Vol.37 No.6　　情 報 処 理　　June 1996

解　説

暗号安全性の最近の動向

1. 暗号安全性の最近の動向†
—総　論—

藤　岡　　淳††

1. はじめに

「暗号」と聞いて，まず，何を連想されるでしょうか？　第2次世界大戦での諜報戦や冷戦時代のスパイ活動，はたまた，シャーロック・ホームズなどの推理小説でしょうか?

実は，この「暗号」に代表されるセキュリティ技術は，現代の我々にとって非常に身近なものなのです．

テレフォンカードの偽造，日米貿易交渉における橋本通産大臣(当時)の電話盗聴，有名なクラッカー(Mitnick)によるインターネットでのクレジットカード番号の不正入手などに代表されるように，情報化社会の到来にともない，我々の生活は様々な危険にさらされています．インターネットの商用利用が検討されている現在，セキュリティ問題はより痛切に意識されていくことでしょう．

これら重要なセキュリティ問題を解決する鍵が，「暗号」技術なのです．1つの暗号アルゴリズムから，通信内容の暗号化や通信内容の認証などのようなプロトコルが構成でき，多種多様なことが実現可能となります．

このように重要な暗号アルゴリズムですが，実際に利用する際に着目すべき点は何なのでしょうか？　当然，利便性や速度といった性能面も重要ですが，その方式の信頼性に多くの注意が払われることでしょう．信頼性，すなわち，暗号強度です．

本特集は，暗号安全性の現状について，その理論的側面を中心に第一線の研究者の方々に解説をお願いしたものです．従来の解説とは逆に，暗号アルゴリズムがどう使われるかといった応用的な解説からスタートします．その後，徐々に理論的な内容に入っていくという構成をとり，最終的には，以下のような疑問に答えたいと考えています．

- インターネットって安全なの?
- Clipper Chip って何?
- 暗号アルゴリズムの評価基準の現状は?
- 線形攻撃法ってどういうもの?
- 差分攻撃法ってどういうもの?

2. 暗号方式

本章では，各解説を理解するに必要な暗号方式の基礎事項について解説します．

2.1 共通鍵暗号方式

暗号には，大きく分けて**公開鍵暗号方式**と**共通鍵暗号方式**の2種類の方式が存在し，本特集では，特に共通鍵暗号方式に関する議論を行います☆．

共通鍵暗号方式は，二者間で同一の**暗号化鍵**を共有し，それを用いることで第三者の不正行為を防止するというもので，これにより，通信内容の**暗号化**，通信内容の**認証**などが可能になります．**DES**(Data Encryption Standard)や**FEAL**(Fast Data Encipherment Algorithm)はこの方式の代表例です．

すなわち，ある平文を送りたい人(**送信者**)は，**受信者**と共有する暗号化鍵で暗号化を行い，暗号文を**通信路**に流します．このとき，暗号文は，暗号化鍵を共有している受信者のみに復号化が可能となり，秘匿性が保証されることになります(**図-1**)．

また，平文の内容保証をしたい人は，受信者と共有する暗号化鍵で暗号化を行い，得られた**認証子**と平文の両方を通信路に流します．受信者は，受信した平文を共有している暗号化鍵で暗号化を行い，その結果が認証子と一致するかどうかを照

† Recent Topics on Information Security — General Remarks — by Atsushi FUJIOKA (NTT Information and Communication Systems Laboratories).

†† NTT 情報通信研究所

☆公開鍵暗号方式は共通鍵暗号方式に比して低速なため，共通鍵暗号方式と組み合わせて用いられることが多い．

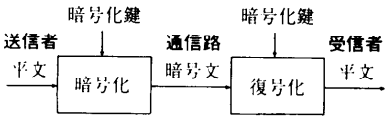

図-1 共通鍵暗号方式を用いた通信内容の暗号化

合して，データの改ざんを防止することができます(図-2)．

2.2 Feistel 型暗号方式

この共通鍵暗号方式として，様々なアルゴリズムが提案されていますが，その多くは，ある基本構造を繰り返して構成されています．特に，DES や FEAL などは Feistel 型と呼ばれる暗号方式であり，排他的論理和の性質により，鍵順序を入れ換えると暗号化と復号化が同じアルゴリズムとなります．図-3 は FEAL-8 の例ですが，P が平文，C が暗号文，K_i が暗号化鍵になります．ここで C を入力とした場合に，入力する鍵を，K_0 と K_7 を K_1 と K_6 を，のように各段ごとに入れ換えて，さらに(K_8, K_9, K_A, K_B)と(K_C, K_D, K_E, K_F)も入れ換えると，出力が P になることが分かります(ここで，分岐は，64 bit のデータを 32 bit ずつに分けることを意味し，また，⊕ は，ビットごとの排他的論理和です)．実際には，DES や FEAL の鍵長は 64 bit ですが，それを鍵拡張アルゴリズムを用いてビット数を増やし，その結果をそれぞれの F 関数で用います．

2.3 暗号攻撃法の分類

情報セキュリティの分野では，暗号化鍵を共有する正当な受信者が平文を求めることを「復号」と，不正者が暗号文などから平文や暗号化鍵を導出しようとすることを「解読」といい，また，不正者がこのような解読を試みることを「攻撃」と呼びます．

共通鍵暗号方式にとっての信頼性は，なんらかの攻撃法により暗号化鍵が導出できるかどうかとなります．単純には，**総当たり攻撃**で鍵を調べれば可能ですが，鍵のビット長が 64bit 以上では現実的には不可能とされています．よって，総当たり攻撃以外の攻撃法で，鍵の総当たりよりも少ない手数で鍵を求められるかどうかが重要となります．

暗号化鍵を算出する攻撃法として，以下の状況設定がよく用いられます．

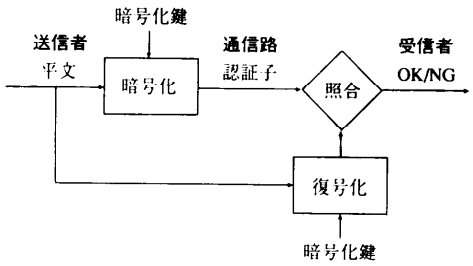

図-2 共通鍵暗号方式を用いた通信内容の認証

選択暗号文攻撃 攻撃者が任意に選んだ暗号文に対して平文を入手可能

選択平文攻撃 攻撃者が任意に選んだ平文に対して暗号文を入手可能

既知平文攻撃 攻撃者は平文と暗号文の対を入手可能

暗号文攻撃 攻撃者は暗号文のみを入手可能

既知平文攻撃の状況は，実際に暗号を用いる場合にもしばしば起こり得るので，既知平文攻撃に対する安全性が保証されていることは必須でしょう．また，選択暗号文攻撃や選択平文攻撃は暗号設計者にとって都合の悪い場合であり，攻撃者にとって都合のいい場合です．そのため，これらの攻撃を避けるには，意味のない平文や暗号文に不用意に暗号化や復号化を施さないことが必要となります．

3. インターネット・セキュリティ

本章以降では，本特集の各解説記事の概要を説明していきます．

まず，解説「インターネット・セキュリティ」では，インターネットの安全性について述べられています．

インターネットはコンピュータ通信の研究に端を発し，研究者のコミュニケーション手段として，互いの組織を接続し，パケットを転送し合うことで発展してきました．このため，「使いやすさ」を最優先に実装が進み，「使いやすさ」を阻害するようなセキュリティ機能の充実は，管理者の性善説に立脚することや利用者である研究者のモラルに任されていて顧みられていませんでした．しかし，現在，インターネットはビジネスに代表されるような一般社会にまで浸透するようになり，そのセキュリティ対策が求められています．

まず，この解説では，インターネットにおける

脅威を以下のように分類し，
・通信プロトコルから見た脅威
・システム運用面から見た脅威
それぞれの代表的な脅威を紹介します．

次に，組織内部のネットワークとインターネット間のアクセスをコントロールする，重要なセキュリティ技術である**ファイアウォール**について解説されています．また，遠隔システム間の相手認証に威力を発揮する**使い捨てパスワード**について述べられます．この方式では，パスワードの有効回数は1回限りなので，通信路の盗聴が行われていても，その後の成りすましを防止できます．この使い捨てパスワードの一方式であるS/KEYには，MD関数とよばれる暗号アルゴリズムが利用されています．

また，セキュリティを確保する方式が提案されているアプリケーションとしては電子メイル，telnet，WWWがあげられますが，それぞれの方式について紹介されています．そのどれもが，秘話性には共通鍵暗号方式を用いた通信内容の暗号化を用いており，また，共通鍵暗号方式を用いた通信内容の認証もサポートしているものがあります．

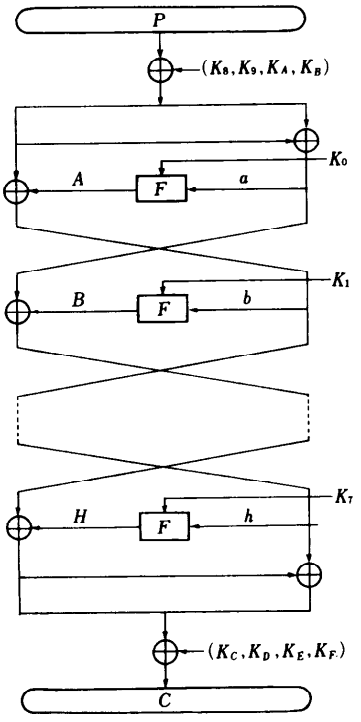

図-3 Feistel型暗号方式（FEAL-8暗号の例）

最後に，項を新たにして，IP addressの枯渇問題に対処するために考えられた次世代IP（IPv6）についても，そのセキュリティ機能について解説されています．

4. 社会での暗号技術の取り扱いとClipper Chipについて

解説「社会での暗号技術の取り扱いとClipper Chipについて」では，Clipper Chipと呼ばれる暗号とプライバシーにとって重要な技術について解説されています．

Clipper Chipとは，1993年にクリントン政権によりその構想が発表されたもので，簡単には「政府などの機関による，合法と認められた盗聴を行う」ために提案された**鍵供託暗号**を実現したものです．これは，近年の暗号技術の進歩により，捜査機関が解読不可能となる暗号通信を犯罪組織が行うことに対する懸念から生じたものです．

暗号通信を行う際には，通常の暗号文だけでなく，通信の暗号化に用いた鍵を装置ごとの暗号化鍵で暗号化して配送する（これをLEAFと呼ぶ）ようにします．

装置ごとの暗号化鍵は鍵保管機関に暗号化された形態で格納されており，裁判所の許可を得た捜査当局は，この装置ごとの暗号化鍵を鍵保管機関から入手して，通信の暗号化鍵を求め，実際の通信を盗聴できるようになっています．

解説では，このClipper Chipの詳しい動作原理について記述されており，また，合法的な盗聴を妨害することを防ぐため，非公開な部分も存在すると述べられています．

また，安全性についても解説されており，基本的にはDESと比較されていますが，しかし，それは総当たり攻撃下での信頼性です．後述する**差分攻撃法**に耐え得るとの記述もあるようですが，差分攻撃法の後に考案された**線形攻撃法**に対しての安全性は不明です．

また，Clipper Chip特有の攻撃法として
・LEAFの偽造
・LEAF feedbackによるLEAFの送信回避
・Squeezing攻撃
があげられています．

5. 暗号アルゴリズムの評価

解説「暗号アルゴリズムの評価」では，暗号アルゴリズムの評価について述べられています．これは，政府の取組みも含めた暗号評価技術の研究開発状況をまとめた最初のもので，日本における暗号評価の現状についてまとめられています．

暗号アルゴリズムの評価には地道な努力が必要であると指摘されています．一般的な評価法としては，

・暗号化鍵の長さ
・平文の長さ

などがあげられ，また，これらは，総当たり攻撃法の有効性の検討につながります．攻撃者が利用すると仮定できる計算機パワーが年々進歩していることから，実用的な長さを評価する必要があります．

また，同じ鍵で暗号化を繰り返して，その周期を調べるという評価方法もあり，

・周期が十分に長いか?
・周期を短くする鍵が存在するか?

といった検討も必要です．

当然，乱数性の統計的評価も重要であり，

・鍵を固定して平文を変化させたときの暗号文の変化
・平文を固定して鍵を変化させたときの暗号文の変化
・平文と暗号文の相関

といったものや，暗号方式が，数学的な関数として代数的構造を持つかどうかも重要な評価基準です．

以上が，暗号アルゴリズムをブラックボックスとして，システム外部から評価したものですが，一方，システム内部からの評価としては，暗号アルゴリズムの構造に立ち入って，

・差分攻撃法
・線形攻撃法

などに対する信頼性を検討する必要もあります．

本稿では，暗号アルゴリズムの評価に対する情報提供の必要性が指摘され，日本の現状として，通産省の提言と施策，および，郵政省のプロジェクトについて述べられています．また，上で解説されたClipper Chipに関しても，日本でも十分議論する必要があると指摘されています．

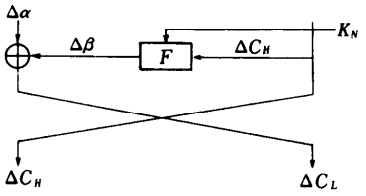

図-4 攻撃する暗号方式の最終段

6. 暗号の攻撃・解読法

最後に，**「暗号の攻撃・解読法：線形攻撃法」，「暗号の攻撃・解読法：差分攻撃法」**と題して，それぞれ代表的な共通鍵暗号方式の解読法である線形攻撃法，差分攻撃法について解説されています．

線形攻撃法も差分攻撃法も，暗号アルゴリズムの固有の構造を利用し，入力値と出力値の間になんらかの相関を見い出し，それを手がかりに，暗号化鍵を推定しようというものです．

6.1 線形攻撃法

線形攻撃法とは，高い確率で入力値と暗号化鍵と出力値のビット間に排他的論理和による関係式が存在する場合に，それを手がかりに暗号化鍵を推定しようというものです．ここで X を平文，Y を暗号文，K を暗号化鍵とし，たとえば，$X[i]$で X の i ビット目を意味するとします．

このとき，X, Y, K の間に，

$$X[i] \oplus K[i]=Y[i]$$

なる関係が存在すれば，逆に，

$$X[i] \oplus Y[i] = K[i]$$

として鍵を求めることができるのは明らかでしょう．

線形攻撃法は，このような関係式を複数のビットに拡張し，関係式が有意な確率で成り立つことを武器に鍵を推定していきます．

DESは，既知平文攻撃下で，この線形攻撃法を用いた計算機実験による解読が実証されています．

6.2 差分攻撃法

差分攻撃法とは，2つの入力の差分値とそれぞれの出力の差分値の間にある暗号化鍵に依存しない関係式を用いて，それを手がかりに暗号化鍵を推定しようというものです．たとえば，X と X^* の差分とは，$\Delta X=X \oplus X^*$ で定義されます．今，

最終段の差分値に関して図－4のような関係を予想します．このとき，高い確率で$\Delta\alpha$になるのであれば，同様に高い確率で，

$$\Delta\beta = \Delta\alpha \oplus \Delta C_L$$

となります．したがって，

$$\Delta\beta \leftarrow F(C_H, K_N) \oplus F(C^*_H, K_N)$$

となる鍵K_Nを総当たりで調べることが可能になります*．こうして，最終段の鍵が求められたならば，順次，その上の段の鍵を求めていけばよいことは明らかです．

差分攻撃法は，DESに対する総当たり攻撃よりも効率的な解読法としてセンセーションを巻き起こしました．また，FEAL-8に対しては，選択平文攻撃下で，計算機実験による解読が実証されています．

7. おわりに

以上，本特集の概要について解説してみました．暗号利用者の立場からは，運用条件(要求速度，実際のサービスにおける平文の扱い等)を分析して攻撃成立の可能性を評価し，暗号アルゴリズム，鍵の変更周期，暗号化段数等を選択することが重要になります．

それでは，暗号理論の面白さをお楽しみください．

(平成8年2月13日受付)

藤岡　淳(正会員)

昭和37年生．昭和60年東京工業大学電気・電子工学科卒業．平成2年同大学院理工学研究科電気・電子工学専攻博士後期課程修了．工学博士．同年日本電信電話(株)入社．平成5年から6年までスイス連邦工科大学客員研究員．現在，NTT情報通信研究所主任研究員．情報セキュリティ，ネットワーク・セキュリティなどの研究開発に従事．平成4年度電子情報通信学会業績賞，小林記念特別賞受賞．電子情報通信学会会員．

* 一般的には，この部分鍵のビット長は暗号化鍵のビット長を超えない．