PSA6000 シリーズ

Windows システム設定

ユーザーガイド

PSA6000-WINSYS-UG-JA.01
02/2026

Pro-face™
by Schneider Electric

法律情報

本書に記載されている情報は、製品/ソリューションに関する一般的な説明、技術的特性、および推奨事項を含んでいます。

本書は、詳細な調査や運用/現場別の開発計画や概略図の代用となるものではありません。また、特定ユーザーの用途に対する製品/ソリューションの適合性または信頼性を判断するために使用すべきものではありません。関連する特定の用途または使用に関して製品/ソリューションの適切かつ包括的なリスク分析、評価、および試験を行うこと、または選択した専門家 (インテグレーター、設計者等) に実施させることは、当該ユーザーの義務とします。

本書で言及されているPro-faceブランドならびにシュナイダーエレクトリックSEおよびその子会社の商標は、シュナイダーエレクトリックSEまたはその子会社の所有物です。その他すべてのブランドは、各所有者の商標である場合があります。

シュナイダーエレクトリックは、「現状のまま」文書を調べる非独占な個人ライセンスを除き、本ガイドまたはその記載内容を商業的に使用する権利またはライセンスを付与することはありません。

シュナイダーエレクトリックは、本書の内容またはその形式に関して、いつでも予告なく変更または更新する権利を有します。

適用法により認められる範囲で、シュナイダーエレクトリックおよびその子会社は、本書の情報コンテンツの誤りや記入漏れまたは本書に含まれる情報の使用に起因する結果、もしくはその結果から生じる結果に関し、一切責任を負いません。

目次

安全に関する使用上の注意

重要情報

本書をよくお読みいただき、装置の正しい取り扱いと機能を十分ご理解いただいた上で、設置、操作、保守を行ってください。本書および装置には以下の表示が使われています。これらは潜在的な危険を警告したり、手順を明確化あるいは簡素化する情報について注意を呼びかけるものです。

この記号が「危険」または「警告」安全ラベルに追加されると、電気的な危険が存在し、指示に従わないと人身傷害の危険があることを示します。

安全警告記号です。人的傷害の危険性があることを警告します。
この記号の後に記載された安全に関する情報に従って、人的傷害や死亡の危険性を回避してください。

⚠ 危険

危険は、危険が生じる可能性のある状況を示します。回避しないと、死亡や重傷を**招きます**。

⚠ 警告

警告は、危険が生じる可能性のある状況を示します。回避しないと、死亡や重傷を**招くおそれ**があります。

⚠ 注意

注意は、危険が生じる可能性のある状況を示します。回避しないと、軽傷を**招くおそれ**があります。

注記

この表示は、指示に従わないと物的損害を負う可能性があることを示します。

以下の点に注意してください。

電気装置の設置、操作、サービス、および保守は有資格者のみが行うことができます。定められた範囲外の使用によって生じた結果については、シュナイダーエレクトリックは一切の責任を負いかねます。

有資格者とは、電気装置の構造および操作ならびに設置に関する技術と知識を持ち、関連する危険性を認識して回避するための安全トレーニングを受けた人を指します。

本書について

本書の適用範囲

本書では、産業または FA システムで使用される PSA6000 シリーズのシステムの設定方法について説明しています。

本書は、システムの設計、またはコンポーネントの設置やメンテナンスを行うユーザーを対象としています。

有効性に関する注意

本書は、PSA6000 シリーズを対象として書かれています。

本書に記載されている製品の特性は、www.pro-face.com に掲載されている特性と一致することを意図しています。継続的改善を目指す当社の企業戦略の一環として、情報をより明確かつ正確なものにするため内容を改訂させていただく場合があります。この文書に記載されている特性と、www.pro-face.com に記載されている特性が異なる場合は、www.pro-face.com に最新の情報が記載されているとお考えください。

製品関連情報

PSA6000 シリーズハードウェアガイドを参照してください。

一般的なサイバーセキュリティー情報

近年、ネットワークに接続されているパソコンや生産プラントの数が増加するにつれ、不正アクセス、データ漏洩、操業中断などのサイバー脅威の可能性が高まっています。したがって、このような脅威から資産やシステムを保護するために、あらゆるサイバーセキュリティー対策を考慮する必要があります。

Pro-face 製品を安全に保護するために、Cybersecurity Best Practices のドキュメントに記載されているサイバーセキュリティーのベストプラクティスを実施することが最善策になります。

Pro-face は、追加情報およびサポートを提供しています。

- Security Notification ページからセキュリティー通知をご確認ください。
- 脆弱性およびインシデントについては、こちらからご連絡ください。

製品関連のサイバーセキュリティー情報

サイバーセキュリティー, 7 ページを参照してください。

本ドキュメントの翻訳言語

本書は以下の言語でご覧いただけます：

- 英語 (PSA6000-WINSYS-UG-EN)
- 日本語 (PSA6000-WINSYS-UG-JA)

関連マニュアル

文書のタイトル	参照番号
Cybersecurity Best Practice	一般的なサイバーセキュリティー情報, 5 ページ を参照してください。
HMI/IPC サイバーセキュリティーガイド	PFHMIIPCCS-MM01-EN (英語) PFHMIIPCCS-MM01-JA (日本語)
PSA6000 シリーズハードウェアガイド	PSA6000-MM01-EN (英語) PSA6000-MM01-FR (フランス語) PSA6000-MM01-DE (ドイツ語) PSA6000-MM01-ES (スペイン語) PSA6000-MM01-IT (イタリア語) PSA6000-MM01-CS (中国語) PSA6000-MM01-JA (日本語) PSA6000-MM01-KO (韓国語)

ソフトウェアマニュアルなど本製品に関連するマニュアルは、Pro-face ダウンロードページ (www.pro-face.com/trans/ja/manual/1085.html) からダウンロードできます。

非包括的または差別的な用語に関する情報

弊社は、責任ある、ソーシャルインクルージョン(社会的包摂)を掲げた企業として、非包括的または差別的な用語を含む文書および製品を順次更新しております。このように努めてはおりますが、弊社が提供するコンテンツに、お客様が不適切と感じる可能性のある用語が含まれている場合がございますことをご了承ください。

商標

Microsoft® と Windows® は米国およびその他の国の Microsoft Corporation における登録商標です。

Intel®、Core™、Atom® は Intel Corporation の登録商標です。

QR コードは株式会社デンソーウェーブの登録商標です。

本書に記載の製品名は、それぞれの権利者の登録商標である場合があります。

サイバーセキュリティー

サイバーセキュリティーガイドライン

本製品は、セキュアな産業制御システムの下で使用してください。サイバー攻撃の脅威からコンポーネント(装置/デバイス)、システム、組織、およびネットワークを総体的に保護するためには、多層的なサイバーリスク低減措置、インシデントの早期発見、インシデント発生時の適切な対処と復旧計画が必要です。サイバーセキュリティーの詳細については、Pro-face HMI/IPC サイバーセキュリティーガイドを参照してください。
https://www.proface.com/ja/download/manual/cybersecurity_guide

⚠警告

システムの可用性、完全性、機密性に対する潜在的な侵害

- デバイスの設定、制御、および情報への不正アクセスを防ぐために、初回使用時に既定のパスワードを変更してください。
- 悪意のある攻撃の経路を最小限に抑えるために、可能な限り、使用していないポート / サービスおよびデフォルトアカウントを無効にしてください。
- ネットワークに接続されたデバイスは、多層のサイバー防御 (ファイアウォール、ネットワークセグメンテーション、およびネットワーク侵入検出と保護など) の背後に配置してください。
- 最新のアップデートと修正プログラムをオペレーティングシステムとソフトウェアに適用してください。
- サイバーセキュリティーのベストプラクティス (例：最低限の権限、職務の分離) を使用して、データやログの不正な漏洩、損失、および改ざん、サービスの中断、または意図しない操作を防止してください。

上記の指示に従わないと、死亡、重傷、または機器の損傷を負う可能性があります。

システム設定

この章の内容

主な機能

マルチランゲージ対応

以下の言語のオペレーティングシステムを搭載しています。

英語 (初期設定)、日本語、フランス語、ドイツ語、スペイン語、イタリア語、ポルトガル語、ロシア語、スウェーデン語、簡体字中国語、繁体字中国語

UEFI BIOS

本製品は UEFI BIOS を搭載しています。UEFI BIOS, 16 ページ を参照してください。

ランチャー

あらかじめ登録しておいたファイルやプログラム、各種設定をアイコンで一覧表示し、タッチ操作によって簡単に起動できるようにするユーティリティーです。ランチャーには、本製品に必要な設定 (Write Filter など) のアイコンがあらかじめ含まれています。ランチャー, 17 ページを参照してください。

セキュリティー対応

本製品は Secure Boot を有効にしています。また TPM を搭載しており、BitLocker などの暗号化ツールに容易に対応することができます。さらに、オプションの Trellix ライセンスをご購入いただくことで、お客様にてより安全な環境を実現することができます。TPM, 25 ページ および Trellix ソフトウェア, 26 ページ を参照してください。

注記： より安全なシステム構築のため、BitLocker を有効にしてください。

初回起動時

本製品の初回起動時に、オペレーティングシステムの初期設定が行われます。電源を入れる前にキーボード、マウスを接続し、画面の指示に従って設定を行ってください。

注記：

本製品では、不正なアクセスや悪意のあるソフトウェアの侵入・感染に対するリスクを抑えるため、サインインパスワードの設定を必須としています。サインインパスワードの条件は以下です。

文字数：以下の使用可能な文字から 3 種類以上 8 文字以上の文字。アカウント名に使用している文字列は使用できません。

使用可能文字種類：

- ヨーロッパ言語の大文字 (A ~ Z、発音区別符号、ギリシャ文字、キリル文字)
- ヨーロッパ言語の小文字 (a ~ z、シャープ記号、ギリシャ文字、キリル文字)
- 数字 (0 ~ 9)
- 英数字以外の文字 (特殊文字)：(~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/) このポリシー設定では、ユーロや英国ポンドなどの通貨記号は特殊文字としてカウントされません。
- アルファベット順に分類されているが、大文字でも小文字でもない Unicode 文字。これには、アジア言語の Unicode 文字が含まれます。
- 失われたユーザー名とパスワードを復元することはできません。

⚠注意

機器の損傷

Write Filter の設定にかかわらず、電源投入直後は本製品の電源を切らないでください。

上記の指示に従わないと、負傷または機器の損傷を負う可能性があります。

注記

データの損失

初期設定実行中は電源を切らないでください。

上記の指示に従わないと、機器の損傷を負う可能性があります。

注記

アクセス不能

デバイスのユーザー名とパスワード情報は安全な場所に保存してください。

上記の指示に従わないと、機器の損傷を負う可能性があります。

Windows Update

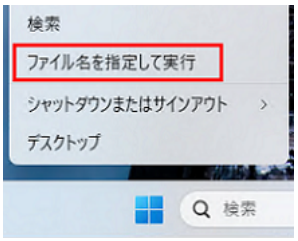
本製品をより安全にご使用いただくため、Windows Update にてオペレーティングシステムを常に最新の状態に保ってください。工場出荷状態では自動セキュリティーアップデート機能を無効にしています。有効にする場合は、以下を参照してください。

注記：

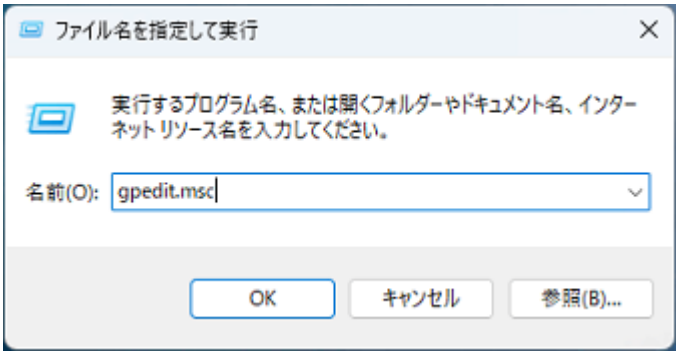
- Write Filter を有効にしている場合は、無効にしてからオペレーティングシステムのアップデートを行ってください。
- セキュリティーアップデートを定期的に適用できない使用環境の場合は、オプションの Trellix ライセンスをご購入いただき、アクセス権限リスト方式のセキュリティー対策の実施をお勧めします。

自動更新を有効にする方法

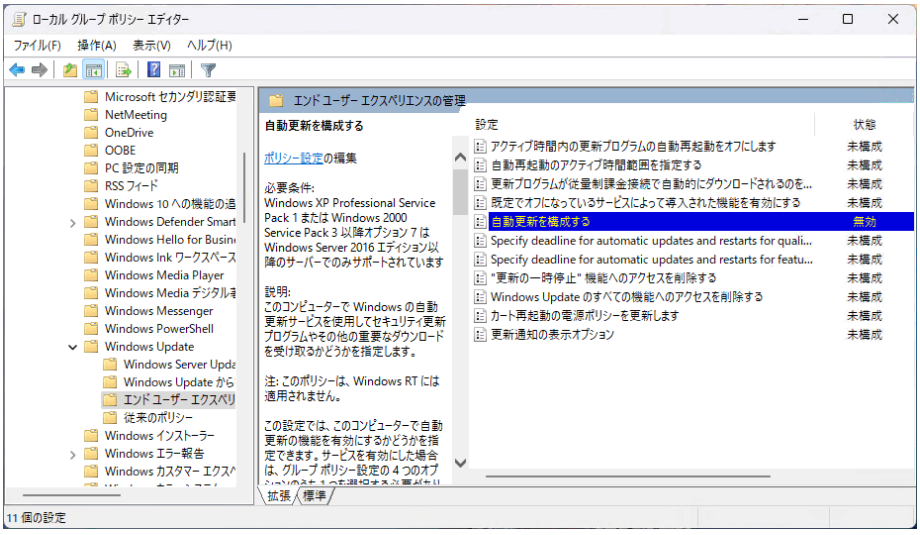
1. **スタート**ボタンを右クリックし、**ファイル名を指定して実行**を選択します。



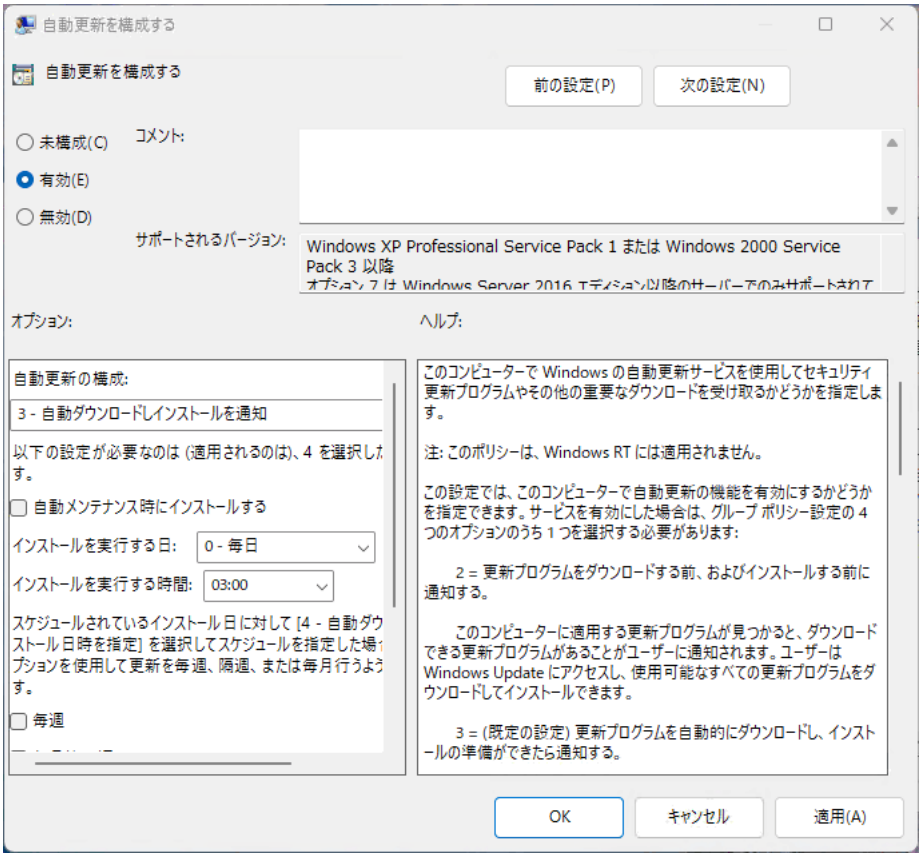
2. `gpedit.msc` を入力し、**OK** を選択します。



3. **コンピューターの更新** > **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** を開きます。

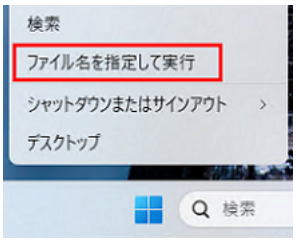


4. 設定を**無効**から**有効**に変更し、ご使用の環境に応じて**オプション**を選択してから、**OK** を選択します。

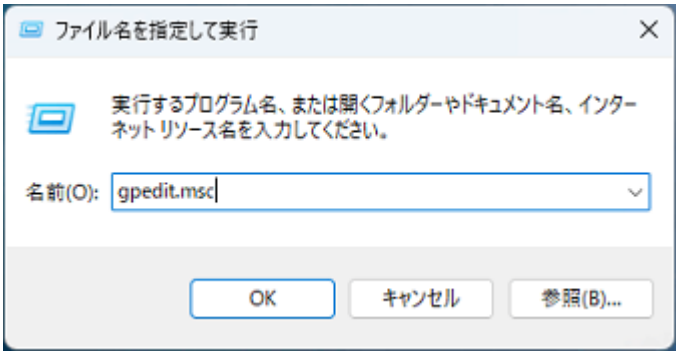


セキュリティーインテリジェンスの更新を有効にする方法

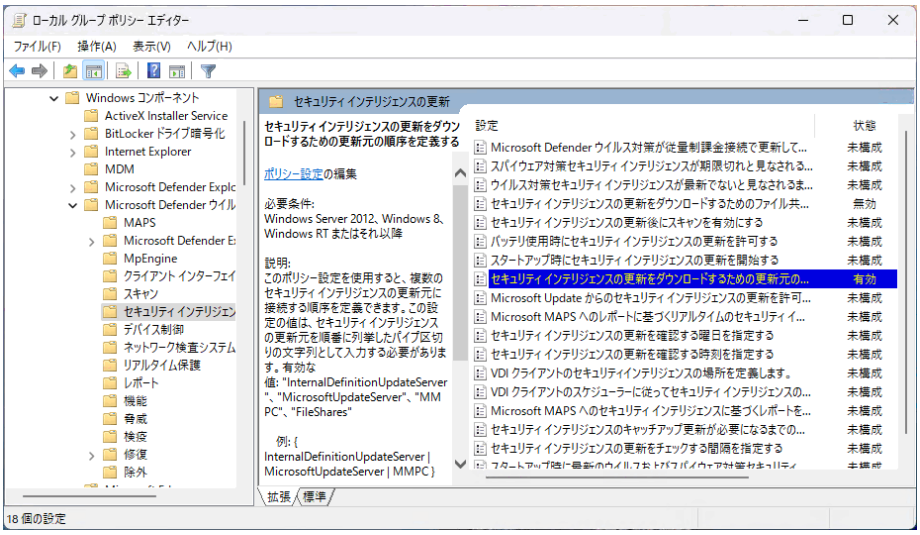
1. **スタート**ボタンを右クリックし、**ファイル名を指定して実行**を選択します。



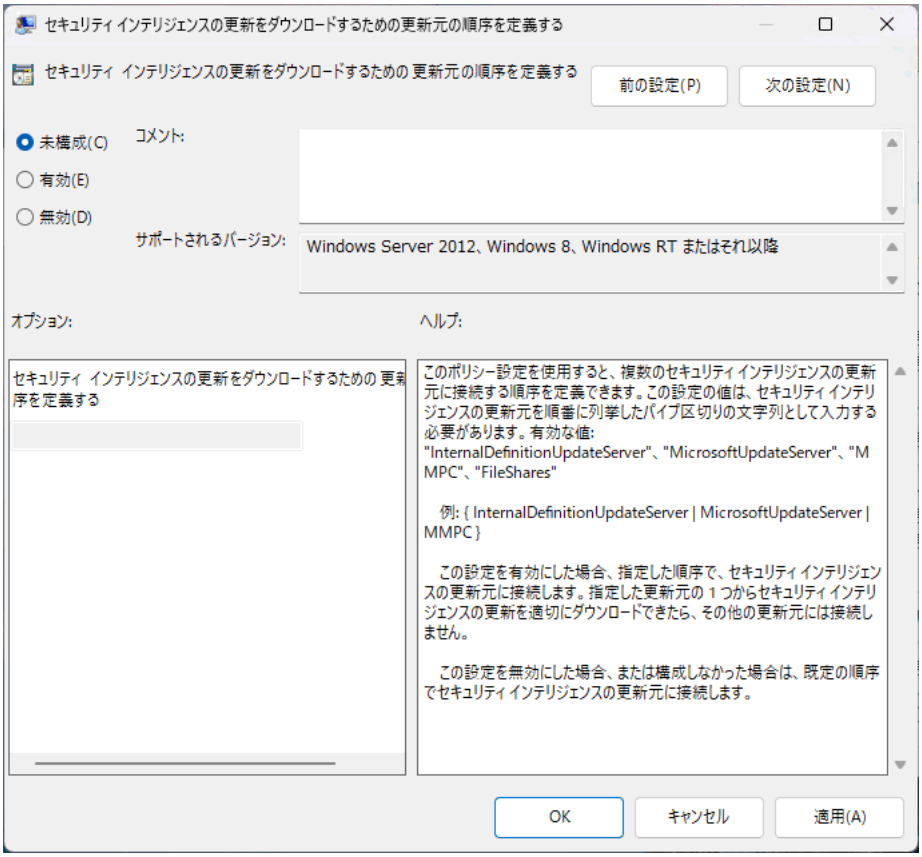
2. `gpedit.msc` を入力し、**OK** を選択します。



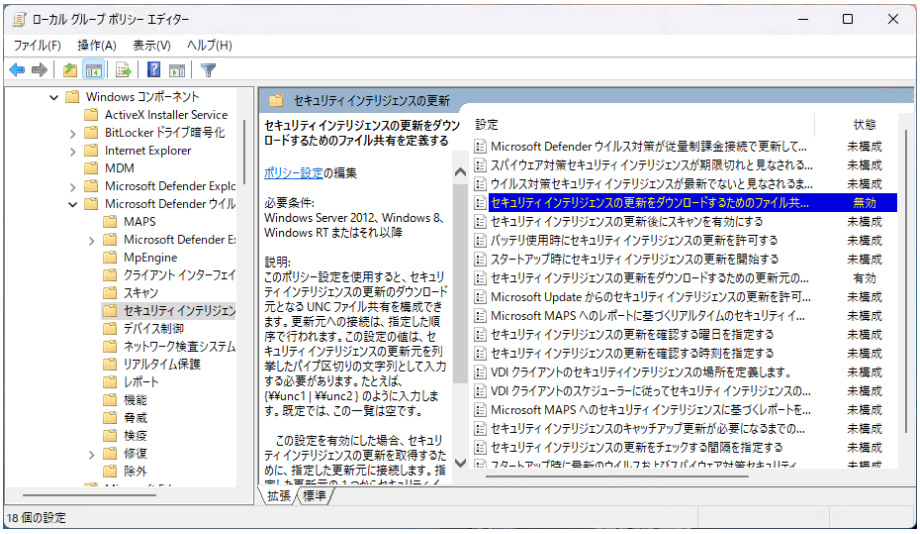
3. **コンピューターの更新 > 管理者用テンプレート > Windows コンポーネント > Microsoft Defender ウイルス対策 > セキュリティインテリジェンスの更新 > セキュリティインテリジェンスの更新をダウンロードするための更新元の順序を定義する**を開きます。



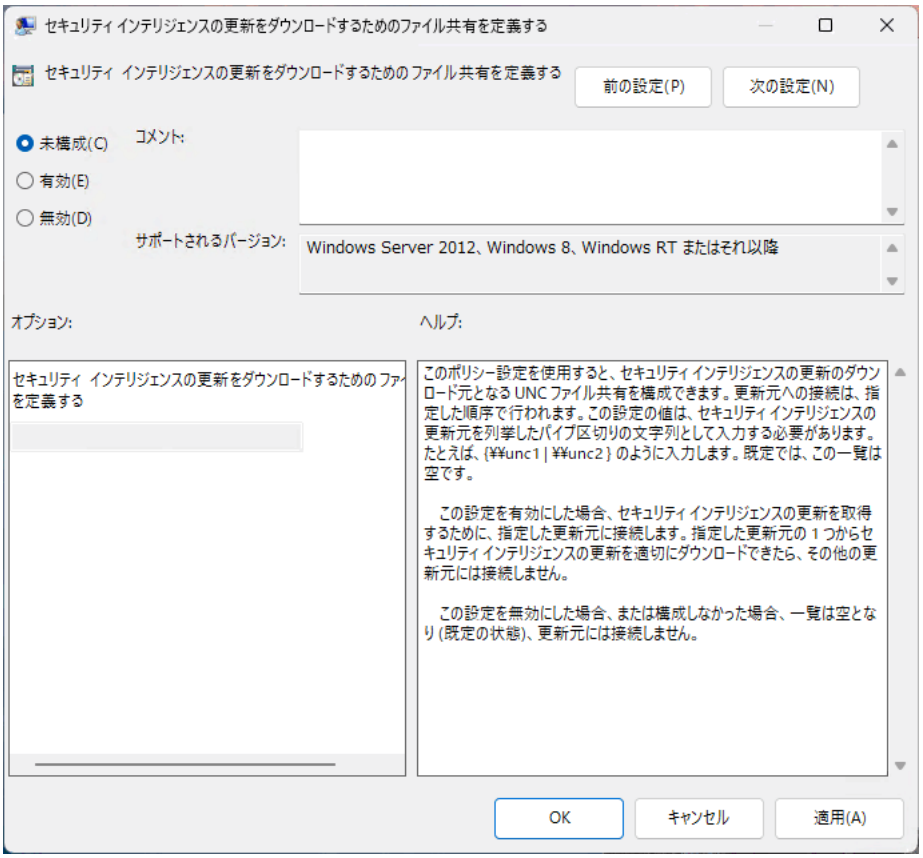
4. 設定を**無効**から**未構成**に変更し、**OK** を選択します。



5. **コンピューターの更新 > 管理者用テンプレート > Windows コンポーネント > Microsoft Defender ウイルス対策 > セキュリティインテリジェンスの更新 > セキュリティインテリジェンスの更新をダウンロードするためのファイル共有を定義する**を開きます。



6. 設定を**無効**から**未構成**に変更し、**OK** を選択します。



ユーザーアカウント

標準ユーザーアカウントの作成方法

アカウントの種類が管理者であるユーザーアカウントは、システム設定の変更が必要な場合にのみ使用してください。

それ以外の通常操作は、標準ユーザーアカウントを使用してください。

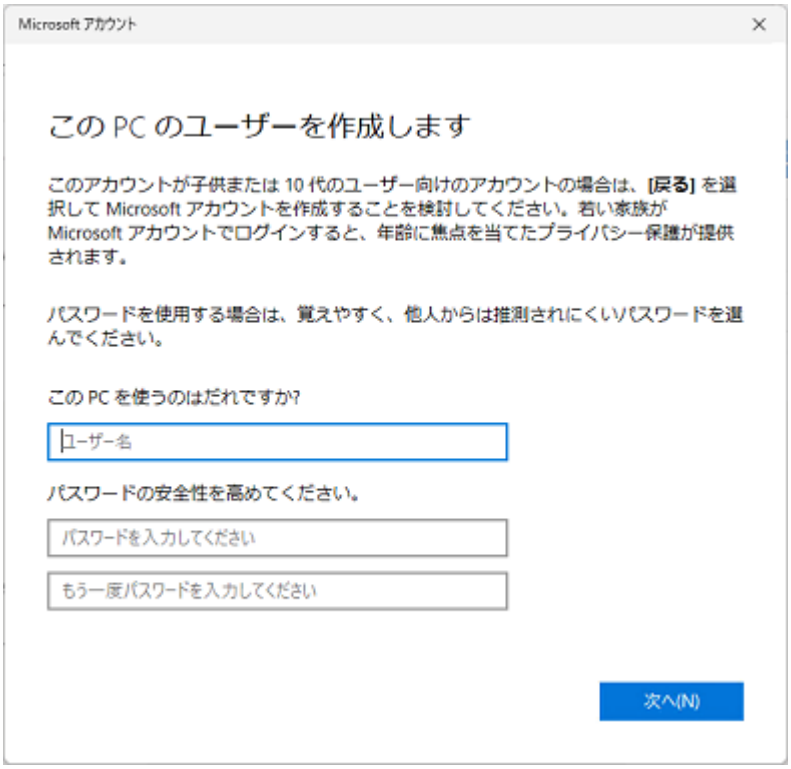
以下に標準ユーザーアカウントの作成方法を示します。

1. **設定**を開きます。

2. **アカウント**を選択します。
3. **その他のユーザー**を選択します。

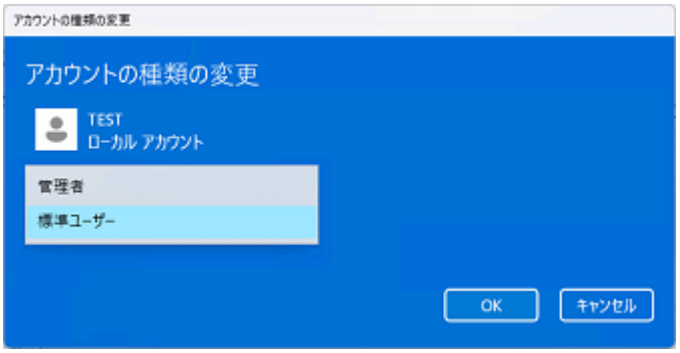
4. **アカウントの追加**を選択します。

5. ユーザー名とパスワードを入力し、**次へ**を選択します。



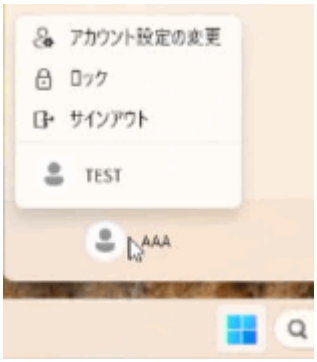
6. 作成したユーザーアカウントを選択し、**アカウントの種類の変更**を選択します。

7. **標準ユーザー**を選択します。



8. **スタート**を選択し、アカウントアイコンを選択します。

9. 作成したユーザーアカウントを選択します。



UEFI BIOS

UEFI BIOS 設定メニュー

UEFI BIOS 設定メニューに入るには、以下を実行します。

1. 本製品の電源を入れます。
2. ブート画面表示中に [DEL] キーを押します。
3. パスワードを入力します (初期パスワード：Pw#12345)*1。
4. BIOS 画面が表示されます。

*1 初期パスワードは必ず変更してください。UEFI BIOS パスワード変更, 16 ページを参照してください。

Fast Boot などの設定により上記手順で BIOS 設定メニューに入れない場合があります。その場合は以下の手順で設定メニューを表示させてください。

1. 本製品の電源を入れ、通常起動させます。
2. **設定**を開きます。

3. **回復**を選択します。
4. **PC の起動をカスタマイズする**で**今すぐ再起動**を選択します。
5. **トラブルシューティング**を選択します。
6. **詳細オプション**を選択します。
7. **UEFI ファームウェアの設定**を選択します。
8. **再起動**を選択します。
9. パスワードを入力します (初期パスワード：Pw#12345)*1。

*1 初期パスワードは必ず変更してください。UEFI BIOS パスワード変更, 16 ページを参照してください。

UEFI BIOS パスワード変更

セキュリティー観点上、初期 BIOS パスワード (Pw#12345) は必ず変更してください。以下にパスワード変更の手順を示します。

注記：

- パスワードには 8 文字以上が必要です。
- バッテリーを交換などの理由で取り外した場合でも、UEFI BIOS のパスワードはリセットされません。

注記
アクセス不能
UEFI BIOS パスワード情報は安全な場所に保存してください。
上記の指示に従わないと、機器の損傷を負う可能性があります。

1. BIOS 画面を表示します。UEFI BIOS 設定メニュー, 16 ページを参照してください。
2. **Security** を選択します。
3. **Administrator Password** を選択します。
4. **Enter Current password** ダイアログが表示されます。現在のパスワードを入力します。
5. **Create New Password** ダイアログが表示されます。新しいパスワードを入力します。
6. **Confirm New Password** ダイアログが表示されます。手順 5 で入力したパスワードを入力します。
7. [F4] キーを押します。
8. **Save & Exit Setup** ダイアログボックスの **Yes** を選択します。
9. 本製品が再起動します。

In-Band ECC (Atom モデルのみ)

本製品の CPU は In-Band ECC に対応しています。以下に In-Band ECC を有効または無効にする手順を示します (初期設定：**Disabled**)。

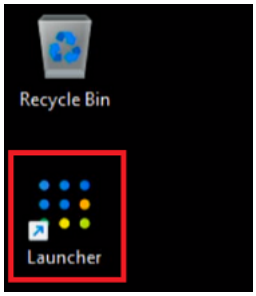
1. BIOS 画面を表示します。UEFI BIOS 設定メニュー, 16 ページを参照してください。
2. **Advanced** > **CPU Configuration** > **In-Band ECC Support** を選択します。
3. **Enabled** または **Disabled** を選択します。
4. [F4] キーを押します。
5. **Save & Exit Setup** ダイアログボックスの **Yes** を選択します。
6. 本製品が再起動します。

ランチャー

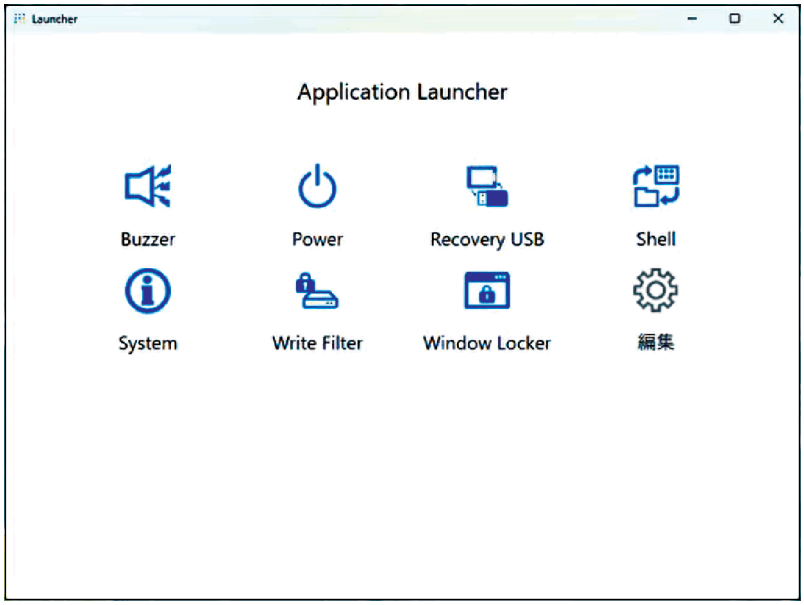
ランチャー起動

ランチャーとは、プログラムや各種設定ができるユーティリティーです。ランチャーにより登録された様々な設定をアイコン表示することで、タッチ操作の利便性が向上します。

ランチャーはデスクトップのショートカットアイコンから起動できます。



ランチャーのトップ画面



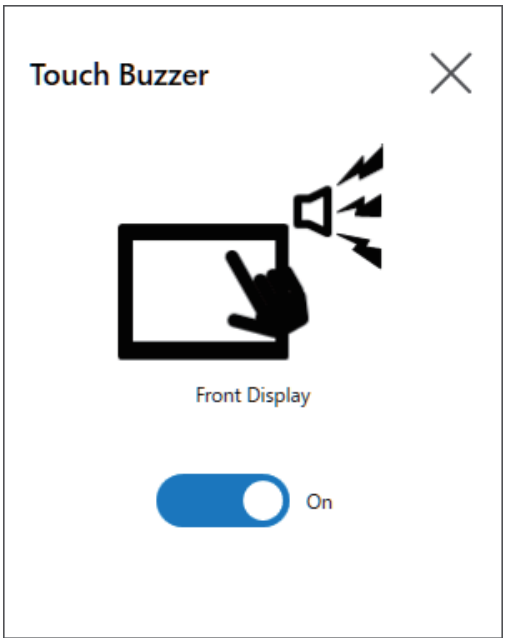
注記：

- ランチャーをカスタマイズするには、編集, 24 ページ を参照してください。
- 以下の URL より最新版の PSA6000 シリーズ用ユーティリティーをダウンロードし、ランチャーを最新の状態に保ってください。
  https://www.pro-face.com/trans/ja/manual/1085.html
- すでにランチャーがインストールされている場合、既存のランチャーは上書きされます。**編集**を使用してランチャーをカスタマイズしていた場合は、再度設定してください。

Buzzer

タッチパネル操作時のブザー音の有効/無効を設定します。

初期値：**On**



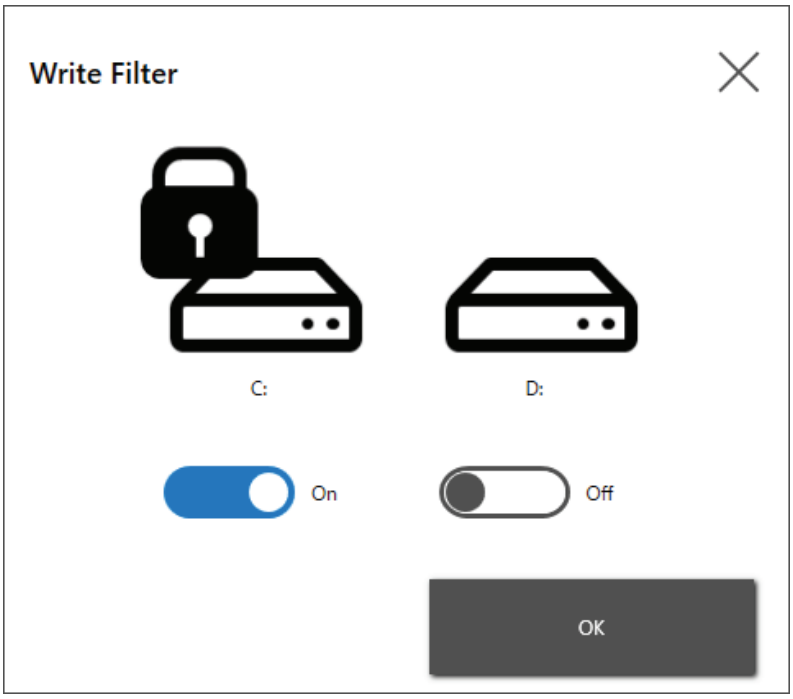
注記： ブザー音は、ランチャーの **Buzzer** 設定よりも UEFI BIOS 設定が優先されます。**Advanced** > **Onboard Device** > **Beep On** の設定が **Enabled** であることを確認してください。(初期設定：**Enabled**)。Enabled になっていない場合、ランチャーの **Buzzer** が **ON** であってもブザー音は鳴りません。

Write Filter

Write Filter は、システムディスクを書き込みアクセスから保護するための機能です。

Write Filter を有効にすることで、システムディスクへの損傷を防ぎ、過剰な書き込みによるディスクの老朽化を防ぐことができます。

初期値：**Off**(無効)



注記：

- Write Filter 対象ボリュームが 1 つの場合は、画面には 1 ボリュームのみ表示されます。
- 設定の変更時 (ランチャー設定の変更、ドライバーの追加、レジストリーの変更、アプリケーションのインストール) は、Write Filter を無効にしてください。Write Filter が有効であると、変更した設定がオペレーティングシステム再起動時にすべて破棄されます。設定の変更後、Write Filter を有効に戻すことをお勧めします。
- Write Filter を有効にすると、高速スタートアップ機能は無効になります。

⚠注意

機器の損傷

Write Filter の設定にかかわらず、電源投入直後は本製品の電源を切らないでください。

上記の指示に従わないと、負傷または機器の損傷を負う可能性があります。

注記

データの損失

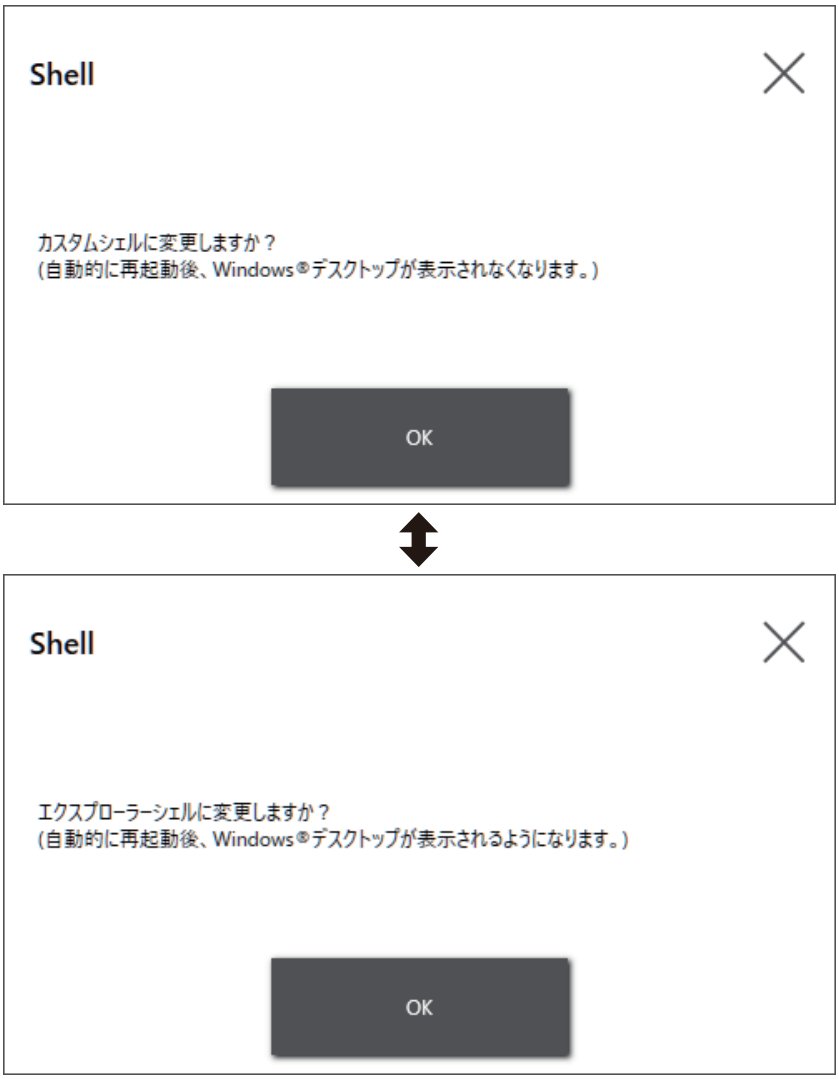
Write Filter で保護されていないストレージデバイスへの書き込み中は、電源を切らないでください。

上記の指示に従わないと、機器の損傷を負う可能性があります。

Shell

エクスプローラーシェルをカスタムシェルに切り替えると、Windows® デスクトップを非表示にできます。

カスタムシェル：Windows® デスクトップは表示されません。製品の起動後、ランチャーのランディングページが表示されます。
エクスプローラーシェル：Windows® デスクトップが表示されます。



注記：

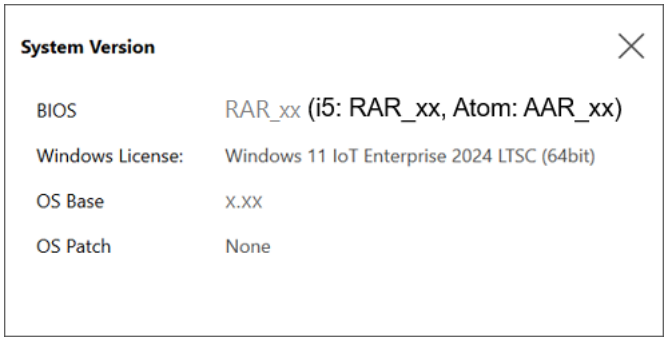
- アプリケーションのインストールは、エクスプローラーシェルで行ってください。
- カスタムシェルに切り替えた場合、エクスプローラーシェルで表示される機能 (Windows® デスクトップ、スタートメニュー、タスクバー等) は使用できません。

Power

この機能を使用して本製品の電源を操作します。

System

本製品のファームウェア、BIOS、オペレーティングシステムのバージョンが表示されます。

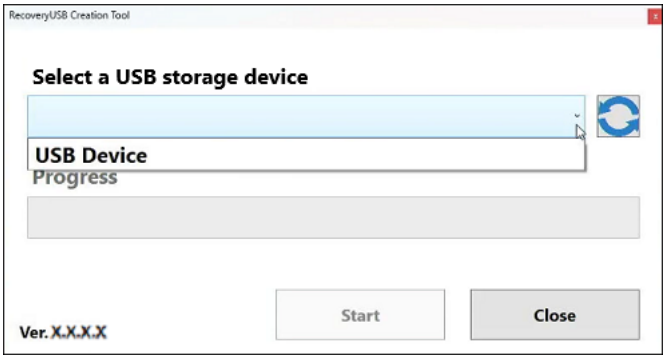


リカバリー USB

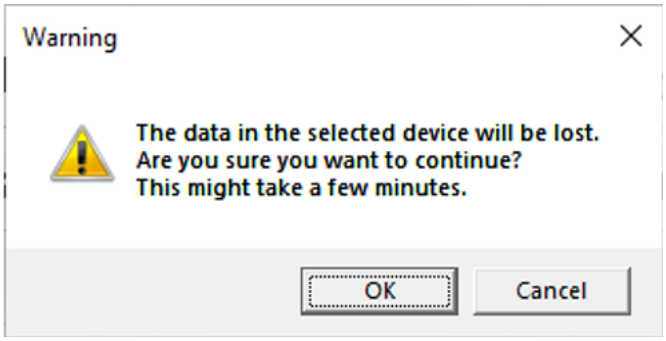
この機能は、システムを復元およびバックアップするためのリカバリー USB を作成するためのものです。リカバリー USB の作成時に、工場出荷時のオペレーティングシステムイメージが自動的に USB に保存されます。このイメージを使用すると、工場出荷時のイメージを復元できます。詳細については、システムリカバリー, 30 ページ を参照してください。現在のシステムをバックアップする必要がある場合、システムバックアップ, 28 ページ を参照してください。

32 GB 以上の市販の USB メモリーを準備しバックアップ USB を作成します。

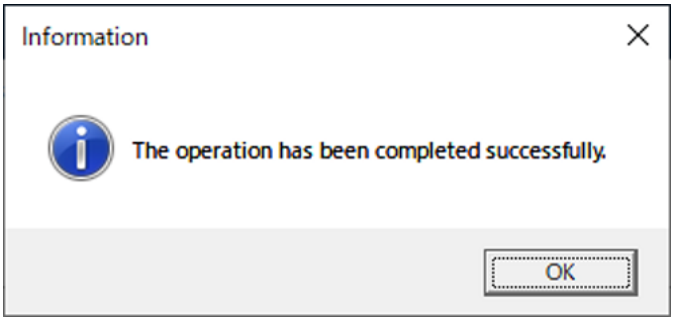
1. 接続されているすべての機器を製品から取り外します。
2. 市販の USB メモリーを挿入します。
3. ランチャーを開きます。
4. **Recovery USB** アイコンを選択します。
5. **Select a USB storage device** で USB メモリーを選択します。



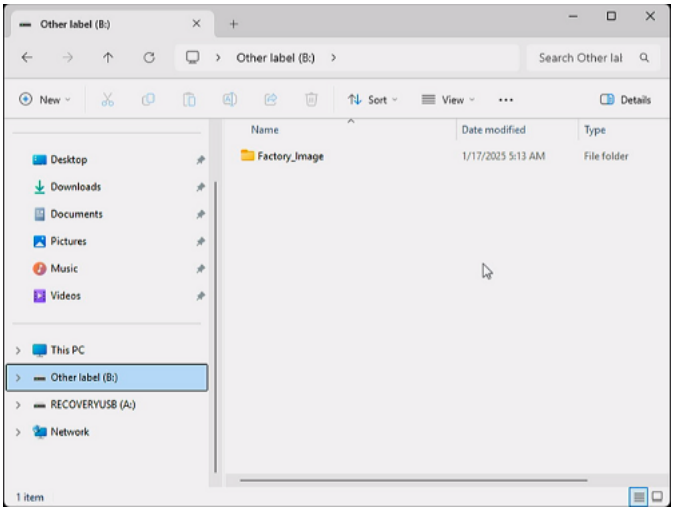
6. **Start** を選択します。
7. 確認画面で **OK** を選択します。



8. 完了すると次のメッセージが表示され、**OK** を選択します。



9. **Recovery USB** 画面を閉じます。
10. 操作後、USB に「Other label」というラベルが付けられたドライブが作成されます。工場出荷時のオペレーティングシステムイメージは、ドライブの「Factory image」という名前のフォルダーに保存されています。



Window Locker

外部ディスプレイへの接続が切断された場合に、表示されているアプリケーションのウィンドウが別の位置または別のディスプレイに移動することがあります。Window Locker を使用すると、アプリケーション起動時のウィンドウ表示位置を固定できるため、外部ディスプレイを再接続した後でも切断前と同じディスプレイに同じ位置でアプリケーションウィンドウを表示できます。

A. LOCK
B. PLAY
C. STOP

1. 表示するディスプレイや位置を固定したいアプリケーションウィンドウをすべて起動します。

   注記： アプリケーションウィンドウをフルスクリーンモードで表示し位置を保存すると、ウィンドウが正常に表示されない場合があります。

2. 各ウィンドウを表示させたい位置に移動します。
3. ランチャーから Window Locker を起動します。
4. **LOCK** を選択すると表示位置が保存されます。

   注記：

   - ウィンドウサイズは **LOCK** 押下時のサイズで固定されます。
   - **更新**に時間を入力すると、**PLAY** を押した後にウィンドウサイズ・位置を変更した場合、入力した時間が経過した後、元のサイズ・位置に戻ります。**ウィンドウの移動を許可する**チェックボックスにチェックを入れると、**PLAY** を押した後に時間が経過してもウィンドウの位置は戻りませんが、サイズは元のサイズに戻ります。
   - **更新**の入力可能範囲は、100 ms から 86,400,000 ms (24 時間) です。

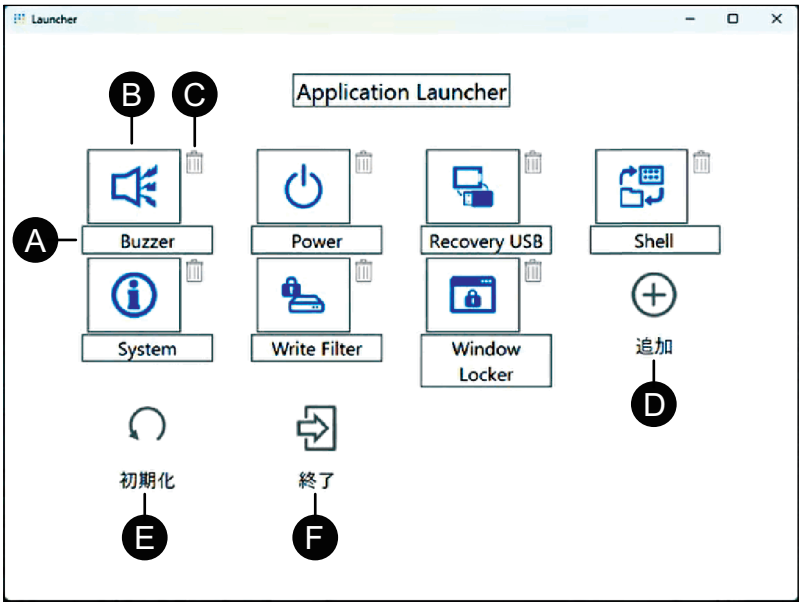
5. **PLAY** を選択します。アプリケーションウィンドウを開くたびに、保存された位置に自動的に表示されます。

注記：

- ウィンドウの位置を保存するときは、Write Filter が無効になっていることを確認してください。Write Filter が有効であると、保存した情報はオペレーティングシステム再起動時にすべて破棄されます。保存後、Write Filter を有効に戻すことをお勧めします。
- 固定位置を一時的に解除するには、**STOP** を選択してください。固定位置に戻すには、**PLAY** を選択してください。
- ウィンドウの表示位置を保存した後に、外部ディスプレイを接続または切断すると表示位置が失われます。接続を追加または切断した場合は、再度表示位置を保存してください。ただし、外部ディスプレイを接続または切断する前と同じ設定に戻した場合は、保存されている表示位置情報が適用されるため、再度表示情報を設定する必要はありません。
- 同じ名前のウィンドウや Windows® Media Player などの内部に複数のウィンドウを持つアプリケーションの表示位置は正常に保存できない場合があります。
- Window Locker でウィンドウの表示位置を保存した後に画面の配置や解像度を変更すると、ウィンドウが正しく表示されない場合があります。画面の設定を変更した場合は、再度ウィンドウの表示位置を保存してください。

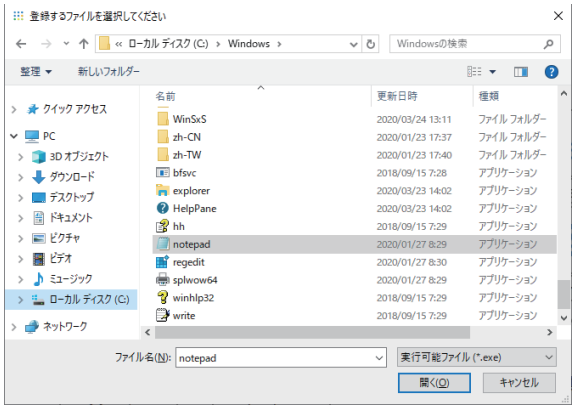
編集

この機能を使用して、ランチャーに表示するアイコンをカスタマイズすることができます。任意のアプリケーションを追加することもできます。



A. アイコンの名前を変更できます。

B. 表示するアプリケーションを変更できます。クリックすると、アプリケーションの exe ファイルを選択できる画面が表示されます。表示したいアプリケーションの exe ファイルを選択します。



C. このマークをクリックするとアイコンが削除されます。

D. 表示させるアプリケーションを追加します。クリックすると、アプリケーションの exe ファイルを選択できる画面が表示されます。表示したいアプリケーションの exe ファイルを選択します。

E. アイコンの表示を工場出荷時の設定に戻します。

F. このボタンで編集モードを終了します。

TPM

本製品には、TPM 2.0 モジュールが搭載されています。

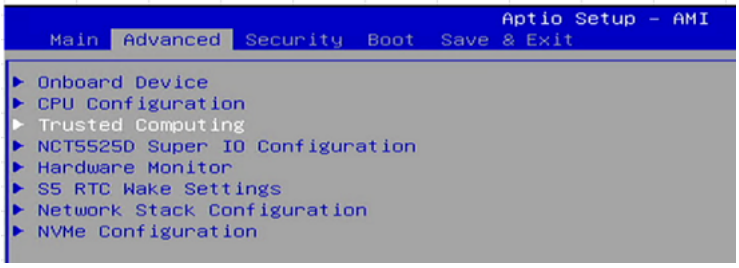
各国の法律、規制、基準に従って TPM を有効または無効にしてください。

初期設定では、TPM が有効になっています。

注記： より安全なシステム構築のため、BitLocker を有効にしてください。

1. 本製品の電源を入れます。
2. ブート画面表示中に TPM を無効にするには、[CTRL]+[D] を押します。TPM を有効にするには、[CTRL]+[E] を押します。

3. 本製品が再起動します。
4. 設定が更新されると、TPM が有効の場合、BIOS **Advanced** メニューに **Trusted Computing** が 表示されます。TPM が無効の場合、**Trusted Computing** は表示されません。



Trellix ソフトウェア

概要

オプションの Trellix ライセンス (PFXYP6LSMCA) をご購入いただき Trellix ソフトウェアをご使用いただくことで本製品のセキュリティーを向上させることができます。ソフトウェアの機能および使用方法については、下記 URL を参照して関連するマニュアルを検索してください。
https://docs.trellix.com/bundle

以下に、ソフトウェアのインストール方法とマニュアルの検索方法について説明します。

インストール

1. Trellix ライセンス USB ストレージを本体に挿入します。
2. USB ストレージの **setup.exe** を実行します。
3. インストーラーが実行されます。

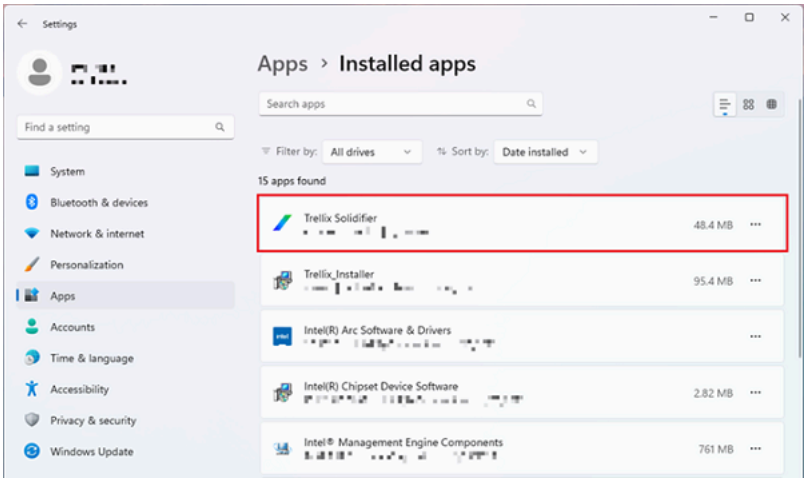
マニュアル検索方法

Trellix ソフトウェアマニュアルの検索方法は以下です。事前にソフトウェアのバージョンを確認する必要があります。

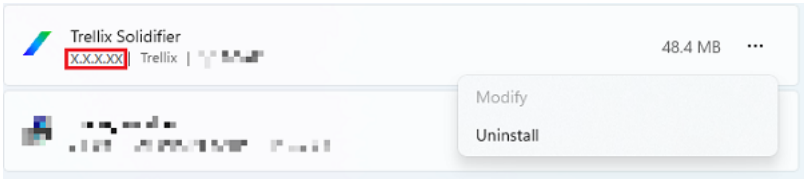
1. **設定**ボタンを選択します。

2. **アプリ**を選択します。

3. **アプリ**の **Trellix Solidifier** を選択します。



4. バージョンを確認します。



5. **アプリ**画面を閉じます。
6. Web ブラウザーで https://docs.trellix.com/bundle を表示させます。
7. 手順 4 で確認したバージョンに対応する **Application and Change Control** を検索します。

   注記 ： 弊社オプションの Trellix ライセンス USB ストレージで提供している Trellix は、Trellix で定義している管理対象外環境 (スタンドアロンまたは自己管理) に対応しています。Trellix ePolicy Orchestrator - On-prem の管理対象環境には対応していません。当該マニュアルを参照する際はご注意ください。

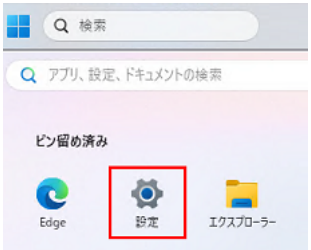
アンインストール

アンインストールをする場合、以下の 2 つのアプリケーションをアンインストールする必要があります。

- Trellix Solidifier
- Trellix Installer

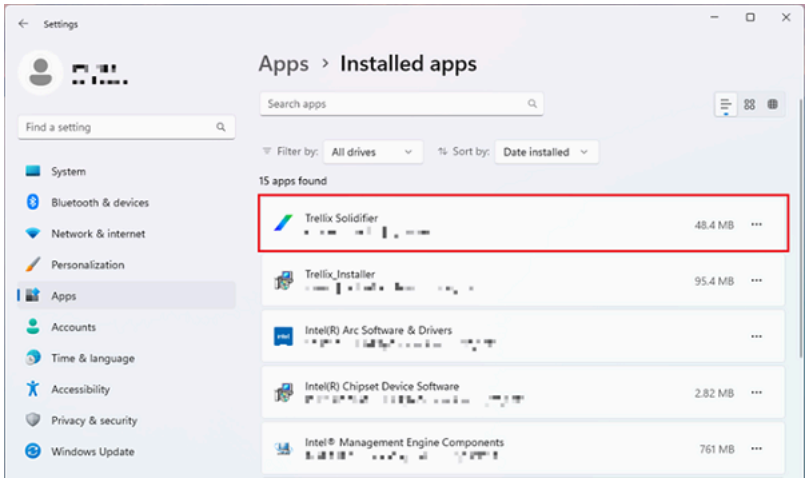
アンインストールの手順は以下のとおりです。

1. **設定**ボタンを選択します。

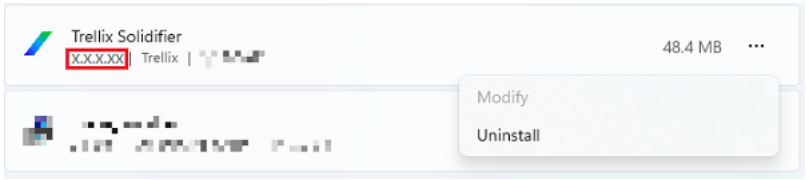


2. **アプリ**を選択します。

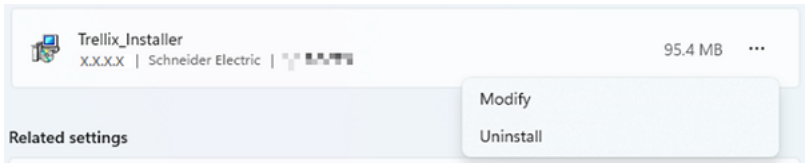
3. **アプリ**の **Trellix Solidifier** を選択します。



4. **アンインストール**を選択します。



5. 同じ手順で **Trellix_Installer** を選択して**アンインストール**を選択します。

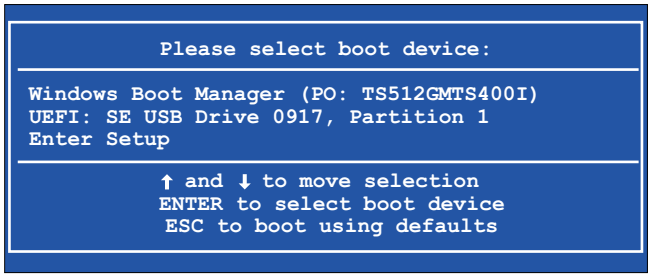


システムバックアップ

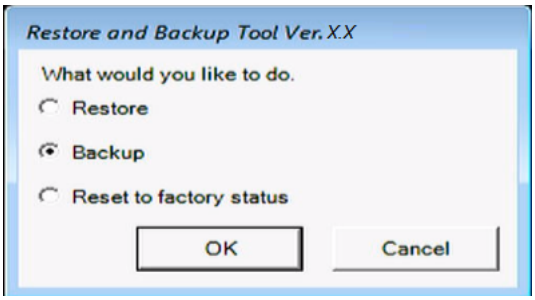
本製品のセットアップ後、システムをバックアップすることを推奨します。32 GB 以上の市販の USB メモリーを準備しバックアップ USB を作成します。

注記： ハイバネーション直後は、システムのバックアップまたはリカバリーを正常に行うことができません。システムのバックアップまたはリカバリーは、シャットダウンを行ってから実行してください。

1. 市販の USB メモリーを準備します。
2. ランチャーの **Recovery USB** を使用して、リカバリー USB の作成を行います。リカバリー USB, 22 ページを参照してください。
3. 手順 2 で作成したリカバリー USB を本製品に挿入します。
4. 本製品の電源を入れます。
5. ブート画面表示中に [F7] キーを押します。
6. パスワードを入力します (初期パスワード：Pw#12345)。
7. 次の画面が表示されるので、リカバリー USB を選択します。



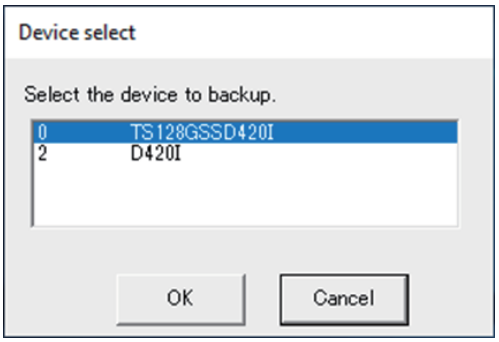
8. **Backup** > **OK** を選択します。



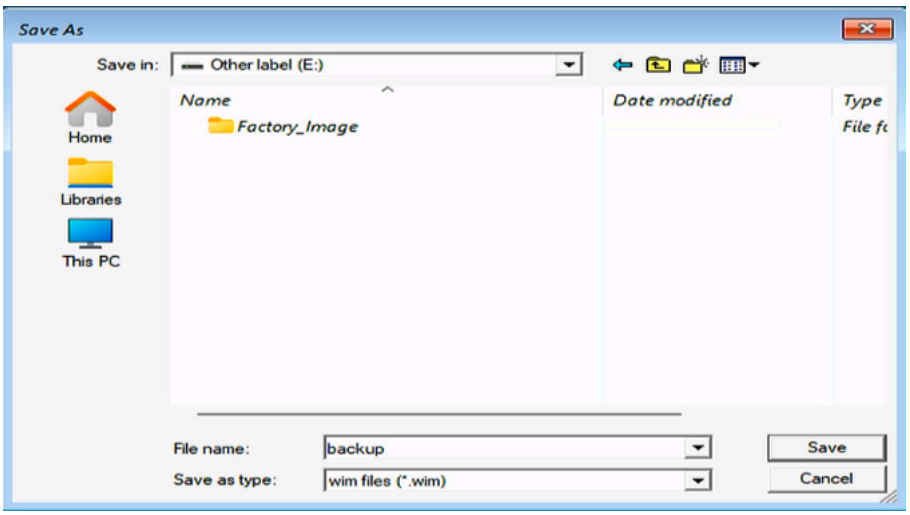
注記：

- 工場出荷時のイメージが保存されている「Factory image」フォルダーが、USB の「Other label」ドライブに残っている場合、**Reset to factory status** が表示されます。
- システムイメージを製品に復元すると、工場出荷時のイメージは失われます。ランチャーの **Recovery USB** を実行しても、工場出荷時のイメージは USB に作成されなくなります。

9. バックアップをするディスクを選択します。C ドライブのみバックアップすることが可能です。ダイアログボックスに複数のストレージデバイスが表示されている場合は、C ドライブのストレージデバイスを選択します。ストレージデバイスが 1 つしかない場合、以下の画面は表示されずに手順 10 に移ります。

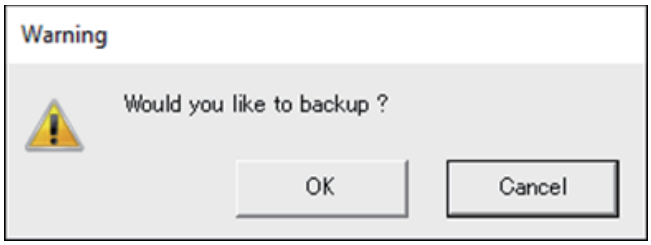


10. 「Other label」表記のドライブを選択、任意のファイル名を入力し、**Save** もしくは **Open** を選択します。

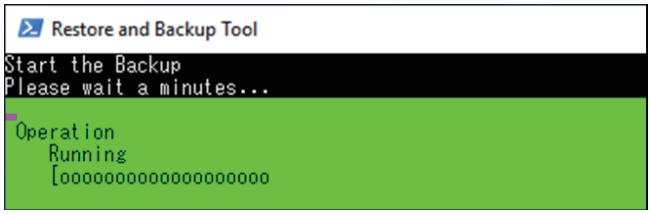


注記：「Factory image」フォルダーにバックアップイメージを作成しないでください。

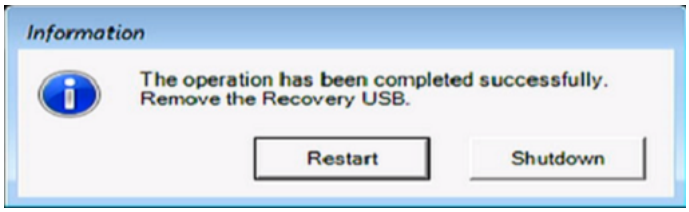
11. 確認画面で **OK** を選択します。



12. バックアップを開始します。



13. バックアップが完了すると以下の画面が表示されます。本製品から USB を抜き取り、**Restart** または **Shutdown** を選択します。

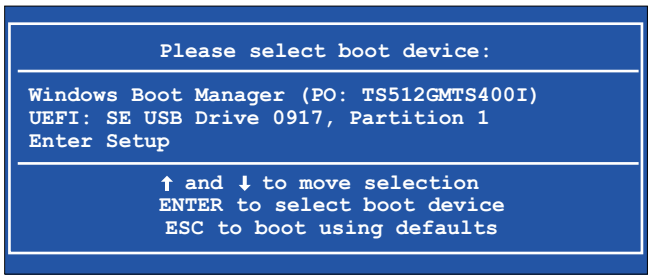


システムリカバリー

システムを復元するには、リカバリー USB が必要です。ランチャーの **Recovery USB** を使用して作成したリカバリー USB を準備します。リカバリー USB, 22 ページを参照してください。

注記： ハイバネーション直後は、システムのバックアップまたはリカバリーを正常に行うことができません。システムのバックアップまたはリカバリーは、シャットダウンを行ってから実行してください。

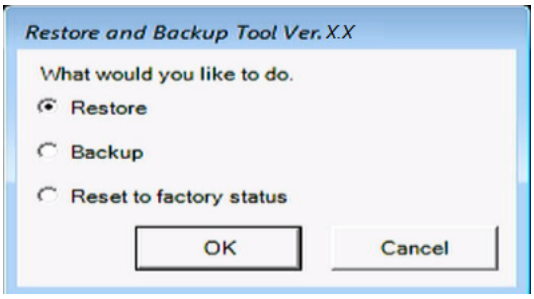
1. リカバリー USB を本製品に挿入します。
2. 本製品の電源を入れます。
3. ブート画面表示中に [F7] キーを押します。
4. パスワードを入力します (初期パスワード：Pw#12345)。
5. リカバリー USB を選択します。



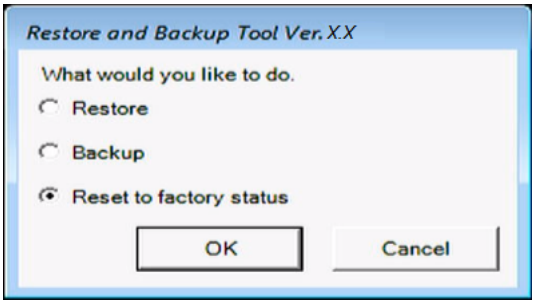
6. ランチャーの **Recovery USB** を使用してバックアップしたシステムイメージを復元するには、**Restore** > **OK** を選択します。

   注記：

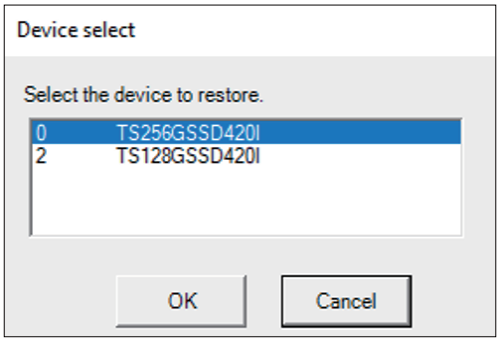
   - 工場出荷時のイメージが保存されている「Factory image」フォルダーが、USB の「Other label」ドライブに残っている場合、**Reset to factory status** が表示されます。
   - **Reset to factory status** は、オペレーティングシステムイメージのみをリセットします。UEFI BIOS 設定はリセットされません。
   - システムイメージを製品に復元すると、工場出荷時のイメージは失われます。ランチャーの **Recovery USB** を実行しても、工場出荷時のイメージは USB に作成されなくなります。



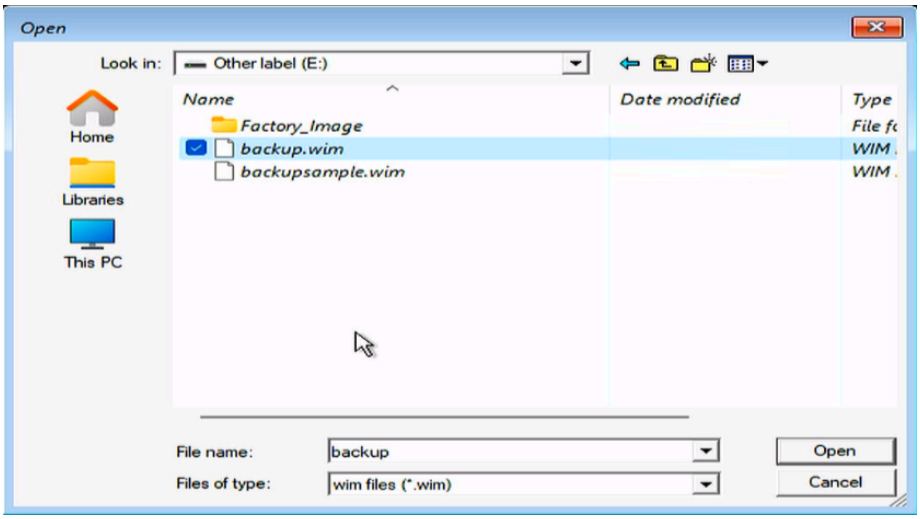
   工場出荷時のイメージを復元するには、**Reset to factory status** > **OK** を選択します。



7. 復元するディスクを選択します。ストレージが 1 つしかない場合、以下の画面は表示されずに手順 8 に移ります。

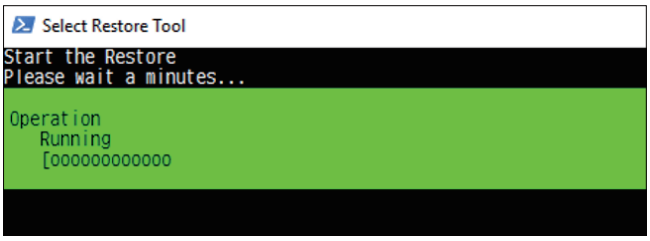


8. 「Other label」の下に wim ファイルが 1 つだけ保存されている場合、または工場出荷時に復元する場合は、手順 9 に進みます。「Other label」の下に 2 つ以上の wim ファイルが保存されている場合、「Other label」> 復元する wim ファイル > **Open** を選択します。

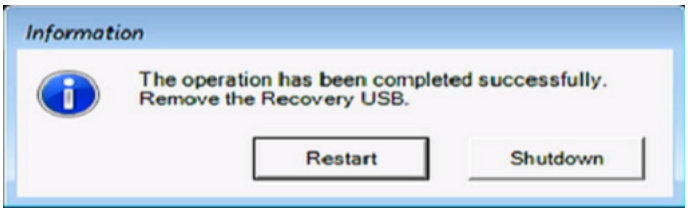


9. 確認画面で **OK** を選択します。

10. 復元が開始します。



11. 復元が完了し以下の画面が表示されたら、本製品からリカバリーメディアを抜き取り、**Restart** または **Shutdown** を選択します。



シュナイダーエレクトリックホールディングス株式会社

大阪府大阪市中央区北浜4-4-9
541-0041 日本

+ 81 (0) 50 4561 4800

www.pro-face.com

PSA6000-WINSYS-UG-JA.01