1. 21世紀初頭の暗号技術

3. 共通鍵暗号の発展

宝木 和夫
(株)日立製作所　takara@sdl.hitachi.co.jp

角尾 幸保
日本電気(株)　tsunoo@bl.jp.nec.com

大熊 建司
(株)東芝　kenji.ohkuma@toshiba.co.jp

松井　充
三菱電機(株)　matsui@iss.isl.melco.co.jp

盛合 志帆
(株)ソニー・コンピュータエンタテインメント
shiho@rd.scei.sony.co.jp

下山 武司
(株)富士通研究所　shimo@flab.fujitsu.co.jp

共通鍵暗号は，安全，安心な社会を実現する上で重要な技術の1つであり，ISOやCRYPTRECなどでさまざまなプラットフォームでの利用を想定した方式が提案されるとともに，普及へ向かっている．共通鍵暗号に関する技術としては，ブロック暗号，ストリーム暗号，擬似乱数生成器，ハッシュ関数などがあり，それぞれの特性と用途を持つ．安全性評価尺度としては，暗号処理仕様を公開するという前提のもとに，鍵の全数探索法，差分攻撃法，線形解読法など種々の解読方法をクリアすることが求められる．ここでは，共通鍵暗号の概要を紹介するとともに，CRYPTREC電子政府推奨暗号リストに掲載されたいくつかの共通鍵暗号方式について紹介する．

共通鍵暗号の進展の経緯と概要

21世紀に入り安全，安心な社会の実現がますます求められるようになってきた．そのためには，暗号などの情報セキュリティ技術を用いて情報の不正な改ざんや盗聴などを阻止することが重要な対策の1つとなる．

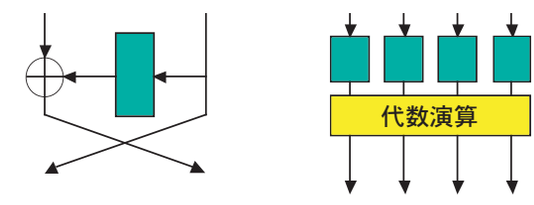
暗号は，情報を守る目的で別の情報に変換する方法である．古来よりさまざまな種類の暗号が考案され，近年に至るまで，主に国家や軍事の目的で使われてきた．1970年代に入りコンピュータネットワークが出現し始めた頃から，商用ネットワーク利用に向けた暗号技術の時代が到来した．21世紀に入ってからは，ISO，AES，CRYPTREC，NESSIEなどで，さまざまなプラットフォームでの利用を想定した次世代の暗号方式が提案され，普及へ向かっている．暗号の標準化に関する変遷については，本誌の暗号標準化に関する記事「評価体制と標準化の内外動向」に詳しく書かれているので興味のある読者は併せて参照されたい．

ここでは，共通鍵暗号について，21世紀初頭の現在の視点から概観する．

●共通鍵暗号の分類，タイプ分け

共通鍵暗号に関する技術には，その要素技術（要素部品）として，ブロック暗号，ストリーム暗号，擬似乱数生成器，ハッシュ関数などがある．これらをうまく使うことで，データの暗号化や改ざん検知（暗号学的チェックサム）を行うことができる．

ブロック暗号を構成するには，**図-1**に示すようなFeistel構造やSP（Substitution-Permutation）構造があり，前者は逆変換（復号）が簡単に実装できる，後者は撹拌効果が高いなどそれぞれ特徴がある．



Feistel構造の段関数　　SPN構造の段関数

ブロック暗号の代表的な構成法に，Feistel構造によるものとSPN構造によるものとが挙げられる．前者では左右を交互にデータ撹拌する構造である一方，後者は局所撹拌と大域的撹拌とを交互に重ねる．Feistel構造は1段の撹拌効果が低い反面，軽量であったり，逆変換が容易などの利点も多い．

図-1　Feistel構造とSPN構造

ブロック暗号に対して，ストリーム暗号と呼ばれるものがある．これは擬似乱数生成器を使ってデータを暗号化する方法である．擬似乱数生成器には，線形フィードバックシフトレジスタに基づくものと，大きな内部状態を使うものとに大別される．前者は，LSIとして実装すると極端に小さくなるので，携帯電話など，低コスト低消費電力が要求されるプラットフォームで利用される．一方，大きな内部状態を使う擬似乱数生成器は処理が高速であるので大容量のコンテンツ向けの処理などに用いられる．

ハッシュ関数は，ディジタル署名などで使用される技術であり，ある種の強固な認証を実現する．ハッシュ関数が達成しようとする安全性には主に2種類があり，それぞれ一方向性，衝突回避性と呼ばれる．一方向性とは，ハッシュ値からそれを生み出すような入力となるデータの生成が困難であること，衝突回避性とは，出力が同じとなるような2つの異なる入力データを生成するのが困難なことである．現在，用いられるハッシュ関数にはMD5，SHA-1，RIPEMDなどがある．

●安全性の考え方

1977年に発表された米国暗号標準DES以来，現代の共通鍵暗号に通じるようないくつかの安全性要件が明らかにされた．

暗号処理の仕様を非公開から公開へ

従来，暗号の利用は比較的狭い範囲に限定されていて，暗号処理の仕様をあえて公開する必要はなかった．しかし，1970年代以降，工業製品としての普及や，第三者による安全性検証等のニーズが生じ，暗号処理の仕様を公開することが求められるようになってきた．DESはその仕様が公開された暗号であった．仕様が公開された場合，暗号への要求はさらに厳しくなる．たとえば，従来からの古典的な暗号解読モデルとしては，敵対者は，入力データや出力データの一部を入手したり変更したりできた．さらに，仕様が公開された場合，暗号化関数も敵対者に知られるという前提が加わり，暗号の設計者は，この前提にも耐えられるような強固な暗号の設計をしなければならない．ここにおいて，後述するように暗号理論上の種々の課題が生じる．

クリアすべき種々の安全性評価尺度

暗号の仕様が完全に公開されて既知であることを前提とする，種々の安全性評価尺度をクリアしなければならない．

(a) 鍵の全数探索に対する安全性

たとえば，鍵が1ビットの長さしかなく，“0”か“1”かのどちらかの2通りであったとすれば，敵対者は暗号文を入手し，2通りの鍵の値を試せば暗号は解けるだろう．同様に，鍵がkビットの長さの場合，2^k通りの鍵の値を全数探索すれば暗号は解けるだろう．さらに全数探索法の改良方法として，鍵を1個1個単純に試すのではなく，事前に平文−暗号文−鍵の照合表を膨大な個数用意しておき，平文−暗号文が得られたら逆引きで高速に鍵を見つけ出すような，タイム−メモリトレードオフ法と呼ばれる強力な解読方法もある．DESでは鍵の長さは56ビットであった．しかし，これでは，現在の高性能なパソコンを複数台用いれば，鍵の全数探索方法で比較的簡単に解けてしまう．現在，暗号の鍵の長さとしては128ビット以上が安全性の1つの目安となっており，次世代米国標準であるAESの仕様にも反映されている．

(b) 差分解読，線形解読等に対する安全性

上記の全数探索方法は，暗号の内部構造の良し悪しに関係なく，とにかく鍵を片っ端から調べていくという，ブルートフォース型の解読方法であった．これに対し，暗号ごとにそれぞれ異なるような内部構造に着目し，鍵を全数探索よりも効率的に見つけ出すという，ショートカット型の暗号解読方法がある．その代表的な方法として，たとえば，差分解読がある．これは，大量の平文／暗号文組を集め，平文同士の差と暗号文同士の差に相関があるかどうかを調べる．もし，相関がある場合，そのことを利用して，鍵を効率的に求めるものである．一方，線形解読は，大量の平文／暗号文組を集め，平文ビットの排他的論理和と暗号文ビットの排他的論理和に相関があるかどうかを調べる．もし，相関がある場合，そのことを利用して，鍵を効率的に求める．その他，高階差分解読など，種々の方法が発表されている．ある暗号に対し，何らかのショートカット攻撃が適用可能であると分かったとき，その暗号は学術的に破られたとみなされる．たとえば，DESの鍵長56ビットについては，その内部構造に着目した解析を行うことで，鍵長49ビット，あるいは43ビット相当の安全性でしかないような欠点が指摘された．ショートカット攻撃については，まだまだ尽きたとは言い難く，今後も，この面からの研究は引き続き重要となろう．

日本では，総務省・経済産業省による電子政府推奨暗号の選定が開始され，国内ベンダをはじめとして，多数の方式応募があった．これらはそれぞれ，個々の特徴を持った暗号方式である．以下の章では，CRYPTREC電子政府推奨暗号リスト[1]に掲載されたいくつかを紹介する．

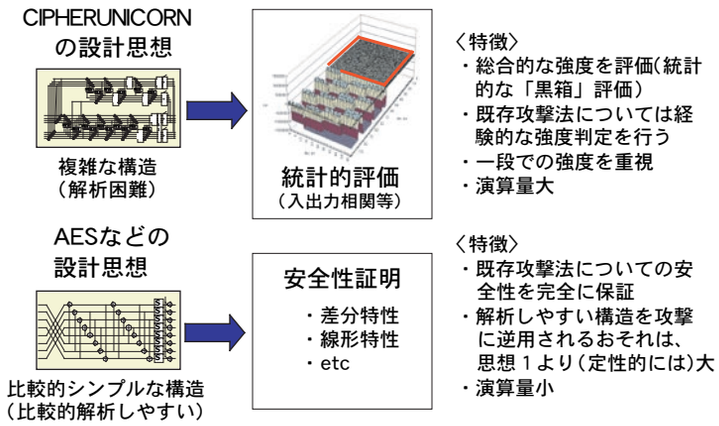


図 -2　設計思想による暗号強度評価方法の違い

CIPHERUNICORN

CIPHERUNICORN（以下 UNICORN と略）は，NEC が提案する「UNICORN 暗号の設計思想」と「用途別暗号設計のコンセプト」に基づいて開発した共通鍵暗号の商標であり，複数の独自暗号アルゴリズムの総称となっている．

UNICORN 暗号の設計思想では，顧客要求と使用環境の許容範囲内で可能な限り安全性を高めることを狙っており，暗号の基本処理であるラウンド関数を複雑にし，暗号解析を困難にすることにより実質的な強度を上げる方針を採用している（**図 -2** 参照）．複雑な構造を持つラウンド関数は，構造に依存した安全性の評価が困難であり，ラウンド関数を「黒箱」とみた総合的な強度評価が必要である．NEC では，入出力のビットごとの相関を詳細に調べるために「統計的評価手法に基づく暗号強度評価装置」を開発し安全性評価に使用している．この暗号強度評価装置は，部品やラウンド関数，暗号全体といった処理の大きさにかかわらず評価が行えるので黒箱評価に適している．UNICORN 暗号の設計思想は，ある種の安全性証明を行いやすい構造を採用し，既知の攻撃法に対する強度を保証しながら可能な限り速度を高めるという設計思想とは対極をなしている．

また近年では，ユビキタス社会やディジタル家電の環境まで暗号需要が広がり，幅広い用途すべての要求を一度に満足する暗号設計は困難である．NEC では，ユーザの環境ごとに最適な設計を行い，安全性と処理性能が最高のパフォーマンスになる暗号を多数開発している．たとえば，日本の電子政府推奨暗号には 128 ビットと 64 ビットのブロック暗号 UNICORN-A と UNICORN-E が選定され，ディジタルスチルカメラや携帯電話などの模造バッテリー検知にはマイクロコントローラ専用の UNICORN-S が開発されている．顧客の要望により名前や存在そのものが秘匿される UNICORN 暗号も多数存在する．これら多種多様な需要に対応するためには効率的な暗号設計技術が不可欠である．NEC では，複数の暗号の特徴や安全性の統一的な評価に暗号強度評価装置を使い，評価結果をシステム的にフィードバックすることで設計の効率化を図っている．

Hierocrypt（ヒエロクリプト）

Hierocrypt は東芝が開発したブロック暗号の総称で，ブロックサイズが 128 ビットの Hierocrypt-3（以下，HC-3）と 64 ビットの Hierocrypt-L1（以下，HC-L1）の 2 種類がある．安全性と実装性能の高さが評価され，2003 年に電子政府推奨暗号に選定された．

Hierocrypt の一番の特徴は，独自開発の入れ子型 SPN 構造を採用したデータ攪拌部である．**図 -3 (a)** と **図 -3 (b)** に通常の SPN 構造と入れ子型 SPN 構造を示す．図 -3 (a) の SPN 構造は並列 S-box からなる層 (S) と線形拡散層 (P) の繰り返しで構成される（S-box 直前の鍵加算は省略）．一方，入れ子型 SPN 構造では上位の SPN 構造の S-box を下位構造の 2 段 SPN 構造で構成する．この再帰的構成の結果，SPN 構造の解析結果が再帰的に適用でき，安全性の評価が容易になる．Hierocrypt という名称は，構造の再帰性を象徴する hierarchy（階層）と，暗号を意味する crypt を組み合わせた造語である．

ブロック暗号の最も重要な安全性評価項目に差分解読法と線形解読法に対する強度がある．最大平均確率はその重要な安全性指標の 1 つで，4 層の HC-3 で 2-96 以下，4 層の HC-L1 で 2-48 以下が数学的に証明できる．この証明可能安全性という性質を持つブロック暗号は，電

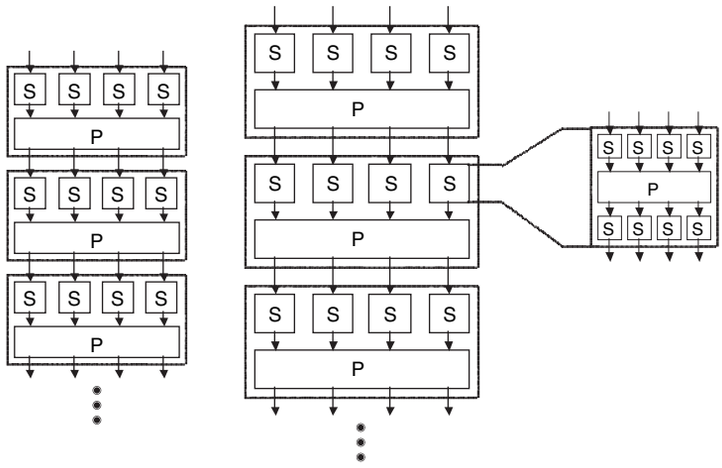


図 -3　SPN 構造と入れ子型 SPN 構造

子政府推奨暗号ではほかにMISTY1とAESだけである．入れ子型SPN構造の証明可能安全性は，設計後に開発者が発見したが，研究の過程で，米国標準暗号のAESが数学的に等価な入れ子型SPN構造に変形でき，AESに対してもHC-3と同等の証明可能安全性があることも発見した[2]．Hierocryptファミリーに対して最も効率の良い攻撃法はSQUARE攻撃に代表される積分攻撃であり，他の攻撃法の適用も研究されているが，現在，現実的な脅威にはなっていない．

Hierocryptはソフトウェアとハードウェアの両方で，高速かつコンパクトな実装が可能である．実装環境に応じて2種類のスペックを使い分けることによってその有効性はさらに高まる．

MISTY1

MISTY1は1996年に三菱電機から発表された共通鍵ブロック暗号で，ブロックサイズは64ビット，鍵サイズは128ビットである[3]．仕様上段数は可変であるが，実際には8段で利用されている．MISTY1の特長は差分解読法や線形解読法に対する証明可能安全性（provable security）を実現したこと，またソフトウェアでの高速化だけでなく，ハードウェアでも小型化，低消費電力化が可能なように設計されている点である．これを実現するためにMISTY1では**図-4**に示すような再帰構造を採用している．この再帰構造によって暗号の安全性の数学的評価が容易になり，しかも小さな関数の繰り返しによって全体が構成できるため，小型化が可能となった．またこの再帰構造は並列度が高いため，処理速度の向上をはかることもできる．

MISTY1は日本の電子政府暗号評価プロジェクトCRYPTRECにおいて電子政府推奨暗号に選定されているほか，欧州の暗号評価プロジェクトNESSIEにおいて，64ビットブロック暗号の中で唯一推奨暗号として採択されている．また国際標準暗号規格ISO/IEC 18033にも提案されている．MISTY1は現在政府・自治体などの情報セキュリティシステムを中心に幅広く用いられているほか，そのバリエーションも国内外で利用されている．たとえばMISTY1を携帯電話向けにさらに低消費電力化したKASUMIは，第三世代携帯電話（W-CDMA）の必須の世界標準暗号としてトランスポート層の秘匿ならびに完全性に用いられている．これは国産暗号技術が必須の国際標準に採用された初めての例である．また2003年にはKASUMIは欧州現世代の携帯電話規格GSMにも採用されている．

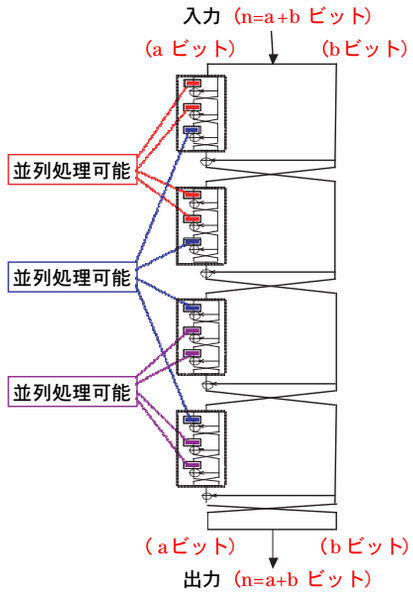


図 -4　MISTY1 の再帰構造（recursive structure）

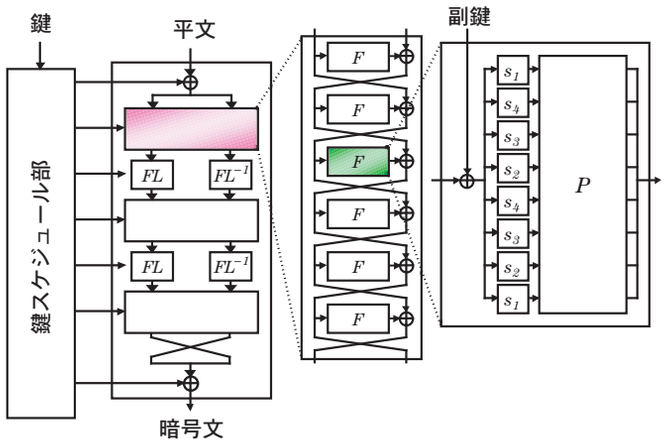


図 -5　Camellia の構造（鍵長 128 ビットの場合）

Camellia

Camellia は，2000 年に NTT と三菱電機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[4]．鍵長は AES と同様，128，192，256 ビットの 3 通りがサポートされている．Camellia はローエンド IC カード等に搭載されている 8 ビット CPU から，高性能 PC・サーバ等に搭載されている 64 ビット CPU に渡る幅広いプラットフォーム上で高速なソフトウェア実装が可能となるよう設計されている．また，ハードウェア実装においては小型・低消費電力の実装が可能となるように設計され，AES と並んで，ゲート数世界最小クラスを達成しているほか，ゲート数当りの暗号化／復号処理速度でも優れた性能となっている．

Camellia 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（**図 -5** 参照）．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，補間攻撃，関連鍵攻撃，丸め差分攻撃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 は電子政府推奨暗号の 1 つとして選定されているほか，EU による暗号評価プロジェクト NESSIE において，応募された 128 ビットブロック暗号の中から唯一，NESSIE 推奨暗号として選ばれた．また，IETF における Camellia に関する RFC（RFC3657，RFC3713）の発行，TV Anytime Forum での標準化，国際標準暗号規格 ISO/IEC 18033 への提案等，さまざまな標準化が進んでいる．

SC2000

SC2000 は富士通研究所と東京理科大学が共同で開発した 128 ビット共通鍵ブロック暗号であり，日本の電子政府推奨暗号の 1 つとして選定されている．SC2000 のキーワードは「高い安全性」，「高速な処理性能」，「フレキシブルな実装性」である[5]．

●高い安全性

暗号の心臓部は，非線形処理と呼ばれる処理部分にある．従来の暗号では，一種類の非線形処理のみを繰り返す方式が大半であるのに対し，SC2000 では，安全性に定評のある Feistel 構造と SPN 構造の 2 種類の非線形処理を効率よく組み合わせる方式（**図 -6** 参照）を採用しており，これにより非常に高い安全性を持つ優れたアルゴリズムとなっている．

●高速な処理性能

ソフトウェア実装による処理速度は，PC，ワークステーション双方において，次世代米国標準 AES をも凌ぐ能力を持っており，またハードウェアにおいても世界最高レベルの暗号化処理が可能である．

●フレキシブルな実装性

特定の CPU のみが持つ命令を使用しない設計によって，IC カード等に搭載されている低機能な CPU からハイエンドサーバ等に搭載されている高性能 CPU まで，あらゆるプラットフォームに実装することが可能であり，省サイズな実装から高速処理用の実装まで，さまざまな要件に対応可能な柔軟性を持っている．

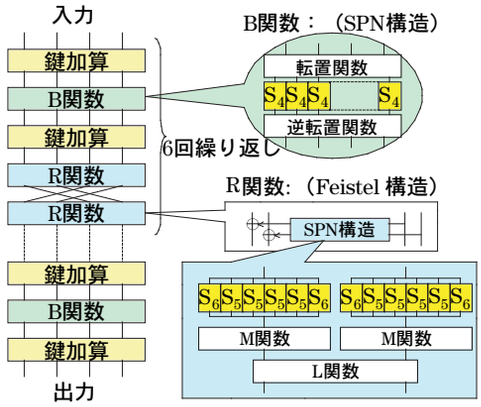


図 -6　SC2000 による暗号化処理（鍵長 128 ビットの場合）

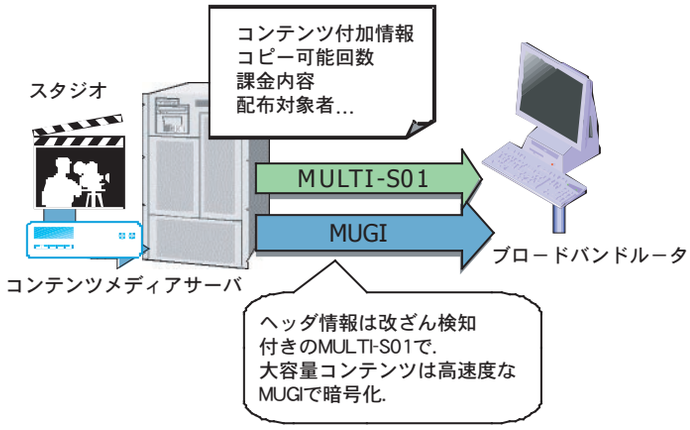


図 -7　MULTI-S01，MUGI によるコンテンツ暗号配信

MULTI-S01，MUGI

擬似乱数生成器（Pseudorandom number generator, PRNG）を使って暗号処理を行うものをストリーム暗号と呼ぶ．個々のストリーム暗号の特徴は，(1) どういうPRNGを使っているのか，(2) どのモードで暗号化しているか，によってさまざまな処理が可能である．ここでは日立製作所が開発した2例を紹介する．

MUGIは，日立製作所が2001年に提案したPRNGである．鍵長，ならびに初期値の長さは128ビットである．アルゴリズムの特徴としては，内部の部分関数に，AESのSボックスやMDS変換を用いることにより，AESに対する豊富な安全性評価が直接流用できる．また，同じ理由からAESと同様，ASIC, FPGAといったハードウェア実装から，8/16/32/64ビットプロセッサにおけるソフトウェアによる実装まで，どのような実装形態でも効率よく実装が可能となっている．

MULTI-S01は，日立製作所が2000年に提案したストリーム暗号であるが，典型的なbinary-additive modeによる暗号処理ではなく，独自のMULTI-S01モードで，暗号化処理を行う．これにより，メッセージは単に暗号化されるだけでなく，改ざんのチェックも行われるようになる．つまり，データを復号するときに，同時にフラグも得られ，このフラグを見ることで通信路における改ざんの有無の判定を行うことができるようになる．原理上，MULTI-S01はどのようなPRNGと組み合わせても使うことができるが，電子政府推奨暗号リストでは，PanamaというPRNGとの組合せの方式が評価・推奨されている．

たとえばコンテンツ配信での利用を考える（**図-7**参照）．課金情報や著作権情報を含むヘッダ部分には，改ざんが行われるべきでないためMULTI-S01を使う．しかし，コンテンツ部分にはMUGIを使って，高速な処理による暗号化を行う．

MULTI-S01とMUGIは電子政府推奨暗号の1つとして選定されているほか，国際標準暗号規格ISO/IEC 18033にも提案されている．

参考文献
1) 暗号技術評価報告書（2002年度版）CRYPTREC Report 2002，情報処理振興事業協会，通信・放送機構（Mar. 2003）．
2) Sano, F., Ohkuma, K., Shimizu, H. and Kawamura, S. : On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis, IEICE Trans., E86-A, No.1, pp.37-46(2003).
3) Matsui, M.: New Block Encryption Algorithm MISTY, 4th International Workshop of Fast Software Encryption, Lecture Notes in Computer Science 1267, Springer Verlag(1997).
4) Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakjima, J. and Tokita, T. : Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms, Proceedings of the 7th Annual Workshop on Selected Areas in Cryptography, SAC2000, LNCS 2012, pp.39-56, Springer-Verlag (2001).
5) Shimoyama, T., Yanami, H., Yokoyama, K., Takenaka, M., Itoh, K., Yajima, J., Torii, N. and Tanaka, H. : The Block Cipher SC2000, Proceedings of the 8th International Workshop on Fast Software Encryption, FSE2001, Lecture Notes in Computer Science 2355, pp.312-327, Springer-Verlag(2001).

（平成16年9月30日受付）