

神奈川工科大学

セキュリティ研究センター

研究報告

第 9 卷

2020 年度

目次

- ・セキュリティ研究センター研究成果報告の発刊に際して

- ・研究所メンバー

- ・分散機械学習モデルに基づいた安全な IoT サービスを実現するための
統合セキュリティ対策技術に関する研究

情報ネットワーク・コミュニケーション学科 岡崎 美蘭

情報工学科 納富 一宏

情報ネットワーク・コミュニケーション学科 岡本 学

情報ネットワーク・コミュニケーション学科 岡本 剛

- ・不可視光画像と AI 技術を利用した物質の表面分析技術の構築

情報メディア学科 西村 広光

情報工学科 須藤 康裕

情報メディア学科 谷田 良子

セキュリティ研究センター 研究成果報告の発刊に際して

研究代表者 情報ネットワーク・コミュニケーション学科 岡崎 美蘭

世界は今、サイバー空間とフィジカル空間を高度に融合させることにより、人々に様々な高度でかつきめ細かなサービスを提供可能にする「Society 5.0」へシフトしている。例えば、工場や農業といったフィジカル空間上に設置されたセンサなどの IoT デバイスによって種々のデータが観測・収集され、ネットワークを介してサイバー空間上のクラウドに集められて AI により分析・予測され新しいサービスがどんどん登場している。一方で、個人情報をはじめとした生活に関わるあらゆる情報がネットワーク上に流通して計算機上で管理・処理されるようになり、機密情報や個人情報などを目的としたサイバー攻撃もその手口が多様化・高度化している。

本研究センターの特色は、情報セキュリティの基礎技術となるネットワークセキュリティ技術や個人認証技術、情報漏えい対策技術だけではなく、応用面での著作権保護技術及び電子透かし技術の研究、さらに組織における情報セキュリティマネジメントシステム (ISMS: Information Security Management System) の実施モデル構築手法の研究、危機管理やサイバー犯罪などのセキュリティと社会の研究を、統合的に行うことである。これにより、現代の安全・安心な情報化社会の実現に向けた将来ビジョンを世界に向けて展開することを目指す。

2020 年度は、学内重点配分研究として 2 つの研究テーマ「分散機械学習モデルに基づいた安全な IoT サービスを実現するための統合セキュリティ対策技術に関する研究」、「不可視光画像と AI 技術を利用した物質の表面分析技術の構築」を実施した。そこで、IoT 認証基盤技術に関する研究、機械学習モデルを使った歩行認証の異常検知手法の研究開発、IoT マルウェアの解析手法の開発、不可視画像と AI 技術を利用した表面分析の検討などを進め、特許出願及び学会発表など多くの成果を上げることができた。

今後は、引き続き IoT セキュリティ基礎基盤技術をより一層高深度化していくとともに、社会インフラの安心・安全の確保などへの適用を検討する。また、高度情報化社会で必要とされる様々な ICT システムへの実用化と応用システムの研究開発を進めて行く。

研究所メンバー

研究代表者

情報学部 情報ネットワーク・コミュニケーション学科 岡崎 美蘭

氏名	所属・職名	研究内容
岡崎 美蘭	情報ネットワーク・コミュニケーション学科・教授	安全性と利便性を考慮した認証方式を用いたモバイルクラウドサービスの実現手法に関する研究
納富 一宏	情報工学科・教授	社会的要請に基づいた組織内情報セキュリティのための ICT プラットフォーム構築に向けた基盤研究
鳥井 秀幸	情報ネットワーク・コミュニケーション学科・教授	情報ハイディング技術に関する研究
岡本 学	情報ネットワーク・コミュニケーション学科・教授	情報漏洩防止にむけての研究
岡本 剛	情報ネットワーク・コミュニケーション学科・教授	サーバアプリケーションのセキュリティ強化に関する研究
西村 広光	情報メディア学科・教授	不可視画像処理を利用した認証技術の研究
須藤 康裕	情報工学科・准教授	使いやすさと安全性を両立する認証方式に関する研究
山本 聡	基礎教養教育センター ・教授	サイバー犯罪の実態と警察の捜査に関する研究
三浦 直子	基礎教養教育センター ・准教授	セキュリティと社会，危機管理に関する研究
佐藤 史緒	教職教育センター	セキュリティと教育に関する調査研究

分散機械学習モデルに基づいた安全な IoT サービスを実現するための 統合セキュリティ対策技術に関する研究

研究者名： 情報ネットワーク・コミュニケーション学科 岡崎 美蘭
情報工学科 納富 一宏
情報ネットワーク・コミュニケーション学科 岡本 学
情報ネットワーク・コミュニケーション学科 岡本 剛

1. 研究の目的

本研究の目的は、誰もが安心して暮らせる超スマート社会を実現するためにフィジカル空間とサイバー空間を融合したすべての部分で安全性と信頼性を確保することができる高度かつ堅牢な IoT セキュリティ統合対策技術を確立することである。具体的には、超スマート社会実現におけるサイバー攻撃の脅威を明確に分析し、フィジカル空間からサイバー空間まで一貫して安全性を提供可能となる高度な IoT セキュリティシステム構築技術の確立について検討する。そして、不正デバイスと不正アプリケーションを見分けることができるデバイス認証技術とユーザ認証技術を開発するとともに、不正データ・異常データをより早く検知することができる信頼性の高い分散機械学習モデル構築手法の研究開発を行うことである。

そこで、初年度となる今年度は、スマートフォンとスマートウォッチのようなウェアラブル端末を用いた IoT セキュリティシステム構築技術の検討とそれらを用いた個人認証方式を提案し、その有効性について検討することを目的とする。さらに、IoT 機器を標的とするマルウェアをより効率的に解析する方法について検討することを目的とする。

2. 研究の必要性及び従来研究

現在 IoT 機器の急増に伴い、IoT 機器の不十分なセキュリティ設定や脆弱性を突いたマルウェア感染、DDoS 攻撃などサイバー攻撃が増加する中で、世界的に IoT セキュリティ対策に関する研究活動も活発に行われている。例えば、フィジカル空間の不正な IoT 機器を検出するために、ネットワークスキャンなどで脆弱な機器を見つける機器推定機能などが提供されている。その IoT 機器の中に、電子的に個人の認証を行い家のドア等の鍵の開閉を行うスマートロックと呼ばれる製品がある。しかし、スマートロックにおける個人認証方式として、従来のパスワード方式ではパスワードが推測されやすくユーザに記憶負荷がかかるという問題点や、毎回記憶したパスワードを端末に入力する必要がある日常的に使う鍵の開閉を行うための個人認証方式としては煩わしさが残る。また、IC チップの埋め込まれたカードや事前に認証を済ませた端末などを持ち歩くことで認証を行う所持認証と呼ばれる方式があるが、スマートロックにおける所持認証方式では、従来の鍵と同様に紛失や

盗難等の危険性が課題として挙げられる。これらの課題点を解消する方式として人間の身体的特徴を用いて認証を行う生体認証方式がある。しかし、スマートロックにおける生体認証方式として、例えば指紋認証方式では、家の前で数秒間立ち止まらなくてはならず、手袋をつけていればそれを外す必要がある。また、顔認証方式においてもドアの前で数秒間立ち止まる必要があり、マスクや帽子等を身に付けていればそれらを外さなくてはならないという煩わしさがある。

本研究ではスマートロックにおける認証の煩わしさを排除するため、ユーザの行動から得られる行動的特徴を用いた歩行認証に着目した。歩行認証とは、歩行時の加速度データや角速度データなどから行動的特徴を抽出し認証を行う生体認証方式の一つであり、日常的に行われる歩行を用いることでユーザが意識することなく認証を行うことができる利便性があると考えられる。しかし、行動的特徴を用いる認証方式では、本人の行動を常に再現することが難しく認証精度に大きな課題がある。これまでも歩行認証は認証精度向上のため多くの研究が行われている。これらの研究では、機械学習や複数のセンサを用いることで認証精度の向上のための研究を行っている。しかし、認証の際に端末の向きを同じにしなくてはならないという煩わしさや、複数の同一センサを身に着ける必要がある等の課題点がある。また、行動的特徴を用いる認証方式には行動を他人に真似され不正なユーザに認証されてしまうという問題点がある。この問題点に対しては、スマートフォンから取得した加速度データを基に歩行認証を行い、なりすまし攻撃に対して有効か確認を行っている研究も実施されているのが現状である。

3. 期待される効果

従来のような端末の向きを考慮せず、さらに複数のセンサを用いることもなく、スマートフォンとスマートウォッチの二つの端末の合成加速度を用いることでユーザが意識することなくスマートロックの個人認証が可能となる。また、事前に登録したウェアラブル端末の ID による所持認証を行うことで歩行認証の認証精度の課題を解消できると期待される。

4. 研究の経過及び結果・評価

現在まで、本研究ではスマートフォンとウェアラブル端末の二つの端末の加速度による歩行認証システムを提案し、機械学習を用いて本人認証率を確認した。また、継続的な歩行認証の有効性を確認するため日にちを開け定期的に歩行実験を行った手法を提案し、その評価実験を行なった。以下に本研究のシステムについての説明と実験結果を報告する。

4.1 二つの端末を用いた異常検知による歩行認証システム

スマートロックという IoT 機器が加速度センサが搭載された二つの端末と、加速度デ

ータを受信しユーザの認証を行うスマートロックで構成される．提案システムモデルを図 1 に示す．

スマートロックと二つの端末の通信方式には Bluetooth を用い，iBeacon によりスマートロックと二つの端末との近接検知を行う．iBeacon では Immediate (約 2cm 未満)，Near (約 2cm～1m)，Far (約 1m～約 50m) の 3 つの近接検知を行うことができ，本提案システムモデルでは Near と Far の二つの近接検知を用いて加速度データの計測を行う．

二つの端末は，以下の手順で認証を行う．

- (1) iBeacon の Far 検知
- (2) 事前登録した二つの端末の ID 送信
- (3) スマートロック内で二つの端末の ID 確認
- (4) 二つの端末での加速度データの計測開始
- (5) iBeacon の Near 検知
- (6) 計測した加速度データをスマートロックへ送信
- (7) スマートロック内で受信した二つの端末の加速度データを処理
- (8) 加速度データから特徴量抽出
- (9) 機械学習による異常検知を行い正常データなら解錠，異常データなら施錠する

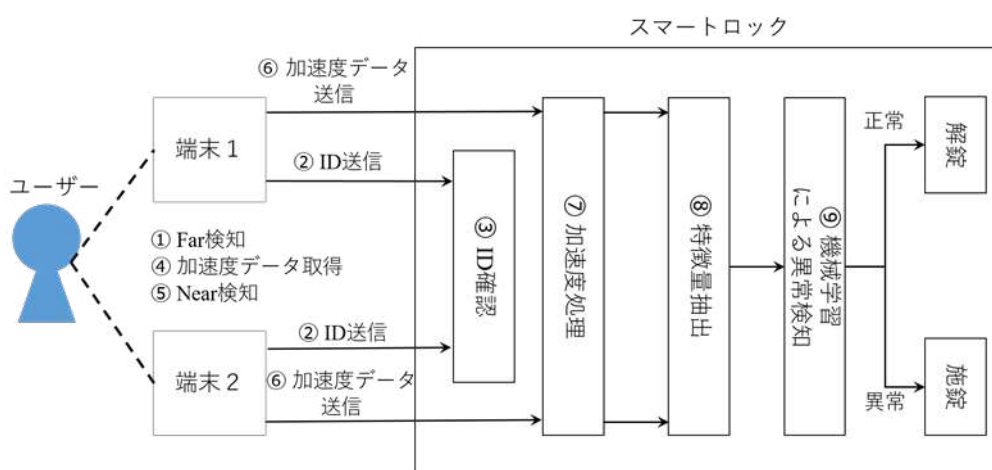


図 1．二つの端末を用いた歩行認証システム

4.2 実験結果

提案手法の有用性を確かめるために，端末 1 にスマートフォン Sony Xperia XZs を用い，端末 2 にウェアラブル端末 Sony SmartWatch3 を用い実装を行った．また，スマートロックの代わりに Linux OS をインストールしたパソコンをサーバとして用意し，各端末から加速度データを取得するため加速度の開始及び終了命令を送信するためのプログラムを実装した．実装したプログラムでは，まずより良い特徴量選択を行うため，

全ての特徴量の組み合わせに対して認証率を計算し、それぞれの機械学習モデルに適した特徴量の選択を行う。次に、選択された特徴量を用いて、機械学習モデルを作成しそれぞれの機械学習のパラメータの調整や異常度を算出しその異常度の閾値を調整することで認証率を計算し、最適なパラメータ及び閾値を決定する。機械学習には Python モジュールの scikit-learn を用い、異常検知アルゴリズムとして、Elliptic Envelope, GMM, Isolation Forest, KDE, LOF, One Class SVM を用いそれぞれの認証率を計算し評価を行った。

その結果、日にちを空けずに行った普段の速度での歩行によって得られる加速度データから特徴量を算出した認証率では、GMM を用いた場合に FAR が 13.6%, FRR が 3.6%であり、Isolation Forest を用いた場合に FAR が 8.3%, FRR が 9.5%であった。

また、日にちを空けた異なる速度での歩行認証の有効性の確認を行うため、早歩き、普通歩き、遅歩きでの三つの速度の歩行を学習させた学習器を作成し、その学習器を基に異常検知を行い本人か他人かを判定しその認証率の計算を行った。その結果、大きく認証率が悪くなった機械学習のアルゴリズムもあればあまり認証率に変化のないアルゴリズムもあることを確認した。例えば、日にちを空けずに行った歩行に比べ KDE では、FAR が+3.4%, FRR が-3.9%とそれほど変わらないという結果となった。また、歩行の速さを変えた場合での歩行認証の認証率では、最も良かった識別率は機械学習に GMM を用いた場合の FAR が 18.8%であり、FRR が 15.0%であった。全体的に、普段の速さで行った場合に比べ認証率は軒並み悪くなった。

5. 今後の計画

歩行認証という人間の行動的特徴を用いた認証方式は、同一人物でも常に同じ歩き方をするというのはなかなか難しく、認証率の精度をいかに上げるかが課題になっている。そこで、異なる速度での歩行認証の有効性を確認するため、学習データには異なる速度の歩行データを学習させ、評価を行った。認証率は悪くなるという結果となったが、大きく FAR や FRR が悪くなってしまった機械学習アルゴリズムもあれば変化の少ないアルゴリズムもあり、特徴量の抽出方法や加速度処理の方法によっては、認証精度の向上ができると考えられる。

今後の課題としては、認証率の向上のためより良い特徴量の抽出や、より良い特徴量選択の方法などが挙げられる。また、眼鏡型のウェアラブル端末など様々なウェアラブル端末から歩行状態の加速度データを取得した場合でも高い精度で認証を行うことができるか確認することが挙げられる。さらに、これらの研究成果と実験結果をまとめて情報処理学会論文誌に投稿できるよう、執筆を行う予定である。

6. 研究成果の発表

(1) 論文

- [1] H. Yamaba, Y. Nagatomo, S. Usuzaki, K. Aburada, T. Katayama, M. Park and N. Okazaki, "Evaluation of Yubimoji Based Gestures for Realizing User Authentication Method Using s-EMG" Proceedings of the Workshops of the 34th International Conference on Advanced Information Networking and Applications (WAINA-2020), pp. 834-844, April, 2020.
- [2] H. Yamaba, K. Shiraishi, S. Usuzaki, K. Takatsuka, K. Aburada, T. Katayama, M. Park, N. Okazaki, "An attempt at an introduction of deep learning for a user authentication system using s-EMG," Proc. The 26th International Symposium on Artificial Life and Robotics, OS-3-3, pp.1-5, 2021/01/21.
- [3] Shu Akabane, Takeshi Okamoto, "Identification of library functions statically linked to Linux malware without symbols," Procedia Computer Science, Vol. 176, No. 2020, pp. 3436-3445.

(2) 学会発表

- [1] 長友 誠, 油田 健太郎, 岡崎 直宣, 朴 美娘, "分散機械学習における勾配の異常検知を用いたブロックチェーンシステムの提案とその実現性の評価," IPSJ-CSEC-88, No22, 2020/03/12.
- [2] 渡辺 一樹, 油田 健太郎, 岡崎 直宣, 朴 美娘 "継続的な認証及び異なる歩行速度での二つの端末を用いた異常検知による歩行認証の研究," ICCS/SPT 研究会 Vol. 2021 SPT-41 No.16, 2021/3/1.
- [3] 嘉藤 鴻介, 渡辺一樹, 油田健太郎, 岡崎直宣, 朴美娘, "ウェアラブル端末を用いた覗き見耐性を持つジェスチャー認証手法の提案と評価," ICCS/SPT 研究会 Vol. 2021 SPT-41 No.17, 2021/3/1
- [4] 赤羽秀, 岡本剛, "シンボル情報が消去された IoT マルウェアに静的結合されたライブラリ関数の特定", コンピュータセキュリティシンポジウム 2020 論文集, pp. 543-550, 2020.

(3) 特許

- [1] 特願 2014-046134 「個人認証装置及びプログラム」
発明者：岡崎 美蘭
出願者：学校法人 幾徳学園
- [2] 特願 2015-165962 「個人認証装置及びプログラム」
発明者：岡崎 美蘭

出願者：学校法人 幾徳学園

[3] 特願 2015-183574 「個人認証用プログラム」

発明者：岡崎 美蘭

出願者：学校法人 幾徳学園

[4] 特願 2018-036579 「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」

発明者：岡崎 美蘭

出願者：学校法人 幾徳学園

[5] 特願 2019-189314 「システム、方法、情報処理装置およびプログラム」

発明者：岡崎 美蘭

出願者：学校法人 幾徳学園

(4) 助成金採択

[1] 平成 26 年～平成 28 年度 文部科学省科学研究費補助金 基盤 (C)

「覗き見耐性とユーザビリティを有するモバイル端末向けユーザ認証方式」

研究代表者：岡崎 美蘭

[2] 平成 29 年～平成 31 年度 文部科学省科学研究費補助金 基盤 (C)

「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」

研究代表者：岡崎 美蘭

[3] 2020 年～2022 年度 文部科学省科学研究費補助金 基盤 (C)

「分散機械学習モデルに基づいた高度かつ堅牢な IoT セキュリティ対策技術に関する研究」

研究代表者：岡崎 美蘭

不可視光画像と AI 技術を利用した物質の表面分析技術の構築

研究者名：	情報メディア学科	西村 広光
	情報工学科	須藤 康裕
	情報メディア学科	谷田 良子

1. 研究の目的

画像処理・認識の技術は可視光映像を中心に発展し、近赤外光映像への応用が一部行われている。しかし、紫外光映像を利用した研究はほとんど行われていない。我々は、これまでに金属鍵を紫外光画像により高精細に識別する基礎技術を開発してきた。紫外光カメラにより金属表面の微細な傷を映像化し、鍵の抜き差しに生じる傷を個体識別に利用できることを確認している。本研究は、可視光・近赤外光・紫外光の映像を利用して、可視情報のみでは識別困難な個体識別技術を確立し、実用レベルの非接触な物質表面の画像装置開発を行う計画である。

2. 研究の必要性及び従来の研究

可視光領域の画像を利用した画像処理・認識の技術は、パターンマッチング・機械学習・深層学習などの技術が蓄積され、対象データ数が大規模に確保できる領域においては高度に発展してきている。一方、近赤外領域の画像処理は、距離画像取得などに活用され、Kinect などで広く知られるように広く応用が進んできている。しかし、紫外線領域の画像処理に関しては、人工衛星画像の高精度解析技術や、精密部品検査技術で一部利用されているものの、活用が進んでいない。

我々は、これまでに可視光画像だけでなく近赤外光画像、紫外光画像を活用した画像処理技術の構築を試みてきた。これまでに以下の技術を開発してきた。

- ・ 近赤外線透過フィルタによる高精度カード認証技術の開発
クレジットカードなどの裏面記載したサイン情報は、防犯カメラなどで容易に読み取ることが可能になっている。そこで、近赤外のある帯域以外を通さない工学フィルタをカード裏面に張り付け、さらに持ち方による生体情報を組み合わせた高精度カード認証技術を開発した。
- ・ 紫外線を利用した金属鍵認証技術の開発
金属の鍵は、3次元スキャニング技術の発展、3次元プリンタの普及により、今後容易にコピーされてしまう危険がある。しかし、紫外光により高精細に

金属鍵の表面を映像化すると、目に見えない微細な傷が、皮膚の指紋のように映像化できる。この情報を利用して、高精度な金属鍵識別技術を開発し、複製された鍵の識別が可能であることを実証した。さらに、鍵の抜き差しによる傷変化の検出が可能であることも確認し、前に抜き差しした鍵かどうかを判別できることを確認している。

建築用資材の時間変化を、可視光・赤外光・紫外光を併用することで非接触に検査する基礎技術の検討を行ってきた。鹿島建設様からの研究資材協力を得て、2019 年度から実験を開始し、新たな現象を発見し、現在その分析を進めている。

こうした紫外光を含む不可視光を利用した画像処理による物体表面分析に関しては他の事例が見当たらず、本研究の独自性が高い視点であるといえる。

3. 期待される効果

本研究は、可視光画像を対象に確立してきた技術を、赤外光や紫外光の範囲に適用し、人間に不可視な情報での識別技術を構築することを目的としている。これまで他に検討された報告が見つからない分野であるが、我々はこれまでに金属鍵認証技術の基盤技術を構築しており、実用化に向けた応用技術を本申請で確立させ、実用化のめどを構築しようとするものである。

具体的に、本研究では建築資材、特にコンクリートやモルタルが硬化する時間変化を、不可視光画像を利用した画像解析で現象をとらえることにこれまで成功している。これは世界初の試みであり、現在鹿島建設様と特許の共同出願の準備を進めている。この現象のさらなる分析を進め、非接触にコンクリートなどの硬化変化をとらえることを目的としている。

4. 研究の経過及び結果・評価

2020 年度の計画では、鹿島建設様からのコンクリート実験資材の提供を受けて、紫外線計測の実験データを増やし、硬化が紫外線で捉えられる理由の分析を進め原理解明を進める計画であった。しかし、コロナ禍で実験資材の提供を受ながら観測実験を行うことが困難な環境となった。そのため、一般に入手可能なセメント素材においてデータの取得を進め、分析を行った。こちらはさらにデータを取得した分析が必要であり、今後も継続して進めていく計画である。

5. 今後の計画

2020 年度に紫外線観測機材を 2 セット稼働できるようにしたため、2021 年度はより効率的にデータ取得ができる見込みである。

2020 年度より実験データの取得をはじめたセメント素材の分析でも一定の成果を確認しているが、まだデータ数が少ない。そのため、さらにデータ数を増やして実験を行い、分析を深めていく計画である。

さらに研究室のみで実験を進めることができる素材として、モルタル素材がある。こちらは DIY などでも比較的容易に利用されている建築素材であるが、硬化具合に関してはコンクリートと同様に、経験と触感によるものが多い。そのため、モルタル素材での実験も進め、分析を進めていく計画である。

加えて、感染予防対策を進めたうえで、2020 年度に予定していた鹿島建設様から実験用資材提供を受けることができるようになれば、コンクリートを対象とした実験も再開していく計画である。

6. 研究成果の発表

2020 年 3 月に鹿島建設様と特許を共同出願（特願 2020-053306）特許願した。

蓄積した成果をあげているが、特許出願前は学会発表は控えてきていたテーマである。その後のコロナ禍で学会への参加困難な状況が続いていたが、オンライン学会などを活用し、今後さらなる機会を作り、成果発表を進めていく計画である。