Vol.2019-HCI-181 No.5
2019/1/21

マウスクリックと視線入力を用いた覗き見耐性の高い認証方式の提案

増山翔[†1]　小倉加奈代[†1]　Bhed Bahadur Bista[†1]　高田豊雄[†1]

概要：現在，パソコンやスマートデバイスは電子商取引や SNS に多く利用され，これらのデバイスには多くの個人情報が格納されている．そのため情報漏えい対策は必要不可欠である．情報漏えい対策には生体認証が多く利用されているが，突破された時のため，新たな認証手法が必要である．本研究では，覗き見耐性を高めることを目的とし，フェイク動作としてマウスクリックを利用する視線入力による認証方式を提案する．従来手法である注視型手法と認証成功率，覗き見攻撃，録画攻撃結果を比較した結果，提案手法の認証成功率は，54.2%と低い結果であったが，覗き見攻撃，録画攻撃いずれにおいても，視線による入力が判別されにくく，注視型手法よりも覗き見耐性，録画攻撃耐性の高い手法であることを確認した．

キーワード：視線入力，覗き見耐性，フェイク動作，認証

1. はじめに

現在，インターネットを介してデータをやりとりし，パソコンやスマートフォンを利用して商品を購入することは，生活の中で必要不可欠である．2017 年の世帯における情報通信機器の保有状況をみると，パソコンは 72.5%でスマートフォンは 75.1%である．また，モバイル端末全体でみると 94.8%と非常に高い水準となっている．次に 2017 年のインターネット利用率をみると，80.9%であり，端末別にみるとパソコンは 52.5%，スマートフォンは 59.7%とインターネットはパソコンやスマートフォンで多く利用されていることがわかる[1]．主な利用目的は，電子メールの送受信や SNS の利用，商品・サービスの購入・取引である．このことから，パソコンやスマートフォンには多くの個人情報が格納されていることが明らかであり，情報漏えい対策は必要不可欠である．

情報漏えい対策には Personal Identification Number（以下，PIN）やパターン，パスワードなどの認証方式がある．これらは覗き見されると簡単に突破されてしまうが，認証情報を変更し対策することができる．また，指紋認証や顔認証などの生体認証も覗き見対策として利用されている．これらは素早く認証でき便利であるが，簡単に認証情報を変更できない．以上より生体認証が突破された時のために，覗き見耐性の高い認証方式が必要である．

情報漏えい対策として，菊池ら[2]は複数の認証手法を用いた視覚的なフェイク入りロック解除方式を提案した．この手法は，複数の認証手法（PIN，パターン，パスワード）を用いた視覚的なフェイク入りロック解除方式で，正規の認証方式とは異なる認証画面が表示される．攻撃者は認証画面を見ただけでは正規の認証方式がわからない．また，覗き見攻撃対策として視線入力を用いた認証手法[3][4][5]が提案されている．Khamis ら[3]はモバイルデバイスで視線と画面タッチを組み合わせた認証方式「GazeTouchPass」を提案した．視線入力は左か右を見ることで行い，画面タッチは数字の 0～9 をタッチする．視線と数字の組み合わせを変えることでセキュリティを高めることができる．Liu ら[4]はスマホのインカメラを利用したユーザ認証のための視線追跡手法を提案した．画面上に複数の移動物体が存在し，そのうち 1 つが正解の対象物となっている．ユーザは物体を目で追い，一致した場合は認証成功となる．

本研究では，覗き見耐性の高い認証方式を実現するために，視線入力を利用し，ユーザが見た数字とボタンをクリックしたタイミングから数字を入力するロック解除方式を提案する．このロック解除方式は，見た数字が認証情報として入力されるが，フェイク動作としてボタンのクリックを同時に行うため，攻撃者は単に画面を見るだけでは認証情報を窃取することができない．

本論文の構成は本章以下，2 章では，関連研究について述べる．3 章では，提案手法について述べる．4 章では，評価実験方法と結果，考察を述べる．第 5 章では，本論文のまとめと今後の課題について述べる．

2. 関連研究

2.1 複数の認証手法を用いた視覚的フェイク入りロック解除方式

菊地ら[2]は，スマートデバイスの盗難・紛失を想定とし，PIN，パターン，パスワードの複数の認証（図 1）を組み合わせた視覚的なフェイク入りロック解除方式（図 2）を提案した．この認証方式は，正規の認証方式とは異なる認証方式をフェイクとしてスマートデバイス上に表示する．スマートデバイス上にはフェイクの認証方式画面を表示させるため，攻撃者は端末画面を見ただけでは正規の認証方式はわからない．提案手法の有効性を確認するために行った評価実験では，単一の認証方式よりも提案方式は，攻撃耐性が高いことがわかった．しかし，スマートデバイスの盗難紛失を想定としているため，あらかじめ覗き見攻撃等に

†1 岩手県立大学ソフトウェア情報学部
Iwate Prefectural University, Faculty of Software and Information Science

よりパスワードがわかっている場合，ロック解除が可能であるという問題点がある．本研究では，菊地らの手法同様に，フェイクを用いるとともに，菊地らの研究の問題点を解決する．

図 1　利用する複数の認証方式
（左から PIN 認証，パターン認証，パスワード認証）

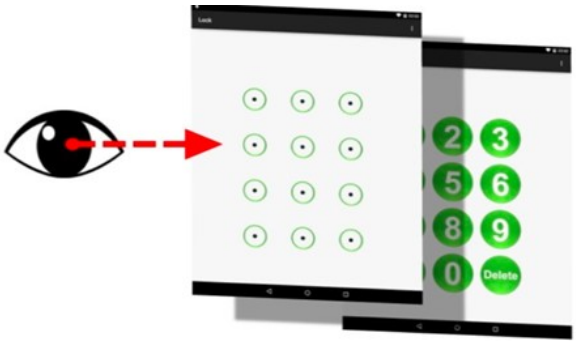

図 2　提案手法のイメージ図
（正規が PIN 認証，フェイクがパターン認証の場合）

2.2　視線入力と数字を組み合わせた認証方式

Khamis ら[3]は覗き見攻撃対策を目的とした，視線入力と数字を組み合わせた認証方式「GazeTouchPass」を提案した．ユーザは数字（0～9 の数字）または視線（左か右を注視）によって入力することができる．攻撃者はパスワードを窃取するためには，デバイスの画面とユーザの目を同時に観察する必要がある．また，数字と視線入力をパスワード中に多く切り替えると攻撃者は推測が困難になる．以下にパスワード入力例と数字と視線入力の切り替え回数を示す．

●1→左を注視→2→右を注視（3 回切り替え）
●1→2→左を注視→右を注視（1 回切り替え）

評価実験として，13 人の被験者に対し，ランダムに生成されたパスワードを使用した実験を行った．その結果，入力時間は数字と視線入力の切り替え回数にかかわらず平均して約 3 秒程度であった．入力成功率は 0 回切り替えの時は 63%，3 回切り替えの時は 77%であった．また，事前に提案手法をビデオ撮影し，被験者に動画を見せ，覗き見攻撃耐性を評価した．その結果，0 回切り替えの時は 44%，3 回切り替えの時は 19%覗き見攻撃が成功した．数字と視線入力の切り替えが多いほど攻撃成功率が低い結果となった．

本研究でも，「GazeTouchPass」と同じように認証に視線入力を利用する．しかし，「GazeTouchPass」は覗き見された場合に，視線は推測できないが，数字は簡単に推測できる．本研究では，マウスを使って数字ボタンをクリックする動作をフェイクとすることで，推測を困難にする．

2.3　スマートフォン認証のための視線追跡手法

Liu ら[4]はスマートフォンの覗き見攻撃や画面の指紋などの汚れから認証情報を推測する汚れ攻撃対策を目的とした視線追跡手法を提案した．スマートフォンのインカメラを利用して，ユーザの視線を捕捉し認証をする．画面上には 1～4 の数字が表示された 4 つの移動物体が存在し，そのうち 1 つが正解の対象物である．ユーザは物体を目で追跡し，その軌跡が目標の物体と一致すると正しい入力となり，この動作を 5 回繰り返すことで認証成功となる．全ての移動物体は毎回ランダムなルートで移動し，攻撃者は視線を真似ただけでは入力することができない．

評価実験として 21 人の被験者が事前に設定した 1～4 からなる 5 桁のパスワードを用いた認証を行った．その結果，認証成功率が 91.6%で 1 回入力を行う時間は約 9.6 秒であった．

本研究も Liu らの研究と同様に覗き見攻撃対策を目的とし，視線を利用した認証方式を提案する．しかし，Liu らの研究では入力可能な数字が 4 つのみであるため，セキュリティを高めるために必然的に入力回数を多くする必要があるという問題がある．そこで本研究では，0～9 の数字を入力可能にすることで入力回数を最小限にし，覗き見耐性を高める．

2.4　注視によるパスワード認証方式

Kumar ら[5]は，覗き見耐性の強化を目的とし，画面上の注視位置により認証情報を入力する「EyePassword」を提案した．ユーザは画面に触れる代わりに，目的の文字・数字を注視するかトリガー（スペースキーなど）を押すことで認証情報できる．本方式では，図 3 のように A ボタンの中央にはフォーカスポイントと呼ばれる赤い点が表示されている．この点を表示させることで視線入力の精度を向上させる効果がある．フォーカスポイントは全てのボタンの中央に表示されている．

図 3　EyePassword の画面

また，18 人の被験者に対し，8～9 文字の大小英文字，数字，記号からなるパスワードを 450ms の注視による入力，

トリガーを利用する入力の 2 つの方式を用い，評価実験した．その結果，注視の場合はエラー率 3%，トリガーの場合はエラー率 15%，入力時間は注視，トリガーともに 10 秒前後であった．

本研究は，「EyePassword」同様に視線入力を利用して認証を行う．しかし，「EyePassword」では，入力するための動作は，注視する，もしくは，トリガーとなる 1 つのボタンを押すことである．そのために，入力方法について攻撃者に判別される可能性がある．そこで本研究では，攻撃者による入力方法の判別を難しくするために，視線入力に加え，フェイク動作としてマウスクリック動作を用いる．

3. 提案手法

3.1 概要

本研究では，覗き見耐性を高めることを目的とし，視線入力に加え，フェイク動作としてマウスクリックを利用する認証手法を提案する．この認証手法ではマウスを使って数字ボタンをクリックする動作をフェイク動作とし，実際の入力は視線を利用する．攻撃者は覗き見だけで秘密情報を取得することは困難である．また，図 4 のように認証画面をパソコンやスマートデバイスでの PIN 認証同様の画面にすることで，認証画面から手法を特定することは困難である．

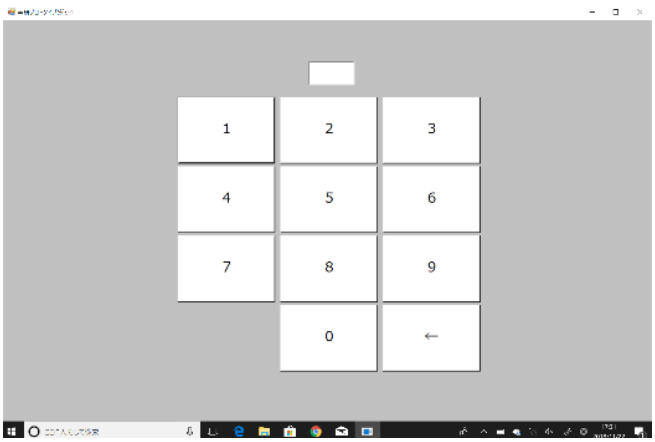

図 4　提案手法の認証画面

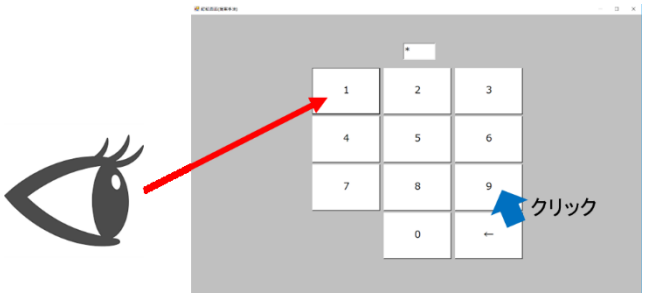

図 5　提案システムの入力例（1 を入力時）

提案手法による認証情報入力例を図 5 に示す．1 の数字を見ているときに 9 のボタンをクリックした場合は，見ている数字の 1 が入力される．上記の例では 9 をクリックしているが，9 以外のどの数字ボタンをクリックしてもユーザが見ている数字が入力される．各数字ボタンのサイズは縦約 2.3cm，横約 3.3cm である．ユーザへのフィードバックとして，数字が入力されるとテキストボックスに「＊」が表示される．ボタン範囲外を見たときに入力を行った場合でも，テキストボックスに「＊」が表示されるが，入力は失敗となる．ボタン範囲外を見たり，違う数字を見たりして，入力を間違えた場合は，右下の「←」ボタンをクリックすると最後に入力した 1 文字が削除される．

3.2 実装環境と認証手順

実装環境は Visual Studio 2013 で言語は C#を使用する．端末は Surface3，視線計測デバイスは Tobii 社の Eye Tracker[6]を使用し，端末の下部の Eye Tracker を固定し使用する．認証手順を図 6，提案手法利用場面を図 7 に示す．

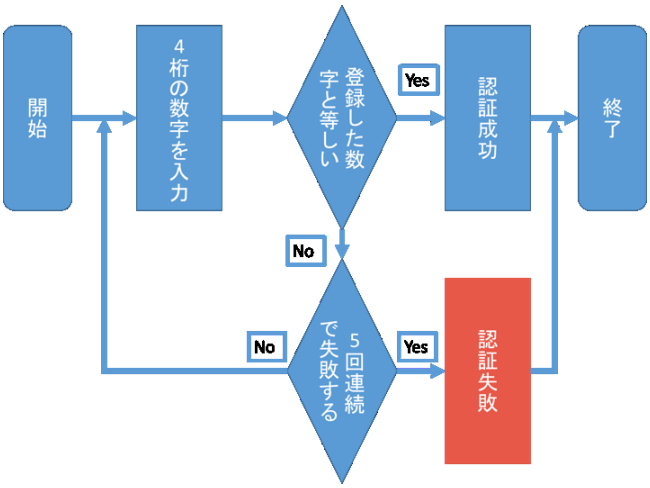

図 6　ユーザの認証手順

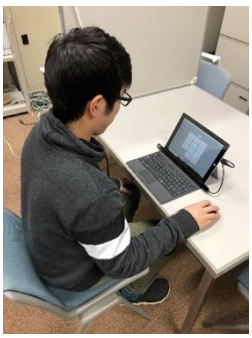

図 7　提案手法利用場面

正確に視線入力を行うために，初回のみ視線計測デバイスのキャリブレーションを行う．ユーザは提案手法利用初回に PIN として数字 4 桁を登録し，各利用時に，登録した PIN を入力する．入力した数字と登録されている PIN を照合し，正しければ認証成功となり，5 回連続で入力に失敗した場合は認証失敗となる．

4. 評価実験

4.1 実験目的と概要

実験では，提案手法について，マウスクリックをフェイク動作とし，視線入力により PIN を入力することで覗き見耐性の高い認証方式を実現できたかを確認する．この際に，Kumar ら[5]が提案した，数字や文字を注視することにより認証情報を入力する手法（以下，注視型入力手法）のフォーカスポイントを削除したシステムを作成し，比較する．なお，注視型入力手法についてフォーカスポイントを削除した理由は，フォーカスポイントがあるとそこから視線を使用して入力していると判別される可能性があるためである．以下 3 つの実験と評価項目により基本性能，覗き見攻撃耐性，録画攻撃耐性を評価する．

- 認証実験
  評価項目：認証成功率，認証時間
- 覗き見耐性実験
  評価項目：視線による認証方式を判別できるか
- 録画攻撃耐性実験
  評価項目：正面から見た時の攻撃耐性はあるか

3 つの実験の被験者は全て同じ，情報系学部に所属する大学生 1～3 年生の 16 名である．実験を実施する順番は覗き見耐性実験，認証実験，録画攻撃実験の順である．覗き見耐性実験は，提案手法を知らない人を対象とするため，初めに行う．録画攻撃耐性実験は，提案手法について十分に理解した人を対象とするため認証実験を先に行い，最後にこの実験を行う．

4.2 認証実験

4.2.1 概要

認証実験では，認証成功率と認証に要した時間（以下，認証時間）を確認する．被験者は，実験者より提案手法と注視型入力手法の説明を受け，視線入力と各認証手法について慣れるために練習する．

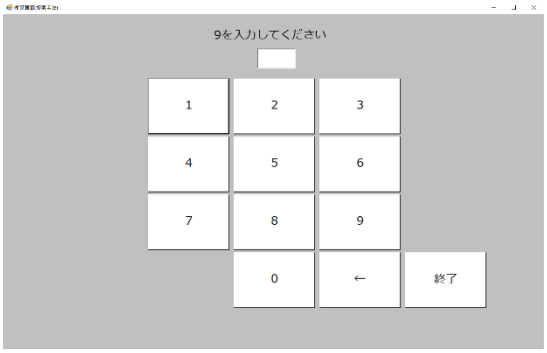

図 8　入力練習画面

図 8 は入力練習画面である．提案手法と注視型入力手法ともに同じ入力練習画面である．画面上部には数字がランダムに表示される．被験者は，表示された数字に従って入力を行う．練習時間は各認証手法につき 5 分程度行う．注視型入力手法については，注視時間 500ms，1000ms を 5 分の間で自由に変えて練習するように説明する．

練習後に各手法を用いて認証する．認証時は提案手法と注視型入力手法の注視時間 500ms，1000ms の 3 種類の手法を利用する．被験者は，PIN を 3 つ登録し，各認証手法について 3 回，計 9 回認証する．認証の順番は 8 人が初めに提案手法をし，その後に注視型入力手法 1000ms，500ms を実施する．残りの 8 人が初めに注視型入力手法 1000ms，500ms をし，その後に提案手法を実施する．注視型入力手法 500ms と 1000ms については，同じ入力手法のため，順番を変えずに認証を実施する．この実験では，各認証手法の認証成功率と認証時間を算出する．また，実験後に被験者は，「提案手法は，注視型入力手法と比較してどのくらい入力しやすかったですか.」という質問からなるアンケートに「入力しやすい，やや入力しやすい，変わらない，やや入力しにくい，入力しにくい」の 5 段階で回答する．

4.2.2 認証実験結果

各認証手法の認証成功率と平均認証時間を表 1 に示す．認証成功率について，提案手法は 54.2%と低い成功率で，注視型入力手法と比較すると，1000ms では 8%程度，500ms では 15%程度低い．平均認証時間については，提案手法は注視型入力手法と比較すると，1000ms では 3 秒程度，500ms では 5 秒程度長い．

表 1　認証実験結果　(n=16)

	認証成功率[%]	平均認証時間[s]
提案手法	54.2	9.759
注視 1000ms	62.3	7.466
注視 500ms	69.2	4.343

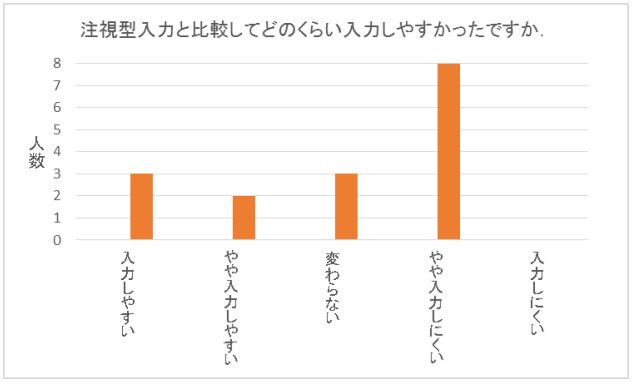

図 9　認証実験アンケート結果 (n=16)

認証実験後のアンケート結果を図 9 に示す．提案手法が注視型手法よりも「入力しやすい」または「やや入力しやすい」と答える人が 3 割程度，「入力しにくい」または「やや入力しにくい」と答える人が半数程度で，入力しにくいと感じる被験者の方がやや多い．

4.2.3 考察

提案手法は，注視型入力手法と比較すると認証成功率は

低かった．これは，提案手法ではマウスカーソルを動かす必要があるために注視型手法よりも視線がずれるなど視線入力の認識に問題が生じているためと推測できる．しかし，注視型手法も 60%台と低い認証成功率であった．被験者からのコメントの中に「数字を見たが反応してくれなかった．」や「隣接している部分の数字が入力されてしまった．」，「数字ボタンの間隔を空ければ使いやすくなりそう．」などの視線を使った入力に関する意見が複数あり，このことから，視線を用いた入力方法そのものが難しい可能性と，本提案手法に限っていえば，数字ボタンの配置やサイズに改善の余地があると考えられる．また，アンケート結果について，提案手法は，注視型入力手法よりも 10%程度認証成功率が低いため，必然的に「やや入力しにくい」と答える人が多かったと推測できる．

4.3 覗き見耐性実験

4.3.1 概要

覗き見耐性実験では，攻撃者が認証場面を覗き見ることで PIN（数字 4 桁）を窃取できるか，認証情報の入力に視線を使っていることを判別できるかの 2 点を確認する．実験では，提案手法と注視型入力手法の注視時間 1000ms を用いた．注視型入力手法で，注視時間 1000ms を採用した理由は，提案手法の認証時間は約 10 秒であり，同程度の認証時間にするために注視時間 500ms ではなく 1000ms を選択した．

この実験では，提案手法のフェイク動作の効果を評価するため，被験者はこれら 2 つの手法を知らない人を対象とする．なお，被験者は，4.1 節で説明した被験者と同一の 16 名であり，4.2 節の認証実験よりも先に実施する．

また，認証情報の PIN はランダムな 4 桁の数字を 2 つ用意し，手法と PIN による偏りを考慮し，手法と PIN の組み合わせにより被験者を 4 グループに分割する．表 2 に実験で使用する手法の順番と PIN を示す．

被験者は，提案手法と注視型入力手法のいずれの入力方法にも慣れた人が認証している場面を実際に見て，PIN を推測する．被験者は，認証している場面を自分の好きな位置から見ることができる．この実験では，推測した PIN とそれに対する被験者自身の確信度（自信の有無），被験者が覗き見した位置・場所を記録する．

表 2　各グループの手法と PIN の組み合わせ順

	1 回目		2 回目	
グループ	手法	PIN	手法	PIN
A	提案手法	9173	注視型	3158
B	注視型	3158	提案手法	9173
C	提案手法	3158	注視型	9173
D	注視型	9173	提案手法	3158

4.3.2 覗き見耐性実験結果

各手法の認証場面から PIN（数字 4 桁）を推測できた人数を表 3 に示す．提案手法では数字 4 桁のうち 1 桁推測できた人が 1 名，注視型では 6 名いた．しかし，推測できた全 7 名で確信度が高いと答えた人はいなかった．

表 3　各手法で PIN（数字 4 桁）を推測できた人数(n=16)

	推測できた人数			
	4 桁全て	3 桁	2 桁	1 桁
提案手法	0	0	0	1
注視型	0	0	0	6

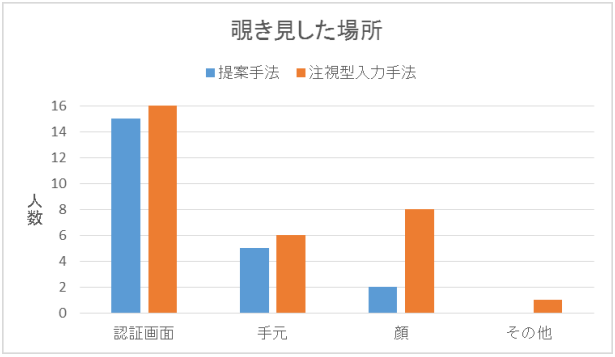

図 10　覗き見位置と人数（複数回答あり）

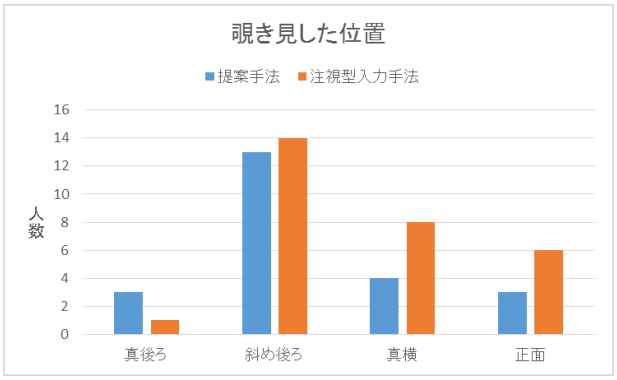

図 11　覗き見した場所と人数（複数回答あり）

また，覗き見位置の結果を図 10，覗き見場所の結果を図 11 に示す．なお，覗き見位置・場所について，被験者は複数回答可能である．覗き見位置に関しては，提案手法と注視型手法のどちらとも斜め後ろから見る人が多かったが，注視型手法については，正面や真横から見る人もいた．覗き見場所に関しては，提案手法と注視型手法のどちらとも認証画面を見る人が多かったが，注視型入力手法については，顔を見て推測する人も複数おり，中には，視線を使って認証していると判別できる人もいた．

4.3.3 考察

覗き見耐性については，提案手法と注視型入力手法のどちらとも PIN を 1 桁推測した人が数名いたが，どの被験者も高い確信度で回答したわけではなく，偶然当てることが

できたと考えられる．このことから，提案手法，注視型手法いずれも覗き見ることで PIN を窃取できず，覗き見耐性が高いといえる．また，被験者からのコメントには，「提案手法は普通に数字を入力していると思った.」,「注視型はどのように入力しているかわからなかった.」という提案手法，注視型入力手法いずれも認証方法の入力に視線を使っているかを判別できないことを示すコメントがあった．また，図 11 の覗き見した場所の結果をみると，注視型手法は顔を見る頻度が提案手法よりもはるかに多い．これは，注視型手法には入力動作がないため，被験者は入力方法について推測するために，位置を変えて顔を見たと考えられる．一方，入力動作がフェイクである提案手法は，認証画面を見る人数が他の場所よりも多く，注視型入力手法よりも入力に視線が使われていることが判別されにくいといえる．

4.4 録画攻撃実験

4.4.1 概要

録画攻撃実験では，認証手法の正面から見た時の攻撃耐性を確認する．被験者は 4.1 節で説明した情報系学部に所属する大学生 1〜3 年生の 16 名であり，提案手法と注視型手法両方を知っている．前節の覗き見攻撃実験と同様に，被験者を 4 つのグループに分け，推測する順番や PIN による推測しやすさなどの偏りをなくなるようにした．また，4.3 節と同様に認証情報の PIN は 2 つ用意した．表 4 に実験で使用する手法の順番と PIN を示す．

表 4　各グループの手法と PIN の組み合わせ順

	1 回目		2 回目	
グループ	手法	PIN	手法	PIN
A	提案手法	4869	注視型	1097
B	注視型	1097	提案手法	4869
C	提案手法	1097	注視型	4869
D	注視型	4869	提案手法	1097

本実験では，事前に提案手法と注視型入力手法を十分に練習した人（実験者）の認証場面を，正面と斜め後ろからビデオ撮影する．被験者は，正面と斜め後ろを同時に視聴可能な動画（図 12）を見て，認証情報の PIN を推測する．動画の再生時間はどちらの手法も約 10 秒程度である．動画の操作条件については，何度でも再生可能であり，停止や巻き戻しを自由に行うことができる．この実験では，推測した PIN とそれに対する被験者自身の確信度（自信の有無），推測までの所要時間を記録する．

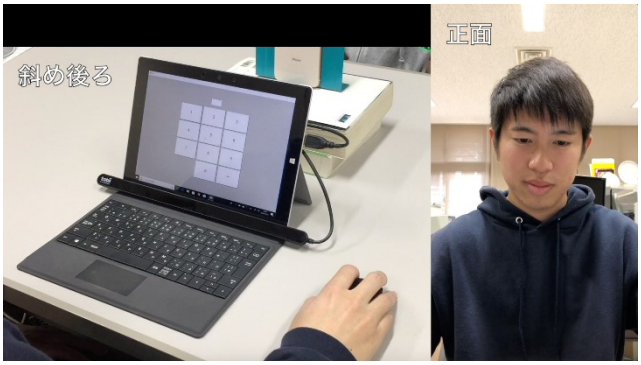

図 12　録画攻撃の動画

4.4.2 実験結果

各手法の認証場面から PIN（数字 4 桁）を推測できた人数と平均推測所要時間を表 5 に示す．提案手法では，4 桁全てを推測できた人はいなかったが，3 桁推測できた人は 3 名いた．注視型入力手法でも，4 桁全てを推測できた人はいなかったが，3 桁推測できた人は 2 名いた．また，推測の確信度が高いと回答した被験者で正解ではない数字を答えていた人が数名いたが，正しい数字の上もしくは下の数字を答えている場合が多かった．平均推測時間については，注視型手法の方が約 26 秒程度短かった．

表 5　各手法で PIN を推測できた人数と平均推測所要時間(n=16)

	推測できた人数				平均推測所要時間
	4 桁	3 桁	2 桁	1 桁	
提案手法	0	3	4	2	3 分 9 秒
注視型	0	2	0	2	2 分 43 秒

また，録画攻撃実験後に「提案手法について，注視型入力手法と比較してどちらが推測しやすかったですか.」という設問からなるアンケートを行った．アンケート結果を図 13 に示す．推測しやすさでは「提案手法」と答える人が 1 割程度，「注視型入力手法」または「変わらない」と答える人が半数程度いた．

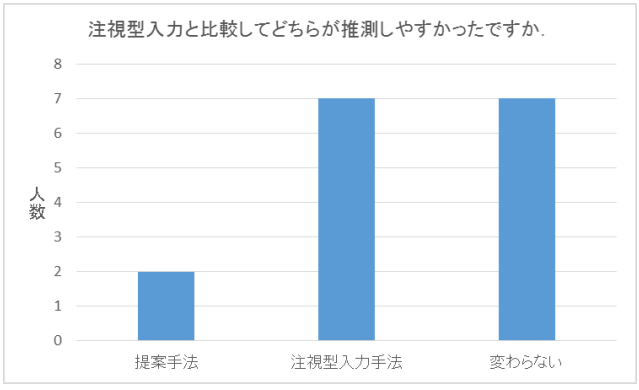

図 13 録画攻撃実験アンケート結果(n=16)

4.4.3 考察

録画攻撃実験では，提案手法と注視型手法のいずれも，4 桁全て推測できた人はいなかったものの，3 桁まで推測できた被験者が複数いることから，認証している人の顔を見るとある程度推測できることがわかった．また，被験者からの推測の理由に関するコメントで「視線が斜め下向きになっていたから.」や「2 桁目は視線が下へ移動していたから.」,「視線が順番に上がっており，画面の右側を見ていたため.」などがあり，数字を正確に推測できなくても，推測する数字が 2，3 個に絞られることがわかった．そのため，前節の覗き見攻撃実験で視線入力を行っていると判別されにくいという結果になった提案手法は，注視型手法に比べて有効であるといえる．また，図 13 のアンケート結果では注視型手法の方が推測しやすかったと答える人が半数程度いた．注視型手法は一定時間数字を見つめることで入力することができるが，提案手法ではマウスカーソルや数字ボタンを見る必要がある分，視線移動が多く，注視型手法よりも推測しにくくなったと考えられる．

5. おわりに

5.1 まとめ

本論文では，覗き見耐性の高い認証方式を実現するために，フェイク動作としてマウスクリックを利用した視線入力による認証方式を提案した．この認証手法ではマウスを使って数字ボタンをクリックする動作をフェイク動作とし，実際の入力は視線を利用する．また，認証画面は一般的な PIN 認証と同じであり，画面からでは視線入力を利用していることは判別困難である．提案手法の基本性能と有効性を評価するために，認証実験，覗き見攻撃実験，録画攻撃実験の 3 つを行い，視線のみで入力する注視型入力手法との比較した．その結果，認証実験では，提案手法は，マウスカーソルを動かす必要があるために注視型入力手法よりも視線の移動が多く，視線がずれるなど視線入力の認識に問題があり認証成功率が低く，認証時間も長くなるという結果となった．覗き見攻撃実験では，提案手法について数字 4 桁の PIN 全てを推測できる人はおらず，マウスクリックのフェイク動作があるため，視線入力で認証していると判別されにくいという結果になった．録画攻撃実験では，提案手法，注視型手法いずれも数字 4 桁全てが推測されることはなかったが，どちらの手法とも認証者の視線を観察することである程度推測できることがわかった．

5.2 今後の課題

前節より，提案手法の大きな問題点として，認証成功率が低いこと，攻撃者が視線を見た際にある程度数字が推測できるという 2 点をあげることができる．認証実験の際に被験者から「数字を見たが反応してくれなかった.」や「隣接している数字が入力されてしまった.」,「数字ボタンの間隔を空ければ使いやすくなりそう.」などの数字ボタンのレイアウトなど，提案手法のインタフェースに関わるコメントが複数あった．数字のボタンの配置や間隔について今後調査し改良することで認証成功率が高くなる可能性があると考える．また，録画攻撃実験の際には推測の理由として「視線が斜め下向きになっていたから.」など視線の動きや移動に関するコメントが複数あった．今度，視線を見られても認証情報の推測ができないようにするための対策を考える必要がある．

参考文献

[1] “総務省：平成 30 年版　情報通信白書｜PDF 版　ICT サービスの利用動向”. http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/pdf/n5200000.pdf, (参照 2018-12-12).
[2] 菊地 友斗，佐々木 慎吾，高橋 啓伸ほか：複数の認証手法を用いた視覚的なフェイク入りロック解除方式の提案，情報処理学会第 78 回全国大会，pp557-558，2016.
[3] Mohamed Khamis，Florian Alt，Mariam Hassib：GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices，CHI’16，pp2156-2164，2016.
[4] Dachuan Liu，Bo Dong，Xing Gao：Exploiting Eye Tracking for Smartphone Authentication，ACNS 2015，pp457-477，2015.
[5] Manu Kumar，Tal Garfinkel，Dan Boneh and Terry Winograd：Reducing Shoulder-surfing by Using Gaze-based Password Entry，SOUPS ‘07，pp13-19，2007.
[6] “Tobii Gaming | Powerful Eye Tracking for PC Games”. https://tobiigaming.com/, (参照 2018-12-12).