Nozawa System

ファイル暗号化サイト
暗号化・復号システムの操作とセキュリティガイド

このサイトは、転送するファイルを暗号化するためのツールです。本ガイドでは、サイトの使用方法と安全に運用するための手順を説明します。

１．システムの基本動作

１．１暗号化の仕組み

■暗号化アルゴリズム：

ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）を使用しています。具体的には、ＡＥＳ－１２８ビットの鍵を用いたＣＢＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モードと、HMAC（Ｈａｓｈ－ｂａｓｅｄ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）による認証が行われます。

■暗号化キー：

‘ｃｒｙｐｔｏｇｒａｐｈｙ’ライブラリの‘Ｆｅｒｎｅｔ．ｇｅｎｅｒａｔｅ＿ｋｅｙ（）’で生成されるランダムな３２バイト（２５６ビット）の値が使用されます。

このキーは暗号化と復号の両方に必要なため、慎重に管理する必要があります。

１．２暗号化プロセス

１．２．１ユーザーがファイルをアップロードします。

１．２．２サーバーが暗号化キーを生成します（‘ｋｅｙ．ｔｘｔ’に保存)。

１．２．３各ファイルが暗号化され、‘．ｎｏｚａｗａｐｒｏｔｅｃｔ’拡張子が付与されます。

１．２．４ 暗号化ファイルと‘ｋｅｙ．ｔｘｔ’がＺＩＰファイルにまとめられ、ユーザーがダウンロードできるようになります。

１．３復号プロセス

１．３．１暗号化ファイル（‘．ｎｏｚａｗａｐｒｏｔｅｃｔ’）と対応する‘ｋｅｙ．ｔｘｔ’をサイトにアップロードします。

１．３．２サイトが‘ｋｅｙ．ｔｘｔ’を読み取り、暗号化ファイルを復号します。

１．３．３復号されたファイルがＺＩＰファイルとして提供されます。

Nozawa System

２．使用手順

２．１暗号化

２．１．１歳との暗号化画面を開きます。

２．１．２暗号化したいファイルを選択してアップロードします。

２．１．３ダウンロードリンクが生成されるので、以下の内容をダウンロードしてください：

‘ｋｅｙ．ｔｘｔ’（暗号化キー）

暗号化されたファイル（‘．ｎｏｚａｗａｐｒｏｔｅｃｔ’拡張子付きのデータ）

２．２復号

２．２．１サイトの復号画面を開きます。

２．２．２復号したい暗号化ファイルと対応する‘ｋｅｙ．ｔｘｔ’をアップロードします。

２．２．３復号されたファイルがＺＩＰファイルとしてダウンロードできます。

３．セキュリティガイド

３．１暗号化キー（‘ｋｅｙ．ｔｘｔ’）の管理

■分離保存：

暗号化データと‘ｋｅｙ．ｔｘｔ’を必ず別の場所に保存してください。

暗号化ファイルをクラウドストレージに保存する場合、‘ｋｅｙ．ｔｘｔ’はＵＳＢメモリやローカルストレージに保存します。

■安全な媒体に保存：

ＵＳＢメモリやHDDに保存する場合、物理的な安全性（例：暗証番号ロック付きのデバイス）を確保します。

パスワードで保護されたＺＩＰファイルに格納するのも有効です。

■共有の注意：

他者と暗号化データを共有する際、暗号化キーは別経路で共有します（例：暗号化メッセージサービス）。

３．２データのバックアップ

暗号化データと‘ｋｅｙ．ｔｘｔ’は、どちらかを失うとデータを復元できなくなります。安全な場所にバックアップを作成してください。

３．３キー管理ツールの活用

大量のデータを扱う場合は、鍵管理システム（KMS）や秘密管理ツール（例；　ＨａｓｈｉＣｏｒｐ　Ｖａｕｌｔ、AWS　KMS）の使用を検討してください。

３．４技術的注意点

■ＡＥＳ－１２８の安全性

ＡＥＳ－１２８は現時点での標準的な暗号化方式で、十分な安全性を提供します。ただし、鍵（‘ｋｅｙ．ｔｘｔ’）の保護が不十分だとセキュリティが損なわれます。

■キーの有効期限

長期間保存するデータに対しては、定期的に暗号化キーを更新することを推奨します。

４ＦＡＱ

Ｑ１．　‘ｋｅｙ．ｔｘｔ’を失った場合、どうすれば良いですか？

Ａ１．　‘ｋｅｙ．ｔｘｔ’がなければ暗号化されたデータを復号することはできません。バックアップを取得していない場合、そのデータは完全に失われます。

Ｑ２．暗号化データが漏洩しても安全ですか？

Ａ２．　暗号化キー（‘ｋｅｙ．ｔｘｔ’）が安全に管理されている限り、漏洩したデータが解読される可能性はほぼありません。

Ｑ３．他人にデータを共有したい場合、どうすれば良いですか？

Ａ３．暗号化データを共有し、‘ｋｅｙ．ｔｘｔ’は別の安全な経路で送信してください。号を安全に運用することができます。