セキュアブート証明書 更新手順

本書は、マイクロソフト社の「Windows セキュアブート証明書の有効期限と CA 更新プログラム」に従い、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を示します。
※事前に Windows Update を実施して最新の状態にして、作業を開始してください。

【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、必要に応じて対象装置のユーザーズマニュアルを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を行います。

1）事前に Windows Update を実施してください。
　※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本更新の必須条件です。

2）Windows 起動後、管理者権限で Windows PowerShell を起動します。

3）Windows PowerShell が起動したら、セキュアブート証明書および Windows ブートマネージャー更新用のレジストリ値設定のため、以下のコマンドを実行します。
コマンドおよび 0x5944 の値は正しく入力していることを確認してください。

[コマンド]

```
reg add HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecureBoot /v AvailableUpdates /t REG_DWORD /d 0x5944 /f
```

4）セキュアブート証明書および Windows ブートマネージャー更新のため、以下のコマンドを実行します。

[コマンド]

```
Start-ScheduledTask -TaskName “¥Microsoft¥Windows¥PI¥Secure-Boot-Update”
```

5）セキュアブート証明書の更新処理が完了したか確認するため、以下のコマンドを実行します。

[コマンド]

```
reg query HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecureBoot /v AvailableUpdates
```

コマンドを実行すると、以下の実行結果が表示されます。

[実行結果]

```
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Secureboot
 AvailableUpdates    REG_DWORD    0x4000
```

AvailableUpdates の値(上記赤枠部分)を確認します。
値が”0x4100”または”0x4000”になっている場合は、手順 6)へ進んでください。
値の更新にしばらく時間がかかる場合があります。値が”0x4100”または”0x4000”以外の場合、しばらく待ってから、手順 5）のコマンドを再度実行してください。
それでも値が”0x4100”または”0x4000”以外の場合、本値になるまで手順 4)に戻り、コマンドを実行してください。

6）OS を再起動してください。

7）Windows 起動後、管理者権限で Windows PowerShell を起動します。

8）セキュアブート証明書の更新処理が完了しているか確認するため、以下のコマンドを実行します。
[コマンド]

```
reg query HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecureBoot /v AvailableUpdates
```

コマンドを実行すると、以下の実行結果が表示されます。
[実行結果]

```
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Secureboot
  AvailableUpdates      REG_DWORD      0x4000
```

AvailableUpdates の値(上記赤枠部分)を確認します。
値が”0x4100”、”0x0100”、”0x0104”、”0x4104”になっている場合は、手順 9）へ進んでください。
値が”0x4000”、”0x0000”になっている場合は、手順 10)へ進んでください。

9）Windows ブートマネージャー更新のため、以下のコマンドを実行します。
[コマンド]

```
Start-ScheduledTask -TaskName “¥Microsoft¥Windows¥PI¥Secure-Boot-Update”
```

10)Windows ブートマネージャーの更新処理が完了しているかどうか確認するため、以下のコマンドを実行します。
[コマンド]

```
reg query HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecureBoot /v AvailableUpdates
```

コマンドを実行すると、以下の実行結果が表示されます。
[実行結果]

```
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Secureboot
 AvailableUpdates    REG_DWORD    0x4000
```

AvailableUpdates の値(上記赤枠部分)を確認します。
値が”0x4000”または”0x0000”になっていることを確認してください。
値の更新にしばらく時間がかかる場合があります。値が”0x4000”または”0x0000”以外の場合、しばらく待ってから、手順 10）を再度実施してください。

それでも値が”0x4000”または”0x0000”以外の場合は、本値になるまで手順 9)に戻り、コマンドを実行してください。

11）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。

12)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）Windows 起動後、管理者権限で Windows PowerShell を起動します。

2）Windows PowerShell が起動したら、Windows ブートマネージャーを確認するための 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ます。

[コマンド]

```
mountvol s: /s
```

3）Windows ブートマネージャーを確認するため、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ます。

[コマンド]

```
copy s:¥EFI¥Microsoft¥Boot¥bootmgfw.efi〈任意のファイル〉
```

例として、Windows ブートマネージャーを c:¥にコピーする場合は、以下のコマンドを実行します。

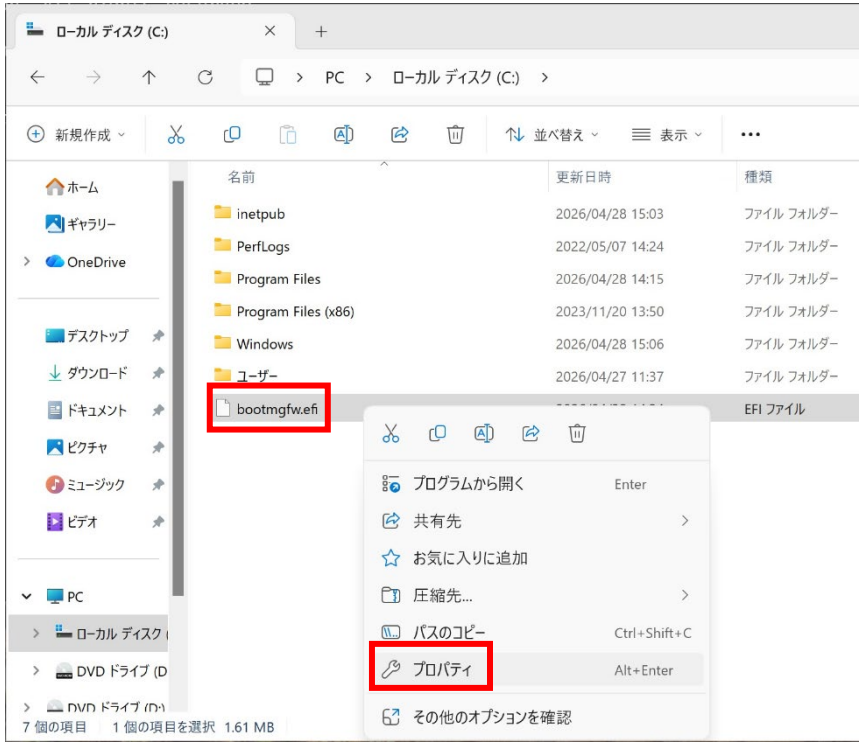
```
copy s:¥EFI¥Microsoft¥Boot¥bootmgfw.efi c:¥bootmgfw.efi
```

4）手順 3)により EFI システムパーティションが不要となるため、アンマウントするため、以下のコマンドを実行します。

[コマンド]

```
mountvol s: /d
```

5）エクスプローラーを起動して、手順 3)でコピーしたファイルを選択して右クリックし、『プロパティ』を開きます。

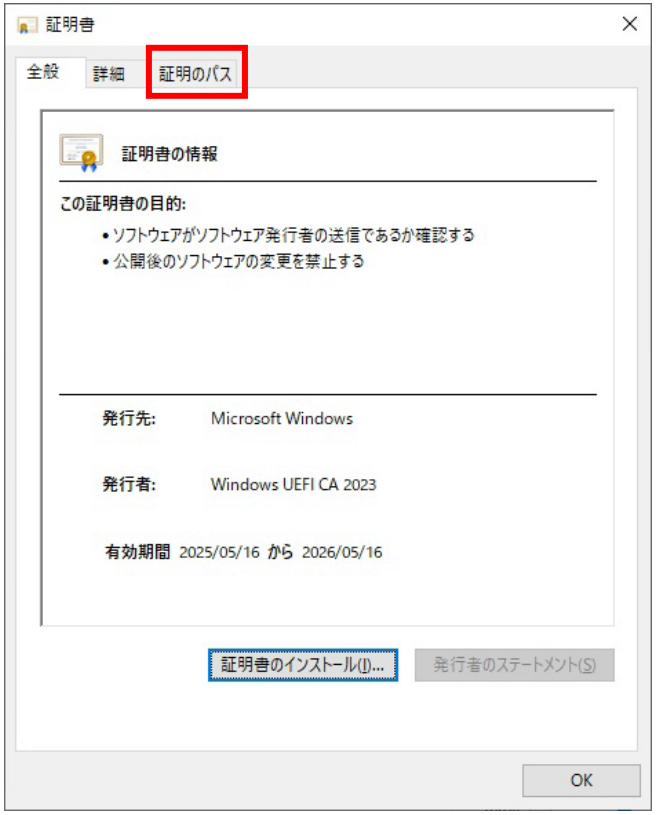


6）Windows ブートマネージャーのデジタル署名を確認するため『デジタル署名』タブを選択します。

7）『デジタル署名』タブを表示したら、[カタログの署名]欄の署名者名が"Microsoft Windows"のエントリを選択し、『詳細』を選択します。

8）『デジタル署名の詳細』画面が表示されたら、『証明書の表示』を選択します。

9）『証明書』画面が表示されたら、『証明のパス』タブを選択します。

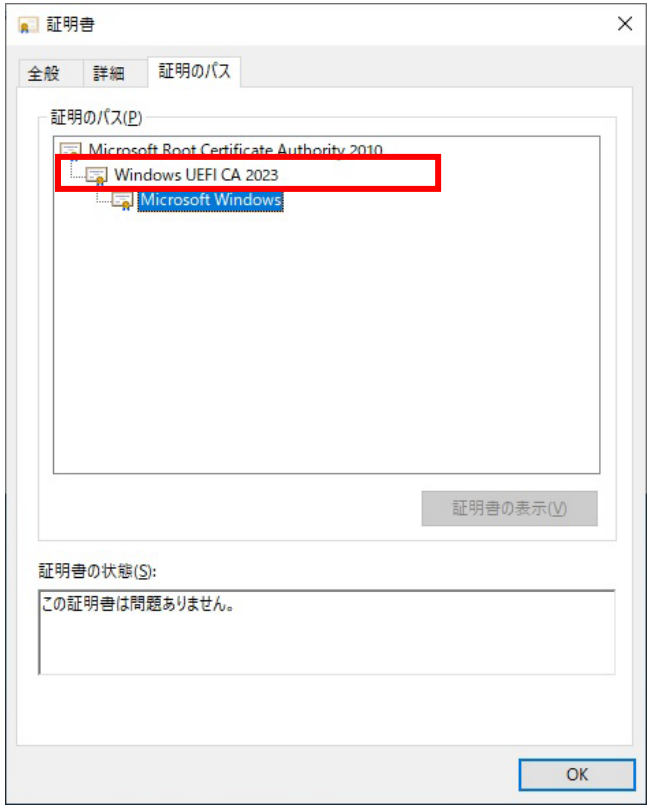


10)『証明のパス』が表示されたら、証明のパスに以下の CA が表示されているかご確認ください。

Windows UEFI CA 2023　：Windows ブートマネージャーが更新されています。

上記以外　　：Windows ブートマネージャーが更新されていません。

本書の最初の手順より再度実施をお願いします。



11)手順 3)でコピーしたファイルを削除してください。

以上で Windows ブートマネージャーの確認作業は終了です。

―以上―