

データ圧縮ツール「縮丸」ご紹介資料

圧縮／暗号技術・インターフェース説明資料



株式会社 富士通アドバンストソリューションズ



目次

1. 特長

- (1) 圧縮技術の特長 -1
- (2) 暗号化技術の特長 -2
- (3) 性能面での特長 -2

2. 圧縮／暗号技術

- (1) 暗号化とは -3
- (2) 暗号化アルゴリズム
 - ①AES -4
 - ②トリプルDES -5
 - ③SC2000 -6
- (3) 縮丸の圧縮技術 -7
- (4) FLDC/SLCの原理 -8

3. インターフェース -9



1.特徴①

(1) 圧縮技術の特長

●マルチプラットフォームサポート

GS/M,Solaris,Windows Server 2008,Windows Vista,Windows 7等の幅広いOSに対応し、異機種間での圧縮形式データの流通が可能です。

(http://jp.fujitsu.com/group/fasol/services/c0901_kiban_124_chi.html)

●独自圧縮ルーチン採用

富士通独自の圧縮方式を採用している為、**特許権や著作権問題が発生しません。**
どんなデータでもアツという間に圧縮・暗号化します。

●高圧縮率を実現

バイナリデータやテキストデータを**30%～50%**に圧縮する事が可能です。
複数ファイルを1つの圧縮・暗号化ファイルとしてまとめます。

●データは完全な形に復元可能

ロスレスタイプのデータ圧縮ソフトウェアです。

ホストーパソコン間での圧縮形式データ互換があります。

注) Solarisは、ORACLE Corporation の商標です。

注) Windows Server 2008, Windows Vista, Windows 7は、Microsoft Corporation の商標です。



1.特徴②

(2) 暗号化技術の特長

●共通鍵暗号方式を採用

128ビットキー世界標準暗号アルゴリズム「AES」を標準採用しています。

●暗号アルゴリズムの選択が可能

「AES (標準)」、「トリプルDES」、「SC2000」から選択する事が可能です。

(3) 性能面での特長

●早い解凍処理

マイクロソフト標準ZIP形式と性能を比較してみると、解凍処理において縮丸の性能が特に優れています。

対象データ	圧縮形式	ファイルサイズ	解凍時間	CPU
Excelファイル	SLC	2,462KB	1.28秒	Pentium M
	ZIP		4.03秒	



2.圧縮／暗号技術①

(1) 暗号化とは

暗号化とは、データ通信を行う当事者以外がデータの中身を確認することをできなくする技術の総称です。簡単に言えば、文字や記号などを一定の約束（暗号アルゴリズム）に従って他の記号に置き換えることです。

この逆の順序で元のファイルやデータを取り出す行程を**復号化**と呼びます。

暗号化、復号化には暗号表にあたる「**鍵**」を使用します。

現在、暗号方式としては、**共通鍵方式**と**公開鍵方式**の2種類があります。

共通鍵方式

暗号化と復号化で同じ鍵を使うことになります。両者が同じ鍵を共有する必要があるため、「**共通鍵方式**」「**対称鍵方式**」とも呼ばれています。扱いが簡単で、処理時間が短いことも普及する要因となっています。代表的な共通鍵暗号としては、アメリカ政府標準となっている**DES**や、DESを3重に繰り返すことによって強度を高める**トリプルDES**などがあります。

『縮丸』はこちらの方式を使用しています。

公開鍵方式

公開鍵方式は、公開鍵と秘密鍵という異なる鍵を利用して暗号化／復号化を行います。「**非対称鍵方式**」と呼ばれることもあります。公開鍵を使ってデータを暗号化し、秘密鍵を利用してデータを復号化するといったことになります。公開鍵方式は、共通鍵方式に比べ共有が容易で、鍵の管理が便利という利点があります。公開鍵で主流となっているアルゴリズムはRSAで、巨大な整数の素因数分解の困難さを利用した方式です。



2.圧縮／暗号技術②

(2) 暗号アルゴリズム

①AES (Advanced Encryption Standard)

米国商務省標準技術局 (NIST) によって選定作業が行われている、米国政府の次世代標準暗号化です。

AESは、**換字** (substitution) と**転置** (permutation) の2種類の行程によって成り立つ暗号方式です。換字とは、平文内のそれぞれの文字を一定の規則に従って別の文字に置き換える暗号化方式のことです。また転置とは、平文内のそれぞれの文字の位置を一定の法則に従って並び変える暗号方式を意味します。

つまり、換字によって暗号化を施するとともに、転置によって情報の並びをランダムに置き換えることで、より強固な暗号化を実現しようとするものです。

さらに、64ビットブロックに対して、128,192,256ビットの鍵を用いることで暗号化を実現しています。強固な暗号化を実現しているものの、シンプルな構造であることから、高速での暗号化・復号化が可能であり、汎用性においても優れています。



2.圧縮／暗号技術③

(2) 暗号アルゴリズム

② トリプルDES (Triple DES:3DES)

IBM社が開発した暗号アルゴリズムです。

同社が開発した秘密鍵型の暗号方式である「DES」を3重に適用し、「DES」の脆弱性を補うものになります。

トリプルDESでは、データを鍵Aで暗号化し、その結果を鍵Bで復号し、さらにその結果を鍵C (鍵Aで行う場合もある) で暗号化するものです。

「DES」の脆弱性は一時的に解消されましたが、CPUの負荷が高くなってしまったという難点があります。



2.圧縮／暗号技術④

(2) 暗号アルゴリズム

③SC2000

SC2000は、AESと同じ鍵長128～256ビット、処理ブロック128ビットの暗号化です。富士通独自の構造を採用することで、安全性を保ちながら各種CPUでの高速性を実現しています。

特徴は、非線形処理(*1)と呼ばれる処理部分です。従来の暗号化は、一種類の非線形処理のみを繰り返す方式が大半でした。これに対し、SC2000では二種類の非線形処理を効率よく組み合わせる方式を用いることで安全性を高めています。

上記の技術を用いることで、AESと同等かそれ以上の安全性を有するとともに、現在のPCやワークステーション上で実装した場合、その処理性能はトリプルDESと比べ5倍以上(株)富士通研究所比)、またAESと比較しても遜色ない処理性能を達成しています。

*1：非線形処理

暗号化のためにデータを変換する処理の一つで、入力を出力の関係が線形(一次)式で表せない処理のことです。この非線形処理により高い安全性が得られます。



2.圧縮／暗号技術⑤

(3) 縮丸の圧縮技術

圧縮前のデータと圧縮・復元後のデータが完全に一致する圧縮、loss-less方式を採用しています。

『縮丸』では、以下の圧縮形式を用意しており、運用形態に合わせて選択していただく事が可能です。

縮丸の圧縮形式

圧縮形式	内容	圧縮率	処理速度
SLC	FLDCの性能向上版で、処理速度・圧縮率ともに優れています。	非常に良い	非常に良い
FLDC1	圧縮率を優先 して処理を行います。 多少処理時間がかかっても圧縮率を高くしたい場合に選択してください。	良い	普通
FLDC1 (BATCH)			
FLDC3	処理速度を優先 して処理を行います。 圧縮率は下がりますが、処理速度はとても早くなります。合わせてCPU負荷も下がるため、マルチタスクOS等で他のプロセスへの影響度も低く抑えることが可能です。	普通	良い
FLDC3 (BATCH)			

BATCH形式とは、ホスト～PC連携時に使用する形式です。



2.圧縮／暗号技術⑤

(4) FLDC/SLCの原理

『縮丸』では、FLDC (Fujitsu Lossless Data Compression) / SLC (Super Lossless Compression) 方式を使用しています。

現在主流となっている「辞書型符号化」とは異なる「確立統計型」を採用しています。「確立統計型」は、米国でもまだ研究段階で実用化されていなかった技術です。


この方式の仕組みは、直前データと関係付けて入力語の出易さを捉え、その出易さに応じて符号の長さを割付けます。例えば直前に何の文字が出たか知らない時は、次にどんな文字が出るか予想できませんが、直前が「富士」と知っていれば、次に来る文字は『山』『川』『通』・・・と候補は大体予想できます。

さらに候補の文字の中でその出易さ(統計的出現確率)に片寄りがあります。今まで入力したデータから直前に関係付けて次の文字候補とその出現割合を記憶しておき、実際に「富士」の次の文字が入力されたとき出現割合が大きい文字程短い符号を割付けます。この符号の並びを符号化テーブルとして関連付けする事により圧縮を実現しています。

この方式の特徴は、動的辞書方式 (compress) より高い圧縮率が得られ、スライド辞書法の特許紛争問題をさける事ができる点です。圧縮可能なデータ種別も幅広く、テキストファイル・ロードモジュール・各種定義体・無圧縮イメージ等が圧縮可能です。



3. インターフェース①

インターフェース	解説	製品名
<p>GUI (グラフィカル ユーザインター フェース)</p>	<p>Windows GUI を使用し「縮丸」のプログラムを呼び出す形式です。 グラフィカルな画面を使用しながら ファイルの圧縮・暗号／復号・復元が可能。</p> <p>画面表示例) 画面は「縮丸V6」の例です。</p> 	<p>縮丸V6 縮丸V5</p>

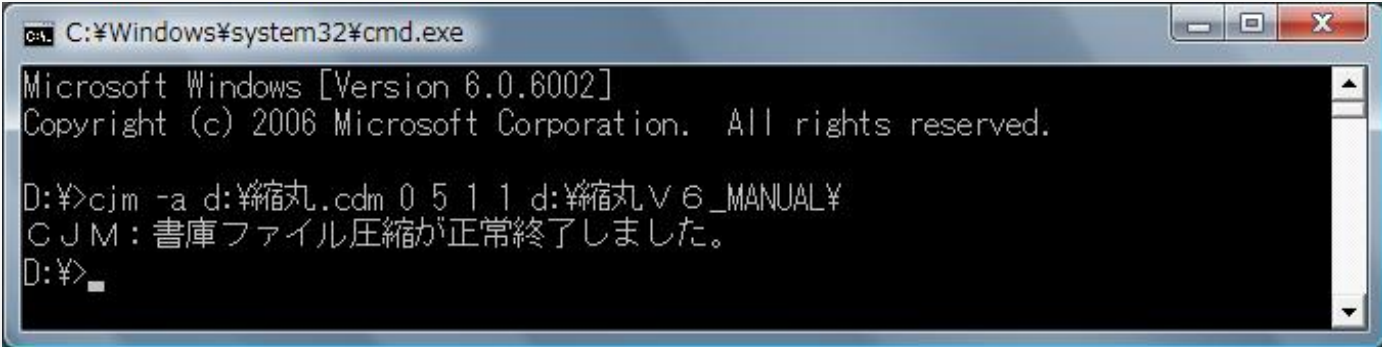


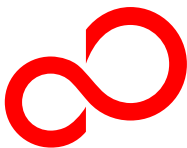
3. インターフェース②

インターフェース	解説	製品名
API (アプリケーションプログラムインターフェース)	<p>ユーザアプリケーションから「縮丸」のプログラムを呼び出す形式です。 LIB,DLL等のライブラリ形式で提供される。 基本的に呼び出しプログラム言語は特定されない。 ファイルの圧縮・暗号／復号・復元が可能。 文字列(バッファ)の圧縮・暗号／復号・復元が可能。 製品添付のマニュアル、ヘッダーファイルを参照し、「縮丸」のAPIを使用して下さい。</p>	縮丸V6



3. インターフェース③

インターフェース	解説	製品名
COMMAND (コマンドインターフェース)	<p>コマンドラインから直接「縮丸」のプログラムを呼び出す形式です。 機能名・入力ファイル名・出力ファイル名を指定して実行する。 ファイルの圧縮／復元が可能。</p> <p>画面表示例) 画面は「縮丸V6」の例です。</p> 	縮丸V6



FUJITSU

shaping tomorrow with you