様式 C-19

科学研究費補助金研究成果報告書

平成 22 年 3 月 31 日現在

研究種目：基盤研究(A)
研究期間：2007～2009
課題番号：19200006
研究課題名（和文）　生体及び人工物の高精度・高信頼認識技術の研究

研究課題名（英文）　Biometrics and artifact-metrics with high performance and high reliability

研究代表者
今井　秀樹（IMAI HIDEKI）
中央大学・理工学部・教授
研究者番号：70017987

研究成果の概要（和文）：
本研究では，情報セキュリティ対策における最も重要で困難な，生体認証や人工物認証の安全性評価手法を確立するために，生体認証及び人工物認証における安全性の概念を構築し，その下で従来の生体認証や人工物認証について安全性評価を行うことで，高い安全性を有する新たな認証技術の実現を目指す．これにより，認証技術の客観的な安全性評価基準を与え，生体認証及び人工物認証の安全性標準策定に貢献する．

研究成果の概要（英文）：
The results of this research provide the definition of security for establishing a security evaluation of the general biometrics and artifact-metrics. Using this definition, we can define a new measure for having high efficiency and high reliability. In addition to this new measure, we make a contribution to decide on a standard of security against the general biometrics and artifact-metrics.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	13,300,000	3,990,000	17,290,000
2008 年度	12,000,000	3,600,000	15,600,000
2009 年度	12,400,000	3,720,000	16,120,000
年度			
年度			
総　計	37,700,000	11,310,000	49,010,000

研究分野：総合領域
科研費の分科・細目：情報学　計算機システム・ネットワーク
キーワード：個人認証技術，生体認証，人工物認証，他人受入率，本人拒否率，ウルフ攻撃確率

１．研究開始当初の背景

安全・安心な情報化社会の構築が政府の重点施策になってから既に久しいが、情報セキュリティに関わる問題は減るどころか次々と新たに発生している状況である。これは、ひとつには情報セキュリティ対策の多くが対症療法的であり，その場しのぎに終始しているからであろう．その根本的原因は安全性

評価の不十分さにある場合が多い．事実，情報セキュリティ対策の基盤技術でさえ，安全性の概念すら確立されていないものがある．そのような安全性が曖昧のままの基盤技術の上に構築された情報システムの安全性が理論的に明確に評価できるはずがない．情報システムの安全性評価を精密なものとしていくためには，情報セキュリティ対策の基盤技術の安全性評価手法を確立することが急務なのである．

情報セキュリティ対策の主要な基盤技術としては，暗号技術，生体認証技術，IC カードなどの人工物認証技術が挙げられる．これらの技術は今日の多くの社会的なシステムにおいて必須のものとなっている．

このうち，暗号はその安全性の概念が証明可能安全性理論等の登場により確立されてきた．これに対し，生体認証や人工物認証の安全性についてはその定義すら確立していない．また，今日の多くの社会システムで，計算能力の低い IC カードなどの小サイズ・小電力の人工物による認証技術が情報セキュリティ対策の切り札として導入されているが，これに関しても安全性に対する評価手法が確立されているわけではない．

生体認証や人工物認証において，このように安全性評価が困難であるのは，基本的には，生体や人工物を数学的に扱いやすい形にモデル化するのが困難であることによる．しかし，これらの認証の安全性評価が，今日の社会における情報システムの安全性を高める上で不可欠であるにも拘らず，生体認証や人工物認証に対する様々な攻撃を取り込んだモデル化の試みさえほとんど行われてはこなかった．既に生体認証や人工物認証は，製品の形で社会の広範囲に普及しており，これらの安全性を高めることは緊急の課題であり，極めて重要である．

２．研究の目的

本研究では，情報セキュリティ対策における最も重要で困難な，生体認証や人工物認証の安全性評価手法の確立を最終的な目標として，暗号理論の手法等を活用した安全性の概念を構築し，その下で安全な生体認証，人工物認証について研究を行う．本研究の成果として安全性基準のベースになる安全性概念やその定義が与えられることにより，将来の生体認証や人工物認証の安全性評価制度に向けた安全性基準に理論的根拠を与えることができることは大変意義深い．

３．研究の方法

本研究では，既存の最先端の技術を利用することで可能となる攻撃手法，コスト，実際的な意味で適切な安全性仮定の置き方について研究を行う．さらにこの結果を受け，生体及び人工物の高精度・高信頼認証技術に向けた数学的に厳密な安全性の定義と仮定，および安全性を満たす構成法について研究を行う．

４．研究成果

本研究の主な研究成果は以下のとおりである．

＜生体認証に関する研究＞

従来，生体認証システムの安全性は他人受入率で評価されてきたが，他人受入率は，偶然他人を受け入れてしまう確率であるため，システムの脆弱性をついて他人になりすますウルフ攻撃に対する安全性の評価には適していない．ウルフ攻撃に対する安全性の評価尺度としてウルフ攻撃確率があり，これは他人受入率より高度な安全性の評価尺度となるが，現状ではウルフ攻撃確率に基づく照合アルゴリズムの安全性評価は，まだ十分とは言えない．そこで本研究では，ウルフ攻撃を考慮した生体認証システムの安全性評価，及びその下で安全な構成法について，以下のような(1)～(7)の研究成果を上げた．

(1)　一般的に精度が高く安全と言われている虹彩認証システムでは，Daugman のアルゴリズムが広く使われており，まぶた等で虹彩の大半が隠れているような状況においても FAR を一定に保つための正規化法を取り入れているが，取得したアイリスコードの符号長に比例して二項分布の自由度が変化する仮定を置いているため，マスク箇所を意図的に選択して攻撃成功確率を最大化するタイプのウルフ攻撃を考慮していない．そこで，領域の分割と周波数成分ごとの情報を利用して，一般的に精度の高いといわれている虹彩認証においても，ウルフ攻撃確率が非常に高くなる場合があることが示された．

(2)　(1)の結果から，高い精度を持った生体認証アルゴリズムでもウルフ攻撃に対する安全性が十分でないことがあることが示されている．このことより，生体認証の安全性の評価には，他人受入率，本人拒否率に加えてウルフ攻撃確率の評価が必要である．しかしながら，ウルフ攻撃確率を算出することは非常に難しい．一般的な生体認証システムでは，ウルフの発見によってシステムが危険であることを示すのは容易であるが，発見できないからといって安全であるとは言えない．そこで本研究では，ウルフ攻撃確率の上界を一意に算出できる照合アルゴリズムを提案した．このアルゴリズムを用いることによ

り，他人受入率とウルフ攻撃確率は減少することが理論的に保証され，さらに照合するテンプレート数をn，誤一致ユーザ数をT-1（Tは自分を含めた一致ユーザ数）としたとき，ウルフ攻撃確率は T/n 以下となることを証明した．これにより，従来は困難であった，ウルフ攻撃に対して安全性の高い生体認証システムを容易に構築することができる．

(3) (2)で提案したアルゴリズムにおいて，ウルフ攻撃確率と他人受入率はトレードオフの関係にあり，照合するテンプレート数 n と一致許容数 T によって，それぞれは増減する．このトレードオフに対して，照合するテンプレート数 n のシステムが存在するとき，最適な一致許容数 T を選ぶことによって，FRR と WAP を同時に小さくすることができることを証明した．

(4) 一般に，ウルフ攻撃に対して安全かつ可用性の高い（本人拒否が多くなく，処理時間も短い）照合アルゴリズムは存在しないということが示されている．そこで，(2)で提案した照合アルゴリズムを虹彩認証と指紋認証の 2 つの認証システムにおいて実装し，従来の照合アルゴリズムと提案アルゴリズムの安全性と可用性の比較を行った．その結果，提案アルゴリズムは従来アルゴリズムと同程度の精度，及び処理時間を保ちつつ，ウルフ攻撃確率を大幅に減少できる，安全性と可用性の高い照合アルゴリズムであることが確かめられた．

(5) (2)でも述べたように，ある生体認証システムに対して，ウルフ攻撃確率を算出することは非常に難しい．そこで，指静脈認証システムにおける，特徴抽出アルゴリズムのウルフ攻撃への耐性を評価する手法として，あいまい領域の割合に基づく評価手法を提案した．提案手法は，認証アルゴリズムが公開されていない状態でも評価可能で，ウルフが存在するかどうかを自動的に発見し，そのウルフがどれだけの照合データと一致する可能性があるのかを評価できる．また，実験により，現在公開されている特徴抽出アルゴリズムに対し，100%なりすましが可能なウルフを発見することができた．この結果は，国際標準に影響を与えるような重要な成果である．

(6) (5)で提案した手法で発見できるウルフ（画像パターン）は，静脈パターンの入力センサを通過した後のウルフに限定されていた．そこで，この手法を改良して，入力センサによるノイズ付加を想定した過程を考慮した安全性評価手法を提案し，さらなる有効性の向上を図った．

(7) (5)で提案した手法は，特定の静脈認証システムに対して，効率的にウルフが探索できる手法であった．そこで，一般の認証システムに適用できるようなウルフ探索手法を提案した．提案手法は，遺伝的アルゴリズムを利用した手法である．この提案手法を用いて，3 つの指紋照合アルゴリズムを対象にウルフ探索を行い，探索結果からウルフ攻撃に耐性のあるアルゴリズムとそうでないものの判別に成功した．

以上のような研究成果から，生体認証システムの安全性評価に対して，ウルフ攻撃確率は極めて重要な評価基準であることがわかった．

＜人工物認証に関する研究＞

計算能力の低い IC カードなどの小サイズ・小電力の人工物を用いた認証技術に対して，インターネット環境等と同様のセキュリティ対策技術を適用すると，計算量等の面で問題が生じ，軽量端末への実装が非現実的となる場合がある．本研究では，小サイズ・小電力の人工物を用いた認証技術における現実的な安全性要件を検討し，実際に即した安全な認証技術の構築を目指すために以下のような研究を行った．

(1) 非対称暗号技術を適用し，プライバシを保護した認証プロトコルを実現するための手法を提案した．この手法は，計算能力の低い小型・省電力の装置での利用に適しており，全数探索や同期を必要としない有効な特性を持っていることがわかった．

(2) ID を埋め込んだタグとリーダ間で無線通信を介して認証を行う RFID システムに対して，利用者のプライバシを確保しつつ，ID 探索の効率化を図る方式を提案すると共に，低コストデバイスである RFID に適応できるようにタグ側に記憶する鍵のサイズを削減する方法を提案した．

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 11 件）

[1] Masatoshi Noguchi, Manabu Inuma,

Rie Shigetomi and Hideki Imai, An Image Sanitizing Scheme Using Digital Watermarking, Eleventh International Conference on Information and Communications Security (ICICS'09), Lecture Notes in Computer Science, vol. 5927, pp. 474-482, 2009, 査読有

[2] Yasuhiro Tanabe, Kazuki Yoshizoe and Hideki Imai, A Study on Security Evaluation Methodology for Image based Biometrics Authentication Systems, IEEE Third International Conference on Biometrics: Theory, Applications and Systems (BTAS 09), 2009, 査読有

[3] Yoshihiro Kojima, Rie Shigetomi, Manabu Inuma, Akira Otsuka and Hideki Imai, A Matching Algorithm Secure against the Wolf Attack in Biometric Authentication Systems, International Conference on Biometric ID Management and Multimodal Communication 2009, Lecture Notes in Computer Science, vol. 5707, pp. 293-300, 2009, 査読有

[4] Tomohiro Sekino, Kazukuni Kobara and Hideki Imai, Anti-Malware Order System Using Multiple Independent Terminals and Authentication Schemes, The 12th International Symposium on Wireless Personal Multimedia Communications (WPMC'09), 査読有

[5] Shigenori Yamakawa, Yang Cui, Kazukuni Kobara and Hideki Imai, Lightweight Broadcast Authentication Protocols Reconsidered, IEEE Wireless Communications & Networking Conference (WCNC2009), 2009, 査読有

[6] Masakazu Yoshida, Takayuki Miyadera and Hideki Imai, Separability Criterion in Prime Dimensions based on Landau-Pollak Uncertainty Relation, 2008 International Symposium on Information Theory and its Applications (ISITA2008), 2008, 査読有

[7] Takahiro Yoshida, Toshiyasu Matsushima and Hideki Imai, A Ramp Scheme for Key Predistribution System against Collusion of Users and Centers, 2008 International Symposium on Information Theory and its Applications (ISITA2008), 2008, 査読有

[8] Yuto Matsunaga, Manabu Hagiwara, Kazukuni Kobara and Hideki Imai, A Study on a Key Establishment Scheme with QC LDPC Codes and UH-Protocols, 2008 International Symposium on Information Theory and its Applications (ISITA2008), 2008, 査読有

[9] Rei Yoshida, Yang Cui, Rie Shigetomi and Hideki Imai, The Practicality of the Keyword Search using PIR, 2008 International Symposium on Information Theory and its Applications (ISITA2008), 2008, 査読有

[10] Rei Yoshida, Rie Shigetomi, Kazuki Yoshizoe, Akira Otsuka, and Hideki Imai, Lecture Notes in Computer Science 4945, Springer, Berlin, pp.1-12, 2008, 査読有

[11] Shigenori Yamakawa, Yang Cui, Kazukuni Kobara, Manabu Hagiwara and Hideki Imai, On the Key-Privacy Issue of McEliece Public-Key Encryption, 17th International Symposium Applied Algebra, Algebraic Algorithms, and Error Correcting Codes(AAECC-17), Lecture Notes in Computer Science 4851, pp.168-177, 2007, 査読有

〔学会発表〕（計 46 件）

[1] 関野智啓，崔洋，古原和邦，今井秀樹，プライバシを考慮したRFID向け個別化公開鍵暗号方式に関する考，2010 年暗号と情報セキュリティシンポジウム(SCIS2010)，2010 年 1 月 22 日，香川県高松市

[2] 恩田泰則, 辛星漢, 古原和邦, 今井秀樹，2010 年暗号と情報セキュリティシンポジウム(SCIS2010), 2010 年 1 月 21 日，香川県高松市

[3] 小島由大，繁富利恵，井沼学，大塚玲，今井秀樹，ウルフ攻撃に対して安全な照合アルゴリズム ～しきい値の最適化と虹彩認証を用いた実験～，2010 年暗号と情報セキュリティシンポジウム(SCIS2010)，2010 年 1 月 20 日，香川県高松市

[4] 田辺康宏，美添一樹，今井秀樹，指紋照合アルゴリズムにおけるウルフ探索，2010 年暗号と情報セキュリティシンポジウム(SCIS2010), 2010 年 1 月 20 日，香川県高松市

[5] 山川茂紀，崔洋，古原和邦，今井秀樹，On the Security of Quasi-Dyadic Code-Based Signature and Its Application to Broadcast

Authentication，2010 年暗号と情報セキュリティシンポジウム(SCIS2010)，2010 年 1 月 20 日，香川県高松市
[6] 鈴木智也，田沼均，堀洋平，今井秀樹，生体認証におけるリスク管理のための FTA 構成法の検討，2009 年暗号と情報セキュリティシンポジウム(SCIS2009)，2009 年 1 月 23 日，滋賀県大津市
[7] 小島由大，繁富利恵，井沼学，大塚玲，今井秀樹，ウルフ攻撃確率を考慮したマッチングアルゴリズムのフレームワーク における安全で可用性の高い認証プロトコル，2009 年暗号と情報セキュリティシンポジウム(SCIS2009)，2009 年 1 月 23 日，滋賀県大津市
[8] 田辺康宏，美添一樹，今井秀樹，指静脈認証システムにおけるウルフ探索アルゴリズムの拡張，2009 年暗号と情報セキュリティシンポジウム(SCIS2009)，2009 年 1 月 21 日，滋賀県大津市
[9] 小島由大，繁富利恵，井沼学，大塚玲，今井秀樹，バイオメトリクス認証におけるウルフ攻撃に対して安全な照合アルゴリズム，コンピュータセキュリティシンポジウム 2008（CSS2008），2008 年 10 月 10 日，沖縄県宜野湾市
[10] 小島由大，繁富利恵，井沼学，大塚玲，今井秀樹，虹彩認証におけるウルフ攻撃確率の理論的考察（その 2），第 13 回バイオメトリックシステムセキュリティ研究会，2008 年 6 月 25 日，東京都新宿区
[11] 田辺康宏，美添一樹，今井秀樹，指静脈認証システムにおける対ウルフ脆弱性の調査-探索アルゴリズムとウルフの性質を含めた考察-，第 13 回バイオメトリックシステムセキュリティ研究会，2008 年 6 月 25 日，東京都新宿区
[12] 小島由大，繁富利恵，井沼学，大塚玲，今井秀樹，虹彩認証におけるウルフ攻撃確率の理論的考察，2008 年暗号と情報セキュリティシンポジウム，2008 年 1 月 24 日，宮崎県宮崎市
[13] 田辺康宏，美添一樹，今井秀樹，指静脈認証システムにおけるセキュリティ評価手法の提案，2008 年暗号と情報セキュリティシンポジウム，2008 年 1 月 24 日，宮崎県宮崎市
[14] 白石桂一，美添一樹，今井秀樹，RFID を用いた位置情報取得における不正対策の検討，2008 年暗号と情報セキュリティシンポジウム，2008 年 1 月 23 日，宮崎県宮崎市
[15] 影山健，吉田怜，島田秋雄，美添一樹，今井秀樹，時刻取得による RFID トレーサビリティ情報の正当性の証明，2008 年暗号と情報セキュリティシンポジウム，2008 年 1 月 23 日，宮崎県宮崎市
[16] Miodrag Mihaljevic, Hajime Watanabe, Hideki Imai, RFID 認証アルゴリズムの安全性と複雑性評価，2008 年暗号と情報セキュリティシンポジウム，2008 年 1 月 23 日，宮崎県宮崎市
[17] 崔洋，古原和邦，今井秀樹，非対称符号ベースのパーベイシブデバイス認証プロトコル，第 30 回情報理論とその応用シンポジウム，2007 年 11 月 29 日，宮三重県志摩市

６．研究組織

(1)研究代表者
今井　秀樹（IMAI HIDEKI）
中央大学・理工学部・教授
研究者番号：70017987

(2)研究分担者
大塚　玲（OTSUKA AKIRA）
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・研究チーム長
研究者番号：50415650

(3)連携研究者
今福　健太郎（IMAHUKU KENTARO）
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・研究センター長
研究者番号：10298169
繁富　利恵（SHIGETOMI RIE）
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・研究員
研究者番号：90443192
美添　一樹（YOSHIZOE KAZUKI）
独立行政法人科学技術振興機構・量子情報システムアナーキテクチャ・研究員
研究者番号：80449115