安全対策を軽視する情報システムと安全を支える情報セキュリティ技術

森田　光（もりた　ひかる）
神奈川大学 工学部

あらまし

情報システムの安全性とそれを支える情報セキュリティ技術について考えたい。具体的に考察するため、銀行カード・システムを例にとり考えよう。歴史が長いシステムであるため、早くからセキュリティの犯罪が起きていて、現在でもホットな話題になっているからだ。また、インターネットが爆発的に延びている社会にあわせて、変革が求められているのが、この情報システムだからだ。一方、欧米の金融業界や研究サイドでは、安全に対して日本とは異なった見方をしていることを示し、セキュリティという安全を扱う分野であっても、仕様を公けにして、議論すべきであることを示す。

1．情報システムと安全性

1．1　銀行カード事件

1981年に、電電公社職員が北海道銀行顧客の暗証番号を盗み、銀行カード（キャッシュカード）を偽造しATM（自動預金預け払い機）から現金を引き出した。電電公社の専用回線が使われていたので、業務の必要からデータを見る機会が日常的にあったと思われるが、得た情報（口座番号と暗証番号）をもとに現金を盗むのは明らかに違法であり犯罪であった。

事件が公けになってから、法律改正や銀行システムの見直しが行われた。しかし、20年以上たった今でも、銀行カードのシステムはほとんど変わっていないし、ATMと金銭出納を管理する計算機センタ間の通信は、技術ではなく、法律によって守られているのだといわれている。

今やATMは、コンビニや駅に置かれる時代になっている。量販店では、銀行カードで直接買い物ができるデビットカードのシステムが導入されている。また、家からインターネット経由で、銀行に振込依頼や定期切り替えなど、口座を管理できる時代になっている。この様に、多様なサービスを提供する著しい進歩はあったものの、果たしてシステムとして安全にユーザの預金を守ってくれているのか心配になってくる。

今年になって、スキミング犯罪が発覚した。覚えている方も多いであろう。銀行カードと暗証番号を用いるのは20年前の犯罪と同じである。違いと言えば、情報がゴルフ場のロッカーから漏れたことである。暗証番号は、ロッカーを管理するパソコンから読み出され、銀行カードはロッカーの中の原物から複製された。

ロッカーの開閉に4桁の暗証番号が使われていて、ユーザは自由に設定可能だったようだ。人はパスワードを何個も覚えられないから、ロッカーで使う暗証番号がそのまま銀行の暗証番号になるケースが多い。この犯罪は、それを利用し、暗証番号はロッカー管理のパソコンから読み出した。銀行カードは、カードの磁気部分から情報をサッと読む（スキミング）だけで必要な口座番号などが入手できるので、持ち主に気付かれる心配が少なく複製できた。そして、ATMでは、銀行カードの磁気部分だけを使って識別していたことも悪用されたのだ。

この事件をきっかけに、不正に引き出された預金の補償額の議論が法律家の中で行われている。クレジットカードの不正利用の場合、保険会社が全額負担というコンセンサスがあるが、銀行カードにはそういうものが無かったらしい。議論によれば、ユーザである顧客の過失の有無により補償の軽重を加減する意見が大勢を占めているようだ。そして、銀行と顧客で負担の割合が議論されつつある。

銀行カードを落とした場合でも過失があったとされ、補償額が少ないことに驚いたユーザが多かったらしい。結果として、全額補償タイプの銀行口座が売りに出されたり、安全を高めたと言われる「手のひら静脈認証技術」を導入した銀行カード・システムが登場したり、安全を強化した新サービスが盛んに宣伝されるに至っている。

1．2　スキミング対策の議論の問題点

銀行システムはどの様な機能構造で、顧客の責任範囲はどこまでなのか明らかになっていない。議論では、補償額の割合ばかりに注目が集まっていて問題だと思う。

情報は複製可能である。従って、情報が漏れたからと言って、顧客本人からなのか、銀行からなのか本来分からないものである。また、20年前の事件にあった様に、通信からも漏れることがあり、特定することは極めて困難である。どこから漏洩したのか証拠がつかめないのに、その議論がなく、責任範囲を適当に決めようとするのは問題である。

1．3　安全を巡る欧米金融業界の動きと日本

先に、20年以上たっても、銀行カードのシステムはほとんど変わってないし、ATMと金銭出納を管理する計算機センタ間の通信は、技術ではなくて法律に守られているので対策しないまま放置されている。という推測話を紹介した。

その一方で、欧米の某有力銀行が国際標準ISO9564[1]の勧告を受け、2000年の暮れ頃、それまで使用していた暗号を、一夜のうちに一斉に置換えたという。DES[2]の脅威が大きくなったので、T-DES[3]に切り替える必要[1]があったためだ。暗号は、ATMと計算機センタ間の通信を秘密にするために使われていた。つまり、通信からの情報漏洩を無くす目的で暗号が導入されていたのである。

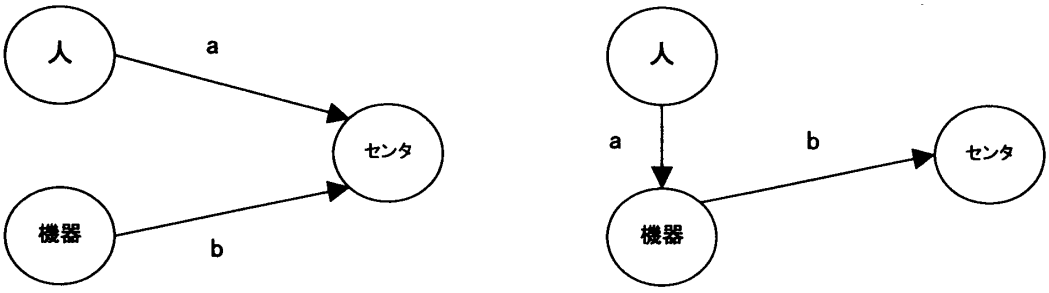
T-DESとDESは、暗号の種類も含め、大きく報道されたわけではなかったが、安全を守っている根幹の部分を公けにして安全対策をしていた組織があったことに注目したい。

日本では良くあるパターンで、20年前の事件では、銀行が如何に無策であり、本支店間では暗号もかけていなかったのではなかったとか、銀行カードの磁気部分には口座番号ばかりか暗証番号も入いっていて、銀行カードのスキミングだけですべての情報がそろう銀行もあった。など、真偽は明らかではないが多くのことを我々は、報道から知ることになった。一方、システムを作っている側からは、自分達のセキュリティの根幹を公けにしてはいけないというルールがあるのだと思う。犯罪者にヒントを与えたくないのがその理由だと思われる。

欧米の視点と同じく日本においても安全対策の仕様を知らせても守れるシステムを作って欲しいものだと思う。一夜のうちに暗号を強化した某銀行の様な例もあるからだ。そして、ユーザたる顧客にそのセキュリティの根幹を納得してもらって、そのリスクをどこまでとるか判断する機会を与えてもらいたいものだ。何も知らされないのに、補償を負担されるのは社会的公平性に欠く。

---

[1] ISOによる暗証番号（PIN）の取扱に関する標準。
[2] 米国政府調達標準FIPSの暗号として規格化され、その後ANSIになり広まった暗号。
[3] DESを三回繰返す構造を持つDESより強化された暗号。トリプルDESとも呼ばれる。



(ア)可動機器の能力が低い場合　　(イ)可動機器の能力が高い場合

図1　3者間の情報の流れ

2．情報セキュリティ技術における研究者の議論

2．1　コンセンサスが取れている仕様公開

安全対策の仕様を漏らすと安全性が損なわれるという議論は正しくない。セキュリティの根幹を提供している「暗号」分野では、暗号の仕様を完全に公開して研究者同士で解読しあうコンセンサスがかなり前からとられている。

こうなったのは、公けにされ欠陥を指摘された暗号の方が、秘密のまま運営されている暗号よりも結果的に強いものになると、経験的に実証されてきたからである。先にでてきたNIST[4]（かつてはNBS）によるDES, T-DES暗号が良い例であり、今は次世代暗号のAES[5]がある。

暗号研究では仕様公開がありえても、実際に利用されている暗号ではありえない。仕様が公けだと、解けてしまったときのインパクトが大きい。との意見がある。しかし、実用システムのほとんどで、今や、T-DESが使われ、将来はAESか、NTTと三菱電機のCamellia暗号[6]に置き換わると言われている。これらの暗号は何れも仕様公開されていることを心に留めたい。

2．2　安全を支える暗号技術の議論

ところで、技術者の間で議論されている暗号は現在ほとんど簡単には解けないのである。従って、議論・分析するために、言わば、将棋で言えば飛車角落ち、囲碁で言えば何目も相手に置かせて、暗号を解きやすい状況に置いて安全性を議論する。

専門的に言えば、メッセージ（平文）を暗号化して、暗号文を作り、暗号文だけで解読すること（単独暗号文攻撃）を一般には期待する。しかし、それは殆んど無理なのだ。そこで、平文と暗号文をペアにして解読する状況（既知平文攻撃）や、攻撃者にとって都合のよい平文や暗号文を選んで解読できる状況（選択平文攻撃または選択暗号文攻撃）などを作って、暗号の強さを調べる。

「世界で一番強い暗号」、「最強の暗号」と鳴り物入りで報道される暗号が時々あるが、仕様を公開しない、暗号処理で利用される秘密パラメータの生成方法を説明しない、暗号分析するためのさまざまな状況設定での分析をさせなく、分析結果を公けにしないものは、おおよそ贋物（にせもの）と考えて良い。最強という根拠が客観的に存在しないのであるから。

---

[4] 米商務省の標準技術局。
[5] NISTにより制定されたDESやT-DESに代わる次世代標準暗号方式。
[6] http://info.isl.ntt.co.jp/crypt/camellia/index.html

表1　安全対策例

情報システム例	a	b	(ア) 又は(イ)の別
銀行システム	暗証番号／静脈	口座番号・氏名	ア
携帯電話システム	暗証番号／指紋	機器認証	イ
インターネット・ショッピング決済	クレジット番号・暗証番号	暗号通信	イ

3．情報セキュリティ技術が作る安全

3．1　安全性を考える対象

ここで具体的に議論するために、図1に銀行システムの様な顧客が係わる情報システムを考えたい。ユーザたる人と、人が持ち運ぶカード、携帯電話、ノートパソコンなどの可動機器と、法人である銀行、電話会社、インターネット商店などのセンタ機能の3者に分けて構成される。磁気式の銀行カードの様に、機能が低いシステムは(ア)に示すように、人と可動機器が一緒になってセンタに作用する。携帯電話やパソコンが可動機器になると、機器の機能が高いので、(イ)に示すように、可動機器が人とセンタとを仲介する機器となる。

3者間で伝える情報は、図中の a と b で示した。これらに着目し、情報システムの代表例を表1に示す。a では、人の記憶に頼る暗証番号（パスワードなど）と、人を区別するための指紋または静脈が使われる。また、人というより決済主体を明確化するためのクレジット番号が使われる場合もある。また、b は、銀行システムの場合、人の記憶を補う形で口座番号や氏名が銀行カードの磁気ストライブに記憶される。同様に、携帯電話では、落とした時の無断使用の防御用に a の暗証番号や指紋が使われることがあるのに対し、課金をきちんとするためには、人が知らないうちに機器識別子に基づく機器認証bがセンタとの間で行われる。一方、インターネット・ショッピングの場合、毎回変化のない a の情報を盗聴され流用されるのを防ぐ意味で、a の情報をセンタへ伝えるためだけに暗号通信 b が使われる。毎回違う暗号が生成されるので、aが不変の情報であっても、情報は安全である。

3．2　情報セキュリティ技術の活躍

a は顧客である人の識別の意味もあり使われるが、決定版は開発されていない。従来は、暗証番号の様に人の記憶に頼る傾向があったのが、人間の身体的特徴を識別に使うバイオメトリックス技術が注目を集めている。ここ数年は、安価になった指紋照合機器の導入が進み若干の進展があった。しかし、指紋は、ガラスに付着した指紋などから複製可能[2]であるため、複製の心配が少ない静脈認証が銀行システムの一部に採用されつつある。

b の部分では、暗号技術が主役になっている（暗号技術の概要は文献[3]を参照）。（ア）の構成の銀行システムの場合、センタのエントリ部分としてATMが仲介する。出納を管理する計算機センタと距離があるため、その区間を暗号化されるべきとされ、前述のIS09564が前提になっている。また、センタから情報が漏れない様に、データベースの暗号化など安全性を強化する対策がとられる。

（イ）の構成の場合、可動機器にある程度の計算能力が期待できるため、安全性に係わるところに暗号が使われている。携帯電話の場合、不正な課金が一番の問題なので、機器を精密に確認する機器認証が進歩した。早く普及した外国では機器を識別する情報（識別子）が、裸のままやりとりされ、傍受され不正利用される事件が起きたことがあった。その後の携帯電話システムは識別子

を裸で送らないで、センタ（基地局）と携帯電話（子機）と情報のやりとりをして確実に相手を確認する技術が導入された。この部分では、暗号方式またはディジタル署名が使われている。どちらも現代の暗号技術を基礎に置く技術であり、不変の識別子を裸で送ることがなくなったので、無線傍受されても安全になった。

インターネットは、無線区間に限らず有線区間でも他人にモニタ（傍受）される危険を避けては通れない。資源を出し合っての互助的な成立経緯があるので、モニタ自体は一般に不正ではない。そこで、中継者に見られても心配ない暗号技術が進歩した。SSLまたはTLSと言われる技術で、使われているときはWEBページの端に「鍵マーク」を表示するなどしている。一般に、公開鍵暗号により鍵を暗号化し、その鍵を用いた共通鍵暗号によって暗号化と復号の暗号通信を行われる。この様に暗号が2段構えになったのは、公開鍵暗号の処理が遅いためである。ここで使われる公開鍵暗号と共通鍵暗号はIETFで推奨されるものが使われていて、これらも現代の暗号技術を基礎に置く技術が採用されている。

4．今後に向けて

暗号は騒がれても、なかなか普及しない技術である。やっと部分的ながらインターネットの普及で広まりつつある。今後は、暗号化が正しく行われていることを、人がどうやって確実に把握するのかが重要な課題になっていくと思う。悪意のある人が不正なWEBページを作成し「鍵マーク」を表示させて安心させておき、裏で情報を不正に入手ということがこれから頻発しそうだからだ。既に、フィッシング（Phishing）という本物に似せたWEBページを作ってクレジット番号を盗んでいる犯罪が広まりつつある。

ここで、ウィルス対策について書いてないのを不思議に思う人が居るかもしれない。言及した暗号通信や、機器認証など暗号技術を活用したものには、ウィルスが入ってくる余地はない。しかし、適用できる範囲は僅かであり、簡単にウィルス対策にはならないのである。暗号技術で身を守るカプセルや、他人から侵入されない強固な防護壁を作っているだけというのが現状である。

なぜ、こうなるかというと、暗号は根本解決を与えるが、OSは暗号との連携を考慮しないで進歩してきたためである。OSはソフトに欠くべからざるもので、アッパーコンパチブル（上位互換性）を優先させるので、導入を不十分にする原因になっている。

一方、インターネットが普及したため、問題が大きくなっているスパム・メールと、一斉に多くのサイトから無駄なアクセスをさせてサーバーを機能不全に陥らせるDDoS攻撃対策の課題がある。これらの対策は急務であるが、暗号技術の導入によりこれから着々と解決されると思う。

また、電子マネー、電子オークション、電子決済など暗号技術をサービスの中心にすえて活用する研究が進んでいる。これらを実際に活用するシステムが、社会にうまく受け入れられる様にすることが、今後重要になると思われる。

参考文献

[1] 岩下直行：「決済システムにおける情報セキュリティ」，日銀金融研，Nov. 2001．ならびに，「金融業界における最近の情報セキュリティ問題について」，日銀金融研，Apr. 2005.
http://www.boj.or.jp/set/forum.htm から参照可.

[2]田辺壮宏、森下朋樹、松本勉：「携帯機器に搭載される指紋照合装置は人工指を受け入れるか」，2005年暗号と情報セキュリティシンポジウム，2A2-4, pp.553-558, Jan. 2005.

[3] 太田和夫、國廣昇：「本当に安全？　現代の暗号」，岩波書店，2005.

略歴

森田 光（もりた　ひかる）

1980, 82, 93年 北海道大学 学士，修士，博士(工学).

1982～2005年　日本電信電話㈱（'85年まで公社）研究所で暗号・情報セキュリティなどの研究開発に従事.

1994～2005年　電気通信大学大学院情報システム学研究科で客員助教授・客員教授として学生指導.

2005年4月より，神奈川大学教授.

連絡先

神奈川大学 工学部

〒221-8624　横浜市神奈川区六角橋3-26-1

電話：045-481-5661

Email: morita@acm.org