Kripta

ユーザーマニュアル

USB メモリとパーティションをガイドに沿って暗号化し、会社のヘルプデスク経由でパスワードを回復できます。



バージョン 1.2 · Windows · macOS · Linux

2026 年 11 月

目次

1 Kripta とは — 用途と必要なもの

2 初回起動 — 企業構成とコンポーネント

3 メインウィンドウ — インジケーター、通知、アイコン

4 ドライブの暗号化 — 4 ステップのウィザード

5 ディスクのパーティション分割 — 暗号化領域と通常領域

6 暗号化ドライブの使用 — ロック解除、開く、ロック

7 パスワードの変更

8 パスワードを忘れた場合 — ヘルプデスクによる回復

9 設定 — 言語、構成、更新

10 他のコンピューターでの使用

11 メッセージとトラブルシューティング

12 よくある質問

A IT 部門向け付録 — パッケージ、署名付き構成、言語

表記について

画面に表示される文字（ボタン、タイトル、項目）は次のように表記します：**ドライブを暗号化**。画面写真は macOS 版のものです。Windows と Linux でもウィンドウは同じで、デバイス名だけが異なります（例：`/dev/disk4s1` の代わりに `E:` や `/dev/sdb1`）。

1 Kripta とは

Kripta は、**USB メモリ**や外付けディスクの**パーティション**のデータを AES-256 暗号化で保護します。暗号化後は、パスワードを知っている人だけがドライブの内容を読み取れます。USB メモリを紛失しても、他の人は開けません。

ガイド付き暗号化
4 ステップ：ドライブを選び、パスワードを決め、確認して、待つだけです。

自動ロック解除
暗号化ドライブを接続すると、Kripta がすぐにパスワードを求めて開きます。

どこでも使える
同じ USB メモリを Windows、macOS、Linux で開けます（標準の VeraCrypt 形式）。

セルフインストール
Kripta が VeraCrypt を自動でインストール・更新し、企業構成はファイルからインポートします。

9 つの言語
イタリア語、英語、フランス語、スペイン語、ドイツ語、ロシア語、アラビア語、中国語、日本語。さらに言語を追加できます。

ヘルプデスクによる回復
パスワードを忘れても、ヘルプデスクがデータを失わずに新しいパスワードを設定するお手伝いをします。

必要なもの

- コンピューターにインストールされた **Kripta**。初回起動時、暗号化エンジン **VeraCrypt**（macOS では **FUSE-T** も）がなければ、Kripta が自動でインストールします：第 2 章。
- IT 部門がまだコンピューターを構成していない場合は、ヘルプデスクから受け取った**署名付き構成ファイル**（`.kripta-config`）。
- 新しいドライブを暗号化するときは**社内ネットワーク**（または VPN）への接続：回復キーがすぐにヘルプデスクへ送信されます。暗号化済みドライブのロック解除にはネットワークは不要です。
- システムが求めたときのコンピューターの**管理者資格情報**（囲み参照）。

> **承認の要求**
> ドライブへの直接の読み書き、コンポーネントのインストール、構成の保存には管理者権限が必要です。 **Windows** では起動時にユーザーアカウント制御の画面が表示されます。**macOS** と **Linux** では 「操作を完了するには、Kripta に管理者の承認が必要です」というメッセージが表示されます。IT 部門が Kripta のシステムサービスをインストールしている場合、これらの要求は表示されません。

回復のしくみ（概要）

暗号化の際、Kripta は 48 桁の**回復キー**を生成して保護し、ヘルプデスクのアーカイブへ送信します。 あなたがキーを見たり保管したりする必要はありません。本人確認の後にヘルプデスクの担当者だけが参照でき、参照はすべて記録されます。

2 初回起動

初回起動時、Kripta は 2 つのことを確認します。会社のヘルプデスクに接続されているか、そしてコンピューターに VeraCrypt があるかです。 不足があれば、ウィンドウ上部に解決用のボタン付きの通知が表示されます。すべてご自身で行えます。



初回起動：構成のインポートと VeraCrypt のインストールが必要です。

企業構成をインポートする

構成は、回復キーをどのヘルプデスクのアーカイブに送るかを Kripta に伝えます。ヘルプデスクから拡張子 `.kripta-config` のファイルとして渡されます。 デジタル署名されているため、誰かが変更すると Kripta が検出します。

1. 受け取ったファイルをコンピューターに保存します（メール、社内ポータル、USB メモリなど）。
2. 通知の **構成をインポート** を押すか、 **設定** （右上の歯車）を開いて **署名付き構成をインポート…** を押します。
3. ファイルを選択します。Kripta が署名を検証し、組織、ヘルプデスクのサーバー、発行日、**署名のフィンガープリント**を表示します。
4. 初回のインポートでは、ヘルプデスクから伝えられたフィンガープリント（電話、イントラネットなど）と**照合**します。一致したら **インポート** を押します。
5. システムの承認要求を確認します。**構成をインポートしました**と表示され、 **Help Desk** インジケーターが緑になります。



署名のフィンガープリントを確認してインポート。

> **フィンガープリントが一致しない場合はインポートしないでください**
> 会社から送られたファイルではない可能性があります。キャンセルしてヘルプデスクに連絡してください。 初回インポート後、Kripta は同じキーで署名された更新のみを受け付けます。偽のファイルは自動的に拒否されます。

VeraCrypt をインストールする

Kripta には VeraCrypt の公式インストーラー（macOS 用は FUSE-T も）が同梱されています。通知の **今すぐインストール** を押し、承認要求を確認します。 Kripta がインストーラーの公式署名を検証し、追加の質問なしでインストールします。



公式署名を確認しながらコンポーネントをインストール。

完了すると**インストールが完了しました**と表示されます。Windows では再起動が必要な場合があります。

VeraCrypt の更新

起動するたび（その後は 1 日 1 回）、Kripta は VeraCrypt の新しいバージョンが公開されていないか確認します。新しいバージョンがあれば、 **更新** ボタン付きの青い通知が表示されます。新しいバージョンは公式サイトからダウンロードされ、VeraCrypt 開発者の署名が有効な場合にのみインストールされます。



VeraCrypt の更新があります。

更新の前に

開いている暗号化ドライブをすべてロックしてください。ロック解除中のドライブがある間、Kripta は VeraCrypt を更新しません。 自動確認は設定でオフにできます（第 9 章）。

3 メインウィンドウ

Kripta を開くとホーム画面が表示されます。ここで新しいドライブを暗号化したり、接続中の暗号化ドライブを管理したりできます。



暗号化ドライブが接続され、ロック解除されているホーム画面。

要素	用途
VeraCrypt	**緑**の点：暗号化エンジンがインストール済み。**赤**：未インストール（第 2 章）。マウスを重ねるとバージョンが表示されます。
Help Desk	緑：キーアーカイブに接続可能。赤：接続不可（ネットワークなし、VPN オフ、構成なし）。
歯車	**設定** を開きます：言語、企業構成、コンポーネント（第 9 章）。
ドライブを暗号化	ウィザードを開始します（第 4 章）。Kripta が未構成か VeraCrypt がない場合は無効です。
パーティションに分割	USB メモリや外付けディスクを複数のパーティションに分割します（第 5 章）。
接続中の暗号化ドライブ	接続中の Kripta ドライブ。**ロック中** または **ロック解除済み** の状態と操作ボタンが表示されます。

通知

ウィンドウ上部に、問題を解決するボタン付きの色付きの枠が表示されることがあります。



ヘルプデスクのサーバーに接続できず、回復キーが 1 件送信待ち。

- **ヘルプデスクのサーバーに接続できません：**ドライブのロック解除はできますが、新しい暗号化はできません。
- **送信待ちの回復キー：**Kripta が自動で再試行します。オンラインに戻ったら **今すぐ再試行** を押してください。**通知が消えるまで Kripta を起動したままにしてください。**
- **Kripta がヘルプデスクに未接続 / VeraCrypt が未インストール / VeraCrypt … が利用可能：**第 2 章を参照してください。

Kripta のアイコン：メニューバーと通知領域

Kripta は暗号化ドライブの接続を検知するためにバックグラウンドで動作し、エンブレムのアイコンから操作します。

システム	アイコンの場所	知っておくと便利
macOS	右上の**メニューバー**。Kripta は **Dock には表示されません**。	ノッチ付きの MacBook では、メニューバーがいっぱいになると余ったアイコンが隠れます。使わないアイコンを削除するか、⌘ を押しながらドラッグしてください。
Windows	右下の時計の近くの**通知領域**。	隠れているアイコンの中にある場合は、^ をクリックしてエンブレムをタスクバーにドラッグします。

システム	アイコンの場所	知っておくと便利
Linux	パネルの**通知領域**。	素の GNOME（Fedora、Debian）では **AppIndicator and KStatusNotifierItem Support** 拡張機能が必要です。

アイコンのメニューには **Kripta を開く**、**ドライブを暗号化…**、**パーティションに分割…**、**すべてのドライブをロック**、**設定…**、**Kripta を終了** があります。項目は選択した言語で表示されます。

> **ウィンドウを閉じても Kripta は終了しません**
> Kripta はメニューバーまたは通知領域で動作し続けます。 ウィンドウを再び開くには **Kripta を開く** を使うか、Kripta をもう一度起動してください。実行中のウィンドウが表示されます。

自動起動

インストール後、Kripta は**サインインのたびに自動的に起動**し、ウィンドウを開かずに常に待機します。暗号化ドライブを接続するとすぐにパスワードを求めます。**設定 › 自動起動** でオフにできます（第 9 章）。**Kripta を終了** すると、次回のサインインまで終了します。

4 ドライブの暗号化

> **暗号化するとドライブの内容はすべて消去されます。**
> 始める前に、残したいファイルを別の場所にコピーしてください。暗号化後、保護されたドライブにコピーし直せます。

USB メモリを接続し、**Help Desk** インジケーターが緑であることを確認して、**ドライブを暗号化**を押します。

ステップ 1 — ドライブ



暗号化するドライブの選択。

1. Kripta が接続中のデバイスを一覧表示します（リムーバブルが先）。**システムディスクは表示されません。**
2. 正しいドライブを選ぶため、**容量と名前**をよく確認してください。
3. USB メモリが表示されない場合は、接続し直して**一覧を更新**を押します。
4. ドライブを選択して**次へ**を押します。

> **「暗号化済み？」ラベル**
> 認識できるファイルシステムのないドライブを示します。おそらくすでに暗号化されています。 再度暗号化すると、現在の内容は失われます。

ステップ 2 — パスワード



条件を満たすとルールが緑になります。

パスワードは**12 文字以上**で、英小文字・英大文字・数字・記号のうち**3 種類以上**を含み、**アクセント記号のない半角英字のみ**を使います。 日本語などの文字は他のシステムで異なる入力になることがあります。色付きのバーは強度を示し、👁 ボタンでパスワードを表示できます。 2 つ目の欄にもう一度入力して **次へ** を押します。

> **ヒント**
> 複数の単語を記号と数字でつないだフレーズ（例： `Densha-Mizuumi-Midori-47` ）は安全で覚えやすいです。会社アカウントのパスワードは使わないでください。

ステップ 3 — 確認



概要と消去の確認。

概要を確認し、**ファイルを保存しました。このドライブを消去して暗号化します**にチェックを入れ、**消去して暗号化**を押します。 システムが管理者の承認を求める場合があります。

ステップ 4 — 暗号化



速度と残り時間付きの進行状況。

Kripta はドライブを準備し、全体をランダムデータで上書きし（最も時間のかかる段階）、exFAT の暗号化ボリュームを作成して、回復キーを生成しヘルプデスクへ送信します。

> **暗号化中は**
> ドライブを取り外したり、コンピューターの電源を切ったりスリープさせたりしないでください。64 GB の USB メモリでおよそ 15 分〜1 時間かかります。



暗号化完了。

回復キーはまだ送信されていませんと表示されても、ドライブは暗号化されて使用できます。Kripta を起動したままネットワークに接続しておけば、できるだけ早くキーが送信されます。 暗号化に失敗した場合は、メッセージに理由が表示されます（第 11 章）。

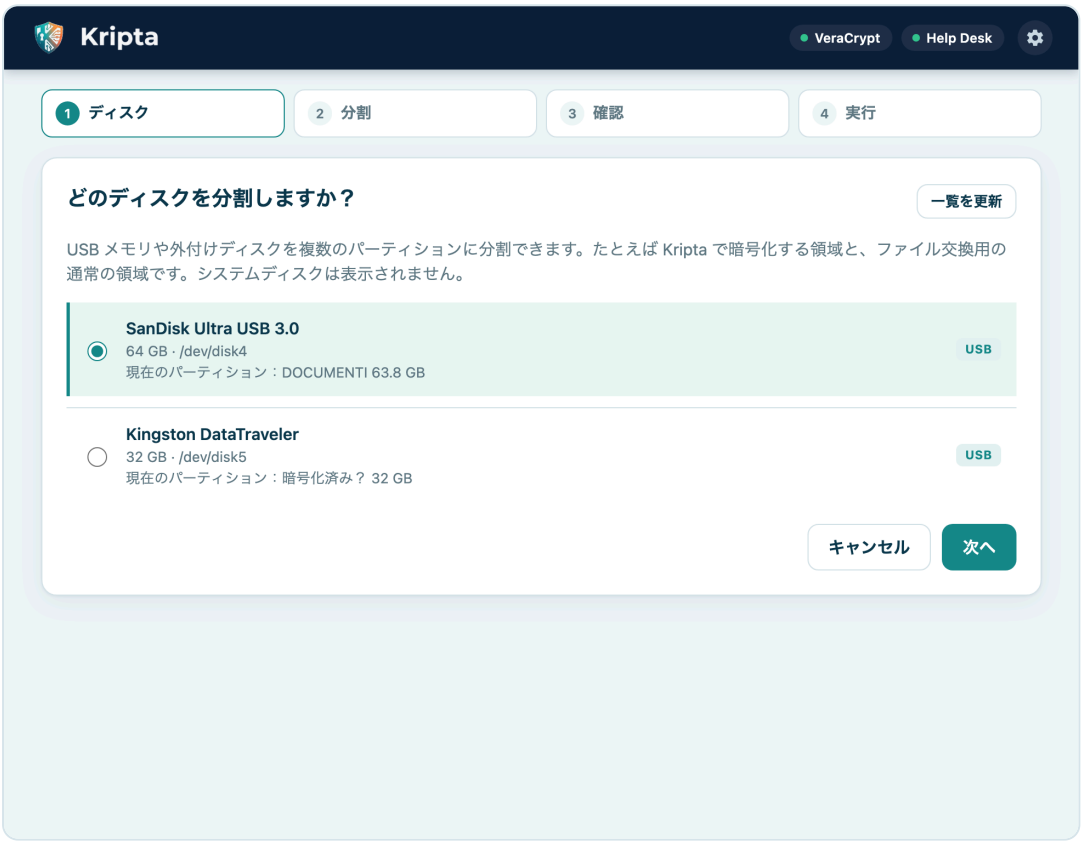
5 ディスクのパーティション分割

パーティションに分割を使うと、USB メモリや外付けディスクを、それぞれ名前とファイルシステムを持つ複数の独立した部分に分割できます。 典型的な使い方は、機密データ用の**暗号化領域**と、Kripta のないコンピューターとファイルを交換するための**通常領域**です。

分割するとディスク全体が消去されます

。既存のパーティションや暗号化済みドライブも含まれます。残したいファイルは別の場所に保存してください。

ステップ 1 — ディスク



現在のパーティションを確認してディスクを選択。

ステップ 2 — 分割



色付きのバーが分割の比率を示します。

テンプレート	結果
暗号化領域 + 通常領域	ディスクの 4 分の 3 を暗号化用、残りを exFAT の通常領域にします。最初に提案されるテンプレートです。
単一パーティション	ディスク全体を 1 つのパーティションにします。
2 等分 / 3 等分	ディスクを同じサイズに分割します。

各パーティションの**名前**（英字、数字、`_`、`-` で 11 文字まで）、**サイズ**（最後のパーティションは残りの容量）、 **ファイルシステム**、**暗号化する**を設定します。**+ パーティションを追加**で追加できます（最大 8 個）。

ファイルシステム	開けるシステム	備考
exFAT（推奨）	Windows、macOS、Linux	ファイルサイズの実質的な制限なし。
FAT32	ほぼすべての機器	ファイルは 4 GB まで。Windows ではパーティションは 32 GB まで。
NTFS	Windows、macOS は読み取り専用	Linux では `ntfs-3g` が必要。
APFS、**Mac OS 拡張**	Mac のみ	Mac からのみ使用可能。

ファイルシステム	開けるシステム	備考
ext4	Linux のみ	Linux からのみ使用可能。

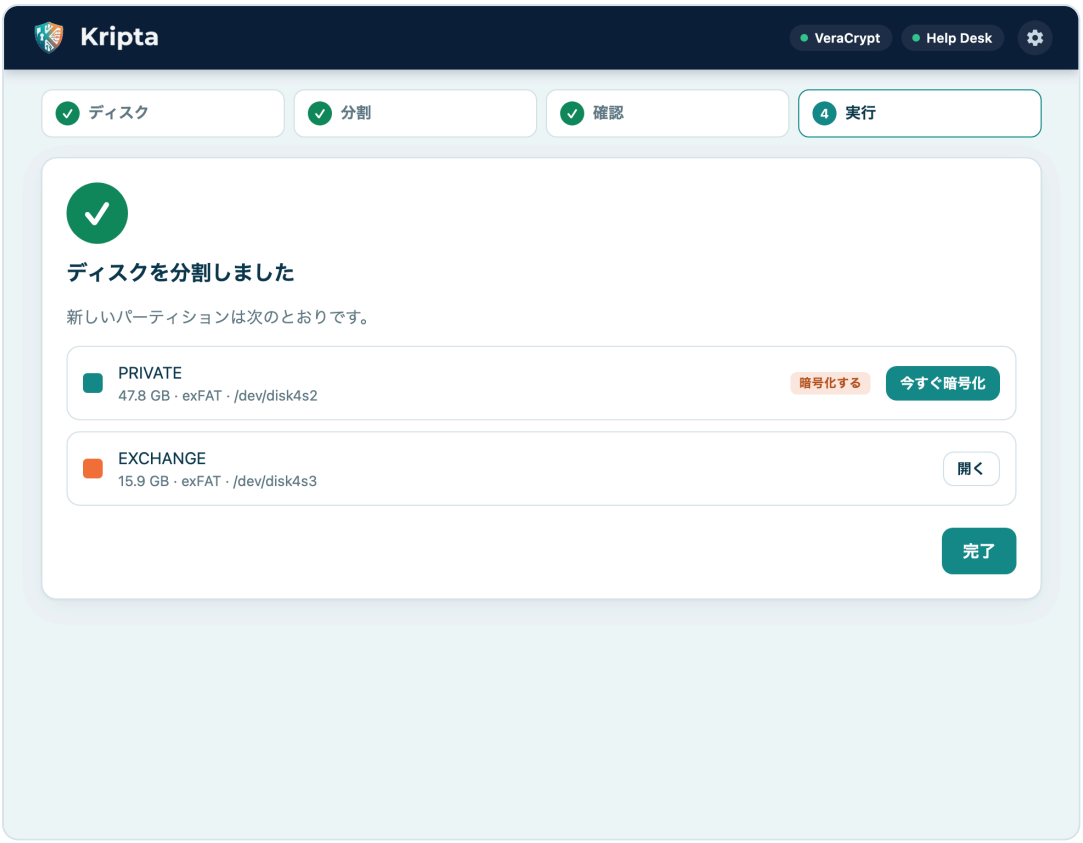
> **MBR 方式**
> テレビ、カーオーディオ、非常に古いコンピューターで使う場合のみ有効にしてください。パーティションは最大 4 個、ディスクは 2 TB までです。

ステップ 3 — 確認、ステップ 4 — 実行



消去前の概要。

確認のチェックボックスをオンにして **消去して分割** を押します。通常は 1 分以内に完了します。



パーティション作成完了：暗号化する領域に「今すぐ暗号化」ボタンがあります。

暗号化するパーティションの横の **今すぐ暗号化** を押すと、そのパーティションが選択された状態で暗号化（第 4 章）が始まります。

> **暗号化するまで「暗号化する」領域は保護されていません**
> 暗号化が完了するまで機密ファイルをコピーしないでください。

6 暗号化ドライブの使用

ロック解除

Kripta の起動中に暗号化ドライブを接続すると、パスワードの入力画面が自動的に表示されます。



接続時のパスワード入力。

1. パスワードを入力して**ロック解除**（または Enter）を押します。
2. ドライブはエクスプローラー、Finder、Linux のファイルマネージャーで通常のディスクとして開きます。
3. **無視**を押すと、後でメインウィンドウからロック解除できます。

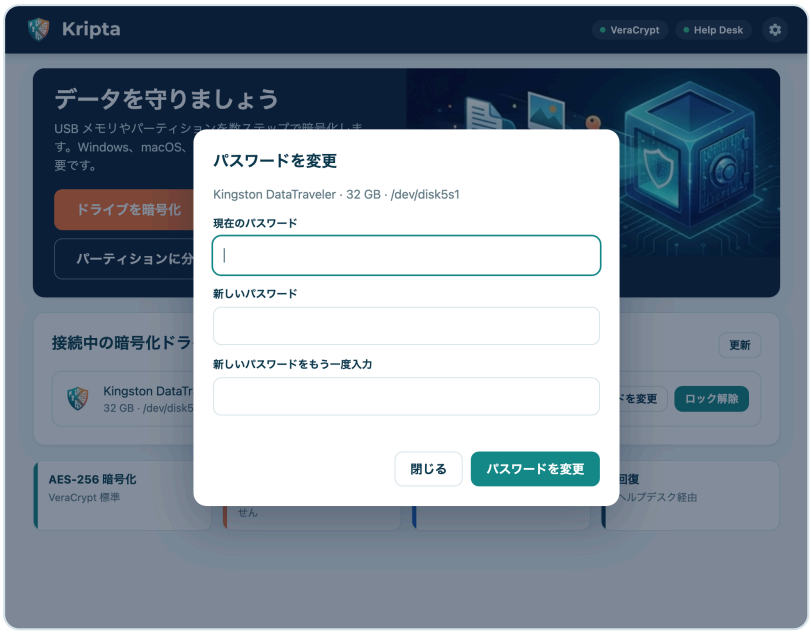
ファイルの操作とロック

ロック解除中はファイルを普通に使えます。書き込んだ内容はすべて自動で暗号化されます。作業が終わったら、開いているファイルを閉じて**ロック**を押し、ドライブを取り外します。

> **ロックせずにロック解除中のドライブを取り外さないでください**
> コピー中のファイルが失われる可能性があります。

7 パスワードの変更

現在のパスワードがわかれば、いつでも変更できます。ドライブ上のデータは変更されません。



パスワード変更の画面。

1. ドライブがロック解除中の場合は、先に **ロック** を押します。
2. ドライブの横の **パスワードを変更** を押します。
3. 現在のパスワードと、新しいパスワードを 2 回入力して（第 4 章と同じルール）、確定します。

> **回復キーは？**
> 引き続き有効です。パスワードを変更した後も、ヘルプデスクはサポートできます。

8 パスワードを忘れた場合

ヘルプデスクからドライブの回復キーを受け取れます。それを使って新しいパスワードを設定し、すべてのファイルを取り戻せます。



ヘルプデスクによる回復。

1. パスワード入力画面で **パスワードを忘れた** を選びます。
2. コンピューター名とドライブ名が表示されます。**表示** を押すとドライブ識別子も表示されます。
3. **ヘルプデスクに連絡**し、これらの情報を伝えます。本人確認の後、**48 桁のキー**が読み上げられます。
4. **回復キー** 欄に入力し、新しいパスワードを設定して **パスワードをリセット** を押します。

キーは 1 回限り
回復のたびに Kripta は新しいキーを生成し、ヘルプデスクへ送信します。

詐欺にご注意ください
ヘルプデスクがパスワードを尋ねることはありません。ヘルプデスクに連絡するのはあなたの側です。

9 設定

右上の歯車、またはアイコンのメニューの **設定…** から開きます。



設定：言語、企業構成、コンポーネント、情報。

言語

一覧から言語を選ぶと、画面、アイコンのメニュー、承認要求がすぐに切り替わります。 **自動** を選ぶとシステムの言語を使います。内蔵の言語：

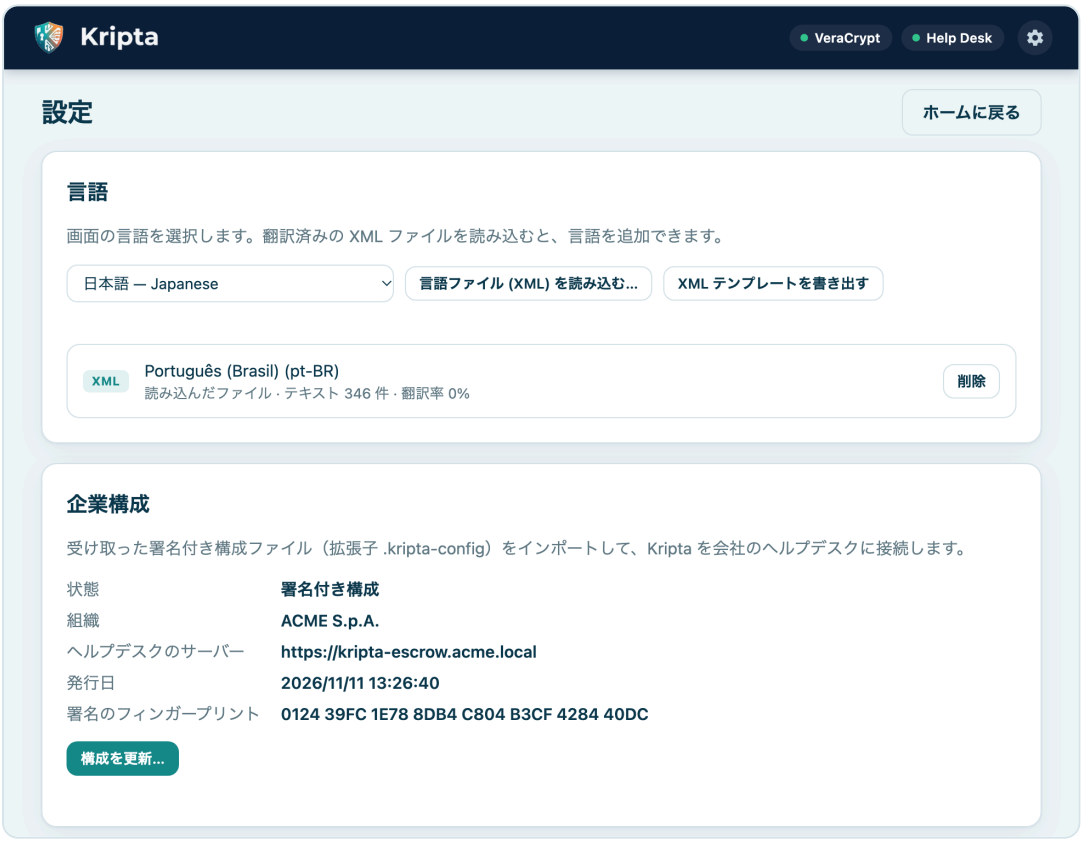
Italiano　English　Français　Español　Deutsch　Русский　العربية　中文　日本語

言語を追加する

翻訳は言語ごとのシンプルな **XML** ファイルです。追加の手順：

1. **XML テンプレートを書き出す** を押すと、現在の言語のファイルがダウンロードフォルダーに保存されます。
2. 各 `<string>` 要素のテキストを翻訳します。`id` 属性とプレースホルダー `{1}`、`{2}` は変更しないでください。
3. ファイルの先頭で `code`（例：`pt` や `pt-BR`）、`name`、`english-name`、`dir`（右から左に書く言語は `rtl`）を設定します。
4. **言語ファイル (XML) を読み込む…** を押してファイルを選びます。言語が翻訳率とともに一覧に表示されます。未翻訳のテキストは英語で表示されます。

```
<kripta-language format="1" code="pt" name="Português" english-name="Portuguese" dir="ltr">
  <string id="home.title">Proteja os seus dados</string>
  …
</kripta-language>
```



XML ファイルから読み込んだ言語と削除ボタン。

内蔵の言語と同じコードのファイルを読み込むと、その言語が置き換わります（用語の修正に便利）。**削除** で元に戻ります。 内蔵の 9 言語のファイルは、このマニュアルと同じ場所の `lang` フォルダーにあります。

企業構成

インストールされている構成の組織、ヘルプデスクのサーバー、日付、フィンガープリントを表示します。**構成を更新…** でヘルプデスクから受け取った新しいファイルをインポートします（第 2 章）。

コンポーネント

インストール済みの VeraCrypt、Kripta に同梱のバージョン、最新のバージョンを表示します。**今すぐ確認** ですぐに確認し、 **インストール** / **VeraCrypt を更新** でインストールを開始します。**起動するたびに…確認する** のチェックで自動確認をオン・オフできます。

自動起動

サインイン時に Kripta を自動的に起動する チェックボックスは既定でオンです。その下に、自動起動がシステムに登録されているかが表示されます。オフにすると、Kripta を開くまで暗号化ドライブは検出されません。

10 他のコンピューターでの使用

Kripta で暗号化したドライブは、標準の **VeraCrypt** 形式と **exFAT** ファイルシステムを使っているため、Windows、macOS、Linux で開けます。

コンピューター	ドライブを接続したときの動作
Kripta が構成済み	パスワードの入力画面が表示されます。すべて自動です。
Kripta はあるが**企業構成がない**（自宅など）	パスワードの入力画面は表示され、ドライブのロックを解除できます。VeraCrypt がなければ、Kripta が **今すぐインストール** を提案します。構成がないと、新しいドライブの暗号化やパスワードの回復はできません。
VeraCrypt のみ	VeraCrypt を開き、空きスロットを選んで**デバイスの選択**から USB メモリのパーティションを選び、**マウント**してパスワードを入力します。
Kripta も VeraCrypt もない	何も表示されません。OS は USB メモリからプログラムを自動起動しません。 システムがドライブの**フォーマット**を提案することがありますが、**必ず拒否してください**。Kripta（社内サイトから入手）をインストールして、ドライブを接続し直してください。

管理者権限
どのコンピューターでも、暗号化ドライブを開くには管理者権限が必要です。VeraCrypt がシステムドライバーを使うためです。 資格情報を持っていないコンピューターでは、ドライブを開けません。

交換用の通常領域
Kripta のないコンピューターをよく使う場合は、**暗号化領域 + 通常領域** テンプレートで USB メモリを分割してください（第 5 章）。 通常領域に Kripta のインストーラーをコピーしておくこともできます。

11 メッセージとトラブルシューティング

メッセージまたは状況	対処方法
Kripta はまだ会社のヘルプデスクに接続されていません	ヘルプデスクから受け取った `.kripta-config` ファイルをインポートしてください（第 2 章）。
パッケージの署名が無効です	ファイルが変更されたか破損しています。ヘルプデスクに再送を依頼してください。
パッケージが異なるキー / 未承認のキーで署名されています	会社からのファイルではありません。使用せず、ヘルプデスクに連絡してください。
構成は IT 部門が管理しているため置き換えられません	コンピューターは一元管理されています。インポートは不要です。
暗号化エンジン VeraCrypt がインストールされていません	**今すぐインストール** を押してください。ボタンがない場合はヘルプデスクに連絡してください。
VeraCrypt の公式署名が無効 / ファイルが署名済みバージョンと一致しません	ダウンロードが改ざんされたか不完全です。インストールは中止されました。後でもう一度お試しください。
VeraCrypt を更新する前に、すべての暗号化ドライブをロックしてください	開いているドライブで **ロック** を押し、更新をやり直してください。
更新を完了するにはコンピューターを再起動してください（Windows）	作業を保存して再起動してください。
ヘルプデスクのサーバーに接続できません。暗号化は開始されませんでした。	社内ネットワークまたは VPN に接続して再試行してください。ドライブのデータは変更されていません。
送信待ちの回復キーがあります	ネットワークに接続して **今すぐ再試行** を押してください。通知が消えるまで Kripta を起動したままにしてください。
使用できるドライブがありません	USB メモリを接続し直し（別の USB ポートも試してください）、**一覧を更新** を押してください。
管理者の承認がキャンセルされた / タイムアウトしました	操作をやり直し、システムの要求を承認してください。
ボリュームをマウント解除 / ロックできません	ドライブから開いた文書やウィンドウを閉じてから再試行してください。
パスワードが正しくありません	Caps Lock とキーボード配列を確認してください。忘れた場合は第 8 章を参照してください。
回復キーが正しくありません	担当者と数字をもう一度確認してください。**最新**のキーが必要です。
ディスクにロック解除中の Kripta ドライブがあります	ホーム画面でロックしてから、分割をやり直してください。

メッセージまたは状況	対処方法
システムが新しいパーティションを検出しませんでした	ドライブを取り外して接続し直してください。
言語ファイルが有効な XML ではない / 使用できない要素があります	メッセージに示されたファイルを修正してください。プレーンテキストの `<string>` 要素のみ使用できます。
接続してもロック解除の画面が表示されません	Kripta が起動していること（バーのアイコン）を確認し、メインウィンドウの**ロック解除**を使ってください。

12 よくある質問

ファイルが入った USB メモリを、ファイルを失わずに暗号化できますか？

できません。暗号化するとドライブは消去されます。ファイルを別の場所にコピーし、暗号化してから戻してください。

コンピューターの内蔵ディスクを暗号化できますか？

できません。Kripta は USB メモリと外付けディスク向けです。システムディスクは表示されません。

ヘルプデスクは私のファイルを読めますか？

ヘルプデスクが保管するのは回復キーだけで、あなたの依頼があった場合にのみ参照でき、アクセスはすべて記録されます。

回復キーを書き留める必要がありますか？

いいえ。キーを見ることはなく、保管する必要もありません。ヘルプデスクに保管されています。

Kripta はコンピューターにプログラムをインストールしますか？

VeraCrypt（macOS では FUSE-T も）のみです。あなたの確認後、かつ開発者の公式署名が有効な場合に限ります。

自宅のコンピューターで USB メモリを使えますか？

はい。Kripta または VeraCrypt をインストールすれば使えます（第 10 章）。社外でのデータ利用に関する会社の規則は必ず守ってください。

必要な言語がありません。どうすればよいですか？

XML テンプレートを翻訳して設定から読み込むか（第 9 章）、IT 部門に配布を依頼してください。

なぜパスワードに日本語やアクセント付きの文字を使えないのですか？

Windows、macOS、Linux でエンコードが異なる場合があり、別のシステムで同じパスワードを入力しても認識されないことがあるためです。

暗号化でどのくらい容量が減りますか？

ごくわずかです。ボリュームヘッダーに数百 KB を使うだけです。

A IT 部門向け付録

パッケージ

システム	パッケージ	備考
Windows 10/11 (x64)	`Kripta_1.2.0_x64-setup.exe`	VeraCrypt の公式 MSI（x64 と ARM64）を同梱。アプリは管理者権限で起動します。
macOS 11+	`Kripta_1.2.0_universal.dmg`	VeraCrypt（FUSE-T 版と macFUSE 版）と、カーネル拡張不要の FUSE-T を同梱。
Debian / Ubuntu	`Kripta_1.2.0_amd64.deb`	Ubuntu 22.04/24.04 と Debian 12/13 用の VeraCrypt を同梱。その他のバージョンでは Kripta が検証済みパッケージをダウンロードします。
Fedora / RHEL	`Kripta-1.2.0-1.x86_64.rpm`	Fedora 44 用の VeraCrypt を同梱。`exfatprogs` もインストールしてください。
その他のディストリビューション	`Kripta_1.2.0_amd64.AppImage`	ポータブル実行ファイル。

署名付き構成

escrow サーバーで一度だけ署名キーを生成し、クライアント構成に署名します（テンプレートは `deploy/client/kripta.toml.example`）。

```
kripta-escrow keygen-sign            # 秘密鍵（オフライン保管）+ 公開鍵 + フィンガープリント
kripta-escrow sign-config client.toml signing.key "ACME" acme.kripta-config
```

`acme.kripta-config` をユーザーに配布し、信頼できる経路（イントラネット、ヘルプデスクの電話）で**フィンガープリント**を公開してください。 Kripta は特権プロセスを通じて構成をシステムの場所（`%ProgramData%\Kripta`、`/Library/Application Support/Kripta`、 `/etc/kripta`）に署名者のキーとともに保存します。以降の更新には同じ署名が必要です。 ユーザーによるフィンガープリントの照合に頼らない場合は、`KRIPTA_PROVISIONING_KEYS=<公開鍵>` を指定して Kripta をビルドしてください。そのキーのみが受け付けられます。 IT 部門が手動でコピーした（署名なしの）構成は、パッケージで置き換えられません。

VeraCrypt のインストールと更新

- 同梱のインストーラーは、ビルド時に `scripts/fetch-veracrypt.py` で用意します。
- インストール前に、特権プロセスが組み込みの IDRIX キー（フィンガープリント `5069 A233 D55A 0EEB 174A 5FC3 821A CD02 680D 16DE`）で 公式 SHA-256 リストの OpenPGP 署名と、ファイルのハッシュを検証します。
- `kripta.toml` のオプション：`veracrypt_update_check = false` で更新確認を無効化。`veracrypt_release_api = "https://mirror.internal/…"` で GitHub API と同じ形式の社内ミラー

を使用。

言語

言語の XML ファイルは `app/ui/lang/`（アプリに同梱）と `docs/manuale/lang/` にあります。ユーザーが読み込んだ言語は ユーザーのデータフォルダー（ `languages/` ）に保存されます。新しい言語を全員に配布するには、ファイルを `app/ui/lang/` に追加し、 そのコードを `app/ui/i18n.js` の一覧に加えてください。

オプションのコンポーネント

- メニューバー / 通知領域での**サインイン時の起動**（ `kripta --background` ）：**自動**。Kripta は起動のたびに登録します（macOS：`~/Library/LaunchAgents/com.kripta.agent.plist` 、異常終了時は再起動；Windows：サインイン時に最上位の特権で実行するタスク「Kripta」、インストーラーでも作成され、アンインストール時に削除；Linux：.deb/.rpm パッケージの `/etc/xdg/autostart/kripta.desktop` 、AppImage は `~/.config/autostart/kripta.desktop` ）。設定でオフにできます。
- サービスとしての**特権ヘルパー**（パスワードの要求なし）：`deploy/macos/com.kripta.helper.plist` 、 `deploy/linux/kripta-helper.service` 。