IMES DISCUSSION PAPER SERIES

金融業務と情報セキュリティ技術：
この10年の経験と今後の展望

岩下直行（いわしたなおゆき）

Discussion Paper No. 2008-J-2

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

日本銀行金融研究所が刊行している論文等はホームページからダウンロードできます。
http://www.imes.boj.or.jp

無断での転載・複製はご遠慮下さい。

備考： 日本銀行金融研究所ディスカッション・ペーパー・シリーズは、金融研究所スタッフおよび外部研究者による研究成果をとりまとめたもので、学界、研究機関等、関連する方々から幅広くコメントを頂戴することを意図している。ただし、ディスカッション・ペーパーの内容や意見は、執筆者個人に属し、日本銀行あるいは金融研究所の公式見解を示すものではない。

IMES Discussion Paper Series 2008-J-2
2008 年 2 月

金融業務と情報セキュリティ技術：この10年の経験と今後の展望

岩下直行（いわしたなおゆき）*

要　旨

日本銀行金融研究所では、1998 年 11 月に第 1 回情報セキュリティ・シンポジウムを開催して以来、同シンポジウムを毎年度開催し、今回、第 10 回の開催を迎えた。第 1 回シンポジウムの開催当時は、まだ普及には時間が掛かると考えられていた IC カード、生体認証、インターネット・バンキング、電子マネーといった技術が、この 10 年間の間に金融分野で広く普及するとともに、学術研究の対象と考えられていた情報セキュリティ技術が、金融実務の世界で欠くことのできないツールとなりつつある。

これまでの情報セキュリティ・シンポジウムでは、その開催時点でわが国の金融業界が直面していた、あるいは、直面する予兆がみられた情報セキュリティ技術上の課題を取り上げて問題提起を行い、金融機関が採用し得る対策や今後の展望について、金融業界の実務家と情報を共有することを目的に、研究発表やパネル討論を実施してきた。

本稿では、これまでの情報セキュリティ・シンポジウムの内容を参照しながら、わが国の金融業界が直面してきた環境変化、情報セキュリティ上の問題とその対応状況について説明し、金融サービスに活用される情報技術や情報セキュリティ対策の今後のあり方について考察する。

キーワード：インターネット、偽造キャッシュカード問題、生体認証、セキュリティ、電子マネー、リテール・バンキング、IC カード

JEL classification: L86、L96、Z00

＊ 日本銀行金融研究所情報技術研究センター長（E-mail: iwashita@imes.boj.or.jp）

本稿は、2008 年 2 月 5 日に日本銀行で開催された「第 10 回情報セキュリティ・シンポジウム」への提出論文に加筆・修正を施したものである。なお、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

目　次

１．はじめに

日本銀行金融研究所では、1998 年 11 月に第 1 回情報セキュリティ・シンポジウムを開催して以来、同シンポジウムを毎年度開催し、今回、第 10 回の開催を迎えた。第 1 回シンポジウムの開催当時は、まだ普及には時間が掛かると考えられていた IC カード、生体認証、インターネット・バンキング、電子マネーといった技術が、この 10 年間の間に金融分野で広く普及するとともに、学術研究の対象と考えられていた情報セキュリティ技術が、金融実務の世界で欠くことのできないツールとなりつつある。

これまでの情報セキュリティ・シンポジウムでは、その開催時点でわが国の金融業界が直面していた、あるいは、直面する予兆がみられた情報セキュリティ技術上の課題を取り上げて問題提起を行い、金融機関が採用し得る対策や今後の展望について、金融業界の実務家と情報を共有することを目的に、研究発表やパネル討論を実施してきた（各回の概要は表 1 参照）。

本稿では、これまでの情報セキュリティ・シンポジウムの内容を参照しながら、わが国の金融業界が直面してきた環境変化、情報セキュリティ上の問題とその対応状況について説明し、金融サービスに活用される情報技術や情報セキュリティ対策の今後のあり方について考察する。

表 1：過去の情報セキュリティ・シンポジウムの開催概要

開催回（年度）	テーマ	キーノート・スピーチにおける説明		キーノート・スピーチ以外の講演のタイトル
		金融業務の現状	主な課題や検討対象	
第 1 回（1998）	金融分野における情報セキュリティ技術の現状と課題	・ネットワークのオープン化 ・電子マネーの各種プロジェクトの実施 ・インターネット・バンキング黎明期 ・欧米における新しい暗号技術の採用	・総合技術としての情報セキュリティ対策の検討 ・情報セキュリティ対策の適切な開示の検討	・金融分野における情報セキュリティ技術の国際標準化動向 ・電子マネーを構成する情報セキュリティ技術と安全性評価 ・共通鍵暗号を取り巻く現状と課題 ・公開鍵暗号の理論研究における最近の動向
第 2 回（1999）	金融業務と認証技術	・インターネットを利用した金融サービスの本格化 →認証技術の重要性の高まり ・「通帳と印鑑」、「磁気カードと暗証番号」といった既存の認証方式のセキュリティ・レベル低下	・将来の技術動向を見据えた適切な認証方式の検討 ・IC カードや生体認証技術も検討の対象にすべき ・SSL の利用にも留意が必要（クライアント認証の必要性）	・金融業界における PKI・電子認証について ・最近のデジタル署名における理論研究動向について ・デジタルタイムスタンプ技術の現状と課題 ・バイオメトリックスによる個人認証技術の現状と課題 ・最近の金融業務における情報セキュリティ評価・認定を巡る動向について
第 3 回（2000）	情報セキュリティ技術の評価と信頼性	・ネットワークのオープン化→金融実務における情報セキュリティ技術の必要性に関する認識の高まり ・インターネット・バンキングやデビットカードのサービス提供	・信頼できる技術の選択の必要性→情報セキュリティ技術の安全性評価の検討 ・国際標準や第三者による評価・認定制度の活用 ・情報セキュリティ技術における脆弱性の報告・対応に関する枠組みの検討	・電子文書の送受信証明を行うためのプロトコルの研究動向と安全性評価 パネル 1：暗号アルゴリズムの安全性評価と国際標準化 パネル 2：IC カードの安全性評価を巡って
第 4 回（2001）	インターネットを利用した金融サービスの情報セキュリティ対策	・インターネット・バンキングは有力なデリバリチャネルとして定着しつつある。 ・無権限者によるなりすましの防止の検討。 ・SSL、パスワード、乱数表を組み合わせた認証方式に問題点がある。	・インターネットにおけるさまざまなセキュリティ上の脅威に対する適切な対策の検討 ・インターネット・バンキングにおける利用者の認証方式が鍵となる。	・金融分野における PKI：技術的課題と研究・標準化動向 ・RSA 署名方式の安全性を巡る研究動向について パネル：インターネット・バンキングにおける情報セキュリティ対策のあり方を巡って
第 5 回（2002）	デジタル署名の長期的な利用とその安全性	・電子署名法の成立と電子政府の実現に向けた取組み。 ・紙の文書をデジタル化された文書に置き換える動き。 ・通常の署名付きの電子文書を長期保管した場合、署名の効力を維持できない。 ・デジタル署名は「取引の瞬間」に短期的に利用されるものにとどまっている。	・通常の署名では、内容を信頼できる期間は高々公開鍵証明書の有効期間内。 ・署名の効力低下への対策として、タイムスタンプの利用等が挙げられる。 ・「システム全体」の防御に加えて、「電子文書単体」の長期的な安全性向上策の検討が望ましい。	・デジタル署名生成用秘密鍵の漏洩を巡る問題とその対策 パネル：デジタル署名を長期的に安全に利用するために

表 1（続き）：過去の情報セキュリティ・シンポジウムの開催概要

開催回（年度）	テーマ	キーノート・スピーチにおける説明		キーノート・スピーチ以外の講演のタイトル
		金融業務の現状	主な課題や検討対象	
第 6 回（2003）	金融分野における人工物メトリクス	・金融取引は証書、カード、紙幣等の人工物に大きく依存しており、セキュリティ対策についても目立った変化はない。 ・デジタル画像処理技術の発達やパソコンの普及等により、人工物が偽造・複製される事件が増えてきている。	・「製造者の技術的優位」から「人工物固有の特徴」を利用した技術を視野に。 ・可能な限り、技術内容を公開する方向での研究が重要。	・人工物メトリクスの精度評価と実装事例 ・人工物メトリクスのセキュリティ評価 パネル：人工物メトリクスの現状と課題
第 7 回（2004）	金融業界における情報システムの脆弱性検知と情報共有	・金融機関とその顧客は、偽造キャッシュカードによる不正預金引出し、フィッシング詐欺等、さまざまな脅威にさらされている。	・金融業界は「インターネットにコミットした業界」といえる。 ・脆弱性届出制度を活用するとともに、金融業界においても脆弱性の検知と情報共有の体制整備が必要。	・生体認証システムにおける脆弱性について ・デジタル署名の長期利用に係る脆弱性 パネル：情報システムの脆弱性検知と情報共有
第 8 回（2005）	金融機関の情報セキュリティ対策のあり方	・偽造キャッシュカード事件、スパイウェアによる個人情報漏洩、インターネット・バンキングでの不正送金。 ・金融情報システムの高度化・複雑化と、情報セキュリティ対策の難解さゆえに、必要な対策を見極めるのが困難。	・システムをブラックボックスのままにしておくのではなく、情報セキュリティ技術の再点検を行うことが必要。 ・対策の有効性や課題について見極める能力を持つ専門家の育成が必要。	・暗号アルゴリズムにおける 2010 年問題について ・金融取引における IC カードを利用した本人認証について パネル：金融機関の情報セキュリティ対策のあり方：研究から実践へ
第 9 回（2006）	リテール・バンキングのセキュリティ	・偽造キャッシュカードによる不正預金引出の被害金額は、引出限度額引下げが奏功し、減少してきている。 ・IC キャッシュカードや生体認証といった新しい情報セキュリティ技術は普及しておらず、その特性が活かされているとは言い難い。	・リテール・バンキングのセキュリティを向上させるためのグランドデザインを描くことが求められている。 ・生体認証については問題点を検討しその結果をオープンにしていくことで信頼を勝ちえることが必要。	・静脈認証システムのテスト物体によるセキュリティ測定・評価 ・生体認証システムのセキュリティ：どこまで評価できるか？ ・IC カード利用システムのセキュリティ ・システム設計から見た IC カードの暗号技術の安全性について

２．情報セキュリティ・シンポジウムの 10 年間

情報セキュリティ技術研究の観点からみると、この 10 年間は、わが国の金融機関が情報セキュリティ対策を高度化させた期間であったといえる。金融機関の情報システムは、提供している業務内容自体はさほど大きくは変化していないが、そこで利用されている情報セキュリティ技術は大きく様変わりしている。

わが国の金融機関において、10 年前の時点で情報セキュリティが重要でなかったわけではない。しかし、当時は、金融機関の情報システムが専用回線を利用したクローズドなネットワーク・システムであることを理由に、回線の暗号化やデジタル署名技術をほとんど利用していなかった。リテール・バンキングにおける顧客の認証も、磁気ストライプカードと暗証番号の照合のみで行っていた。このような比較的素朴な情報セキュリティ対策が主流であったのは、最先端の技術を導入しなくても、一定の安全性が期待できる環境下にあり、利用者が金融ハイテク犯罪の被害者となることがほとんどなかったからである。当時、IC カードや暗号装置といったセキュリティ機器は、需要が少なく高価であったし、顧客から導入を求められてもいなかった。

そうした認識が変わった原因は、インターネットの普及と電子マネーへの関心の高まりであっただろう。10 年前、わが国でインターネットが爆発的に普及し始めていたが、同時に、金融機関のサービスがインターネット経由で利用できないことについて、利用者の不満が高まっていた。電子マネーの実現に対する利用者の期待も強かった。

わが国の金融機関は、ネットワーク・システムを最も早い時期に整備した業界のひとつであり、決して IT 化に立ち遅れていた訳ではなかった。しかし、従来の金融情報システムの開発者からみると、安定性とセキュリティに優れた専用回線とメインフレーム中心の技術から、不安定でセキュリティの劣ったインターネット技術に移行することには抵抗が強く、インターネット上での金融サービスの提供については、当初は必ずしも積極的ではなかった。金融機関がオープンなネットワークで金融サービスを提供し、従来並みのセキュリティを確保するためには、それまであまり馴染みのなかった暗号、デジタル署名、IC カード等の情報セキュリティ技術を利用することが必要であったことが背景にある。

こうした中、第 1 回情報セキュリティ・シンポジウムが開催された。そのキーノート・スピーチでは、金融機関にとっての情報セキュリティ技術の重要性を、以下のように整理している。

「インターネットの爆発的な拡大に伴い、オープンなネットワークを利用した様々なビジネスが拡大してきている。こうした環境変化を受けて、従来はさほど一般には関心を持たれていなかった「情報セキュリティ技術」が、このところ急速に注目を集めるようになってきている。…わが国の金融機関が、これからの新しい金融業務の担い手として金融サービスを安全に提供し続けていくためには、暗号技術などの情報セキュリティ技術を正しく評価し、有効に活用していく能力が必要とされていると言えよう[1]。」

当時、暗号技術は実務とは関係のない単なる学術研究の対象と受け止める向きが多く、金融業務との関連で注目されることもあまりなかった。しかし、インターネットの普及率が高まってくると、金融業界は、インターネットを対顧客取引のチャネルとして積極的に利用し始めた。金融機関は、インターネット・バンキングの導入において、従来にはないセキュリティ上の問題に対処する必要に迫られた。そうした新しい課題への挑戦を経て、金融機関のセキュリティ対策は大きな変化を遂げ、その影響は金融情報システム全体に及んでいる。

その結果、2000 年に開催した第 3 回シンポジウムにおける下記の現状分析にあるとおり、わずか 2 年の間に、わが国の金融機関における情報セキュリティ技術の採用状況は様変わりとなっている。

「暗号、電子認証、ICカード等の情報セキュリティ技術が、わが国の金融業界においても実務に利用されるようになってきた。インターネットを利用した銀行取引や証券取引では、SSLと呼ばれる暗号通信プロトコルによって暗証番号や取引内容の機密を保護することが一般的となっている。銀行が発行するキャッシュカード／デビットカードも、従来の磁気ストライプカードから、耐偽造性を高めたICカードへと移行するための検討が進められている。これまで専用回線を使用したクローズド・システムであることを安全性のよりどころとしてきた銀行の勘定系システムにおいても、通信内容の機密保持や端末機器の認証のために、暗号や電子認証を利用しようとする動きが拡大している[2]。」

このような変化の最大の原因は、利用者の利便性と金融機関の効率化のために、金融情報ネットワークのオープン化が進められたことにある。オープンな環境の下で、従来と同じ素朴なセキュリティ対策のままでは安全性が確保できない。加えて、インターネット上での金融サービスの提供が進むほど、金融実務における情報セキュリティ上の問題点が明らかになり、その改善の為に様々なアイデアが提案されるようになった。本シンポジウムのみならず、様々な場でインターネット・バンキングのセキュリティが話題となり、その検討結果を実務に反映させる中で、セキュリティ対策の高度化が進んでいった。この局面では、金融機関がオープン・ネットワークという新しい環境において、従来と同等なセキュリティ水準を確保するために、徐々に暗号技術を習得するための、将来を見据えた検討作業が順調に進んでいると認識されていた。

[1]松本・岩下［1999］
[2]松本・岩下［2001］

３．偽造キャッシュカード問題の衝撃

ところが、2004 年に、こうした悠長な対応では間に合わない事態が発生してしまった。偽造キャッシュカード問題の深刻化である。

偽造キャッシュカードによる不正預金引出が社会問題となり、銀行の情報セキュリティ対策に関する世間の関心が高まったのは、2004 年から 2005 年にかけてであった。それまで殆ど発生していなかった偽造キャッシュカードによる不正預金引出の被害が、2003 年度から急増し、2004 年度には 10 億円に達した。

当時、ATM で銀行預金を引き出す場合、1 日当たりの上限金額は数百万円が相場であった。それほど高額の預金引出を可能とする認証手段として、磁気ストライプ方式のキャッシュカードと 4 桁の暗証番号だけではセキュリティが十分でないということは、以前から指摘されてきた。1999 年の第 2 回シンポジウムでは、銀行のキャッシュカードと暗証番号による認証方式の見直しの必要性について、次のように指摘していた。

> 「(a)様々な技術革新によって印鑑、印影、各種印刷物、磁気カード等の偽造が容易になっていること、(b)暗証番号の盗用や推定が巧妙に行われるようになっていること、(c)金融機関側も、店舗の人員削減等により、従来ほどのセキュリティ対策への配慮が期待できないおそれがあること、等を考えると、「これまで大丈夫だったので、これからも大丈夫」と判断することには慎重であるべきと思われる。従って、既存の金融取引で利用される認証方式についても、磁気カードよりも安全性の高いICカードの採用や、暗証番号に加えてバイオメトリック認証を導入するといった選択肢について、検討のスコープを広げていくべきであろう[3]。」

2005 年 1 月に、ゴルフ場の貴重品ロッカーからキャッシュカードを盗み出してスキミングする手口で不正預金引出を行っていたグループが逮捕され、その手口が大きな扱いで報道されると、テレビの報道番組や雑誌記事が相次いで被害の深刻さを伝え、銀行の対応の遅れを批判する声が相次いだ。このため、全国銀行協会は、IC カードや生体認証等の新技術の導入、被害者への補償等を内容とする対策を表明した。

こうした慌しい情勢の中で2005年3月に開催された第7回シンポジウムでは、偽造キャッシュカード事件の反省も踏まえ、「金融業界全体の問題として、脆弱性の検知とその情報共有のための体制整備を進める必要がある」との提言がなされている。偽造キャッシュカード事件の原因であったATM取引における認証手段の脆弱性について、上記の第 2 回シンポジウムでの指摘以降も、累次にわたって問題点を指摘していたにもかかわらず、現実の対応が進まなかったことについては、以下のように分析している。

---

[3] 松本・岩下［2000］

「(1) 過去 30 年間、磁気ストライプカードと暗証番号という技術が大きな問題もなく利用され続けてきたため、ICカード等の新しい技術に移行するきっかけがつかめなかったこと、(2) 従来の技術が金融業界全体の基本インフラとして利用されてきたため、業界内の幅広い合意がなければ新しい技術への移行が難しかったことから、ICカードや生体認証等の新技術の導入にかかる意思決定が先送りされてしまった[4]。」

2005 年 2 月には金融庁が偽造キャッシュカード問題に関するスタディグループを発足させ、2005 年 6 月には報告書が公表された。また、国会では、法律によって預貯金者の保護を図るべきという検討が行われ、2005 年 8 月に預金者保護法が公布され、2006 年 2 月 10 日から施行された。この結果、偽造・盗難カードによる不正預金引出に伴う被害については、原則として銀行が被害者に補償を行うこととなった。また、銀行は、被害の補償に加え、偽造カード犯罪の事前予防策として、認証技術の強化等が義務付けられることとなった。

その後、金融機関が ATM における引出限度額を引き下げたことや、利用者への注意喚起を行ったことの効果もあって、偽造キャッシュカードの被害は、2006 年度以降、件数、金額とも減少し、金融機関に対する批判も沈静化してきた。しかし、問題がすべて解消したわけではない。2006 年 3 月に開催された第 8 回シンポジウムでは、

「キャッシュカードのICカード化、ATMにおける生体認証の導入など、偽造キャッシュカードに対するセキュリティ対策は、さまざまな選択肢がよく知られるようになってきた…しかし、実際にこうしたセキュリティ対策を導入し始めた金融機関はまだ限られており、利用者の間での実際の普及率はあまり高くはない。…すなわち、カードと暗証番号のセキュリティについてみた場合、スキミングなどによる偽造カード犯罪に対して脆弱な状態は、セキュリティ技術的には基本的には現在も変わっていない。…次のステップとして、①磁気併用でないICカード化、および／または②生体認証の導入などにより、キャッシュカードとATMにおけるセキュリティ対策を抜本的に向上させ…るという施策が考えられる[5]。」

という問題提起を行っている。

[4] 岩下［2005］
[5] 岩下［2006］

４．脆弱性情報の公開と共有を巡って

本シンポジウムにおいて継続的に取り扱われてきた重要なテーマのひとつに、「金融情報システムにおける脆弱性情報をどう取り扱うべきか」という問題が挙げられる。

偽造キャッシュカード問題が社会問題化する以前にも、わが国の金融業界でセキュリティ侵害事例は発生していたが、それが公になることは少なかった。ごくまれに公になった場合でも、一種の金融スキャンダルとして取り扱われたため、事件の詳細については秘密とされ、その原因が詳細に分析されることは少なかった。

金融機関の場合、セキュリティ問題を「機密事項」として取り扱う傾向が強く、自らの採用する技術がアカデミックな研究の対象とされることや、技術的な論評をされることを忌避する先が多い。その傾向が行き過ぎると、「セキュリティ・システムの欠陥は、実際にその問題が顕現化し、セキュリティが破られて事件とならないと発覚しない」ということになってしまう。

もちろん、具体的なシステム設計や運用の欠陥については、適切なセキュリティのチェックを行うことで発見できるものも少なくない。その意味では、現在、企業のセキュリティ・チェックの仕組みとして広く採用されている PDCA サイクルは、重要なツールである。しかし、PDCA サイクルの実際の適用において問題となるのは、セキュリティ上の問題点を漏れなく検討することの難しさである。PDCA の C（チェック）の段階で、事件等によって露見していない問題点を発見して指摘することは容易ではない。そのシステムを設計･開発したスタッフが設計段階でセキュリティについても一定の検討をしている場合、そこで見逃されていた問題を、当該スタッフ以外の者が事後的に検知することはなかなか難しい。内部でそのようなチェックを行おうとしても、形式的なチェックに止まり、システムの抱える本質的な問題点を指摘できないことが多いだろう。

実際、過去において、脆弱なリテール・バンキング・システムが改善されずに提供され続けてしまった実例は多い。わが国の事例として、ゼロ認証の以前と以後における磁気ストライプ付きのキャッシュカードの偽造や、可変暗証番号方式によるファーム・バンキングにおける不正送金等が挙げられよう。これらは、潜在的な問題点としては認識されていたにもかかわらず、改善につなげられなくて被害が拡大してしまった例である。過去のこうした事例においては、実際に顧客に被害が生じるような事件の発生が、問題点の検知のきっかけとなってきた。実害が発生してからの対応は、どうしても後手に回り効率が悪いし、レピュテーションの観点からもダメージが大きい。こうした悪循環を断ち

切る観点からは、如何に先回りして課題を検討しておくか、という視点が重要であろう。

この点について、2000 年 11 月に開催された第 3 回シンポジウムのキーノート・スピーチでは、万一、金融システムで情報セキュリティ技術の利用に関する欠陥が指摘される事態となった場合、どのような体制が整備されていることが望ましいかについて、以下のような提案を行っている。

> 「情報セキュリティ技術を利用している金融機関の立場からみると、システムの欠陥を指摘されることは快いものではなく、また、特に公表された場合、レピュテーションの低下につながることもあり、できるだけ発見されないことが望ましいと思うのが普通であろう。しかし、事実として欠陥があるならば、これを早期に発見し対応策を講じていくことが重要である。
>
> …
>
> 実際に運用されている金融関連のシステムについて、セキュリティ技術に欠陥があることを発見した人は、どのように振る舞うであろうか。彼がセキュリティ技術の発展に寄与することを願う人であれば、何らかの形で当該システムの提供者に知らせたいと思うであろう。また、例えば、金融取引カードが簡単に偽造できてしまうなど、その欠陥が深刻であり、別のだれかが既に気づいて不正を行っているかもしれない場合には、被害を抑えるために、早期かつ明確にその欠陥を公表して、欠陥の存在する技術の拡散に対する警鐘を鳴らすべきとの考え方もありえよう。しかし、公表という手段をとった場合、有効な対策が講じられない間にその欠陥が悪用されて、かえって被害を拡大してしまうこともありうるし、レピュテーションの低下という形で当該システム提供者の経営にダメージを与えてしまう可能性もある。
>
> …
>
> 例えば、セキュリティ技術の欠陥を発見した場合、そこに届け出ると、その人の発見者としての名誉が保証され、場合によっては経済的な報酬も得られるような届出機関を作り、届けられた欠陥はそこで吟味されてから、適切な方法で公表される、というような仕組みも考えられる[6]。」

[6] 松本・岩下［2001］

５．シンポジウムで指摘された脆弱性の顕現化事例

４．で述べた問題点を幾ばくかでも解消すべく、本シンポジウムでは、金融ハイテク犯罪や情報セキュリティの要素技術の脆弱化の事例について、極力、具体的に取り上げ、分析してきた（表 2 参照)。これらの事例は、それが報道された公知の情報であっても、正式な情報として記録されることが少ないため、時間が経つと忘れ去られてしまうことが多い。海外で発生した犯罪事例や、学会における実験成功に関する情報の場合、わが国の金融業界では認識されないものもある。そうした事例にスポットライトをあてて、警鐘を鳴らすことも、本シンポジウムの重要な役割である。

表 2：シンポジウムで取り上げた金融ハイテク犯罪や要素技術脆弱化の事例

	金融ハイテク犯罪や要素技術脆弱化の事例	それを踏まえた提言
第 1 回	・Netscape Navigator 1.2 の SSL 実装のバグ（1995 年 9 月） ・DES cracker の完成（1998 年 7 月）	
第 2 回	・512bit RSA 公開鍵の素因数分解成功（1999 年 8 月） ・キャッシュカードの偽造、不正使用 ・ATM 取引での暗証番号の盗用、不適切設定の問題	磁気カードはもはや限界。IC カード化と生体認証の導入が必要。
第 3 回	・フランスの銀行 IC カードの偽造犯罪（1999 年末） ・CNS 電子署名偽造攻撃（1999 年）	中立的な機関による暗号技術の安全性評価
第 4 回	インターネット・バンキングにおける各種脆弱性 ・クロスサイト・スクリプティング脆弱性 ・ベーシック認証におけるパスワードの推定 ・乱数表によるチャレンジ・レスポンス方式への攻撃	ワンタイム・パスワードの導入、インターネット・バンキング普及後のリスク管理の強化
第 5 回	・デジタル署名付与文書の長期保管時の署名失効問題	デジタル署名の長期利用のための技術・環境の整備
第 6 回	・印影の偽造による盗難通帳からの不正預金引出 ・クレジットカードの偽造、不正使用	人工物（紙、カード等）のセキュリティを向上させるための技術開発・導入
第 7 回	・キャッシュカードの偽造、不正使用 ・フィッシング詐欺メール、キーロガー ・人工物によって偽造された生体情報によるなりすまし	脆弱性情報届出制度の活用と業界内での情報共有、人工物による生体情報の偽造への対策の検討
第 8 回	・キャッシュカードの偽造、不正使用 ・スパイウェアによるパスワードの盗用 ・暗号アルゴリズムの 2010 年問題	キャッシュカードの全面的な IC カード化、2010 年以降も利用可能な強度の高い暗号アルゴリズムへの移行
第 9 回	・キャッシュカードの偽造、不正使用 ・人工物によって偽造された生体情報やウルフ攻撃によるなりすまし ・EMV 仕様における暗号アルゴリズムの実装上の問題	グランドデザインの検討、生体認証システムのセキュリティ評価手法の確立に向けた取組み

これらの事例をみると、アカデミックな研究動向を眺めておくことで、起こり得るセキュリティ侵害への事前の警鐘として機能すると期待できるケースと、そうでないケースとがあることが分かる。例えば、暗号技術にかかる脆弱性については、暗号技術の情報自体が広く公開されており、誰でもそれを分析できることから、アタックを研究することのハードルが低く、精度の高い研究結果が得られる。同様に、インターネット・バンキングに関する技術研究も、金融機関のシステムの挙動をインターネットを通じて外部から観察できるなど、透明性の高い分野であり、実務で使われている技術に近いものが研究室のなかでも実現できる。こうした研究分野については、セキュリティの研究と実務との距離が近く、研究成果を実務に直接参照することができる。

近年、特にインターネット関連システムのセキュリティ分析を巡っては、セキュリティ・コンサルタントにアタックを試みてもらい、その結果を参考に対策を強化することが普通に行われるようになってきた。IC カードや特殊なセキュリティ・モジュールを組み込んだ製品についても、同様の動きが見られる。これは、インターネットにおけるオープンなシステム開発においては、インフラとなる技術仕様や利用しているソフトウエア製品やハードウエア製品の中に秘密の情報が含まれておらず、システム自体が外部からアクセス可能となっているため、そうした外部の専門家の知恵を借りることに伴うリスクが少ないと判断されているためであろう。

これに対して、例えばキャッシュカードや ATM 等、従来から金融分野で利用されてきた技術については、現在では特定の分野以外ではあまり使われない特殊なインフラ技術を利用しているため、金融機関や IT ベンダー以外にセキュリティ評価を依頼できる専門家が存在しないことが多い。システムの仕様も公開されていないため、セキュリティ評価を行う場合でも外部の専門家に頼る訳にはいかないという問題が存在する。

そうした状況となっていることは、金融システムのセキュリティにとっても必ずしも望ましいものではない。わが国の金融機関の情報システムに関する情報がより幅広く公開されていたとすれば、例えば、偽造カード犯罪が深刻化する前に、脆弱性に関する警鐘が強く鳴らされ、事前に何らかの対策を講じることができたかもしれない。

そうした警鐘を鳴らされること自体は、金融機関にとって必ずしも快くないものであろうし、精度の高くない警告が多発する惧れもある。仮に、誤解に基づいてシステムの安全性への批判が喧伝されてしまうと、本来必要ではない部分で対策を講じることを強いられるかもしれない。とはいえ、セキュリティ技術上の欠陥が存在する可能性はゼロにはならないことを考慮すると、何らかの形で情報が金融機関に知らされるルートを作っておくことは有用であろう。こ

うしたテーマについても、金融業界の問題として検討していく必要があり、そのための材料を提供していくことも、本シンポジウムの重要な役割であろう。

６．おわりに――今後の展望

これまで、過去 10 年間にわたる情報セキュリティ・シンポジウムの内容を振り返ってきた。この 10 年間は、金融情報システムのオープン化と情報セキュリティ技術の高度化が進んだ時期であった。こうしたシステム技術面の変化がさらに続いていった場合、金融機関はどのような影響を受けるのだろうか。

かつて、金融機関がレガシー系の技術で等質の情報システムを維持していた時代には、「金融機関であれば、どこのシステムも安全で信頼できる」という意味で、業界全体としてのブランド化が達成されていた。オープン系の安価な技術を導入せず、高価なレガシー系システムを使い続けることにより、そうした「業界ブランド」の価値が維持できてきたと考えられる。

現在、インターネット・バンキングのセキュリティ向上や IC カード、生体認証等への投資を行っているのは、個別企業として、安全性、信頼性のブランドを向上させたいと希望する金融機関のようである。他方、そうした個別ブランド化を志向しない金融機関は、情報セキュリティ対策に、人的、システム的な投資を多くは振り向けていない。当面の間は、そのような投資判断でも特段の問題は発生しないと思われる。むしろ、過去からの慣性として、金融機関であればどこでも安全で信頼できるという「業界ブランド」が維持されている状況であれば、新しい技術にチャレンジせず、現状維持としていた方が短期的には効率的かもしれない。

しかし、問題は、情報化社会が更に進展し、一部の金融機関がシステムのオープン化とセキュリティの高度化を更に進めるなかで、システムの現状維持を選択すると、安全性、信頼性の観点から、業界全体のブランドが維持できなくなる惧れがあることであろう。そして、金融機関のシステムは相互に連携して機能するものであるため、個別企業のシステムだけが優れていても、全体としては利用者の安全を守ることはできないのである。

こうした観点から考えれば、現在進んでいるシステムのオープン化とセキュリティの高度化は、全ての金融機関が対応していかなければならない変化であると考えられる。特に、セキュリティの高度化を進める上では、人材の育成と業界内での適切な情報共有を進めていくことが必要である。日本銀行金融研究所としても、本シンポジウムを今後も継続していくことにより、広く学界、金融業界の方々の理解とサポートを頂きながら、引き続き、その一翼を担っていきたいと考えている。

参考文献

岩下直行、「金融業界における情報システムの脆弱性検知と情報共有」、『金融研究』第 24 巻第 2 号、日本銀行金融研究所、2005 年、19～34 頁

――――、「金融機関の情報セキュリティ対策のあり方について」、『金融研究』第 25 巻別冊第 1 号、日本銀行金融研究所、2006 年、17～29 頁

松本勉・岩下直行、「金融分野における情報セキュリティ技術の現状と課題」、『金融研究』第 18 巻第 2 号、日本銀行金融研究所、1999 年、17～31 頁

――――・――――、「金融業務と認証技術：インターネット金融取引の安全性に関する一考察」、『金融研究』第 19 巻別冊第 1 号、日本銀行金融研究所、2000 年、1～14 頁

――――・――――、「情報セキュリティ技術の信頼性を確保するために」、『金融研究』第 20 巻第 2 号、日本銀行金融研究所、2001 年、21～32 頁