次世代共通鍵暗号 Hierocrypt™

Hierocrypt™ Next-Generation Symmetric Cipher

大熊　建司　OHKUMA Kenji
佐野　文彦　SANO Fumihiko
村谷　博文　MURATANI Hirofumi

共通鍵（かぎ）暗号は，データの秘匿を高速に実行する，IT（情報技術）社会における必須要素である。近年，計算機技術の発展に伴い，米国連邦標準の64ビット方式DES（Data Encryption Standard）の安全性が不十分となった。それと同時に，次世代向け128ビット方式の必要性が認識され，標準化が活発になっている。当社は，このようなニーズにこたえるため，最近の暗号解析及び設計技術を駆使して，安全性，実装性能に優れた独自の共通鍵暗号Hierocrypt™を開発した。

Hierocrypt™は，構成が簡潔で透明性が高い独自の入れ子型SPN（Substitution Permutation Network）構造を特徴としており，64ビット方式と128ビット方式の2種類のアルゴリズムを用意してある。入れ子型SPN構造は，共通鍵暗号に対するもっとも強力な汎用攻撃法である差分解読法と線形解読法に対する安全性を容易に評価，保証できる。Hierocrypt™は，ほとんどのソフトウェア及びハードウェア実装において高速処理が可能であり，また，実装もコンパクトである。当社は，この暗号方式Hierocrypt™を各種標準化に提案するとともに，SPAgent™などのミドルウェアやスマートカードなどへの普及を目指している。

The symmetric block cipher, which encrypts plain data into an unreadable ciphertext at high speed, is a key component of the information technology society. The Data Encryption Standard (DES), the U.S. federal standard cipher, has been the de facto standard so far. However, the security of DES is no longer adequate because of the rapid improvement of CPU power. The need for 128-bit block ciphers for the next generation has become widely accepted, and the trend of standardization is now active.

To meet this requirement, we have designed a new symmetric block cipher family called Hierocrypt™, which is characterized by the nested substitution permutation network (SPN) structure. The nested SPN structure is very simple, and guarantees high security against differential attacks and linear attacks, which are efficient cryptanalytical methods. Furthermore, the Hierocrypt™ cipher is compact yet it very rapidly encrypts almost all implementations on both software and hardware.

We have proposed the Hierocrypt™ cipher in some standardization projects, and plan to make it widely available for use in many fields such as middleware and smart cards.

1 まえがき

IT社会の情報セキュリティ技術において，データ内容の秘匿には，高速に暗号化を行う共通鍵ブロック暗号技術が中心的役割を果たしている。従来，米国連邦標準だった64ビット方式のDESが事実上の標準として広く利用されていた。しかし，計算機の高性能化や専用解読機の開発などによって，1組の平文・暗号文組が入手できれば，1日足らずで解読できるまで安全性が低下し，次世代向け128ビット方式の必要性は明らかになった。米国NIST（National Institute of Standards & Technology：連邦標準・技術局）は，128ビット方式の標準化のため世界に方式提案を公募し，2000年にベルギーから提案されたRijndaelを次世代標準AES（Advanced Encryption Standard）に内定した[1]。

これに刺激され，2000年に暗号アルゴリズム全般にわたる以下のプロジェクトが開始された。国際標準化組織であるISO（国際標準化機構）とIEC（国際電気標準会議）の合同技術委員会JTC1は，暗号アルゴリズム標準化のプロジェクトを開始し，2003年の標準化を目指している。国内では，IPA（情報処理振興事業協会）が2003年開始予定の電子政府（注1）向けに，暗号技術評価委員会CRYPTREC（CRYPTography Research & Evaluation Committee）を組織し，欧州も暗号技術の評価プロジェクトNESSIE（New European Schemes for Signatures, Integrity, and Encryption）を開始した[2],[3]。

当社は，このような情況を踏まえ，最近の暗号解析及び設計技術を利用して，安全性，実装性能に優れた128ビット共通鍵暗号Hierocrypt™を開発した[4]。この方式は構造が単純で，共通鍵暗号に対するもっとも強力な汎用攻撃法である差分解読法と線形解読法に対する安全性が容易に評価でき，高い安全性が保証できる。また，主要なプラットフォーム上でのソフトウェア及びハードウェア実装において，高速処理が可能であり，また，実装もコンパクトである[5]。

当社は，この暗号方式Hierocrypt™を各種標準化に提案

（注1）　行政を効率化し国民負担の軽減を図るため，申請届出手続きや政府調達など，行政手続きの電子化を実現するシステム。

するとともに，SPAgent$_{TM}$などのミドルウェアやスマートカードなどへの普及を目指している[6]。以下に，そのアルゴリズムの概要と実装性能について述べる。

2 設計指針

暗号を技術的に評価する際の基準は大きく分けて安全性，処理速度，実装サイズの3種類であり，3者にどのような重み付けをすべきかは用途に大きく依存する。今回の設計においては特定用途に絞らず，ローエンドのICカードをはじめ，主要なすべてのプラットフォーム上で優れた実装性能を実現するという方針を立てた。

暗号の基本構造には，**図1**に示すようにFeistel型とSPN型の2種類がある。Feistel型は，暗号化と復号の処理がほぼ同じであり，実装をコンパクトにしやすいという長所がある。しかし，主要な攻撃法に対する安全性の評価はSPN型のほうが容易である。

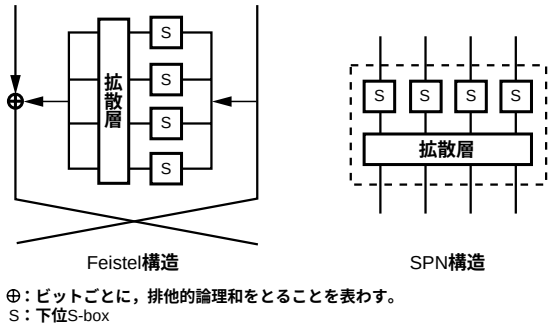

図1．Feistel構造とSPN構造の違い　Feistel構造はブロックを二等分して交互に攪拌し，SPN構造は一様になっている。
Difference between Feistel and SPN structures

今回の開発においては設計期間が限られていたので，安全性が評価しやすいSPN型を基本構造に選び，設計の透明性のためできるだけ単純な構造にした。設計の透明性は，設計者による秘密の弱点の埋込みを困難にすると考えられており，最近の暗号設計では必須の条件になっている。また，ローエンドのICカードでの性能も重視し，8ビット単位の処理だけでも効率的に実行できるという条件を加えた。

また，今後10年程度は64ビット方式の需要が見込まれることから，128ビット方式（Hierocrypt$_{TM}$-3）のほかに64ビット方式(Hierocrypt$_{TM}$-L1)も加え，両方式を同じ構造で構成要素もできるだけ共通化して，並行して設計することにした。

3 アルゴリズムの概要

共通鍵ブロック暗号は，入力する元のデータ（平文）をランダムパターン（暗号文）に変換する“データ攪拌（かくはん）部”と，暗号化鍵からデータ攪拌部に供給するラウンド鍵を生成する“鍵スケジュール部”の2部で構成される。データ攪拌部は，通常，ラウンド関数と呼ばれる処理の繰返しで成っており，繰返し段構造の前後に，初期及び最終処理を行う場合もある。

SPN型の基本は，ブロック長のデータを一定長のサブブロック単位に分け，その各々に代入処理S-box(エスボックス）を並列に行うS-box層と，ブロック幅で線形の混ぜ合わせを行う拡散層の繰返しである。Hierocrypt$_{TM}$-3の入れ子型SPN構造は，上位構造と下位構造の2段階の階層を持っている（**図2**）。上位構造は4個並列の32ビットS-boxから成る層と128ビット幅の拡散層の繰返しであり，最初と最後はS-box層で，このS-box層の層数を段数とする。32ビットS-boxは，4個並列の8ビットS-boxから成る，2層で32ビット幅の拡散層を挟んだ2段構造である。

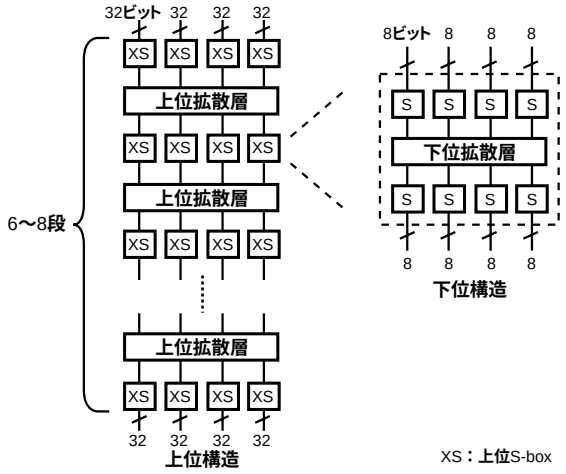

図2．Hierocrypt$_{TM}$-3の入れ子型SPN構造　上位及び下位の2階層が共にSPN構造になっている。
Hierarchical SPN structure of Hierocrypt$_{TM}$-3

入れ子型SPN構造の利点は，上位構造と下位構造を独立に設計できる点である。Hierocrypt$_{TM}$-L1ではHierocrypt$_{TM}$-3の下位構造をそのまま利用し，上位構造の幅を半分にしてある。このため，Hierocrypt$_{TM}$-L1用に新たに設計したのは，上位拡散層だけで済んだ。また，上位構造と下位構造の両方で攪拌性が高ければ，全体としてもむらなく高い攪拌性が保証されるなど，独立に設計しても高い安全性が容易に実現しやすい特長がある。

128ビット暗号Hierocrypt$_{TM}$-3は，3種類の鍵サイズ（128ビット，192ビット，256ビット）が利用でき，上位構造の段数は各々，6段，7段，8段である。この段数を2倍したものが通常のSPN構造暗号の段数，つまり，通常の暗号の12段，

14段，16段に相当する。AESに内定しているRijndaelと比較して，各々2段多い。Rijndaelは，長期の使用を考えると強度上段数が少ないとする見方もあり，Hierocrypt$_{TM}$-3の段数設定は適切と考える。また，64ビット暗号Hierocrypt$_{TM}$-L1の鍵サイズは128ビット，段数は6段である。

入力の変化の影響が局所化せず，広く影響を及ぼすような設計が望ましいと考えられる。Hierocrypt$_{TM}$の拡散層は，上位／下位ともに符号理論を利用して，その条件が満たされるように作られている。

8ビットの非線形入出力変換であるS-boxの構成を**図3**に示す。有限体上のべき乗演算で，後述の差分及び線形解読に対してもっとも高い安全性が実現できる。しかし，そのままでは，代数的に単純なため代数的攻撃法が有効になる。そこで，ビット並べ替えを入力側に挿入し，代数的構造を壊すことでその適用を困難にしている。また，出力側に定数の排他的論理和を入れたのは，入力と出力のハミング重み間の相関を低くするためである。

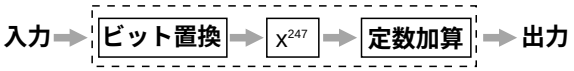

図3．S-boxの構造　ビットの並べ替え，有限体上のべき乗演算，定数の排他的論理和の3段で構成されている。
Structure of S-box

4 安全性

4.1 安全性の評価基準

ブロック暗号の安全性は，特定の攻撃法によって解読するのに必要な平文と暗号文の組数や計算量によって評価する方法と，入出力相関などの統計量によって評価する方法に分かれ，最近では前者の評価が重視される。

1組の平文と暗号文の組がわかっているとき，可能な暗号化鍵を全部試すことによって鍵の候補が1個，又はごく少数個に絞られる。1個に絞りきれないときは，平文／暗号文組を追加することで暗号化鍵が特定できる。このような解読法を“鍵の全数探索法”と呼び，鍵長をLビットとすると，2^L回の暗号化計算で解読できることを意味する。鍵の全数探索法は，あらゆる暗号アルゴリズムに対して有効であり，鍵長は安全性の重要な指標の一つである。また，最近では，鍵の全数探索に要する計算量を下回る計算量の解読法が存在しないことが，安全性に関する暗黙の条件となっている。

4.2 差分・線形解読法

差分解読法は1989年にイスラエルのBihamとShamirによって，線形解読法は93年に三菱電機（株）の松井氏によって提案された汎用の解読法である。これらの解読法は，入出力間の統計的偏りを利用する攻撃法であり，中間段での統計的偏りを利用して両端の段での鍵推定を行う。中間段での統計的偏りの鍵平均の最大値を，最大平均差分確率及び最大平均線形確率と呼び，その逆数程度の平文と暗号文の組が解読に必要であることが知られている。一般に平均確率の評価は困難であり，最大差分特性確率及び最大線形特性確率を尺度とすることが多い。

Hierocrypt$_{TM}$-3では，2段でこれらの値が共に2^{-150}以下となることが保証できる。解読には，平文と暗号文の組が最大差分及び線形確率の逆数個程度必要であることがわかっており，規定の段数では十分安全であると考えられる。より厳密な最大平均差分確率及び最大平均線形確率による評価も可能で，4段で2^{-96}以下であることが保証できる。

4.3 SQUARE攻撃法

差分解読法及び線形解読法以外にも，高階差分解読法，補間攻撃法，不可差分攻撃法，丸め差分攻撃法など多様な攻撃法があるが，SPN型に特に有効な攻撃法にSQUARE攻撃があり，Rijndaelに対しては128ビット鍵のときS-box層数で7層まで，鍵長が192ビット及び256ビットのとき8層まで攻撃可能である。

Hierocrypt$_{TM}$-3では，上位拡散層の結合を密にし拡散性を高くしてあるので，**図4**に示すようにSQUARE攻撃に対してRijndaelより安全性が高い。適用可能な段数は128ビット鍵で6層，192ビット及び256ビットの鍵長では7層までである。この強度の違いは，Rijndaelのように拡散層が1種類であるのに対し，Hierocrypt$_{TM}$-3では，上位及び下位の2種類の拡散層が効果的に組み合わされているためである。

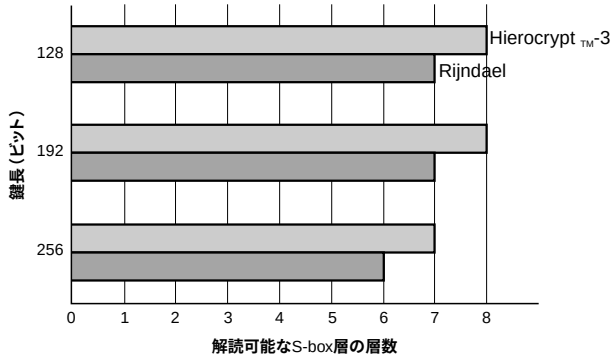

図4．Hierocrypt$_{TM}$-3のSQUARE攻撃に対する安全性　SQUARE攻撃で攻撃可能な段数を，次期AESのRijndaelとの比較で示す。
Strength of Hierocrypt$_{TM}$-3 against SQUARE attack

5 実装性能

5.1 ソフトウェアでの実装性能

暗号アルゴリズムをパソコン（PC）や携帯端末などではソ

フトウェア実装で利用されることが多く，ソフトウェアでの実装性能は重要である。Pentium®(注2) Ⅲ とZ80™で実装した際の性能を図5，図6に示す。

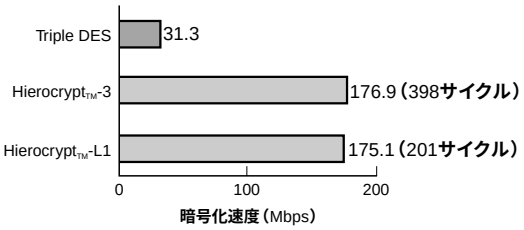

図5．Pentium®Ⅲ（550 MHz）での暗号化速度　Pentium®Ⅲでの Assembly 言語による実装速度を，Triple DESとの比較で示す。
Encryption speed on Pentium®-III 550 MHz processor

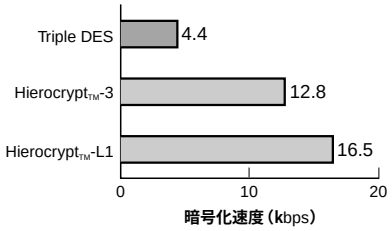

図6．Z80™（5 MHz）での暗号化速度　Z80™での Assembly 言語による実装速度を，Triple DESとの比較で示す。
Encryption speed on Z80™ 5 MHz processor

Hierocrypt-3では，安全性を高めるため，バイト単位の排他的論理和を上位拡散層に利用している。その部分は符号理論に基づいて高い安全性を達成するよう設計されているが，自然な実装法では速度は出ない。ただし，文献に示すノウハウを利用することによって図5に示す性能が得られる。この値は，AESの最終5候補と同等の性能である。

また，8ビットCPUのZ80™による実装結果は，ICカードでも十分実用に耐える性能が出ることを示している。

5.2　ハードウェアでの実装性能

サーバ環境では超高速の処理が，また，ICカードでは極めて小型の実装が必要となり，ハードウェア実装が必要となる。0.14 μm 3層CMOS（相補型金属酸化膜半導体）スタンダードセルでの実装結果を表1に示す。動作条件としてもっとも厳しいコマーシャル ワーストケースでの評価であり，高速性を優先した場合とサイズのコンパクト性を優先した場合の2種類の実装結果を示した。この実装設計は短期間で実施したものであり，更に改良することによって速度及び実装サイズに改善の余地がある。

（注2）　Pentiumは，米国Intel Corporationの登録商標。

表1．ハードウェアでの暗号化速度
Encryption speed on CMOS standard cell implementation

暗号方式と実装オプション	クロック周波数 (MHZ)	暗号化速度 (Mbps)	ゲート数 (× 1,000)
Hierocrypt-L1 （速度優先）	128.2 （クロック数：14）	586	38.2
Hierocrypt-3（256ビット） （速度優先）	126.1 （クロック数：18）	897	81.5
Hierocrypt-3（256ビット） （面積優先）	185.1 （クロック数：280）	84.6	26.7

設計環境：SYNOPSYS社製デザインコンパイラ 1999.10-3
シミュレーション条件：1.35 V 70 ℃

6　あとがき

共通鍵ブロック暗号の設計を行い，次世代向け128ビット版Hierocrypt-3とレガシー用途向け64ビット版Hierocrypt-L1を同時に短期間で完成した。高い安全性と実装性能が両立できたのは，次期AESに内定しているRijndaelと同様のSPN構造を一般化及び改良した入れ子型SPNを採用したことが大きい。両方式ともに，CRYPTREC，NESSIE，ISO/IEC JTC1（ISO/IEC合同技術委員会No.1：国際暗号アルゴリズム標準化プロジェクト）の三つに提案しており，CRYPTRECではトップクラスの評価を得ている。今後，標準化活動の推進に加え，SPAgentなどミドルウェアへの組込みやPCへのバンドルなどへ，広く普及されることを目指している。

文　献

(1) http://csrc.nist.gov/encryption/aes
(2) http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
(3) http://www.cryptonessie.org
(4) http://www.toshiba.co.jp/rdc/security/hierocrypt
(5) 佐野文彦，ほか.“次世代暗号HierocryptのC言語による実装”. 情報処理学会研究報告2000-CSEC-11. 盛岡，2000-09，情報処理学会CSEC研究会．2000，p.49－54.
(6) EC/ASPセキュリティ基盤技術SPAgent．東芝レビュー．**56**，3，2001，p.23.

大熊　建司　OHKUMA Kenji，D.Sc.
研究開発センター コンピュータ・ネットワークラボラトリー研究主務，理博。暗号技術・応用システムの研究・開発に従事。電子情報通信学会，情報処理学会会員。
Computer & Network Systems Lab.

佐野　文彦　SANO Fumihiko
e-ソリューション社 SI技術開発センター SI技術担当。暗号技術と暗号応用システムの研究・開発に従事。電子情報通信学会，情報処理学会会員。
Systems Integration Technology Center

村谷　博文　MURATANI Hirofumi，D.Sc.
研究開発センター コンピュータ・ネットワークラボラトリー研究主務，理博。暗号技術と暗号応用システムの研究・開発に従事。電子情報通信学会，情報処理学会会員。
Computer & Network Systems Lab.