共有する

今日 9:45

SecureBootViolation_rev...
Zip アーカイブ

windows11 で security boot vialation が発生し、添付のバッチファイルを管理者で実行させるように指示がありました。子のバッチファイルは何を実行しているものか教えてください。

10s考えました

添付の `SecureBootViolation_rev2.bat` を確認しました。このバッチファイルは、**WindowsのEFIシステムパーティション内のブートファイルをいったん削除し、Windows標準の `bcdboot` コマンドでブートファイルを再作成する**ものです。

特に重要なのは、次の3行です。

```bat
Mountvol X: /s
del X:\*.* /f /s /q
bcdboot %systemroot% /s X:
```

それぞれの処理は以下の意味です。

1. `Mountvol X: /s`
   通常はドライブ文字が付いていない **EFI System Partition（ESP）** を、一時的に `X:` ドライブとしてマウントします。EFIパーティションには、WindowsをUEFI/Secure Bootで起動するためのブートローダーなどが保存されています。
2. `del X:\*.* /f /s /q`
   ここが最も重要です。**X: にマウントしたEFIシステムパーティション内のファイルを再帰的に削除します。**
   `/f` は読み取り専用ファイルも強制削除、`/s` はサブフォルダも対象、`/q` は確認なしです。
3. `bcdboot %systemroot% /s X:`
   現在起動しているWindows（通常は `C:\Windows`）を元に、EFIパーティションへ**Windowsのブートファイルを新しくコピー・再構築**します。

つまり、概念的には、

```
EFIパーティションを X: として開く
        ↓
既存のEFIブートファイルを削除
        ↓
現在のWindowsから新しいブートファイルを作成
        ↓
X: の割り当てを解除
```

という処理です。

そのほか、バッチには安全確認も多少入っています。最初に

```bat
net session
```

を使って管理者権限で実行されているか確認し、管理者でなければ終了します。また、もともと `X:` ドライブが存在すると、

> X:ドライブは既に使用されています。
> X:ドライブの機器を取り外すかドライブレターを変更し、本ファイルを再度実行ください。

と表示して終了します。これは、誤って通常の `X:` ドライブを削除してしまう事故を防ぐためです。

処理後には `bcdboot` の出力から、

> ブート ファイルは正常に作成されました

という文字列が含まれているか確認しています。成功すれば、

```bat
mountvol X: /d
```

でEFIパーティションの `X:` 割り当てを解除します。

このバッチは危険か

マルウェア的な処理は見当たりませんが、かなり強いシステム変更を行うバッチです。

特に、

```bat
del X:\*.* /f /s /q
```

でEFIパーティションを削除してから作り直すため、途中で `bcdboot` が失敗したり、PCが特殊なマルチブート構成だったりすると、**Windowsや他のOSが起動できなくなる可能性があります。**

一般的な「Secure Boot Violation」の対処として、EFIブートファイルを再生成すること自体は技術的にはあり得る方法です。ただし、このバッチは既存EFIファイルをかなり大胆に削除しています。

特に以下の場合は、そのまま実行しない方が安全です。

- WindowsとLinuxなどのデュアルブート
- BitLockerを使用している
- メーカー独自のEFI領域を利用している
- 複数のWindowsが入っている
- 特殊なリカバリ環境が設定されている

また、このバッチは**Secure Bootそのものを無効化したり、BIOS/UEFIのSecure Boot設定を変更したりするものではありません**。レジストリやBCD設定を直接改ざんする処理もなく、主目的は「EFI上のWindowsブート環境の再構築」です。

もしこのPCが通常の **Windows 11のみのPC** で、このファイルがPCメーカーや保守会社から正式に提供されたものであれば、「Secure Boot Violation発生時に古い／壊れたEFIブートファイルを初期化して再作成する修復ツール」と考えるのが妥当です。

ただ、実行前には少なくとも **BitLocker回復キーを確認しておくこと** と、可能なら重要データのバックアップを強くおすすめします。

必要であれば次に、**このバッチを1行ずつ詳細に解説して、「Windows 11で実行した場合に実際にどのファイルが消えて、何が再作成されるのか」まで具体的に説明できます。**