第6回情報セキュリティ・シンポジウム「金融分野における人工物メトリクス」の模様

1．はじめに

日本銀行金融研究所は、平成16年3月26日、「金融分野における人工物メトリクス」をテーマとして、第6回情報セキュリティ・シンポジウムを開催した。

人工物メトリクスとは、証書、証券、紙幣、カード等の人工的に製造された物理媒体（人工物）を、おのおのの個体に特有の特徴を用いて認証する技術である。近年、デジタル画像処理技術が発達、普及した結果、証書やカードを精巧に偽造・複製・改ざんすることが、従来よりも容易になってきた。金融分野では、有価証券、預金通帳と印鑑、紙幣、キャッシュ・カード、クレジット・カード等さまざまな人工物が利用されているため、それらの偽造・複製・改ざんを防止するための技術を強化していくことが求められている。今回のシンポジウムでは、情報セキュリティ技術の手法を用いて、人工物のセキュリティを向上させる技術である人工物メトリクスに着目し、金融業務における実際の適用事例を紹介するとともに、今後の課題について議論した。

シンポジウムは、キーノート・スピーチ、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（プログラムは下表のとおり）、フロアには情報技術に関連する学界、行政、金融機関、電機メーカー等から研究者・実務家約80名の参加を得た。

〈プログラム〉

キーノート・スピーチ「金融業務と人工物メトリクス」 ：松本勉（横浜国立大学教授）
研究発表1「人工物メトリクスの精度評価と実装事例」 ：松本弘之（日本発条株式会社情報セキュリティ事業部）
研究発表2「人工物メトリクスのセキュリティ評価」 ：宇根正志（日本銀行金融研究所研究第2課）
パネル・ディスカッション「人工物メトリクスの現状と課題」
・パネル発表：小松尚久（早稲田大学教授）
・自由討議 ・パネリスト：松本勉、小松尚久、松本弘之、宇根正志 司会：岩下直行（日本銀行金融研究所研究第2課企画役）
総括コメント：今井秀樹（東京大学教授）

以下では、プログラムに沿って、キーノート・スピーチ、研究発表、パネル・ディスカッション、総括コメントの概要を紹介する（文責、日本銀行金融研究所。文中敬称略）。

2．キーノート・スピーチ「金融業務と人工物メトリクス」

松本（勉）は、岩下との共同論文[1]に基づき、人工物の安全性低下の事例、既存のセキュリティ対策の限界、人工物メトリクスの基本的な考え方について次のように発表した。

（1）人工物の安全性低下の事例

金融業務においては、伝統的に、証書、証券、紙幣、カード等の人工物が使用されてきた。金融取引の電子化が進められているものの、すべての金融取引が電子化に適しているわけではなく、金融業務の安全性は、引き続きこれらの人工物に大きく依存している。ところが、最近、デジタル画像処理技術が発達し、パソコン、スキャナ、プリンタ等が普及した結果、人工物が不正に偽造・複製・改ざんされ、金融取引の安全性、信頼性が損なわれる事件が増えてきている。具体的には、①印鑑の偽造による盗難通帳からの預金払出し、②各種カードの偽造・不正使用、③紙幣の偽造等の事例が挙げられる。

（2）既存のセキュリティ対策の限界

従来、人工物のセキュリティ対策は、「人工物に関する情報を極力秘匿し、人工物を製造する側の技術的優位性を保つ」という考え方に基づくものが中心であった。しかし、情報技術が進歩、普及するとともに、製造者の技術的優位性は小さくなる傾向にある。

そもそも、金融取引に利用される人工物は、一般の利用者の手に渡されてしまうことが多いため、攻撃者にその特徴を分析されてしまうことを防止できない。読取装置が広く普及している人工物の場合、装置の内部構造を秘匿しておくことも難しい。また、人工物のセキュリティ対策に関する情報を秘匿していると、攻撃者が製造者の技術にどの程度追いついてきているかがわからないという問題も発生する。過去のカード偽造犯罪においても、実際に大規模な不正行為が発生してから製造者が不備に気づくという事例が散見された。

1 松本勉・岩下直行、「金融業務と人工物メトリクス」、『金融研究』第23巻第2号、日本銀行金融研究所、2004年、169～186頁（本号所収）。

こうした問題に対処するためには、従来の発想を転換して、人工物の製造技術に関する情報を公開し、人工物のセキュリティを学術研究の対象としてオープンな場で安全性に関する研究を進めていくことが考えられる。例えば、暗号アルゴリズムは、技術内容を公開しつつも、暗号化に必要な「鍵」を秘匿することによって安全性を確保している。その結果、暗号アルゴリズムを学術研究の対象とすることができ、万一安全性に欠陥があれば、オープンな場で問題点が指摘され、迅速な修正が可能となった。しかし、人工物における既存のセキュリティ技術の多くは、情報を秘匿することによって製造者の技術的優位を実現しているため、情報を公開すると安全性が損なわれる惧れがある。このため、上記のようなアプローチをとるためには、「情報を公開しても安全性が損なわれないセキュリティ技術」が必要となる。

(3) 人工物メトリクスの考え方

このような発想から生まれた技術が人工物メトリクスである。人工物メトリクス（artifact-metrics）とは、バイオメトリクス（biometrics、生体認証）という用語を参考に、人工物（artifact）と測定（metrics）を組み合わせた造語であり、おのおのの人工物に対して異なるランダムな固有パターン（人間の指紋に相当するもの）をあらかじめ付与しておき、認証時にその固有パターンを計測し、事前に計測しておいた情報と照合することによって人工物が本物であるかどうかを検証するという仕組みが想定されている。人工物メトリクスを実現するために構築された、個々の人工物を識別して照合するシステムのことを、人工物メトリック・システムと呼ぶ。人工物メトリック・システムにおいては、ランダムに生成された人工物の固有パターンが人為的に再現困難であれば、「製造者と全く同じ材料と装置を用いても人工物が複製できない」という効果が期待できる。その結果、人工物の製造・検証にかかる情報が公知となってもセキュリティが低下する懸念が少ないため、技術内容を公開し、オープンな場での分析の対象とすることができる。

人工物メトリクスに利用される固有パターンを実現する技術としては、さまざまな提案が行われており、これらの技術のなかには、金融取引において利用される証書、証券、紙幣、カード等に適用することが可能と考えられるものも存在する。既に、株券の偽造・複製対策として、磁性ファイバ（磁性材料を内包した繊維）を株券用紙に混入し、用紙内部でランダムに形成される磁性ファイバの三次元構造を固有パターンとして利用するという技術が利用されはじめている。

(4) 人工物メトリクスの安全性評価の方法

人工物メトリクスの利点は、その安全性を客観的かつ定量的に評価できる点にある。人工物の偽造・複製を防止する観点からは、「本物を見本にして固有パターンをコピーしたクローンを作製し、これを提示してシステムの認証を通過させようとする攻撃」（デッド・コピー攻撃）への耐性が問題となる。そこで、さまざまな工夫

を凝らして実際に人工物のクローンを作製し、それがどの程度システムの認証を通過するかを実験することにより、そのシステムの安全性に対する定量的な評価が可能となる。こうした評価結果に基づき、システムの設計を変更したり、リスクを予測したりすることができる。

(5) 今後の課題

人工物メトリクスを今後さまざまな業務に活用していくための課題として、①安全性評価について検討を深めること、②具体的な適用業務を想定して、運用技術やコスト等の条件を加味したより実践的な検討を行うことの2点が挙げられる。特に、人工物メトリクスの安全性評価に関しては、多様な攻撃法を想定して十分な検証が行われることが必要であり、そのためにも、可能な限り技術内容を公開し、オープンな場で議論が行われることが望ましいと考えられる。

3．研究発表1「人工物メトリクスの精度評価と実装事例」

松本(弘) は、宇根、松本(勉)、岩下、菅原との共同論文[2]に基づき、人工物メトリクスの基本的な概念、既存の人工物メトリック・システムの事例、人工物メトリック・システムの認証精度評価の現状と課題について次のように発表した。

(1) 人工物メトリクスとは

人工物メトリクスという言葉は新しく作られたものだが、そのコンセプト自体は比較的古くから提案されていた。提案された人工物メトリック・システムの具体例としては、①光を反射する粒状物をラベルに混入し、その粒状物の光反射のパターンによって偽造や改変を検知するシステム、②窓状の透明な樹脂内でランダムに固まった複数のファイバについて、2つの撮像素子によって異なる角度から観察した画像（視差画像）を得て、その幾何学的な固有パターンを抽出し、個々の被検査対象物の固有パターンとして検証するシステム、③磁性材料を内包したファイバを紙等の基材にランダムに分散させて、磁気センサによりその磁性パターンを個々の証書の固有パターンとして検証するシステム等が挙げられる。

こうした人工物メトリック・システムの主な特徴としては、①人工物の素材や組成を調整し、認証精度や耐久性を操作可能であること、②人工物の形状を規格化し、人工物の読取時に発生する誤差を抑制可能であること、③評価サンプルを揃えやすく、大規模な実験を行いやすいことの3つが挙げられる。

2 松本弘之・宇根正志・松本勉・岩下直行・菅原嗣高、「人工物メトリクスの評価における現状と課題」、『金融研究』第23巻別冊第1号、2004年、61～140頁。

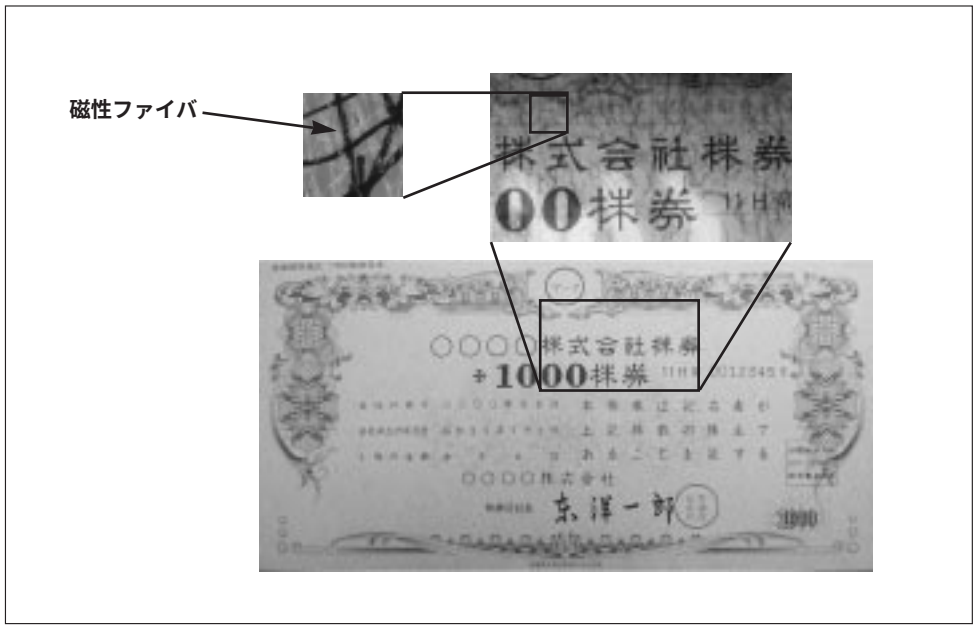
人工物メトリック・システムの用途としては、①人工物が本物であることを検証する用途、②人工物が本来の状態に保たれていることを検証する用途、③人工物を識別する用途が挙げられる。

(2) 金融業務への人工物メトリック・システムの実用化事例

人工物メトリック・システムは、既に、信託銀行における株券の発行・照合装置のセキュリティ対策のために実用化されている。個別株券認証システム（IOSAS）と呼ばれるこの人工物メトリック・システムは、株券用紙に磁性ファイバをランダムに分散させ、磁性ファイバから得られる磁気パターンを固有パターンとして株券を認証する。磁性ファイバは株券用紙内部において紙の繊維と絡み合って複雑な三次元構造を形成し、その三次元構造を再現することは困難とみられている（図1参照）。

IOSASにおいて利用される株券にはそれぞれ個体識別番号が印刷されており、株券発行時には、各株券の固有パターンが抽出され、参照データとして個体識別番号とともにデータベースに記録される。株券検証時には、株券の個体識別番号に対応する参照データがデータベースから読み出され、株券から得られた固有パターンと参照データが照合される仕組みとなっている。

図1　IOSASにおける株券のサンプル



（3）人工物メトリック・システムの認証精度評価の現状

一般的な情報システムをセキュリティの観点から評価する場合には、①機密性、②完全性、③可用性、④責任追跡性、⑤真正性、⑥信頼性という6つの特性に着目するケースが多い。これらのうち、人工物メトリック・システムの場合には、真正性（必要とされる精度で人工物の認証を実行可能であること）の評価が必須である一方、真正性以外の特性については、システム構築におけるセキュリティ管理に依存する部分が大きく、人工物メトリック・システム固有の評価の必要性は少ない。そこで、以下では、真正性の評価、すなわち、認証精度の評価に着目して分析することとする。

いくつかの人工物メトリック・システムにおいて認証精度の評価結果が公表されているが、そのほとんどがクローンによる攻撃を想定しないものとなっている。クローンによる攻撃を想定しない認証精度評価においては、評価指標として、バイオメトリック・システムで使われている指標を利用するケースが多い。例えば、誤一致率（1回の照合において「不一致」とすべき人工物を誤って「一致」と判断する確率）や、誤不一致率（1回の照合において「一致」とすべき人工物を誤って「不一致」と判断する確率）等が代表的な指標として用いられている。

これに対し、クローンを想定した認証精度評価においては、評価指標として、ブルート・フォース攻撃成功率やクローン一致率を利用することが提案されている。クローン一致率とは、1回の照合において、「不一致」とすべきクローンを誤って「一致」と判定してしまう確率である。このようなクローンを想定した精度評価については、人工物メトリック・システムにおける検討がバイオメトリック・システムよりも先行しているといえる。ただし、バイオメトリック・システムの分野においても、近年、「人工指」や「人工虹彩」といった偽造された生体情報に関する研究が開始されている。

（4）認証精度評価に関する今後の課題

人工物メトリック・システムの認証精度評価に関しては、本格的な検討が開始されて間もない段階にあり、今後、以下の検討を進める必要がある。

① 認証精度の評価基盤の構築： 認証精度評価を行う際の用語、想定される攻撃、評価指標等を明確にするとともに、標準化を行うこと。
② 認証精度の評価手法の構築： 共通の評価指標に基づいて認証精度の評価結果を示す手法について検討を行うとともに、シミュレーションによる認証精度評価においては、理論的な説明や実サンプルによる検証によってシミュレーションの妥当性を示す方法を検討すること。
③ 耐クローン性の評価手法の構築： 実際にクローンを作製し、クローン一致率等の指標に基づいて認証精度評価の結果を示す手法について検討すること。

④ 認証精度の基準値設定： 人工物メトリック・システムの利用者が異なるシステムの比較を行ううえで、また、設計者がシステムの仕様を検討するうえで、認証精度の目安となる「基準値」をどのように設定するかについて検討すること。

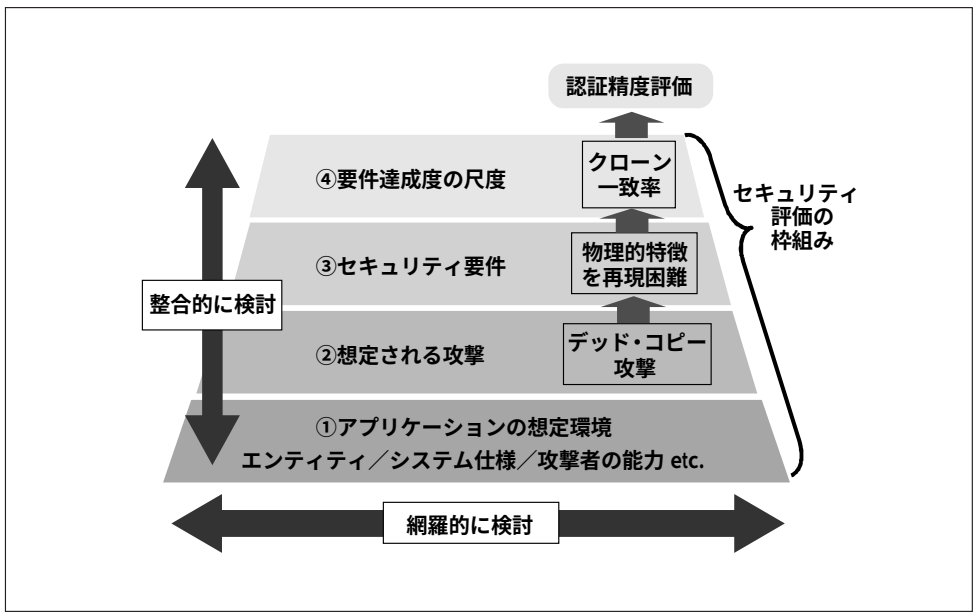
4．研究発表2「人工物メトリクスのセキュリティ評価」

宇根は、松本（弘）、松本（勉）、岩下、菅原との共同論文[3]に基づき、人工物メトリック・システムにおけるセキュリティ評価の枠組みと、デッド・コピー攻撃を想定した認証精度の評価事例に関して次のように発表した。

（1）セキュリティ評価の枠組み

情報システムのセキュリティ評価を行う際には、①アプリケーションの想定環境を明確にして、②想定される攻撃、③セキュリティ要件、④各要件の達成度の尺度を定めることが必要である。これらの要素をまとめて「セキュリティ評価の枠組み」と呼ぶ（図2参照）。

図2　セキュリティ評価の枠組み



3 松本弘之・宇根正志・松本勉・岩下直行・菅原嗣高、「人工物メトリクスの評価における現状と課題」、『金融研究』第23巻別冊第1号、2004年、61〜140頁。

例えば、セキュリティ評価の枠組みを検討する過程において、仮にアプリケーションの想定環境からデッド・コピー攻撃が想定される場合、デッド・コピー攻撃に対抗するためのセキュリティ要件として「人工物の物理的特徴を再現困難であること」という要件を設定し、その達成度の尺度としてクローン一致率を設定することが考えられる。こうした検討は、最終的に、クローン一致率の測定という認証精度評価につながっていく。また、セキュリティ評価の枠組みを検討する際には、各要素間の整合性や網羅性にも留意する必要がある。

(2) セキュリティ評価の枠組みの検討：想定環境

ここでは、特定のアプリケーションを想定せず、人工物メトリック・システムの一般型を対象に、クローンによる攻撃を想定したセキュリティ評価の枠組みについて検討する。

検討対象とするシステムは、利用者、発行者、検証者によって構成されるとする。発行者は、人工物を製造・配布するとともに、人工物を回収・無効化する。検証者は、利用者の求めに応じて人工物を検証し、その結果を利用者に通知する。人工物の検証手続としては、人工物の識別情報（ID）と参照データをペアにしてデータベースに記録するとともに、人工物にIDを記録しておき、検証時には、IDに対応する参照データをデータベースから読み出したうえで、人工物の固有パターンと照合するという方式を想定する。

攻撃の前提条件に関しては、次の4つの想定を置く。すなわち、攻撃者は、①検証者および発行者と結託しない、②人工物の固有パターン抽出方法等の検証手続に関する情報を入手する、③人工物の検証を行う装置（検証用装置と呼ぶ）を不正に操作可能である、④人工物の発行を行う装置を不正に操作することはできないとする。

(3) 攻撃・セキュリティ要件・要件達成度の尺度

こうした想定環境下では、①ブルート・フォース攻撃、②無効な人工物を再利用する攻撃、③デッド・コピー攻撃、④いかなる検証対象に対しても「受理」と判定するように検証用装置を操作する攻撃がまず考えられる。

まず、ブルート・フォース攻撃に対抗するためには、「攻撃に使われる人工物に記録されるIDを適切に偽造することが困難であること」というセキュリティ要件を設定することが考えられる。また、本要件の達成度の尺度としては、ブルート・フォース攻撃成功率等が挙げられる。無効な人工物を再利用する攻撃に対しては、「無効な人工物を再利用することが困難であること」というセキュリティ要件を設定し、人工物の無効化に関するセキュリティ管理・運用がどの程度確実に実行されているかをチェックすることによって、本要件の達成度を測ることが考えられる。デッド・コピー攻撃に対しては、「人工物の固有パターンを再現することが困難で

あること」というセキュリティ要件を設定し、クローン一致率等によって本要件の達成度を測ることが考えられる。検証用装置の不正操作による攻撃に対しては、「検証者に検知されずに検証用装置を不正に操作することが困難であること」というセキュリティ要件を設定することが考えられる。本要件の達成度は、検証用装置の耐タンパー化の度合い、あるいは、耐タンパー性を確保するためにどのような対策が講じられているかによって測ることができると考えられる。

以上のような手順によって、セキュリティ評価の枠組みを検討することができる。今後、クローン一致率をはじめとする各種の要件達成度の尺度をどのように確立していくかが重要な課題である。

(4) デッド・コピー攻撃を前提とした評価事例の紹介

次に、デッド・コピー攻撃を前提とした人工物メトリック・システムの評価事例を紹介する。本事例では、実際に人工物のクローンを作製し、クローン一致率を測定することにより、セキュリティ評価を行った。

評価対象の人工物メトリック・システムは、紙に漉き込まれた磁性ファイバによって生成される磁気パターンを固有パターンとして利用するものであり、認証対象の人工物（以下、F-paperと呼ぶ）、入力端末、データベースを備えたパソコンから構成される（図3参照）。F-paperの表面には識別情報（ID）が印字されている。F-paperの検証時には、まず入力端末にF-paperを挿入して、F-paperの磁気パターンとIDの読取りを行う。次に、パソコンにおいて、読み取った磁気パターンから固有パターンを抽出すると同時に、データベースからIDに対応する参照データを読み出し、固有パターンと照合する。

図3　評価システムの外観

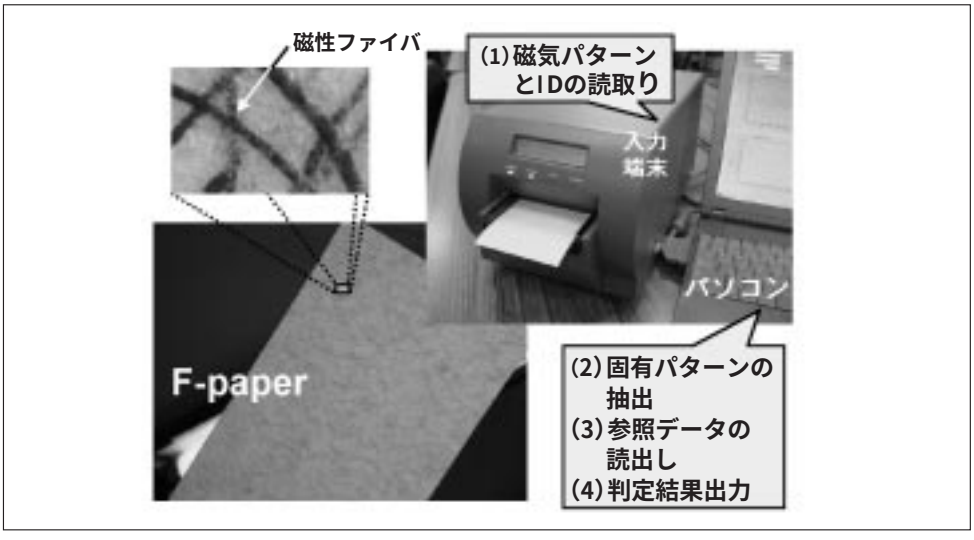
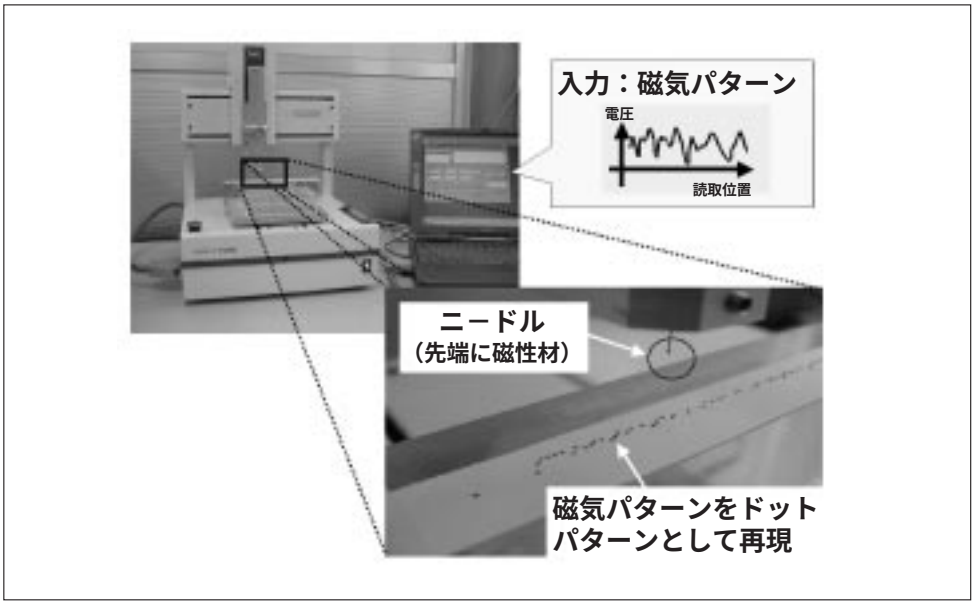


図4　デッド・コピー用のロボットの外観



こうしたシステムに対して、攻撃者がF-paperのデッド・コピーの作製を試みるという状況を考える。ただし、攻撃者は、①発行者および検証者と結託しない、②人工物の固有パターン抽出方法、パターン照合方法を知らない、③パソコンを不正に操作することはできない、④入力端末を用いてF-paperの磁気パターンのみを観察可能であるとする。デッド・コピーの具体的な実行手順は、①正規のF-paperの磁気パターンを入力端末で読み取る、②ロボット（図4参照）を用いて、磁気パターンを再現するように位置を調整しながらドット単位で磁性材を紙に塗布する、③磁性材を塗った紙を別の紙に貼り付け、IDを書き込むというものである。

（5）クローン一致率の測定

以上の手順によってクローンを100枚作製したうえで、判定しきい値、読取範囲、読取時の解像度等のパラメータをいろいろ変えてクローン一致率を測定した結果、次の2つの観察が得られている。

① クローン一致率は、正規のF-paperによって測定された誤一致率よりも大きくなる傾向にある。
② 各種パラメータを変化させた場合、クローン一致率の変化の方向性が誤一致率の変化の方向性と異なる場合がある。

これらの観察から、デッド・コピー攻撃を想定したセキュリティ評価を行う際には、実際にクローンを作製してクローン一致率を測定してみることが必要であるといえ

る。そのうえで、クローン一致率の実測値を手掛かりに、デッド・コピー攻撃に対して十分な安全性を確保できるように、各種パラメータを調整することが求められる。

5．パネル・ディスカッション「人工物メトリクスの現状と課題」

(1) パネル発表「バイオメトリクスと人工物メトリクス」

小松は、人工物メトリクスと対比させつつ、バイオメトリクスにおける認証精度評価の現状について以下のとおり発表した。

バイオメトリクスとは、①普遍性（誰もが持っている）、②唯一性（本人以外は同じ特徴を持たない）、③永続性（時間の経過とともに変化しない）の3つの条件を備えた、人間の生体的な測定結果を指す言葉であり、身体的特徴（指紋、網膜、顔等）と行動的特徴（筆跡、音声等）の2種類に分類できる。バイオメトリクスを利用して本人を自動的に（automatically）確認する技術をバイオメトリック個人認証という。現在、指紋や虹彩を個人認証に利用するバイオメトリック・システムが、金融をはじめとして幅広い分野で採用されはじめている。今回のシンポジウムでは、人工物メトリクスにおいて認証精度の評価をどのように行うかが中心的なテーマとなっているが、バイオメトリクスの分野では、認証精度評価の標準化が活発に進められている。わが国では、日本規格協会・情報技術標準化研究センター（INSTAC）傘下のバイオメトリクス標準化調査研究委員会において、1996年から続けられた検討の成果をもとに、2000年度から標準化作業が開始された。

バイオメトリクスの認証精度評価を適切に行うためには、まず、利用者がどのような条件のもとでバイオメトリック・システムを使いたいと考えているかを明確にしたうえで、その要求条件に対応した情報を提供することができるように評価を行うことが必要である。バイオメトリクス標準化調査研究委員会では、こうした考え方を踏まえたうえで検討を進め、これまでに、指紋、虹彩、血管パターン、顔、音声、署名の認証精度評価方法に関する技術報告書を公表している。

これらの技術報告書は、評価の対象（照合アルゴリズム／照合装置／本人認証システム）を明確にしたうえで、各種評価指標の使い方や評価結果レポートの書き方について規定したものである。バイオメトリック・システムは一種のブラック・ボックスとして捉えられており、認証精度評価の際には、「システムにどのようなデータを与え、どのような出力が得られるのか」を示す内容となっている。

バイオメトリクス標準化調査研究委員会では、バイオメトリック・システムを利用・設計する際の指針として運用要件導出ガイドラインを作成しており、これらも技術報告書として公表されている。運用要件導出ガイドラインには、バイオメトリック・システムの利用者の要求条件を定量的に導出する方法が記述されており、本ガイドラインによって利用者の要求条件が明確になれば、バイオメトリック・システ

ムのベンダーはその要求条件に沿ったシステムを提供しやすくなる。認証精度評価方法に関する技術報告書には、ベンダーがシステムの認証精度を評価する手順と評価項目が記述されており、これらの技術報告書に沿った認証精度評価を実施することによって、システムの利用者は各ベンダーの製品を比較・検討することができる。人工物メトリック・システムにおいても、こうした利用者の要求条件を明確化するための技術報告書を検討することが必要であろう。

また、異なるベンダーが提供するバイオメトリック・システムの相互運用性の確保も重要な課題である。今後バイオメトリクスが普及すると、生体情報の登録を行う装置と検証を行う装置がそれぞれ異なるベンダーから提供されるケースが考えられる。その場合、登録された生体情報のデータを用いて適切に検証を実行できるように、双方の装置において処理されるデータの品質を調整する必要がある。その際には、生体情報の経年変化も考慮することが求められる。こうした相互運用性の確保は、人工物メトリック・システムにおいても重要な課題の1つであると考えられる。

(2) 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、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、人工物メトリクスとバイオメトリクスの関係、および、これらの研究分野における脆弱性分析の重要性についてパネリストの見解を尋ねた。これに対して、**松本(勉)**は、バイオメトリクスとは異なる興味から人工物メトリクスの研究を開始したことを説明した後、基本的な概念や評価の観点や方法については両者の間に密接な関連性があることを説明した。また、今後、バイオメトリクスが日常生活の多くの場面で活用されるようになると予想されるなか、人工物メトリクスと同様に、バイオメトリクスにおいてもクローンを想定した脆弱性分析の重要性が高まっていると指摘した。そのうえで、バイオメトリクスにおいてクローン対策を進めていく際には、人工物メトリクスでは利用することができない「人間の生体検知機能」[4]を活用することが求められるとの見解を示した。一方、**小松**は、脆弱性分析の基本的な考え方は人工物メトリクスが先行しており、バイオメトリクスにおいては、クローンを想定した脆弱性分析がこれまで十分に行われてこなかったと述べた。そのうえで、今後、バイオメトリック・システムにおける脆弱性に関する検討を認証精度評価の枠組みのなかで進めていく必要があるとの見方を示したほか、セキュリティ対策をどのように既存のバイオメトリック・システムに取り込んでいく

4 人工的な模型等を用いて指紋、虹彩等のバイオメトリック認証を不正に通過されることを防ぐために、生体が提示されたことを確認する機能。

か、また、脆弱性やセキュリティ対策の内容を利用者にどのよう伝えるかといった運用上の課題も重視すべきであると説明した。また、クローン対策として、一般には、松本が指摘した生体検知機能を活用する方法に加えて、複数の異なる生体情報を組み合わせた認証方式（マルチモーダル認証）も有効であることを説明した。

次に、**岩下**は、個別株券認証システム（IOSAS）の開発時における問題点や今後の課題、株券の検証を行う装置が複数存在した場合の相互運用性やセキュリティ評価についてパネリストに尋ねた。これに対して、**松本（弘）**は、IOSAS開発時のエピソードとして、顧客に対してIOSASの認証精度を説明する際に、バイオメトリクスの分野で確立されていた各種誤り率の指標が有効であったという事例を紹介した。また、株券の検証を行う装置の相互運用性に関しては、現在実運用されているIOSASでは、検証用装置が東京と大阪の信託銀行の店舗に1台ずつ設置されており、それらの相互運用性が十分に確保されるようにシステムの調整を行っていると説明した。さらに、**松本（弘**）は、検証用装置の台数が増えると、それらの相互運用性を確保するために、認証精度の評価を実施したり、設定の調整を行ったりするための手間が必要となると説明し、シミュレーションを利用した評価手法の確立等によって検証用装置の認証精度評価を効率的に実施できるようにしていくことが望まれると述べた。一方、**宇根**は、検証用装置がどのような環境のもとで管理されるかによって、想定される攻撃やセキュリティ要件が異なってくると説明し、検証用装置が特定の機関だけに設置されている場合とは異なり、一般の商店にあまねく設置されている場合には、攻撃者が検証用装置を不正に操作する等の状況を想定することも必要になると述べた。

最後に、**岩下**は、ICカード、ICチップと人工物メトリクスの選択、両者の長所・短所についてパネリストの見解を尋ねた。これに対して、**松本（勉）**は、ICカードに人工物メトリクスを適用することによって、仮にICカードの耐タンパー性が破られたとしても、人工物メトリクスによってICカードの偽造・複製の有無を検証することができるという意味で、ICカードのセキュリティ向上に人工物メトリクスを活用することができると説明した。さらに、**松本（勉）**は、ICカードの場合にはICチップを使用不能にするという攻撃が考えられるが、人工物メトリクスの場合には、人工物の固有パターンがすべて破壊されない限り、人工物の認証を行う余地が残るという長所があると説明した。

以上の自由討議を踏まえて、**フロア参加者**から、①人工物メトリック・システムにおいて「必要とされる認証精度」が確保されているか否かを評価していく必要があるという議論があったが、こうした「必要とされる認証精度」をどのように決定すればよいのか、また、②人工物メトリクスの認証での判定方法（相関係数等の値と判定しきい値との大小関係によって受理か拒否かを決定）は、暗証番号における判定方法（暗証番号があらかじめ登録されたものと同一であれば受理、そうでなければ拒否）と異なっているが、これらの判定方法の関係をどのように考えればよいかという2つの質問が寄せられた。これらの質問に対して、**松本（勉）**は、現時点

では明確な答えが出ておらず、いずれも今後の重要な課題であると説明したうえで、人工物メトリクスの場合、一定の認証精度が必要とされる場面において、コストが許す範囲で人工物の形状や認証の各種パラメータを調整し、目標とする認証精度に近づけることが可能であると説明した。また、**小松**は、バイオメトリクスの分野においても同様の課題が存在し、明確な回答はないことを説明したうえで、一般には、バイオメトリクスを暗証番号による認証と組み合わせて利用するケースが多く、その場合、バイオメトリクスの認証精度評価によって、従来の暗証番号による認証に比べてどの程度セキュリティが向上したか、その結果、利用者の要求条件が満足されているかを確認することができると説明した。また、**小松**は、「バイオメトリック・システムはある確率で破られてしまう可能性がある」ことを十分認識したうえで、そうした場合においてもセキュリティを維持するためにはどのように対策を講じる必要があるかを検討することが重要であるという点を強調した。

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、**宇根**は、人工物メトリクスやバイオメトリクス等の技術を活用して金融取引のセキュリティ向上を図る際には、学会等における最先端の研究成果を踏まえて何が問題となっているのかを理解すると同時に、どのような環境において技術を利用するのかを明確にすることが重要であると述べた。**松本（弘）**は、利用者が安心して使用できる人工物メトリック・システムやバイオメトリック・システムを提供するという観点では、システムの認証精度の評価基盤・手法の構築が大きな課題であり、こうした課題を学会等のオープンな場での議論を通じて検討していくが重要であると述べた。**小松**は、脆弱性分析を含めた認証精度評価についてオープンな場で議論していくことの重要性を改めて指摘したうえで、技術者として、バイオメトリック・システムや人工物メトリック・システムの認証精度に関する限界を見極め、十分に対応できない部分については運用でカバーしていくといった観点からの検討も必要ではないかと述べた。また、**小松**は、人工物メトリクスにおける認証精度評価を実施する際に、バイオメトリクスの分野で確立された統計的手法を活用すると有用であろうとの見方を示した。**松本（勉）**は、まず、松本（弘）、小松と同様に、オープンな場での議論を通じた人工物メトリック・システムの検討が重要であることを強調した。そのうえで、業界のコンセンサスを得ながら、公開可能な情報は公開し、利用者の要求を反映した指標や評価方法を確立していくことが求められると述べた。

6．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してシンポジウムを締め括った。

今回のシンポジウムでは、「金融取引に利用される証書、証券、紙幣、カード等の人工的に製造された物理媒体」を対象に、それらのセキュリティをいかに確保するかという問題について議論が行われた。多発するカード偽造犯罪や盗難通帳による預金の不正引出し等を考えれば、これらはまさに喫緊の課題といえる。これまでの人工物の偽造防止技術は、情報を秘匿することが必須であったため、オープンな場で議論されることはあまりなかった。この結果、プリペイド・カードの偽造事件にみられるように､安全性に問題のある偽造防止技術が何度も繰り返して採用され､被害が拡大するという事態を招いてしまった。盗難通帳による預金の不正引出しの事例が端的に示しているように、印鑑も、本人確認技術としては既に破綻しているといわざるを得ない。

こうした問題に対し、従来の伝統的な偽造防止技術の立場とは異なり、暗号アルゴリズムの安全性評価等の研究スタイルを参考に、オープンかつ科学的な分析を行っているところに、今回のシンポジウムの特徴がある。

本日議論された人工物メトリクスという技術は、考え方としては比較的古くからある技術であるが、実用化することはなかなか難しいと考えられていた。本日の発表では、人工物メトリクスの技術の1つが実際の株券の偽造防止システムとして実用化されていることが報告されたが、大変先進的な取組みとして評価できるものである。

人工物メトリクスの基本にある考え方は、「物理特性を検出する技術」と「物理特性を複製する技術」が精度を競い合った場合、最終的には「検出する技術」の方が勝つということであろう。これは、細密な文字が「読めるが書けない」ことはあっても､「書けるが読めない」ことはない（読めないほど細密な文字は書けない）という日常的な常識に近いものである。そう考えると、今後、技術革新が進んでも、この技術が有効性を失うことは考えにくいという意味で、非常に将来性のある技術といえる。

現在、電子政府の構築が進められており、政府機関への申請・届出をインターネット経由で電子的に行うことが可能となりつつある。電子政府では、これまで紙の世界で利用されてきた印鑑に代わってデジタル署名を利用することとされており、デジタル署名方式の安全性を評価するプロジェクトが進められている。昨年度までの3年間、経済産業省と総務省が主催する暗号技術検討会 ── CRYPTRECにおいて議論を続け、電子政府推奨暗号を認定した。今年度は、その暗号の安全性を継続的に監視していくための組織が活動を開始し、世界的にみても例のない、暗号技術の安全性に関する厳重な監視体制が築かれている。

しかし、実際の行政手続の場面では、当面紙ベースと電子ベースが混在するほか、将来的にも、紙による申請・届出がなくなることは考えられない。このため、紙を利用した行政手続の安全性に技術的な問題があるとすれば、それは望ましいことではない。こうした問題に対処するためには、ICカードの利用と並んで、人工物メトリクスを適用していくことが考えられよう。

人工物メトリクスは、まだ利用が開始されたばかりであり、学会での研究も十分には進んでいない。しかし、今後、オープンな議論を進めていけば、この技術の可能性がより明確となるであろう。人工物メトリクスが既に株券に利用されているということは、類似の金融業務にも適用の可能性があると思われるし、全く別の用途、例えば、電子文書の長期保存における物理的な証拠としての機能を果たすという効果を期待できるかもしれない。人工物メトリクスに加えて、ICカードやICチップを利用した技術についても、その安全性に関する検討がよりオープンな形で進めば、両者を適切に選択したり、組み合わせたりすることが可能になる。このように、金融業務における物理的な媒体の安全性を高めるための技術の選択肢が増え、おのおのの適用業務において適切な技術を選択することができるようになれば、誰もが安心して利用できる金融システムが構築できるようになると考えられる。今回のシンポジウムは、そうした方向に進むための第一歩と位置付けることができよう。