IMES DISCUSSION PAPER SERIES

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方法の構築に向けて

田村裕子（たむらゆうこ）・宇根正志（うねまさし）

Discussion Paper No. 2009-J-3

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-3
2009 年 3 月

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手法の構築に向けて

田村裕子（たむらゆうこ）*・宇根正志（うねまさし）**

要　旨

人工物メトリクスは、各人工物に固有の特徴を利用して当該人工物の認証を行う技術である。金融分野においては、金融取引に用いられる紙やカード等の人工物の真正性を根拠として取引を行うケースが多く、人工物メトリクスを偽造防止技術の 1 つとして活用することが考えられる。そうした際には、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）を適切に選択することが重要となるが、偽造防止技術として活用するという性格上、人工物の偽造に対して十分な耐性を有しているか否かを確認することが求められる。人工物の偽造の難しさ（耐クローン性）を評価する方法については、現在研究が進められている最中である。

本稿では、既存の評価事例を参考に、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方法のアイデアを示す。具体的には、攻撃に用いられる人工物の偽造方法をリストアップしたうえで、最も効率的とみられるものが用いられたときの偽造にかかる資金や時間を試算し、その結果を耐クローン性の評価尺度の 1 つとするというものである。本稿では、こうした評価方法について説明したうえで、既存の人工物メトリック・システムに関する耐クローン性の評価事例を本評価方法に適用して評価の具体例を示すとともに、本評価方法を精緻化するうえでの今後の課題を説明する。

キーワード：偽造防止技術、人工物メトリクス、人工物メトリック・システム、セキュリティ評価、耐クローン性

JEL classification: L86、L96、Z00

*　日本銀行金融研究所（E-mail: yuuko.tamura@boj.or.jp）

**　日本銀行金融研究所企画役

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。本稿の作成に当たっては、横浜国立大学大学院の松本 勉教授、独立行政法人国立印刷局研究所の山越 学副主任研究員、木村健一副主任研究員、田中純一副主任研究員、古家 眞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

金融分野における取引では、紙やカード等の人工物が利用されることが多く、当該人工物が真正であること（偽造されたものでないこと）を根拠として取引を行うケースが多い（松本・岩下［2004］）。例えば、銀行窓口での個人による預金引出しにおいては、預金通帳と印鑑が預金者本人に対応する真正なものであることが確認されるほか、ATM での預金引出しにおいてもキャッシュカードの真正性確認が行われる。人工物を偽造しにくくする、および、偽造されたものでないことを確認可能にするため、こうした人工物には偽造防止技術が利用されている。一般に、広く利用されている偽造防止技術には、製造方法や材料等に関する情報の非対称性を拠り所とするものが多いといわれているが（松本・岩下［2004］）、こうした偽造防止技術の効果を第三者が評価することは難しい。

人工物に固有の特徴を利用して当該人工物の認証を行う技術である「人工物メトリクス」（松本ほか［2004］）は、人工物の製造方法や材料等に関する情報を公開した場合においても偽造が難しいことを目指した技術であり、オープンな場において第三者による評価を受けることができるという利点がある。人工物の製造過程において意図的に制御することが困難な特徴を利用する場合には、少なくとも製造者と同程度の能力を有する攻撃者に対して安全性を確保することが期待される。

これまでに人工物メトリック・システムとしてさまざまな方法が提案されている。例えば、プラスチック・カード等に埋め込まれた磁性ファイバーの分布を人工物の特徴として利用するシステム（Matsumoto *et al.*［2001］）や紙等の基材表面の微小の凹凸を特徴として利用するシステム（Buchanan *et al.*［2005］）等が挙げられる。また、物理的特徴からユニークな秘密鍵を動的に生成し、当該秘密鍵を用いた認証プロトコルによって当該人工物の認証を行う PUF（physical unclonable function）と呼ばれる方式が複数提案されているが、これらも人工物メトリクスの範疇に入る。PUF のなかでも IC 内部の複数のパス遅延の比較結果を利用する方式（アービター PUF と呼ばれる、Devadas *et al.*［2008］）を搭載した RFID チップが 2008 年 9 月から発売されている（Verayo［2008］）ほか、IC のメモリの各セルにおける電力起動時の電荷分布を利用する方式（イントリンシック PUF と呼ばれる、Guajardo *et al.*［2007］）を搭載した FPGA による偽造防止技術が 2008 年 10 月に製品化されている（Philips［2008］）。

既存の提案方式のいくつかには、一定の攻撃を想定したうえで、人工物の偽造の難しさ（耐クローン性）の評価が行われている。例えば、前述の磁性ファイバーの分布を利用した方式に対しては、適当に準備した人工物や偽造対象の人工物を見本にして複製した人工物を誤って受理させる攻撃を想定し、それらの攻撃の成功確率を

実験によって計測するという研究が報告されている（Matsumoto and Matsumoto［2003］）。また、ランダムな刺激を人工物に付与し、人工物から得られる信号を用いて認証を行ういくつかの方式について、その信号を推定するために必要な情報量や計算量の試算を行う研究も知られている（例えば、Pappu［2001］や DeJean and Kirovski［2007］）。そのほか、人工物を偽造するという攻撃に対して、人工物メトリック・システム一般に求められるセキュリティ要件を導出するとともに、そうした要件の充足度合いによって当該システムを評価するというアイデアの提案も行われている（松本ほか［2004］）。

ただし、こうした既存の評価事例にはいくつかの課題が残されている。例えば、(1) 既存の評価事例では攻撃を構成する一部の行為にのみ着目するケースが多く、攻撃全体を包含する評価になっているとは言い難い、(2) 各評価事例における評価の尺度（計算量、情報量、確率）が統一されておらず、評価結果を比較することが困難である、(3) 評価の前提として攻撃者が利用する資源（計算能力、情報量、人工物製造能力等）が明示的に考慮されているとは言い難いといった指摘がなされている（田村・宇根［2007］）。既存の評価事例を活用しながら望ましい評価方法構築に向けた検討も進められているものの（田村・宇根［2007］）、耐クローン性の具体的な評価方法の確立には至っていないのが実情である。

そこで、本稿では、人工物メトリック・システムの耐クローン性に焦点を当てて、既存の評価事例を参考に耐クローン性の評価方法の構築に向けた検討を行う。具体的には、攻撃者や攻撃方法を分類したうえで、それらの攻撃の成功がどのようなパラメータに依存するかを検討し、そうしたパラメータを用いた評価方法の考え方を示す。さらに、既存研究における評価事例を本評価方法に適用すると、耐クローン性の評価においてどのような解釈が可能かを説明したうえで、本評価方法を精緻化していく際の検討課題を示す。

本稿の構成は以下のとおりである。まず、2 節では、本稿で検討の対象とする人工物メトリック・システムの構成について説明し、3 節において、クローンを利用した攻撃と耐クローン性について説明する。4 節では、クローンを利用した攻撃を構成する行為を整理するとともに、そうした整理に基づいた耐クローン性の評価方法のアイデアを示す。さらに、5 節では既存の人工物メトリック・システムに関する耐クローン性の評価事例を本アイデアに適用する。6 節では、本評価方法を精緻化するうえでの今後の課題を示し、7 節で本稿を締め括る。

2．検討対象とする人工物メトリック・システムの構成

(1) エンティティ

人工物メトリック・システムの構成は、認証の形態に応じてさまざまなバリエーションがある（松本ほか［2004］）。本稿では、理解しやすさの観点から、なるべくシンプルなシステムを想定し、以下のとおり、トークン、発行者、検証装置、ユーザの 4 種類のエンティティで構成されるものとする（図 1 参照）。

- トークン：本システムにおける認証の対象として正規の手続で製造された人工物であり、それぞれ固有の特徴を有するもの。
- 発行者：トークンを製造・発行する機関。
- 検証装置：トークンの登録や 1 対 1 認証を実行する装置。トークンの情報の取得から認証結果の出力までを実行する。
- ユーザ：トークンを保有し、トークンに対応付けされたサービスを実行する際にトークンを検証装置に提示する個人。

(2) 人工物メトリック・システムの基本的構成

本システムにおけるトークンの登録時には、検証装置は登録対象のトークンからその特徴を測定し、測定結果から生成したデータを参照データとして保管する。認証時には、トークンから同様の手続で生成したデータと参照データとの整合性を確認する。トークンの特徴を測定する際には、検証装置は、まず、トークンに何らかの刺激を与え、それに対するトークンからの反応をセンサーで信号に置き換える。トークンへの刺激の付与は「チャレンジ」、チャレンジに対して得られた信号は「レスポンス」と呼ばれる（Pappu［2001］など）[1]。

[1]チャレンジ、レスポンスという呼び方は、暗号技術を利用したユーザ認証方式で用いられている（Menezes,van Oorschot, and Vanstone［2001］）。こうした方式では、認証の都度、認証者が新たに生成した乱数を「チャレンジ」として被認証者に送り、被認証者は送られたチャレンジと秘密鍵を用いて演算した結果を「レスポンス」として認証者に送る。その際、認証者は、レスポンスがチャレンジに対して生成されたものであることの確認によって認証を行う。本方式は、認証者と被認証者間で送信されるデータが盗聴された場合においても、なりすましを防止することを目的としており、一般に、チャレンジ・レスポンス方式と呼ばれる。人工物メトリック・システムにおいても、トークンへの働きかけをランダムに変更するチャレンジ・レスポンス方式でトークンの認証を行う方式が複数提案されている。

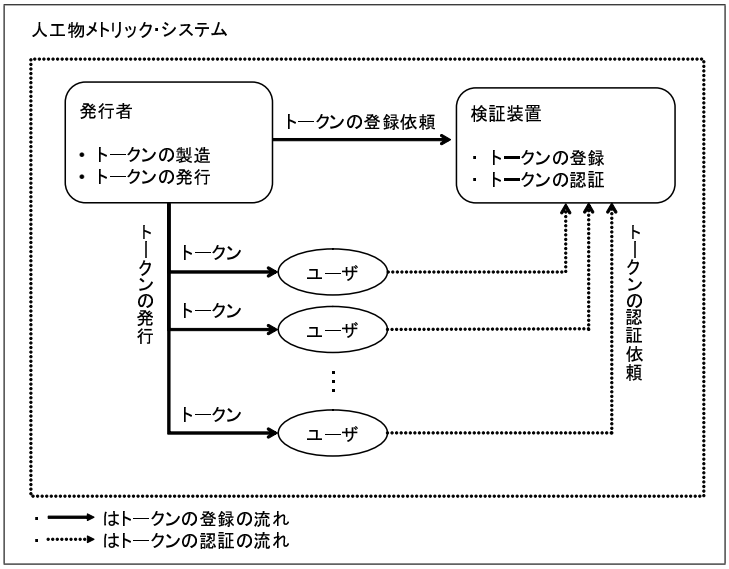

図 1: 人工物メトリック・システムを構成するエンティティ（概念図）

イ．記号の定義

本稿において利用する記号の定義は以下のとおりである。

- c_i：検証装置から与えられるチャレンジであり、その取り得る集合を C とする。チャレンジには、トークンの特徴を測定するために検証装置から与えられる刺激であるプローブ p_i が含まれる。そのほか、センサーが複数存在する場合には利用するセンサーを認証の都度変更するケースが考えられる。また、トークン全体ではなく、トークンの物理構造の一部分の反応を認証に利用するケースでは、認証の都度プローブを当てる範囲を変更することも考えられる。以下では、プローブに反応するトークンの物理構造の範囲を読取範囲と呼ぶ（図 2 参照）。この場合、チャレンジは、どのようなプローブを利用するか、どのセンサーを利用するか、プローブをトークンのどの位置に当てるかといった情報で構成されることとなる。
- f_t：トークン t のチャレンジに対するレスポンスを返す関数である。認証環境 α におけるチャレンジ c_i に対するレスポンスを $r_{t(i,\alpha)} = f_t(c_i, \alpha)$ と表す。認証環境 α はセンサーでの読取誤差を発生させる要因を表すパラメータである。α は、認証時に検証装置の動作を管理するシステム運用者側で制御困難な要因（認証時のトークンの位置ずれや光源のゆらぎ等）に依存して決まる値であるとする。トークン t のチャレンジ c_i に対するレスポンスは、取り得る認証環境の集合を $\mathcal{A}$ としたとき、$\{r_{t(i,\alpha)} \mid \alpha \in \mathcal{A}\}$ の要素となる。

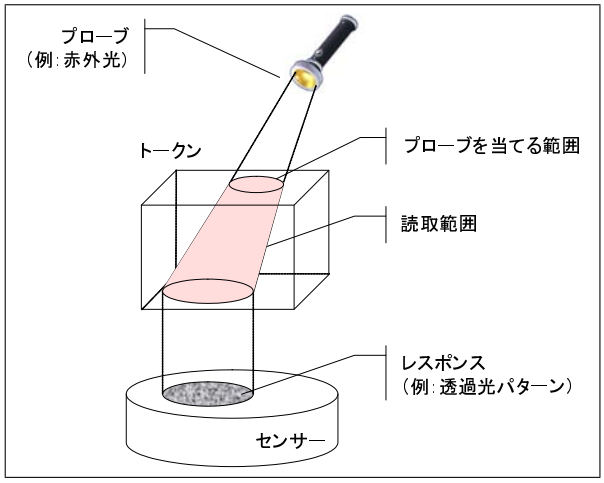

図 2: トークンの読取範囲の例（概念図）

- g：レスポンスを入力として、参照データとの照合を行うためのデータ（固有パターンと呼ぶ）を出力する関数である。レスポンス $r_{t(i,\alpha)}$ から得られる固有パターンを $u_{t(i,\alpha)} = g(r_{t(i,\alpha)})$ と表す。

- h：ある固有パターンと参照データの類似度を出力する関数である。トークン t のチャレンジ c_i に対する固有パターン $u_{t(i,\alpha)}$ と参照データ $ref_{(t,i)}$ との類似度を $s = h(u_{t(i,\alpha)}, ref_{(t,i)}) \in [0,1]$ と表す。なお、参照データ $ref_{(t,i)}$ は、トークン t の識別子 ID_t、チャレンジの識別子 i、登録時のチャレンジ c_i における固有パターンで構成されるものとする。

人工物メトリック・システムにおいては、認証環境によってチャレンジに対するレスポンスにぶれが生じることから、「t 以外のトークンが t である」と誤って判定される確率（誤合致率）と「t が t でない」と誤って判定される確率（誤非合致率）を考慮して判定しきい値が設定される。認証時には、得られた固有パターンとトークン t の参照データとの類似度がシステムで設定された判定しきい値以上であれば、提示されたトークンを t であると判定できるよう関数 g, h が構成されることとなる。

以下では、判定しきい値 $\sigma \in [0,1]$ 以上の類似度の集合を $S_\sigma (= \{j \mid \sigma \leq j \leq 1\})$、参照データ $ref_{(t,i)}$ との類似度が S_σ に含まれる固有パターンを生成するトークン t のレスポンスの集合を $R_{(t,c_i)}$ とおく[2]（図 3 参照）。つまり、$R_{(t,c_i)}$ は、チャレンジ c_i に対するトークン t のレスポンスからなる集合のうち、トークン t であると正しく判定されるレスポンスの部分集合を表す。

[2] $R_{(t,c_i)}$ は $\{r_{t(i,\alpha)} \mid r_{t(i,\alpha)} = f_t(c_i, \alpha), h(g(r_{t(i,\alpha)}), ref_{(t,i)}) \in S_\sigma, \alpha \in \mathcal{A}\}$ と表される。

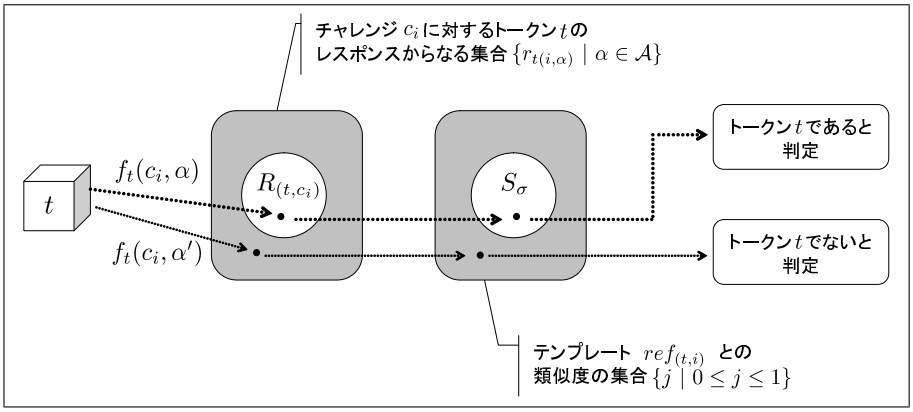

図 3: トークン t として認証されるレスポンスや類似度の集合（概念図）

ロ．トークンの登録と認証

トークンの登録・認証の処理は以下のとおりである。

（イ）トークンの登録の手順

1. 発行者はトークン t とその識別子 ID_t を検証装置に提示する（図 4 参照）。
2. 発行者はトークン t の認証に利用する ℓ (≥ 1) 個のチャレンジを決定し、その集合を $C_{(t,\ell)} \subseteq \mathcal{C}$ とする。以下、3〜5 の手続を $C_{(t,\ell)}$ に含まれるすべてのチャレンジについて実行する。その際の認証環境は $\bar{\alpha}$ とする。
3. 検証装置は、チャレンジ $c_i \in C_{(t,\ell)}$ を選択し、t に与える（ただし、$i = 1, 2, \ldots, \ell$）。
4. 検証装置は、c_i に対する t のレスポンス $r_{t(i,\bar{\alpha})} = f_t(c_i, \bar{\alpha})$ を検出し、固有パターン $u_{t(i,\bar{\alpha})} = g(r_{t(i,\bar{\alpha})})$ を得る。
5. 検証装置はデータベースに参照データ $ref_{(t,i)} = (ID_t, i, u_{t(i,\bar{\alpha})})$ を登録する。
6. 発行者はユーザに当該トークンと ID_t を発行する。

（ロ）トークンの認証の手順

1. ユーザは、トークン $\tilde{t}$ と識別子 ID_t を検証装置に提示する（図 4 参照）。
2. 検証装置は、ID_t に対応する $C_{(t,\ell)}$ を読み出し、あるチャレンジ $c_{\tilde{i}} \in C_{(t,\ell)}$ を一定のルールに従って選択し、$\tilde{t}$ に与える。チャレンジを選択するルールはシステムによって異なる。
3. 検証装置は、認証環境 $\tilde{\alpha}$ のもとで $\tilde{t}$ からのレスポンス $r_{\tilde{t}(\tilde{i},\tilde{\alpha})} = f_{\tilde{t}}(c_{\tilde{i}}, \tilde{\alpha})$ を検出し、$\tilde{t}$ の固有パターン $u_{\tilde{t}(\tilde{i},\tilde{\alpha})} = g(r_{\tilde{t}(\tilde{i},\tilde{\alpha})})$ を求める。

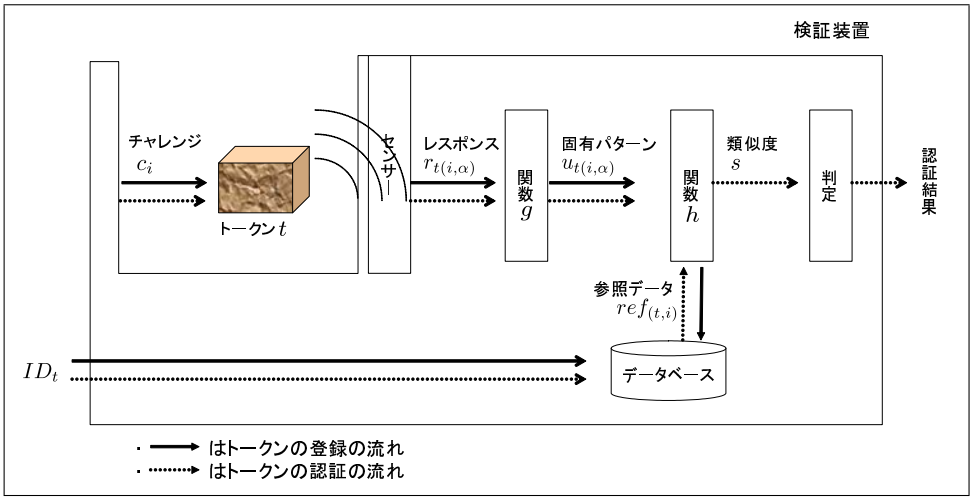

図 4: トークンの登録と認証の流れ（概念図）

4. 検証装置は、トークン t のデータベースに登録されている ℓ 個の参照データのうち、$c_{\tilde{i}}$ に対応する $ref_{(t,\tilde{i})} = (ID_t, \tilde{i}, u_{t(\tilde{i},\tilde{\alpha})})$ に対して $s = h(u_{\tilde{t}(\tilde{i},\tilde{\alpha})}, ref_{(t,\tilde{i})})$ を求め、システム・パラメータとして設定された判定しきい値 σ に対して、$s \in S_\sigma$ であれば $\tilde{t}$ が ID_t に対応するトークン t であると認証する。そうでなければトークン t でないと判定し、その結果をユーザに返す。

3．想定する攻撃と耐クローン性

(1) 想定する攻撃者

想定する攻撃者は、人工物メトリック・システムを利用するアプリケーションに応じて異なる。ただし、高度なセキュリティを達成するように設計された人工物メトリック・システムは、発行者でさえも制御困難な特徴を利用し、少なくとも発行者と同程度の能力を有する攻撃者に対して安全性を確保することが期待される（Matsumoto and Matsumoto［2003］）。本稿では、そうした人工物メトリック・システムを前提として、以下の攻撃者を想定する。

- トークンの製造について、少なくとも発行者と同じ知識・技術・設備・資金（以下、これらをまとめて資源と呼ぶ）を有するほか、トークンの製造に必要な材料を有する。そのため、少なくとも発行者と同じ方法でトークンを製造することが可能である。
- 検証装置について、少なくとも当該装置の製造者と同じ資源を有するほか、検証装置の製造に必要な材料を有する。そのため、正規手続で製造された検証装置と同じ機能を実現する装置を自作可能であり、自作した検証装置についてはチャレンジを攻撃者自身で制御することができる。
- 攻撃対象のトークンを入手可能であり、当該トークンを利用できる時間が制限されない。
- 正規手続で製造された検証装置（実運用に供されているものも含む）を盗取するなどの方法によって入手可能であり、当該装置を利用できる時間が制限されない。ただし、これらの検証装置の内部構造を不正に改変することは困難であるほか、同検証装置に格納されている情報の不正な読出しや改ざんも困難である。
  - 実運用のシステムで利用されている検証装置のうち、トークン t が登録された検証装置には、トークン t の認証に利用するチャレンジの集合 $C_{(t,\ell)}$、および、ℓ 個の参照データ $\{ref_{(t,i)}\}_{(1\leq i\leq \ell)}$ が格納されているが、上記攻撃者はそれらの情報を読み出すことや改ざんすることはできないこととする。ただし、トークン t と検証装置間のチャレンジ・レスポンスを観測することによって $C_{(t,\ell)}$ あるいはその部分集合を得ることができるとする。
- 発行者やシステム運用者の不正は運用によって防止され、トークンの発行者やシステム運用者と結託することができない。

(2) クローンとそれを利用した攻撃

イ．人工物メトリック・システムへの攻撃

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は、システムのライフ・サイクル全体をカバーした検討が必要である。人工物メトリック・システムにおけるライフ・サイクルは、トークンの設計・製造、発行、使用、廃棄のフェーズに分けることができる。これらのうち、以下では、既存の評価研究において主たる対象とされているトークンの使用フェーズの攻撃に焦点を当て、使用以外のフェーズでは運用によって各種の不正を防止できると仮定することとする。

既存の評価研究の 1 つである松本ほか［2004］では、攻撃者がトークンの発行者やシステム運用者と結託するか否か、検証装置の内部構造に関する情報を有するか否かによって攻撃の条件を 5 つに分類したうえで、各条件のもとで想定される攻撃を挙げている。これらのうち、本稿における攻撃者に関する想定に当てはまる攻撃は以下の 2 つである。

- 検証装置に提示する人工物を適当に用意するとともに、発行済みトークンを用いて当該人工物が誤って受け入れられるような ID を探索する。
- 正規の発行済みトークンから得られる情報を利用して、当該トークンを偽造する。

上記攻撃のうち、前者には、ランダムに入手・製造したクローンを提示する「ブルート・フォース攻撃」が含まれる。

これらの攻撃は、いずれも、正規の発行済みトークンから得られる情報等を利用してトークンを偽造するというタイプの攻撃である。検証装置に ID_t とともに提示される人工物であり、正規の手続で発行されたトークン t 以外のものを「クローン」と呼び、クローンを利用した攻撃を次のように定義する。

> **定義 1** 攻撃者が、攻撃対象であるトークンのクローンを正常な検証手続のもとで誤って受理させるための試みを「クローンを利用した攻撃」と呼ぶ。

ロ．5 種類の攻撃

クローンは、あるレスポンスを再現する人工物として入手・製造されるものであるが、トークン t の物理構造の再現を目的とするものとそうでないものが考えられる。また、正規の発行済みトークンから得られる情報は、トークン t のチャレンジ・レスポンスのペア（以下、CRP ＜ challenge-response pairs ＞と呼ぶ）と、

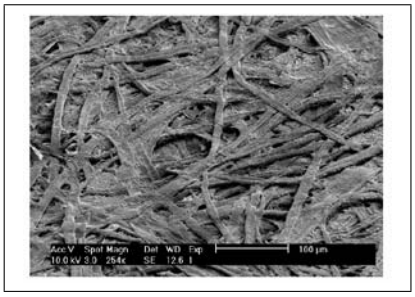

図 5: 紙の表面構造の顕微鏡画像（Cowburn［2008］）

CRP 以外の t に関する情報（以下、観測データと呼ぶ）に大別できる。観測データとしては、例えば、トークンの物理構造を顕微鏡や非接触 3 次元形状スキャナーで観測して得た画像データ等が挙げられる（図 5 参照）。このように、攻撃者が利用する情報の観点からは、クローンは、（A）CRP と観測データをともに利用するもの、（B）CRP のみを利用するもの、（C）観測データのみを利用するもの、（D）両者とも利用しないものの 4 つに分類される。その結果、クローンには 8 のバリエーションがあることがわかる（図 6 参照）。

主な研究事例に登場するクローンを利用した攻撃を整理すると以下の 5 つが挙げられる[3]が、いずれも図 6 に示されているクローンを利用するものとなっている。

- **ハード・コピー攻撃：** トークン t の CRP や観測データからトークン t の特徴を推定し、その特徴を再現するようにクローンを製造・提示する攻撃。認証に利用する人工物の特徴は、人工物の物理構造と材料によって決まる。これらのうち、少なくともトークン t と同じ物理構造を有するクローンを製造・提示する攻撃がハード・コピー攻撃である。
- **リプレイ攻撃：** トークン t の CRP から y $(1 \leq y \leq d)$ 個のレスポンスを再現するクローンを製造・提示する攻撃。ただし、d はチャレンジの取り得る集合の大きさであり $d = |\mathcal{C}|$ である。再現するレスポンスは入手した CRP に含まれるものであり、レスポンスの推測は行わない。
- **シミュレート攻撃：** トークン t やそれ以外のトークンの CRP、あるいは、トークン t の観測データから未知の y $(1 \leq y \leq d)$ 個のチャレンジに対するレスポンスを推測し、当該レスポンスを再現するクローンを製造・提示する攻撃。

[3]松本・岩下［2004］では、クローンを利用した攻撃をブルート・フォース攻撃と、デッド・コピー攻撃に分類したうえで、デッド・コピー攻撃を「本物を見本にして固有パターンを複製したクローンを提示することで、人工物メトリック・システムの認証を通過させようとする攻撃」と定義している。本攻撃で利用されるクローンには、トークンの特徴を再現するクローンとある特定のレスポンスを再現するクローンのいずれも含まれていることから、松本・岩下［2004］におけるデッド・コピー攻撃は本節で整理するハード・コピー攻撃とリプレイ攻撃に対応するものとなっている。

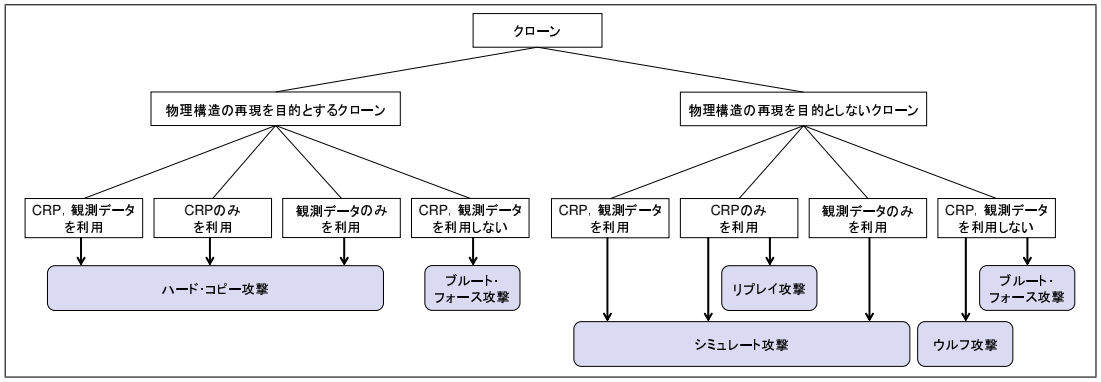

図 6: クローンの分類とクローンを利用した 5 種類の攻撃

- **ウルフ攻撃：** 一致と誤判定される参照データ数が最大となるレスポンス（ウルフ）を探索し、ウルフを再現するクローンを製造・提示する攻撃。
- **ブルート・フォース攻撃：** ランダムに入手・製造したクローンを提示する攻撃。

これらの攻撃に対して、人工物メトリック・システムは十分な耐性を有することが求められる。ただし、本稿では、高度なセキュリティを達成するように設計されたシステムを検討対象としており、ブルート・フォース攻撃のような容易に実行可能な攻撃については十分に低い誤合致率を達成するように対応済みであると仮定し、検討対象外とする。

また、リプレイ攻撃はトークン t から入手したレスポンスを再現する攻撃であるのに対し、シミュレート攻撃は入手したデータから推測して得たレスポンスを再現する攻撃である。これら 2 つの攻撃の違いは再現するレスポンスの入手方法であり、シミュレート攻撃は、リプレイ攻撃にレスポンスを推測する行為を追加した攻撃であると整理することができる。そこで、本稿では、検討の端緒として 2 つの攻撃のうちリプレイ攻撃に焦点を当てて検討を行うこととする[4]。

(3) 耐クローン性

クローン t' が誤ってトークン t であると認証されるケースは、クローンに対するチャレンジを c_k としたとき、次の 2 つに整理することができる。

[4]CRP の空間が大きい人工物メトリック・システムであっても、CRP 間に何らかの相関関係がある場合、少ない CRP で全空間を表現可能となるケースが考えられる。例えば、CRP の空間が線形空間である場合には、基底となる CRP を入手することで空間内のすべての CRP を表すことができる。こうしたケースでは、基底となる CRP に対応するレスポンスを再現するクローンを製造することで、全空間に対応するレスポンスを再現するというシミュレート攻撃が想定される。本攻撃においても、基底に対応するクローンをどのように製造するかというリプレイ攻撃のアイデアが耐クローン性を評価するうえでのポイントとなる。

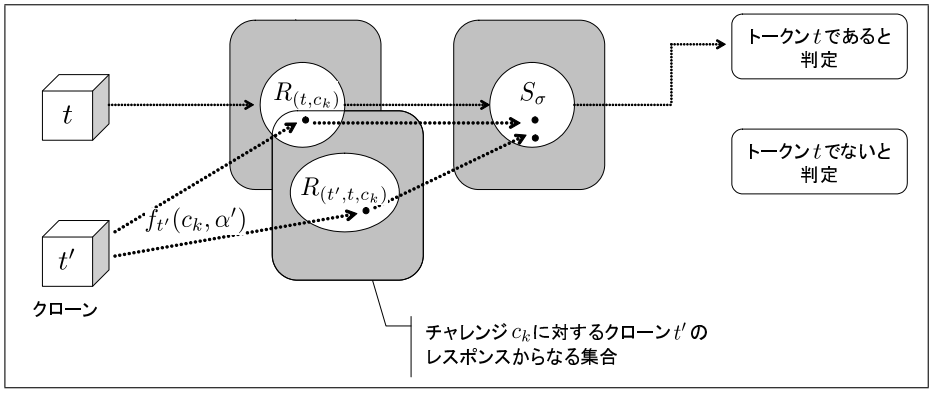

図 7: クローン t' が誤ってトークン t として受け入れられるフロー（概念図）

(A) チャレンジ c_k に対するクローン t' のレスポンスが $R_{(t,c_k)}$ の元となる。

(B) ケース (A) が満足されないものの、クローン t' のチャレンジ c_k に対するレスポンスから得られる固有パターンとトークン t の参照データとの類似度が S_σ の元となる。

ケース (B) での $ref_{(t,c_k)}$ との類似度が S_σ の元となるレスポンスの集合を $R_{(t',t,c_k)} = \{r \mid r = f_{t'}(c_k,\alpha),\ r \notin R_{(t,c_k)},\ h(g(r), ref_{(t,c_k)}) \in S_\sigma, \alpha \in \mathcal{A}\}$ とするとき（図 7 参照）、認証環境 α のもと、チャレンジ c_k に対してクローン t' がトークン t であると誤って認証される確率 $suc_{(t',\alpha)}$ は $suc_{(t',\alpha)} = \Pr[f_{t'}(c_k,\alpha) \in R_{(t,c_k)} \cup R_{(t',t,c_k)}]$ となる。このとき、アプリケーションが要求する許容されるクローン一致率の上限を γ とすると、任意の認証環境 $\alpha \in \mathcal{A}$ のもとで $\gamma \geq suc_{(t',\alpha)}$ が満たされるように、クローンを利用した攻撃への耐性を確保しておく必要がある。

ここで、耐クローン性を改めて次のように定義する。

定義 2 「耐クローン性」とは、セキュリティ評価対象である人工物メトリック・システムにおいて、想定する攻撃者がクローンを利用した攻撃を試みる場合に、その攻撃が成功することの難しさをいう。
また、人工物メトリック・システムのアプリケーションが要求する許容されるクローン一致率の上限 γ に対して、任意の認証環境 $\alpha \in \mathcal{A}$ のもとで任意のクローンについて誤って受け入れられる確率が γ 未満となるとき、当該システムは想定される攻撃者に対して十分な耐クローン性を有するという。

アプリケーションが要求する γ は、当該アプリケーションにおいて許容できるリスクに基づいて算出することが考えられる。例えば、バイオメトリクスの分野

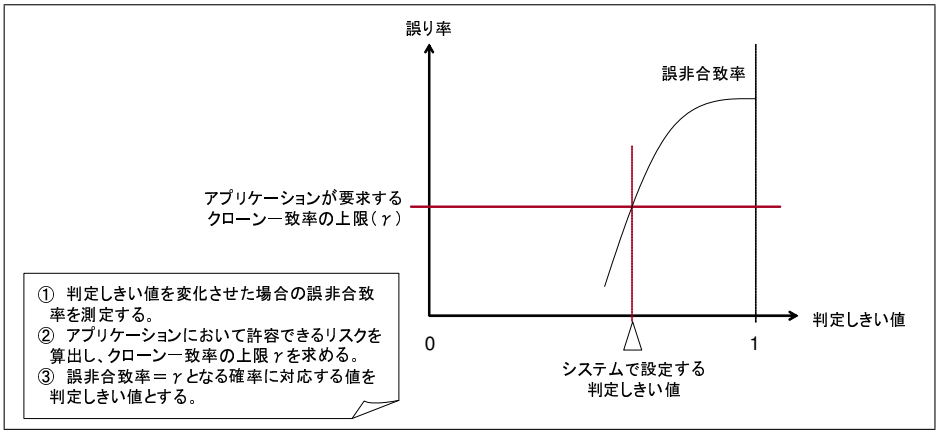

図 8: 判定しきい値の設定（概念図）

においては、リスク分析によって「許容できる誤受入率」を算出する方法が知られており、「バイオメトリクス認証システムにおける運用要件の導入指針」（日本工業標準調査会［2004］）においては以下の算出式が記述されている[5]。

許容できる誤受入率＝（許容できるリスク）／（保護対象の価値 × 不正アクセス頻度 × 不正認証阻止失敗率 ×ID 認知率 × 認証可能回数）

人工物メトリック・システムにおいても、同様の方法によって γ を算出することが考えられる。また、こうした方法等によって γ の要件を決めることができれば、その γ と誤非合致率が等しくなるように判定しきい値を設定することができる[6]（図 8 参照）。

[5]ただし、保護対象の価値はバイオメトリクス認証システムによる保護の対象となっているもの（あるいは情報）の価値、不正アクセス頻度は一定期間における不正アクセスの頻度、不正認証阻止失敗率は不正アクセスの阻止に失敗する確率、ID 既知率は攻撃対象のユーザの ID が攻撃者によって知られている確率、認証可能回数は攻撃者が一定時間内に実行可能な認証回数と定義されている（日本工業標準調査会［2004］）。

[6]2 節（2）イ．で記述したように、システムの判定しきい値は、誤合致率と誤非合致率を考慮して設定される。しかし、クローンを利用した攻撃を想定した場合、クローン一致率は誤合致率に比べて大きくなる傾向にあることが知られている（松本ほか［2004］）。

4．耐クローン性の評価アイデア

本節では、ハード・コピー攻撃、リプレイ攻撃、ウルフ攻撃のそれぞれについて、必要となる行為を整理するとともに、攻撃者が有する資源やシステム・パラメータが耐クローン性にどのような影響を与えるかについて考察を行う。

(1) ハード・コピー攻撃

イ．攻撃を構成する行為

ハード・コピー攻撃は主に以下の行為によって実行され、これらの行為がすべて成功することでクローンが受理されたときハード・コピー攻撃が成功したという（図 9 参照）。

- **設計書の作成に必要な情報の入手** ：クローンを検証装置に提示するタイミングでのチャレンジの候補、および、プローブを当てる範囲を推測し、トークンの読取範囲を得る。そのうえで、読取範囲の物理構造を推定する手掛かりとなる CRP や観測データを取得する[7]。
- **設計書の作成** ：CRP や観測データから読取範囲の物理構造を特定し、クローンを製造可能な加工技術を決定したうえで、具体的な加工工程を示す設計書を作成する。ここで、攻撃者はクローン製造に利用可能と想定される主な加工技術をいくつか知っているものとする。
- **加工** ：設計書を基にクローン t' を製造する。
- **クローンの提示** ：実運用されている検証装置に対して、ある認証環境 α' のもとで ID_t とともにクローン t' を提示する。

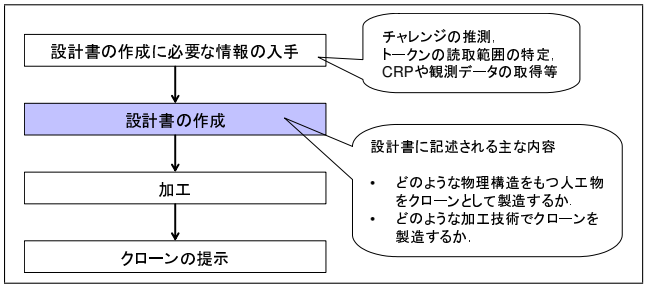

図 9: ハード・コピー攻撃を構成する行為

[7]クローン製造に利用する加工技術を想定したうえで、CRP や観測データを取得することも考えられる。こうしたケースでは、必要な情報の入手と設計書の作成が同時並行で実行されるといえる。

ロ．設計書の作成に必要な情報の入手

・トークンの読取範囲の特定

設計書を作成するに当たっては、トークンのどの部分を再現するクローンを製造するかを決定する必要がある。そのために、まず、クローンを検証装置に提示するタイミングで与えられるチャレンジを推測し、当該チャレンジに対応する読取範囲を特定することとなる。

チャレンジから読取範囲の特定が容易なケースでは、チャレンジを特定できるか否かがポイントとなる。例えば、検証装置によるチャレンジの選択がランダムである場合には、読取範囲のバリエーションの数を d' としたとき、読取範囲の推測が成功する確率は $1/d'$ であり、y $(1 \leq y \leq d')$ 種類の読取範囲を再現するようにクローンを製造するケースでの確率は y/d' である。ただし、攻撃者が実運用されている検証装置にトークン t を提示することによって、チャレンジの集合 $C_{(t,\ell)}$ に対応する読取範囲のバリエーションの一部を得ることも考えられる。こうしたケースでは、攻撃者が入手した情報量によって読取範囲の推測が成功する確率が変化する[8]。

また、検証装置によるチャレンジの選択が過去のチャレンジや時刻等に依存するケースでは、本稿で想定する攻撃者が検証装置の内部構造を知っており、チャレンジの選択方法を知っていることから、確率 1 でチャレンジを特定することができるといえる。

一方、チャレンジから読取範囲の特定が困難なケースでは、読取範囲のバリエーションに依らず、トークン全体の特徴を再現するようにクローンを製造することとなる。

・CRP や観測データの取得

特定した読取範囲におけるトークンの物理構造を記述する際の細かさは、人工物メトリック・システムがどの程度細かくトークンの物理構造を観察しているかに依存する。例えば、ある特定の波長の光をプローブおよびレスポンスとして利用するケースでは、光の波長程度の細かさで記述することになる。また、LC 回路[9]における共振周波数をレスポンスとして利用するケース（Škorić *et al.*［2008］）については、LC 回路の電極の面積、誘電体の誘電率、電極間の距離、コイルの形状によってレスポンスが決まるため、レスポンスに影響を与える細かさで LC 回路の

[8]認証に利用する CRP を 1 回限りにするといった運用がなされているケース（Pappu［2001］）では、こうした方法によって読取範囲の推測が成功する確率を高くすることは困難となる。

[9]LC 回路は、コイルとキャパシタで構成される電気回路であり、コイルの誘電係数とキャパシタの静電容量によって共振周波数が変化する。

構造を記述することが求められる。Škorić *et al.*［2008］では、誘電体として利用されるゲート絶縁膜の厚みを製造者が制御困難であり、ゲート絶縁膜の厚みが 0〜1μm の間で一様でないことを LC 回路の固有の特徴として利用すると記述していることから、少なくともサブ μm オーダーでの記述が必要になるといえる。

このように、トークンのレスポンスに影響を与える物理構造とその細かさを特定し、そうした細かさでの記述を可能とする CRP や観測データを入手する必要がある。こうしたデータの入手可能性は、攻撃者が有する資源に依存するといえる。例えば、クローンで再現する読取範囲に対して要求される細かさが非常に微細である場合や読取範囲が比較的大きい場合には、取得すべき観測データの量が莫大となり相対的に多くの資金と時間が必要になると考えられる。

ハ．設計書の作成

CRP や観測データからトークンの読取範囲の物理構造を特定・記述する方法は、トークンやクローンの種類に依存することになる[10]。例えば、CAD（computer aided design）[11]を利用してトークンの 2 次元構造、あるいは、3 次元構造を製図するという方法が挙げられる。

クローンにおいて再現する物理構造を記述できれば、次に加工技術を決定し設計書に記述する。既存の加工技術の中から適切な方法を選択するに当たっては、以下の 3 点が主な基準になると考えられる（帯川［2008］、日本機械工業連合会・製造科学技術センター［2008］、山形ほか［2007］）。

- **加工の細かさ** ：再現する物理構造において要求される細かさでの加工が可能か。
- **加工可能な材料** ：どのような材料を加工できるか。
- **加工のスピード** ：加工にどのくらいの時間がかかるか。

まず攻撃者は、既存の加工技術のデータベース[12]から、要求される細かさでの加工が可能であり、かつ、トークンと同じ特性を再現できる材料の加工が可能な技術を選択することとなる。クローンに利用する材料については、トークンと同じ

[10] トークンの認証は、参照データとの類似度が判定しきい値以上であるか否かによって行われるため、クローンの物理構造がトークン t と多少異なる場合であっても t と認証されることもある。クローンの物理構造はそうした許容範囲内になるように記述されるものとする。

[11] 製品の形状等のモデルをコンピュータを用いて設計すること、あるいは、その設計支援ツールのことであり、製品の製図を行う際に利用される。

[12] 本節で想定する攻撃者は、クローン製造に利用可能と想定される加工技術をいくつか知っており、そうした情報はデータベース化されているものとする。例えば、産業技術総合研究所デジタルものづくり研究センターでは、設計・製造現場で熟練技術者が暗黙知として持っている技能やノウハウ、経験を広く活用できるようにすることを目的として、機械加工部品の製造に関する幅広い加工技術を「加工技術データベース」として公開している。

材料である必要はなく、クローンと同じようにプローブに対して反応する材料であればよい。

加工技術を決定する方法としては、例えば、CAM（computer aided manufacturing）を利用するという方法が挙げられる。CAM は、CAD によって得られた物理構造のデータを基に必要な加工の細かさや加工可能な材料を考慮したうえで加工技術を検討し、NC プログラム[13]という形で決定結果を出力する[14]。NC プログラムは加工装置へ入力され、クローンが製造されることとなる[15]。ここで、加工装置とは、クローンを製造するために加工を行う機械や設備で構成されるものを指す。

利用可能な加工技術の候補が複数存在する場合には、なんらかの基準で加工技術を選択する必要があるが、例えば、加工にかかる資金と時間を基に最も効率的な方法を選択することが考えられる。

既存の加工技術のデータベースに該当する方法がないと判断された場合には、設計書を作成することができず、攻撃が実行できないこととなる。

ニ．加工

設計書に基づく加工の実行可能性は、クローンを製造するうえでの加工にかかる資金と時間との関係で示すことが考えられる。例えば、「設計書に記述される加工技術によってクローンを製造するには、少なくとも資金 $C_{M(fab)}$ と時間 $C_{T(fab)}$ が必要である[16]」といった評価が考えられる[17]。

クローンの製造は複数の加工技術を組み合わせて実行されることが想定される

[13]NC（numerical control、数値制御）は、加工装置が行う動作（位置、運動等）を表す数値情報によって装置を制御する方式のことであり、本数値情報を記述したものが NC プログラムである。

[14]例えば、3 次元形状を造形する方法としては、現在、CAD/CAM システムから直接 3 次元構造を造形する技術であるラピッド・プロトタイピング（積層造形法とも呼ばれる）の研究が盛んに進められている。ラピッド・プロトタイピングには、光で液体樹脂を硬化させるという方法（光造形法）、熱可塑性樹脂を溶かして積層させるという方法（熱溶解積層法）、粉末や液化した材料を積層させるという方法（3D プリンティング）等、さまざまな加工技術が存在する。仮に、クローンを製造する方法としてラピッド・プロトタイピングを選択した場合においても、上記の各種の方法から加工材料等を考慮して具体的な方法を選択することになろう。

[15]「産業オートメーションと統合」の国際標準化を担当する TC184 では、設計から製造への情報の伝達に関する標準を策定しており、CAD/CAM システム間のデータ・モデルを標準化している。同データでは、加工形状、加工に必要となる作業とその順序、作業方法の詳細等が記述される（坂本［2007］）。

[16]設計書どおりに加工を行うに当たっては、ある程度のトライ・アンド・エラーが発生することが想定される。そうしたトライ・アンド・エラーには一定の時間が必要となるが、より高性能な加工装置を利用するなど、より多くの資金をかけて時間を少なくすることも考えられることから、資金と時間はトレード・オフの関係にあるといえる。加工に必要な資金と時間については、考えられる複数の組み合わせのうち、最も効率的な値で評価することになる。

[17]同様のアイデアで実行可能性を評価している事例としては、専用ハードウエアを利用した素因数分解の実行可能性評価が挙げられる。本分野では、専用ハードウエアの構築にかかる費用と素因数分解にかかる時間によって評価が行われており、1,024 ビットの合成数の素因数分解は約 1,000 万ドルをかけると約 1 年で計算可能であるとする研究成果がある（Shamir and Tromer［2003］）。

ことから、個々の加工技術をそれぞれ上記アイデアに基づいて評価する必要がある。例えば、クローンの製造がA、B、Cの3つの加工技術を利用して実行されるとき、加工技術A、B、Cのそれぞれについて、加工の細かさ、加工可能な材料、加工のスピードを算出する。そのうえで、A、B、Cそれぞれにかかる資金と時間を算出することで、クローン製造の困難性を評価することが考えられる。

クローンの製造に利用される複数の加工技術すべてについて細かく評価すればより正確な評価結果を得ることができるが、最も資金や時間がかかる加工技術に着目して評価を行うということも考えられる[18]。一般には、細かい加工を実現する技術の方が費用がかかると想定されるほか、加工の細かさとそのスピードは反比例の関係にある（帯川［2008］）ことから、最も細かい加工が必要とする技術に着目して耐クローン性評価を行うことも一案であろう。

ホ．クローンの提示

攻撃者はトークンの発行者や検証装置の製造者と同じ資源を有することから、トークン登録時の認証環境$\bar{\alpha}$を選択してクローンを提示することが考えられる[19]。したがって、以下では、クローンを提示するタイミングでの認証環境α'は、トークンtの登録時における認証環境$\bar{\alpha}$と同一であるとして議論を進める。

ヘ．まとめ

このように、ハード・コピー攻撃を構成する4つの行為のうち、同攻撃への耐クローン性評価の観点でポイントになるのは、設計書の作成に必要な情報の入手、設計書の作成、クローンの加工の3つと考えられる。設計書の作成に必要な情報の入手においては、とりわけCRPや観測データの取得が主な評価対象となり、チャレンジが示す読取範囲を特定できる確率、取得する必要があるデータの量、そうしたデータを入手するために必要な資金や時間がベンチマークとなろう[20]。クローンの加工において実現可能な方法が設計書の作成のフェーズで見つかれば、次にクローンの加工にどの程度の資金や時間が必要となるかが評価対象となる。

こうした整理をもとに、検討対象となった加工技術の候補リストをL、チャレンジが示す読取範囲を特定できる確率をδ、CRPや観測データの入手や加工に必要

[18]素因数分解の実行可能性評価では、現時点で最も効率のよい素因数分解アルゴリズムである一般数体ふるい法を構成する処理のうち、ふるい処理に最も多くの計算時間が必要となるとの結果から、ふるい処理にかかる時間によって素因数分解にかかる時間の見積りが行われている（情報通信研究機構・情報処理推進機構［2007］）。

[19]例えば、攻撃者は検証装置における認証の試行を認証環境が$\bar{\alpha}$になるまで繰り返し実行し、$\bar{\alpha}$が実現したタイミングでクローンを提示するという状況が考えられる。

[20]こうした評価を行う際には、1つのトークンのクローンを作製するケースだけでなく、一定数のまとまった数のクローンを作製することを前提とすることも考えられる。

な資金をC_M、時間をC_Tとするとき、ハード・コピー攻撃の耐クローン性を以下のように厳しめに評価することが考えられる。

> **ハード・コピー攻撃に対する耐クローン性の評価** ：想定する人工物メトリック・システムに対して、「加工技術の候補リストLのもとで確率δで正しく読取範囲を特定してハード・コピー攻撃を実行するには、少なくとも資金C_Mと時間C_Tが必要である」と評価するとともに、想定する攻撃者の資源のもとで評価される確率δが当該アプリケーションにおいて要求されるγ未満であるならば、当該システムは想定する攻撃者に対して十分な耐クローン性を有していると評価する。

クローンの製造にかかる資金C_Mや時間C_Tは、他の条件を一定とすると、一般にクローンの大きさ（体積、面積）に伴い増加することから、チャレンジによってトークンの読取範囲が異なるケースでは、δとC_M、C_Tはトレード・オフの関係にあるといえる。そのため、確率δを高くした場合のC_MとC_Tについても上記項目が満足されていることを確認して耐クローン性を評価することが必要である。

(2) リプレイ攻撃

イ．攻撃を構成する行為

リプレイ攻撃[21]は主に以下の行為によって実行され、これらの行為がすべて成功することでクローンが受理されたときリプレイ攻撃が成功したという。

- **設計書の作成に必要な情報の入手** ：クローンを検証装置に提示するタイミングでのチャレンジの候補c_i $(1 \leq i \leq y)$を推測する。そのうえで、ある認証環境αのもとで各c_iに対するレスポンス$r_{t(i,\alpha)}$ $(1 \leq i \leq y)$を取得する。
- **設計書の作成** ：取得したレスポンス$r_{t(i,\alpha)}$から当該レスポンスを再現可能なクローンの物理構造を決定し、そうしたクローンを製造可能な加工技術を選択するとともに設計書を作成する。ここで、攻撃者はクローン製造に利用可能と想定される主な加工技術をいくつか知っているものとする。

[21]暗号技術を利用した認証方式では、正規ユーザからの認証用データを不正に転送することによってなりすましを行う攻撃（一般に、マフィア・フロードと呼ばれる）(Beth and Desmedt［1991］)が知られている。こうした攻撃は、人工物メトリック・システムにおいては、与えられたチャレンジを速やかに検知したうえでそれに対応するトークンtのレスポンスを入手・転送することにより、クローンを誤って受理させる攻撃として想定される。本攻撃は、$y = |\mathcal{C}|$としたリプレイ攻撃として整理することができる。

- **加工** ：設計書を基にクローン t' を製造する。
- **クローンの提示** ：実運用されている検証装置に対して、ある認証環境 α' のもとで ID_t とともにクローン t' を提示する。

ロ．設計書の作成に必要な情報の入手

・チャレンジの推測

本行為の実行可能性はチャレンジの情報量に依存して決まる。検証装置によるチャレンジの選択がランダムである場合には、チャレンジのバリエーションの数を d としたとき、チャレンジの特定に成功する確率は $1/d$ となり、y 個のレスポンスを再現するクローンを製造するケースでは確率は y/d となる。ただし、攻撃者が実運用されている検証装置にトークン t を提示することによってチャレンジの集合 $C_{(t,\ell)}$ の一部を得ることも考えられる。こうしたケースでは、攻撃者が入手した情報量によってチャレンジの推測が成功する確率が変化する。また、検証装置によるチャレンジの選択が過去のチャレンジや時刻等に依存するケースでは、確率 1 でチャレンジを特定することができるといえる。

・レスポンスの取得

本稿で想定する攻撃者は、自作した検証装置を利用して選択したチャレンジに対するレスポンスを得ることができる。また、トークン t の参照データは認証環境 $\bar{\alpha}$ のもとで生成されるが、攻撃者はトークンの発行者や検証装置の製造者と同じ資源を有することから $\bar{\alpha}$ を知っており、同じ認証環境 $\bar{\alpha}$ を選択してレスポンスを取得することが考えられる。したがって、以下では $\alpha = \bar{\alpha}$ と仮定して議論を進める。

このように、本節で想定する攻撃者であればレスポンスの入手は実行可能であると考え、設計書の作成に必要な情報を入手する難しさが、チャレンジの推測に成功することの難しさによって専ら表されるとして議論を進める。

ハ．設計書の作成

レスポンス $r_{t(i,\alpha)}$ を再現するクローンの種類としては、(A) チャレンジとして c_i が与えられたときに $r_{t(i,\alpha)}$ を返すクローン（受動的クローンと呼ぶ）と、(B) どのようなチャレンジに対しても $r_{t(i,\alpha)}$ を返すクローン（能動的クローンと呼ぶ）の 2 種類が考えられる。

また、いずれのクローンにおいても、y種類のレスポンスを複数の物理媒体で再現するケースがある。このようなケースでは、どのチャレンジが与えられたかを速やかに検知したうえで当該チャレンジに対応する物理媒体を提示する必要があり、チャレンジを検知する機構や対応する物理媒体を速やかに提示する機構を含める形で「クローン」が形成される。

クローンの物理構造を決定するうえでは、どのような方法でレスポンスを再現するかについて、レスポンスの形態、チャレンジからレスポンスまでの時間、検証装置の形状等を考慮しつつ検討する必要がある。また、複数のレスポンスを再現するようにクローンを製造する場合には、チャレンジを検知する機構等に関する検討も必要となる。

レスポンスを再現するクローンの物理構造が決定すれば、ハード・コピー攻撃と同様、加工の細かさ、加工可能な材料、加工のスピードを考慮してクローンの製造に利用する加工技術を選択することとなる。ただし、ハード・コピー攻撃では、トークンと同じ物理構造を再現する必要があったのに対し、リプレイ攻撃ではある特定のレスポンスを再現するクローンを製造すればよいことから、加工技術の選択に当たっては、材料や物理構造に関する制限が比較的少ない。また、ハード・コピー攻撃ではレスポンスに影響を与える物理構造の細かさを検討する必要があったが、リプレイ攻撃では主にレスポンスの取得に利用するセンサーの分解能[22]を考慮することで加工の細かさを決定可能なケースが多いと考えられる。

例えば、紙の赤外透過光画像をレスポンスとして利用するシステムでは、取得した画像をそのまま PET 樹脂にコピーする方法を採用した研究事例がある（平良・山越・松本［2007］）。また、紙に埋め込んだ磁気ファイバーの磁気パターンをレスポンスとして利用するシステムでは、トークンと同じ磁気パターンを発生させるように磁性材を紙に塗布してクローンを製造する研究事例がある（松本ほか［2004］）。本事例では、磁気パターン・ピッチと同程度の細かさで磁性材の塗布の制御が行われている。

ニ．加工

リプレイ攻撃における本行為の難しさについても、ハード・コピー攻撃と同様、「設計書に記述される加工技術によってクローンを製造するには、少なくとも資金$C_{M(fab)}$と時間$C_{T(fab)}$が必要である」といった評価が考えられる。例えば、上記の平良・山越・松本［2007］の事例では、「コピー機の調達にかかる資金とコピーの実行の時間が必要である」と評価することができる。

[22]装置において物理量を測定・識別できる能力である。

ホ．クローンの提示

能動的クローンの場合、クローンを提示するタイミングでの認証環境に依らず、クローンは $r_{t(i,\alpha)}$ を検証装置に返す。一方、受動的クローンの場合、α 以外の認証環境におけるレスポンスがトークン t のレスポンスとならないケースが想定されるが、攻撃者は認証環境 α を選択してクローンを提示するものとして議論を進める。

ヘ．まとめ

リプレイ攻撃を構成する 4 つの行為のうち、同攻撃への耐クローン性評価の観点でポイントとなるのは、ハード・コピー攻撃と同様、設計書の作成に必要な情報の入手、設計書の作成、クローンの加工の 3 つと考えられる。設計書の作成に必要な情報の入手においては、チャレンジを推測できる確率や取得する必要がある CRP のデータ量が実行可能性を評価するうえでのポイントとなり、必要なデータを入手するための資金や時間がベンチマークとなる。さらに、レスポンスを再現するクローンの加工技術が設計書の作成のフェーズで見つかれば、クローンの加工にどの程度の資金や時間が必要となるかが評価対象となる。

こうした整理をもとに、検討対象となった加工技術のリストを L、チャレンジを推測できる確率を δ、CRP の入手、設計書の作成、加工に必要な資金を C_M、時間を C_T とするとき、リプレイ攻撃の耐クローン性を以下のように厳しめに評価することが考えられる。

リプレイ攻撃に対する耐クローン性の評価 ：想定する人工物メトリック・システムに対して、「加工技術の候補リスト L のもとで確率 δ で正しくチャレンジを特定してリプレイ攻撃を実行するには、少なくとも資金 C_M と時間 C_T が必要である」と評価するとともに、想定する攻撃者の資源のもとで評価される確率 δ が当該アプリケーションにおいて要求される γ 未満であるならば、当該システムは想定する攻撃者に対して十分な耐クローン性を有していると評価する。

本節で整理したように、リプレイ攻撃は特定のレスポンスを再現するクローンを製造すればよいことから、リプレイ攻撃にかかる資金や時間はハード・コピー攻撃より相対的に少なく評価されるケースが多いと考えられる。ただし、チャレンジの情報量が非常に大きい場合には δ が小さくなる。δ を大きくするには、より多くのチャレンジへのレスポンスを再現するクローンを製造することとなるが、チャレンジを検知して対応するレスポンスを速やかに提示する必要があり、クローンの製造に必要な資金や時間が大きくなるといえる。

(3) ウルフ攻撃

イ．攻撃を構成する行為

ウルフ攻撃は主に以下の行為によって実行され、これらの行為がすべて成功することでクローンが受理されたときウルフ攻撃が成功したという。

- **設計書の作成に必要な情報の入手** ：クローンを検証装置に提示するタイミングでのチャレンジの候補 c_i $(1 \leq i \leq y)$ を推測する。すべてのレスポンスの集合の中から、各チャレンジ c_i に対して認証環境 $\bar{\alpha}$ のもとで一致と誤判定される参照データ数が最大となるレスポンス（ウルフ）$r^w_{(i,\bar{\alpha})}$ を探索する。ウルフの探索に利用する参照データは、実運用されている検証装置に登録されているものではなく、システムとして取り得る参照データの集合となる。
- **設計書の作成** ：探索したウルフ $r^w_{(i,\bar{\alpha})}$ を再現するクローン t' の物理構造を特定するとともに、クローンを製造可能な加工技術を決定し設計書を作成する。ここでは、攻撃者はクローンの製造に利用可能と想定される主な加工技術をいくつか知っているものとする。
- **加工** ：設計書をもとにクローン t' を製造する。
- **クローンの提示** ：実運用されている検証装置に対して、ある認証環境 α' のもとで ID_t とともにクローン t' を提示する。

ウルフ攻撃は、できるだけ多くのトークンに対して誤って一致するようなレスポンスを探索し、当該レスポンスを再現するクローンを提示する攻撃であり、攻撃対象となるトークンを固定しない点が他の攻撃とは異なる。したがって、クローンの提示の際に一緒に提示される ID_t はウルフ探索に用いられる参照データの集合に含まれる任意の ID_t でよい。

ウルフ攻撃とリプレイ攻撃の主な違いはクローンで再現を試みるレスポンスの取得方法であることから、設計書の作成、加工、クローンの提示については、本節で取扱わないこととする。

ロ．設計書の作成に必要な情報の入手

本行為の実行可能性は、ウルフとなるレスポンスを再現するクローンを提示したときに、ある参照データと一致する確率として評価することができ、バイオメトリクスの分野において提案されているウルフ攻撃確率に対応する（Une, Otsuka, and Imai［2008］）。人工物メトリック・システムの文脈では、ウルフ攻撃確率は、

システムにおいて利用されうるすべてのレスポンスの集合を $\mathcal{R}$、登録されている c_i に対応する参照データの集合を $\mathcal{T}$ としたときに、以下のように表される。

$$\max_{r\in\mathcal{R}} \underset{ref\in\mathcal{T}}{Ave} \Pr[h(g(r), ref) \in S_\sigma]$$

いま、攻撃者がレスポンスの部分集合 $\mathcal{R}' \subset \mathcal{R}$ と c_i に対応する参照データの部分集合 $\mathcal{T}' \subset \mathcal{T}$ についてウルフの探索を行うとすれば、そうしたウルフ攻撃の成功確率を以下の式で表すことができる。

$$P_{(wolf,i)} = \max_{r\in\mathcal{R}'} \underset{ref\in\mathcal{T}'}{Ave} \Pr[h(g(r), ref) \in S_\sigma]$$

そのほか、g や h の脆弱性を利用してウルフを探索するケースも考えられる。

(4) 小括

本節では、クローンを利用した攻撃を想定し、人工物メトリック・システムの耐クローン性を評価するアイデアとして、クローンを製造するために必要な資金と時間、および、製造したクローンを提示した場合に誤って受け入れられる確率を利用する方法を示した。評価を行う際には、実際にクローンの設計書を作成し、クローンの製造にかかる資金や時間を推定することが考えられる。こうした評価が可能となれば、さまざまな人工物メトリック・システムの比較も可能となろう。

特に、クローンの製造に必要な資金と時間の評価が妥当であるためには、評価用に作成する設計書が、想定される攻撃者によって採用され得る加工技術の中で最も効率的なものを記述していることが前提となる。公開されている加工技術の情報から最先端の研究開発動向を調査したり、各業界団体から公開されている技術ロードマップを参考にしたりして、設計書の内容を吟味することが必要であろう。特に、クローンの製造に利用可能であると想定されるマイクロ加工やナノ加工の技術レベルは日進月歩であることから、定期的にそうした技術分野の動向を調査し、継続的に評価を行うことが必要であると考えられる。

5．人工物メトリック・システムの耐クローン性評価の例

前節で提案したアイデアに基づく耐クローン性の評価事例について、具体的な人工物メトリック・システムを想定して考察を行う。ここでは、クローンを製造する行為の難しさについて検討を試みた数少ない事例の 1 つである Pappu［2001］を取り上げ、既存研究における評価結果をどのように耐クローン性の評価に利用できるか、また、耐クローン性を評価するには追加的にどのような評価が必要かを明らかにする。

Pappu［2001］とŠkorić *et al.*［2007］は、同じ特徴を利用した人工物メトリック・システムについて検討を行っているが、実装したシステムの仕様は若干異なる。また、Škorić and Tuyls［2007］では、Pappu［2001］で提案された人工物メトリック・システムに対して、チャレンジの情報量やレスポンスの情報量について追加的な検討を行うものとなっている。

（1）想定する人工物メトリック・システム

Pappu［2001］、および、Škorić *et al.*［2007］において検討の対象とされている人工物メトリック・システムは、前節で想定したシステムと同様の属性を有しており、以下の仕様となっている（図 10 参照）。

- トークン：トークンは、表面積 10mm × 10mm、厚さ 2.54mm のエポキシ樹脂に散乱体（ガラス球）をランダムに配置した人工物であり、プラスチック・カードの中央に埋め込まれて利用される。散乱体の屈折率は約 1.5 であり、散乱体の大きさ（直径）は 500〜600μm である。
- チャレンジ：プローブとしてレーザ光を利用する。レーザ光の波長は λ とし、一定の空間光変調[23] I が行われた後、トークンに対して入射角 θ で照射される。パラメータ λ、I、θ はレスポンスに相関が生じない範囲でランダムに選択可能となっている。ただし、Pappu［2001］における実験では、λ（632.8nm）と θ は固定し、I のみを変化させてチャレンジにバリエーションをもたせている。空間光変調は DMD（digital micromirror device）[24]を用いて行っており、微小鏡面（マイクロミラー）の数を $M \times N$ としたうえで、チャレンジのバリエーションを $2^{M \times N}$ と表している。実験では、$1,000 \times 1,000$ のマイクロミラーで構成される DMD が利用されている。また、毎回トークンの表面全体にプローブを当てることとしており、トークンの読取範囲は固定されているといえる。

[23]光の振幅、位相、偏光等の空間的な分布を制御し、光の特性を変化させること。

[24]DMD は薄膜内の微小鏡面（マイクロミラー）の角度を制御することによってレーザ光等を変調する光・電子集積デバイスである。

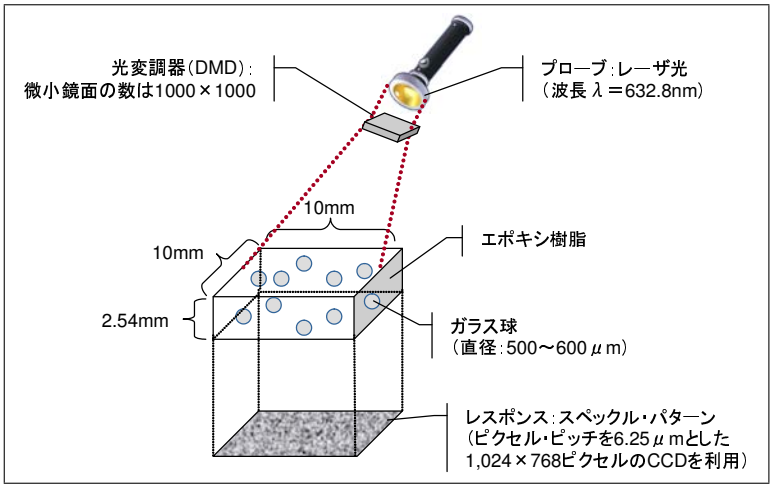

図 10: 想定する人工物メトリック・システム（概念図）

- レスポンス：透過光によるスペックル・パターン[25]をレスポンスとして利用し、同パターンは 1 つの CCD（charge coupled device）によって取得される。Pappu［2001］による実験では、320×240 ピクセルの CCD が利用されているほか、Škorić *et al.*［2007］による実験では、ピクセル・ピッチを 6.25μm とした $1,024 \times 768$ ピクセルの CCD が利用されている。
- 固有パターン：トークンから取得したスペックル・パターンをガボール変換して得た 2,400 ビットのデータを固有パターンとして利用する。

（2）耐クローン性評価

以下では、Pappu［2001］等における検討結果から考察が可能なハード・コピー攻撃とリプレイ攻撃に焦点を当てて検討する。

イ．ハード・コピー攻撃に対する耐クローン性

（イ）設計書の作成に必要な情報の入手

プローブの読取範囲はトークン全体となっており、その物理構造の特定に関しては、Pappu［2001］では、トモグラフィー技術[26]を利用してトークンの 3 次元構造の断面画像を観測データとして取得するという方法に関する記述がある。本技術による観測データの取得方法に関する具体的な検討結果が Pappu［2001］には示されていないものの、国際半導体技術ロードマップ 2007 年版（電子情報技術産業

[25]光が散乱、反射することで生じる明暗の斑点模様のこと。
[26]人体や物体の平面断面部分の放射線写真を撮る技術である。

協会［2008］）によれば、既にナノレベルでの計測が可能であると示されており、こうした観測データの取得も相応の資金によって可能であるとみられる。

（ロ）設計書の作成

要求される加工の細かさは、Pappu［2001］においては、プローブとして利用されるレーザ光の波長λに設定されており、1辺をλとした立方体（ボクセルと呼ばれる）でクローンの3次元構造が表現されている。そのうえで、λの細かさをもつ加工技術としてリソグラフィー技術[27]が取り上げられている。加工に利用する材料については記述されていないが、トークンと同じように、光を透過・散乱させる材料であればよいことから、さまざまな材料を利用可能であり比較的調達が容易と考えられる。ただし、加工のスピードについても記述されておらず、リソグラフィー技術が適用可能な加工技術のうちで最も効率的か否かについても考察されていない。

（ハ）加工

Pappu［2001］では、クローンを製造する加工技術としてリソグラフィー技術を選択したうえで、その技術の確保に必要な資金を1999年の評価をもとに約24億ドルと概算している[28]。加工にかかる時間については、「クローンの縦方向の細かさを50nmで製造した場合には2.54mmの厚さのトークンを製造するに当たって5万層を積層する必要がある」といった例が挙げられており、50nmの細かさで5万層の積層を現実的な時間で行うことは難しいとの見方が示されている。

ロ．リプレイ攻撃に対する耐クローン性

Pappu［2001］やŠkorić *et al.*［2007］では、本稿で定義するリプレイ攻撃とは若干異なるタイプの攻撃を検討対象としている[29]。ただし、本稿のリプレイ攻撃について検討するうえで有益な情報や検討結果が示されていることから、本稿のリプレイ攻撃に適宜当てはめる形で考察する。

---

[27]光を利用した微細加工技法の1つであり、主に大規模集積回路のパターン形成等に用いられている。特定のパターン用原版（原画）を、光や電子に反応する薄膜（レジスト）に覆われたシリコン・ウエハ上に光や電子ビームの照射によって縮小投影して露光するという方法が利用されている（小柳［2005］）。

[28]具体的には、露光工程にかかる費用を816百万ドル、自動フォトレジスト処理工程にかかる費用を288百万ドル、エッチング工程にかかる費用を280百万ドル、洗浄・ストリップ工程にかかる費用を30百万ドル、自動化工程にかかる費用を30百万ドル、インフラ整備にかかる費用を992百万ドルと概算している。

[29]これらの研究事例では、固有パターンを再利用する攻撃をリプレイ攻撃と呼んでおり、検証装置の処理過程に当該固有パターンを挿入する攻撃が想定されている。

（イ）設計書の作成に必要な情報の入手

Pappu［2001］においては、チャレンジのバリエーションが 2^{10^6} と設定されており、バリエーションについての本評価が正しいとすれば、攻撃者がチャレンジを正しく推測する確率は $1/2^{10^6}$ と無視できるほど小さいといえる。また、Pappu［2001］では、攻撃者がすべてのチャレンジに対するレスポンスを格納しておくことは難しいといった評価を行っているほか、レスポンスを保管可能な場合においても、認証に利用する CRP を 1 回限りにするという運用によってリプレイ攻撃を防止可能であると述べている[30]。

（ロ）設計書の作成

クローンの物理構造を決定するに当たっては、特定のスペックル・パターンの再現方法をまず検討することになる。Pappu［2001］等には記述がないが、受動的クローンの例として、レーザ光に対する反射をシミュレートし、その結果に基づいて当該レーザ光に対応するスペックル・パターンをホログラムで再現するといったアイデアが考えられる[31]。能動的クローンの例としては、CCD カメラのピクセル・ピッチと同程度のサイズの発光素子を、再現したいスペックル・パターンに合わせて構成するといったアイデアが考えられよう[32]。

次に、こうしたアイデアに基づいて加工技術を検討することになる。加工技術の加工の細かさは、スペックル・パターンを取得するセンサーの分解能を基準として設定することが考えられる。Pappu［2001］ではセンサーの分解能に関する記述はないが、Škorić *et al.*［2007］では、ピクセル・ピッチを 6.25μm とする CCD が利用されている。このことから、クローンの製造には少なくともサブ μm オーダーの細かさで加工可能な技術が求められる。加工に利用可能な材料については、受動的クローンを製造する場合には、スペックル・パターンを再現するホログラム用材料が考えられるほか、能動的クローンを製造するケースでは、発光素子とそれを制御するための材料が求められる。

---

[30]ただし、本稿で想定する攻撃者は、トークン t を入手しているほか、検証装置の利用や自作も可能であることから、トークン t の認証に使用されていないチャレンジに対するレスポンスを取得できるケースがある。また、認証の回数が増えると、使用可能なチャレンジの数も減り、チャレンジ推測の確率も徐々に高まってくることになる。このように考えると、本稿における攻撃者のもとでリプレイ攻撃を十分に防止可能か否かについては更なる検討が必要といえる。

[31]紙の透過光パターンを利用した人工物メトリック・システムにおける耐クローン性評価事例では、透過光パターンを OHP にコピーしたものをクローンとして利用している。本システムにおいてもスペックル・パターンの斑点模様を透明の物質にコピーすることによってクローンを製造することができる可能性もあろう。

[32]例えば、1cm^2 に 2,500 万個のドットで 390nm の波長を持つ蛍光発光素子が開発されており（物質・材料研究機構［2003］）、こうしたアイデアも実現可能とみられる。

（ハ）加工

受動的クローンとしてスペックル・パターンを再現するホログラムを作成するケースでは、ホログラムの加工装置が必要となる。そうした加工装置を利用するために必要な資金や時間によって評価することが考えられる。例えば、ホログラムの製造設備を有する機関に製造を依頼することでクローンを製造するということも想定される。

また、発光素子をアレイ状に配置した人工物を能動的クローンとして利用するケースでは、必要な発光素子およびそれを制御する装置を製造・調達する資金や時間によって評価することが考えられる。

（3）考察

イ．ハード・コピー攻撃について

こうした評価事例を前節で示した評価のアイデアに当てはめると「確率 1 で正しくチャレンジを推定しハード・コピー攻撃をリソグラフィー技術によって実行するには、少なくとも 24 億ドルの資金が必要である」との評価結果となる。

本評価結果を解釈するに当たっては、いくつかの留意点が存在する。まず、Pappu［2001］はリソグラフィー技術を取り上げて議論しているが、近年マイクロ・ナノ加工技術の研究開発が急速に進められており[33]、Pappu［2001］の検討がクローンの製造に利用可能な既知の主な方法のうち資金と時間の観点で最も効率的に実行可能な方法となっているか否かを確認する必要がある。そうした確認を行ったうえで、どのくらいの時間によってクローンの製造が可能となるかを推定することが求められる。さらに、こうした評価結果によって当該システムが特定のアプリケーションにおいて利用できるかを考える必要がある。システムのユーザ（運用者）は自分のアプリケーションにおける許容されるリスクを明確にしたうえで、上記クローンの製造にかかる資金や時間との比較を行うことになると考えられる。

ロ．リプレイ攻撃について

リプレイ攻撃については、チャレンジの特定に成功する確率が Pappu［2001］において示されているが、設計書の作成方法や加工については検討結果が示されていない。そのため、リプレイ攻撃に対する耐クローン性を評価するに当たっては、

[33]例えば、日本機械工業連合会・日鉄技術情報センター［2008］では、新しい加工技術として、超精密切削、ファインブランキング、プラスチック特殊成形、積層造形、ナノインプリント、大面積電子ビーム、集束イオンビーム・化学気相成長（FIP-CVD：focused ion beam-chemical vapor deposition）、レーザ加工を挙げ、これらの技術動向について取り纏めている。

まず、どのような設計書を作成するかについて検討することが必要である。本節では、一例として、ホログラムや発光素子を利用したクローンのアイデアを示した。このようなアイデアでクローンの物理構造を決定し、当該方法がクローンの製造に利用可能な既知の主な方法のうち資金と時間の観点で最も効率的に実行可能な方法であるか否かを確認する必要がある。そうした確認を行ったうえで、クローンの製造にどのくらいの資金と時間が必要になるかを推定することが求められる。

仮に、ホログラムによってクローンを製造する方法が資金と時間の観点で最も効率的に実行可能であることが確認でき、さらに、その製造に資金 $C_{M(fab)}$ と時間 $C_{T(fab)}$ が必要であるとの評価ができたとしよう。その場合、チャレンジの実質的なバリエーションが d $(\leq 2^{10^6})$ とすれば、「確率 $1/d$ で正しくチャレンジを特定しリプレイ攻撃をホログラムによって実行するには、少なくとも資金 $C_{M(fab)}$ と時間 $C_{T(fab)}$ が必要である」と評価することができよう。例えば、リソグラフィー技術でホログラムを製造する場合には、ハード・コピー攻撃での評価と同様、少なくとも 24 億ドルの資金が必要になると評価することができる。ただし、ハード・コピー攻撃では数万のレジストを積層する必要があり、より多くの資金が必要になると想定されるほか、相対的に多くの時間が必要になると想定される。また、ホログラムの製造設備を有する企業等に製造を依頼するケースでは、同じホログラムを大量に作製する場合、一般に 1 枚あたり数円で製造可能であるほか、製造にかかる時間も 1〜2ヵ月程度と評価することができるとも言われている。

上記評価では、チャレンジの推測に成功する確率を $1/d$ としているが、多くのクローンを準備することとすれば、チャレンジの推測に成功する確率が高くなる。その場合には、一般にクローンの製造に必要な資金と時間が増加する。システムのユーザは、チャレンジの推測に成功する確率とそれに対応する加工に必要な資金と時間のバリエーションを考慮したうえで、アプリケーションが要求する γ、想定する攻撃者が有する資源との比較を行うことになると考えられる。

6．今後の課題

本稿で示した耐クローン性の評価アイデアは、クローン製造にかかる資金と時間で耐クローン性を評価するものであるため、その利点としては、まず、異なる種類の人工物メトリック・システムの耐クローン性の比較が可能な点が挙げられる。また、攻撃者が利用する資源を明示することにより、評価対象となっている人工物メトリック・システムをどのようなアプリケーションで利用可能かを明らかにすることができるという利点もある。

ただし、5節で述べたように、既存の人工物メトリック・システムの耐クローン性を評価するには、既存の評価事例における結果を参照するのみでは不十分であり、追加的に検討が必要な項目も多い。また、具体的に評価方法を適用するうえでは、クローン製造に必要な各行為にかかる資金、時間をどのように試算すべきかについて検討を深める必要がある。そこで、以下では、本評価方法を精緻化するに当たっての検討課題を示す。

(1) 候補リストをどのように作成するか

本稿で示した評価方法に従って耐クローン性を評価するに当たっては、攻撃者が設計書の作成に利用する加工技術の候補となるデータベースをどのように作成するかについて更なる検討が必要である。4節で紹介したとおり、わが国においては産業技術総合研究所デジタルものづくり研究センターによって機械加工部品の製造に関する幅広い加工技術[34]が加工技術データベースとして公開されており、こうしたデータベースを耐クローン性評価に利用するという方法も考えられる。ただし、本データベースは機械加工部品の加工技術を対象としたものであり、当該データベースに含まれていない技術を利用してクローンを製造することも考えられる。クローンの加工技術はトークンの種類にも依存することから、各トークンに適用可能とみられる加工技術を、既存の加工技術のデータベースを参考にしつつどのように網羅的に抽出するかが今後の課題となろう。

(2) 設計書の作成や加工技術をどのように選択するか

本評価方法は、リストアップされた既存の加工技術の中から資金と時間の観点で最も効率がよいものを選択することで、攻撃に必要な資源の下限を示すものであるといえる。そうした観点で設計書の作成や加工技術の選択を適切に実行する

[34]鋳造、鍛造、金属プレス、射出成形、切削、研削、研磨、放電加工、レーザ切断、レーザ溶接、アーク溶接、めっき、PVD-CVD、溶射、熱処理のカテゴリーに分類される加工技術がデータベース化されている。

必要がある。

4節では、加工技術を決定する方法としてCAMの利用を挙げたが、CAMによってすべての人工物におけるクローンの加工技術を適切に決定できるとは限らない。どのような決定の方法が利用可能であるかは人工物メトリック・システムによって異なる可能性もあり、加工技術の適切な決定方法について今後検討が必要であろう。

(3) 評価対象となるシステムの要求仕様をどう決めるか

人工物メトリック・システムの耐クローン性については、想定する攻撃者とアプリケーションのもとで許容されるクローン一致率の上限γについて、任意のクローンが誤って受け入れられる確率がγ以下であるとき、十分な耐クローン性を有するとした。3節で述べたとおり、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が特定されている場合には、許容される誤合致率と等しくなるようにγを設定することができる。γを適切に設定するには、想定するアプリケーションにおけるリスク分析を適切に行うことが必要であり、許容できるリスクをどの程度に見積もるか、保護対象の価値はどの程度かを適切に評価することも重要な課題となる。

一方、ある人工物メトリック・システムをどのようなアプリケーションで利用可能かを検討するうえで耐クローン性の評価を実施するケース等、耐クローン性評価を行う時点で当該システムを適用するアプリケーションが明確になっていない場合には、クローン一致率の上限γを変数として、各γの値に対応する判定しきい値を有するシステムの評価を実施することが考えられる。しかし、複数のγに応じた耐クローン性評価を行う際には、攻撃を実行するのに必要な資金と時間をそれぞれ概算する必要がある。複数のバリエーションについて評価を行うには相応の時間やコストがかかることが予想されるため、耐クローン性の評価を効率的に実施する方法についても検討が必要である。例えば、クローン製造に必要となる資金C_Mや時間C_Tと、攻撃者がチャレンジを推測できる確率δとの関係を何らかの手法で見出し、定式化するといった方法が考えられよう。

(4) 本評価アイデアの妥当性をどのように確認するか

本稿で提案した評価方法に基づく評価結果の妥当性を確認する方法として、耐クローン性評価を行ううえで想定した行為に沿って実際にクローンの製造を試行することが考えられる。つまり、想定したクローンの製造方法では、評価結果として試算された資金C_Mと時間C_T以下でクローンを製造することが困難である

ことを確認するというものである。このとき、C_M と C_T が現実的なケースであれば、それ以下で製造困難であることの確認も現実的であるが、C_M と C_T が非常に大きい値として評価されたシステムについては、こうした方法によって評価の妥当性を確認することが困難となる。そのため、こうしたケースも含めて、本稿で提案した耐クローン性の評価アイデアの妥当性を確認する方法について検討が必要であろう。

(5) クローンを利用したその他の攻撃をどのように取扱うか

本稿では、田村・宇根［2007］で整理されている 5 つの攻撃のうち、ブルート・フォース攻撃とシミュレート攻撃を検討の対象外とした。ただし、ブルート・フォース攻撃は能力の低い攻撃者であっても実行可能な攻撃であることから、そうした攻撃者までも想定するアプリケーションにおいては同攻撃に対する耐クローン性評価も必要となる。また、シミュレート攻撃は、リプレイ攻撃に必要な行為に加えて、入手した CRP から未知のチャレンジに対するレスポンスを推測するという行為が行われるが、クローンで再現を試みるレスポンスの数が非常に大きい場合等、シミュレート攻撃の方がより少ない資源で攻撃を実行可能なケースも考えられる。今後はこうした攻撃についても検討することが必要であろう[35]。

また、本稿で取り上げた 5 つの攻撃は、既存の研究事例を参考に整理したものであることから、クローンを利用した攻撃を網羅しているとは言い切れない。そのため、本稿で取り上げた 5 つの攻撃に対する耐クローン性評価の実施とともに、それ以外の攻撃の可能性についても検討を行うことが必要であろう。例えば、ウルフ攻撃についてはバイオメトリクスの分野において最近提案された攻撃であることから、バイオメトリクスをはじめとする関連分野の研究動向をフォローし、新しい攻撃法の提案等について状況を継続的に把握しておくことも重要であると考えられる。

(6) クローン製造に必要となるノウハウをどう取扱うか

本稿では、基本的に高度なセキュリティを達成するように設計された人工物メトリック・システムを検討の対象とし、想定する攻撃者については、クローン製造に利用可能と想定される加工技術をいくつか知っているとともに加工に関するノウハウや経験を有していることを仮定した。

[35]既存の研究事例では、これらの攻撃に対する検討は比較的多く行われている。例えば、Matsumoto *et al.*［2001］では、ブルート・フォース攻撃の成功確率を導出する方法について検討されているほか、Škorić and Tuyls［2007］では、シミュレート攻撃において未知のチャレンジに対するレスポンスを推測するうえで予め入手しておく必要がある CRP の個数に関する検討が行われている。

しかし、異なる種類の人工物メトリック・システムの評価結果を比較する際には、各システムで想定されるクローンの製造方法に、各分野独自のノウハウが必要になる場合も考えられる。こうした場合には、クローン製造に必要なノウハウを攻撃者の資源として位置付ける必要があり、どのように資金や時間として換算できるかについて検討が必要である。また、ノウハウの定量化が困難であるとすれば、ノウハウを持たない攻撃者とノウハウを有する攻撃者の差異を耐クローン性評価にどのように組み込むかについて検討が必要となろう。加工技術の分野では、これまで非公開であった加工技術に関するノウハウを見せる技術として取扱う方法について検討が行われており、ノウハウを形式化しデータベース化することによって誰もが参照できるようにするといったアイデアが示されていることから（日本機械工業連合会・製造科学技術センター［2008］）、こうした分野の動向についてもフォローしておくことが必要であろう。

7．おわりに

金融分野では、カードや紙等の人工物を利用した金融取引の安全性や信頼性を確保する手段として、各人工物の特性に応じた偽造防止技術を採用してきた。そうした偽造防止技術の１つである人工物メトリクスは、「偽造防止効果を低下させることなく技術内容を公開可能である」という特徴を有し、新たな具体的手法の提案だけでなく、耐クローン性等の観点からの定量的なセキュリティ評価も実施されるようになってきている。

本稿では、こうした既存の評価研究の事例を踏まえつつ、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方法のアイデアを提案し、今後の技術的な検討課題を示した。本稿で提案した評価方法は、さまざまな人工物メトリック・システムを横並びで評価することを目指しており、一定の前提条件のもとで攻撃者が人工物の偽造を試みた場合、どの程度の資金や時間が必要になるかを評価のベンチマークとしている点が特徴である。こうしたアイデアは、人工物メトリクス以外の偽造防止技術にも適用することができると考えられる。

今後は、本稿において説明した評価方法のアイデアの精緻化が検討課題となる。具体的には、人工物の偽造に用いられる加工技術をどのように選択するかといった点について検討する必要がある。また、実際にクローンを作製したうえで、評価結果として示される資金や時間との整合性を検証するなど、本評価方法のアイデアの妥当性や実現可能性についても検討することが求められる。

こうした今後の課題は、情報セキュリティの分野はもとより、印刷技術、光技術、電子工学等、認証に利用される人工物の種類によってさまざまな分野の知見を活用しながら検討を進めていくことが求められる。金融分野においては、関連分野の研究者や技術者と問題意識を共有しつつ、人工物メトリクスをはじめとする偽造防止技術のユーザとして、同技術の動向を今後もフォローしていくことが重要であろう。

参考文献

帯川利之、「MSTC 加工技術ロードマップ」、『第 1 回 2008 年精密工学会秋季大会シンポジウム講演資料』、2008 年

小柳修爾、『オプトロニクス光技術用語辞典第 3 版』、オプトロニクス社、2005 年

坂本千秋、「設計生産情報モデルの標準化－ CAD/CAM 用情報モデル－」、『標準化教育プログラム開発教材 個別技術分野編－機械』、日本規格協会、2007 年（http://www.jsa.or.jp/stdz/edu/bunya-2.asp）

情報通信研究機構（NICT）・情報処理推進機構（IPA）、『CRYPTREC Report 2006』、NICT・IPA、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』、電子情報通信学会、2007 年

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－」、『電子情報通信学会技術研究報告』ISEC2007-91、電子情報通信学会、2007 年、15〜22 頁

――――・――――、「IC カードを利用した本人認証システムにおけるセキュリティ対策技術とその検討課題」、『金融研究』第 26 巻別冊第 1 号、日本銀行金融研究所、2007 年、53〜100 頁

電子情報技術産業協会（JEITA）、『国際半導体技術ロードマップ 2007 年版（和訳）』、JEITA、2008 年

日本機械工業連合会・製造科学技術センター、『平成 19 年度次世代社会構造対応型製造技術の体系・統計調査報告書』、日本機械工業連合会、2008 年

――――・日鉄技術情報センター、『平成 19 年度新加工技術の動向についての調査研究報告書』、日本機械工業連合会、2008 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件の導出指針』、日本規格協会、2004 年

物質・材料研究機構、『ナノオーダーの超小型発光素子に道－シリコン微細加工技術と酸化亜鉛を応用してナノオーダーの発光アレイを実現－』、物質・材料研究機構、2003 年

前田光輝・平良允俊・山越 学・四方順司・松本 勉、「紙の赤外透過光を用いた人工物メトリクスの耐久性評価」、『2007 年暗号と情報セキュリティシンポジウム予稿集』、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 2 号、日本銀行金融研究所、2004 年、169〜186 頁

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

山形 豊・樋口俊郎・森田晋也・大森 整・牧野内昭武、「マイクロメカニカルファブリケーション技術と応用（第 2 報）」、『マイクロ加工研究会技術資料集』、マイクロ加工研究会、2007 年（http://www.micro.ne.jp/materials/sokeizai2a.html）

山越 学・田中純一・古家 眞・平林昌志・松本 勉、「人工物メトリクスによる紙の個別性の評価」、『情報処理学会研究報告』No.2007-CSEC-037、情報処理学会、2007 年、13〜18 頁

Beth, Thomas, and Yvo Desmedt, "Identification Tokens – Or: Solving the Chess Grandmaster Problem," *Proceedings of CRYPTO'90*, LNCS 537, Springer-Verlag, 1991, pp.169–176.

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.

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.

Cowburn, Russell, "Laser Surface Authentication – Natural Randomness as a Fingerprint for Document and Product Authentication", *Proceedings of Optical Document Security 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.

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.

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.

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

————, 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.

Menezes, Alfred J., Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applies Cryptography*, CRC Press, 2001.

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

Philips, *Philips Intrinsic ID*, http://www.research.philips.com /initiatives/intrinsic-id/index.html, 2008.

Shamir, Adi, and Eran Tromer, "Factoring Large Numbers with the TWIRL device, " *Proceedings of CRYPTO 2003*, LNCS 2729, Springer-Verlag, 2003, pp.1-26.

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: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, Springer-Verlag, 2007, pp.255-268.

————, and Pim Tuyls, "On the Amount of Entropy in PUFs," *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, Springer-Verlag, 2007, pp.195-215.

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.

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

Verayo, *Physical Unclonable Functions*, http://www.verayo.com/technology.html, 2008.