BitLockerの機能「デバイスの暗号化」について

本項では、掲記の機能をお使いになるうえで知っておいていただきたいことを記載しています。ご購入のパソコンをお使いになる前に本項をよくお読みになり、正しくお使いいただきますようお願い致します。

◆ご利用時の重要なお知らせ◆

ご購入のパソコンは**Windows10に搭載されている機能**により、**内蔵ストレージが暗号化**されている状態で修理を行うと**OSの起動ができなくなる可能性**があります。

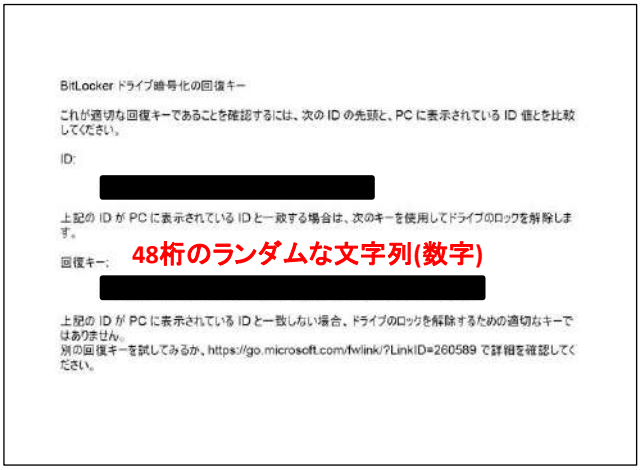
これは、修理後にパソコンを起動するときに**「回復キー」の入力**を求められる場合があり、**正しくキーを入力できないことで発生**します。

一部製品では**内蔵ストレージの暗号化が自動的に実行される**ため、次の**「デバイスの暗号化の自動実行に関する注意事項」**に記載している手順を行い、暗号化が実行されている場合は**「回復キー」を作成して紛失しないように保管**して下さい。

【回復キーメモ欄　合計48桁の文字列】

－　　－　　－　　－　　－　　－　　－

【回復キーの作成例】



次のページより、
・暗号化状態の確認
・回復キーの作成方法
について説明します。

◆デバイス暗号化の自動実行について◆

■注意事項

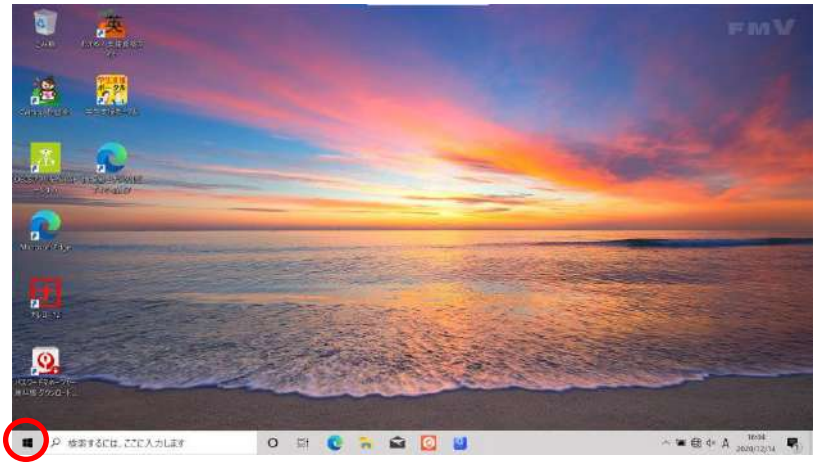
ご購入のパソコンをMicrosoftアカウントまたは、Azure Active Directoryでご利用になった場合、Windows10に搭載されている**BItLockerの機能である「デバイスの暗号化」**により内蔵ストレージが**自動的に暗号化**される場合があります。

パソコンのセットアップ完了後、次の「■暗号化状態の確認」でパソコンの内蔵ストレージが**暗号化されているか確認**してください。

該当するお客様は「■回復キーの作成」を行い、**「回復キー」を作成して紛失しないよう保管**して下さい。

■暗号化状態の確認

次の手順に従って、お使いのパソコンが暗号化されているか確認してください。
※MicrosoftアカウントやAzure Active Directoryのアカウントを利用していない場合は、自動的に暗号化されることはありません。
※画像は一例です。メーカー、モデルにより表示が異なる場合があります。



①スタートボタン
をクリックします。

②設定
をクリックします。

◆デバイス暗号化の自動実行について◆

■暗号化状態の確認(続き1)

次の手順に従って、お使いのパソコンが暗号化されているか確認してください。
※MicrosoftアカウントやAzure Active Directoryのアカウントを利用していない場合は、自動的に暗号化されることはありません。
※画像は一例です。メーカー、モデルにより表示が異なる場合があります

スクロール！！

③スクロールをして
「更新とセキュリティ」の
アイコンを探します。

④**「更新とセキュリティ」**
をクリックします。

⑤**「デバイスの暗号化」**
をクリックします。

次のページへ続く。

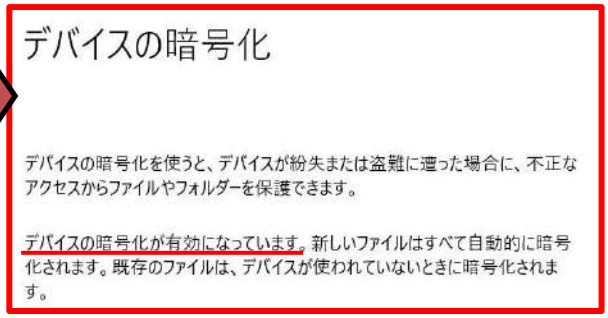
◆デバイス暗号化の自動実行について◆

■暗号化状態の確認(続き2)

次の手順に従って、お使いのパソコンが暗号化されているか確認してください。
※MicrosoftアカウントやAzure Active Directoryのアカウントを利用していない場合は、自動的に暗号化されることはありません。
※画像は一例です。メーカー、モデルにより表示が異なる場合があります

★<u>デバイス暗号化「有効」の確認</u>※Microsoftアカウントでログイン

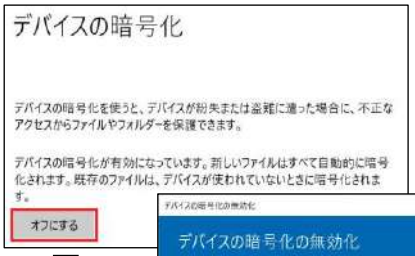
⑥デバイスの暗号化は<u>「有効」</u>



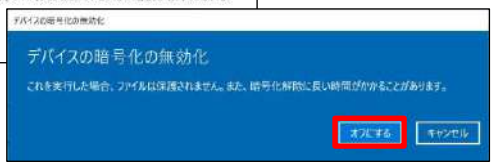
<u>**次のページでBitLocker回復キーの取得方法をご紹介します。**</u>

★<u>デバイス暗号化「無効」の確認</u>※デバイスの暗号化を「オフ」(解除)

※BitLocker回復キーの管理などは不要となりますが、セキュリティー上お勧めできません。
自己責任の下で設定を変更してください。

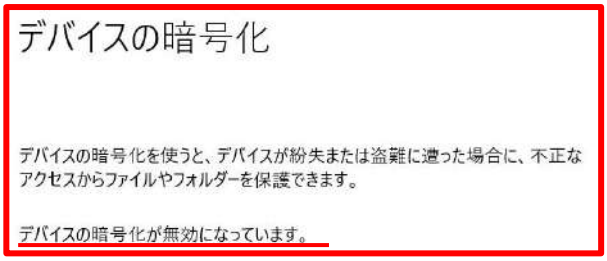


⑥´-1<u>「オフにする」</u>ボタンをクリック



⑥´-2<u>「オフにする」</u>ボタンをクリック
※オフになるまでしばらく時間がかかります

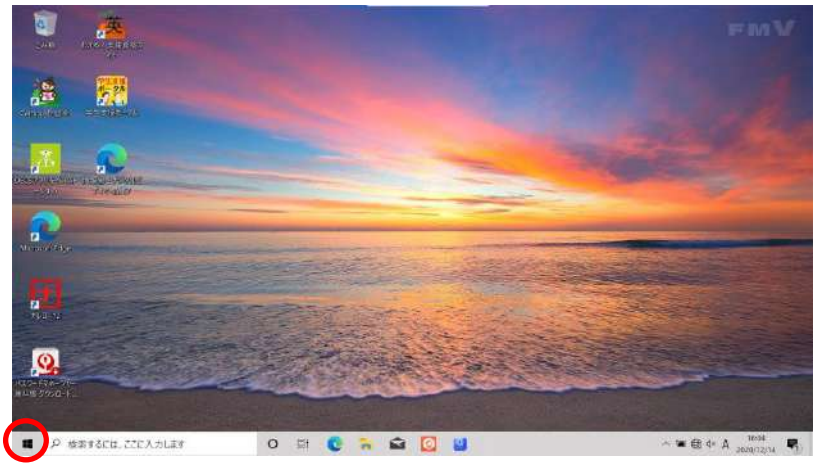
⑥´-3デバイスの暗号化は<u>「無効」</u>



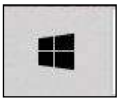
◆デバイス暗号化の自動実行について◆

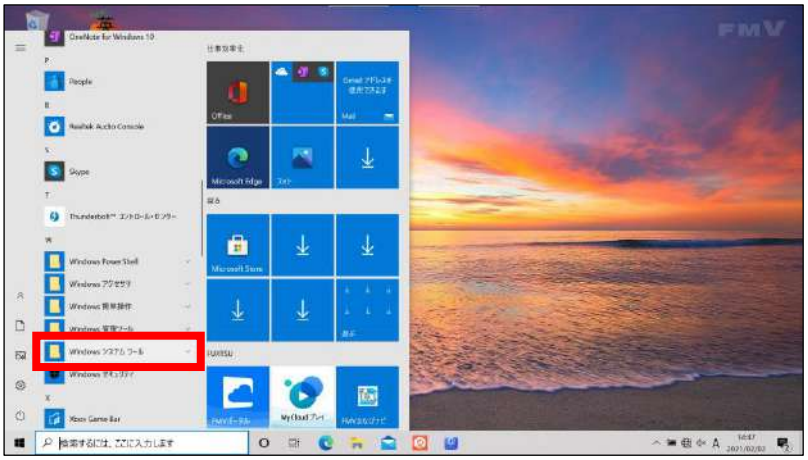
■回復キーの作成

起動できなくなった場合に備え、**必ず「回復キー」を作成**して**紛失しないよう保管**して下さい。

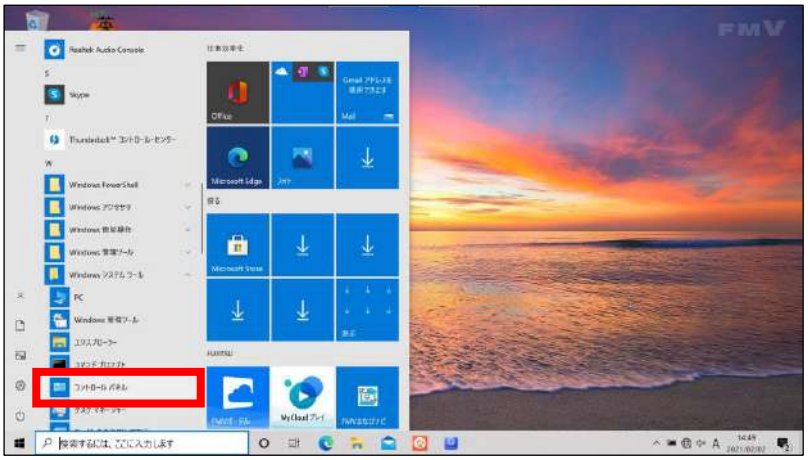


①スタートボタン
をクリックします。





②コントロールパネルを開くために Windowsシステムツール
をクリックします。

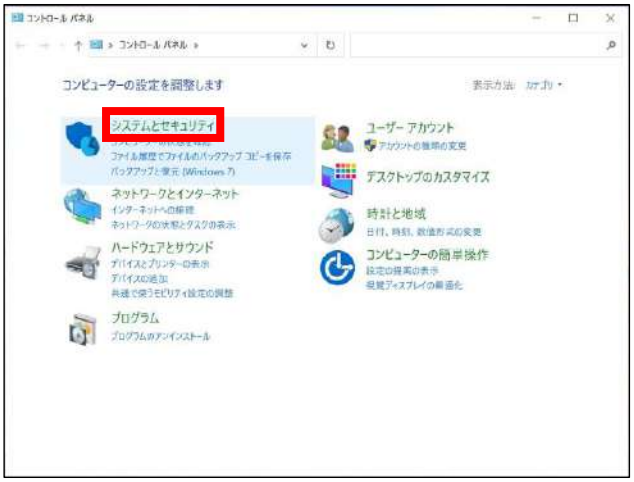


③コントロールパネルを
クリックします。

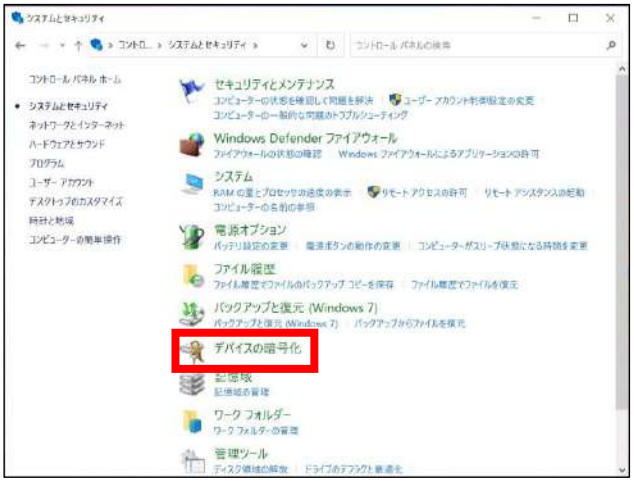
◆デバイス暗号化の自動実行について◆

■回復キーの作成(続き1)

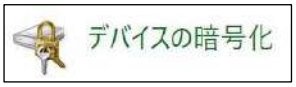
起動できなくなった場合に備え、**<u>必ず「回復キー」を作成</u>**して**<u>紛失しないよう保管</u>**して下さい。



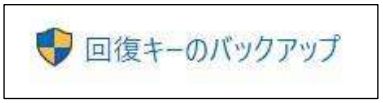
④システムとセキュリティ
をクリックします。
※緑色の文字の部分をクリックしてください。
青色の文字の部分をクリックすると別の画面に移動します。



⑤デバイスの暗号化
をクリックします。



⑥回復キーのバックアップ
をクリックします。



◆デバイス暗号化の自動実行について◆

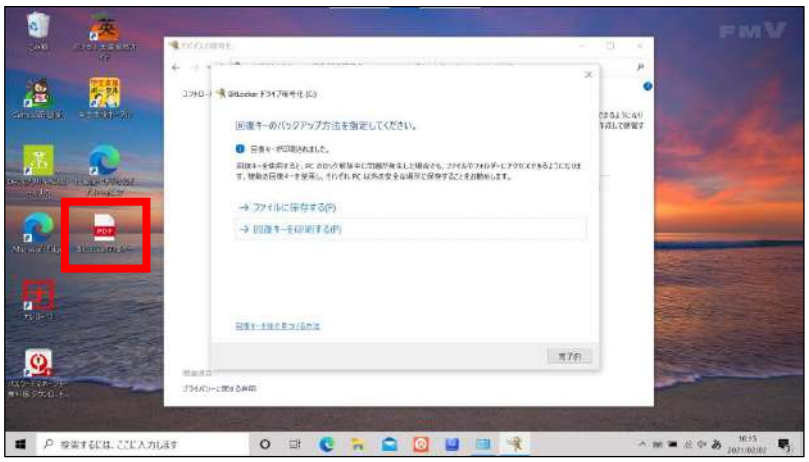
■回復キーの作成(続き1)

起動できなくなった場合に備え、**必ず「回復キー」を作成**して**紛失しないよう保管**して下さい。

⑦回復キーを印刷する(P)をクリックします。

※シンプルな手順をご案内します。「ファイルに保存する(F)」は再起動を伴うため。

⑧Microsoft Print to PDFが選択されていることを確認し、**印刷(P)**をクリックします。



⑨PDFファイルが完成していることを確認します。

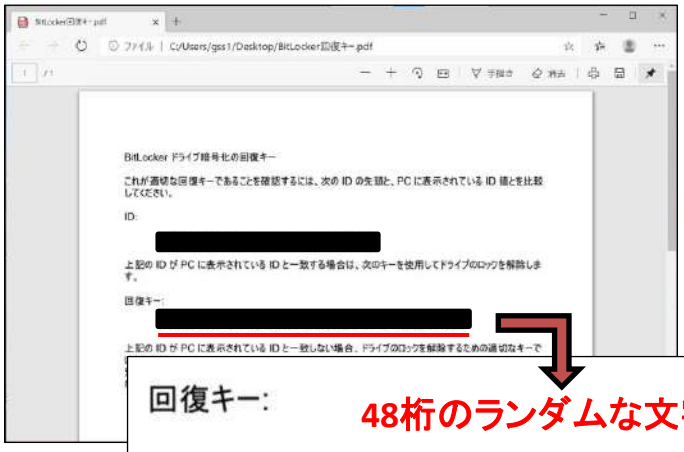
※今回はわかりやすいようにデスクトップにPDFファイルを保存しました。

任意の場所、任意のファイル名で保存してください。

◆デバイス暗号化の自動実行について◆

■回復キーの作成(続き1)

起動できなくなった場合に備え、**必ず「回復キー」を作成**して**紛失しないよう保管**して下さい。



⑩回復キーを確認し、メモを取ります。

※ID:の方をメモしないよう注意してください。IDを入力しても起動しません。

回復キー: **48桁のランダムな文字列(数字)**

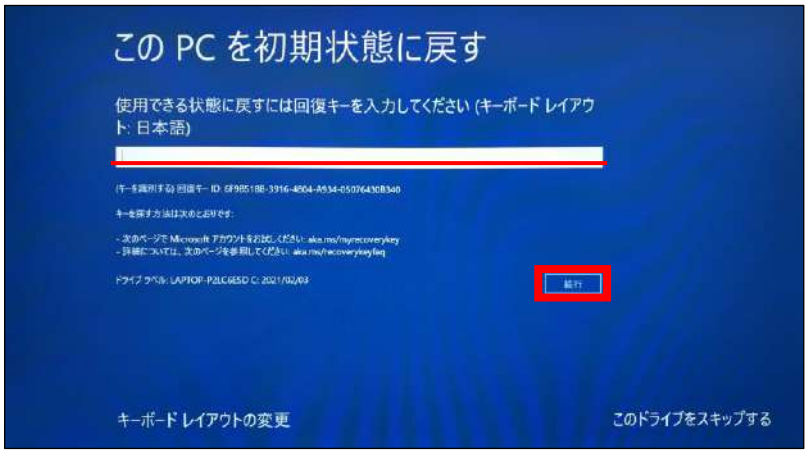
※(注)下記のキーを入力しても**起動しません！**

aaaaaa – bbbbbb – cccccc – dddddd – eeeeee – ffffff – gggggg – hhhhhh

【回復キーメモ欄　合計48桁の文字列】

– – – – – – –

パソコンを初期化したり、修理などを行ってパソコンのハードウェア情報が変わった場合、パソコン起動時に「回復キー」の入力を求められることがあります。



※左の画面はPC初期化手順でのBItLocker回復キー入力画面です。

⑪回復キー入力欄に48桁の回復キーを入力し、続行ボタンをクリックすれば初期化がスタートします。

パソコンを初期化したり、修理などを行ってパソコンのハードウェア情報が変わった場合、パソコン起動時に「回復キー」の入力を求められることがあります。

必ず「回復キー」をメモして**紛失しないよう保管**して下さい。　Fin