コンピュータセキュリティシンポジウム 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

はじめに

このチェックリストは、学術論文の投稿において、サイバーセキュリティ研究に関する典型的な倫理的配慮を著者らに啓発することを主たる目的としています。著者らの研究によっては必ずしも該当しない場合もありますし、チェックリストには記載のない、より高度な倫理的判断が必要となるケースもあります。投稿論文について、このチェックリストの下記項目で確認した上で、より踏み込んだ倫理的配慮の必要性を感じる場合は、学会・研究会等の設置する研究倫理委員会・相談窓口へ別途ご連絡ください。
このチェックリストは著者らの実施状況について把握する目的で回答いただくものです。投稿審査や免責を伴うものではありませんので、事実のままご回答いただくようご協力ください。
なお、チェックリストの回答内容および相談窓口等への相談に関わらず、倫理的な責任は最終的に著者らが負うものであることをご注意ください。

回答収集へのご協力のお願い

みなさまにセルフチェックいただいた結果の提出は必須ではありませんが、差し支えなければGoogleフォームからの回答にご協力いただけますと幸いです(回答はCSS2019開始まで更新可能です)。ご提出いただいた回答は、本シンポジウムのプライバシーポリシーにもとづいて保護され、論文番号と回答者メールアドレスを除く回答部分は、統計情報として公開する可能性がありますことをご了承ください。

投稿論文について、以下について該当するものを選択してください。

(1) 基本的確認

(1-1) 情報処理学会の倫理綱領を確認している。

[Yes, No]

(1-2) 研究・実験に用いた製品やサービスの使用許諾書等に記載されているセキュリティ評価や分析について関連する条項を確認した。

[Yes, No, 該当なし]

(2) 実験のために収集した機微な情報に関して

(2-1) 個人を特定可能な情報(PII, Personally Identifiable Information)を含む機微な情報の取り扱いに配慮したこと、およびその配慮をどのように実施したかについて、文中に明記している。
[Yes, No, 該当なし]

解説：実験が及ぼす影響として、(観測実験に含まれるPIIや場合によってはIPアドレス、URLなども含め)実験参加者のプライバシーや実験で利用するサービスへの負荷なども必要に応じて考慮されるべきです。
参考事例： Mark Allman and Vern Paxon, "Issues and Etiquette Concerning Use of Shared Measurement Data", IMC 2007. (観測データの取り扱いに関するポリシー)

(3) 実験の実施や論文の公開による”ネガティブな影響”について

(3-1) 事前に（製品名・サービス名や、攻撃対象・攻撃手法などの公開に伴う）”ネガティブな影響”の検討を行った。
[Yes, No, 該当なし]

(3-2) 検討結果を踏まえて、関係者への通知（直接通知 or 届出制度を利用）を事前に行った。
[Yes, No, 該当なし]

(3-3) 文中に製品・サービスの具体名を表記している、もしくは、容易に推測できる記述がある場合、そのように記述することの妥当性を検討した。
[Yes, No, 該当なし]

(3-4) 上述の“ネガティブな影響”を最小化するための対策について、また論文で取り上げた対象以外に他の製品・サービス等への影響についても検討した。
[Yes, No, 該当なし]

(3-5) (3-1)～(3-4)の検討内容に関して、必要の程度で文中に明記した。
[Yes, No, 該当なし]

解説1: ここで言う”ネガティブな影響”とは、新たな脆弱性や攻撃手法の発表、あるいは既存の脆弱性・対策の検証など、実験の実施や論文の公開による製品・サービスの関係者(利用者・提供者など)が被るであろうことであり、例えば関係するサービスやサービス提供者への負荷の増加・危害などが挙げられます。

解説2：製品・サービスは商用・非商用に限りません。具体名を記載する場合は、それによってベンダ・組織・個人などの利害関係者に与える不利益を最小化することが、倫理的配慮として期待されます。 このためには、基本的には事前に提供元に確認を取り、協調的に対応を進めていくことが求められると同時に、具体名を記載することの妥当性を文中に明記することが期待されます。

解説3：製品やサービス等の脆弱性を公表することは、場合によっては結果としてベンダのみならず利用者にも危害を及ぼす可能性があります。利害関係者への事前情報開示に努め、危害を最小化することが倫理的配慮として期待されます。 脆弱性の公表に関して、提供元に確認する行為が著者らにも不利益となり得る場合は、例えば脆弱性情報届出制度等を活用するなどが考えられます。 こうした既存の枠組みでは不適切・不十分な場合や、やむを得ない事情で事前の確認が困難な場合などは、先行事例などを参考にしつつ独自の取組みを試みることが必要になるかも知れません。また、その合理性を示すとともに、確認を取らないことによって生じ得る提供元などの危害を最小化するための工夫を示すことが期待されます。
参考事例： IPA, "情報セキュリティ早期警戒パートナーシップガイドライン"

解説4：論文で取り上げた対象以外に他の製品・サービス等にも影響する可能性がある場合、特定の利害関係者のみに不利益が集中しないよう、その影響についても公正に論文中で論じることが期待されます。 例えばAndroidの脆弱性について言及しているが、iOSにも共通する可能性が高いなどであれば、特定の製品・サービスに限った問題ではないことを、(確認済事実や未確認ながら容易に推定可能など)その確度含めて明らかにしておくことが、倫理的配慮として期待されます。