情報セキュリティの基礎技術
～暗号技術～

EHS&S 研究センター上級研究員 兼 情報システム技術本部副本部長　久保田英之

Keyword：セキュリティ，情報セキュリティ，暗号，デジタル署名，ハッシュ関数

1．はじめに

本稿では，情報セキュリティ分野の基礎技術である暗号技術についての概要を解説する。近年では，セキュリティというと多くの場合「情報セキュリティ」を指すことが多いが，情報セキュリティの動向を把握するためには，暗号技術についての知識が必須である。

2．セキュリティとは

2.1　セキュリティの意味

情報セキュリティについて述べる前に，セキュリティとはそもそも何を指すかを明確にしておきたい。一般にセキュリティとは，侵入や盗難，破壊など悪意を持って行われる人的脅威に対しての安全と考えられている。

言語学的にいうと，セキュリティ（security）とはセキュア（secure）な状態を示す名詞形である。secureの語源はラテン語のsecuraで，seが避ける（without），curaが心配ごと（care）であるので，secureとは「心配ごとがないこと」を意味する。

よって，広くは心配ごとすなわちネガティブな要因から解放されていることをセキュリティという。

例えば，お金を貸すといつ返ってくるか不安なので，それを抑える担保のことをsecurityという。また，出資した人・団体を損害から守るので証券のこともsecurityという。

しかし多くの場合，セキュリティは「攻撃から守ることによって得られる安全」「攻撃からの安全を確保する行為」を意味する。

「日米安全保障条約」は，the U.S.-Japan Security Treatyであり，この場合のセキュリティが軍事的脅威という人的脅威からの安全を指していることが分かる。

このように，セキュリティという語を使う場合には，心配ごとすなわち何から何を守るかを明確にすることが重要である。

2.2　セキュリティが守るもの

セキュリティが「守る」ことであるとすれば，セキュリティによって守られる「もの」が存在するということでもある。

古くから「もの」の典型は人命，お金（紙幣・貨幣），宝石・貴金属，有価証券，書類という実体があるものであった。手に取ることができるといい換えてもよい。従ってものを守ることの基本は，そのものを隔離し，外部から見えなくし，容易に接触できなくするということであった。簡単にいえば，入り口に錠を取り付け鍵がないと開けられないようにすることである。

「容易に接触できなくする」と書いたのは，セキュリティが必ずしも「もの」を盗難から守ることではなく，行為や会話を盗み見や盗み聞き（盗聴）から，あるいは書類を書き換え（改竄）から守ることも含むからである。

ところが世が情報（化）社会となり，情報という実体がないものが「もの」と同等な価値を有するようになってくると，情報を守らねばならなくなった。

情報社会ではコンピュータによる処理（情報処理），通信メディアによる伝達（情報伝達）によって，大量の情報が絶え間なく生産・蓄積・伝播される。このような情報を守るのに，これまでのような「隔離して錠と鍵とで守る」方法は取りにくい。

そこで情報セキュリティという言葉が生まれた。

情報セキュリティとは，旧来の「書類等を錠と鍵とで守る」（物理的セキュリティ）だけでなく，「情報処理や情報伝達を通じて情報の機密性・完全性・可用性を確保すること」，と1992年にOECD（経済協力開発機構）のセキュリティガイドラインで定義された[1)]。英語の頭文字をとりCIA3要素と呼ばれている。

また，GMITS（ISO/IEC TR13335）ではCIA3要素に責任追跡性・真正性・信頼性を加え6要素をあげている（表1）。なお，ISO/IEC TR13335の各パートは後にISO/IEC 13335：2004（JIS Q 13335：2006）になり，最終的にこれらの考えはISO/IEC 27001（JIS Q 27001）に引き継がれている。

これら情報セキュリティを構成する6要素のうち，機密性・完全性・責任追跡性を守る手段として，情報を暗号化する技術がある。よって，情報セキュリティには暗号技術が欠かせない。

表１　情報セキュリティを構成する要素

要素	状態	脅かすリスク
機密性（Confidentiality）	意図した相手以外に情報が漏れないこと	盗聴，内部からの情報漏洩
完全性（Integrity）	情報が正確であること	改竄，ノイズによるビット反転・欠落
可用性（Availability）	許可された人が必要な時点で情報を使用できること	過負荷，災害，意図しないロック状態
責任追跡性（Accountability）	ユーザの行動や責任を説明できること	ログの改竄，否認
真正性（Authenticity）	ユーザやシステムによる振る舞いが明確であること	なりすまし
信頼性（Reliability）	システムやプロセスが矛盾なく動作したり一貫して動作したりすること	ハードウェアの故障

３　情報セキュリティのための暗号技術

３.１　暗号の起源と基本用語

もともと暗号は，軍事的な通信を秘匿するためにつくられた。

戦場では，司令室と最前線，戦線同士のやり取りが相手に漏れたら命取りになる。よって古くは伝令が持っていく通信文，近年では電気通信や無線通信にのせる電文を必ず暗号化する。伝令が捕えられ指示書が奪取される，あるいは通信が傍受されるようなことがあっても相手に真意が伝わらないようにするためである。

暗号の基本は，正当な受信者しか復号（暗号化された文書を元の平文（ひらぶん）に戻すこと）ができないということにある。

「ニイタカヤマノボレ」が「対米英開戦」を意味するといった合言葉を拡張した「コード（code）」と呼ばれるものも，古典暗号と呼ばれる暗号の一種である。

一方，本稿ではコンピュータ登場以後の現代暗号と呼ばれるものだけを扱う。とはいうものの，現代暗号だけでも１冊の本になるほどのバリエーションがあるので，ここでは現在最も代表的と考えられるものだけに焦点をあてる。

前提として，平文は電子情報化され，０と１の２値で表現されているものとする。英数漢字はコンピュータで扱うために，一定の約束（文字コード）で２値化（エンコーディング）される。従って，文書は０と１の羅列（ビット列）として扱われる。

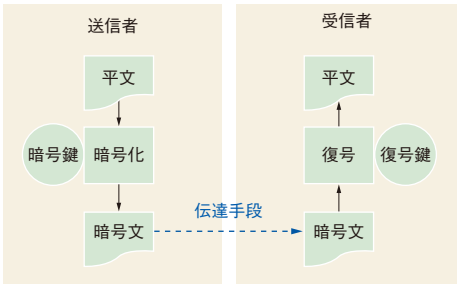

図１　暗号化と復号

以下，平文を暗号文に変換する，もしくは暗号文から平文に変更する際に使用するパラメータを鍵と呼ぶ。方向によって区別する際は前者を暗号鍵，後者を復号鍵と呼ぶ（図１）。鍵を秘匿している場合を秘密鍵，公開している場合を公開鍵と呼ぶ。

一般に，暗号化の方式が同じであっても鍵が異なる場合，同じ平文に対して得られる暗号文は全く異なる。

３.２　共通鍵暗号の代表，バーナム暗号

共通鍵暗号とは，暗号化と復号とで同一の秘密鍵を用いる方式である。秘密鍵が同一であるので共通鍵とも呼ぶ。

ここで取り上げるバーナム暗号は，第一次世界大戦中（1917年）にギルバート・バーナムによって考案された（当時特許が取得されたが現在では切れている）。1949年，クロード・シャノンにより，この暗号は理論的に解読不能であることが数学的に証明されている。

バーナム暗号では，平文と同一の長さの暗号鍵（乱数）を用意する。平文と暗号鍵とをビットごとに排他的論理和（xor：Exclusive OR）を取ることで暗号化している。ここで排他的論理和とは表２のような演算である。

このxorを用いて，平文mと鍵kとで暗号文cを以下のように得る。

$c = m \text{ xor } k$

暗号文を復号するのも，暗号文cと暗号鍵kとをビットごとにxorを取るだけである。

$m = c \text{ xor } k$

これは表３のように，A xor Bの結果に再度xor Bすると，Aと一致することで分かる（Aをm，Bをkと置き換えて考える）。

暗号化・復号とも演算自体は非常に簡単であるが，鍵として平文と同じ長さの乱数を毎回用意しなくてはならない。同じ鍵を複数回使用すると，統計的な処理によりこの暗号方式は解読可能であるとされる[例えば２)]。

表２　排他的論理和

A	B	A xor B
1	1	0
1	0	1
0	1	1
0	0	0

表３　排他的論理和の特性

A	B	A xor B	B	(A xor B) xor B
1	1	0	1	1
1	0	1	0	1
0	1	1	1	0
0	0	0	0	0

暗号通信のたびに，前もって秘密鍵を共有しないとこの暗号方式は使えない。実用的には大量の乱数を用意し，前もって相手に手渡しておいて，通信のたびにそれを使いつぶしていくという方法が考えられる。しかし，いずれは用意した乱数を使い切ってしまう。

3.3　バーナム暗号の改良

大量の乱数を共有するのは大変な労力を伴うので，弱くなることを覚悟できるのであれば，疑似乱数を使うという方法はある。

疑似乱数とは，種（シード）と呼ばれる情報を入力として，決められたアルゴリズムによって生成される乱数のことである。シードだけを送り手，受け手で共有するという策である。

しかしソフトウェアによってつくられた疑似乱数は，いつかは繰り返されてしまうので，原理的には解読されてしまう。

秘密鍵の共有という問題がバーナム暗号の弱点なのであるが，この問題を量子状態の特性（乱れやすい）によって解決しようとするのが量子暗号（量子鍵配送）である。

量子とは，原子より小さい世界を構成する，粒子性（物質の性質）と波動性（状態の性質）を併せ持つ特殊な存在である。量子暗号とは，量子の一種である「光子」を使う技術であり，1984年にチャールズ・ベネット，ジャイルス・ブラザードの発表した論文[3)]で原理が提案された。

光子による通信を第三者が傍受すると必ずそこに乱れ（ノイズ）が発生するため，傍受されたことが検出可能となる。そこで光子通信に秘密鍵をのせて相手に送り，傍受を検出することなく相手が受け取れればその秘密鍵を有効とし，その秘密鍵を使って暗号通信を行う。傍受が検出された場合にはその秘密鍵を無効とし，送信側は新たに秘密鍵を作成し直し，光子通信による鍵配送を試みる，ということを傍受が検出されなくなるまで繰り返す。これが量子鍵配送の原理である。

このように最新と呼ばれる量子暗号方式も，基礎となるのは古典的な技術である。

3.4　公開鍵暗号の原理

共通鍵暗号では，送受信者間で事前に秘密鍵を共有しておかなければならなかった。

1976年，ホイットフィールド・ディフィーとマーティン・ヘルマンによって公開鍵暗号というアイデアが提示された。

公開鍵暗号は図２の３つのアルゴリズムから構成されている。①鍵生成アルゴリズム（KeyGen），②暗号化アルゴリズム（Enc），③復号アルゴリズム（Dec）である。

鍵生成アルゴリズムKeyGenは，セキュリティパラメータkを入力として，公開鍵p_kと秘密鍵s_kの組を生成する。ここでセキュリティパラメータとは，公開鍵や秘密鍵のサイズを決定する値であり，値が大きいほど暗号化強度が強くなる（演算に要する時間は長くなる）。公開鍵p_kから秘密鍵s_kを算出することが実用上不可能であることが，鍵生成アルゴリズムKeyGenの特徴である。

暗号化アルゴリズムEncは，平文mと公開鍵p_kとを入力として，暗号文cを出力する。

復号アルゴリズムDecは，暗号文c，公開鍵p_k，秘密鍵s_kを入力すると復号結果（平文）mを出力する。

以上の３つのアルゴリズムを使い，送信者Aから受信者Bへメッセージを送る手順を説明する。

暗号文を受け取りたい受信者Bは，鍵生成アルゴリズムKeyGenを使い，公開鍵p_kと秘密鍵s_kとのペアを作成し，公開鍵p_kだけを公開する。受信者Bにメッセージを送りたい送信者Aは，Bが公開した公開鍵p_kを使って平文メッセージmを暗号化アルゴリズムEncを使い暗号文cを作成，受信者Bに送付する。受信者Bは，復号アルゴリズムDecに暗号文c，公開鍵p_k，秘密鍵s_kを入力し平文メッセージmを復元する。

暗号化されたメッセージが途中で改竄された場合には，秘密鍵s_kを使って正常に復元できなくなるので，改竄は容易に発覚する。

3.5　実際の公開鍵暗号

1976年にディフィーとヘルマンが発表したのは公開鍵暗号の概念であり，実際に暗号として提唱（公表）されたのは1977年，リベスト，シャミア，エーデルマンの３名連名によるものであった（３人の名前の頭文字をとってRSA暗号という）。

RSA暗号を理解するためには整数論の知識が必要であり，ここでは説明しきれないが，ポイントは２つの巨大素数を使うということである。非常に大雑把にいうと，２つの異なる素数の積を公開鍵とし，個々の素数を秘密鍵としているような方式である。そして２つの巨大素数を掛け算することは簡単であるが，掛け算された数値を２つ

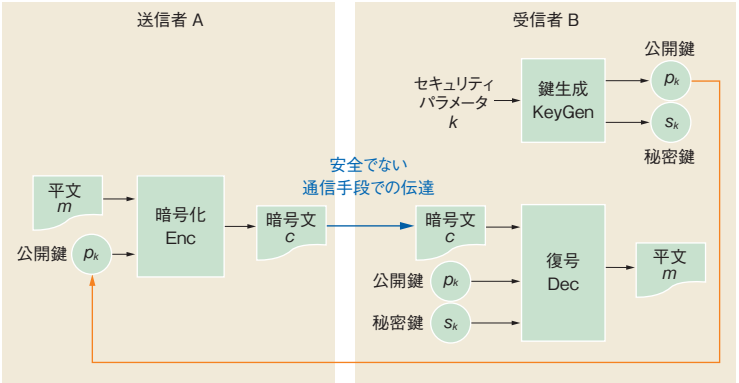

図２　公開鍵暗号を構成するアルゴリズム

の素数の積に戻す（素因数分解する）のは簡単ではない（計算時間が非常にかかる），という一方向性が暗号の強さの源になっている。

暗号の安全性はセキュリティパラメータの大きさ（ビット長）に依存しているが，どれほどの長さをとれば安全（実用的な時間内では素因数分解できないことをもって安全とみなす）であるかは，その時点でのコンピュータの性能に依存する。よって，時代と共にコンピュータの性能が上がれば，かつては安全とされたセキュリティパラメータが安全でなくなる。これを危殆化（きたいか）という。

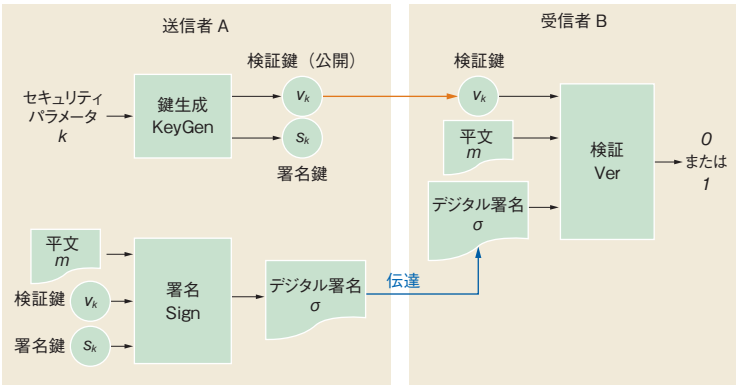

図３　デジタル署名を構成するアルゴリズム

あくまで今あるアーキテクチャのコンピュータの性能では素因数分解に時間がかかることを根拠にしているので，今後画期的な算法が開発される，あるいは新たなアーキテクチャのコンピュータが出現した暁にはこの前提が崩れる恐れはある。すでに量子コンピュータの出現によりこの前提が崩れはじめているという意見もある。

RSA暗号以外にも公開鍵暗号は存在し，代表的なものに楕円曲線暗号がある。また，近年頻繁に取り上げられるようになったブロックチェーンも，公開鍵暗号を利用したものである。これらについては別の機会に紹介することとしたい。

実際にはこれら公開鍵暗号のアルゴリズムは計算量が膨大で演算時間もかかるため，大きなメッセージをやり取りする，あるいはリアルタイム通信を暗号化するには適していない。

そこでメッセージ本文をやり取りする前に，公開鍵暗号方式で秘密鍵の共有を行った後，その秘密鍵を使用して共通鍵暗号方式でメッセージ本文を暗号化して送信を行うことが実際には行われている。この方法は今ではディフィー・ヘルマン鍵交換（DH鍵交換）と呼ばれている。

３.６　デジタル署名

３.４で送信者Aから受信者Bへメッセージmを送る手順について説明した。しかし受け取った受信者Bは，本当に送信者Aから送られてきたものか（他人がなりすましたかどうか），判断することはできない。なぜならば，受信者Bが公開した公開鍵を使えば誰でも受信者Bにしか復号できない暗号文を作成することができるからである。

そこで考案されたのが，デジタル署名である。公開鍵暗号と似たような手順でデジタル署名を行うことができる（図３）。

送信者は鍵生成KeyGenにセキュリティパラメータkを入れ，検証鍵v_kと署名鍵s_kとを得る。検証鍵v_kは公開し署名鍵s_kは秘匿する。送信者Aは続いて署名アルゴリズムSignにメッセージm，検証鍵v_k，署名鍵s_kを入れ，署名σを出力する。

受信者Bは，メッセージm，署名σ，検証鍵v_kを検証アルゴリズムVerに入力する。暗号と異なり復号は不要であり，検証アルゴリズムVerは署名として正しいか正しくないかの判断だけを行う。正しいと判断されれば，署名主すなわち送信者Aから送られたメッセージであると確認できる。

この方法は明快であるが，メッセージ交換する相手ごとに異なる鍵を使わねばならず，手間がかかる。

その課題を解決するために，インターネット上ではPKI（Public Key Infrastructure：公開鍵基盤）という仕組みが利用されることが多い。PKIの仕組みは明確に決められていて，現在流通しているブラウザはそれに準拠しているので，ユーザは意識することなく暗号通信による秘匿環境を使っている。公開鍵の正当性を，信頼できる第三者機関に証明してもらうことで個別に鍵を入手する手間を省くことができる。

公開鍵証明書を発行する主体を一般に認証局（Certificate Authority：CA）と呼ぶ。認証局は，企業から証明書発行の依頼があった場合にはその企業の登記事項証明書や印鑑登録証明書などによって審査を行い，条件を満たせば公開鍵の証明書を発行する（認証局は公開鍵証明書を認証するだけでなく，失効させることも行う）。

証明書を使った代表的なものが，SSL（Secure Socket Layer）/TLS（Transport Layer Security）という暗号化プロトコルであり，Webで使われるプロトコルHTTP（Hypertext Transfer Protocol）と組み合わせて使われるHTTPS（Hypertext Transfer Protocol Secure）はすでに一般的になっている（URLがhttps://で始まるWebページである）。

従来は，通信ごとに暗号化するためサーバーへの負荷が過大になる，あるいは証明書の取得に多額の費用がかかるなどの理由で，個人情報を含むページだけHTTPSによる通信を使う例が多かった。しかしハードウェアの性能向上により，暗号化の負荷が気にならなくなった，競争により証明書を取得するコストが下がった，サーバーのなりすまし防止のためにGoogleが常時HTTPSを推奨するなどの流れがあり，2016年くらいから常時

HTTPS化が普及している。

3.7　ハッシュ関数

最後に，ハッシュ関数について述べる。ハッシュ（hash）とは，ハッシュドビーフやハッシュドポテトのハッシュであり，切り刻んで混ぜるという意味である。

関数というからには入力と出力がある。ハッシュ関数の入力は任意長のメッセージであり，出力が固定長の値である。この出力のことをハッシュ値と呼ぶ。

同じメッセージが入れば，常に同じハッシュ値が出力される。メッセージが1ビットでも変更されればハッシュ値は大きく変わる。

このことは，先に述べた情報セキュリティを構成する6要素のうち，完全性のチェックに使われる。例えばメッセージを保存する際に，メッセージとは別の安全な場所にそのハッシュ値を保存しておく。メッセージが改竄されたかどうかは，現メッセージのハッシュ値と保存しておいたハッシュ値とを比較すれば一目瞭然である。ただし，どこが改竄されたかはこれだけでは不明である。

安全なハッシュ関数として，表4の3点が備わっている必要がある。

簡単にいうと，オリジナルから1ビットでも変更するとハッシュ値が変化する，ハッシュ値を変えずにオリジナルを変更することが極めて困難，という特徴を持つ。

表4　ハッシュ関数の必要条件

一方向性（原像計算困難性）	ハッシュ値が与えられた時，元のメッセージを求めることが困難であること
第2原像計算困難性	あるメッセージ（第1原像）とそのハッシュ値が与えられた時に，同一のハッシュ値になる別のメッセージ（第2原像）を計算することが困難であること
衝突困難性	同一のハッシュ値になる2つの異なるメッセージを求めることが困難であること

4．おわりに

本稿では，情報セキュリティの基本技術である暗号について述べた。

暗号を本格的に語るには数学（特に整数論）に立ち入らねばならないが，それは避けて「こういうアルゴリズムがある」と述べるだけに留め，基本的な技術のさわりだけを紹介した。

情報の安全について，暗号技術は欠かせないものであり，本稿で身近に使われ頻繁に報道等で取り上げられている基礎的な技術について理解頂ければ幸いである。

〔参考文献〕

1）OECD Guidelines for the Security of Information Systems and Networks：Towards a Culture of Security，http://www.oecd.org/sti/ieconomy/15582260.pdf，2018.5.10

2）IPUSIRON，暗号技術のすべて，翔泳社，2017

3）C.H. Bennett, G. Brassard,“Quantum Cryptography：Public Key Distribution and Coin Tossing”, Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India，pp.175～179，December 1984，https://core.ac.uk/download/pdf/82447194.pdf，2018.5.14

久保田（くぼた）　英之（ひでゆき）

EHS&S研究センター上級研究員 兼 情報システム技術本部副本部長 兼 データベースソリューション部長
工学博士，技術士（情報工学部門，総合技術監理部門），情報処理安全確保支援士（第005832号），認定ファシリティマネジャー

Synopsis

Basic Information Security Technologies ～Encryption Technology～

Hideyuki KUBOTA

The term “security” is generally used to mean safety from manmade threats made with malice.

With the advent of the information society and the need to protect information, an intangible asset, “security” is often used to refer to “information security.” Since it has become difficult to protect information by the traditional means of lock and key, encryption has been adopted as a means of protection.

Although conventionally, the common-key encryption method, an approach that involves the use of a common secret key by both sender and recipient, has been used for encryption, this method presents the problem of how to share keys in advance.

On the other hand, while public-key cryptography, a method that has been advanced in recent years, eliminates the need to share secret keys, the processes of encryption and decryption takes time, making this approach unsuitable for tasks such as exchanges of large amounts of information or real-time information exchanges. To get around this problem, it has become common practice to share secret key (common key) in advance of information exchanges using public-key cryptography and using this key to encrypt the text of the information before transmission.

When using public-key cryptography, the recipient uses the public key for encryption, and this makes falsification of the sender easy. To check for sender falsification, a method known as “digital signature” is used.

PKI (Public Key Infrastructure) is a mechanism for the effective use of digital signatures. Certificates issued by a Certificate Authority (CA) guarantee the reliability of digital signatures. This approach is used for purposes such as encrypting web communications and preventing spoofing of senders of information.