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]

[1]早稲田大学，[2]AIST, [3] NICT, [4] RIKEN AIP

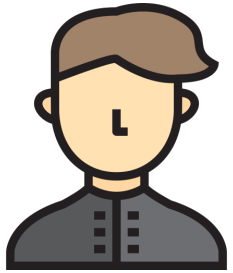
[a)] akihisa@ruri.waseda.jp

生体認証とは？

生体認証とは，顔や指紋など一人ひとりにユニークな身体/動作の特徴を用いた個人認証.

指紋

人によって異なる模様

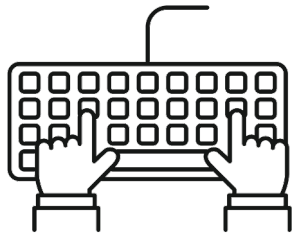


顔

人によって異なる形状

歩容

人によって異なる歩き方

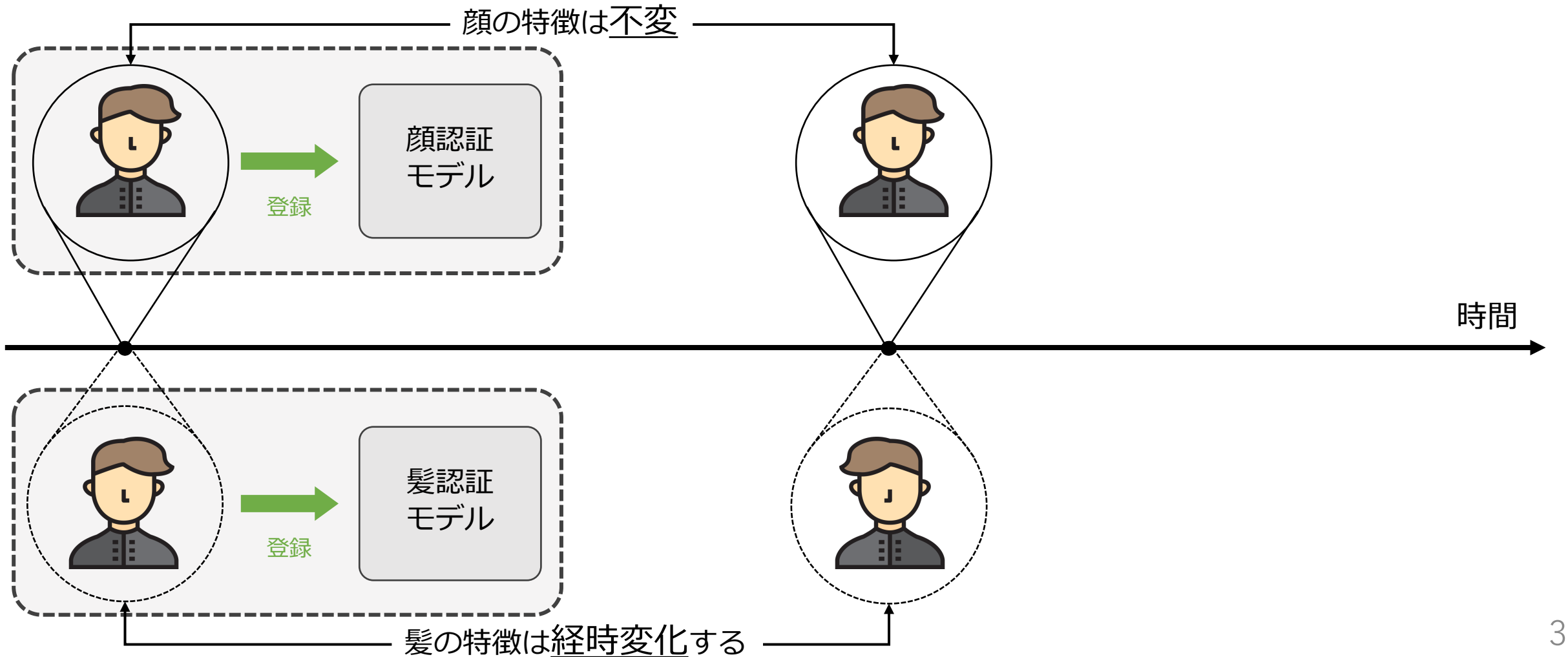


タイピング

人によって異なる打ち方

生体情報の不変性

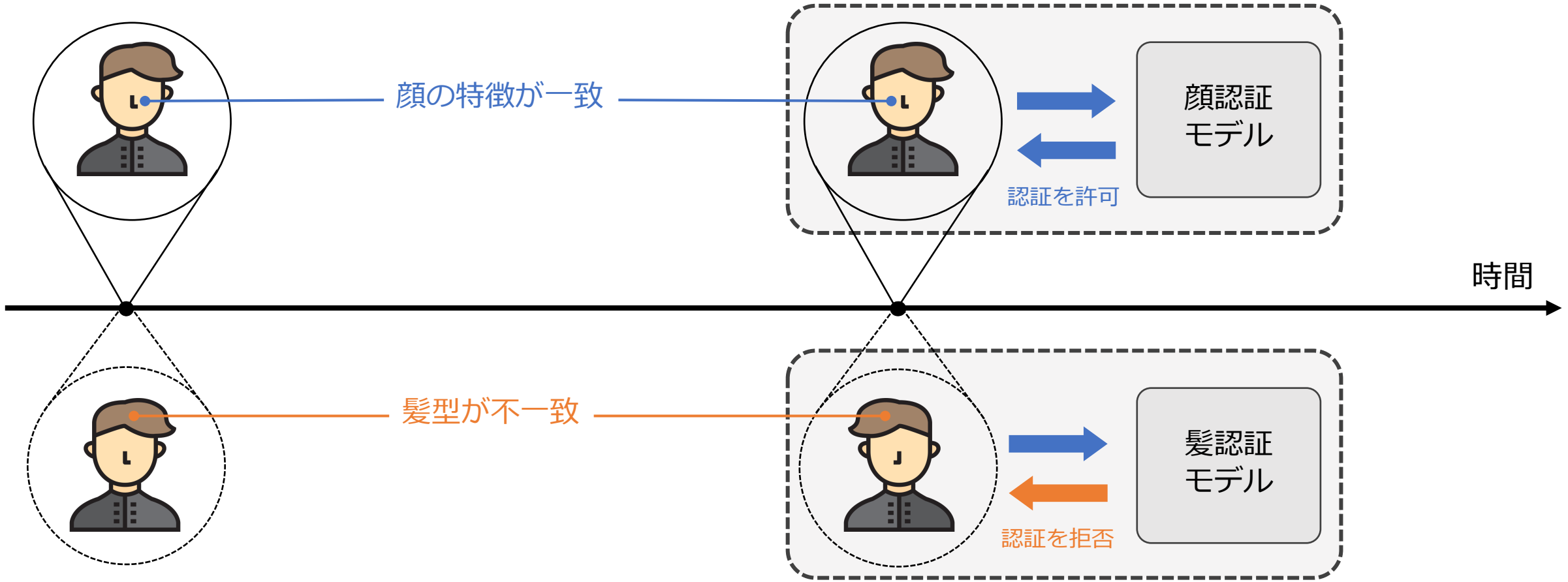
生体特徴が時間の変化に対して一定性（不変性）を持つことが重要.



生体情報の不変性

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．

顔の特徴は時間的不変性があるため時間が経っても認証精度を維持できる．

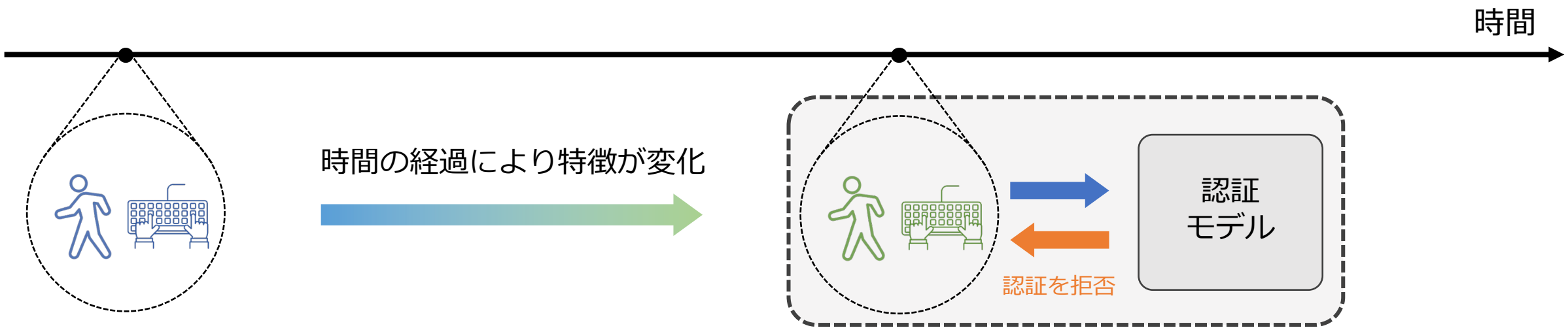


髪の特徴は時間的に変化するため時間が経つと認証精度が低下する．

生体情報の時間変化

生体情報は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.

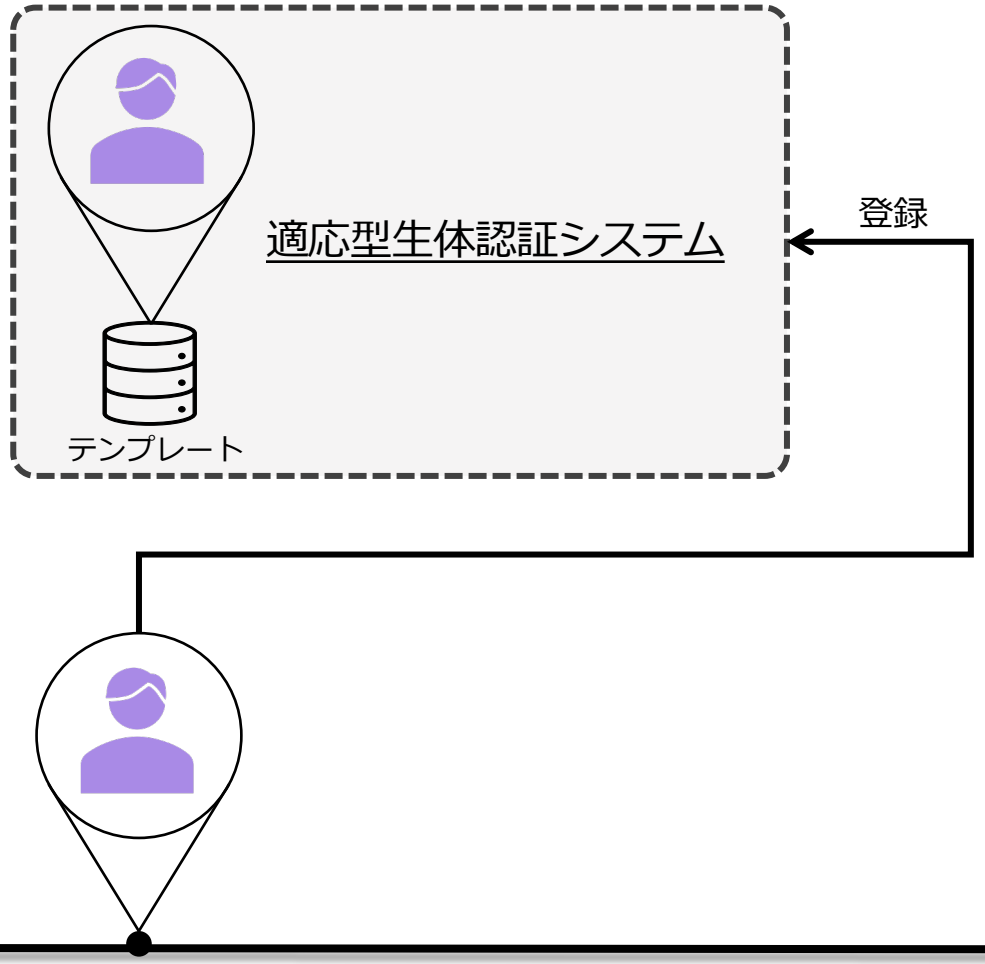
- 生体情報は時間の経過とともに特徴が変化することが知られている[1].
- 特に，歩容[2]やタイピング[3]などの行動生体情報は時間変化が大きい.
- 時間変化による特徴の変化は，行動バイオメトリクスにおける主要な問題の1つ.



[1] Dae Yon Hwang, et al., Variation-Stable Fusion for PPG-Based Biometric System, ICASSP, 2021.
[2] Claudio Filipi Gonçalves dos Santos, et al., Gait Recognition Based on Deep Learning: A Survey, ACM Computing Surveys, 2022.
[3] Jugurta Montalvão, et al., Contributions to Empirical Analysis of Keystroke Dynamics in Passwords, Pattern Recognition Letters, 2015

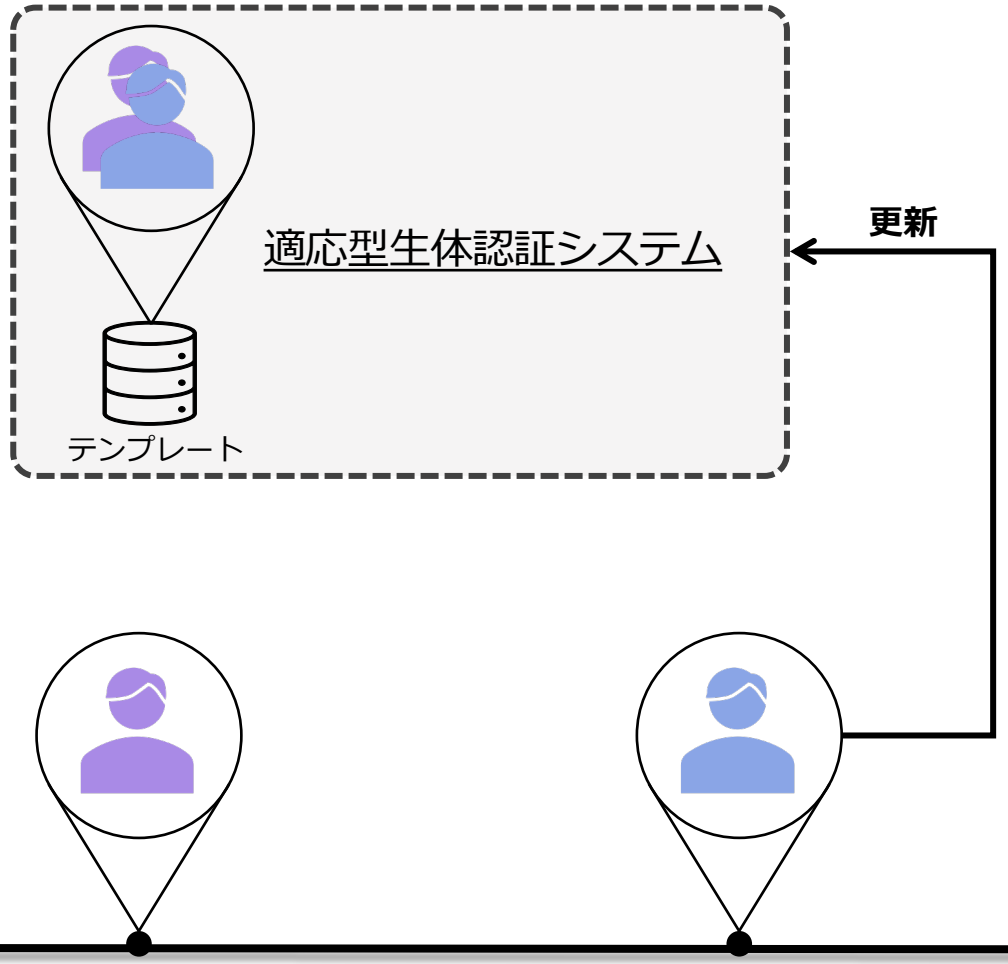
適応型生体認証：生体情報の時間的変化に対応する

時間の経過とともにテンプレートやモデルを自動的に更新して生体情報の変化に対応する.



適応型生体認証：生体情報の時間的変化に対応する

時間の経過とともにテンプレートやモデルを自動的に更新して生体情報の変化に対応する.



更新処理：

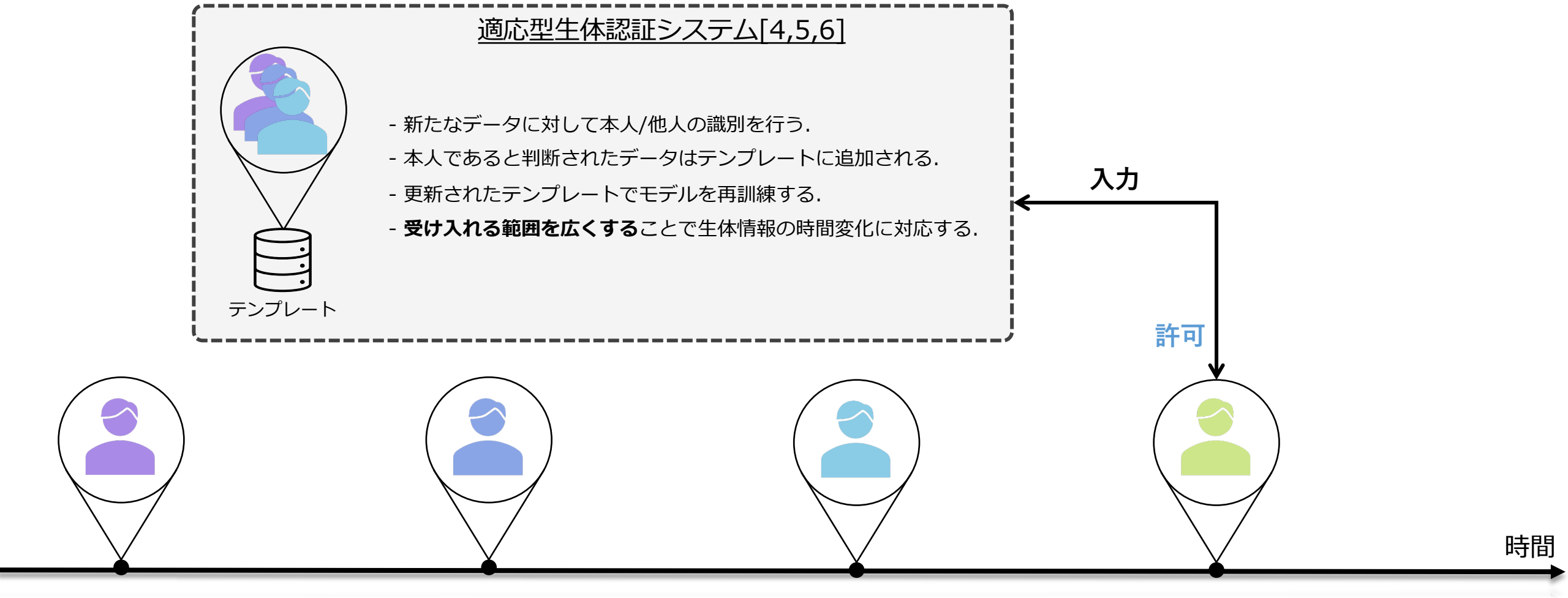
- 新たなデータに対して本人/他人の識別を行う.

- 本人であると判断されたデータはテンプレートに追加される.

- 新たなデータと元のデータでモデルを再訓練する.

適応型生体認証：生体情報の時間的変化に対応する

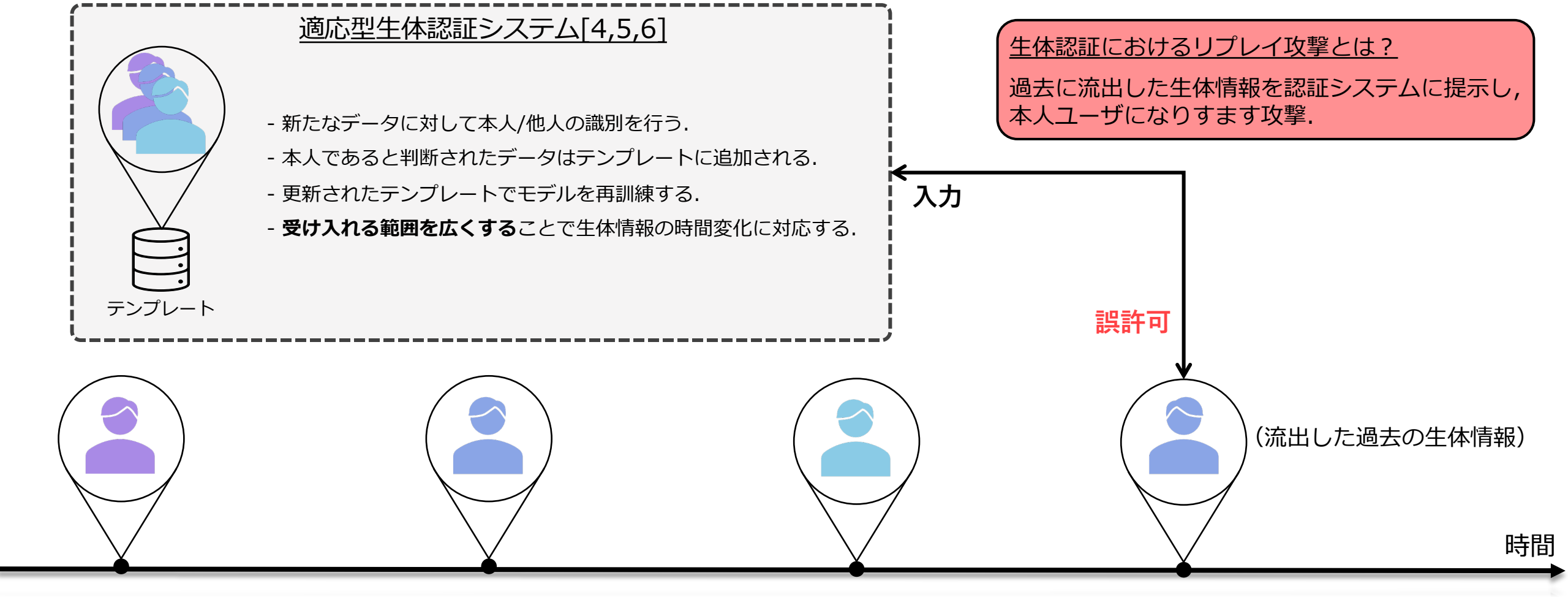
時間の経過とともにテンプレートやモデルを自動的に更新して生体情報の変化に対応する



[4] Paulo Henrique Pisani, et al., Adaptive Biometric Systems: Review and Perspectives, ACM Computing Surveys, 2019
[5] Zhihao Shen, et al., IncreAuth: Incremental Learning based Behavioral Biometric Authentication on Smartphones. IEEE Internet of Things Journal, 2023
[6] X. Yu, et al., ThumbUp: Identification and Authentication by Smartwatch using Simple Hand Gestures, IEEE PerCom, 2020

適応型生体認証：生体情報の時間的変化に対応する

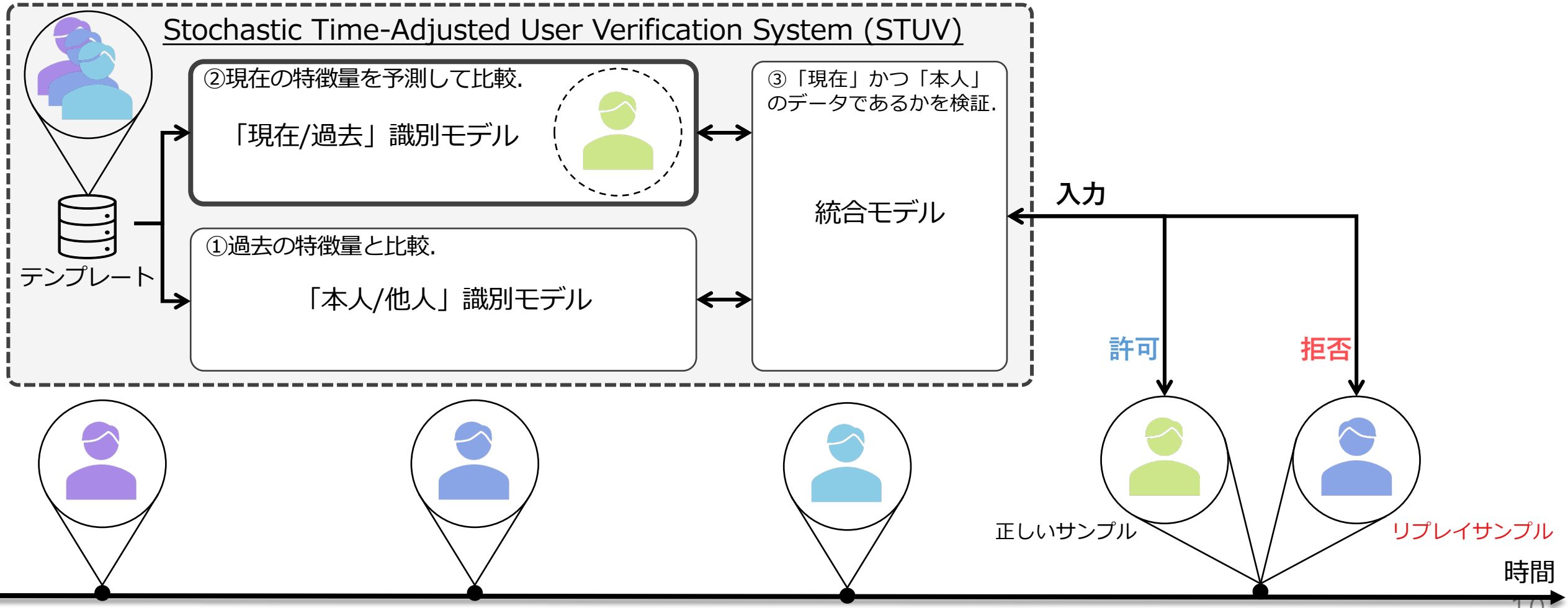
過去の生体情報を受け入れる特性により，リプレイ攻撃に対する脆弱が生まれる．



[4] Paulo Henrique Pisani, et al., Adaptive Biometric Systems: Review and Perspectives, ACM Computing Surveys, 2019
[5] Zhihao Shen, et al., IncreAuth: Incremental Learning based Behavioral Biometric Authentication on Smartphones. IEEE Internet of Things Journal, 2023
[6] X. Yu, et al., ThumbUp: Identification and Authentication by Smartwatch using Simple Hand Gestures, IEEE PerCom, 2020

提案手法

生体情報が時間的に変化することを考慮してリプレイ攻撃を防ぐ認証手法を提案する.



STUV

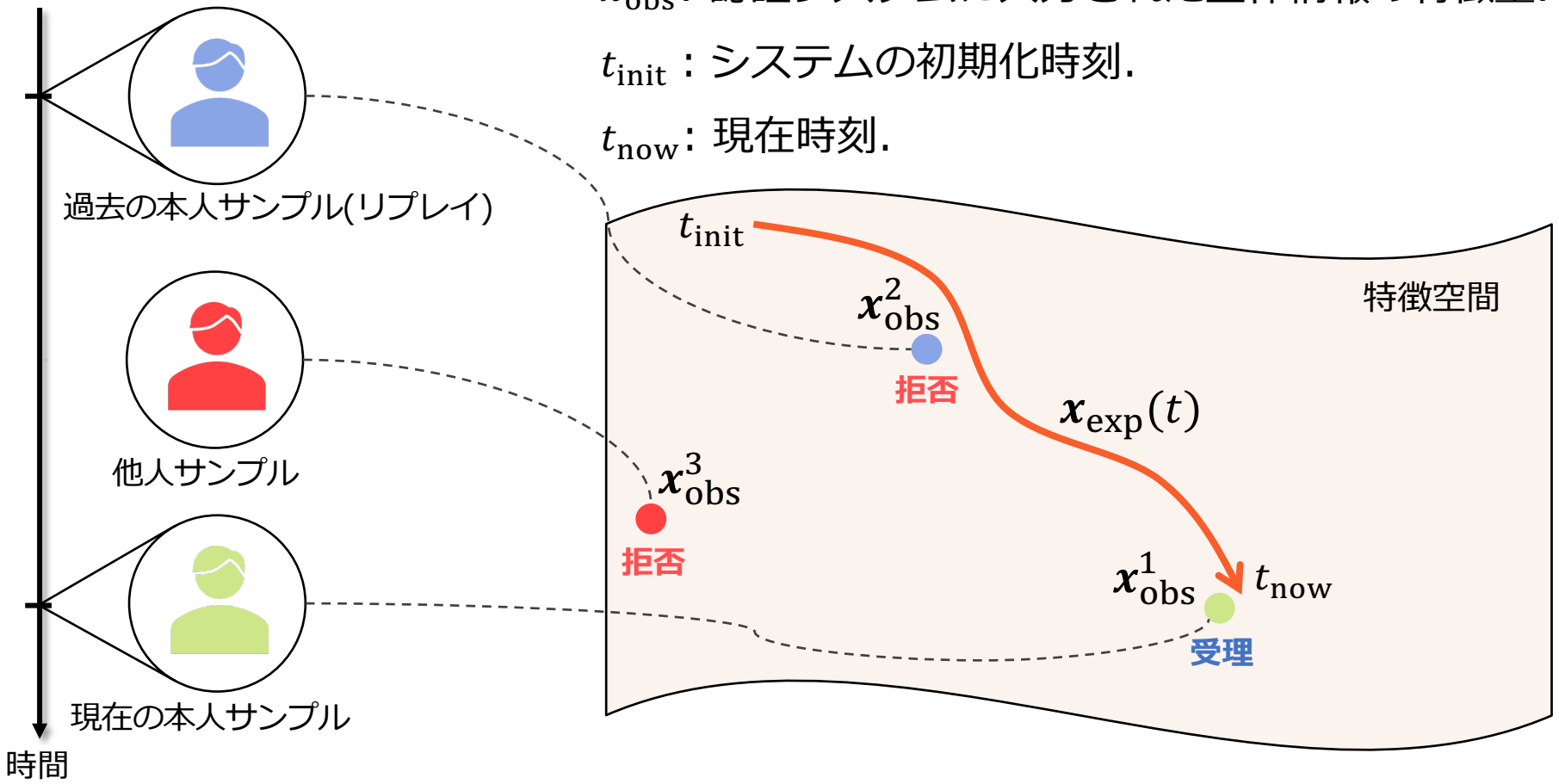
現在の本人サンプルの特徴量のみを受理するモデルを構築する.

$\boldsymbol{x}_{\mathrm{exp}}(t)$：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(特徴量推移曲線).

$\boldsymbol{x}_{\mathrm{obs}}$：認証システムに入力された生体情報の特徴量.

t_{init}：システムの初期化時刻.

t_{now}：現在時刻.



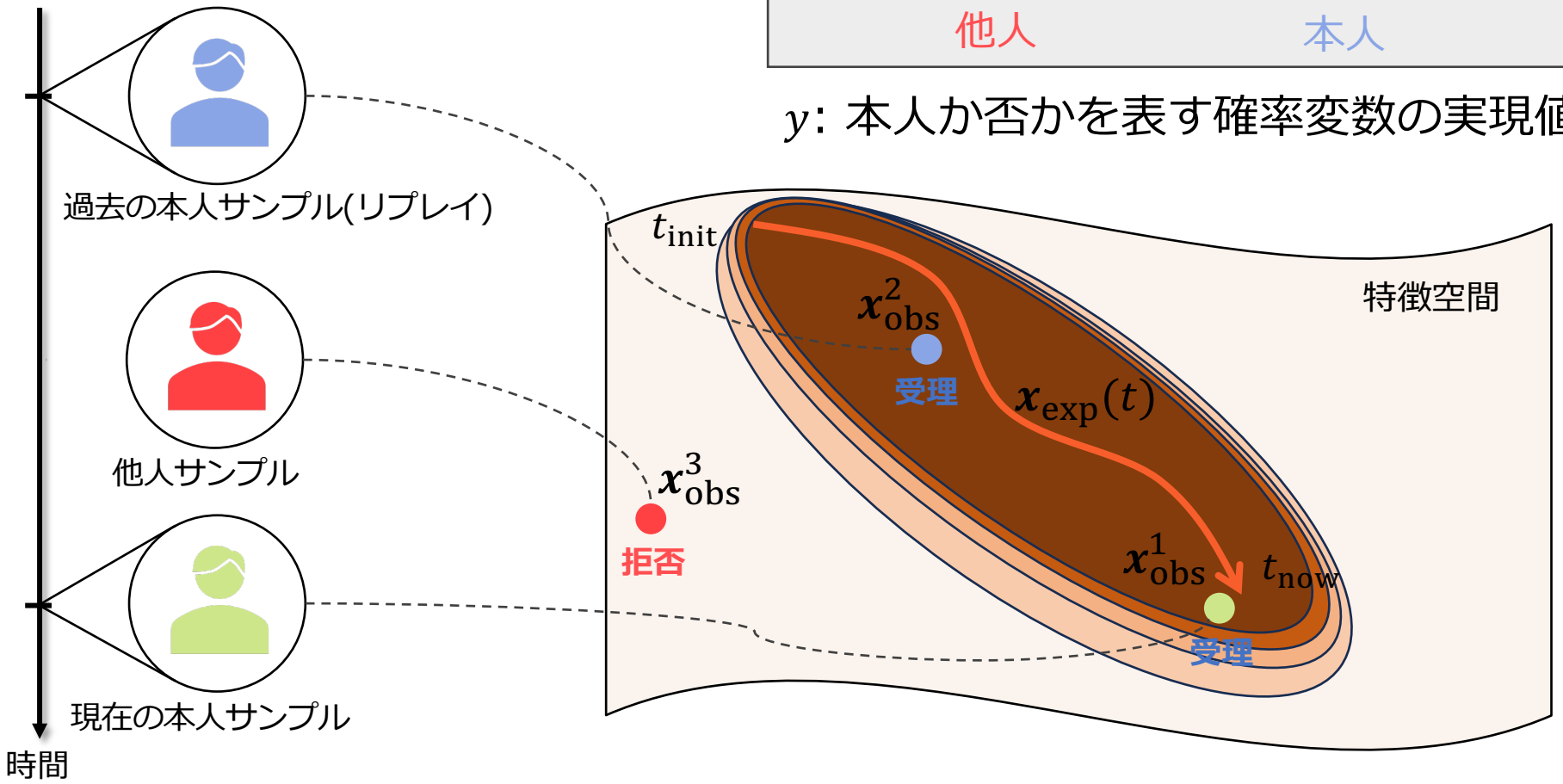
STUV：「他人/本人」識別モデル

「他人/本人」識別モデルは過去の本人サンプルに対しても高い確率を返す.

$$\mathrm{P}(y=1|\boldsymbol{x}^3_{\mathrm{obs}}) < \mathrm{P}(y=1|\boldsymbol{x}^2_{\mathrm{obs}}) \approx \mathrm{P}(y=1|\,\boldsymbol{x}^1_{\mathrm{obs}})$$

他人　　本人　　本人

y: 本人か否かを表す確率変数の実現値 (1:本人，0:他人).



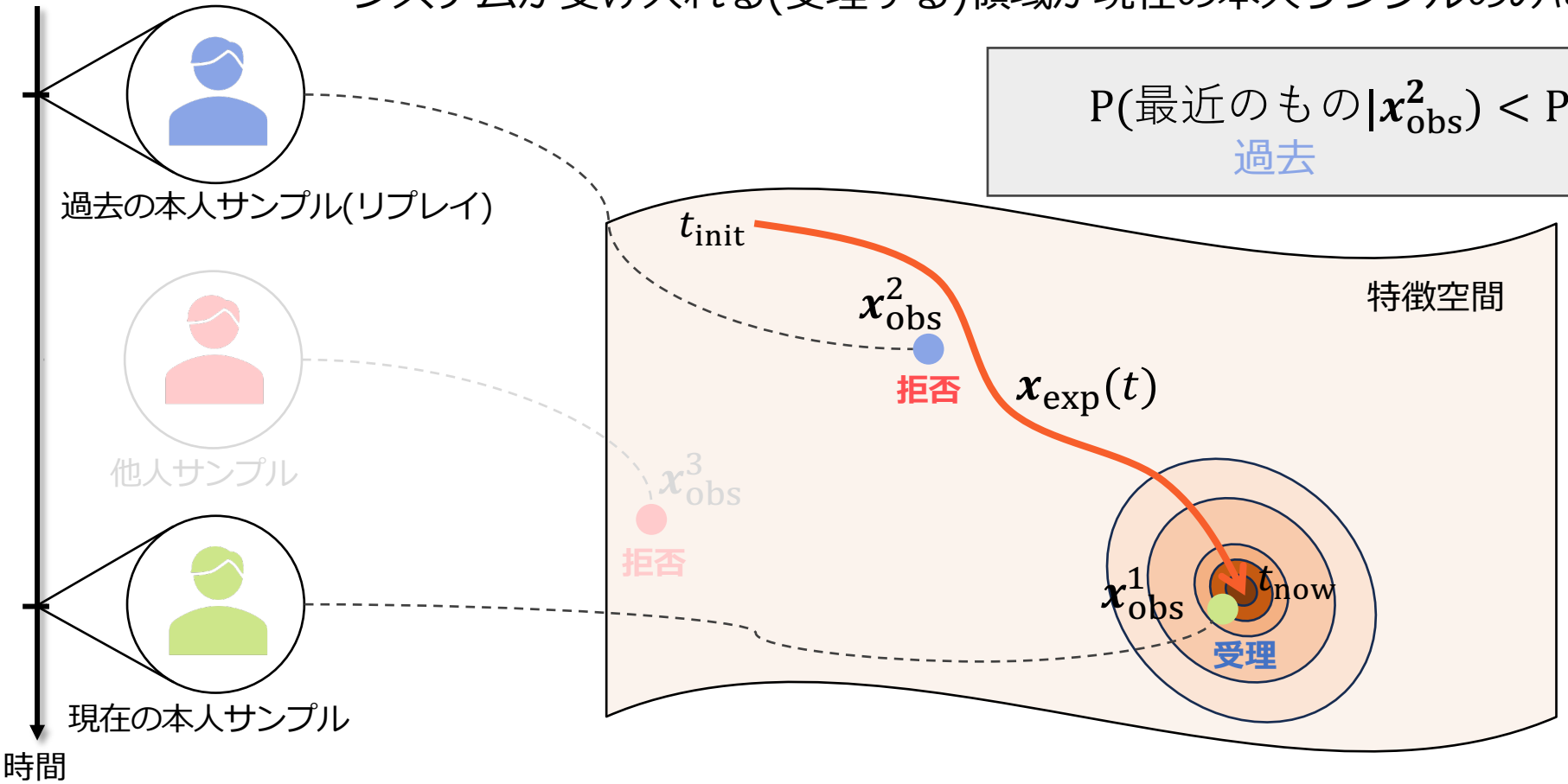
STUV：「現在/過去」識別モデル

現在の本人サンプルの特徴量のみを受理するモデルを構築する.

- 本人のサンプルに着目して現在と過去を区別したい.
- システムが受け入れる(受理する)領域が現在の本人サンプルのみになるように調整.

$$\mathrm{P}(\text{最近のもの}|\boldsymbol{x}^{\mathbf{2}}_{\mathrm{obs}}) < \mathrm{P}(\text{最近のもの}|\,\boldsymbol{x}^{\mathbf{1}}_{\mathrm{obs}})$$

過去　　現在

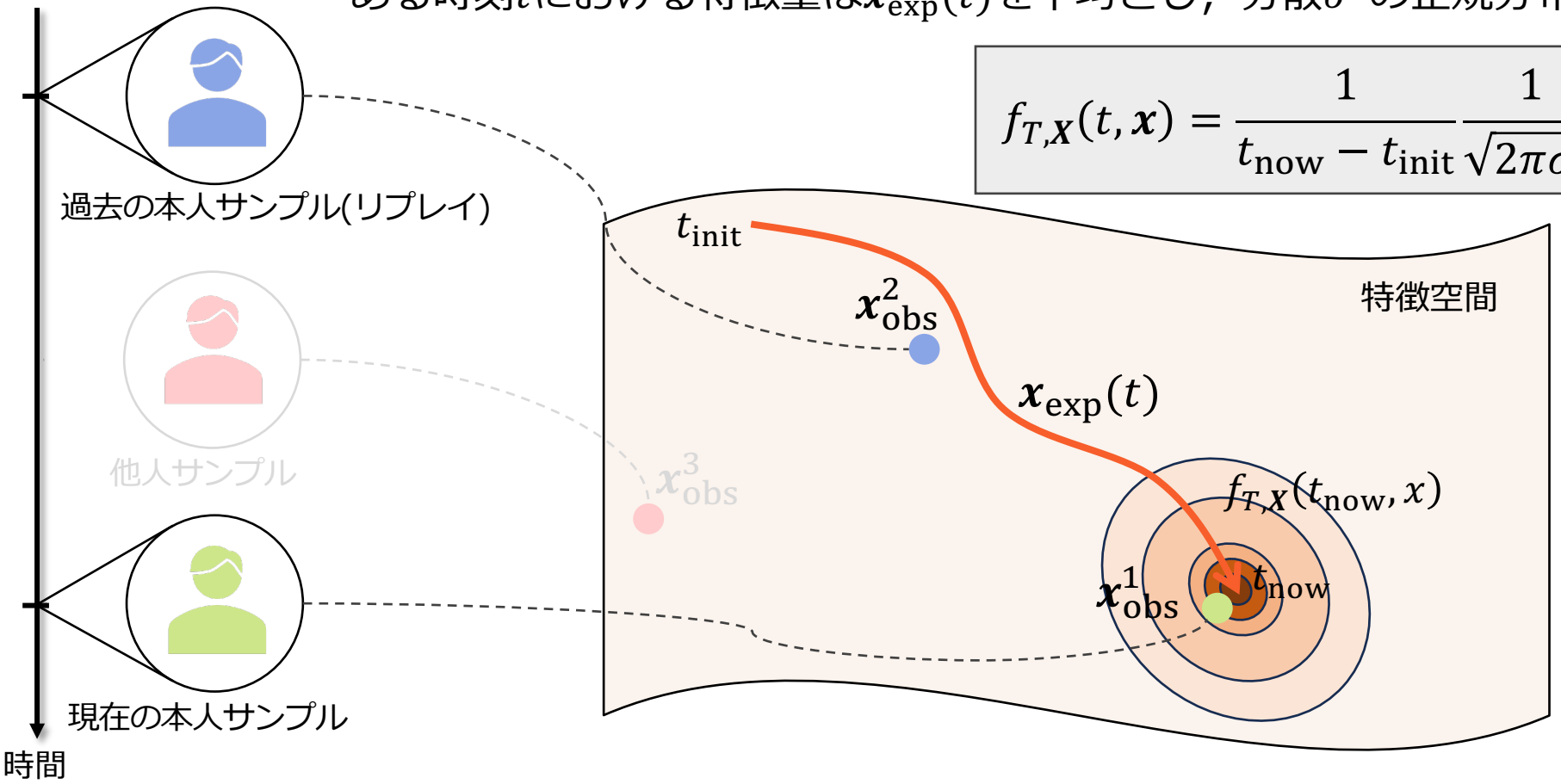


STUV：「現在/過去」識別モデル

時刻と特徴量の同時確率密度関数を以下のように仮定する.

- 特徴量の到着がポアソン過程で仮定すると，到着時刻はt_{init}からt_{now}までの一様分布に従う.
- ある時刻tにおける特徴量は$\boldsymbol{x}_{\mathrm{exp}}(t)$を平均とし，分散$\sigma^2$の正規分布に従うと仮定する.

$$f_{T,X}(t,\boldsymbol{x}) = \frac{1}{t_{\mathrm{now}} - t_{\mathrm{init}}} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(\frac{||\boldsymbol{x} - \boldsymbol{x}_{\mathrm{exp}}(t)||}{\sigma^2}\right)$$

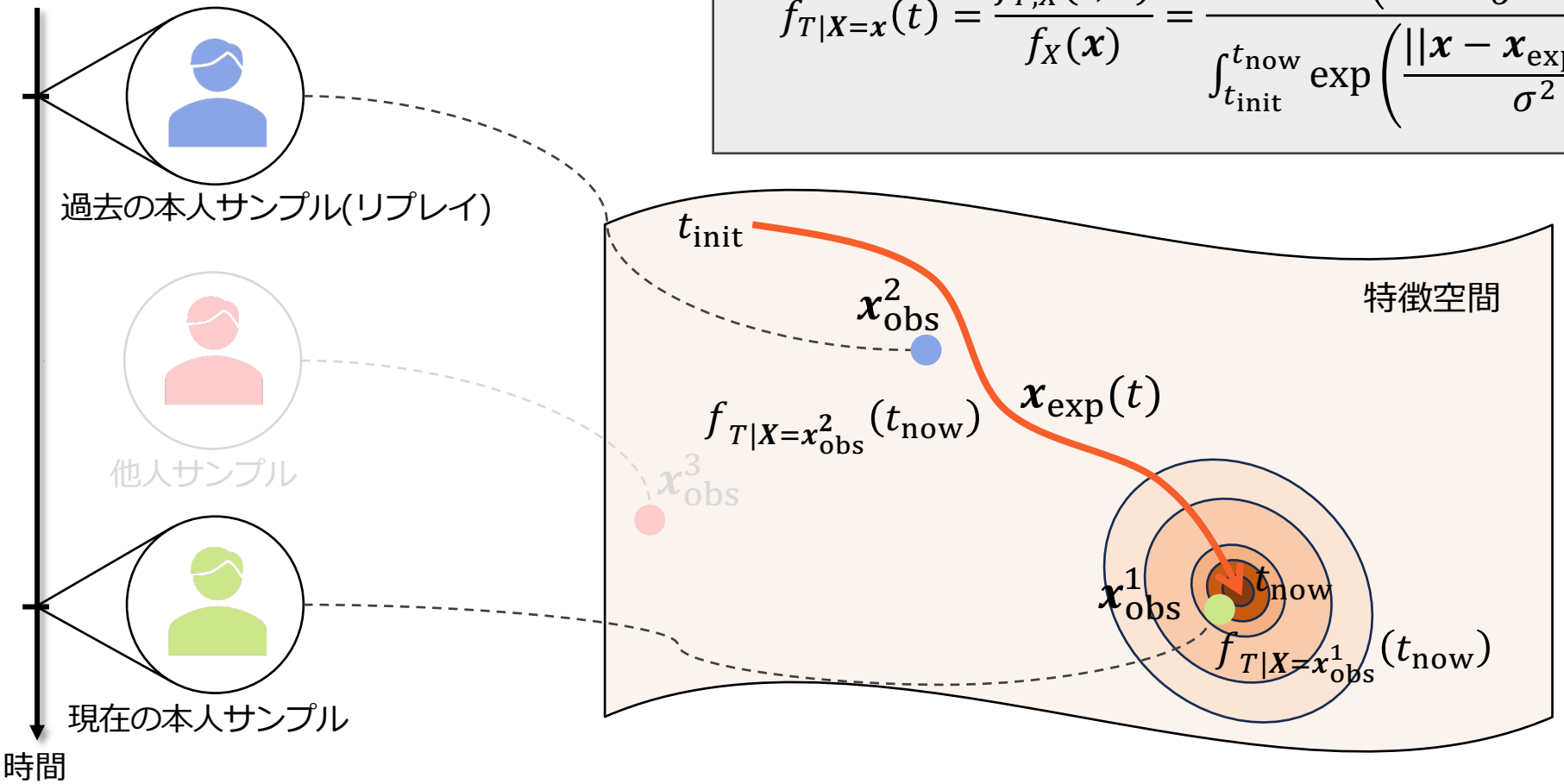


STUV：「現在/過去」識別モデル

特徴量が得られた時刻の条件付き確率密度関数を求める.

$$f_{T|X=x}(t) = \frac{f_{T,X}(t,x)}{f_X(x)} = \frac{\exp\left(\frac{||x - x_{\exp}(t)||}{\sigma^2}\right)}{\int_{t_{\text{init}}}^{t_{\text{now}}} \exp\left(\frac{||x - x_{\exp}(t')||}{\sigma^2}\right) dt'}$$

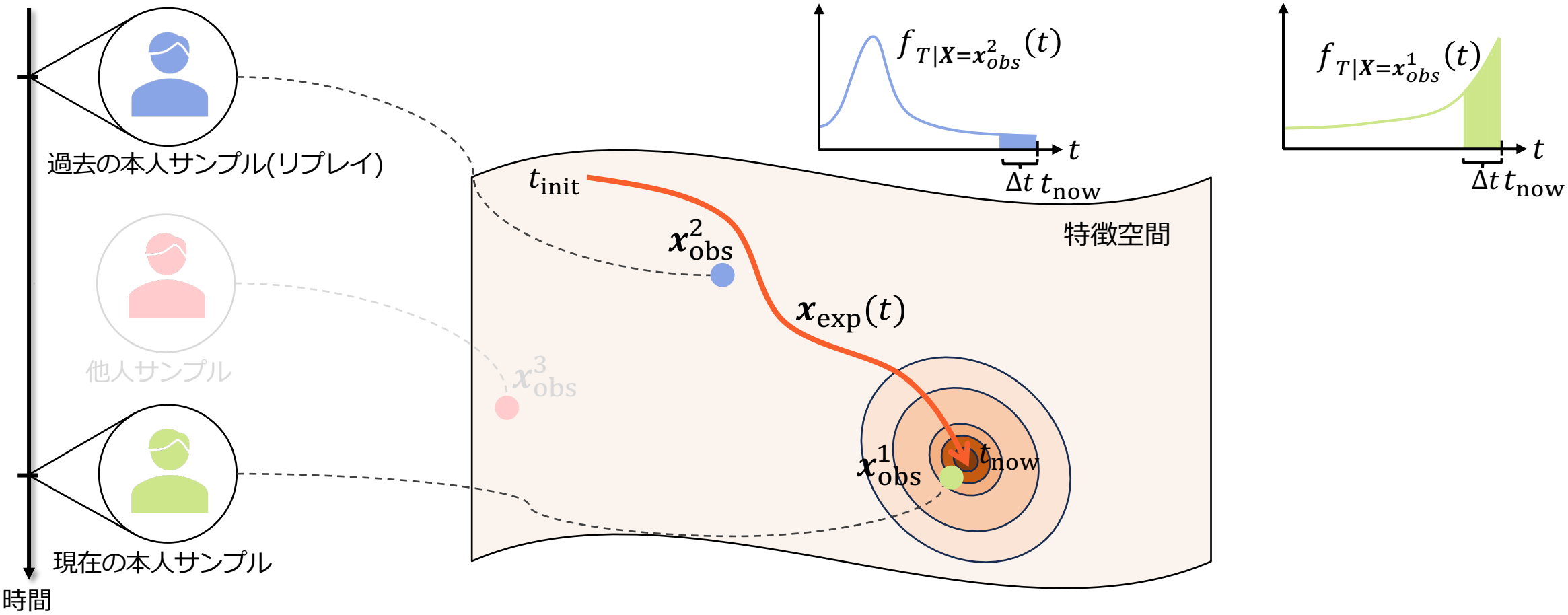
※確率の乗法定理



STUV：「現在/過去」識別モデル

条件付き確率密度関数から特徴量が最近に生成された確率を求める.

- 観測された特徴量がどの時刻に生成されたかを表す確率密度.
- 特徴量が最近に生成された確率とは，それが現在時刻t_{now}からΔt前までの間に生成された確率.

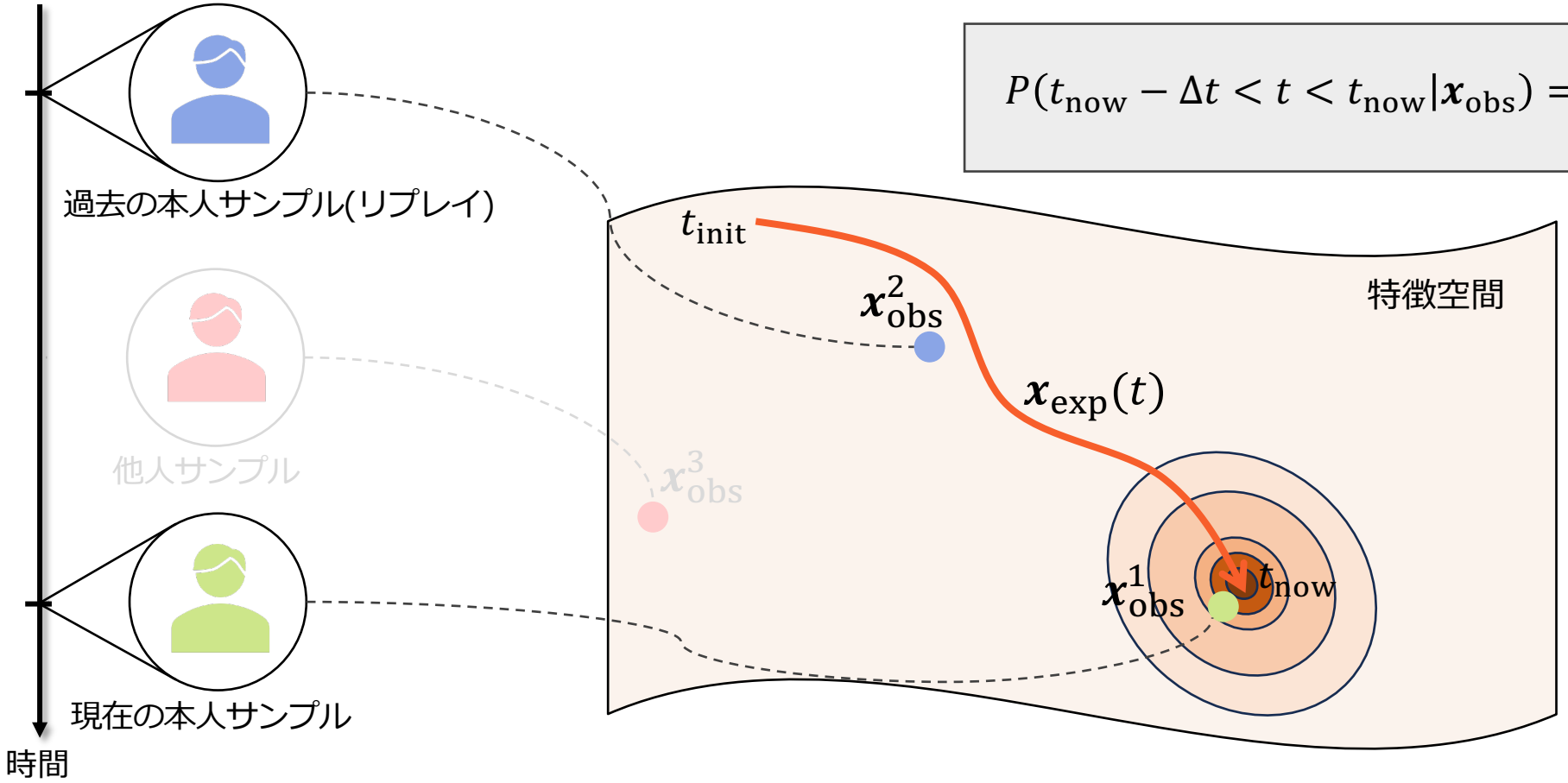


STUV：「現在/過去」識別モデル

条件付き確率密度関数から特徴量が最近に生成された確率を求める.

- 観測された特徴量がどの時刻に生成されたかを表す確率密度.
- 特徴量が最近に生成された確率とは，それが現在時刻t_{now}からΔt前までの間に生成された確率.

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



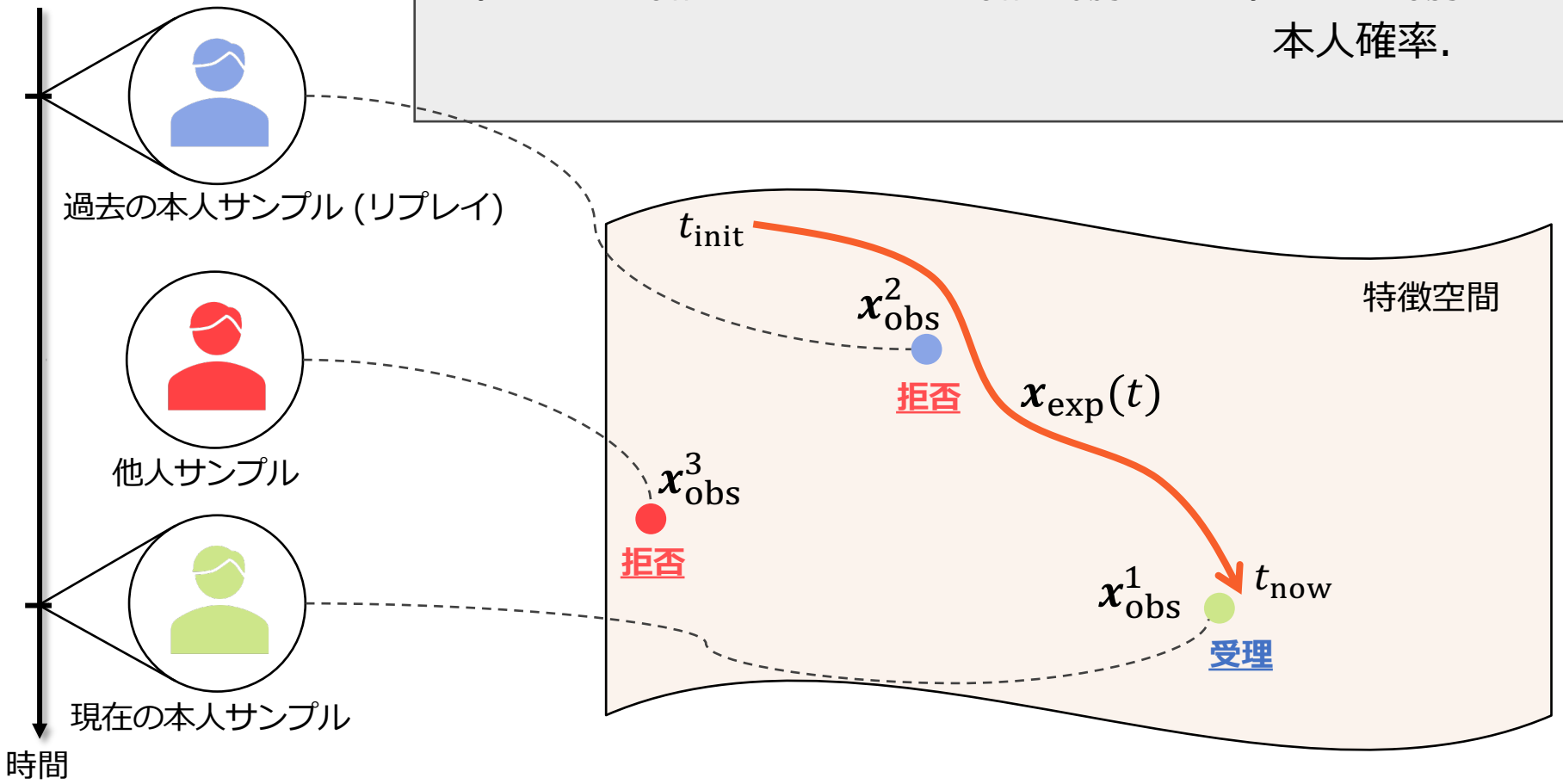
STUV：統合モデル

同時確率から特徴量が本人のものかつ最近に生成されたものである確率を求める.

yとtが独立であると仮定すると,

$$\mathrm{P}(y=1, t_{\mathrm{now}}-\Delta t<t<t_{\mathrm{now}}|\boldsymbol{x}_{obs})=\mathrm{P}(y=1|\boldsymbol{x}_{\mathrm{obs}})\times \mathrm{P}(t_{\mathrm{now}}-\Delta t<t<t_{\mathrm{now}}|\boldsymbol{x}_{\mathrm{obs}})$$

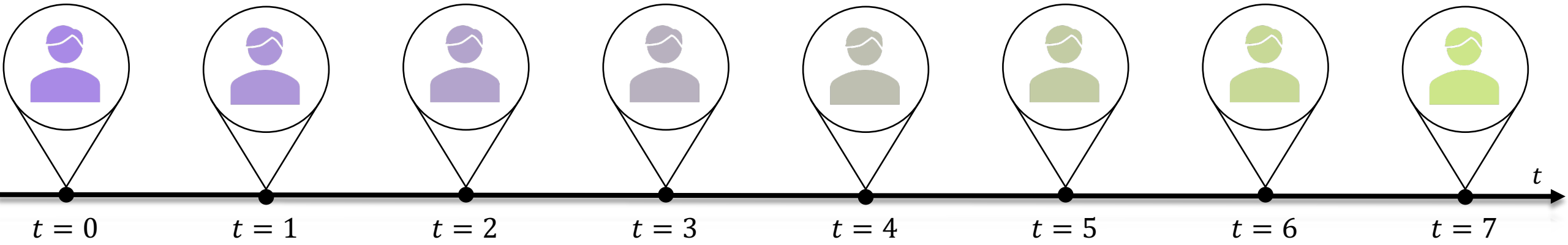
本人確率.　　最近に生成された確率.（現在確率）



実験

キーストローク認証のデータセットを使ってSTUVが効果的にリプレイ攻撃を防げるかを検証する.

- CMU Keystrokeデータセット[6].
  - キーストロークのタイミング情報.
  - 被験者51人.
  - **8セッション**(session:1-2day).
  - 1セッションあたり50回.
- 特徴抽出.
  - Robust Scalerによる標準化.
- 「本人／他人」識別モデル
  - ニューラルネットワーク．ネットワーク構造は[7,8]と同様に(31 dim,64 dim, 128dim, 64dim, 2dim)とした.

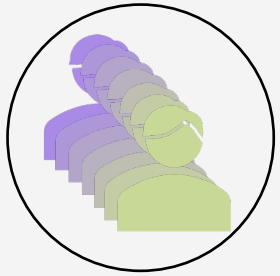


[6] Kevin S. Killourhy and Roy A. Maxion, Comparing anomaly-detection algorithms for keystroke dynamics, IEEE/IFIP International Conference on Dependable Systems Networks, 2009
[7] Blaine Ayotte, et al., Group Leakage Overestimates Performance: A Case Study in Keystroke Dynamics, CVPR Workshops, 2021
[8] Yasin Uzun and KemalBicakci., As econd look at the performance of neural networks for keystroke dynamics using a publicly available dataset, Computers Security, 2012

実験

実験シナリオ.

STUV



- 現在時刻は$t_{\mathrm{now}} = 7$.
- 「最近」の範囲を決めるΔtは0.2に設定.
- $t = 0$から$t = 6$までのテンプレートを用いて学習.
- カーネルリッジ回帰により特徴量推移曲線を近似.

実験

比較対象の手法.

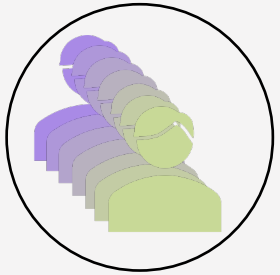
通常の適応型認証システム

- 「他人/本人」識別器のみ.
- 過去の全て($t = 0$~6)のテンプレートを用いて学習.
- 全ての本人データは取得時刻によらず同一のラベル.

忘却型の認証システム

- 「他人/本人」識別器のみ.
- 最新時刻($t = 6$)のテンプレートのみを用いて学習.
- 全ての本人データは同一のラベル.

STUV（提案手法）

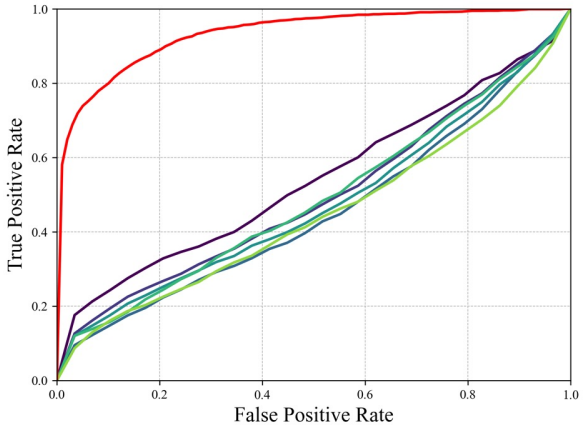


- 「他人/本人」識別器と「現在/過去」識別器を利用.
- 過去の全て($t = 0$~6)のテンプレートを用いて学習.
- 現在の本人データとその他のデータ分類.

結果

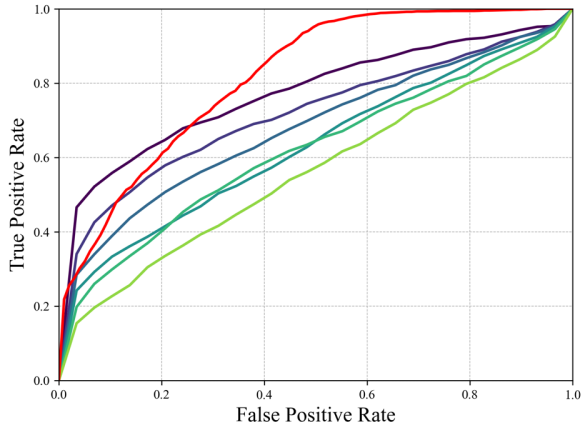
STUVは従来手法よりも効果的にリプレイ攻撃を検知することができる.

「他人/本人」の識別精度は高いが,
リプレイ攻撃を検知できていない.



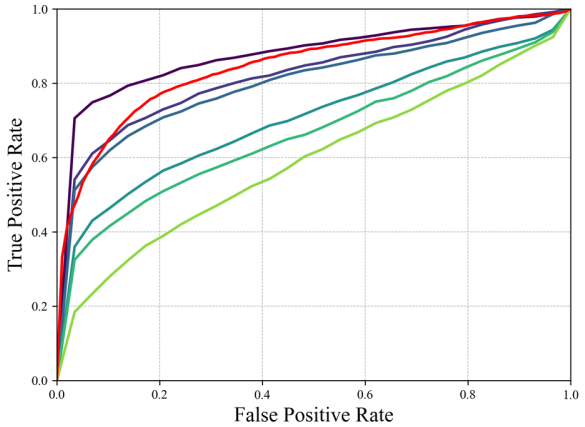
通常の適応型認証システム

リプレイ攻撃は検知できているが,
STUVほど性能(ROC)は良くない.



忘却型の認証システム

「他人/本人」の識別精度をなるべく維持しつつリプレイ攻撃を忘却型よりも高精度に検知した.



STUV（提案手法）

imposter vs genuine(t=7)　t=0 vs t=7　t=1 vs t=7　t=2 vs t=7　t=3 vs t=7　t=4 vs t=7　t=5 vs t=7　t=6 vs t=7

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

議論

適用可能性.

➢ 現在モバイルデバイスで主流となっている顔認証にも適用できるか？

- 従来の顔認証は髪の毛などはマスクされ，モデルからは見えなくなる.
- 新たに髪の毛など時間的に変化する情報に着目することで本手法を適用し，
  リプレイ攻撃に対して認証システムをよりロバストにできる可能性がある.

➢ STUVにはどのような特徴量が必要か？

- 既存の特徴量は時間変化が小さい部分に着目する(不変性).
- STUVには，これまでとは逆に時間変化が大きい部分に着目する特徴量が必要になる.

まとめ

- 生体認証と経時変化.
  - 一般に，生体認証の根拠となる生体情報には，ある程度の不変性が必要である.
  - しかし，実際には，生体情報は心理状態や生活習慣などにより日々緩やかに変化することが知られている（例：歩容，タイピング）.
- 提案手法：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.
  - 従来手法は，不変性を仮定することにより，過去に流出したデータを用いたリプレイ攻撃などを検知できない.
  - 提案手法(STUV)は，生体情報の経時変化特性を考慮し，提示されたデータが「現在」かつ「本人」のものである確率を計算する.
- リプレイ攻撃を検知する性能の評価.
  - キーストローク認証を対象としてSTUVの性能を評価した.
  - その結果，既存の「他人/本人」識別モデルの精度を維持しつつ，従来手法よりも効果的にリプレイ攻撃を検知できることが示された.
- 適用可能性.
  - STUVは，特に，時間変化する生体情報を利用した認証で有効である.
  - 従来の特徴量とは逆に，時間変化する生体特徴を抽出することでさらにモデルをロバストにできる.