バイオメトリクスの経時変化特性を考慮したリプレイ攻撃の対策

渡部 晃久[1,a)]　松本 和樹[1]　森 達哉[1,3,4]　飯島 涼[1,2]

概要：本研究では，提示された生体情報の記録時間を考慮することでリプレイ攻撃を防ぐ手法 (STUV) を提案する．STUV では，入力データが現在時刻を基準とした一定の期間において取得された確率を計算するアルゴリズムにより，提示されたデータが本人のものであり，かつ現在のものである確率に応じて認証を行う．約 2 週間に渡り記録されたキーストロークデータセットを用いて，基礎評価により (1) キーストロークの特徴が時間的に変化すること，(2) 従来の適応型生体認証システムにより認証精度を保てることを確認した後，STUV によるリプレイ攻撃に対する効果を検証した．その結果，本人/他人識別の EER を 18.94%としつつ，現在から 2 週間前のデータを用いたリプレイ攻撃を 84.44%拒否できることが確認された．STUV では，認証モデルやテンプレートの更新により現在のデータ分布に適応するだけでなく，一定以上昔の本人のデータを拒否することができる．これにより，本研究はリプレイ攻撃に対する堅牢性を向上させる新たなアプローチを提供し，生体認証システムの安全性と信頼性の向上に貢献する．

キーワード：バイオメトリクス，確率的時間調整認証 (STUV)，キーストローク認証，忘却モデル，特徴量の時間変動

Time's Up for Replay Attacks: Countermeasures Against Replay Attacks Considering the Temporal Changes of Biometrics

Akihisa Watanabe[1,a)]　Kazuki Matsumoto[1]　Tatsuya Mori[1,3,4]　Ryo Iijima[1,2]

Abstract: In this study, we propose a method (STUV) to prevent replay attacks by considering the recording time of the given biometric information. In STUV, an algorithm calculates the probability that the input data was obtained within a certain time period, and authentication is performed based on the probability that the data belongs to the genuine user and that the data is not obtained from the past. Using a keystroke dataset recorded over approximately two weeks, after confirming through an evaluation where (1) the characteristics of keystrokes change over time and (2) conventional adaptive biometric authentication systems can maintain authentication accuracy, we verified the effectiveness of STUV against replay attacks. As a result, it was confirmed that while achieving an EER (Equal Error Rate) of 18.94%, replay attacks using data from two weeks ago could be rejected at 84.44%. In STUV, not only can it adapt to the current data distribution by updating the authentication model or template, but it can also reject data from a certain past period, even if it belongs to the actual person. Thus, this research offers a new approach to enhancing resilience against replay attacks, contributing to the improvement of safety and reliability of biometric authentication systems.

Keywords: Biometrics, Stochastic Time-Adjusted User Verification, Key-stroke, Catastrophic forgetting, Temporal shift of features

[1] 早稲田大学 / Waseda University
[2] 国立研究開発法人 産業技術総合研究所 / AIST
[3] 国立研究開発法人 情報通信研究機構 / NICT
[4] 国立研究開発法人 理化学研究所 革新的知能統合センター / RIKEN AIP
[a)] akihisa@ruri.waseda.jp

1. はじめに

デジタルデバイスの利用が日常的になるにつれて，ユーザーが自身の身元を証明する認証の機会が増えている．このような状況下で，ユーザビリティの観点から行動バイオメトリクスに基づく生体認証システム，例えばキーストローク認証 [3,12] や歩行認証 [14] などが注目されている．これらの認証システムが長期間にわたり，様々な環境で信頼性を維持するためには，生体特徴が各ユーザ間で一意であることと同時に，時間や環境の変化に対して一定性（不変性）を持つことが重要であると考えられている [5]．この不変性は，時間が経過してもユーザの生体情報が一貫して同一の識別情報として機能することを保証する．

しかしながら，生体情報の不変性は必ずしも成り立たず，ユーザの心理状態や生活習慣の変化に伴い時間的に変化することが知られている [10]．このような変化に対応するため，生体認証システムでは，モデルやテンプレートの更新を行うことが一般的である．タッチベースの認証 [11] やジェスチャ認証 [15] では，本人ユーザであると判定されたサンプルを用いて継続的にモデルの更新が行われる．これら生体情報の不変性を前提としたモデル更新によるアプローチでは，過去の本人ユーザのデータをも受け入れてしまう特性がある．認証モデルがこのような特性を持つ場合，過去に流出した生体情報を認証システムに提示し，本人ユーザになりすますリプレイ攻撃に対して脆弱になる．以上の仮定で生じるリプレイ攻撃を防ぐには，過去の同一人物データを，モデルが本人データとして受け入れることはセキュリティ上好ましくないという事を考慮した新たな認証手法が必要である．

本研究では，行動バイオメトリクスにおいて生体特徴が時間的に変化することを利用してリプレイ攻撃を防ぐ手法を提案する．我々は，本人ユーザの現在の生体情報のみを認証の対象とし，過去の本人ユーザの生体情報を拒否し，リプレイ攻撃を防ぐことを目指す．具体的には，提示されたバイオメトリクスが最近に取得された確率 (現在確率) を計算するモデルを新たに提案する．さらに，現在確率と従来の認証モデルが出力する本人である確率 (本人確率) を統合し，本人かつ現在である確率を計算し，この確率が一定の閾値を超えた場合のみ認証を許可する．これにより，本人/他人の識別精度を維持しつつ，過去の時刻の本人データを用いたリプレイ攻撃を効果的に検出することが可能となる．

本研究の主な貢献は以下の通りである．

- **新たな問題認識の提示:** 従来研究では，生体情報が不変であるという仮定のもとで，認証システム構築が行われていた．本研究では，生体情報の不変性の仮定がリプレイ攻撃の原因となっていることに着目し，過去の本人データは受け入れないモデルを構築するという観点での対策を初めて提案した．
- **過去の本人データを拒否する認証モデルの実現:** 生体情報の記録時間を考慮した認証アルゴリズムを提案する．本手法により，従来のモデル・テンプレート更新では一部実現ができなかった，**過去の本人ユーザの生体情報を拒否**するセキュリティ上安全な認証モデルの開発を行った．本手法により，リプレイ攻撃として最も仮定の強い，モデルに対して直接リプレイサンプルを入力する攻撃に対しても対策を行うことが可能となる．
- **生体データ記録時間推定の確率モデル導入:** 生体データがどの時間に記録されたものであるかを推定するためには，新たな確率モデルの導入が必要である．本研究では，データが 2 週間おきなど離散的な時間間隔でとられたものであっても，その間の時間を補完して生体信号の記録時間を推定できる確率モデルを導入した．
- **実データによる検証:** 本研究では，キーストロークバイオメトリクスを利用した実験により提案手法の有効性を評価した．その結果，本人/他人の識別精度を維持しつつ，過去のデータを用いたリプレイ攻撃を効果的に検出することができることが示された．特に，他人/本人の識別性能を EER18.94%としつつ 2 週間程度離れたデータをリプレイした場合に 88.44%で攻撃を検出できることが確認された．さらに，過去の学習データを忘却するアプローチと比較しても，提案手法は優れたリプレイ攻撃の検知性能を示した．

2. 背景知識

2.1 行動バイオメトリクス

行動バイオメトリクスを用いた認証では，ユーザがジェスチャや歩行など特定の動作を行うことによって認証を行う．知識ベースの認証や静的バイオメトリクスがユーザに明示的な要求を行うのに対して，行動バイオメトリクスはユーザの自然な動作を用いて認証を行うことから，暗黙的に生体特徴を取得することができ，認証プロセスを簡素化できる [1]．そのため，キーストロークを用いた認証 [3,12] やジェスチャ認証 [4,15]，歩行認証 [14]，VR 空間での認証 [8,9] など，行動バイオメトリクス認証はセキュリティとヒューマンコンピュータインタラクションの分野で横断的に研究されている．

行動バイオメトリクス認証は，ユーザの自然な動作を用いるため，その特性は時間とともに変化する．例えば，ユーザの健康状態や気分，疲労度などが変化すると，それに伴い歩行動作やキーストローク動作，ジェスチャ動作の特徴が変化し，この現象は，テンプレートエイジングとして知られている [10]．テンプレートエイジングは，機械学習の文脈では概念ドリフトと呼ばれ，データ分布の変化に

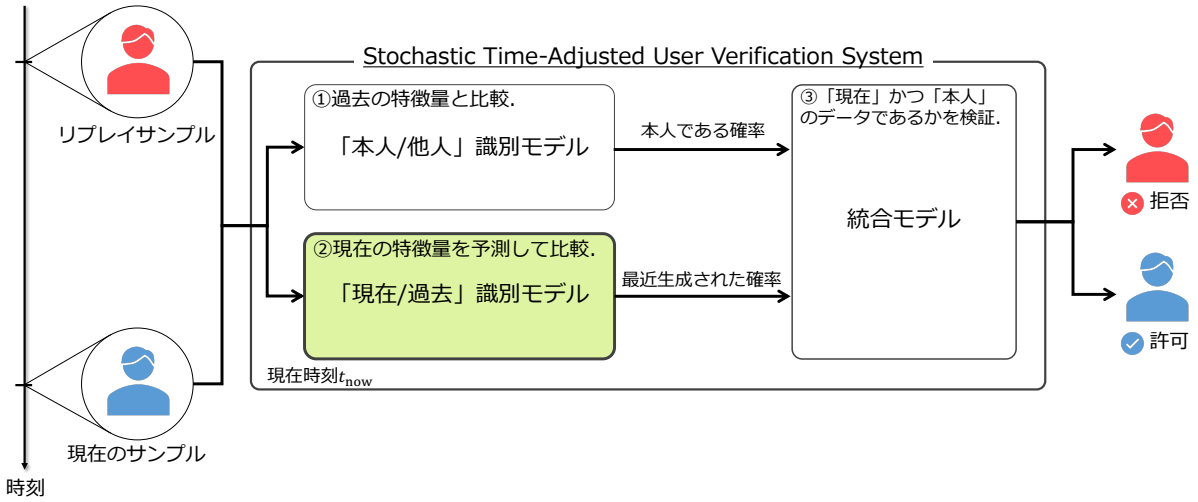

図 1: 提案手法の概略図．予測される現在の本人ユーザの特徴量と類似しない入力はリプレイ攻撃として認証を拒否する．

より学習モデルが新しいデータに対して適応できなくなる問題を引き起こす．この結果，時間の経過に伴い認証モデルの精度が低下する [15]．したがって，行動バイオメトリクスを用いた認証システムは，生体情報の時間的な変化を考慮に入れる必要がある．

2.2 適応型生体認証システム

適応型生体認証システムは，時間の経過とともにテンプレートやモデルが自動的に更新されるシステムのことを指す [10]．このシステムは，テンプレートエイジング問題を解決するために使用される．連続するストリームデータから学習し，モデルの汎化能力を維持させる技術は機械学習の分野では継続学習と呼ばれる．継続学習の手法としては，一般に，損失関数を工夫してストリームデータから逐次的にモデルを学習させる手法と，バッファに格納されたストリームデータを用いてモデルを再学習させる手法がある．

InreAuth [11] では，逐次的な学習手法を用いた適応型生体認証システムを実現している．InreAuth は，勾配ブースティング決定木モデルとニューラルネットワークモデルを統合した認証モデル GBDTNN により，タッチベースの認証において 2 ヶ月間に渡って安定な精度を維持できることを示した．

一方，ThumbUp [15] では，バッファを用いた再学習手法を採用している．ThumbUp は LSTM をベースとした特徴抽出層と MLP を用いた分類層を結合したアーキテクチャを利用して認証モデルを構築し，新しいサンプルをバッファに追加して元の学習データと一緒に分類層のみを再学習させている．これにより，ジェスチャ認証において約 3 ヶ月間に渡って安定な精度を維持できることを示した．

生体認証においては，通常の継続学習とは異なり過去の本人データに対して汎化性能を維持する必要はない．しかし，既存の適応型生体認証システムは過去の本人データに対しても認証を許可する手法が用いられている．本研究では，現在の本人データに対する汎化性能を持ちつつ，過去の本人データを拒否するモデルを構築する．これにより，過去の本人ユーザのデータを再生するリプレイ攻撃に対してロバストな認証システムを提案する．

3. 提案手法

3.1 概略

本手法は，認証システムが受け取るデータが本人ユーザのものであり，かつそのデータが現在のものであることを保証することで，リプレイ攻撃を防ぐことを目指す．現在のデータであるかを推定する機能を従来認証に追加する理由は，リプレイ攻撃に用いられる生体情報が過去の生体情報であり，過去のデータであることを検出できれば，効果的に対策ができると考えられるためである．生体情報の不変性を仮定した従来の認証システムでは，不変性の仮定により過去の本人ユーザのデータと現在の本人ユーザのデータは同一のラベルとしてモデルの更新が行われ，過去の生体情報が現在でも有効とされる．これにより，攻撃者は過去の生体情報を用いて本人ユーザを偽装し，システムへ攻撃することが可能となるため，リプレイ攻撃を原理的に防ぐことが難しい．本手法では，認証システムに提供されるデータに対して，それが本人ユーザのものである確率と，現在のものである確率を計算する．これにより，入力データが本人からのものであると同時に，そのデータが現在のものであることを確認することが可能となる．

3.2 ワークフロー

図 1 に示すように，確率的時間調整認証 (STUV：Stochastic Time-Adjusted User Verification) は 3 つの部分から構成される．1 つ目は，データが本人のものである確率を出力する確率的識別モデルで，これは生体認証システムにお

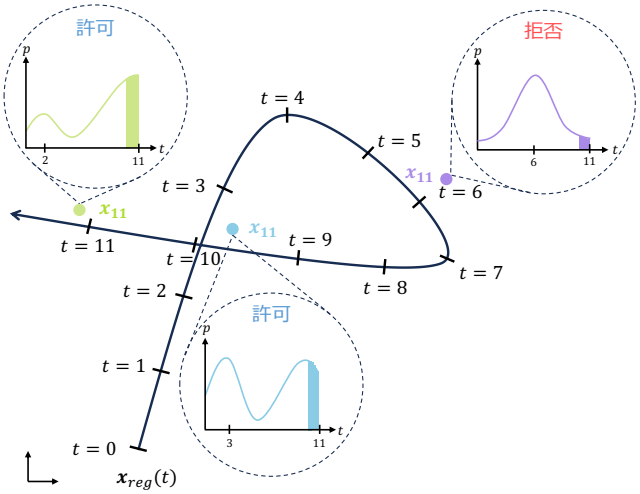

図 2: STUV の概念図．現在時刻 $t = 11$ における特徴量の生成時刻の推定と確率の計算．色付き領域の横の長さが時間 Δt を，面積が確率 $P(11 - \Delta t \leq t \leq 11|\boldsymbol{x}_{11})$ を表す．紫色で示した特徴量は，$t = 6$ 付近の近似特徴量と距離が近くなり，現在時刻 $t = 11$ の予測 (近似) 特徴量 $\boldsymbol{x}_{reg}(11)$ とは距離が離れているため，色付き領域の面積が小さくなり認証が拒否される．

いて一般的に用いられる本人/他人の識別を行うモデルである．2 つ目は，データの時間的な変化を捉えて現在のものである確率を計算するモデルで，これは新たに本研究で提案されるものである．提案手法のモデルでは，過去の生体特徴の時間的な変化を捉えるために，認証システムに保存されているテンプレートを利用して現在の本人ユーザの特徴量を予測する．入力特徴量が予測された現在時刻における本人ユーザの特徴量と類似していれば，データが現在のものである確率は高くなり，そうでなければデータが現在のものである確率は低くなる．そして，3 つ目は，2 つのモデル，本人/他人の識別モデルと過去/現在の識別モデルが出力するそれぞれの確率値を統合することにより，入力データが本人かつ現在のものである確率を計算する．

3.3 確率的時間調整認証 (Stochastic Time-Adjusted User Verification)

STUV では，現在時刻における特徴量が与えられたとき，その特徴量が本人のものである確率（本人確率）と，その特徴量が最近に生成されたものである確率（現在確率）を計算し，その同時確率を用いて認証を行う．これにより，現在から時間的に離れた昔の特徴量をリプレイ攻撃として認証を拒否することを目指す．

本人確率に関しては，提示される N 次元の特徴量 $\boldsymbol{x}_{\text{obs}} \in \mathbb{R}^N$ に対して，その特徴量が本人のものであるか否かを表す確率変数 Y の生起確率 $P(y = 1|\boldsymbol{x}_{\text{obs}})$ を，従来法と同様の確率的識別モデルを用いて得る．

現在確率は本研究で新たに定義するものであり，適当な時間幅 Δt と現在時刻 t_{now} に対し，入力特徴量が時刻 $t_{\text{now}} - \Delta t$ から t_{now} の区間において取得された確率 $P(t_{\text{now}} - \Delta t < t_{\text{obs}} < t_{\text{now}}|\boldsymbol{x}_{\text{obs}})$ として定める．現在確率の導出では，時刻 t において取得される特徴量 $\boldsymbol{x}$ の期待値を表す曲線として，特徴量推移曲線 $\boldsymbol{x}_{\text{exp}}(t)$ を導入する．その上で，時刻 t および特徴量 $\boldsymbol{x}$ がそれぞれ以下の確率分布に従うと仮定する．

$$\begin{aligned} t &\sim \mathcal{U}(t_{\text{init}}, t_{\text{now}}) \\ \boldsymbol{x} &\sim \mathcal{N}(\boldsymbol{x}_{\text{exp}}(t), \sigma^2 I) \end{aligned} \tag{1}$$

ただし，$\mathcal{U}$ および $\mathcal{N}$ は一様分布と N 次元の正規分布を表し，t_{init} はシステムの初期化時刻に対応する．また，分散 σ^2 は分布の広がりを制御するハイパーパラメータである．上記の仮定のもと，時刻と特徴量の同時確率密度関数 $f_{T,\boldsymbol{X}}(t, \boldsymbol{x})$ が

$$f_{T,\boldsymbol{X}}(t, \boldsymbol{x}) = \frac{\exp(-||\boldsymbol{x} - \boldsymbol{x}_{\text{exp}}(t)||_2^2/\sigma^2)}{(t_{\text{now}} - t_{\text{init}})\,(2\pi\sigma^2)^{N/2}} \tag{2}$$

と書ける．さらに，この分布に対してある特徴量 $\boldsymbol{x}_{\text{obs}}$ が提示されたもとでの条件付き確率密度関数 $f_{T|\boldsymbol{X}=\boldsymbol{x}_{\text{obs}}}$ は

$$f_{T|\boldsymbol{X}=\boldsymbol{x}_{\text{obs}}}(t) = \frac{\exp(-||\boldsymbol{x} - \boldsymbol{x}_{\text{exp}}(t)||_2^2/\sigma^2)}{\int_{t_{\text{init}}}^{t_{\text{now}}} \exp(-||\boldsymbol{x} - \boldsymbol{x}_{\text{exp}}(t')||_2^2/\sigma^2)\,dt'} \tag{3}$$

で求められる．このとき，$\boldsymbol{x}_{\text{obs}}$ が時刻 $t_{\text{now}} - \Delta t$ から t_{now} の範囲で得られた確率，すなわち $\boldsymbol{x}_{\text{obs}}$ の現在確率は

$$P(t_{\text{now}} - \Delta t < t_{\text{obs}} < t_{\text{now}}|\boldsymbol{x}_{\text{obs}}) = \int_{t_{\text{now}} - \Delta t}^{t_{\text{now}}} f_{T|\boldsymbol{X}}(t')\,dt' \tag{4}$$

と表される．

これらの同時確率に関しては，Y と T が $\boldsymbol{X}$ を与えたもとで条件付き独立とみなせることから，

$$\begin{aligned} &P(y = 1, t_{\text{now}} - \Delta t \leq t_{\text{obs}} \leq t_{now}|\boldsymbol{x}_{t_{now}}) = \\ &\quad P(y = 1|\boldsymbol{x}_{\text{obs}}) \times P(t_{\text{now}} - \Delta t < t_{\text{obs}} < t_{\text{now}}|\boldsymbol{x}_{\text{obs}}) \end{aligned} \tag{5}$$

が成り立つ．STUV による認証は，この同時確率が閾値 threshold 以上となるときに受理し，そうでない場合に拒否するアルゴリズムとなる．

実用上は，真の特徴量推移曲線 $\boldsymbol{x}_{\text{exp}}(t)$ を求めることが困難なため，過去のテンプレートをもとに推定した近似曲線 $\hat{\boldsymbol{x}}_{\text{exp}}(t)$ を用いる．

4. 実験

我々は，STUV が実際の生体データにおいてどの程度効果的にリプレイ攻撃を防御する能力を持つかを評価するための実験を行う．実験は大きく 2 つに分けられる．まず，生体情報が時間的に変化し，適応型生体認証モデルにより認証精度を維持できることを確認するための予備実験を行う．次に，過去のサンプルを再生するリプレイ攻撃に対し

て STUV の防御能力と認証システム全体としての性能評価を行った．

4.1 認証シナリオ

本実験では，ユーザが日々生体認証システムを利用することで生成されるデータを基に，認証モデルが逐次的に更新されるシナリオを考える．具体的には，ユーザが認証システムを利用するたびに，そのユーザの生体データがシステムに蓄積される．この蓄積されたデータ (テンプレート) は，時間とともに変化するユーザの生体情報を反映する．システムは，これらのデータを用いてユーザの認証モデルを更新し，生体情報の変化に対応する．

認証システムは，システムに登録されているユーザのデータを用いて特徴抽出モデルを事前に学習し，初期時刻における本人データの集合から一部のデータをサンプリングしてテンプレート集合に格納する．また，システムに保存されているデータとテンプレート集合に含まれるデータを用いて認証モデルを訓練する．その後，本人ユーザのデータと他人ユーザのデータを用いて認証モデルをテストする．このテストフェーズでは，システムが適応型認証モデルである場合，本人である確率が高いと予測されたサンプルをテンプレート集合に追加し，認証モデルを更新する．これにより，ユーザの生体情報の変化に対応することが可能となる．一方，静的認証モデルの場合，一度訓練された認証モデルは更新されず，テンプレート集合も固定される．最後に，リプレイ攻撃を実施し，認証モデルがリプレイサンプルに対して認証を拒否できるかを確認する．

4.2 予備実験

本実験では，Carnegie Mellon University (CMU) が提供するキーストロークデータセット [6] を使用する．このデータセットは，キーストローク認証の研究において広く採用されており，標準的なベンチマークとして利用されている [3, 12]．51 人の被験者から収集されたキーストロークデータを含んでおり，各被験者は 1-2 日の間隔で 8 回のセッションを通じてデータを提供している．これにより，約 2 週間に渡る期間でのキーストロークパターンの変化を観察することができる．

予備実験では，特徴量の時間的変動を視覚的に確認する．そのために，t-SNE [13] を用いて特徴量を 2 次元に圧縮する．t-SNE は，高次元空間でのデータポイント間の距離関係を保持しつつ，データを低次元に圧縮する手法である．この手法は，STUV と同様に，近傍データがデータポイント間の距離に基づき確率的に選択されるという仮定を採用している．特に，確率分布が正規分布であるという点で，STUV と同じ考え方を用いている．そのため，t-SNE により圧縮された特徴量の分布の中心が時間経過により移動するかどうかを確認することができる．なお，本研究では 2 次元ガウス分布を用いて特徴量の分布を近似する．

さらに，特徴量が時間経過とともに変化することを確認した後，適応型認証システムがこれらの変化に効果的に対応できることを検証する．具体的には，ThumbUp [15] の手法に従い，各時刻で取得した新たなデータを利用してモデルを再学習させる適応型生体認証システムを構築する．この適応手法により．新しいデータが利用可能になるたびにモデルが逐次的に更新される．これは，学習データが初期の登録データのみで固定され，更新が行われない静的認証モデルとは対照的である．ThumbUp [15] では認証許可の閾値とテンプレート更新の閾値が異なるが，本研究では両者を統一する．これは FaceID など一般的な生体認証システムの設計原理に従っている [2]．すなわち，特定の閾値以上の確信度で本人であると予測されたデータの一部がテンプレート集合に追加される．

以上の適応型生体認証モデルをと静的認証モデルとを比較し，CMU キーストロークデータセットにおいても特徴量の変化に応じてモデルを適応的に更新することで認証性能を維持できることを確認する．

4.3 実験設定

実験では，データセット内の全てのユーザについてシナリオを設定する．さらに，各ユーザについて，システムに登録されているユーザーを 35 人，システムにアクセスしようとする他人ユーザーを 10 人としてシナリオを初期化する．テンプレートの取得は，初期時刻を $t = 0$ として $t = [0, 1, 2, 3, 4, 5, 6]$ で行う．システムの現在時刻は $t = 7$ であり，$t = 0$ から $t = 6$ までのデータを用いてリプレイ攻撃が実施される．

テンプレートの更新手順については，無限窓更新手法 [7] を用いる．すなわち，新しいサンプルの認証が許可されるたびに，それは訓練データに追加される．ただし，本実験ではリプレイ攻撃に用いるデータとモデルの更新に用いるデータを重複させないために保存するテンプレートの数は各時刻で 20 個とし，残りのデータをリプレイ攻撃に用いる．この更新手法は，Apple の FaceID で使用されている教師なし更新プロセス [2] と同様の考え方で，新しく得られたサンプルはノイズレベルが低ければテンプレート集合に追加される．

特徴量の前処理とモデルの設定を行う．特徴量の前処理として，RobustScaler による変換を行う．RobustScaler は，データの中央値と四分位数を用いてスケーリングを行う手法である．これにより，外れ値の影響を受けにくいスケーリングが可能となる．識別モデルとしては，多層パーセプトロンを採用する．具体的には，入力層から出力層への順に，31 次元，64 次元，128 次元，64 次元，2 次元のノードを持つ 5 層 (隠れ層 3 つ) のニューラルネットワークを用いる．これは，キーストローク認証において一般的

に用いられる構成 [3,12] と同様のものである．

また，STUV では分布の広がりを制御するパラメータ $\sigma_{t_{now}}$ の調整が必要である．本実験では，$\sigma_{t_{now}}$ の値を調整するために，保存されているテンプレートデータの中で最新時刻 $t = 6$ のデータを受け入れる設定で探索を行う．探索は，最新時刻のテンプレートデータのラベルを 1，それ以前のものをラベル 0 と設定し，このラベル付けに基づいて交差エントロピー損失を最小化するようにベイズ最適化によって行われる．特徴量の予測モデルとしては，カーネルリッジ回帰を用いる．カーネルリッジ回帰は，特徴量の時間的な変化を捉えるために，認証システムに保存されているテンプレートを利用して現在の本人ユーザの特徴量を予測する．この予測モデルは過去のデータを使って学習し，未来のデータを使って評価するという順序になるようなクロスバリデーションを行い，パラメータはグリッドサーチで最適化する．さらに，時間窓のパラメータ Δt も重要な要素である．Δt は本手法におけるもう一つのハイパーパラメータであり，入力特徴量が過去のどの程度の時間範囲の特徴量と類似しているべきかを決定する時間窓である．本実験では，Δt は 0.2 に固定する．

さらに，提案手法の性能評価のために，以下の 3 つの手法と比較を行う．

通常の適応型認証モデル: 過去の全てのデータを学習データとしてモデルを更新する手法．この手法は，全てのデータを等しく扱うため，ユーザの特徴量が時間とともに変化することを考慮しない．そのため，ユーザの特徴量が時間とともに変化する場合，認証性能が低下する可能性がある．なお，予備実験で用いる適応型認証モデルと同じモデルである．

忘却モデル: 過去のデータを忘却させてモデルを更新する手法．この手法は，一時点前 $t = 6$ のデータだけを用いてモデルを学習し，それを用いて認証を行う．これにより，モデルは常に最新のデータに対して最適化され，過去のデータは忘却される．この手法は，ユーザの特徴量が時間とともに変化することを考慮するが，過去のデータを意図的に拒否する仕組みは用いられていない．

STUV： 入力データが本人である確率と，現在のものである確率の同時確率を用いた認証手法．これは，過去の特徴量から現在の特徴量を予測し，その予測結果と入力特徴量との類似度を用いて，入力特徴量が現在のものである確率を計算する．さらに，確率的識別モデル (通常の適応型認証モデル) を用いて，入力特徴量が本人のものである確率を計算する．これら 2 つの確率の同時確率により，入力特徴量が本人のものであり，かつ現在のものである確率を計算して認証を行う．

これらの 3 つの手法を比較することで，STUV がリプレイ攻撃に対する耐性をどの程度強化できるか，また，認証精度をどの程度維持できるかを評価する．

5. 結果

5.1 特徴量の時間変動と適応型認証モデル

本研究では，キーストロークの特徴量が時間経過とともに変化し，その状況で適応型認証モデルが有効であることを確認するための予備実験を行なった．

図 3 は，特徴量の時間変化の例を示している．各データポイントは特定の時刻における特徴量を表し，その位置は t-SNE [13] によって 2 次元に圧縮された特徴空間上の座標を示している．図中の色付きの領域は，特定の時間帯におけるデータポイントの分布を示す 2 次元ガウス分布を表している．これらのガウス分布の平均が時間経過とともに移動していることが観察された．これは，特徴量が時間の経過とともに変動していることを示している．

図 3 は，特徴量が時間変化する状況下で本人データに対する予測確率がどのように変化するかを示している．青色の線は適応型認証モデルを，橙色の線は静的モデルを表している．この結果から，特徴量が時間経過とともに変化する場合，静的モデルでは本人ラベルのデータに対して本人であると予測する確率が時間経過とともに低下することが観察された．これに対して，適応型認証モデルでは，本人データに対する予測確率が一定の高いレベルを維持していることが確認でき，キーストローク認証においても適応型認証モデルを用いることで特徴量の時間変化に対応して認証性能を維持できることを示している．

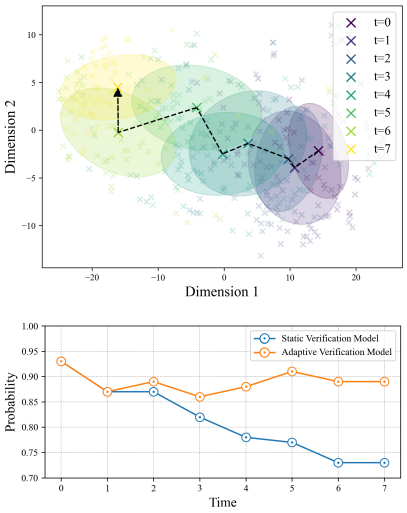

図 3: 特徴量の時間変化とモデルの予測確率の平均値．上は特徴量の時間変化の例であり，色付きの領域で表された特徴量分布の中心が時間の経過とともに移動していることが分かる．下は本人データに対するモデルの予測確率の平均値で，適応型認証モデルは静的認証モデルに比べて，本人データに対する予測確率が横ばいで推移していることが分かる．

5.2 提案手法の評価

提案手法の評価は，本人/他人の識別精度とリプレイ攻撃の検出能力の 2 つの観点から行われた．図 4 には，左から提案手法，忘却モデル，通常の適応型認証モデルの 3 つの手法について，本人/他人の識別能力と各時刻のデータを用いたリプレイ攻撃の検出能力についての ROC 曲線を示している．これらの ROC 曲線は，各時刻での各ユーザについての ROC 曲線を平均したものである．

また，表 1 では，本人/他人の識別における EER 閾値で固定した時にどの程度リプレイ攻撃を拒否できるかを示している．具体的には，各手法について，本人/他人識別の平均 EER と，各時刻 $t = 0$ から $t = 6$ までのリプレイ攻撃の平均拒否率を示している．これにより，各手法の本人/他人の識別精度とリプレイ攻撃に対する耐性を比較することができる．

提案手法は，本人/他人の識別精度を維持しながら，現在時刻 $t = 7$ から離れた時刻の本人データを用いたリプレイ攻撃を効果的に検出できることが確認できた．具体的には，表 1 に示す通り，提案手法は本人/他人の識別で EER 値が 18.94%としつつ，$t = 0$ から $t = 5$ までの各時刻でのリプレイ攻撃の平均拒否率がそれぞれ 84.44%，72.14%，66.99%，49.59%，41.83%，30.19%と最も高い結果を示した．これは，提案手法が効果的にリプレイ攻撃を検出できることを示している．

一方，忘却モデルのリプレイ攻撃の検出能力が提案手法に比べて劣っていることが分かる．忘却モデルは，一時刻前のデータを受け入れるように学習される一方で，過去のデータを意図的に拒否するような学習は行わない．そのため，過去のデータを用いたリプレイ攻撃が行われた場合，そのデータが過去のものであることを検出することが難しくなる．これにより，リプレイ攻撃に対する検出能力が低下したと考えられる．

通常の認証モデルは，本人/他人の識別精度は高いもののリプレイ攻撃の検出能力が低いことが確認された．これは，通常の認証モデルが過去の全てのデータを学習データとして用いるため，現在のユーザの特徴と過去のユーザの特徴を区別する能力が低いためである．

以上の結果から，提案手法は，既存の認証精度を維持しつつリプレイ攻撃に対する耐性を強化することができることが確認できた．

6. 議論

本章では，提案手法の実用性とより効果的にリプレイ攻撃を検知する方法な今後の研究の方向性について議論する．

適用可能性． 提案手法の有効性は，キーストロークダイナミクスに基づく認証システムに対して検証された．特に約 2 週間（$t = 0$ と $t = 7$）離れたデータをリプレイする場合では，本人/他人識別の EER を 18.94%に保ちつつ，84.44%のリプレイ攻撃を検出して拒否することができた（表 1 参照）．この結果は，提案手法が行動バイオメトリクスに基づく認証システムに対して有効である可能性を示唆している．行動バイオメトリクスは，ユーザーの行動特性に基づくものであり，時間とともに変化する可能性が高い．このような時間変化を捉えることが可能な提案手法は，行動バイオメトリクスに対する適用性が高いと考えられる．

一方，顔認証や指紋認証などの静的バイオメトリクスは行動特性に比べて時間変化がなだらかであることが一般的である．そのため，これらの認証システムに対して提案手法を適用する際には，時間変化を適切に捉えるための工夫が必要となる．特に，顔認証システムにおいては，特徴抽出の部分に提案手法の適用限界となりうる固有の問題が存在すると考えられる．顔認証システムでは，深層距離学習が一般的に用いられるが，深層距離学習はクラス内分散を最小化するように学習が行われる．その結果，時間変化を捉えるための特徴量が抽出されにくくなる可能性がある．

攻撃検出能力の向上． 提案手法の特徴量の近似曲線において，交差点が存在する場合，その点の付近では古いデータと新しいデータを区別することが困難となる（図 2 参照）．このような状況では，認証システムは入力データが古いデータであるか，または新しいデータを正確に識別することが困難となるため，提案手法の制約事項である．しかし，攻撃者がこのような交差点周辺の特徴量を狙って生成することも同時に難しい．これは，攻撃者にとって特徴量推移曲線は未知であり，それが交差する時刻のデータを意図的に入力することが困難なためである．

上記の制約を解決するためには，交差がないような特徴量が必要となる．これは，特徴量が時間的に一貫性を持つことを保証し，古いデータと新しいデータを正確に区別することを可能にする．このような特徴量を得るためには，本人/他人の識別と過去/現在の識別の各タスクに対して特徴量を最適化することが効果的であると考えられる．例えば，ユーザ認証のタスクでは，深層距離学習などの手法により獲得した特徴量を使用する一方で，リプレイ攻撃の検出のタスクでは，生体情報の時間変化を反映した特徴量を使用することで，各タスクの性能が最大化されることでが可能となると考えられる．このような特徴量の最適化により，本人/他人の識別と過去/現在の識別の各タスクの性能が向上すると，同時確率を用いる提案手法の認証精度が向上する．これにより，攻撃者が古いデータを用いて認証を試みるリプレイ攻撃をより効果的に防ぐことが可能になると考えられる．

7. 結論

本研究では，生体情報が時間とともに緩やかに変化するという性質を利用し，その変化の傾向にそぐわないデータが入力された場合にリプレイ攻撃として判定する新しい認

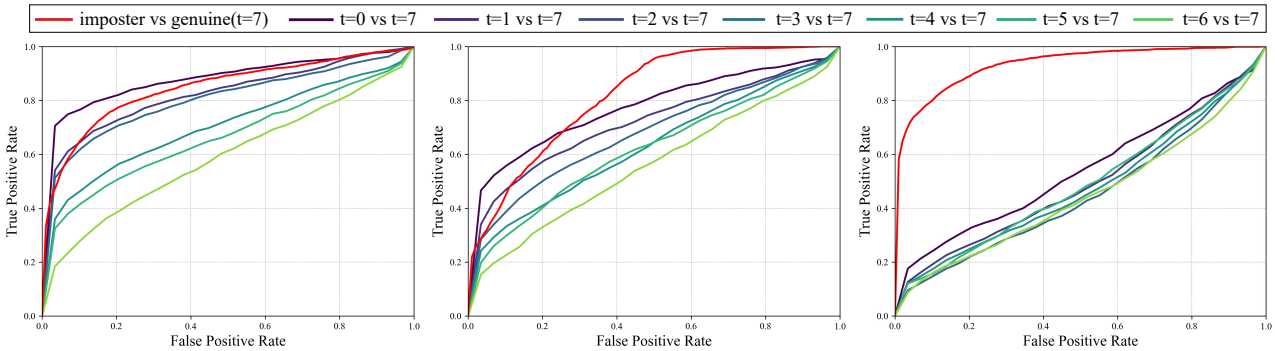

図 4: 提案手法 (左)，忘却モデル (中)，従来の認証モデル (右) に対する平均 ROC 曲線の比較.

手法	他人/本人 平均 EER	リプレイ攻撃の平均拒否率						
		$t=0$	$t=1$	$t=2$	$t=3$	$t=4$	$t=5$	$t=6$
通常の適応型認証モデル	**10.57**	20.26	16.91	15.03	15.23	16.60	13.27	14.51
忘却モデル	21.57	67.38	56.45	47.77	43.02	40.92	30.04	**23.90**
STUV(提案手法)	18.94	**84.44**	**72.14**	**66.99**	**49.59**	**41.83**	**30.19**	15.56

表 1: 本人/他人識別の EER 閾値におけるリプレイ攻撃の平均拒否率.

証システム STUV を開発した．具体的には，システムに保存された過去のバイオメトリクスデータから現在の特徴量を予測し，入力データと予測した特徴量との距離が近ければ認証を許可する確率的なモデルを構築した．さらに，入力データが本人である確率と現在のデータである確率の同時確率を用いて認証を行うことで，本人かつ現在のデータのみを受理する認証モデルを実現した．キーストロークデータを用いた実験により，STUV の有効性を検証した．結果として，2 週間程度離れたデータをリプレイした場合に本人/他人の EER 閾値で 84.44 %の精度で攻撃を検出し，認証を拒否できることが確認された．また，従来認証モデルや，単純に過去の学習データを忘却する認証モデルと同条件で比較しても，提案手法はユーザ認証とリプレイ検知の両方において優れた性能を示した．これらの結果から，提案手法がユーザ認証の精度を維持しつつリプレイ攻撃に対する耐性を強化することができることが示された．

謝辞 本研究の一部は JSPS 科研費 22K19782，22K17890 の助成を受けたものです.

参考文献

[1] Alt, F. and Schneegass, S.: Beyond Passwords—Challenges and Opportunities of Future Authentication, *IEEE Security amp; Privacy*, Vol. 20, No. 01, pp. 82–86 (2022).

[2] Apple: Apple Platform Security, `https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf` (2022). [Accessed 16-08-2023].

[3] Ayotte, B. et al.: Group Leakage Overestimates Performance: A Case Study in Keystroke Dynamics, *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR) Workshops*, pp. 1410–1417 (2021).

[4] Guo, K. et al.: Mudra: A Multi-Modal Smartwatch Interactive System with Hand Gesture Recognition and User Identification, *IEEE INFOCOM 2022 - IEEE Conf. Comput. Commun.*, pp. 100–109 (2022).

[5] Jain, A. K. et al.: An Introduction to Biometric Recognition, *IEEE Trans. Cir. and Sys. for Video Technol.*, Vol. 14, No. 1, p. 4–20 (2004).

[6] Killourhy, K. S. et al.: Comparing anomaly-detection algorithms for keystrokedynamics, *2009 IEEE/IFIP Int. Conf. Dependable Syst. Netw*, pp. 125–134 (2009).

[7] Kloft, M. and Laskov, P.: Security Analysis of Online Centroid Anomaly Detection, *J. Mach. Learn. Res.*, Vol. 13, No. 1, p. 3681–3724 (2012).

[8] Liebers, J. et al.: Understanding User Identification in Virtual Reality Through Behavioral Biometrics and the Effect of Body Normalization, *Proc. 2021 CHI Conf. Hum. Factors Comput. Syst.*, CHI '21, Association for Computing Machinery (2021).

[9] Pfeuffer, K. et al.: Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality, *Proc. 2019 CHI Conf. Hum. Factors Comput. Syst.*, CHI '19, Association for Computing Machinery, p. 1–12 (2019).

[10] Pisani, P. H. et al.: Adaptive Biometric Systems: Review and Perspectives, *ACM Comput. Surv.*, Vol. 52, No. 5 (2019).

[11] Shen, Z. et al.: IncreAuth: Incremental Learning based Behavioral Biometric Authentication on Smartphones, *IEEE Internet of Things Journal*, pp. 1–1 (2023).

[12] Uzun, Y. and Bicakci, K.: A second look at the performance of neural networks for keystroke dynamics using a publicly available dataset, *Computers Security*, Vol. 31, No. 5, pp. 717–726 (2012).

[13] van der Maaten, L. and Hinton, G.: Visualizing Data using t-SNE, *Journal of Machine Learning Research*, Vol. 9, No. 86, pp. 2579–2605 (2008).

[14] Wan, C., Wang, L. and Phoha, V. V.: A Survey on Gait Recognition, *ACM Comput. Surv.*, Vol. 51, No. 5 (2018).

[15] Yu, X. et al.: ThumbUp: Identification and Authentication by Smartwatch using Simple Hand Gestures, *2020 IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, IEEE Computer Society, pp. 1–10 (2020).