マザーボード
マザーボードのTPM 2.0（Firmware TPM）を有効にする方法（AMD CPU用MSI製マザーボード）

TPM 2.0（Firmware TPM）を使用するためには、UEFI（BIOS）設定画面にてFirmware TPMを有効にする必要があります。

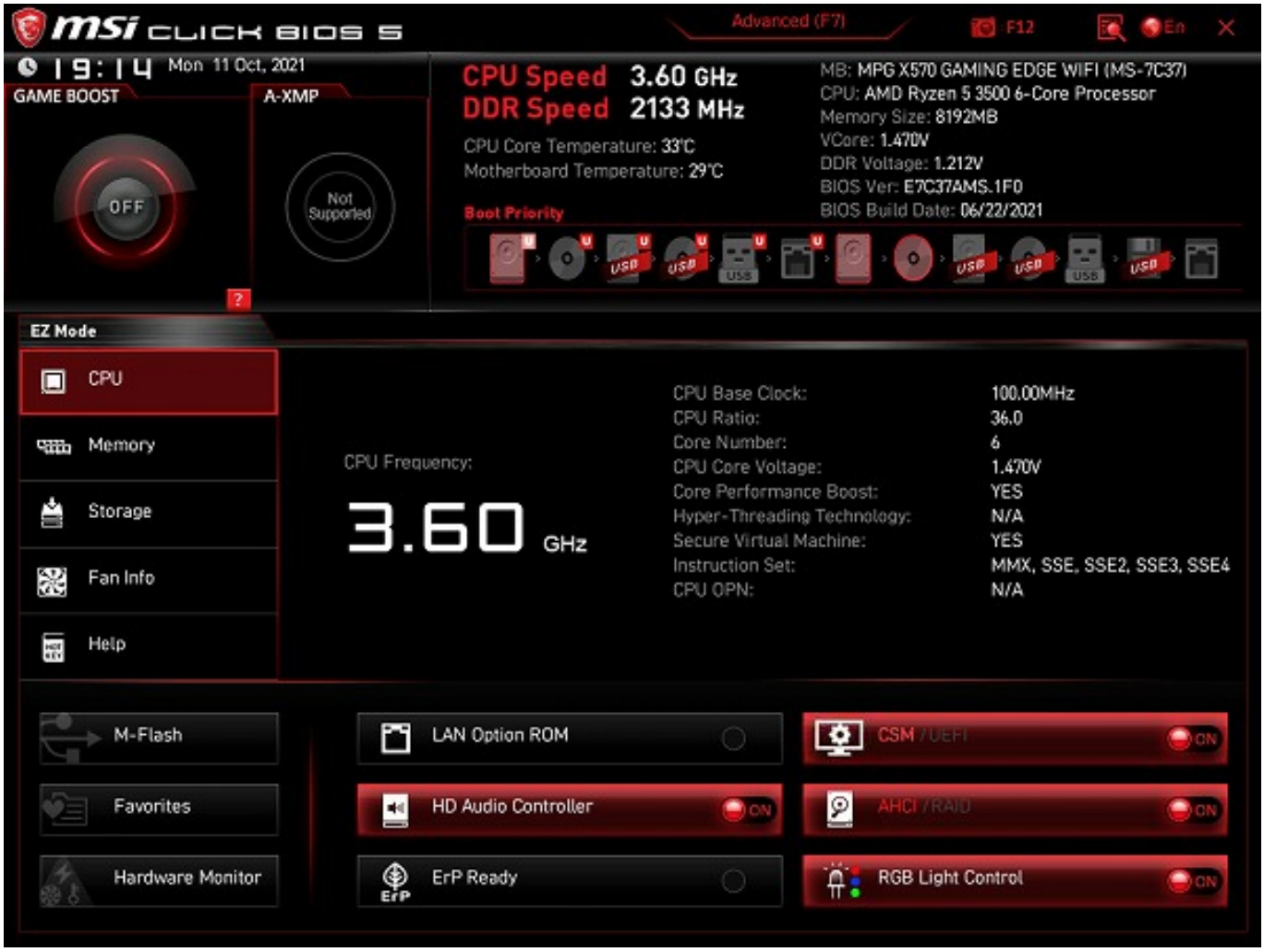
【注意】
※一般にAMD CPU対応マザーボードではRyzenプロセッサー対応マザーボードで、TPM 2.0(Trusted Platform Module 2.0)が有効にできるマザーボードがあります。TPM 2.0を有効にできるかどうかはマザーボードによって異なり、マザーボードによっては有効にできない製品もあります。そのため、すべてのマザーボードで有効にできるとは限りません。
※MSI製マザーボードではほとんどのRyzenプロセッサー対応マザーボードで有効にできます。

こちらではMSIのマザーボードでTPM 2.0（Firmware TPM）を有効にする方法をご案内いたします。

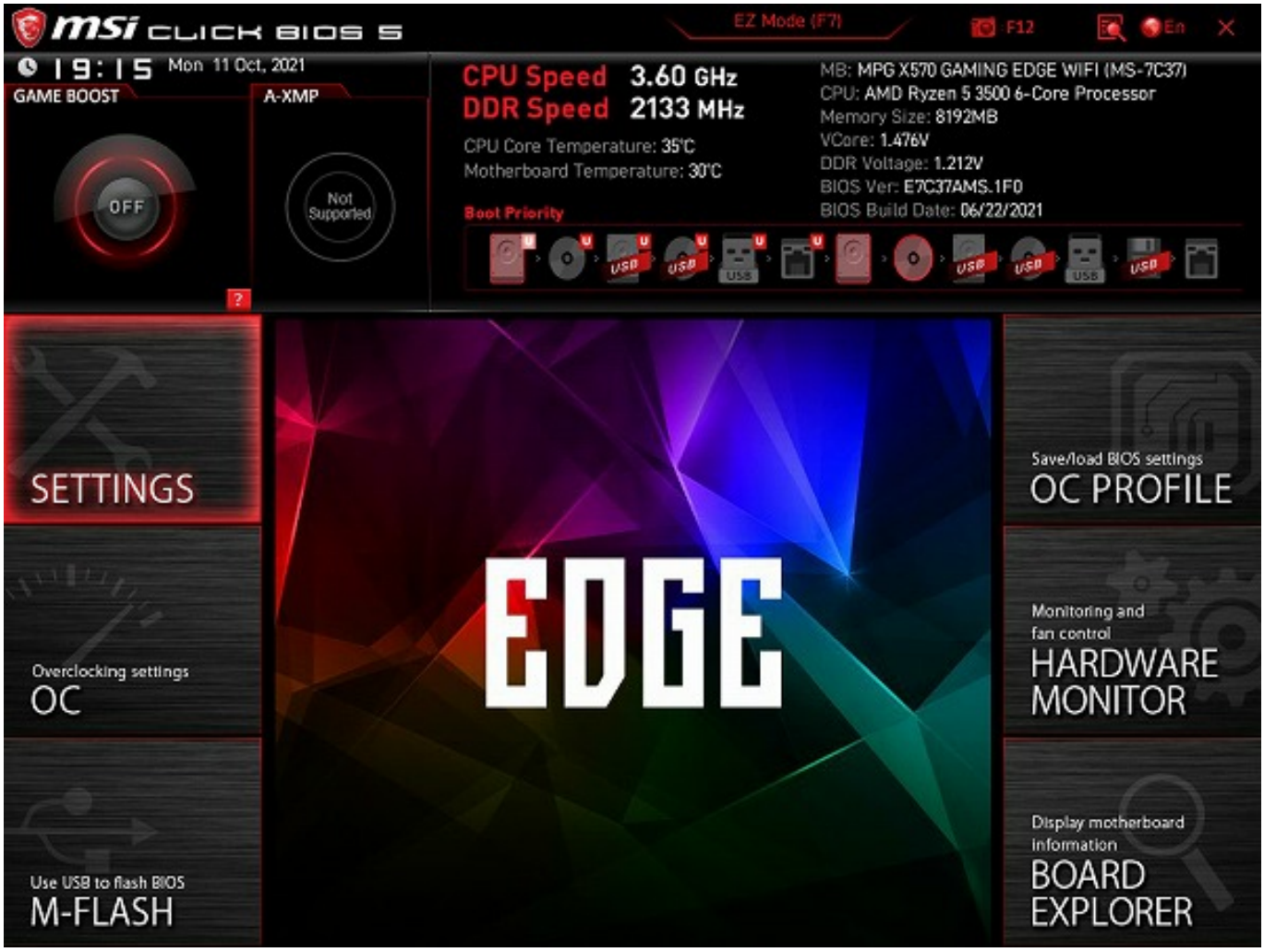
1. パソコンの電源ボタンを押して電源を入れたら、即座に[Del]キーを連打します。メーカーロゴ画面が消えたら押すのを止めます。

2. UEFI（BIOS）設定画面が表示されたら、[F7]キーを押下し[Advanced Mode]に切り替えます。

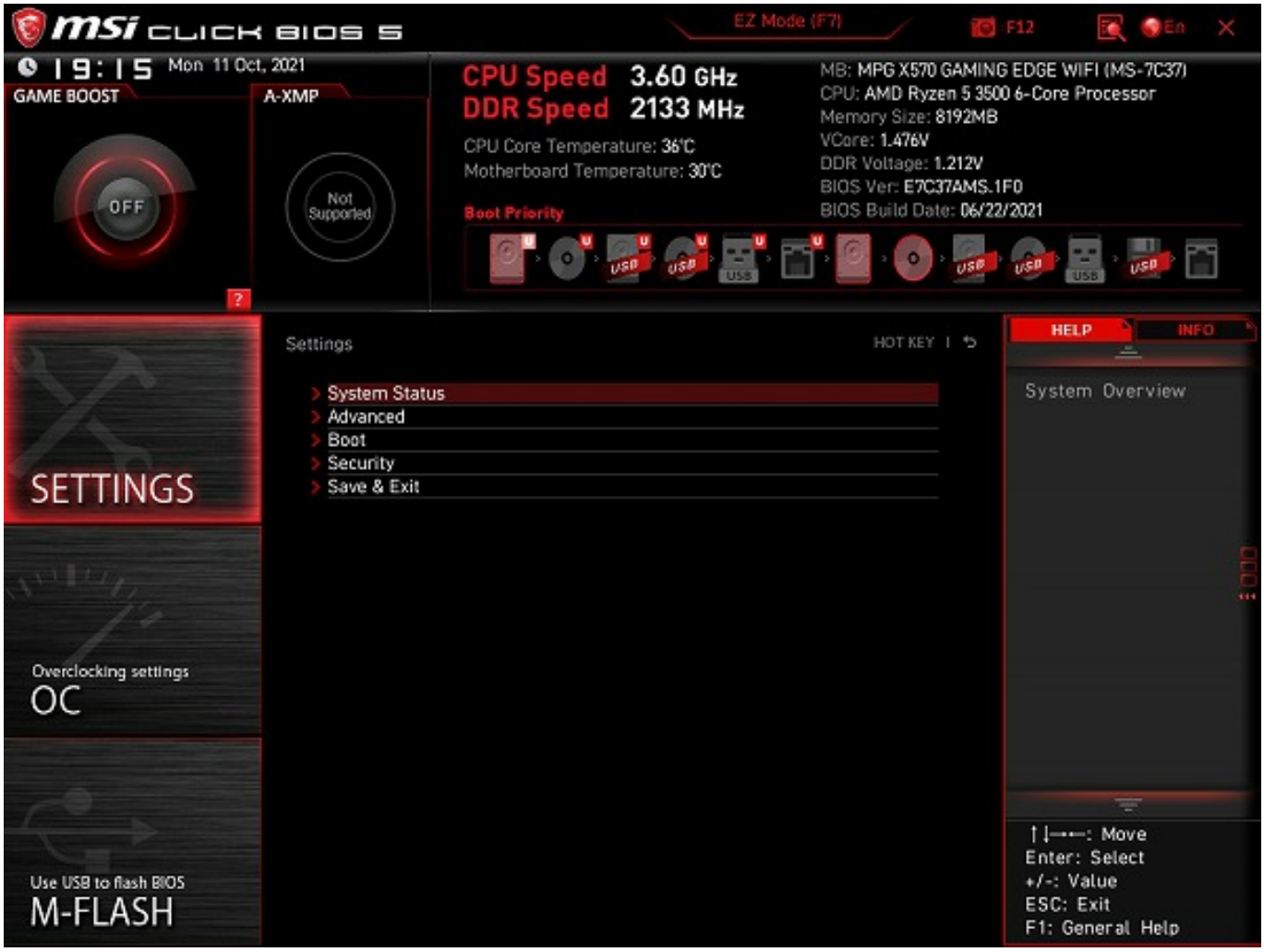
マザーボード



3. 画面が切り替わったら、左側メニューの[SETTINGS]をクリックします。

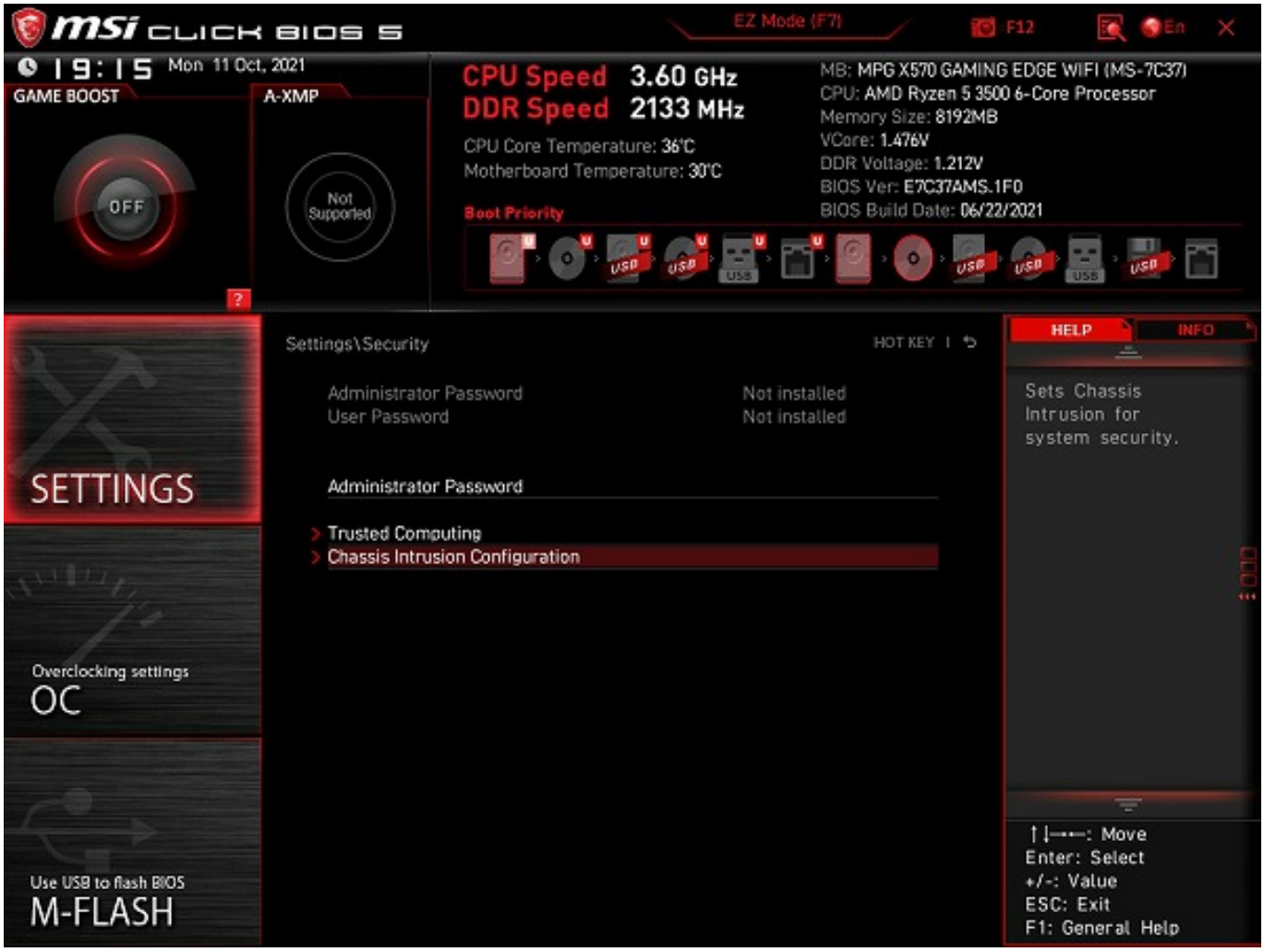


4. 画面が切り替わったら、中央メニューの[Security]をクリックします。



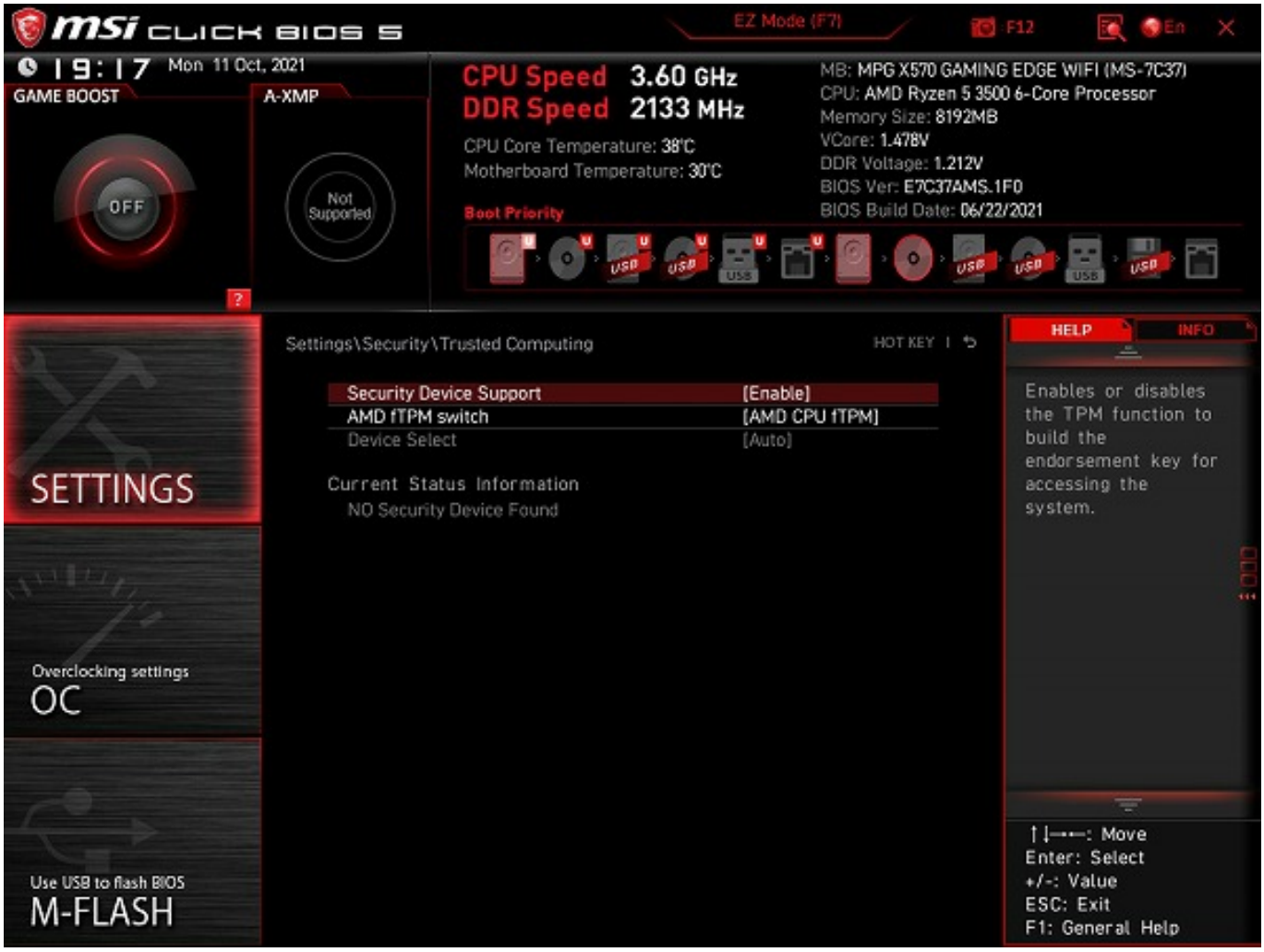
5. Securityの設定画面にて[Trusted Computing]をクリックします。

マザーボード



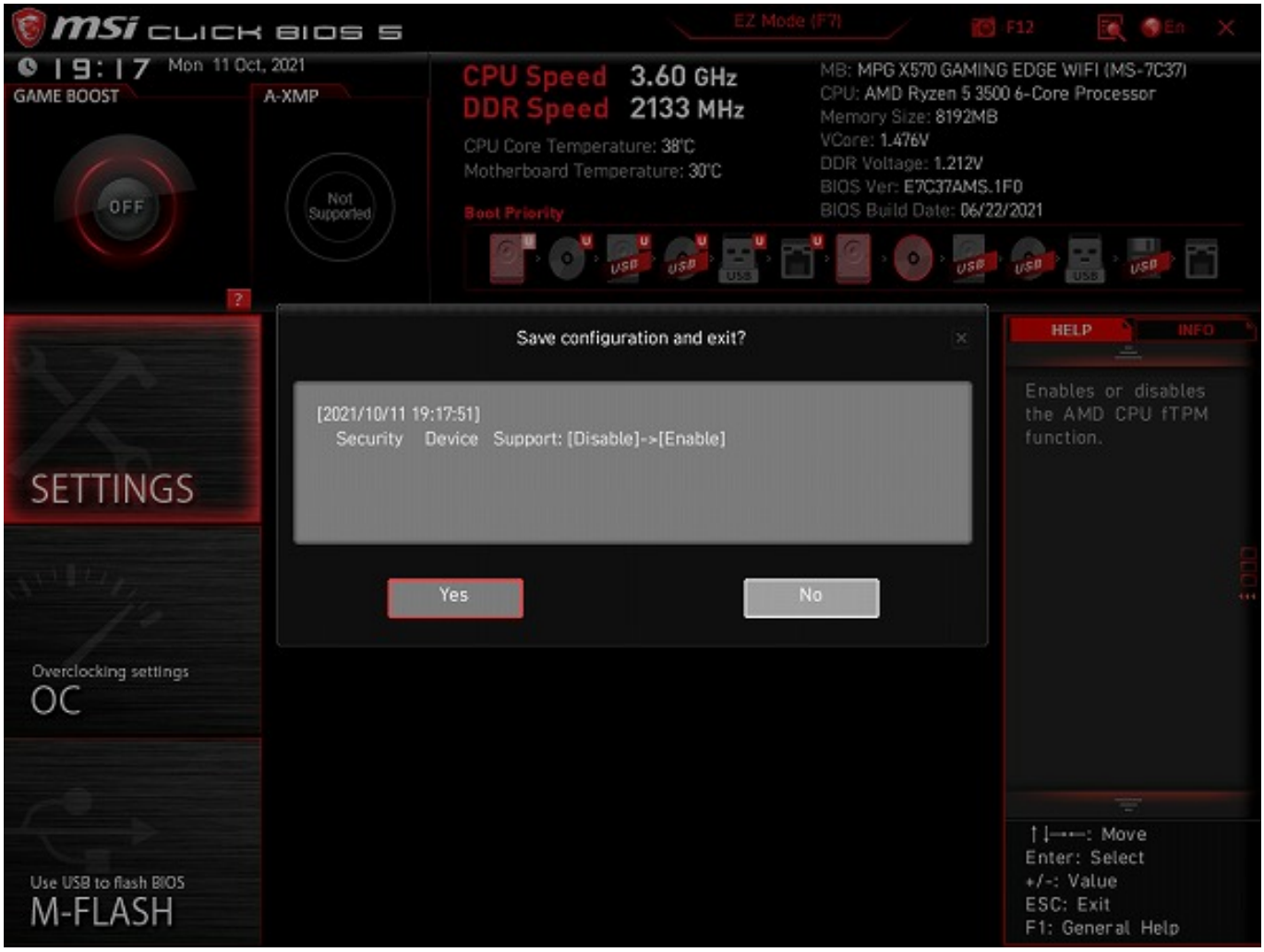
6. Trusted Computingの設定画面にて[Security Device Support]の項目の[Disabled]をクリックして、[Enabled]へ変更します。

更に[AMD fTPM switch]の項目が[AMD CPU fTPM]になっていなければ、[AMD CPU fTPM]へ変更します。



6. [F10]キーを押下して、[Yes]をクリックします。これで設定を保存してUEFI（BIOS）設定画面を終了します。

マザーボード



※画像はMSI MPG X570 GAMING EDGE WIFIのものを使用しています。マザーボードの世代やシリーズの違いにより細部のデザイン等が異なる場合がございます。

※本記事作成時点（2021年10月現在）の情報に基づく記事となります。MSI社でのUEFIの仕様変更などによりこちらの手順通り設定できなくなる場合がございますので、あらかじめご了承ください。

一意的なソリューション ID: #1351
製作者: s.suzuki
最終更新: 2021-10-11 20:01