科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　２４　日現在

機関番号：　２１２０１
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５０００９４

研究課題名（和文）人間科学の最新知見に基づくセキュリティソリューション

研究課題名（英文）Security Solution based on Latest Human Science Study

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）　　4,000,000円、（間接経費）　　1,200,000円

研究成果の概要（和文）：近年、フィッシングやパスワード推測、不注意によるマルウェア感染といった人間を糸口とするセキュリティ被害が増えている。
本研究では、ユーザビリティ工学や教育工学、認知科学といった人間を取り扱う学問の最新成果をとりいれたセキュリティ向上の方策を考案する。
具体的な課題としては 1）最新の認知科学の知識を導入した記憶容易性と安全性を両立させたパスワード認証方式、2）最新の教育工学の知見を導入したセキュリティ教育システム設計方法論の確立、3）可用性を重視した一般ユーザ向けセキュリティ対策ツールや対策システムの確立である。

研究成果の概要（英文）：Recently, security damages caused by users' missuse such as phishing, weak password or inadvertent malware infection are increasing. In this research, we investigate how to improve security by introducing the latest result of various human science study such as usability engineering, education engineering, or cognitive science.
Specifically, we consider the following three subjects: 1) development of password-based authentication schemes based on the latest knowledge of cognitive science which attains both memorability and security, 2) establishment of the design method of education system of security which introduces the latest knowledge of education engineering, and 3) development of security tools or system for end users which realize usability.

研究分野：　総合領域

科研費の分科・細目：　情報学

キーワード：　個人認証　セキュリティ教育　教育工学　ユーザビリティ工学　スマートフォン　マルウェア　セキュリティツール　インターネット観測システム

１．研究開始当初の背景
従来、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。代表的な例としては、フィッシングからのドライブバイダウンロード攻撃、ユーザの個人情報を調べ上げたうえでのパスワード解読等が存在する。
一方、人間の記憶に関するメカニズムの解明等の脳科学、人間の直感的な理解を助け、直観的な操作を容易にするためのヒューマンインタラクション、ネットワークやコンピュータを援用した教育あるいは教材作成方法論を取り扱う教育工学など、広い意味の人間科学に関する進歩は目覚しいものがあるにも拘らず、セキュリティの分野に反映されているとは言い難く、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、サーベイ集や国際会議が開かれているものの日本国内での研究の立ち遅れが目立つ。

２．研究の目的
１節で述べた通り、人間の認知や記憶に関するメカニズムや効率的な教育手法等、それら人間科学に関する最新の知見の導入により、セキュリティを実現する様々なシステムの構築やシステム脆弱個所の解消を図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･記憶のメカニズムに基づく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) HCI に関する最新の知見を採り入れたセキュリティツール、システム開発技法

３．研究の方法
3.1 人間の認知や記憶のメカニズムに即した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、テキストに関する記憶と図的要素に関する記憶、意味記憶とエピソード記憶、認知の融合等)に基づく、記憶容易性と安全性の双方を両立した記憶に基づく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
最近、一般ユーザの心理的盲点をついた様々なネットワーク犯罪(フィッシング、その他ソーシャルエンジニアリング的手法)が急増している。これ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解決する必要がある。
この問題については従来から報告者らのグループで教育システムの試作開発がテーマとして掲げられ、一定の成果を見ている]。本研究の第二の目的は、a)単なる従来の教材設計手法の適用では教材開発コストが高くなり、次々と新しい攻撃手口が発生する本分野への単純な適用は困難、b) [11]で提案の情報活用環境の概念は一定の効果を見たが学習者のセキュリティ意識向上を図る上で一層の洗練が必要、等の問題を解決し、セキュリティ教育向け計算機援用教材開発の方法論を確立することである。

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
また、近年、セキュリティ対策ツールの不適切な設定、利用やセキュリティ対策情報の不足により、ツールやシステムの機能が充分活かされない結果、セキュリティ被害を被る状況を引き起こしかねない状態を招いている。本研究の第三の目的は、HCI に関する知見を導入し、エンドユーザのセキュリティ対策に有用なツールやシステムを開発する技法の確立を図ることである。

４．研究成果
4.1 人間の認知や記憶のメカニズムに即した個人認証方式の確立
4.1.1 こまマンガを用いたパスワードベースの個人認証方式の提案
パスワードによる個人認証方式は主として運用コストの低さから広く用いられているが、クラック困難性と記憶容易性を同時に達成することは困難である。クラック困難なパスワードに関する知識なしに記憶の容易なパスワードを作成可能とするため、本研究では人物の眼や効果等を選択することにより２，３コママンガをユーザに作成させ、そのセリフをパスワードとする方式を提案した。作成したマンガやその作成過程とセリフを結びつけることにより記憶が容易となり、ある程度の長さのセリフを考えることにより意識せず充分な長さのパスワードを作成可能となる。図１はその作成支援プロトタイプシステムのスクリーンショットである。

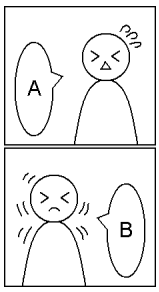

図１．こままんがによるパスワード作成支援システムのパスワード作成過程の図

4.1.2 ユーザのライフログを用いたパスワードベースの個人認証方式の提案
最近、SNS をライフログとして利用するユーザが増加している。ライフログはユーザ個人の体験に根ざすものであり強く記憶と結びついている。本研究ではライフログから抽出した単語と語呂合わせパスワードの考え方を結びつけることにより記憶が容易でクラック困難性の高いパスワードを作成する手法を提案した。図２はその手法のプロトタイプシステムのスナップショットである。

図２．ライフログから抽出した候補単語を選択する画面のスナップショット

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、コンピュータ犯罪の対象としてスマートフォンを狙う攻撃が増加している。攻撃手法として人間の心理や行動を利用するものが主であり、機械的な対策だけでは対処が困難である。そのため、ユーザ自らの対処が必要になるが、実際の場面に直面した場合の行動を想起し辛い。これらを解決するため、報告者のグループを始めとして Goal Based Scenario(GBS)理論に基づいた教材の開発が行われているが、いくつか問題がある。例えば、GBS 理論は選択肢を選びながらシナリオを進めていき、失敗を通して学習するという方法論であるが、失敗が選ばれない場合、十分な学習効果が得られないまま学習が終了してしまうという問題等である。

図３．提案手法に基づくセキュリティ学習教材のスクリーンショット

本研究では従来得られていた研究者グループの教材開発方法論に改良を行った。評価結果として攻撃手法の理解や楽しみながら学習を行えたかといった項目について統計的に有意な差が見られ、提案改良手法の有効性が示された。

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 視線追跡装置を用いたアンチウイルスソフトの使用調査と考察
セキュリティに関する知識が充分ではない一般ユーザにとって、アンチウィルスソフトの不適切なインストールやマルウェア検出の通知の誤認や見逃しにより、セキュリティが保たれない状況が生じることが知られている。本研究ではいくつかの市販アンチウィルスソフトのインストール時やマルウェア検出通知時のユーザの挙動について視線追跡装置やビデオカメラを用いて解析を行い、アンチウィルスソフトの問題点とその改善法について述べた。

4.3.2 Android OS 上のアプリケーション導入時におけるセキュリティ助言システムの開発
Android OS を搭載したスマートフォン等の携帯端末が急速に普及している。それらの端末では新しいアプリケーションを導入する際、パーミッションと呼ばれるメカニズムにより、当該アプリケーションが、インターネット接続、端末内の個人情報の読み取り、GPS2 を用いた位置情報の読み取りといった機能の使用について、ユーザに対して承諾を求める形式をとっている。
近年、ユーザの知識不足やパーミッションの確認不十分により、個人情報漏洩等のセキュリティ問題が頻発している。そのため本研究では、アプリケーションインストール時における，ユーザのセキュリティ管理上の負担軽減と，アプリケーションの危険性理解補助の 2 点に着目し，ユーザの判断支援を行うシステムを提案し、プロトタイプ実装を行った。図４はシステムのスナップショットである。

図４．判断支援システム

36 名の実験協力者により、18 個の通常アプリケーションと 18 個のセキュリティ上問題のあるアプリケーションについて、アプリケーションの導入/非導入を正しく判断できるかどうかの評価実験を行い、判断時間、正答率共に通常のインストール画面と比較して有意な差があることを確認し、ユーザのアプリケーション判断支援に有効であることを示した。

4.3.3 インターネット観測システムに対する新しい攻撃手法と対策手法
近年、新たに発見された脆弱性や攻撃手法に基づくサイバー攻撃が増加している。それらの攻撃は例えば新たに発見された脆弱性に対応したサービスプログラムがサービスを行うポート番号に対する通信の急激な増加という現象を伴う。そのため、インターネット観測システムという様々なインターネットトラフィック動向を収集、開示するシステムが例えば日本では警察庁、通信放送研究機構等により運営されている。
インターネット観測システムでは実際にパケットを観測する観測点というホストの存在を秘匿することが重要であり、存在が知られると、攻撃時に観測点が迂回されたり、攻撃対象となる恐れがある。
近年、そのインターネット観測点検出攻撃について PN 符号を用いた新たな手法が提案されている。本研究の主な成果の第１は、その手法を改良した新たな観測点検出攻撃の提案(これは対策の必要性を喚起するために重要)であり、第２は、それらに対処するための新たな観測システムの提案である。

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１件）
(1) Masaki Narita, Bhed B. Bista, Toyoo Takata: A Practical Study on Noise-Tolerant PN Code-Based Localization Attacks to Internet Threat Monitors, International Journal of Space-Based and Situated Computing, Vol.3, No.4, 2013, pp.215-226.
〔学会発表〕（計１２件）
(1) 吉本 道隆，加藤 貴司，ベッド B. ビスタ，高田 豊雄: ユーザビリティとセキュリティを両立したセキュリティスキャナシステムの開発，マルチメディア，分散，協調とモバイルシンポジウム予稿集，2011，pp.1279-1284.
(2) 吉本 道隆，高田 豊雄: 視線追跡装置を用いたアンチウィルスソフトの使用者に関する動向調査と考察，ヒューマンインタフェースシンポジウム 2011，3241L，2011，6 ページ.
(3) 小原 富美聡，ベッド B. ビスタ，高田 豊雄: クラック困難なパスワードの作成を意識しないユーザでも利用可能な、２コマまんがを用いた認証方法の提案マルチタッチスクリーンを利用した認証方式の提案，コンピュータセキュリティシンポジウム 2011 論文集，2011，pp.54-59.
(4) 成田 匡輝，ベッド B. ビスタ，高田 豊雄: 動的観測点を利用した SYN Flood 攻撃検出手法とその有効性評価について，コンピュータセキュリティシンポジウム 2011 論文集，2011，pp.558-563.
(5) 松戸 隆幸，児玉 英一郎，王 家宏，高田 豊雄: Android OS 上でのアプリケーション導入時におけるセキュリティ助言システムの提案，情報処理学会研究報告，Vol.2012-CSEC-56，No. 12，2012，7 ページ.
(6) Takayuki Matsudo, Eiichiro Kodama, Jiahong Wang and Toyoo Takata: A Proposal of Security Advisory System at the Time of the Installation of Application on Android OS, Proc. of NBIS2012, pp.261-267, 2012.
(7) 成田匡輝，ベッド B. ビスタ，高田 豊雄: PN 符号を利用した観測点検出攻撃のノイズ耐性向上に関する一考察、2012 年コンピュータセキュリティシンポジウム予稿集，pp.587-594，2012.
(8) 小原冨美聡，ベッド B. ビスタ，高田 豊雄: クラック困難なパスワードの作成を意識しないユーザでも利用可能な、まんがを用いた認証方法の提案、2012 年コンピュータセキュリティシンポジウム予稿集，pp.773-780，2012.
(9) 菊池雄大，ベッド B. ビスタ，高田 豊雄: スマートフォンセキュリティ学習を支援する GBS 理論に基づく教材開発について、2013 年暗号と情報セキュリティシンポジウム予稿集，2F4-5，8 ページ，2013.
(10) Masaki Narita, Bhed Bahadur Bista and Toyoo Takata: Study on Noise-Tolerant PN Code-Based Localization Attacks to Internet Threat Monitors by Exploiting Multiple Ports, Proc. of 27th International Conference on Advanced Information Networking and Applications, pp.98-105, 2013.
(11) 坂松春香，小倉加奈代，Bhed B. Bista，高田 豊雄: TweetPass: ツイートを用いたパスワード作成支援システムの開発，2014 年暗号と情報セキュリティシンポジウム予稿集，3B1-5，2014，7 ページ.
(12) 成田匡輝，小倉加奈代，Bhed B. Bista，高田 豊雄: インターネット観測システムへの観測的検出攻撃に対する動的観測手法の有効性評価，2014 年暗号と情報セキュリティシンポジウム予稿集，3A5-1，2014，7 ページ.

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

(3)連携研究者
吉本　道隆　(YOSHIMOTO MICHITAKA)
清泉女学院大学・人間学部・助教
研究者番号： 60551447
(H23)