視覚的形式知を利用した3DCG画像CAPTCHAの研究

静岡大学博士論文

視覚的形式知を利用した3DCG 画像 CAPTCHA の研究

藤 田 真 浩

大学院自然科学系教育部

情報科学専攻

2017 年 12 月

論文要旨

CAPTCHA（Completely Automated Public Turing test to tell Computers and Humans Apart）は，人間には正解容易であるが，機械には正解困難である問題をユーザへ出題し，正解できたユーザを人間，正解できなかったユーザを機械だと判定するセキュリティ技術である．現在，多くの Web サービス提供サイトにおいては，文字列判読型の CAPTCHA，動物画像の判別を用いた Asirra，3 次元の同一物体の認識を用いた YUNiTi CAPTCHA といった，素材の姿形全体に関わる「視覚的形式知」を利用した CAPTCHA が広く採用されている．しかし，これら CAPTCHA は，マルウェアによって破ることが可能であると指摘されている．これら CAPTCHA に代わる，機械がより正解困難，かつ，人間に正解容易な CAPTCHA が必要とされている．ただし，CAPTCHA には，人間が正解容易，機械が正解困難であると同時に，「問題の自動生成が容易である」という要求も存在する．

以上の背景より，機械に正解困難，人間に正解容易，かつ，問題の自動生成が容易な，視覚的形式知を利用した新たな CAPTCHA を追求することが本論文の目的である．はじめに，現在までに提案されている視覚的形式知を利用した CAPTCHA とその問題点を指摘する．そのうえで，現在までに提案されている視覚的形式知を利用した CAPTCHA は，「文字列を素材とした形式」「2 次元画像を素材とした形式」「3 次元モデル（3D モデル）を素材とした形式（3DCG 画像 CAPTCHA）」のように，素材のモダリティによって 3 つの分類が可能であり，それぞれの基本形態は，文字列判読型 CAPTCHA，Asirra，YUNiTi CAPTCHA であることを説明する．その後，各基本形態を発展させていく指針として「より精確な視覚的形式知を利用する」「視覚的形式知からの逸脱を利用する」という 2 つの指針があることを示す．

本論文では，加工が容易である，利用できる次元数が多いといった，3D モデルのメリットに着眼し， 3DCG 画像 CAPTCHA に注目する．3DCG 画像 CAPTCHA を「より精確な視覚的形式知を利用する」「視覚的形式知からの逸脱を利用する」という 2 つの指針でそれぞれ発展させる．3DCG 画像 CAPTCHA の基本形態は，前述のとおり，YUNiTi CAPTCHA である． 3D モデルの姿形全体に関わる視覚的形式知が利用されている．しかし， YUNiTi CAPTCHA は，類似画像選択攻撃や 3D モデル認識攻撃によって突破される恐れがある．

この課題を解決する 3DCG 画像 CAPTCHA として，より精確な視覚的形式知を利用した「Sketcha」が既に提案されている．Sketcha では，単にモデルの姿形全体だけでなく，そのモデルの「上方向」という知識も利用されている．しかし，すべての 3D モデ

ルに対して「どちらが上か」という情報を付与しなければならないため，問題の自動生成に関して課題があった．さらに，90 度回転であるため，1 問あたりの総当たり数が非常に小さい（4 通り）という課題があった．

また，視覚的形式知からの逸脱を利用した 3DCG 画像 CAPTCHA については，筆者が知る限り，現在まで提案がなされていない．視覚的形式知からの逸脱を認識するためには，その CAPTCHA で利用されている（姿形に関わる）視覚的形式知のすべてを獲得する必要があるため，より精確な視覚的形式知を利用した形式より難しい CAPTCHA を実現できるはずである．すなわち，視覚的形式知からの逸脱を利用した 3DCG 画像 CAPTCHA を提案・追求することは，機械の進化に対抗するために非常に重要な研究課題であると考えられる．

そこで，人間に正解容易，機械に正解困難，かつ，問題の自動生成が容易な 3DCG 画像 CAPTCHA を追求するために，上記の課題を解決する二つの CAPTCHA を提案する．

① より精確な視覚的形式知を利用した 3DCG 画像 CAPTCHA「Locimetric 型 YUNiTi CAPTCHA」
Locimetric 型（単一の 3D モデルの中の特定部位を選択する方式）の出題形式を採用した形式である．「モデルの姿形全体」に関する視覚的形式知だけでなく，「モデルの部位」というより精確な視覚的形式知を利用した方式である．

② 視覚的形式知からの逸脱を利用した 3DCG 画像 CAPTCHA「非現実画像 CAPTCHA」
3D モデルデータベースから任意に選んだ 2 体の 3D モデルをめり込み合わせることで，人間が今まで「見たことがないであろう（視覚的形式知から逸脱した）形状の」非現実モデルを生成する．そして，複数の通常の 3D モデルの中に，一体の非現実モデルを配置した一枚の画像を CAPTCHA 画像として出題する．画像中の非現実モデルを選択できたユーザを人間として判定する．

これら提案した CAPTCHA が，既存の CAPTCHA と比較して，人間に正解容易，機械に正解困難，かつ，問題の自動生成が容易であることを示す．さらに，以上 2 つの方式を提案・実装・評価した後，2 方式を統括した議論を行う．本議論を通じて，「提案方式の更なる安全性評価手法」「実用化に向けた課題」等を明らかにする．

目次

図一覧

表一覧

第1章　序論

1.1　本研究の背景と目的

自動プログラム（マルウェア）によって，メールアカウントの不正取得，ブログや掲示板へのスパムコメント書き込み[1]，パスワードリスト攻撃[2][3]といった Web サービス提供サイトに対する不正行為が定常的に行われている．このような不正を防ぐためには，マルウェア（機械）による Web サービスの不正利用と，人間による正規のサービス利用とを識別する技術が必要不可欠である．この要求を実現する技術の一つである CAPTCHA（Completely Automated Public Turing test to tell Computers and Humans Apart，直訳：人間と機械を区別するためのチューリングテスト）[4]は，人間には正解容易であるが機械には正解困難である問題をユーザに出題することで，正解できたユーザを人間，正解できなかったユーザを機械だと判定する技術である．

現状，人間の知識をすべて有した機械は存在しない[11]．よって，人間が正解容易，かつ，機械が正解困難な CAPTCHA は，人間が有しているが，機械が有してない知識を利用することで実現可能である．ただし，人間が有する知識すべてを CAPTCHA に応用することは困難であり，かつ，CAPTCHA は多くの人間が解ける問題でなければならない．また，CAPTCHA としてコンピュータ上で「知識」を表現するためには，形式知（文章，図，数式などで表せる知識）である必要がある．そこで現実問題としては，できるかぎり多くの人間に共通している形式知の中で，可能な限り広範囲の形式知を利用することで CAPTCHA を実現することとなる．

現在，多くの Web サービス提供サイトにおいては，文字列判読型の CAPTCHA，動物画像の判別を用いた Asirra，3 次元の同一物体の認識を用いた YUNiTi CAPTCHA といった，素材の「姿形全体」に関わる視覚的形式知を利用した CAPTCHA がマルウェアの攻撃を防ぐ典型的な手法として広く採用されている．しかし，これらの CAPTCHA は OCR（Optical Character Reader，自動文字読取装置），機械学習，画像認識といった機能を備えたマルウェアによって破ることが可能であると指摘されている．これらの CAPTCHA に代わる，人間に正解容易，機械に正解困難である方式が必要とされている．

多くの研究者は前述の 3 種類の CAPTCHA いずれかにおいて，解く際に利用する知識の量を増やすことで，人間に正解容易，機械に正解困難な CAPTCHA を実現しようとしてきた．ただし， CAPTCHA には，人間が正解容易かつ，機械には正解困難（攻撃耐性が高い）という要求と同時に，「問題の自動生成が容易である」という要求も存在する．問題を無数に自動生成できない場合，問題の総数は有限となる．この結果，正攻法

では解けない問題であっても，機械（マルウェア）は，出題された問題をデータベースに蓄積し，過去に出題された問題を参照するという攻撃方法によって，問題を解くことが可能となる．しかし，そもそも CAPTCHA は，機械（マルウェア）には理解できない問題をその題材として用いるわけであるので，機械（CAPTCHA システム）がそれを認識して適切な問題を自動生成することは非常な困難な要求である．実際，研究者が提案してきた新たな CAPTCHA の多くは，攻撃耐性を重視するあまり問題の自動生成が困難となってしまっている，あるいは，自動生成の実現のために攻撃耐性の向上が不十分である，という課題を抱えている．

以上の背景から，本論文では，人間に正解容易，機械に正解困難，かつ，問題の自動生成が容易な，人間の視覚的形式知を利用した CAPTCHA を追求することが目的である．本論文では，はじめに，現在までに提案されている視覚的形式知を利用した CAPTCHA とその問題点を指摘する．そのうえで，現在までに提案されている視覚的形式知を利用した CAPTCHA は，「文字列を素材とした形式」，「2 次元画像を素材とした形式（2D 画像 CAPTCHA）」，「3 次元モデル（3D モデル）を素材とした形式（3DCG 画像 CAPTCHA）」といったように，素材のモダリティによって 3 種類の分類が可能であること，それぞれの基本形態は，前述の文字列判読型 CAPTCHA，Asirra，YUNiTi CAPTCHA であることを説明する．その後，各形式を発展させていく方法として「より精確な視覚的形式知を利用する」「視覚的形式知からの逸脱を利用する」という 2 つの指針があることを示す．

本論文では，前述した発展形式のうち，3DCG 画像 CAPTCHA の「より精確な視覚的形式知を利用する」「視覚的形式知からの逸脱を利用する」という指針に注目をして研究を進める． 3DCG 画像 CAPTCHA は，他の素材形式と比較して，1 次元分多くの情報が利用可能であり，素材の加工も容易である．3D モデルを組み合わせることで，場面や状況を生成することも可能である．さらに，将来的には，「動き」や「ポーズ」といった情報を利用することも可能となることが期待される．これらの点から，より多くの視覚的形式知を利用することが可能であると期待される．機械にとってより正解困難，かつ，自動生成容易な CAPTCHA を実現可能である可能性が高い．これらアドバンテージを有する一方，他の形式と比較して，十分に研究がなされていないという現状もある．

3DCG 画像 CAPTCHA の基本形態は，前述のとおり，YUNiTi CAPTCHA である．YUNiTi CAPTCHA は，3D モデルの姿形全体に関わる視覚的形式知を利用した CAPTCHA である．YUNiTi CAPTCHA は，出題画像に写されている 3D モデルと同一の 3D モデルを候補画像群の中から正しく選択できたユーザを人間として判別する．出題画像と候補画像では 3D モデルの向きが異なっており，囮モデルの中に含まれる正解モデルを選択する方式の出題形式となっている．出題画像と回答画像に同じ 3D モデルを違う角度で写すだけであるため，問題の自動生成も容易である．しかし， YUNiTi CAPTCHA のような形式の場合は，姿形の異なる複数のモデルの中に出題画像と同一のモデルが 1 体だけ混入する形態となっているため，「候補画像群の中から出題画像に最

も類似した画像を選択する」という単純な戦略（類似画像選択攻撃）によってマルウェアにも正解画像が求められてしまう危険性が存在する．また，画像認識技術が発展してきているため，各画像に写るモデルが何であるかを認識する戦略（3D モデル認識攻撃）によって突破される恐れもある．これらの攻撃は非常に単純ではあるものの，非常に効果的である．これら攻撃に対する耐性を高めるためには，正解モデルと類似した囮モデルを候補画像の中に多数混入することが重要である．しかし，類似したモデルの混入は，人間にも正答が非常に困難となってしまう．

この課題を解決した 3DCG 画像 CAPTCHA として，より精確な視覚的形式知を利用した「Sketcha」が現在までに提案されている[14]．Sketcha は，3D モデルを 2D 画像へ投影し，その 2D 画像に線画化と回転（0，90，180，270 度）を施した上でユーザに提示する．提示画像をユーザが 1 回クリックするごとに，2D 画像が 90 度回転し，画像を直立状態（0 度の回転）に戻すことができたユーザを正規ユーザとして判定する．すなわち，単にオブジェクトの姿形全体だけでなくそのモデルの「上方向」という知識も利用した形式である．1 枚の画像の上方向を回答する形式であるため，類似画像選択攻撃や 3D モデル認識攻撃では正解不可能な形式である．しかし，すべての 3D モデルに対して「どちらが上か」という情報を付与しなければならないため，問題の自動生成に関して課題があった．さらに，90 度回転であるため，1 問あたりの総当たり数が非常に小さい（4 通り）という課題があった．

また，視覚的形式知からの逸脱を利用した 3DCG 画像 CAPTCHA については，筆者が知る限り，現在までに提案がなされていない．視覚的形式知からの逸脱を認識するためには，その CAPTCHA で利用している姿形に関わる視覚的形式知すべてを知る必要があるため，より精確な知覚的形式知を利用する指針より，はるかに難しい CAPTCHA を実現できるはずである．すなわち，視覚的形式知の逸脱を利用した 3DCG 画像 CAPTCHA を提案・追求することは，機械の進化に対抗するために非常に重要な研究課題であると考えられる．

以上まとめるに，現状の視覚的形式知を利用した 3DCG 画像 CAPTCHA には YUNiTi CAPTCHA という基本形態が存在するが，YUNiTi CAPTCHA には，類似画像選択攻撃や 3D モデル認識攻撃に対する脆弱性が存在する．3DCG 画像 CAPTCHA を発展させる方向性としては，「より精確な視覚的形式知を利用する」「視覚的形式知からの逸脱を利用する」という二つの指針があるが，それぞれ次に示す課題が存在した．

① より精確な視覚的形式知を利用する発展形式の 3DCG 画像 CAPTCHA として，Sketcha が現在までに提案されている．しかし，1 問あたりの総当たり数が小さく，さらに，問題の自動生成のためにモデルに対して「上」という情報を付与する必要する必要があるため，攻撃耐性や自動生成の観点で不十分な方式である．

② 視覚的形式知からの逸脱を利用した発展形式の 3DCG 画像 CAPTCHA の実現は重

要な研究課題であるものの，現在までに具体的な方式が提案されてない．

そこで本論文では，人間に正解容易，機械に正解困難，かつ，問題の自動生成が容易な 3DCG 画像 CAPTCHA を達成するために，上記の課題①，②を解決する二つの CAPTCHA を提案・実装・評価する．本論文で提案する CAPTCHA は，以下の二つである．

① より精確な視覚的形式知を利用した 3DCG 画像 CAPTCHA：Locimetric 型 YUNiTi CAPTCHA（第 3 章）
Locimetric 型（単一の 3D モデルの中の特定部位を選択する方式）の出題形式を採用した形式である．モデルの姿形全体だけでなく，「モデルの部位」というより精確な視覚的形式知を利用することによって，YUNiTi CAPTCHA と比較して高い攻撃耐性（3D モデル認識攻撃や類似画像選択攻撃に耐性を有する）を有した方式である．その一方，人間にとっては正解容易であることをユーザビリティ実験によって検証する．さらに，1 つのモデルを違う方向から写した画像 2 枚を用意するだけであるため，問題の自動生成も容易である．

② 視覚的形式知からの逸脱を利用した 3DCG 画像 CAPTCHA:非現実画像 CAPTCHA（第 4 章）
3D モデルデータベースから任意に選んだ 2 体の 3D モデルをめり込み合わせることで「非現実モデル」を生成する．そして，複数の通常の 3D モデルの中に，一体の非現実モデルを配置した一枚の画像を CAPTCHA 画像として出題する．非現実モデルはユーザの視覚的形式知から逸脱した，見たことがないであろう姿形をしているため，人間であれば，そのモデルを発見することは容易である．一方，機械にとっては，重なった関係にある複数のモデルが，機械的に作られたもの（非現実モデル）であるか自然につくられたもの（遮蔽関係や自然なモデル）であるかを識別することが困難であるため，正解困難である．さらに，複数のモデルを平面上に並べ，そのうち 2 体を同じ座標に配置させるだけであるため，問題の自動生成も容易である．

1.2 本論文の構成

本論文の構成は次のとおりである．第 1 章では本研究の背景と目的を述べた．第 2 章では，CAPTCHA に関する説明と要件を再度述べた後，視覚的形式知を利用した CAPTCHA の基本形態と発展指針について説明をする．その後，3D モデルを素材とした CAPTCHA（3DCG 画像 CAPTCHA）に着目する理由と，既存の 3DCG 画像 CAPTCHA の課題を説明することで，本研究の位置づけを明確にする．その後，第 3

章では, より精確な視覚的形式知を利用した 3DCG 画像 CAPTCHA である「Locimetric 型 YUNiTi CAPTCHA」に関して提案・実装・評価する．第 4 章では，視覚的形式知からの逸脱を利用した 3DCG 画像 CAPTCHA である「非現実画像 CAPTCHA」について提案・実装・評価する．第 5 章で，両提案方式を踏まえて，今後の課題と展望について議論する．最後に，第 6 章で，本論文のまとめを述べる．

第2章　視覚的形式知を利用した CAPTCHA の既存研究と本研究の位置づけ

本章では，CAPTCHA と視覚的形式知を利用した CAPTCHA の基本形態（文字列判読型 CAPTCHA，Asirra，YUNiTi CAPTCHA）に関する説明を述べる．その後，それらを発展させた CAPTCHA とその問題点を指摘する．さらに，3D モデルを素材とした CAPTCHA に着目する理由と本研究で取り扱う課題を説明することで，本研究の位置づけを明確にする．

2.1　CAPTCHA と視覚的形式知の利用

自動プログラム（マルウェア）によって，メールアカウントの不正取得，ブログや掲示板へのスパムコメント書き込み[1]，パスワードリスト攻撃[2][3]といった Web サービス提供サイトに対するマルウェアの不正が定常的に行われている．このような不正を防ぐためには，マルウェア（機械）による Web サービスの不正利用と，人間による正規のサービス利用とを識別する技術が必要不可欠である．この要求を実現する技術の一つである CAPTCHA（Completely Automated Public Turing test to tell Computers and Humans Apart，直訳：人間と機械を区別するためのチューリングテスト）[4]は，人間には正解容易であるが機械には正解困難である問題をユーザに出題することで，正解できたユーザを人間，正解できなかったユーザを機械だと判定する技術である．

人間が正解容易，かつ，機械が正解困難な CAPTCHA を実現するためには，人間が有しているが，機械が有してない知識を利用することが必要である．現状，人間の知識をすべて有した機械は存在しない[11]．ただし，人間が有する知識すべてを CAPTCHA に応用することは困難であり，かつ，CAPTCHA は多くの人間が解ける問題でなければならない．また，CAPTCHA としてコンピュータ上で「知識」を表現するためには，形式知（文章，図，数式などで表せる知識）である必要がある．そこで現実問題としては，できるかぎり多くの人間に共通している形式知の中で，可能な限り広範囲の形式知を利用することで CAPTCHA を実現することとなる．

現在，多くの Web サービス提供サイトにおいては，文字列判読型の CAPTCHA，動物画像の判別を用いた Asirra，3 次元の同一物体の認識を用いた YUNiTi CAPTCHA といった，素材の姿形全体に関わる視覚的形式知を利用した CAPTCHA がマルウェアの攻撃を防ぐ典型的な手法として広く採用されている．

2.1.1　文字列を素材とした基本形態（文字列判読型 CAPTCHA）

文字列を素材とした視覚的形式知を利用した CAPTCHA（以下，文字列 CAPTCHA）の基本形態は，歪曲やノイズが付加された文字列画像を Web ページに表示し，閲覧者がその文字を判読できるか否かを試すものである（図 2-1）．ランダムな文字列を生成し，一定のノイズ（歪曲化や線画化など）を加えたうえでユーザにその文字列を提示する．人間であれば，文字列を構成する各文字の姿形を視覚的形式知として有しており，多少のノイズがかかったとしてもその文字列を認識することが可能である．この方式は，文字列判読型 CAPTCHA と呼ばれている．文字列判読型 CAPTCHA は，現在多くの Web サイトによって利用されている CAPTCHA である（たとえば，yahoo[5]や fc2 掲示板[6]）．

しかし，文字列判読型 CAPTCHA は，OCR（文字判読技術）を備えるマルウェアによって解読されることが報告されている[7][8]．文字列に加える変形やノイズを大きくすることによって，機械に解読困難とすることも可能であるが，大きく歪んだ文字列画像は人間にとっても解読困難となるため，人間の正解率を低下させてしまう[9][10]．

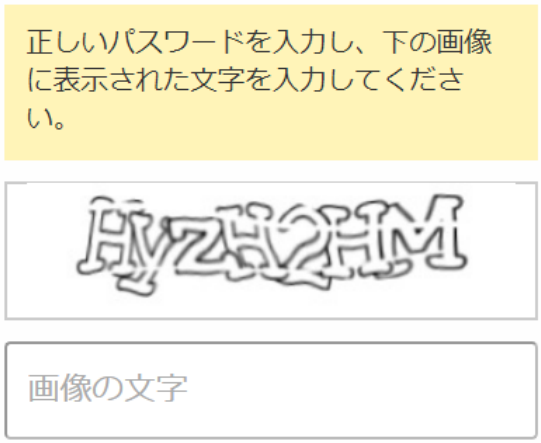

図 2-1　yahoo で利用されている文字列判読型 CAPTCHA の問題例．
表示されている文字列は「HyzH2HM」（yahoo のログイン画面[16]より引用）

2.1.2　2D 画像を素材とした基本形態（Asirra）

2D 画像を素材とした視覚的形式知を利用した CAPTCHA(以下, 2D 画像 CAPTCHA)の基本形態として，Asirra がある[22]．Asirra は，図 2-2 のとおり，犬，または，猫が写る複数の画像をユーザに提示する．ユーザは，その画像群の中から，猫の画像だけを選択することを求められる．すなわち，犬や猫の姿形という視覚的形式知を用いて回答する形式の CAPTCHA である．CAPTCHA で利用する画像は，犬や猫の里親募集サイト petfinder.com[21]から自動的に収集している．しかし，機械学習の発達によって，この程度の問題であれば，機械にも解読可能であることが知られている[23][24]．

図 2-2　Asirra の認証画面例（文献[22]より引用）

なお，Asirra の派生形として，識別する画像のカテゴリを増やした CAPTCHA も存在する．たとえば，SEMAGE[28]，Image Recognition CAPTCHA[29]，Confident CAPTCHA[30]などである．「（複数の画像の中から）特定のカテゴリの画像をすべて選択せよ」あるいは「この画像に写っているモノの名称を答えよ」といった出題形式を採っている CAPTCHA である．しかし，これら CAPTCHA も，Asirra のように，突破可能であるという報告がなされているものが多い．また，各カテゴリの画像を収集する必要がある点（各画像に対して，カテゴリ名のタグ付けが必要である点）で，問題の自動生成が困難である方式も多い．

2.1.3　3D モデルを素材とした基本形態（YUNiTi CAPTCHA）

3D モデルを素材とした視覚的形式知を利用した CAPTCHA（以下，3DCG 画像 CAPTCHA）の基本形態として，YUNiTi CAPTCHA[12][13]がある．YUNiTi CAPTCHA の認証画面例を図 2-3 に示す．YUNiTi CAPTCHA では，「候補画像群の中から出題画像と同じ 3D モデルが写された画像を選ぶ」というタスクが採用されている．人間は，問題画像の 3D モデルの姿形全体を見たとき，自身の視覚的形式知を利用することで，各画像に何のモデルが写されているかを把握することが可能である．さらに，人間であれば，そのモデルを頭の中で回転させながら，各候補画像と比較することで，出題画像と同じ 3D モデルが写る画像を選ぶタスクを容易に行うことが可能である．人間がこのように，頭の中でモデルを回転できる能力は，メンタルローテーションとも呼ばれる[33][34].

YUNiTi CAPTCHA では，3 問の出題画像が一度に提示され，それぞれのモデルが何であるかを 18 個の候補画像の中から正しく選択できたユーザを人間と判定する．出題

画像は毎回異なる視点から 3D モデルを写した画像となっている．候補画像群の撮影方向は不変であり，常に同一の候補画像群が表示される．出題画像と候補画像群には，それぞれ同じモデルを写すだけであるため，問題の自動生成が実現できている．

現在までに突破報告はないが，現在の画像認識技術の発達は著しい．YUNiTi CAPTCHA のような CAPTCHA の場合は，姿形の異なる複数のモデルの中に出題画像と同一のモデルが 1 体だけ混入する形態となっているため「候補画像群の中から出題画像に最も類似した画像を選択する」（類似画像選択攻撃）という単純な戦略によってマルウェアにも正解画像が求められてしまう危険がある．さらに，2D 画像 CATCHA の突破方法と同様な戦略を用いて，すなわち，各画像に写るモデルが何であるかを認識する（3D モデル認識攻撃）という戦略によって，機械にも認識される恐れがある．これら攻撃に対する耐性を高めるためには，正解モデルと類似した囮モデルを候補画像の中に多数含めておくことが重要である．しかし，YUNiTi CAPTCHA においては，類似したモデルの混入は人間の正答率の低下に直結してしまう．

図 2-3　YUNiTi CAPTCHA（YUNiTi.com[12]のアカウント登録画面より引用）

2.2　視覚的形式知を利用した CAPTCHA の発展

2.1 節に示したとおり，文字列判読型 CAPTCHA，Asirra，YUNiTi CAPTCHA には攻撃耐性の観点から課題が残っていた．そこで多くの研究者は，これらの CAPTCHA いずれかを改良することで，人間に正解容易，かつ，機械に正解困難な方式を模索してきた．

ただし，CAPTCHA には，人間が正解容易かつ，機械には正解困難（攻撃耐性が高い）という要求と同時に，「問題の自動生成が容易」であることも必要である．問題を無数に自動生成できない場合，問題の総数は有限となる．この結果，正攻法では解けない問題であっても，機械（マルウェア）は，出題された問題をデータベースに蓄積し，過去に出題された問題を参照するという攻撃方法（データベース攻撃）によって，問題を解くことが可能となる．しかし，そもそも CAPTCHA は，機械（マルウェア）には理解できない問題をその題材として用いるわけであるので，機械（CAPTCHA システム）がそれを認識して適切な問題を自動生成することは非常な困難な要求である．

実際，研究者が提案した新たな CAPTCHA の多くは，攻撃耐性を重視するあまり問題の自動生成が困難となってしまっている，または，自動生成の実現のために攻撃耐性の向上が不十分である，という課題を抱えている．以下，本節では，既存の提案された視覚的形式知を利用した CAPTCHA の発展方式のうち代表的なものを抜粋し，それらを素材のモダリティによって「文字列を素材とした形式（文字列 CAPTCHA）」「2 次元画像（2D 画像）を素材とした形式（2D 画像 CAPTCHA）」「3 次元モデル（3D モデル）を素材とした形式（3DCG 画像 CAPTCHA）」へ分類し，かつ，それらの問題点について指摘をする．

2.2.1　文字列 CAPTCHA の発展形式

人間は，文字や図の姿形全体を見なくとも，その一部を見ただけで，足りない部分を脳内で補完して，元の文字全体を認識することが可能である．すなわち，人間は「文字全体の姿形」に限らず「文字の一部」も自身の視覚的形式知として有しているといえるであろう．この認識能力はアモーダル補完と呼ばれる．このアモーダル補完と呼ばれる能力に注目をして，文字列判読型 CAPTCHA を強化した CAPTCHA が文献[17]にて提案されている（図 2-4）．文献[17]では，アモーダル補完を利用して認識される文字列をユーザへ提示して，その文字列を読めるか否かでユーザが人間か機械であるかを判定している[1]．ただし，本方式も，機械学習を利用して解読可能であることが指摘されている[18].

そのほか，ANIMIERTE CAPTCHA[35], Dracon CAPTCHA[36], CAPTCHANIM[37]

[1] 提案方式は，アモーダル補完を利用することに加えて「CAPTCHA を動画化する」等の工夫をして，さらに機械解読耐性を高めている．ここでは，文字列判読型 CAPTCHA との比較に主眼をおくため，アモーダル補完による攻撃耐性の強化にのみ着目をして説明を行う．

などの CAPTCHA も，妨害図形を用いて文字列判読型 CAPTCHA を強化したものであり，文献[17]と類似した方式として解釈できる．これら CAPTCHA の多くは，機械に容易に正解されるという報告がなされている[38].

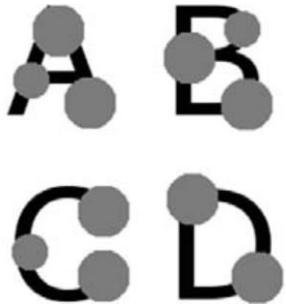

図 2-4　アモーダル補完を利用した文字列 CAPTCHA のコンセプト図
（文献[17]より引用）

文字列を素材とした別のアプローチとして, SS-CAPTCHA[19]がある. SS-CAPTCHA は，ユーザに，人間が作成した自然な文章と機械翻訳により生成された文章とを複数提示し，自然な文章を選択することができたユーザを人間と判定する CAPTCHA である（図 2-5）．機械にとっては，機械翻訳技術は急速な進歩を遂げてきたが，他言語の文章を機械翻訳にかけて生成した母国語は，その母国語を利用する人にとっては不自然な文章（母国語話者が，見たことがないであろう文章）になることも多く，自然な文章を自動的に作り出すことは非常に難しい技術である．

人間は，日常生活の中で多くの文章を見ることで，それらを知識として身に着けてきている．よって，機械翻訳した不自然な（見たことがないであろう）文章と通常の文章を識別することが可能である．ここで，「不自然な文章」を機械が解釈できるのであれば，機械は機械翻訳にかけた言語をセルフチェックすることによって，適切な修正を施すことができるはずである．そのような適切な修正を施すことができていないことは，前述に示した「（母国話者が）見たことのあるであろう文章」や「（母国話者が）見たことがないであろう文章」を機械が解釈することが難しいことを示している．

ただし, SS-CAPTCHA の問題を自動生成するためには多くの自然な文章が必要である．しかし，自然な文章を「機械が利用できない形で」効率よく集めることは難しい．インターネット上には人間が作成した文章が無数に存在しているが，これを CAPTCHA の問題に使うのは適切ではない. マルウェアも, 問題として提示された文章を Web 検索し，当該文章が見つかれば自然な文章であると判定できてしまうためである．さらに，検索でヒットしないように文章を崩した場合，自然な文章が不自然な文章となってしまうため，文章を崩すことも困難である．SS-CAPTCHA と類似の形態を持つ，マルコフ連鎖による合成文書の不自然さを用いた CAPTCHA [20]においても，自然文の自動生成の課題は残されている．

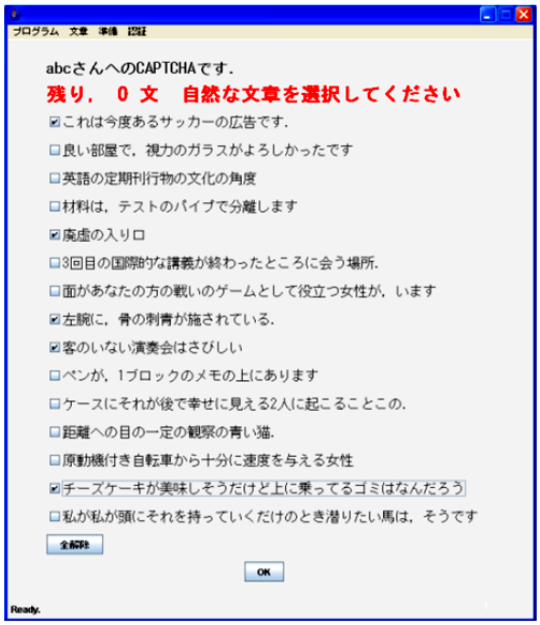

図 2-5　SS-CAPTCHA の認証画面例（文献[19]より引用）

2.2.2　2D 画像 CAPTCHA の発展形式

FaceD CAPTCHA では，図 2-6 のとおり，本物の人間の顔画像とイラストの顔画像（スマイルマーク，アニメのキャラクタの顔画像など）がユーザに提示される[25]．ユーザはその画像群から，本物の人間の顔画像だけを選択することを求められる．すなわち，「本物の人間の顔らしさ（写真）」と「描かれた顔らしさ（イラスト）」という視覚的知識を利用した CAPTCHA である．ここで，Assira は全く異なる「犬」という「猫」とカテゴリの違いを問うている一方，本 CAPTCHA は，同じ「顔」というカテゴリの中で，その細部の違い（本物であるか描かれたものであるか）を識別することを求めていることに注意されたい．筆者が知る限り，突破されたという報告は存在しないが，顔認識技術[26]や人物検出技術[27]が発達している現状に鑑みるに，機械も高い成功率で突破可能である可能性が高い．また，人間やイラストの顔を自動収集する必要がある点で，問題の自動生成に関しても課題がある．

図 2-6　FaceD CAPTCHA の問題画像例（文献[25]より引用）

4 コマ漫画 CAPTCHA は，4 コマ漫画の各コマをランダムに並べ替えることで，起承転結を崩した 4 コマ漫画をユーザに提示する．そして，その 4 コマ漫画の正しい順序を答えることができたユーザを人間として判定する CAPTCHA である（図 2-7）[31]．起承転結を崩した 4 コマ漫画は，人間にとって今まで見たことがないであろう，不自然な 4 コマ漫画となる．よって，人間は，各コマの画像を自身の知識を利用して認識したうえで，もとの順番（見たことがあるような順番）へと戻すことが可能である．しかし，起承転結を備えた 4 コマ漫画を十分な数用意することは困難であるため，自動生成の観点で課題が残る．

図 2-7　4 コマ漫画 CAPTCHA（画像中の 4 コマ漫画の各コマは，左からそれぞれ文献[32]の P.25 の 4 コマ漫画の 1 コマ目，4 コマ目，3 コマ目，2 コマ目より引用）

その他の形式として，動画形式のワンモア CAPTCHA[39]がある[2]．ワンモア CAPTCHA は，動画の一部に対して入れ替えや切り抜きの加工を施すことで，ストーリ性を壊した動画をユーザに提示する（図 2-8）．そして，入れ替えや切り抜きといった加工が施された場面を指摘できたユーザを人間とみなす CAPTCHA である．人間であれば，動画の各コマを認識したうえで，「見たことがない」不自然なシーンを特定することが可能である．一方，このような知識を有しない機械にとっては，特定困難であることが期待される．しかし，ワンモア CAPTCHA に適した，ストーリのわかりやすい動画素材を十分に集める方法が確立されていないため，問題の自動生成が困難である．

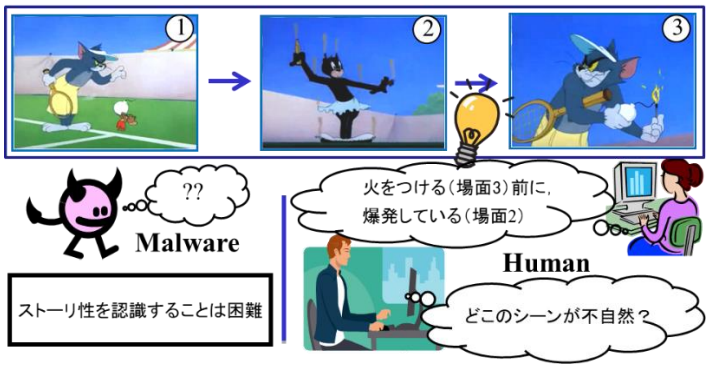

図 2-8　ワンモア CAPTCHA（画像中の動画の各コマは，映像[40]より引用）

[2] ここでいう「動画」は 1 枚 1 枚の画像（コマ）をつなげてストーリ性を持たせたものである．よって，本論文では，画像を素材とした形式に分類をしている．

2.2.3　3DCG 画像 CAPTCHA の発展形式

3DCG 画像 CAPTCHA の発展形式としては，Sketcha が存在する[14]．Sketcha は，3D モデルを 2D 画像へ投影し，その 2D 画像に線画化と回転（0，90，180，270 度）を施した上でユーザに提示する（図 2-9）．提示画像をユーザが 1 回クリックするごとに，2D 画像が 90 度回転し，画像を直立状態（0 度の回転）に戻すことができたユーザを正規ユーザとして判定する形式となっている．すなわち，モデルの「上方向」を問うている CAPTCHA となっている．人間であれば，モデルの姿形を自身の視覚的形式知を利用して認識できる．さらに，そのモデルに対して「上方向がどちらか」という視覚的形式知も有しているため，本 CAPTCHA を解くことが可能である．一方，機械はその視覚的形式知を有していないため，解読困難であると主張されている．しかし，問題画像の自動生成のためにはすべての 3D モデルに対して「どちらが上か」という情報を付与しなければならない点で課題がある．また，90 度単位の回転であるため 1 問あたりの総当たり数が非常に小さい（4 通り）点で，総当たり数攻撃に対する耐性が低下している，という課題もある．

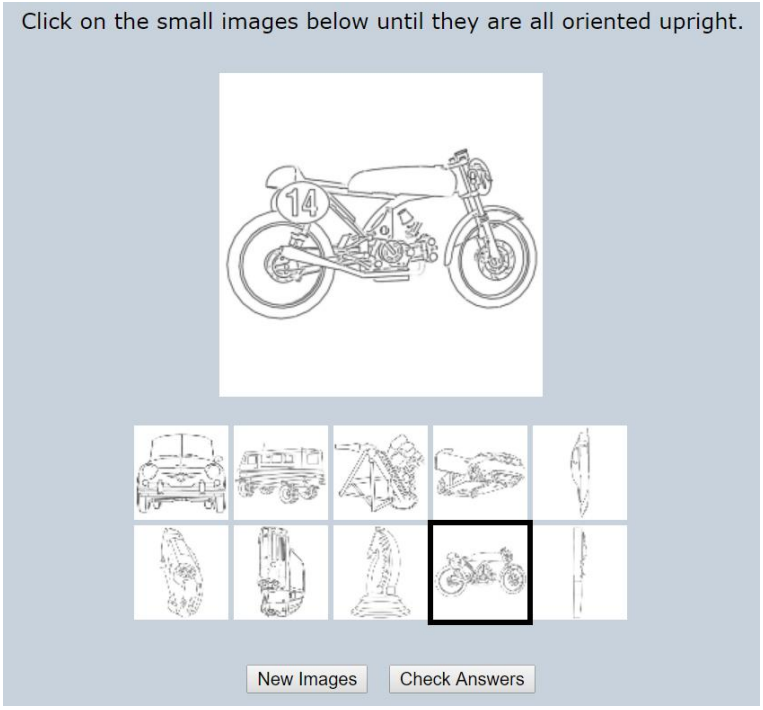

図 2-9　Sketcha（デモサイト[15]より引用）

2.3　視覚的形式知を利用した CAPTCHA の二分類

前節までに，視覚的形式知を利用した CAPTCHA をそのモダリティによって，3 つの形式に分類した．本節では，それらをさらに「より精確な視覚的形式知を利用した形式」と「視覚的形式知からの逸脱を利用した形式」という二つのグループに定義・分類可能であることを示す．

各モダリティ CAPTCHA の基本形態は，素材（文字列・2D 画像・3D モデル）全体の姿形を利用した形式である．より精確な視覚的形式知を利用するという指針とは，素材の姿形全体に関わる知識だけでなく，その素材のより細部に関わる知識までをユーザに問うという手段を用いて，各 CAPTCHA を発展させる指針である．たとえば，

- アモーダル補完を利用した CAPTCHA では，「文字」の姿形全体だけでなく，「ある文字の一部」という知識を利用し，元の文字を認識することが必要となる．
- FaceD CAPTCHA は，「顔」という姿形全体に関わる知識だけでなく，顔が「イラスト」か「本物の人間の顔か」を判別するために「顔の細部」に関わる知識までが必要となる．
- Sketcha は，「モデルが何か」という姿形全体だけでなく，「そのモデルの上方向」という知識も必要となる．

視覚的形式知からの逸脱を利用するという指針は，単にその素材を利用するだけでなく，自然な素材を加工したり組み合わせたりして，ユーザが今まで「見たことがないであろう」不自然な事象を創りだして利用する指針である．不自然な事象を利用することによって，素材の姿形全体に関わる視覚的形式知だけでなく，提示された事象が「今まで見たことがありそうか否か（自然か否か）」を判定するための知識も必要となる．たとえば，

- SS-CAPTCHA は，機械翻訳にかけた不自然な文章（文字列）を利用している．ユーザは，単に文字列の姿形を認識するだけでなく，提示された文字列を今まで見たことがありそうか否か（自然か否か）まで認識する必要がある．
- 4 コマ漫画 CAPTCHA は，ストーリを崩した 4 コマ漫画を利用している．ユーザは，単に各コマの画像を認識するだけでなく，各コマのつながりを今まで見たことがありそうか否か（自然か否か）まで認識する必要がある．

これらの観点に基づいて，前節に述べた CAPTCHA の発展方式を，より精確な視覚的形式知を利用する指針，視覚的形式知からの逸脱を利用する指針に分類し，前節で述べた課題を添えたものを表 2-1，図 2-10 に示す．なお，表 2-1 では，【】内で，各形式が，人間のどのような視覚的形式知を利用しているかを表し，（）内で，各方式の課題を指摘している．

表 2-1　視覚的形式知を利用した CAPTCHA の発展方法（表）

	より精確な視覚的形式知を利用する指針	視覚的形式知からの逸脱を利用する指針
文字列	アモーダル補完を利用した CAPTCHA【文字の一部】（機械に解読可能）	SS-CAPTCHA，マルコフ連鎖による合成文書の不自然さを用いた CAPTCHA【文字列が自然か否か】（自然な文章の用意が困難）
2D 画像	FaceD CAPTCHA【イラストの顔と人間の顔間の細部の違い】（画像認識によって解読可能，タグ付けが必要）	4 コマ漫画 CAPTCHA，ワンモア CAPTCHA【ストーリが自然か否か】（十分な数の 4 コマ漫画や動画の用意が困難）
3D モデル	Sketcha【3D モデルの姿形とその向き】（画像に「上」という情報を付与することが必要，総当たり数）	（著者が知る限り，存在しない）

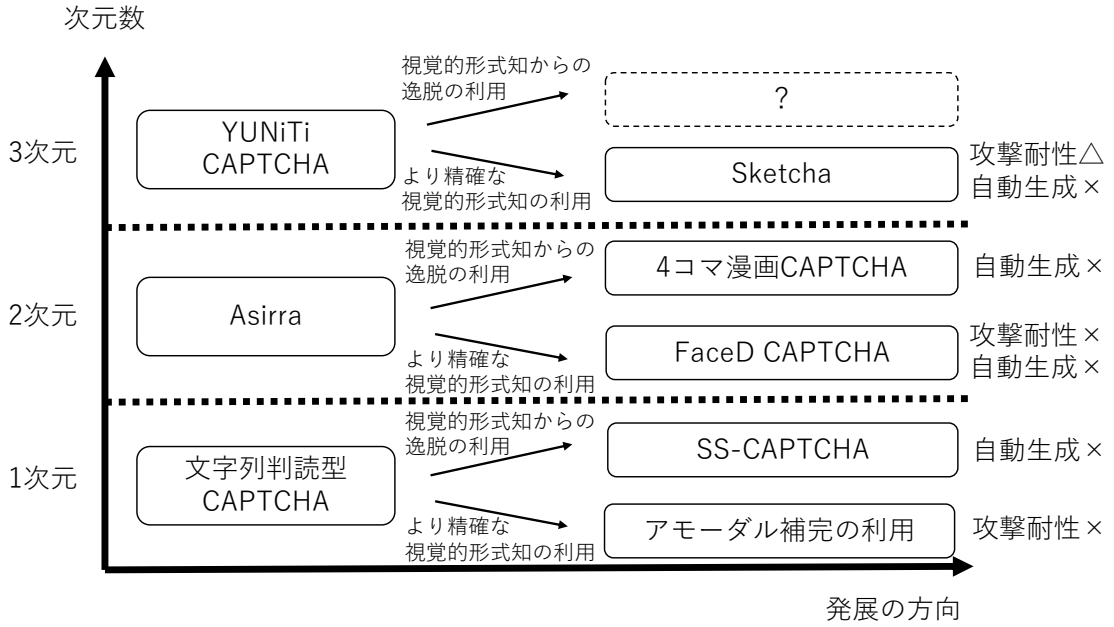

図 2-10　視覚的形式知を利用した CAPTCHA の発展方法（図）

2.4　3DCG 画像 CAPTCHA に着目する理由と課題

2.3 節に示したとおり, 現在までに提案されている各 CAPTCHA には, 機械解読耐性, あるいは，自動生成の観点でそれぞれ課題が存在した．本研究は，このうち視覚的形式知を利用した 3DCG 画像 CAPTCHA に注目し，人間の正解容易性を維持しつつ，機械が正解困難，なおかつ，問題の自動生成が容易な CAPTCHA を追求するものである．以下, 3DCG 画像 CAPTCHA に着目する理由を説明した後, 既存の 3DCG 画像 CAPTCHA から見た，本論文で提案・実装・評価する CAPTCHA の位置づけを説明する．

2.4.1　3DCG 画像 CAPTCHA に着目をする理由

前節で述べたとおり，現在までに提案されている視覚的形式知を利用した CAPTCHA には，攻撃耐性，ユーザビリティ，問題の自動生成のいずれかの点で課題があった．各モダリティ（文章・2D 画像・3D モデル）の各発展（より精確な視覚的形式知を利用する指針・視覚的形式知からの逸脱を利用する指針）について，それぞれ課題を解決した CAPTCHA の実現が望まれる. ただし, 全方式について研究することは困難であるため, 本論文は，このうち，3DCG 画像 CAPTCHA に注目をして研究を進める．3DCG 画像 CAPTCHA に注目する理由は以下のとおりである．

① 他のモダリティでは利用できない，空間的な情報を利用可能である．文字列や 2D 画像を素材とした形式では，x 軸，y 軸で回転するような加工は基本的に困難であり，かつ，奥行情報を利用することもできない.

② 3D モデルは基本的に一つ一つが独立しているため，新しい場面や状況を創りやすい．一方，画像や写真の場合，画像中に様々な物体が写ってしまっている場合も多いため，同様の加工をすることは困難である.

③ 将来的には，3D モデルに「動き」や「ポーズ」などといった情報も付与されることが期待される．これらを利用することで，より「機械に正解困難」あるいは「問題の自動生成が容易」な CAPTCHA が実現できる可能性が高い.

2.4.2　3DCG 画像 CAPTCHA の課題と本研究の位置づけ

本論文は，人間に正解容易，機械に正解困難，問題の自動生成が容易な CAPTCHA として，視覚的形式知を利用した 3DCG 画像 CAPTCHA を追求するものである.

前節でまとめたとおり，より精確な視覚的形式知を利用するという指針で発展させた 3DCG 画像 CAPTCHA には，Sketcha が存在する．しかし，モデルに対して「上」という情報を付与する必要があるため，自動生成の点で課題があった．さらに，「上方向」を回答するという性質上，総当たり数が小さい（4 通り）という課題があった．そこで本研究では，YUNiTi CAPTCHA の課題を解決しつつ，Sketcha の問題点を有しない，より精確な視覚的形式知を利用した 3DCG 画像 CAPTCHA を実現することを一つ目の目標とする．この目標を満たす CAPTCHA として，第 3 章で「Locimetric 型 YUNiTi

CAPTCHA」を提案・実装・評価する．

また，前節では，視覚的形式知からの逸脱を利用するという指針で発展させた 3DCG 画像 CAPTCHA は現在までに提案されていないことを述べた．視覚的形式知からの逸脱を認識するためには，単に姿形だけを認識するだけではなく，創り出した現象が自然か否かを認識する知識も必要である（機械が突破するためには，より多くの知識が必要になる）．すなわち，視覚的知識からの逸脱を利用した 3DCG 画像 CAPTCHA を提案・追求することは，機械の進化に対抗するために非常に重要な研究課題であると考えられる．そこで本研究では，人間に正解容易，機械に正解困難，問題の自動生成が容易である，視覚的知識からの逸脱を利用した 3DCG 画像 CAPTCHA を実現することを二つ目の目標とする．この目標を実現する CAPTCHA として，第 4 章では「非現実画像 CAPTCHA」を提案・実装・評価する．

2.5 その他の方式の CAPTCHA

本論文の主旨と異なるため前節まで説明を省略したが，その他の方式として，視覚障がい者のための音声 CAPTCHA，行動ベースの CAPTCHA である reCAPTCHA，Capy CAPTCHA，Adversarial Examples を利用した CAPTCHA について説明をする．

2.5.1 聴覚的形式知を利用した CAPTCHA（音声 CAPTCHA）

CAPTCHA には，聴覚的形式知を利用した「音声 CAPCHA」もある．音声 CAPTCHA は，文字列を読み上げた音声をユーザが聞き，ユーザは聞き取った文字列を CAPTCHA システムへ入力する．CAPTCHA システムは，読み上げた音声と入力された文字列が一致していれば，ユーザを人間として判定する．文字列判読型 CAPTCHA や画像 CAPTCHA が回答困難であるユーザ，より詳細には，視覚障がい者のための CAPTCHA である．文字列判読型 CAPTCHA 同様，読み上げられる音声に一定のノイズをかけることで，機械にとって認識しにくい形式で出題がなされる場合が多い．ただし，文字列判読型 CAPTCHA 同様，機械学習を利用することによって，機械も高確率で突破できることが指摘されている[41]．機械に認識できないようにノイズを強めることも可能であるが，ノイズを強めすぎた場合，文字列判読型 CAPTCHA 同様，人間にも認識不可能となってしまう[42][43]．音声 CAPTCHA をノイズ付与なしに，どのように強化していくかを探ることも重要な研究課題であるが，本論文は視覚的形式知を利用した CAPTCHA を研究するものである．よって，音声 CAPTCHA についてはスコープ外とする．

2.5.2 行動ベースの CAPTCHA

ユーザに問題を解くタスクを求めるのではなく，ユーザの行動を利用して「人間らしさ」を判定する CAPTCHA が存在する．その代表例として，Google が開発している reCAPTCHA[44]と Capy が開発している Capy CAPTCHA[45]がある．

reCAPTCHA は，図 2-11 に示すようなフォームを表示する[3]．フォーム内のチェックボックスにユーザがチェックを付けた際，そのユーザの過去の Web 上の行動履歴やマウス動作を利用して，そのユーザが人間であるか機械であるかを判定する形式である．内部アルゴリズムの詳細は公開されていないが，cookie に Web の行動ログを蓄積しておき，その行動が一つの要素として利用されていることが推測されている[46]．それゆえ，cookie を偽造するなどして，人間であることを偽造可能であるという報告もなされている[4]．

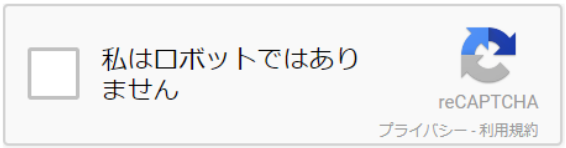

図 2-11　reCAPTCHA（reCAPTCHA の公式サイト[47]より引用）

Capy CAPTCHA は，図 2-12 のような画面を表示する．ユーザは，パズルを解く感覚で，出題画像として提示されたパズルのピースを，回答画像の抜け落ちている部分へ移動させる．パズルを解くこと自体は機械にも容易に行うことができるが[48]，ピースを移動させている最中のピースの移動軌跡（動かし方）が人間らしいかどうかも利用したうえで，人間であるか機械であるかを判定している[5][49]．

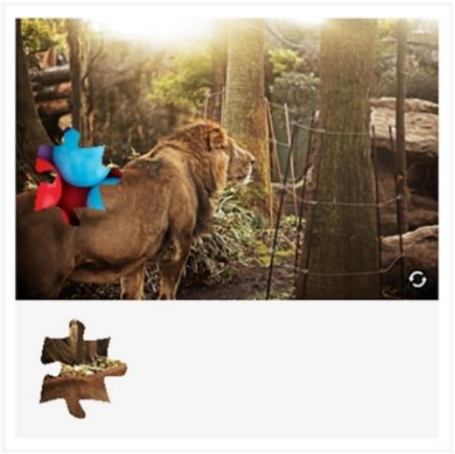

図 2-12　Capy CAPTCHA（CapyCAPTCHA の公式サイト[45]より引用）

---

[3] reCAPTCHA は，複数の形態が存在する．ここで紹介する reCAPTCHA は，そのうちの一形態であり，「No CAPTCHA reCAPTCHA」と呼ばれる形態である．

[4] ただし，Google の ReCAPTCHA は定期的に改良がなされているといわれており，現在はこの攻撃が利用できない可能性も高い．

[5] パズルのピースを移動させる部分は，画像 CAPTCHA で一部を欠損させて，その一部を利用したものである．すなわち，画像 CAPTCHA においてより精確な視覚的形式知を利用したアプローチでもある．ただし，本 CAPTCHA の最大の特長はユーザの行動を利用していることであるため，本 CAPTCHA の説明は本節で行うこととした．

両 CAPTCHA とも内部アルゴリズムや運用状況が非公開であるため，正確な議論が困難であるが，バイオメトリクスの分野で動的な生体認証の認証精度が低い傾向があることに鑑みれば[50]，両 CAPTCHA とも認証精度が低いことが期待される．さらに，行動ログを利用しているがゆえに，行動ログがない状況やトラッキングが失敗した状況では本方式を適用することが難しい．このような場合に備えて，行動ログを利用しない，視覚的形式知を利用した CAPTCHA（前節までに説明したような CAPTCHA）を用意する必要がある．

2.5.3 Adversarial Examples を利用した CAPTCHA

Deep Learning（DL）を用いて学習した識別器に誤認識を起こさせる入力として Adversarial Examples が知られている[51][52]．Adversarial Examples の基本的な仕組みは次のとおりである．

あるクラス C に含まれる画像 x があったとき，摂動ノイズ r を加えた画像を x'=x+r とする．このとき，学習に利用した DL のネットワークとそのパラメータから求めた適切な摂動ノイズ r を利用することによって，人間にはクラス C に含まれると認識されるが，識別器にはクラス C と異なるクラス C'と認識されるような，画像 x'を作成することが可能である．

Adversarial Examples の実例を図 2-13 に示す．図 2-13 では，panda（パンダ）というクラスと認識されるべき画像が，gibbon（テナガザル）というクラスと認識されていることがわかる．

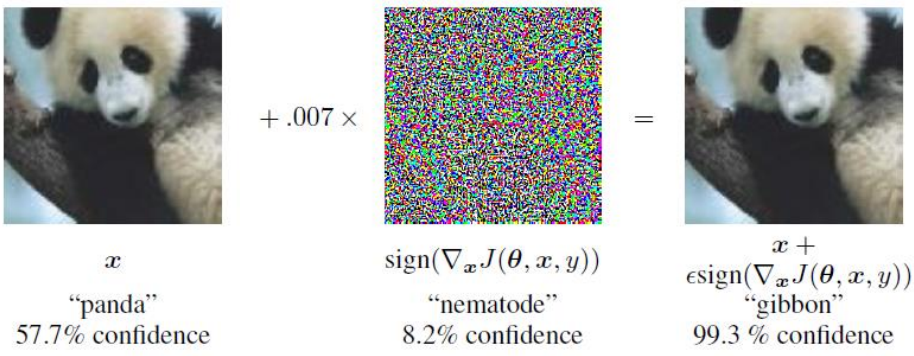

図 2-13 Adversarial Examples の例（文献[52]より引用）

この Adversarial Examples のアイデアを利用して，文字列判読型 CAPTCHA や 2D 画像 CAPTCHA に摂動ノイズを付与した研究が知られている[53][54]．文字列や 2D 画像に対して，適切な摂動ノイズを加えることによって，人間にはもともとのクラス（正解）として認識され，機械には別のクラス（不正解）として認識されるような問題が実現される．たとえば，図 2-14 は，文献[54]で提案されている方式の問題画像例の一部である．人間が見れば明らかに「W」と読み取れるが，識別機には「A」として認識されていることがわかる．

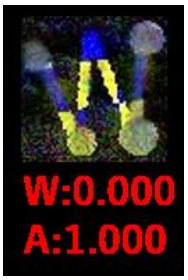

図 2-14　Adversarial Examples を利用した文字列判読型 CAPTCHA の
問題画像例の一部（文献[54]より引用）

ただし，実際の運用では，攻撃者がどの識別機を利用して攻撃するかをあらかじめ予測できないため，（攻撃者が利用する識別機が誤認識するような）適切な画像をあらかじめ用意することが困難である可能性が高い．また，Adversarial Examples による誤認識を防ぐような学習手法も提案されているため[55]，本手法の効果が限定的である可能性も高い．

第3章　Locimetric 型 YUNiTi CAPTCHA

本章では，より精確な視覚的形式知を利用した（3D モデルの中の特定部位を利用した）3DCG 画像 CAPTCHA「Locimetric 型 YUNiTi CAPTCHA」を提案・実装・評価する．

3.1　コンセプト

第 2 章では，YUNiTi CAPTCHA のような出題形式では，機械は正解画像を推定するために，

- 候補画像群の中から出題画像に類似した画像を選ぶ（類似画像選択攻撃）という戦略
- 2D 画像 CAPTCHA と同様に，画像に写るモデルが何であるかを認識する（3D モデル認識攻撃）戦略

を採用することで突破できる可能性が高いことを指摘した．これらの攻撃に対する耐性を高めるためには，正解モデルと類似した囮モデルを候補画像の中に多数混入することが肝要になる．しかし，類似したモデルの混入は，人間の正答率の極端な低下に直結してしまう．そこで，「より精確な視覚的形式知を利用する」ことで，攻撃耐性と利便性を向上させる方法がある．現在までにこの方式によって発展された方式として，モデルの「上方向」という知識を加えた Sketcha がある．しかし，Sketcha は 1 問あたりの総当たり数が小さく，モデルに対して「上」という情報を付与する必要がある点で，望ましい発展方式とはいえない．そこで本章では，「より精確な視覚的形式知を利用する」という発展をしたうえで, Sketcha の問題を有しない(総当たり攻撃耐性を有しており，問題の自動生成が可能である）3DCG 画像 CAPTCHA を提案・実装・評価する．

提案方式は，「単一の 3D モデルの中の特定部位を選択する」というタスクを採用した 3DCG 画像 CAPTCHA「Locimetric 型 YUNiTi CAPTCHA」である．提案方式は，モデルの姿形全体だけでなく，モデルの部位という知識までを利用した形式である．提案方式の認証画面例を図 3-1 に示す．認証画面は，「出題画像」（左側の画像）および「回答画像」（右側の画像）の二枚の画像から構成される．2 枚の画像は同一の 3D モデルを異なる視点から描画した後に線画化した画像であり，出題画像にのみマーカ（灰色の球）が表示されている．ユーザは，出題画像におけるマーカ部位が回答画像ではどこに当たるのかを回答する．人間であれば，出題画像の 3D モデルを頭の中で回転させ，回答画像の 3D モデルと比較することによって，回答画像における正解部位（出題画像

のマーカ部位に対応する部位）を認識可能である．なお，画像生成に使用する 3D モデルの種類，大きさ，視点，マーカ位置は問題生成の度に変更する．

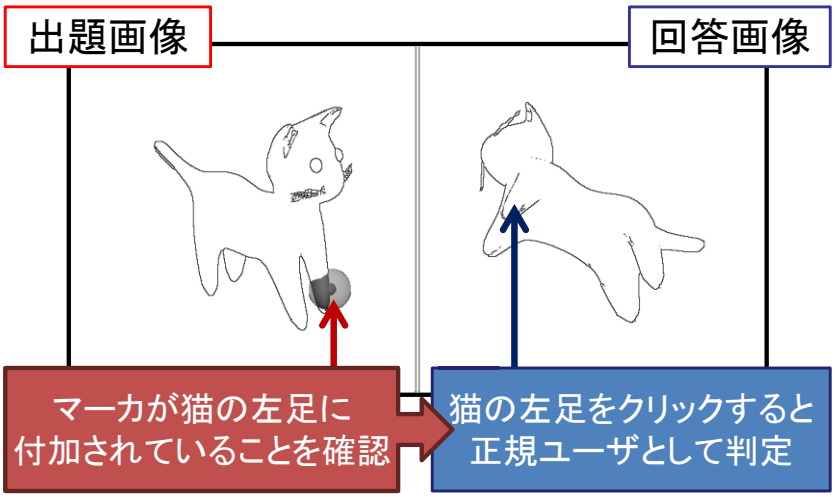

図 3-1　Locimetric 型 YUNiTi CAPTCHA の認証画面例

本方式は，同じモデルを選ぶという YUNiTi CAPTCHA を，同じ部位を選ぶという Locimetric 方式へと改良させた方式ととらえられることから，以下，Locimetric 型 YUNiTi CAPTCHA と呼ぶ．本 CAPTCHA は，前述した YUNiTi CAPTCHA や Sketcha の課題を解決した，人間に正解容易，機械に正解困難，かつ，問題の自動生成が容易な CAPTCHA であることが期待される．具体的には，以下のとおりである．

機械に正解困難：

- 単一のモデルによって構成される Locimetric 型 YUNiTi CAPTCHA では，マルウェアは「最も似ている画像を探す」という，類似画像選択攻撃が利用できなくなる．さらに，モデルの部位まで認識する必要があるため，「単にモデルが何であるかを認識する」という 3D モデル認識攻撃だけでは正解不可能である．これらの攻撃に対する耐性を含めた，提案方式の画像認識攻撃に対する耐性は 3.5.2 項で議論を行う．
- モデルの部位を利用しているため，総当たり数は Sketcha（4 通り）より大きく，YUNiTi CAPTCHA（18 通り）と同程度である．この点については，3.5.1 項で議論する．

人間に正解容易：

- 前述のとおり，YUNiTi CAPTCHA に対して，正解モデルと類似した囮モデルを候補画像の中に多数混入することで，類似画像選択攻撃・3D モデル認識攻撃に対して，耐性を持たせることは可能である．しかし，その方法では人間の正答率が大幅に低下してしまう．一方で，Locimetric 型 YUNiTi CAPTCHA は，類似画像選択攻撃・

3D モデル認識攻撃に耐性をもっている一方, 人間の正答率の低下を抑えることが可能である．この点については，3.4 節で検証を行う．

問題の自動生成が容易：

- 問題画像と回答画像で同じモデルを違う角度で提示するだけであるため，「上」という情報をモデルに付与することは不要である．すなわち，問題の完全な自動生成を実現している．この点については，3.6 節で議論する．

Locimetric 型 YUNiTi CAPTCHA の問題では，同一の 3D モデルを異なる視点から写した 2 枚の 2D 画像（出題画像と回答画像）が提示される形になる．したがって，マルウェアはパターンマッチングや立体認識の技術を利用し，出題画像と回答画像の間の部位の対応を同定する攻撃を試みるであろう．

パターンマッチングは，領域ベースマッチングと特徴ベースマッチングに大別される[56][57]．領域ベースマッチングは画像中の部分領域どうしをマッチングする方式であり，2D 画像の大きな変形に対する耐性が概して乏しい[56][58]．特徴ベースマッチングは，画像中の特徴点（局所記述子）どうしをマッチングする方式であり，2D 画像の拡大・縮小・回転に対する堅牢性がある．しかし，特徴ベースマッチングも，被写体の向きが 3D 的に大きく異なる場合には特徴点の対応付けが難しくなる[58][59]．そこで，提案方式では，出題画像と回答画像の間で，3D モデルを X 軸，Y 軸それぞれに対して 45 度以上の視点の回転を加えることで対策を行う．なお，視点の回転角度は，出題ごとに毎回ランダムに選ばれる．また，モデルのスケールについても，出題ごとに毎回ランダムに変更する．

立体認識は，一つの 3D モデルを異なる二つの視点から撮影した 2 枚の画像から，その 3D モデルの立体形状を同定する技術である[60]．この攻撃に対し，提案方式では，前述のスケール変換に加えて，画像を線画化した状態で出題することで対策を行っている．色や影といった奥行きを知る手がかりとなる情報が取り除かれる分，3D 画像認識の難度が高まることが期待される．

オリジナルの YUNiTi CAPTCHA の場合は，候補画像群の 3D モデルの中に出題画像と同一の 3D モデルが 1 体だけ存在する．類似画像選択攻撃の耐性において，上述のスケール変換，回転角度の下限，線画化等を適用しても，同一の 3D モデルどうしの画像間の類似度は，異なる 3D モデルどうしの画像間の類似度と比べると，概して高いといえる．すなわち，マルウェアが「出題画像と最も類似した画像を探す」という戦略を採ることができるオリジナルの YUNiTi CAPTCHA は，スケール変換，回転角度の下限，線画化などの対策だけでは，類似画像選択攻撃に対して十分な対策効果が見込めない可能性が高いことに注意されたい．この点について著者が検証を行った結果を付録 A に記す．

3.2　手順

提案方式の認証画面作成手順を図 3-2 に示す．なお，システムの 3D モデルデータベースには，大量の 3D モデルが登録されていることを前提とする．以下に，手順の詳細を示す．

① システムは，3D モデルデータベースから，出題画像と回答画像に利用する 3D モデルを任意に選ぶ．
② システムは，①で選んだ 3D モデルにランダムにスケール変換を施し，出題用モデルを生成する．
③ 同様に，システムは，①で選んだ 3D モデルにランダムにスケール変換を施し，回答用モデルを生成する．
④ システムは，出題用モデルに対してマーカの部位をランダムに選ぶ．
⑤ システムは，④で選んだマーカの位置に対応する回答用モデルの部位を求める．
⑥ システムは，出題用モデルの視点をマーカが視認できる範囲で任意に選ぶ．
⑦ 同時に，システムは，回答用モデルの視点を，⑥で選ばれた視点から X 軸・Y 軸ともに 45 度以上異なる範囲から任意に選ぶ．
⑧ システムは，出題画像を描画した上で線画化する．ただし，マーカ部分は線画化せずにグレースケール変換を行う．
⑨ 同時に，システムは，回答画像を描画した上で線画化する．回答画像にもマーカは付加されているが，マーカ自体は描画されない．
⑩ システムは，出題画像と回答画像を表示する．
⑪ ユーザは，回答画像において「出題画像内のマーカ部位（④で選ばれた部位であり，⑤で求めた部位）」を回答する．
⑫ システムは，正答できたユーザを人間，正答できなかった人間をマルウェアと判定する．

システムに大量の 3D モデルを登録しておき，使用する 3D モデル，伸縮率，マーカの位置，視点の位置を，認証のたびにランダムに選ぶことで，ほぼ無数の問題を自動生成することが可能である．

提案方式においては，回答画像にはマーカが描画されていない．したがって，マルウェアは出題画像と回答画像の情報だけを用いて，回答画像におけるマーカ部位を特定しなければならない．これに対し，システムは自動生成の過程で回答画像におけるマーカの位置を知っている．これが「落とし戸」となり，システム（機械）が「マルウェア（機械）には認識できない問題」を自動生成し，かつ，システム（機械）自身が回答に対する正解判定を可能としている．

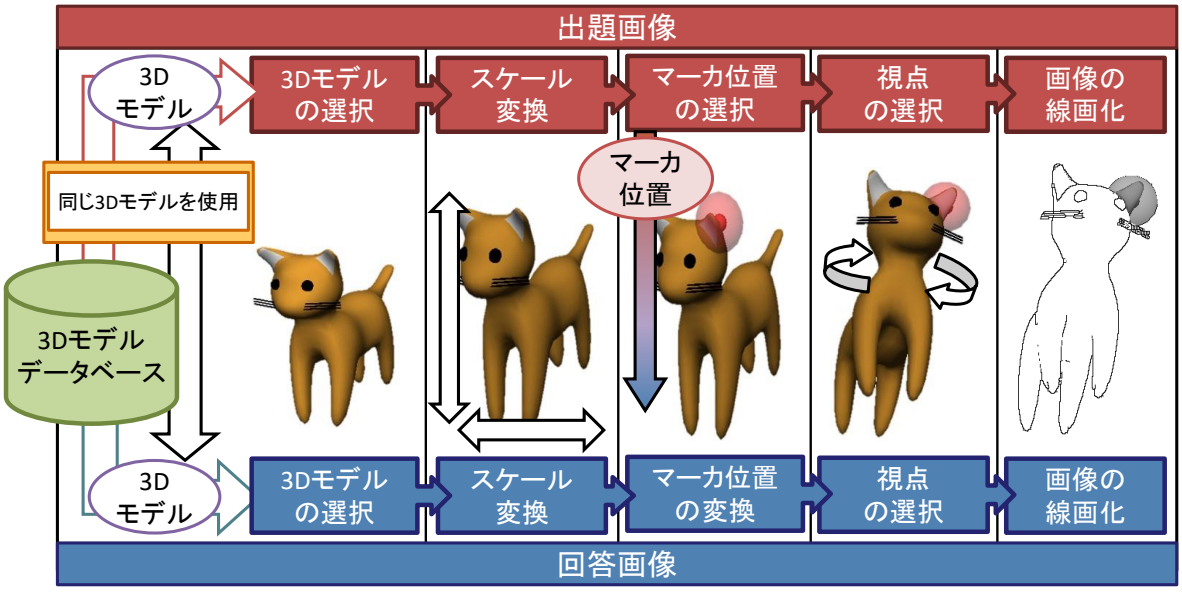

図 3-2　Locimetric 型 YUNiTi CAPTCHA：自動生成の手順

3.3　実装

3.3.1　仕様

提案方式の基礎実験を行うため，実験システムの実装を行った．図 3-3，図 3-4 に実験システムの認証画面例を示す．図 3-3 はユーザからの回答を待機している状態の画面であり，図 3-4 はユーザによる回答後の画面である．ユーザは，出題画像中のマーカ部位（灰色の球）が回答画像上のどの位置となるかを同定し，マウスクリックによって回答する．ユーザがクリックした箇所と正解部位の位置の距離が閾値以下であれば認証成功とした．図 3-3 の例では，出題画像においてマーカが犬の口元に付いているため，回答画像における犬の口元をクリックすれば正解となる．ユーザのクリック後，図 3-4 に示したようにクリック位置（×印）と正解範囲（○印）を表示するとともに，認証の成否と所要時間をユーザに知らせた．

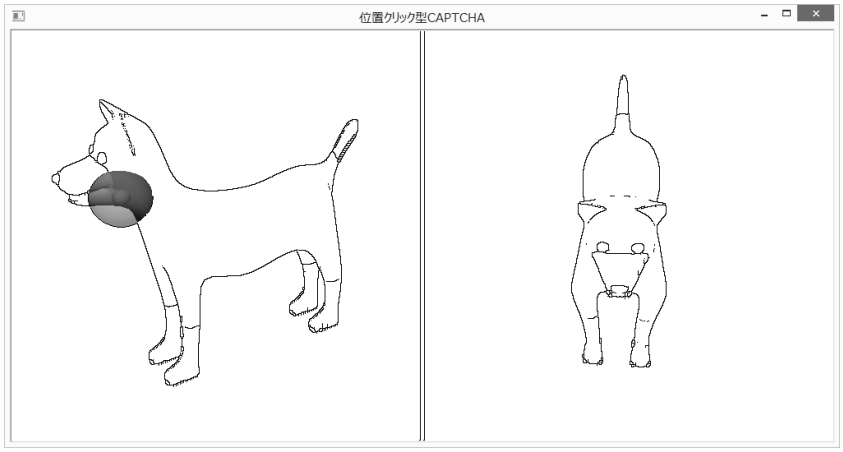

図 3-3　Locimetric 型 YUNiTi CAPTCHA：実験システム画面例（ユーザ回答前）

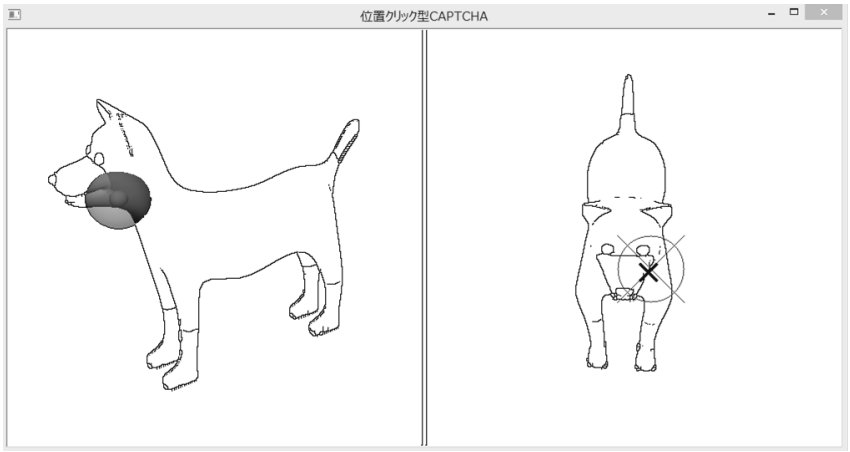

図 3-4　Locimetric 型 YUNiTi CAPTCHA：実験システム画面例（ユーザ回答後）

3.3.2　画像生成に関する制約

提案方式は，画像の生成にあたって，問題画像のサイズ，マーカの大きさ，ならびに，視点についていくつかの制約が存在する．これらの制約に関するパラメータについては，システム実装にあたって予備実験を行い，経験的に適切な値を定めた．以下に，それぞれの詳細について述べる．

（1）　画像サイズ

出題画像と回答画像の画像サイズは，縦 500 画素×横 500 画素とした．左上が(0,0)画素，右下が(499,499)画素である．

（2）　スケール変換

出題画像および回答画像の 3D モデルをスケール変換（3.2 節の手順②③）する目的の一つが，マルウェアに対する解読耐性向上である．今回の実装では，X 軸，Y 軸，Z 軸に対してそれぞれ独立に任意の倍率で伸縮を行った．ただし，モデルが大きくなり過ぎ（認証画面からはみ出し過ぎ）たり，小さくなり過ぎたりしないように，スケール変換の倍率の範囲は 1.0 から 1.5 の間に制限した．

（3） マーカ

回答用モデルにおけるマーカ部位の中心が正解座標となる．ここで，正解座標は 3D データであるのに対し，ユーザによるマウスクリックは（ディスプレイ上の座標情報として得られるため）2D データである．このため，3D モデル上の正解座標がディスプレイ上ではどの座標にあたるかを計算した上で，2D 正解座標とクリックされた座標との距離によって正解判定を行っている．正解範囲は，正解座標を中心とした円の内部であり，今回の実装では 40 画素を半径とした．

（4） 視点

出題画像の視点の選択（3.2 節の手順⑥）において，マーカが視認できなくなる視点が選ばれた場合，正答困難な問題が生成されてしまう．このため，今回の実装では，出題画像の視点は，マーカが付加されている部位が手前側に表示されるような制約を追加した．

回答画像の視点の選択（3.2 節の手順⑦）において，「出題画像の視点」に近い視点が選ばれた場合，出題画像と回答画像が類似した画像となる確率が高まり，両方の画像を比較することでマルウェアがマーカ部位を解読できる危険性が生じる．このため，今回の実装では，回答画像の視点は，出題画像の視点から X 軸および Y 軸に対して 45 度以上離れた角度の中からランダムに選ばれるような制約を追加した．ただし，回答画像中の正解座標が認証画面からはみ出てしまう場合は，視点の再選択を行った．

（5） 画像の線画化

出題画像および回答画像を線画化した状態でユーザに提示する目的の一つが，マルウェアに対する解読耐性の向上である．今回の実装では，マーカの視認性に配慮し，マーカ部分はグレースケール変換を行った．

3.4 利便性に関する評価実験

3.4.1 目的

オリジナル YUNiTi CAPTCHA を再現した CAPTCHA（以下, YUNiTi 型 CAPTCHA），および，類似モデルを含む YUNiTi 型 CAPTCHA の実験システムについて実装する．提案方式とこれらの CAPTCHA を正答率と回答時間の観点から比較することで，提案方式が人間に正解容易な方式であることを確認する．具体的には，「類似モデルを含む YUNiTi 型 CAPTCHA の実験システム」と提案方式の正解率と認証時間を利用することで, 人間の正答率の低下が抑えられていること（類似モデルを含む YUNiTi 型 CAPTCHA と比較して同程度以上であること）を確認する．すなわち，類似画像選択攻撃・3D モデル認識攻撃に耐性を持つことを要件とした場合に，既存方式（YUNiTi CAPTCHA）と比較して高い正答率であることを確認する．

3.4.2 諸元

本実験の被験者は情報系大学生 20 名である．各被験者に，YUNiTi 型 CAPTCHA と提案方式をそれぞれ 5 問連続して解いてもらった. 被験者は, 先に YUNiTi 型 CAPTCHA を解いた後に提案方式を解くグループ α と，逆の順番で CAPTCHA を解くグループ β に分かれて実験を行った．なお，本番の回答に取り掛かる前に，どちらの CAPTCHA も被験者が満足するまで練習を行うことを許した．

3.4.2.1 提案方式

提案方式の実験システムは 3.3 節で実装したシステムである．本実験では，Web 上から収集した，mqo 形式[64]の 10 種類の 3D モデル（A～J）を使用する．今回使用した 3D モデルは，全て動物（哺乳類，鳥類，爬虫類）で統一した．練習では，モデル A～E をランダムに使って問題生成する（被験者は，練習を繰り返す内に，同じモデルに関する問題を複数回目にすることがありえる）．本番では，モデル F～J をランダムな順序で 1 回ずつ使って問題を 5 問生成する（被験者は，5 種類のモデルに関する問題を 1 回ずつ目にする）．スケール変換および視点については，3.3 節で説明した制約の下，毎回ランダムに選ばれる．提案方式における出題画像と回答画像の視点の選ばれ方は，被験者には知らせていない．本実験では，回答（クリック位置），回答正否，所要時間を記録した．各回答の結果は被験者に毎回表示した．

3.4.2.2 YUNiTi 型 CAPTCHA

YUNiTi 型 CAPTCHA の認証画面例を図 3-5 に示す．オリジナルの YUNiTi CAPTCHA は 18 枚の候補画像群の中から 3 種類の正解画像を回答させる形態である．しかし, 5 種類のモデルのみを利用する提案方式と実験条件を一致させるために，「5 枚の候補画像群（図 3-5 における上段の 5 枚の画像）の中から 1 枚の出題画像（図 3-5 における左下の 1 枚の画像）に相当する画像を同定するタスク」を 1 問として扱う．使用する 3D モデルも，提案方式の実験システムと同じ 10 種類のモデル（A～J）である．練習では，モデル A～E を候補画像群として用い，その中から正解となるモデルをランダムに選んで問題を生成する．本番では，モデル F～J を候補画像群として用い，その中から正解となるモデルをランダムな順序で 1 回ずつ使って問題を 5 問生成する．各候補画像と出題画像の画像サイズは，どちらも縦 160 ピクセル×横 160 ピクセルである．視点については毎回ランダムに選ばれるが, オリジナルの YUNiTi CAPTCHA の仕様に合わせてスケール変換は行っていない．表示される画像は全てグレースケール画像である．今回の実験では，回答（選択した画像），回答の正否，所要時間を記録した．各回答の結果は被験者に毎回表示した．

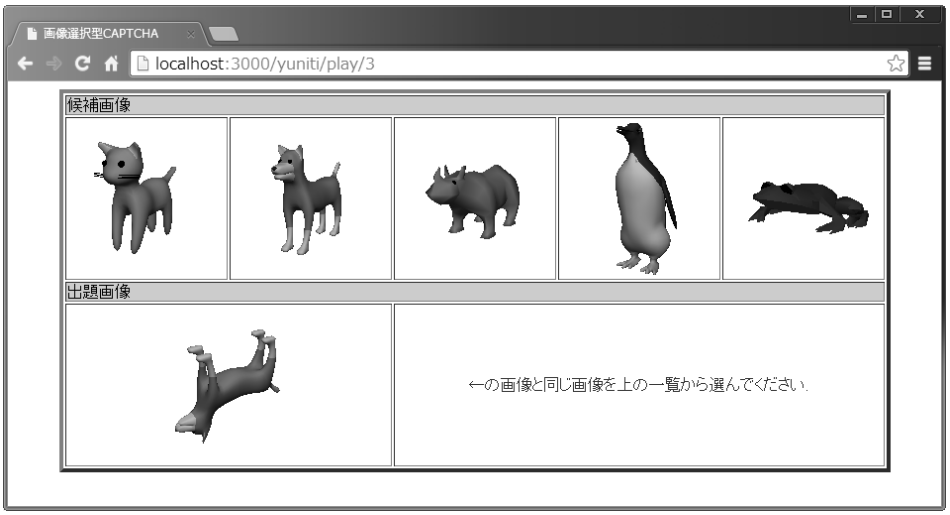

図 3-5　YUNiTi 型 CAPTCHA の認証画面例

3.4.2.3　類似モデルを含む YUNiTi 型 CAPTCHA

YUNiTi 型 CAPTCHA は「同じモデルを選択する」という形式であるため，攻撃耐性を向上させるためには，正解モデルと類似したモデルを候補画像群の中に複数含めておくことが肝要になる．この状況をシミュレートするための実験システムが「類似モデルを含む YUNiTi 型 CAPTCHA」である．具体的には，相異なる 3 体の 3D モデル A，B，C と 2 体の類似した 3D モデル K，L（図 3-6）を 5 枚の候補画像群として用いる形で図 3-5 の実験システムを運用している．類似モデルを含む YUNiTi 型 CAPTCHA の実験においても問題を 5 問生成するが，モデル K または L のいずれかが必ず正解となるように全問題を生成した．極論すると，類似したモデルを選択する攻撃や 3D モデルを認識する攻撃に対する耐性を高めるためには，すべての候補画像を正解モデルと類似したモデルにしなければならないが，今回は被験者の利便性についても配慮して「5 枚の候補画像群の中に回答画像と類似する画像が 2 枚混在する」という実験設定としている．その他の実験条件は類似モデルを含まない YUNiTi 型 CAPTCHA と同一である．

図 3-6　2 体の類似した 3D モデル

3.4.3 実験結果

提案方式，YUNiTi 型 CAPTCHA，類似モデルを含む YUNiTi 型 CAPTCHA の実験結果を表 3-1，図 3-7，図 3-8 に示す.

表 3-1 Locimetric 型 YUNiTi CAPTCHA：実験結果（表）

被験者	提案方式		YUNiTi 型 CAPTCHA			
			類似モデルなし		類似モデルあり	
	正答率	平均時間[s]	正答率	平均時間[s]	正答率	平均時間[s]
1	5/5	6.7	5/5	2.0	3/5	11.9
2	4/5	6.6	5/5	1.9	3/5	7.2
3	3/5	5.6	5/5	1.4	5/5	7.1
4	4/5	3.0	5/5	1.5	4/5	3.0
5	4/5	2.2	5/5	1.3	4/5	2.3
6	4/5	2.3	5/5	2.1	3/5	2.8
7	4/5	3.2	5/5	1.6	3/5	3.6
8	5/5	9.6	5/5	2.8	3/5	9.9
9	4/5	3.6	5/5	2.1	3/5	4.5
10	5/5	3.3	5/5	3.2	4/5	3.8
11	5/5	8.3	5/5	2.8	4/5	9.3
12	5/5	2.9	5/5	2.3	2/5	4.5
13	1/5	6.7	5/5	2.6	2/5	4.6
14	4/5	5.4	5/5	3.1	5/5	3.4
15	5/5	10.2	5/5	2.4	3/5	4.9
16	2/5	3.6	5/5	2.6	3/5	3.5
17	3/5	6.5	5/5	3.8	4/5	6.5
18	4/5	3.2	5/5	2.4	4/5	3.4
19	4/5	6.2	5/5	2.8	3/5	5.5
20	5/5	3.6	5/5	2.2	3/5	4.5
平均	80.0%	5.1	100.0%	2.3	68.0%	5.3
標準誤差	4.8%	0.54	0.0%	0.14	3.7%	0.58

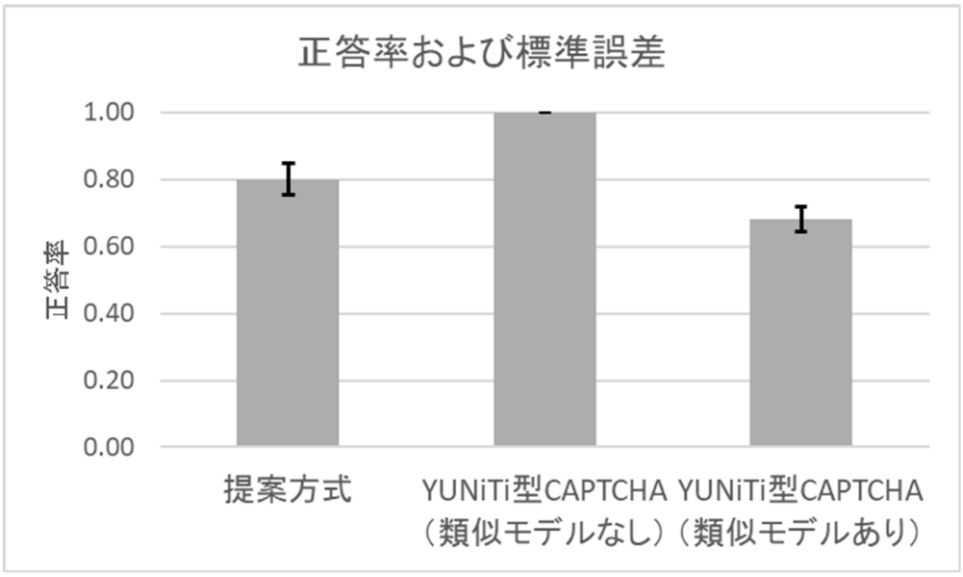

図 3-7　Locimetric 型 YUNiTi CAPTCHA：実験結果（正答率のグラフ）

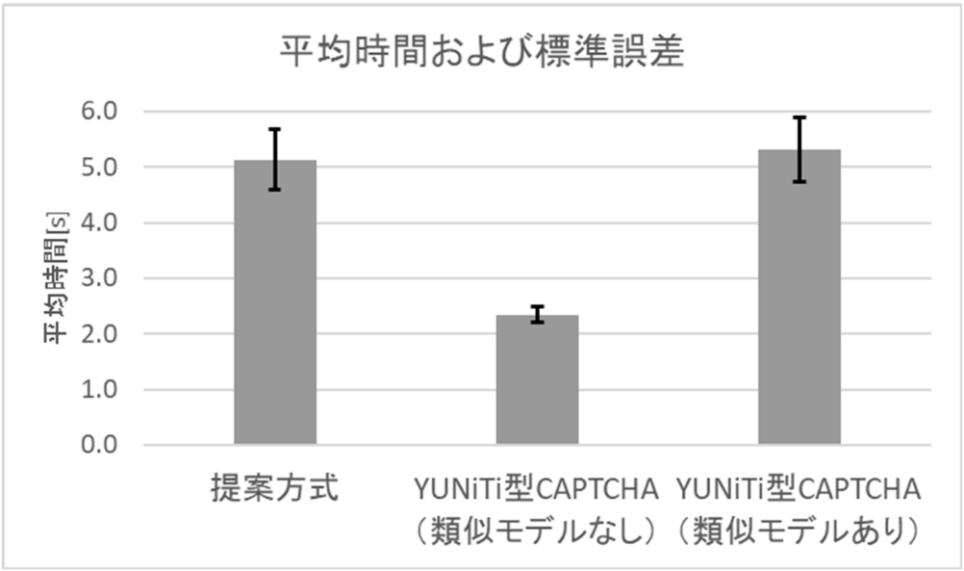

図 3-8　Locimetric 型 YUNiTi CAPTCHA：実験結果（平均時間のグラフ）

実験結果より，全被験者の平均正答率（被験者 20 人が各 5 問ずつ行った全 100 試行の成功確率）は，提案方式では 80%，類似モデルを含まない YUNiTi 型 CAPTCHA では 100%，類似モデルを含む YUNiTi 型 CAPTCHA では 68%である．全被験者の 1 問あたりの平均所要時間は，提案方式では 5.1 秒，類似モデルを含まない YUNiTi 型 CAPTCHA では 2.3 秒，類似モデルを含む YUNiTi 型 CAPTCHA では 5.3 秒である．3 つの群の間の正答率，所要時間の統計値を Steel-Dwass 検定[61]を行って求めた結果を表 3-2 と表 3-3 に示す．

表 3-2　Locimetric 型 YUNiTi CAPTCHA：正答率に関する検定結果（*p<.05）

	類似モデルなし YUNiTi 型 CAPTCHA	類似モデルあり YUNiTi 型 CAPTCHA
提案方式	0.000*	0.049*
類似モデルなし YUNiTi 型 CAPTCHA	—	0.000*

表 3-3　Locimetric 型 YUNiTi CAPTCHA：回答時間に関する検定結果（*p<.05）

	類似モデルなし YUNiTi 型 CAPTCHA	類似モデルあり YUNiTi 型 CAPTCHA
提案方式	0.000*	0.943
類似モデルなし YUNiTi 型 CAPTCHA	—	0.000*

実験結果より，全被験者の平均正答率（被験者 20 人が各 5 問ずつ行った全 100 試行の成功確率）は，提案方式では 80%，類似モデルを含まない YUNiTi 型 CAPTCHA では 100%であり，これらの間には有意差が認められた．さらに， 所要時間については，提案方式が 5.1 秒，類似モデルを含まない YUNiTi 型 CAPTCHA が 2.3 秒であった．これらの間にも有意差が認められた．これら結果から，提案方式が採用している「同じ部位を選ぶ」というタスクは，類似モデルを含まない状況であれば，YUNiTi CAPTCHA にて用いられている「同じモデルを選ぶ」というタスクより難しいことが分かる．

しかし，類似モデルが含まれた状況においては，YUNiTi 型 CAPTCHA の平均正答率は 68%であった（提案方式の平均正答率は 80%である）．提案方式の平均正答率と比較した際には，有意差が認められた．さらに，所要時間については，類似モデルが含まれた YUNiTi 型 CAPTCHA は 5.3 秒であった(提案方式の平均所要時間は 5.1 秒である)．提案方式の平均所要時間と比較した際には，有意差が認められなかった．これら結果から，類似モデルが含まれた状況においては，提案方式のほうが高い正答率を有し，所要時間については，平均値や全体の傾向を見る限り，どちらもほぼ同じ結果となっていることが分かる．

類似画像選択攻撃や 3D モデル認識攻撃に対する攻撃耐性を有することを要件とした場合，提案方式と類似モデルを含む YUNiTi 型 CAPTCHA の比較となる．以上の結果から，正規ユーザ(人間)にとって「提案方式が，類似モデルを含む YUNiTi 型 CAPTCHA

と比較して十分に正解容易な方式であること」が確認できた．さらに，類似モデルを含む YUNiTi 型 CAPTCHA に対して，提案方式と同様にスケール変換や線画化といった攻撃耐性向上策を講じた場合には，正答率の低下や所要時間の増加が予想される．

提案方式において，被験者が認証に失敗した試行には，次に示す 3 つの原因が見られた．これらの原因に対策を行うことで，提案方式の正答率を向上させる余地は多分にあると思われる．

1 つ目の原因は 3D モデルの左右の誤認識である．具体的には，動物の左後ろ足にマーカが付加されている出題画像に対して，左右を混同して回答画像の右後ろ足をクリックしてしまった例があった（図 3-9 が実際の失敗例）．ユーザが左右を意識して回答を行うようになれば，この間違いは少なくなることが期待できる[6]．

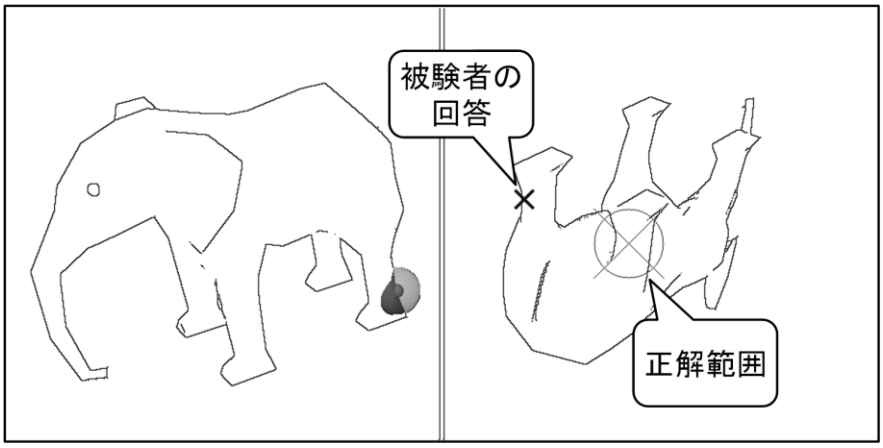

図 3-9　Locimetric 型 YUNiTi CAPTCHA：被験者の失敗例 1

2 つ目の原因は奥行きが認識しづらい視点の存在である．具体的には，出題画像において，3D モデルの真正面や真後ろからの視点が選ばれた場合に，マーカが表示されている位置の奥行方向の認識が困難であった試行がいくつか見られた（図 3-10 が実際の失敗例）．この問題に対しては，真正面や真後ろの視点を選ばないように，出題画像の視点に新たな制限を追加することで対策可能である．ただし，不適切な視点は 3D モデルの形状に応じて異なる可能性もあるため，更なる調査を行う必要がある．

[6] 実験終了後に被験者数名に対して，①まず「被験者本人の身体」を「出題画像に写っているモデル」と同じ向きに合わせることによって，②「自分の身体」のどの部位にマーカに付いているのかを認識し，③その上で「自分の身体」を「回答画像に写っているモデル」と同じ向きに合わせることによって，④回答画像中のどの部位が「自分の身体」のマーカに対応するか把握する，という「解き方のコツ」を伝えたところ，左右の誤認識が抑えられる傾向が見られた．

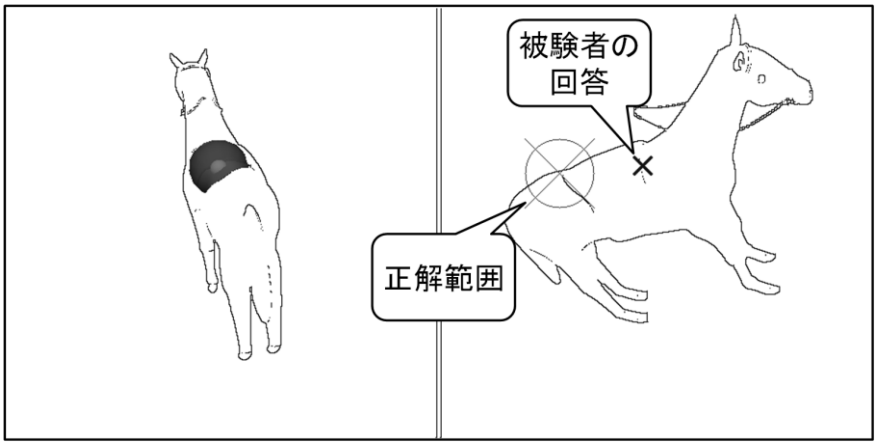

図 3-10　Locimetric 型 YUNiTi CAPTCHA：被験者の失敗例 2

3 つ目の原因は正解部位が隠れてしまう視点の存在である（図 3-11 に実際の失敗例を示す）．具体的には，回答画像において，3D モデルの正解部位とは反対側の視点が選択された場合，クリックすべき位置が隠れてしまった試行がいくつか見られた．正解部位が必ず見える視点を選択することは可能であるが，その制約が攻撃に有利に働く可能性があるかもしれない．この対策については，今後さらに検討する必要がある．

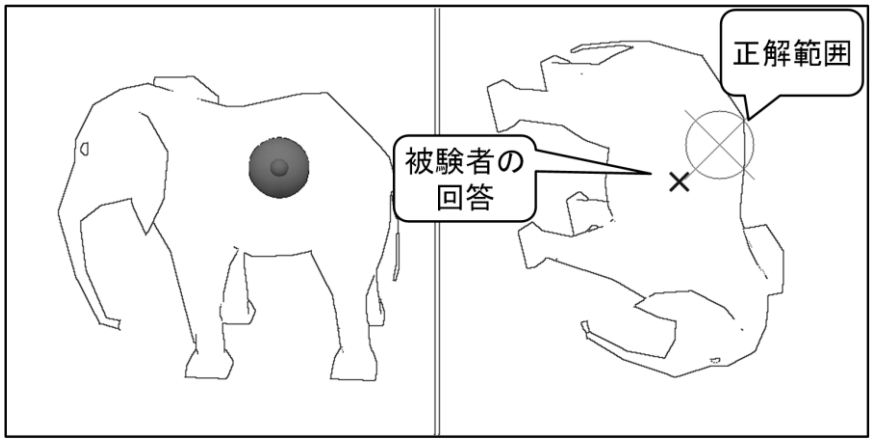

図 3-11　Locimetric 型 YUNiTi CAPTCHA：被験者の失敗例 3

3.5　安全性に関する考察

3.5.1　総当たり攻撃

今回の提案方式の実装では，縦 500 ピクセル×横 500 ピクセルの回答画像中に様々な動物が表示される．この内，総当たり攻撃の攻撃対象となるのは実際に動物が描画されたエリアの面積であり，3.3 節で実装したシステムにおいてこの大きさを実測したところ，平均しておよそ 50,000 平方ピクセルであった．これに対し，正解判定の閾値を半径 40 ピクセルの円（面積は約 5,000 平方ピクセル）と設定したため，単純計算すると総当たり数は約 10 通りとなる．

ただし，評価実験（3.4 節）の結果を分析したところ，もし正解判定の閾値を半径 35 ピクセルの円（面積は約 4,000 平方ピクセル）に設定していたとしても，正答率は低下せずに 80%であったことが確認できた．この場合，総当たり数は約 12 通りとなる．更に，もし半径 30 ピクセルの円（面積は約 3,000 平方ピクセル）に設定したならば，総当たり数は約 17 通りとなり，正答率は 72%であった．

3.4.3 項で述べた被験者の失敗原因への対策は「ユーザにマーカの位置をより正確に伝えること」にも貢献すると期待できるため，将来的には正答率を維持したまま正解判定の閾値の円を小さくすることができるであろう．このため，提案方式も，少なくとも，オリジナルの YUNiTi CAPTCHA（18 種類の候補画像から 1 枚を選択）と同程度の総当たり数（1 問当たり 18 通り）は確保できる見込みが高い．さらに，Sketcha の総当たり数（1 問当たり 4 通り）より非常に大きな値を確保することができている．

以上の議論は，YUNiTi CAPTCHA と同程度の総当たり数を議論しているが，それ以上の総当たり攻撃を確保するためには，以下の二つの方法が考えられる．

- オリジナルの YUNiTi CAPTCHA が 3 問 1 組の問題形式を採用しているように，1 回当たりの問題数を増やす方法
- 問題画像の複数の部位にマークを付与し，各マークに対して対応する部位をすべて回答画像中で答える方法

しかし，上記の改良による総当たり攻撃耐性向上は，利便性の減少とトレードオフとなる．利便性を維持したまま提案方式の総当たり攻撃耐性を向上させる工夫も今後検討する必要があるであろう．

3.5.2　パターンマッチング攻撃および 3D 形状復元攻撃

単一の 3D モデルの中の特定の部位を問う，という形式を利用した提案方式に対しては，類似画像選択攻撃や 3D モデル認識攻撃を利用することはできない．しかし，機械はこれら攻撃に加えて，パターンマッチングや立体認識の技術を駆使することで突破を試みる可能性が考えられる．

提案方式は，出題画像と回答画像は同一の 3D モデルを異なる視点から写した 2 枚の画像を利用しているため，マルウェアはパターンマッチングや立体認識の技術を利用し，出題画像のモデルと回答画像のモデルの部位の対応を同定する攻撃を試みるであろう．3.1 節で説明したように，提案方式では，領域ベースマッチングや特徴ベースマッチングを利用した攻撃については 3D モデルのスケール変換および視点の変更を行うことで，立体認識技術を利用した攻撃についてはスケール変換および線画化を行うことで，それぞれ対策を行っている．

また，パターンマッチングや立体認識の技術は，マルウェアだけでなく提案方式の強化のためにも活用することができる．すなわち，生成された出題画像と回答画像に対してパターンマッチングや立体認識を適用し，マルウェアによる解読の恐れがある画像については，システムがこれを事前に破棄することが可能である．これにより，パターンマッチング攻撃や 3D 形状復元攻撃を高い確率で無効化することが期待できる．

3.5.3　その他の攻撃

提案方式に対する攻撃手法のうち，典型的なものについては，前節までに考察した．しかし，マルウェアによる攻撃手法は多様であり，提案方式の解読耐性が理論的に証明されているわけではない．特に，線画からの立体復元[62][63]の技術については提案方式の深刻な脅威となり得る可能性がある．立体復元攻撃は YUNiTi CAPTCHA や Sketcha にも共通の脅威であるが，今後更なる分析を行う必要がある．なお，その他の攻撃については，第 5 章で改めて議論を行う．

3.6　自動生成に関する考察

提案方式では，3.2 節に示した手順のとおり，3D コンピュータグラフィックス技術を利用して毎回新しい出題画像を容易に生成することができる．3D モデルを利用した Web サービスは近年急激に増加しており，将来的には大量の 3D モデルが世の中に出回ることが予想される．したがって，Web 上から収集した多数の 3D モデルをシステムに登録しておき，使用するモデル，ならびに，モデルのパラメータ（サイズや回転角度）を変更することによって，出題画像を無数に生成することが可能となる．

ただし，「ボールや丸椅子のような 3D モデル」や「透明な部分を持つ 3D モデル」は，マーカの部位が特定できず，回答不能となるため利用することができない．しかし，このような 3D モデルは，モデルの頂点データや色データから識別することが可能であるため，提案方式に適したモデルを自動収集することは十分に現実的である．

3.7　まとめ

本章では，3D モデルの姿形に関わるより精確な視覚的形式知を利用することで，人間に正解容易，機械に正解困難，かつ，問題の自動生成が容易な 3DCG 画像 CAPTCHA を実現した．具体的には，YUNiTi CAPTCHA を Locimetric 方式（単一の 3D モデルの中の特定部位を選択する方式）へと改良した，Locimetric 型 YUNiTi CAPTCHA を提案・実装・評価した．モデルの姿形と向きだけでなく，「モデルの部位」という視覚的知識まで利用することによって，以下のような特長を有していることをユーザビリティ実験，議論，考察によって確認した．

- 類似画像選択攻撃・3D モデル認識攻撃に耐性を持つ一方，人間に正解容易である
- 3D モデルの部位を利用するため，1 問あたりの総当たり数は，「描画されているモデルの面積÷部位の面積」である．この値は，Sketcha の総当たり数よりはるかに大きく，YUNiTi CAPTCHA と同程度の総当たり数と同程度である．
- 問題画像と回答画像に同じモデルを違う角度で表示させることで自動生成可能である．すなわち，各モデルに特別なタグ付けを施さなくても，問題の自動生成が可能な方式である．

今後の課題として，視点の選択範囲の検討（マーカ位置の認識がより容易となるような視点を選択することによって，正規ユーザの正答率が向上する），正解判定範囲の検討（範囲が大きいほど正規ユーザの正答率は向上するが，総当たり攻撃に対して脆弱となる），提案方式の攻撃耐性に関するさらなる検討，等が挙げられる．今回の評価実験の結果を参考にして，これらの検討を進める必要がある．また，出題画像生成時にパターンマッチングや立体認識技術を活用し，マルウェアに対して脆弱な出題画像を予め除去する方法についても検討する必要がある．

第4章　非現実画像 CAPTCHA

本章では，視覚的形式知からの逸脱を利用した 3DCG 画像 CAPTCHA として「非現実画像 CAPTCHA」を提案・実装・評価する．

4.1　コンセプト

第 2 章では，YUNiTi CAPTCHA のような出題形式では，機械は正解画像を推定するために，

- 候補画像群の中から出題画像に類似した画像を選ぶ（類似画像選択攻撃）という戦略
- 2D 画像 CAPTCHA と同様に，画像に写るモデルが何であるかを認識する（3D モデル認識攻撃）戦略

を採用することで突破できる可能性が高いことを指摘した．本章では，「視覚的形式知からの逸脱を利用する」という指針を採用して，3DCG 画像 CAPTCHA を発展させることによって，これらの課題を解決し，かつ，さらに攻撃耐性を高めた 3DCG 画像 CAPTCHA を実現する．

視覚的形式知からの逸脱を利用した 3DCG 画像 CAPTCHA を実現するにあたっては，人間が不自然だと感じる（視覚的形式知から逸脱した，見たことがないであろう）事象と自然だと感じる（視覚的形式知に基づいた，見たことがあるであろう）事象を，3D モデル素材を加工したり組み合わせたりすることで，創りだす必要がある．本論文では，複数の 3D モデルから作られる「不自然な重なり」と「自然な重なり」を利用した 3DCG 画像 CAPTCHA を実現する．

3D モデルを（衝突しないように）平面上に並べたとき，3D モデル同士が遮蔽関係となり，前後に重なった関係となる場合がある．また，3D モデルの中には「鉢」や「草」のようにすでに重なりあった関係にあるモデルも存在する（図 4-1）．これらの「重なり」は，自然に発生したものであり，人間は視覚的形式知に基づいた「自然な重なり」と認識するはずである．そこで，これらを「自然な重なり」として利用をする．

一方，「不自然な重なり」は，ランダムに選んだ 2 つの 3D モデル同士をめりこませることで生成する．このように生成したモデルを，以下「非現実モデル」と呼ぶ．たとえば，犬のモデルに椅子のモデルがめりこんでいれば，図 4-2 に示すような，犬と椅子が結合された非現実モデルが生成される．これらも「二つのモデルが重なりあっている」現象であるが，人間にとってこのようなめり込み関係は，今まで見たことがない不自然な重なり関係である．

図 4-1　鉢と草から構成されるモデル（自然な重なり）の例

図 4-2　非現実モデル（不自然な重なり）の例

本論文では，これら 2 種類の重なりの違いを利用して，視覚的形式知からの逸脱を利用した 3DCG 画像 CAPTCHA を実現する．具体的には，複数の通常の 3D モデルの中に，一体の非現実モデルを配置した一枚の画像を CAPTCHA として出題する．画像中から非現実モデルを選択できたユーザを正規ユーザ（人間）と判断する．本論文では，本方式を「非現実画像 CAPTCHA」と呼ぶ．

提案方式は，以下のとおり，人間に正解容易，機械に正解困難，かつ，問題の自動生成が容易な方式であることが期待される．

人間に正解容易：

- 人間であれば，自身の有する視覚的形式知から逸脱した形状をしている非現実モデルを認識可能であるため，通常のモデル中に紛れている非現実モデルを発見することは容易であると考えられる．この点については，4.4 節で議論する．

機械に正解困難：

- 複数のモデルの中から「不自然なものを認識する」というタスクを利用しているため，類似画像選択攻撃を利用することはできない．
- 単に各モデルの姿形だけでなく，モデル同士の重なり関係が自然か，不自然であるかを識別する必要があるため，3D モデル認識攻撃を利用することはできない．
- また，そのほかの攻撃にも耐性を有した方式である．

以上の 3 点については，4.5 節で議論を行う．

問題の自動生成が容易：

- 複数のモデルを平面上に並べ，そのうち 2 体を同座標に配置することで，非現実モデルにするだけであるため，問題の自動生成も容易である．この点については，4.6 節で議論を行う．

4.2 非現実モデルの自動生成

提案方式では問題画像中に，2 つの 3D モデルをめり込ませ合った非現実モデルを描画する．非現実モデルは図 4-3 に示すとおり，「2 つのモデルを同座標に配置する」という手順を用いることで容易に生成可能である．具体的には，次の手順である．

① 非現実モデルを構成する 2 体のモデル（めり込ませ合う 2 体のモデル）をランダムに選択する．
② ①で選択したモデルのうち，1 体を 3D 平面 α 上の適当な座標 P に配置する．具体的には，モデルが内接する直方体を生成し，その底面の中心点が平面 α 上の点 P に一致するようにモデルを配置する．
③ ①で選択したモデルのうち，②で使用しなかった 1 体を②と同一の座標 P に配置する．②と同様，モデルが内接する直方体の底面の中心点が平面 α 上の点 P に一致するようにモデルが置かれる．

本手順で描画した 2 体のモデルは，共通部分が隠されることで互いにめりこみ合った状態となり，人間にとっては非現実モデルとして認識される[7]．3D モデルを利用した Web サービスは近年急激に増加しており，将来的には大量の 3D モデルが世の中に出回ることが予想される．本手法であれば，任意の通常モデルから非現実モデルを無数に，かつ容易に自動生成することが可能である．

[7] 大きなサイズのモデルと小さなサイズのモデルの 2 体を同一の点 P に配置した場合，大きなモデルの中に小さなモデルが埋まってしまって，2 体がめり込みあったモデルが生成されないといった状況が発生し得る．これを防ぐために，実際のシステムにおいては，各 3 次元モデルがおよそ同じサイズになるようにスケール変換を施している．スケール変換の具体的な方法は 4.4.1.2 項(2)を参照されたい．

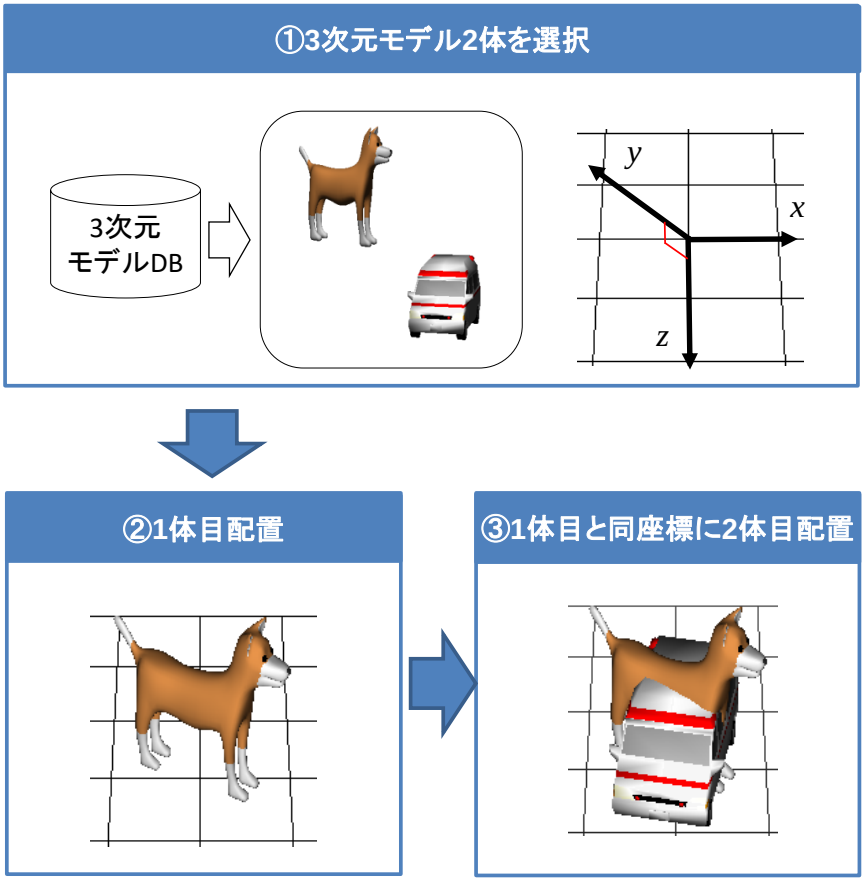

図 4-3　非現実モデルの生成手順

4.3　認証手順

非現実画像 CAPTCHA の認証手順を以下に示す．なお，システムの 3D モデルデータベースには Web 上から収集した通常の 3D モデルが大量に登録されていることを前提とする．1 枚の問題画像中に含まれるモデルの個数 N はセキュリティパラメータである．

① システムは，3D モデルデータベースの中から N+1 体のモデルをランダムに選ぶ．
② システムは，①で選んだ N+1 体のモデルの中から，ランダムに 2 体のモデルを選択する．
③ システムは，②で選んだ 2 体のモデルに対して，それぞれアフィン変換を施すことによってスケールの変更と回転を行う．
④ システムは，③で変換したモデル 2 体を 3D 空間平面 α の任意の同一座標へ配置する．これは，4.2 節で示した手順そのものであり，非現実モデル 1 体を画像中に配置する操作にあたる．

⑤ システムは，①で抽出したモデル N+1 体のうち，②で使用していないモデル N-1 体に対して，以下の処理を行う．
(ア)各モデルにアフィン変換を施すことによってスケールの変更と回転を行う．
(イ)3D 平面 α 上へ，それぞれが衝突しないように配置する．
⑥ システムは，3D 空間平面 α 上のモデル群を 2D 画像へ投影することによって，CAPTCHA の問題画像を生成する．
⑦ システムは，⑥の問題画像をユーザに提示する．
⑧ ユーザは，問題画像中の不自然な部分，すなわち，2 体のモデルがめりこんで生成されている非現実モデルをクリックする．
⑨ システムは，正答できたユーザを人間，正答できなかったユーザをマルウェアとして判別する．

本手順で生成した非現実画像 CAPTCHA の問題画像の例（N=8）を図 4-4 に示す．図 4-4 では，画面中央右に犬と車がめりこんだ非現実モデルが配置されている．

図 4-4　非現実画像 CAPTCHA（N=8）の問題画像例

4.4　ユーザビリティ実験

提案方式を実装した実験環境を構築・実験し，非現実画像 CAPTCHA を人間が正解容易か（複数の通常モデルの中に紛れる非現実モデルをユーザが容易に見つけることができるか）について検証する．

4.4.1　実装

今回の実験環境では，次のような制約の下で提案方式を実装した．

4.4.1.1　3D モデルに関する制約

非現実画像の作成にあたっては，次に示す制約を満たす 3D モデル（以下，通常のモデル）を使用する．

1. 多くのユーザが見たことがないであろうモデルは含まれない．たとえば，世間の認知度が極めて低い特異なアニメキャラクタは含まれない．多くのユーザが見たことがないであろうモデルは，ユーザが，通常モデルか非現実モデルか区別できないためである．
2. 同じカテゴリに含まれるモデルは複数含まれない．たとえば，「草」のモデルが複数あった場合，それらが同一座標に配置されたとしても，単に草がうっそうと生えている通常モデルとして認識されてしまい，ユーザが「めり込み」を認識することが困難なためである．
3. 透明なモデルは含まれない．透明なモデルは，同一座標に配置した際に透けてしまうため，ユーザが「めり込み」を認識することが困難なためである．
4. 複数の独立したモデルから構成されるモデル（たとえば，図 4-5 は「テーブル」と「ソファー」から構成された単体の 3D モデルとなっている）は含まれない．モデル同士のめり込みが生じない（たとえば，「テーブルとソファー」と「傘」をめり込ませようとした場合に，テーブルとソファーの間に傘が配置されて，3 体の通常モデルのように見えてしまう）ことを避けるためである．

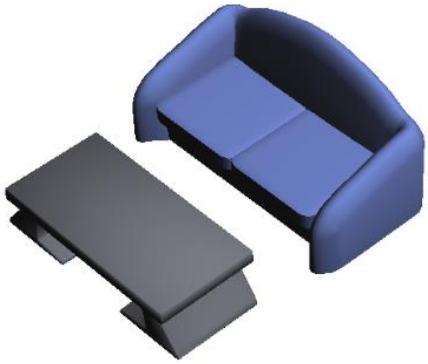

図 4-5　テーブルとソファーから構成されるモデル

4.4.1.2　画像生成に関する制約

提案方式においては，問題画像の生成にあたって，問題画像のサイズ，3D モデルのサイズ，3D 平面のサイズに関するパラメータ，ならびに，3D モデルに適用するアフィン変換のパラメータを設定する必要がある．今回は，システム実装にあたっての予備実験を行い，経験的に各パラメータに対して適正な値を定めた．それぞれの詳細について以下に述べる．

なお，提案方式は 3DCG を利用しているため，プログラム上の 3D 空間とディスプレイ画像上の 2D 空間の間でサイズの概念が異なる．たとえば，3D 空間内で xz 平面上に正方形を描画した場合，それが 2D 平面へ投影された形でディスプレイに表示されるため，ディスプレイ上ではその正方形は台形に映る[8]．以下，本論文内のサイズに関する記載は，個別の説明がない限り，3D 空間上の数値を表している．

(1) 問題画像のサイズ

今回実装した実験システムは，ブラウザ上で動作する．ブラウザに問題画像を表示したときに，ユーザがスクロールをする必要がない程度の大きさにするために，ディスプレイ上の問題画像のサイズが 600×480 画素となるように設定した．左上が第(0,0)画素，右下が第(599,479)画素である．

(2) 3D モデルのサイズ

画像上に表示させる各モデルは，大きさをある程度統一しなければならない．たとえば，画面上に巨大なモデルが一つ存在した場合，そのモデルが画面全体を覆ってしまうことで，他のモデルが隠れてしまうといった現象が発生する．あるいは，二つのモデルを同じ座標に配置した際，片方のモデルがもう一方に埋め込まれてしまって，お互いにめり込んだモデル（非現実モデル）が表示されないといった状況も発生し得る．そこで，3D モデルは，各モデルをデータベースから読み込んだ際に，簡易的なサイズの正規化処理を行うことで大きさを調整している．具体的なサイズ正規化手順は以下のとおりである．

① 平面 α の原点(0,0)にモデルを配置する．
② 1 辺の長さが一定の値（今回は 1.5 とした）の立方体に収まるようにモデルを拡大縮小する．
③ モデルを Y 軸に対して，15 度刻みで 360 度回転させる．その際に，画面上の投影面積（3D モデルを 2D 画面に投影した際の 2D 画像の面積）が一定の値（今回 5000 平方画素とした）以上となる角度があった場合，その都度，モデルの大きさを一定の倍率（今回は 0.9 倍とした）で縮小する．

(3) 3D 平面のサイズ

提案方式は，3D 平面 α 上にモデルを配置する形式をとっている．平面 α に配置されるモデル数に依らず平面 α の面積が一定となっていると，モデル数の多少によってモデルの密集度が変化してしまう．そこで，画像中のモデル数が N体の時，モデルが配置される平面 α の大きさは，原点を中心とした面積 Nの正方形（一辺の長さは$\sqrt{N}$）とした．

[8] 今回使用した実験システムにおいては，3 次元空間上の原点を中心に 1×1 の大きさの正方形を xz 平面に描いた場合に，ディスプレイ画面上では上底 83 画素，下底 90 画素，高さ 48 画素の台形として表示された．

(4) アフィン変換

提案方式では，生成される画像の多様性を増やすために，4.3 節の手順③や手順⑤（ア）にて各モデルにアフィン変換（サイズ変換および回転）を施している．サイズ変換については，モデルが大きくなり過ぎて平面 α 上にすべてのモデルが配置できなくなったり，モデルが小さくなり過ぎて手前のモデルの陰に後方のモデルがすべて隠れてしまったりしないように，スケール変換の倍率は 1.0~1.3 の間に制限した．また，3D モデルの中には，後ろを向いた場合（Y 軸に対して約 180 度回転した場合）に，そのモデルが何であるかを認識することが難しいものも存在する．このため，各モデルの回転については，Y 軸に対して±90 度以内となるように制限した．

4.4.1.3 衝突判定に関する制約

3D 平面 α 上で各モデルが重ならないように配置するために，各モデルを配置する際には簡易的な衝突判定を行い，互いに重なっていないかを確認する必要がある．今回は実装の簡素化のために，各モデルが内接する最小の直方体を生成し，それらの直方体同士が衝突しているか否かを判定する方法を採用した．

4.4.2 実験

4.4.2.1 諸元

複数の通常のモデルの中に紛れる非現実モデルをユーザが容易に見つけることができるか否かを回答時間と正答率の視点から評価する．そのための実験諸元は次のとおりである．

使用する 3D モデルは，4.4.1.1 項の条件を満たす mqo 形式[64]のモデル 34 体を Web 上から収集し，実装システムへ登録した．

被験者は，情報セキュリティ系の研究室に所属する学生 10 名である．被験者には，画像中のモデル数 N が 4，8，12，16 のケースに対して各 5 問，計 20 問の非現実画像 CAPTCHA を解くよう求めた．それぞれのケースの問題画像例を図 4-6～図 4-9 に示す．計 20 問の問題画像は，実験実施前にあらかじめ自動生成した後，20 問の順序をランダムにシャッフルして先頭から順に出題した．

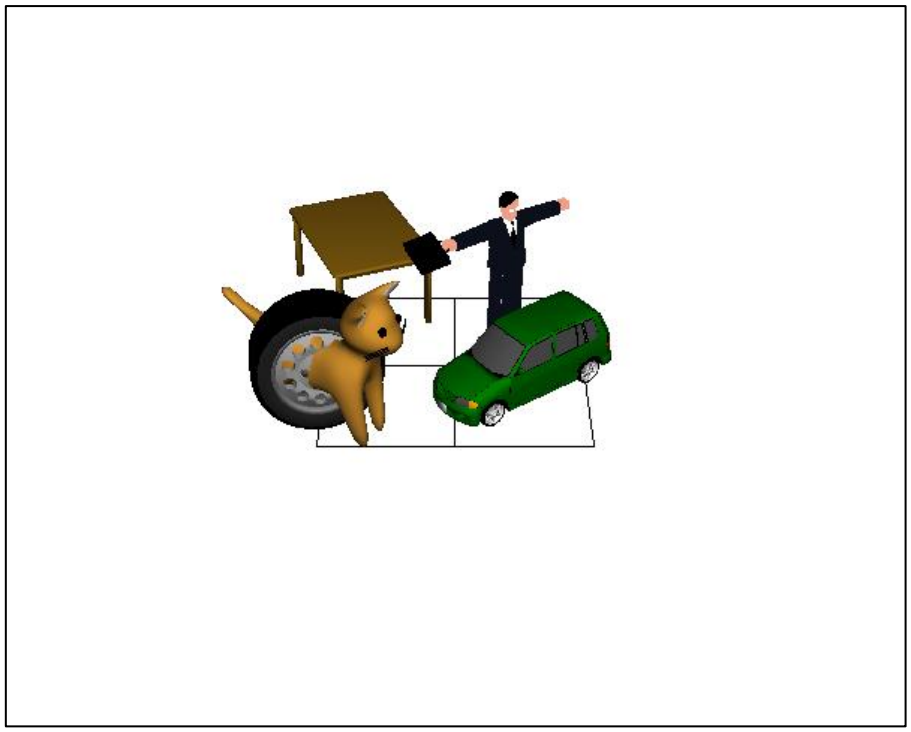

図 4-6　非現実画像 CAPTCHA：ユーザビリティ実験で使用した問題画像例（N=4）

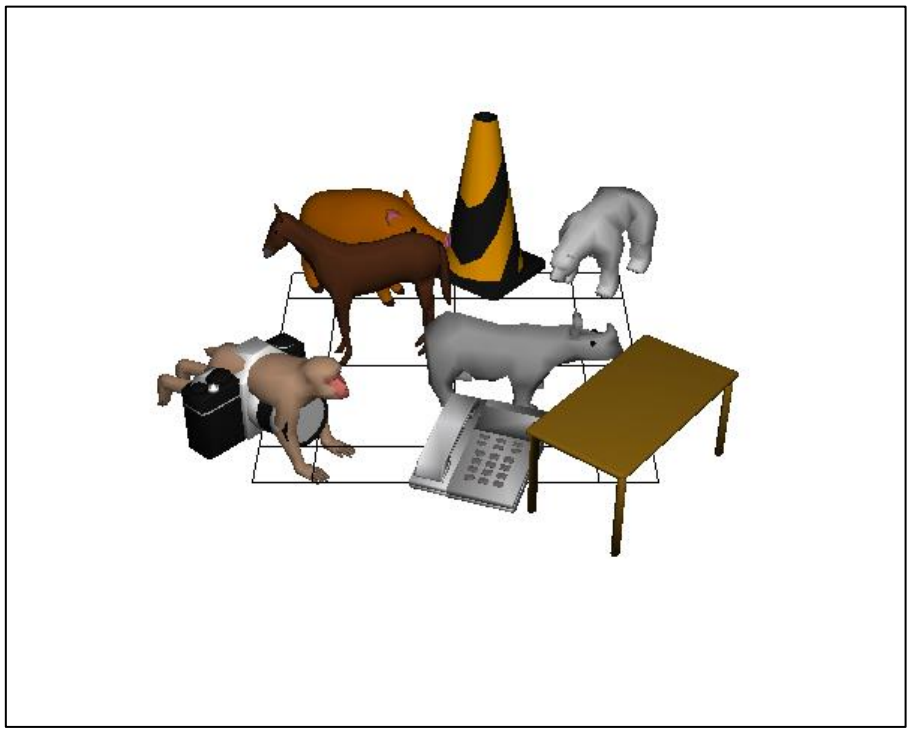

図 4-7　非現実画像 CAPTCHA：ユーザビリティ実験で使用した問題画像例（N=8）

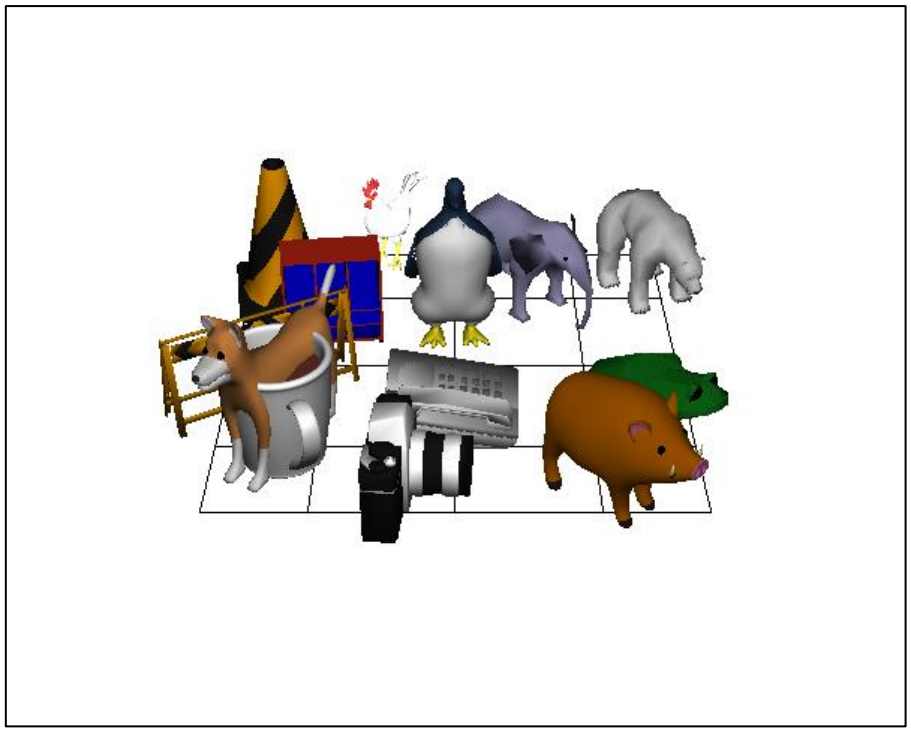

図 4-8　非現実画像 CAPTCHA：ユーザビリティ実験で使用した問題画像例（N=12）

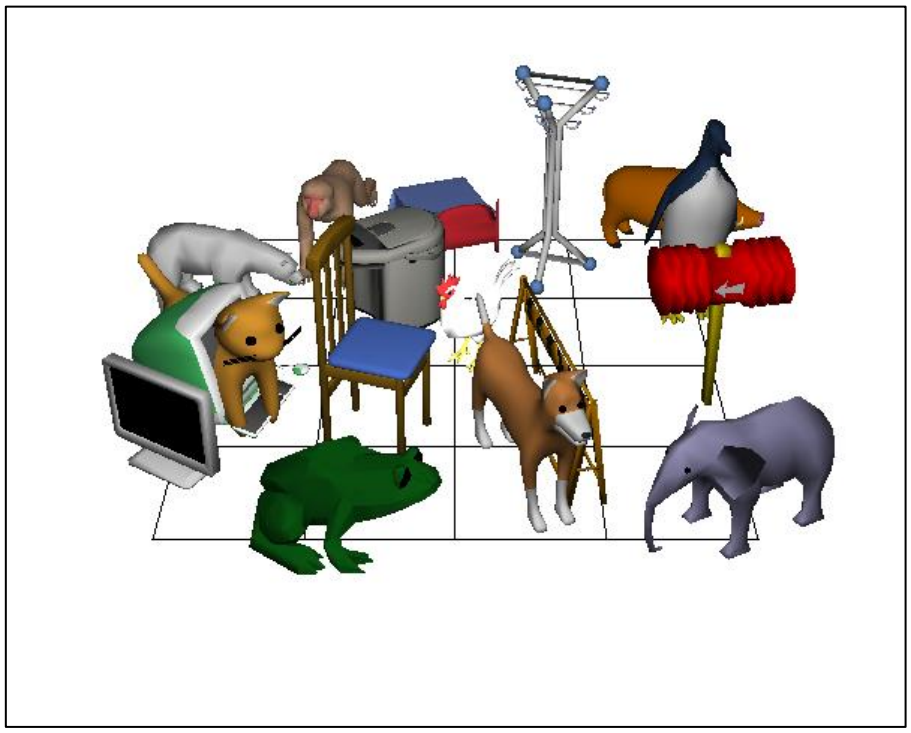

図 4-9　非現実画像 CAPTCHA：ユーザビリティ実験で使用した問題画像例（N=16）

実験システムの操作に慣れるため，各被験者は 20 問の実験の前に，各被験者が十分と思えるまで練習を繰り返すことを許した．練習では，毎回問題を自動生成した．練習における問題画像 1 枚あたりのモデル数は N=4，8，12，16 のうちいずれかのモデル数が任意に選択される．

被験者には，提示された CAPTCHA 画像中から「めりこんでいるモデル」をマウスでクリックするように指示をした．被験者がめり込み合っている 2 体のモデルのどこか一部分でもクリックした場合に正解と判定した．

4.4.2.2 結果

ユーザごとの正答率と 1 問当たりの平均時間をまとめた結果を表 4-1，図 4-10，図 4-11 に示す．これらの表や図より，提案方式の 1 問あたりの正答率は N=4，8，12，16 すべてで 9 割以上であることが分かる．また，1 問当たりの平均時間はモデル数に伴って増加する傾向がみられるが，もっとも長い 16 体でも約 5.5 秒である．

表 4-1　非現実画像 CAPTCHA：ユーザビリティ実験結果（表）

	4 体		8 体		12 体		16 体	
被験者	正答率	平均時間 [s]	正答率	平均時間 [s]	正答率	平均時間 [s]	正答率	平均時間 [s]
1	4/5	4.6	4/5	7.4	5/5	3.0	5/5	3.8
2	5/5	2.2	5/5	3.0	5/5	2.4	5/5	5.0
3	5/5	2.3	5/5	2.9	4/5	5.4	5/5	7.1
4	5/5	2.4	5/5	2.9	4/5	7.6	5/5	10.0
5	5/5	2.3	5/5	1.6	5/5	2.2	5/5	2.7
6	5/5	1.9	4/5	2.9	4/5	7.9	4/5	2.6
7	5/5	1.8	5/5	3.1	5/5	5.5	5/5	14.7
8	5/5	1.4	4/5	1.7	4/5	2.7	5/5	3.0
9	5/5	1.8	5/5	2.9	5/5	2.1	4/5	2.8
10	5/5	1.8	4/5	3.3	4/5	3.6	4/5	3.7
平均	98.0%	2.2	92.0%	3.2	90.0%	4.2	94.0%	5.5
標準誤差	2.0%	0.28	3.3%	0.50	3.3%	0.70	3.1%	1.26

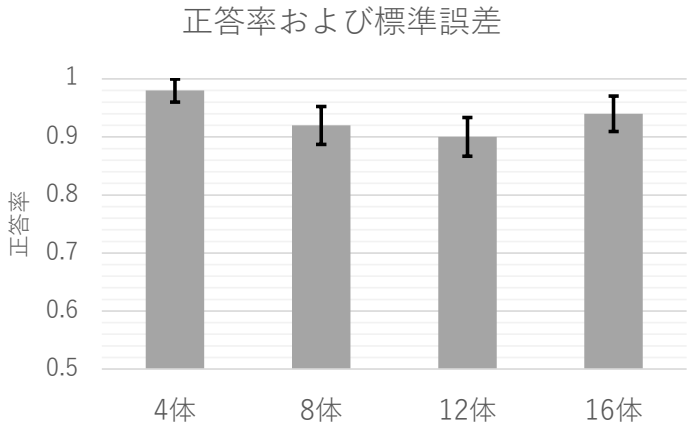

図 4-10　非現実画像 CAPTCHA：ユーザビリティ実験結果（正答率のグラフ）

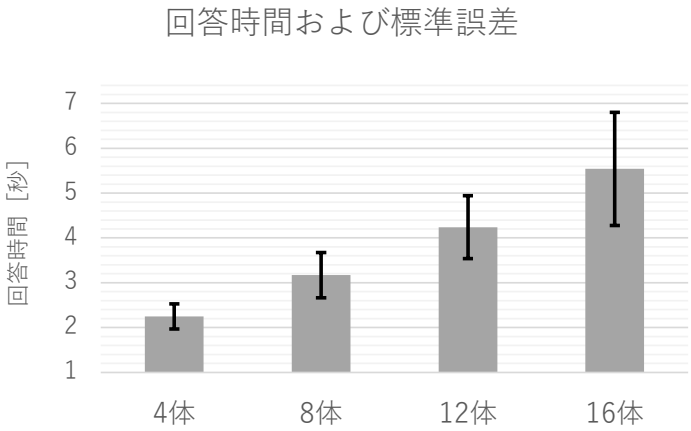

図 4-11　非現実画像 CAPTCHA：ユーザビリティ実験結果（回答時間のグラフ）

4.4.3　考察

提案方式のユーザビリティを「正答率」と「回答時間」から考察を行う．

4.4.3.1　正答率

表 4-1 より，提案方式の 1 問あたりの正答率は N=4，8，12，16 すべてで 9 割以上の値を有している．一般で利用されている文字判読型 CAPTCHA の平均正答率が 1 問あたり約 92%であることに鑑みれば[31]，その値と同程度以上であり，十分高い値であるといえるだろう．

さらに，本実験で行った 4 つの群と第 3 章で行った（3DCG 画像 CAPTCHA の基本形態である）類似モデルなし／ありの YUNiTi 型 CAPTCHA の実験結果 2 群，計 6 群の間で Steel-Dwass 法で統計値を求めたところ，提案方式と YUNiTi 型 CAPTCHA 間の各統計値は，表 4-2 のとおりの結果となった．本結果からは，類似画像選択型攻撃や 3D モデル認識攻撃を有しているという状況下では，YUNiTi 型 CAPTCHA と比較して，十分に簡単に解ける形式であることがわかる．ただし，第 3 章で実施した実験と本章で

行った実験では，実験条件や被験者属性等が異なるため，参考情報として掲載していることに注意されたい．

表 4-2　非現実画像 CAPTCHA と YUNiTi 型 CAPTCHA の正答率の検定（*p<.05）

	類似モデルなし YUNiTi 型 CAPTCHA	類似モデルあり YUNiTi 型 CAPTCHA
非現実画像 CAPTCHA　N=4	0.718	0.001*
非現実画像 CAPTCHA　N=8	0.034*	0.008*
非現実画像 CAPTCHA　N=12	0.009*	0.015*
非現実画像 CAPTCHA　N=16	0.113	0.004*

提案方式において，被験者が誤答した試行には，以下の 4 つの原因が見られた．以下，原因とその対策法について議論する．

1 つ目の原因は，被験者のクリック位置のずれである．正解モデルを認識することはできたものの，クリック位置のわずかなずれによって不正解となった問題があった．正解範囲をモデルより一回り大きな範囲にすることによって対策が可能である．

2 つ目の原因は，画像中に含まれる遮蔽関係を「めり込み」と勘違いした事例である．今後，評価を繰り返すことで，ユーザが遮蔽とめり込みの誤認を起こしやすい条件を探り，問題画像中に遮蔽関係となる部位が含まれる状況を維持しつつ，ユーザが誤認しないであろう工夫を見つける必要がある．なお，画像中に遮蔽関係となる部位が存在しないように各モデルを配置することは可能であるが，遮蔽の存在がマルウェアによるめり込み部位の検出を難しくしている（4.5.1 項で詳細を論ずる）．したがって，遮蔽関係となる部位が含まれる状況を維持しつつ，ユーザに誤認をおこさせない工夫が必要となることに注意されたい．

3 つ目の原因は，モデル同士のめり込みがほとんど起きていなかったため，「非現実モデル」を画像中から発見できなかった場合である．今回は，4.2 節に示したとおり「同一座標に 2 つのモデルを配置する」ことで非現実モデルを生成している．しかし本方法では，モデルの組み合わせによっては，図 4-12 のように 2 つのモデルがわずかにしかめり込まない場合があった．これについては，モデル同士の衝突判定によって対策可能である．たとえば，文献[65]では，各モデルを複数の立方体あるいは球で近似した後，二つのモデル間を構成する立方体や球が互いにどの程度衝突しているかを調査する方法が提案されている．

4 つ目の原因は，通常のモデルを非現実モデルと誤認した場合である．この認識誤りは基本的に対策が困難であるが，人間が誤認識しやすいモデルについて今後条件を調査する必要がある．

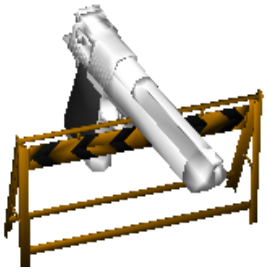

図 4-12　非現実画像 CAPTCHA：被験者の失敗原因 3 の事例

4.4.3.2　回答時間

平均時間は，もっとも長い 16 体の場合でも，1 問あたり約 5.5 秒であった．文字判読型 CAPTCHA の 1 問あたりの平均時間は 12 秒程度であるため[31]，提案方式は比較的短時間で解ける CAPTCHA であるといえるだろう．

さらに，本実験で行った N=4 の実験結果と第 3 章で行った（3DCG 画像 CAPTCHA の基本形態である）類似モデルなし／ありの YUNiTi 型 CAPTCHA の実験結果 2 群，計 3 群間で Steel-Dwass 法で統計値を求めたところ[9]，提案方式と YUNiTi 型 CAPTCHA 間の各統計値は，表 4-3 に示す結果となった．本結果は，類似画像選択型攻撃や 3D モデル認識攻撃に耐性を有しているという状況下では，YUNiTi 型 CAPTCHA と比較して，十分に素早く解けることを示している．また，類似モデルなし YUNiTi 型 CAPTCHA と同程度の時間で解けることが示唆される．ただし，第 3 章で実施した実験と本実験では，実験条件や被験者属性等が異なるため，正答率と同様に，参考情報としての掲載であることに注意されたい．

表 4-3　非現実画像 CAPTCHA と YUNiTi 型 CAPTCHA の認証時間の検定（*p<.05）

	類似モデルなし YUNiTi 型 CAPTCHA	類似モデルあり YUNiTi 型 CAPTCHA
非現実画像 CAPTCHA　N=4	0.554	0.000*

被験者が時間を要した問題に関して，実験終了後に被験者にその理由を尋ねたところ，そのほとんどが「遮蔽関係となっている部位と非現実モデルを見分けるために時間を要した」という理由であった．4.4.3.1 項で述べた「問題画像中に遮蔽関係となる部位が含まれる状況を維持しつつ，その中から非現実モデルを見つけやすくする工夫」は，提案方式の回答時間の短縮にも効果があることが期待される．

[9] 認証時間は，画像中で利用されている 3D モデルの数によって変化する可能性が高い．第 3 章で実験した YUNiTi 型 CAPTCHA は 5 体のモデルを使用しており，提案方式の N=4 でも 5 体のモデルを使用している．これら 2 つの群は使用されているモデル数が統一されているため，これらの 2 つの群間で比較を行った．

4.4.4　注意点

前節までの議論は，今回の実験環境下の議論である．実運用に向けては，データベース内の 3D モデルを増やす等の改定が必要であり，正答率や回答時間が変化する可能性が大いにある．今後，実運用に近づけた状態で提案方式の攻撃耐性についても調査する必要がある．

4.5　攻撃耐性

「複数の通常のオブジェクトの中に紛れる非現実オブジェクトを選択する」という形式を利用した提案方式に対しては，類似画像選択攻撃や 3D モデル認識攻撃といった単純な攻撃を適応することはできない．しかし，機械はこれら攻撃に加えて，めり込みの認識や総当たり攻撃を利用することで突破を試みるであろう．本節では，これらの攻撃手法を議論することによって，非現実画像 CAPTCHA の機械解読耐性について検証する．

4.5.1　めり込みの検出

4.5.1.1　攻撃方法

提案方式に対する攻撃としては，問題画像の一部を切り取り，「画像中に複数のモデルから生成されているモデルが存在するか否か」を検出する攻撃が考えられる．すなわち，機械は画像の一部が自然かどうかは分からないが，モデル同士の「めり込み」を検出しようと試みる攻撃である．具体的な攻撃シナリオは以下のとおりである．

① 攻撃者はあらかじめ大量の問題画像を入手する
② 入手した問題画像から，「問題画像の一部を切り出した画像」と「その部分に正解（すなわち，めり込んでいる部分）が存在するか否か」という教師用データセットを大量に用意する．
③ ②のデータセットを教師データとして機械学習を行い，提案方式に対する分類機（画像中に「めり込みが含まれるか否か」を判定する分類機）を構築する．
④ ③で構築した分類機を実装した自動プログラム（マルウェア）を作成し，これをインターネットに放つ．この自動プログラムは，CAPTCHA の問題画像に対し，次々と一部を切り取ってめり込んだ部分を探すという試みを繰り返す．

4.5.1.2　めり込み検出に対する仮説

4.1 節に示したとおり，機械がめり込みを検出しようとした際には，通常のモデル同士の遮蔽関係やめり込んだ自然なモデルとめり込み関係が区別できずに，正解困難であると考えられる．本論文では，このうち「機械は，遮蔽関係とめり込み関係の区別が困難である」という仮説に対して検証を行う．この仮説が成り立った場合，問題画像中に遮蔽関係を構成するモデルがたくさん存在すればするほど，機械は画像中の「めり込ん

だ部分」を見つけることが困難となる．すなわち，4.5.1.1 項で示した攻撃シナリオでは，提案方式を突破できない可能性が高い．以下，攻撃者が提案方式に対して 4.5.1.1 項の方法で解読を試みた際に，上記仮説が成り立つであろうことを実験によって確かめる．

4.5.1.3　実験方法

「既存のモデル」に関するすべてのめり込み画像および遮蔽画像を学習したニューラルネットワークであっても，「新たなモデル」に関するめり込み画像と遮蔽画像を区別することは困難であることを確かめることで，機械にとってめり込みと遮蔽の区別が困難であることを示す．具体的には，

① 学習用の Nt 体のモデルから 2 体のモデルを選ぶすべての組合せ，および，2 体のモデルの回転角度のすべての組合せを尽くした形で，めり込み画像および遮蔽画像を生成する（以下，「全学習画像群」と呼ぶ）．
② 同様に，評価用の Ne 体のモデルから 2 体のモデルを選ぶすべての組合せ，および，2 体のモデルの回転角度のすべての組合せを尽くした形で，めり込み画像及び遮蔽画像を生成する（以下，「全評価画像群」と呼ぶ）．
③ 全学習画像群をニューラルネットワークに覚えさせることによって，「既存のモデルに関するすべてのめり込み画像および遮蔽画像を学習したニューラルネットワーク」を構築する．
④ ③のニューラルネットワークに対して，全評価画像群の識別検査を実施する．

という手順となる．

ここで，全学習画像群，全評価画像群の作成手順は以下のとおりである．

(1) めり込み画像（学習用）

① Nt 体の 3D モデルの中から 2 体のモデル Oi，Oj（i≠j）を選択する．
② モデル Oi と Oj のサイズを 4.4.1.2 項(2)の方法によって調整する．
③ モデル Oi を Y 軸に対して Ri 度回転する．同様に，モデル Oj を Y 軸に対して Rj 度回転する．
④ モデル Oi の内接する直方体を生成し，その底面の中心点が平面 α 上の原点(0,0)に一致するように Oi を配置する．Oj も同様に平面 α の原点(0,0)に配置する．これによって，Oi と Oj がめり込んだ非現実モデルが生成される．
⑤ ④で生成された 3D 空間平面 α 上の非現実モデルを 2D 画像へ投影する．これを 600×480 画素の画像（4.4.1.2 項(1)参照）上に描画し，(300,200)を中心とした 70×70 画素を切り出すことによって，めり込み画像のサンプルを得る．画像例を図 4-13(a)に示す．

(2) 遮蔽画像（学習用）

① Nt 体の 3D モデル（学習用めり込み画像のサンプルを生成する際に用いたモデルと同一である）の中から 2 体のモデル O'i，O'j（i≠j）を選択する．
② モデル O'i と O'j のサイズを 4.4.1.2 項(2)の方法によって調整する．

③ モデル O'i を Y 軸に対して R'i 度回転する．同様に，モデル O'j を Y 軸に対して R'j 度回転する．

④ モデル O'i が内接する直方体を生成し，その底面の中心点が平面 α 上の原点(0,0)に一致するように O'i を配置する．O'i を構成するすべての頂点(x,y,z)の中で，x の最小値を *ximin*，x の最大値を *ximax* とする．

⑤ モデル O'i が xy 平面と接するまで，O'i を－z 方向に平行移動する．

⑥ モデル O'j が内接する直方体を生成し，その底面の中心点が平面 α 上の座標(*ximax*/2,0)に一致するように O'j を平面 α 上に配置する．

⑦ O'j が O'i と接する位置まで，O'j を z 方向に平行移動する．図 4-14 に手順④～⑦の手順に関するイメージ図を示した．図 4-14 は xz 平面を上側から俯瞰した図となっている．

⑧ 3D 空間平面 α 上のモデル 2 体を 2D 画像へ投影する．これを 600×480 画素の画像（4.4.1.2 項(1)参照）上に描画し，(300,200)を中心とした 70×70 画素を切り出すことによって，O'i の右側手前に O'j が配置された遮蔽画像（以下，「右側遮蔽画像」と呼ぶ）のサンプルを得る．画像例を図 4-13(b)に示す．

⑨ ①から⑧の手順を実行するにあたり，⑥において，モデル O'j の底面の中心点が平面 α 上の座標(*ximin*/2,0) に一致するように O'j を平面 α 上に配置する．これによって，O'i の左側手前に O'j が配置された遮蔽画像（以下，「左側遮蔽画像」と呼ぶ）のサンプルを得る．画像例を図 4-13(c)に示す．

(a)　(b)　(c)

図 4-13　機械学習用データ

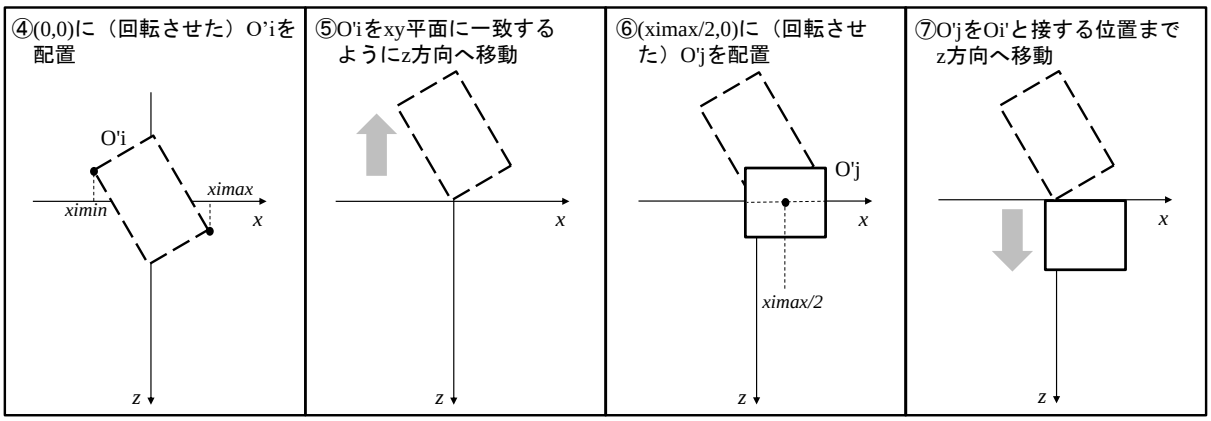

図 4-14　遮蔽画像生成イメージ図

(3) めり込み画像（評価用）

学習用めり込み画像（および遮蔽画像）を生成するために使ったモデルとは異なる Ne 体の 3D モデルを用いること以外は，学習用めり込み画像の生成手順と同じである．

(4) 遮蔽画像（評価用）

評価用めり込み画像を生成するために使ったモデルと同一の Ne 体の 3D モデルを用いること以外は，学習用遮蔽画像の生成手順と同じである．

4.5.1.4　実験諸元

Caffe[66]を利用することで，深層学習を用いて実験を行う．深層学習を行う際のネットワークモデルは，Caffe に付属しているリファレンスモデルを生成した際に用いられた設定ファイル群を用いた．ただし，今回の入力データの条件に合うよう，クラス数，入力画像のサイズに関わる部分については適切に設定を書き換えた．繰り返し数は 500[batch]，1[batch]の画像データ枚数は 128 に設定した．本実験では，Nt と Ne は 3 とした．すなわち，使用するモデルは学習用 3 体，評価用 3 体の計 6 体である．モデルは 4.4.1.1 項のモデル 34 体の中からランダムに選んだ．また，Ri および Rj は{0, 30, 60, 90, 120, 150, 180, 210, 240, 270, 300, 330 度}，R'i および R'j は{0, 60, 120, 180, 240, 300 度}とした．したがって，全学習評価画像群および全評価画像群の総数はどちらも 864 枚（めり込み画像 432 枚，右側遮蔽画像 216 枚，左側遮蔽画像 216 枚）である[10]．

4.5.1.5　実験結果

全学習画像群をニューラルネットへ学習させた結果，全学習画像群を入力した際に 99.8%（めり込み画像を入力して正しく「めり込み画像である」と判定する割合：100.0%，遮蔽画像を入力して正しく「遮蔽画像である」と判定する割合：99.5%）の正解率を有する識別機が構築された．その識別機へ全評価画像群を入力したところ，その正解率は 69.6%（めり込み画像を入力して正しく「めり込み画像である」と判定する割合：47.7%，遮蔽画像を入力して正しく「遮蔽画像である」と判定する割合：91.4%）であった．

この結果からは，「遮蔽関係」と「めり込み」の区別は機械にとって困難であろうことがわかる．すなわち，本実験結果からは，4.5.1.2 項で示した仮説が正しいことがいえるであろう．

---

[10] ニューラルネットワークにめり込み画像と遮蔽画像の識別をバランス良く学習させるために，めり込み画像の枚数と遮蔽画像（右側遮蔽画像と左側遮蔽画像の和）の枚数を合わせるようにした．このため，Ri および Rj が 30 度刻み（0, 30, 60, 90, 120, 150, 180, 210, 240, 270, 300, 330 度）であるのに対し，R'i および R'j が 60 度刻み（0, 60, 120, 180, 240, 300 度）となっている．めり込み画像：3 体のモデルから Oi と Oj の 2 体を選ぶ組合せ ${}_3C_2$ 通り×モデル Oi の回転角度 12 通り×モデル Oj の回転角度 12 通り＝432 枚．右側遮蔽画像：3 体のモデルから O'i と O'j の 2 体を選ぶ組合せ ${}_3P_2$ 通り×モデル O'i の回転角度 6 通り×モデル O'j の回転角度 6 通り＝216 枚．左側遮蔽画像：同じく 216 枚．遮蔽画像：右側遮蔽画像＋左側遮蔽画像＝432 枚．

4.5.2　総当たり攻撃

提案方式に対する総当たり攻撃の耐性を分析するにあたって，分析を簡素にするために，問題画像中に配置されたすべてのモデルの見た目の面積がすべて同じだと仮定する．この場合，マルウェアが画像解析によって問題画像の中のすべてのモデルを抽出できたならば，マルウェアは，抽出したモデルの総数 N に対して，1/N の確率で正答することができる．すなわち，1 問あたりの総当たり数は N となる．なお，今回の実験結果では，N=16 としたとしても十分に高い正答率と短い回答時間を得られることを確認している．

CAPTCHA システムの運営者は，自身の CAPTCHA システムで必要な総当たり数を満たすよう，複数の問題をユーザへ出題し，その問題すべてをユーザに正解してもらう形で運用することとなる．たとえば，自身のシステムで総当たり数 4000 が必要で，N=4 の非現実画像 CAPTCHA を利用する場合，6 問の問題（4^6＝4096 である）を出題することとなる．

4.6　自動生成

本節では，非現実画像 CAPTCHA の問題画像の自動生成は容易であるか否かについて議論する．

提案方式では，4.3 節に示した手順のとおり，3DCG 技術を利用して毎回新しい問題画像を容易に生成することが可能であり，問題画像の完全な自動生成を実現している．Web 上から収集した多数の 3D モデルをシステムに登録しておき，使用するモデル，ならびに，モデルのパラメータ（サイズや回転角度）を変更することによって，問題画像を無数に生成することが可能である．

ただし，提案方式で利用可能な 3D モデルには，現状，4.4.1.1 項に示した 4 つの制約が課せられている．しかし，制約 3（透明なモデル）と制約 4（複数の独立したモデルから構成されるモデル）は，3D モデルの頂点情報や色情報から識別可能である．また，制約 2（同じカテゴリに含まれるモデル）については，3D モデル同士の頂点情報や色情報の類似度からある程度の識別は可能であることが期待される[67]．制約 1（見たことがないであろうモデル）については，世間の認知度が低いきわめて低い特異なアニメキャラクタでもあってもその多くは通常の形状をしており，提案方式の誤答に結びつくような「2 体の動物が合体したキメラ動物」のような 3D モデルは比較的少数であることが予測される．したがって，これらをルール化して 3D モデルを自動収集することは十分に現実的であるのではないかと考えられる．

無論，自動収集した 3D モデルの中に 4.4.1.1 項の 1～4 の制約を満たさないものが含まれる可能性は否定できない．しかし，その結果として，正規ユーザであっても答えに窮するような問題が出題されてしまった場合には，ユーザにリロードボタンをクリックしてもらうことで別の問題を出題するという運用による対策が可能である．

4.7　まとめ

本論文では,「視覚的形式知からの逸脱」を利用して発展させた 3DCG 画像 CAPTCHA として，非現実画像 CAPTCHA のコンセプト提案・実装・評価を行った．人間の正答率を確保しつつ，機械に対する高い攻撃耐性を有し，かつ，3DCG 技術を利用して問題画像の自動生成が容易である点が提案方式の特長である．ユーザビリティ評価のための実験において高い正答率が得られ，提案方式の有用性が示された．また，提案方式の攻撃耐性を評価した結果，機械学習，総当たり攻撃にも耐性を持ちうる方式であること確認した．さらに，問題の自動生成が実際に可能であることを述べた．

今後は，実運用に近づけた上で提案方式の可用性をより深く調査する必要がある．また，本論文では視覚的形式知からの逸脱を生成する方法について，二つのモデルをめり込み合わせる方法（不自然な重なりを利用する方法）を選択した．めり込み以外の方法（たとえば，「モデルの一部を削る」「モデルの一部を拡大する」等）を模索することで，より攻撃耐性が高い，または，より利便性が高い非現実画像 CAPTCHA を実現できる可能性もある．他方式の実装・実験・評価も今後積極的に進める必要がある．

第5章　2 方式を総括した議論

本論文で提案した 2 方式に関して，それぞれの方式における課題や展望は各章で述べた．本章では，2 方式に共通した課題や展望について論ずる．

5.1　更なる安全性検証

本論文で提案した二種類の CAPTCHA の安全性は，筆者が定義した攻撃者モデルに基づいた，定性的な議論，または，実験的評価によって示されたものである．しかし，マルウェアの攻撃手法は多種多様であり，提案した CAPTCHA に対する安全性検証は，引き続き行う必要がある．本節では，今後行うべき更なる安全性検証の方向性について議論を行う．

5.1.1　第三者の攻撃による検証

暗号学やプライバシの分野では，開発した暗号技術による暗号化データや匿名化技術による匿名化データを外部に公開をし，その技術に対して第三者に攻撃（解読）を試みてもらうことで，安全性を検証する試みが行われている．たとえば，RSA Scurity 社[68]は，自身が開発した暗号である RC5[69]に対して，攻撃をしかけてもらうコンテスト RC5 Cracking を開催することで，その安全性を検証していた[11]．プライバシの分野では，PWSCUP と呼ばれるコンテストが 2015 年から開催されている[70][71][72]．PWSCUP では，あるデータを自身の匿名化アルゴリズムによって匿名化したデータを公開し，そのデータに対して第三者に再識別を試みてもらう．その結果，どの程度再識別されるかを評価し，その匿名化アルゴリズムの安全性を評価する取り組みである．

前述のとおり，提案方式に対する攻撃者の攻撃手法は多種多様であり，攻撃者の攻撃方法をすべて網羅して安全性評価することは，個人あるいは一組織レベルでは困難である．提案方式の CAPTCHA に対しても，第三者に公開して，様々な攻撃を仕掛けてもらい，そのノウハウや結果を蓄積することで，提案方式に対する攻撃方法やその効果をより深く検証可能であると期待される．ただし，そのような枠組みを用意するためには，第三者が攻撃するにあたってのインセンティブを用意する必要がある[12]．

---

[11] このコンテストは「安全でない」ことを証明するために開催されたものである．このコンテストは，2017 年現在，すでに終了している．

[12] RC5 Cracking では，賞金を用意することでインセンティブを与えていた．PWS CUP では，コンテスト形式にすることで，参加者にインセンティブを与えている．

5.1.2 理論的な証明

現在のところ，提案方式の安全性は，実験的・定性的に検証されているに過ぎない．提案方式の安全性は，暗号分野における証明のように，理論的（数学的）に証明されることが理想である[13]．以下に，理論的な分析に向けて，筆者が現在までに検討した内容を述べる．

理論的な証明に対するアプローチの一つの可能性として，暗号の分野における「リダクション」と呼ばれる証明技法を利用することが挙げられる．リダクションでは，「すでに困難であることが知られている問題 A」と「困難であることを証明したい問題 B」があるとき，「問題 B が困難でない[14]→問題 A が困難でない」という命題が真であることを証明する．この時，命題が真となったならば，「問題 A が困難である」という既に知られた事実が矛盾してしまうため，「問題 B が困難でない」という仮定が間違っていることとなる．すなわち，「問題 B が困難である」ということが証明されることとなる．本技法を利用することで，Rabin 暗号の安全性証明[73]や Elgamal 暗号の安全性証明[74]が可能であることが知られている．本アプローチを CAPTCHA の安全性証明に適用できた場合，機械にとって解くことが困難であるとすでに知られている問題を A，安全性を証明したい CAPTCHA を B と定義したうえで，「機械が B（CAPTCHA）を解くことが困難であること」を証明することが可能である．

前述のとおり，現在までに検討した内容は，理論的な証明に向けたアプローチの可能性を示したに過ぎない．上記の議論をベースとして，理論的な証明に実現に向けては，更なる検討が必要である．

5.2 3D モデルを特定する攻撃に関して

今回提案した 3DCG 画像 CAPTCHA 方式は，Web 上から収集した大量の 3D モデルをデータベースに格納しておき，それらを素材として利用することで問題画像を生成している．本節では，収集した 3D モデルを特定する，あるいは，あらかじめ攻撃者が全モデルを収集するような攻撃について議論を行う．

5.2.1 Web 探索攻撃

攻撃者は，SS-CAPTCHA（2.2.1 項参照）への攻撃と同様，問題画像中で用いられている素材（3D モデル）を Web 検索によって特定しよう試みる可能性がある．しかし，Web 検索が SS-CAPTCHA の脅威となり得る理由は，SS-CAPTCHA がインターネット上から収集した文章を「無加工」のまま CAPTCHA の問題として利用しているからであ

---

[13] 筆者の知る限り，CAPTCHA の安全性を理論的に証明した先行研究は存在しない[86]．理論的な証明は，重要な検討課題である一方，特に解決困難な課題でもある．

[14] ここでは説明の簡素化のために「困難でない」と記したが，実際には「問題 B を多項式時間で解くアルゴリズムが存在する」などが利用される．

る．これに対し，提案方式は，インターネット上から収集した 3D モデルを「加工」することによって CAPTCHA を生成しているため，問題画像の中で使われているモデルを単純な Web 検索だけで特定することは容易ではないと考えられる．さらに，非現実画像 CAPTCHA については，問題画像中の 3D モデルを特定したうえで，「不自然な重なり」であるか否かを判定する必要がある点で，成功をより困難としている．

5.2.2　すべての問題をデータベースに蓄積する攻撃

攻撃者は，Web 上に存在する 3D モデルをすべて収集し，あらかじめ，あらゆる問題を生成してデータベースに格納しておくことで CAPTCHA を突破してくる可能性がある．この攻撃の脅威度に関しては，「攻撃者がモデルを収集し，あらゆる問題生成をするコスト」と「すでに流通しているモデルの量とモデルを増加させていくコスト」のバランスを考慮することで，今後，詳しく分析する必要がある．しかし，現在，3D モデルは大量に存在しており，日々急激に増加をしているため，あらゆる問題を想定してデータベースに格納するには，時間的にも費用的にも，莫大なコストが必要であると考えられる．

さらに，現在，3D カメラや 3D スキャナの研究開発が進められている（たとえば，EORA 3D[75]や Kinect Fusion[76]）．将来的には，これらがさらに進化した技術を利用することで，現在のカメラによる写真撮影のように，任意の 3D モデルを一般の人々が日々生成できる世の中になるであろう．このような 3D モデルの自動生成技術が一般的，かつ，容易となった暁には，それらを利用して，毎回新たな 3D モデルをシステム内で自動生成して利用することが可能である．各システムが独自のモデルを利用することが可能となることで，そのモデルを攻撃者が収集不可能な状況にすることができる．

5.3　リレーアタックに対する対策

不正者が，インターネットの第三者を利用して CAPTCHA を解読する「リレーアタック」が知られている．リレーアタックは，以下の手順で実施される．

① CAPTCHA サーバは，ユーザ X（自動プログラム）に CAPTCHA の問題を出題する．
② X は，出題された CAPTCHA の問題を，第三者（人間）Y に転送する．
③ Y は，転送されてきた CAPTCHA の問題を解き，その答えを X へ送信する．ここで，X は Y に CAPTCHA を解くことを依頼，あるいは，Y を騙して（Y が自主的に）解かせる必要がある．これを実現するための方法として，文献[77]には次の 4 つの方法が示されている．
   （1）ポルノ画像閲覧の対価として解かせる（ポルノアタック）[78]
   （2）報酬を支払って解かせる（労働者募集サイト）[79]

（3）トロイの木馬に感染させることで解かせる[80]
（4）ボットに感染させることで解かせる[81]

④ Xは送信されてきた答えを受け取り,①で出題されたCAPTCHAサーバへ送信する.

⑤ CAPTCHAサーバが受け取った答えは，②で第三者（人間）が解いた答えであるため，（通常）正解と判定される．すなわち，Xは正規ユーザ（人間）として判定される．

そもそもCAPTCHAは「人間には正解容易」な問題を利用しているため，CAPTCHAを第三者の人間に解かせる本攻撃は，根本的な対策が非常に困難である．リレーアタックに関する既存対策としては，X と Y の IP アドレスの違いを利用した方式[77]，CAPTCHAサーバ・X間，X・Y間の伝送遅延を利用した方式[82]が提案されている．しかし，前者は，ユーザが特殊なプラグインを入れる必要がある点，適用先が文字列判読型CAPTCHAに限定される点で課題がある．後者は，CAPTCHAサーバとX間の通信遅延を見積もる必要がある点，攻撃者がCAPTCHA・サーバX間での通信遅延を偽造してきた場合に耐性がない点で課題がある．これらの方式の課題を解決しつつ，提案方式にリレーアタックの耐性を付与する方法を検討する必要がある．

5.4 幅広い属性でのユーザ実験

第3章，第4章で実施したユーザ実験は，大学生を被験者として扱った．しかし，それぞれのCAPTCHAの正答率・回答時間は，年齢，性別，文化圏等の違いによって個人差がある可能性が高い．クラウドソーシングサービス（たとえば，Amazon Mechanical Turk[83]や Lancers[84]）を利用することで，実験者を増やしていくとともに,様々な被験者に対して実験を繰り返すことで,提案方式のユーザビリティをより広く調査する必要がある．

5.5 実運用化

本論文で提案したCAPTCHAに関して，今後，実運用性（実際のWebサービスで利用できること）を検証することも重要である．そこで，本節では，実運用を目的とした場合，本論文で提案したCAPTCHAがどのような位置づけにあるかを議論する．

提案方式は，問題の自動生成を実現しているため，問題を提供するサーバを実装することで，Web サービスにおいて実運用可能な CAPTCHA である．実運用を実現するフレームワーク概念図を図 5-1 に示す．図 5-1 に示すとおり，①3D モデルの収集，②問題作成，③出題正解判定の機能を備えたサーバ（CAPTCHA サーバ）を Web 上に公開しておく．各 Web サービスの管理者は，問題画像の取得と，正解判定を依頼する機能

を実装する．なお，リプレイ攻撃[85]に耐性を持たせるために，一度利用した問題は，再利用しないようにする必要があることに注意されたい．このように運用することによって，Web サービス開発者は文字列判読型 CAPTCHA と同様に，提案 CAPTCHA を利用することが可能となる．

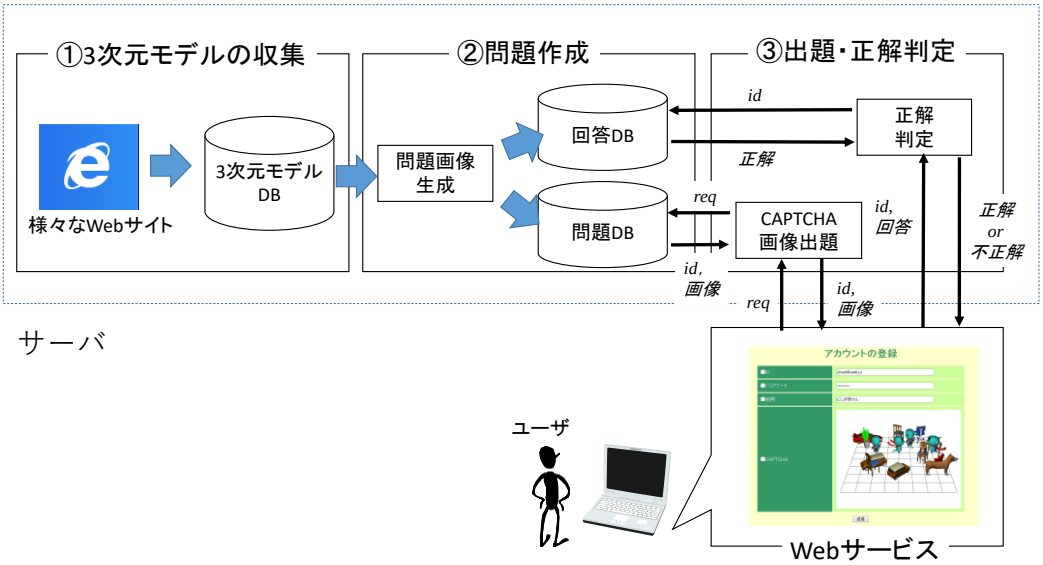

図 5-1　実運用におけるフレームワークの概念図

一方で，実運用に向けては以下の点について，実装上の課題が残っている．今後は，CAPTCHA 本体の検討のほかに，これらの点についても検討・開発を進める必要がある．

- 本研究で実装したシステムによって，「②問題作成」「③出題・正解判定」部がすでに実現されている．一方で，本研究では，3D モデルは筆者が Web 上から手作業で収集した．すなわち，自動的に「①3D モデルの収集」する機能を追加する必要がある．
- 本研究で利用した三次元モデルは，実装の簡素化のために，mqo ファイル形式の 3D モデルに限定している．すべてのファイル形式の 3D モデルから問題画像を生成できるよう，「②問題作成」部分を拡張する必要がある．

5.6　今後の発展方向

5.1 節に述べたとおり，提案方式の攻撃耐性については，今後さらに検証をしていかなければならない．加えて，今後も機械の計算機能力や認識能力の進化は続いていくため，攻撃耐性の検証は常時行わなければならない．これらの検証の中で，提案方式の安全性が危殆化してしまう可能性も十分に残る．本論文の最後の議論として，「提案方式

の安全性が危殆化してしまったとして」，今後どのような方向性で CAPTCHA を発展させていくべきか，筆者が考える現状の指針を論ずる．

① 動きや物理エンジンの利用

将来的には，3 次元モデルには「動き」の情報が付与されることが期待される．また，物理エンジンの発達によって，3 次元モデルに物理情報（重さなど）や物理的な動きが付与されることも期待される．これらのとおり 3D 技術が発達した暁には，あるモデルに違うモデルの動きをマッピングした「非現実な動きをするモデルを選択する CAPTCHA」であったり，「物理的に矛盾した動きをするモデルを選択する CAPTCHA」であったりといった，新たな CAPTCHA を実現することが可能である．

② 計算機援用型の CAPTCHA

パスワード認証における計算機援用ユーザ認証[87]や鍵生成における brcrypt[88]などで利用されているような，正規ユーザも，パスワード認証や鍵生成を行う際に計算機能力を利用する方式へと CAPTCHA を改良することが挙げられる．本アイデアをより詳細に説明するために，具体例として，文献[87]に示されている「計算機援用ユーザ認証の手順」を示す．

【計算機援用ユーザ認証の手順（基本形態）】

計算機援用ユーザ認証とは，認証情報の一部が正規ユーザにも未知となっていて，その未知情報を総当たり試行によって求めるというユーザ認証方式である．p_u はユーザが所持すべき秘密情報，p_r は総当り試行によって求める認証情報，p=p_u ∣p_r とする．登録フェーズにて，H(H(p))が認証サーバに登録されている．ここで，p_u ∣p_r は p_u と p_r のビット列の連結を表し，H(･)はハッシュ関数である．

1. サーバはクライアント端末に，H(H(p))を送信する
2. ユーザはクライアント端末に，p_u を入力する．
3. クライアント端末は H(H(p_u ∣p_r))と，H(H(p))が一致するような p_r を総当り試行によって探索する．
4. クライアント端末は，H(p_u ∣p_r)をサーバに送信する．
5. サーバは，H(H(p_u ∣p_r))と H(H(p))が一致したらユーザを認証する．

p_u と p_r のビット長をそれぞれ k_u，k_r とする．p_u を所持している正規ユーザは，未知である p_r のみを総当たり試行によって求める形となるため，負担する計算コストは最大で 2^(k_r)回である．一方，攻撃者にとっては p_u と p_r の両者が未知であるため，なりすましに必要となる総当たり試行は最大で 2^(k_u+k_r)回の計算コストとなる．

通常のパスワード認証では，秘密情報 p_u のエントロピは計算機能力の進化にともなって増加させなければならない．しかし，本方式では，認証時に，正規ユーザにも計算機能力の利用（総当たり）を求めている．これによって，計算機能力が進化したとしても，秘密情報 p_u のエントロピを増加させる必要がない方式になっている．

たとえば，「正規ユーザの計算コストが 1 秒，攻撃者の計算コストが 1 年となること」をセキュリティ要件とする．このとき，ある時刻 t1 おいて，この要件を満たすよう p_u と p_r のビット長 k_u，k_r を決定した後，時刻 t2 にて CPU の計算機能力が 2 倍になったとする．その時点で，p_r のビット長を k_r + 1 ビットに増やしてやるだけで（p_u のエントロピを増加させる必要なしに），「正規ユーザの計算コストが 1 秒，攻撃者の計算コストが 1 年」という状況が維持されることとなる．

以上のアイデアを CAPTCHA に応用した場合，CAPTCHA の問題を「人」と「最先端の機械」が協調しなければ，解けない問題へと改良することとなる．この場合，いかに機械が発達しようとも，「人」分のアドバンテージが，正規ユーザ（人間）には上乗せされるため，機械単独では解けない問題が実現されることが期待される．

第6章　まとめと今後の展望・課題

6.1　全体のまとめ

本論文では，人間に正解容易，機械に正解困難，問題の自動生成が容易な CAPTCHA を追求する上で，視覚的形式知を利用した 3DCG 画像 CAPTCHA に着目した．現状の視覚的形式知を利用した 3DCG 画像 CAPTCHA には，YUNiTi CAPTCHA という基本形態が存在するが，YUNiTi CAPTCHA には，類似画像選択攻撃や 3D モデル認識攻撃に対する脆弱性が存在した．3DCG 画像 CAPTCHA を発展させる方向性としては，「より精確な視覚的形式知を利用する」「視覚的形式知からの逸脱を利用する」という二つの指針があるが，3DCG 画像 CAPTCHA の発展においては，次に示す 2 つの課題が存在した．

① より精確な視覚的形式知を利用するという指針で発展させた 3DCG 画像 CAPTCHA として，Sketcha が現在までに提案されているが，1 問あたりの総当たり数が小さく，問題の自動生成のためにモデルに対して「上」という情報を付与する必要するがあるため，攻撃耐性や自動生成の観点で不十分である．

② 視覚的形式知からの逸脱を利用するという指針で発展させた 3DCG 画像 CAPTCHA の実現は，重要な研究課題であるものの，現在までに具体的な方式が提案されてない．

これら 2 つの課題それぞれを解決する，新たな 3DCG 画像 CAPTCHA を実現することを目的として研究を遂行した．具体的には，以下のとおりである．

第 2 章では，既存の「視覚的形式知を利用した CAPTCHA」を素材のモダリティによって分類した後，CAPTCHA を発展させる形式には，「より精確な視覚的形式知を利用する」「視覚的形式知からの逸脱を利用する」という二つ指針が存在することを明らかにした．その後，3DCG 画像 CAPTCHA に関する研究を行う重要性や意義を述べた後，上述した，既存 3DCG 画像 CAPTCHA の課題を明らかにした．

第 3 章では，上述の課題①を解決する方式として，より精確な視覚的形式知を利用した 3DCG 画像 CAPTCHA である「Locimetric 型 YUNiTi CAPTCHA」を提案・実装・評価した．Locimetric 型（単一の 3D モデルの中の特定部位を選択する方式）の出題形式を採用することで，YUNiTi CAPTCHA を改良した方式である．議論やユーザ実験を通じて，本方式が，既存 CAPTCHA より，人間に正解容易・機械に正解困難・問題の自動生成が容易であることを確認した．

第 4 章では，上記の課題②を解決する方式として，視覚的形式知からの逸脱を利用した 3DCG 画像 CAPTCHA である「非現実画像 CAPTCHA」を提案した．本方式は，3D モデルデータベースから任意に選んだ 2 体の 3D モデルをめり込み合わせることで「非現実モデル」を生成する．そして，複数の通常の 3D モデルの中に一体の非現実モデルを配置した一枚の画像を CAPTCHA 画像として出題する方式である．ユーザビリティ実験，機械学習実験，議論を通じて，本方式が，既存 CAPTCHA より，人間に正解容易・機械に正解困難・問題の自動生成が容易であることを確認した．

第 5 章では，2 方式を統括した議論を行った．その結果，「提案方式の更なる安全性評価手法」「実用化に向けた課題」等を明らかにした．これらは，本研究，および，CAPTCHA 研究全体の今後の研究課題を示したものである．

以上が本論文の貢献である．

6.2 今後の展望と課題

CAPTCHA は，今日のインターネット上で必要な不可欠な技術である．しかし，現在利用されている CAPTCHA はすでに非常に高い確率で解読されており，攻撃耐性が極めて低いと言わざるを得ない．このような背景のもと，本論文では，既存 CAPTCHA に代わる CAPTCHA を追求し，具体的な方式を提案・実装・評価した．本論文で提案した CAPTCHA は，いずれも（既存の CAPTCHA より），人間に正解容易，機械に正解困難，問題の自動生成容易な方式である．提案 CAPTCHA が将来的に Web 上で利用できるようになれば，すべてのインターネットユーザのスパムコメントやアカウントの不正登録に対する不安が大幅に軽減される．

ただし，各章に述べたとおり，各提案方式にはいくつかの課題が残っている．以下，各章にてそれぞれ述べた課題のうち，主な課題を改めて以下へ列挙する．

- Locimetric 型 YUNiTi CAPTCHA
  視点選択範囲の検討，正解範囲の検討
- 非現実画像 CAPTCHA
  めり込み以外の加工方法の検討
- 共通の課題
  様々な条件下でのユーザビリティ実験（登録モデルの増加，幅広い年代等），
  攻撃耐性の更なる検証，リレーアタックへの対策，実運用化

付録

A. スケール変換・回転角度の下限・線画化の対策を施した YUNiTi CAPTCHA の類似画像選択攻撃に対する耐性

A.1　目的

3.1 節にて，「マルウェアが『出題画像と最も類似した画像を探す』という戦略を採ることができる，オリジナルの YUNiTi CAPTCHA の場合は，スケール変換，回転角度の下限，線画化などの対策だけでは十分な対策効果が見込めない可能性が高い」と述べた．この点について著者らが調査を行った結果を記す．

A.2　実験諸元

5 体の 3D モデル（3.3 節で実装したシステムで使用したモデル A～E）を利用して，候補画像 5 枚（S1～S5）と問題画像 5 枚（T1～T5）を作成した．候補画像 S1～S5 は，モデル A～E をそれぞれ x 軸に対して反時計周りに 10 度，y 軸に対して時計周りに 30 度回転した上で，線画化（3.3.2 項(5)）を適用することによって生成されている（図 A.1 右）．問題画像 T1～T5 は，モデル A～E をそれぞれ x 軸に対して反時計周りに 10 度，y 軸に対して反時計周りに 15 度回転した（これによって，候補画像 Si と問題画像 Ti は，それぞれ y 軸に対して 45 度回転した画像となる）上で，x，y，z 軸方向にそれぞれランダムに 1.0～1.5 倍のスケール変換（3.3.2 項(2)）と線画化（3.3.2 項(5)）を適用することによって生成されている（図 A.1 左）．

「候補画像 S1～S5 の中から各問題画像 Ti（i＝1～5）に一番近い画像を選択する」というタスクを構成してやることによって，YUNiTi にスケール変換，回転角度の下限（45 度），線画化を適用した CAPTCHA をシミュレートすることができる．各問題画像 Ti（i＝1～5）に対して，パターンマッチングを用いて，候補画像 Sj（j＝1～5）の中から問題画像 Ti に一番近い画像を選択する．Ti に対して Si が選ばれる確度が高ければ，「YUNiTi にスケール変換，回転角度の下限，線画化を適用した CAPTCHA」は類似画像を選択するパターンマッチング攻撃に脆弱であるということになる．

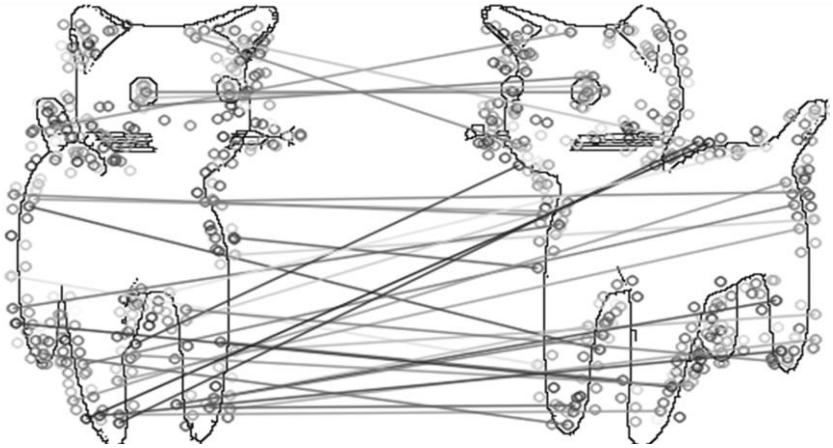

図 A-1　パターンマッチング（SURF）の結果の例

A.3　パターンマッチング手順

今回の調査では，以下の手順によって，候補画像 S1～S5 の中から問題画像 Ti に一番近い画像を選ぶ.

1. 問題画像 Ti に写っているモデルのサイズに合わせて，候補画像 S1～S5 の縮尺を正規化する．具体的には，モデルの x 方向の長さと y 方向の長さの内，大きいほうの長さをモデルのサイズと捉え，Ti と Sj のモデルのサイズが等しくなるように，S1～S5 を拡大縮小する，
2. 領域ベースマッチングによって Ti に近い Sj（j＝1～5）を選別する．領域ベースマッチングには種々の方法が考えられるが，今回はもっともシンプルな方法の一つである「面積比を求める」方法を利用した．具体的には，Ti の面積と Sj（j＝1～5）の面積を比較して，その差が θ_1 以下であれば「一致」と判定する．以下，手順 2 で一致と判定された候補画像を Sj*（j*＝1～5）と記す.
3. Sj*（j*＝1～5）に対し，特徴ベースマッチングによって Ti に最も近い Sj を選出する．今回は，特徴ベースマッチングにおいて，最もよく利用されている特徴量の一つである SURF[57]を採用した．具体的には，Ti と Sj*（j*＝1～5）のそれぞれの画像ペアに対して SURF を適用し，距離関数の値が閾値 θ_2 以下である特徴点対を抽出する．特徴点対の総数が最大となった画像 Sj を Ti に最も近い候補画像として選出する.

なお，閾値 θ_1，θ_2 は予備実験を通じて経験的に決定した．今回の各閾値の値は次のとおりである．θ_1＝12500，θ_2＝0.17.

A.4　実験結果

A.3 の手順により，各問題画像 Ti（i＝1～5）に対し，候補画像 Sj（j＝1～5）の中から一番近い画像を選択した結果，全問正解となる画像が選出された．この結果から，「YUNiTi にスケール変換，回転角度の下限，線画化を適用した CAPTCHA」は類似画像を選択するパターンマッチング攻撃によって突破されるケースがあることが確認された．

ただし，A.3 の手順 3 で実行した SURF によって抽出された特徴点対を確認したところ，問題画像のモデルと候補画像のモデルの各部位間の対応については，SURF はこれを確実には発見できていないことが認められた．実際の例として，問題画像 T1 と候補画像 S1 の SURF マッチングの結果を可視化した画像を図 A.1 に示した．図 A.1 左が T1，右が S1 であり，対応がとれた特徴点対が線で結ばれている．対応がとれた特徴点対の総数自体は多いため，A.3 の手順 3 のルールによって S1 が（T1 に一番近い画像として）正しく選出されたものの，部位間のマッチングとしては誤った結果が得られている箇所が少なくないことが分かる．これは，Locimetric 型（問題画像と候補画像の対応部位を解答する形式）の CAPTCHA である提案方式が，同じ部位を選択するパターンマッチング攻撃に耐性を有することを示す結果にもなっていることに留意されたい．

参考文献

[1] B. Bevans, B. DeBruhl, F. Khosmood : Understanding Botnet-driven Blog Spam: Motivations and Methods, Abstracts of Digital Humanities 2017（2017）.

[2] Security NEXT : 東京ガスの料金照会サイトに PW リスト攻撃 - 10 万回超のログイン試行（オンライン），入手先〈http://www.security-next.com/085400〉（参照 2017-10）

[3] Security NEXT : 会員サイトへ PW リスト攻撃、一部改ざんやポイント使用 - ロート製薬（オンライン），入手先〈http://www.security-next.com/085900〉（参照 2017-10）

[4] The Official CAPTCHA Site（オンライン），入手先〈http://www.captcha.net〉（参照 2017-10）

[5] Yahoo! JAPAN : Yahoo! JAPAN ヘルプ - 画像や音声による認証について（オンライン），入手先〈https://captcha.yahoo.co.jp/help/captcha_help.php〉（参照 2017-10）

[6] FC2 掲示板 : 不正防止機能（オンライン），入手先〈http://bbs.fc2.com/point5.html〉（参照 2017-10）

[7] J. Yan, A. S. E. Ahmad : Breaking Visual CAPTCHAs with Naive Pattern Recognition Algorithms, Proceedings of 2007 Annual Computer Security Applications Conference（2007）.

[8] Caca Labs : PWNtcha – captcha decoder（オンライン），入手先〈http://caca.zoy.org/wiki/PWNtcha〉（参照 2017-10）

[9] J. Yan, AS. EI Ahmad : Usability of CAPTCHAs or usability issues in CAPTCHA design, Proceedings of the 4th symposium on Usable privacy and security, pp.44-52（2008）.

[10] Gigazine : 無力感で心が折れそうなほどある意味ひどい認証用の CAPTCHA 画像まとめ（オンライン），入手先〈http://gigazine.net/news/20121218-captcha-fail/〉（参照 2017-10）

[11] D. A. Norman（安村通晃，岡本明，伊賀聡一郎，上野晶子訳）: 未来のモノのデザイン，新曜社（2008）.

[12] YUNiTi.com（オンライン），入手先〈http://www.yuniti.com/〉（最終参照 2014-12．注：2017-10 現在，サイト閲覧不可能）.

[13] CNET Japan : 3D ベースの CAPTCHA が登場--ソーシャルウェブサイトの YUNiTi.com が作成（オンライン），入手先〈https://japan.cnet.com/article/20390559/〉（参照 2017-10）
[14] S. A. Ross, J. A. Halderman, A. Finkelstein : Sketcha: A Captcha Based on Line Drawings of 3D Models, Proceedings of the 19th international conference on World wide web, pp.821-830（2010）.
[15] Sketcha（オンライン），入手先〈http://sketcha.cs.princeton.edu〉（参照 2017-10）.
[16] Yahoo! : ログイン（オンライン），入手先〈https://login.yahoo.co.jp/config/login〉（参照 2017-10）.
[17] K. Sawada, R. Uda : Effective CAPTCHA with Amodal Completion and Aftereffects, Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication（2016）.
[18] T. Azakami, C. Shibata, R. Uda : Challenge of Deep Learning against CAPTCHA with Amodal Completion and Aftereffects by Colors, Proceedings of the 19th International Conference on Network-Based Information Systems（2016）.
[19] T. Yamamoto, J. D. Tyger, M. Nishigaki : CAPTCHA Using Strangeness in Machine Translation, Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications, pp.430-437（2010）.
[20] 鴨志田芳典，菊池浩明：マルコフ連鎖による合成文書の不自然さを用いた CAPTCHA の提案と安全性評価，情報処理学会論文誌，Vol. 54，No. 9，pp. 2156-2166（2013）.
[21] Petfinder（オンライン），参照先〈https://www.petfinder.com〉（参照 2017-12）.
[22] J. Elson, J. R. Douceur, J. Howell, J. Saul : Asirra: A CAPTCHA that Exploits Interest-Aligned Manual Image Categorization, Proceedings of the 14th ACM conference on Computer and communications security, pp.366-374（2007）.
[23] P. Golle : Machine learning attacks against the Asirra CAPTCHA, Proceedings of the 15th ACM conference on Computer and communications security, pp.535-542（2008）.
[24] 飯田貴章，藤本衡：ASIRRA システムに対する機械的な突破の検証，日本ソフトウェア科学会第 31 回大会講演論文集（2014）.
[25] G. Goswamia, B. M. Powell, M. Vatsa, R. Singh, A. Noore : FaceDCAPTCHA: Face detection based color image CAPTCHA, Future Generation Computer Systems, Vol.31, pp.59-58（2014）.

[26] F. Schroff, D. Kalenichenko, J. Philbin : FaceNet: A Unified Embedding for Face Recognition and Clustering, Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition 2015（2015）.

[27] 林健太郎 , 羽下哲司, 関真規人 , 笹川耕一 : 映像監視における人物位置行動の検出技術, 情報処理学会論文誌, Vol.47, No.SIG9 (CVIM14), pp.12-20 (2016).

[28] S. Vikram, Y. Fan, G. Gu : SEMAGE: a new image-based two-factor CAPTCHA, Proceedings of the 27th Annual Computer Security Applications Conference, pp.237-246（2011）.

[29] M. Chew, J. D. Tygar : Image Recognition CAPTCHAs, Proceedings of the 7th International Information Security Conference, pp.268-279（2004）.

[30] Confident Technologies : Confident CAPTCHA, 入手先〈http://confidenttechnologies.com/confident-captcha/〉（参照 2017-10）.

[31] 可児潤也, 鈴木徳一郎, 上原章敬, 山本匠, 西垣正勝 : 4 コマ漫画 CAPTCHA, 情報処理学会論文誌, Vol.54, No.9, pp.2232-2243（2013）.

[32] 植田まさし, 新コボちゃん 8, 芳文社（2006）.

[33] R. N. Shepard, L. A. Cooper : Mental images and their transformations, The MIT Press（1986）.

[34] R. N. Shepard, J. Metzler : Mental rotation of three dimensional objects, Science, New Series, Vol.171, No.3972, pp.701-703（1971）.

[35] Animiertes Sicherheitsfeld - animierte Captcha - grafischer sicherheitscod（オンライン）, http://www.animierte-captcha.de（最終参照 : 2014-01. 注 : 2017-10 現在, サイト閲覧不可能）.

[36] Dracon™ : Visual Flash CAPTCHA - Telling Humans And Computers Apart（オンライン）, 入手先〈http://www.dracon.biz/captcha.php〉（参照 2017-10）.

[37] G. Elber : CAPTCHANIM（オンライン）, 入手先〈http://www.cs.technion.ac.il/~gershon/personal/captchanim/〉（参照 2017-10）.

[38] V. D. Nguyen, Y. Chow, W. Susilo : Attacking Animated CAPTCHAs via Character Extraction, Proceedings of The 11th International Conference on Cryptology and Network Security, pp.98-113（2012）.

[39] J. Kani, M. Nishigaki : Gamified CAPTCHA, Proceedings of the 1st International Conference on Human Aspects of Information Security, Privacy, and Trust, pp.39-48（2013）.

[40] フレッド・クインビー, ウィリアム・ハンナ（監督）: テニスなんて楽なんだね, トムとジェリー, Vol.7[DVD], ワーナー・ホーム・ビデオ（2000）.

[41] H. Meutzner, V. Nguyen, T. Holz, D. Kolossa : Using automatic speech recognition for attacking acoustic CAPTCHAs: the trade-off between usabil

ity and security, Proceedings of the 30th Annual Computer Security Appl ications Conference, pp.276-285（2014）.

[42] J. P. Bigham, A. C. Cavender : Evaluating existing audio CAPTCHAs and an interface optimized for non-visual use, Proceedings of the SIGCHI Co nference on Human Factors in Computing Systems, pp.1829-1838（2009）.

[43] E. Bursztein, S. Bethard, C. Febry, J. C. Mitchell, D. Jurafsky : How Go od Are Humans at Solving CAPTCHAs? A Large Scale Evaluation, Procee dings of the 2010 IEEE Symposium on Security and Privacy, pp.399-413（2010）.

[44] Google : reCAPTCHA（オンライン）, 入手先〈https://www.google.com/recaptc ha/〉（参照 2017-10）.

[45] Capy : 不正ログイン対策なら Capy（キャピー）（オンライン）, 入手先〈https: //www.capy.me/jp/〉（参照 2017-10）.

[46] S. Sivakorn, Jason Polakis, A. D. Keromytis : I'm not a human: Breakin g the Google reCAPTCHA, Black Hat Asia 2016（2016）.

[47] Google : reCAPTCHA デモ（オンライン）, 入手先〈https://www.google.com/re captcha/api2/demo〉（参照 2017-10）.

[48] GEHIRNews : IVS で優勝したというパズル型 CAPTCHA Capy を突破してみた（オンライン）, 入手先〈https://news.gehirn.jp/security/513/〉（参照 2017-10）.

[49] Tech Crunch : パズル CAPTCHA の「Capy」、MS Ventures で採択されて創業者らがイスラエルに（オンライン）, 入手先〈http://jp.techcrunch.com/2014/09/ 11/capy-has-been-accepted-to-ms-accelerator-program/〉（参照 2017-10）.

[50] バイオメトリクスセキュリティコンソーシアム : バイオメトリックセキュリティ・ハンドブック, オーム社（2006）.

[51] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, et al. : Intriguing prope rties of neural networks（オンライン）, 入手先〈https://arxiv.org/abs/1312.6 199〉（参照 2017-10）.

[52] I. J. Goodfellow, J. Shlens, C. Szegedy : Explaining and Harnessing Adve rsarial Examples（オンライン）, 入手先〈https://arxiv.org/abs/1412.6572〉（参照 2017-10）.

[53] M. Osadchy, J. Hernandez-Castro, S. Gibson, O. Dunkelman, D. Pérez-C abo : No Bot Expects the DeepCAPTCHA! Introducing Immutable Adversa rial Examples with Applications to CAPTCHA, IEEE Transactions on Info rmation Forensics and Security, Vol.12, Issue.11, pp.2640-2653（2017）.

[54] 阿座上知香, 柴田千尋, 宇田隆哉 : 畳込みニューラルネットワークに耐性のある C APTCHA の提案, マルチメディア, 分散, 協調とモバイル（DICOMO2017）シンポジウム論文集, pp.1786-1795（2017）.

[55] N. Papernot, P. McDaniel, X. Wu, S. Jha, A. Swami : Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks, Proceedings of 2016 IEEE Symposium on Security and Privacy（2016）.
[56] 伊藤康一，高橋徹，青木孝文：高精度な画像マッチング手法の検討，第 25 回信号処理シンポジウム論文集，pp.547-552（2010）.
[57] 藤吉弘亘，安倍満：局所勾配特徴抽出技術:–SIFT 以降のアプローチ–，精密工学会誌，Vol.77，No.12，pp.1109-1116（2011）.
[58] 熊沢逸夫：コンピュータビジョンの基礎となる対応点問題をめぐって，映像情報メディア学会誌，Vol.60，No.3，pp.313-320（2006）.
[59] 金沢靖，金谷健一：2 画像間の特徴点対応の自動探索--シーンに関する知識を上手に使う，画像ラボ，Vol.15，No.11，pp.20-23（2004）.
[60] R. Hartley，A. Zisserman：Multiple view geometry in computer vision，Cambridge University Press（2003）.
[61] スティール・ドゥワス(Steel-Dwass)の方法による多重比較（オンライン），入手先〈http://aoki2.si.gunma-u.ac.jp/R/Steel-Dwass.html〉（参照 2017-12）.
[62] 小林 孝至，西村 治，角所 考，淡 誠一郎，北橋 忠宏：単一手書き線画に基づく大まかな 3 次元形状伝達のための立体復元，電気学会論文誌 C，Vol.116，No.9，pp.998-1006（1996）.
[63] 五十嵐 健夫：スケッチインタフェースの研究動向，コンピュータソフトウェア，Vol.23，No.4（2007）.
[64] metaseq.net | 3D モデリングソフトウェア「Metasequoia（メタセコイア）」公式サイト（オンライン），入手先〈http://www.metaseq.net/jp/〉（参照 2017-10）.
[65] W. Stahler（山下恵美子訳）：ゲーム開発のための数学・物理学入門，ソフトバンク クリエイティブ株式会社（2005）.
[66] Caffe（オンライン），入手先〈http://caffe.berkeleyvision.org〉（参照 2017-10）.
[67] 石橋研二：形状の検索・分類の技術と類似形状検索エンジン，ユニシス技法，Vol.32，No.4，pp.51-61（2013）.
[68] RSA Security（オンライン），入手先〈https://www.rsa.com/en-us〉（参照 2017-10）.
[69] R. L. Rivest : The RC5 Encryption Algorithm，Proceedings of the 2nd International Workshop on Fast Software Encryption，pp.86-96（1994）.
[70] 菊池浩明，山口高康，濱田浩気，山岡裕司ほか：匿名加工・再識別コンテスト Ice & Fire の設計，コンピュータセキュリティシンポジウム 2015 論文集，pp.363-370（2015）.
[71] 菊池浩明，小栗秀暢，野島良，濱田浩気ほか：PWSCUP: 履歴データを安全に匿名加工せよ，コンピュータセキュリティシンポジウム 2016 論文集，pp.271-278（2016）.

[72] 菊池浩明，小栗秀暢，中川裕志，野島良ほか：PWSCUP2017: 長期間の履歴データの再識別リスクを競うコンピュータセキュリティシンポジウム 2017 論文集，pp.128-135（2017）．
[73] M. O. Rabin : Digitalized Signatures and Public-Key Functions as Intractable as Factorization，MASSACHUSETTS INST OF TECH CAMBRIDGE LAB FOR COMPUTER SCIENCE（1979）．
[74] T. Elgamal : A public key cryptosystem and a signature scheme based on discrete logarithms，IEEE Transactions on Information Theory，Vol.31，Issue.4，pp.469-472（1985）．
[75] EORA 3D（オンライン），入手先〈https://eora3d.com〉（参照 2017-10）．
[76] Microsoft : KinectFusion Project Page（オンライン），入手先〈https://www.microsoft.com/en-us/research/project/kinectfusion-project-page/〉（参照 2017-11）．
[77] 鈴木徳一郎, 山本匠, 西垣正勝: リレーアタックに耐性をもつ CAPTCHA の提案，情報処理学会研究報告（CSEC），Vol.2010，No.21，pp.1-8（2010）．
[78] C. Dctorow : Solving and creating captchas with free porn（オンライン），入手先〈https://boingboing.net/2004/01/27/solving-and-creating.html〉（参照 2017-10）．
[79] ZDNet : Inside India's CAPTCHA solving economy（オンライン），入手先〈http://www.zdnet.com/article/inside-indias-captcha-solving-economy/〉（参照 2017-10）．
[80] Symantec : Trojan.Captchar.A（オンライン），入手先〈https://www.symantec.com/security_response/writeup.jsp?docid=2007-103012-0328-99&tabid=2〉（参照 2017-10）．
[81] M. Egele，L. Bilge，E. Kirda，C. Kruegel : CAPTCHA Smuggling: Hijacking Web Browsing Sessions to Create CAPTCHA Farms，Proceedings of 25th ACM Symposium on Applied Computing（2010）．
[82] 立田怜平，山場久昭，久保田真一郎，朴美娘，岡崎直宣 : マウストラッキングを用いた CAPTCHA 方式の検討，IPSJ 火の国シンポジウム 2016（2016）．
[83] Amazon Mechanical Turk（オンライン），入手先〈https://aws.amazon.com/jp/mturk/〉（参照 2017-11）．
[84] Lancers（オンライン），入手先〈https://www.lancers.jp〉（参照 2017-11）．
[85] OWASP : Testing for Captcha (OWASP-AT-008)（オンライン），入手先〈https://www.owasp.org/index.php/Testing_for_Captcha_(OWASP-AT-008)〉（参照 2017-10）．

[86] 土屋貴史，神農泰圭，藤田真浩，高橋健太ほか：Man In The Browser 攻撃対策を実現する人間・銀行サーバ間のセキュア通信プロトコル（その 2），情報処理学会研究報告，Vol.2017-CSEC-76，No.6，pp.1-7（2017）．
[87] 兼子拓弥，本部栄成，高橋健太，西垣正勝：計算機援用ユーザ認証，情報処理学会論文誌，Vol.55，No.9，pp.2072-2080（2014）．
[88] N. Provos，D. Marières：A Future-Adapable Password Scheme，Proceedings of 1999 USENIX Annual Technical Conference，pp.81-92（1999）．

謝辞

本研究を進めるにあたり，指導教員としてご丁寧，的確，かつ，きめ細やかなご指導を賜り，常に励まし続けてくださった静岡大学　西垣正勝教授に心より御礼申し上げます．また，ゼミにご参加いただき，貴重なご意見をくださいました，静岡大学　大木哲史講師に御礼申し上げます．

博士論文審査委員として，事前審査・本審査を通じて，本論文に関して数多くのご助言をしてくださった，静岡大学　竹内勇剛教授，海老澤嘉伸教授，峰野博史准教授に深謝申し上げます．

本研究を進めるにあたり，静岡産業大学　漁田武雄教授には認知心理学の観点からご助言をいただきました．静岡大学　中谷広正教授，佐治斉教授には画像分野の観点からご助言をいただきました．同大学　西村雅史教授，筑波大学 日野英逸准教授には機械学習に関してご教授いただきました．静岡大学　堀内裕晃教授には，国際会議へ投稿する際に，英語論文に対するご指導をいただきました．皆様に御礼申し上げます．

本研究の一部は，西垣研究室の先輩である可児潤也氏，同期である池谷勇樹氏，後輩である佐野絢音氏との共同研究の成果です．また，研究を進めるにあたっては，西垣研究室の皆さまとの日ごろの議論が欠かせませんでした．お三方を含む西垣研究室の皆さまに対して心より御礼申し上げます．

本研究では，システム構築・運用を行うことも多くありました．システム構築・運用に関するスキルの多くは，学部時代に，デジタルセンセーション株式会社（現　株式会社エクサウィザーズ）　坂根裕氏や静岡大学　石川翔吾助教のご指導によって獲得したものです．ここに御礼申し上げます．

論文の評価実験では，メタセコ素材!（http://sakura.hippy.jp/meta/），TurboSquid（http://www.turbosquid.com/），のぼり坂一丁目（http://www.geocities.jp/oirahakobito2/sozai/sozai.html）などで公開されている無料素材の 3D モデルを利用させて頂きました．

筆者は，本論文で取り扱った研究以外にもいくつかの研究に参加しており，その中でも多くの方々にお世話になりました．（株）日立製作所　高橋健太氏，情報セキュリティ大学院　大塚玲教授には，バイオメトリクスの分野で多くの貴重なご意見を頂戴いたしました．東京電機大学　佐々木良一教授，創価大学　勅使河原可海名誉教授，NTT セキュアプラットフォーム研究所　間形文彦氏，東芝デジタルソリューションズ　加藤岳久氏，東京電機大学　高橋雄志氏には TSAP の場を中心に多くのご指導をいただきまし

た．小林信博氏，山本匠氏をはじめとした，三菱電機情報技術総合研究所情報セキュリティ技術部の皆様には，共同研究や学会の場を通じて多くのご指導をいただきました．皆様に深く御礼申し上げます．

研究会・学会活動でも多くの方にお世話になりました．明治大学　菊池浩明教授，富士通研究所　小栗秀暢氏には，PWS（プライバシー・ワークショップ）の場を中心に多くのご指導をいただきました．東邦大学　金岡晃准教授，株式会社インターネットイニシアティブ　須賀祐治氏には，筆者が実行委員長を務めた CSS×2.0 in CSS2016 の運営にあたって，多大なるご支援とお気遣いをいただきました．セコム株式会社 IS 研究所島岡政基氏には，研究所訪問の機会をいただいたほか，学会の場では常にお声がけをいただきました．立命館大学　毛利公一教授には，学会でのお話をきっかけとして，西垣・毛利研究室合同ゼミを開催させていただき，その中でご指導をいただきました．京都産業大学　瀬川典久准教授には，インタラクティブシステムの研究会である WISS をご紹介いただき，WISS に参加した際には，会場で多くのお気遣いをいただきました．皆様にこの場を借りて御礼申し上げます．

筆者は，修士 2 年から博士 3 年の各 4 年間で 2 週間ずつ，オーストリアのアッパーオーストリア応用科学大学に短期滞在して勉強をする機会をいただきました．このような貴重な機会を与えてくださり，現地で様々なご指導をしてくださった，津田塾大学　村山優子教授に心より御礼申し上げます．現地での滞在においては，同大学　大塚亜未助教にもお世話になりました．重ねて御礼申し上げます．

研究を進める上での事務手続きや資料の印刷等では，西垣研究室　安藤敦子秘書にお世話になりました．安藤秘書がご不在の際には，峰野研究室　岩田あずさ秘書にご対応いただくこともありました．また，一昨年度までは，岩田秘書の前任である峰野研究室鈴木佳代子（元）秘書にご対応いただくこともありました．お三方に御礼申し上げます．

最後に，学部時代から博士課程まで，9 年間という長い大学生活において，著者が学業に専念できたのも家族の協力があったからこそです．このような環境を用意してくださった，両親，弟，祖父母に心より御礼を申し上げます．

発表論文等

1. 学位論文資格に関わる論文

1) **藤田真浩**, 池谷勇樹, 可児潤也, 西垣正勝：Locimetric 型メンタルローテーション CAPTCHA，情報処理学会論文誌，Vo.57，No.9，pp.1954-1964（2016）.
2) **藤田真浩**, 池谷勇樹, 可児潤也, 西垣正勝：非現実画像 CAPTCHA:常識からの逸脱を利用した 3DCG 画像 CAPTCHA, 情報処理学会論文誌, Vol.56, No.12, pp.2324-2336（2015）.

2. 学位論文内容に関わる論文

1) **M. Fujita**，Y. Ikeya，J. Kani，M. Nishigaki：Chimera CAPTCHA: A Proposal of CAPTCHA using Strangeness in Merged Objects，Proceedings of the 3rd International Conference on Human Aspects of Information Security, Privacy, and Trust，pp. 48-58（2015）.
2) Y. Ikeya，**M. Fujita**，Y. Yoneyama，J. Kani，M. Nishigaki：An image-based CAPTCHA using sophisticated mental rotation，Proceedings of the 2nd International Conference on Human Aspects of Information Security, Privacy, and Trust，pp.57-68（2014）.

3. その他の論文

1) **藤田真浩**，眞野勇人，村松弘明，高橋健太，西垣正勝：マイクロ生体認証の提案とその一事例報告, 電子情報通信学会論文誌 A, Vol.100-A, No.12, pp.465-474（2017）.
2) 白井丈晴，**藤田真浩**，荒井大輔，大岸智彦，西垣正勝：スマートフォンの通信遅延におけるユーザのアウェアネスと QoE の関係に関する基礎検討，情報処理学会論文誌，Vol.58，No.12，pp.1901-1911（2017）.
3) A. Sano，**M. Fujita**，M. Nishigaki：Directcha-maze: A Study of CAPTCHA Configuration with Machine Learning and Brute-Force Attack Defensibility along with User Convenience Consideration，Proceedings of the 12th International Conference on Broad-Band Wireless Computing, Communication and Applications，pp.489-501（2017）.
4) K. Mukaiyama，**M Fujita**，T. Shirai，S. Kobayashi，M. Nishigaki：Slyware Prevention: Threat of Websites Inducing Accidental Taps and Countermeasures，Proceedings of the 20th International Conference on Network-Based Information Systems，pp.539-552（2017）.

5) **藤田真浩**，山田眞子，西垣正勝：エンターテイメントを活用したセキュリティ強化：パスワード強化要素を組み込んだゲームの実装とその有効性，情報処理学会論文誌，Vol.57，No.12，pp.2654-2663（2016）．
6) 有村汐里，**藤田真浩**，松野宏明，可児潤也，司波章，西垣正勝：i/k-Contact:物理的ソーシャルトラストを利用した適応型 2 段階認証，情報処理学会論文誌，Vol.57，No.12，pp.2644-2663（2016）
7) A. Sano，**M. Fujita**，M. Nishigaki：Directcha: A Proposal of Spatiometric Mental Rotation CAPTCHA，Proceedings of the 14th Privacy, Security and Trust Conference，pp.585-592（2016）．
8) T. Shirai，**M. Fujita**，D. Arai，T. Ogishi，M. Nishigaki：Study on Relationship between User Awareness and QoE in Communication Delay on Smartphones，Proceedings of the 14th Privacy, Security and Trust Conference，pp.573-580（2016）．
9) **M. Fujita**，Y. Mano，T. Kaneko，K. Takahashi，M. Nishigaki：A Micro Biometric Authentication Mechanism Considering Minute Patterns of the Human Body：A Proposal and the First Attempt，Proceedings of the 19th International Conference on Network-Based Information Systems，pp.159-164（2016）．
10) **M. Fujita**，M. Yamada，M. Nishigaki：Implementation and initial evaluation of game in which password enhancement factor is embedded，HCI International 2016 – Posters' Extended Abstracts，pp.476-481（2016）．
11) T. Tsuchiya，**M. Fujita**，K. Takahashi，T. Kato，F. Magata，Y. Teshigawara，R. Sasaki，M. Nishigaki：Secure Communication Protocol between a Human and a Bank Server to Prevent a Man In The Browser Attack，Proceedings of the 4th International Conference on Human Aspects of Information Security, Privacy, and Trust，pp.77-88（2016）．
12) **M. Fujita**，M. Yamada，S. Arimura，Y. Ikeya，M. Nishigaki：An Attempt to Memorize Strong Passwords while Playing Games，Proceedings of the 18th International Conference on Network-Based Information Systems，pp.264-268（2015）．
13) **M. Fujita**，Y. Ikeya，S. Arimura，C. D. Jensen，M. Nishigaki：Physical Trust-based Persistent Authenticatio，Proceedings of the 13th Annual Conference on Privacy, Security and Trust，pp.186-190（2015）．
14) S. Arimura，**M. Fujita**，S. Kobayashi，J. Kani，A. Shiba，M. Nishigaki：i/k-Contact: a context-aware user authentication using physical social trust，Proceedings of the 12th Annual Conference on Privacy, Security and Trust，pp.407-413（2014）．

4. 口頭発表など

1) 杉本元輝，**藤田真浩**，眞野勇人，大木哲史，西垣正勝：使い捨て可能な生体認証の提案 ～爪の模様を用いたマイクロ生体認証～，電子情報通信学会技術研究報告，Vol.117，No.513， pp.127-132（2018）．
2) **M. Fujita**，A. Sano，Y. Mano，T. Ohki，M. Nishigaki：Micro Biometric Authentication using Skin Texture: Implementation of Prototype system，Proceedings of the 4th International Symposium toward the Future of Advanced Researches in Shizuoka University，p.35（2018）．
3) 遠藤将，松野宏昭，村松弘明，**藤田真浩**，西垣正勝：利便性と安全性に配慮したチャレンジ・レスポンス分離型ユーザ認証の提案，情報処理学会研究報告コンピュータセキュリティ，Vol.2018-CSEC-80，No.14（2018）．
4) 佐野絢音，**藤田真浩**，西垣正勝：機械解読耐性の向上とユーザのメンタル負荷軽減を両立する CAPTCHA 出題形式に関する検討（その 2），2018 年暗号と情報セキュリティシンポジウム予稿集，2F4-3（2018）．
5) **藤田真浩**，眞野勇人，佐野絢音，高橋健太，大木哲史，西垣正勝：肌理を利用したマイクロ生体認証：プロトタイプシステムの構築，第 7 回バイオメトリクスと認識・認証シンポジウム論文集，pp.1-2（2017）．
6) 杉本元輝，**藤田真浩**，眞野勇人，村松弘明，西垣正勝：爪の微細部位を用いたマイクロ生体認証の提案，第 7 回バイオメトリクスと認識・認証シンポジウム論文集，pp.88-89（2017）．
7) **藤田真浩**： “I feel stupid I can’t delete...”: A Study of Users’ Cloud Deletion Practices and Coping Strategies の紹介，SOUPS2017 論文読破会（2017）．
8) **藤田真浩**，眞野勇人，佐野絢音，高橋健太，大木哲史，西垣正勝：肌理を利用したマイクロ生体認証：ユーザビリティ向上のためのプロトタイプシステム改良，コンピュータセキュリティシンポジウム 2017 論文集，pp.704-711（2017）．
9) 佐野絢音，**藤田真浩**，西垣正勝：機械解読耐性の向上とユーザのメンタル負荷軽減を両立する CAPTCHA 出題形式に関する検討，コンピュータセキュリティシンポジウム 2017 論文集，pp.720-727（2017）．
10) 上原航汰，向山浩平，**藤田真浩**，西川弘毅，山本匠，河内清人，西垣正勝：OSINT を利用した標的型メール攻撃手法に関する基礎検討，コンピュータセキュリティシンポジウム 2017 論文集，pp.222-229（2017）．
11) **藤田真浩**，眞野勇人，佐野絢音，高橋健太，大木哲史，西垣正勝：肌理を利用したマイクロ生体認証:プロトタイプシステムの構築，情報学シンポジウム 2017 予稿集，p.20（2017）（査読あり）．
12) 向山浩平，**藤田真浩**，白井丈晴，小林真也，西垣正勝：Slyware 対策:意図しないタップを誘発する Web サイトの脅威と対策に関する検討，情報学シンポジウム 2017 予稿集，p.19（2017）（査読あり）．

13) 佐野絢音，**藤田真浩**，西垣正勝：機械解読耐性の向上とユーザのメンタル負荷軽減を両立する CAPTCHA 出題形式に関する検討，情報学シンポジウム 2017 予稿集，pp.19-20（2017）（査読あり）．
14) **藤田真浩**，眞野勇人，村松弘明，高橋健太，大木哲史，西垣正勝：肌理を利用したマイクロ生体認証：プロトタイプシステムの構築，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2017）論文集，pp.1861-1866（2017）．
15) **藤田真浩**，眞野勇人，村松弘明，高橋健太，西垣正勝：マイクロ生体認証：人間の微細生体領域を利用した生体認証, 第 24 回インタラクティブシステムとソフトウェアに関するワークショップ予稿集，pp.31-36（2016）（査読あり）．
16) A. Sano，**M. Fujita**，M. Nishigaki：A Study of CAPTCHA configuration with Machine Learning Attack Defensibility and User Convenience Consideration，The 12th International Workshop on Security（2017）．
17) 杉本元輝，**藤田真浩**，眞野勇人，村松弘明，西垣正勝：爪の微細部位を用いたマイクロ生体認証の提案，電子情報通信学会技術研究報告，Vol.116，No.527，pp.93-97（2017）．
18) 樋口和輝，佐野絢音，土屋貴史，**藤田真浩**，西垣正勝：エンターテイメントを活用したセキュリティ強化： 長いパスワードの記憶維持に必要な復習頻度の検討，情報処理学会研究報告コンピュータセキュリティ，Vol.2017-CSEC-76，No.1，pp.1-6（2017）．
19) 土屋貴史，神農泰圭，**藤田真浩**，高橋健太，尾形わかは，西垣正勝：Man In The Browser 攻撃対策を実現する人間・銀行サーバ間のセキュア通信プロトコル（その 2），情報処理学会研究報告コンピュータセキュリティ，Vol.2017-CSEC-76，No.6，pp.1-7（2017）．
20) 佐野絢音，**藤田真浩**，西垣正勝：総当たり数の確保とユーザのメンタル負荷軽減を実現する CAPTCHA 出題形式の検討，2017 年暗号と情報セキュリティシンポジウム予稿集，3B4-2（2017）．
21) **藤田真浩**：Use the Force: Evaluating Force-Sensitive Authentication for Mobile Devices の紹介，SOUPS2016 論文読破会（2016）．
22) **藤田真浩**，眞野勇人，村松弘明，高橋健太，西垣正勝：肌理画像を利用したマイクロ生体認証の長期実験に関する報告，第 6 回バイオメトリクスと認識・認証シンポジウム論文集，pp.96-97（2016）．
23) **藤田真浩**，眞野勇人，村松弘明，高橋健太，西垣正勝：肌理画像を利用したマイクロ生体認証の長期実験に関する報告，電子情報通信学会技術研究報告，Vol.116，No.263，pp.77-82（2016）．
24) H. Muramastu，**M. Fujita**，Y. Mano，K. Takahashi，M. Nishigaki：A proposal of a biometric authentication system using human minute patterns，The 11th International Workshop on Security（2016）．

25) T. Tsuchiya，**M. Fujita**，K. Takahashi，T. Kato，F. Magata，Y. Teshigawara，R. Sasaki，M. Nishigaki：Secure Communication Protocol Using an Advanced Human-cognitive-processing Ability for Preventing Man-in-the-Browser Attacks，The 11th International Workshop on Security（2016）

26) **藤田真浩**，眞野勇人，高橋健太，西垣正勝：マイクロ生体認証の提案とその一事例報告，第 19 回画像の認識・理解シンポジウム予稿集，PS3-53（2016）．

27) 向山浩平，**藤田真浩**，白井丈晴，小林真也，西垣正勝：Slyware 対策:意図しないタップを誘発する Web サイトの対策に関する考察，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2016）論文集，pp.387-395（2016）．

28) 白井丈晴，**藤田真浩**，荒井大輔，大岸智彦，西垣正勝：スマートフォンの通信遅延におけるユーザのアウェアネスと QoE の関係に関する基礎検討，情報処理学会研究報告セキュリティ心理学とトラスト，Vol.2016-SPT-18，No.15（2016）．

29) NGUYEN Xuan Nghia，**藤田真浩**，西垣正勝：フリーメールの広告推薦モデルにおけるプライバシー向上に関する一提案，情報処理学会研究報告コンピュータセキュリティ，Vol.2016-CSEC-72，No.36（2016）．

30) 遠藤将，村松弘明，**藤田真浩**，西垣正勝：メンタルタスクと視線遮断動作を併用したユーザ認証の覗き見対策の提案，情報処理学会研究報告コンピュータセキュリティ，Vol.2016-CSEC-72，No.22（2016）．

31) 佐野絢音，**藤田真浩**，西垣正勝：Spatiometric 型メンタルローテーション CAPTCHA の提案，2016 年暗号と情報セキュリティシンポジウム予稿集，3C2-1（2016）．

32) **藤田真浩**，有村汐里，可児潤也，司波章，西垣正勝：i/k-Contact：ユーザ間の信頼関係を利用したコンテキストアウェア認証，第 23 回インタラクティブシステムとソフトウェアに関するワークショップ予稿集，pp.43-48（2015）（査読あり）．

33) 有村汐里，**藤田真浩**，松野宏昭，可児潤也，司波章，西垣正勝：i/k - Contact:物理的ソーシャルトラストを利用した適応型 2 段階認証，情報処理学会研究報告セキュリティ心理学とトラスト，Vol.2015-SPT-16，No.15（2015）．

34) **藤田真浩**：Learning Random Secrets for Unlocking Mobile Devices の紹介，SOUPS2015 論文読破会（2015）．

35) **藤田真浩**，眞野勇人，兼子拓弥，高橋健太，西垣正勝：マイクロ生体認証の提案とその一事例，第 5 回バイオメトリクスと認識・認証シンポジウム論文集，pp.28-29（2015）．

36) **藤田真浩**，山田眞子，西垣正勝：エンターテイメントを活用したセキュリティ強化：パスワード強化要素を組み込んだゲームの開発とその有効性の検討，コンピュータセキュリティシンポジウム 2015 論文集，pp.763-770（2015）．

37) **藤田真浩**，池谷勇樹，西垣正勝：全周囲型メンタルローテーション CAPTCHA の提案，プロトタイプシステムの構築，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2015）論文集，pp.1816-1822（2015）．

38) 村松弘明，西澤璃音，兼子拓弥，眞野勇人，**藤田真浩**，西垣正勝：体感型アプリプライバシポリシ―ユーザの動作はプライバシ意識の向上に寄与し得るか?―，電子情報通信学会技術研究報告，Vol.115，No.117，pp.79-84（2015）．

39) 土屋貴史，**藤田真浩**，高橋健太，加藤岳久，間形文彦，勅使河原可海，佐々木良一，西垣正勝：Man In The Browser 攻撃対策を実現する人間・サーバ間のセキュア通信プロトコル，情報処理学会研究報告コンピュータセキュリティ，Vol.2015-CSEC-69，No.22，pp.1-9（2015）．

40) 白井丈晴，小林真也，鈴木富明，**藤田真浩**，荒井大輔，大岸智彦，峰野博史，西垣正勝：端末による LTE 制御信号スパイク制御方式におけるインセンティブと QoE の関係に関する基礎検討，情報処理学会研究報告コンピュータセキュリティ，Vol.2015-CSEC-68，No.34，pp.1-8（2015）．

41) グエンスアンギア，**藤田真浩**，池谷勇樹，米山裕太，可児潤也，西垣正勝：SNOW NOISE CAPTCHA：無意味な情報を利用した動画 CAPTCHA の提案，情報処理学会研究報告コンピュータセキュリティ, Vol.2014-CSEC-64, No.29, pp.1-7（2014）.

42) **藤田真浩**，池谷勇樹，可児潤也，西垣正勝：キメラ CAPTCHA：3DCG を利用した違和感画像 CAPTCHA，第 23 回インタラクティブシステムとソフトウェアに関するワークショップ論文集，pp.213-214（2014）．

43) **藤田真浩**：The Password Life Cycle: User Behaviour in Managing Passwords の紹介，SOUPS2014 論文読破会（2014）．

44) **M. Fujita**，Y. Ikeya，J. Kani，M. Nishigaki：Chimera CAPTCHA: A proposal of CAPTCHA using Strangeness in Merged Objects，The 9th International Workshop on Security（2014）．

45) **藤田真浩**，池谷勇樹，可児潤也，西垣正勝：非現実画像 CAPTCHA：モデルのめり込みを利用した違和感画像 CAPTCHA，第 17 回画像の認識・理解シンポジウム予稿集，SS2-8（2014）．

46) **藤田真浩**，池谷勇樹，可児潤也，米山裕太，西垣正勝：高度なメンタルローテーションを利用した画像 CAPTCHA の提案, 電子情報通信学会技術研究報告, Vol.114, No.83，pp.7-12（2014）．

47) **藤田真浩**，池谷勇樹，可児潤也，西垣正勝：オブジェクトのめり込みを利用した違和感 CAPTCHA の提案, 2014 年暗号と情報セキュリティシンポジウム予稿集, 4B2-4（2014）．

5. 学術雑誌等又は商業誌における解説，総説

1) 西垣正勝, **藤田真浩**, 眞野勇人 : ボイスチェンジャを利用したワンタイム音声認証, 自動認識 2014 年 12 月号，pp.20-25（2014).

6. 表彰

1) SBRA2017 優秀発表賞受賞
藤田真浩，眞野勇人，佐野絢音，高橋健太，大木哲史，西垣正勝：肌理を利用したマイクロ生体認証：プロトタイプシステムの構築，第 7 回バイオメトリクスと認識・認証シンポジウム論文集，pp.1-2（2017）に対して．

2) SBRA2017 優秀発表賞受賞
杉本元輝，**藤田真浩**，眞野勇人，村松弘明，西垣正勝：爪の微細部位を用いたマイクロ生体認証の提案，第 7 回バイオメトリクスと認識・認証シンポジウム論文集，pp.88-89（2017）に対して．

3) DICOMO2017 優秀論文賞受賞
藤田真浩，眞野勇人，村松弘明，高橋健太，大木哲史，西垣正勝：肌理を利用したマイクロ生体認証：プロトタイプシステムの構築，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2017）論文集，pp.1861-1866（2017）に対して．

4) DICOMO2017 野口賞第 3 位受賞
藤田真浩，眞野勇人，村松弘明，高橋健太，大木哲史，西垣正勝：肌理を利用したマイクロ生体認証：プロトタイプシステムの構築，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2017）論文集，pp.1861-1866（2017）に対して．

5) 電子情報通信学会バイオメトリクス専門研究委員会，2016 年 BioX 研究会奨励賞受賞
藤田真浩，眞野勇人，村松弘明，高橋健太，西垣正勝：肌理画像を利用したマイクロ生体認証の長期実験に関する報告，電子情報通信学会技術研究報告，Vol.116，No.263，pp.77-82（2016）に対して．

6) 静岡大学，2016 年度学長表彰
2016 年度山下記念研究賞（**藤田真浩**，池谷勇樹，西垣正勝：全周囲型メンタルローテーション CAPTCHA の提案，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2015）論文集，pp.1816-1822（2015）に対する表彰）の受賞に対して．

7) 情報処理学会，2016 年度山下記念研究賞受賞
藤田真浩，池谷勇樹，西垣正勝：全周囲型メンタルローテーション CAPTCHA の提案，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2015）論文集，pp.1816-1822（2015）に対して．

8) 日本セキュリティマネジメント学会，辻井重男セキュリティ論文賞特別賞受賞
藤田真浩，池谷勇樹，可児潤也，西垣正勝：非現実画像 CAPTCHA:常識からの逸脱を利用した 3DCG 画像 CAPTCHA，情報処理学会論文誌，Vol.56，No.12，pp.2324-2336（2015）に対して．