様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ９ 月 ２５ 日現在

機関番号：８２６２６
研究種目：基盤研究(A)（一般）
研究期間：2013～2015
課題番号：２５２４００１７

研究課題名（和文）複数主体のバイオメトリクスデータベース管理と評価技術の研究

研究課題名（英文）Study on biometrics database management and evaluation technology of multiple entities

研究代表者

寶木　和夫（TAKARAGI, Kazuo）

国立研究開発法人産業技術総合研究所・情報技術研究部門・副研究部門長

研究者番号：６０４１７０３７

交付決定額（研究期間全体）：（直接経費）　　33,500,000円

研究成果の概要（和文）：ATM、災害対策等の観点から利用検討が進んでいる生体認証について、今後、組織間連携など利用が広がるにつれて、生体認証精度のばらつきやユーザのプライバシ懸念、嫌悪感などバイオメトリクスデータ特有の課題が生じると予想される。そこで、生体情報のコピーを作成が可能ということを示したウルフという安全性尺度を展開するとともに、プライバシに関して、k匿名性という概念を踏まえて、信頼性をおくことについてのこれまでの研究を発展させた。結果として、複数主体が管理する際のデータ連係における限界点の解明や、生体情報特有のユーザ感覚に対する解決法の提案などを行なうことができ、問題解決に向けて大きく前進した。

研究成果の概要（英文）：Biometrics is now progressing use study from the viewpoint of ATM, disaster preparedness and other applications. In near future, as its use spreads from single to inter-organizational cooperation, problem is expected to occur in the variations of biometric authentication accuracy, privacy concerns and disgust specific to biometrics. This study deploys the safety measure of Wolf that enables the spoofing of biological information and develops the prior studies about establishing the trust based on the concept of k-anonymity in the area of privacy. As a result, a critical point of data linkage by multiple entities is elucidated, a solution to the user feeling specific to biometrics is proposed, that would be a major step forward towards problem solving.

研究分野：暗号、情報セキュリティ

キーワード：暗号・認証等　セキュア・ネットワーク　アルゴリズム　情報システム　ディペンダブル・コンピューティング

１．研究開始当初の背景

バイオメトリクスは、我が国では、入国管理、銀行 ATM、ビル入退出管理などで使われ、また、災害対策、安全保障等の観点から利用検討が進んでいる。欧米やアジア、アフリカでも同様の動きとともに身分証明など新たな活用の動きが見られる。市場規模、成長率ともに大きい（世界約 7000 億円/年、20%）。これまで、バイオメトリクスは組織単体での採用がほとんどであった。今後、組織間連携など利用が広がるにつれ、生体認証精度のばらつきやユーザのプライバシ懸念、嫌悪感などバイオメトリクスデータ特有の問題が顕著になる。バイオメトリクスがコモディティ化する前に、この問題を解決しなければならかった。

２．研究の目的

過去に生体認証とプライバシの検討を行った経験の両面を踏まえ、今回は一つの団体でのデータ管理だけではなく、複数の管理者のデータベース構築の困難さと信頼性という概念を持ち込むことに着目し、複数主体のバイオメトリクスデータベース管理と評価技術の研究を行なう。

３．研究の方法

生体認証は、パスワードや物による認証と違い、忘却や紛失の恐れがなく、漏洩や盗難が困難であることから様々な場に利用されている。また、本人以外の人がなりすます危険性が少ないことから、入国管理や厳格なセキュリティゲートでの利用といった、国単位での利用がある。同時に、民間において、日本においては一部の銀行での利用がされる中、欧州での銀行においても利用が検討されるなど、利用範囲が急激に拡大しつつある。こういった利用は、収集したデータの管理者が国というとても信頼できる団体や、民間であっても管理の範囲が限られるような単体の団体が行うことで、プライバシやユーザの嫌悪感の問題の解決を図ることで利用の範囲を増やしてきた。

しかし、今後は、複数の所属を持つ管理者が入り乱れてデータの管理を行うことが考えられる。例えば、欧州での銀行は他銀行においてもお金を引き出すことが可能で有り、そういったデータのやりとりなどが考えられる。また、バイオメトリクスの利用が簡便であることを活用して、民間の利用の場所拡大から、収集者と利用者が違うようなサービスの活用も考えられる。特に生体認証装置は、価格の幅も広がり、非常に安価で携帯電話にのるようなものから、生体反応を検出するような方式や３Ｄでのデータ解析が可能となるような高価なものまで様々あり、今後より身近に利用されるような製品となることが考えられる。このようなセキュリティ用途が多岐にわたるにつれ、従来の一元的なデータ管理ではなく、複数の主体が複数のポリシーで管理する必要性が出てきている。

今回、特に生体認証の認証方式の安全性において、本人拒否率や他人受け入れ率という尺度だけでは不十分であることを示し、生体情報のコピーを作成が可能ということを示したウルフという安全性尺度を展開する。同時に、プライバシに関して、データ管理者がある決まりに従って本人が特定不可能とするデータを作成する k 匿名性という概念を踏まえて、信頼性をおくとはどのようなことかについてのこれまでの研究を発展させる。そのためのキー技術として、信頼できるバイオメトリクス認証精度評価技術および関連するデータベース構築手法の研究を行う。

４．研究成果

本研究を通じて次の成果を得た。

（1）複数主体が管理する際のデータ連係における限界点の解明： Ground Truth データに基づく情報量分析の研究結果を反映し、複数組織連携データ管理・認証システムにおいて組み合わせ可能なデータサイズを測定し、達成可能な信頼性の限界を示した。

（2）複数組織連携データベースにおけるプライバシ保護データ管理技術の研究開発：信頼のできる認証方式や端末を活用する Trust の概念を導入した課題の解決法を提案し、基本的なデータベースモデルに対する管理技術を応用して、高信頼性を有する複数組織連携のバイオメトリクス ID 連携技術の研究開発を行った。

（3）生体情報特有のユーザ感覚に対する解決法の提案： 生体情報には、プライバシ情報の収集に関して嫌悪感がある、という課題がある。嫌悪感の払拭には、インセンティブを与える方法が考えられる。インセンティブの定量化とプライバシの関係について、生体情報に限らずより一般にユーザ登録時の要求情報がシステムに与える影響をセキュリティエコノミクスの実証分析で明らかにした。さらに、その実証分析用に応用範囲の広い分析手法を開発した。とくに、脅威と脆弱性に分けて代理変数を設定する手法は、バイオメトリクス普及時により詳しい分析を実施し技術的改善の知見を出す際に有用である。本研究では、一つの事例として、脆弱性指標算出から得た知見に基づいて、証明可能安全性を持つフォールバック認証技術を開発した。また、個人情報保護法の改正が行われ、バイオメトリクスも保護対象として明文化される方向にある。監視カメラや、追跡利用における２次利用時の法的、技術的、社会的な問題を明確にした。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 20 件）

(1)大木 哲史、大塚 玲、宝木 和夫、「生体認

証装置に対するなりすまし行為の現状と課題」、電子情報通信学会バイオメトリクス研究会資料、BIOX2013-16、2013 年、pp.59-64.
(2) 瀬戸 洋一、「バイオメトリクスとプライバシー」、情報規格調査会 NEWSLETTER、vol. 99、2013 年、pp.3-9.
(3) Bongkot Jenjarrussakul, Hideyuki Tanaka, Kanta Matsuura、”Sectoral and Regional Interdependency of Japanese Firms under the Influence of Information Security Risks ”(In Rainer Boehme (ed.), The Economics of Information Security and Privacy, In Rainer Boehme (ed.), The Economics of Information Security and Privacy, 2013 年、pp.115-134.
(4) 宝木 和夫、「セキュリティ技術標準化の軌跡 ー 暗号からクラウド, M2M のセキュリティ標準まで ー」、電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, Vol.7, No.1, 2013 年、pp.51-59.
(5) 宝木 和夫、「情報セキュリティの新しい課題について」、日本セキュリティマネジメント学会誌、28 巻 1 号、2014 年、pp.36-43.
(6) 大木 哲史, 大塚 玲, 甲藤 二郎、「GMM-UBM に基づく話者認識方式のウルフ安全性評価」、電子情報通信学会論文誌 A、vol.J97-A,No.12、2014 年、pp.726-734.
(7) 宝木 和夫、「オリンピックのセキュリティ」、情報処理 / 情報処理学会 編、Vol.55, No.11、2014 年、pp.1196-1203.
(8) Aysajan Abidin, Kanta Matssura, Aikaterini Mitrokotsa, “ Security of a Privacy-Preserving Biometric Authentication Protocol Revisited, ” Lecture Notes in Computer Science, 8813, 2014 年、pp.290-304.
(9) Bongkot Jenjarrussakul, Kanta Matsuura, “ Japanese Loyalty Programs: An Empirical Analysis on their Liquidity, Security Efforts, and Actual Security Levels, ” 日本セキュリティ・マネジメント学会誌、vol. 28, 2014 年、pp.17-32.
(10) Sanggyu Shin, Yoichi Seto, Sadamu Takasaka, Eiichi Sekizuka, 「個人情報影響評価の電子カルテシステムへの適用」、Korea Information Processing Society Review, Vol. 21, No. 5, 2014 年、pp.64-72.
(11) 瀬戸洋一、「バイオメトリック認証技術の研究開発と製品化への期待」、IEICE Fundamentals Review, Vol.8、No.2, 2014 年、pp.77-83.
(12) 瀬戸洋一、「バイオメトリック製品の世界市場の俯瞰」、月刊自動認識、2014 年 4 月号、2014 年、pp.55-62.
(13) 瀬戸洋一、「第５回バイオメトリクスとプライバシー前編」、月刊自動認識、2014 年 8 月号、2014 年、pp.58-63.
(14) 瀬戸洋一、「第６回バイオメトリクスとプライバシー後編」、月刊自動認識、2014 年９月号、2014 年、pp.51-58.
(15) Snaggy Shin, Yoichi Seto, “A Study of Cancelable Biometrics in the Security Improvement of Biomestric Authentication System Using Fault Tree Analysis,” International Journal of Affective Engineering, 2016.
(16) Shiori Shinoda and Kanta Matsuura, “Empirical Investigation of Threats to Loyalty Programs by Using Models Inspired by the Gordon-Loeb's Formulation of Security Investment,” Journal of Information Security, vol.7, 2016, pp.29-48.
(17) 村山 優子, 松浦 幹太, 西垣 正勝、「セキュリティ技術の人間的側面に関する研究領域の紹介」、ヒューマンインタフェース学会誌、vol.17, 2015, pp.188-193.
(18) Sven Wohlgemuth, Kazuo Takaragi and Isao Echizen, “Privacy with Secondary Use of Personal Information,” EU-Japan Newsletter - Jun 2016 Issue, Jun 2016, pp.25-25.
(19) 大木 哲史, 大塚 玲、「人工物を用いた生体認証装置の性能推定について」、電子情報通信学会 信学技報、115(117)、2015 年、pp.73-78.
(20) 大木 哲史、大塚 玲、「人工物を用いた生体認証装置の性能推定について（その 2)」、電子情報通信学会 信学技報、115(188)、2015 年、pp.39-44.

〔学会発表〕（計 34 件）
（1）豊丹生祐輝, 西内 信之、「バイオメトリック認証における連続する認証エラーに対するユーザ行動」、学会等名日本人間工学会アーゴデザイン部会主催 コンセプト事例発表会 2013、首都大学東京、2013 年 9 月 2 日.
（2）豊丹生 祐輝, 西内 信之、「バイオメトリック認証における連続する認証エラーに対するストレスの評価」、電子情報通信学会バイオメトリクス時限研究専門員会主催、第 3 回バイオメトリクスと認識・認証シンポジウム、日本科学未来館、2013 年 11 月 26 日 ～2013 年 11 月 27 日.
（3）慎祥 揆、瀬戸 洋一、「韓国におけるプライバシー影響評価の制度と実施状況」、暗号と情報セキュリティシンポジウム SCIS 2014、鹿児島市、2014 年 1 月 23 日 ～2014 年 1 月 23 日.
（4）大木 哲史, 大塚 玲、「尤度比に基づく生体認証方式の脆弱性とウルフ安全性評価」、暗号と情報セキュリティシンポジウム 2015(SCIS2015)、リーガロイヤルホテル小倉、2015 年 1 月 20 日～2015 年 1 月 23 日.
（5）宝木 和夫、社会インフラへのバイオメトリクス適用状況と課題、電子情報通信学会 BioX ITE-ME ITE-IST、金沢大学 角間キャンパス、2014 年 6 月 16 日～2014 年 6 月 17

日
(6) Tetsushi Ohki, Akira Otsuka “ Theoretical vulnerability in likelihood-ratio-based biometric verification, ” Biometrics (IJCB), 2014 IEEE International Joint Conference on Biometrics, Clearwater, Florida, USA, 2014 年 9 月 29 日～2014 年 10 月 2 日.
（7） Bongkot Jenjarrussakul, Kanta Matsuura, “Analysis of Japanese Loyalty Programs Considering Liquidity, Security Efforts, and Actual Security Levels ” 13th Workshop on the Economics of Information Security (WEIS2014), Pennsylvania, USA, 2014 年 6 月 23 日～2014 年 6 月 24 日.
(8) 篠田 詩織、松浦 幹太、「ロイヤルティプログラムのセキュリティインシデントインパクト分析に向けたポイント流動性の定義に対する考察」、2015 年暗号と情報セキュリティ・シンポジウム(SCIS2015)、リーガロイヤルホテル小倉、2015 年 1 月 20 日～2015 年 1 月 23 日.
(9) Bongkot Jenjarrussakul, Kanta Matsuura、”Impact from Security Incidents and Partnership in Japanese Loyalty Program, ”
2015 年暗号と情報セキュリティ・シンポジウム(SCIS2015)、リーガロイヤルホテル小倉、2015 年 1 月 20 日～2015 年 1 月 23 日.
(10) 小泉 実沙子、西内 信之、「行動的特徴を用いた生体認証の連続エラーに対するユーザビリティ評価の提案」、日本人間工学会アーゴデザイン部会 2014 コンセプト事例発表会、首都大学東京、2014 年 9 月 16 日～2014 年 9 月 16 日.
(11) Sanggyu Shin, Yoichi Seto, Sadamu Takasaka, Eiichi Sekizuka, Evaluation of Privacy Impact Assessment for the Electronic Medical Record System in Saitama Hospital, The 2014 Fall Conference of the KIPS, Busan, Korea, 2014 年 11 月 7 日
～2014 年 11 月 7 日.
(12) 瀬戸 洋一、慎 祥揆、「バイオメトリクスのプライバシー性に関する一考察」、第 4 回バイオメトリクスと認識・認証シンポジウム、産業技術総合研究所臨海副都心センター、2014 年 11 月 25 日～2014 年 11 月 25 日.
(13) 西内 信之、小泉 実沙子、「リズム認証時の連続エラーに対するユーザビリティ評価」、電子情報通信学会 2015 年総合大会、立命館大学、2015 年 3 月 10 日～2015 年 3 月 10 日.
(14) 瀬戸 洋一、「ビッグデータ時代のバイオメトリクスにおけるプライバシー保護」、電子情報通信学会 2015 年総合大会、立命館大学、2015 年 3 月 11 日～2015 年 3 月 11 日.
(15) 大木 哲史, 大塚 玲、「尤度比に基づくバイオメトリック個人認証の脆弱性について」、バイオメトリクスと認識・認証シンポジウム 2014(SBRA2014)、産業技術総合研究所臨海副都心センター、2014 年 11 月 25 日～2014 年 11 月 26 日.
(16) 上田 周誠, 大木 哲史, 大塚 玲, 今井 秀樹、「人工物を用いた生体認証装置の性能評価」、バイオメトリクスと認識・認証シンポジウム 2014(SBRA2014)、産業技術総合研究所臨海副都心センター、2014 年 11 月 25 日～2014 年 11 月 26 日.
(17) 上田 周誠, 大木 哲史, 大塚 玲, 今井 秀樹、「人工物を用いた生体認証装置の性能評価法の提案」、暗号と情報セキュリティシンポジウム 2015(SCIS2015)、リーガロイヤルホテル小倉、2015 年 1 月 20 日～2015 年 1 月 23 日.
(18) Hiroya Susuki, Rie Shigetomi Yamaguchi, “User Authentication Trial by Behavior Data of Wearable Devices, ” International Workshop on Security (IWSEC 2014), 弘前大学、2014 年 8 月 27 日～2014 年 8 月 29 日.
(19) 鈴木 宏哉, 山口 利恵、「ウェアラブルデバイスを活用した個人の行動によるユーザ認証の検討」、暗号と情報セキュリティシンポジウム 2015(SCIS2015)、リーガロイヤルホテル小倉、2015 年 1 月 20 日～2015 年 1 月 23 日.
(20) 山口 利恵、坂本 静生、鈴木 宏哉、「スマートフォンを事例とする多要素認証確率の提案」、暗号と情報セキュリティシンポジウム 2015(SCIS2015)、リーガロイヤルホテル小倉、2015 年 1 月 20 日～2015 年 1 月 23 日.
(21) Snaggy Shin, Yoichi Seto, “ Can Cancelable Biometrics Contribute to the Security Improvement of Biometric Authentication Systems? ”ICCSA 2015 (国際学会)、Banff, Alberta, Canada, 2015 年 6 月 22 日～2015 年 6 月 25 日.
(22) Nobuyuki Nishiuchi, Yuki Buniu, “ Usability Evaluation for Continuous Error of Fingerprint Authentication, ” CIMIM 2015（国際学会）, Warsaw, Poland, 2015 年 9 月 24 日～2015 年 9 月 26 日.
(23) Sanggyu Shin, Yoichi Seto, “Study of Cancelable Biometrics in Security Improvement of Biometric Authentication System ICBAKE, ” CIMIM 2015（国際学会）, Warsaw, Poland, 2015 年 9 月 24 日～2015 年 9 月 26 日.
(24) 馬 小飛, 佐々木 真由美, 黒沢 裕太, 沖村 星児, 阪本 圭, 慎 祥揆, 瀬戸 洋一、「ネットワーク型多目的カメラシステムのプライバシー問題の検討」、2016 年電子情報通信学会総合大会、九州大学 伊都キャンパス（福岡市）、2016 年 3 月 16 日～2016 年 3 月 16 日.
(25) Andreas Gutmann, Karen Renaud, Joseph Maguire, Peter Mayer, Melanie, Volkamer, Kanta Matsuura, and Joern

Mueller-Quade, “ZeTA — Zero-Trust Authentication: Relying on Innate Human Ability, not Technology,” The 1st IEEE European Symposium on Security and Privacy（国際学会）, Saarbruecken, Germany, 2016 年 3 月 21 日～2016 年 3 月 24 日.
(26) 篠田 詩織, 松浦 幹太、「ロイヤルティプログラムのセキュリティインシデントに関する実証分析および制度設計の検討」、第 29 回日本セキュリティ・マネジメント学会全国大会、東京大学生産技術研究所, 東京都目黒区、2015 年 6 月 27 日～2015 年 6 月 27 日.
(27) 大畑 幸矢, 松田 隆宏, 松浦 幹太、「証明可能安全なパスワード再発行プロトコル・改」、CSS2015、長崎ブリックホール, 長崎市、2015 年 10 月 21 日～2015 年 10 月 23 日.
(28) 篠田 詩織, 松浦 幹太、「ロイヤルティプログラムのセキュリティに対するネットワーク分析指標に着目した考察」、CSS2015、長崎ブリックホール, 長崎市、2015 年 10 月 21 日～2015 年 10 月 23 日.
(29) 大畑 幸矢, 松田 隆宏, 松浦 幹太、「パスワード再発行プロトコルの安全性について」、SCIS2016、ANA クラウンプラザホテル熊本ニュースカイ, 熊本市、2016 年 1 月 19 日～2016 年 1 月 19 日.
(30) Sven Wohlgemuth, Kazuo Takaragi and Isao Echizen, “ Privacy with Secondary Use of Personal Information, ” MKWI2016（国際学会）, Ilmenau, Germany, 2016 年 3 月 3 日～2016 年 3 月 3 日.
(31) Akira Otsuka, Tetsuhi Ohki, “ Security Evaluation of vascular biometrics, ” IBPC2016（国際学会）, Gaithersburg, MD, 2016 年 5 月 3 日～2016 年 5 月 5 日.
(32) Ryosuke Kobayashi, Rie Shigetomi Yamaguchi, “ A Behavior Authentication Method Using Wi-Fi BSSIDs around Smartphone Carried by a User, ” CANDAR 2015, Sapporo, Hokkaido, Japan, 2015 年 12 月 08 日～2015 年 12 月 11 日.
(33) 鈴木 宏哉, 山口 利恵、「モバイル端末保持者の周辺無線 LAN AP のベンダー情報と時間帯の相関」、SCIS2016、ANA クラウンプラザホテル熊本ニュースカイ, 熊本市、2016 年 1 月 19 日～2016 年 1 月 19 日.
(34) 石川 寛朗, 鈴木 宏哉, 山口 利恵、「GINGERALE：ジェスチャ認識を用いたスマートグラスのための認証方式」、DICOMO2015、ホテル安比グランド、岩手、2015 年 07 月 08 日～2015 年 07 月 10 日.

〔図書〕（計 4 件）
(1)瀬戸 洋一、「高精度化する個人認証技術最前線、第３章バイオメトリック認証技術の標準化と市場動向」、NTS、2014 年、総ページ数 13.
(2) 山口 昌樹監修、瀬戸 洋一著、「ヒューマンインタフェースのための計測と制御　普及版、第９章　バイオメトリック認証技術」、シーエムシー出版、2014 年、総ページ数 18.
(3)瀬戸 洋一監修、「プライバシー影響評価ガイドライン実践テキスト」、インプレス、2016 年、総ページ数 160.
(4) 松浦 幹太、「サイバーリスクの脅威に備える ～私たちに求められるセキュリティ三原則」、化学同人、総ページ数 228.

〔産業財産権〕
○出願状況（計 0 件）

○取得状況（計 0 件）

〔その他〕
特になし。

６．研究組織
(1)研究代表者
寶木 和夫（TAKARAGI, Kazuo）
国立研究開発法人産業技術総合研究所・情報技術研究部門・副研究部門長
研究者番号：60417037

(2)研究分担者
今井 秀樹（IMAI, Hideki）
東京大学・名誉教授
研究者番号： 70017987

松浦 幹太（MATSUURA, Kanta）
東京大学・生産技術研究所・教授
研究者番号： 00292756

山口 利恵（繁富 利恵）（YAMAGUCHI, Rie）
東京大学・大学院情報理工学系研究科・特任准教授
研究者番号： 904431192

大塚 玲（OTSUKA, Akira）
国立研究開発法人産業技術総合研究所・情報技術研究部門・主任研究員
研究者番号： 50415650

瀬戸 洋一（SETO, Yoichi）
産業技術大学院大学・産業技術研究科・教授
研究者番号： 50417036

西内 信之（NISHIUCHI, Nobuyuki）
首都大学東京・システムデザイン研究科・准教授
研究者番号： 70301588

愼 祥揆（SHIN, Sang-Gyu）
産業技術大学院大学・産業技術研究科・助教

研究者番号： 60615540

以上