# セキュリティに関する研究活動を進める上での倫理的課題

2018年1月24日

齋藤孝道（明治大学）

# 自己紹介

- 明治大学理工学部情報科学科教授，博士（工学）
- 専門：Web セキュリティ，ブラウザブラウザーフィンガープリント技術やメモリ破壊攻撃対策など

  SCISデビューは，SCIS'99（1999年1月27,28,29日開催,神戸）
  タイトル：仕様記述言語を用いたセキュリティプロトコルの検証

- 「情報処理技術者・情報処理安全確保支援士」試験委員（2001年より現在まで）
- 著書：「マスタリング TCP/IP 情報セキュリティ編」（オーム社），「マスタリング TCP/IP SSL/TLS編」（オーム社），「プロフェッショナルSSL/TLS」（ラムダノート社）
- レンジフォース株式会社（2016年設立） 代表取締役
  （受託開発・ITコンサルティング・セキュリティ演習サービス販売，セミナー等）

# 情報セキュリティ研究室の紹介（2018）

- 明治大学理工学部情報科学科14研究室の一つ（2005年～）
- 教員（1名）
- M2（5名），M1（6名），B4（9名），B3（8名） 合計28名（女子2名）（博士課程募集中）
- 最近の就職先の例：NRI（セキュア），Nコム，Yahoo他

# （本学の）研究倫理を取り巻く概況

倫理＜**公金の適正利用**

- 2014年：「研究機関における公的研究費の管理・監査のガイドライン（実施基準）」の改正（文科省）
- 2015年：「CITI Japanの研究倫理教育プログラム」 **受講義務化**（本学）

**研究の不正**：「預け金」「カラ出張・給与・謝金」，**「データの捏造改竄」，「剽窃」**

**受講義務の根拠規定ありますか？**

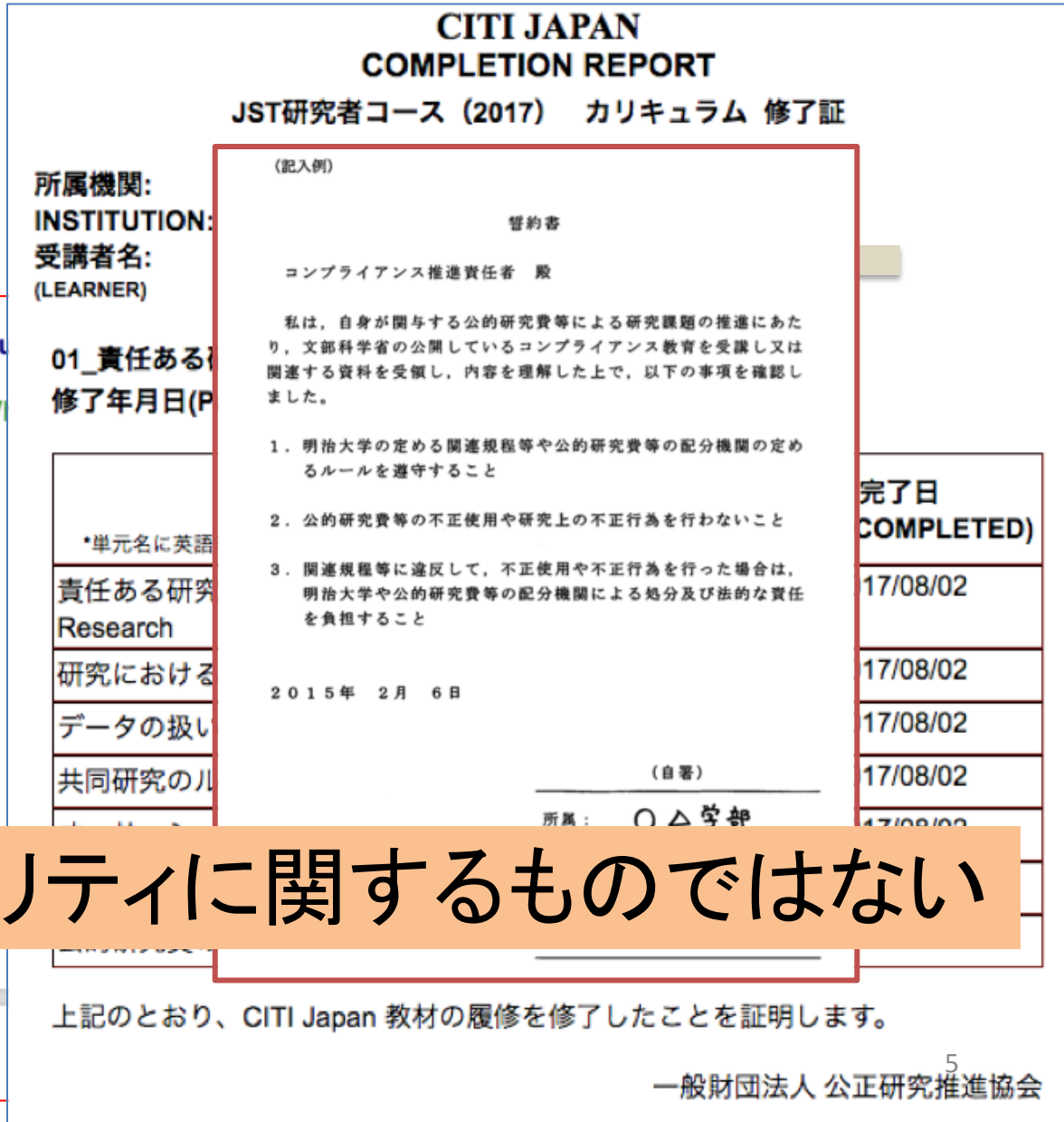
・明治大学倫理審査委員会運営内規
・明治大学倫理教育委員会に関する内規
・明治大学における研究費の適正管理に関する規程(改正後 2015 年 4 月より施行)
・研究活動の不正行為にかかわる通報処理に関する規程(改正後 2015 年 4 月より施行)
・研究活動の不正行為にかかわる通報処理に関する運用細則(2015 年 4 月より施行)

「明治大学における研究費の適正管理に関する規程」の
第15条のコンプライアンス教育・研究倫理教育等の実施に基づきます。

# CITIの研究倫理教育ジャパンプログラム

eラーニングによる
研究者行動規範教育
を提供するサービス

- 対象：教員・研究員等
- 受講間隔は5年に1度
- 誓約書の提出



CITI JAPAN
COMPLETION REPORT
JST研究者コース（2017）　カリキュラム 修了証

所属機関:
INSTITUTION:
受講者名:
(LEARNER)

01_責任ある
修了年月日(P

| *単元名に英語 | 完了日 (COMPLETED) |
|---|---|
| 責任ある研究 Research | 17/08/02 |
| 研究における | 17/08/02 |
| データの扱い | 17/08/02 |
| 共同研究の | 17/08/02 |

（記入例）

誓約書

コンプライアンス推進責任者　殿

私は，自身が関与する公的研究費等による研究課題の推進にあたり，文部科学省の公開しているコンプライアンス教育を受講し又は関連する資料を受領し，内容を理解した上で，以下の事項を確認しました。

1．明治大学の定める関連規程等や公的研究費等の配分機関の定めるルールを遵守すること

2．公的研究費等の不正使用や研究上の不正行為を行わないこと

3．関連規程等に違反して，不正使用や不正行為を行った場合は，明治大学や公的研究費等の配分機関による処分及び法的な責任を負担すること

２０１５年　２月　６日

（自署）

所属：　○△学部

上記のとおり、CITI Japan 教材の履修を修了したことを証明します。

一般財団法人 公正研究推進協会

**ただし，セキュリティに関するものではない**

# 参考：米国大学でのカリキュラム

ACM/IEEE コンピュータ・サイエンス標準カリキュラムCS2013
IAS/Foundational Concepts in Security

## IAS/Foundational Concepts in Security

*[1 Core-Tier1 hour]*

***Topics:***

- CIA (Confidentiality, Integrity, Availability)
- Concepts of risk, threats, vulnerabilities, and attack vectors (cros- reference SE/Software Project Management/Risk)
- Authentication and authorization, access control (mandatory vs. discretionary)
- Concept of trust and trustworthiness
- Ethics (responsible disclosure). (cross-reference SP/Professional Ethics/Accountability, responsibility and liability)

***Learning outcomes:***

1. Analyze the tradeoffs of balancing key security properties (Confidentiality, Integrity, and Availability). [Usage]
2. Describe the concepts of risk, threats, vulnerabilities and attack vectors (including the fact that there is no such thing as perfect security). [Familiarity]
3. Explain the concepts of authentication, authorization, access control. [Familiarity]
4. Explain the concept of trust and trustworthiness. [Familiarity]
5. Describe important ethical issues to consider in computer security, including ethical issues associated with fixing or not fixing vulnerabilities and disclosing or not disclosing vulnerabilities. [Familiarity]

# 研究活動における倫理的懸念

*某S研究室の事例を中心に*

# セキュリティ研究特有の懸念

## 研究活動フェーズごとの懸念

**教育**

- 「どこまで教えていいの？」
- 意図せぬ不法行為幇助

**実験**

- 「これってやっていい？」
- データ採取・解析・攻撃的な行為，他

**執筆・作成**

- 「どこまで書いていいの？」
- responsible disclosure（関係者へ告知）
- プロセス≒研究倫理委員会(IRB)？

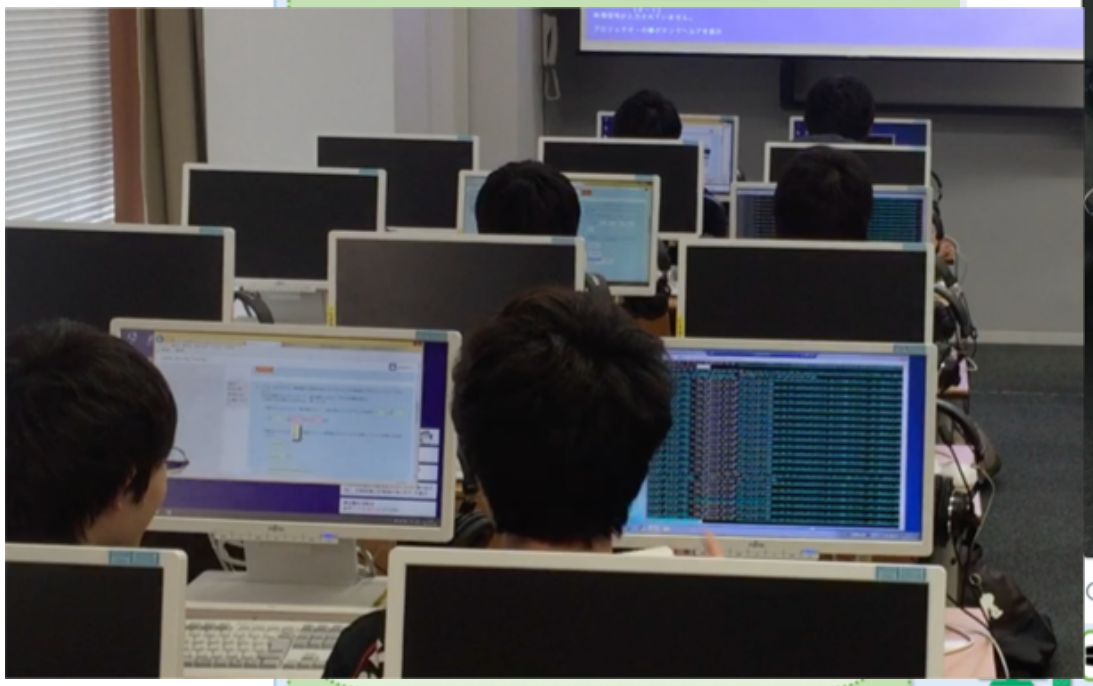
**投稿・公表**

- 「大丈夫かな？」
- 炎上リスク
- 刑事・民事訴訟リスク

# 教育時の懸念

## （学内）セキュリティ演習で・・・
大学の授業（演習科目），及び，付属中高の授業にて

こんなこと教えていいかな？
＞大学生，高校生，中学生ごとに



# 実験時の懸念

- データ採取にて

  専用サイトでフィンガープリントを採取している（クラウドソーシング）
  → もちろん，「説明＋合意」を取っている（はず）
  ＞＞それでもトラブルになることも・・・

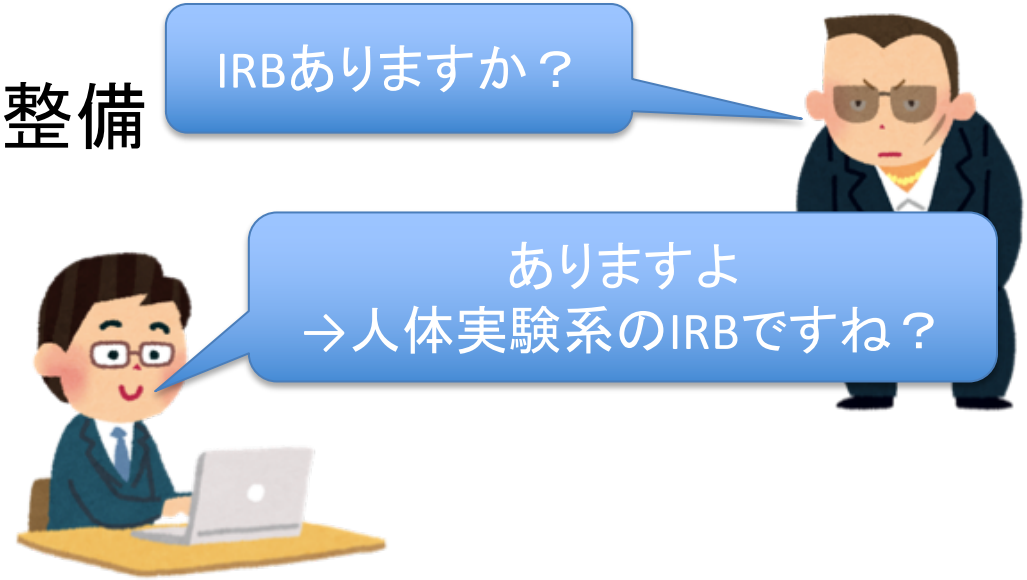

- 調査にて
  - 「リバースエンジニアリングしていいの？」
    海外だと「公益性が・・」とかあるようですが・・・
  - クローラーの運用
  - IDEを鳴らす 「某S研からまた攻撃が出てるけど（怒」

# 執筆・作成時の懸念

- 攻撃方法の解説を書いていいの？
  - XX Shock攻撃を使った攻撃の紹介
    ー＞論文に入れることを断念，プレゼンのみ
- 事実であれば，喋っていいの？
  - 「これは・・・まずいじゃないの？」（断定困難）
    ー＞ぼやかしつつ，社名などは書かない

# 投稿時の懸念

- 組織内プロセスの未整備
  - 規定・IRB未整備
  - 理解されていない




- 「responsible disclosureした？」
  - でも・・・「これ脆弱性？」
  - 採録決定後じゃダメ？
  - 欧米ではより進んでいる！？


投稿前に関係者に知らせたよね？

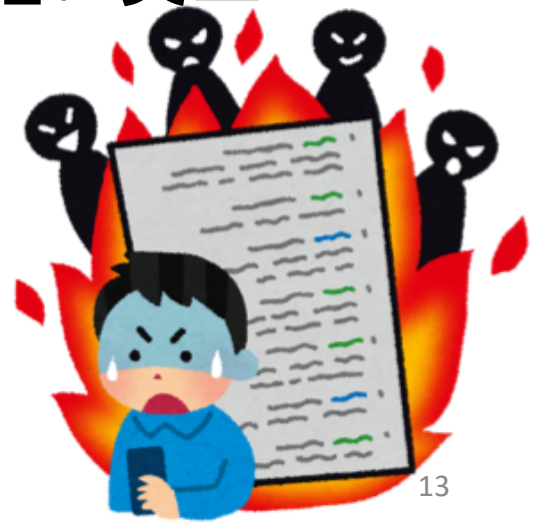
# 公開時の懸念

S研究室では教育・宣伝も兼ね，各種解説ページを作成

- バッファオーバーフローへの対策技術入門（2017/10）
- OAuthの仕組み丸分かり体験サイト（2017/2）
- Web Browser Fingerprint解説ページ（2014/10）
- Webアプリケーションの脆弱性の解説＆体験ページ（2014/6）

某CTCのF氏など「専門家」達に批判され軽い炎上

ー＞学生ショック



# ペナルティーについて

＜事例１＞

M大学：規定で複数のPCへの同時ログイン禁止

背景：インターネット接続は講習会を受けた人だけにしたい

実際：（様々な理由で）破る人がいます

（Question1）当該学生の処分は？

＜事例２＞

X大学：学生が攻撃ツールを作り公表

（Question2）当該学生の処分は？

# 合理的な判断

研究活動フェーズごとの懸念

教育
- 「どこまで教えていいの？
- 意図せぬ不法行為幇助

実験
- 「これってやっていい？」
- データ採取（「採取

執筆・作成
- 「どこまで書いて
- responsible disclosure（関係者へ[illegible]知）
- 研究倫理委員会(IRB)

投稿・公表
- 「大丈夫かな？」
- 炎上リスク
- 刑事・民事訴訟リ

リスク

エッジが効いた研究・教育

危ないから・面倒だから
やめよう・控えよう

# 悩み

- 表立って聞けない（だれに？どのように？）
- 場合・人によって言っていることが違う
- 今日話したことも・・・「不適切では？」とか

# ありがとうございました

## 免責事項

この資料では，情報・資料の内容には注意を払っておりますが，掲載された情報の内容の正確性については一切保証しません．また，この資料に掲載された情報・資料を利用，使用するなどの行為に関連して生じたあらゆる損害等についても，理由の如何に関わらず，サイトウは一切責任を負いません．

提供しているコンテンツ（文字、写真、画面、表、図版などのすべての提供形態が該当します）に関して，その一部またはすべてを著作権者の許可なく，私的目的以外での使用を禁止いたします．すべてのコンテンツの著作権はコンテンツの創作者（サイトウ）が所有しており，著作権者あるいは肖像権者の許諾を得ない「私的目的以外の複製」および「引用」の範囲を超えたコンテンツの複製，転載，改変，頒布などの行為は著作権法により罰せられます．

この発表の一部はフィクションであり，実在の人物及び団体とは 一切関係ありません．