# 第12回
# 情報セキュリティ・シンポジウム
# 「環境変化に耐える情報セキュリティ・システムとは」の模様

## 1. はじめに

日本銀行金融研究所は、2010年3月5日、「環境変化に耐える情報セキュリティ・システムとは」をテーマとして、第12回情報セキュリティ・シンポジウムを開催した（プログラムは次頁のとおり）。

近年、金融分野では、暗号アルゴリズムやICカード等の情報セキュリティ技術を利用したシステム（「情報セキュリティ・システム」。以下、システムと呼ぶ）が普及しつつある。こうしたシステムを中長期にわたって活用していくうえで、情報セキュリティ技術の経年劣化、システムの大規模化や複雑化等の環境変化に対して適切に対応していくことが必要となっている。

こうした問題意識に基づき、本シンポジウムでは、環境変化によるシステムへの影響と対応のあり方について、情報セキュリティに加えて、ヒューマン・エラーへの対応等を考慮したディペンダビリティの観点も踏まえて議論を行った。キーノート・スピーチでは、金融機関を取り巻く環境変化とそれらへの対応に資する情報セキュリティ技術について説明が行われ、リスク管理の精緻化や関係者間の連携の必要性が指摘された。2件の発表では、環境変化への対応の事例として、暗号アルゴリズムの移行問題と、新技術としての非接触ICカードの導入におけるリスク管理のあり方についてそれぞれ説明が行われた。

また、「環境変化に対してロバストな情報セキュリティ・システムを目指して」と題するパネル・ディスカッションでは、4名の専門家をパネリストに迎え、環境変化への対応について議論を行った。その結果、システムの情報セキュリティに関する説明責任（アカウンタビリティ）を金融機関が果たしていくことが必要であるとの認識が各パネリストから共通に示された。そのうえで、説明責任を果たしていくた

本稿に示された意見はすべて発言者ら個人に属し、その所属する組織の公式見解を示すものではない。

めには、①情報技術に対するリテラシーの向上、②第三者によるシステムの評価・認証制度の活用、③障害データの積極的な公表等への取組みが重要であるとの意見が示された。また、情報セキュリティやディペンダビリティに関する対応を検討する際には、④これらの分野の専門家に積極的に相談し、その知見を活用することが有用であるとの意見も示された。

本シンポジウムのフロアには、情報セキュリティ対策にかかわる金融機関の実務家や官庁関係者、暗号学者、ベンダーにおいてシステムの開発・運用に携わる実務家や技術者等、約 100 名が参加した。

以下では、プログラムに沿って、本シンポジウムの概要を紹介する（以下、敬称略、文責：日本銀行金融研究所）[1]。

【第 12 回情報セキュリティ・シンポジウムのプログラム】

- キーノート・スピーチ「環境変化に耐える情報セキュリティ・システムとは」
  ――松本　勉（横浜国立大学大学院教授）
- 発表 1「暗号アルゴリズム移行問題とその対応」
  ――鈴木雅貴（日本銀行金融研究所）
- 発表 2「金融機関は新技術とどう向き合うべきか」
  ――廣川勝久（日本銀行金融研究所テクニカル・アドバイザー）
- パネル・ディスカッション
  「環境変化に対してロバストな情報セキュリティ・システムを目指して」
  - パネル発表 1：南谷　崇（東京大学教授）
  - パネル発表 2：岩野和生（日本アイ・ビー・エム株式会社執行役員）
  - 自由討議
    - パネリスト：松本、南谷、岩野、廣川
    - モデレータ：宇根正志（日本銀行金融研究所企画役）
- 総括コメント――今井秀樹（中央大学教授）

## 2. キーノート・スピーチ「環境変化に耐える情報セキュリティ・システムとは」

松本は、金融機関のシステムにおける環境変化や、そうした変化への対応に資する情報セキュリティ技術等について次のとおり発表を行った。

1 文中における各参加者の所属および肩書きはシンポジウム開催時点のものである。

## (1) 金融機関のシステムにおける環境変化とその影響

近年、金融機関のシステムにおける環境が大きく変化してきている。技術面では、最近の暗号アルゴリズムの安全性低下に関する問題に代表されるように、技術の経年劣化が環境変化の 1 つとして挙げられる。また、IC カードや生体認証等の新技術の登場も重要な環境変化といえる。金融機関では、こうした新しい技術を金融サービスに活用してきている。新しい技術を利用するに当たっては、セキュリティ評価の手法が十分に確立されていないケースが少なくないため、新たな脅威や脆弱性が出現する可能性に留意しておく必要がある。また、広く利用されている技術の場合には、提案されてから相応の時間が経過している場合が多く、研究対象としての学界の関心が失われてしまうという傾向が強い。したがって、古い技術の経年劣化の状況を学界の動向から把握することが難しいというのが実情である。

管理・運用面での環境変化としては、インターネット等の外部システムとの相互接続や複数の金融機関におけるシステムの統合・共同利用等、システムのオープン化・複雑化が顕著である。この結果、他のシステムの障害等による影響が高まってきているほか、システム全体における脆弱性の把握が困難になってきている。また、システムの管理者やエンドユーザー等の関係者が多様化し、各エンドユーザーのリテラシーの程度も区々であるため、環境変化への対応が金融機関だけでは実施困難になってきている。

## (2) 環境変化への対応に資する技術

こうした環境変化への対応に資する情報セキュリティ技術が研究されている。具体的には、一定の安全性を証明可能な技術や、大幅な修正を加えることなく新たな脅威にも対応できる技術が挙げられる。

安全性証明可能な技術は、環境変化により攻撃手法が高度化していくなかで、一定の条件が満たされる限り、そうした影響を受けずに安全性が保証されるというものである。例えば、安全性が攻撃者の計算能力の向上に左右されない暗号技術や、一定の安全性を有する暗号モジュールにおいて、それらを組み合わせて使用した場合であっても、個々の暗号モジュールの安全性が損なわれないという性質をもつ技術が挙げられる。安全性が計算能力の向上の影響を受けない技術については、長期間修正を加えずに利用可能な性質（メンテナンスフリー性）を重視するインフラ系のシステムにおいて今後有益な技術になると考えられる。

新たな脅威に対応可能な技術に関しては、新たな脅威が出現した場合に、その脅威を追加的に学習するといった技術が研究されている。例えば、新しいウイルスが出現した場合に、当該ウイルスだけでなく、それをベースに作成される「亜種ウイルス」を予測して対応するという技術が挙げられる。このほか、生体認証システムへのなりすましに利用される人工物（ゼラチン製の指等）について、新しい手法で

作製された人工物を検知・排除するように追加的に学習するという技術も研究されている。

### (3) 環境変化に対応する際の留意点

金融機関が環境変化へ適切に対応していくためには、そうした変化を前提として、システムで利用している技術の安全性評価やシステム全体の脆弱性の洗出しを実施するなど、システムのリスク分析をより精緻化することが必要である。環境変化への対応に資する新しい情報セキュリティ技術の活用を今後検討することも有用である。さらに、エンドユーザーを含むシステムの関係者とリスクに関する認識を共有し、連携して取り組む姿勢が求められる。抱えている問題やニーズを必要に応じて技術の専門家に伝え、専門家の知見を活用していくという姿勢が重要であろう。

## 3. 発表1「暗号アルゴリズム移行問題とその対応」

鈴木は、宇根・黒川・鈴木・田中［2010］と松本・宇根［2010］に基づき、暗号アルゴリズムの移行問題について次のとおり発表した。

### (1) 暗号アルゴリズムの経年劣化

金融機関では、インターネット・バンキング等においてさまざまな暗号アルゴリズムを利用している。例えば、鍵長1,024ビットのRSA（1,024ビットRSA）は、2000年頃から金融機関のサーバーの認証等に利用されている。しかし、近年では、一部の暗号アルゴリズムの安全性低下が顕著となってきており、1,024ビットRSAは、2010年代後半に解読されるおそれがあるとみられている。こうした暗号アルゴリズムの安全性低下は、「攻撃手法の高度化」「計算機性能の向上」といった環境変化によって引き起こされたものといえる。

暗号アルゴリズムが解読された場合には、金融機関のサーバーへのなりすましや金融取引データの改ざん等につながる可能性がある。このため、暗号アルゴリズムを利用する立場からは、各アルゴリズムの利用可能な期間が関心事項となる。金融業界では、金融サービスに関する国際標準化を担当しているISO/TC 68において、推奨される暗号アルゴリズムや使用推奨期間が検討されるなど（図表1参照）、暗号アルゴリズムの移行に向けた対応が進められている。

図表 1　ISO/TC 68 が公表する暗号アルゴリズムの使用推奨期間（一部）

| | 共通鍵暗号 | | | ハッシュ関数 | | 公開鍵暗号 | |
|---|---|---|---|---|---|---|---|
| | 2-key トリプル DES | 3-key トリプル DES | AES | SHA-1 | SHA-256 | 1,024 ビット RSA | 2,048 ビット RSA |
| 使用推奨期間 | 条件付きで最長 2030 年末 | 2030 年末 | 2030 年超 | 2010 年末 | 2030 年末 | 2010 年末 | 2030 年末 |

## (2) 暗号アルゴリズム移行の際の留意点

暗号アルゴリズムを新しいものに移行する際には、まず、次世代の暗号アルゴリズム（新アルゴリズム）の選定や移行開始時期を決定することが必要となる。新アルゴリズムの使用を開始した後、新旧の暗号アルゴリズムのいずれも使用可能な期間を設けたうえで、古い暗号アルゴリズムの使用を終了させることとなる。例えば、EMV 仕様[2]の事例をみると、IC カード認証に利用する RSA の鍵長について、複数の選択肢を用意し、鍵長ごとに使用推奨期間を規定している[3]。これにより、鍵長に関する移行の円滑化を図っている。

暗号アルゴリズムの移行を検討する際には、暗号アルゴリズムの安全性低下による影響や移行に要する時間を見積もるほか、移行完了前に当該アルゴリズムが解読された場合の対応を明確にしておくことが重要である。特に、移行に要する時間については、複数のシステムが相互接続されている場合や、エンドユーザーの端末の OS やブラウザーの設定が多様化している場合、関係者間の調整に相応の時間が必要となり、移行に要する期間が長期化する可能性がある。

## (3) 今後の対応のあり方

今後もシステムのオープン化やユーザー等の関係者の多様化により、金融機関が直接制御困難な要素が増加し、移行に要する期間が長期化する方向に進むとみられる。外部のシステムの関係者においても対応が必要となるケースについては、関係者との問題意識の共有やシステムの更新に向けた体制の整備を予め進めておくことが重要である。

2 EMV 仕様：クレジットカード取引等における IC カードと端末に関する国際的な業界標準であり、これらのデータ体系や処理内容に加えて、推奨する暗号アルゴリズム等を規定している。本仕様の改訂・管理は EMVCo が行っており、 2008 年に公表された EMV 4.2 が最新版である。

3 2009 年に公表された EMV 仕様の付属文書によると、鍵長 1,024 ビットは 2012 年末までの使用が推奨されているほか、同 1,152 ビットは 2016 年末まで、同 1,408 ビットと同 1,984 ビットはいずれも 2019 年末までの使用がそれぞれ推奨されている。これらの使用推奨期間は毎年見直しが行われている。

また、普及している暗号アルゴリズムは古いものが多く、それらは学術研究の対象として学界で議論されなくなる傾向にある。こうした点を踏まえると、学界における最新の研究成果のみを参照し、問題点の指摘が行われていないという事実をもって暗号アルゴリズムの安全性を判断することは必ずしも適切とはいえない。金融機関は、古い暗号アルゴリズムの安全性評価を専門家に依頼するなど、自らリスクを把握する努力を行うことが求められる。

## 4. 発表２「金融機関は新技術とどう向き合うべきか」

廣川は、廣川［2010］に基づき、新しい技術の採用がシステムに与える影響とそうした際のリスク管理上の留意点について、非接触 IC カードの事例を交えて次のとおり発表した。

### (1) 新しい技術による影響とリスク管理

金融機関は、これまで新しい情報技術を活用しながら新しい金融サービスを開発・提供してきた。古くは、磁気カードの登場により ATM 取引が可能になったほか、1980 年代には IC カードを活用したキャッシュレス・ショッピングやファーム・バンキング等の検討が開始された。こうした新しい技術の利用によって、金融機関のシステムにさまざまな変化が生じるほか、管理・運用面においても、関係者やその役割が変化していくことになる。

新技術の利用に伴うこうした環境変化は、新たなリスクを発生させる可能性がある。リスクへの対応という観点では、まずビジネス要件を定義し、守るべき資産を明確にすることが必要である。そのうえで、セキュリティ要件を洗い出し、リスク管理を行うことになる。その際、関連技術や環境の変化による影響をシステムに反映させるために「エンタープライズ・アーキテクチャ[4]」の考え方を参考にすることが有用である。

### (2) 社会的安心の獲得のために

新しい技術を利用する際には、そうした技術への社会的安心を獲得するための取組みが必要である。新しい技術が導入された当初は、十分な運用実績がなく、社会的に広く認知されていない場合がある。そうした際には、例えば、専門家による客観的

4 エンタープライズ・アーキテクチャ（Enterprise Architecture）：業務プロセスやシステムの構造に基づいてシステムの理想形と現状を分析し、関連技術や環境の変化を踏まえて次に目指すべきシステムの形態を明確にする手法である。本手法では、政策・業務体系、データ体系、処理体系、技術体系の観点から、システム全体が最適化されるように分析を行う。

なセキュリティ評価結果を示すことが有用である。IC カードを用いたシステムの場合には、業界独自の認定スキームのほかに、コモン・クライテリア[5]や JCMVP[6]等の枠組みを活用することが考えられる。コモン・クライテリアでは、対象製品の開発者が定めたセキュリティ機能とその実装について評価が行われる。したがって、評価結果を参照する際には、実装されたセキュリティ機能が目的とするシステムの運用環境に適合していることを確認することが求められる。仮に、適合しない場合には期待したセキュリティの効果を得ることができない可能性がある。

### (3) 新技術を用いたシステムの事例

新技術として非接触 IC カードを利用した電子マネー等のリテール取引の事例を取り上げる。非接触 IC カードの利用によって、取引時にカードを財布等から取り出して端末に挿入する必要がなくユーザーの利便性が向上する。しかし、非接触 IC カードは、電力供給の制約により利用可能な暗号機能が制限される場合があり、IC カード（端子付き）と同一のセキュリティ機能を提供できない状況も生じる。また、電子マネー等のリテール取引におけるシステムでは、利用範囲の拡大に伴い加盟店や電子マネー発行者等の関係者が変化していくことに留意する必要がある。

こうした変化を十分考慮してリスク管理を行うことが重要である。その際、利便性等に配慮しつつ、リスクに見合う対策を必要に応じて講じることが求められる。例えば、運用面での対策として、用途の限定や取引限度額の引下げ等が考えられる。

### (4) 環境変化への対応における留意点

新しい技術の活用によって、さまざまな環境変化が発生し、その結果としてリスクも変化する。ビジネス要件やセキュリティ要件を明確にしたうえで、システム全体における利便性とリスクのバランスを図っていくことが求められる。特に、重要インフラの一角を担う金融機関においては、金融サービスに対する社会的な安心を獲得することが重要であり、ビジネスを健全に発展させていくことが期待される。

5 コモン・クライテリア（Common Criteria）：情報システムや製品が一定のセキュリティ要件を満足していることを評価・認証するための枠組みであり、国際標準（ISO/IEC 15408）として制定されている。

6 JCMVP（Japan Cryptographic Module Validation Program）：暗号化やデジタル署名等のセキュリティ機能を実装したハードウエアやソフトウエアが、適切に実装され、かつ、暗号鍵等の秘密情報を適切に保護できることを、第三者が試験・認証するための制度である。

## 5. パネル・ディスカッション

パネル・ディスカッションでは、南谷と岩野から、環境変化への対応に資する技術についてそれぞれパネル発表が行われた後、自由討議等が行われた。

### (1) パネル発表 1

南谷は、ディペンダビリティに焦点を当てて、情報セキュリティとの関係、研究動向、環境変化への対応のあり方について次のとおり説明した。

ディペンダビリティは、「自然現象、経年劣化、設計ミス等、偶発的な障害原因（フォールト）が発生しても仕様どおりのサービスを提供できる」というシステムの属性である。一方、情報セキュリティは、意図的な不正アクセスや不正操作等を前提としたうえで、「情報をその生産者、運用者、利用者が合意した意図のとおりに利用できることを保証する」というシステムの属性である。情報セキュリティの分野では、操作ミスによる暗号鍵の漏洩や設計ミス等の偶発的なフォールトを想定していない。したがって、情報セキュリティを確保するためにはディペンダビリティを考慮する必要がある。

ディペンダビリティを確保する方法として、フォールトを予防・除去・予測する方法のほかに、処理の多重化のように、フォールトが発生してもシステム全体としては正常な処理が維持されるようにする方法が研究されている。ディペンダビリティの評価では、障害が発生する確率をフォールトの発生確率等に基づいて見積もる方法や、システムをソフトウエア等でシミュレートして評価する方法等が開発されている。しかし、複雑なシステムについてはディペンダビリティを評価する手法が十分に確立しているとはいえず、ディペンダビリティ確保にどの程度の投資を行うのが適切かを判断することが困難となっている。

過去 40 年間をみると、計算機性能は 10 億倍になり、インターネットも小規模ネットワークからネットワーク人口 10 億人の大規模なものに成長した。一方で、システムを管理する人間の能力は 40 年前と変わっておらず、設計や操作のミス等の人為的フォールトが深刻な問題になっている。環境変化に対応していくためには、こうした人為的フォールトに加えて、複数のシステムを組み合わせることで初めて顕現化する相互作用的なフォールトへの対応が重要になってきている。また、システム全体のディペンダビリティを評価する手法の確立も重要な課題である。

### (2) パネル発表 2

岩野は、システムが複雑化するなかで、人間によるシステムの管理を支援する技術について次のとおり説明した。

システムのオープン化等に伴ってシステム全体が複雑になり、脆弱性の把握が困難になってきている。システムにおける障害の約 8 割は人為的フォールトであるといわれており、人間が管理できる限界を超えつつある。また、企業の情報技術への投資の約 8 割は維持・管理費であるといわれており、システムの維持・管理の負担が非常に大きくなってきているとみられる。

こうした課題への対応として、予め設定したポリシーに従い、システム自身が状況に応じて自律的に判断・対応するというコンセプトに基づく「オートノミック（自律型）・コンピューティング」が 2001 年頃から研究されている。こうした研究の流れのなかで、本コンセプトに基づく技術がクラウド・コンピューティング等において実用化されているほか、システムの構成要素間でやり取りされるデータ等に関する標準化が進められている。

また、近年では、高い業務継続性が重視されるアプリケーションにおいて、人間によるシステムの管理を支援する技術へのニーズが高まっている。例えば、電力や物流等の物理インフラの状態をリアルタイムに把握したうえで、物理インフラでの処理が最適化されるようにフィードバックするという処理を行う技術が挙げられる。さらに、脆弱性の顕現化を予測して事前に対応するとともに、ビジネス戦略や業務プロセス等の観点から整合的に業務継続の方針を設定するというアプローチの技術が研究されている。障害が発生しても業務を継続できるようにする、あるいは、システムが停止しても早急に復旧するという本技術のコンセプトは「レジリエンス（resilience）」と呼ばれており、ディペンダビリティに近い概念であるといえる。さらに、レジリエンスの観点からシステムへの要求を明確にしたうえで、それに合致した技術や業務プロセス等を選択し、システム全体のレジリエンスを確保するという手法（「レジリエンス・パターン」と呼ばれる）に関する議論も行われている。

金融機関を含め、企業のシステムに対する社会の要請は多様化してきており、レジリエントなシステム等を含めて、企業の目的に沿ったシステムを構築・運用していくことが求められている。

### (3) 自由討議

自由討議では、環境変化に対する金融機関の対応について、フロア参加者からの質問も交えつつ議論を行った。概要は次のとおりである。

#### イ．パネリストによる議論

##### (イ) 説明責任について

金融機関のシステムに対するニーズとして、岩野は、システムのセキュリティやディペンダビリティに関する説明責任が強く求められるようになってきたとの見方を示した。例として、金融機関では取引先企業や顧客等に関する大量のデータを扱

うようになっており、こうしたデータの管理の適切さを関係者に示すことが求められていると説明した。これを受けて、松本は、説明責任の形態として、金融機関が他の企業や顧客に果たすケースと、ベンダーやアウトソース先が金融機関に果たすケースがあると説明した。また、何を示すことができれば説明責任を果たしたことになるかが明確になっていないと指摘した。

説明責任をどのように果たしていくかについて、南谷は、技術の効果が評価できない場合には投資判断が難しくなるが、一方で、システムに欠陥がないことを証明するといった問題のように本質的に解決困難な問題があると述べた。そのうえで、こうした問題に対しては、技術に関する不利な情報も含めて開示することによって、「自信があるからオープンにしている」と判断され、当該技術への信頼が高まる傾向が最近みられるようになってきていると説明した。技術の情報をオープンにするという観点から、松本は、IC チップへの暗号アルゴリズムの実装において、コモン・クライテリアや JCMVP 等の枠組みを利用することで説明責任を果たすことが可能になる場合も考えられると説明した。そのうえで、生体認証システム等、評価の枠組みが整備されていないものも存在しており、今後の重要な課題であると指摘した。

（ロ）ディペンダビリティ確保に向けた取組みについて

システム全体のディペンダビリティを確保するためのアプローチに関して、南谷は、プロセッサーやモジュール等のレベルにおいてディペンダビリティを確保する方法が確立されつつあると紹介した。そのうえで、状況に合わせて最適な方法を組み合わせることによって、システム全体のディペンダビリティを確保するという手法の検討が今後進展するのではないかと説明した。同様に、岩野は、オートノミック・コンピューティングにおいても、システム全体の業務継続性等を確保するために、ビジネス戦略、組織の体制、業務プロセス等のレイヤーごとにポリシーを設定したうえで、システム全体を構築するというアプローチが注目されていると述べた。これを補足するかたちで、南谷は、金融機関のシステムのディペンダビリティを検討する際に、電力や情報通信等の他のインフラとの関係についても十分に考慮する必要があると強調した。

こうした問題を難しくしている要素の１つとして、松本は、レガシー系システムを維持したままシステムの更改等を行う必要がある点を挙げた。そのうえで、レガシー系システムをいつまで利用し続けるかといった使用期限等の設定が重要になると述べた。金融機関のレガシー系システムに関する対応について、岩野は、システム更改の際にレガシー系システムと他のシステムとの連携を図るために、レガシー系システムの入出力を変換するレイヤーを新たに追加するなどの対応が必要となった事例があると紹介した。そのうえで、こうした対応が、システム全体をより複雑なものにすると同時に、新しい技術への移行のハードルを高めてしまっているとの見方を示した。

廣川は、古い技術が長期間利用され続ける場合はそれがセキュリティ・ホールと

なりうるため、新技術への移行を促進するためのビジネス的な施策も必要になると説明した。具体例として、クレジットカード業界では、IC カードに移行済みの国で発行された IC・磁気併用カードが、磁気カードのみの環境にとどまっている国において磁気カードとして不正使用された場合には、磁気カードのみにとどまっている国により多くの責任を課している旨を紹介した。また、廣川は、異なる仕様のシステムを共存させる場合のアプローチとして、各システムに共通な部分を合意仕様とし、各システムに固有の部分をオプションとする方法を紹介した。そのうえで、本アプローチは、EMV 仕様と各国際ブランド固有仕様との関係で具体化されており、システム全体の共通化を図りつつ独自部分の追加を可能としているという点でビジネス的にもメリットがあると説明した。

## ロ．フロアからの質問

### （イ）製品やシステムに関するデータの公表について

フロア参加者から、説明責任を果たすために障害データ等の自社の製品やシステムに不利な情報を公表した場合、受け手のリテラシーによっては逆に不安に感じてしまう可能性があるのではないかとの質問が寄せられた。

これに対して、南谷は、ディペンダビリティの分野においても、かつては、障害データを公表すると自社製品の不利益につながるとの判断から、そうしたデータを公表しないという考えが支配的であったと紹介した。そのうえで、最近は、関係者の考え方が変わってきており、自分のシステムに自信があるからそうしたデータを公表していると理解されるようになってきていると説明した。また、廣川は、サービス提供者、システムの外部委託業者、ユーザー等の間で、障害データ等の公表に対する認識を共有していくことが重要であると指摘した。

松本は、そうした障害データが情報セキュリティにおける脆弱性情報に相当するとの見方を示した。そのうえで、わが国の脆弱性情報届出制度においては、脆弱性への対応を実施した後にそうした情報が公表されていると述べた。さらに、松本は、研究成果の公表に関連して、例えば、学会で発表されたコンピュータ・ウイルスの解析結果を攻撃者が学習し、より強力なコンピュータ・ウイルスを作成する可能性があるため、研究者は、攻撃者に学習された場合への対策まで想定したうえで研究成果を公表する必要があるのではないかとの問題提起を行った。これに関連して、南谷は、人為的フォールトについては評価手法が十分に確立されていないものの、そうしたフォールトに基づく障害データが公表されるケースがあると説明し、必ずしも対策が検討されている障害データだけが公表されているわけではないと述べた。人為的フォールトの評価手法の確立について、岩野は、そうした障害データの蓄積が研究を進めるうえでは有用であるものの、企業が障害データをそのまま公表することは難しいとの見方を示した。そのうえで、人為的フォールトについて分析可能な程度に加工した後に障害データを公表するという方法を今後検討していく必要があると説明した。

（ロ）模擬攻撃の必要性について

フロア参加者から、EMV 仕様における取組みのように強制力がある場合には技術の移行がスムーズに進むとみられるが、一般的には、環境変化によるリスクを適切に評価することが難しく、事件や事故が発生するまで対応実施のモチベーションが高まりにくいとの意見が示された。そのうえで、実際に運用されているシステムに対して演習として模擬攻撃を実施し、耐性があるかを確認するというアプローチが有効ではないかとの質問が寄せられた。

リスク評価に関して、南谷は、トヨタの ABS 制御プログラムに関連したリコール問題では数千億円の損失が発生する見込みとの報道もあるが、こうした損失を見積もることによって環境変化への対応に関するモチベーションが高まるのではないかと説明した。クレジットカード業界の状況について、廣川は、磁気カードを利用し続けた場合の損失や IC カードへ移行する際の投資額等を踏まえ、IC カードへの移行が判断されていると説明した。そのうえで、ビジネス要件やセキュリティ要件を明確化し、環境変化がシステムに与える影響を検討したうえで、利用する技術の見直しを行うことが重要であると強調した。また、松本は、模擬攻撃のアイデアに賛意を示したうえで、例えば、磁気カードを利用しているシステムに対して模擬攻撃を実施するというアイデアが考えられると述べた。

### ハ．金融機関への期待

自由討議での議論を踏まえて、金融機関に対する期待等について、各パネリストから次のとおり発言があった。

岩野は、重要インフラとして金融機関が果たす役割は拡大しており、そうしたなかで金融機関のシステムのディペンダビリティをどのように確保していくかを改めて検討する必要があると説明した。松本は、新しい技術を積極的に活用する攻めの姿勢を期待するとともに、何か問題を抱えている場合には専門家に是非相談してほしいと述べた。廣川は、変化する環境のなかでビジネスの目的とセキュリティ要件を再確認し、それに基づいてシステムの構築・レベルアップを行うことが重要であると述べた。南谷は、情報化社会を生き抜くためには情報技術の積極的な活用が鍵であり、特に金融機関の経営層には情報技術の利点や欠点を十分理解することが求められると説明した。

## 6．総括コメント

今井は、シンポジウムの内容を振り返ったうえで次のとおりコメントを行い、シンポジウムを締め括った。

今回のシンポジウムでは、「環境変化に耐える情報セキュリティ・システムを構築するためには何が求められるか」という金融業界にとって重要なテーマが取り上げられた。金融機関は、システムのオープン化、新たな脅威や脆弱性の出現、他のシス

テムの障害による影響の増大といった新たな問題に直面しており、更なる対応が求められている。学界でもこうした問題に関する議論が活発化しており、タイムリーなテーマであった。

パネル・ディスカッションでは、環境変化に関係する問題として、レガシー系システムの取扱い、社会的な安心の獲得における説明責任の重要性、障害データの公表のあり方等、さまざまな論点が取り上げられ、大変興味深い内容であった。特に、障害データの公表については、日本学術会議の提言にもあるように、障害発生時にそうしたデータを管理・分析する第三者機関の設立等、今後の重要な課題として認識されている。

技術と運用の双方から環境変化に対応していくためには、金融機関はシステムで利用している技術の効果と限界を常に把握していることが必要となる。日本銀行金融研究所情報技術研究センターには、そうした金融機関を支援する活動を今後も継続していただきたい。また、重要インフラとしての金融業界の情報セキュリティやディペンダビリティを確保していくためには、業界全体で取り組む必要がある。金融分野におけるセプター[7]の役割も一層重要になってくると考えられる。今回のシンポジウムの議論を契機に、金融業界における検討が一層進展することを期待したい。

7 セプター（CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response）：重要インフラ（金融、電力、情報通信等）における情報セキュリティ向上等を目的に、各業界内において情報の共有や分析を行うために設立された組織。また、セプター間の業界横断的な連携を目的として「セプター・カウンシル」が設立されている。

## 参考文献

宇根正志・黒川貴司・鈴木雅貴・田中秀磨、「暗号ユーザーが暗号アルゴリズムの安全性評価結果をどう活用するか」、『金融研究』第 29 巻第 2 号、日本銀行金融研究所、2010 年 4 月、201～228 頁

廣川勝久、「非接触インタフェース経由取引の技術とビジネスリスク管理の課題」、『金融研究』第 29 巻第 4 号、日本銀行金融研究所、2010 年、79～106 頁〈本号所収〉

松本　泰・宇根正志、「SSL 証明書における暗号アルゴリズム移行の現状と今後の課題」、『金融研究』第 29 巻第 4 号、日本銀行金融研究所、2010 年、107～130 頁〈本号所収〉