Computer Security Symposium 2017
23 - 25 October 2017

マウス操作を用いた個人認証方式のユーザビリティと覗き見耐性の実験と評価

長友 誠[1]　喜多 義弘[2]　油田 健太郎[3]　岡崎 直宣[3]　朴 美娘[1]

概要：現在，サービスのログイン・コンピュータのロック解除の個人認証に，キーボードでの文字列による認証が用いられる．近年では，その代替として，指紋などによる生体認証が普及している．生体認証は，記憶負荷がない利点があるが，生体情報が漏洩すれば再登録が難しくなる欠点がある．マウスを用いた生体認証には，マウス軌跡による署名を用いる研究があるが，覗き見耐性や録画耐性が無い問題点を持つ．本論文では，マウス操作を用いた覗き見耐性を持つ個人認証方式について検討する．マウスの操作で，マトリクス状のセルが持つ情報を一つずつ指定する方式を提案する．提案を実装し，ユーザビリティと覗き見耐性の実験を行い，それらの評価を行う．

キーワード：個人認証，覗き見耐性，マウス

Examination of Personal Authentication with Shoulder Surfing Resistance using Mouse Operations

Makoto Nagatomo[1]　Yoshihiro Kita[2]　Kentaro Aburada[3]　Naonobu Okazaki[3]　Mirang Park[1]

Abstract: Currently, password authentication by keyboard is mainly used. Biometric authentication is used as substitute of this method, and has advantage of no memory burden, but has difficulty of reregistration for the revealed information. There exists the method using mouse signature, but this method has no shoulder surfing and recording resistance. In this paper, we propose the authentication method having shoulder surfing resistance with mouse operations. The user specifies information that the matrix's cell has. We implement the proposed method, and perform experiments of usability and shoulder surfing, and evaluate the proposed method.

Keywords: Personal authentication, Shouldr surfing resistance, Mouse

1. はじめに

現在，公共の場でPCを用いて個人認証を行う機会が増えている．仕事場ではユーザが自身のパソコンのロックを解除し，ネットカフェなどでは公共のパソコンを使ってパソコンでフリーメールのサービスへのログインをする．公共の場でユーザが個人認証を行う際に，覗き見や録画による認証情報の漏洩が起こりやすい問題点がある [1]．これは，ユーザがキーボードを隠すことしないことが原因である．認証のたびにキーボードを隠すことは煩わしい．

近年，キーボードによる認証に変わる認証として生体認証が普及し始めている．生体認証には指紋や虹彩などの身体的特徴を用いた認証と，署名や歩行などの行動的特徴を用いた認証がある．身体的特徴を用いた認証は，記憶負荷がない利点があるが，情報が漏洩すると再登録が難しく，PCに多く普及していない問題点がある．PCにお

[1] 神奈川工科大学
Kanagawa Institute of Technology
[2] 東京工科大学
Tokyo University of Technology
[3] 宮崎大学
University of Miyazaki

いて，行動的特徴を用いた認証には，例えば，マウスの軌跡 [2], [3] や，マウスを使った署名を特徴として認証をする方式 [4], [5] が提案されている．しかし，これらは常に画面から視覚的なフィードバックを得ながら認証を行う必要があるため，覗き見や録画に対する耐性が低い．また，個人によって認証精度が変化してしまう問題点もある．

このように，デスクトップ，ノート PC において，覗き見耐性や録画耐性を持ち，かつ公共の場やパソコンで使える認証方式が存在しない．そこで本論文では，以前我々が提案した，デスクトップ PC やノート PC における，覗き見に対する耐性を持つ個人認証方式の提案 [6] について，5×5 のマトリクス上の場所をマウス操作を用いて指定する方式の覗き見耐性について検討し，1 回の録画耐性について考察する．

この方式では，また，認証時に視覚的なフィードバックを必要としない方式で，マウスを机の下に隠しながら認証を行うことができる．これによって覗き見に対する耐性が向上することが見込まれる．さらに，PC で使われるマウスを用いることにより，公共のパソコンでも認証が可能となる．

以下，2 章で関連研究の紹介，3 章で提案方式の説明，4 章で提案方式の実装を述べる．5 章で実験と評価を行う．6 章で録画耐性の考察をし，最後に 7 章で全体をまとめる．

2. 関連研究

2.1 マトリクス認証

マトリクス認証とは，ワンタイムパスワードの一種で，マトリクスの各セルに文字や数字がランダムに配置され，認証の際には，セル上にある文字や数字をキーボードで打つことによって認証を行う方式である．毎回ランダムに文字・数字が表示されるので，文字・数字だけが漏洩しても問題がない．例えば，SECUREMATRIX[7] は複数の 4×4 のマトリクスを用いた認証方式である．マトリクスの位置が認証情報であり，それを 1 つのイメージとして記憶できるのでユーザへの記憶負荷が少ない．しかし，キーボードとモニターを覗き見，または録画されると認証情報が漏洩する可能性がある．

2.2 覗き見耐性を持つ認証

PC で認証を行う，覗き見耐性を持つ個人認証には，認証方式 [8] がある．認証情報としてユーザに対する記憶負荷が少ないアイコンを用いている．認証する際には，パスアイコンを含むアイコン群がモニター上を動き回り，ユーザはパスアイコンを目で追いかけることでそのアイコンを選択することに替える．目のアイコン追跡の認識にはカメラを用いる．精度は高く，99%であるが，モニターの前にカメラを設置する必要がある．

スマートフォンでの個人認証には，STDS[9], Puzzle authentication[10], CCC[11] がある．STDS は 4×4 のマトリクス上にアイコンをランダムに表示し，登録したアイコンを選択する手法である．シフト規則を使い，本物のアイコンから離れたアイコンを選択することによって本物のアイコンを選択したことに替える．シフト規則を使えば，覗き見耐性が高くなるが，2 回の録画攻撃で情報が漏洩する可能性がある．

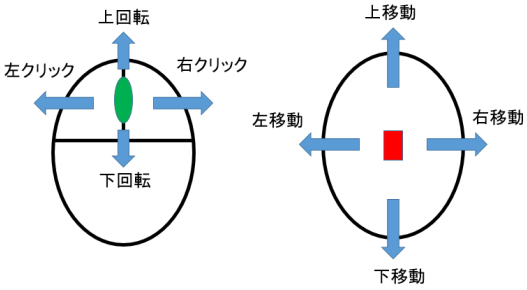

図 1 マウス (入力インタフェース)

Puzzle authentication は 4×4 のマトリクス上に数字をランダムに表示し，数字を入れ替えながら，登録した場所と数字を合わせる認証方式である．この方式では，数字を入れ替える際に，登録した数字と関係のない数字も入れ替えなければならないため，覗き見耐性が高い．しかし，覗き見耐性をつけたまま操作するには一定の慣れが必要である．

CCC は振動機能を用いた認証方式である．ダイヤルの上に数字が並んでおり，カーソルがダイヤルの上を回り続け，指定するべきダイヤルの上に来れば振動を行い，ユーザに場所を知らせる．ユーザはその場所に PIN をダイヤルを回して合わせる．この方式は，振動機能を用いて情報をユーザに伝える手法なので，他人に振動位置が判別される可能性が少なく，覗き見耐性を持つ．しかし，画面上の数字を直接手でタッチして選択する PIN を打つ速度に比べれば，振動で認証位置を特定する分，認証時間が遅くなる．

3. マウスを用いた認証方式

この章では，マウスを用いた覗き見耐性を持つ認証方式 [6] について説明する．入力インタフェースはマウス (**図 1**) であり，出力インタフェースはモニターに表示される $N \times N$ のマトリクス (**図 2**) である．ここで，マウスは，右クリック・左クリック・ホイールクリック・ホイール回転・マウス移動ができるマウスとする．

認証情報は，マトリクス上の複数場所とその選択した順番とし，ユーザはマウス操作のみを用いて登録する．認証を行う際は，登録と同じようにマウスを用いて登録した順番にマトリクス上の場所を指定する．登録と認証のプロセスは以下の通りである．

登録：

(1) $N \times N$ のマトリクスが表示される．初期位置はランダ

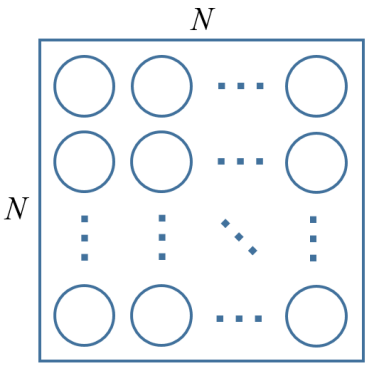

図 2 マトリクス (出力インタフェース)

ムに決定される．

(2) ユーザは登録したい場所にマウス操作を用いて移動し，登録する．マウス操作とその効果の組み合わせは，”右クリック：1 つ右に移動”，”左クリック：1 つ左に移動”，”上ホイール回転：1 つ上に移動”，”下ホイール回転：1 つ下に移動”，”ホイールクリック：現在位置を登録” である．現在位置は画面に表示され，ユーザが現在位置を確認しながら操作できる．

(3) 手順 (1), (2) を任意の回数繰り返す．

認証：

(1) 登録で表示した同じ大きさを持つマトリクスを表示する．初期位置はランダムである．

(2) ユーザは登録した場所にマウス操作で移動し，指定を行う．ここでは，初期位置だけが表示され，覗き見耐性をつけるために現在位置は表示されない．

(3) 手順 (1), (2) を登録した順番通りに指定を繰り返す．

この方式の利点は，マウスを隠すことにより覗き見耐性を高めることができる点である．例えば，机の下に隠す・マウスを操作している手をもう片方の手で隠す，などを行えば，攻撃者はマウスの音のみで認証位置を当てる必要がある．また，操作が直感的である．キーボードであれば隠して打つことが出来ない人が一定数いるが，マウスはマウスを見ずに操作可能である．既存のマウスを用いた手法は，マウスを机の上のみに置くことを前提としている．その他の場所では操作が難しいが，提案手法ではユーザの任意の場所で操作可能である．

4. 実装

提案を実装する際に，マトリクスの大きさとパスワードの長さを決める必要がある．1 回の認証で偶然に認証が成功する確率 (偶然認証確率) を 1/10,000 以下にすることを目標とする．$N \times N$ のマトリクスにおいて，m 桁のパスワードを設定したとすれば，偶然認証確率は，$1/N^{2m}$ である．今回は，[6] で実装したものと同じ 5×5 のマトリクスを用いて覗き見耐性の実験を行うので，N=5 であり，偶然認証確率は $1/5^{2m}$ となる．$1/5^{2m} \leq 1/10{,}000$ である m は

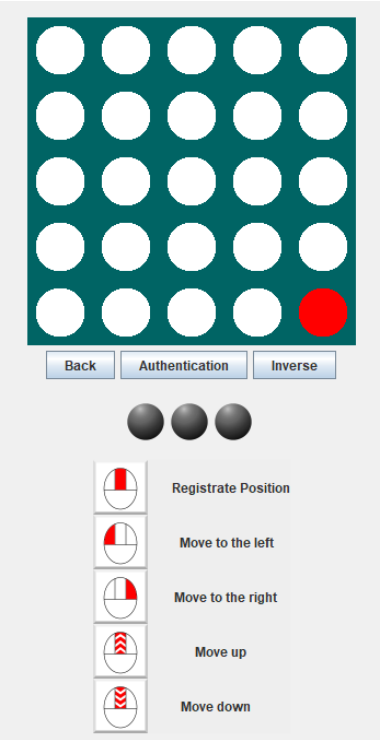

図 3 認証画面

$m \geq 3$ であるので，ユーザが登録できるパスワードの長さを 3 桁以上にした．

座標の移動については，初期位置が認証位置に近ければ覗き見で認証位置が漏洩する可能性が高くなるので，覗き見耐性をつけるために最低 3 回移動しなければ登録ができないようにした．

認証画面を**図 3** に示す．マトリクス中には赤色の初期位置が表示れさる．マトリクスの下に，左から back ボタン，authentication ボタン，inverse ボタンを配置した．back ボタンは最後に選択した場所を消去するボタン，authentication ボタンは認証を行うときに押すボタン，inverse ボタンはユーザがマウスを机の裏で操作することを想定し，マウスの操作が左右逆になるボタンである．ボタンの下にはインジケータと，ユーザがマウス操作の方法を忘れても思い出せるよう，操作説明を追加している．以下で登録段階と認証段階の例を 1 つずつ挙げる．

登録段階 (図 4)：

この段階で，ユーザは対角線上の座標 (1, 1)，(3, 3)，(5, 5) をこの順番で登録したいとする．各座標の位置はホイールクリックで登録できる．

(1) 5×5 の初期位置 (3, 3) がランダムに選択されたマトリクスが表示される．ユーザはホイール上回転を 2 回，左クリックを 2 回行い，座標 (1, 1) を登録する．

(2) 初期位置が (2, 2) であるマトリクスが表示される．ユーザはホイール下回転を 2 回，右クリックを 1 回，ホイール上回転を 1 回を行い (3, 3) に移動し登録する．(2, 2) から (3, 3) まで移動するための最低操作回

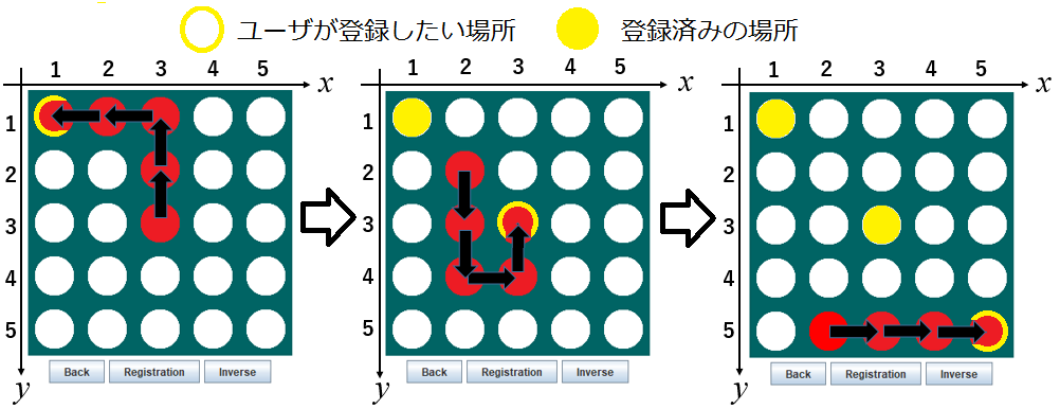

図 4 登録段階

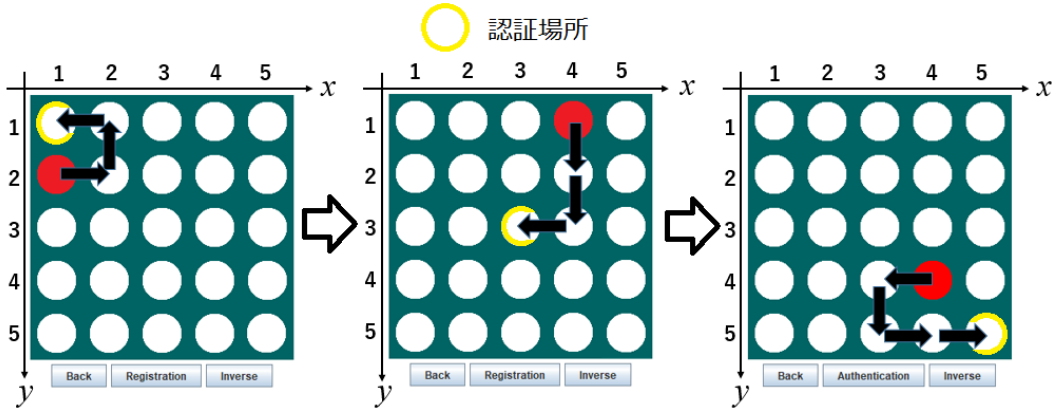

図 5 認証段階

数は 2 回である．3 回以上の移動を行うために回り道をした．

(3) 初期位置が (2, 5) であるマトリクスが表示される．ユーザは右クリックを 3 回行なって座標 (5, 5) に移動し登録する．

(4) registration ボタンを押し，((1, 1), (3, 3), (5, 5)) が登録される．登録した順番も認証情報に含まれることに注意する．

認証段階 (図 5)：

ユーザは上述した ((1, 1), (3, 3), (5, 5)) を登録したと仮定する．各座標の指定はホイールクリックで行うことができる．

(1) 初期位置 (1, 2) がランダムに選ばれた 5×5 のマトリクスが表示される．ユーザは右クリックを 1 回，ホイール上回転を 1 回，左クリックを 1 回行い，(1, 1) に移動し，指定する．初期位置だけが赤く常に表示され，座標を移動している間，現在位置は表示されない．ユーザは自分が行うマウス操作で現在位置を認識する．

(2) 初期位置が (4, 1) であるマトリクスが表示され，ユーザは下ホイール回転を 2 回，左クリックを 1 回行い (3, 3) に移動し，指定する．

(3) 初期位置 (4, 4) のマトリクスが表示され，ユーザは左クリックを 1 回，ホイール下回転を 1 回，右クリックを 2 回行い (5, 5) に移動し，指定する．

(4) authentication ボタンを押し，((1, 1), (3, 3), (5, 5)) が指定され，登録した情報と一致し，認証成功となる．

5. 提案手法のユーザビリティと覗き見耐性の実験

5.1 実験環境および手順

提案した認証方式について，ユーザビリティの実験は [6] で行った．神奈川工科大学の学生 20 人を被験者とし，操作のチュートリアルと，登録，認証，アンケートを行なった．認証は 3 回成功するまで行ってもらい，認証時間を測った．アンケートでは，5 つの項目（理解しやすさ，使いやすさ，慣れれば使いやすさ，覗き見に対する安全性，また使いたいか）を 1-5 の 5 段階で調べた．本論文では提案した方式に覗き見の耐性があるかどうかの実験を理想的な環境で行う．理想的な環境とは，攻撃者が覗き見をする際に認証情報の推測材料の取得を阻害するものが無い環境のことである．実験の環境と実験手順は以下の通りである．

実験環境：

被験者　神奈川工科大学の学生 16 名

実験マウス　クリック音が明瞭に聞こえるマウス（ロジクール/ワイヤレス光学式マウス M186）

認証する人　椅子に座り，マウスを机の下に隠し，モニ

表 1 10 回覗き見を行なった時の各桁数の特定率

	1 桁	2 桁	3 桁
特定率	22.8%	8.6%	1.4%

ターを見ながら認証

覗き見する人　認証する人の右，左斜め後ろ 1m 以内で覗き見をする．モニターに映っている初期位置と，親が行うマウス操作によるクリック音，ホイール回転の音や入力時間を推測材料とし，認証位置を推測する．覗き見をしている間はノートを取っても良い．

実験手順：

(1) 5 または 6 人の班を作る
(2) 班の中から親を 1 人決める
(3) 親が 3 桁のパスワードを登録する．その他の被験者は登録の様子を見ない．
(4) 親は 10 回成功するまで認証を行う．この時，同じ班の他の被験者は親の後ろから覗き見を行う．
(5) (2)-(4) を班の全員が親を終えるまで行う．

以上の実験を 6 人の班を 1 つ，5 人の班を 2 つで合計 3 つの班に分けて行なった．

5.2 実験結果

ユーザビリティの実験において，チュートリアルにおいて操作に慣れるまでの時間は 1 分未満であり，認証を行った際の 3 回目成功の認証時間は平均で約 15 秒であった．

覗き見耐性実験について，被験者 16 人の中で，1 人は 3 桁全てを推測された．15 人は 1 桁以上を推測された．実験から得られた，ユーザが 10 回の覗き見をされた時の，1 桁，2 桁，3 桁の認証情報の特定率を**表 1** に示す．本論文では，ユーザが 5 章で示した覗き見をする理想的な環境で 10 回認証が成功するまで行い，覗き見による 3 桁全て特定された割合はわずか 1.4%であった．現実的な場面では更に認証位置が推測される可能性が低くなる．例えば，公共の場での環境は，マウスクリック音は周りに聞こえやすいが，ホイール回転は聞き取りにくい．また，クリック音が聞こえにくいマウスもあり，そのマウスを使えば認証位置を当てることは不可能になる．よって，提案した認証方式は覗き見に対する耐性があると言える．

アンケートについて，使いやすさに関しては，平均が約 3 であり，慣れによる使いやすさの平均は約 4 であった．また，覗き見に対する安全性は 4.5 以上であった．よって，本提案法式はユーザビリティが確保されている．

6. 録画耐性に関する考察

この章では，提案手法を実装した 5×5 のマトリックスにおける，1 回の録画耐性に関する考察を行う．攻撃されるユーザは，最短操作回数で認証を行うとし，ホイール音とクリック音が聞き取れるとする．ホイール音は上下どちらか，クリック音は左右どちらかに移動したかを示す．

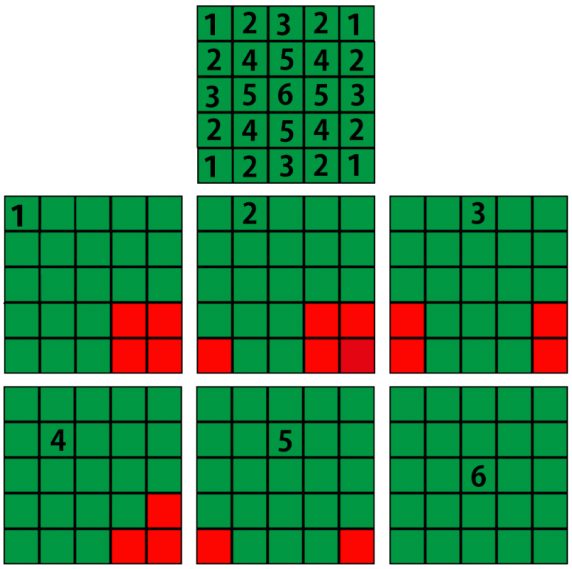

図 6 各位置における特定される初期位置

図 6 は各位置における，1 回の録画で認証位置が特定される箇所を表している．各番号の認証位置に対して，赤色の場所が初期位置である場合に，認証位置が特定されることを表している．同じ番号の場所は対称の関係にあるので省略している．

例えば，1 の場所が認証位置の場合（図 6 中段左）を考える．**図 7** において，赤の場所から 1 の場所に移動する場合，マウスクリックを 3 回，ホイール回転を 3 回行う必要がある．それらの操作で最短距離で到達できる場所を黄色で表すと，1 のみである．**図 8** においては，マウスクリックを 2 回，ホイール回転を 2 回行う必要があり，移動時に最低移動回数が 3 回であることを考慮すれば，認証位置の可能性がある場所が複数個ある．

各 1〜6 の場所において，ランダムに初期位置が設定された場合に認証位置が特定される確率は，4/25, 5/25, 4/25, 3/25, 2/25, 0 であり，各番号の個数は 4, 8, 4, 4, 4, 1 である．よって，ユーザがランダムに認証位置を 1 つ設定する場合，録画攻撃で特定される確率は，

$$(4(4/25) + 8(5/25) + 4(4/25) + 4(3/25) + 4(2/25))/25 = 0.14$$

である．3 桁の場合は $(0.14)^3 = 0.003$ となり，実装した提案手法は 1 回の録画攻撃に対する耐性がある．

7. まとめ

本論文では，マウス操作を用いた個人認証方式について，覗き見耐性の実験と録画耐性についての考察を行なった．覗き見実験は理想的な環境で，学生 16 人に対して実験を行なった．16 人中 15 人の被験者が 1 桁以上を推測されたたが，その中で 11 人が 1 桁のみ推測された．全ての

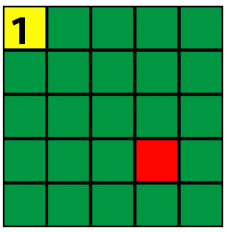

図 7 1 つに特定される場合

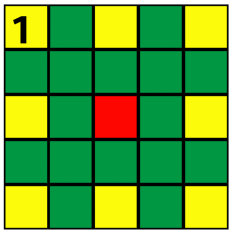

図 8 複数可能性がある場合

認証位置 3 箇所を推測された被験者は 1 人のみであった．マウス音だけで認証位置が漏洩する可能性があることがわかったが，現実の環境では覗き見に対する耐性がある．また，1 回の録画に対する耐性があることがわかった．今後の課題を以下に述べる．

- マウスの音による覗き見耐性の低下への対策
  今回の実験で，提案手法では覗き見でパスワードが漏洩する可能性があることが分かった．提案手法の覗き見耐性を更に上げる手法として，パソコンからダミーの音を出す手法や，ダミーの場所移動をする手法が考えられる．
- ユーザビリティの改善
  本論文で紹介した手法では，[6] で実験したように，ユーザビリティは確保できているが，高いとは言えない．出力インタフェースを $N \times N$ のマトリクス以外を用いることで改善する可能性がある．
- 録画耐性の評価と対策
  本論文では 1 回での録画耐性のみを評価したが，複数回の録画が行われた時の考察をする必要がある．

参考文献

[1] Davide Balzarotti, Marco Cova, Giovanni Vigna, *ClearShot: Eavesdropping on Keyboard Input from Video*, Proceedings of the 2008 IEEE Symposium on Security and Privacy, pp. 170-183, 2008.

[2] Masud Karim, Hasnain Heickal, and Md. Hasanuzzaman, *User Authentication from Mouse Movement Data Using Multiple Classifiers*, Proceedings of the 9th International Conference on Machine Learning and Computing, pp. 122-127, 2017.

[3] Nan Zheng, Aaron Paloski, and Haining Wang, *An Efficient User Verification System via Mouse Movements*, Proceedings of the 18th ACM conference on Computer and communications security, pp. 139-150, 2011.

[4] Ross A, J. Everitt, Peter W. McOwan, *Java-Based Internet Biometric Authentication System*, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.25, no.9, pp. 1166-1172, 2003.

[5] 渡辺優，西山裕之，*Support Vector Machine* を用いたマウス認証による個人認証方法の提案, The 27th annual Conference of the Japanese Society for Artificial Intelligence, 2013.

[6] 長友誠，朴美蘭，岡崎直宣，覗き見耐性を持つマウス操作を用いた個人認証方式の提案，コンピュータセキュリティ (CSEC) 研究報告，2017.

[7] ”CSE: SECUREMATRIX” https://www.cseltd.co.jp/product/smx/, (参照 2017-08-01).

[8] Vijay Rajanna, Seth Polsley, Paul Taele, Tracy Hammond, *A Gaze Gesture-Based User Authentication System to Counter Shoulder-Surfing Attacks*, Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp.1978-1986, 2017.

[9] 喜多義弘，岡崎直宣，西村広光，鳥居秀幸，岡本剛，朴美娘，覗き見耐性を持つユーザ認証システムの実装と評価, 電子情報通信学会論文誌，vol. J97-D, no.12, pp. 1770-1784, 2014.

[10] Yoshihiro Kita, Kentaro Aburada, Mirang Park, Naonobu Okazaki, *Proposal of a Puzzle Authentication Method with Shoulder-sufing Attack Resistance and High-usability*, IEICE ComEX, vol.4, no.3, pp.95-98, 2015.

[11] 石塚正也，高岡哲司，CCC: 振動機能を応用した携帯端末での個人認証方式における覗き見攻撃対策手法の提案，情報処理学会インタラクション 2014，pp.501-503，2014.