Vol.2014-DPS-158 No.29
Vol.2014-CSEC-64 No.29
2014/3/6

SNOW NOISE CAPTCHA: 無意味な情報を利用した動画 CAPTCHA の提案

グエンスアンギア[†1]　藤田真浩[†2]　池谷勇樹[†2]
米山裕太[†2]　可児潤也[†2]　西垣正勝[†2]

既存の CAPTCHA の多くは，文字，静止画，動画など，意味を有する情報（有形物）を難読化するというアプローチで設計されている．しかし，マルウェアの攻撃技術が急速に発達しており，このような既存の CAPTCHA は限界を迎えている．この問題を解決するため，ゲシュタルト心理学における「共通運命の法則」を利用することで，無意味な情報（ランダムドット）の中からその都度意味を生成するという新たなアプローチに基づいた動画 CAPTCHA「SNOW NOISECAPTCHA」を提案する．提案方式では，マルウェアが動画中の意味を検出した時には，意味が変化しているという特徴を持つため，マルウェアによる解答は困難である．また，無意味な情報を利用しているため，総当たり攻撃に対する高い耐性を持つ．回答のタイミングをサーバにいかに伝えるかが課題である．

SNOW NOISE CAPTCHA: A Proposal of Movie-based CAPTCHA using Meaningless Information

NGUYEN XUAN NGHIA[†1]　MASAHIRO FUJITA[†2]　YUKI IKEYA[†2]
YUTA YONEYAMA[†2]　JUNYA KANI[†2]　MASAKATSU NISHIGAKI[†2]

There are many existing CAPTCHAs like text-based CAPTCHA, image-based CAPTCHA and movie-based CAPTCHA that are generated by obfuscating the meaning information (like material objects) to protect web services from automated attack by malware. However, as the technique of malware is developing rapidly day by day, it is predicted that the existing CAPTCHAs are coming to limit. To solve the problem, we present SNOW NOISE CAPTCHA, a movie-based CAPTCHA that using the Gestalt Theory of Principal of Common Fate to generate meaning information from meaningless information (random dots). In the proposed system, as the meaning information will be changed while malware is detecting meaning information from movie CAPTCHA, malware hardly unlocks CAPTCHA. In addition, because of using the meaningless information, it is expected that SNOW NOISE CAPTCHA has a high tolerance with the brute-force attack. However, there is still the problem that is how to send the timing of the client answer to the server.

1. はじめに

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やブログへのスパムコメント書き込みといった Web サービス提供サイトに対する DoS（Denial of Service，サービス不能）攻撃が定常的に行われている．このような攻撃を防ぐためにはマルウェアによる Web サービスの不正利用と，人間による正規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 は，人間には容易に解答できるがコンピュータには判別が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だと判定する技術である．

多くの Web サービス提供サイトでは，文字判読型の CAPTCHA（図 1）[1]や動物画像の判別を用いた Asirra（図 2）[2]などの画像 CAPTCHA をマルウェアの攻撃を防ぐ典型的な手法として採用している．しかし，これらの CAPTCHA は OCR（自動文字読取）や機械学習の機能を備えたマルウェアによって破られており[3][4]，文字判読型 CAPTCHA や画像 CAPTCHA をより高度化していくことが求められている．この要求に応じて，多くの研究者が様々な手法を用いて CAPTCHA の高度化を行ってきたが，現在までに利用された手法は，次に示す二つのアプローチへ主に分類される．

一つ目は，CAPTCHA 高度化の黎明期から用いられてきたアプローチであり，文字や画像などの有意味な情報（有形物）を難読化するアプローチである[5][6]．しかし，本アプローチを用いた CAPTCHA の多くは「難読化した情報を，難読化する前の状態へ近づけて認識する」手法を用いた攻撃によって突破されている[7][8].

これを解決するために，二つ目のアプローチとして，有意味な情報と人間の高度な認知能力を組み合わせたアプローチが提案されている[9][10][11][12]．高度な認知能力の模倣は，マルウェアにとって最も困難な事象のうちの一つであると期待されており，近年提案される CAPTCHA では本アプローチを用いたものが多い．

後者のアプローチを用いた CAPTCHA は，一定の有用性が示唆されたものが多い．しかし，後者のアプローチを用

†1 静岡大学情報学部情報科学科
Department of Computer Science, Faculty of Informatics, Shizuoka University
†2 静岡大学大学院情報学研究科
Graduate school of Informatics, Shizuoka University

Vol.2014-DPS-158 No.29
Vol.2014-CSEC-64 No.29
2014/3/6

図 1　文字判読 CAPTCHA の認証画面例

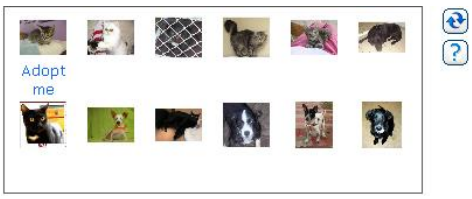

図 2　Asirra の認証画面例

いた CAPTCHA の中にも突破報告がなされている CAPTCHA が複数存在しているように[13][14]，マルウェアの攻撃手法は多様化している．多様化するマルウェアの攻撃手法に対抗するためには，各アプローチに基づく CAPTCHA の種類を増やしていくだけでなく，CAPTCHA の生成アプローチ自体を多様化していくことも重要だと筆者らは考えている．

そこで本稿では，無意味な情報（ランダムドット）の中からその都度生成した意味を利用するという新たなアプローチに基づいた動画 CAPTCHA「SNOW NOISE CAPTCHA」を提案する．提案方式ではランダムドットの背景を用意し，ランダムドットから構成される正解パターンをその上で移動させる．このとき人間であれば，ゲシュタルト心理学の「共通運命の原則」[15]によって，動画中の意味（正解パターン）を認識可能である．また，攻撃耐性を高めるために，背景と正解パターンのランダムドットを 1 フレームごとに更新することで問題を難読化する．したがって，マルウェアが動画解析によって動画中の意味（正解パターン）を検出できたとしても，マルウェアの回答時にはすでに意味が変化しているためマルウェアによる解答は困難である．

以下，本稿では 2 章で CAPTCHA の既存アプローチについて述べる．3 章で提案方式を説明し，4 章で基礎実験の結果を示す．5 章で提案方式について考察した後，6 章でまとめと今後の課題を述べる．

2. CAPTCHA の既存アプローチ

既存の CAPTCHA の多くは，文字，静止画，動画など，有意味な情報（有形物）を難読化する，あるいは，有意味な情報と高度な認知処理能力を組み合わせるアプローチのいずれかを用いることが一般的である．本章では，それぞれのアプローチに基づいた既存研究について述べる．

2.1 有意味な情報の難読化に基づく CAPTCHA

文字列 CAPTCHA の難読化として Animierte CAPTCHA[5]が提案されている．ボールなどの障害物を文字列上で動かす動画 CAPTCHA であり，1 フレームごとに障害物で文字列の一部を隠すことで難読化をしている（図 3）．動画中から文字列を読み取り，その文字列をフォームへ入力できたユーザを正規ユーザ（人間）であると判定する．このとき人間であれば，出題画像を観察して文字列全体を推測可能することで解答可能である．一方で，障害物によって文字列を難読化しているため，1 フレームの画像を取得しただけでは文字列を解読することは不可能である．したがって，提案時には OCR を適用する攻撃に対する高い耐性が期待されていた．しかし現在では，複数フレームの出題画像を合成し，文字列全体を復元した後，OCR を適用する攻撃が可能であることが指摘されている[7].

図 3　Animierte CAPTCHA の認証画面例

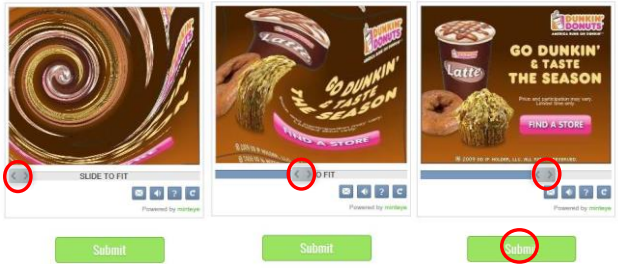

図 4　Minteye　CAPTCHA の認証画面例

一方で画像 CAPTCHA の難読化としては Minteye CAPTCHA[6]が提案されている（図 4）．Minteye CAPTCHA は渦巻きフィルタを用いて難読化した画像をユーザに提示する．ユーザは，画像下に用意されているスライダを左右に動かし，渦巻きフィルタの強さを調整する．そして，渦巻きフィルタが適用されていないタイミングで Submit ボタンをクリックできたユーザを人間として判別する．提案時には，マルウェアがフィルタの適用されていない状態であるか否か，すなわち，難読化前の画像であるか否かを識別することは困難であると期待されていた．しかし現在では，機械もエッジ抽出によって難読化前の状態であるか否かを識別可能であることが指摘されている[8].

2.2 有意味情報と高度な認知能力の組み合わせに基づく CAPTCHA

2.1 節に示したとおり，難読化に基づくアプローチでは「難読化した情報を，難読化する前の状態へ近づけて認識する」手法を用いることでマルウェアによって突破される危険性が高い．そこで 2.1 節に示したアプローチに代わる，有意味な情報と人間の高度な認知能力を組み合わせるアプローチが提案されている．高度な認知能力の模倣は，マル

Vol.2014-DPS-158 No.29
Vol.2014-CSEC-64 No.29
2014/3/6

図 5　Avatar CAPTCHA の認証画面例

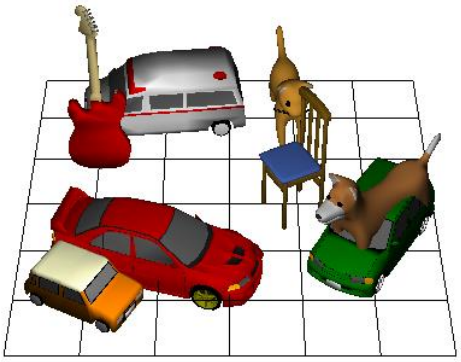

図 6　非現実画像 CAPTCHA の認証画面例

ウェアにとって最も困難な事象のうちの一つであると期待されており，近年提案される CAPTCHA では本アプローチを用いたものが多い．

たとえば，高度な認知能力の一つである「違和感を覚える」能力を利用した CAPTCHA として，Avatar CAPTCHA[9]が提案されている．人間の画像と Avatar 画像が複数枚ずつ含まれた 12 枚の画像をユーザに提示する（図 5）．その中から Avatar 画像のみを選択できるユーザを人間と判定する．人間であれば Avatar 画像に対して違和感を覚えるため，提示された画像から Avatar 画像のみを選択することは容易である．一方で，違和感を覚える能力を持たないマルウェアにとっては困難であると期待されていた．しかし現在では，人間の顔らしさ，Avatar の顔らしさを機械学習することで高い確率で突破可能であることが指摘されている[13].

また，違和感を利用する CAPTCHA の発展形としては，非現実画像 CAPTCHA[12]が提案されている．動物や車のように現実に存在する 3 次元オブジェクト（通常のオブジェクト）複数体と，二つのオブジェクトをめり込ませ合った非現実オブジェクト 1 体を出題画像中に配置する（図 6）．人間であれば，常識から逸脱した形をしている非現実オブジェクトに対して「違和感を覚える」ため，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発見することは容易である．現時点では，マルウェアが通常のオブジェクトと非現実オブジェクトとを識別することは困難であると期待されており，有用性が示唆されている．

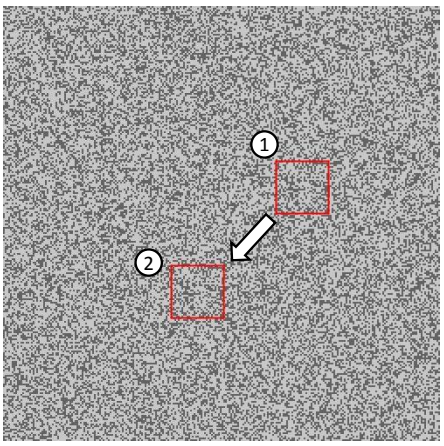

図 7　SNOW NOISE CAPTCHA のコンセプト図

3. SNOW NOISE CAPTCHA

本章では筆者らが提案する「SNOW NOISE CAPTCHA」におけるコンセプト，認証手順，実装について述べる．

3.1 コンセプト

2 章に示したアプローチのうち，2.2 節に示したアプローチで提案された CAPTCHA の多くは有用性が示唆されている．しかし，Avatar CAPTCHA がマルウェアによって突破可能であるという報告がなされているように，マルウェアの攻撃手法は日々多様化している．多様化するマルウェアの攻撃手法に対抗するためには，各アプローチに基づく CAPTCHA の種類を増やしていくだけでなく，CAPTCHA の生成アプローチ自体を多様化していくことも重要だと筆者らは考えている．

そこで本研究では，無意味な情報（ランダムドット）の中からその都度生成した意味を利用するという新たなアプローチに基づいた動画 CAPTCHA「SNOW NOISE CAPTCHA」を提案する．提案方式ではランダムドットの背景を用意し，その上でランダムドットから構成される正解パターンを 1 フレーム毎に移動させる（図 7）．

ゲシュタルト心理学における「共通運命の原則」によれば，人間の脳には，同時に発生し，同じような経緯で変化している複数のできごとをひとまとまりのものとして認識する機能が備わっていることが知られている[15]．すなわち、人間であれば正解パターンの動きを，1 ランダムドット各々が移動しているのではなく，まとまった一つの意味（すなわち，正解パターン）が動いていると認識可能である．したがって，人間はランダムドット背景中から正解パターンを容易に発見し，選択することができる．

一方，ランダムドット背景上で正解パターンを動かすだけでは，マルウェアも動画から 2 フレームを抽出し，その差分を利用することで正解パターンを容易に発見可能である．そこで提案方式では上記の手順に加えて，背景と正解

Vol.2014-DPS-158 No.29
Vol.2014-CSEC-64 No.29
2014/3/6

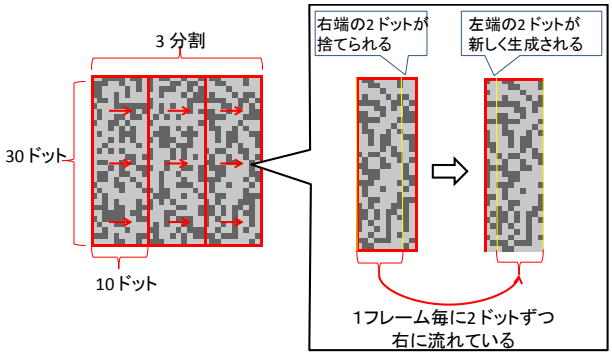

図 8　正解パターンの変化例

パターンのランダムドットを 1 フレームごとに変化することで難読化を行う．ただし，正解パターンのランダムドットは 1 フレーム前の状態をある程度保持した形で変化させる．

図 8 に正解パターンの変化例を示す．図 8 の例では，正解パターンは縦 30 個×横 30 個，計 900 個の正方形ランダムドット（以下，ランダムドットの 1 辺の長さを 1 ドットと呼ぶ）で構成されており，横 10 ドットごとに 3 分割されている．分割されたそれぞれの内部では 1 フレームごとに右に 2 ドット流れている．したがって，1 フレーム後には左端 2 ドット分の空きができるため，空いた 2 ドットには新しくランダムドットを生成する．

3.2　認証手順

SNOW NOISE CAPTCHA の認証手順を図 9 に示す. なお，図 9 中の「ユーザの入力があるか」とは，ユーザが出題動画中で正解パターンと思われる座標を入力する操作を指す. また,「正解判定」はユーザが入力した座標が正解パターンの一部であるか否かを判定する操作を示す.

3.3　プロトタイプシステムの実装

3.1 節に示したコンセプトに基づき，提案方式のプロトタイプシステムを実装する．なお，今回は提案手法の有効性を検証する段階であるため，サーバ・クライアント間の実装は行わず，スタンドアロン PC 上のアプリケーションとして実装を行う．

プロトタイプシステムに用いた各パラメータは図 10 のとおりである．各パラメータの詳細を以下に示す．

- 更新頻度：1 秒あたり 10 フレーム表示される．背景と正解パターンは 1 フレームごとに同時に更新される．
- ランダムドット：ランダムドットの 1 辺の長さ（1 ドット）は 2 ピクセルである．ランダムドットを構成する色は，明色時（R,G,B）＝（200,200,200）であり，暗色時（R,G,B）＝（100,100,100）である．
- ウィンドウサイズ：高さ 250 ドット，幅 250 ドットである．
- 正解パターン：高さ 30 ドット，幅 30 ドットの正方形

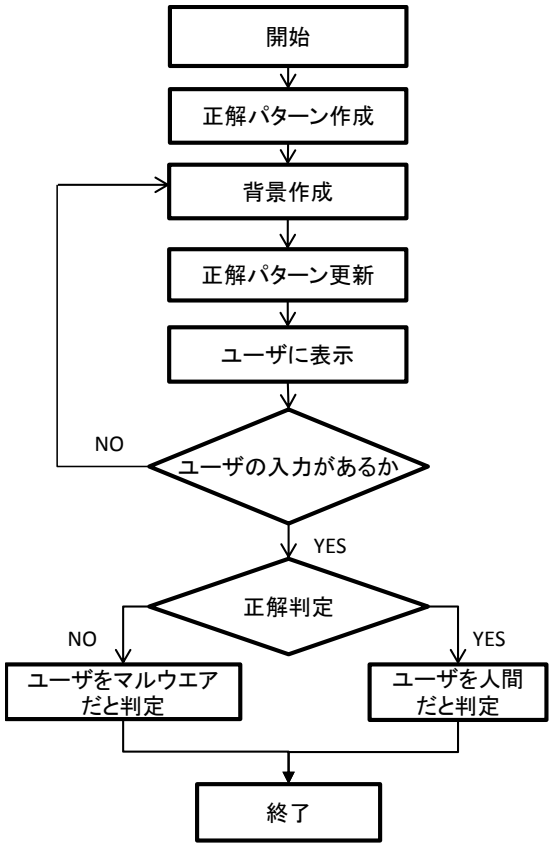

図 9　SNOW NOISE CAPTCHA 認証手順図

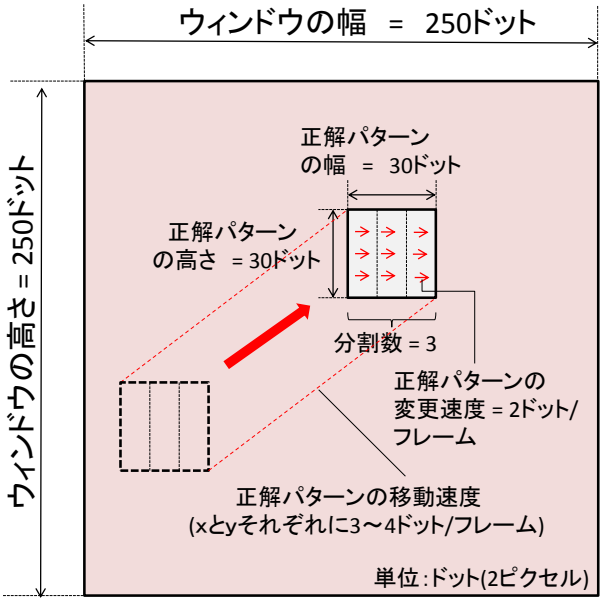

図 10　プロトタイプシステムのパラメータ関係

である．1 フレームごとに，図 8 に示した変化と同様の変化をする（すなわち，正解パターンは 3 分割され，各々が 2 ドットずつ右に移動する）．毎フレーム、x 軸方向に 3～4 ドット，y 軸方向に 3～4 ドットの速度で移動する．直線運動をするが，ウィンドウの端に到達した場合，逆方向に跳ね返る．その際に，x 軸方向，y 軸方向の速度も上記の範囲で再設定される．

Vol.2014-DPS-158 No.29
Vol.2014-CSEC-64 No.29
2014/3/6

4. 基礎実験[a]

4.1 目的

3.2 で実装したプロトタイプシステムを用いて，SNOW NOISE CAPTCHA がユーザ（人間）の正答が可能な CAPTCHA であることを確認する．また，被験者に対してアンケート調査を行い, SNOW NOISE CAPTCHA の有用性について調査する．

4.2 実験条件

被験者は情報セキュリティ系の研究室に所属する学生 5 名である．各被験者は，3 回の実験本番の前に，各被験者が十分と思えるまでの回数の練習を行った．練習および本番における各被験者の各回の問題（正解パターンと背景）は毎回ランダムに自動生成を行っており，それぞれ違う問題が出題される. 被験者には, 提示された出題 動画中から，正解パターンを推測し，クリックするよう指示した．入力インタフェースはマウスを使用し，被験者が正解パターンの一部をクリックした場合に正解と判定する．今回の実験では，各問題に対して，被験者の回答の正否，回答にかかった所要時間，クリックした位置を記録した．また，被験者にアンケートに回答してもらった．アンケートの質問項目を以下に示す．質問①，③，⑤は 1〜5 点の点数で回答してもらった．

① 簡単に解けたか（簡単なら 5）
② 質問①で 2 や 1 を選択した場合，その理由は何か
③ 面倒だと感じたか（面倒でないなら 5）
④ 質問③で 2 や 1 を選択した場合，その理由は何か
⑤ 面白いと感じたか（面白いなら 5）
⑥ 質問⑤で 5 や 4 を選択した場合，その理由は何か
⑦ 何問までならば続けて解いてもよいと思うか．また，
⑧ その理由は何か.
⑨ 実際の Web サービス利用の場面で CAPTCHA を解くことが要求された場合，文字判読型 CAPTCHA と SNOW NOISE CAPTCHA のいずれかを選ぶことができたらどちらを選ぶか．また，その理由は何か.

4.3 実験環境

本実験で用いる端末の情報は以下のとおりである．

- 実験端末：Panasonic Let’s note CF-S9
- OS：Windows7(32bit)
- CPU：Intel(R)Core(TM) –i5 CPU(2.4GHz)
- メモリ：4,096MB
- 解像度：1,280×800

a) 実験中に実験用システムの不具合による表示ミスが発見されたため，システムの改修によってこれに対応しながら実験を完遂させた．

表 1 実験結果

	正答率	平均所要時間[秒]
ユーザ 1	3/3	8.8
ユーザ 2	3/3	11.6
ユーザ 3	2/3	13.5
ユーザ 4	1/3	4.9
ユーザ 5	1/3	10.2
平均	66.67%	9.8

4.4 実験結果

4.4.1 正答率と所要時間

ユーザごとの正答率と平均所要時間をまとめた結果を表 1 に示す. 提案方式は機械耐性を高めるために問題の「難読化」を施しているが，各ユーザは 3 回の試行のうち少なくとも 1 回は正答しており，本提案方式が人間にとって正答が可能な方式であることが示唆された．しかし，全ユーザの平均正答率は 66.67%（全ユーザ 5 名×3 回＝15 回の試行を行ったうち，正答が 10 回，失敗が 5 回）である．一般的な文字判読型 CAPTCHA の平均正答率は約 93%であるため[16]，現時点では実用に供するには低い値となっており，この点は今後改良をしていく必要がある．

ユーザが失敗した問題について実験後に検証を行ったところ，失敗した理由は次の二つの理由に大別された．ユーザが失敗した問題 5 問のうち，3 問の原因は正解パターンから数ドット離れた位置をユーザがクリックしたことであった. これは正解パターンを画像中で発見できたものの，正解パターンは常に動いているため，正解パターンから若干ずれた位置をクリックしてしまったと考えられる．残りの 2 問についてはクリックされた位置が正解パターンの位置と大きく異なっていたため，ユーザが正解パターンでない部分を正解パターンであると誤認した可能性が高かった.

表 1 より，SNOW NOISE CAPTCHA の回答に要する平均所要時間は一問あたり約 10 秒である。一般的な文字判読型 CAPTCHA の平均所要時間は約 12 秒であるため[16]，SNOW NOISE CAPTCHA は文字判読 CAPTCHA より若干短い時間で解ける CAPTCHA であることが示唆される．

なお，正解率や所要時間は，正解パターンの動き方，移動スピード，ランダムドットのサイズなどのパラメータに依存すると考えられる．今後はこれらのパラメータを調整しながら評価実験を繰り返していく必要がある．

4.4.2 利便性

被験者から得られたアンケートをまとめた結果を表 2 に示す．表 2 のとおり，「③面倒のなさ」「⑤面白さ」といった項目は平均値（3.0 点）である．

一方で，「①簡単さ」という項目は平均値よりも小さな値（2.0 点）である．また，「⑧どちらを選ぶか」という項目では 5 名中 4 名のユーザが文字判読型 CAPTCHA を選択

表 2　アンケート結果

	①簡単さ	③面倒のなさ	⑤面白さ	⑦回数	⑧どちらを選ぶか
ユーザ 1	2	4	3	2	文字判読型
ユーザ 2	2	4	3	2	文字判読型
ユーザ 3	1	1	2	1	文字判読型
ユーザ 4	2	2	3	2	文字判読型
ユーザ 5	3	4	4	3	SNOW NOISE
平均	2.0	3.0	3.0	2.0	

している．前者については，簡単でない（2 や 1）と答えたユーザから，「常にクリック先が変化するため」や「正解パターンを見つけたと思っても実は違ったことがあった」といったコメントが得られた．同様に後者については，「(SNOW NOISE CAPTCHA は）目がチカチカするため」「(SNOW NOISE CAPTCHA は）目が疲れるため」といった理由が得られた．これらのコメントからは，本方式が無意味情報の「難読化」を利用していることが両項目の低評価の原因であると推測される．ランダムドットから構成された出題動画を 1 フレーム毎に更新することで難読化を行って安全性を高めているが，それに伴ってユーザの利便性（特に，問題解答の容易性）も低下していることが推測される．解答不能を招くほどの影響は与えていないが，この点については今後，機械耐性を保ちつつユーザの負荷を減らす難読化方法や，無意味情報と人間の高度な認知能力を組み合わせていく方法を検討することで解決をはかっていく．

5. 考察

5.1 攻撃耐性

5.1.1 フレーム同士の差分を利用する攻撃

提案方式に対しては，動画から数フレームを抽出し，抽出したフレームの差分を利用して正解パターンの位置や模様を把握する攻撃が考えられる．提案方式では数フレーム後に正解パターンが全く異なる位置に移動しており，さらに正解パターンの模様が完全に変化しているという特徴を持つ．したがって攻撃者が正解パターンの位置を把握できた場合には，発見した位置から正解パターンが完全に離れるまでにクリックすれば攻撃に成功する．模様を把握した場合は，正解パターンの模様が完全に変化する前に，発見した模様をヒントとして動画中から正解パターンを探索できれば攻撃に成功する．

たとえばプロトタイプシステムでは，1 秒あたり 10 フレーム表示される．また，正解パターンのサイズは 30 ドット×30 ドットであり，毎フレーム x 方向に 3 ドット～4 ドット，y 方向に 3 ドット～4 ドットの速度で移動し，正解パターンの模様は毎フレーム 20%の面積が変化する(すなわち，0.5 秒で正解パターンは完全に変化する)．したがって攻撃者は，位置を検出する手法では最大 1 秒以内に，模様を検出する手法では 0.5 秒以内に攻撃を終える必要がある．

5.1.2 総当たり攻撃

ウィンドウ中の任意の座標を無作為にクリックする総当たり攻撃に対する耐性を検討する．このとき，総当たり攻撃が成功する確率は，およそ「正解パターンのサイズ÷ウィンドウサイズ」である．したがって，プロトタイプシステムで用いたパラメータにおいては，(30 ドット×30 ドット)÷(250 ドット×250 ドット)≒0.014 である．

5.2 運用方式

提案方式は動画 CAPTCHA であり，正解パターンの位置が常に変化するという特徴を持つため，サーバとクライアント間で常に通信しながら実行する必要がある．あらかじめサーバからクライアントへ出題動画を送信した後，クライアント上で実行するという方式では，攻撃者に動画を解析する十分な時間を与えることにつながりかねない．したがって，サーバとクライアントが動画やユーザの回答をリアルタイムに送受信可能な環境を構築することが必要要件となる．しかし，現時点では通信遅延等の問題から要件を満たす環境は構築できていないため，運用方式については今後早急に検討していかなければならない．

6. まとめと今後の課題

本稿では，無意味な情報（ランダムドット）からその都度意味を生成し，さらに生成した意味を難読化するという新たなアプローチに基づいた動画 CAPTCHA「SNOW NOISE CAPTCHA」を提案した．提案方式のプロトタイプシステムを実装し，基礎実験を行った．基礎実験の結果，提案方式が正規ユーザ（人間）にとって正答が可能な方式であることを示した．また，提案方式を実用に供するまで発展させるにあたって解決しなければならない事項を示した．

今後は，各種パラメータを変更して繰り返し評価実験を行い，提案方式の可用性や攻撃耐性について引き続き調査していく．これと並行して，動画をクライアントに配信する方法も検討していく．また，人間がどのように正解パターンを認知しているかも調査していきたい

参考文献

1) Unlocking Google's Gmail CAPTCHA, http://www.gmailhelp.com/2009/10/unlocking-googles-gmail-captcha/
2) ASIRRA ‐ Microsoft Research, http://research.microsoft. com/en-us/um/redmond/projects/asirra/
3) J.Yan, A.S.E.Ahmad: Breaking Visual CAPTCHAs with Naïve Pattern Recognition Algorithms, 2007 Computer Security Applications Conference, pp.279-291 (2007).

4) P.Golle: Machine Learning Attacks, Against the ASIRRA CAPTCHA, 2008 ACM CSS, pp.535-542 (2008).
5) Animiertes Sicherheitsfeld - animierte Captcha - grafischer sicherheitscode, http://www.animierte-captcha.de/
6) Minteye-slide-to-fit CAPTCHA&Advertisement Solutions, http://www.minteye.com/
7) Vu Duc Nguyen, Yang-Wai Chow, Willy Susilo: Breaking an Animated CAPTCHA Scheme, Applied Cryptography and Network Security ,Lecture Notes in Computer Science Volume 7341, pp.12-29 (2012).
8) Breaking the minteye captcha again - Hack a Day, http://hackaday.com/2013/01/19/breaking-the-minteye-captcha-again/
9) D.D'Souza, P.Polina, and R. Yampolskiy: Avatar captcha: Telling computers and humans apart via face classification, In Proceedings of IEEE International Conference on Electro/Information Technology (EIT), (2012).
10) YUNiTi.com - Social Networking At Its Best http://www.yuniti.com/
11) 池谷勇樹, 可児潤也, 米山裕太, 西垣正勝: メンタルローテーションを利用した画像 CAPTCHA の提案, JSSM 第 27 回全国大会, (2013).
12) 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, The 31st Symposium on Cryptography and Information Security（CD-ROM）, (2014).
13) Mohammed Korayem, Abdallah A. Mohamed, David Crandall, Roman V. Yampolskiy: Advanced Machine Learning Technologies and Applications Communications in Computer and Information Science Volume 322, pp 102-110 (2012).
14) TechnoBabble Pro: How they'll break the 3D CAPTCHA , http://technobabblepro.blogspot.jp/2009/04/how-theyll-break-3d-captcha.html
15) Tom Stafford and Matt Webb: Mind Hacks, Oreilly & Associates Inc, (2004).
16) 上原章敬, 鈴木徳一郎, 山本匠, 西垣正勝: 4 コマ漫画 CAPTCHA の検討, 第 52 回コンピュータセキュリティ合同研究発表会予稿集（CD-ROM）(2011).