Crypt/MF®のご紹介
（暗号化・復号化プログラム）

株式会社　*ピーアンドディー*

目次

- 概要
- 特徴・機能
- 導入・実行環境
- 実行図
- 実行JCLサンプル
- 実行パフォーマンス例
- 制限事項

概要

- IBM・富士通・日立のメインフレームで稼動するデータの暗号化・復号化プログラム
- C4テクノロジー社の強力な暗号化・復号化エンジンを内部で使用
- ユーティリティー・ジョブの様にバッチジョブ形式で実行
- 暗号化したデータを別プラットフォームと受け渡し復号化が可能（＊1）

注釈：＊1－AS／400、UNIX, WINDOWSでC4テクノロジー社の暗号化・復号化エンジンを使用したプログラムが導入されている事が前提になります。

特徴・機能

Crypt／MFの特徴は次の通りです。

- 取り扱うファイル媒体及びファイル形式
  DASD及びTAPEのシーケンシャル・データセット及びVSAMデータセット
- 取り扱うレコードフォーマット
  F, FB, V, VB, U, FBS, VBS
- 暗号化・復号化フィールド
  レコード上の全フィールド、または特定フィールドの選択可能
- 暗号化・複合化の内部処理
  BLKSIZE以上に内部でブロック化し処理を行なうため効率が良い
- 処理結果
  分析レポート出力　：　レコード件数、全容量、CPUタイム、ELAPSEタイム、他

導入・実行環境

Crypt／MFは特別な導入・実行環境を必要としません。

- OS／390、z／OS、MSP，XSP，VOS3上に導入、実行可能
- システム環境の変更は必要ないため導入後即使用可能
  （APFやLPAへの登録は不要です）
- Crypt／MFプログラム全体で3シリンダーのDASD容量を使用
- 実行REGIONサイズは500KB位から稼動
  （暗号化・復号化の効率を上げる場合は更に大きなREGIONが必要になります）
- REALメモリーの指定は不必要

実行図

Crypt／MFは一般的ユーティリティーの様に実行します。

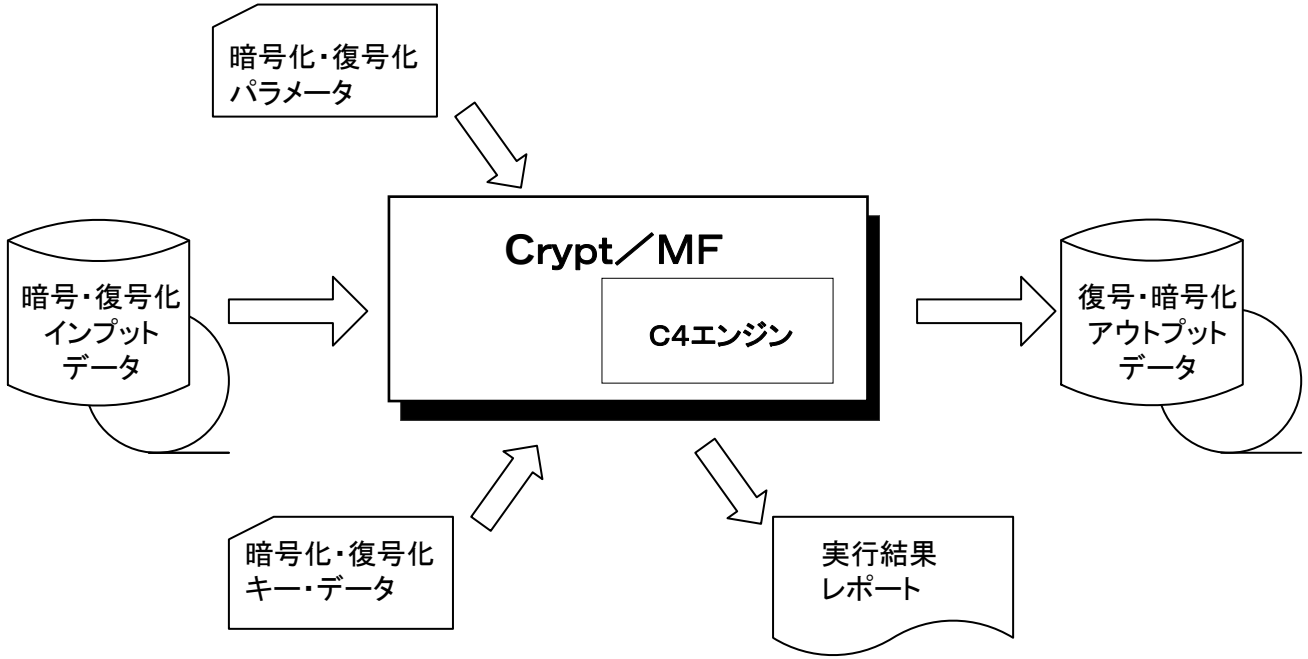

図1．　Crypt／MF実行図

実行JCLサンプル

Crypt／MF実行JOBサンプルは次の通りです。
（IBM Z／OS, OS／390, 富士通 MSP, 日立 VOS3）

```
//Job-Name JOB (Account),MSGLEVEL=1,,,,
//Step名   EXEC  PGM=CRYPTMF,PARM='暗号化･複合化パラメータ'
//STEPLIB   DD  DISP=SHR,DSN=xxxx.CRYPT390.V2M0.LOAD
//SYSPRINT  DD  SYSOYT=*
//C4PRINT   DD  SYSOUT=*
//C4PARM    DD  DISP=SHR,DSN=xxxx.CRYPT390.V2M0.PARM
//C4UT1     DD  (暗号化･復号化インプット･データ)
//C4UT2     DD  (暗号化･復号化アウトプット･データ)
//C4UT2XX   DD  (暗号化アウトプット･データ2)
//C4KEY     DD  *
 (暗号化･復号化キー･データ)
/*
```

実行JCLサンプル

Crypt／MF実行JOBサンプルは次の通りです。

（富士通　XSP）

```
$ JOB ENCSALES,LIST=(A,JS)
$ EX CRYPTMF,RSIZE=4096K
$ PARA ENC
$ FD PRGLIB=DA,FILE=KOAP.CRYPTMF.V241.LOAD
$ FD C4PRINT=DA,VOL=WORK,TRK=(10,1,SOUT=A
$ FD C4KEY=DA,FILE=KAOP.MARKET.KEY
$ FD C4UT1=DA,    (暗号化・復号化インプット・データ)
$ FD C4UT2=DA,    (暗号化・復号化アウトプット・データ)
$ FD C4UT2XX=DA,  (暗号化アウトプット・データ2)
$ JEND
```

実行パフォーマンス例

- **実行環境**

  25MIPS相当のシステムを使用しテストした結果です。

- **実行結果**

ケース	RECFM	LRECL	BLKSIZE	BUFNO	レコード件数	暗号・復号内部領域	CPUタイム（秒）	ELAPSEタイム（秒）
1	FB	80	8,000	50	1,282,320	32KB	16.5	27
2	F	8,000	8,000	50	12,824	32KB	13.8	26
3	FB	4,200	24,960	50	24,660	32KB	13.3	21
4	VB	32,000	32,004	50	76,032	32KB	8.4	17

制限項目

Crypt／MFの機能・実行制限は下記の通りです。

- Crypt／MFはバッチ・モードのみで実行可能
- リエントラント・コーディングになっていないためリンクパックエリア（LPA）に常駐不可
- 暗号・復号キーはユーザ管理が必要

株式会社ピーアンドディー

お問合せ先:

株式会社ピーアンドディー

〒107-0062

東京都港区南青山1-15-37

TEL: 03-3505-4984 / FAX: 03-3505-5386

E-mail: sales@pandd.co.jp

URL　: http://www.pandd.co.jp