HD革命/WinProtector Ver.8

Network Controller / Standard

イーディーコントライブ株式会社

第1版

パソコンの利用後、再起動１回で元の状態へ戻すソフトウェアです

再起動・シャットダウンのタイミングで、利用中の操作を無効化し、
利用前の環境に戻すソフトウェアです。

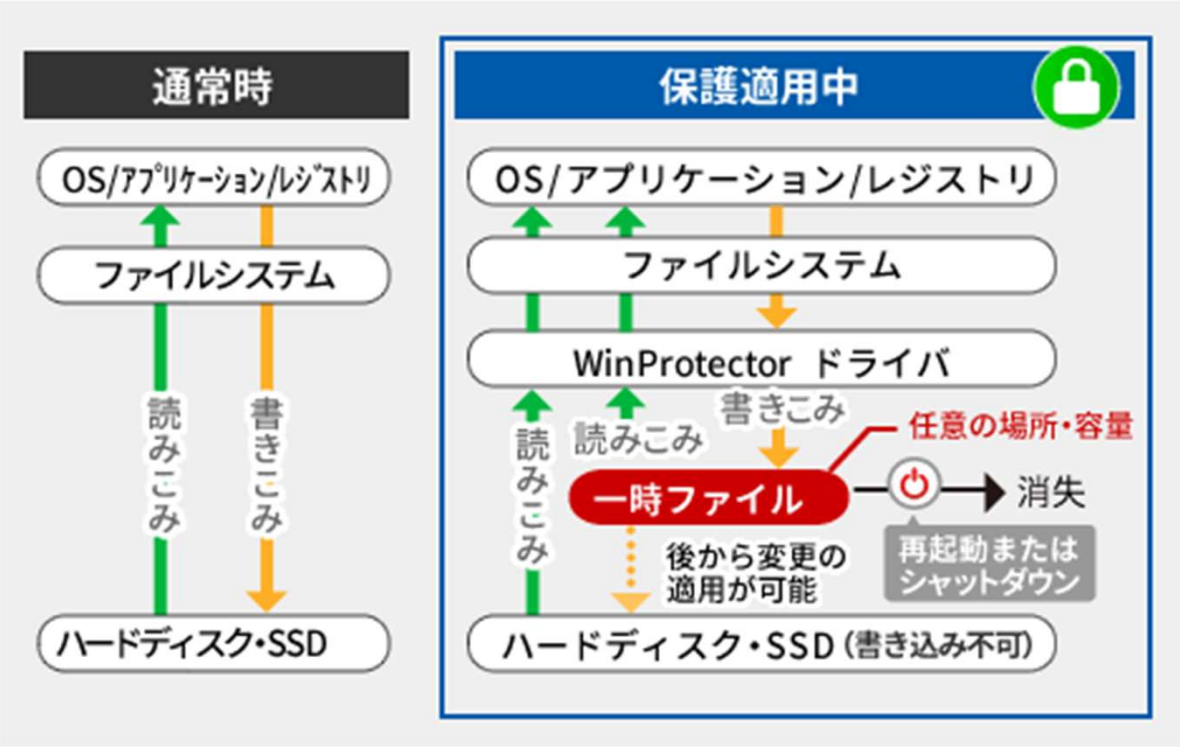
情報漏えい防止　**改ざん防止**　**保守コスト削減**

パソコンに不要なデータが残らないので、利用者の個人情報の漏えいリスクを軽減します。
意図的な改ざんの防止、外部からの攻撃や侵入を防御、クリーンな状態の維持などにより、
保守コストの削減にもつながります。

HD革命/WinProtector とは…　環境復元のしくみ

任意のハードディスクドライブへの書き込みをすべて「HD革命/WinProtector」が作成した一時ファイルに退避（書き込み）します。
再起動・シャットダウン・保護解除のいずれかのタイミングで一時ファイルを破棄することで、保護中の操作を全て無効にし、保護を開始した状態に戻す、『環境復元ソフト』です。

HD革命/WinProtector 使用時のデータの流れ



一時ファイルの保存先は、任意のメモリやハードディスクを指定することができます。
同様に記憶する容量についても指定が可能です。
また、一時ファイルの使用量が任意の値になると、メッセージやアラームでユーザに通知することも可能です。

HD革命/WinProtector とは…　環境復元機能を支えるさまざまな機能

「HD革命/WinProtector」では、お使いの環境に合わせた様々な設定が可能です。

- 導入時に便利な設定情報入出力、サイレントインストール
- ドライブ毎の保護設定
- パスワード設定
- ウィンドウ（クライアント側画面）の表示/非表示設定
- 一時ファイルの保存先・容量指定

  一時ファイルを内蔵ハードディスク以外にメモリーに保存することができ、高速の環境復元が可能です。

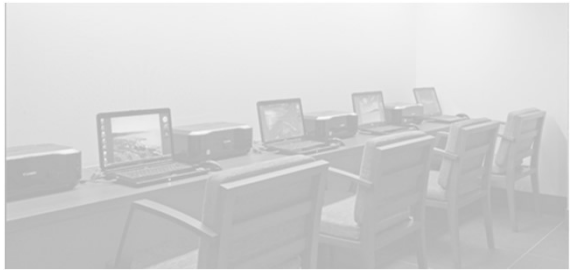
- Windows Update 連携（⇒P.9～P.10 New!）
- アンチウイルスソフトの更新連携（⇒P.9～P.10 New!）
- ログオンユーザー毎の保護・権限設定
- 保護除外フォルダー設定（フォルダ/ファイル/レジストリキー）
- トラブル時の救済措置を強化 New!
- 継続保護設定

  再起動後も保護を継続することが可能です。再起動が必要なソフトウェアのインストールも可能です。
  ※GPTディスク環境では対応しておりません。

環境復元ソフトの利用シーン

不特定多数の方が利用するパソコン

- 学校のPCルーム、PC教室で。
- インターネットカフェ、マンガ喫茶で。
- ホテルや図書館、公共施設などのインターネットコーナーで。
- パソコンショップなどの展示コーナーで。



貸出用のパソコン

- ホテルのレンタルパソコンに。
- 授業や会議時の貸出用パソコンに。
- 展示会など一時レンタルサービスに。
- 病院の患者レンタル用タブレットに。

Windows環境の固定が必要なパソコン

- 精密な結果が常に求められる機器に。
- ソフトウェアの検証に。
- 疑似シンクライアント環境として。

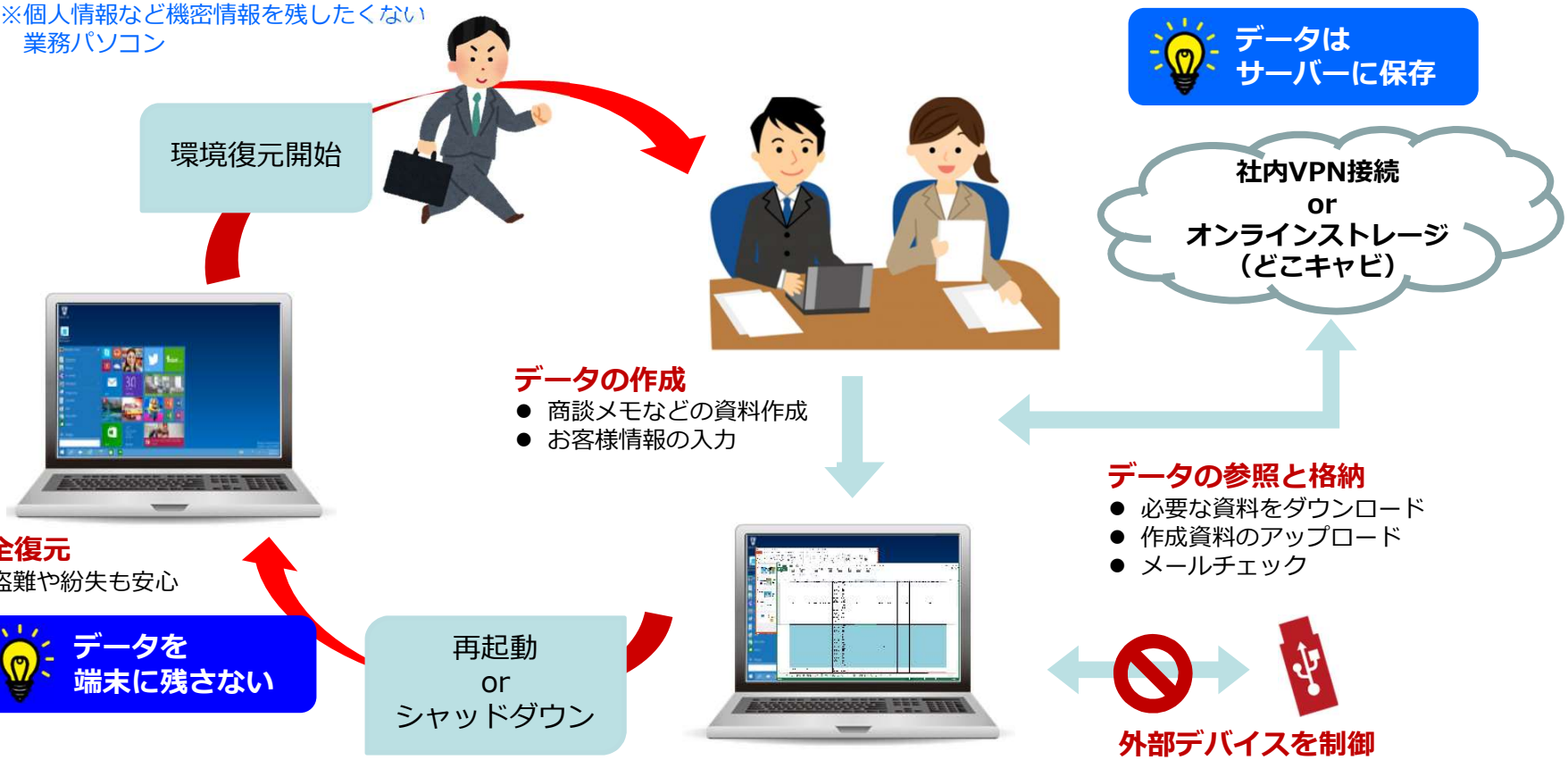
さまざまな場所に持ち出すパソコン

- 営業マンがお客様先へ。
- 技術作業員が現場へ。
- 企業内、部内の共有パソコンにも。

環境復元ソフトの利用シーン①

持ち出しパソコンの場合

※個人情報など機密情報を残したくない
業務パソコン



BitLockerの併用 により、強固なセキュリティを実現できます

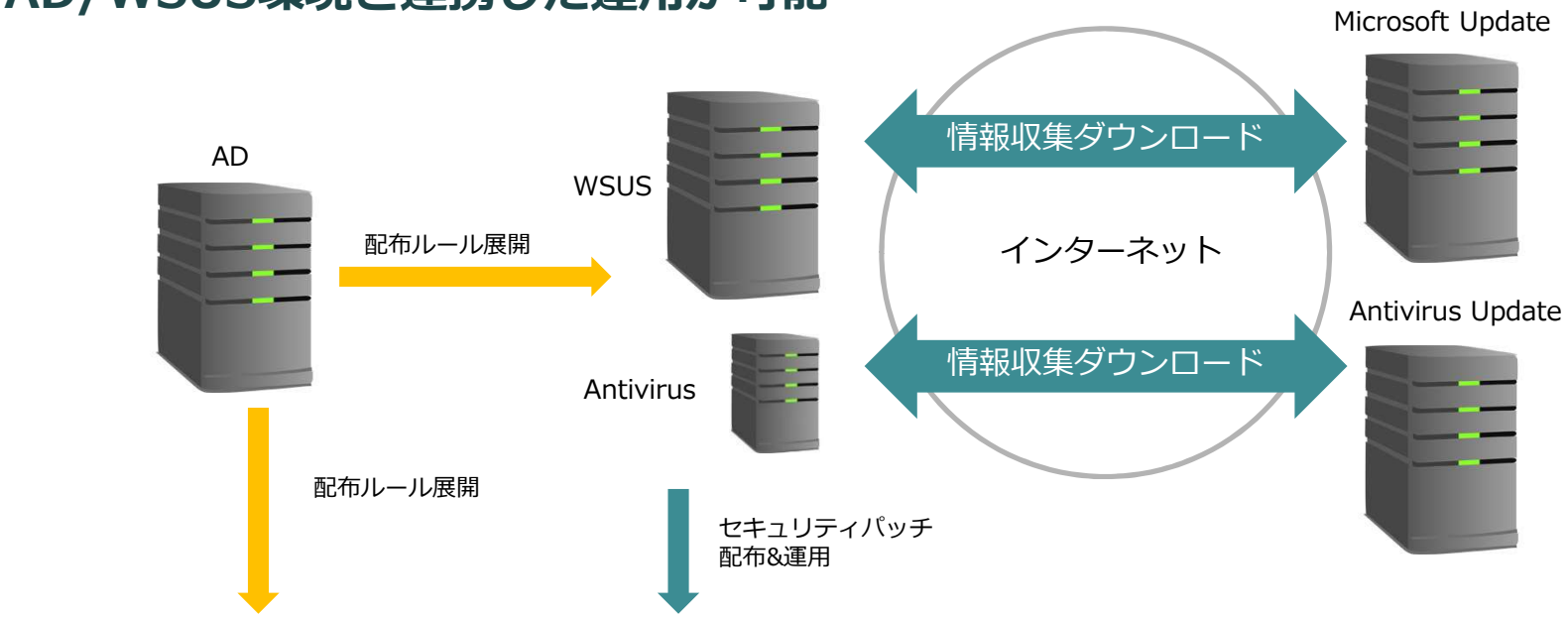
- 持ち出しパソコンでは、ハードディスクの暗号化は必須
- 万が一の紛失・盗難時も安心です

アップデート連携 により、常に安全な状態を維持します

- Windows Updateとの連携
- アンチウィルスソフトの更新との連携（定義データ、パッチ適用）

環境復元ソフトの利用シーン②

AD/WSUS環境と連携した運用が可能



アップデート連携

常に安全な状態を維持します

- Windows Updateとの連携
- アンチウィルスソフトの更新との連携
  （定義データ、パッチ適用）

保護モードで利用 → 作業内容を一時ファイルに記録 → 再起動で完全復元 → 一時ファイルを削除

データを端末に残さない

シンクライアント環境から漏れた端末のセキュリティ対策にも！
環境復元でランサムウェア対策として！

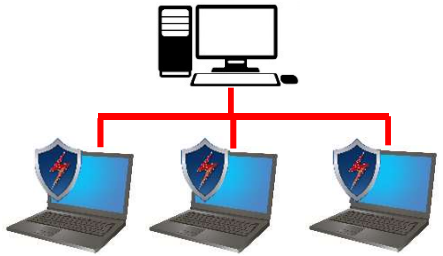
ラインナップ

●ネットワーク対応タイプ

Windows環境復元ソフト
HD革命 WinProtector Ver.8
HD革命/ウィンプロテクター Network Controller

複数のパソコンの操作を一括で管理・操作

**大規模ネットワーク向け管理ツール
ネットワークコントローラー搭載！**



●スタンドアローンタイプ

Windows環境復元ソフト
HD革命 WinProtector Ver.8
HD革命/ウィンプロテクター Standard

オフライン端末でも環境復元を実施

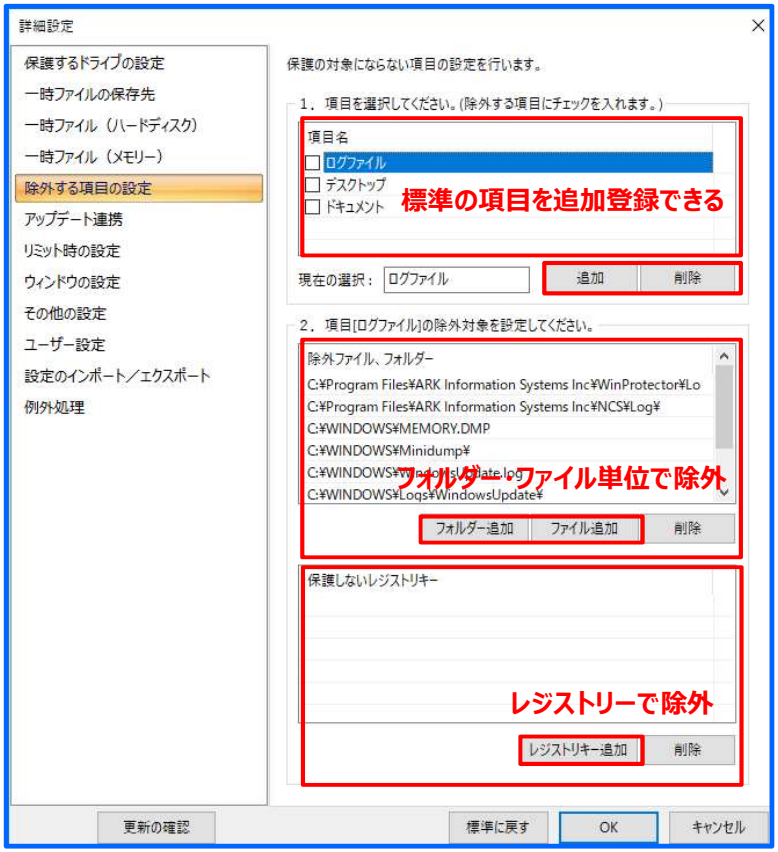
**環境復元の基本機能をすべて搭載
したスタンダードモデル！**

パソコンの運用方法、セキュリティ方針、ネットワーク環境などに合わせてお選びいただけます。

【HD革命/WinProtector】保護除外ファイル/フォルダ設定機能

ed-contrive イーディーコントライブ株式会社

●除外する項目の設定



保護対象のドライブ(パーティション)・ハードディスク内の任意の
フォルダーを保護対象から除外することができます。
複数の除外フォルダーをまとめて1項目として登録することもできます。
除外フォルダー内では保護中でもファイルの更新や追加などが可能です。
フォルダー単位のほか、ファイル単位や、レジストリキーでの指定も
可能です。

運用に合わせて保護の除外設定が可能

- ファイル単位での除外やレジストリキーの除外が可能
- 再起動することなくアンチウィルスソフトの更新も可能
- 運用時のログファイルなどを直接指定して除外が可能

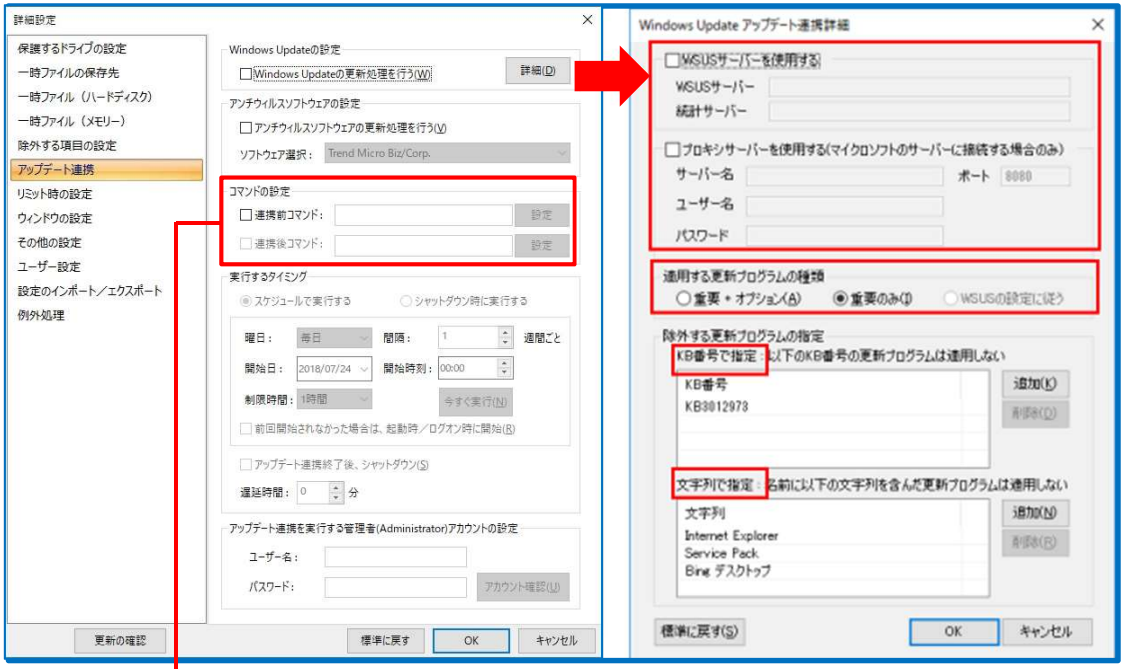
複数ドライブのフォルダー、ファイルをまとめて1項目として
設定できます。

※BitLockerが有効化された環境では「除外する項目の設定」は使用できません。
※「除外項目の設定」は、個々のソフトウェアや特定の環境による動作を保証するものではありません。
　お客様自身による十分な確認と検証のもとでご利用ください。
※「除外する項目の設定」と「継続保護の設定」は同時に設定できません。

【HD革命/WinProtector】アップデート連携

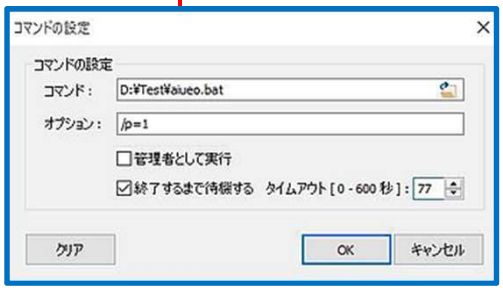
●Windows Update、アンチウィルスソフトウェアとのアップデート連携

保護中でも、Windows Update や アンチウィルスソフトウェアと連携して、クライアントパソコンの
アップデートを実施することが可能です。最新のセキュリティ環境で、パソコンを利用できます。
スケジュール実行時に電源が入っていなかった場合には次回の起動時/ログオン時に開始するオプションや、
シャットダウン時に実行など、運用に即した設定でアップデート連携が行えます。



「詳細」ではWindows Update 連携時のWSUS
サーバー、プロキシサーバーの設定も可能です。
その他「詳細」ではWindows Updateで
「適用する更新プログラムの種類(「重要＋オプ
ション」「重要のみ」「WSUSの設定に従う」と
「除外する(適用しない)更新プログラムの指定」
の設定ができます。適用しない更新プログラムは
「KB番号」または「文字列」で指定します。

※「継続保護の設定」と「アップデート連携」は、同時に
設定できません。
※WSUSサーバー設定は、Windowsグループポリシーの設定を
変更します。
HD革命/WinProtectorのアップデート連携を介さない、通常の
Windows Updateも設定されたWSUSサーバーを通して実行
されるようになります。
また、設定したまま HD革命/WinProtector をアンインストール
するとグループポリシーの設定は残ったままになりますので、
注意してください。



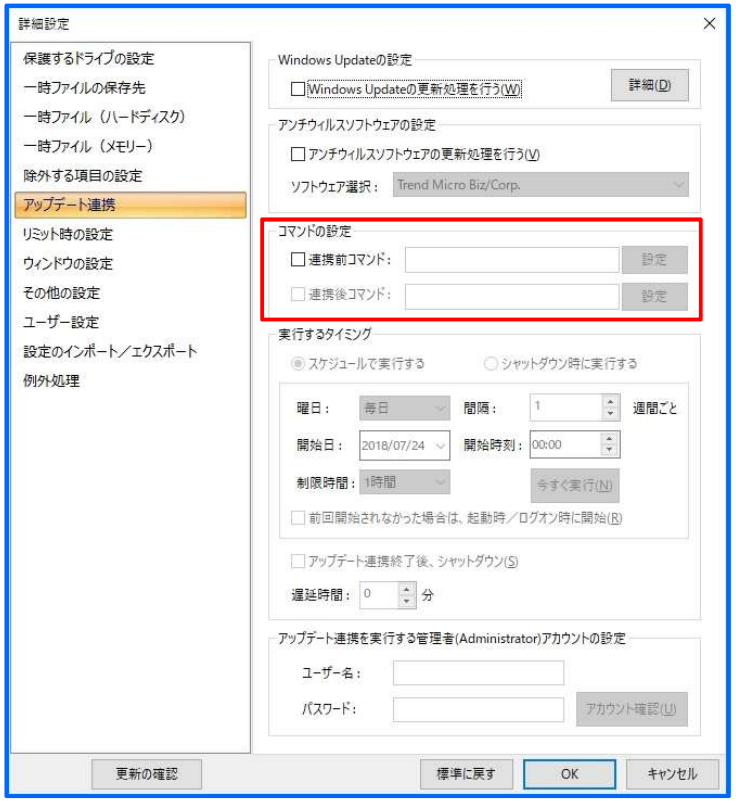
アップデート連携の実行前／実行後にコマンドを実行することが可能です。
例えば、AdobeやJavaのアップデートや、新規アプリケーションの
インストールに利用できます。

※再起動を伴うコマンドは使用できません。
※インストールは、サイレントインストールが可能なアプリケーションに限ります。

【HD革命/WinProtector Ver.8】新機能 / アップデート連携を強化

●指定コマンドのみを実施させることが可能

Windows Updateの設定、アンチウィルスソフトの設定を
行わずにコマンドだけを実行させることが可能です。

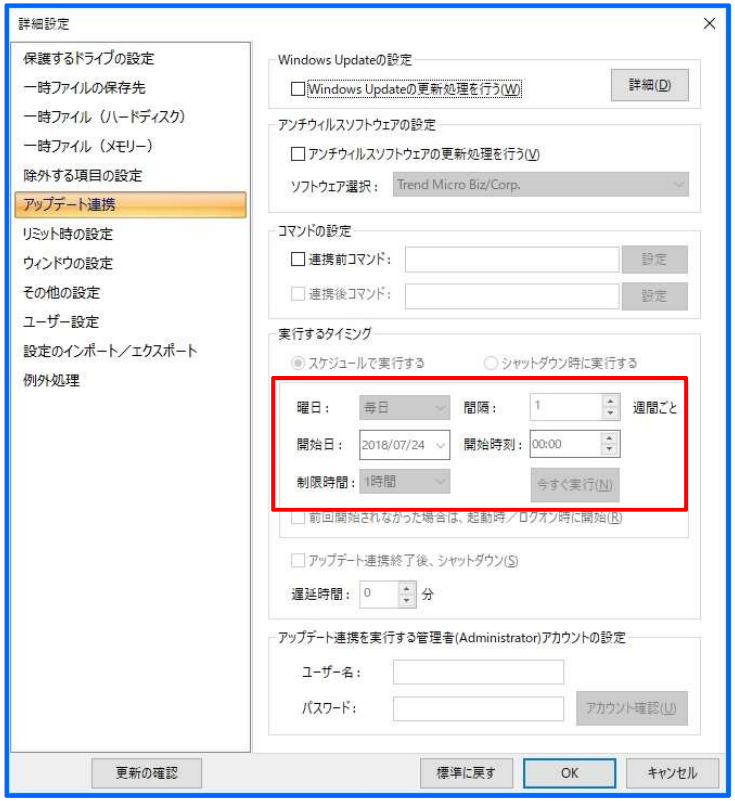


「連携前コマンド」のみがONにされている場合でも
「実行するタイミング」「管理者アカウント」の設定が行えます。

※コマンドのみ実行する場合は、「連携前コマンド」にチェックを入れて
実行するコマンドを設定してください。
※「Windows Updateの更新処理を行う」または、
「アンチウィルスソフトの更新処理を行う」のいずれかにチェックが
入っている場合のみ「連携後コマンド」の設定が行えます。

●アップデート連携実施スケジュールに隔週対応を追加

Windows Update、アンチウィルスソフトの更新処理の
タイミングに「開始日」「週の間隔」の設定が可能です。

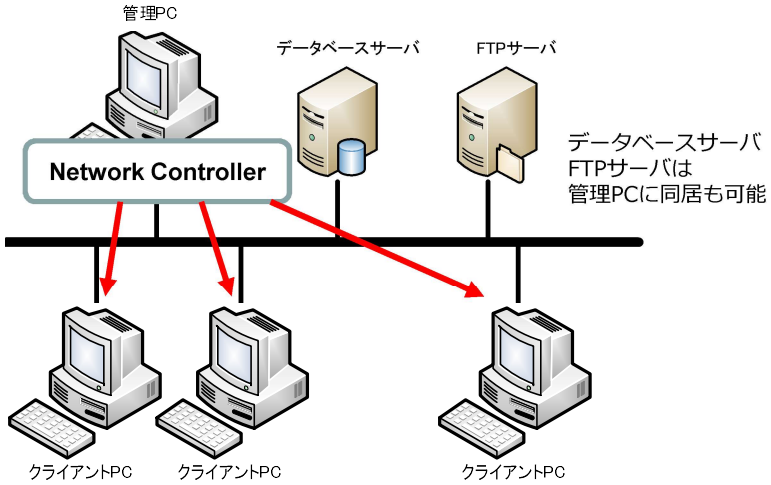


アップデート実行のタイミングを
「曜日」「日付」「時刻」「週の間隔」から決めていただく
ことが可能です。
運用に合わせた実行タイミングをお選びください。

【Network Controller】概要

Windows環境復元ソフト
HD革命 WinProtector Ver.8
HD革命/ウィンプロテクター
Network Controller

保護の開始から、
デバイス接続やファイル削除などの運用管理まで、
クライアントPCを一元管理し、
遠隔で一括操作できます



クライアントパソコンをグループで一元管理

- グループは最大7階層
- ホスト名、電源状態、ログインユーザ、保護状態などを一覧表示

クライアントパソコンの詳細情報を収集して状態を把握

- 情報取得の為の豊富なメニューを用意
- イベントログ、ディスク使用量など利用状況を正確に把握

電源ON/OFFや資料配布などを遠隔で操作、スケジュールで省力化

- WinProtectorの設定変更、保護の開始／解除、アップデート連携の実施
- スケジュールの設定と同時にメッセージの送信設定も可能

アプリケーションのインストール／アップデートが可能

- 一括操作で管理を効率化

情報の持ち出し、持ち込みをシャットアウト

- USB-HDD、USBメモリ、光学ドライブの利用設定が可能

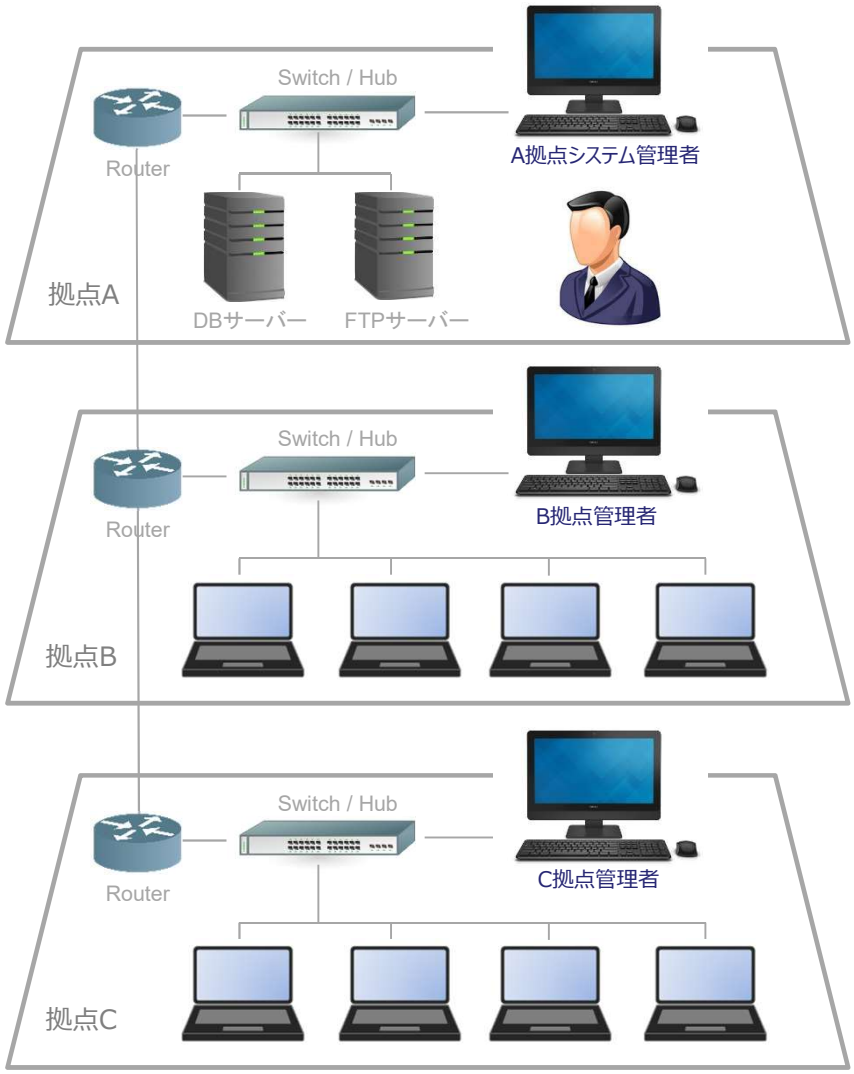
ファイル抹消

- 革命シリーズ実績の抹消ソフトにより、データを完全消去
- Windows／ブラウザの履歴からアカウント、空き領域まで

各操作を登録、バッチ処理が可能

- タスクの連続実行、再利用が可能です
- 作業時間の短縮、快適な運用を実現

「システム管理者」と「グループ管理者」によるクライアントPC管理の分散化が可能



●システム管理者からサブネットを超えるPC操作が可能

管理者には、すべての権限を持つ「システム管理者」と、リモート操作できるクライアントPCや「Network Controller」で実行できる操作を限定した「グループ管理者」を、いずれも複数設定することができます。

利用シーンとしては、所在場所の異なる拠点間において「システム管理者」は独立した環境において主に設定変更などのメンテナンス作業とし、運用は各拠点に管理PCとクライアントPCを設置して「拠点管理者」を配置し、リモートでクライアントPCの監視や操作を行う※といったことが可能です。

クライアントPCの管理・操作を分散化することで、クライアントPCへの操作ミスを防ぎ、管理者の負担と管理PCへの負荷も軽減され、より安全・確実にクライアントPCを管理することが可能です。

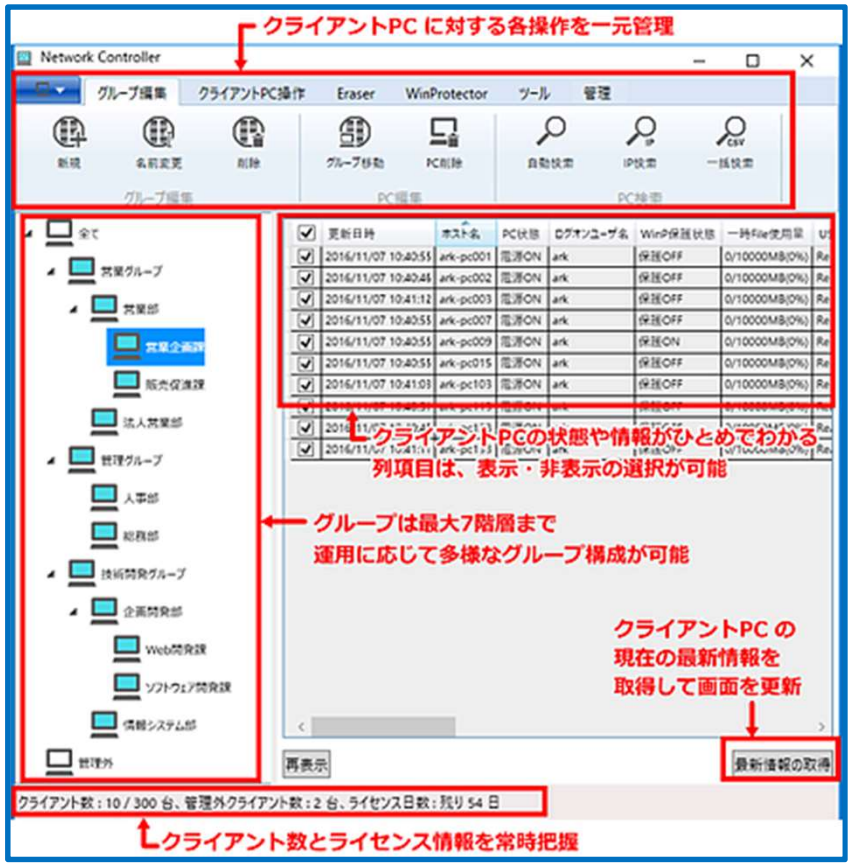
※各管理PCは、データベースサーバーに接続できる必要があります。
　また、各クライアントPCは、FTPサーバーに接続できることが必要です。
※各拠点はVPN通信で接続されている必要があります。

AWS / Azureでの運用も可能です！

クライアントPCの情報をグループごとにまとめて管理

●グループで管理、最大7階層。IP検索、ソートも可能。

文教現場であれば、グループや教室ごとに、企業であれば、
組織や部署ごとに、など運用状況にあわせたグループ構成が可能です。



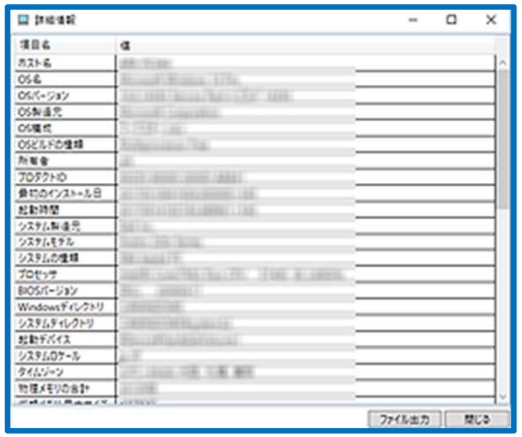
●イベントログ

クライアントPCのアプリケーション、セキュリティ、
システムの各Windowsログが取得可能。スピーディーな問題の
解決につなげることができます。

●詳細情報

起動時間、ログオン履歴、アプリケーション一覧、メモリ使用量など細部にわたる情報を取得可能です。クライアントPCの利用状況を正確に把握できます。

さらにCSVファイルで一覧出力も可能。自由な編集で、有効に活用できます。



クライアントPCの電源管理、資料配布・収集、デバイスロックを操作

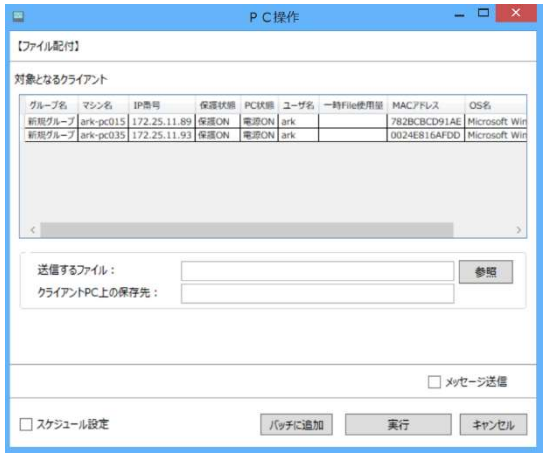
●PC電源操作

メイン画面で選択したクライアントPCの、電源ON、シャットダウン、再起動、強制ログオフが操作できます。
※電源ONはクライアントPCがWake On LAN 機能に対応し、BroadCastが届くネットワーク内にあることが条件となります。

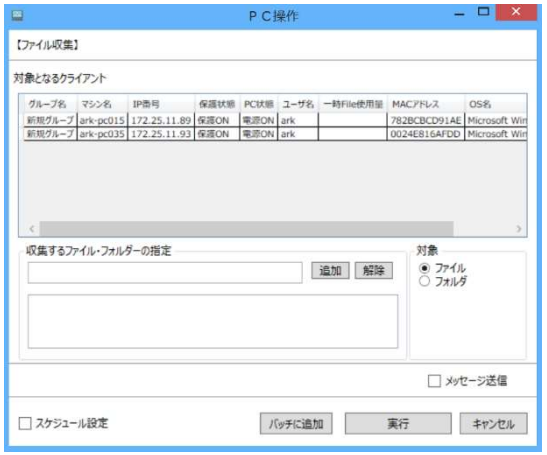
●PC操作

メイン画面で選択したクライアントPCをコマンドにより操作したり、資料の配付・収集や、メッセージを送ることができます。

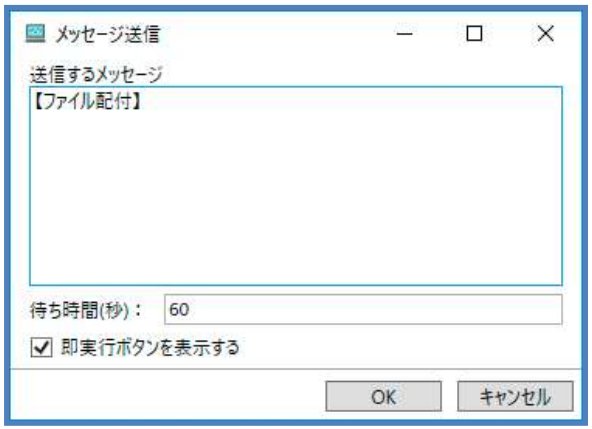
ファイル配布の設定画面



ファイル収集の設定画面



メッセージ送信画面



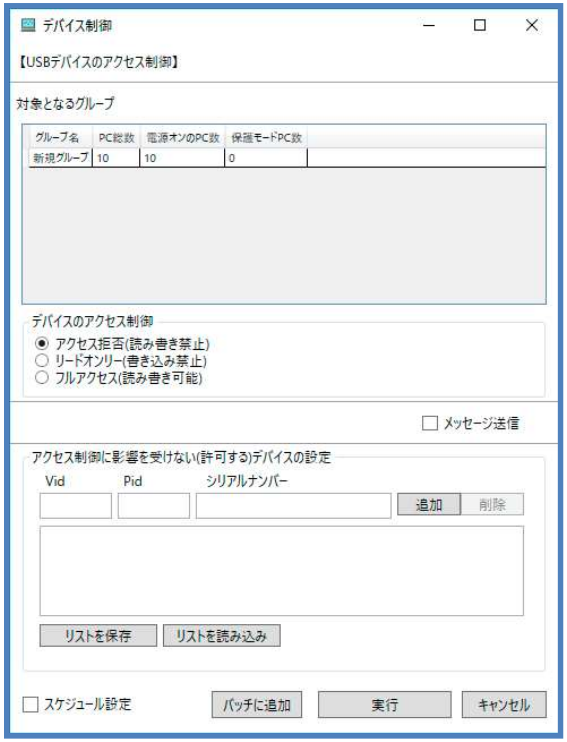
【Network Controller】クライアントPC操作－2

●デバイスロック

マウス／キーボード、デスクトップの画面のロック、CD/DVD、USB、スマホのデバイスを制御します。

※iPhoneには対応していません。

USBデバイスの制御設定画面



・USBデバイス制御について

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。

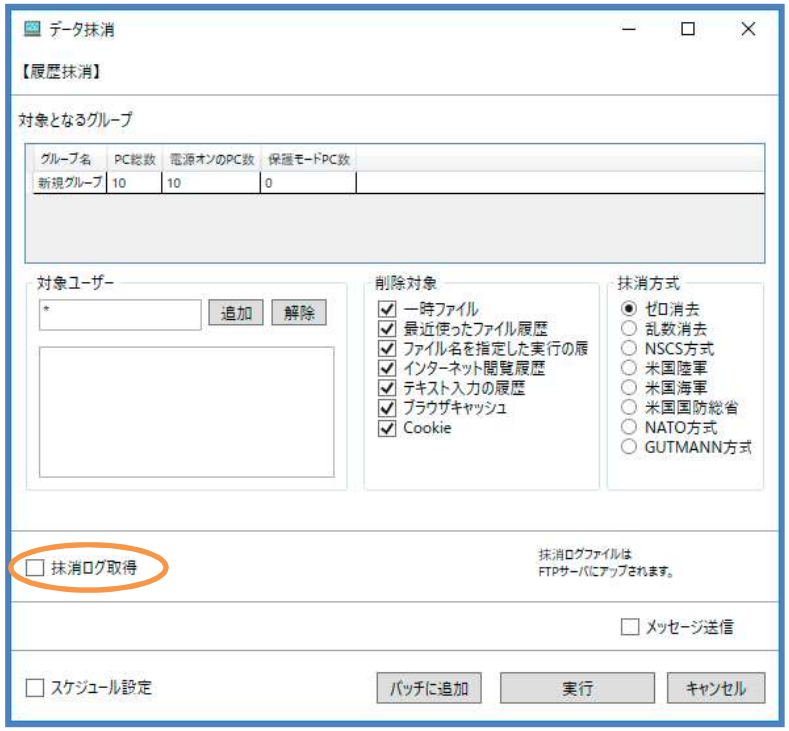
・SDカード制御について

NetworkControllerではUSBデバイス制御と連動してRemovableDiskも制御可能です。一般的にSDカードは「RemovableDisk」と判断されますので、SDカードも制御可能ですが、内部デバイスとして一般のHDDと認識するPCもあるかもしれない為、お客様環境で動作検証などを実施する必要がございます。

データを消去　紛失・盗難時などの情報漏えいリスクも軽減

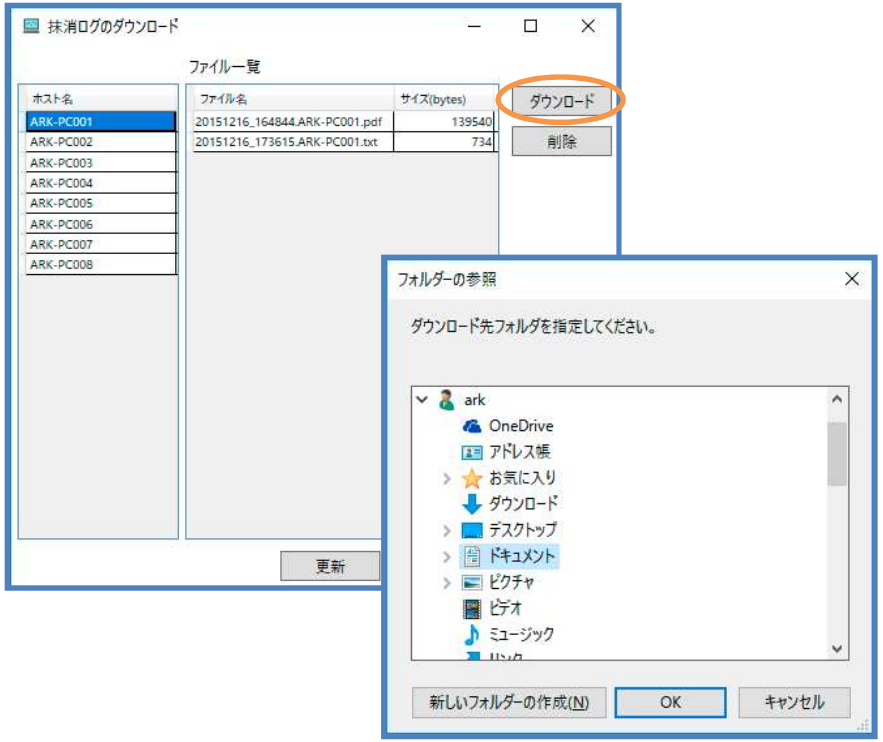
●データ抹消

「HD革命/Eraser　ファイル抹消」機能で履歴抹消、ファイル抹消、アカウント抹消、空き領域抹消ができます。



●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サーバに抹消ログが保存され、抹消ログをダウンロードできます。



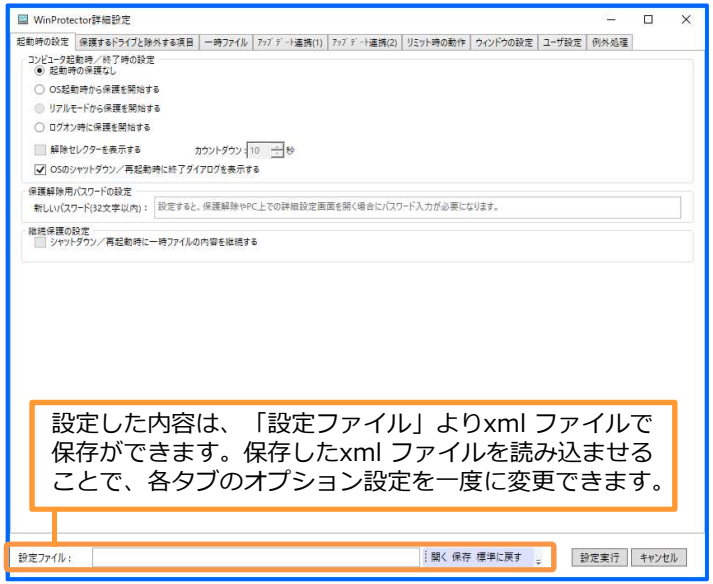
HD革命/WinProtectorに関する設定、アップデート連携を操作

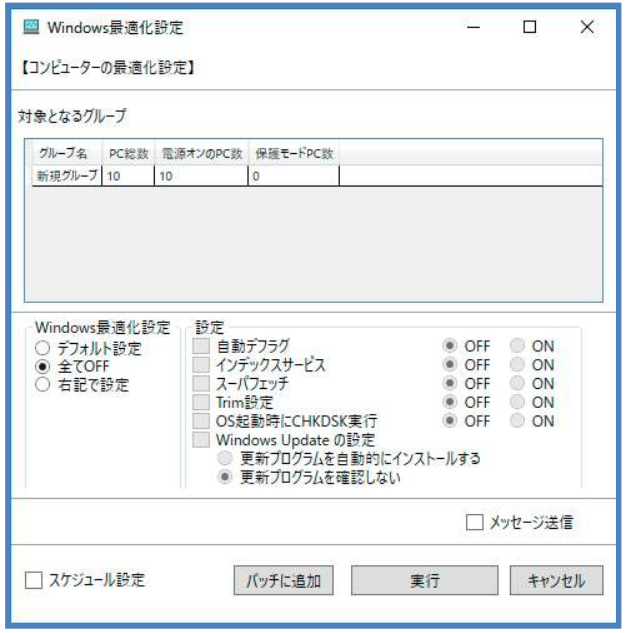
●PC保護

メイン画面で選択したクライアントPCの保護開始、保護解除、「詳細設定」の「アップデート連携」で設定した内容「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。

●詳細設定

WinProtector詳細設定画面が表示され各タブでオプション設定を行います。また最適化設定ではWinProtectorの環境復元機能をスムーズに運用できるように、クライアントPCのWindowsなどの設定を最適化します。



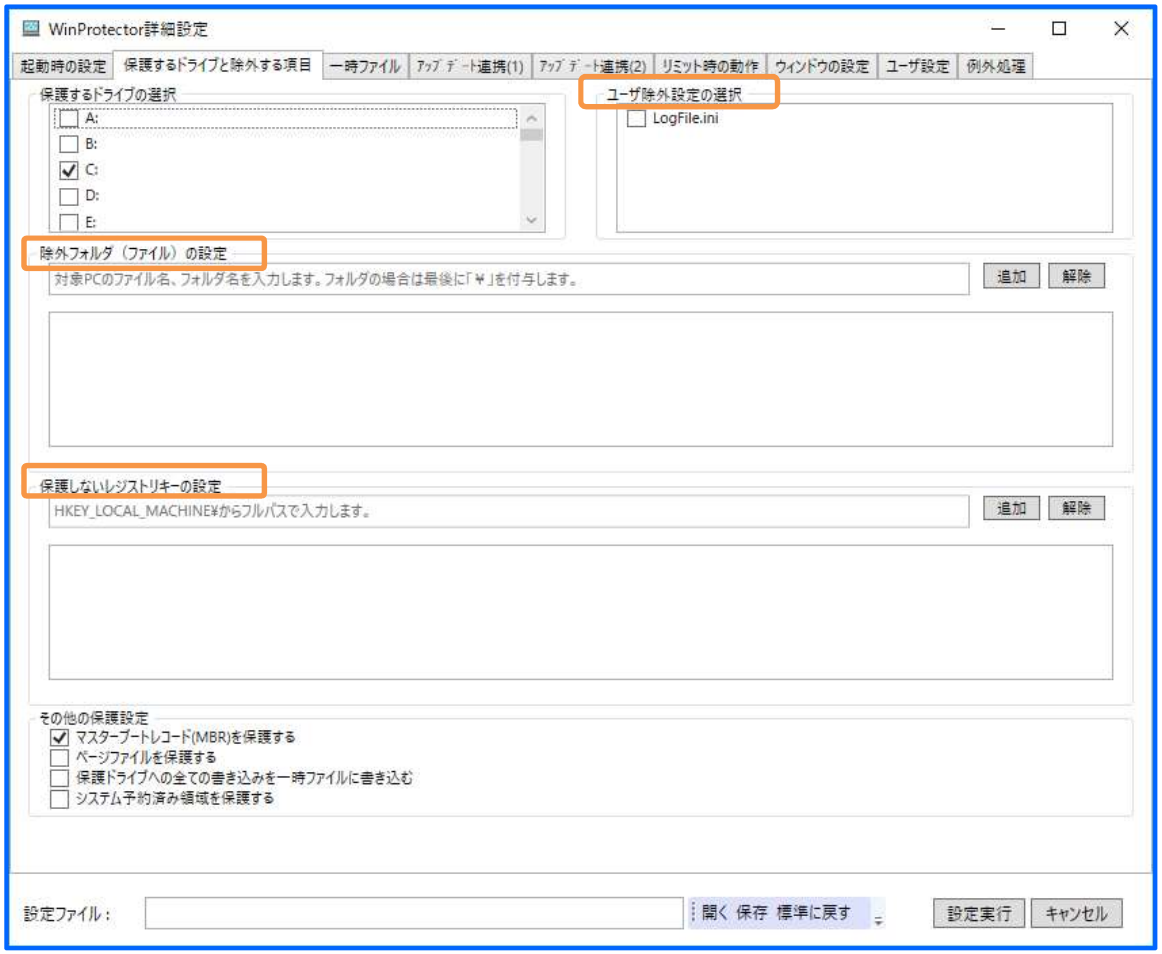


●詳細表示

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。

運用に合わせて保護を除外設定し維持したいデータはそのままに

- ファイル単位での除外やレジストリキーの除外が可能
- 再起動することなくアンチウィルスソフトの更新も可能
- 運用時のログファイルなどを直接指定して除外が可能



●ユーザー除外設定の選択

保護中に除外する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。

●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。

※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。

保護中でもアップデート連携 により、常に安全な状態を維持します

- Windows Updateとの連携
- アンチウィルスソフトの更新との連携（定義データ、パッチ適用）　※検証済みアンチウィルスソフト一覧は24ページをご覧ください。
- 連携タイミングの選択が可能

● Windows Update 設定

クライアントPC において、Windows Update を行うように設定します。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。

●アンチウィルスアップデート設定

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。

●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。指定したタイミングになるとコンピュータが再起動し、更新処理が実行されます。
アップデート連携中は保護が解除された状態で実行されるため、常に安全なPC環境を維持することができます。

●更新処理を実行するアカウント

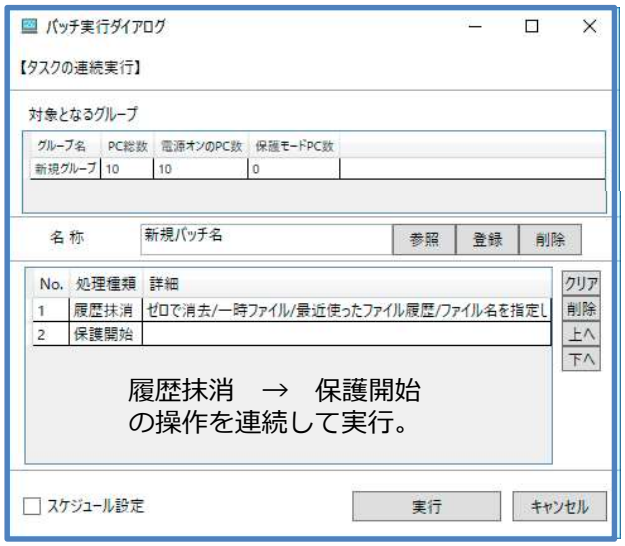
Windows Update やアンチウィルスソフトによりコンピューターの再起動が行われた場合、自動的にログオンするためのユーザー名とパスワードを入力します。

バッチ登録によるタスクの連続実行と、実行操作の履歴を確認

●連続実行

各操作設定画面の　「バッチに追加」ボタンを押下すると
バッチ一覧に追加されます。

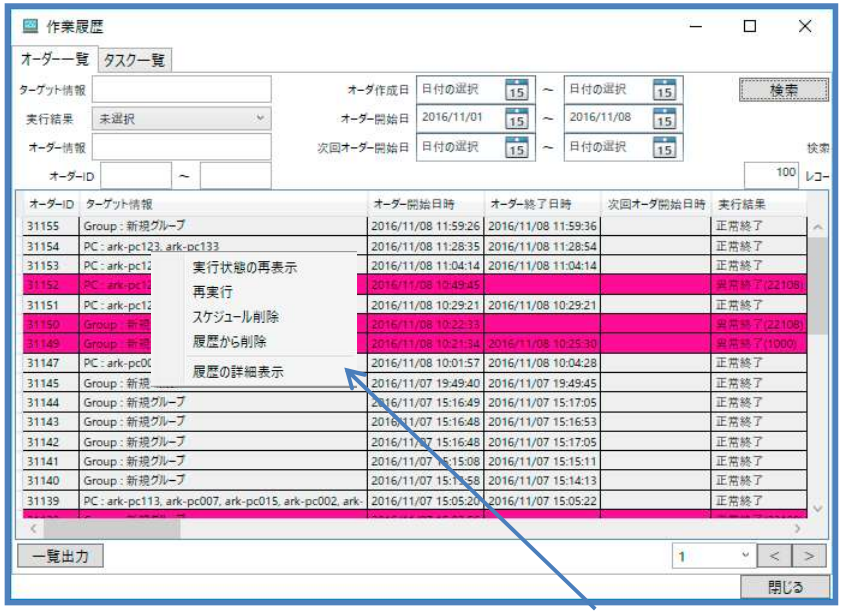
設定した内容で「タスク」が下の画面に追加されます。
登録された順番でタスクを連続実行できます。



●作業履歴

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。

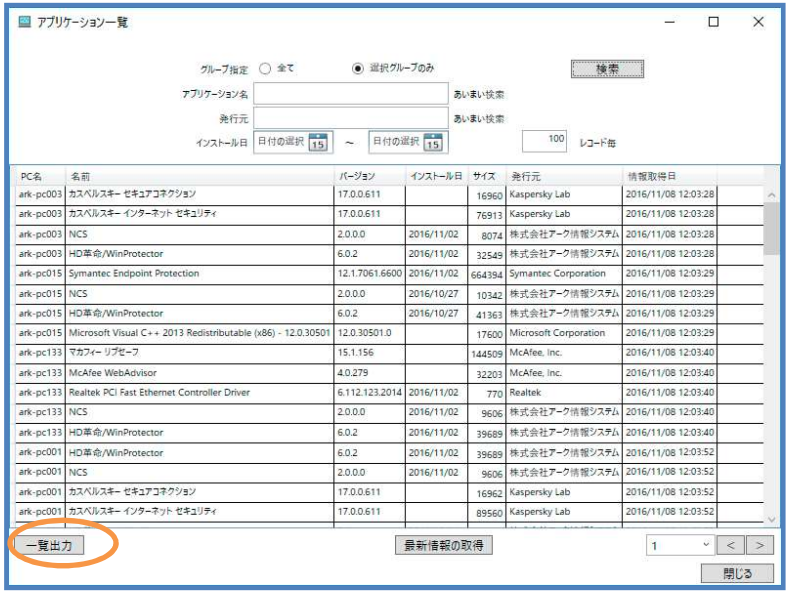


右クリックで再実行と履歴の削除ができます。

資料のダウンロード、PC利用状況(アプリケーション、ログオン履歴)を管理

●PC情報

「アプリケーション一覧」では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。

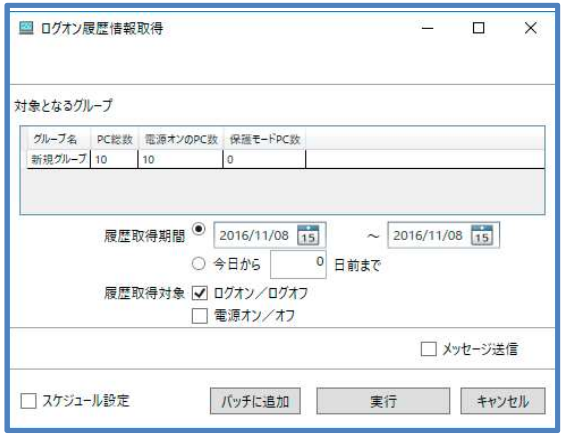


「一覧出力」をクリックすることで、表示されている内容をCSVファイルに出力できます。

●FTP

「資料収集」で収集したファイルをFTPサーバからダウンロードします。

「ログオン履歴」では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。



HD革命/WinProtector Ver.8　環境復元機能一覧

機能		Network Controller	Standard
環境復元機能（端末機能）	Windows 10 対応	○	○
	BitLocker対応　※1		
	保護対象ドライブの選択　※2		
	パスワード設定		
	一時ファイルの保存先（ハードディスク/メモリー）		
	作業した内容の適用		
	Windows Update 連携　※3		
	アンチウィルスソフト更新連携　※3		
	ログオンユーザー別の保護と権限設定		
	保護除外項目の設定　※3※4		
	再起動後の保護の継続　※4※5		
	サイレントインストール		
	詳細設定項目のインポート/エクスポート機能		
	アップデート連携の即時実行		
	WinProtectorの更新（アップデータの確認・適用）		
	小規模ネットワーク管理　Network Manager搭載　※6		

※1　BitLockerが有効化された環境では「除外する項目の設定」は使用できません。またBitLocker以外の暗号化製品はサポート対象外です。
※2　複数のドライブを保護する場合、物理的に異なるドライブ（パーティション）にまたがっての設定はできません。同一ディスク上のドライブ（パーティション）となります。
※3「アップデート連携」と「継続保護の設定」は同時に設定できません。
※4「除外する項目の設定」と「継続保護の設定」は同時に設定できません。
※5　GPTディスクの環境では「継続保護の設定」はできません
※6　Network Manager の機能は全て、Network Controllerに搭載されています。

Network Controller　集中管理機能一覧

機能		Network Controller	Standard
集中管理機能	リモート操作（電源OFF【シャットダウン】/再起動/復元操作）	○	×
	リモート操作（電源ON※1/ログオフ）		
	資料配布・収集		
	マウス・キーボード・デスクトップ制御		
	CD/DVD/CDドライブ制御		
	USBデバイス制御		
	MTPデイバイス制御※2		
	ファイル/アカウント/領域抹消		
	コマンド実行、バッチ操作		
	スケジュールによるリモート操作実行		
	アプリーション一覧		
	ログオン/ログオフ、電源ON/OFFの履歴		
	システム管理者によるグループ管理者の権限設定		

※1　WOL対応機種のみ。
※2　iPhoneは非対応。

他社製品機能比較

運用支援機能	WinProtector Ver.8		A社製品	B社製品	C社製品	D社製品
	Network Controller	Standard				
環境復元	○	○	○	○	○	○
Windows Update連携	○	○	○	○	○	○
アンチウィルスソフト更新連携	○※1	○※1	○※1	○	△	○
リモート操作(電源OFF/再起動/復元操作)	○	○	○	○	○	○
リモート操作(電源ON※2/ログオフ)	○	×	○	○	○	○
資料配布	○	×	○	×	-	○
マウス/キーボード/ディスクトップ制御	○	×	○	○	-	○
CD/DVD/BDドライブ制御	○	×	×	×	×	×
USBデバイス制御	○	×	×	○	×	×
スマートフォン※3（MTPデバイス）制御	○	×	×	○	×	×
ファイル/アカウント/空き領域抹消	○	×	×	×	×	×
コマンド実行、バッチ操作※2	○	×	○	×	-	○
アプリケーションの※4インストール/アップデート	○	×	×	×	-	×
スケジュールによるリモート操作実行	○	×	○	○	○	○
アプリケーション一覧	○	×	×	×	×	×
ログオン/オフ、電源オン/オフの履歴	○	×	○	×	×	○
BitLocker対応	○	○	×	×	×	×

※1　A社製品はフォルダ保護モード時に連携可能で、ドライブ保護モードでは不可。WinProtectorはドライブ保護モードのみ。
※2　WOL対応機種のみ。
※3　iPhoneには非対応。
※4　サイレントインストール可能なアプリケーションに限る。

HD革命/WinProtector Ver.8　動作環境

	HD革命/WinProtector Ver.8（クライアント）	Network Controller（ネットワークコントローラー）
対応OS	日本語版の以下に示すOS Windows 10　32bit/64bit版 Windows 8.1 Update 32bit/64bit版 Windows 7　32bit/64bit版（SP1以降） ※大型Windows Updateへは順次対応しています。 ※Windows RT/RT8.1には対応していません。 ※サーバー系のOS には対応していません。 ※アドミニストレータ権限(管理者権限)が必要です。	日本語版の以下に示すOS Windows 10　32bit/64bit版 Windows 8.1 Update 32bit/64bit版 Windows 7　32bit/64bit版（SP1以降） Windows Server 2016 64bit版 Windows Server 2012 / 2012 R2 64bit版 ※大型Windows Updateへは順次対応しています。 ※Windows RT/RT8.1には対応していません。 ※アドミニストレータ権限(管理者権限)が必要です。
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。	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 ： 2GB以上 Windows 10/8.1/7 32bit版 ： 1GB以上 ※メモリー上に「一時ファイル」を設定する場合、保護を行うためのメモリーとは別に、インデックス用としてドライブサイズに対して約1,000分の1のメモリー容量が必要です。	Windows 10/8.1/7 64bit版 ： 2GB以上 Windows 10/8.1/7 32bit版 ： 1GB以上 Windows Server 2016 64bit版 ： 4GB以上 Windows Server 2012 / 2012 R2 64bit版 ： 4GB以上
CD/DVDドライブ	DVD-ROMを読み込めるドライブ（Network Controller） CD-ROMを読み込めるドライブ（Standard）	DVD-ROMを読み込めるドライブ
SSD/HDD	50MB以上の空き容量 （本製品のインストール用として）	100MB以上の空き容量 （本製品のインストール用。その他にデータベースの保存領域が必要）
対応ファイルシステム	FAT32、NTFS（FAT16、exFATには対応していません） ※ダイナミックディスクの環境では使用できません。 ※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。 ※Windows 10/8.1/の「記憶域」で作成したディスクに対して保護を行うことは動作保証外となります。	
その他	.Net Framework 4.6.2以上が必要 （Network Controller版）	データベースサーバーとして SQL Server 2016 Express SQL Server 2012 Express Edition FTP サーバーとしてInternet Information Service IIS7以上がインストール可能であること 管理PC およびクライアントPC には「.Net Framework 4.6.2」以上

【HD革命/WinProtector（クライアント用プログラム）について】
●SSD(Solid State Drive)上のドライブを保護をするには、Trim機能をオフにする必要があります。
●システムドライブの断片化が進んでいる場合、保護を行うことはできません。
●複数のドライブを保護する場合、物理的に異なるドライブ（パーティション）にまたがっての設定はできません。同一ディスク上のドライブ（パーティション）となります。
●GPTディスクの環境では「継続保護の設定」はできません。
●BitLockerが有効化された環境では「除外する項目の設定」は使用できません。
●「継続保護の設定」と「除外する項目の設定」は同時に設定できません。
●「継続保護の設定」と「アップデート連携」は同時に設定できません。
※同時に設定できない機能は、オプションを設定した際にメッセージが表示されます。
ここで「はい」を選択すると、同時に設定できない機能の設定が自動的に変更されます。
●お使いの環境によっては、HD革命/WinProtector を使用している間はWindowsの休止状態/サスペンド、スタンバイ/スリープ等の省電力機能が正しく動作しない場合があります。
●HD革命/WinProtectorでドライブの保護を行っている間は「ディスクデフラグ」また　はそれと同様の機能を持つディスク最適化ソフトウェアによる最適化は行わないでください。
●マルチブートなどの環境で、OSの起動に関わるファイルが、保護されているドライブ以外にある場合は、そのファイルは保護されていないためにファイルの破損・変更があるとOSの起動ができなくなります。
●Intel 6 シリーズ以降のチップセット（Z68、Z77、Z87 など）を搭載したコンピューターで RAID 機能（Intel Smart Response Technology）が有効の場合は、「リアルモードから保護を開始する」オプションを選択しても、メモリー不足により保護を開始することができません。
●ドライブを保護中にコンピューターをリセットした場合や、一時ファイルが限界値に達して再起動した場合、保護中に変更されたデータは破棄されてしまいます。

【ネットワークマネージャーについて】
●HD革命/WinProtector とNetwork Managerの「ネットワークマネージャー」は同一PC上にはインストールできません。
●「ネットワークマネージャー」機能を使用する場合は、ファイアウォールの例外処理を行っています。この例外処理は「HD革命/WinProtector」および「ネットワークマネージャー」のインストール時に行われます。そのため、後からセキュリティソフトウェアがインストールされた場合、例外処理が行われていないためにリモートでの保護の開始、解除ができません。「HD革命/WinProtector」または「ネットワークマネージャー」を一度アンインストールし、再度インストールしてください。

【ネットワークコントローラーについて】
●HD革命/WinProtector とNetwork Controllerの「ネットワークコントローラー」は同時にインストールできません。
●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。
●ネットワーク脅威防止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。その場合はネットワーク脅威防止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）、SQLServer（1433 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、実証実験はおこなっていません。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。
●リモートデスクトップを利用している場合、画面操作に関連する操作に問題が発生することがあります
①メッセージ送信関連で、リモートデスクトップが最小化されていると、最小化が解除されないとメッセージが表示されない場合があります。
②デスクトップのロックが解除されない場合があります。
●デバイスロック機能に関して
・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 デバイス、CD/DVDおよびスマートフォンのアクセス制御は、ログアウト（シャットダウン）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／解除をおこな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。
●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、「オーダ一覧」に登録されたオーダを右クリック→「スケジュール削除」と選択することで削除が可能です。

【メモリー使用について】
●コンピューターによってはOS管理外のメモリーを使用するにあたり、BIOSの設定（メモリーマップ機能）を有効にする必要があります。
●コンピューターによっては3GB以上のメモリーを搭載していてもOS管理外のメモリーを使用できない場合があります。
●他のOS管理外のメモリーを使用するソフトウェアと同時にOS管理外のメモリーを使用することはできません。
●休止状態/サスペンドなどの省電力機能を使用される場合は、OS管理外のメモリーを使用できません。
●一時ファイルとして設定できるメモリー容量は、搭載メモリー容量や環境により異なります。

【他社ソフトならびに革命シリーズとの共存について】
●Symantec社の「Norton GoBack」(「SystemWorks」に含まれる「NortonGoBack」を含む)との共存はできません。
●SSD革命/SpeedAdvance Ver.1(Hi-Gradeも含む)とは同時にインストールできません。
●HD革命/BackUp、HD革命/CopyDrive、および「BOOT革命/USB」の各製品とは共存できません。
●HD革命/WinProtectorでシステムを保護している間は、「ディスクの管理」や「HD革/PartitionEX」、そのほかのツールでドライブの作成や削除などの操作を行わないでください。
●Memory革命/RAM Driveをインストールしている場合、OS管理外のメモリーを同時に使用はできません。

お問合わせ先

【問い合わせ先／販売元】

イーディーコントライブ株式会社

営業推進部　HD革命/WinProtector 担当

東日本エリア：03-6238-3501　西日本エリア：06-6838-3177
E-mail ： WP-info@ed-contrive.co.jp
Web：https://www.winprotector.jp/

【開発元】

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

【会社概要】

名称 ： イーディーコントライブ株式会社

本社住所 ： 〒102-0073 東京都千代田区九段北4-1-3 飛栄九段北ビル6階

設立 ： 平成18年10月2日

資本金 ： 9,900万円

従業員数 ： 21名　（2018年1月1日現在）

代表取締役社長 ：尾上　昌隆

URL：http://www.ed-contrive.co.jp/