セキュアブート証明書 更新手順

本書は、「Windows セキュアブート証明書の有効期限切れ」の対応として、セキュアブート証明書および Windows ブートマネージャーの更新手順について示します。

【事前準備】
本更新手順を実施するためには、2025 年 11 月以降の累積更新プログラムが
適用されていることが必須条件となります。
事前に Windows Update を実施して最新の状態にしてください。
本書末尾に各 OS の Windows Update 手順を記載していますのでご参照ください。

【作業時間の目安】
本更新作業の目安は以下となります。　（Windows Update の作業時間は除く）
なお、作業時間は装置構成や環境条件により変動する場合があります。
1. セキュアブート証明書とブートマネージャーの更新　約 10 分
2. Windows ブートマネージャーの確認　約　5 分

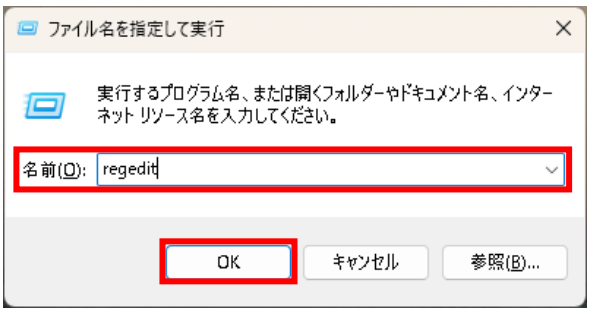
【更新手順】
以下の手順で実施してください。
実際の設定項目については、対象装置のユーザーズマニュアルをご参照の上、読み替えて実施をお願いします。

1．セキュアブート証明書とブートマネージャーの更新

以下の手順で実施してください。

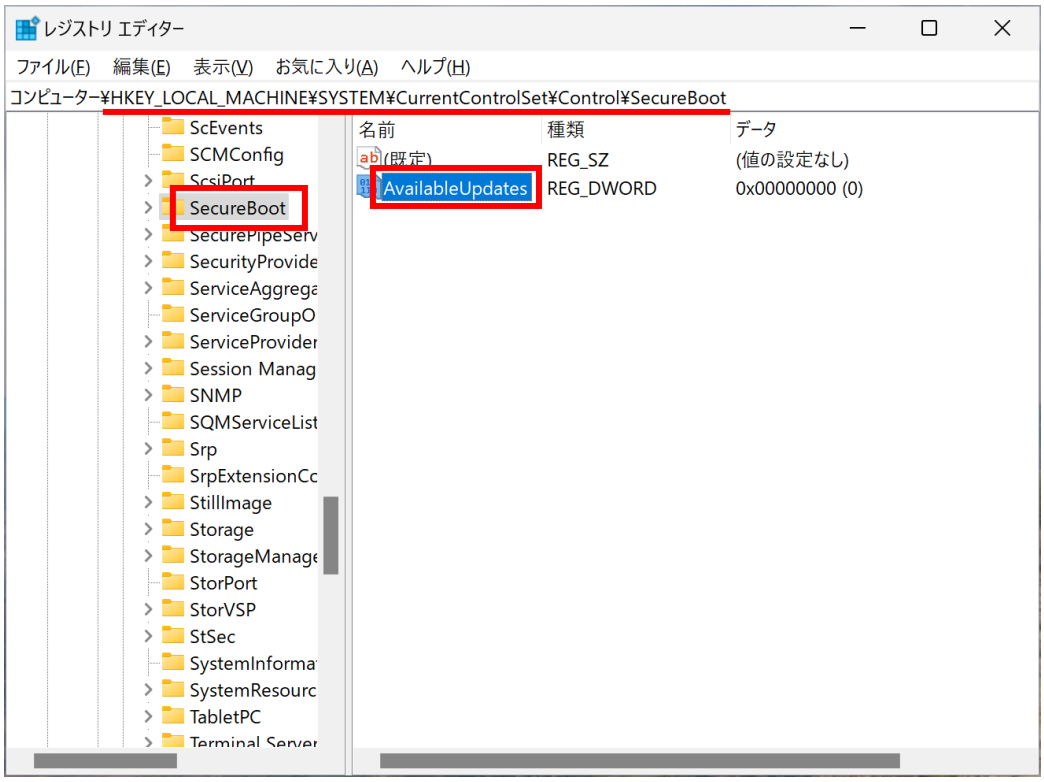
1)Windows 起動後、スタートボタンを右クリックし、「ファイル名を指定して実行」を選択してください。

2)「名前 (O):」欄に「regedit」と入力し、「OK」をクリックしてください。



3)「ユーザー アカウント制御」 画面が表示された場合は、[はい] をクリックしてください。

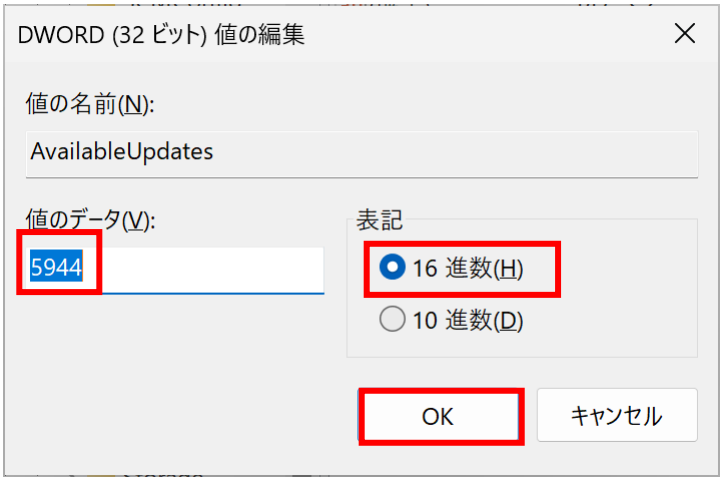
4)レジストリエディターが起動します。
レジストリエディターの左のウィンドウで
「HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecureBoot」を選択してください。



5)右ウィンドウで「AvailableUpdates」をダブルクリックすると、6)で示す画面が表示されます。

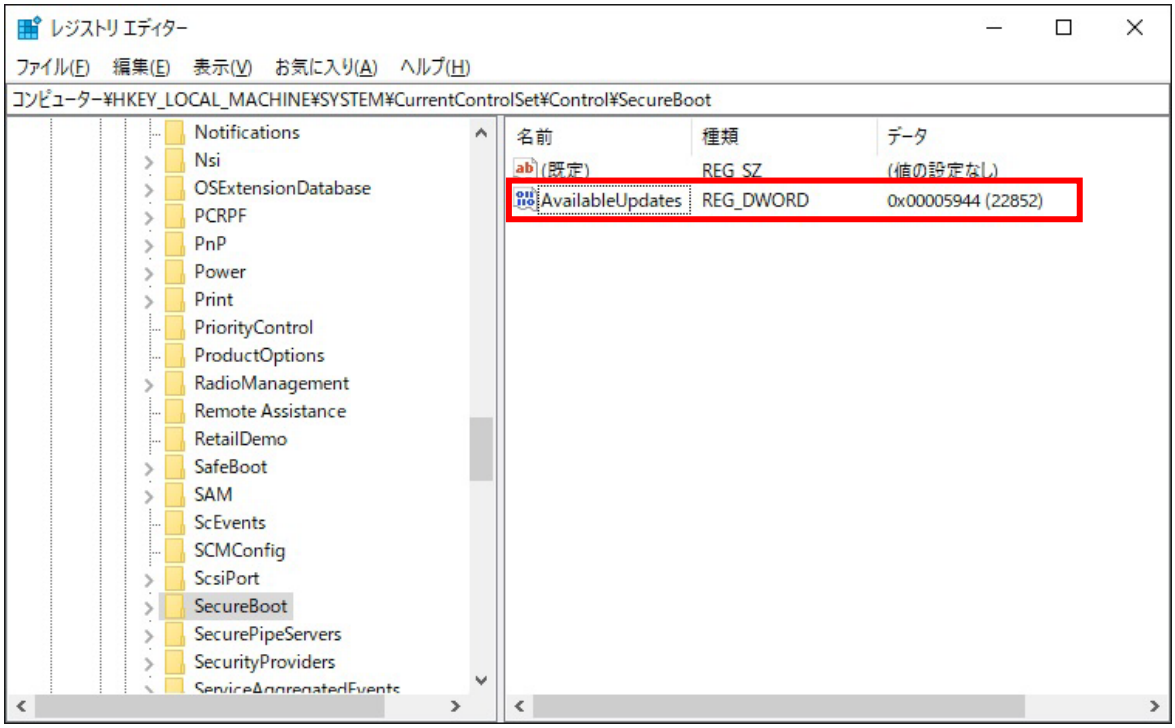
6)以下のように設定し「OK」を選択してください。

・値のデータ(V)　　5944 を入力
・表記　　16 進数(H) を選択



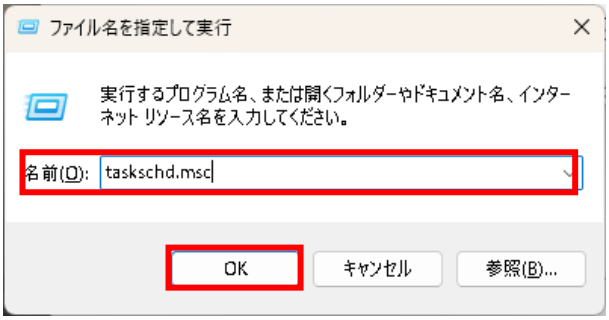
7)レジストリエディター右ウィンドウで以下の値となっていることを確認してください。

・名前　　AvailableUpdates
・種類　　REG_DWORD
・データ　　0x00005944 (22852)



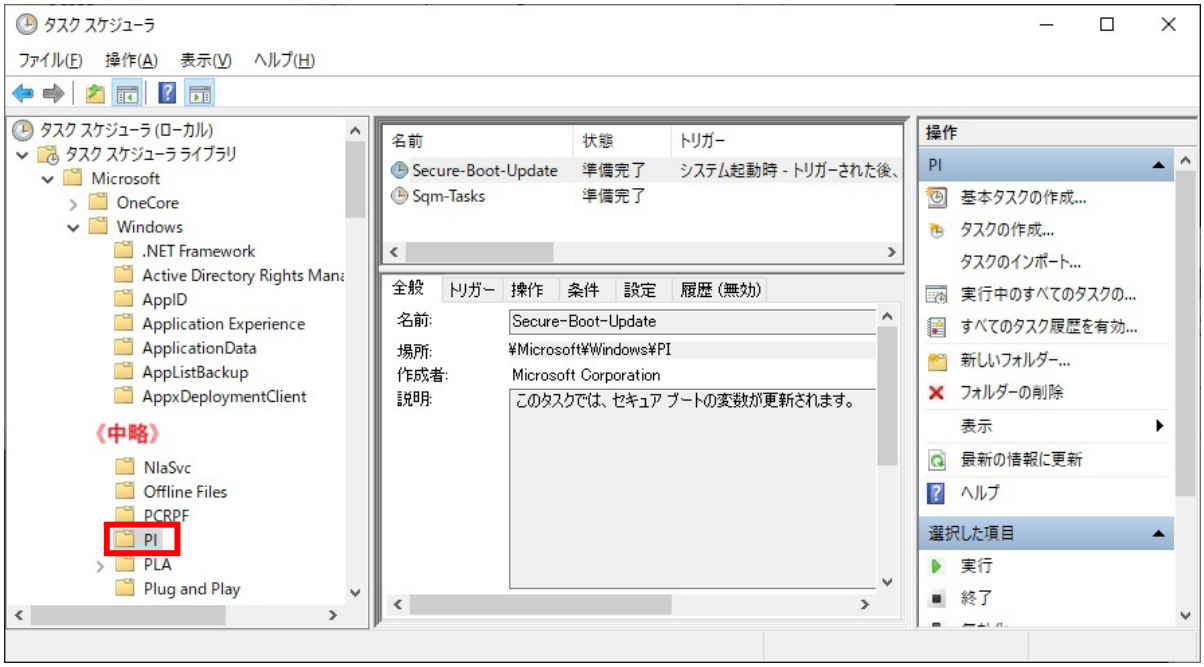
8)スタートボタンを右クリックし「ファイル名を指定して実行」を選択してください。

9)「名前 (O):」欄に「taskschd.msc」と入力し、「OK」をクリックしてください。

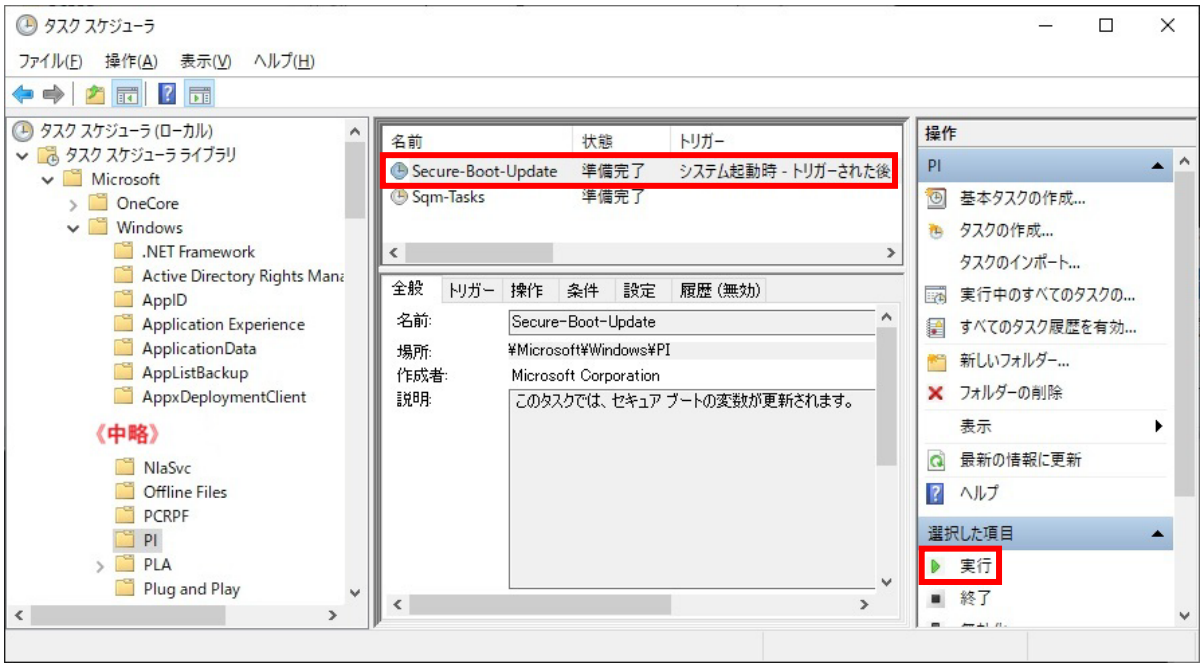


10)「ユーザー アカウント制御」 画面が表示された場合は、[はい]をクリックしてください。

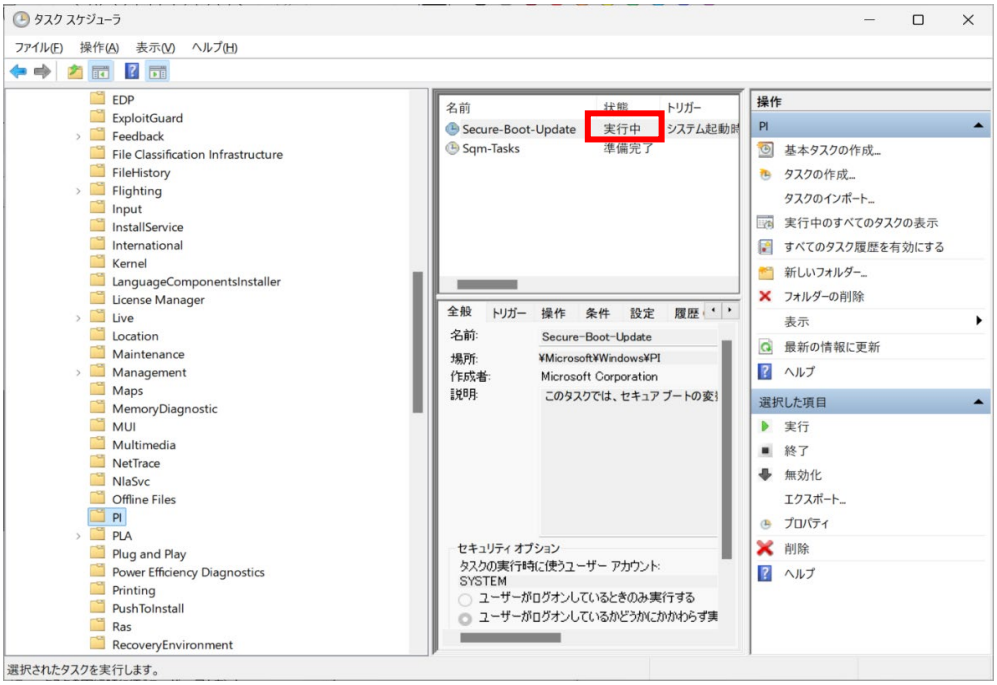
11）タスクスケジューラの左のウィンドウで「タスクスケジューラライブラリ」の下の「Microsoft」-「Windows」-「PI」を選択してください。



12）中央上のウィンドウで「Secure-Boot-Update」を選択し、右のウィンドウの「実行」をクリックしてください。



13) 「Secure-Boot-Update」が「実行中」に変更されたことを確認してください。

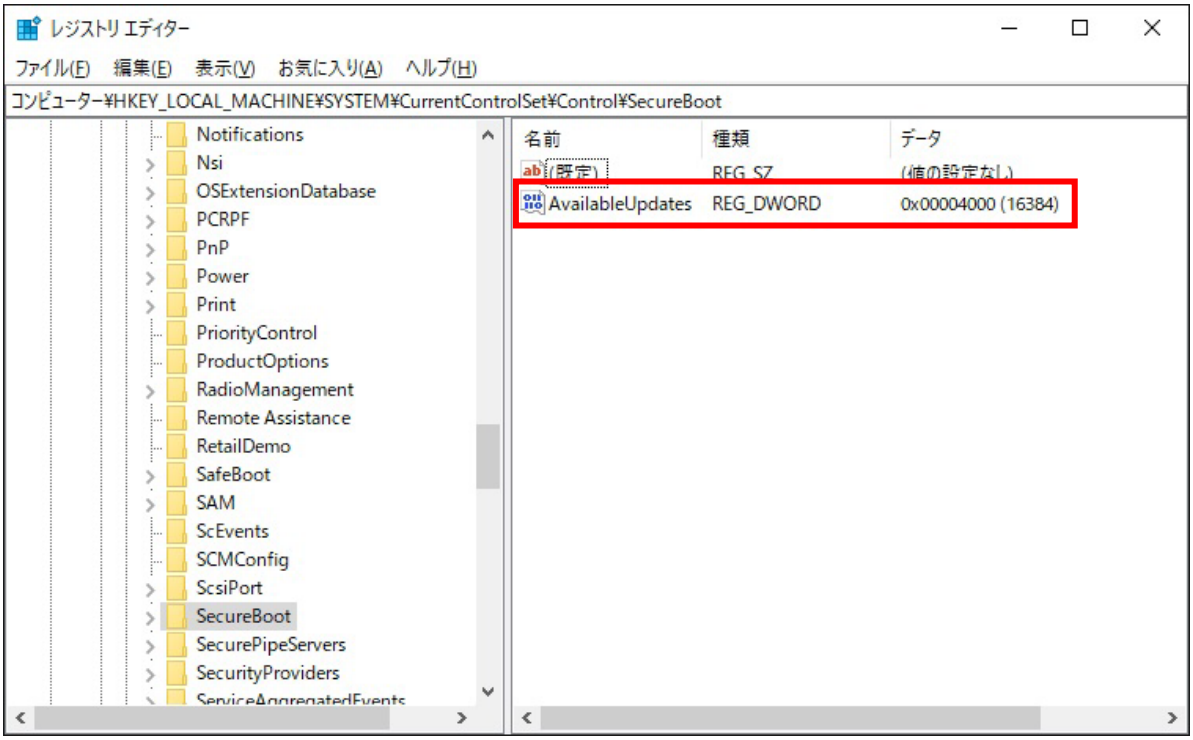


14) 1)～3)の手順でレジストリエディターを開きます。

15) レジストリエディター左のウィンドウで
「HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecureBoot」
を選択してください。

16) 画面上部の [表示] → [最新の情報に更新] をクリックしてください。

17) 「AvailableUpdates」の値(下記赤枠部分)を確認してください。



18) 「AvailableUpdates」の値が”0x00004100”または”0x00004000”になっている場合は、次へ進んでください。

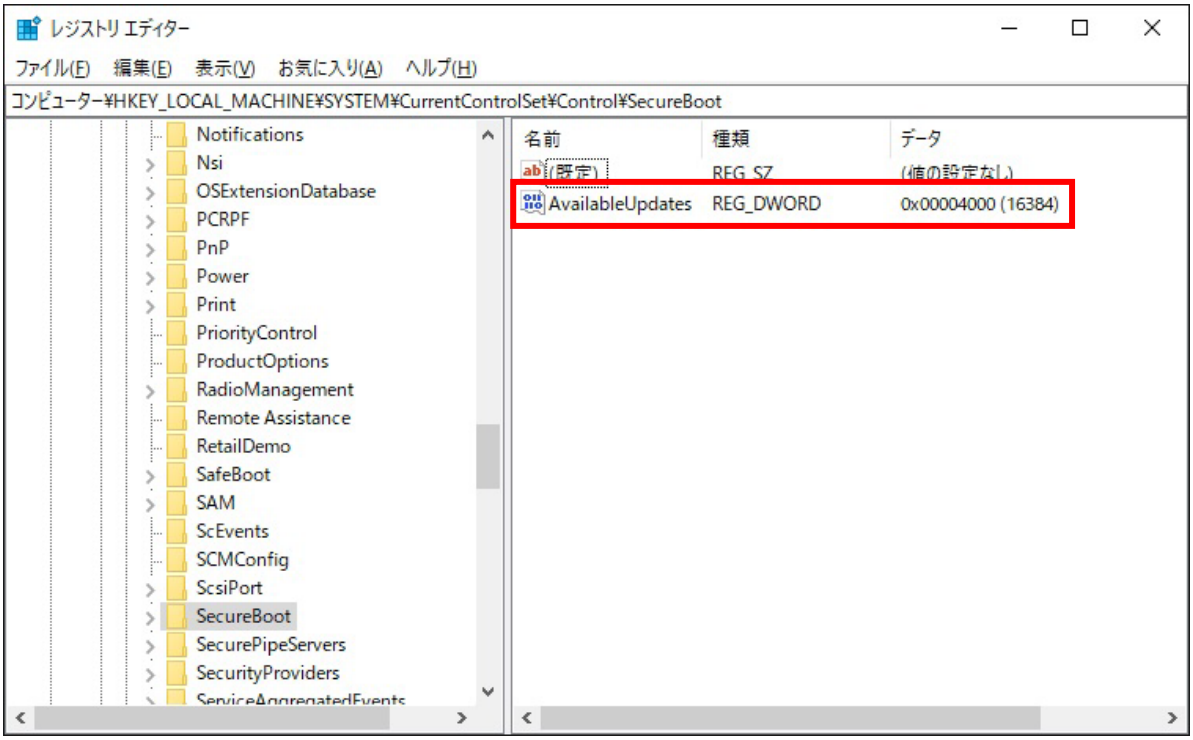
※値が更新されるまでに時間がかかる場合があります。
値が変わっていない場合は、30 秒～5 分程度待ってから再度確認してください。5 分以上経過しても値が変わらない場合は、再度 8)以降を実施してください。

19) レジストリエディターとタスクスケジューラを閉じ、OS を再起動してください。

20) Windows 起動後、1)～3)の手順でレジストリエディターを開きます。

21) レジストリエディター左のウィンドウで「HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecureBoot」を選択してください。

22) 右ウィンドウの「AvailableUpdates」の値(下記赤枠部分)を確認してください。
値が”0x00004100”、”0x00000100”、”0x00000104”、”0x00004104”の場合は、8)以降を再度実施してください。
値が”0x00004000”、”0x00000000”になっている場合は、次へ進んでください。



23) 以上で、セキュアブート証明書および Windows ブートマネージャーの更新作業は終了です。OS を再起動してください。

続いて「2．Windows ブートマネージャーの確認」へ進んでください。

２．Windows ブートマネージャーの確認

以下の手順で Windows ブートマネージャーが更新されていることを確認してください。

1)タスクバーの Windows アイコンを右クリックし、表示されたメニューから次のいずれかをクリックしてください。

・Windows PowerShell（管理者）
・ターミナル（管理者）

2)「ユーザー アカウント制御」 画面が表示された場合は、[はい] をクリックしてください。

3)Windows PowerShell が起動したら、EFI システムパーティションをマウントするため以下のコマンドを実行してください。

[コマンド]
mountvol s: /s

4)Windows ブートマネージャーを任意の場所にコピーするため、以下のコマンドを実行してください。

[コマンド]
copy s:¥EFI¥Microsoft¥Boot¥bootmgfw.efi <任意の保存先(ファイルパス)>

例として、Windows ブートマネージャーを c:¥にファイル名：bootmgfw.efi でコピーする場合は、以下のコマンドを実行してください。

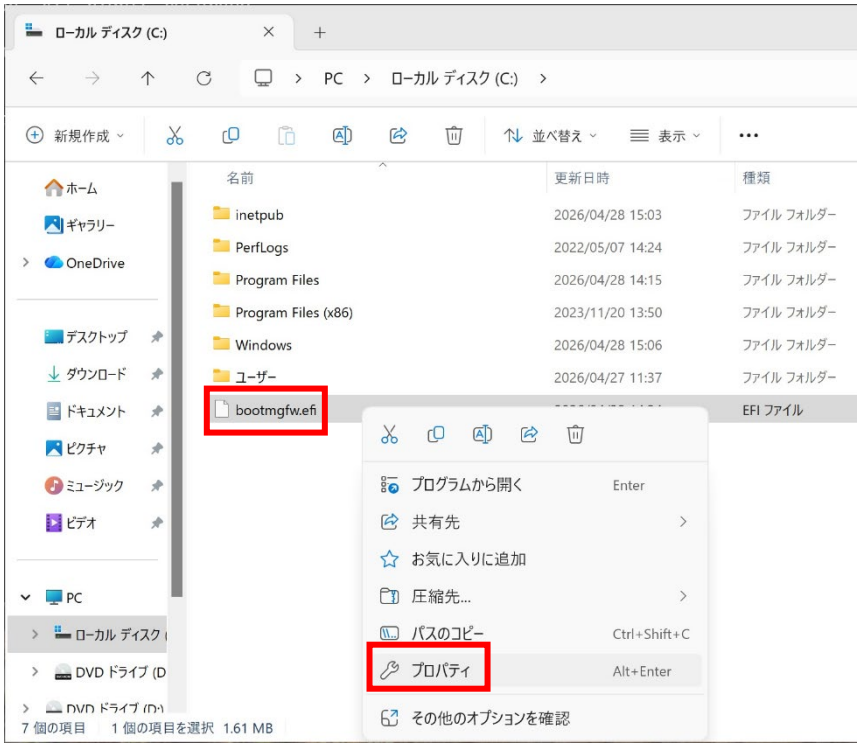
[コマンド]
copy s:¥EFI¥Microsoft¥Boot¥bootmgfw.efi c:¥bootmgfw.efi

5)EFI システムパーティションのマウントを解除するため、以下のコマンドを実行してください。

[コマンド]
mountvol s: /d

6)エクスプローラーを起動します。

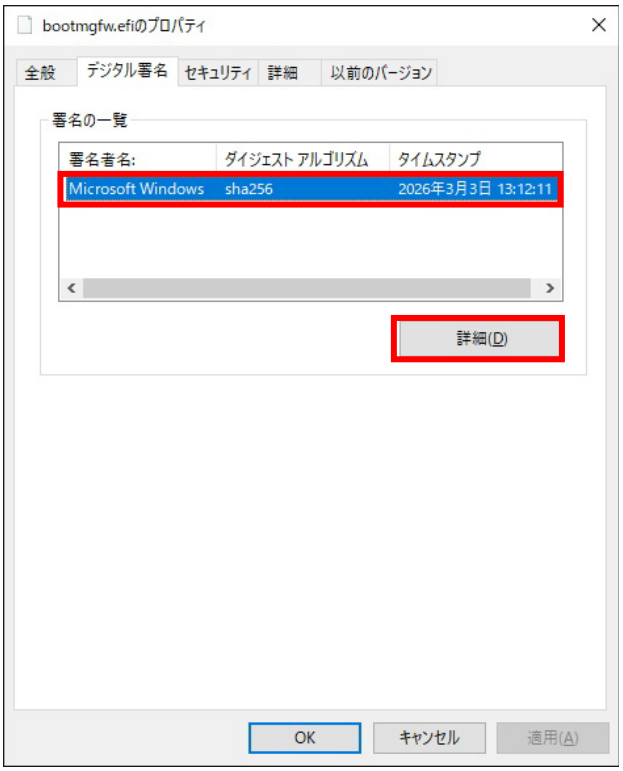
7) 4)でコピーしたファイルを選択し右クリックして『プロパティ』を開きます。



8)『デジタル署名』タブを選択してください。

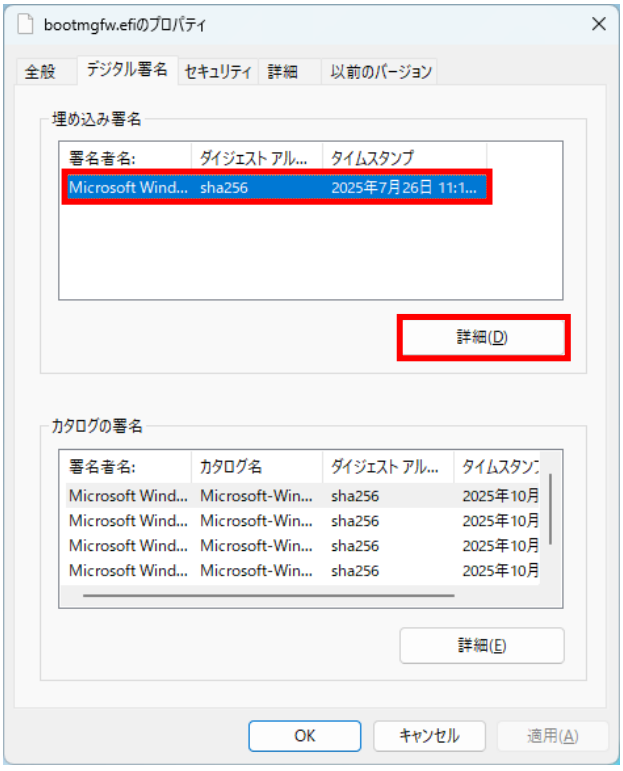
9)ご使用の OS によって『デジタル署名』タブの画面が異なります。
以下、ご使用の OS の手順を実施してください。

◇「Windows 10 IoT Enterprise」、「Windows Server 2016 for Embedded」、「Windows Server IoT 2019」、「Windows Server IoT 2022」の場合



[署名の一覧]欄の署名者名で"Microsoft Windows"を選択し、『詳細』ボタンをクリックしてください。

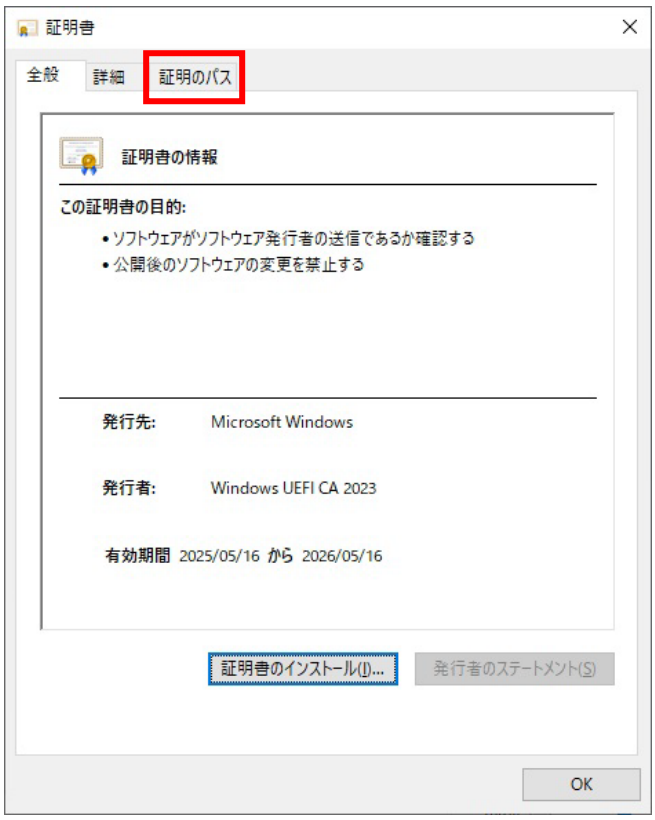
◇「Windows 11 IoT Enterprise」、「Windows Server IoT 2025」の場合



[埋め込み署名]欄の署名者名で"Microsoft Windows"を選択し、『詳細』ボタンをクリックしてください。

10）『デジタル署名の詳細』画面が表示されたら、『証明書の表示』を選択してください。

11）『証明書』画面が表示されたら、『証明のパス』タブを選択してください。

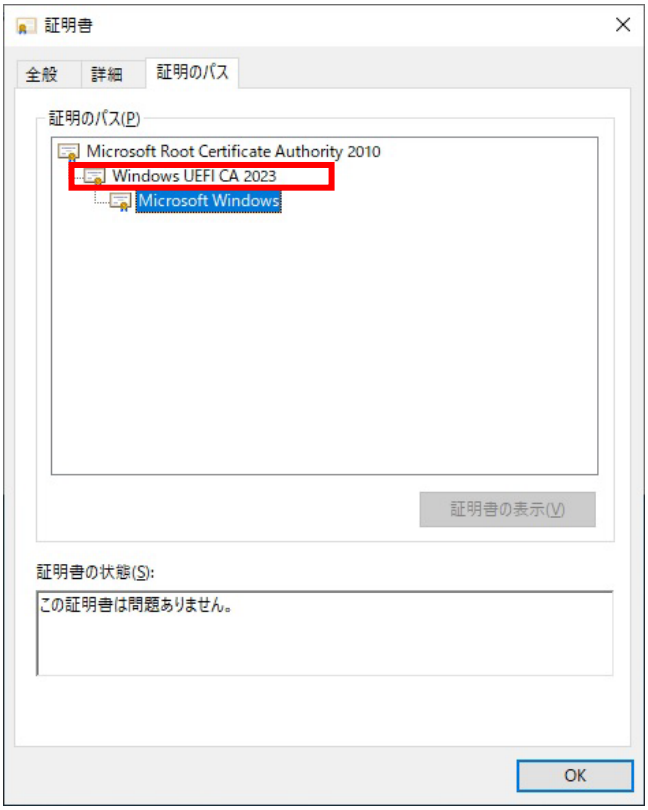


12) 『証明のパス』が表示されたら、証明のパスに以下の CA が表示されているか確認してください。

Windows UEFI CA 2023 ：Windows ブートマネージャーが更新済みです。

上記以外 ：Windows ブートマネージャーは未更新です。

「1.セキュアブート証明書とブートマネージャーの更新」に戻って、最初から実施してください。



13) 4)でコピーしたファイル（bootmgfw.efi）を削除してください。

以上で、確認作業は終了です。

―以上―

【補足】各 OS の Windows Update 手順

プリインストールモデルやリカバリディスクで再セットアップをした場合、Windows Update のサービスは無効となっています。以下の手順で Windows Update サービスを開始し、Windows Update を実施してください。

※Windows Update による予期しない挙動を防ぐため、必要な Update 完了後は設定を元に戻すことを推奨します。

【Windows® 10 IoT Enterprise 2016 LTSB の場合】

1. 画面左下隅を右クリックし、一覧より「コンピューターの管理」をクリックしてください。
2. 画面左側の「サービスとアプリケーション」にある「サービス」をクリックしてください。
3. 「Windows Update」を右クリックし、プロパティをクリックしてください。
4. 以下の設定を変更してください。
   サービスの状態　　：開始
   スタートアップの種類：自動

【Windows® 10 IoT Enterprise 2019 LTSC の場合】

Windows Update サービスが起動しないようにするため複数の設定を行っています。

⑴ グループポリシー設定の変更

1. 画面左下隅を右クリックし、一覧より「ファイル名を指定して実行」をクリックしてください。
2. 「gpedit.msc」と入力し、OK をクリックしてください。
3. 左画面の「コンピューターの構成」にある以下のメニューを開きます。
   「管理者用テンプレート」→ 「Windows コンポーネント」→ 「Windows Update」
4. 以下の設定を変更してください。
   推奨される更新の自動更新を構成する：未構成
   自動更新を構成する　　：未構成

⑵ Windows Update サービスの変更

1. 画面左下隅を右クリックし、一覧より「コンピューターの管理」をクリックしてください。
2. 画面左側の「サービスとアプリケーション」にある 「サービス」をクリックしてください。
3. 「Windows Update」を右クリックし、プロパティをクリックしてください。
4. 以下の設定を変更してください。
   サービスの状態　　：開始
   スタートアップの種類：自動

【Windows® 10 IoT Enterprise 2021 LTSC の場合】

Windows Update サービスが起動しないようにするため複数の設定を行っています。

(1) グループポリシー設定の変更

1. 画面左下隅を右クリックし、一覧より「ファイル名を指定して実行」をクリックしてください。
2. 「gpedit.msc」と入力し、OK をクリックしてください。
3. 左画面の「コンピューターの構成」にある以下のメニューを開きます。
   「管理者用テンプレート」→「Windows コンポーネント」→「Windows Update」
4. 以下の設定を変更してください。
   推奨される更新の自動更新を構成する：未構成
   自動更新を構成する　　：未構成

(2) Windows Update サービスの変更

1. 画面左下隅を右クリックし、一覧より「コンピューターの管理」をクリックしてください。
2. 画面左側の「サービスとアプリケーション」にある「サービス」をクリックしてください。
3. 「Windows Update」を右クリックし、プロパティをクリックしてください。
4. 以下の設定を変更してください。
   サービスの状態　　：開始
   スタートアップの種類：自動

【Windows® 11 IoT Enterprise LTSC 2024 の場合】

1. タスクバーの Windows アイコンを右クリックし、[ファイル名を指定して実行]をクリックしてください。
2. 「gpedit.msc」と入力し、OK をクリックしてください。
3. 左画面の「コンピューターの構成」にある以下のメニューを開きます。
   「管理者用テンプレート」→「Windows コンポーネント」→「Windows Update」→「従来のポリシー」
4. 以下の設定を変更してください。
   推奨される更新の自動更新を構成する：未構成
5. 手順 3 に引き続き、次のメニューを開き、以下の設定を変更してください。
   「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　：未構成

【Windows Server IoT 2016 for Embedded Systems の場合】

1. 画面左下隅を右クリックし、一覧より「コンピューターの管理」をクリックしてください。
2. 画面左側の「サービスとアプリケーション」にある 「サービス」をクリックしてください。
3. 「Windows Update」を右クリックし、プロパティをクリックしてください。
4. 以下の設定を変更してください。
   サービスの状態　　：開始
   スタートアップの種類：自動

【Windows Server IoT 2019 の場合】

1. 画面左下隅を右クリックし、一覧より「コンピューターの管理」をクリックしてください。
2. 画面左側の「サービスとアプリケーション」にある 「サービス」をクリックしてください。
3. 「Windows Update」を右クリックし、プロパティをクリックしてください。
4. 以下の設定を変更してください。
   サービスの状態　　：開始
   スタートアップの種類：自動

【Windows Server IoT 2022 の場合】

Windows Update サービスが起動しないようにするため複数の設定を行っています。

(1) グループポリシー設定の変更

1. 画面左下隅を右クリックし、一覧より「ファイル名を指定して実行」をクリックしてください。
2. 「gpedit.msc」と入力し、OK をクリックしてください。
3. 左画面の「コンピューターの構成」にある以下のメニューを開きます。
   「管理者用テンプレート」→ 「Windows コンポーネント」→ 「Windows Update」
4. 以下の設定を変更してください。
   推奨される更新の自動更新を構成する：未構成
   自動更新を構成する　　：未構成

(2) Windows Update サービスの変更

1. 画面左下隅を右クリックし、一覧より「コンピューターの管理」をクリックしてください。
2. 画面左側の「サービスとアプリケーション」にある 「サービス」をクリックしてください。
3. 「Windows Update」を右クリックし、プロパティをクリックしてください。
4. 以下の設定を変更してください。
   サービスの状態　：開始
   スタートアップの種類：自動

【Windows Server® IoT 2025 の場合】

1. タスクバーの Windows アイコンを右クリックし、[ファイル名を指定して実行]をクリックしてください。
2. 「gpedit.msc」と入力し、OK をクリックしてください。
3. 左画面の「コンピューターの構成」にある以下のメニューを開きます。
   「管理者用テンプレート」→ 「Windows コンポーネント」→ 「Windows Update」→「従来のポリシー」
4. 以下の設定を変更してください。
   推奨される更新の自動更新を構成する：未構成
5. 手順 3 に引き続き、次のメニューを開き、以下の設定を変更してください。
   「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　：未構成

-以上-