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　５ 年　 ６ 月 ２２ 日現在

機関番号：６２６１５
研究種目：基盤研究(A)（一般）
研究期間：2018～2020
課題番号：１８Ｈ０４１２０

研究課題名（和文）個人の利便性確保となりすまし防止を実現する生体情報保護活用基盤

研究課題名（英文）Biometric Information Protection Utilization Infrastructure to Ensure Personal Convenience and Prevent Identity Theft

研究代表者

越前　功（Echizen, Isao）

国立情報学研究所・情報社会相関研究系・教授

研究者番号：３０４６２１８８

交付決定額（研究期間全体）：（直接経費）　　33,200,000円

研究成果の概要（和文）：高性能なカメラやマイクロフォンの普及により，他人の顔，音声，歩行動作，さらには指紋，静脈，虹彩といった生体情報が，遠隔からの撮影や録音を経て，サイバー空間に共有されることで，生体認証の突破や，詐欺や詐称といった「なりすまし」の脅威となることが指摘されている．一方で生体認証は本人認証の手段として広く普及しているため，本人認証の際には不便なく生体情報を提供できることが望ましい．本研究では，現実空間における生体認証の利便性を確保しながら，遠隔からの生体情報の取得や，サイバー空間における生体情報の流通を，本人の意思に応じて制御可能な技術基盤を検討した．

研究成果の学術的意義や社会的意義
本研究の学術的意義および社会的意義は，現実空間とサイバー空間をつなぐ多種多様なセンサ群や，サイバー空間における多種多様なサービスへの依存性を極力排除しながら，人間に関わる最もセンシティブな生体情報の流通を，現実空間の利便性を担保した上で，自らの意思により制御できることにある．本研究で構築する生体情報保護活用基盤により，生体情報をやり取りする遠隔医療・カウンセリングや，高い信用性と匿名性を必要とする電子投票といった応用への波及効果が期待される．さらに，個人の同意のもと多様な生体情報が活用できるため，人流解析から遠隔見守りや位置探索サービスといった多様な分野への貢献が期待される．

研究成果の概要（英文）：With the spread of high-performance cameras and microphones, it has been pointed out that biometric information such as the face, voice, gait, fingerprints, veins, and iris of another person can be remotely captured or recorded and shared in cyberspace, posing a threat to biometric authentication and "spoofing," such as fraud and impersonation. On the other hand, since biometric authentication is widely used as a means of identity authentication, it is desirable to be able to provide biometric information without inconvenience. In this study, we investigated a technological infrastructure that can control the remote acquisition of biometric information and the distribution of biometric information in cyberspace according to the user's intention, while ensuring the convenience of biometric authentication in real space.

研究分野：情報セキュリティ

キーワード：生体情報保護

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

Internet of Things の進展により，現実空間の様々な情報をサイバー空間に収集して分析することで，生活のあらゆる時間・空間で有益なサービスが受けられるようになった．一方で，カメラやマイクロフォンを内蔵したスマートフォンの急速な普及や，メディア処理技術の進展により，人間という知的センサによって，現実空間で取得した画像，映像，音声などの情報をサイバー空間で無秩序に共有・分析することによる，プライバシー侵害やセキュリティ問題が懸念されている．特に人物の顔，音声，歩行動作，さらには指紋，静脈，虹彩といった生体情報が，遠隔からの撮影や録音を経て，サイバー空間に共有されることで，第三者が他人の生体情報を復元・合成し，他人になりすまして生体認証を突破する「なりすまし」の脅威が指摘されている．2017 年には研究代表者の越前が，市販のカメラで 3m の距離から撮影した人物のピース写真から指紋情報を復元し，指紋認証のなりすましに成功している．また，同年にはドイツに拠点を置くハッカー集団が，市販のカメラの夜間撮影モード（赤外カメラ）により撮影した顔写真から虹彩情報を復元し，スマートフォンの虹彩認証のなりすましに成功している．さらに，このような「なりすまし」は生体認証を欺くだけではなく，人間自身を直接的に欺く手段として，その脅威が指摘されている．取得した人物の顔や音声，身体動作などの情報をサイバー空間で合成することで，当該人物になりすまし，詐欺や詐称といった深刻な被害をもたらす可能性がある．生体情報は終生不変な情報であるため，生体情報の不正な取得や取得した生体情報を用いた「なりすまし」を防止することは，我々の生涯に関わる重要な課題である．

一方で生体認証は，パソコンやスマートフォンのユーザー認証だけではなく，入退室管理システムや決済サービスなど，本人認証の手段として広く普及しているため，本人認証の際には，生体情報をセキュリティカメラや指紋センサなどの生体認証センサにいつでも提供できるように利用者の利便性を確保する必要がある．すなわち，現実空間における本人認証の利便性を確保しながら，生体情報の不正な取得やサイバー空間への流通，取得した生体情報を用いた「なりすまし」を防止する技術群の確立が急務である．

２．研究の目的

本研究では，現実空間における生体認証の利便性を確保しながら，遠隔からの生体情報の取得や，サイバー空間における生体情報の流通を，本人の意思に応じて制御可能な技術群を確立する．期間内の研究目的を示す．

[目的 1] 現実空間における生体情報ジャミング機構の実現：カメラやマイクロフォンなどのセンサと人間との物理的距離に基づいて，センサを介した生体情報の復元を困難にする生体ジャミング機構を実現する．具体的には，生体認証時の近接距離における生体情報のセンシングは可能としながら，遠隔からのセンシングを経た生体情報の復元を困難にするジャミングパターンの生成・実装技術を確立する．
[目的 2] サイバー空間における生体情報匿名化機構の実現：カメラやマイクロフォンなどのセンサによって取得された複数の生体情報を含むメディア（画像，音声）の視聴者から見た違和感を最小限にしながら，当該メディアからの顔認識，話者認識などの認識アルゴリズムによる人物の特定や，「なりすまし」に必要な生体情報の抽出を困難にする匿名化メディア処理技術群を確立する．
[目的 3] 個人の利便性確保となりすまし防止を実現する生体情報保護活用基盤の構築：[目的 1]と[目的 2]で取り組んだ研究成果の知見を活用して，本人の意思に応じてサービス毎の生体情報の利用可否を柔軟に制御可能なポリシーベース生体情報制御機構を構築する．

３．研究の方法

[目的 1]現実空間における生体情報ジャミング機構の実現については，以下の 2 つの課題に取り組み，成果をプロトタイプとして試作する．

[課題 1-1] センサと人間との物理的距離に基づいて生体情報の復元を困難にするジャミングパターンの検討

[課題 1-2] 利便性とセキュリティを両立した生体情報ジャミング機構の実現

[目的 2]サイバー空間における生体情報匿名化機構の実現については，以下の 2 つの課題に取り組み，成果をプロトタイプとして試作する．

[課題 2-1] 生体への違和感を低減しながら個人識別と生体情報の復元を不能にする匿名化処理の検討

[課題 2-2] プライバシー侵害と「なりすまし」を防ぐ生体情報匿名化機構の実現

[目的 3]個人の利便性確保となりすまし防止を実現する生体情報保護活用基盤の構築については，以下の 2 つの課題に取り組む
[課題 3-1] 現実空間とサイバー空間の連携によるポリシーベース生体情報制御機構の実現
[課題 3-2] 生体情報保護活用基盤の構築・実証実験への取り組み

４．研究成果

2018年度は,[目的1] 現実空間における生体情報ジャミング機構の実現の以下の2つの課題,[課題 1-1]センサと人間との物理的距離に基づいて生体情報の復元を困難にするジャミングパターンの検討，および[課題 1-2]利便性とセキュリティを両立した生体情報ジャミング機構の実現，に取り組んだ．[課題 1-1]では，現実空間における生体認証の利便性を確保しながら，遠隔からの生体情報の取得や，サイバー空間における生体情報の流通を防止するために，近接距離での生体認証は可能としながら，遠隔からのセンシングを経た生体情報の復元や本人識別を困難にするジャミングパターンを検討した．ジャミングパターンは，顔，音声，指紋，静脈などの生体情報を対象として検討した．[課題 1-2]では，[課題 1-1]で検討したジャミングパターンを，指表面などに装着可能な形態として実装を行った．生体情報ジャミング機構を適用した生体部位に対して，視覚上の印象評価，近接距離における生体認証に対する精度評価，遠隔距離からセンシングした生体情報の妨害度合いの評価を行い，利便性とセキュリティを両立した生体情報ジャミング手法を実現した．2018 年 11 月に「写真からの指静脈パターン復元を防止する手法を提案」というタイトルで国立情報学研究所からニュースリリースを発出し，本件のシンポジウム論文がコンピュータセキュリティシンポジウム 2018 にて優秀論文賞を受賞した．

2019 年度は，[目的 2]サイバー空間における生体情報匿名化機構の実現，の以下の 2 つの課題,[課題 2-1]生体への違和感を低減しながら個人識別と生体情報の復元を不能にする匿名化処理の検討，および[課題 2-2]プライバシー侵害と「なりすまし」を防ぐ生体情報匿名化機構の実現に取り組んだ．[課題 2-1]では，話者認識，歩容認識などの生体認識を用いた人物の特定を困難にする匿名化メディア処理技術群を検討した．具体的には，深層学習（Deep Learning）を発展させた敵対的生成ネットワーク（GAN: Generative Adversarial Network）等により，画像，映像，音声メディアにおける生体への視聴覚的な違和感を低減しながら，生体情報の復元や上述の生体認識を不能にする匿名化メディア処理技術を検討した．また，生体情報を用いたなりすまし検知方法の基礎検討を行った．その結果，偽画像に微小なノイズを付加する敵対的サンプルと呼ばれる攻撃方法により，なりすまし検知方法による偽画像の検知が困難になることが分かったため，なりすまし検知の前処理として，敵対的サンプルを検知する方法についても検討を行った．[課題 2-2]では，[課題 2-1]で検討した匿名化技術に対して，匿名化処理されたメディアの視聴覚的な違和感，および生体認識の精度に対して，評価実験を実施し，検討した匿名化技術の有用性を検証した．

2020 年度は，[目的 3]個人の利便性確保となりすまし防止を実現する生体情報保護活用基盤の構築の以下の 2 つの課題,[課題 3-1]現実空間とサイバー空間の連携によるポリシーベース生体情報制御機構の実現，および[課題 3-2]生体情報保護活用基盤の構築・実証実験への取り組みを行った．[課題 3-1]では，現実空間とサイバー空間の連携により，本人の意思に応じてサービス毎の生体情報の利用可否を柔軟に制御可能なポリシーベース生体情報制御機構の検討を行った．具体的には顔や指紋，歩容といった多様なモダリティを対象に本人の意思に応じた生体情報の利用可否を制御可能な技術的手段を実現した．また，敵対的サンプル（Adversarial Examples）により生体情報の入手を困難にするプライバシー保護技術を確立し，評価実験により有効性を示した．[課題 3-2]では，主に[課題 3-1]で検討した複数の技術的手段の有効性を検証するために，大規模データセットの構築を含む評価実験を実施し，当該手段の有効性を示した

５．主な発表論文等

〔雑誌論文〕　計15件（うち査読付論文　14件／うち国際共著　6件／うちオープンアクセス　11件）

１．著者名 HIROSE Yuki、NAKAMURA Kazuaki、NITTA Naoko、BABAGUCHI Noboru	４．巻 E102.D
２．論文標題 Discrimination between Genuine and Cloned Gait Silhouette Videos via Autoencoder-Based Training Data Generation	５．発行年 2019年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 2535～2546
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2019EDP7042	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 Kazuaki Nakamura, Naoko Nitta, and Noboru Babaguchi	４．巻 Vol.14, No.5
２．論文標題 Encryption-Free Framework of Privacy-Preserving Image Recognition for Photo-Based Information Services	５．発行年 2019年
３．雑誌名 IEEE Transactions on Information Forensics and Security	６．最初と最後の頁 1264～1279
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIFS.2018.2876752	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 Bui Thach V.、Kuribayashi Minoru、Kojima Tetsuya、Haghvirdinezhad Roghayyeh、Echizen Isao	４．巻 27
２．論文標題 Efficient (nonrandom) Construction and Decoding for Non-adaptive Group Testing	５．発行年 2019年
３．雑誌名 Journal of Information Processing	６．最初と最後の頁 245～256
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.27.245	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Tieu Ngoc-Dung T.、Nguyen Huy H.、Nguyen-Son Hoang-Quoc、Yamagishi Junichi、Echizen Isao	４．巻 46
２．論文標題 Spatio-temporal generative adversarial network for gait anonymization	５．発行年 2019年
３．雑誌名 Journal of Information Security and Applications	６．最初と最後の頁 307～319
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jisa.2019.03.002	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Bui Thach V.、Kuribayashi Minoru、Cheraghchi Mahdi、Echizen Isao	4．巻 65
2．論文標題 Efficiently Decodable Non-Adaptive Threshold Group Testing	5．発行年 2019年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 5519～5528
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2019.2907990	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 ECHIZEN Isao、BABAGUCHI Noboru、YAMAGISHI Junichi、NITTA Naoko、NAKASHIMA Yuta、NAKAMURA Kazuaki、KONO Kazuhiro、FANG Fuming、MYOJIN Seiko、KUANG Zhenzhong、NGUYEN Huy H.、TIEU Ngoc-Dung T.	4．巻 E104.D
2．論文標題 Generation and Detection of Media Clones	5．発行年 2021年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 12～23
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2020MUI0002	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 Chang Ching-Chun、Wang Xu、Chen Sisheng、Echizen Isao、Sanchez Victor、Li Chang-Tsun	4．巻 11
2．論文標題 Deep Learning for Predictive Analytics in Reversible Steganography	5．発行年 2023年
3．雑誌名 IEEE Access	6．最初と最後の頁 3494～3510
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2023.3233976	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 該当する

1．著者名 Gao Kai、Chang Ching-Chun、Horng Ji-Hwei、Echizen Isao	4．巻 2022
2．論文標題 Steganographic secret sharing via AI-generated photorealistic images	5．発行年 2022年
3．雑誌名 EURASIP Journal on Wireless Communications and Networking	6．最初と最後の頁 2~11
掲載論文のDOI（デジタルオブジェクト識別子） 10.1186/s13638-022-02190-8	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 該当する

1．著者名 Chen Sisheng、Chang Ching-Chun、Echizen Isao	4．巻 9
2．論文標題 Steganographic Secret Sharing With GAN-Based Face Synthesis and Morphing for Trustworthy Authentication in IoT	5．発行年 2021年
3．雑誌名 IEEE Access	6．最初と最後の頁 116427～116439
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2021.3105590	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 該当する

1．著者名 Bui Thach V.、Cheraghchi Mahdi、Echizen Isao	4．巻 -
2．論文標題 Improved non-adaptive algorithms for threshold group testing with a gap	5．発行年 2020年
3．雑誌名 2020 IEEE International Symposium on Information Theory (ISIT)	6．最初と最後の頁 1414~1419
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISIT44484.2020.9174212	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 該当する

1．著者名 BABAGUCHI Noboru、ECHIZEN Isao、YAMAGISHI Junichi、NITTA Naoko、NAKASHIMA Yuta、NAKAMURA Kazuaki、KONO Kazuhiro、FANG Fuming、MYOJIN Seiko、KUANG Zhenzhong、NGUYEN Huy H.、TIEU Ngoc-Dung T.	4．巻 E104.D
2．論文標題 Preventing Fake Information Generation Against Media Clone Attacks	5．発行年 2021年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 2～11
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2020MUI0001	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 Nguyen Huy H.、Marcel Sebastien、Yamagishi Junichi、Echizen Isao	4．巻 4
2．論文標題 Master Face Attacks on Face Recognition Systems	5．発行年 2022年
3．雑誌名 IEEE Transactions on Biometrics, Behavior, and Identity Science	6．最初と最後の頁 398～411
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TBIOM.2022.3166206	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 NGUYEN Huy H.、KURIBAYASHI Minoru、YAMAGISHI Junichi、ECHIZEN Isao	4．巻 E105.D
2．論文標題 Effects of Image Processing Operations on Adversarial Noise and Their Use in Detecting and Correcting Adversarial Images	5．発行年 2022年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 65～77
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2021MUP0005	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 Chang Ching-Chun、Wang Xu、Chen Sisheng、Kiya Hitoshi、Echizen Isao	4．巻 82
2．論文標題 On the predictability in reversible steganography	5．発行年 2023年
3．雑誌名 Telecommunication Systems	6．最初と最後の頁 301～313
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s11235-022-00985-0	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 該当する

1．著者名 Ji Yi、Le Trung-Nghia、Nguyen Huy H.、Echizen Isao	4．巻 -
2．論文標題 Purifying Adversarial Images using Adversarial Autoencoder with Conditional Normalizing Flows	5．発行年 2023年
3．雑誌名 IEEE Open Journal of Signal Processing	6．最初と最後の頁 1～9
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/OJSP.2023.3275053	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 該当する

〔学会発表〕　計51件（うち招待講演　4件／うち国際学会　43件）

1．発表者名 Yuki Hirose, Kazuaki Nakamura, Naoko Nitta, and Noboru Babaguchi
2．発表標題 Anonymization of Gait Silhouette Video by Perturbing Its Phase and Shape Components
3．学会等名 Proc. of Asia-Pacific Signal and Processing Association Annual Summit and Conference (APSIPA ASC 2019)（国際学会）
4．発表年 2019年

１．発表者名
H. Luong and J. Yamagishi

２．発表標題
Bootstrapping Non-Parallel Voice Conversion from Speaker-Adaptive Text-to-Speech

３．学会等名
2019 IEEE Automatic Speech Recognition and Understanding Workshop (ASRU)（国際学会）

４．発表年
2019年

１．発表者名
Shuhei Kato, Yusuke Yasuda, Xin Wang, Erica Cooper, Shinji Takaki, Junichi Yamagishi

２．発表標題
Rakugo speech synthesis using segment-to-segment neural transduction and style tokens : toward speech synthesis for entertaining audiences

３．学会等名
10th ISCA Speech Synthesis Workshop（国際学会）

４．発表年
2019年

１．発表者名
Yusuke Yasuda, Xin Wang, Junichi Yamagishi

２．発表標題
Initial investigation of encoder-decoder end-to-end TTS using marginalization of monotonic hard alignments

３．学会等名
10th ISCA Speech Synthesis Workshop（国際学会）

４．発表年
2019年

１．発表者名
Xin Wang, Junichi Yamagishi

２．発表標題
Neural Harmonic-plus-Noise Waveform Model with Trainable Maximum Voice Frequency for Text-to-Speech Synthesis

３．学会等名
10th ISCA Speech Synthesis Workshop（国際学会）

４．発表年
2019年

１．発表者名
Fuming Fang, Xin Wang, Junichi Yamagishi, Isao Echizen, Massimiliano Todisco, Nicholas Evans, Jean-Francois Bonastre

２．発表標題
Speaker Anonymization Using X-vector and Neural Waveform Models

３．学会等名
10th ISCA Speech Synthesis Workshop（国際学会）

４．発表年
2019年

１．発表者名
Lauri Juvela, Bajibabu Bollepalli, Junichi Yamagishi, Paavo Alku

２．発表標題
GELP: GAN-Excited Linear Prediction for Speech Synthesis from Mel-Spectrogram

３．学会等名
Interspeech 2019（国際学会）

４．発表年
2019年

１．発表者名
Massimiliano Todisco, Xin Wang, Ville Vestman, Md Sahidullah, Hector Delgado, Andreas Nautsch, Junichi Yamagishi, Nicholas Evans, Tomi Kinnunen, Kong Aik Lee

２．発表標題
ASVspoof 2019: Future Horizons in Spoofed and Fake Audio Detection

３．学会等名
Interspeech 2019（国際学会）

４．発表年
2019年

１．発表者名
Mingyang Zhang, Xin Wang, Fuming Fang, Haizhou Li, Junichi Yamagishi

２．発表標題
Joint Training Framework for Text-to-Speech and Voice Conversion Using Multi-Source Tacotron and WaveNet

３．学会等名
Interspeech 2019（国際学会）

４．発表年
2019年

１．発表者名
S. Seshadri, L. Juvela, J. Yamagishi, O. Rasanen and P. Alku

２．発表標題
Cycle-consistent Adversarial Networks for Non-parallel Vocal Effort Based Speaking Style Conversion

３．学会等名
ICASSP 2019（国際学会）

４．発表年
2019年

１．発表者名
X. Wang, S. Takaki and J. Yamagishi

２．発表標題
Neural Source-filter-based Waveform Model for Statistical Parametric Speech Synthesis

３．学会等名
ICASSP 2019（国際学会）

４．発表年
2019年

１．発表者名
山岸 順一

２．発表標題
話者照合の生体検知チャレンジ「ASVspoof 2019」の概要と今後の展望

３．学会等名
第9回バイオメトリクスと認識・認証シンポジウム（招待講演）

４．発表年
2019年

１．発表者名
山岸 順一

２．発表標題
音声の個人性に関する多角的研究

３．学会等名
日本音響学会2019年秋季研究発表会（招待講演）

４．発表年
2019年

１．発表者名
山岸 順一

２．発表標題
フェイク動画問題: メディア解析技術によるアプローチ

３．学会等名
JST/CRDS 公開ワークショップ 「意思決定のための情報科学 ～情報氾濫・フェイク・分断に立ち向かうことは可能か～」（招待講演）

４．発表年
2019年

１．発表者名
Junichi Yamagishi

２．発表標題
Speaker Identity Cloning and Protection

３．学会等名
AFEKA SPEECH PROCESSING CONFERENCE 2019: 10-YEAR ANNIVERSARY CONFERENCE　Afeka Center for Language Processing (ACLP)（国際学会）

４．発表年
2019年

１．発表者名
T. V. Bui, M. Kuribayashi, T. Kojima, and I. Echizen

２．発表標題
Sublinear decoding schemes for non-adaptive group testing with inhibitors

３．学会等名
Proc. of the Theory and Applications of Models of Computation (TAMC 2019)（招待講演）

４．発表年
2019年

１．発表者名
Huy H. Nguyen, Junichi Yamagishi, and Isao Echizen

２．発表標題
Capsule-forensics: using capsule networks to detect forged images and videos

３．学会等名
IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)

４．発表年
2019年

１．発表者名
Fuming Fang, Xin Wang, Junichi Yamagishi, and Isao Echizen

２．発表標題
Audiovisual speaker conversion: jointly and simultaneously transforming facial expression and acoustic characteristics

３．学会等名
Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)（国際学会）

４．発表年
2019年

１．発表者名
Fuming Fang, Xin Wang, Junichi Yamagishi, Isao Echizen, Massimiliano Todisco, Nicholas Evans, Jean-Francois Bonastre

２．発表標題
Speaker Anonymization Using X-vector and Neural Waveform Models

３．学会等名
Proc. of the 10th ISCA Speech Synthesis Workshop (SSW10)（国際学会）

４．発表年
2019年

１．発表者名
Huy H. Nguyen, Fuming Fang, Junichi Yamagishi, Isao Echizen

２．発表標題
Multi-task Learning For Detecting and Segmenting Manipulated Facial Images and Videos

３．学会等名
Proc. of the BTAS 2019（国際学会）

４．発表年
2019年

１．発表者名
N. Teraura, I. Echizen, and K. Iwamura

２．発表標題
Implementation of a Digital Signature in Backward-Compatible QR Codes Using Subcell Division and Double Encoding

３．学会等名
Proc. of the Innovative Mobile and Internet Services in Ubiquitous Computing(IMIS2019)（国際学会）

４．発表年
2019年

１．発表者名
Ngoc-Dung T. Tieu, Huy H. Nguyen, Fuming Fang, Junichi Yamagishi, Isao Echizen

２．発表標題
An RGB Gait Anonymization Model for Low Quality Silhouette

３．学会等名
roc. of the AsiaPacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2019)（国際学会）

４．発表年
2019年

１．発表者名
David Ifeoluwa Adelani, Haotian Mai, Fuming Fang, Huy H. Nguyen, Junichi Yamagishi, Isao Echizen,

２．発表標題
Generating Sentiment-Preserving Fake Online Reviews Using Neural Language Models and Their Human- and Machine-based Detection

３．学会等名
Advanced Information Networking and Applications (AINA 2020)（国際学会）

４．発表年
2020年

１．発表者名
H. H. Nguyen, T. N.-D. Tieu, H.-Q. Nguyen-Son, J. Yamagishi, and I. Echizen

２．発表標題
Transformation on Computer-Generated Facial Image to Avoid Detection by Spoofing Detector

３．学会等名
IEEE International Conference on Multimedia and Expo (ICME) 2018（国際学会）

４．発表年
2018年

１．発表者名
H. H. Nguyen, T. N.-D. Tieu, H.-Q. Nguyen-Son, V. Nozick, J. Yamagishi, and I. Echizen

２．発表標題
Modular Convolutional Neural Network for Discriminating between Computer-Generated Images and Photographic Images

３．学会等名
International Conference on Availability, Reliability and Security (ARES 2018)（国際学会）

４．発表年
2018年

１．発表者名
T. Ogane and I. Echizen

２．発表標題
BiometricJammer: Use of pseudo fingerprint to prevent fingerprint extraction from camera images without inconveniencing users

３．学会等名
IEEE International Conference on Systems, Man, and Cybernetics (SMC2018)

４．発表年
2018年

１．発表者名
D. Afchar, V. Nozick, J. Yamagishi, and I. Echizen

２．発表標題
MesoNet: a Compact Facial Video Forgery Detection Network

３．学会等名
MesoNet: a Compact Facial Video Forgery Detection Network, " Proc. of the IEEE International Workshop on Information Forensics and Security (WIFS 2018)（国際学会）

４．発表年
2018年

１．発表者名
F. Fang, J. Yamagishi, I. Echizen, MD Sahidullah , T. Kinnunen

２．発表標題
Transforming acoustic characteristics to deceive playback spoofing countermeasures of speaker verification systems

３．学会等名
IEEE International Workshop on Information Forensics and Security (WIFS 2018)（国際学会）

４．発表年
2018年

１．発表者名
大金 建夫、越前 功

２．発表標題
可視画像からの指静脈認証のなりすまし可能性の検討とその対策手法

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム 2018（CSS2018）

４．発表年
2018年

１．発表者名
H.-Q. Nguyen-Son, H. H. Nguyen, N.-D. Tieu, J. Yamagishi, and I. Echizen

２．発表標題
Identifying Computer-Translated Paragraphs using Coherence Features

３．学会等名
Pacific Asia Conference on Language, Information and Computation (PACLIC 32)（国際学会）

４．発表年
2018年

１．発表者名
Kazuhiro Kono, Takaaki Yoshida, Shoken Ohshiro, and Noboru Babaguchi

２．発表標題
Passive video forgery detection considering spatio-temporal consistency

３．学会等名
International Conference on Information Assurance and Security (IAS)

４．発表年
2018年

１．発表者名
David Ifeoluwa Adelani, Haotian Mai, Fuming Fang, Huy H. Nguyen, Junichi Yamagishi, Isao Echizen,

２．発表標題
Generating Sentiment-Preserving Fake Online Reviews Using Neural Language Models and Their Human- and Machine-based Detection

３．学会等名
Advanced Information Networking and Applications (AINA 2020)（国際学会）

４．発表年
2020年

１．発表者名
Huy H. Nguyen, Junichi Yamagishi, Isao Echizen, Sebastien Marcel

２．発表標題
Generating Master Faces for Use in Performing Wolf Attacks on Face Recognition Systems

３．学会等名
IJCB 2020（国際学会）

４．発表年
2020年

１．発表者名
Rong Huang, Fuming Fang, Huy H. Nguyen, Junichi Yamagishi, Isao Echizen

２．発表標題
Security of Facial Forensics Models Against Adversarial Attacks

３．学会等名
ICIP 2020（国際学会）

４．発表年
2020年

１．発表者名
S. Gupta, H. Nguyen, J. Yamagishi, and I. Echizen

２．発表標題
Viable Threat on News Reading: Generating Biased News Using Natural Language Models

３．学会等名
Proc. of the NLP+CSS Workshop at EMNLP 2020（国際学会）

４．発表年
2020年

１．発表者名
R. Huang, F. Fang, H. Nguyen, J. Yamagishi, and I. Echizen

２．発表標題
A Method for Identifying Origin of Digital Images using a Convolutional Neural network

３．学会等名
Proc. of the APSIPA Annual Summit and Conference 2020 (APSIPA ACS 2020)（国際学会）

４．発表年
2020年

１．発表者名
N. Tieu, J. Yamagishi, and I. Echizen

２．発表標題
Color Transfer to Anonymized Gait Images While Maintaining Anonymization

３．学会等名
Proc. of the APSIPA Annual Summit and Conference 2020 (APSIPA ACS 2020)（国際学会）

４．発表年
2020年

１．発表者名
H. Kaur, I. Echizen, and R. Kumar

２．発表標題
Smart Data Agent for Preserving Location Privacy

３．学会等名
Proc. of the 2020 IEEE Symposium Series on Computational Intelligence (SSCI) (SSCI 2020)（国際学会）

４．発表年
2020年

１．発表者名
Khanh-Duy Nguyen, Huy H. Nguyen, Trung-Nghia Le, Junichi Yamagishi, Isao Echizen

２．発表標題
Effectiveness of Detection-based and Regression-based Approaches for Estimating Mask-Wearing Ratio

３．学会等名
The International Workshop on Face and Gesture Analysis for COVID-19 (FG4COVID19) held in conjunction with FG 2021 (（国際学会）

４．発表年
2021年

１．発表者名
Sosuke Nishikawa, Ikuya Yamada, Yoshimasa Tsuruoka, Isao Echizen

２．発表標題
A Multilingual Bag-of-Entities Model forZero-Shot Cross-Lingual Text Classification

３．学会等名
ACL-IJCNLP 2021 Student Research Workshop (non-archival option)（国際学会）

４．発表年
2021年

１．発表者名
Trung-Nghia Le, Huy H. Nguyen, Junichi Yamagishi, Isao Echizen

２．発表標題
OpenForensics: Large-Scale Challenging Dataset For Multi-Face Forgery Detection And Segmentation In-The-Wild

３．学会等名
ICCV 2021（国際学会）

４．発表年
2021年

１．発表者名
Harkeerat Kaur, Rohit Kumar, and Isao Echizen

２．発表標題
Reinforcement Learning based Smart Data Agent for Location Privacy

３．学会等名
The 35th International Conference on Advanced Information Networking and Applications (AINA-2021)（国際学会）

４．発表年
2021年

１．発表者名
Marc Treu, Trung-Nghia Le, Huy H. Nguyen, Junichi Yamagishi, Isao Echizen

２．発表標題
Fashion-Guided Adversarial Attack on Person Segmentation

３．学会等名
omputer Vision and Pattern Recognition WORKSHOP ON MEDIA FORENSICS 2021（国際学会）

４．発表年
2021年

１．発表者名
Sosuke Nishikawa, Ikuya Yamada, Yoshimasa Tsuruoka, Isao Echizen

２．発表標題
A Multilingual Bag-of-Entities Model for Zero-Shot Cross-Lingual Text Classification

３．学会等名
The SIGNLL Conference on Computational Natural Language Learning (CoNLL 2022)（国際学会）

４．発表年
2022年

１．発表者名
Trung-Nghia Le, Ta Gu, Huy H. Nguyen, Isao Echizen

２．発表標題
Rethinking Adversarial Examples for Location Privacy Protection

３．学会等名
IEEE International Workshop on Information Forensics and Security, 2022 (WIFS 2022)（国際学会）

４．発表年
2022年

１．発表者名
Minh-Quan Le, Trung-Nghia Le, Tam V. Nguyen, Isao Echizen, Minh-Triet Tran

２．発表標題
GUNNEL: Guided Mixup Augmentation and Multi-View Fusion for Aquatic Animal Segmentation

３．学会等名
CV4Animal Workshop, CVPR 2022（国際学会）

４．発表年
2022年

１．発表者名
Sosuke Nishikawa, Ryokan Ri, Ikuya Yamada, Yoshimasa Tsuruoka and Isao Echizen

２．発表標題
EASE: Entity-Aware Contrastive Learning of Sentence Embedding.

３．学会等名
NAACL 2022（国際学会）

４．発表年
2022年

１．発表者名
H. Kaur, R. Shukla, I. Echizen, and P. Khanna

２．発表標題
Secure and Privacy Preserving Proxy Biometrics Identities

３．学会等名
AINA 2023（国際学会）

４．発表年
2023年

１．発表者名
Y. Sun, Z. Zhang, I. Echizen, H. H. Nguyen, C. Qiu, and S. Lu

２．発表標題
Face Forgery Detection Based on Facial Region Displacement Trajectory Series

３．学会等名
Winter Conference on Applications of Computer Vision Workshop (WACV-W) 2023（国際学会）

４．発表年
2023年

１．発表者名
Futa Waseda, Sosuke Nishikawa, Trung-Nghia Le, Huy H. Nguyen, and Isao Echizen

２．発表標題
Closer Look at the Transferability of Adversarial Examples: How They Fool Different Models Differently

３．学会等名
IEEE/CVF Winter Conference on Applications of Computer Vision (WACV 2023)（国際学会）

４．発表年
2023年

１．発表者名
Huy H. Nguyen, Trung-Nghia Le, Junichi Yamagishi, and Isao Echizen

２．発表標題
Analysis of Master Vein Attacks on Finger Vein Recognition Systems

３．学会等名
IEEE/CVF Winter Conference on Applications of Computer Vision (WACV 2023)（国際学会）

４．発表年
2023年

〔図書〕　計3件

１．著者名	４．発行年
Mahdi Khosravy, Isao Echizen, Noboru Babaguchi	2022年
２．出版社	５．総ページ数
Springer	289
３．書名	
Frontiers in Fake Media Generation and Detection	

１．著者名	４．発行年
越前 功, 馬場口 登, 笹原 和俊	2022年
２．出版社	５．総ページ数
映像情報メディア学会	-
３．書名	
映像情報メディア学会誌（2022年07月号）特集：インフォデミック時代のAIとサイバーセキュリティ"フェイクメディア克服の最前線"	

１．著者名 Trung-Nghia Le, Huy H Nguyen, 山岸順一, 越前功	４．発行年 2022年
２．出版社 映像情報メディア学会	５．総ページ数 -
３．書名 映像情報メディア学会誌（2022年07月号）特集：インフォデミック時代のAIとサイバーセキュリティ "Deepfake生成と検出の現状"	

〔出願〕　計1件

産業財産権の名称	発明者	権利者
話者変換装置，話者変換方法，学習装置，学習方法及びプログラム	房 福明，越前 功， 山岸 順一	大学共同利用機関法人情報・システム研究機構
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願2018-226844	2018年	国内

〔取得〕　計0件

〔その他〕

https://www.nii.ac.jp/news/release/2018/1106.html

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	馬場口　登 (Babaguchi Noboru) (30156541)	大阪大学・工学研究科・教授 (14401)	
研究分担者	山岸　順一 (Yamagishi Junichi) (70709352)	国立情報学研究所・コンテンツ科学研究系・教授 (62615)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関