サイバーセキュリティ　第192委員会
2017年度　公開シンポジウム

Innovative R&D by NTT

サイバーセキュリティ研究倫理の課題

NTTセキュアプラットフォーム研究所
秋山 満昭
2017.11.8

Sony vs. GeoHot

Sony Settles with GeoHot in PS3 Hacking Lawsuit

By Evan Narcisse | April 11, 2011

Share Tweet G+ Share ピン Read Later

The lawsuit that called down the wrath of Internet bogeymen Anonymous will go no further, as Sony Computer Entertainment America announced today that they'd reached a settlement with hacker George Hotz.

Email Print

+ Share

Follow @techland

(More on TIME.com: Playstation vs. Anonymous: Rogue Hacker Collective Targets Sony's Networks, Execs)

Hotz's hacking unlocked the PlayStation 3's super-secret root keys earlier this year, allowing users to install unauthorized software on the device. Sony maintained that Hotz's posting of the hack on his website violated federal law and opened the door to PS3 piracy. For his part, Hotz held that he didn't do anything wrong.

Sony issued a press release this morning, stating among other things that

http://techland.time.com/2011/04/11/sony-settles-with-geohot-in-ps3-hacking-lawsuit/

Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer [USENIX Security'13]

BBC News Sport More Search

NEWS

Home Video World Asia UK Business Tech Science More

Technology

Car key immobiliser hack revelations blocked by UK court

29 July 2013 | Technology Share

A High Court judge has blocked three security researchers from publishing details of how to crack a car immobilisation system.

Megamos Crypto transponders are built into car keys to disable the vehicles' engine immobilisers

German car maker Volkswagen and French defence group Thales obtained the interim ruling after arguing that the information could be used by criminals.

http://www.bbc.com/news/technology-23487928

ZMap: Fast Internet-Wide Scanning and its Security Applications [USENIX Security'13]

- インターネットを超高速にスキャンする技術
- 研究倫理に関する議論
  - インターネットに与える悪影響が少ないことを主張
  - 研究者に対してスキャンのガイドラインを提示
  - 著者が実際に経験した、ユーザからの応答(苦情)も共有

1. Coordinate closely with local network admins to reduce risks and handle inquiries.
2. Verify that scans will not overwhelm the local network or upstream provider.
3. Signal the benign nature of the scans in web pages and DNS entries of the source addresses.
4. Clearly explain the purpose and scope of the scans in all communications.
5. Provide a simple means of opting out, and honor requests promptly.
6. Conduct scans no larger or more frequent than is necessary for research objectives.
7. Spread scan traffic over time or source addresses when feasible.

スキャンのガイドライン

Responses from 145 users

Blacklisted 91 entities
(3.7 M total addresses)

15 hostile responses

2 cases of retaliatory traffic

Entity Type	Responses
Small Business	41
Home User	38
Corporation	17
Academic Institution	22
Government	15
ISP	2
Unknown	10
Total	**145**

ユーザからの応答

質問

- Q1: 世の中には、どのようなサイバーセキュリティに関する 研究倫理のコンセンサス があるのか？

- Q2: どのように 倫理的な研究 を実践すればよいか？

サイバーセキュリティの
先進的な研究 を 萎縮することなく 促進したい

サイバーセキュリティ研究倫理に関する議論・イベントの開催

- （2016/5）MWSプレミーティング「Ethicsを議論しよう」

- （2017/1）SCIS「MWS企画セッション: 研究活動とResponsible disclosure」

- （2017/5）MWSプレミーティング「BoF: 研究倫理」

- （2017/10）MWS「MWS企画セッション: 研究倫理/Responsible disclosure」

世の中の研究倫理に関する動向：生物医学からサイバーセキュリティへの発展

- 研究倫理のガイドライン/基本原則
  - Belmont Report (1978)：生命医療倫理を対象
  - Menlo Report (2012)：サイバーセキュリティに拡張
- 国際ワークショップ開催
  - CREDS (2013), CREDSII (2014), NS-Ethics (2015)
- 国際会議でのパネルディスカッション
  - 「Panel on Research Ethics」USENIX Security (2015)
- 国際会議CFPでの明記
  - 「Human Subjects and Ethical Considerations」USENIX Security (2013-)
  - 「Human Subjects and Ethical Considerations」IEEE S&P (2017)

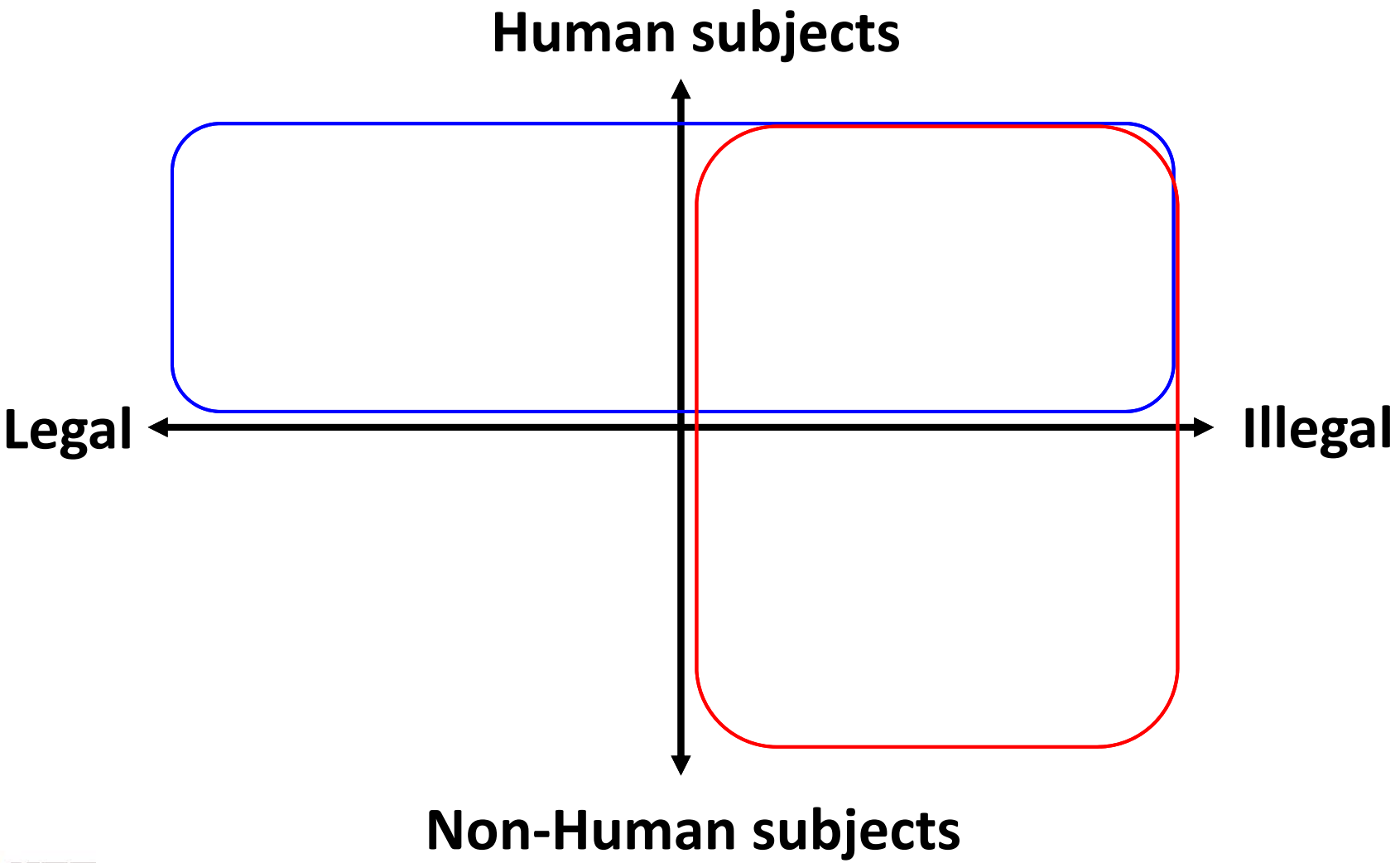
Belmont Report (1978)

- 生物医学/行動科学分野の研究倫理に関するガイドライン
  - 米国政府関連の委員会（National Commission for the Protection of Human Subjects）が策定
- 人間被験者（Human subjects）を用いた研究が主な対象
- 中核となる倫理3原則
  - Respect for Persons（人格の尊重）
    - 本人が自由に意思決定することを尊重
    - 実験参加の自由、適切なインフォームドコンセント
  - Beneficence（恩恵）
    - 患者/被験者や広く世の中に対して恩恵があること
  - Justice（正義）
    - 個人の平等な取り扱い（研究対象の公正な選択/平等な負担、研究の恩恵の平等な配分）

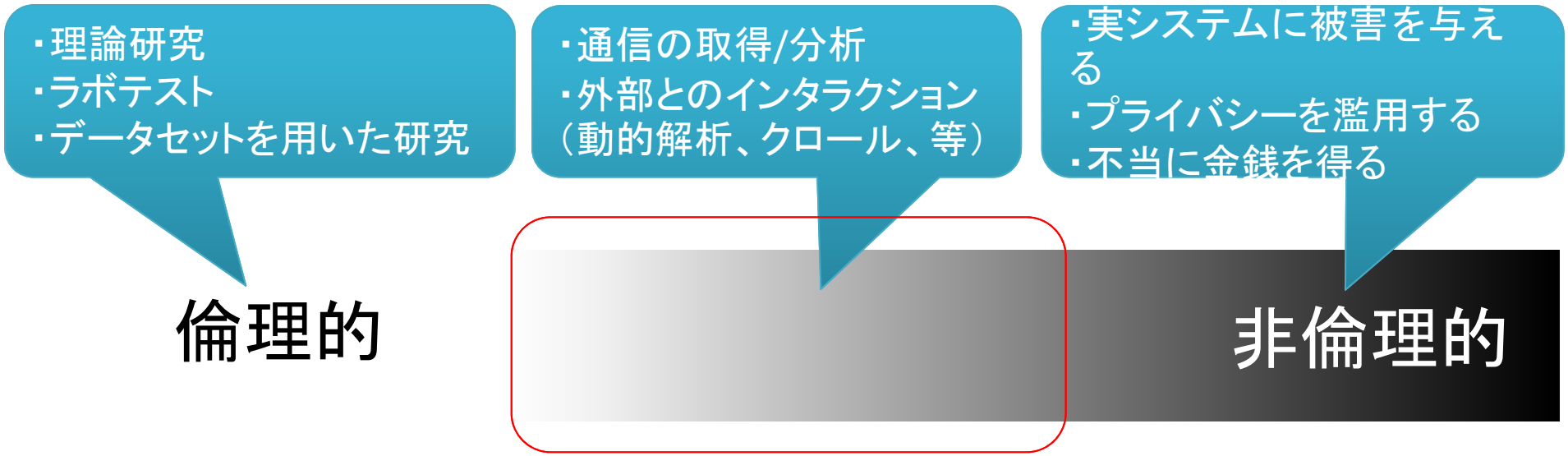
Menlo Report（2012）

- コンピュータ/情報のセキュリティにおける研究倫理のガイドライン/フレームワーク
  - アメリカ合衆国国土安全保障省（DHS）が公開
- 中核となる倫理原則
  - 【Belmont Reportから継承】
    Respect for Persons, Beneficence, and Justice
  - 【Menlo Reportで新たに追加】
    Respect for Law and Public Interest
    - 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

サイバーセキュリティの研究倫理が対象とする領域

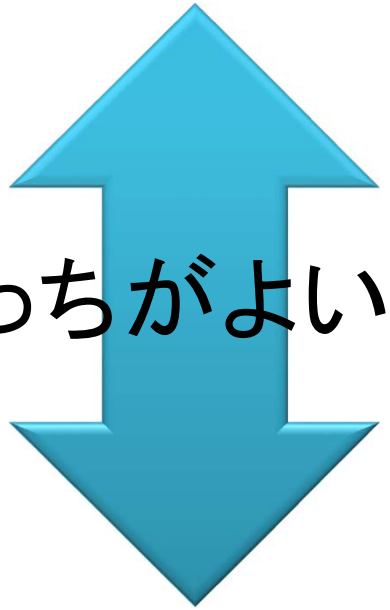


研究倫理の議論が必要な領域（その1）



研究倫理の議論が必要な領域（その2）
脆弱性を発見したら…

発見したら直ちに、あらゆる情報を、あらゆる人に公表する



どっちがよいか？

発見したとしても、一切の情報を、誰に対しても公表しない

Responsible disclosure

- 責任のある情報公開

- “誰に/何に” 対する “Responsible” なのか？
  - 発見者とベンダの対立構造
    - ベンダ「まだパッチができていないのに公表するのは responsible じゃない！」
    - 発見者「この脆弱性をすぐに修正しないのは responsible じゃない！」

    → 発見者/ベンダの双方が責任ある対応をすべき

われわれサイバーセキュリティ研究者は「発見者」として、responsibleな対応をしなければならない

Disclosureの種類
（状況によって複数の方法が実施される）

- No disclosure
  - NDA (Non-Disclosure Agreement, 守秘義務契約)が締結されている場合
- Private disclosure
  - ベンダが自身のプロダクトに脆弱性を発見した場合に、自身で対応し個別に顧客への通知などを行う場合
- Coordinated (vulnerability) 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
  - ステークホルダが複雑な場合（サプライチェーン等）に、仲介組織（IPA/JPCERT等）が介在することも
- Limited/partial disclosure
  - 一部の情報を公表する一方で、詳細情報をベンダに通知して対策を促す
- Full disclosure
  - 脆弱性の詳細情報やPoCをすべて公表する
  - ベンダーへの事前通知なし、もしくは通知をベンダーが無視する場合に行われることも

ステークホルダが誰なのか、彼らに対する影響を考慮して、最善と考えられる方法で実施すべき

Grace period

- Grace periodとは
  - 脆弱性をベンダーに通知してから、脆弱性の詳細が公表されるまでの猶予期間
  - ベンダーはこの間に脆弱性を修正しなければ、情報公開によって自身の製品・サービスに悪影響が出る可能性がある
- 業界によって異なる？
  - ソフトウェアとハードウェアで修正の容易さが違う
  - デファクトスタンダードは？

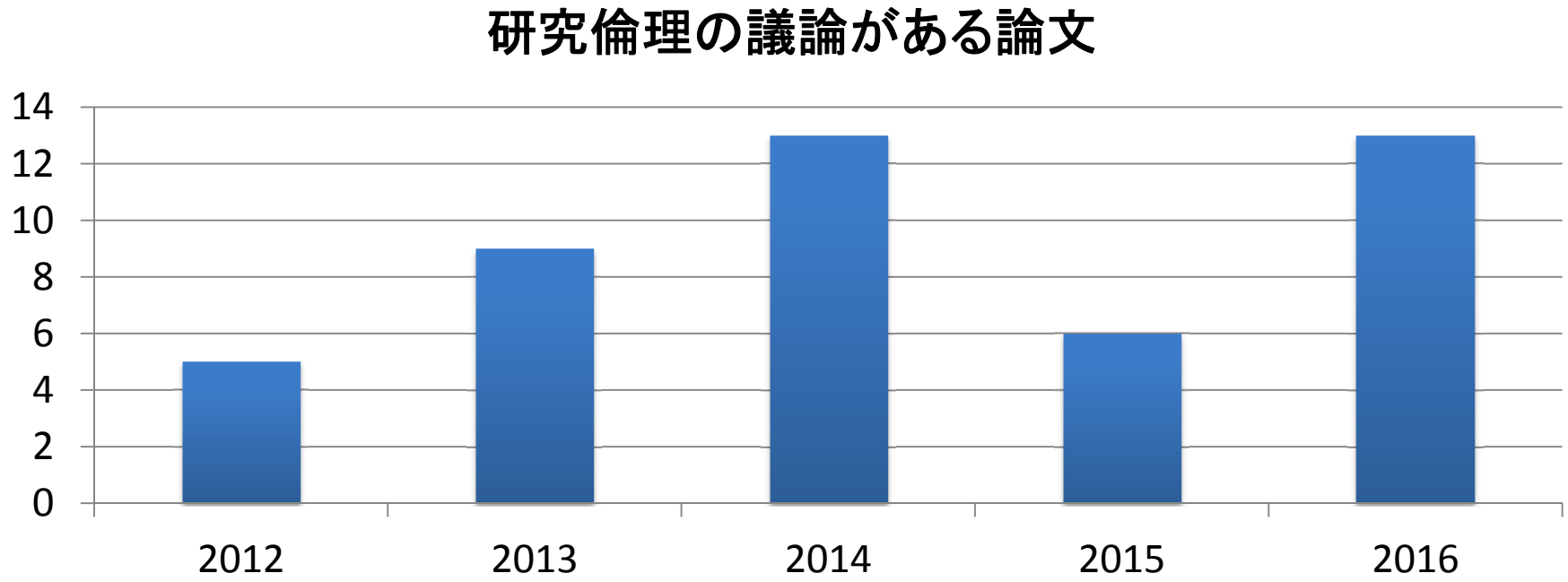
【参考】Google Project Zero

- Googleによる、未知の脆弱性発見と情報公開のプロジェクト
- Grace period (猶予期間)
  - ベンダーに脆弱性を報告した後、脆弱性のパッチがリリースされたら、もしくは90日経過したら、脆弱性情報を公開

研究倫理の言及がある論文数

USENIX Securityの過去5年間（2012-2016）で発表された論文 全293本を調査

→ **<u>計46本で研究倫理の議論があった</u>**



※ キーワード（ethics/ethical/IRB等）ベースで大まかに抽出したため正確な数字ではない可能性あり

議論の種別

- 同意/承認の獲得
  - ユーザ（被験者）の同意
  - サービス事業者の承認
  - 研究倫理委員会の承認
- 手順の正当性
  - Responsible disclosure
  - ポリシー/ガイドラインの準拠
  - 匿名化
  - 適法性
  - 代替手段なし
- リスク/被害のコントロール
  - 新たな被害は発生しない
  - リスクの最小化
- 利益
  - ベストプラクティスの共有
  - 公益性
- その他
  - Human subjectsではない
  - 研究用途

具体例: 同意/承認の獲得

- [サービス事業者の承認] We directly contacted Twitter to receive permission to conduct our study [1]
- [ユーザ(被験者)の同意] We obtained informed written or verbal consent from all participants, both to participate in the study as well as to have the interviews audio recorded. [2]
- [研究倫理委員会の承認] The studies have received an approval from our institutional ethics review board. [3]
- [(例外)] Our Universities do not have an IRB, but the study conformed to the strict data protection law of Germany and informed consent was gathered from all participants [4]
- [(例外)] We worked with the director of UC San Diego's Human Research Protections Program, who certified our study as exempt from IRB review. [5]

具体例: 手順の正当性

- [匿名化] We took careful protections to ensure that our live data collection did not breach users' anonymity. [6]
- [ポリシー・ガイドラインの準拠] All telemetry data is subject to strict privacy policies and participants can opt out by changing their settings [7]
- [ポリシー・ガイドラインの準拠] We followed the guidelines for ethical scanning behavior outlined by Durumeric et al. [8]
- [Responsible disclosure] We reported all the attacks discussed below to the software vendors affected in the last week of August 2013. [9]

具体例: リスク/被害のコントロール

- [リスクの最小化] Following the ethical hacking practice, we immediately removed the app from App Store [10]
- [新たな被害は発生しない] We use the passwords alone, excluding usernames and email addresses. [11]
- [新たな被害は発生しない] This data is already broadly available [12]

具体例: その他

- [研究用途] We followed the ethical practice and never utilized the leaked passwords for reasons other than understanding the overall statistical observation of passwords [13]
- [Human subjectではない] This work is not considered human subjects research [7]

具体例で引用した論文

- [1] Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse, USENIX Security 2013
- [2] Investigating the Computer Security Practices and Needs of Journalists, USNEIX Security 2015
- [3] Privacy in Epigenetics: Temporal Linkability of MicroRNA Expression Profiles, USNEIX Security 2016
- [4] An Empirical Study of Textual Key-Fingerprint Representations, USENIX Security 2016
- [5] Measuring the practical impact of DNSSEC Deployment, USNEIX Security 2013
- [6] Never Been KIST: Tor's Congestion Management Blossoms with Kernel-Informed Socket Transport, USENIX Security 2014
- [7] Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness, USENIX Security 2013
- [8] You've Got Vulnerability: Exploring Effective Vulnerability Notifications, USENIX Security 2016
- [9] The Emperor's New Password Manager: Security Analysis of Web-based Password Managers, USENIX Security 2014
- [10] Jekyll on iOS: When Benign Apps Become Evil, USENIX Security 2013
- [11] How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation, USENIX Security 2012
- [12] PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs, USENIX Security 2012
- [13] A Large-Scale Empirical Analysis of Chinese Web Passwords, USENIX Security 2014

倫理的研究の実践
自チームのCSS2017発表論文（その1）

2D1-4: オンラインオークションにおける プライバシーリスクとユーザ認識の調査

5.3 研究倫理

本研究は Menlo Report に記載されている研究倫理の原則に基づいて，実験の設計・実施と実験データの管理を行った [7]．オンラインオークションを対象にするにあたり，実際のサービス上での実験を実施した．その際に，ユーザが攻撃に巻き込まれることによる被害が新たに発生しないように配慮した．実験では，特定のアカウントに対する購入商品の列挙はしておらず，また特定のアカウントと他のサービスのアカウントを紐付けることもしていない．またユーザスタディのアンケートにおいては，個人情報の収集は実施しておらず，回答項目の統計情報のみを利用した．

- 手順の正当性
- リスク/被害のコントロール

＋ 実際のサービス事業者に事前に論文内容を確認してもらいアドバイスをいただいた

倫理的研究の実践
自チームのCSS2017発表論文（その2）

2C4-4: ユーザブロック機能の光と陰: ソーシャルアカウントを特定するサイドチャネルの構成

6.3　研究倫理

本研究では，攻撃の実現性と影響力を評価するため，実サービスを用いた実験を行った．実験は限られた量のトラフィックしか生成しないよう注意深くデザインされ，サービスの運営に悪影響を与えることはなかった．またユーザ特定は我々が保有するアカウントに対してのみ行われ，他のユーザは攻撃に一切関与していない．本研究で提唱された攻撃はサービスの脆弱性に起因するものではないが，実サービスに与えるインパクトを鑑みて，手法の詳細や実験結果を事業者に報告する準備を進めている．

- 手順の正当性
- リスク/被害のコントロール

各組織の倫理規定

- ACM: Code of Ethics and Professional Conduct (1992)
  - http://ethics.acm.org/code-of-ethics
- 情報処理学会: 倫理綱領 (1996)
  - http://www.ipsj.or.jp/ipsjcode.html
- 電子情報通信学会: 行動指針 (2011)
  - http://www.ieice.org/jpn/about/code2.html
- IEEE: IEEE Policies *7.8 Code of Ethics*
  - https://www.ieee.org/about/corporate/governance/p7-8.html
- Honeynet Project: Code of Conduct (2012)
  - https://www.honeynet.org/codeofconduct

課題（その1）

- ケーススタディの積み上げと知見共有のために
  - ガイドライン/コンセンサスの理解
    - Menlo report，各種倫理規定，先行研究の方法/作法
  - 上記に従った研究の実践
    - 自身の研究に当てはめて実践し、倫理的だと説明できるか？
  - Responsible disclosureの実践
    - 脆弱性の報告手順は確立されている（IPA, JPCERT/CC）
    - “脆弱性”とまではいえないような微妙なラインは？
  - チェックリスト/ツール
    - 研究を始める段階で有益
    - 例：CREDS toolをより詳細にしたものなど
  - 知見共有の場

課題（その2）

- 学術界/研究者が“何を/どこまでやりたい”かを主張できていない、そのような議論を行う場がない
  - 現状の法解釈で単純に線引きをするのではなく、技術発展/社会貢献を目的として、学術界/研究者がやりたいことを主張し、世論を説得することが重要
  - 例：「脆弱性研究において、市中製品を解析したいが、利用規約によって解析が禁止されている」

課題（その3）

- 学術界と産業界がWin&Winになるには？
  - 「見えない」から「安全」では、攻撃者に対抗できない
  - ハッカーカンファレンスでは、自身の雇用機会創出のため、responsible disclosureを無視した発表も
    - （研究者も生活が掛かっている、成果を発表したい）
  - 研究者 と 産業界 の信頼関係を構築するには？
    - ベンダーに十分な “情報” と “猶予期間” が与えられているか？
    - 研究者がワークアラウンドを提示しているか？
    - バグバウンティプログラムはうまくいっている一例

課題（その４）

- 組織横断的に議論を進めていくために
  - 十分なノウハウ蓄積は、単一の組織では難しい
    - 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には？
      - CSEC, ICSS, SPT, MWS, SCIS, …
      - 第192委員会
    - 産業界を巻き込んで議論するには？
      - grace period や responsible disclosureの考え方は業界によってまちまち…

課題（その5）

- 学生が研究を始める際に知っておくべき研究倫理とは？
  - 「ウェブに情報が書いてあるけど、やったらダメなの？」
  - 「サイバー特有の“やってはいけないこと”って？」
    - 例：「”内部情報.xslx” がメール添付で送られてきたので、VTに投稿してチェックしました！」
    - 例：「世の中に脆弱性なサイトがどの程度存在するか調査するために、AlexaTop1000のサイトにMetasploitを打ち込んでみました！」

- 学生にサイバーセキュリティ研究倫理をどのように教えればいいか？
  - 大学のカリキュラムは、生命医学倫理や一般的な研究倫理（研究不正など）がメイン
  - 学生向けの適切な書籍/ドキュメントはあるか？

続きはパネルディスカッションで

SCIS2018

>ENGLISH

2018年暗号と情報セキュリティシンポジウム

2018 Symposium on Cryptography and Information Security

1月23日（火）～26日（金）
朱鷺メッセ（新潟）

MWS企画セッション、来年もやります