[山口県銀行協会、山口経済同友会共催による経済産業省局長表彰記念講演会]

2009 年 11 月 6 日

金融取引の安全と安心を守るために
― 電子商取引時代の情報セキュリティ対策

日本銀行下関支店長　岩下直行

1. 謝辞

本日は、表彰記念講演会にお集まり頂き、誠にありがとうございます。

今回、経済産業省・商務情報政策局長から、情報セキュリティ促進の表彰を賜りましたことは、私の過去 15 年間の研究活動の成果を評価して頂いたという意味で、研究者として大変誇らしく思うと同時に、本日、皆様に、私が研究してきた内容についてお話しをするきっかけを与えて下さったことについても、大変ありがたく思っております。

最初に、本日の講演会の開催にご尽力頂いた関係者の皆様に、心より御礼を申し上げます。まず、さきほどご挨拶を頂戴した、山口県銀行協会会長であり、山口経済同友会代表幹事でもある、山口銀行・福田頭取には、本講演会の開催をご発案頂いたことに加え、お祝いの言葉を頂戴し、感謝の念に堪えません。山口県銀行協会の林常務理事には、本日の講演会・懇親会の開催を巡って、様々なご配意を賜り、誠にありがとうございました。経済産業省・中国経済産業局の小嶋地域経済部次長には、遠路広島より足をお運び下さり、表彰状授与式を執り行って下さいました。誠にありがとうございました。そして何より、本日、お忙しい中、この席に足をお運び下さった皆様に、改めて御礼を申し上げます。

これから、「金融取引の安全と安心を守るために」というタイトルで 40 分程度、お話をさせて頂きます。やや硬い演題で恐縮ですが、できる限り平易に、つまり数式を使わないで、金融業界において暗号技術、情報セキュリティ対策が重要なものとなってきた経緯から、私が日本銀行・金融研究所で取り組んでいた研究の内容、そして今回の表彰に至るまでの軌跡をご紹介します。

2. 銀行の建物にみる「安全と安心」

下関市観音崎町の「やまぎん資料館」は、かつて山口銀行の本店だった建物で、山口県指定有形文化財に指定されています。山口県徳山産の花崗岩に覆われた外壁には、重厚な彫刻が施され、昭和 20 年 7 月 2 日の大空襲や、過去 90 年間の風雪に耐えた力強さを感じます。

下関が誇る郷土の童謡詩人、金子みすゞが下関を詠んだ数少ない詩のひとつに、この建物の姿が描かれているのをご存知でしょうか。「はつ秋」と題されたその詩は、次のようなものです。

白いいかめしい日曜の銀行に、
ころ、ころ、ころ、とこほろぎが鳴き、

白いやうにうすい朝の空を、
すらすらと蜻蛉(とんぼう)が飛ぶ。

（秋は今朝、
港に着いた。）

白い巨きな日曜の銀行に、
陽はかつきりと影をつくり、

白い絲のついた蝉は電線にからまつて、
うすい翅(はね)をふるはせてゐる。[1]

この詩は、大正 14 年秋のこの建物のことを詠ったものだと研究者は指摘しています[2]。秋の始めの良く晴れた日曜日にやまぎん史料館を訪れれば、日差しを浴びた外壁が白く輝き、みすゞの詩に描かれた風景が再現されているように感じることができます。

この山口銀行旧本店を始め、歴史的建造物として各地に保存されている古い銀行の建物は、頑丈な石造りのいかめしい外壁や、立派な金庫によって、自らが、地震や火災、あるいは強盗といった脅威に対して「安全」であることをアピールしています。その姿は、当時の銀行の顧客に「安心」を与える、信頼の象徴だったことでしょう。戦時中に大空襲に耐えた銀行の建物は、人々に安心を与え、その後の復興にも大きく貢献したはずです。当時から、安全対策を充実させて人々に安心を与えることは、銀行の責任でもあった訳です。それは、もちろん現代でも同じです。

しかし、現代の銀行が直面しているのは、物理的な脅威だけではありません。偽造キャッシュカード事件に代表されるように、銀行を脅かす新手の金融ハイテク犯罪の手口が次々に出現しているからです。現代の銀行が顧客に「安心」を与えるためには、建物の外観が頑健であるだけではだめで、その内側にある銀行の情報システムやネットワークがきちんと守られ、金融取引の安全性が確保されていることを信頼して頂くことが必要なのです。

私が過去 15 年間にわたり研究し、今回の表彰の対象となったのは、「暗号技術」、「情報セキュリティ技術」です。かつて、研究を始めた当初は、「そ

[1] 金子みすゞ、『さみしい王女』、新装版 金子みすゞ全集・Ⅲ、JULA 出版局、1984 年。
[2] 今野勉、『金子みすゞふたたび』、小学館、2007 年。

んなことを研究しても銀行の役には立たないのでは」と懐疑的にみられていた特殊な研究分野ですが、今では、金融取引の安全と安心を守るために必要不可欠な技術として、その重要性が広く理解されるようになりました。それは、時代が変わり、人々が日常的に情報セキュリティを意識するようになったからでもあるのです。

3. 電子商取引の時代の到来

現代は電子商取引の時代といわれます。確かに、携帯電話やインターネットの回線を通じて、有料の音楽や動画をダウンロードすることは、特に若い世代の人々の間では当たり前のことですし、amazon.com や kakaku.com を利用して書籍や家電製品を自宅のパソコンから購入することも、ごく日常的なことになりました。電子商取引の多くでは、代金決済のために、インターネットでクレジットカード番号を入力したり、インターネット・バンキングを利用したりする必要がありますが、そうした電子的な資金決済手段も、すっかり日常的なものとなりました。不動産や車といった高額商品の販売から、旅行や事務用品のネット注文まで、インターネットを利用した新しいビジネスモデルが広く普及し、私たちは現在、好むと好まざるとにかかわらず、「日常的に電子商取引を利用する時代」を生きている訳です。

パソコンや携帯電話が不得意な方もおられますから、受け止め方は人それぞれでしょうが、一般の消費者が、多種多様な商品・サービスを迅速かつ効率的に選択し、購入できるようになったという意味で、今の時代は、10 年前とは比較にならないほど便利になったと私は思います。加えて、従来、買物で外出するのが大変だった高齢者や障がい者の方々が、パソコンや携帯電話を通じて、体に負担をかけずに経済活動に参加できるようになったことは、電子商取引の普及が社会にもたらした大きなメリットだと思います。このような経済全体の「質的な向上」は、GDP 統計には反映されないので、ついつい軽視されてしまうのですが、人々の生活水準を実質的に引き上げているという意味で、とても意義深い変化であると思います。

4. 電子商取引を支える暗号技術

この電子商取引という新しい便利な仕組みは、それを支える様々な情報技術の上に成り立っています。その代表選手が、本日お話をする「暗号技術」、「情報セキュリティ技術」です。

例えば、中高生が着メロをダウンロードしている携帯電話の中や、会社で事務職員がコピー用紙をネット注文しているパソコンの中では、現代の情報技術の粋を集めた暗号プログラムが常に動いています。一般利用者からは、

そのようなプログラムが動いていることは判別できませんが、安全な電子商取引のためには、それは必要不可欠な仕組みです。

「暗号は機密保護のために利用されるのだから、その技術は秘密なのでしょう？」と良く尋ねられます。しかし、現在普及している暗号には、秘密のベールに包まれた部分はありません。暗号化の具体的な手順（これを「暗号アルゴリズム」と言います）はすべて公開されており、暗号学者は研究のために暗号アルゴリズムの弱点を探し、様々な攻撃を試み、その結果を論文で詳細に公表しているのです。

暗号の仕組みや弱点を広く公開してしまって、安全性に問題はないのでしょうか。実は、むしろ公開する方がより安全になるのです。暗号アルゴリズムは、高度な数学に基づいて考案され、複雑なコンピュータ・プログラムとして実現されます。基礎となる理論に見落としはないか、プログラムに欠陥はないか、チェックすべき多くの項目があります。技術を公開して、大勢の学者、研究者の目にさらされることによって問題点が洗い出され、必要であれば改良が施され、より安全性が増すのです。

暗号を利用するときは、この暗号アルゴリズムに加えて、「鍵」と呼ばれる数十～数百桁のランダムな数値列を合わせて使用します。この「鍵」は、ダイヤル式金庫の秘密の番号のようなもので、「鍵」を知っている人だけが暗号化や復号（暗号文を元のデータに戻すこと）を行うことができます。異なる「鍵」を用いれば、多くの人が同じ暗号アルゴリズムを利用して、別々に暗号を利用することもできます。実際、皆さんのパソコンや携帯電話の中に組み込まれている暗号化のためのプログラムはだいたい共通なのですが、「鍵」だけはすべて異なります。皆さんがインターネットでクレジットカード番号や個人情報を入力しても、それが皆さん専用の「鍵」で正しく暗号化されたものであれば、他の人が同じプログラムを使っていても「鍵」が違うので解読できず、通信内容が漏洩する心配はありません。

5. 暗号技術と銀行

それにしても、なぜ、日銀の支店長が暗号技術を研究しているのかと、いぶかしく思われる方もいらっしゃると思います。かつて暗号は、軍事機密や外交機密の秘匿のために利用されるものであり、銀行の業務とはまったく関係のないものでした。

しかし今や、暗号技術は、銀行にとって欠くことのできない、極めて重要な技術となっています。そのような変化が最初に生じたのは、1970 年代の米国でした。米国で通信ネットワークを銀行業務に活用しようという動きが出始めた際に、セキュリティ確保のために暗号を使いたいというニーズが強

まったのが、そのきっかけです。

軍事や外交のために開発された古典的な暗号に対して、ビジネスに利用されるために開発されたものを現代暗号と呼びます。その現代暗号の始まりは、1977 年に米国政府標準となった DES 暗号[3]です。DES 暗号は、元々は、米国の銀行が通信ネットワークのセキュリティを守る目的で米国 IBM 社に開発を依頼したものが原型となっています。その後、一部設計を変更した上で、米国政府標準に採用され、世界中に普及しました。特に、欧米の金融業界の決済ネットワークに DES 暗号によるセキュリティ対策が次々に導入され、銀行は暗号技術の最大のユーザーとなったのです。

そもそも銀行は、コンピュータによるネットワーク・システムを最も早い時期に整備した業種でした。そして、通信ネットワークの安全性を守るためには、暗号技術が不可欠です。暗号技術は、高度な数学や情報技術を利用して実現するものですから、銀行が利用者として暗号技術を使いこなすためには、ある程度は専門的な知識を身につけておかないと、暗号を不適切に利用してしまったり、強度が低下した暗号を使い続けたりするおそれがあります。特に、毎日巨額の資金をコンピュータ・ネットワークで決済している日銀としては、自らの利用するセキュリティ対策に遺漏なきよう、綿密にチェックしておく必要がある訳です。日銀の職員が暗号技術の研究をしてきたのも、こういう理由によるものなのです。

6. 最初の暗号危機: DES 暗号の強度低下

日本銀行は、1988 年に稼働開始した日銀ネットと呼ばれるオンライン・システムにおいて、DES 暗号を全面的に採用しました。当時、国内において、暗号を採用しているコンピュータ・ネットワークは他にほとんどなく、日銀はわが国における暗号ユーザーの先駆け的な存在でした。

ところが、1990 年代に入ると、海外の暗号学者の間から、「DES 暗号の強度が低下している」という論文が発表され始めました。これらの論文は当然、専門家が専門家向けに書いたものですから難解で、また当時は専門家の間でも DES 暗号の強度低下については必ずしも意見が一致していた訳ではなかったので、それらの論文の当否を判断するのはとても難しいことでした。

そこで、日本銀行・金融研究所において、暗号の強度評価に関する学術的な研究を進める必要があるとの認識が高まり、国内の有力な暗号学者の先生方の指導を仰ぎながら、研究チームを立ち上げました。それは、私が日本銀

[3] DES 暗号（Data Encryption Standard）：米国の標準暗号に採用されていた代表的な共通鍵暗号（暗号化と復号に同じ鍵を利用する暗号）。鍵の長さは 56 ビット。入力データを 64 ビットずつ区切って暗号化する。

行・金融研究所に異動し、暗号技術の研究を始めた、1994 年頃のことです。

7. 「暗号の強度低下」とはどういうことか

そもそも、「暗号の強度低下」とは、どういうことでしょうか。暗号はコンピュータ・プログラムの形で利用されるものですから、一旦、ちゃんとしたプログラムを作っておけば、未来永劫、安全性が確保できるように思ってしまいます。しかし、残念なことに暗号には、「耐用年数」とでもいうべき安全性の期限があるのです。

暗号は、「鍵」と呼ばれるランダムな数値を秘密に保持することにより、通信の秘密を守ります。例えば、自転車の盗難防止に利用されるダイヤル式の南京錠の例で説明しましょう。よくある南京錠は、3 本のリングを持ち、各々のリングに 0 から 9 までの数字が刻印され、リングを回すと「000」から「999」までの組合せが可能なタイプです。このタイプの南京錠は、解錠するための番号を知らなくても、「000」から「999」まで、1000 個の組合せをすべて試してみれば、どこかで錠を破ることができます。しかし、それは実際にはかなり時間がかかります。仮に 1 秒に 1 個の試行ができたとしても、すべての組合せを試すのに 17 分かかる計算になるので、自転車を盗まれない程度の安全性は確保できると考えられているのでしょう。もしも自転車が高価で、安全性をより高めたいのならば、リングを 4 本に増やし、「0000」から「9999」まで、10000 個の組合せが可能な錠に変えれば良いでしょう。この新しい錠を破るために必要な時間は、10 倍（約 3 時間）になります。

暗号もほぼ同じように説明することができます。DES 暗号は、56 ビット、つまり 2 進数で 56 桁の「鍵」を使う暗号アルゴリズムです。これは、十進数では約 17 桁に当たりますので、17 本のリングの付いた南京錠を想像して下さい。これに対して同じように 1 つの「鍵」を 1 秒で試行したとすれば、すべての「鍵」を試すのに約 23 億年かかる計算になります。もしこれが南京錠であれば、自転車はとてつもなく安全だといえるでしょう。

しかし問題は、「1 試行 1 秒」という前提です。DES 暗号はコンピュータ・プログラムですから、高性能なコンピュータを使えば 1 試行にかかる時間を短縮することができます。複数のコンピュータで並列処理すれば、更に時間を短縮できます。このような総当たりの試行は、高性能なコンピュータが安価に入手できる環境となれば、より容易になります。そして、コンピュータのコスト・パフォーマンスは、1 年半の周期で倍増するという経験則（ムーアの法則）が知られています。このため、ある時点で十分安全と考えられていた暗号アルゴリズムも、長い時間が経過すると、安全性の前提条件が変化し、現実的なコストと時間で「鍵」の総当たりによる解読が可能になってし

まうという宿命を負っています。これが暗号に「耐用年数」が発生する原理です。

DES 暗号は、開発当初である 1977 年頃のコンピュータの性能を前提とすれば、現実的な時間内にすべての「鍵」の総当たりをすることは難しいと考えられていました。しかし、その後のコンピュータ技術の発展によって、1990 年代前半には、DES 暗号の強度は既にかなり低下しており、より安全な次世代の暗号に乗り換えていく必要性が高まっていたのです。

1994 年から 1998 年にかけて、日本銀行・金融研究所で暗号技術の研究チームとして研究を深める過程で、こうした実態を把握することができました。その後、国内的には、関係者に対して次世代の安全な暗号への移行を働きかけるとともに、国際的な議論のための取り組みを進めたのです。

8. 国際標準化機構･金融専門委員会での議論

1990 年代後半、DES 暗号は欧米の金融業界における標準暗号であり、銀行間の通信ネットワークから ATM、IC カード内の暗号化まで、いたるところで DES 暗号が使われていました。したがって、その強度低下は欧米の金融機関にとって大問題でした。

この問題を世界各国の銀行業界が話し合った場が、「国際標準化機構・金融専門委員会（ISO/TC68）」でした。日本銀行・金融研究所は ISO/TC68 の日本事務局であり、毎回の国際会議に日本代表として参加していたので、DES の強度低下の問題を指摘し、対応策の必要性を訴えました。1996 年には日本から詳細な技術レポートを提出し、次世代暗号への移行が必要になっていることをアピールしました。こうした議論を積み重ねた結果、DES の後継暗号であるトリプル DES[4]や AES[5]の標準化が進められ、日本を含む各国の銀行は、DES 暗号の強度低下が深刻な被害をもたらす前に、より安全な次世代の暗号に移行することができたのです。

国際標準化機構・金融専門委員会では、その後も、電子認証、IC カード、生体認証といった、金融業界にとって重要な情報セキュリティ対策に関する国際標準化の場として機能し続けました。そして、2005 年以降は、２回目の暗号危機である「暗号技術の 2010 年問題」（詳細後述）に対応した新たな

---

[4] トリプルDES：異なる２つないしは３つの56ビットの鍵を使って、DES暗号のアルゴリズムを３回繰り返して暗号化・復号する方式。信頼性の高いDES暗号のアルゴリズムを利用しながら全数探索法に対する安全性を高める方式として、広く採用された。暗号鍵の長さは112ビットまたは168ビット。入力データを64ビットずつ区切って暗号化する。

[5] AES（Advanced Encryption Standard）：DES 暗号の後継の米国標準暗号。公募された多くの暗号の中からコンテストによって選定された。暗号鍵の長さは 128 ビット、192 ビット、256 ビットの 3 つが利用できる。入力データを 128 ビットずつ区切って暗号化する。

国際ガイドライン作りの場として、再度活躍することになります。

私は、1995 年のサンフランシスコでの会議から、14 年間連続して国際会議に参加しました。国際会議の主催は各国回り持ちで、北はフィンランド、スウェーデンから、南はアルゼンチン、南アフリカまで、世界各国の様々な都市で開催され、得難い経験をすることができました。私が参加し始めた当初は、情報セキュリティ技術面の蓄積が少なく、国際会議における日本の存在感はやや希薄だったのですが、その後、学術研究の成果を会議で報告し続けていくことで徐々に信頼を勝ち得て、議論をリードできるようになったと思います。次回、2010 年 5 月には、東京で年次総会が開催される予定です。

9. 暗号技術検討会（CRYPTREC）の創設と電子政府推奨暗号リストの策定

以上述べたように、日本銀行・金融研究所における暗号技術研究は、自らが利用している暗号アルゴリズムの強度が低下するという切実な問題を契機としたものでしたが、暗号学者や各国の金融業界と協力することによって、危機が深刻化する前に対応を進めることができました。こうした経験は、その後、政府が電子政府に利用する暗号技術を選定するために創設した暗号技術検討会（CRYPTREC）の活動にも役立てることができました。

経済産業省と総務省は、2000 年に国内の有力な暗号学者、暗号研究者を集めて、暗号技術検討会を創設しました。政府機関における行政手続のオンライン化を促進し、行政の効率化を図っていく際に、どのような暗号技術を選定すべきかが大きなテーマでした。そこでの議論の結果、2003 年に策定されたのが「電子政府推奨暗号リスト」です。このリストは、政府機関のみならず、銀行を始めとする民間企業においても、信頼できる暗号のリストとして広く参照されており、これを策定したことは大きな意義がありました。

私は、暗号技術検討会に構成員として参加し、金融分野における暗号危機の経験を踏まえ、ユーザー側の視点から、どのような暗号リストを策定すべきか、策定したリストをどう維持管理していくかについて議論を重ねました。構成員としての活動は、2009 年 6 月に下関支店に転勤するまで、10 年間続きました。わが国では、ユーザー側の立場で暗号技術を検討している研究者が少なく、時に暗号のメーカー側である暗号学者の構成員と意見が対立することがありましたが、そうした議論をすることで検討が深まり、リストをより良いものにできたのではないかと思います。

10. 二回目の暗号危機: 暗号技術の 2010 年問題

最初の暗号危機から 10 年経った 2005 年、二回目の暗号危機の発生を予感させる出来事がおこりました。米国政府が、トリプル DES に対する米国政

府標準暗号の指定を廃止し、2010 年以降はその安全性に対する「お墨付き」を延長しないことを表明したのです。トリプル DES は、当時も現在も、世界中の金融機関が最も広く利用している暗号アルゴリズムです。米国政府の「お墨付き」が廃止されたからといって、直ちに危険になるという訳ではありませんが、「安全・安心」を重視する銀行業界としては、看過できない問題ですし、実際、コンピュータ技術の進歩によって、トリプル DES を含む幾つかの暗号の安全性が低下しつつあることは否定できないことでした。

この時、私は、10 年前の最初の暗号危機の時の対応を思い出し、その経緯をなぞることで、問題が解決できるのではないかと考えました。そこで、国際標準化機構・金融専門委員会の場で、議長（米国代表）に働きかけて、次世代暗号への移行を主要議題に取り上げてもらい、国内の暗号研究者と日本銀行・金融研究所とが共同で技術レポートを作成して国際会議に提出したのです。これらはすべて、10 年前に我々が試行錯誤の中で取り組んだことの再現でした。

幸い、国内向けに論点を整理した「暗号技術の 2010 年問題」という論文が注目を集め、問題の所在を多くの人々に知ってもらうことができました。国際会議においても、次世代暗号への移行問題を専門に取り扱う作業部会が組成され、移行に向けてのガイドラインが作成されました。まだ予断は許されないものの、二回目の危機も、深刻な事態に陥る前に、より安全な次世代の暗号アルゴリズムに移行を進めることができるところまで漕ぎつけたと感じています。

11. 安全で安心な金融システムを守るために

暗号技術、情報セキュリティ技術の難しさは、一般の利用者がどんなに熱心に調査しても、良い技術と悪い技術の違いが分からない、という点にあります。このため、専門家の支援がないと、利用者は適切な判断ができません。良い技術が利用できるためには、多くの技術者、学者、研究者が協力し、切磋琢磨して研究を深め、良い技術を普及させていくことが必要です。しかし、そうした専門家による研究は、なかなか一般の方々には理解し難い内容が多いのです。電子商取引や金融システムにおいて、安全・安心が大切ということは理解されていても、暗号技術に関する難解な研究が広く理解されることは、なかなか難しいだろうと思います。

毎年 10 月の「情報化月間」に、情報化の促進に貢献した個人を政府[6]が表彰する制度は、陰に隠れがちな「縁の下の力持ち」の役割を果たす人々に光

[6] 現在、本事業を推進しているのは、経済産業省、内閣府、総務省、財務省、文部科学省、国土交通省の１府５省。

を当てるものであり、一般に理解されにくい技術研究を進めてきた立場からは、大変ありがたいものと感謝しております。

吉田松陰先生は、自らの学問に対する姿勢について、「学は書を読み古(いにしへ)を稽(かんが)ふるの力にはあらざるなり。天下の事体に達し、四海の形勢を審(つまびら)かにする、是のみ。」[7]とおっしゃっています。松陰先生は、松下村塾では主として漢籍を教えられたのですが、中国の古典を通して、「今、我々が何をなすべきか」を考えることこそが学問であるとおっしゃっているのです。時代を若干下りますが、福沢諭吉先生の唱えられた「実学」の思想も、これと通じるものがあります。

こうした先人たちの言葉は、我々の進めてきた情報セキュリティ技術研究にも当てはまります。我々の研究も、専門分野に閉じこもり、「書を読み古(いにしへ)を稽(かんが)ふる」だけのものではだめです。「四海の形勢」、つまり、国内外における研究・実務動向にも注意を払いつつ、この研究分野において我々が何をなすべきかを真剣に考え、実行していくことが求められているのです。

我々金融業界の人間にとって、情報セキュリティはとても大切なものですが、それは最先端の技術研究と、実務での利用が上手に連携して初めて達成されるものです。その意味で、私が本年 6 月に着任した下関支店長という新しい職務の下でも、金融業界が安全で安心な金融サービスを提供し続けることができるよう、微力ながら貢献して参りたいと考えております。

ご清聴をどうもありがとうございました。

以　上

[7] 山口県教育委員会編、『吉田松陰全集』三、「丙辰幽室文稿・自書松柳詩後」、岩波書店、1939年。