（1）タイトル

開発者に対するデセプションを用いたユーザ調査研究の仮想事例

（2）本文

セキュリティの研究に従事する研究者Aは、ソフトウェアの開発段階で発生しうるセキュリティ問題に着目した研究を進めていた。昨今のソフトウェアはOSS（オープンソースソフトウェア）として開発されることが一般的であるため、研究者AもOSSの開発プロジェクトに目を付けた。OSSとは、ソースコードが一般に公開され、誰でも自由に使用、変更、配布することができるソフトウェアのことを指す。多くの場合、OSSはコミュニティベースの開発プロジェクトによって開発される。このようなオープンな開発においては、開発者やユーザーは、ソフトウェア開発への参加、バグ報告、改善点の提案などが自由にできる。

ある時、研究者AはOSSの開発プロジェクトはオープンであるがゆえに悪意のある第三者（攻撃者）が開発に紛れ込むセキュリティ脅威の可能性があることを思いついた。具体的には、攻撃者が脆弱性（本来意図しない動作によってセキュリティ問題を引き起こすバグ）や悪性な機能（バックドアなど）を気付かれないように仕込んだコードを善意の開発者を装って開発プロジェクトに投稿することで当該OSSに混入させることができる、というセキュリティ脅威である。

研究者Aは、このセキュリティ脅威がどれほどの影響があるのかを検証することで問題提起をしようと考えた。一方で研究者Aは、検証のための実験をする際に、ラボテスト（対象を実験室のような特別な環境で調査すること）では生態学的妥当性（ecological validity）の問題があることを懸念した。生態学的妥当性とは、実験環境が現実の状況をどれだけ反映しているのかを示す考え方である。現実の状況と実験室研究に大きな違いがある場合に、実験室研究で得られた実験結果には一般性や信頼性が低くなり、実験結果に基づいた提案や対策が効果的に機能しない可能性がある。

研究者Aは、生態学的妥当性を高めるために、実在するOSSプロジェクトにおいてこのセキュリティ脅威を検証することを計画した。研究者Aが実験対象に選んだのは、あるOSS開発プロジェクト（仮にOSS-X開発プロジェクトと呼ぶ）である。OSS-X開発プロジェクトは、PCを始めモバイルデバイスやIoT機器などで共通的に利用されている暗号通信ライブラリを開発しており、世界中から多数の開発者が参画している。OSS-X開発プロジェクトで脅威が実証できればこれ以上ないインパクトであると考えたからである。

研究者Aはさらに高い生態学的妥当性を実現するために実験をよりリアリティのある状況で実施しようと考え、実験意図を事前に伝えない“デセプション”と呼ばれる方法を用いることにした。具体的には、OSS-X開発プロジェクトの責任者や開発者には実験を実施することは一切伝えず、研究者が偽名で参加した上で善意を装ったコード修正パッチを投稿する。このパッチには脆弱性を誘発するコードが隠されている。もしOSS-X開発プロジェクトで実施されているコードレビュープロセス（投稿されたコードの機能性やセキュリティ問題の有無などを審査する工程）で気づかれることなく、このパッチが採用された場合には“攻撃が成功した”とみなせる。

研究者Aは、この実験を実施するにあたって、所属組織の研究倫理審査委員会に申請するかを悩んだ。研究倫理審査委員会は基本的にはヒューマンファクター研究（人間を対象にする研究）を範囲に

している。しかし、この実験は特定の個人を直接的に対象にする実験ではなく対象はOSSプロジェクトという組織であり、さらには組織内部のコードレビュープロセスを対象にしているため、研究者Aはこの実験が研究倫理審査委員会の審査対象であるかよくわからなかった。研究者Aは悩んだ結果、“ヒューマンファクター研究ではない”として研究倫理審査委員会に報告し、研究倫理審査委員会からは審査の免除を受けた。

研究者Aは審査の免除を受けたため、OSS-X開発プロジェクトに対するデセプションに基づいた実験を開始した。研究者Aは生態学的妥当性を損なわないようにOSS-X開発プロジェクトに対して事前に実験意図を伝えることなく、身元を偽り善意の貢献者として脆弱性を誘発するコード修正パッチを投稿する実験を実施した。これによってOSS-X開発プロジェクトの正規の開発者らは当該パッチの真意を知ることなくコードレビュープロセスを実施し労力を費やすことになった。結果として、投稿した脆弱性を誘発するコード修正パッチはコードレビュープロセスにおいて採用基準を満たさず拒否されたため、実験自体がOSS-X開発プロジェクトのコードに悪影響を与えることはなかった。このため、研究者AはOSS-X開発プロジェクトに実験を実施したことも報告しなかった。その後、研究者Aは攻撃のコンセプト、実験結果、攻撃成功率を向上させるためのさらなるアイデア、およびOSS開発プロジェクトにおける対策手法をまとめて論文を公開した。

その後、OSS-X開発プロジェクトの責任者や開発者らは、研究者Aの公開された論文によって当該実験が実施されたことを初めて知った。OSS-X開発プロジェクトの責任者Bは当該実験が一切の通知もなく実施されていることに強い懸念を持ち、他の潜在的な実験事例の可能性を疑った。最終的に、責任者Bは過去数年にわたって投稿された全てのコードを再度検証するという判断をした。この再検証に多数の開発者の膨大な時間と労力を費やす結果になった。

その後、OSS-X開発プロジェクトは、研究者Aおよび所属大学に対して実験に関する強い抗議を表明するとともに、当該開発プロジェクトへの今後の関与を禁止した。事態を重く見た研究者Aおよび所属大学は、実験内容や手順および審査プロセスが不適切だったことを認め、論文を取り下げた。

（3）考えてみよう

（3−1）現状の研究倫理審査委員会の倫理審査の範囲と限界

一般的に、研究組織（大学、研究所、病院等）毎に設置されている研究倫理審査委員会は、世界医師会による「ヘルシンキ宣言」（1975）[1]、米国生物医学および行動学研究の対象者保護のための国家委員会による「ベルモントレポート」（1979年）[2]、また日本では文部科学省等による「人を対象とする生命科学・医学系研究に関する倫理指針」[3]などの趣旨に沿って、人を対象とする研究が倫理的に実施されているかを審査します。人を対象とする研究とは、人由来の試料(血液・体液や抽出された DNA 等、個人に関する情報など)を用いた研究、研究対象者の行動情報（反応時間等）・生理指標（心拍数等）・脳活動（fMRI等）等を計測・評価する研究、アンケート調査研究などが含まれる場合などです。なお、人を対象とする研究は、生命科学・医学系研究以外の分野も当てはまり、日本心理学会の倫理規定においても倫理的な基礎理念および倫理上の方針が示されています[4]。同様に、日本社会学会、日本文化人類学会（旧、日本民族学会）などでも同様の研究倫理規程が整備されています[5][6]。

一方で、2000年代以降はICT（情報通信技術）やコンピュータセキュリティの発達によって、これまで想定されなかった新たな研究倫理の問題が顕在化しました。例えば、従来の人を対象とする研究では対面に実験参加者がいて実験の影響を直接的に観察することができますが、しかしICTの発達によって、実験の対象が対面にいるとは限らないこと、実験の影響が瞬時に世界に波及しうること、システムの脆弱性は間接的に個人や組織に損害を与えうること、などが挙げられます。ベルモントレポートの倫理原則をICT・コンピュータセキュリティの文脈で再考し、さらに新たに倫理原則を加えた「メンローレポート」が2012年に米国国土安全保障省から発表されました[7]。メンローレポートでは、研究対象が直接的な個人であるかを超えて研究の倫理指針を示しています。

しかし、日本を含めた世界各国の研究機関における研究倫理審査委員会の大多数は「ヘルシンキ宣言」「ベルモントレポート」などに基づいた「人を対象とする研究」を審査の対象にしているため、上記仮想事例にあるように、研究が”個人”かどうかが審査の要否の分かれ目になっており、コミュニティや組織のプロセスなどは定義が曖昧であるために、見過ごされてしまいました。

サイバーセキュリティの著名国際会議であるUSENIX Securityの投稿ポリシーでは、研究倫理審査委員会の審査を推奨するものの、研究倫理審査委員会の限界（コンピュータセキュリティ研究をよく理解しているわけでも、この分野のベストプラクティスやコミュニティ規範を知っているわけでもないこと）を指摘しており、承認/審査免除されたからといって研究者が倫理的側面への配慮を免除されるものではないとしています[8]。直接的に「人を対象とする研究」かどうかや研究倫理審査委員会の承認/審査免除を超えて、研究者には、研究の利益が害を上回る理由、安全性を確保する方法、潜在的なリスクを最小限に抑えるための方法と実践、ベストプラクティス、などについて実践と論文上での明確な記述が求められています。

（3−2）ユーザ調査における倫理的なデセプション実施

ユーザ調査においてデセプションはどのように倫理的に実施すればいいでしょうか？

デセプションは実験参加者の自然な行動や反応を観察する方法の一つとして用いられています。しかし、上記仮想事例のように、実施方法によっては実験参加者に対して身体的・心理的に過度なストレスや不快感を与える可能性があります。このようなリスクを回避するために、以下の観点で研究を進めることが一般的です[4][5][6][9][10][11][12]。

・研究計画の立案：研究目的、デセプションの必要性、デセプションが実験参加者に与える可能性のあるリスクや不利益について検討して明確にする。また代替手段がないかを検討し、もしあればデセプション以外の方法を用いる。
・第三者によるリスクアセスメントの実施：研究グループとは独立した第三者（例えば組織の研究倫理審査委員会や組織長など）に研究計画を提出し、デセプションを含む研究の倫理的妥当性について承認を得る。
・インフォームド・コンセント（事前同意）の取得：可能な限り実験参加者に研究の概要とリスクを説明し、同意を得る。
・実験の実施：研究計画に従ってデセプションを実施する。実験参加者の権利や尊厳を尊重し、過度な身体的・心理的なストレスや不快感を与えないよう注意する。

・デブリーフィング（事後説明）：実験終了後、速やかに実験参加者に対してデセプションの内容とその理由を説明する。実験参加者の質問に真摯に答え、必要に応じて身体的・心理的サポートを提供する。実験に協力しない（当該参加者の実験データの削除等）という選択肢も提供する。

デセプションでは、実験前に実施するインフォームド・コンセントにおいて完全な説明ができないことから、実験後に実施するデブリーフィングが重要になります。つまり、”騙したまま”で研究を終了してはなりません。デブリーフィングで実験参加者に対して真摯に説明および対応することで納得してもらうことが重要です。

今回の事例では、「第三者によるリスクアセスメントの実施」は研究者の所属組織においては審査免除になっていて十分に審査できていないこと、「インフォームド・コンセント（事前同意）の取得」は実施されていないこと、また「デブリーフィング（事後説明）」も実施されておらず、論文公開後に当該実験参加者（参加の意思はそもそも確認されていないので自由意志の参加ではないが）が知ることになった点などが、研究者AとOSS-X開発プロジェクトの対立を深めた要因になりました。

なお、「インフォームド・コンセント（事前同意）の取得」については、コミュニティに対して実施する場合についてさらに（3−3）で議論します。

（3−3）コミュニティに対するユーザ調査におけるコミュニティオーナーとの協議

ユーザ調査において参加者個人への実験前のインフォームドコンセントは重要であるが、コミュニティに対する調査を実施する場合はどのように実施すればいいでしょうか？

コミュニティに対する調査を実施する際には、事前にコミュニティオーナー（自治体の代表、団体の責任者など）に調査の詳細を説明し、協力を依頼することが望ましいです。コミュニティオーナーを通じて、コミュニティ全体に情報共有を行い、理解と支持を得ることが重要である。コミュニティオーナーの許可を得ることは、研究者とコミュニティの信頼関係が構築でき、調査の透明性向上と説明責任を果たすことでコミュニティの利益や期待に調査内容が一致しやすくなること、またコミュニティからの連携・協力が得られやすくなります。特にデセプション調査は参加者に対して身体的・心理的な影響を与える可能性が高いことから、慎重な調査方法の設計とコミュニティから事前に理解と許可を得ておくことが安全です。

なお、コミュニティによっては当該コミュニティに対する調査のガイドラインが設定されているものや、調査の事前相談を受け付けているものもあります。
例えばTor Project（オンラインプライバシーとセキュリティを向上させることを目的して、インターネット上の匿名通信を可能にするオープンソースのソフトウェアTorなどを開発するプロジェクト）[13]では、Tor Safety Research Board[14] を設置し、研究者がTorに対するセキュリティ・プライバシー調査研究を実施する際に安全に実施するためのガイドラインや事前相談を実施しています。この取り組みによって、研究者は事前に実施する研究内容がTorやそのユーザを危険に晒すことがないかをTor Porject側から確認することができます。

これ以外にも、研究コミュニティとしての互助的な取り組みとして、コンピュータセキュリティシンポジウム（CSS）では2018年からサイバーセキュリティに関する研究倫理相談窓口が設置されています

[15]。本倫理相談窓口はサイバーセキュリティに関する専門家、法学、弁護士などの有識者から構成され、倫理的に判断が難しい研究や実験について適切な対応方法に関するアドバイスをしています。

[参考文献]

[1] 日本医師会, WMAヘルシンキ宣言,
<https://www.med.or.jp/doctor/international/wma/helsinki.html>

[2] 米国「生物医学および行動学研究の対象者保護のための国家委員会 (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research)」, The Belmont Report, <https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html>

[3] 文部科学省, 厚生労働省, 経済産業省, 人を対象とする生命科学・医学系研究に関する倫理指針, 令和3年3月 23 日
<https://www.meti.go.jp/press/2021/03/20220310006/20220310006-1.pdf>

[4] 日本心理学会, 日本心理学会倫理規定
<https://psych.or.jp/wp-content/uploads/2017/09/rinri_kitei.pdf>

[5] 日本社会学会, 日本社会学会倫理綱領にもとづく研究指針
<https://jss-sociology.org/about/researchpolicy/>

[6] 日本文化人類学会, 日本文化人類学会倫理綱領 <https://www.jasca.org/onjasca/ethics.html>

[7] 米国国土安全保障省, The Menlo Report,
<https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf>

[8] USENIX Security '24 Submission Policies and Instructions
<https://www.usenix.org/conference/usenixsecurity24/submission-policies-and-instructions>

[9] University of California, Berkeley, DECEPTION AND INCOMPLETE DISCLOSURE IN RESEARCH <https://cphs.berkeley.edu/deception.pdf>

[10] 日本社会心理学会, NHK「大心理学実験」関連情報,
<https://www.socialpsychology.jp/pr/jssppr/topics/bigpsyexp_nhk/>

[11] 一般社団法人社会調査協会倫理規程 <https://jasr.or.jp/chairman/ethics/>

[12] 眞嶋 俊造・奥田 太郎・河野 哲也『人文・社会科学のための研究倫理ガイドブック』慶應義塾大学出版会. <https://www.keio-up.co.jp/np/isbn/9784766422559>

[13] Tor Project <https://research.torproject.org>

[14] Tor research Safety Board <https://research.torproject.org/safetyboard/>

[15] コンピュータセキュリティシンポジウム（CSS）<https://www.iwsec.org/css/>