SCIS2018 MWS企画セッション

Innovative R&D by NTT

先進的研究における研究倫理
～我々の状況とこれから～

秋山 満昭（NTTセキュアプラットフォーム研究所）
吉岡 克成（横浜国立大学）

2018.1.25

モチベーション

- 世の中を変えるサイバーセキュリティ研究
  - ボットネットの観測/壊滅手法
    - Stone-Gross et al.（CCS'09）, P2PWNED（S&P'13）
  - SSL実装脆弱性発見手法
    - MalloDroid（CCS'12）
  - 高速ネットワークスキャン手法
    - ZMap（SEC'13）, Censys（CCS'15）

- 世の中を変える研究成果を日本から発信したい。そのような研究ができるコミュニティを作りたい。

- 無責任に攻撃手法・脆弱性を公開するのではなく、責任ある研究者/技術者として、どのように倫理的に取り組めばよいか？

これまでの取り組み

- **2016年5月** MWS意見交換会
  - 「Ethicsを議論しよう」: 議論の必要性を訴求
- **2017年1月** SCIS2017
  - 「企画セッション」: 世界（欧米）の状況，問題領域の構造、経験談を講演、パネルディスカッション
- **2017年6月** MWS意見交換会
  - 「Research Ethics」: BoF形式でアクションプランを参加者と議論
- **2017年11月** JSPS 第192委員会公開シンポジウム
  - 最新事例の共有、現状の課題、パネルディスカッション

これまでの取り組みから見えてきたこと

- 最先端のサイバーセキュリティ研究においては、研究倫理の考察と実践が十分にされている
  - CFP（USENIX Security, IEEE S&P等）
  - ガイドライン/ポリシーの準拠に加えて、事例に対応するための研究者自身の考察と実践
  - これができていない研究論文は難関会議では受理されない

- 日本において、サイバーセキュリティの研究倫理を十分に審査できる研究倫理委員会（IRB）はほとんど存在しない

- 研究倫理とは、研究者各自が持ち合わせておくべき素養
  - ICTの進展にともない、誰も踏み入れたことがない・前例が十分にない倫理的領域が出てくる
  - 自身の研究の可否をIRBに対して任せるだけではなく、自身が適切にリスクと利益のバランスを勘案すべき

倫理的研究を実践するために

- Step1: 原理原則から学ぶ
  - **Menlo report**: 生物医学にける研究倫理の原則をまとめたBelmont Report をベースとして、サイバーセキュリティに拡張した文書
- Step2: 先人の経験から学ぶ
  - 難関学術会議における研究倫理を考慮した研究
  - 研究倫理の問題に直面した研究者の経験
- Step3: 自身の研究を研究倫理の観点から実践して論じる
  - ステークホルダ（利害関係者）の明確化、インパクトの見積もり、リスクの最小化努力、Responsible disclosureの実施
  - 自身の研究を総合的に正当化できるか？

Menlo report

- サイバーセキュリティの研究倫理に関する白文書
  - 2012年に米国DHSが発行
  - 生命医学分野のBelmont reportが定める3原則をベースにICT研究に拡張
- 中核となる倫理原則
  - Respect for Persons（人格の尊重）
  - Beneficence（恩恵）
  - Justice（正義）
  - Respect for Law and Public Interest（法と公益の尊重）
    - 法令遵守、公共の利益を尊重
    - 説明責任(Responsible disclosure)と評価/実行手順の透明性

Responsible disclosure

- 攻撃手法/脆弱性/セキュリティホールに対する責任ある情報開示
- ステークホルダが誰なのか、彼らに対する影響を考慮し、最善と考えられる方法で情報開示すべき
- 情報開示の種類
  - No disclosure, Private disclosure, Coordinated (vulnerability) disclosure, Limited/partial disclosure, Full disclosure
- Coordinated disclosure
  - 詳細情報をベンダに通知して対策を促し、対策が完了した後に公表する
- 事例紹介
  - Yokoyama et al., RAID'16（横国大）
  - Korczynski et al., IMC'16（デルフト工科大）

課題(その1) 実践と知見共有

- ケーススタディの積み上げ
  - 世の中へのインパクト・利益はケースバイケース
  - 実践して知見を積み上げるしかない
- Responsible disclosureの実践
  - 脆弱性報告手順(情報セキュリティ早期警戒パートナーシップ(IPA, JPCERT/CC))
  - “脆弱性”ではないが Responsible disclosure が必要な場合もあり、研究者が主体で実施しなければならない
- 知見共有の場
  - 十分なノウハウ蓄積は単一の組織では困難
    - 歴史ある巨大な研究機関だけが可能
  - 組織横断的な議論が望ましい
    - 学会横断的に進めるための仕組み

課題(その2) 研究的意義

- 研究的意義とは何か？
  - 研究倫理の議論が必要な研究においては、攻撃手法や脆弱性を見つけたこと自体ではないはず
    - それだけではトップ学術会議には受理されない
    - 売名のための発表であってはならない
  - それを発見した工学的手法の研究的価値
    - 発見手法がわかれば広く世の中に恩恵がある
      (e.g., 開発者自身がチェックできる，開発段階で発見できる)
  - Common pitfallとその根本的な対処方法を明らかにすることの研究的価値
    - 問題/対策を一般化して世の中に広めることにより後世に恩恵がある

課題(その3) 産学連携

- 学術界と産業界の連携によってはじめて実質的な対策ができる
  - 産業界を巻き込んで議論が必須
    - Grace period や responsible disclosureは業界毎に異なる
  - 産学の信頼関係構築にむけた研究者の努力
    - Responsible disclosureの遵守
      - 十分な “情報” と “猶予期間”
      - ワークアラウンドの提示

まとめ

- 研究者個人として
  - 研究的意義を見出そう
  - 自身の研究を倫理の観点から実践し、説明しよう

- コミュニティとして
  - 議論・相談・知見が共有できる場を提供しよう