Computer Security Symposium 2017
23 - 25 October 2017

サイバーフィジカル時代の物理媒体による認証・識別に関する考察

加藤 大弥[1,a)]　林 達也[1]　砂原 秀樹[1]

概要：現在, 認証・識別において, 長い時間をかけて社会システムとして確立してきた物理媒体による認証や識別手法が, 電子化の普及により変革を迫られている点があり, パスワード認証の限界を始め, 例として, 指紋認証の初期時代におけるいわゆる「グミ指」と言われる攻撃手法や 3D プリンターによる「印鑑の危殆化」が喫緊の課題として挙げられる. これらは NIST SP800-63-3 における知識, 生体, 所有の典型例でもあり, 認証手法に関する社会的な転換を迫られている. そこで本論では所有による認証・識別に焦点をあて, 改ざん・複製の検証を行い, 実生活における人間の目視での認証と機械的なパターン認識での受容についての考察を行う.

キーワード：UWS, 認証, 偽造, 公共認証, CPS

A Stady of Authentication and Identification by Physical Medium in the Cyber Physical Systems

Daiya Kato[1,a)]　Tatsuya Hayashi[1]　Hideki Sunahara[1]

Abstract: Authentication and identification methods based on physical media established as a social system over a long period of time are being urged to change due to the spread of electronicization. As an example, an urgent issue is cited as an attack method called "Gummy Finger" in the early days of fingerprint authentication, and "Compromise of Seal" by 3D printers. These are typical examples of "Something You Know,Something You Are,Something You Have" in NIST SP 800 - 63 - 3, and they are being pressed for social transformation concerning authentication methods. In this paper we will focus on authentication and identification by ownership, verify tampering and replication, and consider the acceptance by human visual recognition and mechanical pattern recognition in real life.

Keywords: UWS, Authentication, Counterfeiting, Public Authentication, Cyber Physical System

1. はじめに

様々な電子機器の IoT 化が急速に進めらており, さまざまな危機感でのネットワークが形成され, モノ同士で多種多様な情報の通信が行われ始めている. 同様に, 昨今,CPS(Cyber Physical System:サイバーフィジカルシステム) という, あらゆるシステムがコンピューターにより制御されるようになり, 効率化とともに新たな価値の創造が行われ, 人間にとってよりよい社会が実現するために物理世界とサイバー世界を融合するという概念が提唱されている. この世界が実現することで, 実世界のあらゆる情報がインターネット上で利用することが可能になる.

これらの情報を利用する場合, 誰もが自由に利用することができる公な情報と, 自分や家族・組織・会社等の限定されたコミュニティでのみ公開する情報の差別化が必要になる. サイバー空間上では一般的に,User/Passwrod でのユーザー認証や証明書を利用した認証, 公開鍵を利用した認証使用されている. これらの認証は,1990 年初頭より運用

[1] 慶應義塾大学院メディアデザイン研究科
Keio University Graduate School of Media Design
[a)] i.mas.trunk@kmd.keio.ac.jp

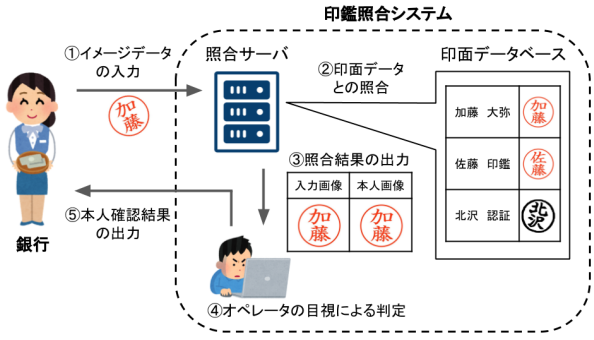

図 1 銀行における印鑑での認証の流れ

され始めてから, 様々な改善を繰り返すことで現在までの安全性を担保している. また, 日々新しい認証技術が開発され,Blockchain を用いた認証の開発やサービス運用の可用性の検証も行われ始めている [1].

しかし, 物理世界上においては日本を例に挙げるとサインと印鑑が大部分を占めている. 銀行においては, **図 1** で示すような, 画像解析を行って適合率を算出する方法 [2] とディスプレイに登録された印鑑画像が表示され, 銀行員が目視で判断する方法を組み合わせる手法が多く用いられている. 前者の方法に関しては, 塩野らのパラーメータ平面を用いた印鑑画像の認識 [3] に挙げられるように,1990 年初頭から用いられている手法であり, 田中らの印影画像のテンプレートマッチングによる同種の印章に関するの研究 [4] のような, 印鑑画像の識別制度を向上させる研究が行われているが, 基本的な画像を用いた認証方法そのものは長期間変化していない. 後者に関しても同様であり, 人間の経験と判断力を利用した画像認識であり, 認証強度に関してはオペレータに完全に依存する. このことから, 地面師を代表するような印鑑の偽造によるなりすましと認証が可能であるという問題が発生している. また近年,3D プリンターの一般化やカメラ・画像処理ソフトの向上から職人技であった偽造から大衆的に誰もが印鑑を代表する認証の物理媒体を偽造することが可能になると考えられている.

そこで, 本研究では印鑑を主とした認証に使用される物理媒体の偽造をもとに, 様々なソフトウェアと 3D プリンターを用いた偽造の可用性を制作時間, 値段, 難易度等で検証を行う.

2. 物理媒体での認証と問題点

2.1 物理媒体での認証の現状

物理世界における物理媒体を利用した認証の現状の調査を行った. 調査の方法としては,2017 年に NIST が発行した SP800-63-3Digital Identity Guidelines[5] をもとに評価するものとした. 本ガイドラインは連邦政府機関における電子認証を実装する際の技術的な指針を提供するものである. その中から評価の軸として, トークン (物理媒体) の要素・検証者による所有の証明 (PoP)・攻撃者によるトークンの脅威を参照し調査・評価を行った.

表 1 物理世界でのサービスと認証

	サービス	物理媒体	併用される認証
銀行窓口	口座振替	印鑑	—
銀行窓口	手形	印鑑	自署 or 記名捺印
大学窓口	勤務表	印鑑	自署
スマートフォン	本人確認	指紋	—
銀行 ATM	出金	通帳 or IC チップ	4 桁 PIN コード

調査した物理世界でサービスを使用する際の認証例を場所, サービス, 物理媒体の種類, 併用される認証について **表 1** に示す.

基本的な認証の運用方針としては,SP800-63-3 より, 知っていること (パスワード等), 持っているもの (身分証明書など), 持っている特徴 (生体情報など) の 3 つが基本要素となっており, これらの要素の組み合わせによって認証の強度が定められ, 適切なサービスを提供している.

表 1 より, 銀行 ATM においては, 通帳及びキャッシュカードとパスワードという組み合わせにおいて運用がなされている. これは, 本人しか持ち得ないキャッシュカードと知り得ないパスワードを込みあわせることで認証強度を担保している.

銀行窓口でのサービスに関しては, 印鑑という本人しか持ち得ない物理媒体を利用し, 人間が最終的な判断を行うことで金銭のやり取りを行っている. 印鑑を利用した認証では, 銀行だけではなく産業機関や教育機関を含む様々な機関においても同様の手法でサービスを提供している.

2.2 認証におけるユーザビリティ

これらの認証が多く使用されている理由としては, ユーザビリティに大きく関係している. 前項でも上げたように銀行を例に取ると, 銀行での取引においてユーザー名とパスワードを要求された場合, 認証強度としては貧弱であるため, パスワード長を 16 文字以上にしなければならないとなった場合ユーザーへの記憶の負担が大きくユーザビリティが損なわれてしまう. また, 認証強度に関してもユーザーの記憶力に影響してしまい, その結果としてメモを取るといった行動から様々なインシデントが発生する恐れがあるため, ユーザビリティの確保と認証強度のバランスを取ることが難しい.

その点, 詳細は後述するが, 物理媒体を用いた認証においては偽造が困難であるといった点からそれ単体の認証強度が非常に高いとされていた. また, このトークンは本人のみが用いている所有という面でも個人を特定するのものとしての役割も兼ね備えているため, 単体での認証を用いるサービスを幅広く利用することが可能な非常に有益なものである. ユーザビリティの面から見ても, 印鑑に関しては押印を行うだけという非常に容易なに印象であり, すべてのユーザーが同様の認証強度を保持することが可能である.

このように一定の信頼のもとに成り立っている物理媒体での認証は非常に柔軟でユーザビリティに優れており, 現代の社会生活においても重要な役割を担っている.

2.3 トークンへの攻撃の可能性

このような印鑑やキャッシュカードのような物理媒体の認証強度が担保される理由としては, これらのトークンの偽造が困難である, もしくは, ハードトークンに多要素な暗号鍵を保持しており再現することが困難であるということにある. 印鑑を例に挙げると, 判子職人が手彫りで判子を１つ１つ製造するため, 同じ犯行は世界に１つとないという信頼のもとで印鑑の認証強度は担保されている. この印鑑における認証強度の信頼は表 1 から見てもわかる通り, 日本における銀行窓口での口座振替を見てもわかる通りであり, 印鑑だけでの金銭のやりとりを可能にしている.

この体制から印鑑を偽造し, 銀行から不正にお金を引き出す行為は古くから行われている. 例として, 不動産登記の偽装がある. これは, 不動産登記を第三者が何かしらの方法で印面を取得・偽造し, 土地の権利を取引するものである. これにより, 第三者は不正に多額の金額を手に入れることが可能でとなる.. 近年では積水ハウスが 8 月 2 日に発表した分譲マンション用地の購入に関する取引事故につきまして[*1]にあるように,63 億円を第三者に横領される事件が発生した. これは地面師とよばれる詐欺グループが登記, 身分証明書, 印鑑を偽造し土地の権利者になりすまし不動産料をだまし取るものである.

またこのような個人, 企業から金銭をだまし取るようなプロフェッショナルによる印鑑の偽装だけではなく, 金銭目的以外にも中学教諭による教頭の印鑑を偽造した嫌がらせや, 韓国では相手の印鑑を偽造して婚姻を出すといった, 技術を持ち合わせていない一般の人々による印鑑の偽造において様々な機関や人間の目による認証をすり抜ける事件も発生している.

このような一般の人々による印鑑の偽造が増加している一例として,3D プリンターの普及が挙げられる.3D プリンターはモデルデータからエンジニアリングプラスチックや液体樹脂を利用し三次元造形を行うものである. 基本特許が 2009 年に失効したことによりオープンソース化が進んだことで, 価格の低下と造形精度の上昇が急速に普及が進んでいる急速に普及が進んでいる. また, 造形代行サービスも数多く存在し, 一定の料金を支払うことで約 2 週間で造形物を手に入れることができる. このように誰もが偽造を行うことが可能にな環境になりつつあり, 印鑑のような伝統的なトークンの強度は今日も著しく低下していると考えられる.

[*1] 積水ハウス HP -ニュースリリース 8 月 2 日 分譲マンション用地の購入に関する取引事故につきまして:https://www.sekisuihouse.co.jp/company/topics/datail/__icsFiles/afieldfile/2017/08/02/20170802.pdf

2.4 日本における攻撃対策と問題

物理世界でのトークンの偽造に関しての対策を印鑑を例に挙げる. 近年までの日本において印鑑の偽造は,1. 印面の入手, 2. 印面のスキャン, 3. 印鑑を彫るが基本的な流れであった. 銀行においてこれまで通帳の先頭ページにあった印面の表示を廃止するといった点である. また, 印面の偽造を困難にするために銀行印と呼ばれるような複雑な印面をプロフェッショナルが作成するということ対策が行われている. このことから考察できることとしては印鑑においては, 元データ (印面) の入手を困難にする, 入手された場合においては偽造が困難な複雑な印面にする, もしくは偽造を行うのに長い時間を要するといった、再現性を低くする・時間による制約による対策を取っていることがわかる.

法律に関しては, 刑法 164-168 条において印章偽造の罪として規定されている. これは, 文書偽造罪や有価証券偽造罪の予備や未遂的な行為を処罰するものであり, 基本的な内容としては, 行使の目的で印章を偽造した場合に罪に問われるといったものである. これらの対策においては, 前項でも述べたとおり, 複雑な印面においても特異な技能を持たない人々が短時間で正確に造形することができるため対策が適切ではなくなってきていることが考察できる.

3. 物理認証媒体の偽造と検証実験

前章までの調査と考察から, 本研究では技術を持たない一般の人における印鑑偽造の可能性の調査と考察を実際に印鑑を造形することで検証を行った. なお本実験においては, 制作した印鑑のデータの漏洩と第三者からの利用に細心の注意を払い, 偽造する印鑑に関しては一般的に販売されている安価な印鑑を利用するものとし, 印面の漏洩による被害を出さないための状況下で実験を行うものとした.

3.1 実験機器とソフトウェア

今回の実験では 2 種類の現在販売されている 3D プリンタと様々なソフトウェアを用いた. 詳細を**表 2** に示す.3D プリンタは**表 3** で示すとおりそれぞれ価格・造形方式・材料等の違いのものを使用した. 使用するモデルに関しては stl ファイルとして出力した同様の印鑑を造形する. 印面を取得する際には, 一般の人における偽造の可能性を検証するためスマートフォンのカメラとアプリストアからダウンロードすることが可能なソフトウェアを使用することとした. 本実験に用いた 3D プリンタは購入済みの大学備品を使用した. スマートフォンとノートパソコンに関しては著者が普段使用しているものを使用し,Adobe CC に関しては学生割引のコンプリートパックを購入した.

表 2　本実験で利用した機材・ソフトウェア

製品名	価格	詳細
Replicator 2X	2,499$	3D プリンタ
Objet260 Connex3	21,000,000 円	3D プリンタ
thinkpad X220	25,000 円	Windows10,Intel Core i5
Galaxy S5	70,000 円	Android スマートフォン
Adobe Capture	—	Android アプリ
Adobe Illustrator CC	1,980 円/月	デスクトップアプリ
123D Design	—	デスクトップアプリ

表 3　3D プリンタの性能の比較

	Replicator 2X	Objet260 Connex3
価格	2,499$	21,000,000 円
材料	PLA 樹脂	UV 硬化アクリル系樹脂
印刷方式	熱溶解積層	積層インクジェット
造形解像度	粗	精

3.2　印鑑における偽造の手法

今回の実験では以下の順序で印鑑の偽造を行った.

- 紙面に押印された印面を Adobe Capture で撮影
- 目視で確認しながら印面データを作成
- Adobe Illustrator CC で印面データのパスを作成
- 123D Design で印面データの 3D モデルを作成
- 3D プリンタで造形し, 印面のヤスリがけ等の微調整

本研究は特異な技術力を保持していない一般の人による偽造の可能性を検証するため, 特殊で高価なソフトウェアを使用せずプログラミングや彫刻を行わないような手法を用いた.

3.3　造形した印鑑の評価手法

今回の評価軸と手法に関しては, 銀行における認証を参考にした際の印面の造形精度・人間の目による判別を検証するだけではなく, 先にも述べたように偽造にかかる時間・費用を評価することで一般の人が偽造を行う可能性の検証を行った. 印面の比較に関しては, 実際に近い方式を参考にし, 本物の印面画像と偽造した印面画像を目視で比較・画像の重ね合わせによる確認を行うことで評価を行った. また, 本実験で実際に使用した実験機材やソフトウェアだけではなく, 現在さまざな企業が提供しているサービスを利用した際の同様の評価を行う.

4.　実験結果および考察

4.1　印面の撮影とデータ化

本実験では一般的に売られているシャチハタ 11mm の村上を用いて, シャチハタで押印した資料から印面データを取得するという手法を用いた. まず, 用意したスマートフォンに Adobe Capture のインストールを行う。Adobe Captuer は Adobe が無料で公開しているトレースアプリであり, 本来の使用用途としては, スマートフォンのカメラ機能を使用することで簡単に写真や絵のトレース・色の抽出・ベクター化を行うためのツールである. このアプリケーションを利用することで印面を真上から垂直に撮影し, 印面のベクターデータを作成した. 図 1 に示した図は, 左から Adobe Capture で印面を撮影している様子である. このように周辺の明るさや影にあまり影響なく簡単に中央図のようなトレースを撮影することが可能である. 最後に印面以外のシェイプやゴミを消しゴム機能で削除することで, 右図のような印面データを作成することができる. このデータは Adobe CC に有料登録することで png のようなラスタ形式の他にも svg のようなベクタ形式での出力が可能になっている. 今回は印面の大きさを調整する必要があるため, ベクタ形式での出力を行った.

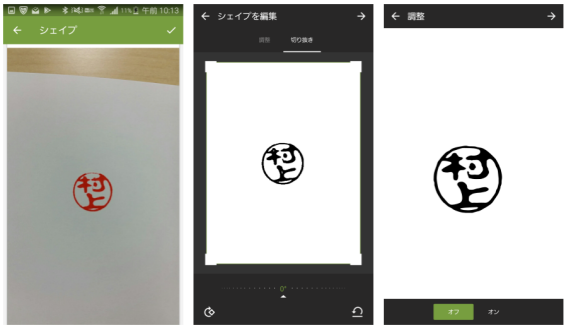

図 2　Adobe Capture を用いた印面データの取得

4.2　3D モデルの作成

次に印面のベクタから印鑑の 3D モデルを作成する. まず, **図 3** の左図のように印面のベクタデータ Adobe Illustrator CC で取り込み, 印面をトレースし印面のパスを作成する. これにより印面部分のみのベクタデータを作成することが可能である. また, ここで印面の大きさの微調整を行い印面データが完成する.

次に, 作成した印面データを 123D Design に取り込む.123D Design は Autodesk が無償で公開していた 3D CAD ツールである.2017 年 3 月に配布が終了されたため, 代替として Tinkercad や Fusion 360 を用いることが望ましい. まず, 作成した印面データを取り込むと平面上の印面が表示される. ここから印面を選択肢し, エッジの押出しを行うことで印面を図 3 の右図のように上方向へ筒状に伸ばすことが可能であり, 簡単に印面から印鑑モデルを作成することに成功する. 完成した 3D データは基本的な拡張子であり, 様々な 3D プリンタで使用することができる stl 形式で保存する.

4.3　印鑑の造形

前項まで作成した 3D モデルを実際に 3D プリンタで出力する. 今回使用した 3D プリンタは印鑑の比較を行うために表 3 で示した 2 種類のものを使用する. まず,Replicator 2X での造形に関して, このプリンタはフィラメント樹脂を

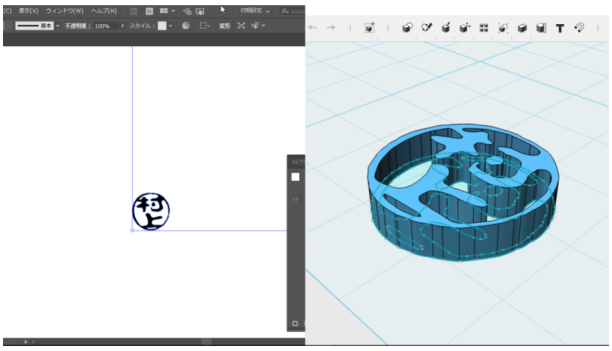

図 3 左:Adobe Illustrator CC を用いた印面データの作成
右:123D Design を用いた 3D モデルの作成

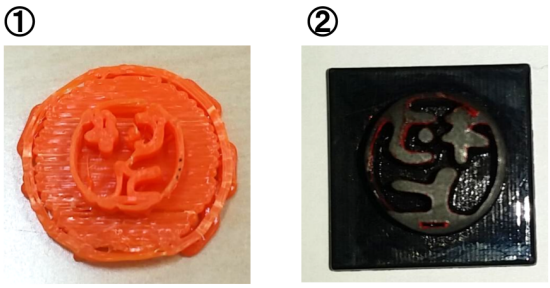

図 4 左:Replicator 2X 右:Objet260 Connex3

高温で熱することで溶かし積層していくことでモデルを造形する. 価格としては比較的安価であるが細かい造形を行うことができない.Objet260 Connex3 では光硬化樹脂をインクジェットで印刷し積層していくことでモデルを造形する. こちらは非常に高価であるが, とても細かい造形が可能であり 3D モデルデータとほぼ同様の造形を行うことが可能である. それぞれには専用の造形用アプリケーションが用意されており,stl 形式の取り込みが極めて用意になっている.3D モデルの配置や造形方法・サポートの造形に関してはそれぞれのアプリケーションにおいて, ボタンをクリックするだけで自動で行うことができるため特殊な知識を持っていなくとも使用することが可能である. 造形された印鑑は**図 4** であり, 左図が Replicator 2X, 右図が Objet260 Connex3 となっている. 詳しい造形の評価・印面の比較に関しては後述する.

ここまでの一連の作業を行うことで, 比較的容易に押印された印面から印鑑を偽造することが可能である.

4.4 印面の比較

今回偽造した印鑑の比較を行う. まず, 造形の完成度に関しては図 4 から確認できる通り, 安価なフィラメント樹脂による造形では極端に精度が低いことがわかる. 印面には凹凸が多く見られ, 村の部分においては木と中心の点がうまく造形されていないことがわかる. これは印面の大きさが 11mm と小さくフィラメントの太さが約 1mm もあるこ

図 5 押印された印面と偽造した印面の重ね合わせによる比較

とに起因していると考えられ, この偽造した判子においては押印する必要もなく実用不可能であると評価した.

一方, 光硬化樹脂を使用した場合においては, 印面が滑らかであり, 文字の丸みや点・はらいなどが正確に造形されていることが確認できる. また印面の外枠部分に関しても左下の一部がかけているものの非常に細かく造形されている. この印鑑に関しては, 造形された印面の段階において目視でも一般的に売られている印鑑と変わらないものであると評価した. 次に, **図 5** は実際に紙面に押印した本物の印面と Objet260 Connex3(図 4 右) で造形した印鑑による押印した印面を比較したものである. 図 5 左は, 左側の印面が偽造した印鑑, 右側の印面が本物の印鑑による押印である. 偽造した印鑑に関しては右側の欠けや朱肉の染み込み具合の違いがあるものの, 高精度で印面が偽造されていることがわかる. 図 5 右は印面データを重ね合わせたものである. この手法は実際の公共機関における目視による印鑑照合に使用される方式の一つである. 結果として, 重ね合わされた印面がほぼ一致していることが目視でわかり, 照合を行うオペレーターによっては適合していると判断する可能性が十分あるレベルでの銀像が行われたと考察できる.

このことから 3D プリンタの性能次第では印鑑の特異な技術を持たない一般の人による偽造が十分可能であると評価した.

4.5 偽造に要した時間

本実験手順における印鑑の偽造にかかった時間を**表 4** に示す. 今回の手順において著者が所要した時間は合計で 1 時間 35 分であり, このことから印鑑の偽造に対して長い時間を要する物理媒体であるといった認証強度がほぼ無意味であるということが考察できる. それぞれの内訳の中で一番時間を要したのは 3D プリンタによる造形であった. その他の作業に関しては印面データではカメラをつかった撮影を行うため明るさなどの調整,3D モデルの作成に関しては,Adobe Illustrator CC や 123D Design の使い方の模索に時間を要した. また, すべての作業において約 15-25 分程度の短い時間での作業から全体的な作業難易度は低く, ある程度の PC 操作能力があれば多くのユーザーが偽造可能

表 4 各手順における所要時間と内訳

	所要時間	内訳
印面の取得	15 分	印面の撮影とデータ化:15 分
3D モデルの作成	25 分	印面のパス化:10 分
		3D モデルの作成:15 分
3D プリンタでの造形	40 分	モデルの配置:10 分
		造形時間:30 分
合計	1 時間 35 分	

であると評価した.

4.6 外部サービスによる印鑑偽造の考察

本実験で偽造を行うために一番重要な点としては 3D プリンタを保有しているか否かというところである. 今回偽造に対して有効であると評価した 3D プリンターは表 3 からもわかるとおり約 2000 万円であり, 一般の人々が気軽に購入することができる金額ではないことがわかる.

しかし, 近年 3D モデルを提出し一定の金額を支払うことで,3D プリントを代行するサービスが台頭し始めている. 日本では DMM.make が代表的である. 他にも国内では rinkak, 海外では shapeways などが存在しており, 価格に関しては使用する材料とモデルの大きさによって料金を見積もるといったサービスになっている. これらのサービスは支払いから約 4-12 日程度の比較的短い期間で造形・発送を行っている. これを利用することで, 一般の人々でも 3D モデルを作成する手順までを行うことで印鑑を偽造することが可能であると言える.

DMM.make を例に詳細を考察する.DMM.make では国内の 3D プリントサービスの中でも比較的安価で様々なモデル材から造形することが可能になっている.DMM.make[*2]では, 材料費＋空間費＋諸経費が造形にかかる費用になっており, 造形の細かさ・材料の質によって様々な 3D プリンタを選ぼことが可能になっている. この中から今回使用した 3D プリンタと同程度もしくはそれ以上の製品で造形した場合の金額を示す. 本実験で造形した印鑑は $10cm^3$ の材料を使用している. まず, アクリル (Ultra Mode) を利用した場合,2500+100+1799=4399 円となる. また, さらに造形が細かいアクリル (Xtreme Mode) においては,5000+250+1799=7049 円で造形を行うことができる. この金額は 3D プリンタを購入するよりも遥かに安易であり, 金額自体も 1 万円以下と比較的安価に印鑑を偽造することができる可能であることがわかり, これらはユーザーの増加につれて今後更に安価になると考えられ, 一般の人々においても手軽に偽造を行い易い環境になっていくと考えられる.

4.7 偽造した印鑑のユーザビリティ

今回偽造した印鑑に関しては,UV 硬化アクリル系樹脂造形しているため硬度に関しては繰り返し使うことが可能であり, 造形方法によっては実際の象牙や石よりも硬度を担保することも可能である. 使用感においては通常の印鑑と全く遜色はなく, 印鑑の胴体部分を大きくし持ちやすくすることさえ可能である.

造形された印鑑をサービスを利用する際に提出しなければならない場合においても, 様々な素材・色・大きさで造形が可能であるため, 外観としての偽造も十分に可能である. また, 押印のみが必要な場合においても,3D プリンタによる造形は非常に柔軟であり, 本実験のように印面のみを造形し胴体に取り付けるアタッチメント方式を取ることが可能である, 利便性だけで言えば通常の印鑑のようにかさばることもなく. 非常に扱いやすいものを造形することが可能である.

以上から, ユーザビリティの点においては実際の印鑑と同様の性能を担保しており, 自由度の高い造形からユーザビリティを更に向上できるものであるといえる.

5. 印鑑を用いた認証の対策案

今回のように印鑑は比較的容易に偽造ができ, 目視による認証においても誤って許可してしまう可能性が十分にあると考えられる. このように印鑑の偽造における対策例を考察すると, 現在の印鑑の仕組みにおいは偽造を防止をすることは困難であると考える. そこで解決策としては 2 パターンが考えられる. 1 つめは,SP800-63-3 に述べられているように多要素化し, 従来の印鑑の保有と指紋等の持っているものと持っている特徴を組み合わせるという方法がある. これにより認証強度のレベルを上げると同時にユーザビリティを損なわない認証が実現できると考察できる. もう一つは, トークンを完全に置き換えるという方式である. 印鑑のような偽造可能な物理媒体からマイナンバーカードやデジタル証明書や秘密鍵を保持する USB や IC トークンを用いることで偽造そのものを困難にする. この方式は単一の認証であり印鑑を直接的に代替するトークンであるため, デジタル技術に親しみのない年配者にも受け入れやすいかたちであると考える.

6. 結論

本研究では, サイバーフィジカルの到来に向けて, 物理世界とサイバー世界においての認証にあり方について物理世界で用いられている物理媒体を用いた認証の現状についての調査と評価を NIST SP800-63-3 を用いて行った. その結果として, 印鑑の認証強度が近年, 危殆化してきていることが考察できた. また, 日本における印鑑の信頼が非常に高く銀行においては印鑑のみで口座振替や手形の換金を行うことが可能であり, これらを象徴するように企業では数十億円規模の詐欺が発生している現状がある. このことから, 物理媒体の偽造における攻撃を日本において信頼されてい

[*2] DMM.make HP:http://make.dmm.com/print/material/#2

る印鑑に着目し, 実際に偽造を行うことで特異な技能を保持していない一般の人々からの攻撃の可能性を偽造の難易度・所要時間・金額の面から調査・考察を行った.

印鑑の偽造については古くから用いられている印面を彫ることで偽造するといった特殊な技能を有するものでは無く, 現在, 一般的に普及し始めてきている 3D プリンタを使用し, 印面データの取得や 3D モデルの作成においても一般的に広く使用されているソフトウェアも用いて実験を行った. このことから, 特殊な技能を持たない人が印鑑の偽造を 2 時間以内で行うことができ,3D プリンタの性能如何で印鑑偽造が十分に可能であると評価した.

しかし, 高精度の 3D プリンタは非常に高価であることから 3D プリンタによる偽造可能性は低いように思える. そこで, 現在急速に普及が進んでいる 3D プリントサービスを用いる場合を調査したところ, 印鑑ひとつあたりを 5000 円程度で作成することが可能であることが調査から判明した.

これらを対策するためには印鑑の偽造は避けられないため, 印鑑の他にバイオメトリクスを使用した多要素認証を用いるか印鑑そのものを偽造しにくいデジタル証明書や秘密鍵を保有している別のトークンに置き換える方法を提案した.

以上のことから, 印鑑の偽造には特殊な技能と道具を用いること無く, 使用するソフトウェアや 3D プリンタによっては 1 万円程度で偽造することが可能であり, その精度は実際のさまざまなサービスや組織での認証において十分使用できる可能性があると評価した.

参考文献

[1] Kishigami, Junichi, et al. "The blockchain-based digital content distribution system." Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on. IEEE, 2015.

[2] 高橋知敦:印鑑照合システム 金融機関における導入事例, 沖テクニカルレビュー 2003 年 1 月／第 193 号 Vol.70 No.1.

[3] 塩野充, 小高秀徳, 佐藤正宏：パラメータ平面を用いた印鑑画像の認識, 岡山理科大学紀要. A, 自然科学 29(1993).

[4] 田中昭二, 上田道夫, 紙谷卓之:印影画像のテンプレートマッチングによる同種の印章に関する研究―ゴム印および樹脂印を使用した実験―, 日本法科学技術学会誌 18.2 (2013).

[5] NIST:SP800-63-3 Digital Identity Guidelines (2017)