博士論文

キー操作とマウス操作の
動的バイオメトリクスを用いた
継続認証に関する研究

2020年9月

鹿児島大学大学院
理工学研究科　総合理工学専攻

山田　猛矢

目 次

第1章　はじめに

1.1　研究背景

サイバー攻撃，サイバー犯罪は年々増加しており，2018 年においては，仮想通貨交換業者等への不正アクセス等による不正送信事犯の被害額は約 677 億 3,820 万円相当であった [1]．不正アクセス行為の手口としては,「利用権者のパスワードの設定・管理の甘さにつけ込んだもの」が 55.4%と半分以上となっている．これは利用権者の ID，パスワードの設定・管理の難しさを表している．近年の不正アクセスによる具体的な事案として，2019 年 1 月に株式会社オージス総研がクラウド環境上で運営しているファイル転送サービス「宅ファイル便」が不正アクセスを受け，ログ分析の結果，悪意のある第三者による不正な操作の実行が確認された事案がある．その結果，約 481 万件の情報（氏名，ログイン用メールアドレス，ログインパスワード，生年月日，性別，職業，居住都道府県名，メールアドレス 2，メールアドレス 3）が漏洩したことが発覚した．漏洩した情報にはパスワードも含まれていたため，リスト型攻撃による 2 次被害も懸念されている．2018 年 8 月には，大阪医科大学で教師用パソコンに貼られていたシールに書かれていた ID とパスワードを利用して講義データを USB メモリに保存して持ち帰ったところ，メモリ内に保存されていたバックアップソフトにより，患者データ 46 万件が流出したという事案もある．過去（1995 年）にはオーストラリアで病院のコンピュータにアクセスし，患者に投与すべき医薬に係るデータを改ざんし，事情を知らない看護師が改ざんされたデータ通りに薬を与えたため，患者が死亡した例もある．大阪医科大学の学生の動機は講義データの入手にあったが，セキュリティの低さがもたらす非常に怖い話である．また，2014 年 5 月には，インターネット上に流出していた他人の ID，パスワードを多数入力して大手通販サイトのサーバに不正アクセスし，サーバ内に保存されている他人の ID を変更するとともに，他人に成りすまして商品を購入したという事件もある．このような状況の中，不正アクセスに対する対策は非常に重要であり，セキュリティ強化は喫緊の課題である．

さて，このような状況の中，現在のコンピュータのユーザー認証に目を移すと，ログイン時に ID とパスワード，バイオメトリクス認証（生体認証）など，ログイン時だけチェックを行うものがほとんどである．そのため，コンピュータの前を離れるときに画面ロックを掛け忘れると，不正ユーザーに容易に操作されてしまい，甚大な被害を被る可能性がある．不正ユーザーが容易に操作できる状態はセキュリティレベルの低い状態であり，何かしらの対策を講じ，セキュリティを高める必要がある．

セキュリティを高める 1 つの方法として，ログイン後も継続的に認証を行う継続認証という認証方法がある．継続認証を行うにはいくつかの方法がある．1 つは従来型の ID とパスワードによる認証を定期的に行う方法である．ID とパスワードによる認証方式の利点は，認証精度が 100%であるということである．この利点を活かし，定期的に ID とパスワードの入力を求めることで継続認証を行うというものである．しかしながら，この方法はコンピュータでの作業中に何度も ID とパスワードが求められ，そのたびに作業が中断されユーザー負担が大きくなってしまう．また，この方法の課題として「漏洩」がある．ID とパスワードが漏洩してしまうと，継続認証を行っていたとしても不正ユーザーが自由に操作可能となる．

ID とパスワードによる継続認証の他に，バイオメトリクス継続認証がある．バイオメトリクスには，身体的特徴を用いた認証と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としては，指紋認証や虹彩認証，顔認証などがある．これらの認証方法は精度も高く実用的であり，継続認証にも応用可能である．しかしながら，これらの認証にも課題がある．指紋認証においては，前述の ID とパスワードによる継続認証と同様，定期的に認証を求められるためユーザー負担が大きくなる．一方，虹彩認証，顔認証においては，ユーザー負担は軽減されるものの，専用の機器が必要であり，認証コストが大きくなる．また，顔認証においては常に外部にさらされているため，容易に偽造が可能である．さらに，リモートアクセスにおける継続認証においては，認証情報を送信する必要があるため情報漏洩やプライバシー侵害の課題がある．上記に加え，身体的特徴を用いた認証の問題点として，1 度盗まれると本人であるにも関わらず，2 度とそれを認証に使えなくなるという問題点を有する．

そこで我々が着目したのが行動的特徴による継続認証である．行動的特徴を用いた認証には，筆跡，声紋，歩容などがあるが，コンピュータのセキュリティに使用可能なものに，キー操作・マウス操作から得られる特徴量を用いた認証がある．身体的特徴を用いた認証に比べ，認証精度，認証速度は劣るものの，ユーザー負担が小さく，専用の機器を導入する必要もない．また，偽造がされにくくプライバシー性も低いため，心的ストレスもなく導入もしやすい．現在の認証システムとの組み合わせも容易なため，継続認証を融合することによりセキュリティ強化が見込める．

本論文では，キーボード，マウスの操作から得られる特徴量を用いた継続認証のための新規アルゴリズムを提案する．

1.2 キー操作・マウス操作による継続認証

継続認証の重要性を最初に提唱したのは，D. Umphrees, G. Williams の論文（1985）[2] である．しかしながら，この論文では決められた文字のキー入力タイミングによる認証を行っており，現在の継続認証とはかけ離れている．現在行われている継続認証の始まりは 2000 年を過ぎた辺りからで，この頃はキー操作による認証研究が盛んで，マウス操作による認証研究は少ない．キー操作による認証研究としては，キーの押下

時間を測定し χ^2 検定により正規ユーザーか不正ユーザーかを判定するもの [3] や 2 連字キー，3 連字キーの入力タイミングにより [4] 判定するものがあった．その後，2010 年を越えたあたりから，正規ユーザーか不正ユーザーかの分類に機械学習が利用され始めた．またこの頃になるとマウス操作による認証研究も行われ始めた．

キー操作から得られる特徴量としてはキー押下時間，2 連字キーの入力タイミングが主流で，正規ユーザーか不正ユーザーかを分類する方法として様々な機械学習アルゴリズムが試されていった．多層パーセプトロン [5, 6]，決定木 [7]，k 近傍法 [8, 9, 10, 11, 12]，サポートベクターマシン [7, 12, 13, 14, 15]，リカレントニューラルネットワーク [16]，カオスニューラルネットワーク [17]，混合ガウスモデル [18]，多次元ガウス密度関数 [19]，また，畳み込みニューラルネットワークとリカレントニューラルネットワークの組み合わせ [20] などを使用して分類が行われ，キー操作における適切な機械学習は何かが調べられていった．またマウス操作による認証にも機械学習が利用され始め，サポートベクターマシン [21]，ニューラルネットワーク [22] などが試された他，マウスアクションを階層化し応答時間を短縮しながら精度を高める研究 [23] 等も行われた。また，検出速度を高めるためにキー操作とマウス操作を組み合わせて認証を行う研究 [24, 25, 26] も始まった．さらに，Web メール [27]，ショートメッセージサービスのメッセージログ [28]，Web セッション [29, 30]，パスワード入力タイミング [31] など様々な場面での継続認証研究が行われた．

そのような中，キー操作，マウス操作のデータベースの必要性が叫ばれ，Web アプリケーションを使用したデータベースの作成 [32]，決められたパスフレーズ，画像を見て何をしているか自由に書く，決められた文字の入力（英語）[33] でデータベースが作成された．しかしながら，若い年齢層に偏ったデータとなっており，また全て英語のデータということから，年齢，言語など限定的であり適切ではない [34] という意見もある．

近年では，英語だけでなく韓国語 [35, 36] やアラビア語 [37] の研究も行われ，言語の違いによる特徴もわかりつつある．また，機械学習においても，学習データに対して事前に意味不明なテキストを除外したり [38]，人工的に学習データを生成したり [39]，正規ユーザーのデータに不正ユーザーのデータを入れる [40] などして学習効果を高めている．また機械学習アルゴリズムを組み合わせたり [41]，行動プロファイリングを組み合わせる [42] などして認証精度を高めている．その他，キーを押すときの圧力の利用 [43]，キー操作をアナログの電気信号に変換するキーボードを作成し認証に利用 [44]，筋電図を利用 [45] する研究もある．

認証精度の評価方法としては，本人拒否率（False Recognition Rate（FRR））, 他人受入率（False Acceptance Rate（FAR））および FRR と FAR が一致するように閾値を調整した等価エラー率（Equal Error Rate（EER））が一般的に用いられる．しかしながら，これらの評価だけでは不十分であるためジニ係数を用いるべきという主張 [46] や後述する継続認証性能表を用いるべきという主張 [47] もある．

継続認証の課題としては不正ユーザーの検出速度が 1 番に挙げられるが，その他，1 日の間でも疲れが出たりするとタイピングパターンが変わるという指摘 [48] や時間とと

もに変化するタイピングリズムに対する経時変化にどう対応するのか [49] などもある．

多くの研究が行われる中，継続認証の評価の高い方法に Dynamic Trust Model（DTM）がある [52]．DTM は，Trust Model（TM）[50] を改良し認証精度を高めたものであり，様々な研究が行われている [47, 51, 53]．これらの研究は本研究との関係が深いため，第 2 章で詳しく述べる．

1.3 研究目的と本論文の構成

本研究の目的は，

- キー操作・マウス操作から得られる特徴量を用いた継続認証アルゴリズム Dynamic Probability Trust Model（DPTM）の提案
- 評価実験により DPTM の有用性の確認
- 既存研究である DTM との比較および優位性の主張

である．

第 2 章では，本研究と関連の深い Trust Model（TM），Dynamic Trust Model（DTM）について説明し，その課題について明らかにする．

第 3 章では，本研究で新たに提案する DPTM について解説する．まず DPTM の骨子について詳細に説明し，その後，DPTM に現れるパラメータの決定方法について説明する．

第 4 章では，DPTM の有用性を確認するために行った評価実験およびその結果について記述する．正規ユーザーか不正ユーザーかを判定するための閾値を変化させ，本人拒否率（FRR），他人受入率（FAR）を計算し，そこから等価エラー率（EER）を算出する．また継続認証性能表も作成する．

第 5 章では，既存研究である DTM との比較実験およびその結果について記述する．DTM の FRR，FAR を計算し，EER 算出後，継続認証性能表を作成する．

第 6 章では，認証精度，DTM との比較，ユーザープロファイルの更新，動的パラメータ α_i の初期値 α_{i0} の個人識別可能性に関する考察を行う．

第 7 章では，本研究の成果についてまとめ，今後の課題について述べる．

第2章　関連研究

本章では，本研究に関係の深い Trust Model（TM）と Dynamic Trust Model（DTM）について述べる．

2.1　Trust Model

Trust Model（TM）は，不正ユーザーをできるだけ早く検出するために提案された継続認証アルゴリズムである [50]．TM が提案される前までは決められた時間または決められた操作数ごとに正規ユーザーか不正ユーザーかを判定してきた．しかしながら，この方法では，決められた時間または操作数の間，不正ユーザーが自由に操作できてしまう．そこで，TM では Trust 値と呼ばれる値 T を導入し，決められた時間，操作数に達しなくても Trust 値の変動により不正ユーザーを検出し，ロックアウトを可能にした．操作が行われるごとに Trust 値を変動させ，ある閾値を下回ると不正ユーザーと判断しロックアウトする．Trust 値の変動のさせ方としては，ユーザーの操作ごとに得られる特徴量と正規ユーザーの特徴量を比較し，特徴量が近い値であれば Trust 値を上げ，遠い値であれば下げるというものである．また，Trust 値には上限が決められている（文献 [50] では 100）．これは正規ユーザーが操作を続けたとき，Trust 値の上限を決めていなければ，Trust 値が非常に大きな値となるためである．Trust 値が非常に大きい値のとき不正ユーザーが操作をしても，閾値を下回るまでに長い時間がかかってしまい，長く操作を続けることができてしまう．Trust 値の上限を決めることで，不正ユーザーの早期検出が可能となる．

TM では，まず本人のキー操作のログデータを収集する．次に収集したログデータから各キーの押下時間を計算する．具体的には，i 回目にキー k が入力されたとき

$$d_{i,k} = t_{i,k}^{\mathrm{up}} - t_{i,k}^{\mathrm{down}} \tag{2.1}$$

を計算する．ただし，$t_{i,k}^{\mathrm{down}}$ は i 回目にキー k が押された時間を表し，$t_{i,k}^{\mathrm{up}}$ は離された時間を表す．この押下時間 $d_{i,k}$ の平均

$$\mu_k = \frac{1}{n}\sum_{i=1}^{n} d_{i,k} \tag{2.2}$$

(2.3)

および標準偏差

$$\sigma_k = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(d_{i,k} - \mu_k)^2} \tag{2.4}$$

を計算する．ただし，n は入力回数である．この平均 μ_k，標準偏差 σ_k から距離

$$D_j = \frac{|\mu_k - d_{j,k}|}{\sigma_k} \tag{2.5}$$

を定義し，この距離 D により Trust 値を変化させる．ただし，$d_{j,k}$ は継続認証中，j 回目に入力されたキー k の押下時間である．

式（2.5）の距離 D_j を用いて Trust 値 T を変化させる．その際，閾値 T_D を設定し，距離 D_j が閾値 T_D より小さければ Trust 値 T を増加させ，大きければ Trust 値 T を減少させる．

キーが 2 回連続で入力された場合（2 連字キー）は，次のようにして距離 D_j を決める．j 回目に p が入力され $j+1$ 回目に q が入力された場合

$$\tilde{d}_{j,\mathrm{p}} = \frac{|\mu_\mathrm{p} - d_{j,\mathrm{p}}|}{\sigma_\mathrm{p}} \tag{2.6}$$

$$\tilde{d}_{j+1,\mathrm{q}} = \frac{|\mu_\mathrm{q} - d_{j+1,\mathrm{q}}|}{\sigma_\mathrm{q}} \tag{2.7}$$

$$\tilde{d}_{j,\mathrm{pq}} = \frac{|\mu_\mathrm{pq} - d_{j,\mathrm{pq}}|}{\sigma_\mathrm{pq}} \tag{2.8}$$

から，距離

$$D_j = \frac{\tilde{d}_{j,\mathrm{p}} + \tilde{d}_{j+1,\mathrm{q}} + \tilde{d}_{j,\mathrm{pq}}}{3} \tag{2.9}$$

を決める．ただし，$d_{j,\mathrm{pq}}$ は p が離されてから q が押されるまでの時間

$$d_{j,\mathrm{pq}} = t^{\mathrm{down}}_{j+1,\mathrm{q}} - t^{\mathrm{up}}_{j,\mathrm{p}} \tag{2.10}$$

であり，μ_pq は $d_{i,\mathrm{pq}}$ の平均，σ_pq は標準偏差である．キー押下時間および 2 連字キーから得られる距離 D_j（式（2.5）, (2.9)）より Trust 値 T を変動させ不正ユーザーを検出する．

TM が提案された文献 [50] では，収集したログデータ量の関係で押下時間に使用したキーが E，A，T，I，N，O，S，L，スペースキー，バックスペースであり，2 連字キーとして使用されたのが AT，TH，HE，ME，AN，IC，IS，OF，TE，BE，OC，OR，BY であった．これらのキーを用いて，まず Trust 値の初期値

$$T_0 = 100 \tag{2.11}$$

とし，キー操作が行われるごとに距離 D_j を計算し，$D_j < T_D$ のとき Trust 値

$$T_{j+1} = \min\{T_j + R, 100\} \tag{2.12}$$

と Trust 値 T の値を更新する．ただし，$\min\{X, Y\}$ は X, Y のうち小さい方の値を取ることを意味する．また，$D_j \geq T_D$ のとき Trust 値

$$T_{j+1} = T_j - (D_j - T_D). \tag{2.13}$$

と更新する．なお，上記キー以外のキー操作が行われた場合は

$$T_{j+1} = T_j - \alpha \tag{2.14}$$

とする．式中の T_D, R, α はパラメータであり，文献 [50] では $T_D = 0.5, R = 1.3, \alpha = 0.01$ と設定している．そのほかに設定しなければならないパラメータとして，不正ユーザーと判定するための閾値 T_{lockout} がある．T_{lockout} の設定値については，文献 [50] では正規ユーザーが不正ユーザーと判定されない固有の値としている．つまり，本人拒否率を 0 とするように T_{lockout} を決めている．

図 2.1 は正規ユーザーが操作を行った時の Trust 値の変動である．縦軸に Trust 値を取り，横軸に Event Number を取っている．Event Number はキー操作が行われるたびに加算される数であり，キー操作の回数を表す．また，文献 [50] では不正ユーザーと判定するための閾値 $T_{\text{lockout}} = 90$ としている．図 2.1 を見ると，Trust 値は 100 に近いところで変動していることがわかる．図 2.2 は不正ユーザーがキー操作を行ったときの Trust 値の変動である．図 2.2 を見ると，操作数 500 の間に 5 回，閾値 90 を下回っているのがわかる．なお，閾値を下回ったとき，Trust 値は再び 100 に戻している．定期的に不正ユーザーかどうかのチェックを入れる場合，その時間，操作数に達するまで不正ユーザーと判断できない．しかしながら，図 2.2 の 3 回目に閾値を割ってから 4 回目，5 回目と TM ではすぐに不正ユーザーを検出できる．TM により不正ユーザーの早期検出が可能となった．

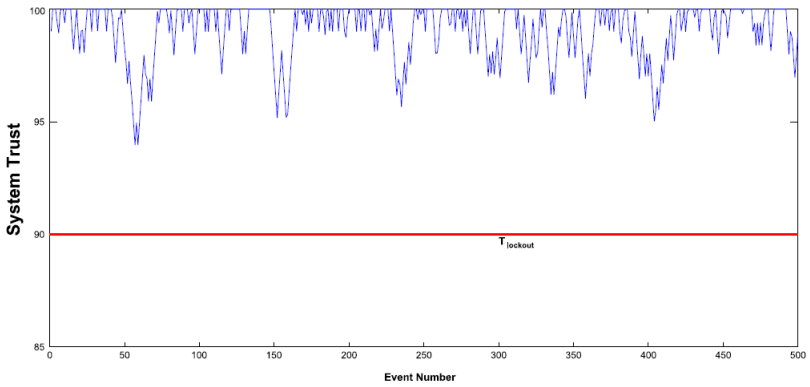


図 2.1: 正規ユーザーが操作したときの Trust 値の変動

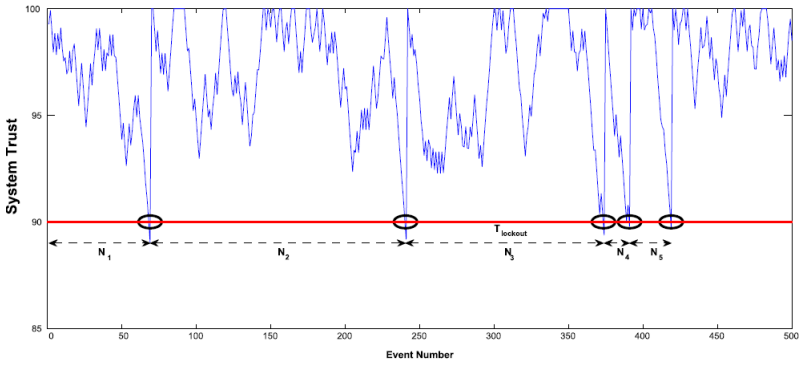


図 2.2: 不正ユーザーが操作したときの Trust 値の変動

文献 [50] での評価実験では，24 人のユーザーを対象に行われ，不正ユーザーの検出までにかかるキー操作数の平均が 98 という結果を得ている．なお，一般的な生体認証の評価を行うものに本人拒否率（False Recognition Rate（FRR））, 他人受入率（False Acceptance Rate（FAR））がある．しかしながら，TM の提案者である P.Bours はこれらの評価は継続認証には不適切であると主張している．たとえ不正ユーザーを検出できたとしても，検出までに長い時間がかかっていては意味がなく，その間に様々な操作が可能となるからである．FAR が 0 だったとしても，検出までに長い時間がかかってしまっては，FAR = 0 は意味も持たない．また逆に不正ユーザーがあまり操作行わなかった場合，不正ユーザーと検出されない．この場合，FAR が大きくなってしまうが，そもそも操作をあまり行っていないためであり（継続認証の不正ユーザー検出にはある程度の操作数が必要），FAR の値が大きいから検出率が低いとは言えない．FRR においても正規ユーザーが長い時間操作を続けると，不正ユーザーと判定される操作が入るかもしれない．このような理由から，FRR や FAR で継続認証の評価は行えないと主張している．そこで文献 [50] では，不正ユーザーと検出されるまでのキー操作数で継続認証を評価すべきだとしている．

TM により不正ユーザーの早期検出が可能となったが以下のような課題もある．

- Trust 値の増やすか減らすかを決める閾値 T_D をどのよう決めるか
- Trust 値の増加量 R をどのように決めるか
- 平均，標準偏差の得られていないキーが押されたときの Trust 値の減少量 α をどのように決めるか
- 不正ユーザーと判定するための T_{lockout} をどのように決めるか
- 押下時間の分布をガウス分布と仮定し距離 D を決めているがそれでかまわないのか

などである．文献 [50] では，これらのパラメータの決定方法は明らかにされておらず，試行錯誤的に決定しなければならない．設定値によって不正ユーザーの検出速度が変わってくるのは明らかであり，TM の課題である．これを受けて S.Mondal と TM の提案者である P.Bours は，TM を改善した Dynamic Trust Model（DTM）を提案 [52] した．次節ではこの DTM について説明する．

2.2 Dynamic Trust Model

TM を改善し不正ユーザーの検出速度を高めたのが Dynamic Trust Model（DTM）[52] である．DTM においても，TM と同様に Trust 値を変動させ正規ユーザーか不正ユーザーかを判断する．DTM では，まず i 回目の操作が行われたとき，その操作から得られる特徴量を用いてスコア $sc_i (0 \leq sc_i \leq 1)$ を決める．sc_i の決定は機械学習等を用いて決定する．次に sc_i を用いてパラメータ 4 つ（A, B, C, D）を含む次の式から Trust 値 T の変化量 ΔT を決める．

$$\Delta T(sc_i) = \min\{-D + \frac{D \times (1 + \frac{1}{C})}{\frac{1}{C} + \exp(-\frac{sc_i - A}{B})} \ , \ C\}. \tag{2.15}$$

ただし，$\min\{X, Y\}$ は X, Y のうち小さい方の値を取ることを意味する．その後，次の式により Trust 値 T_{i+1} を決定する．

$$T_{i+1} = \min\{ \max\{ T_i + \Delta T(sc_i) \ , \ 0 \} \ , \ 100 \} \tag{2.16}$$

$\max\{X, Y\}$ は X, Y のうち大きい方の値を取ることを意味する．つまり，Trust 値 T は $0 \leq T \leq 100$ の範囲で変動する．何かしらの操作が行われるごとに Trust 値 T は変化し，TM と同様，不正ユーザーと判定するための閾値 T_{lockout} を下回ると不正ユーザーと判断される．

式（2.15）には，4 つのパラメータが存在する．A は Trust 値を増やすか減らすかを決めるための閾値，B はシグモイド曲線の幅，C は Trust 値の最大増加量，D は Trust 値の最大減少量である．各パラメータはユーザーごと，各特徴量ごとに決めることができる．図 2.3 は，$\Delta T(sc)$ のグラフである．縦軸に ΔT，横軸に sc を取っている．4 つのグラフの違いは，パラメータ A, B, C, D の値の違いである．パラメータ A は Trust 値 T を増やすか減らすかの閾値パラメータのため，$sc = A$ のところではどのグラフも $\Delta T = 0$ となっている．パラメータ B はシグモイド曲線の幅を表す．図 2.3 の左上（$B = 0.11, C = 1, D = 1$）と左下（$B = 0.04, C = 1, D = 1$）を比較すると，左上の方が -1 から 1 への変化が緩やかであり，左下の方は急激に変化している．パラメータ C は ΔT の最大値を，パラメータ D は ΔT の最小値の大きさを表し，図 2.3 の右下の図（$C = 1.5, D = 1.5$）では，最小値は -1.5，最大値は 1.5 となっている．

DTM が提案された文献 [52] においては，スコア sc を 3 種類の機械学習アルゴリズムを組み合わせて決定している．事前に正規ユーザー，不正ユーザーのキー操作・マウス

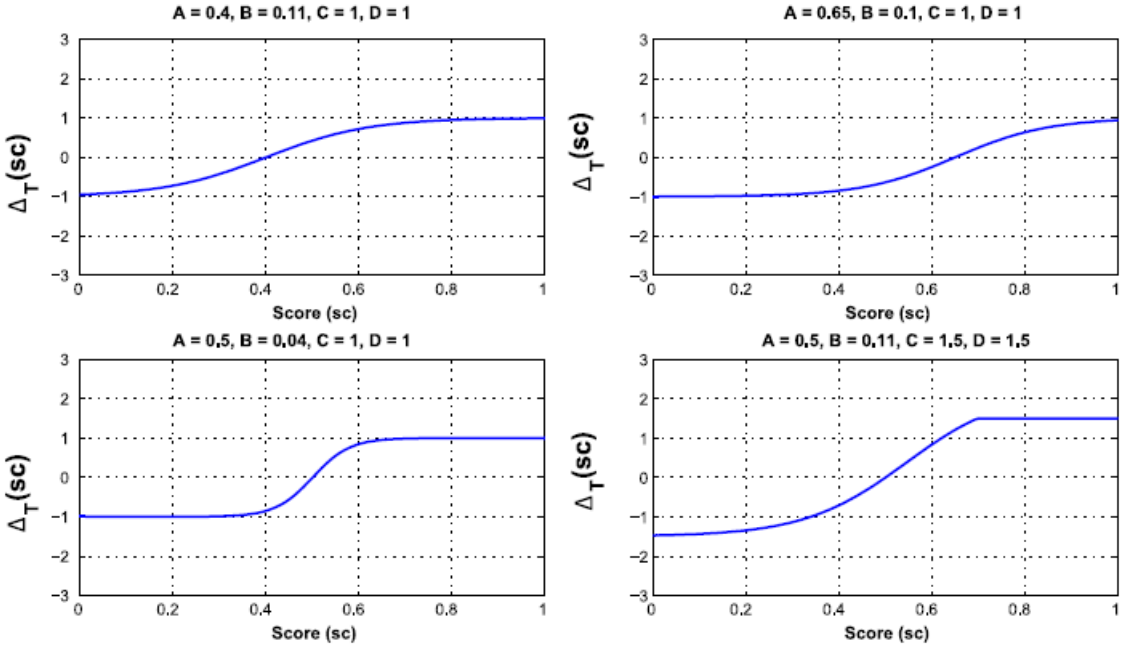


図 2.3: DTM の Trust 値 T の変化量 ΔT

操作のログデータを用いて Artificial Neural Network（ANN），Counter-Propagation Artificial Neural Network（CPANN），Support Vector Machine（SVM）でモデルを構築し，ユーザーの操作が得られたときに，各モデルからスコア sc を算出する．ANN から得られるスコアを sc_{ANN}，CPANN から得られるスコアを sc_{CPANN}，SVM から得られるスコアを sc_{SVM} とし

$$(f_1, f_2, f_3) = (sc_{\mathrm{ANN}}, sc_{\mathrm{CPANN}}, sc_{\mathrm{SVM}}) \tag{2.17}$$

とするとき，以下のようにスコア sc を決定する．

$$sc = \frac{\sum_{j=1}^{3} w_j f_j}{\sum_{j=1}^{3} w_j}. \tag{2.18}$$

ただし，w は重みであり，遺伝的アルゴリズムの最適化手法により決定する．このようにして算出された sc を (2.15) 式に代入することにより信頼値 T の変化量 ΔT を計算し，信頼値 T を変化させていく．

実験は 53 名に対して行われた．特徴量は以下のものを扱っている．

- キー操作
  - キー押下時間
    キーを押してから離すまでの時間（図 2.4）

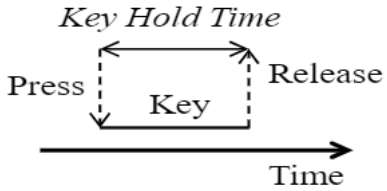


図 2.4: キー押下時間

– 2 連字キー（図 2.5）
  * 1 つ目のキーを押してから，2 つ目のキーを離すまでの時間
    Key Press-Release（KPR）
  * 1 つ目のキーを押してから，2 つ目のキーを押すまでの時間
    Key Press-Press（KPP）
  * 1 つ目のキーを離してから，2 つ目のキーを押すまでの時間
    Key Release-Press（KRP）
  * 1 つ目のキーを離してから，2 つ目のキーを離すまでの時間
    Key Release-Release（KRR）

• マウス操作
  – クリック時間
    キー押下時間と同様，マウスのボタンを押してから離すまでの時間
  – ダブルクリック
    2 連字キーと同様に
    * Mouse Press-Release（MPR）
    * Mouse Press-Press（MPP）
    * Mouse Release-Press（MRP）
    * Mouse Release-Release（MRR）
  – マウス移動
    マウス移動に伴う移動距離，平均の速さなど
  – ドラッグ&ドロップ
    ドラッグ&ドロップに伴う移動距離，平均の速さなど

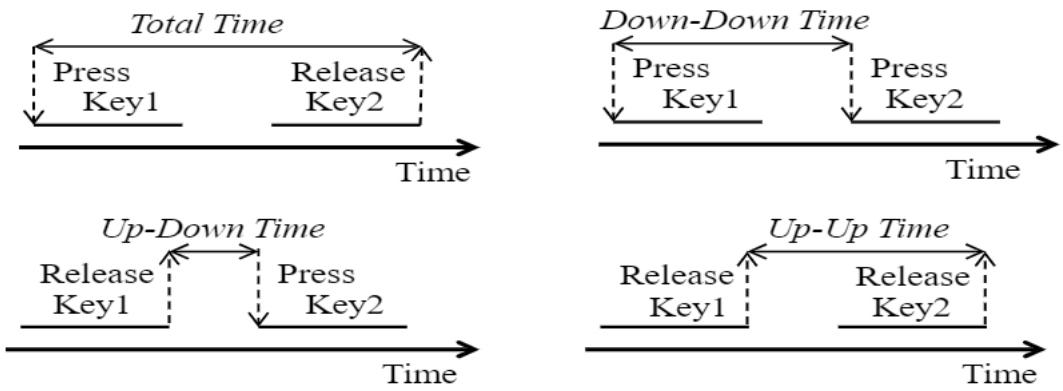


図 2.5: 2 連字キー

以上の特徴量を用いて DTM の評価実験を行っている．

また，文献 [52] では継続認証の評価方法についても提案している．継続認証において本人拒否率（FRR），他人受入率（FAR）よりも，不正ユーザーがどれくらいのアクション数（操作数）で検出されたか，正規ユーザーが誤ってロックアウトされたとき，アクション数がどれだけあったかの方が重要だという主張である．継続認証においては不正ユーザーを検出するためにある程度の操作数が必要となる．そのため，たとえ FRR および FAR，また 2 つの値が等しくなる等価エラー率（Equal Error Rate（EER））が 0% だったとしても，検出されない間に操作が可能となる．不正ユーザのアクション数がどれほどなのかは継続認証において重要な指標となる．そこで，不正ユーザー平均持続アクション数（Average Number of Imposter Actions（ANIA））および正規ユーザー平均持続アクション数（Average Number of Genuine Actions（ANGA））から継続認証を評価する方法を提案している．当然のことながら，ANIA は可能な限り低く，ANGA は可能な限り高い方が評価は高い．

ANIA は次のように定義する．正規ユーザー g の操作データを学習したモデルを用いて不正ユーザー i のログデータを DTM で計算する場合を考える．このとき，k 回ロックアウトされ，それぞれのアクション数が $N_1, N_2, \cdots, N_k$ だったとき

$$ANIA_g^i = \frac{1}{k}\sum_{j=1}^{k} N_j \tag{2.19}$$

で定義し，これより正規ユーザー g に対する不正ユーザーの平均持続アクション数

$$ANIA_g = \frac{1}{M-1}\sum_{i=1\ldots M,\ i\neq g} ANIA_g^i \tag{2.20}$$

となる．ここで M は全ユーザー数であり，正規ユーザーを除く $M-1$ 人の不正ユーザーに対して計算を行う．これを全ユーザーに対して計算し以下で DTM の不正ユーザー平均持続アクション数を決定する．

$$ANIA = \frac{1}{M}\sum_{g=1}^{M} ANIA_g. \tag{2.21}$$

同様に，自分自身の操作データを学習したモデルを用いて自分の操作ログデータを DTM で計算したとき k 回ロックアウトされ，それぞれのアクション数が $N_1, N_2, \cdots, N_k$ だったとき

$$ANGA_g = \frac{1}{k}\sum_{j=1}^{k} N_j \tag{2.22}$$

から，DTM の正規ユーザー平均持続アクション数

$$ANGA = \frac{1}{M}\sum_{g=1}^{M} ANGA_g \tag{2.23}$$

となる．この ANIA および ANGA で評価を行うが，さらに詳細に評価を行うために，次の 4 つのカテゴリに分け ANIA，ANGA を計算する．

+/+： 正規ユーザーの拒否なし，不正ユーザーの受け入れなし

+/−： 正規ユーザーの拒否なし，不正ユーザーの受け入れあり

−/+： 正規ユーザーの拒否あり，不正ユーザーの受け入れなし

−/−： 正規ユーザーの拒否あり，不正ユーザーの受け入れあり

このカテゴリを用いて作成した DTM の継続認証性能表が表 2.1 である（なお，表 2.1 は，文献 [52] からの引用であるが，本論文で行っている継続認証とは条件が異なる）．表の 1 列目はカテゴリ，2 列目がユーザー数，3 列目は正規ユーザー平均持続アクション数，4 列目は不正ユーザー平均持続アクション数，5 列目は検出できなかった不正ユーザー数である．表を見ると，正規ユーザーの拒否がなく，不正ユーザーの受け入れもなかった「+/+」が 29 人いて，不正ユーザーの平均持続アクション数が 282 とわかる．この実験は全部で 53 人で行われており，1 人を正規ユーザーとしたとき，残りの 52 人は不正ユーザーとなる．その状況で DTM の計算を行い，正規ユーザーは拒否せず，不正ユーザーは 52 人とも検出されたという結果が得られた正規ユーザーが 29 人いたということを意味する．なお，正規ユーザーの拒否はなかったので ANGA は空欄，また不正ユーザーの受け入れもなかったので，#Imp. ND（検出できなかったユーザー）も空欄となる．「+/−」では，不正ユーザーとして検出できなかったユーザーが 7 人おり，その平均持続アクション数が 3518 となったことがわかる．「+/+」と同様，「+/−」にお

いても正規ユーザーの拒否はないので ANGA は空欄となる.「−/+」では，19 人の正規ユーザーが不正ユーザーとして検出されており，その平均持続アクション数が 6593 だったことがわかる．また，このとき不正ユーザーは全て検出しており，その平均持続アクション数が 349 であることがわかる．なお，不正ユーザーの受け入れはないので，#Imp. ND（検出できなかったユーザー）は空欄である．最後に −/− だが，正規ユーザーにもかかわらず不正ユーザーと判定された人が 2 人おり，その平均持続アクション数は 25203，不正ユーザーにもかかわらず検出されなかったユーザーも 2 人おり，その平均持続アクション数が 1083 であることがわかる．

表 2.1: 継続認証性能表

Category	#User	ANGA	ANIA	#Imp. ND
+/+	29		282	
+/−	3		3518	7
−/+	19	6593	349	
−/−	2	25203	1083	2

TM を改善し，不正ユーザの検出速度を高めた DTM ではあるが，以下のような課題がある．

- スコア sc を決定するための最適な機械学習アルゴリズムが明らかでない
- パラメータ A, B, C, D の調整方法が明らかでない
- パラメータ A, B, C, D は各ユーザー，各特徴量ごとに調整する必要があり，扱いが困難
- 経時変化に対する対応が困難（スコア sc を決定するためのモデルの再学習をいつどのように行うか）

などがある．1 つ目については，現在も様々な機械学習アルゴリズムや，またいくつかの機械学習アルゴリズムを組み合わせたものが試されているが，キー操作・マウス操作の継続認証に最適な機械学習アルゴリズムは，まだ明らかになっていない．当然のことながらスコア sc は，継続認証の性能に大きく寄与するため重要な課題である．2 つ目，3 つ目はパラメータ調整の困難性である．調整方法が明らかにされおらず，また各ユーザー，各特徴量ごとに 4 つのパラメータを決定するとなると相当な労力となる．最適なパラメータを設定すれば，良い結果が得られるかもしれないが最適なパラメータ設定自体が非常に困難である．4 つ目は経時変化に対する対応の困難性である．行動的特徴を用いた継続認証においては，特徴の経時変化にどのように対応するかが課題の 1 つとしてある．1 日の間でも，疲れ具合，集中の度合いなどの違いからキー操作・マウス操作から得られる特徴量の変動幅が大きくなるという指摘もある．さらに，1 年

後，2 年後，5 年後，10 年後と時が経つにつれてその特徴が変わるのは自然なことである．それに対応するようにモデルを再構築する場合，いつ，どのように行うかは大きな課題となる．

本論文では，キー操作・マウス操作から得られる特徴量の確率分布群を用いた扱いやすい継続認証アルゴリズム Dynamic Probability Trust Mocel（DPTM）を提案し，評価実験により DTM より良い結果が得られたことを報告する．

第3章　DPTMアルゴリズム

本章では，本論文で新規に提案するDPTMアルゴリズム，DPTMの動的パラメータの初期値α_{i0}の決定方法について説明する．

3.1　DPTMアルゴリズム

Dynamic Probability Trust Model（DPTM）は，キー操作・マウス操作等の行動的特徴を用いた継続認証のためのアルゴリズムである．DPTMは，Trust Model（TM）やDynamic Trust Model（DTM）と同様，Trust値と呼ばれる値Tが，ユーザーが操作を行うたびに変化し，閾値を下回ると不正ユーザーと判定するというアルゴリズムである．Trust値Tの変化量ΔTは，事前に取得した正規ユーザーの操作から得られる特徴量の確率分布群（正規ユーザープロファイルと呼ぶ）とユーザーの操作から得られる特徴量により算出される．なお，実際に計算を行う際は，無限に操作データを取得することは不可能なので頻度分布群で代用する．以下で，DPTMの具体的な処理について説明する．

t回目のアクション[1]が発生したとき，取得した特徴iの値がv_{it}であり，その確率分布が$P_i(v_i)$のとき

$$\Delta T_{it} = \begin{cases} P_i(v_{it}) & (\, P_i(v_{it}) \geq \alpha_i \,) \\ \tanh\left(\dfrac{P_i(v_{it}) - \alpha_i}{K\alpha_i} \right) & (\, P_i(v_{it}) < \alpha_i \,) \end{cases} \tag{3.1}$$

でΔTを定義する．ただし，KはΔTが$-1, 1$に収束する速さを決める静的パラメータであり，α_iは動的パラメータである（α_iの詳細については後述する）．

図3.1は，$K = 0.2, \alpha_i = 0.15$のときの$y = \tanh(\frac{x-\alpha_i}{K\alpha_i})$のグラフである．また，図3.2は，$K = 0.35, \alpha_i = 0.15$のグラフである．図3.2を見ると，図3.1に比べてyの値がが$-1, 1$に緩やかに収束するのがわかる．つまり，Kの値により，yの値を$-1, 1$に収束させる速さを決めることができる．また，図3.1，図3.2ともに$x = 0.15$のとき$y = 0$となっている．これは$\alpha_i = 0.15$にしているためであり，$x = \alpha_i$のとき$y = 0$となる．このことから，式（3.1）において$P_i(v_{it}) = \alpha_i$のとき$\Delta T_{it} = 0$となる．また，式（3.1）を見ると，$P_i(v_{it})$がα_i以上か，それより小さいかでΔTの取る値が決まる．操作によ

[1]キー操作やマウス操作などが行われたときに，その操作から得られた情報から着目している特徴量を得ることができる．ここでは，特徴量が得られるこれらの操作のことをアクションと呼ぶ．

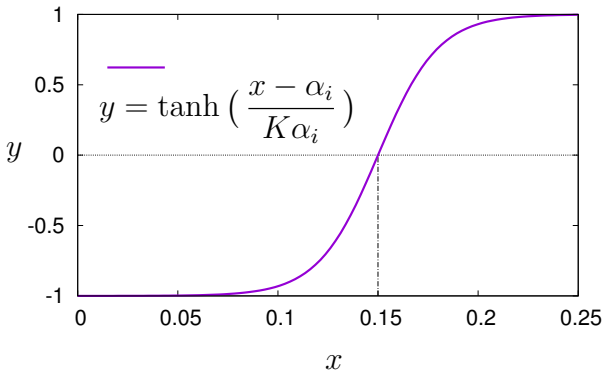


図 3.1: $K = 0.2, \alpha_i = 0.15$

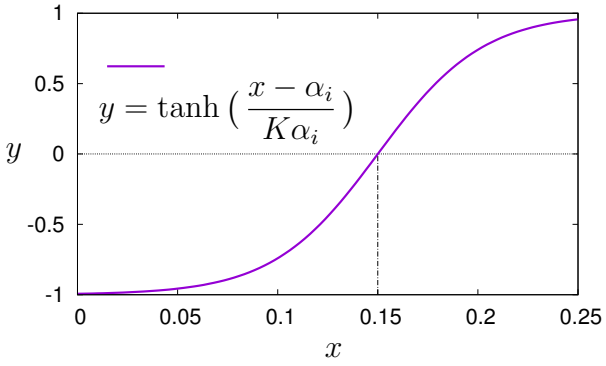


図 3.2: $K = 0.35, \alpha_i = 0.15$

り得られた値の確率 $P_i(v_{it})$ が α_i より大きいときは，確率 P_i の値がそのまま ΔT の値となり（常に正の値），小さいときは，ハイパボリックタンジェントの式で値が決まる．図 3.1，図 3.2 からわかるように，$P_i(v_{it})$ が α_i より小さいときはハイパボリックタンジェントの式は常に負の値を取る．これは α_i が境界値となり ΔT_{it} が $P_i(v_{it})$ という正の値を取るのか，$\tanh(\frac{x-\alpha_i}{K\alpha_i})$ という負の値を取るのかが決まるということを意味する．つまり，α_i は Trust 値 T を上げるのか下げるのかを決める重要なパラメータとなる．

式 (3.1) から決まる ΔT_{it} を用いて Trust 値

$$T_{t+1} = \min\{\ T_t + \sum_i \Delta T_{it}\ ,\ 100\ \} \tag{3.2}$$

を更新する．ただし，$\min\{\ X\ ,\ Y\ \}$ は X, Y のうち小さい方の値を取ることを意味する．つまり Trust 値 T の最大値は 100 となる．最大値を決めるのは不正ユーザーを速く検出するためである．Trust 値 T の上限を定めなければ，正規ユーザーが操作を続けたとき Trust 値 T は上がり続け非常に大きな値となる．その状態で不正ユーザーが操作をすると，Trust 値 T が閾値を下回るのに長い時間がかかってしまう．Trust 値 T の上限を定めることで，不正ユーザーが操作したとき，すぐに Trust 値 T が閾値を下回り不正ユーザーと判定できる．なお，最大値を 100 としたのは既存研究である TM や DTM と同一条件とするためである．

さらに他人を速く検出するために，パラメータ α_i を動的に変化させる．動的パラメータ α_i の初期値を α_{i0} とし，ΔT_{it} が n 回連続で負の値を取るとき

$$\alpha_i = \alpha_{i0} + f(n) \tag{3.3}$$

と変化させる．ただし，$f(n)$ は単調増加関数とする．この動的パラメータ α_i により，$\Delta T < 0$ を取り続けると動的パラメータ α_i の値が大きくなり，$P_i(v_i) \geq \alpha_i$ となるような特徴量 v_i を取りにくくなる．つまり，不正ユーザーの操作は $\Delta T < 0$ を連続で取りやすいため，動的パラメータ α_i の値が大きくなり，ますます $\Delta T > 0$ を取りづらくな

る．その結果，Trust 値が下がりやすい状態となり，より速く不正ユーザーを検出することが可能となる．

図 3.3 に DPTM の処理の流れを示す．まず，キー操作・マウス操作から特徴量 v_{it} を取得し，正規ユーザープロファイルを用いて ΔT_{it} を計算する．ΔT_{it} より Trust 値 T_{t+1} を計算し，動的パラメータ α_i の更新を行う．ここで，Trust 値が閾値を下回っていれば画面をロックし，そうでなければ次の特徴量を取得する．この一連の処理を繰り返す．

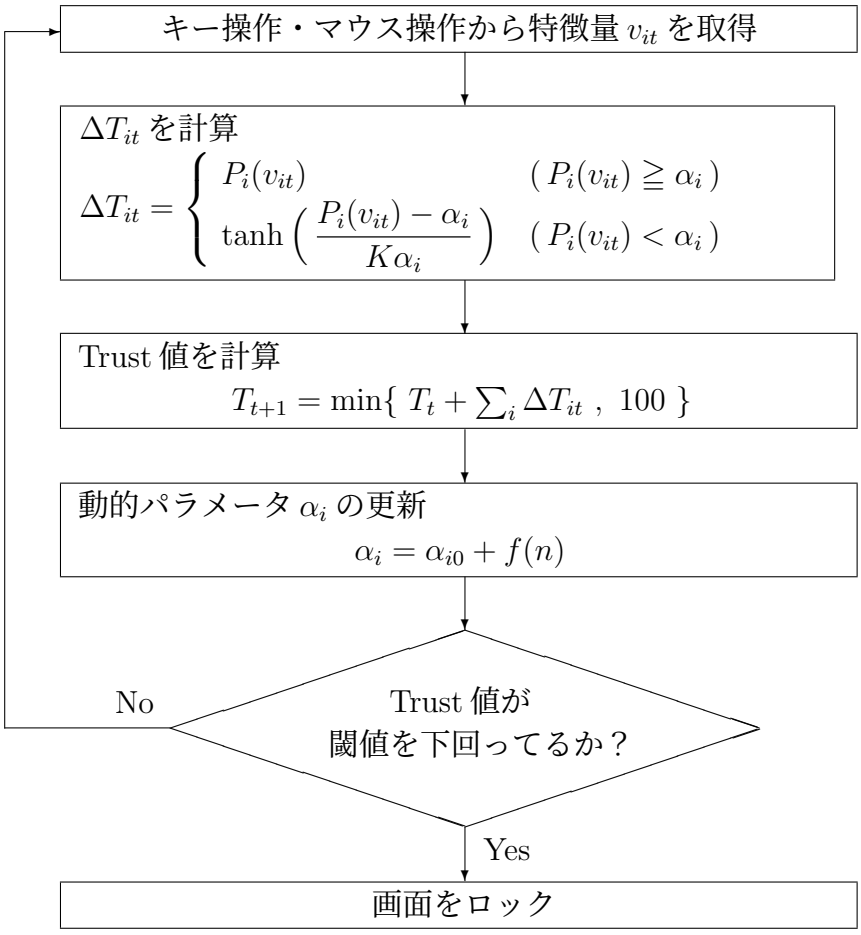


図 3.3: DPTM の処理の流れ

3.2 動的パラメータの初期値 α_{i0} の決定方法

動的パラメータの初期値 α_{i0} は，正規ユーザープロファイルおよび正規ユーザーのログデータより決定する．つまり，本人のログデータのみで決定する．これは，他人のログデータを大量に取得することは困難であることに比べ，本人のログデータはコンピュータを扱っただけ取得が可能であり，使えば使うだけデータが蓄積されるため，本人らしさが α_{i0} に反映されると考えるからである．

では，具体的に α_{i0} の決定方法について記述する．まず，すべての特徴量 i の動的パラメータの初期値 α_{i0} を 0 とおく．その状態で正規ユーザーのログデータを用いて DPTM の計算を行う．このとき，動的パラメータ α_i は動的に変化させない．正規ユーザープロファイルを用いた DPTM に，正規ユーザーのログデータを入れているので Trust 値 T は 100 近傍で変化する．図 3.4 は 100 近傍で変化する Trust 値 T の例であり，縦軸に Trust 値 T，横軸にアクション数を取ったグラフである．このときの Trust 値の最小値を $T_{\mathrm{min},0}$ とする．図 3.4 では，アクション数 285 で Trust 値 T が 95.53 と最小になるため $T_{\mathrm{min},0} = 95.53$ となる．

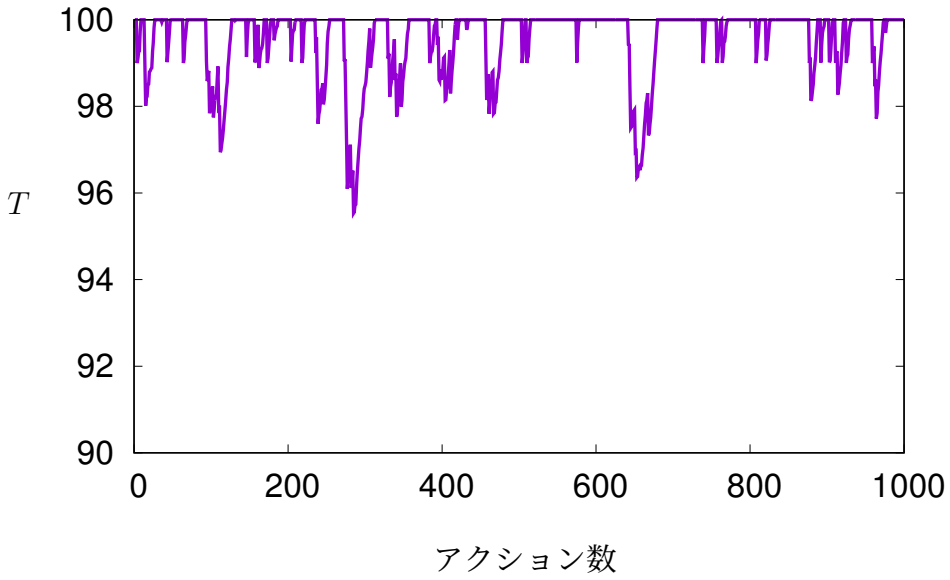


図 3.4: $\alpha_{i0} = 0$ での Trust 値の変化

次に，ある特徴量 i の初期値 α_{i0} のみを正の方向へ $\Delta\alpha'_{i0}$ だけ微小変化させる．その際，i 以外の特徴量 j $(j \neq i)$ の α_{j0} については 0 のままにしておく．この状態で正規ユーザーのログデータを用いて DPTM の計算を再度行い，α_{i0} を微小変化させた後の

Trust 値の最小値 $T_{\min,i}$ を求める．ここで，α_{i0} を微小変化させたときの $T_{\min}$ の変化量を

$$\frac{\partial T_{\min}}{\partial \alpha_{i0}} = \frac{T_{\min,i} - T_{\min,0}}{\Delta \alpha'_{i0}} \tag{3.4}$$

と表記する．すべての特徴量について $T_{\min}$ の変化量 $\frac{\partial T_{\min}}{\partial \alpha_{i0}}$ を計算し，その変化量の指数をとった値の割合を 1 から引いた値

$$R_i = 1 - \frac{\exp\Big(-\dfrac{\partial T_{\min}}{\partial \alpha_{i0}}\Big)}{\displaystyle\sum_i \exp\Big(-\frac{\partial T_{\min}}{\partial \alpha_{i0}}\Big)} \tag{3.5}$$

を導入する．なお，(3.5) 式で $\frac{\partial T_{\min}}{\partial \alpha_{i0}}$ にマイナスがついているのは，$\frac{\partial T_{\min}}{\partial \alpha_{i0}} < 0$ となるためである．α_{i0} を少し大きくすることは条件が厳しくなることであり，$T_{\min,i}$ は $T_{\min,0}$ より必ず小さくなる．$-\frac{\partial T_{\min}}{\partial \alpha_{i0}}$ は，α_{i0} を微小変化させたときの Trust 値の変化量を表す．指数を取っているのは，それぞれの差を際立たせるためである．また，R_i の右辺第 2 項は，必ず 0 と 1 の間の値となるため，1 から引くことにより，大きい値は小さく，小さい値は大きくなる．つまり，特徴 i の条件を厳しくしたときに，Trust 値 T が大きく下がるものについては R_i は小さく，少ししか下がらないものについては大きな値を取るように定義している．最後に，この R_i を用いて α_{i0} の変化量

$$\Delta \alpha_{i0} = \frac{R_i}{\displaystyle\sum_i R_i} \Delta p \tag{3.6}$$

を決める．ただし，Δp は α_{i0} に加える値 $\Delta \alpha_{i0}$ の総量 $\Delta p = \sum_i \Delta \alpha_{i0}$ である．(3.5) 式の R_i を用いて，その割合で Δp を分配し，α_{i0} に加え，α_{i0} を更新する．つまり，α_{i0} を微小変化させたとき $T_{\min,0}$ が大きく変化するものに対しては $\Delta \alpha_{i0}$ を小さく，ほとんど変化しないものに対しては $\Delta \alpha_{i0}$ を大きくする．この操作を繰り返すことで動的パラメータの初期値 α_{i0} を決定する．これにより，正規ユーザーの Trust 値 T の最小値の減少を最小にしながら条件を厳しく（α_{i0} を大きく）することが可能となる．このようにして決定した各特徴量の α_{i0} の集合は，ユーザーにより様々な値を取るため，ユーザーの特徴を表す集合となる可能性がある．

第4章　DPTMの評価実験

DPTM の有用性を検証するために，キー操作・マウス操作のログデータを収集し認証精度実験を行った.

4.1　ログデータ収集

第一工業大学の学生 51 名に協力してもらい，コンピュータ関係の講義 3 回分（270 分）のキー操作・マウス操作のログデータを収集した（協力してくれる学生全員に対して付録 A の個人識別可能取扱い同意書にサインしてもらった）．操作内容は指定せず，サンプリング間隔は 16ms である．表 4.1 はユーザー 01 から収集したログデータの一部である.（連続した生データの一部（Seq.0〜Seq.300）を付録 B.1 に掲載する．また比較のためユーザー 02 のデータも付録 B.2 に掲載する.）各列のデータは以下のとおりである．Seq はシーケンスナンバーを表す．Evt には M（MOUSE），K（KEY），process があり，M がマウス操作，K がキー操作を表す．process については，本研究では使用しない．Act は，キー操作，マウス操作の動作内容を表す．キー操作の場合，P（PRESSED）が押す，R（RELEASED）が離すを表し（キー操作については P と R のみ），マウス操作の場合，これに加えて CLICKED（今回は CLICKED は利用せずマウスボタンの PRESSED および RELEASED でクリックを判断する），M（Moved）が移動，D（Dragged）がドラッグを表す．また今回使用しない process に対しては，RUN がソフトの実行，EXIT がソフトの終了を表す．Time は UNIX 時間であり単位は ms である．また Value については，マウス操作の場合は Value1，Value2 が x 座標，y 座標を表し，Value3 がマウスのどのボタンが押されたかを表す．0 の場合，ボタンは押されておらず，1 の場合は左ボタン，2 の場合は右ボタンが押されたことを表す．キー操作の場合は，Value1 がどのキーかを Value2 がキーコードを表し Value3 は空欄となる．

表 4.1 の Seq 352 は，Evt=M，Act=P，Value3=1 なのでマウスの左ボタンを押したときのログであり，同様に，Seq 353 は離したときのログである．つまり，Seq 352 と Seq 353 でマウスの左クリックが行われたことがわかる．また，Seq 452 でマウスの左ボタンが押され，Seq 453〜483 の間は押されたまま移動し（ドラッグ中は Act=D，Value3=0 となる），Seq 484 でマウスの左ボタンが離される．これはドラッグ&ドロップが行われたことを表す．Seq 487〜492 はマウスを動かしている状態を表す．Seq 1074,1075 でキーコード 73 の「I」がタイプされたことがわかる．

得られた各ユーザーのログデータは，それぞれ 3 等分し，1 つはユーザープロファイ

ル作成用データ，1 つは 3.2 で説明した動的パラメータ α_i の初期値 α_{i0} の決定用データ，1 つは評価実験用データとする．

表 4.1: 収集したデータ例

Seq	Evt	Act	Time	Value1	Value2	Value3
1	M	M	1515631142165	326	938	0
...	...	...	...	...	...	...
351	M	M	1516601650732	1677	1059	0
352	M	P	1516601650831	1677	1059	1
353	M	R	1516601650884	1677	1059	1
...	...	...	...	...	...	...
450	M	M	1516601655748	972	763	0
451	M	M	1516601655756	972	763	0
452	M	P	1516601655996	972	763	1
453	M	D	1516601656108	972	764	0
454	M	D	1516601656116	972	767	0
455	M	D	1516601656124	972	770	0
...	...	...	...	...	...	...
481	M	D	1516601656508	965	804	0
482	M	D	1516601656516	965	805	0
483	M	D	1516601656548	965	806	0
484	M	R	1516601656804	965	806	1
...	...	...	...	...	...	...
487	M	M	1516601663549	967	806	0
488	M	M	1516601663556	975	806	0
489	M	M	1516601663564	984	804	0
490	M	M	1516601663572	997	801	0
491	M	M	1516601663580	1008	799	0
492	M	M	1516601663588	1020	796	0
...	...	...	...	...	...	...
1074	K	P	1515631519994	I	73	
1075	K	R	1515631520088	I	73	
...	...	...	...	...	...	...

4.2 扱う特徴量

本研究で扱う特徴量は，キー操作・マウス操作において一般的によく扱われている以下の量とする．

- キー操作による特徴量（図 4.1）

  - Key Hold Time (KHT)
    図 4.1 の Key1 において，Press されてから Release されるまでの時間．

  - 2 連続キーの特徴量
    図 4.1 において，Key1 がタイプされた後，Key2 がタイプされたときに取得する特徴量．

    * Key Press-Release (KPR)
      Key1 が Press され，Key2 が Release されるまでの時間．

    * Key Press-Press (KPP)
      Key1 が Press され，Key2 が Press されるまでの時間．

    * Key Release-Press (KRP)
      Key1 が Release され，Key2 が Press されるまでの時間．

    * Key Release-Release (KRR)
      Key1 が Release され，Key2 が Release されるまでの時間．

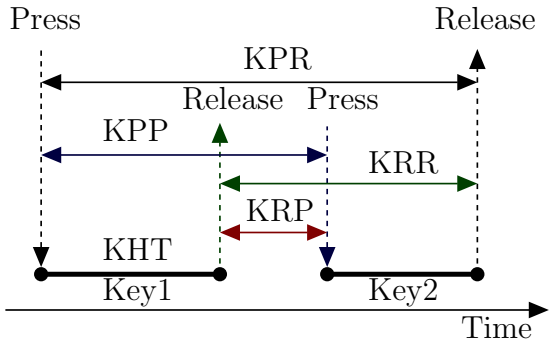


図 4.1: キー操作の特徴量

- マウス操作による特徴量

  マウスによるクリック，ダブルクリックにおいては，キー操作と同様の特徴量を取る．

  - Mouse Hold Time (MHT)
  - Mouse Press-Release (MPR)
  - Mouse Press-Press (MPP)
  - Mouse Release-Press (MRP)
  - Mouse Release-Release (MRR)

  さらに，マウスカーソル移動時に次のような特徴量を取る．

  - Mouse Drag-Drop Time (MDD)
    マウスがドラッグ&ドロップする間の時間.

  - Mouse Actual Distance (MAD)
    マウス移動の際の始点から終点までの直線距離
    $\mathrm{MAD} = \sqrt{(x_0 - x_n)^2 + (y_0 - y_n)^2}$

  - Mouse Actual Speed(MAS)
    MAD 移動の際の平均の速さ
    $\mathrm{MAS} = \dfrac{\mathrm{MAD}}{\Delta t}$

  - Mouse Curve Length(MCL)
    マウス移動の際の視点から終点までの曲線の長さ
    $\mathrm{MCL} = \sum_{i=0}^{n-1} \sqrt{(x_i - x_{i+1})^2 + (y_i - y_{i+1})^2}$

  - Mouse Curve Speed(MCS)
    MCL 移動の際の平均の速さ
    $\mathrm{MCS} = \dfrac{\mathrm{MCL}}{\Delta t}$

  ただし，(x_0, y_0) はマウスカーソル移動の始点，(x_i, y_i) は移動中の座標，(x_n, y_n) は終点，Δt はマウスカーソルの移動にかかった時間を表す．

本節の最後に特徴量の個数についてまとめておく．キー操作については，キー押下時間 KHT として各アルファベット，数字，記号，Enter キー，スペースキーなど 68 個の特徴量となる．2 連字キーの特徴量である KPR，KPP，KRP，KRR はデータ量の関係から文字の区別は行わない．すなわち，「y」,「a」と入力したときと「s」,「i」と入力したときで区別は行わず，その入力タイミングだけを特徴量として使用するので 2 連字キーの特徴量は 4 個となる．マウス操作についてはクリック時間 MHT が 1 個，ダブルクリック時間の MPR，MPP，MRP，MRR が 4 個，またドラッグ& ドロップ MDD が 1 個，マウス移動による特徴量 MAD，MAS，MCL，MCS の 4 個となるので，合計 82 個となる．つまり，特徴量の次元数は 82 次元となる．

4.3 正規ユーザープロファイルの作成

正規ユーザープロファイルは，キー操作・マウス操作から得られる特徴量の確率分布群が理想である．しかしながら，無限大のログデータを取得するのは不可能であり，現実的には頻度分布により正規ユーザープロファイルを作成する．

4.3.1 キー操作による正規ユーザープロファイル

ユーザーから収集したログデータの 3 分の 1 を用いてユーザープロファイルを作成する．図 4.2 はユーザー 01 から得られるバックスペースキーの KHT の頻度分布である．縦軸に確率 P，横軸は時間 t〔ms〕である．

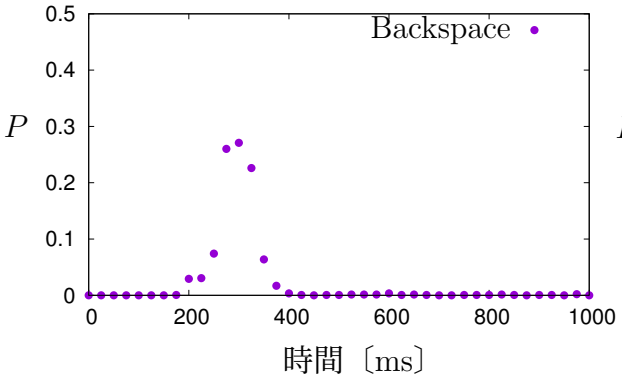


図 4.2: Backspace の KHT

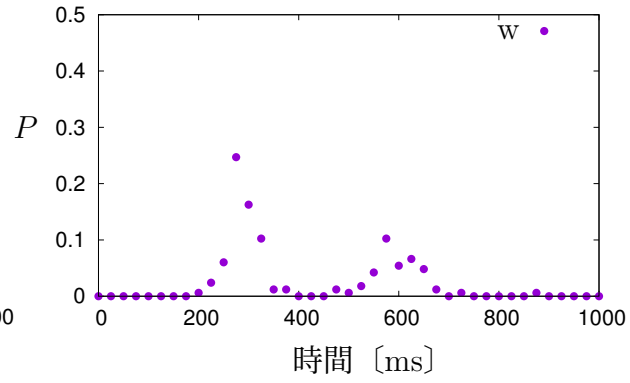


図 4.3: w キーの KHT

この図を見ると，ピークが 300 ms 辺りにあるガウス分布のように見える．しかしながら，全ての分布がガウス分布に近いというわけではない．図 4.3 は w キーの押下時間の頻度分布だが，300 ms 辺りのピークに変わりはないが，もう 1 つ 600 ms 辺りにもピークがある．それぞれの特徴量により分布は様々であり，一概にガウス分布となる

とは言えない．このような頻度分布を，全てのキーごとに作成する．ユーザー 01 の各キーの KHT は付録 C.1 に掲載する．また，比較のためにユーザー 02 の各キーの KHT も付録 C.2 に掲載する．なお，キーによっては入力されずに頻度分布の作成ができなかったものもある．頻度分布の無いキーについては頻度分布 $P_i = 0$ となるので，Trust 値 T の変化量 ΔT は常に負の値となる．

次に 2 連字キーの頻度分布を見る。2 連字キーについては，2 つのキーの組み合わせ数が多く，それぞれの組合せのデータが十分得られなかったため，キーの区別はせずに頻度分布を作成した．図 4.4，図 4.5，図 4.6，図 4.7 がそれぞれユーザー 01 の特徴量 KPR（Key Press-Release），KPP（Key Press-Press），KRP（Key Release-Press），KRR（Key Release-Release）の頻度分布である．当然のことながら KPR の時間が一番長く，KRP の時間が一番短い．また，その間に KPP，KRR の時間があることが図からわかる．

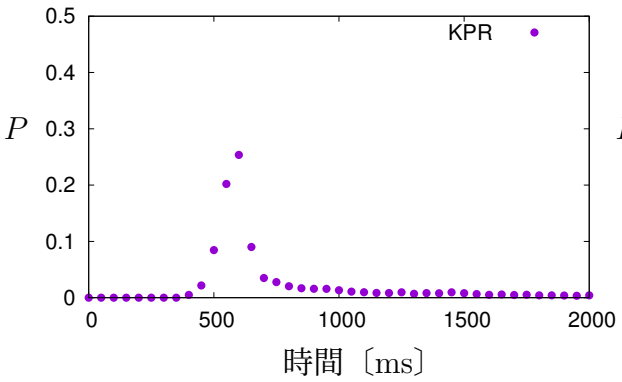


図 4.4: ユーザー 01 の KPR

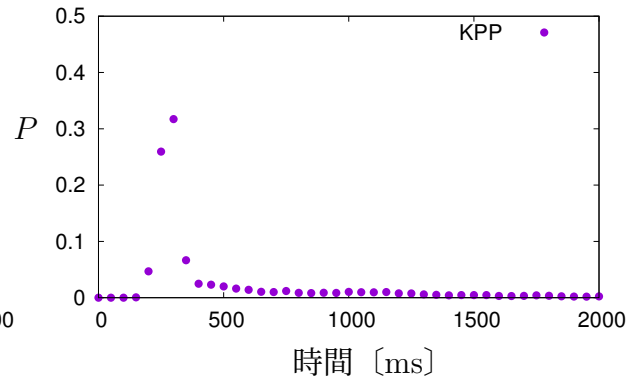


図 4.5: ユーザー 01 の KPP

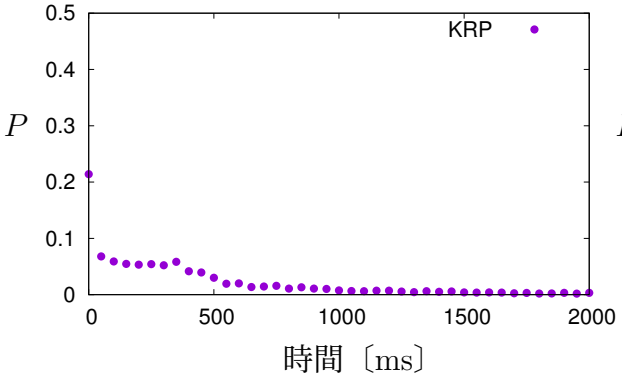


図 4.6: ユーザー 01 の KRP

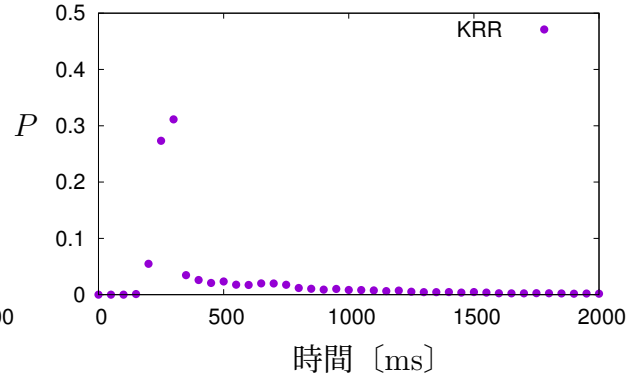


図 4.7: ユーザー 01 の KRR

また，比較のためにユーザー 02 の KPR（図 4.8），KPP（図 4.9），KRP（図 4.10），KRR（図 4.11）を掲載する．ユーザーの違いによる分布の違いが図からわかる．

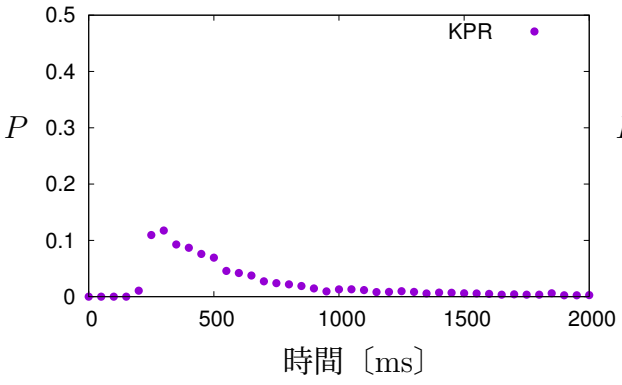


図 4.8: ユーザー 02 の KPR

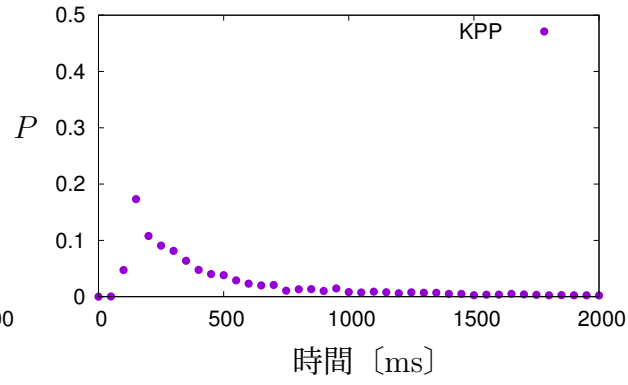


図 4.9: ユーザー 02 の KPP

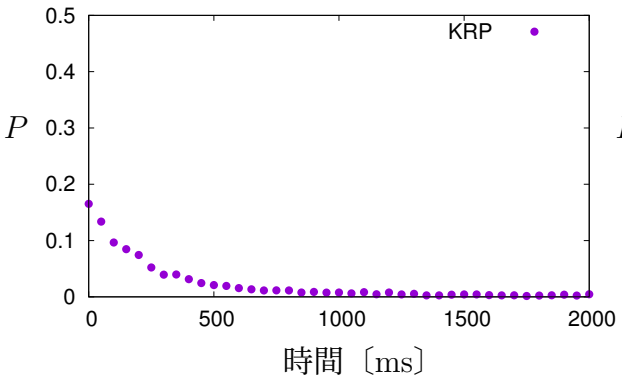


図 4.10: ユーザー 02 の KRP

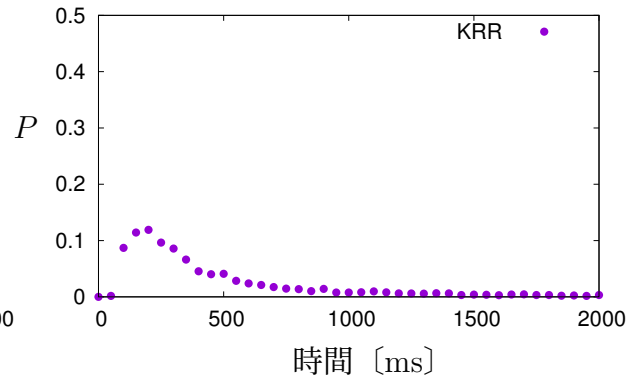


図 4.11: ユーザー 02 の KRR

4.3.2　マウス操作による正規ユーザープロファイル

次に，マウス操作から得られる特徴量の頻度分布を見る．

図 4.12 がユーザー 01 の，図 4.13 がユーザー 02 のクリック時間（Mouse Hold Time）の頻度分布である．ユーザー 01 の方が分布の幅が小さいことが図からわかる．

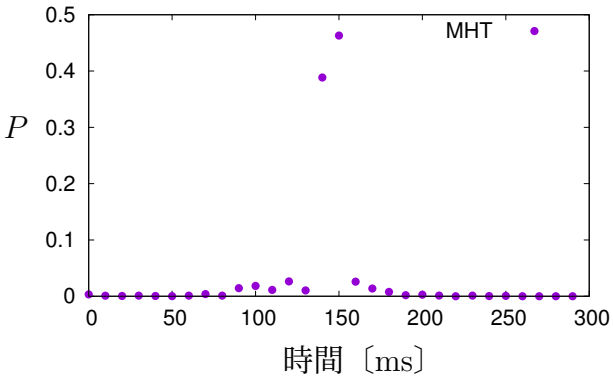


図 4.12: ユーザー 01 の MHT

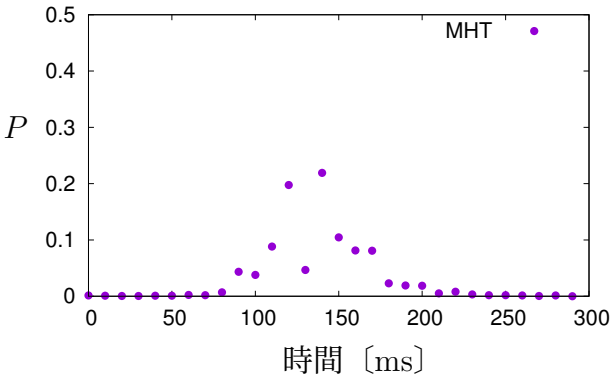


図 4.13: ユーザー 02 の MHT

また，図 4.14 がユーザー 01 の，図 4.15 がユーザー 02 のドラック&ドロップ（MDD）の時間の頻度分布である．

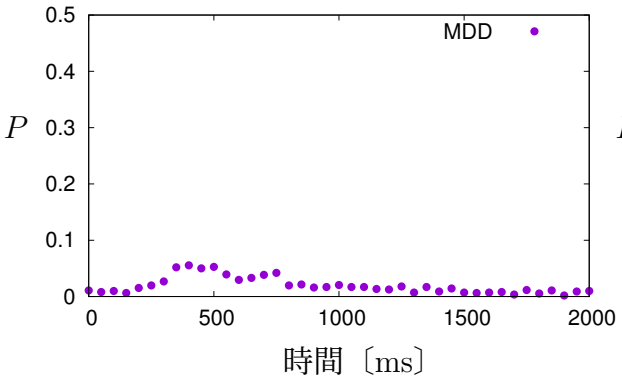


図 4.14: ユーザー 01 の MDD

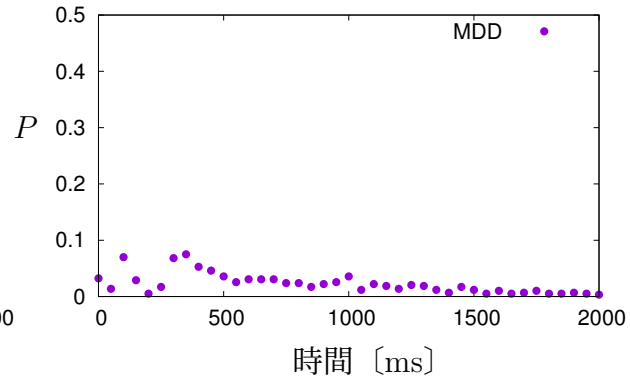


図 4.15: ユーザー 02 の MDD

図4.16，図4.17，図4.18，図4.19がそれぞれユーザー01の特徴量MPR（Mouse Press-Release），MPP（Mouse Press-Press），MRP（Mouse Release-Press），MRR（Mouse Release-Release）の頻度分布である．

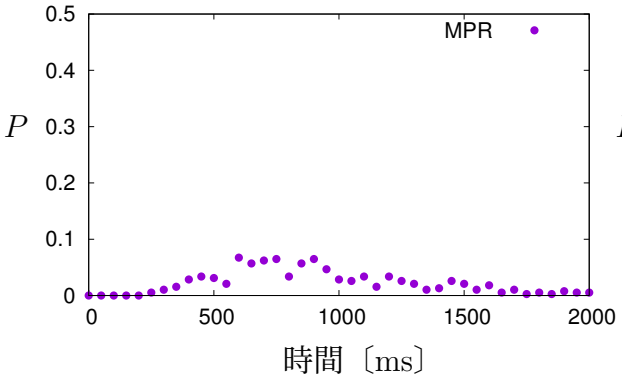


図 4.16: ユーザー 01 の MPR

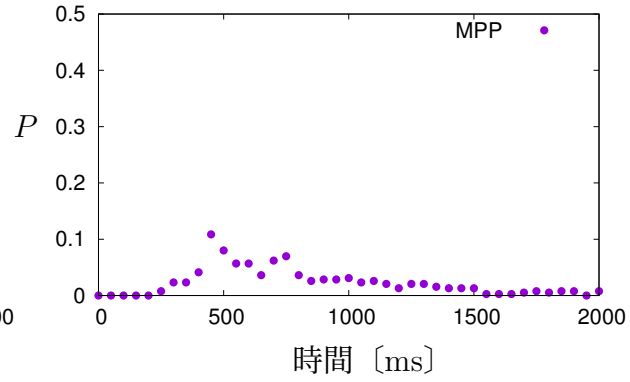


図 4.17: ユーザー 01 の MPP

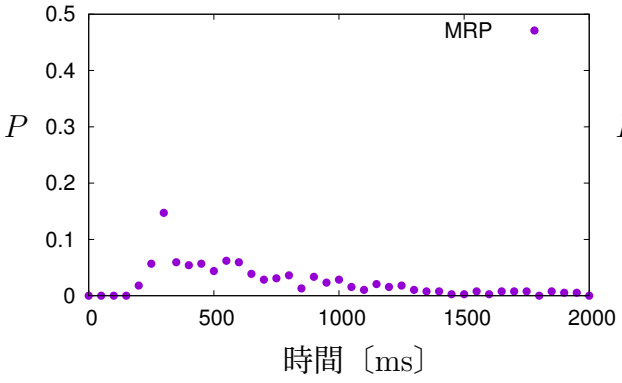


図 4.18: ユーザー 01 の MRP

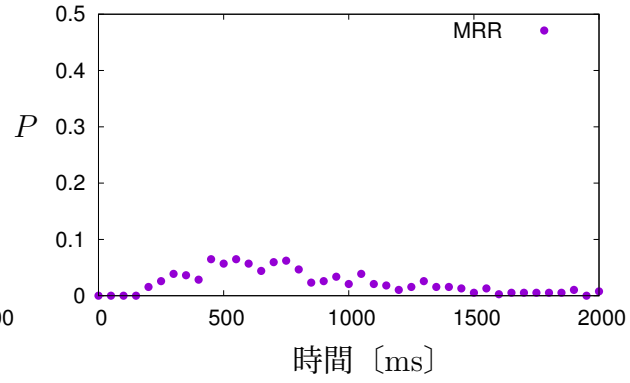


図 4.19: ユーザー 01 の MRR

また，比較のためにユーザー 02 の MPR（図 4.20），MPP（図 4.21），MRP（図 4.22），MRR（図 4.23）を掲載する．

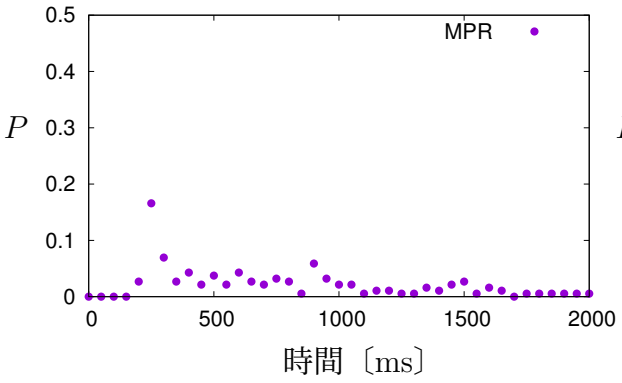


図 4.20: ユーザー 02 の MPR

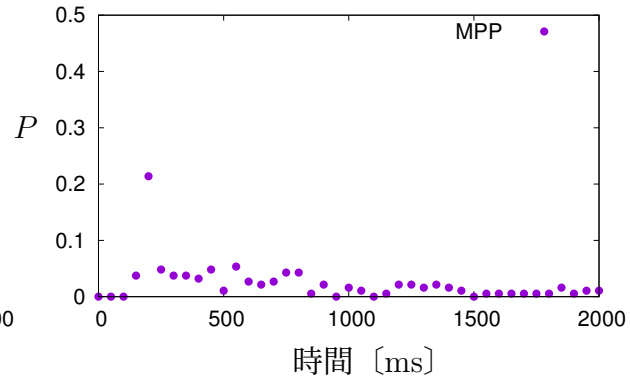


図 4.21: ユーザー 02 の MPP

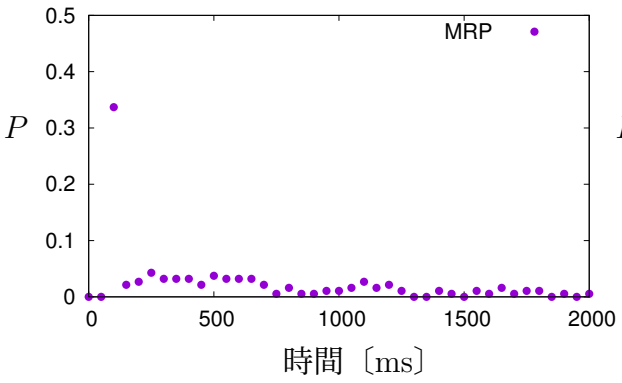


図 4.22: ユーザー 02 の MRP

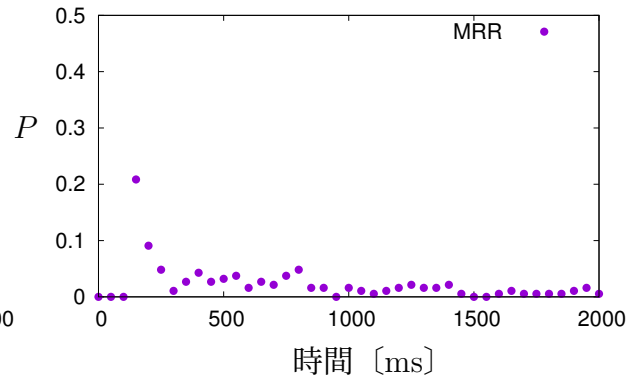


図 4.23: ユーザー 02 の MRR

図 4.24，図 4.25，図 4.26，図 4.27 がそれぞれユーザー 01 の特徴量 MAD（Mouse Actual Distance），MAS（Mouse Actual Speed），MCL（Mouse Curve Length），MCS（Mouse Curve Speed）の頻度分布である．

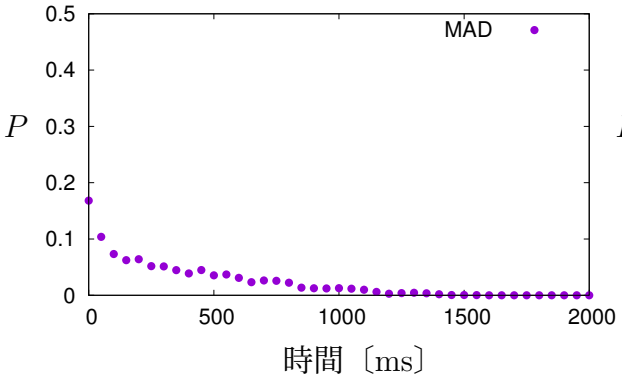


図 4.24: ユーザー 01 の MAD

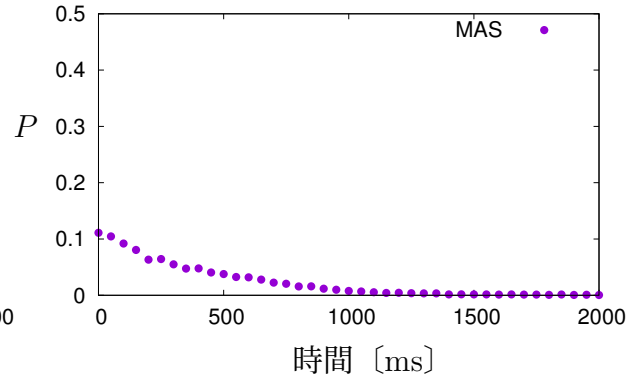


図 4.25: ユーザー 01 の MAS

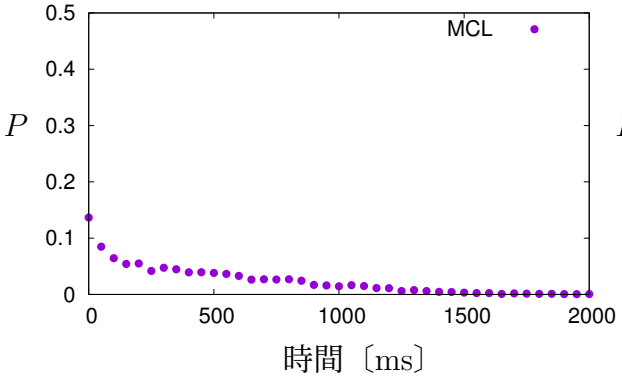


図 4.26: ユーザー 01 の MCL

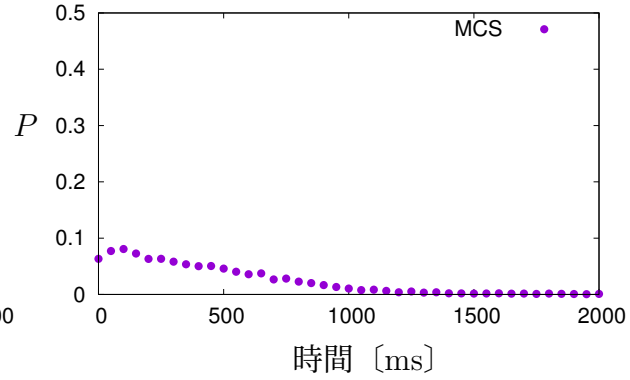


図 4.27: ユーザー 01 の MCS

比較のためにユーザー 02 の MAD（図 4.28），MAS（図 4.29），MCL（図 4.30），MCS（図 4.31）を掲載する．

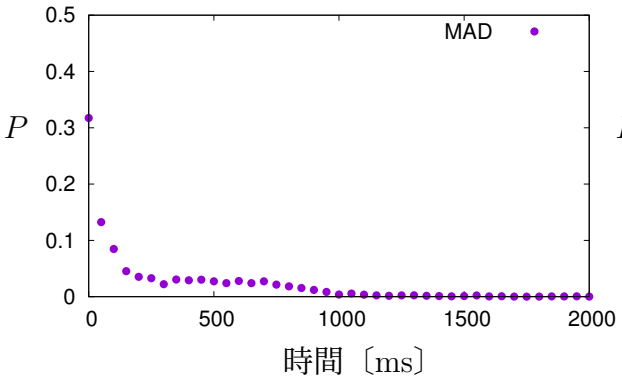


図 4.28: ユーザー 01 の MAD

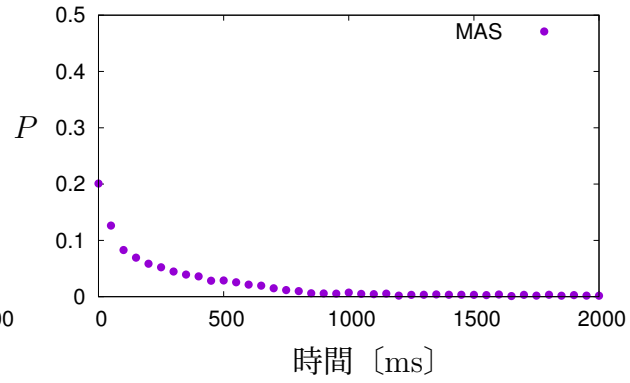


図 4.29: ユーザー 01 の MAS

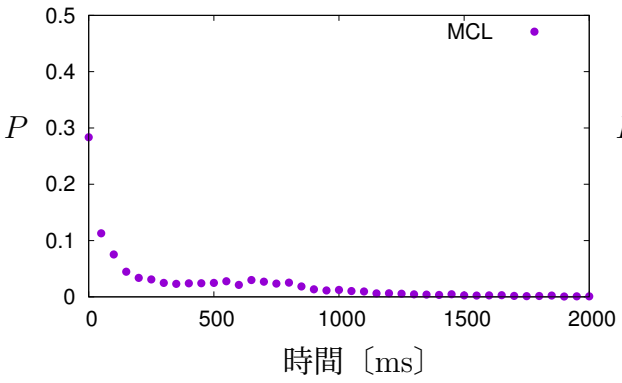


図 4.30: ユーザー 01 の MCL

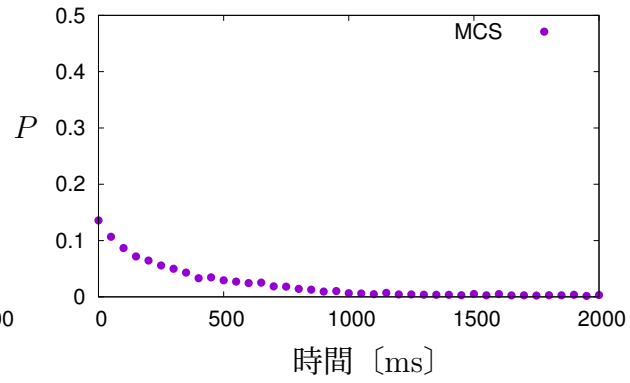


図 4.31: ユーザー 01 の MCS

4.4 パラメータ設定

DPTM において設定すべきは，式（3.1）の静的パラメータ K，動的パラメータ α_i の初期値 α_{i0}，式 (3.3) の単調増加関数 $f(n)$ である．しかしながら，動的パラメータ α_i の初期値 α_{i0} は，3.2 節で決定方法を与えているので，設定すべきパラメータは静的パラメータ K と単調増加関数 $f(n)$ である．

まず，静的パラメータ K の設定値について記述する．静的パラメータ K は，式（3.1）において $-1, 1$ に収束する速さを決めるパラメータであり，Trust 値 T の変動幅を決める．本研究は DPTM の認証精度を等価エラー率（EER）で評価する．つまり，正規ユーザーか不正ユーザーかを判定するための閾値を変化させ，本人拒否率（FRR）と他人受入率（FAR）を一致させた EER で評価を行う．EER を求める際，静的パラメータ K を大きくすると Trust 値の変化量 ΔT が小さくなり，不正ユーザー検出速度が低下する．その結果，FRR は低くなり，FAR は高くなるため，EER を求めるときの閾値が小さくなる．逆に静的パラメータ K を小さくすると Trust 値の変化量 ΔT が大きくなり，不正ユーザー検出速度が速くなる．その結果，FRR は高くなり，FAR は低くなるため，EER を求めるときの閾値が大きくなる．つまり，静的パラメータ K の値は EER を決めるときの閾値に大きな影響を与えるが，EER の値自体にはそれほど影響しない．しかしながら，静的パラメータ K の値は不正ユーザー検出速度に影響を与えるため，適切に設定しなければならない．

本評価実験では $K = 0.19$ とした．この値は，操作から得られる特徴量の確率 P の値が，動的パラメータ α_i の初期値 α_{i0} の半分，すなわち $\frac{\alpha_{i0}}{2}$ より小さいときに $\Delta T < -0.99$ となるように設定した．正規ユーザーの操作に近いかどうかで Trust 値 T の変化量 ΔT の正負は決まるが，その閾値が α_{i0} である．α_{i0} の半分の値であれば，不正ユーザーの可能性が高いと考え，そのときの Trust 値 T の変化量 ΔT を -0.99 より小さくするために $K = 0.19$ とした．具体的な値の求め方としては，式（3.1）の $P_i(v_{it})$ に $\frac{\alpha_i}{2}$ を代入すると

$$\Delta T_{it} = \tanh(-\frac{1}{2K}) \tag{4.1}$$

となる．また，

$$\tanh x = \frac{e^{2x} - 1}{e^{2x} + 1} \tag{4.2}$$

から

$$\Delta T_{it} = \frac{e^{-\frac{1}{K}} - 1}{e^{-\frac{1}{K}} + 1} \tag{4.3}$$

と決まる．これを K について解くと

$$K = \frac{1}{\log(1 - \Delta T_{it}) - \log(1 + \Delta T_{it})} \tag{4.4}$$

となるので，$\Delta T_{it} = -0.99$ を代入することで $K = 0.1889$ が得られる．これより，$K = 0.19$ とした．

次に式（3.3）の単調増加関数 $f(n)$ の設定について記述する．$f(n)$ は $\Delta T < 0$ を連続で取るときに α_i をどのように増加させるかを決める関数である．α_i が大きくなるということは $\Delta T > 0$ を得るための条件が厳しくなることを意味する．この α_i が動的に変化することで不正ユーザーをより速く検出可能となる．

本評価実験では

$$f(n) = (n-1)\alpha_{i0} \tag{4.5}$$

とした．これを式（3.3）に代入すると

$$\alpha_i = n\alpha_{i0} \tag{4.6}$$

となる．n 回連続で $\Delta T < 0$ を取るときに α_i をどのように変化させるかを考えたとき，式（4.6）のように n に比例した形で α_i を増加させるのは，まず試してみたい形である．

本節の最後に動的パラメータ α_i の初期値 α_{i0} を具体的に計算する際に必要な微小量について記述する．ユーザーから収集したログデータの 3 分の 1 を用いて α_{i0} を計算する際，微小量 $\Delta\alpha'_{i0}$ および Δp が必要となる．本評価実験において $\Delta\alpha'_{i0} = 0.01$,$\Delta p = 0.01$ とした．$\Delta\alpha'_{i0}$ は小さい値で計算したほうがよいが，小さすぎると $T_{\min}$ の変化量が 0 となってしまう．今回は予備実験を行い 0.01 が適切だと判断した．Δp においても，小さい値ほど正確な値に近づくが，小さすぎると計算時間が非常に長くなってしまう．こちらも予備実験において $\Delta p = 0.01$ と決めた．$\Delta p = 0.001$ で計算を行ったが，計算時間が非常に長くなってしまったにもかかわらず精度はほとんど変わらなかったためである．また，α_{i0} を決定するまでの繰り返し回数だが，予備実験において $\alpha_{i0} = 0.1$ として DPTM を計算したとき，全ユーザーが本人拒否率 0 となる閾値が -50 だったため，$T_{\min} < -50$ で計算を繰り返し α_{i0} を決定した．

図 4.32 が各ユーザーの α_{i0} の概略をレーダーチャートとして表したものである．中心の値が 0, 目盛り幅が 0.02，一番外側の目盛りが 0.16 である．また，KHT 平均は 68 個の KHT の平均を取ったものであり，2 連字キー平均は KPR，KPP，KRP，KRR の平均を取ったものである．MHT は MHT の α_0，ダブルクリック平均は MPR，MPP，MRP，MRR の平均である．マウス移動に関する平均は MAD，MAS，MCL，MCS の平均であり，MDD はドラッグ&ドロップの α_0 である．図 4.32 を見てわかるように，ダブルクリック平均や MDD はユーザー間の差が小さいのに比べ，KHT 平均やマウス移動に関する平均はユーザー間の差が大きい．

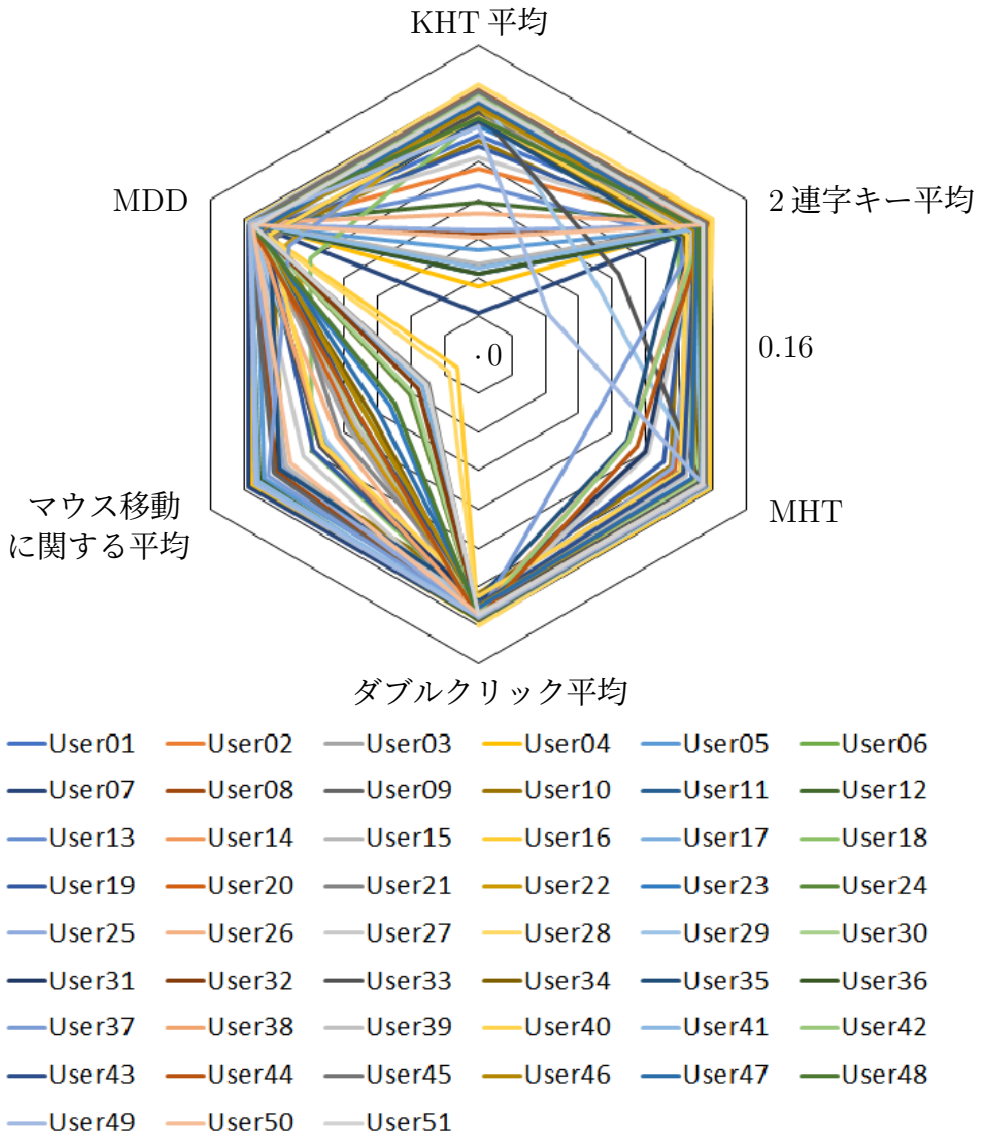


図 4.32: α_{i0} のレーダーチャート

4.5 実験結果

実験協力者51名分の正規ユーザープロファイルを準備し，DPTMの評価実験を行った．

4.5.1 DPTMのTrust値の変化

DPTMの評価実験には，収集したログデータの3分の1を正規ユーザープロファイル作成用に，3分の1をα_{i0}決定用データに，残りをテスト用データに使用した．

図4.33〜図4.42は，ユーザー01のプロファイルを用いて計算した結果であり，縦軸にTrust値T，横軸にアクション数を取ったものである．ユーザー01については，自分自身のプロファイルを用いてDPTMにかけているので，Trust値Tは100近傍で変化している．一方，ユーザー01以外は，Trust値Tがすぐに下がっていくのがわかる．比較のためユーザー02のプロファイルを用いた計算結果を付録D.1に掲載する．

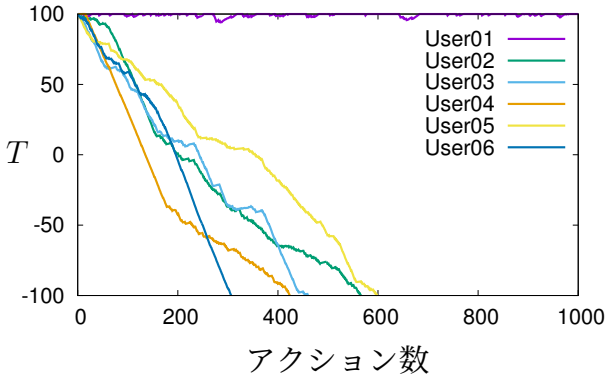


図4.33: Trust値の変化
（正規ユーザー01，不正ユーザー02〜06）

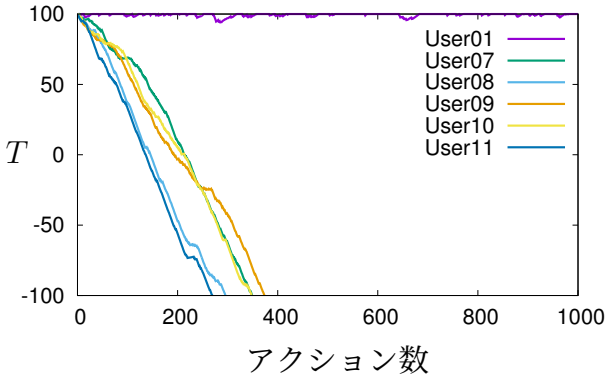


図4.34: Trust値の変化
（正規ユーザー01，不正ユーザー07〜11）

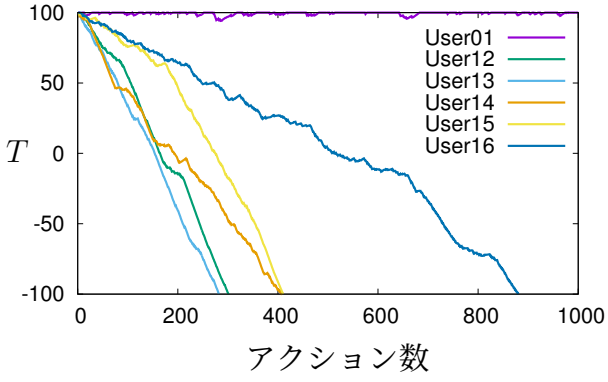


図4.35: Trust値の変化
（正規ユーザー01，不正ユーザー12〜16）

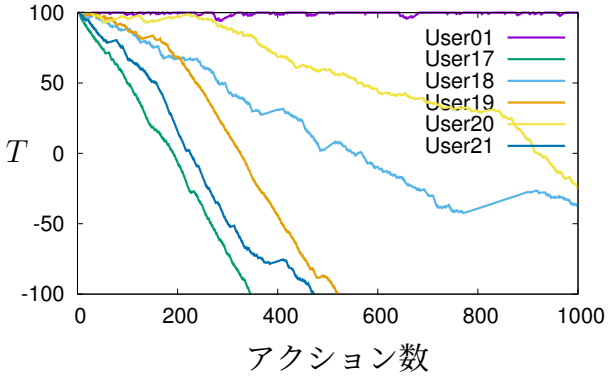


図4.36: Trust値の変化
（正規ユーザー01，不正ユーザー17〜21）

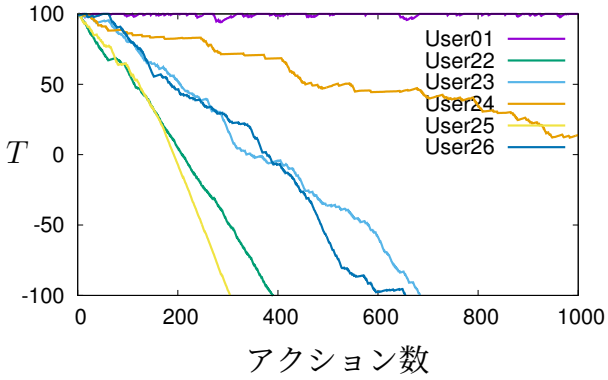


図 4.37: Trust 値の変化
（正規ユーザー 01，不正ユーザー 22〜26）

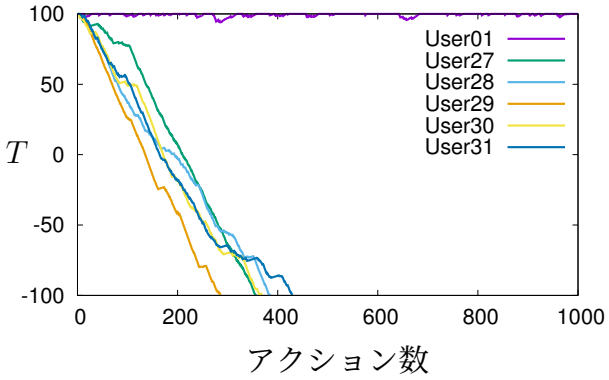


図 4.38: Trust 値の変化
（正規ユーザー 01，不正ユーザー 27〜31）

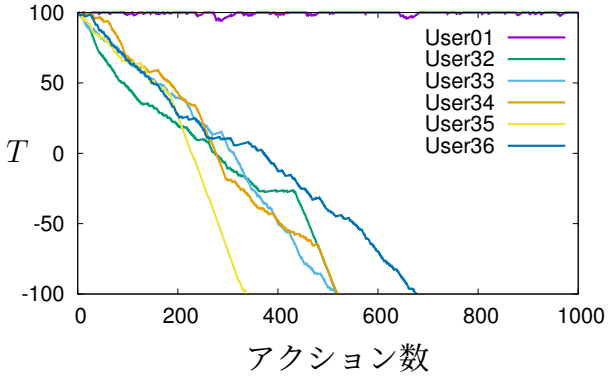


図 4.39: Trust 値の変化
（正規ユーザー 01，不正ユーザー 32〜36）

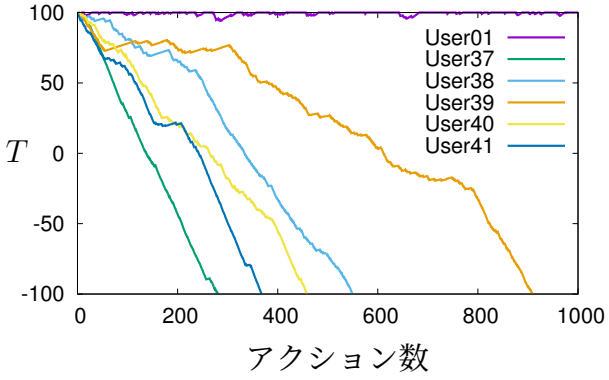


図 4.40: Trust 値の変化
（正規ユーザー 01，不正ユーザー 37〜41）

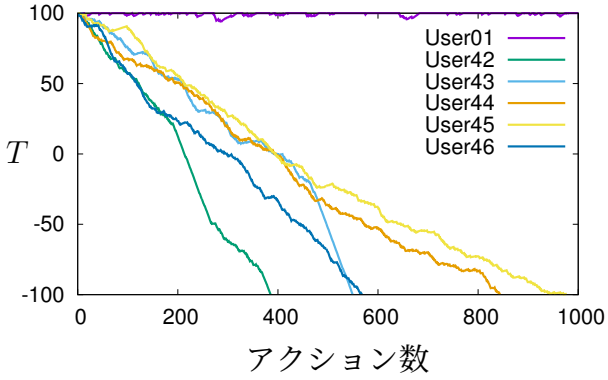


図 4.41: Trust 値の変化
（正規ユーザー 01，不正ユーザー 42〜46）

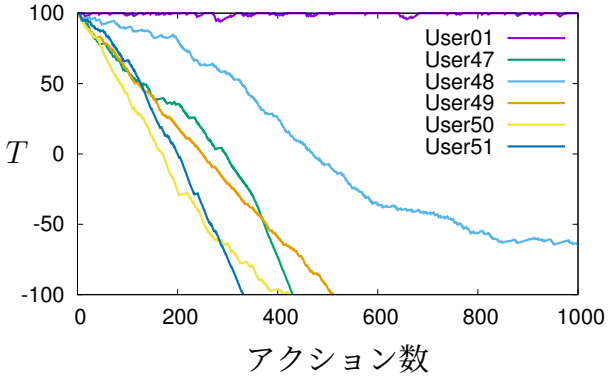


図 4.42: Trust 値の変化
（正規ユーザー 01，不正ユーザー 47〜51）

図 4.33〜図 4.42 を見ると，ユーザー 01 以外の多くのユーザーは Trust 値が急激に落ちているが，中には緩やかに落ちていくユーザーもいる．図 4.35 の User16 や図 4.36 の User18，User20，図 4.37 の User24，図 4.40 の User39，図 4.42 の User48 である．しかしながら，User01 と比較すると確実に落ちている．急激に落ちているユーザーと比較すると検出速度こそ遅くなってしまうが，Trust 値が緩やかに落ちていくユーザも検出可能である．

また，ログデータ収集において特に指定をせずにキー操作・マウス操作を行ってもらったため各ユーザにより全アクション数は様々である．表 4.2 は各ユーザーの全アクション数 A_i であり，平均値

$$m = \frac{1}{51}\sum_{i=1}^{51} A_i = 8051 \tag{4.7}$$

となった．なお，全アクション数の平均 m は，継続認証性能表の Summary を計算するときに使用する．

表 4.2: 各ユーザーの全アクション数

ユーザー	User01	User02	User03	User04	User05	User06
アクション数	6493	13627	6190	5272	4190	3438
ユーザー	User07	User08	User09	User10	User11	User12
アクション数	3457	6044	9048	1355	8001	8537
ユーザー	User13	User14	User15	User16	User17	User18
アクション数	4494	5054	9823	33877	5063	3867
ユーザー	User19	User20	User21	User22	User23	User24
アクション数	7064	8819	2043	10796	8479	4076
ユーザー	User25	User26	User27	User28	User29	User30
アクション数	11601	10797	6548	6282	2863	2335
ユーザー	User31	User32	User33	User34	User35	User36
アクション数	2246	7373	7992	6096	5485	5595
ユーザー	User37	User38	User39	User40	User41	User42
アクション数	3518	6792	4365	1324	4244	4203
ユーザー	User43	User44	User45	User46	User47	User48
アクション数	3175	8232	5596	3206	1742	18923
ユーザー	User49	User50	User51			
アクション数	58458	25884	6624			

また，各特徴量が Trust 値の変動にどれくらい寄与したかを表したのが表 4.3 である．全ユーザーの KHT による ΔT の平均を取ると -0.82 となった．また，各ユーザーの KHT による ΔT の標準偏差を求め，平均した値が 0.21 となった．同様に，2 連字キーは KPR，KPP，KRP，KRR の平均，DoubleClick は MPR，MPP，MRP，MRR の平均，マウス移動は MAD，MAS，MCL，MCS の平均，D&D はドラッグ&ドロップである．表より，KHT の寄与が一番大きいことがわかり，マウス移動やドラッグ&ドロップは変化量が小さいことがわかる．

表 4.3: 各特徴量の Trust 値の変化量 ΔT の平均

	KHT	2 連字キー	MHT	DoubleClick	マウス移動	D&D
ΔT の平均	-0.82	-0.29	-0.26	-0.44	-0.049	-0.079
ΔT の標準偏差	0.21	0.15	0.26	0.23	0.059	0.093

4.5.2 DPTM の EER

本小節では，DPTM の評価のために等価エラー率（EER）を求める．正規ユーザーか不正ユーザーかを判定するための閾値を 100 から −100 まで変化させながら，本人拒否率（FRR），他人受入率（FAR）を計算し，それらが一致する EER を求める．FRR は，本人のテストデータを本人プロファイルを用いた DPTM にかけ，51 ユーザー中，何人が拒否されるかで決定される．また，FAR は，1 人の正規ユーザーに対して 50 人の不正ユーザーが存在するので，$51 \times 50 = 2550$ 人中，何人が拒否されないかで FAR が決まる．

図 4.43 が FRR，FAR をプロットした図である．縦軸が本人拒否率，他人受入率であり，横軸が閾値である．閾値が 100 のときは，Trust 値 T が 100 を下回るとすぐに不正ユーザーと判定されるため，正規ユーザーであってもすぐに不正ユーザーと判定されてしまう．そのため FRR = 1.0 となる．また，このとき不正ユーザーが正規ユーザーと判定されることもないので，FAR = 0.0 となる．閾値を 100 から小さくしていくと FRR は小さくなり，FAR は大きくなる．2 つの値が交差するところが EER であり，EER = 4.57% となった．また，そのときの閾値は 3.33 であった．図 4.44 は縦軸に他人受入率（FAR），横軸に本人拒否率（FRR）を取った ROC 曲線（Receiver Operatorating Characteristic curve）である．FAR = FRR の直線との交点が EER となる．

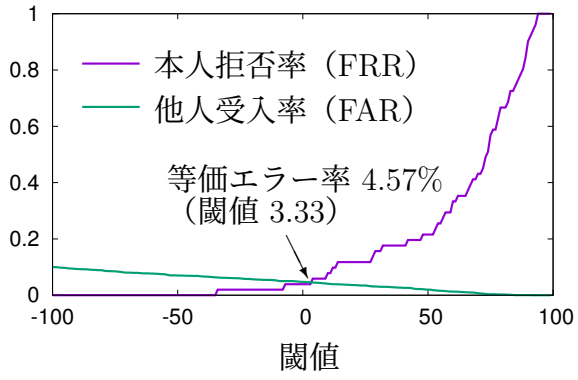


図 4.43: DPTM の本人拒否率，他人受入率

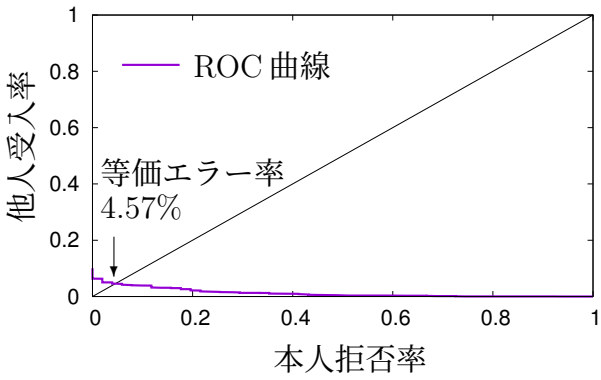


図 4.44: DPTM の ROC 曲線

4.5.3 DPTM の継続認証性能表

次章で DTM との比較を行うために，本小節では第 2 章で紹介した DPTM の継続認証性能表を作成する．継続認証性能表は正規ユーザーの平均持続アクション数（ANGA）や不正ユーザの平均持続アクション数（ANIA）を求めるため，正規ユーザーか不正ユーザーかを判定する閾値に大きく依存する．本論文では，継続認証性能表を作成する際，等価エラー率のときの閾値を用いる．

等価エラー時の閾値 3.33 を用いた DPTM の継続認証性能表が表 4.4 である．表 4.4 の 1 列目の Category はカテゴリー，2 列目の#User はユーザー数，3 列目の ANGA（Average Number of Genuine Actions）は正規ユーザーの平均持続アクション数，4 列目の ANIA（Average Number of Imposter Actions）は不正ユーザーの平均持続アクション数，5 列目の#Imp. ND（Imposters Not Detected）は検出できなかった不正ユーザー数である．なお，Category の 4 つ（+/ + , + / − , − / + , − /−）については以下の通りである．

+/+ ：正規ユーザーの拒否なし，不正ユーザーの受け入れなし
+/− ：正規ユーザーの拒否なし，不正ユーザーの受け入れあり
−/+ ：正規ユーザーの拒否あり，不正ユーザーの受け入れなし
−/− ：正規ユーザーの拒否あり，不正ユーザーの受け入れあり

なお，+/+ については，正規ユーザーの拒否がないので，ANGA（正規ユーザー平均持続アクション数）は空欄となる．また，不正ユーザーの受け入れもないので#Imp. ND（検出できなかった不正ユーザー）も空欄となる．同様に，+/− の ANGA も空欄となり，−/+ の#Imp. ND も空欄となる．

表 4.4: DPTM の継続認証性能表

Category	#User	ANGA	ANIA	#Imp. ND
+/+	16		545	
+/−	32		782	112
−/+	2	6114	251	
−/−	1	3002	507	1
Summary	51	7876	1004	113

表 4.4 を見ると，+/+ が 16 ユーザーおり，不正ユーザーの平均持続アクション数（ANIA）が 545 アクションということがわかる．+/− が 32 ユーザーで，ANIA が 782 アクション，検出できなかった不正ユーザー数が 112 ユーザーである．−/+ は 2 ユーザー，つまり，正規ユーザーなのに拒否されたユーザーが 2 人おり，その平均持続アクション数（ANGA）は 6114 アクションである．−/− は 1 ユーザーおり，その 1 ユーザーの持続アクション数が 3002 アクション，また検出できなかったユーザーも 1 人（受け入れた不正ユーザー 1 人）で，その持続アクション数（ANIA）は 507 アクションとなる．この ANIA が 507 ということは，そもそものアクション数が 507 しかなかったことを意味し（全体の平均アクション数は 8051 アクション），507 アクションの間に不正ユーザーと検出できなかったということである．

表 4.4 の 6 行目の Summary については，#User と#Imp. ND については合計数だが，ANGA および ANIA については次のように計算する．まず ANGA について計算

する．16 名 + 32 名 = 48 名 は正規ユーザーの拒否はないので，テスト用データから得られる最大アクション数の全体平均値 $m = 8051$（式（4.7））を用いて，$-/+$ の 2 名は不正ユーザーと検出されるまでの 6114 アクション，$-/-$ の 1 名は不正ユーザーと検出されるまでの 3002 アクションを用いて

$$\text{Summary ANGA} = \frac{(16+32)\times m + 2\times 6114 + 1\times 3002}{51} \tag{4.8}$$

$$= 7876 \tag{4.9}$$

と計算する．ANIA については，次のように計算する．全体で 51 名のログデータを用いているので，正規ユーザー 1 名に対して 50 名の不正ユーザーが存在する．つまり，$+/+$ は 16 名の正規ユーザーに対して，それぞれ不正ユーザーが 50 名存在し，その不正ユーザーの平均持続アクション数が 545 アクションとなるため $(16\times 50\times 545)$ と計算する．同様に $+/-$ については $(32\times 50\times 782)$ となるが，検出できなかった不正ユーザーが 112 名いるため，112 名については全体のアクション数の平均値 $m = 8051$ をかけて $(((32\times 50)-112)\times 782 + 112\times m)$ と計算する．同様に $-/+$ は $(2\times 50\times 251)$，$-/-$ は $(((1\times 50)-1)\times 507 + 1\times m)$ を計算し，51 名 × 50 名 で平均を取る．つまり，

$$\begin{aligned}\text{Summary ANIA} = \frac{1}{51\times 50}\Big[\ & (16\times 50\times 545)\\ & + \{\ (32\times 50 - 112)\times 782 + 112\times m\}\\ & + (2\times 50\times 251)\\ & + \{(1\times 50 - 1)\times 507 + 1\times m\}\ \Big] \end{aligned} \tag{4.10}$$

$$= 1004 \tag{4.11}$$

となる．つまり，DPTM の ANGA（正規ユーザー平均持続アクション数）=7876 アクション，ANIA（不正ユーザー平均持続アクション数）=1004 アクションとなる．

第5章　DTMとの比較実験

本章では，既存研究であるDTMと本論文で提案するDPTMの比較を行う．比較するために，DTMで使用されたログデータでDPTMの計算を行えばよいが，個人識別可能情報ということで公開されていない．そこで，本研究で収集したログデータを使用してDTMの計算を行う．

5.1　Trust値の変化

DTMで使用したログデータは公開されていないため，本研究で収集した51名のログデータを用いてDTMの計算を行う．また，本研究と条件を同じにするため，本人データのみで学習，パラメータ調整を行うプロセス（文献[47]，Verification Process 4）で計算を行う．なお，キー操作・マウス操作のログデータにおいては，DPTMと同様，3等分し，2つのデータを学習，パラメータ調整に用い，残りの1つのデータでテストを行った．また，扱う特徴量もDPTMの評価実験で扱ったものと同じにした．

まず，Verification Process 4について説明する．このプロセスでは，本人データのみからスコアscを算出し，それを式（2.15）からTrust値Tの変化量ΔTを計算し，Trust値を変化させる．各特徴量のスコアscの算出方法は以下の通りである．

- Key Hold Time（KHT）
  事前にプロファイルデータとして，あるキーの押下時間v_iがn個あるとする（v_i（$i = 1$〜n））．ここに，あるキーの押下時間aが入ってきたとき，次のようにスコアscを計算する．まず，f_1, f_2, f_3を準備する．

$$f_1 = \frac{1}{n}\sum_{i=1}^{n}|v_i - a| \tag{5.1}$$

$$f_2 = \min_i\{v_i - a\} \tag{5.2}$$

$$f_3 = \max_i\{v_i - a\} \tag{5.3}$$

  ただし，$\min_i\{X_i\}$は，$X_1, X_2, \cdots, X_n$の最小値を取ることを意味し，$\max_i\{X_i\}$は，$X_1, X_2, \cdots, X_n$の最大値を取ることを意味する．このf_1, f_2, f_3を用いて

$$sc = 1 - \frac{f_1 - f_2}{f_3 - f_2} \tag{5.4}$$

と計算する．

- 2 連字キー
  KHT のときと同様，事前にプロファイルデータとして n 個データ（v_i^{pr}, v_i^{pp}, v_i^{rp}, v_i^{rr}）があるとする．ただし，v_i^{pr} は 1 つ目のキーが押されて 2 つ目のキーが離されるまでの時間（KPR）。他も同様に，v_i^{pp} が KPP，v_i^{rp} が KRP，v_i^{rr} が KRR である．ここに，$(a^{\mathrm{pr}}, a^{\mathrm{pp}}, a^{\mathrm{rp}}, a^{\mathrm{rr}})$ が入ってきたとき，

$$f_1 = \frac{1}{n}\sum_{i=1}^{n}\sqrt{(v_i^{\mathrm{pr}}-a^{\mathrm{pr}})^2+(v_i^{\mathrm{pp}}-a^{\mathrm{pp}})^2+(v_i^{\mathrm{rp}}-a^{\mathrm{rp}})^2+(v_i^{\mathrm{rr}}-a^{\mathrm{rr}})^2} \tag{5.5}$$

$$f_2 = \min_i\{\ \sqrt{(v_i^{\mathrm{pr}}-a^{\mathrm{pr}})^2+(v_i^{\mathrm{pp}}-a^{\mathrm{pp}})^2+(v_i^{\mathrm{rp}}-a^{\mathrm{rp}})^2+(v_i^{\mathrm{rr}}-a^{\mathrm{rr}})^2}\ \} \tag{5.6}$$

$$f_3 = \max_i\{\ CC_i\ \} \tag{5.7}$$

とし，

$$sc = \frac{f_1}{f_2}\cdot f_3 \tag{5.8}$$

と計算する．ただし，

$$CC_i = \frac{\sum_{T=\mathrm{pr,pp,rp,rr}}(a^T-\bar{a})(v_i^T-\bar{v_i})}{\sqrt{\sum_{T=\mathrm{pr,pp,rp,rr}}(a^T-\bar{a})^2}\sqrt{\sum_{T=\mathrm{pr,pp,rp,rr}}(v_i^T-\bar{v_i})}} \tag{5.9}$$

であり，

$$\sum_{T=\mathrm{pr,pp,rp,rr}} X^T = X^{\mathrm{pr}}+X^{\mathrm{pp}}+X^{\mathrm{rp}}+X^{\mathrm{rr}} \tag{5.10}$$

を表す．

- MHT（Mouse Hold Time）
  事前にプロファイルデータとして，クリック時間 v_i が n 個あるとする（$v_i(i=1\sim n)$）．ここに，テストデータのクリック時間 a が入ってきたとき，次のようにスコア sc を計算する．まず，f_1, f_2, f_3 を準備する．

$$f_1 = \frac{1}{n}\sum_{i=1}^{n}|v_i-a| \tag{5.11}$$

$$f_2 = \min_i\{v_i-a\} \tag{5.12}$$

$$f_3 = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(v_i-a)^2} \tag{5.13}$$

この f_1, f_2, f_3 を用いて

$$sc = \frac{w}{f_1 + f_3} + (1 - w)(1 - \frac{f_1 - f_3}{f_2 - f_3}) \tag{5.14}$$

で計算する．ただし，w は重みであり，今回の計算においては 0.5 とした．

- ダブルクリック
  ダブルクリック時間については 2 連字キーと同様にスコア sc を計算する．

- マウス移動，ドラッグ&ドロップ
  文献 [47] では，マウス移動とドラッグ&ドロップについては，他人のデータも用いて式（2.17），式（2.18）を用いて計算していた．今回は本人データのみで計算しているので，KHT と同様にスコア sc を計算した．

図 5.1〜図 5.10 は，正規ユーザー 01 で DTM を計算した結果である．比較のためユーザー 02 のプロファイルを用いた計算結果を付録 D.2 に掲載する．DPTM のときと同様に，本人データは Trust 値 T が 100 近傍で変動しているが，他ユーザーは Trust 値 T が落ちていく．

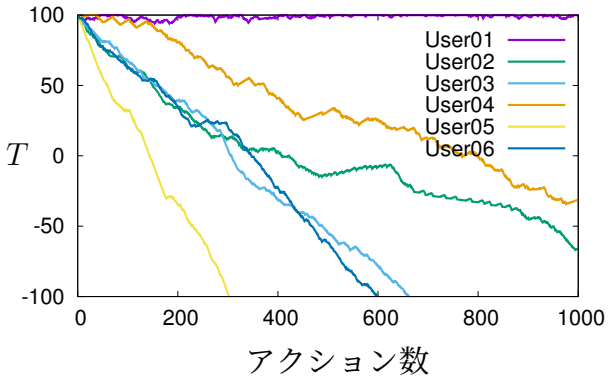


図 5.1: DTM の Trust 値の変化
（正規ユーザー 01，不正ユーザー 02〜06）

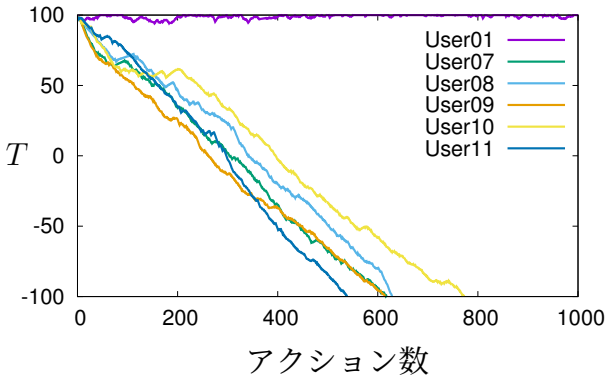


図 5.2: DTM の Trust 値の変化
（正規ユーザー 01，不正ユーザー 07〜11）

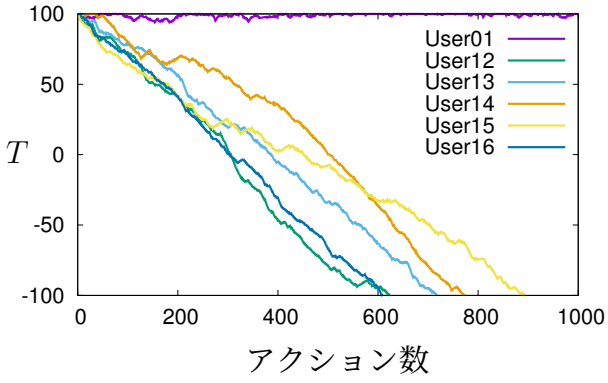


図 5.3: DTM の Trust 値の変化
（正規ユーザー 01，不正ユーザー 12〜16）

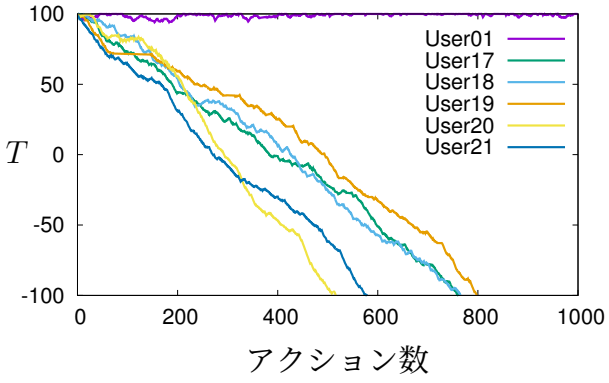


図 5.4: DTM の Trust 値の変化
（正規ユーザー 01，不正ユーザー 17〜21）

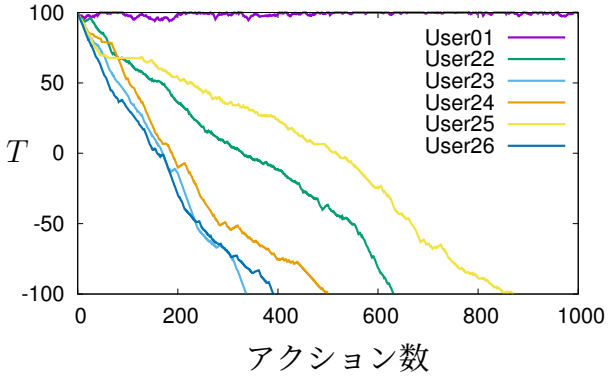


図 5.5: DTM の Trust 値の変化
（正規ユーザー 01，不正ユーザー 22〜26）

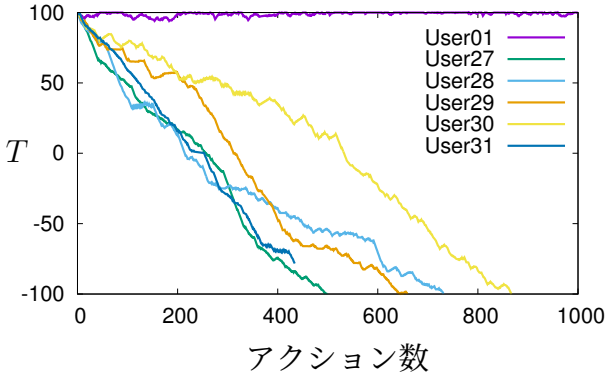


図 5.6: DTM の Trust 値の変化
（正規ユーザー 01，不正ユーザー 27〜31）

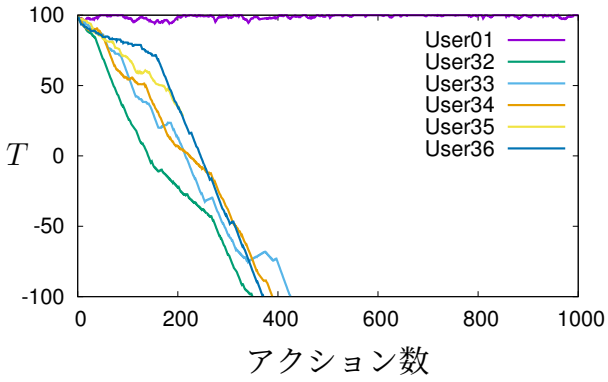


図 5.7: DTM の Trust 値の変化
（正規ユーザー 01，不正ユーザー 32〜36）

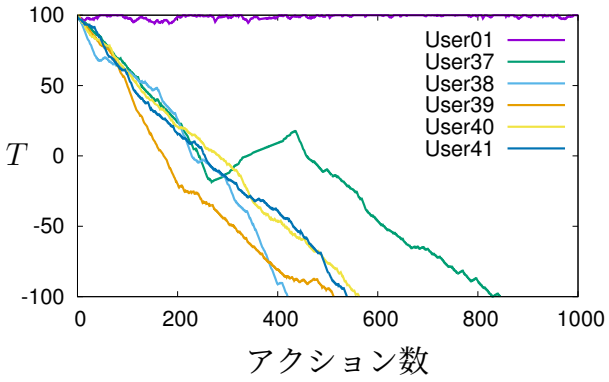


図 5.8: DTM の Trust 値の変化
（正規ユーザー 01，不正ユーザー 37〜41）

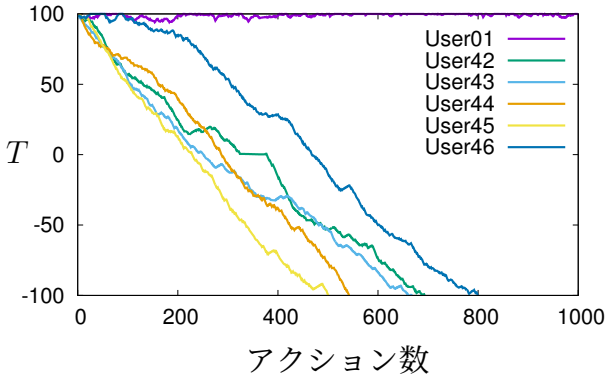


図 5.9: DTM の Trust 値の変化
（正規ユーザー 01，不正ユーザー 42〜46）

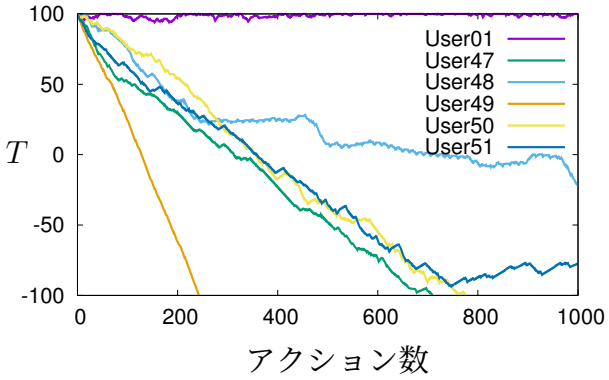


図 5.10: DTM の Trust 値の変化
（正規ユーザー 01，不正ユーザー 47〜51）

5.2 EER

次に，DTM の等価エラー率（EER）を求める．図 5.11 は，正規ユーザーか不正ユーザーかを判定する閾値を変化させたときの DTM の本人拒否率（FRR）と他人受入率（FAR）をプロットした図である．また図 5.12 は，DTM の ROC 曲線である．図 5.11 より FRR と FAR の一致する閾値を求めたところ −130 となり，EER= 25.9%となった．なお，DTM のパラメータ調整をさらに細かく行えば EER の精度を上げることは可能と考えるが，文献 [47] で，性能が近いと書かれているいくつかのアルゴリズムの EER が 20%前半ということを考えると EER= 25.9%は妥当だと考える．

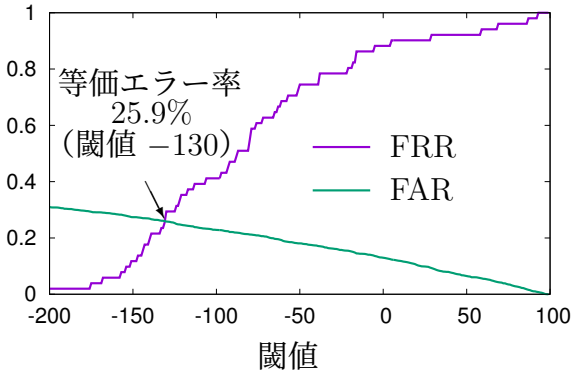


図 5.11: DTM の本人拒否率，他人受入率

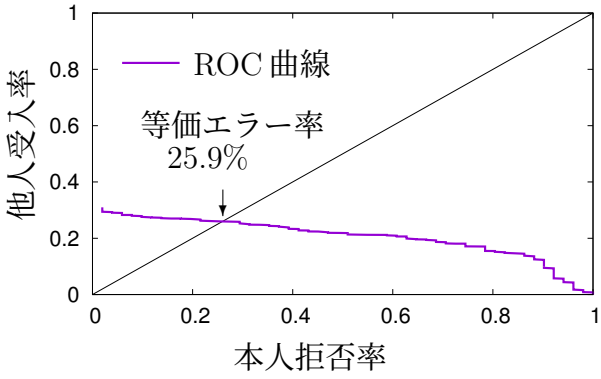


図 5.12: DTM の ROC 曲線

また，図 5.13 は前章で掲載した DPTM の本人拒否率，他人受入率（図 4.43）と図 5.11 を重ねた図である．図 5.13 の水色実線が DPTM の FRR，水色点線が DPTM の FAR である．また，紫色実線が DTM の FRR，紫色点線が DTM の FAR である．

まず，FRR（本人拒否率）に注目すると，閾値を 100 から下げていくとき，どちらも 1 から 0 に落ちていくが，DTM に比べ DPTM の方が急激に落ちていくのが見て取れる．FRR は 0 となるのが望ましいので，図 5.13 から FRR については，急速に 0 に近づいていく DPTM の方が DTM よりも優れていることがわかる．次に FAR（他人受入率）について見る．閾値を 100 から下げていくとき，どちらも 0 から値が上昇していく．しかしながら，DPTM と DTM では上昇の仕方が違う．DPTM の方が DTM よりもゆっくりと上昇していく．FAR についても 0 となるのが望ましいので，FAR についても，Trust 値 T の上昇率の小さい DPTM の方が DTM よりも優れていることがわかる．

図 5.14 は，前章で掲載した DPTM の ROC 曲線（図 4.44）と図 5.12 を重ねた図である．水色の実線が DPTM の ROC 曲線であり，紫色の実線が DTM の ROC 曲線である．ROC 曲線は，FRR = FAR の直線との交点が EER を表し，EER も 0 に近いほう

がよい．図 5.14 を見ると，DPTM の交点の方が DTM の交点より 0 に近く、DPTM の方が優れていることがわかる．

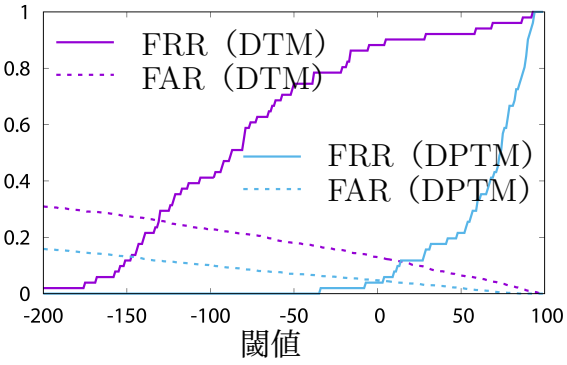


図 5.13: DTM および DPTM の本人拒否率，他人受入率

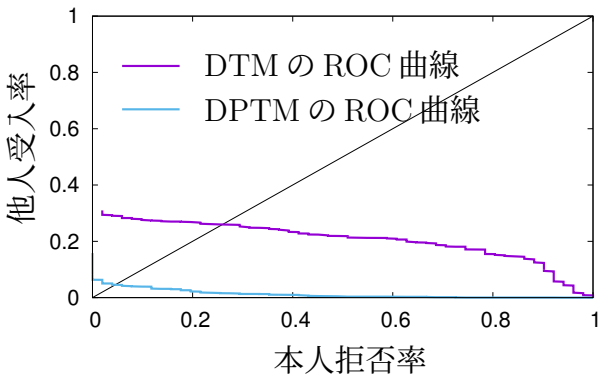


図 5.14: DTM および DPTM の ROC 曲線

5.3 継続認証性能表

本章の最後に，DTM の継続認証性能表を掲載する．DTM の継続認証性能表作成においては，DPTM で継続認証性能表を作成したときと同じ条件にするために EER=25.9%のときの閾値 −130 で作成した．表 5.1 が DTM の継続認証性能表である．正規ユーザーの拒否がなく，不正ユーザーの受け入れもなかった「+/+」が 1 ユーザーであり，不正ユーザーの平均持続アクション数（ANIA）が 723 アクションであった．正規ユーザーの拒否はないものの，不正ユーザーの受け入れのあった「+/−」が 38 ユーザーであり，不正ユーザーの受け入れは 639 ユーザーで，その平均持続アクション数（ANIA）は 1594 アクションとなった．正規ユーザーの拒否があり，不正ユーザーの受け入れがあった「−/+」が 0 ユーザーであった．また，正規ユーザーの拒否および不正ユーザーの受け入れがあった「−/−」が 12 ユーザーであり，そのときの正規ユーザーの平均持続アクション数（ANGA）は 2245 アクションであった．不正ユーザーの受け入れは 12 ユーザーで，不正ユーザーの平均持続アクション数（ANIA）は 1224 アクションであった．Summary も DPTM のときと同様に計算すると，正規ユーザーの平均持続アクション数（ANGA）が 5181 アクション．不正ユーザーの平均持続アクション数（ANIA）が 2511 アクション，検出できなかった不正ユーザーは 651 ユーザーとなった．

表 5.1: DTM の継続認証性能表

Category	#User	ANGA	ANIA	#Imp. ND
+/+	1		723	
+/−	38		1594	639
−/+	0			
−/−	12	2245	1224	12
Summary	51	5181	2511	651

表 5.2: DPTM の継続認証性能表

Category	#User	ANGA	ANIA	#Imp. ND
+/+	16		545	
+/−	32		782	112
−/+	2	6114	251	
−/−	1	3002	507	1
Summary	51	7876	1004	113

表 5.2 は DPTM の継続認証性能表の再掲載である．表 5.1 と表 5.2 を見ると,「+/+」においては，不正ユーザー平均持続アクション数（ANIA）が，DTM では 723 アクションなのに対して DPTM は 545 アクションと DPTM の方が ANIA が小さいことがわかる．これは検出速度が速いことを意味する.「−/+」においても検出できなかった不正ユーザー数（#Imp. ND）が DTM は 639 ユーザーなのに対して DPTM は 112 ユーザーと DPTM の方が検出率が高いことがわかる.「−/+」においては，DTM は 0 ユーザーだったのに対して DPTM は 2 ユーザーとなっている．しかしながら，単純に比較はできないが，DPTM の正規ユーザーの平均持続アクション数（ANGA）は 6114 アクションと非常に長く（今回収集したログデータの全アクション数の平均 m は 8051 アクション），不正ユーザーの平均持続アクション数（ANIA）は 251 アクションと非常に短い（他の項目と比較して 251 アクションは一番小さい）．また,「−/−」に対しては，検出できなかった不正ユーザー（#Imp. ND）が DTM では 12 ユーザーだったのに対して DPTM では 1 ユーザーとここでも検出率が高いことを示している．さらに，ANGA については，DTM2245 アクションに対して DPTM3002 アクションと DPTM の方がアクション数が長い．これは正規ユーザーであれば長く操作可能であることを意味し DPTM の方が優れていることを表す．また ANIA においては，DTM1224 アクションに対し DPTM507 アクションと検出速度も DPTM の方が優れていることがわかる．Summary においても正規ユーザーの平均持続アクション数は DPTM の方が長く（DPTM:7876 アクション，DTM:5181 アクション），不正ユーザーの平均持続アク

ション数は短い（DPTM:1004 アクション，DTM:2511 アクション）．また，検出できなかった不正ユーザー数も DPTM は 113 ユーザー，DTM は 651 ユーザーと検出率も高い．以上のことから，継続認証性能表においても DPTM の方が DTM より優れていることがわかる．

なお，DTM の継続認証性能表（表 5.1）を作成したときの FRR= 23.5%，FAR= 25.5%であり，DPTM の継続認証性能表（表 5.2）を作成したときの FRR= 5.88%，FAR= 4.43%であった．

第6章　考察

6.1　認証精度に関する考察

本論文では，継続認証のためのアルゴリズム Dynamic Probability Trust Model（DPTM）を新規に提案し，実験協力者 51 名分のログデータを用いて認証精度実験を行った．本人拒否率（FRR），他人受入率（FAR）から等価エラー率（EER）を求め EER = 4.57%が得られた（図 6.1）．今回のログデータ取得は，3 回分の講義（270 分）の中で，特に作

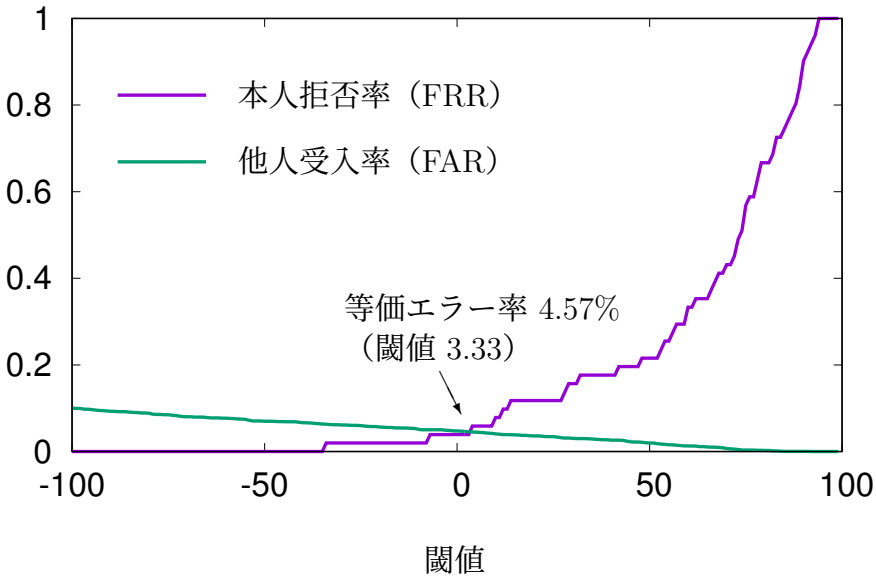


図 6.1: DPTM の本人拒否率，他人受入率

業内容も指定しないという状況の中で取得したため，すべての特徴量において十分なデータが得られていない．特に，キー入力については，入力頻度の高いキーであればよいが，z や q，記号などは全員分の頻度分布を得ることができなかった．なお，頻度分布が得られていない操作については頻度分布 $P = 0$ なので，常に Trust 値の変化量 $\Delta T < 0$ となる．また，2 連字キーにおいても，データ量が少ないことから，キーの種類に関係なく特徴量 KPP，KPR，KRP，KRR を計算し Trust 値を変化させた．しか

しながら，このような状況でも EER =4.57% が得られたことは，DPTM の可能性を示唆している．十分なログデータによる正規ユーザープロファイルの作成を行えば，今回得られなかった頻度分布，2 連字キーにおける各キーの組み合わせが活用可能となり，今回の結果と比べ，さらなる認証精度向上が期待できる．また，DPTM は本人のログデータのみで継続認証を行う．そのため，DPTM 継続認証を使えば使うほど，本人ログデータは蓄積され精度が向上が期待できる．

6.2 DTM との比較に関する考察

本論文では，新規に提案する DPTM と既存研究である DTM との比較実験も行った．比較実験を行うにあたり，DTM の文献 [47, 52] で使用したログデータを使用して DPTM の計算を行いたかったが，個人識別可能情報ということもあり公開されていない．そのため，本研究で取得したログデータを用いて DTM の計算を行い比較を行った．DTM の計算に際し，本研究と同条件にするため本人データのみで学習，パラメータ調整を行うプロセスを採用し計算を行った．

6.2.1 継続認証の性能について

図 6.2 は，DPTM，DTM の正規ユーザー，不正ユーザーを判定するための閾値を変化させたときの本人拒否率（FRR），他人受入率（FAR）である．これより DPTM の EER = 4.57%，DTM の EER = 25.9%となった．また，図 6.2 からわかるように，DPTM は閾値を 100 から下げていくと，FRR が急激に下がるのに対し，DTM は緩やかに下がる．また，FAR においては，閾値を 100 から下げていくとき，DPTM よりも DTM の方が上昇が大きい．

また，文献 [52] で提案された継続認証性能表についても作成した（表 6.1，表 6.2）．表の Summary を見ると，正規ユーザーの平均持続アクション数（ANGA）は，DPTM が 7876 アクション，DTM が 5181 アクションと DPTM の方が長い．これは，正規ユーザーがロックアウトされずに長く作業できることを意味する．また，不正ユーザーの平均持続アクション数（ANIA）は，DPTM が 1004 アクション，DTM が 2511 アクションと DPTM の方が短い．これは，不正ユーザーが速く検出されることを意味する．また検出できなかった不正ユーザー数（#Imp. ND）は，DPTM が 113 ユーザー，DTM が 651 ユーザーと検出率も高い．以上のことから，DPTM は DTM に比べ不正ユーザー検出率も高く，検出速度も速いことがわかる．DTM については，パラメータ調整をより細かく行うことで精度向上，検出速度向上が見込まれるが，劇的に良くなるとは考えにくい．DPTM の EER=4.57%，DTM の EER=25.9%からも DPTM の方が性能が良いと言える．また，他人検出速度も DPTM が 1004 アクション，DTM が 2511 アクションと DPTM の方が DTM よりも 2 倍以上速い．このことからも DPTM の方が DTM よりも優れていることがわかる．

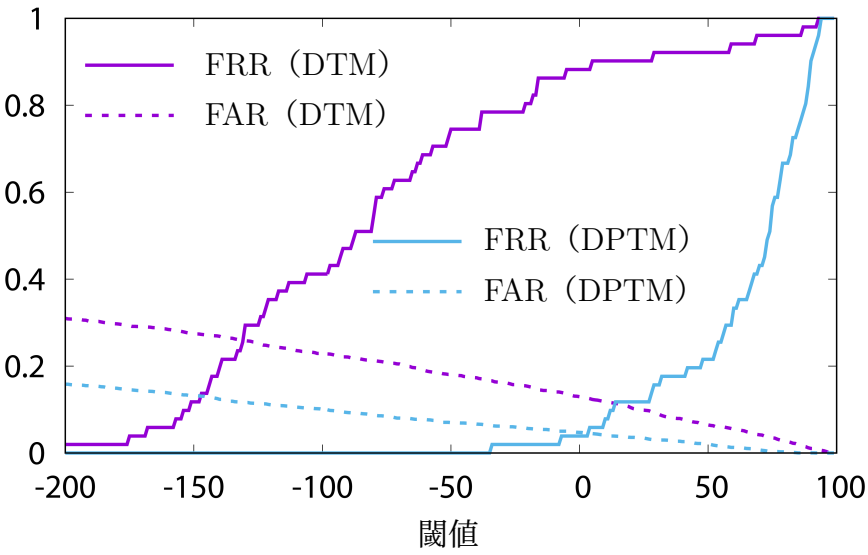


図 6.2: DTM および DPTM の本人拒否率，他人受入率

表 6.1: DPTM の継続認証性能表

Category	#User	ANGA	ANIA	#Imp. ND
+/+	16		545	
+/−	32		782	112
−/+	2	6114	251	
−/−	1	3002	507	1
Summary	51	7876	1004	113

表 6.2: DTM の継続認証性能表

Category	#User	ANGA	ANIA	#Imp. ND
+/+	1		723	
+/−	38		1594	639
−/+	0			
−/−	12	2245	1224	12
Summary	51	5181	2511	651

6.2.2 パラメータ調整について

DTM の課題の 1 つにパラメータ調整の困難性が挙げられる．DTM では，Trust 値 T の変化量 ΔT を決定するために，まずスコア（sc）を決めなければならない．文献 [52] では，得られた操作データから特徴量を抽出し，Artificial Neural Network（ANN），Counter-Propagation Artificial Neural Network（CPANN），Support Vector Machine（SVM）でそれぞれスコア sc を計算し，それぞれのスコア sc に重み w をかけて ΔT を計算するためのスコア sc を決定している．具体的には

$$(f_1, f_2, f_3) = (sc_{\mathrm{ANN}}, sc_{\mathrm{CPANN}}, sc_{\mathrm{SVM}}) \tag{6.1}$$

とし，以下のようにスコア sc を決定している．

$$sc = \frac{\sum_{j=1}^{3} w_j f_j}{\sum_{j=1}^{3} w_j}. \tag{6.2}$$

ただし，sc_{ANN} は ANN から得られるスコア，sc_{CPANN} は DPANN から得られるスコア，sc_{SVM} から得られるスコアである．しかしながら，スコア算出に最適な機械学習アルゴリズムは明記されておらず，ハイパーパラメータも不明である．そのため，どのようにスコア sc を算出するかを試行錯誤により決めなければならない．さらに，スコア算出方法が決まっても，次の式

$$\Delta T(sc_i) = \min\{-D + \frac{D \times (1 + \frac{1}{C})}{\frac{1}{C} + \exp(-\frac{sc_i - A}{B})} \ , \ C\} \tag{6.3}$$

により Trust 値の変化量 ΔT を決めなければならない．ΔT を決定する式中には，4 つのパラメータ（A, B, C, D）が入っており，これら 4 つのパラメータを決めなければ ΔT が計算できない．しかしながら，この 4 つのパラメータの決定方法も明記されていない．なお，文献 [?] では，この 4 つのパラメータは各ユーザーごとに決めることで精度が高まることも書かれており，そうなると「4 つ × 正規ユーザー数」だけの調整が必要となり，パラメータ調整が非常に困難である．

一方，DPTM で決めなければならないパラメータは 3 つ（K,α_{i0}, $f(n)$）である．しかしながら，α_{i0} については，3.2 節で具体的な決定方法を示しており，調整が必要なパラメータは実質 2 つである．K については，信頼値の変化量 ΔT が -1 に収束する速さを決める DPTM の静的パラメータであるため，個人ごとに決める必要はなく，1 つ決めればよい．今回は $P_i(v_i) < \frac{\alpha_{i0}}{2}$ のとき $\Delta T_i < -0.99$ となるように $K = 1.9$ とした．$f(n)$ については，単調増加関数であればよいため無数にある．その中で今回は，$\alpha_i = n\alpha_{i0}$ となるように $f(n) = (n-1)\alpha_{i0}$ とした．これは，動的パラメータ α_i が，$\Delta T < 0$ の連続回数 n と α_{i0} に比例するようにである．K, $f(n)$ ともに最適値，最適関数を探す必要はあるが，個人ごとに決める必要はないため，2 つ決めればよい．

以上のことから，DPTM の方が DTM よりパラメータ調整が容易であるといえる．

6.3 経時変化に関する考察

継続認証の課題として，経時変化への対応が挙げられる．時間の経過とともに変化するタイピングパターンやタイピングリズムにどう対応するかという課題である．一般的な認証システムにおいて初期登録した認証情報の更新は，その煩わしさもあり頻繁に行われることは少ない．そのため，登録後，数年経つと，正規ユーザーが不正ユーザーとして判定され，拒否されることもある．

DTM のような機械学習を用いる継続認証アルゴリズムにおいては，経時変化への対応として再学習を行うことで対応可能である．しかしながら，いつ，どのように行うかは課題である．再学習にあたってはコンピュータへの負荷も大きく，1 日単位で行った場合，その負荷に値するだけの精度向上が見込めるかを考えると，期待は薄い．どの程度の期間ごとに再学習を行うかは，個人に依存する可能性もあり難しい課題である．また，使用し続けることでデータ量は多くなるが，その分，負荷も大きくなり，学習時間も長くなる．再学習のためにコンピュータのリソースを取られてしまうと本末転倒である．また DTM においては，各パラメータを個人ごとに設定するため，学習後にパラメータの再設定が必要になる可能性がある．各パラメータの設定方法が明らかではない DTM においては深刻な課題となる．経時変化にどう対応するかは継続認証の課題となる．

一方，DPTM は経時変化にも対応可能だと考えている．DPTM で使用する正規ユーザープロファイルは，キー操作・マウス操作から得られる特徴量の頻度分布群であるため，更新が容易で常に最新の状態を保つことが可能である．本人が意識することなく，1 日単位で更新することや適度なデータ量が集まったときに更新することが可能である．頻度分布を作成するのみなのでコンピュータへの負荷も小さい．また，時間的な重みを考慮することで，過去のデータも活用しながら現在の状況をよく反映している正規ユーザープロファイルの作成が可能であると考えている．また使い続けることで本人のログデータは着実に蓄積され，各特徴量の頻度分布が確率分布に近づいていくため，時間の経過に伴って認証精度も高まることも期待している．しかしながら，以上の内容についてはまだ推察の域をでない．時間的な重みをどのように設定するか等も含め今後の課題としたい．

6.4 動的パラメータの初期値 α_{i0} に関する考察

DPTM の動的パラメータ α_i の初期値 α_{i0} は個人を特徴づける量となる可能性がある．各ユーザーの α_{i0} は 3.2 節の方法で本人のログデータのみを用いて決定する．α_{i0} は，ΔT を正にするか負にするかの閾値となっており，特定の特徴量の α_{i0} を微小変化させたときに Trust 値 T がどのように変化するかで α_{i0} を決めていく．Trust 値 T が大きく変化するような特徴量の α_{i0} は小さく，Trust 値 T が少ししか変化しないような特徴量の α_{i0} は大きく変化させる．この操作により，各特徴量が個人の操作にどのように依存しているかが α_{i0} に反映される．

図 6.3 は 51 名の各特徴量の α_{i0} をレーダーチャートとして表したものである．KHT 平均は 68 個の KHT の平均を取ったものであり，2 連字キー平均は KPR，KPP，KRP，KRR の平均を取ったものである．MHT は MHT の α_0，ダブルクリック平均は MPR，MPP，MRP，MRR の平均である．マウス移動に関する平均は MAD，MAS，MCL，MCS の平均であり，MDD はドラッグ&ドロップの α_0 である．図 6.3 を見てわかるように，ダブルクリック平均や MDD はユーザー間の差が小さいのに比べ，KHT 平均やマウス移動に関する平均はユーザー間の差が大きい．今回はデータ量の関係から，平均値で表示しているが十分なデータから正規ユーザープロファイルを作成し α_{i0} を決定することで，各特徴量による個人差が現れると期待している．今後の課題とはなるが，十分なデータから α_{i0} を決定し，ユーザーを識別する固有の統計量となること確認したい．

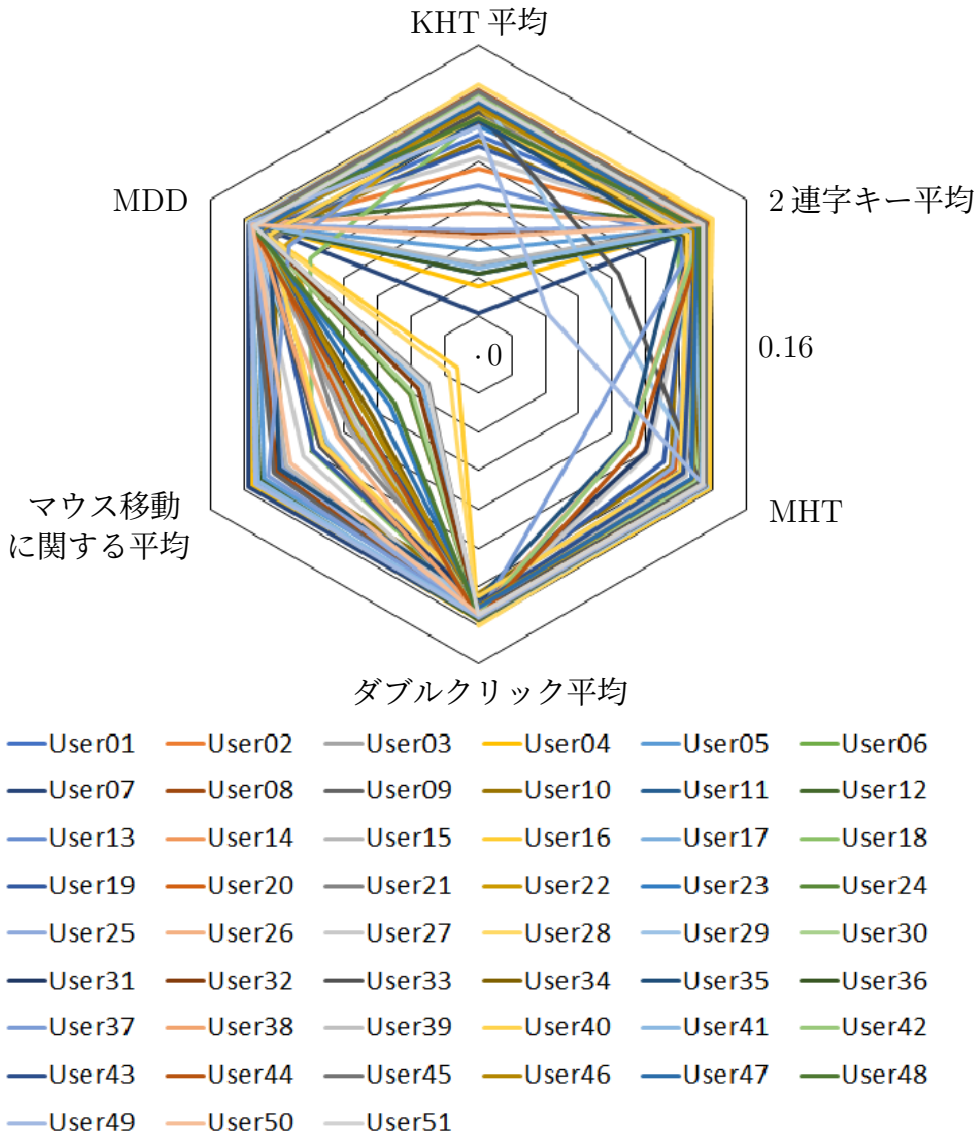


図 6.3: α_{i0} のレーダーチャート

第7章　まとめと今後の課題

本論文は，キー操作・マウス操作を用いた継続認証アルゴリズム Dynamic Probability Trust Model（DPTM）を新たに提案した．DPTM は，正規ユーザーの操作から得られる特徴量の確率分布群 P_i を用いて（実際に計算を行うときは頻度分布群で代用する.）信頼値 T を変動させ，信頼値 T が閾値を下回ったとき不正ユーザーと判定する．t 回目のアクションで取得した特徴 i の値が v_{it} のとき

$$\Delta T_{it} = \begin{cases} P_i(v_{it}) & (P_i(v_{it}) \geqq \alpha_i) \\ \tanh\left(\dfrac{P_i(v_{it}) - \alpha_i}{K\alpha_i} \right) & (P_i(v_{it}) < \alpha_i) \end{cases} \tag{7.1}$$

で信頼値 T の変化量を計算し，

$$T_{t+1} = \min\{\ T_t + \sum_i \Delta T_{it}\ ,\ 100\ \} \tag{7.2}$$

により，信頼値 T を決定する．ただし，K は静的パラメータ，α_i は動的パラメータである．このとき，信頼値 T が不正ユーザー閾値を下回るとき，不正ユーザーと判定しロックアウトする．

また，他人を速く検出するために，パラメータ α_i を動的に変化させる．信頼値の変化量 ΔT_{it} が連続で負の値を取るとき

$$\alpha_i = \alpha_{i0} + f(n) \tag{7.3}$$

とする．ただし，α_{i0} は動的パラメータの初期値であり，$f(n)$ は単調増加関数とする．これにより，$\Delta T < 0$ を取り続けると α_i の値が大きくなり，$\Delta T > 0$ を取ることが困難になり，さらに $\Delta T < 0$ を取り続ける．その結果，信頼値 T が下がり続け，不正ユーザーの早期検出が可能となる．

動的パラメータの初期値 α_{i0} は正規ユーザープロファイルおよび正規ユーザーのログデータより決定する．その決定方法は，まず，すべての特徴量の動的パラメータの初期値 α_{i0} を 0 とおく．その状態から，他を固定し，ある特徴量 i の初期値 α_{i0} を微小変化させる．その状態で正規ユーザーのログデータを用いて DPTM の計算を行う．このとき，動的パラメータ α_i は動的に変化させない．正規ユーザープロファイルを用いた DPTM に，正規ユーザーのログデータを入れているので信頼値 T は 100 近傍で変化する．このときの信頼値の最小値を $T_{\min}$ とする．ここで，α_{i0} を微小変化させたときの

$T_{\min}$ の変化量を $\frac{\partial T_{\min}}{\partial \alpha_{i0}}$ と表記する．すべての特徴量について $T_{\min}$ の変化量 $\frac{\partial T_{\min}}{\partial \alpha_{i0}}$ を計算し，その変化量の指数をとった値の割合を 1 から引いた値

$$R_i = 1 - \frac{\exp\left(\frac{\partial T_{\min}}{\partial \alpha_{i0}}\right)}{\sum_i \exp\left(\frac{\partial T_{\min}}{\partial \alpha_{i0}}\right)} \tag{7.4}$$

を用いて α_{i0} の変化量

$$\Delta\alpha_{i0} = \frac{R_i}{\sum_i R_i}\Delta p \tag{7.5}$$

を求める．ただし，Δp は α_{i0} に加える値の総量 $\Delta p = \sum_i \Delta\alpha_{i0}$ である．このようにして求めた R_i を用いて，その割合で Δp を分配し，α_{i0} に加え，α_{i0} を更新する．つまり，α_{i0} を微小変化させたとき $T_{\min}$ が大きく変化するものに対しては $\Delta\alpha_{i0}$ を小さく，ほとんど変化しないものに対しては $\Delta\alpha_{i0}$ を大きくする．この操作を繰り返すことで動的パラメータの初期値 α_{i0} を決定する．

DPTM の有用性を確認するために，実験協力者 51 名により評価実験を行った．図 7.1 がユーザー 01 のプロファイルを用いて DPTM を計算した結果である．図 7.1 を見てわかるように，ユーザー 01 の Trust 値 T は 100 近傍で変化しているが，他のユーザーは Trust 値 T の値が操作を行うごとに落ちている．

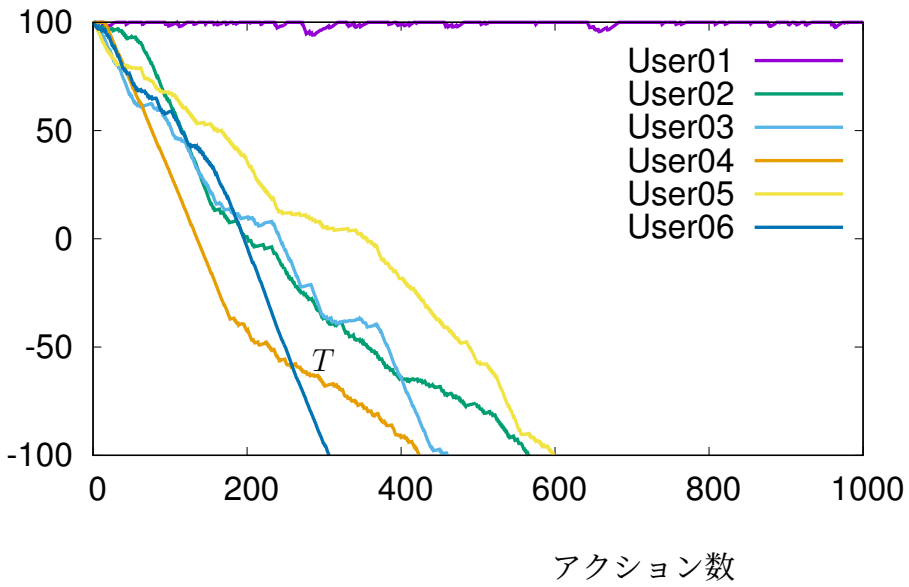


図 7.1: Trust 値の変化（正規ユーザー 01，不正ユーザー 02〜06）

また，正規ユーザーか不正ユーザーかを判定する閾値の値を変化させ，本人拒否率，他人受入率を計算し（図 7.2），等価エラー率を求めたところ，等価エラー率 4.57%が得られ，有用性が確認できた．

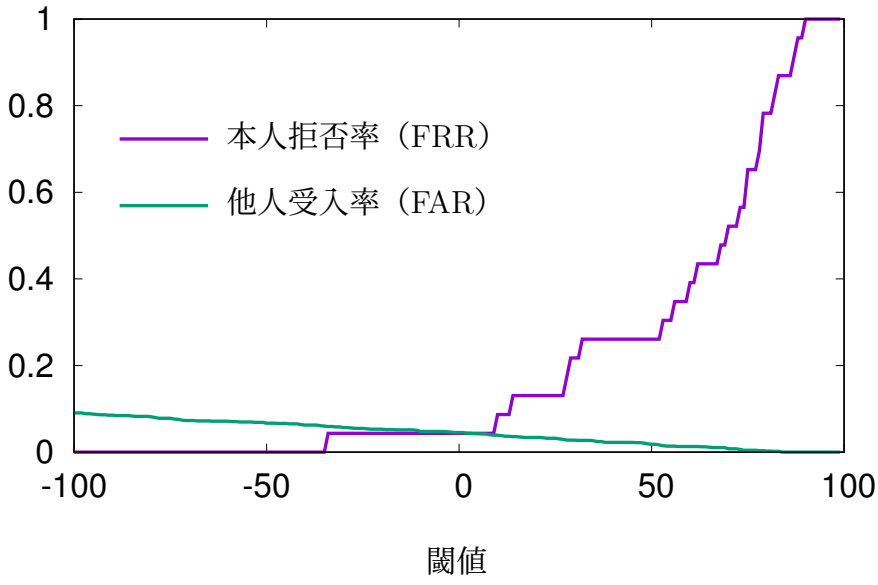


図 7.2: 本人拒否率，他人受入率

既存研究である DTM との比較実験も行った．図 7.3 は，DPTM，DTM の正規ユーザー，不正ユーザーを判定するための閾値を変化させたときの本人拒否率（FRR），他人受入率（FAR）である．これより DPTM の EER = 4.57%，DTM の EER = 25.9%となった．また，図 6.2 からわかるように，DPTM は閾値を 100 から下げていくと，FRR が急激に下がるのに対し，DTM は緩やかに下がる．また，FAR においては，閾値を 100 から下げていくとき，DPTM よりも DTM の方が上昇が大きいことから，DPTM の方が DTM より良いアルゴリズムであることがわかった．

また，文献 [52] で提案された継続認証性能表についても作成した（表 7.1，表 7.2）．表の Summary を見ると，正規ユーザーの平均持続アクション数（ANGA）は，DPTM が 7876 アクション，DTM が 5181 アクションと DPTM の方が長く，また，不正ユーザーの平均持続アクション数（ANIA）は，DPTM が 1004 アクション，DTM が 2511 アクションと DPTM の方が短い．つまり，DPTM の方が DTM より不正ユーザーの検出速度が速いことがわかった．さらに，検出できなかった不正ユーザー数（#Imp. ND）は，DPTM が 113 ユーザー，DTM が 651 ユーザーと DPTM の方が DTM より検出率が高いこともわかった．

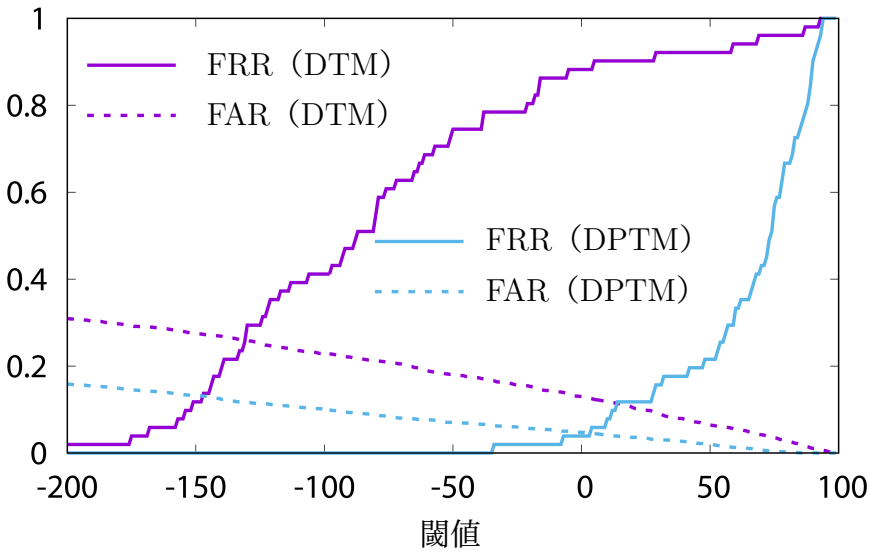


図 7.3: DTM および DPTM の本人拒否率，他人受入率

表 7.1: DPTM の継続認証性能表

Category	#User	ANGA	ANIA	#Imp. ND
+/+	16		545	
+/−	32		782	112
−/+	2	6114	251	
−/−	1	3002	507	1
Summary	51	7876	1004	113

表 7.2: DTM の継続認証性能表

Category	#User	ANGA	ANIA	#Imp. ND
+/+	1		723	
+/−	38		1594	639
−/+	0			
−/−	12	2245	1224	12
Summary	51	5181	2511	651

今後の課題は，さらなる認証精度，他人検出速度の向上である．そのためには十分なログデータの収集が必要となる．本論文では，十分なログデータが得られなかったた

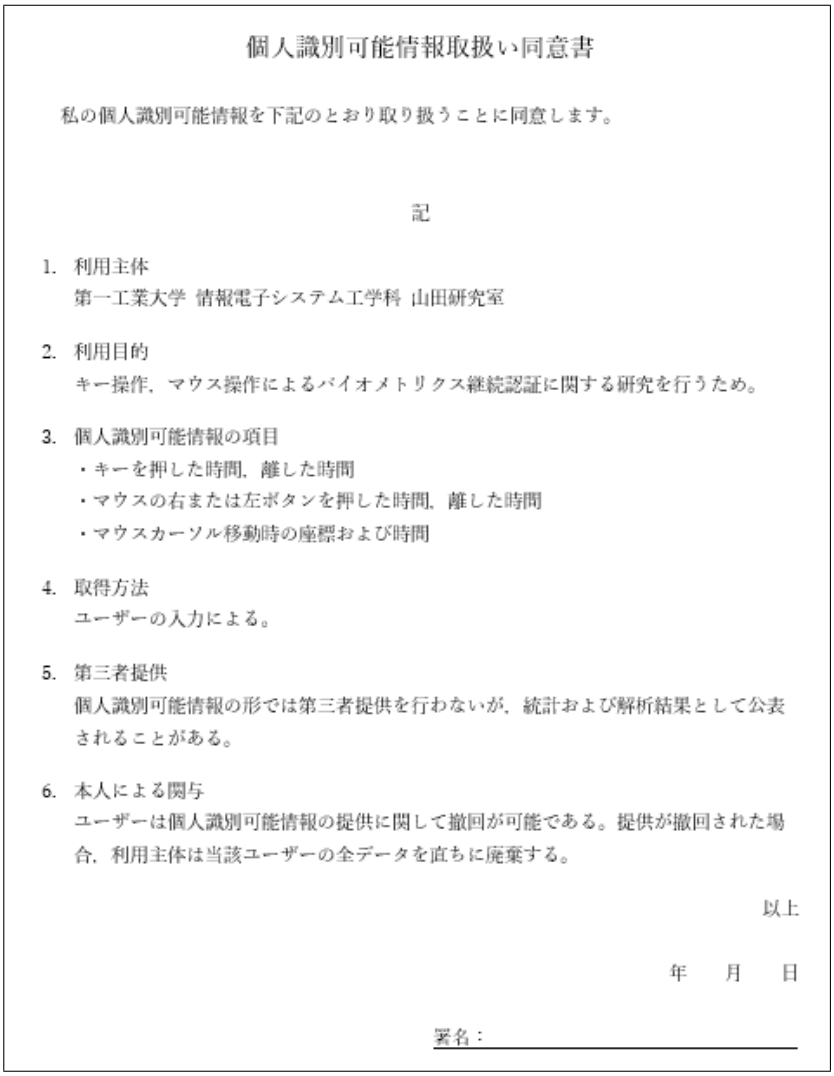
め，全てのキー操作の頻度分布が得られていない．また，2 連字キーにおいても，キーの区別をせずに DPTM の計算を行った．十分なログデータが得られることで，より詳細な継続認証を行うことが可能となる．その際，十分なログデータとはどの程度なのか，認証精度はどこまで向上させることができるのかを明らかにすることは今後の課題である．

また，十分なログデータが得られれば，動的パラメータの初期値 α_{i0} もより詳細に調べることが可能となる．α_{i0} は，ユーザーを識別する固有の統計量となる可能性があるため，α_{i0} のより詳細な解析を行うことが今後の課題である．

一般的な認証システムの課題でもある経時変化への対応も今後の課題である．DPTM は，正規ユーザープロファイルが頻度分布であるため更新が容易で，使用を続けることで大量のログデータが得られるため認証精度向上が見込める．しかしながら，現段階ではプロファイルの更新は行っていない．時間が経過してもプロファイルの更新をかけることで認証精度を向上させることが今後の課題である．

付 録A　個人識別可能情報取扱い同意書

評価実験に協力してくれた全ての人に以下の同意書にサインしてもらった。



個人識別可能情報取扱い同意書

私の個人識別可能情報を下記のとおり取り扱うことに同意します。

記

1. 利用主体
   第一工業大学 情報電子システム工学科 山田研究室

2. 利用目的
   キー操作，マウス操作によるバイオメトリクス継続認証に関する研究を行うため。

3. 個人識別可能情報の項目
   ・キーを押した時間，離した時間
   ・マウスの右または左ボタンを押した時間，離した時間
   ・マウスカーソル移動時の座標および時間

4. 取得方法
   ユーザーの入力による。

5. 第三者提供
   個人識別可能情報の形では第三者提供を行わないが，統計および解析結果として公表されることがある。

6. 本人による関与
   ユーザーは個人識別可能情報の提供に関して撤回が可能である。提供が撤回された場合，利用主体は当該ユーザーの全データを直ちに廃棄する。

以上

年　月　日

署名：

図 A.1: 個人識別可能情報取扱い同意書

付 録B　収集したログデータ

B.1　ユーザー01から取得したログデータ

以下に，ユーザー01から収集したログデータの一部（Seq.0〜Seq.300）を掲載する．

Seq,Evt.Type,Action,Time,Value1,Value2
0,MOUSE,MOVED,1503307409209,157,442,0
1,MOUSE,MOVED,1503307409224,183,435,0
2,MOUSE,MOVED,1503307409240,199,430,0
3,MOUSE,MOVED,1503307409246,218,426,0
4,MOUSE,MOVED,1503307409262,234,421,0
5,MOUSE,MOVED,1503307409277,250,417,0
6,MOUSE,MOVED,1503307409293,273,410,0
7,MOUSE,MOVED,1503307409308,329,396,0
8,MOUSE,MOVED,1503307409324,345,392,0
9,MOUSE,MOVED,1503307409324,360,390,0
10,MOUSE,MOVED,1503307409346,375,388,0
11,MOUSE,MOVED,1503307409377,387,387,0
12,MOUSE,MOVED,1503307409391,408,385,0
13,MOUSE,MOVED,1503307409407,415,385,0
14,MOUSE,MOVED,1503307409422,420,384,0
15,MOUSE,MOVED,1503307409436,435,383,0
16,MOUSE,MOVED,1503307409451,442,382,0
17,MOUSE,MOVED,1503307410081,441,381,0
18,MOUSE,MOVED,1503307410095,440,380,0
19,MOUSE,MOVED,1503307410111,438,379,0
20,MOUSE,MOVED,1503307410125,431,373,0
21,MOUSE,MOVED,1503307410140,428,371,0
22,MOUSE,MOVED,1503307410154,425,368,0
23,MOUSE,MOVED,1503307410169,424,366,0
24,MOUSE,MOVED,1503307410183,421,364,0
25,MOUSE,MOVED,1503307410200,419,362,0

26,MOUSE,MOVED,1503307410214,413,357,0
27,MOUSE,MOVED,1503307410229,410,355,0
28,MOUSE,MOVED,1503307410244,407,353,0
29,MOUSE,MOVED,1503307410259,405,352,0
30,MOUSE,MOVED,1503307410281,400,349,0
31,MOUSE,MOVED,1503307410297,397,348,0
32,MOUSE,MOVED,1503307410311,393,347,0
33,MOUSE,MOVED,1503307410327,393,346,0
34,MOUSE,MOVED,1503307410340,392,346,0
35,MOUSE,MOVED,1503307410355,391,346,0
36,MOUSE,MOVED,1503307410370,391,344,0
37,MOUSE,MOVED,1503307410399,390,342,0
38,MOUSE,MOVED,1503307410415,390,342,0
39,MOUSE,MOVED,1503307410429,390,340,0
40,MOUSE,MOVED,1503307410445,390,340,0
41,MOUSE,MOVED,1503307410460,390,339,0
42,MOUSE,MOVED,1503307410475,390,338,0
43,MOUSE,PRESSED,1503307410841,390,338,1
44,MOUSE,RELEASED,1503307410994,390,338,1
45,MOUSE,CLICKED,1503307410995,390,338,1
46,process,RUN,1503307411455,audiodg.exe,4808
47,process,EXIT,1503307411465,dllhost.exe,5096
48,KEY,PRESSED,1503307411872,7,55
49,KEY,RELEASED,1503307412139,7,55
50,KEY,PRESSED,1503307412139,J,74
51,KEY,RELEASED,1503307412586,J,74
52,KEY,PRESSED,1503307413302,Q,81
53,KEY,RELEASED,1503307413625,Q,81
54,KEY,PRESSED,1503307413625, 逆引用符,192
55,KEY,RELEASED,1503307413903, 逆引用符,192
56,KEY,PRESSED,1503307413903,W,87
57,KEY,PRESSED,1503307414203, 逆引用符,192
58,KEY,RELEASED,1503307414504,W,87
59,KEY,RELEASED,1503307414520, 逆引用符,192
60,KEY,PRESSED,1503307414520,R,82
61,KEY,RELEASED,1503307414874,R,82
62,KEY,PRESSED,1503307415230,Shift,160
63,KEY,PRESSED,1503307415589, ピリオド,190
64,KEY,RELEASED,1503307415933, ピリオド,190

65,KEY,RELEASED,1503307415933,Shift,160
66,KEY,PRESSED,1503307415933, スペース,32
67,KEY,RELEASED,1503307416292, スペース,32
68,KEY,PRESSED,1503307416355,Enter,13
69,KEY,RELEASED,1503307416683,Enter,13
70,KEY,PRESSED,1503307417183,Enter,13
71,KEY,RELEASED,1503307417496,Enter,13
72,KEY,PRESSED,1503307417746,Enter,13
73,KEY,RELEASED,1503307418058,Enter,13
74,MOUSE,MOVED,1503307419433,391,337,0
75,MOUSE,MOVED,1503307419449,435,324,0
76,MOUSE,MOVED,1503307419464,451,321,0
77,MOUSE,MOVED,1503307419480,472,317,0
78,MOUSE,MOVED,1503307419496,496,312,0
79,MOUSE,MOVED,1503307419511,552,300,0
80,MOUSE,MOVED,1503307419527,563,297,0
81,MOUSE,MOVED,1503307419543,572,295,0
82,MOUSE,MOVED,1503307419543,582,291,0
83,MOUSE,MOVED,1503307419558,592,289,0
84,MOUSE,MOVED,1503307419574,611,283,0
85,MOUSE,MOVED,1503307419589,617,280,0
86,MOUSE,MOVED,1503307419605,622,277,0
87,MOUSE,MOVED,1503307419621,625,275,0
88,MOUSE,MOVED,1503307419636,629,273,0
89,MOUSE,MOVED,1503307419652,633,271,0
90,MOUSE,MOVED,1503307419667,643,264,0
91,MOUSE,MOVED,1503307419683,647,262,0
92,MOUSE,MOVED,1503307419699,653,259,0
93,MOUSE,MOVED,1503307419714,657,255,0
94,MOUSE,MOVED,1503307419730,663,252,0
95,MOUSE,MOVED,1503307419746,667,249,0
96,MOUSE,MOVED,1503307419933,667,249,0
97,MOUSE,MOVED,1503307419949,670,246,0
98,MOUSE,MOVED,1503307419964,675,242,0
99,MOUSE,MOVED,1503307419980,682,236,0
100,MOUSE,MOVED,1503307419996,691,228,0
101,MOUSE,MOVED,1503307420011,700,220
102,MOUSE,MOVED,1503307420027,719,207
103,MOUSE,MOVED,1503307420043,725,204

104,MOUSE,MOVED,1503307420058,734,198
105,MOUSE,MOVED,1503307420074,738,196
106,MOUSE,MOVED,1503307420089,741,195
107,MOUSE,MOVED,1503307420105,744,193
108,MOUSE,MOVED,1503307420121,747,193
109,MOUSE,MOVED,1503307420136,750,191
110,MOUSE,MOVED,1503307420152,757,187
111,MOUSE,MOVED,1503307420168,759,185
112,MOUSE,MOVED,1503307420183,761,184
113,MOUSE,MOVED,1503307420183,763,182
114,MOUSE,MOVED,1503307420199,766,181
115,MOUSE,MOVED,1503307420214,771,175
116,MOUSE,MOVED,1503307420230,773,173
117,MOUSE,MOVED,1503307420246,776,171
118,MOUSE,MOVED,1503307420261,776,169
119,MOUSE,MOVED,1503307420277,777,169
120,MOUSE,MOVED,1503307420293,778,167
121,MOUSE,MOVED,1503307420308,780,166
122,MOUSE,MOVED,1503307420324,781,165
123,MOUSE,MOVED,1503307420339,783,163
124,MOUSE,MOVED,1503307420355,788,160
125,MOUSE,MOVED,1503307420371,788,159
126,MOUSE,MOVED,1503307420386,789,158
127,MOUSE,MOVED,1503307420527,789,158
128,MOUSE,PRESSED,1503307420902,789,158
129,MOUSE,DRAGGED,1503307421027,787,158
130,MOUSE,DRAGGED,1503307421043,784,158
131,MOUSE,DRAGGED,1503307421058,778,159
132,MOUSE,DRAGGED,1503307421074,770,161
133,MOUSE,DRAGGED,1503307421089,749,165
134,MOUSE,DRAGGED,1503307421105,742,167
135,MOUSE,DRAGGED,1503307421121,735,169
136,MOUSE,DRAGGED,1503307421121,729,171
137,MOUSE,DRAGGED,1503307421136,723,174
138,MOUSE,DRAGGED,1503307421152,720,177
139,MOUSE,DRAGGED,1503307421167,709,182
140,MOUSE,DRAGGED,1503307421183,705,185
141,MOUSE,DRAGGED,1503307421199,703,186
142,MOUSE,DRAGGED,1503307421214,702,186

143,MOUSE,DRAGGED,1503307421230,701,187
144,MOUSE,DRAGGED,1503307421246,701,187
145,MOUSE,DRAGGED,1503307421355,701,190
146,MOUSE,RELEASED,1503307421371,701,190
147,MOUSE,PRESSED,1503307421683,701,190
148,MOUSE,RELEASED,1503307421824,701,190
149,MOUSE,CLICKED,1503307421839,701,190
150,KEY,PRESSED,1503307426433,S,83
151,KEY,RELEASED,1503307426730,S,83
152,KEY,PRESSED,1503307426730,H,72
153,KEY,RELEASED,1503307427027,H,72
154,KEY,PRESSED,1503307427214, 引用符,222
155,KEY,RELEASED,1503307427558, 引用符,222
156,KEY,PRESSED,1503307427558, 逆引用符,192
157,KEY,RELEASED,1503307427871, 逆引用符,192
158,KEY,PRESSED,1503307428511,Tab,9
159,KEY,RELEASED,1503307428855,Tab,9
160,KEY,PRESSED,1503307428933,Enter,13
161,KEY,RELEASED,1503307429246,Enter,13
162,KEY,PRESSED,1503307429308,Shift,160
163,KEY,PRESSED,1503307429636, カンマ,188
164,KEY,RELEASED,1503307429886, カンマ,188
165,KEY,RELEASED,1503307429886,Shift,160
166,KEY,PRESSED,1503307429886, スペース,32
167,KEY,RELEASED,1503307430183, スペース,32
168,KEY,PRESSED,1503307430183, スペース,32
169,KEY,RELEASED,1503307430527, スペース,32
170,KEY,PRESSED,1503307430527,Enter,13
171,KEY,RELEASED,1503307430777,Enter,13
172,KEY,PRESSED,1503307430777,S,83
173,KEY,PRESSED,1503307431042,E,69
174,KEY,RELEASED,1503307431324,S,83
175,KEY,PRESSED,1503307431324,N,78
176,KEY,RELEASED,1503307431605,N,78
177,KEY,RELEASED,1503307431605,E,69
178,KEY,PRESSED,1503307431605,N,78
179,KEY,RELEASED,1503307431902,N,78
180,KEY,PRESSED,1503307431902,Backspace,8
181,KEY,RELEASED,1503307432183,Backspace,8

182,KEY,PRESSED,1503307432183,Backspace,8
183,KEY,RELEASED,1503307432511,Backspace,8
184,KEY,PRESSED,1503307432511,Backspace,8
185,KEY,RELEASED,1503307432824,Backspace,8
186,KEY,PRESSED,1503307432824,Backspace,8
187,KEY,RELEASED,1503307433105,Backspace,8
188,KEY,PRESSED,1503307433121,P,80
189,KEY,RELEASED,1503307433418,P,80
190,KEY,PRESSED,1503307433418,Y,89
191,KEY,RELEASED,1503307433730,Y,89
192,KEY,PRESSED,1503307433730,B,66
193,KEY,RELEASED,1503307433980,B,66
194,KEY,PRESSED,1503307433980,4,52
195,KEY,RELEASED,1503307434261,4,52
196,KEY,PRESSED,1503307434261,Tab,9
197,KEY,RELEASED,1503307434636,Tab,9
198,KEY,PRESSED,1503307434652,Enter,13
199,KEY,RELEASED,1503307435011,Enter,13
200,KEY,PRESSED,1503307435011,N,78
201,KEY,RELEASED,1503307435324,N,78
202,KEY,PRESSED,1503307435324,O,79
203,KEY,RELEASED,1503307435605,O,79
204,KEY,PRESSED,1503307435605,Backspace,8
205,KEY,RELEASED,1503307435902,Backspace,8
206,KEY,PRESSED,1503307435902,Backspace,8
207,KEY,RELEASED,1503307436214,Backspace,8
208,KEY,PRESSED,1503307436214,K,75
209,KEY,RELEASED,1503307436511,K,75
210,KEY,PRESSED,1503307436511,Enter,13
211,KEY,RELEASED,1503307436808,Enter,13
212,KEY,PRESSED,1503307437652,T,84
213,KEY,RELEASED,1503307437902,T,84
214,KEY,PRESSED,1503307437902,H,72
215,KEY,RELEASED,1503307438214,H,72
216,KEY,PRESSED,1503307438214,P,80
217,KEY,RELEASED,1503307438542,P,80
218,KEY,PRESSED,1503307438542,Y,89
219,KEY,RELEASED,1503307438855,Y,89
220,KEY,PRESSED,1503307438855,P,80

221,KEY,RELEASED,1503307439167,P,80
222,KEY,PRESSED,1503307439167,E,69
223,KEY,RELEASED,1503307439496,E,69
224,KEY,PRESSED,1503307439496,Tab,9
225,KEY,RELEASED,1503307439824,Tab,9
226,KEY,PRESSED,1503307439824,Enter,13
227,KEY,RELEASED,1503307440121,Enter,13
228,KEY,PRESSED,1503307441136, 引用符,222
229,KEY,RELEASED,1503307441511, 引用符,222
230,KEY,PRESSED,1503307441511,K,75
231,KEY,RELEASED,1503307441855,K,75
232,KEY,PRESSED,1503307441855, スペース,32
233,KEY,RELEASED,1503307442214, スペース,32
234,KEY,PRESSED,1503307442480,Enter,13
235,KEY,RELEASED,1503307442777,Enter,13
236,KEY,PRESSED,1503307444261,L,76
237,KEY,RELEASED,1503307444589,L,76
238,KEY,PRESSED,1503307444589,J,74
239,KEY,RELEASED,1503307444933,J,74
240,KEY,PRESSED,1503307445293,E,69
241,KEY,RELEASED,1503307445636,E,69
242,KEY,PRESSED,1503307445636,Y,89
243,KEY,RELEASED,1503307445933,Y,89
244,KEY,PRESSED,1503307446418,Q,81
245,KEY,RELEASED,1503307446793,Q,81
246,KEY,PRESSED,1503307446793, 逆引用符,192
247,KEY,RELEASED,1503307447183, 逆引用符,192
248,KEY,PRESSED,1503307447183, バックスラッシュ,220
249,KEY,RELEASED,1503307447527, バックスラッシュ,220
250,KEY,PRESSED,1503307447527, スペース,32
251,KEY,RELEASED,1503307447855, スペース,32
252,KEY,PRESSED,1503307447855,Enter,13
253,KEY,RELEASED,1503307448183,Enter,13
254,KEY,PRESSED,1503307448511,Shift,160
255,KEY,PRESSED,1503307448824, カンマ,188
256,KEY,RELEASED,1503307449152, カンマ,188
257,KEY,RELEASED,1503307449152,Shift,160
258,KEY,PRESSED,1503307449152, スペース,32
259,KEY,RELEASED,1503307449449, スペース,32

260,KEY,PRESSED,1503307449449, スペース,32
261,KEY,RELEASED,1503307449793, スペース,32
262,KEY,PRESSED,1503307449793,Enter,13
263,KEY,RELEASED,1503307450136,Enter,13
264,KEY,PRESSED,1503307450136,Enter,13
265,KEY,RELEASED,1503307450449,Enter,13
266,KEY,PRESSED,1503307450589,A,65
267,KEY,RELEASED,1503307450933,A,65
268,KEY,PRESSED,1503307451214,Backspace,8
269,KEY,RELEASED,1503307451589,Backspace,8
270,KEY,PRESSED,1503307451636,3,51
271,KEY,RELEASED,1503307451949,3,51
272,KEY,PRESSED,1503307451949,L,76
273,KEY,RELEASED,1503307452277,L,76
274,KEY,PRESSED,1503307452277,T,84
275,KEY,RELEASED,1503307452621,T,84
276,KEY,PRESSED,1503307452621, 逆引用符,192
277,KEY,RELEASED,1503307452918, 逆引用符,192
278,KEY,PRESSED,1503307452918,S,83
279,KEY,PRESSED,1503307453246,4,52
280,KEY,RELEASED,1503307453496,S,83
281,KEY,RELEASED,1503307453496,4,52
282,KEY,PRESSED,1503307453496,B,66
283,KEY,RELEASED,1503307453730,B,66
284,KEY,PRESSED,1503307453730, 逆引用符,192
285,KEY,RELEASED,1503307454011, 逆引用符,192
286,KEY,PRESSED,1503307454011,X,88
287,KEY,PRESSED,1503307454339, 逆引用符,192
288,KEY,RELEASED,1503307454621,X,88
289,KEY,RELEASED,1503307454621, 逆引用符,192
290,KEY,PRESSED,1503307454621,E,69
291,KEY,RELEASED,1503307454918,E,69
292,KEY,PRESSED,1503307454918,J,74
293,KEY,RELEASED,1503307455246,J,74
294,KEY,PRESSED,1503307455246,D,68
295,KEY,RELEASED,1503307455558,D,68
296,KEY,PRESSED,1503307455558,Q,81
297,KEY,RELEASED,1503307455886,Q,81
298,KEY,PRESSED,1503307455886, スペース,32

299,KEY,RELEASED,1503307456230, スペース,32
300,KEY,PRESSED,1503307456230,Shift,160

B.2　ユーザー 02 から取得したログデータ

比較のため，ユーザー 02 から収集したログデータの一部（Seq.4300〜Seq.4600）を掲載する．

Seq,Evt.Type,Action,Time,Value1,Value2
4300,MOUSE,MOVED,1519866538161,437,353
4301,MOUSE,MOVED,1519866538176,430,351
4302,MOUSE,MOVED,1519866538176,423,350
4303,MOUSE,MOVED,1519866538192,417,348
4304,MOUSE,MOVED,1519866538192,410,346
4305,MOUSE,MOVED,1519866538208,405,344
4306,MOUSE,MOVED,1519866538208,400,343
4307,MOUSE,MOVED,1519866538223,397,342
4308,MOUSE,MOVED,1519866538223,393,341
4309,MOUSE,MOVED,1519866538239,390,340
4310,MOUSE,MOVED,1519866538239,387,339
4311,MOUSE,MOVED,1519866538255,384,338
4312,MOUSE,MOVED,1519866538255,381,337
4313,MOUSE,MOVED,1519866538270,379,336
4314,MOUSE,MOVED,1519866538270,376,335
4315,MOUSE,MOVED,1519866538286,374,335
4316,MOUSE,MOVED,1519866538286,372,334
4317,MOUSE,MOVED,1519866538301,369,333
4318,MOUSE,MOVED,1519866538301,368,332
4319,MOUSE,MOVED,1519866538317,366,332
4320,MOUSE,MOVED,1519866538317,364,331
4321,MOUSE,MOVED,1519866538333,361,330
4322,MOUSE,MOVED,1519866538333,360,329
4323,MOUSE,MOVED,1519866538348,358,328
4324,MOUSE,MOVED,1519866538348,356,327
4325,MOUSE,MOVED,1519866538364,353,326
4326,MOUSE,MOVED,1519866538364,352,326
4327,MOUSE,MOVED,1519866538380,351,325

4328,MOUSE,MOVED,1519866538380,350,325
4329,MOUSE,MOVED,1519866538395,349,325
4330,MOUSE,MOVED,1519866538395,349,324
4331,MOUSE,MOVED,1519866538411,348,324
4332,MOUSE,MOVED,1519866538411,348,324
4333,MOUSE,MOVED,1519866538426,348,324
4334,MOUSE,MOVED,1519866538536,347,324
4335,MOUSE,MOVED,1519866538551,346,325
4336,MOUSE,MOVED,1519866538551,342,331
4337,MOUSE,MOVED,1519866538567,338,336
4338,MOUSE,MOVED,1519866538567,334,342
4339,MOUSE,MOVED,1519866538583,331,347
4340,MOUSE,MOVED,1519866538583,329,350
4341,MOUSE,MOVED,1519866538598,329,350
4342,MOUSE,MOVED,1519866538598,328,352
4343,MOUSE,MOVED,1519866538614,328,352
4344,MOUSE,MOVED,1519866538666,328,352
4345,MOUSE,MOVED,1519866538666,328,352
4346,MOUSE,MOVED,1519866538682,328,351
4347,MOUSE,MOVED,1519866538682,328,350
4348,MOUSE,MOVED,1519866538698,328,348
4349,MOUSE,MOVED,1519866538698,328,347
4350,MOUSE,MOVED,1519866538713,328,346
4351,MOUSE,MOVED,1519866538713,328,345
4352,MOUSE,MOVED,1519866538729,328,344
4353,MOUSE,MOVED,1519866538729,328,344
4354,MOUSE,MOVED,1519866538838,328,343
4355,MOUSE,MOVED,1519866538854,328,343
4356,MOUSE,MOVED,1519866538854,328,342
4357,MOUSE,MOVED,1519866538869,328,342
4358,MOUSE,MOVED,1519866538885,328,341
4359,MOUSE,MOVED,1519866538885,328,341
4360,MOUSE,MOVED,1519866538901,328,341
4361,MOUSE,MOVED,1519866538916,328,341
4362,MOUSE,MOVED,1519866538916,328,341
4363,MOUSE,MOVED,1519866538932,328,340
4364,MOUSE,MOVED,1519866538948,328,340
4365,MOUSE,MOVED,1519866538948,328,339
4366,MOUSE,MOVED,1519866538963,327,339

4367,MOUSE,MOVED,1519866538963,327,339
4368,MOUSE,MOVED,1519866538979,327,338
4369,MOUSE,MOVED,1519866538994,327,338
4370,MOUSE,MOVED,1519866538994,327,338
4371,MOUSE,MOVED,1519866539010,327,338
4372,MOUSE,MOVED,1519866539010,327,338
4373,MOUSE,MOVED,1519866539041,326,337
4374,MOUSE,MOVED,1519866539041,326,337
4375,MOUSE,MOVED,1519866539057,326,337
4376,MOUSE,MOVED,1519866539073,326,337
4377,MOUSE,MOVED,1519866539088,325,336
4378,MOUSE,MOVED,1519866539104,325,336
4379,MOUSE,MOVED,1519866539119,325,336
4380,MOUSE,MOVED,1519866539119,325,336
4381,MOUSE,MOVED,1519866539135,324,336
4382,MOUSE,MOVED,1519866539151,324,335
4383,MOUSE,MOVED,1519866539166,324,335
4384,MOUSE,MOVED,1519866539182,324,335
4385,MOUSE,MOVED,1519866539198,324,335
4386,MOUSE,MOVED,1519866539229,324,334
4387,MOUSE,PRESSED,1519866539739,324,334
4388,MOUSE,RELEASED,1519866539926,324,334
4389,MOUSE,CLICKED,1519866539926,324,334
4390,MOUSE,MOVED,1519866542630,324,336
4391,MOUSE,MOVED,1519866542630,324,336
4392,MOUSE,MOVED,1519866542645,325,337
4393,MOUSE,MOVED,1519866542645,325,337
4394,MOUSE,MOVED,1519866542664,325,337
4395,MOUSE,MOVED,1519866542667,326,338
4396,MOUSE,MOVED,1519866542667,327,339
4397,MOUSE,MOVED,1519866542682,327,339
4398,MOUSE,MOVED,1519866542682,328,340
4399,MOUSE,MOVED,1519866542698,329,341
4400,MOUSE,MOVED,1519866542698,331,342
4401,MOUSE,MOVED,1519866542713,332,343
4402,MOUSE,MOVED,1519866542713,334,344
4403,MOUSE,MOVED,1519866542729,337,345
4404,MOUSE,MOVED,1519866542745,338,346
4405,MOUSE,MOVED,1519866542745,340,347

4406,MOUSE,MOVED,1519866542760,343,348
4407,MOUSE,MOVED,1519866542760,346,349
4408,MOUSE,MOVED,1519866542776,350,350
4409,MOUSE,MOVED,1519866542776,355,352
4410,MOUSE,MOVED,1519866542792,359,353
4411,MOUSE,MOVED,1519866542792,364,355
4412,MOUSE,MOVED,1519866542807,369,357
4413,MOUSE,MOVED,1519866542807,373,358
4414,MOUSE,MOVED,1519866542823,378,360
4415,MOUSE,MOVED,1519866542823,383,362
4416,MOUSE,MOVED,1519866542838,387,363
4417,MOUSE,MOVED,1519866542838,392,365
4418,MOUSE,MOVED,1519866542854,396,366
4419,MOUSE,MOVED,1519866542854,399,368
4420,MOUSE,MOVED,1519866542870,403,370
4421,MOUSE,MOVED,1519866542870,406,372
4422,MOUSE,MOVED,1519866542885,409,374
4423,MOUSE,MOVED,1519866542885,410,376
4424,MOUSE,MOVED,1519866542901,412,376
4425,MOUSE,MOVED,1519866542901,414,377
4426,MOUSE,MOVED,1519866542917,415,378
4427,MOUSE,MOVED,1519866542917,417,378
4428,MOUSE,MOVED,1519866542932,417,378
4429,MOUSE,MOVED,1519866542932,418,379
4430,MOUSE,MOVED,1519866542948,418,379
4431,MOUSE,MOVED,1519866542948,419,379
4432,KEY,PRESSED,1519866544442,Enter,13
4433,process,RUN,1519866544666,ImeBroker.exe,9960
4434,process,EXIT,1519866544666,smartscreen.exe,1532
4435,KEY,RELEASED,1519866544666,Enter,13
4436,KEY,PRESSED,1519866545895,バックスラッシュ,220
4437,KEY,RELEASED,1519866546020,バックスラッシュ,220
4438,KEY,PRESSED,1519866546552,B,66
4439,KEY,RELEASED,1519866546807,B,66
4440,KEY,PRESSED,1519866546807,E,69
4441,KEY,RELEASED,1519866546901,E,69
4442,KEY,PRESSED,1519866547072,G,71
4443,KEY,PRESSED,1519866547213,I,73
4444,KEY,RELEASED,1519866547338,G,71

4445,KEY,RELEASED,1519866547338,I,73
4446,KEY,PRESSED,1519866547338,N,78
4447,KEY,RELEASED,1519866547463,N,78
4448,KEY,PRESSED,1519866547848,Shift,160
4449,KEY,PRESSED,1519866548223, 左大カッコ,219
4450,KEY,RELEASED,1519866548363,Shift,160
4451,KEY,RELEASED,1519866548363, 左大カッコ,219
4452,KEY,PRESSED,1519866548667,M,77
4453,KEY,PRESSED,1519866548854,I,73
4454,KEY,RELEASED,1519866548964,M,77
4455,KEY,RELEASED,1519866548964,I,73
4456,KEY,PRESSED,1519866548964,N,78
4457,KEY,PRESSED,1519866549073,I,73
4458,KEY,RELEASED,1519866549182,N,78
4459,KEY,RELEASED,1519866549182,I,73
4460,KEY,PRESSED,1519866549432,P,80
4461,KEY,RELEASED,1519866549557,P,80
4462,KEY,PRESSED,1519866549589,A,65
4463,KEY,RELEASED,1519866549754,A,65
4464,KEY,PRESSED,1519866549785,G,71
4465,KEY,PRESSED,1519866549941,E,69
4466,KEY,RELEASED,1519866550051,G,71
4467,KEY,RELEASED,1519866550066,E,69
4468,KEY,PRESSED,1519866550582,Shift,160
4469,KEY,PRESSED,1519866551057, 右大カッコ,221
4470,KEY,RELEASED,1519866551182, 右大カッコ,221
4471,KEY,RELEASED,1519866551198,Shift,160
4472,KEY,PRESSED,1519866552504, 左大カッコ,219
4473,KEY,RELEASED,1519866552684, 左大カッコ,219
4474,KEY,PRESSED,1519866552887,T,84
4475,KEY,RELEASED,1519866553027,T,84
4476,KEY,PRESSED,1519866553184, 右大カッコ,221
4477,KEY,RELEASED,1519866553340, 右大カッコ,221
4478,KEY,PRESSED,1519866554917,Shift,160
4479,KEY,PRESSED,1519866555245, 左大カッコ,219
4480,KEY,RELEASED,1519866555401, 左大カッコ,219
4481,KEY,RELEASED,1519866555417,Shift,160
4482,KEY,PRESSED,1519866558285,7,55
4483,KEY,RELEASED,1519866558426,7,55

4484,KEY,PRESSED,1519866558760,C,67
4485,KEY,RELEASED,1519866558932,C,67
4486,KEY,PRESSED,1519866558979,M,77
4487,KEY,RELEASED,1519866559120,M,77
4488,KEY,PRESSED,1519866559620,Shift,160
4489,KEY,PRESSED,1519866560191, 右大カッコ,221
4490,KEY,RELEASED,1519866560363, 右大カッコ,221
4491,KEY,RELEASED,1519866560363,Shift,160
4492,KEY,PRESSED,1519866562192, 下,40
4493,KEY,RELEASED,1519866562333, 下,40
4494,KEY,PRESSED,1519866562411, 下,40
4495,KEY,RELEASED,1519866562567, 下,40
4496,KEY,PRESSED,1519866562567, 下,40
4497,KEY,RELEASED,1519866562682, 下,40
4498,KEY,PRESSED,1519866562713, 下,40
4499,KEY,RELEASED,1519866562838, 下,40
4500,KEY,PRESSED,1519866562870, 下,40
4501,KEY,RELEASED,1519866563041, 下,40
4502,KEY,PRESSED,1519866563057, 下,40
4503,KEY,RELEASED,1519866563166, 下,40
4504,KEY,PRESSED,1519866563166, 下,40
4505,KEY,RELEASED,1519866563276, 下,40
4506,KEY,PRESSED,1519866565448, 上,38
4507,KEY,RELEASED,1519866565605, 上,38
4508,KEY,PRESSED,1519866566020,Enter,13
4509,KEY,RELEASED,1519866566192,Enter,13
4510,KEY,PRESSED,1519866567692,Backspace,8
4511,KEY,RELEASED,1519866567848,Backspace,8
4512,KEY,PRESSED,1519866568963, バックスラッシュ,220
4513,KEY,RELEASED,1519866569119, バックスラッシュ,220
4514,KEY,PRESSED,1519866569307,E,69
4515,KEY,RELEASED,1519866569463,E,69
4516,KEY,PRESSED,1519866569494,N,78
4517,KEY,RELEASED,1519866569651,N,78
4518,KEY,PRESSED,1519866569651,D,68
4519,KEY,RELEASED,1519866569754,D,68
4520,KEY,PRESSED,1519866570154,Shift,160
4521,KEY,PRESSED,1519866570357, 左大カッコ,219
4522,KEY,RELEASED,1519866570497,Shift,160

4523,KEY,RELEASED,1519866570497, 左大カッコ,219
4524,KEY,PRESSED,1519866570770,M,77
4525,KEY,PRESSED,1519866570911,I,73
4526,KEY,RELEASED,1519866571036,M,77
4527,KEY,RELEASED,1519866571036,I,73
4528,KEY,PRESSED,1519866571036,N,78
4529,KEY,PRESSED,1519866571145,I,73
4530,KEY,RELEASED,1519866571239,N,78
4531,KEY,RELEASED,1519866571286,I,73
4532,KEY,PRESSED,1519866571379,P,80
4533,KEY,RELEASED,1519866571536,P,80
4534,KEY,PRESSED,1519866571551,A,65
4535,KEY,RELEASED,1519866571684,A,65
4536,KEY,PRESSED,1519866571731,G,71
4537,KEY,RELEASED,1519866571871,G,71
4538,KEY,PRESSED,1519866571871,E,69
4539,KEY,RELEASED,1519866571996,E,69
4540,KEY,PRESSED,1519866572449,Shift,160
4541,KEY,PRESSED,1519866572816, 右大カッコ,221
4542,KEY,RELEASED,1519866572941, 右大カッコ,221
4543,KEY,RELEASED,1519866572941,Shift,160
4544,KEY,PRESSED,1519866573379,Enter,13
4545,KEY,RELEASED,1519866573551,Enter,13
4546,MOUSE,MOVED,1519866574260,420,380
4547,MOUSE,MOVED,1519866574260,420,380
4548,MOUSE,MOVED,1519866574276,436,391
4549,MOUSE,MOVED,1519866574276,459,408
4550,MOUSE,MOVED,1519866574292,509,451
4551,MOUSE,MOVED,1519866574292,569,506
4552,MOUSE,MOVED,1519866574307,629,565
4553,MOUSE,MOVED,1519866574307,688,626
4554,MOUSE,MOVED,1519866574323,743,686
4555,MOUSE,MOVED,1519866574323,793,743
4556,MOUSE,MOVED,1519866574338,838,794
4557,MOUSE,MOVED,1519866574338,877,836
4558,MOUSE,MOVED,1519866574354,909,870
4559,MOUSE,MOVED,1519866574370,951,912
4560,MOUSE,MOVED,1519866574370,961,921
4561,MOUSE,MOVED,1519866574385,962,922

4562,MOUSE,MOVED,1519866574385,962,922
4563,MOUSE,WHEEL,1519866574680,962,922
4564,MOUSE,WHEEL,1519866574692,962,922
4565,MOUSE,MOVED,1519866574880,962,922
4566,MOUSE,MOVED,1519866574895,964,922
4567,MOUSE,MOVED,1519866574895,965,921
4568,MOUSE,MOVED,1519866574911,968,919
4569,MOUSE,MOVED,1519866574911,973,917
4570,MOUSE,MOVED,1519866574926,978,916
4571,MOUSE,MOVED,1519866574926,982,915
4572,MOUSE,MOVED,1519866574942,985,914
4573,MOUSE,MOVED,1519866574942,985,913
4574,MOUSE,MOVED,1519866574958,986,913
4575,MOUSE,MOVED,1519866574973,986,912
4576,MOUSE,MOVED,1519866574973,986,912
4577,MOUSE,MOVED,1519866574989,986,911
4578,MOUSE,MOVED,1519866574989,987,909
4579,MOUSE,MOVED,1519866575005,988,908
4580,MOUSE,MOVED,1519866575020,991,906
4581,MOUSE,MOVED,1519866575020,992,905
4582,MOUSE,MOVED,1519866575036,996,904
4583,MOUSE,MOVED,1519866575036,1000,902
4584,MOUSE,MOVED,1519866575052,1004,900
4585,MOUSE,MOVED,1519866575052,1009,898
4586,MOUSE,MOVED,1519866575067,1013,895
4587,MOUSE,MOVED,1519866575067,1015,892
4588,MOUSE,MOVED,1519866575083,1017,890
4589,MOUSE,MOVED,1519866575083,1018,888
4590,MOUSE,MOVED,1519866575098,1018,887
4591,MOUSE,MOVED,1519866575114,1018,887
4592,MOUSE,MOVED,1519866575114,1018,887
4593,MOUSE,MOVED,1519866575130,1018,886
4594,MOUSE,MOVED,1519866575130,1018,885
4595,MOUSE,MOVED,1519866575145,1018,885
4596,MOUSE,MOVED,1519866575145,1018,883
4597,MOUSE,MOVED,1519866575161,1018,880
4598,MOUSE,MOVED,1519866575177,1017,879
4599,MOUSE,MOVED,1519866575177,1016,876
4600,MOUSE,MOVED,1519866575192,1014,871

付 録C　特徴量KHTの頻度分布

C.1　ユーザー01の特徴量KHTの頻度分布

以下にユーザー01のログデータから作成した特徴量KHTの頻度分布を掲載する。

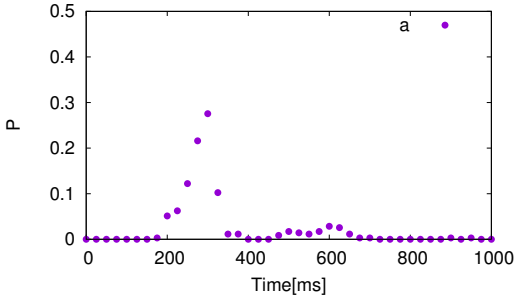


図 C.1: a

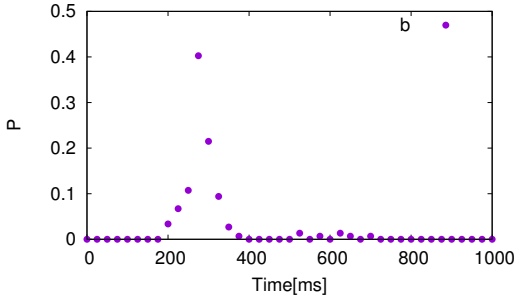


図 C.2: b

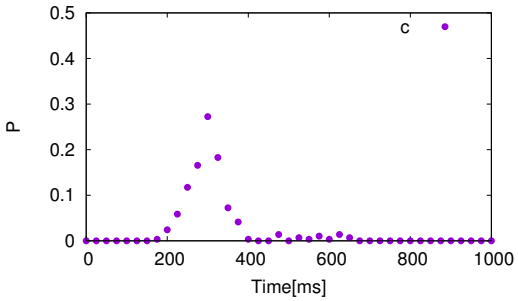


図 C.3: c

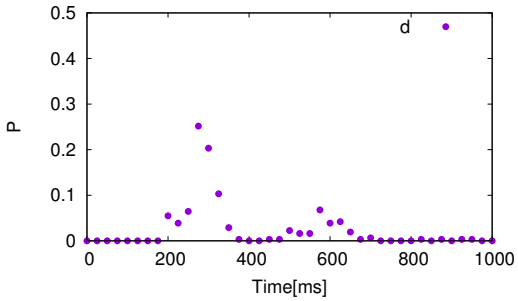


図 C.4: d

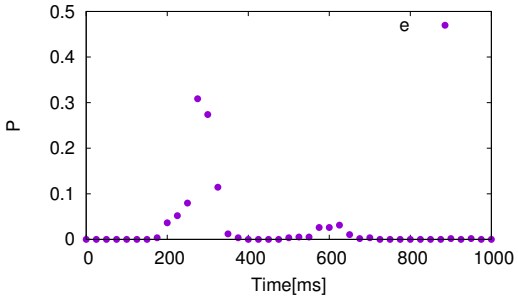


図 C.5: e

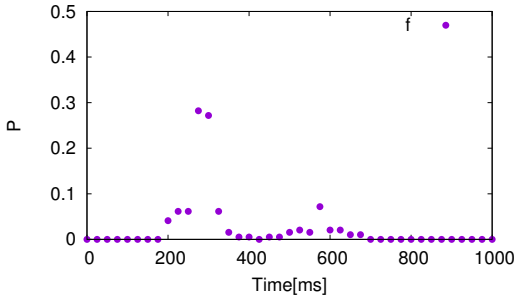


図 C.6: f

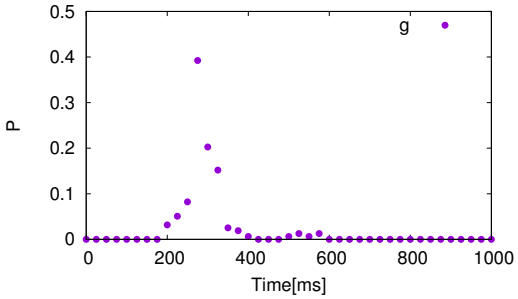


図 C.7: g

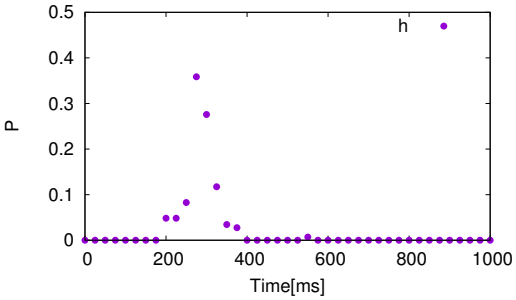


図 C.8: h

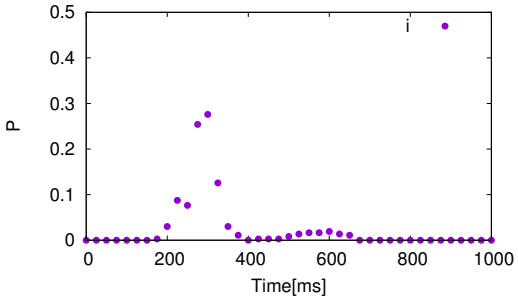


図 C.9: i

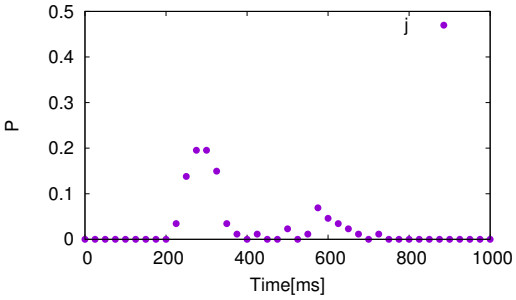


図 C.10: j

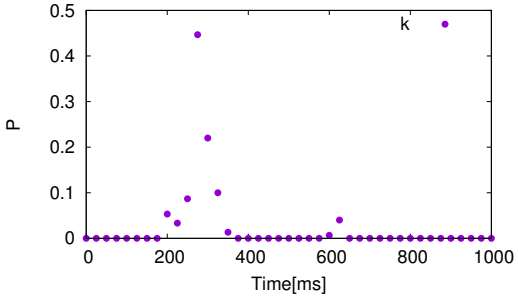


図 C.11: k

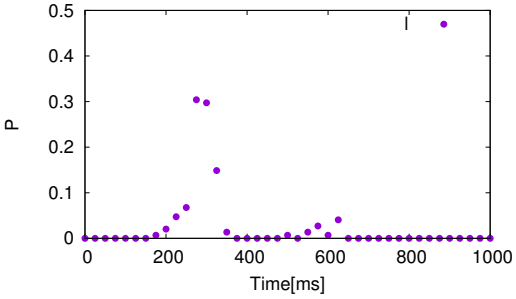


図 C.12: l

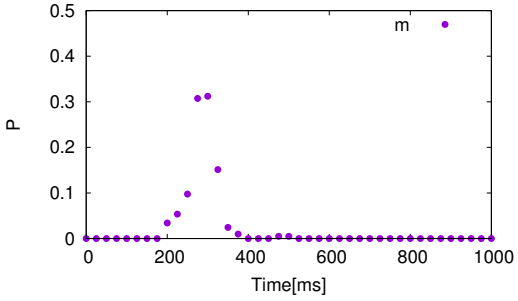


図 C.13: m

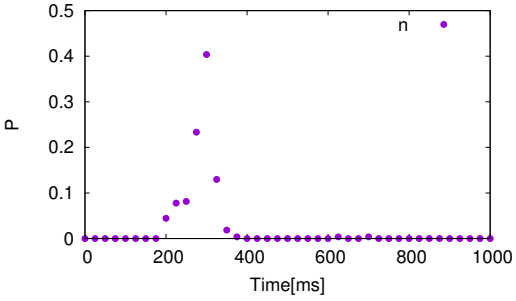


図 C.14: n

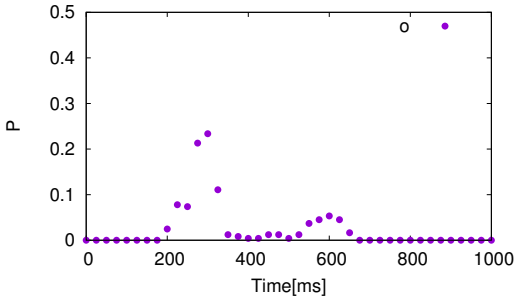


図 C.15: o

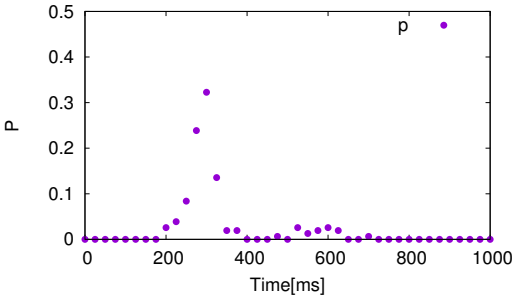


図 C.16: p

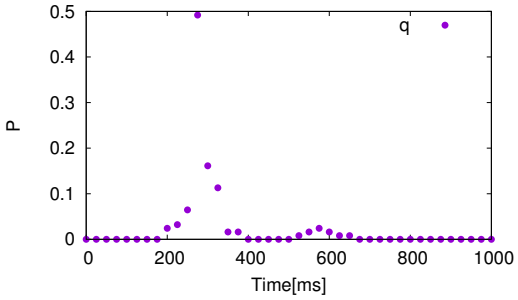


図 C.17: q

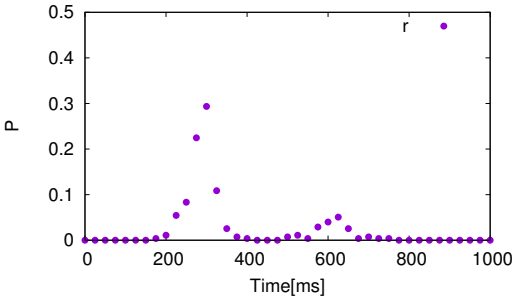


図 C.18: r

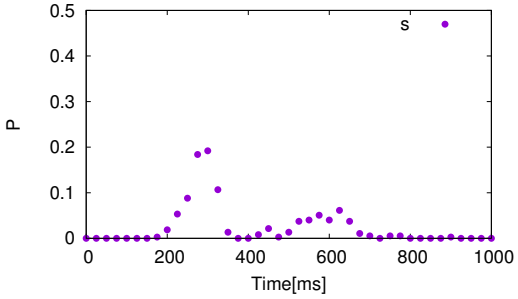


図 C.19: s

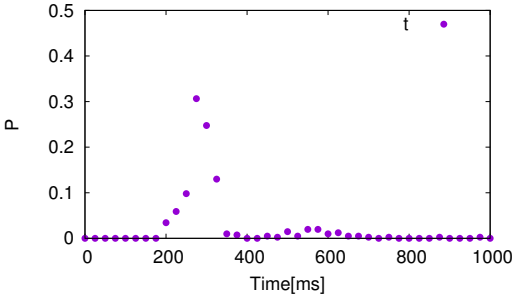


図 C.20: t

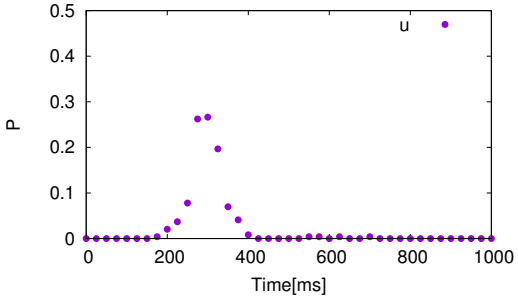


図 C.21: u

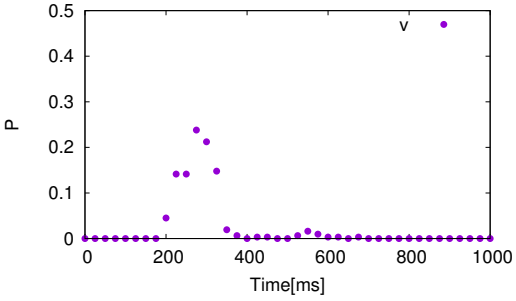


図 C.22: v

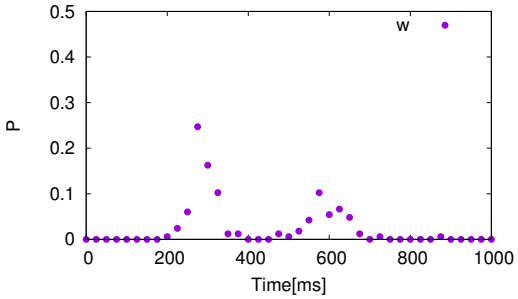


図 C.23: w

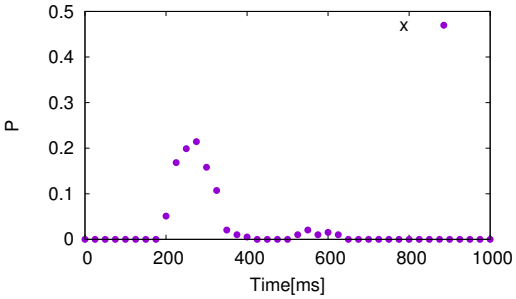


図 C.24: x

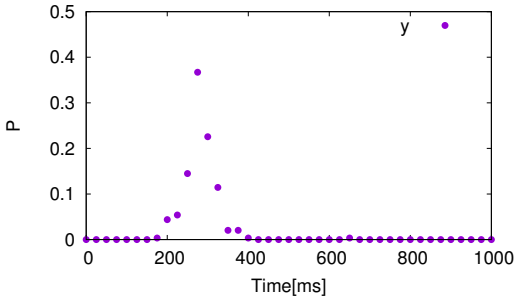


図 C.25: y

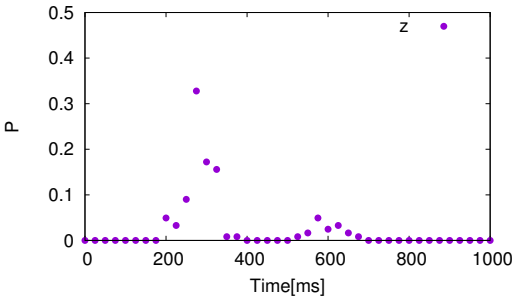


図 C.26: z

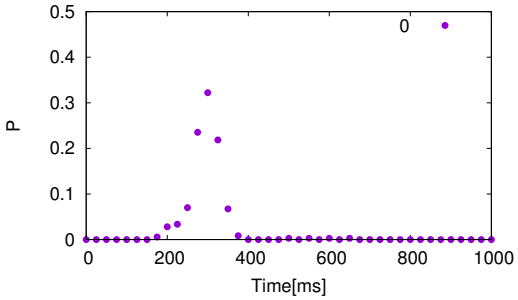


図 C.27: 0

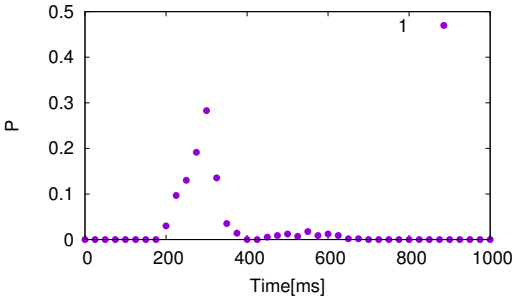


図 C.28: 1

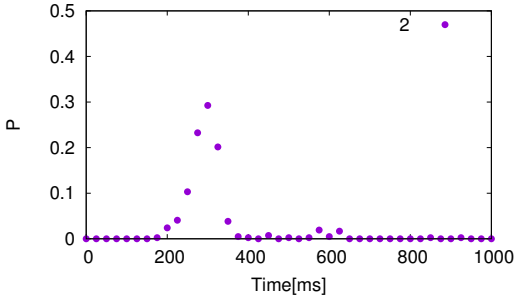


図 C.29: 2

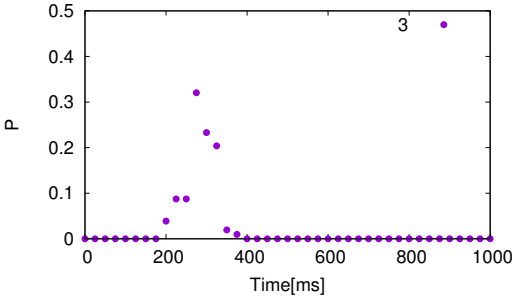


図 C.30: 3

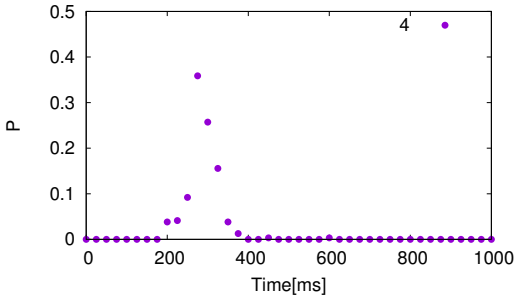


図 C.31: 4

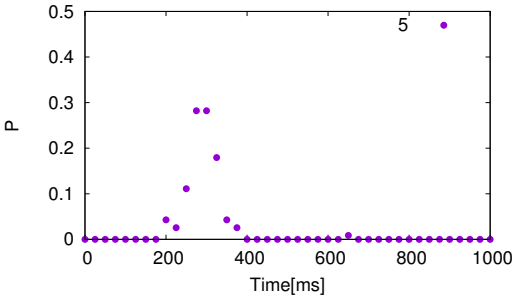


図 C.32: 5

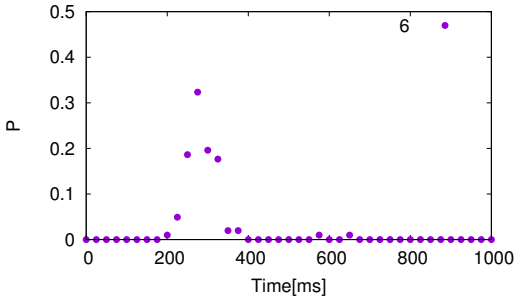


図 C.33: 6

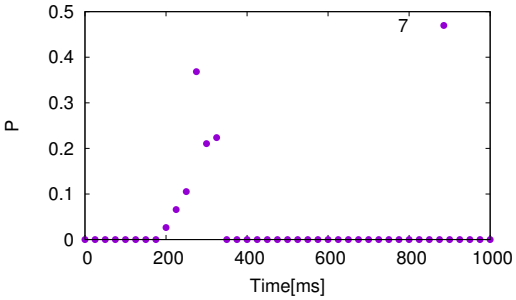


図 C.34: 7

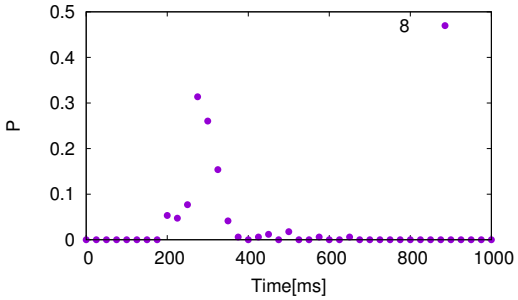


図 C.35: 8

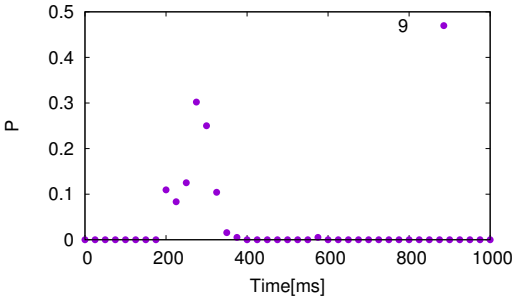


図 C.36: 9

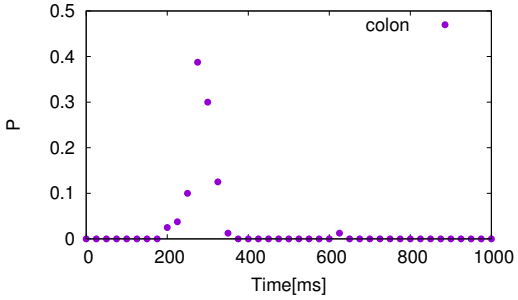


図 C.37: :

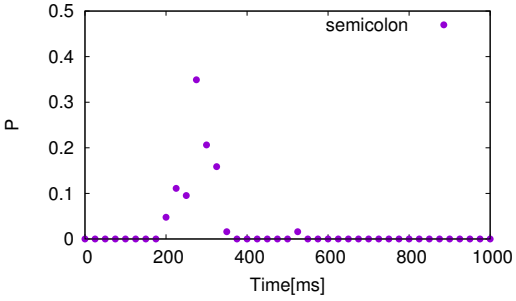


図 C.38: ;

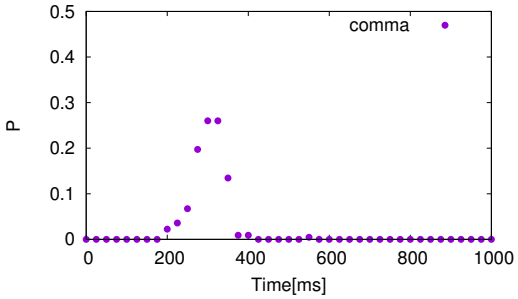


図 C.39: ,

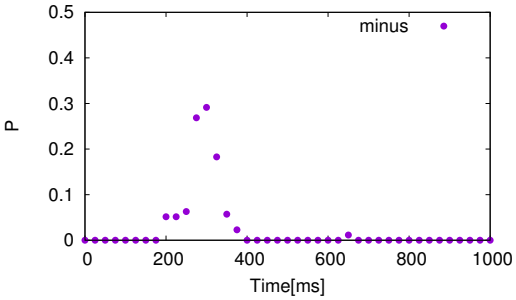


図 C.40: -

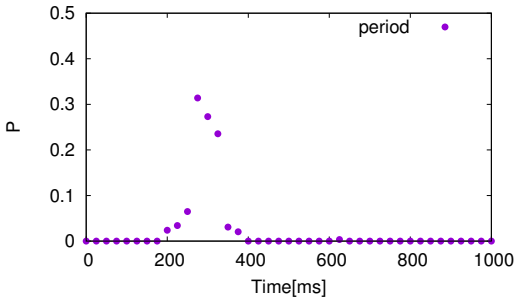


図 C.41: .

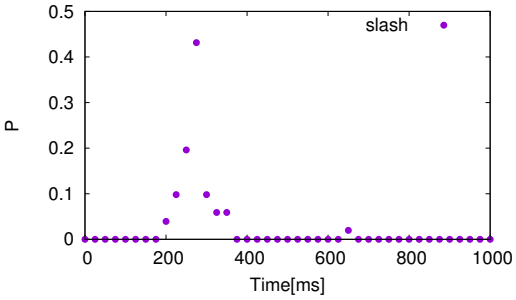


図 C.42: /

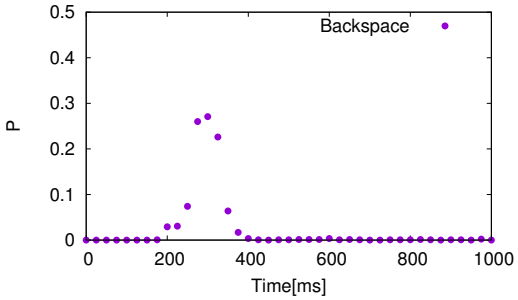


図 C.43: BackSpace

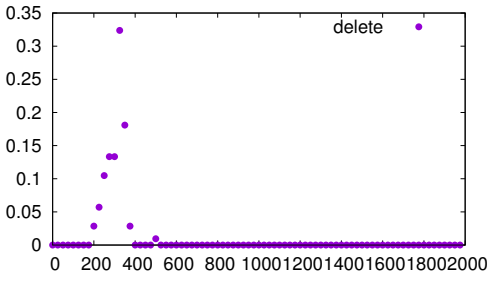


図 C.44: Delete

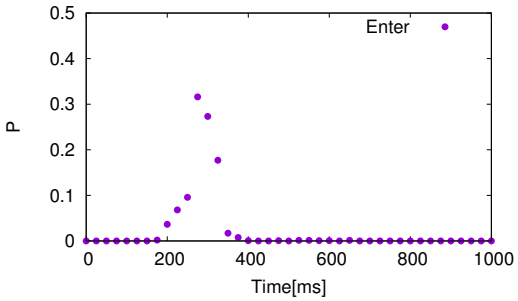


図 C.45: Enter

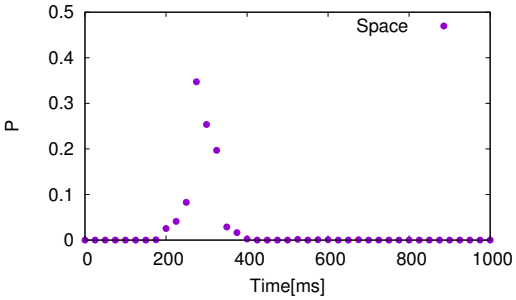


図 C.46: Space

C.2　ユーザー 02 の特徴量 KHT の頻度分布

比較のためにユーザー 02 のログデータから作成した特徴量 KHT の頻度分布を掲載する。

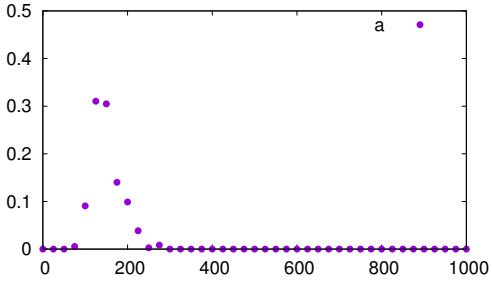


図 C.47: a

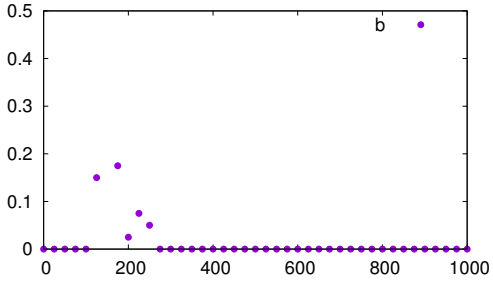


図 C.48: b

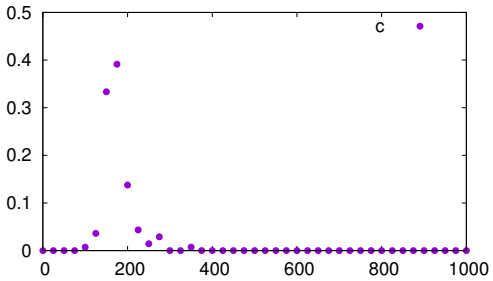


図 C.49: c

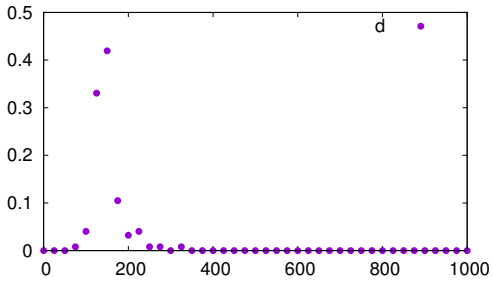


図 C.50: d

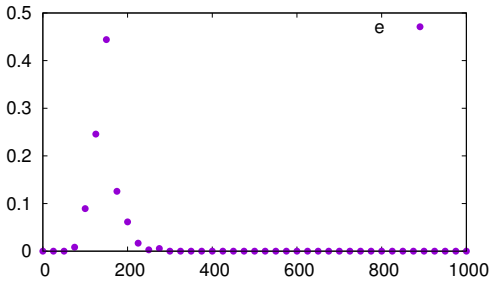


図 C.51: e

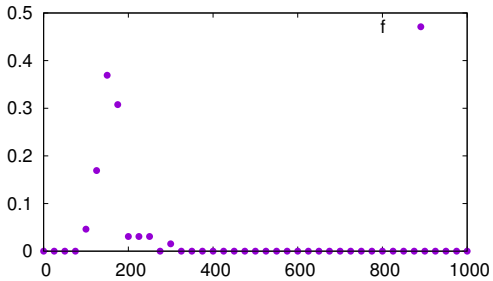


図 C.52: f

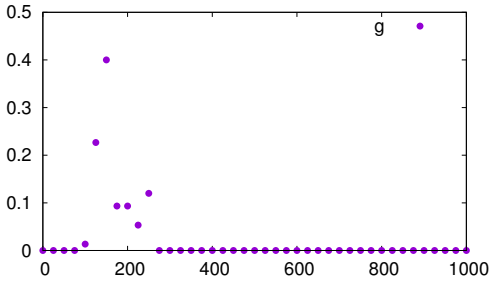


図 C.53: g

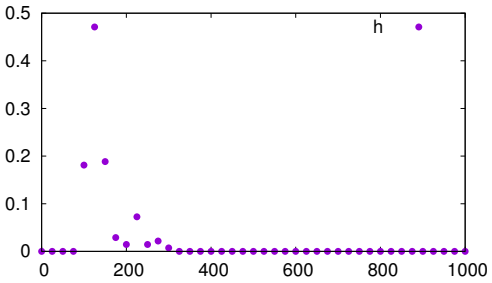


図 C.54: h

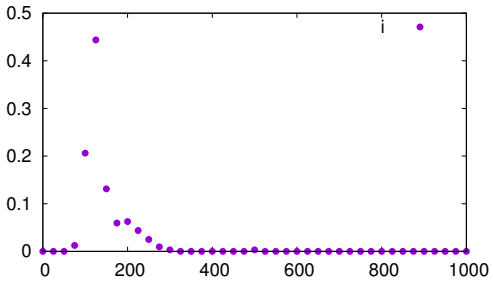


図 C.55: i

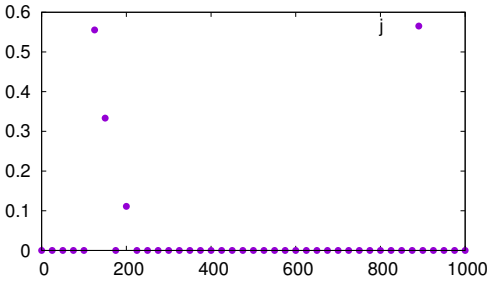


図 C.56: j

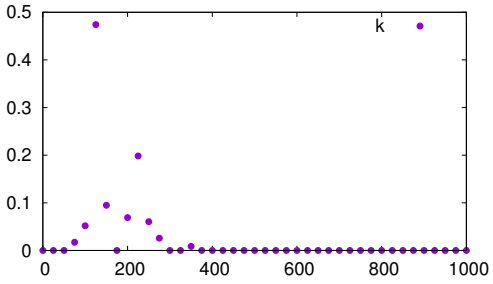


図 C.57: k

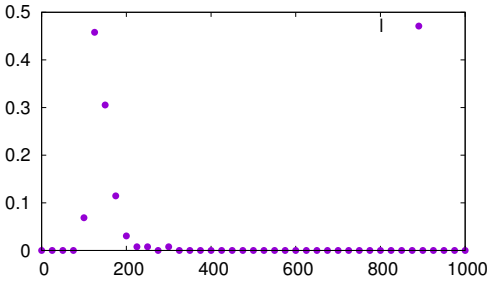


図 C.58: l

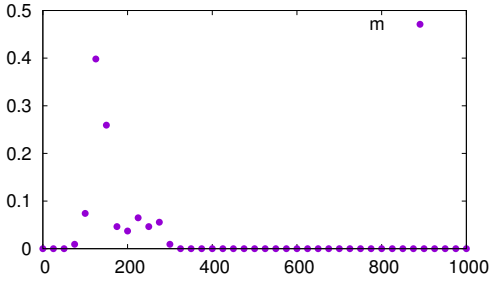


図 C.59: m

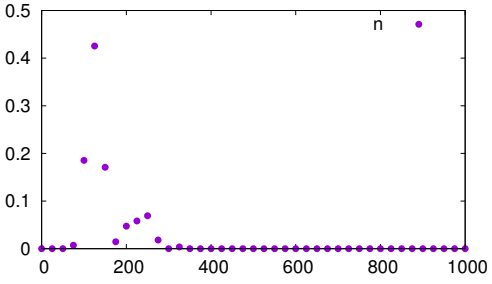


図 C.60: n

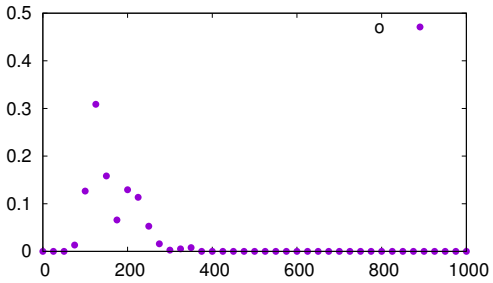


図 C.61: o

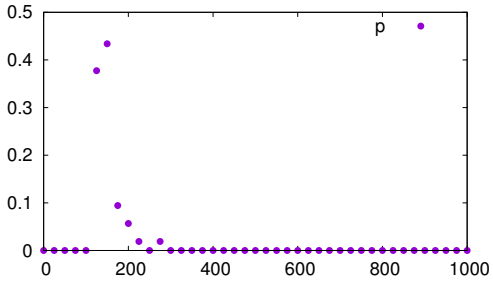


図 C.62: p

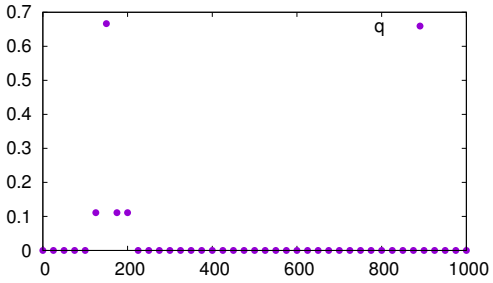


図 C.63: q

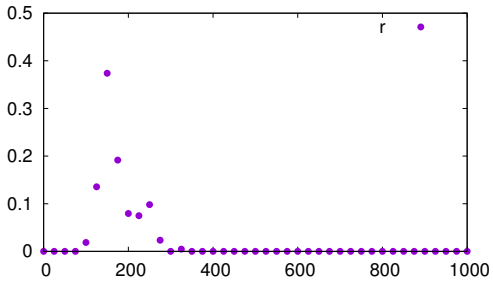


図 C.64: r

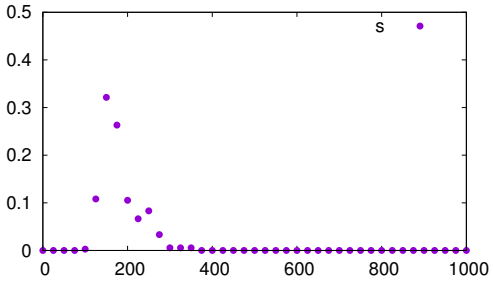


図 C.65: s

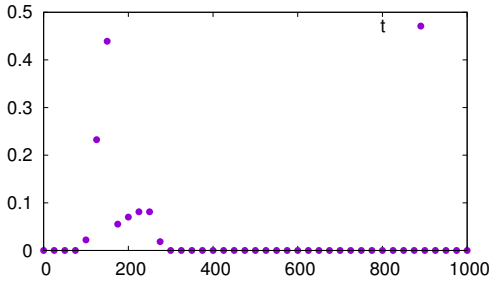


図 C.66: t

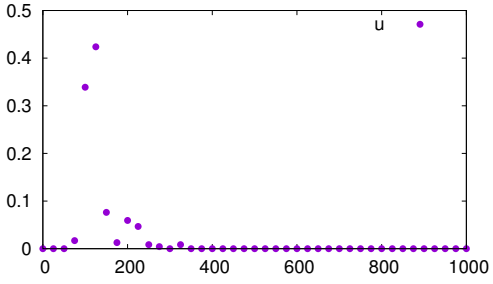


図 C.67: u

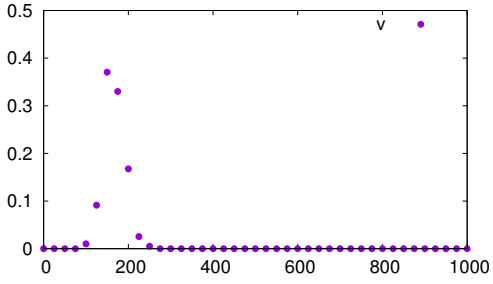


図 C.68: v

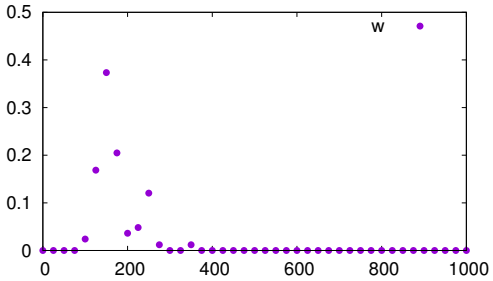


図 C.69: w

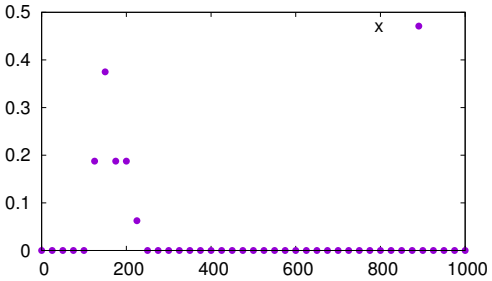


図 C.70: x

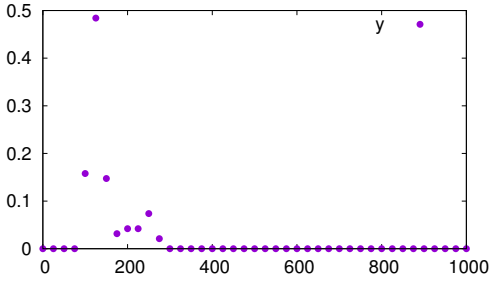


図 C.71: y

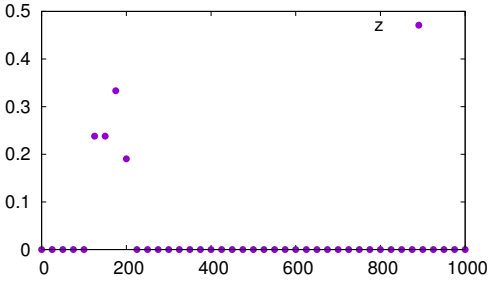


図 C.72: z

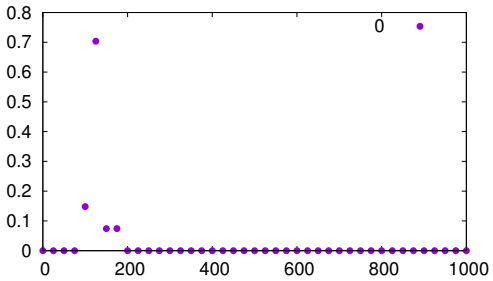


図 C.73: 0

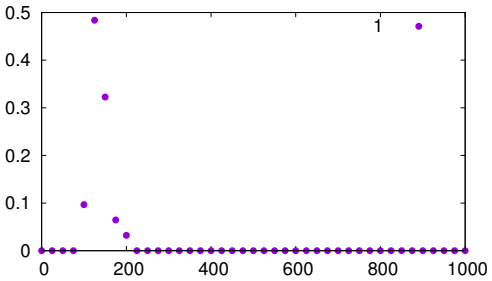


図 C.74: 1

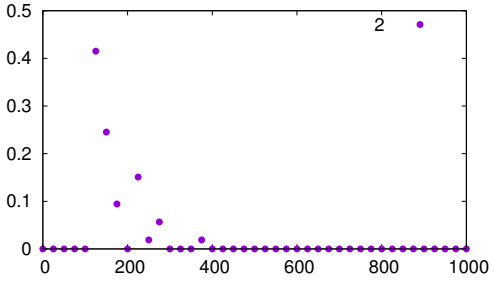


図 C.75: 2

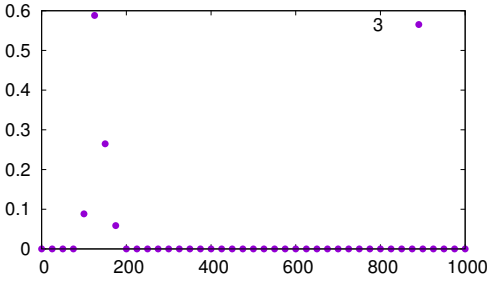


図 C.76: 3

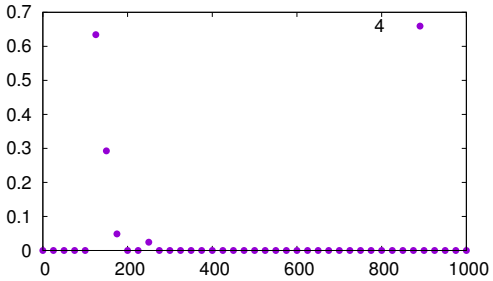


図 C.77: 4

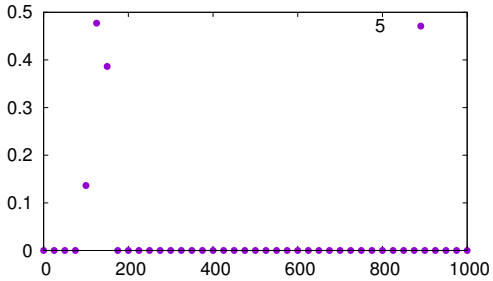


図 C.78: 5

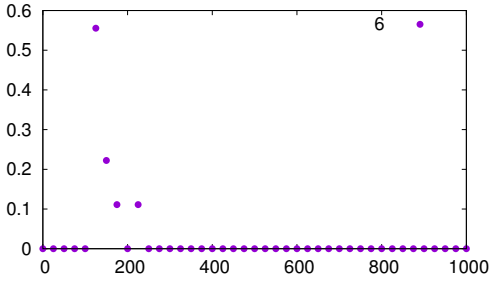


図 C.79: 6

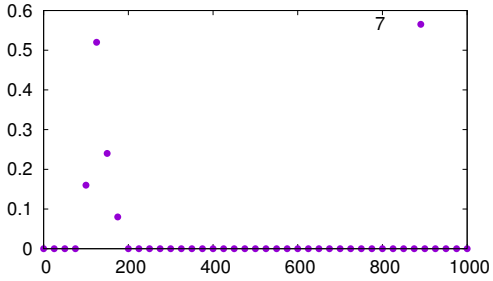


図 C.80: 7

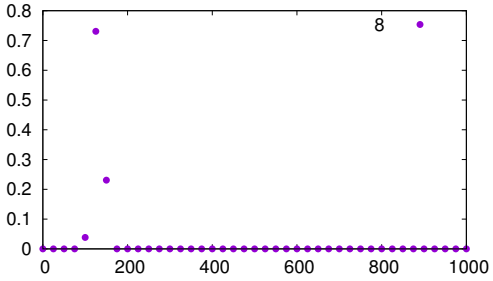


図 C.81: 8

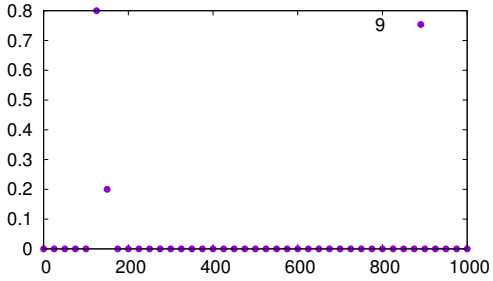


図 C.82: 9

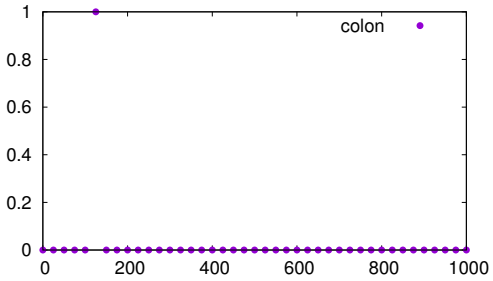


図 C.83: :

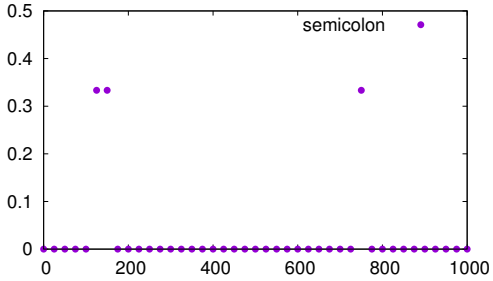


図 C.84: ;

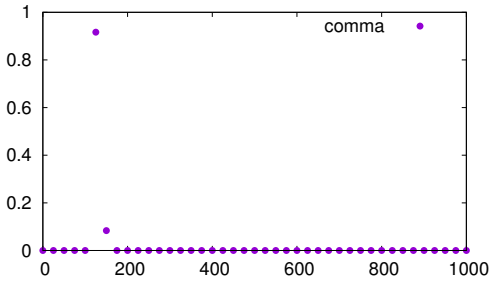


図 C.85: ,

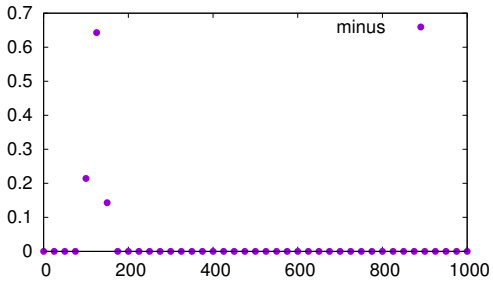


図 C.86: -

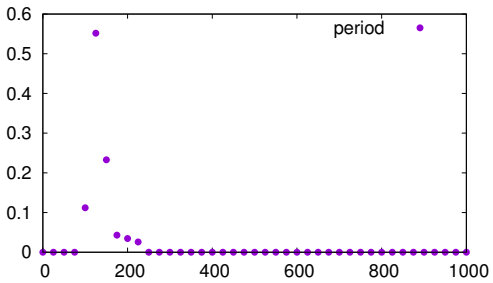


図 C.87: .

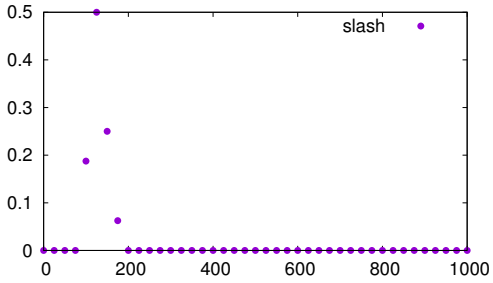


図 C.88: /

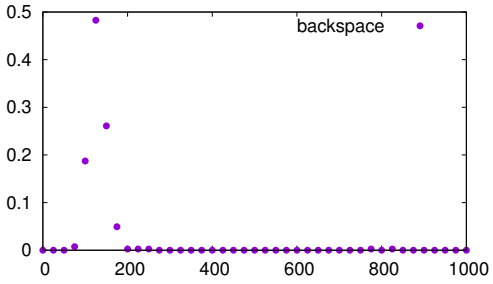


図 C.89: BackSpace

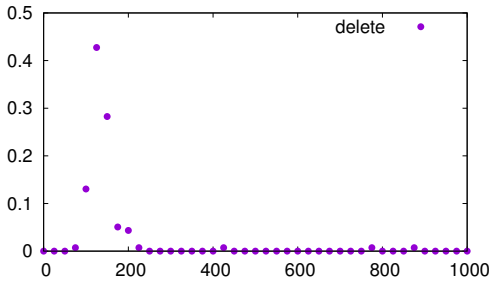


図 C.90: Delete

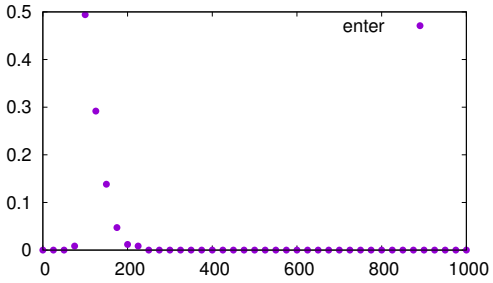


図 C.91: Enter

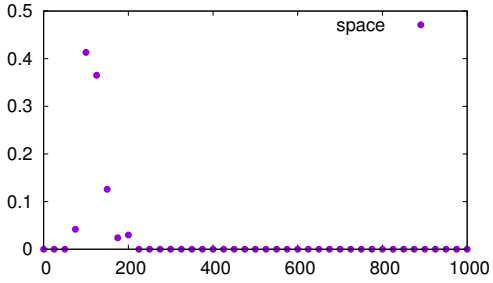


図 C.92: Space

付 録D　正規ユーザー02のTrust値Tの変化

D.1　DPTMにおけるユーザー02のTrust値Tの変化

以下は，ユーザー 02 のプロファイルを用いた DPTM の結果である．

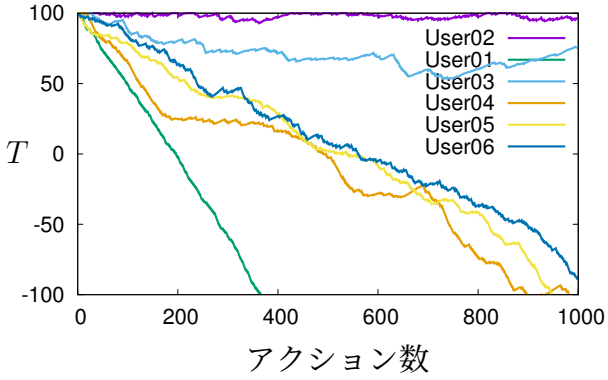


図 D.1: Trust 値の変化
（正規ユーザー 02，不正ユーザー 01，03〜06）

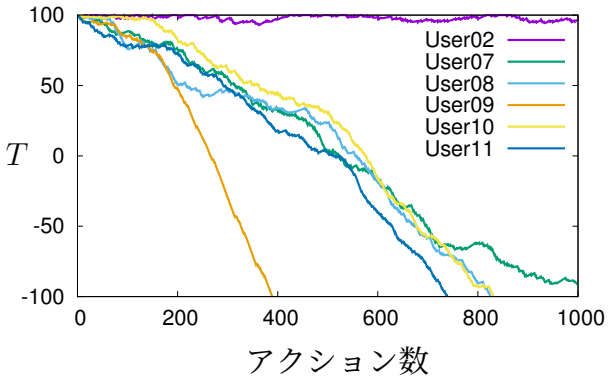


図 D.2: Trust 値の変化
（正規ユーザー 02，不正ユーザー 07〜11）

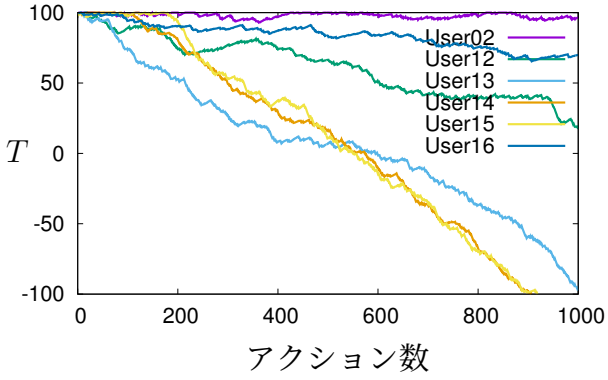


図 D.3: Trust 値の変化
（正規ユーザー 02，不正ユーザー 12〜16）

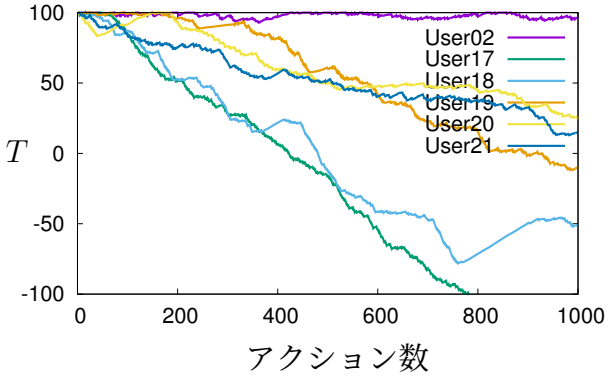


図 D.4: Trust 値の変化
（正規ユーザー 02，不正ユーザー 17〜21）

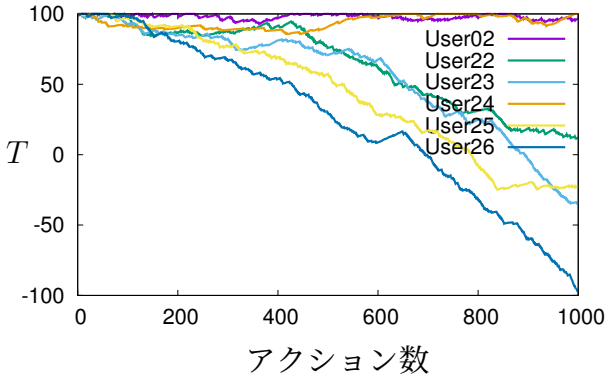


図 D.5: Trust 値の変化
（正規ユーザー 02，不正ユーザー 22〜26）

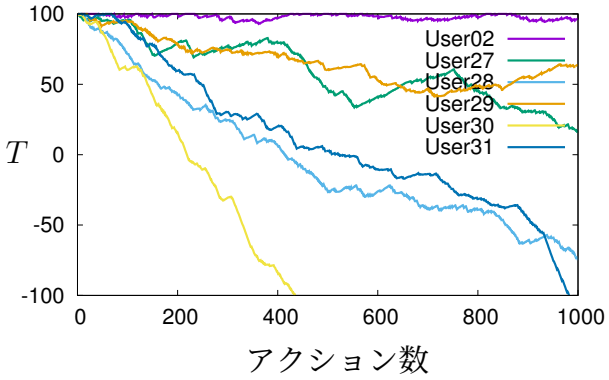


図 D.6: Trust 値の変化
（正規ユーザー 02，不正ユーザー 27〜31）

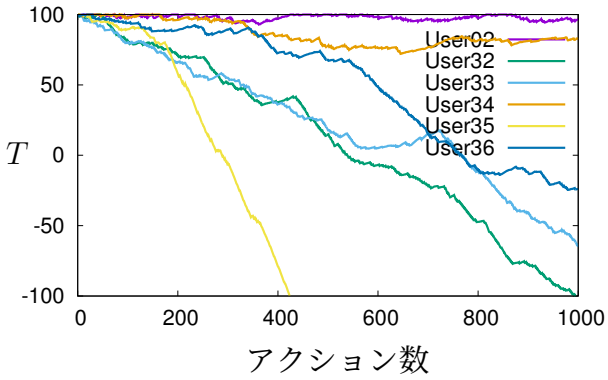


図 D.7: Trust 値の変化
（正規ユーザー 02，不正ユーザー 32〜36）

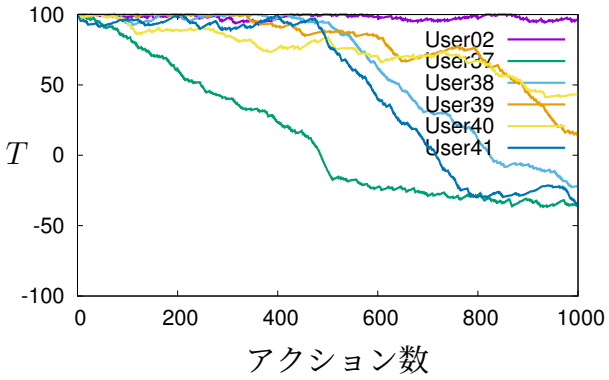


図 D.8: Trust 値の変化
（正規ユーザー 02，不正ユーザー 37〜41）

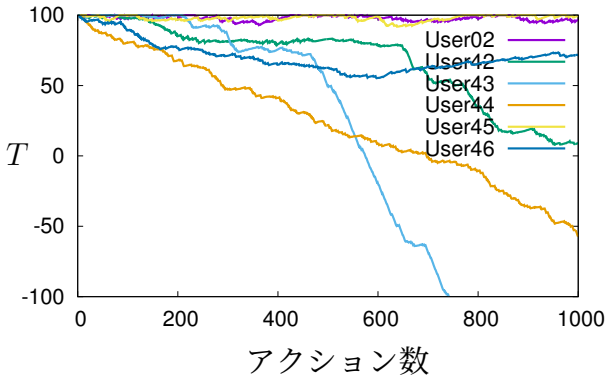


図 D.9: Trust 値の変化
（正規ユーザー 02，不正ユーザー 42〜46）

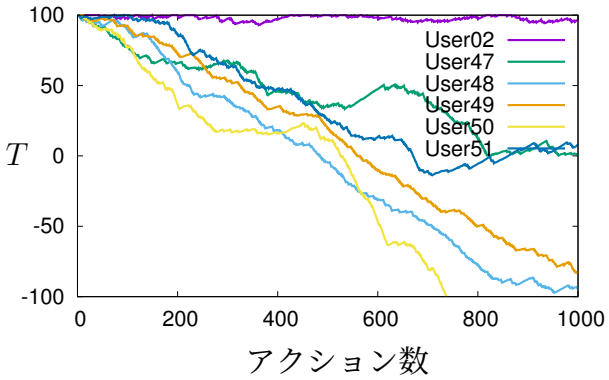


図 D.10: Trust 値の変化
（正規ユーザー 02，不正ユーザー 47〜51）

D.2　DTM におけるユーザー 02 の Trust 値 T の変化

以下は，ユーザー 02 のプロファイルを用いた DTM の結果である．

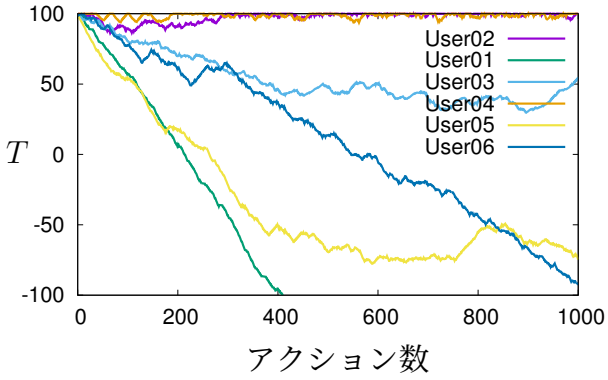


図 D.11: Trust 値の変化
（正規ユーザー 02，不正ユーザー 01，03〜06）

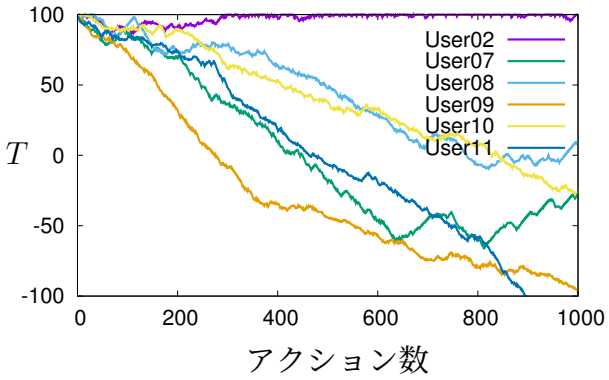


図 D.12: Trust 値の変化
（正規ユーザー 02，不正ユーザー 07〜11）

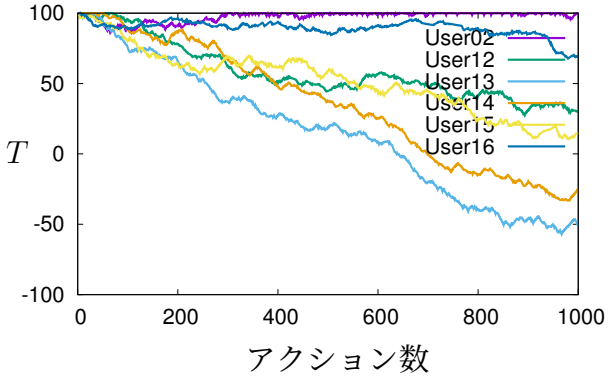


図 D.13: Trust 値の変化
（正規ユーザー 02，不正ユーザー 12〜16）

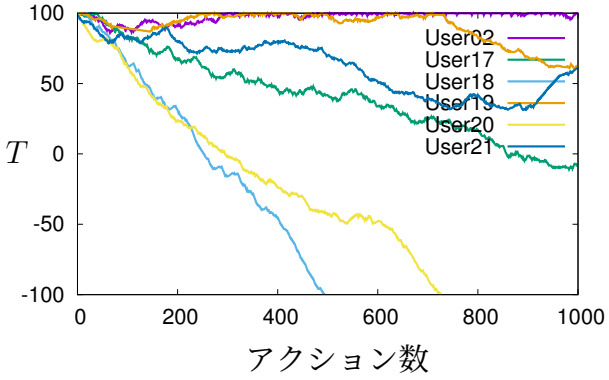


図 D.14: Trust 値の変化
（正規ユーザー 02，不正ユーザー 17〜21）

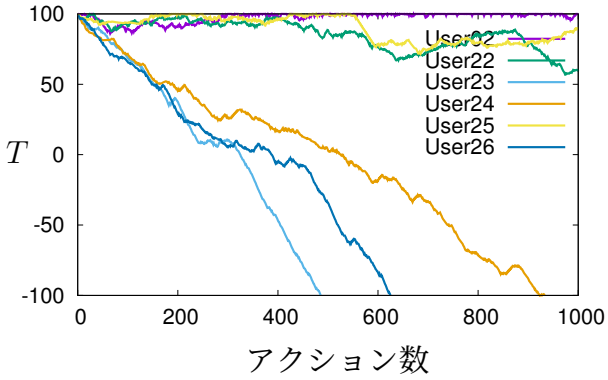


図 D.15: Trust 値の変化
（正規ユーザー 02，不正ユーザー 22〜26）

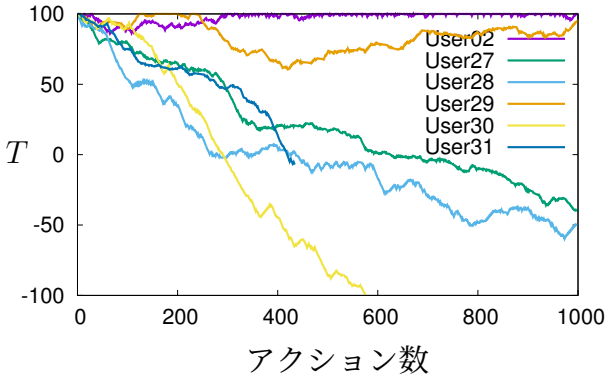


図 D.16: Trust 値の変化
（正規ユーザー 02，不正ユーザー 27〜31）

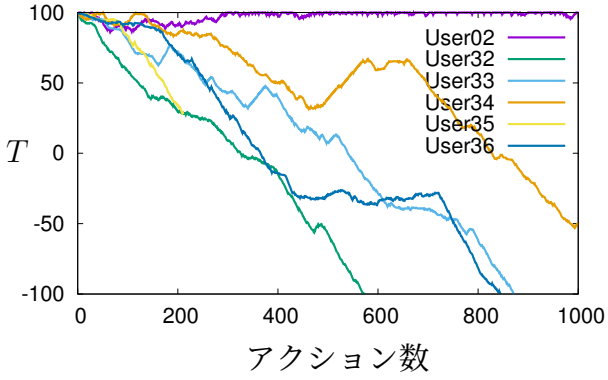


図 D.17: Trust 値の変化
（正規ユーザー 02，不正ユーザー 32〜36）

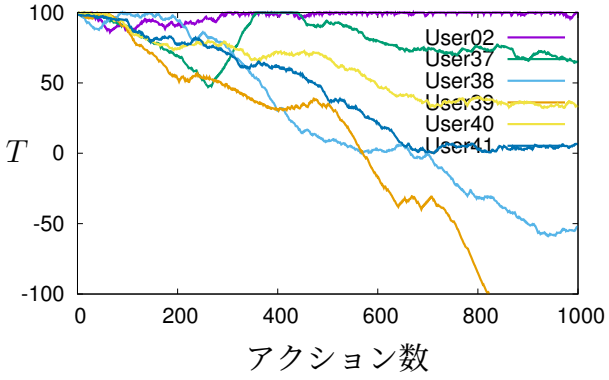


図 D.18: Trust 値の変化
（正規ユーザー 02，不正ユーザー 37〜41）

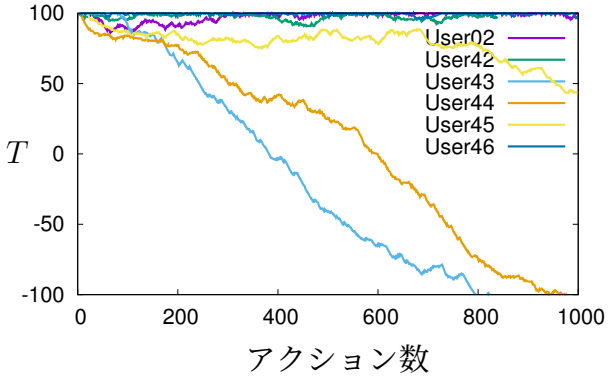


図 D.19: Trust 値の変化
（正規ユーザー 02，不正ユーザー 42〜46）

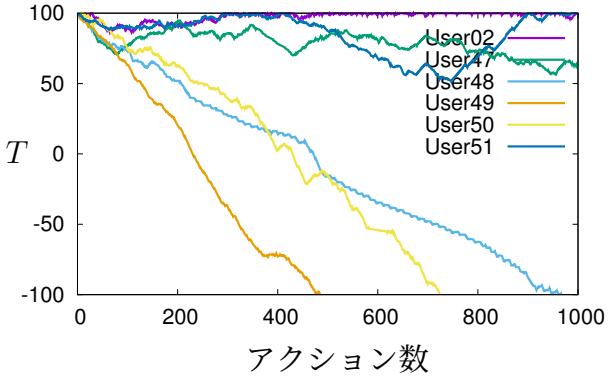


図 D.20: Trust 値の変化
（正規ユーザー 02，不正ユーザー 47〜51）

参考文献

[1] 警察庁，平成 30 年におけるサイバー空間をめぐる脅威の情勢等について，
http://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf

[2] D. Umphress, G. Williams, "Identity verification through keyboard characteristics", International Journal of Man-Machine Studies, vol.23, pp263-273, 1985.

[3] P. Ordal, D. Ganzhorn, D. Lu, W. Fong, J. Norwood, M. Scott, "Continuous identity verification through keyboard biometrics", Journal of Undergraduate Research, vol.4, pp20-24, 2005.

[4] P. Dowland, and S. Furnell, "A long-term trial of keystroke profiling using digraph, trigraph and keyword latencies", Security and Protection in Information Processing Systems, vol.147, pp.275-289, 2004.

[5] N. Harun, W.L. Woo, S.S. Dlay, "Performance of keystroke biometrics authentication system using artificial neural network (ANN) and distance classifier method", International Conference on Computer and Communication Engineering, ICCCE'10, 2010.

[6] M. Kaur, R. Virk, "Security System Based on User Authentication Using Keystroke Dynamics", Ijarcce.Com, vol.2, pp2111-2117, 2013.

[7] A. Alsultan, K. Warwick, H. Wei, "Non-conventional keystroke dynamics for user authentication", Pattern Recognition Letters, vol.89, pp53-59, 2017

[8] Charles C. Tappert, Sung-Hyuk Cha, Mary Villani, and Robert S. Zack, "A keystroke biometric system for long-text input", International Journal of Information Security and Privacy, vol.4, pp32-60, 2010.

[9] J.V. Monaco, N. Bakelman, S.H. Cha, C.C. Tappert, "Developing a keystroke biometric system for continual authentication of computer users", Proceedings - 2012 European Intelligence and Security Informatics Conference, EISIC 2012, vol.1, pp210-216, 2012.

[10] Y. Zhong, Y. Deng, A.K. Jain, "Keystroke dynamics for user authentication", Computer Vision and Pattern Recognition Workshops (CVPRW), 2012 IEEE Computer Society Conference, pp117-123, 2012.

[11] J. Monaco, N. Bakelman, S. Cha, C. Tappert, "Recent advances in the development of a long-text-input keystroke biometric authentication system for arbitrary text input", Proceedings - 2013 European Intelligence and Security Informatics Conference, EISIC 2013, pp60-66, 2013.

[12] A. Darabseh, A. Namin, "On Accuracy of Classification-Based Keystroke Dynamics for Continuous User Authentication", Proceedings - 2015 International Conference on Cyberworlds, CW 2015, pp.321-324, 2016.

[13] R. Giot, M. El-Abed, B. Hemery, C. Rosenberger, "Unconstrained keystroke dynamics authentication with shared secret", Computers and Security, vol.30, pp.427-445, 2011.

[14] D. Stefan, X. Shu, D. Yao, "Robustness of keystroke-dynamics based biometrics against synthetic forgeries", Computers and Security, vol.31 pp.109-121, 2012.

[15] A. Darabseh, A.S. Namin, "On accuracy of keystroke authentications based on commonly used English words", Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI), 2015.

[16] P. Kobojek, K. Saeed, "Application of Recurrent Neural Networks for User Verification based on Keystroke Dynamics", Journal of Telecommunications and Information Technology, pp80-90, 2016.

[17] P. Baynath, K.M.S. Soyjaudah, M.H.M. Khan, "Keystroke recognition using chaotic neural network", Proceedings - 3rd Iranian Conference on Signal Processing and Intelligent Systems, ICSPIS 2017, pp59-63, 2018

[18] Y. Deng, Y. Zhong, "Keystroke Dynamics User Authentication Based on Gaussian Mixture Model and Deep Belief Nets", Hindawi Publishing Corporation ISRN Signal Processing, 2013.

[19] P.S. Teh, S. Yue, A.B.J. Teoh, "Improving keystroke dynamics authentication system via multiple feature fusion scheme", Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012, pp277-282, 2012.

[20] X. Lu, S. Zhang, S. Yi, "Continuous authentication by free-text keystroke based on CNN and RNN", Procedia Computer Science, vol.147, pp.314-318, 2019.

[21] N. Zheng, A. Paloski, H. Wang, "An efficient user verification system via mouse movements", Proceedings of the 18th ACM conference on Computer and communications security - CCS '11, pp.139, 2011.

[22] B. Sayed, I. Traore, I. Woungang, M. Obaidat, "Biometric authentication using mouse gesture dynamics", IEEE Systems Journal, vol.7, pp.262-274, 2013.

[23] C. Feher, Y. Elovici, R. Moskovitch, L. Rokach, A. Schclar, "User identity verification via mouse dynamics", Information Sciences, vol.201, pp.19-36, 2012.

[24] H. Jagadeesan, M.S. Hsiao, "A novel approach to design of user re-authentication systems", IEEE 3rd International Conference on Biometrics: Theory, Applications and Systems, BTAS 2009, 2009.

[25] K. Bailey, J. Okolica, B. Peterson, "User identification and authentication using multi-modal behavioral biometrics", Computers and Security, vol.43, pp.77-89, 2014.

[26] S. Mondal, P. Bours, "Combining keystroke and mouse dynamics for continuous user authentication and identification", ISBA 2016 - IEEE International Conference on Identity, Security and Behavior Analysis, 2016.

[27] A. Messerman, T. Mustafic, S.A. Camtepe, S. Albayrak, "Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics", 2011 International Joint Conference on Biometrics, IJCB 2011, 2011.

[28] H. Saevanee, N.L. Clarke, S.M. Furnell, "Multi-modal behavioural biometric authentication for mobile devices", IFIP Advances in Information and Communication Technology, pp465-474, 2012.

[29] I. Traore, I. Woungang, M.S. Obaidat, Y. Nakkabi, I. Lai, "Combining mouse and keystroke dynamics biometrics for risk-based authentication in web environments", Proceedings - 4th International Conference on Digital Home, ICDH 2012, pp138-145, 2012.

[30] I. Traore, I. Woungang, M. Obaidat, Y. Nakkabi, I. Lai, "Online risk-based authentication using behavioral biometrics", Multimedia Tools and Applications, 2014.

[31] A. Alsultan, K. Warwick, "User-friendly free-text keystroke dynamics authentication for practical applications", Proceedings - 2013 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2013, pp4658-4663, 2013.

[32] M. Rybnik, M. Tabedzki, M. Adamski, K. Saeed, "An exploration of keystroke dynamics authentication using non-fixed text of various length", Proceedings - 2013 International Conference on Biometrics and Kansei Engineering, ICBAKE 2013, pp245-250, 2013.

[33] E. Vural, J. Huang, D. Hou, S. Schuckers, "Shared research dataset to support development of keystroke authentication", IJCB 2014 - 2014 IEEE/IAPR International Joint Conference on Biometrics, 2014.

[34] M.L. Ali, J.V. Monaco, C.C. Tappert, M. Qiu, "Keystroke Biometric Systems for User Authentication", Journal of Signal Processing Systems, vol.86, pp175-190, 2017

[35] P. Kang, "The effects of different alphabets on free text keystroke authentication: A case study on the Korean-English users", Journal of Systems and Software, vol.102, 2015.

[36] J. Kim, H. Kim, P. Kang, "Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection", Applied Soft Computing Journal, vol.62, 2018.

[37] A. Alsultan, K. Warwick, H. Wei, "Free-text keystroke dynamics authentication for Arabic language", IET Biometrics, vol.5, 2016.

[38] J. Huang, D. Hou, S. Schuckers, S. Upadhyaya, "Effects of text filtering on authentication performance of keystroke biometrics", 8th IEEE International Workshop on Information Forensics and Security, WIFS 2016, 2017.

[39] E. Ivannikova, G. David, T. Hamalainen, "Anomaly detection approach to keystroke dynamics based user authentication", Proceedings - IEEE Symposium on Computers and Communications, 2017.

[40] J. Huang, D. Hou, S. Schuckers, "A practical evaluation of free-text keystroke dynamics", 2017 IEEE International Conference on Identity, Security and Behavior Analysis, ISBA 2017, 2017.

[41] L. Xiaofeng, Z. Shengfei, Y. Shengwei, "Continuous authentication by free-text keystroke based on CNN plus RNN", Procedia Computer Science, vol.147, pp314-318, 2019.

[42] H. Saevanee, N. Clarke, S. Furnell, V. Biscione, "Continuous user authentication using multi-modal biometrics", Computers and Security, vol.53, pp234-246, 2015.

[43] R. Doroz, P.Porwik, H.Safaverdi, "Person Verification Based on Keystroke Dynamics", Journal of Medical Informatics and Technologies, vol. 24, pp.39-44, 2015.

[44] C. Wu, W. Ding, R. Liu, J. Wang, A.C. Wang, J. Wang, S. Li, Y. Zi, Z.L. Wang, "Keystroke dynamics enabled authentication and identification using triboelectric nanogenerator array", Materials Today, vol.21, pp216-222, 2018.

[45] S. Venugopalan, F. Juefei-Xu, B. Cowley, M. Savvides, "Electromyograph and keystroke dynamics for spoof-resistant biometric authentication", IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp.109-118, 2015.

[46] S. Eberz, K.B. Rasmussen, V. Lenders, I. Martinovic, "Evaluating behavioral biometrics for continuous authentication: Challenges and metrics", ASIA CCS 2017 - Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security, pp386-399, 2017.

[47] S. Mondal, P. Bours, "A study on continuous authentication using a combination of keystroke and mouse biometrics", Neurocomputing, vol.230, pp.1-22, 2017.

[48] S.P. Banerjee, D. Woodard, "Biometric Authentication and Identification Using Keystroke Dynamics: A Survey", Journal of Pattern Recognition Research, vol.7, pp116-139, 2012.

[49] P.H. Pisani, A.C. Lorena, A. De Carvalho, "Adaptive approaches for keystroke dynamics", Proceedings of the International Joint Conference on Neural Networks, 2015

[50] P. Bours, "Continuous keystroke dynamics: A different perspective towards biometric evaluation", Information Security Technical Report, vol.17, pp.36-43, 2012

[51] S. Mondal, P. Bours, "A computational approach to the continuous authentication biometric system", Information Sciences, vol.304, pp28-53, 2015.

[52] S. Mondal, P. Bours, "Context independent continuous authentication using behavioural biometrics", 2015 IEEE International Conference on Identity, Security and Behavior Analysis, ISBA 2015, 2015

[53] S. Mondal, P. Bours, "Continuous Authentication in a real world settings", ICAPR 2015 - 2015 8th International Conference on Advances in Pattern Recognition, 2015.

研究業績

- 論文（査読有）
  - 山田猛矢，福元伸也，鹿嶋雅之，佐藤公則，渡邊睦，”キー操作とマウス操作の動的バイオメトリクスを用いた継続認証アルゴリズム DPTM の提案と認証精度”，電子情報通信学会論文集，Vol. J103-A，No.11，(2020.11).

- 国際学会（査読有）
  - T. Yamada, W. Motoyama, S. Fukumoto, M. Kashima, K. Sato, M. Watanabe, ”Proposal of DPTM Algorithm for Continuous Authentication Using Probability Distribution”, 2018 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing（NCSP2018）, proc. of NCSP2018, pp.463-466, (2018.3).

- 国際学会（査読無）
  - T. Yamada, W. Motoyama, S. Fukumoto, M. Kashima, K. Sato, M. Watanabe, ”Application of Keystroke and Mouse Dynamics Biometrics to Continuous Authentication Using DPTM Algorithm”, International Conference on Functional Materials and Applications 2017 (ICFMA2017), proc. of ICFMA2017, pp.1-4, (2017.12).

- 口頭発表
  - 山田猛矢, 福元伸也, 鹿嶋雅之, 佐藤公則, 渡邊睦，”キー操作とマウス操作の動的バイオメトリクスを用いた継続認証アルゴリズム DPTM の提案と認証精度”，第 8 回バイオメトリクスと認識・認証シンポジウム（SBRA2018），S4-17，pp.89-90，(2018.11).
  - 山田猛矢, 福元伸也, 鹿嶋雅之, 佐藤公則, 渡邊睦, ”キー操作とマウス操作の動的バイオメトリクスを用いた継続認証アルゴリズム DPTM の提案”, 電子情報通信学会技術研究報告, Vol.118, No.219, PRMU2018-42, pp.41-46, (2018.9).

– 山田猛矢, 元山航, 福元伸也, 鹿嶋雅之, 佐藤公則, 渡邊睦，”キー操作とマウス操作の動的バイオメトリクスを用いた継続認証に関する研究”，第 7 回バイオメトリクスと認識・認証シンポジウム（SBRA2017），S4-3，pp.80-81，(2017.11).

謝辞

本論文をまとめるにあたり，多くの皆様にご指導を賜りました．この場を借りてお礼申し上げます。本当にありがとうございました．

29 才の時に鹿児島大学大学院理工学研究科博士後期課程生命物質システム専攻を中途退学し，その後，第一工業大学で勤務しながら研究を続けていくつもりが，日常業務に追われ，大した成果も出せずにいる中，学生時代の恩師である秦浩紀先生に 40 才の時，再び博士後期課程に社会人として受け入れていただきました．秦先生，ありがとうございました。その後，紆余曲折あり，工学の世界へ分野変更を行うこととなり，その際，快く引き受けてくれた佐藤公則先生，ありがとうございました．また，佐藤先生が東京工科大学へ移動となるとき，快く引き受けてくれた渡邊睦先生，ありがとうございます。研究に関する多くのご指導，ご助言を賜りましたことに，心より感謝申し上げます．

また，第一工業大学の先生方にも大変お世話になりました．ありがとうございました．特に，福永知哉先生には学生時代から大変お世話になっています．本論文作成中も様々なことを手伝っていただき，また心の支えになってくれたことを心より感謝申し上げます．次は福永先生の手番です．待望の手番が回ってきましたが，どう攻めますか？
また，実験に協力してくれた第一工業大学の学生の皆さんにも感謝いたします．ありがとうございました．

最後に，一番感謝を伝えたい幸恵さん，太郎さん，素直さん，真生さん，ありがとうございます。ダメダメ父ちゃんでごめんなさい．いろいろと迷惑をかけてますが，みんなのおかげでやっとここまで辿り着いたという感じです．本当にありがとうございます．またこれまで経済的に支えてくれた力さん，玲子さん，ありがとうございました．あと，研究時間を作ってくれたマムシさん，ありがとうございました．

関わってくれた全ての方々に心より感謝申し上げます．本当にありがとうございました．これまでに得てきた知識，技術，経験を今後の教育研究活動に有効に活用したいと考えております．今後ともよろしくお願い申し上げます．