3W-03

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

梶原 礼† 河合 博之† 納富 一宏†
神奈川工科大学†

1 はじめに

情報化社会になった現在では，多くの人々がパソコンや携帯電話などの通信電子機器を利用し，インターネットに接続している．インターネットを使う際に重要な点として，情報セキュリティ対策が挙げられる．これを怠ってしまった場合，コンピュータ・ウイルスの感染や不正アクセス等による被害を受けてしまう[1]．このような被害を抑えるためには，本人と悪意のある第三者を見分ける本人認証技術の確立が重要である．

本人認証技術の分類としては，パスワードなど本人の記憶情報による認証，身分証明書や IC カードなどの所持情報による認証，人間一人一人が固有に持つ生体情報を用いた認証に大別される．現在，パソコンなどの端末を利用する際には，パスワード認証による本人認証が多く用いられている．しかし，パスワードによる認証方法には，忘却や盗み見による盗難の問題点がある．そのため，近年では，人間の生体情報を用いた生体認証が注目されている．

生体認証は認証者本人の身体的特徴を鍵とするため，パスワード認証のように忘却や盗難の心配がない．また，生体的特徴以外だけでなく，個人の習慣による行動を使った認証も生体認証に分類される．生体認証は今までの認証方法より，本人である場合高い精度で認証することができ，生体情報を模倣することが難しいためなりすましや推測が困難な利点がある．

しかし，これまでに挙げてきた認証システムは端末を使用するはじめの一回だけ入力することが多い．一回だけの認証では，認証後の利用者が端末の持ち主本人かどうか分からない問題がある．はじめに本人が端末を使用するため認証を行った後，第三者がその端末を使っているときでもそれを検出することができない．したがって第三者が悪意を持った攻撃者であった場合，データの盗難，改ざんの被害に遭ってしまう可能性も考えられる．

この問題を解決するには，端末の利用中でもリアルタイムで継続的に認証をする必要がある．これを継続認証と呼ぶ．継続認証を実現するには利用者が能動的にデータを提示するのではなく，無意識の状態でデータが取得されなければならない．逐一本人を確認する認証手法が安全性を高められるので望ましいと考えられるが，利用者の利便性を損ねる欠点もあるため，継続認証のシステムが少ないというのも現状である．

そこで，本研究では利用者が入力したコマンド打鍵時の時間情報を鍵とする手法を提案する．この手法は利用者の癖を特徴とするため，侵入者は正当な利用者の癖を真似することが困難であると考えられる．本手法は，事前に利用者が入力したコマンド打鍵の情報を特徴点として登録し，打鍵時の情報と比較することで認証を行う[2]．今回我々は，サーバ操作時を想定し，その時に使用する UNIX コマンドを打鍵情報とした継続認証の検証実験を実施した．その結果を報告する．

2 実験

2.1 実験方法

被験者は日常的にパソコンを使っている 20 代の男性 10 名である．サーバ管理によく用いられる UNIX コマンド 4 種類を 1 人 10 回連続で打鍵してもらう．打鍵した文字の押した時間と離した時間の時間データを記録し，そのデータを打鍵時の間隔データとして分析を行う．また，4 つ全てを 1 纏りとして分析をする．コマンドを打鍵する UNIX コマンドを表 1 に示す．

表 1 実験用 UNIX コマンド

1	ps aux | grep nginx
2	netstat –antp
3	vmstat 1 -w
4	top -d

2.2 実験結果

まず始めに，各被験者の打鍵のばらつきを見るために標準偏差を求めた．各被験者の標準偏差のグラフを図 1 に示す．グラフの縦軸が標準偏差，横軸が回数である．

Study on Continuous Personal Authentication Method with Key-stroking Features for Server Operation
Hiromu Kaziwara†, Hiroyuki Kawai†, Kazuhiro Notomi†
†Kanagawa Institute of Technology
Shimo-ogino 1030, Atsugi, Kanagawa, 243-0292, Japan

Copyright ©2017 Information Processing Society of Japan.
All Rights Reserved.

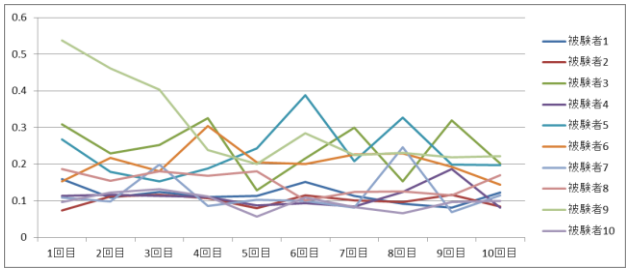

図 1　標準偏差のグラフ

2.3　偏差平方和による分析

2.3.1　分析方法

被験者の時間データを偏差平方和に計算し分析を行う．偏差平方和は，平均値と各データの差の平方の和から求める．被験者 1 人の 10 回分の偏差平方和の平均値から，被験者ごとの 1 回目から 10 回目の偏差平方和の差から最小値を求める．一番小さい最小値が求まった被験者を一番打鍵の特徴が似ている被験者とする．

2.3.2　分析結果

実験より，10 人中 9 人が同じ被験者の中から最小値が検出された．偏差平方和による実験結果を表 2 に示す．

表 2　偏差平方和による分析の結果

被験者	最小値を持った被験者	最小値
被験者 1	被験者 1	0.007
被験者 2	被験者 2	0.005
被験者 3	被験者 3	0.007
被験者 4	被験者 8	0.014
被験者 5	被験者 5	0.024
被験者 6	被験者 6	0.021
被験者 7	被験者 7	0.005
被験者 8	被験者 8	0.010
被験者 9	被験者 9	0.040
被験者 10	被験者 10	0.003

2.4　自己組織化マップによる分析

2.4.1　分析方法

実験で求めた時間データを自己組織化マップで分析する．マップサイズ 30×30，50×50，70×70 の 3 種類を各 5 回，学習用データ 5 回分，検証用データ 5 回分，学習回数は全て 60,000 回でマップを作成した．次に，認証精度の評価方法には，本人拒否率（FRR：False Reject Rate）と，他人受容率（FAR：False Accept Rate）を用いた[3].

2.4.2　分析結果

オプションなしの場合とありの場合を比較した．オプションなしの場合を表 3，ありの場合を表 4 に示す．

表 3　認証精度結果(オプションなし)

マップ	閾値	FAR[%]	FRR[%]	認証精度[%]
30×30	9.5	29.1	33.2	68.85
50×50	17	32.1	32.0	67.95
70×70	23.5	32.8	31.2	68.00

表 4　認証精度結果(オプションあり)

マップ	閾値	FAR[%]	FRR[%]	認証精度[%]
30×30	9.5	26.5	26.8	73.35
50×50	16	26.7	24.8	74.25
70×70	22.5	26.9	27.2	72.95

2.5　考察

検証実験より，2 つの方法で分析を行った結果，偏差平方和による分析では 90%の認証精度であり，自己組織化マップによる分析では全体で平均すると約 70%の認証精度であった．偏差平方和による分析では，90%の精度であったが，最小値 1 つだけで決める方法なので，今回のように被験者 4 のときに被験者 8 となってしまうことが考えられる．自己組織化マップによる分析では，オプションありとオプションなしで比較した場合オプションありの時のほうが，認証精度が上がった．単純にオプションありのほうが，データ数が多いので正確な分析ができたと考えられる．

3　まとめ

今回我々は打鍵情報による継続認証手法を提案するため，検証実験をおこなった．その結果，個人のコマンドの打鍵時の時間情報で違いが表れた．今後の課題として，あるコマンドが打鍵されたら打鍵間隔のデータ，回数、頻度などを自動で記録し，個人の打鍵コマンドモデルを作成する．そのモデルを作成することで，長い期間自動でデータを蓄積することができ，継続認証をする際にも蓄積されたコマンドデータを利用して継続認証が可能であると考えられる．コマンドに付与するオプションも個人ごとに特徴が表れるデータであるので，そのデータを記録することでより特徴が表れるため認証精度も高くなると考えられる．

参考文献

[1] 中村行弘，横田翔著：事例から学ぶ情報セキュリティ：基礎と対策と脅威のしくみ，技術評論社(2015).

[2] 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).

[3] 野口敦弘，高橋雅隆，納富一宏，齋藤恵一：自己組織化マップを用いたキーストローク認証手法の提案―覗き見によるなりすまし評価―，FIT2011 講演論文集，第 4 分冊，L-27，pp237-238(2011).

Copyright ©2017 Information Processing Society of Japan.
All Rights Reserved.