様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月 １２ 日現在

機関番号：３２７１４
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００１３９

研究課題名（和文）安全なIoTサービスを実現するためのセキュリティ技術に関する研究

研究課題名（英文）Research on security technology for realizing sacure IoT services

研究代表者
岡崎　美蘭（Okazaki, Miran）

神奈川工科大学・情報学部・教授

研究者番号：００５４５１５５

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：　本研究では，スマートフォンなどのモバイル端末を用いてサービスを利用する際の情報流出防止対策として,サービスを提供するサーバと利用者のモバイル端末との相互認証手法について検討を行った．特に,モバイル端末が無線LANを利用してサーバに接続する際の中間者攻撃による不正アクセス防止対策として,サーバ側でカメラという視覚的なチャンネルを用いて正規なモバイル端末を認証できる新たなセキュアペアリング手法について検討した．そこで，カメラが認識できるマーカーと加速度データ及び変位データなどを用いて，正規なデバイスかを判断する手法を提案した．さらに，提案手法の有効性を確かめるための実装・実験を行った．

研究成果の学術的意義や社会的意義
通常，モバイル端末同士のペアリングを行う一つの方法として，キーとなる情報やパスワードをデバイスに手動で入力することにより相互認証を行う方法がある．しかし，機器同士のペアリングを行う機会が多くなれば，逐一手動で相互認証を行うことは手間のかかる作業となる．よって，即時的で手軽であり，加えて空間的に精密に分けることができるペアリング手法が必要となる．
本研究は，特殊なカメラを必要とせず，安価な通常の機器を用いることにより，増加するペアリング機器のコストを削減できると考えられる．また，ペアリング機器同士を高精度に認識できる手法を実現することでより安全なペアリングを行うことができると期待される．

研究成果の概要（英文）：Recently, the number of mobile devices deployed wireless technologies is rising, and the opportunity of wireless communication is also increasing. However, there is a problem that information is leaked by man-in-the-middle attacks. Therefore, the communicating devices must authenticate each other to confirm that they are legitimate devices. Hence, devices must conduct secure pairing, which is exchange of key necessary for encrypting communication contents, before the communication.
We propose a method that perform pairing using devices' accelerometers and markers displayed on devices, and a camera of authentication server.This method has advantage that can detect devices' inclination by recognizing markers' inclination. We performed three types of experiments to conform the similarity of displacement data and acceleration data, whether an impersonator outside camera range can perform pairing, and possibility of several devices pairing together.

研究分野：情報セキュリティ

キーワード：デバイス認証　IoT　ユーザ認証

１．研究開始当初の背景

（1）Wi-Fi や Bluetooth，NFC(Near-Field-Communication）などの無線技術の発展により，それらの技術を搭載したウェアラブルデバイス（スマートウォッチ）やモバイルデバイス(スマートフォン，タブレット端末）など IoT デバイスを利用した様々なサービスが出現していた．しかし，このような IoT サービスを利用する際には，保護すべきデバイスの設定情報や各種サービスのユーザ情報などが漏えい・改ざんされる脅威はもちろん，クラウドサービスやインターネット上に接続された中継機器への不正アクセスが課題であった．さらに，利用者がサービスのリモート制御・監視に利用するスマートフォン（以下，スマホ）がウィルスに感染されるなど様々な脅威が想定されていた．

（2）モバイルデバイスがサーバと無線で様々なデータのやり取りを行う際に，盗聴や中間者攻撃などの攻撃を受ける可能性がある．そこで，モバイル端末とサーバが安全なデータのやり取りを行うために，お互いに認証し，データの暗号化・復号のための鍵を安全に交換しなければならないという課題があった．

２．研究の目的

（1）本研究の目的は，ウェアラブルデバイスやモバイルデバイスなどを用いた IoT サービスを誰でも安心して利用できるように IoT システムのセキュリティ基盤技術を確立することである．そこで，IoT システムの脅威を分析し，デバイスレベルからアプリケーションレベルまで一貫したセキュリティプラットフォームの構築技術を確立することである．

（2）本研究では，モバイル端末などの IoT デバイスを用いたクラウドサービスを利用する際の情報流出防止対策として,サービスを提供するサーバと利用者のモバイル端末との相互認証手法について検討する．特に,モバイル端末が無線 LAN を利用してサーバに接続する際の中間者攻撃による不正アクセス防止対策として,サーバ側でカメラという視覚的なチャンネルを用いて正規なモバイル端末を認証できる新たな認証方式の研究開発を目指す．

３．研究の方法

(1) カメラと加速度センサを用いたデバイスペアリング方式の提案

通常のカメラを搭載したサーバと，加速度センサを搭載したモバイルデバイスをペアリングする手法である．この手法を用いればユーザがモバイルデバイスをカメラに向けて振るだけでペアリングを行うことができる．この手法の特徴は，マーカーと呼ぶカメラが認識しやすい画像の動きでデバイスの動きを代替することで，デバイスの認証精度を高めている点である．

図１に本提案方式におけるペアリング手順について示す．まず，モバイルデバイスがマーカーを画面上に表示する．次にユーザはモバイルデバイスを動かし，デバイスで取得される加速度情報をサーバに無線で送信する．この時，モバイルデバイスの画面上に表示されるマーカーの種類が一定時間ごとに変化する．同時に，サーバ側のカメラではマーカーの種類と動きを取得し，カメラ画像上でのデバイスの変位情報を取得する．その後に，変位情報を微分，加速度情報を積分して速度情報に変換する．最後に，カメラが読み取ったマーカーの種類の列とデバイスから送信されたマーカーの種類の列の類似度と，変換された二つの速度情報の類似度を算出し，一定の閾

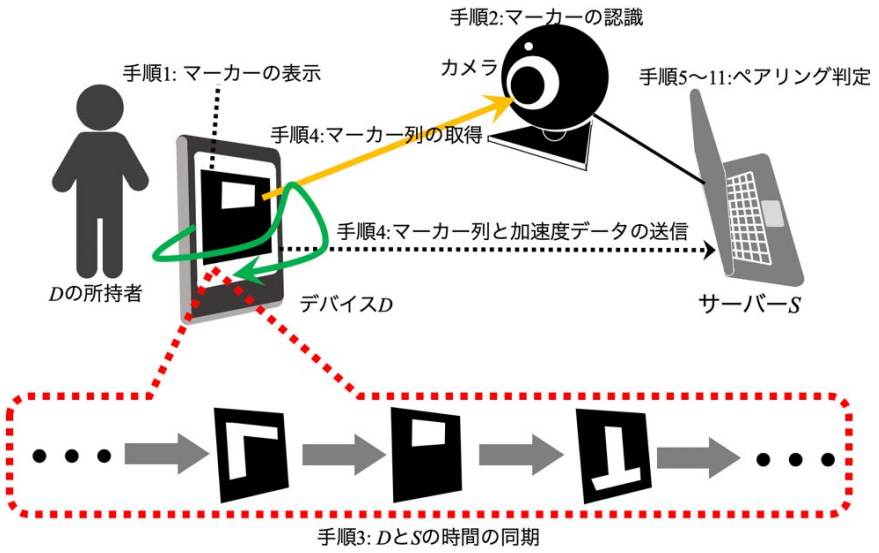

図１．提案手法のペアリング手順

値以上の値を得ることができればペアリング完了になる．

(2) 実装・実験

提案手法の有用性を確かめるためのプロトタイプとして，実装・実験を行った．サーバ側はノート P C，サーバに接続するカメラは外付けの WEB カメラ GROWFAST ASX001B を用いる．モバイルデバイス側はスマートフォン(Nexus 5X)とタブレット(Nexus 7) を用意し，加速度センサは備え付けのものを用いる．また，マーカー認識のプログラムを作成ために，OpenCV のライブラリである Aruco を用いる．無線通信にはルータを介した Wi-Fi によるソケット通信を用いる．実装画面を図 2 に示す．サーバのアプリケーションを立ち上げた後に，モバイルデバイス側のアプリケーションを起動すると双方が接続される．モバイルデバイスのディスプレイ上にマーカーが表示され，サーバではマーカーの認識確認のためにカメラの映像上にマーカーの種類が表示される．また，カメラに関してもノート PC 内蔵のカメラを用いる場合と，外付けのカメラを用いる場合によって，マーカーを認識できる距離が異なるので，それぞれの認識の精度についても実験を行った．変位データと加速度データを正規化したデータを図 3 に示す．カメラから得られた変位データと比べて，加速度センサから得られたデータはノイズが含まれているため細かな凹凸が激しいが，概形の類似を確認することができる．

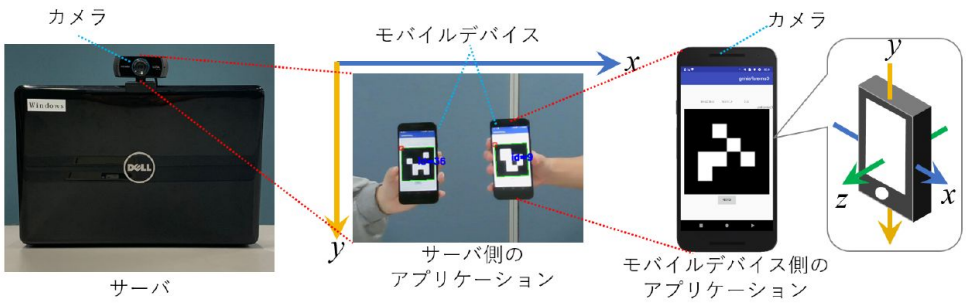

図２．実装画面

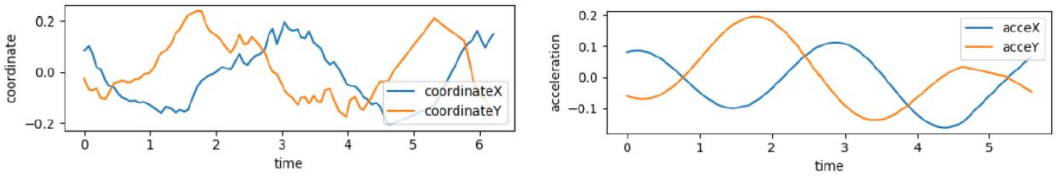

図３．正規化データ

【実験 1：類似度確認実験】

マーカー列と速度データの類似度を確認する実験を行った．被験者は神奈川工科大学生 11 名である．実験手順は以下の通りである．

① 被験者はモバイルデバイス(Nexus 5X，Nexus7）を持ち，カメラから(1.0m，2.0m，3.0m）離れる．

② 被験者はモバイルデバイスのアプリケーションを起動し，マーカーの表示されているディスプレイをカメラに向ける．

③ 被験者はモバイルデバイスを持っている手でモーション(○，1）を 5 秒間描く．

④ 手順 ①～③ を 5 回繰り返す．

実験結果マーカー列の類似度については，0.8-0.9 程度となった．標準偏差が平均類似度と比べて小さいことから，マーカー列によるデバイスの認識は安定して行えていると言える．また，距離，モーションの組み合わせによる類似度の差はほとんどなかったが，サイズの大きい(表示されたマーカーが大きい)Nexus 7 の方の類似度が高くなった．

【実験 2：なりすましの実験】

提案システムのデバイスペアリングでは，ユーザがモバイルデバイスで描くモーションと部屋外の第三者のモーションが類似する可能性がある．そこで，その最悪のケースとしてなりすまし者がユーザのモーションを真似した際に不正なペアリングができるか確認する実験を行った．被験者は神奈川工科大学生 8 名であり，ユーザとなりすまし者の役割を持つ被験者が二人一組で実験を行った．なりすまし者はカメラ範囲外でユーザのモーションが見える位置に立ち，ユーザのモーションを真似することでなりすましを行う．以下の手順で実験を行なった．

① ユーザとなりすまし者はモバイルデバイス(Nexus 5X，Nexus 7）を持ち，ユーザはカメラから(1.0m，2.0m，3.0m）離れ，なりすまし者はカメラ範囲外でユーザのモーションが見える位置に移動する．

② ユーザとなりすまし者はモバイルデバイスのアプリケーションを起動する．ユーザはマーカーが表示されているディスプレイをカメラに向ける．

③ ユーザはモバイルデバイスを持っている手でモーション(○，∞）を 5 秒間描く．同時になりすまし者はユーザの動きを真似する．

④ 手順 ①～③ を 5 回繰り返す．

上記の手順で実験を行なった結果，類似度を平均的に見ればユーザとなりすまし者を区別することができた．ここでマーカー列の類似度を見ると，ユーザの類似度となりすまし者の類似度の差

が顕著に表れている．よって，マーカー列の類似度の閾値を 0.1 や 0.2 に設定することによってモバイルデバイスの区別が可能であることが分かった. また, 速度データの類似度に関しても, ほぼ全ての実験の組み合わせでユーザの類似度の方が高かった. 仮にマーカー列をカメラの範囲外で撮影した, 同じマーカー列を持つなりすまし者でもなりすましが難しいことが分かる．しかし, 速度データのみによるなりすまし者を区別出来た割合を算出したところ, 標準偏差が大きいことが原因で 64.4% となったため，今後その対策方法を検討する必要がある．

【実験 3: 複数デバイスのペアリング実験】

提案システムでは, 複数デバイスが同時にペアリングを行うことを想定しているため, それが可能かどうかを確認する実験を行った. 具体的には, 3 人のペアリングが同時に成功する割合を算出する．被験者は神奈川工科大学生 6 名であり，三人一組で実験を行った．カメラと 3 人の距離を(1.0m，2.0m，3.0m) 離して実験を行った.

今回の実験では, 変位データを分ける手段として, 前フレームの変位データとの距離が最も短い変位データを同じモバイルデバイスとみなすことで実現している.

この結果から, カメラとモバイルデバイスの距離が離れるほどペアリング成功率が上がっていることが分かった．これは，カメラとモバイルデバイスの距離が近くなるとカメラの範囲に映る 3 つのデバイスの距離が近くなってしまうため, サーバ内で変位データを分けることが難しくなったからだと考えられる．よって，複数同時にペアリングが可能であることが確認できたが，デバイス同士の距離が近ければ変位データを分けることが難しくなるため, ある程度距離を離してペアリングを行う必要があることが分かった.

４．研究成果

（1）本研究では，IoT デバイスを用いた安全なサービスを実現するための手法としてカメラと加速度センサによるセキュアデバイスペアリングについて検討を行った. また, そのプロトタイプをノート PC とスマートフォン・タブレットに実装し，実用化に向けた評価実験を行った．結果として平均的に見れば正規のユーザとなりすまし者を区別することができ，また，3 人同時にペアリングを行う実験を行った結果，カメラとモバイルデバイスの距離が 3.0m のとき，ペアリング成功率が 94.4% となり，複数人同時にペアリングを行えることが確認できた.

（2）今回の実験では，被験者にシンプルなモーションである○と，複雑なモーションである∞を描いてもらった. しかし, 実際にユーザがペアリングを行う際は任意のモーションを描くことが想定されるため，それを考慮した実験を行う必要がある.

（3）今回実施した実験では，速度データの類似度における標準偏差が大きくなり，安定したペアリングが難しい結果となった. そこで, 従来の受信信号強度（RSS：Received Signal Strength）などを用いたペアリング手法のような, ユーザが意識することなく行われる手法と併用することにより, よりセキュアなデバイスペアリングができるかについてさらに検討していく必要があると考えられる.

５．主な発表論文等

〔雑誌論文〕　計6件（うち査読付論文　6件／うち国際共著　0件／うちオープンアクセス　6件）

１．著者名 M. Nagatomo, K. Aburada, N. Okazaki and M. Park	４．巻 2
２．論文標題 Proposal of Ad-Hoc Secure Device Pairing Method with Accelerometer and Camera Using Marker	５．発行年 2019年
３．雑誌名 International Journal of Networking and Computing	６．最初と最後の頁 318-338
掲載論文のDOI（デジタルオブジェクト識別子） www.ijnc.org, ISSN 2185-2847	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 M. Nagatomo, K. Watanabe, K. Aburada, N. Okazaki and M. Park	４．巻 12
２．論文標題 Personal Identification with Any Shift: Authentication method for smartwatches having shoulder-surfing resistance	５．発行年 2019年
３．雑誌名 IEICE ComEX	６．最初と最後の頁 495-500
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1587/comex.2019GCL0024	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 K. Aburada, S. Usuzaki, H. Yamaba, T. Katayama, M. Park and N. Okazaki	４．巻 3
２．論文標題 Implementation of CAPTCHA suitable for mobile devices	５．発行年 2019年
３．雑誌名 IEICE ComEX	６．最初と最後の頁 55-60
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1587/comex.2019GCL0060	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 K. Sakamoto, M. Nagatomo, N. Okazaki, and M. Park	４．巻 8
２．論文標題 Examination of personal authentication method achieving shoulder-surfing resistance by combining mouse operation and number matrix	５．発行年 2019年
３．雑誌名 IEICE ComEX	６．最初と最後の頁 61-66
掲載論文のDOI（デジタルオブジェクト識別子） DOI:https://doi.org/10.1587/comex.2018XBL0143	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 M. Nagatomo,Y. Kita, K. Aburada, N. Okazaki and M. Park	4．巻 7(3)
2．論文標題 Implementation and user testing of personal authentication having shoulder surfing resistance with mouse operations	5．発行年 2018年
3．雑誌名 IEICE ComEX	6．最初と最後の頁 77-82
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/comex.2017XBL0170	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 S. Usuzaki, Y. Arikawa, H. Yamaba, K. Aburada, S. Kubota, M. Park, N. Okazaki	4．巻 26
2．論文標題 A Proposal of Highly Responsive Distributed Denial-of-Service Attacks Detection Using Real-Time Burst Detection Method	5．発行年 2018年
3．雑誌名 Journal of Information Processing	6．最初と最後の頁 257-266
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.2197/ipsjjip.26.257	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計15件（うち招待講演　0件／うち国際学会　6件）

1．発表者名 K. Watanabe, M. Nagatomo, K. Aburada, N. Okazaki and M. Park
2．発表標題 Gait-Based Authentication using Anomaly Detection with Acceleration of Two Devices in Smart Lock
3．学会等名 Proceedings of the 14th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2019)（国際学会）
4．発表年 2019年

1．発表者名 M. Nagatomo, K. Watanabe, K. Aburada, N. Okazaki and M. Park
2．発表標題 Proposal and Evaluation of Authentication Method having Shoulder-Surfing Resistance for Smartwatches using Shift Rule
3．学会等名 The 22nd International Conference on Network-Based Information Systems (NBiS2019)（国際学会）
4．発表年 2019年

１．発表者名
M. Nagatomo, K. Aburada, N. Okazaki, H. Yamaba, and M. Park

２．発表標題
Proposal of Ad-Hoc Secure Device Pairing Method Using Similarity Between Marker Movement and Acceleration

３．学会等名
Proceedings of the Workshops of the 33rd International Conference on Advanced Information Networking and Applications (WAINA-2019)（国際学会）

４．発表年
2019年

１．発表者名
H. Yamaba, S. Usuzaki, K. Aburada, T. Katayama, M. Park, and N. Okazaki

２．発表標題
Evaluation of Manual Alphabets Based Gestures for a User Authentication Method Using s-EMG

３．学会等名
The 22nd International Conference on Network-Based Information Systems (NBiS2019)（国際学会）

４．発表年
2019年

１．発表者名
渡辺 一樹，長友 誠，油田 健太郎，岡崎 直宣，朴 美娘

２．発表標題
スマートロックにおける異常検知を用いた二つの端末の加速度による歩行認証の提案

３．学会等名
マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2019）

４．発表年
2019年

１．発表者名
坂本 憲理、長友 誠、岡崎 直宣、朴 美娘

２．発表標題
スマートホーム内のIoT機器を対象としたサイバー攻撃への耐性評価

３．学会等名
ICCS/SPT研究会

４．発表年
2019年

１．発表者名
長友 誠，油田 健太郎，岡崎 直宣，朴 美娘

２．発表標題
マーカーを用いたカメラと加速度センサによるセキュアデバイスペアリング手法の評価

３．学会等名
研究報告コンピュータセキュリティ(CSEC)

４．発表年
2019年

１．発表者名
長友 誠、渡辺 一樹、油田 健太郎、朴 美娘、岡崎 直宣

２．発表標題
覗き見耐性を持つ小型タッチスクリーン端末における個人認証方式の提案

３．学会等名
Symposium on Cryptography and Information Security(SCIS2019)

４．発表年
2019年

１．発表者名
M. Nagatomo, K. Aburada, N. Okazaki, and M. Park

２．発表標題
Proposal and Evaluation of Secure Device Pairing Method with Camera and Accelerometer

３．学会等名
Proceedings of 2018 Sixth International Symposium on Computing and Networking Workshops(CANDARW)（国際学会）

４．発表年
2018年

１．発表者名
M. Nagatomo, K. Aburada, N. Okazaki, and M. Park

２．発表標題
An Examination of Pairing Method with Camera and Acceleration Sensor

３．学会等名
ICMU2018（国際学会）

４．発表年
2018年

１．発表者名
長友 誠，油田 健太郎，岡崎 直宣，朴 美娘

２．発表標題
カメラと加速度センサを用いたデバイスペアリング方式の提案とその評価

３．学会等名
マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2018）

４．発表年
2018年

１．発表者名
坂本 憲理、長友 誠、岡崎 直宣、朴 美娘

２．発表標題
覗き見耐性を持つマウス操作と数字盤を組み合わせた個人認証方式の提案と評価

３．学会等名
コンピュータセキュリティシンポジウム（CSS2018）

４．発表年
2018年

１．発表者名
渡辺 一樹、長友 誠、油田 健太郎、岡崎 直宣、朴 美娘

２．発表標題
スマートフォンとウェアラブル端末の加速度センサを用いたスマートロックにおける歩行認証

３．学会等名
コンピュータセキュリティシンポジウム（CSS2018）

４．発表年
2018年

１．発表者名
長友誠，喜多義弘，油田健太郎，岡崎直宣，朴美娘

２．発表標題
マウス操作を用いた個人認証方式のユーザビリティと覗き見耐性の実験と評価

３．学会等名
コンピュータセキュリティシンポジウム

４．発表年
2017年

１．発表者名 長友　誠，朴 美娘，岡崎 直宣
２．発表標題 覗き見耐性を持つマウス操作を用いた個人認証方式の提案
３．学会等名 CSEC/SPT研究報告
４．発表年 2017年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称	発明者	権利者
加速度センサを搭載したモバイル端末を正規の通信相手として認証する方法および認証装置	岡崎　美蘭、長友　誠、岡崎　直宣	学校法人　幾徳学園
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願2018-036579	2018年	国内

〔取得〕　計0件

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	岡崎　直宣 (Okazaki Naonob) (90347047)	宮崎大学・工学部・教授 (17601)	