■1 群（信号・システム）- 3 編（暗号理論）

1 章 ブロック暗号

（執筆者：盛合志帆）[2009 年 2 月 受領]

■概要■

【本章の構成】

■1 群 - 3 編 - 1 章

1-1 ブロック暗号の概要

（執筆者：盛合志帆）[2009 年 2 月 受領]

1-1-1 ブロック暗号とは

ブロック暗号は，一定長のブロック単位で暗号化・復号を行う共通鍵暗号アルゴリズムである．ブロック長は，64 ビットや 128 ビットが代表的であるが，可変長のものや 256 ビットなど長いものもある．ブロック暗号は，主として守秘機能を実現するために用いられるが，メッセージ認証やエンティティ認証プロトコルの構成要素として用いられるなど，最も基本的で広く利用されている暗号プリミティブといえよう．

代表的なブロック暗号として，米国政府により制定された DES，Triple DES，AES のほか，企業や大学で開発され，各種分野で利用されているブロック暗号も数多く存在する．1997 年より始まった米国での AES 制定プロジェクトに影響を受けて，日本や欧州でもこのような暗号アルゴリズムを公募・評価・選定するプロジェクトが行われた（15 章参照）．

本章ではまずブロック暗号の概要について述べる．次に代表的なブロック暗号として，米国政府標準暗号 DES，Triple DES，AES について述べ，日本で開発された MISTY1，Camellia，CLEFIA についても紹介する．

1-1-2 ブロック暗号の基本構成

ブロック暗号の基本構成を図 1·1 に示す．ブロック暗号は平文ブロックを暗号文ブロックに変換する「データランダム化部」と，鍵からデータランダム化部で用いられる鍵データ（副鍵）を生成する「鍵スケジュール部」からなる．暗号化の手順は，まず，鍵スケジュール部において鍵から複数の副鍵が生成され，その副鍵を用いてデータランダム化部で平文ブロックから暗号文ブロックへの変換が行われる．復号の手順も同様に，鍵スケジュール部において鍵から副鍵が生成され，その副鍵を用いてデータランダム化部により暗号文ブロックから平文ブロックへの変換が行われる．暗号によっては，副鍵の生成とデータランダム化部での暗号化（復号）処理が同時に（on-the-fly で）実行できるものもある．

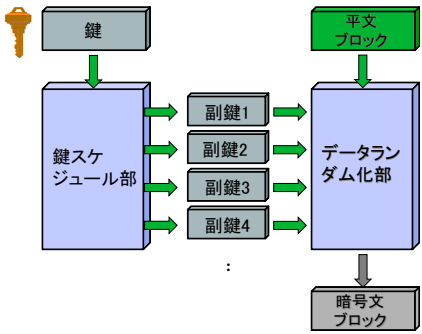

図 1·1　ブロック暗号の基本構成

1-1-3 ブロック暗号の代表的な構造

ブロック暗号のデータランダム化部は，複数のラウンド関数を繰り返した構造（積暗号（product cipher））になっており，多くの場合，回路規模を小さくするために同一のラウンド関数を繰り返す構造（繰り返し暗号（iterated cipher））になっている．各ラウンドのラウンド関数には，ラウンドごとに異なる副鍵が入力される．代表的な構成法として図 1･2 に示す Feistel 構造と図 1･3 に示す SPN 構造がある．Feistel は暗号学者 Horst Feistel にちなんでおり，SPN は Substitution Permutation Network の略である．

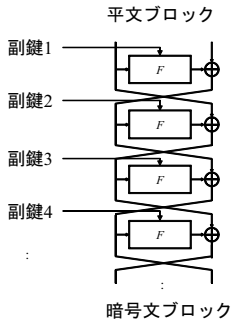

図 1･2 Feistel **構造**

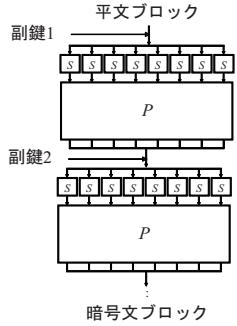

図 1･3 SPN **構造**

(1) Feistel 構造

Feistel 構造は図 1･2 に示すように，平文ブロックを 2 分割し，片方を F 関数へ入力し，その出力ともう片方と排他的論理和をとるという処理を繰り返し適用することで暗号化を行うものである．DES がこの構造を初めて採用し，その後多くの暗号に採用されている．Feistel 構造には以下のような特徴がある．

- 暗号化／復号が同じロジック
  Feistel 構造では，副鍵の順序を入れ換えるだけで暗号化モジュールが復号にも利用できる．したがって，暗号化モジュールだけをもっていれば暗号化も復号も行うことができ，回路規模やプログラムエリアを節約できる．また暗号化処理と復号処理がほぼ同じ速度となる．

- F 関数の制約が少ない
  Feistel 構造では復号時に F 関数の逆関数を計算する必要がないため F 関数は全単射である必要がない．

- コンパクトな実装向き
  データ幅がブロック長の半分でよいため，コンパクトな実装に向いている．一方，1 ラウンドでブロックの半分しか変換されないため，十分なデータかく拌を行うためには SPN 構造より多くのラウンドが必要となる．

（2）SPN 構造

SPN 構造は図 1･3 に示すように，S ボックス（Substitution）と呼ばれる変換と Permutation と呼ばれる変換を組み合わせたものである．S ボックスは通常，非線形変換で，ソフトウェアではテーブル参照で実装されることが多く，入力サイズは実装コストを考慮して 8 ビット程度以下であることが多い．Permutation は複数の S ボックスからの出力を入力とする置換処理で，S ボックスからの出力結果を拡散する役割を担っている．SPN 構造の特徴は以下のとおりである． SPN 構造をもつ代表的な暗号には，AES がある．

- 暗号化／復号が違うロジック
  S ボックスや Permutation などの構成モジュールは暗号化と復号で異なる．しかし，実装時に暗号化と復号でモジュールが共有できるよう設計上様々な工夫がされることが多い．

- S ボックスや Permutation などの構成モジュールは全単射でなければならない
  これは復号関数が暗号化関数の逆関数となるために必要な条件である．

- データ幅がブロック長と等しく，高速な実装に向いている

■1 群 - 3 編 - 1 章

1-2 代表的なブロック暗号

（執筆者：盛合志帆）[2009 年 2 月 受領]

1-2-1 米国政府標準暗号 DES, Triple DES, AES

米国は 1970 年代から積極的に政府主導で暗号技術の評価や標準化に取り組んできた．米国政府標準のブロック暗号 DES, Triple DES, AES の制定はその代表的な取り組みである．

（1）DES

DES（Data Encryption Standard）は 1977 年に米国連邦政府情報処理規格 FIPS（Federal Information Processing Standards）46[1)] として制定された，初めてのアルゴリズム公開の商用暗号である．オープンネットワークを介して安全に情報交換を行うためには，暗号のしくみ（アルゴリズム）を公開する必要がある．DES は，アルゴリズムを公開にしても鍵さえ秘密にしておけば，その安全性が保たれるような暗号として設計された．DES の誕生はこの点で画期的である．DES は米国政府により 1983 年から 5 年ごとに見直しが行われ，20 年以上利用されてきた．しかし，コンピュータやネットワークの進展により，DES の 56 ビットという鍵長が鍵の全数探索により現実的に解読可能な範囲に入ってきたことなどから，1993 年には米国政府調達暗号としての DES の利用は 1998 年で打ち切ることが示され[2)]，2005 年に廃止された．

（2）Triple DES

Triple DES は，DES の難点である 56 ビットという鍵長の短さを克服し，より長い鍵を用いることにより安全性を向上したアルゴリズムである．Triple DES は 1999 年に当面の米国政府標準暗号として FIPS46-3[3)] に規定された．Triple DES の実装には，DES のモジュールを活用することができる．E_K を鍵 K による DES の暗号化関数，D_K を復号関数とし，平文ブロックを M，暗号文ブロックを C とすると，Triple DES による暗号化処理及び復号処理はそれぞれ式 (1･1)，式 (1･2) のように表される（図 1･4 参照）．

$$C = E_{K3}(D_{K2}(E_{K1}(M))) \tag{1･1}$$

$$M = D_{K1}(E_{K2}(D_{K3}(C))) \tag{1･2}$$

ここで三つの鍵 $K1$，$K2$，$K3$ はそれぞれ 56 ビットで，独立に選ばれる必要がある．この方式を特に 3-Key Triple DES と呼んでいる．これに対し，$K1 = K3$ の場合を 2-Key Triple DES と呼ぶ．また $K1 = K2 = K3$ とすれば Triple DES は DES と等価なアルゴリズムとなるため，鍵の運用で DES との互換性をとることが可能となっている．なお，2-Key Triple DES の強度は 80 ビット相当であるため，米国政府系システムでの使用は 2010 年までとなっている[4)]．

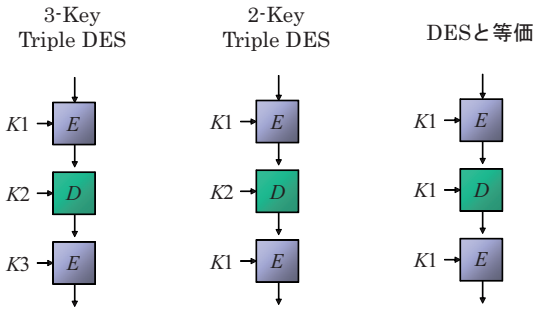

図 1･4 Triple DES

（3）AES

1997 年，米国政府は新しい米国政府標準暗号 AES（Advanced Encryption Standard）の制定作業を開始することを発表し，世界中から AES の候補となる暗号を公募した．応募された暗号の中から 15 方式が AES 候補暗号として認定され，このうち，ベルギーのデーメン（Daemen）とライマン（Rijmen）が提案したレインダール（Rijndael）という暗号が 2001 年末に米国連邦政府情報処理規格 FIPS 197[5]として制定された．AES はソフトウェア実装，ハードウェア実装とも非常に優れた処理性能をもち，IC カードなど制限された環境にも適している．また，処理並列度が高いこと，実装攻撃に対する防御が容易であるなどの特徴ももっている．

米国政府標準暗号の歴史を表 1･1 にまとめる．

表 1･1 米国政府標準暗号の歴史

1977 年	DES を FIPS46 として登録
1983 年	DES を再承認
1988 年	FIPS46-1 発行（DES を再承認）
1993 年	FIPS46-2 発行（DES を再承認したが代替アルゴリズムを検討開始）
1997 年	AES プロジェクト開始
1999 年	Triple-DES を FIPS46-3 として登録
2001 年	AES を FIPS197 として登録
2005 年	FIPS46-3 を廃止, NIST SP800-67 へ移行

1-2-2 そのほかのブロック暗号

（1）MISTY1

MISTY1 は 1996 年に三菱電機株式会社が開発したブロック長 64 ビット，鍵長 128 ビットのブロック暗号である[6]．MISTY1 の安全性の根拠の一つは，差分解読法（differential cryptanalysis）と線形解読法（linear cryptanalysis）に対する証明可能安全性（provable security）を示せる構造を採用していることにある．差分解読法と線形解読法は，ブロック暗号に対する汎用的な解読法として最も強力なものとされており，暗号設計者にはこれらに

対する十分な強度を保証することが求められる．MISTY1 は証明可能安全性の理論に基づいて，差分解読法や線形解読法に対する安全性を数値として示している．そのほか，サイズの異なる S ボックスや，鍵に依存してかたちの変化する線形変換（FL 関数）の採用など安全性を高める工夫も施されている．更に MISTY1 は並列処理を強く意識して設計されており，ハードウェアや，命令レベルでの並列処理が可能なプロセッサ上で高速に実装することが可能となっている．また，ハードウェアでは 10K ゲート以下で実装できることも特徴の一つとなっている．

また，MISTY1 をベースとして設計された 64 ビットブロック暗号 KASUMI は移動体通信方式 GSM ，W-CDMA の標準暗号化アルゴリズムとして採用されている．

（2）Camellia

Camellia は 2000 年に日本電信電話株式会社と三菱電機株式会社によって共同開発されたブロック長 128 ビットのブロック暗号である[7]．鍵長は AES と同様，128，192，256 ビットの 3 種類をサポートしている．その基本構造は，鍵長が 128 ビットの場合，18 段の Feistel 構造，鍵長が 192 ビットまたは 256 ビットの場合，24 段の Feistel 構造であり，6 段ごとに鍵依存線形変換 FL/FL^{-1} 関数が挿入されている．Camellia は差分解読法や線形解読法に対する安全性はもちろん，その後発表された高階差分攻撃（higher-order differential attack），補間攻撃（interpolation attack），関連鍵攻撃（related-key attack），丸め差分攻撃（truncated differential attack）などの攻撃法に対しても安全となるように設計されている．

Camellia はローエンド IC カード搭載の 8 ビット CPU から高性能サーバなどに搭載される，64 ビット CPU に渡る幅広いプラットフォーム上でのソフトウェア実装とハードウェア実装の両面で効率的な実装が可能となるように設計されている．

（3）CLEFIA

CLEFIA は 2007 年にソニー株式会社と名古屋大学によって共同開発された 128 ビットブロック暗号である[8]．鍵長は AES と同様，128，192，256 ビットに対応しており，高い安全性を保ちつつコンパクト性と高速性を両立している点が大きな特長である．CLEFIA の全体構造は一般化 Feistel 構造を採用し，拡散行列切り替え法[9]（DSM: Diffusion Switching Mechanism）などの設計技法を用いることで少ない処理量で高い安全性を確保した．拡散行列切り替え法とは，複数の拡散行列を利用することで差分解読法や線形解読法に対する強度を向上する手法である．この結果，ハードウェア，ソフトウェアを問わず高速かつコンパクトな実装を可能にしている．ハードウェア実装においては，0.09 μm CMOS 標準セルライブラリを使用した場合に 6Kgate 以下で 1.60 Gbps を達成しており，更にソフトウェア実装においては，クロック周波数 2.4 GHz の AMD Athlon 64 プロセッサで 12.9 cycles/byte, 1.48 Gbps を達成している．CLEFIA は小型ハードウェア実装において AES を大きく上回る性能を発揮する．

■参考文献

1) National Bureau of Standards, “ Data Encryption Standard, ” FIPS Publication 46, 1977.
2) National Institute of Standards and Technology, “ Data Encryption Standard, ” PIPS Publication 46-2, 1993.

3) National Institute of Standards and Technology, “ Data Encryption Standard, ” FIPS Publication 46-3, 1999.
4) “ Recommendation for Key Management, ” NIST SP 800-57 Part 1, 2007.
5) National Institute of Standards and Technology,“ Announcing the Advanced Encryption Standard (AES), ” FIPS Publication 197, 2001.
6) M. Matsui,“ New Block Encryption Algorithm MISTY, ”Proceedings of the 4th international workshop of Fast Software Encryption, Lecture Notes in Computer Science 1267, pp.54-68, Springer-Verlag, 1997.
7) K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakjima, and T. Tokita, “ Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms, ” Proceedings of the 7th Annual Workshop on Selected Areas in Cryptography, SAC2000, Lecture Notes in Computer Science 2012, pp.39-56, Springer-Verlag, 2001.
8) T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata,“ The 128-bit Blockcipher CLEFIA, ”Proceedings of the 14th international workshop, FSE 2007, Lecture Notes in Computer Science 4593, pp.181-195, 2007.
9) T. Shirai and K. Shibutani, “ On Feistel structures using a diffusion switching mechanism., ” Proceedings of the 14th international workshop, FSE ’ 06, Lecture Notes in Computer Science 4047, pp.41-56, Springer-Verlag, 2006.