解 説

暗号方式と応用†

宝木和夫†† 中村 勤††

1. はじめに

情報処理，および，通信のシステムが将来にわたって人類に恩恵をもたらすためには，セキュリティが前提になることはいうまでもない．本稿では，セキュリティを確保するための一つの手段としての暗号について述べる．

最近，ハッカーらによるコンピュータへの不当アクセス，あるいは，データやプログラムの改変，通信傍受，データ盗取のような意図的な不当行為に対するセキュリティの必要性がクローズアップされている[1)~3)]．暗号は情報処理，および，通信のシステムをこのような意図的な不当行為から守るための一つの手段である．

すでに，われわれ個人に身近になっている暗号の例としては，市販されているコードレス電話の秘話機能，有料衛星放送テレビのスクランブラがあげられる．また，以前からいくつかの金融機関や公共団体などにおいては通信を秘匿するために暗号装置が導入されている．国際標準化機構 ISO においては，暗号利用技術を標準化しており[4)~9)]，これに対応して日本工業規格 JIS が制定されている[10)]．

このように，商業上の利用を目的として暗号を使う機会が増えつつある．暗号には用途に応じていろんな方式がある．

本稿は，実用レベルの暗号技術に着目し，暗号を実現するうえでポイントとなる暗号アルゴリズムの選定に関する考え方，鍵管理方法，および，評価方法について述べる．また，いくつかの応用例を紹介する．

† Cryptographic Method and Application by Kazuo TAKARAGI and Tsutomu NAKAMURA (Systems Development Laboratory, Hitachi, Ltd.).

†† (株)日立製作所システム開発研究所

2. 暗号アルゴリズム

暗号は，一言でいうと，データに不当にアクセスされても大丈夫なようにデータを白色雑音化したり，改ざん検知用コードを生成する技術である．

暗号には，手続き公開タイプと手続き秘匿タイプの二種類がある（図-1 参照）．手続き公開タイプはメッセージ（暗号文）と鍵から暗号文（メッセージ）に変換する手続きを公開し，鍵だけを送信者と受信者が秘匿してもつ方法である．一方，手続き秘匿タイプは鍵も手続きも公開せずに送信者と受信者が秘匿してもつ方法である．

（1） 手続き公開タイプ (procedure open type)

長所：手続き公開タイプは，手続き＝暗号装置（プログラム）の製造仕様書をオープンにできる．したがって，ある分野の標準暗号として複数のメーカで暗号装置を製造できる，不特定多数参加のネットワークにおいて，パソコンやワークステーションのソフトウェアとして暗号の機能を実現できるなどの商業上のメリットが得られる．

短所：しかし，その反面，メッセージ（暗号文）と鍵から暗号文（メッセージ）に変換する手続きはユニバーサルにだれにでも公開されている．このため，メッセージや暗号文の一部が敵対者に知られた場合に，鍵を逆に推定するための手掛かりとしてその手続きが用いられやすい．ある日，世界のどこかでだれかがその暗号解読方法を発表した場合，その日でその暗号の寿命は終わる恐れがある．手続きを公開することによって暗号の寿命は短くなり安全性は低下する．いままで，いくつかの手続き公開暗号が破られている．

いまだ 10 年以上破られていない手続き公開暗号の代表例として，DES (Data Encryption Standard)[11)]，RSA (Rivest, Shamir, Adleman)[12)] などがある．

（2） 手続き秘匿タイプ (procedure secret type)

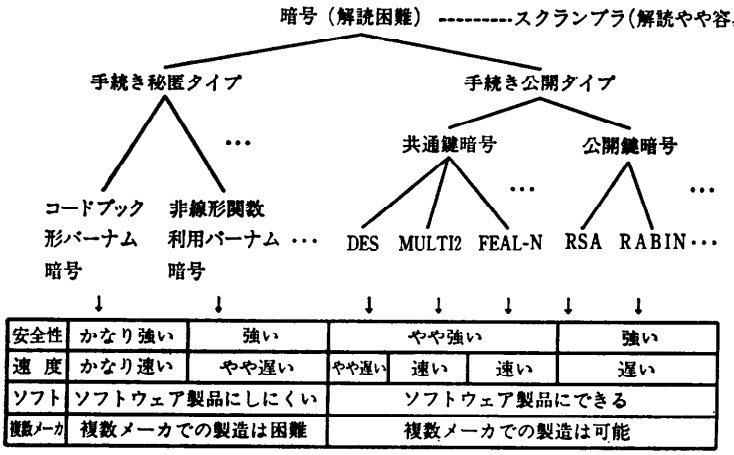


図-1 暗号アルゴリズムの分類

長所：手続き秘匿タイプでは，メッセージ（暗号文）と鍵から暗号文（メッセージ）に変換する手続き，および，その鍵が秘匿される．したがって，暗号の寿命は比較的長く安全性は比較的高い．

短所：しかし，その反面，暗号装置（プログラム）の製造仕様書はオープンにできないため，複数メーカでの製造は一般に難しい．また，不特定多数参加のネットワークにおいて，パソコンやワークステーションのソフトウェアとして暗号の機能を実現することも難しい．

このタイプの暗号装置は通常一つのメーカが厳重な情報管理のもとで製造する．いろんなメーカが出している商用暗号装置や各国の軍事用暗号装置の多くはこのタイプである．

メッセージ（暗号文）と鍵から暗号文（メッセージ）を計算する手続きのことを暗号アルゴリズムという．暗号アルゴリズムは大きく二種類ある．

（a） 共通鍵暗号アルゴリズム (common key cipher algorithm)

暗号文を作成するときに用いる鍵（暗号化鍵）と，暗号文をもとに戻すときに用いる鍵（復号化鍵）が同じ数値データであるとき共通鍵暗号アルゴリズムという．比較的小規模のハードで高速な暗号を実現しやすいという利点がある．その反面，鍵は暗号化側または復号化側のいずれで漏洩してもいけないので鍵管理を厳重に行うことが必要である．前述の DES は共通鍵暗号アルゴリズムの一つであり，0.4 M～14 M ビット/秒程度の暗号化/復号化処理速度をもつ LSI が開発されている[13]．

（b） 公開鍵暗号アルゴリズム (public key cipher algorithm)

暗号化鍵と復号化鍵が異なった数値データであり，一方の鍵（暗号化鍵）と暗号アルゴリズムを知ったとき，それから他方の鍵（復号化鍵）を計算によって導くことが困難であるとき，公開鍵暗号アルゴリズムという．もし，暗号化鍵が漏洩したとしても，復号化鍵は漏洩しないので暗号文が復号化されることはない．公開鍵暗号アルゴリズムによる暗号通信を行う場合に，鍵が漏洩しては困る箇所が受信者1カ所だけに減少するという意味で，共通鍵暗号アルゴリズムより安全性は増す．また，暗号化鍵を意図的に関係者に公開し（公開鍵），復号化鍵（秘密鍵）でメッセージを変換し，公開鍵でその逆変換を行うような処理により，ディジタル署名といわれる認証機能を実現することができる．その反面，比較的大規模のハードを必要とし，かつ，速度はあまり速くない．前述の RSA は公開鍵暗号の一つであり，1 K～40 K ビット/秒程度の暗号化/復号化処理速度をもつ LSI が開発されている[14]．これは，前述の DES の LSI に比べ数百倍遅い．

共通鍵暗号アルゴリズムについては，DES 以外にもいくつかの暗号アルゴリズムが実用化されている．共通鍵暗号アルゴリズムの代表的な具体例を次に紹介する．

（i） バーナム型の暗号[15] (vernam cipher)

バーナム型の暗号の原理を図-2 に示す．メッセージと鍵のビットごとの排他的論理和をとったものが暗号文となる．鍵が独立した乱数であれば，メッセージに対して暗号文は乱数になる．メッセージ長と同じ長さの乱数表を関係者以外には分からないよう生成し，かつ，送受信者間で共有し合うことができれば，安全な暗号通信を行うこ

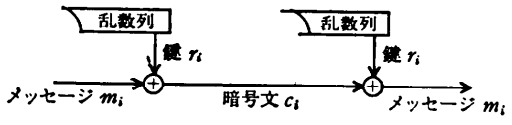
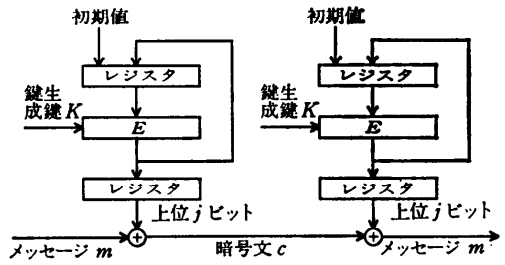


図-2 バーナム暗号の原理

とができる．バーナム型の暗号において，安全上鍵を繰り返し用いてはならないので，鍵長はメッセージ長より等しいか長くなければならない．実用上，比較的簡単な関数を用いて擬似乱数を生成し，これを鍵とすることもある．古典的な擬似乱数生成方法としては，M系列を用いる方法など[16]があるが，これは手続き秘匿暗号タイプとして用いられる．もし，安全な手続き公開タイプのファイスタル型の暗号（後述）が存在すれば，これを用いて安全な手続き公開タイプのバーナム暗号を簡単に構成できる（図-3 参照）．

（ii） ファイスタル型の暗号[17] (feistal cipher)

ファイスタル型の暗号の原理を図-4 に示す．



E: 1ブロックの暗号化関数

図-3 OFB (output feedback mode) によるバーナム暗号の実現例

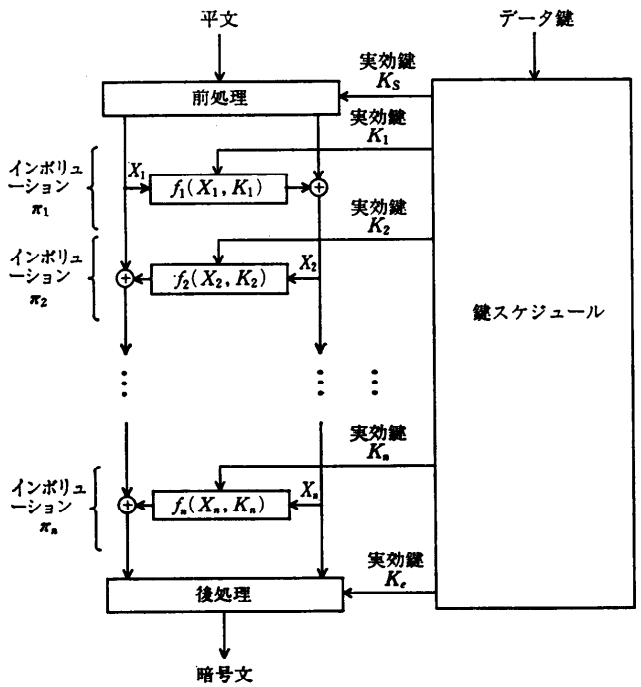


図-4 ファイスタル型の暗号の原理

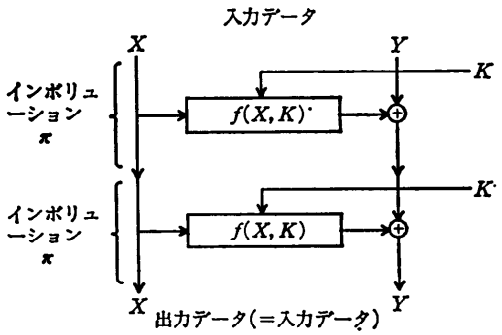


図-5 インボリューションの性質

ここで用いているインボリューション (involution) $\pi_1, \pi_2, \cdots, \pi_n$ は図-5 に示すように同じインボリューションを2回続けて実行すると実行結果が最初の入力値と等しくなるという性質を有するものである．関数 $fi(Xi, Ki)$ は，どのような関数であってもこの性質をもつ．

暗号化：平文を入力として，ある鍵を用いて

前処理→π_1→π_2→⋯→π_n→後処理

の順に処理を行い，出力を暗号文とする．

復号化：暗号文を入力として，同じ鍵を用い，

後処理$^{-1}$→π_n→⋯→π_2→π_1→前処理$^{-1}$

の順に処理を行う．出力はもとの平文となる．

ここに，前処理$^{-1}$，後処理$^{-1}$はそれぞれ前処理，後処理の逆変換を示す．また，図-4 の鍵スケジュールは，上記の暗号化，復号化に先立って，暗号化，復号化に用いる実効鍵を一定長のデータ鍵から生成する部分である．

ファイスタル型の暗号は，いくつも発表されているが，このうち，DES, FEAL-N (Fast Data Encipherment Algorithm-N)[18], MULTI 2 (Multimedia Encryption 2)[19] の概要を表-1 に示す．

DES は，1977年米国において標準暗号とされて以来，銀行などで多くの使用実績がある．専用 LSI を使えば高速な暗号化が可能である．一方，通常のコンピュータでのソフトウェア処理は，もともと考慮に入れて設計されていないため，あまり速くない．安全性についてはいまのところ，大きな欠点はみつかっていない[20]．

表-1 ファイスタル型の暗号方式比較

No	比較項目	DES	FEAL-N	MULTI 2
1	発表年	1977年	1990年	1989年
2	ブロックサイズ	64ビット	64ビット	64ビット
3	データ鍵サイズ	56ビット	64ビット，または 128ビット	64ビット，または 128ビット
4	データ鍵以外の鍵	なし	なし	システム鍵 256ビット
5	処理段数 n	16段	N段($N \geqq 4$)	8段
6	使用演算	⊕，ビットごと転置，6ビット→4ビット換字 (1ビットの処理中心)	⊕，+，ROT_2 (8ビットの処理中心)	⊕，+，−，∨，ROT_1，ROT_2，ROT_4，ROT_8，ROT_{16} (32ビットの処理中心)
7	ハード速度	速い	速い	未発表
8	ソフト速度	遅い	速い	速い
9	データ鍵総当たり探索回数	2^{56} 回	2^{64} または 2^{128} 回	2^{64} または 2^{128} 回
10	ランダム性	やや飽和状態	飽和状態 ($N \geqq 4$)	飽和状態
11	選択平文攻撃回避段数	16段以上	32段以上	二重暗号化以上 (16段以上に相当)

凡例：以下の例で，FEAL-N に対して，$L=8$，MULTI 2 に対して $L=32$ である．
⊕：ビットごとの排他的論理和，+：モジュロ 2^L の加算，−：モジュロ 2^{32} の減算，
ROT_2：Lビットのデータの左2ビット循環シフト，
ROT_a：32ビットのデータの左aビット循環シフト ($a \neq 2$)，∨：ビットごとの論理和

FEAL-N は，以前，清水，宮口らが発表した FEAL-8 の発展形であり，ハードウェア，および，ソフトウェアでの高速処理を特徴とする．インボリューション段数 N は可変であり，N を大きくすると安全性が増し，$N \geqq 32$ のとき，ビーハム，シャミアの選択平文攻撃（後述）に対して安全になるとされている[20]．

MULTI 2 は通常の 32 ビットコンピュータに装備されているマシーン命令で高速処理できるよう設計されている．二重暗号化 (16 段) 以上で使用したとき，ビーハム，シャミアの選択平文攻撃（後述）に対して安全になるとされている[21]．

上記の三つの暗号は，表-1 の項目 9〜11 に示すような安全性の条件が学会で公表されている共通鍵暗号アルゴリズムである．表-1 の項目 9〜11 は暗号強度の評価指標についてであり，次に示す評価を行うものである．

暗号強度の評価指標

（1） データ鍵総当たり探索回数：通常，暗号通信を行うとき，一つのデータ鍵を一定期間用いて比較的長いメッセージを暗号化するような運用を行う．もし，不正行為者がすべての暗号文を盗取しており，かつ，なんらかの手段によりメッセージの一部を知ったとする．そのとき，不正行為者は自分の計算機に盗取したデータを入力して，鍵を一つ一つ試していけば，いずれ正しい鍵に行き当たる．鍵をいったん知れば，盗取した暗号文を復号化してもとのメッセージすべてを入手することができる．これは既知平文攻撃 (known plaintext attack) といわれる暗号破りの一方法である．データ鍵総当たり探索回数とはこの鍵の試行回数のことをいう．FEAL-Nや MULTI 2 のように鍵長が 64 ビット長の場合，正しい鍵に行き当たるまで最短で 1 回，最長で 2^{64} 回（いずれも実際上ありえない），平均で 2^{63} 回（実際上この近辺の回数となる）の鍵の試行が必要となる．仮にスーパコンピュータで 1 秒間に十億回鍵を試行したとしても，2^{63} 回試行するまでに約 300 年かかる．

（2） ランダム性：暗号通信すべきメッセージには似たようなビットパターンがよく表れる．鍵も似たようなビットパターンのものが用いられる可能性がある．もし，不正行為者が暗号文をすべて盗取していたとする．このとき，もし，暗号文にも似たようなパターンが多数生じていれば統計的処理を行うことによりメッセージの一部を推定

される可能性が生じる．このような暗号破りの方法のことを暗号文攻撃 (ciphertext attack) という．この暗号破りに対し，メッセージまたは鍵の変化に対して暗号文はランダムに変化することが望ましい．このランダム性の評価方法としては，宮口らの二項分布近似度評価方法[17]，金らの統計的検証方法[29]などがある．ランダム性が十分な暗号関数を用い，さらに CBC (cipher block chaining) モード(**図-6**)を用いることにより，メッセージの途中にまったく同じ文字パターンが表れたとしても，対応する暗号文はまったく異なったものになる．

（3） 選択平文攻撃回避段数：通信すべきメッセージに，不正行為者が自分に都合のよいように一部のメッセージを挿入することも可能性として考えられる．この場合，暗号文（ノイズ）のなかから鍵情報（シグナル）を抽出する方法（選択平文攻撃：chosen plaintext attack）をビーハムとシャミアが発表した[20]．この方法は，攻撃対象となる暗号装置に，ある一定の差分（ビットごとの排他的論理和をとった結果）をもつ二つのメッセージの組をいく通りも入力する．このうち，一定割合（p とする）のメッセージ組については，その差分があらかじめ推定した一定の変形を受けながら暗号処理過程を伝搬する．このとき，不正行為者の計算機において正しい鍵が算出される．他のメッセージ組については，誤った鍵が算出される．このように算出される鍵の分布を作ったとき，算出される鍵全体の平均出現回数に対し正しい鍵の出現回数の比率がきわだって大きければ，正しい鍵がみつけられるとしている．この比率に相当するシグナル，ノイズ比 (S/N) の算出方法が示されている．一般に，インボリューション処理段数を増やすと，S/N，または，p が小さくなり選択平文攻撃は困難になる．さらに，この選択平

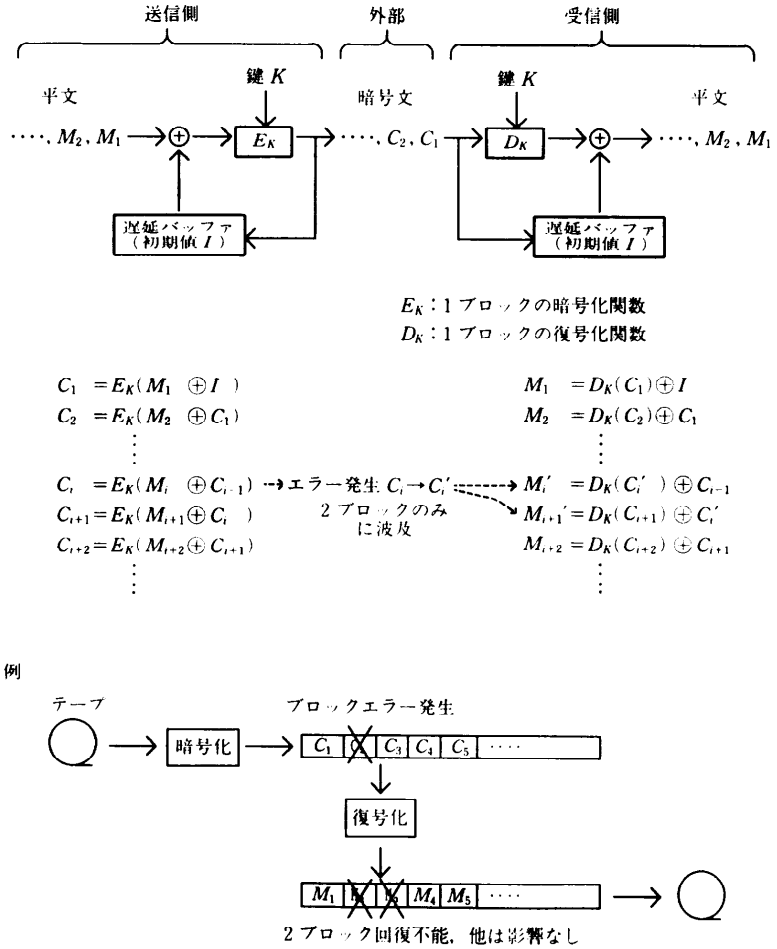


図-6　暗号文ブロック連鎖方式（CBC モード）と伝送誤り伝搬

文攻撃がうまくいくためには，攻撃対象となる暗号装置に設定されているデータ鍵が変わらないうちに，解析者に都合のよいメッセージを多量に入力しなければならない．この都合よく入力できるメッセージの長さを $2^{56}\times 8$ バイト長程度（普通の暗号装置なら千年以上要する長さ）とした場合に，選択平文攻撃を回避できるとされている段数[20),21)]を表-1，No. 11 に示す．

3. 鍵 管 理

暗号を実現するためには，暗号アルゴリズムを単にコンピュータ，あるいは，通信装置内に実装するだけでは不十分である．鍵を生成，配布，あるいは，管理するような鍵管理機能をも実装しなければならない．

ISO 8732「鍵管理」では次のことが記述されている[9)]．

（1） 鍵は裸の形で暗号機構（cryptographic facility）の外に出してはいけない．ここで，暗号機構とは，許可なくデータが露見，変更，追加，再試行，挿入，あるいは，削除されないように保護されているエリアのことである．

（2） 鍵の変更周期はシステムに存在するリスクの度合いに依存して決められる（ただし，ISO 8732では具体的な変更周期は規定されていない）．

一方，コンピュータの安全性について，ベロビンらは次のようにいっている[22)]．

（3） コンピュータのメモリは必ずしも暗号機構に相当する保護がなされているわけではない．

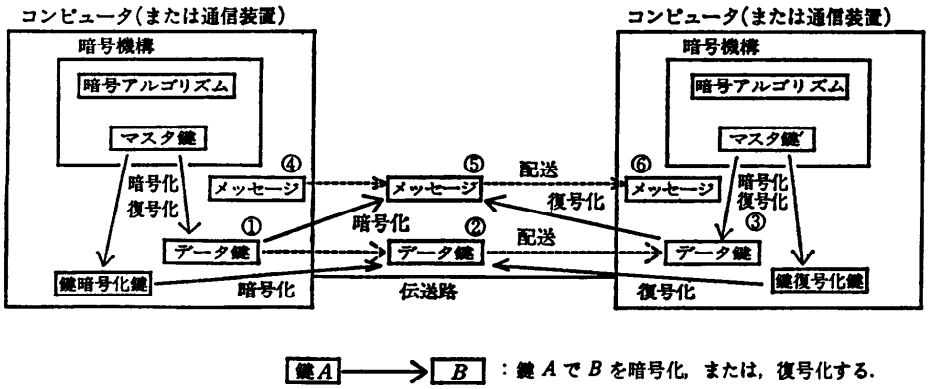
上記は鍵の安全性に関する事項である．もし，鍵が漏洩した場合，過去に通信した暗号文，および，将来の暗号文がすべて解読される恐れが生じるので，通常のコンピュータ内部のデータよりも鍵の保護を厳重にすべきとの考えであろう．このような事項を考慮に入れながら効率のよい鍵管理システムを構築する．

鍵管理システムの構築方式の一例として，階層的鍵管理方式の原理を図-7 に示す．この方式では，暗号機構（たとえば，暗号装置）に暗号アルゴリズムとマスタ鍵を置く．保持すべき鍵の個数が多いなどの理由により，コンピュータ内部で，かつ，暗号機構外部に鍵を保持する必要が生じた場合に，それらをマスタ鍵で暗号化することにより保護する．これにより，上記（1）と（3）の安全要件を満足させる．もし，コンピュータ全体に上記の意味での暗号機構と同等の安全性が確保されていれば，マスタ鍵による暗号化は不要である．また，直接メッセージに作用して暗号化を行うデータ鍵は，送受信者間で頻繁に交換できるように鍵暗号化鍵で暗号化してコンピュータ外部へ送信できるようにする．また，マスタ鍵，鍵暗号化鍵，および，鍵復号化鍵は安全に設定，変更できるメカニズムを組み込む．これにより，上記（2）の安全要件を満足させる．

マスタ鍵，鍵暗号化鍵，および，鍵復号化鍵がなんらかの手段によって図-7 に示すように安全に設定できたとする．このとき，データ鍵，および，メッセージの暗号通信の方法を次に示す．

（a） 共通鍵暗号のみを用いる方式

図-7 の暗号アルゴリズムを共通鍵暗号のみと



注） ①→②→③の暗号化，復号化の後，④→⑤→⑥の暗号化，復号化を行う．
マスタ鍵は，他の暗号機構とは無関係に独立に設定する．

図-7 階層的鍵管理の原理

する方法が発表されている[23]．この場合，鍵暗号化鍵＝鍵復号化鍵であり，①→②→③のデータ鍵の暗号化，復号化を共通鍵暗号で行うのに用いる．その後，④→⑤→⑥のメッセージの暗号化，復号化はこのデータ鍵と共通鍵暗号を用いて行う．

（b） 公開鍵暗号と共通鍵暗号を用いる方式

図-7 の暗号アルゴリズムを公開鍵暗号と共通鍵暗号の二つとする MIX 方式と名付けられた方法が発表されている[24]．この方法では，鍵暗号化鍵≠鍵復号化鍵であり，①→②→③のデータ鍵の暗号化，復号化は公開鍵暗号を用いて行う．その後，④→⑤→⑥のメッセージの暗号化，復号化はこのデータ鍵と共通鍵暗号を用いて行う．

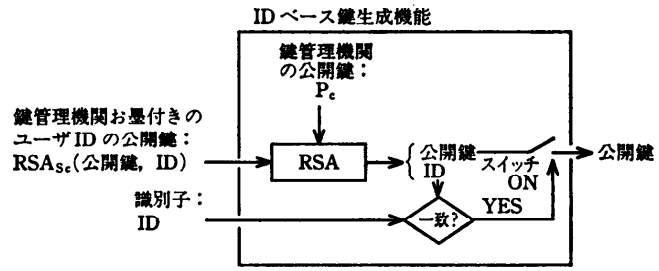
上記(a)，または，(b)を行うに先立ち，鍵暗号化鍵と鍵復号化鍵を送受信者間で図-7 のように配送，設定する必要がある．この方法として，次のいずれかが考えられる．

（1） 手持ちで配送，設定する：一般に，鍵暗号化鍵，および，鍵復号化鍵の変更周期はデータ鍵の変更周期より長くできる．手持ちで鍵を配送してもシステムの運用に大きな支障を与えないような変更周期であれば，信頼できる配送者を選び，鍵暗号化鍵，あるいは，鍵復号化鍵を手持ちで配送，設定するようにしてもよい[9]．

（2） ID（識別子）ベース鍵生成機能を用いる：鍵を手持ちでなく通信により配送，変更できるような ID ベース鍵生成機能を用いることもできる[25)~27]．これは，通信したい相手の ID，および，第三者に見られてもかまわないような数値データのみを送受信者間で通信することにより，鍵を安全に配送，あるいは，変更することを可能にする方法である．ID ベース鍵生成機能の一例を図-8 に示す．図-8 の ID ベース鍵生成機能は，図-7 の暗号機構内部に置かれ，ユーザ ID の公開鍵を欲しい場合は，鍵管理機関から

RSA_{Sc}（公開鍵，ID）……（1）

を送信してもらう．(1)式で示されるデータはユーザ ID の公開鍵と ID 名を鍵管理機関の秘密鍵 Sc でディジタル署名にしたものであり，公開鍵 Pc で復号化すると元のデータを取り出せる．もし，(1)式のデータが1ビットでも変更されていると，Pc で復号化したとき，意味のないランダムな数値となる．(1)式のデータは，鍵管理機関が発行する登録証明書のような働きをするので，「お墨付き」ともいわれる．送信者は「お墨付き」を鍵管理機関からでなく，あらかじめ受信者本人が鍵管理機関に登録して取得しておいた「お墨付き」のコピーを受信者から直接送ってもらってもよい．



Sc：鍵管理機関の秘密鍵

図-8 ID ベース鍵生成機能の一例（Kohnfelder の方法）

4. 応　用

暗号は情報システムにおいて，文字どおりの暗号化を行う以外に，認証，アクセス管理，あるいは，システム保護を行うことを目的として用いることができる（表-2 参照）．ここでは，表-2 のうちの項番1，2，3，および，10 の応用として暗号通信とファイル暗号および電子認証の実施例を示す．

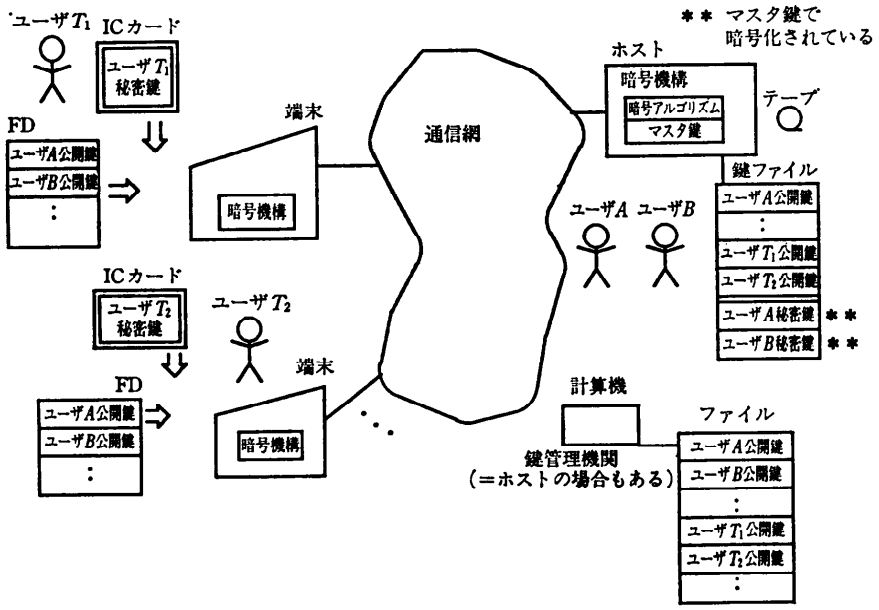
図-9 のシステムにおいて，各ユーザは秘密鍵を保持している．この秘密鍵は鍵管理機関またはユーザが生成した(秘密鍵，公開鍵)の片割れである．他方の公開鍵は鍵管理機関のファイルにユーザ名とともに登録されている．この公開鍵のファイルは各ユーザが参照できる形になっている．

（1） 暗 号 通 信

いま，端末側のユーザ T_1 がホスト側のユーザ A と暗号通信をしたいとする．このとき，ユーザ T_1 の端末では図-10 に示すように，まず，乱数を生成してこれをデータ鍵とする．そして，公開鍵暗号アルゴリズムを用いて，このデータ鍵をユーザ A の公開鍵で暗号化する．この暗号化されたデータ鍵はユーザ T_1 でも元に復号化することはできない．元に復号化できるのは，ユーザ A の秘密鍵にアクセスできるユーザ A だけである．暗号化されたデータ鍵を通信文のヘッダ部に載せる．さらに，共通鍵暗号アルゴ

表-2 情報セキュリティ技術の概要

No	目的	技術項目		技術内容	代表的技術（含国際標準）	暗号の必要性
1	(a)暗号化 情報を盗んでも無意味なものにする	暗号	手続き秘匿暗号	手順そのものを秘匿する暗号変換方法	軍事暗号（各国）	○
2			手続き公開暗号	手順を公開し，鍵のみを秘匿する暗号	米国暗号標準 DES	○
3		鍵管理	1対1鍵管理	通信相手ごとに鍵が異なる方法	ISO/CD11166（バンキング）	○
4			グループ鍵管理	複数の通信相手で鍵一つを共有	アナログ系スクランブラ	○
5	(b)認証 発信元が正当であるかどうかを確認する	相手確認	パスワード確認	暗証番号など記憶情報により確認	ISO/CD10203（バンキング）	△
6			所有物確認	IC カードなどの保持物により確認	ISO/CD10203（バンキング）	△
7			個人属性確認	指紋，声紋，筆跡などにより確認	各種技術	△
8			ゼロ知識証明	秘密情報を漏らさずに確認させる	研究レベル	○
9		認証	簡易認証	データの改ざんの有無を確認	ISO8731（バンキング）	○
10			電子認証	上記＋秘密情報を漏らさない	ISO/CD11166（バンキング）	○
11	(c)アクセス管理 資格に応じ情報授受を制限	任意アクセス管理		資格に応じアクセスを制限	米国 DOD 評価Cレベル	△
12		強制アクセス管理		資格，内容に応じ情報の流れを制御	米国 DOD 評価B，Aレベル	△
13		推論制御		統計情報から原情報の類推防止	研究レベル	○
14	(d)システム保護 侵入を発見し除去する	システム監査		客観的な立場で安全性を監査	システム監査基準（米，日ほか）	×
15		ウイルス対策		ウイルス防止，または混入検知，除去	各種ワクチン	○
16		セキュリティ評価		種々の不正行為に対する安全度を評価	各種セキュリティ評価手法	×



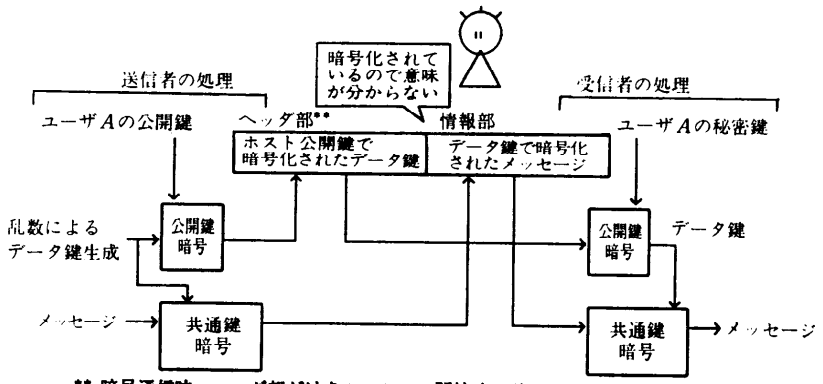
前準備　公開鍵の生成，登録，配布，保管：
生成，配布，保管……各ユーザ，または，鍵管理機関
登録……鍵管理機関

図-9 システム構成例

リズムを用いてメッセージをデータ鍵で暗号化し，これを通信文の情報部に載せる．通信文を受け取ったユーザ A は図-10 に示す手順で元のメッセージを得る．このようにすると，ユーザ A 以外はメッセージを得ることはできない．

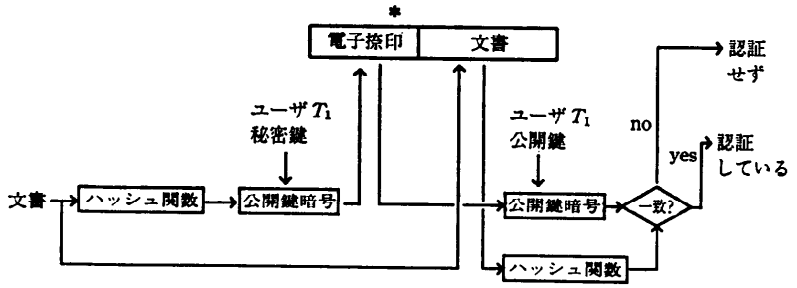
（2） ファイル暗号

ユーザ A が磁気テープを暗号化したいとする．このとき，図-10 の左側に示すような暗号化を行



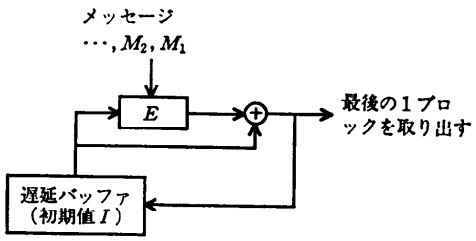
** 暗号通信時，ヘッダ部だけをセッション開始時に送ってセッションの間有効な暗号鍵として設定してもよい．
ファイル暗号時，ヘッダ部と情報部の両方をファイルに記録してもよい．

図-10　暗号化の実施例



*電子捺印（64 バイト長程度）は文書と対応可能な場所に記録される．

図-11　電子認証の実施例



E: 1ブロックの暗号化関数

図-12　ハッシュ関数実現例（Davies-Price の方法）

う．ただし，作成されたヘッダ部と情報部は磁気テープに書き込む．後日，元のメッセージに復元したい場合には，図-10 の右側に示すような復号化を行う．暗号アルゴリズムの運用モードとして，前述の CBC モードを用いる．このようにすれば，図-6 に示すように，テープの保管中にビットエラーが発生しても 2 ブロックが回復不能になるだけであり，他は元に復元される．

（3）電子認証

端末側のユーザ T_1 がメッセージを作成し，これをユーザ A に送って認証してもらいたいとする．このとき，ユーザ T_1 の端末では図-11 に示すように，メッセージのハッシュ結果 (hash result) を作成し，それを公開鍵暗号アルゴリズムを用いてユーザ T_1 の秘密鍵で暗号変換する．ハッシュ結果はメッセージに変化があった場合にその値がまったく変わってしまうような改ざん検知用のコードであり，図-12 に示すような方法で算出する[28]．

5. おわりに

情報処理，および，通信のシステムのセキュリティを確保するため暗号は有効な手段の一つである．

今回，実用レベルにある暗号技術を中心に紹介し，公開鍵暗号と共通鍵暗号を用いて暗号通信，ファイル暗号，および，電子認証を行う応用例を示した．

暗号技術の本格的利用はいまだ端緒についたばかりであり，今後，情報化の一層の進展とともに暗号を利用する機会はますます増えるものと思われる．

なお，今回述べなかったが通信回線を用いて無

記名投票やポーカゲームなどを行うことを可能にするゼロ知識証明の研究動向は注目される（表-2 No. 8）.

最後に，安全なシステムを構築するうえで安全性に漏れがないかどうかを分析，評価するセキュリティ評価（表-2, No. 16）を実施することは重要であることを付け加えておく.

参考文献

1) 金融機関等コンピュータシステムの安全対策基準解説書，(財)金融情報システムセンター（1991）.
2) 電子ウイルスの現状と課題，IPA 技術センター電子ウイルス対策研究会（1989）.
3) 郵政省電気通信局電気通信技術システム課監修：ネットワークセキュリティ，リックテレコム（1989）.
4) ISO 8372, Modes of Operation for 64-bit Block Cipher Algorithm.
5) ISO 9160, Data Encipherment—Physical Layer Interoperability Requirements.
6) ISO 9797, Data Integrity Mechanithm Using an n-bit Secret Key Algorithm.
7) ISO 8731/1, Approved Algorithm for Message Authentication—Part 1 DEA-1 Algorithm.
8) ISO 8731/2, Approved Algorithm for Message Authentication—Part 2 Message Authentication Algorithm.
9) ISO 8732, Key Management (Wholesale).
10) 物理層におけるデータ暗号化，JIS X 5051 (ISO 9160)，日本工業規格（1990）.
11) Data Encryption Standard, FIPS-PUB-46 (1977).
12) Rivest, R. L., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signature and Public-Key Cryptosystems, Comm., ACM, Vol. 21, No. 2, pp. 120-126 (1978).
13) 蓮井，秋山，太田：暗号処理用 LSI，エレクトロニクス，昭和59年10月号，p. 60 (1984).
14) 小山：暗号の数理と最近の発展[I]，電子情報通信学会誌，Vol. 73, No. 5, p. 522 (1990).
15) D. E. R. デニング著，上園，小嶋，奥島訳：暗号とデータセキュリティ，培風館（1988）.
16) 伏見：擬似乱数の発生法について，情報処理，Vol. 21, No. 9, pp. 968-974 (1980).
17) 辻井，笠原編著：暗号と情報セキュリティ，昭晃堂（1990）.
18) Miyaguchi, S., Kurihara, S., Ohta, K. and Morita, H.: Expansion of FEAL Cipher, NTT Review, Vol. 2, No. 6 (1990).
19) 宝木，佐々木，中川：マルチメディア向け高速暗号方式，情報処理学会，マルチメディア通信と分散処理研究会報告 No. 40-5 (1989).
20) Biham, E. and Shamir, A.: Differential Cryptanalysis of DES-Like Cryptosystems, CRYPT '90 (1990).
21) Takaragi, K., Hashimoto, K. and Nakamura, T.: On Differential Cryptanalysis, Special Issue on Cryptography and Information Security, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Japan (1991) (To appear).
22) Bellovin, S. M. and Merritt, M.: Limitation of the Kerberos Authentication System, Computer Communication Review, ACM SIGCOMM, Vol. 20, No. 5, pp. 119-132.
23) カール．H. マイヤー，スティーブン．M. マティス著，細貝他訳：暗号，自然社（1986）.
24) 一松監修：データ保護と暗号化の研究，日本経済新聞社（1985）.
25) Shamir, A.: Identity-Based Cryptosystems and Signature Schemes, CRYPTO '84 (1984).
26) 松本，今井：暗号鍵を通信なしで共有する方法，電子情報通信学会誌 A, Vol. J71-A, No. 11, pp. 2046-2053 (1988).
27) 岡本，田中：ID 情報に基づく暗号鍵配送方式の提案，電子情報通信学会論文誌 D-I, Vol. J72-D-1, No. 4, pp. 293-300 (1989).
28) Davies, D. W. and Price, W. L.: Digital Signature—an Update, Proc. of the Seventh International Conference on Computer Communication, Sydney Australia, North-Holland Publishing Company, pp. 845-849 (1984).
29) 金，松本，今井：暗号系の統計的安全性について，1989年暗号と情報セキュリティシンポジウム資料，電子情報通信学会（1989）.

（平成3年5月10日受付）

宝木 和夫（正会員）

昭和50年九州工業大学工学部制御工学科卒業．昭和52年東京工業大学大学院修士課程修了．同年(株)日立製作所入社．以来，同社システム開発研究所において，システム高信頼化，安全性評価，暗号と情報セキュリティの研究に従事．現在，同社システム開発研究所第4部主任研究員．東京大学工学博士．電子情報通信学会，電気学会，IEEE 各会員．

中村 勲（正会員）

昭和46年京都大学工学部電気工学科卒業．昭和48年同大学院修士課程修了．昭和53年カリフォルニア大学ロサンゼルス校大学院コンピュータサイエンス学科卒業．同年(株)日立製作所入社．以来，コンピュータネットワーク，衛星通信システム，ネットワーク管理システム，ネットワークセキュリティ，分散 OLTP システム等の研究に従事．現在，同社システム開発研究所第4部主任研究員．京都大学工学博士．IFIP TC6 Fourth International Conference on Data Communication Systems and Their Performance において Best Paper 受賞（1990-06）.