替え玉による測定を防止する血圧測定システムの設計と実装

高橋元[1] 鈴木晴佳[1] 藤村香央里[1] 中村亨[1] 早川和宏[1]

概要： IoT 時代を迎え，個人が自ら健康データを測定し，健康管理を行うサービスが普及している．また，保険契約者が健康データを測定し，保険会社など第三者が測定したデータを活用して保険契約者へ利益を還元するサービスが始まっている．第三者のデータ活用においては，データを測定した個人自身による替え玉やねつ造のリスクがある．個人の健康データを第三者が活用するためには，替え玉により測定されたものでないことを保証することが重要である．本研究では，血圧測定時に，指静脈認証デバイスと血圧計とから同時に脈波を取得し，取得した 2 つの脈波の特徴を照合することで，被認証ユーザとカフを巻いて血圧を測定した人が同一人物であることを確認する．本稿では，既存血圧計に比べユーザビリティを損なわず，本人を確認できる血圧測定システムの設計・実装について示す．また，安価な装置構成でのハードウェアに対する攻撃への対策の実現に着目し，新たな脈波センサを実装せず，１つのセンサのデータから血圧値と脈波を取得するワンソースマルチユースによる血圧測定装置の設計・実装を行った．実装と評価では，実装した血圧測定システムにより脈波の同一人物性の確認を行うために必要な測定毎に異なる脈波の揺らぎが取得できることを確認し，他人受入率/本人拒否率について示す．

The design and implementation of blood pressure monitor system preventing of unauthorized data registered by imposters

GEN TAKAHASHI[1] HARUKA SUZUKI[1] FUJIMURA KAORI[1]
TORU NAKAMURA[1] KAZUHIRO HAYAKAWA[1]

1. はじめに

IoT 時代を迎え，個人が健康データを測定し，健康管理を行うクラウドサービスが普及している．また，自分自身の健康管理だけではなく，例えば，保険会社など第三者が個人で測定したデータを活用し，保険契約者へ利益還元するサービス[1]が始まっている．

第三者のデータ活用では，サービス利用者による替え玉やねつ造のリスクがある．個人の健康データを第三者が活用するためには，替え玉により測定されたものでないことを保証することが重要である．本稿では，替え玉測定を防止する血圧測定システムの設計と実装について示す．

2. 従来技術

パスワード認証や生体認証など従来の認証技術では，正しいユーザの持つ知識や物，生体としての特徴量が検証されるが，認証行為と同時もしくは引き続き行われる測定などの行為の主体が誰であるかまで特定できない．このため，認証されたユーザと測定された人が同一人物であること確認する方法がなかった．

3. 血圧測定システムの要件

本研究では，生体認証による被認証者と血圧測定の被測定者との同一人物性を確認することで替え玉による血圧測定を防止する．本節では，替え玉による測定を防止する血圧測定システム設計・実装の要件について述べる．

- 認証と測定の関連付け機能

血圧測定では，生体認証を行ったとしても，認証と測定が関連づけられていないため，測定の対象が誰であるか特定できない．このため，本研究では，血圧測定のようなどの誰に対して行った行為かシステムで直接認証できない事象を，本人認証と関連付ける．関連付けは，図１に示すようにユニファイアと呼ぶ情報を用いて行う．

ユニファイアは，測定毎に異なる特徴量を持つ必要がある．認証や血圧測定時に取得でき，測定毎に異なる特徴量を持つユニファイアとして，脈波を利用できる．本研究では，血圧測定時に，指静脈認証デバイスと血圧計とから同時に脈波を取得する[2]．取得した２つの脈波を照合することで，カフを巻いて血圧を測定した人と被認証ユーザとが同一人物であることを確認する．このため，カフを巻いたユーザと認証デバイスにより認証されたユーザの脈波を取得する機能を必要とする．また，健康な人の場合，脈波の周期は一定ではなく，ランダムな揺らぎが観測される．周期のランダムな揺らぎを特徴量として，同時に取得した２つの脈波の照合を行うため，周期の揺らぎをシステムで検出できる必要がある．

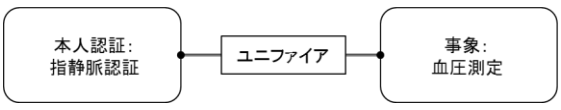

図 1 ユニファイアによる事象と認証の関連付け

1 NTT セキュアプラットフォーム研究所

● 攻撃への耐性

本研究では，指静脈認証デバイスと血圧計とから同時に脈波を取得し，取得した２つの脈波を照合することで認証されたユーザと測定された人が同一人物であること保証する．このため，血圧値を測定したユーザから取得された脈波であることをシステムで保証する必要がある．また，認証されたユーザから取得された脈波であることをシステムで保証する必要がある．これに対し，ハードウェアへの攻撃やソフトウェアへの攻撃、論理的攻撃により不正な脈波を血圧計や認証デバイスへ入力する攻撃が考えられる[3].

1. ハードウェアへの攻撃

血圧計や認証デバイスに備わる脈波センサを物理的に分離し本来取得対象ではない不正なユーザの脈波を取得する

2. ソフトウェアへの攻撃

ソフトウェアの脆弱性を攻撃し，常に２つの脈波の照合が成功するコードに書き換える

3. 論理的攻撃

中間者攻撃など血圧計や認証デバイス間の通信路の設計ミス等の脆弱性を利用し，入力される脈波データを改ざんする

ソフトウェアへの攻撃やプロトコルの設計ミス等を利用した論理的攻撃については，セキュアプログラミングや暗号技術による対策が多く研究されている．ハードウェアへの攻撃に対しては，分解が困難なネジや分解されたことが分かる封印，メッシュセンサでチップを覆うなどの対策がある．家庭血圧を想定し，コンシューマ機器への実装が容易となるよう安価な装置構成でのハードウェアに対する攻撃への対策の実現に着目する。

● ユーザビリティ

家庭血圧は，正確性や安全性，効率性が重視される医療従事者等のエキスパートではなく操作の分り易さが求められる一般ユーザによる利用が想定される．このため，血圧計の操作のためのインタフェースや血圧測定に要する時間が従来の血圧計と同等である必要である．

4. 設計

4.1 システムアーキテクチャ

本システムのアーキテクチャを図 2 に示す．血圧測定時に，認証装置で認証を行った後，血圧測定中は，認証装置及び血圧測定装置から同時に脈波を取得する．アプリケーションで同時に取得した脈波を照合[4]し，認証と血圧測定との同一人物性を確認する．

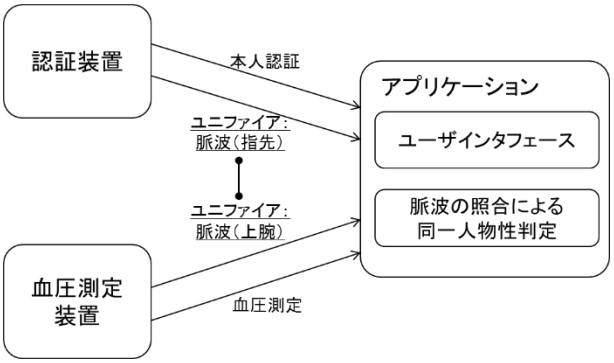

図 2 アーキテクチャ

4.2 血圧測定装置

血圧測定装置では，血圧の被測定者と同一人物から脈波を取得することを保証する必要がある．また，この同一人物性の保証に対して，既存の血圧装置と同程度の安価な装置構成での対策を目指す。さらに，血圧測定装置は，従来の血圧計の操作性を損なわない装置設計とするため，血圧計の操作のためのインタフェースとして加圧開始/停止ボタンを設け，血圧測定時間も既存の血圧計と同等の 25 秒とする．

血圧値を測定したユーザと脈波を取得したユーザが同一人物であることを保証するため，１つのセンサのデータから血圧値と脈波を取得するワンソースマルチユースによる血圧計測定システムの設計とした．図 3 に示すように，測定したい測定値である血圧値とユニファイアである脈波を１つのセンサモジュールから取得する．

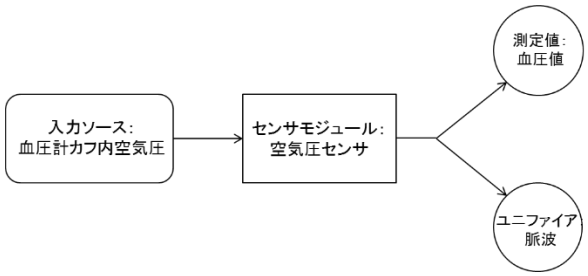

図 3 ワンソースマルチユースによる測定値とユニファイアの取得

本システムでカフを不正なユーザが装着した状態で血圧計に本人の脈波を入力しようとする場合，センサを分解するだけでは不十分でセンサの出力やマイコンファームウェアの改ざんが必要となる．

4.3 認証装置

認証装置は，被認証者と同一人物から脈波を取得することを保証する必要がある．図 4 のように新たに脈波センサを指静脈認証デバイスに追加し，認証中に被認証者の脈波を取れる設計とした．さらに，同時に１本の指しか挿入できない閉じられた筐体構造とすることで，不正なユーザの脈波を入力できない筐体設計とした．また，指離れを検知することで，認証中にのみ脈波を取れる設計とした．

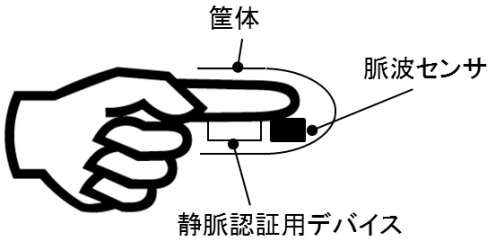

図 4 認証装置の設計

5. 実装と評価

5.1 実装

実装した血圧測定システムについて図 5 に示す．脈波を取得できる血圧計と指静脈認証デバイスおよび，血圧値の表示や脈波の照合を行う PC で構成される．血圧計及び指静脈認証デバイスは，USB により PC に接続される．

- PC

Intel(R) CoreTM M -5Y71 vPro(TM) プロセッサ 1.20GHz，メモリ 8G, OS:Windows 8.1 pro 上で，認証，血圧計及び認証デバイスからの脈波取得，血圧値の計算と測定結果の表示を行うアプリケーションの実装を行った．

- 血圧測定装置

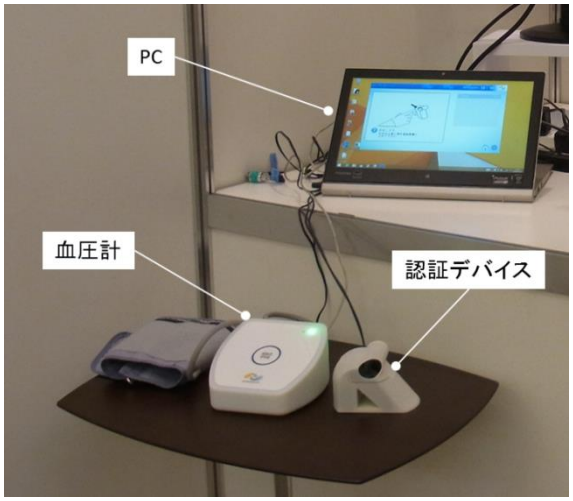

図 6　血圧測定システム

H8 ファミリマイコン[5]を用いて，血圧測定に必要なカフの加圧減圧制御，カフ内の空気圧を検出するセンサのデータ取得と PC へのデータ送信を実装した．一般的に心電図は，1ms から 8ms の分解能で測定される[9]. このため，空気圧センサは，5.12msec でのサンプリングが可能な MITSUMI MMR901XA[6]を用いた．脈波を取得する専用のセンサは配置せず，空気圧センサから取得した圧力データを PC に送信し，PC で脈波及び血圧値を算出する．

- 認証装置

認証装置は，指静脈認証デバイスに mofiria 社 FVA-U3SX[7]を用い，脈波取得センサに東京デバイセズ社 IW9PLS[8]を用いて，図 5 に示すようにこれらを 1 つの筐体に収めることで同時に 1 本の指しか挿入できない閉じられた筐体を実装した．

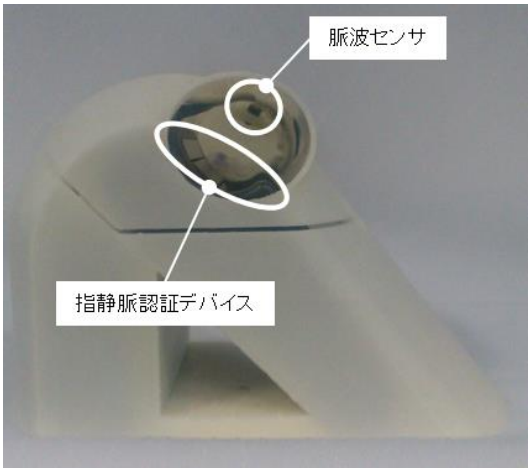

図 5 認証装置

5.2 評価

脈波取得方法は，皮膚の圧力から求めるもの，皮膚にあてた光電センサの光源の反射／透過量から求めるものなど様々なものがある．血圧計において，血圧値を取得するセンサとユニファイアを取得するセンサが異なる場合，装置を分解するなどで，不正なユーザの血圧値をユニファイアと関連づけることが容易であるため，耐タンパ技術により対策が必要となる．

本設計・実装のように，1 つの圧力センサから血圧値及び脈波を算出することで，不正な脈波をシステムに入力するためには，センサの出力やマイコンファームウェアの改ざんが必要となり，低いコストでの血圧測定装置への本人の脈波の不正な入力が困難となる．また，カフ内の空気圧から脈波を取得するため，ユーザは被服の上から脈波を測定でき，従来の市販血圧計の操作性を保てる．

次に，実装した血圧測定システムでの脈波の揺らぎについて示す．被験者に本システムを用いて，血圧測定を行ってもらい，カフの減圧中の脈波の揺らぎを抽出し，図 7 に，ポアンカレプロットとして表現した．ポアンカレプロットとは，ある時刻のピークの間隔を横軸にとり，次に続くピークの間隔を縦軸にとってプロットしたもので，心拍の揺らぎが大きいほどプロットが分散する．心拍の揺らぎは人により数百ミリ秒の範囲で揺らいでいる[9]. 図 8 の被験者は，脈波の揺らぎが少ない．本研究では，測定毎に異なる脈波の揺らぎを用いて，被認証者と被測定者との同一人物性の確認を行う．図 7 及び図 8 のポアンカレプロットに示すように，本実装では，同一人物性の確認を行うために必要な測定毎に異なる脈波の揺らぎが取得できた．

また，脈波照合の他人受け入れ率及び本人拒否率は，20 代～50 代の被験者 18 名による評価では，他人を本人であ

ると誤判定する他人受入率(FAR)は 2.78%, 本人を他人であると誤判定する本人拒否率(FRR)は 8.33% [4]となった．NIST の評価[11]では，2000 年当初の顔認証における FAR と FRR は，それぞれ 1%と 10%であり，音声認証は，それぞれ 2%と 10%である．方式では，初期の顔認証や音声認証と同程度の FAR/FRR を実現できている．

6. まとめと今後の課題

本稿では，替え玉測定を防止する血圧測定システムの設計，実装および評価について示した．本研究では，血圧測定時に，指静脈認証デバイスと血圧計とから同時に脈波を取得し，取得した 2 つの脈波を照合する．これにより，被認証ユーザとカフを巻いて血圧を測定した人が同一人物であることを確認できる．

今後，IoT デバイスなどを活用し個人が生成するデータは爆発的に増加することが予想される．これらクラウドに蓄積される個人の真正性を確保するため，ユニファイアを用いた真正性保証方式を血圧値以外の新たな領域へ広げ，データの第三者活用を促進することを目指す．

例えば，近年，インターネット環境があれば世界どこからでも，誰でも無料で利用できる大規模公開オンライン講座（Massive Open Online Course: MOOC）[10]が注目されている．受講者の回答の本人性の信頼が不十分であるため，e-learning 受講者の情報を雇用者に販売するなどのマネタイジングが課題[10]となっている．MOOC における試験の回答の本人性の保証することで，受講者情報を雇用者へ販売するなど新たなサービスの実現につながる．

MOOC に関する近年の研究[12]では，認証に加え，IoT デバイスを用いて脳波や視線トラッキングなどを用いて，オンラインでの不正受験を検知する研究されている．これら IoT デバイスを用いたシステムにおいても血圧測定と同様に認証と IoT デバイスによる被測定者の同一人物性の実現が重要となる．こういった IoT を活用したシステムにおいて，ユニファイアとして何が活用できるか検討を行うことが課題である．

参考文献

[1] Liam Boogar: Reduce your Health Insurance bill by tracking steps with wearables (online), available from 〈http://www.rudebaguette.com/2014/06/02/reduce-health-insurance-bill-tracking-steps-wearables/〉 (accessed 2016-04-28).

[2] 中村 亨，高橋 誠治，藤村 香央里，森村 一雄，前田 裕二：医療・健康データの真正性担保についての基礎検討，第 19 回日本医療情報学会春季学術大会，Vol. 19，No.19, pp.142-143（2015）

[3] 松本 勉, 大石 和臣, 高橋 芳夫: 実装攻撃に対抗する耐タンパー技術の動向,情報処理, Vol.49,No.7, pp 799 – 809(オンライン), 入手先< https://ipsj.ixsq.nii.ac.jp/ej/>(2008)

[4] 鈴木晴佳，高橋 元，藤村 香央里，中村 亨，早川和宏：個人が生成するデータの帰属性保証についての検討， 2016 年電子情報通信学会総合大会プログラム・抄録集, VolXX,No.XXpp.zz-zz, Mar. (2016).

[5] ルネサス エレクトロニクス株式会社：H8 マイコン，ルネサス エレクトロニクス株式会社（オンライン），入手先〈http://japan.renesas.com/products/mpumcu/h8/index.jsp〉（参照 2016-04-28）.

[6] ミツミ電機株式会社： MMR901XA，ミツミ電機株式会社（オンライン），入手先〈http://www.mitsumi.co.jp/latest/Catalog/pdf/sensor_mmr_901.pdf〉（参照 2016-04-28）.

[7] 株式会社モフィリア：FVA-U3SX，株式会社モフィリア（オンライン），入手先〈http://www.mofiria.com/product〉（参照 2016-04-28）.

[8] 東京デバイセズ：IW9PLS，東京デバイセズ（オンライン），入手先〈https://tokyodevices.jp/items/94〉（参照 2016-04-28）.

[9] 早野順一郎，岡田暁宣，安間文彦：心拍の揺らぎ:そのメカニズムと意義，人口臓器，Vol36，No.5，pp870—880(オンライン), DOI:doi.org/10.11392/jsao1972.25.870(1996)

[10] JMOOC : MOOC，JMOOC (オンライン), 入手先〈http://www.jmooc.jp/about/〉(参照 2016-04-28).

[11] Nguyen Minh Duc and Bui Quang Minh: Your face is NOT your password Face Authentication ByPassing Lenovo – Asus – Toshiba (online), available from 〈https://www.blackhat.com/presentations/bh-dc-09/Nguyen/BlackHat-DC-09-Nguyen-Face-not-your-password.pdf〉 (accessed 2016-04-28).

[12] Li,X.,Chang, K., Yuan, Y. and Hauptmann, A.: Massive Open Online Proctor: Protecting the Credibility of MOOCs certificates,Proc. CSCW'15,pp.1129-1137, ACM(2015)

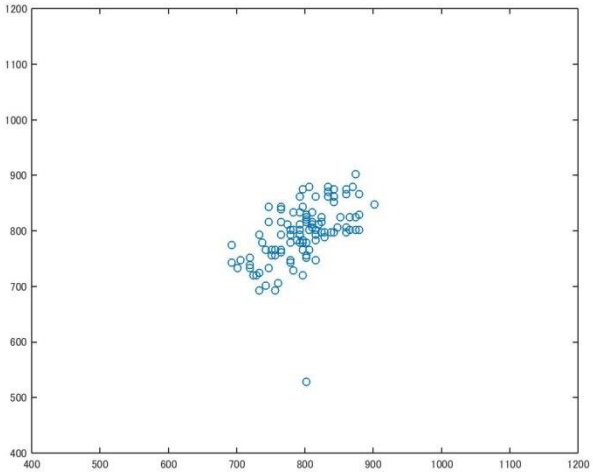

図 7 脈波の揺らぎ

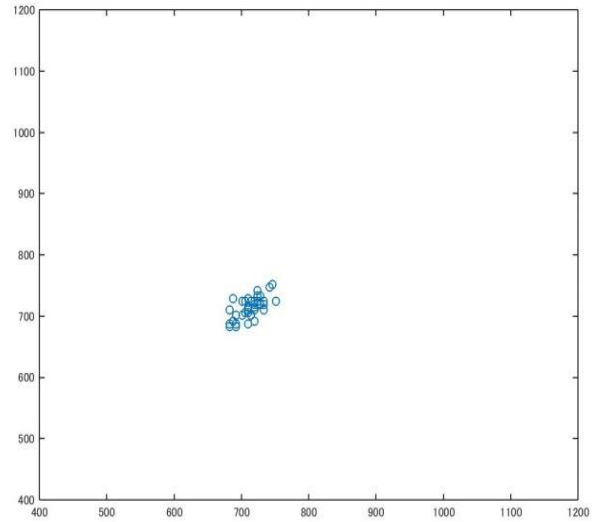

図 8 脈波の揺らぎが少ない