第7回情報セキュリティ・シンポジウム「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」の模様

１．はじめに

日本銀行金融研究所は、平成17年3月29日、「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」をテーマとして、第7回情報セキュリティ・シンポジウムを開催した。

現在の金融業界の情報システムは、コンピュータ・ウィルスから、フィッシング詐欺、個人情報漏洩、偽造キャッシュカードによる不正預金引出しに至るまで、さまざまな脅威にさらされている。重要インフラの1つである金融業界には、こうした脅威の原因となっているシステムの脆弱性を的確に検知し、これを是正することが求められている。

今回のシンポジウムでは、まず、金融業界の情報システムにおける脆弱性とその対応状況について説明し、問題提起を行った。そのうえで、そうした脆弱性の具体例として、生体認証技術やデジタル署名の長期利用技術に関する最近の研究成果を報告するとともに、今後、金融業界がこうした問題に適切に対処していくために脆弱性検知や情報共有をどのように進めていくべきかについて議論した。

シンポジウムは、開会挨拶、キーノート・スピーチ、2件の研究発表、パネル・ディスカッション、総括コメントによって構成された（プログラムは次頁のとおり）。フロアには、金融業務における情報セキュリティ対策を担当している金融機関関係者のほか、暗号学者、金融業務と情報セキュリティ技術に関係の深い官庁関係者、電機メーカーの研究開発部門・標準化部門の実務家や技術者約150名の参加を得た。

- **開会挨拶：**翁邦雄（日本銀行金融研究所）
- **キーノート・スピーチ：**「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」― 岩下直行（日本銀行金融研究所）
- **研究発表1：**「生体認証システムにおける脆弱性について―身体的特徴の偽造に関する脆弱性を中心に―」― 松本勉（横浜国立大学教授）
- **研究発表2：**「デジタル署名の長期利用に係る脆弱性」― 宇根正志（日本銀行金融研究所）
- **パネル・ディスカッション：**「情報システムの脆弱性検知と情報共有―金融業界へのインプリケーション―」
  - **パネル発表1：**「情報システムの脆弱性対策―情報セキュリティ早期警戒パートナーシップの全体構成と運用状況―」― 早貸淳子（情報処理推進機構セキュリティセンター）
  - **パネル発表2：**「Telecom-ISAC Japan、SPREADを通した情報共有について」― 中尾康二（KDDI（株）技術開発本部）
  - **パネル発表3：**「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」― 高木浩光（産業技術総合研究所グリッド研究センター）
  - **自由討議**
    ― パネリスト：松本勉、早貸淳子、中尾康二、高木浩光
    ― 司会：岩下直行
- **総括コメント：**今井秀樹（東京大学教授）

（備考：所属についてはシンポジウム当日現在のもの。）

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（文責、日本銀行金融研究所。文中敬称略）。

2．開会挨拶

翁は、本シンポジウムの開会に当たり、以下のように挨拶を行った。

今回のシンポジウムでは、「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」をテーマとして掲げることとした。現在、金融機関の情報システムにおいては、フィッシング詐欺や偽造キャッシュカード問題等の脆弱性問題が社会的関心を集めているが、今回のシンポジウムが、関係者間における脆弱性情報の取扱いについての議論を深める一助になればと考えている。

また、日本銀行金融研究所では、金融業界が情報化社会において直面している課題に適切に対処していくことをサポートするために、現在の情報技術研究担当の研

究活動をより強化することを展望して、平成17年4月1日付けで情報技術研究センター（CITECS：Center for Information Technology Studies、日本語呼称：サイテックス）を設立することとした。CITECSでは、金融サービスの発展や金融システムの安定確保を図っていくうえで重要性が一層高まってきている情報技術の基盤構築に研究面から貢献していくことを予定している。具体的には、①新しい情報セキュリティ技術等の研究・開発、②金融業務に係る技術の国際標準化の推進、③重要情報インフラ保護対策への貢献等の役割を担っていくことを想定している。CITECSが金融界・学界・IT実務家間の掛け橋となり、金融業界における情報システムのセキュリティ強化に貢献できるよう、CITECSの機能の強化を図っていきたい。

３．キーノート・スピーチ「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」

岩下は、標記論文[1]に基づき、金融業界における情報システムの脆弱性検知や情報共有に関する現状と課題について以下のとおり発表した。

（1）金融ハイテク犯罪と銀行の対応

歴史的建造物となっている古い銀行の建物は、レンガや花崗岩の外装等、頑丈な外観を持つものが多い。こうした外観は、銀行が地震・火災・盗難等の脅威に対して高い安全性を有していることをアピールするものであり、銀行の顧客からみれば信頼の象徴といえるものであった。同様に、1970年代に構築された第2次オンライン・システム以来、銀行のオンライン・システムもこれまで高い頑健性、安全性を実現していると考えられてきた。キャッシュカードやCD/ATMの基本設計は、30年間にわたって維持されてきた。

しかし、偽造キャッシュカード事件、フィッシング詐欺事件、インターネット・バンキングにおける不正送金等の金融ハイテク犯罪の発生によって、銀行のセキュリティに関する顧客の信頼は揺らぎつつある。金融ハイテク犯罪の手口は高度化しており、常に最新のセキュリティ対策を講じていくことは、銀行にとっても容易ではない。銀行は、自らの情報セキュリティ対策の信頼性について、顧客に積極的にアピールし、その信認をつなぎとめることが求められている。

1 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」、本号所収。

（2）偽造キャッシュカード問題とその教訓

全国銀行協会によれば、偽造キャッシュカードによる預金引出しは平成15年度以降急増し、昨年4～12月の被害額は8億円に達した。被害額自体はプリペイドカードやクレジットカード等に比べて小さいものの、一般の預金者が被害に遭う可能性があるほか、被害額が銀行によって補償されない可能性があるため、偽造キャッシュカード事件は大きな社会問題として注目を集めている。

現在の磁気ストライプのキャッシュカードが認証手段として十分な強度を有していないことは、平成11年に開催した第2回の本シンポジウムのキーノート・スピーチ「金融業務と認証技術」において指摘しており、当時から認識されてはいた。全国銀行協会は、昭和63年にICカードの業界標準を制定する等、ICカードへの移行の準備を進めていた。しかし、過去30年間利用されてきた技術に特段の問題がみられず、新しい技術に移行するきっかけがつかめなかったほか、金融業界全体の基本インフラを変更することに関する業界内の幅広い合意が得られなかったこと等から、ICカードや生体認証等の新技術の導入に係る意思決定が先送りされてしまった。本来であれば、金融業界が自らの判断で将来発生しうる脅威を想定して既存の技術の脆弱性を評価し、戦略的に新しい技術に移行するのが望ましい展開であった。今回の偽造キャッシュカード問題を奇貨として、銀行の情報システムの脆弱性を正確かつタイムリーに検知し、その是正に戦略的に対応していく体制を構築していくことが必要となってきている。

（3）インターネット・バンキングのセキュリティに関する銀行の対応

インターネット・バンキングに関しても、フィッシング詐欺メールやキー・ロガーに用いたログインID、パスワードの盗用等が問題となっている。こうした問題は、金融業界の根幹となる勘定系のシステムがレガシー技術によって構築されていること等から、銀行の情報システムの脆弱性として位置付けられないことが多い。しかし、顧客とのインターフェース部分にはインターネット技術が利用されており、仮にそこに問題が発生すれば、業務全体が影響を受ける可能性がある。このため、金融業界は、インターネットの脆弱性の影響をより深刻に受けるという意味で、インターネットにコミットした業界であり、インターネット経由でサービスを提供する際のセキュリティ対策について真剣に取り組む必要がある。

（4）銀行の情報システムにおける脆弱性の位置付けと対応

脆弱性（vulnerability）は、一般に、傷つきやすさ、攻撃に対するもろさを意味するが、セキュリティの文脈では、システムの機能や性能を損なう問題箇所、といった意味で使われることが多い。その定義は利用目的によってさまざまであるが、狭義の定義によれば、その対象範囲は実装されたソフトウエア製品のみとなっている

ほか、広義の定義では当該システムに採用されている要素技術から実際の運用方法までが対象とされている。

金融業界内で検知と情報共有を行っていくべき脆弱性の範囲は、できるだけ広くとっておくことが適当である。情報システムの要素技術としては、暗号アルゴリズムやハッシュ関数、生体認証の基礎技術等が含まれるが、それらの脆弱性は、主として学者・研究者によって検知され、学術雑誌等で情報共有されることが多く、脆弱性の情報とその影響範囲を業界内に迅速に伝える枠組みが必要である。業務アプリケーションや運用方法については、個別性が高く、外部からの脆弱性の指摘や情報共有にそぐわないものも多いため、各銀行が自らチェックできることが望ましい。

ソフトウエア製品やウェブ・アプリケーションの脆弱性情報については、平成16年7月から開始された脆弱性関連情報届出制度によって入手できる。本制度によって入手できる脆弱性情報のうち、コンピュータ・ウィルス、サーバ・プログラムやハードウエアの欠陥を突いた攻撃等、どのユーザにも発生しうる一般的な攻撃に関するものについては、金融業界も汎業界的な対策を積極的に利用することができる。これに対して、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、インターネット・バンキングでの不正送金のように、銀行のシステムに固有の攻撃に対しては、脆弱性の検知や情報共有のための枠組みが整備されておらず、今後の検討課題である。

海外の事例をみると、フランスでは、約20年前に国を挙げてキャッシュカードのICカード化に取り組み、国内の銀行取引カードをすべてICカード化することに成功している。ドイツでは、磁気カードに独自の偽造防止技術を組み入れることによってスキミングの被害を抑制している。米国では、業界内で脆弱性情報を検知、共有する仕組みとして、ISAC（Information Sharing and Analysis Center）と呼ばれる組織が設立されている。なお、日本でも、情報通信業界において平成14年7月にインシデント情報共有・分析センター（Telecom-ISAC Japan）が組成され、活動を開始している。

（5）今後の課題

金融業界が巨大な情報システムを管理する装置産業である以上、そこで利用されている技術を分析・研究して脆弱性を検知し、脅威を未然に取り除くことは金融業界自身にとって当然の責務である。銀行は、自らの情報システムの脆弱性を正確かつタイムリーに検知してその情報を業界内で適切に共有し、その是正に戦略的に対応するための体制を早急に構築する必要がある。金融業界全体の問題として、こうした体制整備に向けた議論を始めるべき時期に来ている。

4．研究発表1「生体認証システムにおける脆弱性について ―身体的特徴の偽造に関する脆弱性を中心に―」

松本は、宇根との共同論文[2]に基づき、指紋、虹彩、静脈パターンを用いた生体認証システムの脆弱性に関する最新の研究成果を紹介するとともに、そうした脆弱性への今後の対応方針について、以下のとおり説明した。

(1) 生体認証技術と銀行での利用

生体認証技術は、身体的特徴や行動的特徴等、各個人に固有の特徴を用いて個人の認証を自動処理によって行う技術である。生体認証技術に用いられる個人に固有の特徴として、指紋、虹彩、血管パターン、顔、声紋等が挙げられる。生体認証技術の金融分野における利用状況についてみると、従来から事務センターにおける職員の入退室管理等の手段として銀行内部で主として利用されてきたが、最近では、スルガ銀行や東京三菱銀行による手のひらの静脈パターンを用いた本人確認サービスの提供開始等、銀行の窓口やATMにおける顧客の本人確認手段としても活用されており、生体認証技術が活用される場面が増加している。

(2) 身体的特徴の偽造による脆弱性と生体検知機能

生体認証システムにおける脆弱性には、生体認証の要素技術に立ち入って対策を講じる必要があるもの、認証精度評価にかかわるもの、セキュリティ要件の設定に関するもの、管理・運用による対策の実施が適当と考えられるものまで、その利用環境に応じて多種多様なものが想定される。これらのうち、要素技術に立ち入った対策が求められるものとして、物理的に偽造された身体的特徴を誤って受け入れてしまうというタイプの脆弱性に着目して議論する。

身体的特徴の偽造による脆弱性への対策の1つとして、生体情報が生きた人間の体から直接提示されているか否かを確認する機能（生体検知機能）を組み込むことが考えられる。生体検知機能の実現方法としては、例えば、生体に固有の性質（皮膚における光の吸収・反射等）、生体から自然に発せられる情報（脈拍や体温等）、外部からの刺激に応じて生体から発せられる情報（光に対する瞳孔の変化等）を利用するものが挙げられる。これらは特許資料等から参照できるものの、市販の生体認証システムで実際にどのような手法が採用されているかに関してはあまり公開されていないのが実情である。

身体的特徴の偽造による脆弱性について具体的な装置を対象に評価する場合、評

2 宇根正志・松本勉、「生体認証システムにおける脆弱性について：身体的特徴の偽造に関する脆弱性を中心に」、本号所収。

価者がその装置に関してどの程度の知識を有しているかによって評価の性格が変わってくる。次に紹介する研究では、評価対象をほぼブラック・ボックスとして評価している。評価の内容は、「生体認証システムに生体でない対象物を提示し、登録できるか否か、また、登録できた場合には再度同一の対象物を提示して受け入れられるか否かを確認する」という第1段階の評価と、「生体によって登録を行った後、何らかの手段によって偽造した（生体でない）身体的特徴によって照合に成功するか否かを確認する」という第2段階の評価に分けられる。

（3）指紋および虹彩の照合装置における脆弱性の研究

まず、指紋照合装置の脆弱性評価に関しては、ゼラチン等を材料として表面に指紋のパターンが複製された人工指を作製し、19種類以上の指紋照合装置において実験を行った。その結果、2段階の評価のいずれにおいても、すべての装置が人工指を高い割合で受け入れるという結果を得た。

虹彩照合装置については、虹彩の画像を撮影したうえでその画像を紙に印刷し、瞳孔部分を切り抜くという手順で人工虹彩を作製して実験を行った。3種類の虹彩照合装置を対象としたが、そのうち2機種は2段階の評価ともに人工虹彩が高い割合で受け入れられた。残り1機種については、第1段階の評価において人工虹彩での登録が不可能であったものの、第2段階の評価における人工虹彩での照合は高い割合で成功した。

こうした実験結果は、現状で実装されている指紋や虹彩の照合技術に脆弱性が存在することを示している。セキュリティ向上を意図して導入される指紋照合システム等においては、利便性の低下をできる限り抑えたうえで、生体検知機能の充実を図っていく必要があるといえる。

（4）静脈照合装置における脆弱性の研究

静脈のパターンを使用する認証技術は、静脈を流れる血液に含まれる還元ヘモグロビンが特定波長の光を吸収しやすいという性質を利用しているといわれている。手のひらや指に近赤外線を当てると、静脈の部分だけ光が多く吸収されて画像上暗く映し出されるため、これを撮影して静脈パターンを抽出するという仕組みであるとされている。しかし、市販の静脈照合装置では、実際にどのようにして静脈パターンを抽出し、照合を行っているかに関する情報がほとんど公開されていないようであり、静脈照合装置は事実上ブラック・ボックスと同様の状態となっている。

インターネット上で販売されている指の静脈パターンを利用する装置（指静脈照合装置）を1機種購入し、第1段階の評価の実験を行った。指静脈照合装置に提示する物質としては、光の分散の具合が人間の指や手と類似しているという観点から、大根を人間の指のようにスティック状に切り出して料理用のラップで包んだものと、人工雪材とエポキシ樹脂を混合させて透明なビニール管に注ぎ、指の形状に固め

たものの2種類を準備した。実験の結果、大根スティック、人工雪材のいずれも高い割合で登録可能であったほか、登録した同じ大根スティックや人工雪材で再度照合を行った結果、いずれも同様に高い割合で照合に成功した。これにより、実験対象とした指静脈照合装置においては、生体でない物質を用いて登録を行い、その物質を他人に渡して照合を行わせるといった行為が実行できることが明らかとなった。

(5) 今後の課題

身体的特徴の偽造による脆弱性への今後の対応として、まず、脆弱性評価手法の確立が挙げられる。物理的偽造に関する脆弱性の評価では、偽造に利用可能と考えられる物理媒体や機器等を使って実際に偽造を行い、それを用いて評価を行うという手法が採用されてきた。こうした評価研究を継続して脆弱性評価に関するノウハウを蓄積し、効率的で洗練された評価手法を確立することが重要である。そのためには、評価研究の結果を、第三者が追試可能なように実験の手順や条件を詳細に公表することが必要である。

また、身体的特徴の偽造を検知するための生体検知機能の検討も重要である。実際の生体認証システムに実装されている生体検知機能を評価することが検討の第一歩になると考えられるが、こうした検討の実効性を高めるためには、関連する情報を開発・設計者、評価者、利用者間で共有し、評価結果等について議論する場を準備することが求められる。

生体認証システムを長期間にわたって安全かつ安定して利用していくためには、導入時点では知られていなかった脆弱性が将来顕現化する可能性についても考慮しておく必要がある。具体的には、システムを構成する要素や技術を別のものに置き換えることが相対的に容易であるという意味で、拡張性の高い生体認証システムを採用する、また、脆弱性に関する最新情報を正確かつ迅速に収集し、その脆弱性が生体認証システムに与える影響を分析する体制を整備するといった対応が求められる。また、新たな脆弱性が発見された場合に、生体認証システムの利用者となる顧客に対して、当該脆弱性がシステムに及ぼす影響やその対応について迅速に情報提供を行うことも重要である。

5．研究発表2「デジタル署名の長期利用に係る脆弱性」

宇根は、田村、岩下、松本、松浦、佐々木との共同論文[3]に基づき、デジタル署名の長期利用とその脆弱性について以下のとおり発表を行った。

3 田村裕子・宇根正志・岩下直行・松本勉・松浦幹太・佐々木良一、「デジタル署名の長期利用について」、『金融研究』第24巻別冊第1号、日本銀行金融研究所、2005年7月、121～176頁。

（1）デジタル署名の長期利用について

電子政府の推進や民間での電子文書の利用に関する法整備も進み、紙文書から電子文書への移行が進展している。電子文書は、紙文書とは異なり、痕跡を残さずに内容を改ざんすることが容易であるため、電子文書の作成者や一貫性の確認が求められる。これらを確認する手段として、デジタル署名を挙げることができる。しかし、デジタル署名を長期間検証可能にしておくためには、公開鍵証明書の有効期間切れの問題等、考慮すべき問題が山積しているのが実情である。こうした点については、平成15年3月に開催した「デジタル署名の長期的な利用とその安全性」をテーマとする第5回情報セキュリティ・シンポジウムにおいて議論し、対策の検討が必要であることを説明した。

今回は、デジタル署名の長期利用に関する概念を整理したうえで、具体的な対策技術に関する分析を行う。

（2）デジタル署名とPKIについて

デジタル署名は公開鍵暗号技術の特性を利用している。署名者は秘密に保管する署名生成鍵を用いて電子文書に対するデジタル署名を生成する。署名検証者は、当該署名生成鍵に対応し、公開されている署名検証鍵を用いてデジタル署名の検証を行う。署名生成鍵の持ち主が当該署名生成者であること、および、署名生成鍵が署名生成者によって適切に管理されていることが確認できるとき、デジタル署名の検証によって電子文書の一貫性とデジタル署名の生成者が確認可能となるが、こうした機能を担っているのがPKI（public-key infrastructure）である。PKIでは、認証機関（CA：certification authority）と呼ばれる第三者機関が、署名検証鍵とその所有者を関連付ける公開鍵証明書を生成・発行するほか、署名生成鍵が適切に管理されているか否かを確認可能にする情報として、証明書失効リスト（CRL：certification revocation list）等を発行する。以下では、署名生成者（PKIの利用者）に係る公開鍵証明書を「利用者証明書」と呼ぶほか、証明書失効情報としてCRLを利用する場合に絞って議論する。

（3）デジタル署名の長期利用に関する概念整理

デジタル署名の長期利用については、いろいろな文脈で取り上げられるものの、その意味については統一的なものは存在しない。ここでは、デジタル署名の長期利用を、「デジタル署名の生成者、および、署名対象データの一貫性を事後的に確認するための利用」と定義し、署名生成の一定期間後に改めて実行される署名検証を「署名再検証」と呼ぶこととする。

一般に、検証者は、利用者証明書がCAによって発行されたものであり、検証に必要な各種データが署名生成時点において有効であったか否かを確認することとな

る。したがって、以下の4つのデータがあれば原理的に署名再検証が可能となる。

〈1〉利用者証明書：有効期間に署名生成時点を含むもの。
〈2〉証明書失効情報：署名生成後、最初に更新されたもの。
〈3〉CA証明書：CAによって生成されたことが確認可能であり、有効期間に署名生成時点を含むもの。
〈4〉CA証明書失効情報：CAによって公表されたことが確認可能であり、署名生成時点におけるCA証明書の失効の有無を確認できるもの。

これらのデータを用いた再検証処理に係る主な脆弱性としては、①CAが保管している上記データの破損・損失、②CAの署名生成鍵の漏洩等が考えられる。

（4）具体的な対策技術に関する分析

以上の署名再検証に係る2つの脆弱性①、②に対する対策技術として、さまざまな手法が提案されているが、脆弱性①、②ともに対応可能とされている、欧州電気通信標準化機構（ETSI）の技術仕様ETSI TS 101 733の署名トークンを分析対象に選んだ。分析の内容は、2つの脆弱性がそれぞれ顕現化した場合に署名トークンによって署名再検証が実行可能となるための十分条件を導出するというものであり、署名再検証に必要なデータをすべて入手可能である場合を署名再検証可能であると定義し、分析を行う。

ETSI TS 101 733には、10種類の署名トークンが規定されているが、そのなかでもES-Aと呼ばれるものに関する分析結果を説明する。

まず、脆弱性①が顕現化した場合、署名再検証を行う調停者は、署名トークンに含まれるデータを用いる必要がある。署名トークン（ES-A）には、利用者証明書とCRLが含まれているものの、CA証明書失効情報が格納されていないほか、署名トークン内のCA証明書がCAによって発行されたことを確認できない。このため、CAによって発行されたことが確認可能なCA証明書とその失効情報を入手するという条件が満足されるならば、署名再検証が実行可能となる。

また、脆弱性②が顕現化した場合、特に利用者証明書生成用の鍵が漏洩したケースにおいては、利用者証明書が偽造されたものであるか否かの判断が不可能となる。CAの署名生成鍵が漏洩する状況を3つに分類したうえで検討を行うと、まず、署名生成後に鍵漏洩が発生し、そのことを調停者が認知していた場合（状況1）には、署名トークン全体に対して付与されるタイムスタンプが効果を発揮し、署名再検証が実行可能であるための十分条件は鍵漏洩がない場合と同一となる。しかし、署名生成前に鍵漏洩が発生した場合（状況2）や、署名生成と鍵漏洩の時間的前後関係を調停者が認知していない場合（状況3）においては、タイムスタンプが状況1のような効果を発揮せず、CAによって発行されたことを別の手段によって確認できる利用者証明書を入手するという条件を状況1の十分条件に追加することが求め

られる。このように、顕現化する脆弱性の種類や想定環境によって、署名再検証が実行可能となるための十分条件は異なることが明確となった。

(5) 今後の課題

今回の分析によって明らかにした十分条件を満足する具体的な方法として、例えば、セキュア・ストレージ・サービスを利用する方法や、他の利用者や各種メディアにおいて分散して保管されるデータを利用する方法等が考えられる。こうした方法をうまく組み合わせて、署名トークンが有効に機能する状況をどのように作り出すかが今後の課題の1つといえる。デジタル署名を長期利用する際には、利用環境に即して、どのような脆弱性が想定されるかを明確にしたうえで、対策技術が期待通りの効果を発揮するかを評価する必要がある。

6．パネル・ディスカッション「情報システムの脆弱性検知と情報共有―金融業界へのインプリケーション―」

(1) パネル発表1「情報システムの脆弱性対策―情報セキュリティ早期警戒パートナーシップの全体構成と運用状況―」

早貸は、脆弱性関連情報の流通の枠組みである情報セキュリティ早期警戒パートナーシップの概要について以下のとおり発表した。

近年、ソフトウエア等の脆弱性情報がコンピュータ・ウィルスや不正アクセス等の攻撃に悪用されるケースが増加しており、脆弱性情報の公開から攻撃手法が流布するまでの期間が短くなる傾向にある。脆弱性に伴う被害の発生を防ぐためには、攻撃手法の流布以前のユーザ・サイドにおける対策実施が必須であることから、脆弱性情報を円滑に流通させ、対策の普及を図るための官民連携体制を整備する必要が高まっていた。

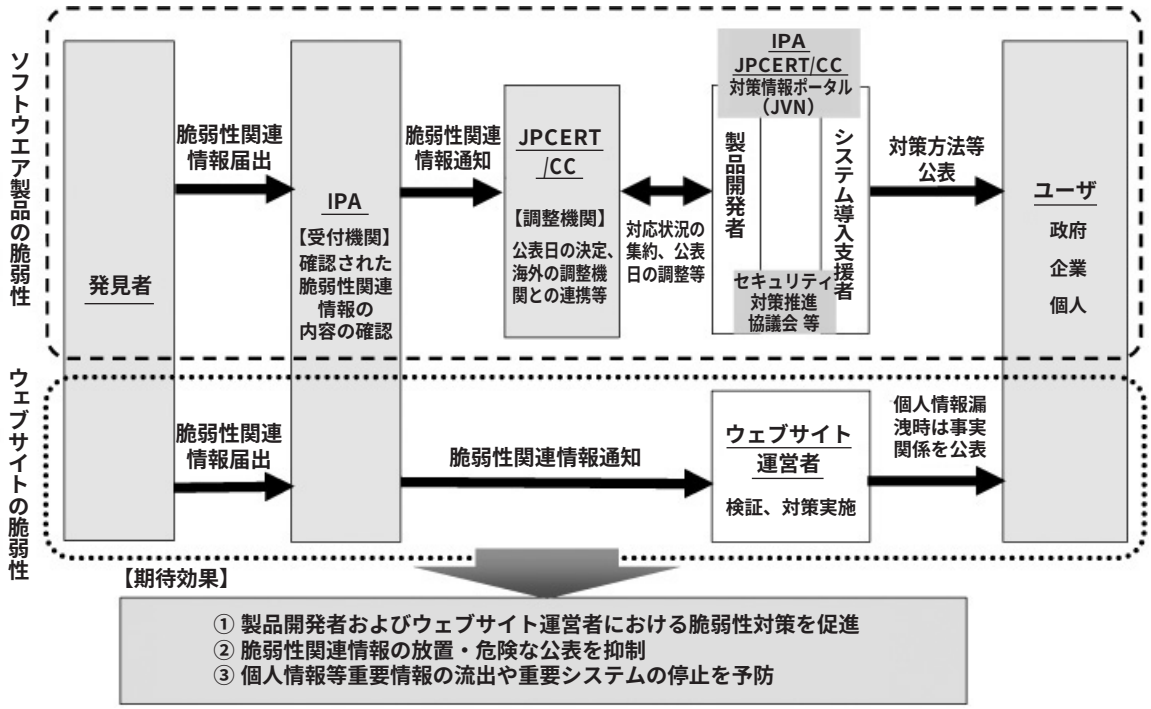
こうしたなか、平成16年7月に、情報処理推進機構（IPA：Information-technology Promotion Agency, Japan）を脆弱性情報の届出窓口、JPCERTコーディネーションセンター（JPCERT/CC）を調整機関とする情報セキュリティ早期警戒パートナーシップの運用が開始された。本パートナーシップは、関係者間の適切な情報共有と連携によって、製品開発者およびウェブサイト運営者による脆弱性対策の促進、脆弱性情報の放置や危険な公表の抑制等の効果を期待するものである。ソフトウエア製品の脆弱性に関しては、ベンダー間での調整が必要との考えから、IPAは脆弱性発見者からの情報の内容を調整機関であるJPCERT/CCに通知する。JPCERT/CCは、開発ベンダーと対応状況の集約や、脆弱性情報とその対策技術の公表日の調整等を行うほか、海外の調整機関と連携しながら、最終的に対策方法等を公表する。これに対し、ウェブサイトの脆弱性に関しては、IPAは調整機関を通さず、直接ウェブサイ

ト運営者に対して脆弱性情報を通知する形を採用している（図1参照）。

最近の本パートナーシップの運用状況（平成16年7月～平成17年3月）をみると、ソフトウエア製品の脆弱性に関しては、ウェブ・ブラウザ、アンチウィルス・ソフト、情報家電、携帯機器等、幅広い製品に関する脆弱性が43件届け出られている。対策に関しては約半数において完了しており、既に公表済みとなっている。また、ウェブ・アプリケーションの脆弱性についても、210件の届出があり、そのうち半数以上が対策を完了している。

インターネット・バンキング等の運営者である金融機関に対しては、クロスサイト・スクリプティング攻撃[4]への対策を講じること、また、インターネット・ユー

図1　情報セキュリティ早期警戒パートナーシップの概要



資料：早貸氏プレゼンテーション用スライド

4 クロスサイト・スクリプティング攻撃とは、攻撃者が攻撃対象のクライアントのブラウザにジャバスクリプト等のスクリプト言語で書かれたコードを実行させ、当該クライアントがアクセスする他のサイトのウェブ・サーバから当該クライアントに関する情報を、クライアントのブラウザを経由して攻撃者へ転送させる攻撃法のことである。この攻撃が実行された場合、利用者が金融機関のウェブ・ページに入力した個人情報等が別のウェブ・サイトに送信される等の脅威が発生しうる。

ザとしての金融機関に対しては、JVN（Japan Vendor Status Notes）[5]、IPA、JPCERT/CC等から、脆弱性や対策情報を適宜入手し、自発的にセキュリティ対策を実施することを要請したい。

（2）パネル発表2「Telecom-ISAC Japan、SPREADを通した情報共有について」

中尾は、Telecom-ISAC Japanとセキュリティ対策推進協議会（SPREAD：Security Promotion Realizing sEcurity meAsures Distribution）の活動内容と今後の展望等について以下のとおり発表した。

情報セキュリティ対策を実行するうえで、われわれは何を守る（＝資産）のか、守るべき資産のリスクは何であるかを整理し、リスクの低減、回避、移転の方法は何であるかを考察することが重要である。守るべき資産に関して、その重要性、周辺脅威、存在する脆弱性を評価できれば、物理的対策、人的対策、技術的対策、運用上の対策、緊急時における対策等の適切な実施につながる。さらに、資産の洗出しや分類、資産リスクの分析と算定、セキュリティ要求条件の抽出、各種対策の選定・実施、見直し・監査という情報セキュリティ・マネジメントの一連のサイクルを継続的に繰り返すことによって、セキュリティの一層の向上を図ることができる。このようなサイクルにおける各種対策の選定・実施を行ううえで、脆弱性情報の共有・分析が重要となる。

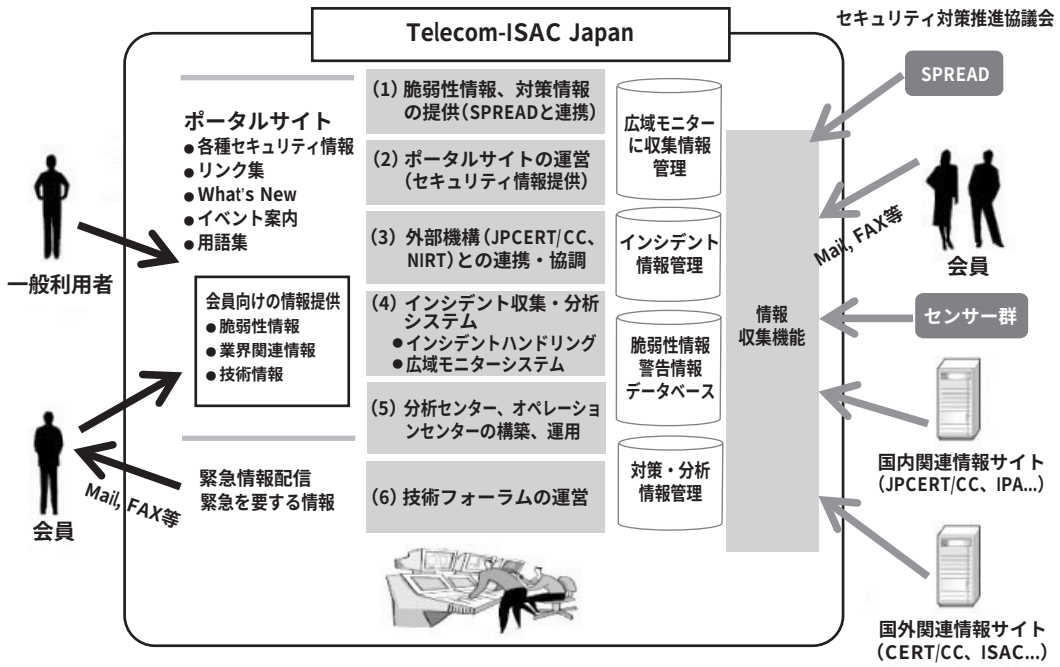
情報通信事業者を中心とする会員制で運営されるTelecom-ISAC Japanは、平成14年5月に、わが国の重要インフラである情報通信基盤の安全性確保を目的として設立され、通信サービスの提供を妨げる各種インシデント（セキュリティ侵害を引き起こす事象）に関する情報の収集、および、会員間での共有・連絡・連携を図る役割を担っている（次頁図2参照）。

現在、Telecom-ISAC Japanでは、広いネットワークを同時に監視するという広域モニターの考え方を実施し、インシデント分析の精度・提供情報量の向上を図っている。広域モニタリング・システムでは、膨大な量のデータを解析する必要があるため、現状のインターネットのリスク状況を迅速に把握することを目的とした1次分析とインターネットのリスク状況をきめ細かく分析することを目的とした2次分析に分類することにより適切な処理を実施している。

SPREADは、インターネットのセキュリティ対策を推進するための各種情報を、わかりやすく迅速かつ確実に会員に提供することを目的として設立された協議会であり、平成17年4月の活動開始を予定している。SPREADでは、OS、閲覧ソフト、メールソフト等のソフトウエア製品ならびにソフトウエアを組み込んだハードウエア製品を対象としており、IPA、JPCERT/CC、Telecom-ISAC Japan、日本ネット

5 経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」を受けて、JPCERT/CCとIPAが共同で運営している、日本国内の製品開発者の脆弱性対応状況を公開するサイト。

図2　Telecom-ISAC Japanの概要



資料：中尾氏プレゼンテーション用スライド

ワークセキュリティ協会（JNSA：Japan Network Security Association）をはじめとするさまざまな業界や団体と密接に連携している。SPREADでは、一般消費者レベルにおける脆弱性への対策の徹底が社会インフラの維持に大きく影響を与えるという考えから、サポーター体制を導入している。サポーターとなる個人・団体が、自らが伝達できる範囲のユーザに対してSPREADから通知されたセキュリティ対策情報を告知する役割を担うことで、脆弱性に対する回避方法や修正方法を迅速にユーザに直接通知することを目指している。

重要インフラの1つである金融業界においても、業界内で脆弱性情報を検知・共有するための金融ISACを立ち上げることが考えられる。この場合、SPREADからの情報を利用して、各金融機関におけるインシデント・マネジメントの高度化を図ることができると考えられる。

（3）パネル発表3「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」

高木は、金融機関を含むさまざまな業種の情報システムにおける脆弱性の検知、通報を行った事例、今後の検知・情報共有体制構築への提言、方向性等について以下のとおり発表した。

脆弱性は、欠陥であることが自明であるものと、脆弱性として議論の余地があるものに分類される。

欠陥であることが自明である脆弱性に関しては、平成14年2月に国内のある大手金融機関が提供していたインターネット・バンキングの例がある。アクセス制御に利用されるクッキーのセッションIDの予測が可能であったために、セッションのハイジャックが可能になってしまうという脆弱性が存在することを発見し、当該金融機関に通知した。この種の脆弱性は平成13年5月に既にベンダーから修正パッチが公開されていたにもかかわらず、当該金融機関は未対応のままとしていた。当時は、このような明らかな脆弱性に関しても、個人的に運営者サイト側に対して注意勧告を行うしかなかったが、現在では、IPA等の脆弱性届出窓口に通知するという手段で、運営者サイト側に改善を求めることができる。

脆弱性として議論の余地がある場合における過去の事例としては、一部の金融機関が提供するインターネット・バンキングにおいて、ユーザが接続しているサイトのアドレスが隠されてしまうということがあった。通常、アドレス・バーに表示されたURLによって接続先を確認可能であるが、これらの金融機関のサイトでは接続先の確認ができないため、フィッシング詐欺等において利用されるような偽ウィンドウによる攻撃に対して脆弱になってしまう。これについては、個人的に当該金融機関に対して注意勧告したにもかかわらず、金融機関側はこれを脆弱性として認めず、その後3年間にわたり、この脆弱性は放置された。

このような脆弱性として議論の余地があるものの、顕現化すれば致命的となるおそれのある問題においては､改善を求める適当な手段がないというのが実情である。IPA等の脆弱性届出窓口へ通知したとしても、通知先がそれを脆弱性であると判断し、適切な対策を実施するとは限らない。また、運営者サイトに直接連絡する場合においても、それが脆弱性として受け入れられる可能性は低い。このような問題を解決する手段としては、金融業界全体としてのセキュリティの重要性に対する意識を向上させていくとともに、まず、業界内において情報共有の場を準備することが有効である。特に、重要インフラの1つである金融分野においては、脆弱性情報を公表する前に、金融業界内での情報共有の場において優先的に情報を開示し、しかるべき対応方法について検討できるようにしておくことが重要であろう。

(4) 自由討議と質疑応答

上記のキーノート・スピーチ、研究発表およびパネル発表の内容を受けて、以下のとおり､パネリストによる自由討議およびフロアとの間での質疑応答が行われた。

まず、**岩下**は、偽造キャッシュカード、フィッシング詐欺メール、キー・ロガーといった、金融業界における脅威を巡る問題のうち、何が最も深刻と考えるかについて、パネリストの見解を尋ねた。**松本**は、偽造キャッシュカードの対策として導入が進められているICカードの形態について、利便性の問題から磁気ストライプが

併用されるICキャッシュカードは、磁気ストライプ部分を狙った既存の攻撃への対策とはなっていないため、ICカード化を進めても直ちには脆弱性が解消しないことが当面の最大の問題と考えられるとした。**早貸**は、情報提供者側の観点から、金融機関においても汎用製品を利用している以上、それに係る脆弱性情報を外部からいち早く収集し、迅速に対応すべきであると指摘したうえで、脆弱性に対する適切な対応を行うための体制整備が進んでいないことが問題であると述べた。次に**中尾**は、金融システムには、制御系、情報系、インターフェース系等が存在するが、それぞれのシステムが持つ脅威の洗出しがまず必要であり、そのうえで脆弱性情報を業界内で共有する体制を整えていく必要があると述べた。**高木**は、金融機関が適切なセキュリティ対策を実施するインセンティブがないことが問題であると指摘した。

次に、**岩下**は、金融関連のウェブ・アプリケーションにおける脆弱性の届出状況について早貸に尋ねた。**早貸**は、平成16年7月から平成17年3月までに受け付けたウェブ・アプリケーションに関する脆弱性の届出件数210のうち5件が金融関連であり、既に対策の手法が明らかであったものばかりであったと説明した。そのうえで、脆弱性情報を積極的に収集し、システム内に脆弱性が放置されることのないように対応することを金融業界に対して求めた。

続いて**岩下**は、業界内での情報共有に関する金融業界の対応のあり方についてパネリストに見解を尋ねた。**中尾**は、企業が各自で脆弱性問題に取り組むような体制には限界があり、セキュリティ対策には競合他社との情報交換・共有が有効であると指摘したうえで、金融業界においても、Telecom-ISAC Japanにみられるように、同業種間で共通性を見出し、情報を共有することが必要であると述べた。また、**高木**は、非公式な場での情報交換・共有も有益であるが、これを適切に機能させるためには、情報提供者のインセンティブの確保や、非公式な情報の取扱いの方法について今後検討していく必要があると述べた。

最後に、**岩下**は、今後金融機関が生体認証技術を利用していくうえでの留意点等についてパネリストに尋ねた。これに対し、**松本**は、緊急に対応すべき脆弱性と、偽造キャッシュカード問題にみられるようなグランド・デザインの変更を余儀なくされる脆弱性とを分けて検討していかなければならないと指摘した。緊急対応が必要な部分については、IPA等によって提供される情報を利用する手段が考えられるが、グランド・デザインの変更が必要な部分については、コストの問題やその効果について、時間をかけ慎重に議論すべきであると述べた。

以上の自由討議を踏まえて、**フロア参加者**から、金融サービスのチャネルが多様化するなかで、顧客とのインターフェースがセキュリティの観点で統一かつ整合的になるように情報システムの設計を行う必要があるのではないかという意見が寄せられた。これに対して、**松本**は、示された意見に賛意を表したうえで、顧客とのインターフェースが問題となる例の1つとして、ATMにおける個人認証について取り上げ、ATMが顧客を認証するだけでなく、顧客側がATMを認証し、偽ATMの存在を排除できるようなシステムの必要性を述べた。

また、別の**フロア参加者**からは、セキュリティ・レベルを高めるために必要となるコストや利便性の損失についてバランスをどのように確保すればよいかとの質問が寄せられた。これに対して、**高木**は、セキュリティ・レベルは想定される被害とのバランスによって設定すべきであり、従来、銀行は利便性を重視しすぎてきた傾向があるのではないかとの見方を示した。そのうえで、コスト削減や利便性の追求によって生じた事故についてはシステム提供側が責任を負うべきであると述べた。また、**早貸**は、コストを投入して高い安全性を実現している製品は、相対的にセキュリティ面で競争力を獲得することができるとの考え方を示したうえで、利用者自らが安全性と利便性のバランスについて考えることができる環境を醸成していくことも必要であると述べた。**中尾**は、高い安全性を達成するために、コストを投入して、企業活動を安定させ、ブランド・イメージを守ることの重要性を指摘したうえで、守るべき資産において残存するリスクとコストのバランスを検討することが必要であると述べた。

最後に、パネル・ディスカッションのまとめとして、各パネリストが本シンポジウムにおいて議論された内容に関して短くコメントを行った。まず、**松本**は、金融研究所内に設立されるCITECSには、金融業界におけるセキュリティ研究機関として中心的役割を担っていってもらいたいと述べた。**早貸**は、金融業界内で情報を共有できる枠組みを整備し、IPAが提供する脆弱性情報を有効に活用することを要請した。**中尾**は、脆弱性を扱ううえでのリスク分析の必要性と情報交換の重要性を強調し、金融業界に適切な対応を求めた。最後に**高木**は、システム設計時に脆弱性を放置してしまう原因として、システム構築に携わる技術者間のコミュニケーション不足を指摘し、銀行においても同様の問題があるとすれば早急に解決しておくことが必要であると述べた。

7．総括コメント

今井は、総括コメントとして、キーノート・スピーチ、研究発表およびパネル・ディスカッションの内容を振り返ったうえで、次のようにコメントを行い、シンポジウムを締め括った。

今回のシンポジウムでは、金融機関のさまざまな情報システムにおける脆弱性検知と情報共有のあり方について議論が行われた。現在、フィッシング詐欺、偽造キャッシュカードによる不正預金引出し、個人情報漏洩等、金融機関の情報システムに対する信任を揺るがせる深刻な事件が多発しており、金融サービスにおける情報システムのセキュリティ対策は喫緊の課題となっている。

しかし、キーノート・スピーチにおいて問題提起されたように、金融機関システムにおける脆弱性の検知やその情報共有の方法については、具体的な方策が定まっていないのが実情である。このような状況が継続すれば、脆弱性是正の遅延が発生し、被害の拡大を招く惧れがあるほか、業界としても適切なセキュリティ対策に関

するコンセンサスが醸成されないという問題が発生する可能性もある。金融業界においては、今後、脆弱性の検知と情報共有をどのように行っていくかについて議論を行い、積極的に対応を検討していくことが必要である。

研究発表においては、生体認証システムやデジタル署名の長期利用に係る脆弱性に関する最近の研究成果とそのインプリケーションに関して発表があった。生体認証技術は、金融機関のATM等における本人確認に利用されつつあることからも、今後、そのセキュリティ評価について、さまざまな角度から検討を行う必要がある。また、パネル・ディスカッションにおいては、ソフトウエア製品やウェブ・アプリケーション等における脆弱性の検知や情報共有に関連する既存の枠組みについて紹介があったほか、金融機関の情報システムにおける脆弱性とその対応等について、これまでの事例が紹介された。自由討議では、金融機関の取組み姿勢に対してやや厳しい意見も出たが、金融業界はそれらを真摯に受け止めて対応していくことが求められている。

本シンポジウムの冒頭で翁所長から、平成17年4月1日に日本銀行金融研究所にCITECSを設立するとの説明があった。本シンポジウムの発表やパネル・ディスカッションで示されたように、重要インフラの1つである金融機関の情報システムのセキュリティが社会全体に与える影響は大きい。新たに発足するCITECSにおいては、こうした金融業界の社会における位置付けを明確にしたうえで、安心できる金融情報システムの構築に貢献していただきたい。

産業技術総合研究所においても、4月1日に情報セキュリティ研究センター（RCIS：Research Center for Information Security）が発足し、私がセンター長に就任する予定である。RCISは、セキュリティ基盤技術研究、物理解析、ソフトウエア・セキュリティ研究の3つのチームで構成され、16名のスタッフでスタートする。今後は、センター・プロパーの研究員を増員していくとともに、東京大学やIPA等とも深く、実効的な研究活動の連携を進めていく方針である。もちろん、CITECSとも研究員の人事交流を含めて密接な関係を築いていきたいと考えている。CITECSの今後の活動に期待したい。