パソボラレベルアップ資料

2018.7.14　米久保昌司

暗号と情報のセキュリティについて

暗号とは

秘密通信の手段として文章にいろいろな操作を施し、第三者が見ても意味が分からないように変換する技法

用語

・元の文章　平文
・暗号化アルゴリズム：文章を暗号化および復号する際のルー ル
・鍵：平文を暗号文にまたは暗号文を平文に変換するための手掛かり
・暗号文：平文を暗号化アルゴリズムと鍵によって変換された文章
・復号：暗号文を平文に戻す作業
・解読：正当な受け手でない者が内容を盗み見ること
　　研究のために元の文章を読み解くこと

暗号の歴史

１．ヒエログリフ

古代エジプトで王や神官の間で使われていた神聖文字。永久に解明されないと思われていたが１７９９年８月にエジプトのロゼッタ村で発見された石版により解明が進んだ。碑文は神聖文字（ヒエログリフ）と民衆文字（デモティック）、ギリシア文字の三種類の文字で記述されている。同一の文章が全部で三つの書記法で著されていると早くから推測され、１８２２年シャンポリオンによって解読された。解読までに２０年も要したのは、同じ文字がある時は表意文字としてある時は表音文字として使われていたためである。

２．シーザー暗号

古代ローマの軍事指導者ジュリアス・シーザーによって考案された暗号。

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
↓ ↓
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

暗号化アルゴリズム：文字をずらす　　鍵：前に３文字

ＰＡＳＯＢＯＲＡ→ＳＤＶＲＥＲＵＤ

シーザー暗号はその文字をずらすことから、「シフト暗号」とも言われ、シフト暗号をアルファベッ トで用いる場合最大 26 パターン試せば暗号が解読される。これを均等にずらすのではなく１文字目は３文字、２文字目は４文字というようにランダムに並べ替えればそのパターンは大きく増加し、解読は飛躍的に困難になる。このように、一定のルールで文字を入れ替えて暗号化する方式を「換字式（かえじしき）暗号方式」という。

3．女王メアリの暗号

シーザー暗号に代表される「単一換字式暗号」の弱点は、アルファベット 1 文字につき 1 つの暗号文字しか割り当てられないことにある。この弱点を克服した暗号として有名なのが、16 世紀のスコッ トランド女王メアリ・スチュアートの暗号である。メアリはイングランドのエリザベス女王暗殺を企てその共謀者とのやり取りに暗号を利用したが、解読されて計画は失敗に終わった。

メアリの暗号は「ノーメンクラター」と呼ばれる暗号で、アルファベットを置き換える他に、フレーズを記号などに置き換える「コード」を加えたものである。この「コード」は送り手と受け手で 事前に「コードブック」を共有することによって、その暗号の解読をより困難にするもので、これも暗号の「鍵」 にあたる。

4．ヴィジュネル暗号

女王メアリの用いた暗号は、膨大なコードブックの準備と、コードブックの共有が暗号利用者の悩みの種であった。この「鍵の受け渡し」は暗号技術が進歩した近代以降の暗号においても利用者にとって課題になっている。

15 世紀になると、レオン・バッティスタ・アルベルティが、二つ以上の暗号アルファベットを使う「多表式」の暗号の原型を思いつき、その後発展を遂げて 16 世紀にはブレーズ・ド・ヴィジュ ネルが多表式の最終的な強力な暗号を考案したことから、ヴィジュネル暗号と呼ばれている。

ヴィジュネル暗号は、ヴィジュネル方陣と呼ばれる表を用いる方式である。

5．上杉暗号

同じく 16 世紀に日本でも、同様に方陣を用いた暗号が編み出されている。戦国の武将、上杉謙信の軍師だった宇佐美定行が著した兵法書に暗号の作り方が記されていて、これはいろは 48 文字を 7×7 のマス目に書き 1 つの文字を行と列の数字で表す暗号である。

6．暗号機　エニグマの誕生

19 世紀まで手作業で作成されていた暗号は、20 世紀に入ると機械式暗号機の登場によって、その解読の難易度が飛躍的に増すことになった。

エニグマは、1918 年にドイツの発明家アルトゥール・シェルビウスによって発明された機械式暗号機で、 携行性と機密性を売りにして販売された。ドイツは第一次世界大戦でイギリスによって暗号が解読されていたことで戦争に敗れたこと知り、暗号が国家の存亡を左右するという危機感からエニグマ採用を決定した。

エニグマの暗号方式は多表式換字式暗号で、「スクランブラー」と呼ばれるアルファベット 26 文字が刻まれた数枚の歯車（ローター）と、プラグボードと呼ばれる単文字変換を行う仕組みの組み合わせが「鍵」になる。まず、スクランブラーをセットした上で、平文をキーボードで打つとスクランブラーを通じて暗号化された文字がランプボードに表示される。スクランブラーは 1 文字打つごとに目盛りがひとつ回転することによって、1 文字ごとに異なる鍵を使って暗号化することになる。

ドイツ軍はエニグマ採用後もその改良を続け、5 枚あるローターの中から 3 枚を選んでスクランブラーを構成したり、当初 3 枚であったローターを最大 5 枚まで設置可能にしたりするなどの手を加えて、世界で最強の暗号機と言われるまでになった。

7．現代の暗号　～　コンピュータ・インターネット時代の暗号

第二次世界大戦以降暗号の作成と解読は機械からコンピュータに移り、コンピュー タの急速な発展とインターネットの普及によって暗号は軍事用途だけでなく、企業間の商取引など民間用途での必要性が高まってきた。現代の暗号技術を支える柱は主に下記の 3 つのである

（1）ハッシュ関数

ハッシュ関数は情報の信憑性のチェックに用いられる。

送信側　送りたい情報からハッシュ値を求める。
　　送りたい情報とハッシュ値の両方を相手に送る

受信側　送られてきた情報からハッシュ値を求める。
　　このハッシュ値と送られてきたハッシュ値を比較する。
　　改竄が行われていればハッシュ値が一致しない。

今回の特集は暗号技術がテーマです。　　4c03f263557・・・・・・・8ab31
今回の特集は暗号技術がテーマですよ。　　e8fd7193452・・・・・・・a452e

・ハッシュ値は１文字変わっただけでも大きく変化する。
・メッセージの長さに関係なくハッシュ値は長さが一定（１６０ビット）
・ハッシュ値から元の情報が推定できない。（一方向の関数）

（2）共通鍵暗号

共通鍵暗号は暗号化する鍵と復号する鍵が同じ暗号で、その代表的なものは DES 暗号である。
1973 年、米国商務省標準局（NIST）は米国政府が標準利用する暗号方式を公募した。
ＩＢM社がルシファーという暗号システムを提案しそれを国家安全保障局が改良を施して完成させた。
DES 暗号の仕組みは平文のデータを 64 ビット長のブロックに分割し、各ブロックを 56 ビット長の鍵で排他的論理和の計算を行って暗号化する。
現在は DES を更に進化させた AES が使われている。

（3）公開鍵暗号

・ディフィー・ヘルマン・マークルの 3 人は、ネットワークコンピュー タ時代を予想して、共通鍵の問題を解決することに取り組み、1976 年全米コンピュータ会議において、非対称な鍵（公開鍵、秘密鍵）を用いれば事前に鍵を配送することなく暗号化通信ができる「公開鍵暗号方式」 を発表した。これは、暗号化するための鍵を公開鍵として誰でも入手できるようにし、復号のためには 本人しか知らない秘密鍵を使うというものである。
・ディフィー・ヘルマン・マークルの提唱した公開鍵のアイデアを実現する数学的手法は、マサチューセッツ工科大学の研究者、・リベスト・シャミア・アドルマンの 3 人によって開発された。この公開鍵暗号は開発者 3 人の頭文字を取って「RSA 暗号」 と名付けられた。RSA 暗号方式は「素数」による素因数分解を用いている。（素数：2，3，5，7，11・・・のように 1 と自分自身以外では割り切れない数）
素因数分解とは、以下のようにある数を素数に分解することである。

95=5×19
851=23×37
176653=241×733
9831779=X×Y

これを公開鍵暗号方式に用いる場合、イコールの左側の数字（N）と右側の二つの数字から、数学的処理によりD、Eという二つの数字を作り、左側の数字とDを公開鍵とし、Eを秘密鍵として厳重に保管する。情報の受け手はNとDを公開する。送り手はNとDを用いて平文を暗号化して送る。受け手はEの秘密鍵を用いて復号する。
もし左側の素数が途方もなく大きい数であれば、素因数分解によってイコールの右側に使われている素数

を現実的な時間内に解読するのは困難であり、公開鍵から秘密鍵を解読するのは事実上不可能である。
左側の数字（N）は当初 1024 ビット（10 進数で 309 桁）であったがコンピュータの性能が上がり解読の危険性が出てきたため、2014 年以降は 2048 ビット（10 進数で 617 桁）が使われている。

現在広く使われているセキュリティプロトコルＳＳＬはハッシュ、共通鍵暗号、公開鍵暗号の全てを組み合わせて使用している。（ＳＳＬは米ネットスケープ社が開発した技術である。）
その後インターネット技術の標準化団体であるＩＥＴＦがＳＳＬを基にしたＴＬＳを標準仕様に採用した。ＴＬＳのことを単にＳＳＬと表記したりＳＳＬ／ＴＬＳと併記したりする。

我々の情報を護るには

パスワードについて

通常はユーザ ID と対にして用いる。あらかじめ登録されているそのユーザ ID のパスワードと、操作者によって入力されたパスワードが一致していることによって、操作者がそのユーザ ID の使用者本人であると認識する。
パスワードのうちで、数字のみで構成される文字列を**暗証番号**、ＰＩＮ（Personal Identification Number）という。金融機関のＡＴＭや携帯電話の本人確認で利用される。

２０１８年４月１７日の朝日新聞の記事

タイトル：**パスワード「定期変更は不要」**

セキュリティー対策を紹介する総務省の「国民のための情報セキュリティーサイト」で３月、「定期的にパスワードを変更しましょう」という文言が削除された。
日本のセキュリティー対策の司令塔である「内閣サイバーセキュリティセンター」が２０１６年末に定期的変更は不要と呼びかけたことを受け、総務省でも表記を改めたという。
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

この理由は、利用者にパスワードの変更を求めても簡単な文字列になりがちで、破られやすい傾向が出てきたためだという。（記号１文字を削除したり a を A に置き換えたりする程度）
いままでは
パスワードを定期的に変更→誕生日や名前など類推されやすい文字、短い文字列、使い回しなどで
逆効果
新しい見解は→定期的な変更は不要。守るべき事は

- 英数字を組み合わせて複雑にする。
- １０桁以上の長さにする。
- 使い回しをしない。

２０１７年の危険なパスワードランキング（米スプラッシュデータ社まとめ）

１位	12345	６位	123456789
２位	password	７位	letmein
３位	12345678	８位	1234567
４位	qwerty	９位	football
５位	12345	１０位	iloveyou

パスワードの強度チェッカー
https://www.benricho.org/password_meter/

参考文献
暗号の科学　熊谷直樹著　すばる舎
すべてわかるセキュリティー大全　2017　日経ＢＰ社
朝日新聞　2018 年 4 月 17 日朝刊
ＵＲＬ　簡単にわかる暗号の歴史
https://www.digicert.co.jp/welcome/pdf/wp_encryption_history.pdf#search=%27%E6%9A%97%E5%8F%B7%E3%81%AE%E6%AD%B4%E5%8F%B2%27

以　上