5ZA-07

継続的打鍵情報を用いたサーバ操作中のなりすまし検出

滝本　将司†　　納富　一宏†

神奈川工科大学大学院工学研究科†

1. はじめに

情報化社会が進み情報端末の普及と同時に，不正アクセスによる情報セキュリティに関する問題も増加している．そのため，従来に比べてセキュリティ対策は重要な課題であるといえる．

こうした状況の中，近年では低コストで実現が可能であることとその汎用性の高さの面から，いまだにパスワード認証が用いられるケースが多い．しかしながら，従来型のパスワード認証方式では一度何らかの方法で突破されてしまうと，その後の第三者の悪用を防ぐことはできないものがほとんどである．そのため，重要な情報を扱うサーバ管理においては，不正アクセスに対する対策はより重要なものであるといえる．

そこでパスワード認証における不正アクセス防止のため，サーバなどの重要なシステムの操作時には継続的に個人認証を行う必要があると考えられる．しかし，継続的個人認証を行う場合，ユーザに対して頻繁にパスワード入力などが必要となるため，ユーザの負担が大きくなることが想定される．ゆえに，ユーザの意識を必要としない認証方法が望ましいといえる．そこで著者らは，重要な情報を管理するサーバ操作の場面を想定し，コマンド入力から得られるキーストローク情報を用いた継続的な個人認証を行うことで，第三者のなりすまし防止を目的とするシステムの開発を行っている**エラー！参照元が見つかりません。**[2]．本稿では，打鍵情報（キーストローク）による継続的個人認証において，他人によるなりすまし操作のシミュレーション実験を行った結果となりすまし検出精度について述べる．また本提案手法の有効性について考察する．

2. 実験 1

先行研究[4]では，認証精度実験を行う際，図 1 のように，5 名のデータを登録用データとし，投入データをその登録した者の中から利用した．実験 1 では，図 2 に示すように，登録者以外のデータを投入データとして利用する．

Impersonation detection method during server operation using continuous keystroke sequence
Masashi Takimoto†, Kazuhiro Notomi†
†Dept. of Kanagawa Institute of Technology Graduate school
Shimo-ogino 1030, Atsugi, Kanagawa, 243-0292, Japan

登録者以外のデータが投入された場合についても正解となる判定を行えるかについて実験を行う．

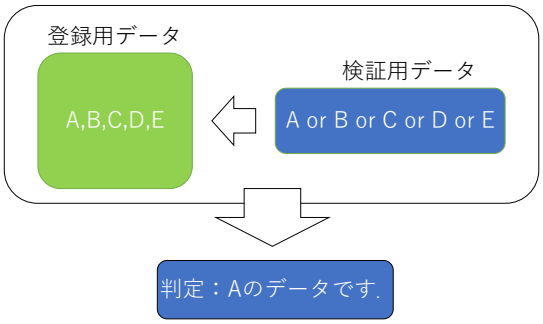

図 1 先行研究[4]で利用したデータ

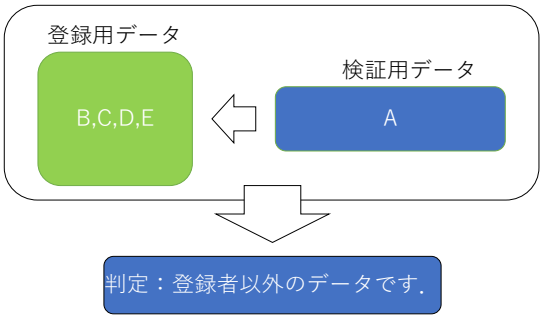

図 2 実験 1 に利用するデータ

2.1. 判定精度

判定手法は先行研究[4]同様に，登録用データ内の同一人物間のユークリッド距離と不同人物間のユークリッド距離の中間点を閾値として利用し，閾値を超えた場合に登録者以外のデータであるとの判定を行う．また，5 人の内 1 人のデータを登録用データから除き，登録者以外のデータとして検証用の投入データに利用する．5 人それぞれのデータを投入データとした場合の検出率を表 1 に示す．

表 1 登録者外データの検出率

データ	検出率	閾値
A	0.00	0.054
B	0.00	0.055
C	0.40	0.055
D	1.00	0.054
E	0.00	0.056
平均	0.28	0.055

精度結果は，データによって大きくバラつきがでており，平均して 28%という結果となっていた．

2.2. 閾値設定による精度の推移

閾値を 0.05，0.04，0.03 の 3 パターンに設定し，3 つの設定された閾値において，登録者内のデータと登録者以外のデータを投入データに利用した場合の判定正解率と検出率を図 3 および表 2 にそれぞれ示す．

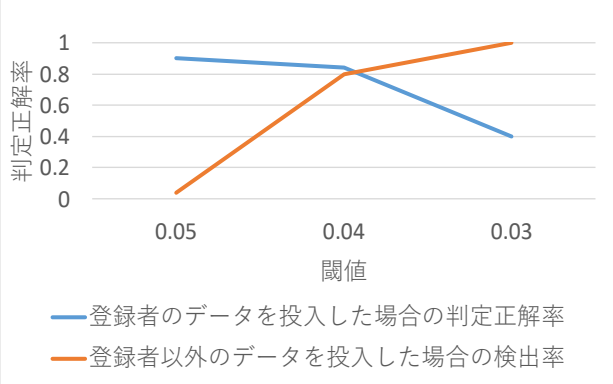

図 3 判定正解率と検出率の推移

表 2 判定正解率と検出率

投入データ		閾値
登録者内	登録者外	
0.90	0.04	0.05
0.84	0.80	0.04
0.40	1.00	0.03

3. 実験 2

先行研究[4]の手法では，登録者内のデータの判定正解率は高い値であるが，登録者以外のデータの場合では大幅に精度を低下させてしまっていた．そこで，登録者内のデータと登録者外のデータを投入データとした場合，両方のデータでの精度を向上させるため，先行研究[4]の閾値の設定方法に修正を加え，登録者内のデータと登録者外のデータを投入データとした場合の精度計算を行う．閾値は，登録用データの同一人物間のユークリッド距離の平均を利用する．結果を表 3 に示す．

表 3 精度結果

データ	判定正解率	検出率	閾値
A	0.60	0.80	0.040
B	0.40	0.80	0.043
C	0.60	0.85	0.040
D	1.00	0.85	0.044
E	0.80	0.95	0.044
平均	0.68	0.85	0.042
平均	0.765		

結果は，登録者のデータを投入データとした場合で 68%，登録者外の場合で 85%，平均して 76.5%という結果であった．

4. 考察

閾値が 0.05，0.04，0.03 の場合のみで精度の計算を行った結果，0.04 の場合では，登録者内と登録者外の平均で 82%の精度が確認された．また，さらに閾値を細かくしたとき，閾値が 0.04 の場合より精度が向上するケースが考えられる．そのため，実験 2 の精度結果では平均で 76.5%となっているが，閾値の調整次第では，82%以上の精度が期待できることが考えられる．

5. まとめ

本稿では，他人によるなりすまし操作のシミュレーションを行い，なりすまし検出精度について実験を行った．先行研究[4]で利用した手法の場合では，登録者内のデータであれば高い判定精度が確認されたが，登録者外のデータでは検出率を大幅に下げてしまう結果となっていた．しかし，閾値の設定方法に修正を加えた場合では，精度を向上させることができ，継続的個人認証に利用可能な値が得られる結果となった．また，今後の課題は，閾値設定の最適化手法の検討と，さらなる精度向上である．

参考文献

[1] 梶原 礼, 河合博之, 納富一宏:"サーバ操 作時の打鍵情報による継続的な個人認証手 法の検討", 情報処理学会 第 79 回全国大 会講演論文集 第 3 分冊，3W-03, pp.569-570，(2017.03).

[2] 滝本将司, 納富一宏, 斎藤恵一:サーバ操作時のキーストローク情報による継続的個人認証, バイオメディカル・ファジィ・システム学会, (2017-11)

[3] 滝本将司, 納富一宏, 斎藤恵一:"サーバ操作時の継続的個人認証 -キーストロークを使用した自己組織化マップによる-", 情報処理学会 第 80 回全国大会講演論文集 第 3 分冊，3W-05, pp.503-504，(2018.03).

[4] 滝本将司, 納富一宏:"継続的個人認証を用いたサーバ操作中の不正侵入検出手法", バイオメディカル・ファジィ・システム学会 第 31 回年次大会講演論文集, pp.53-56, (2018.11).