話題の
PRODUCT
プロダクト
暗号技術

ビジネスの世界で注目を集め始めた暗号技術

安全保障上の壁を乗り越えられるか

アメリカの安全保障・暗号政策を統括するNSA（National Security Agency：国家安全保障局）のホームページ。冷戦時代にはその存在すら秘密のベールに包まれていたが、現在では暗号博物館を設置し一般公開している（写真左）。日本では通商産業省が音頭をとり、ECに積極的に取り組んでいる。一般消費者を対象としたECOMに100億円、企業間取引を扱うEDIに200億円以上が投入されているという（写真右）。

ゴア米副大統領の情報スーパーハイウェイ計画に触発され
インターネットが爆発的普及したことで、
暗号技術の商用利用と暗号ビジネスが、がぜん注目を集める結果となった。
各国でネットワーク社会に対応したECの実験が始まっているが、
実用化段階でどの方式がデファクトスタンダードの地位を獲得しているのだろうか。

10

ネットワーク社会が必要とする暗号技術

暗号ー推理小説やCIA・KGBといった諜報機関が暗躍する映画の世界ならいざ知らず、実生活でお目にかかることは滅多にないものだった。しかしここ数年、ビジネスの分野でこの暗号が話題を集めている。そのきっかけは、やはりインターネットの爆発的普及だ。

1969年に軍事目的で開発の始まったARPAnet（Advanced Research Projects Agency Network）を引き継ぐ形で、1983年に全米科学財団が開設したNFSnet（National Science Foundation Network）が基幹ネットワークとなり、1991年にCIX（Commercial Internet Exchange Association）が設立されたことで、インターネットの商用利用が本格化した。NFSnetは、大学や政府・企業の研究機関を結ぶ学術利用が中心だったことから、セキュリティ上、さまざまな課題を抱えていた。そのシステムをそのまま商用利用に開放したため、「インターネットは無法地帯」と形容されるほど、インターネットのインフラは、セキュリティの面で脆弱なものとなっている。

アメリカは国土が広く、物流体制を整えたり、店舗網を整備することが難しい側面がある。このため通信販売が発達した。インターネットを使った商品の受発注は、このアメリカの商習慣にマッチしていた。またアメリカではクレジットカードによる決済がもっとも一般的な方法となっている。つまりインターネット上で商取引の情報や、決済に必要なクレジットカード番号といったデータがやり取りされることになる。こうした経済行為に対して悪意ある攻撃が行われた場合、インターネットはまったく無防備なのだ。そこで登場してきたのが暗号技術である。

シーザーも利用した暗号技術

ここで暗号の基本的な仕組みを考えてみよう。暗号とは、平文と呼ばれる元の文章やデータを、見ただけではわからない形に変形してしまうことだ。しかし変形したものが元に戻せなくては意味がない。この変形された暗号文を元に戻すことを復号という。

最も古い暗号方式の一つが、古代スパルタで使われていた転置式暗号といわれている。これは同じサイズの細い指揮棒を2本用意し、自分と伝えたい相手が1本ずつ持っておく。通信の必要が生じたら、細長いパピルス（当時の紙）を指揮棒に巻き付け、巻き付けた方向と直角に文字を書き込んでからパピルスをはずし、伝令に手渡して相手に届けてもらうというものだった。一巻きで3文字書ける太さの指揮棒を使用するとお互いに取り決めておけば、通信文を受け取ったものは、パピルスを指揮棒に巻き付けることで、元の文章に復号することができるわけだ。

また推理小説の謎解きなどに登場する、古代ローマ帝国のジュリアス・シーザーが用いたといわれるシーザー暗号もよく知られている。たとえば次のような文章を、アルファベットを3つ後ろの文字に置換して暗号化してみよう。

平　文　All roads lead to Rome

暗号文　DOO URDVOHDG WR URPH

この方法は、換字式暗号と呼ばれる。

暗号文を複号化する場合に必要な情報は、暗号化するアルゴリズムと鍵である。上の暗号化では、換字方式というアルゴリズムを使っていて、鍵はアルファベットを後ろに3つずらすということになる。これを数式で表すと、

$y = x + 3 \bmod 26$

となる。実際には、シーザー暗号では換字表と呼ばれる変換表をお互いが持っていて、暗号文を解読していた。この方法は非常に簡単だが、それだけに第三者に解読される危険性も高い。そこで鍵の3を固定せず、しょっちゅう変更することによってよりセキュリティを高めることができる。またパラメーターを2つにして、

$y = ax + b \bmod 26$

という暗号式を使えば、より解読しにくい暗号文が作成できる。この関数をアフィン（affine）関数と呼ぶことから、この暗号方式をアフィン暗号と呼ぶ。シーザー暗号はアフィン暗号のパラメーターa＝1、b＝3の事例ということになる。上記の文章をa＝7、b＝3のアフィン関数で暗号化すると、

DCC SXDYZ CFDY GX SXJF

となる。

革命をもたらした公開鍵暗号

暗号を利用するのは、ある特定の相手だけに通信文を伝えることが目的であるから、伝えたい相手に、どういうアルゴリズムで暗号化されており鍵はなにかが知らされている必要がある。スパイが利用する暗号なら、アルゴリズムも鍵も秘密にしておいたほうが都合がいいだろうが、ビジネスの世界ではそういうわけにはいかない。どういうアルゴリズムを使っているかだけは公開して、鍵のみを秘密にする暗号を秘密鍵暗号と呼ぶ。この場合、鍵の管理を相当厳重に行う必要がある。また先のシーザー暗号では、暗号化するときも復号化するときも、同じ3という鍵を使用した。こういう暗号形式を共通鍵暗号と呼ぶ。

共通鍵暗号では、相手に鍵をどのようにして伝えるかが常に問題となる。

1976年、DiffeとHellmanによって暗号技術の歴史上画期的な理論が発表された。公開鍵暗号である。公開鍵暗号では、鍵を暗号化する公開鍵と復号化用の秘密鍵を別々に用意する。暗号文は、暗号化に使われた鍵では、復号化できない仕組みになっている。

ここでX氏からY氏に対して、公開鍵暗号を使って通信文

11

世界の主な暗号

	開発者	鍵長(ビット)	アルゴリズム	商用実績
DES	アメリカ政府	56	公開	有
SkipJack	アメリカ政府	80	非公開	有
RC2	RSADSI	128ほか	非公開	有
RC4	RSADSI	128ほか	非公開	有
FEAL-N	NTT	64	公開	有
MULTI2	日立製作所	320	公開	有
MYSTY	三菱電機	128	公開	有
ENCLIP	NEC	非公開	非公開	有
IDEA	Ascom Tech	128	非公開	不明
B-CHIPER	BT	64	非公開	不明

を送信する場合を考えてみよう。Y氏はX氏に対してあらかじめ公開鍵を平文で送っておく。X氏はその公開鍵を使って暗号文を作成し、Y氏に送る。Y氏は自分だけしか知らない秘密鍵を使って暗号文を復号し通信の内容を読むことができる。ここで第三者であるZ氏が暗号文を手に入れても、Y氏が公開している鍵では復号できないため通信の秘密は守られる。

公開鍵暗号が画期的だったのは、鍵のやり取りが安全に行えるだけではない。再びX氏とY氏の間で通信文をやり取りする場合を考えてみる。Y氏は、彼しか知らない秘密鍵を使って平文を暗号化し、X氏に送ったとする。X氏はY氏が公開している公開鍵で暗号文を復号することができる。このとき、この暗号文を作成できるのは世界中にY氏しかいないことになる。

事前にX氏とY氏の間で、秘密鍵を使って暗号文を作り送信すれば契約に合意した印だと取り決めておけば、この暗号文は契約書類に署名捺印したのと同じ効力を持たせることが可能だ。これが電子捺印技術（digital signature）の原理である。

たとえば第三者であるZ氏がこの暗号文を横取りし、Y氏の公開鍵で復号して内容を読むことはできる。そこでこっそり内容を改ざんして、再び公開鍵で暗号化しX氏に送ったとしよう。しかしこの暗号文はY氏の公開鍵では復号することはできないため、X氏はこの暗号文を送ったのはY氏ではないと判断することができる。

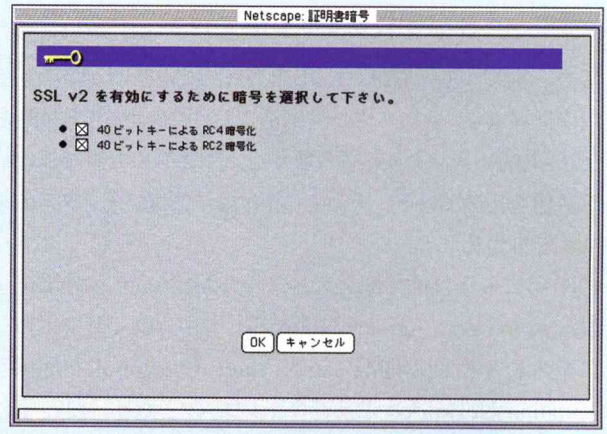
このように、公開鍵暗号を利用すれば、通信の守秘性を高めるだけでなく、電子捺印や相手の認証といった利用も容易に行える。

解読技術開発とイタチゴッコを繰り返す暗号開発

暗号技術に革命をもたらした公開鍵暗号だが、一つ欠点がある。秘密鍵暗号に比べて計算が複雑で時間がかかることだ。また暗号はいずれ解読される宿命をもっている。そのためより解読が難しい暗号方式が次々に開発されている。たとえば現在、公開鍵暗号といえばRSAが一般的だが、安全性を高めるため鍵のビット長がどんどん長くなっている。またRSAは整数の因数分解の困難性を基礎に成り立つ暗号方式だが、部分集合和問題の難しさに基礎を置いたMerkle-Hellmanナップサック、代数的符号理論に基づいたMcEliece、従来の公開鍵暗号系を修正した楕円曲線暗号など、現在の暗号理論は、数学の先端理論を基礎にしたものばかりだ。

もう一つ暗号技術が抱える問題として、軍事的な側面も見逃せない。アメリカでは従来、暗号は軍事技術として厳しい輸出規制が取られていた。1996年末に暗号は武器指定からはずされ、輸出に関しても国務省から商務省に管轄が移されているが、ビット長など依然厳しい制限が設けられている。日本や欧米各国でもなんらかの輸出規制が行われている。

現在、各国でエレクトロニック・コマース（electronic

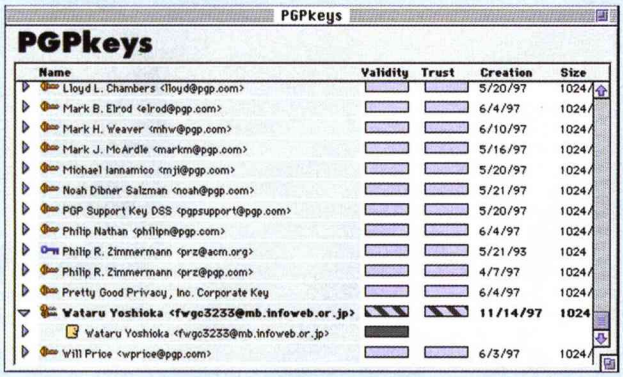


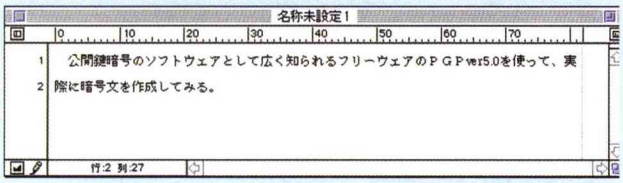
デファクトスタンダードとなったRSA

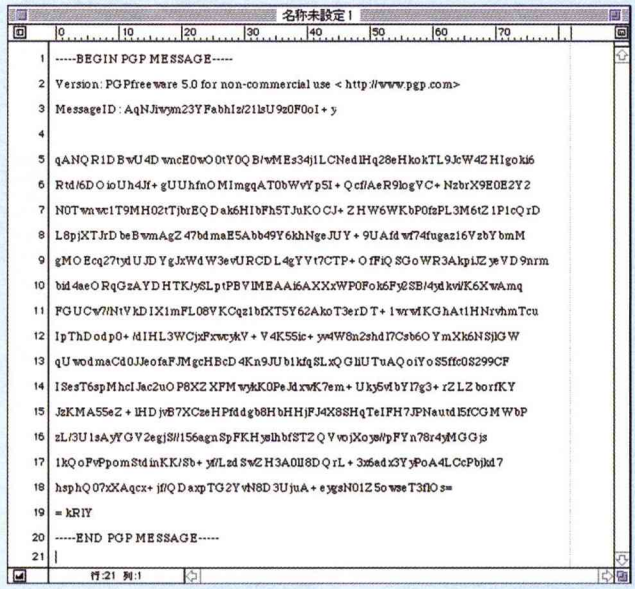
1977年、MITのRivest、Shamir、Adlemanという3人の教授が公開鍵暗号理論を使った暗号システムを開発した。その暗号は3人の頭文字を取ってRSAと名づけられた。3人は1982年にRSAデータセキュリティ社（RSADSI）を設立、ベンチャービジネスに進出した。設立後数年は赤字が続いたが、経営手腕を持つ社長を迎え、さらに時代が暗号ソフトを求めたことで急成長を遂げた。そのきっかけとなったのがNetscape NavigatorやInternet ExplorerといったWWWブラウザソフトにRSAの暗号ソフトが組み込まれたことだ。その後、RSADSIの暗号ソフトはさまざまな通信ネットワーク系のソフトウェアに採用され、会社は急成長を遂げる。

しかし、暗号はいまだにアメリカ政府による輸出規制の対象となっている。そのためNetscape社はアメリカ国内向けと海外向けに2種類のNavigatorを用意せざるをえなかった。違いは使用できる暗号の種類と強度である。たとえば日本仕様のNavigatorでは40ビットキーによるRC4とRC2の2種類の暗合しか使用できない（写真上）。また、RSA暗号の特許はMITが所有しているが、RSADSIとMITとの独占使用契約は2000年で期限切れを迎える。日本をはじめイスラエルなど各国が公開鍵暗号の新方式の開発にしのぎを削っているが、現在のRSA独占状態が大きく変化する可能性も秘めているのだ。

12







暗号文を作成してみる

実際に公開鍵暗号方式を組み込んだ暗号ソフトウェアを使って暗号文を作成してみよう。使用したのはフリーウェアのPGP version 5.0のMacintosh版だ。

PGPをパソコンにインストールし自分のフルネームと電子メールアドレスを入力する。次にパスワードを設定するとPGPkeysに自分の公開鍵と秘密鍵が登録される（図左上）。エディターソフトでPGPを使用可能に設定し図左下のような文章を作成した。これをPGPで暗号化すると図右のような暗号文が作成される。

今回は自分の公開鍵で暗号化したため、自分の秘密鍵で復号することができるが、通常は送信する相手の公開鍵を使って暗号化し、その暗号文を相手に送ることになる。この場合は、暗号化した本人も復号することはできない。相手の秘密鍵を知らないからだ。

PGPというのはPretty Good Privacy（なかなかよいプライバシーとでもいう意味）の略で、開発者はフリーのプログラマーだったPhilip Zimmermann。アメリカ政府が進めていたクリッパー計画という暗号政策に疑問をもったZimmermannは、1991年たった一人でPGPを完成させる。しかしこのソフトウェアはRSAの特許技術を利用していたため販売することはできなかった。しかたなくZimmermannは、友人たちにこのソフトを無料で配布する。そのうちのだれかがPGPをインターネット上に掲載し自由にダウンロード可能にした。PGPは瞬く間に世界中に広まる結果となった。

当時、暗号技術は軍事技術に指定され、国務省により輸出は厳しく制限されていた。Zimmermannは国際武器流通規定という法律に違反した罪で起訴される。輸出が許されていたのは40ビット以下の鍵を使う暗号に限られ、128ビット鍵を使用していたPGPはその規定に抵触するというのだ。Zimmermannは市民のプライバシー保護の象徴的な存在となり、さまざまな支援活動が展開され、PGPもあらゆるぷらっとフォームに移植された。1996年末、Zimmermannは不起訴となり、晴れて自由の身になっている。

現在もPGPはアメリカ国内のみならず世界中で、MS-DOS、Windows、Macintosh、Unixなどで使用されている。Zimmermannはプログラムではなくプログラムソースを印刷し海外に持ち出すことで、暗号の輸出規制をクリアした。欧州でもイギリス、フランスなどは厳しい規制が敷かれているが、ノルウェーなどの北欧では規制がないため、PGPはこうした国に設置されたサーバからダウンロード可能となっている。

参考 • http://www.ifi.uio.no/pgp/download.shtml

commerce：EC）の実証実験が行われている。電子商取引と訳されているが、欧米のECは「市場調査、取引先の選定、商談、契約、商品発注、出荷、請求・支払いといった商取引にかかわるすべての業務を企業間の情報ネットワーク上で処理するシステム」といった少し広い意味で使われている。

従来のグループ企業間や特定業種間での閉ざされたネットワーク上であれば、セキュリティ問題もそれほど大変ではなかった。しかしECのように異業種間やグローバルで行う場合は、暗号や電子捺印システムといったものが不可欠になってくる。公開鍵暗号は、こうしたオープンなネットワーク時代のニーズを満たす基礎技術として注目を集めている。

暗号技術は、どれが優れているかよりどの方式が一般化しているか（デファクトスタンダード）という部分が重要になる。しかし、その方式に欠点や解読方法が見つかると、セキュリティが崩壊してしまう危険性をはらんでいる。

暗号ビジネスの市場規模は、まだ10億円にも満たないといわれている。大企業が進出するには十分成長しているとはいいがたい。新たなベンチャー企業が登場する余地が残されている世界なのだ。

13