L-018

行動的特徴を利用した認証システムへのなりすまし攻撃に関する考察
A Study of Spoofing Attacks on Authentication Systems Based on User Behavior Patterns

池田 美穂† 長谷川 慶太† 工藤 史堯† 川邊 秀樹† 大田 幸由†
Miho Ikeda Keita Hasegawa Fumiaki Kudo Hideki Kawabe Yukiyoshi Ota

1. はじめに

個人の動作の加速度，位置情報等の行動的特徴を示すデータを測定できるデバイスの普及により，行動的特徴を個人認証に利用する研究が進められている[1][2]．行動的特徴は時間経過等により変化するため，認証で本人でも拒否されて利便性が低下する可能性がある．この課題を解決するために，本人の行動的特徴を学習し，認証システムに登録されている行動的特徴の情報（登録された情報をテンプレートと呼ぶ）を継続して更新する方法が考えられる[3]．

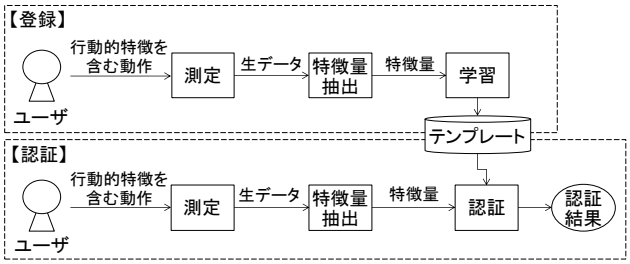
安心・安全な認証システムを実現するには，設計段階からセキュリティ対策を組み込むことが重要である．例えば，なりすまし攻撃で狙われる可能性のある脆弱性を把握し，技術的対策を施して攻撃耐性を高めることが求められる．

本稿では，行動的特徴を利用する認証システムのセキュリティの確保に向けて，脅威分析を試行し，当該システムへのなりすましの攻撃シナリオとその技術的対策を検討した．また，身体的特徴のテンプレートと比較して，行動的特徴のテンプレートとその生成に特有の課題を考察する．

2. 行動的特徴を利用する認証システムの想定

想定した行動的特徴を利用する認証システムのプロセス図を図 1 に示す．認証システムは，センサで測定した行動的特徴を含むデータから特徴量を抽出して学習することでテンプレートを生成する．この手順を学習対象のデータが発生する毎に実施することでテンプレートを更新する．また，認証時の特徴量（以下，認証データと記す）とテンプレートとを照合することで認証を実施する．

本稿では，この認証システムを，ユーザがスマートフォンを利用して web サイトへアクセスするときの個人認証に用いると想定し，スマートフォンで測定と特徴量抽出，サーバで学習，認証とテンプレートの保管を行うものとした．



※テンプレートは、学習した特徴量と認証の判断ポリシ（閾値等）を含むことを想定。

図 1 行動的特徴を利用する認証システムのプロセス図

3. 関連研究

行動的特徴を利用する認証システムの安全性の評価には，身体的特徴を利用する認証システムの指標が適用できると考えられる．例えば，センサに対して何らかの情報を提示してなりすましを試みる攻撃(Presentation Attack)のセキュリティ評価手法が，国際標準化機構(ISO)から発行されている（ISO/IEC 30107 シリーズ）．また，テンプレートを更新して他人受入を起こしやすいテンプレート(Lamb)に少しずつ変える Frog-Boiling Attack が指摘されている[4]．

†NTT セキュアプラットフォーム研究所

4. 脅威分析の手順

本稿では，想定した認証システムの脅威分析を，脅威モデリングの手法を用いて以下の手順で実施した．まず，図 1 を基に，データフローダイアグラムを作成した．次に，データフローダイアグラムに基づき，各データ・各プログラムにおける脅威を，STRIDE[5]や情報セキュリティの CIA（完全性・機密性・可用性）の観点を参考に抽出・分類した．抽出した脅威を基に，なりすまし攻撃のアタックツリーを作成して脅威を評価した．

5. 脅威分析の結果と考察

5.1 なりすまし攻撃の全体像

想定した認証システムに対するなりすまし攻撃のアタックツリーの概略を図 2 に示す．なお，図 2 で分岐の終端にある事象（脅威）には，実際には下位の事象（脅威または脆弱性）が続くことに留意を要する．また，図 2 の(1)-(6)は，後述する表 1 の番号に対応し，関連があることを示す．

なりすまし攻撃は，行動的特徴を用いる認証システムと身体的特徴を用いる認証システムとで基本的には共通であるが，(6)に関しては以下の差異があると考えられる．

(6)配下のテンプレートの改竄の脅威は，身体的特徴より行動的特徴のテンプレートで発生しやすいと考えられる．テンプレートの改竄に繋がる箇所は，脅威分析から，テンプレートの DB，テンプレートの生成に関係するプログラムまたはデータ，が抽出される．後者が継続して改竄されると Frog-Boiling Attack が実現する．身体的特徴の場合は，例えばテンプレートを複数用いるとき(Multiple Templates)，身体的特徴の永続性に着目して登録・更新許容範囲を設定することで，テンプレートの不正更新を防止できると考えられる．一方，行動的特徴の場合は，変化の速さや幅等が個人で異なるため，そのような設定が困難であり，特に不正データ（本人以外のデータ等）の学習によるテンプレートの不正更新が起こる可能性が高まると考えられる．

5.2 なりすましの攻撃シナリオと狙われる脆弱性

図 2 を基に，想定した認証システムへのなりすましの攻撃シナリオと攻撃で狙われる認証システムの脆弱性を整理したものを表 1 に示す．なお攻撃シナリオは，偽装の手間や回数等が少ないと思われる順で記載している．

なりすまし攻撃で狙われる脆弱性の箇所は，学習・認証の機構（(1),(5),(6)），認証システムの用法（(2)-(4)）に分類できる． 5.1 で指摘したように，(6)は学習機構の脆弱性が原因と考えられる．

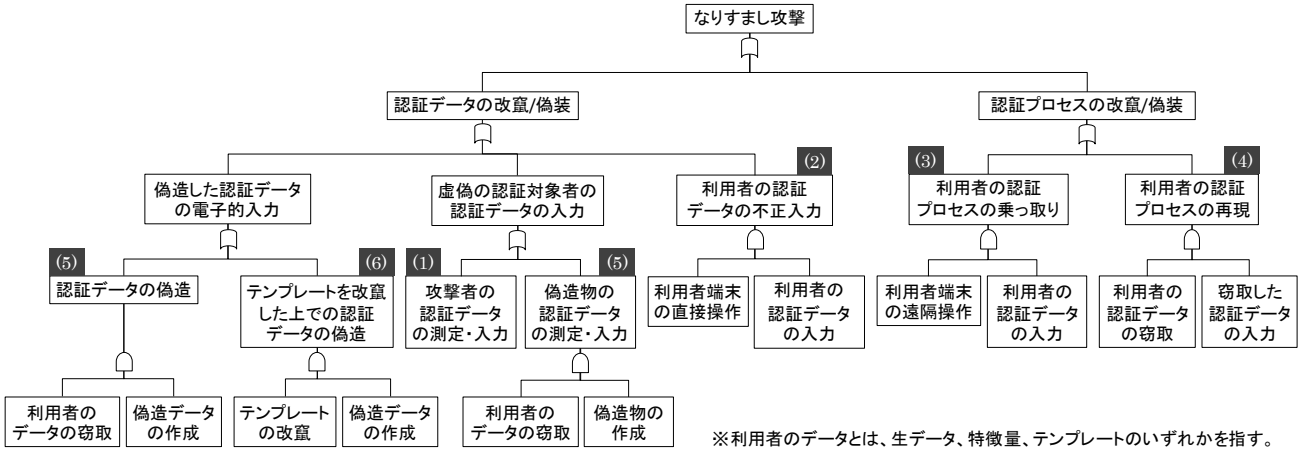


図 2 行動的特徴を用いる認証システムへのなりすまし攻撃のアタックツリーの概略

表 1 なりすましの攻撃シナリオと狙われる脆弱性

	なりすましの攻撃シナリオ	狙われる認証システムの脆弱性
(1)	攻撃者自身または共犯者等のデータを入力	利用者と攻撃者の行動的特徴が類似している（FARが高い）
(2)	利用者端末を直接操作して利用者の過去のデータを入力	•認証時から直近の時刻ではないデータを認証データとして許容する •認証時の動作に関係のない行動的特徴を用いて認証する
(3)	利用者端末を遠隔操作して利用者の（現在の）データを入力	認証時の動作や認証場所に関係のない行動的特徴を用いて認証する
(4)	窃取した利用者の過去の認証データを入力（リプレイアタック）	過去に処理した認証要求の特徴量と同じ特徴量が設定された認証要求を受け付ける
(5)	窃取した利用者のデータを基に偽造データを作成して入力	漏洩した利用者のデータが有効な（＝認証OKとなる）データである
(6)	テンプレートを改竄/不正更新した上で認証OKとなる偽造データを作成して入力	テンプレート、テンプレート生成に関係するプログラムまたはデータの改竄検知・削除・修復ができない

5.3 なりすまし攻撃への技術的対策

表 1 を基に，想定した認証システムにおける，なりすまし攻撃への技術的対策を検討したものを表 2 に示す.

表 2 なりすまし攻撃への技術的対策

	対策箇所	技術的対策	技術的対策が有効な攻撃シナリオ	課題
(A)	学習・認証の機構	FARの低い特徴量を用いる	(1)	•FARの精度 •FARの個人差
(B)		データを暗号化/変換したまま学習・認証を行う（テンプレート保護型生体認証）	(5),(6)	テンプレート保護型生体認証の既存手法の適用可能性
(C)		テンプレート・プログラム・データの改竄/不正検知を行う	(6)	•データの真正性 •学習・認証を考慮した改竄/不正検知の実装
(D)	認証システムの用法	認証データの時刻制約を設定する	(2)-(4)	適切な時刻制約の設定
(E)		認証場面に関係のある行動的特徴を用いる（生体検知を含む）	(2)-(6)	ユースケースに適合する行動的特徴の選定
(F)		複数の行動的特徴を用いる	(4)	
(G)		同じ特徴量は再び認証処理しない（例:チャレンジ・レスポンス）	(4)	（チャレンジ・レスポンスの実装方法は認証機構に依存する）

技術的対策のうち(B)，(C)は特に，テンプレートの改竄対策として有効であるが，既存手法の適用可能性の検証が必要と考えられる．(B)は，テンプレート保護型生体認証の実施を意味するが，行動的特徴の変化，テンプレートと認証データとのずれ幅の個人差，また(A)の課題に挙げる認証精度を考慮すると，Key Binding 技術を用いたテンプレート更新手法[6]等を適用して，データを暗号化／変換したまま学習・認証を行うことが可能か検証を要する．(C)は，特に学習対象のデータの改竄/不正検知が重要であるが，行動的特徴の変化のためデータ値での検知は難しいと予想される．解決策として，データの真正性の保証，改竄検知機能付の暗号方式等の適用が考えられるが，前者は実施方法，後者は暗号化／変換に関する課題が残る．以上の課題は，身体的特徴の場合も発生するが，行動的特徴の場合は，特徴量の変化のために，難易度が高くなると考えられる．

6. おわりに

本稿では，行動的特徴を利用する認証システムの脅威分析を行い，なりすましの攻撃シナリオと技術的対策を検討した．結果，行動的特徴を利用する認証システムでは，行動的特徴の変化のために，テンプレートの不正更新によるなりすましの脅威が発生しやすいこと，技術的対策としてテンプレート保護型生体認証の既存手法が適用可能か検証を要することを明らかにした.

参考文献

[1] 山口利恵，“行動解析と多要素・他段階認証”，ソーシャル ICT 研究センター 第 3 回シンポジウム, 講演 6, pp.11-16, 2015 年 6 月 12 日. http://www.sict.i.u-tokyo.ac.jp/news/sympo20150612/（参照 Jun. 6, 2016）
[2] androidcentral, “Project Abacus is an ATAP project aimed at killing the password”, 2015 年 5 月 29 日, http://www.androidcentral.com/project-abacus-atap-project-aimed-killing-password（参照 Jun. 6, 2016）
[3] 工藤 史堯 他，“ユーザに適した認証処理の動的選択方法の検討”，信学技報 Vol. 115 No. 486(2016)
[4] Wang et al., “Transforming Animals in a Cyber-Behavioral Biometric Menagerie with Frog-Boiling Attacks”, BTAS'12, pp.289-296(2012)
[5] Microsoft, “The STRIDE Threat Model”, https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx（参照 Jun. 6, 2016）
[6] 杉村 由花 他，“格子マスキング利用の Key Binding 技術におけるテンプレート更新機能”，DICOMO 2014, pp.1035-1043(2014)