暗号 DLL

WILL

株式会社ウィル

白紙ページ

白紙ページ

目 次

はじめに 3
商品に含まれるもの 5
動作環境について 6
インストール 7
ライセンスの登録 10
サンプルを見る 11
サポートについて（無償） 12
バージョンアップについて（無償） 13
実行時に必要なファイル 15
再配布について 15

製品概要 16
特 徴 18

プログラミング概要 20
宣 言 22
暗号化および復号化 23
要約値の計算 25
エラー処理 26

プロパティ 28
Error プロパティ 30
ErrorMessage プロパティ 31
Copyright プロパティ 32

メソッド 34
OpenRC4 メソッド 36
Encrypt メソッド 37
Decrypt メソッド 38
CloseRC4 メソッド 39
GetCSPName メソッド 40
OpenDigest メソッド 41
AddDigest メソッド 42
GetDigestValue メソッド 43
GetDigestHexString メソッド 44
CloseDigest メソッド 45

エラーコード 46
発生しうるエラーコード 48

サンプル 50

WillCrypt 52
暗号 DLL for VB Script(ASP)サンプル 53

索　引 56

はじめに

白紙ページ

商品に含まれるもの

1．CD-ROM
- Willware.exe
  （暗号 DLL 開発環境用セットアップキット）
- Cryptdll.exe
  （暗号 DLL 実行環境用セットアップキット）
- readme.txt

2．使用許諾契約書

3．マニュアル

動作環境について

■対応 OS

暗号 DLL は、以下に示す OS で動作確認を行っております。

Microsoft Windows 95、Microsoft Windows 98、
Microsoft WindowsNT 4.0、Microsoft Windows 2000
Microsoft Windows XP、Microsoft Windows 2003
Active Server Pages(ASP)

暗号 DLL を使用するには Microsoft RSA Base Provider が必要です。Microsoft RSA Base Provider は、Windows 95(OSR2 以降または IE3.02 以降)、Windows 98、Windows NT 4.0、Windows 2000、Windows XP で動作します。

■開発に必要なソフトウェア

暗号 DLL をご使用いただくには、以下のいずれかのソフトウェアが必要です。

Microsoft Visual Basic Ver 5.0
Microsoft Visual Basic Ver 6.0
Microsoft Office 2000 (Access、Excel)
Microsoft Visual Basic Scriting Edition (VB Script) Ver3 以上

■参照設定

暗号 DLL を利用する際に参照設定が必要になる場合があります。その場合はプロジェクトの参照設定で WILL CRYPT DLL にチェックしてください。

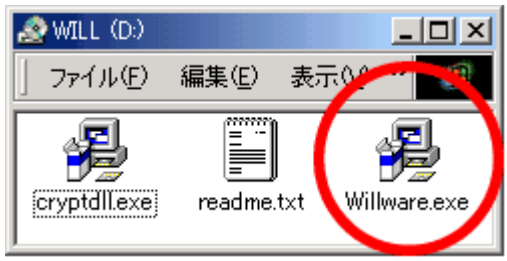
暗号 DLL は、Microsoft Visual C++ Ver 5.0 で作成しています。サンプルは、Microsoft Visual Basic Ver 5.0 で作成しています。
※ 本製品は日本語環境のみの対応となります。

インストール

暗号 DLL のインストールは、開発環境と実行環境によって、利用するセットアップファイルが異なります。

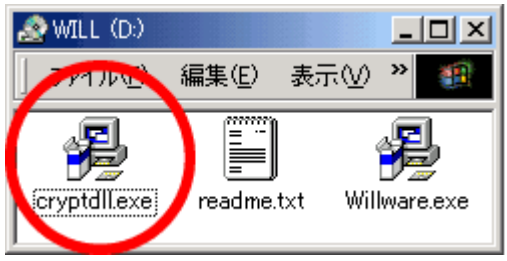
■開発環境へのインストール

Willware.exe を利用してインストールを行います。WILLWAREComponents 全製品及びそれに付随するマニュアルやサンプルがインストールされます。



■実行環境へのインストール

Cryptdll.exe を利用してインストールします。暗号 DLL のマニュアル及びサンプルはインストールされません。

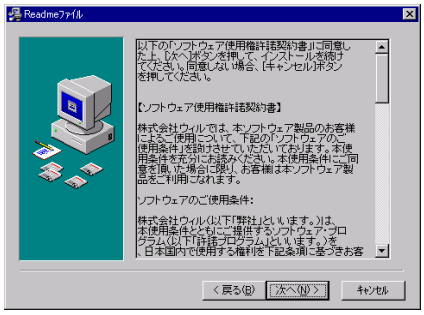


■インストールの手順

画面にしたがって、インストールを進めて下さい。

1. インストールを始めます。「次へ」をクリックして下さい。

2. 使用許諾契約書です。内容に同意される場合は「次へ」をクリックして下さい。



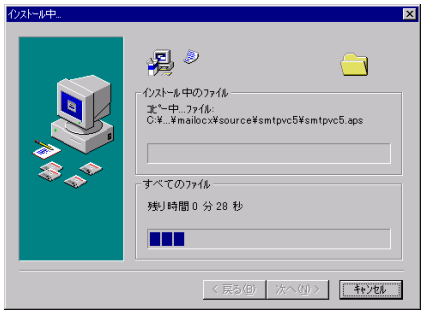
3. インストール先のフォルダを指定します。初期設定でよろしければ「次へ」をクリックして下さい。別のフォルダを指定したい場合は「参照」をクリックし、フォルダを指定して下さい。

4. インストール中に置換されるファイルのバックアップを作成できます。そのバックアップファイルの保存先フォルダを指定します。初期設定でよろしければ「次へ」をクリックして下さい。

5. WILLWARE Components を登録するスタートメニュー又はプログラムマネージャのグループフォルダを指定します。初期設定では、新規に「WILLWARE Components」の名前でフォルダを作成します。特に指定する必要がなければ、初期設定をお勧めします。

6. プログラムのコピーを開始します。「次へ」をクリックして下さい。

7. プログラムのコピーをしています。中断する場合は、「キャンセル」をクリックして下さい。



8. インストールが完了しました。「完了」をクリックし、インストールを終了して下さい

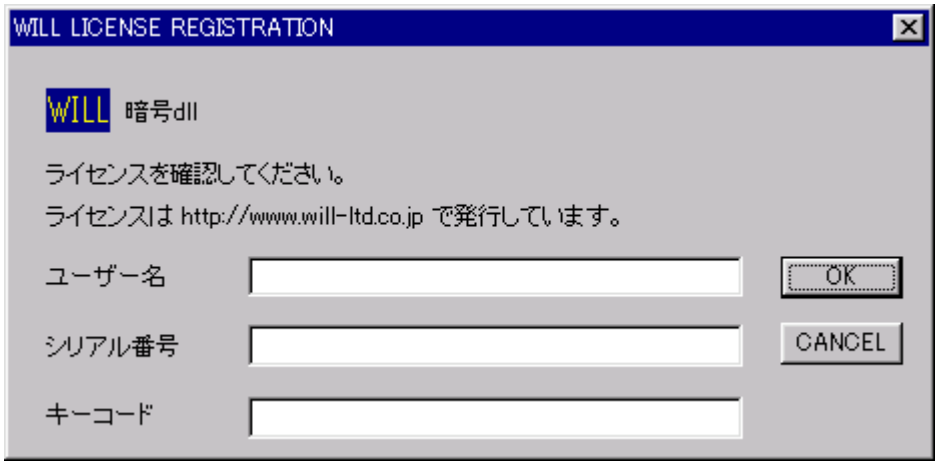
ライセンスの登録

ライセンスを登録します。

スタートメニューより、「プログラム」→「WILLWARE Components」→「ライセンス登録」→「暗号 DLL」を起動してください。

以下の「WILL LICENSE REGISTRATION」画面が起動しますので、ソフトウェア使用許諾契約書に明記されている「ユーザー名」、「シリアル番号」、「キーコード」を入力してください。

トライアルライセンスから正規ライセンスへ移行する場合も、こちらの画面で登録を行ってください。



■ライセンス入力時のご注意

※ライセンスが入力できない！？

入力したライセンスにスペースが含まれていないか確認して下さい。

（ライセンスに、スペースは使用していません。）

サンプルを見る

インストールが完了すると、スタートメニューに「WILLWARE Components」が追加されます。

「WILLWARE Components」の「サンプル」を起動すると「WILLWARE Components サンプル」画面が表示されます。サンプルの起動、またはそれぞれのソースを開くことができます。但し、ソースを開くにはライセンスが必要です。トライアルライセンス又は、正規ライセンスを登録してご利用下さい。（ライセンスの登録方法は前項の「ライセンスの登録」をご覧下さい。）

サポートについて（無償）

サポートは基本的に電子メールで受け付けております。サポートは無償でご利用いただけます。

■お問い合わせの前に

サポート作業を円滑に行うために、お問い合わせの際には以下の情報をご用意下さい。

1. 製品名及びバージョン
2. 開発環境（OS の種類及びバージョン、サービスパッケージの種類）
3. 開発ツール及びバージョン
4. サーバーの種類
5. 問題点
   (1) エラー内容又は、エラー状況のハードコピー
   (2) 問題点となる部分のサンプルソースコード

■FAQ

弊社ホームページの「サポート」のページで、キーワードを入力して FAQ を検索できます。休業日などサポートの対応が遅れる場合もありますので、まずはこちらをご確認下さい。

■お問合せ先

info@will-ltd.co.jp

バージョンアップについて（無償）

製品のバージョンアップは、すべて無償です。

■バージョンアップ情報の入手方法

バーションアップの情報は、弊社ホームページの新着情報で通知し、各商品のページの更新履歴で更新内容を掲示致します。

■最新バージョンの入手方法

最新バージョンのプログラムは、弊社ホームページ（http://www.will-ltd.co.jp/）のダウンロードのページよりダウンロードすることが出来ます。ダウンロードするファイルは、以下のバージョンアップの目的により異なりますのでご注意下さい。

開発環境でのバージョンアップ

● **WILLWARE Components（全製品）のバージョンアップ**

ダウンロードファイル名　：「Willware.exe」

「Willware.exe」は全ての製品の最新版をインストールするためのものです。そのため本製品以外の製品及びサンプル、マニュアルも同時にバージョンアップされます。

● **暗号 DLL 単体のバージョンアップ**

ダウンロードファイル名　：「Cryptdll.exe」

「Cryptdll.exe」は暗号 DLL の dll ファイル及び依存ファイルのみの最新版をインストールするためのものです。サンプル及びマニュアルはバージョンアップされませんのでご注意下さい。

実行環境でのバージョンアップ

● **暗号 DLL 単体のバージョンアップ**

ダウンロードファイル名　：「Cryptdll.exe」

暗号 DLL の dll ファイル及び、依存ファイルがバージョンアップされます。

■バージョンアップをする前に

各セットアップキットを利用してバーションアップをする前に、以下のことにご注意下さい。

● **WILLWARE Components（全製品用）セットアップキット**を利用してバージョンアップする場合は、古いバージョンをアンインストールしてから、最新バージョンをインストールすることをお勧めいたします。
※ アンインストールの方法は、スタートメニューから「設定」→「コントロールパネル」→「アプリケーションの追加と削除」の画面で、「WILLWARE Components」を選択し、画面の指示に従って行って下さい。

● **各コンポーネント毎のセットアップキット**を利用してバージョンアップする場合は、最新バージョンをそのままインストールして下さい。古いファイルは上書きされます。
※ 弊社製品を複数ご利用いただいている場合、いずれか１つをバーションアップしても他の製品に影響はありません。

■バージョンアップの方法

セットアップキットをダブルクリックし、画面の指示に従ってインストールを進めて下さい。

実行時に必要なファイル

暗号 DLL は ATL を用いて作成していますので、実行時に暗号.dll 以外に必要なファイルはありません。

再配布について

■作成したアプリケーションの配布時

作成したアプリケーションに本プログラムを組み込んで再配布した場合、実行するマシン毎にライセンスが必要になります。

■著作権

- 暗号 DLL およびこれに付随するマニュアルの著作権は株式会社ウィル（横浜市保土ヶ谷区）にあります。
- 本ソフトウエアおよびマニュアルを運用した結果については、当社は一切責任を負いません。
- 本ソフトウエアの仕様またはマニュアルに記載されている事項は予告無く変更することがあります。
- マニュアルなどに記載されている会社名、製品名は、各社の商標および登録商標です。
- 暗号 DLL を利用するアプリケーションは暗号 DLL の著作権表示を行わなければなりません。Copyright プロパティに暗号 DLL の著作権を示す文字列があります。アプリケーションまたはドキュメントのいずれかにこの文字列を表示して、暗号 DLL を使用していることを示してください。

製 品 概 要

白紙ページ

特 徴

暗号 DLL は、データの暗号と復号、およびデータの要約値の計算を行うためのインプロセス Active X オートメーションサーバーです。VB や VC++はもとより ASP などのスクリプト環境からも利用できます。

暗号 DLL の暗号方式は米 RSA 社の RC4 と呼ばれる暗号方式です。RC4 は SSL でも採用されていて、高速であること、バイト単位のデータの暗号化ができること、40 ビットから 128 ビットまでの暗号強度を選択できることなどが特徴です。RC4 の鍵は秘密鍵（共通鍵）方式で、いわゆるパスワードを用いて暗号を行います。

暗号 DLL は、Microsoft Cryptographic Provider を利用しています。

暗号 DLL は暗号 OCX と暗号データに互換性があります。暗号 OCX で暗号化したデータを暗号 DLL で復号化することやその逆を行うことができます。

要約値の計算は、MD5 および SHA-1 の2つの方法から選択できます。要約値は、データに固有な値を表現しますので、データの同一性を保証するためやデータの改竄（かいざん）を検出するために利用されます。

白紙ページ

プログラミング概要

白紙ページ

宣 言

VB における宣言の方法は 4 種類あります。

その1	Dim Crypt1 As New WILLCRPT
その 2	Dim Crypt1 As WILLCRPT Set Crypt1 = New WILLCRPT
その 3	Dim Crypt1 As WILLCRPT Set Crypt1 = CreateObject("WILLCRPT")
その 4	Dim Crypt1 As Object Set Crypt1 = CreateObject("WILLCRPT")

VBScript(ASP)の場合の宣言の方法

```
Dim Crypt1
Set Crypt1 = Server.CreateObject("WILLCRPT")
```

暗号化および復号化

暗号化する手順は

1. OpenRC4 メソッド
2. Encrypt メソッド（必要に応じて繰り返し呼び出す）
3. CloseRC4 メソッド

です。
暗号結果は Encrypt メソッドに渡した変数に戻されます。

OpenRC4 メソッドでパスワード、パスワードのハッシュ方法、暗号強度、文字データを暗号化した場合の出力フォーマットを指定します。パスワードは、Unicode で指定してください。このパスワードのハッシュ値（要約値またはダイジェスト値とも呼ぶ）を用いて暗号化します。

ハッシュ方法は、MD5 と SHA-1 のいづれかを選択できます。MD5 を利用するときは、0 を、SHA-1 を利用するときは、1 をパスワードのハッシュ方法として指定してください。

暗号強度は、40 から 128 までの値を指定できますが、利用できる暗号プロバイダ (Cryptographic Provider)によって指定できる値に制限があることがあります。

暗号プロバイダー名	利用できる強度(ビット数)
Microsoft Base Cryptographic Provider v1.0	40,128
Microsoft Base Cryptographic Provider v1.0	40-56,128
Microsoft Enhanced Cryptographic Provider	40-128
Microsoft Strong Cryptographic Provider	40-128

「Microsoft Base Cryptographic Provider v1.0」は 2 種類あり、初期のもの(IE4.0 以前に附属のもの)は 40 または 128 ビットしか指定できません。強度と互換性を考えると、128 ビットを選択するのが良いでしょう。暗号プロバイダを確認するには、GetCPSName メソッドを呼び出してください。GetCPS メソッドはいつでも呼び出すことができます。

暗号化するデータが文字列の場合、そのまま暗号化すると、暗号結果が文字列としては正しくなくなる場合があります。暗号後も文字列として扱いたい場合は、出力フォーマットに 0 を指定することで、16 進文字列として暗号結果を格納することができます。(デフォルト)ただし、この場合、出力される文字列の長さは暗号前の長さの 2 倍になるので、格納するエリアの大きさに注意してください。

逆に、暗号結果をバイナリ文字列として扱いたい場合は 1 を指定してください。この場合、暗号前の文字列の長さと暗号後の文字列の長さは同じになります。

データを暗号化するには、Encrypt メソッドを呼び出します。引数は、ユーザー定義型、オブジェクト型を除くすべての型とその一次元配列（ただしバリアントおよび文字列の配列は除く）を指定できます。暗号化した結果はもとの変数に格納されます。大きなファイルを暗号化する場合や、ネットワークで転送しながら暗号化する場合には、データを小分けにして複数回 Encrypt メソッドを呼び出してください。分ける最小単位はバイトです。効率を考えてある程度の大きさでわけると良いでしょう。

暗号化が終了したら CloseRC4 メソッドを呼び出してください。このメソッドを呼び出さないと再度 OpenRC4 メソッドを呼び出すことができません。

復号化する手順は

1. OpenRC4 メソッド
2. Decrypt メソッド（必要に応じて繰り返し呼び出す）
3. CloseRC4 メソッド

です。

復号結果は Decrypt メソッドに渡した変数に戻されます。

復号化では暗号化を行ったパラメータを使って OpenRC4 メソッドを呼び出してください。ことなるパラメータを使うとエラーにならずに異なる結果を生み出します。

ただしく復号されたかどうかを知るには、暗号するデータにチェック用のデータを忍ばせておくのが良いでしょう。正しく復号化できたときだけ正しいチェック用のデータが得られます。

要約値の計算

要約値は、データに依存する 16 バイトまたは 20 バイトの値です。

要約値を計算する手順は OpenDigest メソッド

1. AddDigest メソッド（必要に応じて繰り返し呼び出す）
2. GetDigestValue メソッドまたは GetDigestHexString メソッド
3. CloseDigest メソッド

です。

要約値の計算方法は 2 つあります。MD5 と SHA-1 です。AddDigest で要約計算対象となるデータを渡します。大きなファイルの要約値を計算する場合はデータを小分けにして複数回 AddDigest メソッドを呼び出してください。分ける最小単位はバイトです。効率を考えてある程度の大きさでわけると良いでしょう。

要約値を取り出すには、GetDigestValue メソッドまたは GetDigestHexString メソッドを使います。GetDigestValue メソッドはバイナリ文字列、GetDigestHexString メソッドは 16 進文字列を返します。

エラー処理

暗号 DLL はトラップ可能なエラーを発生しません。そのかわり、各メソッドの戻り値でエラーかどうかを判定できるようにしています。エラーが発生した場合は、戻り値、Error プロパティの値、ErrorMessage プロパティの値を確認してください。

白紙ページ

プロパティ

白紙ページ

Error プロパティ

■機　能

エラーコードが格納されています。

■構　文

Object.Error
Error プロパティの構文の指定項目は次のとおりです。

(指定項目)	(内　容)
Object	暗号 DLL オブジェクトです。

■データ型

長整数(Long)

ErrorMessage プロパティ

■機　能

エラーの説明が格納されています。

■構　文

Object.ErrorMessage
ErrorMessage プロパティの構文の指定項目は次のとおりです。

(指定項目)	(内　容)
Object	暗号 DLL オブジェクトです。

■データ型

文字列(String)

Copyright プロパティ

■機　能

暗号 DLL のバージョン番号が格納されています。

■構　文

Object.Copyright
Copyright プロパティの構文の指定項目は次のとおりです。

(指定項目)	(内　容)
Object	暗号 DLL オブジェクトです。

■データ型

文字列(String)

白紙ページ

メソッド

白紙ページ

OpenRC4 メソッド

■機　能

RC4 暗号及び復号を行う為の準備を行います。

■構　文

Object.OpenRC4(PassWord As String, HashAlgorithm As Long, Bits As Long, [Format])
OpenRC4 メソッドの構文の指定項目は次のとおりです。

(指定項目)	(内　容)
Object	暗号 DLL オブジェクトです。
PassWord	パスワードです。
HashAlgorithm	ハッシュアルゴリズムです。 0:MD5 1:SHA
Bits	暗号強度(40 から 128 の間の数値)です。
Format	変換フォーマットです。 0:HEX 1:なし

■戻り値

長整数(Long)。戻り値が示す値は以下の通りです。

(値)	(説　明)
0	正常
0 以外	エラー

■解　説

Encrypt,Decrypt をおこなう前にかならず実行します。暗号強度は、40 から 128 までの間の数値を指定できますが、57 から 127 までの値を設定する場合は、Windows の暗号強度を 128 ビットにしておく必要があります。サポートしていない強度を選択するとエラーになります。CRYPTOCX と互換を取るには、40 または 128 を指定してください。(40 の時は CreateSalt を False に、128 のときは、CreateSalt を True に設定したものに対応します。)変換フォーマットは、文字列の暗号化にのみ有効です。Encrypt と Decrypt は同じフォーマットを選択する必要があります。

Encrypt メソッド

■機　能

データを暗号化します。

■構　文

Object.Encrypt(Data)
Encrypt メソッドの構文の指定項目は次のとおりです。

(指定項目)	(内　容)
Object	暗号 DLL オブジェクトです。
Data	暗号化する任意の変数です。

■戻り値

長整数(Long)。戻り値が示す値は以下の通りです。

(値)	(説　明)
0	正常
0 以外	エラー

■解　説

Data には、任意の変数（1 次元配列も含む）を指定できます。（Object 型、ユーザー指定型、文字列型の配列、VARIANT 型の配列は除きます。）Data に文字列を指定した場合、OpenRC4 で指定した Format に従った変換を行います。暗号結果は元の変数に格納します。

Decrypt メソッド

■機　能

データを復号化します。

■構　文

Object.Decrypt(Data)
Decrypt メソッドの構文の指定項目は次のとおりです。

(指定項目)	(内　容)
Object	暗号 DLL オブジェクトです。
Data	復号化する任意の変数です。

■戻り値

長整数(Long)。戻り値が示す値は以下の通りです。

(値)	(説　明)
0	正常
0 以外	エラー

■解　説

Data には、任意の変数（1 次元配列も含む）を指定できます。（Object 型、ユーザー指定型、文字列型の配列、VARIANT 型の配列は除く）Data に文字列を指定した場合、OpenRC4 で指定した Format に従った変換を行います。復号結果は元の変数に格納します。

CloseRC4 メソッド

■機　能

暗号・復号処理を終了します。

■構　文

Object.CloseRC4()

CloseRC4 メソッドの構文の指定項目は次のとおりです。

(指定項目)	(内　容)
Object	暗号 DLL オブジェクトです。

■戻り値

長整数(Long)。戻り値が示す値は以下の通りです。

(値)	(説　明)
0	正常
0 以外	エラー

■解　説

RC4 暗号処理のための資源を解放します。

GetCSPName メソッド

■機　能

CSP(CryptographicServiceProviders)名を取得します。

■構　文

Object.GetCSPName
GetCSPName メソッドの構文の指定項目は次のとおりです。

(指定項目)	(内　容)
Object	暗号 DLL オブジェクトです。

■戻り値

文字列(String)

OpenDigest メソッド

■機　能

要約を得るための準備を行います。

■構　文

Object.OpenDigest(HashAlgorithm As Long)
OpenDigest メソッドの構文の指定項目は次のとおりです。

(指定項目)	(内　容)
Object	暗号 DLL オブジェクトです。
HashAlgorithm	ハッシュアルゴリズム 0:MD5 1:SHA

■戻り値

長整数(Long)。戻り値が示す値は以下の通りです。

(値)	(説　明)
0	正常
0 以外	エラー

AddDigest メソッド

■機　能

データの要約値を計算します。

■構　文

Object.AddDigest(Data)
AddDigest メソッドの構文の指定項目は次のとおりです。

(指定項目)	(内　容)
Object	暗号 DLL オブジェクトです。
Data	ダイジェスト値を計算する任意の変数です。

■戻り値

長整数(Long)。戻り値が示す値は以下の通りです。

(値)	(説　明)
0	正常
0 以外	エラー

■解　説

Data には、任意の変数(1 次元配列も含む)を指定できます。
(Object 型、ユーザー指定型、文字列型の配列、VARIANT 型の配列は除きます)。

GetDigestValue メソッド

■機　能

ダイジェスト値をバイナリとして取り出します。

■構　文

Object.GetDigestValue()
GetDigestValue メソッドの構文の指定項目は次のとおりです。

(指定項目)	(内　容)
Object	暗号 DLL オブジェクトです。

■戻り値

Variant。戻り値が示す値は以下の通りです。

(値)	(説　明)
""	エラー
""以外	正常。バイナリ文字列が格納されます。

■解　説

MD5 の場合は 16 バイト、SHA の場合は 20 バイトになる

GetDigestHexString メソッド

■機　能

要約値を 16 進文字列として取り出します。

■構　文

Object.GetDigestHexString
GetDigestHexString メソッドの構文の指定項目は次のとおりです。

(指定項目)	(内　容)
Object	暗号 DLL オブジェクトです。

■戻り値

文字列(String)。戻り値が示す値は以下の通りです。

(値)	(説　明)
""	エラー
""以外	正常

■解　説

MD5 の場合は 32 文字、SHA の場合は 40 文字になります。

CloseDigest メソッド

■機　能

要約処理を終了します。

■構　文

Object.CloseDigest()
CloseDigest メソッドの構文の指定項目は次のとおりです。

(指定項目)	(内　容)
Object	暗号 DLL オブジェクトです。

■戻り値

長整数(Long)。戻り値が示す値は以下の通りです。

(値)	(説　明)
0	正常
0 以外	エラー

■解　説

ダイジェスト値計算処理のための資源を解放します。

エラーコード

白紙ページ

発生しうるエラーコード

メソッド名	戻値	ErrorMessage
OpenRC4	-1	すでにオープンしています
	-2	HashAlgorithm の値が範囲外です
	-3	Bits の値が範囲外です。
	-4	ライセンスが正しくありません
	-10	API エラー
	-11	API エラー
AddDigest	-2	オープンしていません
	-3	文字列の配列は扱うことができません
	-4	バリアントの配列は扱うことができません
	-5	一次元配列以外は扱うことができません
	-6	取り扱えない変数です
	-7	取り扱えない変数です
	-8	API エラー
	-9	API エラー
	-10	API エラー
GetDigestHexString	""	オープンしていません
	""	API エラー
GetDigestValue	""	オープンしていません
	""	API エラー
Encrypt	-2	オープンしていません
	-3	文字列の配列は扱うことができません
	-4	バリアントの配列は扱うことができません
	-5	一次元配列以外は扱うことができません
	-6	取り扱えない変数です
	-7	取り扱えない変数です
	-8	API エラー
	-9	API エラー
	-10	API エラー
	-11	API エラー
	-12	API エラー
Decrypt	-2	オープンしていません

	-3	文字列の配列は扱うことができません
	-4	バリアントの配列は扱うことができません
	-5	一次元配列以外は扱うことができません
	-6	取り扱えない変数です
	-7	取り扱えない変数です
	-8	API エラー
	-9	API エラー
	-10	API エラー
	-11	API エラー
	-12	API エラー

サンプル

WillCrypt

（Ver1.00）

WillCrypt は、RC4(データ)の暗号化と復号化するサンプルです。

■使い方

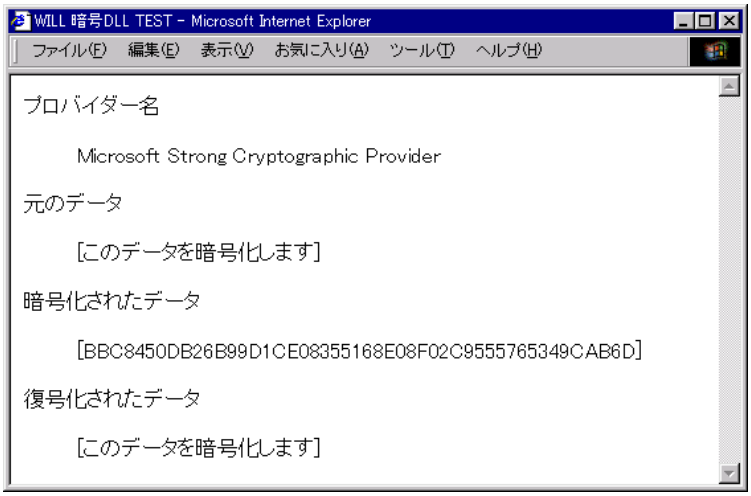
1. 暗号したい文を「平文」に入力して下さい。
2. パスワードを指定して下さい。
3. 128 ビットを指定する場合は、チェックボックスにチェックをつけてください。
4. 「暗号化」ボタンを押すと。入力した文が暗号化されます。
5. 「複合化」ボタンを押すと暗号化された文が複合化されます。

暗号 DLL for VB Script (ASP) サンプル

(Ver1.00)

暗号 DLL を VB Script でコーディングする為のサンプルです。

■ サンプル表示画面



■ サンプルソースコード

```
<HTML>
<HEAD><TITLE>WILL  暗号 DLL TEST</TITLE></HEAD>
<BODY>
<%
        Dim CSP,ORG,ENC,DEC,ERRNUM,ERRMSG
        Dim pass,hash,bits,obj

        pass = "password"
        hash =    0 'MD5
        bits = 128 '暗号強度
        ORG = "このデータを暗号化します" '平文

        '暗号 DLL のインスタンスを得る
        Set obj = Server.CreateObject("WILLCRPT")

        'プロバイダー名を得る
        CSP = obj.GetCSPName

        DO
                '暗号化する
                ERRNUM = obj.OpenRC4(pass,hash,bits)
                If ERRNUM <> 0 Then Exit Do
```

```
                    ENC= ORG
                    ERRNUM = obj.Encrypt(ENC) 'ENC に暗号結果が格納される
                    If ERRNUM <> 0 Then Exit Do
                    obj.CloseRC4

                    '復号化する
                    ERRNUM = obj.OpenRC4(pass,hash,bits)
                    If ERRNUM <> 0 Then Exit Do
                    DEC = ENC
                    ERRNUM = obj.Decrypt(DEC) 'DEC に復号結果が格納される
                    If ERRNUM <> 0 Then Exit Do
                    obj.CloseRC4
        Loop While(0)

        'エラーメッセージを得る
        If ERRNUM <> 0 Then
                ERRMSG = obj.ErrorMessage
        End If
%>
        <p>プロバイダー名 </p>
        <blockquote>
          <p><% = CSP %></p>
        </blockquote>
<%
        If ERRNUM = 0 Then
%>
        <p> 元のデータ</p>
        <blockquote>
          <p>[<% = ORG %>]</p>
        </blockquote>
        <p> 暗号化されたデータ</p>
        <blockquote>
          <p>[<% = ENC %>]</p>
        </blockquote>
        <p> 復号化されたデータ</p>
        <blockquote>
          <p>[<% = DEC %>]</p>
        </blockquote>
<%
        Else
%>
        <p><BR>
          エラーが発生しました。 </p>
        <blockquote>
          <p> <% = ERRMSG %>(<% = ERRNUM %>) </p>
        </blockquote>
<%
        End If
%>
</BODY>
</HTML>
```

索 引

AddDigest メソッド 42
CloseDigest メソッド 45
CloseRC4 メソッド 39
Copyright プロパティ 32
Decrypt メソッド 38
Encrypt メソッド 37
ErrorMessage プロパティ 31
Error プロパティ 30
GetCSPName メソッド 40
GetDigestHexString メソッド 44
GetDigestValue メソッド 43
OpenDigest メソッド 41
OpenRC4 メソッド 36

暗号 DLL マニュアル

2002 年 4 月 12 日 初版第 1 版
発行所　株式会社ウィル
住所 神奈川県横浜市保土ヶ谷区西久保町 15
グランディシンヤ 302
〒240－0022
TEL：045－338－3525
FAX：045－338－3526
Mail-Address：info@will-ltd.co.jp
URL：http://www.will-ltd.co.jp /
発行者　小川 史彦