IMES DISCUSSION PAPER SERIES

# 偽造防止技術の新潮流：
# 金融分野における人工物メトリクスの可能性

いわしたなおゆき
岩下直行

Discussion Paper No. 2009-J-1

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

**IMES Discussion Paper Series 2009-J-1**
**2009 年 3 月**

# 偽造防止技術の新潮流：金融分野における人工物メトリクスの可能性

岩下直行（いわしたなおゆき）*

要　　旨

金融取引においては、証券、紙幣、小切手、預金通帳、カード等の人工的に製造された物理媒体（人工物）が使用されている。こうした人工物は、偽造や不正使用を防ぐために、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を実装している。ところが、こうした偽造防止技術は、最近の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。将来にわたって金融取引の安全性を確保していくために、偽造防止技術の更なる高度化に向けて検討を進めていく必要がある。

こうした問題意識に基づき、人工物メトリクスと呼ばれる技術が提案された。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の難しいランダムな固有パターン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に対する抵抗力を維持できると考えられている。この性質を利用すれば、偽造防止技術の安全性を客観的に評価できるため、情報技術の進展による有効性の低下に対応することも可能かもしれない。偽造防止技術の研究領域においては、この新しい技術は、理論面、実装面の双方で、新しい潮流として定着しつつある。広く実務に適用することはまだ難しいものの、将来の偽造防止技術のあり方を考えるうえで無視できない存在となりつつある。

また、人工物メトリクスが目的とした、「安全性を客観的に評価できる偽造防止技術」というアプローチと似た動きが、既存のさまざまな偽造防止技術の研究においてもみられ始めている。

本論文では、人工物メトリクスという新技術を踏まえて、既存技術を含めた金融分野での偽造防止技術のあり方を検討し、次世代に向けた展望を示す。

キーワード：偽造防止技術、人工物メトリクス、セキュリティ、印刷技術、ホログラム、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: naoyuki.iwashita@boj.or.jp）

本稿は、2009 年 3 月 11 日に日本銀行で開催された「第 11 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．偽造防止技術の新しい潮流

金融取引においては、価値を表象するものとして、あるいは取引における正当な権利者であることを証明する目的で、さまざまな物理媒体が利用されている。証券、紙幣、小切手、預金通帳等には特殊な印刷を施した紙が、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にはプラスチックが使われている。これらの人工的に製造された物理媒体を、以下では「人工物」と呼称することとしよう。

歴史的にみると、こうした人工物には、以前は貨幣用の金、銀のようにそれ自体が価値を持つ素材が利用されていたが、その後、特にそれ自体は高価ではない紙やプラスチックが素材として利用されるようになった。そうした素材を利用することは、偽造防止という課題を背負い込むことを意味する。素材が安価であれば、それを加工して高額の金融取引に利用される人工物を偽造し、不正に利益を得たいという犯罪者側のインセンティブが高まるからである。このため、金融取引に利用される人工物には、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考案され、実装されてきた。ところが、こうした偽造防止技術は、最近の情報技術の進展に伴うデジタル画像処理技術の高度化や高性能な複写・印刷機の普及によって、その有効性が徐々に低下してきている。現段階では、既存技術を適切に利用している限り深刻な問題が生じる訳ではないが、将来にわたって金融取引の安全性を確保していくために、偽造防止技術の更なる高度化に向けて検討を進めていく必要がある。

これまで人工物に利用されてきた既存の偽造防止技術の大半は、「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、技術内容の詳細は秘密とされてきた。そのようなアプローチは、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、①技術進歩や秘密情報の漏洩により技術的優位性を喪失するという問題と、②そのセキュリティがどの程度脅威にさらされているかが、製造者側で検証できないという問題が存在している。特に②の問題は、製造者側が攻撃者の技術レベルを見通すことが難しいため、実際に大規模な不正行為が発覚するまでそれと気づかず、事態を深刻化させてしまうことがある。過去に何度か発生したプリペイドカードの偽造犯罪事例では、偽造が発生してから製造者側が迅速な対応を取れなかったために被害が拡大したといわれている（松本・岩下[2004]）。

こうした既存の偽造防止技術における問題を回避し得る新しい技術として、人工物メトリクスが提案されている。人工物メトリクスは、おのおのの人工物

に固有の特徴を利用して認証を行う技術である。典型的には、人工物に対して、おのおの異なるランダムな固有パターンをあらかじめ付与しておき、取引の都度、その固有パターンを計測し、事前に計測され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仕組みが利用される。人為的に制御することの難しいランダムな固有パターンを認証に利用することによって、人工物の製造方法や検証方法を秘匿しなくても偽造に対する抵抗力を維持できると考えられている。この性質を利用すれば、従来秘密とされていた人工物の製造技術に関する情報を公開し、アカデミックな分析の対象とすることが可能となる。こうしたアプローチによって、偽造防止技術の安全性を客観的に評価し、技術進歩による安全性の低下に対応しようという構想が示されている（松本ほか[2004]）。

この新しい構想は、日本銀行金融研究所が 2004 年に開催した第 6 回情報セキュリティ・シンポジウムの場で詳しく紹介された（日本銀行金融研究所[2004]）。その時点では、その理論的な枠組みも、その実装事例も、まだごく初期の素朴なものにすぎなかった。しかし、その後、約５年が経過し、人工物メトリクスは偽造防止技術の研究領域における新しい潮流として定着しつつある。すなわち、実装面では、人工物メトリクスの範疇に含まれる新しい技術提案が徐々に増えつつある。理論面についても、従来よりも洗練された安全性評価手法が考案されるなど、国内外で研究成果が蓄積されてきている。いずれもまだ技術的に完成したものとは言い難く、直ちに金融分野で広く実務に適用することは難しいが、将来の偽造防止技術のあり方を考えるうえで無視できない存在となりつつあるといえるだろう。

こうした潮流に歩調を合わせるように、人工物メトリクスが目的とした、「安全性を客観的に評価できる偽造防止技術」というアプローチと似た動きが、既存のさまざまな偽造防止技術の研究においてもみられ始めている。対象となる偽造防止技術によって異なるものの、一部では、学界レベルで定量的な評価方法が検討されるようになっているほか、製造業者の間で情報を共有し、用語・概念等の標準化を進める動きもある。既存の偽造防止技術においては、情報の秘匿が必要とされる部分も多いため、そうした動きがどこまで広がるか、その影響を含めて慎重に見極めていく必要はあるものの、セキュリティを向上させるという観点からは、そうした検討が進んでいくことは有意義と考えられる。人工物メトリクスによる新しいアプローチを踏まえて、既存技術を含めた幅広い視点から偽造防止技術の研究が進められていくことが望ましいと考えられる。

## ２．情報技術の進歩を味方につけるために

人工物の偽造防止は、それを製造・運用する側にとって、古くから存在していた課題であった。製造者と攻撃者が類似した伝統的な製造方法を利用している場合、技術レベルの差や秘密情報の有無によって「人工物を製造する側の技術的優位性」が強く働くため、製造者側は偽造のリスクについてある程度の見通しを立てることができていた。そうした見通しに基づき、例えば、定期的に採用する偽造防止技術を高度なものに更新していくといった対応が可能であった。

ところが、最近の情報技術の進歩は、こうした構造を大きく変えてしまった。「製造者と攻撃者が類似した製造方法を用いる」という前提が崩れ、例えば、「製造者が伝統的な印刷技術を利用する一方、攻撃者はデジタル画像処理技術を利用する」といった組合せが出現したのである。これらの技術は、技術が進歩してきた速さが全く異なる。伝統的な紙への印刷の技術が長い年月をかけて徐々に進化してきたのに比べて、デジタル画像処理技術が出現してから現在のレベルに高精度化したスピードは極めて急速であった。この場合、製造者側は、どのタイミングで偽造のリスクが高まるかを見通すことが難しくなる。

実際、デジタル画像処理技術の発達とパソコンの普及によって、高度な印刷の専門技術や高価な印刷機械を持たなくても、印鑑の印影、証券、紙幣等を高精度で複製することが可能になり、金融業務の現場で利用されている偽造防止技術の安全性、信頼性が損なわれる事例が数多くみられるようになった。もちろん、金融分野で実際に利用されている人工物は、さまざまな偽造防止技術が複合的に組み入れられているため、攻撃者が高精度のデジタル画像処理技術を使ったからといって、偽造が成功するとは限らない。しかし、情報技術の分野で、これまでの技術進歩のスピードが今後も続くとすれば、そうした問題はますます深刻化すると考えておかなければならないだろう。

印刷の精細さだけでなく、素材の質感、風合いなど、人間の感覚に影響を与える技術に関する研究が進むほど、「本物そっくり」の模造品、偽造品を製作するノウハウが豊かになる。そうした新しい技術を、特定の専門家だけではなく、一般人も簡単に使いこなすことができるというのが、最近の技術進歩の特徴である。個々の情報技術は、より美しい印刷物や便利な電子機器を製造するために発展してきたものであるが、それらが一般に普及することで、攻撃者側が偽造をし易くなる。情報技術が進歩し普及すればするほど、偽造の攻撃手法が高度かつ安価なものとなり、攻撃者側の能力が高まり、潜在的なリスクが高まることとなる。つまり、攻撃者側は、情報技術の進歩を味方につけた状態にある。

これに対して、現在人工物に利用されている偽造防止技術は、一部に情報技術を利用している部分もない訳ではないが、人間が視覚や触覚で確認を行うことを前提として、伝統的な技術に基づいて製造されたものが多い。このため、技術進歩が偽造抵抗力を高める方向に働く仕組みとなっていない。今後、情報技術が加速度的に発展していけば、攻撃者側にとって一方的に有利な方向に振れてしまうことにならないだろうか。

そうした事態に陥ることを回避するためには、製造者側が採用する偽造防止技術も、技術進歩に応じて偽造抵抗力が高まるものとすることが考えられる。つまり、製造者側も技術進歩を味方につける戦略を検討していく必要があろう。

## ３．人工物を機械読み取りさせることの意味

現在、金融業務の現場において、人工物の検証や真偽判定は、専用の読取装置において行われることが多い。その意味では、既に情報技術が利用されているといえなくはない。しかし、単に機械による読み取りを導入するだけでは、偽造防止について「技術進歩を味方につける戦略」となるとは限らない点には注意が必要である。

例えば、美術品などの真贋鑑定を人間が行うことからも分かるように、適切な訓練を積んだ専門家が慎重に作業する限り、人間の視覚や触覚は極めて高性能な検証装置の役割を果たす。これに対し、一般人がさまざまな環境下で検証する場合、その検証精度はばらつきが大きく、常に信頼できるという訳ではない。このため、人工物を機械で読み取り、真偽判定をするようにした場合、検証の精度を一定の水準にすることはできる。

しかし、これまで人工物を機械読み取りさせる技術として利用されてきたものの多くは、「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」といった、極めて単純な仕組みの技術であり、「読み取りが成功すれば真正な人工物とみなす」というロジックで設計されている。攻撃者が人工物の特徴点や読取装置の内部構造に関する情報を入手し、それを利用して偽造を行うと、容易に破られてしまうのだ。人工物に秘密のパターンを書き込んでおき、それを読み出すという偽造防止対策は、攻撃者にその仕組みを知られた途端、むしろ弱点となってしまうという危険性がある。システムの運営者が機械読み取りの結果を信頼していればいるほど、その被害が拡大しやすい。そのような「機械読み取りによる一見安全そうな検証システム」が攻撃されて深刻な被害を受ける事例が、過去にも数多く報告されている。

やや性格の異なるものとして、次のような事例を考えてみよう。最近、ユビ

キタス社会に向けての構想の一環として、さまざまな対象物に ID を付与し、これを多くの検知装置で読み取らせ、情報システムで活用する提案が盛んに行われている。ID を機械読み取りによってデータベースに登録、管理することで、サービスを高度化するとともに、偽造防止の効果も期待できるという主張を耳にする。しかし、こうした提案の多くは、ID 付与によるコントロールに主眼が置かれ、それがどの程度、偽造防止のために役立っているのかという視点からの検討が十分でないものが多いように思われる。もし同一の ID を持つ人工物のクローンが容易に製作できてしまうのであれば、どれだけ背後の情報システムを整備したとしても偽造防止の効果は限定的である。このように、人工物を人間の視覚等で検証する方式に比べ、専用装置が真偽を判定する方式が、常により高度で安全とは限らないのである。

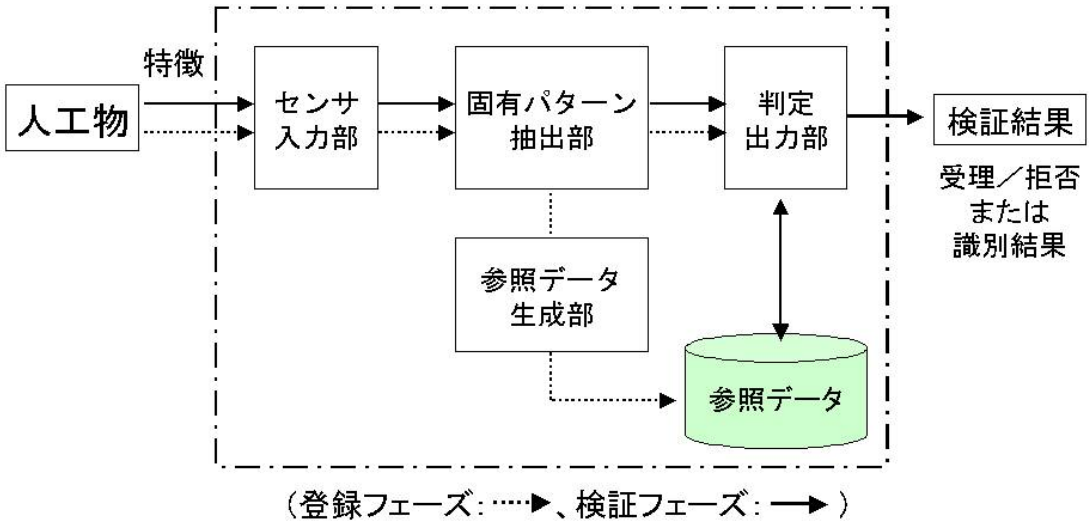
人工物を単に「機械が読み取る情報を搬送する媒体」と位置付けて利用する情報システムは、偽造防止という観点からは多くを期待できない。人工物と情報システムが一体となって、偽造防止の効果をシステム全体で引き上げるという発想が重要である。こうした観点から提案されているのが、人工物メトリクスなのである。

## ４．人工物メトリクスの可能性

ここで人工物メトリクスの基本構造を改めて整理しておこう。本論文で取り上げている人工物は、紙やプラスチックからなる工業製品であり、同じ性質を有するものを複数製造することができる。しかし、紙もプラスチックも、その人工物の細部までみれば、例えば紙における表面のざらつき具合や繊維の絡まり具合は個体ひとつひとつに微妙な差異があり、いわば、各人工物の「個性」というべき固有パターンが存在する。これら人工物の固有パターンが、おのおのの人工物を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持っていれば、これを偽造防止技術として利用できる。人工物メトリクスは、このような考え方を基本としている。

ある固有パターンを人工物メトリクスとして利用する場合、まず、この固有パターンを含んだ人工物の特定部分を検知装置によって読み取り、得られた情報を「参照データ」としてデータベースに記録しておく（図表 1、登録フェーズ）。この人工物を取引に利用し、それを検証する際、検証者は人工物の特定部分を同様に検知装置で読み取り、得られたデータを記録された「参照データ」と比較して、その一致度合いを計測し、一定のしきい値を超えた場合に、本物と判定する（図表 1、検証フェーズ）。

図表 1 人工物メトリック・システムの基本構成




このように、人工物メトリクスによる偽造防止技術は、おのおのの人工物によって異なる「指紋」に相当するランダムな固有パターンを人工物に記録し、利用の都度、機器を使ってその特徴を読み取り、情報処理によって真偽を判定する仕組みである。人間の感覚を利用することの多い既存の偽造防止技術と比較すると大掛かりであり、そのような仕組みを偽造防止の目的で利用することはやや突飛な印象を受けるかもしれない。人工物メトリクスは、どの程度、実現可能性のあるものなのだろうか。

実は、「専用機器に人工物の特徴を読み取らせ、その情報を処理することによって真偽判定を行うシステム」は既に金融分野に存在し、広範に利用されている。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がその典型である。例えば、かつて、ATM 取引は、「(1)キャッシュカード所持と(2)暗証番号による二要素認証」にあたると考えられてきた。つまり、キャッシュカードが正当な預金者であることを証明する人工物であり、そこに記録された磁気ストライプ情報は、それが読み取れるかどうかで真偽を機械で判定する、偽造防止技術のひとつと理解されてきたのである。

しかし、過去に発生した多くの偽造カード事件でも明らかになったように、従来から利用されている磁気ストライプ方式のカードは、その仕組みが広く知られており、磁気ストライプ部分の情報を偽造することは比較的容易にできる。通常の ATM 取引では、キャッシュカードについて特別の真偽判定は行われておらず、「カードの磁気情報が正常に読み取れること」がその判定基準に利用されている。ATM 取引では、その磁気情報に含まれる口座番号等の ID を読み取り、データベースを参照することで検証を行っているが、それがカード側の不正検知のために利用されている訳ではない。このため、磁気ストライプに記録され

た情報さえ複製すれば、カードの所持認証をクリアできることになってしまうのである。

磁気ストライプカードを利用したシステムの持つこの弱点は、さまざまな偽造事件を通じて広く認識され、金融機関では、その改良に乗り出している。キャッシュカードやクレジットカードについては、磁気ストライプカードからICカードへの移行が進められている。磁気ストライプカードは静的にIDを記録しておく能力しかないが、ICカードはチャレンジ・レスポンス方式などの動的な認証が可能である。また、偽造抵抗力についても、ICカードは、耐タンパー性が維持される限り、格納されている情報の読み出しや、偽造カードの作製は難しい。しかし、ICカードは、それ自体が能動的に偽造防止技術を実現しているものではない。金融取引用に利用されている接触型ICカードも、IC乗車券や電子マネーに利用されている非接触型ICカードも、カード内部のメカニズム自体は広く普及している技術である。ICカードには多くの実装形態があるが、その中のあるICカードについては、ICカードの耐タンパー性が破られて内部から秘密情報が盗み出され、それを利用して同等の挙動をする偽造カードが作り出された事件も知られている。ICカードの耐タンパー性に依拠してシステムの安全性を確保しようとするのであれば、耐タンパー性とそれへの攻撃に関する最新の技術動向に注意を払っておく必要がある。

このように考えていくと、人工物メトリクスは、人工物と情報システム、データベースを組み合わせた環境で利用されるものであり、その仕組み自体が大掛かり過ぎるということではないものと考えられる。そのうえで、人工物メトリクスは、人工物と情報システムを組合せ、全体として偽造防止を実現しようとしているという意味で、優れた特徴を持った技術である。もちろん、現段階ではまだ学術研究の対象であり、金融業務の実務システムへの広範な適用を検討するレベルには達していないものの、将来の偽造防止技術のあり方を考える際には、そのコンセプトを踏まえておく必要のある技術といえるであろう。

## ５．最近の人工物メトリクスに関する研究開発動向

人工物メトリクスの分野における研究開発の事例は、松本ほか［2004］において既にいくつか紹介されているが、同文献以降の動向をみると、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といえる（宇根・田村・松本［2009］）。

新しい技術提案の代表的なものとしては、人工物にレーザ光を照射し、その反射光のスペックル・パターンを当該人工物の固有パターンとして用いるシステム（Buchanan *et al.*［2005］）や、半導体素子内のメモリー・セルの電荷量

のばらつき度合いや回路上を流れる信号の遅延パターンを固有パターンとして用いるシステム（Guajardo *et al.*［2007］、Lim *et al.*［2005］、Suh and Devadas［2007］、Devadas *et al.*［2008］）が挙げられる。これらのシステムは既に商用製品として実用化されている（図表 2）。

図表 2 主な人工物メトリック・システムに利用される人工物の特徴

| 特性 | 人工物の特徴 |
|---|---|
| 光学特性 | ・基材中の光輝性粒状物の分布（反射光画像）（Pappu［2001］、Poli［1978］、Škorić *et al.*［2007］、Tuyls *et al.*［2005］）<br>・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）（NRC［1993］pp.74-75）<br>・基材に付与された斑の分布（反射あるいは透過光の画像）（Goldman［1988］）<br>・透明樹脂内のポリマー・ファイバーの分布（視差画像）（van Renesse［1995］）<br>・基材中のファイバーの分布（Brzakovic and Vujovic［1996］）<br>・基材表面の微小の凹凸（レーザ・スペックル・パターン）（Buchanan *et al.*［2005］）<br>・紙片表面の紙繊維の分布（反射光画像）（伊藤ほか［2005］）<br>・紙片中の紙繊維の分布（透過光画像）（Yamakoshi *et al.*［2008］） |
| 磁気特性 | ・基材中の磁性ファイバーの分布（電気信号波形）（Matsumoto *et al.*［2001］）<br>・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）（Fernandez［1993］）<br>・磁気ストライプ上の磁性粒子の分布（Inedk *et al.*［1995］、Hayosh［1998］）<br>・基材中の伝導性物質の分布（電磁波パターン）（DeJean and Kirovski［2007］） |
| 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（Fernandez［1997］、Guajardo *et al.*［2007］）<br>・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（Tuyls *et al.*［2006］）<br>・半導体素子におけるランダムな回路遅延のパターン（Gassend *et al.*［2002］、Lim *et al.*［2005］、Suh and Devadas［2007］、Devadas *et al.*［2008］）<br>・複数のリング・オシレータから出力される周波数（Suh and Devadas［2007］）<br>・コイルとコンデンサーで構成される LC 回路の共振波形（Škorić *et al.*［2008］） |
| 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（Samyn［1989］）<br>・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（Olinger, Burr, and Vnuk［1994］） |

人工物の耐偽造性の評価に関する代表的な検討事例としては、紙の赤外透過光のパターンを固有パターンとするシステムを対象に、同透過光の画像をプリントした OHP シートを「紙の偽造物」とするという攻撃の成功確率を計測した研究（平良・山越・松本［2007］）が挙げられる。また、微細なガラス球を含むエポキシ樹脂の基材にレーザ光を照射し、その透過光によるスペックル・パターンを固有パターンとするシステムにおいて、当該スペックル・パターンを予測するために必要な計算量や処理時間をベンチマークとして、当該基材の耐偽造性の評価を試みる研究（Tuyls *et al.*［2005］）も代表的な検討事例の 1 つとして挙げられる。こうした人工物の耐偽造性に関する既存の研究成果のサーベイは田村・宇根［2007］において行われており、本文献の中で今後の課題についても考察されている。

## ６．人工物メトリクス以外の偽造防止技術の研究開発動向

人工物の偽造防止技術は、金融取引のセキュリティを守るうえで、重要な構成要素である。しかし、金融分野におけるセキュリティを巡る従来の議論の中では、伝統的な偽造防止技術に関する分析は、あまり取り上げられてこなかった。人工物の偽造抵抗力を維持していくためには、偽造防止技術を巡る情報を秘匿する必要があり、オープンな議論の対象にすることがためらわれたことがその一因であろう。

確かに、特殊な印刷技術やICカードの内部構造などについては、詳細情報を適切にコントロールすることが必要である。しかし、より一般的な情報までも秘匿されると、例えば、ある偽造防止技術に問題があるにもかかわらず、関係者の間で情報が適切に共有されないまま利用され続け、偽造犯罪が発生してしまうという問題も生じかねない。影響度合いを慎重に見極めつつ、金融取引のセキュリティを向上させる観点から、伝統的な偽造防止技術についても、その研究動向が関係者に共有されることが望ましいと考えられる。

こうした観点からみると、最近、伝統的な偽造防止技術の分野でも、程度の差はあるものの、安全性の客観的な評価のあり方をオープンな場で議論しようという動きがみられている。以下では、人工物メトリクス以外の代表的な偽造防止技術として、印刷技術、ホログラム、ICカードの３者についてみてみよう。

### (1) 印刷技術

印刷技術に関しては、個々の技術の情報や評価結果の詳細が公開されるケースは引き続き少ないものの、印刷による偽造防止技術がスコープに含まれる評価方法の研究事例がいくつか報告されるようになってきている。例えば、Saksena, Dubbel, and Spicer［2002］とSaksena and Lucarelli［2004］は、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と人工物偽造のプロセスを確率モデルとして表現し、仕様解明の難易度とコストを試算する方法を検討しており、本試算によって仕様解明のコストと成功確率の関係を明らかにする方法を提案している。また、米財務省印刷局が組成した銀行券偽造防止技術委員会（Committee on Technologies to Deter Currency Counterfeiting）の報告書（NRC［2007］）が公表されており、銀行券の偽造防止目的に利用可能な印刷技術の候補がいくつか紹介されているほか、それらの技術の耐偽造性に関する同委員会の評価も紹介されている。なお、本報告書では、印刷技術のみならず、ホログラムをはじめとする光学素子の技術や液晶等の電子デバイスの技術についても代表的なものが紹介されている。

### ⑵ ホログラム

ホログラムに関しては、最近の主な研究事例として、ホログラムの一種である回折格子型光学的変化素子における耐偽造性評価方法の提案が挙げられる（Andrade and Rebordão［2002］）。本研究は、当該素子のセキュリティ特性を基に評価項目と各項目の評価値を設定してモデルを構築し、評価値を重み付けして合算し当該素子のスコアを算出するという方法を提案している。各評価値や重みは当該素子の開発者やユーザーによって決定される扱いとなっており、評価項目や評価値の妥当性の確認等いくつかの課題が残されているものの、ホログラムの評価方法の確立に向けた取り組みの 1 つとして注目される。

また、わが国において、ホログラムの記録材料における光学的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。ホログラムの記録材料に関する標準仕様書は、TS Z 0019（日本工業標準調査会［2006］）として 2006 年に発行されており、現在、本TSを日本工業標準（JIS）にするプロジェクトが進められている（産業技術総合研究所［2006］）。本TSは、回折効率[1]等の評価指標を規定しており、従来各メーカーでまちまちであった指標の測定方法を統一化するものとして注目される。ホログラムの記録材料の評価指標が統一化されれば、低い品質のホログラムを排除しやすくなり、適切な品質のホログラムのみ使用することによって偽造防止の効果を向上させることができると期待される。

### ⑶ IC カード

IC カードを含む暗号ハードウエアに関しては、一定の要件を充足しているか否かを第三者の専門機関が評価・認証する枠組みが既に整備されている。欧米のセキュリティ評価基準を基に作成されたコモンクライテリア（Common Criteria）に基づく制度と、米国連邦政府の情報処理標準規格 FIPS 140-2 や ISO/IEC 19790 に基づく試験・認証制度が挙げられる。これらの枠組みによる評価・認証を得た暗号ハードウエアは既に数多く存在しており、それらの評価・認証の内容を手掛かりにすることによって、ユーザーが自分のアプリケーションの要件を満足する機能を持つ暗号ハードウエアを選択することが可能となっている。

また、わが国の暗号技術検討会傘下の CRYPTREC 暗号モジュール委員会においては、サイドチャネル攻撃の実験評価用のハードウエアを用いて評価方法を確立するための検討が行われている（情報通信研究機構・情報処理推進機構［2008］）。最近では、サイドチャネル攻撃実験用標準評価ボード（SASEBO）と同ボードで利用するテスト用暗号アルゴリズムのハードウエア回路データが

[1] ホログラムの回折効率は、再生される画像の明るさを表す尺度の 1 つであり、再生照明光の強度に対する回折光の強度の比率によって示される。

産業技術総合研究所と東北大学によって開発され、暗号モジュール委員会はもとより、国内外の研究者によって利用されている。今後、こうした共通の暗号ハードウエアにおける耐タンパー技術の評価研究、および、それらを活用した評価方法に関する研究が一層活発化するものとみられる。

## ７．偽造防止技術に関する検討の枠組み整備の動き

６．で述べたアカデミックな動きとは別に、偽造防止技術を組み込んだ製品を製造している実務家側の動きとして、業界団体における偽造防止技術に関する情報の共有や業界横断的な用語・概念の整理等を目的とした活動等の事例がみられるようになってきている。

例えば、欧州においては、ブランド品メーカー等の偽造防止製品ユーザーや偽造防止製品メーカーが参画し、関係者間の情報交換、偽造防止の機能や役割に関する理解向上、偽造品検査の標準的な手続やプロトコルの検討を主な目的とする検討部会（Workshop on Anti-counterfeiting）が、2007 年、欧州標準化委員会（CEN: Comité Européen de Normalisation）において設置された（Lancaster［2008］）。本検討部会での議論は、オープンな場の議論として位置付けられており、偽造防止技術の評価に関する共通認識の確立に向けた動きとして注目される。

また、国際標準の場においては、2009 年 2 月、偽造防止技術を対象とする専門委員会としてTC247（fraud countermeasures and control）を組成することが、ISOの技術管理評議会（TMB: technical management board）において承認された。本件は、各種製品の偽造や横流し等の不正行為への対策をスコープとする専門委員会をISO傘下に設置してはどうかとのANSIおよびNASPO[2]からの提案がきっかけとなって実現した（NASPO［2008］）。NASPOの提案書では、TC68（金融）、TC223（社会セキュリティ）、TC34（食品）等の専門委員会において各種製品の不正行為への対策に関する検討が今後求められるようになるとしたうえで、各種の不正行為を防止するための認証用機器のセキュリティ評価方法や評価のための枠組み、金融取引に用いられる書類やシステムに

[2] NASPO（North American Security Products Organization）は、製品の偽造や盗取をはじめとする各種不正行為の防止に資する生産・流通管理のための各種ガイドラインを策定する非営利団体（米国とカナダが拠点）である。2003 年からは、各種不正行為を防止するための生産・流通管理手法を規定した同組織のガイドラインである“security assurance standard”に基づき、同ガイドラインに沿って適切な生産・流通管理が実施されていることを第三者の監査人（NASPO auditor）が検査を行って認証（NASPO Certification）を付与するスキームの運営を開始している（NASPO［2003］）。2005 年には、上記ガイドラインは米国の国内標準（ANSI/NASPO-SA-v3.0P）となっている。

ついても標準化の対象にしてはどうかとのアイデアが盛り込まれている。新しいTCの設置が承認されたことによって、今後、偽造防止技術に関する評価基盤の検討がISOの場で進められることが期待される。

## ８．偽造防止技術の将来

2004 年に開催されたシンポジウムで人工物メトリクスについて提案してから約５年間で、人工物メトリクスの技術研究は大きく進歩した。この間、株券の電子化が進められ、金融業務に利用されてきた重要な人工物のひとつである株券は姿を消した。そもそも長い目でみれば、人工物を介在させる金融取引は、すべて電子ベースで完結する取引と比べて非効率であり、更に人工物の偽造というリスクを負っている。株券のように、人工物を廃止してオンライン取引に移行することができるのであれば、その取引の効率性は高まるであろう。しかし、すべての金融取引が完全にオンライン取引に移行できる訳ではない。個人の少額決済のようなリテール金融取引の世界では、現在の進んだ情報技術を前提としても、何らかの人工物を介在させることで、利便性やセキュリティを高めることに合理性があり、利用者のニーズは残っていくものと考えられる。問題は、そうしたニーズに対して、どのような技術で応えていくことが望ましいかということである。

情報技術の発達は、伝統的な偽造防止技術の安全性の根拠を不確かなものとしている。人工物メトリクスは、そうした事態に対するひとつの回答であった。これに対し、伝統的な偽造防止技術の分野からも、新しい技術提案がなされている。幾つかの技術分野では、従来以上にオープンな形で知識を共有し、より良い技術を提案しようとしている。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ものである。そして、こうした技術のユーザーである金融業界は、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検討を深めていく必要があるだろう。

以　上

## 参考文献


伊藤健介・左右田宏之・井原富士夫・木村哲也・布施マリオ、「紙ドキュメントのセキュリティ」、『富士ゼロックス　テクニカルレポート』No.15、富士ゼロックス、2005 年、36～37 頁

宇根正志・田村裕子・松本　勉、「偽造防止技術の中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」、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、2009-J-2、日本銀行金融研究所、2009 年

産業技術総合研究所、「ホログラム記録材料の光学的特性測定方法」、『平成 18 年度工業標準化研究開発進捗総覧』、産業技術総合研究所、2006 年、14 頁

情報通信研究機構・情報処理推進機構、『CRYPTREC Report 2007』、情報通信研究機構・情報処理推進機構、2008 年

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について　―どのように耐クローン性を評価するか―」、信学技報 ISEC2007-91、電子情報通信学会、2007 年、15～22 頁

日本銀行金融研究所、「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」、『金融研究』第 23 巻第 1 号、日本銀行金融研究所、2004 年、153～168 頁

日本工業標準調査会、『TS Z 0019：ホログラム用記録材料―フォトポリマー―光学的特性測定方法』、日本規格協会、2006 年

平良允俊・山越　学・松本　勉、「紙の赤外透過光を用いた人工物メトリクスの耐クローン性評価」、『2007 年暗号と情報セキュリティ・シンポジウム予稿集』、電子情報通信学会、2007 年

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 1 号、日本銀行金融研究所、2004 年、169～186 頁

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、日本銀行金融研究所、2004 年、61～140 頁

Andrade, Ana A., and José M. Rebordão, “Evaluation of DOVID Security under First Line Inspection,” Proceedings of SPIE, Vol.4677, 2002, pp.299-313.

Brzakovic, Dragana, and Nenad Vujovic, “Authentication of random pattern by finding a match in an image database,” *Image and Vision Computing*, 14, 1996, pp.485-499.

Buchanan, James D. R., Russell P. Cowburn, Ana-Vanessa Jausovec, Dorothee Petit, Peter Seem, Gang Xiong, Del Atkinson, Kate Fenton, Dan A. Allwood, and Matthew T. Bryan, “Forgery: ‘Fingerprinting’ documents and packaging,” *Nature*, 436 (475), 2005, p.475.

DeJean, Ferald, and Darko Kirovski, “RF-DNA: Radio-Frequency Certificates of Authenticity,” *Proceedings of CHES 2007*, LNCS 4727, Springer-Verlag, 2007, pp.346-363.

Devadas, Srinivas, Edward Suh, Sid Paral, Richard Sowell, Tom Ziola, and Vivek Khandelwal, “Design and Implementation of PUF-Based “Unclonable” RFID ICs for Anti-Counterfeiting and Security Applications,” *Proceedings of IEEE International Conference on RFID 2008*, IEEE, 2008, pp. 58-64.

Fernandez, Alberto J., *Data Verification Method and Magnetic Media*, Xtec Inc., U.S. Patent 5,235,166, 1993.

———, *Method and apparatus for securing data stored in semiconductor memory cells*, Xtec Incorporated, U.S. Patent 5,644,636, 1997.

Gassend, Blaise, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas, “Silicon Physical Random Functions,” *Proceedings of the Computer and Communication Security Conference*, ACM 2002, pp.148-160.

Goldman, Robert N., *Non-counterfeitable System*, Light Signature Inc., U.S. Patent 4,786,290, 1988.

Guajardo, Jorge, Sandeep S. Kumar, Geert-Jan Schrijen, and Pim Tuyls, “FPGA Intrinsic PUFs and

Their Use for IP Protection," *Proceedings of CHES 2007*, LNCS 4727, Springer-Verlag, 2007, pp.63-80.

Hayosh, Thomas D., "Self-Authentication of Value Documents," *Proceedings of SPIE*, Vol. 3314, SPIE-IS&T, 1998, pp.140-149.

Inedk, Ronaldo S., Marcel W. Moller, George L. Engel, and Alan L. Hege, "Method and Apparatus for Fingerprinting and Authenticating Various Magnetic Media," Washington University, St. Louis, U.S. Patent 5,428,683, 1995.

Lancaster, Ian M., "The Case for Authentication Standards," *Proceedings of ODS 2008*, 2008.

Lim, Daihyun, Jae W. Lee, Blaise Gassend, Gookwon Edward Suh, Marten van Dijk, and Srinivas Devadas, "Extracting Secret Keys From Integrated Circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 13 (10), IEEE, 2005, pp.1200-1205.

Matsumoto, Hiroyuki, Itsuo Takeuchi, Hidekazu Hoshino, Tsugutaka Sugahara, and Tsutomu Matsumoto, "An Artifact-metric System Which Utilizes Inherent Texture," *IPSJ Journal*, 42 (8), IPSJ, 2001, pp.139-152.

National Research Council of the National Academies (NRC), *Counterfeit Deterrent Features for the Next-Generation Currency Design*, Publication NMAB-472, National Academy Press, 1993.

———, *A Path to the Next Generation of U.S. Banknotes: Keeping Them Real*, the National Academy of Sciences, 2007.

North American Security Products Organization (NASPO), *Security Risk Management Requirements Definition Document: Overview for Prospective Members, Version 4.0*, NASPO, September 24th, 2003.

———, *Proposal Outline for a new ISO Technical Committee on Fraud Countermeasures and Control*, NASPO, July 8th, 2008.

Olinger, Chad T., Tom Burr, and Daniel R. Vnuk, "ACOUSTIC RESONANCE SPECTROSCOPY INTRINSIC SEALS," *Annual meeting proceedings of Institute of Nuclear Materials Management*, Vol.23, 1994, pp.776-782.

Pappu, Ravikanth, *Physical One-Way Functions*, Ph.D. thesis, Massachusetts Institute of Technology, 2001

Poli, David L., "Security Seal Handbook," *Sandia Report*, SAND 78-0400, Sandia National Laboratory, 1978, pp.1-44.

van Renesse, Rudolf, Leopold, "3DAS: A 3 Demensional-structure Authentication System," *ECOS95, European Convention on Security and Detection*, 1995, pp.54-59.

Saksena, Anshu, Daniel C. Dubbel, and Jane W. Maclachlan Spicer, "Probabilistic model for comparing the effectiveness of counterfeit deterrent features," *Proceeding of SPIE*, Vol 4677, 2002, pp.56-64.

———, and Dennis Lucarelli, "Probabilistic risk assessment for comparative evaluation of security features," *Proceedings of SPIE,* Vol. 5310, 2004, pp.74-81

Samyn, Johan, *Method and Apparatus for Checking the Authenticity of Documents*, N. V. Bekaert S. A., U.S. Patent 4,820,912, 1989.

Škorić, Boris, Thijs Bel, Toon Blom, Boudewijn de Jong, Hennie Kretschman, and Ton Mellissen, "Randomized resonators as uniquely identifiable anti-counterfeiting tags," *Proceedings of SECSI Workshop*, 2008.

———, Geert-Jan Schrijen, Wil Ophey, Rob Wolters, Nynke Verhaegh, and Jan van Geloven, "Experimental Hardware for Coating PUFs and Optical PUFs," *Security with Noisy Data*, Pim Tuyls, Boris Škorić, and Tom Kevenaar (Eds.), Springer-Verlag, 2007, pp.255-268.

Suh, Gookwon Edward, and Srinivas Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," *Proceedings of DAC 2007*, 2007, pp.9-14.

Tuyls, Pim, Geert-Jan Schrijen, Boris Škorić, Jan van Geloven, Nynke Verhaegh, and Rob Walters, "Read-Proof hardware from Protective Coating," *Proceedings of CHES 2006*, LNCS 4249, Springer-Verlag, 2006, pp.369-383.

———, Boris Škorić, Sjoerd Stallinga, Anton H. M. Akkermans, and Wil Ophey, "Information-Theoretic Security Analysis of Physical Uncloneable Functions," *Proceedings of Financial Cryptography 2005*, LNCS 3570, Springer-Verlag, 2005, pp.141-155.

Yamakoshi, Manabu, Junichi Tanaka, Makoto Furuie, Masashi Hirabayashi, and Tsutomu Matsumoto, "Individuality evaluation for paper based artifact-metrics using transmitted light image," *Proceedings of SPIE*, Vol. 6819, SPIE-IS&T, 2008, pp.68190H-1-68190H-10.