光過程のランダムネスと人工物メトリクス

松　本　　勉

Randomness in Optical Process and Artifact-Metrics

Tsutomu MATSUMOTO

“Artifact-metrics,” which utilizes physical features unique to individual artifact objects, is a security technology that aims to achieve cloning resistance (difficulty of copying) by utilizing the fact that a physical feature can be measured more precisely than it can be formed. This article reviews examples of optical artifact-metrics in the form of media such as paper. In view of the recent advances in micro-fabrication technologies, it is valid to seriously consider artifact-metrics at the nanometer scale as an important issue. This article also reviews recent research achievements regarding the “nano-artifact-metrics.”

Key words: information and physical security, artifact-metrics, cloning resistance, electron beam lithography, resist collapsing

紙に光を当てたときに得られる反射光や透過光のパターンを測定して一つひとつの紙を見分けたり，個々の紙の情報を引き出したりして利用するセキュリティー技術がある．測定される光のパターンが，紙漉きの段階で形成される紙の繊維のランダムな三次元的な構造に依存するため，特定の個体に対する光のパターンを再現する別の個体を偽造することはきわめて困難とみられることが，この技術の根拠である．このような，人工物（典型的には工業的に生産された物体）の個体に固有の物理的特徴を活用する技術を，人工物メトリクス（artifact-metrics）という．

1.　人工物メトリクス

1. 1　人工物メトリクスの定義と要件

人工物メトリクス（artifact-metrics）は人工物（artifact）と測定（metrics）が結合した用語であり，一言でいえば，人工物の個体に固有の物理的特徴（人工物メトリクス要素）を活用する技術を意味する．ここで人工物メトリクス要素とは，対象とする物体の電磁気的特性や機械振動特性などのさまざまな物理的特性のいずれか一つまたは組み合わせによる物理的特徴であり，それを測定した値（情報）は，厳密には対象の物体と測定システム（人工物メトリック・システム）との組により定められる（図1）．

同じ原料で同じ工業プロセスにより製造された物体であっても，細かく調べれば，避けられないランダムネスにより生みだされた個体差がある（図2）．その個体差を安定して測定できる方法が存在することと，長期間にわたって個体差が安定していることとを前提として，物理的特徴の測定がその形成に比べて相対的に高精度で行えるという測定と形成の精度の非対称性に基づく耐クローン性（コピー困難性）が成立する範囲で，活用することを狙っている．

整理すると，人工物メトリクスには，(1) 個体により値が異なること（個別性），個別性の指標として誤一致率（false match rate）がある，(2) 個体から安定して値が測定できること（読み取り安定性），読み取り安定性の指標として誤不一致率（false non-match rate）がある，(3) 個体の利用により変化・劣化した人工物メトリクス要素から，安定して登録時と同等の値を測定できること（耐久性），(4) どの個体に対しても，その個体と同等の値が測定される別の物体（クローン）を作製することがきわめて困難であること（耐クローン性），が求められる．人工物メトリクスのサーベイとしては，文献 1), 2), 3) などがある．

1. 2　個体認証と値抽出

これまで人工物メトリクスは，

(A) 人工物の個体認証： 対象とする個体の人工物メト

横浜国立大学大学院環境情報研究院（〒240–8501 横浜市保土ヶ谷区常盤台 79–7）　E-mail: tsutomu@ynu.ac.jp

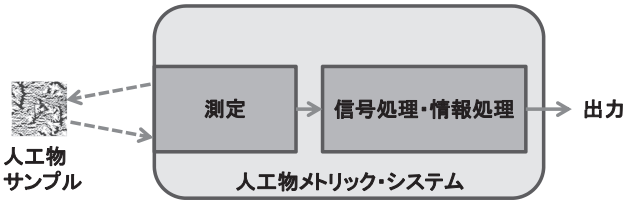

図1　人工物メトリクス.

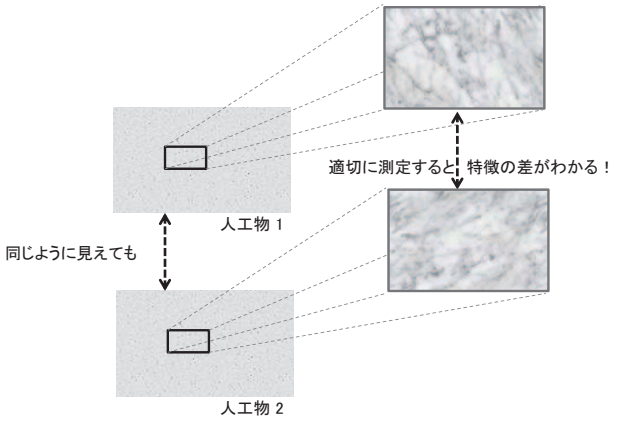

図2　工業製品にも個体差がある.

リクス要素を一度測定して得た値と，再度測定して得た値との間の相関係数などを指標とする「類似度」を計算し，類似度が閾値を超えれば同一の個体であり，そうでなければ異なる個体であるという判断を行う

を目的としたものが圧倒的に多かったが，

（B）人工物の個体からの固有な値の抽出：その物体がないと値が得られないという利用を目的として，対象とする物体と，それに対応する補助データとから，情報通信や記録の分野で開拓されたディジタル誤り訂正符号の技術を併用して，その物体に固有の値を再現性よく抽出する

という新たな文脈においても研究開発が進められている（図3）.

前者の実用化例として，ソフト磁性体の粉末をアクリル製のチューブに詰め込んだ微小磁性ファイバーを紙パルプと一緒に漉いて製紙した紙を磁界センサーで測定する方式は，耐久性に優れ，日本の株券の偽造検知技術として大規模に利用された.

また，後者の実用例としては，人工物の特徴を関数として捉えたPUF（physical unclonable function）とよばれるものがある[4,5]．これは，1997年頃に筆者らが「耐クローン（性）モジュール」[6]という名称で考察したものと本質的に等価である．PUFは，現在，ICチップなどの電子回路におけるゲート遅延のばらつきや，スタティックRAMの電源投入時のメモリー内容などを固有パターンとする実

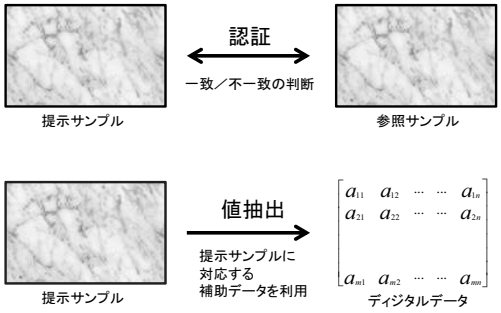

図3　認証と値抽出.

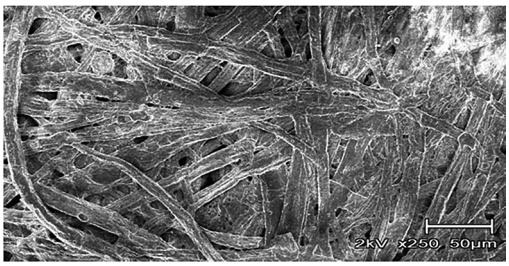

図4　普通紙の走査電子顕微鏡画像.

装例が実用化されている.

2.　光学的な人工物メトリクス

冒頭で挙げた，紙に光を当てたときに得られる反射光や透過光のパターンを用いて一つひとつの紙を個体として認証する，という方式群がある．これらの方式は，紙の特徴が紙の繊維の三次元構造（図4）によって決定されるためにその再現が困難とみられるほか，認証の対象となる紙に特別な処理を施す必要がないという利点もある.

紙の赤外透過光画像を利用する方式[7]は，理論値としては誤一致率と誤不一致率を同時に10^{-20}程度にできることがわかっている．また，紙の可視反射光画像を利用する方式[8]や，スペックルパターン（レーザー光を当てた際に紙の表面の各点で散乱した光が干渉して生じる複雑なパターン）を利用する方式[9]も提案されており，実験による認証精度の測定結果が学会で発表されている．文献10）は紙の可視光反射型人工物メトリクスに対する複合機（MFP）を利用したクローン攻撃の最新の検討事例である.

3.　ナノ人工物メトリクスに向けて

3.1　マイクロメートルスケールからの脱却

上記で具体的に紹介した事例は，マイクロメートルスケールのパターンの測定と偽造の攻防に関わるものであった．微細加工技術の近年の進歩を踏まえると，ナノメートルスケールにおける人工物メトリクス（ナノ人工物メトリクス）を本格的に検討することが重要となる.

3.2　レジスト倒壊を利用したナノ人工物メトリクス

人工物メトリクス要素として，シリコン基板上にランダ

ムに形成されたナノメートルオーダーの凹凸パターンを考える．集積回路開発製造に用いられる微細加工に関するコア技術として，電子線リソグラフィーがある．その手順は，まず，シリコン基板上に電子線レジストを塗布し，所望のパターンに沿った電子線露光によりレジストの特性を変化させ，現像処理によりレジストに覆われている部分とそうでない部分を生じさせる．そしてエッチングにより基板上に凹凸パターンを形成し，不要なレジストを除去する．

レジストの厚さや電子線露光時間やパターンの細かさによっては，レジスト倒壊が起こり，形成されるパターンが崩れる．このため，レジスト倒壊が生じないように諸条件を工夫して設計図通りのパターンを形成する技術が確立されている．レジストのピラー（柱）を並べたパターン（ピラーアレイ）を考えたとき，ピラーの配置の密度（ピッチ）をどれくらい小さくできるかが関心事項となる．この最小ピッチは 2015 年で 30 nm，2010 年で 20 nm といったトレンドにある．これは，クローン攻撃を行う攻撃者が狙い通りに作製できる微細パターンのサイズに相当する．

これに対し，微細パターンの測定（撮影）では，長さ測定に特化した測長走査電子顕微鏡（CD-SEM）を用いればナノメートルオーダーの精度での測定が可能であり，精度はさらにサブナノメートルにも及ぶ動向にある[11]．

したがって，攻撃者には狙って形成できないほど微細な凹凸パターンを有するシリコン基板を作ることができるかがおもな関心事項となる．そこで筆者らは，レジストのピラーアレイ（等間隔に並ぶピラーの配列）がランダムに倒壊するように条件を設定し，ナノメートルスケールのランダムな凹凸構造をシリコン基板上に形成することとした．ピラーの底面 $w \times w$ は $w = 60$ nm とし，ピッチ $p = 120$ nm とした．ピラーアレイ領域は 2 μm 角と設定した．レジスト倒壊が起き，形成されたパターンの例を図 5 に示す．10 nm より細かい構造が出現していることが確認できる[12]．パターンの照合の類似度として相関係数をベースとする関数を利用した簡易な人工物メトリックシステムを構成したところ，誤不一致率および不一致率の点で驚くべき高い精度が達成されることが明らかとなってきた[13]．

3. 3　偽造防止技術のパラダイムチェンジ

偽造者に対する製造者の技術的優位性を根拠とし，したがって詳細がオープンな議論にさらされることの少ない既存の多くの偽造防止技術には，以下の問題点がある．

(1) その偽造防止技術が担うセキュリティーがどの程度脅威にさらされているか，製造者側で検証できない．

(2) 攻撃技術進歩や機密情報の漏洩により，製造者側が技術的優位性を喪失し，セキュリティーが損なわれる可能性がある．

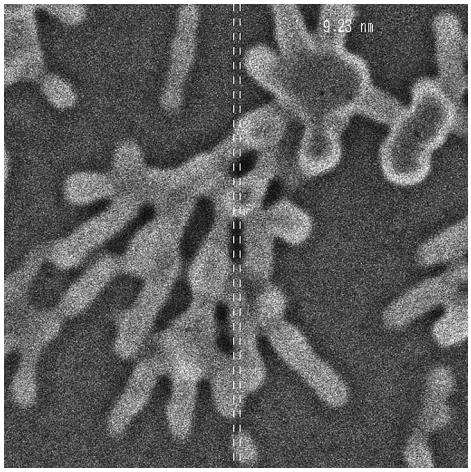

図 5　電子線レジスト倒壊に基づくシリコン基板の凹凸（走査電子顕微鏡画像，点線間の距離は 9.23 nm）．

しかし，本稿で例示したように，人工物メトリクスでは，人為的に制御が困難であるランダムな固有パターンを利用可能であり，製造方法や検証方法を秘匿しなくても耐クローン性を維持可能であることが期待されることから，人工物の製造技術をアカデミックでオープンな研究対象とすることができ，それにより客観的な評価がなされ，攻撃技術の進歩によるセキュリティー低下への適切な対応がとれる．このように，人工物メトリクスは偽造防止技術におけるパラダイムチェンジに貢献し得るといえよう．

文　　献

1) 松本弘之，ほか：金融研究，**23**，別冊 1 号 (2004) 61–140.
2) 宇根正志，ほか：金融研究，**28** (2009) 143–182.
3) 松本　勉：応用物理，**80** (2011) 30–35.
4) R. Pappu: *Physical One-Way Functions* (PhD Thesis, MIT, 2001).
5) P. Tuyls, B. Škorić and T. Kevenaar: *Security with Noisy Data* (Springer, 2007).
6) 松本　勉，ほか：暗号と情報セキュリティシンポジウム (SCIS 97) 講演論文集，19C (電子情報通信学会，1997).
7) 山越　学，ほか：コンピュータセキュリティ研究会 2007-48 (情報処理学会，2007) pp. 13–18.
8) 伊藤健介，ほか：富士ゼロックステクニカルレポート，No. 15 (2005) 32–41.
9) J. D. R. Buchanan, *et al.*: Nature, **436** (2005) 475.
10) 花木健太，ほか：暗号と情報セキュリティシンポジウム (SCIS 2013) 講演論文集，2D2-4 (電子情報通信学会，2013).
11) 日本顕微鏡学会関東支部編：新・走査電子顕微鏡 (共立出版，2011).
12) 松本　勉，ほか：電子情報通信学会技術研究報告，**IEICE-112** (2013) 217–222.
13) 松本　勉，ほか：暗号と情報セキュリティシンポジウム (SCIS 2014) 講演論文集，2E2-3 (電子情報通信学会，2014).

(2014 年 1 月 9 日受理)