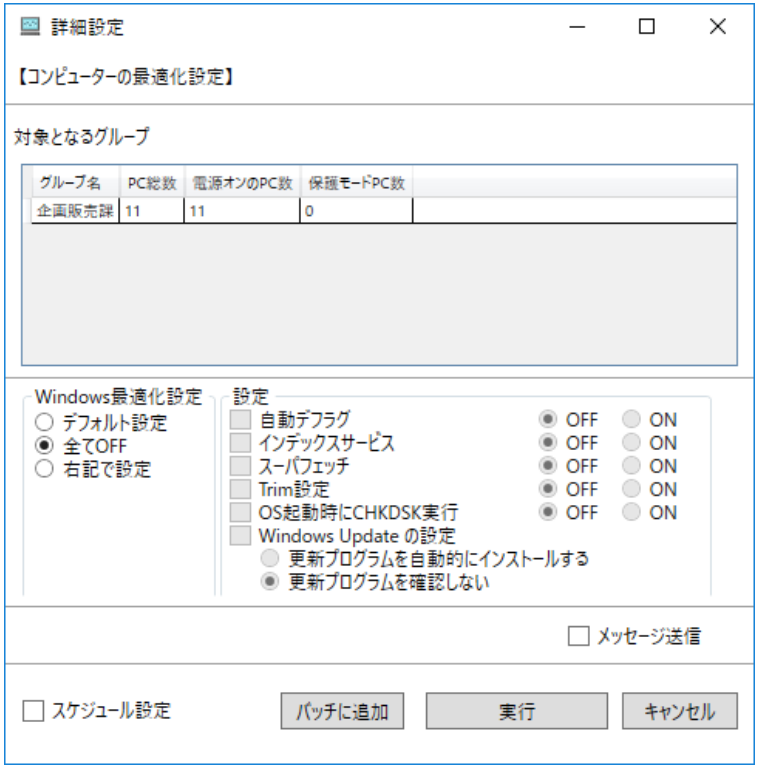
②「ユーザー設定」で、Administrator の「保護の開始」を OFF

に設定することで実現できます。

ただし、Administrator 以外のユーザーでログオンして保護が開始された後、そのユーザーがログオフし、次に Administrator がログオンした場合は、保護がかかったままになります。

■最適化設定

Windows にはパフォーマンスを向上させるために環境を最適化する機能がありますが、この機能が動作するとハードディスクへの書き込みが発生し、HD 革命 /WinProtector の「一時ファイル」を増加させる原因となります。ここでは、Windows に付属している機能の設定を変更することができます。



● Windows の最適化設定

右側の「設定」欄の各項目の動作を制御します。

●設定

・自動デフラグ

Windows は、何も操作がされていない状態（アイドル状態）のときに自動的にデフラグを実行しています。この自動デフラグの設定を変更します。

・インデックスサービス

Windows は、ファイルやフォルダーのインデックスを作成し、このインデックスを参照することで高速な検索を可能としています。このインデックスを作成する機能の設定を変更します。

・スーパーフェッチ

頻繁に使用するファイルやアプリケーションを解析し、あらかじめメモリにロードしてパフォーマンスを向上させる機能です。

・Trim 設定

SSD の性能低下を抑制するために OS から SSD に対して行われる Trim コマンドの設定を変更します。HD 革命 /WinProtector でクライアント PC の保護を行うには、Trim コマンドは必ず OFF の状態にしておく必要があります。

・OS 起動時に CHKDSK 実行
エラーが生じた場合など、Windows の起動時にチェックディスクが行われることがありますが、この機能を有効にするかどうかを設定します。
・Windows Update の設定
Windows Update による更新プログラムのインストール方法を設定します。HD 革命 /WinProtector でクライアント PC が保護されている場合、保護中に行われた更新確認プログラムのインストールは「一時ファイル」を適用しない限り破棄されてしまいます。HD 革命 /WinProtector でアップデート連携を行っている場合は、「更新確認プログラムを確認しない」に設定にすることを推奨します。

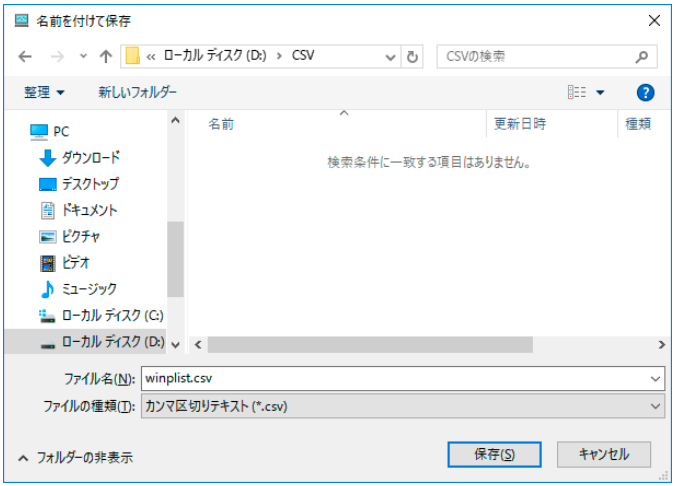
詳細表示

■詳細表示

メイン画面で選択したクライアント PC において、HD 革命 /WinProtector の設定内容を表示します。表示されている内容は、画面左下の「一覧出力」より CSV ファイルで保存できます。

項目	ark-pc001	ark-pc203	ark-pc003
更新日	2017/11/07 14:43:21	2017/11/07 12:16:06	2017/11/07 12:12:17
「起動時の設定」	- - - - -	- - - - -	- - - - -
コンピュータ起動時/終了時の設定	NoProtect	NoProtect	NoProtect
解除セレクターを表示する	False	False	True
解除セレクターのカウントダウン(秒)	10	10	10
OSのシャットダウン/再起動時に終了ダイアログを表示する	True	True	True
保護解除用パスワード			
シャットダウン/再起動時に一時ファイルの内容を継承する	False	False	False
「保護するドライブと除外フォルダ」	- - - - -	- - - - -	- - - - -
保護するドライブ	C	C	C
除外フォルダ			
除外レジストリーキー			
マスターブートレコード(MBR)を保護する	True	True	True
ページファイルを保護する	False	False	False
保護ドライブへの全ての書き込みを一時ファイルへ書き込む	False	False	False
システム予約済み領域を保護する	False	False	False
「一時ファイル」	- - - - -	- - - - -	- - - - -
一時ファイルの場所(保存先)	Harddisk	Harddisk	Harddisk
インデックスの場所(保存先)	SystemMemory	SystemMemory	SystemMemory
一時ファイルのドライブの設定	C	C	C
一時ファイルのサイズの設定(MB)	10000	10000	10000

「一覧出力」をクリックすることで、表示されている内容を CSV、INI ファイルに出力できます。ini ファイルで出力すると、詳細設定の設定ファイル（32 ページ）として利用できます。



アップデート連携について

「アップデート連携」は、HD 革命 /WinProtector で保護を行っている間に、Windows Update 、アンチウィルスソフトウェアの自動更新を行う機能です。設定した日時になると、保護を一時解除し、ダウンロード、適用した上で保護を再開します。「アップデート連携」には、いくつかの制限および注意事項があります。以下に「アップデート連携」を実行するタイミングの例をあげて、動作を説明します。

〈タイミングの設定例〉

間　　隔：金曜日
開始時刻：23：00
制限時間：5 時間

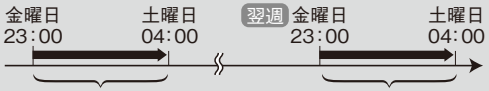
Point

この設定では、毎週金曜日の 23 時になると「アップデート連携」機能により自動更新が開始します。制限時間（開始から終了までの時間）はユーザーがリストの中から指定（最大 5 時間）できますが、実行可能なアップデートがすべて適用された場合は、制限時間の終了を待たずにコンピューターが再起動し保護を継続します。

アップデートの実行内容

●アップデートが指定した時間内に終了しなかった場合

更新が制限時間（例では5時間）内に完了しなかった場合、残りの更新は、次の「アップデート連携」が実行されるタイミングで適用されます。
例えば更新プログラムが 10 個あり、制限時間内に 6 個まで完了した場合、残りの 4 個は次の「アップデート連携」のタイミングで適用されます。なお、終了時刻になっても更新が実行中だった場合、その更新は途中でキャンセルされ次のアップデート連携のタイミングで再度適用されます。

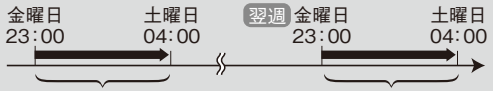


更新が 10個存在し、そのうち6個が制限時間内で完了すると…

前回の残り4個を実行します。この時点で最新の更新プログラムが存在する場合、合わせてそれも実行します。

●更新プログラムの順序に依存関係がある場合

更新プログラムⒶに依存する更新プログラムⒷが存在する（更新プログラムⒶが先に適用されていないと、更新プログラムⒷが適用できない）場合、はじめに更新プログラムⒶを適用した後、次のアップデート連携のタイミングに更新プログラムⒷが適用されます。

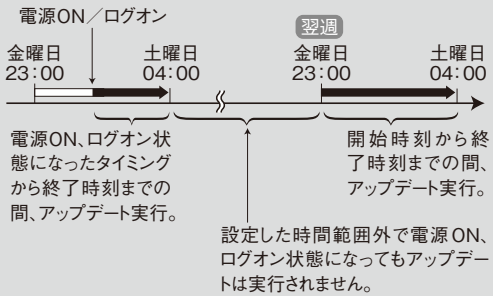


更新プログラムⒶを適用。この時点では更新プログラムⒷは適用されません。

更新プログラムⒷが適用。この時点で最新の更新プログラムが存在する場合、合わせてそれも適用されます。

●「実行するタイミング」（37 ページ）で「前回開始されなかった場合は、起動時／ログオン時に開始する」が OFF の場合

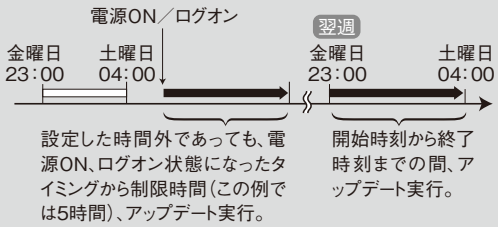
アップデートの実行には、「実行するタイミング」で設定した制限時間内で、コンピューターの電源が ON、かつ、ログオン状態である必要があります。
制限時間内にログオンされていない場合は、アップデートは実行されません。アップデートが実行されるのは、終了時刻までの間のみとなります。



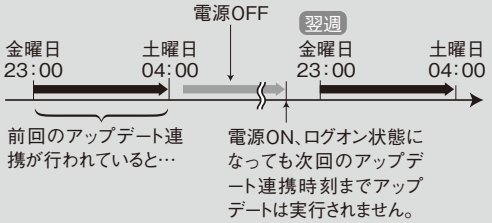
●「実行するタイミング」（37 ページ）で「前回開始されなかった場合、起動時／ログオン時に開始する」が ON の場合

アップデート連携の開始時刻から制限時間内に、コンピューターが起動していなかった等の理由でアップデート連携が行われていないとき、「前回開始されなかった場合は、起動時／ログオン時に開始する」オプション（37 ページ）が ON の場合は、コンピューターの電源が ON になった時やログオン時にアップデート連携を開始します。

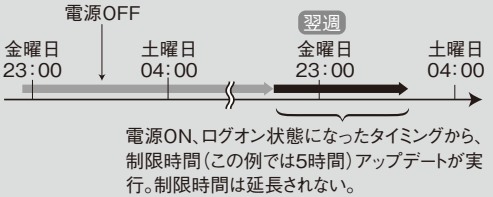
※ログオン時に開始される場合は、通常のアップデート連携時と同様に「アップデート連携の開始時刻になりました。」のダイアログが表示され、コンピューターが再起動します）



前回のアップデート連携が行われている場合は、次回のアップデート連携開始時刻までアップデートは実行されません。



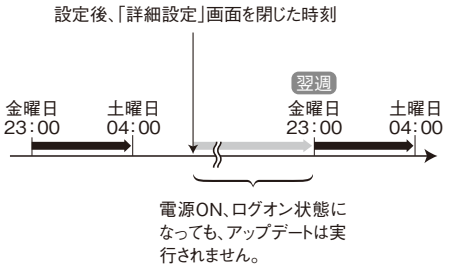
アップデート連携が設定されている時間範囲外にアップデート連携が開始し、アップデート連携の開始時刻を跨ぐ場合、アップデート開始から制限時間（この例では 5 時間）経過するまでアップデートが実行されます。
この場合、実行予定だったアップデート連携はキャンセルされ、次回のアップデート連携開始時刻までアップデートは実行されません。



Point

オプション設定直後のアップデート連携について

「前回開始されなかった場合は、起動時／ログオン時に開始する」オプションを ON にして「OK」を押し、「詳細設定」画面を閉じたのが 4:00 以降とすると、次のアップデート連携実行タイミング (次の 23:00) までの間は、時間範囲外でもアップデート連携は開始されません。
次の実行タイミングの終了時刻（次の 4:00）以降は、時間外でもアップデート連携を開始する対象となります。



除外する項目（保護の対象としない項目）を登録

「保護するドライブと除外フォルダ」タブの「ユーザー除外設定の選択」（34 ページ）において、「Kaspersky2016.ini」が初期値として登録されています。「.ini」ファイルを作成することで、ユーザーが設定した内容で除外を行うことができます。
「.ini」ファイルを登録してクライアント PC に反映するには、以下の手順で操作を行います。

手順 1：除外設定を記述した「.ini」ファイルを作成する
手順 2：作成した「.ini」ファイルを特定フォルダーへ保存
手順 3：「ユーザー除外設定の選択」で「.ini」ファイルを選択し「設定実行」をクリック

手順 1　除外設定を記述した「.ini」ファイルを作成する

メモ帳などで、拡張子が「.ini」のファイルを作成します。「.ini」ファイルを開き、指定の書式で除外する項目を記述します。
「.ini」ファイルの名前は自由につけられますが、区別しやすい名前にすることをおすすめします。
標準で「Kaspersky 2016 / 2017」の「.ini」ファイルが保存されていますので、それを参考にして作成してください。

「.ini」ファイル記述例

```
❶ [WPAVS]
❷ Name= 除外リスト
❸ Enable=1
❹ EnableDef=0
❺ EditMode=0
❻ PathNum=3
❼ RegNum=2
❽ Path0=C:\Program Files\ARK Information Systems Inc\WinProtector\
  Path1=C:\Users\ark\Pictures\
  Path2=C:\ 資料 \Readme.txt
❾ Reg0=HKEY_LOCAL_MACHINE\SOFTWARE\ARK Information Systems Inc.
  Reg1=HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\xxxx
```

❶ [WPAVS]
「.ini」ファイル内でのカテゴリ名で、「.ini」ファイルの先頭に記述します。

❷ Name=
「項目名」に表示する名前を記述します。

❸ Enable=
項目名の有効、無効を設定します。
0：この項目名が無効（「除外する項目の設定」タブで項目名のチェックが OFF）となります。
1：この項目名が有効（「除外する項目の設定」タブで項目名のチェックが ON）となります。

❹ EnableDef=
「標準に戻す」ボタンが押されたときの動作を設定します。
0：「標準に戻す」ボタンが押されたときに、項目を無効（チェックを OFF）にします。
1：「標準に戻す」ボタンが押されたときに、項目を無効（チェックを ON）にします。

❺ EditMode=
登録される項目名の編集を許可するかどうかを設定します。
0：　除外するファイル、フォルダー、保護しないレジストリの編集が不可（「追加」、「削除」ボタンがグレーアウト）となります。
1：　除外するファイル、フォルダー、保護しないレジストリの編集が可能（「追加」、「削除」ボタンが有効）となります。
2：　除外するファイル、フォルダー、保護しないレジストリの編集が不可（「追加」、「削除」ボタンがグレーアウト）となり、かつ、設定されているファイル、フォルダー、レジストリの内容を表示しません。この場合、「この項目は自動的に設定されます。」と表示されます。

❻ PathNum=

除外ファイル、フォルダーの総数を記載します。この「.ini」ファイルの記述例では、2つのフォルダーと1つのファイルが除外されますので、「3」と記載しています。

❼ RegNum=

保護しないレジストリの総数を記載します。この「.ini」ファイルの記述例では、2つのレジストリが除外されますので、「2」と記載しています。

❽ PathX=

「X」には「0」から始まる数字が入ります。「Path0=」のように記載し、その後ろに除外するファイル、フォルダーのパスを記述します。フォルダーを除外する場合は、必ず最後に「\」を付けてください。

❾ RegX=

「X」には「0」から始まる数字が入ります。「Reg0=」のように記載し、その後ろに保護しないレジストリのパスを記述します。「HKEY_LOCAL_MACHINE\ 」を必ず先頭に付けてください。

手順 2 作成した「.ini」ファイルを特定フォルダーへ保存

編集した「.ini」ファイルを、Network Controller クライアントソフトウェアのインストールフォルダーと、クライアント PC の「HD 革命 /WinProtector」インストールフォルダーの下にある「DefExd」というフォルダーに保存します。

●サーバー PC 上の保存先：

C:\Program Files\ARK Information Systems Inc\NCS\DefExd\

●クライアント PC 上の保存先：

C:\Program Files\ARK Information Systems Inc\WinProtector\DefExd\

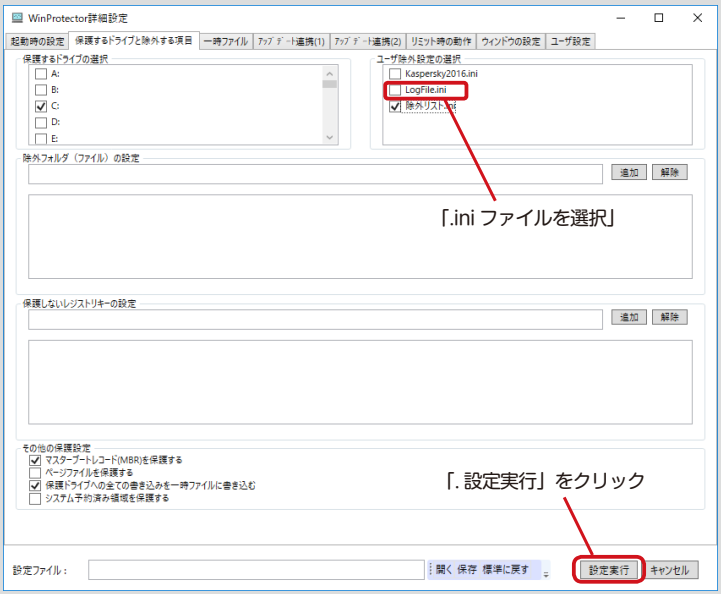
Point

「.ini」ファイルは、「資料配付」機能（16 ページ）で送信することができます。
「送信するファイル：」で編集した「.ini」ファイルを、「クライアント PC 上の保存先：」で以下の場所を指定して実行してください。

C:\Program Files\ARK Information Systems Inc\WinProtector\DefExd\

手順 3 「詳細設定」の「除外する項目の設定」タブを開く

「WinProtector」タブ→「詳細設定」→「保護するドライブと除外フォルダ」と選択します。「ユーザー除外設定の選択」で、手順 1 で作成した「.ini」ファイルをチェックして、「設定実行」をクリックします。「.ini」ファイルを保存しただけでは除外設定は有効になりませんので、必ずこの操作を行いクライアント PC に設定を反映するようにしてください。



除外設定は、クライアント PC の保護が行われていない状態で行ってください。保護された状態で操作を行っても設定が反映されません。

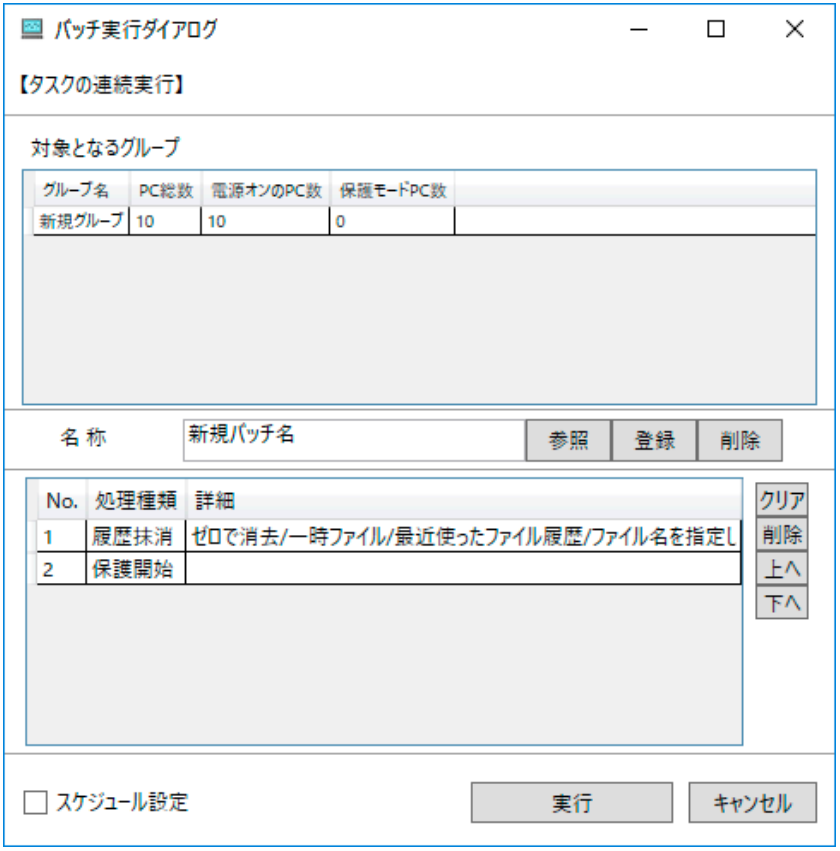
タスクの連続実行、その他のツール（「ツール」タブ）

「ツール」タブでは、バッチ登録によるタスクの連続実行と、実行した操作の履歴を確認できます。

連続実行

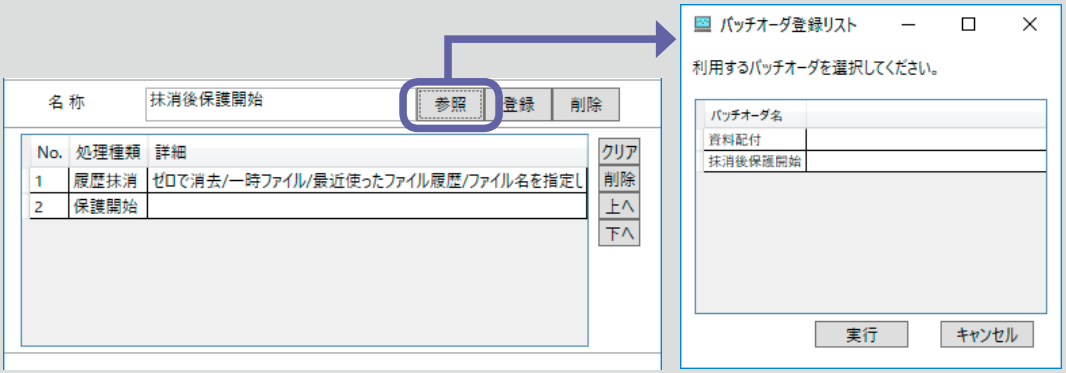
■連続実行

各操作画面で「バッチに追加」をクリックすると、設定した内容で「タスク」が下の画面に追加されます。登録されている順番でタスクを連続実行できます。



バッチオーダー登録

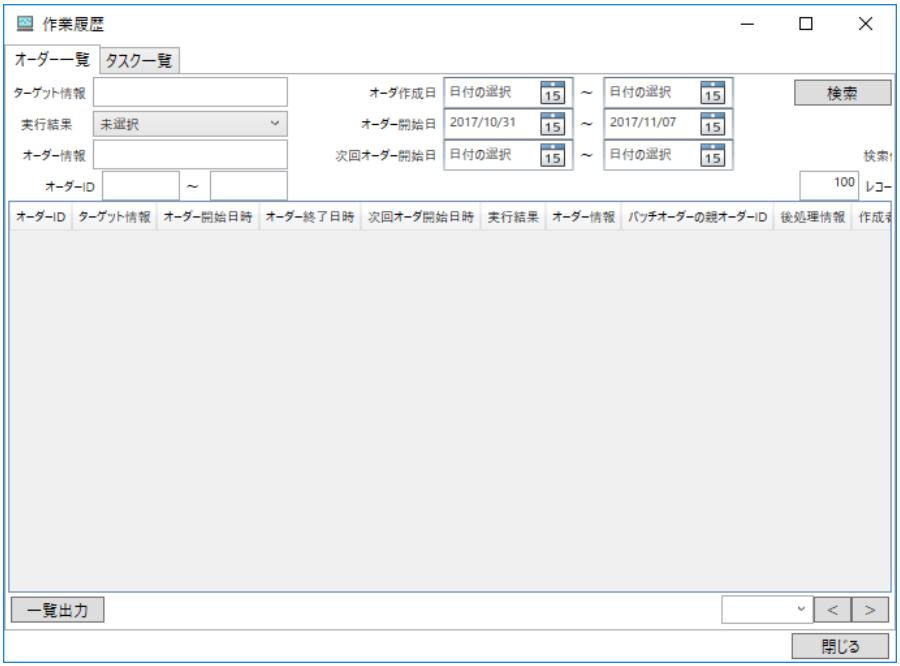
「バッチ実行ダイアログ」画面では、登録されているタスクの内容を登録（保存）することができます。これにより、特定のオーダーを繰り返し行うような場合に、登録した情報を読み込むことで簡単に追加できるようになります。
登録したバッチオーダーは、「参照」をクリックして呼び出します。



作業履歴

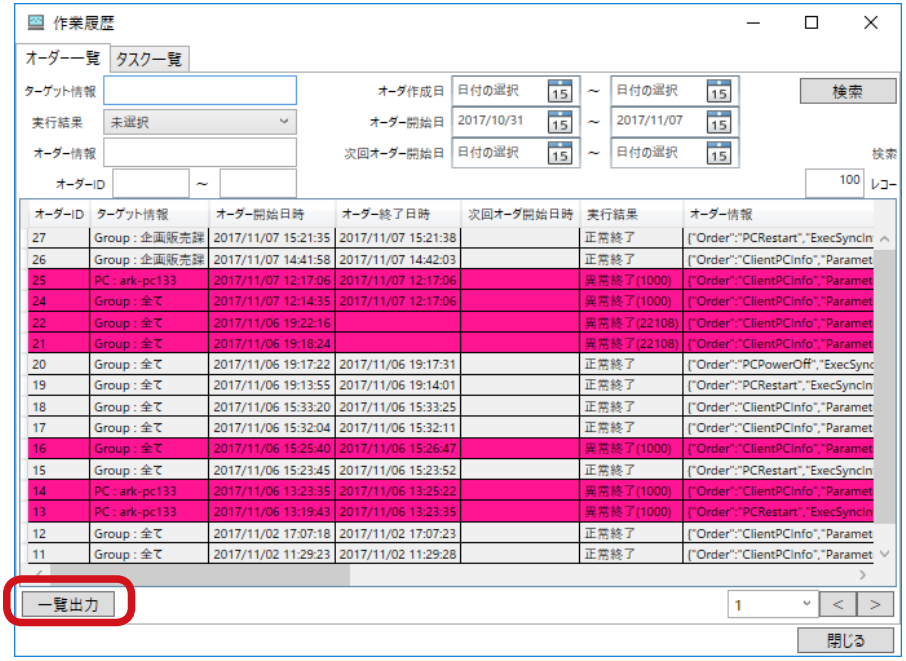
■作業履歴

「作業履歴」画面では、オーダーおよびタスクの履歴を確認できます。「検索」をクリックするとオーダーまたはタスク一覧が表示されます。オーダーおよびタスクは、画面上の検索欄で条件を指定することで絞り込みが可能です。

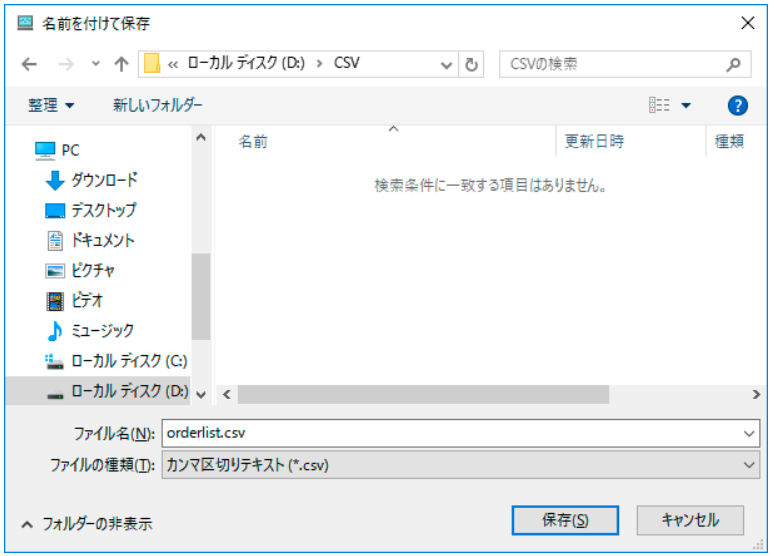


■作業履歴―「オーダー一覧」タブ

「オーダー一覧」タブを選択して「検索」をクリックすると、実行されたオーダーの一覧が表示されます。「ターゲット情報」と「オーダー情報」で検索を行う場合は、文字列を入力します。必要に応じて日付や文字列で絞り込みを行ってください。

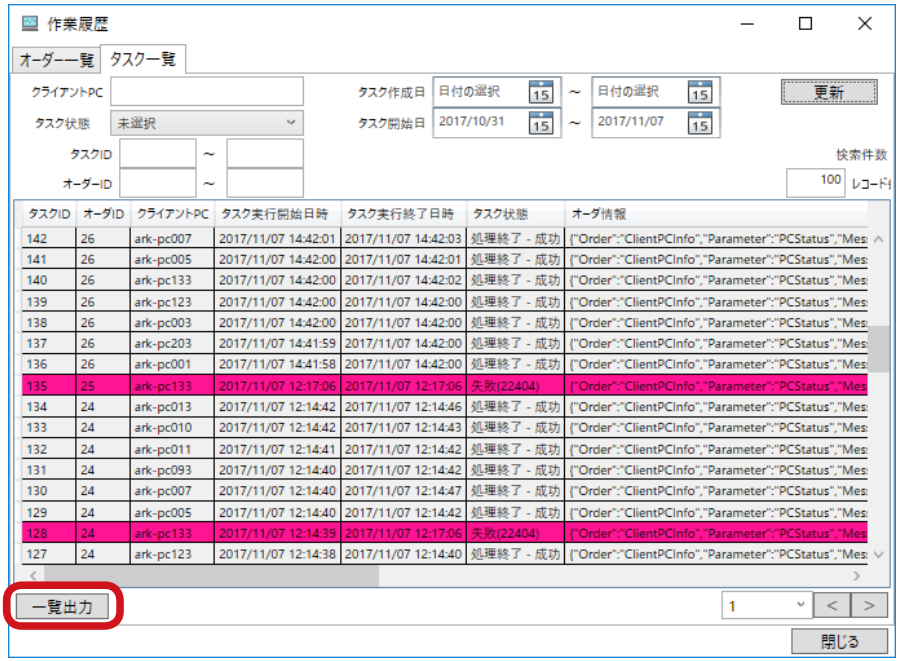


「一覧出力」をクリックすることで、表示されている内容を CSV ファイルに出力できます。

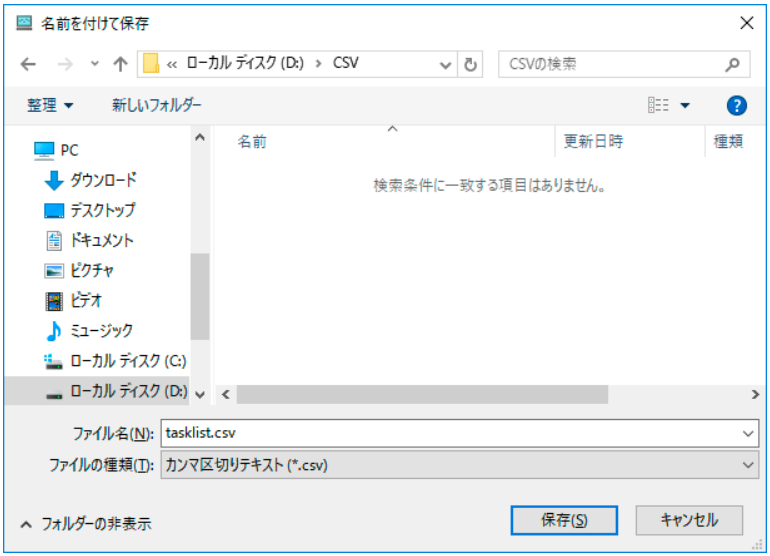


■作業履歴―「タスク一覧」タブ

「タスク一覧」タブを選択して「検索」をクリックすると、実行されたタスクの一覧が表示されます。「クライアント PC」で検索を行う場合は、文字列を入力します。必要に応じて日付や文字列で絞り込みを行ってください。



「一覧出力」をクリックすることで、表示されている内容を CSV ファイルに出力できます。



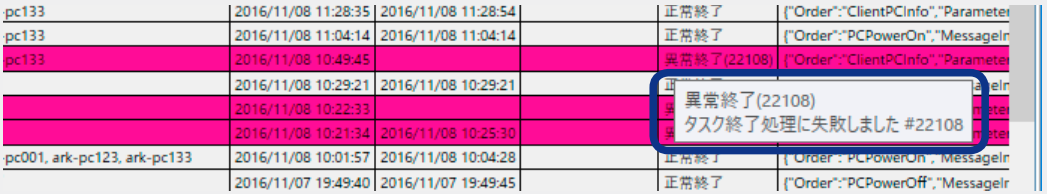
再実行と履歴の削除

オーダーまたはタスクの履歴画面で右クリックするとメニューが表示されます。選択した行のオーダーまたはタスクの再実行や履歴の削除を行うことができます。オーダーにおいては、この画面からタスクスケジューラーに登録されているスケジュールを削除することもできます。

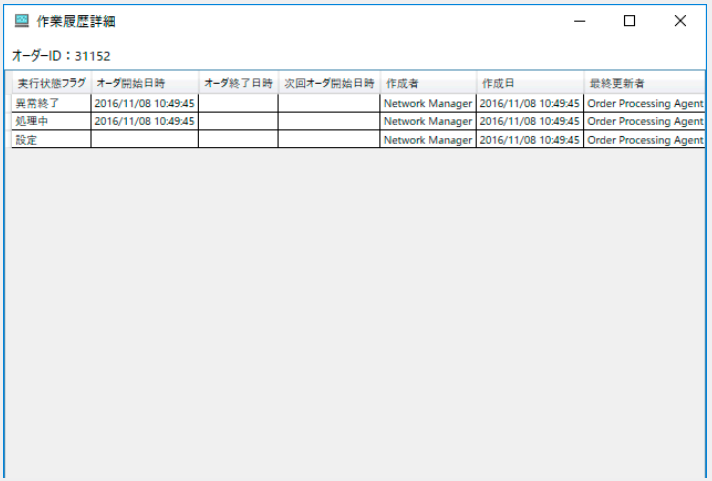
●オーダーの右クリックメニュー

●タスクの右クリックメニュー

エラーが発生したオーダーまたはタスクは色がついた状態で表示され、「タスク状態」欄でマウスポインタをかざすとエラー内容がポップアップします。



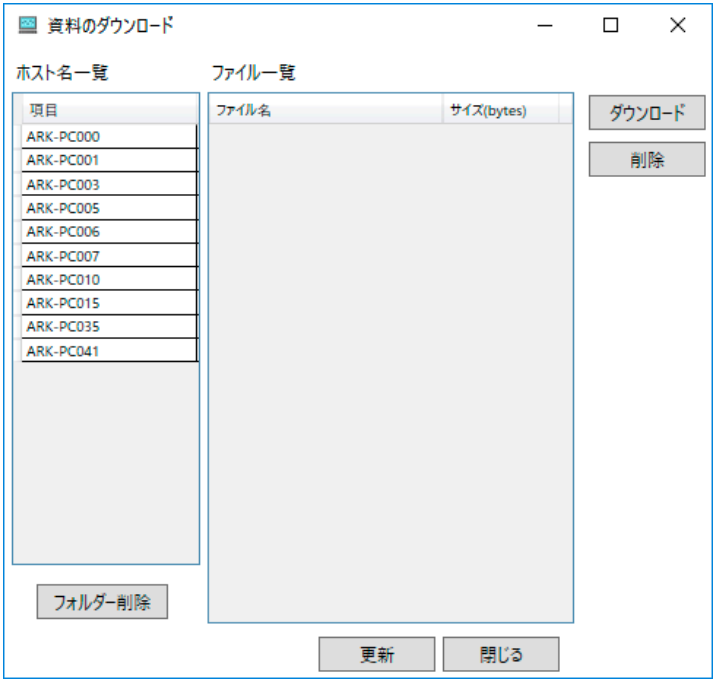
右クリックメニューで「履歴の詳細表示」を実行すると、選択したオーダー ID またはタスク ID における詳細を確認できます。



FTP

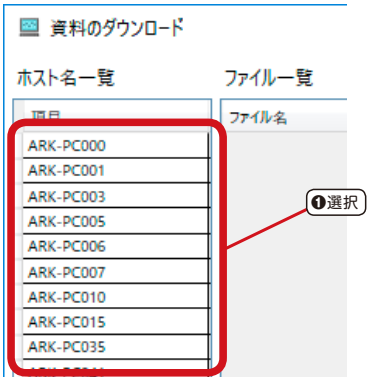
■ダウンロード

「資料収集」で収集したファイルは FTP サーバーに保存されます。「ダウンロード」をクリックすると下の画面が表示されますので、この画面から FTP サーバーに保存されているファイルをダウンロードします。ファイルは、クライアント PC 単位で保存されています。

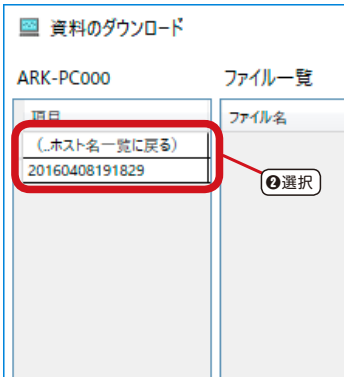


ファイルのダウンロードは、次の手順で行います。

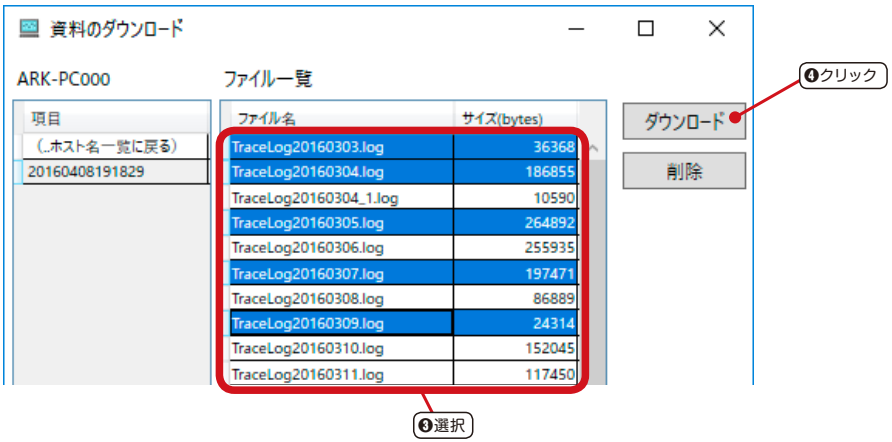
①画面左の「ホスト名一覧」で対象のクライアント PC を 1 つ選択します。



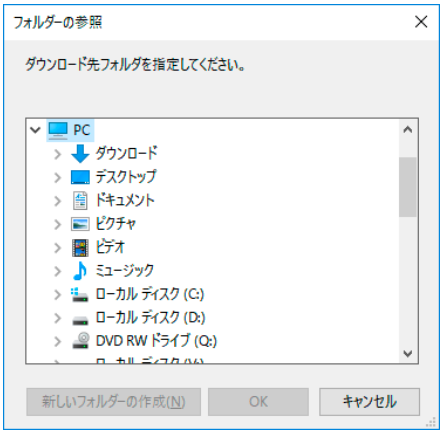
②アップロードした日付のフォルダーが表示されますので、1 つフォルダー選択します。



③「ファイル一覧」にファイル名が表示されます。対象のファイルを選択（複数可）して「ダウンロード」をクリックします。



④フォルダー選択ダイアログが表示されるので、ダウンロードしたいファイルを選択し、「OK」ボタンを押します。



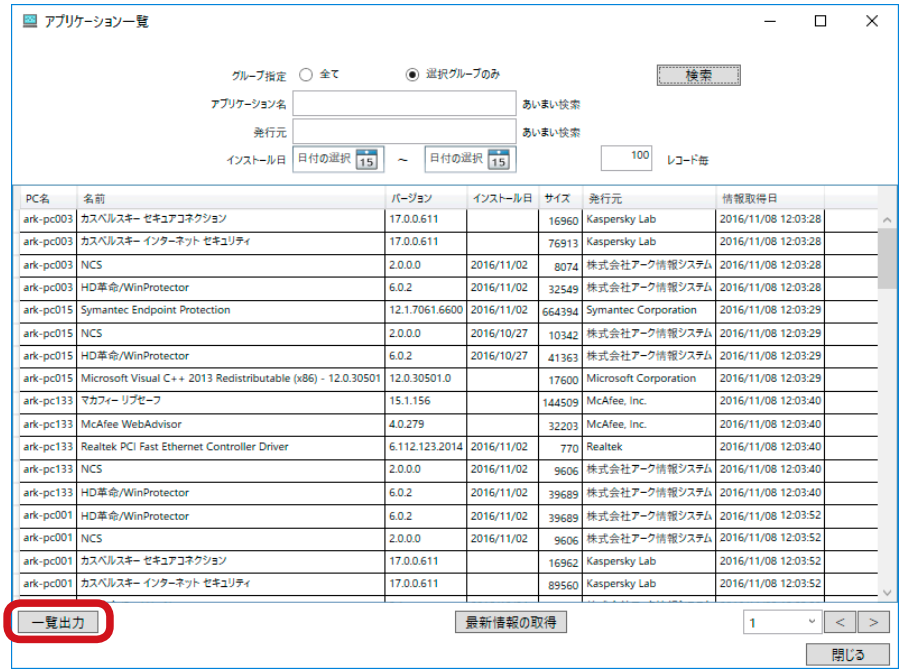
FTP サーバー上のファイルを削除したい場合は、ダウンロードと同じ手順を行い「削除」をクリックします。また、ファイルが置かれているアップロードした日付のフォルダーを削除する場合は、左側のリストでフォルダーを選択し、左下の「フォルダー削除」ボタンをクリックします。フォルダーを削除するとフォルダー内のファイルも同時に削除されます。なお、ホスト名（この例では ARK-PC000 など）は削除できません。

⚠ FTP サーバー内のファイルは自動的に削除されません。ディスク容量が一杯になるとファイルを保存できなくなりますので定期的に整理（削除）してください。

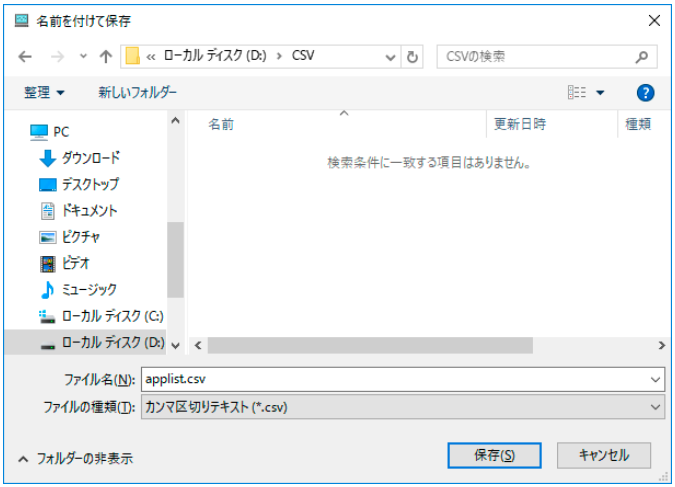
PC 情報

■アプリケーション一覧

メイン画面において、所属するグループに登録されているクライアント PC にインストールされているアプリケーション一覧を取得し表示します。画面上の検索欄で条件を指定することで絞り込みが可能です。「アプリケーション名」と「発行元」で検索を行う場合は、文字列を入力してください。表示されている内容は、画面左下の「一覧出力」より CSV ファイルで保存できます。



「一覧出力」をクリックすることで、表示されている内容を CSV ファイルに出力できます。

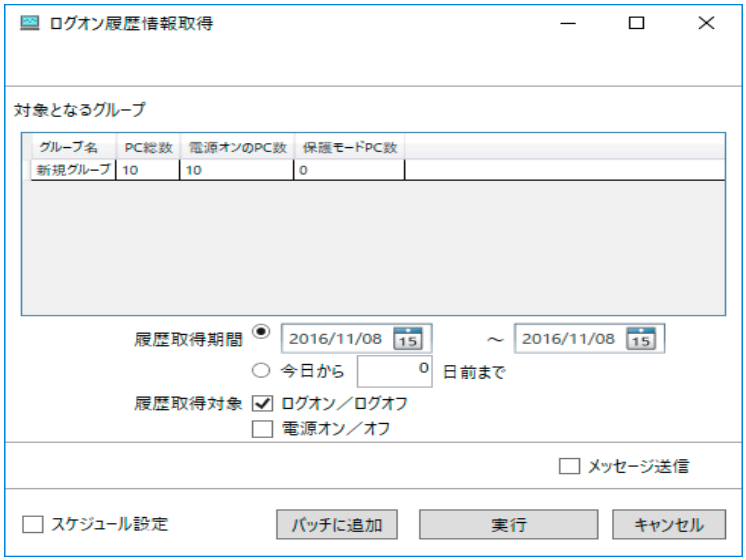


■ログオン履歴

メイン画面で選択したクライアント PC のログオン／ログオフ、電源オン／オフの履歴を取得します。取得した情報は FTP サーバーにファイル名に日時が入った CSV ファイル（例：2016/11/09 18：52：07 の場合は「lhist20161109185207.csv」）として保存されますので、ダウンロード（54 ページ）を行ってください。

● CSV ファイルに出力される項目

状態：状態表示（PowerOn,PowerOff,Logon,Logoff, Wakeup, Sleeping）
日時：発生日時
名前：ログオン／ログオフしたアカウント
ドメイン名：ログオンアカウントのドメイン名（マシン名と同じ場合はローカルアカウント）
マシン名：クライアント PC のコンピューター名
IP アドレス：IPv4 アドレス（リモートからログオンした場合はリモート端末の IP アドレス）
Subject ユーザ名：クライアント PC のコンピューター名
Subject ドメイン名：ワークグループまたはドメイン名

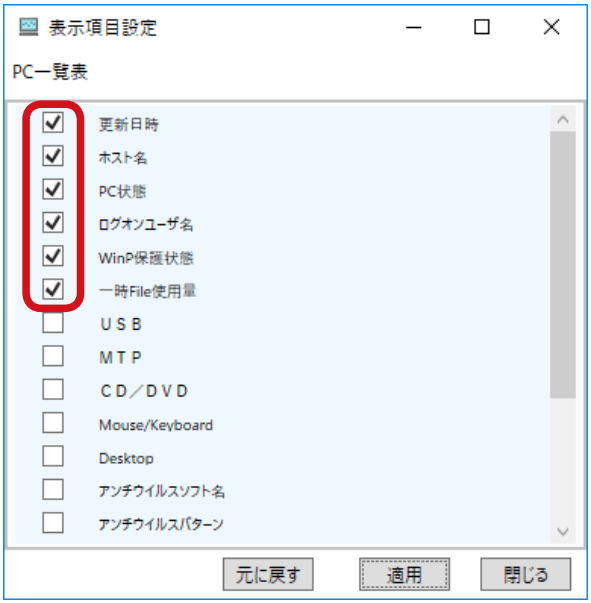


・取得する履歴は、クライアント PC の Windows イベントログファイルから取得しますので、取得可能な期間はイベントログファイルに依存します。
・クライアント PC が HD 革命 /WinProtector で保護されている間は、再起動することでイベントログに書き込まれた情報も破棄されてしまうので、行われた操作履歴を取得できません。

カスタマイズ

■ PC 一覧表

メイン画面右側の PC 一覧において表示する項目を選択します。



「表示項目設定」画面でチェックを入れた項目がメイン画面に表示されるようになりますので、必要な情報が見やすくなります。

スケジュールの設定

各操作画面下にある「スケジュール設定」にチェックを入れ、スケジュールを設定して操作を実行することができます。画面が下に延びてスケジュールを登録することができます。スケジュールを設定する場合は、バッチ処理との併用はできません。

● 1 回のみ有効

1 回のみ有効なスケジュールです。「開始日」に過去の日時が指定された場合は、抹消が即時実行されます。

●週単位でスケジュール

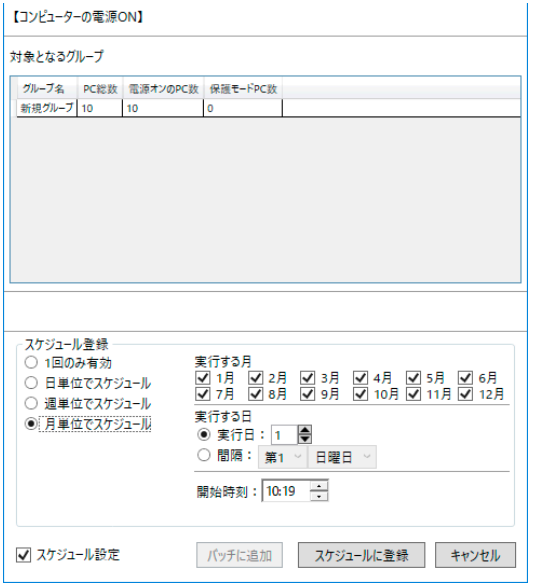
週単位のスケジュールでは、週の特定の曜日、特定の時間にスケジュールを実行することができます。一定の間隔でスケジュールを実行するには、「間隔」を 1 週 (毎週) ～ 52 週 (1 年ごと) の範囲で入力します。

●日単位でスケジュール

日単位のスケジュールでは、毎日または一定の間隔でスケジュールを実行することができます。「開始日」に過去の日時が指定された場合は、登録日を起点として次回のスケジュールが計算されます。一定の間隔でスケジュールを実行するには、「間隔」は、1 日 (毎日) ～ 365 日 (1 年ごと) の範囲で入力します。

●月単位でスケジュール

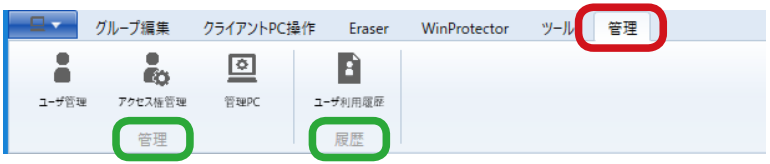
月単位のスケジュールでは、特定の月、特定の日にスケジュールを実行することができます。「実行日」は 1 日～ 31 日が指定できますが、2 月 30 日や 31 日のない月で 31 日を指定すると、実行できる日時が存在しないためスケジュールが実行されません。



ユーザー管理（「管理」タブ）

「管理」タブでは、メイン画面を起動するユーザーや操作できる機能を制限することができます。

これにより、システム管理者には Network Controller のすべての操作を行う権限をもたせ、オペレーターには特定の機能のみ実行可能にすることができるようになります。

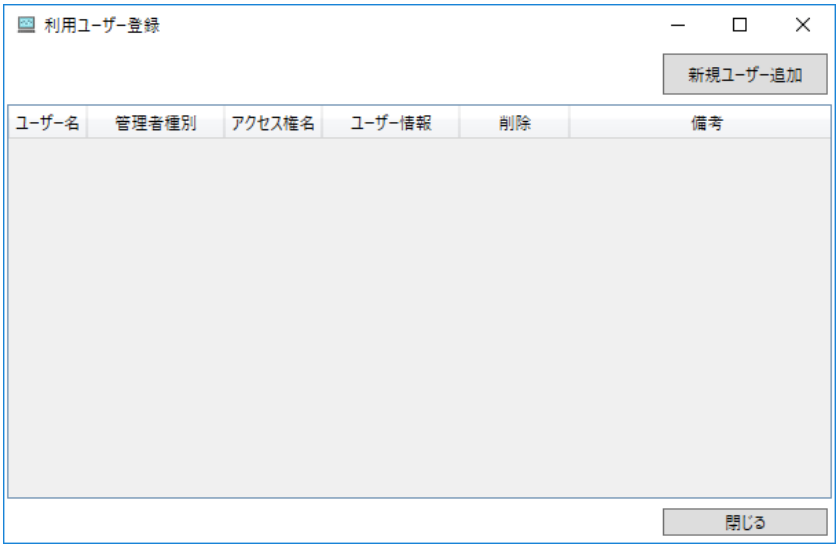


管　理

■ユーザー管理

メイン画面で「ユーザー管理」をクリックすると、ユーザー登録の画面が表示されます。

ユーザーを登録することでメイン画面の起動時にログイン画面で「ログイン名」と「パスワード」の入力が求められるようになりますので、セキュリティ対策となります。

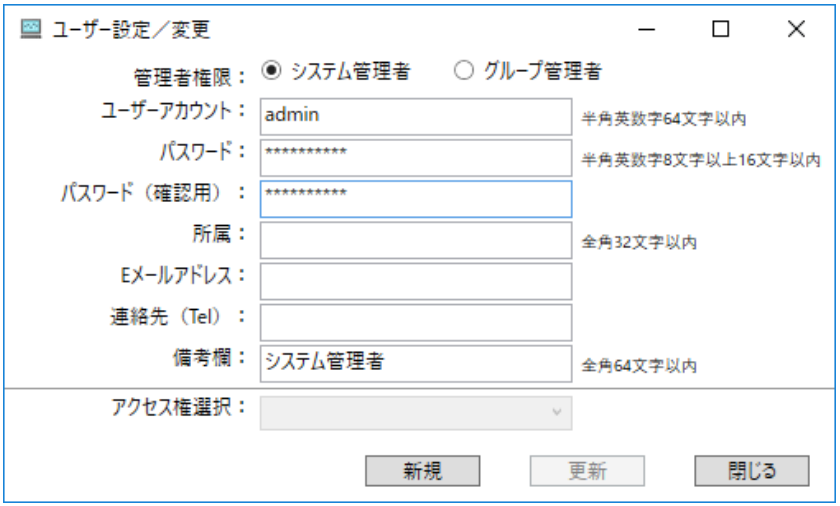


「新規ユーザー登録」をクリックしてユーザーアカウント、パスワード、その他必要な情報を入力して「新規」をクリックします。

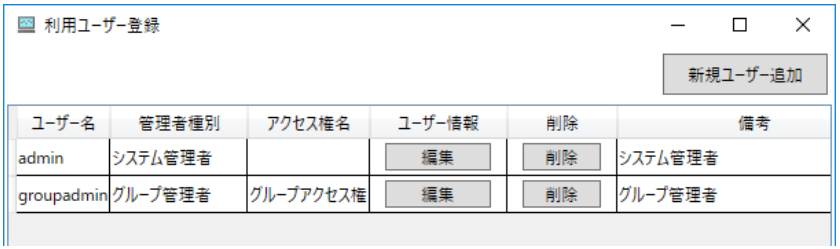
登録するユーザーを「システム管理者」とする場合、Network Controller のすべての操作を行うことができます。

登録するユーザーを「グループ管理者」とする場合、後述の「アクセス権管理」で設定したアクセス権を選択できます。

なお、「グループ管理者」メイン画面「管理」タブでの操作はできません。

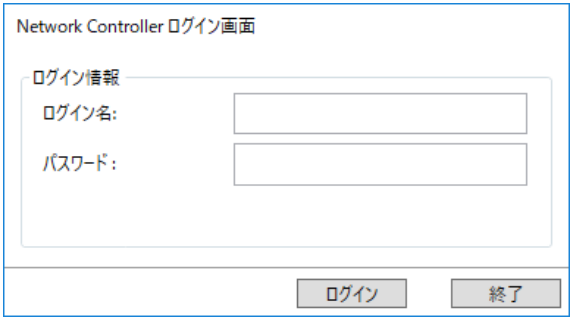


ユーザーは複数登録することができます。他のユーザーを登録するには、上記操作を繰り返し行います。



初期状態ではユーザーが１つも登録されていないため、メイン画面の起動時にユーザーアカウントとパスワードの入力はありません。しかし、ここで新規にユーザー登録を行うと、起動時に右のログイン画面が表示されます。

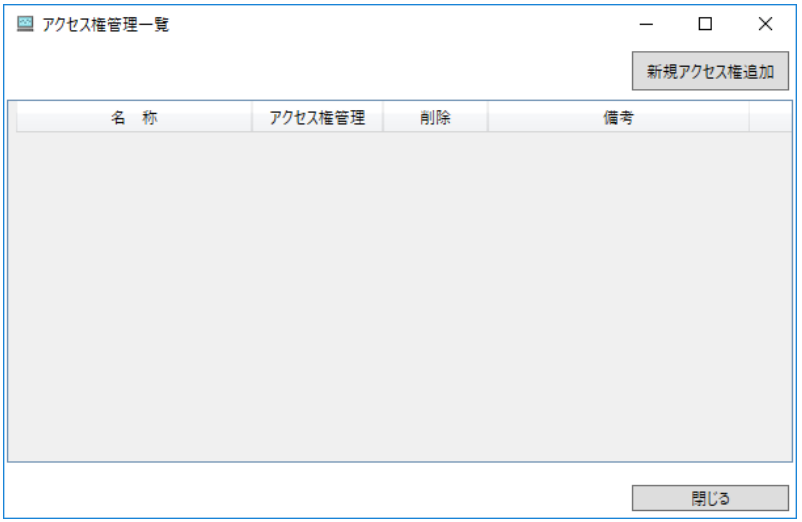
上記の「利用ユーザー登録」画面では、最低１つはユーザーが登録されていなければならず、すべてのユーザーを削除することはできません。



■アクセス権管理

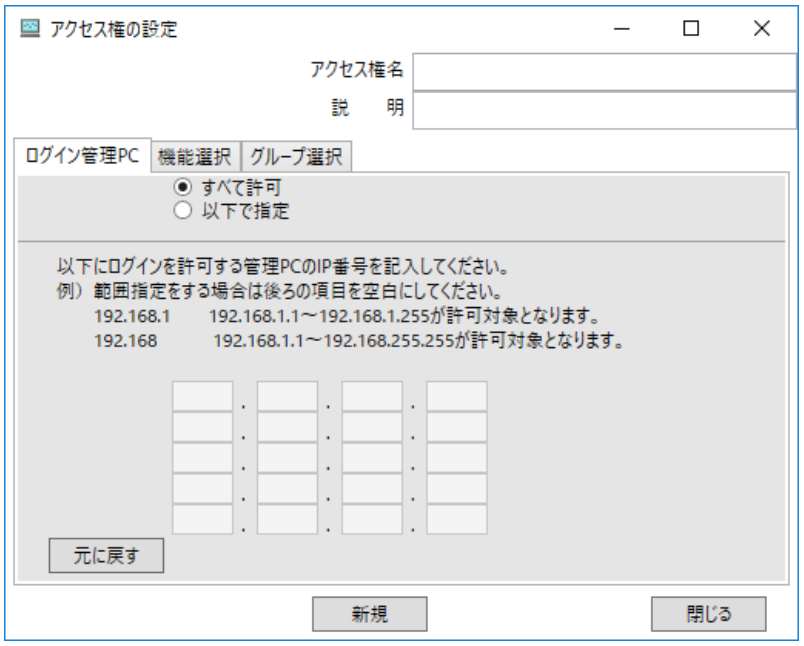
「ユーザー管理」で追加したユーザーに対してアクセス権を設定することで、メイン画面での操作を制限することができます。

アクセス権の追加は、ユーザー管理でユーザーを登録する前に行ってください。



「新規アクセス件追加」をクリックすると、次の「アクセス権の設定」画面が表示されます。

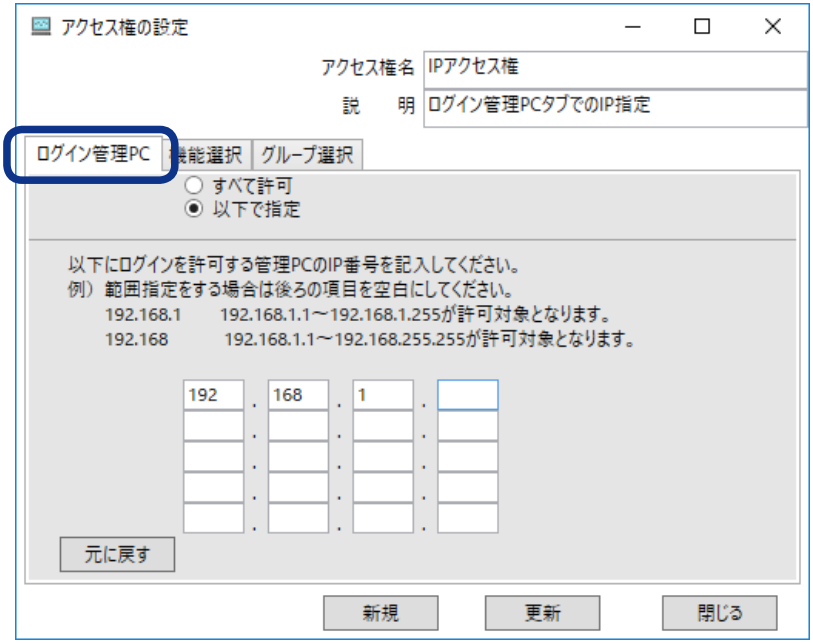
ここでは、IP、メイン画面で選択できる機能、クライアント PC が所属するグループから必要な設定を行います。



●ログイン PC 管理

「ログイン管理 PC」タブでは、「ユーザー管理」で登録したユーザーが利用可能な管理 PC を IP で制御することができます。

「以下で指定」を選択し、フィールドに固定 IP、または IP の範囲を入力しますが、IP の指定にワイルドカード（＊、？）は使用できません。



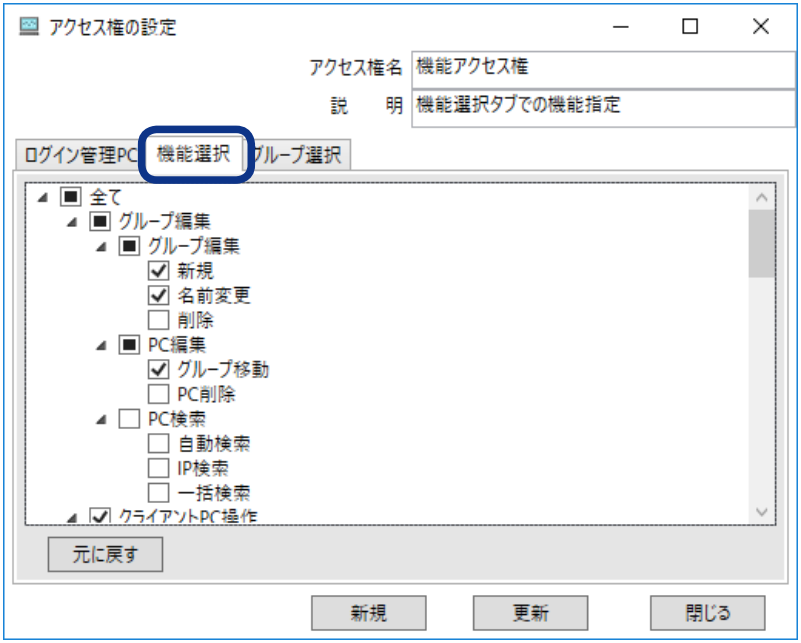
《アクセス権設定例》

・ネットワーク環境に Network Controller がインストールされた 2 台の PC があるものとします。
　管理 PC1　……（IP：192.168.1.10）
　管理 PC2　……（IP：192.168.1.20）
・Network Controller の上記の「ログイン管理 PC」タブで、それぞれ次のようにアクセス権を指定した 2 つのユーザーがあるものとします。
　User1……「192.168.1.10」と設定
　User2……「192.168.1. 空欄」と設定
・このような場合、
User1 は、管理 PC1 で Network Controller を起動（ログイン）することができますが、管理 PC2 では Network Controller を起動（ログイン）することができません。
User2 は、管理 PC1 と管理 PC2 で Network Controlle を起動（ログイン）することができます。

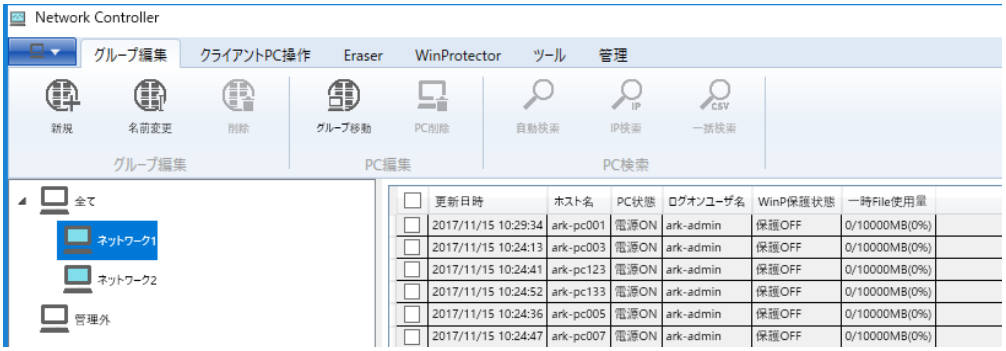
このように、登録するユーザーと IP を紐付けることで、他の場所にある Network Controlle での操作を制限することができるようになります。

●機能選択

「機能選択」タブでは、「ユーザー管理」で登録したユーザーがメイン画面で使用できる機能を指定します。

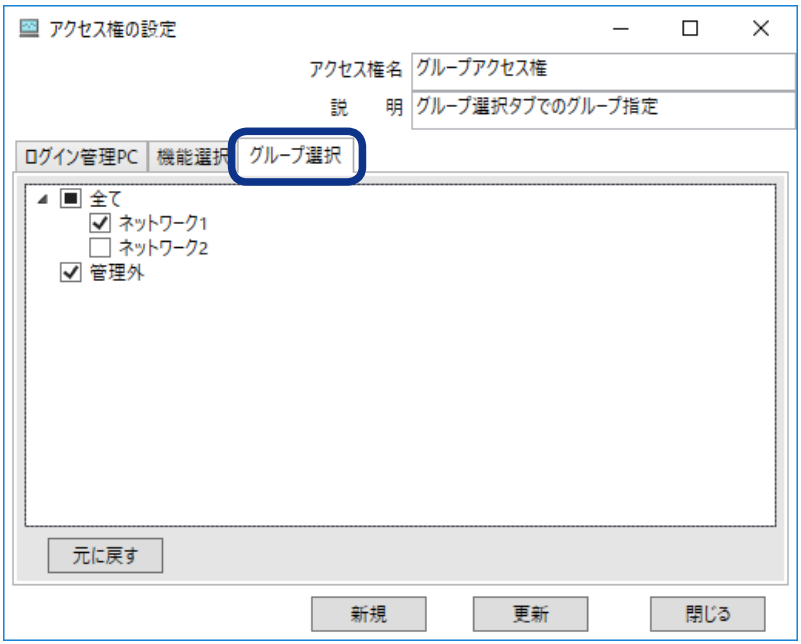


アクセス権を設定したユーザーで Network Controller を起動（ログイン）した場合、「機能選択」タブで選択されていない機能はメイン画面でグレー表示となり使用できなくなります。

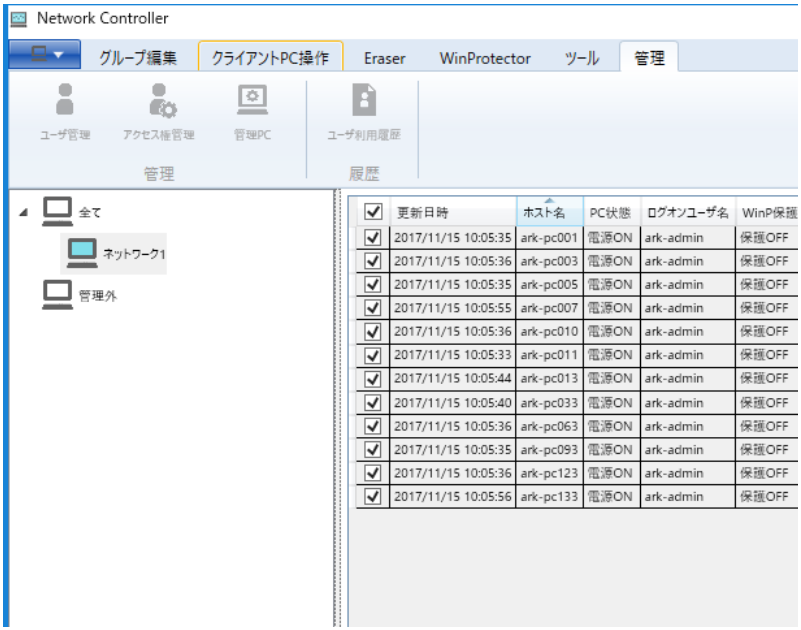


●グループ選択

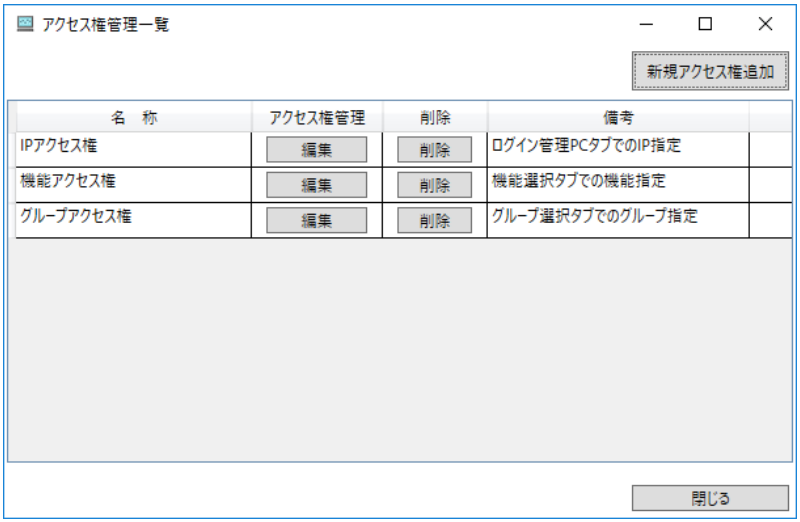
「グループ選択」タブでは、「ユーザー管理」で登録したユーザーがメイン画面で使用できるグループを指定します。



アクセス権を設定したユーザーで Network Controller を起動（ログイン）した場合、「グループ選択」タブで選択されていないグループはメイン画面で表示されなくなります。



アクセス権の設定規則は複数作成することができます。アクセス権を追加するには、これまでの操作を繰り返し行います。

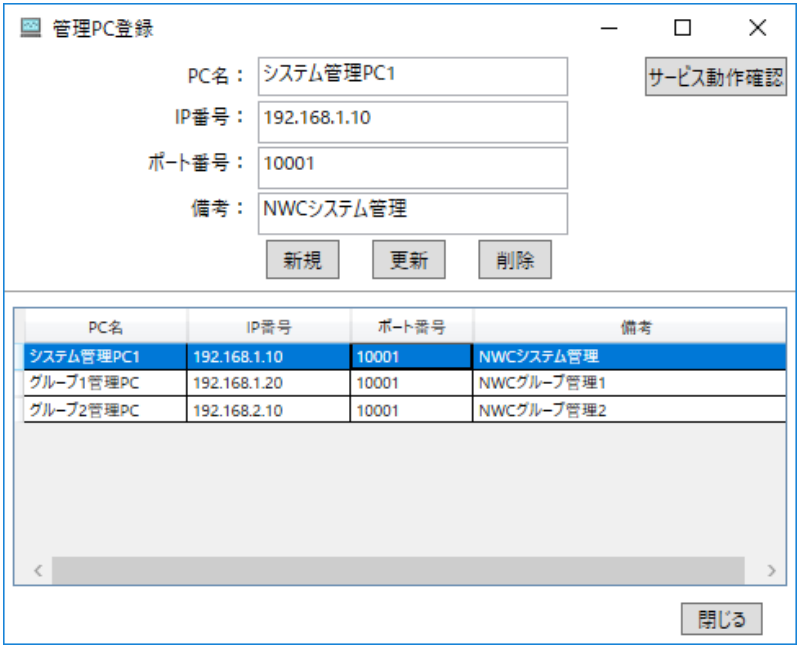


■管理 PC

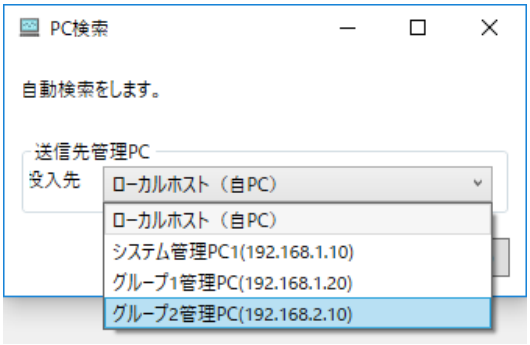
使用しているネットワークが複数のサブネットで構成され、それぞれのサブネットに管理 PC が置かれているとします。

「管理 PC 登録」画面で各サブネットの管理 PC を登録することで、そのサブネット内にある接続可能なクライアント PC を検索することができます。

検索された PC はメイン画面に登録され、他のサブネットのクライアント PC に対して資料配付などの各操作、HD 革命 /WinProtector による保護を行うことができるようになります。



「管理 PC 登録」画面で管理 PC を登録すると、「グループ編集」タブの PC 検索の各機能（＊ページ）で送信先管理 PC を選択することができる画面に変わります。

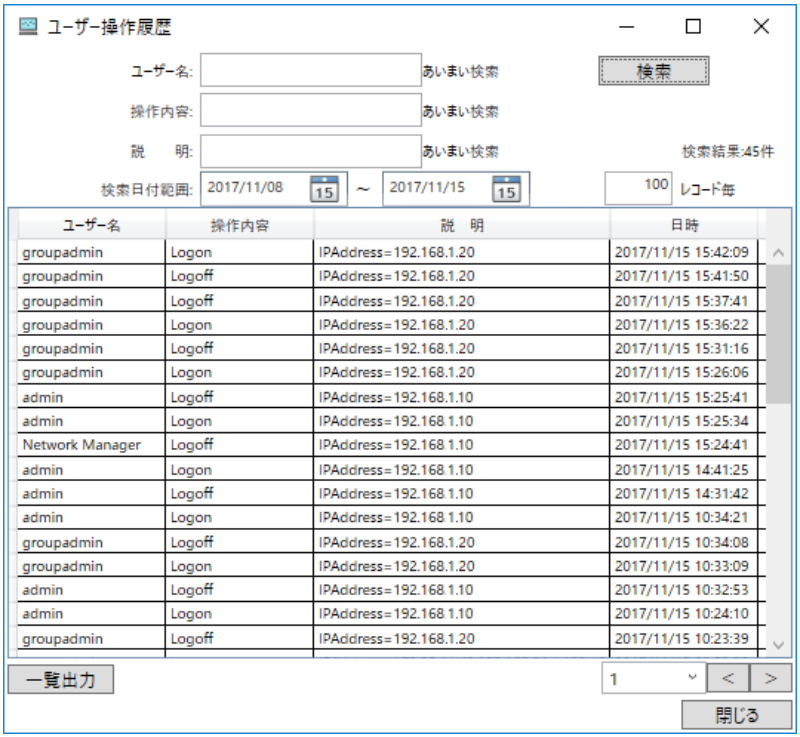


履　歴

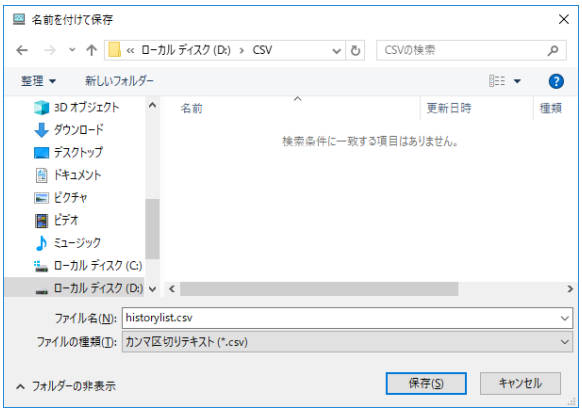
■ユーザー利用履歴

「ユーザー利用履歴」では、どのユーザーがいつ Network Controller を起動（ログイン）したかを一覧で表示することができます。履歴が多い場合などは、ユーザー名などで絞り込み検索も可能です。

なお、ユーザー名の欄が「Network Manager」となっているものは、ユーザーが登録されていないため、ログイン名とパスワードを入力せずに Network Controller を起動したことを表しています。



「一覧出力」をクリックすることで、表示されている内容を CSV ファイルに出力できます。

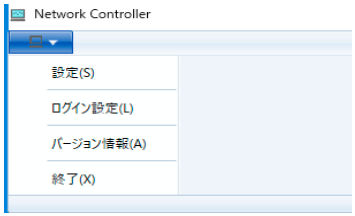


その他の機能（メイン画面から）

メイン画面から、データベースサーバーの設定、ライセンス情報の確認、クライアント PC の詳細情報の出力などが可能です。

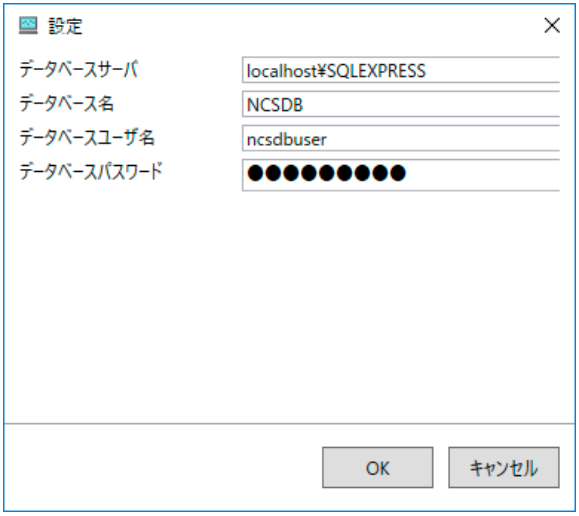
データベース設定とライセンス情報の確認

メイン画面の左上のメニューを開きます。



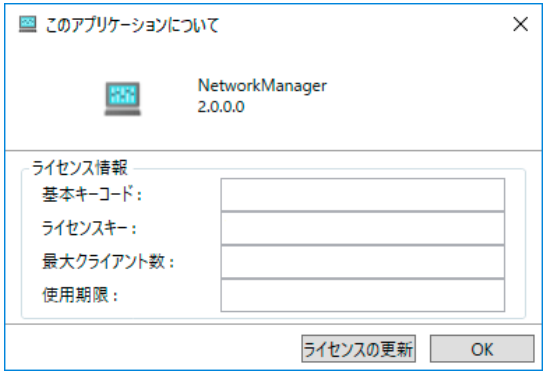
●データベースサーバーの設定

メニューで、「設定」を選択すると、データベースサーバーの詳細を確認できます。サーバーを変更するには、この画面でサーバー名を変更してください。



●ライセンス情報の確認

メニューで、「バージョン情報」を選択すると、Network Controller のライセンス情報を確認できます。ライセンス期間が切れた場合など、新しいライセンスキーを入力する場合はこの画面から行ってください。

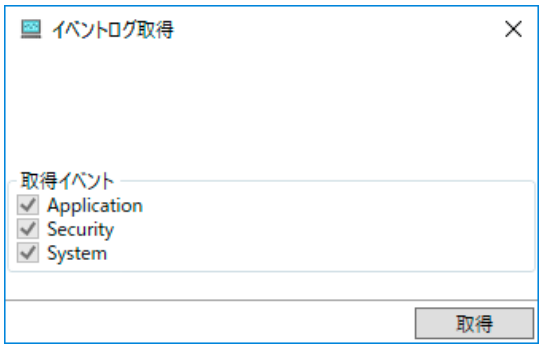


クライアント PC の情報確認

メイン画面で、「クライアント PC 一覧」を右クリックしてメニューを開きます。

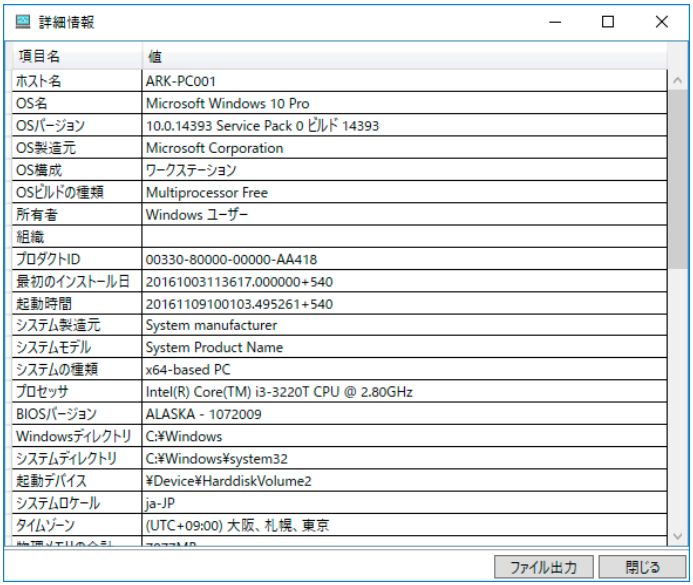
●イベントログ

クライアント PC のイベントログを取得します。



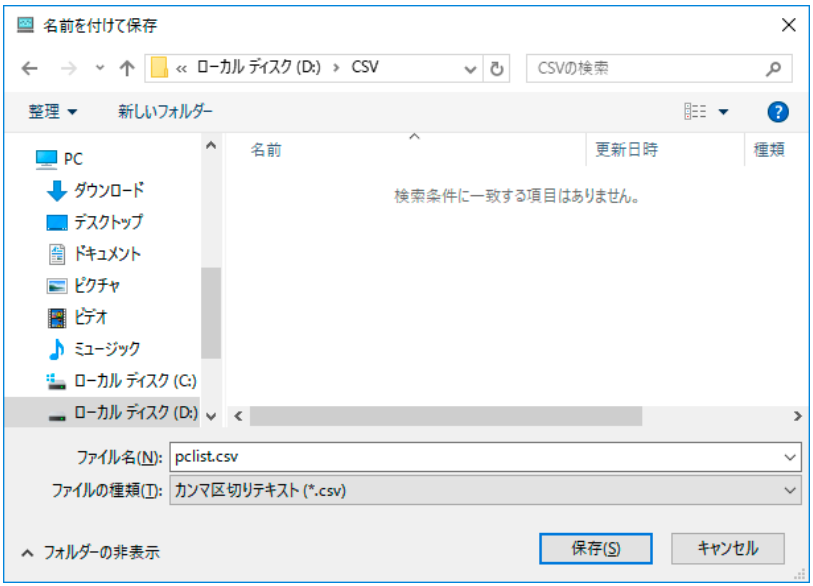
●詳細情報

クライアント PC の情報を表示します。CSV ファイルに出力することができます。



●一覧出力

クライアント PC 一覧を CSV ファイルに出力します。



・本ユーザーズ・マニュアルは PDF ファイルとして提供しており、Adobe Reader（Adobe 社の閲覧ソフトウェア）を使用し、オンラインマニュアルとしてご利用いただくことができます。
・Adobe Reader はセットアップ画面からインストールすることができます。

Network Controller ユーザーズ・マニュアル

2017 年 12 月 1 日　第 5 版発行
発　行　株式会社アーク情報システム
〒 102-0076　東京都千代田区五番町 4- 2　東プレビル