

パソコンを安全にご使用いただくために…

## 【BitLocker 編】

第1版（2026年3月）

ICT 推進センター

# 目次

◆	注意事項	1
1.	BitLocker とは？	1
2.	BitLocker の設定が可能なドライブの種類	2
2.1	オペレーティングシステムドライブ	2
2.2	固定データドライブ	2
	【参考】リムーバブルデータドライブ	2
3.	BitLocker の設定（有効／無効）を確認する方法	3
4.	BitLocker が有効だった場合の対応	5
4.1.	回復キーの取り扱いに関する注意事項	5
4.2.	オペレーティングシステムドライブの回復キー保存方法	5
4.3.	固定データドライブの回復キー保存方法	7
4.4.	BitLocker を無効化する方法	8
4.4.1.	オペレーティングシステムドライブの BitLocker を無効化する方法	9
4.4.2.	固定データドライブの BitLocker を無効化する方法	10
5.	BitLocker が無効だった場合の対応	11
5.1.	BitLocker の有効化に関する注意事項	11
5.2.	オペレーティングシステムドライブの BitLocker を有効化する方法	11
5.3.	固定データドライブの BitLocker を有効化する方法	14

## ◆ 注意事項

- ・ご利用の PC やバージョンによって、画面の見え方や選択肢の文言が異なる場合があります。
- ・この手順書に記載の手順と異なる表示やエラーなどご不明な点がございましたら以下お問合せ先までご連絡ください。

※本学（学部等事務室、ICT 推進センター）では回復キーの紛失や入力時のエラーについて対応することができませんので、必ず個人での管理・保管をお願いいたします。

【お問合せ先】

ICT 推進センター 学生ヘルプデスク

メール：[k-help@kitasato-u.ac.jp](mailto:k-help@kitasato-u.ac.jp)

## 1. BitLocker とは？

BitLocker（ビットロッカー）は、Windows に標準搭載されているドライブ暗号化機能です。PC のデータを守るための「鍵」のような役割で、万が一 PC を紛失したり盗まれたりした場合でも、第三者がデータを読み取ることを防ぎます。

BitLocker の設定は、Windows Update などにより自動的に有効になる場合があります。そのため、知らないうちに暗号化が有効になり、回復キーの保存が必要な状態になっていることがあります。PC から回復キーの入力を求められた際に、**事前に回復キーを保存していない場合、PC を起動することができず、PC 本体を初期化しなければならない可能性があります。（PC 本体を初期化すると、保存していたデータも削除されてしまいます。）**

**安心して PC を使い続けるために、BitLocker の状態を定期的に確認することを推奨します。**

この手順書では、BitLocker の状態（有効／無効）確認と設定方法、回復キーの保存方法について説明します。

（参考）BitLocker の回復キー入力画面



## 2. BitLocker の設定が可能なドライブの種類

### 2.1 オペレーティングシステムドライブ

オペレーティングシステムドライブとは、Windows がインストールされているドライブのことです。通常は「C ドライブ」が該当します。

- 特徴
  - ・ Windows の起動に必要なファイルが含まれる
  - ・ BitLocker を有効にすると、起動時のセキュリティが強化される

### 2.2 固定データドライブ

固定データドライブとは、PC に内蔵されている追加ストレージ（D ドライブ、E ドライブなど）のことです。

- 特徴
  - ・ データ保存用のドライブ
  - ・ オペレーティングシステムドライブとは独立して BitLocker を有効／無効にできる
  - ・ BitLocker を有効にすると、データ漏えいリスクを低減できる

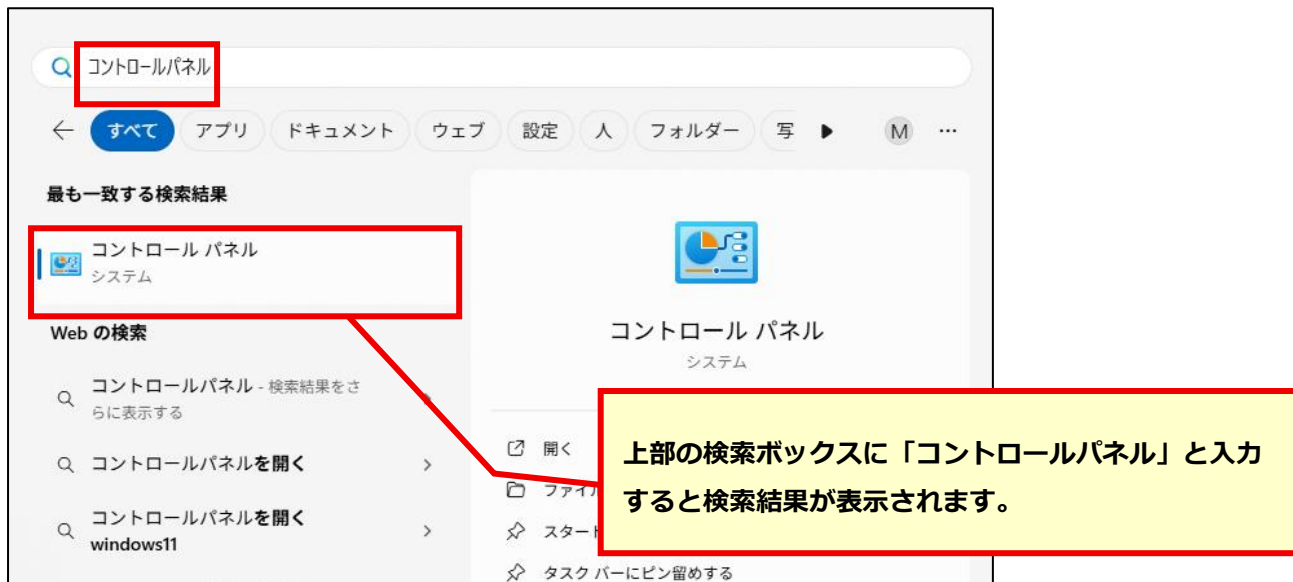
### 【参考】 リムーバブルデータドライブ

リムーバブルデータドライブとは、USB メモリや外付け HDD／SSD、SD カードなどの取り外し可能なストレージのことです。使用頻度が高い場合や外付け HDD にバックアップを保存している場合は暗号化しておくことで安心です。

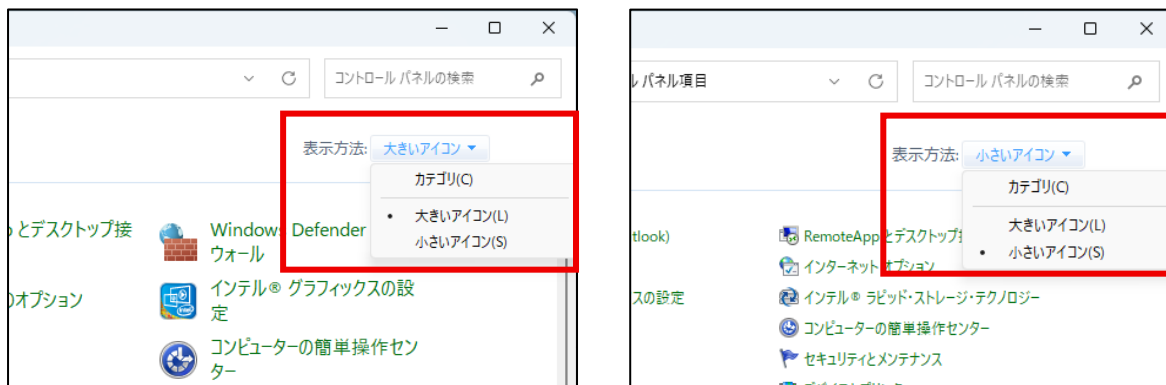
- 特徴
  - ・ オペレーティングシステムドライブとは独立して BitLocker を有効／無効にできる
  - ・ 他の PC に接続した際も保護されるため、解除キーを知らなければアクセスできない

### 3. BitLocker の設定（有効／無効）を確認する方法

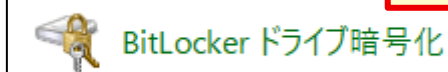
1. 画面下部のスタートボタンをクリックします。
2. 検索ボックスに「コントロールパネル」と入力し、表示された「コントロールパネル」を選択します。



3. 右上の表示方法を「大きいアイコン」または「小さいアイコン」に変更し、「BitLocker ドライブ暗号化」をクリックします。



一覧の中から「BitLocker ドライブ暗号化」をクリックします。



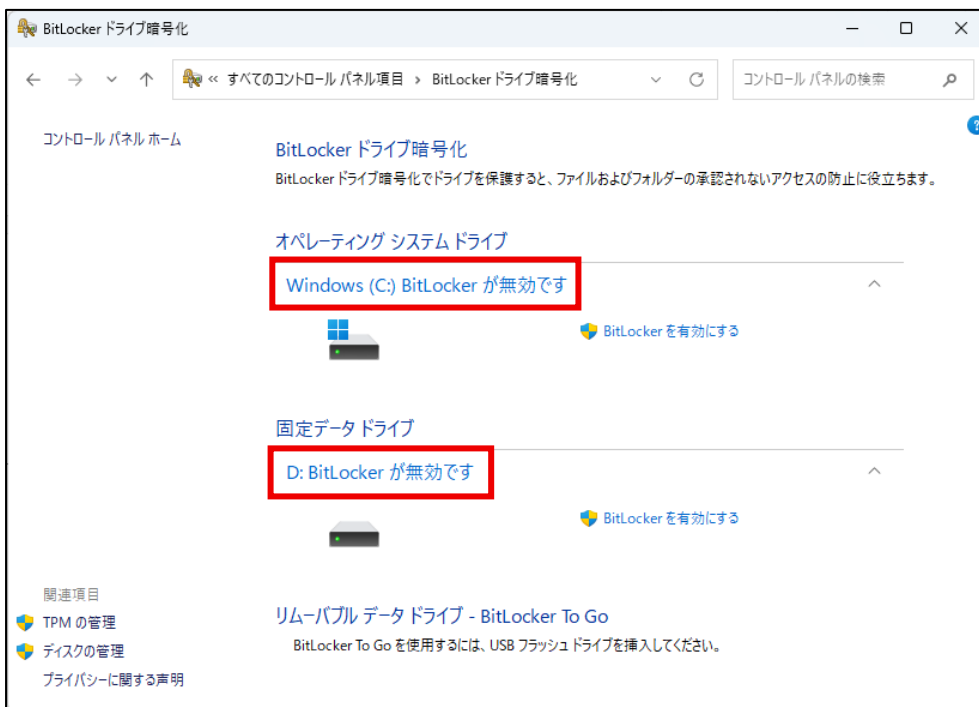
#### 4. BitLocker の設定を確認します。

※オペレーティングシステムドライブと固定データドライブのうち、一方のみが有効/無効となっている場合もあります。

##### ● BitLocker が有効（オン） の場合



##### ● BitLocker が無効（オフ） の場合



## 4. BitLocker が有効だった場合の対応

データにアクセスするための回復キーを保存する必要があります。オペレーティングシステムドライブと固定データドライブで手順はほぼ同じですが、どのドライブの回復キーかを明確に区別して保存することが重要です。

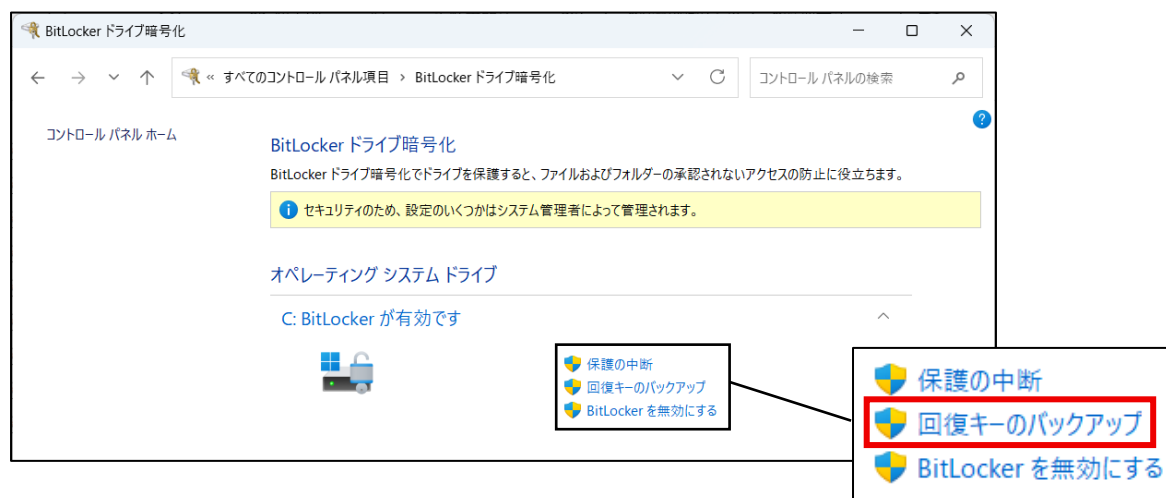
**手順 4.1.回復キーの取り扱いに関する注意事項**を確認し、以降の手順を参照して保存を行ってください。

### 4.1. 回復キーの取り扱いに関する注意事項

- 回復キーは第三者に知られないよう厳重に管理してください。
- 回復キーを紛失すると、データにアクセスできなくなる可能性があります。
- 回復キーはPC内に保存しないでください。
- 回復キーはPC以外のデバイス（USB やクラウドストレージ（Box や Google Drive など）など、ご自身がいつでも確認できる場所に保存してください。BitLocker が有効になった場合、回復キーをPC内に保存していると確認することができません。
- オペレーティングシステムドライブと固定データドライブの回復キーを混同しないよう注意してください。

### 4.2. オペレーティングシステムドライブの回復キー保存方法

1. BitLocker ドライブ暗号化のオペレーティングシステムドライブから「回復キーのバックアップ」を選択します。選択肢が表示されていない場合は、「C: BitLocker が有効です」という表示をクリックするとメニューが展開します。



2. 回復キーの保存方法を選択し、保存後に右下に表示される「完了」をクリックしてウィンドウを閉じます。(PC の設定や利用環境により、選択肢が異なる場合があります。)

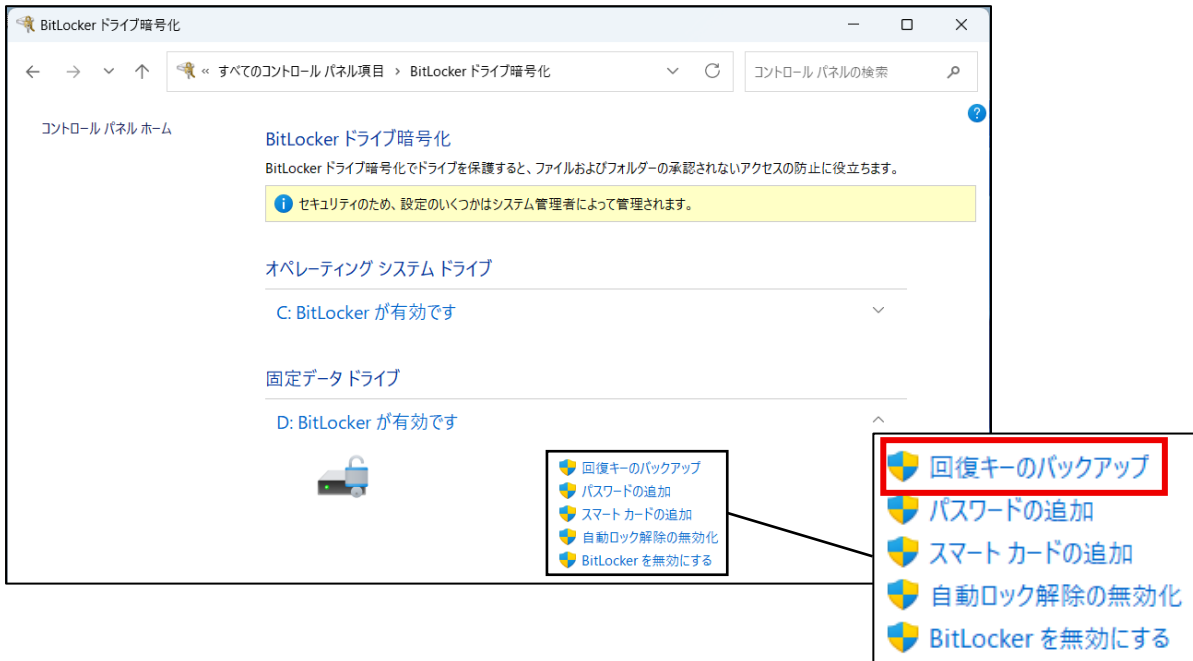
- Microsoft アカウントに保存する【推奨】  
⇒回復キーを自分の Microsoft アカウントに紐づけてオンライン保存する方法です。PC を紛失してもスマートフォンなどから確認することができます。
- ファイルに保存する【推奨】  
⇒回復キーをテキストファイルとして PC や USB メモリに保存する方法です。保存したテキストファイルを USB やクラウドストレージ (Box や Google Drive など) などの複数の場所にコピーしておくことで安心です。
- 回復キーを印刷する  
⇒回復キーを紙に印刷して物理的に保管する方法です。オフラインで管理でき、紛失リスクの分散に役立ちます。



3. 選択した保存方法で回復キーが保存されていることを必ず確認してください。

### 4.3. 固定データドライブの回復キー保存方法

1. BitLocker ドライブ暗号化の固定データドライブから「回復キーのバックアップ」を選択します。選択肢が表示されていない場合は、「D:BitLocker (または E:BitLocker) が有効です」という表示をクリックするとメニューが展開します。



2. 回復キーの保存方法を選択します。(PC の設定や利用環境により、選択肢が異なる場合があります。)

以下 3 点の保存方法の詳細については、[手順 4.2.オペレーティングシステムドライブの回復キー保存方法内の手順 2.](#)から確認してください。

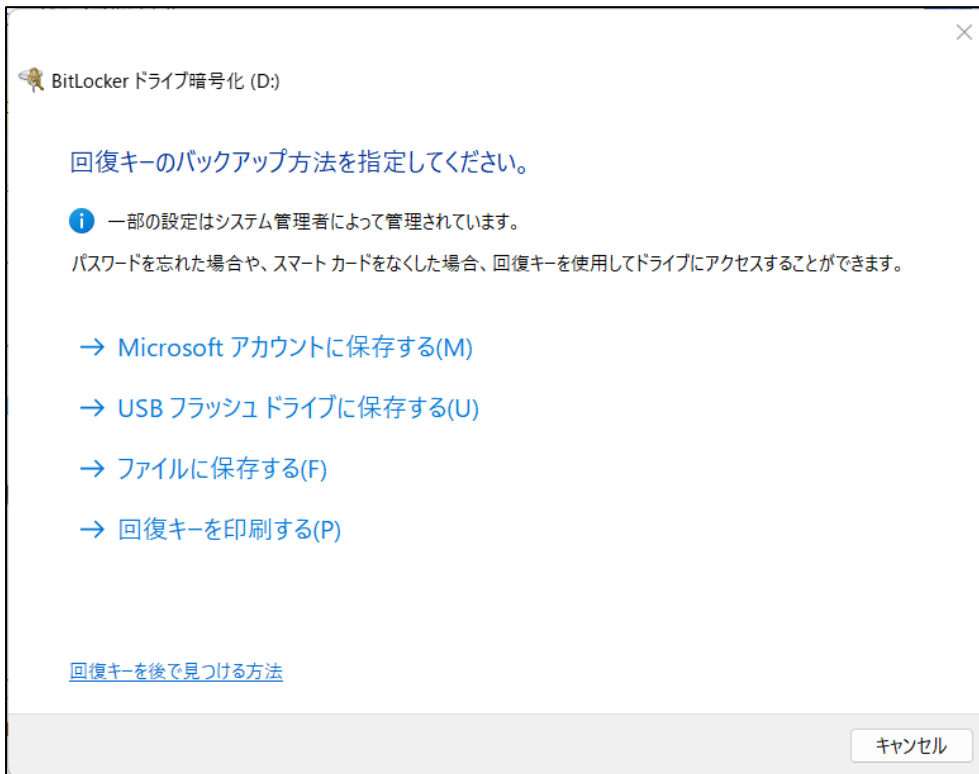
- ・ Microsoft アカウントに保存する
- ・ ファイルに保存する
- ・ 回復キーを印刷する

(次ページへ続く)

(前ページより続き)

・ USB フラッシュドライブに保存する

⇒回復キーを USB メモリにテキストファイルとして保存する方法です。ネットに接続できない環境でも安全に保管できます。



3. 選択した保存方法で回復キーが保存されていることを確認し、どのドライブ（D ドライブや E ドライブなど）の回復キーが分かるように名前を付けるなどして保管します。

#### 4.4. BitLocker を無効化する方法

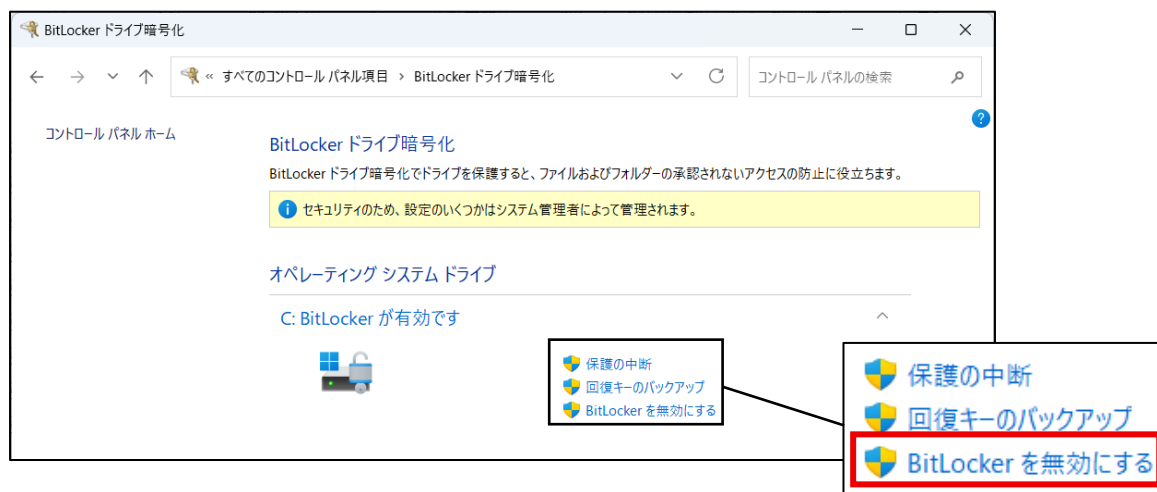
BitLocker の有効化は任意の設定のため、無効化を希望する場合は、以下の手順を参照してください。

BitLocker を無効にした場合、PC の紛失・盗難時の個人情報などのデータ漏えいリスクが高まります。PC やデータの管理には十分ご注意ください。

なお、本学では BitLocker の有効化を推奨している訳ではありません。BitLocker の有効化／無効化については、上記のリスク等を考えてご自身の判断で行うものとなります。

#### 4.4.1. オペレーティングシステムドライブの BitLocker を無効化する方法

1. BitLocker ドライブ暗号化のオペレーティングシステムドライブから「BitLocker を無効にする」を選択します。選択肢が表示されていない場合は、「C: BitLocker が有効です」という表示をクリックするとメニューが展開します。

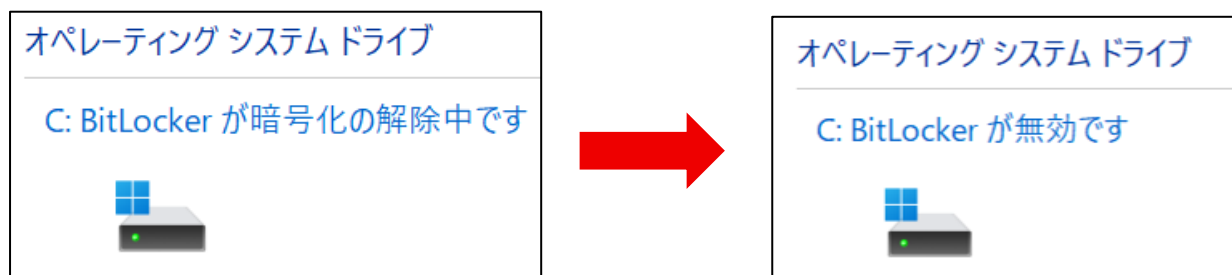


2. 「BitLocker ドライブ暗号化」という設定解除の確認ウィンドウが表示されるので、「BitLocker を無効にする」を選択します。

※固定データドライブが有効になっている場合、まとめて無効化される可能性があります。必要に応じて再度、有効化を行ってください。



3. 「C: BitLocker が暗号化の解除中です」という表示から「C: BitLocker が無効です」に変わると無効化が完了です。※無効化が完了するまで、PC の電源を切らないでください。



#### 4.4.2. 固定データドライブの BitLocker を無効化する方法

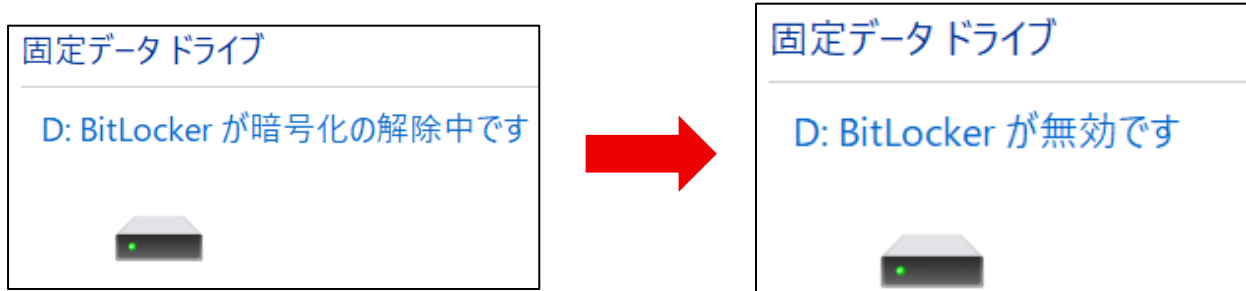
1. BitLocker ドライブ暗号化の固定データドライブから「BitLocker を無効にする」を選択します。選択肢が表示されていない場合は、「D:BitLocker (または E:BitLocker) が有効です」という表示をクリックするとメニューが展開します。



2. 「BitLocker ドライブ暗号化」という設定解除の確認ウィンドウが表示されるので、「BitLocker を無効にする」を選択します。



3. 「D:BitLocker (または E:BitLocker) が無効化中です」という表示から「D:BitLocker (または E:BitLocker) が無効です」に変わると無効化が完了です。※無効化が完了するまで、PC の電源を切らないでください。



## 5. BitLocker が無効だった場合の対応

BitLocker が無効の場合、必要に応じて有効にすることができます。

有効化は必須ではありませんが、有効化することで PC の紛失・盗難時の個人情報などのデータ漏えいリスクを軽減できます。

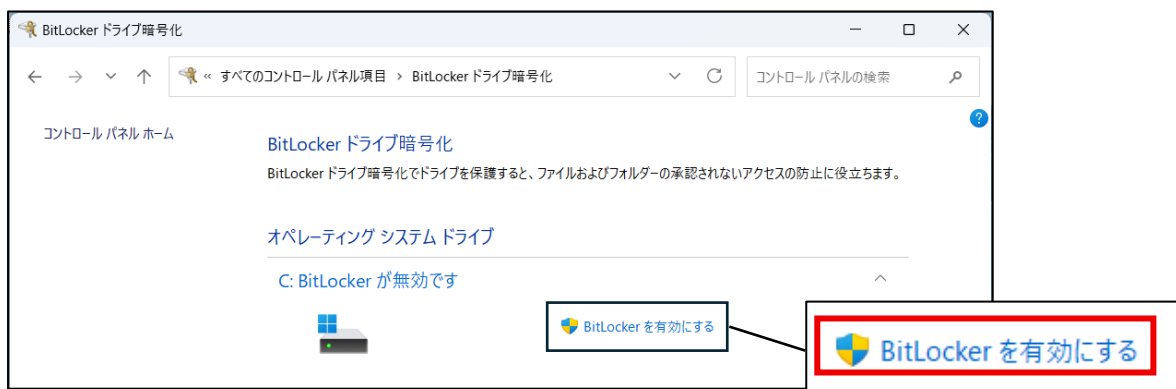
有効化を希望する場合は、[手順 4.3.回復キーの取り扱いに関する注意事項](#)と、[手順 5.1.BitLocker の有効化に関する注意事項](#)を確認し、以降の手順を参照して設定を行ってください。

### 5.1. BitLocker の有効化に関する注意事項

- 本学では BitLocker の有効化を推奨している訳ではありません。BitLocker の有効化／無効化については、上記のリスク等を考えてご自身の判断で行うものとなります。
- 暗号化中は PC の電源を切らないでください。PC 内のデータが破損する可能性があります。
- 暗号化の完了までに 10 分程度かかる場合があります。
- BitLocker の有効化後は必ず回復キーを保存してください。

### 5.2. オペレーティングシステムドライブの BitLocker を有効化する方法

1. BitLocker ドライブ暗号化のオペレーティングシステムドライブから「BitLocker を有効にする」を選択します。選択肢が表示されていない場合は、「C:BitLocker が無効です」という表示をクリックするとメニューが展開します。



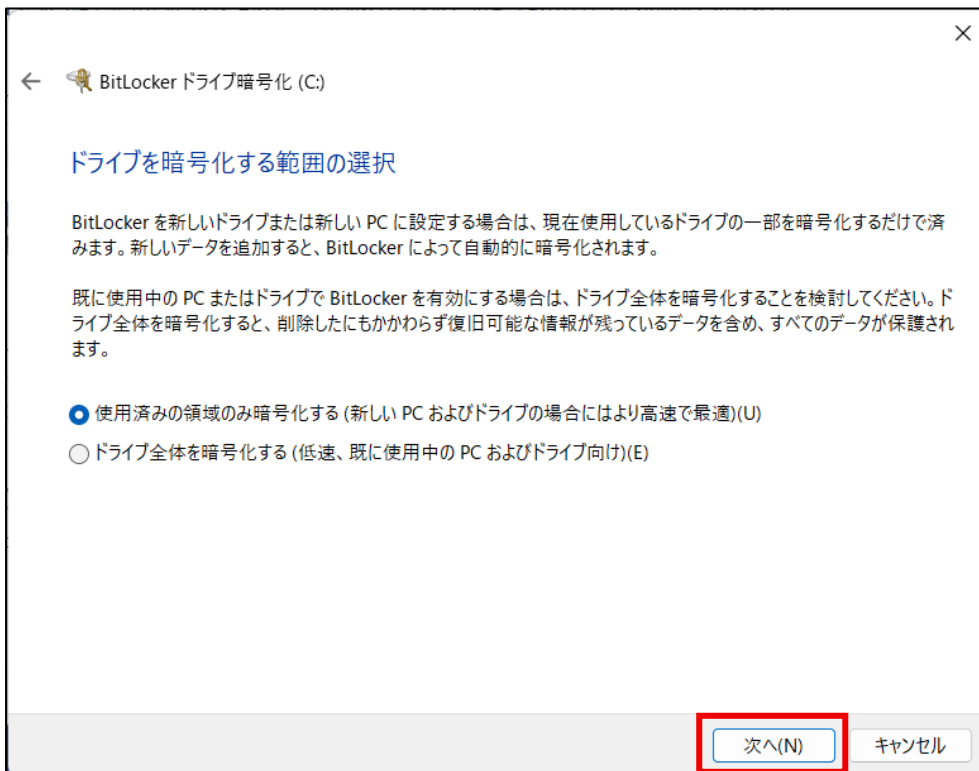
2. 回復キーのバックアップ方法を指定します。(PC の設定や利用環境により、選択肢が異なる場合があります。)

保存方法の詳細については、[手順 4.2.オペレーティングシステムドライブの回復キー保存方法内の手順 2.](#)から確認してください。

3. 回復キーのバックアップが完了すると、右下の「次へ」が選択できるようになるので、クリックして進みます。



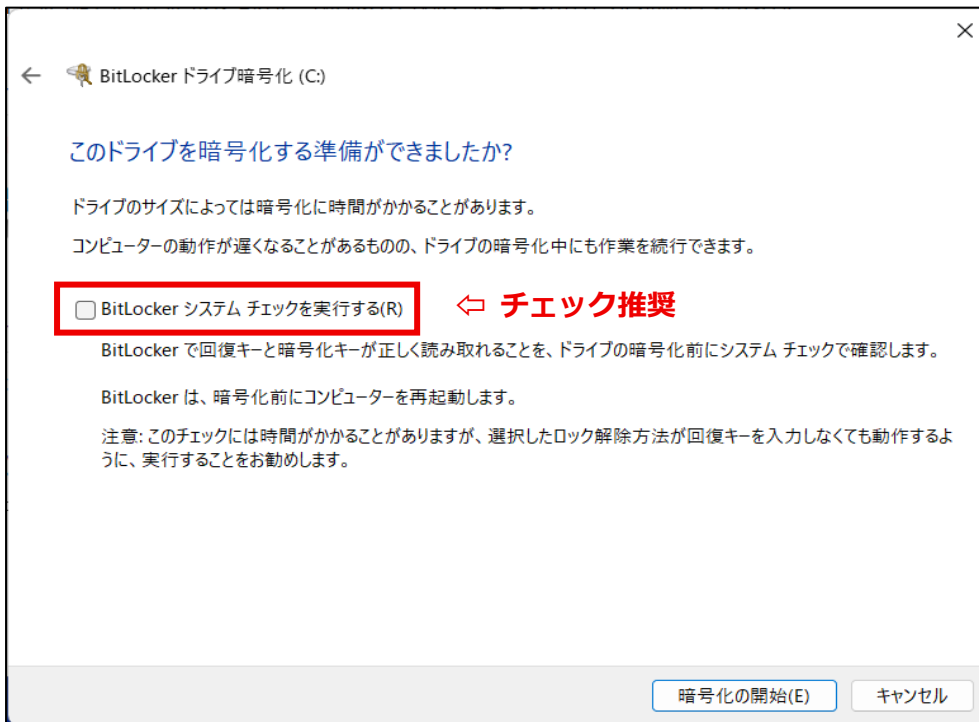
4. ドライブを暗号化する範囲を選択し「次へ」をクリックします。通常は、使用済みの領域のみの暗号化で問題ありません。



5. 使用する暗号化モードを選択し「次へ」をクリックします。通常は、新しい暗号化モードで問題ありません。



6. BitLocker システムチェックの実行確認が表示されます。  
初期状態ではチェックが外れていますが、チェックを入れて進めることを推奨します。



(次ページへ続く)

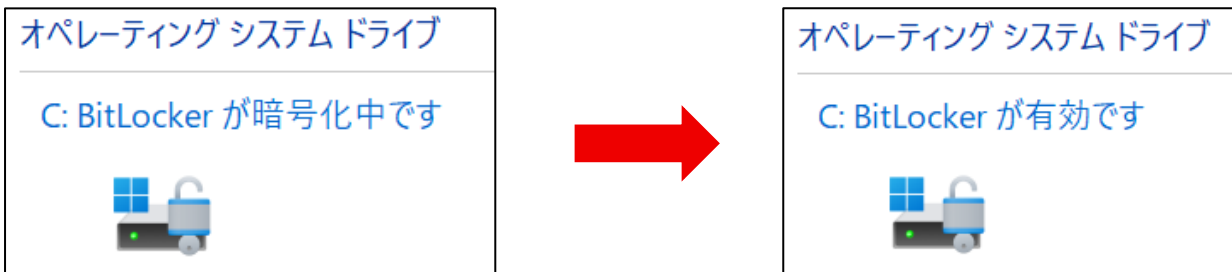
(前ページより続き)

このチェックを入れると、PC が正しく暗号化できるか事前に確認することができるため、設定後のトラブル（PC を起動できない、暗号化が途中で失敗するなど）を防ぐことができます。

チェックを入れて「続行」をクリックし、画面の表示に従い PC の再起動を行ってください。起動後は、再度「BitLocker ドライブ暗号化」を開きます。（BitLocker ドライブ暗号化の開き方は、[3.BitLocker の設定（有効／無効）を確認する方法](#)を参照してください。）

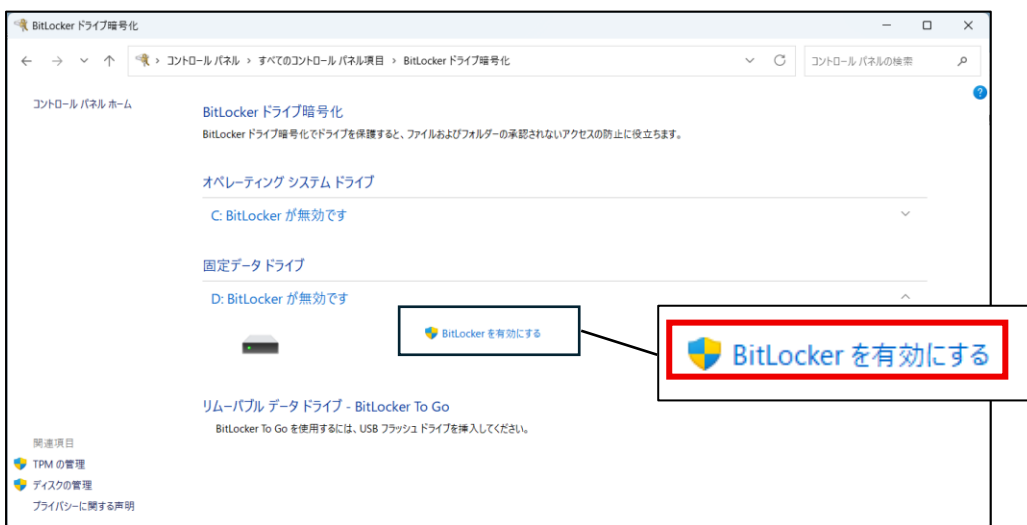
システムチェックを実行しない場合は、チェックを入れずに「暗号化の開始」をクリックすると暗号化が始まります。

7. 「C:BitLocker が暗号化中です」という表示から「C:BitLocker が有効です」に変わると有効化が完了です。



### 5.3. 固定データドライブの BitLocker を有効化する方法

1. BitLocker ドライブ暗号化の固定データドライブから「BitLocker を有効にする」を選択します。選択肢が表示されていない場合は、「D:BitLocker（または E:BitLocker）が無効です」という表示をクリックするとメニューが展開します。



## 2. 固定データドライブのロック解除方法を選択し「次へ」をクリックします。

- ・パスワードを使用してドライブのロックを解除する  
⇒最も一般的な方法で、ドライブを開くとパスワード入力画面が表示され、正しいパスワードを入力するとロックが解除されます。
- ・スマートカードを使用してドライブのロックを解除する  
⇒IC カード+PIN を使用する方法です。
- ・このコンピューターでこのドライブのロックを解除する  
⇒オペレーティングシステムドライブの BitLocker が有効な場合のみ表示されます。

The screenshot shows the BitLocker drive encryption dialog box for drive D:. The title bar reads "BitLocker ドライブ暗号化 (D:)". The main heading is "このドライブのロック解除方法を選択する". There are three radio button options:

- パスワードを使用してドライブのロックを解除する(P)  
パスワードには大文字、小文字、数字、空白文字、記号を含めてください。  
パスワードを入力してください(E) [input field]  
パスワードをもう一度入力してください(R) [input field]
- スマート カードを使用してドライブのロックを解除する(S)  
スマート カードを挿入する必要があります。ドライブのロックを解除するときは、スマート カードの PIN が必要です。
- このコンピューターでこのドライブのロックを自動的に解除する(A)

At the bottom right, there are two buttons: "次へ(N)" and "キャンセル". A red box highlights the "次へ(N)" button, and a yellow callout box with a red border points to it, containing the text: "ロック解除方法を選択するとクリックできるようになります。"

## 3. 回復キーのバックアップ方法を指定します。(PC の設定や利用環境により、選択肢が異なる場合があります。)

保存方法の詳細については、[手順 4.3.固定データドライブの回復キー保存方法内の手順 2.](#)から確認してください。

## 4. [手順 5.2.オペレーティングシステムドライブの BitLocker を有効化する方法内の手順 4.~5.](#)と同様に画面の表示を確認しながら進みます。

5. 「暗号化の開始」をクリックすると暗号化が始まります。



6. 「D:BitLocker（または E:BitLocker）が暗号化中です」という表示から「D:BitLocker（または E:BitLocker）が有効です」に変わると有効化が完了です。

