人工物メトリクスによってICカードのセキュリティを高める方法☆

松本 勉† 青柳 真紀子†

カードや証書など物理媒体の偽造防止のために，ICチップを用いて耐タンパー性を高める方法は有効である．しかし，ICチップへの直接的あるいは間接的な各種攻撃を考慮した場合，単純なICカード化では達成可能なセキュリティに限界がある．本稿では，カードや文書などの個々の人工物に対して異なるランダムな固有パターンを付与しておき，そのパターンの照合によって真贋判定をする，「人工物メトリクス」という技術を，ICチップと組み合わせて用いる方法によるカードセキュリティ強化の可能性について論じる．

A Method of Applying Artifact-metrics for Enhancing Smart Card Security

Tsutomu Matsumoto† and Makiko Aoyagi†

Using Integrated Circuit chips (IC chips) to make documents and cards tamper-resistant is very effective for deterring counterfeits. However smart cards i.e., plastic cards that install IC chips have limitations on their tamper-resistance because of the emerging various types of direct and indirect attacks. To greatly enhance the total security of smart cards it is promising to adopt technology categorized as *Artifact-metrics*, or the use of intrinsic patterns randomly created on the individual body of smart cards.

1. はじめに

一般的な取引において，証書，証券，紙幣，プラスチックカードなどの人工的に製造された物理媒体（人工物）を利用した，いわば古典的手法が依然として用いられている．これらの物理媒体の偽造防止方法としては，透かしやマイクロプリンティングやホログラムなど，製造者側の技術的優位性を安全性の根拠としたものが主流であった．しかし，近年の画像処理技術の発達やディジタル機器の高性能化・日用品化にともなう，攻撃者側の使える技術の進歩にともない，製造者側の優位性のマージンが失われつつあり，紙やカードなどの人工物のセキュリティは，大きな脅威にさらされているといえよう．

このような状況において，クレジットカードやキャッシュカードなどの偽造防止対策として，ICチップを用いて耐タンパー性を高める方法が提案され普及している．しかし，ICチップを用いたカードについては，直接的，間接的な解析法が存在することが明らかとなっており[1)~4)]，単純にICカード化するだけでのセキュリティ上の限界があることも指摘されはじめている．そこで，この限界を打ち破ることを検討することは意義がある．

本稿では，「人工物メトリクス」とよばれる技術[5)~11)]を活用することによりICチップを内蔵する人工物であるICカードのセキュリティが強化できる可能性があることを示す．なお，この内容は，日本銀行金融研究所第6回情報セキュリティシンポジウム「金融分野における人工物メトリクス」のパネル討論（文献11)，p.165）において筆者の1人（松本）が示した見解「ICカードに人工物メトリクスを適用することによって，仮にICカードの耐タンパー性が破られたとしても，人工物メトリクスによってICカードの偽造・複製の有無を検証することができるという意味で，ICカードのセキュリティ向上に人工物メトリクスを活用することができる．ICカードの場合にはICチップを使用不能にするという攻撃が考えられるが，人工物メトリクスの場合には，人工物の固有パターンがすべて破壊されない限り，人工物の認証を行う余地が残るという

† 横浜国立大学大学院環境情報研究院
Graduate School of Environment and Information Sciences, Yokohama National University

☆ 本稿は文献12)を発展させたものである．

長所がある」を，やや詳細化して論じるものである．

2. IC チップの利用

2.1 IC カードシステムの構成

クレジットカードや銀行のカードは最近まで磁気ストライプに情報を書き込み，端末で読み取って利用する方式が主流であった．しかし，このタイプのカードの偽造が増加したことを背景に，IC チップを用いて耐タンパー性を高めた方式，すなわち IC カード/スマートカードの適用が拡大しつつある．IC チップは CPU を内蔵し，端末からの電源供給を受けて処理を行う．基本機能としてアクセス制御などの制御機能，情報の管理などの管理機能，暗号化などのセキュリティ機能を持つ．

2.2 IC カードシステムの構成

本稿で考察する IC カードシステムは，IC カード，リーダ/ライタ，端末からなるものとする．一般に IC カードの種類として接触型，非接触型，一体型（接触，非接触両方の特性を持つ）がある．接触型の IC カードは IC チップ，リーダ/ライタとの接点である接触端子，チップが載っているプラスチックカードからなる．また，それに加えて磁気ストライプを有しているものもある．非接触型はリーダ/ライタと直接接触しないので，端子のかわりにアンテナコイルが内蔵されている．IC カードシステムにおける認証手続きにおいて取り扱う情報としては，カードの ID，秘密鍵などの秘密情報，所有者情報（PIN など），管理・制御情報があげられる．またそれらの情報がどこに保管され，どこで処理されるかによって，さまざまな実装方式がある．

2.3 IC カードの脆弱性

IC チップを用いることによって，磁気ストライプカードよりもはるかにセキュリティ面が強化されるとされている．一方で，プロービングや FIB（Focused Ion Beam），EB（Electron Beam）などによる直接的な解析方法や，故障利用攻撃やサイドチャネル攻撃などの間接的な解析法が提案されるなど，脆弱性があることも明らかになっている[1)~4)]．特にサイドチャネル攻撃は，攻撃に特殊な装置や技術を必要とせず，一般に攻撃にかかるコストが低い．また，攻撃の痕跡を残さないため，攻撃の発見が遅れやすく，被害が拡大する可能性があることも大変な脅威である．こういった攻撃に対する対策として，攻撃を受けたとしてもそのことが検出できれば，被害を小さくとどめることができる．

3. 人工物メトリクスの適用

3.1 人工物メトリクス

「人工物メトリクス（artifact-metrics）」とは，著者の 1 人（松本）がバイオメトリクス（biometrics）という用語を参考にして，人工物（artifact）と測定（metrics）を組み合わせた造語であり，一言でいえば「人工物に固有の特徴を用いて人工物を認証する技術」という意味である．典型的には，人工物の個体に対して，各々異なるランダムな固有パターン（人間の指紋や虹彩に相当するもの）をあらかじめ付与しておき，取引のつど，その固有パターンを計測し，事前に計測されて保存されていたパターン情報と照合することによって，人工物が本物であるかどうかを検証する技術のことを指す．このような目的で用いられる固有パターンには，光学特性，磁気特性，電気特性，振動特性などのさまざまな物理的特性を用いたものがあり，たとえば，(イ）基材にランダム分散した［粒状物の光反射パターン/光ファイバの透過光パターン/ファイバの画像パターン/磁性ファイバの磁気パターン］,（ロ）基材のランダムな斑の透過光パターン,（ハ）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,（ニ）磁気ストライプ［にランダムに記録された/の製造時にランダムに配置された］磁気パターン,（ホ）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,（ヘ）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,（ト）容器に貼ったシールを振動させたときの共鳴パターン，などが提案されており[10)]，複製が困難であることが第 1 の要件となる．人工物メトリクスを実現する装置やシステムのことは，人工物メトリック・システム（artifact-metric system）とよばれる[5)]．

3.2 人工物メトリクスを取り入れた IC カードシステムの構成

文献 6) では（イ）の磁性ファイバを利用したものに関して，FRR（誤拒否率：False Rejection Rate）や FAR（誤受理率：False Acceptance Rate）などの指標を用いて，実際に人工物メトリック・システムの認証システムとしての評価を行っている．FRR と FAR はともに 0.01%程度であり，認証システムとして完成度が高いことが示されている．この技術は株券に利用されるなど大規模な実用化例もあり，人工物を認証する技術としての有効性が示されている[5)~11)]．

前述したように，IC チップを用いる偽造対策技術の脆弱性が指摘されているが，偽造や複製の防止・検知の意味で人工物メトリクス技術を用いることによっ

てICカードのセキュリティが強化できる．提案するシステムは，プラスチックカードが人工物メトリクスの意味での固有パターンを持つICカードシステムと定義する．3.1節であげた固有パターンの例の中では，基材に何らかの物質を分散させたときのパターン（イ，ロ，ハ，ヘ）を想定している．このシステムにおいて，認証手続時に取り扱う情報として，2.2節で示したものに加え人工物メトリクスのテンプレートデータがある．テンプレートデータとは，あらかじめ計測し記録したプラスチックカードの固有パターンを指す．

3.3 実装方式の例

ICカードシステムに人工物メトリクスを用いる方式については，テンプレートデータの保存場所や，照合処理を行う場所などの違いにより，いくつかの方式が考えられる．テンプレートデータの保管場所としては，① ICチップ内，② ICカードに添付された磁気ストライプなどの記録媒体，③ データベース．照合処理を行う場所としては，① ICチップ内，② 端末内，③ ホストなどが考えられる．これらをふまえると，実装方式として以下のようなタイプが考えられる．

A) テンプレート保管型
テンプレートをICチップ内に保管し，照合処理は端末で行う．

B) テンプレート保管処理組み込み型
テンプレートをICチップ内に保管し，照合処理もICチップ内で行う．

C) テンプレート添付型
テンプレートを記録媒体に記録してカードに添付しておき，照合処理は端末で行う．

D) テンプレート問合せ型
テンプレートをデータベースに保管し，照合時にデータを呼び出して処理する．

E) 処理問合せ型
テンプレートをデータベースに保管し，読み取ったデータを送ってホストで照合処理する．

それぞれのタイプにおいて，カード認証処理の際にはつねに人工物メトリクスによる認証を行う場合と，利用のつど毎回人工物メトリクスによる認証は行うとは限らないが，非常時や定期的な検査の際には行うという場合とが，考えられる．

また，ICカードには接触型のものと非接触型のものがあるが，人工物メトリクス利用のICカードについても接触型のものと非接触型のものが考えられる．人工物メトリクスを利用する場合，カードの読み取りにはリーダ/ライタと人工物メトリクスセンサが必要であり，その両方に対して接触，非接触の実装方法が考えられる（**表1**）．ICチップが接触型のものについては4章，非接触型のものについては5章で述べる．

表1 人工物メトリクス利用ICカードシステムの実装方式
Table 1 Classification of smart card system applying artifact-metrics based on sensor type.

	方式1	方式2	方式3	方式4
リーダ/ライタ	接触	接触	非接触	非接触
センサ	接触	非接触	接触	非接触

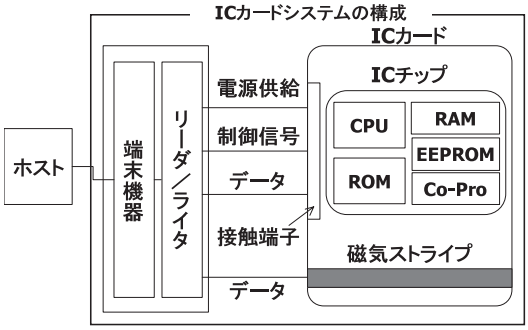

図1 ICカードシステムのモデル
Fig. 1 A model of smart card system.

4. システムのモデル（接触型ICカード）

ここまで，既存のICカードシステムと人工物メトリクスを取り入れたICカードシステムについて述べてきたが，実装方式はデータの取扱いや利用方法に応じて多様なものがある．以下では，両カードシステムについてある種の限定をした例をあげる．

4.1 接触型ICカードシステムのモデル

- 端末で読み取るカードの情報は，① ICチップ，および，② 磁気ストライプ，とし，券面デザインの認証などは行わないものとする．
- ICチップ内には秘密鍵，カードID，所有者情報が，磁気ストライプにはカードIDが保管されているとする．

システムの構成を**図1**に示す．

4.2 人工物メトリクス利用接触型ICカードシステムのモデル

- カードが人工物メトリクスの意味での固有パターンを持ち，認証に用いられる．
- 端末で読み取るカードの情報は，① ICチップ，② 磁気ストライプ，③ カードの固有パターン，とする．
- 利用時にはつねに人工物メトリクス認証をする．

人工物メトリクスセンサは接触（方式1）の場合と非接触（方式2）の場合が考えられるが，ここでは方式1についてシステムの構成を**図2**に示す．

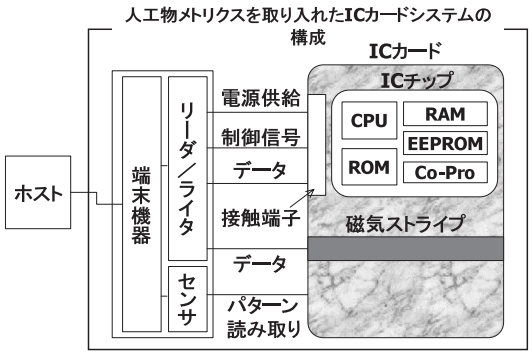

図 2 人工物メトリクス利用 IC カードシステムのモデル（方式 1）
Fig. 2 A model of smart card system applying artifact-metrics (System 1).

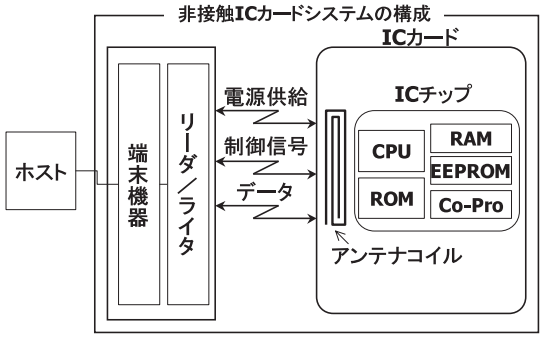

図 3 非接触 IC カードシステムのモデル
Fig. 3 A model of noncontact smart card system.

5. システムのモデル（非接触型 IC カード）

ここでは，非接触型のものについて，前章同様ある種の限定をした例をおいて両システムのセキュリティを比較する．接触型と比べ大きく異なる点は，接触端子のかわりに通信用のアンテナコイルが内蔵されている点と，磁気ストライプが添付されていないという点である．非接触型カードの場合，データの読み書きができる距離によって大きく密着型，近接型，近傍型の 3 つに分類されるが，ここでは特にそれについての限定はしないことにする．

5.1 非接触型 IC カードシステムのモデル

- 端末で読み取るカードの情報は，① IC チップ，とする．
- IC チップ内には秘密鍵，カード ID，所有者情報が保管されているとする．

システムの構成を**図 3** に示す．

5.2 人工物メトリクス利用非接触型 IC カードシステムのモデル

- カードが人工物メトリクスの意味での固有パターンを持ち，認証に用いられる．

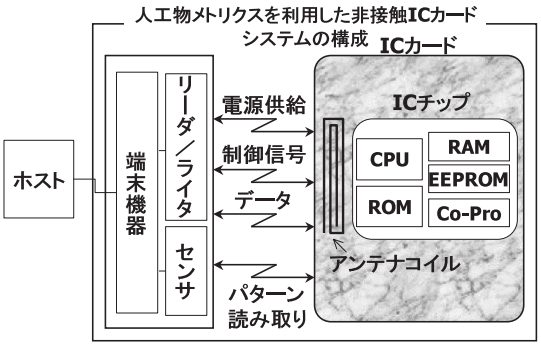

図 4 人工物メトリクス利用非接触 IC カードシステムのモデル（方式 4）
Fig. 4 A model of noncontact smart card system applying artifact-metrics (System 4).

- 端末で読み取るカードの情報は，① IC チップ，② カードの固有パターン，とする．
- 利用時にはつねに人工物メトリクス認証をする．

同様に人工物メトリクスセンサについては接触（方式 3）の場合と，非接触（方式 4）の場合が考えられるが，ここでは方式 4 についてシステムの構成を**図 4** に示す．

6. システムに対する攻撃と対策

4 章および 5 章であげた例について，既存の IC カードシステムと人工物メトリクスを取り入れた IC カードシステムについてセキュリティの比較を行う．

IC カードは正当な利用者が正しく利用でき，不当な利用者は利用することができないことが求められる．よって攻撃は，正当な利用者が正しくカードを利用できないようにする行為や不当な利用者が不正利用する行為，または不正利用するためのカードの解析行為とする．

人工物メトリクスを取り入れた場合，カードが攻撃されたときに固有パターンが変更されるようにしておけば攻撃を検知することができる．一方，すべての固有パターンを破壊することが困難なことから，攻撃をされても固有パターンが変更されないで残る可能性があり，カードの正当性を検証できる可能性がある．よって，カードのセキュリティを強化できる．

このことをより詳細に見るために，システムに対して考えられる攻撃を分類し，さらにそれらに対する対策を検討して**表 2** に整理した．ここでは IC カードとリーダ/ライタを通してやりとりされるデータ，またリーダ/ライタやセンサを含む端末機器への攻撃を考える．

- カードに対する攻撃の場合，その攻撃対象をプラ

表 2 IC カードシステムに対する攻撃と対策
Table 2 Attacks against smart card systems and measures to each attack.

	攻撃法	具体例	対策の方針	既存のICカードシステムにおける対応	人工物メトリクス利用 IC カードシステムにおける対応
カードに対する攻撃 1	カードを破壊する	折り曲げ，切断などをして物理的に破壊する．攻撃者は故意に正当な利用者へのサービス提供を阻害する．	カードの正当性が検証できるようにする． ※カードの正当性を証明できる方法があれば，カードの機能を回復できる．	チップは壊れていないので，アンテナコイルが破壊されなければ非接触のタイプなら利用できる可能性がある．	固有パターンをすべて破壊することは困難なため，カードの正当性を検証できる可能性がある．Ⅲ
	カードを改ざんする	カードの外見を一部書き換えて（顔写真など）不正に利用する．	カードに不正な処理が施されたことが検出できるようにする．	正規のカードの表面デザインや記載情報を登録しておき，カード表面のデザインなどを検査すれば検出できる．	カードの固有パターンが変更されるようにしておけば検出できる．Ⅱ
	チップを取り外す	カードを破壊して物理的にチップを取り外す．	カードが破壊された場合にその痕跡が残るようにする．	カードに残された痕跡を検査する手段があれば検出できる．	カードの固有パターンが変更されるようにしておけば検出できる．Ⅱ
	カードを偽造する	正規のチップを偽造したカードに入れて利用する．	プラスチックカードを認証する機能をもたせる．	プラスチックカードの真偽を検査する手段があれば検出できる．	カードの固有パターンを複製することは困難なため，テンプレートデータとの不一致により検出できる．
	磁気ストライプへの攻撃[1]	磁気ストライプを無効にしたり，改ざんしたりする．	磁気ストライプが不正に変更されたことを検出できるようにする．	チップ内のデータとの不一致により検証できる．	
	アンテナコイルを破壊する．[2]	アンテナコイルを破壊して通信できないようにする．	カードの正当性を検証できるようにする．	左記機能の実現．	固有パターンをすべて破壊することは困難なため，カードの正当性を検証できる可能性がある．Ⅲ
	カードの固有パターンを破壊する	カードを傷つけるなどして固有パターンの一部を破壊する．	効果的に固有パターンを破壊することが困難にする．		IC チップによってカードの正当性を検証できる． もしくは，固有パターンがすべて破壊されなければ，カードの正当性を検証できる可能性がある．Ⅲ

続く

スチックカードおよびアンテナコイル/接触端子か，IC チップとし，次のように分類する．

1. 「カードに対する攻撃 1」では，プラスチックカードおよびアンテナコイル/接触端子を攻撃対象とする攻撃である．
2. 「カードに対する攻撃 2」では，IC チップを攻撃対象とする攻撃である．
3. 「カードに対する攻撃 3」では，プラスチックカードおよびアンテナコイル/接触端子と，IC チップともに攻撃対象とする攻撃である．ただし，カードに対する攻撃 1，2 で述べたものは除く．

- 「データに対する攻撃」では，IC カードとリーダ/ライタ間でやりとりされるデータを攻撃対象とする攻撃である．ただし，リーダ/ライタや端末機器は正常に動作しているものとする．
- 「機器に対する攻撃」は，リーダ/ライタやセンサ，端末機器に対して，それらの改変や不正操作を行う攻撃である．

攻撃と対策について，接触型の場合，非接触型の場合で重複する部分が多いため，表の大部分は接触，非接触に共通していえることである．また，人工物メトリクスを取り入れたシステムに関しては，3.3 節で述べたタイプ A〜E すべてについて考慮している．ただし，表中の一部はいくつかの実装方式のみにおいて成り立つ項目である（表の注参照）．なお，表 2 において網掛けの部分は攻撃に対する対策方法が具体的に示せることを示す．人工物メトリクスを利用した場合，

カードに対する攻撃2	チップの無効化	チップを破壊して利用できなくする	チップ以外にもカードを認証する手段をもたせる.	プラスチックカードによって真偽を検査する手段があれば検出できる.	チップとしての機能が破壊されても, チップそのものやカードの固有パターンを用いてインテグリティを確認できる.
	非破壊攻撃によって秘密情報を読み出す	サイドチャネル攻撃や故障利用攻撃.	所有者とカードの対応が正当であることを認証する機能をもたせる.	演算有アルゴリズムや回路的なサイドチャネル攻撃対策. 故障利用攻撃に対しては攻撃検知センサによる対策.	
	非破壊攻撃によって内部情報を改ざんする	故障利用攻撃. 放射線照射によってビット反転を起こすなど. 改ざんの対象として①秘密情報②ID③管理・制御情報	内部情報が不正に変更されたことがわかるようにする.	②は磁気ストライプとのデータの不一致により検出できる.	
		④テンプレートデータ[3]			④はデータの不一致により検出できる.
	チップを偽造する	偽造したチップを正規の媒体（カード）に入れて利用する.	カードに, あるべきチップが入っていることを検証する機能をもたせる.	チップとカードの対応が正当であることを認証する手段があれば検出できる.	攻撃者がテンプレートデータを複製できなければ検出できる.
カードに対する攻撃3	破壊攻撃によって秘密情報を読み出す（再利用不可）	プロービングや FIB など. オリジナルのチップは破壊され, コピーが不正に利用される.	チップやカードに物理的な改変が加えられたときにその痕跡が残ったり, 利用できないようにする.	カードに残された痕跡を検査する必要がある.	カードの固有パターンが変更されるようにしておけば検出できる. [II]
	破壊攻撃によって秘密情報を読み出す（再利用可）	プロービングや FIB, EB など. オリジナルのチップは元通りに利用できる.			
	破壊攻撃によって内部情報を改ざんする	プロービングや FIB, EB など. 改ざんの対象として①秘密情報②ID③管理・制御情報		②は磁気ストライプとのデータの不一致により検出できる.	
		④テンプレートデータ[3]			
	IC カードを偽造する	偽造したチップを偽造したカードに入れて利用する.	カードやチップが正当に作られたものであることを検証できるようにする.	発行処理やカード, チップの正当性を確かめる手段があれば検出できる.	攻撃者がテンプレートデータを作成することができなければ検出できる.
	無効とされたカードの再利用	攻撃者がカードを不正に更新するなど.	無効化されたカードが確実に破棄される仕組みをもたせる.	無効化手続を確実にする必要がある. 更新依頼人の認証.	固有パターンを破壊することによって確実に無効化できる.

続く

いくつかの攻撃に対して人工物メトリクスが持つ性質（表中の番号 I〜III）により対策がとれるが, 対策となるためには実装のうえでいくつかの条件が必要な点があり, 7 章で具体例を用いて説明する.

7. 人工物メトリクスが対策となるための条件

IC カードシステムに人工物メトリクスを取り入れた場合, 人工物メトリクスが以下の性質を持つことによって安全性が強化できるといえる. 表中の番号（ローマ数字）は攻撃に対する対応策がどの性質に基づくものであるかを示す. ここでは, それぞれの性質がセキュリティ強化に働く条件を述べる.

I. 固有パターンの複製の困難さ

人工物メトリクスの固有パターンは無作為に作られたものであるため, 人間が意図的にパターンを複製することは困難である. よって, パターンの固有性が高

データに対する攻撃	データのすり替え[4]	人工物メトリクスセンサには正規の固有パターンを提示し，偽チップが通信する．	カードとチップの関係を確認する手段をもたせる．		攻撃者がテンプレートデータを作成することができなければ検出できる．
	データの漏洩	R/W とカード間における情報伝達や認証の際の情報漏洩．	耐タンパー性や暗号化機能をもたせる．	秘密情報はチップ内だけに留め，外部に出さない．もしくは暗号化する．	
	データの改ざん	やり取りされるデータを改ざんし，不正なカードを受理させる．	データに改変が加えられたことを検出できるようにする．	左記機能の実現．	固有パターンの複製は困難なため検出できる．[1]
		やり取りされるデータを改ざんし，正規のカードを拒否させる．		左記機能の実現．	
	データの捏造	データを捏造して R/W と通信する．	正規のカードと通信している事を確認できるようにする．	正規のカードと通信していることを確認する必要がある．	固有パターンの複製は困難なため検出できる．[1]
	データ通信の妨害[2]	IC カード本体や R/W をシールドするなどしてデータ通信できないようにする．	カードや機器が正常な状態にあることを検知できるようにする．	左記機能の実現．	
機器に対する攻撃	いかなる入力も受理するように操作する	装置を不正なものに改造したり，故障利用などにより誤動作させたりする．	不正な装置とのアクセスを制御する認証機能や装置が通常の状態に保たれて機能していることを検証する機能をもたせる．	左記機能の実現．	
	正規のカードを利用できなくする	R/W を不正に操作したり誤動作を起こさせたりして正規のカードを拒否するように動作させる．			
	不正な書き込みを行う	攻撃者が意図的に操作するなどして不正に書き込みを行う．			
	IC カードへの電源供給の不安定化	電源供給を不安定にするなどの異常を起こし，認証や書き込みに影響を与える．	安定した電源供給を制御する機能をもたせる．		
	磁気ストライプリーダへの攻撃[1]	リーダに不正な信号を侵入させたり，読み取り機能を無効化させたりする．	センサ出力信号が不正な信号だと判断できるようにする．	チップ内のデータとの不一致により検証できる．	
	人工物メトリクスのセンサへの攻撃	センサを不正に操作したり，読み取り機能を無効化させたりする．			テンプレートデータとの不一致により検出できる．
	R/W を壊す	読み出し，書き込みなどの操作ができないようにする．	R/W の故障検知機能をもたせる．	左記機能の実現．	

[1] 接触型 IC カードシステムに対してのみ考えられる攻撃（表 1 中では方式 1，方式 2）．
[2] 非接触 IC カードシステムに対してのみ考えられる攻撃（表 1 中では方式 3，方式 4）．
[3] 3.3 節のタイプ A,B に対して考えられる攻撃．
[4] 表 1 中の方式 2，方式 3，方式 4 に対して考えられる攻撃．

いほど安全性も高くなるといえる．

また，テンプレートデータが盗まれた場合でも，そのデータからパターンを再現することが困難であることが必要であるが，人工物メトリクスを利用することによって，この条件を満たすことができる．

II. 固有パターンの再生の困難さ

複製が困難であること同様，一度破壊されたパターンを意図的に再生することは困難である．よって，何らかの物理的改変を受けた場合，固有パターンが変更されていることによって攻撃を検出できる．ただし，以下の条件が必要である．

- 攻撃がなされたときに固有パターンが変更される必要がある．
- その変更が正しく検出される必要がある．

上記の条件を満たすためには，攻撃対象になると想定される箇所に人工物メトリクスの固有パターンを埋め込み，そのパターンを認証に用いればよい．

III. 固有パターン破壊の困難さ

人工物メトリクスの固有パターンとする物理的特徴は図 2 や図 4 のようにカード本体が持つ．よって，カードそのものを焼却するなどしない限り，すべての固有パターンを破壊するのは困難であり，固有パターンの一部が破壊されたとしてもカードのインテグリティを保つことができる．ただしこの場合，以下のことが必要であると考えられる．

- 複数のテンプレートデータを保管するなど，扱うデータ量が多くなる．
- システムに求められるセキュリティ要件やコストなどに依存した方式がとられなければならない．

カードの何カ所かの固有パターンを記録しておけば，II と III を両立させることが可能である．

8. ま と め

本稿では，IC チップによる偽造防止技対策と人工物メトリクスによる偽造防止対策を併用することによって，カードのセキュリティが強化できることについて論じた．ディジタル情報を複製することは容易であるが，人工物メトリクスの固有パターンを複製することは困難であり，また，破壊された固有パターンを再生することも困難であることから，IC カードへの人工物メトリクスの適用はセキュリティ強化につながることが分かる．

接触型 IC カードシステムと非接触型 IC カードシステムについて，人工物メトリクスを採用した場合とそうでない場合のシステムのモデル例についてやや具体的に考察した結果，攻撃に対する耐性は，確かに人工物メトリクスを取り入れたシステムのほうが高くできることを示せた．また，人工物メトリクスを用いることで，攻撃されたことを検出できることもセキュリティ上有効であるといえる．

ただし，人工物メトリクスを取り入れることによってカードの認証手続きにかかわる項目が増える分，FRR が高くなることが予想される．また，既存の IC カードシステムと比べると認証手続き時の手間や，運用のコストが高くなることも考えられる．システムに求められるセキュリティ要件などを組み合わせた検討が必要であると考えられる．

本稿では，人工物メトリクスを取り入れたシステムではつねに人工物メトリクス認証をするという設定にしているが，非常時や定期的な検査のときのみ認証する場合についても考察の余地があると考えられる．なお，IC チップと人工物メトリクスを組み合わせたシステム構成には本稿で検討したモデル以外にもさまざまなものが考えられるので，それらのそれぞれにつき，セキュリティ，コスト，運用などを考慮した検討が必要となると考えられる．

参 考 文 献

1) 電子商取引安全技術研究組合：「システム LSI チップのセキュリティ評価」に関する調査研究報告書，経済産業省委託調査 (Mar. 2004).
2) 中島 蕃，柴田 直，山岸篤弘，松本 勉：集積回路のセキュリティ：故障解析技術を用いた攻撃に対する耐性（I)—故障解析技術から見た LSI の耐タンパー性，電子情報通信学会集積回路研究会 (Sep. 2004).
3) 中島 蕃，柴田 直，山岸篤弘，松本 勉：集積回路のセキュリティ：故障解析技術を用いた攻撃に対する耐性（II)—LSI の耐タンパー性向上技術，電子情報通信学会集積回路研究会 (Sep. 2004).
4) 中島 蕃，柴田 直，山岸篤弘，松本 勉：集積回路のセキュリティ：故障解析技術を用いた攻撃に対する耐性（III)—代表的なサイド攻撃とこれに必要なリソースおよびスキル，電子情報通信学会集積回路研究会 (Sep. 2004).
5) Matsumoto, H. and Matsumoto, T.: Artifactmetric Systems, Technical Report of IEICE, ISEC 2000-59, pp.7–14 (Sep. 2000).
6) Matsumoto, H., Takeuchi, I., Hoshino, H., Sugahara, T. and Matsumoto, T.: An artifactmetric system which utilizes inherent texture, IPSJ Journal, Vol.42, No.8, pp.1992–2005 (Aug. 2001).
7) Matsumoto, H. and Matsumoto, T.: An Evaluation Method for a Magnetic Artifact-metric System, IPSJ Journal, Vol.43, No.8, pp.2458–

2466 (Aug. 2002).
8) Matsumoto, H. and Matsumoto, T.: Clone Match Rate Evaluation for an Artifact-metric System, IPSJ Journal, Vol.44, No.8, pp.1–11 (Aug. 2003).
9) 青柳真紀子，竹村泰司，松本　勉：磁性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，電子情報通信学会 2004 年暗号と情報セキュリティシンポジウム予稿集，pp.573–578 (Jan. 2004).
10) 松本　勉，岩下直行：金融業務と人工物メトリクス，金融研究，Vol.23, No.2, pp.169–186 (2004). http://www.imes.boj.or.jp/japanese/kinyu/2004/yoyaku/kk23-2-7.html
11) 日本銀行金融研究所：第 6 回情報セキュリティシンポジウム「金融分野における人工物メトリクス」の模様，金融研究，Vol.23, No.2, pp.153–168 (2004). http://www.imes.boj.or.jp/japanese/kinyu/2004/yoyaku/kk23-2-6.html
12) 松本　勉，青柳真紀子：人工物メトリクスによる IC カードのセキュリティ強化の可能性，情報処理学会 2004 年コンピュータセキュリティシンポジウム予稿集，pp.259–264 (Oct. 2004).

(平成 16 年 11 月 29 日受付)
(平成 17 年 6 月 9 日採録)

松本　勉（正会員）

1986 年東京大学大学院博士課程修了．工学博士．同年横浜国立大学工学部専任講師．同助教授，教授を経て，2001 年より同大学大学院環境情報研究院教授．これまで，カールスルーエ大学（ドイツ）客員教授，ケンブリッジ大学（イギリス）ニュートン数理科学研究所研究員，日本銀行金融研究所客員研究員等を兼務した．1981 年より暗号や情報セキュリティの研究に従事．「明るい暗号研究会」創設メンバー．現在，情報セキュリティ，暗号アルゴリズム，認証プロトコル，ディジタル証拠性，情報ハイディング，バイオメトリクス，人工物メトリクス，耐タンパーハードウェア，耐タンパーソフトウェア等に広く関心をもつ．国際暗号学会 IACR 理事．暗号技術検討会構成員．CRYPTREC 暗号モジュール委員会委員長．CRYPTREC 署名・認証技術調査ワーキンググループ主査．INSTAC 耐タンパー性標準化調査研究委員会委員長．金融庁偽造キャッシュカード問題に係るスタディグループ委員等．電子情報通信学会より「情報セキュリティの基礎理論」への貢献に関して業績賞を受賞．

青柳真紀子

2003 年横浜国立大学工学部電子情報工学科卒業．2005 年同大大学院環境情報研究院博士課程前期修了．在学中，人工物メトリクス等，セキュリティ技術の研究を行う．同年日本電信電話（株）入社．現在，情報流通プラットフォーム研究所所属．電子情報通信学会会員．情報処理学会 2004 年コンピュータセキュリティシンポジウム CSS2004 学生優秀論文賞受賞．