脈波計測値を改変するための腕締め付けデバイスの設計と実装

澤野 亮太[1,a)]　岡本 雅弘[1]　土田 修平[2]　寺田 努[2]　村尾 和哉[1,3,b)]

概要：本研究では，ウェアラブル機器への攻撃可能性を明らかにするために，スマートウォッチなどに搭載されている心拍数を計測する脈波センサを誤認させる腕締め付けデバイスの設計と実装を行う．実装したデバイスを用いて腕締め付けを行い，市販のスマートウォッチの脈波計測を誤認させる評価実験を行った．実験は平常時と運動後の高心拍時の 2 パターンで行った．被験者 1 人で行った結果，平常時には 1 つのデバイスで，高心拍時には 2 つのデバイスで計測心拍数を誤認させることができた．

1. 研究の背景と目的

IoT 機器がインターネットに接続されることでハッキングや踏み台など IoT 機器を狙う攻撃の脅威がある．また，ハードウェアトロイと呼ばれる悪意のある回路が IC に混入され，システムの機能低下や停止，情報漏洩の脅威もある．これらの脅威は解決すべき喫緊の課題であり，既に多くの企業や研究施設が対策に取り組んでいる．これらの脅威以外にも，ウェアラブルデバイスに搭載されているセンサに対する攻撃で，センサデータを利用する上流の機器やアプリケーションが誤った処理や動作をする脅威がある．センサデータを解析することで，健康管理，行動認識，セキュリティなどの用途に用いられ，この数年で保険や医療などの社会保障や福祉インフラに入り込み個人特化した商品やサービスが提供されている．センサによる計測を誤らせる方法として，実世界の計測対象物である道路標識にシールを貼り画像認識結果を誤らせる攻撃 [1] や，加速度センサ素子に超音波を当てて任意の波形を出力させる攻撃 [2]，人間に対する情報提示によって生体情報を制御する手法 [3] が報告されている．また，センサへの攻撃検知として加速度，角速度，地磁気の 3 種類のデータを分類する研究も報告されている [4].

筆者らは，ウェアラブル機器のセキュリティリスクとして，装着者の身体への攻撃による生体情報の操作を懸念している．生体情報操作によって取得されたセンサ値は正しいため，計測以降のハードウェアやネットワーク，クラウドストレージが強固なセキュリティを備えていたとしても，既存の技術では攻撃を検知することは困難である．本研究では，ウェアラブル機器への攻撃可能性を明らかにするために，スマートウォッチなどに搭載されている心拍数を計測する脈波センサを誤認させる腕締め付けデバイスの設計と実装を行う．

[1] 立命館大学大学院情報理工学研究科
[2] 神戸大学大学院工学研究科
[3] JST さきがけ
[a)] ryota.sawano@iis.ise.ritsumei.ac.jp
[b)] murao@cs.ritsumei.ac.jp

2. 提案デバイス

上腕を圧迫する手法として送気ポンプを使用し，カフに空気を送って膨らます手法を採用した．実装したデバイスを**図 1** にデバイスの内部構成を**図 2** 示す．脈波を制御するためには任意のタイミングでの上腕の締め付けが必要なため，カフに対して空気を送るポンプとしてマイクロエアポンプモータを用い，空気を抜くバルブとしてソレノイドバルブを用いた．マイクロエアポンプモータとソレノイドバルブは共に Arduino UNO に接続されており任意のタイミングでのカフへの送気および空気を抜くことができる．Arduino UNO は 9V 電池で動作するため PC に繋ぐ必要はなく腕の圧迫を行える．また，Arduino には pulsesensor.com 製の脈波センサが 2 個接続されおり，上腕のデバイス前後の脈波を観察し，制御に使用する．セットアップとして気圧センサを用いてデバイス使用者ごとの血流が止まる空気圧の限界値を見つけることで，個人に合った圧迫を実現している．マイクロエアポンプモータ，ソレノイドバルブ，気圧センサ，Arduino UNO，9V 電池は 3D プリンタにより自作した箱に格納されている．

3. 評価実験

実装したデバイスを用いて上腕を圧迫して血液を止めた

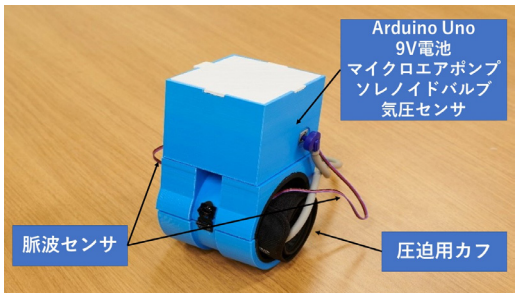

図 1　腕締め付けデバイスの外観

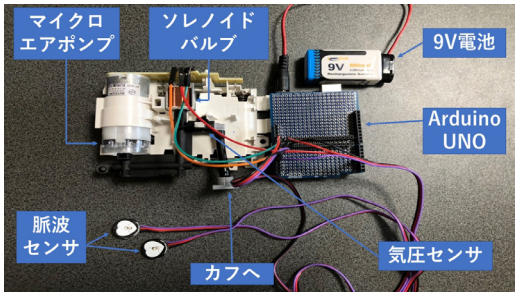

図 2　腕締め付けデバイスの内部構成

とき，市販のスマートウォッチが計測する心拍数の変化を平常時と運動後の 2 パターンで計測した．

3.1　実験環境

被験者は 20 代男性 1 名で，左上腕に実装したデバイス，左手首に市販のスマートウォッチ，左手人差し指に自作の脈波センサを装着した．自作のセンサは pulsesensor.com 製の脈波センサを使用し Arduino UNO を介して PC で脈波を 100Hz で計測した．計測したデータはデバイスが正常に動いているかどうかの確認に使用する．市販のスマートウォッチは FitBit Charge3，AppleWatch Series3，Paenoon フルタッチスクリーンスマートウォッチの 3 機種で実験を行った．Fitbit，AppleWatch，Paenoon 共にもともと搭載されている心拍数モニタで心拍数を 2 分間観察し記録した．計測開始からカフに空気を送り上腕の血液を止めた状態にする．その後 3 秒の加圧をして上腕を締め付け，さらにその後 1 秒間ソレノイドバルブを開放して締め付けを止めた．3 秒加圧あり，1 秒加圧なしを 1 サイクルとして 2 分間繰り返した．計測は各スマートウォッチごとに平常時と運動後の 2 通りで 2 回ずつ行った．

3.2　結果と考察

計測開始時，1 分経過時，計測終了時（2 分時）に各スマートウォッチに表示された心拍数を**表 1** に示す．結果より Fitbit は平常時，運動後共に大きな変化はなかった．AppleWatch は平常時に大きな変化はなかったが，運動後は実際の心拍数より大きく下回った値を示していた．Paenoon は平常時，運動後共に実際の心拍数よりも大きく下回った値を示していた．

表 1　デバイスで計測された心拍数

デバイス	状態	計測開始時	1 分経過	計測終了時
Fitbit	平常時	96 bpm	94 bpm	97 bpm
	平常時	97 bpm	96 bpm	95 bpm
	運動後	164 bpm	141 bpm	122 bpm
	運動後	144 bpm	128 bpm	126 bpm
Apple Watch	平常時	79 bpm	84 bpm	88 bpm
	平常時	85 bpm	82 bpm	84 bpm
	運動後	156 bpm	121 bpm	62 bpm
	運動後	167 bpm	81 bpm	41 bpm
Paenoon	平常時	84 bpm	76 bpm	59 bpm
	平常時	88 bpm	63 bpm	61 bpm
	運動後	150 bpm	59 bpm	60 bpm
	運動後	125 bpm	54 bpm	58 bpm

平常時は心拍数の変化がなかったスマートウォッチでも運動後などの高心拍の時のみ計測値が異常値を示したことから，運動後や飲酒時などの高心拍時には心拍数を制御できるのではないかと考えている．平常時でもより短い間隔での加圧，減圧を実装することで計測値を騙せると考えている．

4.　まとめ

本研究では脈波センサへの攻撃を実現するための腕締め付けデバイスを実装し，上腕の加圧による圧迫が平常時，運動後に市販のスマートウォッチの脈波計測に与える影響を調査した．結果として平常時に計測された心拍数を誤認させられたデバイスは 1 つであったが，運動後の高心拍時では 2 つのデバイスを誤認させることができた．今後は，運動中や運動後，飲酒などで心拍数が高くなった状態での腕締め付けが市販のスマートウォッチの脈波計測に及ぼす影響について更なる調査を行っていく．また，実装した脈波制御デバイスを使用し様々なデバイスに対する腕締め付けの影響を調査する．

謝辞　本研究は，科学技術振興機構戦略的創造研究推進事業さきがけ（JPMJPR1937）の支援を受けたものである．ここに記して謝意を表す．

参考文献

[1] Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Bo Li, Amir Rahmati, Chaowei Xiao, Atul Prakash, Tadayoshi Kohno, and Dawn Song: Robust Physical-World Attacks on Deep Learning Visual Classification, CVPR2018, pp. 1625–1634 (2018).

[2] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, Kevin Fu: WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks, EuroSP2017, pp. 3–18 (2017).

[3] 中村憲史，片山拓也，寺田 努，塚本昌彦: 虚偽情報フィードバックを用いた生体情報の制御手法, 情報処理学会論文誌, Vol. 54, No. 4, pp. 1433–1441 (2013).

[4] Philipp M. Scholl, Keristof van Laerhoven: On the statistical properties of body-worn inertial motion sensor data for identifying sensor modality, ISWC2017, pp. 50–53 (2017)