解説

ユーザブルセキュリティ†

金岡 晃*

1. はじめに

情報通信技術が発展する中で守るべき情報やシステムが明確になり、防御するニーズとともにセキュリティ技術は発展していった。発展したセキュリティ技術は我々の生活の各所に浸透していき、いまやセキュリティ技術なしでは安全な世の中は実現しえないと言ってよいだろう。

会員諸氏もさまざまな形でセキュリティ技術と触れる機会が多いのではないだろうか。たとえばエンドユーザとして、Web上のサービスやスマートフォンアプリケーションで認証を求められる場面があるだろう。あるいは開発者として、開発しているシステムやソフトウェアでデータの暗号化や改ざん防止を施す場面があるだろう。そして研究者として、データの漏えいや悪用の可能性を検討する場面があるだろう。

様々な場面においてセキュリティ技術と触れ合い、扱うことが多くなってきているが、一方でこういった印象はないだろうか。曰く「セキュリティは外部から『やれ』と言われていたからやっている」。このことはある種の本質を突いているといえる。Web上のサービスやスマートフォンのアプリケーションに代表されるような我々が利用あるいは開発するソフトウェアやシステムは、情報の交換や商取引、娯楽などさまざまな目的を持つ。セキュリティ自身はそれらのソフトウェアやシステムの本来の目的ではない。少し乱暴な言い方をすれば、セキュリティ自身は本来目的達成のためには不要であり、本来目的を「安全に」達成するために必要となる非機能要件なのだと位置付けることができよう。現代では「本来目的を安全に達成すること」は当然のように求められるようになったため、必須の条件として考えられることも多くなったのだろう。

セキュリティ技術に適切に情報などの資産を保護すると、必要な機能以外は制限されることが一般的である。そういった制限はソフトウェアやシステムを快適に利用することを妨げてしまうことがある。それがゆえにユーザは使いづらさを感じ、「セキュリティとユーザビリティはトレードオフである」といったことが言われるようになった。急激な情報通信技術による生活の発展が従来では考えられなかった脅威を生むことになり、使いづらさはありながらもセキュリティはされなければならない状況となり、現在まで続いているのだろう。

そんな中、学術的なセキュリティの研究に1つの流れが起きた。本来目的を阻害することなく、ユーザが効率的に有効的にそして満足のいく形でセキュリティを実践できる「ユーザブルセキュリティ」がそれである。20年ほど前から始まったこの潮流はいまはセキュリティやプライバシーの学術研究において大きな位置を占めており、それらの成果が着実に世の中に展開されていっている。そして今、新たな段階に踏み出した時期にある。

ユーザブルセキュリティの研究はセキュリティやプライバシーの技術面だけでなく、心理学や社会学、行動経済学などを取り入れたアプローチがされている。その裾野はさらに広がりつつあり、本学会がサポートする分野を含む広範な分野に至ると考えられる。

本稿は、ユーザブルセキュリティの研究成果や動向を概観し、会員諸氏に知っていただくことでセキュリティは決してユーザの負担になる作業ではないことと、負担軽減に向けた研究開発が進んでいることを認識いただくことを第1の目的とし、広くわたる本分野への興味を持っていただくことで裾野の拡大に寄与することを図るものである。

2. 研究アプローチ

ユーザビリティにより提供される効率や有効性そして満足度は、ユーザにより異なるものである。ユーザ全員が高いユーザビリティを達成することは難しいが、できるだけ多くのユーザに高いユーザビリティを提供したい。そこで重要になるのがユーザの行動原理である。ユーザの行動原理を知りその原理に合わせた方策を提供することで多くのユーザにとっての高いユーザビリティを望むことができる。

工業製品のユーザビリティは長い間の知見があるため、ユーザの行動特性は十分に調査されてきた。一方で、情報通信技術が急激な発展を迎えた現代は、あまりに早く広がったためにユーザの行動原理が分かっているものも多い。たとえばインターネットやスマートフォンによる行動様式の変化などがある。2000年代に入る前には電車内で新聞を読む乗客はたくさんいたが、いまでは貴重なものとなっている。電車内は読書といった情報のインプット場所だけでなく、SNSなど情報のアウトプット場所ともなった。そういった行動の原理の変化は、まだ判然としていない部分が多い。

そのため、ユーザブルセキュリティの研究では、まず研究対象に関するユーザの行動原理を知ることから始められることがほとんどである。それらを把握したうえで、有効な対策が提案されていく。

† Usable Security
Akira KANAOKA

* 東邦大学
Toho University

行動原理の調査や対策の有効性評価にはユーザ実験が欠かせない。ユーザブルセキュリティでは、実験参加者にアンケート回答を求めたりマイクロタスクと呼ばれる小さな作業を主にオンラインでもらいその結果を集計・分析する量的評価と、実験参加者に実際に提案手法を実施してもらいその模様を録画や録音をした後にインタビューを行いその結果を集計・分析する質的評価に二分される。

量的な評価では Amazon Mechanical Turk (MTurk) が用いられることが多く、他の研究との比較のときにはプラットフォームとして MTurk で揃えることを行っている研究もある。

質的な評価は多岐にわたるが、実験参加者へのインタビューを半構造化インタビュー手法で深く参加者に語ってもらい、そこで発せられた言葉などをまとめることでグラウンデッド・セオリーを作り出す GTA (Grounded Theory Approach) が多く行われている。

3. 代表的な事例

ここでは学術研究の成果が実社会に活かされている代表的な事例を2つ挙げる。

3.1 パスワード管理

2009年、米国のWebサービスであったRockyou.comが侵入を受けた。Rockyou.comは会員のIDとパスワードを暗号化せずに保管していたために、侵入により3200万を超える会員のパスワードが盗まれた。これほどの大規模な漏えい事件はあまりなく大きなインパクトを持って迎えられたが、そのパスワードデータがWeb上公開されたことでさらに注目を浴びた。皮肉なことに、この公開データがパスワードに関する研究を飛躍的に向上させることになる。

2010年WeirらはRockyouデータを用いた分析を行い、ユーザが設定するパスワードの特徴を詳細に明らかにした[1]。例をいくつか挙げよう。ユーザがパスワードを生成するときの制約として「数字を少なくとも1つはつけるように」というものがある。そういったケースでは、ユーザの6割以上がパスワードの最後にまとめて数字を付ける傾向にあることがこの研究で示された。またその時に1割を超えるユーザが「1」を使うことなど、いくつかの視点でのユーザ特性が明らかにされた。Weirらはそれら特徴を盛り込み、効果的にパスワードを推測する手法を示した。

大量のデータにより学習された推測手法は高い精度でパスワード推測を可能にする一方で、研究者らはその推測手法を強度評価に用いた。ある制約を設けた場合に実験参加者が生成したパスワード群へ推測手法を適用し、どれほどのパスワードが推測されるかを測り、その制約がもたらすパスワード強度への影響としたのである。これにより、入力されたパスワードの強度を示すパスワード強度メータ[2]や、種々のパスワード構成ポリシ[3]の効果や有効な手法などが明らかにされていった。

同じ時期にもう1つ興味深い研究が行われた。Zhangらは、パスワードの定期的な変更が強制されたときのユーザの振る舞いを調査した[4]。その結果、変更を強制されたユーザの多くは簡単な変更だけを行うことや、数回の変更を経て元のパ

図1 Google Chrome 37でのWebサーバ証明書エラー画面 (2014年7月)

スワードに戻るケースがあるなど、その効果への疑義が示された。

これらの成果は、米国標準技術研究所(NIST)が発行するドキュメントSP 800-63の改訂に影響を与えた。それまでは定期的な変更の推奨などが書かれてきていたものが、2017年の改訂ではその文言が消え、むしろ非推奨と明記されることとなった[5]。その影響は日本へと及び、2017年の総務省「国民のための情報セキュリティサイト」では定期的な変更が不要なことが明記され、2018年に改訂された内閣サイバーセキュリティセンター「ネットワークビギナーのための情報セキュリティハンドブック」でも同様の記載がされるなどの影響を与えた。

パスワードに関する学術研究の進展が社会へ展開した良い例と言えるだろう。

3.2 ブラウザの表示

現代のブラウザは単にWebサイトの情報を表示するだけでなく、さまざまなサービスのインターフェースとして重要性が増している。ブラウザを介したリスクも増大していく中で、ブラウザを提供する事業者もさまざまなリスクの表示を工夫してきている。そこにユーザブルセキュリティ研究の成果が活かされている。

SSLやTLSを使ってWebアクセスをするときに、Webサーバの電子証明書が使われるが、その証明書がなんらかの理由で正しい状態にないときにブラウザは警告を出す。Google Chromeでは2014年のChrome 37より証明書のエラー表示画面を一新した。それまでの画面ではビジュアル表示に黄色を用い文章も技術用語の多いものだったが(図1)、ビジュアル表示をグレーをベースに赤いアイコンとし、文言も簡易なものに変更した(図2)。

この変更は、Feltらの研究結果をもとに行われた[7]。彼女らの研究では、さまざまなアイコンや色、文言などを用意しそれらを異なるユーザ群で実験をし、効果的な表示が何かを探っていた。そのほかにもGoogle Chromeでは自社の研究グループの研究成果をもとにインターフェースを変更するなど活発な研究が行われている。

図2 Google Chrome 79 での Web サーバ証明書エラー画面 (2019 年 12 月)

4. 特定の属性を持つユーザ集団

パスワードやブラウザの表示は広範なユーザに影響を与えるものであり、2000 年代半ばから 2010 年代半ばまでは、そういった一般ユーザが広く使うプラットフォームを対象にユーザブルセキュリティの研究が多くされてきた。スマートフォンのユーザインタフェースやアプリケーションへのパーミッション付与のやり方、あるいは Web サービスの規約 (Terms of Use) の同意などもこういった一般ユーザ向けの研究として進められてきた。

2010 年代半ばに入り、その傾向に変化が訪れだした。最も大きな変化は、研究対象となるユーザの集合が一般ユーザから特定の属性を持つ集合へ移っていったことだろう。Web サービスにおける認証の困難性を視覚障害者の視点から調査したものや、子供のインターネット利用におけるプライバシー、ソフトウェア開発者の暗号利用、高齢者のインターネット利用、金融関連企業の雇用者のセキュリティへの姿勢など、大きな展開を迎えた。

Dosono らが行った視覚障害を持つユーザに対する調査では、意外とも思える結果が並んだ [8]。実験では既存の Web サービスにログインをしてもらうというものであったが、実験参加者の多くが実験の完了ができなかったと報告した。そして、そもそもページ上でログイン要素の識別ができないことや、アクセスした段階では当該 Web サービスに誰かがログイン中なのか誰もログインしていないのかの状態確認が難しいことや、サイトに記載してある内容を音声で読み上げるスクリーンリーダが読むコンテンツの順番と実際に UI 上で並んでるコンテンツの配置に関連はなく認証のフォームにたどり着くことが難しいことなど、多くのことが判明した。認証のユーザビリティ議論をする前にそもそも認証行為自身ができなかったのである。

2014 年の Li らは、中国で漏洩したパスワードのデータセットを用いて、中国人が生成するパスワードの特徴を分析した [9]。その結果が示したものは Weir らの調査と大きく異なったものだった。たとえば、Rockyou データではパスワードの構成はアルファベットのみを使ったユーザが最多であったのにく

らべ、中国のパスワードデータセットは数字だけで構成されたパスワードが最多となっていた。中国では携帯電話のショートメッセージサービス (SMS) が多く使われており、そういったインフラの利用状況の違いが影響した可能性があることが示唆されていた。2018 年に森らも日本人を対象にパスワード生成の特徴を調査し、これまでの研究にあったユーザ母集団とは違う傾向を示すことを明らかにするなど、技術の普遍性への疑問と改良の余地が示された [10]。

こういった研究により、ユーザの母集団が変わることでその技術の効果が大きく変わる可能性が示された。このあたりから、ユーザブルセキュリティの研究は研究コミュニティとして新たな方向に動き出すことになる。

ソフトウェアやシステムの開発者はさまざまな知識を動員して開発していかなければならないが、その必要な知識にはセキュリティも当然含まれる。しかしセキュリティはそのソフトウェアやシステムの本来目的ではないためか、優先度は下がってくる。優先度が低い状態でソフトウェアやシステムにセキュリティを施すと、脆弱性が生まれやすくなる。そこに着目したソフトウェアやシステムの開発者に向けたユーザブルセキュリティ研究は、いま最も盛んな研究分野となっている。

知識獲得に余裕がない開発者は、そのソフトウェアやシステムの主要な機能に注力して知識獲得を行い開発を行う。そのためにセキュリティの部分については十分な知識を持たないために、できるだけ簡易に済ませるような対応を取るのかもしれない。その兆候はさまざまなところで見られている。暗号に用いる鍵をソフトウェアのソースコードにそのまま記載しているケースや、乱数生成の種 (シード) を固定にしているケース、証明書検証時に内容がなんであろうと常に検証成功と判定するケース、動作はするが脆弱性があるコード断片 (スニペット) をコピーしてそのまま流用するケース、などさまざまである。

開発者向けユーザブルセキュリティとしては、その行動原理の把握や対応など、多くの研究が行われている。それらは暗号技術を中心に展開されており、開発者の多くが簡単な暗号技術でさえ誤った使用をすることが多いことを示した研究や、マーケットに展開されている多くのアプリケーションで暗号利用の不備が見つかった研究、各種の暗号 API の誤使用発生の多さとその原因の研究などが行われている。得られた行動原理からの応用として、統合開発環境において誤使用と思しき部分があった場合の警告システムなども研究されている。

開発者向けユーザブルセキュリティは、いま 1 つの岐路にあると言ってもよい。複雑化するセキュリティ技術を適切に採用してソフトウェアやシステムを開発することの困難性はあがり、従来のように開発者自身がセキュリティを学び自身のソフトウェアやシステムに採用することは現実的ではなくなった。ユーザブルセキュリティの研究としては重要なテーマであるが、研究の帰結として開発者がどうあるべきかの議論は十分にされているとは言えない。開発者自身がセキュリティを安全に適用することが難しくなったのなら、セキュリティのソフトウェアやシステムへの適用は自動化あるいは他の補助ツールに依存して開発者はあまり意識しないままにセキュリティを実現するのか、あるいは、開発者自身が安全に適用することを可能

にそのような教育やチュートリアル、サンプルコードなどを充実させるのか、どちらの方策を取るかで研究のアプローチも大きく変わる。この点はまだ結論が出ていない問題であり、今度双方の研究が進んでいく中で進む方向が見えてくるものと考えられる。

5. 再現性への挑戦

前章で挙げたユーザ集団の違いによる実験結果の違いは、研究コミュニティに新たな課題を投げかけた。これまでに培われてきた知見が誤って利用される可能性に気づいたと言えよう。

同時期に心理学の研究分野を中心にユーザ実験の再現性への疑問が大きく議論されるようになった。2015年にNosekらは、心理学研究100件の再現実験の結果、当初の報告と同じ結果になったものは39%にとどまったと報告した[11]。この研究は国内でも大きなニュースとなった。Nosekらの研究自体にはその手法に批判があるなど数値をそのまま信頼することに躊躇はするものの、再現性に問題がある点が脚光を浴びた影響は少なくなかっただろう。

ユーザブルセキュリティの研究コミュニティは過去の研究に対する再現性の検証やユーザ集団を変えたときの差異についての調査研究を広く受け入れるようになった。この分野を牽引する国際会議 Symposium on Usable Security and Privacy (SOUPS) では Call for Paper (CFP) に追試 (Replication Study) の受け入れを積極的に行う旨が示されている。SOUPS 2016のCFPに募集する論文の種類として「reports of replicating previously published studies and experiments」が項目の1つに入り、SOUPS 2017ではさらに協調され以下の3つの視点での追試研究が募集された。

- Full replication (完全追試) : 同じ実験手順と同じタイプの集団
- Variation (変種) : 1つのデザイン変数が変わったもの。たとえば同じアンケートを同じサービスの別集団で行うことや、ユーザ実験を異なる国で行うことなど。
- Triangulation (三角測量) : 同じ目的での実験であるが、その実験手法が異なるもの

こういったアプローチはこれまでの研究を支えるためにも重要であり、今後もこの傾向は続くと思われる。そしてこの傾向はともすれば世界的には後発であった日本のユーザブルセキュリティ研究コミュニティにとって大きなチャンスとなる。各地域でのローカライズ研究は、ユーザブルセキュリティ分野に留まらずアジアを中心に日本も得意とするところであり、それらを発展させた統合的な研究も期待することができる。

6. 時代の変化とトラスト

先述した再現性問題は、ユーザ母集団の違いだけでなく、同じ背景を持つ母集団でも起きうる。その最たるものが経年変化である。

2013年にRuotiらはメッセージ暗号化のユーザビリティ向上の研究成果において、興味深いユーザの振る舞いを紹介した[12]。電子メール等のメッセージを暗号化して送信すると

きに、インターフェース上にランダムな文字を出すことでメッセージが暗号化された様子を表す手法と、インターフェース上では通常と変わりなくメッセージの暗号化が自動的に（彼らはそれを透過的と呼んでいる）行われる手法を比較した場合、後者の手法でしばしば実験参加者が混乱することを示した。実験参加者のある一定の数が「暗号化される情報はランダム化された文字として表示される」という思いがあり、そういった表示が無いことで混乱をきたし、自動的に暗号化されているにもかかわらず暗号化をしなくてはという考えに至り逆に暗号を解く行動を取ってしまうものであった。この振る舞いは2014年のFahlらの研究でも同様のことが示されていた。

2016年にBaiらが発表した研究では、メッセージの暗号化において透過的に暗号化をしても利用者は混乱せずに利用できていることが示されていた[13]。Ruotiらの研究が示した振る舞いと逆のものである。この結果の違いは、実験手法の違いや母集団の違いなどに起因するものかもしれない。しかし著者はこれを母集団の経年での変化だと捉えた。RuotiやFahlらの研究からBaiらの研究までの間に、社会ではメッセージの暗号化において大きな変革を迎えていた。それまではユーザが明示的に暗号化の作業を行うあるいは暗号化ソフトウェアをインストールしなければ実施されてこなかったエンド間での暗号化が、設定無しあるいは簡単な設定のみで実施されるようになってきた。この時期に、WhatsApp、Facebook messenger、LINEなど代表的なメッセージングツールが次々とエンド間暗号化（エンドツーエンド暗号化）を採用している。それらはいずれもランダム化された文字は見せず、Ruotiらの言う「透過的な」暗号化が施されている。こういった世の中の動向がユーザの振る舞いに影響した可能性は高いと著者は考える。

これが示すものは、ユーザビリティの評価は地域や文化の違い、年齢といった母集団の違いにも依存するだけでなく、ほぼ同じ母集団であっても経年変化が起これば数年後には評価が異なってしまうことである。ユーザの行動原理は不動なものではなく、急激な発展を遂げ続けている情報通信技術に従いユーザ集団自身が変わっているのだ。正しいユーザブルセキュリティの技術は現時点では望めないのかもしれない。現時点での最良な手を模索し、それらの改良を定期的に行っていくことが重要になっていくのだろう。

そういった流動性はなぜ起きるかを考えたときに1つヒントとなるのが信頼（トラスト）かもしれない。研究コミュニティではまだ深い議論はされていないものの、ユーザブルセキュリティが達成すべき要素には満足度といったユーザの心理に由来するものが含まれている。ユーザはいつ満足するかを考えたときに、その技術自身や技術を提供している事業者への信頼が関わってくるのではないか。だれも知らない組織が新しく出した技術と、技術的な高評価を社会から得ている組織が新しく出した技術では、同じ技術だったとしても後者がユーザブルセキュリティとして高く評価されるのではないか。

中谷内は過去の研究での言及をまとめ、信頼を「信頼とは相手の行為しだいで被害を被る危険性も、よい結果が得られる可能性もあるという状況の中で、よい結果が得られるだろうと期待して、被害を被りうる（vulnerable）立場に身を置こうとい

う心理的な状態」と定義した [14]。ICT の発展により急激に生活が変わる中、ソフトウェアやシステムのセキュリティを満足するためにはその技術自身や提供する事業者の信頼が重要であり、今後のユーザブルセキュリティはトラストを含めた議論が進んでいくだろう。

7. まとめ

本稿では、サービスなどの本来目的を阻害することなくユーザが効率的、有効的に、そして満足のいく形でセキュリティを実践できるユーザブルセキュリティについて成果や動向を解説してきた。

ユーザブルセキュリティの業界は、いままさに新たな展開を迎えたところである。

本稿はセキュリティに注力した紹介をしたが、当然プライバシーとその保護技術についてもユーザビリティの問題があり、ユーザブルプライバシーとして議論されている。

同時に、新しい技術の流入も盛んである。新しい技術が社会に広まると、そこにセキュリティとプライバシーの問題は起こる。近年であれば、Google Home や Amazon Echo に代表されるスマートスピーカーが挙げられる。すでにプライバシーの問題等の技術面での学術的な調査は進んでいるが、それらを生活において利用するユーザのセキュリティとプライバシーに対する姿勢や振る舞いの調査はまだ始まったばかりである。そういった新しい技術の登場とともにさらにユーザの行動原理が調べられ、明らかになっていくであろう。

本稿をご覧になった諸氏が日頃触れ合う技術にはきっとセキュリティとプライバシーの問題が存在していて、解決することが負担になっているかもしれない。ユーザブルセキュリティはその負担を取り除く試みであり、どのユーザにも身近なものである。我々はユーザブルセキュリティ研究の進展が社会へ届く努力を続けるとともに、諸氏が新たに我々のコミュニティに気軽に参加してくれることも強く期待するものである。

参 考 文 献

- [1] M. Weir et al.: "Testing metrics for password creation policies by attacking large sets of revealed passwords," *Proc. of the 17th ACM Conf. on Computer and Communications Security*, pp. 162-175, 2010.
- [2] B. Ur et al.: "How does your password measure up? the effect of strength meters on password creation," *Proc. of the 21st USENIX Conf. on Security Symp.*, 2012.
- [3] P. G. Kelley et al.: "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms," *2012 IEEE Symp. on Security and Privacy*, 2012.
- [4] Y. Zhang, F. Monrose, and M. K. Reiter: "The security of modern password expiration: An algorithmic framework and empirical analysis," *Proc. of the 17th ACM Conf. on Computer and Communications Security*, 2010.
- [5] P. A. Grassi et al.: "Digital Identity Guidelines: Authentication and Lifecycle Management," *No. Special Publication (NIST SP)-800-63B*, 2017.
- [6] 総務省, 国民のための情報セキュリティサイト: https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/ [accessed Mar. 10, 2020]
- [7] A. P. Felt et al.: "Improving SSL warnings: Comprehension and adherence," *Proc. of the 33rd Annual ACM Conf. on Human Factors in Computing Systems*, 2015.

- [8] B. Dosono, J. Hayes, and Y. Wang.: "“I’m Stuck!”: A Contextual Inquiry of People with Visual Impairments in Authentication," *11th Symp. on Usable Privacy and Security*, 2015.
- [9] Z. Li, W. Han, and W. Xu: "A Large-Scale Empirical Analysis of Chinese Web Passwords," *23rd USENIX Security Symp.*, 2014.
- [10] K. Mori et al.: "Comparative Analysis of Three Language Spheres: Are Linguistic and Cultural Differences Reflected in Password Selection Habits?," *2019 IEEE European Symp. on Security and Privacy Workshops*, 2019.
- [11] A. A. Aarts et al.: "Estimating the reproducibility of psychological science," *Science*, Vol.34, No.6251, aac 4716-4716, 2015.
- [12] S. Ruoti, et al.: "Confused Johnny: when automatic encryption leads to confusion and mistakes," *Proc. of the 9th Symp. on Usable Privacy and Security*, 2013.
- [13] W. Bai et al.: "An inconvenient trust: User attitudes toward security and usability tradeoffs for key-directory encryption systems," *12th Symp. on Usable Privacy and Security*, 2016.
- [14] 中谷内一也: リスクの社会心理学, 有斐閣, 2012.

(2020 年 2 月 21 日 受付)

[問い合わせ先]

〒274-8510 千葉県船橋市三山 2-2-1

東邦大学理学部

金岡 晃

TEL: 047-472-8676

E-mail: akira.kanaoka@is.sci.toho-u.ac.jp

—— 著 者 紹 介 ——

かなおか あきら
金岡 晃 [非会員]

2004 年筑波大学大学院博士課程システム情報工学研究科修了。同年セコム(株)入社。筑波大学システム情報工学研究科研究員、同助教を経て 2013 年より東邦大学理学部講師。2017 年より准教授。2010–2016 年情報通信研究機構招へい専門員、2016–2018 年放送大学非常勤講師。セキュリティとプライバシーのユーザビリティ、暗号技術の応用、ネットワークセキュリティに関する研究に従事。