様式 C-19

科学研究費補助金研究成果報告書

平成 23 年 4 月 21 日現在

機関番号：２１２０１
研究種目：基盤研究（C）
研究期間：2008～2010
課題番号：２０５０００７２
研究課題名（和文）　人間に焦点を当てた情報セキュリティ向上方策に関する研究

研究課題名（英文）　Research on Security Improvement Focusing on Human

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

研究成果の概要（和文）：情報セキュリティの実現には管理的対策と技術的対策の双方が重要であることは従来より指摘されていた。本研究では、従来学術的な側面からは殆ど省みられることがなかった管理的対策、特に人の問題を解決することを目的とする。具体的には (1) ユーザビリティを考慮した、十分な専門知識を必ずしも有さない一般個人ユーザ向けセキュリティツールの開発を行った．作業例題としてはセキュリティスキャナを用い、総括的評価の結果，開発したセキュリティスキャナが既存のものと比較しユーザビリティに優れることを確認した．(2) Web 環境で自習可能なソーシャルエンジアリング対策教材の開発について、学習効果と開発効率に優れる開発手法の提案を行った．
研究成果の概要（英文）：To achieve sufficient security, we need to measure it from both the technical and administrative points of view. In this research, we focus on an administrative point of view, especially human factor. We focus on the following two projects: the first one is development of a security tool with usability for individual users that don't necessarily have sufficient knowledge for security. We adopt development of a security scanner as a working example. We conduct summative evaluation for our proposed and developed security scanner and existing one and as a result, we show our developed one attains considerably good usability. The second project is development of a web based self-learning system for countermeasure of social engineering. We show our development scheme attains both effectiveness of learning and efficiency of development.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,700,000	510,000	2,210,000
2009 年度	800,000	240,000	1,040,000
2010 年度	600,000	180,000	780,000
年度			
年度			
総　計	3,100,000	930,000	4,030,000

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：情報セキュリティ、管理的対策、ユーザビリティ、セキュリティ教育

１．研究開始当初の背景

情報セキュリティの実現には管理的対策と技術的対策の双方が重要であることは従来より専門家の間で指摘されていた。しかしながら、管理的対策、特に人の問題は、システムやネットワークの管理などの実務に携わる者の間では重要視されてきたが、学術的な側面からは殆ど省みられることがなかった。アメリカ

では散発的ながらも比較的早くからこの問題に着目されており、研究開始当初では例えば、学会雑誌で特集が組まれ①、サーベイ集が出版され②、セキュリティとユーザビリティの問題を専門に取り扱う国際会議が 2005 年より開かれるようになった③。
一方、国内では報告者の研究グループの他は研究集会発表のレベルで個別テーマに「ユーザビリティ」等のキーワードがつくことがあったが、利便性向上を安全性向上に結びつけることを、研究課題として正面から取り扱うものは少ないという現状であった。
① L.F. Cranor et al.(eds), “Usability and Security,” IEEE Security & Privacy, Vol. 2, No.5, 2004.
② L.F. Cranor, S. Garfinkel (eds), Security and Usability, O’Reilly, 2005.
③ Symposium on Usable Privacy and Security, http://cups.cs.cmu.edu/soups/

２．研究の目的
そのため本研究では次の２つの課題に取り組んだ。
(1) 非専門家向けセキュリティ対策ツール開発技法の確立
単なる技術的観点からは十全と思われている数々のセキュリティ対策も、知識や意識の欠如の問題から非専門家にとっては充分ではないことが多い。そのため、それらの一般ユーザに対しては専門家向けとは異なるアプローチに基づくセキュリティ対策を行う必要がある。本研究の第一の目的は、ウェブユーザビリティ向上技法等の HCI に関する知見をセキュリティ対策に導入することにより非専門家向けのセキュリティ対策ツールの開発技法を確立することである。
一対一評価や小集団評価等の形成的評価、その後の総括的評価を経て、その間に浮かび上がった問題点をインターフェース改良等に漸次結びつけることにより、ツールの洗練を図る技法がセキュリティ対策ツールにも有効であることを示す。

(2) 一般個人向けセキュリティ管理的対策の計算機援用教育システムの試作開発
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。これも技術的対策の不備が問題というよりも、むしろ 研究目的の(1)と同様に、一般ユーザの知識や意識の欠如に起因するところが大きいため、技術的対策だけでそれらの犯罪を防ぐことは困難である。
本研究の第二の目的はソーシャルエンジニアリングに代表される心理的盲点をつく犯罪対策を目的とした計算機援用教育支援システムの設計と実現である。本課題で取り上げる問題領域、達成目標の特殊性ゆえ通常の教育工学における計算機援用教育支援システムの作成方法論の単純な適用とはなり難い点がいくつか存在する。例えば、
① 学習課題の属する領域がセキュリティ意識といった情意領域に属すること。
② 敵対者はしばしばセキュリティ上の弱点を的確に突いてくることから、学習者の弱点の克服に重点をおいた教育支援を行わなければならないこと。
以上の様なセキュリティに関する問題の特殊性を考慮した教育支援システムの構築を目指す。

３．研究の方法
(1) 研究目的の(1)については、作業例題として、セキュリティスキャナを採り上げ、そのユーザビリティ改善を図ることにより、セキュリティの向上を図ることを考える。ユーザビリティの評価指標には様々な標準が存在し、その中から、本研究目的に相応しい評価指標を選択する。また、ユーザビリティ改善のための手法もいくつかあるため、その中から適切なものを選ぶ必要がある。抽出された問題点を元にユーザビリティ改善を進め、開発の途中段階においてフィードバックを得るために被験者を用いたユーザビリティ評価を行う。った．最終的に総括的評価を行い，客観的な評価指標により高いユーザビリティを確保していることを確認する。

(2) 研究目的の(2)については、Goal Based Scenario 理論などのインストラクショナルデザイン理論の中から、一般ユーザにとってセキュリティ意識の変容を促すことのできる学習理論を導入し、ソーシャルエンジニアリング対策教材に相応しいカスタマイズを図る。教材のプロトタイプ完成後は、研究課題の(1)と同様に形成的評価と総括的評価を行い、既存の教材設計技法との比較により、教材の学習効果を評価する。また、ネットワーク犯罪は、新たな手口が次々と生み出されることに素早く対応するため教材の開発効率も重視される。教材設計技法の評価では教材の開発効率も評価尺度の一つとする。

４．研究成果
(1) 非専門家向けセキュリティ対策ツール

開発技法の確立

本課題では，まず、Norman らによって提唱された“ユーザ中心設計”に着目し、ISO9241-11 で示されるユーザビリティ 3 要素を評価尺度として用いることとした．通常の開発方法ではセキュリティツール開発者が想像するユーザ像と，実際のユーザの間には差異がある場合があり，開発者が想像するとおりにユーザはそのツールを使いこなすことが出来ない場合が多分にある．また，ユーザビリティ工学において，ユーザの意見の把握・評価を開発の前後に行う従来方法では潜在する重大なユーザビリティ問題を完全に見つけることが出来ないとされている．一般にユーザ中心設計において，開発者はシステム開発以前において実際のユーザの要求を把握し，開発の途中段階において開発指標としてユーザの多くの意見を採用することとされており、この方法を用いることによって，開発者は潜在的で重大な問題点を全て発見することが出来るとされている．本課題で開発・評価したセキュリティスキャナではこの手法を採用すると共に，開発したシステムをユーザが効率的かつ効果的に使用可能とするためのユーザサポートデータベース等の仕組みを考案した．ユーザサポートデータベースにおいては操作や判断を手助けするバルーンヘルプや，発見された脆弱性を効率よく修正するための手助けとなる追記情報などを提供する仕組みを採った．

また，ISO9241-11 ではユーザビリティ 3 要素が示されている．そこでは，1)効果的， 2)効率的に，3)満足に使えることがユーザビリティとして求められており，セキュリティツールを使用する上においても，その 3 要素を満足すべきである。そこで，本課題では総括的評価において被験者を用いたパフォーマンス測定を行い，3 要素について数値化された結果を得ることによって，客観的な評価結果を得た。

本課題の評価の一連の流れを図 1 に示す．開発指標としてユーザ中心設計を用いる．まずユーザの実際の利用状況を把握し，ユーザニーズの把握を行う．そのニーズを満たすようなプロトタイプを作成し，ユーザビリティ評価を行う．そしてその問題点を発見し，修正し，評価するプロセスを繰り返し行う．

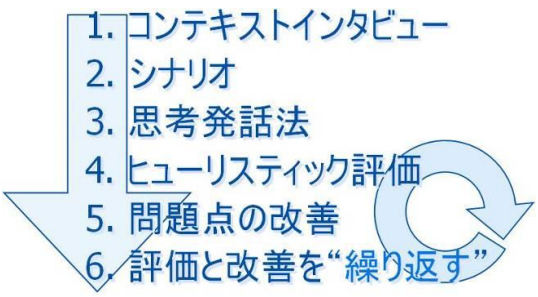


図 1. 課題(1)における評価の流れ

事前の予備調査により得られた既存のセキュリティスキャナの問題点の摘出結果を反映した、セキュリティスキャナの開発を行った。開発したセキュリティスキャナは Nessus を核として Web ベースのインターフェースを採用することにより、ユーザビリティを確保する。本課題で開発したセキュリティスキャナの動作画面の一例を図 2 に示す。プロトタイプの実装後は、図 1 で示された通りの評価と改善のプロセスを繰り返した。

総括的評価として、ISO9241-11 で示された 3 要素それぞれについて、本課題で開発したセキュリティスキャナと既存のセキュリティスキャナである NessusWX との間で比較を行った。ここではそのうち、効率について行った評価結果を図 3 に示す。ここでは、30 名の被験者を用いて、3 つのタスクを行ってもらった。

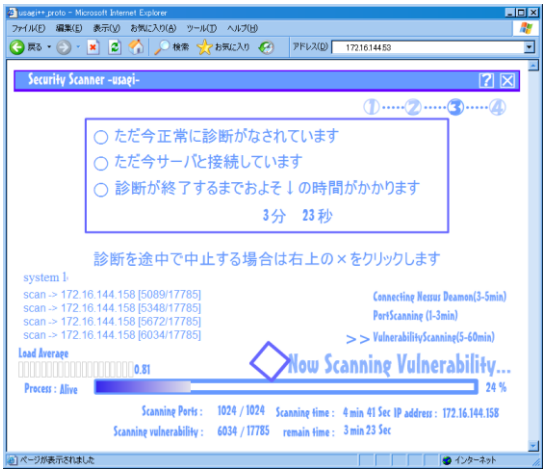


図 2. 開発したセキュリテイスキャナの画面例

タスク 1,2,3 はそれぞれ、評価対象を用いてクライアント PC に脆弱性があることを診断すること、スキャナのメッセージに基づいて最低 1 つの脆弱性を修正すること、全ての脆弱性を修正し，評価対象を用いて脆弱性が無

いことを確認することである。
評価実験の結果 NessusWX は平均して 56 分 4 秒要しているのに対し，提案システムは 19 分 6 秒で全てのタスクを完了しており、開発システムの効率の高さが示された。

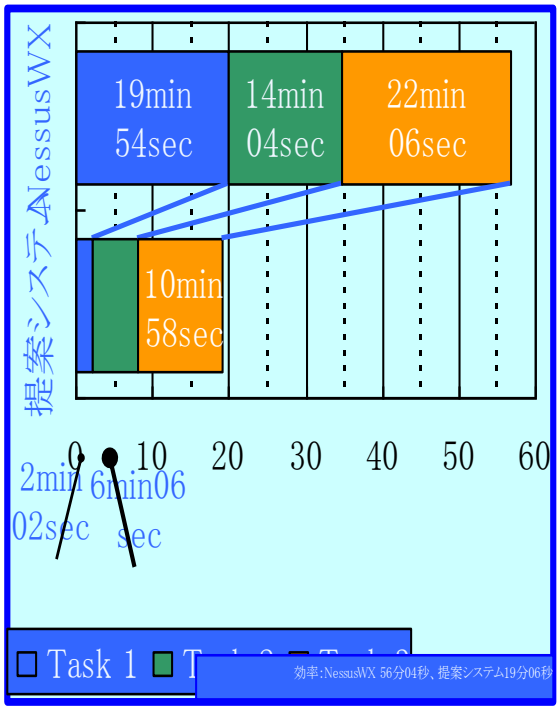


図 3. 「効率」に関する評価結果

同様の方法で、他のユーザビリティ要素についても同様の評価を行い、全体としてユーザビリティの高いシステムが開発されていることを確認した。

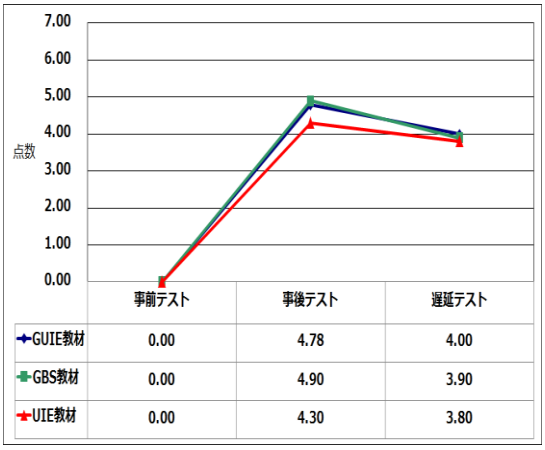
(2) 一般個人向けセキュリティ管理的対策の計算機援用教育システムの試作開発

本課題ではソーシャルエンジニアリングのいくつかある手口のうち、フィッシングについて取り上げ、フィッシング対策を自習可能な Web 教材の開発を行った。ここでは UIE (User's Information usage Environment) という概念を提案した。UIE とは学習者が日常慣れ親しんでいる IT 利用環境のことであり、例として、携帯電話のキャリア、よく利用する SNS やポイントサイト、メールを送受信するとき、パソコンと携帯電話でどちらをよく利用するか等があげられる。UIE の導入により、教材中で提示される具体的な犯罪手口に対して、より一層の迫真性を持たせることが期待される。

本課題では、教材設計手法として、Goal Based Scenario (GBS)理論をベースとし、以下の 3 つの組み合わせで教材を作成し、その学習効果や、教材開発効率を測定した。

1) GBS 理論のみ適用(GBS 教材)
2) UIE のみ反映(UIE 教材)
3) GBS 理論を適用し、UIE を反映(GUIE 教材)

学習効果については、(a) 知識、(b)態度・技能の両面から測定を行った。知識を問う 7 点満点の問題を学習前(事前テスト)、学習直後(事後テスト)、学習終了一週間後(遅延テスト)の 3 回行った。知識に関する比較結果を図 4. に示す。

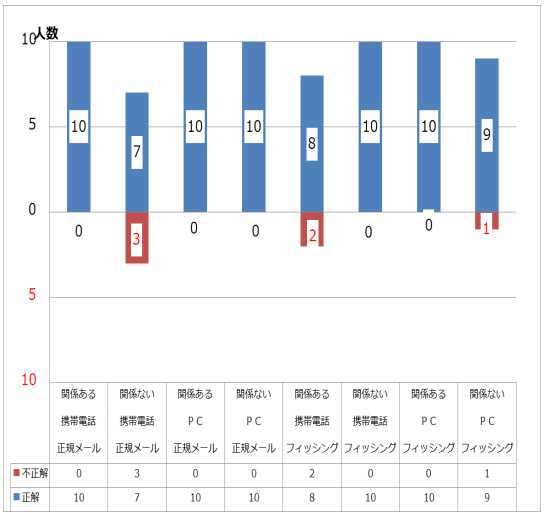


	事前テスト	事後テスト	遅延テスト
GUIE教材	0.00	4.78	4.00
GBS教材	0.00	4.90	3.90
UIE教材	0.00	4.30	3.80

図 4. 知識に関する学習効果の測定結果

また、態度に関する評価では、学習終了一週間後に、8 通のメールを被験者に送り、その処理を口頭で回答してもらうことで測定した。8 通の内訳はフィッシングを模したメール/正規メール、PC/携帯電話、ユーザに関係のあるメール/関係のないメールの 3 項目の組み合わせ(8 通り)である。

その結果、GBS 教材、UIE 教材、GUIE 教材を利用したユーザのそれぞれ 15%、42%、60%が 8 通のメールすべてについて正しい対処ができた。それらの評価結果のうち、UIE 教材に関する詳細を図 5 に示す。



	関係ある 携帯電話 正規メール	関係ない 携帯電話 正規メール	関係ある PC 正規メール	関係ない PC 正規メール	関係ある 携帯電話 フィッシング	関係ない 携帯電話 フィッシング	関係ある PC フィッシング	関係ない PC フィッシング
不正解	0	3	0	0	2	0	0	1
正解	10	7	10	10	8	10	10	9

図 5. UIE 教材の態度・技能テスト結果

また、教材の開発時間については、GBS 教材、UIE 教材、GUIE 教材それぞれ、82 時間、22 時間、94.5 時間となった。GBS 教材、GUIE 教材では、シナリオを反映した教材作成にそれぞれ 68.5 時間、80.5 時間を要している。
それら、学習効果と教材開発時間の双方の評価結果から、本研究で提案した UIE の概念は、学習効果も高く、教材開発時間を短く抑えることのできる優れた開発概念であることがわかった。

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１件）

[1] 吉本 道隆、加藤 貴司、Bhed Bahadur Bista、高田 豊雄、ユーザビリティ工学に基づく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のインタフェースの開発と評価、情報処理学会論文誌、査読有、51 巻、2010、pp.529-541

〔学会発表〕（計６件）

[1] 千葉 緑、加藤 貴司、藤原 康宏、ベッド B. ビスタ, 高田 豊雄、情報活用環境を用いたソーシャルエンジニアリング対策教材の開発、2009 年暗号と情報セキュリティシンポジウム講演論文集、査読無、SCIS09-2D1-4、2009.01.21、6 ページ.

[2] 吉本 道隆、加藤 貴司、ベッド B. ビスタ、高田 豊雄、アンチウィルスソフトのユーザビリティに関する問題点の発見と改善法の提案、2009 年暗号と情報セキュリティシンポジウム講演論文集、査読無、SCIS09-2E1-4、査読無、2009.01.21、6 ページ.

[3] 千葉 緑、加藤 貴司、ベッド B.ビスタ, 高田 豊雄、UIE を用いた一般ユーザ向けソーシャルエンジニアリング対策教材の評価、第 8 回情報科学技術フォーラム(FIT2009)論文集、K-034、査読無、2009.09.02、pp.607-610.

[4] 千葉 緑、加藤 貴司、ベッド B.ビスタ、高田 豊雄、情報活用環境のソーシャルエンジニアリング対策教材への適用、2010 年暗号と情報セキュリティシンポジウム講演論文集, SCIS10-3E3-4、査読無、2010.01.21、6 ページ.

[5] 吉本 道隆、澤村 隆志、加藤 貴司、ベッド B. ビスタ、高田 豊雄、セキュリティ製品におけるユーザビリティとの両立性に関する一提案、ヒューマンインタフェースシンポジウム 2010(HIS2010)予稿集、査読無、2010.09.09、pp.593-600.

[6] 千葉 緑、加藤 貴司、ベッド B.ビスタ, 高田 豊雄、ソーシャルエンジニアリングの学習を支援するための教材開発手法の比較、2011 年暗号と情報セキュリティシンポジウム講演論文集、SCIS11-2F2-3、査読無、2011.01.26、6 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 Bista（Bhed Bahadur 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

加藤貴司（KATOH TAKASHI）
岩手県立大学・ソフトウェア情報学部・講師
研究者番号：20323115