正当性検証を備えた脈波認証

令和5年 3月

日夏 俊

正当性検証を備えた脈波認証

博士（工学）論文提出先
大阪大学大学院基礎工学研究科

令和5年 3月

日夏 俊

正当性検証を備えた脈波認証

日夏 俊

内容梗概

多様なサイバ攻撃への対策を施すことは，現代社会における重要な課題である．代表的な攻撃の一つとして対象者のなりすましが挙げられるが，その典型的な対策方法はパスワード入力等の認証である．しかし，認証後に対象者が離れた際に，攻撃者が対象者になりすます可能性がある．以上の状況への対策として，認証を繰り返す “継続認証” が求められている．継続認証の実現のため，光電容積脈波 (以下脈波と記す) を利用した認証手法 (脈波認証) が提案されている．脈波は心身状態の推定にも利用可能であるため，個人および心身の状態に応じたサービス提供を，脈波認証とともに 1 個のセンサを用いて実現できる可能性がある．しかし，他の生体認証手法と同様に，脈波認証に対する攻撃が行われる可能性があるため，脈波認証に対して起こり得る攻撃を検討し，同時に対策も検討することが必要である．

本研究では，攻撃対策を備えた脈波認証システムの開発を目的として，脈波認証に対して起こり得るなりすまし攻撃を検討し，同攻撃への対策を提案する．検討する攻撃は，脈波が身体上の様々な部位で計測可能であることに着目する．脈波認証デバイスにより特定の部位で計測される，認証に必要な情報は漏洩しており，別の部位からも計測される可能性を仮定する．同攻撃は，脈波認証デバイスによる計測部位とは別の部位から，被害者に気づかれないように不正に計測した脈波を利用する．続いて，計測した脈波を基に攻撃用の信号を生成し，脈波認証デバイスに入力することで認証の突破を目指す．さらに，同攻撃への対策として，高い搭載性を実現するため，他のセンサ等の要素を追加しない手法を提案する．同対策では，脈波から得られる情報が計測部位毎に異なることに着目し，計測部位を識別することで，入力信号の正当性を検証し，攻撃を検出する．

認証に必要な情報の漏洩を検証するため，身体上の複数部位において脈波計測可能な装置 (脈波計測装置) を構築した．脈波計測装置を利用した実験により，実験参加者の手や指の複数部位で脈波を同時に計測した．続いて，各部位で計測された脈波から特徴量を抽出し，誤差や相関，認証や攻撃への寄与を調査した．その結果，本来の認証に必要となる，手首から得られる情報が，別の部位からも計測される可能性が示唆された．また，特徴量の組合せにより，攻撃成功率を最大 62.8 %低減可能であることが示された．

続いて，提案する攻撃の実現可能性を検証するため，脈波認証システムを試作した．同システムは，脈波計測装置と，脈波認証アルゴリズムで構成される．実験において，各参加者の手首で計測された脈波から抽出した特徴量を利用して識別器を生成して攻撃対象とし，指で計測された脈波から抽出した特徴量を同識別器に入力することで，攻撃が成功するか否かを検証した．その結果，攻撃成功率は 0.800 以上であり，センサを固定した理想的な条件下において，攻撃が成功する可能性が示唆された．

さらに，脈波認証に対するなりすまし攻撃への対策として提案した，計測部位の識別の有効性を検証した．12 名の実験参加者の 6 部位で計測した脈波のデータセットに加えて，22 名の 2 部位で計測された脈波を含む公開データセットを利用した．各データセットに含まれる脈波間の類似性を評価するとともに，各脈波から特徴量を抽出し，計測部位を識別可能か否かを検証した．その結果，計測部位の識別率は 0.800 以上であり，提案した対策が同攻撃に対して有効である可能性や，同対策は時間経過後も有効である可能性が示唆された．

本研究は，脈波の解析に基づいて，脈波認証に対する攻撃を検討し，同攻撃の実現可能性を示した．さらに，脈波の解析に基づいて同攻撃に対する対策を提案して，その有効性を示した．搭載性の優れた対策を備えた脈波認証システムにより，脈波に基づいた個人および心身の状態に応じたサービス提供を，安全に実現することが期待される．

キーワード

生体認証，無意識計測，継続認証，光電容積脈波，なりすまし攻撃，情報漏洩，検証

Photoplethysmographic Authentication with Correctness Verification

Shun Hinatsu

Abstract

It is important to implement countermeasures against various cyber attacks such as identity spoofing. A typical countermeasure against the spoofing is an authentication such as inputting passwords. However, after the successful authentication, an attacker may take over while a genuine user is absent. "Continuous authentication", which requires authentication process repeatedly, is needed to cope with this situation. Several studies proposed continuous authentication using photoplethysmogram (PPG) signal used to estimate personal mind and body conditions, which could connect services based on the conditions and the authentication seamlessly with one sensor. The investigation of both the probable attacks and the countermeasures for PPG-based authentication are required in case there may be attacks against the authentication as well as other authentication.

In this study, to develop a PPG-based authentication system with countermeasures, the author investigates a presentation attack (PA) against the authentication and a countermeasure against the PA. The author focuses on the advantage of PPG signal, which can be recorded on various sites on a body, and assumes that the information required for the authentication may be leaked and recorded on non-genuine sites. The PA stealthily records PPG signals on a non-genuine measurement sites on a victim, and inputs the signal to an authentication device to pass the authentication. In addition, the author proposes a countermeasure against the PA, which utilizes the measurement-site-specific feature values in PPG signals to realize high mountability without adding any components such as other sensors. The countermeasure verifies the correctness of the input to detect the PA by identifying the measurement sites using the feature values.

The author developed a PPG recording device for multiple measurement sites, and recorded PPG signals on participants. The author investigated the error and correlation between feature values extracted from the signals, and assessed the contribution of each value to the authentication and the PA. The result indicated that the information required for authentication, which was originally from the wrist, can be acquired from other sites. The result also showed that the feature value selection could reduce the feasibility of the PA up to 62.8 %.

The author developed a prototype of PPG-based authentication system comprising of the recording device and an authentication algorithm to investigate the feasibility of the PA. The author input the feature values extracted from the PPG signals recorded on the finger to the classifier generated by the values from the signals on the wrist as the genuine site. The result indicated that the PA could occur under an ideal condition with the probability more than 0.800; the sensors were stabilized on the bodies.

After that, the author investigated the identification of the PPG measurement sites as the countermeasure against the PA by using two datasets including PPG signals recorded at multiple measurement sites on total 34 participants. The author evaluated the similarity between the PPG signals, and investigated the feasibility of the measurement site identification by using the feature values extracted from the signals. The result indicated that the countermeasure could be effective against the PA regardless of the elapsed time with the probability more than 0.800.

In this study, the author predicted the PA against PPG-based authentication, and investigated the feasibility of the PA based on the analysis of the PPG signals. The author proposed the countermeasure against the PA, and investigated its feasibility based on the analysis of the PPG signals. PPG-based authentication system with the high mountable countermeasure is expected to realize several services safely for personal mind and body based on PPG measurement.

Keywords:

Biometric authentication, Unconscious measurement, Continuous authentication, Photoplethysmogram, Presentation attack, Information leakage, Verification

目 次

図 目 次

表 目 次

第1章

はじめに

人間は，自分以外の他者と関わりを持ち，集団や社会を形成している．その中では，自分と他者との間において，情報伝達が行われる [1]．古代では，情報伝達の方法は，他者と対面した状態で，音声や身振り手振り，文字や絵の使用が主な手段であった．19 世紀以降は，電報や電話の発達により，遠隔地に居る人間同士でも一対一の情報伝達が行えるようになった [2]．また，20 世紀以降は，ラジオやテレビの発達により，一つの場所から遠隔地にいる多数の人間に対して情報伝達が行われるようになった [2]．さらに，1990 年代以降はインターネットおよびインターネットを利用できる個人端末が普及し，人数や伝達の方向を問わず，遠隔地に居る人間同士でも情報伝達が可能となっている [3,4]．インターネットの普及以前の情報伝達は，即時実施可能という利点があり，現在でも緊急時の連絡等の目的では重宝されることが多い [5]．しかし，人数や伝達の方向に加えて，内容に制限があり，一対一の会話や，特定の人間からの情報発信等が中心であった [6]．一方，インターネットの普及以後は，人数や伝達の方向，内容を問わない情報伝達が可能となっている．例えば，インターネット上における，不特定多数の人間に向けた商品販売等のサービスも実現されている [7]．2020 年以降は，新型コロナウィルスの感染拡大による外出制限に伴い，インターネット上において自宅から参加可能な一対多の授業や，多人数が参加する会議も普及している [8,9]．

しかし，インターネットの普及以後は，悪意を持つ者，すなわち，攻撃者 (Attacker) が，伝達される情報の窃取等を目的として，情報伝達技術の利便性を悪用し，特定の人物，いわゆる，被害者 (Victim) に不利益を生じさせることがある [10]．様々なサイバ攻撃への対策を施すことは，ネットワークを介して様々なサービスが提供される現代社会における重要な課題である．以下では，サイバ攻撃への対策を分類し，その中の一つの対策における課題を明らかにする．

1.1 サイバ攻撃への対策

一般的に，サイバ攻撃への対策は，以下の 3 種類に大別される [11, 12].

- サイバ攻撃の発生前に実施する，情報の暗号化，対象者の認証等の “予防”
- サイバ攻撃の発生後に実施する，通信遮断，状態回復等の “対応”
- サイバ攻撃の発生時に実施する，記録・監視した通信内容を検証し，攻撃を見つけ出す “検出”

上記の 3 種類の対策は必ずしも独立したものではなく，複数の対策の組合せにより，効果が発揮される場合が多い．例えば，“対応” は，通信機器の停止等に代表される，被害者の不利益を防ぐために不可欠であるが，事前の “検出” により通信内容を検証することで，同機器の接続先の制限等，適切な対応内容の選択が可能である [13]．また，起こり得る不利益を最小限に抑えるため，対応や検出に加えて，可能な限り早い段階での対策となる，事前に “予防” を実施しておくことは重要である [14].

一方，代表的なサイバ攻撃の一つとして，個人情報等の窃取や悪用を目的として行われる，被害者へのなりすまし攻撃が挙げられる．なりすまし攻撃への典型的な対策は，同攻撃の予防となる認証を実施し，その対象者が別人ではない，正しい人物であることを検証することである [15]．認証手法は，以下の 3 種類に大別される [16].

- 対象者が，キーボードやタッチパネル等を自ら操作してパスワード等を入力する，“知識による認証”
- 対象者が所有する IC カードやハードウェアトークン等の機器を使用する，“所有物による認証”
- 対象者の指紋や顔等，身体の一部または全体をセンサに提示する，“身体的な特性による認証 (生体認証)”

上記の 3 種類の認証手法のうち，生体認証においては，認証に必要な情報を忘却したり，紛失したりする可能性がないことから [17]，急速に普及が進んでおり，顔認証機能や指紋認証機能を搭載した PC，スマートフォン等の端末が販売されている [14].

1.2 継続認証

1.1 節では，サイバ攻撃への予防として認証を実施する重要性を述べたが，対象者の認証を一度行うだけでは，対象者が認証された場所を離れたり，対象者が別人と入れ替わったりした場合の対策を行うことができない．このような事態への対策として，一度対象者の認証を行った後に，なりすまし攻撃の検出のために認証を繰り返し，検出後の遮断等の対応に繋げる “継続認証” が求められている．継続認証は，対象者に負担を課さないことや，攻撃者に気づかれないようにすること等の目的から，時間経過後に対象者が無意識の状態で実施することが望ましい．したがって，対象者の意思に基づく，キーボードを用いたパスワード入力等の知識による認証や，IC カードの提示等の所有物による認証ではなく，対象者が意識しなくても計測 (以下，無意識計測と記す) 可能である生体信号を利用した，生体認証により継続認証を実現することが望ましい [18]．一方，認証への利用が研究されている生体信号として，心電図 (ECG: Electrocardiogram) が挙げられる．現在，心電図を簡易的に計測できるウェアラブルデバイスの普及が進んでおり，心電図を認証に利用するデバイス (心電図認証デバイス) も存在する [19]．しかし，心電図計測は，特定の姿勢での計測や，身体上の計測部位等の制限，さらには国や地域によっては販売や使用の制限があり [20]，継続認証のために使用することは難しいと考えられる．

以上の課題を解決するため，本研究は，血管の挙動を光学センサを用いて計測する光電容積脈波 (PPG: Photoplethysmogram，以下脈波と記す) [21] を利用した継続認証 (脈波認証) を対象とする．脈波は，計測の簡便さから心電図の代替として利用されることが多く，心拍数 (HR: Heart rate) や呼吸数 (RR: Respiratory rate) 等の生体情報を推定し，ヘルスケア等の用途に活用される [22]．同計測は，一度身体にセンサを装着すれば姿勢を問わず無意識計測が可能であり，さらに身体の様々な部位において計測可能である．また，同計測は心電図計測とは異なり，国や地域による販売や使用の制限がないという利点もあり，手首に装着するスマートウォッチでの計測が普及している [20, 23]．さらに，計測した脈波を解析し，精神状態や，身体の特定部位の姿勢，接触力を推定する研究も存在するため [24–26]，図 1.1 に示すように，脈波計測デバイスによる認証機能の実行後，ネットワークを介して個人や心身状態に応じたサービスも提供できる可能性がある [27]．

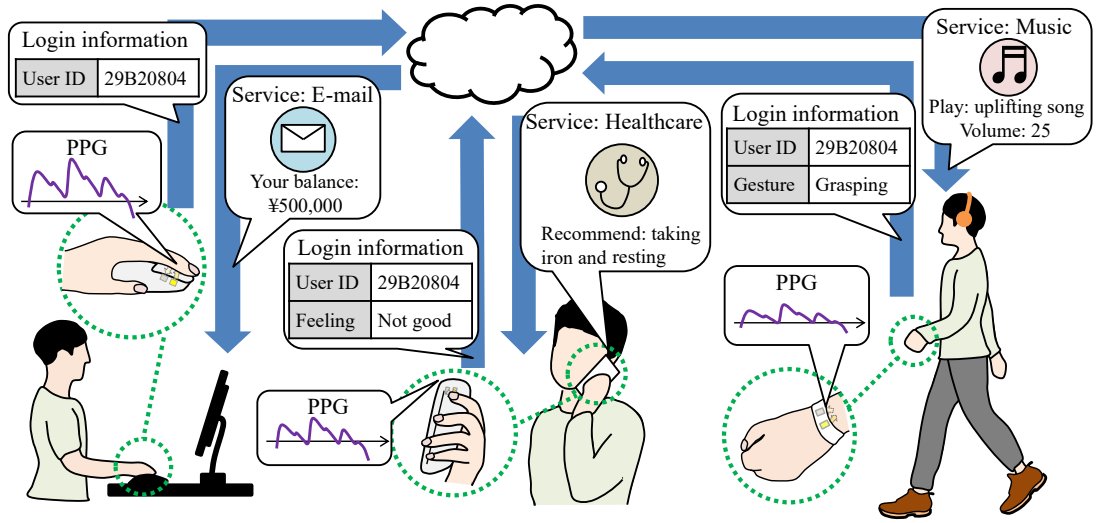


図 1.1: 脈波計測を利用した，個人および心身に適切なサービスの提供

しかし，一つの攻撃に対して，一つの対策を実行するのみでは不十分となる場合がある．例えば，なりすまし攻撃への典型的な対策である顔認証に対して，顔を計測するカメラに顔写真等の人工物を提示して認証を突破する攻撃 (PA: Presentation attack) が検討および実証されている [28]．したがって，一つの対策を実行するのみではなく，同対策に対して起こり得る攻撃を先立って検討し，追加すべき対策を検討し実行することは重要である [29]．脈波認証に対しては，脈波が身体の様々な部位において計測可能であることから，攻撃者が脈波を不正に計測および解析し，なりすまし攻撃を試みる可能性もある．したがって，本研究では，なりすまし攻撃対策を備えた脈波認証システムの実現を目的として，身体上の様々な部位で計測可能という脈波の利点に着目して起こり得るなりすまし攻撃を検討し，同攻撃への対策を提案する．攻撃者は，本来の計測部位とは別の部位から，対象者に気づかれないように脈波を不正に計測および解析し，不正に計測した脈波を基に生成した，偽の信号を脈波認証システムへ入力し，認証の突破を目指すことが考えられる．同攻撃への対策は，脈波は様々な部位で計測可能であるが，各部位で計測される波形間には差が存在することに着目する．提案する対策では，脈波を解析して得られる，各部位で計測される波形間の差を利用して，脈波認証システムへの入力の正当性を検証することで，なりすまし攻撃を “検出” し，その結果を基に “対応” を実施する．

1.3 研究の位置づけ

一般的に，生体認証システムへ搭載するなりすまし攻撃対策の一つは，センサが計測している対象が偽の入力ではなく，正当な生体であることを検証して確認することで実現される．例えば，指紋認証システムへの温度センサの追加や [30]，心電図認証デバイスへの湿度センサの追加等が提案されており [31]，認証に必要な情報とは別の情報を取得するためのセンサを要する場合が多い．一方，本研究の対象である脈波を計測して解析することで，個人や心身に適したサービスの提供，認証に加えて，なりすまし攻撃の検討，同攻撃への対策が実現できる可能性がある旨を，1.2 節で述べた．したがって，図 1.2 に示すように，脈波の解析に基づいて，サービスの提供，認証，なりすまし攻撃の検討，さらに同攻撃への対策といった複数の事項を一貫して，一つのデバイスに搭載した一つの脈波センサを基に扱える可能性がある．本研究は，脈波計測および解析により実現され得る機能の融合や拡張への先駆けとなる研究である．

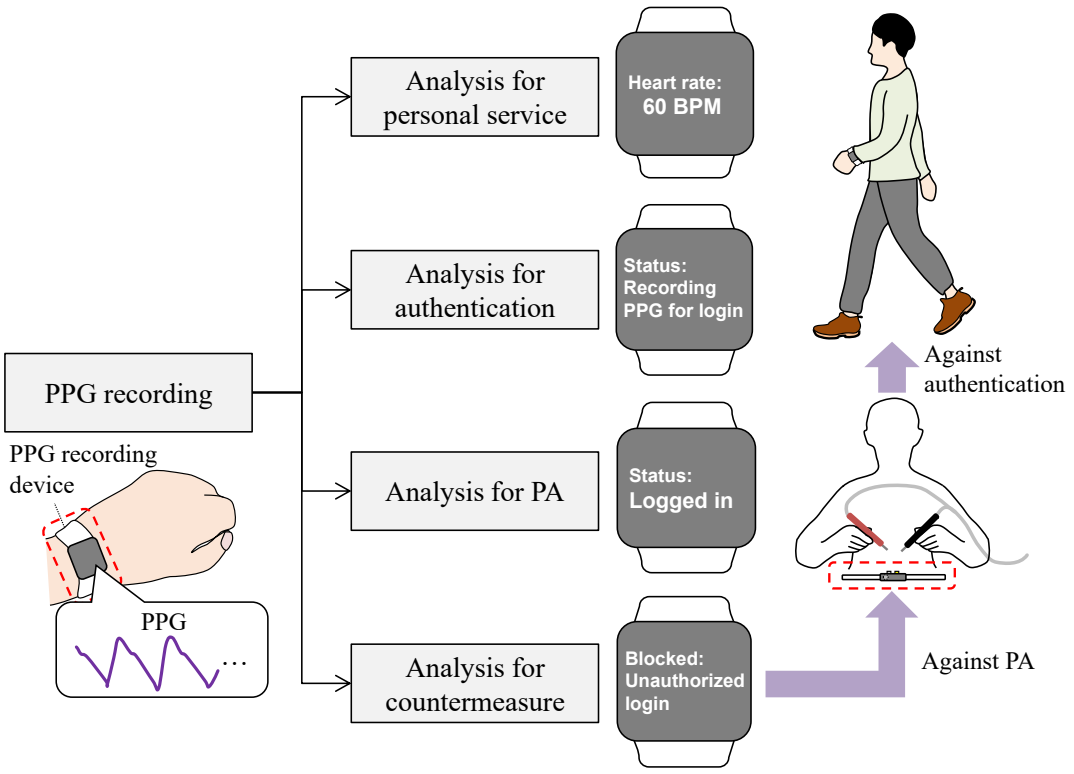


図 1.2: 脈波の解析に基づくサービス提供，認証，なりすまし攻撃，対策

図 1.3 に，本研究の位置づけを，普及済の生体認証手法である指紋認証や顔認証，さらにウェアラブルデバイスの開発・普及が進む心電図を利用した認証と比較して示す．図 1.3 は，各手法が無意識計測可能か否か，なりすまし攻撃に対する脆弱性の度合い，さらに追加する対策の搭載性を観点としており，同図では右上に位置し，かつ濃色円で示される手法が優れている．対策の搭載性は，生体認証システムにおいて，センサが計測している対象が生体であることの確認の容易さを表し，別のセンサ等の物理的要素を追加する必要がある場合は対策の搭載性が高く，別の要素を要する場合は対策の搭載性が低いと考える．指紋認証は，センサに自ら指を接触させる必要があるため，無意識に計測することが難しい．また，事前に型を取って生成した人工指で突破できるため [30]，なりすまし攻撃に対する脆弱性は高いと考えられる．また，対策としては温度センサや光源等の要素を追加する手法が主であり，対策の搭載性は低いと考えられる [30,32]．顔認証は，環境に設置したカメラを用いて無意識に計測することは可能だが，顔を撮影した写真や液晶画面をカメラに提示することで突破できることが示されているため [33]，単独ではなりすまし攻撃に対する脆弱性は高いと考えられる．また，対策としては光源等の要素を追加する手法も存在するが，同一のカメラで取得した画

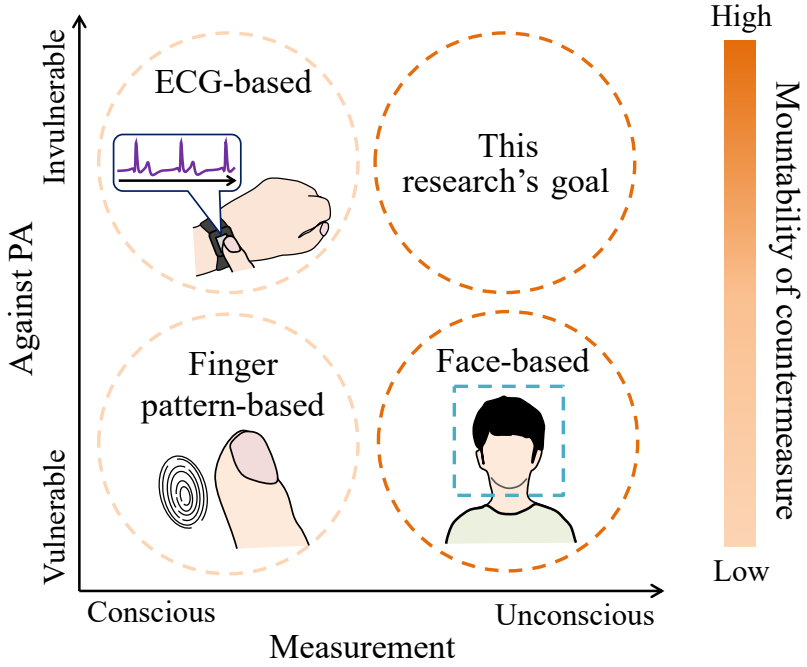


図 1.3: 従来の認証手法に対する本研究の位置づけ

像の処理で実現する手法も存在するため，対策の搭載性は高いと考えられる [28]. 心電図を利用した認証は，人工的に生成した偽の信号を入力して突破できることが示されているが [31]，事前の信号取得や生成に多くの機材を必要とするため，指紋認証や顔認証と比べると，なりすまし攻撃に対する脆弱性は比較的低いと考えられる．しかし，心電図の計測時は特定の姿勢が求められるため [19]，無意識計測は難しいと考えられる．また，対策としては湿度センサ等の要素を追加する手法が主であり，対策の搭載性は低いと考えられる [31]．本研究では，無意識計測により実現でき，なりすまし攻撃に対する耐性，さらに対策の搭載性を兼ね備えた，図 1.3 右上に位置し，かつ濃色円で示される認証手法の開発を目指す．

1.4 論文の構成

本論文では，なりすまし攻撃対策を備えた脈波認証システム脈波認証システムについて述べる．1 章では，サイバ攻撃への対策の必要性，対策の一つである継続認証の有効性を明らかにし，脈波を継続認証に利用する本研究の目的や位置づけについて述べた．2 章では，既存の認証における継続認証の位置づけや代表例とともに，生体認証に対する攻撃の分類や代表例を対策とともに挙げる．3 章では，本研究の対象である脈波認証の原理を述べたうえで，同認証における課題について述べる．4 章では，3 章で述べた課題に着目し，脈波認証に対して起こり得る攻撃を検討するとともに，攻撃の特徴に着目した対策を提案する．5 章では，対象者の複数部位で脈波を同時に計測し，脈波認証に使用される情報の漏洩を検証し，認証および攻撃への同情報の寄与を評価した結果を述べる．6 章では，既存の認証手法を利用して試作した脈波認証システムに対して，提案する攻撃の実現可能性を検証した結果を述べる．7 章では，対策を備えた脈波認証システムの評価のため，脈波のデータセットを利用して同対策手法の有効性を検証した結果を述べる．最後に，8 章では，本研究で提案した，対策を備えた脈波認証システムに関する結論と展望を述べる．

第2章

生体認証と攻撃

本章では，一般的な認証の手法と継続認証の関係を示したうえで，継続認証を実現する手法を代表例と共に分類し，本研究の対象とする認証手法の利点や課題を説明する．続いて，生体認証への攻撃手法についても代表例と共に分類し，本研究の対象とする攻撃手法を説明する．

2.1 認証手法の分類

一般的な認証の手法と継続認証の関係を図 2.1 に示す．一般的な認証の手法は，以下の 3 種類に大別される [16].

- 対象者が，キーボードやタッチパネル等を自ら操作してパスワード等を入力する，“知識による認証”
- 対象者が所有する IC カードやハードウェアトークン等の機器を使用する，“所有物による認証”
- 対象者の指紋や顔等，身体の一部または全体をセンサに提示する，“身体的な特性による認証 (生体認証)”

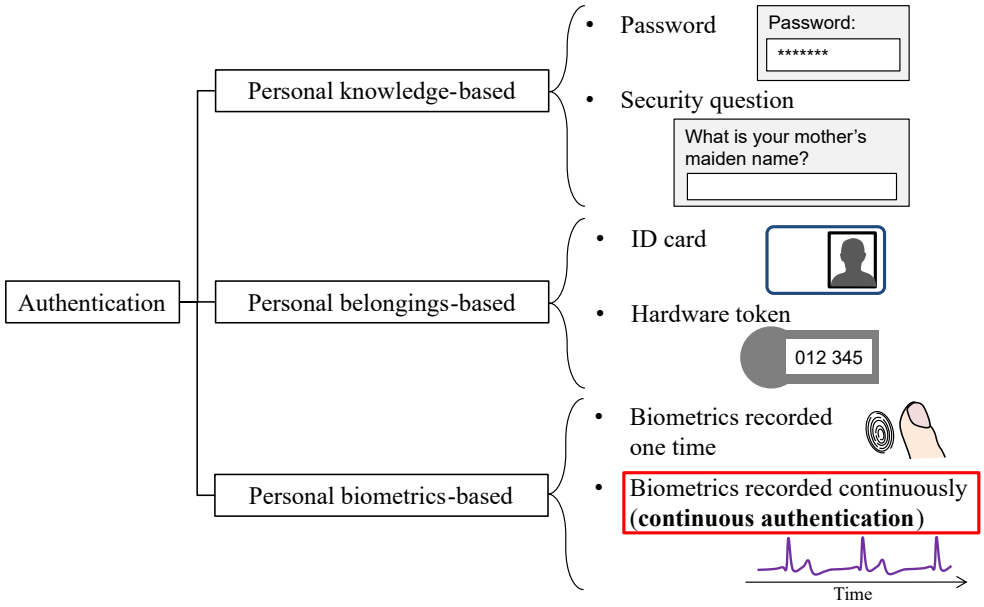


図 2.1: 一般的な認証手法と継続認証の関係

1.2 節で述べた継続認証においては，認証に用いる情報を継続的に得る必要がある．したがって，継続的に計測可能である身体的な特性を用いた生体認証により，継続認証は実現される [18].

2.2 認証に対する攻撃手法の分類

サイバ攻撃への対策である認証手法に対する，さらなる攻撃も多く存在する．Gamundani らは，認証に対する攻撃を，以下の 3 種類に分類した [34].

- 認証用デバイス自体を窃取したり，窃取したデバイスまたはキーボード等からパスワードを総当たりで入力したりする，“デバイスにおける攻撃”
- ネットワーク上を伝搬する，パスワード等の情報を窃取したり，窃取した情報の再送等により認証を突破したりする，“ネットワークにおける攻撃”
- 認証機能を含む複数のアプリケーション間で使用される情報を窃取したり，アプリケーションを改ざんしたりする，“アプリケーションにおける攻撃”

特に，生体認証はセンサを含むデバイスの使用を前提とするため，“デバイスにおける攻撃” に関して，多くの研究および報告が行われている．生体認証に対する攻撃の分類や例は，2.4 節で後述する．

2.3 継続認証とソフト・ハードバイオメトリクス

継続認証には，身体の形状，電気的活動等の個人差に基づく，身体の物理的特性を利用した認証と，道具操作等の個人差に基づく，行動特性を利用した認証が存在する．また，継続認証では，ソフトバイオメトリクス (Soft biometrics) と呼ばれる情報が使用される場合が多い．ソフトバイオメトリクスは，図 2.2 に示すように，身長等の身体的特性や，歩容等の行動特性，服等の所持・装飾物，年齢や性別等，多岐に渡る [35]．また，継続的に計測可能な生体信号から抽出される情報も，ソフトバイオメトリクスとして使用される [36]．必ずしもソフトバイオメトリクス単体で個人を識別可能である必要はなく [37]，指紋や顔等，単体で個人を識別を可能とする情報であるハードバイオメトリクス (Hard biometrics) とは区別されることが多い [38]．複数のソフトバイオメトリクス，またはソフトバイオメトリクスとハードバイオメトリクスの組合せにより，認証が実現される場合がある [37]．以降では，既存の継続認証を，“身体の物理的特性を利用した認証”，“行動の特徴を利用した認証” に大別し，各手法の代表例や利点，課題を挙げる．各手法において，ソフトバイオメトリクスが使用されている場合は，その旨も記載する．

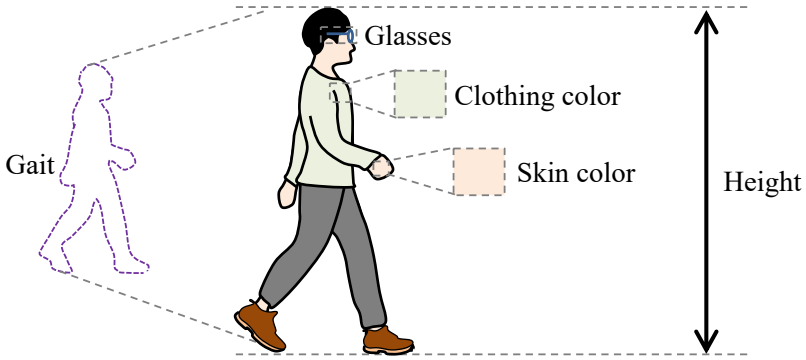


図 2.2: 継続認証に使用されるソフトバイオメトリクスの例

2.3.1 身体の物理的特性を利用した認証

心電図を利用した認証

Shen らは，肌に複数の電極を接触させることで計測できる心電図 (ECG: Electrocardiogram) を利用した生体認証手法を提案している [39]．また，心電図の計測装置として図 2.3 に示すような装着型デバイス等が開発されており，同デバイスで簡易的に計測して得られる心電図を認証に使用する試みがある [19]．しかし，同デバイスは二つの電極を有し，同デバイスを装着していない方の手指でデバイスの電極に触れて静止する必要があり，特定の姿勢を要求されるため，対象者の運動や作業を阻害する場合がある．また，心電図の計測装置は国によっては販売や使用に制限があり [20]，導入が難しい場合もある．

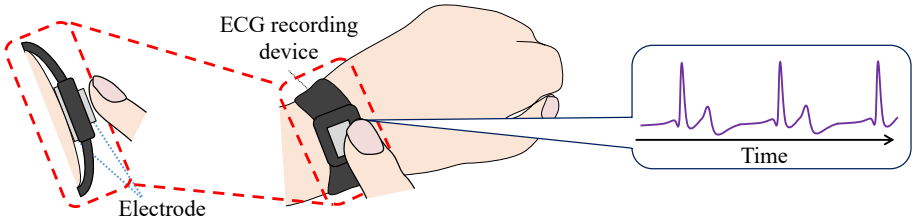


図 2.3: 心電図計測による認証 [19]

脈波を利用した認証

Zhao らは，皮膚を介して血管に対して光を照射し，その反射光または透過光を取得して計測できる脈波 (PPG: Photoplethysmogram) を利用した生体認証手法を提案している [40]．脈波の計測装置は国による販売や使用に制限がなく，手首に装着するスマートウォッチを用いて安価かつ簡便に計測可能であり，心電図の代替として用いられる場合もある [22]．しかし，脈波には体動アーチファクトが重畳するため [41]，対象者の運動中は安定した計測が難しいことが知られている．

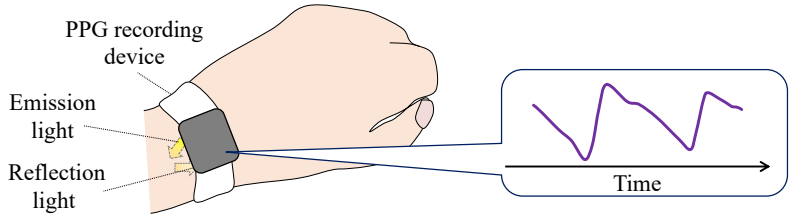


図 2.4: 脈波計測による認証 [40]

脳波を利用した認証

Nakanishi らは，脳波 (EEG: Electroencephalogram) 計測を利用した生体認証手法を提案している [18]．図 2.5 に示すように，頭部に装着した脳波計測デバイスにより計測された波形から特徴量を抽出して認証に用いている．本手法は，デバイスを頭部に装着し，対象者は手や脚を動かしている状態でも認証を行えるため，自動車運転時への適用が検討されている．しかし，信号の再現性が低いことが課題であり [18]，継続認証としての実現には課題がある．

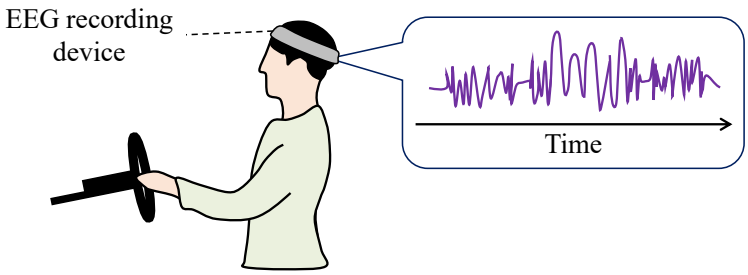


図 2.5: 脳波計測による認証 [18]

筋電図を利用した認証

Venugopalan らは，筋電図 (EMG: Electromyogram) を利用した生体認証手法を提案している [42]．図 2.6 に示すように，対象者の手の甲や腕に電極を装着し，計測された筋電図の波形から特徴量を抽出して認証に用いている．本手法は，手の甲や腕に限らず身体上の様々な部位への応用が可能と考えられるが，信号の再現性が低いため，継続認証としての実現には課題がある．

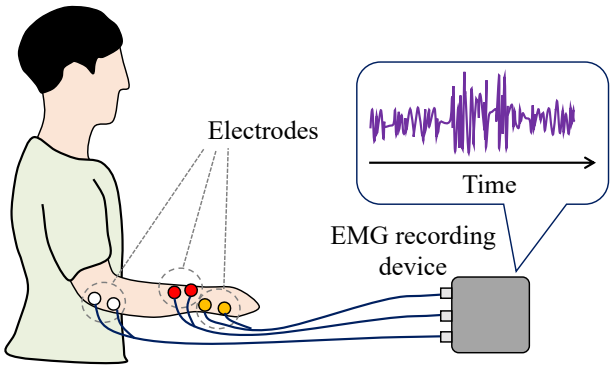


図 2.6: 筋電図計測による認証 [42]

耳音響計測を利用した認証

Mahto らは，図 2.7 に示すような，耳に装着したイヤホン型デバイスから音声信号を放射し，外耳道の形状に基づく反射音 (耳音響) を計測し，周波数解析を行って特徴量を抽出することで，認証を行っている [43]．本手法は，デバイスを耳に装着した状態で，対象者は比較的自由に手足等の動作を行うことができる．しかし，耳音響を計測するために放射する音声信号の音量や周波数帯，放射回数によっては対象者の意識や動作を妨げてしまう可能性がある．

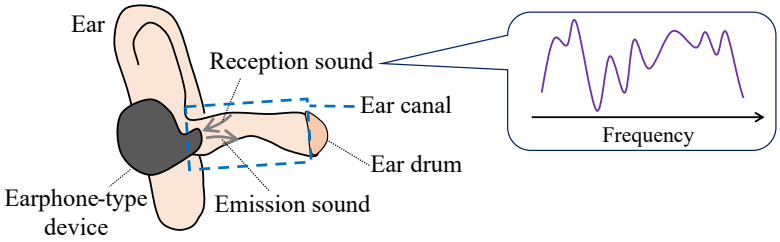


図 2.7: 外耳道計測による認証 [44]

人体通信を利用した認証

Inada らは，人体通信により，手の平に伝搬する信号を利用した生体認証手法を提案している [45]．図 2.8 に示すように，手の平に信号出力デバイスの電極を装着して電気信号を加え，同デバイスから離れた位置で計測された波形を周波数解析して特徴量を抽出し，認証に用いている．本手法は，手の平に限らず身体上の様々な部位への応用が可能と考えられるが，信号の再現性が低いことが課題であり [45]，継続認証としての実現には課題がある．

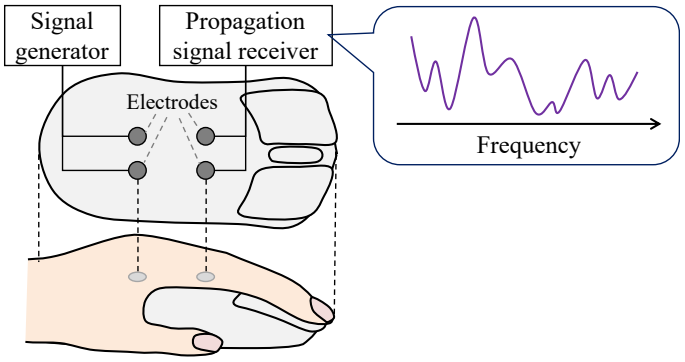


図 2.8: 手の平での伝搬信号計測による認証 [45]

顔計測・脈波計測を利用した認証

Hernandez-Ortega らは，カメラによる顔認証と，カメラによる脈波の計測の組合せによる認証手法を提案している [46]．図 2.9 に示すように，カメラで対象者の顔を計測して認識するとともに，肌の色の変化から脈波を計測して特徴量を抽出することで，一度顔認証を行った後も，継続してその対象者が存在することを担保することができる．しかし，本手法は，対象者の行動がカメラの画角内に制限される．

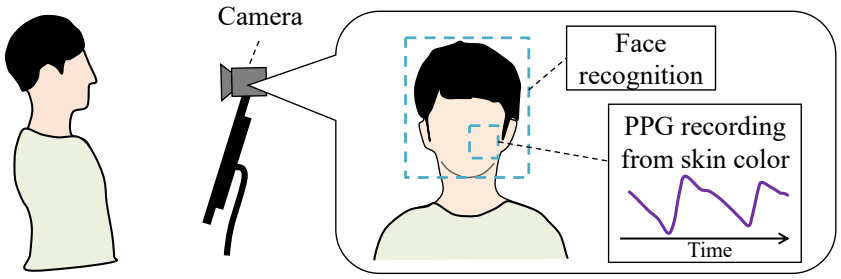


図 2.9: 顔計測・脈波計測を利用した認証 [46]

2.3.2 行動特性を利用した認証

歩容計測を利用した認証手法

Shigeki らは，ソフトバイオメトリクスにも分類される [35]，歩容を利用した認証手法を提案している [47]．図 2.10 に示すように，環境内に設置した複数のカメラにより，対象者の輪郭を取得して，個人の識別に利用する．本手法は，同環境内であれば，対象者の負担や意思を問わず実現できるという利点がある．しかし，本手法の適用は，対象者が特定の環境内を歩行している場合に限られ，対象者が他の環境に存在する，または他の動作を行っている場合には適用できない．

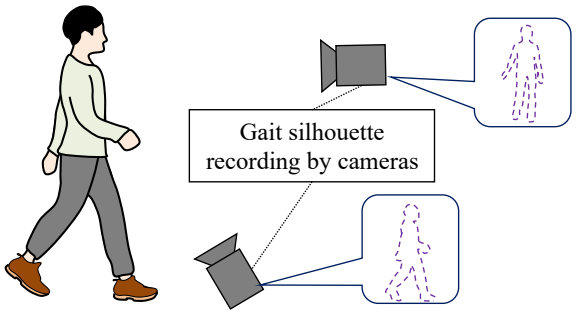


図 2.10: 歩容計測を利用した認証 [47]

キーボード・マウス操作の計測を利用した認証手法

Mondal らは，キーボード・マウス操作の計測を利用した認証手法を提案している [48]．図 2.11 に示すように，キーを 1 回押下するのに要する時間や，マウスを机上で動かす際の速度等を特徴量として利用し，両者を登録および識別に用いている．本手法は，日常的に入手可能なキーボードとマウスを用いることで実現できるという利点がある．しかし，本手法の適用は，対象者が PC を用いて作業を行う場合に限られ，歩行等の動作を行っている際には適用できない．

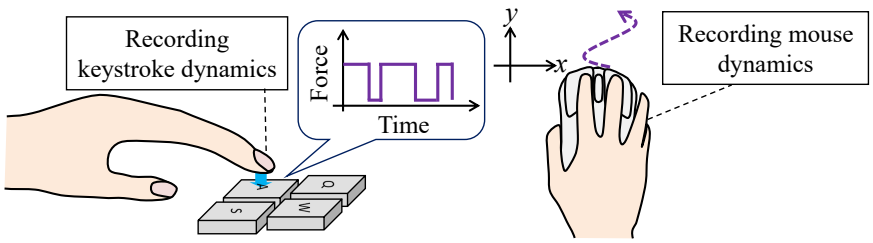


図 2.11: キーボード・マウス操作の計測を利用した認証 [48]

顔・色分布計測を利用した認証

Niinuma らは，ソフトバイオメトリクスに分類される [35]，カメラで計測される顔や服の色を利用した認証手法を提案している [49]．図 2.12 に示すように，カメラで対象者の顔や服を計測し，顔を認識するとともに顔と服の位置の変化やその色分布の変化を取得して，顔と服の色分布をテンプレートと比較することで，一度パスワード入力や顔認証を行った後も，継続して対象者が存在することを担保することができる．しかし，本手法は，対象者の行動がカメラの計測範囲内に制限される．

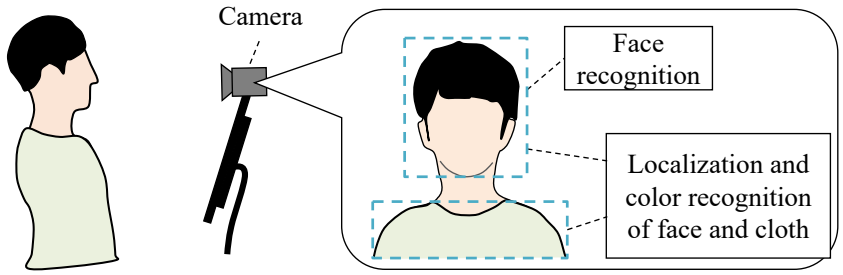


図 2.12: 顔・色分布計測を利用した認証 [49]

呼吸時の胸部変位計測を利用した認証

Rahman らは，呼吸時の胸部の変位計測を利用した認証手法を提案している [50]．図 2.13 に示すように，呼吸時の胸部の変位をドプラレーダで計測し，その変位の大きさや頻度等を特徴量として使用している．本手法は，人間が無意識に繰り返し行っている呼吸動作を利用するため，継続認証を実現できる可能性を検討している．しかし，計測の範囲や方向がドプラレーダによる電波の送信方向に依存するため，対象者の位置や胸部の向きが制限される．

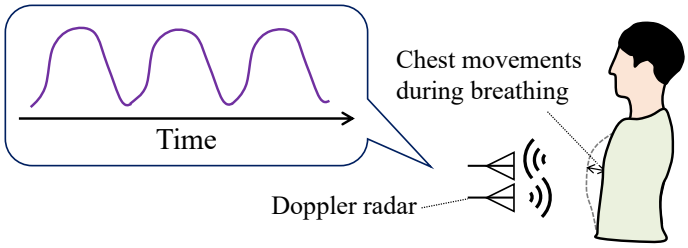


図 2.13: ドプラレーダによる胸部変位計測を利用した認証 [50]

呼吸音計測を利用した認証

Chauhan らは，呼吸時に発生する音 (呼吸音) を利用した認証手法を提案している [51]．図 2.14 に示すように，呼吸音をスマートフォンのマイクで計測し，周波数解析を適用して認証に利用する．本手法は，Rahman らの手法と同様に，日常的に行っている呼吸動作の利用により，継続認証を実現できる可能性がある．しかし，現状では意図的に行う深呼吸が対象であり，マイクを鼻に接近させて計測する必要があることから，対象者の日常的な活動を妨げる可能性もある．

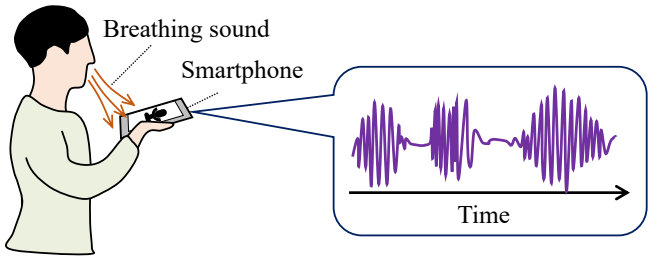


図 2.14: 呼吸音計測を利用した認証 [51]

2.3.3 本研究の対象とする認証手法

本研究では，脈波認証を対象として，起こり得る攻撃および同攻撃への対策を検討する．脈波は単純，安価な装置を用いて，身体上の様々な部位で計測可能であるため，スマートウォッチ等の装着型デバイスでの計測も，環境内に設置するカメラ等による非接触計測も可能である [41,52]．以上の利点を活用して，脈波計測を認証に利用する研究は多く行われており [53–55]，2.3.1 節に示した通り，脈波から得られる情報をソフトバイオメトリクスとして，顔等のハードバイオメトリクスとの組合せにより認証システムを実現する例もある．しかし，脈波認証は一般消費者への普及には至っていない．そのため，脈波認証に対する攻撃に関する研究，さらに同攻撃に対する対策を検討した例は少ない．Seepers らは，心拍数を利用した認証システムに対して，対象者の顔をカメラで撮影することで，非接触計測した脈波を利用して突破する攻撃を検討している [56]．しかし，従来の脈波認証では，波形から抽出した最大値や最小値等，多くの特徴量を使用する場合が多いが [57]，Seepers らが同検討において特徴量として扱ったのは，心拍数のみである．今後，脈波認証が普及することを想定して，同認証に対して起こり得る様々な攻撃を検討するとともに，同攻撃への対策も検討する必要がある．

2.4 生体認証への攻撃

本節では，一般的な生体認証に対して起こり得る攻撃を分類する．続いて，分類した攻撃のうち，特に容易に起こり得る攻撃と具体例について述べる．具体例のうち，対策も検討されている場合は，その概要も記載する．

2.4.1 生体認証への攻撃の分類

生体認証への攻撃手法について，多くの研究および報告が行われている．Ratha らは，センサ・特徴量抽出器・比較器で構成される一般的な生体認証手法 [58,59] に対して起こり得る攻撃手法を，図 2.15 および以下に示す 8 種類の手法に分類した [60].

- 偽の生体情報をセンサに提示
- 古い生体情報を再送信
- 特徴量抽出器を改ざん
- 特徴量を改ざん
- 比較器を改ざん
- 登録済テンプレートを改ざん
- 比較器と，登録済テンプレートの間のデータを改ざん
- 比較器の出力を改ざん

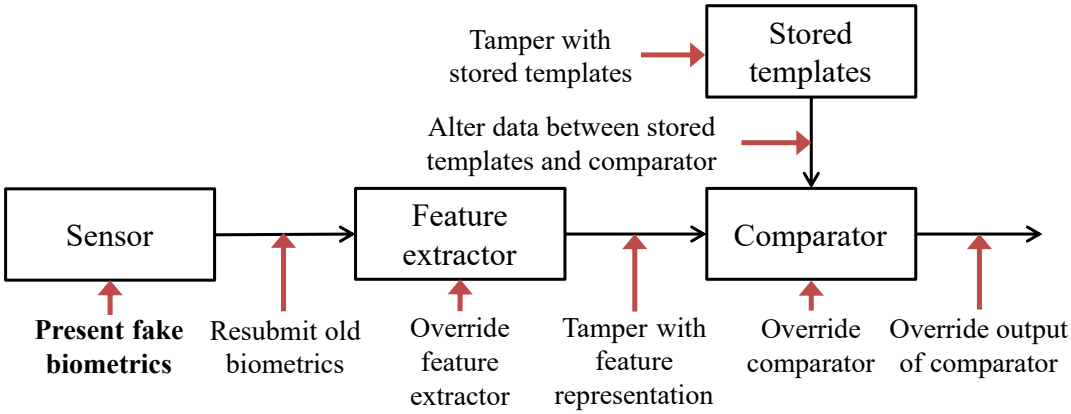


図 2.15: 生体認証への攻撃手法の分類 [60]

8 種類の攻撃方法のうち，太字で示した “偽の生体情報をセンサに提示” を除き，概して生体認証システムを構成するソフトウェアやハードウェアに手を加える必要がある．したがって，同システムの管理者へのなりすましや，物理的な破壊等を前提とするため，一般的に難易度は高いと考えられる．一方で，“偽の生体情報をセンサに提示” は，簡便に手に入る素材や装置の利用により，なりすましを容易に実現できる場合が多い [28, 30]．したがって，生体認証への攻撃手法の中でも，“偽の生体情報をセンサに提示” は比較的難易度が低いため，様々な生体認証に対するなりすまし攻撃およびその対策の検討が求められる．なお，以下では特に断りのない限り，“偽の生体情報をセンサに提示” する攻撃を “なりすまし攻撃” と記載する．

2.4.2 画像ベース認証に対するなりすまし攻撃

PC やスマートフォンとともに，顔認証や指紋認証といった画像ベースの生体認証が普及している．一方で，普及している各認証に対する攻撃に関する研究および報告が行われている．

顔認証に対するなりすまし攻撃

Ma らは，PC やスマートフォンに搭載されている顔認証に対するなりすまし攻撃および対策を検討している [61]．同攻撃では，図 2.16 に示すように，対象者の顔写真や，対象者の顔を撮影した動画を表示したディスプレイ，または対象者の顔を基に作成した 3 次元モデルをカメラに提示することで，顔認証を突破する．対策として，カメラに入力された画像を分割した小さな画像において本物の顔または偽物 (顔写真またはディスプレイ) の識別を行い，各画像での識別結果を総合して，カメラの計測対象が本物の顔または偽物と判断する手法が検討されている．

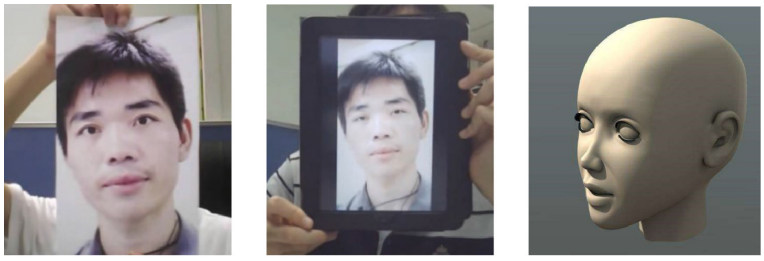


図 2.16: 顔認証に対するなりすまし攻撃 [61]

指紋認証に対するなりすまし攻撃

Cao らは，PC やスマートフォンに搭載されている指紋認証に対するなりすまし攻撃および対策を検討している [32,62]．同攻撃では，図 2.17 に示すように，対象者の指紋を特殊なインクで印刷した紙をスマートフォン搭載の指紋センサに接触させることで，指紋認証を突破する．対策として，指紋センサで取得する画像と同時に，指紋に対して光を照射した際の反射光から得られる画像を利用することで，計測対象が生体であることを確認する手法が検討されている．

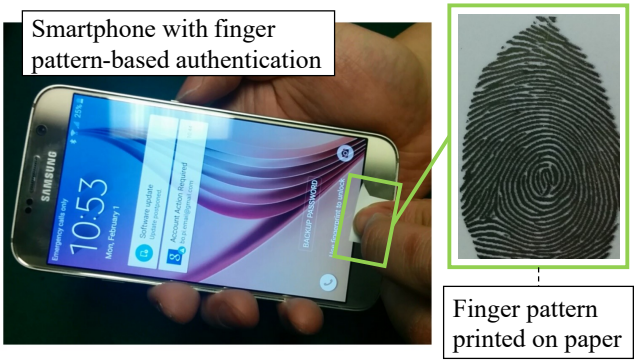


図 2.17: 指紋認証に対するなりすまし攻撃 [62]

虹彩認証に対するなりすまし攻撃

Czajka らは，スマートフォンへの搭載が進んでいる虹彩認証に対するなりすまし攻撃および対策を検討している [63]．同攻撃では，図 2.18 に示すように，対象者の虹彩の画像を表示したディスプレイをカメラに提示することで，虹彩認証を突破する．対策として，波長の異なる複数の光源を利用した撮影や，虹彩の動的特性の計測により，カメラの計測対象が生体であることを確認する手法が検討されている．

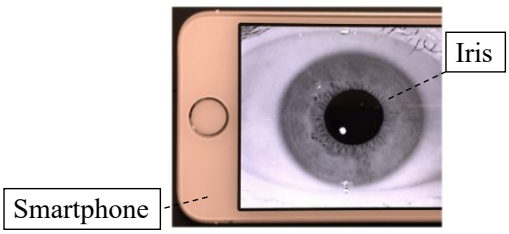


図 2.18: 虹彩認証に対するなりすまし攻撃 [63]

2.4.3 時系列信号ベース認証に対するなりすまし攻撃

時系列データとして得られる生体信号を利用した生体認証は，画像ベースの生体認証に比べると一般に普及していない．しかし，時系列信号ベースの生体認証に対するなりすまし攻撃に関する研究および報告も行われている．

音声認証に対するなりすまし攻撃

Ahmed らは，音声信号を利用した認証に対するなりすまし攻撃および対策を検討している [64]．同攻撃では，図 2.19 に示すように，スマートフォンで被害者の音声を録音し，被害者のスマートフォンのマイクに向けて再生し，音声認証を突破する．対策として，話者による肉声と，スピーカが再生する音声の周波数帯域の差異を利用し，生体からの発声であることを確認する手法が検討されている．

図 2.19: 音声認証に対するなりすまし攻撃 [65]

脳波認証に対するなりすまし攻撃

Shukla らは，頭部で計測される脳波を利用した認証に対するなりすまし攻撃を検討している [66]．同攻撃では，図 2.20 に示すように，脳波の計測と同時に，被害者の手の動作を計測および解析することで，認証に使用される脳波の波形を推定し，脳波認証を突破する．

図 2.20: 脳波認証に対するなりすまし攻撃 [66]

心電図認証に対するなりすまし攻撃

Eberz らは，装着型デバイスとして実現されている心電図認証に対して，人工的に生成した偽の信号によるなりすまし攻撃および対策を検討している [31]．同攻撃では，図 2.21 に示すように，心電図計測デバイスに対して，任意波形発生器を用いて信号を入力することで，心電図認証を突破する．対策として，湿度センサ等を利用して，同デバイスが生体に装着されていることを検証する手法が検討されている．一方で，心電図の代替として用いられることが多い脈波を利用した認証も研究されている．したがって，心電図認証に続いて脈波認証の普及を想定し，脈波認証へのなりすまし攻撃および対策を検討する必要がある．

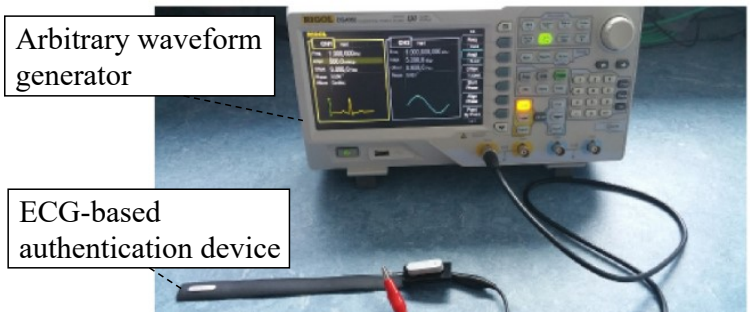


図 2.21: 心電図認証に対するなりすまし攻撃 [31]

2.5 まとめ

本章では，2.1 節で一般的な認証の手法と継続認証の関係を示したうえで，2.3 節で継続認証を実現する生体認証手法を分類した．続いて，本研究において攻撃および対策を検討する対象である脈波認証を含む，既存の認証手法の代表例や利点，課題等を挙げた．さらに，2.4 節で生体認証への攻撃手法を分類し，既存の攻撃手法の代表例や，各攻撃への対策として検討されている手法を説明した．特に，心電図認証に対するなりすまし攻撃について述べ，同認証の代替となり得る脈波認証の普及を想定し，脈波認証へのなりすまし攻撃および対策を検討する必要があることを説明した．本論文では，3 章において，脈波認証の概要を脈波計測の原理に基づいて説明したうえで，脈波認証の課題について述べる．続いて，4 章において，脈波認証へのなりすまし攻撃を提案するとともに，同攻撃に対する対策についても説明する．

第3章

脈波認証

本章では，本研究において攻撃および対策を検討する対象である，脈波認証の概要を脈波計測の原理に基づいて説明し，実装するシステムに含まれる計測装置や回路構成について述べる．続いて，脈波認証の課題を検討し，2.4 節で述べた生体認証への攻撃および脈波認証の利点に着目した本研究の方針について述べる．

3.1 脈波計測

本節では，脈波認証に含まれる脈波計測の原理や，同計測に必要な装置の構成，同装置に含まれる回路について説明する．

3.1.1 脈波計測の原理

脈波認証に含まれる脈波計測の概要を図 3.1，同計測で利用するヘモグロビンの構造を図 3.2(a) に示す．ヘモグロビンは血液中の赤血球が有する蛋白質であり，ヘムとグロビン蛋白より構成される [67]．ヘムは中心に酸素と結合する鉄原子を持ち，ヘモグロビンには酸素化ヘモグロビンと脱酸素化ヘモグロビンが存在する [68]．脈波計測では，図 fig:hemoglobinFeature(b) に示す両ヘモグロビンの吸光特性 [69] を利用して，血管の収縮・弛緩等の挙動に応じた電気信号を得る．照光部 (主に LED: Light emission diode) と受光部 (主に PTr: Phototransistor) で構成される回路を対象者の肌に近づけて光を照射し，その反射光または透過光を取得する．照射した光が血管を通過する際，ヘモグロビンによる光の減衰量に応じて，反射光または透過光も変化する．その結果，脈波は心臓の挙動に応じて変化する血管の挙動を反映し，時系列信号として出力される．

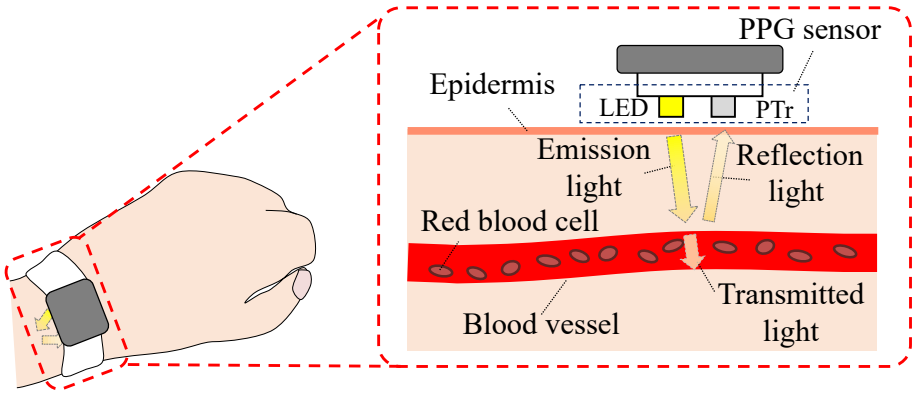
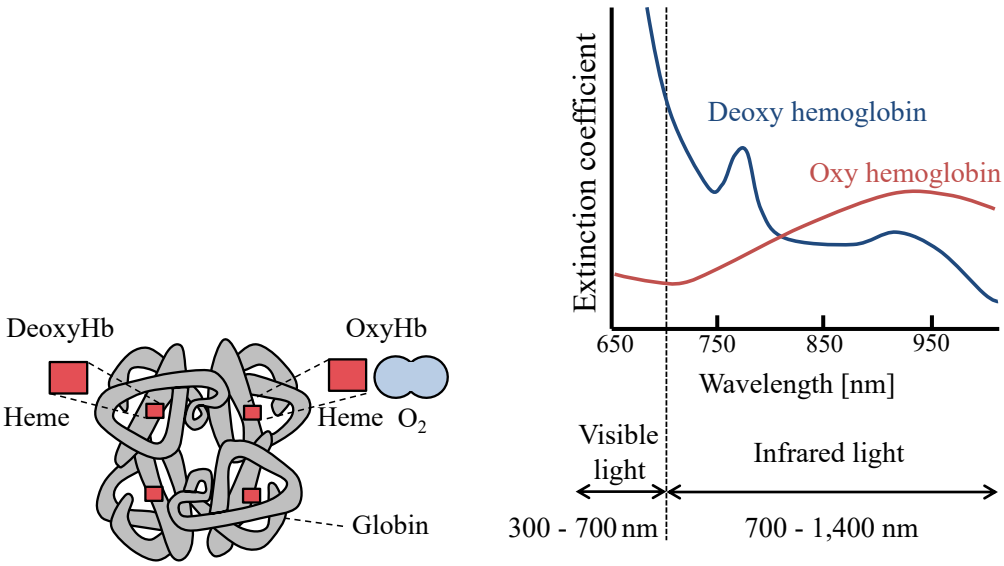


図 3.1: 脈波計測の概要



(a) 構造　　(b) 吸光特性 [70]

図 3.2: ヘモグロビンの特徴

前段落で述べたように，脈波は肌に照光部と受光部で構成される回路を近づけることで，血管の挙動を時系列信号として取得でき，身体上の様々な部位で計測可能であることが利点である．脈波の代表的な計測部位として，額，耳朶，上腕，手首，基節部，指先等が挙げられる [41,71]．脈波の計測部位の例を図 3.3 に示す．

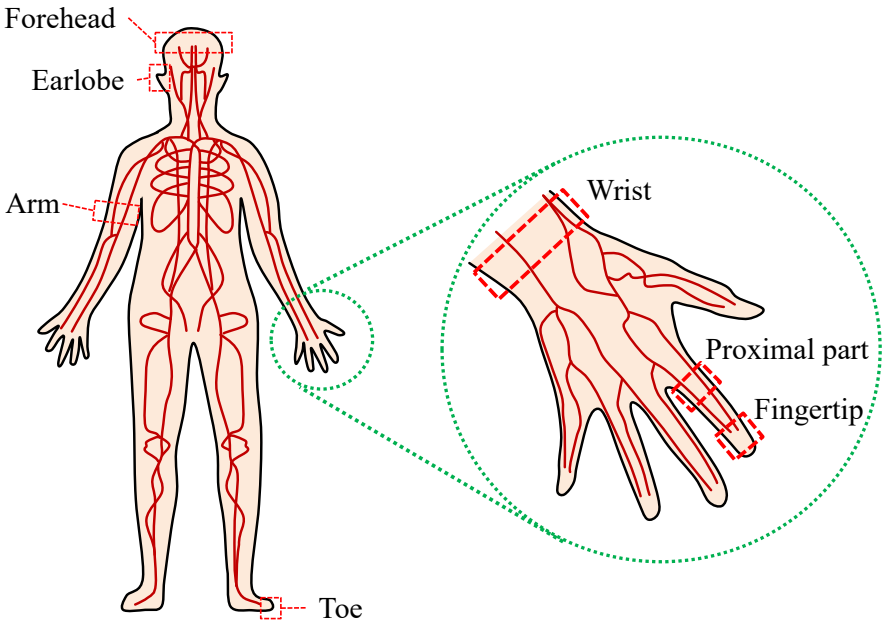


図 3.3: 脈波の計測部位の例

3.1.2 脈波計測装置の構成

脈波計測装置の一般的な構成を図 3.4 に示す．脈波計測装置には，主にセンサ，フィルタ，増幅器が含まれる [72]．3.1.1 節で述べたように，センサは照光部と受光部で構成され，照光部から対象者の肌に対して光を照射し，その反射光または透過光を取得して電気信号に変換する．フィルタは，電気信号に含まれる成分のうち，血管の挙動により変化しない表皮，真皮，皮下組織等に由来する直流成分，さらに体動等に由来する不要な成分に相当する周波数帯域を遮断する．増幅器は，フィルタ通過後の微小な信号を，入力先となる PC において処理可能な大きさの振幅を持つ信号へ増幅する．一般的な脈波計測システムでは，増幅後の信号を PC やマイクロコントローラに取り込んで処理し，HR 等の生体情報を推定し，ヘルスケア等の用途に活用される [22]．

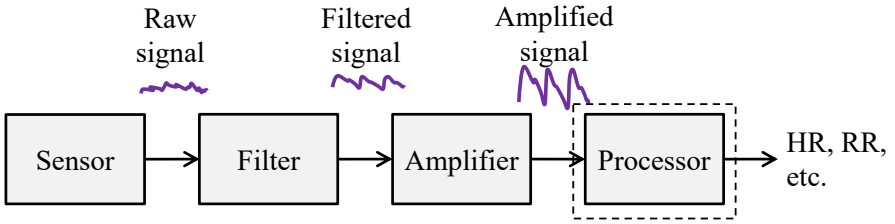


図 3.4: 一般的な脈波計測装置の構成

3.1.3 脈波計測回路

脈波計測回路の例を図 3.5 に示す．ただし，実際はオペアンプに対して電源を供給する必要があるが，図 3.5 では省略している．図 3.5 に含まれる光-電流変換回路のうち，赤点線で囲んだ箇所は，指や手首等の身体への接触または装着を想定した送受光部であり，LED により血管に対して光を照射し，その反射光または透過光を PTr により計測することで，脈波を電気信号として取得する．PTr の出力インピーダンスは高いため，脈波信号をボルテージフォロワ回路へ入力することで，低い出力インピーダンスに変換する．脈波信号には体動アーチファクトをはじめとする雑音が重畳してしまうため，帯域通過フィルタを適用し，雑音を除去する．図 3.5 の帯域通過フィルタの遮断周波数は式 (3.1)，(3.2) で表される．心拍に由来する成分が集中する周波数帯域である 0.83 Hz から 1.5 Hz の確保や，0.5 Hz 未満の心拍変動や呼吸に由来する成分の除去を目的として，脈波計測回路の帯域通過フィルタによる遮断周波数も $f_{\mathrm{HPF}} = 0.5$ Hz，$f_{\mathrm{LPF}} = 4.0$ Hz 程度で設定されることが多い [73]．

$$f_{\mathrm{HPF}} = \frac{1}{2\pi C_{\mathrm{HPF}} R_{\mathrm{HPF}}} \tag{3.1}$$

$$f_{\mathrm{LPF}} = \frac{1}{2\pi C_{\mathrm{LPF}} R_{\mathrm{LPF}}} \tag{3.2}$$

PTr から出力される電流や，帯域通過フィルタを適用後の脈波信号は微小であるため，非反転増幅回路を用いて増幅を行う．図 3.4 の非反転増幅回路の入力電圧 $v_{\mathrm{IN}}(t)$ と出力電圧 $v_{\mathrm{OUT}}(t)$ の関係は式 (3.3) で表される．ただし，t は連続時刻である．

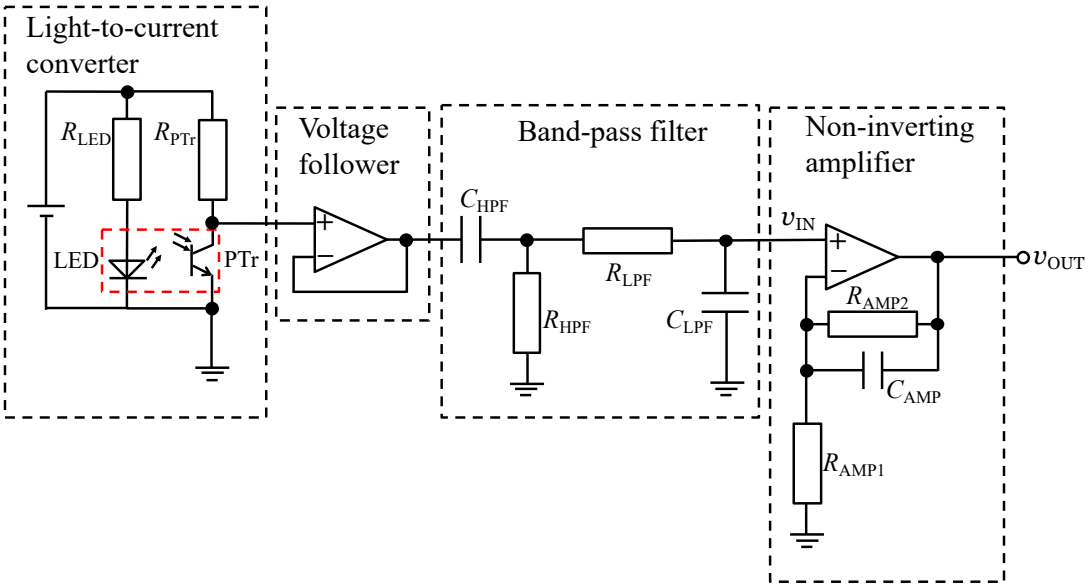


図 3.5: 脈波計測回路の例

$$v_{\mathrm{OUT}}(t) = \left(1 + \frac{R_{\mathrm{AMP2}}}{R_{\mathrm{AMP1}}}\right) v_{\mathrm{IN}}(t) \tag{3.3}$$

$v_{\mathrm{OUT}}(t)$ が，本回路により出力される脈波信号である．出力された $v_{\mathrm{OUT}}(t)$ に対して周波数解析等の処理を行うことで，心拍数や呼吸数等の生体情報を推定し，ヘルスケア等の用途に活用することができる．ただし，後述の 5 章における実装では，同回路の出力電圧を AD 変換して PC に取り込むため，n を離散時刻とした出力電圧 $v_{\mathrm{OUT}}[n]$ を用いて説明する．ただし，t と n の関係は，標本化周期 T_{s} を用いて，式 (3.4) で表される．

$$t = nT_{\mathrm{s}} \tag{3.4}$$

3.2 脈波の認証応用

無意識に計測可能である点や，簡便に計測できる点等を利用して，脈波を認証に用いる研究は多数行われている [55, 57]．一般的な脈波認証の処理手順を図 3.6 に示す．図 3.4 に示した脈波計測装置と同様に，センサやフィルタ，増幅器を用いて脈波を計測する．計測された脈波から，図 3.6 の破線部において，個人特有の情報を表す特徴量を抽出する処理や，抽出した特徴量をデータベースに登録済の特徴量と比較する処理等により，対象者を認証する．

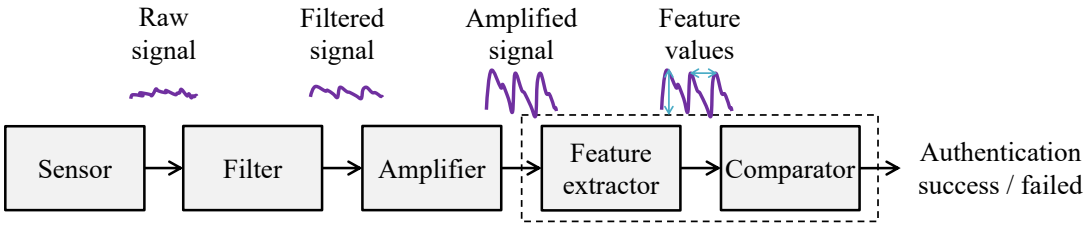


図 3.6: 一般的な脈波認証システム構成

3.3 脈波認証における課題

脈波には，2.3 節で述べた通り，認証に利用できるハードバイオメトリクスや，顔等のハードバイオメトリクスとの組合せにより認証を実現するソフトバイオメトリクス等，多数の情報が含まれている．しかし，脈波は様々な部位で計測可能であるため，他者によって脈波が不正に計測および解析された場合，計測対象者に不利益が生じる可能性がある．例えば，対象者が手首にスマートウォッチを装着し，健康状態を計測している場合，他者により手首以外で脈波が不正に計測されると，同脈波を解析することで対象者の健康状態が推定され，プライバシの侵害に繋がり得る [74]．また，脈波センサに対して照射する光量の制御や，脈波センサが装着された部位の意図的な圧迫により，同センサに対して任意の信号を計測させる研究が存在する [75, 76]．したがって，今後，脈波認証が普及した場合，他者により対象者の脈波が不正に計測および解析されて，認証システムに搭載された脈波センサに攻撃用の信号を入力され，認証の突破に利用される可能性がある．2.4.3 節でも示した通り，脈波認証同様に時系列信号ベースの手法である心電図認証は，装着型デバイスの開発も進んでいるが，同デバイスに対するなりすまし攻撃が既に提案および実証されている [31, 77]．同攻撃は，正規の心電図認証デバイスとは別のデバイスを使用して，別の部位で計測された心電図を入力したり，変形した信号を生成して入力することで認証を突破する．したがって，心電図認証に続いて脈波認証も普及することを想定すると，身体上の様々な部位で計測可能であるという脈波の特徴を考慮したうえで，脈波認証へのなりすまし攻撃および対策を検討しておく必要がある．

3.4 まとめ

本章では，本研究において攻撃および対策を検討する対象である，脈波認証の理論について説明した．3.1 節では，脈波認証に含まれる脈波計測の原理や，必要な装置の構成を説明し，3.2 節では，脈波計測を認証に利用する際のシステム構成を説明した．続いて，3.3 節では，脈波認証の課題として，様々な部位で計測可能である脈波の特徴に着目し，不正計測や解析に基づいたなりすまし攻撃が起こり得る可能性を説明した．4 章では，本章で説明した脈波計測の原理や，脈波認証の課題に基づいて，脈波認証に対して起こり得るなりすまし攻撃を検討する．さらに，同攻撃の特徴に基づいた対策を提案する．

第4章

脈波認証への攻撃と対策

本章では，脈波認証に対して起こり得るなりすまし攻撃を検討し，攻撃者がなりすましを試みる相手である被害者の条件や，攻撃者の手順について説明する．さらに，同攻撃に対する対策についても説明する．

4.1　脈波認証へのなりすまし攻撃

本節では，3 章で述べた脈波計測の利点である，身体上の様々な部位で計測可能である点に着目して起こり得るなりすまし攻撃を検討する．また，なりすまし攻撃の対象である被害者の条件や，攻撃者の手順についても説明する．さらに，高度な攻撃者を想定して，脈波の変形を含む攻撃手法も提案する．

4.1.1　なりすまし攻撃の概要

提案するなりすまし攻撃の具体例を図 4.1 に示す．攻撃者によるなりすましの対象である被害者は，脈波認証機能を搭載した装着型デバイスを所有している．一方，被害者へのなりすましを試みる攻撃者は，被害者に気づかれないように脈波を不正に計測および解析して，同デバイスが行う脈波認証の突破を目指す．以降では，図 4.1 の具体例における被害者の条件 (**Step 0**)，攻撃者の手順 (**Step 1, 2, ..., 5**)，脈波の変形方法について説明する．

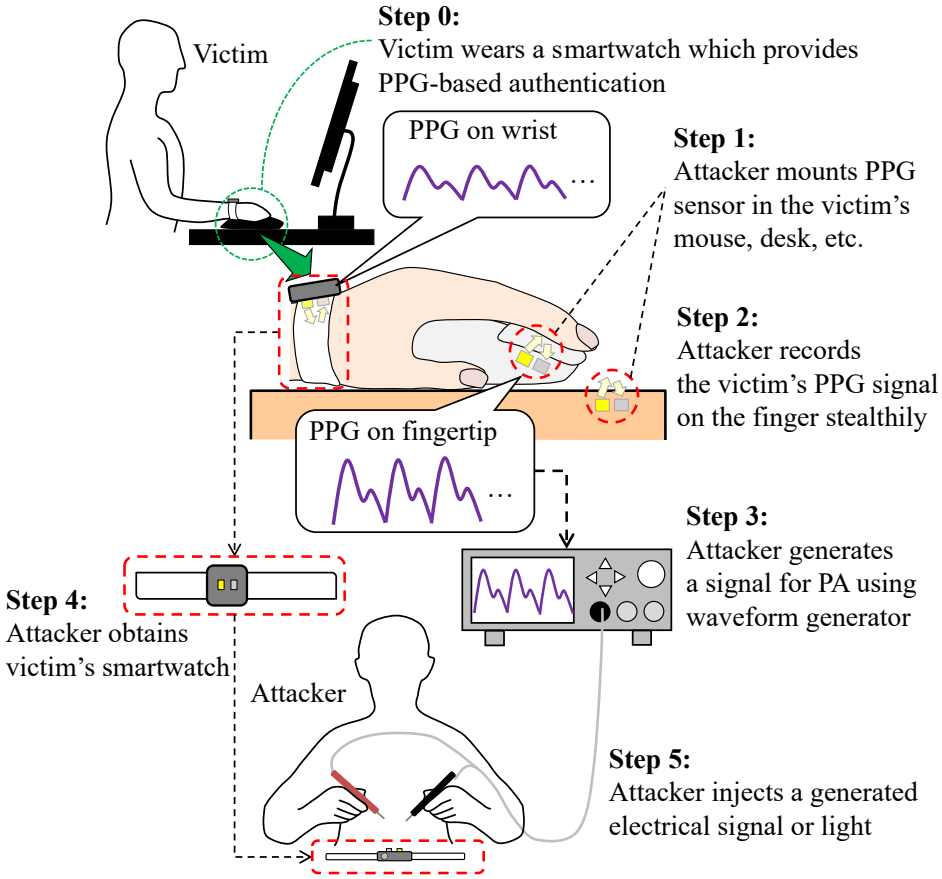


図 4.1: 提案する攻撃の概要

4.1.2 被害者の条件

図 4.1 の **Step 0** に示すように，攻撃者によるなりすましの対象である被害者は，脈波認証機能を搭載したスマートウォッチを日常的に手首に装着している．同認証機能によるログイン後，ヘルスケアアプリケーションやメッセージ交換アプリケーション等，個人情報や機密情報を取り扱うアプリケーションを使用する．しかし，被害者は，充電時等にはスマートウォッチを取り外すため [78]，他者が物理的にアクセス可能な場所に放置することがある．また，攻撃者が不正な計測を目的としてセンサを設置していることに気づかずに，手指を接触させてマウスやテーブル等のオフィス用品や日用品を使用する．

4.1.3 攻撃者の実行手順

攻撃者は，被害者になりすますことで，スマートウォッチを経由して被害者の個人情報や機密情報を窃取することを目的とする．以下では，図 4.1 の **Step 1, 2, ..., 5** に示す，攻撃者による実行手順を説明する．

Step 1

マウスやテーブル等，被害者が手指で接触し得るオフィス用品・日用品等へセンサを設置する．

Step 2

Step 1 で設置したセンサに被害者の手指が接触した際に，被害者には気づかれないように脈波を計測し保存する．

Step 3

Step 2 で計測した脈波を基に，任意波形発生器等を用いて攻撃用の信号を生成する．本手順では，計測した脈波を攻撃用の偽の信号として使用する可能性もあるが，高度な攻撃者は攻撃の成功率を向上させるために脈波を変形させて，スマートウォッチで計測される脈波に類似した信号を生成する可能性もある．

Step 4

被害者がスマートウォッチを取り外した隙に，同スマートウォッチを盗む．

Step 5

Step 3 で生成した攻撃用の偽の信号をスマートウォッチ内の回路へ入力したり，同信号に基づいて明るさを時間変化させた光をセンサへ照射したりすることで，スマートウォッチによる脈波認証を突破し，被害者の個人情報や機密情報を窃取する．

4.1.4 脈波の変形

高度な攻撃者は，図 4.1 の **Step 3** において，センサを設置して計測した脈波を解析し，同脈波を変形して攻撃用の偽の信号を生成し，攻撃の成功率を向上させる可能性がある．このような高度な攻撃への対策も考慮し，脈波の変形を含む高度な攻撃手法も提案する．生体信号の波形変形に関する既存手法は，概して，二つの波形間の関係から生成した伝達関数を利用して，一方の波形を変形して，もう一方の波形を推定している．例えば，脈波認証と同様に，時系列信号ベースの手法である心電図認証に対する攻撃手法では，心電図認証デバイスで計測した心電図と，別のデバイスで計測した心電図，または被害者以外の人物から計測した心電図の間の伝達関数を最適化問題を解くことで求め，被害者の心電図を推定している [31, 77]．また，脈波と心電図の周波数特性を利用して，両者に離散コサイン変換 (DCT: Discrete cosine transform) を適用し，脈波を心電図波形に変換する伝達関数を生成して，脈波から心電図を推定する手法も存在する [79]．一方，脈波と動脈圧 (ABP: Arterial blood pressure) の間の類似性から，両者の周波数特性を利用して両者の間の伝達関数を生成し，脈波から動脈圧を推定する手法が存在する [80]．脈波は身体上の様々な部位で計測可能であるが，各部位で計測される脈波には差が存在する．しかし，多くの場合は各脈波から同様の特徴量を抽出可能であることや，指先脈波の振幅は他部位の脈波の振幅よりも大きくなること等の傾向が存在する [81]．同傾向から，図 3.3 に示した各部位で計測される脈波間において，図 4.2 に示すように伝達関数 E^{pw}, E^{fw} が存在すると考えられる．

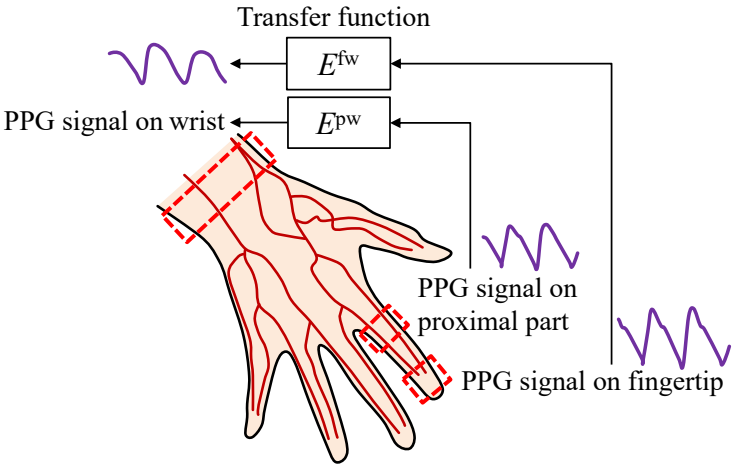


図 4.2: 異なる部位で計測された脈波と伝達関数に関する仮定

したがって，今回提案する攻撃では，異なる部位で計測された脈波の間に伝達関数の存在を仮定する．計測対象者間での脈波の差から，周波数特性も同様に差が存在する可能性があるが，前段落で述べた通り，各部位における脈波の振幅の大小等の傾向を利用して，各対象者において，脈波間の伝達関数を導出できる可能性がある．被害者の脈波を，攻撃者を含む他人の脈波から導出した伝達関数を用いて推定できれば，脈波認証に対する脅威となり得る．今回提案する攻撃では，二つの部位で計測された脈波のうち，不正に計測したとみなす一方の脈波から，周波数特性を伝達関数として利用して，もう一方の脈波を推定する．

以下では，指先と手首で計測される脈波 (以下，指先脈波，手首脈波と記す) の間に周波数特性の存在を仮定する．手首と指先で計測された脈波間に仮定する関係を図 4.3 に，脈波の変形手順を図 4.4 に示す．同手順では，脈波計測回路の出力電圧 $v_{\mathrm{out}}[n]$ に対するフーリエ変換を利用して周波数特性を取得し，同周波数特性を伝達関数として脈波の変形に利用する．脈波 $v[n]$ の離散フーリエ変換 $V[k]$ は，式 (4.1) で表される．ただし，N はデータ点数，k は離散周波数，j は虚数単位である．

$$V[k] = \sum_{n=0}^{N-1} v[n] \exp\left(-j\frac{2\pi kn}{N}\right) \tag{4.1}$$

また，$V[k]$ の逆離散フーリエ変換は，式 (4.2) で表される．

$$v[n] = \frac{1}{N}\sum_{k=0}^{N-1} V[k] \exp\left(j\frac{2\pi nk}{N}\right) \tag{4.2}$$

まず，図 4.1 に示したように，指先脈波を不正計測された脈波とみなす．2 部位で計測された脈波間に，図 4.3 に示す関係がある場合，対象者 q の周波数特性 $G^q[k]$ は式 (4.3) で表される．ただし，脈波を計測する時間は短いとみなし，2 部位

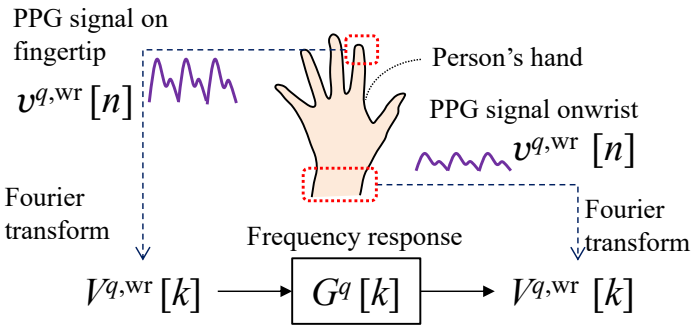


図 4.3: 手首と指先で計測された脈波間に仮定する関係

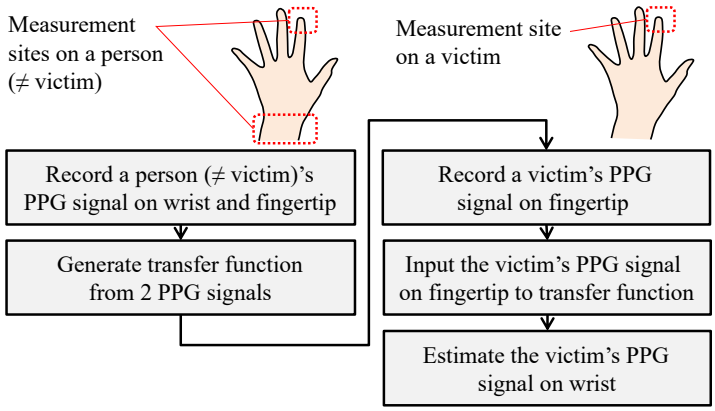


図 4.4: 導出した周波数特性を利用して脈波を変形する手順

で計測された脈波の間の関係として線形時不変システムを仮定した．また，$V^{q,\mathrm{fi}}[k]$ は対象者より計測した指先脈波 $v^{q,\mathrm{fi}}[n]$ の離散フーリエ変換，$V^{q,\mathrm{wr}}[k]$ は同対象者より計測した手首脈波 $v^{q,\mathrm{wr}}[n]$ の離散フーリエ変換である．脈波には周期性を有する心拍に加えて自律神経活動等の様々な成分が寄与することから，任意の k において $V^{q,\mathrm{fi}}[k] \neq 0$ と仮定する [41]．

$$G^{q}[k] = \frac{V^{q,\mathrm{wr}}[k]}{V^{q,\mathrm{fi}}[k]} \tag{4.3}$$

続いて，式 (4.3) および不正に計測した指先脈波を用いて，対象者 q とは別人である被害者 $p\,(\neq q)$ の手首脈波を推定する．人物間で周波数特性に類似性があり，式 (4.4) が成立すると仮定する．

$$G^{p}[k] \simeq G^{q}[k] \tag{4.4}$$

式 (4.4) を用いて被害者の手首脈波を推定すると，式 (4.5) が得られる．ただし，$\hat{V}^{p,\mathrm{wr}}[k]$ は推定される被害者の指先脈波 $\hat{v}^{p,\mathrm{wr}}[n]$ の離散フーリエ変換，$G^{p}[k]$ は被害者の周波数特性，$V^{p,\mathrm{fi}}[k]$ は被害者の指先脈波 $v^{p,\mathrm{fi}}[n]$ の離散フーリエ変換である．

$$\begin{aligned} \hat{V}^{p,\mathrm{wr}}[k] &= G^{p}[k]V^{p,\mathrm{fi}}[k] \\ &\simeq G^{q}[k]V^{p,\mathrm{fi}}[k] \end{aligned} \tag{4.5}$$

$\hat{V}^{p,\mathrm{wr}}[k]$ を逆離散フーリエ変換することで，被害者の手首脈波 $\hat{v}^{p,\mathrm{wr}}[n]$ を推定することができる．高度な攻撃者は，以上の手順で推定した手首脈波を利用して，脈波認証へのなりすまし攻撃を行うことを想定する．

4.2 なりすまし攻撃への対策

本節では，4.1 節で述べた，脈波認証へのなりすまし攻撃に対する対策を提案する．同攻撃は，様々な部位で計測可能である脈波計測の利点に着目した攻撃であるが，攻撃と同様にその利点に着目した対策を提案する．

4.2.1 攻撃の特徴に基づいた対策の検討

生体認証システムに対するなりすまし攻撃への一般的な対策は，対象が人工物ではなく生体であることの確認である [82]．同対策は，1.1 節で述べた 3 種類の対策である，“予防”，“検出”，“対応” のうち，“検出” が該当し，攻撃の検出後は，対象者の強制的なログアウトやパスワード入力の要求等の “対応” を行う [83,84]．検出の例として，指紋認証システムにおいて，体温を計測する温度センサを使用して，認証の対象が生体であることを確認する方法が提案されている [30]，また，心電図認証システムにおいて，汗を計測する湿度センサを使用して，認証の対象が生体であることを確認する方法が提案されている [31]．4.1 節で検討した，脈波認証へのなりすまし攻撃は，不正計測を行った後，人工的に生成した信号を脈波センサへ入力する．したがって，同攻撃に対しても，入力信号の正当性を検証し，脈波センサの計測対象が生体であることを確認する検出が対策となり得る．

一方，顔認証システムや，心電図認証システムにおいては，脈波センサを使用して，認証の対象が，血管を有する生体であることを確認する手法も存在する [77,85]．したがって，脈波認証システムに含まれる脈波センサは，認証に使用するだけではなく，なりすまし攻撃の対策にも利用できる可能性がある．また，同攻撃は，認証デバイスにより脈波計測が行われる，正当な部位とは異なる部位で計測した脈波を利用する．しかし，各部位で計測される脈波には，類似性がある一方，抽出される特徴量に違いが存在することが知られており [81]，一部の特徴量は計測部位を表すソフトバイオメトリクスとして利用できる可能性がある．したがって，脈波から抽出するハードバイオメトリクスとなる特徴量を認証に利用すると同時に，ソフトバイオメトリクスとなり得る部位特有の特徴量を利用して，入力信号およびその計測部位の正当性を検証することで，攻撃の検出を実現できる可能性がある．したがって，4.1 節で検討した脈波認証へのなりすまし攻撃とともに，脈波から抽出可能な特徴量を利用した，計測部位の識別による対策を検討する．

4.2.2 提案する対策

図 4.5 に，脈波認証へのなりすまし攻撃に対して提案する対策の概要と位置づけを示す．同対策は，図 3.6 の点線部分に示した一般的な脈波認証システムにおける，センサやフィルタ，増幅器を利用した脈波認証の後に実施される．同対策では，正当な対象者 (Genuine person) を一度認証した後も，脈波計測を継続する．継続して計測した脈波から，計測部位によって値が異なる特徴量を抽出する．その後，同特徴量を識別器に入力し，脈波の計測部位を識別する．以上の処理により，センサが計測している対象が，偽の入力ではなく，正当な部位で計測された脈波であると判断した後に，図 3.6 に示した一般的な脈波認証システムと同様に，破線部の処理で対象者を認証する．脈波が正当な部位で計測されたものではないと判断した場合は，認証を行わずに処理を終了する．

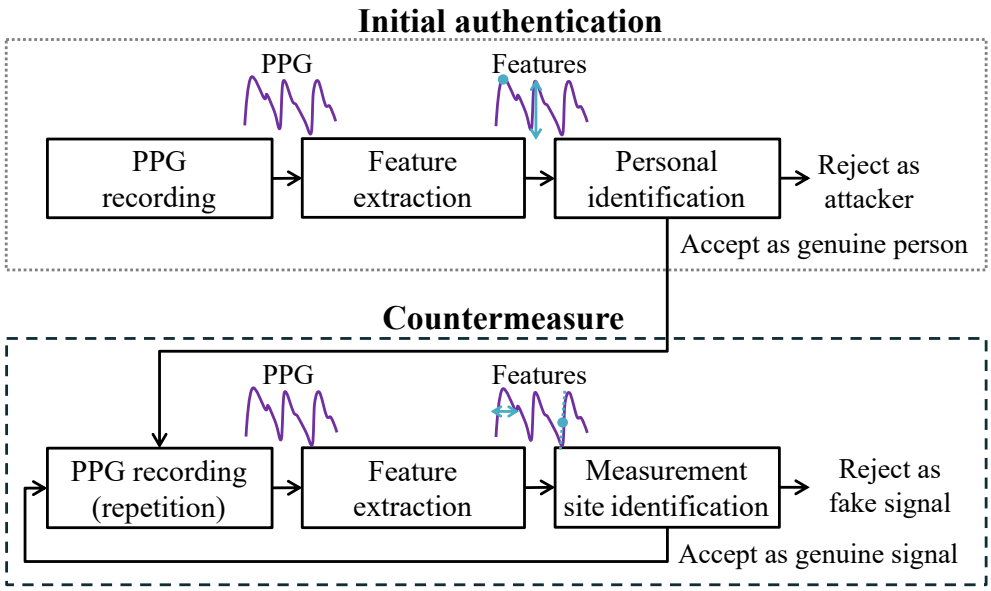


図 4.5: 提案する対策の概要と位置づけ

なりすまし攻撃の検出は，実施頻度の適切な設定が重要である [86]．既存の顔認証システムにおいて，なりすまし攻撃を検出するために脈波を用いられる場合があるが，その頻度は，最大値・最小値等の特徴量を抽出可能な時間幅を基に設定されている [46]．したがって，本研究で提案する対策は，脈波 1 周期分を 1 セグメントとし，同セグメント毎に特徴量を抽出して検証を行う．

4.3 まとめ

本章では，4.1 節で脈波認証に対して起こり得るなりすまし攻撃を検討し，攻撃の対象である被害者の条件や，攻撃者の手順について説明した．同攻撃は，2.4 節で述べた心電図認証へのなりすまし攻撃や，3.3 節で述べた脈波認証の課題を基に，脈波が手首以外の部位で不正に計測され，脈波認証デバイスに入力され得ることに着目したものである．続いて，4.2 節で同攻撃に対する対策を提案した．同対策は，脈波は身体上の様々な部位で計測可能であるが，計測される脈波間には差があることに着目する．脈波を解析して得られる部位特有の特徴量を利用して，入力された信号およびその計測部位の正当性を検証することで，なりすまし攻撃を検出する．5 章では，実験参加者の複数部位で計測した脈波を利用して，脈波認証に使用される情報の漏洩の検証や，特徴量の評価を行う．続いて，6 章において，既存の脈波認証アルゴリズムを利用して，4.1 節で提案した攻撃の実現可能性を検証する．さらに，7 章において，脈波のデータセットを利用して，4.2 節で提案した対策手法の有効性を検証する．

第5章

情報漏洩検証と特徴量評価

本章では，提案する脈波認証へのなりすまし攻撃の実現可能性のため実施した実験について述べる．実験のため実装した脈波計測装置や，認証に必要な情報の漏洩の検証，特徴量の評価の手順や結果，考察についても述べる．

5.1 実装した脈波計測装置

本節では，本実験で使用した脈波計測装置に含まれる脈波計測回路について説明する．続いて，同回路への電力供給や，同回路の出力信号を処理するために使用した実験機器について説明する．

5.1.1 脈波計測回路

提案する攻撃手法の検証のため，計測装置に含まれる図 3.5 の脈波計測回路を実装した．図 5.1 に同回路に含まれる送受光部を装着した様子，図 5.2 に実装した送受光部を示す．現在普及している，脈波計測を行えるスマートウォッチ [23, 25] と同様に，利き手とは逆の手首での脈波計測を想定した．また，同じ対象者から攻撃用の信号を計測するため，他の部位でも計測を行った．脈波は身体上の様々な部位で計測可能だが，臨床現場での計測箇所として一般的な指先と [41]，指輪型デバイスによる計測が可能である基節部 [87] で計測を行った．したがって，本実験では，指先，基節部，手首の全 3 部位で脈波を計測した．送受光部には光源となる LED と，光を電流に変換する PTr が含まれる．一般に，脈波計測回路では，一般的に緑色光または赤外光の LED が用いられるが，スマートウォッチでは，緑色の LED が搭載されている場合が多いため [23]，本回路でも，緑色の LED を採用した．波長の短い緑色光を用いる方が，赤外光を用いるよりも，光の到達深

度および光路長が短くなる分，体動アーチファクトの寄与が小さくなり，いずれの計測部位においても頑強に計測できる [88] [89]．緑色光よりも波長の短い青色光を用いる試みも存在するが [90]，十分な光の到達深度が得られず，正確に HR 等の生体情報を推定できない場合がある [91]．実装した LED・PTr は，図 5.3 に示す両素子が一体となったチップであり，発光ピーク波長は 570 nm である．本実験では，図 5.2(a) に示すように送受光部では回路を実装した基板に面ファスナを取り付け，指や手首に着脱可能な形とした．

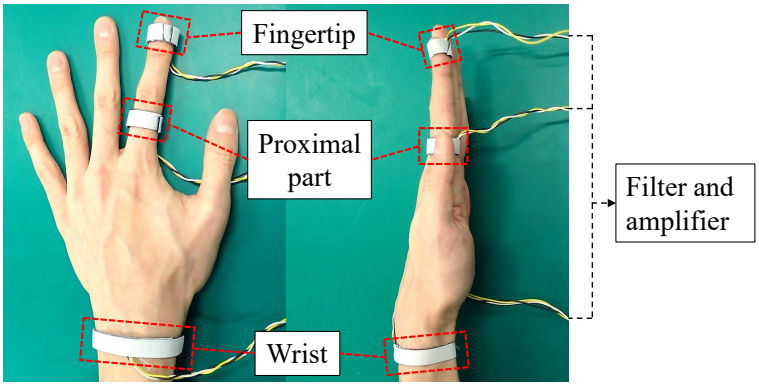


図 5.1: 送受光部を装着した様子

(a) 正面　　(b) 側面

図 5.2: 実装した送受光部

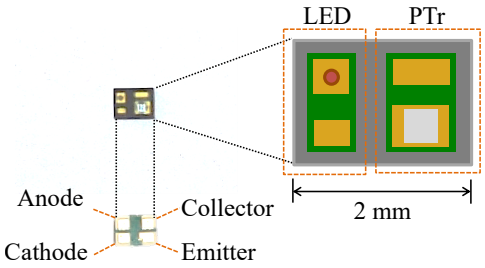


図 5.3: 実装に用いた LED・PTr (NJL5303R-TE1)

図 5.4 に，図 3.5 の送受光部以外を基板に実装した回路 (フィルタ・増幅回路) を示す．心拍に由来する成分が集中する周波数帯域である 0.83 Hz から 1.5 Hz の確保や，0.5 Hz 未満の心拍変動や呼吸に由来する成分の除去を目的として，一般的な脈波計測システムに含まれる帯域通過フィルタによる通過範囲は，0.5 Hz から 4.0 Hz 等と設定されることが多い [73]．しかし，脈波認証においては，心拍よりも中心周波数が低い呼吸成分等も認証および攻撃の検討に有効である可能性がある．したがって，今回実装した回路では，脈波に含まれる心拍に加えて呼吸成分等も計測するため，一般的な脈波計測システムよりも，帯域通過フィルタによる通過範囲を広く確保するため，低域側の遮断周波数を $f_{\mathrm{HPF}} = 0.01$ Hz，高域側の遮断周波数を $f_{\mathrm{LPF}} = 4.0$ Hz と設定した．そのために式 (3.1)，(3.2) において，抵抗やコンデンサを $R_{\mathrm{H}} = 1.68$ MΩ，$C_{\mathrm{H}} = 1.0$ μF，$R_{\mathrm{L}} = 39$ kΩ，$C_{\mathrm{L}} = 1.0$ μF と設定した．計測される脈波の振幅は数 mV であり，本計測回路を用いて数 V の振幅を実現するため，増幅率を 220 倍と設定した．したがって，式 (3.3) において，抵抗の値を $R_{\mathrm{A1}} = 1.0$ kΩ，$R_{\mathrm{A2}} = 220$ kΩ と設定した．本実験では，指先，基節部，手首の全 3 部位で計測を行うため，図 3.5 の回路を各部位につき 1 個実装した．

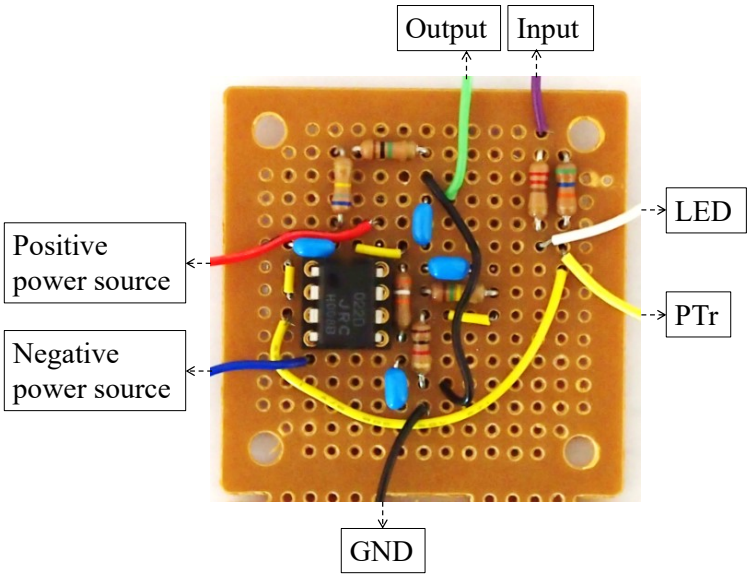


図 5.4: 実装したフィルタ・増幅回路

5.1.2 実験機器

本実験では，回路に対して電力を供給し，回路で計測した脈波を AD 変換器を経由して PC に取り込んで処理する．構築した計測装置を図 5.5 に示す．また，計測装置において，オペアンプに必要な正負電圧を出力する DC-DC コンバータを図 5.6 に示す．計測装置に含まれる機器を表 5.1 に，PC の仕様を図 5.2 に示す．5.1.1 節で述べた通り，脈波の周波数帯域の上限は 4.0 Hz であるため，標本化定理から，標本化周波数は 8.0 Hz 以上が必要である．脈波を利用して個人識別するためには十分に高い標本化周波数を設定することが望ましいため，AD 変換器の標本化周波数 1 kHz に設定した．また，同 AD 変換器が計測できる電圧の範囲は -10 V から 10 V であり，個人識別のための分解能として 0.100 mV を満たすために量子化数 16 bit に設定し，最大量子化誤差 $(10-(-10))/2^{16} = 0.031$ mV を得た．

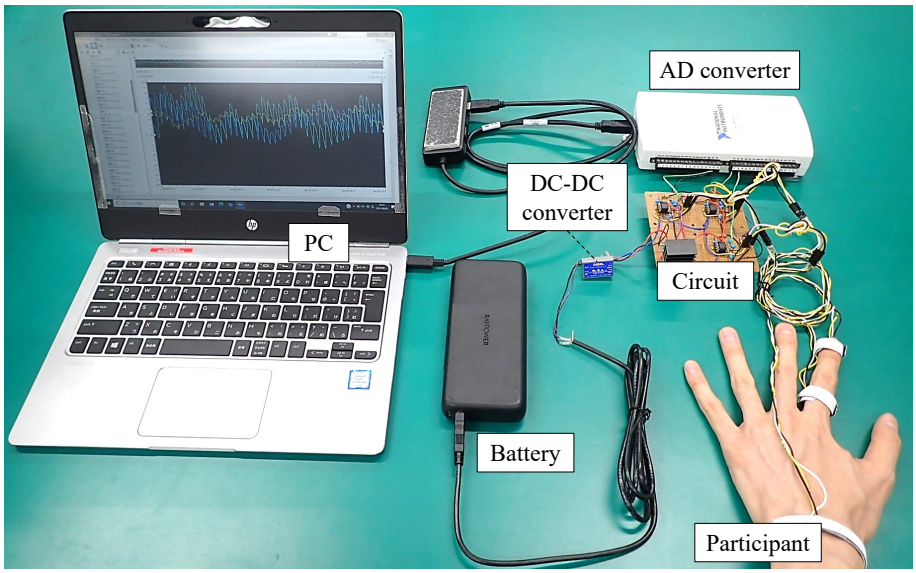


図 5.5: 計測装置

図 5.6: DC-DC コンバータ

表 5.1: 計測装置に含まれる機器

機器名	用途	型番
電源	脈波計測回路への電力供給 (+5 V)	RAVPower RP-PB201
DC-DC コンバータ	回路中のオペアンプへの電力供給 (±12 V)	COSEL ZUW1R50512
AD 変換器	回路出力信号取得	NATIONAL INSTRUMENTS USB-6216

表 5.2: 使用した PC

項目	型番・性能
OS	Microsoft Windows 10 Enterprise
CPU	Intel Core i5 2.50 GHz
メモリ	8.0 GB

5.2 情報漏洩検証と特徴量評価の手順

本節では，情報漏洩検証と特徴量評価の手順を説明する．実験手順の概要を図 5.7 に示す．本実験では，まず，各実験参加者の複数部位で脈波を計測し，各脈波および抽出した特徴量の比較により，認証に必要な情報の漏洩を検証する．続いて，同特徴量や，識別器を利用して，認証および攻撃を実施し，評価指標を得る．同時に，認証および攻撃における特徴量の寄与を評価し，特徴量を選定して，再度認証および攻撃を実施し，評価指標を得る．

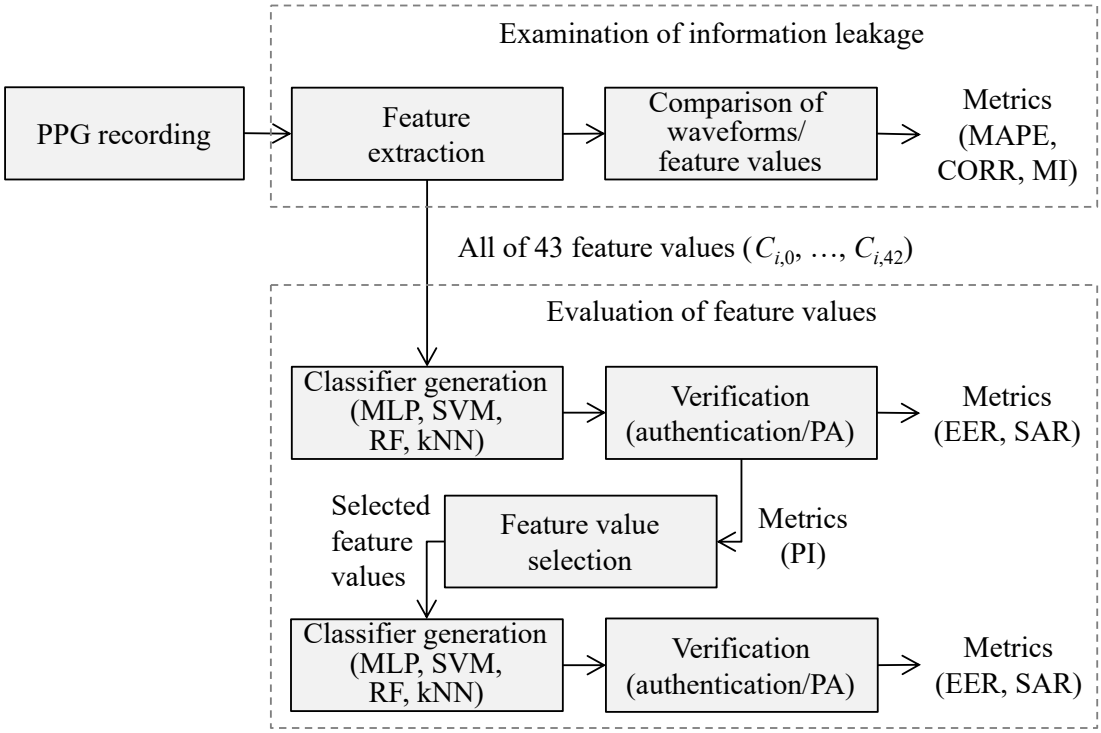


図 5.7: 実験手順の概要

5.2.1 脈波計測および計測後の処理

実装した脈波計測装置を用いて，実験参加者の脈波を計測した．計測には男性 11 名，女性 1 名，計 12 名 (P0，P1，…，P11，平均年齢 27.3 ± 1.8 歳) が参加し，図 5.1 に示した全 3 部位での脈波計測を行った．参加者は全員右利きだったため，スマートウォッチと同様に利き手とは逆の手指で脈波計測を行うと想定し，左手指の全 3 部位を計測部位とした．計測時は椅子に着座し，30 s 間の計測を 1 試行として，全 5 試行 (T0, T1, ..., T4) を実施した．

本実験では，既存の脈波認証手法 [57] と同様に，実験参加者から計測した脈波 $v_{\mathrm{raw}}[n]$ から特徴量を抽出する前に，式 (5.1) により平均 0，標準偏差 1 となるように標準化を行った．ただし，μ_{raw} は $v_{\mathrm{raw}}[n]$ の平均，σ_{raw} は $v_{\mathrm{raw}}[n]$ の標準偏差である．

$$v_{\mathrm{std}}[n] = \frac{v_{\mathrm{raw}}[n] - \mu_{\mathrm{raw}}}{\sigma_{\mathrm{raw}}} \tag{5.1}$$

本実験における特徴量は，脈波を 1 周期毎に分割して得られる信号 (セグメント) から抽出した．まず，図 5.8 に示すように，標準化した脈波から極小値を 2 点抽出した．続いて，その二つの極小値間に極大値が 1 点含まれている場合，極小値 2 点およびその間に含まれるデータ点の集合を 1 セグメントとして分割した．以下では，i 番目のセグメントに含まれるデータ点数を N_i とする．

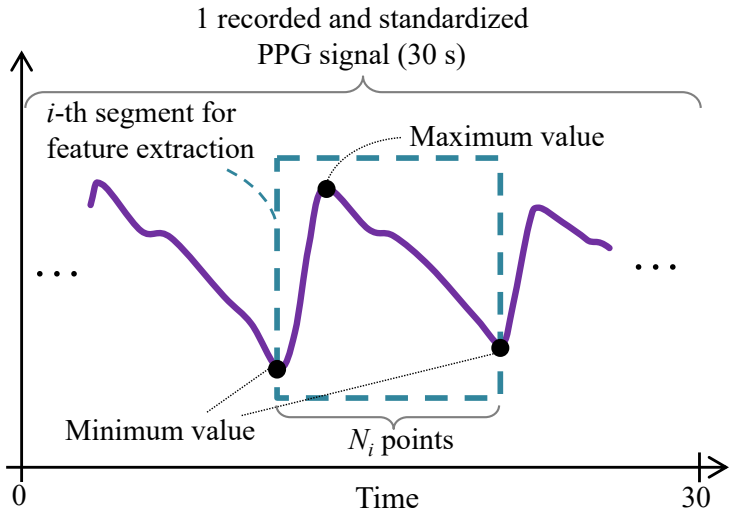


図 5.8: 脈波からのセグメント抽出

5.2.2 脈波間の相関の指標

計測された脈波 $v^{\mathrm{wr}}[n]$，$v^{\mathrm{pr}}[n]$，$v^{\mathrm{ft}}[n]$ の各信号間の相関の指標として，式 (5.2), (5.3) に示す Pearson の積率相関係数 (CORR: Correlation coefficient) [92] を求めた．ただし，$v_i^{\mathrm{wr}}[n]$, $v_i^{\mathrm{pr}}[n]$, $v_i^{\mathrm{fi}}[n]$ は，それぞれ $v^{\mathrm{wr}}[n]$，$v^{\mathrm{pr}}[n]$，$v^{\mathrm{fi}}[n]$ の i 番目のセグメントである．また，$\bar{v}_i^{\mathrm{wr}}$，$\bar{v}_i^{\mathrm{pr}}$，$\bar{v}_i^{\mathrm{fi}}$ はそれぞれ $v_i^{\mathrm{wr}}[n]$, $v_i^{\mathrm{pr}}[n]$, $v_i^{\mathrm{fi}}[n]$ の平均である．

$$\mathrm{CORR}_i^{\mathrm{wr,pr}} = \frac{\sum_{n=0}^{N-1}(v_i^{\mathrm{wr}}[n]-\bar{v}_i^{\mathrm{wr}})(v_i^{\mathrm{pr}}[n]-\bar{v}_i^{\mathrm{pr}})}{\sqrt{\sum_{n=0}^{N-1}(v_i^{\mathrm{wr}}[n]-\bar{v}_i^{\mathrm{wr}})^2}\sqrt{\sum_{n=0}^{N-1}(v_i^{\mathrm{pr}}[n]-\bar{v}_i^{\mathrm{pr}})^2}} \tag{5.2}$$

$$\mathrm{CORR}_i^{\mathrm{wr,fi}} = \frac{\sum_{n=0}^{N-1}(v_i^{\mathrm{wr}}[n]-\bar{v}_i^{\mathrm{wr}})(v_i^{\mathrm{fi}}[n]-\bar{v}_i^{\mathrm{fi}})}{\sqrt{\sum_{n=0}^{N-1}(v_i^{\mathrm{wr}}[n]-\bar{v}_i^{\mathrm{wr}})^2}\sqrt{\sum_{n=0}^{N-1}(v_i^{\mathrm{fi}}[n]-\bar{v}_i^{\mathrm{fi}})^2}} \tag{5.3}$$

5.2.3 本実験で使用した特徴量

本実験では，各部位で計測された脈波から全 43 個の特徴量 ($C_{i,0}$, ..., $C_{i,42}$) を抽出し，誤差や相関を確認することで，認証に必要な情報の漏洩を検証した．既存の脈波認証手法で用いられている特徴量として，Jindal らが提案した 11 個の特徴量 ($C_{i,0}$, ..., $C_{i,10}$) [57]，Gu らが提案した 4 個の特徴量 ($C_{i,11}$, ..., $C_{i,14}$) [93]，Siam らが提案した 24 個の特徴量 ($C_{i,15}$, ..., $C_{i,38}$) [94] を抽出した．さらに，脈波認証手法に関する研究ではないが，計測部位による値の変化の検証のため，Hartmann らが提案した 4 個の特徴量 ($C_{i,39}$, ..., $C_{i,42}$) [81] を抽出した．以下では，本実験で使用した各特徴量の概要や定義について述べる．全 43 個の特徴量とその意味の一覧は，後記の表 5.3 に記載する．

Jindal らが提案した 11 個の特徴量

Jindal らは，5.2.1 節で述べた処理により抽出した各セグメントから，11 個の特徴量 ($C_{i,0}$, ..., $C_{i,10}$) を抽出し，個人識別に使用することを提案している [57].

である．

$C_{i,0}$ は i 番目のセグメント $v_{\mathrm{std},i}[n]$ の平均であり，式 (5.4) で表される．

$$C_{i,0} = \frac{1}{N_i} \sum_{n=0}^{N_i-1} v_{\mathrm{std},i}[n] \tag{5.4}$$

$C_{i,1}$ は $v_{\mathrm{std}}[n]$ の標準偏差であり，式 (5.5) で表される．

$$C_{i,1} = \sqrt{\frac{1}{N_i} \sum_{n=0}^{N_i-1} (v_{\mathrm{std},i}[n] - C_{i,0})^2} \tag{5.5}$$

$C_{i,2}$ は，動的時間伸縮法 (DTW: Dynamic time warping) [95] により求めた，i 番目のセグメント $v_{\mathrm{std},i}[n]$ と i' 番目のセグメント $v_{\mathrm{std},i'}[n]$ の類似度であり，式 (5.6) で表される ($i' \neq i$).

$$C_{i,2} = \frac{1}{M} \sum_{i'=0}^{M-1} \mathrm{DTW}(v_{\mathrm{std},i}[n], v_{\mathrm{std},i'}[n]) \ (i \neq i') \tag{5.6}$$

$\mathrm{DTW}(v_{\mathrm{std},i}[n], v_{\mathrm{std},c}[n])$ は，以下の手順により求められる．$v_{\mathrm{std},i}[n]$ と $v_{\mathrm{std},i'}[n]$ に含まれる各点の値を $v_{i,\iota}$，$v_{i',\iota'}$ とする．ただし，$0 \leq \iota \leq N_i - 1$，$0 \leq \iota' \leq N_{i'} - 1$ であり，$N_{i'}$ は i' 番目のセグメントに含まれるデータ点数である．$v_{i,\iota}$，$v_{i',\iota'}$ を用いて $\delta(\iota, \iota') = |v_{i,\iota} - v_{i',\iota'}|$ と定義すると，DTW は式 (5.7) で表される．ただし，$\max(N_i, N_{i'}) \leq K \leq N_i + N_{i'} - 1$ であり，$\max(N_i, N_{i'})$ は N_i と $N_{i'}$ を比較して小さくない方の数値を表す．また，$\min \sum_{\kappa=0}^{K-1} \delta(\iota, \iota')$ は，$0 \leq \kappa \leq K - 1$ における $\delta(\iota, \iota')$ の最小値を表す．

$$\mathrm{DTW}(v_{\mathrm{std},i}[n], v_{\mathrm{std},i'}[n]) = \min \sum_{\kappa=0}^{K-1} \delta(\iota, \iota') \tag{5.7}$$

同アルゴリズムは，抽出したセグメント中の最大値や最小値，さらに最大値や最小値となる時刻も特徴量として使用する．$C_{i,3}$，$C_{i,4}$ は $v_{\mathrm{std},i}[n]$ の最大値と最小値であり，それぞれ式 (5.8)，(5.9) で表される．

$$C_{i,3} = \max_{n \in [0, N_i - 1]} v_{\mathrm{std},i}[n] \tag{5.8}$$

$$C_{i,4} = \min_{n \in [0, N_i - 1]} v_{\mathrm{std},i}[n] \tag{5.9}$$

$C_{i,5}$，$C_{i,6}$ は，$v_{\mathrm{std},i}[n]$ がそれぞれ最大，最小を示す時刻であり，式 (5.10)，(5.11) で表される．

$$C_{i,5} = \underset{n\in[0,N_i-1]}{\arg\max}\, v_{\mathrm{std},i}[n] \tag{5.10}$$

$$C_{i,6} = \underset{n\in[0,N_i-1]}{\arg\min}\, v_{\mathrm{std},i}[n] \tag{5.11}$$

同アルゴリズムは，抽出したセグメントに対してウェーブレット変換を行って得られる信号も特徴量抽出に利用する．$C_{i,7}$，$C_{i,8}$ は式 (5.14) で表される，$v_{\mathrm{std},i}[n]$ に離散ウェーブレット変換を施して得られる係数の最大値および最小値であり，それぞれ式 (5.12)，(5.13) で表される．

$$C_{i,7} = \max_{n\in[0,N_i-1]} W_{\mathrm{std},i}[b,a] \tag{5.12}$$

$$C_{i,8} = \min_{n\in[0,N_i-1]} W_{\mathrm{std},i}[b,a] \tag{5.13}$$

ただし，$W_{\mathrm{std},i}$ は式 (5.14) で表され，ψ はマザーウェーブレット，b はトランスレート，a はスケールパラメータである．また，$\overline{\psi}$ は ψ の複素共役を表す．

$$W_{\mathrm{std},i}[b,a] = \frac{1}{\sqrt{a}} \sum_{n=0}^{N_i-1} v_{\mathrm{std},i}[n] \overline{\psi\left(\frac{n-b}{a}\right)} \tag{5.14}$$

同アルゴリズムは，脈波から抽出したセグメントの形状を表す指標も特徴量として抽出する．$C_{i,9}$ は $v_{\mathrm{std},i}[n]$ の歪度であり，$v_{\mathrm{std},i}[n]$ の平均 $C_{i,0}$ および標準偏差 $C_{i,1}$ を用いて式 (5.15) で表される [96]．

$$C_{i,9} = \frac{1}{N_i {C_{i,1}}^3} \sum_{n=0}^{N_i-1} \left(v_{\mathrm{std},i}[n] - C_{i,0}\right)^3 \tag{5.15}$$

$C_{i,10}$ は $v_{\mathrm{std},i}[n]$ の尖度であり，式 (5.15) と同様に，$C_{i,0}$ および $C_{i,1}$ を用いて式 (5.16) で表される [97]．

$$C_{i,10} = \frac{\displaystyle\sum_{n=0}^{N_i-1} \left(v_{\mathrm{std},i}[n] - C_{i,0}\right)^4}{{C_{i,1}}^4} \tag{5.16}$$

Gu らが提案した 4 個の特徴量

Gu らは，離散信号として得た脈波および脈波の一階差分を計算して得られる信号から，図 5.9 に示す 4 個の特徴量 $C_{i,11}$，…，$C_{i,14}$ を抽出して認証に使用している [93].

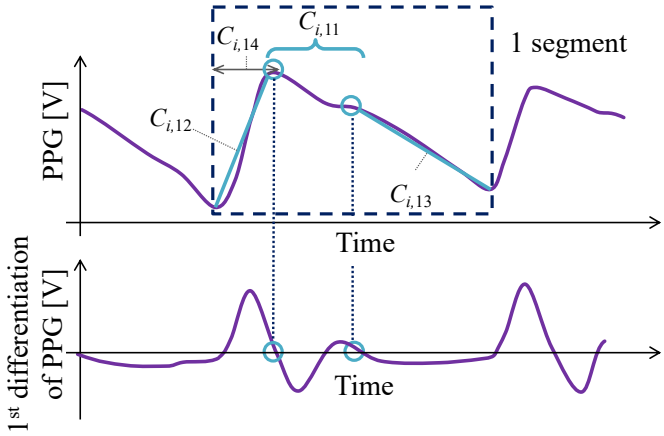


図 5.9: Gu らが提案する特徴量および抽出の概要

本実験では，1 セグメントに含まれる極大値の個数を特徴量 $C_{i,11}$ として使用する．同特徴量は，脈波の一階差分を計算して得られる信号において，値の符号が正から負に変わる点の個数として求められる．

1 セグメントの開始時刻と，1 個目の極大値との間の正の傾きを特徴量 $C_{i,12}$ として使用する．同特徴量は，脈波の一階差分を計算して得られる信号において，値の符号が正から負に変わる点のうち，1 個目の点の時刻である．i 番目のセグメントにおける，1 個目の極大値を $v_{\max,i,0}$，1 個目の極大値の時刻を $n_{\max,i,0}$ とすると，$C_{i,12}$ は式 (5.17) で表される．

$$C_{i,12} = \frac{v_{\max,i,0} - v_{\mathrm{std},i}[1]}{n_{\max,i,0}} \tag{5.17}$$

2 個目の極大値と 1 セグメントの終了時刻との間の負の傾きを特徴量 $C_{i,13}$ として使用する．同特徴量は，脈波の一階差分を計算して得られる信号において，値の符号が正から負に変わる点のうち，2 個目の点の時刻である．i 番目のセグメントにおける，2 個目の極大値を $v_{\max,i,1}$，2 個目の極大値の時刻を $n_{\max,i,1}$ とすると，$C_{i,13}$ は式 (5.17) で表される．

$$C_{i,13} = \frac{v_{\mathrm{std},i}[N_i] - v_{\max,i,1}}{N_i - n_{\max,i,1}} \tag{5.18}$$

さらに，1 個目の極大値の時刻を特徴量 $C_{i,14}$ として使用する．$C_{i,14}$ は式 (5.18) で表される．

$$C_{i,14} = n_{\max,i,0} \tag{5.19}$$

Siam らが提案した 24 個の特徴量

Siam らは，音声認識で用いられることの多い特徴量である，メル周波数ケプストラム係数を脈波認証における特徴量として使用することを提案している [94]．以下では，本実験で使用する 24 個の特徴量 (MFCC0，...，MFCC23) である，メル周波数ケプストラム係数 $C_{i,15}$, ...，$C_{i,38}$ を脈波から抽出する手順を示す．

脈波に対して離散フーリエ変換を適用して得られる振幅を求める．その際，高周波帯域を強調するため，プリエンファシス係数 ρ を利用したプリエンファシスフィルタを適用する [98]．$v[n]$ に対してプリエンファシスフィルタを適用して得られる信号 $v_{\mathrm{pre}}[n]$ は，式 (5.20) で表される．一般に，$\rho = 0.97$ が用いられる．

$$v_{\mathrm{pre}}[n] = v[n] - \rho v[n-1] \tag{5.20}$$

続いて，式 (5.21) に示すように，式 (5.20) に対して離散フーリエ変換を適用して振幅を求める [98]．ただし，$h[n]$ は窓関数であり,，対象の信号の不連続性に由来する雑音の発生を抑制するために使用する．

$$V_{\mathrm{dft}}[k] = \sum_{n=0}^{N-1} v_{\mathrm{pre}}[n] h[n] \exp\left(-\frac{2\pi k n}{N}\right) \tag{5.21}$$

本実験では，窓関数として，脈波をはじめとする生体信号の解析で使用されている，Hamming 窓を採用する [94, 99]．Hamming 窓は，式 (5.22) で表される [100]．

$$h[n] = 0.54 - 0.46 \cos\frac{2\pi n}{N} \tag{5.22}$$

式 (5.21) で求めた振幅 $V_{\mathrm{dft}}[k]$ に対して，人間の聴覚特性に基づき，式 (5.23) に示す対数変換 (Mel-scale 変換) を施す [98, 101]．ただし，対数の底は，慣習的に使用されている Napier 数 $e = 2.718...$ である [102]．

$$V_{\mathrm{mel}}[k] = 1127.01048 \log_e\left(\frac{V_{\mathrm{dft}}[k]}{700.0} + 1.0\right) \tag{5.23}$$

式 (5.23) で得た $V_{\mathrm{mel}}[k]$ に対して，メルフィルタバンクを適用することで，特定の個数の振幅のみを抽出する．メルフィルタバンクとは，図 5.10 に示す三角窓のバンドパスフィルタ $H_0[k], H_1[k], H_2[k], \ldots$ の集合である．各バンドパスフィルタ間の間隔は，対数軸において等間隔になるように設計されている．メルフィルタバンク中の g 番目のフィルタ $H_g[k]$ は，式 (5.24) で表される [103].

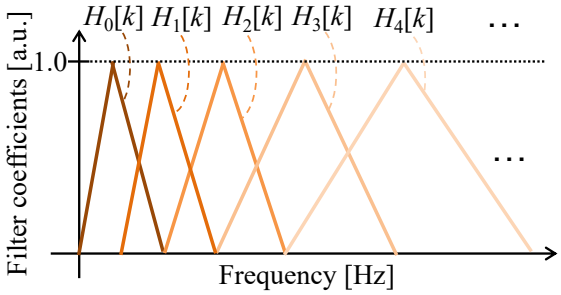


図 5.10: メルフィルタバンク

$$H_g[k] = \begin{cases} 0, & g < V[k-1] \\ \dfrac{g - V[k-1]}{V[k] - V[k-1]}, & V[k-1] \leq g \leq V[k] \\ \dfrac{V[k+1] - k}{V[k+1] - V[k]}, & V[k] \leq g \leq V[k+1] \\ 0, & g > V[k+1] \end{cases} \tag{5.24}$$

式 (5.24) で示したメルフィルタバンクを適用した振幅に対して DCT を適用し，式 (5.25) が得られる [104]．ただし，η_{all} はメルフィルタバンクの個数である．振幅に DCT による直交変換を適用することで，最終的に得られる係数同士の相関が弱くなるため，認証システムにおいて使用する特徴量の個数が少なくても，個人を識別可能となる [94].

$$V_{\mathrm{dct}}[g] = \frac{2}{\eta_{\mathrm{all}}} \sum_{\eta=0}^{\eta_{\mathrm{all}}-1} V_{\mathrm{mel}}[k] H_g[k] \cos \frac{(2k+1)\eta\pi}{2\eta_{\mathrm{all}}} \tag{5.25}$$

式 (5.25) で表される $V_{\mathrm{dct}}[g]$ がメル周波数ケプストラム係数であり，本実験における特徴量として使用する．メルフィルタバンクの個数を変更することで，任意の個数のメル周波数ケプストラム係数を抽出することができる．Siam らは，脈波認証に最適なメル周波数ケプストラム係数は 24 個であると主張しているため，本

実験では，メルフィルタバンク数を 24 個と設定することで，抽出する特徴量数を 24 個とした．

Hartmann らが提案した 4 個の特徴量

本実験で使用する，Hartmann らが提案する 4 個の特徴量 ($C_{i,39}$, ..., $C_{i,42}$) および抽出の概要を図 5.11 に示す．

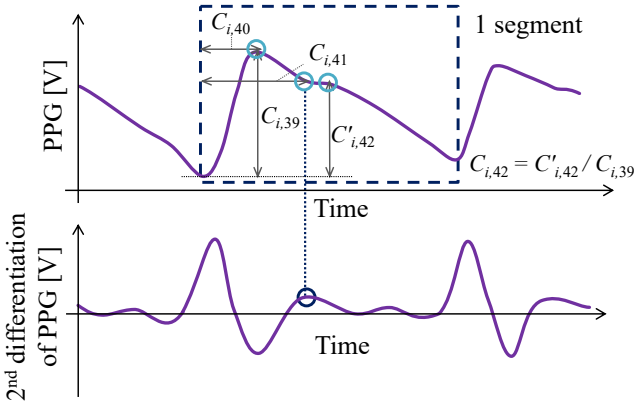


図 5.11: Hartmann らが提案する特徴量および抽出の概要

本実験では，脈波の各セグメントにおける最大値と最小値の差を特徴量として使用する．i 番目のセグメント $v_{\mathrm{std},i}[n]$ における特徴量 $C_{i,39}$ は，式 (5.26) で表される．

$$C_{i,39} = \max_{n\in[0,N_i-1]} v_{\mathrm{std},i}[n] - \min_{n\in[0,N_i-1]} v_{\mathrm{std},i}[n] \tag{5.26}$$

続いて，脈波の各セグメントにおいて最大値となる時刻を特徴量として使用する．i 番目のセグメント $v_{\mathrm{std},i}[n]$ における特徴量 $C_{i,40}$ は，式 (5.27) で表される．

$$C_{i,40} = \arg\max_{n\in[0,N_i-1]} v_{\mathrm{std},i}[n] \tag{5.27}$$

続いて，脈波の各セグメントに現れる小さな窪みである重複切痕 (Dicrotic notch) [81] の時刻を特徴量 $C_{i,41}$ として使用する．重複切痕の時刻を抽出する前に，式 (5.28) に示す通り，i 番目のセグメント $v_{\mathrm{std},i}[n]$ の二階中心差分を計算する．

$$\ddot{v}_{\mathrm{std},i}[n] = v_{\mathrm{std},i}[n+1] - 2v_{\mathrm{std},i}[n] + v_{\mathrm{std},i}[n-1] \tag{5.28}$$

i 番目のセグメント $v_{\mathrm{std},i}[n]$ における重複切痕の時刻 $C_{i,41}$ は，同セグメントにおいて最大値となる時刻後に極小値を持つ時刻であり [105]，式 (5.29) で表される．

$$C_{i,41} = \underset{n\in(C_{i,40},N_i]}{\arg\max}\ \ddot{v}_{\mathrm{std},i}[n] \tag{5.29}$$

さらに，脈波の各セグメントにおける重複切痕後の極大値と $C_{i,39}$ との比を特徴量 $C_{i,42}$ として使用する．i 番目のセグメント $v_{\mathrm{std},i}[n]$ における重複切痕の時刻は，同セグメントにおいて重複切痕となる時刻後に極大値を持つ時刻であり，同極大値 $C'_{i,41}$ は式 (5.30) で表される．

$$C'_{i,42} = \max_{n\in(C_{i,41},N_i]} v_{\mathrm{std},i}[n] \tag{5.30}$$

したがって，i 番目のセグメント $v_{\mathrm{std},i}[n]$ における重複切痕後の極大値と $C_{i,39}$ との比 $C_{i,42}$ は，式 (5.31) で表される．

$$C_{i,42} = C'_{i,41}/C_{i,39} \tag{5.31}$$

以上で述べた，全 43 個の特徴量とその意味を表 5.3 に示す．本実験では，参加者の身体上の各部位で計測された脈波から同特徴量を抽出し，認証に必要な情報の漏洩の検証に使用する．

表 5.3: 情報漏洩の検証で用いた特徴量

番号	特徴量	意味
$C_{i,0}$	平均	動脈径，組織の厚み
$C_{i,1}$	標準偏差	1 セグメントにおける動脈径の変化
$C_{i,2}$	DTW	1 試行における動脈径の変化
$C_{i,3}$	最大値	動脈径
$C_{i,4}$	最小値	動脈径
$C_{i,5}$	最大値時刻	動脈径の変化速度
$C_{i,6}$	最小値時刻	動脈径の変化速度
$C_{i,7}$	Wavelet 係数最大値	動脈径変化の周波数特性
$C_{i,8}$	Wavelet 係数最小値	動脈径変化の周波数特性
$C_{i,9}$	歪度	動脈径の変化速度
$C_{i,10}$	尖度	動脈径，動脈径の変化速度
$C_{i,11}$	極大値個数	
$C_{i,12}$	正の傾き	動脈径の変化速度
$C_{i,13}$	負の傾き	動脈径の変化速度
$C_{i,14}$	1 個目の極大値時刻	動脈径の変化速度
$C_{i,15}$〜$C_{i,38}$	MFCC0〜MFCC23	動脈径変化の周波数特性
$C_{i,39}$	振幅	動脈径の変化
$C_{i,40}$	最大値時刻	動脈径の変化速度
$C_{i,41}$	重複切痕時刻	動脈径の変化速度
$C_{i,42}$	振幅比	心臓からの駆出波に対する血管の反射波の大きさ

5.2.4 情報漏洩検証のため使用した評価指標

本実験では，各部位で計測された脈波から抽出した特徴量を比較することで，認証に必要な情報の漏洩の有無を検証した．同検証は，表 5.3 に示した各特徴量について，誤差，相関係数，相互情報量の 3 種類の評価指標を算出することで実施した．以下では，各評価指標の概要や定義について述べる．

誤差

本実験では，複数部位で計測された脈波同士から抽出した特徴量の比較のため，誤差を評価指標として利用した．誤差の算出の際は，手首脈波から抽出した特徴量を真値とした．ただし，脈波から抽出する特徴量には，振幅や時間等の次元が異なるものが存在するため，各特徴量の値域が大きく異なる場合があり，比較が難しい場合がある．本実験では，平均絶対誤差率 (MAPE: Mean absolute percentage error) を使用することで，誤差を真値に対する割合として算出した．手首脈波と指先脈波から抽出した特徴量間の MAPE を式 (5.33) に，手首脈波と基節部脈波から抽出した特徴量間の MAPE を式 (5.33) に示す [106]．ただし，$m = 0, 1, ..., 42$ は特徴量の番号，I_{all} は特徴量を抽出した全セグメント数，$C^{\mathrm{wr}}_{i,m}$ は真値とみなした手首脈波から抽出した特徴量，$C^{\mathrm{fi}}_{i,m}$ は指先脈波から抽出した特徴量，$C^{\mathrm{pr}}_{i,m}$ は基節部脈波から抽出した特徴量を表す．

$$\mathrm{MAPE}^{\mathrm{fi}}_{m} = \frac{1}{I_{\mathrm{all}}} \sum_{i=0}^{I_{\mathrm{all}}-1} \left| \frac{C^{\mathrm{wr}}_{i,m} - C^{\mathrm{fi}}_{i,m}}{C^{\mathrm{wr}}_{i,m}} \right| \tag{5.32}$$

$$\mathrm{MAPE}^{\mathrm{pr}}_{m} = \frac{1}{I_{\mathrm{all}}} \sum_{i=0}^{I_{\mathrm{all}}-1} \left| \frac{C^{\mathrm{wr}}_{i,m} - C^{\mathrm{pr}}_{i,m}}{C^{\mathrm{wr}}_{i,m}} \right| \tag{5.33}$$

特徴量間の相関係数

本実験では，複数部位で計測された各脈波から抽出した特徴量の相関を調査するために，特徴量間についても Pearson の積率相関係数を算出した．手首脈波と指先脈波から抽出した特徴量間の相関係数を式 (5.34) に，手首脈波と基節部脈波から抽出した特徴量間の相関係数を式 (5.35) に示す [92].

$$\mathrm{CORR}_m^{\mathrm{fi}} = \frac{\sum_{i=0}^{I_{\mathrm{all}}-1}(C_{i,m}^{\mathrm{wr}} - \bar{C}_{i,m}^{\mathrm{wr}})(C_{i,m}^{\mathrm{fi}} - \bar{C}_{i,m}^{\mathrm{fi}})}{\sqrt{\sum_{i=0}^{I_{\mathrm{all}}-1}(C_{i,m}^{\mathrm{wr}} - \bar{C}_{i,m}^{\mathrm{wr}})^2}\sqrt{\sum_{i=0}^{I_{\mathrm{all}}-1}(C_{i,m}^{\mathrm{fi}} - \bar{C}_{i,m}^{\mathrm{fi}})^2}} \tag{5.34}$$

$$\mathrm{CORR}_m^{\mathrm{pr}} = \frac{\sum_{i=0}^{I_{\mathrm{all}}-1}(C_{i,m}^{\mathrm{wr}} - \bar{C}_{i,m}^{\mathrm{wr}})(C_{i,m}^{\mathrm{pr}} - \bar{C}_{i,m}^{\mathrm{pr}})}{\sqrt{\sum_{i=0}^{I_{\mathrm{all}}-1}(C_{i,m}^{\mathrm{wr}} - \bar{C}_{i,m}^{\mathrm{wr}})^2}\sqrt{\sum_{i=0}^{I_{\mathrm{all}}-1}(C_{i,m}^{\mathrm{pr}} - \bar{C}_{i,m}^{\mathrm{pr}})^2}} \tag{5.35}$$

相互情報量

Pearson の積率相関係数は，2 変量が線形関係である場合に有効な評価指標であり，非線形関係である場合には評価指標として適さない場合がある．本実験では，複数部位で計測された各脈波から抽出した特徴量が非線形関係にある場合の相関を調査するため，相互情報量 (MI: Mutual information) を算出した．手首脈波と指先脈波から抽出した特徴量間の相互情報量を式 (5.36) に，手首脈波と基節部脈波から抽出した特徴量間の相互情報量を式 (5.37) に示す [107]．ただし，$\mathrm{PRB}(C_i^{\mathrm{wr}})$ は特徴量 $C_{i,m}^{\mathrm{wr}}$ の取り得る値の確率密度関数，$\mathrm{PRB}(C_i^{\mathrm{fi}})$ は特徴量 $C_{i,m}^{\mathrm{fi}}$ の取り得る値の確率密度関数，$\mathrm{PRB}(C_i^{\mathrm{pr}})$ は特徴量 $C_{i,m}^{\mathrm{pr}}$ の取り得る値の確率密度関数，$\mathrm{PRB}(C_i^{\mathrm{fi}}, C_{i,m}^{\mathrm{wr}})$ は特徴量 $C_{i,m}^{\mathrm{fi}}$，$C_{i,m}^{\mathrm{wr}}$ の同時確率密度関数，$\mathrm{PRB}(C_i^{\mathrm{pr}}, C_{i,m}^{\mathrm{wr}})$ は特徴量 $C_{i,m}^{\mathrm{pr}}$，$C_{i,m}^{\mathrm{wr}}$ の同時確率密度関数を表す．対数の底は，慣習的に使用されている 2 と設定した [108].

$$\mathrm{MI}_m^{\mathrm{fi}} = \sum_{C_{i,m}^{\mathrm{fi}}}\sum_{C_{i,m}^{\mathrm{wr}}} \mathrm{PRB}(C_{i,m}^{\mathrm{wr}}, C_{i,m}^{\mathrm{fi}}) \log_2 \frac{\mathrm{PRB}(C_{i,m}^{\mathrm{wr}}, C_{i,m}^{\mathrm{fi}})}{\mathrm{PRB}(C_{i,m}^{\mathrm{wr}})\mathrm{PRB}(C_{i,m}^{\mathrm{fi}})} \tag{5.36}$$

$$\mathrm{MI}_m^{\mathrm{pr}} = \sum_{C_{i,m}^{\mathrm{pr}}}\sum_{C_{i,m}^{\mathrm{wr}}} \mathrm{PRB}(C_{i,m}^{\mathrm{wr}}, C_{i,m}^{\mathrm{pr}}) \log_2 \frac{\mathrm{PRB}(C_{i,m}^{\mathrm{wr}}, C_{i,m}^{\mathrm{pr}})}{\mathrm{PRB}(C_{i,m}^{\mathrm{wr}})\mathrm{PRB}(C_{i,m}^{\mathrm{pr}})} \tag{5.37}$$

5.2.5 特徴量評価のため使用した識別器

本実験では，5.2.3 節に示した全 43 個の特徴量による，認証および攻撃における寄与を，既存の脈波認証アルゴリズムにおいて，個人を識別するために使用されている識別器を利用して評価した．使用した識別器は，多層パーセプトロン (MLP: Multi layer perceptron), Support vector machine (SVM), Random forest (RF), k-Nearest neighbor (KNN) の 4 種類である．各識別器において，対象者以外の人物 (他人) が対象者 (本人) として識別される割合である他人受入率 (FAR: False acceptance rate) と，対象者が対象者以外の人物として識別される割合である本人拒否率 (FRR: False rejection rate) が一致する，等価エラー率 (ERR: Equal error rate) が得られる閾値を設定した [109]．以下では各識別器の概要を示す．

MLP の概要

MLP は，図 5.12 に示す単純パーセプトロン (SP: Simple perceptron) を連ねた識別器である．SP は，入力と出力をノードで表記し，入力 $C_0, C_1, ...$ に対して，重み係数としてそれぞれ $\gamma_0, \gamma_1, ...$ を乗じた結果を出力することを表す [110]．MLP は，SP を連ねた識別器であり，入力層・中間層・出力層で構成され，各層には複数のノードが含まれ，複数の入力に対する論理演算を行う．本実験では，Jindal らの提案 [57] および図 5.13 に示すように，MLP 各層のノード数は，入力層 11，中間層 (40, 40, 10)，出力層 12 とした．ただし，MLP のみでは，いずれの入力に対しても出力層の 1 ラベルに識別されるため，脈波からセグメントや特徴量が適切に抽出できない場合も 12 名中の 1 名に必ず識別される．本実験では，出力層で得られる各ラベルへの所属確率を利用した．識別結果となるラベルへの所属確率が閾値以上なら本人として受け入れ，閾値未満なら他人として拒否した．

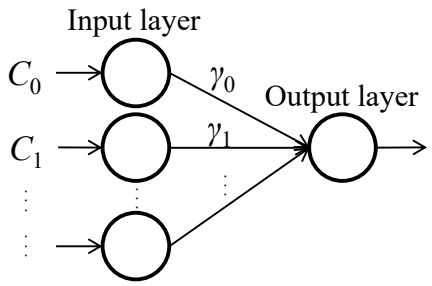


図 5.12: 単純パーセプトロン

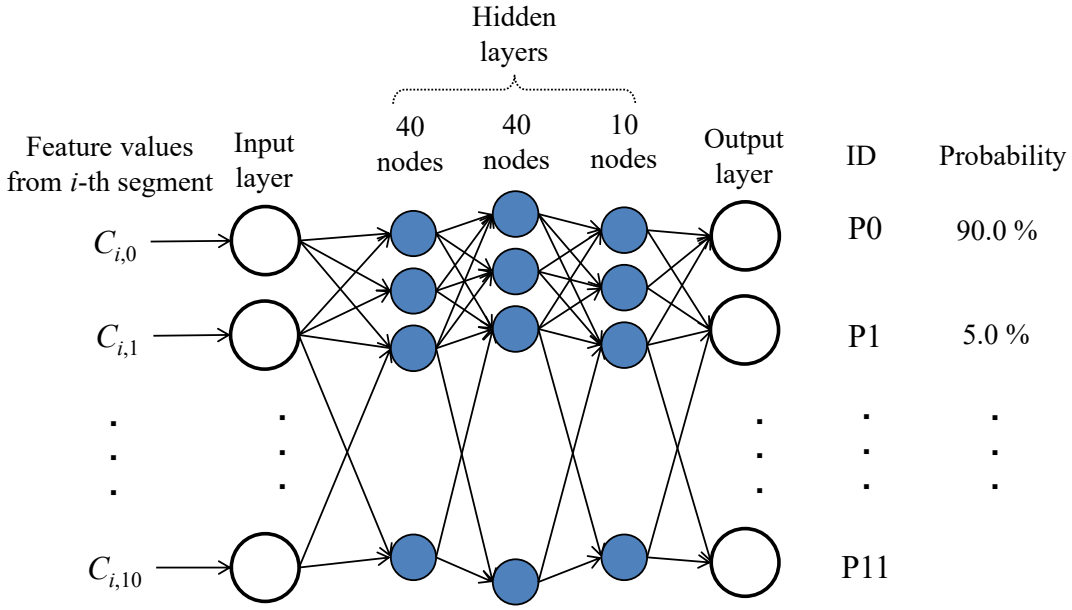


図 5.13: 実装した認証アルゴリズムに含まれる多層パーセプトロンの構成

SVM の概要

SVM は，空間にプロットしたデータ間の境界を決定する識別器であり，2 データ間の距離を最大化する平面を決定する [111]．SVM を用いて U 個の入力データ $\boldsymbol{x}_u(u = 0, 1, ..., U-1)$ を 2 クラスに分類する場合，ラベル $\boldsymbol{y}_u = 1, -1$ が $\boldsymbol{x}_u$ のクラスに該当する．SVM による識別の概要を図 5.14 に示す．図 5.14 のように，2 次元平面にプロットしたデータの全てを直線 (1 次関数) で 2 クラスに分離できる場合，または d 次元平面にプロットしたデータの全てを $(d-1)$ 次関数で 2 クラスに分離できる場合，データは線形分離可能と表現する．以下では，データを線形分離可能な場合と，線形分離不可能な場合の 2 種類に分けて説明する．

入力データ $\boldsymbol{x}_u$ が線形分離可能である場合，識別器を表す決定関数は式 (5.38) で表される [112]．ただし，$\boldsymbol{w}$ は d 次元係数ベクトル，$\boldsymbol{w}^{\mathsf{T}}$ は $\boldsymbol{w}$ の転置ベクトル，β はバイアス項を表す．

$$\boldsymbol{D}(\boldsymbol{x}) = \boldsymbol{w}^{\mathsf{T}}\boldsymbol{x}_u + \beta \tag{5.38}$$

2 クラス分類 SVM では，識別器を用いてデータをラベル $\boldsymbol{y}_u = 1, -1$ のいずれかに分類すると考える．したがって，式 (5.38) の関数を用いてデータ $\boldsymbol{x}_u$ を線形分

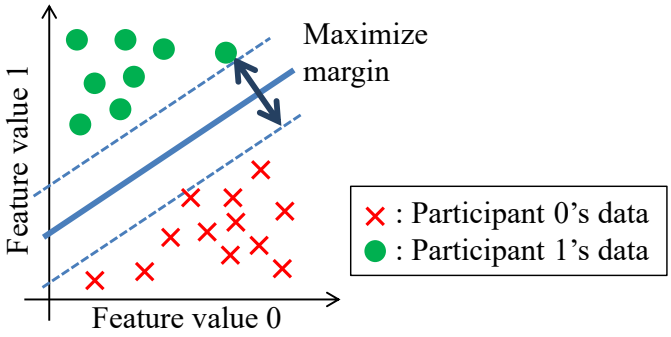


図 5.14: SVM による識別の概要 (線形分離可能な場合)

離可能である場合，式 (5.39)，(5.40) が成り立ち，式 (5.41) が得られる [112].

$$\boldsymbol{w}^{\mathsf{T}}\boldsymbol{x}_u + \beta \geq 1,\ y_u = 1 \tag{5.39}$$

$$\boldsymbol{w}^{\mathsf{T}}\boldsymbol{x}_u + \beta \leq -1,\ y_u = -1 \tag{5.40}$$

$$y_u(\boldsymbol{w}^{\mathsf{T}}\boldsymbol{x}_u + \beta) \geq 1 \tag{5.41}$$

以降では，式 (5.38) が表す平面と最も近いデータとの距離 (Margin) を最大化する平面を決定する手順を説明する．データ $\boldsymbol{x}_u$ と，平面 $\boldsymbol{y}_u(\boldsymbol{x})$ との距離 LEN_u は，式 (5.42) で表される．ただし，本節における距離関数は，SVM にて多用されるユークリッド距離である [113].

$$\mathrm{LEN}_u = \frac{\boldsymbol{D}(\boldsymbol{x}_u)}{||\boldsymbol{w}||} \tag{5.42}$$

式 (5.42) において距離 LEN_u の最大値を $\mathrm{LEN}_{\max}$ とすると，式 (5.43) が常に成り立つ必要がある．

$$\frac{\boldsymbol{D}(\boldsymbol{x}_u)}{||\boldsymbol{w}||} \geq \mathrm{LEN}_{\max} \tag{5.43}$$

式 (5.39)，(5.43) より得られる $\mathrm{LEN}_{\max}||\boldsymbol{w}|| = 1$ から，$\mathrm{LEN}_{\max}$ を最大化するためには，$||\boldsymbol{w}||$ を最小化する必要がある．したがって，各クラスに対して距離を最大化するために，式 (5.44)，(5.45) で表される最小化問題を，ラグランジュ乗数 $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, ..., \lambda_{U-1})$ を利用して，式 (5.46) で表されるラグランジュ関数とする．

$$\min_{\boldsymbol{x},\beta} \mathcal{L}(\boldsymbol{x}, \beta) = \frac{1}{2}||\boldsymbol{w}||^2 \tag{5.44}$$

$$y_u(\boldsymbol{w}^{\mathsf{T}}\boldsymbol{x}_u + \beta) \geq 1 \tag{5.45}$$

$$\min_{\boldsymbol{x},\beta,\lambda} \mathcal{L}(\boldsymbol{x}, \beta, \lambda) = \frac{1}{2}\boldsymbol{w}\boldsymbol{w}^{\mathsf{T}} - \sum_{u=0}^{U-1} \lambda_u y_u(\boldsymbol{w}^{\mathsf{T}}\boldsymbol{x}_u + \beta) - 1 \tag{5.46}$$

式 (5.46) の最適解を得るため，$\mathcal{L}$ を $\boldsymbol{x}$ で偏微分して得られる式 (5.47), $\mathcal{L}$ を β で偏微分して得られる式 (5.48) を解くと，式 (5.49)，(5.50) が得られる．

$$\frac{\partial \mathcal{L}(\boldsymbol{x}, \beta, \lambda)}{\partial \boldsymbol{x}} = \mathbf{0} \tag{5.47}$$

$$\frac{\partial \mathcal{L}(\boldsymbol{x}, \beta, \lambda)}{\partial \beta} = 0 \tag{5.48}$$

$$\boldsymbol{w} = \sum_{s=0}^{U-1} \lambda_u y_u x_u \tag{5.49}$$

$$\sum_{u=0}^{U-1} \lambda_u y_u = 0 \tag{5.50}$$

また，式 (5.46) の各項の条件から，式 (5.51)，(5.52) が得られ，$\lambda_u = 0$，または $\lambda_u \neq 0$ かつ $y_u(\boldsymbol{w}^\mathsf{T}\boldsymbol{x}_u + b) = 1$ を満たす必要がある．

$$\lambda_u y_u(\boldsymbol{w}^\mathsf{T}\boldsymbol{x}_u + \beta) - 1 = 0 \tag{5.51}$$

$$\lambda_u \geq 0 \tag{5.52}$$

また，式 (5.46)，(5.49) を解くと，式 (5.53) が得られる．

$$\max_{\boldsymbol{\lambda}} \mathcal{L}(\boldsymbol{\lambda}) = \sum_{u=0}^{U-1} \lambda_u - \frac{1}{2} \sum_{u,u'=0}^{U-1} \lambda_u \lambda_{u'} y_u y_{u'} \boldsymbol{x}_u^\mathsf{T} \boldsymbol{x}_{u'} \tag{5.53}$$

式 (5.46)，(5.50) を解くと，式 (5.54) が得られる．

$$\sum_{u=0}^{U-1} \lambda_u y_u = 0 \tag{5.54}$$

以上から，式 (5.38) で表した決定関数は，式 (5.55)，(5.56) で表すことができる．

$$D(\boldsymbol{x}) = \boldsymbol{w}^\mathsf{T}\boldsymbol{x}_u + \beta \tag{5.55}$$

$$\beta = y_u - \boldsymbol{w}_u^\mathsf{T}\boldsymbol{x}_u \tag{5.56}$$

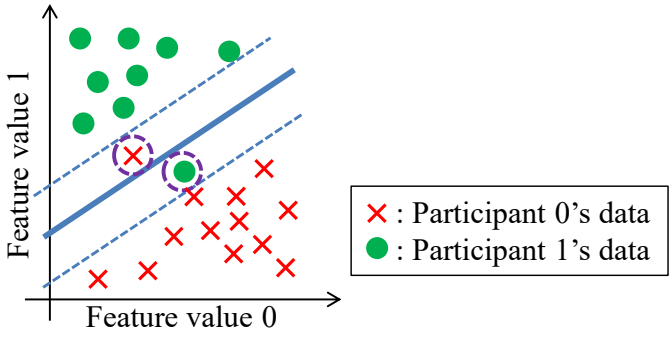


図 5.15: SVM による識別の概要 (線形分離不可能な場合)

一方，図 5.15 に示すように，入力データが線形分離不可能である場合がある．この場合は，図 5.14 に示した，線形分離可能である場合の式 (5.41) で表した条件を緩和するための変数 ξ_u を導入する [114]．この操作により，式 (5.57) が得られる．

$$\boldsymbol{y}_u(\boldsymbol{x}) = \boldsymbol{w}^{\mathsf{T}}\boldsymbol{x}_u + \beta \geq 1 - \xi_u \tag{5.57}$$

続いて，線形分離可能である場合の最適化問題を利用して，線形分離不可能である場合の最適化問題に拡張する．線形分離不可能である場合の最適化問題は，線形分離不可能なデータの許容度を表す変数 ζ を利用して，以下の式 (5.58)，(5.59) で表される．

$$\min_{\boldsymbol{w},\beta,\boldsymbol{\xi}_u} \mathcal{L}(\boldsymbol{x},\beta,\boldsymbol{\xi}_u) = \frac{1}{2}||\boldsymbol{w}||^2 + \zeta\sum_{u=0}^{U-1}\xi_u \tag{5.58}$$

$$\boldsymbol{w}^{\mathsf{T}}\boldsymbol{x}_u + \beta \geq 1,\ y_u = 1 \tag{5.59}$$

式 (5.58)，(5.59) の最適化問題を解く場合，線形分離可能である場合と同様にして，$\mathcal{L}$ を $\boldsymbol{x}$ または β で偏微分し，各項に対する条件を利用して，式 (5.60)，(5.61) が得られる．

$$\max_{\lambda}\mathcal{L}(\lambda) = \sum_{u=0}^{U-1}\lambda_u - \frac{1}{2}\sum_{u,u'=0}^{U-1}\lambda_u\lambda_h y_u y_{u'}\boldsymbol{x}_u^{\mathsf{T}}\boldsymbol{x}_{u'} \tag{5.60}$$

$$\sum_{u=0}^{U-1}\lambda_u y_u = 0 \tag{5.61}$$

線形分離不可能である場合の決定関数は，線形分離可能である場合と同様に，式 (5.55)，(5.56) で表される．

RF の概要

Random forest (RF) は，決定木と呼ばれる多数の識別器の組合せにより，高い精度での識別を可能とする．RF は多くの特徴量やクラスを扱えることから [111]，脈波から抽出する多数の特徴量を利用して，多人数の識別にも適用できる可能性がある．本節では，RF の基本である決定木および RF の概要を説明する．

RF を構成する要素である決定木 (Decision tree) の概要を図 5.16 に示す [115]．決定木自体が識別器の一種であり，入力したデータに対して識別結果であるクラスを出力する．決定木を用いて個人を識別する場合は，入力するデータが特徴量，出力されるクラスが各対象者に該当する．決定木は，多数のノード (Node, 接点) で構成され，データが入力される最上部のノードは根ノード (Root node)，クラスが出力されるノードは葉ノード (Leaf node) と呼ばれる [116]．決定木にデータが入力されると，下方の根ノード・葉ノード以外の内部ノード (Internal node) において，分割関数が与える条件に応じて下方のノードへ進み，葉ノードに達した時点でクラスが決定される．図 5.16 の赤で示した線やノードは，根ノードにデータが入力されてから，葉ノードにおいて “Participant 0” としてクラスが出力されるまでの経路を表す．

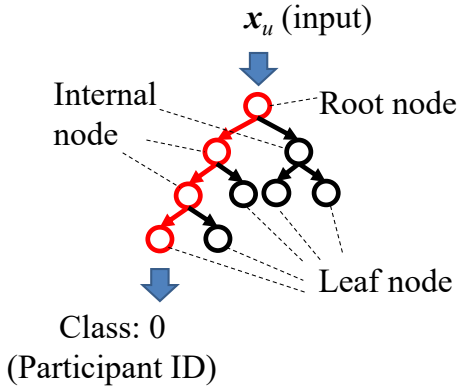


図 5.16: 決定木の概要

分割関数 CL の例を，式 (5.62) に示す．$\boldsymbol{x}_u$ は入力データ，θ はノードの番号を表す．

$$\mathrm{CL}(\boldsymbol{x}_u, \gamma_\theta) \in \{0, 1\} \tag{5.62}$$

ただし，$\gamma = (\phi, \psi, \epsilon)$ であり，ϕ は入力データ (多次元ベクトル) から特定の次元の成分を抽出する関数，ψ は分割基準のパラメータ，ϵ は分割の閾値を表す．式

(5.62) が，2 クラスの識別を行う二分決定木に含まれる分割関数である場合，分割関数は式 (5.63) で定義される．式 (5.63) において，$\epsilon_0 = \infty$ または $\epsilon_1 = -\infty$ の場合，単一の不等式で表される分割関数となる．

$$\mathrm{CL}(\boldsymbol{x}_u, \gamma_j) = [\epsilon_0 \geq \phi(\boldsymbol{x}_i) \cdot \psi \geq \epsilon_1] \tag{5.63}$$

複数の決定木を利用した，RF の概要を図 5.17 に示す．RF は，識別器を複数利用するアンサンブル学習の一つであり [117]，決定木を複数使用し，各々の識別結果を集計することで，単一の決定木よりも高い予測性能を実現する [115]．

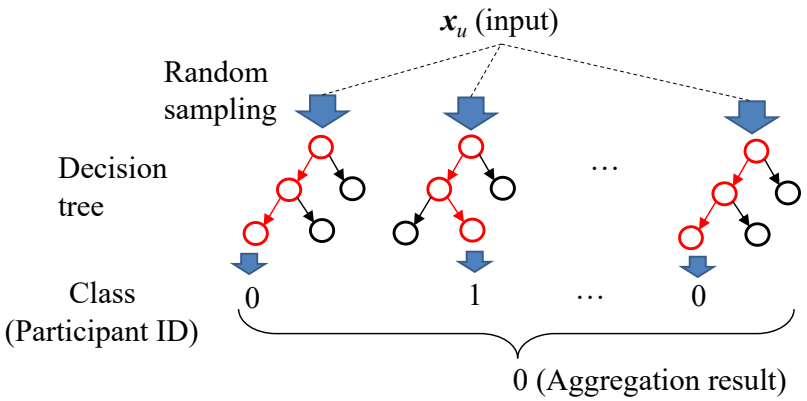


図 5.17: RF の概要

RF に対して入力されるデータを $\boldsymbol{x}_u$ とすると，決定木毎にデータに含まれる特徴量が重複を許して無作為に選択される．続いて，決定木の各接点において，分割関数のパラメータ γ の設定を無作為に行う．各決定木は，通常の決定木と同様に，識別結果としてクラスを出力する．図 5.17 の赤で示した線やノードは，各決定木の根ノードにデータが入力されてから，葉ノードにおいてクラス “Participant 0” や “Participant 1” が出力されるまでの経路を表す．最終的な識別結果は，式 (5.64) のように各決定木から求めた確率の算術平均を求めることで決定する．ただし，$\tau \in 0, 1, ..., \tau_{\mathrm{all}} - 1$ は決定木の番号を表す．$\mathrm{PRB}_{\mathrm{tr}}(u|\boldsymbol{x})$ は入力データ $\boldsymbol{x}$ に対する決定木 τ での識別結果がクラス u である確率を表す．

$$\mathrm{PRB}(u|\boldsymbol{x}) = \frac{1}{\tau_{\mathrm{all}}} \sum_{\tau=0}^{\tau_{\mathrm{all}}-1} \mathrm{PRB}_{\tau}(u|\boldsymbol{x}) \tag{5.64}$$

kNN の概要

kNN は，特徴量空間における近接性に基づいてデータを分類する識別器である [118]．kNN の概要を図 5.18 に示す．kNN は，特徴量空間に学習用データを配置し，テスト用データに対して，最も近い位置に存在する指定個数のデータのうち，最も個数の多いデータに該当するラベルを出力する．例えば，図 5.18 において，個数を 1 個と指定する場合は，実線円内にデータ 1 個が存在する Participant 0 が出力される．個数を 3 個と指定する場合は，点線円内にデータ 2 個が存在する Participant 1 が出力される．

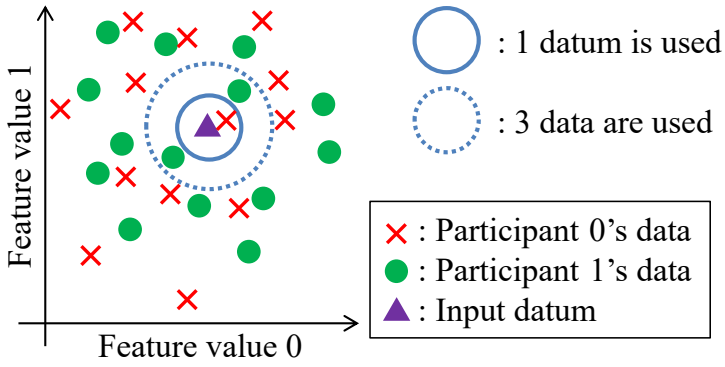


図 5.18: kNN の概要

kNN を使用する際は，特徴量間に相関が存在する場合，データ間の距離関数を選択することが重要である [119]．また，脈波から抽出する複数の特徴量の間には，相関が存在することが知られている [120]．したがって，本章における評価では，kNN における距離関数として，データに含まれる特徴量間の相関を考慮し，脈波認証を含む生体認証手法において用いられている [121, 122]，マハラノビス距離 (MD: Mahalanobis distance) を使用した．MD は式 (5.65) で表される．

$$\mathrm{MD}(\boldsymbol{C}_{\mathrm{test}}, \boldsymbol{C}_{\mathrm{train}}) = \sqrt{||\boldsymbol{C}_{\mathrm{test}} - \boldsymbol{C}_{\mathrm{train}}||^{\mathsf{T}} \boldsymbol{A}^{-1} ||\boldsymbol{C}_{\mathrm{test}} - \boldsymbol{C}_{\mathrm{train}}||}$$

ただし，$\boldsymbol{C}_{\mathrm{train}}$，$\boldsymbol{C}_{\mathrm{test}}$ はそれぞれ学習用データ，テスト用データの特徴量ベクトルであり，$\boldsymbol{A}$ は $\boldsymbol{C}_{\mathrm{train}}$ の分散共分散行列，$\boldsymbol{A}^{-1}$ は $\boldsymbol{A}$ の逆行列である．

5.2.6 特徴量の評価

本実験では，5.2.3 節に示した全 43 個の特徴量について，5.2.5 節に示した識別器を利用した評価を行う．以下では，評価の手順や，評価指標となる特徴量重要度について述べる．

特徴量の評価手順

認証や攻撃における特徴量を評価する前に，全参加者の手首脈波に含まれる全セグメントから特徴量を抽出して各識別器を生成し，式 (5.67) で正解率を算出して識別性能を確認すると同時に，各識別器による受入・拒否に必要な閾値を導出した．本手順では，5-fold 交差検証に基づいて正解率を算出した．全参加者の 1 試行分の手首脈波に含まれる全セグメントから特徴量を抽出して 1 データとし，全 5 試行のうち 4 試行を学習用データとし，残りの 1 試行をテスト用試行とする処理を繰り返し，全試行が一回ずつテスト用データとして使われるようにした．本実験で行った，5-fold 交差検証におけるデータの組合せ例として，試行 T0-T3 を学習用データ，試行 T4 をテスト用データとした場合を図 5.19 に示す．

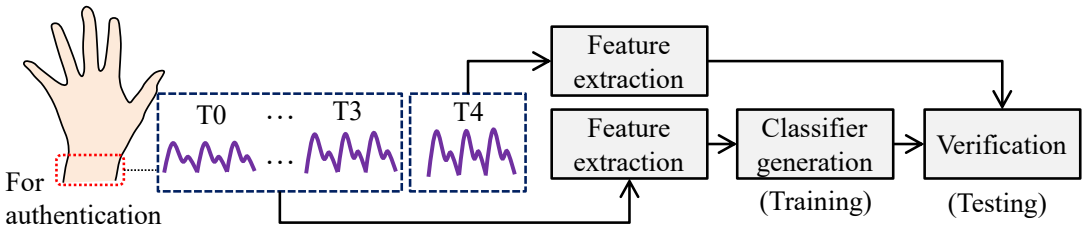


図 5.19: 認証における特徴量評価時のデータ組合せ例

続いて，攻撃における特徴量の評価を行った．本評価では，各参加者の全 5 試行分の手首脈波に含まれる全セグメントから特徴量を抽出して，各識別器を生成した．攻撃の検証として，図 4.1 **Step 5** のようにセンサへ信号を入力する代わりに，攻撃者が不正に計測したとみなす脈波から特徴量を抽出し，同 MLP へ入力した際の出力を確認した．前段落で述べた閾値を用いて，所属確率が閾値以上であれば攻撃成功したセグメント，閾値未満であれば攻撃失敗したセグメントとみなした．本実験では，全 5 試行のうち 4 試行の手首脈波をテスト用データとし，残りの 1 試行の基節部脈波または指先脈波から推定した手首脈波を学習用データとする処理を繰り返し，全試行が一回ずつテスト用試行として使われるようにし

た．本実験におけるデータの組合せ例として，試行 T0-T3 の手首脈波を学習用データ，試行 T4 の指先脈波をテスト用データとした場合を図 5.20 に示す．

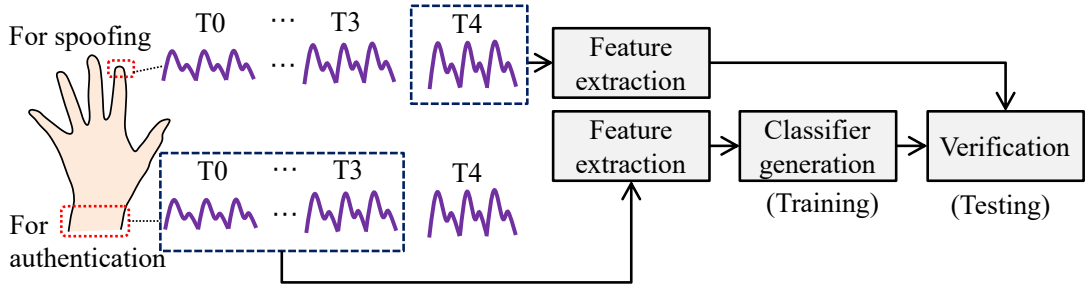


図 5.20: 攻撃における特徴量評価時のデータ組合せ例

攻撃の評価として，FRR と FAR，EER と比較するため，1 試行においてセグメントが受け入れられる割合 SAR (Segment acceptance rate) を式 (5.65) で定義した．ただし，T は試行の番号，T_{all} は全試行数，$M_{\mathrm{suc},T}$ は T 番目の試行で計測した脈波に含まれる全 M_T セグメントのうち攻撃成功したセグメント数である．

$$\mathrm{SAR} = \frac{\sum_{T=0}^{T_{\mathrm{all}}-1} M_{\mathrm{suc},T}}{\sum_{T=0}^{T_{\mathrm{all}}-1} M_T} \tag{5.65}$$

特徴量重要度

認証および攻撃における特徴量の評価では，5.2.3 節に示した全 43 個の特徴量について，認証および攻撃における寄与を，式 (5.66) に示される特徴量重要度 (PI: Permutation importance) [123] を，式 (5.67) で表される正解率 (ACC: Accuracy) を利用して算出し，評価した．$\mathrm{ACC}_{l,m}$ は特徴量ベクトル中の特徴量 m の順番を無作為に変更した際の正解率，L は繰り返し回数を表す．また，TP は True positive，TN は True negative，FP は False positive，FN は False negative を表す．

$$\mathrm{PI}_m = \mathrm{ACC} - \frac{1}{L}\sum_{l=0}^{L-1} \mathrm{ACC}_{l,m}, \tag{5.66}$$

$$\mathrm{ACC} = \frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}} \tag{5.67}$$

続いて，各特徴量について算出した PI の大小を比較して，特徴量の組合せを変更した．既存の脈波認証に関する研究では，使用する特徴量の適切な個数は 15 個から 24 個と示されていることから [94,120,124]，本実験では，特徴量の組合せを以下の 4 種類 i), ii), iii), iv) で変更し，各識別器を用いて認証および攻撃を再度検証した際の，認証精度 EER および攻撃成功率 SAR を算出し，比較した．ii), iii), iv) は特徴量の個数が同一である組合せであり，iii) は攻撃における PI の大きな特徴量のみであり，ii) は認証における PI の大きな特徴量であるが，攻撃における PI の大きな特徴量が一部含まれる可能性があり，iv) は攻撃における PI の大きな特徴量が含まれないという点で異なる．特に，ii), iii), iv) の比較により，攻撃における PI の大きな特徴量の使用による，SAR への寄与を確認する．

i) 全 43 個

ii) 認証における PI の大きい特徴量上位 20 個

iii) 攻撃における PI の大きい特徴量上位 20 個

iv) 認証における PI の大きい特徴量のうち，iii) を除いた上位 20 個

5.3 情報漏洩の検証結果

本節では，5.2 節で手順を説明した，実験参加者から計測した脈波や，情報漏洩の検証のため実施した波形や特徴量の評価結果を示す．

5.3.1 計測された脈波間の相関

本実験にて，3 部位で同時に計測された脈波の例を図 5.21 に示す．$\mathrm{PPG}^{\mathrm{wr}}$，$\mathrm{PPG}^{\mathrm{pr}}$，$\mathrm{PPG}^{\mathrm{fi}}$ は，それぞれ手首脈波，基節部脈波，指先脈波を表す．式 (5.2)，(5.3) により得られる，3 部位で計測された脈波間の相関係数を表 5.4 に示す．ただし，各参加者について，全 5 試行の平均値を記載した．

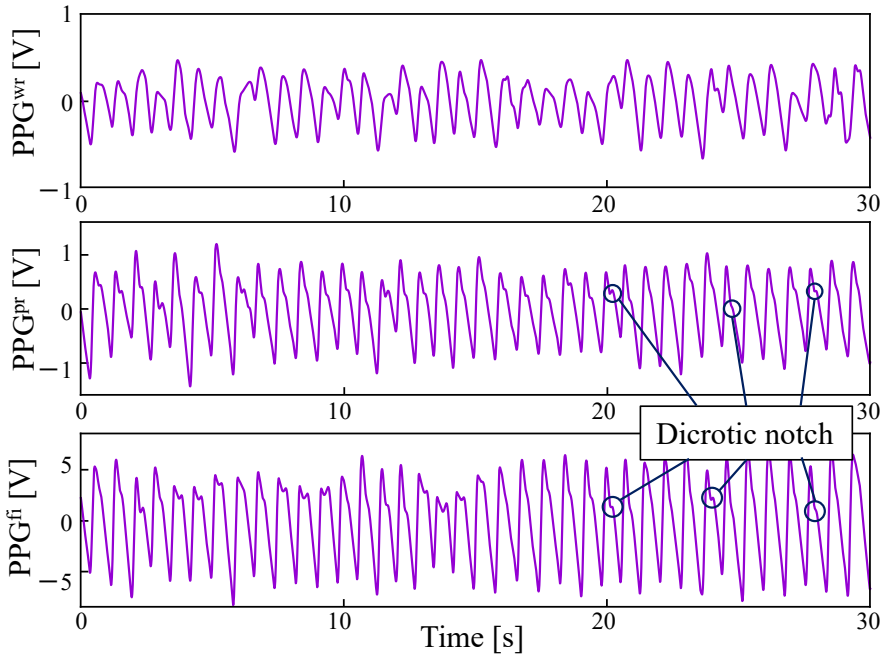


図 5.21: 計測された脈波の例

表 5.4: 3 部位で計測された脈波間の相関係数

計測部位	参加者 P0	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P1	平均 ± 標準偏差
手首，基節部	0.646	0.918	0.674	0.838	0.889	0.935	0.901	0.877	0.829	0.815	0.795	0.906	0.835 ± 0.111
手首，指先	0.750	0.882	0.674	0.845	0.914	0.960	0.772	0.877	0.819	0.753	0.822	0.880	0.829 ± 0.100

続いて，全参加者の 3 部位で計測された各脈波の各セグメントから特徴量を抽出した．表 5.5 に，本実験において各参加者の各部位で計測した脈波から抽出したセグメント数を示す．ただし，全 5 試行の平均値を記載した．

表 5.5: 計測した脈波から抽出したセグメント数

計測部位	参加者												平均 ± 標準偏差
	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	
指先	37.4	40.0	31.4	32.0	33.8	35.0	29.4	36.2	34.6	36.0	37.6	43.2	34.9 ± 3.2
基節部	36.4	41.2	31.2	30.4	32.8	34.8	29.8	35.6	34.0	35.2	37.0	42.0	34.3 ± 3.4
手首	31.4	37.4	27.4	29.0	33.2	34.8	28.2	35.0	33.4	35.4	35.0	39.4	32.7 ± 3.4

5.3.2 計測された特徴量間の相関

以下では，本実験において，3 部位で同時に計測された脈波から抽出した特徴量の誤差，相関係数，相互情報量を示す．Jindal らが提案する特徴量の誤差，相関係数，相互情報量を表 5.6 に示す．

表 5.6: Jindal らが提案する特徴量間の誤差，相関係数，相互情報量

番号	特徴量	指先			基節部		
		誤差	相関係数	相互情報量	誤差	相関係数	相互情報量
$C_{i,0}$	平均	2.487	0.015	0.074	3.125	0.153	0.028
$C_{i,1}$	標準偏差	0.624	0.248	0.036	0.543	0.307	0.086
$C_{i,2}$	DTW	0.573	0.389	0.218	0.542	0.236	0.145
$C_{i,3}$	最大値	4.052	0.136	0.063	4.277	0.245	0.098
$C_{i,4}$	最小値	0.631	0.079	0.102	0.591	0.170	0.121
$C_{i,5}$	最大値時刻	0.349	0.171	0.104	0.325	0.204	0.091
$C_{i,6}$	最小値時刻	0.057	0.398	0.353	0.069	0.214	0.475
$C_{i,7}$	Wavelet 係数最大値	0.809	0.128	0.036	0.714	0.231	0.008
$C_{i,8}$	Wavelet 係数最小値	0.431	0.210	0.042	0.406	0.166	0.015
$C_{i,9}$	歪度	0.978	0.137	0.023	0.999	0.196	0.049
$C_{i,10}$	尖度	1.177	0.153	0.028	1.023	0.171	0.034

Gu らが提案する特徴量の誤差，相関係数，相互情報量を表 5.7 に示す.

表 5.7: Gu らが提案する特徴量間の誤差，相関係数，相互情報量

番号	特徴量	指先			基節部		
		誤差	相関係数	相互情報量	誤差	相関係数	相互情報量
$C_{i,11}$	極大値個数	0.044	0.232	0.000	0.031	0.147	0.000
$C_{i,12}$	正の傾き	1.602	0.422	0.139	1.375	0.430	0.172
$C_{i,13}$	負の傾き	0.334	0.143	0.078	0.515	0.319	0.154
$C_{i,14}$	1 個目の極大値時刻	0.594	0.252	0.139	0.305	0.397	0.159

Siam らが提案する特徴量の誤差，相関係数，相互情報量を表 5.8 に示す.

表 5.8: Siam らが提案する特徴量間の誤差，相関係数，相互情報量

番号	特徴量	指先			基節部		
		誤差	相関係数	相互情報量	誤差	相関係数	相互情報量
$C_{i,15}$	MFCC0	0.916	-0.073	0.095	1.006	0.038	0.046
$C_{i,16}$	MFCC1	2.628	-0.035	0.000	3.785	0.016	0.056
$C_{i,17}$	MFCC2	1.471	-0.038	0.000	1.548	0.017	0.018
$C_{i,18}$	MFCC3	0.356	-0.093	0.000	0.411	-0.062	0.000
$C_{i,19}$	MFCC4	0.926	-0.063	0.000	0.992	-0.038	0.000
$C_{i,20}$	MFCC5	0.720	-0.070	0.000	0.766	-0.043	0.000
$C_{i,21}$	MFCC6	0.419	-0.112	0.000	0.455	-0.065	0.094
$C_{i,22}$	MFCC7	0.365	-0.089	0.000	0.433	-0.033	0.002
$C_{i,23}$	MFCC8	0.343	-0.073	0.000	0.396	-0.005	0.016
$C_{i,24}$	MFCC9	0.328	-0.081	0.000	0.368	-0.045	0.000
$C_{i,25}$	MFCC10	0.501	-0.080	0.128	0.590	-0.053	0.013
$C_{i,26}$	MFCC11	0.470	-0.095	0.030	0.501	-0.056	0.000
$C_{i,27}$	MFCC12	0.408	-0.115	0.376	0.457	-0.068	0.000
$C_{i,28}$	MFCC13	0.375	-0.100	0.188	0.431	-0.050	0.000
$C_{i,29}$	MFCC14	0.348	-0.116	0.092	0.389	-0.005	0.072
$C_{i,30}$	MFCC15	0.322	-0.088	0.000	0.373	-0.058	0.093
$C_{i,31}$	MFCC16	0.387	-0.054	0.131	0.445	-0.076	0.000
$C_{i,32}$	MFCC17	0.430	-0.126	0.000	0.460	-0.080	0.000
$C_{i,33}$	MFCC18	0.443	-0.144	0.000	0.491	-0.075	0.158
$C_{i,34}$	MFCC19	0.400	-0.110	0.000	0.425	-0.019	0.153
$C_{i,35}$	MFCC20	0.363	-0.060	0.080	0.419	-0.000	0.000
$C_{i,36}$	MFCC21	0.343	-0.052	0.005	0.386	-0.044	0.000
$C_{i,37}$	MFCC22	0.452	-0.070	0.000	0.507	-0.049	0.057
$C_{i,38}$	MFCC23	0.438	-0.064	0.095	0.495	-0.013	0.054

Hartmann らが提案する特徴量の誤差，相関係数，相互情報量を表 5.9 に示す.

表 5.9: Hartmann らが提案する特徴量間の誤差，相関係数，相互情報量

番号	特徴量	指先			基節部		
		誤差	相関係数	相互情報量	誤差	相関係数	相互情報量
$C_{i,39}$	振幅	9.869	0.212	0.329	4.371	0.033	0.247
$C_{i,40}$	最大値時刻	0.340	0.178	0.168	0.309	0.264	0.293
$C_{i,41}$	重複切痕時刻	0.114	0.335	0.149	0.101	0.471	0.243
$C_{i,42}$	振幅比	0.178	0.049	0.117	0.184	0.146	0.052

5.4 特徴量の評価結果

各特徴量について PI を算出し，その大小を比較して得られた順位 (PI 順位) を表 5.10 に示す．ただし，攻撃時の PI の算出には，表 5.6，5.7，5.8，5.9 において，基節部脈波よりも，誤差が小さく，相関係数や相互情報量が大きい傾向があった，指先脈波から抽出した特徴量を使用した.

表 5.10: 各特徴量の PI 順位

変数名	特徴量の概要	PI 順位 (認証/攻撃)							
		MLP		SVM		RF		kNN	
$C_{i,0}$	平均	27	26	30	42	6	22	14	40
$C_{i,1}$	標準偏差	11	8	22	5	8	32	21	22
$C_{i,2}$	DTW	2	3	2	9	2	2	1	17
$C_{i,3}$	最大値	31	30	36	32	25	8	13	15
$C_{i,4}$	最小値	18	9	21	43	24	10	33	30
$C_{i,5}$	最大値時刻	5	15	8	11	7	43	4	6
$C_{i,6}$	最小値時刻	36	33	35	38	4	4	34	26
$C_{i,7}$	Wavelet 係数最大値	7	17	13	24	22	14	5	33
$C_{i,8}$	Wavelet 係数最小値	4	5	6	10	55	17	6	20
$C_{i,9}$	歪度	8	14	9	3	3	6	34	29
$C_{i,10}$	尖度	12	35	14	27	20	21	7	36
$C_{i,11}$	極大値個数	38	23	39	30	16	35	2	8
$C_{i,12}$	正の傾き	10	4	4	2	15	3	9	37
$C_{i,13}$	負の傾き	13	20	10	22	21	7	20	28
$C_{i,14}$	1 個目の極大値時刻	9	13	7	43	13	16	24	11
$C_{i,15}$	MFCC0	3	7	5	14	19	19	29	7
$C_{i,16}$	MFCC1	42	39	42	19	18	42	36	2
$C_{i,17}$	MFCC2	39	31	41	31	17	37	25	10
$C_{i,18}$	MFCC3	33	19	32	17	26	36	30	13
$C_{i,19}$	MFCC4	43	22	43	28	23	33	37	12
$C_{i,20}$	MFCC5	28	27	38	16	10	38	27	16
$C_{i,21}$	MFCC6	32	18	31	36	29	40	18	31
$C_{i,22}$	MFCC7	17	38	40	23	30	20	38	38
$C_{i,23}$	MFCC8	37	40	29	34	31	13	31	42
$C_{i,24}$	MFCC9	19	41	28	26	32	25	39	35
$C_{i,25}$	MFCC10	14	32	16	29	43	39	41	9
$C_{i,26}$	MFCC11	25	28	18	20	34	27	10	19
$C_{i,27}$	MFCC12	20	37	17	35	35	30	40	4
$C_{i,28}$	MFCC13	16	42	26	25	36	11	11	41
$C_{i,29}$	MFCC14	41	16	33	40	37	26	43	25
$C_{i,30}$	MFCC15	29	11	15	12	38	23	8	27
$C_{i,31}$	MFCC16	15	34	20	6	39	34	24	14
$C_{i,32}$	MFCC17	40	36	19	15	40	29	35	23
$C_{i,33}$	MFCC18	24	24	23	33	41	31	32	39
$C_{i,34}$	MFCC19	26	29	24	39	14	28	22	32
$C_{i,35}$	MFCC20	34	25	25	21	42	18	26	3
$C_{i,36}$	MFCC21	21	43	11	37	28	41	19	24
$C_{i,37}$	MFCC22	22	21	27	13	27	12	17	43
$C_{i,38}$	MFCC23	35	10	12	18	33	24	42	18
$C_{i,39}$	振幅	30	12	37	41	12	15	28	34
$C_{i,40}$	最大値時刻	1	1	3	4	11	5	12	5
$C_{i,41}$	重複切痕時刻	6	12	1	1	1	1	15	1
$C_{i,42}$	振幅比	23	6	34	8	9	9	3	21

表 5.11 に，特徴量と識別器の組合せによる，認証精度 EER と攻撃成功率 SAR の比較を示す．ただし，攻撃時の PI の算出には，表 5.10 の PI 順位と同様に，指先脈波から抽出した特徴量を使用した．

表 5.11: 特徴量と識別器の組合せによる，認証精度と攻撃成功率の比較

識別器	評価指標	特徴量の組合せ			
		i)	ii)	iii)	iv)
MLP	EER	0.015	0.010	0.006	0.029
	SAR	0.279	0.272	0.274	0.130
SVM	EER	0.010	0.007	0.011	0.031
	SAR	0.242	0.234	0.252	0.144
RF	EER	0.005	0.004	0.005	0.027
	SAR	0.222	0.226	0.249	0.084
kNN	EER	0.001	0.001	0.002	0.002
	SAR	0.197	0.233	0.244	0.149

5.5 情報漏洩の検証結果の考察

5.5.1 波形に着目した考察

本実験では，実験参加者の身体上の 3 部位で同時に脈波を計測し，各波形を比較することで，認証に必要な情報の漏洩の有無を検証した．図 5.21 に示した計測結果の波形から，計測部位の異なる脈波間でも，振幅等には差が存在するが，同程度の周期で増減を繰り返すことが確認できた．したがって，計測部位の異なる脈波間において，相関が存在することが定性的に確認できた．また，表 5.4 で示した通り，異なる部位で計測した脈波間の相関係数を算出した結果，全参加者の相関係数の平均および標準偏差は，$\mathrm{CORR}^{\mathrm{wr,pr}} = 0.835 \pm 0.111$，$\mathrm{CORR}^{\mathrm{wr,pr}} = 0.829 \pm 0.100$ であった．Patil らは，脈波を認証に用いることを想定して，特定の部位で脈波を計測し，一定の時間経過後も同じ部位で脈波を計測した場合，多くの実験参加者において，脈波間の相関係数 CORR について，$|\mathrm{CORR}| > 0.8$ となることを示している [125]．また，Mukaka は，2 データ間の相関係数 CORR に対して，$|\mathrm{CORR}| > 0.9$，$0.7 < |\mathrm{CORR}| < 0.9$，$0.5 < |\mathrm{CORR}| < 0.7$，$0.3 < |\mathrm{CORR}| < 0.5$ であれば，同データ間にそれぞれ非常に強い相関，強い相関，中程度の相関，弱い相関が存在すると定めている [92]．したがって，本実験で得られた相関係数に対して，Mukaka が定めた基準を適用すると，手首と基節部で計測された脈波，手首と指先で計測された脈波の間に，いずれも強い相関が存在すると考えられる．したがって，本実験で得られた相関係数から，脈波認証に利用される，手首において計測される脈波と，別の部位において計測される脈波が類似することが示唆された．

5.5.2 特徴量に着目した考察

本実験では，4.1 節で検討した攻撃の実現可能性を検証するため，各部位で計測された脈波から抽出した特徴量間の誤差や，相関を調査した．表 5.6，5.7，5.8，5.9 に示した特徴量間の誤差から，一部の特徴量について，異なる部位で計測された脈波から抽出した特徴量の誤差が小さくなることや，相関係数や相互情報量の値から，同特徴量間の相関の存在を確認できた．

Jindal らが提案した特徴量間の相関例として，図 5.22(a) に手首脈波・指先脈波から抽出した DTW $C_{i,2}$，(b) に手首脈波・指先脈波から抽出した最小値時刻 $C_{i,6}$ の相関を示す．図 5.22(a) の DTW $C_{i,2}$ では，表 5.6 から，$0.3 < |\mathrm{CORR}| < 0.5$ となり，Mukaka らが定めた基準を適用すると，弱い相関の存在を確認できた．図 5.22(b) の最小値時刻 $C_{i,7}$ では，特徴量が 0 となる場合を除けば，特徴量間の線形関係が目視で確認できた．また，表 5.6 から，誤差が 10 %未満となることや，今回の検証対象とした全特徴量の中で相互情報量が最大となることが確認できた．

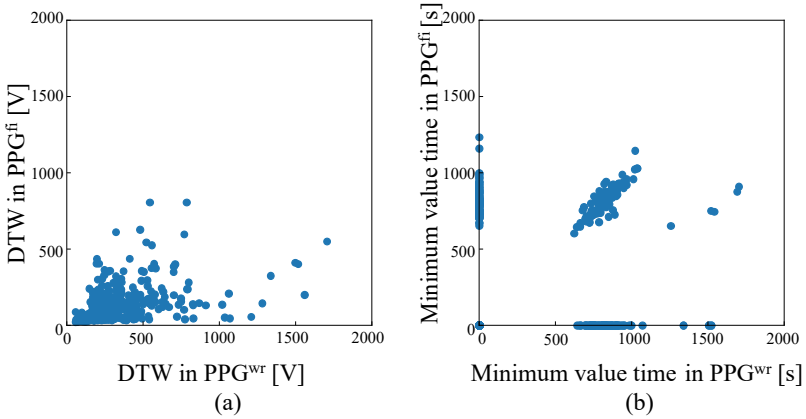


図 5.22: Jindal らが提案する特徴量間の相関例

Gu らが提案した特徴量間の相関例として，図 5.23(a) に手首脈波・指先脈波から抽出した極大値個数 $C_{i,11}$，(b) に手首脈波・指先脈波から抽出した正の傾き $C_{i,12}$ の相関を示す．図 5.23(a) の極大値個数 $C_{i,11}$ では，特徴量が取り得る値の種類が少ないことが確認でき，攻撃者が値を予測することは可能と考えられる．図 5.23(b) の正の傾き $C_{i,12}$ では，表 5.7 から，$0.3 < |\mathrm{CORR}| < 0.5$ となり，Mukaka らが定めた基準を適用すると，弱い相関の存在を確認できた．

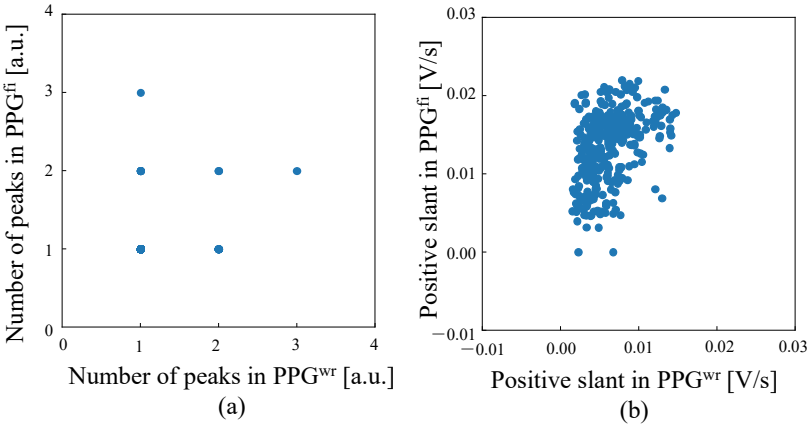


図 5.23: Gu らが提案する特徴量間の相関例

Hartmann らが提案した特徴量間の相関例として，図 5.24(a) に手首脈波・指先脈波から抽出した振幅 $C_{i,39}$，(b) に手首脈波・指先脈波から抽出した重複切痕時刻 $C_{i,41}$ の相関を示す．図 5.24(a) の振幅 $C_{i,39}$ では，指先脈波の値域に対して手首脈波の値域が小さいことが目視で確認でき，表 5.9 から，指先においては最小値時刻 $C_{i,8}$ に次いで相互情報量が大きいことが確認できた．図 5.24(b) の重複切痕時刻 $C_{i,41}$ では，表 5.9 から，$0.3 < |\mathrm{CORR}| < 0.5$ となり，Mukaka らが定めた基準を適用すると，弱い相関の存在を確認できた．

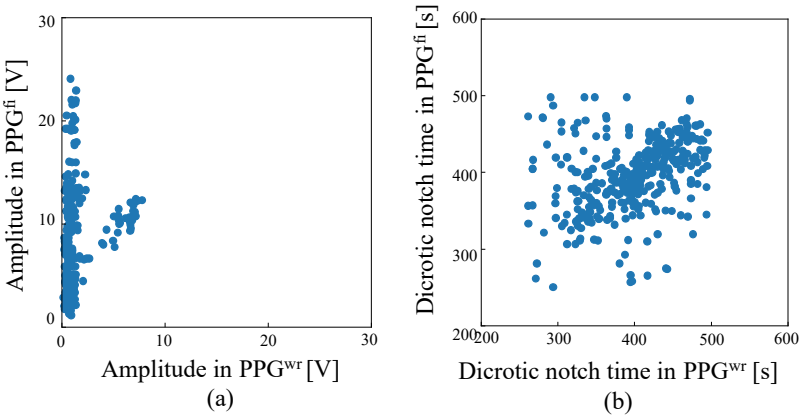


図 5.24: Hartmann らが提案する特徴量間の相関例

以上の検証により，脈波から特徴量を抽出して認証に用いる場合，他部位で脈波を計測されることにより，認証に必要な情報が漏洩する可能性が示唆された．したがって，4.1 節で検討した，正規の計測部位とは異なる部位で計測した脈波を利用して認証を破る攻撃の実現可能性が示唆された．

一方，計測部位間で誤差が大きい特徴量や，相関が確認できない特徴量も存在した．Siam らが提案した特徴量間の相関例として，図 5.25(a) に手首脈波・指先脈波から抽出した MFCC0 $C_{i,15}$，(b) に手首脈波・指先脈波から抽出した MFCC1 $C_{i,16}$ の相関を示す．図 5.25(a) の MFCC0 $C_{i,15}$ および (b) の MFCC1 $C_{i,16}$ では，特徴量間の相関の有無を目視で判断することは困難である．また，表 5.8 に示した通り，全ての特徴量について $|\mathrm{CORR}| < 0.3$ となり，さらに相互情報量が 0.000 となる特徴量も散見されるため，各評価指標からも特徴量間の関係を判断することは困難である．したがって，このような特徴量を手首脈波から抽出して認証に用いる場合は，他部位で不正に脈波計測が行われた場合でも，認証に必要な情報は漏洩していないと考えられる．このような特徴量を認証アルゴリズムに利用することで，4.1 節で検討した攻撃の成功率を低減できる可能性がある．

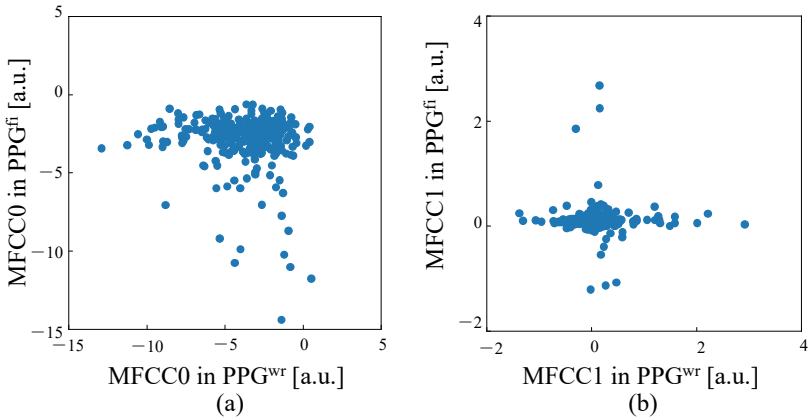


図 5.25: Siam らが提案する特徴量間の相関例

5.6 特徴量の評価結果の考察

5.6.1 各特徴量の PI の比較

本実験では，認証および攻撃における特徴量の寄与を評価するため，各特徴量について PI を算出し，その大小を比較した．表 5.10 に示す通り，一部の特徴量について，MAPE が小さく，|CORR| と MI が大きいものは PI 順位が高くなる傾向が確認できた．例えば，表 5.6 および図 5.22 において，各部位間で相関の存在を示した DTW は，多くの識別器において，認証および攻撃ともに，PI 順位が 10 位以内となった．一方，メル周波数ケプストラム係数は，表 5.8 および図 5.25 において示した通り，情報漏洩の可能性は低かったが，PI を算出した結果，認証および攻撃の両方において PI 順位は低い傾向があった．

手首脈波および指先から同じ特徴量 m を $C^{\mathrm{wr}}_{i,m}, C^{\mathrm{fi}}_{i,m}$ として抽出した場合，両者の値が近く，$C^{\mathrm{wr}}_{i,m} \simeq C^{\mathrm{fi}}_{i,m}$ のように表される場合と，ある関数 FUNC を用いて $C^{\mathrm{wr}}_{i,m} \simeq \mathrm{FUNC}(C^{\mathrm{fi}}_{i,m})$ のように表される関係となる場合があり，PI 順位に影響を与えた可能性がある．前者の例として，図 5.24(a) および表 5.9 に示した重複切痕時刻 $C_{i,41}$ のように，特徴量間の誤差は小さく，表 5.10 に示した通り，各識別器を使用した場合において PI 順位が高くなる場合があった．一方，後者の例として，図 5.24(b) および表 5.9 に示した，係数 γ $(\neq 1)$ を用いて $C^{\mathrm{wr}}_{i,39} \simeq \gamma C^{\mathrm{fi}}_{i,39}$ が成立する可能性がある振幅 $C_{i,39}$ が挙げられる．振幅 $C_{i,39}$ は，相関係数や相互情報量が良好な結果である比較的大きな値を示したが，誤差が大きいために，表 5.10 に示した通り，各識別器を使用した場合において PI 順位が低くなったと考えられる．しかし，この場合でも，4.1.4 節で検討した波形変形により，指先脈波および伝達関数を用いて手首脈波を推定することが有効となる可能性がある．

表 5.10 に示した通り，同一の特徴量についても，使用する識別器を変更した場合，PI 順位は異なり，特に RF と kNN を使用した場合は，他の識別器を使用した場合とは PI 順位が大きく異なる場合があった．例えば，最小値時刻 $C_{i,6}$ は，識別器として RF を使用した場合，認証および攻撃において PI 順位が高くなったが，他の識別器を使用した場合，PI 順位が低くなった．また，極大値個数 $C_{i,11}$ は，識別器として kNN を使用した場合，認証および攻撃において PI 順位が高くなったが，他の識別器を使用した場合，PI 順位が低くなった．図 5.22(b) に示した通り，最小値時刻 $C_{i,6}$ のように，特徴量の取り得る値の分布が 0 と 0 以外の値で二極化するような場合，SVM 等において算出する特徴量間の距離が適切に定

まらず，識別に寄与し難かった可能性がある．一方，RF は取り扱う値の分布を問わず使用可能であることや [126]，複数の決定木での識別結果を集計して最終的な識別結果を得ることから，特徴量の取り得る値の分布が二極化するような場合でも，同特徴量が識別に寄与し得ることが，PI 順位が高くなったことの一因と考えられる．また，他の識別器と比較して，kNN による識別結果は，入力における雑音や外れ値の寄与が大きいことが知られているが [127, 128]，図 5.23(a) に示した通り，極大値個数 $C_{i,11}$ のように，特徴量の取り得る値の種類が非常に少ない場合，雑音や外れ値に該当する値が存在しないと考えられる．さらに，図 5.18 に概要を示した kNN において，入力となる特徴量の値と一致する値が多くなり得ることも，同特徴量の PI 順位に寄与したと考えられる．以上の結果から，使用した特徴量に基づいて，識別器を適切に選定することが重要である．

5.6.2 特徴量の組合せによる EER および SAR の変化

本実験では，各特徴量の PI を基に，特徴量の組合せを変更して，認証精度 EER および攻撃成功率 SAR の値を比較した．表 5.11 に示す通り，特徴量および識別器の全組合せにおいて，SAR > EER となった．また，全ての SAR は，参加者 12 名中 1 名を無作為に選択する確率 $(1/12 = 0.083)$ よりも高かった．したがって，既存の脈波認証において使用されており，情報漏洩が起きている可能性がある特徴量を利用して，攻撃が成功する可能性が示唆された．

一方，PI を基に，認証時に使用する特徴量の組合せを変更することで，EER や SAR が変化することと，EER の変化よりも，SAR の変化が大きいことが確認できた．また，表 5.11 において，使用する特徴量数が同一の 20 個である ii) と iv) を比較すると，攻撃における PI の大きな特徴量の使用による，SAR への寄与が確認でき，MLP，SVM，RF，kNN において，それぞれ SAR が 52.4 %, 38.6 %, 62.8 %, 35.8 %減少したことが確認できた．iv) においても SAR > EER となっており，依然として攻撃が成功する可能性はあるが，情報漏洩が起きていても，認証に使用する特徴量の組合せを適切に設定することで，SAR を低減できる可能性が示唆された．

5.7 本実験の制限

本実験では，実験参加者の複数部位で計測した脈波から特徴量を抽出し，情報漏洩の検証や，特徴量の評価を行った．その結果，各部位で計測される脈波および特徴量間の相関や，認証や攻撃の精度に寄与する特徴量が示された．しかし，攻撃者が，計測した脈波に手を加えずに，なりすまし攻撃に利用するとは限らない．市販の心電図認証デバイスに対するなりすまし攻撃では，他部位で計測した心電図を変形した場合は，変形しない場合よりも高い確率で攻撃に成功することが示されている [31]．また，5.6.1 節で述べた通り，脈波の波形を変形することで，手首脈波の特徴量の値を $C_{i,m}^{\mathrm{wr}} \simeq \mathrm{FUNC}(C_{i,m}^{\mathrm{fi}})$ のように求めることができれば，攻撃に寄与する可能性がある．したがって，脈波認証に関しても，高度な攻撃者を想定して，4.1.4 節で検討した脈波の変形方法に基づいて，他部位で計測した脈波を変形して求めた手首脈波を利用することで，実際に攻撃が成立するか否かに関しても検証する必要がある．

5.8 まとめ

本章では，4.1 節で検討したなりすまし攻撃の実現可能性の検証のため実施した実験について説明した．実験のため実装した脈波計測装置や，使用した特徴量，識別器について述べた．同装置を利用して，12 名の実験参加者の複数部位で脈波を計測し，各部位で計測した脈波間の波形の相関や，抽出した特徴量の誤差や相関の調査結果から，脈波認証において必要となる，手首において計測される情報が，別の部位からも計測される可能性が示唆された．また，各特徴量について，認証および攻撃時の重要度を算出し，認証時に使用する特徴量の組合せを変更することで，攻撃成功率を低減できることが確認できた．一方，5.7 節では，高度な攻撃者を想定して，脈波の変形を含む攻撃についても検証する必要性について述べた．6 章では，既存手法を基に脈波認証システムを試作して，脈波の変形を含む攻撃の実現可能性を検証する．

第6章
なりすまし攻撃の検証

本章では，5 章で示した，脈波認証における情報漏洩を前提として，なりすまし攻撃の実現可能性を検証する．本実験では，既存手法を基に試作した脈波認証システムを攻撃対象とし，5.7 節で言及した高度な攻撃者を想定して，脈波の変形により，攻撃成功率を高める可能性も考慮する．以下では，攻撃の実現可能性の検証のために行った実験の手順や結果，考察を述べる．

6.1 攻撃対象の脈波認証システム

本実験では，脈波認証へのなりすまし攻撃を検証するため，既存手法を基に脈波認証システムを試作した．同システムは，5 章で説明した脈波計測装置と，既存の認証アルゴリズムで構成される．認証アルゴリズムは，生体認証システムにおける識別器として多用される MLP を，脈波認証に対して初めて適用した手法であり，他の脈波認証手法の基ともなっている [94, 129]，Jindal らが提案する手法 [57] を基に実装した．同アルゴリズムは，5.2.3 節で述べた Jindal らが提案する 11 個の特徴量 $C_{i,0}$, ..., $C_{i,10}$ の抽出と，5.2.5 節の情報漏洩の検証と同一のノード数である，入力層 11，中間層 (40, 40, 10)，出力層 12 により構成される MLP が含まれる．

6.2 攻撃の検証手順

4.1 節で検討した攻撃の実現性を検討するため，5 章で実装した脈波計測装置により，実験参加者から計測した脈波を用いて検証を行った．検証に用いた脈波は，5 章における情報漏洩の検証で使用した脈波と同一であり，実験参加者 12 名 (P0, P1, ..., P11) の図 5.1 に示した指先，基節部，手首の全 3 部位で 30 s 間計測した，全 5 試行 (T0, T1, ..., T4) 分の脈波である．

攻撃を検証する前に，全参加者の 1 試行分の手首脈波に含まれる全セグメントから特徴量を抽出して MLP を生成し，式 (5.67) で正解率を算出して識別性能を確認すると同時に，MLP による受入・拒否に必要な閾値を導出した．本評価では，図 5.19 に示した，認証における特徴量の評価と同様に，5-fold 交差検証に基づいて正解率を算出した．全参加者の 1 試行分の手首脈波に含まれる全セグメントから特徴量を抽出して 1 データとし，全 5 試行のうち 4 試行を学習用データとし，残りの 1 試行をテスト用試行とする処理を繰り返し，全試行が一回ずつテスト用データとして使われるようにした．

続いて，脈波の変形を含まない場合の攻撃の検証を行った．本実験では，各参加者の全 5 試行分の手首脈波に含まれる全セグメントから特徴量を抽出して MLP を生成した．攻撃の検証として，図 4.1 **Step 5** のようにセンサへ信号を入力する代わりに，攻撃者が不正に計測したとみなす指先脈波，基節部脈波から特徴量を抽出し，同 MLP へ入力した際の出力を確認した．前段落で述べた閾値を用いて，所属確率が閾値以上であれば攻撃成功したセグメント，閾値未満であれば攻撃失敗したセグメントとみなした．本評価では，図 5.20 に示した，攻撃における特徴量の評価と同様に，全 5 試行のうち 4 試行の手首脈波をテスト用データとし，残りの 1 試行の基節部脈波または指先脈波から推定した手首脈波を学習用データとする処理を繰り返し，全試行が一回ずつテスト用試行として使われるようにした．

さらに，脈波の変形を含む場合の攻撃の検証を行った．本実験では，被害者とみなす参加者 1 名の指先脈波と，同参加者以外の指先・手首脈波から導出した周波数特性を伝達関数として利用して，式 (4.3)，(4.5) により，被害者の手首脈波を推定した．全参加者の全試行について，被害者を除いた 11 名 $\times$ 5 試行分の周波数特性を伝達関数として利用し，同周波数特性の参加者間での有効性の評価として，推定した手首脈波が，真の手首脈波と同様に周期的に増減するか否かを確

認するため，式 (6.1) により相関係数を算出した．

$$\mathrm{CORR}^{\mathrm{wr}} = \frac{\sum_{n=0}^{N-1}(v^{\mathrm{wr}}[n] - \bar{v}^{\mathrm{wr}})(\hat{v}^{\mathrm{wr}}[n] - \bar{\hat{v}}^{\mathrm{wr}})}{\sqrt{\sum_{n=0}^{N-1}(v^{\mathrm{wr}}[n] - \bar{v}^{\mathrm{wr}})^2}\sqrt{\sum_{n=0}^{N-1}(\hat{v}^{\mathrm{wr}}[n] - \bar{\hat{v}}^{\mathrm{wr}})^2}} \tag{6.1}$$

ただし，$\hat{v}^{\mathrm{wr}}[n]$ は基節部脈波または指先脈波の変形により推定した手首脈波であり，$\bar{\hat{v}}_{\mathrm{wr}}$ は $\hat{v}^{\mathrm{wr}}[n]$ の平均である．

加えて，本手順においても，センサへ信号を入力する代わりに，推定した手首脈波から抽出した特徴量を同 MLP へ入力した際の出力結果から，セグメント毎の攻撃成功および攻撃失敗を確認した．本実験でも，全 5 試行のうち 4 試行の手首脈波をテスト用データとし，残りの 1 試行の基節部脈波または指先脈波から推定した手首脈波を学習用データとする処理を繰り返し，全試行が 1 回ずつテスト用試行として使われるようにした．本実験におけるデータの組合せ例として，試行 T0-T4 の手首脈波を学習用データ，試行 T4 の指先脈波から推定した手首脈波をテスト用データとした場合を図 6.1 に示す．

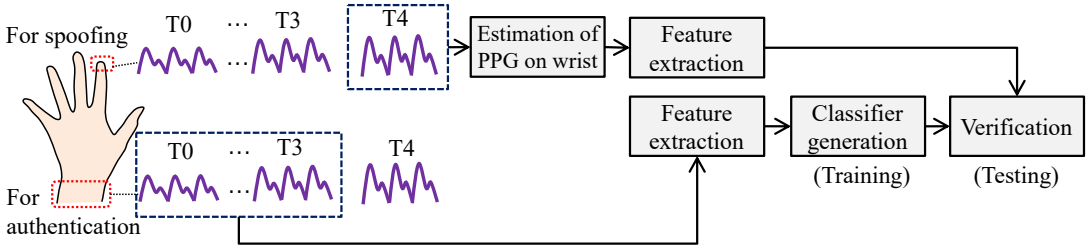


図 6.1: 脈波の変形を含む攻撃の検証におけるデータ組合せ例

また，各条件における攻撃結果を評価するため，試行観点での成功率 SR (Success rate) を式 (6.2) で定義した．さらに，FRR と FAR，EER と比較するため，式 (5.65) で定義した SAR も使用した．ただし，T_{suc} は全試行数 T_{all} のうち 1 セグメント以上攻撃成功した試行数である．

$$\mathrm{SR} = \frac{T_{\mathrm{suc}}}{T_{\mathrm{all}}} \tag{6.2}$$

6.3 攻撃の検証結果

全参加者の 3 部位で計測された各脈波から，本実験において実装した認証アルゴリズムにおいてセグメントを抽出し，各セグメントから 11 個の特徴量を抽出した．4.1 節で検討した攻撃の実現可能性を検証する前に，本実験にて手首脈波から生成する MLP による識別性能を検証した．本手順では，5-fold 交差検証により，全試行が 1 回ずつテスト用データとして使われるようにテストを 5 回繰り返した結果から，正解率 ACC = 0.867 が得られた．また，FRR と FAR，EER の関係から，EER = FAR = FRR = 0.015 が得られた．本実験のうち，試行 T0-T3 のデータを学習用データ，試行 T4 のデータをテスト用データとした場合に得られた FRR と FAR，EER の関係を図 6.2 に示す．

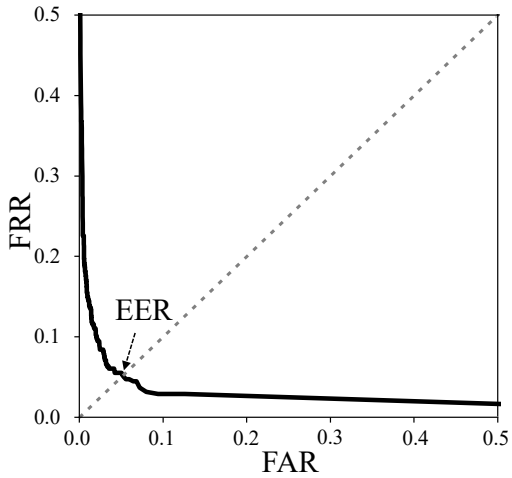


図 6.2: FRR と FAR，EER の関係の例

6.3.1 攻撃結果

4.1 節で検討した攻撃の実現可能性を検証するため，全試行で計測した基節部脈波および指先脈波から特徴量を抽出し，手首脈波から抽出した特徴量より生成した MLP へ入力した結果を表 6.1，6.2 に示す．表 6.1，6.2 には試行毎の攻撃結果を記載しており，○は攻撃成功，× は攻撃失敗，添字は各試行の (攻撃成功したセグメント数/全セグメント数) を表す．表 6.1，6.2 において灰色に着色した部分は，攻撃に失敗した試行である．本条件での攻撃成功率として，式 (6.2) より，

基節部脈波を利用した場合は $T_{\mathrm{all}} = 60$，$T_{\mathrm{suc}} = 49$ より SR $= 0.817$，指先脈波を利用した場合は $T_{\mathrm{all}} = 60$，$T_{\mathrm{suc}} = 51$ より SR $= 0.850$ が得られた．

表 6.1: 基節部脈波による攻撃結果 (攻撃に失敗した試行を灰色に着色)

参加者	試行				
	T0	T1	T2	T3	T4
P0	× (0/40)	× (0/39)	× (0/40)	× (0/39)	× (0/39)
P1	○ (1/38)	× (0/39)	× (0/39)	× (0/39)	× (0/39)
P2	○ (5/30)	○ (5/30)	○ (8/30)	○ (4/30)	○ (6/30)
P3	○ (15/31)	○ (11/31)	○ (22/30)	○ (12/29)	○ (14/29)
P4	○ (2/34)	○ (2/34)	○ (3/34)	○ (3/34)	○ (7/34)
P5	○ (19/34)	× (0/34)	○ (1/34)	○ (4/34)	○ (1/34)
P6	○ (14/32)	○ (21/31)	○ (20/32)	○ (22/32)	○ (25/32)
P7	○ (11/37)	○ (16/37)	○ (23/38)	○ (16/38)	○ (23/37)
P8	○ (5/33)	○ (10/35)	○ (9/35)	○ (8/35)	○ (1/35)
P9	○ (1/35)	○ (3/36)	○ (4/35)	○ (1/36)	× (0/36)
P10	○ (15/36)	○ (14/36)	○ (19/36)	○ (20/36)	○ (16/36)
P11	○ (4/34)	○ (13/33)	○ (3/32)	○ (6/31)	○ (11/32)

表 6.2: 指先脈波による攻撃結果 (攻撃に失敗した試行を灰色に着色)

参加者	試行				
	T0	T1	T2	T3	T4
P0	× (0/37)	○ (3/37)	○ (3/38)	○ (1/37)	× (0/37)
P1	× (0/39)	× (0/40)	× (0/40)	○ (2/40)	× (0/39)
P2	○ (4/30)	○ (7/30)	○ (6/30)	○ (7/30)	○ (8/30)
P3	○ (11/33)	○ (11/33)	○ (15/33)	○ (12/33)	○ (13/33)
P4	○ (1/26)	○ (3/28)	○ (2/29)	○ (2/30)	○ (3/30)
P5	○ (13/33)	○ (4/34)	× (0/34)	○ (7/34)	× (0/34)
P6	○ (16/31)	○ (16/32)	○ (15/32)	○ (9/32)	○ (13/32)
P7	○ (17/37)	○ (17/36)	○ (19/37)	○ (20/37)	○ (20/36)
P8	○ (6/34)	○ (8/34)	○ (20/34)	○ (11/34)	○ (21/33)
P9	○ (1/30)	○ (4/30)	○ (1/29)	○ (1/30)	× (0/29)
P10	○ (23/36)	○ (24/36)	○ (16/36)	○ (19/36)	○ (13/36)
P11	○ (2/37)	○ (1/37)	× (0/35)	○ (4/34)	○ (4/34)

続いて，高度な攻撃者を想定し，提案手法により基節部脈波および指先脈波を変形して手首脈波を推定した．式 (6.1) により算出した，真の手首脈波と，基節部脈波から推定した手首脈波の相関係数を図 6.3 に示す．また，真の手首脈波と，指先脈波から推定した手首脈波の相関係数を図 6.4 に示す．図 6.3，6.4 中の矩形は，同一の参加者の試行 T0-T4 による，真の手首脈波と，推定した手首脈波による相関係数を表す．矩形内に含まれない，異なる参加者の脈波を使用した場合，図 6.3 において最も相関係数が大きな値となった組合せは，参加者 P7 試行 T3 の手首脈波と基節部脈波から導出した周波数特性により，参加者 P5 試行 T4 の手首脈波を推定した場合 ($\mathrm{CORR}^{\mathrm{wr}} = 0.867$) であった．同様に，図 6.4 において最も相関係数が大きな値となった組合せは，参加者 P10 試行 T1 の手首脈波と指先脈波から導出した周波数特性により，参加者 P5 試行 T4 の手首脈波を推定した場合 ($\mathrm{CORR}^{\mathrm{wr}} = 0.812$) であった．

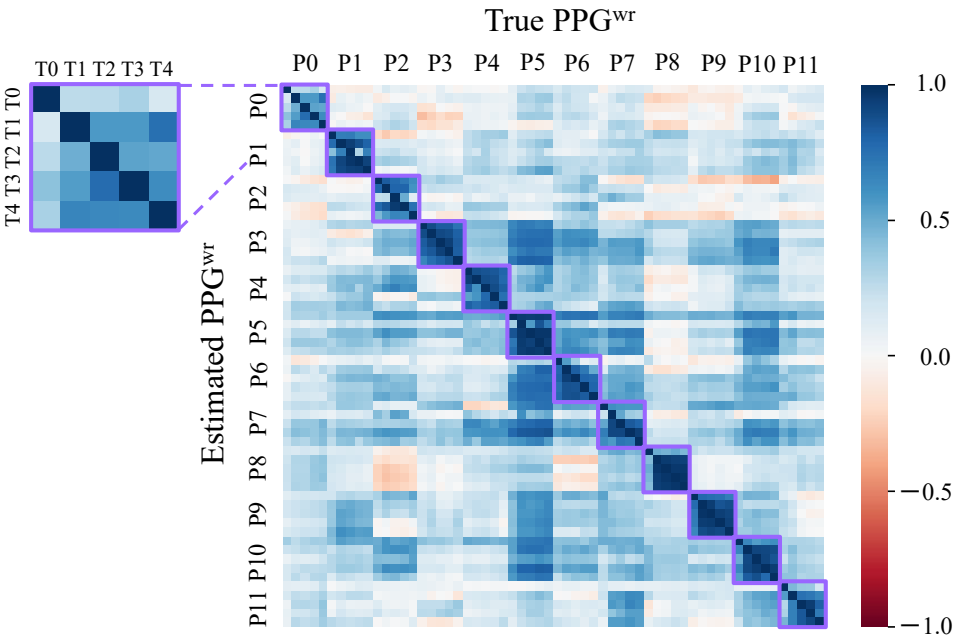


図 6.3: 真の手首脈波と，基節部脈波から推定した手首脈波の相関係数

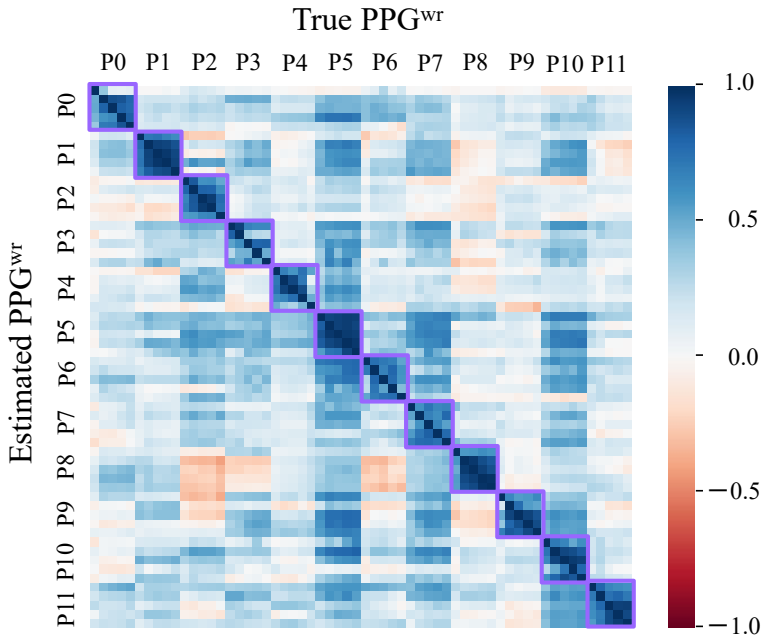


図 6.4: 真の手首脈波と，指先脈波から推定した指先脈波の相関係数

推定した脈波の例を図 6.5，6.6 に示す．ただし，真の手首脈波と，推定した手首脈波の値の増減を比較するため，値域が $[0, 1]$ となるように各信号を正規化した．図 6.5(a) は，参加者 P7 試行 T3 の基節部脈波から導出した周波数特性により，参加者 P5 試行 T4 の手首脈波を推定した例である．図 6.5(b) は，参加者 P7 試行 T3 の基節部脈波から導出した周波数特性により，参加者 P8 試行 T1 の手首脈波を推定した例である．図 6.6(a) は，参加者 P10 試行 T1 の指先脈波から導出した周波数特性により，参加者 P5 試行 T4 の手首脈波を推定した例である．図 6.6(b) は，参加者 P10 試行 T1 の指先脈波から導出した周波数特性により，参加者 P0 試行 T1 の手首脈波を推定した例である．図 6.5(a)，6.6(a) は比較的高精度，図 6.5(b)，6.6(b) は低精度な推定結果である．

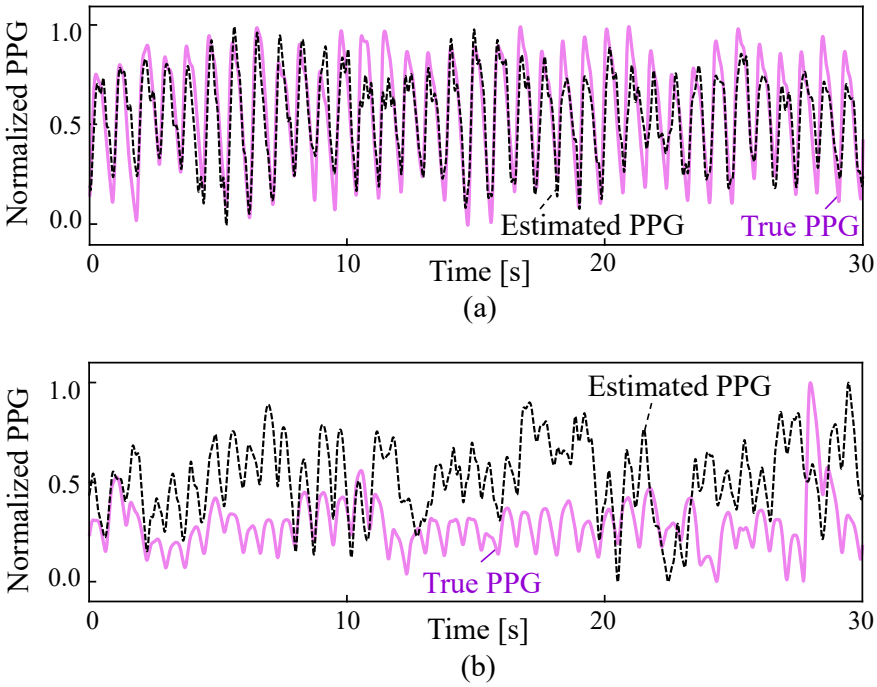


図 6.5: 基節部脈波から手首脈波を推定した例．(a) 高精度の推定例，(b) 低精度の推定例

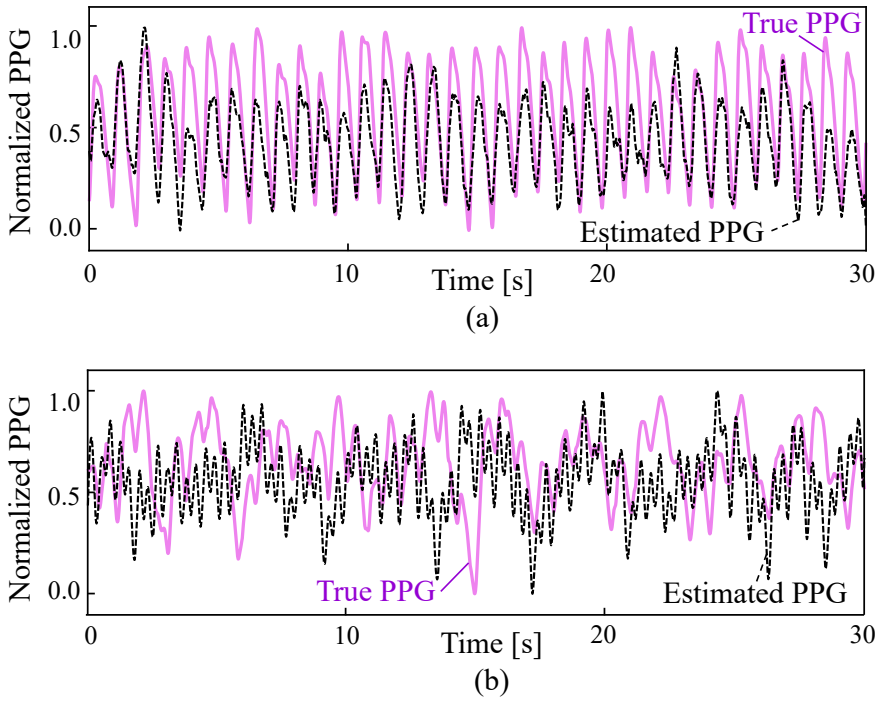


図 6.6: 指先脈波から手首脈波を推定した例．(a) 高精度の推定例，(b) 低精度の推定例

変形を含む攻撃の検証のため，推定した手首脈波から特徴量を抽出し，MLP へ入力した結果を表 6.3，6.4 に示す．ただし，試行と周波数特性の全組合せのうち，表 6.3 は，参加者 P10 試行 T1 で計測された基節部脈波および手首脈波から導出した周波数特性を適用した結果であり，表 6.4 は，参加者 P7 試行 T3 で計測された指先脈波および手首脈波から導出した周波数特性を適用した結果である．表 6.1，6.2 と同様に，〇は攻撃成功，添字は各試行の (攻撃成功したセグメント数/全セグメント数) を表す．灰色に着色した部分は，変形なしの条件と同様に攻撃に失敗した試行であり，赤色に着色した部分は，変形なしの条件では攻撃に失敗したが，変形ありの条件では攻撃に成功した試行である．また，周波数特性導出に使われた参加者 P7 の指先脈波には，同周波数特性を適用していないため，P7 の行には “−” を記載した．本条件での試行毎の攻撃成功率として，式 (6.2) より，基節部脈波を利用した場合は $T_{\mathrm{all}} = 55$，$T_{\mathrm{suc}} = 47$ より $\mathrm{SR} = 0.855$，指先脈波を利用した場合は $T_{\mathrm{all}} = 55$，$T_{\mathrm{suc}} = 50$ より $\mathrm{SR} = 0.873$ が得られた．さらに，同手法による脈波の変形なし・変形ありの両条件において，参加者毎に式 (5.65) より SAR を算出した結果を表 6.5，6.6 に示す．ただし，変形ありの条件では，試行と

周波数特性の全組合せで変形を行い，各組合せで得た攻撃成功セグメント数，全セグメントの総数より SAR を算出した．

表 6.3: 基節部脈波から推定した手首脈波による攻撃結果 (変形なしでは攻撃に失敗した試行を灰色，変形なしでは攻撃に失敗し，変形ありでは攻撃に成功した試行を赤色に着色)

参加者	試行				
	T0	T1	T2	T3	T4
P0	○ (1/32)	○ (2/93)	× (0/41)	○ (2/36)	× (0/40)
P1	○ (1/34)	○ (2/39)	○ (2/40)	○ (1/38)	× (0/38)
P2	○ (4/28)	○ (5/28)	○ (5/29)	○ (8/29)	○ (7/29)
P3	○ (5/24)	○ (11/24)	○ (3/31)	○ (7/21)	○ (3/23)
P4	× (0/33)	× (0/34)	× (0/34)	× (0/34)	○ (2/34)
P5	× (0/35)	○ (4/34)	○ (6/34)	○ (4/34)	○ (4/35)
P6	○ (7/30)	○ (5/30)	○ (13/31)	○ (10/31)	○ (10/28)
P7	–	–	–	–	–
P8	○ (2/26)	○ (3/34)	○ (3/35)	○ (2/35)	○ (5/33)
P9	○ (5/32)	○ (4/32)	○ (2/34)	○ (6/32)	○ (6/33)
P10	○ (6/28)	○ (2/34)	○ (10/33)	○ (9/34)	○ (5/33)
P11	○ (14/29)	○ (8/28)	○ (12/31)	○ (11/31)	○ (10/30)

表 6.4: 指先脈波から推定した手首脈波による攻撃結果 (変形なしでは攻撃に失敗した試行を灰色，変形なしでは攻撃に失敗し，変形ありでは攻撃に成功した試行を赤色に着色)

参加者	試行				
	T0	T1	T2	T3	T4
P0	○ (6/16)	○ (4/22)	○ (6/19)	× (0/23)	○ (5/24)
P1	○ (2/17)	○ (3/27)	○ (3/27)	○ (4/28)	○ (8/27)
P2	○ (1/29)	○ (4/24)	○ (4/26)	○ (2/28)	○ (5/28)
P3	○ (2/29)	○ (8/30)	○ (9/31)	○ (3/30)	○ (6/29)
P4	○ (4/25)	○ (1/22)	○ (3/27)	○ (4/27)	○ (1/29)
P5	○ (3/32)	○ (4/34)	○ (2/35)	○ (8/34)	○ (12/34)
P6	× (0/28)	○ (4/28)	○ (1/28)	○ (3/29)	○ (4/26)
P7	○ (7/35)	○ (5/34)	○ (9/34)	○ (7/33)	○ (6/36)
P8	× (0/16)	○ (1/17)	○ (1/13)	○ (1/13)	○ (2/15)
P9	○ (1/16)	○ (1/14)	○ (1/16)	× (0/14)	× (0/17)
P10	–	–	–	–	–
P11	○ (3/16)	○ (1/19)	× (0/16)	× (0/15)	× (0/15)

表 6.5: 基節部脈波に対する変形の有無による SAR の比較

参加者	変形なし	変形あり
P0	0.000	0.028
P1	0.005	0.031
P2	0.187	0.202
P3	0.494	0.245
P4	0.100	0.012
P5	0.147	0.105
P6	0.642	0.300
P7	0.476	0.230
P8	0.190	0.092
P9	0.051	0.142
P10	0.467	0.198
P11	0.166	0.369
平均 ± 標準偏差	0.244 ± 0.208	0.163 ± 0.109

表 6.6: 指先脈波に対する変形の有無による SAR の比較

参加者	変形なし	変形あり
P0	0.037	0.216
P1	0.010	0.156
P2	0.213	0.121
P3	0.376	0.187
P4	0.070	0.100
P5	0.125	0.171
P6	0.434	0.087
P7	0.508	0.198
P8	0.392	0.069
P9	0.047	0.039
P10	0.528	0.394
P11	0.063	0.048
平均 ± 標準偏差	0.234 ± 0.191	0.149 ± 0.093

6.4 攻撃結果の考察

表 6.1，6.2 に示した脈波を変形しない場合の結果から，4.1 節で検討した攻撃が成立する可能性が示唆された．さらに，表 6.1，6.2 に示した通り，参加者全体での平均の SAR は，攻撃を検証する前に算出した EER = FAR = FRR = 0.015 より高かったため，他人を本人として受け入れてしまう場合よりも高い確率で，提案する攻撃が成立する可能性が示唆された．しかし，参加者間で結果には差があり，特に参加者 P0，P1 は試行毎の攻撃成功数および攻撃に成功したセグメント数も少なかった．攻撃に失敗した理由の一つとして，脈波からのセグメント抽出の失敗が挙げられる．表 5.5 に示した通り，同じ試行でも各部位で計測された脈波から抽出したセグメント数は必ずしも一致しない．また，図 5.21 に示した通り，各部位で計測される脈波の振幅の大きさは異なり，特に手首脈波の振幅は小さい傾向があるため [81]，極大値・極小値を正しく抽出できなかった可能性も考えられる．

図 6.3，6.4 に示した通り，真の手首脈波と，基節部脈波または指先脈波から推定した手首脈波の相関係数は，正の値となる場合が多く，特に同参加者間では強い相関を有する傾向が確認できた．加えて，他参加者間でも強い相関を有する組合せも存在したため，脈波を変形して他部位の脈波を推定できる可能性が示唆された．しかし，実際に基節部脈波および指先脈波を変形して手首脈波を推定した場合，推定精度には差が生じた．図 6.5(a)，6.6(a) は真の手首脈波と同程度の周期での増減が確認できるが，図 6.6(b) は高周波雑音の寄与が大きく，周期を確認することが困難である．しかし，脈波変形の有無による攻撃結果として，表 6.1 と表 6.3，表 6.2 と表 6.4 を比較すると，変形なしの条件で攻撃失敗した参加者・試行について，変形ありの条件では攻撃成功した場合があった．ただし，変形後に攻撃成功したセグメント数が減少した試行が多かった．表 6.5，6.6 に示した通り，全参加者の SAR の平均は，12 名中 1 名を無作為に選択する確率 (1/12 = 0.083) より高いが，参加者毎の SAR は変形なしの方が高く，一部参加者の SAR は 0.083 を下回った．脈波に対する変形なし・変形ありの条件による攻撃結果である，表 6.1 と表 6.3，表 6.2 と表 6.4 の各組合せにおける全セグメント数の変化から，本結果にもセグメント抽出の失敗が寄与した可能性がある．図 6.6(b) のように高周波雑音の寄与が大きい場合は，適切なセグメント抽出が困難と考えられる．

前段落で述べた通り，手首脈波の推定のため，伝達関数を用いて基節部脈波または指先脈波を変形した場合，推定精度には差が生じた．4.1.4 節では，計測対象者間での脈波の波形の傾向，さらに脈波間に線形時不変システムが存在することを仮定して伝達関数を導出した．しかし，実際には脈波の波形における個人差や，時間変化の影響を無視できず，同仮定が成立しない場合があったことが，推定精度の差に寄与したと考えられる．そのため，波形における高周波雑音の寄与や，1 試行における攻撃成功したセグメント数の減少，さらに SAR の低下が生じたと考えられる．一方，図 6.3，6.4 に示した通り，真の手首脈波と，基節部脈波または指先脈波から推定した手首脈波の相関係数は，正の値となる場合が多く，他参加者間でも強い相関を有する組合せも存在した．したがって，手首脈波を推定するためには，個人に対して適切な伝達関数を選定することが重要であると考えられる．

本実験では，同じ仕様のセンサ 3 個を手指に固定し，着座した状態で脈波を計測した．したがって，比較的安定して計測可能であり，攻撃者には理想的な条件下で計測した脈波を利用して，提案する攻撃の検証を行った．図 4.1 のように攻撃者が脈波を計測する際は，スマートウォッチと同仕様のセンサを使用できるとは限らない．また，センサを手指に固定せずマウス等に埋め込んだ場合や，参加者が作業をしている状態では，安定した計測が難しいと考えられる．今後は，他の条件下での検証も求められる．

6.5 まとめ

本章では，5 章で述べた，脈波認証における情報漏洩を前提として，脈波認証へのなりすまし攻撃の実現可能性を検証した．本実験は，既存手法を基に試作した脈波認証システムを攻撃対象とし，5.7 節で言及した高度な攻撃者を想定して，脈波の変形により，攻撃成功率を高める可能性も考慮した．本実験の結果，理想的な条件下において，基節部脈波を利用した場合，指先脈波を利用した場合の攻撃成功率はいずれも 0.800 以上となり，攻撃の実現可能性が示唆された．また，脈波を変形する攻撃についても検証した結果，個人に適切な伝達関数を選定することで，変形しない場合では攻撃失敗した試行について，攻撃成功することが示唆された．7 章では，5 章および本章において検証したなりすまし攻撃への対策の評価のため実施した，脈波のデータセットを利用した実験について説明する．

第7章

なりすまし攻撃への対策の検証

本章では，5，6 章で検証した，脈波認証システムへのなりすまし攻撃に対する，4.2 節で提案した対策の有効性を検証する．提案する対策に含まれる計測部位の識別の検証手順や，同手順において使用するデータセット，脈波から抽出する特徴量や識別器について説明し，検証結果，考察を述べる．

7.1　対策の検証手順

提案する対策の有効性を検討するため，5 章で実装した脈波計測装置により，実験参加者から計測した脈波を用いて検証を行った．本手順は，図 7.1 に示すように，波形の評価，対策の評価に分かれる．まず，波形の評価として，複数部位で計測された脈波の類似性から，攻撃が成立する可能性を確認する．同時に，被害者の手首脈波を推定するために変形した脈波について，真の手首脈波との類似性を確認する．続いて，対策の評価として，提案する対策の評価のため，各脈波から特徴量を抽出し，部位が識別可能か確認する．同時に，特徴量の部位識別への寄与を確認し，同識別に有効な特徴量を確認する．最後に，提案する対策である部位識別における，時間経過の影響を確認する．

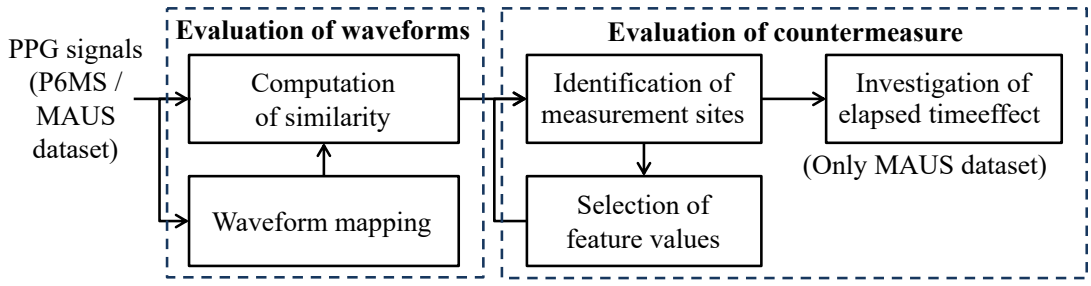


図 7.1: 対策の検証手順

7.1.1 対策の検証に用いたデータセット

提案する対策は，身体上の異なる部位で計測した脈波の差を利用し，脈波の計測部位を識別することで，脈はセンサへの入力の正当性を検証し，なりすまし攻撃を検出する．したがって，本実験では，実験参加者の身体上の複数部位で同時に計測した脈波が含まれる，2 種類のデータセットを利用した．いずれのデータセットも，手首脈波に加え，手首以外の部位で計測された脈波を含む．一方のデータセットは，6.4 節で課題として挙げた，攻撃者にとっては理想的ではない条件で計測された脈波も含む．

P6MS データセット

本実験のため，5 章における情報漏洩の検証，6 章におけるなりすまし攻撃の検証において使用した脈波計測システムを用いて脈波を計測した．本計測は，男性 11 名，女性 1 名，計 12 名の参加者 (P0，P1，…，P11) を対象とした．参加者の年齢の平均および標準偏差は，27.3 ± 1.8 歳であった．図 7.2 に示した全 6 部位で，180 s 間の計測を 1 回行った．なお，以下では，本脈波のデータセットを，P6MS (PPG on 6 measurement sites) データセットと記載する．また，左手の人差し指の基節部を左基節部，左手の人差し指の指先を左指先，右手の人差し指の基節部を右基節部，右手の人差し指の指先を右指先と記載する．

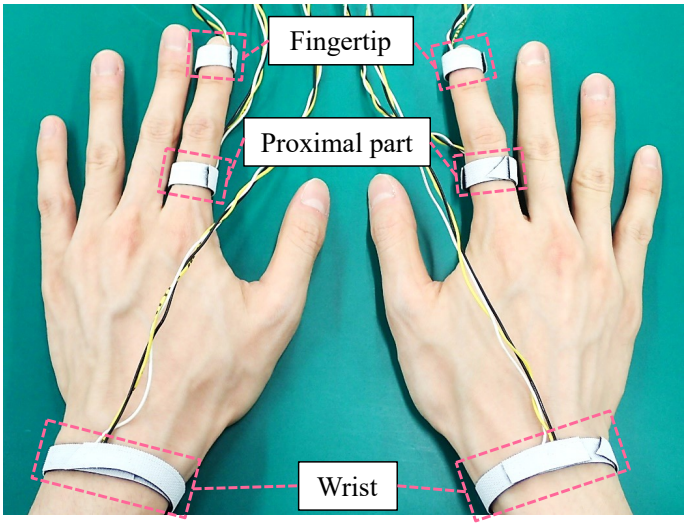


図 7.2: P6MS データセットにおける計測部位

MAUS データセット

P6MS データセットに加えて，MAUS (Mental workload assessment on n-back task using wearable sensor) データセット [130, 131] を使用した．MAUS データセットは，実験参加者の複数部位で計測した脈波が含まれている唯一の公開データセットであり，計測部位は指先と手首の計 2 箇所である．参加者は，男性 20 名，女性 2 名の計 22 名 (P12，P13，…，P33) であり，年齢の平均および標準偏差は 23.0 ± 1.7 歳である．MAUS データセットに含まれる指先脈波は，赤外光の LED を含む脈波センサで計測された [132]．用いられた AD 変換器 (ProComp Infiniti) の標本化周波数は 256 Hz，量子化数は 14 bit，計測できる電圧の範囲は 1.104 V から 4.496 V であるため [133]，最大量子化誤差 $(4.496 - 1.104)/2^{14} = 0.207$ mV である．一方，MAUS データセットに含まれる手首脈波は，緑色光の LED を含む脈波センサを有するスマートウォッチ (PixArt PPG Watch) を用いて，標本化周波数 100 Hz にて計測された [131, 134]．

MAUS データセットには，安静時に 300 s 間計測した脈波に加えて，ストレス負荷を計測するための実験である，N バック課題の実施中に計測した脈波が含まれている．N (Number) は同課題において，実験参加者に指定される数を表す．参加者に対して数字を連続的に提示し，参加者は，その数字が，指定された数 N だけ前の数字と一致した際に，手元のボタンを押す [131]．本データセットは，参加者に作業を課していることから，P6MS データセットと比較して安定した計測は行えない，攻撃者にとって理想的な条件ではないと考えられる．N バック課題は，300 s 間，6 試行 (T'0, T'1, ..., T'5) に渡って，120 s の休憩を挟んで実施されており，実験に要した合計時間は 2,820 s となる．

本実験では，2 種類のデータセットを比較するため，特徴量を抽出する前に，MAUS データセット中の各脈波に対して線形補完を施すことで，標本化周波数を P6MS データセットと同様の 1 kHz とした．また，MAUS データセットの各脈波は，単位が不明であるため，各脈波の i 番目のセグメント $v_i[n]$ に対して，式 (7.1) で表される正規化を施した $v_{i,\mathrm{norm}}[n]$ を得た．

$$v_{i,\mathrm{norm}}[n] = \frac{v_i[n] - \min\limits_{n\in[0,N_i]} v_i[n]}{\max\limits_{n\in[0,N_i]} v_i[n] - \min\limits_{n\in[0,N_i]} v_i[n]} \tag{7.1}$$

なお，本処理に伴い，各セグメントから特徴量として，最大値，最小値を抽出する場合，その値はそれぞれ 1，0 となる．したがって，対策の検証においては，5.2.3

節に示した全 43 個の特徴量 $C_{i,0}$, ..., $C_{i,42}$ のうち，最大値および最小値に関係する，最大値 $C_{i,3}$，最小値 $C_{i,4}$，振幅 $C_{i,39}$ の 3 個を対象外とした，40 個の特徴量を使用した.

本実験で使用した 2 種類のデータセットの比較を表 7.1 に示す.

表 7.1: P6MS データセットと MAUS データセットの比較

データセット	参加者数	年齢	計測状態 (時間)	計測部位	標本化周波数	LED 色 (波長)
P6MS	12 (男性 11 名, 女性 1 名)	27.3±1.8	安静 (180 s)	指先, 基節部, 手首 (左・右)	1 kHz	緑 (570 nm)
MAUS	22 (男性 20 名, 女性 2 名)	23.0±1.7	安静 (300 s), N バック課題 (300 s)	指先 (非利き手)	256 Hz	赤外 (N.A.)
				手首 (非利き腕)	100 Hz	緑 (N.A.)

7.1.2 波形の評価

本実験では，提案する対策を評価する前に，データセットに含まれる脈波，さらに脈波を変形した脈波の波形について，評価を行った．以下では，同評価の指標や，変形の方法について述べる．

脈波の類似性の確認

提案する対策の有効性を検証する前に，複数部位で計測された脈波の類似性を確認し，攻撃が成立する可能性を確認する．類似性の指標として，生体信号間の類似性の指標として最も頑強であり [135]，脈波認証における評価指標としても使用される [125]，相関係数を使用した．式 (5.2)，(5.3) で表した相関係数と同様に，手首脈波，基節部脈波，指先脈波間の相関係数を算出した．

脈波の変形

7.1.2 節においては，攻撃の向上のため変形した脈波についても，真の手首脈波との類似性を確認する．本節では，対策の検証において実施する脈波の変形方法について説明する．本変形は，4.1.4 節で述べた変形方法と同様に，脈波の周波数特性を利用する．認証に使用される手首脈波と，手首以外の部位で計測された脈波間の伝達関数を，DCT を利用して導出し，手首脈波の推定に利用する．4.1.4 節で述べた変形方法は，参加者および試行毎に伝達関数が存在し，変形に使用する伝達関数を選定する必要があり，選定次第で手首脈波の推定精度に差が生じたが，本実験では，複数の参加者から一つの伝達関数を生成して変形に使用する．

図 7.3，7.4 に，対策の検証で実施する脈波変形の例として，左指先脈波を変形して左手首脈波を推定するための学習，テストの手順を示す．本変形では，攻撃者は，被害者 p 以外の人物複数名の手首脈波と指先脈波を入手可能と仮定する．また，認証に利用される，被害者 p の手首脈波は入手不可能だが，指先脈波は入手可能と仮定する．図 7.3 に示す通り，攻撃者は，被害者以外の人物 $q\,(\neq p)$ について，指先脈波の DCT 係数 $\boldsymbol{V}^{q,\mathrm{fi}} = (\boldsymbol{V}_0^{q,\mathrm{fi}}\,\boldsymbol{V}_1^{q,\mathrm{fi}}\,...\,\boldsymbol{V}_{I-1}^{q,\mathrm{fi}})$，手首脈波の DCT 係数 $\boldsymbol{V}^{q,\mathrm{wr}} = (\boldsymbol{V}_0^{q,\mathrm{wr}}\,\boldsymbol{V}_1^{q,\mathrm{wr}}\,...\,\boldsymbol{V}_{I-1}^{q,\mathrm{wr}})$ を入手する．ただし，I はセグメント数を表す．続いて，被害者 p 以外の複数名の人物から計測した指先脈波の DCT 係数について，$\boldsymbol{V}^{\mathrm{fi}} = (\boldsymbol{V}^{0,\mathrm{fi}}\,\boldsymbol{V}^{1,\mathrm{fi}}\,...\,\boldsymbol{V}^{Q-1,\mathrm{fi}})$ とする．同様に，手首脈波の DCT 係数について，$\boldsymbol{V}^{\mathrm{wr}} = (\boldsymbol{V}^{0,\mathrm{wr}}\,\boldsymbol{V}^{1,\mathrm{wr}}\,...\,\boldsymbol{V}^{Q-1,\mathrm{wr}})$ とする．ただし，被害者 p の指先脈波の DCT 係

数 $\boldsymbol{V}^{p,\mathrm{fi}}$，手首脈波の DCT 係数 $\boldsymbol{V}^{p,\mathrm{wr}}$ は含まない．Q は実験参加者人数である．そして，伝達関数となる行列 $\boldsymbol{F}^*$ を，式 (7.2) に示す最小二乗法を用いて求める．

$$\boldsymbol{F}^* = \arg\min_{\boldsymbol{F}} ||\boldsymbol{F}\boldsymbol{V}^{\mathrm{fi}} - \boldsymbol{V}^{\mathrm{wr}}||^2 \tag{7.2}$$

図 7.4 に示す通り，攻撃者は，被害者 p の手首脈波の DCT 係数 $\hat{\boldsymbol{V}}^{p,\mathrm{wr}}$ を，式 (7.3) により，被害者 p 以外の脈波から導出した $\boldsymbol{F}^*$ と，被害者 p の指先脈波 $\boldsymbol{V}^{p,\mathrm{fi}}$ を利用して推定する．最後に，$\hat{\boldsymbol{V}}^{p,\mathrm{wr}}$ に逆 DCT を適用して，$\hat{\boldsymbol{v}}^{p,\mathrm{wr}}$ を導出する．

$$\hat{\boldsymbol{V}}^{p,\mathrm{wr}} = \boldsymbol{F}^* \ \boldsymbol{V}^{p,\mathrm{fi}} \tag{7.3}$$

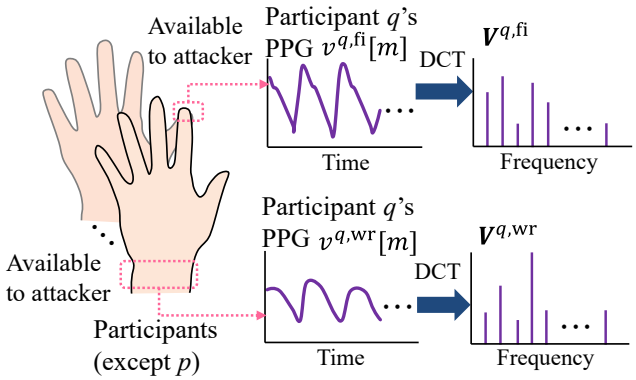


図 7.3: 対策の検証で実施する脈波変形における学習

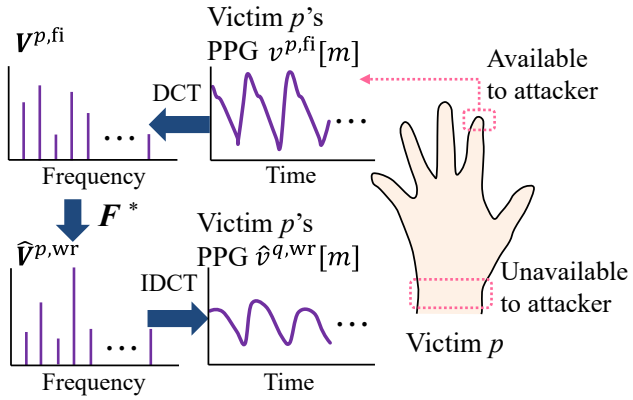


図 7.4: 対策の検証で実施する脈波変形におけるテスト

以上では，左手首脈波を推定するため，左指先脈波を変形する手順を示したが，他の部位の脈波についても，同様の手順で変形を行う．P6MS データセットの場合は，左手首脈波を推定するため，左基節部脈波，左指先脈波，右手首脈波，右基節部脈波，右指先脈波を同様の手順で変形する．MAUS データセットの場合は，手首脈波を推定するため，指先脈波を変形する．

7.1.3 対策の評価

提案する対策の評価では，脈波から抽出した特徴量を用いて部位識別が可能か否か，同対策は時間経過の影響を受けるか否かを検証した．また，各検証では，特徴量を評価することで，その組合せを決定した．

部位識別の検証

図 4.5 に示した通り，提案する対策では，両データセットの脈波から抽出した特徴量を利用して，計測部位を識別する．本実験では，5.2.3 節に示した全 43 個の特徴量 $(C_{i,0}, ..., C_{i,42})$ のうち，最大値および最小値に関係する，最大値 $C_{i,3}$，最小値 $C_{i,4}$，振幅 $C_{i,39}$ の 3 個を対象外とした，40 個の特徴量および PI を利用する．各部位で計測した脈波から抽出した特徴量に差があれば，同特徴量を利用して計測部位を識別することが可能となる．したがって，本実験では，40 個の特徴量には，手首や指先，基節部で計測した脈波間でも差があるものが存在する可能性を仮定し，計測部位の識別による対策に利用する．同特徴量は，5 章で説明した情報漏洩の検証や，6 章で説明した攻撃の検証で抽出した特徴量と同様に，脈波に対する事前処理で得られた各セグメントから抽出する．さらに，5 章の情報漏洩検証で使用した，各特徴量の PI を部位識別においても算出し，対策に有効な特徴量を求める．

図 4.5 に示した通り，前段落で述べた特徴量を識別器に入力し，計測部位を識別することで，なりすまし攻撃への対策とする．識別器は，未学習データに関しても汎化能力の高い識別が可能であり [114]，さらに既存の生体認証手法において，高い識別精度を達成していることから [111]，SVM を使用する．提案する対策では，正当な計測部位と他部位を識別するため，本節では，2 クラス分類 SVM を利用する．

本実験では，スマートウォッチで計測する手首脈波を認証に利用することを想定し，手首と他の部位を識別可能か検証した．また，高度な攻撃者による手首脈波を推定する攻撃への有効性を検証するため，他部位の脈波を変形した場合についても同様の検証を行った．本手順では，交差検証を行い，式 (5.67) により識別成功率を算出した．P6MS データセットを使用した際は，全参加者の脈波 180 s 分に含まれる全セグメントから特徴量を抽出し，学習用・テスト用データを得て，6-fold 交差検証を行った．具体的には，同データを 6 データに分割し，5 データを

学習用データとし，残りの 1 データ 30 s 分をテスト用データとする処理を繰り返し，全データが 1 回ずつテスト用データとなるようにした．MAUS データセットを使用した際は，全参加者の安静時の脈波 300 s 分に含まれる全セグメントから特徴量を抽出し，学習用・テスト用データを得て，10-fold 交差検証を行った．具体的には，同データを 10 データに分割し，9 データを学習用データとし，P6MS データセットと同じ 30 s 分となる残りの 1 データをテスト用データとする処理を繰り返した．

部位識別に使用する特徴量の評価と選定

本実験では，5.2.3 節に示した全 43 個の特徴量について，部位識別における寄与を，式 (5.66) に示した PI を算出して評価した．続いて，PI の大小を比較して，部位識別に使用する特徴量を選定し，その個数を変更した場合の部位識別の精度の変化を確認した．既存の脈波認証に関する研究では，使用する特徴量の適切な個数は 15 個から 24 個と示されている [94, 120, 124]．なりすまし攻撃への対策において，認証のように特徴量数を多く設定することで，正当な入力を攻撃として検出してしまう場合が増えることは望ましくないと考えられる．したがって，本実験では，特徴量数を 1 個から 20 個まで変更した場合の，部位識別の精度の変化を確認した．

部位識別における時間経過の影響の検証

本実験では，部位識別における，時間経過の影響を確認するため，1 試行における脈波の計測時間が 180 s である P6MS データセットより長い，合計 2,820 s の実験時間により計測された MAUS データセットを使用する．本実験における識別は，7.1.3 節で述べた部位識別と同様に，識別器として SVM を使用した．7.1.3 節で行った特徴量の選定において，MAUS データセットのうち，安静時に計測した脈波から抽出した特徴量を評価対象とし，PI が大きい特徴量を選定して本実験に利用した．

7.2 対策の検証結果

本節では，7.1 節で述べた対策の検証によって得られた，データセットに含まれる脈波の評価結果，提案する対策の評価結果について述べる．

7.2.1 波形の評価結果

提案する対策の検証の前に，使用したデータセットに含まれる脈波間の類似性の指標として，相関係数を算出した．P6MS データセットにおける，左手首脈波と他部位脈波の相関係数の比較を表 7.2 に示す．

表 7.2: P6MS データセットにおける左手首と他部位の脈波の相関係数比較

計測部位	相関係数の平均 ± 標準偏差	
	変形なし	変形あり
左指先	0.829 ± 0.100	0.874 ± 0.080
左基節部	0.835 ± 0.111	0.879 ± 0.073
右指先	0.818 ± 0.116	0.862 ± 0.084
右基節部	0.844 ± 0.090	0.863 ± 0.090
右手首	0.845 ± 0.118	0.872 ± 0.089

MAUS データセットにおける，手首脈波と指先脈波の相関係数の比較を表 7.3 に示す．各試行における () 内の数字は，N バック課題において，提示された数字と比較する数字の位置として，参加者に指定した数を表す．

表 7.3: MAUS データセットにおける手首と指先脈波の相関係数比較

試行	相関係数の平均 ± 標準偏差	
	変形なし	変形あり
安静	0.676 ± 0.132	0.919 ± 0.068
T’0 (0)	0.700 ± 0.141	0.928 ± 0.072
T’1 (2)	0.705 ± 0.136	0.920 ± 0.073
T’2 (3)	0.729 ± 0.121	0.916 ± 0.081
T’3 (2)	0.724 ± 0.110	0.933 ± 0.055
T’4 (3)	0.727 ± 0.123	0.917 ± 0.064
T’5 (0)	0.721 ± 0.115	0.929 ± 0.056

P6MS データセットにおける脈波変形結果の例を図 7.5，7.6 に示す．いずれの例も，安静状態で計測された脈波を利用している．図 7.5 は，参加者 P12 の左指先脈波を利用して左手首脈波を推定した例であり，図 7.6 は，参加者 P6 の右手首脈波を利用して左手首脈波を推定した例である．

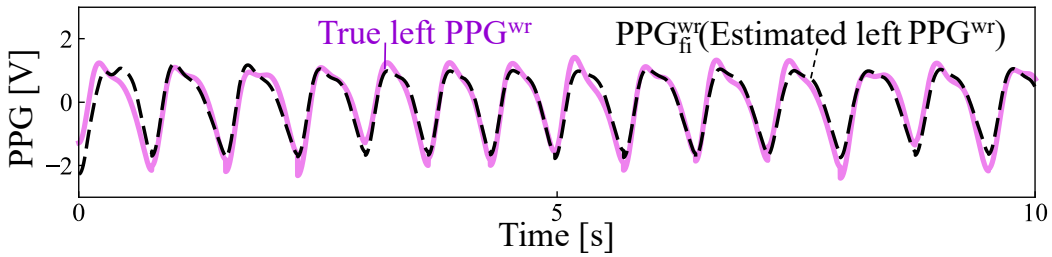


図 7.5: P6MS データセットにおける脈波変形結果 (参加者 P12，安静状態)

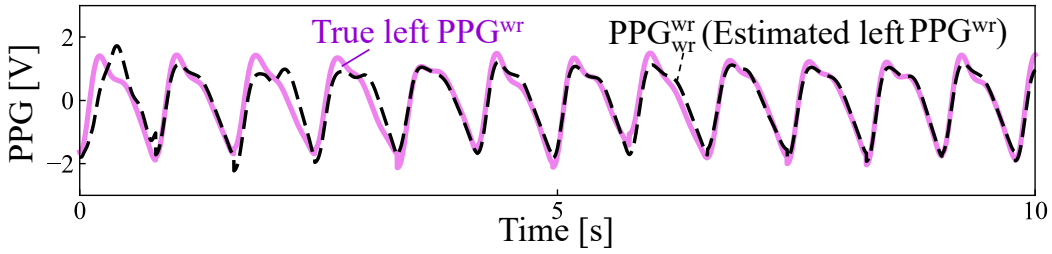


図 7.6: P6MS データセットにおける脈波変形結果 (参加者 P6，安静状態)

MAUS データセットにおける脈波変形結果の例を図 7.7 に示す．参加者 P17 の安静状態で計測した指先脈波から，手首脈波を推定した例である．

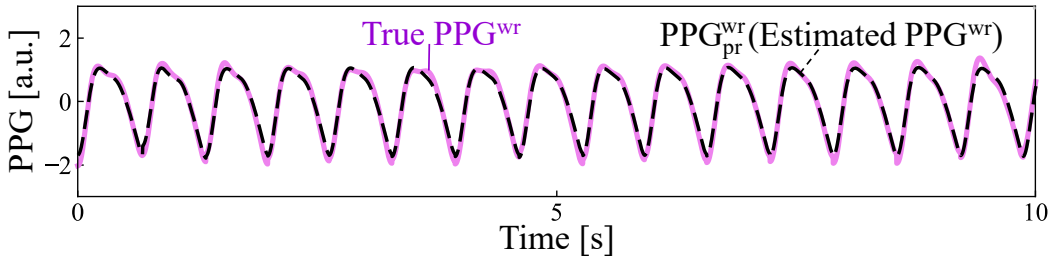
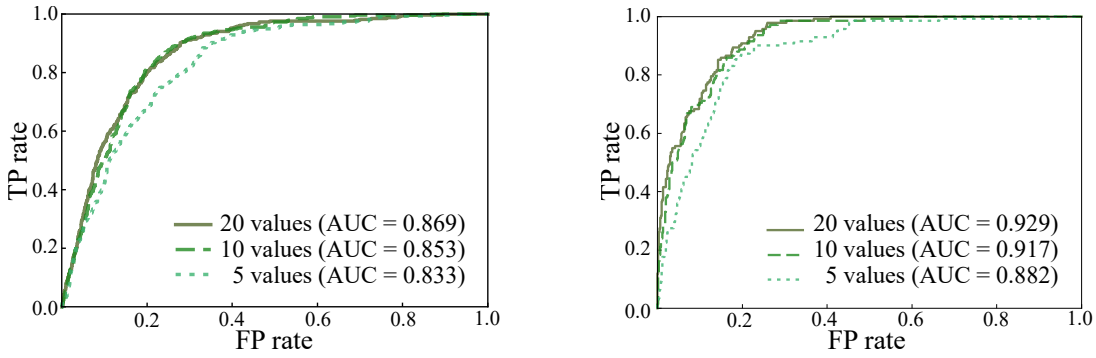


図 7.7: MAUS データセットにおける脈波変形結果 (参加者 P17，安静状態)

7.2.2 対策の評価結果

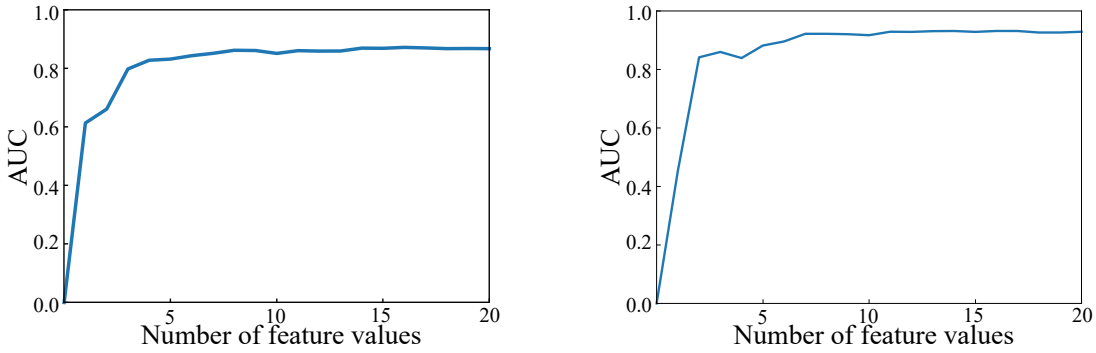
部位識別の評価結果

図 7.8(a)(b) に，P6MS データセットにおいて，それぞれ脈波を変形しない場合，脈波を変形した場合の手首の識別に関する ROC (Receiver operating characteristic) 曲線を示す．特徴量数は 5, 10, 20 個と変更して比較した．また，同 ROC 曲線の評価指標として，ROC 曲線と，右側の縦軸と，下側の横軸で囲まれた面積 AUC (Area under the curve) [136] を算出した．図 7.9 に，同データセットにおいて，それぞれ脈波を変形しない場合，脈波を変形した場合の AUC と特徴量数の関係を示す．また，脈波を変形しない場合，脈波を変形した場合において，特徴量 5 個を使用して得られる部位識別の正解率は，それぞれ 0.827，0.845 であった．



(a) 脈波を変形しない場合　　(b) 脈波を変形した場合

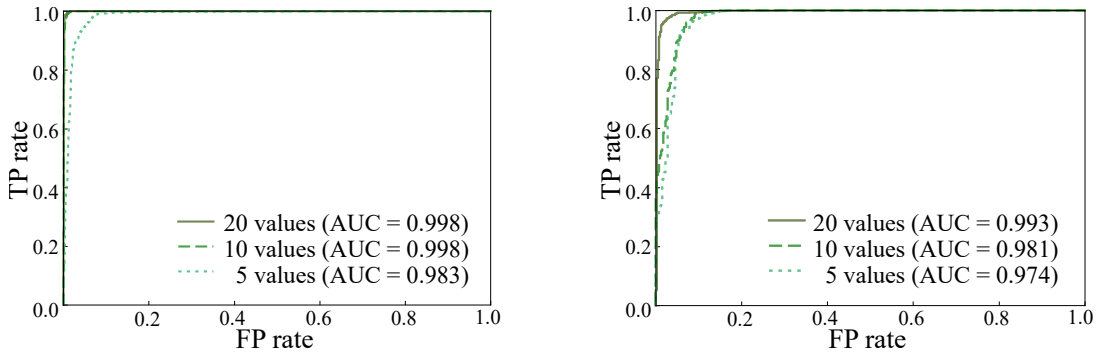
図 7.8: P6MS データセットを使用して手首脈波を識別した際の ROC 曲線



(a) 脈波を変形しない場合　　(b) 脈波を変形した場合

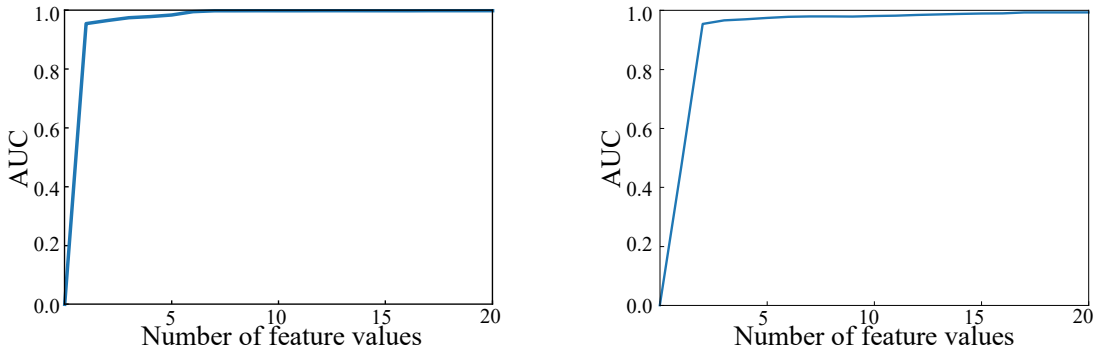
図 7.9: P6MS データセットにおける手首脈波識別時の AUC と特徴量数の関係

図 7.10(a)(b) に，MAUS データセットにおいて，それぞれ脈波を変形しない場合，脈波を変形した場合の手首の識別に関する ROC 曲線を示す．P6MS データセットと同様に，特徴量数は 5, 10, 20 個と変更して比較し，ROC 曲線の下側の面積 AUC を算出した．図 7.11 に，同データセットにおいて，それぞれ脈波を変形しない場合，脈波を変形した場合の AUC と特徴量数の関係を示す．また，脈波を変形しない場合，脈波を変形した場合において，特徴量 5 個を使用して得られる部位識別の正解率は，それぞれ 0.946，0.956 であった．



(a) 脈波を変形しない場合　　(b) 脈波を変形した場合

図 7.10: MAUS データセットを使用して手首脈波を識別した際の ROC 曲線



(a) 脈波を変形しない場合　　(b) 脈波を変形した場合

図 7.11: MAUS データセットにおける手首脈波識別時の AUC と特徴量数の関係

部位識別において，各特徴量について PI を算出し，その大小を比較して得られた PI 順位を表 7.4 に示す．PI 順位により選定した，対策における時間経過の影響の検証に使用した特徴量 5 個については，太字で記載した．

表 7.4: 部位識別における各特徴量の PI 順位

変数名	特徴量の概要	PI 順位
$C_{i,0}$	平均	7
$C_{i,1}$	**標準偏差**	5
$C_{i,2}$	**DTW**	2
$C_{i,5}$	最大値時刻	18
$C_{i,6}$	最小値時刻	11
$C_{i,7}$	Wavelet 係数最大値	12
$C_{i,8}$	**Wavelet 係数最小値**	4
$C_{i,9}$	歪度	10
$C_{i,10}$	尖度	33
$C_{i,11}$	極大値個数	37
$C_{i,12}$	**正の傾き**	27
$C_{i,13}$	負の傾き	26
$C_{i,14}$	1 個目の極大値時刻	28
$C_{i,15}$	MFCC0	24
$C_{i,16}$	MFCC1	16
$C_{i,17}$	MFCC2	35
$C_{i,18}$	MFCC3	39
$C_{i,19}$	MFCC4	31
$C_{i,20}$	MFCC5	40
$C_{i,21}$	MFCC6	26
$C_{i,22}$	MFCC7	17
$C_{i,23}$	MFCC8	9
$C_{i,24}$	MFCC9	38
$C_{i,25}$	MFCC10	34
$C_{i,26}$	MFCC11	29
$C_{i,27}$	MFCC12	22
$C_{i,28}$	MFCC13	30
$C_{i,29}$	MFCC14	21
$C_{i,30}$	MFCC15	19
$C_{i,31}$	MFCC16	32
$C_{i,32}$	MFCC17	36
$C_{i,33}$	MFCC18	15
$C_{i,34}$	MFCC19	8
$C_{i,35}$	MFCC20	23
$C_{i,36}$	MFCC21	1
$C_{i,37}$	MFCC22	6
$C_{i,38}$	MFCC23	14
$C_{i,40}$	最大値時刻	20
$C_{i,41}$	**重複切痕時刻**	3
$C_{i,42}$	振幅比	13

時間経過の影響の評価結果

MAUS データセットを利用して，時間経過に伴う対策の有効性の変化を検証した．安静状態の脈波から抽出した特徴量で識別器を生成し，N バック課題実施時の脈波から抽出した特徴量を入力した際の正解率を算出した．表 7.5 に時間経過に伴う対策の有効性の変化を検証した結果を示す．表 7.3 と同様に，各試行における () 内の数字は，N バック課題において，提示された数字と比較する数字の位置として，参加者に指定した数を表す．

表 7.5: 時間経過に伴う対策の有効性の変化

試行	正解率	
	変形なし	変形あり
T’0 (0)	0.966	0.909
T’1 (2)	0.962	0.928
T’2 (3)	0.944	0.907
T’3 (2)	0.951	0.941
T’4 (3)	0.952	0.953
T’5 (0)	0.952	0.945

7.3 対策の検証結果の考察

本節では，7.2 節で述べた，提案する対策の有効性の検証結果を考察する．まず，2 種類のデータセットを利用した，波形の評価について述べる．続いて，対策の評価として，部位識別の精度や，時間経過の影響，有効な特徴量，対策の拡張性について述べる．

7.3.1 波形の評価

提案する対策の検証の前に，2 種類の脈波データセットを利用した場合の攻撃の成立の可能性を調査するため，波形間の類似性の指標として相関係数を算出した．P6MS データセットを用いた場合，表 7.2 に示した通り，左手首脈波と他部位脈波の全ての組合せにおいて，脈波を変形しない場合は，脈波間の相関係数 CORR について，$|\mathrm{CORR}| > 0.800$ となることが確認できた．また，脈波を変形した場合も，$|\mathrm{CORR}| > 0.800$ となり，全ての部位において，脈波を変形しない場合よりも，|CORR| が大きくなることが確認できた．MAUS データセットを用いた場合，表 7.3 に示した通り，手首脈波と指先脈波の組合せにおいて，脈波間の CORR について，脈波を変形しない場合は安静状態を除いて $|\mathrm{CORR}| > 0.700$ となることが確認できた．脈波を変形した場合は全ての条件について $|\mathrm{CORR}| > 0.900$ となり，脈波を変形しない場合よりも，|CORR| が大きくなることが確認できた．

Mukaka は，2 データ間の CORR に対して，$|\mathrm{CORR}| > 0.9$ であれば，同データ間に非常に強い相関が存在すると定めている．また，$0.7 < |\mathrm{CORR}| < 0.9$ であれば，同データ間に強い相関が存在すると定めている [92]．したがって，P6MS データセットに含まれる，異なる部位で計測された脈波間には，脈波の変形の有無に関わらず，強い相関があると考えられる．MAUS データセットに含まれる，異なる部位で計測された脈波間には，脈波を変形しない場合は強い相関，脈波を変形した場合は非常に強い相関があると考えられる．さらに，Patil らは，脈波認証に使用する指標として相関係数を採用しており，同じ人物の同じ部位で計測した脈波間の CORR について，多くの試行において，$|\mathrm{CORR}| > 0.800$ を満たすことを示している [125]．したがって，両データセットにおける異なる部位で計測された脈波間の相関から，異なる部位で計測した脈波の利用，さらに脈波の変形により，脈波認証へのなりすまし攻撃が成立する可能性が確認できた．

7.3.2 対策の評価

部位識別の評価

提案する対策の検証では，2 種類の脈波データセットを利用して，特徴量を利用した部位識別により，手首脈波を識別可能か否か，ROC 曲線および AUC を算出して検証した．Zhu らは，識別結果として得られた ROC 曲線に対して，AUC の値による評価として，$0.9 \leq \mathrm{AUC} \leq 1.0$ であれば優秀，$0.8 \leq \mathrm{AUC} \leq 0.9$ であれば良好，$0.7 \leq \mathrm{AUC} \leq 0.8$ であれば無価値，$0.6 \leq \mathrm{AUC} \leq 0.7$ であれば無駄，と定めている [137]．Zhu らが定めた基準を適用すると，特徴量を 5 個程度使用すれば，いずれのデータセットにおいても，脈波変形の有無を問わず，良好な識別率が確認できた．また，7.2.2 節で述べた通り，特徴量 5 個を部位識別に利用した場合，脈波変形の有無を問わず，P6MS データセットについては 0.800 以上の正解率，MAUS データセットについては，0.950 程度の正解率が得られた．したがって，特徴量を利用した部位識別による対策の有効性が示唆された．

7.3.1 節では，各データセットに含まれる，手首以外で計測された脈波を変形することで，脈波認証へのなりすまし攻撃の成功可能性が向上する可能性が示唆された．しかし，7.2.2 節で述べた通り，5 個の特徴量を利用して，提案する対策における部位識別を検証した結果，各データセットにおいて脈波の変形により正解率が向上したことから，他部位脈波と真の手首脈波の識別よりも，他部位脈波を変形した脈波と真の手首脈波の識別の方が容易であることが示された．一般に，周波数解析等に基づいて，生体信号の波形を推定する場合の推定精度と，推定した波形の個人差にはトレードオフの関係があることが知られている [138–140]．したがって，本実験においては複数の人物の脈波から伝達関数を生成したことにより，被害者の真の手首脈波だけではなく，複数の人物の手首脈波に類似した波形が生成されたことで，被害者の真の手首脈波との識別は却って容易となった可能性が考えられる．ただし，表 7.2 および表 7.3，7.3.1 節で示した通り，各データセットにおいて，手首以外で計測された脈波を変形した方が，真の手首脈波との CORR は大きくなった．CORR は認証における評価指標として使用されることがあるため [125]，脈波の変形がなりすまし攻撃において有効である可能性も示されている．

脈波は様々な部位で計測可能であるが，今回の検証では，近接した部位である手首，手指において計測された脈波を対象とした．他の計測部位としては，手首や指から離れた部位である，額や上腕，足指等が挙げられる [71,89]，今回の検証では，提案する対策である脈波の計測部位の識別が，手首や指から離れた部位に対しても有効か否かは検証していない．一方，近接した複数の部位で脈波を計測する場合は，離れた部位で計測する場合よりも，類似した波形が得られることが知られている [81]．したがって，今回の検証対象より離れた部位である，額や上腕，足指等で計測された脈波に対しても，提案する対策である計測部位の識別は有効と考えられる．また，今回使用したデータセットは，脈波センサを手首や指に接触させて計測された脈波が含まれているが，顔をカメラで撮影して得られる映像を利用することで，センサを特定部位に接触させずに脈波を計測することも可能である．カメラで顔を撮影して得られる脈波を利用した，脈波認証へのなりすまし攻撃が検証されているが [56]，攻撃成功率はカメラの仕様に依存し，画質やフレームレートを高く設定可能なカメラ以外では，攻撃に適切な波形の生成が困難であることが示されている [141]．したがって，カメラで顔を撮影して得られる脈波に対しても，多くの場合は，手首の脈波か否かの識別は可能と考えられる．

時間経過の影響の評価

部位識別の評価に続いて，MAUS データセットを用いて，提案する対策の有効性の時間経過に伴う変化を検証した．本評価では，表 7.4 に記載した特徴量のうち下線を付記した，PI の大きい特徴量 5 個を使用した．表 7.5 に示すように，試行を続けるにつれて，脈波を変形しない場合は，正解率が減少する傾向があったが，いずれの試行においても，正解率は 0.940 を上回った．また，試行 T’4 を除いて，脈波を変形した場合は，変形しない場合の正解率を下回った．したがって，本評価における多くの試行において，脈波を変形した場合，変形しない場合よりも高い確率で攻撃が成立してしまう可能性が示唆された一方で，脈波を変形しない場合には存在しなかった，正解率が 0.910 を下回る試行も存在し，提案する対策の有効性も示された．また，本評価では，実験参加者が N バック課題を実施している状態において，計 2,820 s 間計測した脈波が含まれるデータセットを使用している．N バック課題と同様に，デバイスを装着して机上で一定の作業をしている状態において，同程度の時間内に計測された脈波であれば，計測部位の識別による対策が有効となる可能性がある．

対策に有効な特徴量

本章では，部位識別に対する時間経過の影響の評価のため，表 7.4 に記載した特徴量のうち下線を付記した，PI の大きい特徴量 5 個を使用した．一方，5 章では，表 5.10 に記載した通り，攻撃および認証における各特徴量の寄与を PI を用いて評価した．その結果，5.6 節で述べた通り，メル周波数ケプストラム係数等，情報漏洩の可能性が低く，攻撃における PI の小さい特徴量を認証に利用することで，攻撃成功率を低減できる可能性を示した．また，表 5.10 で PI 順位が高い特徴量と，表 7.4 で下線を付記した特徴量は，共通のものが存在する．例えば，DTW $C_{i,2}$ は，識別器として SVM を利用した際に，認証時の PI 順位は 2，攻撃時の PI 順位は 9 だった．また，特徴量間の相関を示した表 5.6 や図 5.22(a) において，DTW は漏洩していることが示されており，認証への利用は適切ではない．しかし，表 7.4 に記載した通り，対策である部位識別において DTW を利用することは有効であった．したがって，図 4.5 に示した認証と対策の位置づけにおいて，認証に有効な特徴量と，対策に有効な特徴量は必ずしも一致しなかった．図 4.5 のような攻撃対策を含む認証手法の開発には，各処理において PI 等の評価指標の算出により，使用する特徴量を適切に選定することに加えて，情報漏洩の検証により，漏洩の可能性が低い特徴量を認証に利用することが重要であると考えられる．

一般に，脈波のような生体情報を長い時間計測して認証に利用する場合，時間経過によりその波形は変化して，認証精度は低くなる [54]．また，パスワードの変更と同様に，脈波のような生体情報を変更することは不可能であり，同じ種類の生体情報を長い期間利用し続ける場合，情報漏洩および攻撃に利用される可能性が高くなると考えられる [142]．しかし，本検証では，前段落で述べた DTW のように，脈波計測において漏洩している情報を敢えて利用することで，なりすまし攻撃の検出が可能であることを示した．したがって，提案する対策は，生体情報を継続的に取得することで実現される，継続認証において有効であると考えられる．

対策の拡張性

本検証では，識別器に対して特徴量を入力して，脈波の計測部位を識別した．本算出における特徴量の入力は，脈波の 1 周期分である 1 セグメント分の信号の入力に該当する．しかし，6.2 節において，複数のセグメントを含む試行観点での攻撃成功率を考慮したように，実際の攻撃では，複数周期の信号を入力し続ける可能性がある．このような攻撃に対しては，試行回数の上限の設定と，同回数に応じた対応が有効である．例えば，一定時間内において，部位識別に基づく検出により，攻撃と識別された試行回数が上限に達した場合，対応として対象者を強制的にログアウトさせ，数分間再認証禁止とする．一方，一定時間内において，攻撃として識別された試行回数が上限未満だった場合は，再認証を要求する．したがって，提案する対策を拡張し，その後の対応との組合せにより，攻撃に応じた動的な対策が可能である．

7.4 まとめ

本章では，5，6 章で実現可能性を検証した，脈波認証へのなりすまし攻撃に対する，4.2 節で提案した対策の有効性を検証した．同対策は，身体上の様々な部位で計測可能である脈波間の差に着目して部位特有の特徴量を抽出し，計測部位を識別することで入力の正当性を検証し，攻撃を検出する．本実験では，複数の部位で計測された脈波のデータセットを 2 個用意し，計測部位を識別可能か検証した．その結果，各データセットにおいて，脈波に対する変形の有無を問わず，計測部位の識別率は 0.800 以上となり，提案する対策の有効性が示唆された．提案する対策では，情報漏洩の可能性がある特徴量の利用も可能であり，同対策を拡張してその後の対応との組合せにより，攻撃内容に応じた動的な対策が実現可能である．

第8章

おわりに

本章では，本研究で検討した，脈波認証システムに対して起こり得るなりすまし攻撃，同攻撃への対策を，検証結果とともにまとめる．続いて，本研究の社会的展望についても述べる．

8.1　攻撃対策を備えた脈波認証システムの実現

本研究では，無意識計測により対象者に負担を課さない，さらに攻撃対策を備えた認証システムの実現を目的として，一度認証を行った後も認証処理を繰り返す “継続認証” への光電容積脈波の利用を検討した．続いて，脈波認証システムに起こり得る攻撃を検討し，さらに同攻撃への対策についても検討した．以下では，同攻撃および同対策に関する検討内容と検証結果についてまとめる．

脈波認証システムに対して起こり得る攻撃として，身体上の様々な部位で計測可能という脈波の利点に着目し，将来的に起こり得るなりすまし攻撃を検討した．同攻撃では，複数部位で計測可能である脈波計測の利点を攻撃者が悪用し，認証に必要な情報が正規の計測部位以外からも得られ，攻撃者による偽の入力として利用されることを想定した．認証に必要な情報の漏洩を検証するため，複数部位で脈波を計測する装置を構築し，同装置を利用して，12 名の実験参加者の複数部位で脈波を計測した．各部位で計測した脈波間の相関や，抽出した特徴量の誤差や相関の調査結果から，脈波認証において必要となる，手首において計測される情報が，別の部位からも計測される可能性が示唆された．また，既存研究において使用されている全 43 個の特徴量について，認証および攻撃時の重要度を算出した．同重要度を基に，認証時に使用する特徴量の組合せを変更，攻撃成功率を最大 62.8 %低減できることが確認できた．

情報漏洩の検証および特徴量の評価結果を踏まえて，検討したなりすまし攻撃の実現可能性を検証した．本検証では，攻撃者は，不正なセンサを設置して被害者の脈波を計測し，同脈波をセンサに対する偽の入力として認証の突破に利用することに加えて，攻撃成功率向上のため脈波を変形することも想定した．本検証では，脈波を計測する装置と，既存手法における識別アルゴリズムの組合せにより，脈波認証システムを試作した．センサを手指に固定した理想的な条件下において，計測 1 回分の脈波を 1 回分の攻撃に用いた場合の攻撃成功率を求めた結果，基節部脈波を利用した場合，指先脈波を利用した場合の攻撃成功率はいずれも 0.800 以上となり，攻撃の実現可能性が示唆された．攻撃の成功率向上のために脈波を変形した場合は，伝達関数の適切な選定により，変形しない場合では攻撃失敗した試行について，攻撃成功することが示唆された．

検討したなりすまし攻撃の実現可能性が示唆されたため，同攻撃の特徴である，正規の計測部位以外で計測した脈波を利用することに着目した対策を検討した．同対策では，高い搭載性の実現を目標として，脈波認証システムに対して脈波センサ以外のセンサ等を追加せず，脈波から部位特有の特徴量を抽出して計測部位を識別する．同識別により，脈波認証システムへの入力の正当性を検証することでなりすまし攻撃を検出し，検出に応じて対象者の強制ログアウト等の対応を実施する．同対策は拡張性を有しており，試行回数の上限等も設定することで，その後の対応との組合せにより，攻撃内容に応じた動的な対応が可能である．実験において，複数の部位で計測した脈波のデータセットを 2 個用意し，各脈波から抽出した特徴量を用いて，計測部位を識別可能か否か検証した．その結果，各データセットにおいて，脈波に対する変形の有無を問わず，計測部位の識別率は 0.800 以上となったことから，脈波から抽出した特徴量を使用する対策の有効性が示唆された．

以上の結果から，脈波認証システムに対して起こり得る，認証に必要な情報の漏洩の可能性と，同漏洩を利用したなりすまし攻撃の実現可能性が示唆された．加えて，同攻撃への対策として，脈波認証システムに対して脈波センサ以外のセンサ等の要素を追加せずに，脈波から得られる情報を検出に利用することの有効性も示唆された．提案する対策は拡張性を有しており，その後の対応との組合せにより，攻撃に応じた動的な対策が可能である．したがって，図 8.1 に示すように，計測した脈波の解析を基にして，攻撃内容に応じた動的な対策を備えた脈波認証システムの実現可能性が示された．

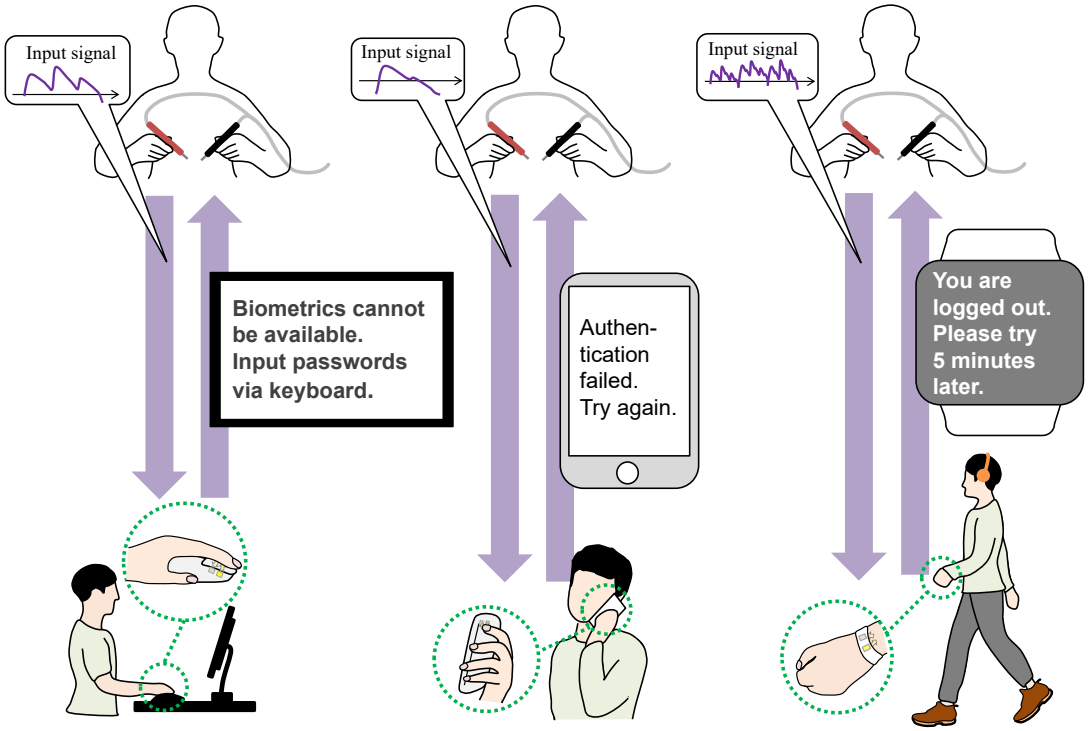


図 8.1: 動的な攻撃対策を備えた脈波認証システム

8.2 社会的展望

本研究では，無意識計測が可能である光電容積脈波に着目し，継続認証への利用を提案するとともに，脈波認証へ起こり得るなりすまし攻撃，同攻撃への対策を検討した．本研究の社会的貢献の可能性を示すため，無意識計測・なりすまし攻撃耐性・対策搭載性を観点とした，従来の認証手法と提案手法の比較を図 8.2 に示す．図 8.2 右上に位置されるように，継続認証への利用を提案した光電容積脈波は，無意識的に計測可能であり，脈波認証は他の認証手法と比較すると，計測対象者への負荷が比較的小さい．また，提案する対策は，脈波センサ以外の物理的要素の追加は不要であり，対策の搭載性は高い．さらに，脈波は計測対象者の心身の状態に関する情報を含んでいるため，脈波を計測および解析して認証に利用するとともに，個人および心身の状態に応じたサービスの提供も実現できる可能性がある．本研究では，脈波を計測し，同脈波を解析して得られる情報を利用した脈波認証に対する攻撃を検討するとともに，同解析により得られる情報を利用した，同攻撃に対する対策を提案して，その有効性を示した．同対策は，脈波センサを搭載した市販のスマートウォッチ等に実装可能な機能として，脈波認証とともに攻撃対策を実現できると考えられる．攻撃対策を備えた脈波認証システムにより，脈波に基づいた個人および心身の状態に応じたサービス提供を，安全に実現することが期待される．

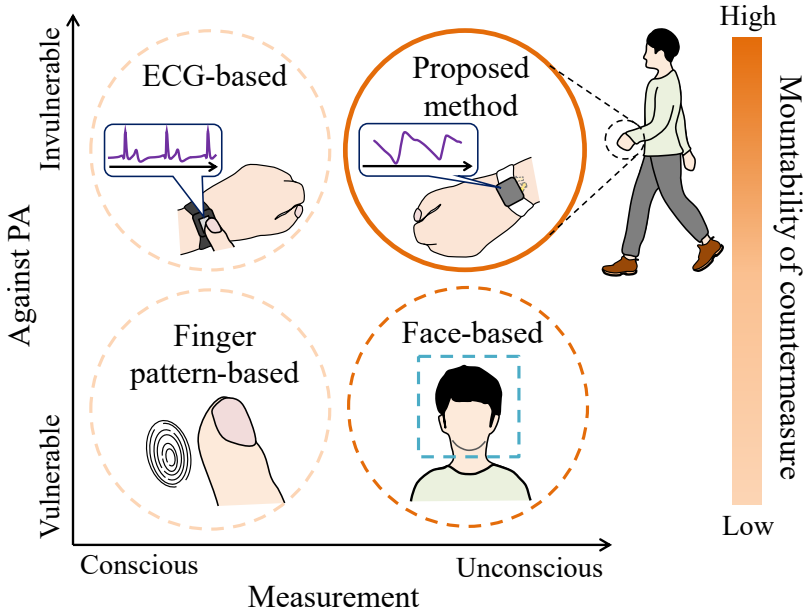


図 8.2: 従来の認証手法と提案手法の比較

謝 辞

本研究は大阪大学 大学院基礎工学研究科で行った．

博士後期課程に入学して3年間が経過しました．社会人学生という立場や，新型コロナウィルスの感染拡大に伴って，思い通りに活動できないこともありましたが，非常に充実した3年間を過ごすことができました．大城研究室スタッフの皆様をはじめとする方々に数々のご協力をいただき，深く感謝申し上げます．

博士後期課程学生としての受け入れを快諾して頂き，本研究の方向性に関して多大なるご指導を頂きました，大阪大学 大学院基礎工学研究科 大城 理 教授に厚くお礼申し上げます．社会人学生であることも考慮して頂き，対面や遠隔を問わず，学部生および博士前期課程学生時代と同様にご指導をして頂きました．重ねて感謝申し上げます．

本論文の副査を引き受けて頂き，数多くのご意見およびご指導を頂きました，大阪大学 大学院基礎工学研究科 青井 伸也 教授ならびに，大阪大学 大学院基礎工学研究科 清野 健 教授に深く感謝致します．

本研究の有用化や差別化に向けた質問やアイデアを提示して頂いた，大阪大学 大学院基礎工学研究科 池田 聖 准教授に厚くお礼申し上げます．実装方法や文献調査方法に関しても丁寧にご指導頂きました．重ねて感謝申し上げます．

本研究の方針や投稿論文に関して鋭く有用なご意見を頂いた，大阪大学 大学院基礎工学研究科 石塚 裕己 助教に厚くお礼申し上げます．博士後期課程学生としての姿勢に関しても熱心にご指導頂きました．重ねて感謝申し上げます．

学部生時代，学術文書の執筆や研究の進め方を丁寧にご指導頂きました，関西学院大学 工学部 井村 誠孝 教授に厚くお礼申し上げます．ご栄転後も研究会等でお会いした際にお気遣いを頂きました．重ねて感謝申し上げます．

博士前期課程学生時代，理論を基に研究を進めることの重要性を教えて頂きました，筑波大学 システム情報系 黒田 嘉宏 教授に厚くお礼申し上げます．ご栄転後も連絡を差し上げた際にお気遣いを頂きました．重ねて感謝申し上げます．

学部生時代および博士前期課程学生時代，論文投稿や研究に取り組む姿勢に関しても基本から丁寧にご指導を頂きました，東京大学 大学院新領域創成科学研究科 吉元 俊輔 講師に厚くお礼申し上げます．ご栄転後も私の社会人生活を気にかけて頂きました．重ねて感謝申し上げます．

博士前期課程学生時代，食事の際に気さくに話しかけて頂く等，様々なお気遣いを頂きました，大城研究室 秘書 杉浦 延予 氏に感謝いたします．

企業の研究員としての姿勢を教えて頂きました，三菱電機株式会社 情報技術総合研究所 情報セキュリティ技術部 大松 史生 部長にお礼申し上げます．博士後期課程進学に関して快諾して頂き，進学後は研究進捗に関してお気遣いを頂きました．重ねて感謝申し上げます．

業務と学業の両立に関して配慮して頂いた，三菱電機株式会社 情報技術総合研究所 情報セキュリティ技術部 開発第 1 グループ 松田 規 グループマネージャにお礼申し上げます．研究に関して相談に応じて頂きつつ，私の業務負荷に関しても常にお気遣いを頂きました．重ねて感謝申し上げます．

本研究の方向性に関して相談に応じて頂いた，三菱電機株式会社 情報セキュリティ統括室 セキュリティ技術部 PSIRT グループ 鈴木 大輔 グループマネージャにお礼申し上げます．セキュリティ研究者としてのご意見から，論文投稿や国際会議発表に有用な多くのことを学びました．重ねて感謝申し上げます．

新入社員時代，育成指導担当としてお世話になった，三菱電機株式会社 情報技術総合研究所 情報セキュリティ技術部 開発第 1 グループ 清水 孝一 主席研究員にお礼申し上げます．セキュリティに関して何の知見もなかった私に，基礎から丁寧にご指導を頂きました．重ねて感謝申し上げます．

学部生での研究室配属時から，何もわからない私に親身になってご指導を頂いた，研究室先輩の皆様に感謝します．学部生時代および博士前期課程学生時代，毎日切磋琢磨し合った研究室同期の皆様に感謝します．研究室後輩の皆様には，熱心に研究に取り組む姿勢から刺激を受けました．感謝します．

本研究を進める上では，他にも多くの方にご理解およびご協力を頂きました．本論文に名前を記すことができなかった多くの方々に感謝します．

本研究における実験は，三菱電機 東部研究所地区 倫理審査委員会の承認 (2020-B001) を得て行った．実験参加者には実験内容について説明を行い，書面にて同意を得られた場合にのみ計測を行った．

参考文献

[1] J. Ruesch. Synopsis of the theory of human communication. *Psychiatry*, Vol. 16, No. 3, pp. 215–243, 1953.

[2] G. Balbi and J. Kittler. One-to-one and one-to-many dichotomy: Grand theories, periodization, and historical narratives in communication studies. *International Journal of Communication*, Vol. 10, p. 20, 2016.

[3] L. Fortunati, F. Cavallo, and M. Sarrica. Multiple communication roles in human–robot interactions in public space. *International Journal of Social Robotics*, pp. 1–14, 2018.

[4] G. Roussos, A. J. Marsh, and S. Maglavera. Enabling pervasive computing with smart phones. *IEEE Pervasive Computing*, Vol. 4, No. 2, pp. 20–27, 2005.

[5] J. Morris, S. LaForce, and J. Mueller. Emergency communications and people with disabilities: 9-1-1 communication, public alerts, and social media. *Wireless RERC*, pp. 1–16, 2011.

[6] D. Laursen and K. Sandvik. Talking with tv shows: Simultaneous conversations between users and producers in the second-screen television production voice. *Northern Lights: Film & Media Studies Yearbook*, Vol. 12, No. 1, pp. 141–160, 2014.

[7] R. S. Sexton, R. A. Johnson, and M. A. Hignite. Predicting internet/e-commerce use. *Internet Research*, 2002.

[8] A. Gillis and L. M. Krull. Covid-19 remote learning transition in spring 2020: class structures, student perceptions, and inequality in college courses. *Teaching Sociology*, Vol. 48, No. 4, pp. 283–299, 2020.

[9] A. L. Blanchard. The effects of covid-19 on virtual working within online groups. *Group Processes & Intergroup Relations*, Vol. 24, No. 2, pp. 290–296, 2021.

[10] M. Kjaerland. A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security*, Vol. 25, No. 7, pp. 522–538, 2006.

[11] M. Riaz, S. Elder, and L. Williams. Systematically developing prevention, detection, and response patterns for security requirements. In *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)*, pp. 62–67, Beijing, China, 2016. IEEE.

[12] S. Jajodia and S. Noel. Topological vulnerability analysis: A powerful new approach for network attack prevention, detection, and response. In *Algorithms, Architectures and Information Systems Security*, pp. 285–305. World Scientific, 2009.

[13] C. J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang. Nice: Network intrusion detection and countermeasure selection in virtual network systems. *IEEE Transactions on Dependable and Secure Computing*, Vol. 10, No. 4, pp. 198–211, 2013.

[14] G. I. P. Duppa and N. Surantha. Evaluation of network security based on next generation intrusion prevention system. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, Vol. 17, No. 1, pp. 39–48, 2019.

[15] H. Deng, W. Wang, and C. Peng. Ceive: Combating caller id spoofing on 4g mobile phones via callee-only inference and verification. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18)*, pp. 369–384, New Delhi, India, 2018.

[16] M. Zviran and Z. Erlich. Identification and authentication: technology and implementation issues. *Communications of the Association for Information Systems*, Vol. 17, No. 1, p. 4, 2006.

[17] S. Lee, W. Choi, and D. H. Lee. Usable user authentication on a smartwatch using vibration. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pp. 304–319, Virtual Event, Republic Korea, 2021. ACM.

[18] I. Nakanishi, S. Baba, and C. Miyamoto. Eeg based biometric authentication using new spectral features. In *2009 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, pp. 651–654, Kanazawa, Japan, 2009. IEEE.

[19] F. Agrafioti, K. Martin, and S. Oung. Preauthorized wearable biometric device, system and method for use thereof. U.S. Patent 9 472 033 B2, 2016.

[20] Apple. watchos - feature availability. https://www.apple.com/watchos/feature-availability/. accessed on October 30, 2022.

[21] A. B. Hertzman. Photoelectric plethysmography of the fingers and toes in man. *Proceedings of the Society for Experimental Biology and Medicine*, Vol. 37, No. 3, pp. 529–534, 1937.

[22] M. A. F. Pimentel, A. E. W. Johnson, P. H. Charlton, D. Birrenkott, P. J. Watkinson, L. Tarassenko, and D. A. Clifton. Toward a robust estimation of respiratory rate from pulse oximeters. *IEEE Transactions on Biomedical Engineering*, Vol. 64, No. 8, pp. 1914–1923, 2016.

[23] Apple. Monitor your heart rate with apple watch. https://support.apple.com/en-us/HT204666. accessed on October 30, 2022.

[24] S. Heo, S. Kwon, and J. Lee. Stress detection with single ppg sensor by orchestrating multiple denoising and peak-detecting methods. *IEEE Access*, Vol. 9, pp. 47777–47785, 2021.

[25] T. Buddhika, H. Zhang, S. W. T. Chan, V. Dissanayake, S. Nanayakkara, and R. Zimmermann. fsense: Unlocking the dimension of force for gestural interactions using smartwatch ppg sensor. In *Proceedings of the 10th Augmented Human International Conference 2019*, pp. 1–5, Reims, France, 2019. ACM.

[26] S. A. Mascaro and H. H. Asada. Measurement of finger posture and three-axis fingertip touch force using fingernail sensors. *IEEE Transactions on Robotics and Automation*, Vol. 20, No. 1, pp. 26–35, 2004.

[27] T. Zhao, Y. Wang, J. Liu, J. Cheng, Y. Chen, and J. Yu. Robust continuous authentication using cardiac biometrics from wrist-worn wearables. *IEEE Internet of Things Journal*, Vol. 9, No. 12, pp. 9542–9556, 2021.

[28] R. Ramachandra and C. Busch. Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Computing Surveys (CSUR)*, Vol. 50, No. 1, pp. 1–37, 2017.

[29] A. B. Ajmal, M. A. Shah, C. Maple, M. N. Asghar, and S. U. Islam. Offensive security: Towards proactive threat hunting via adversary emulation. *IEEE Access*, Vol. 9, pp. 126023–126033, 2021.

[30] C. Sousedik and C. Busch. Presentation attack detection methods for fingerprint recognition systems: a survey. *Iet Biometrics*, Vol. 3, No. 4, pp. 219–233, 2014.

[31] S. Eberz, N. Paoletti, M. Roeschlin, M. Kwiatkowska, I. Martinovic, and A. Patané. Broken hearted: How to attack ecg biometrics. In *NDSS Symposium 2017*, pp. 1–15, San Diego, USA, 2017. Internet Society.

[32] J. J. Engelsma, K. Cao, and A. K. Jain. Raspireader: Open source fingerprint reader. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 41, No. 10, pp. 2511–2524, 2018.

[33] E. M. Nowara, A. Sabharwal, and A. Veeraraghavan. Ppgsecure: Biometric presentation attack detection using photopletysmograms. In *2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017)*, pp. 56–62, Washington, USA, 2017. IEEE.

[34] A. M. Gamundani, A. Phillips, and H. N. Muyingi. An overview of potential authentication threats and attacks on internet of things (iot): A focus on smart home applications. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications*

(GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 50–57, Melbourne, Australia, 2018. IEEE.

[35] A. Dantcheva, P. Elia, and A. Ross. What else does your biometric data reveal? a survey on soft biometrics. *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 3, pp. 441–467, 2015.

[36] M. N. Yaacob, S. Z. S. Idrus, W. N. A. W. Ali, W. A. Mustafa, M. A. Jamlos, and M. H. Abd Wahab. Soft biometrics and its implementation in keystroke dynamics. *Journal of Physics: Conference Series*, Vol. 1529, No. 2, p. 022086, 2020.

[37] A. Dantcheva, C. Velardo, A. D'angelo, and J. L. Dugelay. Bag of soft biometrics for person identification. *Multimedia Tools and Applications*, Vol. 51, No. 2, pp. 739–777, 2011.

[38] S. S. Gornale. Fingerprint based gender classification for biometric security: A state-of-the-art technique. *American International Journal of Research in Science, Technology, Engineering & Mathematics (AIJRSTEM)*, Vol. 9, No. 1, pp. 39–49, 2015.

[39] T. W. Shen, W. J. Tompkins, and Y. H. Hu. One-lead ecg for identity verification. In *Proceedings of the Second Joint 24th Annual Conference and the Annual Fall Meeting of the Biomedical Engineering Society*, Vol. 1, pp. 62–63. IEEE, 2002.

[40] T. Zhao, Y. Wang, J. Liu, Y. Chen, J. Cheng, and J. Yu. Trueheart: Continuous authentication on wrist-worn wearables using ppg-based biometrics. In *IEEE Conference on Computer Communications (INFOCOM)*, pp. 30–39, Toronto, Canada, 2020. IEEE.

[41] Y. Sun and N. Thakor. Photoplethysmography revisited: from contact to noncontact, from point to imaging. *IEEE Transactions on Biomedical Engineering*, Vol. 63, No. 3, pp. 463–477, 2015.

[42] S. Venugopalan, F. Juefei-Xu, B. Cowley, and M. Savvides. Electromyograph and keystroke dynamics for spoof-resistant biometric authentication. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPR)*, pp. 109–118, Boston, USA, 2015. IEEE.

[43] S. Mahto, T. Arakawa, and T. Koshinak. Ear acoustic biometrics using inaudible signals and its application to continuous user authentication. In *2018 26th European Signal Processing Conference (EUSIPCO)*, pp. 1407–1411, Rome, Italy, 2018. IEEE.

[44] T Arakawa. Ear acoustic authentication technology: Using sound to identify the distinctive shape of the ear canal. *NEC Technical Journal Special Issue Social Value Creation Using Biometrics*, Vol. 13, No. 2, pp. 87–90, 2019.

[45] T. Inada, Y. Sodani, and I. Nakanishi. Intra-palm propagation signals as suitable biometrics for successive authentication. *Journal of Computer Technology and Application*, Vol. 7, No. 2, pp. 65–72, 2016.

[46] J. Hernandez-Ortega, J. Fierrez, E. Gonzalez-Sosa, and A. Morales. Continuous presentation attack detection in face biometrics based on heart rate. In *Video Analytics. Face and Facial Expression Recognition: Third International Workshop, FFER 2018, and Second International Workshop, DLPR 2018*, pp. 72–86, Beijing, China, 2018. Springer.

[47] Y. Shigeki, F. Okura, I. Mitsugami, K. Hayashi, and Y. Yagi. Directional characteristics evaluation of silhouette-based gait recognition. *IPSJ Transactions on Computer Vision and Applications*, Vol. 10, No. 1, p. 10, 2018.

[48] S. Mondal and P. Bours. A study on continuous authentication using a combination of keystroke and mouse biometrics. *Neurocomputing*, Vol. 230, pp. 1–22, 2017.

[49] K. Niinuma, U. Park, and A. K. Jain. Soft biometric traits for continuous user authentication. *IEEE Transactions on information forensics and security*, Vol. 5, No. 4, pp. 771–780, 2010.

[50] A. Rahman, V. M. Lubecke, O. Boric-Lubecke, J. H. Prins, and T. Sakamoto. Doppler radar techniques for accurate respiration characterization and subject identification. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, Vol. 8, No. 2, pp. 350–359, 2018.

[51] J. Chauhan, Y. Hu, S. Seneviratne, A. Misra, A. Seneviratne, and Y. Lee. Breathprint: Breathing acoustics-based user authentication. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys 2017)*, pp. 278–291, Niagara Falls, USA, 2017. ACM.

[52] S. Khan, S. Parkinson, L. Grant, N. Liu, and S. McGuire. Biometric systems utilising health data from wearable devices: Applications and future challenges in computer security. *ACM Computing Surveys (CSUR)*, Vol. 53, No. 4, pp. 1–29, 2020.

[53] Y. Y. Gu and Y. T. Zhang. Photoplethysmographic authentication through fuzzy logic. In *IEEE EMBS Asian-Pacific Conference on Biomedical Engineering, 2003.*, pp. 136–137, Kyoto, Japan, 2003. IEEE.

[54] A. Bonissi, R. D. Labati, L. Perico, R. Sassi, F. Scotti, and L. Sparagino. A preliminary study on continuous authentication methods for photoplethysmographic biometrics. In *2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BioMS)*, pp. 28–33, Napoli, Italy, 2013. IEEE.

[55] J. Sancho, Á. Alesanco, and J. García. Biometric authentication using the ppg: a long-term feasibility study. *Sensors*, Vol. 18, No. 5, p. 1525, 2018.

[56] R. M. Seepers, W. Wang, G. De Haan, I. Sourdis, and C. Strydis. Attacks on heartbeat-based security using remote photoplethysmography. *IEEE Journal of Biomedical and Health Informatics*, Vol. 22, No. 3, pp. 714–721, 2017.

[57] V. Jindal, J. Birjandtalab, M. B. Pouyan, and M. Nourani. An adaptive deep learning approach for ppg-based identification. In *2016 38th Annual*

International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 6401–6404, Orlando, USA, 2016. IEEE.

[58] A. Jain, L. Hong, and S. Pankanti. Biometric identification. *Communications of the ACM*, Vol. 43, No. 2, pp. 90–98, 2000.

[59] A. Hadid, N. Evans, S. Marcel, and J. Fierrez. Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. *IEEE Signal Processing Magazine*, Vol. 32, No. 5, pp. 20–30, 2015.

[60] N. K. Ratha, J. H. Connell, and R. M. Bolle. An analysis of minutiae matching strength. In *International Conference on Audio-and Video-Based Biometric Person Authentication*, pp. 223–228. Springer, 2001.

[61] Y. Ma, L. Wu, Z. Li, and F Liuc. A novel face presentation attack detection scheme based on multi-regional convolutional neural networks. *Pattern Recognition Letters*, Vol. 131, pp. 261–267, 2020.

[62] K. Cao and A. K. Jain. Hacking mobile phones using 2d printed fingerprints. *Michigan State University, Tech Report MSU-CSE-16-2*, 2016.

[63] A. Czajka and K. W. Bowyer. Presentation attack detection for iris recognition: An assessment of the state-of-the-art. *ACM Computing Surveys (CSUR)*, Vol. 51, No. 4, pp. 1–35, 2018.

[64] M. E. Ahmed, I.-Y. Kwak, J. H. Huh, I. Kim, T. Oh, and H. Kim. Void: A fast and light voice liveness detection system. In *the 29th USENIX Conference on Security Symposium*, pp. 2685–2702, Boston, USA, 2020. USENIX.

[65] Z. Wu, N. Evans, T. Kinnunen, J. Yamagishi, F. Alegre, and H. Li. Spoofing and countermeasures for speaker verification: A survey. *Speech Communication*, Vol. 66, pp. 130–153, 2015.

[66] D. Shukla, P. P. Kundu, R. Malapati, S. Poudel, Z. Jin, and V. V. Phoha. Thinking unveiled: An inference and correlation model to attack eeg biometrics. *Digital Threats: Research and Practice*, Vol. 1, No. 2, pp. 1–29, 2020.

[67] A. N. Schechter. Hemoglobin research and the origins of molecular medicine. *Blood, The Journal of the American Society of Hematology*, Vol. 112, No. 10, pp. 3927–3938, 2008.

[68] L. Pauling and C. D. Coryell. The magnetic properties and structure of hemoglobin, oxyhemoglobin and carbonmonoxyhemoglobin. *Proceedings of the National Academy of Sciences*, Vol. 22, No. 4, pp. 210–216, 1936.

[69] B. L. Horecker. The absorption spectra of hemoglobin and its derivatives in the visible and near infra-red regions. *Journal of Biological Chemistry*, Vol. 148, No. 1, pp. 173–183, 1943.

[70] I. Fine. The optical origin of the ppg signal. In *Saratov Fall Meeting 2013: Optical Technologies in Biophysics and Medicine XV; and Laser Physics and Photonics XV*, Vol. 9031, p. 903103. International Society for Optics and Photonics, 2014.

[71] R. Itoigawa, Y. Maeda, K. Mizutani, and N. Wakatsuki. Comparison of measurement sites in instantaneous orthostatic pulse rate measurement. *Advanced Biomedical Engineering*, Vol. 8, pp. 14–22, 2019.

[72] T. Tamura. Current progress of photoplethysmography and spo2 for health monitoring. *Biomedical Engineering Letters*, Vol. 9, No. 1, pp. 21–36, 2019.

[73] M. R. Ram, K. V. Madhav, E. H. Krishna, N. R. Komalla, and K. A. Reddy. A novel approach for motion artifact reduction in ppg signals based on as-lms adaptive filter. *IEEE Transactions on Instrumentation and Measurement*, Vol. 61, No. 5, pp. 1445–1457, 2011.

[74] G. Udovičić, J. Derek, M. Russo, and M. Sikora. Wearable emotion recognition system based on gsr and ppg signals. In *Proceedings of the 2nd International Workshop on Multimedia for Personal Health and Health Care*, pp. 53–59, New York, USA, 2017. ACM.

[75] A. Fujii, K. Murao, and N. Matsuhisa. disp2ppg: Pulse wave generation to ppg sensor using display. In *2021 International Symposium on Wearable Computers*, pp. 119–123, Virtual, Global, 2021. ACM.

[76] Y. Akimoto and K. Murao. Design and implementation of an input interface for wearable devices using pulse wave control by compressing the upper arm. In *Augmented Humans Conference 2021*, pp. 280–282, Online, 2021. ACM.

[77] N. Karimian, D. Woodard, and D. Forte. Ecg biometric: Spoofing and countermeasures. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, Vol. 2, No. 3, pp. 257–270, 2020.

[78] H. Jeong, H. Kim, R. Kim, U. Lee, and Y. Jeong. Smartwatch wearing behavior analysis: a longitudinal study. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, Vol. 1, No. 3, pp. 1–31, 2017.

[79] Q. Zhu, X. Tian, C.-W. Wong, and M. Wu. Ecg reconstruction via ppg: A pilot study. In *2019 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI)*, pp. 1–4. IEEE, 2019.

[80] A. Dash, N. Ghosh, A. Patra, and A. D. Choudhury. Estimation of arterial blood pressure waveform from photoplethysmogram signal using linear transfer function approach. In *2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*, pp. 2691–2694, Montreal, Canada, 2020. IEEE.

[81] V. Hartmann, H. Liu, F. Chen, Q. Qiu, S. Hughes, and D. Zheng. Quantitative comparison of photoplethysmographic waveform characteristics: effect of measurement site. *Frontiers in physiology*, Vol. 10, p. 198, 2019.

[82] T. Herzog and A. Uhl. Analysing a vein liveness detection scheme. In *2020 8th International Workshop on Biometrics and Forensics (IWBF)*, pp. 1–6, Porto, Portugal, 2020. IEEE.

[83] M. Smith-Creasey, F. A. Albalooshi, and M. Rajarajan. Continuous face authentication scheme for mobile devices with tracking and liveness detection. *Microprocessors and Microsystems*, Vol. 63, pp. 147–157, 2018.

[84] A. Garbuz, A. Epishkina, and K. Kogos. Continuous authentication of smartphone users via swipes and taps analysis. In *2019 European Intelli-*

gence and Security Informatics Conference (EISIC), pp. 48–53, Oulu, Finland, 2019. IEEE.

[85] J. Spooren, D. Preuveneers, and W. Joosen. Ppg 2 live: Using dual ppg for active authentication and liveness detection. In *2019 International Conference on Biometrics (ICB)*, pp. 1–6, Crete, Greece, 2019. IAPR.

[86] S. Makowski, P. Prasse, D. R. Reich, D. Krakowczyk, L. A. Jäger, and T. Scheffer. Deepeyedentificationlive: Oculomotoric biometric identification and presentation-attack detection using deep neural networks. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, Vol. 3, No. 4, pp. 506–518, 2021.

[87] A. Maijala, H. Kinnunen, H. Koskimäki, T. Jämsä, and M. Kangas. Nocturnal finger skin temperature in menstrual cycle tracking: ambulatory pilot study using a wearable oura ring. *BMC Women's Health*, Vol. 19, No. 1, pp. 1–10, 2019.

[88] Y. Maeda, M. Sekine, and T. Tamura. The advantages of wearable green reflected photoplethysmography. *Journal of Medical Systems*, Vol. 35, No. 5, pp. 829–834, 2011.

[89] Y. Maeda, M. Sekine, and T. Tamura. Relationship between measurement site and motion artifacts in wearable reflected photoplethysmography. *Journal of Medical Systems*, Vol. 35, No. 5, pp. 969–976, 2011.

[90] E. Shchelkanova, L. Shchapova, A. Shchelkanov, and T. Shibata. Blue as an underrated alternative to green: Photoplethysmographic heartbeat intervals estimation under two temperature conditions. *Sensors*, Vol. 21, No. 12, p. 4241, 2021.

[91] J. Lee, K. Matsumura, K. Yamakoshi, P. Rolfe, S. Tanaka, and T. Yamakoshi. Comparison between red, green and blue light reflection photoplethysmography for heart rate monitoring during motion. In *2013 35th annual international conference of the IEEE engineering in medicine and biology society (EMBC)*, pp. 1724–1727, Osaka, Japan, 2013. IEEE.

[92] M. M. Mukaka. A guide to appropriate use of correlation coefficient in medical research. *Malawi Medical Journal*, Vol. 24, No. 3, pp. 69–71, 2012.

[93] Y. Y. Gu, Y. Zhang, and Y. T. Zhang. A novel biometric approach in human verification by photoplethysmographic signals. In *4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine*, pp. 13–14, Birmingham, UK, 2003. IEEE.

[94] A. I. Siam, A. Abou Elazm, N. A. El-Bahnasawy, G. M. El Banby, and F. E. Abd El-Samie. Ppg-based human identification using mel-frequency cepstral coefficients and neural networks. *Multimedia Tools and Applications*, Vol. 80, pp. 1–19, 2021.

[95] D. J. Berndt and J. Clifford. Using dynamic time warping to find patterns in time series. In *Workshop on Knowledge Discovery in Databases (KDD)*, pp. 359–370, Seattle, USA, 1994. AAAI.

[96] J. P. Huelsenbeck. Tree-length distribution skewness: an indicator of phylogenetic information. *Systematic Biology*, Vol. 40, No. 3, pp. 257–270, 1991.

[97] R. D. De Roo, S. Misra, and C. S. Ruf. Sensitivity of the kurtosis statistic as a detector of pulsed sinusoidal rfi. *IEEE Transactions on Geoscience and Remote Sensing*, Vol. 45, No. 7, pp. 1938–1946, 2007.

[98] S. Molau, M. Pitz, R. Schluter, and H. Ney. Computing mel-frequency cepstral coefficients on the power spectrum. In *International Conference on Acoustics, Speech, and Signal Processing. Proceedings*, Vol. 1, pp. 73–76, Salt Lake City, USA, 2001. IEEE.

[99] S. R. Moosavi. Ppg-keygen: Using photoplethysmogram for key generation in wearable devices. *Procedia Computer Science*, Vol. 184, pp. 291–298, 2021.

[100] P. Podder, T. Z. Khan, M. H. Khan, and M. M. Rahman. Comparative performance analysis of hamming, hanning and blackman window. *International Journal of Computer Applications*, Vol. 96, No. 18, 2014.

[101] B. Logan. Mel frequency cepstral coefficients for music modeling. In *International Symposium on Music Information Retrieval*, Vol. 270, pp. 1–11, Plymouth, USA, 2000. ISMIR.

[102] T. Gulzar, A. Singh, and S. Sharma. Comparative analysis of lpcc, mfcc and bfcc for the recognition of hindi words using artificial neural networks. *International Journal of Computer Applications*, Vol. 101, No. 12, pp. 22–27, 2014.

[103] S. K. Kopparapu and M. Laxminarayana. Choice of mel filter bank in computing mfcc of a resampled speech. In *10th International Conference on Information Science, Signal Processing and their Applications (ISSPA 2010)*, pp. 121–124, Kuala Lumpur, Malaysia, 2010. IEEE.

[104] N. Ahmed, T. Natarajan, and K. R. Rao. Discrete cosine transform. *IEEE Transactions on Computers*, Vol. 100, No. 1, pp. 90–93, 1974.

[105] M. Ghamari, C. Soltanpur, S. Cabrera, R. Romero, R. Martinek, and H. Nazeran. Design and prototyping of a wristband-type wireless photoplethysmographic device for heart rate variability signal analysis. In *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pp. 4967–4970, Orlando, USA, 2016. IEEE.

[106] A. R. Kavsaoğlu, K. Polat, and M. Hariharan. Non-invasive prediction of hemoglobin level using machine learning techniques with the ppg signal's characteristics features. *Applied Soft Computing*, Vol. 37, pp. 983–991, 2015.

[107] M. H. M. Rasid, N. L. Simon, and A. Adam. Using neural network with random weights and mutual information for systolic peaks classification of ppg signals. In *Proceedings of the 2020 10th International Conference on Biomedical Engineering and Technology*, pp. 276–283, Tokyo, Japan, 2020. ACM.

[108] A. Riera, A. Soria-Frisch, M. Caparrini, C. Grau, and G. Ruffini. Unobtrusive biometric system based on electroencephalogram analysis. *EURASIP Journal on Advances in Signal Processing*, Vol. 2008, No. 1, p. 143728, 2007.

[109] J. Malik, D. Girdhar, R. Dahiya, and G. Sainarayanan. Reference threshold calculation for biometric authentication. *IJ Image, Graphics and Signal Processing*, Vol. 2, pp. 46–53, 2014.

[110] S. I. Gallant. Perceptron-based learning algorithms. *IEEE Transactions on neural networks*, Vol. 1, No. 2, pp. 179–191, 1990.

[111] M. Liu, M. Wang, J. Wang, and D. Li. Comparison of random forest, support vector machine and back propagation neural network for electronic tongue data classification: Application to the recognition of orange beverage and chinese vinegar. *Sensors and Actuators B: Chemical*, Vol. 177, pp. 970–980, 2013.

[112] J. A. K. Suykens and J. Vandewalle. Least squares support vector machine classifiers. *Neural processing letters*, Vol. 9, No. 3, pp. 293–300, 1999.

[113] J. Ye and T. Xiong. Svm versus least squares svm. In *Proceedings of the Eleventh International Conference on Artificial Intelligence and Statistics*, pp. 644–651, San Juan, Puerto Rico, 2007. PMLR.

[114] T. Kurita. Support vector machine and generalization. *Journal of Advanced Computational Intelligence and Intelligent Informatics*, Vol. 8, No. 2, 2004.

[115] E. Scornet. Tuning parameters in random forests. *ESAIM: Proceedings and Surveys*, Vol. 60, pp. 144–162, 2017.

[116] Y. Y. Song and L. Ying. Decision tree methods: applications for classification and prediction. *Shanghai Archives of Psychiatry*, Vol. 27, No. 2, p. 130, 2015.

[117] G. Biau and E. Scornet. A random forest guided tour. *Test*, Vol. 25, No. 2, pp. 197–227, 2016.

[118] N. García-Pedrajas, J. A. R. Del Castillo, and G. Cerruela-García. A proposal for local k values for k-nearest neighbor rule. *IEEE Transactions on Neural Networks and Learning Systems*, Vol. 28, No. 2, pp. 470–475, 2015.

[119] K. Chomboon, P. Chujai, P. Teerarassamee, K. Kerdprasop, and N. Kerdprasop. An empirical study of distance metrics for k-nearest neighbor algorithm. In *Proceedings of the 3rd International Conference on Industrial Application Engineering*, pp. 280–285, Kitakyushu, Japan, 2015.

[120] G. Lovisotto, H. Turner, S. Eberz, and I. Martinovic. Seeing red: Ppg biometrics using smartphone cameras. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, pp. 818–819, Seattle, USA, 2020.

[121] A. Nakagawa, J. Kim, and K. Nakajima. Personal identification using a ballistocardiogram during urination obtained from a toilet seat. *Advanced Biomedical Engineering*, Vol. 9, pp. 233–240, 2020.

[122] Y. Ye, G. Xiong, Z. Wan, T. Pan, and Z. Huang. Ppg-based biometric identification: Discovering and identifying a new user. In *2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*, pp. 1149–1152. IEEE, 2021.

[123] G. Zhang, M. Wang, and K. Liu. Deep neural networks for global wildfire susceptibility modelling. *Ecological Indicators*, Vol. 127, p. 107735, 2021.

[124] A. R. Kavsaoğlu, K. Polat, and M. R. Bozkurt. A novel feature ranking algorithm for biometric recognition with ppg signals. *Computers in Biology and Medicine*, Vol. 49, pp. 1–14, 2014.

[125] O. R. Patil, W. Wang, Y. Gao, W. Xu, and Z. Jin. A non-contact ppg biometric system based on deep neural network. In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–7, Redondo Beach, USA, 2018. IEEE.

[126] R. C. Chen, C. Dewi, S. W. Huang, and R. E. Caraka. Selecting critical features for data classification based on machine learning methods. *Journal of Big Data*, Vol. 7, No. 1, p. 52, 2020.

[127] K. S. Kim, H. H. Choi, C. S. Moon, and C. W. Mun. Comparison of k-nearest neighbor, quadratic discriminant and linear discriminant analysis

in classification of electromyogram signals based on the wrist-motion directions. *Current Applied Physics*, Vol. 11, No. 3, pp. 740–745, 2011.

[128] Y. Ma, R. Huang, M. Yan, G. Li, and T. Wang. Attention-based local mean k-nearest centroid neighbor classifier. *Expert Systems with Applications*, Vol. 201, p. 117159, 2022.

[129] D. Biswas, L. Everson, M. Liu, M. Panwar, B. E. Verhoef, S. Patki, C. H. Kim, A. Acharyya, C. Van Hoof, M. Konijnenburg, and N. Van Helleputte. Cornet: Deep learning framework for ppg-based heart rate estimation and biometric identification in ambulant environment. *IEEE Transactions on Biomedical Circuits and Systems*, Vol. 13, No. 2, pp. 282–291, 2019.

[130] W. K. Beh, Y. H. Wu, and A. Y. A. Wu. Maus: A dataset for mental workload assessment on n-back task using wearable sensor. https://ieee-dataport.org/open-access/maus-dataset-mental-workload-assessment-n-back-task-using-wearable-sensor, 2021. accessed on October 30, 2022.

[131] W. K. Beh, Y. H. Wu, and A. Y. Wu. Maus: A dataset for mental workload assessment on n-back task using wearable sensor. *arXiv preprint arXiv:2111.02561*, 2021.

[132] T. Aydemir, M. Şahin, and O. Aydemir. Sequential forward mother wavelet selection method for mental workload assessment on n-back task using photoplethysmography signals. *Infrared Physics & Technology*, Vol. 119, p. 103966, 2021.

[133] Thought Technology Ltd. Procomp infiniti hardware manual. https://biomedical.com/media/support/sa7510.pdf. accessed on December 24, 2022.

[134] W. K. Beh, Y. H. Wu, and A. Y. A. Wu. Robust ppg-based mental workload assessment system using wearable devices. *IEEE Journal of Biomedical and Health Informatics*, 2021.

[135] A. Kianimajd, M. G. Ruano, P. Carvalho, J. Henriques, T. Rocha, S. Paredes, and A. E. Ruano. Comparison of different methods of measuring sim-

ilarity in physiologic time series. *IFAC-PapersOnLine*, Vol. 50, No. 1, pp. 11005–11010, 2017.

[136] J. Huang and C. X. Ling. Using auc and accuracy in evaluating learning algorithms. *IEEE Transactions on Knowledge and Data Engineering*, Vol. 17, No. 3, pp. 299–310, 2005.

[137] W. Zhu, N. Zeng, and N. Wang. Sensitivity, specificity, accuracy, associated confidence interval and roc analysis with practical sas implementations. *NESUG Proceedings: Health Care and Life Sciences, Baltimore, Maryland*, Vol. 19, p. 67, 2010.

[138] M. Pal and G. Saha. On robustness of speech based biometric systems against voice conversion attack. *Applied Soft Computing*, Vol. 30, pp. 214–228, 2015.

[139] J. Xu, G. Yang, K. Wang, Y. Huang, H. Liu, and Y. Yin. Structural sparse representation with class-specific dictionary for ecg biometric recognition. *Pattern Recognition Letters*, Vol. 135, pp. 44–49, 2020.

[140] Y. H. Chen, D. Y. Wu, T. H. Wu, and H. Y. Lee. Again-vc: A one-shot voice conversion using activation guidance and adaptive instance normalization. In *2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 5954–5958. IEEE, 2021.

[141] L. Li, C. Chen, L. Pan, J. Zhang, and Y. Xiang. Video is all you need: Attacking ppg-based biometric authentication. In *Proceedings of the 15th ACM Workshop on Artificial Intelligence and Security*, AISec'22, p. 57–66, New York, USA, 2022. ACM.

[142] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K. K. R. Choo. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 9, pp. 9390–9401, 2020.

研究業績

- 関連論文

  1. S. Hinatsu, N. Matsuda, H. Ishizuka, S. Ikeda, and O. Oshiro. Identification of PPG Measurement Sites Toward Countermeasures Against Biometric Presentation Attacks. IEEE Access, Vol. 10, pp. 118736-118746, 2022.
  2. S. Hinatsu, D. Suzuki, H. Ishizuka, S. Ikeda, and O. Oshiro. Evaluation of PPG Feature Values Toward Biometric Authentication Against Presentation Attacks. IEEE Access, Vol. 10, pp. 41352-41361, 2022.
  3. S. Hinatsu, D. Suzuki, H. Ishizuka, S. Ikeda, and O. Oshiro. Basic Study on Presentation Attacks against Biometric Authentication using Photoplethysmogram. Advanced Biomedical Engineering, Vol. 10, pp. 101-112, 2021.

- 参考論文

  1. S. Yoshimoto, S. Hinatsu, Y. Kuroda, and O. Oshiro. Hemodynamic Sensing of 3-D Fingertip Force by using Non-pulsatile and Pulsatile Signals in the Proximal Part. IEEE Transactions on Biomedical Circuits and Systems, Vol. 12, No. 5, pp. 1155-1164, 2018.
  2. 日夏 俊, 吉元 俊輔, 黒田 嘉宏, 大城 理. 基節部における脈波計測を利用した指先接触力推定. 生体医工学, Vol. 55, No. 3, pp. 115-124, 2017.

- 国際会議

1. S. Hinatsu, D. Suzuki, H. Ishizuka, S. Ikeda, and O. Oshiro. Attack on PPG Biometrics: Presentation Attack by Stealth Recording and Waveform Estimation. 43rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC2021), pp. 64-67, Guadalajara, November 2021.
2. S. Hinatsu, D. Suzuki, H. Ishizuka, S. Ikeda, and O. Oshiro. Photoplethysmographic Subject Identification by Considering Feature Values Derived from Heartbeat and Respiration. 42nd Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC2020), pp. 902-905, Montreal, July 2020.
3. S. Hinatsu, K. Shimizu, T. Ueda, B. Boyer, and D. Mentré. Automatic Vulnerability Identification and Security Installation with Type Checking for Source Code. The 22nd International Conference on Network-Based Information Systems (NBiS2019), pp. 292-304, Oita, September 2019.
4. S. Yoshimoto, S. Hinatsu, Y. Kuroda, and O. Oshiro. Hemodynamic Sensing of 3D Fingertip Force using PPG device on Proximal Part. 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC2017), pp. 3289-3292, Jeju, July 2017.

- 国内発表

1. 日夏 俊, 鈴木 大輔, 石塚 裕己, 池田 聖, 大城 理. 脈波を利用した認証における情報漏洩となりすましに対する安全性評価. 第 61 回日本生体医工学会大会, O1-5-1-3, 新潟, 2022 年 6 月.
2. 日夏 俊, 鈴木 大輔, 石塚 裕己, 池田 聖, 大城 理. 光電容積脈波を利用した認証に対するなりすまし攻撃への対策検討. 第 60 回日本生体医工学会大会, O1-4-2-9, p. 29，オンライン, 2021 年 6 月.
3. 日夏 俊, 鈴木 大輔, 石塚 裕己, 池田 聖, 大城 理. 脈波を利用した認証に対するなりすまし攻撃の検証. SCIS2021 暗号と情報セキュリティシンポジウム, 3F3-3，オンライン, 2021 年 1 月.
4. 日夏 俊, 鈴木 大輔, 石塚 裕己, 池田 聖, 大城 理. 光電容積脈波を利用した生体認証に対するなりすまし攻撃手法の提案. 生体医工学シンポジウム 2020, 1A-10，弘前, 2020 年 9 月.
5. 植田 武, 清水 孝一, 日夏 俊, 大松 史生. 設計モデルを用いた情報資産セキュリティ特性の推測手法. 第 36 回セキュリティ心理学とトラスト研究発表会，那覇, 2020 年 3 月.
6. 日夏 俊, 鈴木 大輔, 石塚 裕己, 池田 聖, 大城 理. 光電容積脈波中の呼吸成分を利用した個人識別手法. SCIS2020 暗号と情報セキュリティシンポジウム, 1E2-2，高知, 2020 年 1 月.
7. 植田 武, 清水 孝一, 日夏 俊, 小林 信博. 脅威分析と S/W モデルの関連性を用いた脆弱性分析. SCIS2019 暗号と情報セキュリティシンポジウム, 2F3-4, 大津, 2019 年 1 月.
8. 日夏 俊, 清水 孝一, 植田 武, 市川 幸宏, 中井 綱人, 小林 信博. 情報資産価値を考慮したセキュリティ機能適切配置手法. SCIS2019 暗号と情報セキュリティシンポジウム, 3E1-1, 大津, 2019 年 1 月.
9. 市川 幸宏, 中井 綱人, 清水 孝一, 植田 武, 日夏 俊, 小林 信博. 脅威分析による対策を標準要件で分類するセキュリティ機能分類方式の提案. SCIS2018 暗号と情報セキュリティシンポジウム, 1C1-2, 新潟, 2018 年 1 月.
10. 清水 孝一, 植田 武, 市川 幸宏, 中井 綱人, 日夏 俊, 小林 信博, ブノワ・ボワイエ, ダヴィド・モントレ. ステートマシンで表した動作モデル

を用いた脆弱性の特定. SCIS2018 暗号と情報セキュリティシンポジウム, 1C1-3, 新潟, 2018 年 1 月.

11. 植田 武, 清水 孝一, 日夏 俊, 中井 綱人, 市川 幸宏, 浅井 健志, 小林 信博. 設計モデルを用いたセキュリティ脆弱性分析方法. SCIS2018 暗号と情報セキュリティシンポジウム, 1C1-4, 新潟, 2018 年 1 月.
12. 日夏 俊, 清水 孝一, 植田 武, 市川 幸宏, 中井 綱人, 小林 信博. モデルベース開発技術を利用したセキュリティ機能導入パターン生成. SCIS2018 暗号と情報セキュリティシンポジウム, 1C1-5, 新潟, 2018 年 1 月.
13. 日夏 俊, 吉元 俊輔, 黒田 嘉宏, 大城 理. 指先接触力の推定性能向上のための高相関な脈波特徴量の検討. 第 21 回パターン計測シンポジウム, 徳島, 2016 年 11 月.
14. 日夏 俊, 吉元 俊輔, 黒田 嘉宏, 大城 理. 基節部における脈波計測を利用した指先接触力推定. 生体医工学シンポジウム 2016, p. 96, 旭川, 2016 年 9 月.
15. 日夏 俊, 吉元 俊輔, 黒田 嘉宏, 大城 理. 光電容積脈波計測による指先押下力推定手法の基礎検討. 計測自動制御学会関西支部・システム制御情報学会若手研究発表会, pp. 140-145, 吹田, 2016 年 1 月.

- 受賞

1. 日夏 俊. 海外研修奨励賞. 2017 年 1 月.
2. 日夏 俊. BioEngineering Colloquium 優秀発表賞. 2016 年 7 月.
3. 日夏 俊. 基礎工学部賞. 2015 年 3 月.

- 特許

1. 日夏 俊. 認証装置、認証方法及び認証プログラム. 特願 2021-526815.
2. 日夏 俊, 鈴木 大輔. 生体認証装置、生体認証方法、および、生体認証プログラム. 特願 2020-537028.
3. 日夏 俊, 清水 孝一, 植田 武. セキュリティ設計装置、セキュリティ設計方法およびセキュリティ設計プログラム. 特願 2019-538449.
4. 植田 武, 清水 孝一, 日夏 俊, 丹治 雅道. 情報処理装置、情報処理方法及び情報処理プログラム. 特願 2019-520661.
5. 清水 孝一, 植田 武 , 日夏 俊. 情報処理装置、情報処理方法及び情報処理プログラム. JP2019025382.

- その他

1. Shun Hinatsu. Security Assessment for Blood Flow-based Biometric Authentication and Identity Spoofing. BioEngineering Colloquium 2022, 豊中, 2022 年 7 月.
2. Shun Hinatsu. Biometric Authentication Using Blood Flow: Spoofing and Countermeasure. BioEngineering Colloquium 2021, オンライン, 2021 年 7 月.
3. Shun Hinatsu. Biometric Authentication Utilizing Multiple Factors in Blood Flow Change. BioEngineering Colloquium 2020, オンライン, 2020 年 7 月.
4. 日夏 俊. 指輪型脈波計測デバイスによる手指動作推定. 河原研-大城研合同セミナー, 豊中, 2016 年 7 月.
5. 日夏 俊. 血流変化を利用した指接触力センシング. BioEngineering Colloquium 2016, 豊中, 2016 年 7 月 (**BioEngineering Colloquium 優秀発表賞**).
6. 日夏 俊. ワクワク留学体験記 University of Oulu. 日本バーチャルリアリティ学会誌, Vol. 21, No. 1, pp. 66-67, 2016 年 3 月.

- 研究助成等

1. 大阪大学 未来基金 平成 27 年度 第 3 回 研究留学助成金. 2015 年 10 月.