IMES DISCUSSION PAPER SERIES

人工物メトリクスの評価における現状と課題

松本弘之（まつもとひろゆき）・宇根正志（うねまさし）・松本 勉（まつもとつとむ）・岩下直行（いわしたなおゆき）・菅原嗣高（すがはらつぐたか）

Discussion Paper No. 2004-J-13

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

IMES Discussion Paper Series 2004-J-13
2004 年 4 月

人工物メトリクスの評価における現状と課題

まつもとひろゆき　うね まさし　まつもとつとむ　いわしたなおゆき　すがはらつぐたか
松本弘之[*]・**宇根正志**[**]・**松本 勉**[***]・**岩下直行**[†]・**菅原嗣高**[‡]

要　旨

人工物メトリクスは、人工物に固有の特徴を用いて人工物を認証する技術である。金融分野においては、証書やカードなどの人工物を用いた取引や処理が随所で行われており、その安全性や信頼性を高める手段として、人工物メトリクスが有用であると考えられる。

人工物メトリクスを活用するためには、人工物メトリクスの認証精度の評価を適切に行い、アプリケーションに見合った技術を採用する必要がある。しかし、従来、個別の人工物メトリクスの技術情報が開示されることは少なく、学会などのオープンな場において認証精度の評価に関する議論が活発に交わされるケースは稀であった。この結果、認証精度の評価基盤や評価手法が十分に確立されていないのが実情である。

今後は、認証精度の評価基盤および評価手法の構築にまず取り組む必要がある。特に、人工物メトリクスにおける認証に成功するような人工物の複製がどの程度困難か（耐クローン性）を評価することが重要であると考えられる。こうした検討を行う際には、バイオメトリクス（生体認証技術）の先行事例を参照することが有用であろう。

本論文では、まず、人工物メトリクスの概念を整理する。その上で、認証精度の評価の現状を概観し、バイオメトリクスにおける先行事例を踏まえながら、認証精度の評価基盤を今後整備していく上で対応すべき課題について述べる。さらに、そうした課題の 1 つであるセキュリティ評価の枠組みについて検討するとともに、代表的な人工物メトリクスの事例を紹介する。

キーワード：人工物メトリクス、セキュリティ評価、耐クローン性、
認証精度、バイオメトリクス
JEL classification：L86、L96、Z00

*　日本発条株式会社情報セキュリティ事業部 (E-mail: h.matsumoto@nhkspg.co.jp)
**　日本銀行金融研究所研究第 2 課 (E-mail: masashi.une@boj.or.jp)
***　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)
‡　日本発条株式会社情報セキュリティ事業部 (E-mail: sugahara@nhkspg.co.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。なお、本論文に示されている内容および意見は筆者たち個人に属し、日本銀行あるいは金融研究所の公式見解を示すものではない。

目　次

１．はじめに

人工物メトリクス（artifact-metrics）は、各人工物に固有の特徴を用いて人工物の認証を行う技術である。人工物メトリクスは、検証対象となる人工物が特定の人工物であるか否かを確認する機能（1 対 1 照合）や、人工物がどの人工物なのかを特定する機能（1 対 N 照合）をもっている。人工物メトリクスという用語は、バイオメトリクス（biometrics、生体認証技術）と対をなす用語であり、認証の対象が「人工物」か「生体」かという点で異なっている。人工物メトリクスを実現する装置やシステムに対しては、人工物メトリック・システム（artifact-metric system）という用語が当てられている。

人工物メトリクスには、たとえ攻撃者が人工物の製造方法や認証方法などの情報を入手していたとしても、認証に成功するようなクローンを作製することが困難であることが求められる。このような性質を「耐クローン性」と呼ぶ。高度な耐クローン性を確保する方法としては様々な可能性が考えられるが、これまでに提案されている人工物メトリクスでは、人工物の製造者でさえも再現困難なランダムな特徴を各人工物に付与する、あるいは、各人工物がもともと備えているランダムな特徴を利用するといった方法が主流となっている。例えば、磁性ファイバを紙に無作為に混入し、紙の中で形成される磁性ファイバの 3 次元構造を「再現困難な特徴」として利用する技術が提案されている。磁性ファイバの構造は、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、いったん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であると考えられる。

人工物メトリクスは、金融分野において、各種取引の安全性を確保する上で有用な技術と考えられる。金融業務では、手形、小切手、各種帳票などの紙の証書が用いられるほか、キャッシュカードなどの各種トークンが取引実行時に必要とされるケースがある。こうした従来の証書やトークンの耐クローン性は、印刷技術の向上やパソコンによる画像処理能力の向上といった技術進歩に伴って徐々に低下するという性格を有している。また、証書のクローン対策の 1 つとして印鑑の印影を証書に付加する方法があるが、近年、特定の印影を容易に偽造することが可能になっており、対策としての有効性が低下しつつある。もちろん、金融取引のセキュリティはこうした証書やトークンにのみ依存しているわけではなく、これらの安全性の低下が直ちに金融取引の信頼性に影響を与えるとはいえない。しかし、証書やトークンに対して従来期待されていたセキュリティ・レベルが低下しつつあるのは事実であり、セキュリティ・レベルの低下を補強する技術として、高度な耐クローン性を意図して設計された人工物メトリクスが有望であると考えられる。

ただし、現時点では、利用者が一定の要件に見合った人工物メトリクスを適切に選択することは容易でない。これは、人工物メトリクスの認証精度評価の基盤や手法が十分に整備されていないことなどによるとみられる。人工物メトリクスの認証精度評価を適切に行うためには、人工物メトリクスの概念や用語を統一した上で、認証精度の指標やその測定方法を確立する必要がある。しかし、これまで人工物メトリクスに属する個別技術の情報が開示されてこなかったという経緯もあって、学会や標準化団体などのオープンな場において人工物メトリクスの認証精度評価の基盤構築に関して議論が行われることは稀であり、概念・用語の整備、認証精度評価の基盤・手法の確立や標準化といった重要な課題が残されている。現在では、人工物メトリクスの認証精度評価は高い技術力を有するとみられている専門の評価機関において実施されるケースが多い。これに対して、バイオメトリクスでは、指紋や虹彩などの生体情報を利用した認証技術に関して、様々な観点からの研究成果が学会で発表されているほか、バイオメトリクスの標準化を担当する ISO/IEC JTC1/SC37 を中心に、用語や精度評価の手法などに関する国際標準の審議が進められている。

こうしたバイオメトリクスに関する動向を踏まえ、人工物メトリクスの分野においても、今後、認証精度をどのように評価するかについて検討を進めることが必要である。その際には、認証精度をセキュリティ特性の 1 つに位置づけた上で、攻撃者が人工物の複製を作製するといった攻撃が起こりうることを想定し、セキュリティ評価の一部として認証精度の評価について検討することが求められる。また、オープンな場での議論を通じて、こうした認証精度の評価に関する検討を深めていくことが重要であると考えられる。

本論文は、人工物メトリクスの概念や特性を整理し、人工物メトリクスの認証精度評価の現状について説明するとともに、認証精度の評価基盤確立に向けての今後の課題を提示する。

本論文の構成は以下のとおりである（次頁の図 1.1 参照）。まず、２章において、人工物メトリクスの概念や機能、バイオメトリクスとの関連性、人工物メトリクスの既存技術について述べ、本論文の検討対象を示す。

３章では、人工物メトリクスの認証精度評価の方法と現状を、バイオメトリクスと対比しつつ説明する。特に、人工物のクローンを作製するという攻撃を前提とした認証精度評価の重要性を強調するとともに、今後の主な課題として、①認証精度の評価基盤の構築、②認証精度の評価手法の構築、③耐クローン性の評価手法の構築、④認証精度の基準値の設定、の 4 つを挙げる。

４章では、３章において提示した 4 つの課題の中でも「認証精度の評価基盤の構築」に焦点を当て、評価基盤の構築に向けて最初に検討すべき「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」について議論する。クローンを用いた攻撃を想定し、一定の利用環境を規定した上で、最低限考慮すべき主な攻撃方法としてどのようなものが考えられるかを検討する。次に、それらの攻撃に対抗するためのセキュリティ要件を明らかにし、各要件の達成度合いを評価するための尺度の候補を検討する。

５章では、既存の評価事例として、磁性ファイバを利用した人工物メトリック・システムを取り上げ、その結果を紹介する。具体的には、４章において列挙した攻撃の中からブルートフォース攻撃とデッドコピー攻撃を取り上げ、これらの攻撃に対してどの程度の耐性を有しているかを定量的に評価した結果とそのインプリケーションを説明する。

６章では、論文のポイントや主張を再度整理して、論文全体を締めくくる。

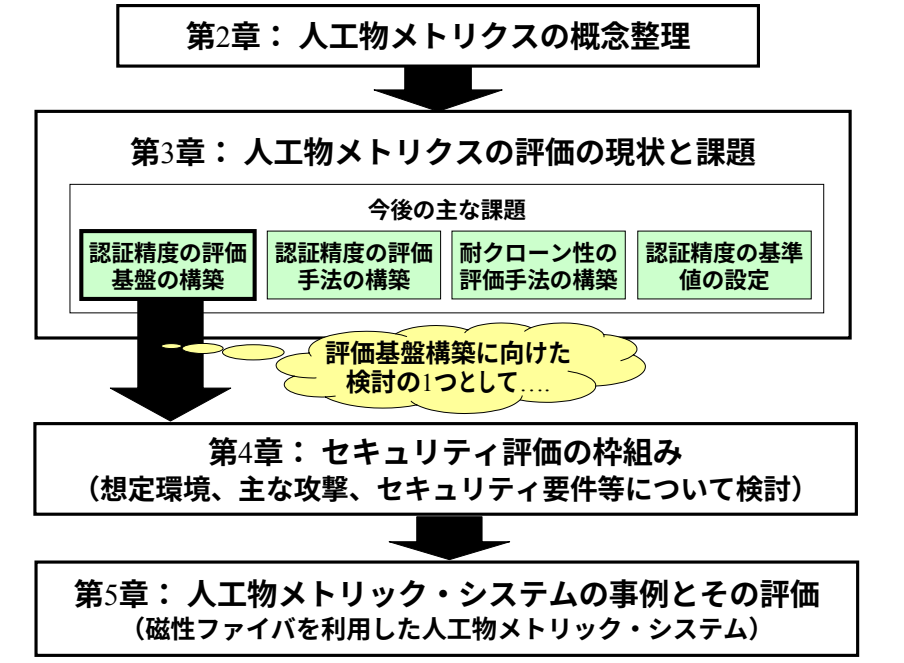

図 1.1 本論文の主要パートの位置付け

２．人工物メトリクスとは？

本章では、まず人工物メトリクスおよび関連技術の概念整理を行う。その上で、人工物メトリクスの基本構成について説明し、人工物メトリクスに属する既存の技術を紹介する。

（1）人工物メトリクスとバイオメトリクス

イ．人工物メトリクスの概念整理

（イ）人工物メトリクスの定義

人工物メトリクス（artifact-metrics）は、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、次のように定義することができる。

> **【人工物メトリクスの定義】**
>
> 各人工物に固有の特徴を用いて人工物の認証を行う技術

人工物メトリクスは、上記定義に該当する技術を研究対象とする「学問領域」を示す用語として使われることもあるが、本論文では、特に断らない限り「技術」を意味するものとする。また、人工物メトリクスを実現するシステムは、「人工物メトリック・システム（artifact-metric system）」と呼ばれる（Matsumoto *et al.* [2001]）。

上記の定義では、①どのような「固有の特徴」を用いるのか、②「人工物の認証」とはどのような処理を指すのか、について明確に示されておらず、いろいろな解釈があり得る。以下では、人工物メトリクスと呼ばれる技術が一般にどのような技術を指すのかを追加的に説明する。また、同時に、本論文において議論の対象とする人工物メトリクスの範囲についても説明する。

（ロ）各人工物に固有の特徴

人工物メトリクスにおける「各人工物に固有の特徴」としては、作製された当初より人工物が備えている物理特性から得られる特徴（物理的特徴と呼ぶ）を利用するケースが多い。具体例については後述するが、例えば、紙の証書などにランダムに分散させた磁性ファイバから得られる磁気パターンや、ラベルなどにランダムに分散させた粒状物の光反射パターンなどが挙げられる。このほか、物理的特徴として、人工物の動作から得られ

る特徴（行動的特徴とも呼ばれる）を利用することも考えられる。

本論文では、比較的提案事例が多く、金融業務に利用される証書やカードなどへも適用可能な「物理的特徴を用いた人工物メトリクス」を検討対象とする。

なお、人工物をその特徴によって直接認証するだけでなく、個人が所持している人工物を用いてその個人を間接的に認証するケースや、人工物 A に添付された別の人工物 B を用いて人工物 A を間接的に認証するケースもある。これらを考慮すると、人工物の特徴は間接的または並列的に組み合わされる場合もあるといえる。

（ハ）人工物の認証の形態

①1 対 1 照合と 1 対 N 照合

人工物の認証の形態としては、「1 対 1 照合（verification）」と「1 対 N 照合（identification）」が挙げられる。

人工物の認証における 1 対 1 照合は、「検証対象となっている人工物が、予め識別された人工物であるか否かを確認する」という処理である。検証時に、検証対象の人工物そのものに加え、その人工物を識別するための情報（ID と呼ぶ）が提示され、検証対象の人工物の特徴と、提示された ID に対応する人工物の特徴が照合されることとなる。

一方、人工物の認証における 1 対 N 照合は、「検証対象となっている人工物を識別するための ID が予め提示されることなく、検証対象の人工物がどの人工物なのかを識別する」という処理である。検証時には、検証対象の人工物だけが提示され、検証対象の人工物の特徴と、候補となる人工物の特徴が順次照合されることとなる。両者の特徴が一致すると判断された場合には、検証対象の人工物の ID が出力される。また、検証対象の人工物がブラックリストなどに登録されている人工物でないことを上記と同様の手続で確認する処理（ネガティブ識別と呼ばれる）も 1 対 N 照合に対応する。

②人工物の認証のレベル：個体とグループ

人工物を認証する際に「人工物をどのレベルまで認証するか」という点に着目すると、検証対象の人工物がどの個体であるかを明らかにするケースと、検証対象の人工物がどのグループに属するかを明らかにするケースとに分けられる。これらのケースはバイオメトリクスにおいても当てはまる。具体例は以下のとおりである。

- **「どの個体であるか」を認証するケース**
  - 例 1：株券に漉き込まれた磁性ファイバによって生み出される磁性パターンを用いて、検証対象となっている株券を一意に特定する（人工物メトリクスの例）。
  - 例 2：指紋や DNA から個人を特定する（バイオメトリクスの例）。
- **「どのグループに属するか」を認証するケース**
  - 例 3：磁性インクによる画一的な印刷が施された証書から得られる磁気パターンを用いて、証書の真贋判定を行う（人工物メトリクスの例）。
  - 例 4：血液や体液から、その個人の血液型を特定する（バイオメトリクスの例）。

「どの個体であるか」を認証するケースは、「どのグループに属するか」を認証するケースに比べて、高い確率でより狭い範囲のグループに絞り込むケースであると考えることができる。

これらのケースのうち、本論文では、検証対象の人工物がどの個体であるかを認証するケースに焦点を当てる。これは、本論文が、「各人工物に固有な物理的特徴を用いた人工物メトリクス」を対象としており、各人工物に固有の特徴によって「どの個体であるか」を認証可能であることによる。

③機械による処理

人工物の認証を機械によって実行する場合と、人手によって実行する場合が考えられる。ただし、通常の人工物メトリクスでは、センサによる物理的特徴の読取りや複雑な演算処理を実行する必要があることから、機械によって処理を行う場合が一般的である。こうしたことから、本論文においても、機械によって認証の処理を行う人工物メトリクスを議論の対象とする。

（ニ）耐クローン性

人工物メトリクスが適切に機能するためには、必要とされる精度で人工物を正しく認証することが必須である。仮に、人工物の複製品（クローンと呼ぶ）を、その人工物メトリクスの認証において正当な人工物と判定されるように作製することが容易であるならば、1 つの人工物からクローンが複数作製され、それらが「正当に作製された人工物」として不正に使用されるおそれがある。特に、金融分野をはじめとする高度なセキュリティ

が要求される場合には、たとえ攻撃者が人工物の製造方法や認証方法などの情報を入手していたとしても、攻撃者は人工物メトリクスにおける認証に成功するようなクローンを作製困難であることが求められる。本論文では、このようなセキュリティ特性を「耐クローン性」と呼び、耐クローン性の確保を意図して設計された人工物メトリクスに限定して議論することとする。

このように、上記**（イ）**で定義した人工物メトリクスには様々なバリエーションが考えられる。その中でも本論文において対象とするものを改めて整理すると以下のとおりである。

【本論文の検討対象】

物理的特徴を用いて機械によって認証を行う人工物メトリクスのうち、耐クローン性の確保を意図して設計されたもの

ロ．バイオメトリクスとの関係

人工物メトリクスという用語がバイオメトリクスを参考にして考案されたことから推察できるように、人工物メトリクスの概念整理は、検討が先行しているバイオメトリクスの概念整理を参考に行われてきた。こうした背景を踏まえ、前節までの概念整理に沿って、人工物メトリクスとバイオメトリクスの関係を説明する。

まず、定義に関しては、バイオメトリクスを定義している文献は数多く存在するが（例えば、Jain, Bolle and Pankanti [1999]、Bolle *et al.* [2003]）、基本的には、「各個人に固有の行動的・身体的な特徴を用いて個人の認証を行う技術」という点で共通していると考えられる[1]。このような定義を前提とすれば、認証の対象が人工物か個人かという点を除き、人工物メトリクスの定義はバイオメトリクスの定義とほぼ対応する。人工物や生体を総称して「個体」と呼び、個体を認証するシステムを「個体認証システム（individual authentication system）」と呼ぶケースもあるが（Matsumoto and Matsumoto [2003]）[2]、こうした場合、人工物メトリック・システムとバイオメトリック・システムはいずれも個体認証システムの一分野と整理することができる。

[1] 現実に実装されるバイオメトリック・システムを想定する場合には、バイオメトリクスを、「機械によって認証する技術」という属性を加えて定義することが一般的である（例えば、瀬戸 [2003]）。

[2] このほか、“ individual ”を「個人」と解釈して検証対象を人間に限定し、“ individual authentication system ”を「個人認証システム」と呼ぶ場合もある。

認証に用いられる「固有の特徴」や認証の形態も、人工物メトリクスとバイオメトリクスとでほぼ対応している。まず、固有の特徴については、バイオメトリクスにおいても物理的特徴（例えば、指紋、虹彩）と行動的特徴（行例えば、手書き署名などの筆跡）に分類される。認証の形態に関しては、バイオメトリクスにおいても1対1照合、あるいは、1対N照合が行われるほか、機械読取りによって認証が行われる場合とそうでない場合が考えられる。

こうした対応関係によって、バイオメトリクスの評価に関する研究成果が人工物メトリクスにおいても適用可能となるケースが少なくない。詳細は3章にて説明するが、物理的特徴を利用する人工物メトリック・システムでは、センサ入力における変動や固有パターン抽出における量子化誤差などに起因して、誤受理率（システムが拒否すべき個体を誤って受理する確率）や誤拒否率（システムが受理すべき個体を誤って拒否する確率）などの誤り率が存在する。こうした誤り率を測定・評価する際に、バイオメトリック・システムにおける評価指標が用いられるケースが多い。

ただし、人工物メトリクスは、バイオメトリクスとは異なり、人工物の設計・製造時に一定の自由度をもち、次のような操作が可能になる。

- 人工物の素材や組成を調整することで、認証精度や耐久性を向上させることが可能である。
- 形状を規格化することができるため、センサ入力における人工物の変動を抑えやすい。
- 一般に、人工物の評価サンプルを揃えやすく、認証精度や耐久性などを確認するための大規模な実験を行いやすい[3]。

（2）人工物メトリック・システムの構成

イ．基本構成

一般的な人工物メトリック・システムでは、まず、検証対象として提示された人工物の特徴をセンサによって捕捉し、得られた電気信号から人工物の固有パターンを抽出する。次に、人工物の登録フェーズでは、抽出された固有パターンから参照データが生成され、参照データが人工物メトリック・システムのデータベースに記録される。一方、人工物の検証フェーズでは、人工物から抽出された固有パターンと参照データを用いて一定の検証処理を

[3] バイオメトリクスでもこうした点を補う方法が検討されている。例えば、指紋センサの評価を大規模実験によって行う手段として、人工指による認証精度評価の方法についての研究が進められている（松本ほか[2004]）。

行い、検証結果（受理／拒否、または、人工物の識別結果）を出力する。

こうした流れを整理すると、人工物メトリック・システムは、次の一連の処理を自動的に実行するシステムとして表わすことができる（図 2.1 参照）。

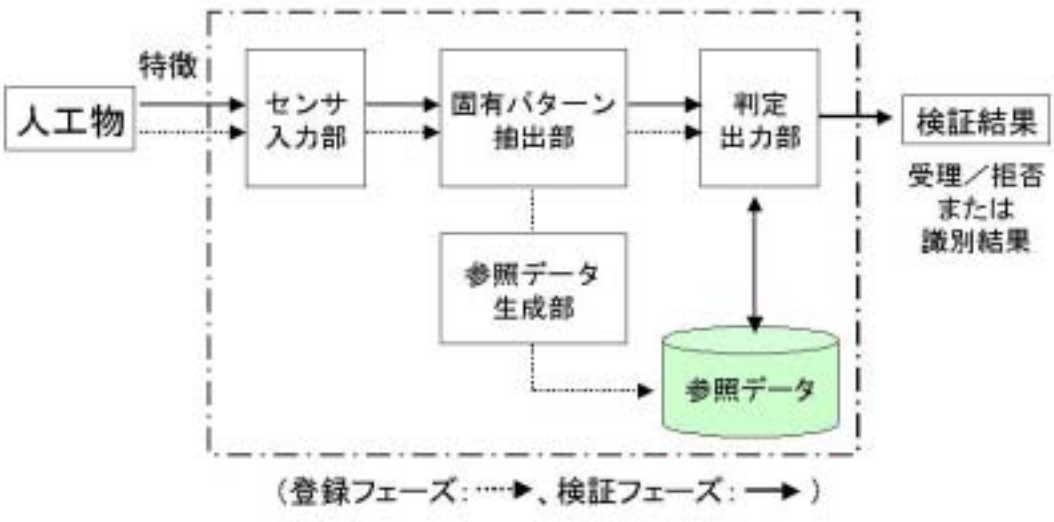

図 2.1 **人工物メトリック・システムの基本構成**

【登録フェーズ】

① 人工物からその特徴のサンプルを捕捉する（センサ入力部）。

② そのサンプルから固有パターンを抽出する（固有パターン抽出部）。

— 抽出された固有パターンの品質を検査し（判定出力部）、予め設定されたレベルの品質を下回る場合には再度固有パターンの抽出が行われる場合もある。

③ 固有パターンから参照データを生成し、データベースなどに登録する（参照データ生成部）。

【検証フェーズ】

① 人工物からその特徴のサンプルを捕捉する（センサ入力部）。

② そのサンプルから固有パターンを抽出する（固有パターン抽出部）。

③ 1 個もしくは複数の参照データと固有パターンを比較してどの程度一致するかを判定し、検証結果を出力する（判定出力部）。

ロ．検証結果

判定出力部から出力される検証結果は、人工物の認証形態によって異なる。

どの個体であるかを識別した上で検証を行う場合、1 対 1 照合においては、「検証対象の人工物が特定の 1 つの人工物であると判定する（受理）」、もしくは、「判定しない（拒否）」のいずれかが検証結果として出力される。1 対 N 照合においては、受理の場合、検証対象の人工物を識別するための ID が検証結果として出力される場合もある。

一方、グループの検証の場合にも同様の検証結果が出力される。1 対 1 照合では、「検証対象の人工物が、予め識別されたグループに属すると判定する（受理）」、もしくは、「判定しない（拒否）」のいずれかが検証結果として出力される。1 対 N 照合においては、受理の際に、検証対象の人工物が属するグループを識別するための ID が検証結果として出力される場合もある。

ハ．用途

人工物メトリック・システムの主な用途としては、次の 3 つが挙げられる。

① 個体が本物であることを検証する用途

・例 1：証券、小切手、紙幣、身分証明書などの真贋確認

② 個体が本来の状態に保たれていることを検証する用途

・例 2：証書の記載内容の改ざん検知、封書や容器の開封検知

・例 3：使用済みの投票用紙などが再利用されていないことの確認（非可逆性の証明）

— 例えば、使用済みの投票用紙を穿孔し、投票用紙の固有パターンを復元困難な形態に変化させるといった方法が考えられる。

③ 個体を識別する用途

・例 4：発行元、流通ルートなどの遡及・追跡

（3）人工物メトリック・システムの提案事例

イ．固有パターンの例

これまでに提案されてきた人工物メトリック・システムで採用されている固有パターンの例を物理特性の種類によって整理する（表 2.1 参照）。

表 2.1　人工物メトリック・システムで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) 基材にランダムに分散した粒状物の光反射パターン (ロ) 基材にランダムに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) 基材にランダムに分散したファイバの画像パターン
磁気特性	(ヘ) 基材にランダムに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に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

これらの人工物メトリック・システムの事例について以下で説明する。

ロ．固有パターンと主な人工物メトリック・システムの事例

（イ）基材にランダムに分散した粒状物の光反射パターン

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が、原理試作として提案されている（Poli [1978]）。同システムは、水晶片、金属片、アルミニウム化合物をかぶせた微粒子などをラベルの製造時にランダムに分散させ、点光源やフォト・ディテクタの位置を変えることによってそれらの配置を検出し、検出したデータを個々のラベルの固有パターンとするものである。

（ロ）基材にランダムに分散した光ファイバの透過光パターン

紙に光ファイバの小片を分散して埋め込むというアイデアのシステムが提案されている（National Material Advisory Board [1993]）。紙にランダムにすき込んだ光ファイバは、その一端に光が照射されると、ファイバ内を透過した光で他端が光輝く。同システムは、光を照射しながら紙を搬送して、フォトダイオード・アレイでこの輝きのパターンを捉えることで、個々の証書の固有パターンを検証する。

（ハ）基材のランダムな斑の透過光パターン

紙の透過光や反射光の斑を光センサで検出し、検出された光の斑を、個々の紙製タグの固有パターンとして利用するシステムが提案されている（Goldman [1988]）。

（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

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“3 Dimensional-structure Authentication System (3DAS)”が提案されている（Renesse [1995]、ORBID Corporation B.V. [2004]、図 2.2 参照）。

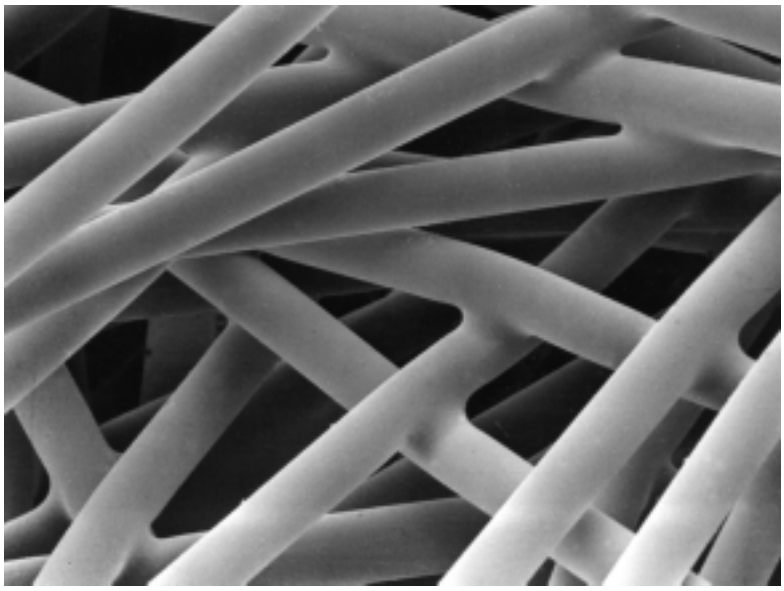

図 2.2 **樹脂内のファイバ（**3DAS**）**

（ホ）基材にランダムに分散したファイバの画像パターン

ファイバをランダムに分散させた紙片を撮像した画像を用いるシステムが提案されている（Brzakovic and Vujovic [1996]）。同報告では、シミュレーションと実際の紙片により、システムにおける照合アルゴリズムの性能の確認が行われている。

（ヘ）基材にランダムに分散した磁性ファイバの磁気パターン

磁性材料を内包したファイバを紙など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が提案されている（Matsumoto *et al.* [2001]、図 2.3 参照）。

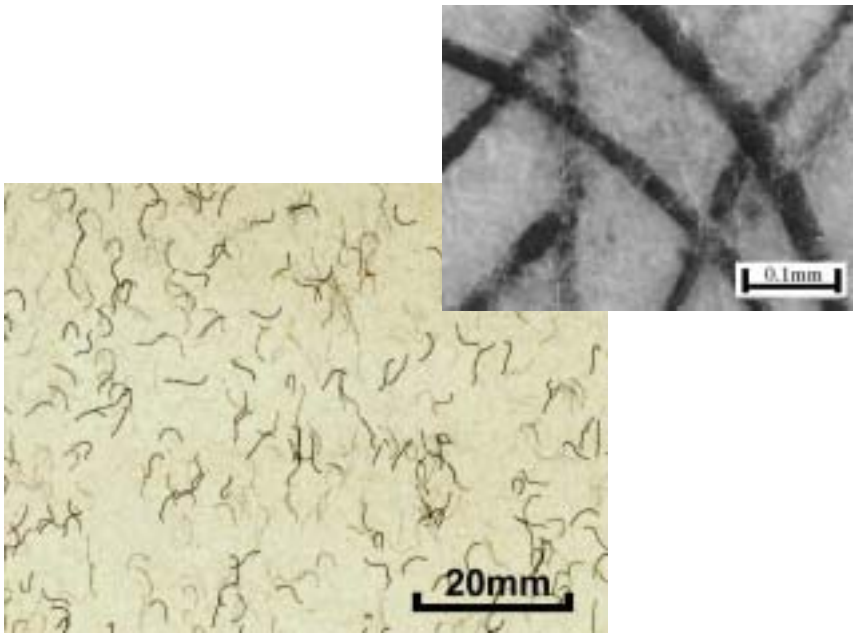

図 2.3 磁性材料を内包したファイバ

（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

磁気ストライプへの記録において、磁性ストライプ素材の特性や磁気ヘッドの書込み特性のばらつき、書込み時搬送速度の変動などの影響を受け、“ジッタ”と呼ばれる波形の歪が生じる（図 2.4 参照）。このジッタを固有パターンとして利用することによって、個々の磁気ストライプを検証するシステムが提案されている（Fernandez [1993]）。

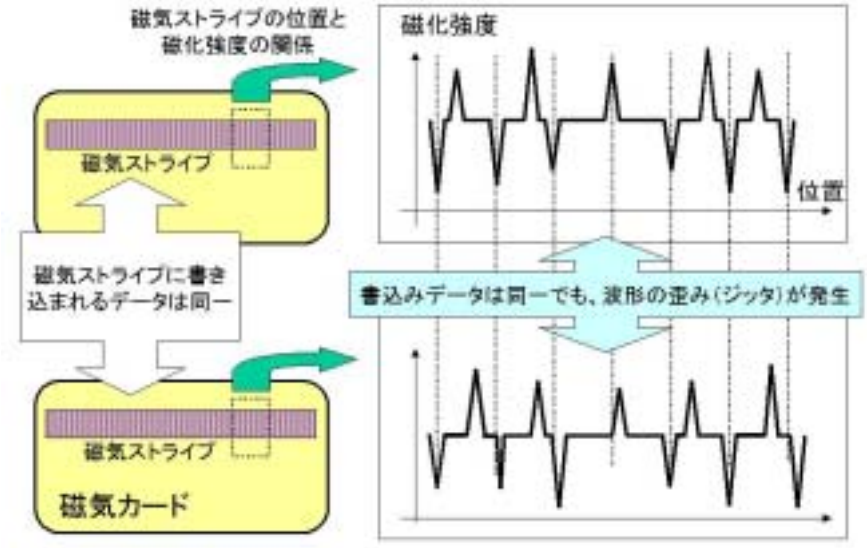

図 2.4 磁気ストライプにおけるジッタ（イメージ図）

（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

磁気ストライプ内の磁気粒子の微細な欠陥や不規則性から発生する磁気ノイズを固有パターンとして用いるシステムが提案されている（Inedk *et al.* [1995]）。また、磁気ストライプ内にランダムに配置される磁気ベクタから発生する磁気ノイズを固有パターンとして用いるシステムも提案されている（Hayosh [1998]）。

（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

半導体素子の半導体メモリ・セル内の捕獲電荷量がランダムに微妙な違いをもつことから、予め決められたデータを書き込んだ際の複数セルの電荷量を固有パターンとして利用するシステムが提案されている（Fernandez [1997]）。

（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

導電性ファイバを紙などの基材にランダムに分散させ、マイクロ波を発信してその反射波を固有パターンとして用いるシステムが提案された（Samyn [1989]）。

（ル）容器に貼ったシールを振動させたときの共振パターン

ロス・アラモス国立研究所（Los Alamos National Laboratory）で開発された非破壊評価技術 ARS（Acoustic Resonance Spectroscopy）は、容器と蓋の間に貼った“ intrinsic seal ”に振動を与えることで、その圧力分布から生じる振動を固有パターンとしてタンパー検知を行うシステムである（Olinger, Burr and Vnuk [1994], Sinha [1992], Sinha and Apt [1992]）。

このように、人工物メトリック・システムの提案事例では、人工物の検証に用いられる固有パターンとして、人工物固有の斑や、人工物内部に分散させた粒状物・薄片・ファイバなどによって生成されるデータが利用されている。こうした固有パターンは、人工物の正当な製造者であっても意図的に再現することは困難であるとみられている。

（４）人工物メトリック・システムの実用化事例－個別株券認証システム IOSAS

金融分野において既に実用化されている株券の人工物メトリック・システムの事例として IOSAS（イオサス：Inherence Of Stock Authentication System）を紹介する。なお、本論文の筆者のうち、松本弘之と菅原嗣高は、IOSAS の

開発に直接携わってきた。

IOSAS は、株券用紙の製造工程において原料に磁性ファイバを配合し、用紙内部に磁性ファイバをランダムに分散させ、個々の株券に固有でランダムな物理的特徴をもたせるというアイデアに基づいている。製造された株券用紙の内部で磁性ファイバが紙の繊維と絡み合い、複雑な 3 次元構造を構成するため、物理的特徴の固有パターンを再現することは困難とみられている（図 2.5 参照）。

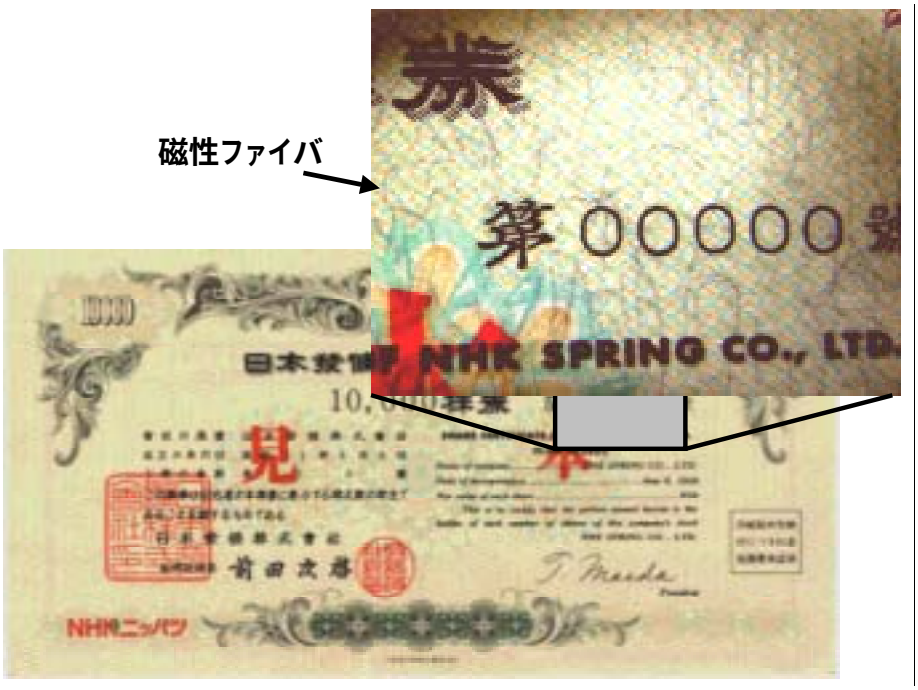

図 2.5　IOSAS **における株券（サンプル）の券面**

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る。株券の発行・照合装置（図 2.6 参照）は、OCR （optical character reader）によって個体識別番号を読み取ると同時に、株券の物理的特徴から固有パターンを抽出する。株券の発行フェーズでは、固有パターンは、参照データとして個体識別番号とともにパーソナル・コンピュータ上のデータベースに記録される。一方、株券は、株式名簿上の名義書換などに際して、企業の委託を受けて株券の管理を行う銀行に提出され、真贋判定が行われる。この場合、IOSAS の発行・照合装置は、読み取った個体識別番号をもとに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。このように、IOSAS は 1 対 1 照合を行う人工物メトリッ

ク・システムである。

図 2.6　IOSAS **の株券の発行・照合装置（外観）**

３．人工物メトリック・システム評価の現状と課題

２章で述べたように、物理的特徴を利用する人工物メトリック・システムでは、センサ入力における変動や固有パターン抽出における量子化誤差などに起因して、検証時に避けることのできない誤り率（誤受理率と誤拒否率）が存在する。人工物メトリック・システムでは、このような誤り率を低く抑えて人工物をより正確に認証する必要があり、認証精度の適切な評価が求められる。

本章では、まず、人工物メトリック・システムの主たる評価項目の中でセキュリティに着目した上で、セキュリティ特性の 1 つとして認証精度を位置づける。次に、人工物メトリック・システムにおける認証精度評価の現状を述べ、これまでに提案されている認証精度の指標を紹介する。最後に、人工物メトリック・システムの認証精度評価における今後の課題とその方策について述べる。

（1）人工物メトリック・システムの評価

人工物メトリック・システムを構築する際には、①セキュリティ、②利便性、③コスト、④社会的受容性の観点から評価することが必要である。そこで、以下では、これらの項目について、２章で紹介した IOSAS を例に挙げて評価を行う。なお、既に述べたように、本論文の筆者のうち、松本弘之と菅原嗣高は IOSAS の開発に携わっていることから、筆者らは、IOSAS を客観的に評価する立場にはない。しかし、IOSAS は人工物メトリック・システムの数少ない実用化事例であるため、具体的なイメージを描きやすくするために、その利点について、筆者らの考えを説明することとしたい。

①セキュリティ

情報システムをセキュリティの観点から評価する際には、詳しくは次節で説明するが、いくつかの特性に着目する必要がある。人工物メトリック・システムの場合、様々な攻撃の対象となることを前提とした上で、「人工物をいかに正確に認証することができるか」という“認証精度”の評価が重要であり、認証精度をセキュリティ特性の 1 つとして位置づけることができる。また、耐クローン性の評価は、クローンを用いた攻撃を前提とした認証精度評価と考えることができる。

IOSAS の場合、認証の対象となっているのは株券である。株券は市場で長期間流通することが想定されるため、採用する技術として、長期的に耐クローン性を確保できるものが望まれる。材料の入手・加工の困難さのみに依拠するシステムの場合、材料や加工における技術革新により、耐クローン性が低下する危険性も出てくる。IOSAS では、材料の加工の困難さだけでなく、

個体のランダムな物理的特徴を複製することの難しさを拠り所としており、攻撃者が発行・照合装置を利用できない場合、相異なるクローンを大量に作製することを困難にするように設計されている。

②利便性

利便性は、人工物メトリック・システムの使い勝手の良し悪しを意味する。いくらセキュリティ面で評価の高いシステムであっても、利用者の立場からみて使いにくいものであった場合、そのシステムは有用であるとはいえなくなってしまう。具体的には、操作方法の簡便さ、発行・検証時間の短さ、異なるメーカー間での人工物あるいは検証用機器の互換性といった点を評価することが必要である。

利便性の観点では、IOSAS は、株券の真贋判定を高速かつ自動的に実行可能にすることを通じて、株券の検証に必要な時間を短縮することができるという特徴をもつ。また、複数台の装置間で認証精度の互換性を確保し、遠隔地での装置の併用を実現している。さらに、株券が市場を流通している間に、発行時に固有パターンを抽出した物理的特徴が損傷することも想定される。そこで、発行・照合装置とは別に精査用装置を備えている。精査用装置は、発行・照合装置で照合する券面上の通常の走査領域以外に、複数の走査領域から固有パターンを抽出して照合し、より精密な真贋判定を行う装置である。

③コスト

人工物メトリック・システムの構築・運用などにかかるコストも評価することが必要である。

株券の認証の場合、株券の偽造品の鑑定を行うためには特殊な知識や技能が必要とされ、株券の鑑定は少数の専門家に限定されていた。このため、株券の鑑定には一定の時間が必要であったほか、少数の鑑定者に作業が集中する傾向にあり、鑑定者の負荷軽減や鑑定作業の効率化が課題とされていた。IOSAS を導入することによって、導入当初は専用の株券用紙の準備、発行・照合装置の設置といったコストが必要となるものの、真贋判定の自動化によって、鑑定者の負担軽減や判定ミスの低減を比較的小さなコストで達成することが可能となる。IOSAS の実用化には、こうしたコスト面でのメリットも貢献している。

④社会的受容性

社会的受容性の観点からは、人工物メトリック・システムの環境や人体への影響度や、社会への適用性（利用に際して違和感や抵抗感がないか）に関

しても評価することが必要である。具体的には、「人工物を廃棄した場合に自然環境に対して有害な物質が放出されないか」、「人工物を誤って飲み込んだときに人体に悪影響を及ぼすおそれがないか」、といった点について評価することが求められる。さらに、社会への適用性という点では、適用対象となるアプリケーションにおいて人工物メトリック・システムが違和感なく受け入れられるかについて評価することが必要である。例えば、「人工物の検証結果などの情報が、人工物の所持者のプライバシーを侵害するおそれはないか」といった評価が必要になる場合も考えられる。

株券の場合、企業の委託を受けて当該株券を発行・管理を行う信託銀行は、株券保有者からの信頼を維持するため、株券の偽造品を株券保有者へ還流させるようなことがあってはならない。さらに、偽造品の発覚時には、偽造品であることを十分な証拠をもとに第三者に対して証明可能であることが重要である。IOSAS は、個々の株券のランダムな物理的特徴から得られる固有パターンを利用することによって、確実な真贋判定を実現するとともに、「確実な真贋判定が行われたことを第三者に示すことが容易である」という意味で証拠性の確保にも役立つ。このように、株券を発行・管理する信託銀行にとっての信頼性や証拠性といった観点で、IOSAS は受け入れられやすい特性を有している。

なお、上記①～③の特性は、いずれかの特性を高めようとすると他の特性を損ねるといったように互いにトレードオフの関係にある。各特性に優先順位を付けた上で、それらのバランスをとりながらシステムを構築することが求められる。本論文では、これらの特性の中で、特にセキュリティに主眼をおいて議論を進める。

（2）人工物メトリック・システムのセキュリティ評価

人工物メトリック・システムを情報システムの 1 つとして捉えると、以下に示されるセキュリティ特性を満足する必要がある（ISO/IEC　[1996], 日本工業標準調査会 [2001]）。以下の定義の日本語訳は JIS TR 0036-1（日本工業標準調査会 [2001]）から引用したものである。

①機密性（confidentiality）

許可されていない個人、エンティティ、またはプロセスに対して情報を使用不可あるいは非開示にする特性

②完全性（integrity）

データ完全性とシステム完全性から構成される。

・データ完全性（data integrity）：許可されていない方法でデータが改ざんまたは破壊されていない特性
・システム完全性（system integrity）：システムが、意図的または偶発的な不正の操作から妨害されることなく、本来果たすべき機能を滞りなく実行する特性

③可用性（availability）
許可されたエンティティによって要求されたときにアクセスと使用が可能な特性

④責任追跡性（accountability）
あるエンティティの動作が、そのエンティティに対して一意に追跡できることを保証する特性

⑤真正性（authenticity）
対象またはリソースが要求されているものと同一であることを主張する特性。ユーザー、プロセス、システム、情報などのエンティティに対して適用される。

⑥信頼性（reliability）
矛盾のない計画どおりの動作および結果を確保する特性。

これらのセキュリティ特性を人工物メトリック・システムに当てはめると、次頁の表 3.1 のように整理することができる。同表に示すように、人工物メトリック・システムをセキュリティの観点から評価する場合、「真正性」に対応する“ 認証精度 ”が必須の特性であると考えられる[4]。一方、「真正性」以外の特性は、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い。

しかしながら、実際に認証精度の評価を行うにあたっては、「真正性」以外の特性にも配慮する必要がある。例えば、認証精度の設計値を高く設定しすぎて、人工物や読取センサの汚れや損傷、電気的なノイズの影響を受けやすかったり、装置間の互換性がとり難かったりといったように「可用性」や「信頼性」が低下する場合もある。こうした「真正性」と「可用性」・「信頼性」との間のトレードオフ関係に留意する必要がある。

さらに、これらのセキュリティ要件を満たしたとしても、例えば、人工物の寸法形状が扱い難いものであったり、装置の発行／照合時間が遅かったり、人

[4] 本論文では、認証精度をセキュリティの特性の 1 つとして位置づけている。ただし、バイオメトリクスの分野では、認証精度は、クローン作製などの攻撃を想定しない状況において議論されるケースが多く、セキュリティ特性として位置づけていない場合もある点に留意する必要がある。

工物や装置が高額であったりしたのでは、「利便性」や「コスト」の観点で難点が生じることになる。したがって、より実用的な人工物メトリック・システムを構築するためには、本章の冒頭に示した「利便性」や「コスト」の観点で許容される範囲において、可能な限り高い認証精度を実現することが必要である。

表 3.1 人工物メトリック・システムのセキュリティ特性

特性	人工物メトリック・システムにおいて対応する特性	説明
①機密性	システムにおいて取り扱われる情報やシステム仕様に関する情報などへのアクセス管理が適切に実行されること。	本特性をどの程度考慮するかはアプリケーションに依存する。また、人工物の検証結果に関する情報がその人工物の所持者の情報と結び付けられる可能性もあるため、プライバシー保護の観点からも考慮が必要な場合もある。
②完全性	人工物の発行・検証手続が不正に操作されることがないとともに、処理対象となるデータや処理結果のデータの改ざんが防止・検知されること。	人工物を含めたシステム全体の耐タンパー性を向上させるとともに、例えば、検証用装置を不正に改変された場合、それを検知して警報を発する仕組みを採用するなどの対策も重要である。
③可用性	利用者が、必要に応じて人工物の発行・検証の手続を実行可能であること。	人工物がある程度汚れたり損傷したりしても検証可能である、異なるメーカーの検証用装置が同一の認証精度を提供可能であるなどの特性が対応する。
④責任追跡性	システムの動作を、第三者がログなどによって後日確認することが可能であること。	人工物の発行者や検証者が「信頼できるエンティティ」である場合など、本特性を評価する必要がない場合もある。
⑤真正性	必要とされる認証精度によって、人工物の認証を実行可能であること。	本特性は、人工物メトリック・システムにおいて必須の特性である。
⑥信頼性	人工物メトリック・システムが設計・仕様どおりに機能し、故障しないこと。	可用性と近い概念であり、信頼性が失われた場合、可用性が失われる可能性が高い。ただし、信頼性が維持されていても可用性が失われるケースが考えられる（サービス妨害攻撃など）。

（3）一般的な人工物メトリック・システムの認証精度の評価

イ．認証精度評価の現状

２章で紹介した人工物メトリック・システムの提案事例の中で、認証精度の評価について述べられているものを取り上げ、その評価方法を以下に示す。

（イ）パターン類似度の統計的な分布による評価

容器に貼ったシールを振動させたときの共鳴パターンを利用して、容器の開封確認を行う人工物メトリック・システム ARS（Acoustic Resonance Spectroscopy）では、完全性が保たれている（剥がされていない）シールと剥がされたシールの固有パターンの照合における相関係数の統計的な分布の違いにより、システムの判別性能が評価された（Olinger, Burr and Vnuk [1994]）。

（ロ）試行回数と判定結果による評価

証書にランダムに分散させたファイバの画像を用いた人工物メトリック・システムでは、アルゴリズムの判別性能について検討が行われた。シミュレーション実験では、人工的に生成した画像を用いたパターン照合を行って、10,000 回の照合ですべて判別できたことが示されている。ここでは、ファイバの損傷／消失についての検討を行うとともに、50 枚の実際の紙片によってシミュレーションの有効性について確認も行っている（Brzakovic and Vujovic [1996]）。

（ハ）誤アラーム率／誤受理率による評価

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を利用する人工物メトリック・システムにおいては、誤アラーム率（false alarm rate）と誤受理率（false accept rate）という指標が定義され、その目標値が示されているほか、複数の読取装置を用いた評価結果が報告されている（Hayosh [1998]）。その中で、誤アラーム率は「本物が本物と認められなかった割合」と定義されているほか、その目標値に関して、「リトライなしで 1%未満となるように設定されるべきである」とされている。誤受理率については、「偽造品を誤って本物と認める割合」と定義され、目標値については「実用的には 1.0×10^{-4} 未満とすべきである」とされている。

（ニ）誤拒否率／誤受理率による評価

基材にランダムに分散した磁性ファイバの磁気パターンを用いた人工物メトリック・システムにおいては、バイオメトリック・システムの評価手法を応用し、誤拒否率（false rejection rate）と誤受理率（false acceptance rate）によってシステムの認証精度の評価結果が示されている（Matsumoto *et al.* [1997, 2001], Matsumoto, Suzuki and Matsumoto [1998]）。また、同研究では、実験により得られた認証精度の結果について、欧州中央銀行のレポートで紹介されている各種バイオメトリック・システムの誤り率の最

小値（1.0×10^{-3}）（ECBS [1996]）を認証精度の比較対象として援用し、評価を行っている。

認証精度の評価に関して評価結果や評価指標を公表している人工物メトリック・システムは少ないが、バイオメトリック・システムの認証精度の評価指標を適用する手法が一般的になりつつある。さらに、認証精度の基準値については、一部の文献で示されているものの、人工物メトリック・システムを設計する上で参考になる具体的な基準値は見当たらない。

ロ．バイオメトリック・システムの評価指標の適用

２章で述べたように、バイオメトリック・システムと人工物メトリック・システムはいずれも個体認証システムの一種だと考えることができる。そこで、バイオメトリック・システムの分野において検討が進められている認証精度の評価指標・表示方法を次のように定義し直して、人工物メトリック・システムにおける認証精度の評価指標・表示方法として利用することができる（図 3.1、図 3.2 参照）。

- **指標 1：誤受理率（**FAR; false acceptance rate**）**
  システムが拒否すべき人工物を誤って受理する確率

- **指標 2：誤一致率（**FMR; false match rate**）**[5]
  照合アルゴリズムが１回の照合において、不一致と判断すべき人工物を誤って一致と判定する確率

- **指標 3：誤拒否率（**FRR; false rejection rate**）**
  システムが受理すべき人工物を誤って拒否する確率

- **指標 4：誤不一致率（**FNMR; false non-match rate**）**[5]
  照合アルゴリズムが 1 回の照合において、一致と判断すべき人工物を誤って不一致と判定する確率。

[5] 人工物メトリック・システムでは、複数回の照合や複数のセンシングなどにより判定を行うシステムが存在するため、システムの総合的な認証精度の指標として誤受理率（FAR）・誤拒否率（FRR）を用い、照合アルゴリズムの認証精度の指標として誤一致率（FMR）・誤不一致率（FNMR）を用いることで、指標を区別している。ここでは、人工物メトリック・システムへ適用することを主眼として各種指標を定義しており、日本規格協会情報技術標準化研究センター（INSTAC）バイオメトリクス標準化調査研究委員会が精度評価方法の標準情報（TR: technical report）で定義している内容と若干異なっているので注意されたい（日本工業標準調査会 [2002a, 2002b]）。

• **指標 5：**ROC **曲線（**receiver operating characteristic curve**）**

認証精度の表示方法で、（誤受理率, 誤拒否率）または（誤一致率, 誤不一致率）を任意の判定しきい値についてプロットする表示方法（原点に近いほど精度が高い）

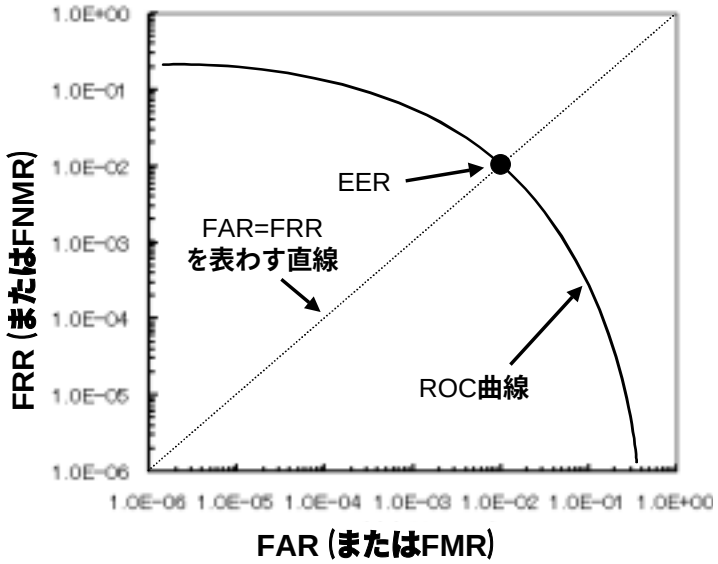

図 3.1 ROC **曲線と** EER**（縦・横軸は対数目盛）**

• **指標 6：**FAR（FMR）**曲線（**FAR or FMR curve**）**

認証精度の表示方法で、横軸に判定しきい値をとり、誤受理率または誤一致率を任意の判定しきい値についてプロットする表示方法

— これらの曲線は、試験的に照合アルゴリズムによる認証精度の概略の違いを比較するような場合、サンプル数が少ないと ROC 曲線が描き難いため、有用な表示方法である。

• **指標 7：**FRR（FNMR）**曲線（**FRR or FNMR curve**）**

認証精度の表示方法で、横軸に判定しきい値をとり、誤拒否率または誤不一致率を任意の判定しきい値についてプロットする表示方法

— これらの曲線は、試験的に照合アルゴリズムによる認証精度の概略の違いを比較するような場合、サンプル数が少ないと ROC 曲線が描き難いため、有用な表示方法である。

• **指標 8：等誤り率（**EER: equal error rate**）**

誤受理率と誤拒否率、または、誤一致率と誤不一致率が等しくなる場合

の誤り率

— バイオメトリック・システムにおいて判定しきい値を設定する際には、等誤り率に対応するしきい値を選択するケースが多く、等誤り率は、照合アルゴリズムを比較する場合に認証精度の代表的な指標として使われる。

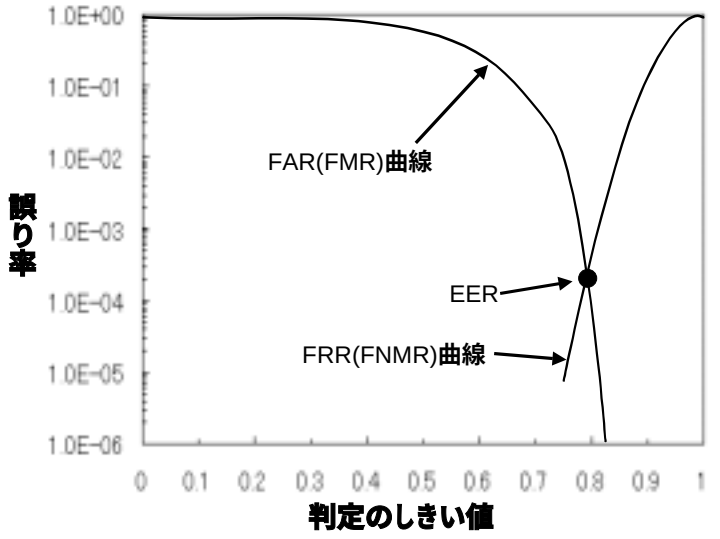

図 3.2 FAR **曲線と** FRR **曲線（**FMR **曲線と** FNMR **曲線）**

図 3.1 と図 3.2 のように、各種誤り率の曲線は通常対数目盛をとって表示される。

ハ．シミュレーションによる評価

認証精度の評価においては、シミュレーションを用いた評価も有用である。シミュレーションを用いた人工物メトリック・システムの評価に関する研究事例を以下に示す。

（イ）人工物のモデル化

ファイバを証書にランダムに分散させ、そのパターンの画像を用いた人工物メトリック・システムでは、擬似乱数を用いた生成器により生成した 10,000 枚の評価用のサンプル画像を用いて、照合アルゴリズムの評価が行われている（Brzakovic and Vujovic [1996]）。また、50 枚の実サンプル画像を用いて、その結果の検証も行われている。誤不一致率の評価は、評価サンプル画像の一部をランダムに欠損させることで評価が行われている。

（ロ）実サンプル走査時の統計的な誤差分布を利用

基材にランダムに分散した磁性ファイバの磁気パターンを用いた人工物メトリック・システムを対象に、シミュレータを併用して照合アルゴリズムの評価が行われている（Matsumoto and Matsumoto [2002]）。具体的には、実験で得た 1.0×10^3～4.0×10^3 個の固有パターンをシミュレータによって 7.4×10^4～2.9×10^5 個の評価サンプルに拡張し、それらのデータを用いて誤不一致率を計算・評価している。

（ハ）人工物およびセンサのモデル化

基材にランダムに分散した磁性ファイバの磁気パターンを用いた人工物メトリック・システムにおいて、磁性ファイバをモデル化し、その磁界分布を数値解析することによって、センシングにより得られる固有パターンをシミュレートした結果が報告されている（青柳・竹村・松本[2004]、Aoyagi, Matsumoto and Takemura [2004]）。シミュレーションによって得た誤一致率と誤不一致率を比較することによって、磁性ファイバの密度やセンサの走査位置による固有パターンの相違が認証精度に及ぼす影響を評価している。

一般に、人工物メトリック・システムでは、人工物の特性を調整したり、人工物の形状を規格化したりして認証精度の向上が図りやすく、各種の誤り率を低く抑えることが可能となる。認証精度の評価（特に、誤拒否率または誤不一致率の評価）を行う際には、被認証物が人工物であるため、バイオメトリック・システムに比べて評価サンプルを揃えやすく大規模な実験確認を行いやすい。しかし、大規模な実験確認を行うためには、大量の評価用サンプルや試行が必要となり、評価には相応のコストを要することになる。そこで、ここに挙げた評価事例に示されるように、特に、ハードウェアや照合アルゴリズムの調整段階においては、実際のサンプルによる評価に加えて、シミュレーションによる効率的な評価が有用である。

（4）人工物メトリック・システムの耐クローン性の評価

本論文ではセキュリティ特性の 1 つとして認証精度を位置づけているが、従来は、クローンの提示がない状態を前提とした認証精度評価が一般的であり、「認証精度をセキュリティ特性の 1 つと位置づける」という考え方に基づいた評価の結果はほとんど公表されていなかった。このため、公表されているものをみる限り、認証精度評価としては偏ったものが多かった。しかし、最近では、以下で紹介するように、クローンの提示を想定した認証精度評価を行う上で有用な指標が提案されている。

イ．ブルートフォース攻撃に対する評価

「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・システムの認証をパスしようとする攻撃」はブルートフォース攻撃と呼ばれる。本攻撃は、必ずしもクローンの作製を行うものではないが、実行に際して専門的な知識や技能を必要とせず実行が容易であるため、その攻撃成功率は耐クローン性を評価する際の基本的な指標である。ブルートフォース攻撃成功率は、認証精度評価において得られる誤受理率（FAR）を用いて、攻撃試行回数から攻撃成功率を推定することができる（Matsumoto *et al.* [2001] 5章参照）。

・指標 9：ブルートフォース攻撃成功率（success rate of brute force attacks**）**

攻撃者が、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試行において、提示したものをシステムに受理させる確率（図 3.3 参照）

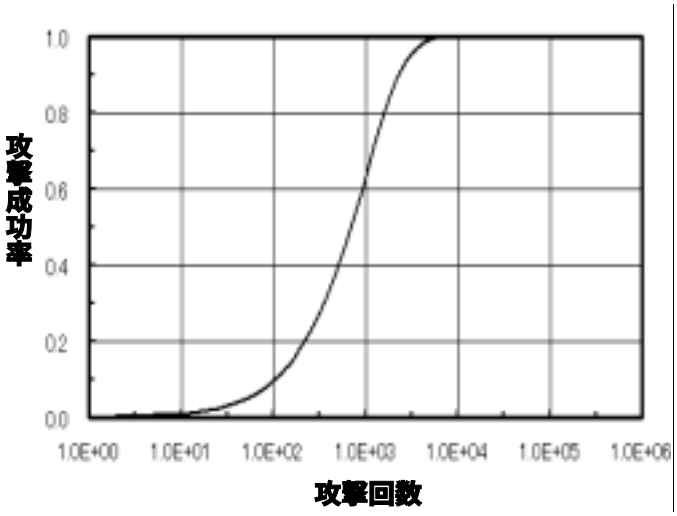

図 3.3 攻撃回数と攻撃成功率

ブルートフォース攻撃に限らず、攻撃者の攻撃試行における成功率を示す指標は、照合アルゴリズムにおける判定のしきい値設定や認証における拒否判定の連続許容回数を設定する際の目安となる。

ロ．デッドコピー攻撃に対する評価

「本物を見本にして物理的特徴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・システムの認証をパスしようとする攻撃」はデッドコピー攻撃と呼ばれる。クローンに対する安全性の評価指標としてクローン一致率

（CMR; clone match rate）が提案されており、①照合アルゴリズムのパラメータによってクローン一致率が変化する、②クローンの提示がない状態で測定された認証精度からクローン一致率の高低を推定することは困難である、といった結果が得られている（Matsumoto and Matsumoto [2003] 5 章参照）。クローンに対する安全性は、人工物メトリック・システムにおける主要な基本性能の 1 つであり、次のような指標に基づいた評価が重要である（図 3.4 参照）。

・**指標 10：クローン受理率（**CAR; clone acceptance rate**）**[6]
　システムが拒否すべきクローンを誤って受理する確率

・**指標 11：クローン一致率（**CMR; clone match rate**）**
　照合アルゴリズムが 1 回の照合において、不一致と判断すべきクローンを誤って一致と判定する確率

・**指標 12：**CAR（CMR）**曲線（**CAR or CMR curve**）**
　クローンに対する認証精度の表示方法で、横軸に判定しきい値をとり、クローン受理率またはクローン一致率をプロットする表示方法

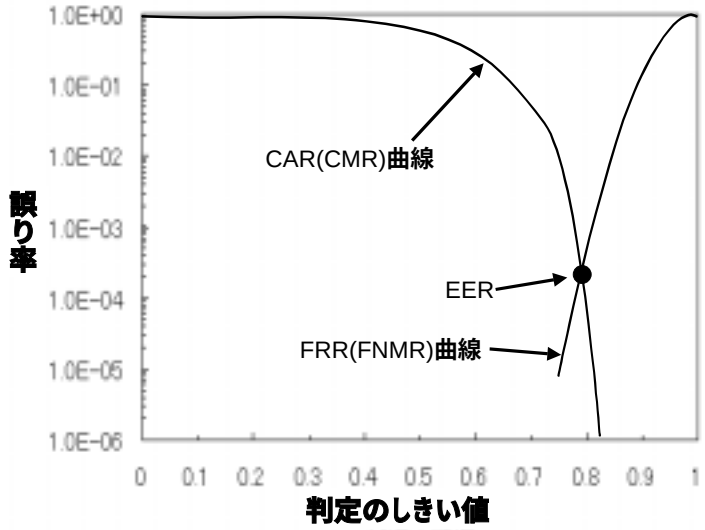

図 3.4 CAR **曲線と** FRR **曲線（**CMR **曲線と** FNMR **曲線）**

クローンの提示を想定するケースにおいては、誤受理率（あるいは誤一致

[6] 一般的な誤受理率（FAR; false acceptance rate）とクローンに対するシステムの受理率を区別するための用語として定義する。

率）の代わりにクローン受理率（あるいはクローン一致率）に着目し、クローン受理率（あるいはクローン一致率）と誤拒否率（あるいは誤不一致率）が等しくなる場合の等誤り率を評価の指標とすることが適当と考えられる。

（5）バイオメトリック・システムの認証精度の評価

バイオメトリック・システムでは、様々な理論的な検討が進められてきた（Jain, Bolle and Pankanti [1999]）ものの、クローンの提示がない状態を想定しての認証精度の測定が一般的であった。

しかしながら、例えば、指紋照合システムにおいて、登録者以外の攻撃者が自らの生体指や攻撃協力者の生体指を（ID の提示が必要なシステムであれば ID とともに組み合わせて）無作為に提示し、認証をパスしようとするといったブルートフォース攻撃が考えられる。このような攻撃を想定し、攻撃者が登録者の指紋や ID についてどの程度の知識を有しているかを仮定した上で、その攻撃成功率を事前に推定してその対策を検討しておく必要がある。したがって、バイオメトリック・システムにおいても、攻撃者の知識や能力を想定したブルートフォース攻撃成功率の評価は重要だといえる。

さらに、例えば、指紋照合システムに対して、登録者の生体指を見本にして指紋を複製したクローン（人工指）を提示することで、システムの認証をパスしようとする攻撃（デッドコピー攻撃）が考えられる。このようなデッドコピー攻撃についての評価事例として、生体指や残留指紋から複製したゼラチン製の人工指を市販の指紋照合装置に提示すると、かなり高い確率で受け入れられることが報告されている（山田・松本・松本 [2000a, 2000b, 2001]、Matsumoto *et al.* [2002]、星野ほか [2002]）。また、唾液をつけたシリコーンゴム製の人工指が市販の指紋照合装置に受け入れられる事実も報告されている（Putte and Keuning [2001]）。さらに、虹彩（アイリス）を用いた認証装置については、登録装置画面の表示画像から複製した人工虹彩が受け入れられることが報告されている（松本・平林 [2003a, 2003b]、松本・平林・佐藤 [2004]）。これらの報告を契機に、バイオメトリック・システムの分野でも、耐クローン性の評価の重要性が認知され始めている（三村ほか [2003]、Valencia [2003]、Maltoni [2003]）。

このように、バイオメトリック・システムについて、学会などのオープンな場においてクローンへの耐性などに関して議論されるようになったのは、人工物メトリック・システムと同様に最近のことである。バイオメトリック・システムの評価においても、クローンの存在を前提とした認証精度の評価を行う場合には、ブルートフォース攻撃成功率、クローン受理率またはクローン一致率が有用な指標になると考える。

また、一般的に、認証精度の評価に際して大量の被験者（生体評価サンプル）

を集めにくいバイオメトリック・システムにおいても、人工物メトリック・システムと同様に、シミュレーションによる評価やシミュレーションを併用する認証精度の評価手法は有用である。

（６）人工物メトリック・システムの認証精度評価における課題と方策

バイオメトリック・システムと対比させつつ、人工物メトリック・システムの認証精度評価の現状を図式的に示すと図 3.5 のようになる。

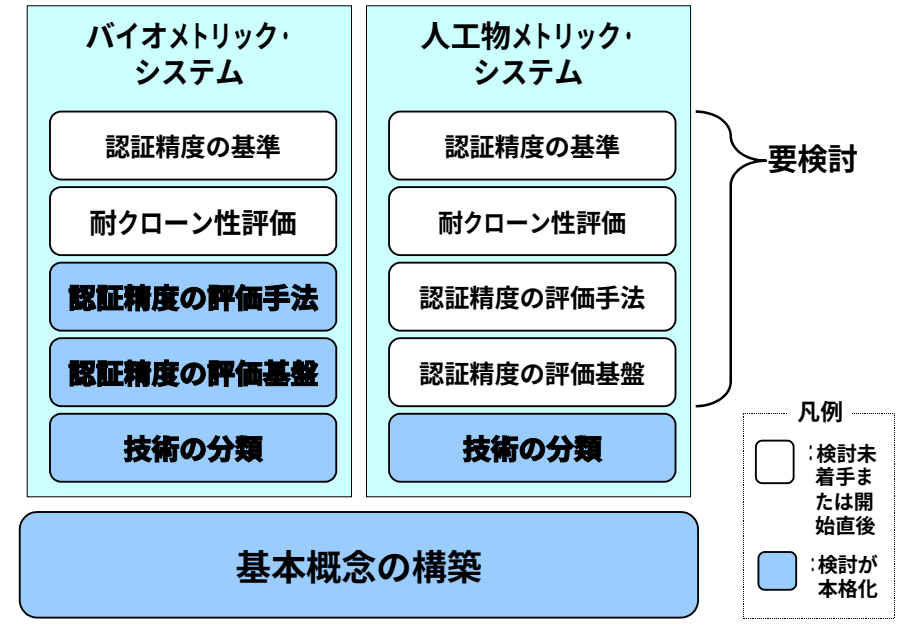

図 3.5 人工物メトリック・システムの認証精度評価の現状

図 3.5 からわかるように、人工物メトリック・システムの評価は、理論的な評価の枠組みや定量的な評価手法の検討が開始されて間もない段階にあり、認証精度の評価については、①認証精度の評価基盤の構築、②認証精度の評価手法の構築、③耐クローン性の評価手法の構築、④認証精度の基準値設定、という 4 つの課題が挙げられる。以下、課題ごとにその方策を述べる。

イ．認証精度の評価基盤の構築

人工物メトリック・システムにおける認証精度の評価を適切に行うためには、システムに対する様々な攻撃を想定しておく必要がある。具体的には、クローンの提示だけでなく、人工物の発行者や検証者による不正行為、検証用装置の不正操作など、情報システム一般において想定される攻撃も考慮し

ておく必要がある。情報システム一般のセキュリティ評価の基盤としては、ISO/IEC 15408（ISO/IEC [1999a, 1999b, 1999c]）や ISO/IEC 17799（ISO/IEC [2000]）などの国際標準が制定されており、これらに基づいた第三者機関による評価も行われている。人工物メトリック・システムにおいて認証精度を評価する際には、これらの国際標準を活用することが可能であると考えられる。

ただし、ISO/IEC 15408 や ISO/IEC 17799 は情報システム一般を対象として用語・概念を規定しているため、人工物メトリック・システムに適用するためには、今後、人工物メトリック・システムに固有の用語・概念や評価手法を確立し、標準化することが必要である。こうした点に関して、バイオメトリック・システムでは、既に、日本規格協会（JSA）情報技術標準化研究センター（INSTAC）によって、バイオメトリクス認証システムの精度評価方法に関する標準情報（TR: Technical Report）が策定されているほか（日本工業標準調査会 [2002a, 2002b]）、ISO/IEC JTC1/SC37 では、認証装置の運用要求仕様、バイオメトリクスに関する用語、センサ精度評価手順などの国際標準化作業が進められている。

このように、バイオメトリック・システムにおける標準作業が進んでいる状況を踏まえると、人工物メトリック・システムの認証精度の評価基盤は、バイオメトリック・システム評価の標準化を参考にしながら構築していくことになるであろう。

ロ．認証精度の評価手法の構築

各種人工物メトリック・システムの研究や評価結果に関して、学会などのオープンの場で公表するなどして、さらなる理論構築や評価技術の発展を図ることが求められる。また、シミュレーションによる評価手法は、人工物メトリック・システムで利用している物理的特徴や照合アルゴリズムに依存する部分が多く、必然的に各システムにより多様になると考えられる。したがって、シミュレーションを用いた認証精度の評価などにおいては、第三者が追試できるように、評価サンプルの生成方法や生成手順、評価におけるサンプル数や試行回数など実験の条件を明示した上で、①共通の指標に基づいて認証精度の評価結果を示すとともに、②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ことが必要である。

ハ．耐クローン性の評価手法の構築

前項に述べたように、耐クローン性に関する評価については、バイオメトリック・システムにおいてもようやく認知され始めた状況にあり、今後十分

な議論と研究を進めた上で評価手法の標準化に取り組む必要がある。

クローンの作製方法や手順は多岐にわたると考えられるため、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は、想定される作製方法によって実際にクローンを作製し、そのクローンに対する認証精度を評価することが望ましい。ここで、クローンの作製方法は、人工物メトリック・システムで利用している物理的特徴や人工物の加工方法に依存する部分が多く、必然的に各システムにより多様になると考えられる。

したがって、耐クローン性の評価においては、第三者が追試可能なように、クローンの作製方法や作製手順、評価におけるサンプル数や試行回数など実験の条件を明示した上で、クローン受理率やクローン一致率など共通の指標に基づいて認証精度の評価結果を示す必要がある。また、評価結果を学会などのオープンの場で公表するなどして、バイオメトリック・システムも含めて評価手法に関する議論や研究を活性化させることが耐クローン性評価技術の発展につながると考えられる。

ニ．認証精度の基準値設定

人工物メトリック・システムの設計者にとっては設計目標を検討する上で、また、人工物メトリック・システムの利用者にとっては各社システムの比較や選定を行う上で、参考となる認証精度の基準値が示されることが望ましい。

バイオメトリック・システムに関しての認証精度の基準値としては、1992年に、英国の決済サービス協会（APACS: Association for Payment Clearing Services）が策定したバイオメトリック手法に対する基準（European Committee for Banking Standards [1996]）がある。同基準では、「誤拒否率（FRR）： 1 in 100,000 or 0.001%、誤受理率（FAR）： 1 in 20 or 5.00%」とされているが、耐クローン性の評価も加味した上で見直しを行う必要があると考えられる。こうした認証における誤り率の基準値が人工物メトリック・システムにおいても検討されることが今後求められる。

本章では、人工物メトリック・システムに関して、耐クローン性の評価も含めた認証精度評価に関連する用語とその定義を述べた。その内容は、表 3.2 のとおりである。

表 3.2 人工物メトリック・システムの認証精度評価に関連する用語

分類	用語	定義
クローンの提示を想定しない場合の認証精度の指標	＜指標 1＞誤受理率（FAR; false acceptance rate）	システムが拒否すべき人工物を誤って受理する確率
	＜指標 2＞誤一致率（FMR; false match rate）	照合アルゴリズムが 1 回の照合において、不一致と判断すべき人工物を誤って一致と判定する確率
	＜指標 3＞誤拒否率（FRR; false rejection rate）	システムが受理すべき人工物を誤って拒否する確率
	＜指標 4＞誤不一致率（FNMR; false non-match rate）	照合アルゴリズムが 1 回の照合において、一致と判断すべき人工物を誤って不一致と判定する確率
認証精度の表示	＜指標 5＞ROC 曲線（receiver operating characteristic curve）	認証精度の表示方法で、（誤受理率, 誤拒否率）または（誤一致率, 誤不一致率）を任意の判定しきい値についてプロットする表示方法
	＜指標 6＞FAR（FMR）曲線（FAR or FMR curve）	認証精度の表示方法で、横軸に判定しきい値をとり、誤受理率または誤一致率を任意の判定しきい値についてプロットする表示方法
	＜指標 7＞FRR（FNMR）曲線（FRR or FNMR curve）	認証精度の表示方法で、横軸に判定しきい値をとり、誤拒否率または誤不一致率を任意の判定しきい値についてプロットする表示方法
	＜指標 8＞CAR（CMR）曲線（CAR or CMR curve）	クローンに対する認証精度の表示方法で、横軸に判定しきい値をとり、クローン受理率またはクローン一致率を任意の判定しきい値についてプロットする表示方法
	＜指標 9＞等誤り率（EER: equal error rate）	誤受理率と誤拒否率または誤一致率と誤不一致率が等しくなる場合の誤り率、または、クローン受理率と誤拒否率またはクローン一致率と誤不一致率が等しくなる場合の誤り率
クローンの提示を想定する場合の認証精度の指標	＜指標 10＞ブルートフォース攻撃成功率（success rate of brute force attacks）	攻撃者が、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試行において、提示したものをシステムに受理させる確率
	＜指標 11＞クローン受理率（CAR; clone acceptance rate）	システムが拒否すべきクローンを誤って受理する確率
	＜指標 12＞クローン一致率（CMR; clone match rate）	照合アルゴリズムが 1 回の照合において、不一致と判断すべきクローンを誤って一致と判定する確率

４．セキュリティ評価の枠組み

３章では、人工物メトリック・システムにおける認証精度評価の現状と今後の課題を提示した。その中で、今後の課題の 1 つとして「認証精度の評価基盤の構築」を挙げ、評価基盤として ISO/IEC 15408 などを活用することが可能であると説明した。ただし、ISO/IEC15408 に基づく評価を行う場合にせよ、利用者が独自の評価を行う場合にせよ、認証精度の評価を行う前に、人工物メトリック・システムを適用するアプリケーションのセキュリティ・ポリシーを定めた上で、そのシステムに対してどのような攻撃がどのような環境の下で行われることを想定するかをまず検討する必要がある（セキュリティ評価の枠組みの検討)。そうした検討の結果を踏まえ、どのようなセキュリティ要件を設定する必要があるかを吟味しなければならない。こうした検討の結果が、ISO/IEC 15408 の枠組みでは、セキュリティ要件仕様書（protection profile）としてまとめられ、第三者によるセキュリティ評価において重要な情報となる。

本章では、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して、最低限考慮すべき攻撃方法やセキュリティ要件について検討を行う。

（1）検討対象

本章においても、物理的特徴を利用した人工物メトリック・システムを想定し、検討の対象とする。ただし、具体的な人工物メトリック・システムを前提とするわけではなく、抽象的なシステムを想定する。

（2）攻撃の目的

人工物メトリック・システムのセキュリティ評価を行うためには、まず、攻撃者がどのような目的で攻撃を仕掛けるかを定める必要がある。攻撃者が人工物メトリック・システムを攻撃の標的とする場合、①クローンを利用した不正行為、②人工物メトリック・システムのサービス妨害、という 2 種類の攻撃が想定される。

これらのうち、上記①の攻撃が最も基本的なものであり、人工物メトリック・システムにおいて最初に対策が講じられるべき攻撃である。そこで、「検証者に検知されることなく検証に成功するようにクローンを作製する」という攻撃を検討対象とする。

（3）想定環境

イ．エンティティ

人工物メトリック・システムを構成するエンティティとして、発行者、検

証者、利用者を想定する。これらのエンティティによって構成される人工物メトリック・システムには、様々な実現形態が想定される。そうした中から、ここでは、一般的な実現形態として次のような役割・性格をもつ発行者と検証者を想定する（図 4.1 参照）。

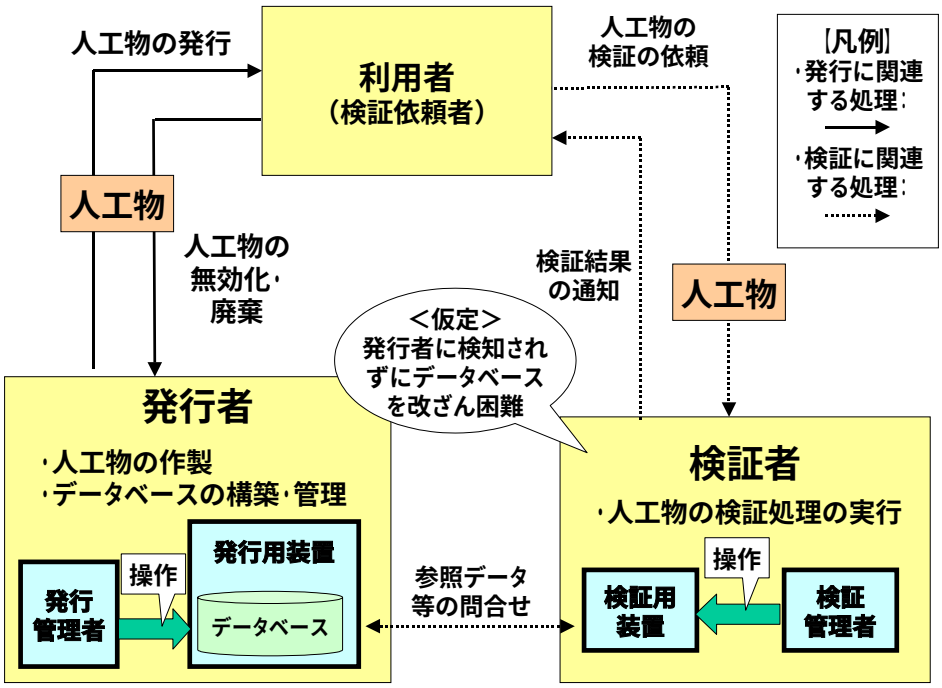

図 4.1　各エンティティの役割

（イ）発行者

発行者は、人工物を作製・発行し、利用者に提供するエンティティである。また、発行した人工物の有効期限が切れた場合などには、その人工物を無効化・廃棄する。検証時に参照データなどを格納したデータベースが利用される場合においては、発行者がデータベースを構築・管理する。

発行者は、人工物を作製・発行・無効化・廃棄する「発行用装置」（機械・システム）と、発行用装置を管理・操作する「発行管理者」（人間）から構成される。データベースは発行用装置の一部とする。

（ロ）検証者

検証者は、人工物を検証するエンティティである。検証時における人工物の固有パターン（人工物の物理的特徴を表わす検証用のデータ）の読取りは機械（検証用装置と呼ぶ）によって行われる。また、検証用装置の操

作・管理は「検証管理者」（人間）によって行われる。このように、検証者は、検証用装置と検証管理者から構成される。

検証用装置は、図 2.1 で示したように、センサ入力部、固有パターン抽出部、判定出力部から構成される。これらの要素は近接して設置される場合のほか、それぞれ異なる場所に設置される場合も考えられる。例えば、各要素が異なる場所に設置される場合として、判定出力部が 1 か所のセンターに設置される一方、センサ入力部と固有パターン抽出部は分散して設置され、固有パターンなどのデータをネットワーク経由でセンターに送信して検証を行う、という実現形態が考えられる。

データベースに格納された参照データなどを検証時に利用するタイプの検証手続の場合には、検証者は発行者に対して参照データの送信を必要に応じて要求・取得する仕組みとする。ただし、検証者は、データベースからデータを入手することができるものの、発行者に検知されることなくデータベースのデータを改ざんすることは困難とする。

ロ．検証手続の種類

図 2.1 をベースに人工物の検証手続の種類としてどのようなものが想定されるかを整理する。代表的なものとして、①人工物記録型 1 対 1 検証、②データベース記録型 1 対 1 検証、③データベース記録型 1 対 N 検証、の 3 つが挙げられる。

（イ）人工物記録型 1 対 1 検証

本検証手続は、検証対象の人工物から固有パターンを読み出すとともに、人工物あるいはそれが埋込・貼付される物品から参照データを読み出し、固有パターンと参照データの整合性を検証するという方式である（次頁の図 4.2 参照）。本検証手続では、発行者がデータベースに参照データを格納する必要がないという特徴がある。

人工物の発行時には、人工物から固有パターンを抽出し参照データを生成した上で、何らかの手段で人工物に参照データを記録する、あるいは、人工物が埋込・貼付された物品に参照データを記録するという処理が行われる。

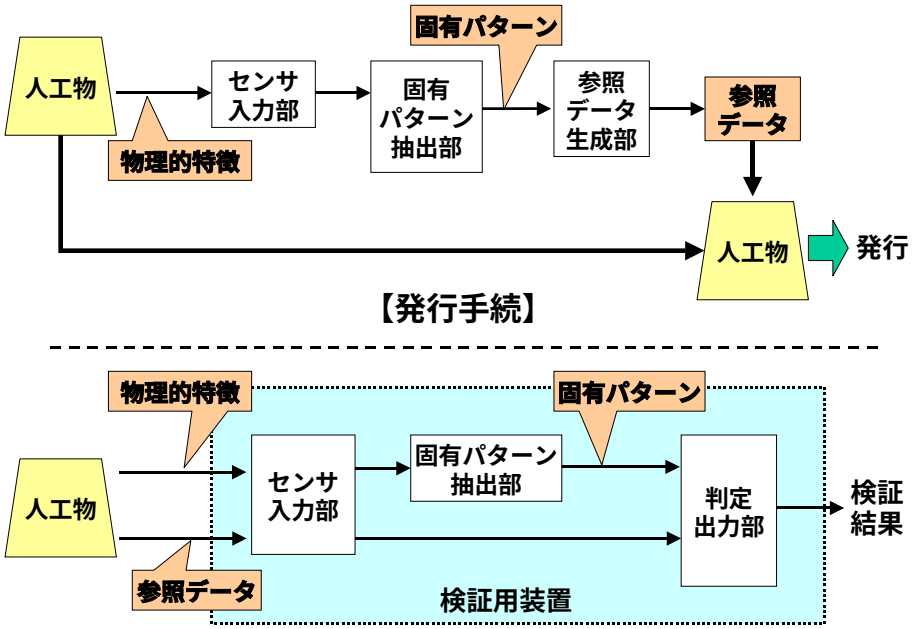

図 4.2　人工物記録型 1 対 1 検証

（ロ）データベース記録型 1 対 1 検証

本検証手続は、人工物の発行時に各人工物の ID（識別データ）と参照データをペアにしてデータベースに格納しておき、検証対象となった人工物あるいはそれが埋込・貼付された物品から ID を抽出した上で、その ID に対応する参照データをデータベースから検索・出力し、人工物から抽出した固有パターンとの整合性を検証するという方式である（次頁の図 4.3 参照）。ここで、ID を「人工物に付与されるシリアル番号であり、各人工物に対応する参照データとともに管理されるデータ」と定義する。検証時には、検証者が発行者のデータベースに検証対象の人工物の ID を送信し、その ID に対応する参照データを発行者から返信してもらう。

人工物を発行する際の処理の手順は次のとおりとする。

① 人工物から固有パターンを抽出する（センサ入力部、固有パターン抽出部）。
② 固有パターンから参照データを生成する（参照データ生成部）。
③ 人工物の ID を生成する（ID 生成部）。
④ ID と参照データをペアにしてデータベースに格納する。
⑤ 何らかの手段で人工物に ID を書き込む、あるいは、人工物が埋込・貼付された物品に ID を書き込む。

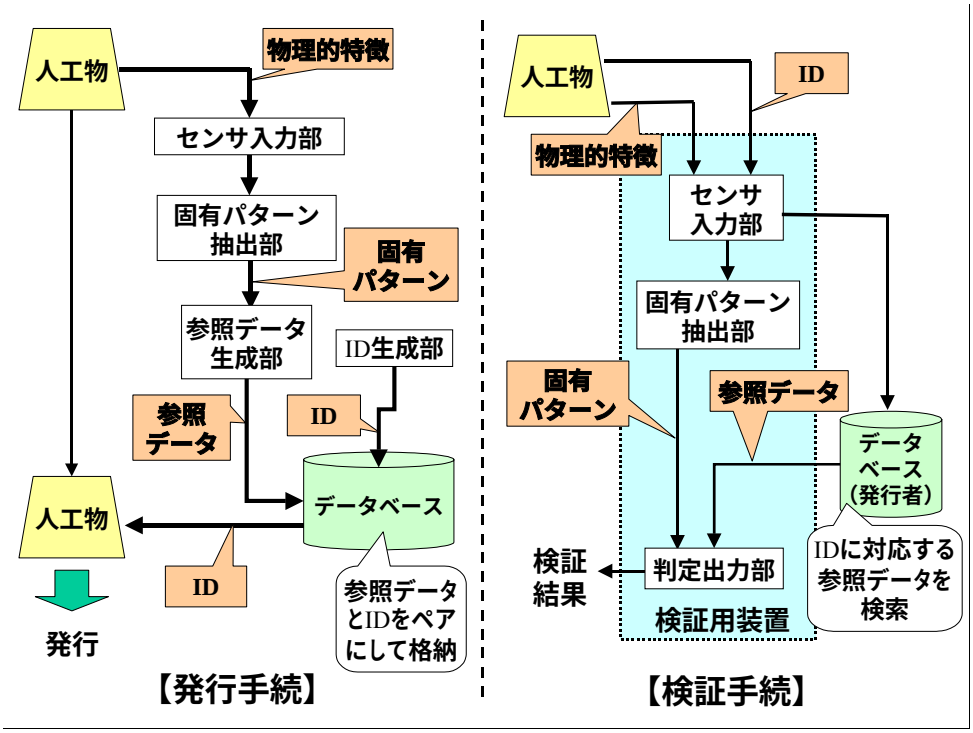

図 4.3 データベース記録型 1 対 1 検証

（ハ）データベース記録型 1 対 N 検証

本検証手続は、人工物の発行時に各人工物の参照データをデータベースに格納しておき、検証対象となった人工物から固有パターンを読み出し、その固有パターンと整合的な参照データをデータベースにおいて検索するという方式である（次頁の図 4.4 参照）。検証対象となった人工物の固有パターンと整合的な参照データがデータベースに記録されていた場合、その人工物の識別データなどが検証結果として出力される。本検証手続では、他の手続とは異なり、人工物の検証時に検証者に対して参照データや ID を提供する必要がないという特徴がある。

人工物を発行する手順は、①人工物を作製して参照データを抽出する（センサ入力部、固有パターン抽出部、参照データ生成部）、②参照データをデータベースに格納する、③人工物を発行する、となる。

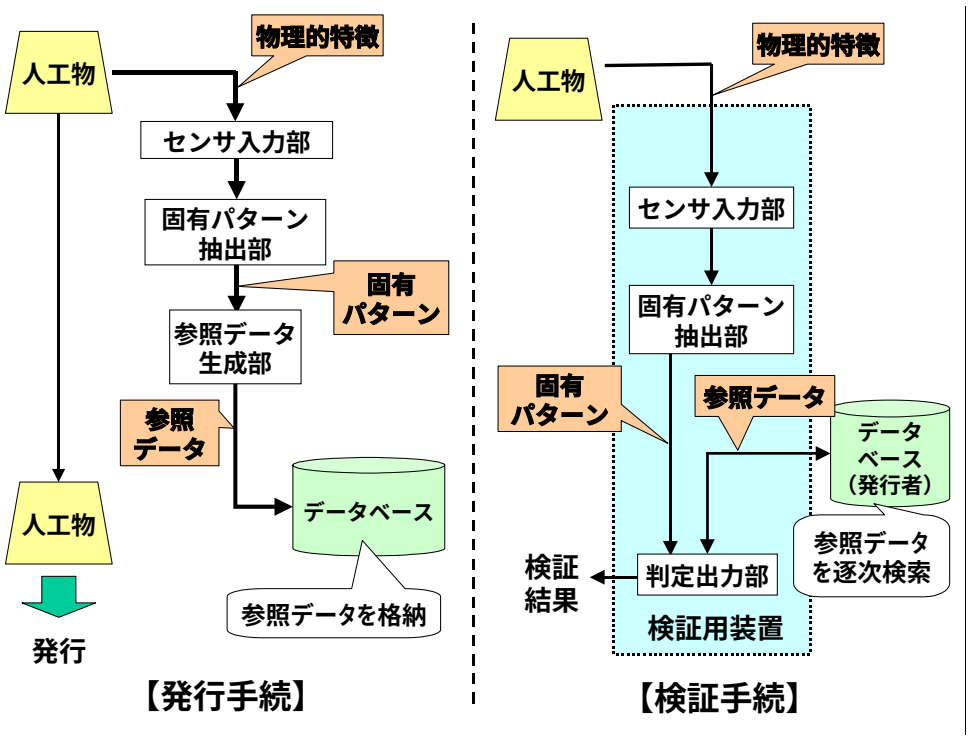

図 4.4 データベース記録型 1 対 N 検証

ハ．交信データのセキュリティ特性

人工物の発行・検証時において各要素（センサ入力部、固有パターン抽出部、判定出力部、データベース）間で交信されるデータに関しては、第三者に対して守秘性が確保されるほか、通信相手やデータの一貫性の確認が確実に実行され、その証跡がログとして残されると仮定する。

ニ．攻撃者の能力

攻撃者が利用可能な情報の観点から、攻撃者の能力を次のように想定する。

①発行者との結託可能性

攻撃者は、発行者と結託する場合と結託しない場合がある。結託する場合としては、発行管理者が不正を行う状況を想定する。ただし、発行管理者が積極的に攻撃者に協力する場合だけではなく、発行管理者が攻撃者に脅迫されて不正を行う場合や、発行管理者自らが自発的に攻撃者となる場合（内部犯行のケース）も含む。発行者との結託によって、攻撃者は次の不正が可能となる。

- データベースに登録されているデータを、第三者に検知されることなく覗き見・改ざんすることができる。ただし、人工物の参照データを

生成する際に秘密のデータが用いられる場合（例えば、デジタル署名生成用の秘密鍵）、そのデータを入手することは不可能である（すなわち、発行者と同様の手順によって人工物の参照データを生成することは困難）。

- 攻撃者が選択した人工物を発行処理させることが可能である。

また、攻撃者は、発行者と結託することなく、発行用装置を不正に操作することは困難とする。

②検証者との結託可能性

攻撃者は、検証者と結託する場合と結託しない場合がある。結託する場合として、検証管理者が不正を行う状況を想定する。発行者との結託と同様に、検証管理者が検証者から脅迫されて不正を行う場合や、自ら攻撃者となって不正を行う場合も含まれる。攻撃者は、検証者との結託によって、検証用装置を不正に操作可能となる。

― 例えば、①判定出力部の真偽判定方法におけるしきい値を不正に操作する、②判定出力部の入力（参照データなど）を正規の人工物のものに置き換える、③検証に用いられるデータベースを覗き見するといった不正が可能になると想定する。

ただし、攻撃者が検証者と結託する場合でも、発行者と結託しない限り、データベースのデータを第三者に検知されることなく改ざんすることは困難とする。

③情報の入手可能性

攻撃者がどのような情報を入手するかに関しては、まず、攻撃者は人工物を作製する方法を知っているとする。

第二に、攻撃者は、検証手続情報を知らない場合と知っている場合がある。検証手続情報とは、人工物の物理的特徴のセンサ読取方法、固有パターン抽出方法、参照データ生成方法、判定方法を指す。攻撃者が発行者や検証者と結託する場合、攻撃者はこうした検証手続情報を入手する。ただし、これらの検証手続を実行する上で第三者に対して秘密とされるデータが存在する場合、安全性上の欠陥が存在するケースを除き、攻撃者がそれらのデータを知ることは困難である。

― 既存の人工物メトリック・システムでは、人工物の作製方法や検証方法を一般に公開しないケースが多い。しかし、検証用装置が攻撃者によって解析された場合、検証手続に関する情報が攻撃者の手にわたる可能性がある。こうした可能性を考慮し、上記の場合分けを行う。

第三に、攻撃者は、発行者によって正規に発行された人工物をいくつか入手する。ただし、入手した正当な人工物からそれらの固有パターンや参照データを入手するか否かは、攻撃者が検証手続情報を入手しているか否かに依存することとする。

（4）攻撃の条件と効果

イ．5 種類の攻撃条件

攻撃者が攻撃を行う際の環境を以下では「攻撃条件」と呼ぶ。**（3）**の整理に基づき、検証者との結託の有無、発行者との結託の有無、検証手続情報の入手の有無、の 3 つの観点から攻撃条件を整理すると、表 4.1 のとおり 5 つに分類される。

表 4.1 **攻撃条件の分類**

攻撃条件	検証者との結託	発行者との結託	検証手続情報
攻撃条件 1	結託しない	結託しない	入手しない
攻撃条件 2			入手する
攻撃条件 3		結託する	入手する
攻撃条件 4	結託する	結託しない	入手する
攻撃条件 5		結託する	

攻撃者が検証者と結託しない場合、発行者との結託の有無によって 2 通り、検証手続情報の入手の有無によって 2 通りが想定される。攻撃者が発行者と結託しない場合、検証手続情報を入手しないケース（攻撃条件 1 と呼ぶ）と検証手続情報の一部または全部を入手するケース（攻撃条件 2 と呼ぶ）が想定される。攻撃者が発行者と結託する場合には、攻撃者は検証手続情報も入手するケース（攻撃条件 3 と呼ぶ）のみが想定される。また、攻撃者が検証者と結託する場合には、攻撃者が発行者と結託しないケース（攻撃条件 4 と呼ぶ）と結託するケース（攻撃条件 5 と呼ぶ）が想定されるが、これらの攻撃条件の下では、攻撃者は検証手続情報を入手する。

攻撃条件を比較すると、攻撃条件 5 が攻撃者にとって最も有利な状況であり、攻撃条件 1 が最も不利な状況である。ただし、攻撃条件 1 は攻撃実行の条件が最も緩く、攻撃条件 1 の下での攻撃は最も容易に実行可能であると考

えることができる。また、その他の攻撃条件をみると、「攻撃条件 1→攻撃条件 2→攻撃条件 4→攻撃条件 5」の順番で、また、「攻撃条件 1→攻撃条件 2→攻撃条件 3→攻撃条件 5」の順番で、攻撃者にとって有利な状況となっている。攻撃条件 3 と攻撃条件 4 を直接比較することはできない。

こうした関係を実際の人工物メトリック・システムにおけるセキュリティ評価に適用する際には、そのシステムの特性やアプリケーションの形態を十分に考慮する必要がある。例えば、攻撃条件 3 と攻撃条件 4 のどちらが攻撃者に有利な状況であるかは、実際のシステムにおける発行者の信頼性、および、検証手続に関する情報の管理形態に依存すると考えられる。検証者が第三者と結託することがないと判断することができる十分な根拠がある場合には、攻撃条件 4 と攻撃条件 5 を無視することができるため、攻撃条件 3 が攻撃者にとって相対的に有利な状況になっていると考えられる。

また、どの攻撃条件が最も現実的な脅威に対応するかについては、具体的なアプリケーションに依存することとなる。通常、人工物の発行者と検証者は「信頼できるエンティティ」であると考えられる点を踏まえると、攻撃条件 1 と 2 が現実的な脅威であると考えられる。したがって、少なくとも、これらの攻撃条件を想定したセキュリティ評価が必要であると考えられる。

ロ．2 種類の効果

人工物メトリック・システムに対する攻撃の効果は、攻撃が人工物メトリック・システムに対して及ぼす影響の度合いによって示される。そこで、攻撃の効果を分類する方法として、攻撃の被害が当該アプリケーションにおいて許容されるか否かによって二分するという方法が考えられる。具体的には次のように整理することができる。

- **全面的成功**：攻撃者が作製したクローンによって、当該アプリケーションにおいて許容される範囲を超える不正行為が可能となる場合
- **部分的成功**：攻撃者が作製したクローンによって不正が行われたとしても、当該アプリケーションにおいて許容される範囲内の不正行為にとどまる場合

このように整理すると、ある特定の攻撃が全面的成功をもたらすか、あるいは、部分的成功をもたらすかは、アプリケーションに応じて決定されることとなる。セキュリティ評価の結果、全面的成功をもたらす攻撃が想定された場合、その攻撃に対して優先的にセキュリティ対策を講じる必要があると

の判断がなされる。

（5）攻撃の方法

次に、「検証者に検知されることなく検証時に受理されるようにクローンを作製する」という攻撃がどのような手順で実行されるかについて、3 種類の検証手続と 5 つの攻撃条件に沿って検討する。ただし、こうした攻撃の具体的な実行方法は人工物メトリック・システムやそのアプリケーションの形態に応じて無数の可能性が想定され、それらをすべて列挙することは困難である。ここでは、人工物メトリック・システムのセキュリティを検討する際に「最低限考慮しておく必要がある」と考えられる攻撃の方法のみを取り上げることとする。

イ．人工物記録型 1 対 1 検証

人工物記録型 1 対 1 検証の場合、参照データが人工物やそれに付随する物品に記録される。攻撃者は正規の人工物を入手可能であるため、人工物およびその参照データを操作することが想定される。また、発行者や検証者と結託することによって、発行手続や検証手続を不正に操作する可能性も考えられる。

（イ）攻撃条件 1 の場合

攻撃条件 1（攻撃者は検証者・発行者のいずれとも結託しない、かつ、検証手続情報を入手しない）の下では、攻撃者が操作可能なのは、正規に発行された人工物とそれに対応する参照データのみである。このため、以下の攻撃が想定される。

【攻撃 1】人工物やその他の媒体を適当に準備し、他の発行済み人工物およびその参照データを用いて、その固有パターンに対応する参照データを偽造する。

― 例えば、参照データを磁気ストライプなどの媒体に記録する場合、その記録媒体を切貼りすることによって、クローンに対応する参照データを生成する、といったケースが考えられる。また、本攻撃は、適当に準備した人工物を無作為に提示して認証をパスしようとするブルートフォース攻撃の一種である。

【攻撃 2】無効とされた正規の人工物を再利用する。

― 例えば、使用期限を過ぎた人工物が発行者によって適切に廃棄されず、攻撃者が入手した場合が想定される。

（ロ）攻撃条件 2 の場合

攻撃条件 2（攻撃者は検証者・発行者のいずれとも結託しない、かつ、検証手続情報を入手する）の下においても、攻撃者が操作可能なのは、正規に発行された人工物とそれに対応する参照データのみである。したがって、攻撃 1、2 が実行可能であるほか、検証手続情報を用いることによって以下の攻撃も想定される。

【攻撃 3】正規の発行済み人工物から参照データを入手し、その参照データに対応するクローンを作製する。

― 本攻撃では、固有パターンの生成方法や判定方法に関する情報を必須とすることから、攻撃者が検証手続情報を入手しないと実行困難と考えられる。本攻撃は、正規の人工物を見本にして人工物のクローンを作製するというデッドコピー攻撃に対応する。

【攻撃 4】クローンを検証した際に、「受理」との判定結果が必ず出力されるように、検証用装置を不正に操作する。

― 本攻撃も、攻撃者が検証手続情報を入手しないと実行困難と考えられる。本攻撃の例として、外部から検証用装置を何らかの手段で不正に操作するといったケースが考えられる。具体的には、検証用装置を改造する、あるいは、検証用装置に電磁波を照射して内部の回路を誤動作させるといった攻撃（故障利用攻撃）が想定される。

（ハ）攻撃条件 3 の場合

攻撃条件 3（攻撃者は発行者のみと結託する、かつ、検証手続情報を入手する）の下では、攻撃者が発行者と結託し、発行手続を不正に操作することも可能となる。このため、攻撃 1～4 に加えて次の攻撃も想定される。

【攻撃 5】クローンを適当に準備し、発行前の正規の人工物として発行用装置に潜り込ませ、正規の手続によって発行させる。

― 具体的には、攻撃者が発行者と結託し、発行前の人工物の 1 つとしてクローンを発行用装置に潜り込ませ、発行時に生成される参照データをクローンに付与するという方法が考えられる。

（ニ）攻撃条件 4 の場合

攻撃条件 4（攻撃者は検証者のみと結託する、かつ、検証手続情報を入手する）の下では、攻撃者は検証者と結託し、検証手続を不正に操作することが可能となる。こうした不正な操作は上記攻撃 4（クローンが受理されるように検証用装置を不正に操作）に含まれることから、攻撃 1～4 が想定される。

― 攻撃 4 に関しては、検証者との結託によって検証用装置の設定（例えば、判定しきい値）を不正に変更することも可能になる。この攻撃は、攻撃条件 2、3 の下での攻撃 4 とは異なる。

（ホ）攻撃条件 5

攻撃条件 5（攻撃者は検証者・発行者の両方と結託する、かつ、検証手続情報を入手する）の下では、攻撃者は発行者・検証者の両者と結託して発行・検証手続において不正を実行可能であり、攻撃 1～5 が想定される。

ロ．データベース記録型 1 対 1 検証

データベース記録型 1 対 1 検証の場合、発行済み人工物の ID と参照データがペアでデータベースに管理されるため、データベースに格納されているデータの覗き見や改ざんを利用した攻撃が想定される。

（イ）攻撃条件 1 の場合

攻撃条件 1 の下では、攻撃者は、正規の発行済み人工物を攻撃に利用可能であるものの、発行者のデータベースに記録される ID や参照データを改ざんすることは困難である。したがって、想定される攻撃は、検証手続情報を入手しなくても実行可能な攻撃である攻撃 1、2 となる。

― ただし、データベース記録型 1 対 1 検証では、人工物やそれに付随する物品に（参照データでなく）ID が記載されているため、攻撃 1 は「人工物やその他の媒体を適当に準備し、他の発行済み人工物およびその参照データを用いて、その固有パターンに対応する ID を偽造する」という攻撃に対応する。

（ロ）攻撃条件 2 の場合

攻撃条件 2 の下でも、攻撃者が操作可能なのは、正規の発行済み人工物とそれに対応する ID である。ただし、攻撃者は検証手続情報を入手するため、正規の発行済み人工物のクローンを作製する攻撃として攻撃 1～3 が想

定されるほか、検証用装置の不正操作による攻撃（攻撃 4）も想定される。

（ハ）攻撃条件 3 の場合

攻撃条件 3 の下では、攻撃条件 2 の下で想定される攻撃（攻撃 1～4）に加えて、攻撃者が発行者と結託することによって実行可能となる攻撃も想定される。すなわち、攻撃者がデータベースに記録されるデータを覗き見・改ざんすることによって、攻撃 5 と以下の攻撃 6、7 も想定される。

【攻撃 6】まずクローンを適当に作製し、発行者のデータベースから正規の人工物の情報（ID、参照データ）を入手する。次に、正規の人工物の参照データが、予め作製していたクローンの固有パターンに対応しているか否かを確認し、対応する参照データと ID のペアを探索する。最後に、その参照データに対応する ID をクローンに付与する。

― 本攻撃は、参照データを発行者のデータベースから検索するという手段を利用する点において攻撃 1 と異なる。

【攻撃 7】まずクローンを適当に作製し、そのクローンの固有パターンに対応する登録データが発行者のデータベースに記録されていないことを確認する。次に、当該クローンの固有パターンに対応する参照データ（データ A とする）を何らかの方法で偽造する。最後に、当該クローンに対して適当な ID を割り振り、その ID と参照データ A をデータベースに不正に追加する（あるいは、データベースの別の参照データを改ざんする）。

― 本攻撃は、①ID と参照データを偽造する、②データベースに記録されているデータの改ざんを行う、という 2 点において攻撃 6 と異なる。

（ニ）攻撃条件 4 の場合

攻撃条件 4 の下では、攻撃条件 2 の下で想定される攻撃（攻撃 1～4）がまず想定される。さらに、攻撃者は、検証者と結託することによって、データベースに記録されているデータを覗き見することができるため、攻撃 6 も想定される。

（ホ）攻撃条件 5

攻撃条件 5 の下では、攻撃者がデータベースに記録されるデータを覗き

見・改ざんすることが可能となるほか、検証者とも結託可能であるため、攻撃 1～7 が想定される。

ハ．データベース記録型 1 対 N 検証

データベース記録型 1 対 N 検証の場合、データベース記録型 1 対 1 検証と同様に、発行済み人工物の参照データがデータベースに管理されるため、データベースに記録されるデータの覗き見や改ざんを利用した攻撃が想定される。以下のとおり、データベース記録型 1 対 1 検証と同様の攻撃が想定されると考えられる。

（イ）攻撃条件 1 の場合

攻撃条件 1 の下では、攻撃者は、正規の発行済み人工物を攻撃に利用可能であるものの、発行者のデータベースに記録される参照データを改ざんすることは困難である。このため、検証手続情報を入手しなくても実行可能な攻撃（攻撃 1、2）のみが想定される。

― ただし、データベース記録型 1 対 N 検証では、人工物やそれに付随する物品に参照データや ID が記載されていないため、攻撃 1 は「人工物やその他の媒体を適当に準備し、検証用装置に提示する」という攻撃に対応する。

（ロ）攻撃条件 2 の場合

攻撃条件 2 の下でも、攻撃者が攻撃に利用可能なのは正規の発行済み人工物のみである。ただし、攻撃者は検証手続情報を入手するため、攻撃 1、2 に加えて攻撃 3 も想定される。また、検証用装置の不正操作を利用した攻撃（攻撃 4）も想定される。

（ハ）攻撃条件 3 の場合

攻撃条件 3 の下では、攻撃条件 2 の下で想定される攻撃（攻撃 1～4）に加えて、攻撃者が発行者と結託することによって実行可能となる攻撃も想定される。すなわち、攻撃者が検知されずにデータベースを覗き見・改ざんすることが可能となり、攻撃 5～7 も想定される。

（ニ）攻撃条件 4 の場合

攻撃条件 4 の下では、攻撃条件 2 の下で想定される攻撃（攻撃 1～4）と同じ攻撃が想定される。また、攻撃者が検証者と結託するため、攻撃 6 も想定される。

（ホ）攻撃条件 5

攻撃条件 5 の下では、攻撃者がデータベースに記録されているデータを覗き見･改ざんすることが可能となるため、上記の攻撃 1～7 が想定される。

（６）セキュリティ要件と対策例

攻撃 1～7 に対して十分な安全性を有する人工物メトリック・システムを実現するためには、攻撃条件の顕現化を防止すること、あるいは、攻撃条件の顕現化を前提としたセキュリティ対策を講じることが必要である。以下では、各攻撃に対抗するためのセキュリティ要件について検討するほか、各要件を満足させるための対策例を挙げる。

一般に、セキュリティ要件は、具体的な人工物メトリック・システムの特性、アプリケーションの形態などを考慮した上で設定される。ここでは、具体的なアプリケーションおよび人工物メトリック・システムを想定しているわけではないため、最低限設定することが必要と考えられる上位レベルのセキュリティ要件を検討の対象とする。

イ．攻撃 1（参照データの偽造）に関する要件

攻撃 1 に関するセキュリティ要件として以下が挙げられる。

【セキュリティ要件 1】発行済み人工物の参照データを用いて、与えられた固有パターンに対応する参照データや ID を偽造することが困難であること

本要件の成否は参照データの生成アルゴリズムのセキュリティ特性に依存する。本要件を満足させるためには、例えば、参照データの生成アルゴリズムとして何らかの一方向性関数を採用するとともに、発行者のみが固有パターンから参照データを生成可能にする仕掛け（落し戸）をその生成アルゴリズムに組み込むことが考えられる。具体例として、公開鍵暗号に基礎をおくデジタル署名方式の採用が挙げられる。発行者のみが保有する秘密鍵（署名生成鍵）を用いて固有パターンに対するデジタル署名を生成し、それを参照データとして使用するといった方法が挙げられる。

ただし、いくら安全なアルゴリズムを適用したとしても、用意したクローンの固有パターンがたまたま参照データに対応するという可能性は否定できない。したがって、こうした可能性を十分小さくしておくことも必要である。

これらの点を考慮すると、本要件の達成度合いを評価する際には、まず、参照データを生成するアルゴリズムのセキュリティ特性に着目する必要がある。例えば、固有パターンに対する（公開鍵暗号に基礎を置く）デジタル署名を参照データとして採用する場合を想定する。この場合、そのデジタル署名方式の安全性に焦点を当てることとなる。具体的には次の項目に着目することが考えられる。

① 安全性が理論的に証明可能であるか否か、また、その証明内容はどのようなものか。

— 例えば、攻撃者のタイプ（能動的攻撃、受動的攻撃）、攻撃の効果、署名方式が依拠している困難性（素因数分解問題の困難性、離散対数問題の困難性など）、安全性証明のモデル（ランダムオラクル・モデルなど）を考慮する。

② セキュリティ・パラメータが適切に設定されているか。

— 例えば、署名生成鍵、署名検証鍵のサイズが、アプリケーションにおいて要求されるセキュリティ・レベルを達成される上で十分であるか否かを考慮する。

③ アプリケーションにおける実装環境が署名方式の安全性を損なう懸念はないか。

このように、アルゴリズムの特性に関する項目を列挙した上で、どの項目が満足されているかを確認し、その結果に基づいて本要件の満足度合いを評価することが考えられる。

デジタル署名方式の場合においては、アルゴリズムの安全性の概念やその評価の枠組みが確立しており、理論的な安全性証明の方法についても活発な研究が進められている。また、CRYPTREC 評価報告書（情報処理振興事業協会 [2003]）や NESSIE 評価報告書など、デジタル署名方式の安全性評価に関する各種報告書が近年発表されている。上記項目が満足されているかを検証する際には、こうした最新の評価結果を参照することも有用であろう。

また、「無作為に準備した人工物やその他の媒体における固有パターンがたまたま参照データと一致する」という攻撃はブルートフォース攻撃に対応し、こうした可能性を評価する尺度として、３章で説明したブルートフォース攻撃成功率が利用可能である。ブルートフォース攻撃成功率の導出や評価方法については、５章において具体的に説明する。

ロ．攻撃 2（無効な人工物の再利用）に関する要件

攻撃 2 を実行するためには、攻撃者は、「有効な人工物」として再度利用することが可能な状態で「無効となった人工物」を手に入れる必要がある。したがって、本攻撃に対応するセキュリティ要件として、以下が考えられる。

【セキュリティ要件 2】無効化した人工物を、再利用が困難な形態で確実に廃棄すること

本要件は、発行者のセキュリティ・マネジメントと深い関係がある。本要件に基づくセキュリティ対策の方向性としては、①人工物の無効化・廃棄を担当する発行管理者による不正行為を防止・検知する、②無効化された人工物が検証対象であった場合に、その人工物を拒否するように検証用装置を調整する、という 2 つが挙げられる。こうした対策がどの程度講じられているかを尺度として本要件の達成度を評価するという方法が考えられる。

発行管理者による不正行為の防止・検知に関する対策を評価する場合、例えば、次の項目に着目することが考えられる。

① 人工物の無効化手続時に、無効化対象の人工物の抜取りを防止する仕組みが講じられているか。

— 例えば、人工物の無効化手続に携わる担当者を複数配置し、複数の担当者が協力しないと実行することができない仕組み（ツーパーソン・コントロール）となっているか。また、無効化の対象となっている人工物の個数を無効化手続の前後でそれぞれ計測し、両者が一致していることを確認する機構が採用されているか。

② 無効化手続を実行する発行用装置のハードウェアには、外部からの不正操作を困難にするための機構が組み込まれているか。

③ 無効化手続の実施結果を後日検証することが可能な仕組みになっているか。

— 例えば、無効化手続の実行者・日時・処理内容を後日確認するためのログを生成し、改ざんを検知可能な形態でログを保管しているか。

また、無効化された人工物が検証用装置において確実に拒否されるための手段がどの程度講じられているかに関しては、例えば、次の項目に着目する

ことが考えられる。

① 人工物の無効化手続によって人工物の固有パターンが著しく変形し、参照データとの整合性が失われているか（また、整合性損失の度合いを示す数値が利用可能ならば、その数値から整合性が十分に損失されていると考えられるか）。

— 例えば、無効化された人工物の固有パターンを無効化手続後に再現することが困難となるように、無効化手続において人工物を細かく裁断しているか。

② 人工物記録型 1 対 1 検証の場合、人工物に記録されている参照データを無効化手続によって削除するなど、参照データを検証用装置によって読取困難にする仕組みが採用されているか。

③ データベース記録型 1 対 1 検証、あるいは、データベース記録型 1 対 N 検証の場合、無効化手続において、無効化の対象となった人工物の参照データをデータベースから削除する処理が行われているか。

— また、データベースにおける参照データ削除の手続について、その実行者・日時・処理内容を後日確認するためのログを生成し、改ざんを検知可能な形態でログを保管しているか。

このような項目を抽出して一種の「チェックリスト」を作成し、どの程度まで対策が講じられているかを尺度として、本要件の達成度合いを評価することができる。ただし、セキュリティ対策の具体的な内容は個々の人工物メトリック・システムとそのセキュリティ・ポリシーに依存することから、アプリケーションに応じたチェックリストを利用者が作成する必要がある。

ハ．攻撃 3（クローンの作製）に関する要件

攻撃 3 を防止するためには、与えられた参照データに対応するクローンを作製困難であることが必要であり、以下の要件を設定することが求められる。

【セキュリティ要件 3】特定の固有パターンを、別の人工物やクローンにおいて意図的に再現することが困難であること

攻撃 3 を実現する方法として次の 2 つが挙げられる。

①「ある人工物の固有パターンと同一」と判定される固有パターンをもつ別の正規の人工物をみつける。

②「ある人工物の固有パターンと同一」と判定される固有パターンをもつクローンを作製する。

これらの攻撃を前提として本要件を満足させるためには、クローン受理率を十分に小さくなるように設定する必要がある。したがって、クローン受理率がアプリケーションにおいて要求されるセキュリティ・レベルに見合っているか否かを検証することによって、本要件の達成度合いを評価することができる。ただし、3章においても今後の課題として指摘したように、「信頼できる精度でクローン受理率を測定するためにはどのような方法を用いるとよいか」という問題が残されている。

ニ．攻撃 4（検証用装置の不正操作）に関する要件

攻撃 4 に関するセキュリティ要件としては、次の要件が挙げられる。

【セキュリティ要件 4】攻撃者が検証者と結託困難であり、かつ、検証者に検知されず検証用装置を不正に操作困難であること

（イ）検証者との結託困難

セキュリティ要件 4 を達成するためには、まず、攻撃者が検証者と結託困難である状態にする必要があり、その達成度は検証者がどの程度信頼できるエンティティかを評価することによって判断することができる。しかし、現時点では、検証者などのエンティティの属性を評価するための客観的な尺度として利用可能なものが確立されていない。このため、検証者が採用している個々のセキュリティ対策の内容を吟味して判断を下すことが必要となる。その際に、具体的にどのような項目に着目すればよいかが問題となるが、例えば次の項目が考えられる。

① 検証者の内部担当者の 1 人が攻撃者と協力関係を結んだとしても、不正行為の実行を防止する仕組みが講じられているか。

— 例えば、検証管理者を複数配置し、単独では各種手続を実行できない仕組みが採用されているか、また、検証管理者が攻撃者から脅迫されていた場合でも、攻撃者に悟られないようにその事実を第三者に通報する仕組み（デュレス・コントロール）が採用されている

か（大島・松本 [2003]）。

② 検証手続などの処理内容について後日確認することが可能な仕組みになっているか。

— 例えば、検証手続やデータベースへのアクセスなどに関して処理の実行者・日時・処理内容を後日確認するためのログを生成し、改ざんを検知可能な形態で保管しているか。

③ 検証手続において、複製が容易な固有パターンをもつ人工物やクローンを排除するための機構が準備されているか。

また、セキュリティ・マネジメントが適切に行われているか否かを第三者機関が評価する制度も運用されており、検証者がそうした評価を受けている場合にはその評価結果を利用することも可能である。こうした制度の代表的なものとして、BS 7799 に基づくセキュリティ管理の第三者評価制度や、同制度をベースとしてわが国で運用が開始された「情報セキュリティマネジメントシステム（ISMS）適合性評価制度」が挙げられる。

（ロ）検証用装置の不正操作困難

セキュリティ要件 4 の達成度合いは、検証用装置のセキュリティ対策の内容によっても評価される。評価を行うにあたって具体的にどのような攻撃を想定するかは、アプリケーションの形態やセキュリティ・ポリシーに依存する。例えば、検証用装置に直接アクセスするケースと遠隔地から間接的にアクセスするケースが考えられる。

検証用装置に直接アクセスするケースとしては、攻撃者が検証用装置のハードウェアに電磁波などを照射し内部の回路に対して意図的に故障を発生させることによって、判定出力部の出力を変化させるといった攻撃（一種の故障利用攻撃）が考えられる。こうした攻撃が想定される場合に評価すべき項目として以下が挙げられる。

① ハードウェアが電磁波などを異常に照射された場合、それを検知し、異常を操作担当者に通知する機構が組み込まれているか。

② ハードウェア内部の回路が異常に動作した場合、それを検知してハードウェアの機能を停止させる機構が組み込まれているか。

こうしたハードウェアのセキュリティについて判断する場合、第三者か

ら一定の評価を受けているならば、その評価結果を参考にすることができる。暗号モジュールを対象とした第三者評価の代表的な制度としては、米国の政府機関（NIST）とカナダの政府機関（CSE）が運営する CMVP（Cryptographic Module Validation Program）が挙げられる。本制度では、NIST などから評価機関 CMT（Cryptographic Module Testing laboratories）として認可を受けた第三者機関が、FIPS 140-2（NIST [2001]）に準拠して作製された暗号モジュールをテストし、FIPS 140-2 のセキュリティ要件が満足されているか否かを評価する。その上で、CMT の評価結果に基づき、NIST や CSE が「評価対象となった暗号モジュールが FIPS 140-2 に準拠して作製され、一定要件を満足している」旨の認定を行うという仕組みになっている。

また、攻撃者が遠隔地から間接的に検証用装置にアクセスするという形態としては、検証用装置が何らかのネットワークに接続している場合に想定される。例えば、攻撃者が、検証用装置が接続しているネットワークを経由して検証用装置に不正侵入し、検証用装置を制御するソフトウェアを不正に書き換えるといった攻撃が考えられる。こうした攻撃を想定する場合、次のような項目を評価することが求められる。

① 外部のネットワークから検証用装置にアクセスするエンティティを適切に確認するための手段が講じられているか。

② 検証用装置を制御するソフトウェアを更新・書換えした場合に、その事実を記録するためのログが生成されているか。また、ログの改ざんを検知するための手段が講じられているか。

こうした項目を抽出した上で、それらが実際にどの程度適用されているかを尺度として要件の達成度を評価することができると考えられる。

ホ．攻撃 5（クローンを正規の発行手続を経て発行）に関する要件

攻撃 5 を成功させるためには、攻撃者は発行者と結託することが必要である。したがって、以下のセキュリティ要件を設定することが考えられる。

【セキュリティ要件 5】攻撃者が発行者と結託困難であること

セキュリティ要件 5 を満足させるためには、攻撃者が発行者と結託困難な状態にする必要があり、本要件の達成度合いをどう評価するかについてはセキュリティ要件 4 と同様の議論となる。すなわち、発行者の属性を評価する

ことが必要となるが、そのための客観的な尺度として利用可能なものは現時点では確立されていない。このため、発行者が採用している個々のセキュリティ対策の内容を吟味して判断を下すこととなる。吟味の対象となるセキュリティ対策としては、セキュリティ要件 4 において説明した項目（ただし、検証者を発行者に読み替える必要あり）が例として挙げられる。

へ．攻撃 6（クローンに対応する参照データを検索）に関する要件

攻撃 6 は、データベース記録型 1 対 1 検証、および、データベース記録型 1 対 N 検証において想定される攻撃であり、以下のセキュリティ要件を設定することが考えられる。

【セキュリティ要件 6】 データベースに格納されている（発行済み人工物の）参照データの中から、適当に作製したクローンの固有パターンに対応する参照データを探索困難であること

本要件を満足させるためには、「データベースに記録される参照データの中から、適当に作製したクローンに対応する参照データをみつける可能性」を十分に小さくすることが必要である。したがって、本要件の達成度合いの尺度として、「正規の人工物の参照データや発行者のデータベースの中から、適当に作製したクローンに対応する参照データの探索に成功する確率」が考えられる。こうした攻撃の成功率を算出することができるならば、アプリケーションにおいて許容される確率の上限値と比較して、本要件が満足されているか否かを確認することができる。

類似の攻撃成功率を導出し、実際に定量的なセキュリティ評価を行った研究事例として、松本･田中の研究を挙げることができる（松本･田中 [2001]）。松本・田中は、暗号処理などがどのハードウェアにおいて実行されたかを後日特定可能にする方式として、「実行ハードウェア確認タグ方式」を提案している（松本・田中 [2000]）。本方式は、入出力機能を有し複製困難な「耐タンパー・ハードウェア」を採用し、耐タンパー・モジュールの出力によって実行ハードウェアの特定を可能にする。松本・田中は、本方式のセキュリティ評価の一環として、「耐タンパー・モジュールの入出力ペアを複数入手した後、ある入力が与えられたときに、その入力に対する同モジュールの出力を入手する確率がどのように表わされるか」という問題を取扱っている。検討結果として、ハードウェア・モジュールの入出力のサイズや、予め入手した入出力のペア数などから、上記確率を計算する数式が導出され、定量的

なセキュリティ評価が可能であることが示されている。

こうした研究を人工物メトリック・システムに応用し、セキュリティ要件 6 において想定されている攻撃の成功確率を導出・評価することも今後の研究の重要な項目の 1 つに数えられる。

ト．攻撃 7（データベースに参照データを追加）に関する要件

攻撃 7 は、データベースを利用する検証手続において想定される攻撃である。攻撃 7 を成功させるためには、クローンに対応する参照データを偽造するとともに、その参照データなどをデータベースに不正に追加する必要がある。したがって、本攻撃に対しては、セキュリティ要件 1 とセキュリティ要件 5 を設定することが求められる。

攻撃 7 を想定してセキュリティ要件 5 を満足させる方法としては、データベースに関する適切なセキュリティ・マネジメントの実施が挙げられる。例えば、データベースへのデータの書込み・読出しを行う際には複数の担当者の協力を義務付ける、データベースへのアクセス・ログを生成し安全に保管する、といった対応が考えられる。

（7）各攻撃の想定環境・効果・セキュリティ要件

以上の検討結果を整理・考察する。攻撃 1～7 がどの検証手続・攻撃条件において想定されるか、また、どのようなセキュリティ要件を設定する必要があるかを整理すると、表 4.2 のとおりである。

表 4.2　各環境において想定される攻撃とセキュリティ要件

攻撃条件	各検証手続に適用される攻撃		
	人工物記録型 1 対 1 検証	データベース記録型 1 対 1 検証	データベース記録型 1 対 N 検証
攻撃条件 1	攻撃 1, 2 （セキュリティ要件 1, 2）		
攻撃条件 2	攻撃 1～4 （セキュリティ要件 1～4）		
攻撃条件 3	攻撃 1～5 （セキュリティ要件 1～5）	攻撃 1～7 （セキュリティ要件 1～7）	
攻撃条件 4	攻撃 1～4 （セキュリティ要件 1～4）	攻撃 1～4, 6 （セキュリティ要件 1～4, 6）	
攻撃条件 5	攻撃 1～5 （セキュリティ要件 1～5）	攻撃 1～7 （セキュリティ要件 1～7）	

（注）シャドー部分は、現実的な脅威として考慮する必要がある攻撃を示す。

イ．攻撃条件

各攻撃の想定環境（攻撃条件）に焦点を当てると、攻撃 1（参照データの

偽造）と攻撃 2（無効な人工物の再利用）は、検証者・発行者との結託や検証手続情報の入手が不要であり、7 種類の攻撃の中で最も攻撃実行のハードルが低い。また、3 種類の検証手続のいずれにも適用可能である。

攻撃 3（特定の参照データに対するクローンを作製）と攻撃 4（検証用装置の不正操作）は、検証手続情報の入手が必要となるが、発行者や検証者との結託が必要でないため、攻撃 1、2 の次に実行しやすい攻撃と位置づけることができる。

以上の攻撃 1～4 は、発行者や検証者と結託が不要であり、現実的な脅威になる可能性が相対的に高いと考えられる。したがって、人工物メトリック・システムの耐クローン性評価を行う際には、これらの攻撃を前提とすることが求められる。

一方、攻撃 5～7 は、実行するためのハードルが相対的に高い攻撃である。人工物記録型 1 対 1 検証においては、攻撃 5 を実行するためには少なくとも発行者と結託する必要がある。また、データベース記録型 1 対 1 検証とデータベース記録型 1 対 N 検証においては、攻撃 6、7 を実行するためには、少なくとも検証者、発行者とそれぞれ結託することが求められる。一般には、発行者や検証者を「信頼できるエンティティ」と想定するケースが多いが、こうした場合には、攻撃 5～7 は現実の脅威として考慮する必要はなくなる。

ロ．セキュリティ要件と達成度

（6）で明らかにしたセキュリティ要件をベースとして、各攻撃条件の下で設定すべき要件を整理する。

まず、人工物記録型 1 対 1 検証では、攻撃条件 1 の下ではセキュリティ要件 1、2 を設定し、攻撃条件 2、4 の下ではセキュリティ要件 1～4 を設定することが求められる。また、発行者との結託を想定する攻撃条件 3、5 の下では、セキュリティ要件 1～4 に加えて、セキュリティ要件 5（発行者との結託を困難にすること）を設定することも求められる。

データベース記録型 1 対 1 検証とデータベース記録型 1 対 N 検証の場合、データベースに記録されているデータの覗き見や改ざんを利用した攻撃が想定されるため、そうした攻撃に対応するためのセキュリティ要件を追加設定することが必要となる。こうした攻撃は、攻撃者が発行者あるいは検証者と結託する場合（攻撃条件 3～5 に対応）に実行可能であり、攻撃条件 3～5 の下ではセキュリティ要件 7 を追加的に設定することが求められる。

各攻撃が実際に成功するか否かについては、各攻撃に対して実施されるセキュリティ対策の有効性に左右される。したがって、実施した対策の効果によって各要件がどの程度満足されるかを確認することが重要である。各要件

の達成度を測る尺度の候補を整理すると表 4.3 のとおりである。

表 4.3 セキュリティ要件の達成度合いの尺度

セキュリティ要件	尺度
要件 1	**参照データ生成アルゴリズムに関する評価項目（チェックリスト）の達成度、ブルートフォース攻撃成功率などの指標** （項目例）証明可能安全性の有無、パラメータ設定の適切さ
要件 2	**人工物無効化手続に関する評価項目（チェックリスト）の達成度** （項目例）無効化対象の人工物の抜取防止、ハードウェアの耐タンパー化、無効化手続のログ管理、参照データの削除
要件 3	**クローン受理率などの指標**
要件 4	**検証者に関する評価項目（チェックリスト）の達成度** （項目例）操作者の共同作業化、処理内容のログ管理、ハードウェアの耐タンパー化 ― 第三者機関によるセキュリティ管理・運用体制に関する評価結果（ISMS 適合性評価制度など）の利用も考えられる。
要件 5	**検証用システムに関する評価項目（チェックリスト）の達成度** （項目例）ハードウェアの耐タンパー化、不正侵入対策 ― 第三者機関による暗号モジュールのセキュリティ評価結果（CMVP など）を利用することも考えられる。
要件 6	**発行者に関する評価項目（チェックリスト）の達成度** （項目例）操作者の共同作業化、処理内容のログ管理、ハードウェアの耐タンパー化、データベースの改ざん検知 ― 第三者機関によるセキュリティ管理・運用体制に関する評価結果（ISMS 適合性評価制度など）の利用も考えられる。
要件 7	**参照データの探索による攻撃の成功率などの指標**

これらのうち、セキュリティ要件 3 においては定量的な尺度となりうるものが提案されており、今後、クローン受理率などをどのように測定するかといった課題が残されている。また、その他の要件に関する評価の尺度については、次のような点について検討することが求められる。

① セキュリティ・ポリシーなどに基づいてセキュリティ対策に関する項目のチェックリストを作成し、各セキュリティ要件の満足度を評価する方法

② 参照データの検索によってクローンを作製する攻撃の成功率を評価する方法

特に、上記①は、ISO/IEC 15408 に基づく評価手法など、既存のセキュリティ評価手法との関連も踏まえて検討することが現実的である。例えば、人

工物メトリック・システムに対して ISO/IEC 15408 に基づく評価手法を適用する場合、上記①におけるチェックリストの内容をセキュリティ要件仕様書（protection profile）に反映させることができれば、各セキュリティ要件の達成度合いについても評価を得ることができる可能性がある。

バイオメトリック・システムにおいては、ISO/IEC 15408 ベースの評価を実現する方向で既に検討が進められている。バイオメトリック・システム用のセキュリティ要件仕様書がいくつか作成されている（United Kingdom Government Biometrics Working Group [2001], Kong *et al.* [2002]）ほか、バイオメトリック・システムのセキュリティ評価を行う際の方法論（Biometrics Evaluation Methodology）の検討も進められている（Common Criteria Biometric Evaluation Methodology Working Group [2002]）。こうした動向を踏まえて、人工物メトリック・システムの検討を進めることが有用であろう。

ハ．攻撃の効果

攻撃の効果自体はアプリケーションに依存し、どの攻撃が全面的成功に該当するかといった点に関してここで具体的に議論することはできない。ただし、攻撃の効果に関連して、不正に利用される可能性のあるクローンが制限されるか否かという観点から考察することはできる。こうしたクローンが一定の範囲に制限される場合には、制限されない場合に比べて攻撃成功による影響が小さく、攻撃成功時の被害も相対的に小さいと考えることができる。

まず、攻撃 2 では、不正利用されるクローンが「無効とされた正規の人工物」に限定される。また、攻撃 6 では、不正に利用されるクローンは「データベース記録されている参照データに対応する固有パターンを有するもの」に限定される。これら以外の攻撃では、不正に利用されるクローンが限定されることがなく、攻撃成功時の被害が比較的大きくなる可能性が考えられる。

ニ．検討結果の活用方法

最後に、本章での検討結果を実際の人工物メトリック・システムにおけるセキュリティ評価においてどのように活用することができるかを検討する。評価手順の一例として次のような手法が考えられる。

＜1＞　人工物メトリック・システムの利用環境を、当該アプリケーションのセキュリティ・ポリシーやセキュリティ対策の実施規程などを踏まえつつ吟味する。特に、次の点に着目する。

①発行者において、人工物の発行手続およびデータベースはどのように管理・運用されているか（内部者による不正行為を防止・検

知する機構は準備されているか)。

②検証者において、人工物の検証手続がどのように管理・運用されているか（内部者による不正行為を防止・検知する機構は準備されているか)。

③検証手続に関する情報（固有パターン抽出方法や参照データ生成方法など）がどのように管理されているか。

＜2＞　上記＜1＞の結果を踏まえ、セキュリティ評価を行う上でどの攻撃条件を想定するのが妥当かを決定し、その攻撃条件の下で想定される攻撃がどれかを明らかにする。

―　例えば、攻撃条件 2（検証者・発行者との結託なし、攻撃者による検証手続に関する情報の入手を想定）が妥当であると判断された場合、攻撃 1～4 が「実行されうる攻撃」として検討の対象となる。こうした判断を行う上で、人工物メトリック・システムのアプリケーションにおける脅威・リスク分析を行うことが考えられる。

＜3＞　上記＜2＞で選択した攻撃への対策の優先順位を、攻撃の効果、セキュリティ・ポリシーや人工物の利用状況などを考慮して決定する。

―　上記＜2＞の例では、攻撃 1～4 のうち、攻撃 2 が部分的成功の可能性を有し、その他の攻撃は全面的成功の可能性を有している。このため、まず攻撃 1、3、4 を想定したセキュリティ評価が求められると考えられる。その他の攻撃については、セキュリティ・ポリシーなどを参照しつつ優先順位を設定する。

＜4＞　優先順位に沿って、各攻撃に対応するセキュリティ要件がどの程度達成されているかを評価する。最終的には、アプリケーションにおけるリスク許容度が満足されているか否かを確認する。

―　評価を行うにあたっては、人工物メトリック・システムの種類に応じて、どのような尺度に基づいてセキュリティ要件の達成度を測るかを決定しておく必要がある。

以上の一連の処理を行い、対策が不十分と判断された攻撃に関しては、追加的な対策の実施を検討することとなる。上記＜4＞における評価の実施主体は、例えば ISO/IEC 15408 ベースでの評価の場合には、評価機関として認定を受けた第三者機関となるし、可能であれば、利用者自身が評価を行う

ケースも考えられよう。ただし、そのためには、３章でも指摘したように評価手法の整備などの課題をクリアしていくことが必要となる。

５．人工物メトリック・システムのセキュリティ評価事例

本章では、人工物メトリック・システムのセキュリティ評価事例について述べる。このシステムは、IOSAS と同じ原理に基づいているものの、人工物メトリック・システムのセキュリティ評価を意図して新たに構築したシステムであり、IOSAS とは異なる。ここで紹介する評価対象システムは、４章で述べた「人工物記録型 1 対 1 検証」と「データベース記録型 1 対 1 検証」の 2 種類の検証手続を用いたシステムに相当し、ブルートフォース攻撃の成功率の評価事例とデッドコピー攻撃の成功率の評価事例を示す。これらの評価は Matsumoto and Matsumoto [2002, 2003]において行われたものであり、本章の内容は同論文をベースとしている。

（1）磁性ファイバを利用する人工物メトリック・システム

イ．評価対象システムの基本構成

磁性ファイバを紙に分散させた証書（以下、F-paper と呼ぶ）を利用する人工物メトリック・システム（評価対象システム）の基本構成を図 5.1 に示す。検証用装置は、「ランダムな磁性ファイバにより生成される磁気信号から得られる固有パターン」と「発行時に予め記録された参照データ」の相関係数を計算し、パターン照合（基本的な照合アルゴリズムは付録を参照）を行って固有パターンを検証する。この検証結果を基に、F-paper の受理または拒否の判定を行う。

ここで、参照データは、①検証用装置内や遠隔地にデータベースとして記録する場合（データベース記録型 1 対 1 検証に対応）と②F-paper 上に記録する場合（人工物記録型 1 対 1 検証に対応）とが考えられる。評価対象システムでは、認証精度を調整できるようにパターン照合の範囲と分解能をそれぞれパラメータ d、a_0 として設定変更できるようにしている。

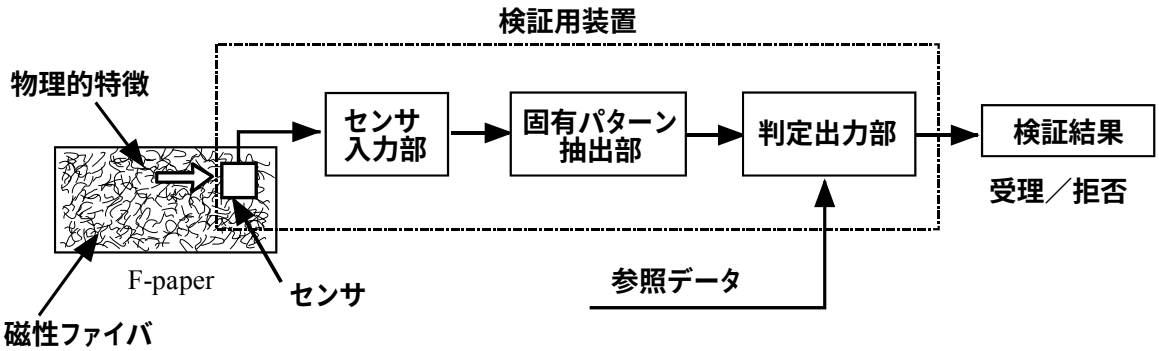

図 5.1 評価対象システムの基本構成

ロ．評価対象の認証精度

評価対象システムの認証精度をみるために、実験によって得られた ROC 曲線を図 5.2 に示す。ROC 曲線は、判定しきい値を変化させたときに、対応する誤一致率（FMR）と誤不一致率（FNMR）のペアをプロットしたものである。図 5.2 におけるパラメータ d はパターン照合の範囲を設定する値であり、固有パターンのデータ・サイズを表わす。この d の値に比例してパターン照合の範囲が大きくなる。パターン照合の分解能のパラメータは a_0 とし、ここではいずれも a_0=10 とした。

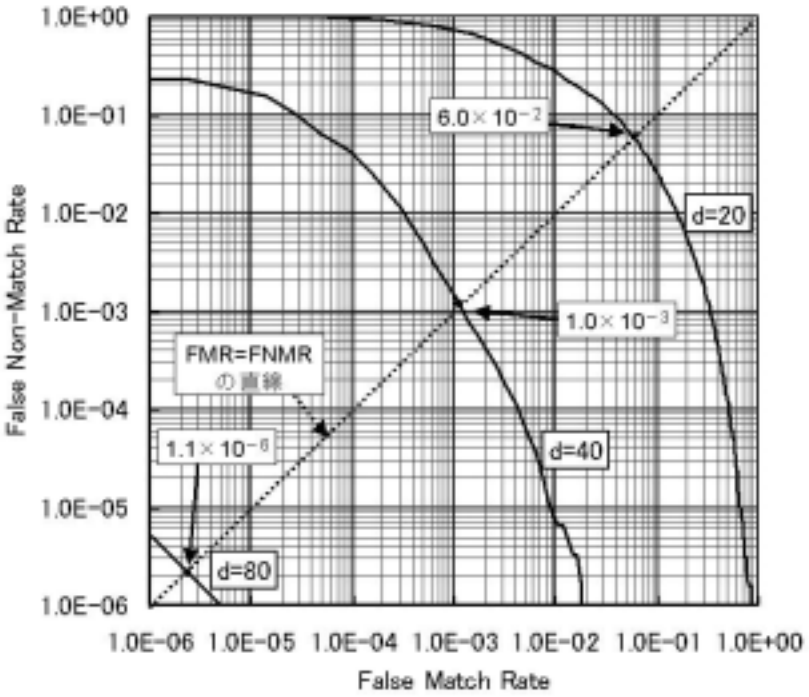

図 5.2　**評価対象システムの認証精度**

図 5.2 から、クローンによる攻撃が存在しないときの等誤り率（EER）、すなわち、誤一致率と誤不一致率が一致する場合の等誤り率は、d = 20、40、80 の場合、それぞれ6.0×10^{-2}、1.0×10^{-3}、1.1×10^{-6} となる。

（2）ブルートフォース攻撃に対する評価事例

イ．評価対象

検証手続の種類として、４章で述べた「人工物記録型 1 対 1 検証」を行うシステム（以下、評価対象システムⅠと呼ぶ）を評価対象とする。本システ

ムは、図 5.3 に示すように、F-paper と検証用装置によって構成される。F-paper の記録エリアには、図示されていない発行装置により予め参照データがデジタル署名とともに“記録データ”として記録される。検証用装置は、デジタル署名を検証するとともに、参照データを用いて固有パターンを検証する。これらの検証結果を基に、F-paper の受理または拒否の判定を行う。

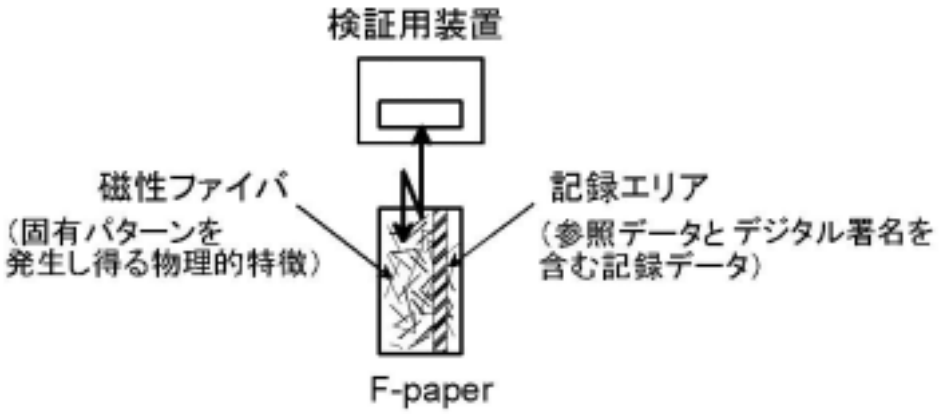

図 5.3　評価対象システムⅠの構成

ロ．評価における前提条件

以下の前提条件の下で、システムの安全性評価を行う。

(a-1) 暗号技術（デジタル署名）により安全が保たれているため、攻撃者は、記録データの生成方法を知ることができない。
(a-2) 攻撃者は F-paper から得られる固有パターンを観察することができない。
(a-3) 攻撃者は、F-paper の発行装置（記録データ生成機能）を利用することも発行装置に関する秘密の情報を得ることもできない。
(a-4) 攻撃者は、F-paper から得られる固有パターンの特徴抽出方法やパターン照合方法を知ることができず、実際の検証用装置で検証を試行するしかない。

これらの前提条件は、４章で定義した「攻撃条件 1」に対応する。さらに、ここでは以下の前提条件を加える。

(a-5) 攻撃者は、固有パターンを意図的に作製することができない。

ハ．想定される攻撃

評価対象システムⅠの検証用装置にはF-paperが提示され、検証用装置は、F-paper の記録データから得られる参照データと物理的特徴から得られる固有パターンを照合する。攻撃者が「検証対象以外の提示物によって検証用装置から受理の判定を 1 回でも得た場合」を攻撃成功と考える。こうした攻撃を具体的に実行する方法としては、図 5.4 に示すようなものが想定される。

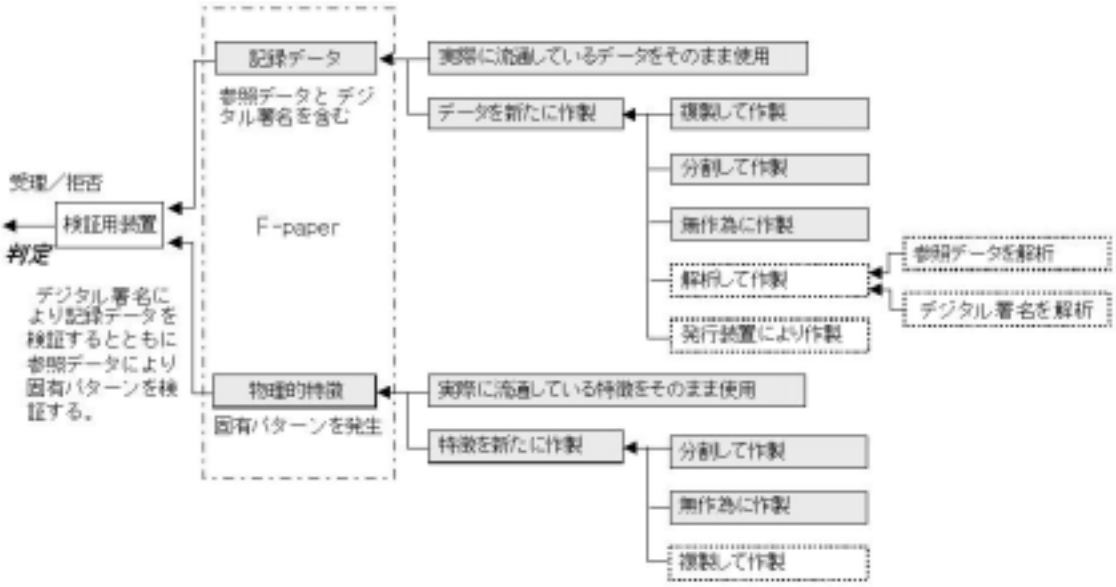

図 5.4　評価対象システムⅠに対する攻撃

まず、記録データを偽造するという方法が考えられる。しかし、記録データにはデジタル署名が添付されており、前提条件(a-1)から、参照データを含む記録データの無作為な改変は論理的な矛盾を生じる可能性が高く、提示物の受入率は本来の誤受理率を超えることは困難であると考えられる。

次に、物理的特徴を操作する方法を考えると、前提条件(a-2)、(a-3)、(a-4)、(a-5)から、現実的な攻撃方法としては、「無作為に F-paper の物理的特徴を改変・複製する、あるいは、組み合わせて用いる」という方法に限定される。

以上より、ここでは、「記録データと物理的特徴を順次組み合わせてクローンを作製し、検証用装置に提示する」という攻撃（ブルートフォース攻撃の 1 つ）に絞って検討する。

なお、４章で述べたように、人工物記録型 1 対 1 検証において攻撃条件 1 を想定する場合、上記攻撃（攻撃 1 に対応）だけでなく、無効化された人工物を用いる攻撃（攻撃 2 に対応）も考慮する必要がある。ただし、ここで対象としているシステムは、無効化の方法を具体的に想定しているわけではな

いため、無効化された人工物を用いる攻撃については検討対象外とする。

ニ．ブルートフォース攻撃に対するセキュリティ評価事例

ブルートフォース攻撃に対する評価対象システムⅠの安全性を理論的に評価する。ここで、より厳しい評価を行うために、攻撃者は、「正規の F-paper から複写するなどして得た有効な記録データと、F-paper の素材を入手するなどして得た固有パターンを発生し得る物理的特徴（有効な物理的特徴と呼ぶ）を組み合わせて、クローンを効率的に作製する」と想定する。

有効な物理的特徴 $\boldsymbol{p}_i^v$ (i=1, 2, …, N_1) を要素とする有限集合を $\boldsymbol{X}_{\boldsymbol{p}}^v$ とする。また、有効な記録データ $\boldsymbol{w}_i^v$ (i=1, 2, …, N_2) を要素とする有限集合を $\boldsymbol{X}_{\boldsymbol{w}}^v$ とする。ここで、 N_1 と N_2 は十分に大きいとする。攻撃者が n_1 個の有効な物理的特徴 $\boldsymbol{p}_j^s \in \boldsymbol{X}_{\boldsymbol{p}}^v$ (j=1, 2, …, n_1) と、n_2 個の有効な記録データ $\boldsymbol{w}_j^s \in \boldsymbol{X}_{\boldsymbol{w}}^v$ (j=1, 2, …, n_2) を用いて攻撃を行った場合、攻撃が 1 つのクローンでも成功する確率（すなわち、ブルートフォース攻撃成功率） $P(n_1, n_2)$ は、

$$P(n_1,1) = 1-(1-FA)^{n_1} \tag{5.1}$$

および、

$$\begin{aligned} &P(n_1,n_2) \\ &= P(n_1,n_2-1)+\{1-P(n_1,n_2-1)\}P(n_1,1) \end{aligned} \tag{5.2}$$

と表わされる。ここで、FA はシステムの誤受理率（FAR）を表わす。

(5.2)式より、

$$\begin{aligned} &P(n_1,n_2) \\ &= P(n_1,1)+\{1-P(n_1,1)\}P(n_1,n_2-1) \\ &= P(n_1,1)+P(n_1,1)\left\{(1-P(n_1,1))+(1-P(n_1,1))^2+\cdots+(1-P(n_1,1))^{(n_2-1)}\right\} \\ &= P(n_1,1)+P(n_1,1)\left[\{1-P(n_1,1)\}\frac{1-\{1-P(n_1,1)\}^{(n_2-1)}}{1-\{1-P(n_1,1)\}}\right] \\ &= 1-\{1-P(n_1,1)\}^{n_2} \end{aligned}$$

であり、(5.1)式より、

$$1-\{1-P(n_1,1)\}^{n_2} = 1-(1-FA)^{n_1 \cdot n_2} \tag{5.3}$$

となる。

このように、ブルートフォース攻撃成功率は、システムにおける誤受理率

FA と、サンプル数を乗算した数 $n_1 \times n_2$ に依存することになる。あるシステムへの攻撃が成功するか否かは、攻撃を行うために有効な記録データおよび有効な物理的特徴をいかに多く入手できるかに依存することがわかる。

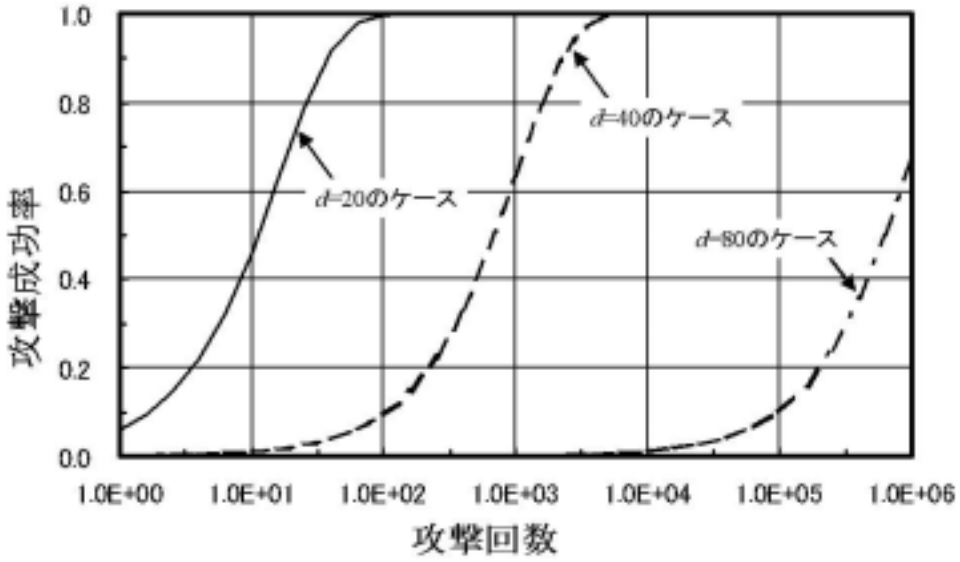

図 5.5　**ブルートフォース攻撃成功率（a_0=10）**

図 5.2 で示した評価対象システムⅠの誤受理率を(5.3)式に代入し、ブルートフォース攻撃成功率を計算すると、図 5.5 が得られる。パターン照合の範囲 d が大きくなるにつれて、同一の攻撃回数に対する攻撃成功率が低くなっており、「照合の範囲を柔軟に設定することによって攻撃成功率をアプリケーションにおいて許容されるレベルに抑える」といった対応が可能であることがわかる。

（3）デッドコピー攻撃に対するセキュリティ評価事例

イ．評価対象

検証手続の種類として、４章で述べた「データベース記録型 1 対 1 検証」を行うシステム（以下、評価対象システムⅡと呼ぶ）を評価対象とする。このシステムは、図 5.6 に示すように、パーソナル・コンピュータ（PC）と入力端末からなる検証用装置、および、F-paper から構成される。検証用装置は、磁性ファイバにより生成される物理的特徴から得られる固有パターンと、記録エリアに記録されている ID コードを PC へ受け渡す。PC は、当該 ID コードに対応して予め PC 内のデータベースに記録されている参照データにより、受け渡された固有パターンを検証する。この検証結果を基に、F-paper を受理するか、または、拒否するかの判定を行う。

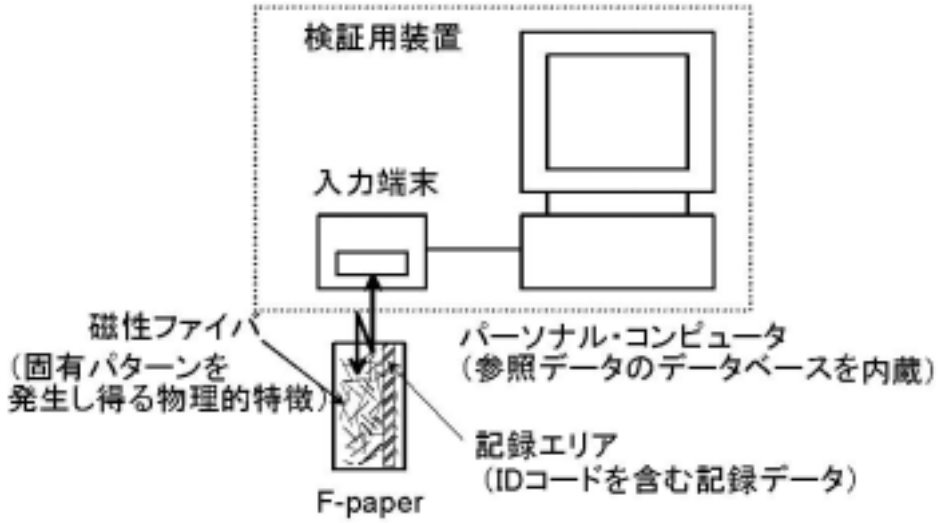

図 5.6　**評価対象システムⅡの構成**

ロ．評価における前提条件

以下の前提条件の下で、システムの安全性評価を行う。

(b-1) 攻撃者は発行者と結託しない。また、セキュリティ管理により検証用装置の安全が保たれており、攻撃者が、検証用装置を改造したり、データベース上の参照データを改ざんしたりすることはできない。

(b-2) 攻撃者は、F-paper から得られる固有パターンを観察するために、別途入力端末を利用できる。

(b-3) 攻撃者は、F-paper から得られる固有パターンの特徴抽出方法やパターン照合方法を知ることができず、実際の検証用装置でクローンの有効性を確かめるしかないこととする。

このように、攻撃者は入力端末を利用して固有パターンを観察可能であり、ここでの前提条件は４章で説明した「攻撃条件 2」に対応する。

ハ．想定される攻撃

前提条件(b-1)により、攻撃者は検証用装置にアクセスできないので、評価対象システムⅡに対しては、図 5.7 に示すような攻撃が想定される。

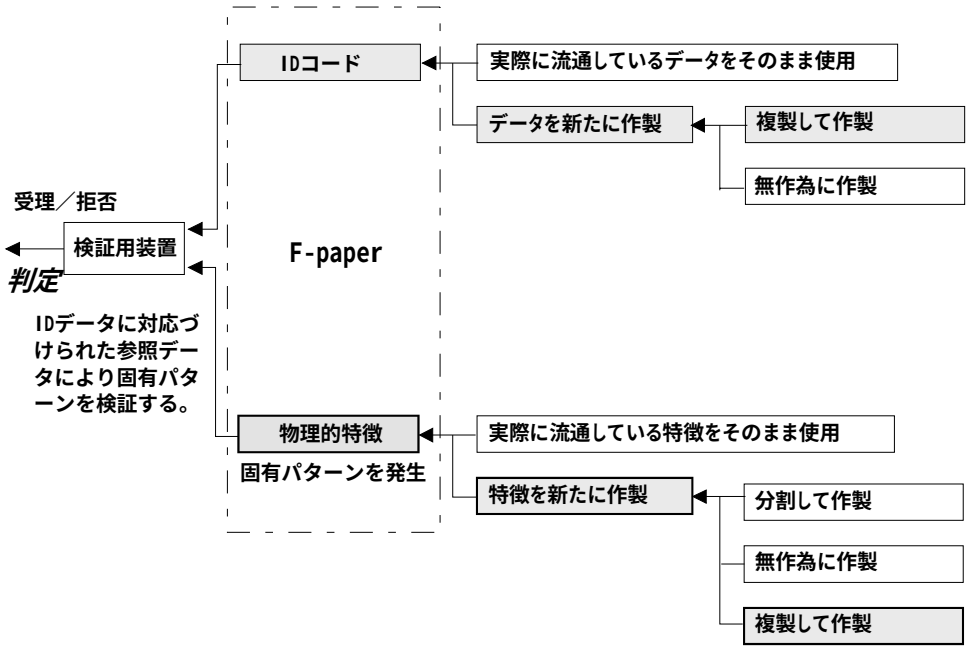

図 5.7　**評価対象システム**Ⅱ**に対する攻撃**

検証用装置には F-paper が提示され、検証用装置は、F-paper の記録データから得られる ID データによりデータベースから参照データを得て、物理的特徴から得られる固有パターンを検証する。「攻撃者が作製した F-paper のクローンにより検証用装置から受理の判定を 1 回でも得た場合」を攻撃成功と考える。攻撃者に有利になるように、ID コードは容易に複製して用いることができるとすると、攻撃者がいかにして本物に近い物理的特徴を作製できるかが攻撃の成功の鍵を握る。本物の F-paper の物理的特徴を見本としてクローンを作製（複製）して攻撃する場合、無作為に物理的特徴を作製するよりも、攻撃成功の可能性は高くなると考えられる。また、検証される物理的特徴部位を分割して用いる場合に比べて、より多くのクローンを効率的に得られる可能性も高くなるとも考えられる。以上より、評価システムⅡについて、「複製した ID コードと複製した物理的特徴を組み合わせてクローンを作製して提示する攻撃」（デッドコピー攻撃、４章の「攻撃 3」に対応）に対する安全性を検討する。

ニ．デッドコピー攻撃

磁性材料を用いて物理的特徴を複製して作製したクローンの受入率を実験的に確かめることで、評価対象システムⅡのデッドコピー攻撃に対する評価を行う。図 5.8 に示すように、F-paper は、紙片に磁性ファイバをランダムに内在させたものであり、入力端末により得られる固有パターン $y[n]$ は、F-paper に存在する磁気量の入力 $x[n]$ により制御できる制御系の出力とみなすことができる。そこで、攻撃者が市販の磁性材料を入手し、市販のディスペンサ・ロボットを利用できることを想定し、入力端末を利用して固有パターンを観察しながら磁性量を線形的に制御して作製したクローンに対する評価を行う。ここで、より多額の投資を行ってより高精度な装置やより精密な制御を行うことも可能と考えられるが、対策を講じるべき攻撃のレベルとして、以上のような攻撃者の具体的な能力を設定した。

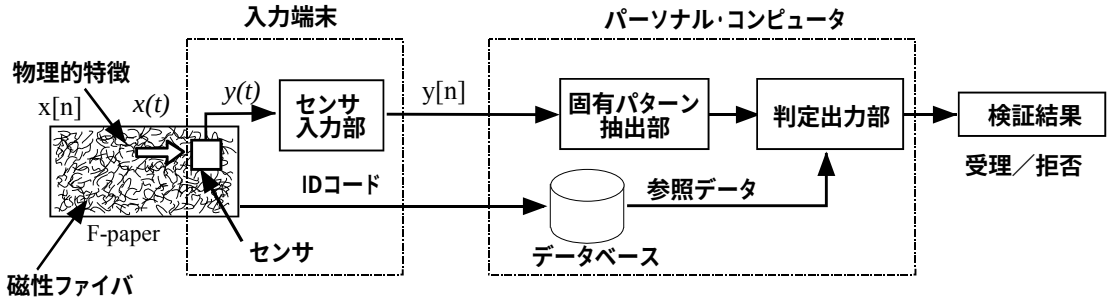

図 5.8　評価対象システムⅡのブロック図

以下にデッドコピー攻撃の手順を示す。

【手順 1】インパルス応答の測定

図 5.9 に示すように、単位入力 $\delta[n]$ によってロボットを制御し、単位量の磁性材料を紙片に塗布したものを入力端末で走査して、入力端末の擬似インパルス応答 $h_1[n]$ を測定する[7]。

[7] ロボットの制御における位置決め誤差や入力端末における検出誤差が含まれるため、“擬似インパルス応答”と表現している。

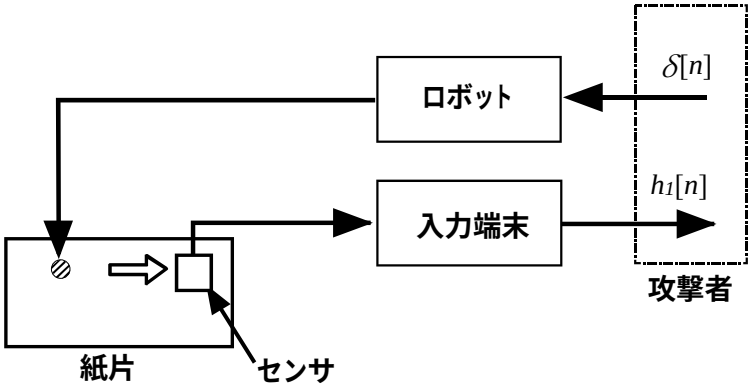

図 5.9　**インパルス応答の測定**

【手順 2**】見本波形の測定**

図 5.10 に示すように、見本とする F-paper を入力端末で走査して、固有パターンの見本波形 $y_1[n]$ を測定する。

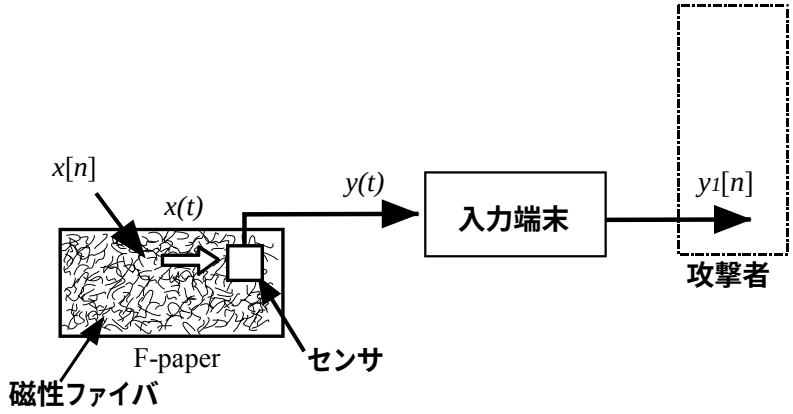

図 5.10　**見本波形の測定**

【手順 3**】制御入力の計算**

擬似インパルス応答 $h_1[n]$ と見本波形 $y_1[n]$ を用いて以下の関係から、制御入力 $x_1[n]$ を計算する。

$$\boldsymbol{x}_1 = \boldsymbol{h}_1^{-1} \cdot \boldsymbol{y}_1 . \tag{5.4}$$

ここで、 $\boldsymbol{x}_1 = (x_1[0], x_1[1], \ldots, x_1[N])^t$、 $\boldsymbol{y}_1 = (y_1[0], y_1[1], \ldots, y_1[N])^t$、

$$\boldsymbol{h}_1^{-1} = \begin{bmatrix} h_1[0] & 0 & \cdots & 0 \\ h_1[1] & h_1[0] & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ h_1[N] & h_1[N-1] & \cdots & h_1[0] \end{bmatrix}^{-1}$$

とする。なお、N は自然数とする。

【手順 4】物理的特徴の複製

図 5.11 に示すように、計算した制御入力 $x_1[n]$ によりロボットを制御して、紙片に磁性材料を塗布することで物理的特徴を複製し、複製固有パターン $y_2[n]$ を得る。

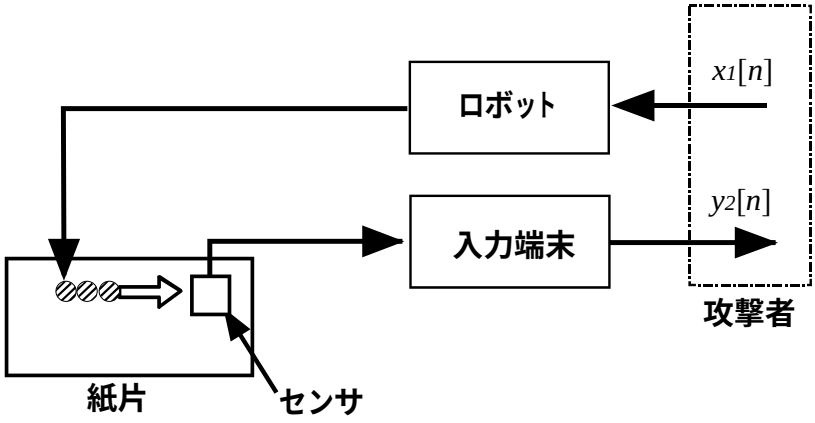

図 5.11　物理的特徴の複製

【手順 5】クローンの作製

見本とした F-paper の ID コードを複製して複製固有パターンと組み合わせて、F-paper のクローンを作製する。

ホ．デッドコピー攻撃の対するセキュリティ評価

実験に用いた機器構成とロボットの仕様を図 5.12、表 5.1 にそれぞれ示す。ロボットは 3 軸ロボットで、先端にニードルを装着し、容器に入れた磁性材を先端に付着させて紙片に塗布する形で動作させて用いた。磁性材は、工業用に市販されている酸化鉄を主成分とする磁性粉末を用い、紙片は事務機器用のコピー用紙を用いた。磁性粉末は、安定した塗布ができるように水に溶かし、整髪用ジェルを混ぜて粘度を調整した。

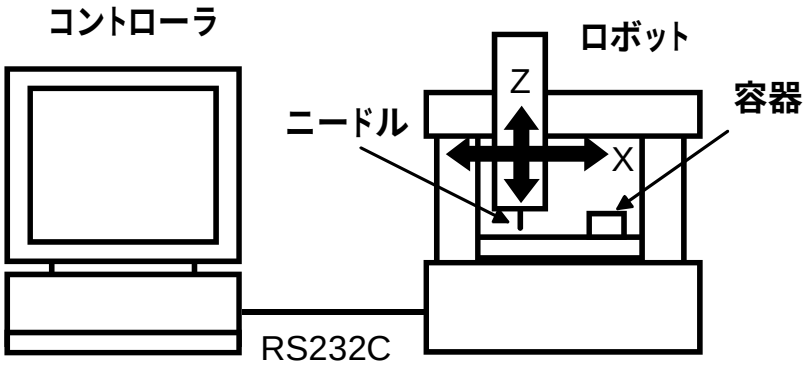

図 5.12 **実験に用いた機器構成**

表 5.1 **ロボットの仕様**

項目	仕様
動作範囲	X: 200mm Y: 200mm Z: 50mm
位置決め精度	X, Y: >±0.05mm, Z: >±0.05mm
搬送速度	X, Y: 1～500mm/sec, Z: 1～200mm/sec
分解能	0.0125mm/pulse

図 5.13 に示すように、磁性材は、入力端末内のセンサにより走査される紙片上の位置を中心に点状に塗布する。制御入力 $x_1[n]$により、走査線と塗布位置の距離を線形制御することで、磁性入力の強弱を調整する。

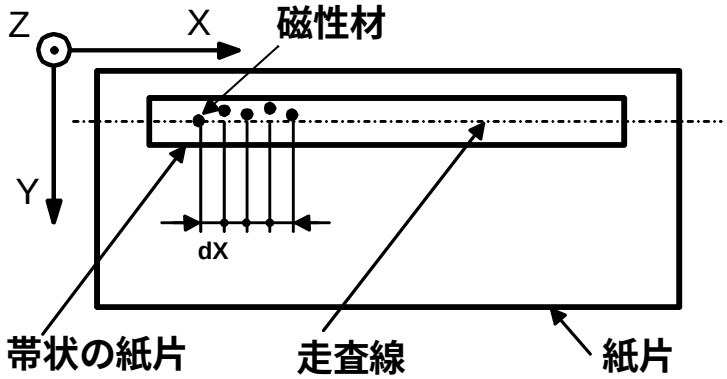

図 5.13 **磁性材の塗布位置**

図 5.14 の写真は、帯状の紙片へ磁性材を塗布している様子を示している。図 5.15 の写真は、帯状の紙片を F-paper と同一寸法の紙片に貼り付けて作製したクローンの外観である。

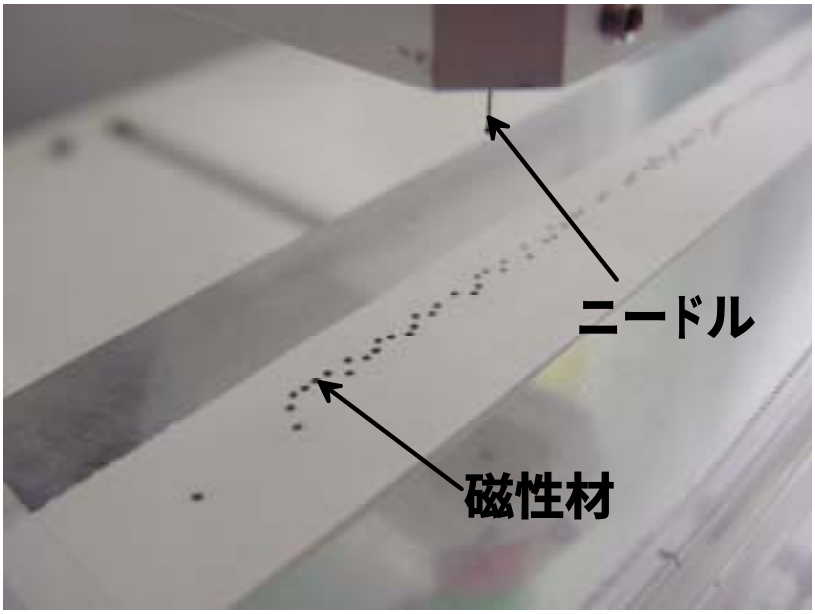

図 5.14 **磁性材を塗布している様子**

図 5.15 **作製したクローンの外観**

磁性材を走査線の中心に 1 点だけ塗布した場合には、図 5.16 に示すような擬似インパルス応答が入力端末から得られる。複数の磁性材が塗布されたクローンを読み取る場合には、こうした応答が重なり合って複雑な波形が得られることとなる。

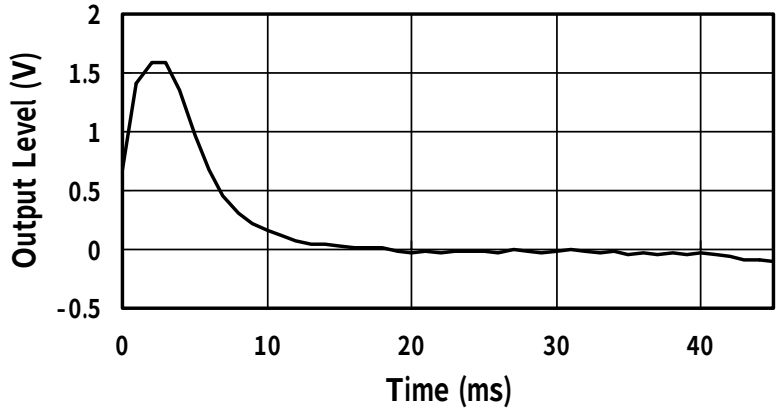

図 5.16 **入力端末の擬似インパルス応答**

作製したクローンから得られた固有パターンの一例を図 5.17 に示す。この例では、作製したクローンの固有パターン（破線）は、見本とした F-paper の固有パターン（実線）に類似しており、距離が大きくなるにつれて、制御の誤差が大きくなっている。

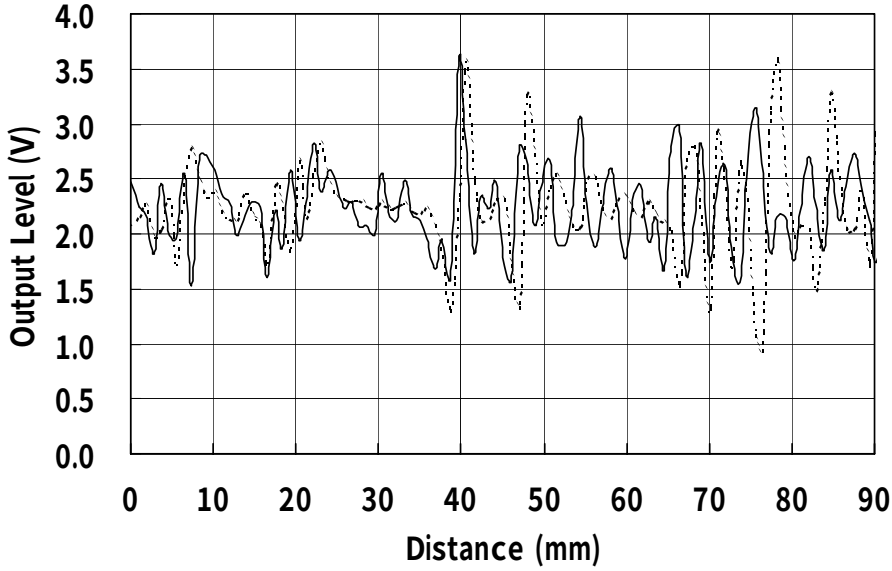

図 5.17 **見本とした固有パターン（実線）と**
クローンから得られた固有パターン（破線）

作製したクローンがどの程度の割合で受け入れられるかが、デッドコピー攻撃の成功率であり、その評価指標としてクローン一致率（CMR）を用いる。

$$CMR = n_a / n_t . \qquad (5.5)$$

ただし、n_t はクローンの検証回数、n_a はクローンが受理された回数である。

100 枚のクローン紙片を作製して、パターン照合の範囲を d=20、40、80（それぞれ長さ 3.5mm、7.0mm、14mm に相当、検証回数 n_t はそれぞれ 2000、1300、300 回に相当）とした場合について、評価対象システムⅡでパターン照合を行った。その結果として得られたクローン一致率を図 5.18～図 5.20 に示した。図中の誤一致率と誤不一致率は、評価対象システムⅡについてクローンが存在しない状態で評価を行った際に得られたものである。なお、どの図もクローン一致率の曲線も途中で切れているが、これは、評価に用いたクローン紙片の数の制約によって計測不可能となった部分があることによる。

図 5.18～図 5.20 を比較すると、まずクローンが存在する場合の等誤り率（クローン一致率と誤不一致率が一致する場合の等誤り率）が、クローンが存在しない場合の等誤り率（誤一致率と誤不一致率が一致する場合の等誤り率）に比べて大きくなっていることがわかる。図 5.18 の場合（d=20 のケース）、クローンが存在する場合の等誤り率は 1.0×10^{-1} であり、クローンが存在しない場合の等誤り率（1.5×10^{-2}）よりも大きい。また、各図のクローン一致率を比較すると、パターン照合の範囲を大きくする（d を大きくする）につれて、クローン一致率も低下する傾向にあることも読み取れる。

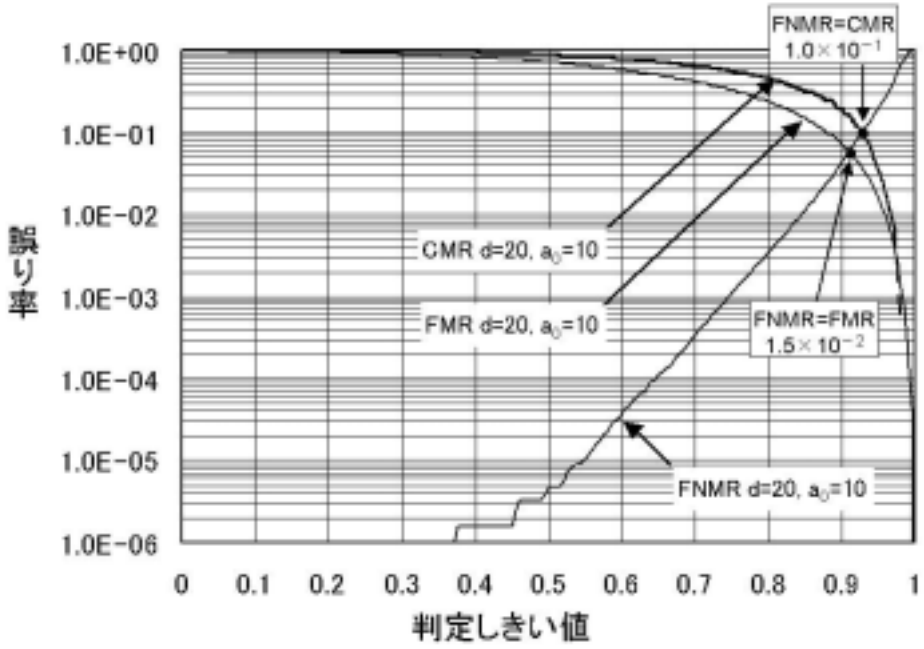

図 5.18　**評価対象システムⅡの** CMR(d=20)

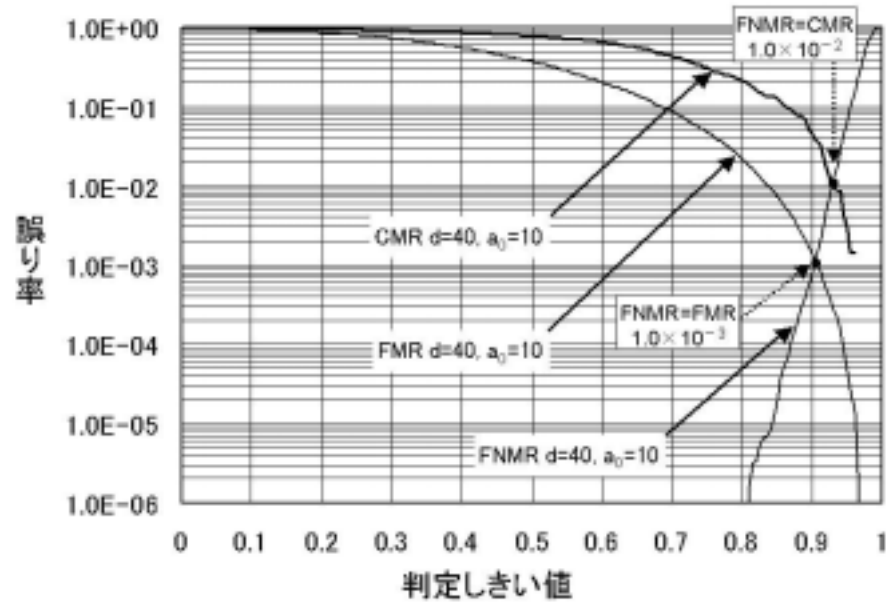

図 5.19　**評価対象システムⅡの** CMR(*d*=40)

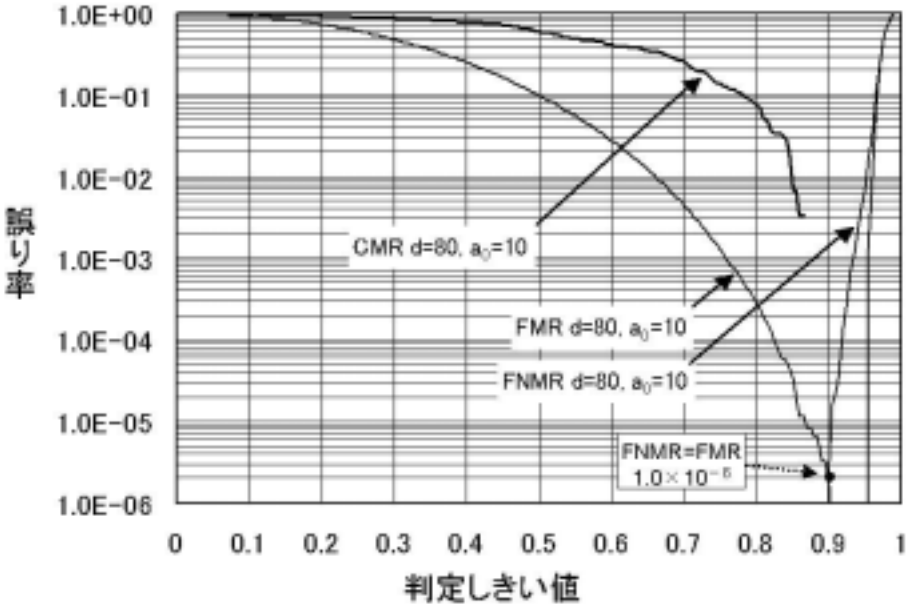

図 5.20　**評価対象システムⅡの** CMR(*d*=80)

次に、パターン照合の範囲 d とパターン照合の分解能 a_0 を変化させた場合について、クローン一致率を以下の図 5.21～図 5.23 に示した。これらの図をみると、d や a_0 のパラメータを変化させた場合に、①誤一致率はほとんど変化しないが、クローン一致率が著しく変化するケース（図 5.21）や、②誤一致率は著しく変化する一方、クローン一致率はほとんど変化しないケース（図 5.22、図 5.23）が観察されている。こうしたケースがどのような要因に

よって引き起こされるかを明らかにするためには追加的な検討を行う必要があるものの、「誤一致率や誤不一致率によって示される認証精度からクローン一致率を類推することは困難である」点は明らかである。

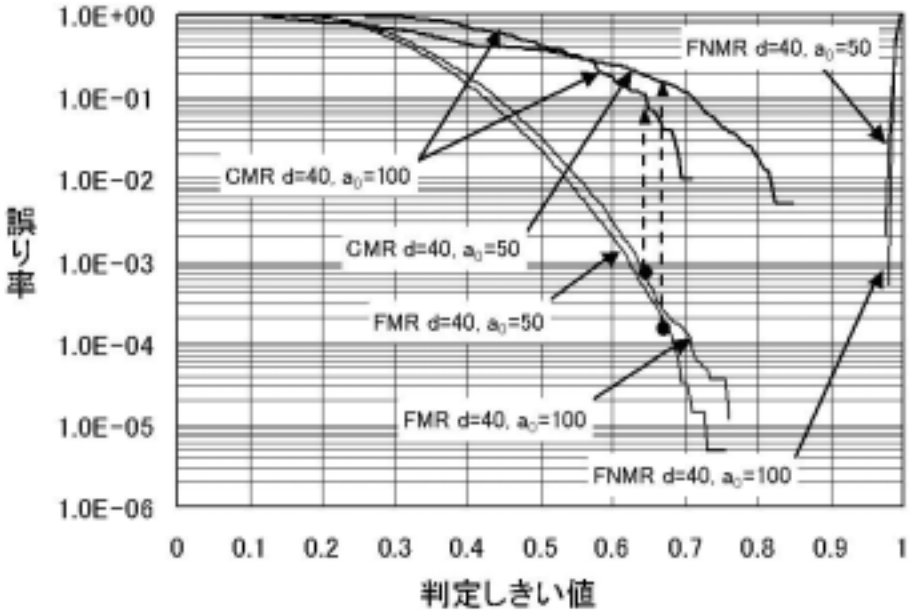

図 5.21　**評価対象システム**Ⅱ**の** CMR;
(d=40, a_0=50)**と**(d=40, a_0=100)**の比較**

図 5.21～図 5.23 をやや詳しくみる。まず、図 5.21 は、パターン照合の範囲を表わすパラメータ d を 40 に固定した上で、パターン照合の分解能 a_0 を変化させた場合（a_0=50, 100）を示している。読取り部分の長さは、a_0=50 の場合には 35.0mm、a_0=100 の場合には 70.0mm である。a_0 が大きくなると、誤一致率はほとんど変化しないものの、クローン一致率は、判定しきい値 0.5～0.6 あたりを境に逆転している。すなわち、判定しきい値 0.5 以下では、a_0=100 の場合のクローン一致率が相対的に小さく、判定しきい値 0.6 以上では、逆に a_0=100 の場合のクローン一致率が相対的に小さくなっている。

図 5.22 は、固有パターンの読取り部分の長さを一定（35.0mm）に固定し、パターン照合の範囲と分解能のパラメータを同時に変化させた場合を示している。パラメータ設定は、(d, a_0)=(40, 50)の場合と(d, a_0)=(20, 100)の場合の 2 通りである。誤一致率に着目すると、パターン照合の分解能のパラメータが大きくなると、誤一致率が著しく小さくなっているものの、クローン一致率の低下は限定的となっている。

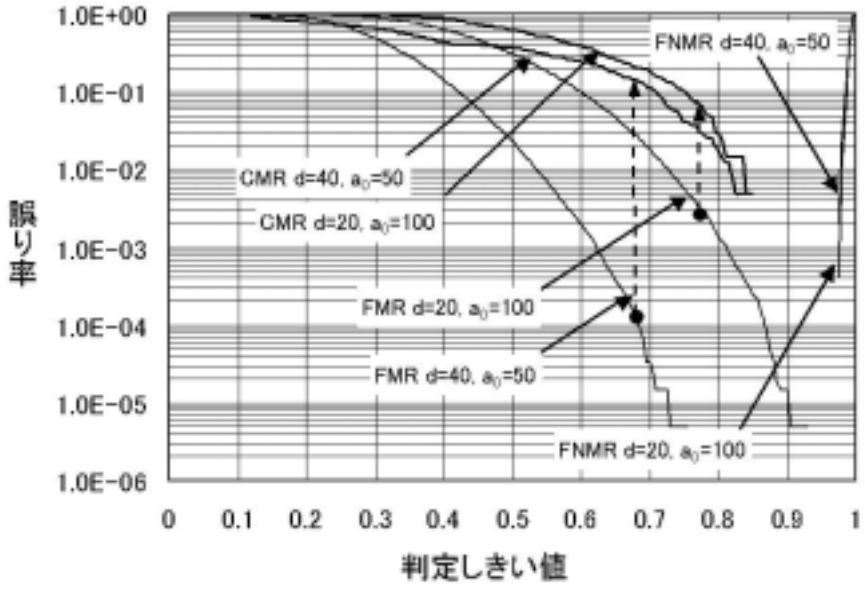

図 5.22　**評価対象システムⅡの** CMR;
(d=20, a_0=100)と(d=40, a_0=50)の比較

図 5.23 では、図 5.22 と比較的似た傾向がみられる。図 5.23 は、固有パターンの読取り部分を固定しないで、2 つのパラメータを同時に変化させた場合を示している。パラメータ設定は、(d, a_0)=(40, 10)の場合（読取り部分の長さは 7.0mm）と(d, a_0)=(20, 50)の場合（読取り部分の長さは 17.5mm）の 2 通りである。(d, a_0)=(20, 50)の場合、(d, a_0)=(40, 10)の場合に比べ、誤一致率が著しく小さくなっているものの、クローン一致率はほぼ同一の水準となっている。

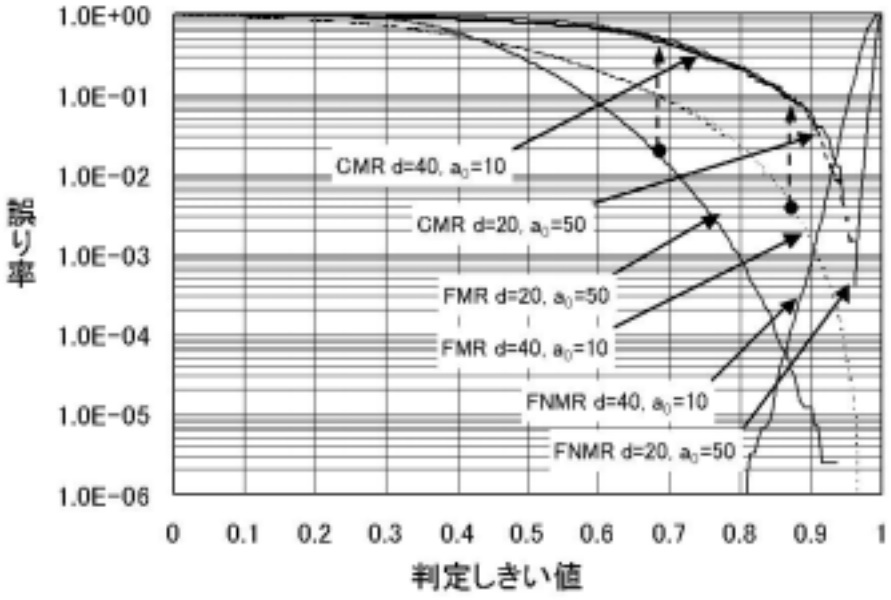

図 5.23　**評価対象システムⅡの** CMR;
(d=20, a_0=50)**と**(d=40, a_0=10)**の比較**

以上より、①クローン一致率は誤一致率に比べて大きな値となる傾向にある、②各種パラメータを変化させた場合に、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、という 2 点が明らかになった。したがって、デッドコピー攻撃に対するセキュリティ評価を行う際には、誤一致率を測定するだけでなく、アプリケーションにおいて想定される環境を考慮した上でクローン一致率を測定し、許容される水準以下にクローン一致率を抑えるようにパラメータを選択する必要がある。

（4）評価事例のまとめ

最後に、本章で紹介した評価結果を整理する。

ブルートフォース攻撃は、検証対象以外のものを無作為に提示する攻撃であり、例えば、紙幣をカラー複写機、PC、スキャナーやプリンターなどを用いて複製するといったような攻撃と同様に、偽造に関する知識や技能のない素人でも容易に実行できる攻撃（カジュアル攻撃と呼ばれる）の 1 つである。したがって、人工物メトリック・システムを構築する上で、ブルートフォース攻撃は、必ず想定しなければならない攻撃であり、各アプリケーションに応じた利便性やコストの観点から、そのセキュリティ評価が行われるべきである。本章で述べた評価事例のように、誤一致率を測定した上で、想定されるブルートフォース攻撃の攻撃成功率を計算することによって、利便性やコストの目標に照らし合わせて、照合アルゴリズムを調整しながら「どの程度の攻撃成功率まで許容するか」を検討することが可能である。

一方、デッドコピー攻撃は、攻撃に使用する材料や装置など、ある程度の準備立てが必要な攻撃であり、ブルートフォース攻撃に比べると一般的にはコストを要する攻撃である。本章で紹介したデッドコピー攻撃に対する評価事例では、「この程度の攻撃にはセキュリティを保ちたい」という観点から、攻撃者が利用可能な磁性材料、工業用ロボットやその制御方法についての条件がまず設定され、その上で実際にクローン一致率が測定された。もちろん、アプリケーションによっては、攻撃に利用可能な材料、装置、制御方法などに関する条件が今回の評価事例の条件と異なるケースも想定される。実際のクローン一致率の測定では、どのような条件が適切かを十分に考慮することが必要である。

今回の評価事例から､2 つのインプリケーションを導くことができる｡1 つは、「クローン一致率が誤一致率に比べて大きくなる傾向にある」という 点である。もう 1 つは、「誤一致率や誤不一致率を測定したからといって、それらの指標からクローンに対するセキュリティ・レベルを評価することが困難なケースがある」という点である。したがって、攻撃者が利用可能な材料や装置などを限定

することが困難な場合であっても、具体的に攻撃者の能力を想定した上で、デッドコピー攻撃を加味した認証精度の評価を行うことが重要である。その上で、アプリケーションにおいて許容されるセキュリティ・レベルをクリアしているかどうかを確認するとともに、クリアしていない場合には、固有パターンの読取りやパターン照合などに関するパラメータの設定を見直すことが求められる。このような意味から、今回紹介した評価事例を参考にしてデッドコピー攻撃への対応を検討していく必要があろう。

６．おわりに

人工物メトリクスは、紙やカードなどの耐偽造性を向上させる有用な技術であり、今後金融分野においても有効に活用していくことが望まれる。その際には、セキュリティ、利便性、コスト、社会的受容性の観点から十分な評価を行い、アプリケーションの各種要件に見合った技術を採用することが求められる。

本論文では、こうした観点から、人工物メトリクスの概念や特徴を整理するとともに、認証精度評価の現状と今後の課題について述べ、人工物メトリクスの評価基盤を確立していく上での問題提起を行った。特に、人工物のクローンを利用した攻撃を前提とした認証精度の評価の研究が重要である点を指摘し、そうした研究の推進力を高める上で、研究成果について学会等のオープンな場で議論することが有用であることを強調した。

また、今後人工物メトリクスの認証精度の評価手法を確立・活用していく上で、バイオメトリクスの動向に注目しておくことも重要である。バイオメトリクスの分野では、認証精度評価に関する国際標準の審議が開始されており、認証精度基盤の確立に向けた取組みという点において人工物メトリクスよりも進んでいる。こうした先行事例を参考にして人工物メトリクスの検討を行うことが有用であろう。

以 上

【参考文献】

青柳真紀子・竹村泰司・松本勉（横浜国立大)、「磁性繊維を用いた人工物メトリック・システムのモデル化と数値解析」、『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、573～578 頁

大島康志・松本勉、「ユーザ認証における非常時通報」、『電子情報通信学会技術研究報告』ISEC2003-52、電子情報通信学会、2003 年、17～22 頁

情報処理振興事業協会、『暗号技術評価報告書（2002 年度版)』、2003 年（http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/c02_2.pdf）

瀬戸洋一（編著)、『ユビキタス時代のバイオメトリクスセキュティ』、日本工業出版、2003 年

日本工業標準調査会、『TR X 0036-1：IT セキュリティマネジメントのガイドライン－第 1 部：IT セキュリティの概念及びモデル』、日本規格協会、2001 年

――、『TR X 0053：指紋認証システムの精度評価方法』、日本規格協会、2002 年 a

――、『TR X 0072：虹彩認証システムの精度評価方法』、日本規格協会、2002 年 b

星野哲・遠藤由紀子・松本弘之・松本勉（横浜国立大)、「指紋画像からの人工指作製（その２)」、『2002 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、2002 年、821～826 頁

松本勉（横浜国立大)・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、〇～〇頁

――・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

――・田中直樹、「計算の実行ハードウェアを確認する方法」、『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、2000 年 10 月、199～204 頁

――・――、「計算実行ハードウェアの物理的仮定に基づく認証」、『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 1 月、613～618 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

三村昌弘・高橋健太・磯部義明・瀬戸洋一、「生体認証における脅威および脆弱性に関する

分析」、『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、43～47 頁

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』ISEC 2000-45、電子情報通信学会、2000 年 a、159～116 頁

―――・―――・―――、「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、2000 年 b、109～114 頁

―――・―――・―――、「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

Aoyagi, Makiko, Tsutomu Matsumoto (Yokohama National University) and Yasushi Takemura, “A Numerical Model to Efficiently Evaluate the Accuracy of Authentication of a Magnetic Artifact-metric System for Document Security,” *9th Joint MMM-Intermag Conference*, GW-2, 2004.

Bolle, Ruud M, Jonathan H connell, Sharath Pankanti, Nalini K Ratha and Andrew W Senior, *Guide to Biometrics*, Springer Professional Computing, 2003.

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

Common Criteria Biometric Evaluation Methodology Working Group, *Biometric Evaluation Methodology Supplement* (BEM), Version 1.0, August 2002.

European Committee for Banking Standards, *TR* 400: *Biometrics: A snapshot of Current Activity* - 1996, 1996.

Fernandez, Alberto J., Xtec Incorporated, *Data Verification Method and Magnetic Media*, patent number US5235166, 1993.
(http://www.mediametrics.com/technologies/magneticmediametrics.html)

―――, *Method and apparatus for securing data stored in semiconductor memory cells*, patent number US 5644636, 1997.
(http://www.mediametrics.com/technologies/memorymediametrics.html)

Goldman, Robert N., Light Signatures Inc., *Non-counterfeitable Document System*, patent number US4785290, 1988.

Hayosh, Thomas D., “Self-Authentication of Value Documents,” *Proceedings of SPIE*, 3314, 1998, pp.140-149.

Inedk, Ronaldo S., Marcel W. Moller, George L. Engel and Alan L. Hege, Washington Univ. St. Louis, *Method and Apparatus for Fingerprinting and Authenticating Various Magnetic Media*, patent number US5428683, 1995.

International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 13335-1: Information technology – Security techniques – Guidelines for the management of IT Security ― Part 1: Concepts and models for IT Security*, 1996.

――― and ―――, *ISO/IEC 15408-1: Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general models*, 1999a.

——— and ———, *ISO/IEC 15408-2: Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements*, 1999b.

——— and ———, *ISO/IEC 15408-3: Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements*, 1999c.

——— and ———, *ISO/IEC 17799: Information technology – Security techniques – Code of practice for information security systems*, 2000.

Jain, Anil K., Ruud Bolle and Sharath Pankanti, *Biometrics: Personal Identification in Networked Society*, The Kluwer Academic Publishers, Jain, Anil K. *et al.* eds., 1999.

Kong, Anne, Andrea Griffith, David Rhude, Gary Bacon and Swati Shah, *DoD and Federal Biometric System Protection Profile for Medium Robustness Environments*, March 2002.

Maltoni, Davide, Dario Maio, Anil K. Jain and Salil Prabhakar, "Fake Finger Attacks," *Handbook of Fingerprint Recognition*, Springer-Verlag, Maltoni, D. et al. eds., Chapter 9, 2003, pp.286-291.

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.

———, Keiichi Suzuki and Tsutomu Matsumoto (Yokohama National University), "A Clone Preventive Authentication Technique Which Features Magnetic Micro-fibers and Cryptography," *Proceedings of SPIE*, 3314, 1998, pp.275-286.

———, 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.

National Institute of Standards and Technology, *FIPS PUB 140-2: Security Requirements For Cryptographic Modules*, May 25, 2001. (http://csrc.nist.gov/publications/fips/fips1402.pdf)

National Material Advisory Board: Commission on Engineering and Technical Systems, National Research Council, *Counterfeit Deterrent Features for the Next-Generation Currency Design*, Publication NMAB-472, National Academy Press 1993, pp.74-75.

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

ORBID Corporation B. V., "3DAS ORBID," http://www.orbidcorp.com/products/3das.asp, access

date: March 9, 2004.

Poli, David L., "Security Seal Handbook," *Sandia Report*, SAND78-0400, Sandia National Laboratory, 1978, pp.1-44.

van der Putte, Ton and Jeroen Keuning, "Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned," *SMART CARD RESEARCH AND ADVANCED APPLICATIONS*, *IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications*, 2001, pp. 289-303.

van Renesse, Rudolf L. "3DAS: A 3Dimensional-structure Authentication System," *ECOS*95, European Convention on Security and Detection, Brighton UK, 1995.

Samyn, Johan, N. V. Bekaert S.A., *Method and Apparatus for Checking the Authenticity of Documents*, patent number US4820912, 1989.

Sinha, Dipen N., "Acoustic resonance spectroscopy (ARS)," *IEEE POTENTIALS*, 1992, pp. 10-13.

Sinha, Dipen N. and Kenneth E Apt, "Acoustic resonance spectroscopy in Verification Technologies," *DOE/Office of Arms Control and Nonproliferation report*, DOE/DP/OAC/VT-92A, 1992, pp. 52-58.

United Kingdom Government Biometrics Working Group, *Biometric Device Protection Profile*, Draft Issue 0.82, September 2001.

Valencia, Valorie S., "Biometric Liveness Testing, " *BIOMETRICS: Identity Assurance in the Information Age*, McGraw-Hill, John D. Woodward, Jr. *et al.* eds., Chapter 8, 2003, pp.139-149.

付録： 評価対象システムにおける照合アルゴリズム

５章で評価を行った磁性ファイバを紙に分散させた証書を利用する人工物メトリック・システム（評価対象システムⅠ、Ⅱ）が人工物の検証に採用した照合アルゴリズムを以下に示す。

- **固有パターンの抽出**

センサ入力部を通じて検証用装置は、AD 変換後の生データ

$$\boldsymbol{r} = (r_1, r_2, \ldots, r_n)^t \tag{A1}$$

を受け取る。ここで、r_i $(i = 1, 2, \ldots, n)$ は、i 番目の生データを示す。

検証用装置は、グリッジ・ノイズを除去するため、生データ $\boldsymbol{r}$ を $a_0 (\geq 1)$ 個の要素ごとに平均をとり、

$$\boldsymbol{c} = (c_1, c_2, \ldots, c_m)^t \tag{A2}$$

として、データ圧縮する。ここで、c_j $(j = 1, 2, \ldots, m)$は、j ブロックの平均値を示し、

$$c_j = \frac{1}{a_0} \sum_{i=(j-1)a_0+1}^{j \cdot a_0} r_i \tag{A3}$$

と表わされる。$\boldsymbol{c}$ より、連続する d $(1 \leq d \leq m)$ 個の要素を組み合わせて、固有パターン

$$\boldsymbol{P}_{d,k} = (c_k, c_{k+1}, \ldots, c_{k+d-1})^t \tag{A4}$$

を抽出する。ここで、$1 \leq k \leq m$、$k + d - 1 \leq m$ である。

- **参照データの登録処理**

同一の F-paper を検証用装置に読み込ませることで、参照データ $\hat{\boldsymbol{P}}_{d,r}$ が作成される。ここで、添え字 r は、参照位置を $k = r$ とすることを示す。検証用装置は、得られた $M (\geq 1)$ 個の固有パターン $\boldsymbol{P}_{d,r}^i$（$i = 1, 2, \ldots, M$）について、$\boldsymbol{P}_{d,r}^i$ の k 番目の要素を

$$p_k = \frac{1}{M} \sum_{i=1}^{M} c_k^i \tag{A5}$$

として平均化する。ここで、$k = r, r+1, \ldots, r+d-1$ である。

結果として、以下のような参照データ $\hat{\boldsymbol{P}}_{d,r}$ を生成し、記録する。

$$\hat{\boldsymbol{P}}_{d,r} = (p_r, p_{r+1}, \ldots, p_{r+d-1})^t \tag{A6}$$

- **固有パターンの照合処理**

検証用装置は、提示された F-paper について、それから新たに得られる固有パターンと予め記録されている参照データを用いて、相関係数によるパターンマッチング処理を行う。まず、提示された F-paper から圧縮データ $\boldsymbol{c} = (c_1, c_2, \ldots, c_m)^t$ を得て、固有パターン $\boldsymbol{P}_{d,r} = (c_r, c_{r+1}, \ldots, c_{r+d-1})^t$ が抽出される。次に、予め記録されている参照データの対応する参照位置から、$\hat{\boldsymbol{P}}_{d,r} = (p_r, p_{r+1}, \ldots, p_{r+d-1})^t$ を抽出し、パターンマッチングの計算を行う手順で行われる。新たに得られた固有パターン $\boldsymbol{P}_{d,r}$ と参照データ $\hat{\boldsymbol{P}}_{d,r}$ の類似度 $S(\boldsymbol{P}_{d,r}, \hat{\boldsymbol{P}}_{d,r})$ は

$$S(\boldsymbol{P}_{d,r}, \hat{\boldsymbol{P}}_{d,r}) = \frac{\sum_{i=r}^{r+d-1}(c_i - \bar{c}_r)\cdot(p_i - \bar{p})}{\sqrt{\sum_{i=r}^{r+d-1}(c_i - \bar{c}_r)^2}\cdot\sqrt{\sum_{i=r}^{r+d-1}(p_i - \bar{p})^2}} \tag{A7}$$

として計算する。ここで、$\bar{c}_r$ と $\bar{p}$ は、それぞれ $\boldsymbol{P}_{d,r}$ と $\hat{\boldsymbol{P}}_{d,r}$ の各要素の平均値である。

さらに、実際の照合処理では、入力端末の搬送のぶれなどによって照合位置がずれるため、検証用装置は、F-paper から $(2s+1)$ 個の固有パターン $\boldsymbol{P}_{d,(r-s)}, \boldsymbol{P}_{d,(r-s+1)}, \ldots, \boldsymbol{P}_{d,r}, \ldots, \boldsymbol{P}_{d,(r+s-1)}, \boldsymbol{P}_{d,(r+s)}$ を抽出して照合を行う。ここで、$s(\geq 0)$ は、圧縮データ $\boldsymbol{c}$ から固有パターンを抽出する際の抽出位置のシフト数である。その結果、類似度は、

$$S_{\min}(\boldsymbol{P}_{d,r}, \hat{\boldsymbol{P}}_{d,r}) = \min_{-s\leq k\leq s} S(\boldsymbol{P}_{d,(r+k)}, \hat{\boldsymbol{P}}_{d,r}) \tag{A8}$$

として計算する。ただし、参照位置 r は、$s+1 \leq r \leq m-d-s+1$ である。

結局、検証用装置は、提示された F-paper の判定を行うにあたり、予め設定した類似度のしきい値 α を基に、$S_{\min}(\boldsymbol{P}_{d,r}, \hat{\boldsymbol{P}}_{d,r}) > \alpha$ となった場合、判定結果を受理とし、それ以外の場合は、拒否とする。