

シニアのためのパソコン&スマホ広場(その 156)

「Bitlocker」が「回復キー」を求めてくるケースと「回復キー」の入手方法

個人で使用するパソコンで、紛失や盗難にあうリスクが低く、パソコンに保存しているデータも、それ程重要性が無いと判断した場合、「Bitlocker」機能を「無効」にするのがお勧めですが、使用するパソコンが、個人情報や“機密性が高い情報”を扱う場合、「Bitlocker」機能を「有効」にしておくと、パソコンの紛失や盗難にあったとき“セキュリティ効果”が高まるので安心です。

但し、「Bitlocker」機能を「有効」にすると、紛失や盗難以外の以下のようなときに「回復キー」の入力を求める画面が表示されるので、事前に「回復キー」を入手しておくことが重要です。

1. 「Bitlocker」から「回復キー」の入力を求めてくるケース



① Windows Update の不具合

”Windows Update”は、OS(Windows)の安全性やパソコンの機能向上に必要ですが、更新内容によって「Bitlocker」の動作に影響を及ぼすことがあります。

約2年程前に、「脆弱性対策を含む更新プログラム」(Windows Update)によって「Bitlocker」が誤作動し、突然、「回復キー」入力を求められるというトラブルが発生したことにより多くのユーザが混乱させられた事例がありました。



② 不正アクセスの検知

Windowsログイン時に、パスワードの”入力ミス”を何度も繰り返した場合、「Bitlocker」は不正アクセスの可能性があると判断して、「回復キー」の入力を求めてくる場合があります。



③ パソコンの初期設定

Windows11 のバージョン「24H2」以降のパソコンを購入すると、「Bitlocker」が自動的に「有効」設定されているメーカーや機種があります。

自動的に「有効」設定されているパソコンを「マイクロソフトアカウント」でログインする場合、「回復キー」は「マイクロソフトアカウント」に保存されるので、自分のパソコンに「Bitlocker」機能が働いてデータが暗号化されていることを知らずに使用しているユーザが多く居ます。



また、企業向けに出荷されたパソコンが、リース切れ等により中古パソコンとして販売されている機種を購入した場合、「Bitlocker」が有効化されていることがあるので、その状態で Windows Update や設定変更を行うと、「Bitlocker」が異常と判断し、突然「回復キー」の入力を求める場合があります。

そのため、自分が使用するパソコンの「Bitlocker」機能が「有効」になっているのか「無効」なのかの確認を「パソコン & スマホ広場(その155)」の1項の操作手順により確認し、必要な対処をしてください。

④ BIOS・UEFIの更新・変更

BIOSやUEFIは、システム起動時にハードウェアを制御する裏方で働く重要なプログラムです

が、その構成が変わると、「Bitlocker」は「システムが改ざんされた可能性がある」と判断して、安全性を確認するために「回復キー」の入力を求めてくることがあります。

⑤ ハードウェアの変更(交換修理)・ファームウェアの変更

補助記憶装置の“SSD”や“HDD”、“メモリ”、“マザーボード(基盤)”などのハードウェアを交換して“システム構成の変更”を行うと、「Bitlocker」はセキュリティリスクとみなあして、「回復キー」の入力を求めてくることがあります。

特に、パソコンの「マザーボード(基盤)」交換修理は TPM(セキュリティチップ)の識別情報が変わるため、「回復キー」の入力要求が発生する可能性が高いです。



⑥ 「電源」ボタンの長押しによる強制切断

「電源」ボタンの長押しによるパソコンの“強制切断”をすると様々な致命的なトラブルを誘発しますが、その中の一例として次回電源を入れたときに、不正アクセスの可能性があると判断して、「回復キー」の入力を求めるケースが多々あります。



2. 「回復キー」の入手手順

購入時から「Bitlocker」機能が「有効」に設定されているパソコンを、「有効」のまま使用を続けるときは、できるだけ早く「マイクロソフトアカウント」でログインして、「回復キー」(数字48桁)を入手しておくことをお勧めします。

<手順>

- ① パソコンの型番を調べる。(例: 東芝ノートパソコン 型番 PTEX-65ABJW)
- ② ブラウザを起動して、URL欄に半角で“aka.ms/rk”と入力する。
- ③ サインイン画面が開くので、“マイクロソフトアカウント(メールアドレス)”と“PIN コード””パスキー”、“パスワード”でログインする。
- ④ マイクロソフトアカウントにログインできたら、画面左列にある「デバイス」アイコンをクリックする。
- ⑤ デバイス画面が開くので、「詳細を見る」をクリックする。
- ⑥ 開いた画面を下方にスクロールすると、「BitLocker データ保護」のところの「回復キーの管理」をクリックする。
- ⑦ マイクロソフトアカウントを使用しているパソコン(デバイス)ごとに回復キーが表示されるので該当するパソコンに該当するデバイス名とデバイスID、回復キーを印刷するか、メモする。

| デバイス名 | キー ID | 回復キー |
|---------|----------|---|
| TEX65AW | 46DC03B0 | 142362- 298925- 482823- [REDACTED] 297924- 380831- 710622 |



6桁ずつ“—”(ハイフン)で区切られた数字48桁が「回復キー」です。

田辺・西牟婁地区協議会

森田 那華雄