MWS企画セッション①
研究倫理取り組み事例紹介
（USENIX Security等の最新研究事例より）

秋山満昭 NTTセキュアプラットフォーム研究所
畑田充弘 NTT/MWS組織委員会

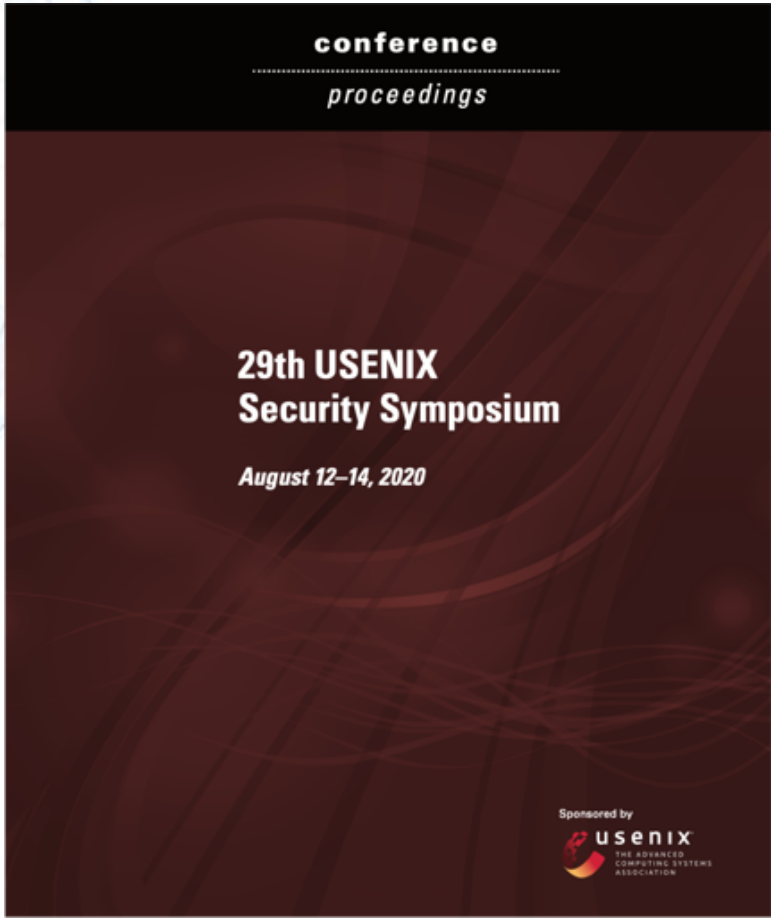
背景・モチベーション

- サイバーセキュリティ研究において研究対象/行為が多様化
- 法制度や社会的コンセンサスは時代とともに変化する
- どのような倫理的配慮をどこまでやればいいか

- 倫理的な研究を実践するために（※SCIS2018 MWS企画セッションより）
  - Step1: 原理原則から学ぶ
  - Step2: 先人の経験から学ぶ
  - Step3: 実践して論じる

本発表の着目点

※ http://www.iwsec.org/mws/2017/20180125/3F2-2.pdf



157論文

https://www.usenix.org/conference/usenixsecurity20/technical-sessions

分析手順

抽出 → 分類 → 傾向分析

分析手順

type of devices, and show some examples in Table 1. For each device, the protocols are ranked by the frequency of captured packets. We can observe that each device family may have its distinct frequency pattern of protocols. Different products from the same manufacturer may show the same/similar pattern of protocols, e.g., several DLink devices demonstrate identical patterns of protocols. Most likely, such devices share the same hardware and software in their WiFi component.

The initial analysis suggests the possibility of using features extracted from BC/MC packets to identify the make, type, and model of the devices. The complexity of the patterns also implies that it could be very challenging for adversaries to perfectly spoof the network features of other devices.

3.2 Ethical Considerations

We collected data through a completely passive approach. We did not turn on promiscuous mode. That means, we were

*According to OS market share by country reported by https://gs.statcounter.com/os-market-share/

キーワード検索：ethics, ethical, disclosure, IRB, legal, vendor, feedback, CVE

抽出 → 分類 → 傾向分析

分析手順

the scope of all of our datasets in Table 1. Note that this data was collected ethically and in compliance with user privacy laws within the originally-intended context (see Section 8.4).

ourselves to a very small-scale experiment: we opted to select and analyze only one representative app, *Hunter Assassin* [44],

While we are not directly interacting with users, our study is an empirical investigation of an *in situ* system at Facebook that is. Thus, although IRB approval is not applicable to this

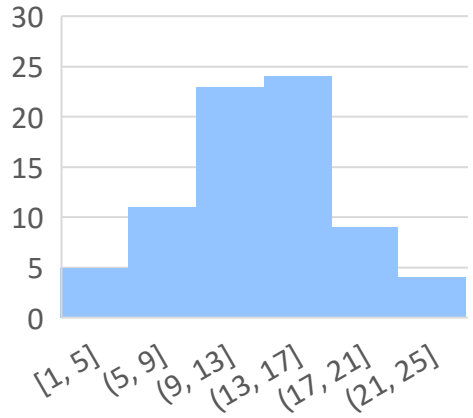
media data has potential for abuse, we implemented many measures to protect our participants' privacy. We did not col-

When initially finding *CVE-2019-11516*, it was exploitable on any *Broadcom* chip we tested. Surprisingly, during responsible disclosure, *Broadcom* stated that they knew about the

to Bluetooth Special Interest Group (SIG), Google Android Security Team, Apple, Windows, and Texas Instruments

抽出 → 分類 → 傾向分析

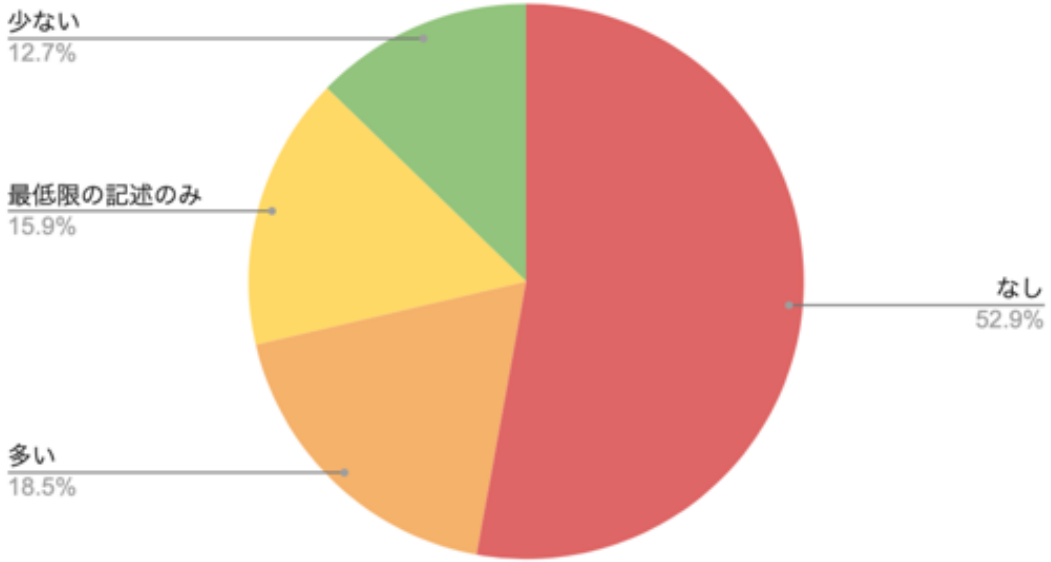
分析手順



抽出 → 分類 → 傾向分析

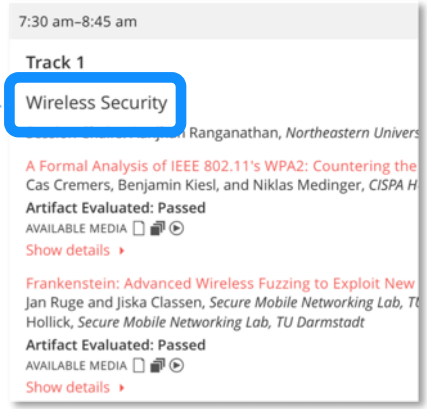
研究倫理の記述の有無・分量

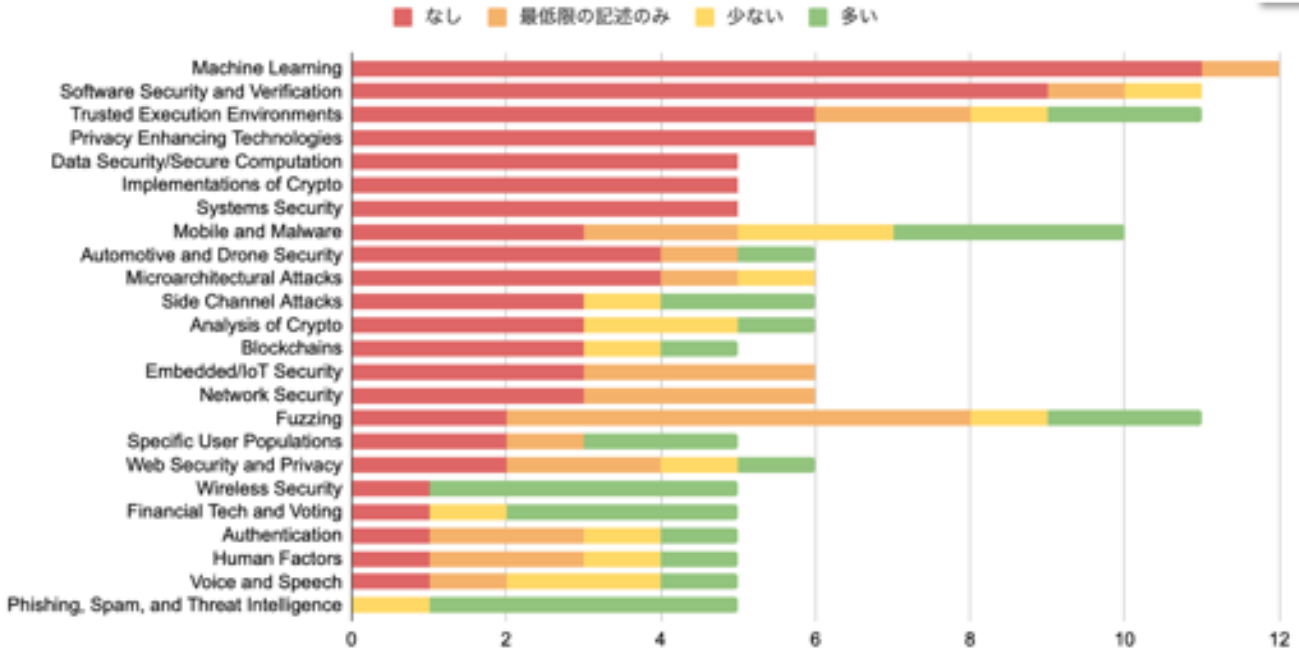
- 記述あり：**47.1% (74/157)**
  - 参考：コンピュータセキュリティシンポジウム2020の記述あり **10.7% (19/177)**
- 記述の量
  - “多い” > “少ない” > “最低限の記述のみ”



研究分野と記述有無・分量

- 「セッション名」毎に集計
  - 同一分野で複数セッションあるものはマージ
    （例 “Machine Learning 1” と “Machine learning 2”）





- 傾向
  - 理論系論文は記述が無い・少ない
  - 実際のシステム・サービス・人間を対象にした論文は記述が多い

サイバーセキュリティ研究倫理に関する６種類（＋１）の分類軸

- 手続き
  - **Consent and approval**：事前にやること(事前同意/承認)
  - **Responsible disclosure**：事後にやること(関係各所への通知)
  - **Ground for the exception**：例外として扱う根拠：
- 対応手段
  - **Protect user‘s privacy**：プライバシー保護：
  - **Respect for law/policy/guideline/contract**：法令等遵守
  - **Balance risks and benefits**：リスクと利益のバランス
- その他
  - **Other**：上記に定義されない倫理的配慮：

分類手順

- 手順1: コードブックを分析者二名の合議で作成
  - コードブック：分類（前ページに記載）についての意味と具体例

- 手順2: コードブックに従って二名の分析者が独立して分類
  - 論文に対して各分類の
    フラグを付与することで分類

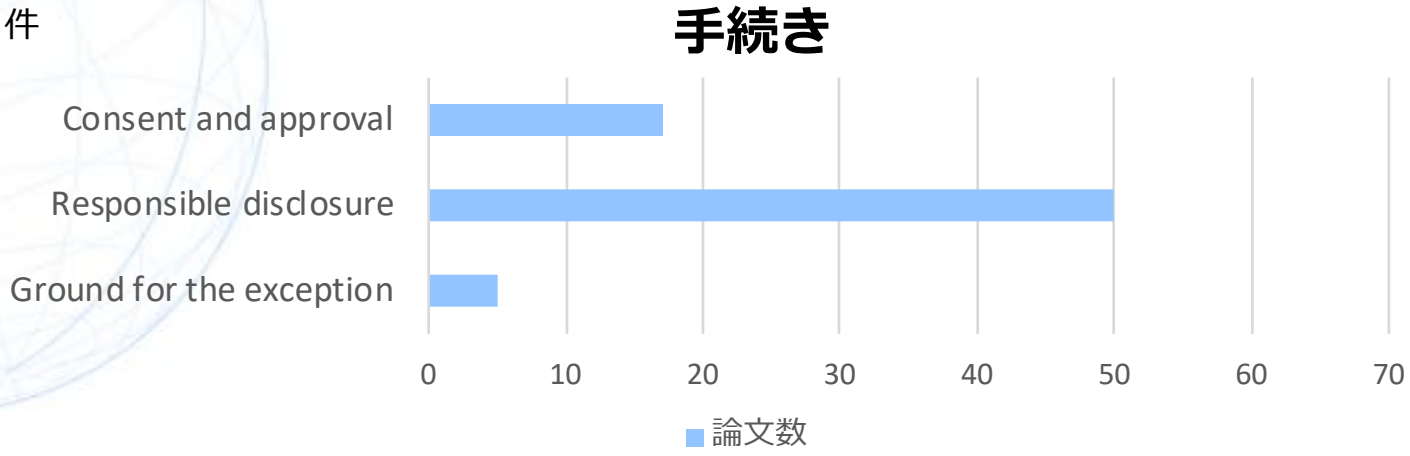
論文	分類1	分類2	分類3
#1	no	yes	no
	no	yes	no
#2	yes	no	no
	yes	no	no

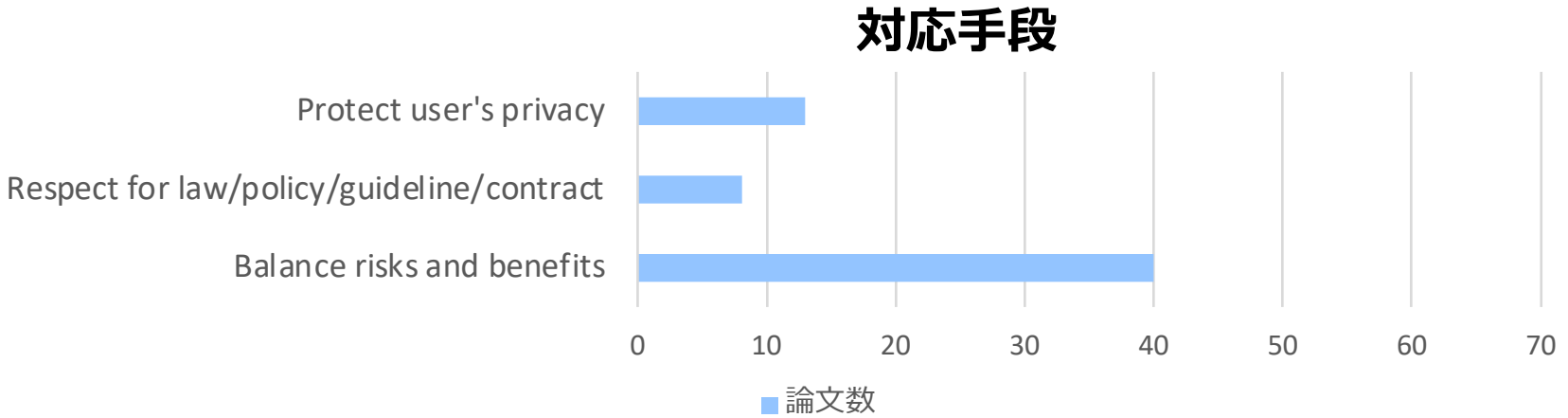
分析者A
分析者B

- 手順3: 一致率の検証
  - Cohen’s kappa係数は 0.75 以上で信頼性あり（未満の場合、手順1に戻る）
  - **今回は Cohen’s kappa係数 が 0.803 だったため1発OK**

分類結果

※Otherは１件





手続き：Consent and approval

- 実験参加者の承諾
  - 実験前に同意書（consent form）を参加者から受領

    All respondents explicitly gave their consent …

- IRBの承認
  - IRBの審査を受けて承認取得

    This study was approved by our institutions' IRB.

  - IRBから審査免除された（Human factorでないため）

    The IRB Exempt certificates were obtained from our institutes.

人間を対象にしない研究ではこれらの言及がないものが多い

手続き：Responsible disclosure

- 発見した脅威/脆弱性をステークホルダに通知
  - 通知した事実

    We have disclosed the details of this attack to [vendor], who has acknowledged its validity.

  - 取得した脆弱性ID

    [vendor] has also assigned [CVE-ID] to [product name]

  - 対応状況

    We worked with the [software] authors to patch these bugs.

脆弱性を対象にする研究では必須

Ground for the exception

- （省略）

対応手段：Protect user’s privacy

- PII（Personally-identifiable Information）の匿名化

> we have scrubbed information that might trace back to the people behind the pseudonyms

- PIIを収集しない

> … using IP country geolocation instead of the full IP address

> all traces are collected from an automated browser and none of them are from real users

人間を対象にした研究、通信を観測する研究ではほぼ必須

対応手段：Respect for law/policy/guideline/contract

- 法律への準拠
  - GDPR

> As some of our participants were from the UK and [service] is located in the UK, we complied with GDPR.

  - 米国連邦法

> Federal law also mandates […] Throughout our study, all the calls that we recorded were made to the inbound lines we owned.

- 弁護士の見解

> we consulted with our lawyers and they confirmed that what we did was legal, and we believe that it is ethical.

サイバー犯罪系の研究で言及が多い

対応手段：Balance risks and benefits

- リスクの低減・最小化
  - 実験参加者、実験対象サーバ/サービスへの配慮
- ワークアラウンドの提示
  - 攻撃手法の論文だが、対策手法まで実装して事業者に提示
- Responsible disclosureのプロセス詳細
  - 各ベンダの対応手順や状況の詳細をGithubで説明
  - Disclosureを実施する際の課題をまとめている
  - Ethereumの脆弱なSmart Contractの作者を探す方法の説明

実際の人間・システム・サービスを対象とした研究全般で言及される

分かったこと

- USENIX Security 2020では研究倫理の言及をしている論文が約半数
  - 文献[A]より、USENIX Security 2012-2016ではわずか 15.6% (46/293) だった
    [A] 秋山,研究倫理に関して我々の置かれている状況, SCIS2017 MWS企画セッション (MWSCIS), http://www.iwsec.org/mws/2016/pdf/4E2-2.pdf
  - サイバーセキュリティ研究における倫理的配慮の重要性は確実に高まっている

- 研究倫理に関する記述の粒度・観点・分量が統一されていない
  - 研究分野による差異
    - 理論系研究は必須ではない
    - 実社会に直ちに影響を及ぼす研究（サイバー犯罪/実サービスへの攻撃)では綿密な議論がされる
  - 研究者/研究グループの特性もあるかも

- 「先人の経験から学ぶ」ことは重要
  - しかし、現状は情報が構造化されていないため、簡単に検索したり活用することが難しい…

研究コミュニティでの“知見の活用”に向けて

- 研究倫理決定木（Ethical decision tree）
  - セコム様が開発したサイバーセキュリティ研究倫理判断のサポートツール
  - 過去の論文における倫理的判断をDB化してUIでインタラクティブに検索可能
    - 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

- 最新情報を反映して研究コミュニティで活用できないか？

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.