MWSプレミーティング

研究倫理について：Hypocrite Commits論文の状況から考える

2021年6月2日

秋山満昭

Hypocrite Commits（偽善者のコミット）論文

NTT

ミネソタ大の研究者が “脆弱性入りのパッチ” をLinuxカーネルにコミット

目的：故意に脆弱性を入れた偽装性の高いパッチをコミットすることができる、それをカーネル開発者が見分けることが難しいことを実証したい

2020年8月 著者らが身元を偽って５件のパッチをコミット

2020年11月 IEEE S&P2021論文採択・論文公開

2020年12月1日 Sarah Jamie Lewisが公論文の研究倫理について懸念、S&P2021に意見書送付

2020年12月15日 著者ら「人間が関わる研究ではないので研究倫理審査の免除を受けた」との声明発表

2021年4月6日 著者らは新しい研究プロジェクトの実験として低品質のパッチを大量にコミット

2021年4月20日 Linuxカーネル開発者の**Greg Kroah-Hartman氏が強い批判**、ミネソタ大の全コミット調査

2021年4月21日 高まる批判を受け **ミネソタ大が関連する研究プロジェクトの中止** と詳細調査/対応を宣言

2021年4月23日 Linux Foundationがミネソタ大に意見書送付

2021年4月26日 **著者らによる論文取り下げ**

2021年5月6日 IEEE S&P2021が経緯と再発防止のための声明発表

研究者側

開発者側

学会

何が問題だったのか？今後どうすればいいか？

- 研究倫理審査委員会（IRB）はうまく機能していたか？
- 査読プロセスはうまく機能していたか？
- このような実験をする際の倫理的な手順としてどうすべきだったか？
- 今後、研究コミュニティとしてどのような取り組みをすべきか？

Hypocrite Commits論文後のIEEE S&P 2021の反応

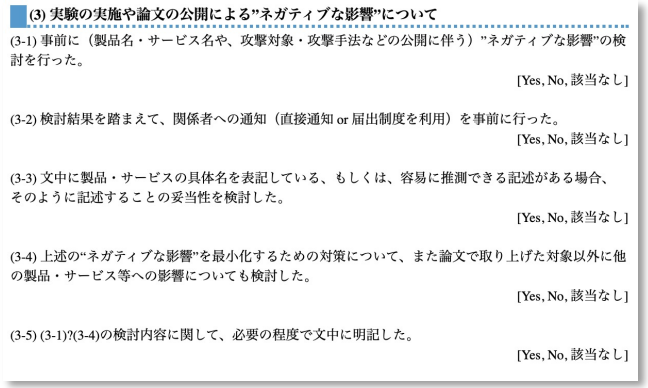
- Hypocrite Commits論文に関する声明
  - https://www.ieee-security.org/TC/SP2021/downloads/2021_PC_Statement.pdf
- S&P2022での対策
  - プログラム委員会にEthical Review Committeeを設置、全ての論文を研究倫理の観点からチェック
    - › IRB承認を受けているかにかかわらず、研究行為そのもので判断する
    - › 倫理原則にそぐわない論文はそれを理由にRejectされることがある
  - 投稿時の研究倫理チェックボックス追加
  - 査読時の研究倫理チェックボックス追加
  - CFPで研究倫理を強調

奇しくもCSSで既に実践していた！

研究倫理で迷ったら

- **① 指導教官/上長に懸念点を伝えて相談する**

- ② CSS研究倫理チェックリスト
  - 基本的な注意事項をまとめたチェックリストを参考にセルフアセスメントをしてください



(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]

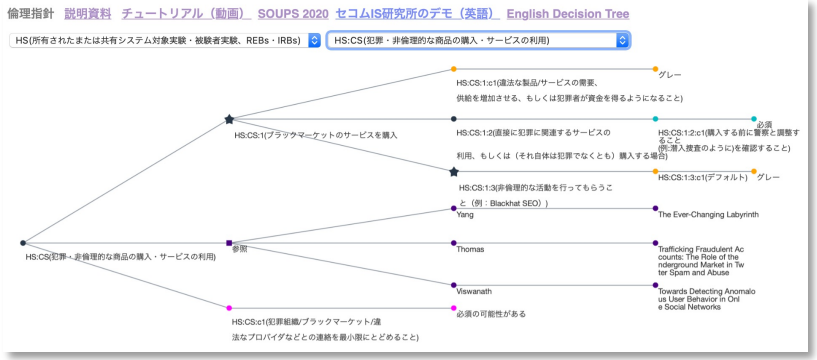
(3-5) (3-1)?(3-4)の検討内容に関して、必要の程度で文中に明記した。
[Yes, No, 該当なし]

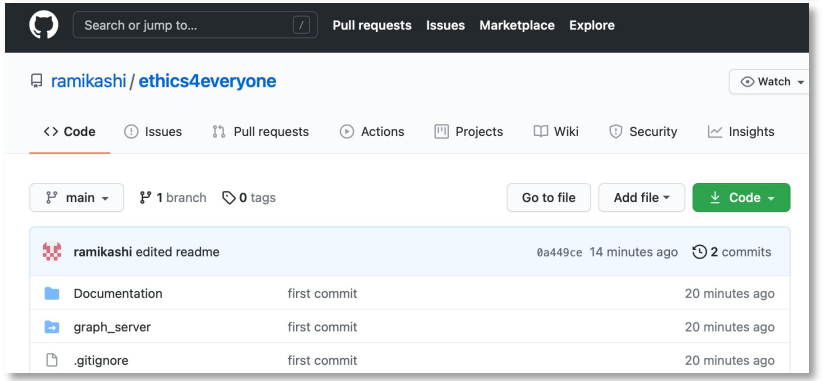
- ③ CSS研究倫理相談窓口
  - チェックリストではカバーできない難しい問題に関しては相談窓口に相談してください
    - › 昨年のページ https://www.iwsec.org/css/2020/ethics.html
  - 相談受付期間はCSS論文締切の約2週間前ぐらい

==========(相談フォーム)==========
相談者のお名前:
相談者の連絡先メールアドレス:
研究内容:
※研究倫理的にどのような問題が生じ得るかを検討するため，計画している（または実施中の）研究内容をできるだけ詳細に
研究倫理上考えられる問題点:
※研究内容についてご相談者ご自身が考える研究倫理的問題点
研究倫理対応案:※上記問題への対応案
希望トラック:
備考:その他，特筆事項等があればお知らせください
==========

研究コミュニティでの “知見の活用” に向けて

- 知識ベースと研究倫理決定木
  - セコム様開発のツール、過去論文の倫理的判断をDB化、UIでインタラクティブに検索
  - すでに議論/実践されていること・されていないことがわかる
  - オープンソース化
    (https://github.com/ramikashi/ethics4everyone)
- 研究コミュニティで
  活用できないか？
  - 誰がどう使う？維持管理は？
  - まずはCSS研究倫理TF（相談窓口）
    で活用してみる予定





Ramirez et al., A Cybersecurity Research Ethics Decision Support UI, SOUPS2020 poster session.
Ramirez et al., Knowledge-Base Practicality for Cybersecurity Research Ethics Evaluation, UWS 2020.

参考情報

- On the Feasibility of Stealthily Introducing Vulnerabilities in Open-Source Software via Hypocrite Commits
  - https://github.com/QiushiWu/QiushiWu.github.io/blob/main/papers/OpenSourceInsecurity.pdf
- Report on University of Minnesota Breach-of-Trust Incident
  - https://lkml.org/lkml/2021/5/5/1244
- Statement from CS&E on Linux Kernel research
  - https://cse.umn.edu/cs/statement-cse-linux-kernel-research-april-21-2021
- Ethical conduct in cybersecurity research
  - https://davisjam.medium.com/ethical-conduct-in-cybersecurity-research-86d13b6b6eed
- Clarifications on the “hypocrite commit” work (FAQ)
  - https://www-users.cs.umn.edu/~kjlu/papers/clarifications-hc.pdf
- Program Committee Chairs Report for the IEEE Security and Privacy Symposium 2021
  - https://www.ieee-security.org/TC/SP2021/downloads/Oakland_PC_Report_2021.pdf