



リモートクライアント管理ツール

スマートコントロール

<インストール / 操作ガイド>

Ver.2.5

- この度は、本製品をお買い上げいただきまして誠にありがとうございます。
- 本製品の性能を十分に引き出してご活用いただくために、ご使用前に必ずこの取扱説明書をお読みください。また、お読みになった後は、本製品近くの見やすい場所に保管してください。

ARVANICS Corporation

商標について

- Windows、Windows10、Windows11 は Microsoft Corporation の登録商標です。
- その他、記載されている会社名、製品名は、各社の登録商標または商標です。なお、本文中において、®マークや™マークを省略している場合があります。

この取扱説明書をお読みいただく前に

- この取扱説明書の無断転載を禁じます。
- お客様がお持ちの製品のバージョンによっては、この取扱説明書に記載される画像とメニュー項目などが、一部異なる場合がありますのでご了承ください。
- 取扱説明書は改善のため、事前の予告なく変更することがあります。最新の取扱説明書は、弊社のホームページからダウンロードすることができます。
<https://arvanics.com/>

必ずお読みください

本製品をご使用前に必ずお読みください。

この取扱説明書には、製品を安全に正しくお使いいただくために、重要な内容を記載しています。

製品について

● ライセンス認証について

ライセンスの認証方法は以下の2通りがあります。それぞれの条件により、インストール手順が異なりますのでご注意ください。

(1) インターネット経由でライセンスを認証

インストール時にライセンスを認証します。

ご利用のインターネット接続がプロキシ環境の場合は、「(2) インターネット環境が無い場合や、Proxy 環境での認証（手動認証）」にてインストールを行ってください。

(2) インターネット環境が無い場合や、Proxy 環境での認証（手動認証）

インストール後に作業が必要となります。必ず手動認証手続きを行ってください。

● ドライブシールド SS との接続条件に関して

ドライブシールド SS を一括認証で使用する場合、常にスマートコントロールとの接続を行った状態で使用してください。ドライブシールド SS とスマートコントロールが未接続の状態では 270 日経過すると、ドライブシールド SS は起動して 1 時間後にライセンス認証が解除され、自動的に再起動を行いプロテクト解除モードで起動します。

ライセンス認証が解除された場合、再びスマートコントロールと接続しない限りプロテクトモードにすることができません。ただし、270 日以上通信を行わなかった場合でも、ドライブシールド SS が起動後 1 時間以内にスマートコントロールと正常に通信を行えば認証は解除されません。

必ず、スマートコントロールを先に起動してから、ドライブシールド SS を起動し、接続を行うようにしてください。

ドライブシールド SS を単独認証にてご利用の場合は、上記に該当しません。継続してのご利用が可能です。

● スマートコントロールを操作する際の Windows のアカウントについて

スマートコントロールを操作するためには、Windows の管理者権限のあるアカウントでログオンする必要があります。制限付きアカウントでは正常に動作しません。

● **ドライブシールド SS とスマートコントロールの共存について**

ドライブシールド SS とスマートコントロールは同一コンピュータにインストールできません。

インストール前の事前設定について

インストール前に下記設定をご確認ください。

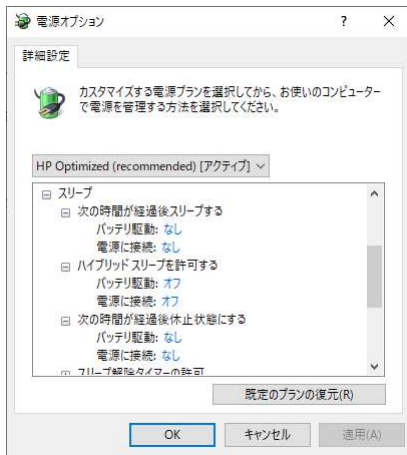
非対応の環境で本製品を使用すると、正常に動作しない場合や誤動作につながる可能性がありますのでご注意ください。

● **スマートコントロールのインストール環境について**

OS をクリーンインストールした状態でご使用ください。OS の上書きインストールなどにより、以前の OS の設定やドライバが残っている状態で使用すると、予期せぬ不具合を引き起こす場合があります。

● **電源オプションについて**

本製品をご利用する際は、電源オプションの、スリープモード、ハイブリッドスリープ、休止状態を無効にしてください。



● **Windows Update について**

Windows Update によって OS の環境が大きく変更されると、予期しない動作を引き起こす場合があります。Windows Update の自動更新を無効にする際は、以下の設定をご参照ください。

<手順>

Windows OS の Windows Update を「更新プログラムを確認しない」に設定変更してください。

Windows10、Windows11 は Pro 以上のエディションにて、グループポリシーから自動更新を無効にすることができます。

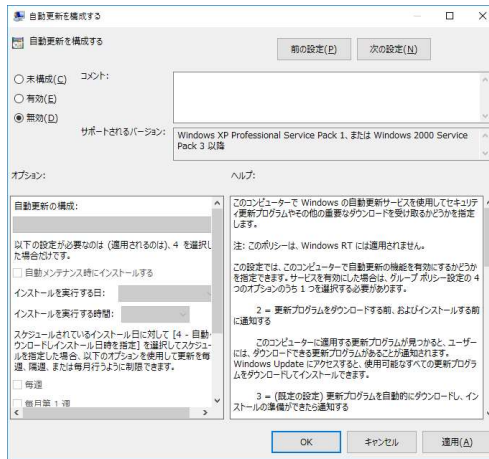
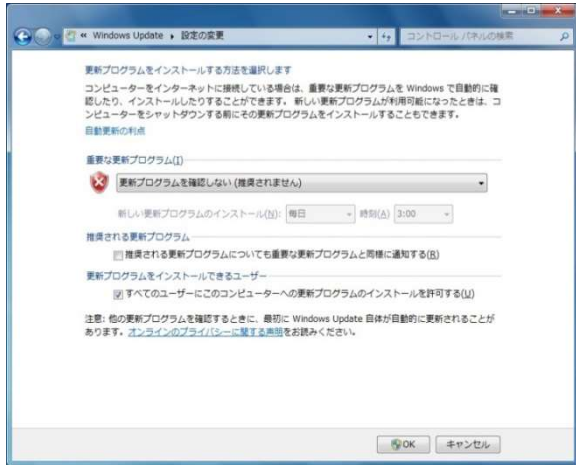
Windows10 :

「コンピュータの構成」>「管理者用テンプレート」>「Windows コンポーネント」>「Windows Update」>「自動更新を構成する」の設定を無効にしてください。

Windows11 :

「コンピュータの構成」>「管理者用テンプレート」>「Windows コンポーネント」>「Windows Update」>「エンドユーザーエクスペリエンスの管理」>「自動更新を構成する」の設定を無効にしてください。

※Windows Home エディションは設定変更できません。設定変更せずにご使用ください。



高速スタートアップについて

Windows の高速スタートアップ機能により、コンピュータ起動後の動作に影響が出る可能性があります。高速スタートアップ機能は無効にしてください。

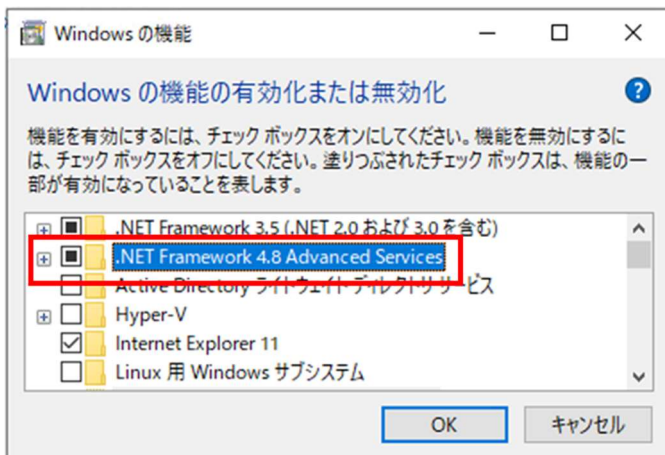


● .NET Framework について

本製品をインストールする際は、事前に「.NET Framework 4.0」以上を有効化する必要があります。「.NET Framework 4.0」以上が有効化されているかは以下の手順でご確認ください。

<手順>

1. コントロールパネルを起動します。
2. 表示方法を「カテゴリ」にし、プログラムのアンインストールをクリックします。
3. 画面左側から「Windows の機能の有効化または無効化」をクリックします。
4. 下図のように「.NET Framework 4.xx」のチェックボックスにチェックを入れて「OK」ボタンをクリックします。



目次

| | |
|---|----|
| 1. 製品概要 | 8 |
| 1.1 ドライブシールドSSとは | 8 |
| 1.2 スマートコントロールとは | 8 |
| 1.3 プロテクトモードの基本概念 | 8 |
| 2. 動作条件 | 9 |
| 3. 試用版について | 9 |
| 4. インストール方法 | 10 |
| 4.1 スマートコントロールのインストール方法 | 10 |
| 4.2 手動認証によるインストール後の認証作業 | 14 |
| 5. 操作方法 | 17 |
| 5.1 スマートコントロールの起動方法 | 17 |
| 5.2 画面の説明 | 17 |
| 5.3 ツールバーのカスタマイズ | 18 |
| 5.4 クライアントリストのグループ作成 | 19 |
| 5.4.1 新規グループを作成する | 19 |
| 5.4.2 サブグループを作成する | 19 |
| 5.4.3 クライアントをグループに登録する | 19 |
| 5.4.4 グループフィルタに登録する | 20 |
| 5.4.5 グループを削除する | 20 |
| 5.4.6 クライアントをグループから削除する | 20 |
| 5.5 基本操作 | 21 |
| 5.5.1 コントロールの対象とするクライアントの選択方法 | 21 |
| 5.5.2 プロテクト/プロテクト解除モード | 21 |
| 5.5.3 USB ブロッキング | 22 |
| 5.5.4 キーボード・マウスのロック | 23 |
| 5.5.5 ステルスモード | 24 |
| 5.5.6 電源管理 | 25 |
| 5.5.7 クライアントのパスワード管理 | 28 |
| 5.5.8 Optional Directory Protection (ODP) | 30 |
| 5.5.9 印刷の制限機能 | 30 |
| 5.5.10 アプリケーションの禁止設定 | 31 |
| 5.5.11 スマートコントロールの変更について | 32 |
| 5.5.12 リモート実行について | 33 |
| 5.5.13 クライアントのプロパティ | 33 |
| 5.5.14 クライアントのログオフを再起動に変更する | 33 |
| 5.5.15 設定のインポート・エクスポートについて | 34 |
| 5.5.16 別コンピュータへのスマートコントロールの移行について | 34 |
| 5.5.17 Windows Update 連携機能について | 35 |
| 5.5.18 WSUS/SUS 設定について | 37 |
| 5.5.19 ファイル転送について | 37 |
| 5.5.20 一時保存領域のサイズ変更 | 38 |
| 5.5.21 クライアントに単独認証用ライセンスキーを割り当てる | 39 |
| 5.5.22 スケジューリング | 39 |
| 6. 仮想化ソフトをご利用の場合 | 45 |
| 7. ライセンス認証の解除 | 46 |
| 8. アンインストール | 46 |
| 9. お問い合わせ先 | 46 |

1. 製品概要

1.1 ドライブシールド SS とは

ドライブシールド SS は、コンピュータのハードディスクへの変更操作をプロテクトするためのセキュリティツールです。

コンピュータを常に同じ状態に保つことで、管理に要する時間を節約し、ウイルスやマルウェアの脅威からコンピュータを保護します。

1.2 スマートコントロールとは

スマートコントロールは、ドライブシールド SS を遠隔制御するための管理用ソフトウェアです。

1.3 プロテクトモードの基本概念

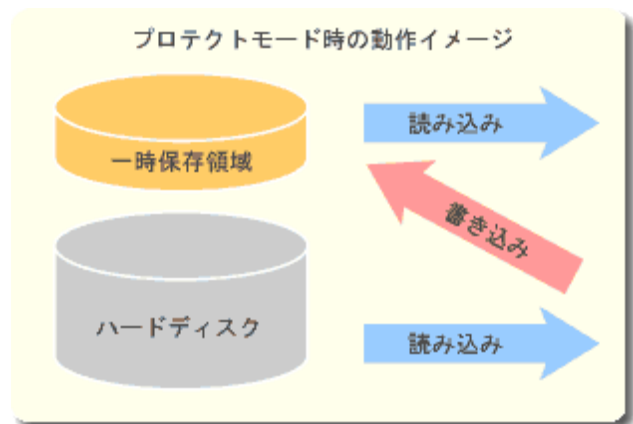
ファイルの新規作成や変更、削除、パーティションのフォーマットや削除、レジストリやシステムフォルダへの変更操作を行った場合でも、コンピュータを再起動するだけでそれらの操作は無効になり、元の状態に戻ります。

ドライブシールド SS をインストールしたコンピュータをプロテクトモードで起動すると、ハードディスクへの書き込みや削除、設定変更等の操作は一切禁止されます。しかし、これらの操作情報は一時保存領域に蓄積されていくため、一見通常と変わらないコンピュータの操作が可能です。

コンピュータを再起動すると、一時保存領域に蓄積されたデータはリセットされ、初期状態の環境が復元されます。

お客様が設定したパスワードを使用して、プロテクト機能の有効 / 解除が可能です。

プロテクトを解除した状態では、通常のコンピュータと同様に、ハードディスクへの書き込みや削除、設定変更が可能です。



2. 動作条件

| | |
|----------|---|
| 動作環境 | .NET Framework 4.0 以上が必要 |
| 対応 OS | Windows11 バージョン 22H2 以降 Windows10 (32bit / 64bit) バージョン 22H2 以降 Windows Server 2016、2019、2022 ※ Windows11、10 大型アップデートへの対応状況につきましては、弊社ホームページをご確認ください。 |
| メモリ | 8GB 以上推奨 |
| ファイルシステム | NTFS |
| ネットワーク | TCP/IP |
| 解像度 | 1024x768 以上 |
| ライセンス認証 | 製品のアクティベーションの際に、インターネット接続 (SSL 通信) を使用します。 プロキシ環境をご利用の場合は、手動認証による手順を実施してください。 |
| その他 | スマートコントロールを導入される端末は静的 IP アドレスを推奨しています。 DHCP 環境でも動作は可能ですが、ネットワーク機器に問題が発生した場合、クライアント(ドライブシールド)端末との通信エラーにつながる可能性があります。 |

3. 試用版について

試用版をご利用いただくには試用版ライセンスキーが必要です。
各社ホームページの専用フォームより試用版ご利用のお申込みが可能です。

株式会社アルバニクス

https://www.arvanics.com/solution/app_bunkyo/form/form_trial_request/

株式会社アイ・ディ・ケイ

https://www.idk.co.jp/solution/series_bunkyo/form/form_trial_request/

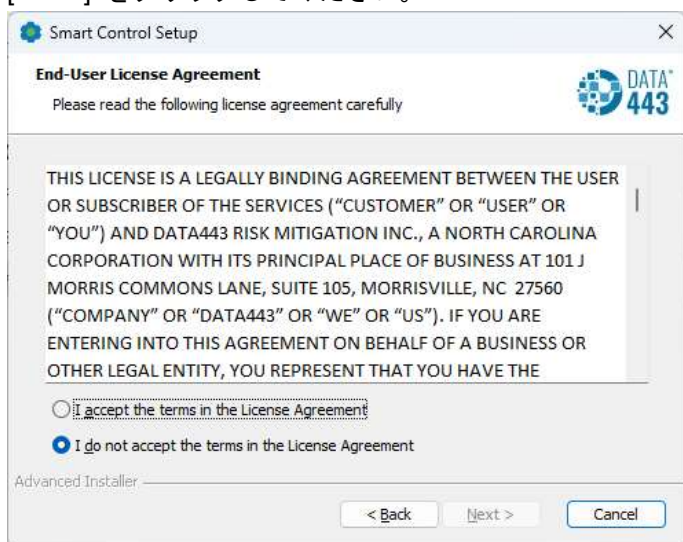
4. インストール方法

4.1 スマートコントロールのインストール方法

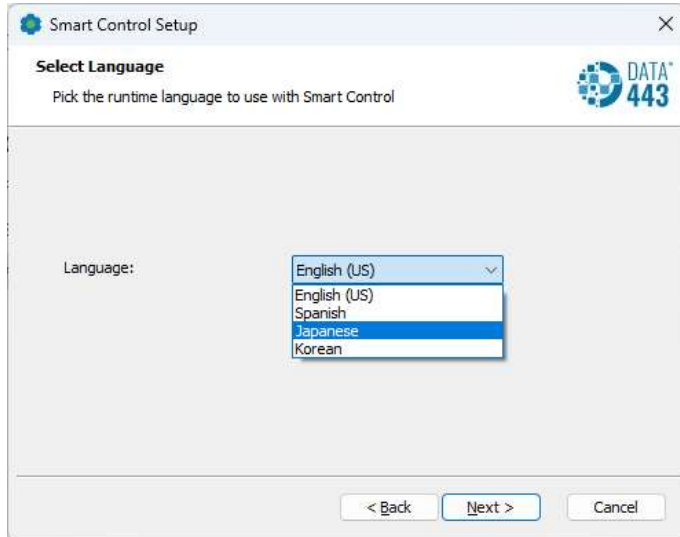
- (1) コンピュータに管理者権限でサインインしてください。
- (2) 「smartcontrol_ver※※※※_ja.exe」というファイルをダブルクリックしてください。スマートコントロールのインストールプログラムが起動します。
※ プログラム名の※※※※部分はバージョンによって表記が異なります。
- (3) [Next] をクリックしてください。



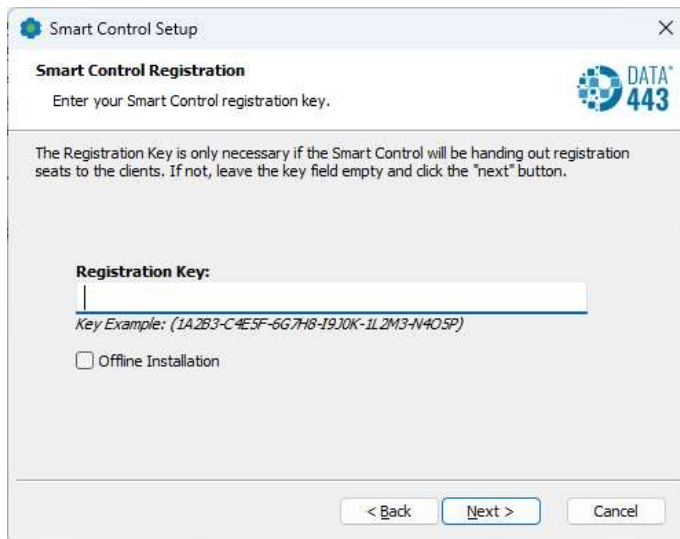
- (4) 画面の内容をよくお読みの上、 [I accept the terms in the License Agreement] にチェックを入れ、 [Next] をクリックしてください。



- (5) [Language] のリストから [Japanese] を選択し、[Next] をクリックしてください。



- (6) ライセンスキーを入力します。入力後 [Next] をクリックします。
ライセンスキーは “ - ” も含めて全て入力してください。



インターネット環境が無い場合や、Proxy 環境での認証（手動認証）を実行する際は [Offline Installation] にチェックを入れてください。

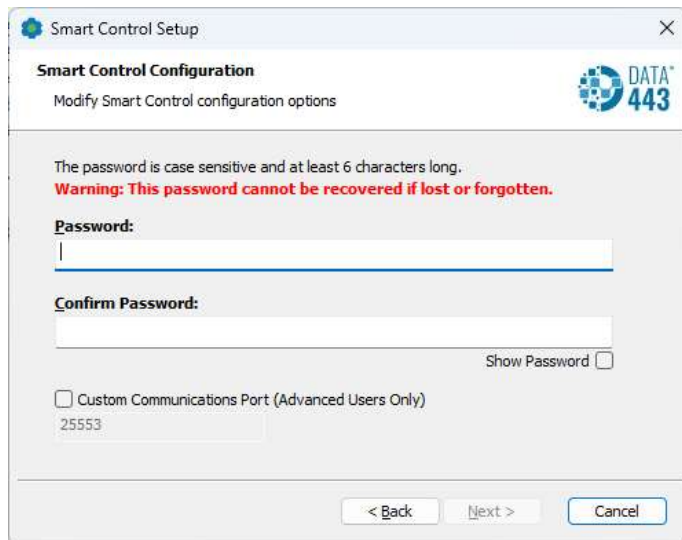
単独認証ライセンスのクライアントを遠隔制御する場合は、ライセンスキーを入力せずに [Next] をクリックしてください。詳細は [5.5.23 単独認証ライセンスのドライブシールドを遠隔制御する] を参照してください。

手動認証でインストールを実施した場合は、コンピュータの再起動後に認証作業が必要です。
インストール完了後、[4.2 手動認証によるインストール後の認証作業] を実施してください。

(7) 設定用のパスワードを設定します。

上段のテキストボックスに6文字以上の半角英数字で入力してください。

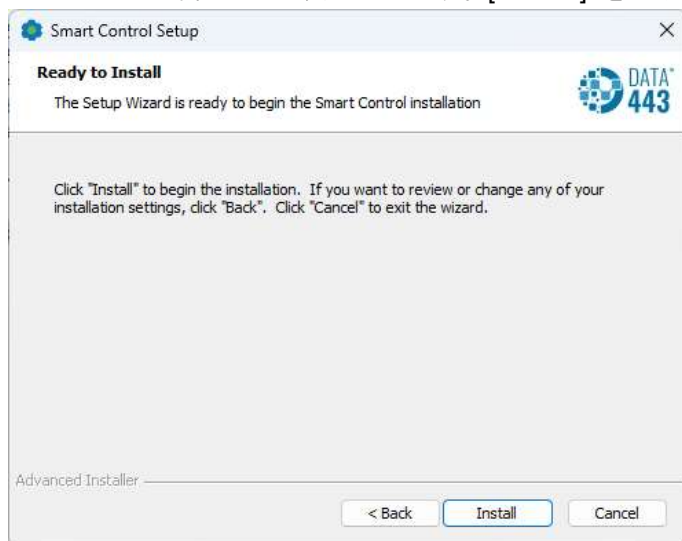
入力確認用の下段テキストボックスに同じパスワードを入力し、[Next] をクリックしてください。



The image shows a Windows-style dialog box titled "Smart Control Setup" with a close button (X) in the top right corner. The main title is "Smart Control Configuration" and the subtitle is "Modify Smart Control configuration options". The DATA 443 logo is in the top right. The text reads: "The password is case sensitive and at least 6 characters long. Warning: This password cannot be recovered if lost or forgotten." Below this are two text input fields: "Password:" and "Confirm Password:". To the right of the "Confirm Password:" field is a "Show Password" checkbox. Below the input fields is a checkbox labeled "Custom Communications Port (Advanced Users Only)" with the value "25553" in a small text box. At the bottom are three buttons: "< Back", "Next >", and "Cancel".

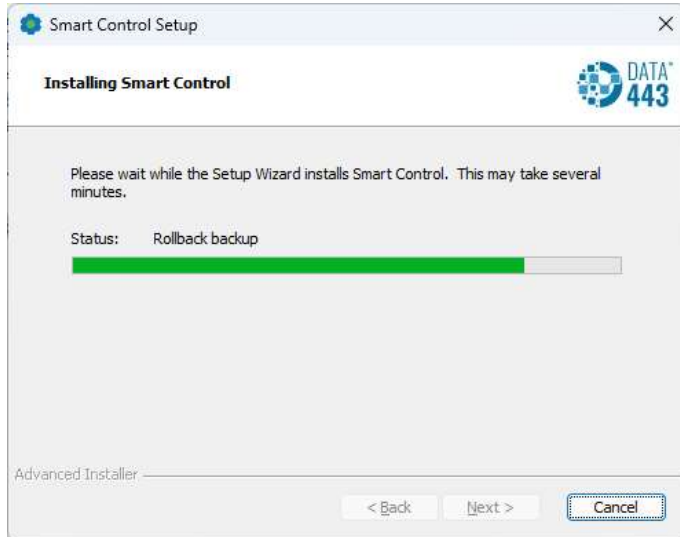
※ パスワードはお客様管理となります。紛失されないようご注意ください。

(8) インストール確認画面が表示されます。[Install] をクリックします。

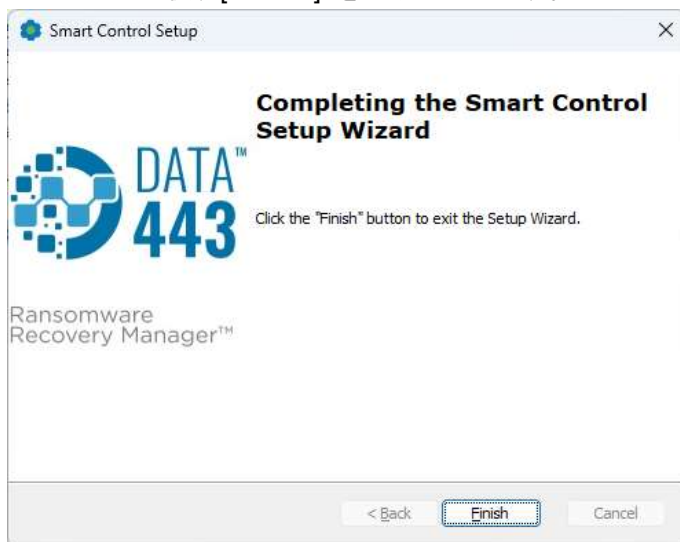


The image shows a Windows-style dialog box titled "Smart Control Setup" with a close button (X) in the top right corner. The main title is "Ready to Install" and the subtitle is "The Setup Wizard is ready to begin the Smart Control installation". The DATA 443 logo is in the top right. The text reads: "Click 'Install' to begin the installation. If you want to review or change any of your installation settings, click 'Back'. Click 'Cancel' to exit the wizard." At the bottom are three buttons: "< Back", "Install", and "Cancel".

(9) インストールが開始されます。しばらくお待ちください。



(10) インストール後、[Finish] をクリックします。

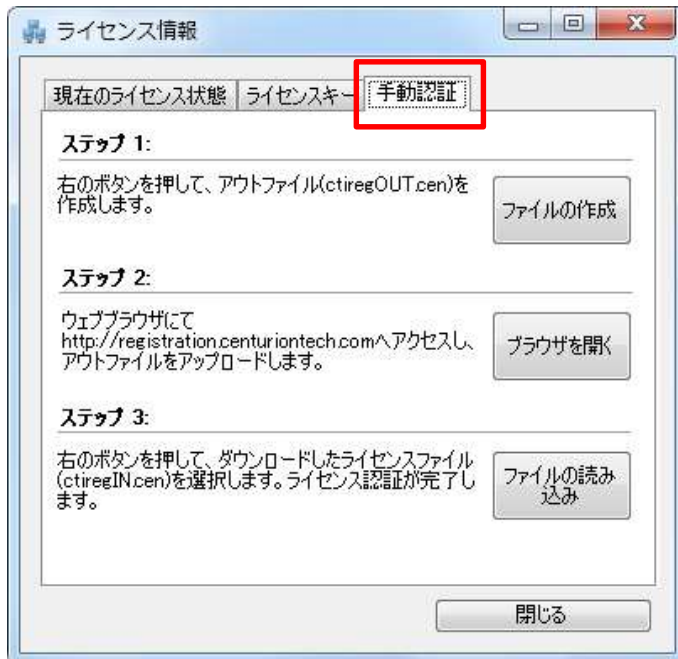


4.2 手動認証によるインストール後の認証作業

- (1) スマートコントロールを起動後、画面左の [127.0.0.1] を右クリックします。[ライセンス情報] をクリックします。

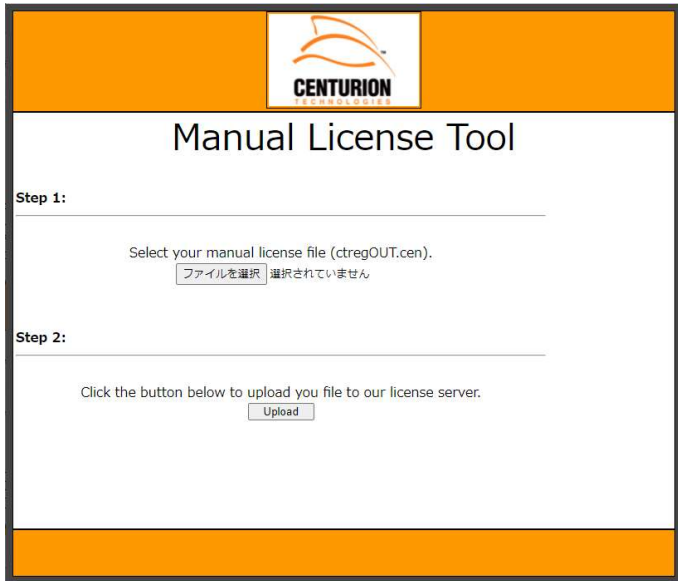


- (2) [手動認証] タブを開きます。ステップ 1 の [作成] をクリックし、ファイルを保存する場所を指定します。保存先に ctiregOUT.cen というファイルが作成されます。
※ ctiregOUT.cen のファイル名は変更しないでください。

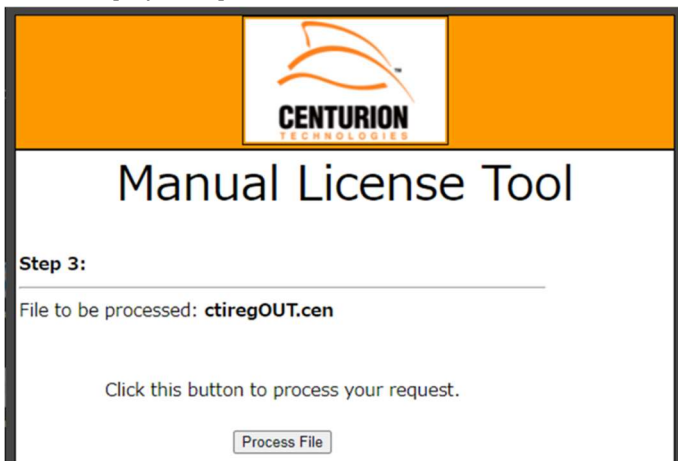


- (3) 次にステップ2の [ブラウザを開く] をクリックします。手動認証専用のウェブページへアクセスします。インターネットが使用できない環境の場合は、インターネットが使用できる端末から下記 URL へアクセスしてください。

<https://registration.centuriontech.com>



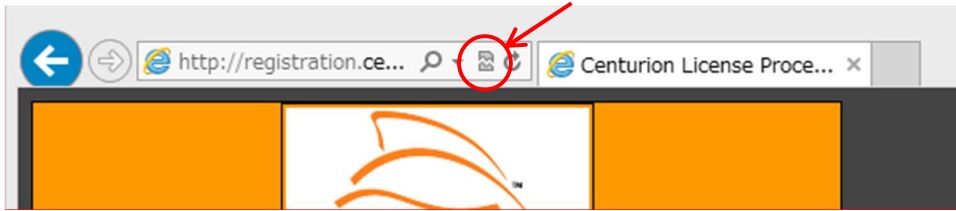
- (4) [ファイルを選択] をクリックし、(3) で作成した ctiregOUT.cen ファイルを選択します。その後、[Upload] をクリックします。画面内に File to be processed: ctiregOUT.cen と表示されます。



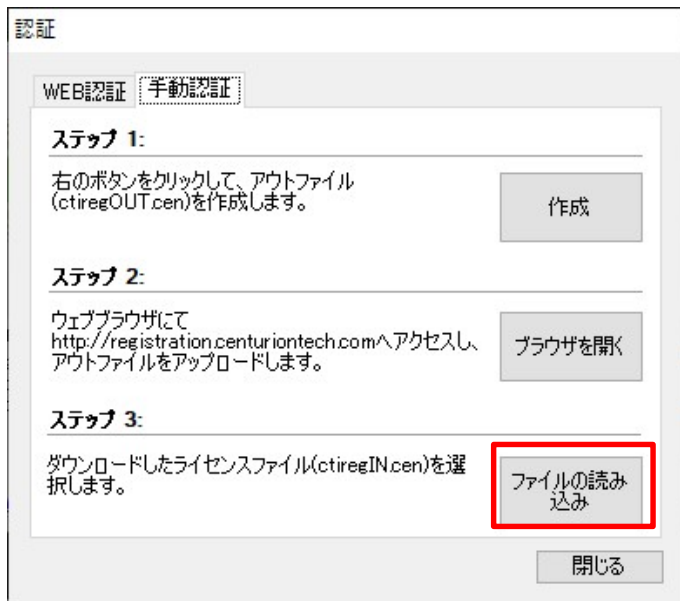
- (5) [Process File] をクリックします。画面内に表示された Download File をクリックし、ctiregIN.cen ファイルをダウンロードします。ファイルを任意の場所に保存してください。
 ※ ctiregIN.cen のファイル名は変更しないでください。



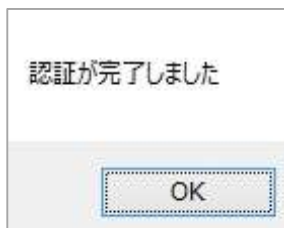
- ※ Internet Explorer 10 以降をご使用の場合、ファイルのダウンロードができない場合があります。この場合は、認証ページのトップページにて、アドレスバーの右にある互換表示ボタンをクリックして、互換性表示を有効にしてからファイルのアップロード、ダウンロードを実施してください。



- (6) (1)~(2) の手順で再度認証画面を開き、ステップ 3 [ファイルの読み込み] をクリックします。ダウンロードした ctiregIN.cen を選択してください。



- (7) 認証が成功すると、以下の画面が表示されます。コンピュータを再起動してください。



5. 操作方法

5.1 スマートコントロールの起動方法

スマートコントロールはインストール後、自動的にデスクトップ上に[Smart Control]アイコンを作成します。このアイコンをダブルクリックすることで、スマートコントロールが起動します。

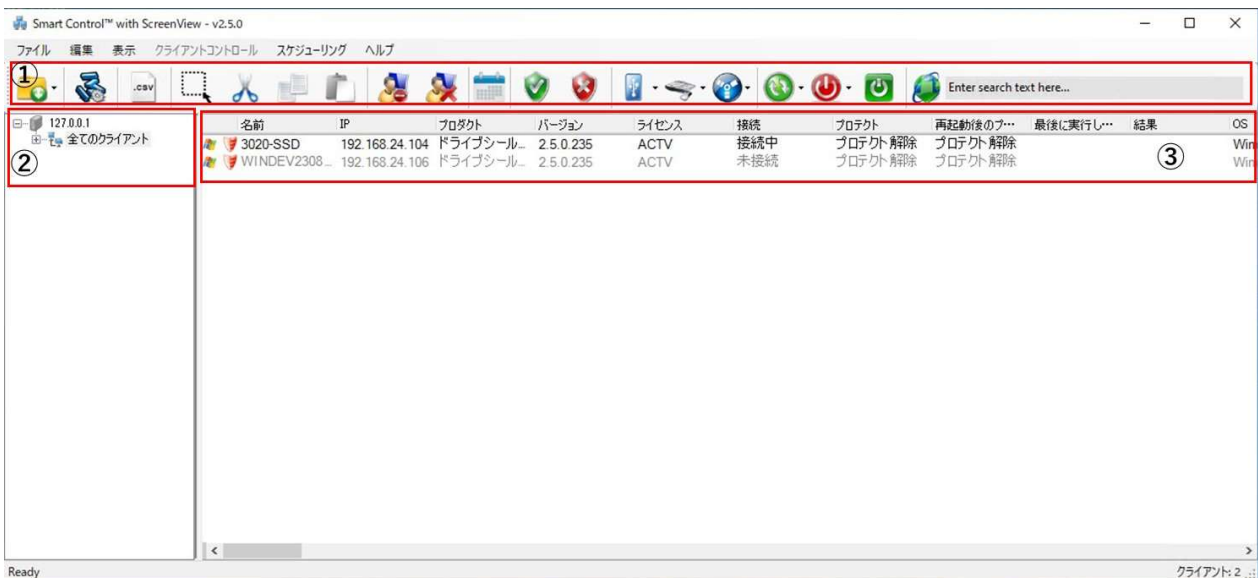


誤ってアイコンを削除した場合は以下のプログラムから起動することが可能です。

C:\Program Files\Data443 Risk Mitigation, Inc\Smart Control\CtiControlCenter.exe

5.2 画面の説明

スマートコントロールの画面です。接続したクライアントの情報が一覧で確認できます。



- ① ツールバー
スマートコントロールの設定変更やクライアントコンピュータを制御するアイコンが表示されています。アイコン上にマウスポインタを重ねると、その機能の簡単な説明を表示します。
- ② グループペイン
接続したクライアントを表示します。
グループを作成し、クライアントをグループ別に表示させることができます。
- ③ クライアントリスト
このスマートコントロールに接続したクライアントコンピュータのリストです。
インストールしているドライブシールド SS のバージョンやコンピュータ名などのステータスを確認することができます。

5.3 ツールバーのカスタマイズ

メニューバーの [表示] → [ツールバー] からアイコンの表示/非表示のカスタマイズが可能です。
項目からチェックを外すと、構成されたアイコンが非表示になります。

アイコンの構成

| | |
|-------|------------------|
| 標準 | |
| プロテクト | |
| 電源管理 | |
| モジュール | ※これらの機能は使用できません。 |

各アイコンの説明

| アイコン | 機能 | アイコン | 機能 |
|------|---------------------------|------|-------------------------|
| | 新規グループ グループフィルタの作成 | | 初期設定 |
| | CSV エクスポート | | 全てを選択 |
| | 切り取り | | コピー |
| | 貼り付け | | グループからクライアントを 削除 |
| | スマートコントロールから クライアントを削除 | | スケジューリング |
| | プロテクトモード | | プロテクト解除モード |
| | USB デバイスの ロック/ロック解除 | | キーボードとマウスのロック/ ロック解除 |
| | Firewire のロック/ロック解除 | | 再起動 |
| | シャットダウン | | 起動 |

| | |
|---|--|
| <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> Enter search text here... </div> | <p>検索バー クライアントのステータスを横断的に検索できます。検索可能項目：名前、IP、バージョン、OS バージョン、MAC、最後に実行したコマンド、結果</p> |
|---|--|

5.4 クライアントリストのグループ作成

グループを作成し、クライアントをグループ別に表示させることができます。

プロテクトモードへの変更などの操作がグループ単位で可能になるため、管理するクライアントの台数が多い場合、グループ分けを行うと便利です。



5.4.1 新規グループを作成する

- (1) 画面左ツリーの「127.0.0.1」を選択した状態で、メニューバーの [ファイル]-[新規]-[グループ] を選択するか、画面左ツリー下の空欄部分を右クリックし、[新規グループ] をクリックします。
- (2) [新規グループ] というフォルダが作成されます。グループ名を変更するには、作成したグループを右クリックし、[名前変更] を選択します。

5.4.2 サブグループを作成する

- (1) 新規グループにて作成したグループを右クリックし、[新規(サブグループ)] を選択します。
- (2) [新規グループ] というフォルダが作成されます。グループ名を変更するには、作成したグループを右クリックし、[名前変更] を選択します。

5.4.3 クライアントをグループに登録する

- (1) 画面左側で [全てのクライアント] をクリックした後、画面右側のリストから、対象のクライアントを選択します。
- (2) メニューバーの [編集]-[コピー] をクリックし、登録したいグループのフォルダをクリックした後、[編集]-[貼り付け] をクリックします。または、対象となるクライアントを選択したまま、登録したいグループのフォルダにドロップします。

5.4.4 グループフィルタを登録する

フィルタリングを使用してクライアントのグループ分けが可能です。

- (1) 画面左ツリーの「127.0.0.1」を選択した状態で、メニューバーの [ファイル] - [新規] - [グループフィルタ] を選択するか、または右クリックし、[新規グループフィルタ] を選択します。フィルタリングの設定画面が表示されます。

- (2) [グループフィルタ名] にグループフォルダの名前を入力します。
- (3) それぞれのフィルタリングの設定を行った後、[保存] ボタンをクリックします。フィルターグループが作成されます。

5.4.5 グループを削除する

グループのフォルダを右クリックし [削除] を選択します。グループのフォルダが削除されます。

5.4.6 クライアントをグループから削除する

対象のグループフォルダをクリックし、表示されたクライアントを選択した後、メニューバーの [編集] → [グループからクライアントを削除] を選択します。

または、クライアントを右クリックで選択し、[グループからクライアントを削除] を選択します。

5.5 基本操作

スマートコントロールからクライアントを制御するための基本的な操作方法です。

5.5.1 コントロールの対象とするクライアントの選択方法

(1) 全てのクライアントを選択する方法

左側の画面で [全てのクライアント] をクリックし、右側のクライアントの一覧内をクリックした後、メニューバーの [編集] → [全てのクライアントを選択] を選択します。

(2) グループ内の全てのクライアントを選択する方法

左側の画面で対象のグループフォルダを選択し、右側のクライアントの一覧内をクリックした後、メニューバーの [編集] → [全てのクライアントを選択] を選択します。

(3) 任意の複数のクライアントを選択する方法

範囲選択：

キーボードの [Shift] を押しながら、選択したい範囲内の一番上と一番下のクライアントをクリックします。

任意選択：

キーボードの [Ctrl] を押しながら、選択したいクライアントを1台ずつクリックしていきます。

5.5.2 プロテクト/プロテクト解除モード

プロテクトモードにする方法

(1) 対象のクライアントを選択します。

(2) メニューバーの [クライアントコントロール] → [プロテクトモード] → [クライアントをプロテクトモードへ] を選択します。または、画面上部の [プロテクト] ボタン をクリックします。

(3) [パスワード入力] というダイアログが表示されますので、クライアント側のドライブシールド SS に設定したパスワードを入力し、[OK] をクリックします。

(4) 次に、メニューバーの [クライアントコントロール] から [電源管理] → [クライアントを再起動] 又は [クライアントを遅延再起動] を選択し、クライアントを再起動します。

※未保存のデータがあっても強制的に再起動されますので、ご注意ください。

(5) 再起動後、対象のクライアントがプロテクトモードになります。

プロテクト解除モードにする方法

(1) 対象のクライアントを選択します。

(2) メニューバーの [クライアントコントロール] → [プロテクトモード] → [クライアントをプロテクト解除モードへ] を選択します。または、画面上部の [プロテクトを解除] ボタン をクリックします。

(3) [パスワード入力] というダイアログが表示されますので、クライアント側のドライブシールド SS に設定したパスワードを入力し、[OK] をクリックします。

(4) 次に、メニューバーの [クライアントコントロール] から [電源管理] → [クライアントを再起動] 又は [クライアントを遅延再起動] を選択し、クライアントを再起動します。

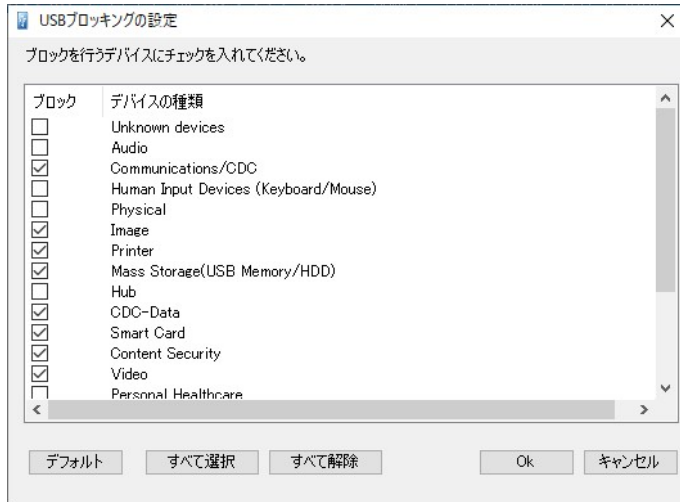
※未保存のデータがあっても強制的に再起動されますので、ご注意ください。

(5) 再起動後、対象のクライアントがプロテクトモード解除モードになります。

5.5.3 USB ブロッキング

USB ブロッキングを有効にする

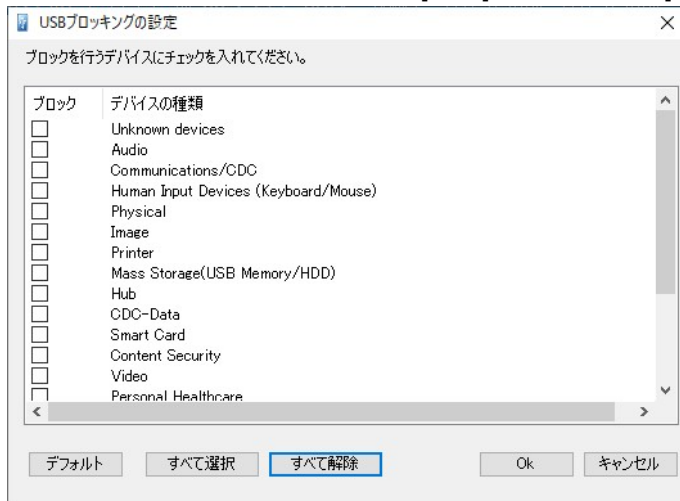
- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [プロテクトモード] → [USB ブロッキングを有効] を選択します。または、画面上部の [USB] ボタン から [USB ブロッキングを有効] をクリックします。



- (3) [パスワード入力] というダイアログが表示されますので、クライアント側のドライブシールド SS に設定したパスワードを入力し、[OK] をクリックします。
- (4) “結果”のステータスに[Success]と表示されれば、操作完了です。

USB ブロッキングを無効にする

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [プロテクトモード] → [USB ブロッキングを無効] を選択します。または、画面上部の [USB] ボタン から [USB ブロッキングを無効] をクリックします。



- (3) [パスワード入力] というダイアログが表示されますので、クライアント側のドライブシールド SS に設定したパスワードを入力し、[OK] をクリックします。
- (4) “結果”のステータスに[Success]と表示されれば、操作完了です。

5.5.4 キーボード・マウスのロック

クライアントのキーボードとマウスをロック（使用不可）/ロック解除（使用可能）にする事が可能です。また、ロック時に表示される画面の背景色、文章を変更することも可能です。

キーボードとマウスをロック（使用不可）する

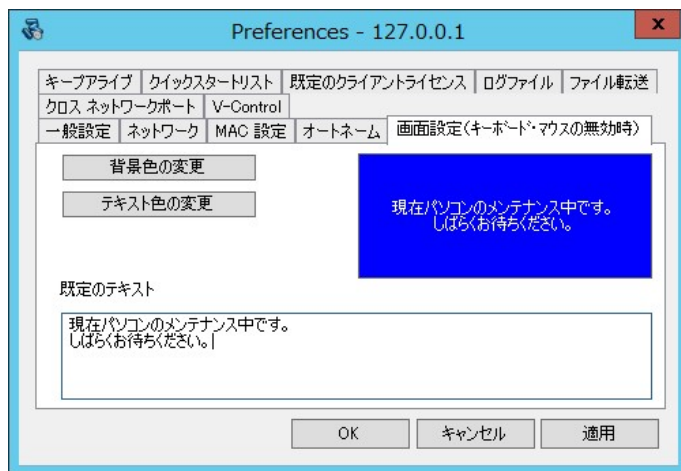
- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [プロテクトモード] → [キーボードとマウスを無効] を選択します。または、画面上部の [キーボード・マウス] ボタン から [キーボードとマウスを無効] をクリックします。
- (3) クライアントの画面が赤くなり、キーボードとマウスがロックされている旨のメッセージが表示されます。キーボードとマウスが使用不可となります。
※ログイン画面では、キーボードとマウスのロック時の赤色画面は表示されません。

ロック時の画面を変更する

ロック時にクライアントに表示される文章と背景色を設定することが可能です。

- (1) メニューバーの [ファイル] → [初期設定] をクリックします。
- (2) 「画面設定(キーボード・マウス無効時)」のタブを開きます。
- (3) 背景色の変更は「背景色の変更」をクリックして任意の色に変更後、「OK」をクリックします。
- (4) 文字色の変更は「テキスト色の変更」をクリックして任意の色に変更後、「OK」をクリックします。
- (5) 文章の変更は「既定のテキスト」欄に任意のメッセージを記入し、「OK」をクリックします。

設定例：

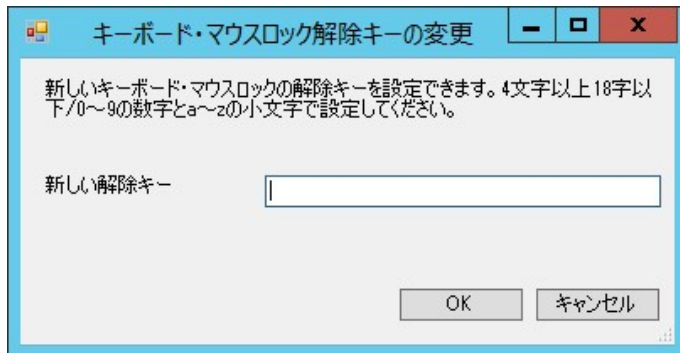


キーボードとマウスをロック解除（使用可能）する

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [プロテクトモード] → [キーボードとマウスを有効] を選択します。または、画面上部の [キーボード・マウス] ボタン から [キーボードとマウスを有効] をクリックします。
- (3) クライアントの赤い画面が消え、クライアントのキーボードとマウスが使用可能となります。

キーボードとマウスのロック解除キーの変更

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [プロテクトモード] → [キーボード・マウスのロック解除キーの変更] を選択します。以下のダイアログが表示されます。



- (3) 新しく設定する解除キーを入力し、OK をクリックします。
- (4) [パスワード入力] というダイアログが表示されますので、クライアント側のドライブシールド SS に設定したパスワードを入力し、[OK] をクリックします。
- (5) “結果”のステータスに[Success]と表示されれば、操作完了です。

5.5.5 ステルスモード

クライアントのプロテクト/プロテクト解除の状態を示すアイコンを表示、または非表示に設定できます。ステルスモードがオンの場合、アイコンは非表示になります。ステルスモードについての詳細は、ドライブシールド SS のマニュアルをご確認ください。

ステルスモードを有効にする

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [その他の設定] → [ステルスモードを有効] を選択します。
- (3) [パスワード入力] というダイアログが表示されますので、クライアント側のドライブシールド SS に設定したパスワードを入力し、[OK] をクリックします。
- (4) “結果”のステータスに[Success]と表示されれば、操作完了です。

ステルスモードを無効にする

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [その他の設定] → [ステルスモードを無効] を選択します。
- (3) [パスワード入力] というダイアログが表示されますので、クライアント側のドライブシールド SS に設定したパスワードを入力し、[OK] をクリックします。
- (4) “結果”のステータスに[Success]と表示されれば、操作完了です。

5.5.6 電源管理

クライアント端末の電源オン/オフ/再起動などを管理することが可能です。

再起動する方法

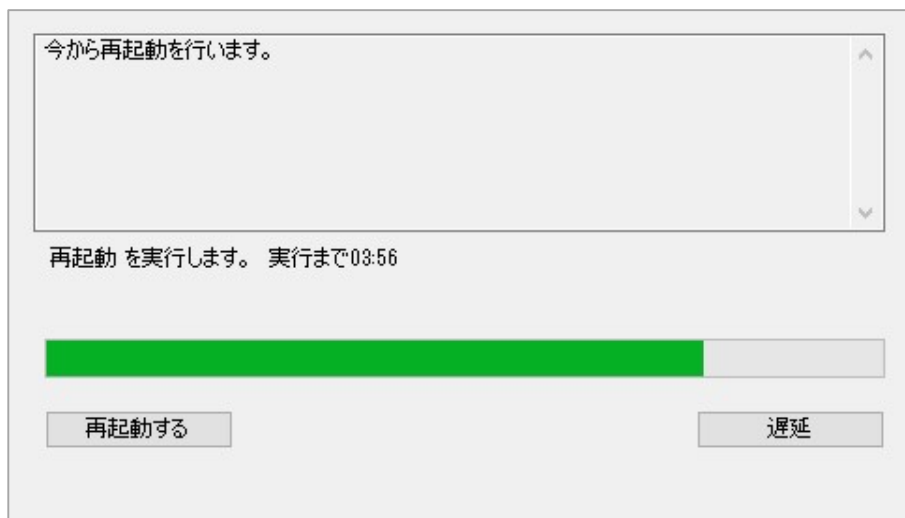
- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [電源管理] → [クライアントを再起動] を選択します。
- (3) クライアントの再起動が始まります。

指定した時間後に再起動する方法

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [電源管理] → [クライアントを遅延再起動] を選択します。
- (3) クライアントに通知するメッセージをメッセージ欄に入力します。その後、時間と保留回数を指定し、[OK] ボタンをクリックします。



- (4) クライアント側では、次のようなダイアログが表示されます。
[遅延] をクリックすると、現在の残り時間に、指定した時間が追加されます。
[再起動する] をクリックすると、すぐに再起動を行います。



再起動をキャンセルする方法

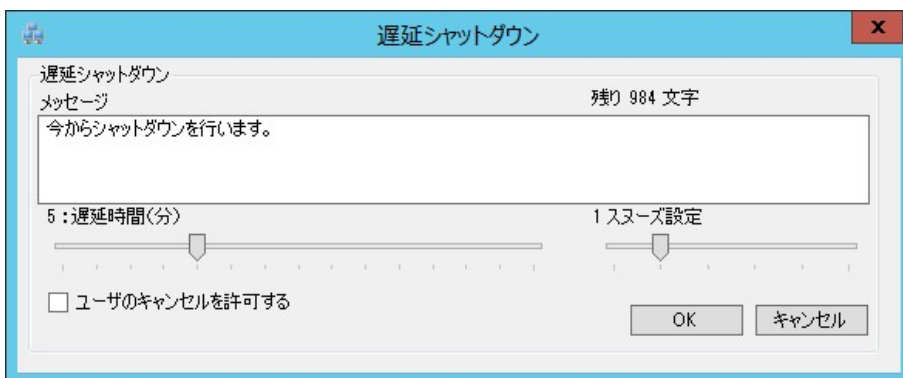
- (1) 実行したクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [電源管理] → [遅延再起動をキャンセル] を選択します。
- (3) 再起動がキャンセルされます。

シャットダウンする方法

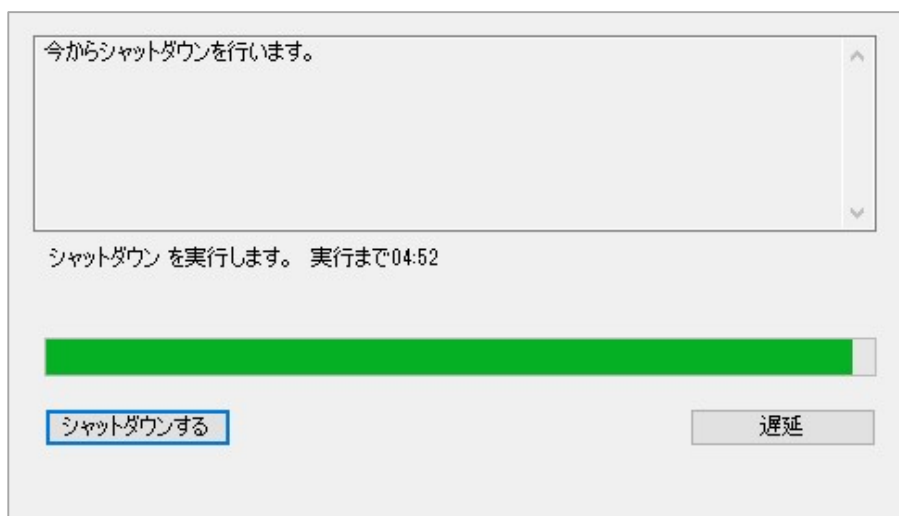
- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [電源管理] → [クライアントをシャットダウン] を選択します。
- (3) シャットダウンが始まります。

指定した時間後にシャットダウンする方法

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [電源管理] → [クライアントを遅延シャットダウン] を選択します。
- (3) クライアントに通知するメッセージをメッセージ欄に入力します。その後、時間と保留回数を指定し、[OK] ボタンをクリックします。



- (4) クライアント側では、次のようなダイアログが表示されます。ここで [遅延] をクリックすると、現在の残り時間に、指定した時間が追加されます。[シャットダウンする] をクリックすると、すぐにシャットダウンを行います。



シャットダウンをキャンセルする方法

- (1) 実行したクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [電源管理] → [遅延シャットダウンをキャンセル] を選択します。
- (3) シャットダウンがキャンセルされます。

起動する方法

※ 起動には、対象のコンピュータが Wake on LAN に対応している必要があります。対象のコンピュータの Wake on LAN 対応の可否、または Wake on LAN 自体の設定方法等につきましては、各コンピュータのベンダー様へお問い合わせください。

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [電源管理] → [起動 (Wake on LAN)] を選択します。
- (3) クライアントの起動が始まります。

再起動する時間を設定する

クライアントコンピュータを 1日 1回、指定した時間に自動的に再起動を実行させることが可能です。

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [その他の設定] → [デイリー・リブート] を選択します。設定ダイアログが表示されます。



- (3) 「有効」にチェックをいれ、クライアントを再起動させる時間を設定します。
- (4) [OK] をクリックします。パスワード入力画面が表示されます。パスワードを入力し [OK] をクリックしてください。

5.5.7 クライアントのパスワード管理

クライアントのドライブシールド SS に設定したパスワードを変更することができます。

パスワードの変更

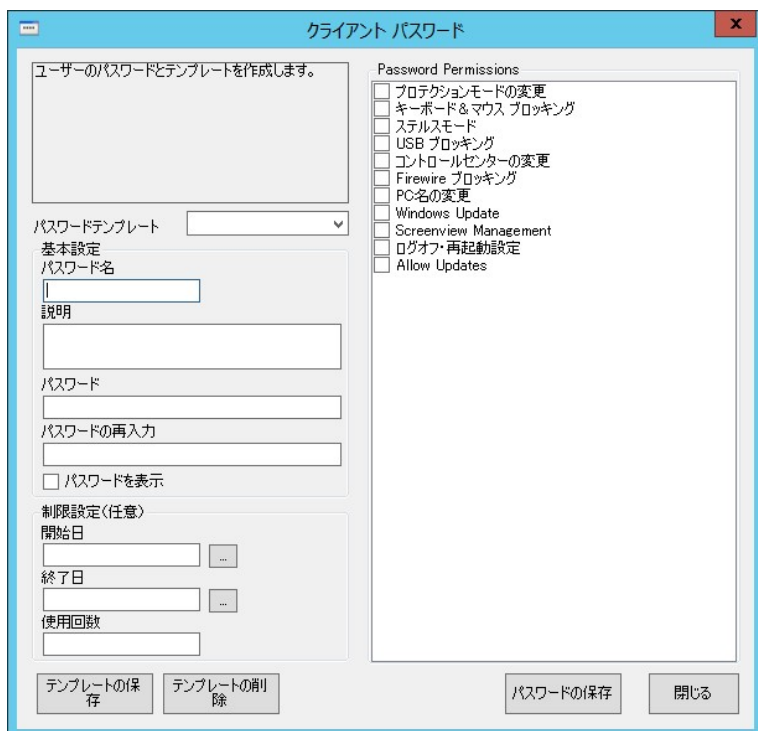
- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [パスワード] → [パスワード管理] をクリックします。
- (3) 次のダイアログが表示されます。上の段に従来のパスワード、中段に新しいパスワードを入力し、確認の為、下段に新しいパスワードを再入力し [OK] をクリックしてください。
※ “パスワード表示” にチェックを入れると、入力内容の確認ができます。



機能毎にパスワードを設定する

プロテクトモード変更時のみ適応されるパスワードや USB デバイス制御設定変更時のみ適応されるパスワードを設定できます。

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [パスワード] → [パスワードの追加] を選択します。下図の設定画面が表示されます。



- (3) [Password Permissions] 欄より、パスワードを設定したい機能を選択します。
- (4) 「基本設定」からパスワード名やパスワードを設定します。

[パスワード名]

パスワード名を設定します。

[説明]

設定するパスワードに注釈を加える場合はこの欄に記入します。

[パスワード]

設定するパスワードを入力します。

[パスワードの再入力]

確認用にもう一度パスワードを設定します。

- (5) 「制限設定(任意)」よりオプションの設定を行います。
※こちらの設定は必要な場合のみ行ってください。

[開始日]

パスワードの開始時期を設定します。

[終了日]

パスワードの終了時期を設定します。

[使用回数]

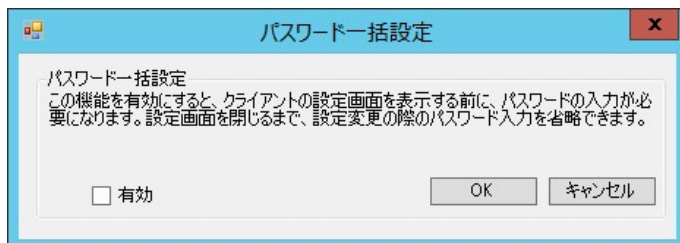
パスワードの使用回数を設定します。

- (6) 「パスワードの保存」をクリックし、インストール時に設定したパスワードを入力します。
- (7) 設定したパスワードはメニューバーの [クライアントコントロール] → [パスワード] → [パスワードの確認] から確認できます。

パスワード一括入力設定

この設定を行うことで、クライアントで行う設定変更時のパスワード入力を省略することが可能です。

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [その他の設定] → [パスワード一括設定] を選択します。設定ダイアログが表示されます。



- (3) [有効] にチェックいれ、「OK」をクリックします。パスワード入力画面が表示されます。パスワードを入力し「OK」をクリックします。

5.5.8 Optional Directory Protection (ODP)

ODP を使用することで、ドライブ内にあるフォルダをプロテクト対象から除外することが可能です。プロテクト状態のドライブでも、指定したフォルダ内のファイルの更新維持が可能になります。

※機能詳細についてはドライブシールドのインストール/操作ガイドをご参照ください。

- (1) 対象のクライアントを選択します。
- (2) メニューバーの[クライアントコントロール] → [その他の設定] → [Optional Directory Protection] を選択します。
- (3) テキストボックスの中に、対象のフォルダをフルパスで入力します。
- (4) [OK] をクリックします。以下のダイアログが表示されます。
- (5) [はい] をクリックして、パスワードを入力します。クライアントの再起動後、設定が適用されます。

指定を解除する場合は、解除したいフォルダをフルパスで入力し、[プロテクトの除外を解除] にチェックを入れます。その後、[OK] をクリックし、パスワードを入力します。再起動後に変更が適用されます。

※フォルダを ODP から解除しても、実際のフォルダは削除されません。

5.5.9 印刷の制限機能

クライアントで実行される印刷の許可・制限をスマートコントロールから制御できます。

印刷を無効にする

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [その他の設定] → [印刷を無効] を選択します。
- (3) パスワード入力画面が表示されます。パスワードを入力し[OK]をクリックします。

印刷を有効にする

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [その他の設定] → [印刷を有効] を選択します。
- (3) パスワード入力画面が表示されます。パスワードを入力し[OK]をクリックします。

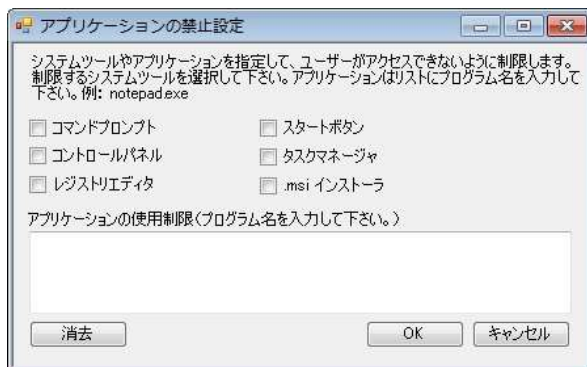
5.5.10 アプリケーションの禁止設定

コンピュータのシステムツールや、指定したアプリケーションをユーザが使用できない様に、アクセス制限を設定することが可能です。

- (1) 対象のクライアントを右クリックで選択します。
- (2) [その他の設定] → [禁止設定] を選択します。設定ダイアログが表示されます。
- (3) アクセス制限を設定する項目にチェックを入れてください。以下の機能が選択可能です。

| 設定項目 | 動作内容 |
|-------------|-----------------------|
| コマンドプロンプト | コマンドプロンプトの起動を禁止します |
| コントロールパネル | 設定、コントロールパネルの起動を禁止します |
| レジストリエディタ | レジストリエディタの起動を禁止します |
| スタートボタン | タスクバーを非表示にします |
| タスクマネージャ | タスクマネージャの起動を禁止します |
| .msi インストーラ | .msi インストーラの起動を禁止します |

アプリケーションを指定する場合は、[アプリケーションの使用制限] 欄のテキストボックスにプログラム名を入力してください。例：msedge.exe



- (4) [OK] をクリックします。パスワード入力画面が表示されます。パスワードを入力し [OK] をクリックしてください。クライアントを再起動後、設定が反映されます。
- (5) 制限を解除する場合は、[消去] をクリックしたあと、[OK] をクリックします。パスワード入力画面が表示されます。パスワードを入力し [OK] をクリックします。再起動後、制限が解除されます。

5.5.11 スマートコントロールの変更について

クライアントが接続を行うスマートコントロールを変更します。

※クライアントの設定画面にある [スマートコントロール] から接続設定を変更することも可能です。

※設定変更後に接続するスマートコントロールは、予めインストールしておく必要があります。

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [コントロールセンターの変更] → [Primary] をクリックします。
- (3) 次のダイアログが表示されます。上段に変更先のスマートコントロールがインストールされたコンピュータの IP アドレスを入力し、下段にポート番号を入力します。（ポート番号既定値：25553）



- (4) 入力後、[テスト] をクリックします。

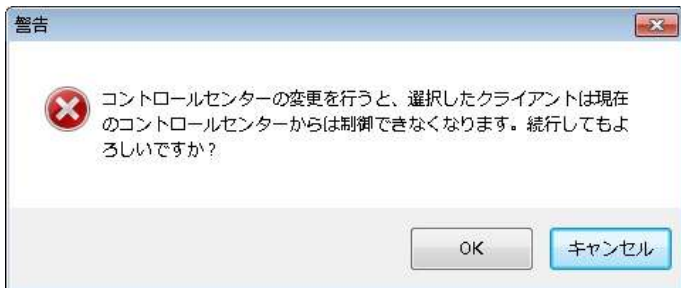
- (5) [OK] をクリックします。



- (6) 接続テストの完了後に [OK] ボタンをクリックします。



- (7) [OK] をクリックします。



- (8) [パスワード入力] ダイアログが表示されます。クライアント側のドライブシールド SS に設定したパスワードを入力し、[OK] をクリックします。
- (9) 接続先のスマートコントロールにて、該当のクライアントが正常に接続されたかをご確認下さい。

5.5.12 リモート実行について

この機能は、指定したバッチファイルをクライアントへ実行させることができます。使用例として、Windows の設定変更や、特定のソフトウェアの更新などが可能になります。

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [リモート実行] をクリックします。
- (3) 次のダイアログが現れます。フォルダアイコンをクリックし、ファイル一覧から実行するバッチファイルを選択します。
※指定できるファイルサイズは、50kb が上限です。
- (4) [リモート実行] ボタンをクリックします。クライアント側でバッチファイルが実行されます。



5.5.13 クライアントのプロパティ

クライアントの端末の情報や、現在の設定内容を確認できます。

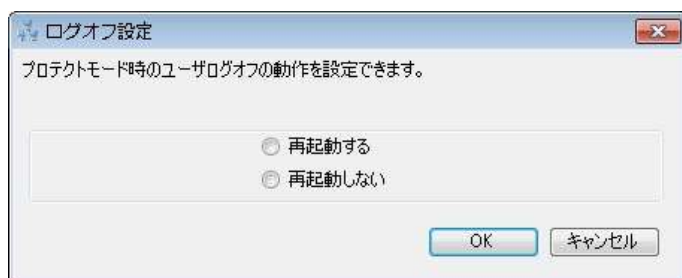
- (1) 対象のクライアントを右クリックで選択します。
- (2) メニューから[プロパティ] を選択します。表示された画面にて、現在の設定内容等を確認することができます。

5.5.14 クライアントのログオフを再起動に変更する

ドライブシールド SS の環境復元機能は、コンピュータの電源を再起動することで、一時保存領域に蓄積されたデータがリセットされ、元の状態に復元されます。そのため、「ログオフ」 - 「ログオン」の動作では復元されません。

以下の設定を変更することで、クライアントがログオフを行った際に再起動を実行し、環境復元を行う事が可能です。

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [その他の設定] → [クライアントのログオフ設定] を選択します。

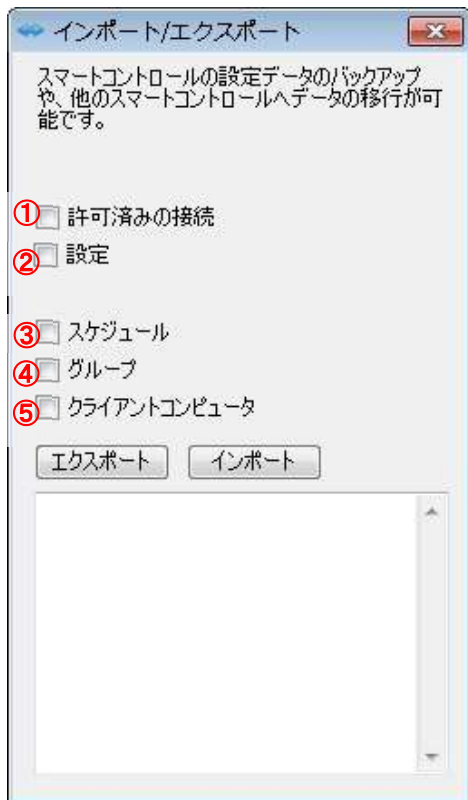


- (3) [再起動する] を選択し、[OK] をクリックします。パスワード入力画面が表示されます。パスワードを入力し[OK] をクリックします。

5.5.15 設定のインポート・エクスポートについて

スマートコントロールで設定したスケジュールやグループフォルダなどをファイル形式で保存することが可能です。保存した設定ファイルは、移行先のスマートコントロールにもインポートが可能です。

- (1) メニューバーの[ファイル] → [データのインポート/エクスポート]を選択します。以下のダイアログが表示されます。



- | | |
|----------------|--------------------------|
| ① 許可済みの接続 | リモート接続しているスマートコントロールの設定 |
| ② 設定 | スマートコントロールの初期設定 |
| ③ スケジュール | スマートコントロールにて作成したスケジュール |
| ④ グループ | スマートコントロールにて作成したグループフォルダ |
| ⑤ クライアントコンピュータ | 接続されているクライアントコンピュータの情報 |

- (2) それぞれエクスポートしたい設定のチェックボックスにチェックを入れ、[エクスポート]ボタンをクリックします。
- (3) ファイル名を付けて保存します。設定をインポートする場合は、[インポート] ボタンをクリックして保存したファイルを選択します。

5.5.16 別コンピュータへのスマートコントロールの移行について

設定のインポート・エクスポート機能を使用して、別コンピュータへスマートコントロールを移行することが可能です。移行時には、スマートコントロールのライセンスキーの認証リセットが必要です。保守サポート期間内にサポート窓口へ認証リセットを依頼してください。

ライセンスキーの認証リセットが完了してから、前項(2)の設定ファイルのエクスポート実施後、下記の手順をご実施ください。

- (1) 移行前のコンピュータからスマートコントロールをアンインストールします。
- (2) 移行先のコンピュータにスマートコントロールをインストールします。
- (3) インストール後、メニューバーの [ファイル] → [データのインポート/エクスポート] をクリックします。
- (4) [インポート]ボタンをクリック後、移行前のスマートコントロールから書き出した.cenx ファイルを選択して下さい。
- (5) インポート完了後、クライアント、グループ、スケジュール等が復元されているかご確認下さい。

移行後のコンピュータの IP アドレスが移行前のコンピュータと異なる場合、クライアントのドライブシールド SS の接続先設定を変更する必要があります。以下の手順で設定を変更することが可能です。

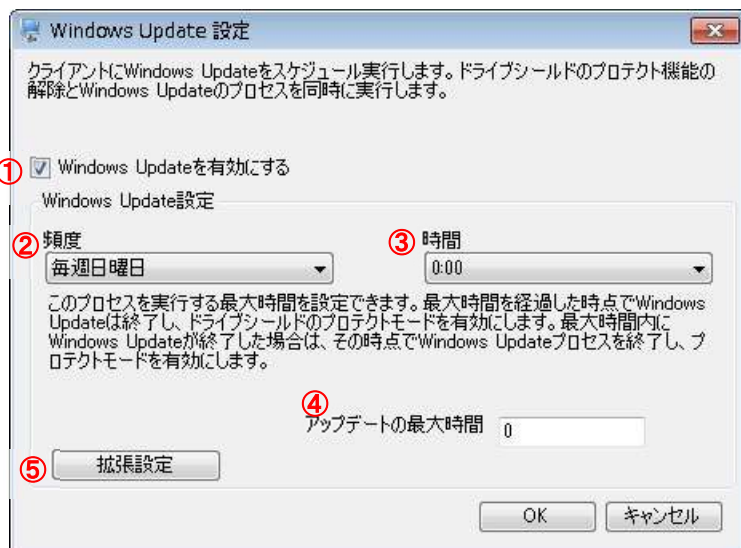
- (1) 接続先設定を変更するクライアントコンピュータにて、ドライブシールドの設定画面を開きます。
- (2) [管理設定] > [スマートコントロール] をクリックします。
- (3) [IP アドレス] 欄に移行先のスマートコントロールがインストールされているコンピュータの IP アドレスを入力します。
- (4) [DNS 名] 欄にスマートコントロールがインストールされているコンピュータのコンピュータ名を入力します。
- (5) [ポート] 欄にスマートコントロールと通信を行うポートを設定します。デフォルトの値は [25553] です。
- (6) [保存] をクリックします。次画面で再起動が必要と表示されますので [OK] をクリックします。
- (7) パスワード入力画面が表示されます。パスワードを入力し [OK] をクリックするとコンピュータが再起動し、設定が適用されます。

5.5.17 Windows Update 連携機能について

ドライブシールドには Windows Update を自動実行する[Windows Update 連携機能]があります。この機能の設定をスマートコントロールから行うことができます。

※Windows Update の実行中は、キーボード・マウスの操作を受け付けません。ご注意ください。
また、クライアントの Windows Update はスマートコントロールの[スケジューリング]機能でも実施することが可能です。設定方法につきましては[スケジューリング]の項目をご参照ください。

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [その他の設定] → [クライアントの Windows Update 設定] を選択します。以下のダイアログが表示されます。



- ① Windows Updates を有効にする
チェックを入れるとクライアントの Windows Update 機能を有効にします。
- ② 頻度
Windows Update を実行する曜日を指定します。

③ 時間

Windows Update を開始する時間を指定します。

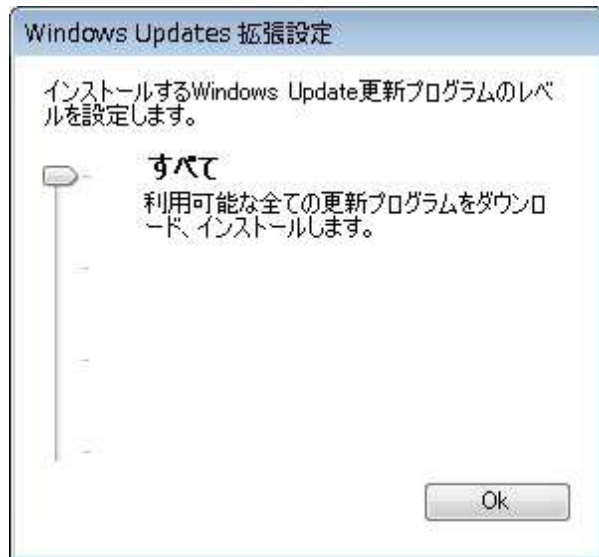
④ アップデートの最大時間

Windows Update を実行する最大時間を設定します。最小の設定は 40 分です。

⑤ 拡張設定

拡張設定ボタンをクリックすると、以下のダイアログが表示されます。

クライアントに適用する更新プログラムを 4 段階で指定することが可能です。



・すべて

利用可能な更新プログラムを全てダウンロードし、インストールします。

・推奨

深刻度「警告」「重要」「緊急」の修正プログラムをダウンロードし、インストールします。

・重要

深刻度「重要」「緊急」の修正プログラムをダウンロードし、インストールします。

・緊急

「緊急」の更新プログラムのみをダウンロードし、インストールします。

(3) [OK]ボタンをクリックし、パスワードを入力します。Windows Update の設定がクライアントコンピュータに適用されます。

5.5.18 WSUS/SUS 設定について

クライアントコンピュータの Software Update Services (以下 SUS) や、Windows Server Update Services (以下 WSUS) サーバの割り当てをスマートコントロールから変更することが可能です。

- (1) 対象のクライアントを選択します。
- (2) メニューバーの[クライアントコントロール] → [その他の設定] → [WSUS/SUS 設定]を選択します。
- (3) 以下のダイアログが表示されます。



- (4) [サーバ名]の欄に、WSUS/SUS サーバ名を http://の後に入力します。[チェックを入れると ~]の項目にチェックを入れると、クライアントから Windows Update の設定変更を防止することが可能です。
- (5) [OK]ボタンをクリックし、パスワードを入力します。クライアントコンピュータに WSUS/SUS サーバの設定が適用されます。

5.5.19 ファイル転送について

スマートコントロールのコンピュータからクライアントコンピュータへファイルを転送できます。

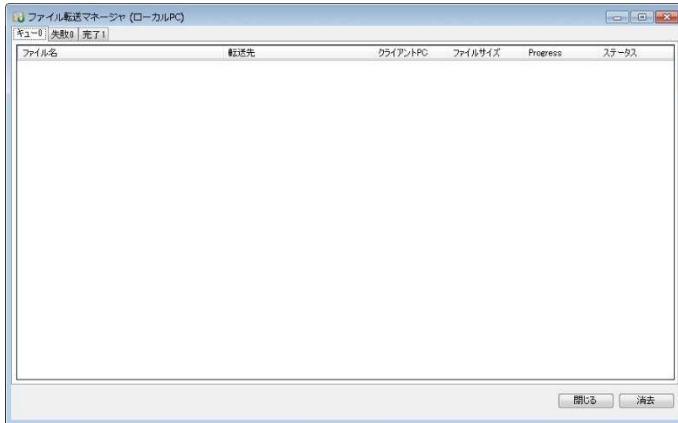
※ネットワークドライブや、サーバ上の共有フォルダから転送することはできません。対象のファイルをスマートコントロールコンピュータのハードディスクに保存し、ファイル転送を行ってください。

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [その他の設定] → [ファイル転送] を選択します。
- (3) 以下のダイアログが表示されます。



- (4) [転送するファイルを選択]をクリックします。ファイル選択ダイアログが表示されます。転送するファイルを選択します。
- (5) [転送先]では、転送先の保存場所を指定します。[デスクトップ]を選択すると、クライアントコンピュータのデスクトップにファイルが転送されます。指定したディレクトリに転送したい場合は、[ファイル転送先を指定する]を選択し、空欄に転送先のパスを入力します。

- (6) [送信]をクリックします。ファイル転送マネージャが表示され、対象のクライアントコンピュータにファイルが転送されます。

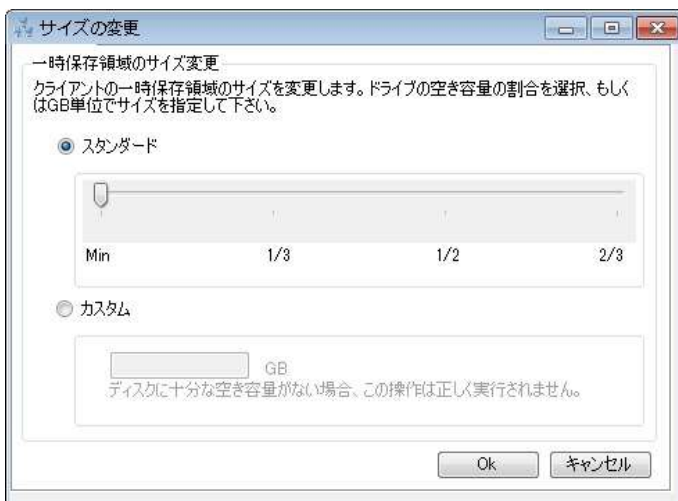


- ・ キュー
転送を待機しているクライアントを表示します。
- ・ 失敗
転送が失敗したクライアントを表示します。
- ・ 成功
転送が完了したクライアントを表示します。

5.5.20 一時保存領域のサイズ変更

クライアントコンピュータのドライブシールド SS が使用する一時保存領域の容量を、スマートコントロールから設定変更する事が可能です。

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [一時保存領域のサイズ変更] を選択します。設定画面が表示されます。



- (3) 一時保存領域のサイズを指定します。

- ・ スタンダード
一時保存領域のサイズを、ハードディスクの空き容量の Min (最小サイズ)、1/3、1/2、2/3 から選択できます。

- ・カスタム
- 一時保存領域のサイズを、GB 単位で入力して指定できます。

- (4) OK ボタンをクリックし、パスワードを入力します。クライアントコンピュータにてプロセスが実行され、一時保存領域のサイズが変更されます。

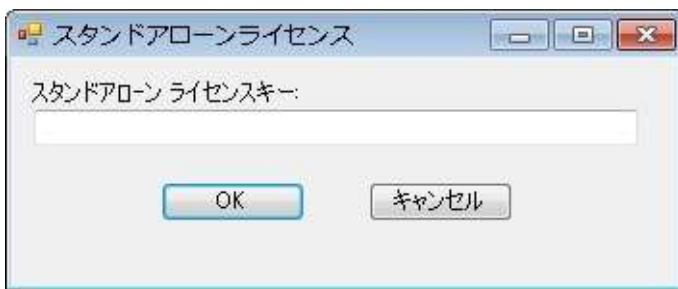
5.5.21 クライアントに単独認証用ライセンスキーを割り当てる

スマートコントロールと通信中のクライアントに、単独認証用のライセンスキーを割り当てます。単独認証用のライセンスキーを割り当てることで、クライアントはスタンドアロンの状態でも使用することが可能になります。

※ライセンス認証の際は、クライアントのコンピュータがインターネットへの接続と SSL プロトコルが利用可能である必要があります。

※プロキシ環境をご利用の場合は、ライセンスキーを割り当て後に手動認証の手順を実施してください。

- (1) 対象のクライアントを選択します。
- (2) メニューバーの [クライアントコントロール] → [スタンドアローンライセンスの割り当て] をクリックすると設定ダイアログが表示されます。



- (3) 入力欄に単独認証用ライセンスキーを入力し、[OK] ボタンをクリックします。
- (4) クライアントコンピュータの再起動が必要とのメッセージが表示されます。[はい] をクリックし、再起動します。起動後、クライアントコンピュータにライセンスキーが割り当てられます。

5.5.22 スケジューリング

スケジューリングの機能により、クライアントのプロテクトやプロテクト解除、再起動やシャットダウンの操作を自動的に行う事ができます。

この機能を利用する事により、例えば、深夜の時間帯に自動的にウイルス対策ソフトの定義ファイルの更新や Windows Update を行う事が可能になります。

※但し、ウイルス対策ソフトは指定した日時、またはコンピュータ起動時に自動的にアップデートされる設定になっている必要があります。

スケジュールの作成

画面の構成と、スケジュールの設定例をご説明します。

設定例として、特定のクライアントに対して、毎週水曜日の 21 時にプロテクトを解除し、23 時半にプロテクトを有効にし、シャットダウンを行います。

※ スケジュールは、21 時にプロテクトを解除する設定と 23 時半にプロテクトを有効にし、シャットダウンする設定の 2 つを作成します。

スケジュール 01：クライアント起動 → プロテクト解除 → 再起動

スケジュール 02：プロテクト → シャットダウン

スケジュール 01 と 02 の間に、プロテクト解除の状態が、2 時間半あります。

この時間を利用し、ウイルス対策ソフトの自動アップデート等を行う事ができます。

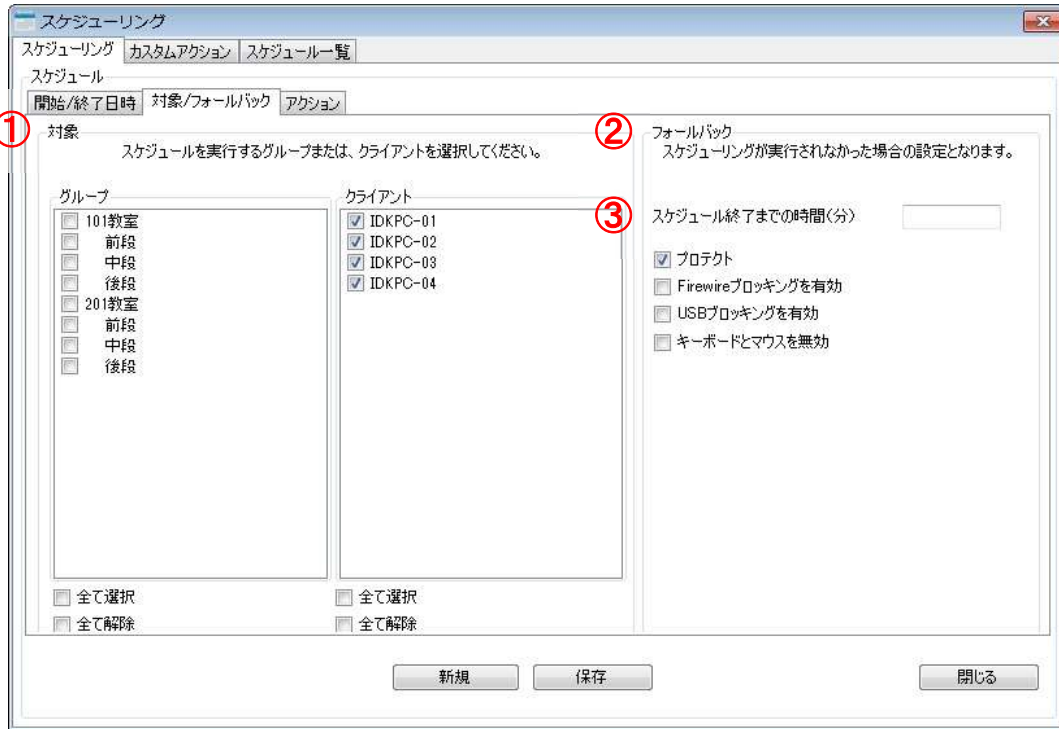
※ ウィルス対策ソフトの自動アップデートの設定に関しては、各ソフトウェアベンダー様へお問い合わせください。

初めに、スケジュール 01 を作成します。

- (1) メニューバーの [スケジュールリング] → [スケジュールリング] をクリックします。
- (2) [開始/終了日時] タブにて、開始/終了日時、スケジュール名等の設定を行います。

- ① 時間
開始時刻：スケジュールの開始時刻を設定します。
- ② 日程
1 回のみ、毎日、毎週（曜日指定）：毎月（日にち指定）の中から指定します。
- ③ 期限
スケジュールの開始日と終了日を指定します。
- ④ 名前
スケジュール名を指定します。補足事項がある場合は説明欄に記載します。

(3) [対象/フォールバック]タブにて、対象のクライアント等の設定を行います。



① 対象

スケジュールを実行する対象グループまたはクライアントにチェックを入れてください。チェックが入っていない対象にはスケジュールは実行されません。

② フォールバック

スケジュール開始後、何らかの理由（停電など）により、予定時間内（スケジュール終了までの時間）にスケジュールが完了しなかった場合、クライアント側に反映される設定となります。

| | チェック有り | チェック無し |
|--------------------|----------|------------|
| プロテクト | プロテクトモード | プロテクト解除モード |
| Firewire ブロックングを有効 | ブロック ON | ブロック OFF |
| USB ブロックングを有効 | ブロック ON | ブロック OFF |
| キーボード・マウスを無効 | ブロック ON | ブロック OFF |

③ スケジュール終了までの時間

スケジュール終了までの時間（分単位）を設定します。本設定は、スケジュールの開始から終了までの目安時間となります。1つの動作につき、5分が既定値として必要になります。今回の設定では、下記のようになります。

[スケジュール 01]

起動(Wake On LAN) : 5分
 プロテクト解除 : 5分
 再起動 : 5分

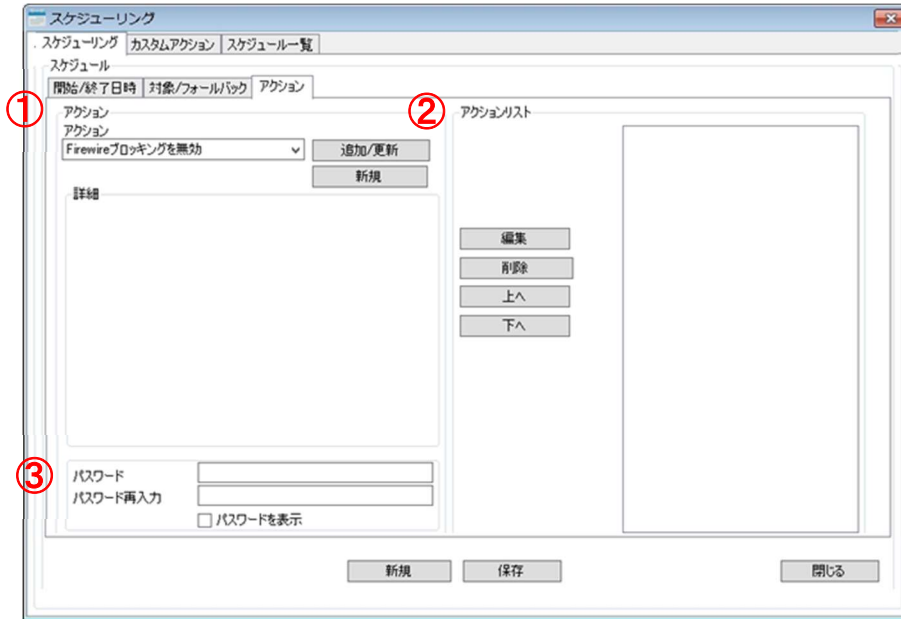
} 5+5+5=15分

[スケジュール 02]

プロテクト : 5分
 シャットダウン : 5分

} 5+5=10分

(4) [アクション]タブにて、スケジューリングを行う動作の設定を行います。



① アクション

実行したい動作を選択後、[追加/更新] をクリックすることで、画面右側のアクションリストにアクションが追加されます。一連の動作を追加してください。

| 項目 | 機能 |
|-------------------------|---|
| Firewire ブロッキングを有効 | Firewire のロック |
| キーボードとマウスを無効 | キーボードとマウスのロック |
| USB ブロックを有効 | USB デバイスのロック |
| 遅延 | 遅延動作 (1分～300分) |
| 遅延再起動 | 遅延再起動 (1分～15分) |
| 遅延シャットダウン | 遅延シャットダウン (1分～15分) |
| プロテクトを解除 | プロテクト解除モード |
| プロテクト | プロテクトモード |
| ファイル転送 | ファイル転送の実行 |
| 再起動 | 再起動の実行 |
| リモート実行 | クライアントのリモート実行 |
| シャットダウン | シャットダウンの実行 |
| Firewire ブロッキングを無効 | Firewire のロック解除 |
| キーボードとマウスを有効 | キーボードとマウスのロック解除 |
| USB ブロッキングを無効 | USB デバイスのロック解除 |
| 起動(Wake On LAN) | Wake On LAN を使用したクライアントのリモート電源 ON |
| Windows Update(推奨アクション) | Windows Update を実行します。実行中はキーボードとマウスのロック、背景画面の変更も同時に行います。 |
| Windows Update(実行のみ) | Windows Update の動作のみを実行します。実行中のキーボードとマウスのロック、背景画面の変更は行いません。 |
| メッセージ送信 | クライアントにメッセージを表示します。 |

※Update Client Software、ウイルススキャン実行は未対応です。ご使用にならない様ご注意ください。

② アクションリスト

アクションで追加した動作が登録されます。動作の編集を行う場合は、該当の動作を選択した後 [編集] をクリックします。動作を削除する場合は、該当の動作を選択した後 [削除] をクリックしてください。スケジュールはアクションリストの一番上から実行されます。実行順を変更する場合は、該当の動作を選択した後、画面中央の [上へ][下へ] ボタンで並び替えを行ってください。

③ パスワード

クライアント側に設定したパスワードを入力してください。パスワードが異なる場合でもスケジュールは実行されますが、パスワードを必要とするアクションでスケジュールが失敗となり、フォルバックで設定した内容が反映されます。パスワード間違いにはご注意ください。

- (5) すべての設定が完了後に、画面下の [保存] をクリックします。
- (6) スケジュールが作成されました。[OK] をクリックしてください。
- (7) [スケジュール一覧] タブを選択することで、作成したスケジュールの内容を確認できます。



① 編集

スケジュールを編集します。該当のスケジュールを選択後、[編集] をクリックします。編集が完了しましたら、[保存] をクリックします。

② スケジュールをコピー

スケジュールをコピーすることができます。コピーしたスケジュールは [編集] にて設定内容を更新してください。

③ CSV エクスポート

スケジュールを CSV 形式にエクスポートします。該当のスケジュールを選択後 [CSV エクスポート] をクリックします。保存ダイアログにて、保存先とファイル名を指定し保存してください。

④ 削除

スケジュールを削除します。該当のスケジュールを選択後 [削除] をクリックします。
 ※実行中のスケジュールは削除できません。

⑤ 今すぐ実行

スケジュールを実行します。スケジュールの動作確認の際に使用します。この機能を使用したスケジュール実行後も、指定した時間に再度スケジュールは実行されます。

⑥ 有効／無効

設定したスケジュールの有効／無効を設定できます。無効にした場合、スケジュールの実施日時になっても実施されません。

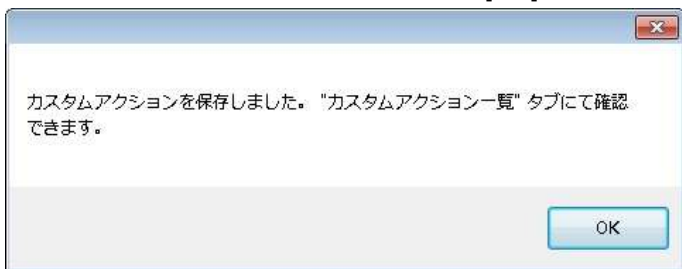
以上で、スケジュールの作成は完了です。

スケジュール 01 を作成後、同様の手順にてスケジュール 02 を作成します。

カスタムアクション

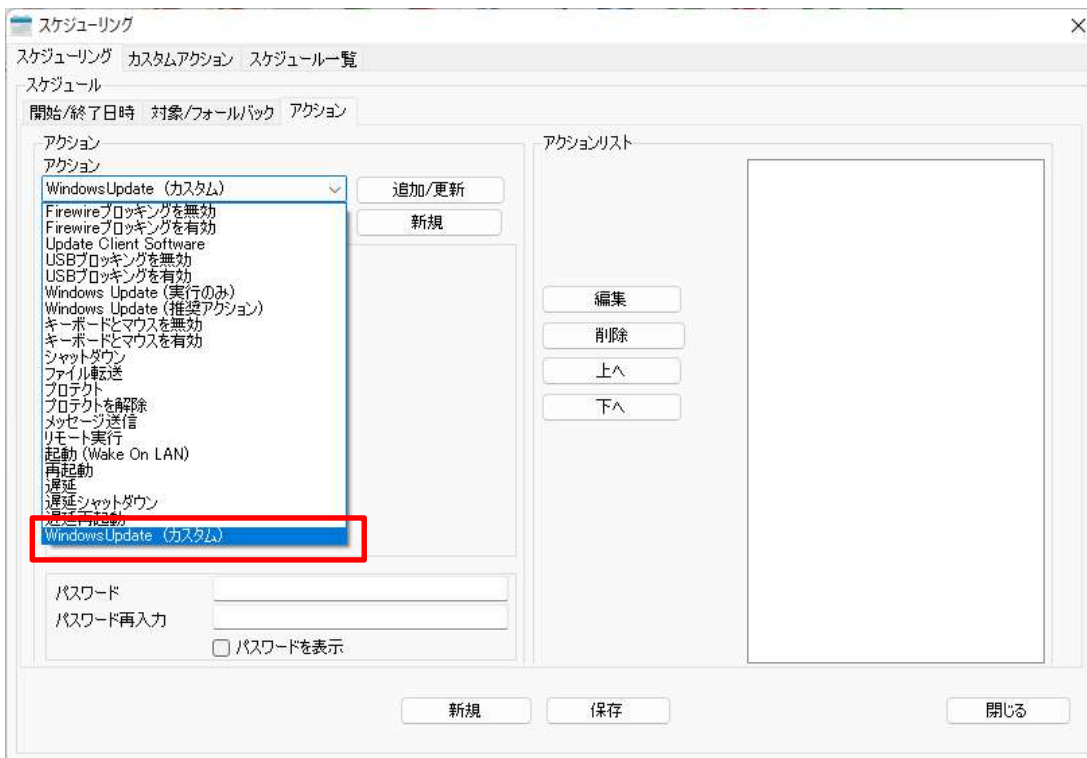
[カスタムアクション] タブにて、一連の動作を予め登録しておくことが可能です。ここで登録したカスタムアクション は [スケジューリング] の [アクション] 一覧に登録され、使用することができます。

- (1) メニューバーの [スケジューリング] → [スケジューリング] をクリックします。
- (2) 次のダイアログにて [カスタムアクション] タブをクリックします。スケジュール作成と同様に、一連の動作をアクションリストに追加します。
- (3) 画面下の[カスタムアクション名] へ動作の名前を入力し、[保存] をクリックします。
- (4) カスタムアクションが作成されました。[OK] をクリックしてください。



作成したカスタムアクションは[カスタムアクション一覧] タブで削除・編集ができます。

- (5) 作成したカスタムアクションはスケジューリングの [アクション] 一覧に追加されます。



Windows Update の推奨スケジュール設定

スケジューリング機能でクライアントの Windows Update を自動実行する場合は、以下のスケジュール設定をご参照ください。

起動 (Wake-On-LAN) → プロテクトを解除 → 再起動 → 遅延 (5 分) → Windows Update (推奨アクション) → 遅延 (5 分) → プロテクト → 再起動 → シャットダウン

※Wake-On-LAN について

スマートコントロールからクライアントへブロードキャスト送信しております。ブロードキャスト送信はルーターを越えた別のネットワークには届かない為、[起動 (Wake-On-LAN)] の機能は、別セグメントのクライアントへは対応していません。ルーターによっては、別セグメントにマジックパケットを再送するリピーター機能が備わっているものもございますので、ネットワーク管理者やルーターの各メーカーにご確認ください。

5.5.23 単独認証ライセンスのドライブシールドを遠隔制御する

所有ライセンスが単独認証ライセンスの場合でも、スマートコントロールを使用してクライアントを遠隔制御することができます。

※一括認証ライセンスとは異なり、クライアントのライセンス認証管理はできません。

- (1) 管理用コンピュータに、ライセンスキーを入力せずに、スマートコントロールをインストールします。
- (2) 遠隔制御を行うクライアントの、ドライブシールドの設定画面を開きます。
- (3) [管理設定] > [スマートコントロール] をクリックします。
- (4) [IP アドレス] 欄に移行先のスマートコントロールがインストールされているコンピュータの IP アドレスを入力します。
- (5) [ポート] 欄にスマートコントロールと通信を行うポートを設定します。デフォルトの値は [25553] です。
- (6) [保存] をクリックします。次画面で再起動が必要と表示されますので [OK] をクリックします
- (7) パスワード入力画面が表示されます。パスワードを入力し [OK] をクリックするとコンピュータが再起動し、設定が適用されます。

6. 仮想化ソフトをご利用の場合

VMWare 等の仮想化ソフトを使用しているクライアントコンピュータが複数ある場合、スマートコントロールのリスト上のクライアントを正しく表示できない場合があります。

これは、複数のクライアントコンピュータに同じ MAC アドレスの仮想ネットワークアダプターが存在していることにより起こります。

その場合、下記設定を行う事でリストを修復できます。

- (1) スマートコントロールのメニューより、[ファイル]-[初期設定] をクリックします。
- (2) [MAC 設定] のタブをクリックします。画面下の入力欄に、仮想アダプタの各 MAC アドレスをすべて登録し、[OK]をクリックします。
- (3) スマートコントロールのコンピュータを再起動し、すべてのクライアントのリストが正常に表示されたかをご確認ください。
VMware をデフォルトの状態で使用している場合は、以下の 2 つの MAC アドレスを登録してください。

00-50-56-C0-00-01

00-50-56-C0-00-08



7. ライセンス認証の解除

インターネットに接続した状態でスマートコントロールのアンインストールを行うことで、ライセンスの認証状態が解除されます。ライセンス認証の解除後は別の端末でスマートコントロールのライセンス認証が可能です。

端末の故障やインターネットへ接続した状態でアンインストールができない場合は、ライセンス認証の解除を行うことができません。

その場合は保守サポート期間内にサポート窓口へご連絡ください。保守サポート期間内であれば、ライセンス認証のリセットを行うことが可能です。

8. アンインストール

スマートコントロールのアンインストール方法

アンインストールを実施する場合は Administrator 権限でサインインしてください。

- (1) Administrator 権限でログオンし、[コントロールパネル] の [プログラムと機能] をクリックします。
- (2) Smart Control TM を選択し、[アンインストール] をクリックします。
- (3) [Remove] をクリックしたあと、[Next] をクリックします。
- (4) [Reboot computer now] にチェックを入れ、[Finish] をクリックします。

9. お問い合わせ先

製品のお問い合わせ先につきましては、製品パッケージ内に同封されている「保守サービス証書」をご確認いただくか、ご購入先の販売店へお問い合わせ願います。

また、お問い合わせの前に本製品に関する下記の FAQ ページをご確認願います。

株式会社アルバニクス

https://www.arvanics.com/solution/app_bunkyo/faq/

株式会社アイ・ディ・ケイ

https://www.idk.co.jp/solution/series_bunkyo/faq/

スマートコントロール
<インストール / 操作ガイド>

Ver.2.5

発行日 2023年11月29日



株式会社アルバニクス

本 社 〒242-0021 神奈川県大和市中央 7-9-1
TEL: (046) 259-6920
FAX: (046) 259-6930
E-mail: info@arvanics.com
URL: <https://www.arvanics.com/>