IMES DISCUSSION PAPER SERIES

金融業務と人工物メトリクス

まつもと　つとむ　　いわした　なおゆき
松本　勉・岩下　直行

Discussion Paper No. 2004-J-12

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 日本橋郵便局私書箱 30 号

日本銀行金融研究所が刊行している論文等はホームページからダウンロードできます。
http://www.imes.boj.or.jp

IMES Discussion Paper Series 2004-J-12
2004 年 4 月

金融業務と人工物メトリクス

まつもと　つとむ　　いわした　なおゆき
松本　勉 *・**岩下　直行** **

要　　旨

情報通信ネットワークを利用した電子金融取引が拡大する中、情報セキュリティ技術を利用して取引の安全性を確保する方法についての検討が進んでいる。これに対して、一般的な金融取引では、証書、証券、紙幣、プラスチックカード等の人工的に製造された物理媒体（人工物）を利用した従来型の取引手法が維持されており、安全性確保の方策にもあまり変化はない。ところが、金融業務に利用されている紙やカードなどの人工物のセキュリティは、近年の技術進歩に伴い、大きな脅威にさらされている。現代の金融業務が、その安全性をこれらの人工物に大きく依存していることを考えると、中長期的な観点から、その安全性、信頼性を維持するための枠組みを整備していくことは、金融業界における重要な課題と考えられる。

そこで、本論文では、情報セキュリティ技術の手法を用いて、人工物を利用した取引の安全性、信頼性を向上させる仕組みである、人工物メトリクスについて考察する。人工物メトリクスとは、筆者の一人がバイオメトリクスという用語を参考に造った言葉であり、「人工物に固有の特徴を用いて人工物を認証する技術」という意味である。典型的には、人工物に対して、人間の指紋に相当する、各々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技術のことを指している。

本論文では、人工物メトリクスの基本的なコンセプトを紹介するとともに、金融業務分野での実際の適用事例を踏まえて、今後の研究課題に関する問題提起を行うこととしたい。

キーワード：人工物メトリクス、人工物メトリック・システム、バイオメトリクス、情報セキュリティ技術、偽造対策
JEL classification: L86、L96、Z00

*　横浜国立大学大学院環境情報研究院（E-mail: tsutomu@mlab.jks.ynu.ac.jp）
**　日本銀行金融研究所研究第 2 課（E-mail: iwashita@imes.boj.or.jp）

本論文は、2004 年 3 月 26 日に日本銀行で開催された「第 6 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。

目　次

１．はじめに

インターネットなどの情報通信ネットワークを利用した金融業務が拡大する中で、電子金融取引の安全性と信頼性を確保するために、さまざまな情報セキュリティ技術が利用されるようになってきた。金融機関が適切な情報セキュリティ技術を選択するための基盤も徐々に整備されつつあり、暗号アルゴリズム、デジタル署名、ハッシュ関数等については、信頼性の高い中立的な評価機関によって安全性を評価された技術が採用されるようになっている[1]。金融機関によるシステムの運用管理についても、セキュリティ・ポリシーの策定と遵守、外部機関による安全性チェック等の枠組みが整備され、実際に利用され始めている[2]。

これに対し、一般的な金融業務においては、従来からの取引手法が維持されており、セキュリティ対策についても目立った変化はない。例えば、銀行窓口での預金引出しにおいては、紙製の預金通帳と預金払戻請求書と印鑑を用いて事務が進められている。株式や債券といった有価証券の受渡しにおいては、電子取引の比率が高まってはいるものの、紙製の現物証券が利用されることも少なくない。金融機関の CD／ATM での預金預入れ、払出しにおいては、プラスチック製のキャッシュカードが利用されている。日々の人々の決済には、紙製の紙幣やプラスチック製のクレジットカード、プリペイドカードが利用されている。このような金融業務に利用される証書、証券、紙幣、プラスチックカード等の人工的に製造された物理媒体（以下では、「人工物」と呼ぶ。）は、それらが仮に不正に複製されたり、改ざんされたりすると、取引の安全性、信頼性を損なう結果、経済全体に大きな損失をもたらしかねない。その意味では、現代の金融業務は、その安全性をこれらの人工物に大きく依存しているといえるだろう。

もしも将来、金融取引の電子化が更に進み、物理媒体を介する金融取引が行われなくなるのであれば、金融取引の安全対策は、情報セキュリティ技術の問

---

[1] 松本・岩下[2001]、情報処理振興事業協会・通信放送機構[2003]
[2] 金融情報システムセンター[2003]

題と考えることができるようになり、人工物のセキュリティ対策はさほど重要な問題ではなくなるだろう。しかし、金融取引の実態をみると、すべての取引が電子化に適しているわけではない。小額の金融取引や、個人間の資金決済などは、紙幣やカードなどの人工物を利用した取引の方が簡便で好まれる傾向があるし、企業間の取引でも、契約期間が長期間に亘る場合、システムに保管された情報の証拠性が問題となるため、物理媒体を証拠に利用したいというニーズがある。こうした事情から、人工物を利用した取引が全く存在しなくなることは考えられない。

人工物のセキュリティについては、これまでは主として経験的な観点からセキュリティ対策が選択されることが多く、どのような材質で、どのような製造技術を利用した人工物であれば、どの程度、偽造・複製・改ざんが困難なのかという点について、科学的な分析結果が公開されることはあまりなかった。そもそも、こうした人工物は、人間の視覚や触覚に頼って検証されることが多いため、厳格にチェックされることもある一方、運用によっては簡易なチェックにとどめることもあるなど、検証作業の精度にばらつきがあり、安全性に関する定量的な基準を設けることが難しいという面があった。また、利用される用途によっては、対面取引での本人確認など、別の手段でセキュリティを確保していることを理由に、人工物そのもののセキュリティ対策はさほど重視されないというケースもあった。そして何よりも、そうした人工物のセキュリティ対策について分析が行われたとしても、対策の有効性を損なう惧れがあるため、その内容が公表されることは少なかった。

しかし、最近、金融業務の現場で利用されている人工物が不正に偽造、複製、改ざんされ、取引の安全性、信頼性が脅かされる事件が増えてきている。その背景には、デジタル画像処理技術の発達とパソコンの普及により、高度な印刷技術や高価な印刷機械を持たなくても、印影や証券・紙幣の券面を高い精度で偽造・複製することが容易になったという環境変化がある。例えば、盗難通帳の副印鑑をスキャナで読み取って印影を偽造し、預金を不正に引き出すといった事件が多発している。クレジットカード、プリペイドカードなどを精巧に偽

造して不正利用する組織的な犯罪も後を絶たない。紙幣の偽造件数も増えている。高額の有価証券を偽造して換金しようとする犯罪も目立つ。

このように、現在の金融業務が人工物の安全性、信頼性に大きく依存しており、その状況が近い将来も大きくは変わらないと考えられる以上、中長期的な観点から、人工物の安全性、信頼性を維持するための技術的な枠組みを整備しておくことは、金融業界における重要な課題と考えられる。

そこで、本論文では、情報セキュリティ技術の手法を用いて、人工物の安全性、信頼性を技術的、定量的に評価し、向上させることを企図した「人工物メトリクス」と呼ばれる技術について紹介するとともに、人工物メトリクスを金融業務に実際に適用した事例を踏まえて、今後の研究課題に関する問題提起を行うこととしたい。

２．人工物の安全性低下の事例

（1）印鑑の偽造による盗難通帳からの預金払出し

最近、金融取引に利用される人工物の安全性、信頼性が低下していることを示す端的な例として、盗難通帳による預金の払出しの増加が挙げられる。全国銀行協会が全国銀行協会正会員・準会員 183 行を対象に行ったアンケート調査[3]によれば、平成 14 年度中に盗難通帳から払い出された金額（利用者申告ベース）は、それまでの水準を大きく上回り、40 億円を超えている（図表１。ただし、15 年度入り後は、金融機関窓口における対策の強化もあり、件数、金額ともに減少してきている）。過去においても、預金通帳と印鑑が同時に盗難に遭い、金融機関への通報も遅れたため、預金が不正に払い出されてしまうという事例がなかったわけではない。しかし、最近の手口は、預金通帳に押された副印鑑[4]をデジタルカメラやスキャナで読み取り、預金払戻請求書等にプリンタで印刷することによって印影を複製し、金融機関の窓口で不正に預金を払出すという巧

[3] 全国銀行協会[2004]

[4] 副印鑑：金融機関に届け出る印影（正印鑑）のほかに、通帳に押印した同一の印影のこと。正印鑑は預金者の取引店に保管されることが多く、金融機関窓口における日々の印鑑照合事務は、通帳上の副印鑑と顧客が預金払戻請求書等に押印した印影とを照合するのが一般的であった。

妙なものとなってきていると指摘されている。新聞報道等によれば、そのような不正払出しを狙って意図的に預金通帳のみを盗み出す盗難事件も発生しており、印鑑を預金通帳とは別に厳格に保管していたにもかかわらず、被害に遭うケースが増えていると伝えられている。

図表１　盗難通帳による払出し件数・金額等に関するアンケート結果
（対象：全国銀行協会正会員・準会員 183 行）

	件 数	金 額
12 年度	1,118 件	2,178 百万円
13 年度	786	1,658
14 年度	1,294	4,165
15 年度	567	1,735

(注１) 15 年度は、15 年 4 月～15 年 12 月（9 ヶ月間）
(注２)「盗難通帳による払出し」とは、銀行の顧客等から「盗難通帳により払い出された」との申し出があり、実際に預金が払い出されているもの
(注３)「件数」は原則として預金名義人単位

(資料：全国銀行協会)

こうした状況を踏まえて、金融機関側でも、窓口における確認作業を厳格化するほか、預金通帳の副印鑑を廃止するとか、預金者への注意喚起のための広報活動を強化するといった対策を講じている。しかし、新しく発行された預金通帳の副印鑑が廃止されたとしても、副印鑑が残っている古い通帳から印影が複製されるケースもあり、こうした手口による預金の不正引出しを確実に阻止できるわけではない。このため、一部の金融機関では、預金引出し時の本人確認手段として、窓口においても暗証番号の入力を要求するよう、システムを変更する動きがみられ始めている。

そもそも印鑑は、印影が複写された場合はそれが検知できることを前提に利用されている技術である。目視による照合で偽造と判定できないような印影の複写が可能となる事態は想定されていなかったからこそ、副印鑑が通帳に押印されていたのである。預金者が、銀行取引用の印鑑を他の用途での押印に利用することが珍しくないように、印影は、パスワードのような「秘密の情報」として扱われているわけではない。デジタル画像処理技術の発展・普及を踏まえると、「正印鑑／副印鑑と預金払戻請求書等に押印された印影との照合」という手法は、人工物を確認する技術としては安全性、信頼性に乏しくなったといわざるを得ない。現状、金融機関は、窓口における顧客の行動パターンのチェッ

クなどの追加的な手段で不正払出しを排除するよう努めているが、預金者を保護する観点から、より安全性、信頼性の高い技術の導入を検討していくことが望ましいと考えられる。

（2）カードの偽造・不正使用

プリペイドカード、クレジットカード等の磁気ストライプカードも、偽造の被害に遭いやすい人工物である。かつて、磁気ストライプ方式のテレホンカード、パチンコカードが大規模に偽造され、大きな被害が出たことが報道された。最近では、ハイウェイカードの偽造被害が大きく報道され、高額面のカードの利用が停止された。こうした磁気ストライプ方式のプリペイドカードは、元々、機械読取による事務の効率化を企図して開発されたものであり、組織的な偽造に対して十分な耐性がなかったことに加え、大規模な不正行為を許す運用環境に置かれていたことも、偽造被害が拡大した原因と伝えられている。

同じ磁気ストライプ方式のクレジットカードの不正使用も大きな問題となっている。日本クレジット産業協会の調査[5]によれば、かつては不正利用のほとんどが盗難、紛失カードの第三者使用であったが、平成 10 年頃から偽造による不正使用が急増し、平成 15 年 1～9 月期は、被害総額約 209 億円のうち、6 割以上が「偽造カード被害」となっている（図表２）。このように偽造犯罪が増加した背景として、クレジットカードを偽造する犯罪組織が存在することが報道されている。

図表２　クレジットカード不正使用被害の発生状況

（単位：億円、%）

期　　間	クレジットカード不正使用被害額	クレジットカード不正使用被害額の内訳			
		偽造カード被害額		その他不正使用被害額	
		被害額	構成比	被害額	構成比
平成 9 年	188.0	12.0	6.4%	176.0	93.6%
平成 10 年	216.0	28.0	13.0%	188.0	87.0%
平成 11 年	271.7	91.0	33.5%	180.7	66.5%
平成 12 年	308.7	140.2	45.4%	168.5	54.6%
平成 13 年	275.7	146.4	53.1%	129.3	46.9%
平成 14 年	291.4	165.0	56.6%	126.4	43.4%
平成 15 年(1 月～9 月)	209.2	125.7	60.1%	83.5	39.9%

(資料：日本クレジット産業協会)

[5] 日本クレジット産業協会[2004]

（3）紙幣の偽造件数の増加

デジタル画像処理技術の発達が人工物の偽造を容易にしているという問題は、紙幣の偽造件数の推移からも読み取ることができる。警察庁の調査によれば、わが国での紙幣（日本銀行券）の偽造の発見枚数は、平成 11 年以降急増し、平成 14 年には 2 万枚を超え、平成 15 年も 1 万 6 千件と高水準となっている（図表３）。平成 15 年版の警察白書[6]では、最近の紙幣偽造の特徴点について、「同一の被疑者によって偽造銀行券が大量に偽造されていること、被疑者が低年齢層に広がってきていることなどが挙げられる。これらの特徴的傾向の背景としては、パソコン用プリンタ等の機器の普及・高性能化が進み、これらの機器を利用することにより、精巧な偽造が容易になっていることが挙げられる」と記述している。

図表３　偽造通貨の発見枚数

（単位：枚）

	平成 10 年	平成 11 年	平成 12 年	平成 13 年	平成 14 年	平成 15 年
１万円券	752	2,346	2,394	3,207	6,815	6,138
５千円券	8	1,051	1,671	1,274	754	1,097
２千円券	－	－	2	4	5	99
千円券	47	25	190	3,128	12,637	9,576
偽造銀行券合計	807	3,422	4,257	7,613	20,211	16,910
5 百円貨幣	358	7,336	4,747	3,232	2,092	2,625

・ 発見枚数とは、届出等により警察が押収した枚数である。
・ 平成 11 年以降の偽造一万円券および偽造五千円券の増加は、主にパソコン・プリンター等により偽造されたものの増加による。
・ 平成 13 年以降の偽造千円券の増加は、主に両替機、飲料水の自動販売機等を対象に行使された特異な偽造千円券行使事件の発生による。

（資料：警察庁）

３．既存の人工物のセキュリティ対策の限界

こうした人工物の安全性を確保するために、これまでも、さまざまな技術が利用されてきた。証券や紙幣には、偽造・複製を防止するためにさまざまな特殊印刷技術が利用されているし、磁気ストライプ方式のプリペイドカードにも、偽造・複製・改ざんがされにくいようなさまざまな工夫が施されている。しか

[6] 警察庁[2003]

し、これまで利用されてきた人工物のセキュリティ対策技術は、「人工物を製造する側の技術的優位性」を拠り所とするものがほとんどであった。こうした技術は、攻撃者が高度な技術を容易かつ安価に利用できるようになると、製造者は新たな技術を開発、活用していかなければ、偽造・複製・改ざんを防止できないという宿命を持っている。こうした既存のセキュリティ技術の限界について、幾つかの例をみてみよう。

（1）視覚を利用したセキュリティ対策

例えば、証券、紙幣などの偽造防止対策として、マイクロ文字と呼ばれる極めて小さな文字が印刷されることがある。この技術は、「証券、紙幣等をスキャナとプリンタ、コピー機などで複製しようとしても、読取り、書込みの解像度が低いため、正確に複製できない」という効果を期待したものである。この技術は、市販の印刷装置の解像度が低い間は非常に有効な対策であるが、解像度の高い印刷装置が一般に利用されるようになると、マイクロ文字を複製すること自体がさほど困難ではなくなり、徐々にその有効性が低下してしまう。これは、市販の印刷装置の技術進歩によって、偽造防止技術の有効性が低下する典型的な例である。

これに限らず、どのような技術であっても、印刷の細密さや色合い等を利用して、人間の視覚で違いを検知させるセキュリティ対策には、同様の限界があるといわざるを得ない。人間の視覚に頼った人工物のセキュリティ対策の場合、技術進歩により解像度の高い複製が可能となると、「視覚による検証の限界」に突き当たるからである。マイクロ文字の例でいえば、仮に、製造者が製造装置の改良を続けることにより、常に攻撃者よりも細密な文字を印刷することが可能であったとしても、製造者と攻撃者が競い合って精細さを引き上げていった場合、ある一定レベルを超えると、その違いを視覚によって峻別できなくなる。この限界は、視覚という「解像度に限界のある検証装置」を利用している以上、避けられないものである。

実際の人工物の中には、ホログラムや特殊インキを利用した印刷技術など、

容易には複製されにくく、視覚でも検証が容易なセキュリティ対策技術が導入されているものもある。しかし、こうした「製造する側の技術的な優位性」を利用したセキュリティ対策は、導入されてから当面の間は有効であるものの、過去のさまざまな偽造犯罪の経験を踏まえると、技術の普及とともに技術的な優位性が低下し、効力が失われるという一般的な傾向があるようである。特に最近は、磁気ストライプカードの偽造犯罪の例にみられるような、大規模で組織的な偽造犯罪が増えており、実際、クレジットカードの偽造対策として利用されるホログラム画像については、既に組織的な偽造が行われていると報道されている。

（2）人工物の機械読取によるセキュリティ対策

人間の視覚、触覚などを利用した人工物の検証は、例えば美術品、骨董品の真贋鑑定の例にみられるように、熟練者が慎重に検証作業を行うことによって、極めて精度の高い検証が可能となる。その反面、検証者の錬度や検証作業がどの程度注意深く行われるかといった前提条件が変化し得るため、セキュリティ対策の有効性を客観的に測定することができない。このため、人工物に一定水準以上の安全性を確保させるためには、機械で人工物を読み取ることを前提に、セキュリティ対策を設計するのが一案である。

しかし、これまで人工物を機械読取させる技術として利用されてきたものの多くは、「特別な手を加えない磁気パターンを人工物に直接書き込んでおき、それを磁気センサーで機械読取する」といった、極めて単純な仕組みの技術であった。例えば、自動販売機や両替機で紙幣を読み取る際に、紙幣に印刷されている磁性インキの分布パターンを利用して真贋判定を行う、といった技術である。しかし、単に一定の磁気パターンを人工物に書き込んでおき、それを機械読取するというだけの対策では、書き込まれている情報やシステムの内部構造が解析されてしまえば複製は容易であるため、セキュリティ対策としてはあまり強度が高いとはいえなかった。実際、過去に発生した紙幣偽造事件では、何の印刷もされていない紙に、紙幣の磁性インキ分布パターンを複写した「偽札」が

作製され、自動販売機を欺いて不正に利用されたことがある。いくつかのプリペイドカードの大規模な偽造犯罪事件においても、カードに記録された磁気ストライプ情報が偽造・複製され、読取装置を欺く手口が利用された。

金融取引に利用される人工物は、証書、証券、紙幣、カードのように、利用者の手に渡ってしまうものが多いため、利用者によってその構造が解析されることを防止できない。多くの利用者が利用する人工物であるほど、人工物の特徴点や読取装置の内部構造に関する情報を秘密に保つことは難しい。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セキュリティ対策は、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。

（3）IC カード、IC チップ等を利用したセキュリティ対策

こうした問題を解決するために提案されているのが、IC カードのような耐タンパー性[7]を持ったデバイスを利用することである。IC カードは、CPU を内蔵したプラスチック製のカードであり、正規の手順を踏むことなしに内部メモリの情報にアクセスして情報を読み出すことが困難な仕組みになっている。IC カードが十分な耐タンパー性を持っている場合、攻撃者が IC カードに格納された情報を不正に読み取って、その情報を基に偽造・複製を作製することが困難であるため、人工物のセキュリティ対策として有効な技術のひとつと考えられる。

ただし、IC カードの耐タンパー性については、さまざまな攻撃法が提案されており[8]、そうした攻撃法に対する耐性が慎重に評価されていない場合、内部の情報が不正に読み出されてしまうリスクがあることには注意が必要である。この部分に対する研究はなお発展途上であるが、そうした脅威に十分な考慮が払われていない場合、耐タンパー性を安全性の拠り所にすることは難しい。その場合は、事実上、「（内部の情報が漏洩したとしても）IC カードを複製するコス

---

[7] 耐タンパー性：外部からの不正な手続き等により、秘密の情報を観測･改変することや、本来の設計意図とは異なる不正な動作を行わせること等が困難であること。
[8] 情報処理振興事業協会[2000]

トが高いこと」を偽造・複製・改ざんの抑止力として期待することになる。

また、これに似た考え方として、人工物にICチップを添付することによって、不正な複製物の作製コストを高めるというアプローチも提案されている。しかし、添付されたICチップに耐タンパー性がない場合、内部の情報が容易に読み取られ、解析されてしまう惧れがある。その場合、複製コストが高いことのみがセキュリティ対策と位置付けられることとなる。確かに、同様に機能するICチップを複製するコストは、通常の印刷物や磁気ストライプカードと比較すれば高いと考えられるが、それは前提条件によって大きく変化しうるので、セキュリティ対策の根拠としては利用しにくい面がある。攻撃者のコストを多少高めても、攻撃者の側にそれを越える利益が生じるような場合、コストだけでは不正を防止することはできない。例えば、過去には、本物とほぼ同一の純度の金を用いることによって、真偽判定が極めて困難な偽造金貨を作製するという事件も起きている。過去に発生したプリペイドカードの偽造事件の経験を踏まえても、偽造品の製造コストに着目したコンセプトの偽造対策には限界があるように思われる。

４．人工物のセキュリティに関する新しい発想の必要性

このように、「人工物を製造する側の技術的優位性」に立脚するセキュリティ対策は、①技術進歩や秘密情報の漏洩により優位性が喪失されるという問題と、②その人工物のセキュリティがどの程度脅威にさらされているかを製造者が検証できないという問題を抱えている。①については、人工物のセキュリティ対策に利用される技術の裾野が広がり、国内外でさまざまな企業が人工物のセキュリティ対策に関与していることや、IT化の進展により、技術進歩のサイクルが短くなってきていることを考えると、従来に比べ、問題がより深刻になっていると考えるべきであろう。また、②については、攻撃者がどの程度、製造者側の技術に追いついてきているかを検知することが難しいため、実際に大規模な不正行為が発生するまで、製造者側がそれと気づかないという深刻な事態を招来しかねない点に注意が必要である。実際、過去にいくつかの種類のプリ

ペイドカードの大規模な偽造犯罪が発生した際も、偽造が発覚してから製造者側が迅速な対応を取れなかったことが被害を大きくしたといわれている。

こうした問題を回避する手段としては、これまで秘匿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によって、安全性についての客観的基準を持つことができるようにすることが考えられる。しかし、現在の人工物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性」を実現しているため、情報を公開することが難しい。そこで参考になるのは、暗号技術、デジタル署名技術などの情報セキュリティ技術の考え方である。例えば、暗号アルゴリズムは、その技術内容そのものはすべて公開されている一方、暗号化のために必要となる「鍵」を秘匿し、その鍵を推定することが計算量的に困難であることを利用して安全性を確保している。正規のシステム利用者と攻撃者が同程度の技術水準であったとしても、システム利用者が管理している秘密の「鍵」の情報が知られなければ、安全性が保たれるという仕組みとすることによって、暗号技術やデジタル署名技術を学術的な分析の対象とすることができるため、万一、暗号アルゴリズムの安全性に欠陥があればオープンな場で問題が指摘され、修正が可能となる。人工物のセキュリティ対策に対して、このようなアプローチが可能になれば、上記のような問題を回避し、セキュリティ対策の水準を高めていくことが期待できるだろう。

しかし、暗号技術やデジタル署名技術を単純に人工物のセキュリティ対策に適用してもうまくいかない。例えば、紙にシリアルナンバーとそれに対応するデジタル署名を印刷したとしても、それはその紙を複製する際の障害にはならない。デジタル署名もろとも、その人工物全体の複製物が作製できてしまうからである。そこで、人工物と情報セキュリティ技術とを結びつける工夫が必要となってくる。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。

５．人工物メトリクスの考え方──人工物の固有パターンの利用

「人工物メトリクス（artifact-metrics）」とは、著者の一人がバイオメトリクス（biometrics）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、「人工物に固有の特徴を用いて人工物を認証する技術」という意味である。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（人間の指紋に相当するもの）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技術のことを指している。人工物メトリクスを実現する装置やシステムのことを、人工物メトリック・システム（artifact-metric system）と呼ぶ[9]。

本論文で議論の対象としている人工物は、紙に印刷したものであれ、プラスチック製のカードであれ、一種の工業規格品であるから、同じ製造技術を用いれば同じ性質を有するものを複数製造することが可能である。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、例えば紙における繊維の絡まり具合いなどはおのおの異なり、人工物毎の「個性」ともいうべき固有パターンを持っている。このような個々の人工物の固有パターンが、例えばバイオメトリクスにおける人間の指紋のように、個々の人工物を識別するために利用でき、かつ、人為的な偽造・複製が困難であれば、これをセキュリティ対策に利用することができる。これが、人工物メトリクスの基本的な考え方である。

もちろん、通常の製造技術で製造した紙やプラスチックの固有パターンを、個体の識別に利用することは難しい。個体別に個性が際立つような製造技術が必要である。そのような目的で利用できる固有パターンとして、さまざまな提案がなされている。詳しくは別稿[10]に譲るが、図表４に掲げるようなさまざまな技術がその候補として提案されている。

---

[9] Matsumoto *et al.* [2001]
[10] 松本・宇根・松本・岩下・菅原[2004]

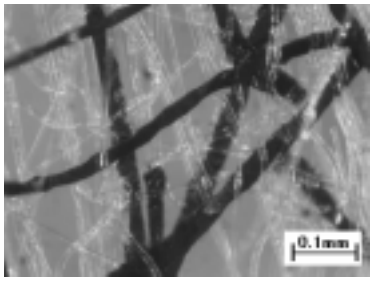
図表４　人工物メトリクスに利用される固有パターンの例

物理特性	固有パターンの例
光学特性	（イ）基材にランダム分散した粒状物の光反射パターン （ロ）基材にランダム分散した光ファイバの透過光パターン （ハ）基材のランダムな斑の透過光パターン （ニ）ランダムに配置されたポリマ・ファイバの視差画像パターン （ホ）基材にランダム分散したファイバの画像パターン
磁気特性	（ヘ）基材にランダム分散した磁性ファイバの磁気パターン （ト）磁気ストライプにランダムに記録された磁気パターン （チ）磁気ストライプの製造時にランダムに配置された磁気パターン
電気特性	（リ）半導体素子内のメモリ・セルにランダムに蓄積された電荷量パターン
振動特性	（ヌ）導電性ファイバをランダム分散した基材の共振パターン （ル）容器に貼ったシールを振動させたときの共鳴パターン

人工物メトリクスの金融業務への適用とは、金融取引における決済手段や取引証跡等に利用されるさまざまな人工物（証書、証券、紙幣、カード等）について、人工物メトリクスに基づくシステムを導入して偽造、複製、改ざんを防止し、安全性、信頼性を維持することを意味する。

具体的な例で説明しよう。磁性ファイバ（磁性材料を内包した繊維）を紙に混入して製紙することにより、紙の中でランダムに形成される磁性ファイバの三次元構造を「人工物の制御困難な固有パターン」として利用する技術が提案されている（前掲図表４の(**ヘ**)、図表５の顕微鏡写真を参照)。磁性ファイバの三次元構造は、磁性ファイバの配置だけでなく紙の繊維との絡まり具合などによっても決定されるため、ランダムに形成された磁性ファイバの構造を、別の紙において寸分違わず再現することは困難と考えられる。

図表５　磁性ファイバを混入して製紙した紙の顕微鏡写真

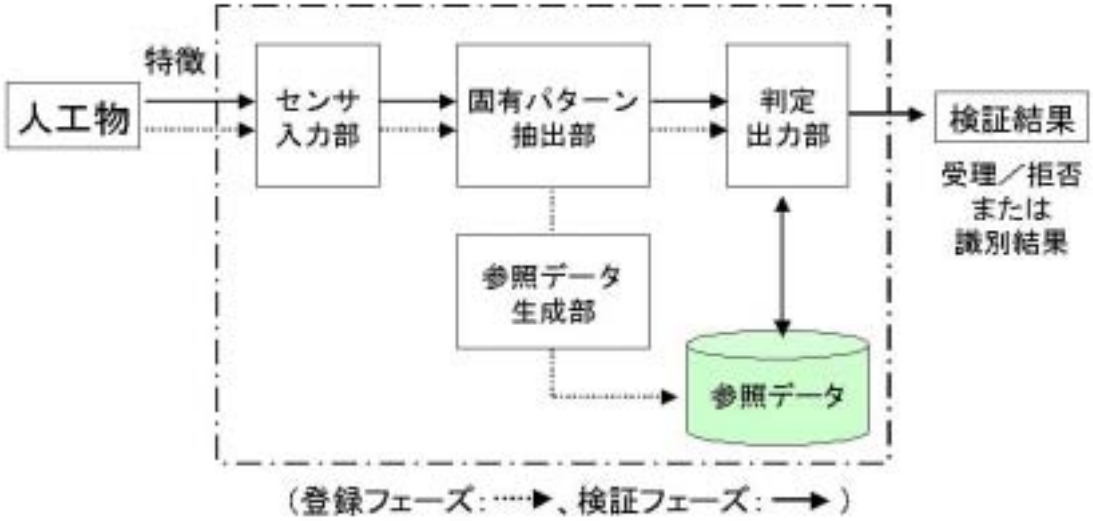


黒い磁性ファイバが白い媒体繊維と絡まり、三次元構造を形成している

（資料：Matsumoto *et al.* [2001]）

この技術を人工物メトリック・システムに適用する場合、まず、この磁性ファイバによる固有パターンを含んだ人工物の特定部分を磁気センサーによって読み取り、得られた電気信号をデジタル変換したデータを「参照データ」として人工物メトリック・システムのデータベースに記録しておく（図表６の登録フェーズ)。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磁気センサーで読み取り、得られたデータを記録された「参照データ」と比較してどの程度一致するかを判定する（図表６の検証フェーズ)。

図表６　人工物メトリック・システムの基本構成



このような技術は、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。IOSAS（イオサス：Inherence Of Stock Authentication System）と呼ばれるこの人工物メトリック・システムでは、株券用紙の製造工程において原料に磁性ファイバを混入することでおのおのの株券に固有パターンを付与し、株券の発行フェーズにおいて、各株券の固有パターンを読み取り、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。株券の検証フェーズにおいては、参照データをデータベース内で検索し、株券から得られた固有パターンが個体識別番号に対応する固有パターンであるか否かを確認することで株券の真贋判定を行う仕組みとなっている。

６．人工物メトリック・システムへの攻撃

このように、人工物メトリクスを実現するためには、個々の人工物を識別して照合する複雑なシステムの構築が必要となるが、その分、人工物のセキュリティを大幅に高めることができる。この技術が適切に設計、運用されていれば、仮に、その人工物の製造者と全く同じ材料と装置を用いて人工物を複製しようとしても、検証を通過して本物として受理されるような複製物を作製できない、という効果が期待できるため、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。人工物メトリクスは、「いかなる手段を用いても人工物の偽造が不可能になる」ということまでを主張するものではない。しかし、上記のような特性から、技術内容を公開し、さまざまな攻撃法についてアカデミックな分析の対象にできるため、精巧に複製が行われた場合に、どの程度の確率で複製物が検証を通過してしまうかを定量的に評価することができる[11]。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可能になる。

それでは、どのような方法で人工物メトリック・システムを攻撃できるのであろうか。システム全体への攻撃にはさまざまなものが考えられるが、特に、人工物の偽造・複製・改ざんとの関係で重要な攻撃は、①ブルートフォース（brute force、「腕力ずくの」といった意味。）攻撃と、②デッドコピー（dead copy、「丸ごとの複製物」といった意味。）攻撃である。攻撃の詳細と実際の人工物メトリック・システムの適用事例における評価の詳細については前記の別稿に譲ることとし、以下ではその概要を整理することとする。

（１）ブルートフォース攻撃

ブルートフォース攻撃とは、「検証対象となっている人工物以外のものを無作為に提示することで、人工物メトリック・システムの認証を通過させようとする攻撃」と定義される。人工物メトリック・システムは、互いに異なる人工物の固有パターンを読み込んで検証するシステムであるが、同じ人工物を読み込

[11] Matsumoto and Matsumoto[2002, 2003]

んでも、そこで観測される固有パターン情報は毎回微妙に異なる。このため、あらかじめ登録された固有パターンの情報と、観測された情報とを照合し、誤差が小さければ受理と判定する仕組みを採用している。ここで、条件を厳しくすれば、正規の人工物が不受理とされることがあるという問題が生じ、条件を緩やかにすれば正規でない人工物が受理されることがあるという問題が生じる。このため、受理の条件をどの水準に設定するかが大きな問題となる。人工物メトリクスを金融業務に適用した場合、極力、不正規の人工物を受理してしまわないよう、効率性よりも安全性を重視した設計にする必要があるが、それでも、不正規の人工物を受理してしまう確率（誤受理率、FAR; false acceptance rate）をゼロにすることは難しい。ここを悪用するのがブルートフォース攻撃である[12]。具体的には、正規のものと同じ形状で、同じようにランダムな固有パターンを持った人工物を大量に作製し、それが検証で受理されるかどうか、繰り返し試行する攻撃のことである。

ブルートフォース攻撃は、専門的な知識や技能がなくとも実行が容易な攻撃であるため、人工物メトリック・システムを実用化する際には、十分な耐性を持たせておくべき攻撃である。ブルートフォース攻撃への耐性の高さは、①繰り返し攻撃を許さない運用環境となっていること、②システムの実用性を損なわない範囲内で誤受理率が低く抑えられていること、の２点に依存している。前者は運用管理の問題、後者はシステムの認証精度の問題であり、システムの安全性を確保するためには、当然充足しなければならない条件である。

（２）デッドコピー攻撃

これに対し、デッドコピー攻撃とは、「本物を見本にして固有パターンを複製したクローンを提示することで、人工物メトリック・システムの認証を通過させようとする攻撃」と定義される。

人工物メトリクスにおける固有パターンとして、製造過程に偶然発生するランダムなパターンを利用する場合、本物と同じ材料・装置・製法で人工物を作

[12] Matsumoto *et al.* [1997]

製しても、固有パターンが一致する確率は低い（どの程度低いかは、利用する固有パターンの情報量およびランダム性に依存する）。この確率が十分低い場合、本物と同じ製法で複製を作ることは困難と考えられる[13]。

しかし、その場合でも、「本物と異なる製法」を用いて、人工物の読取装置が「本物と同一の固有パターンを持つ」と誤認するような複製を作ることは可能かもしれない。そのような複製物をクローンと呼ぶ。例えば、人工物にランダムな磁気パターンを付着させて、これを固有パターンとして利用する場合、本物から磁気パターンを読み取って、特殊なプリンタによって磁気パターンを正確に複写することができれば、クローンが作製できる。これに対し、例えば、人工物の上に特殊な三次元構造を持つ磁気パターンをランダムに生成する仕組みであって、その構造を読取装置がきちんと読み取れる仕組みであれば、プリンタによってクローンを作製することは困難であろう。なお、特殊な三次元構造を持つ磁気パターンであっても、読取装置がそれを単純な情報として読み取っている場合、クローン作製の難易度は高まらない。

このようなデッドコピー攻撃への耐性、すなわち、人工物においてクローンを作製することが困難であるような性質を「耐クローン性」と呼ぶ[14]。耐クローン性は、人工物メトリック・システムの安全性の核となる特性であるが、ある人工物メトリック・システムにおいて、人工物が耐クローン性を持つかどうかを評価するためには、さまざまな角度からの分析が必要となる。人工物のクローンが作製できるか否かの評価は、どのような手法でクローンを作製しようとするかに依存するからである。筆者らを含む研究チームでは、人工物メトリック・システムの実験装置を利用して具体的なクローン作製を試みることにより、耐クローン性の評価を行った[15]が、こうした評価は、常に新しい技術革新を取り入

---

[13] 本物と同じ材料・装置・製法で作ったものであっても、その人工物の固有パターンがデータベースに登録されていないので、人工物メトリクス・システムの認証で受理されないため。

[14]「耐クローン性」という概念は、人工物メトリック・システムを評価する文脈だけではなく、バイオメトリック・システムの安全性を分析する文脈でも利用される（山田・松本・松本［2000a, b, 2001］、Matsumoto *et al.* [2002]、松本・竹田・星野・田辺・平林[2004]、松本・平林[2003a, b]、松本・平林・佐藤[2004]）。

[15] Matsumoto and Matsumoto[2003]、松本・宇根・松本・岩下・菅原[2004]

れつつ、継続的に実施される必要がある。

７．おわりに

本論文で論じてきた人工物のセキュリティは、人々の身近で利用される技術でありながら、従来、あまりオープンな場で議論されることのなかったテーマである。これまでこうした議論が秘密とされることが多かったのは、人工物の安全性の根拠を「製造者の技術的優位性」に依拠させてきたからである。しかし、情報技術の発達が、そうした安全性の根拠を不確かなものとしつつあることを考えると、今後は、従来とは異なる考え方が必要とされているのではないか、というのが、本研究の基本にあるコンセプトである。

情報セキュリティ技術の分野でも、かつてはその技術研究の内容が秘密とされた時代があった。しかし、米国の政府標準暗号である DES が、比較的オープンな場で議論の対象となり、その技術内容が公開されたことなどをきっかけとして、暗号アルゴリズムやデジタル署名方式などの分野では、その技術を公開して大勢の研究者がその安全性を検討するという研究スタイルが確立している。もちろん、個別システムのセキュリティ対策とか、IC カードの耐タンパー性の問題のように、技術内容を公開してしまうと攻撃を受けやすくなるリスクのある技術分野もあり、公開の仕方には工夫が必要である。しかし、人工物の安全性、信頼性を維持するためにさまざまな叡智を糾合するという観点からは、可能な限り、技術内容を公開する方向で研究を進めていくことが望ましいと考えられる。

本論文で紹介した人工物メトリクス技術は、提案されているもののほんの一部に過ぎない。例えば、おのおのの人工物の固有パターンに対応する参照データをどのように管理するかについては、さまざまなバリエーションが提案されている。本論文で紹介したのは、参照データをデータベースに格納して検証時に参照するという最も基本的な方式であるが、例えば、参照データを人工物に書き込み、それに対応するデジタル署名を付与しておくことによって、人工物をオフラインの検証装置を用いて単独で検証するという方式が可能になる。こ

の方式は、株券よりも幅広い利用者が検証作業を行う業務用途に向いているだろう。そうした観点を含め、人工物メトリクスをさまざまな業務用途に適用範囲を拡大していくためには、運用技術やコストなどの条件を加味した、より実践的な検討を深めていく必要があろう。

また、セキュリティ評価に関する研究を更に深化させることも大切である。特に、人工物メトリクスの中核ともいえる耐クローン性については、具体的なクローン作製方法を想定し、その方法に対する安全性を評価するというアプローチを取らざるを得ない。今回、われわれが研究の対象とした人工物メトリック・システムの実験装置に限定したとしても、研究の中で取り上げたクローン作製方法は一例であって、それ以外にもさまざまな方法が考えられる。より優れたクローン作製方法が考案されれば、耐クローン性に対する安全性評価をより厳しく見積もる必要があり、システム設計やパラメータ選択に影響を与えるし、人工物に固有パターンを付与するために磁性ファイバを用いるのがよいか、他の技術を用いるのがよいか、といった選択にも影響を与える。あらかじめ、すべてのクローン作製方法を考えておくことはできないので、新たに考案される脅威に備えて、どの程度、安全性のマージンを取っておくかが重要なポイントとなる。そのためにも、さまざまな角度から人工物メトリクスの安全性が評価されることが望ましく、オープンな場で十分な検討が行われることが望ましいと考えられる。

【参考文献】

金融情報システムセンター、『金融機関等コンピュータシステムの安全対策基準・解説書（第 6 版）』、2003 年 11 月

警察庁、『警察白書〈平成 15 年版〉―組織犯罪との闘い』、2003 年 9 月

情報処理振興事業協会、『平成 11 年度 スマートカードの安全性に関する調査 報告書』、2000 年 2 月（http://www.ipa.go.jp/security/SmartCard/sc-survey.pdf）

情報処理振興事業協会・通信放送機構、『暗号技術評価報告書（2002 年度）』（CRYPTREC Report 2002）、2003 年 12 月（http://www.ipa.go.jp/security/enc/CRYPTREC/）

全国銀行協会、「盗難通帳による払出し件数・金額等に関するアンケート結果について」、2004 年 2 月（http://www.zenginkyo.or.jp/news/16/index160232.html）

日本クレジット産業協会、「クレジットカード不正使用被害の発生状況」、2004 年 2 月（http://www.jccia.or.jp/toukei_fusei.html）

松本勉（横浜国立大）・岩下直行、「情報セキュリティ技術の信頼性を確保するために」、『金融研究』第 20 巻第 2 号、日本銀行金融研究所、2001 年 4 月、21～32 頁

――・竹田恒治・星野幸夫・田辺壮宏・平林昌志、「人工指による指紋センサ評価の可能性」、『2004 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、2004 年、585～590 頁

――・平林昌志、「虹彩照合技術の脆弱性評価（その１）」、『ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会・第 1 回研究発表会予稿集』、電子情報通信学会、2003 年 a、53～59 頁

――・――、「虹彩照合技術の脆弱性評価（その２）」、『コンピュータセキュリティシンポジウム 2003 論文集』、情報処理学会、2003 年 b、187～192 頁

――・――・佐藤健二、「虹彩照合技術の脆弱性評価 （その３）」、『2004 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、2004 年、701～706 頁

松本弘之・宇根正志・松本勉（横浜国立大）・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」、IMES Discussion Paper Series No.2004-J-13、日本銀行金融研究所、2004 年 4 月

山田浩二・松本弘之・松本勉（横浜国立大）、「指紋照合装置は人工指を受け入れるか」、『電子情報通信学会技術研究報告』Vol. 100 No.213、ISEC2000-45、電子情報通信学会、2000 年 7 月 a

――・――・――、「指紋照合装置は人工指を受け入れるか（その２）」、『コンピュータセキュリティシンポジウム 2000 論文集』、情報処理学会シンポジウムシリーズ Vol. 2000 No.12、情報処理学会、2000 年 10 月 b

――・――・――、「指紋照合装置は人工指を受け入れるか（その３）」、『2001 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、2001 年、719～724 頁

Matsumoto, Hiroyuki and Tsutomu Matsumoto (Yokohama National University), “An Evaluation Method for a Magnetic Artifact-metric System,” IPSJ Journal, 43 (8), 2002, pp. 2458-2466.

—— and ——, “Clone Match Rate Evaluation for an Artifact-metric System,” IPSJ Journal, 44 (8), 2003, pp. 1991-2001.

——, Hidekazu Hoshino, Tsugutaka Sugahara and Tsutomu Matsumoto (Yokohama National University), “A clone preventive authentication technique which utilizes physical characteristics,” HELSINKI’97 I.C.P.O.-Interpol 9th International Conference on Currency Counterfeiting and 3rd International Conference on Fraudulent Travel Documents, 1997.

——, Itsuo Takeuchi, Hidekazu Hoshino, Tsugutaka Sugahara and Tsutomu Matsumoto (Yokohama National University), “An Artifact-metric System Which Utilizes Inherent Texture,” IPSJ Journal, 42 (8), 2001, pp. 139-152.

Matsumoto, Tsutomu (Yokohama National University), Hiroyuki Matsumoto, Koji Yamada and Satoshi Hoshino, “Impact of Artificial "Gummy" Fingers on Fingerprint Systems, ” Optical Security and Counterfeit Deterrence Techniques IV, Proceedings of SPIE, 4677, 2002, pp.275-289.