合衆国商務省長官　William M. Daley
米国標準技術局局長　Raymond G. Kammer

はじめに

National Institute of Standards and Technology(NIST)(米国標準技術局)の連邦情報処理基準は、Information Technology Management Reform Act (情報技術管理改正法)(Public Law 104-106, 1996 年) 第 5131 項、及び Computer Security Act (コンピュータセキュリティー法)(Public Law 100-235, 1987 年)の規定のもと認可され、公布された一連の公式刊行物である。連邦政府のコンピュータや関連通信システムの利用と管理を向上させる、という重大な責務を、商務長官及び NIST に委託したものである。NIST は情報技術研究所を通じて、そうした領域における標準やガイドラインを作りあげるべく、指揮をとり、技術指導や政府への協力をおこなっている。

FIPS 刊行物に関する意見をお待ちしています。宛先:
The Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Dr. Stop 8900, Gaithersburg, MD 20899-8900

William Mehuron, Director
Information Technology Laboratory

概要

あらゆる連邦政府組織は、電子データシステムにふさわしいセキュリティを確保する上で、技術的な、関連性のある処理上の安全措置を適用する重要な責任がある。この刊行物は、扱いに注意を要するデータを保護するために連邦組織で使用される二つの暗号アルゴリズム、Data Encryption Standard(DES)と Triple Data Encryption Algorithm(TDEA)について詳しく述べたものである。送信時もしくは保存時のデータの保護は、データの中に書かれている情報の秘密性や完全性を守るために必要である。このアルゴリズムは、データを暗号文に、また暗号文をもとの形に変換するのに必要な数学的な手順をそれぞれ定義している。DES は、物理的セキュリティ処理、的確な情報管理の実行、コンピュータシステムやネットワークのアクセスコントロールなどからなるトータルセキュリティの状況下において、連邦機関で使用することができるよう作成されている。この改訂は FIPS46-2 を全面的に更新した物である。

Federal Information Processing Standards Publication
連邦情報処理規格刊行
46-3

1999 年　8 月 25 日

DATA ENCRYPTION STANDARD(データ暗号化標準) について

Federal Information Processing Standards Publication(連邦情報処理企画刊行物)は、Information Technology Management Reform Act (情報技術管理改正法)(Public Law 104-106, 1996 年) 第 5131 項、及び Computer Security Act (コンピュータセキュリティー法)(Public Law 100-235, 1987 年)に準ずる商務省の認可を受けて、National Institute of Standards and Technology (米国標準技術局)より発行されている。

1, 標準名　Data Encryption Standard(DES)(データ暗号化標準)

2, 標準の分類　コンピュータセキュリティー、暗号

3, 解説

Data Encryption Standard(DES)は FIPS 140-1 で要求される通り、認可された２つの FIPS 暗号アルゴリズムを規定している。American National Standards Institute (ANSI)(米国規格) X9.52 標準と併用した場合、バイナリコード化された情報の暗号化と復号化のための完全な数学的アルゴリズムを提供する。データの暗号化によりデータを暗号という判読不可能な形に変換し、暗号文の復号化によって、そのデータを平文と呼ばれる元の形へと戻す。この標準のアルゴリズムは暗号化と復号化双方の処理を規定しており、その処理は二進数の鍵に基づいている。

DES 鍵は 64 桁の二進数(0 もしくは 1)で成り立っており、そのうち 56 ビットはランダムに生成され、直接アルゴリズムで使用される。残りの 8 ビットはアルゴリズムでは使われず、エラー発見のために使用される。エラー発見用の 8 ビットは、8 ビットずつの奇数パリティになっており、すなわち、各 8 ビットの中に奇数個の 1 が含まれている。TDEA 鍵は 3 つの DES 鍵から成り、キーバンドルとも呼ばれる。許可を受けて暗号化されたコンピュータデータを使用するユーザーは、復号化のために、暗号化の際に使われた鍵を知っていなければならない。この標準で規定された暗号アルゴリズムは、この標準の利用者の間で共通に知られている。データの暗号化セキュリティは、暗号化と復号化の際に使われる鍵にかかっている。

データは暗号化の時使われたのと全く同じ鍵を用いた場合のみ元通りの形になる。暗号を受け取った人が許可を受けていない場合、アルゴリズムを知っていても正しい鍵を知らなければ、アルゴリズムを通じて元のデータを引き出すことはできない。ただし、手あたり次第“総当たり攻撃”で鍵を見つけ出すことは可能といえる。また、鍵とアルゴリズムを知っている人なら簡単に暗号を復号化し、原文を手に入れることができる。標準アルゴリズムはセキュアキーに基づいているため、データを見ることを許された人には、暗号化に使われた鍵を発行することで暗号化されたコンピュータデータの受け渡しができることになる。

当局によって扱いに注意を要すると認められたデータ、高い価値のあるデータは、転送の際や保存中に不当に暴露されたり、秘密裏に変更されたりといった攻撃を受けやすい場合、暗号化によって保護されなければならない。潜在的な脅威を見極めるため、当局の指導のもとリスク分析を行わなければならない。この標準を用いた暗号化保護策に必要なコスト、またはそれに変わりうる保護策とそれにかかるコストを見積もり、そしてそれらの分析に基づいて、暗号化保護策とこの標準を使用するかどうか決定する必要がある。

4, 認証機関　商務長官

5, 管理機関　合衆国商務省、米国標準技術局(NIST)、情報技術研究所

6, 適用性　この標準は、以下の条件が満たされる場合、連邦局や機関で使用され得る。

1, データやコンピュータシステムのセキュリティを担当する公的機関や管理者が暗号化による保護が必要であると決断し、また

2, そのデータが 1947 年の改正安全保障法や 1954 年の改正原子力法により機密扱いになっていない場合

これらの法で機密扱いになっているデータの保護に暗号化デバイスを使用する連邦省庁は、この標準の代わりにそれらのデバイスを使用できる。

FIPS140-1 を満たす場合は、この標準に加えて、またはその代わりに、他の認可された FIPS 暗号アルゴリズムを使うこともできる。

加えて、この標準は非連邦政府組織でも採用し、使用することができる。民間の営利組

織において適切なセキュリティを提供できる場合、そうした民間組織での使用を奨励する。

7, アプリケーション

データの暗号化は様々なアプリケーションや動作環境において利用される。暗号化の利用の詳細と DES や TDEA の実行は、個々のコンピュータシステムやそれに関わるコンポーネントの様々な要因に基づく。一般に、暗号化は、データが二地点で受け渡される際、または物理的な脅威にさらされやすい環境で保存される際に使用される。伝達時のセキュリティは、送信地点で暗号化を行い、受信地点で復号化することでデータ保護を行う。ファイルセキュリティは、保存場所に記録するときに暗号化し、再び読み込むときに復号化する。前者の場合には、受け渡しの際、送り手と受け手が同時に同じ鍵を共有していなければならない。後者では、保存している間ずっと鍵を保有しておく必要がある。FIPS 171 では、この標準で規定されているアルゴリズムで使われる鍵を保管するための方法を提供している。プロトコルに基づく公開鍵も使用可能である。(例 ANSI X9.42)

8, 実行

この標準を実行する暗号化モジュールは FIPS 140-1 の条件に従う。アルゴリズムはソフトウェア、ファームウェア、ハードウェアまたはそれらの組み合わせのなかで実行される。実行の詳細はアプリケーションや環境、使われる技術等の様々な要因に基づく。この標準に応じた実行は、電子デバイス(例：VLSI チップパッケージ)、マイクロプロセッサーを使ったリードオンリーメモリ (ROM)、プログラマブル ROM (PROM)、イレーザブル ROM (EEROM)、メインフレームコンピュータを使ったランダムアクセスメモリ(RAM)を含む。アルゴリズムをソフトウェアまたはファームウェアで実行する場合は、アルゴリズムが動く処理プログラムの認証を受けなければならない。NIST によりテストされ認可されたアルゴリズムを実行することは、この標準に従うものと見なされる。FIPS 140-1 は政府使用の暗号化モジュールに追加の要求事項を付け加えているため、注意してほしい。認可されたデバイス、また、この標準や FIPS 140-1 に従ったデバイスのテストと認可の手続きに関する情報は、NIST の情報技術研究所(住所：100 Bureau Dr. Stop 8900, Gaithersburg, MD 20899-8900)で公開している。

9, 輸出制限

暗号化デバイスとそれに関わる技術データは連邦政府の輸出制限に従う。また、この標準と技術データを実行する暗号化モジュールの輸出はそれら連邦政府の規制に従い、米国商務省の輸出管理局に許可を受けなければならない。

10, 特許

この標準を実行する暗号化デバイスは、International Business Machines Corporation

が発行する特許を含む、国内外の特許が認められている。しかし IBM は特許下において、この標準に伴う一式の作成、使用、販売をおこなうことを、非独占的に、特許権使用料無料で許可している。それらのライセンスの期間、条件、範囲に関しては、Official Gazette of the United States Patent and Trademark Office が 1975 年 5 月 13 日と 1976 年 8 月 31 日に発行した告示にて明示してある。

11, DES、TDEA 使用のモード選択

FIPS PUB81、“ DES モードでの操作 ” では、DES を用いた四通りのモードを説明している。それら四つのモードは Electronic Codebook (ECB)モード、Cipher Block Chaining(CBC)モード、Cipher Feedback (CFB)モード、Output Feedback (CFB)モードと呼ばれる。ECB はデータの暗号化と復号化のための DES アルゴリズムに直接使われるアプリケーションである。CBC は ECB が強化されたもので、暗号文のブロックをつなげる働きをする。CFB はあらかじめ DES への入力として生成された暗号文を使って、平文と結びついて暗号文を作る擬似ランダム出力を作り、結果として生じる暗号文をつなぎあわせる。OFB は CFB とほとんど同じであり、唯一違うのは、CFB ではあらかじめ作られた暗号文が入力として使われていたが、OFB では DES の前もって出た出力が入力として使われるという点である。OFB は暗号文をつなぎ合わせることはしない。

X9.52 標準の “ TDEA モードでの操作 ” では、TDEA を使った 7 通りのモードについて書いている。それらは、TDEA Electronic Codebook Mode of Operation(TECB)モード、TDEA Cipher Block Chaining Mode of Operation(TCBC)、TDEA Cipher Block Chaining Mode of Operation-Interleaved(TCBC-I) 、 TDEA Cipher Feedback Mode of operation(TCFB)、TDEA Cipher Feedback Mode of operation-Pipelined(TCFB-P)、TDEA Output Feedback Mode of operation(TOFB) 、 TDEA Output Feedback Mode of operation-Interleaved(TOFB-I)と呼ばれる。
TECB、TCBC、TCFB、TOFB モードはそれぞれ ECB、CBC、CFB、OFB モードに基づいており、TDEA 暗号化/復号化 操作において、DES 暗号化/復号化 操作での各モードに変わるのものとして存在する。

12, 標準の実行

この標準は 1977 年 7 月から有効であり、1983 年、1988 年、1993 年、1999 年に再認されている。あらゆる連邦機関やその請負業者、また連邦政府にかわってその職務を果たすために、コンピュータやテレコミュニケーションシステムをもちいて情報処理を行う組織に適用される。各連邦機関、省庁は、それぞれのデータセキュリティの必要性に基づいた管理ユニットによって、この標準の使用に対する内部指示を出すこともある。

FIPS 46-2 における修正

1, ANSI X9.52 で書かれているように、トリプル DES も FIPS の認可アルゴリズムとして認定される。
2, トリプル DES は、FIPS として制定された対照暗号アルゴリズムとなる。
3, シングル DES の使用はレガシーシステムのみを対照とする。可能であれば、レガシーシステムのサポートとして、シングル DES 用の環境設定で動くトリプル DES 製品を使用することを推奨する。
4, 旧 DES システムを使用している政府機関には、関連リスクへの保護手段として十分な強度を持つ、慎重な戦略に基づいたトリプル DES へ移行することを推奨する。

注：FIPS として認可されたアルゴリズムとして、DES と AES が、AES への前進的な移行を見込みつつも共存することが期待される。(AES は NIST が開発中の、対称鍵による新しい暗号化標準であり、扱いに注意を要する情報の保護のために、二十一世紀の強力な暗号化セキュリティを提供するものである。)

NIST は、標準やガイドラインの発行、また個々の保証付きのプロジェクトを通じて、連邦機関のデータ暗号化の実践に技術的な援助を行っている。

13, 仕様 FIPS 46-3、データ暗号化標準(DES)

14, 索引

a, FIPS PUB 31, ADP フィジカルセキュリティとリスクマネージメントのガイドライン
b, FIPS PUB 39, コンピュータセキュリティシステムに関する用語解説
c, FIPS PUB 73, コンピュータアプリケーションのセキュリティに関するガイドライン
d, FIPS PUB 74, NBS データ暗号化標準の実行と使用のガイドライン
e, FIPS PUB 81, DES モード操作
f, FIPS PUB 87, ADP コンティンジェンシープランへのガイドライン
g, FIPS PUB 112, パスワードの取扱い
h, FIPS PUB 113, コンピュータデータ認証
i, FIPS PUB 140-1, 暗号化モジュールのセキュリティ要求
j, FIPS PUB 171, ANSI X9.17 を用いた鍵の管理
k, ANSI X9.42, Diffie-Hellman・MQV アルゴリズムを使った対称鍵の呼応
l, ANSI X9.52, TDEA モード操作

15, 修正

この標準と、この標準を用いた際に起こり得る、セキュリティ低下の恐れの双方は、新技術の存在も考慮に入れつつ NIST によって適切なものに再検討される。加えて、なんらかの技術の躍進やアルゴリズムの数学的脆弱性が明らかになった場合は、NIST は標準を再査定し必要な改訂を加える。

単独 DES の使用に関しては、技術の進化に伴い、DES への徹底的な攻撃、すなわちあらゆる可能性のある鍵を試していくことで DES 暗号文を突破するということがますます可能になっている。最新のハードウェアを用いた DES 鍵への総当たり的な攻撃を考えると、NIST はもはや様々なアプリケーションでの単独 DES の使用をサポートすることはできない。従って、レガシーシステム上で単独 DES を使用している政府機関へは、トリプル DES への移行を推奨する。代理機関へは、新しいシステムを構築する際トリプル DES を実行することを勧める。

16, 意見

この標準とその使用に関する意見、提案をお待ちしています。

National Institute of Standards and Technology, Information Technology Laboratory 所長宛, 100 Bureau Dr. Stop 8900, Gaithersburg, MD 20899-8900

17, 権利放棄の手続き

なんらかの例外的な状況下では、連邦省庁や代理機関の長は FIPS に対し権利放棄を認める事がある。各機関の長は、USC 第 44 編第 3506(b)条に準じて指名された上位機関にのみ、その権限を再委託することができる。権利放棄は以下の場合のみ認められる。

a, 標準に従うことが、連邦のコンピュータシステム管理者の任務遂行に悪影響をもたらす場合

b, 標準に従うことが、政府の救済措置をもってしても埋め合わせできないほどの経済的悪影響を管理者に与える場合

各機関の長は、上記の詳細を添えた権利放棄要求書にしたがって手続きを行う。また標準を満たすための条件が満たされないと判断した場合は、要求書なしでも可能である。権利放棄の承認は、必要事項を記した書面を通じてのみ行われる。各決定事項のコピーと、扱いに注意を要する、または機密の部分を明確に指定したものを、下記の宛先まで送付すること。

National Institute of Standards and Technology, FIPS Waiver Decisions 宛, 100 Bureau Stop 8970, Gaithersburg, MD 20899-8970

加えて、認可された権利放棄と、権利放棄承認権の委任に関する記録は即座に the Committee on Government Operation of the House of Representatives と the Committee on government Affairs of the Senate へ送られ、連邦記録の中で公開される。

権利放棄の決定が設備機器やサービスの取得に関連するときは、権利放棄決定の書類は取得要求の記録として the Commerce Business Daily の中で公開されなければならず、もしそれら記録の公開の後で権利放棄の決定がなされた場合は、記録の修正を行わなければならない。

権利放棄の書面や付属の書類、権利放棄承認の書類やそれに付随する書類は、USC 第 5 編 552(b)条に基づき、認可された上で削除されたものとともに、データ調達文書とされ、当該機関によって保管される。

18, 特記事項

当標準の規約に基づき、1977 年の採用から 5 年ごとに標準の再検討が行われ、各検討期ごとに追認される。今回の文書の改訂では、アルゴリズムのソフトウェアにおける実行や、他の FIPS に指定された暗号アルゴリズムの使用を認め、またトリプル DES へ移行を FIPS 認定暗号アルゴリズムに指定している。

19, 当標準のコピーの入手先

コピーは、米国商務省の National Technical Information Service（Springfield, VA22161）から販売されている。注文の際は FIPSPUB46-3 を照会し、タイトルを明示すること。マイクロフィッシュを希望する場合はその旨記載すること。価格は、NTIS から最新カタログや他の発行物が出版されている。支払いは小切手や郵便為替、口座振込や NTIS 指定のクレジットカードで可能である。

FIPS46-3

1999.8.25

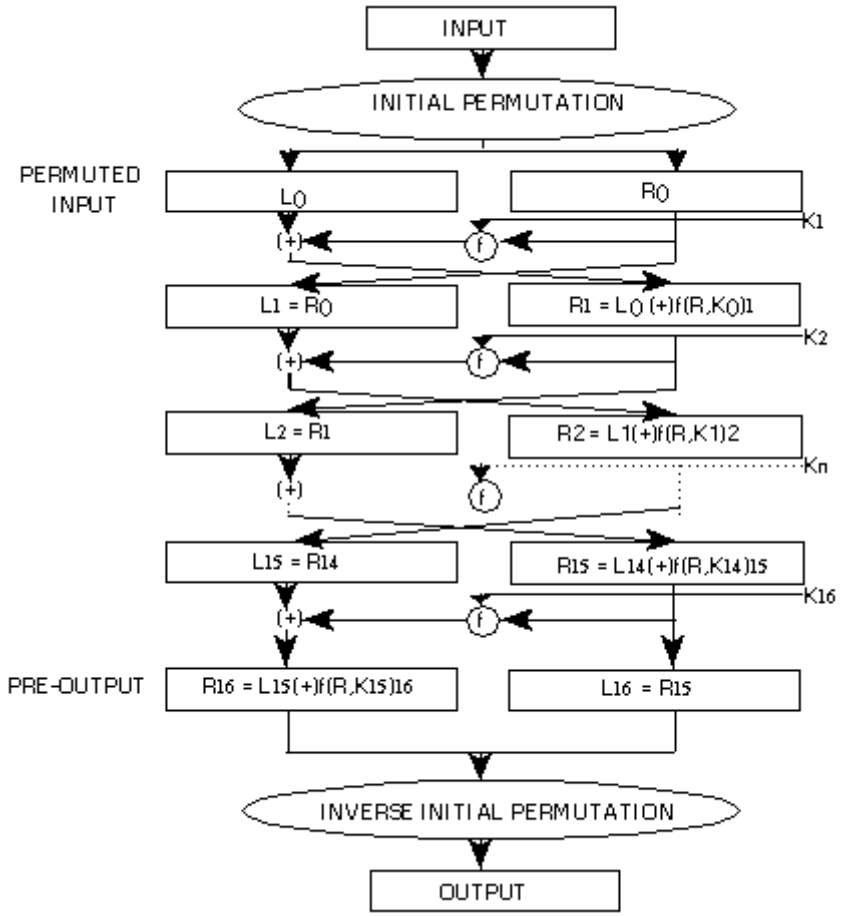
データ暗号化標準(DES)の詳細

データ暗号化標準(DES)は、データ暗号アルゴリズム(DES)とトリプルデータ暗号アルゴリズム(TDEA)から成る。これらの装置は、コンピュータシステムやネットワークにおいて、バイナリコード化されたデータを暗号化により保護するものである。実行方法はアプリケーションや環境により異なる。下記のアルゴリズムで規定された変換を正確に行うようテストされ、認証されるような方法で実行されなければならない。

データ暗号アルゴリズム

はじめに

このアルゴリズムは、64 ビットの鍵の制御下において、64 ビットのデータブロックを暗号化、復号化するものである。復号化は暗号化の時と同じ鍵を使って行わなければならないが、鍵は復号化のプロセスが暗号化の逆になるよう変更される。暗号化されるブロックは initial permutation(**IP**、初期転置)が行われ、次に鍵を用いた複雑な処理を受け、最後に **IP** の逆の転置、**IP-1** を受ける。鍵による処理は function **f**
(暗号化関数)、また function **KS**(キースケジュール)と定義される。はじめに、暗号化の際にどのようにアルゴリズムが働くのか詳細に見た後で、復号化のためのアルゴリズムの用法を説明していきたい。最後になるが、暗号化関数の定義は、選択関数 **Si**、また転置関数 **P** と呼ばれる基本関数によって行われる。**Si, P, KS** は付録１に収録されている。



<図 1>

L と **R** の二つのブロックが与えられた場合、**LR** とは **L** のビットの後に **R** が続いているブロックを示す。連結に結合性がある場合、たとえば **B1B2…B8** となっていたら、**B1** のビットの後に **B2** が続き…というふうにして **B8** まで続くブロックを示すことになる。

暗号化

暗号化処理の見取り図は図１の通りである。

暗号化される 64 ビットのインプットブロックは、はじめに、次の 初期転置 **IP** と呼ばれる転置を受ける。

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

そうして転置された入力データは、第一ビットに 58、第二ビットに 50、そうして最終ビットに 7 を持っていることになる。そのインプットブロックが今度は後に記す、鍵による複雑な処理への入力となる。そしてその結果出てきたプレアウトプットと呼ばれる出力データは、**IP** の逆である下記の転置**(IP-1)**を受ける。

IP-1

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

このようにして、アルゴリズムの出力は、プレアウトプットブロックの第一ビットに 40、第二ビットに 8 と続いて、最終ビットに 25 が入る。

下記の、32 ビットと 48 ビットの二つのブロックを操作して 32 ビットのブロックを作る暗号化関数 **f** を用いた計算式の、16 番目の操作、最後のブロック置き換え以外は、転置されたインプットブロックを入力として使い、プレアウトプットブロックを作る処理が成立する。

64 ビットのインプットブロックを、32 ビットのブロック **L** と、それに続く 32 ビットの

ブロック **R** から成る反復処理にかける。‘ はじめに ’で定義した表記を使うならば、インプットブロックは **LR** となる。

64 ビットの鍵から選ばれた 48 ビットのブロックを **K** とする。インプット **LR** に一回処理を行って生じるアウトプット **L'R'**は、次のように定義される。

(1) $$L'=R$$
$$R'=L(+)f(R,K)$$

(+)はビットごとの排他的論理和を示す。

先にも述べたように、反復処理の第一回目の入力は転置されたインプットブロックである。16 回目の処理の出力が **L'R'**であれば、**R'L'**がプレアウトプットブロックになる。各処理で、**KEY** により指定された 64 ビットの鍵から、それぞれ異なる鍵ブロック **K** が選ばれる。

この反復計算をさらに詳しく説明しよう。**KS** を、1 から 16 までの整数ｎをとり、64 ビットのブロック **KEY** をインプットとして、**KEY** から選出し転置された 48 ビットのブロック **Kn** を算出する関数とする。

(2) $$Kn = KS\ (n,KEY)$$

Kn は KEY から取り出された 48 ビットから決定される。(1)の n 番目の処理で使われるブロック **K** は(2)で決定されるブロック **Kn** であるため、**KS** はキースケジュールと呼ばれる。

同様に、転置されたインプットブロックを **LR** とする。n を 1 から 16 までの整数とし、L と R がめいめい **Ln-1**、**Rn-1** であり、**K** が **Kn** であるとき、**L0** と **R0** をそれぞれ **L**、**R**、**Ln** と **Rn** を **L'**、**R'**とする。

(3) $$Ln = Rn\text{-}1$$
$$Rn = Ln\text{-}1(+)f(Rn\text{-}1,Kn)$$

プレアウトプットブロックは **R16L16** となる。

アルゴリズムのキースケジュール **KS** は、付録に詳しく記載している。キースケジュールはアルゴリズムに必要な 16 の **Kn** を生成する。

復号化

プレアウトプットブロックにかけられる転置 **IP-1** は、インプットにかけられる初期転置 **IP** の逆である。さらに、(1)から、次のようになる。

(4) $$R = L'$$
$$L = R'(+)f(L',K)$$

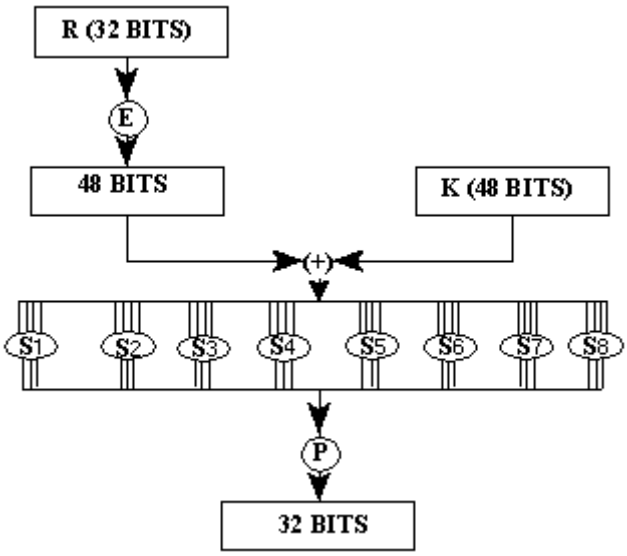
従って復号化のためには、処理の各回において暗号化の時と同じ鍵ビット **K** が使われていることに注意しつつ、暗号化されたメッセージブロックに全く同じアルゴリズムを当てていけばいいだけである。前回と同じ表記をすると、次の方程式で表すことができる。

(5) $$Rn-1 = Ln$$
$$Ln-1 = Rn(+)f(Ln,Kn)$$

この場合 **R16L16** が復号化処理の転置インプットブロックとなり、**L0R0** がプレアウトプットブロックになる。つまり、**R16L16** を転置インプットとした復号化処理において、**K16** が一番目の処理に、**K15** が二番目、**K1** が 16 番目の処理に使用される。

暗号化関数 f

f(R,K)の処理の略図を図 2 に示す。



<図 2>

E は、入力に 32 ビットのブロックをとり、48 ビットのブロックを出力する関数を表す。8 つの 6 ビットブロックで書かれた 48 ビットのアウトプットは、入力に、下の表にしたがってビットを順に選択していくことによって得られる。

<E ビット選択表>

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

E(R)の最初の 3 つのビットは 32、1、2 の位置にある 3 ビットであり、最後の 2 つのビットは 32、1 の位置にあるビットである。

それぞれの選択関数 **S1**、**S2･･･S8** は 6 ビットブロックを入力にとり、4 ビットブロックを

出力するものである。S1 の表を使って説明する。

<S1>

Column Number

Row No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S1 がこの表で定義される関数で、**B** が 6 ビットのブロックだとすると、**Si(B)**は次のように定められる。**B** の最初と最後のビットは二進法で 0 から 3 までの中の 1 つの数字を表し、その数値を **i** とする。**B** の中の 4 ビットも同じように 0 から 15 の 1 つの数字を表し、これを **j** とする。上の表の、横 **i** 番目、縦 **j** 番目の数字を見てほしい。この数字は 0～15 のどれかで、4 ビットブロックで表される。そのブロックが、インプット **B** に対する **S1** のアウトプット **S1(B)**である。たとえば、入力に 011011 が与えられたとすると、横の数値は 01、つまり横一列目であり、縦の数値は 1101、縦 13 列で表される。横 1 列目、縦 13 列目の数字は 5 であり、従って 0101 が出力される。**S1S2･･･S8** の選択関数は付録 1 に記載している。

転置関数 **P** は、32 ビットのインプットを転置することで 32 ビットのアウトプットをつくる。その関数は下の表で定義される。

<P>

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

この表で定義される関数 **P** のアウトプット **P(L)**は、**P(L)**のはじめのビットに **L** の 16 番目のビット、**P(L)**の 2 番目のビットに **L** の 7 番目のビットと続いて **P(L)**の 32 番目のビットに **L** の 25 番目のビットがはいるように、インプット **L** から得られる。アルゴリズムの反復関数 **P** は、付録 1 に再度収録している。

さて、**S1･･･S8** をそれぞれ 8 つの選択関数、**P** を置換関数、**E** を先に定義した関数だとする。

f(R,K)を定義するために、まず **B1･･･B8** をそれぞれ 6 ビットのブロックになるよう定めなければならない。

(6) **B1B2…B8 = K(+)E(R)**

するとブロック **f(R,K)**は次のように定義される。

(7) **P(S1(B1)S2(B2)…S8(B8))**

K(+)E(R)は、まず(6)で示されているように、8 つのブロックに分けられる。それぞれの **Bi** は **Si** へのインプットとなり、それぞれ 4 ビットで 8 ブロックの **S1(B1)S2(B2)…S8(B8)**は、**P** へのインプットとなる 32 ビットの、1 つのブロックに統合される。アウトプット(7)は、インプット **R**、**K** への関数 **f** のアウトプットとなる。

トリプルデータ暗号アルゴリズム（TDEA）

鍵 **K** により、DES を使って **I** の暗号化、復号化を行うことをそれぞれ **EK(I)**、**DK(I)**とする。TDEA の暗号化/復号化の各操作は、DES の暗号化、復号化を複合させたものである。下記の処理が行われる。

1. TDEA 暗号化処理：64 ビットのブロック **I** を、下に定められた 64 ビットのブロック **O** に変換する。

O = EK3(DK2(EK1(I)))

2. TDEA 復号化処理：64 ビットのブロック **I** を、下に定められた 64 ビットのブロック **O** に変換する。

O = DK1(EK2(DK3(I)))

この標準は、キーバンドル**(K1、K2、K2)**を用いたキーイング(鍵かけ)を下記の三通りに規定している。

1. キーイングオプション 1：**K1**、**K2**、**K3** はそれぞれ異なる鍵である。

2. キーイングオプション 2：**K1**、**K2** は異なる鍵で、**K3=K1** である。

3. キーイングオプション 3：**K1=K2=K3**

TDEA モードでの処理は、共通して使えるキーイングオプションを使えば、対応するシングル DES と後進的に互換性を持つ。

1. シングル DES モードで処理し、暗号化した平文は、対応する TDEA モードで正しく復号化される。

2. TDEA モードで処理し、暗号化した平文は、対応するシングル DES モードで正しく復号化される。

キーイングオプション 3 を用いた場合は、TECB、TCBC、TCFB、TOFB モードはそれぞれシングル DES へ移行モードの ECB、CBC、CFB、OFB モードでの処理に後進的に互換性を持つ。

付録 2 の図は、TDEA の暗号化、復号化を説明したものである。

付録 1

データ暗号アルゴリズムのための基本関数

基本関数 **KS**、**S1･･･S8**、**P** の選択が、このアルゴリズムによる暗号化の強度を決定することになる。下に挙げたものは推奨される関数の組み合わせで、**S1･･･S8** と **P** をアルゴリズムの中とおなじように記載している。これら関数の表の説明は、本文の、アルゴリズムについて述べている部分を参考にしていただきたい。

<基本関数 **S1･･･S8**>

S1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

<基本関数 **P**>

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Kn (1≦n≦16)はアルゴリズムの式(2)の、48 ビットのブロックである。従って、**KS** を説明

するには、**KEY** からとった **Kn(n=1,2…,16)**の処理式を挙げればよい。その処理式は図 3 に示す。さらに **KS** の定義を完全なものにするため、レフトシフトの図と一緒に二つの転置選択を記載する。それぞれ 8 ビットバイトの **KEY** のうち 1 ビットは、鍵生成の際のエラー探知や転送、保存のために使われる。ビット 8、16、…、64 は、それぞれのバイトが奇数のパリティからなるようにするために使われる。

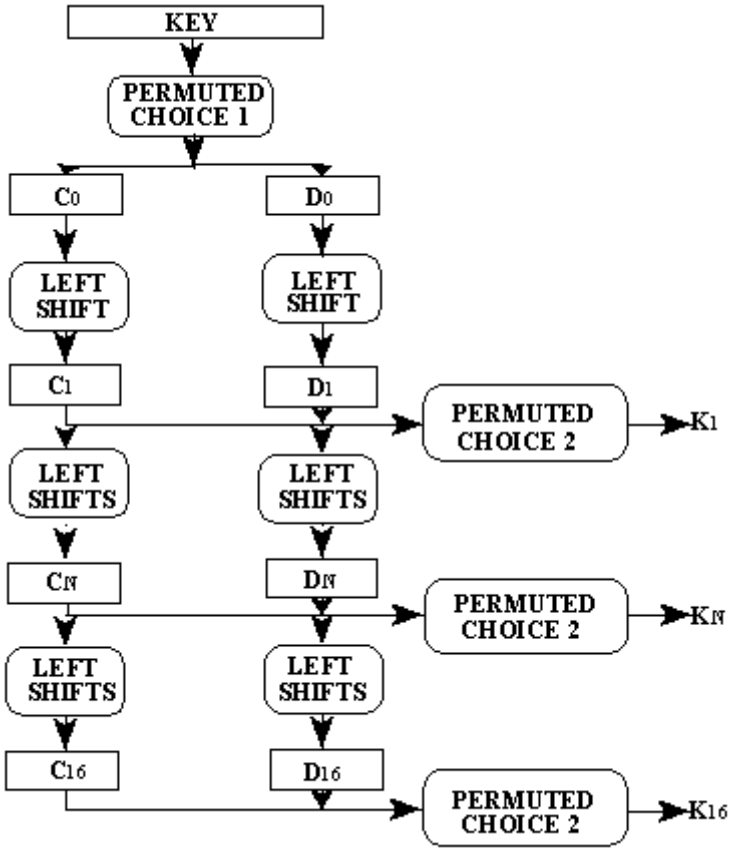
転置選択 1 は、下記の表から決定される。

<PC-1>

57	**49**	**41**	**33**	**25**	**17**	**9**
1	**58**	**50**	**42**	**34**	**26**	**18**
10	**2**	**59**	**51**	**43**	**35**	**27**
19	**11**	**3**	**60**	**52**	**44**	**36**
63	**55**	**47**	**39**	**31**	**23**	**15**
7	**62**	**54**	**46**	**38**	**30**	**22**
14	**6**	**61**	**53**	**45**	**37**	**29**
21	**13**	**5**	**28**	**20**	**12**	**4**

この表は、**C0**の選択に使われる上のパートと、**D0**の選択に使われる下のパートの二つに分けられている。KEY のビットは 1 から 64 の数字が割り当てられていて、**C0**のビットは **KEY** の 57、49、41、…、44、36 のビット、**D0**は **KEY** の 63、55、47、…、12、4 のビットが割り振られている。

C0と **D0**が定義されたら、今度は、ブロック **Cn** と **Dn** がそれぞれどのようにブロック **Cn-1**、**Dn-1** から得られるのかを定義することができる。下記の図の、個々のブロックのレフトシフトに従って見ていこう。


KEY
PERMUTED CHOICE 1
C0
D0
LEFT SHIFT
LEFT SHIFT
C1
D1
PERMUTED CHOICE 2
K1
LEFT SHIFTS
LEFT SHIFTS
CN
DN
PERMUTED CHOICE 2
KN
LEFT SHIFTS
LEFT SHIFTS
C16
D16
PERMUTED CHOICE 2
K16

<図 3>

Iteration Number , Number of Left Shifts

1	**1**
2	**1**
3	**2**
4	**2**
5	**2**
6	**2**
7	**2**
8	**2**
9	**1**
10	**2**
11	**2**
12	**2**
13	**2**
14	**2**
15	**2**
16	**1**

例えば、**C3** と **D3** はそれぞれ二度のレフトシフトによって **C2**、**D2** から得られ、**C16** と **D16** は一度のレフトシフトにより、**C15**、**D15** から得られる。1 レフトシフトとは各ビットを一コマ左に移動させることを意味し、従って一回レフトシフトを行うと、1、2、3･･･28 とあったものは、2、3・・・28、1 に変わる。

転置選択 2 は次の表のように表される。

<PC-2>

14	**17**	**11**	**24**	**1**	**5**
3	**28**	**15**	**6**	**21**	**10**
23	**19**	**12**	**4**	**26**	**8**
16	**7**	**27**	**20**	**13**	**2**
41	**52**	**31**	**37**	**47**	**55**
30	**40**	**51**	**45**	**33**	**48**
44	**49**	**39**	**56**	**34**	**53**
46	**42**	**50**	**36**	**29**	**32**

従って、**Kn** の最初のビットは **CnDn** の 14 個目のビット、2 番目は 17 個目と続いて、47 番目は 29 個目、48 番目は 32 個目のビットとなる。

付録 2
TRIPLE DES ブロック図
(ECB Mode)

TDEA 暗号方式:

$$I \rightarrow DES\ E_{K1} \rightarrow DES\ D_{K2} \rightarrow DES\ E_{K3} \rightarrow \quad O$$

TDEA 復号方式:

$$I \rightarrow DES\ D_{K3} \rightarrow DES\ E_{K2} \rightarrow DES\ D_{K1} \rightarrow \quad O$$