IMES DISCUSSION PAPER SERIES

偽造防止技術の中の人工物メトリクス：
セキュリティ研究開発の動向と課題

宇根正志（うねまさし）・田村裕子（たむらゆうこ）・松本 勉（まつもとつとむ）

Discussion Paper No. 2009-J-2

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2009-J-2
2009 年 3 月

偽造防止技術の中の人工物メトリクス：セキュリティ研究開発の動向と課題

宇根正志（うねまさし）*・田村裕子（たむらゆうこ）**・松本 勉（まつもとつとむ）***

要　　旨

個人の預金取引においてキャッシュカードや預金通帳が利用されるように、金融取引においてはさまざまな人工物が利用されている。これらは当該取引の安全性や信頼性を確保するうえで、重要な役割を果たしていることが多い。特に、偽造キャッシュカード問題の事例に代表されるように、人工物が偽造され不正使用された場合には金融取引に影響が出る可能性があり、人工物の偽造が困難であることが重要なセキュリティ要件となる。その意味で、人工物の偽造がどの程度困難か（耐クローン性）を客観的に評価できる技術が望ましい。

耐クローン性の評価という点で、人工物メトリクスは新しいタイプの偽造防止技術として近年注目を集めている。人工物メトリクスは、各人工物に固有の特徴を利用して認証を行う技術であり、2000 年以降急速に研究開発が進展している。本技術のポイントは、各人工物における制御困難な特徴を認証に利用することによって、耐クローン性を低下させることなく当該技術の詳細な情報を公開できると期待される点である。最近では、具体的な手法の提案やセキュリティ評価結果の報告が学会において行われ、活発に議論されている。

本稿では、こうした人工物メトリクスの研究開発の動向について耐クローン性評価の観点から説明するとともに、偽造防止に利用される印刷技術、光学素子（ホログラム）の技術、暗号ハードウエアの耐タンパー技術、人工物メトリクスの類似技術であるバイオメトリクスの動向を説明する。そのうえで、人工物メトリクスにおける耐クローン性の評価方法確立に向けた今後の課題を示す。

キーワード：暗号ハードウエア、印刷、偽造防止技術、人工物メトリクス、セキュリティ、バイオメトリクス、ホログラム

JEL classification: L86、L96、Z00

*　日本銀行金融研究所企画役（E-mail: masashi.une@boj.or.jp）

**　日本銀行金融研究所

***　横浜国立大学大学院環境情報研究院（E-mail: tsutomu@ynu.ac.jp）

本稿は、2009 年 3 月 11 日に日本銀行で開催された「第 11 回情報セキュリティ・シンポジウム」への提出論文に加筆・修正を施したものである。本稿を作成するに当たり、独立行政法人国立印刷局研究所の山越学副主任研究員と木村健一副主任研究員から有益なコメントを頂戴した。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

目　次

１．はじめに

金融取引にはさまざまな人工物が使われている。例えば、通常の個人の預金取引においてはキャッシュカードや預金通帳が利用されているほか、個人が金融取引を金融機関と開始する際には、当該個人の本人確認用として、住民票、運転免許証、健康保険証等の提示が求められるケースがある。これらの人工物は金融取引の安全性や信頼性を確保する手段として従来から重要な要素であり、当該人工物が「本物」であることを相応の確からしさによって検証可能であることが求められる。

キャッシュカードに着目すると、従来は磁気ストライプのみを貼付したカードによる取引がATM取引全体を占めていたが、その後、同カードのセキュリティが低下し、2004 年頃には偽造キャッシュカードによる預金の不正引出しが相次いで発生した。このように、人工物のセキュリティの低下は、正規の製造・発行手続を経ることなく準備される別の人工物（以下、クローンと呼ぶ）による不正な金融取引につながる可能性がある。金融機関側では、攻撃者の技術の向上に先回りして人工物の偽造防止技術の高度化を進める必要があるが、そのためには候補となる偽造防止技術のうち当該アプリケーションに相応しいものを評価・選択することが求められる。

このように、偽造防止技術においては、クローンの作製の困難性（以下、耐クローン性と呼ぶ）等の定量的なセキュリティ評価方法の開発が望まれる。既存の偽造防止技術においては、その内容を秘匿することによって耐クローン性を維持してきたケースが少なくなかった（松本・岩下［2004］）というのが実情であるほか、セキュリティ評価の方法としても主観的あるいは定性的な評価が中心であった（Wielandt［1998］、NRC［2007］）。ただし、技術分野によってまちまちであるものの、定量的な評価方法の確立に向けた検討が学界を中心に現在進められているところである。また、偽造防止製品のベンダーをはじめとする関係者間での情報共有を促進し、用語・概念や偽造品検査の標準的な手順の検討に向けた動きもみられる（Lancaster［2008］、NASPO［2008］）。

そうしたなかでとりわけ注目されるのが人工物メトリクスである。人工物メトリクスは、各人工物に固有の特徴を利用して認証を行うという技術であり、人工物の製造や認証の方法を秘匿する必要がなく、基本的には技術の内容を公開可能であり、第三者による評価を受けることが可能であるという利点を有している（松本・岩下［2004］）。近年では、人工物メトリクスに属する新しい手法の提案や、人工物メトリクスを実現するシステム（人工物メトリック・システムと呼ばれる）の商用製品化の事例も徐々に増えてきている。

人工物メトリクスにおけるセキュリティ評価に関しては、クローンを利用したいくつかの攻撃法への耐性を評価する際の尺度（例えば、ブルート・フォー

ス攻撃成功率、クローン一致率）が提案され、それらの尺度を利用した評価事例もいくつか報告されている。ただし、さまざまなタイプの人工物メトリック・システムに対して共通に適用可能な評価方法が確立しているという段階までには至っていないのが実情である。一方、人工物メトリクスの語源となっているバイオメトリクスの分野では、セキュリティ評価方法や評価基盤に関する検討が先行しており、同分野の知見や成果を活用する余地が存在する。このような動向を踏まえると、人工物メトリクスにおけるセキュリティ評価方法の確立に向けた検討が今後進展することが期待される。

人工物メトリクスにおける今後の主な検討課題としては、定量的な評価方法の確立に加え、人工物メトリクスを他の偽造防止技術と横並びで評価する方法の検討が望まれる。人工物メトリクスは、基本的には機械読取による技術であって人間の感覚による真偽判定には向いていないほか、真偽判定を実行するためには専用の装置が必要となるなど、利便性やコストも考慮するとアプリケーションによっては適用困難なケースが考えられる。したがって、どのような場面において人工物メトリクスが有効に機能するかを明確にしておくことが望ましい。そのためには、他の偽造防止技術と横並びで人工物メトリクスを評価し、長所や短所を把握しておくことが有用である。

人工物メトリクスや他の偽造防止技術には、さまざまな技術分野が関係している。上記のような課題を今後検討していく際には、各種技術分野における知見を活用することが重要であり、そうした分野の専門家と議論しながら進めていくことが有用である。金融分野においても、金融取引に用いられる人工物のユーザとして、人工物メトリクスやその他の偽造防止技術の動向をフォローしていくとともに、今後の人工物メトリクスの活用のあり方についても中長期的に議論していくことが重要であろう。

本稿の構成は次のとおりである。２節では、偽造防止技術の概念整理として技術の構成、評価項目、分類方法を説明するほか、人工物メトリクスのコンセプトを説明する。３節では、最近の人工物メトリック・システムの提案や商用化の事例を紹介するとともに、耐クローン性に関する最近の評価研究を整理し、研究の進展の状況を説明する。４節は、代表的な偽造防止技術として、印刷による偽造防止技術、偽造防止目的のホログラムの技術、暗号ハードウエアの技術を耐クローン性評価の観点から説明するとともに、人工物メトリクスの語源となったバイオメトリクスの動向を説明する。これらを踏まえたうえで、５節では人工物メトリクスにおける今後の研究開発の課題を示し、６節で本稿を締めくくる。

２．人工物の偽造防止技術と人工物メトリクス

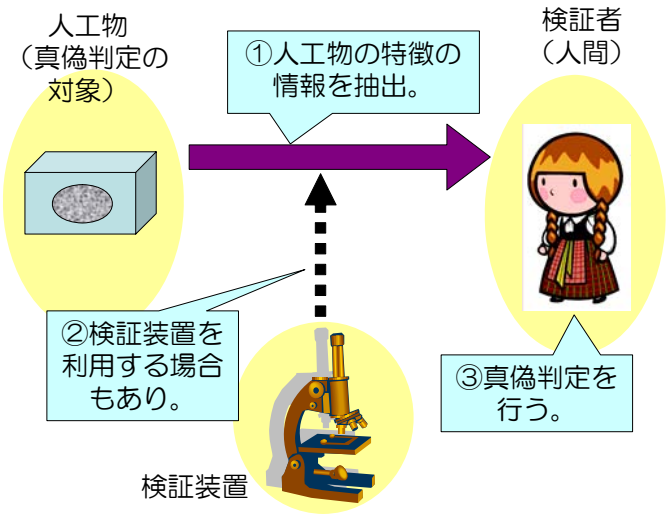
(1)偽造防止技術の構成と評価項目

イ．偽造防止技術の構成

偽造防止技術は多岐にわたる[1]が、真偽判定の対象となっている人工物の特徴の情報を得て判定を行うという点で共通している。ここで、「人工物の特徴」は人工物の物理構造や材料を意味し、「人工物の特徴の情報」は、人工物の特徴を人間や機械が測定して得た情報であり、真偽判定に利用されるものを意味する。

本稿において検討対象とする偽造防止技術は、真偽判定の対象となる人工物、真偽判定を行う検証者（人間）、真偽判定のために当該人工物の特徴の情報を得る機構（検証装置）の 3 者から構成されるとする。真偽判定の際には、①まず検証者は人工物の特徴の情報を抽出する、②その際、検証者は検証装置を利用する場合がある、③検証者は抽出した情報を基に当該人工物の真偽判定を行う（図表 1 参照）。検証装置が真偽判定の結果（受理あるいは拒否等）を出力する場合も考えられる。また、検証者は、真正な人工物が有する特徴の情報（以下、参照データと呼ぶ）を予め準備しておき、真偽判定の際には、参照データとの整合性の有無を手掛かりに判定を行うものとする[2]。

真偽判定は、対象となる人工物がどの個体であるかを明らかにするケース（以



図表１：偽造防止技術における真偽判定（概念図）

[1] 各種の偽造防止技術を紹介する文献としては、例えば、技術情報協会［2004］、情報機構［2006］、van Renesse［2005］、NRC［2007］が挙げられる。

[2] 例えば、検証者が印刷物の真偽判定をその図柄によって行う場合、本物の印刷物の図柄を何らかの方法で記憶しておく必要がある。この場合には、検証者が記憶する「本物の印刷物の図柄」が参照データに対応することとなる。

下、個体識別型と呼ぶ）と、当該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（以下、グループ識別型と呼ぶ）とに分けられる（松本ほか［2004］）。個体識別型では、グループ識別型に比べて、高い確率でより狭い範囲のグループに絞込みを行うケースであると考えることができる。また、「真偽判定の対象となっている人工物があらかじめ識別された人工物であるか否かを確認する」という 1 対 1 照合（verification）と、「当該人工物を個体として識別するための情報（IDと呼ぶ）が提示されることなく、どの人工物かを識別する」という 1 対*N*照合（identification）が考えられる[3]。

ロ．評価項目

偽造防止技術一般に求められる要件を考えるうえで、松本ほか［2004］による人工物メトリック・システムの評価項目が参考になる。人工物メトリクスについての詳細は後述するが、人工物メトリクスは偽造防止技術の 1 つであり、上記文献の内容は偽造防止技術の具体的なシステムにも当てはまると考えられる。松本ほか［2004］では、以下のように、セキュリティ、利便性、コスト、社会的受容性の 4 項目を主な評価項目として挙げている。

- **セキュリティ**
  - 想定される各種攻撃に対する耐性の度合い[4]。攻撃の種類によって耐性を測る尺度は異なってくる。例えば、個体識別型の真偽判定において、その対象となっている正規の人工物以外のものを無作為に製造・入手し、それらを検証装置に提示して「真正」と誤判定させるという攻撃（ブルート・フォース攻撃と呼ばれる、松本ほか［2004］）では、たまたま真正と誤判定される確率によって本攻撃への耐性が評価される。
- **利便性**
  - 使い勝手の良し悪し。操作方法の簡便さ、真偽判定の実行時間の短さ、人工物の特徴の読取りの安定性、異なるメーカー間での人工物や検証装置の互換性、耐久性といった項目が該当する。
- **コスト**
  - 偽造防止技術を実現するシステムの構築・運用等にかかる費用や時間。

---

[3] 検証対象の人工物がブラックリストに登録されている人工物ではないことを確認する処理（ネガティブ識別と呼ばれる）も 1 対*N*照合に対応する。

[4] セキュリティに関連する代表的な特性としては、機密性（confidentiality）、完全性／一貫性（integrity）、可用性（availability）、責任追跡性（accountability）、真正性（authenticity）、信頼性（reliability）が挙げられる。これらが偽造防止技術に当てはめたときに具体的にどのような特性として解釈されるかについては、松本ほか［2004］を参照されたい。

- **社会的受容性**
  - 偽造防止技術の社会一般への受け入れられやすさ。人工物の環境や人体への影響度、社会への適用性（利用に際して違和感や抵抗感があるか否か）といった項目が該当する。プライバシーに関する抵抗感についても本項目に含まれる。

偽造防止技術を評価する際には、少なくとも上記の項目について検討を行うことが必要である。具体的なアプリケーションへの適用を検討する場合には、当該アプリケーションにおける要件をこれらの評価項目について設定し、各要件の充足度合いを評価するという方法が考えられる。評価項目の優先度合いについても基本的にはアプリケーションに依存する部分が大きいが、偽造防止技術導入の第 1 の目的が「真正」と誤って判定するクローンを作製困難にすることである点を踏まえると、セキュリティの評価項目のなかでも耐クローン性の評価がまず必要である。本稿においてもセキュリティ評価、とりわけ、耐クローン性評価に軸足を置く。ただし、偽造防止技術一般に通用する耐クローン性の評価方法や尺度が確立しているわけではなく、今後の課題となっている。

(2)偽造防止技術の分類と各要件との関連性

イ．偽造防止技術の 3 つのカテゴリー

次に、偽造防止技術をいくつかのカテゴリーに分類する。偽造防止技術の分類方法は着眼点によって多種多様であるが、偽造防止技術の効果を左右する重要な要素である「真偽判定の形態」に着目して考えると、以下のとおり、「第 1 次検証（first line inspection）」、「第 2 次検証（second line inspection）」、「第 3 次検証（third line inspection）」の 3 つに分類するケースが多い。例えば、van Renesse［2005］においては次のとおり紹介されている。

- 第 1 次検証：道具（tool）を利用しないで人間の感覚によって実行される真偽判定。例えば、（真偽判定に関する特別な訓練を受けていない）一般人によって実行されるケースが想定される。
- 第 2 次検証：道具を用いて実行される真偽判定。例えば、一定の訓練を受けた人間（小売店店員等）等によって実行されるケースが想定される。
- 第 3 次検証：専用の機器（equipment）を用いて実行される高度な真偽判定。例えば、専門の研究所や関連施設において実行されるケースが想定される。

本分類方法では真偽判定に「道具」と「機器」が利用されているが、これらはいずれも本節(1)**イ**．の「検証装置」に相当すると考えることができる。

図表 2：IC カードにおける偽造防止技術の分類

分類	特徴・機能	偽造防止技術の代表例
感覚による真偽判定	【意匠的要素】カードの種別、適用範囲等を容易に認識可能。複製・複写を困難にする画線技術や画線パターン等によって視覚的に真偽判定を実施。	ロゴマーク、特殊フォント、特殊画線（複写防止画線等）
	【光学的要素】プロセス印刷では再現困難な色によって視覚的に真偽判定を実施。	特色インキ、ホログラム、光学的変化材料、潜像模様
	【形状的要素】表面に凹凸や穴等を形成する技術によって指感的、視覚的に容易に真偽判定を実施。	エンボス加工、凹凸付与、穿孔
補助器具による真偽判定	【意匠的要素】ルーペ等の拡大器具や特殊フィルター等の補助器具によって真偽判定を実施。	微細画線、特殊画線、マイクロ文字、特殊形状スクリーン
	【光学的要素】特殊な光学的特性を示す材料を基材、ラミネート･フィルム､インキ等に混入し､特殊フィルター、紫外線ランプ等の補助器具を用いて真偽判定を実施。	発光基材､発光ラミネート･フィルム、発光インキ、サーモクロミック･インキ､フォトクロミック・インキ
機械処理による真偽判定	【磁気・光学的要素】磁気的・光学的特性を示す材料を基材、ラミネート・フィルム、インキ等に混入し、検出機器を用いて真偽判定が可能。また、コード化した特定の情報を付与し、磁気・光学検出機器を用いて真偽判定や認証を実施。	発光材料、磁気材料、光学的認識要素、OCR、磁気バーコード
	【カード内 CPU を利用した真偽判定】カード・リーダー等との間で暗号技術を利用した認証処理等を実施し、アクセス管理や真偽判定を実施。	暗号技術によるチャレンジ・レスポンス認証

（備考）財務省印刷局［2002］の 6.1 節の表を基に作成したもの。

以上の第 1～3 次検証と完全に対応しているわけではないが、類似のアイデアによる代表的な偽造防止技術の分類方法として、財務省印刷局［2002］の分類方法（ICカードを対象としたもの）が挙げられる。本文献では、「(ICを除く)カード自体の物理仕様上の対策」を、「感覚による真偽判定」、「補助器具による真偽判定」、「機械処理による真偽判定」の 3 つに分類し、各カテゴリーに対応する偽造防止技術の例を紹介している（図表 2 参照）。本分類は、ICカードに限らず一般の偽造防止技術にも適用可能と考えられる[5]。また、「カード内CPUが行うアクセス管理やデータの暗号化等の電子的な対抗策」は、上記分類から除外して整理されているが、「CPUで行われる処理結果をカード・リーダーが確認し、同リーダーから出力される確認の結果を真偽判定結果として検証者が認識する」と整理できる。そこで、本稿では上記対策を「機械処理による真偽判定」の一形態として整理する。

[5] 本分類においては「補助器具」と「機械」の差異が明記されていない。例示の偽造防止技術から勘案すると、補助器具は、人間に代わって人工物の特徴を抽出するものであり、真偽判定にあたって「真正」と判断される度合い（スコア）や判断の結果（OKあるいはNG）は出力しないもの（真偽判定は人間が実行）を指していると考えられる。機械については、人間に代わって人工物の特徴を抽出し、スコアや真正か否かの判断の結果を出力するもの（機械の出力を基に最終的な真偽判定は人間が実行）を指していると考えられる。

ロ．耐クローン性

図表 2 における 3 種類の真偽判定について耐クローン性の観点から検討する。

（イ）感覚による真偽判定の場合

感覚による真偽判定は、(A)人工物の特徴の情報を人間（検証者）が感覚によって抽出し、(B)当該情報を用いて真偽判定を検証者が行うものと整理することができる。本真偽判定は、人間の感覚のみによって実行可能であり、使い勝手がよいという意味での利便性が高いほか、補助器具や機械が不要という観点からコストも相対的に抑えることが可能である。社会的受容性については個々の偽造防止技術の形態に依存する。耐クローン性については、上記(A)と(B)に対応させて考えると、検証時に人工物の特徴の情報を抽出する能力（以下、特徴抽出能力と呼ぶ）と、当該情報を用いて既定の真偽判定を適切に実行する能力（以下、判定実行能力と呼ぶ）に左右されると整理することができる。

特徴抽出能力に関しては、検証者となる各個人の感覚のレベルに依存する。当該人工物の取扱いに精通する個人や知覚能力が優れている個人が検証者の場合、本真偽判定は高い効果を発揮すると考えられる。ただし、検証者が常に優れた感覚を有する個人とはいえないケースもあるほか、人間の生来の知覚能力には一定の制約も存在する[6]ことから、偽造防止技術に利用可能な人工物の特徴もある程度限定される。例えば、印刷された画線パターンの細線が人間の肉眼によって識別可能なサイズよりも細い場合、検証者がその特徴を視覚的に正しく抽出することは困難となる。こうした特徴抽出能力のばらつきや制約を考慮すると、感覚による真偽判定において一般の個人が抽出可能と期待される情報量は補助器具や機械を利用する場合に比べて少ないと考えられる。

判定実行能力に関しても各検証者に依存する。真偽判定の方法を各検証者が理解したとしても、その際に利用される参照データが適切か否か、また、「真正」と判定される対象が許容される範囲に収まっているか否か（判定しきい値が適切に運用されているか否か）を確認困難である。一定の印刷物における図柄を目視で真偽判定するという例で考えると、検証者が参照すべき図柄の細部（参照データに対応）を正確に記憶しておくことが困難な場合、不適切な参照データが利用されることとなり、「大雑把には似ているようにみえる」別の図柄を誤って真正と判定する可能性がある（van Renesse［2006］）。また、一般の個人が記憶可能な参照データの情報量もある程度限定されることから、大量の人工

[6] 例えば、人間の目で感知できる光（可視光線）は 400～700 ナノ・メートル（1 ナノ・メートル＝10^{-9}メートル）の波長帯に制限され、同波長帯から外れる紫外線や赤外線は肉眼でみることができない。また、写真を 30cmの距離からみたときに、1 mmの幅に 11～16 ドット以上の解像度を肉眼では区別困難といわれている（池田・徳永［2009］）。

物を対象とする個体識別型の真偽判定は実現しづらく、グループ識別型となるケースが多い。

このように、本真偽判定においては、特徴抽出能力と判定実行能力の点で一定の制約を受ける場合が考えられる。

（ロ）補助器具による真偽判定の場合

補助器具による真偽判定は、ルーペ、特殊フィルター、紫外線ランプ等の補助器具を用いて当該人工物の特徴を抽出し、当該情報を用いて真偽判定を検証者が行うものである。感覚による真偽判定と比較すると、補助器具が必要であるという意味で利便性の低下やコストの増加につながる。耐クローン性は、上記（**イ**）と同様、特徴抽出能力と判定実行能力によって左右される。

特徴抽出能力については、補助器具の使用によって向上すると期待される。例えば、印刷された微細な文字を人工物の特徴として利用しつつ補助器具としてルーペを用いるケースでは、当該文字が拡大され、感覚のみを利用するケースに比べて文字の形状を正しく認識しやすくなる。その結果、特徴抽出能力の制約が緩くなるとともに、検証者による個人差も小さくなることが期待される。

特徴抽出能力の向上は、判定に利用される人工物の特徴の情報量の増加とともに、判定実行能力の個人差による変動や制約の緩和につながると考えられることから、感覚による真偽判定に比べて真偽判定の適切性の向上が期待される。ただし、真偽判定は人間が行うことから、多くの参照データを記憶することは困難であり、認証の形態はグループ識別型となるケースが多いと考えられる。

このように、補助器具による真偽判定は、感覚による真偽判定と比べて特徴抽出能力や判定実行能力の点で優れており、偽造防止技術が期待どおりの効果を発揮することによって、本真偽判定における耐クローン性が感覚による真偽判定の場合よりも高くなるケースが考えられる。

（ハ）機械処理による真偽判定の場合

機械処理による真偽判定では、人工物の特徴の情報を抽出するところから判定結果を出力するところまでを機械が実行し、人間が介在しないケースも少なくない。本真偽判定には専用の装置が必要となるという点で利便性の低下やコストの増加が見込まれるものの、人間による真偽判定の手間が軽減される、高速処理が可能になる等のメリットが考えられる。

耐クローン性については、人間の感覚によっては抽出困難であった微細な領域の特徴や各種物理特性も抽出可能になることから、特徴抽出能力の向上が期待される。また、真偽判定の処理については、検証者の個人差による変動や制約がなくなり、既定の真偽判定の処理がほぼ均質化されて実行され、判定実行

能力が向上すると考えられる。さらに、真偽判定時に利用可能な参照データの情報量も格段に増加することが見込まれることから、人工物を個体として識別して認証を行うことも可能となる。

ただし、機械処理による真偽判定では、その機械の脆弱性を突いた攻撃が可能になるおそれがある点には留意しておく必要がある。例えば、抽出対象となる特徴とは別の部分も本物と似せて偽造する必要がなくなり、逆に偽造が容易になる可能性もある。また、当該機械を誤動作させ、どのような人工物に対しても「真正」と誤って判定するように攻撃者が不正操作することも考えられる[7]。したがって、本真偽判定では、検証を実行する機械が適切に製造・運用されていることが前提となる。

(3)人工物メトリクスの特徴

イ．基本アイデア

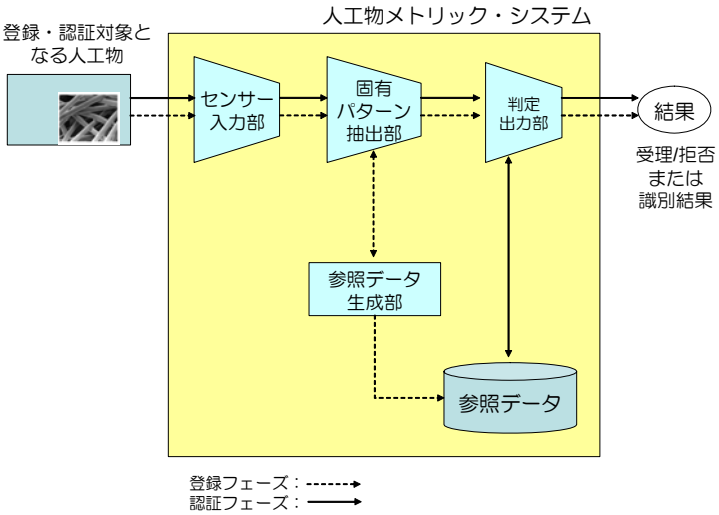
人工物メトリクス（artifact-metrics）は、バイオメトリクス（biometrics）という用語を参考に人工物（artifact）と測定（metrics）を組み合せた造語であり、「各人工物に固有の特徴を用いて人工物の認証を行う技術」と定義されている（松本ほか［2004］）。バイオメトリクスにおいては、各個人が先天的あるいは後天的に得た身体的特徴や行動的特徴を利用するのに対し、人工物メトリクスの場合、人工物の製造過程で形成される自然発生的な特徴を利用するというアイデアである。微視的にみるとどのような人工物も完全に同一となることはありえず、そうした特性を認証に利用するという点が人工物メトリクスのコンセプトである（松本・岩下［2004］）。ただし、現実の利用場面において人工物メトリック・システムの効果を高めるために、製造段階において各人工物の特徴の情報を抽出しやすくする「仕掛け」を付与するというケースが多い。例えば、証書を対象とする場合に、製造段階で個々の証書に磁性ファイバーを漉き込み、各証書から磁気ヘッドによって読み取られた信号を認証に利用するという手法が提案されている（Matsumoto *et al.*［2001］）。同システムの場合、磁性ファイバーの埋込みがここでの「仕掛け」に対応する。

人工物メトリック・システムにおける登録・認証は、製造した人工物から一定の特徴を測定して得たデータ（固有パターンと呼ばれる）を参照データとして登録時に保管し、認証時には人工物から同様の手続で生成した固有パターンと参照データとの整合性を確認するという流れとなる（松本ほか［2004］、図表3参照）[8]。これらのうち、センサー入力部で取得される情報が本節(1)**イ**．にお

---

[7] こうした耐クローン性以外のセキュリティ特性に関する評価については、３節(2)**イ**．において紹介するように、松本ほか［2004］で既に議論されている。

[8] ただし、松本ほか［2004］に示されているように、被認証物である人工物に当該参照デー



図表 3：人工物メトリック・システムの基本構成
（松本ほか［2004］の図 4 を引用）

いて説明した「人工物の特徴の情報」に対応する。したがって、人工物の耐クローン性は、人工物の特徴自体の複雑さや微細さに加えて、センサーによって人工物の特徴の情報がどのように抽出されるかにも依存する。人工物の特徴が微視的には十分な固有性を有していたとしても、分解能が低いセンサーで測定した場合、人工物の特徴の情報における固有性も低下する。こうした点から、人工物の特徴の測定方法が人工物の耐クローン性を評価するうえで重要である。

ロ．人工物メトリクスの認証形態の主な特徴

人工物メトリクスにおける認証形態の主な特徴を整理すると、まず認証の形態としては 1 対 1 照合と 1 対 *N* 照合の 2 種類が想定されるほか、個体識別型とグループ識別型の両方とも想定される。また、人工物の認証を機械によって実行する場合と、人間の感覚によって実行する場合が考えられるが、センサーによる人工物の微細な特徴の読取りや複雑で大量の演算処理を実行することが必要となることが多く、図表 2 の分類のうち「機械処理による真偽判定」の技術に概ね対応するといえる。

ハ．耐クローン性等の評価項目について

人工物メトリクスにおける偽造防止効果については、本節（2）**ロ**．（**ハ**）の「機械処理による真偽判定」と同様の考察が当てはまる。人工物メトリクスが

タを記録・保持しておく場合と別の場所に記録・保持しておく場合があるなど、上記の基本形をベースとして人工物メトリック・システムのさまざまな実現形態が考えられる。

有効に機能するためには、参照データとして登録されているいずれかの固有パターン（あるいは同パターンと高い類似度を有するもの）に対応する人工物の偽造が十分に困難であることが求められる。こうした要件は人工物メトリクス以外の「機械処理による真偽判定」を行う偽造防止技術の要件でもある。

ただし、人工物メトリクスは、人工物の製造過程において偶然形成される特徴を真偽判定に利用するという点がポイントであり、こうした点を活用することによって耐クローン性の向上が期待される。例えば、人工物の特徴を製造過程において意図的に制御することが困難な場合、仮に、製造者レベルの攻撃者が現れたとしても、真偽判定にパスするレベルの人工物の偽造が引き続き困難であるという効果を期待することができる。一方、人工物メトリクスでない偽造防止技術については人工物の特徴を製造過程において制御可能であることから、製造者であれば一定の特徴を有する人工物を製造することが原理的に可能であり、製造者レベルの攻撃者が現れたときには期待される偽造防止効果が発揮されない可能性がある。個々の人工物メトリック・システムの評価を行う際にはこうした効果の度合いを検証する必要があるが、そうした評価を行う方法が確立されるまでには至っていないのが実情である。

その他の評価項目（利便性、コスト、社会的受容性）についても、他の偽造防止技術と同様に、人工物メトリック・システムの実装性を評価するうえで重要な項目となる。社会的受容性に関しては、個体識別型の場合、真偽判定時にどのような人工物が判定の対象となったかが明確になり、そうした情報の悪用によって当該人工物の所持者の行動を追跡できるといった問題が存在する。こうした観点からの評価も今後の重要な課題であるといえる。

３．人工物メトリクスの研究開発の動向

人工物メトリクスの最近の研究開発をみると、人工物メトリクスの新たな手法の提案が増えているほか、具体的なシステムの開発や商用サービス開始の事例もみられ、実用化段階に達しつつある。一方、人工物の耐クローン性等に関する評価方法についてもいくつかの研究報告がみられるようになってきている。

(1)人工物メトリック・システムの主な事例

近年提案されている主な人工物メトリック・システムを紹介する。図表４は、松本ほか［2004］において紹介された事例に最近の事例を追加して作成したものであり、追加した事例の中から市販されているシステムとして、スペックル・パターンを利用するシステムとフィジカル・アンクローナブル・ファンクション（PUF: physical unclonable function）を利用したシステムについて紹介する。

イ．スペックル・パターンを利用するシステム

スペックル・パターンは、物体において反射したり透過したりした光によって空間上に発生する斑点状の模様であり、当該物体の表面の微小な凹凸や内部

図表４：主な人工物メトリック・システムに利用される人工物の特徴

特性	人工物の特徴
光学特性	・基材中の光輝性粒状物の分布（反射光画像）（Pappu [2001]、Poli [1978]、Škorić *et al.* [2007]、Tuyls *et al.* [2005]） ・紙に漉き込まれた光ファイバー小片の分布（透過光の輝点分布）（NRC [1993] pp.74-75） ・基材に付与された斑の分布（反射あるいは透過光の画像）（Goldman [1988]） ・透明樹脂内のポリマー・ファイバーの分布（視差画像）（van Renesse [1995]） ・基材中のファイバーの分布（Brzakovic and Vujovic [1996]） ・基材表面の微小の凹凸（レーザ・スペックル・パターン）（Buchanan *et al.* [2005]） ・紙片表面の紙繊維の分布（反射光画像）（伊藤ほか [2005]） ・紙片中の紙繊維の分布（透過光画像）（Yamakoshi *et al.* [2008]）
磁気特性	・基材中の磁性ファイバーの分布（電気信号波形）（Matsumoto *et al.* [2001]） ・データ書込みに伴う磁気ストライプ上の磁気分布（電気信号波形）（Fernandez [1993]） ・磁気ストライプ上の磁性粒子の分布（Inedk *et al.* [1995]、Hayosh [1998]） ・基材中の伝導性物質の分布（電磁波パターン）（DeJean and Kirovski [2007]）
電気特性	・半導体素子内のメモリー・セルの電荷量のばらつき度合い（Fernandez [1997]、Guajardo *et al.* [2007]） ・ランダムに分散した絶縁粒子を含むIC保護コーティングの電荷量（Tuyls *et al.* [2006]） ・半導体素子におけるランダムな回路遅延のパターン（Gassend *et al.* [2002]、Lim *et al.* [2005]、Suh and Devadas [2007]、Devadas *et al.* [2008]） ・複数のリング・オシレータから出力される周波数（Suh and Devadas [2007]） ・コイルとコンデンサーで構成されるLC回路の共振波形（Škorić *et al.* [2008]）
振動特性	・導電性ファイバーをランダムに分散した基材のマイクロ波の反射（Samyn [1989]） ・容器に貼ったシールを振動させたときの共鳴周波数分布（Olinger, Burr, and Vnuk [1994]）

（備考）本図表は松本ほか［2004］の表１に最近の事例（シャドー部分）を追加して作成したもの。

構造に依存する。人工物にレーザ光を照射し、その反射光のスペックル・パターンを用いて認証するシステムが提案されている（Buchanan *et al.*［2005］）。

同システムは、各種証券、ID カード、医薬品のパッケージ等への応用を目的に英国のインジニア・テクノロジー（Ingenia Technology）社によって LSA（Laser Surface Authentication）という名称で開発され、欧州の医薬品や煙草のメーカーにおいて本システムが組み込まれた製造・物流管理システムの試験運用が実施されている。LSA においては、スキャナー上に認証対象の人工物（紙等）を置いたうえで、波長 635nm のレーザ光を当該人工物に照射し（照射エリアは 4mm×0.07mm）、反射光から得られるスペックル・パターンを 4 つの受光素子によって取得し固有パターンを得る。認証は、登録データと認証時の固有パターンとの照合によって実施されるという仕組みになっている。本システムの評価として、以下のとおり、個別性、読取りの安定性、耐久性についての評価結果が提案者によって報告されている（Buchanan *et al.*［2005］）。

- 個別性 : 同一の固有パターンを有する人工物が出現する確率を一定の条件のもとで試算しており、紙の場合には 10^{-72}程度、マット仕上げされたプラスチック・カードやコーティングされた板紙の場合には 10^{-20}程度との見積りが示されている。
- 読取りの安定性 : 人工物の認証を正しく実行するうえでスキャナー上に人工物を置く位置のズレの許容度を測定したところ、±1mm 程度の平行移動、±2 度程度の角度誤差が許容されるとの結果が示されている。
- 耐久性 : 紙を認証対象とした場合、次の操作に対して耐性がある旨が示されている。
  - 紙を小さなボールにねじ込んで取り出し平らにする。
  - 冷水に 5 分程度浸し、自然乾燥させる。
  - 30 分間オーブンによって 180 度で表面を焼く。
  - 黒のマーカーペンやボールペンで表面に適当な模様を書く。
  - 研磨タイプの清掃用パッドで紙の表面を擦る。

ロ．PUF を利用したシステム

PUF は、物理的に複製が困難となるように設計された人工物であり、当該人工物の特徴の情報を得るために人工物に与えられる刺激（チャレンジと呼ばれる）に対して当該情報（レスポンスと呼ばれる）を出力するという関数の機能をもつものとして Pappu［2001］によって提案された。同文献は PUF を次の性質を有するように設計された人工物として定義している。

- PUF へのチャレンジのバリエーションが莫大であり、認証時にはチャレンジがランダムに選択されるため、レスポンスを予測困難である。
- チャレンジとレスポンスの対応関係はモデル化困難である。
- PUF の物理的構造を特定困難である。

PUF の主な実現方法として最近提案されたものとして、以下のイントリンシック PUF、コーティング PUF、シリコン PUF、リング・オシレータ PUF、LC-PUF が挙げられる。

- イントリンシック PUF : 半導体素子内のメモリ・セルの電荷量のばらつき度合いをデジタル・データに変換する回路を PUF とするもの（Guajardo *et al.*［2007］）。
- コーティング PUF：ランダムに分散した絶縁粒子を含む IC 保護コーティングの電荷量を出力する回路を PUF とするもの（Tuyls *et al.*［2006］）。
- シリコン PUF：IC 内部のパス遅延をデジタル・データに変換する回路を PUF とするもの（Gassend *et al.*［2002］）。最近では、複数のパスの遅延を比較しその結果をデータに変換するタイプの PUF（アービターPUF、Lim et al.［2005］、Suh and Devadas［2007］、Devadas *et al.*［2008］）が提案されている。
- リング・オシレータPUF : 複数のリング・オシレータ[9]を用いたPUFであり、各リング・オシレータから出力される周波数の複数の比較結果をレスポンスとして利用する（Suh and Devadas［2007］）。
- LC-PUF：LC回路[10]をPUFとするものであり、LC回路の共振波形をレスポンスとして利用する方式である（Škorić *et al.*［2008］）。

PUF の利用方法には、図表 3 に示したシステムに加え、レスポンス等から暗号用の鍵を動的に生成し各種の暗号処理を実行するシステムも提案されている。本システムは、暗号処理結果の整合性確認によって当該人工物の真偽判定を実行可能であり、人工物メトリック・システムに含まれると考えられる。

Tuyls *et al.*［2006］は、コーティング PUF を備えた IC によるデジタル署名用の鍵生成方式を提案している。PUF からのレスポンスとして得られる電荷量の

[9] リング・オシレータは、発振回路の一種であり、インバータ等の論理素子をリング状に配置した発振回路の一種である。各論理素子における入出力には一定の遅延が発生し、そうした遅延を製造段階において制御困難とみられていることから、PUFに利用されている。
[10] LC回路はコイルとキャパシタによって構成される回路であり、コイルにおける電磁誘導によって同回路を流れる電流が周期的に変化する（同波形は共振波形と呼ばれる）という特性を有している。

データを誤り訂正符号の手法によって訂正し、訂正後のデータを署名生成鍵として利用するものである。IC のメモリには、①IC の発行者の署名検証鍵 *pk*、②当該 IC の署名検証鍵 *P*(*K*)（対応する署名生成鍵は *K*）、③*P*(*K*)に対する発行者の署名 *σ*(*P*(*K*))、④訂正のための補助データ *w*（helper data と呼ばれる）、⑤*w* に対する発行者の署名 *σ*(*w*)を格納しておく。鍵生成の手順は次のとおりである。

【1】IC の発行者の署名検証鍵 *pk* を用いて *w* に対する署名 *σ*(*w*)を検証。
【2】PUF からのレスポンスと補助データ *w* から、署名生成鍵の候補 *K'*を計算。
【3】*K'*から同鍵に対応する署名検証鍵 *P*(*K'*)を計算。
【4】署名検証鍵に対する署名 *σ*(*P*(*K*))と上記【3】で生成した *P*(*K'*)が整合していることを確認。確認が成功した場合には正しい鍵が生成できたと判断し、*K'*を署名生成鍵として利用する。本署名生成鍵によって生成される署名の検証が成功すれば、当該 IC を真正と判定する。

本システムのセキュリティ評価に関しては、想定される攻撃として集束イオン・ビーム装置[11]によってICを穿孔し内部のデータを盗取するという攻撃を紹介したうえで、本攻撃では同ビームが保護コーティングを破壊し静電容量が変化してしまい、鍵生成が適切に実行困難となるとしている（Tuyls *et al.*［2006］）。さらに、鍵が適切に生成されなかった場合にデバイスの機能を無効化する機構を組み込むという対策が紹介されている。

こうしたPUFを利用するシステムの製品化については、米国の半導体メーカーのベラヨ（Verayo）社が 2008 年 9 月からアービターPUFを搭載したRFIDチップを“Vera X512H”として発売している[12]。また、オランダのフィリップス（Philips）社は、イントリンシックPUFの実用性に関する評価結果を発表したほか（Bösch *et al.*［2008］）、同社から独立したイントリンシック・アイディ（Intrinsic-ID）社は、2008 年 10 月に、イントリンシックPUFを搭載したFPGAによる偽造防止技術を“Quiddikey”という名称で商品化している[13]。

(2)人工物メトリック・システムのセキュリティ評価に関する事例

イ．評価の枠組み

人工物メトリック・システムにおいて最低限考慮すべき攻撃方法とセキュリティ要件を検討した先行研究として松本ほか［2004］が挙げられる。松本ほか

[11] 集束イオン・ビーム装置（focused ion beam）は高電圧によって加速されたイオンの束を照射する装置であり、半導体の微細加工等に用いられている。
[12] 詳細は同社サイト（http://www.verayo.com/solutions.html）を参照されたい。
[13] 詳細は同社サイト（http://83.137.193.31/~intrinid000/html/products. html）を参照されたい。

図表 5：セキュリティ要件と達成度合いの測り方の例

セキュリティ要件	各要件の達成度の測り方の例
特定の固有パターンに対応する参照データが偽造困難であること。	・ 参照データの生成アルゴリズムの評価項目集（項目例．判定しきい値等のパラメータ設定）を作成し、達成度を確認。 ・ ブルート・フォース攻撃の成功確率を測定。
無効化した人工物を再利用困難な形態で廃棄すること。	・ 人工物無効化手続の評価項目集（項目例．人工物の抜取り防止措置、ハードウエアの耐タンパー化、無効化手続のログ管理、参照データの削除）を作成し、達成度を確認。
特定の固有パターンを別の人工物によって再現困難であること。	・ クローン一致率等を測定。
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に検証装置を不正に操作困難であること。	・ 検証者に関する評価項目集（項目例．操作者の共同作業化、処理内容のログ管理、ハードウエアの耐タンパー化）を作成し、達成度を確認。 ・ 検証装置やシステムの評価項目集（項目例．不正侵入対策、ハードウエアの耐タンパー化）を作成し、達成度を確認。
攻撃者が発行者と結託困難であること。	・ 人工物の発行システムに関する評価項目集（項目例．処理内容のログ管理、データベースの改ざん検知策の適用、操作者の共同作業化、ハードウエアの耐タンパー化）を作成し、達成度を確認。
クローンの固有パターンに対応する参照データをデータベースから探索困難であること。	・ 参照データの検索の成功確率を測定。

（備考）本図表は松本ほか［2004］の表 6 をベースに作成したもの。

［2004］は、クローンを用いて検証者に検知されることなく認証を成功させるという攻撃に焦点を当てて、一定の環境と攻撃者のもとで想定される代表的な攻撃法、セキュリティ要件、同要件の達成度合いの測り方を整理している（図表 5 参照）。ただし、達成度合いの測り方に関する具体的な内容については、個々の人工物メトリック・システムや適用対象のアプリケーションによって異なるとして詳細な検討を行っていない。

ロ．クローン作製による攻撃の種類と評価尺度

松本ほか［2004］において整理された結果をより深く検討した最近の研究をみると、図表 5 に挙げられている「特定の固有パターンをクローンによって再現困難であること」の評価方法や評価事例に関する成果がいくつかみられる。田村・宇根［2007］は、そうした既知の攻撃法を次の 5 つに整理している。

- ブルート・フォース攻撃：クローンを無作為に入手・製造し、当該クローンをシステムに提示するという攻撃。
- ウルフ攻撃：数多くの参照データと「一致」と誤判定される固有パターン（ウルフに対応する）を探索し、当該ウルフをクローンとして製造・提示するという攻撃。
- リプレイ攻撃：認証時等に検証装置と人工物でやり取りされる情報（チャ

レンジ・レスポンス・ペア、CRP）を入手し、当該情報を再現するクローンを製造・提示するという攻撃。ただし、当該 CRP 以外を推定しない。
- シミュレート攻撃:攻撃時における検証装置と人工物との間の CRP を推定し、当該情報を再現するクローンを製造・提示するという攻撃。
- ハード・コピー攻撃：人工物の特徴そのものを推定し、当該特徴を有するクローンを製造・提示するという攻撃。

ブルート・フォース攻撃とウルフ攻撃に対する評価尺度として、「ブルート・フォース攻撃成功率」と「ウルフ攻撃確率（WAP: wolf attack probability）」がそれぞれ適用可能なほか、リプレイ攻撃、シミュレート攻撃、ハード・コピー攻撃に対しては、「クローン一致率（clone match rate）」が提案されている。

ブルート・フォース攻撃成功率は、クローンの数をN_1、参照データの数をN_2、実際に評価対象システムにおいて測定して得られた誤合致率を*FMR*としたときに、少なくとも 1 つのクローンが誤って受け入れられる確率 $1-(1-FMR)^{N_1 \times N_2}$として見積ることができる（Matsumoto *et al.*［2001］）。本尺度はクローンの種類に依存しており、本尺度を利用する際にはクローンの想定の妥当性を明らかにしておく必要がある。本尺度による評価事例としては、無作為に紙に埋め込まれた磁性ファイバーの分布を利用したシステムの評価事例が知られている（Matsumoto *et al.*［2001］）。

ウルフ攻撃確率（Une, Otsuka, and Imai［2008］）は、生体認証システムにおける評価尺度として提案されているが、人工物メトリック・システムにも適用可能である。その場合、ウルフ攻撃確率は、「“一致”と誤判定される参照データの数が最大となる固有パターンを提示した際に、特定の参照データと一致と誤判定される確率」と表現され、ウルフ攻撃の成功確率における理論上の上限となる。ただし、筆者らが知る限り、個別の人工物メトリック・システムのウルフ攻撃確率を評価した事例はこれまで発表されていないようである。

クローン一致率は、本物を見本にするという方法で作製されたクローンが提示され、1 回の照合において一致と誤判定する確率である（Matsumoto and Matsumoto［2003］）。クローン一致率も、ブルート・フォース攻撃成功率と同様にクローンの種類に依存する。紙に埋め込まれた磁性ファイバーの分布を利用した人工物メトリック・システムを対象に、磁性材を紙表面にロボットによって塗布したクローンを用いて算出した事例（Matsumoto and Matsumoto［2003］）が知られており、誤合致率よりも高い値となることが確認されている。また、紙の赤外線透過光を用いた人工物メトリック・システムにおいて、スキャナーによる同透過光の画像をプリントした OHP シートを「紙のクローン」として準備しクローン一致率を算出した事例（平良・山越・松本［2007］）もある。

このほか、偽造の対象となる人工物と検証装置との間の CRP や当該人工物の特徴を示す情報の特定にかかる計算量を尺度とする事例もみられる。例えば、Pappu［2001］と Tuyls *et al.*［2005］は、基材中の光輝性粒状物の分布を利用する人工物メトリック・システムを対象に、検証装置と人工物との間の CRP をすべて得るために必要な計算量や処理時間を一定の理論モデルを前提に推定している。ただし、本評価はリプレイ攻撃に関する評価とみることができるものの、攻撃実行にはすべての CRP を入手する必要があるか否かが明確になっておらず、推定結果の妥当性を見極める必要がある。また、DeJean and Kirovski［2007］は、基材中の伝導性物質の分布を利用する人工物メトリック・システムを対象に、特定の CRP を再現する人工物の特徴を一定の手法のもとで推定するために必要な計算量を検討している。本評価についてもリプレイ攻撃を前提としたものといえる。

このように、人工物メトリック・システムを対象とするセキュリティ評価、とりわけクローンを利用した攻撃への耐性に関して研究成果が報告されるようになってきている。ただし、こうした耐性の評価の前提となっている理論モデルの妥当性等についてさらなる検討が求められる。

４．関連技術分野の動向

本節では、印刷、光学素子、耐タンパー性を有するIC等の暗号ハードウエアを利用した偽造防止技術や、人工物メトリクスの語源となった生体認証技術を取り上げ、セキュリティ評価という観点から最近の動向を紹介する。光学素子については、クレジットカードをはじめとして金融分野で広く利用されているホログラムの技術に焦点を当てることとする。

(1)印刷による偽造防止技術

イ．偽造防止効果を高めるためのアイデア

印刷は、文字、絵、写真等の図柄を施した印刷版にインキを付与し、印刷基材にこのインキを転移することで図柄を迅速かつ精密に複製する技術であり、その研究開発には非常に長い歴史がある。これまでに多種多様な印刷技術が生み出されており、そうした技術を偽造防止に活用するために、インキ、印刷基材、印刷によって表現される図柄、印刷版にそれぞれ工夫を施すといった方向で研究開発が進められてきた。

インキ自体への工夫としては、特殊な性質を有するインキを開発する（特殊なインキの開発)、複数の種類のインキを組み合せて利用する（複数のインキの組合せ）といったアイデアが挙げられる。特殊なインキの開発に対応するものとしては、図表 2 から紹介すると、特色インキ、発光インキ、サーモクロミック・インキ、フォトクロミック・インキ[14]が挙げられる。条件等色インキ[15]（メタメリック・インキ)、磁気インキ、パールインキ、合成された特殊な結晶顔料を含むインキも含まれる。複数種類のインキの組合せに対応するものとしては、カラー画像における 3 原色の彩度[16]を微妙に変化させて印刷することによって当該画像に一定の情報を埋め込むという手法（NRC［2007］）が挙げられる。

印刷基材への工夫としては、特殊な素材（例えば、各種繊維を一定の比率で配合した紙、ポリマー、セキュリティ・スレッド、蛍光発光粒子等を漉き込んだ用紙）を基材に利用したり、基材に特殊なパターン（例えば、すかし、エンボス加工等）を施したりするという方法が挙げられる。これらの方法から得られる独特の手触りや視覚的効果等が真偽判定の手掛かりとして利用されている。

印刷基材上の図柄への工夫としては、印刷の文字や線をより細かくする（図

---

[14] サーモクロミック・インキは温度によって発色または変色するインキであり、フォトクロミック・インキは紫外線等が照射されると発色または変色するインキである。

[15] 条件等色インキは、本来異なる性質（分光分布）を有し、ある条件のもとでは同じ色にみえるが、別の条件下では異なる色にみえるという性質を有するインキである。

[16] 彩度は、色の種類（色相)、色の明るさ（明度）とともに色彩の属性を示す要素の 1 つであり、色の鮮やかさを示す。

柄の微細化・細線化)、観察される図柄が観察の際の環境条件によって変化するように図柄をデザインしインキを塗布する（図柄の可変化）といったアイデアが挙げられる。図柄の微細化・細線化には、図表 2 から紹介すると、マイクロ文字、特殊形状スクリーン[17]、微細画線が対応する。図柄の可変化に対応するものとしては、観察する角度を変えると現れる潜像模様を利用するという方法や、一定レベルの解像度のスキャナーによる図柄読取りの際にモアレ模様[18]が発生するように図柄を構成するという方法が挙げられる（Schell［1998］）。

また、印刷版については、凸版印刷、凹版印刷、平板印刷等、さまざまな方式が開発されている。これらの方式は上記の各種の特殊な図柄を実現するうえで寄与しており、例えば、潜像模様は凹版印刷によるインキの微細な 3 次元構造の形成によって実現されているほか、インキの分布や形状を手触り等によって検知し真偽判定に利用するという方法もある。

ロ．ナノ・テクノロジを利用した技術

最近注目される研究動向として、ナノ・テクノロジ[19]を利用した技術のうち、ナノ粒子印刷、超微細インクジェット、ナノ結晶顔料の研究について紹介する。

（イ）ナノ粒子印刷

既存のグラビア印刷は、版面にインキを付着させた後に余剰なインキをかきとって印刷基材に転移させる。これに対して、ナノ粒子印刷では、インキに含まれるナノ粒子が版面の微小な窪みに引き寄せられて配置され、印刷基材にナノ粒子が転写されて微細なパターンを実現する。本技術は 2007 年に IBM 社から報告され（Tobias *et al.*［2007］）、用いられる版面は数十ミクロンの凹凸を有する母型を型押しして作成される。本技術は、ナノ粒子を含む特殊なインキの開発、図柄の微細化、印刷版の開発に基づくものといえる。

（ロ）超微細インクジェット

超微細インクジェットは、微小なノズルを用いてインキを印刷基材に直接噴射して印刷を行う技術である。市販されているインクジェット・プリンタの最小液滴量は 2 ピコリットル（$=2\times10^{-12}$リットル）程度であり、直径 16 ミクロン（$=16\times10^{-6}$メートル）程度の液滴の体積に相当するが、微細回路形成等の用途

[17] 特殊形状スクリーンは、微細かつ特殊な形状の網点によって画像を表現する技術である。
[18] モアレ模様は、一定の繰返しパターンを持つ図柄を重ね合わせた際に発生する干渉縞のことである。
[19] ナノ・テクノロジは、物質をナノ・メートルのレベル、すなわち、原子・分子のレベルで操作・制御し、ナノ・サイズ特有の物質特性を利用して新しい機能や特性を有する物質を形成する技術の総称である

を想定すると液滴の一層の微細化が望まれていた。そうした中、直径 1 ミクロン程度の超微細液滴によるインクジェット印刷の技術が開発された（産業技術総合研究所［2002］）。本技術は、ナノ・サイズのインクの液滴を実現したという意味で図柄の微細化と印刷版の開発に基づくものといえる。

（ハ）ナノ結晶顔料

ナノ結晶顔料はナノ・サイズの結晶を成分とする顔料であり、同結晶によって実現される色変化等の独自の性質をインキに利用するための研究が行われている（例えば、Hu *et al.*［2006］、Macfaland and Van Duyne［2003］）。ナノ結晶顔料は、紫外から赤外域において反射、吸収、散乱等における独特の光学特性を有し、一般の顔料では実現困難とみられている。そこで、特殊な装置によって顔料の特性を読み取り、当該人工物の真偽判定における法科学的な検証手段として利用することが提案されている。ナノ結晶顔料を利用する偽造防止技術は、特殊なインキの開発に基づいた技術といえる。

ハ．偽造防止効果の評価方法に関する検討

上記の各種技術の偽造防止効果は、２節(2)において整理したように、特徴抽出能力や判定実行能力に左右される。仮に、これらの能力が検証者において期待どおりであったとすれば[20]、真偽判定時の特徴抽出の細かさで人工物を偽造することがどの程度困難かがポイントとなる。その際、人工物の製造者と同等の能力を有する攻撃者であれば当該人工物を製造可能である点を踏まえると、そうした能力を具備するためのハードルの高さが 1 つの基準となる。例えば、人工物の材質、構造、製造方法に関する情報やノウハウが第三者に漏洩しないように厳格に管理されているか、製造工程を実現する装置や材料の入手が困難かなどが評価項目となる。こうした事情から、個々の技術の情報や評価結果の詳細が公開されるケースは少ない（Wielandt［1998］）。

ただし、印刷による偽造防止技術がスコープに含まれる汎用的な評価方法の研究はいくつか報告されている。例えば、Wielandt［1998］においては、偽造防止技術の評価を行う際の留意点[21]を整理したうえで、個々の技術の偽造防止効果を定性的に 5 段階に分類し、個々の技術間の比較やそれらを組み合せた際の全体としての偽造防止効果の評価を行うというアイデアを示している。また、

[20] 検証者による人工物の特徴抽出が期待通りに実行されるためには、当該特徴の情報を検証者に提供し理解してもらう必要がある。そうした情報提供の方法のあり方についても学会等において検討が進められている（例えば、van Renesse［2006］）。

[21] 具体的は、評価者は製造者等の関係者と独立であること、評価の際には当該人工物やシステムの詳細な仕様・材料・製造方法を参照できること、技術の偽造防止効果や品質は時間とともに低下することを意識しておくことといった指摘がなされている。

Saksena, Dubbel, and Spicer［2002］とSaksena and Lucarelli［2004］においては、技術仕様が秘匿されている偽造防止技術を対象にその仕様解明と人工物偽造のプロセスを確率モデルとして表現し、仕様解明の難易度とコストを試算する方法を検討しており、本試算によって仕様解明のコストと成功確率の関係を明らかにする方法を提案している。このように、印刷を含む偽造防止技術の効果の定量的な評価方法確立に向けた研究が進められているのが実情である。

(2)偽造防止目的のホログラムの技術

イ．偽造防止効果を高めるためのアイデア

ホログラムは、物体から反射したり透過したりする光（物体光と呼ばれる）と別の光（参照光と呼ばれる）を干渉させ、その干渉縞を記録した箔状の人工物であり、参照光を当てると当該物体の 3 次元画像が再生されるという特性を有する[22]。偽造防止目的のホログラムの多くは、光の種類や見る角度に応じて再生される図柄や色が複雑に変化するなど、カラー・コピー機やスキャナー等を利用しただけでは再現困難と期待される光学特性を備えている[23]。ホログラムの偽造防止効果はこうした光学特性の再現の困難さにあり、光学特性を左右するホログラムの物理構造や材料の改良・開発が偽造防止上重要となっている。

具体的には、電子線によるホログラム表面加工の微細化や薄膜形成技術に基づくホログラム材料の多層化等が挙げられる。その結果、再生画像の微細化、多色化（フルカラー画像の再生等）、複数チャネル化（1 つのホログラムにおける複数の再現画像の付与等、例：マルチチャネル・レインボー・ホログラム）、動画化（再現画像の連続的な変化の付与等、例：キネグラム、ホログラフィック・ステレオグラム）、立体化（奥行をもつ画像の再生等、例：マルチプレイン・レインボー・ホログラム）といった効果をもつホログラムが開発されている（van Renesse［2005］）。さらに、ホログラムにマイクロ文字を追加する、液晶や特殊フィルム等の光学素子と組み合せるといった手法も知られている（NRC［2007］）。

また、再生される画像を機械によって読み取り真偽判定を行う手法も開発されている。例えば、特定の光による再生画像と予め登録されていた画像を照合して真偽判定を行うという手法（大日本印刷［2008］）や、特定の波長帯に対して金属光沢を示す薄膜フィルム上にホログラムを形成し、ホログラムと薄膜フィルムによる複合的な効果を機械等によって読み取り真偽判定を行うという手法が挙げられる（Takeuchi *et al.*［2000］）。

---

[22] 物体からの光を記録・再現する技術はホログラフィと総称されている。

[23] このような光学特性を備えた素子は一般に光学的変化素子（optically variable device）と呼ばれており、ホログラムは光学的変化素子の 1 つとなる。

ロ．偽造防止効果の評価方法に関する検討

前述の各種ホログラムのなかで特定のアプリケーションに相応しいものを適切に選択する際には、それらの耐クローン性の評価が必要となる。耐クローン性は、特徴抽出能力や判定実行能力に左右されると考えられるが、現時点では印刷技術の場合と同様、個々のホログラムに関する技術情報や評価結果の詳細が公開されるケースは少なく、評価方法についても研究段階にある[24]。

最近の主な研究報告の 1 つとして、回折格子型光学的変化素子における偽造防止効果の評価方法の提案が挙げられる（Andrade and Rebordão［2002］）。本研究は、回折格子型光学的変化素子のセキュリティ特性を基に評価項目と各項目の評価値を設定してモデルを構築し、重み付けした評価値を合算して当該素子のスコアを算出するという方法を提案するものである。回折格子型光学的変化素子のセキュリティ特性として、一般の検証者の視覚による真偽判定、専門知識を有する検証者による真偽判別（装置による認証を含む）、偽造への耐性の 3 つを挙げ、さらに全体で 17 の評価項目に細分化したモデルを示している[25]。各評価値や重みは当該素子の開発者やユーザによって決定される扱いとなっているほか、実用されている 3 つの素子に対して本方法を適用した場合の評価事例が示されている。本方法には評価項目や評価値の妥当性の確認等いくつかの検討課題が存在するものの、回折格子型光学的変化素子の評価方法の確立に向けた取組みとして注目される。

また、関連する動向として、ホログラムの記録材料における光学的特性の評価方法の標準化が注目される。仮にホログラムの評価方法がまちまちであり期待どおりの品質を達成していないホログラムが普及すると、想定よりも簡単にホログラムの偽造が可能となるおそれが出てくる。こうした問題を回避するうえで、本評価方法の標準化は重要である。わが国では、ホログラム用記録材料の中でもフォトポリマーを対象とした光学的特性測定方法の標準仕様書がTS Z 0019（日本工業標準調査会［2006］）として 2006 年に発行されている。本TSは、回折効率[26]等の指標を規定しており、従来各メーカーでまちまちであった指標の

---

[24] ホログラムにおいても印刷技術と同様に技術情報やホログラム材料の調達管理等が耐クローン性上重要となっており、ホログラムを供給するメーカーが適切な管理を実行しているか否かがポイントの 1 つとなる。欧州では、ホログラムの製造プロセスにおける管理の適切性に関するホログラム製造者の認証スキームが欧州標準化委員会（CEN: European Committee for Standardization）傘下において運営されている。国際ホログラム製造者協会（IHMA: International Hologram Manufacturers Association）のウェブサイトを参照されたい（http://ihma.org/content/hologram-manufacturers-certification.php）。

[25] 例えば、一般の検証者の視覚による真偽判定については、「人目を引くものであるか」、「視覚的な効果やデザインが認識しやすいか」、「画像変化等の特性の周知が行われているか」、「観察環境への依存性が高いか」等の 9 項目に細分化されている。

[26] ホログラムの回折効率は、再生される画像の明るさを表す尺度の 1 つであり、再生照明

測定方法を統一化するものとして注目される。現在、本TSをJIS化するプロジェクトが進められている（産業技術総合研究所［2006］）。

(3)偽造防止目的の暗号ハードウエアの技術

イ．偽造防止効果を高めるためのアイデア

暗号を実装するICチップ等のハードウエア（以下、暗号ハードウエアと呼ぶ）を人工物に埋込・貼付し、その動作を手掛かりとして当該人工物の真偽判定を行うという方法が、キャッシュカードやクレジットカード等の偽造防止目的で利用されている。こうした方法は、カードの検証装置が暗号ハードウエアと交信してデジタル署名等の演算結果によって真偽判定を実行することから、真偽判定時の特徴抽出能力や判定実行能力を比較的制御しやすい。したがって、ハードウエア自体の偽造防止の効果は、主に、当該ハードウエアからの不正な情報の読出しや内部の機能の改変に対する耐性（耐タンパー性）[27]や、ハードウエアの仕様や秘密情報が漏洩した際に同一の機能を有するハードウエアを製造することの困難性に依存すると考えられる（松本・岩下［2004］）。

暗号アルゴリズムや鍵管理方法等が適切に選択されているという状況下では、暗号ハードウエアの耐タンパー性を向上させるための技術（以下、耐タンパー技術と呼ぶ）は想定される攻撃法に応じて決定・適用されるが、そうした攻撃法として、暗号ハードウエアのパッケージを加工するタイプの攻撃（パッケージ加工型）と加工しないタイプの攻撃（パッケージ非加工型）が知られている（松本・大石・高橋［2008］）。

パッケージ加工型の攻撃としては、IC チップ等のカバーを開封し、極細のプローブやイオン・ビームを当てて回路構造を直接観察することによってアルゴリズム等を推定するという攻撃や、回路動作確認用のテスト回路を再利用できるように改変しICチップに格納されているデータを読み出すという攻撃が挙げられる。こうした攻撃への主な対策としては、加工に伴うハードウエアへの物理的な作用を検知し、ハードウエアのデータを消去したり処理を停止したりするという方法が挙げられる。例えば、イオン・ビーム等によるプローブを検知するセンサーの層を回路全体に形成するという方法や、クロック・サイクルの異常検知用センサーを設置するという方法が知られている（Kömmerling and Kuhn［1999］）。また、テスト回路をテスト後に再利用できないように破壊する

光の強度に対する回折光の強度の比率によって示される。

[27] 暗号ハードウエア内部には暗号鍵が秘密に格納され、仮に同一の仕様のハードウエアを作製可能としても、正当なハードウエアに格納されている鍵を入手できない場合には同一の暗号機能を実現できない仕組みとなっていることが多い。こうしたケースでは、暗号ハードウエアの偽造に成功するためには秘密の鍵の入手が必要となる。

という方法も知られている。

パッケージ非加工型の攻撃としては、例えば、意図しないチャネルから漏洩する情報（サイドチャネル情報、例：回路動作時の消費電力や処理時間のパターン）を手掛かりに署名生成鍵等を効率的に推定するという方法（サイドチャネル攻撃、Kocher, Jaffe, and Jun［1999］）や、レーザ光の照射等によって意図的に誤動作を発生させ、その際の処理結果を用いて署名生成鍵等を効率的に推定するという方法（故障利用攻撃、Boneh, DeMillo, and Lipton［1997］）が挙げられる。

サイドチャネル攻撃への対策の基本アイデアは、サイドチャネル情報と署名生成鍵との関連性を断ち切るという点にある。例えば、署名生成鍵による処理の途中のデータに乱数等を付加して当該データや処理の内容を動的に変化させるという方法、署名生成鍵による処理内容によらずサイドチャネル情報がほぼ一定となるようにするという方法、サイドチャネル情報自体にノイズを付加するという方法等が知られている（Mangard, Oswald, and Popp［2007］、Mayes and Markantonakis［2008］）。故障利用攻撃への対策としては、誤動作を引き起こすレーザ光の照射等をセンサーで検知し署名生成鍵による処理を停止させる、同一の処理を複数回実施してそれらの結果を比較し、誤動作の発生を検知した場合にはその誤りを訂正するといった方法が知られている（神永・渡邊［2005］）。

ロ．偽造防止効果の評価方法に関する検討

暗号ハードウエアのセキュリティ評価に関しては、一定の要件を充足しているか否かを第三者が評価・認証する制度的枠組みが整備されており、欧米のセキュリティ評価基準を基に作成されたコモンクライテリア（Common Criteria）に基づく制度と、米国連邦政府の情報処理標準規格FIPS 140-2やISO/IEC 19790に基づく試験・認証制度が挙げられる[28]。こうした枠組みは個々の暗号ハードウエアやそれらによって構成される情報システムを評価対象としているものの、評価を実施する機関がどのような手法によって評価を行っているかについては当該機関のノウハウとして一般には公開されないケースが多い。そのため、各種の耐タンパー技術の効果についてユーザ等が情報を得るためには、学会等のオープンな場における研究報告を参考にせざるを得ないのが実情である。

また、学会における研究報告を参考にするとしても、暗号ハードウエアの脆弱性や攻撃法に関する報告に比べて耐タンパー技術の評価方法に関する報告は少ないほか、個々の研究のベースとなっている暗号ハードウエアや実験環境がまちまちであり、研究成果を相互に比較することが困難なケースが多い。その

[28] わが国においても、これらに対応する制度として、「ITセキュリティ評価及び認証制度」と「暗号モジュール試験及び認証制度」がそれぞれ整備・運用されている。こうした制度の内容や現状については田村・宇根［2008］を参照されたい。

結果、耐タンパー技術の効果を横並びで定量的に評価するための手法はまだ確立されていないのが実情である。

こうしたなか、わが国の暗号技術検討会傘下の CRYPTREC 暗号モジュール委員会においては、サイドチャネル攻撃の実験評価用のハードウエアを用いて評価方法確立に向けた技術的な検討が行われている（情報通信研究機構・情報処理推進機構［2008］）。最近では、2007 年に、サイドチャネル攻撃実験用標準評価ボード（SASEBO）と同ボードで利用するテスト用暗号アルゴリズムのハードウエア回路データが産業技術総合研究所と東北大学によって開発され、暗号モジュール委員会はもとより、国内外の研究者によって利用されはじめている。今後、こうした共通の暗号ハードウエアにおける耐タンパー技術の評価研究、および、それらを活用した評価方法に関する研究の動向が注目される。

(4)バイオメトリクス

イ．人工物メトリクスとの関連性

バイオメトリクスは、身体的特徴や行動的特徴を用いて個人を認証する技術である（Jain, Bolle, and Pankanti［1999］）。代表的な身体的特徴として、指紋、手のひらや指の静脈パターン、虹彩、顔の輪郭、目鼻の形状や位置、声紋等を利用する認証システムが提案・開発されている。2001 年の同時多発テロ以降、米国を中心に開発・実用化が進み、わが国においては、2004 年頃から ATM における利用者の本人確認を中心に導入が本格的に始まり、空港等における入国管理をはじめとする幅広い分野で利用されている。

２節(3)において触れたように、バイオメトリクスという用語は人工物メトリクスという用語の語源となっており、両者は、認証対象が生きている個人か人工物かという点で異なっているものの、認証対象に固有の特徴を用いて認証を実行する、認証の形態は参照データとの整合性確認であるといった点で共通している。その結果、認証精度評価の尺度やセキュリティ評価の際に想定すべき脅威においても両者に共通して想定されるものが多い（松本ほか［2004］）[29]。

ロ．なりすましへの耐性の評価研究

バイオメトリクスにおいては、脅威としてなりすましを前提とした場合に想定される脆弱性と攻撃法が整理されている（図表 6 参照、情報処理推進機構［2006］）。図表 6 をベースとすれば、主な攻撃として、なりすまし対象となっている個人の身体的特徴の模造物を作製してセンサー等に提示する「模造物による攻撃」、行動的特徴を他人が模倣して提示する「模倣による攻撃」、他人で

[29] 人工物メトリクスが偽造防止技術の 1 つであることを考えると、偽造防止技術一般の評価について検討する際にも、バイオメトリクスの経験が参考になると考えられる。

図表 6：バイオメトリクスにおける主な脆弱性と攻撃

脆弱性	脆弱性の概要	脆弱性を利用した攻撃
生体特徴の偽造	顔、指紋、虹彩など、身体的特徴に基づくバイオメトリック認証技術には、生体に似せた人工物等によって他人になりすませる可能性がある。	模造物による攻撃
合成サンプル	合成したサンプルがシステムに受け入れられる場合があり、そうしたサンプルにより他人へのなりすましが起こる可能性がある。	
生存判定の欠如	生存判定機能が弱いバイオメトリック認証技術は、生存中の生体と生存していない生体を区別できないことがあり、切り離された他人の身体の一部を用いてなりすませる可能性がある。	
生体特徴の秘匿不能性	顔、指紋、声など体の表面の生体情報は、一般の生活において他人に知られないようにすることが困難であり、第三者に盗まれる危険性がある。盗まれた生体情報は、生体特徴の偽造や生体特徴の模倣を通じて、他人へのなりすましに利用される可能性がある。	模造物や模倣による攻撃
生体特徴の模倣	声紋、署名等、行動的特徴に基づくバイオメトリック認証技術には、他人の特徴を模倣して他人になりすませる可能性がある。	模倣による攻撃
生体情報データの漏洩と差替え	システムの各処理部の連結箇所には盗聴の危険性がある。また、連結箇所で不正なデータに差し替えられると、他人へのなりすましが起こる可能性がある。	
類似	生体情報の中には、異なる個人間で特徴が類似する場合がある。そうした個人間で互いになりすませる可能性がある。	類似した生体情報に基づく攻撃
特殊な生体特徴	稀に通常に比べて多くの他人に照合する人がいることがあり、なりすまし等に悪用される可能性がある。	

（備考）情報処理推進機構［2006］の記述を基に作成したもの。

あっても本人と類似する生体特徴を有するケースがあり、そうした生体特徴を何らかの手段で提示する「類似した生体情報に基づく攻撃」が挙げられる。

模造物による攻撃に関する研究としては、一部の市販の指紋照合装置において、生体の指で登録された参照データがゼラチン製の人工指によって提示された本人の指紋のデータと「一致」と高い頻度で誤判定するとの実験結果が報告されているほか（Matsumoto *et al.*［2002］）、同様の手法によって、虹彩や静脈パターンを利用した一部の照合装置の実験結果も示されている。また、模造物を一定の手順によって作製しそれらの受入率によって個々の照合装置における同攻撃法への耐性を評価しようするアプローチ（テスト物体アプローチと呼ばれる）についても研究が活発に進められている（例えば、松本・田中［2007］）[30]。

模倣による攻撃についても、手書き署名による認証を中心に攻撃法や対策に

[30] こうした模造物が受け入れられてしまう確率については、人工物メトリクスにおけるリプレイ攻撃等への耐性の評価尺度であるクローン一致率と同一とみることができる。こうした確率の算出については、バイオメトリクスの分野で先行して提案・検討されてきたものの、クローン一致率という評価尺度が先に定義・提案されたのは人工物メトリクスの分野であったという経緯がある。模造物による攻撃に関する研究の経緯については、松本・宇根［2005］を参照されたい。

関する研究が進められている。例えば、ペン先の位置と筆圧を用いる照合装置を対象とする強力な攻撃法として、ユーザが書き終わった署名のデータからペン先の位置と筆圧の時系列的変化を推定するアルゴリズムを開発し、その出力結果を用いてなりすましを試みるという手法が提案され、同攻撃の成功確率の評価結果が示されている（Hennebert［2007］）[31]。

類似した生体情報に基づく主な攻撃法としてはウルフ攻撃が該当する。ウルフ攻撃は、**3節(2)ロ**．において紹介したように、バイオメトリクスの分野において提案され、評価尺度であるウルフ攻撃確率に関する研究も進展している。最近では、一部の指静脈パターン照合アルゴリズムやマニューシャ照合アルゴリズムにおいて強力なウルフが存在することが報告されているほか、虹彩認証アルゴリズムにおいてもウルフの存在の可能性が指摘されている（小島ほか［2008］）。また、誤非合致率の上昇を抑えながらウルフ攻撃確率を一定水準以下とすることが可能な照合アルゴリズムの構成法の提案（Inuma, Otsuka, and Imai［2009］）や、強力なウルフを確率的に探索するアルゴリズムも提案されている。

ハ．評価結果の活用と新たな脆弱性への対応

上記のとおり、各種攻撃法とその耐性評価に関する研究が進展するなかで、研究成果を市販のシステムの評価に活用するための枠組みに関する議論・検討も進んでいる。セキュリティ評価・認証については、なりすましへの耐性評価をはじめとするセキュリティ評価をコモンクライテリアの枠組みに基づいて実施するための機構や手続を規定する国際標準（ISO/IEC 19792）の審議が進められている（三村［2007］）。こうした枠組み整備と並行してセキュリティ評価方法の技術的な検討が進展すれば、適切なシステムの選択を可能とする評価制度の実現につながっていくことが期待される。

ただし、評価制度が確立できたとしても、未知の脆弱性が後日顕現化した場合には、既に普及しているシステムの安全性や信頼性に深刻な影響が及ぶ可能性がある。こうした新たな脆弱性の発見に伴うメリット（より安全性・信頼性の高いシステムの研究開発への情報提供等）を享受しつつデメリット（当該脆弱性に関する誤解による風評被害等）を抑えるためには、脆弱性情報を適切に取扱うための枠組みが必要であるとの指摘がなされており（例えば、瀬戸［2005］、日本自動認識システム協会［2007］）、同枠組みに関する本格的な検討も開始されつつある（情報処理推進機構［2008］）。

---

[31] 照合に利用される参照データが漏洩し、当該データから本人の生体特徴を推測する等の方法によってなりすましを試みるといった攻撃が考えられる。こうした参照データを不正に利用するというタイプの攻撃に対してはテンプレート保護技術と呼ばれる技術分野の研究が進められている。同分野の最新の動向については例えば山崎［2006］を参照されたい。

５．耐クローン性の評価方法の検討における今後の課題

３節で紹介したように、人工物メトリクスの研究開発が進展してきているものの、セキュリティ（特に、耐クローン性）に関する評価方法の確立が重要な課題として残されている。本節では、そうした課題と対応を考察する。

(1)人工物メトリック・システムにおけるセキュリティ評価上の課題

イ．先行研究が示唆する課題

人工物メトリック・システムにおけるセキュリティ評価上の課題として、先行研究である松本ほか［2004］は、「認証精度の評価方法の構築」、「耐クローン性の評価方法の構築」、「認証精度の評価基盤の構築」、「認証精度の基準値設定」を挙げている。ここでの「認証精度」は、「人工物をいかに正確に認証することができるか」を意味する用語として利用されており、耐クローン性も加味した意味で用いられている。

認証精度の評価方法の構築に関して、松本ほか［2004］は、バイオメトリクスの分野で確立された評価尺度（誤合致率、誤非合致率等）を参照可能となってきているほか、耐クローン性の観点では、クローン一致率等の独自の評価尺度が提案されているなど、認証精度の評価方法の構築に関連する検討が進展している旨を紹介している。そのうえで、「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進展を図ることが求められる」と説明している。

「耐クローン性の評価方法の構築」は認証精度の評価方法の構築に含まれる課題といえるが、松本ほか［2004］は特に重要な検討課題として挙げている。具体的には、「今後十分な議論と研究を進めたうえで評価手法の標準化に取り組む必要がある」としたうえで、「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」と説明されている。

認証精度の評価基盤の構築に関しては、「人工物メトリック・システムに固有の用語・概念や評価方法を確立し、標準化すること（が必要である）」と説明しており、他分野における評価基盤構築の事例として、コモンクライテリアによる評価･認証の枠組みや ISO/IEC JTC1/SC37 におけるバイオメトリクスの各種精度評価方法に関する国際標準の策定を挙げている。

認証精度の基準値設定に関しては、「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うえで、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うえ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」と説明している。

これらのいずれの項目も現時点における検討課題としてそのまま当てはまる

項目であり、以下では現在の検討状況を踏まえて考察する。

ロ．認証精度や耐クローン性の評価方法の構築

認証精度という（耐クローン性よりも）広い概念のなかで、「さらなる理論構築や評価技術の進展」が求められるのが耐クローン性の評価であると考えられる。田村・宇根［2007］において挙げられているように、クローン一致率をどのように測定すればよいか、ウルフ攻撃やハード・コピー攻撃への耐性の評価をどのように行うか、評価を実施する際に攻撃者が利用可能な資源をどのように考慮するか等の検討が今後必要であると考えられる。

こうした課題を検討するうえで、「どのようなクローンを前提として評価を行うことが妥当か」を明らかにすることが求められる。人工物を偽造するタイプの攻撃の場合、クローンの作製方法として原理的には莫大な数のバリエーションが想定され、特定のクローンを前提とした評価結果が他のクローンにおいても同様に成立するか否かは定かでない。多くの想定されるクローンの評価結果を代表するような特定のクローン（の集合）が明確になれば、そうした「基底」のような位置付けのクローンに関する評価を優先的に実施し、評価結果を複数の人工物メトリック・システム間の比較に利用することが考えられる。クローンを作製する際には当該クローンの材料や加工方法がポイントとなることから、候補となる材料に関する技術や加工技術の動向も考慮するなど、学際的な検討が必要になると考えられる。

本課題の重要性はバイオメトリクスの分野においても認識されており、テスト物体アプローチによって市販のシステムの評価を実施するプロジェクトが米国の金融業界を中心に進められている（IBG［2006］）。こうしたバイオメトリクスの分野における先行研究の成果を適切に活用することも今後重要である。

ハ．認証精度の評価基盤の構築

上記**ロ**．の評価方法の検討と並行して、評価基盤の構築に向けた検討の進展が望まれる。人工物メトリクスを含む偽造防止技術を対象とする評価基盤構築に向けた検討については、業界団体における偽造防止技術に関する情報の共有や業界横断的な用語・概念の整理等を目的とした欧州における活動の事例や、偽造防止技術の国際標準化に向けた活動の事例が挙げられる。

欧州においては、偽造品検知の手順（Protocols for Detection of Counterfeits）をテーマとする偽造防止技術の検討部会（Workshop on Anti-counterfeiting）が欧州標準化委員会（CEN: Comité Européen de Normalisation）において、2007 年に設置されている（Lancaster［2008］）。本検討部会は、ブランド品メーカー等の偽造防止製品ユーザや偽造防止製品メーカーを中心に 28 のメンバー（2007 年 10 月

2 日時点）が参画し、関係者間の情報交換、偽造防止の機能や役割に関する理解向上、偽造品検査の標準的な手続やプロトコルの検討を主な目的としている。CEN の本検討部会での議論は、具体的な欧州標準の策定を視野に入れたものか否かは現時点で定かでないが、オープンな場の議論として位置付けられており、偽造防止技術の評価に関する共通認識の確立に向けた動きとして注目される。

国際標準の場においては、2008 年、各種製品の偽造や横流し等の不正行為への対策をスコープとする国際標準化の推進母体となる専門委員会（TC: technical committee）をISO傘下に設置してはどうかとの提案が米国のANSIおよびNASPO[32]からISO事務局に対して行われた（NASPO［2008］）。NASPOの提案書では、TC68（金融）、TC223（社会セキュリティ）、TC34（食品）等の専門委員会において各種製品の不正行為への対策に関する検討が今後求められるようになるとしており、そうした業界横断的な検討を行うTCの設立が望まれるとの見方が示されている。そのうえで、不正行為への対策に関する用語や概念の整理、各種製品のメーカーにおける生産・物流管理やリスク管理のガイドライン策定がスコープに含まれるほか、各種の不正行為を防止するための認証用機器のセキュリティ評価方法や評価のための枠組み、金融取引に用いられる書類やシステムについても標準化の対象にしてはどうかとのアイデアが記述されている。

本提案については、ISO の技術管理評議会（TMB: technical management board）において2009年2月に承認され、偽造防止技術を対象とする専門委員会がTC247（fraud countermeasures and control）として組成されることとなった。今後、偽造防止技術に関する評価基盤の検討がISOにおいても行われることが期待される。

また、**４節(4)ハ.** において紹介したように、人工物メトリクスと非常に近い分野であるバイオメトリクスにおいては、バイオメトリック認証システムのセキュリティ評価・認証の枠組みに関する検討が ISO/IEC 19792 の国際標準化とともに進められている。同標準では、セキュリティ評価を実施する際に評価対象となりうる各種脆弱性や対策、評価の手続等が規定される見通しとなっており、人工物メトリクスにおける評価基盤の検討の際にも参考になると考えられる。

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

ニ．認証精度の基準値設定

認証精度の基準値については、評価方法や評価基盤が確立した後の次の検討課題となる。基本的には各アプリケーションに依存して決定されることとなるが、金融分野においても、カード類をはじめとする金融取引用の人工物に関して認証精度の基準値を検討する場面も将来的には想定される。

こうした検討の際に参考になると考えられるのは、バイオメトリクスの分野におけるシステムの運用要件の導出指針の標準仕様書（TS X 0100、日本工業標準調査会［2004］）である。本標準仕様書では、各アプリケーションの要求条件から各種評価尺度の要求値を導出する方法が記述されており、人工物メトリック・システムにおける認証精度の基準値を検討するうえで参考になる。また、本標準仕様書をベースとする運用要件の国際標準化がバイオメトリクスに関する国際標準化を担当する ISO/IEC JTC1/SC37 において進められており（瀬戸［2008］）、本標準化の今後の動向も注目される。

(2)他の偽造防止技術との比較を可能にする評価方法に向けた検討

偽造防止技術の採用をユーザが検討する際には、人工物メトリクスを含むさまざまな候補技術を耐クローン性の観点からも比較できることが望まれる。ただし、異なる原理に基づく技術間の比較は容易でなく、現時点では定性的かつ主観的な比較の段階に止まっている（van Renesse［2005］、NRC［2007］、Church *et al.*［2008］）。今後、人工物メトリック・システムの評価方法の検討を進める際には、将来的に他の偽造防止技術と横並びで評価できるようにすることも念頭において検討することが重要である。

各種の偽造防止技術の原理や特性が多岐にわたっている点を考慮すると、あらゆる偽造防止技術を対象に検討を開始するよりも、比較的類似した特性や真偽判定の形態を有する技術群を選択し、それらに適用可能な評価方法の検討から着手するというアイデアが方向性の 1 つとして考えられる。

こうしたアイデアに関連するセキュリティ評価方法の検討事例として、バイオメトリクスの分野における松本＝田中の研究が挙げられる（松本・田中［2008］）。本研究では、個々のシステムではなく、赤外透過光によって非接触で生体情報を取得し認証を実行するシステム群を対象としたうえで、テスト物体アプローチを適用する際の汎用的なテスト物体の構造とその作製方法を提案している。本研究は、赤外透過光によって生体情報を取得するタイプのシステム群をカバーするものであり、今後本研究が精緻化されれば、静脈パターンであっても指の真皮のパターンであっても赤外透過光を用いるシステムであれば本手法によって統一的に評価可能になることが期待される。

人工物メトリクスやその他の偽造防止技術に本アイデアを適用することを想

定すると、例えば、２節(2)で紹介した真偽判定の 3 つのバリエーションや、人工物の特徴の情報を抽出する際に利用される物理特性の種類等に焦点を当てて、同一のカテゴリーに属する技術群に適用可能な評価方法を検討するという方向性が考えられる。

例えば、人工物表面の凹凸の形状に依存して決定される反射光のパターンを利用する偽造防止技術というカテゴリーで考えると、ホログラムの再生画像を利用した偽造防止技術や LSA のようなスペックル・パターンに基づく人工物メトリクスが同カテゴリーに含まれる。ホログラムの場合には、ホログラムの製造者が、当該再生画像を決定したうえで、実際に一定の精度で再生されるようにホログラムの物理構造を設計・製造する。一方、スペックル・パターンに基づく人工物メトリクスでは、基本的には、真偽判定の対象となる人工物になんら特別な処理が加えられず、製造過程で得られる人工物の物理構造が利用される。こうした差異を考慮したうえで、双方の耐クローン性評価に適したクローンの効率的な作製方法を探索するといった研究テーマが考えられよう。

また、人工物における演算処理結果を基に真偽判定を行う技術というカテゴリーで考えると、例えば、暗号ハードウエアにおけるデジタル署名を用いて真偽判定を行うという技術と、コーティング PUF やイントリンシック PUF といった人工物メトリクスが、同一のカテゴリーに含まれることとなる。暗号ハードウエアにおけるデジタル署名による技術の場合、秘密に割り当てられた署名生成鍵が各暗号ハードウエア内部に格納されており、それが漏洩しないようにどのようにして保護しつづけるかが耐クローン性を考えるうえでのポイントとなる。これに対して、PUF の場合、署名生成鍵がメモリ上にデータの形で格納されているわけではないという点で異なる。ただし、PUF の出力を利用して実行される署名生成処理に対してサイドチャネル攻撃をはじめとする攻撃法が適用可能か否かについては明確になっていないのが実情である。このように考えると、少なくとも、暗号ハードウエアの耐タンパー性の評価方法の文脈で議論されている事項が PUF にも適用できるか否かといった検討課題が想起される。

こうした検討を、バイオメトリクスにおけるテスト物体アプローチの研究成果等も参照しながら進めていくことが有用であろう。

６．おわりに

人工物メトリクスは、各人工物に固有の特徴を利用して認証を行うという技術であり、近年、新しい手法の提案や人工物の偽造への耐性の評価に関する研究が発表されてきている。特に、紙やプラスチック・カードに埋め込まれた磁性ファイバーからの電気信号を利用するシステム、人工物表面の光のスペックル・パターンを利用したシステム、IC 保護コーティングにおける電荷量を利用したシステム等、商用製品として提供される人工物メトリック・システムのバリエーションも徐々に増えてきている。

こうした状況を踏まえると、人工物メトリクスを機械読取による真偽判定を行う偽造防止技術の 1 つと位置付け、各種カード等の人工物を用いた金融取引の安全性や真正性を確保する手段として活用していくことが考えられる。今後、人工物の偽造の困難性評価をはじめとして人工物メトリクスをさまざまな角度から評価する方法を検討するとともに、人工物メトリクスがどのようなアプリケーションに適用することが望ましいかを明確にしながら、他の偽造防止技術と横並びで評価する方法についても検討していくことが望まれる。

本稿では、人工物メトリクスの最近の研究開発動向について紹介したうえで、主としてセキュリティ評価という観点から、印刷による偽造防止技術等の動向や、人工物メトリクスの語源となったバイオメトリクスの検討状況を紹介した。そのうえで、技術分野によってまちまちではあるが、セキュリティ評価方法の開発に向けた検討が進展している旨を説明し、今後の課題として、人工物メトリクスにおける評価方法や評価基盤の検討、および、他の技術と比較可能な評価方法のアイデアについて考察した。今後、人工物メトリクスの研究開発や偽造防止技術の横並びでの評価を実現させるうえで、バイオメトリクスにおける知見や議論を参考にするほか、情報セキュリティ技術や印刷技術等、関連分野の専門家と議論しながら進めていくことが有用である。

こうした点を踏まえ、人工物メトリクスの分野自体に加えて、バイオメトリクスをはじめとする関連分野の動向をフォローしていくとともに、各分野の専門家との議論を通じて金融分野における人工物メトリクスの活用のあり方を検討していくことが重要であろう。

以　上

参考文献

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

池田文人・徳永史生、「総論：視覚情報の処理と利用」、『情報処理』vol.50、no.1、情報処理学会、2008 年、3～7 頁

宇根正志・田村裕子、「生体認証における生体検知機能について」、『金融研究』第 24 巻別冊第 2 号、日本銀行金融研究所、2005 年、1～56 頁

――――・松本　勉、「生体認証システムにおける脆弱性について：身体的特徴の偽造に関する脆弱性を中心に」、『金融研究』第 24 巻第 2 号、日本銀行金融研究所、2005 年、35～83 頁

神永正博・渡邊高志、『情報セキュリティの理論と技術：暗号理論から IC カードの耐タンパー技術まで』、森北出版、2005 年

技術情報協会、『先端偽造防止技術―事例集―』、技術情報協会、2004 年

小島由大・繁富利恵・美添一樹・井沼 学・大塚 玲・今井秀樹、「虹彩認証におけるウルフ攻撃確率の理論的考察」、『2008 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、2008 年

財務省印刷局、『連携 IC カード券面の偽造防止技術ハンドブック』、財務省印刷局、2002 年

産業技術総合研究所、「従来の 1/1000 以下の微細液滴を吐出する超微細インクジェット技術を開発」、『産業技術総合研究所プレスリリース』、2002 年 4 月 1 日

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

情報機構、『ホログラム最新技術～感光材料の開発から実製品への応用まで～』、情報機構、2006 年

情報処理推進機構、『バイオメトリクス・セキュリティ評価に関する研究会・平成 18 年度研究会中間報告書』、情報処理推進機構、2006 年

――――、『バイオメトリクス・セキュリティ評価に関する研究会・調査報告書』、情報処理推進機構、2008 年

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

瀬戸洋一、「バイオメトリクスの脅威及び脆弱性公開におけるガイドライン」、『第 5 回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発表会予稿集』、電子情報通信学会、2005 年、29～36 頁

――――、「SC37（Biometrics／バイオメトリクス）総会報告」、『情報技術標準 NEWSLETTER』no.79、情報処理学会情報規格調査会、2008 年、19～21 頁

大日本印刷、「大日本印刷　国内初　エンボス型ホログラムの真贋を判定する画像処理技術を開発」、『大日本印刷ニュースリリース』、大日本印刷、2008 年 2 月 27 日

田村裕子・宇根正志、「人工物メトリック・システムにおける耐クローン性について　―どのように耐クローン性を評価するか―」、『信学技報』ISEC2007-91、電子情報通信学会、2007 年、15～22 頁

――――・――――、「情報セキュリティ製品・システムの第三者評価・認証制度について：金融分野において利用していくために」、『金融研究』第 27 巻別冊第 1 号、日本銀行金融研究所、2008 年、79～114 頁

――――・――――、「人工物メトリクスにおける耐クローン性の評価方法の構築に向けて」、日本銀行金融研究所ディスカッション・ペーパー・シリーズ、2009-J-3、日本銀行金融研究所、2009 年

日本工業標準調査会、『TS X 0100 : バイオメトリクス認証システムにおける運用要求の導出指針』、日本規格協会、2004 年
————、『TS Z 0019 : ホログラム用記録材料―フォトポリマー―光学的特性測定方法』、日本規格協会、2006 年
日本自動認識システム協会、『バイオメトリクス・セキュリティ・コンソーシアム安全ワーキング・グループ平成 18 年度活動報告書』、日本自動認識システム協会、2007 年
平良允俊・山越　学・松本　勉、「紙の赤外透過光を用いた人工物メトリクスの耐クローン性評価」、『2007 年暗号と情報セキュリティシンポジウム予稿集』no.2F4-6、電子情報通信学会、2007 年
松本　勉・岩下直行、「金融業務と人工物メトリクス」、『金融研究』第 23 巻第 1 号、日本銀行金融研究所、2004 年、169～186 頁
————・宇根正志、「バイオメトリクス認証の実用におけるぜい弱性と対策」、『電子情報通信学会誌』vol.90、no.12、電子情報通信学会、2007 年、1051～1055 頁
————・大石和臣・高橋芳夫、「実装攻撃に対抗する耐タンパー技術の動向」、『情報処理』vol.49、no.7、情報処理学会、2008 年、799～809 頁
————・田中瑛一、「指静脈認証システムのテスト物体によるセキュリティ測定法の研究」、『2007 年暗号と情報セキュリティシンポジウム予稿集』no.3F3-4、電子情報通信学会、2007 年
————・————、「透過光利用バイオメトリック認証システムのためのテスト物体作製方法」、『2008 年暗号と情報セキュリティシンポジウム予稿集』no.3B4-1、電子情報通信学会、2008 年
松本弘之・宇根正志・松本　勉・岩下直行・菅原嗣高、「人工物メトリクスの評価における現状と課題」、『金融研究』第 23 巻別冊第 1 号、日本銀行金融研究所、2004 年、61～140 頁
三村昌弘、「バイオメトリクスの現状」、『連続セミナー2007「情報セキュリティ 2.0 第 5 回バイオメトリクスの現状と今後」予稿集』、情報処理学会、2007 年
山崎　恭、「安全性対策技術の動向」、『情報処理』vol.47、no.6、情報処理学会、2006 年、600～604 頁

Andrade, Ana A., and José M. Rebordão, “Evaluation of DOVID Security under First Line Inspection,” *Proceedings of SPIE*, Vol.4677, SPIE-IS&T, 2002, pp.299-313.
Boneh, Dan, Richard A. DeMillo, and Richard J. Lipton, “On the importance of checking cryptographic protocols for faults,” *Proceedings of EUROCRYPT `97*, LNCS 1233, Springer-Verlag, 1997, pp.37-51.
Bösch, Christoph, Jorge Guajardo, Ahmad-Reza Sadeghi, Jamshid Shokrollahi, and Pim Tuyls, “Efficient Helper Data Key Extractor on FPGAs,” *Proceedings of CHES 2008*, LNCS 5154, Springer-Verlag, 2008, pp.181-197.
Brzakovic, Dragana, and Nenad Vujovic, “Authentication of random pattern by finding a match in an image database,” *Image and Vision Computing*, 14, 1996, pp.485-499.
Buchanan, James D. R., Russell P. Cowburn, Ana-Vanessa Jausovec, Dorothee Petit, Peter Seem, Gang Xiong, Del Atkinson, Kate Fenton, Dan A. Allwood, and Matthew T. Bryan, “Forgery: ‘Fingerprinting’ documents and packaging,” *Nature*, 436 (475), 2005, p.475.
Church, Sara, Theodoros Garanzotis, Martine Lacelle, and Andrea Firth, “Methodology for Establishing Bank Note Security Requirements,” *Proceedings of ODS 2008*, 2008.
DeJean, Ferald, and Darko Kirovski, “RF-DNA: Radio-Frequency Certificates of Authenticity,” *Proceedings of CHES 2007*, LNCS 4727, Springer-Verlag, 2007, pp.346-363.
Devadas, Srinivas, Edward Suh, Sid Paral, Richard Sowell, Tom Ziola, and Vivek Khandelwal, “Design and Implementation of PUF-Based “Unclonable” RFID ICs for Anti-Counterfeiting and Security Applications,” *Proceedings of IEEE International Conference on RFID 2008*, IEEE, 2008, pp. 58-64.

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

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

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

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

Guajardo, Jorge, Sandeep S. Kumar, Geert-Jan Schrijen, and Pim Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," *Proceedings of CHES 2007*, LNCS 4727, Springer-Verlag, 2007, pp.63-80.

Haslop, John M., "Security Printing Techniques," *Optical Document Security Second Edition*, Rudolf L. van Renesse (Eds.), Artech House, 1998, pp.151-168.

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

Hennebert, Jean, Renato Loeffel, Andreas Humm, and Rolf Ingold, "A New Forgery Scenario Based on Regaining Dynamics of Signature," *Proceedings of ICB 2007*, LNCS 4642, Springer-Verlag, 2007, pp.366-375.

Hu, Min, Jingyi Chen, Zhi-Yuan Li, Leslie Au, Gregory V. Hartland, Xingde Li, Manuel Marqueze, and Younan Xia, "Gold nanostructures: engineering their plasmonic properties for biomedical applications," *Chemical Society Review*, 35, 2006, pp.1084-1094.

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

International Biometric Group (IBG), *Spoof 2007: High-Level Test Plan, Draft 1.0*, IBG, 2006.

Inuma, Manabu, Akira Otsuka, and Hideki Imai, "A new framework for constructing matching algorithms secure against the wolf attack in biometric authentication systems," *Proceedings of SCIS 2009*, 2F2-4, IEICE, 2009.

Jain, Anil, Ruud Bolle, and Sharath Pankanti, *BIOMETRICS: Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999.

Kocher, Paul, Joshua Jaffe, and Benjamin Jun, "Differential Power Analysis," *Proceedings of CRYPTO`99*, LNCS 1666, Springer-Verlag, 1999, pp.388-397.

Kömmerling, Oliver, and Markus G. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors," *Proceedings of USENIX Workshop on Smartcard Technology*, 1999, pp.9-20.

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

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

Macfaland, Adam D., and Richard P. Van Duyne, "Single Silver Nano Particles as Real-Time Optical Sensors with Zeptomole Sensitivity," *Nano Letters,* 3 (8), 2003, pp.1057-1062.

Mangard, Stefan, Elisabeth Oswald, and Thomas Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Springer-Verlag, 2007.

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

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

Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino, "Impact of artificial `Gummy' fingers on fingerprint systems," *Proceedings of SPIE*, vol.4677, SPIE-IS&T, 2002, pp.275-289.

Mayes, Keith E., and Konstantinos Markantonakis, *Smart Cards, Tokens, Security and Applications*, Springer-Verlag, 2008.

McGrew, Stephen P., "Hologram Counterfeiting, Problems and Solutions," *Proceedings of SPIE*, Vol. 1210, SPIE-IS&T, 1990, pp.66-76.

————, “Countermeasures Against Hologram Counterfeiting,” *Proceedings of Optical Security Systems Symposium*, 1987.

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

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

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

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

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

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

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

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

————, *Optical Document Security*, Third Edition, Artech House, 2005.

————, “Public Education by Central Banks on the Internet,” *Proceedings of SPIE*, Vol.6075, SPIE-IS&T, 2006, pp.607504-1-607504-11.

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

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

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

Schell, Karel J., “The Historical Development of Security Printing: Design and Technology,” *Optical Document Security Second Edition*, Rudolf L. van Renesse (Eds.), Artech House, 1998, pp.131-150.

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

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

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

Takeuchi, Itsuo, Kenji Yamamotoyama, Tsugutaka Sugahara, Hidekazu Hoshino, Hiroyuki Matsumoto, and Tsutomu Matsumoto, “CPLgram: an advanced machine readable OVD that is obtained by combining diffraction gratings and liquid crystals,” *Proceedings of SPIE*, Vol. 3973, SPIE-IS&T, 2000, pp.238-246.

Tobias, Kraus, Laurent Malaquin, Heinz Schmid, Walter Riess, Nicholas D. Spencer, and Heiko Wolf, “Nanoparticle Printing with Single-Particle Resolution,” *Nature Nanotechnology*, 2 (9), 2007, pp.570-576.

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

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

Une, Masashi, Akira Otsuka, and Hideki Imai, “Wolf Attack Probability: A Theoretical Security Measure in Biometric Authentication Systems,” *IEICE Trans. Inf. & Syst.*, E91-D (5), IEICE, 2008, pp.1380-1389.

Wielandt, Ralph Tadema, “The Evaluation of Document Fraud Resistance,” *Optical Document Security Second Edition*, Rudolf L. van Renesse (Eds.), Artech House, 1998, pp.57-73.

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