

セキュアブートの証明書の話

2026-03-20

自分の理解確認用

登場要素

- KEK更新を許可する鍵（管理者）
- DB 起動していい名簿（ホワイトリスト）
- DBX 絶対ダメな名簿（ブラックリスト）
- Win Windowsのブートローダー

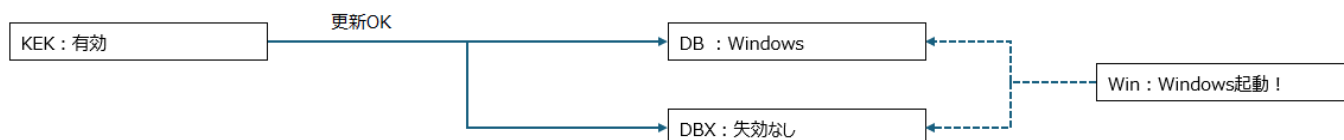
要素の更新順

この順で更新が行われる。

1. 新しいKEKに更新
2. 新しいDBに更新
3. 新しいブートローダーに更新
4. 新しいDBXに更新

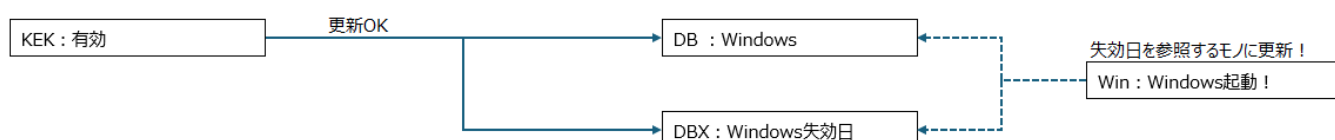
まずい事が起きるシナリオ

2026年6月より前の状態 1



2026年6月より前の状態 2

WindowsUpdateでWin DBXに更新が入る。まだ失効日は来ない。

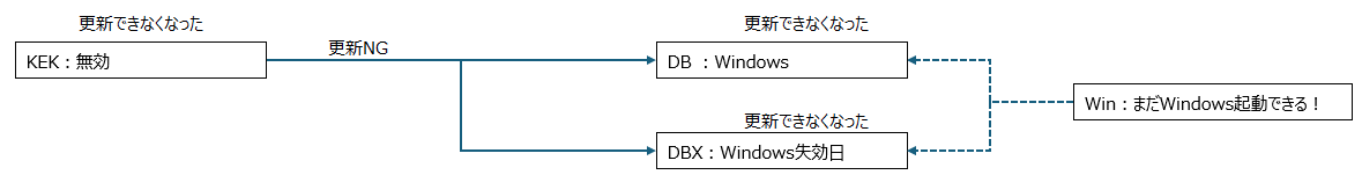


2026年6月 期限切れ

WindowsUpdateでKEKの更新をしていなければ、KEKの期限切れでKEK自身を更新できなくなった。

KEKが期限切れのままなのでWinDBDBXの更新もできなくなった。

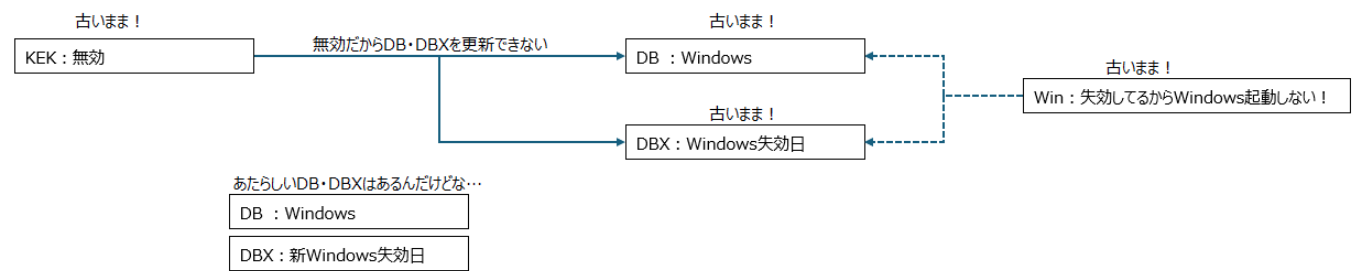
なおKEKが無効でもUEFIファームウェア更新等によりDBXだけが更新される可能性は残る。



起動しない日が来た

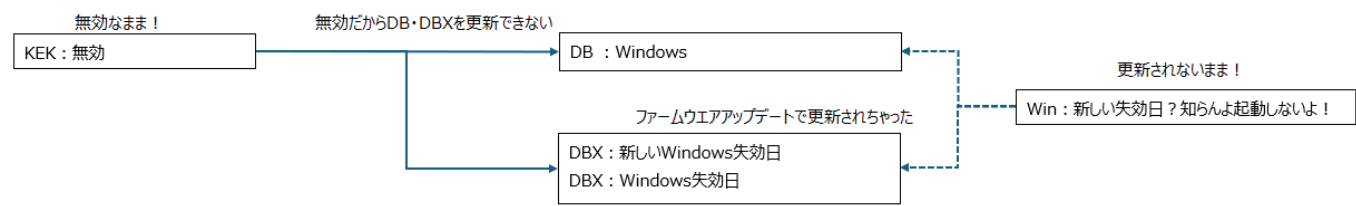
失効日が来ちゃった場合

KEKが期限切れになっているのでDBDBXを新しいもので更新できない。だからWindowsは起動しない。



DBDBXが更新されちゃった場合

UEFIのファームウェア側でDBDBXが更新される可能性がある。
Winが更新できていないので古い失効日を見てしまいWindowsの起動を停止してしまう。



Windows,セキュアブート

From:
<https://wiki.hgotoh.jp/> - 努力したWiki

Permanent link:
<https://wiki.hgotoh.jp/documents/windows/wu/doc-001?rev=1774024053>

Last update: 2026/03/20 16:27