3W-05

サーバ操作時の継続的個人認証
-キーストロークを用いた自己組織化マップによる-

滝本　将司†　　納富　一宏†　　斎藤　恵一‡

神奈川工科大学情報工学科†　　国際医療福祉大学大学院医療福祉学研究科‡

1. はじめに

情報化社会が進んだ現在，多くの人々がパソコンやスマートフォンなどの端末を所持することが多くなっている．平成 29 年版の総務省の白書によると 2016 年時点での日本国内における情報通信端末の世帯保有率の割合がスマートフォンの場合では 71.8%，パソコンの場合では 73.0%となっている[1]．

こうした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となり，様々な対策が検討・実施されている[2]．

近年では顔認証や指紋認証といった生体認証が用いられる場合が増えてきているが，低コストで実現が可能であることとその汎用性の高さから，いまだにパスワード認証が多く用いられている．しかし，従来のパスワード認証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[3]．そのため，重要な情報を扱うサーバ管理において，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．

そこでセキュリティ向上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が，現在の認証方法は 1 度認証を行ったユーザに対して再度認証を要求するものは少なく[4]，大抵の場合，認証は 1 度しか行われない．したがって，継続的な個人認証を実現する場合，サーバ操作を行うユーザに対して頻繁にパスワード入力などの認証のための動作（操作）を要求することになってしまう．ゆえにその負担を軽減するため「ユーザが意識せずに認証を行える方法」を執ることが利便性の観点から重要であるといえる．そこで本研究では行動的特徴量となる生体情報を用いた個人認証手法の検討を行っている[4],[5]．具体的にはキーボードの打鍵動作から得られるキーストローク情報のうちタイミングとしての打鍵間隔時間を用いる．この理由は，例えば顔認証のように外部デバイスとなるカメラ装置等を別途追加する必要もなく，最小限のハードウェアのみで十分であるため扱いが容易であり，その分コスト面でも有利であるためである．

こうした背景から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，第三者の成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[4],[5]．本稿では継続的個人認証の実現可能性について検討した結果を報告する．

2. 継続的個人認証

2.1.概要

現在想定している継続的個人認証システムは，あらかじめ登録用のコマンドをいくつか用意し，サーバからのコマンド入力とその登録されているコマンドが一致した場合に，自己組織化マップ（Self-Organizing Maps: SOM）によって作成されたマップを介して照合することで，継続的個人認証を行っていくものである．

2.2.継続的個人認証システム

継続的個人認証の概要を図 1 に示す．図 1 では，8 つのコマンドを登録済みとしており，さらにそのコマンドごとに SOM によって学習されたマップをコマンドそれぞれが持っている状態を表している．また，図中の網掛け部分は個人認証が行われる期間，すなわち「認証可能（既登録）コマンド実行区間」を表し，逆に，個人認証が行われていない期間，すなわち「認証不能（未登録）コマンド実行区間」を表し，各時間を Δt_n としている．

具体的な例で考えると，最初に ls コマンドが入力された場合，ls コマンドは登録済みのコマンドとして用意されているので学習済みの SOM マップを介して照合することが可能である．このようにサーバ操作を行っている間，登録済みのコマンドと入力されたコマンドが一致した場合，照合を繰り返すことで継続的個人認証を行っていくことが可能となる．

Continuous personal authentication during server operation-Based on self-organizing map using keystrokes-

Masashi Takimoto†, Kazuhiro Notomi† and Keiichi Saito‡

†Dept. of Information and Computer Sciences, Kanagawa Institute of Technology

Shimo-ogino 1030, Atsugi, Kanagawa, 243-0292, Japan

‡Graduate School of Health and Welfare Sciences, International University of Health and welfare

サーバ操作中に行われる照合回数は登録されているコマンド数に影響される．そのため，登録されているコマンド数が少なければ，認証不能時間も増えることが考えられる．サーバ操作中に行われるコマンド入力が，未登録のコマンドであった場合，そのコマンドの実行区間は認証不能となる．この認証不能の時間が小さければ問題ないが，未登録のコマンド入力が続いてしまった場合，認証不能時間は大きくなってしまい，その間まったく認証が行われないので，継続的個人認証として問題が生じてしまうことが想定される．そこで，継続的に認証を行えるようにするため，次の認証が行われるまでの Δt_n が，小さくなるようにする必要がある．

コマンド入力による継続認証処理を図 **2** に示す．

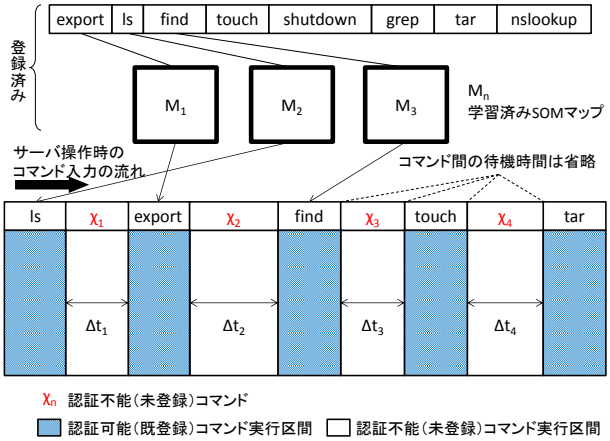

図 1　継続的個人認の概要

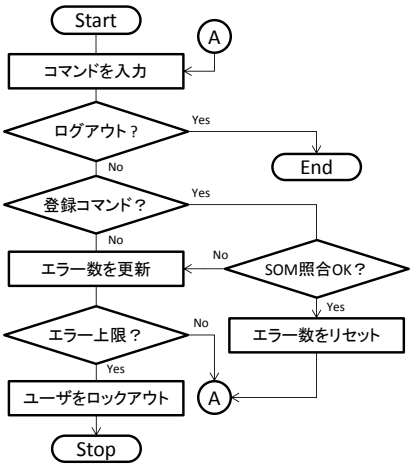

図 2　コマンド入力による継続認証処理

3. コマンド入力による個人認証

サーバ操作時に使用するコマンドの打鍵情報から認証精度を求める検証実験を行った[5]．コマンドを入力文字数の多いものから少ないものまでの 8 種類をピックアップし，キーロガーを用いてそのコマンドの入力から打鍵情報の取得を行った．得られた打鍵情報を元に SOM によってコマンドごとのマップの作成を行い，作成されたマップからコマンドそれぞれの認証精度を求めた．その結果コマンド入力から得られる打鍵情報を利用した場合，75.70%の認証精度があることがわかった．またその内，最も精度が良かったもので 85.06%の認証精度が得られた．

実験の結果，入力文字数の少ないサーバ操作用のコマンド入力を利用した場合でも個人認証として用いることが十分可能であることがわかった．8 種類のコマンドの認証精度の結果を表 1 に示す．

表 1　認証精度結果一覧[5]

No.	入力コマンド	認証精度
1	touch test.txt	85.06%
2	ls -a -l	84.48%
3	find -mtime 0	79.67%
4	export	75.84%
5	shutdown -r +60	74.99%
6	grep -i ab sample.txt	73.73%
7	tar tf tar_file	71.05%
8	nslookup kanagawa-it.ac.jp	60.79%

本稿では，継続的個人認証を行うにあたり認証不能区間の問題について述べた．現在はサーバ操作中に一定の間隔で行われる個人認証がどの程度の時間範囲内で行われる必要があるのか検証する予定である．

また，本研究では継続的個人認証に用いるサーバ操作用のコマンド入力から得られる打鍵情報から認証精度を求めた．その結果，個人認証としての利用可能性が示唆された．今後はこのサーバ操作用のコマンドを利用し，継続的個人認証を行うことで，本人のなりすましの有無を判定するシステムの完成と実証実験による動作検証を行う．

参考文献

[1] 総務省：総務省｜平成 29 年版 情報通信白書｜平成 29 年版　情報通信白書のポイント，http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/na000000.html，(2017-10-11).

[2] 山田健一郎，納富一宏，斎藤恵一：スマートフォン操作時における行動的特徴量を利用した個人に識別手法，バイオメディカル・ファジィ・システム学会，(2014-4).

[3] 中田明秀，小高知宏，白井治彦，黒岩丈介：ユーザのコマンド履歴を用いた Adaboost による認証手法改善の試み，福井大学 大学院工学研究科 研究報告，第 63 巻，pp.87-95，(2015-3).

[4] 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).

[5] 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)