第11回
情報セキュリティ・シンポジウム「偽造防止技術の新潮流：金融業務における人工物メトリクスの可能性」の模様

1. はじめに

日本銀行金融研究所は、2009年3月11日、「偽造防止技術の新潮流：金融業務における人工物メトリクスの可能性」をテーマとして、第11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）。

金融取引においては、証券、紙幣、小切手、預金通帳等の物理媒体（人工物）が利用されており、当該取引の安全性や信頼性を確保するうえで重要な役割を果たしている。ただし、こうした人工物の偽造抵抗力は、デジタル画像処理技術をはじめとする情報技術の進展に伴い徐々に低下してきており、今後、技術進歩を取り入れた新しい偽造防止技術の活用が求められている。そうした技術の候補として、「人工物メトリクス」が注目を集めている。

人工物メトリクスは、人工物に固有の特徴を利用する偽造防止技術であり、人為的に制御することが困難とみられるランダムな特徴を認証に利用することによって、技術内容を公開しても偽造抵抗力を維持できる技術として期待されるものである。

こうした背景から、今回のシンポジウムにおいては、人工物メトリクスをはじめとする偽造防止技術の研究動向やセキュリティ評価の現状と課題について議論した。まず、キーノート・スピーチにおいて、伝統的な偽造防止技術の現状や人工物メトリクスの研究動向を説明したうえで、環境変化に対応した将来のための新しい偽造防止技術に関する検討が必要ではないかという問題提起を行った。2件の発表においては、人工物メトリクスの提案事例やセキュリティ評価研究の動向を説明するとともに、人工物の偽造の困難性を評価する手法について説明した。

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。

「偽造防止技術を評価するために」と題するパネル・ディスカッションにおいては、人工物メトリクスのほかに、印刷技術、ホログラム、暗号ハードウエアの耐タンパー技術を取り上げ、各偽造防止技術の最新動向を紹介した後、各種技術を横並びで定量的に評価する方法について議論を行った。議論の結果、偽造防止技術の評価方法に関する検討を行う際には、技術情報を可能な範囲で公開したうえで、オープンな場における議論を通じて、偽造防止技術にかかわる実務家や研究者の間で相互の理解を深めていくことが重要であるとの認識が共有された。

本シンポジウムのフロアには、情報セキュリティ対策を担当している金融機関関係者、暗号学者、情報セキュリティ技術に関係の深い官庁関係者、偽造防止技術に関するベンダーの研究開発部門の実務家や技術者等、約 120 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 11 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**「偽造防止技術の新潮流：金融業務における人工物メトリクスの可能性」
  ―岩下直行（日本銀行金融研究所情報技術研究センター長）
- **発表 1**「人工物メトリクスの研究開発の動向と課題」
  ―松本　勉（横浜国立大学大学院教授）
- **発表 2**「人工物メトリック・システムにおける耐クローン性の評価方法について」
  ―田村裕子（日本銀行金融研究所情報技術研究センター）
- **パネル・ディスカッション**「偽造防止技術を評価するために」
  - **パネル発表 1**：印刷関連技術による偽造防止技術
    ―金子英信（国立印刷局研究所首席研究員）
  - **パネル発表 2**：ホログラム技術の特徴と評価手法
    ―福田隆史（産業技術総合研究所光技術研究部門主任研究員）
  - **パネル発表 3**：偽造防止を目的とした暗号ハードウエアとその耐タンパー技術の動向
    ―本間尚文（東北大学大学院助教）
  - **自由討議**
    - **モデレータ**：岩下直行
    - **パネリスト**：松本　勉、金子英信、福田隆史、本間尚文
- **総括コメント**―今井秀樹（中央大学教授）

1 文中における各参加者の所属ならびに肩書きはシンポジウム開催時点のものである。

2. キーノート・スピーチ「偽造防止技術の新潮流：金融業務における人工物メトリクスの可能性」

岩下は、岩下［2009］に基づき、人工物メトリクスを偽造防止技術の 1 つと位置付けたうえで、金融業務における偽造防止技術のあり方について、次のとおり発表を行った。

(1) これまでの偽造防止技術の限界と情報技術を活用した対策

金融取引においては、証券、紙幣、小切手、預金通帳等の特殊な印刷を施した紙、キャッシュカード、クレジットカード、プリペイドカード等のさまざまな物理媒体（人工物）が利用されている。こうした人工物は、高価ではない素材から作られるケースが多く、紙の表面に特殊な印刷を施したり、カードにホログラムを貼付したりするなど、さまざまな偽造防止技術が実装されてきた。

こうした偽造防止技術は、情報技術の進展に伴いその有効性が徐々に低下してきている。伝統的な偽造防止技術が長い年月をかけて徐々に進化し偽造抵抗力を高めてきたのに対し、デジタル画像処理技術に代表される情報技術を用いた偽造力は、極めて速いスピードで高まってきている。こうした状況に対処するうえで、技術進歩を味方につける戦略を検討していく必要がある。

しかし、単に機械読取りの技術を導入するだけでは有効とは限らない。例えば、カードに記載された磁気ストライプ情報を読み取る、紙幣に印刷された磁気インキの分布パターンを読み取る、RFID をさまざまなセンサーで読み取ってデータベース上の情報と照合するといった仕組みの技術であれば、攻撃者が人工物の特徴や読取装置の内部構造に関する情報を入手し、それを利用して同一の特性や ID をもつクローンを作製することで偽造が成功してしまうおそれがある。人工物を単に「機械が読み取る情報を搬送する媒体」と位置付けて利用するのではなく、人工物と情報システムが一体となって偽造防止の効果をシステム全体で引き上げるという発想が重要であり、こうした観点から提案されているのが人工物メトリクスである。

(2) 人工物メトリクスの特徴と最近の動向

紙もプラスチックも、その細部をみれば個体 1 つ 1 つに微妙な差異があり、各人工物の「個性」というべき固有パターンが存在する。人工物メトリクスは、人工物の固有パターンが各人工物を個体識別できるほど明瞭であり、かつ、人為的に偽造・改変することが困難なランダム性をもっていれば、これを偽造防止技術として利用できるという考え方を基本としている。さらに、人工物メトリクスでは、人工物の

製造技術を公開しても偽造抵抗力が低下しないため、学会等のオープンな場において評価の対象にすることができるというメリットがある。

これに対して、伝統的な偽造防止技術は、「人工物を製造する側の技術的優位性」をその安全性の拠り所とし、技術の詳細を秘密にしてきた。こうしたアプローチは、製造者側が情報を適切に管理している限り一定の安全性を確保できる一方、技術進歩や秘密情報の漏洩により技術的優位性が喪失してしまうほか、当該技術がどの程度脅威にさらされているかを製造者側が検証困難であるという問題が存在している。人工物メトリクスの場合には、技術情報を公開可能であることから、こうした問題を回避することができる。

人工物メトリクスの分野については、新しい技術の提案や人工物の耐偽造性の評価方法に関する検討の報告に加え、実用化の事例も徐々に増えてきている。例えば、人工物にレーザ光を照射し、その反射光のスペックル・パターン（干渉模様）を当該人工物の固有パターンとして利用するシステムが挙げられる。本システムは、英国の大学の研究者によって提案されたものであり、学術雑誌に評価結果の一部が公開されているほか、同システムは市販の製品としても提供されている。こうしたシステムは、既存の偽造防止技術と比較すると大掛かりなシステム導入を必要とするようにみえる。しかし、専用機器によって人工物の特徴を読み取り、その情報を処理して真偽判定を行うというタイプのシステムは、キャッシュカードのシステムをはじめとして既に金融分野に数多く存在しており、人工物メトリクスの仕組み自体が特別大掛かりというわけではない。

(3) 伝統的な偽造防止技術と検討体制整備に向けた取組み

人工物メトリクスの検討が進展するなかで、伝統的な偽造防止技術の分野においても、安全性の客観的な評価をオープンな場で議論しようという動きがみられはじめている。印刷技術については、米財務省印刷局による銀行券偽造防止技術委員会の報告書が公表されているほか、技術仕様が秘匿されている偽造防止技術を対象にその仕様解明のコストと成功確率を算出するモデルの研究成果も学会で発表されている。ホログラムに関しては、セキュリティ特性の評価に関する研究が学会で報告されてきているほか、わが国では、ホログラムの記録材料における光学特性の評価方法の標準化が世界に先駆けて進められている。IC カードを含む暗号ハードウエアに関しては、一定のセキュリティ要件を充足しているか否かを第三者の専門機関が評価・認証する制度が整備されているほか、共通の評価用ハードウエアを用いた研究環境が普及しつつある。

偽造防止技術の開発者や同技術を組み込んだ製品の製造者の側においても、業界団体における偽造防止技術に関する情報の共有や用語・概念の整理等に関して、オープンな議論を進めていこうとする動きがみられる。例えば、欧州標準化委員会（CEN）において、偽造防止の機能や役割に関する理解向上や情報交換、偽造品検査の標準

的な手続やプロトコルの検討等を主な目的とする検討部会が 2007 年に設置されている。また、国際標準化機構（ISO）においては、2009 年 2 月、各種製品の偽造や横流し等への不正行為への対策をスコープとする新しい専門委員会 TC247 が組成されることが承認された。

(4) 偽造防止技術の将来

2004 年の人工物メトリクスをテーマとした第 6 回のシンポジウム以降、約 5 年の間に人工物メトリクスの研究開発は大きく進歩し、偽造防止技術の新潮流となったといえる。今後も、金融分野では、何らかの人工物を介在させて金融取引の利便性やセキュリティを高めるニーズは存在すると考えられる。人工物の偽造防止技術は、決して古めかしい過去のものではなく、最先端の研究分野であり、今後も環境変化に対応して進化していく。偽造防止技術のユーザである金融業界は、新しい技術提案に対応して、将来のための新しい偽造防止技術について引き続き検討を深めていく必要があろう。

3. 発表 1「人工物メトリクスの研究開発の動向と課題」

松本は、宇根・田村・松本［2009］に基づき、人工物メトリクスにおける最近の提案事例とセキュリティ評価研究の動向について、次のとおり発表を行った。

(1) 人工物メトリクスの最近の提案事例

人工物メトリクスは、やや噛み砕いた表現を用いると、人工物における「読めるが（誰にも）書けない」特徴を用いて人工物の認証を行う技術といえる。人工物メトリクスには、①各個体の特徴が互いに十分に異なる（個別性）、②人工物の特徴を繰り返し安定的に読取りできる（読取安定性）、③人工物の利用に伴う外的要因に対して人工物の特徴が安定している（耐久性）、④人工物の偽造が困難である（耐クローン性）といった性質が求められる。これらの性質を満足するとみられている人工物の特徴として近年さまざまなものが提案されている（表 1 参照）。

最近提案された代表的なものとしては、紙に光を当てたときに得られる反射光や透過光のパターンを用いて 1 つ 1 つの用紙を個体として認証するという方式が挙げられる。これらの方式は、用紙の特徴が紙の繊維の三次元構造によって決定されることからその再現が困難とみられるほか、認証の対象となる用紙に特別な処理を施す必要がないという利点もある。赤外透過光画像を利用する方式は横浜国立大学と国立印刷局研究所によって提案されているほか、用紙の反射光によるスペックル・

表１　人工物メトリック・システムに利用される人工物の主な特徴

特性	人工物の特徴（網掛け部分は 2005 年以降提案されたもの）
光学特性	・基材中の光輝性粒状物の分布（反射光画像） ・紙に漉き込まれた光ファイバー小片の分布（透過光の輝点分布） ・基材に付与された斑の分布（反射あるいは透過光の画像） ・透明樹脂内のポリマー・ファイバーの分布（視差画像） ・基材中のファイバーの分布 ・基材表面の微小の凹凸（スペックル・パターン） ・紙の表面や内部の繊維の分布（反射光画像、透過光画像）
磁気特性	・基材中の磁性ファイバーの分布（電気信号波形） ・データ書込みに伴う磁気ストライプ上の磁気分布（電気信号波形） ・磁気ストライプ上の磁性粒子の分布 ・基材中の伝導性物質の分布（電磁波パターン）
電気特性	・半導体素子内のメモリー・セルの電荷量のばらつき度合い ・ランダムに分散した絶縁粒子を含む IC 保護コーティングの電荷量 ・半導体素子におけるランダムな回路遅延のパターン ・複数のリング・オシレータから出力される周波数 ・コイルとキャパシタで構成される LC 回路の共振波形
振動特性	・導電性ファイバーをランダムに分散した基材のマイクロ波の反射 ・容器に貼ったシールを振動させたときの共鳴周波数分布

パターンの画像を利用する方式も英国の大学から提案されており、実験による認証精度の測定結果が学会で発表されている。

また、人工物の特徴の情報を得るために、与えられる刺激に対して当該情報を出力する関数の機能をもつように設計された PUF（physical unclonable function）と呼ばれる人工物の研究開発事例も増えてきている。電子回路へ実装された PUF の事例の報告が学会において盛んに行われているほか、一部の PUF については商品化されている。

（2）人工物メトリクスの評価研究の動向

セキュリティ評価の観点では、耐クローン性の評価が重要である。第 6 回のシンポジウムにおいては、人工物の偽物をクローンとして作製し、それが誤って本物として受け入れられる確率（クローン一致率）を評価した研究が紹介された。対象となったのは、紙にランダムに漉き込まれた磁性ファイバーから読み取られる電気信号のパターンを利用する方式であった。当該用紙から読み取った電気信号のパターンに基づいて別の用紙の表面に磁性材を塗布してクローンを作製し、クローン一致率を測定したところ、正規の異なる用紙を照合したときに誤って一致と判定される確率よりもクローン一致率が大きいという結果が得られたというものであった。

こうしたクローン一致率による評価方法は、その後、さまざまな人工物メトリクスの耐クローン性評価に採用されている。先ほど紹介した紙の赤外透過光画像を利

用する方式においても同様の評価が行われており、用紙の登録時に得られる赤外透過光画像に変換を加えて OHP シートに印刷してクローンを作製し、当該クローンによるクローン一致率を測定した結果が発表されている。本結果においても、クローン一致率が大きくなるという傾向が現れているが、測定結果を利用することによって、より高精度な照合方法やその際の判定しきい値の適切な設定方法の検討も行われている。

(3) 人工物メトリクスの展開に向けた今後の課題

本発表で紹介したように、人工物メトリクスに関する研究開発の裾野は広がっており、適切な評価の実施に向けた検討が今後一層本格化していくことが期待される。そうしたなかで主な課題として挙げられるのは、①人工物を個体として認証する際の精度や耐クローン性の評価方法の構築、②同評価方法を実際に運用するための評価基盤の構築、③金融業務をはじめとする個々のアプリケーションに応じた認証精度の基準値の設定の 3 点である。

また、偽造防止技術のなかでの人工物メトリクスという位置付けで捉えると、人工物メトリクスを他の偽造防止技術と横並びで比較するための評価方法の検討も重要となる。近年、印刷技術においては、ナノ・テクノロジーを利用した新しい技術の研究開発が進められているほか、ホログラムの分野においては、再生画像の微細化、動画化、立体化といった方向性での研究開発が進められている。金融機関等においては、こうした他の技術の動向も踏まえつつ、人工物メトリクスと他の技術をどのように使い分けていくかについて検討していくことが有用であろう。

4. 発表 2「人工物メトリック・システムにおける耐クローン性の評価方法について」

田村は、田村・宇根［2009］に基づき、人工物メトリック・システムにおける耐クローン性の定量的な評価方法について、次のとおり発表を行った。

(1) 人工物メトリック・システムの基本的構成と評価の現状

人工物メトリック・システムにおいては、一般に、認証の対象となる人工物（トークンと呼ぶ）から得られたデータと、予め登録しておいた参照データとの整合性の確認が行われる。こうしたデータを取得する際、検証装置は、トークンに何らかの刺激を与え、それに対するトークンからの反応をセンサーで信号に変換する。トークンへの刺激の付与は「チャレンジ」と呼ばれ、利用するセンサーの種類や刺激が

付与される範囲等をランダムに変化させるケースもある。また、チャレンジに対して得られた信号に影響を与えるトークンの物理構造の範囲を読取範囲と呼ぶ。

こうした人工物メトリック・システムにおける既存の提案方式のいくつかにおいては、一定の攻撃を想定したうえでトークンの偽造の難しさ（耐クローン性）の評価を試みるものがある。しかし、現時点では、耐クローン性の具体的な評価方法の確立に至っておらず、ユーザが人工物メトリック・システムを採用したいと考えたとしても、想定するアプリケーションに適したシステムを選択することが困難であるのが実情である。

(2) 想定される攻撃と耐クローン性

人工物メトリック・システムにおいてクローンの偽造を試みる攻撃にはいくつかのバリエーションが考えられるが、ここでは、トークンの物理構造を検証装置のセンサーの細かさで再現するクローンを製造・提示する「ハード・コピー攻撃」に焦点を当てる。本攻撃に対する耐クローン性の評価では、想定する攻撃者がどのレベルの細かさでクローンを製造できるかが重要なポイントとなる。

想定する攻撃者に関しては、高度なセキュリティを達成するように設計された人工物メトリック・システムであれば、トークンを製造・発行する「発行者」でさえも制御困難な物理構造を利用しており、少なくとも発行者と同程度の能力を有する攻撃者に対して安全性を確保することが期待される。そのため、ハード・コピー攻撃を実行する攻撃者は、少なくともトークンの発行者や検証装置の製造者と同程度の能力を有し、発行者と同じ方法でトークンを製造したり、正規手続で製造された検証装置と同じ機能を実現する装置を自作したりすることができると仮定する。

このような攻撃者がハード・コピー攻撃を成功させることの難しさを「ハード・コピー攻撃に対する耐クローン性」と定義する。このとき、人工物メトリック・システムのアプリケーションが要求する「許容されるクローン一致率」の上限 γ に対して、ハード・コピー攻撃による任意のクローンが誤って受け入れられる確率が γ 未満となるとき、「当該システムは想定される攻撃者によるハード・コピー攻撃に対して十分な耐クローン性を有する」という。

(3) 耐クローン性の評価アイデア

こうした評価を行うに当たっては、想定される攻撃者の資源によってどのようなクローンを作製できるかについて検討する必要がある。攻撃者の資源とクローンの関係について、ここでは、ハード・コピー攻撃を複数の行為に分割したうえで、各行為が当該攻撃者によってどの程度実行可能であるかを考察するというアプローチを採用する。ハード・コピー攻撃を整理すると、クローンを製造する行為は、設計書の作成に必要な情報の入手、設計書の作成、加工の 3 つに分類される。

イ．設計書の作成に必要な情報の入手

クローンを検証装置に提示するタイミングで与えられるチャレンジを推測し、当該チャレンジによる読取範囲を特定する。そのうえで、再現する読取範囲の物理構造を推定する手掛かりとなる情報を取得する。本行為の実行可能性は、主に、読取範囲の特定に成功する確率で示すことが考えられる。

ロ．設計書の作成

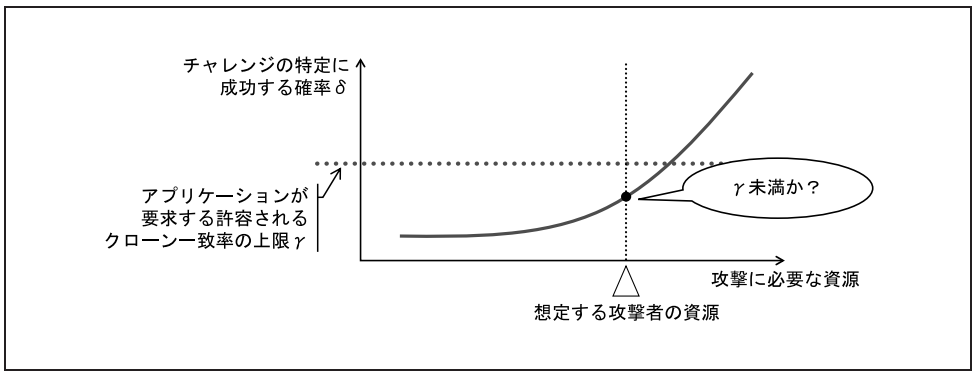
入手した情報から再現する物理構造を特定し、主に、加工の細かさ、加工可能な材料、加工のスピードを基準として適切な加工技術を選択したうえで、具体的な加工工程を示す設計書を作成する。

ハ．加工

設計書に基づいてクローンを加工する。その実行可能性は、加工にかかる資金と時間をベンチマークとして評価することが考えられる。クローンの製造が複数の加工技術を組み合わせて実行されるケースでは、最も資金や時間がかかる加工技術に着目して加工にかかる資源の下限を示すことが考えられる。

このように、ハード・コピー攻撃に対する耐クローン性を評価するうえでの主なベンチマークとして、チャレンジが示す読取範囲の特定に成功する確率 δ、攻撃者が利用する既存の加工技術の候補リスト L、クローン製造全体にかかる資金 C_{M} と時間 C_{T} が挙げられる。これらのパラメータを適切に算出することができれば、評価対象である人工物メトリック・システムの耐クローン性を「加工技術の候補リスト L のもと、確率 δ で正しく読取範囲を特定してハード・コピー攻撃を実行するには、少なくとも資金 C_{M} と時間 C_{T} が必要である」と厳しめに評価することが考えられる。さらに、想定する攻撃者の資源のもとで評価される確率 δ が当該アプリケーションにおいて要求される γ 未満であるならば、「当該システムは想定する攻撃者によるハード・コピー攻撃に対して十分な耐クローン性を有している」と評価することができる（図 1 参照）。

図 1　耐クローン性の評価アイデア（概念図）



(4) 今後の課題

本評価アイデアは、主にクローン製造にかかる資金と時間で耐クローン性を評価するものであるため、異なる種類の人工物メトリック・システムの耐クローン性の比較が可能であるほか、人工物メトリクス以外の偽造防止技術にも適用可能であると考えられる。

今後の課題は本評価アイデアの精緻化であり、本アイデアの妥当性や実現可能性について検討を深めていく必要がある。こうした課題については、情報セキュリティの分野はもとより、さまざまな分野の知見を活用しながら学際的な検討を進めていくことが求められる。金融機関においては、関連分野の研究者や技術者と問題意識を共有しつつ、人工物メトリクスをはじめとする偽造防止技術のユーザとして、同技術の動向をフォローしていくことが重要である。

5. パネル・ディスカッション「偽造防止技術を評価するために」

(1) パネル発表1：印刷関連技術による偽造防止技術

金子は、印刷技術による偽造防止技術の分類や評価手法について、次のとおり発表を行った。

イ. 印刷技術による偽造防止技術の分類

近年、コピー機やスキャナー等のデジタル機器の高性能化や商業用材料・装置の低価格化に加え、インターネットから偽造に関する情報や材料・装置を入手することが容易になってきており、印刷物等の偽造手段の高度化・多様化が進んでいる。こうした動向に対応し、独自の材料や装置を用いた高度な技術の開発、複数の偽造防止技術の組合せ等の対策が講じられている。国立印刷局においても、印刷用の用紙やインキを独自に開発するなどの取組みを行っている。

偽造防止技術は、偽造防止に用いられる人工物（偽造防止要素）の特徴を確認する方法によって、第1～3認証レベルに大別される。第1認証レベルは、偽造防止要素を触る、透かす、傾けるといった人間の五感を用いるという方法である。このレベルを想定した偽造防止技術は、補助具等を利用しないで検証可能であることが求められるケースが多く、有価証券等に広く利用されている。各偽造防止要素が単独で利用されるケースに加え、さらに他の技術を組み合せることで偽造防止効果を高める工夫が施されることもある。第2認証レベルは、ルーペやフィルタ等の補助具を用いて偽造防止要素を観察するという方法であり、第3認証レベルは、偽造防止要素を機械で読み取るという方法である。人工物メトリクスは、第3認証レベルを想定した技術であると考えられる（表2参照）。

表 2　認証レベルによる偽造防止技術の分類

認証レベル	項目	偽造防止技術の効果
第 1 認証レベル：五感による真偽判定	Feel（触る）	手触り感によって確認できる技術。
	Look（見る／透かす）	単純に見ること／透かすこと等によって確認できる技術。
	Tilt（傾ける）	傾けることによって確認できる技術。
第 2 認証レベル：補助具を用いた真偽判定	ルーペ、フィルタ、UV ランプ等の判別補助具を使うことによって確認できる技術。	
第 3 認証レベル：機械による真偽判定	機械により確認できる技術。	

ロ．評価手法の現状と課題

偽造防止技術の評価尺度には、光の波長等の物理量以外に、物理的な刺激を人間が感じる強さで評価した量（心理物理量）がある。第 1 認証レベルを想定した技術を評価する際には心理物理量を用いるほか、第 2 認証レベルを想定した技術には物理量や心理物理量を、第 3 認証レベルを想定した技術には物理量をそれぞれ用いることが考えられる。ただし、心理物理量を用いた評価は容易でなく、評価手法が十分確立しているとはいえないのが実情である。

偽造防止技術を評価するに当たっては、技術の進歩により偽造が容易になる可能性がある点に留意することが必要である。こうした動向を注視しつつ、偽造防止技術の再評価を適宜行うことが重要である。また、家庭用プリンターを用いて印刷物を偽造する場合と業務用印刷機を用いて偽造する場合では、偽造可能な偽造防止要素や偽造の精巧さに差異があるように、想定される偽造手段に応じて評価することが求められる。

(2) パネル発表 2：ホログラム技術の特徴と評価手法

福田は、ホログラムの光学特性に関する評価手法と人工物メトリクスとの関係について、次のとおり発表を行った。

イ．ホログラムの種類

ホログラムは、物体において反射したり透過したりする光（物体光）と別の光（参照光）を干渉させ、その干渉縞を記録した箔状の人工物であり、参照光を当てると当該物体の立体像が再生されるという特性を有する。こうした特性はコピー機では再現できないため、偽造防止技術の 1 つとして、有価証券や ID カード等に利用されている。また、意匠性にも優れており、ブランド・プロテクションやセールス・プロモーションの用途にも利用されている。現在、実用化されている主なホログラム

表３　実用化されている主なホログラム

偽造防止効果 高い

種類	特徴
エンボス・ホログラム	・微細な凹凸を銀色の箔上に形成したもの。 ・量産化により最も広く普及している。
リップマン・ホログラム	・屈折率が異なる構造を厚みのあるフィルム内部に形成したもの。 ・エンボス・ホログラムよりも立体感や遠近感のある画像が再現可能。
計算機ホログラム	・計算機によって求めた光の回折・干渉を生じさせる構造を形成したもの。 ・視認性と複製のしにくさを両立する技術。

には、エンボス・ホログラム、リップマン・ホログラム、計算機ホログラムがある（表３参照）。

ロ．光学特性の評価

ホログラムの光学特性の評価については、これまで個々の研究者や企業がそれぞれ独自の基準や測定手段によって進められており、測定結果を比較する際にデータの互換性の観点から問題が生じるケースがあった。そのため、測定する物理量の定義や測定手段の国内標準（JIS）を策定する取組みが開始されている。例えば、ホログラムに照射した照明光の強さに対して再生される光の強さを「回折効率」と定義し、その測定手段についても規定している。こうした取組みにより、データの信頼性や互換性の確保が図られ、一定の品質を満たすホログラムを選別可能になり、ホログラムの利用が促進されることが期待される。

また、偽造防止の観点からみると、偽造されたホログラムの画質は劣化する傾向にあるため、規定された測定手段によって得られた正規のホログラムの光学特性と比較することにより、偽造されたホログラムを排除することができるという利点がある。

ホログラムの偽造防止効果の向上を意図して、他の微細加工技術と組み合わせた技術も実用化されている。ただし、こうした技術の偽造防止効果は、材料や製法の秘匿や製造者の製造設備の優位性を根拠としており、客観的な評価には至っていないのが実情である。

ハ．人工物メトリクスとの関係

人工物メトリクスとホログラムを比較した場合、両者の親和性は高いとみられる。例えば、アルミ蒸着部分を部分的に除去することで高精度なパターンを形成するタイプのホログラム（ディメタライズド・ホログラム）は、レーザ光を人工物に照射して得られるスペックル・パターンを用いた人工物メトリクスの類型の１つとなりうる。また、用紙に漉き込むかたちで利用する短冊状のホログラム（ホログラム・スレッド）は、基材中のファイバーの分布を利用した人工物メトリクスに類似した技術に

なりうる。こうしたことから、ホログラムの偽造防止効果を向上させるための方向性として、人工物メトリクスのような人工物固有の特徴を利用するというアイデアは有用であり、今後、こうした方向性の研究を進めていくことが考えられる。また、人工物メトリクスにおける取組みのように、評価手法をオープンにしていくことで、ホログラムの利用促進や研究開発の裾野の拡大を図っていくことも重要である。

(3) パネル発表 3：偽造防止を目的とした暗号ハードウエアとその耐タンパー技術の動向

本間は、暗号ハードウエアにおける耐タンパー技術の研究動向と、耐タンパー技術と人工物メトリクスとの関係について、次のとおり説明を行った。

イ．暗号ハードウエアの耐タンパー技術とサイドチャネル攻撃

金融分野においては、IC キャッシュカードに代表されるように、高度な暗号機能を有する暗号ハードウエアが広く利用されている。IC カードの場合、IC チップ内部の情報の不正な読出しや内部機能の改ざん等を防止する技術（耐タンパー技術）を実装可能であり、偽造防止の観点で高い安全性を確保することができる。例えば、暗号アルゴリズムによる認証機能を耐タンパー技術として利用する場合、当該暗号ハードウエアを偽造するためには、暗号アルゴリズムを解読することが必要となる。

暗号ハードウエアのセキュリティに関して、最近では、暗号ハードウエアの正規の入出力チャネル以外から漏れるさまざまな情報を手掛かりにハードウエア内部の秘密鍵を効率よく推定するという「サイドチャネル攻撃」が注目を集めている。代表的なサイドチャネル攻撃である電力解析攻撃は、暗号処理時における消費電力量が秘密鍵の値に依存するという点に着目し、消費電力量から秘密鍵を推定するという攻撃であり、約 10 年前に学会において発表された。その後、サイドチャネル攻撃に関するセキュリティ評価や対策に関する研究が盛んに行われているものの、異なる実装環境のもとで得られた結果を直接比較することは容易でないなどの事情から、サイドチャネル攻撃に対するセキュリティ評価の手法が確立するまでには至っていないのが実情である。

ロ．暗号ハードウエアの評価・認証の枠組みと関連する取組み

暗号ハードウエアの普及が進むなかで、暗号ハードウエアのセキュリティを第三者の専門機関に評価・認証してほしいというニーズが高まり、そうした評価・認証の枠組みが整備されてきている。わが国においては、2001 年に「IT セキュリティ評価及び認証制度（JISEC）」の運用が開始されたほか、2007 年には「暗号モジュール試験及び認証制度（JCMVP）」の運用が開始されている。JCMVP については、評価・認証の対象となるセキュリティ要件が米国連邦政府標準規格 FIPS 140-2 をベースとしたものとなっているが、FIPS 140-2 においてサイドチャネル攻撃への耐性が明示

的に規定されていなかったという問題があった。現在、FIPS 140-2 の改定が進められており、サイドチャネル攻撃への耐性が新たにセキュリティ要件として追加される見通しとなっている。

また、CRYPTREC においては、2003 年に「CRYPTREC 暗号モジュール委員会」が発足し、電子政府推奨暗号を実装した暗号モジュールに対するセキュリティ要件や試験要件の策定に向けた検討が進められている。また、同委員会傘下の「電力解析実験ワーキンググループ」においては、電力解析攻撃を中心としたサイドチャネル攻撃とその対策に関する実験を実施している。また、電力解析攻撃に関する研究を同一の実装環境において実施し、評価手法の確立に結び付ける試みとして、2007 年に、東北大学と産業技術総合研究所は共同で標準評価ボード（SASEBO）を開発している。SASEBO は、2009 年 3 月現在、国内外で 47 の企業や大学等に配布され、電力解析実験ワーキンググループにおいても実験用プラットフォームとして採用されている。

ハ．暗号ハードウエアにおける人工物メトリクス

このように、暗号ハードウエアのセキュリティ評価に向けた取組みは進展しており、暗号ハードウエアの偽造防止の効果についてもそうした取組みのなかで定量的に評価できるようになってきている。ただし、暗号ハードウエアの耐タンパー技術も絶対安全というわけではなく、仮に、強力な攻撃者によって何らかの手段で秘密鍵が盗取された場合、暗号ハードウエアの偽造が成功してしまう可能性は否定できない。こうした状況を想定する必要があるようなアプリケーションにおいては、耐タンパー技術の「奥の手」として人工物メトリクスのような技術を採用しておくことが求められる。

暗号ハードウエアにおける人工物メトリクスとしては、与えられる刺激に対して人工物の特徴に関する情報を出力する関数の機能をもつように設計された PUF（physical unclonable function）を活用することが考えられる。IC の回路を人工物として、当該 IC 固有の物理現象を利用した PUF の研究が進展しており、人工物メトリクスの有力な候補として挙げられる。PUF については、学会において既にいくつもの研究成果が発表されているほか、欧米においては一部商品化が行われている。ただし、そうした PUF の実現可能性やテスト方法については課題も残されており、今後の研究の進展が期待される。

（4）自由討議

上記のパネル発表の内容を受けて、各技術における偽造抵抗力の評価方法と、そうした技術の評価をオープンに実施することの是非について、パネリストによる自由討議を次のとおり行った。

イ．各技術における偽造抵抗力の評価方法について

モデレータの岩下は、最初の論点として、本日紹介されたおのおのの偽造防止技術において偽造抵抗力がどのように評価されているかについて、各パネリストからの説明を求めた。

まず、松本は、人工物メトリック・システムの場合、人工物とその特徴を読み取って検証を行う検証装置とをセットで評価することとなり、人工物のクローンをいくつか準備し、それらを検証装置に提示して評価を行うという手法（テスト物体アプローチ）が利用可能であると説明したうえで、同様の評価手法は他の偽造防止技術にも適用可能であるとの見方を示した。さらに、松本は、印刷技術ベースの偽造対策を施した物の場合においても、例えば、当該印刷物の偽造物として精巧なものから粗雑なものまでいくつか準備しておき、それらを当該印刷物の検証装置に提示するという方法で評価できるのではないかと説明した。

こうした見方について、金子は、印刷用の偽造防止技術としては多種の技術があり、それぞれ性質も異なっているので、1 つの偽造防止技術の評価には可能でも異なった技術同士を客観的に評価することは難しいと述べた。そのうえで、テスト物体アプローチの適用可能性について、金子は、高級ブランド品の偽造防止等の一般製品分野で、標準的な評価手法の構築に対するニーズもあると思われると説明した。

ホログラムに関して、福田は、近年エンボス・ホログラムの精巧な偽造の脅威が現実のものになりつつあると説明し、そうしたホログラムの偽造防止効果がどの程度低下したかを適切に評価するためには、偽造防止効果のレベルを何らかの方法で定量化する手法が必要であると説明した。そのうえで、福田は、人工物メトリック・システムの耐クローン性評価における定量的な評価尺度（偽造に必要な資金や時間等）が他の偽造防止技術にも適用可能であるとの本シンポジウムの発表 2 の説明を引用しつつ、そうした評価手法の検討が今後進展すれば、同評価手法によってホログラムも評価できるようになる可能性があるとの見方を示した。

暗号ハードウエアの耐タンパー技術に関して、松本は、人工物メトリック・システムにおけるテスト物体アプローチは、標準的な人工物を準備するとともに当該人工物の偽造をさまざまな方法によって試みるというものであると説明したうえで、こうした標準的なテスト物体が耐タンパー性の評価における標準的なプラットフォーム SASEBO に対応するという意味で、SASEBO による評価のアプローチはテスト物体アプローチと共通する部分が多いとの見方を示した。

次に、岩下は、人間の五感によって真偽判定を行う偽造防止技術の場合、真偽判定を行う主体は検証装置でなく人間となるが、そうした技術に対してもテスト物体アプローチのような評価手法を適用することが可能であるかと尋ねた。

金子は、印刷技術について、テスト物体が提示されたときに人間の感覚がどのように反応するかを評価することになると説明したうえで、その場合には、人間の感覚を定量化することが必要であり、そうした評価尺度として心理物理量を利用することができると説明した。また、金子は、心理物理量を測定するためには標準的な観測者が必要であり、また人の感覚という要素が入るため数量化は困難であると説

明し、偽造物と本物との差異を心理物理量に基づいて評価した結果が報告されたという事例は知られていないようであると付け加えた。

福田は、ホログラムについて、偽造防止目的のホログラムの評価を心理物理量によって行うという試みはこれまでのところ報告されていないのではないかと説明した。ただし、福田は、ホログラムをはじめとする光学素子を利用したアートや立体ディスプレイの研究分野においては、そうした光学素子が人間の感覚に与える影響を定量的に評価しようという研究の報告がいくつか知られており、そうした分野の知見を活用しながら偽造防止目的のホログラムの評価方法を検討するという方向性も考えられるとの見方を示した。

また、松本は、人間の標準的な感覚モデルを構築し、人間の五感を計算機上でシミュレートするというアプローチが今後の研究テーマの１つとして考えられるのではないかというアイデアを説明した。

ロ．オープンな場における偽造防止技術の評価について

２つ目の論点として、岩下は、偽造防止技術の効果に対するエンドユーザの信頼を得るためには評価をオープンに実施していくことが必要ではないかとの問題意識を示し、各パネリストの見解を尋ねた。

松本は、暗号分野においては、暗号鍵等の秘密にすべき情報を適切に管理していれば暗号アルゴリズム自体を公開しても安全性を損なう心配はないことから、オープンな場で評価が行われているという現状を紹介した。そのうえで、人工物メトリクスにおいても、人工物の製造時に発生するランダム性の再現の難しさに基づいて安全性を確保しており、人工物メトリクスにおける認証の方法自体を公開して評価することができると説明した。さらに、松本は、どの技術分野においても、偽造防止効果を損ねない範囲で情報を公開して議論を行い、共通認識を醸成することが重要であると述べた。

印刷技術による偽造防止技術について、金子は、紙幣等のアプリケーションにおいては評価をオープンに実施することは現実的とはいえないものの、ブランド・プロテクション等のアプリケーションにおいては、メーカー間で標準的な評価手法の構築に対するニーズもあるとみており、オープンな場での評価の意義について議論して共通認識を形成することは有用であるとの見方を示した。また、金子は、人間の五感による真偽判定を行う偽造防止技術については、真偽判定のポイントを適切に公開し、エンドユーザを啓蒙することで偽造防止効果の向上を図ることが重要であると述べた。

福田は、ホログラムは人工物メトリクスと比較すると既に広く普及しており、材料や製法に関する詳細な情報を公開することは現実的とはいえないとの認識を示したうえで、それらの情報が非公開であっても、ホログラムの光学特性に関する標準的な測定手法を構築することで一定の評価を実施可能であり、現在、測定手法や関連する用語の標準化を進めている最中であると説明した。そうした標準化による効果

として、用語等に対する共通認識を形成しオープンな議論を行いやすくなることに加えて、統一的な評価により品質の低いホログラムを排除可能となり、偽造防止効果の向上やホログラムの産業振興につながるとの見方を示した。また、福田は、人間の五感によるホログラムの真偽判定においてもエンドユーザの啓蒙が重要であると説明した。

本間は、まず、暗号ハードウエアの耐タンパー技術においてもオープンな場での評価が必要であるとの見方を示した。そのうえで、個々の暗号ハードウエアの実装に関する詳細な情報を公開することは困難であるのが実情であるが、可能な範囲で情報をオープンにしていくとともに、技術仕様が公開されている SASEBO を用いて評価を行い、その結果をオープンにして共通認識を形成するというアプローチが可能であると説明した。

ハ．偽造防止技術の評価に関する今後の方向性について

最後に、岩下は、今後の各偽造防止技術の評価や人工物メトリクスの検討のあり方について各パネリストの見解を尋ねた。本間は、現行の IC カードをはじめとする暗号ハードウエアの偽造防止効果は相当高いレベルにある点を強調したうえで、今後、さらに偽造防止効果を高めていくための新しい技術として人工物メトリクスの利用を検討することは有用であると説明した。福田は、ホログラムの偽造防止効果を向上させるうえで人工物メトリクスのアイデアは有効と考えられると説明したうえで、ホログラムと人工物メトリクスを組み合わせて利用する際には、読取安定性等の面からも客観的に評価していくことが求められると述べた。金子は、印刷技術についても特に一般製品分野等では可能な範囲で情報をオープンにしたうえで評価を行っていくことが望ましいとの認識を示したほか、人間の五感による偽造防止技術を定量的に評価する方法として心理物理量に基づく評価が考えられるが、こうした分野の研究も今後進展していくことを期待したいと説明した。松本は、機械読取りを想定した人工物メトリクスだけでなく、人間の五感によって真偽判定を行うタイプの人工物メトリクスも考えられるとのアイデアを示したうえで、今後も人工物メトリクスの研究を深めていきたいと述べた。

各パネリストの発言を受けて、岩下は、いずれの分野においても、偽造防止技術の効果の定量的な評価とオープンな議論が重要であるとの認識が示されたことは今後の検討を進めていくためにも有益と思われると述べ、自由討議を締め括った。

(5) フロアからの主な質問

フロア参加者から、人工物メトリクスが普及する重要なポイントの 1 つは安価に実装可能であるか否かであると考えられるが、例えば、安価な読取装置によって実現可能な人工物メトリクスとしてはどのようなものが有望と考えられるかとの質問が寄せられた。これに対して、松本は、IC チップ内に格納された PUF による人工物

メトリクスの場合には認証に用いるデータの読取りがICチップ内で行われるため、別途読取装置を用意する必要がないケースがあるほか、別途読取装置を用意する必要があるケースの場合でも、当該人工物メトリクスが普及すれば量産化によって安価な読取装置を使用することが可能になると期待できると説明した。本間は、PUFを実装する回路を比較的安価に製造できる可能性があるとの見方を示したほか、人工物メトリクスの場合、人工物の製造時に個体識別するためのIDを書き込む処理が不要であるというメリットがあると説明した。

また、フロア参加者から、真偽判定を行う場合には人工物が本物の集合（グループ）に含まれるか否かを識別する「グループ識別」で十分であり、個体識別は必要ないように思われるが、どのようなアプリケーションであれば個体識別が求められるかとの質問が寄せられた。これに対して、松本は、個体識別はグループ識別よりも高い確率でより狭い範囲のグループに絞り込んで認証を行うものであり、高度なセキュリティを確保したいアプリケーションに用いられることが想定されると説明した。そのうえで、電子データを用紙に印刷して相手に渡す際に、取引慣行上の理由等から当該用紙を特定して確認できることが求められるケースが考えられると説明し、家庭用のプリンターやスキャナー等の安価な装置を用いて実現可能な人工物メトリクスが開発されれば、さまざまな用途に利用できるようになる可能性があると回答した。

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し、シンポジウムを締め括った。

今回のシンポジウムにおける発表や議論をみると、キーノート・スピーチにあったように、人工物メトリクスが偽造防止技術における新潮流として定着したとの印象をもった。具体的には、伝統的な偽造防止技術にはなかった「暗号学的アプローチ」に基づくセキュリティ評価が人工物メトリクスを対象にオープンな場において行われるようになってきたということである。暗号学的アプローチとは、評価対象となるシステム、想定される攻撃者、安全性の概念を明確に記述したうえで、当該システムの安全性を評価するというものである。こうしたアプローチを暗号アルゴリズムだけでなく、生体認証や量子暗号にも適用する研究事例が発表されており、同じ傾向が人工物メトリクスの研究においても読み取れる。

パネル・ディスカッションについては、印刷技術、ホログラム、暗号ハードウエアの耐タンパー技術と多様な分野における研究開発の動向が紹介され、大変興味深い内容であった。特に、暗号学的アプローチの浸透度合いが、印刷技術、ホログラム、暗号ハードウエアの耐タンパー技術の順に段階的に高くなっており、各分野におけるセキュリティ評価に向けた取組みに差異が生じている一方で、オープンな議論を通じて共通認識を形成していくことがいずれの分野においても重要であること

が確認できたのは、今回のシンポジウムの大きな成果であったといえよう。

また、人間の五感によって真偽判定を行う技術に関して、個人差等によって十分な判定を毎回期待しづらいとの話もあった。そうした人間が関与する部分をどう取り扱うかはセキュリティ技術分野共通の課題であり、重要な研究テーマである。印刷技術の評価手法の 1 つとして心理物理量を利用するという説明があったが、そうした人間の心理や感覚に関係する研究成果を他の情報セキュリティ分野にも適用できないかについては検討することも有用であろう。

日本銀行金融研究所情報技術研究センターには、今後も情報セキュリティ・シンポジウムを継続して開催し、わが国の金融業界における情報セキュリティの一層の向上に資する活動を引き続き行っていくとともに、金融業界、学界、産業界の人材交流の場を提供するための積極的な取組みを期待したい。

参考文献

岩下直行、「偽造防止技術の新潮流：金融業務における人工物メトリクスの可能性」、『金融研究』第 28 巻第 2 号、日本銀行金融研究所、2009 年、129～142 頁（本号所収）

宇根正志・田村裕子・松本　勉、「偽造防止技術のなかの人工物メトリクス：セキュリティ研究開発の動向と課題」、『金融研究』第 28 巻第 2 号、日本銀行金融研究所、2009 年、143～182 頁（本号所収）

田村裕子・宇根正志、「人工物メトリック・システムにおける耐クローン性の評価方法の構築に向けて」、『金融研究』第 28 巻第 2 号、日本銀行金融研究所、2009 年、183～218 頁（本号所収）