2021 年 2 月

Web ドキュメント
保護ソリューション

説明書

目次

1. 暗号化 Web ドキュメントの閲覧

暗号化 Web ドキュメントは専用ブラウザで閲覧します。このブラウザは正しく設定された USB キーが接続されているときのみ起動します。USB キーがなければブラウザを使うことはできません。ブラウザが起動したら通常のブラウザと同じように Web サイトを閲覧できます。

ただし暗号化 Web ドキュメントを閲覧するには、USB キーの設定はドキュメントを暗号化した USB キーの設定と一致していなければなりません。 暗号化 Web ドキュメントがどこにあるのかは事前にブラウザに設定しておきます。例えば
ホスト www.ribig.cp のパス examples/ が設定されているとすると https://www.ribig.jp/examples/ 内のファイルやサブフォルダのファイルすべてが復号化されます。

送付 USB キーはサンプル暗号化ファイルを閲覧できるよう設定済みです。サンプル暗号化ファイルを含む場所も事前にブラウザに設定済みです。USB キーを接続して専用ブラウザを起動後、サンプル暗号化ドキュメントにアクセスしてみてください。各種サンプル暗号化ドキュメントのリンクは以下URLに記載されています。

https://www.ribig.jp/download.html

暗号化ドキュメントの種類
2つの方法のどちらかでデータは暗号化されます。

1. Web サーバにアップロード前にツールを使って手動で事前に暗号化
2. Web サーバから配信時に自動で動的に暗号化

事前暗号化したファイルはオンライン再生したり、別途ダウンロードしてローカル再生したりすることが可能です。動的暗号化したファイルはローカル再生はできません

動的暗号化には2つの方法があります。Web アプリ出力のように事前暗号化できないデータを Web アプリ自身で暗号化する方法、そして、プレーンな html/jsp 出力を出力時に Servlet コンテナの暗号化フィルタで自動暗号化する方法の2つです。後者ではコンテナが出力データを自動暗号化するため、プレーンなWebドキュメントを通常通りデプロイ

できます。Jsp アプリも暗号化を気にせずに通常通りプレーンテキストを出力をすることができます。

2. USB キー設定

送付 USB キーでサンプル暗号化 Web ドキュメントを閲覧できるのは、ドキュメントを暗号化した USB キーの設定と同じ設定になっているからです。

USB キーの設定はツールで変更できます。設定パラメータは保存できます。サンプルドキュメントを暗号化した USB キーの設定パラメータも保存されています。このため、USBキーの設定を変更しても、保存済み設定に戻すことが可能です。

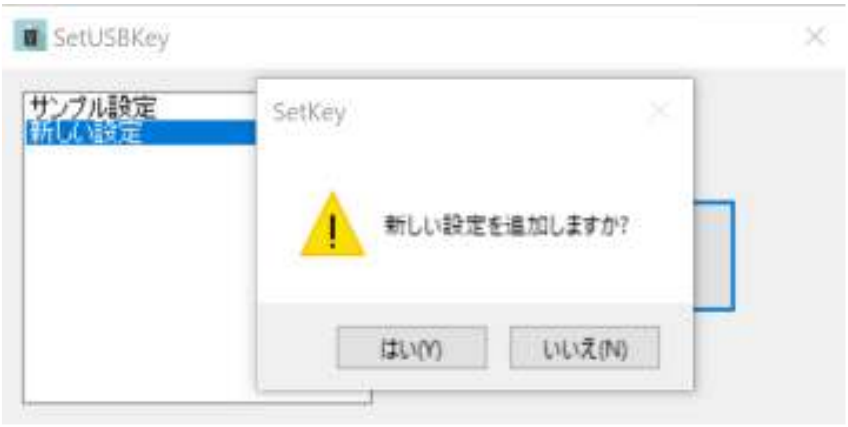
USB キーの設定をユーザ毎に変更することで、ユーザはお互いの暗号化ファイルを閲覧できなくなります。

USB キー設定変更ツール setUSBKey.exe
USB キー設定変更は setUSBKey.exe で行います。同じフォルダにファイル“uc.bin”がなければなりません。 起動前に最低1つの USB キーを接続してください。

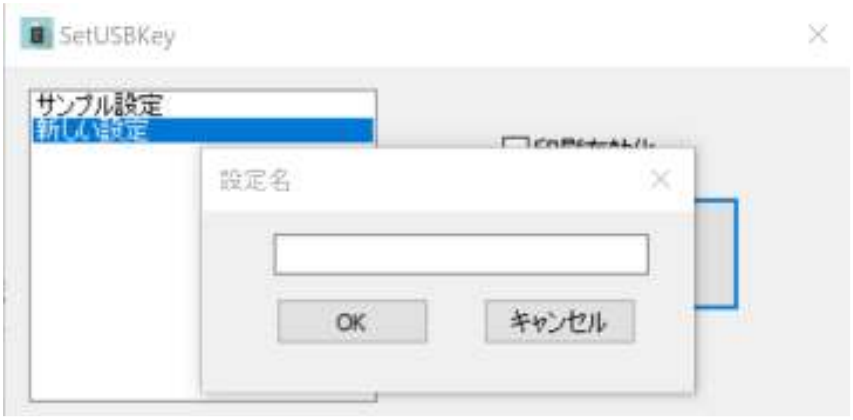
保存した設定ない状態はリストボックスでは ”新しい設定” だけが表示されます。サンプル設定が添付されている場合、“サンプル設定”が表示されます。

設定する USB キーを接続してください。複数本同時に接続しても構いません。

リストボックスで“新しい設定”が選択されていることを確認してから[USB キー設定] ボタンを選択すると USB キー設定が開始します。

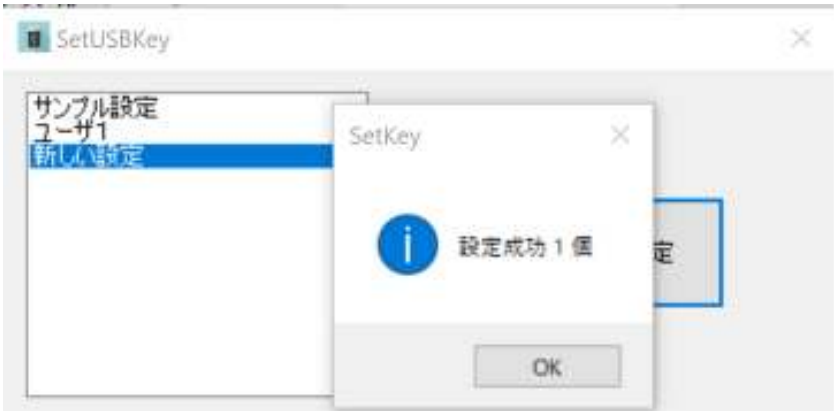


「はい」を選択すると USB キー設定が開始します。完了後、設定パラメータを保存するファイル名を入力します。



設定を保存しないと、同じ設定に USB キーを変更できなくなります。

例えば、“ユーザ1” と入力してから “OK”をクリックすると“ユーザ1”がリストボックスに追加されます。



＊設定名はそのままファイル名として使われます。設定名は全角文字で入力するか、半角文字で入力したらファイル名として許可されている文字だけを使うようにしてください。

＊設定は、setUSBkey.exe と同じフォルダに保存されます。
setUSBkey.exe は同じフォルダにある設定ファイルのみを読み込みます。

＊設定ファイル名は “(設定名).cfg” になります。設定情報を含む重要なファイルです。管理者のみがアクセスできるようにしてください。

＊設定名と同じ名前のフォルダが作成されます。このフォルダ内に動的暗号化に必要なファイルが作成されます。

“ユーザ1”で設定した USB キーでブラウザを起動して、サンプル暗号化 Web ドキュメントにアクセスしてみてください。ページは正しく表示されません。

既存設定を使った USB キーの設定

リストボックスで設定名を選択後、[USB キー設定]をクリックしてください。
USB キーは選択した設定と同一の設定になります。 “サンプル”を選択して USB キーを再設定すると、サンプル暗号化 Web ドキュメントを閲覧できるようになります。

印刷の有効化

設定する USB キーでブラウザを起動したときに印刷できるかどうかを指定します。チェックを付けて設定すると印刷が可能になります。印刷チェックボックスは接続USBキーの設定状態を反映しているわけではありません。これから設定する状態を示しています。

3. ファイル暗号化

“サンプル設定”以外の設定をした USB キーで暗号化 Web ドキュメントを閲覧できるようにするには、その USB キー、または、同じ設定の USB キーで Web ドキュメントを暗号化しなければなりません。

ファイルの暗号化は ツール matrix_enc.exe で行います。

matrix_enc.exe は、コンソールプログラムです。コマンドプロンプト / PowerShell プロンプトを開いて、コマンドを入力して実行してください。同じフォルダに ファイル”uc.bin”がなければなりません。

1. 起動前に USB キーを接続してください。

2. matrix_enc コマンド引数

   .¥matrix_enc 入力指定 出力指定

   入力指定 —— ファイル名、フォルダ名を指定できます

   出力指定 —— 入力指定がファイルであれば、ファイル名/フォルダ名
   入力指定がフォルダであればフォルダ名

   出力先にフォルダが見つからなければ作成します。

例1： 指定フォルダ以下すべてのフォルダ/ファイルを別フォルダに暗号化

.¥matrix_enc c:¥html c:¥html_user1

フォルダ c:¥html 以下のすべてのファイル、フォルダを
c:¥html_user1 に暗号化して保存します。フォルダ html_user1
構造は html 以下と同じフォルダ構造になります。

例 2：　個別ファイルの暗号化

.¥matrix_enc c:¥html¥index.html c:¥html_user1

index.html と同じ名前の暗号化ファイルがファルダ html_user1 に置かれます

例3：　個別ファイルの暗号化

.¥matrix_enc c:¥html¥index.html c:¥html_user1¥index1.html

C:¥html¥index.html が暗号化ファイル index1.html 名で c:¥html_user1 に置かれます

例4：　ワイルドカード

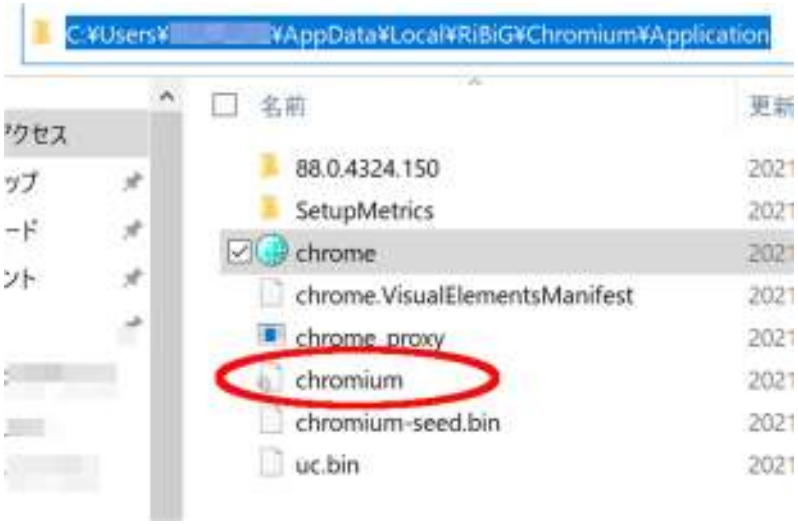
.¥matrix_enc c:¥html¥.html c:¥html_user1*

拡張子が .html のファイルを暗号化して同名の暗号化ファイルを c:¥html_user1 フォルダに作成します。

4. ブラウザ設定

暗号化したファイルはブラウザで設定されたパスに置かなければ、ブラウザは復号化しません。

暗号化ファイルを置く場所は、ブラウザの実行ファイルと同じフォルダにある chromium.ini で指定します。



このファイルをテキストエディタで開いてください。

```
[LocalEncryptedFolder]
Folder0=c:¥myweb¥htdocs¥

[WebEncryptedPath]
Path0=www.ribig.jp/examples/
Path1=www.ribig.co.jp/test/test/
```

＊ ローカルパスの末尾の¥ はフォルダを表すために必須です
＊ Web パスの末尾の / はフォルダを表すために必須です

暗号化ファイルを置くローカルフォルダは[LocalEncryptedFolder]セクションで、Web パスは[WebEncryptedPath]で指定します。 ローカルフォルダは Folder0, Folder1, Folder2 .. Path7 まで指定できます。Web パスは 0 から最大15まで指定できます。番

号は0から順番に振ってください。 Path0 を指定せずに Path1 から始めてしまうと何も指定したことにはなりません。途中で番号をスキップするとその時点で指定は終了してしまいます。

[LocalEncryptedFolder]セクションで指定したローカルフォルダに暗号化ファイルを置き、暗号化した USB キーを接続してブラウザを起動してください。

file:///c:/myweb/htdocs/xxx.html

などとして暗号化ファイルを開いて正しく表示されれば成功です。

[WebEncryptedPath]セクションで指定した Web サーバのパスに暗号化ファイルをアップロードしてブラウザでアクセスしてみてください。 正しく表示されれば成功です。

指定フォルダ/Web パス以外へのアクセスは通常のブラウザとして動作します。

5. 動的暗号化

スタティックコンテンツとは異なり、Web アプリの出力を事前に暗号化するのは容易ではありません。そこで、事前にデータを暗号化するのではなく、データを都度暗号化して出力する方法が用意されています。

方法1:
PHP の Web アプリは出力をバッファリングできます。 バッファリングを有効にすると出力したデータはクライアントに送られずにバッファに書き込まれます。 出力処理が完了したら、バッファ内のデータを暗号化してからクライアントに出力することで動的暗号化が可能です。

暗号化クラス webprotect.php を提供します。 Web サーバには USB キー設定時に設定名と同じフォルダ内に生成された chromium-seed.server を配置します。 webprotect.php はこのファイルを使って暗号化処理を行います。また、ブラウザの実行ファイルと同じフォルダの chromium-seed.bin を USB キー用のものに置き換えます。

コード例:

```
<?php
require ”webprotect.php”;

// 出力バッファリング有効化
ob_start();

// create the encryption instance
$wp = new WebProtect();

header(”Content-Type: text/html; charset=UTF-8”);
$wp->setHeaders();

printAuthPage();

// バッファデータ取得
$output = ob_get_contents();
ob_end_clean();

// 取得したデータの暗号化と出力
header(”Content-Length: ” . strlen($output ) );
echo $wp->encBuffer($output);
exit;

function printAuthPage()
{
?>

<html>
<head>
<title>動的ページの暗号化</title>
</head>
<body>
```

```
<div style="padding:5px">
USB キーの PIN を入力してください
<p/>
<form method="post" >
<input type="password" name="pin" size="8" maxlength="6" />
<button id="submit" name="submit">了解</button>
</form>
<p>
</div>

</body>
</html>
<?php
}
?>
```

方法2：
Tomcat コンテナで暗号化フィルタを設定すると、コンテナ内に配置したスタティックコンテンツ、Web アプリの出力は暗号化フィルタで暗号化されてからクライアントに送られるようになります。事前にファイルを暗号化したり、Web アプリで出力を暗号化する必要はありません。

暗号化フィルタ クラスファイルを提供します。 Web サーバには USB キー設定時に設定名と同じフォルダ内に生成された chromium-seed.server を配置します。フィルタははこのファイルを使って暗号化処理を行います。また、ブラウザの実行ファイルと同じフォルダの chromium-seed.bin を USB キー用のものに置き換えます。

Tomcat の暗号化フィルタが有効になるパスは、ブラウザで指定する暗号化パスに含まれなければなりません。

＊動的暗号化関連ファイル・サポートは有償版のみに含まれます。