情報セキュリティ（特に暗号）について

竹内　博

Notes on Information Security, in Particular Cryptography

Hiroshi TAKEUCHI

ABSTRACT

Cryptography has recently been given attention as one of security technology　In this paper we survey the modern cryptography such as DES, RSA cryptosystem, and zeroknowledge system

KEYWORDS　cryptography, security

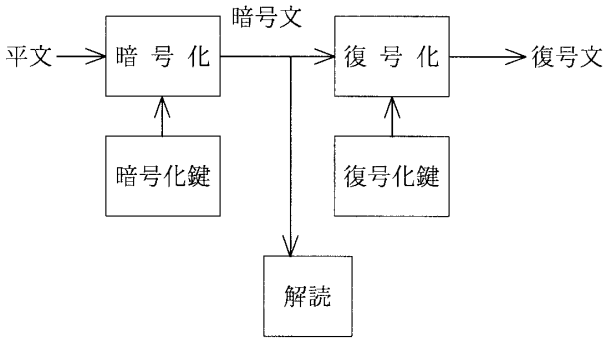
1　まえがき

情報セキュリティ又は情報セキュリティ対策とは広義には災害，過失，悪意等様々な脅威に対する情報の安全性，信頼性対策をすべて含む。狭義には信頼性を含めないのが一般的である。ここではさらに主として人間の悪意や不正行為に対する情報の安全性という面に焦点をあてた対策技術，暗号技術を考える。

暗号とは情報の意味が当事者以外にはわからないようにするための方法及び関連技法の全般を指しその技術を暗号技術という。昔，暗号といえば軍事研究，すなわち秘密の軍事命令，通信，外交官への政府からの指令，スパイからの報告などに実用的意味があった。現在，情報ネットワークの発達により商用にもプライバシーの保護の目的のために受信者以外に秘密にしたいという要求か生じてきた。情報の漏洩，不正使用，改ざんにたいする保護対策としての情報セキュリティ技術の１つとして暗号が利用される。もちろん情報セキュリティ対策は暗号以外にその他，管理面，法律等の対策もある。

2　モデル

ある情報を意味が分からないように変換することを暗号化，元に戻すことを復号化という。暗号化する前の情報を平文，暗号化された情報を暗号文という。暗号化は暗号化鍵というパラメータに依存する変換である。当事者以外の第三者が暗号文をもとの平文に戻すこと，あるいは復号化鍵を見いだすことを解読という。モデルは以下の図式のようになる。



例

2．1　シーザ暗号．もっとも古い暗号で平文をIBMとして暗号文HALとする。このとき１文字のずらしなので鍵はN=1となる。

問題点として簡単に解読されるので単に同し数をずらす以外の工夫か考えられる。例えはI→A，B→K，C→Nなど（換字暗号）

このときは置き換え表か鍵となる。しかし暗号化鍵と復号化鍵の共有が大変。また同じ鍵を通信に対して何度も使うとまたまた解読されやすくなる。ちなみに英文ではｅの文字

の出現回数かもっとも多い。

2 2　ビジネル暗号（16世紀－　）

暗号における文字の出現確率か均等になるように工夫された暗号

例　HOW ARE YOU　　平文

ENG LAN DEN　　鍵

（A＝0，B＝1，C＝2，　,Z＝25として）

LBC LRR BSH　　暗号文

（H＋E＝L（7＋4＝11））

問題点　鍵の長さを平文と同しぐらいにとると安全てあるか，鍵の共有とその保管か大変。同し鍵を何度も使うとやはり解読される。

2 3　転 置 式

順番を入れ替える。（12345）の順を（31254）に換える。

例　　平文　KEIEI　暗号文　IKEIE　このとき鍵は（31254）となる。

以上か典型的古典的暗号である。

エピソード　暗号は軍事用として早くから使用されていた。日本でも，たとえは日露戦争時の日本海海戦の連合艦隊から大本営への報告として有名な（敵艦隊見ゆるとの警報に接し連合艦隊は直ちに出動。これを撃滅せんとす。本日天気晴朗なれども波高し）の暗号電報文かのこっている。

第2次大戦中には暗号機か作られ実用されていたか，使用していたドイツのエニクマ暗号，日本の紫（パープル）暗号は，英国，米国に解読されていたらしい。

推理小説のほうではその初期から暗号は大活躍し，エドガアランポーの黄金虫，江戸川乱歩の二銭銅貨なとかある。

3　現代暗号

情報ネットワーク等非常に多くの人か暗号を使うことを考えるときに，暗号のやり方すなわち方式自体を秘密にすることは，不可能てありまた効率も悪い。この考え方により現代暗号か研究されている。

3 1　DES型暗号

この暗号は1977年米国において標準化されている。（DATA ENCRIPTION STANDARD）方式は入力64ビット出力64ビット鍵64ビットて転置と換字を基本にしてのくりかえしを行う。
これは発表以来全世界の人々かいろいろ解読を試みているか，15年以上たった今も解読されず一応安全と考えられ，実用化も多い。

日本ても1986年FEAL（FAST ENCRIPTION ALGORITHM）の名前でNTTにより開発発表された。FEALはF関数の実現てDESに比へメモリコストか少なくなる方式てあった。発表の2，3年後には解読法の公募も1年間かけて行った（懸賞金100万円）か応募もなく安全な暗号のように思えた。ところか1991年ころからFEALについての解読法か出始め，現在安全性について問題かある。
設計後5年あまりてあった。

3 2　公開鍵暗号

暗号についての画期的アイティアか1976年始めて示された。以前の暗号系はいすれも暗号化鍵，復号化鍵ともに秘密にするものであった。しかしこの公開鍵暗号方式は暗号化鍵は秘密にせす，公開する（公開鍵）。こうすることによりいちいち鍵を慎重に配送する必要かなくなる。復号化鍵は秘密にする。この復号化鍵を知らないと復号化かてきない（困難）方式てある。例えは今AさんからBさんに暗号文を送るとき

1。Bさんか暗号化鍵Kと復号化鍵Hを決める。そしてKをAさんに送る。（公開ファイルに登録されていてもよい）

2。Aさんはこの鍵を使って平文を暗号化してBさんに暗号文を送る。

3。Bさんは復号化鍵Hを使って復号文を得る。
盗聴者は暗号文と暗号化鍵を得ることは可能であるが，これだけからは復号文を得られない方式である。（計算量的に困難）
具体的実現を始めて行ったのかRivest，Shamir，Adelemanでありの RSA 方式と呼ばれる。方法は以下のように行う。
準備　p，qの2つの大きな素数を選ぶ。（10進数50から100桁）この積 n＝pq を計算する。d＝(p－1)(q－1) を計算する。（実は（p－1）と（q－1）の最小公倍数でよい） e として ed＝1（mod n）となる数をとる。（これはユークリッドの互除法により可能）
「記号の説明　整数aを整数nで割ったときの余りをa（mod n）で表す。
a（mod n）＝b（mod n）の時a＝b（mod n）と書く。」

今平文Mをある数字に変換された物とする。（ASCIコードなど）
1。$C=M^e$（mod n）を暗号文として送る。
　暗号化鍵は（e，n）で公開される。
2．復号は $C^d=(M^e)^d=M$（mod n）によりなされる。
　復号化鍵はdで秘密。この式はフェルマの小定理 $M^{p-1}=1$（mod p）を使って示される。（フェルマの大定理 $x^n+y^n=z^n$（n＞2）をみたす自然数x，y，zはないだろうという問題は200年らいの難問であったか最近解決された。）
この方式の安全性は素因数分解の困難さに基ずいている。例えば11×13＝143の計算は容易であるが，143から11と13を見つけるのは大変。
RSA は発表以来20年近くたち，また公開鍵暗号の代表として登場したがまだ解読されていない具体的実現という点でその価値は大きい。その他公開鍵暗号は各種提案されては解読された暗号も多い。有名なものではマークルとヘルマンによりナップザック問題に基ずいた公開鍵暗号か1978年提案されたがこれはみごとにシャミアにより1982年解読された。

RSA の問題点
1。大きいべき乗（d＝100～200桁）の計算を必要とするので，かなり計算時間を必要とする。高速処理に向かない。
2。公開鍵ファイルの管理が大変（特に大規模ネットワークになると）になる。

そうすると鍵配送を工夫して DES 型暗号を使った方法が実用的。鍵配送の方式として公開鍵方式方式の利用か考えられる。たんに鍵の配送たけならは1976年ディフィとヘルマンにより提案されたDH 法がある。之は以下のように行う。

今AさんとBさんが鍵を共有したいとする。A，Bさん達はあらかじめ自分の秘密鍵を決める。
例　0以上p－1以下の乱数（pは150桁程度）としてa，bとする　また mod p での原始根 α を取る。そして各自 $a'=\alpha^a$（mod p），$b'=\alpha^b$（mod p）を計算して公開する（実際はセンターなどに登録）。AさんはBさんの公開鍵b'を調べ，これに自分の秘密鍵aを使って $k=b'^a$（mod p）の計算をする この鍵kを使ってAさんはBさんに暗号文を送ることができる。ただしBさんはあらかじめ自分の鍵がb'であることをAさんに伝える必要はある　Bさんは暗号文をうけ取るとAさんの鍵a'を調べ自分の秘密鍵bを使って $k=a'^b$（mod p）を計算する。α^{ba}（mod p）$=\alpha^{ab}$（mod p）によりAさんとBさんは同じ鍵が共有される。一般にa'からaを求める問題を離散対数問題と言うか之は困難である。

4　ディジタル署名（電子印鑑），認証

認証は情報の正当性，完全性を確保するための技術である。暗号は情報の秘匿を目的とするか，認証では情報か変えられていないことの確認を目的とする。認証自体は暗号とは独立した概念であるか暗号技術の応用で実現される。このうちディジタル署名は，

普通のサインと同しくメッセージや情報の作成者か確かにそれを作成したことを示すもの。DES, RSA 方式により可能てあるか，米国に於いて標準化か進められているものの原型である離散対数問題に基ずくエルガマル公開暗号による方式か有力てある。電子印鑑システムの NTT の構成例としては，IC カート（各人かそれそれ持つ印鑑と思う），IC カート読みとり装置，パソコンか必要となる。
エルカマル方式は以下のように行う。

今Aさんか署名しBさんか検証する場合を考える。しはしはAさんを証明者Bさんを検証者とも言う。Aさんは大きな素数 p を選ひ，mod p ての原始根 α を取る。$0<x<p-1$なる乱数 x を選ひ $y=\alpha^x \pmod p$ を計算し（y, p, α）を公開する（公開ファイルに登録）。(x, p, α）かこのときの秘密鍵。さて認証つきメッセージの送り方は以下の手順

1。Aさんは$p-1$と互いに素な乱数 k を生成する
2。Aさんは $r=\alpha^k \pmod p$ と $s=(m-xr)\times k^{-1} \pmod{p-1}$ を計算してmと(r, s) をBさんに送る。
3　Bさんは受け取った m, (r, s) から $\alpha^m=y^r y^s \pmod p$ か成立するかどうかみる。もしAさんからの正しいメッセージならは成立する。

最近（といっても数年前から）注目を俗ひているのかゼロ知識証明方式と呼はれる方法かある。これは証明者と検証者か対話しなから証明者か秘密情報を全く漏らすことなくその情報を知っていることを検証者に納得させる方法です。例えは銀行の暗証番号を証明者は知っているとするかそれ自体を明かすことはいろいろと危険てある。このとき暗証番号を知っていることを相手に納得させれはよい。
実現方法は1986年フィアットとシャミアによって提案された FS 法か有名。
これは証明者か持っている秘密情報 s を１ビットも漏らさずに検証者にその秘密情報 s を証明者が持っていることを理論的に納得させることかできる。認証に利用する。以下のように行う。

1。証明者Aは大きな素数 p，q から $n=pq$ を計算し公開する。
　また秘密情報 s に対して $c=s^2 \pmod n$ は検証者も既知とする。
2。証明者Aは乱数 r を生成する。
3。$x=r^2 \pmod n$ を検証者Bに送信する。
4。検証者Bは e としてランタムに 0 または 1 を選ひ証明者Aに送る。
5。証明者Aは $y=rs^e \pmod n$ を検証者Bに送る。
6。検証者Bは $y^2=xc^e \pmod n$ をチェックする。
　（成立すれは合格，しなけれは不合格）
2－6のやりとりを t 回くりかえしてすへて合格の時，最終的に合格とするとき s を知らないのをこまかせる確率は $(1/2^t)$ となる。

最近出版された［4］にはゼロ知識証明の詳しい解説かある。

5　応　　用

情報ネットワークとそのセキュリティを考えるとき暗号を利用しようとするのは以上のことから自然である。しかしそのセキュリティの必要度合いを考えそれほどの装備を必要としないケースも多い。このバランスか実際は重要であろう。

5 1　電子金融システム，電子現金（電子通信を用いて資金移動を行う）

銀行間なとの金融機関どうしの資金移動ではセキュリティは重要であり，実用されているのてはなかろうか。
個人と金融機関の間ではプリペイドカート，クレシットカードは既に現在普及しているかプライバシーなとの点て問題かある。
　電子印鑑はまさにティジタル署名そのもの。
　将来は個人間，法人間での取引にも利用。(貨

幣，手形の代わり）

5 2　電子選挙

家庭で選挙投票を行う。選挙の管理者を完全に信用でき，また記名投票でよいならディジタル署名をつけて，管理者に送ればよいのでなにも問題なし。
しかしこれではプライバシーが守れない。電子無記名投票。

5．3　ネットワークでゲーム（じゃんけん）

宝くじ，競売

5．4　ICカード

現在磁気カードか普及しているか低記憶容量とデータ保護機能で問題かある。この対策としてICカードが検討されるが後者の対策として暗号の利用。

5 5　コンピュータにおけるセキュリティ

アクセス制御（パスワード等），ファイルの暗号化

5 6　ゼロ知識証明は暗号の分野からひろがり理論計算機分野の計算量の話と密接に結びついた。IP＝PSPACE（shamır）

代数との結ぶつきではこれまではどちらかというと初等整数論という感じであったか楕円曲線による公開鍵暗号も提案され理解するのも難しい暗号も登場している。

5 7　放送における利用

著者か暗号に実際関わったのは，衛星放送におけるスクランブル放送の分野である。放送におけるセキュリティ技術は通信におけるセキュリティとは異なる面かある。放送番組自体か扇れても受信者か損害を被ることはなく，受信者には完全な鍵管理を期待できない。暗号の鍵は受信者にもわからない必要がある。このためには鍵を受信機等に収めてしまう方法か考えられる。
信号のスクランフルも必ずしもその内容の秘匿が完全である必要もない。不正に受信使用とする人か復元できないようにすればよい。正規の手続きを経てそして契約後，受信機にはスクランブル鍵，暗号化鍵，番組に関する情報か関連情報として電波で送られる。料金に関する媒体はまた別経路となる。
映像のスクランブルは走査線内信号切り替え方式（ラインローテーション）と走査線転移方式（ラインパーミュテーション）の組み合わせ，音声信号はPN信号の加算で行われる。

6 まとめ

暗号を用いた情報セキュリティ技術は一時期のブームともいえる研究段階から実用段階に入ったといえる。しかし暗号は常にとんでもないアイデアにより解読される危険性かある。そのために次の代わりになるものを用意する必要かある。DES，RSAともにその安全性についての保証は理論的にはなされていない。

DESにしてもRSAにしても発表されないか既に解読されているかもしれない。今後提案される暗号はこの安全性の検討付きのものとなろう。
応用面では利用できる分野もその他あるように思われるか，今後の課題であろう。

参考文献

［1］暗号理論入門　岡本　栄司　著　1993年　共立出版
［2］暗号のおはなし　今井　秀樹　著　1993年　日本規格協会
［3］情報セキュリティの科学　太田和夫　他著　1994年フルーハックス　B-1055　講談社
［4］暗号・セロ知識証明・数論　岡本龍明，太田和夫編　1995年　共立出版