

CVE-2023-24932(セキュア ブートのセキュリティ機能のバイパスの脆弱性)の対応後、従来の Windows メディアから起動できなくなる場合の対処について

2024 年 9 月 17 日

当社の製品をご使用いただき、誠にありがとうございます。

セキュアブート保護が有効なマシンで、Windows インストールメディアやリカバリメディア(以降、Windows メディア¹)から起動できない場合があります。これにより、再インストールやリカバリ作業が中断される可能性があります。

本書では、このような現象が発生した場合に、Windows メディアから一時的に起動し、必要な作業を行うための手順についてご案内いたします。

1. 問題の現象と環境

● 現象

CVE-2023-24932(セキュア ブートのセキュリティ機能のバイパスの脆弱性)の対応のため、KB5025885²を適用して UEFI 禁止リスト(DBX)を有効にすると、下記の現象が発生します。

- ◇ これまで起動できていた、従来の Windows メディアから起動できない
- ◇ KB5025885² 適用以前のイメージを使って、リカバリ または 再インストールした OS から起動できない

● 環境

下記の 2 つの条件を満たす物理マシンまたは仮想マシン

- ◇ 2024 年 4 月 9 日以降にリリースされた Windows セキュリティ更新プログラムを適用
- ◇ KB5025885² の手順に従って UEFI 禁止リスト(DBX)を有効化

● 対象

機種	PRIMERGY PRIMEQUEST
OS	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows Server 2012 R2/Windows Server 2012 Azure Stack HCI

¹ 富士通から購入したインストール DVD メディアや Microsoft から購入したインストールメディアなどを指します。

² KB5025885 については、<https://support.microsoft.com/ja-jp/topic/5025885> をご参照ください。

2. 問題発生後の復旧方法

従来の Windows メディアから起動するためには、セキュアブートを一時的に無効にしてください。セキュアブート有効の状態では起動すると図 1 のようにメッセージが表示され、起動できません。



図 1 RX2540 M5 の場合のメッセージ

KB5025885²の手順に従って UEFI 禁止リスト(DBX)を有効にした後に、バックアップイメージを取得している場合と取得していない場合で、復旧方法が異なります。

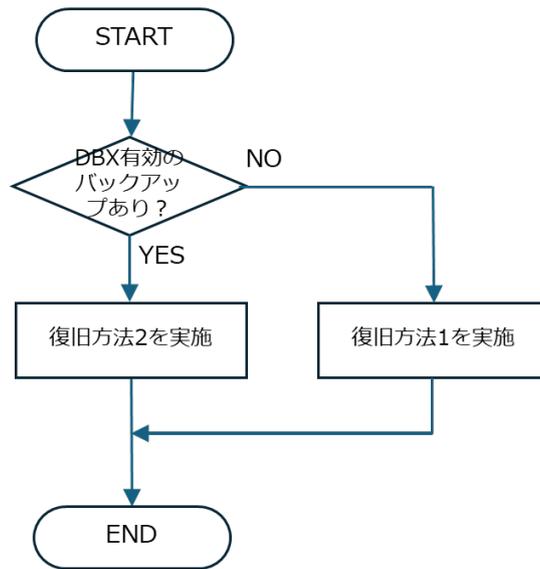


図 2 復旧方法の違い

2.1 復旧方法 1

1. UEFI 禁止リスト(DBX)を工場出荷時の状態に戻します。

図 3 のタイミングで F2 キーを押下し、BIOS 画面より工場出荷時の状態に戻します(図 4)。

各マシンの BIOS 操作方法については別途マニュアルをご確認ください³。



図 3 RX2540 M5 の場合の F2 キー押下時の画面

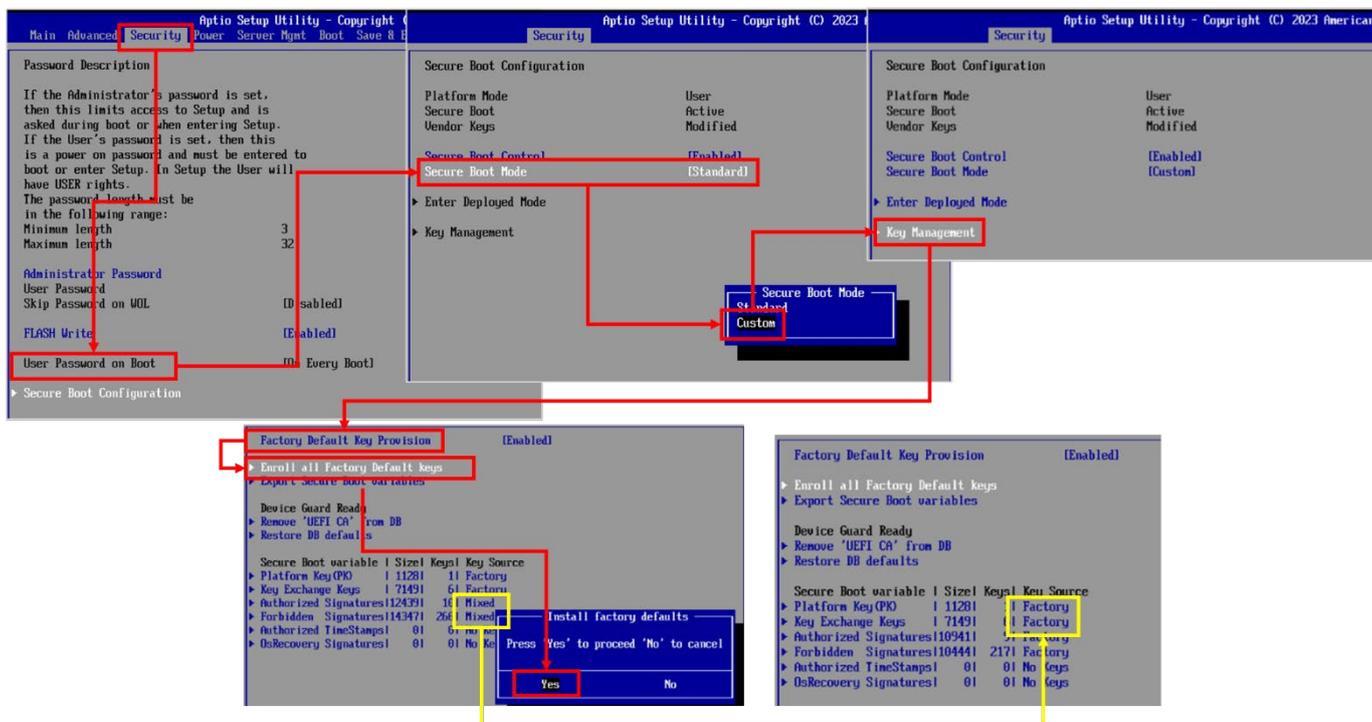


図 4 RX2540 M5 の「工場出荷時への復元」

³ PRIMERGY のマニュアルは以下よりマシン毎の「BIOS セットアップユーティリティ リファレンスマニュアル」を参照ください。

<https://www.fujitsu.com/jp/products/computing/servers/primergy/manual/>

PRIMEQUEST のマニュアルは以下を参照ください。

<https://www.fujitsu.com/jp/products/computing/servers/primequest/products/4000/catalog/>

<https://www.fujitsu.com/jp/products/computing/servers/primequest/products/3000/catalog/>

<https://www.fujitsu.com/jp/products/computing/servers/primequest/products/2000/catalog/manual/2000/index.html>

2. セキュアブートを無効にします。

図 5 のように BIOS 画面でセキュアブートを無効にします。
BIOS 操作方法については別途マニュアルをご確認ください³。

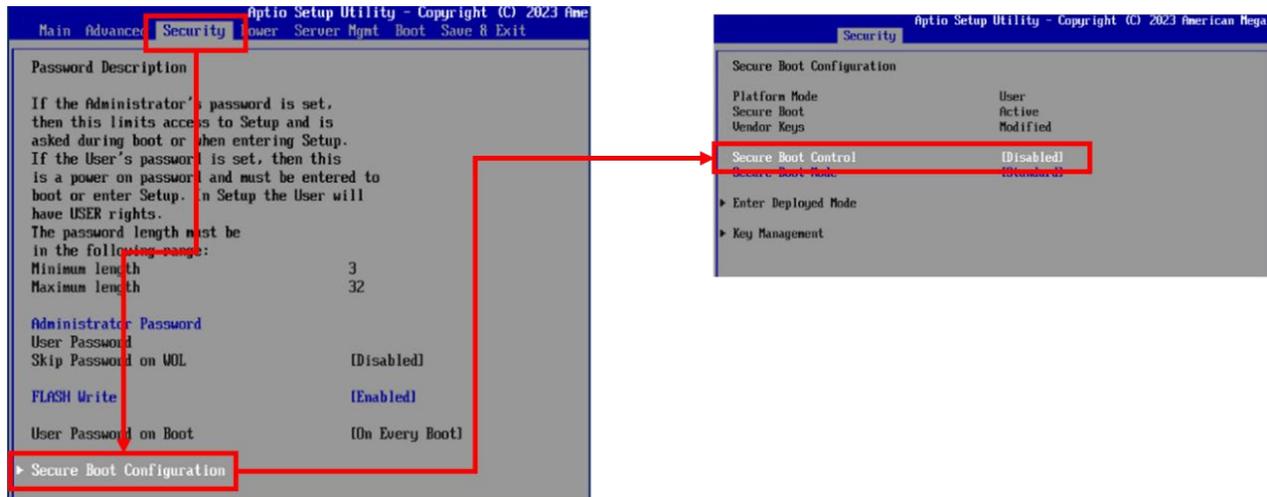


図 5 RX2540 M5 の「セキュアブート保護の無効」

3. 従来の Windows メディアで起動し、OS の再インストールをします。または、リカバリをします。

4. 3.にて OS が起動できていることを確認し、OS を再起動します。

5. 図 3 のタイミングで F2 キーを押下し、BIOS 画面でセキュアブートを再度有効にします。

6. 2024 年 4 月 9 日以降にリリースされた更新プログラムがインストールされていない場合は、インストールします。

7. 管理者コマンドプロンプトを起動し、以下のコマンドを実行した後、OS を 2 回再起動します⁴。

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Secureboot /v AvailableUpdates /t REG_DWORD /d 0x40 /f
```

8. 管理者コマンドプロンプトを起動し、以下のコマンドを実行した後、OS を 2 回再起動します⁴。

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Secureboot /v AvailableUpdates /t REG_DWORD /d 0x100 /f
```

9. 管理者コマンドプロンプトを起動し、以下のコマンドを実行した後、OS を 2 回再起動します⁴。

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Secureboot /v AvailableUpdates /t REG_DWORD /d 0x80 /f
```

⁴ 反映確認方法は、以下のマイクロソフトのサイトを参照してください。

[軽減策の展開ガイドライン](#)

2.2 復旧方法 2

1. セキュアブートを無効にします。
[図 5](#) のように BIOS 画面でセキュアブートを無効にします。
BIOS 操作方法については別途マニュアルをご確認ください³。
2. 従来の Windows メディアで起動します。
UEFI 禁止リスト(DBX)を有効にした後に取得したバックアップイメージを使ってリカバリをします。
3. 2.にて OS が起動できていることを確認し、OS を再起動します。
4. [図 3](#) のタイミングで F2 キーを押下し、BIOS 画面でセキュアブートを再度有効にします。

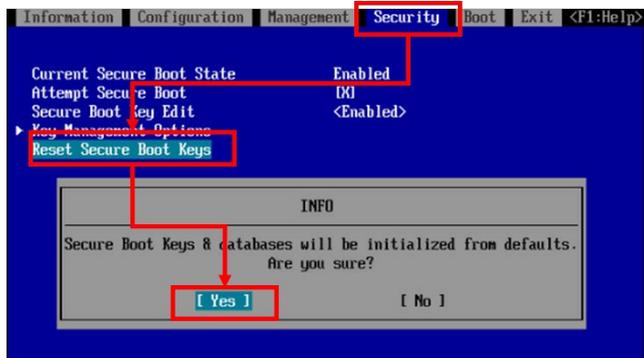
3. その他 参考情報

マシンによって BIOS 画面が異なります。図 3、図 4、および図 5 に関して RX2540 M7 の画面イメージを紹介します。

RX2540 M7 の F2 キー押下時の画面



RX2540 M7 の「工場出荷時への復元」



RX2540 M7 の「セキュアブート保護の無効」

