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

平成 ２９ 年　 ７ 月　 ３ 日現在

機関番号：２１２０１
研究種目：基盤研究(C)（一般）
研究期間：2014～2016
課題番号：２６３３０１５９

研究課題名（和文）エンドユーザ保護のための包括的セキュリティ技術

研究課題名（英文）Multifarious Security Solution for Protecting End Users

研究代表者
高田　豊雄（Takata, Toyoo）

岩手県立大学・ソフトウェア情報学部・教授

研究者番号：５０２１６６５２

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：何らかのセキュリティを実現するシステムにおいて、人間を最も脆弱なシステム要素として狙う手法が増加している。一方、一般個人ユーザは充分な技術的知識やセキュリティ意識を有しているとは言い難い。本研究課題では、それらの問題を認知科学、HCI 等に関する最新の知見の導入により解決することを目的とする。主要な成果としては、1) スマートフォンの様々な組込みセンサを活用したキーストロークダイナミクス認証方式、2) パスワードリスト攻撃を防止するパスワード使い分けを支援する手法、3) インターネット観測システムの観測点検出攻撃防御手法、4) slow HTTP DOS 攻撃に対する防御手法、の確立がある。

研究成果の概要（英文）：In security systems, since attackers tend to aim most vulnerable part of the target system, the number of attacks are increasing that human as a component of the system is targeted. In this research project, we aim to resolve the above-mentioned problem by employing recent results of HCI or cognitive science. Concretely, as a main result, we establish the following that (1) an authentication scheme for smartphones with keystroke dynamics combined with outputs of various bulit-in smartphone sensors, (2) a password management scheme for proper use of several passwords against password list attack, (3) a method for preventing of a location attack using PN codes for internet threat monitoring, and (4) a defense method against various distributed slow HTTP DOS attacks.

研究分野：情報セキュリティ

キーワード：個人認証　スマートフォン　キーストロークダイナミクス　パスワード認証　ネットワークセキュリティ　インターネット観測システム　分散型サービス拒否攻撃　slow HTTP DOS

１．研究開始当初の背景

何らかのセキュリティを実現するシステムにおいて、攻撃者は、その最も弱い個所を狙う傾向があり、その結果、近年では人間を最も脆弱なシステム要素として狙う手法が増加している。例えば、近年増加傾向にある標的型攻撃では、ソーシャルエンジニアリング手法により攻撃の糸口を掴むことが常套的に行われていると指摘されている。更に、スマートフォン等の可搬型デバイスの普及により従来のセキュリティ技術を単純に応用することが困難な局面が生じている。

一方、脳科学、ヒューマンインタラクション、教育工学など、エンドユーザを対象とした学問領域が著しい進展を見せているが、セキュリティ分野への反映はまだまだ途上である。国外では、ユーザビリティ工学を反映させたセキュリティシステムについて、いち早くサーベイ集や国際会議 SOUPS が開かれている。一方国内では、早くからエンドユーザに着目したセキュリティ研究の重要性が主導的立場にある研究者から提唱されてきた(今井秀樹: ヒューマンクリプト、辻井重男: 情報社会のセキュリティと倫理の課題等)ものの、今日に至るまで学問領域として充分に立ち上がっているとはいえない。また、数年前より HCI 研究者の間で個人認証が研究対象となりつつあったが、セキュリティ研究の立場から安全性を充分吟味しているものとは言い難い。

２．研究の目的

本研究課題では、前述の問題を脳科学、HCI 等に関する最新の知見の導入により解決することを目的とする。具体的には、以下の３点の確立を行う。

1) 認知・記憶や HCI に関する最新の知見を採り入れた新しい個人認証手法の開発、
2) 新しい教育理論に基づくセキュリティ教材開発手法の確立、
3) 可搬型デバイスや SNS を対象としたエンドユーザ向けセキュリティツール・システム開発技法の確立を行う。

３．研究の方法

3.1 人間の認知や記憶のメカニズム, HCI の最新の研究知見に基づく個人認証方式の確立

運用容易性や経済性の点から、パスワード等の記憶に基づく個人認証方式は依然として盛んに利用されている。しかしながら、従来の記憶に基づく方式は、記憶容易性と安全性の折り合いをつけることが困難である。本研究の第一の目的は、最新の脳科学の研究成果(例えば、図的要素に関する記憶、意味記憶とエピソード記憶等)に基づく、記憶容易性と安全性の双方を両立させた記憶に基づく個人認証方式、ならびにスマートフォン等の可搬型デバイスの特質を活かし、HCIの最新知見を導入した個人認証方式の確立である。

3.2 セキュリティ対策に関する計算機援用教材開発方法論の確立

広く一般にスマートフォンやタブレット型コンピュータが普及すると共に、エンドユーザが様々なネットワーク犯罪(個人情報漏洩、詐欺等)に巻き込まれる事態が急増している。これらは従来の技術的対策で補いきれる問題ではなく、ユーザの知識不足やセキュリティ意識の欠如といった問題を、それぞれの性別や年齢層に相応しい形で解決する必要がある。

3.3 HCI に関する最新の知見を採り入れたセキュリティ対策ツール・システム開発技法の確立

リソース制約や搭載 OS のセキュリティモデルの特殊性により、可搬型デバイスのセキュリティ対策は、従来の対策手法、ツール(例えばアンチウィルスソフト)をそのまま適用することは有効ではない。また、近年、個人の情報発信が容易になっており、インターネット常時接続環境の普及と合わせ、エンドユーザの運営するサーバを保護する手法を確立する必要がある。最新のセキュリティ攻撃動向や HCI 研究の知見をにらみつつ、それらの課題を解決する。

４．研究成果

4.1 人間の認知や記憶のメカニズム, HCI の最新の研究知見に基づく個人認証方式の確立

4.1.1 スマートフォンのキーストロークダイナミクスを中心としたキー入力特徴に基づく個人認証方式

近年スマートフォンは電子商取引やインターネットバンキング等に利用され、内部に個人情報や秘密情報が大量に格納されている。そのためスマートフォンは攻撃者にとって格好の標的となっており、セキュリティ対策が急務となっている。スマートフォンのセキュリティ対策の一つにバイオメトリクス認証の一種であるキーストロークダイナミクス認証があり、報告者のグループを含め多くの研究がなされている。しかしそれらの多くは着席時や起立時を想定した認証方式である。スマートフォンは通勤通学など移動中に用いることが多くあり現実の利用局面のカバーが全く充分ではない。また、最近のスマートフォンは加速度センサ等様々なセンサを内蔵している一方、既存研究はそれらを充分使い切っているとは言えなかった。そこで本研究課題では移動を考慮し、スマートフォンの様々なセンサ出力を利用した個人認証方式を活用することである。

本課題ではキー入力時にフリック入力を仮定し、スマートフォンから得られる特徴量として次の 14 の特徴量を利用する。

・タッチパネルのキー入力操作の時間に関する特徴量(４種類，図1):

- Hold Time (HT): タッチパネルを押してから離すまでの時間
- KeyDown-KeyDown Time (DDT): タッチパネルを押してから次のキーを押すまでの時間
- KeyUp-KeyDown Time (UDT): タッチパネルを話してから次のキーを押すまでの時間
- KeyUp-KeyUp Time (UUT): タッチパネルを話してから次のキーを離すまでの時間

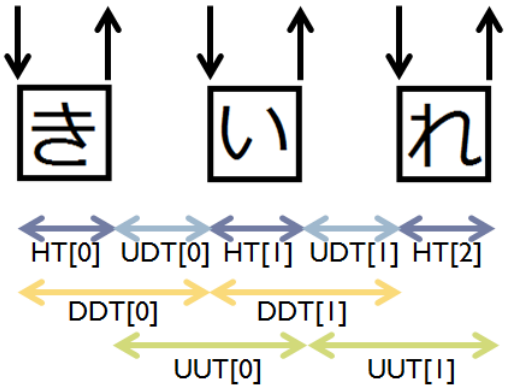

図 1: キー入力操作に関する特徴量

・フリック操作に関する特徴量(図 2, 3 種類)
- Flick Distance (FD): フリック入力時に指を押し続けた距離
- Flick Angle (FA): 指を押し始めた始点と離した終点のなす角度
- Flick Speed (FS): 指を押してから離すまでに動かした指の速度

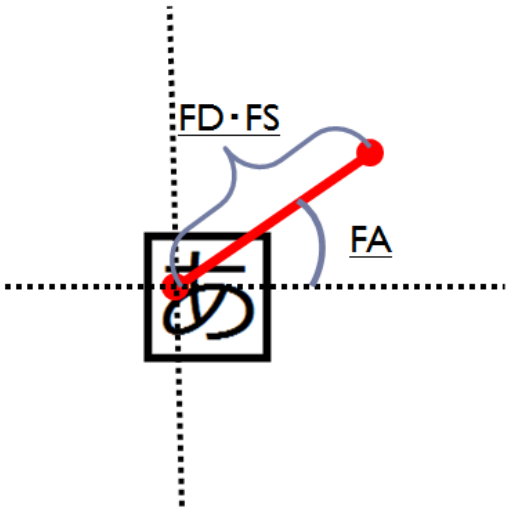

図 2: フリック操作に関する特徴量

・スマートフォンの様々な組込みセンサから得られる特徴量
- Finger Pressure (FP) : タッチパネルを押して離すまでの指圧の平均値. (0〜1 までに正規化された値)
- Touch Size (TS) : タッチパネルを押して離すまでのタッチ面積の平均値
- Event Count (EC) : タッチパネルを押して離すまでに発生したイベント数. Down, Move, Up イベントの合計値.
- Position (P) : タッチパネルを押して離すまでにタッチした座標の平均値. X 座標(横軸), Y 座標 (縦軸) から構成される.
- Acceleration (AC) : タッチパネルを押して離すまでのスマートフォンの単位時間当たりの速度の変化率 (加速度) の平均値. X 座標 (横軸), Y 座標 (縦軸), Z 座標 (手前軸) から構成される. (m/s^2)
- Angular Velocity (AV) : タッチパネルを押して離すまでのスマートフォンの回転の速さ (角速度) の平均値. X 座標 (横軸), Y 座標 (縦軸), Z 座標 (手前軸) から構成される. (rad/s)
- Orientation (O) : タッチパネルを押して離すまでのスマートフォンの傾きの平均値. Azimuth (外に向かう軸), Roll (端末上側の軸), Pitch (端末右向きの軸) から構成される. (rad)

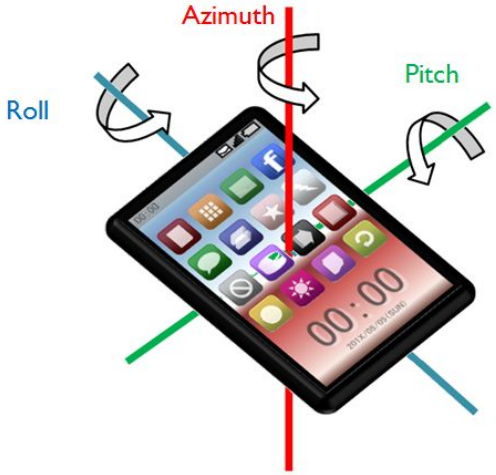

図 3 : スマートフォンの傾きに関する特徴量

登録された認証テンプレートと認証時の入力との比較照合には以下の 11 のアルゴリズムを用いることとする。
・Euclidean
・Euclidean (normed)
・Manhattan
・Manhattan (filtered)
・Manhattan (scaled)
・Mahalanobis
・Mahalanobis (normed)
・Nearest-neighbor (z-score)
・Outlier-counting
・SVM (one-class)
・K-means
以上の 14 の特徴量の組合せと 11 の照合アルゴリズムから、移動状態(歩行時、自動車乗車時)の認証に最適な組み合わせを評価実験により求めた。
評価実験では入力は「きいれまそてこはやに」の 10 文字を被験者によらず共通で用いることとし、被験者は 20 名、各 20 回のキー

ストロークデータを収集した。20 回のキーストロークデータの前半 10 回分から認証テンプレートを作成し、後半 10 回分のキーストロークデータを用いて認証を試みる。
特徴量の組合せとアルゴリズムの組合せの評価には本人拒否率と他人受入率が一致する時の誤り率である等誤り率 EER を尺度として用いた。
結果の詳細については省略するが例えば、歩行時のデータを歩行時の認証テンプレートで認証した時の EER は特徴量として、{HT, UUT, P, FD, AC, O, AV} の組合せ、照合アルゴリズムとして Outlier-counting を用いた時に EER=0.24%となり、乗車時のデータを乗車時の認証テンプレートで認証した時の EER は特徴量として{ UDT, TS, P, FA, FD, AV, EC} の組合せ、照合アルゴリズムとして Outlier-counting を用いた時に EER=0.13%となり、かなり良好な結果を得た。
4.1.2 その他
本研究課題では他にもスマートフォン等の携帯端末に表示運的に搭載されている振動機能を活用した端末ロック解除方式を提案した。提案方式では振動で形成されたパターンを用いることにより端末を把持している利用者にのみ必要な情報を伝えることにより覗き見による認証情報の特定を困難にする。

4.2 セキュリティ対策に関する計算機援用教材開発方法論の確立
近年、Web アプリケーションを標的とした攻撃による被害が多く報道されている。これらの被害の原因はアプリケーション開発時に作りこまれる脆弱性がある。これらはセキュアな Web プログラミングを行うことで防げることが多く、そのため、開発者に対する教育の必要性が増している。このことから実際に脆弱な Web アプリケーションに攻撃を行う演習を用いた教育方法が提案されている。しかし、それらの方法では脆弱性毎に淡々と学習と実践を繰り返し行っていることから学習者の意欲を保つことが無塚しい。そこで本研究課題ではハッキング競技の一種目である CTF (Capture The Flag)を用いたセキュア Web プログラミング教育手法を提案した。
CTF には様々な形式が存在するが、ここでは Jeopardy 方式を用いる。
提案手法は演習システムの形で実装され、問題サーバとスコアサーバからなる。問題サーバは学習者が攻撃を行う脆弱な Web アプリケーションを公開しているサーバである。公開されている Web アプリケーションには既知の脆弱性が含まれており特定の攻撃に成功すると学習者の目標である Flag 文字列が表示される。スコアサーバは学習者の情報と問題を管理する Web アプリケーションが稼働するサーバであり、学習者登録機能、出題機能、ランキング機能、等が存在する。
学習内容は OWASP の公開する Web アプリケーションの 10 大リスクのうち上位 3 項目の脆弱性を扱う。
4.2.2 その他
本研究では、一般ユーザのセキュリティ教育を行う自習型計算機教材の構成法(教材単元の長さと演習問題の挿入タイミングが学習効果に与える影響)に関する研究を行った。
4.3 HCI に関する最新の知見を採り入れたセキュリティ対策ツール・システム開発技法の確立
4.3.1 サイトの安全性と重要度に応じたパスワード管理ツールの開発
現在、多くのオンラインサービスにおいて依然パスワード認証方式が主流となっている。現状のパスワード認証方式は(1)ユーザは推測されやすい脆弱なパスワードを使用する傾向にある点、(2) ユーザが同じパスワードを複数のサイトで再利用する傾向にある点の 2 つの問題点が存在する。複数の異なるパスワードを管理する方法の一つとしてパスワード管理ツールの利用があるが、PC とスマートフォンなど、異なるプラットフォームでツールを用いるためにはクラウド等何らかのオンライン上に秘密情報を格納する必要があるため、第三者への情報漏えいやデータ紛失のリスクが存在するため普及に至っていない。そのため本研究課題では情報漏えい時の被害の程度と安全性がサイトによって異なることに着目しサイトの安全性と重要度に応じたパスワードの使い分け手法を提案すると共に、具体的な使い分けのグループ等の情報をローカル上で管理するツールを開発した。
サイトの重要度については、サービスサイトの種別(金銭に関連したサービスサイトであるか否か、個人的な情報に関連する情報を取り扱うか等)、当該サイトの認知度、利用状況に関する評価に基づいて数値化する。また、安全性については当該サイトのウィルス検査、ブロックリスト判定、総合的安全性評価に関する既存の評価サービスを用いて評価を行い数値化する。

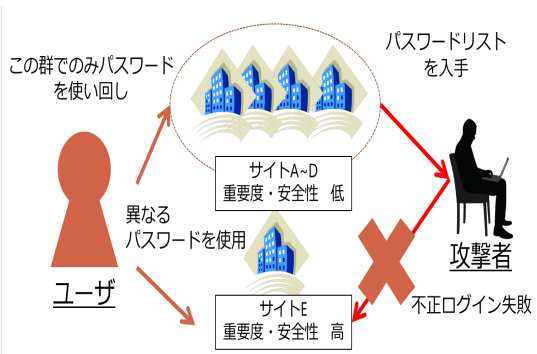

図 4. 提案方式のパスワード使い分け例

提案ツールでは図 4.のように個々のサイトの安全性と重要度を評価した上でグループ分けを行い、グループ内同士でパスワードの使い分けを行うことや、重要度の高いサイト

グループではより強固なパスワード利用を奨励する等の支援を行う。本ツールの構成を図 5 に示す。ユーザが新規アカウントを作成しようとしたとき，ユーザは本ツールに対して登録サイトの URL を入力する．本ツールは，URL からサイトの安全性・重要度を計算し，その値から，既存のパスワードグループの中から利用推奨されるパスワードグループを提示する．もし，推奨できるパスワードグループがなければ，新規パスワードグループを作成するようユーザに提示する．

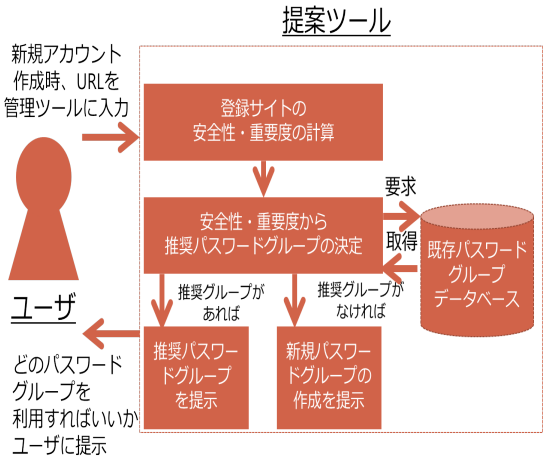

図 5．提案ツールの構成

4.3.2 分散型 slow HTTP DOS 攻撃手法に対する防御手法の確立

近年、複数の攻撃元が協調してサービス拒否攻撃(DOS 攻撃)を行う分散型 DOS 攻撃の脅威が深刻化している。最近特に必ずしも大量のトラフィックを発生させる必要のないアプリケーション層での DOS 攻撃が増加しており、少数のホストから効果的な攻撃が可能でかつ攻撃の検知が困難であることから、その対策は急務かつ重要である。そのような攻撃の一つに HTTP サーバを攻撃対象とする slow HTTP DOS 攻撃が存在する。Slow HTTP DOS 攻撃とは Web サーバの処理中のリクエストを飽和させる攻撃であり、現在、Slowloris、R.U.D.Y, Slow Read DOS の 3 手法が知られており、例えば Slowloris 攻撃は、Web サーバに対し、不完全な HTTP ヘッダを時間をかけて送信することでコネクションを長時間維持し他の HTTP リクエストを受付困難とする攻撃手法である。

本研究課題の提案手法では、サーバのコネクション数が上限に達する前に、slow HTTP DOS 攻撃の特徴である長時間維持される大量のコネクションを選択的に切断することで効果的な防御を実現するものである。

攻撃側ホスト 10 台、30 アドレスからなる分散型 slow read DOS 攻撃を模倣する実験環境を構築し提案手法の評価実験を行った。提案手法中のパラメータを適切に設定することにより効率的に攻撃を抑止し、サーバが飽和状態に陥らないことを確認した。また、WIDE ネットワーク上のトラフィックから作成された MAWI Working Group の公開データセットを用いて正当クライアントのリクエストを模擬することにより、提案手法が正当リクエストの QOS に与える影響を評価した。その結果、提案手法の設定パラメータと正当クライアントのリクエストが誤切断される確率の間に一定のトレードオフが存在することが確認された。

4.3.3 その他

その他、本研究課題では以下を実施した。

・ダークネット上のパケット観測に関して、観測点検出を防止しつつ、パケット観測結果に与える影響を抑止する観測パケットのサンプリング手法に関する研究

・画像局所特徴量を利用したフィッシングサイト検知手法に関する研究

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）

〔学会発表〕（計 16 件）

1) Masaki Narita, Kanayo Ogura, Bhed Bahadur Bista and Toyoo Takata: Evaluating a Dynamic Internet Threat Monitoring Method for Preventing PN Code-Based Location Attack, Proc.17th International Conference on Network-Based Information Systems (NBiS 2014), pp.271-278 (2014)

2) 小倉加奈代，坂松春香，Bista,B.B.，高田豊雄：想起性と安全性を両立するパスワード生成過程の分析，日本認知科学会第 31 回大会論文集，pp.662-671 (2014)

3) 鎌田恵介，成田匡輝，小倉加奈代，Bista,B.B.，高田豊雄：ダークネット上の観測点保護のためのパケットサンプリング手法の有効性評価，2015 年暗号と情報セキュリティシンポジウム予稿集 (SCIS2015)，3C1-1(CD-ROM) (2015)

4) 高橋央弥，小倉加奈代，Bista,B.B.，高田豊雄：スマートフォンにおけるキーストロークダイナミクスの移動状態に関する一検討，2015 年暗号と情報セキュリティシンポジウム予稿集 (SCIS2015)，2B3-3(CD-ROM) (2015)

5) 小松勇毅，児玉英一郎，王家宏，高田豊雄：Android OS におけるユーザー習熟度を用いたマルウェア被害防止システムの提案，2015 年暗号と情報セキュリティシンポジウム予稿集 (SCIS2015)，4A1-2(CD-ROM，8 ページ) (2015)

6) 成田匡輝，鎌田恵介，小倉加奈代，ベッドバハドゥールビスタ，高田豊雄： ダークネット観測におけるポート毎の動的観測に関する一検討，コンピュータセキュリティシンポジウム 2015，3E4-1(USB) ，2015.10.

7) 鎌田恵介，成田匡輝，小倉加奈代，ベッドバハドゥールビスタ，高田豊雄：ダークネット上の観測点保護のためのパケットサンプリング手法に

関する一検討，2016 年暗号と情報セキュリティシンポジウム予稿集，4B2-1(CD-ROM)，2016.1.
8) 坂松春香，小倉加奈代，Bhed Bahadur Bista，高田豊雄：サイトの安全性と重要度に応じたパスワード管理ツールに関する検討，2016 年暗号と情報セキュリティシンポジウム 2016 予稿集，1F1-3(CD-ROM)，2016.1.
9) 平川哲也，小倉加奈代，ベッドバハドゥールビスタ，高田豊雄：分散型 Slow HTTP DoS 攻撃に対する防御手法の提案，2016 年暗号と情報セキュリティシンポジウム 2016 予稿集，3B3-5(CD-ROM)，2016.1.
10) M. Narita, K. Kamada, K. Ogura, B. B. Bista and T. Takata, A Study of Packet Sampling Methods for Protecting Sensors Deployed on Darknet, 2016 19th International Conference on Network-Based Information Systems (NBiS), pp. 76-83, 2016.9.
11) T. Hirakawa, K. Ogura, B. B. Bista and T. Takata, "A Defense Method against Distributed Slow HTTP DoS Attack," 2016 19th International Conference on Network-Based Information Systems (NBiS), pp. 152-158, 2016.9.
12) Hiroya Takahashi, Kanayo Ogura, Bhed Bahadur Bista and Toyoo Takata, A User Authentication Scheme Using Keystrokes for Smartphones while Moving, 2016 International Symposium on Information Theory and Its Applications (ISITA), pp. 310-314, 2016.11.
13) 高橋啓伸，小倉加奈代，Bhed Bahadur Bista，高田豊雄，画像局所特徴量を利用したフィッシングサイト検知手法の実装と評価，コンピュータセキュリティシンポジウム 2016(CSS2016)論文集，3B4-3，2016 年 10 月
14) 平川哲也，小倉加奈代，ベッドバハドゥールビスタ，高田豊雄，分散型 Slow HTTP DoS 攻撃に対する防御手法の評価，2017 年暗号と情報セキュリティシンポジウム(SCIS2017)予稿集，2C1-3(USB)，2017 年 1 月
15) 立花聖也，小倉加奈代，BHED BAHADUR BISTA，高田豊雄，バイブレートパターンを利用した覗き見攻撃対策認証方式の提案，2017 年暗号と情報セキュリティシンポジウム(SCIS2017)予稿集，3D3-1(USB)，2017 年 1 月
16) 山田恭平，小倉加奈代，ビスタ ベッド，高田豊雄，スマートフォンの画面サイズによる制約を考慮したセキュリティ意識向上のための警告ダイアログの検討，情報処理学会研究報告ヒューマンコンピュータインタラクション(HCI)，2017-HCI-172，no.21，pp.1-8，2017 年 3 月

６．研究組織

(1)研究代表者
高田　豊雄　（TAKATA TOYOO）
岩手県立大学・ソフトウェア情報学部・教授
研究者番号：50216652

(2)研究分担者
Ｂ．Ｂ．　ビスタ　（B．B．BISTA）
岩手県立大学・ソフトウェア情報学部・准教授
研究者番号：10305287

小倉　加奈代　（OGURA KANAYO）
岩手県立大学・ソフトウェア情報学部・講師
研究者番号：10432139

(3)連携研究者
王　家宏　（OH KAKOU）
岩手県立大学・ソフトウェア情報学部・教授
研究者番号：80305292

児玉　英一郎　（KODAMA EIICHIROU）
岩手県立大学・ソフトウェア情報学部・講師
研究者番号：00305031

(4)研究協力者
（　　）