サイバーセキュリティ研究のグレーゾーン

横浜国大　吉岡克成

CSS2018　企画セッション
「サイバーセキュリティ研究のグレーゾーン」

2018.10.24

１．CSS2018研究倫理委員会の活動についてご紹介

２．私(吉岡)の所感と今後に向けた提言

３．法執行機関と上手に付き合って成果を出した研究例

謝辞：研究倫理委員会の説明資料はＮＴＴ秋山様がご作成されたものに一部追記を行いました。資料のご提供に感謝いたします。

背景

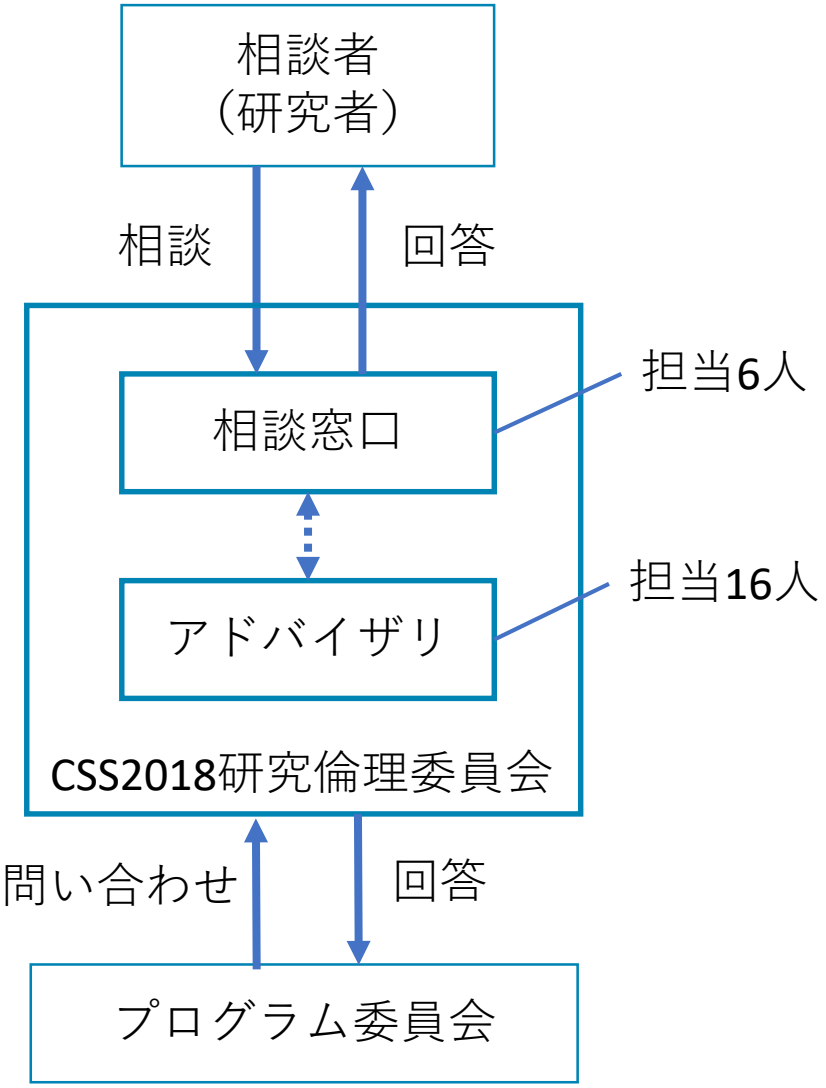
下記のような研究が発表される機会がＣＳＳでも増加(世界的なトレンド)

- 新たな攻撃手法、脆弱性の発表
- 実運用中のシステムに影響のある実験
- 被験者に危害が及ぶ可能性のある実験

疑問：
研究成果が悪用される恐れはないか？
実験が人・システムに危害を与えていないか？
この研究はやってよいのか？

CSS2018研究倫理委員会/相談窓口

- CSS2018に論文投稿を検討している研究者に対して、研究倫理に関する相談窓口を設置
- 相談者は相談フォームに基づいて問い合わせ、相談窓口担当が回答
  - 回答内容は過去の事例や世の中の状況を鑑みて”**アドバイス**”を行うものであり、”**お墨付き**”を与えるものではない
  - 相談内容は基本的には窓口担当に閉じるが、窓口担当で扱いきれない場合はアドバイザリにも共有し議論する
- プログラム委員会からの問い合わせにも回答する場合がある
- 例：論文の内容について研究倫理面で懸念点が生じた場合、必要な対応を議論



相談と回答

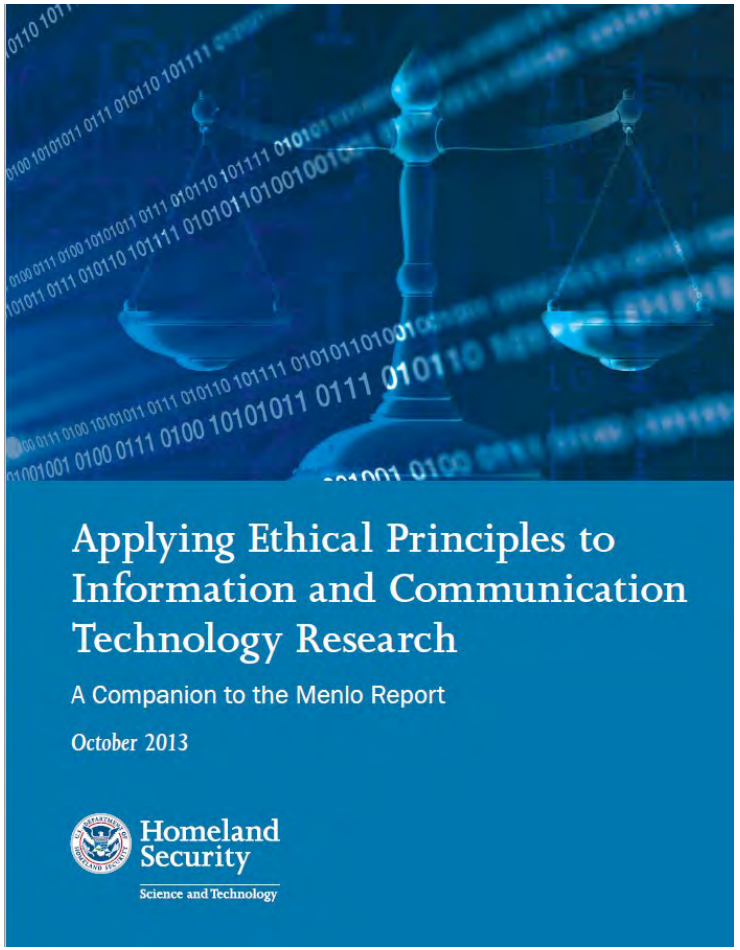
相談者の相談内容

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お知らせください
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をお知らせください
研究倫理対応案：※上記問題への対応案があればお知らせください

研究倫理相談窓口の回答

相談内容の整理 ：相談内容に基づいて、相談者が実施しようとしている研究行為、研究者が抱いている倫理的懸念、相談者の研究倫理対応案、を明確にする。
利害関係者の識別 ：だれが利害関係者（ステークホルダ）なのかを列挙する。
相談内容についての回答 ：相談者の対応に関する意見、過去の類似研究事例、推奨する対応、相談者が見逃している懸念事項、など。

研究倫理に関する(吉岡の)よりどころ



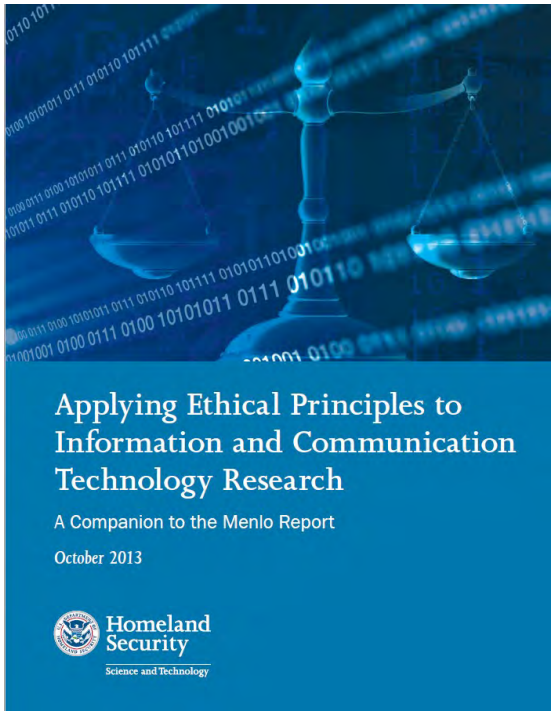
メンロレポート[1]とは

- 2012年8月に米国DHSが発行
- 正式名はThe Menlo Report –Ethical Principles Guiding Information and Communication Technology Researchであり、ICT研究における研究倫理の原則(Principles)を定めるものである†
- 生物医学と行動科学における3原則を定めたベルモントレポートの理念をベースに、さらに1原則を追加し、4原則を定めている
- 15名程度の産学官有識者によるWG構成と執筆

†一部報告書内の説明が不統一であり、Executive SummaryにはThis report proposes a framework for ethical guidelines for computer and information security researchと記載があるものの、他はICT研究に対する言及となっている．実態としてはセキュリティ関連研究が強く意識されている．

補足文書[2]

- Applying Ethical Principles to Information and Communication Technology Research –A Companion to the Menlo Reportというタイトルで2013年10月に米国DHSが発行
- 原則の記述しかないメンロレポートの、より具体的な解釈が記載
- メンロレポートが13ページに対して補足文書は32ページあり、実際の研究事例の説明もある
- メンロレポートの主旨を理解する上ではこちらの補足文書の方が役に立つ(メンロレポート本体のおさらいにもなる)



メンロレポートが定めるICT研究倫理4原則

- **人格の尊重(Respect for Persons)**
  - 研究対象の参加は本人の自由意志によって決まり、インフォームドコンセントによるべきである．本人が意思決定する権利を尊重すること．直接的な研究対象だけでなく、研究によって影響を受ける可能性があるが、自身の意思決定によりこれを決められない個人も保護の対象である
- **恩恵(Beneficence)**
  - 危害を加えないこと．研究により得られ得る恩恵を最大にし、与えうる危害を最小にすること．リスクと危害と恩恵のアセスメントを行うこと．
- **正義(Justice)**
  - 個人は自身の扱いについて平等に配慮を受けるべきであり、研究の恩恵は平等に分配されるべきである．研究対象の選択は公正に行われ、負担は研究対象に対して同等に分担されるべきである．
- **法と公益の尊重(Respect for Law and Public Interest)**
  - 法に従うこと．研究方法と結果の透明性を保つこと．

恩恵＞＞危害

であるべきという合理的な考え方

相談のハンドリングと回答

- CFP公開（６月下旬）から発表登録締切（８月上旬）までに**４件**の相談があった
- ハンドリング手順
  - 相談 → 担当者決定 → 議論推進/取りまとめ → 回答

案件①：データ符号化技術の仕様・実装に関連する脆弱性の開示に関する相談

相談 → 回答（**9営業日**）

案件②：広域スキャンにおける探索対象への影響等に関するご相談

相談 → 回答（**5営業日**）

案件③：質問紙調査における回答者への影響に関するご相談

相談 → 担当決定（**2営業日**） → 回答（**5営業日**）

案件④：広域スキャンにおける探索対象への影響等に関するご相談

相談 → 回答（**4営業日**）

→ およそ５営業日で対応できるようになった。

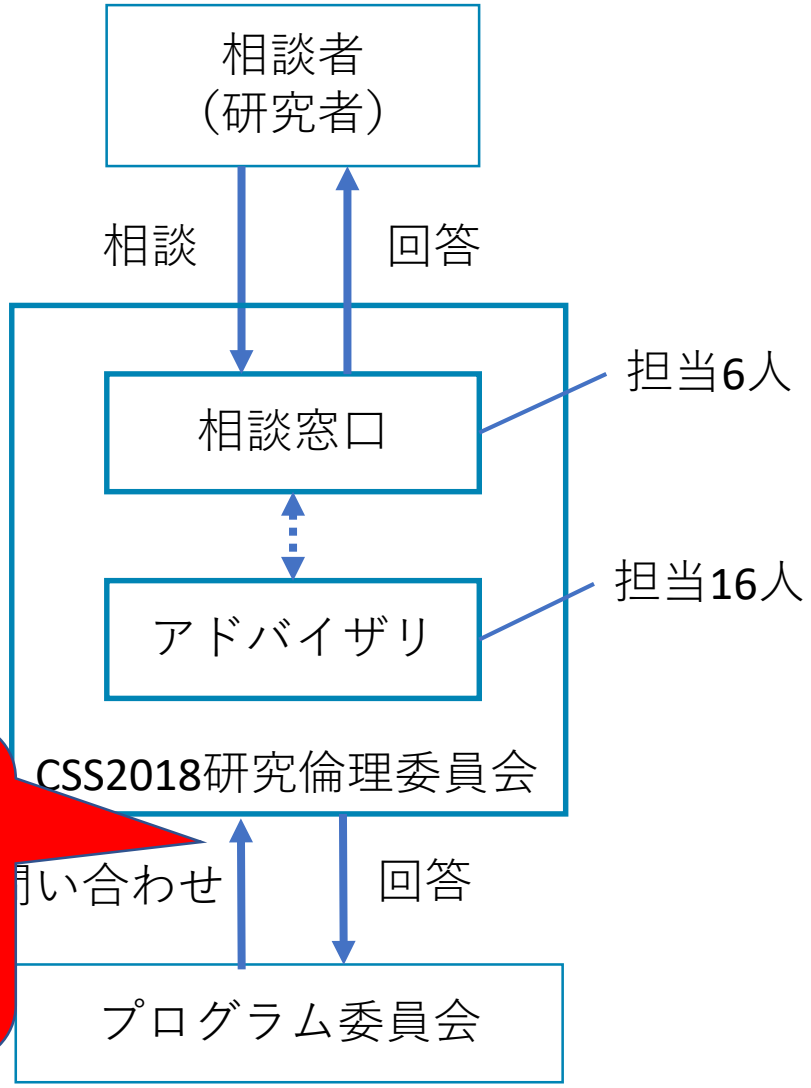
※ただし対応期間は重複していない

研究倫理について触れている論文数

※倫理教育や倫理そのものを議論しているものは除く

CSS2018研究倫理委員会/相談窓口

- CSS2018に論文投稿を検討している研究者に対して、研究倫理に関する相談窓口を設置
- 相談者は相談フォームに基づいて問い合わせ、相談窓口担当が回答
  - 回答内容は過去の事例や世の中の状況を鑑みて”**アドバイス**”を行うものであり、”**お墨付き**”を与えるものではない
  - 相談内容は基本的には窓口担当に閉じるが、窓口担当で扱いきれない場合はアド
- 例：論文の内容について研究倫理面で懸念点が生じた場合、必要な対応を議論



全部で４件。いずれも「脆弱性の開示方法」いわゆるResponsible Disclosureに関する指摘。

「投稿論文倫理チェック」課題と反省

- 事前周知が不十分
- 著者に修正の検討をお願いする際、
  修正期間が短い(論文集印刷期限のため)
- 論文修正要否の基準が不明確(それぞれ個別に要否を議論)

２つの対極的なケース

- 「**窓口相談**」は未来志向の建設的な活動
  - どうすればインパクトのある研究を適切に行えるか、という観点での議論

- 「**(投稿論文の)研究倫理チェック**」は、指摘する方もされる方もつらい作業.
  - しかし、研究コミュニティとして向き合わなければいけない問題でもある

これからに向けた提言

- 未来志向の議論は、今後も継続されることを期待
  - 事例を積み上げて研究倫理的センス・経験値を高める
  - 共通の問題意識をもつ有志での検討会
  - 本来の目的は世の中を良くすること。論文を通すための言い訳になっていないか。

- 投稿論文倫理チェックの負荷が減るような工夫が必要
→入口(投稿時、または、それ以前)で気づく仕組み
  - チェックリストによる自己判断
  - 特定イベント(CSS2018)での対応(今回)から
学会等での継続的な周知、啓蒙へ

法執行機関と上手に付き合って成果を出した例

DDoS-as-a-Service: Investigating Booter Websites

José Jair Cardoso de Santanna

In Chapter 4, entitled Distinguishing Booters Based on Their Attacks, we addressed RQ4. Based on the observation (from Chapter 1) that anyone

The main contributions of this these are that we show: (1) how to find booters, (2) how to detect their clients accessing and using them, (3) the characteristics of their attacks, (4) what third-party companies are used by them to maintain their operations, (5) which booters are the most dangerous and (6) which ethical arguments can be used to support mitigation actions against them. Finally, while the core of this thesis is based on scientific publications, a number of solutions proposed in this thesis are actively deployed by network operators worldwide. In addition to this, the methodologies in this thesis are used by the Dutch High Tech Crime Unit for collecting evidences for prosecution cases.

https://ris.utwente.nl/ws/portalfiles/portal/18494043/jjsantanna_thesis.pdf

In this appendix, we present the advise by the SURFnet responsible (Roland van Rijswijk) for interacting with a Dutch public prosecutor (Danielle Laheij) about the research performed in this thesis.

From: Roland.vanRijswijk@surfnet.nl
Subject: Citing contact with public prosecutor in paper
Date: 18 December 2014 at 17:16
To: Jair Santanna j.j.santanna@utwente.nl
Cc: Anna Sperotto a.sperotto@utwente.nl

この研究の手法が法的グレーゾーンと認識。

Hi Jair,

You can refer to our contact with the public prosecutor in any papers resulting from the research as follows:

"We are aware that research of this nature may touch on, or cross, legal boundaries, but we are convinced that the results from this research will benefit future mitigation methods and thus help combat Booters, both operationally as well as legally. In order to be transparent about our work, we have informed the office of the public prosecutor in the Netherlands about our intention to pursue this research."

This formulation is approved by them.

Cheers,

Roland

研究の透明性を保つため、 実験協力者から
オランダ検察へ研究の意図について説明を
行った旨が示されている