サイバーセキュリティ研究における倫理的配慮のサポート

応般

秋山満昭 | NTT セキュアプラットフォーム研究所　島岡政基 | セコム（株）IS 研究所

サイバーセキュリティ研究を取り巻く状況

サイバーセキュリティの研究は，十分に前例のない領域を研究対象として取り扱うことが多く，一方でその行為が社会に対して直接的な影響を与え得るために“倫理的”な問題にも直面しやすい．より先進的で革新的な研究を実施する場合はなおさらである．たとえば以下に示す状況において，研究者はどのように行動すればよいかについて，ICT 技術・社会的状況・法制度などのさまざまな観点から議論が尽きない．

- ネットワーク上に蔓延する脆弱なデバイスを発見するためのネットワークスキャン
- セキュリティ上の欠陥を発見するために実在するシステムに対して行う調査
- 欠陥や脆弱性を発見した場合に発見者としてとる行動

このような研究にはステークホルダ（利害関係者）が存在し，彼らは研究成果の恩恵が得られる一方で，研究行為やその結果の公表によって被害を受ける可能性もある．研究行為そのものや成果の世の中への伝え方を誤ったが故に，世間から批判される事例や法廷闘争に発展する事例が多々ある．このような研究行為のグレーゾーンにおいては倫理的な研究プロセスが必要であるということが国内外のさまざまな研究コミュニティにおいて広く議論されている．つまり，無責任に危険な実験を実施したり攻撃手法・脆弱性をむやみに公開するのではなく，研究が世の中に与える影響を考慮した上でどのように倫理的に取り組めばよいかを考えることは今日のサイバーセキュリティ研究者としての必須の素養となっている．しかし一方で，進展の早いサイバーセキュリティの分野では十分に議論されていない領域の倫理的問題に研究者が直面することがしばしばある．そのような判断が難しい状況において，研究者自身の自己責任とするのは研究者の萎縮を招く可能性がある．このような萎縮によって科学技術の発展が妨げられるのは避けなければならず，研究コミュニティとして先進的な研究をサポートするために何ができるのかを考えなくてはならない段階に入っている．

研究倫理原則

研究倫理は幅広く大きい概念である．研究倫理の全体像とセキュリティ研究が特に対象とする研究倫理の関係について，後述の日本学術振興会サイバーセキュリティ第 192 委員会ワーキンググループがとりまとめた図 -1[☆1] に基づいて説明する．科学と科学的知識の利用について概念的にまとめた「ブダペスト宣言」（1999 年）や日本学術会議の「科学者の行動規範」に関する声明（2006 年）は，さまざまな研究分野に共通的なベースとなる研究倫理の要素から構成されている．文部科学省は特に，研究活

☆1 サイバーセキュリティ研究における倫理的な研究プロセスの普及啓発について．http://www.iwsec.org/mws/2018/20181220/jsps-192-ethicsWG.pdf より抜粋．

動の不正行為（捏造，改ざん，盗用等）の観点からの研究倫理とその対応に関するガイドライン（2006年）を発行している．米国政府委員会は，生物医学分野などの人を取り扱う研究における研究倫理原則をとりまとめたベルモントレポート（1979年）を発行している．このベルモントレポートでは3つの研究倫理原則として以下のように示されている．

- **人格の尊重（Respect for Persons）**
  研究の実験への参加は本人の自由意志によって決められるべきであり，本人への十分な説明をした上で本人が意思決定する権利を尊重すること（インフォームドコンセントの考え方）．
- **恩恵（Beneficence）**
  研究により得られ得る恩恵を最大にし，与え得る危害を最小にするためのリスクアセスメントを行うこと．
- **正義（Justice）**
  個人の扱いについて平等に配慮を行い，また研究の恩恵は平等に分配し，負担は研究対象に対して同等に分担すること．

ベルモントレポートの研究倫理原則を踏襲しつつ，ICT/セキュリティ研究に対応したメンロレポート（2012年）が米国国土安全保障省によって発行された．メンロレポートでは，3つの研究倫理原則をICT研究の文脈で解釈することに加えて，下記の研究倫理原則を新たに追加している．

- **法と公益の尊重（Respect for Law and Public Interest）**
  法令を遵守し，公共の利益の尊重すること．研究方法と結果の透明性を担保し，その行為に責任を持つこと．

メンロレポートで新たに追加されたこの原則は，地域間における法律の対立や曖昧さ，ステークホルダの特定の難しさ，法と公益の間の不一致，などを明示したものである．たとえば，研究過程でセキュリティホールを発見した場合は，ステークホルダを特定して，被害を最小化した上で世の中に情報を伝えるための責任ある情報開示（Responsible disclosure）を実践しなければならない．

メンロレポートは今日のICT/サイバーセキュリ

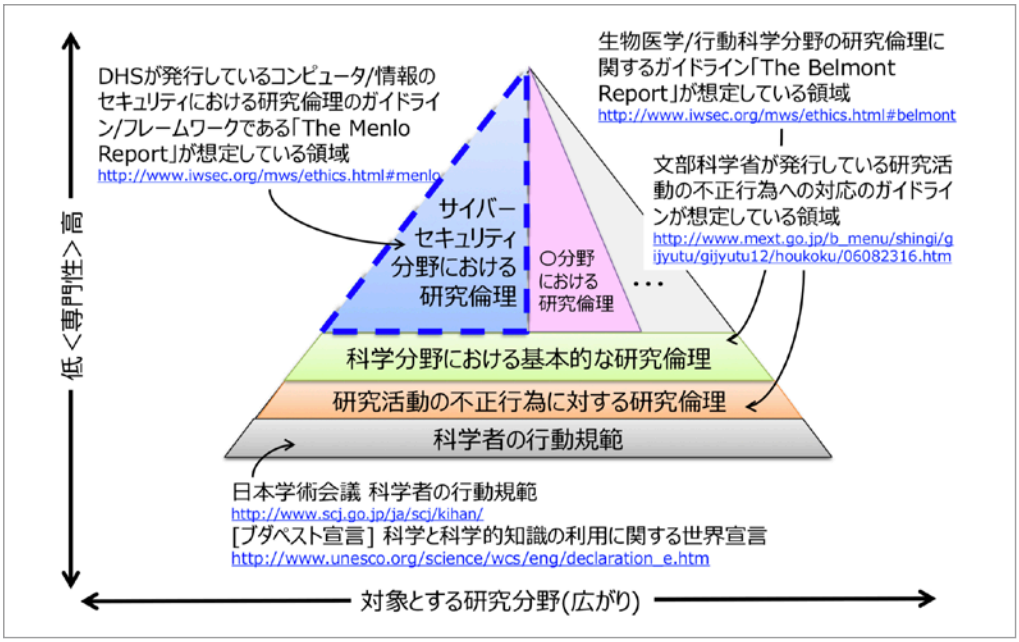

図-1
研究分野と専門性に対応する各種研究倫理原則

ティ研究の倫理原則として認識されているが，この原則をさまざまな状況で適切に実践することは容易ではない．たとえば，大規模なユーザデータを取り扱う際のインフォームドコンセントの取り方，複雑な分散 ICT 環境においてインフォームドコンセントを獲得する主体の特定が容易ではないこと，影響が瞬時に伝達される状況におけるリスクと被害についての迅速かつ的確な判断等，これらはベルモントレポートが制定された当時では想定し得なかった環境条件に基づいて実施される場合の難しさである．

世の中の動向

このようなサイバーセキュリティの研究倫理への関心の高まりを受けて，学術国際会議において研究倫理の議論が取り上げられることが増えてきた．サイバーセキュリティ研究倫理をテーマとした新たな学術国際会議として CREDS や NS-Ethics（2013 ～ 2015 年）が開催され，研究倫理の議論が不十分だった過去の研究事例の再レビュー，ベストプラクティスの共有，倫理的な研究プロセスの設計，などを実施し，ICT 環境の変化に対応したよりよい倫理的研究のサポートを試みている．また，サイバーセキュリティのトップ学術会議である IEEE S&P・ACM CCS・USENIX Security・ISOC NDSS では，2013 年頃から Call For Paper において「研究倫理の議論を喚起しそうな論文については，適切な手順に基づいてどのように実施しているかを明記すること」を求めており，不適切な論文は採択されない可能性があることが明記されている．

トップ国際会議論文に学ぶ倫理的配慮

では実際に世の中のサイバーセキュリティ研究者はどのように倫理的に研究を実践しているのだろうか？　サイバーセキュリティ分野のトップ国際会議の 1 つである USENIX Security において，メンロレポート発行以降の 2012 年から 2019 年までに発表された論文の中から研究倫理の言及がある約 100 本の論文について研究倫理に関する記述を調査した．その結果，研究倫理の議論・主張や実践について大まかに以下のように分類できた．

- **同意・許可の獲得**
  実験の対象になる主体（ユーザ／サービス事業者／ネットワーク管理者等）からの同意・許可を得ている．
- **行為の正当性**
  ガイドラインやポリシーに準拠している．データを匿名化している．法律に準拠している．Responsible disclosure を実施している．ほかに代替手段がない．
- **所属組織の承認**
  所属組織の研究倫理委員会（Institutional Review Board，IRB）から研究内容に関するレビューを受けた上で研究実施の許可を得ている．
- **リスクアセスメント**
  実験を行うことによって生じる新たなリスクはない．リスクや実際の被害を最小化するための努力をしている．
- **公益性**
  ベストプラクティスを共有している．公共の利益に貢献している．

これらはさまざまな研究行為に対して実施されたある種のベストプラクティスと位置付けることができ，同様の研究行為を行う場合に大いに参考にすべきケーススタディである．

倫理的配慮をサポートするための試行

前述のとおり，2012 年に発行されたメンロレポートによって欧米の学術国際会議を中心としてサイバーセキュリティ分野における研究倫理の認識が広がっていった．日本においても，2016 年頃からマルウェア対策人材育成ワークショップ（MWS）を

中心とした研究コミュニティにおいて多数のイベントが開催され，現状の認識，課題の整理，ベストプラクティスの共有，アクションプランなどが話し合われている[1]．2018年には，日本学術振興会のサイバーセキュリティ第192委員会にワーキンググループが設置され，学会横断的にサイバーセキュリティ研究倫理の啓発活動が推進されている．また同年，日本最大級の学術セキュリティシンポジウムであるコンピュータセキュリティシンポジウム(CSS)において，サイバーセキュリティに関する研究倫理委員会が設置され，論文投稿を検討する研究者に対しての研究倫理相談窓口が開設された．さらに2019年には，CSSは「サイバーセキュリティ研究における倫理的配慮のためのチェックリスト」（以降，チェックリスト）を整備し，論文投稿予定の研究者が活用できるようになった．以降では，研究倫理相談窓口とチェックリストの詳細な説明を行う．

研究倫理相談窓口の設置

CSSで設置された研究倫理委員会は，サイバーセキュリティの専門家や法学者，弁護士から構成されている．本研究倫理委員会は「研究の承認」を行うことを目的としておらず，研究倫理相談窓口（以降，相談窓口）を研究者とのインタフェースとして適切な倫理的配慮の実施をサポートすることを目的としていることが特徴である．相談窓口は，論文募集要項の発表から発表申込締切までを問合せ受付期間として開設している．論文投稿を検討しているが研究倫理的に不安のある研究者は，相談フォームに記入の上，相談窓口に問い合わせる（図-2）．相談フォームでは，研究者が実施しようとしている研究内容，研究倫理上考えられる問題点とその対応案等を記入するようになっている．相談窓口では，受け取った相談内容を内部の委員間で整理した上でレビューする．委員は，類似の研究事例・倫理的対応や法制度・社会情勢を調査した上で，研究行為のステークホルダの識別と，相談内容に関する回答，および参考情報や事例を相談者である研究者と共有している．

これまでに6件の相談(2018年4件, 2019年2件)があり，5営業日以内での回答を行っている．2019年に問合せが減少した原因の1つとして，後述するチェックリストの活用によって，基本的な懸念については解消された可能性がある．

チェックリストの試行

2018年の相談窓口の知見から，2019年はサイバーセキュリティ研究における倫理的配慮のためのチェックリスト[2]を整備し，相談窓口と併せて活用を推奨することとした．チェックリストの目的は，当該論文に倫理的配慮の観点を著者らに認知してもらうこと，その上で必要に応じて論文への記載を検討してもらうこと，そしてそれらが実施されたことの観測の3点とした．すなわち，回答が適切であれば倫理的問題がないことを保証するものではなく，また不適切だからただちに倫理的問題があることを意味するものではない．チェックリストは，現時点における共通的な落とし穴（Common pitfall）を列挙することに注力し，主に1）基本事項の確認，2）機微情報の扱い，3）ネガティブな影響に関する配慮の3項目（全9項目）とした．

プライバシや広域スキャンなどに関する項目についても議論はあったが，回答者の負担増や回答精度

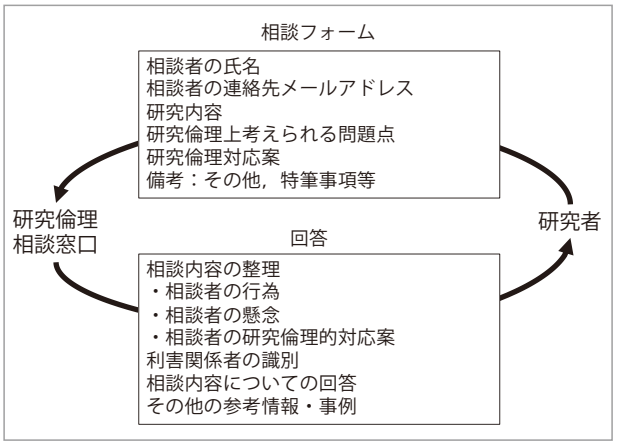

図-2　研究倫理相談窓口

の低下，また長期的な視点からリストの肥大化を避け基本原則の確認に注力すべき，などの議論を経て，きわめてシンプルなものにとどめた．項目数を厳選した一方，倫理的配慮の知識が不十分な著者でも回答できるよう，いくつかの項目には解説や参考事例を補記し読解性に配慮した．

これら項目の解説やチェックリストの趣旨などについては，投稿締切までのコンピュータセキュリティ研究会（CSEC）において何度か企画セッションを設けて周知を行った．

チェックリストは投稿時のセルフチェックとし，チェックの有無にかかわらず投稿は可能としたところ，投稿 223 件[☆2] 中 216 件（96.9%）がチェックしたとの回答を得た．

倫理的配慮を実施する論文の推移

さて，これまで日本のコミュニティが行ってきた前述の啓発活動，研究倫理相談窓口，チェックリストは，どの程度の効果があっただろうか？　効果の一側面ではあるが，倫理的配慮について言及する論文の推移について過去 4 年間の CSS 論文と USENIX Security 論文を調査した（図 -3）．USENIX Security では毎年 10 本を超える論文が研究倫理の配慮に関する記述を行っており，その数は年々増加している．CSS では 2016 年にはそのような論文はわずか 1 本であったが，年々増加傾向にあり，2018 年の 9 件から 2019 年では 17 件と倍近く増加している．これは，倫理的配慮が必要な先進的な研究が増えてきたこと，そして倫理的配慮を実施して論文中に記述するという意識が広まってきたことが要因として考えられる．

☆2　最終的な投稿受理件数．発表申込時点では 257 件．

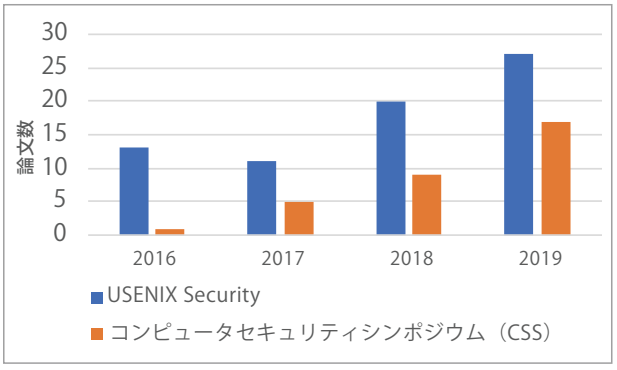

図 -3　倫理的配慮を実施する論文の推移

今後の展望

チェックリストのフィードバック分析

論文投稿者の一部から，チェックリストのチェック結果について具体的な回答 22 件を得て，分析を行った．このうち機微情報を扱ったものは 8 件あり，いずれも論文中で適切に明記したとの回答を得た．また，ネガティブな影響を含むものは 15 件あり，うち該当するすべての項目について適切に論文に記載したものは 6 件，一部明記しなかった論文が 6 件，特に明記しなかった論文が 3 件であった．これらの比率や件数についてはサンプル数が少ないため議論を避けるが，一定の配慮がされているものも少なくないこと，また明記しなかった論文についても，チェックリストを通じて配慮の余地があることを著者らに認知することができたと考えられる．

これら著者からの任意のフィードバックとは別に，最終的に収録された論文 223 件について倫理委員会有志にて分析した結果，前述の通り倫理的配慮が明記された論文 17 件を確認した．また，一部には倫理的配慮のためにチェックリストを活用したとの記述もあった．前述の通りチェックリストは倫理的問題の有無を保証する性質のものではないが，一方で研究コミュニティにおけるコンセンサスに基づいたある種の行動指針となる可能性が示されたと考えている．

チェックリストのアップデート

これらのフィードバックや，国内外のサイバーセキュリティ研究およびその倫理的配慮に関する最新

動向を踏まえながら，チェックリストのアップデートに取り組んでいきたいと考えている．啓発を強化する観点では，既存項目も含め解説や事例の充実を図っていきたい．特に事例に関しては，サイバーセキュリティの分野は（たとえばサービス妨害攻撃と判断されるアクセス頻度の多寡のように）社会理解の変化も著しく，事例が陳腐化しやすいケースもあるため，細心の倫理的配慮の動向に注意を払いながら事例を示していく必要があると認識している．また，サイバーセキュリティ分野と一口に言っても範囲は広く，プライバシや広域スキャンへの配慮など取り組んでいくべき領域は少なくないと認識している．一方で，前述の通りチェックリストの肥大化は望ましい方向性ではないとも考えており，安易に項目数が増加しないよう最大限の注意を払っていきたい．

啓発活動の横展開

本取り組みはコンピュータセキュリティシンポジウムを端緒としているが，同シンポジウムに限らずサイバーセキュリティに関連する研究コミュニティに幅広く関係する問題である．CSS およびその主催研究会である CSEC の啓発活動を通じて，他学会も含めいくつかの研究コミュニティから関心を寄せられている．

有志の負担に依存せずに取り組みを広げていくためにも，前述の解説や事例の充実がポイントとなる．チェックリストの試行はもちろんのこと，解説や事例の充実に貢献いただける有志も大いに歓迎したい．また，CSS に限らず各シンポジウムや研究会など研究コミュニティで必要に応じて相談窓口を設置することも検討いただければ幸いである．窓口を介した相談プロトコルは図 -2 が参考になるだろう．

最後に，セキュリティ分野に限らず，たとえば適用領域における社会変化や技術革新の著しい分野等においても，研究倫理的課題に直面している研究分野は少なからずあるのではないだろうか．直接的に資する点はそれほど多くないかもしれないが，研究倫理的課題に対する研究コミュニティとしての取り組みにおいて，本活動が多少なりと参考になれば幸いである．

参考文献

1) マルウェア対策人材育成ワークショップ（MWS），サイバーセキュリティ研究における倫理的な研究プロセスについて，https://www.iwsec.org/mws/ethics.html
2) コンピュータセキュリティシンポジウム（CSS）2019，サイバーセキュリティ研究における倫理的配慮のためのチェックリスト，https://www.iwsec.org/css/2019/ethics_list.html

（2019 年 12 月 27 日受付）

秋山満昭（正会員） akiyama@ieee.org

2007 年奈良先端科学技術大学院大学情報科学研究科修士課程修了．同年日本電信電話（株）入社，NTT 情報流通プラットフォーム研究所にてマルウェア対策技術の研究開発に従事．2016 年 NTT セキュアプラットフォーム研究所特別研究員．2019 年同所上席特別研究員．主としてサイバー攻撃対策技術の研究開発に従事．博士（工学）．電子情報通信学会・IEEE 各会員．

島岡政基（正会員） m-shimaoka@secom.co.jp

1998 年慶應義塾大学大学院理工学研究科修士課程修了．同年セコム（株）入社．2004 年より同 IS 研究所．2005 ～ 2010 年まで国立情報学研究所特任准教授（後に客員准教授），2019 年より筑波大学システム情報系客員准教授を兼務．2014 年総合研究大学院大学複合科学研究科情報学専攻博士課程修了．博士（情報学）．認証基盤とトラストの研究開発に従事．本会コンピュータセキュリティ研究会幹事（2015 年～），本会セキュリティ心理学とトラスト研究会運営委員（2014 ～ 2017 年），本会論文誌ジャーナル /JIP ネットワークグループ編集委員（2015 ～ 2018 年）．本会論文誌ジャーナル編集委員会副編集長／ネットワークグループ主査（2018 年）．