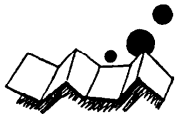
解　説



暗号方式の標準化動向†

苗村憲司†† 宮口庄司††

1. はじめに

1.1 標準化活動の概要

ISO における暗号方式の標準化動向を解説する.

標準化の検討は主として, ISO/TC 97/WG1(1981～1983), 及び ISO/TC 97/SC 20 (1984～) にて行われ, 現在までに, 5回の会議が開かれた. 標準化の審議対象は, 暗号アルゴリズムと, 暗号利用法である. 暗号アルゴリズムは, 米国政府規格である DES(Data Encryption Standard) を基とした 'DEA 1' が標準化対象である. 暗号利用法は, DEA 1 等を対象とした 64 ビットブロック暗号利用モードである. この他, 暗号利用法として, 暗号のネットワークアーキテクチャへの適用法が審議されている. 公開鍵暗号については, 今後, 具体的検討が行われる予定である.

ISO/TC 97/SC 20 の標準化審議範囲はデータの暗号のみでなく, 情報処理システム全般をカバーする方向にある.

1.2 標準暗号方式の意義

暗号方式の強さを保証するものとして, 暗号アルゴリズム, 暗号利用法, 及び, 暗号鍵を考えることが出来る. 従来, 暗号は, 暗号を使う当事者が, 暗号アルゴリズム, 暗号利用法を独自に定め, 暗号鍵と共に, 秘密に使うものであった. 最近は, 暗号アルゴリズムと暗号利用法は公開し, 暗号鍵の秘密だけで, 暗号全体の秘密を守る技術が確立されてきた. 暗号アルゴリズム等を秘密にせず, これを, 第三者に公開できれば, 次の効果が期待できる.

(a) 暗号の広範囲利用

暗号アルゴリズム等が公開できるものであれば, その標準化が可能となる. 標準化した暗号を, 通信プロトコルに適用することなどにより, 暗号が, 公衆データ通信などで, 広範囲に利用できる.

(b) 暗号製品・運用の低コスト化

暗号装置/暗号 LSI (暗号アルゴリズム等に依存) は, 標準仕様に基づき, 量産が可能となり, 低コスト化が期待できる. 暗号処理プログラムも, プログラムの統一が図れるため, 二重開発が避けられる. また暗号アルゴリズム等を秘密に保持するためのコストは, 発生しない (コストは大きい).

(c) 安全性の向上

秘密は暗号鍵に限定されているから, それだけ, 秘密範囲の小さい安全な暗号システムが実現できる.

例えば, 暗号システム内で運用されている数千台の暗号装置のうち, 1台が盗まれた場合, 被害は, その暗号装置と暗号鍵に限定される. 一方, 秘密アルゴリズムを採用している暗号システムでは, 1台の暗号装置が盗まれ, 暗号アルゴリズムが解読されると, 他の暗号装置は, すべて使えなくなる恐れがある.

1.3 検討経過

情報処理に関する国際標準化を担当する ISO/TC 97 において, 1980 年, データ暗号方式を主担務とする WG 1 が設置され, 次の作業項目 (Work item=project) が割り当てられた.

97・WG 1・1　暗号アルゴリズム
97・WG 1・2　暗号利用法
97・WG 1・3　暗号利用指針

WG 1 は, 第1回会議 (1981・1　ロンドン) 以来, 4回の会議を重ね, 暗号アルゴリズムである DEA 1 (Data Enciphering-Specification of Algorithm) の DP (Draft Proposal) 化[1], 及び, 暗号利用法である 64 ビットブロック暗号利用モード (Modes of Operation for a 64—bit Block Cipher Algorithm) の DP 化[2] を行った. 暗号のネットワークアーキテクチャへの適用法については, OSI 参照モデル[6] の, 第1層 (物理層), 第6層 (プレゼンテーション層) 等への適用法が検討された. この他, SC 20 第一回会議 (1984・1～2) では, 作業項目につき, 以下が決議された.

† The Trend of Standardization for Data Encryption by Kenji NAEMURA and Shoji MIYAGUCHI (Data Communication Division Yokosuka Electrical Communication Laboratory, N. T. T.).

†† 日本電信電話公社横須賀電気通信研究所データ通信研究部

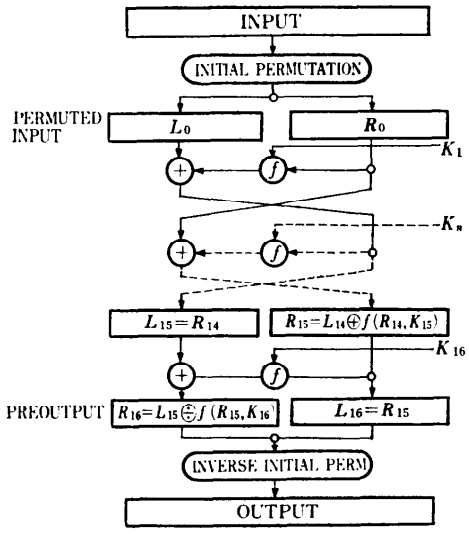


図-1 DEA 1 の暗号化の概要

(a) 暗号利用指針を，作業項目から削除する．

(b) 認証とデータ完全性 (Authentication and Data Integrity) 及び，ディジタル署名 (Digital Signatures) を，作業項目として追加する．

2. 暗号アルゴリズム

2.1 仕様の概要

暗号アルゴリズムとして最初に標準化の候補とされたのは，DES[3]を参考とした，DEA 1 である．

DEA 1 は，64 ビットの平文を，64 ビットの暗号文に暗号化し，また，平文に復号化するアルゴリズムである．暗号鍵は，64 ビット（うち，8 ビットは使われない．または，パリティビットとして，使われる）であり，暗号化と復号化とで，同一の暗号鍵を用いる．DEA 1 の暗号化の概要を，**図-1** に示す．入力データは，まず，初期転置 IP (Initial Permutation) と呼ばれる，ビットごとに転置処理を行い，これを，左右 32ビットずつのブロック L_0, R_0 に分け，次式による暗号処理を 16 回繰り返す．

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i),\quad i=1, 2, \cdots, 16$$

この出力に，IP の逆転置 IP^{-1} を施したものが，暗号化の出力である．K_i は，暗号鍵から生成される繰り返し計算用の鍵である．f は，その逆関数を求める計算量が膨大な性質を有する関数である．DEA 1 の詳細については，文献 1), 4) 等に詳しいので，参照されたい．

2.2 米国標準との相違点

米国・連邦情報処理標準 (FIPS) として定められている DES の場合，暗号鍵のビット位置 8, 16, 24, …, 64 の 8 つのビットはそれぞれ，それらのビットを含む左側の 1 オクテットの奇数パリティビットである．DEA 1 の場合これらのビットの用途は，特に規定されていない．したがって，DEA 1 は，DES の拡張形となっている．

3. 64 ビットブロック暗号利用モード

暗号の利用分野にもよるが，平文は，同じビットパターンの繰り返しが多い．これを，一意の暗号アルゴリズムと，暗号鍵とで暗号化すると，暗号文に，繰り返しパターンが現われる．これは，暗号文の統計解析に使われる危険があり，暗号全体の安全性が低下するおそれがある．このような問題を考慮して，暗号利用モードが検討された．

3.1 仕様の概要

(1) 利用モード

ISO 標準案は，暗号アルゴリズム利用モード (Modes of Operation) として，4 種を規定している．利用モードは，64 ビット，及び，64 ビット未満の暗号アルゴリズムに適用される．基本となるモードは，ECB モード (Electric Code Book mode of operation) である．

ECB モードは，暗号アルゴリズムを，そのまま繰り返し利用するモードである．暗号の利用法を拡張するモードとしては，CBC モード (Cipher Block Chaining mode of operation)，CFB モード (Cipher Feed Back mode of operation)，及び，OFB モード (Output Feed Back mode of operation) がある．

(2) 規定理由

暗号の利用法を拡張する理由は，次のとおりである．

(a) 安全対策

(b) 暗号化単位長・可変

CBC，CFB，OFB の各モードは，同一の平文，及び，鍵で暗号処理を繰り返しても，別の暗号文を生成するため，安全である．また，同じ鍵が使えれば，鍵の配送コストも抑制できる．

条件 (b) は，暗号化の単位を 64 ビット固定でなく，1〜64 ビットの間で，可変とするものである (ECB/CBC モードを除く)．このようにすると，例えば，一文字 (= 8 ビット) ごとの暗号化が可能となる．

(3) 拡張モード各論

CBC モードを，**図-2** に示す．平文は，P_i，暗号文

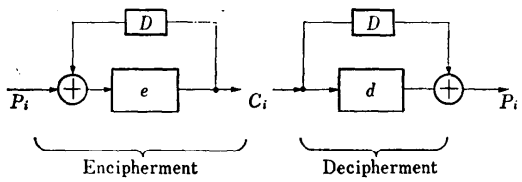


図-2 CBC モード

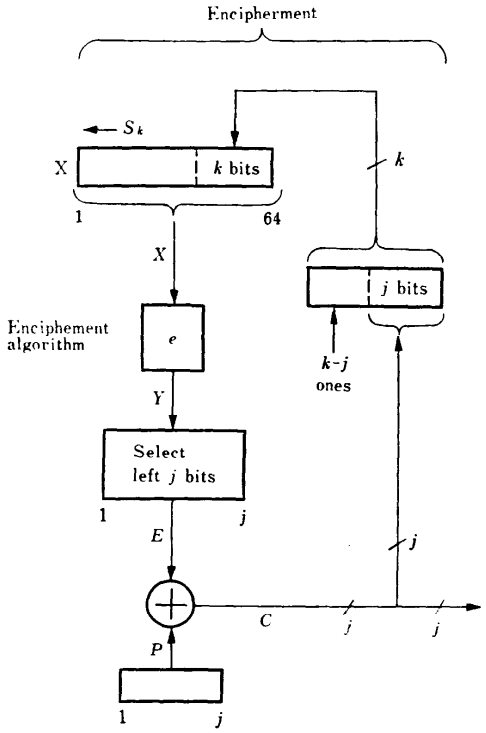


図-3 CFB モード（その1）

は $C_i(i=1,2,\cdots)$ で示す．ただし，暗号鍵は，省略してある．e は，暗号化を，d は，復号化を示す．D は64ビットのレジスタであり，最初に，IV (Initial Value) が格納される．IV は，暗号化側と復号化側とで，同一の値を用いる．IV を変えると，同じ平文から，異なった暗号文が生成される．IV の値は，第三者に知られても良い．

なお，ECB，CBC 各モードとも，暗号化の単位は，64ビット固定である．

CFB モード (暗号化側) を，図-3 に示す．ここで，X は，64ビット左シフトレジスタであり，毎回の暗号化のつど，k ビット左シフトを行う．IV の長さは，k ビットであり，最初に，レジスタ X の右側 (LSD

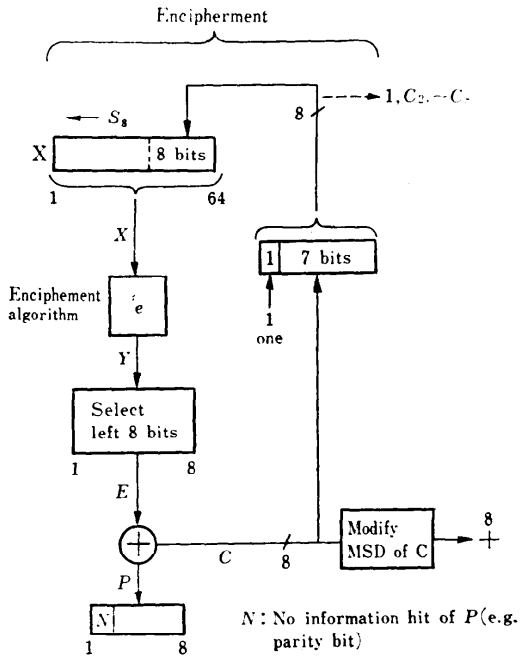


図-4 CFB モード（その2）

側）に置かれる．IV の上位側は，0とするよう規定されている．例えば，$j=8$ とすれば，8ビット単位の暗号化と復号化が行える．なお，$j=k$ が，各国の合意により推奨されている．

この他，CFB モードには，図-4 に示す特殊な CFB モードがある．この CFB モードにおいては，8ビット単位の暗号化を行う．8ビット単位の平文の MSB (最上位ビット) は，パリティなどの非情報ビットとして扱われる．図-4 において，暗号文が，通信路とインタフェースを有する部分 (Modify MSD of C で表示) は，C の MSB を強制的に，0，1，または，パリティとするか，または，元のままとするかの，4通りの変換機能がある．ただし，どれを採用するかは，暗号化側と復号化側とが，予め定めておく．この CFB モードは，暗号文でも，パリティチェックを行う場合などに，有効である．

OFB モード (暗号化側) を，図-5 に示す．この場合，暗号アルゴリズムは，乱数発生機構として使われる．IV は，CFB モードと同様，レジスタ X 内に置かれる．

CFB モード，OFB モードとも，暗号文の復号において，復号化アルゴリズムは使われない．両モードとも，64ビット未満の暗号化が行える利点があるが，暗

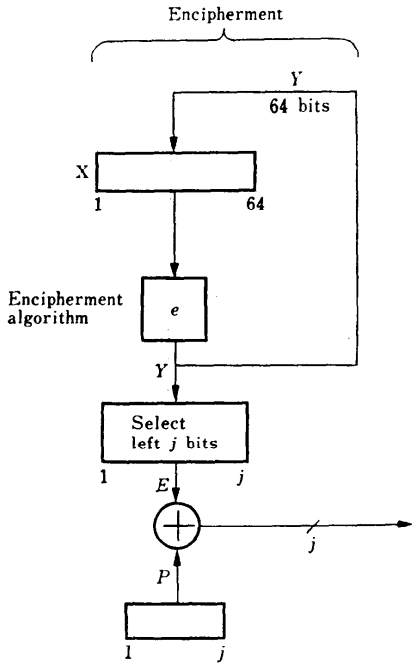


図-5 OFB モード

号化の速度は遅いという欠点がある.

3.2 米国標準との相違点

米国標準[5]は, CFB モードと, OFB モードに, 以下の点で若干の相違がある.

(1) CFB モード

(a) ISO 案の $j=k$ のみの規定である.

(b) ISO 案の $j=7$, $k=8$ のみの規定である.

(2) OFB モード

米国標準は, フィードバックを, 64 ビットでなく, j ビット ($1 \leq j \leq 64$) とするよう規定している. 即ち, 図-5 において, フィードバックは Y からでなく, E から j ビットが, X の下位 j ビットに入力するように行われる. このとき, レジスタ X は, 暗号化のつど, j ビットの左シフトを行うレジスタとなる.

したがって, ISO の暗号モードの規定は, OFB モードを除き, 米国標準をカバーしていることがわかる.

4. OSI 参照モデルにおける暗号方式

審議された主要点について, 解説する.

4.1 (N)-暗号接続

本節の検討は, TC 97/SC 16 で行われている[7]. N レイヤエンティティ中の, 同位の暗号機能により保護される. (N)-接続 ((N)-Connection) を, (N)-暗号接続 ((N)-Cryptographic Connection) と定義している. 暗号接続では, 同位のエンティティには, 同じ暗号鍵, 及び, 同じ暗号機構が必要とされる.

(N)-暗号接続の結果, 暗号サービスとして,

(a) Data Privacy (N)-Service

(b) Data Integrity (N)-Service

(c) Authentication (N)-Service

が提供される. ここで, a は, データの秘密保持を, b は, データが正しいこと (データ完全性) を, c は, 通信相手の確認を, それぞれ保証する.

なお, 暗号処理及び, 暗号鍵管理は, 各レイヤごとに独立したものと定められている.

4.2 物理層/データリンク層の暗号化[9),10)]

物理層/データリンク層については, FIPS 1026 を元に審議されている. 物理層/データリンク層の暗号方式・標準化の目的は暗号装置 (DEE: Data Encipherment Equipment)の運用基準(Inter Operability)を規定することである. 暗号装置は, データ端末装置 (DTE: Data Terminal Equipment) と, データ回線終端装置 (DCE: Data Circuit-terminating Equipment) の間に, 接続される. 回線インタフェースは, CCITT インタフェース (V・24, X20 他) に従う. 暗号アルゴリズムは, DEA 1 に代表される 64 ビット暗号アルゴリズムである.

(1) 物 理 層

暗号利用モードは, 1 ビット CFB モードを使う. IV 長は, 利用者の選択範囲を広げるため, 48 ビット (クラスⅠ) と, 64 ビット (クラスⅡ) と, 2 種類が規定されている. 物理層の暗号装置は, 伝送制御手順に依存しないため, その適用範囲は広い.

(2) データリンク層

暗号利用モードは, 4 種類が許される. 伝送制御手順は, HDLC である. 暗号化の範囲は, 2 通りある. 第一の規格は, 全フレームの暗号化であり, 第二の規格は, Ⅰフィールドの暗号化である (**図-6** 参照). Ⅰフィールドの暗号化は, 分岐/ループ・リンクにおいて, 別々の暗号鍵が利用でき, 安全性は高い. 一方, 全フィールド暗号化において, 暗号装置は, データリンク層の制御フィールド (A, C) を読取る必要はない.

5. 公開鍵暗号

5.1 技術参考資料の作成

技術参考資料の作成理由は, その内容が, いずれ

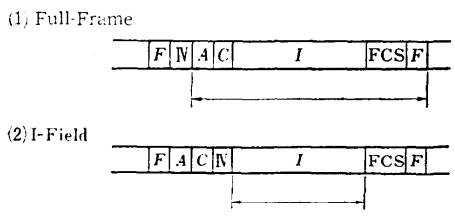


図-6 データリンクレイヤの暗号化範囲

表-1 公開鍵暗号の審議範囲

応用 / 方法	鍵配送	ディジタル署名	調停者付ディジタル署名	メッセージ内容の隠ぺい
RSA	○	○	○	○
DH	○	—	—	—

は，ISOのデータ暗号標準になると期待できる点で意義があると，各国が同意したことによる．

5.2 技術参考資料の範囲

技術参考資料 (consultative document) は，年次報告として，毎年更新し，以下の内容を含むものとされている．

（a） 最新の実用的な，暗号/セキュリティ技術

（b） 特定分野の，国際規格化の検討開始時期

（c） 次年度の作業項目・案

1984年2月現在の技術参考資料のカバー範囲は，**表-1** に示すものであり，RSA法[12]と，DH法[13]が，含まれている．

6. むすび

暗号方式の標準化動向について，ISOの動向を中心に解説した．

今後我が国においても，データ通信，データベースの普及に伴って，暗号が利用されることは，必至とみられる．暗号を，広く多数者間で使うための重要な課題の一つは，暗号方式の標準化である．

標準化のための検討は，ISO/TC 97/SC 20，SC 16で行われている．その範囲も，暗号技術だけにとどまらず，認証，ディジタル署名等に拡大される方向にある．これは，各国が，セキュリティ技術に関する国際規格化の重要性を認識してきた結果といえる．

なお，SC 20発足に伴い，情報処理学会規格委員会SC 20専門委員会が設置され（59年1月；主査：東大宮川教授），我が国としても，本格的な技術検討を行うこととなった．

参考文献

1) Data Encipherment-Specification of Algorithm DEA 1, ISO/DP 8227 (1982-12-16).
2) Modes of Operation for a 64-bit Block Cipher Algorithm, ISO/DP 8372 (1983-7-1).
3) Data Encryption Standard, FIPS PUB 46, NBS (Jan. 1977).
4) 土居他：公衆暗号系，情報処理，Vol. 22, No. 1, pp. 38-46 (Jan. 1981).
5) DES Modes of Operation, FIPS PUB 81, NBS (Dec. 1980).
6) 苗村他：ネットワークアーキテクチャ，情報処理，Vol. 24, No. 10, pp. 1211-1217 (Oct. 1983).
7) Working Draft for an Addendum to ISO 7498 on security, ISO/TC 97/SC 16 N 1643 (Oct. 1983).
8) Minutes of the Meeting of the Adhoc Group of ISO/TC 97/WG 1, Held in AFNOR, on 1981 May 11-13.
9) Interoperability Requirements for the Use of a 64-bit Block Cipher Algorithm in the Physical Layer of Data Communications, ISO/TC 97/WG 1, N 96 (Mar. 1983).
10) Interoperability and Security Requirement for Use of the Data Encryption Standard in the Physical and Data Link Layers of Data Communications, ISO/TC 97/WG 1, N 22 (Jun. 1981).
11) Brief Report of Fourth Meeting, 14-17(Feb. 1983), London, ISO/TC 97/WG 1, p. 2 (Mar. 1983).
12) Rivest et al. A Method for Obtaining Digital Signatures and Public-key Cryptosystems, Com. of the ACM, Vol. 21, No. 2, pp. 120-126 (Feb. 1978).
13) Diffie et al. New Direction in Cryptography, IEEE Trans. on Information Theory, Vol. IT-22, No. 6, pp. 644-654 (Nov. 1976).
14) House Report No. 96-1540, The Goverment's Classification of Private Ideas, Thirty-fourth Report by the Committee on Government Operations (Dec. 22, 1980), note 7, International Traffic in Arms Regulations, pp. 105-108.

（昭和59年1月30日受付）