Windows11Home の BitLocker をオフにする

パソ救・勉強会 2023(R5).3.26

~~2023.1.11~~ 2023.3.19 T.Ogawa

1. Windows11 への CPU 条件はセキュリティ部品への条件だった

Windows10 から Windows11 への「CPU 条件」は、CPU ではなかった。

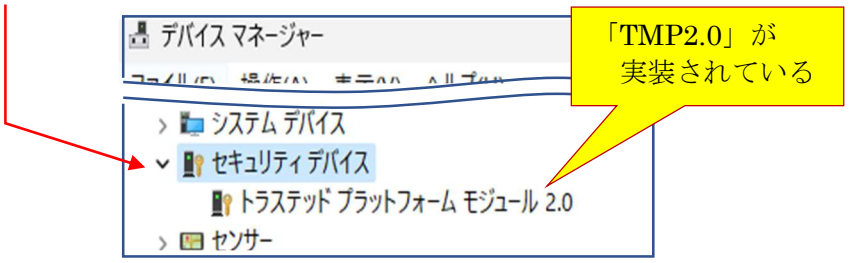
① Intel CPU は「Intel Core」8 世代（i3-8300、i5-8500、i7-8700 等）以降の CPU
② AMD CPU は「Zn1」以降の CPU

①、②の CPU を持つ PC は最新のセキュリティ部品（TMP2.0）を持つから

2. TMP2.0 の実装を確認する手順

Windows PC に実装されている TPM の種類は次の手順で確認できる。

【手順】①「スタート」→「Windows ツール」→「コントロールパネル」
→「デバイスマネージャー」で「デバイスマネージャー」画面を表示
②「セキュリティデバイス」をダブルクリックして開く



3. TMP はセキュリティ部品であり TPM1.2 と TPM2.0 がある

TPM (※1) には旧仕様の TPM1.2(※2)と新仕様の TPM2.0 (※3) があり、
Windows 11 ではハッカーからの攻撃に強いセキュリティレベルの高い TMP2.0 を求めている。

（※１）TPM（Trusted Platform Module は「信頼性の基盤になる半導体部品」を意味している。言い換えると『セキュリティ関連の暗号プロセッサ』である。

（※２）「TPM1.2」は Vista（2006）以降の Windows PC に組み込まれた「データ保護」を目的にした機能部品である。

- TPM1.2 は 1 階層（暗号化キー関連機能）だけの半導体部品である。
- 暗号キーをメモリのファームウエアに持つので外部からの攻撃に弱い。

（※３）TPM2.0 は 2019 年以降の Windows PC に組み込まれた「データ保護」と「不正アクセス防御」を目的にした機能部品である。

- TPM2.0 は 3 階層（暗号化キー生成、暗号化キー保存、プライバシー保護、UEFI 関連）の半導体部品である。 ￥
- 暗号キーをハードウェア（TPM）内に持つので外部からの攻撃に強い。TPM2.0 は不正アクセス防止機能その他が追加されている。

4. BitLocker（ビットロッカー）とは

BitLocker は前記のセキュリティ部品（TMP1.2／TMP2.0）を用いて、HDD／SSD 内のデータを暗号化 ／複合化する機能であり、データが漏洩することを防ぐセキュリティ機能である。

BitLocker は Vista 以降の PC に搭載されたデータ保護機能であり、下表に示すように Windows の上位エディション（**Pro**、**Enterprise**、**Education**）に対応する。

4.1. メーカ製 Windows 11 Home 搭載 PC は BitLocker が『オン』

PC メーカ製の Windows 11 搭載 PC は、次表に示すように「**Home**」エディションが『**オン**』になっている。

バージョン	BitLocker に対応する上位エディション			
Windows Vista	—	Professional	Enterprise	Ultimate
Windows 7	—	Professional	Enterprise	
Windows 8／8.1	—	Pro	Enterprise	
Windows 10	—	Pro	Enterprise	Education
Windows 11	Home（重要）	Pro	Enterprise	Education

（重要）PC メーカ製の Windows 11 搭載 PC は、
最下位の「**Home**」エディションでも BitLocker が『**オン**』になっている。

BitLocker の『オン』／『オフ』

【手順】 「設定」→「プライバシーとセキュリティ」→「デバイスの暗号化」

（追記）上図は 2021 年 1 月に筆者が購入した「Dell 社製の Windows 11 Home 搭載 PC」の画像であり、
今回この資料の執筆時に BitLocker が有効化されていることを知った。

4.2. 個人使用の PC で BitLocker は必要か（私見）

PC に興味がある皆さんは『ランサムウェア』という言葉を聞いたことがありますね。

ランサムウェアは、コンピュータをロックしたり、ファイルを暗号化したりして使用不能にした後、復元のみ返りに「身代金」を要求するマルウェア（悪意のあるソフト）です。

BitLocker は、PC 内臓のハードウェア（TPM）を用いて HDD／SSD 内のデータを暗号化／複合化することでランサムウェア、の攻撃を防御する機能であり、「Pro」等の上位エディションで利用されている。

【 欠点 】起動しなくなった PC をセーフモードで起動しようとした場合、ドライブが暗号化されていると BitLocker 回復キーの入力を求められる。
https://pc.watch.impress.co.jp/docs/column/win11tec/1406634.html

このことから、消費者（一般ユーザ）が使用する「Windows 11 Home」エディションではランサムウェアの攻撃対象になり得ず不要な機能と考えている。

5. BitLocker の無効果

4.1 項（メーカ製 Windows 11 Home 搭載 PC は BitLocker が『オン』）で述べたとおり、PC メーカ製の Windows 11 搭載 PC は『Home』でも、BitLocker が『オン』になっている。

ここでは、消費者に不要で技術知識が必要な BitLocker を『オフ』にする手順を説明する。

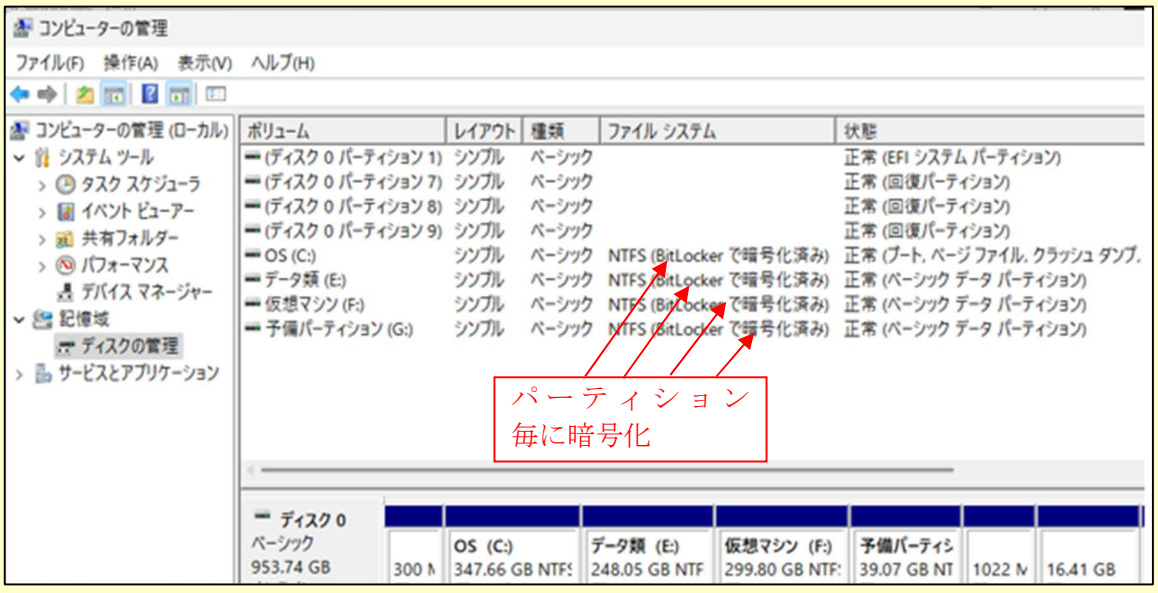
5.1. パーティション分割した SSD の BitLocker の確認

ユーザの多くは大容量の SSD でも間仕切り（パーティション分割）することなく、PC 購入時のまま、OS（C:）パーティションを使用していると思う。

筆者は 1TB（1000GB）の SSD を用途別にパーティション分割（小部屋に間仕切）して、OS（C:）、データ類（E:）、仮想マシン（F:）、予備（G:）の小部屋として使用している。

BitLocker「オン／オフ」の見方　・・・　方法 1

【手順】［Windows ツール］→［コントロールパネル］→［コンピュータの管理］



BitLocker「オン／オフ」の見方　・・・　方法２

【手順】　［設定］→［ストレージ］→［ストレージの詳細設定］
→［他のドライブで使用済みストレージ］

5.2.　BitLocker をオフにする

Windows 11 Home を搭載 CP は個人ユーザをターゲットにした PC である。
そのため「Home」エディション搭載 PC をロックしても、満足のいく身代金を得られないのでランサムウェアとしてのビジネスは成り立たない。

このためホームユーザ前提の Windows 11 Home への BitLocker の搭載は無用の長物と断言する。

ホームユーザは、ランサムウェア（身代金要求ウィルス）の攻撃に対して、攻撃者が要求する満足な身代金を支払わない／支払えないからである。

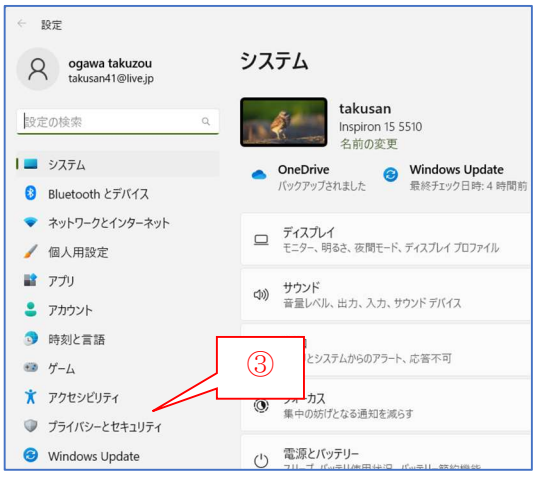
ここでは、Windows 11 Home 搭載 PC で設定されている「BitLocker」を「オフ」にする手順を説明する。

【手順】

1　タスクバーの〔検索窓〕に「設定アプリ」と入力し［設定アプリ］を検索する

2　［ 設定アプリ］をクリックして、
設定の［システム］画面を表示する

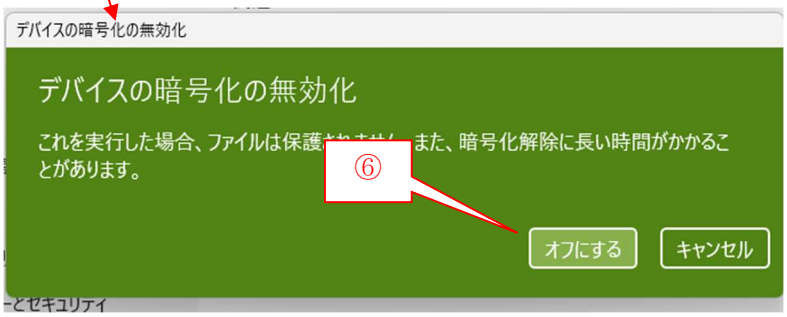
3　左ペインの［プライバシーとセキュリティ］をクリックして、
設定の［プライバシーとセキュリティ］画面を表示する

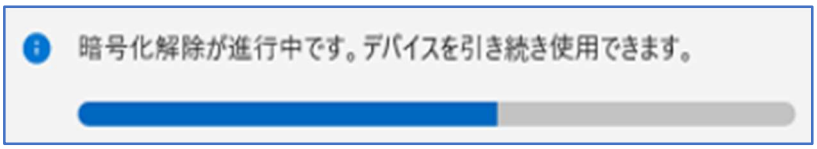


4 ［ デバイスの暗号化］右の ❯ をクリックして、
［セキュリティとデバイス ❯ デバイスの暗号化］画面を表示する

5 ［デバイスの暗号化］右の［ オン］をクリックすると、スイッチが［ オフ］に変化すると共に、「デバイスの暗号化の無効化］ポップアップウィンドウを表示する

6 ［オフにする］をクリックして『デバイスの暗号化を無効化する』を実行する





【重要】暗号化の解除は、バックグラウンドで実行されるので、無効化の途中でも PC を利用できる。

お疲れさまでした ！