コンピュータ・セキュリティの話題

技術士（情報工学）
丑田俊二
ushida@jp.ibm.com

この連載も開始後7回目を迎えました。今号でも授業中に生徒のみなさんの興味を引くような話題を取り上げてみました。コンピュータ・セキュリティの重要性はご存知ですね。今やコンピュータには欠かせない暗号技術，そして最近関心が高まってきた認証技術の話題です。これらの技術は，テロリストの出入国や活動を防ぐ対策としても注目され始めてきました。暗号技術については，古代に使われたものから現代の技術までを紹介し，認証技術については，現在研究が進んでいるバイオメトリクス認証を紹介します。

1．暗号技術

暗号は正当な受信者だけが理解できるように，メッセージを暗号化する技術です。不当な受信者がメッセージを盗み見しても，内容を理解できないようにするのが目的です。例えば戦争中に，通信や命令の内容を敵に知られずに味方に伝えるためや，宝の隠し場所などを一部の人だけしか分からないようにするために利用されてきました。

昔からよく使われている合言葉は，暗号ではなくその文自体が意味を持っている「隠語文」に相当します。太平洋戦争開始時（1941年）・日本海軍の真珠湾攻撃命令として有名な「ニイタカヤマノボレ1208」は，「12月8日0時以降，戦闘状態に入る。各部隊は予定のごとく行動せよ」という意味で使われました。映画の題名にも表れた「トラトラトラ」は「われ奇襲に成功せり」を意味する隠語文でした。

これに対して，野球で使われるサインは暗号の一種です。昔は，グー（直球）・チョキ（カーブ）・パー（シュート）の3種類だけの極めて単純な暗号でした。最近は作戦も多様になっており，複雑なブロックサインや，乱数票を使った暗号に変わりました。ブロックサインは，身体などのいろんな部分を次から次に触っていくもので，鍵（キー）になる部分を決めてその次に触った部分が実行というパターンが多くなっています。例えば，頭を盗塁実行と決めておいて，鍵を胸とするならば，いろんな部分を触り相手をかく乱しながら，「胸」→「頭」と続いたら盗塁のサインということになります。

2．シーザー暗号

よく知られた暗号として，2000年以上前にローマで生まれたシーザー暗号（Caesar cipher）があります。古代ローマの英雄，ジュリアス・シーザーが利用したと言われています。シーザー暗号は，平文（ひらぶん）（もとの文）の各文字をそれぞれ他の文字に1対1に対応させて暗号文とする，「換字式暗号」でした。

単純な暗号ですが，現代の暗号でも基本となっている，2つの重要な要素が含まれていました。規則（アルゴリズム）と鍵（キー）です。シーザー暗号のアルゴリズムは，アルファベットのある特定の文字を，それよりも特定の数だけ後ろにある文字と置き換える手順です。鍵は何文字ずらすかという数です。シーザーが実際に用いた鍵は「3」でした。これによれば，“ABC”という平文を暗号化すると，“DEF”となり，「3」という鍵を知らなければ復号できません。しかし，鍵の種類は26種類しかありませんので，暗号アルゴリズムが分かれば，鍵を破るのは簡単です。今では，シーザー暗号を解読するためのコマンドcaesarが装備されているOSもあります。

今も時々テレビで再放映される，映画『2001年宇宙の旅（1968年，スタンリー・キューブリック監督）』は，人類の夜明けから月面そして木星への旅を通し，知的生命体の接触を描くSF映画の傑作でした。木星探査船ディスカバリー号に搭載された「ヒューリスティカリィ・プログラムド・アルゴリズミック・コンピュータ　HAL 9000」の人工知能が，この映画の一方の主役として登場します。やがてHAL 9000は人間の愚かさに気づき反乱をおこします。ところで「HAL」は「IBM」を1文字だけずらした，極めて単純な換字暗号でした。

シーザー暗号では，すべての文字を同じ数だけ

ずらしていましたが，1文字ごとにずらす数を変えれば，より複雑な暗号が作れることが考えられます。そこで考えられたのが，多表式換字暗号・ビジネル暗号（Vegenere Ciphers）です。アルファベットをシフトして並べた25×25のマトリックスの縦横に，平文と鍵語を対応させ，交差する地点の文字に換字します。この暗号は，鍵によって全く異なった暗号文ができるため，万一換字表が漏れても，鍵を知らなければ解読が困難です。

3．古代の暗号

シーザー暗号以外にも，古代には次のような暗号が使われていました。

ヒエログリフ・紀元前19世紀頃の古代エジプト

最古の暗号は，動植物や身の回りの物をかたどったヒエログリフ（象形文字）だと言われています。この時代の石碑の一つから，標準以外のヒエログリフを用いたものが発見されており，歴史に残る最古の暗号文とされています。

アトバシュ・紀元前5世紀頃の旧約聖書

旧約聖書には，バビロンという地名が，ヘブライ語の換字式暗号アトバシュで記載されていると言われています。この暗号は，文字に番号をつけて，最初からの順番と末尾からの順番を入れ替えて作ります。アルファベット26文字を暗号にする場合には，AをZに，BをYに，というように順番を置き替えて作ります。

スキュタレー・紀元前5世紀頃のギリシャ

都市国家スパルタでは，一定の太さの棒（スキュタレー）と革ひもを用いた暗号が使われていました。革ひもに書かれている言葉はでたらめですが，この棒に革ひもを巻きつけていくと，意味のある言葉が現れます。

ポリュビオアス・紀元前2世紀頃のギリシャ

政治家・軍人・歴史家ポリュビオアスは，文字を数字に変換する暗号を発明しました。5×5＝25のマス目にアルファベットを記入した表を使って，1つのアルファベットを2桁の数字で表す換字式暗号です。暗号に乱数を加えることを可能にする画期的な発明でした。

4．暗号とネットワーク

21世紀の情報化社会では，経済や産業・学術・日常生活において，地球規模の巨大なネットワークを介しての取引や情報のやりとりがすでに広がっています。例えば，一般消費者がパソコンからネットワーク上のバーチャルモール（仮想商店街）で商品を購入し，クレジットカードで支払いを済ませる（インターネットショッピング），企業の資材調達は電子入札により世界中から提案書を求め，取引き・決済する（電子入札），などです。その他，個人情報，企業間の機密情報，秘密のメールなど，無関係の第三者に知られては困る情報が，ネットワークの中を所狭しと飛び交っており，暗号の必要性が増しています。ネットワークの中にはクラッカー（以前はハッカーと呼ばれていた）が，虎視眈々と侵入を狙っています。アメリカ国防省や日本の官公庁のシステムにハッカーが侵入し，機密データが盗まれたなどという話も珍しくなくなりました。

5．インターネットショッピングでの危険

今や普通になったインターネットショッピングを考えてみましょう。ネットワークの中では，4つの危険（リスク）が発生します。

（1）なりすまし
（2）否認
（3）データ改ざん
（4）カード番号などの盗聴

これらのリスクを防止するためには，本人確認，クレジットカード番号や銀行の口座番号の盗聴および悪用の防止，オンライン決済における安全性の確保が重要であり，何よりも安全・確実に情報を送る技術が必須になっています。このために使われるのが暗号で，数学とコンピュータを融合化させた重要な技術です。

6．軍隊で使われた暗号

ナポレオン時代，フランス軍の砲兵士官だったバルビエ大尉は，立体の暗号文字を発明しました。暗闇の中で解読でき，かつ秘密保持できる文字として開発されました。すべて凸部の点よりできており，兵士が闇夜の中で命令を読み，報告を書くことができるように考案された，触覚で読み取る軍事用の文字でした。バルビエはこの夜間文字の実用性を確認するために，パリ盲学校の生徒に実験を依頼しました。目の見えない生徒が読めれば夜間に兵士たちも使用できるいうわけです。

これがきっかけとなり，バルビエはこれを盲人用文字としても活用するため，様々な改良を加えます。1825年には，パリ訓盲院教官ルイ・ブライユが，現存の6点式による点字を考案しました。

6点点字は縦3点・横2点の6つの点の組み合わせで，表面の凹凸による指先の感触で文字を読み取ることができます。

日本には1880年頃伝わりました。東京盲唖学校長・小西信八は同校教員・石川倉次に，6点式を日本語に適用する研究を命じ，石川はブライユ点字の列点法を大きく変更する事により，6点で日本語のかな文字を表すことに成功します。

ナポレオン軍で発明された暗号文字が，今では点字として発展し，視覚障害者のみなさんのお役に立っているわけです。

7．秘密鍵暗号

軍隊では以前から秘密鍵暗号と呼ばれる暗号を使っていました。秘密鍵暗号とは，情報の発信者と受け手が共通の鍵（乱数表）を持ち，第三者には分からないようにするものです。暗号化（平文をスクランブルして判読不能にし，暗号文に変換する）と，復号（暗号文を元の状態の平文に戻す）には，同じ鍵を使います。

1941年12月，日本から暗号電報が送られているにもかかわらず，大使館での復号が遅れ，アメリカ政府に宣戦布告できないまま太平洋戦争が開始されてしまうという，重大な事件が起きました。日本政府は攻撃前日から，ワシントンの日本大使館宛に15通もの長文電報を送信していました。この日大使館員は，夜に催された同僚の送別会のため，夕方からほとんどが不在になっていました。夜になって，政府から開戦をアメリカに通告する最後の1通が届けられた時には誰も残っていませんでした。暗号電報最後の1通を，二日酔いで出勤してきた大使館員が手にしたのは，次の日の朝も，かなり遅い時間になってからだったと言われています。館員が急いで復号し，さらにそれを英語に翻訳してタイプしている間も刻々と時間が過ぎています。タイプが終り日本大使が車を飛ばして，宣戦布告書をアメリカ政府に渡したのは，なんと真珠湾攻撃の55分後になってからでした。このため日本は「リメンバー・パールハーバー」とアメリカ世論の怒りを買ってしまい，やがて4年間も続く泥沼の戦争に突入することになりました。

そればかりか今でも，「真珠湾攻撃」と「2001年ニューヨーク貿易センタービル・テロ事件」を同列に置かれ，未だに日本は大変な不利益をこうむっています。

この後のソロモン海戦，ミッドウエィ海戦など，第二次世界大戦は秘密鍵暗号の解読合戦でした。秘密鍵は当事者間で同じ鍵を使わなければ，暗号化・復号できません。このため秘密鍵が簡単に盗まれやすいという欠点があります。例え盗まれなくとも，単純な秘密鍵は，コンピュータの処理速度が速くなれば，いずれは解読されます。

8．数学理論と公開鍵暗号

秘密鍵の欠点を補うために考え出されたのが，現在の暗号化技術の主流「公開鍵暗号」です。1977年マサチューセッツ工科大学の，リベスト（Rivest），シャミア（Shamir），アドルマン（Adleman）によって実用化され，3名の頭文字を取ってRSA暗号とも呼ばれています。

これは一般に公開する公開鍵と，厳重に保管する秘密鍵を組み合わせる方式です。つまり暗号化時と復号時に異なるキーを使う暗号アルゴリズムです。

公開鍵暗号は素因数分解の原理を利用し，自由に選んだ異なる2つの素数を掛けた数を基準にして鍵を生成します。実際には2つの数の素因数分解が困難なくらい大きな素数を掛け合わせて暗号としています。現在のところまだ巨大な2つの素数を掛け合わせた数を素因数分解する効率的な方法（アルゴリズム）が見つかっていません。

公開鍵暗号を始めとする暗号は，全て数学理論に基づいて「強度計算（解読にどれくらいの時間がかかるかということ）」されています。どんな暗号でも人間が考えて作り上げた以上絶対安全ということはありません。しかし公開鍵暗号は，コンピュータの処理能力と，現在知られているアルゴリズムで解読するにはあまりに時間がかかり過ぎるため，事実上安全であるということになっています。

公開鍵暗号の元になった素数の原理は，数学の巨人と言われたオイラー（Leonhard Euler スイス 1707－1783）が1761年に発見し，オイラー関数という名で知られています。しかし和算家・久留島義太（？－1757）は，オイラーより先にオイラー関数の公式を発見していたという記録が残されています。久留島は和算家のほかに，詰め将棋作家としても有名で，4枚の桂馬を駆使して美しく詰み上げる「四桂詰め」は今でも傑作として残されています。

9．21世紀の暗号理論

しかしコンピューターの進歩で，素因数分解の難しさも力でねじ伏せられかねない状況になり，現在では，2の500乗程度（10の150乗。江戸時代の数の単位，無量大数はせいぜい10の71乗）の巨大な2つの素数の積を用いなければ安心出来ない状況となっています。最近では離散対数問題を利用して，楕円曲線を用いた楕円暗号が実用化されかかっています。さらに次世代以降，超楕円暗号など，さらに進んだ数学理論にもとづく暗号システムが出現するでしょう。

10．あなたを証明する技術

浦島太郎のように，あなたを知っている人が回りに誰もいなくなりました。あなたは自分であることをどうやって証明するでしょうか。証明書（身分証明書・健康保険証・パスポート），IDカード（入館証）などがあれば有効です。「預金通帳と印鑑」，「キャッシュカードと暗証番号」，「クレジットカードとサイン」の組み合わせも役に立ちます。朝パソコンの電源を入れると「PC，ネットワーク，OS，グループウェア，イントラネット」など，次々とパスワードをキーインします。これだけ多いパスワード，机の隅にでも刻み込んでおかなければ覚えてはいられません。身分証明書や印鑑，パスワードなどは本人であることを証明し，あなたを知っている人が誰もいない状況でも，正当な権利を主張しサービスを受けることができます。この仕組みを「認証」と言います。認証には「持ち物による認証」と「知識による認証」があります。大人になって，店頭で買い物しクレジットカードで支払うとします。お客は「持ち物（クレジットカード）」と「知識（カード面記載と同じサイン）」により本人である確認を受けます。しかし「持ち物や知識」を「忘れる，紛失する，盗難に遭う，偽造される」と，とたんに大変な状況に陥いります。海外でパスポートを紛失すれば，すぐ大使館・領事館に駆け込まなければなりません。続いて明日の帰国フライト（飛行機）もキャンセルとなります。

一方インターネットショッピングでは証明書もパスワードさえも不要です。「カード番号と有効期限」だけキーインすれば買い物できます（もちろん未成年は保護者の許可が必要です）。しかしデータがネットワークを通過している時に，カード番号と有効期限を盗み見されたらどうなるでしょうか。

これらの危険を未然に防止するため，公開鍵暗号，ディジタル署名（文書の作成者であることを証明する電子署名），認証局（電子証明書を発行する第三者機関）などの認証技術が発達してきました。

11．スキミングの被害

最近，スキミングによる被害が急増してきました。スキミングとは，カード所有者がほんの少しの時間カードから目を離している間に，小型カードリーダーを使って，直接カード情報を読み取る方法です。読み取ったカード情報を，別の磁気カードに記録すれば，まったく同じキャッシュカードやクレジットカードになります。もっと悪質で組織的な方法もあります。カードそのものを盗まれているわけではないので，カードを所有している本人は気がつきません。キャッシュカードの場合，数日経過して預金残高が大幅に減っているのに気が付きます。実際には，数千万円の被害に合ったケースも報告されています。これは証明書を簡単に偽造された例です。

12．バイオメトリクス認証

情報社会がさらに進展すると，本人認証はますます重要になり，誰もが安全に簡単に使える認証システムが求められます。認証には「持ち物・知識」以外にも最近「身体的特徴による認証」が注目されています。「バイオメトリクス（生物測定学）」とは，生物の変異の状態を数学的・統計的に研究する学問です。研究が進んでいる「バイオメトリクス認証（生体認証）」は，人間の身体的特徴や特性を利用した認証技術で，これらの持つ「普遍性・唯一性・永続性」を根拠としています。具体的には「指紋，手のひら，顔面，声・声紋など」によって本人確認を行ないます。身体的特徴は長期間にわたって変化しにくく，類似する第三者が存在しないか極めて少ないという利点があります。

従来のパスワード認証方式は「パスワード忘れ，パスワード盗難」という欠点がありました。バイオメトリクス認証では，事前に本人固有の情報を計測しシステムに登録します。取引やサービスを受けるたびに，登録してあるデータと一致するかを確認し，本人の真正性を認証します。

13．バイオメトリクス認証の問題点

昔から拇印は手軽で優れた本人確認手段に使われてきました。しかし指紋認証となると，犯罪者の捜査を思わせ抵抗感があります。手のひら認証は，やけどや損傷があると判定しにくくなります。顔面認証は髪型や髭など，声や声紋による認証は声の調子により影響されやすい傾向があります。認証には誤認識がつきものです。正当な利用者である本人と認識されないと，間違いなくその場でクレームが発生します。しかし商店では本人確認できない以上，取引は成立しません。他人を正当な本人と認識する誤認はさらに問題があります。知らないうちに預金残高が減っていけば，認証システムの信用にかかわります。バイオメトリクス認証は，誤認識率が極めて低くならなければ実用化は難しくなります。高速処理装置や大量の記憶装置が必要でコスト高になる欠点もあります。

14．実用化へ向けて

今後はさらに精度の高い認証方法が求められます。現在では「目の虹彩（瞳の模様）や網膜」や，「個人のDNA情報を秘密鍵に埋め込み，認証やディジタルによる認証署名を行なう方式」も研究されています。虹彩は2歳程度で形成され，生涯変わらないとされています。

バイオメトリクス認証は，かつては軍事施設や原子力発電所など，特殊な場所でしか使われていませんでした。しかしカードや暗証番号などに比べ，盗難や偽造の心配も少ないことから，最近では，携帯電話やパソコンなど身近な生活場面でも使われつつあります。指紋認証機能を搭載したモバイル・ノートパソコンや，分譲マンションの共同玄関への虹彩認証装置の導入などが一例です。

個人情報の保護が重要視される金融機関でも，高度なセキュリティを必要としており，バイオメトリクス認証技術の導入が進んでいます。スルガ銀行（本店・沼津市）では，2004年7月から「てのひら静脈認証」を使い，国内金融機関では初めて，キャッシュカードが不要な「バイオセキュリティ預金」を始めました。東京三菱銀行も，2004年秋に導入する予定です。一方，さまざまな認証技術が混在してくると，利用者が混乱する恐れもあるため注意が必要です。

15．ICパスポートの実験

これらの技術は，テロリストの出入国を防ぐ対策としても注目されています。2001年のアメリカ同時多発テロの後，欧米を中心に導入を検討する動きが広がっています。アメリカはすでに，顔写真付きICチップ・パスポートの導入を各国に求め，入国する外国人の指紋採取や顔写真登録を始めています。

日本でもこの動きに呼応し，2003年1月より成田空港にて「顔と虹彩による認証」を使用した「e－チェックインの実証実験」が開始されました。この実験は出国時の搭乗手続き簡素化を目的とした「e－airportプロジェクト（国土交通省推進）」の一環です。

さらに2005年1月からは，パスポートに顔写真や指紋，虹彩を記録して個人認証に活用する実験を開始します。顔写真を入力したICチップ・パスポートに，指紋や虹彩を含めることについては，個人情報保護との関連で慎重論も根強く残っています。まず法務省を中心とした政府の職員が実験に参加し，実効性を確認するとのことです。実験では，民間企業などで導入されている読み取り・照合装置をパスポート用に改良し，成田空港に数台を設置します。ICチップ・パスポートにより，出入国管理の本人確認にどれだけ有効かを確かめ，顔写真照合システムのノウハウ作りにも生かす方針です。

読み取り機器が悪用されると，かばんやポケットに入れたICチップ・パスポートから個人情報が盗み取られる危険性もあります。このため，実用化の際は暗号化などの防御策も課題になります。

16．まとめ

『将来はお年寄りを認識すると，自動的に表示文字を大きくするパソコンや，暑がっている人がいると室温を下げるエアコンなどの製品が市場に出回るかもしれません。（オムロン社談）』21世紀はまだ始まったばかりです。ITを基礎とした科学技術の発展は限りなく進んでいます。情報を勉強する高校生のみなさんの，柔軟なアイデアをお待ちしています。

参考文献

[1] 丑田俊二「数学が思わず好きになってしまう本」（中経出版，2002年）

[2] 暗号の歴史
http://www.mitsubishielectric.co.jp/security/info/misty/index_b.html

[3] 産経新聞　2004年8月27日朝刊