Vol.2018-SPT-27 No.32
2018/3/8

ユーザブルセキュリティワークショップ（UWS）2017 発表論文の特徴分析

金岡 晃[1,a)]

概要：ユーザブルセキュリティ・プライバシに特価したワークショップとして 2017 年に初めて開催されたユーザブルセキュリティワークショップ（UWS）2017 では、16 本の論文が投稿そして発表された。ユーザブルセキュリティとプライバシに焦点をあてた研究報告を行う場として日本において初めて実施されたと言っていいこのワークショップにおいて、どういった論文が発表され、これまでの他のセキュリティシンポジウムで発表されてきた論文とどういった違いがあるかを定性的と定量的の両面から分析する。

An Analysis on Usable Security Workshop (UWS) 2017 Papers

Akira Kanaoka[1,a)]

1. はじめに

2017 年 10 月に開催されたコンピュータセキュリティシンポジウム 2017 (CSS2017) において、併催のワークショップとして初めてユーザブルセキュリティワークショップ（UWS）が開催された。

ユーザブルセキュリティあるいはユーザブルプライバシに焦点をあてて開催された学術的なワークショップとしては国内で初めての試みであった。

セキュリティとユーザビリティについては、Whitten と Tygar が 1999 年に電子メールの暗号化を対象にした研究が発表されたことをきっかけに、大きな動きとなって現在に至っている [1]。

学術的には、その中心は国際会議 SOUPS と言っていい。SOUPS は Symposium on Usable Privacy and Security の略称であり、2005 年より開催されてきた。SOUPS では年とともに参加者と投稿数、採録数が増加しており、いまでは難関国際会議の 1 つとなっている。ユーザブルセキュリティあるいはユーザブルプライバシの研究は SOUPS にとどまらず、その後はトップに位置付けられる IEEE Symposium on Security and Privacy (S&P)、USENIX Security Symposium (SEC)、ACM Conference on Computer and Communications Security (CCS) 、Network and Distributed System Security Symposium (NDSS) といった難関国際会議でも多くの論文が採録されてきた。また、SOUPS に続く国際会議として USEC （Workshop on Usable Security）や EuroUSEC （European Workshop on Usable Security) が立ち上げられ、それぞれの国際会議も多くの投稿がされているなど、研究分野としての盛り上がりを見せている。

国内においては、ユーザブルセキュリティあるいはユーザブルプライバシの研究は主に情報処理学会セキュリティ心理学とトラスト（SPT）研究会により推進されてきた。分野の重要性や世界的な研究の現状を概観し裾野を広げるために、SOUPS で発表された論文を参加者同士で協力し発表論文を読破し内容を紹介する勉強会「SOUPS 論文読破会」が立ち上げられた。SOUPS 論文読破会は 2011 年に始まり、これまでに 7 回が開催されてきた。

そういった SOUPS 論文読破会での成果の発展の 1 つとして、国内のユーザブルセキュリティあるいはユーザブルプライバシ研究者の研究発表と議論の場所が求められるようになった。そしてユーザブルセキュリティワークショップ（Usable Security Workshop, UWS）が、セキュリティと高いユーザビリティを両立させる、技術だけではない分

[1] 東邦大学
Toho University
[a)] akira.kanaoka@is.sci.toho-u.ac.jp

野横断的な研究の発展とその成果普及の促進、さらに研究者や技術者の相互協力の促進を目的として立ち上げられた。

本稿では、初めての UWS でどういった論文が投稿され、それらはこれまでの国内のセキュリティの論文とどう違うかを定性的と定量的の両面から分析をしていく。

2. ユーザビリティとセキュリティ

ユーザビリティとセキュリティはトレードオフの関係にあるという認識は、多くの場所で見ることができる。日本における最近の例としては、情報処理推進機構が公開した調査レポート「暗号に関する国内外のガイドラインの実態調査の調査報告書」を例にあげることができる [2]。本レポートは暗号に関する実態調査になっているが、そこの調査項目「暗号技術を利用・運用する際の課題」として最も多く挙げられた項目が「ユーザの利便性と暗号技術の導入によるセキュリティ対策のバランスをとるのが難しい」であり、その率は 26.6% となっていた。

ユーザビリティそのものの研究や解決のアプローチは古くより行われてきた。ISO 9241-11 では、ユーザビリティを以下のように定義している。

> *Extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.*

この ISO 規格に対応する JIS Z 8521 では、以下のようにユーザビリティが定義されている。

> ある製品が、指定された利用者によって、指定された利用の状況下で、指定された目的を達成するために用いられる際の、有効さ、効率及び利用者の満足度の度合い

Web 技術のユーザビリティとして多く参照される Jacob Nielsen は、ユーザビリティは質的な属性 (Quality Attribute) であり、「学習しやすさ（Learnability）」「効率（Efficiency）」「記憶しやすさ（Memorability）」「エラー（Errors）」「満足（Satisfactioin）」の 5 つの質的コンポーネントにより定義されるとした [5]。

Whitten と Tygar はユーザビリティとセキュリティの関係について、ユーザインタフェースに焦点をあてて、標準のアプローチとは違うアプローチが必要であることを指摘した。そしてセキュリティのユーザビリティ（Usability for Security）を以下のように定義した。

> 利用者が以下の 4 つの事柄が可能なときに、そのセキュリティソフトウェアはユーザブル（Usable）である。
>
> - 利用者がやるべきセキュリティの作業を確かに (reliably) 認識する
> - 利用者がそれらの作業をうまく (successfully) 実施する方法を理解可能である
> - 利用者が危険なエラーを起こさない
> - 利用者がそのインタフェースを継続して使うことを十分に快適に感じる (comfortable)

Whitten と Tygar による論文は、電子メール暗号化技術である PGP 5.0 に焦点を当てた研究であったが、ユーザビリティの定義や評価としてのユーザ実験の方法などセキュリティとユーザビリティの分野に多くの先駆的な考え方を持ち込み、大きな影響を与えた。

3. Schecter 文書

ユーザブルセキュリティとプライバシの分野の研究では、それまでの技術中心であったセキュリティとプライバシの研究から、提案された技術を実際にユーザにより評価を行う社会学的な側面が含まれることとなった。研究が進む中で、技術中心で研究を行ってきた研究者が社会学的な側面を持つ技術の提案や実験を行う場合に、いくつかの不適切な評価が共通して行われることが目立ってきた。そこで Schecter はセキュリティとプライバシについて利用者（ユーザ）に関係する実験をして論文を書くときに陥りがちな落とし穴と、それの回避方法のガイドラインとなる文書を発表した [6]。

Schecter による文書は端的に重要な視点が記載されており、現在の SOUPS では Call for Paper においてこの文書を一読することが推奨されるなど、本研究分野で重要な位置を占める。

例を挙げると、仮説の明確化や明確な脅威モデルの提示、被験者行動の観察と評価についての注意深い記載、実験への倫理的な考察などが示されている。こういった部分は、国内の研究においても十分に考慮されなければいけない点であり、UWS 開催により土壌が培われていくことが期待されている部分でもある。

4. UWS2017 投稿論文概観

本章では、UWS2017 でどういった論文が投稿されたなどの概観を示す。

UWS2017 では 16 本の論文が投稿された [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22]。

その中では、認証を主題にした論文が 7 本と最も多く [11], [12], [13], [15], [16], [17], [18]、次いで暗号技術 [7], [8] がプライバシ [9], [10] それに続いた。そのほかには、ユーザインタフェース [14] やユーザの行動心理の調査 [21] といったものがあった。また、直接的なユーザブルセキュリティあるいはユーザブルプライバシの研究ではなく、その研究において重要となるユーザ実験での倫理面や同意取得についての詳細を紹介したメタ視点の論文 [19] もあった。

項目	該当論文
倫理関連の記載	[7], [8], [10], [19]
同意取得	[7], [8], [19], [22]
実験詳細記述	[7], [8], [14], [15], [16], [17], [21], [22]
被験者募集方法詳細	[7], [8], [10], [14], [19], [21]
クラウドソーシング利用	[10], [21]

表 1 UWS2017 論文における記載事項の特徴抽出

シンポジウム名	投稿論文数
UWS2017	16
CSS2017（UWS 以外）	205
CSS2016	192
SCIS2018	361

表 2 調査対象シンポジウムと投稿論文数

5. UWS2017 投稿論文の特徴分析

5.1 定性的評価

UWS が扱うターゲットでは、提案技術の評価にあたりユーザ実験を行うものが多くなる。UWS でもユーザ実験を行った研究は多く、16 本中 11 本の論文がユーザ実験を行っていた [7], [8], [10], [12], [14], [15], [16], [17], [18], [21], [22]。

Schecter 文書にあったように、ユーザ実験設定の詳細記述や、ユーザ実験を行うにあたっての倫理性の考察や同意取得、倫理委員会（Internal Review Board, IRB）からの承認といったことが明確に記載されていた論文も存在していた。

表 2 にそれぞれの項目があったと判断した論文を示す。

実験の詳細記述や被験者募集方法の詳細記述がされている論文が多く、社会学の側面が強い本分野の特徴となっていることが伺える。一方で、セキュリティやプライバシに関するユーザ実験で重要となる倫理に関する記載は 4 本にとどまっていた。ユーザ実験を 11 本の論文が行っている中で少ない数値とも思えるが、未記載の論文を概観すると、非常に限定された技術であることや、実証実験であり被験者のセキュリティやプライバシを棄損することでないことが明確であるがゆえに記載がされていないと思わしき論文も多くあった。

組織内の倫理委員会に関する記載があったのは 3 本だけであり [7], [8], [19]、こちらも少なさが伺えた。未記載の論文を概観すると、必要性こそ薄いものの委員会に通しておくことが望ましい論文もいくつかあり、この点での未成熟さが存在する可能性が考えられるものであった。一方で、UWS2017 では母体となっている CSS2017 に合わせてページ制限が 8 ページになっており、16 本中 12 本が 8 ページを満たすものとなっていたことから、記載するスペースの関係上倫理的な審査の記載が不要としたものがある可能性も考えられる。

5.2 定量的評価

前節では、UWS2017 に投稿された論文の特徴を定性的に評価したが、それが UWS2017 だけの特徴であるかの判断は難しい。そこで本節では簡易な調査をすることで、これまでの国内シンポジウムとの傾向を比較することとする。

傾向比較として、ユーザブルセキュリティとプライバシ研究において特徴的と思われるキーワードをリスト化し、各シンポジウム発表論文内にそれらのキーワードが含まれるかを調査した。調査のシンポジウム対象は CSS2016 と SCIS2018（2018 年暗号と情報セキュリティシンポジウム）とした。CSS2016 は、UWS2017 の母体となった CSS2017 の前年のシンポジウムであり、SCIS2018 は CSS と並んで国内最大規模のセキュリティ関連の学術イベントとなっているために選択した。また UWS2017 論文と CSS2017 の UWS 以外の論文も調査対象とした。

調査は単純なキーワード一致検索を行い実施された。具体的には、PDF ファイルを linux 上で pdftotext でテキストファイル化したのち、改行を除いた。その後、それぞれのテキストファイルに該当キーワードが含まれるかを grep コマンドにより調査した。

調査したキーワードは「実験」「被験者」「ユーザ実験」「ユーザ」「同意」「倫理」の 6 つとした。

「実験」「被験者」「ユーザ実験」「ユーザ」に関しては、ユーザ実験の有無を抽出を意図するためのものであり、技術的な提案においても実験を行うことは多いことからキーワード「実験」で実験を実施している論文の総数を測り、「被験者」「ユーザ実験」といったキーワードでユーザ実験を行っている論文を推測することを意図している。

また、Schecter 文書で明記されているなかで特徴的である「同意取得」や「倫理性」といった部分に焦点をあて、それらに言及をしている論文を抽出することで、UWS と他のシンポジウムの特徴の違いがでるかを見ることを目的に「同意」「倫理」のキーワードを含ませた。調査の結果を表 3 に示す。

6. 考察

得られた結果からいくつかの考察を行う。

まず UWS2017 では、これまでの国内論文とは異なる特徴として、ユーザ実験の多さや充実した実験内容の記載などが定性的に分析がされた。定量的評価の結果は、それらを裏付ける結果となったと言えよう。実験の実施については、キーワード「実験」の割合において UWS 以外のシンポジウムは 40-50%台である一方で UWS2017 論文は 93.75%となっており、実験実施の率が高いことが伺える。その実験にユーザ実験が多いこともうかがえる。キーワード「被験者」の出現割合が、UWS2017 では 75.0%であるのにくらべ、他のシンポジウムでは 1 桁台のパーセンテージ

キーワード	UWS2017	CSS2017	CSS2016	SCIS2018
実験	15 (93.75%)	117 (57.07%)	102 (53.13%)	154 (42.66%)
被験者	12 (75.00%)	8 (3.90%)	11 (5.73%)	13 (3.60%)
ユーザ実験	1 (6.25%)	0 (0.00%)	0 (0.00%)	1 (0.28%)
ユーザ	16 (100.00%)	113 (55.12%)	117 (60.94%)	143 (39.61%)
同意	3 (18.75%)	12 (5.85%)	13 (6.77%)	20 (5.54%)
倫理	4 (25.00%)	8 (3.90%)	4 (2.08%)	17 (4.71%)

表 3 各シンポジウム・ワークショップのおける特定キーワードを含んだ論文数と割合

となっている。キーワード「ユーザ」の出現割合はどのシンポジウム・ワークショップでも高いことから、UWS2017 でのユーザ実験実施の高さがわかる。

同意取得については、他のシンポジウムが 1 桁台のパーセンテージである中、UWS2017 は 18.75%と高い数字を示しているが、Schecter 文書の存在を考慮すると、決して高い数字とは言えず、分野としてはこの数字がより大きくなっていくことが望まれる。

倫理についても同様である。他のシンポジウムが 1 桁台のパーセンテージである中、UWS2017 は 25.00%と高い数字を示している。こちらについては、ユーザ実験を多く行う UWS の論文では当然である一方、近年のセキュリティの技術的な研究ではオフェンシブな研究も増えていることから、倫理についての検討や記述はセキュリティやプライバシの分野全体で推進されるべきことであり、UWS のみならず他のセキュリティシンポジウムでもこの数字が大きくなっていく必要があると考える。

7. 重要な制限

本論文の定量的評価においては、キーワードの検索を日本語だけで行ったが、各シンポジウム・ワークショップの投稿規定には日本語の必要性は指定されておらず、英語での論文記載も認められている。実際、SCIS や CSS では英文の論文も投稿されている。今回の実験では和文論文と英文論文の判別や分別は行っていないため、CSS や SCIS の傾向については厳密性を欠いている部分がある。具体的な数値がないためにその影響は不明確だが、英文論文の投稿数は多くはないため、傾向としては大差はないと考えられる。なお、UWS2017 に投稿された論文はすべて和文であったため、この制限にはかからない。

8. まとめ

本論文では、2017 年 10 月に開催されたユーザブルセキュリティシンポジウム（UWS）の投稿論文 16 本の特徴を分析し、これまでの国内シンポジウムとの比較を行った。その結果、分野的な特徴から多くの論文がユーザ実験を行っていることに加え、それら実験についての記述が詳細にわたっていること、また同意取得や倫理的な観点の記載などが行われている様子が見て取れた。一方でそれらの記載はまだ十分とは言えず、特にユーザ実験での同意取得に関する記載や倫理的な考慮についての記載は今後より多くなっていく必要がある。今後のユーザブルセキュリティあるいはユーザブルプライバシ研究がますますの発展を迎え、より利用者にとってユーザブルで安全な世界が推進されることを祈る。

参考文献

[1] A. Whitten, J. D. Tygar. Why Johnny Encrypt: A Usability Evaluation of PGP 5.0. In 8th USENIX Security Symposium. 1999. Microsoft Technical Report,
[2] 情報処理推進機構: 暗号に関する国内外のガイドラインの実態調査の調査報告書. https://www.ipa.go.jp/security/fy29/reports/crypto_survey/index.html, 2018
[3] ISO, W. 9241-11. Ergonomic requirements for office work with visual display terminals (VDTs). The international organization for standardization, 1998, 45: 9.
[4] 日本工業規格. JIS Z 8521 人間工学-視覚表示装置を用いるオフィス作業-使用性についての手引. 日本工業調査会, p2, 1999.
[5] NIELSEN, Jakob. Usability 101: Introduction to usability. 2003.
[6] S. Schecter. Common Pitfalls in Writing about Security and Privacy Human Subjects Experiments, and How to Avoid Them. https://goo.gl/bm2BwV, 2013
[7] 立川 彰宏 、 緑川 達也 、 金岡 晃 : オンラインストレージサービスに対するクライアント側暗号化と検索可能暗号のユーザビリティ評価、コンピュータセキュリティシンポジウム 2017（CSS2017）、2017
[8] 緑川 達也 、 立川 彰宏 、 金岡 晃 : ジョニーが検索するのを助ける : Web メールにおける対称型検索可能暗号の透過的適用、コンピュータセキュリティシンポジウム 2017（CSS2017）、2017
[9] 坂本 一仁 : Web トラッキングにおけるユーザブルプライバシーの調査、コンピュータセキュリティシンポジウム 2017（CSS2017）、2017
[10] 長谷川 彩子 、 秋山 満昭 、 八木 毅 、 森 達哉 : オンラインオークションにおけるプライバシーリスクとユーザ認識の調査、コンピュータセキュリティシンポジウム 2017（CSS2017）、2017
[11] 小林 良輔 、 佐治 信之 、 山口 利恵 : ライフスタイル認証の活用事例とその検証 : 低リスクシナリオ、コンピュータセキュリティシンポジウム 2017（CSS2017）、2017
[12] 大神 渉 、 五味 秀仁 : 利用者のコンテキストを信頼する同行者検証、コンピュータセキュリティシンポジウム 2017（CSS2017）、2017
[13] 加藤 大弥 、林 達也 、砂原 秀樹 : サイバーフィジカル時代の物理媒体による認証・識別に関する考察、コンピュータセキュリティシンポジウム 2017（CSS2017）、2017
[14] 皆川 諒 、 高田 哲司 : 馴化を抑制しうる新たなセキュ

リティ警告の探求:かわいいとその付加刺激の効果に関する評価、コンピュータセキュリティシンポジウム 2017（CSS2017)、2017
[15] 藤田 真浩 、眞野 勇人 、佐野 絢音 、高橋 健太 、大木 哲史 、 西垣 正勝 : 肌理を利用したマイクロ生体認証 : ユーザビリティ向上のためのプロトタイプシステム改良、コンピュータセキュリティシンポジウム 2017（CSS2017)、2017
[16] 山岸 伶 、 高田 哲司 : 私的な連想情報の再認による個人認証と安全性評価、コンピュータセキュリティシンポジウム 2017（CSS2017)、2017
[17] 佐野 絢音 、 藤田 真浩 、 西垣 正勝 : 機械解読耐性の向上とユーザのメンタル負荷軽減を両立する CAPTCHA 出題形式に関する検討、コンピュータセキュリティシンポジウム 2017（CSS2017)、2017
[18] 小林 心 、 小國 健 、 中川 正樹 : ボタン移動の追跡困難性を利用した覗き見耐性を持つ暗証番号入力手法、コンピュータセキュリティシンポジウム 2017（CSS2017)、2017
[19] 鈴木 宏哉 、山口 利恵 : 倫理審査, 同意取得, アプリ審査の壁を越えて…ライフスタイル認証実証実験の履歴収集に関して、コンピュータセキュリティシンポジウム 2017（CSS2017)、2017
[20] 金森 祥子 、 野島 良 、 岩井 淳 、 川口 嘉奈子 、 佐藤 広英 、 諏訪 博彦 、 太幡 直也 : プライバシーポリシーを読まない理由に関する一考察、コンピュータセキュリティシンポジウム 2017（CSS2017)、2017
[21] 西岡 大 、 大山 慎也 、 齊藤 義仰 : オンラインショッピングサイトにおけるユーザの安心感の数値化の検討、コンピュータセキュリティシンポジウム 2017（CSS2017)、2017
[22] 畑島 隆 、永井 啓太 、谷本 茂明 、金井 敦 : 大学生の情報セキュリティ疲れの可視化に関する一考察、コンピュータセキュリティシンポジウム 2017（CSS2017)、2017