トップ会議/論文誌の採択者に聞く、ユーザブルセキュリティ研究の面白さと心得

開発者向けユーザブルセキュリティ研究編

ユーザブルセキュリティワークショップ（UWS 2023）
2023年10月30日
NTTコミュニケーションズ株式会社
金井文宏

自己紹介：金井 文宏（Fumihiro Kanei）

- 経歴/所属
  - 2015年　日本電信電話株式会社 入社
    セキュアプラットフォーム研究所
    社会情報研究所
  - 2023年7月 NTTコミュニケーションズ
    イノベーションセンター 所属
- 研究分野
  - ユーザブルセキュリティ
    - 開発者向けユーザブルセキュリティ分野
      CSS2020 最優秀論文賞, ACSAC'21, CHI'23 採択
  - モバイルセキュリティ
    - Androidアプリ/マルウェアの解析
  - Webセキュリティ
    - 広告不正検知

開発者向けユーザブルセキュリティ研究とは？

- ユーザブルセキュリティ研究：
  - **人間的側面**からセキュリティ技術を検討する研究分野
  - ユーザ属性とコンテキストの組み合わせによる様々な検討領域が存在

非専門家（Non-expert）
エンドユーザ など

専門家（Expert）
ソフトウェア開発者
システム管理者
SOCアナリスト
CISO など

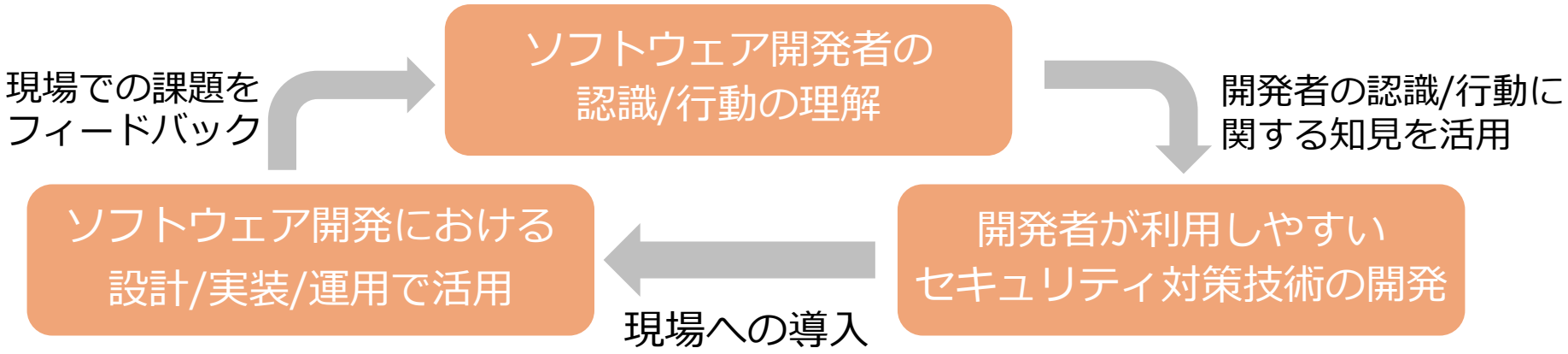
開発者向けユーザブルセキュリティ研究

ユーザブルセキュリティ研究のうち、
対象とするユーザ属性として**開発者**
に着目した研究領域

なぜ「開発者」に着目する必要があるか？

- システムの設計・実装段階でセキュリティ対策を講じる事で脆弱性の被害を未然に防ぎたい
- 性能的に優れたセキュリティ技術でも現場の開発者視点で効果や利便性が高くないと活用は困難
  - 例：とても高精度な脆弱性検査ツールらしいけど、ウチの環境だと導入しづらい…
    どれくらい効果があるか分からないから導入判断が難しい…

- **ソフトウェア開発者の認識/行動を分析し理解**することで、
  現場の開発者にとって利用しやすいセキュリティ対策の開発に活用したい



CHI'23 研究紹介：
セキュア開発ガイドラインに関する調査（CHI'23）

- **論文情報**
  - タイトル：Analyzing the Use of Public and In-house Secure Development Guidelines in US and Japanese Industries
  - 著者：金井文宏[*1]、長谷川彩子[*2]、塩治榮太朗[*3]、秋山満昭[*3]
    - *1 NTTコミュニケーションズ（発表時はNTT社会情報研究所），*2 情報通信研究機構, *3 NTT社会情報研究所

- **会議情報**
  - ACM CHI Conference on Human Factors in Computing Systems (CHI 2023)
  - ヒューマンコンピュータインタラクション（HCI）分野の最難関国際会議

CHI'23 研究紹介：
セキュア開発ガイドラインに関する調査（CHI'23）

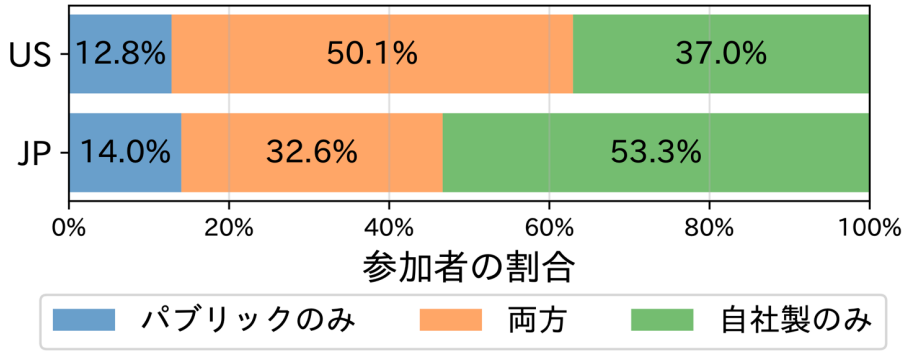
- **研究背景**
  - セキュア開発ガイドライン：安全なソフトウェアを実装するための方法/方針が体系的に記されたドキュメント
  - セキュア開発ガイドラインに関する**学術研究と産業界のギャップ**
    - 自社製ガイドラインの利用実態、既存研究が提案する推奨事項の実践可能性、国ごとの開発者の認識の差異 など

- **アプローチ**
  - セキュア開発ガイドラインに対する認識/実態を日米産業界の開発者へのユーザ調査にて調査
    - パブリック/自社製どちらのガイドラインが利用されているか？ユーザビリティは？利用・運用しやすいか？

- **結果**
  - 学術界では注目されてこなかった**自社製のガイドライン**が産業界では広く利用されている
  - **開発現場における組織的な制約**(e.g., 受託開発、小規模開発 など)を考慮した提案が必要

CHI'23 研究紹介：
調査結果・提言

- **自社製ガイドラインの利用実態**
  - 産業界では自社製のガイドラインの方が広く利用されている
    ⇛ 既存研究が着目していない**自社製ガイドラインに対する理解/実態解明の重要性**を定量的に明らかにした



参加者が利用しているガイドラインの種別の割合
（アメリカ：N=359, 日本：N=285）

- **より実践しやすいガイドラインの運用法の必要性**
  - 特定の属性を持つ開発現場では既存研究が推奨するガイドラインの運用方法が実践しにくい
    - 例：受託開発、小規模開発 など

研究者

- ガイドラインの責任者を定めるべき！
- ガイドラインに準拠して開発されたか検査すべき！

- 小規模なプロジェクトなので人員が足りない…
- 委託元からの指示が無いと勝手に実施できない…

開発者

- 小規模開発
- 受託開発 など

CHI'23 研究における苦労・工夫点

- **アンケート設計における工夫**
  - パイロットインタビュー / パイロット調査に基づいたアンケートの質の向上
    - JPCERT/CC, Software-ISAC等、産業界コミュニティと連携し 10社（19名）へ事前のインタビューを実施
  - バイアス軽減に向けた質問設計
    - 例：全ての設問を匿名回答/任意回答とすることで **社会的望ましさバイアス**※を軽減
      ※ 参加者が自身の立場/所属によって社会的に好ましいであろう回答をしてしまうバイアス

- **調査対象となる開発者募集の難しさ**
  - 一般的なエンドユーザ向け調査と異なり、開発者（＝特定の属性をもつ人）の調査は参加者募集が難しい
  - ウェブ調査会社に依頼して海外の提携調査会社と連携し日米の開発者を募集（そこそこの費用）
  - ウェブ調査会社 or クラウドソーシング のどちらが良いかは要議論
    - 再現性の観点からクラウドソーシングサービスのほうが査読者の印象は良い・・・？

CHI'23 採択までの流れ

2021.12～ パイロットインタビュー &パイロット調査実施

2022.4 アンケート調査実施

2022.6 USENIX Security '23 投稿

2022.8 USENIX Security '23 Rebuttal → 不採択
- 2: Accept on Shepherd Approval x1
- 3: Accept Conditional on Major Revision x1
- 4: Reject x3

2022.9 CHI '23 投稿

2022.11～12 CHI '23 Resubmission 期間
- 2: Accept with Minor Revisions or Revise and Resubmit x2
- 3: Revise and Resubmit x2

2023.1 CHI '23 採択
- 1: Accept with Minor Revisions x3
- 2: Accept with Minor Revisions or Revise and Resubmit x1

CHI'23 レビュワーの主な指摘事項

- **調査設計への指摘**
  - リクルーティング方法/参加者属性は適切か？
  - 調査対象国として日米を選定した理由は？ など

査読結果への対応
- 引用/補足説明の追記
- 調査会社への問合せ
- 既存研究の再調査 等

- **統計分析への指摘**
  - 用いた統計検定手法の妥当正
  - 統計分析の結果の解釈が不適切
  - 報告すべき統計量が不足している点　など

査読結果への対応
- 図表の修正/追記
- 一部データの再分析
- 記載するデータの追加 等

CHI'23 レビュワーの主な指摘事項：
具体例

- **EX）参加者属性に関する指摘**
  - 査読コメント：調査対象国として日本/アメリカを選定した理由は？
  - 対応：日米のソフトウェア開発業界の違いに関する説明を追記（e.g., 自社開発/受託開発の傾向）

- **EX) 参加者募集方法に対する指摘**
  - 査読コメント：参加者募集方法の妥当性に関する説明を追加せよ。利用した調査会社はどのように開発者を募集しているか？過去に学術研究で利用された実績はあるか？
  - 対応：利用したWeb調査会社による参加者募集や品質管理に関する説明を追記
    Web調査会社を利用している既存研究をリストアップし過去に利用実績がある点を主張

- **EX）統計検定に関する指摘**
  - 査読コメント：統計検定における効果量（Effect Size）の解釈に関する説明が不足している。
  - 対応：類似の統計分析を行っている既存論文での記述を参考に説明を追記

ユーザブルセキュリティ研究の論文採択に向けて

- **適切な方法論（調査設計・分析手法）の採用**
  - ユーザブルセキュリティ研究おいては適切な方法で調査/分析をしたか（方法論）が特に重要視される
    - RQを踏まえた適切な調査対象者の選定、質問設計、分析方法　等
- **科学的な品質の確保**
  - 分析結果の理論的根拠（統計検定等）、再現性の確保が求められる
    - 適切な統計検定の実施/統計量の報告、実験手順書/質問紙の提出 等
- **研究倫理への配慮**
  - 人間を中心とした研究分野のためユーザ調査がほぼ必須であり、適切な倫理的配慮が求められる
    - IRB承認、インフォームド・コンセント、個人情報の取り扱い、参加者報酬 等

既存研究を参考に確立された実績のある方法を採用すべき（我流はNG）

- 以下、参考資料

開発者向けユーザ調査を行うにあたって

- 開発者向けユーザ調査では**開発者特有のユーザ属性**の考慮が必要

一般的なユーザ属性の例

- 年齢
- 性別
- 母国語
- 教育的バックグラウンド
- ハンディキャップ　など

開発者特有のユーザ属性の例

- 立場：プロ, フリーランス, 学生
- プログラミングスキルの有無
- 役職：デベロッパ, マネージャ …
- 業務内容：実装, テスト…
- 所属企業：大企業, 中小企業

例えば下記のような調査設計は　Ecological Validityに問題があるとされる

- プロ向けの開発サポートツールの評価に大学生を募集

開発者のリクルーティング

- 一般的にエンドユーザと比較して開発者のリクルーティングは難しい
  - スキルのある参加者を募集しづらい、コンタクト先が少ない、費用がかかりやすい、など

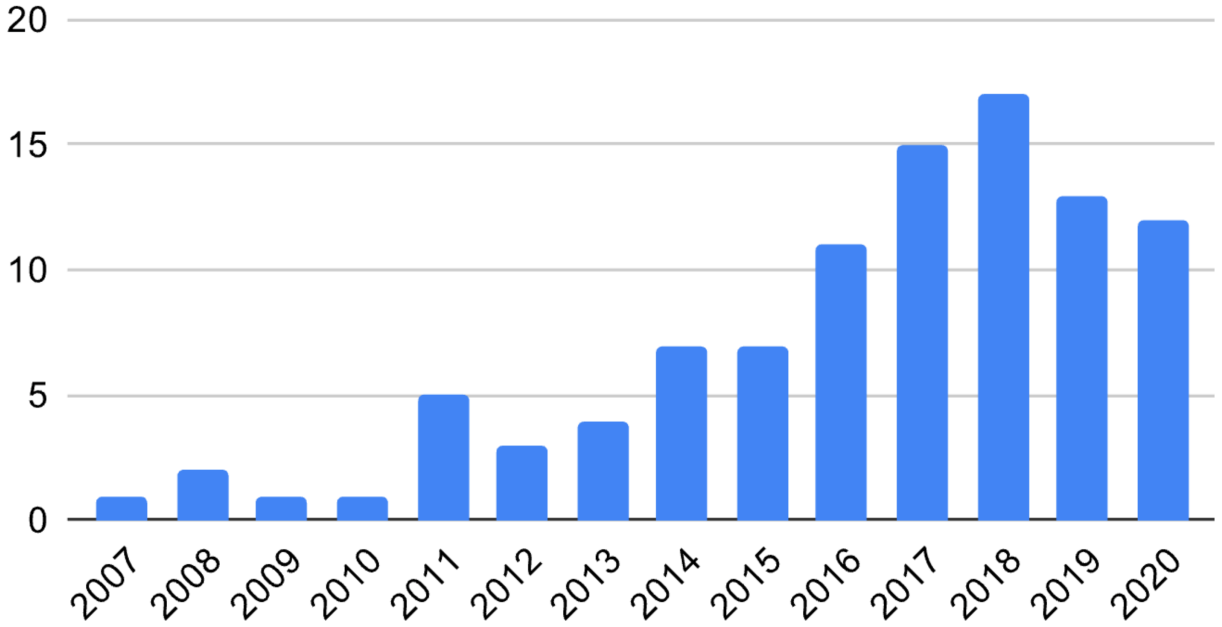
- 既存研究で用いられている開発者のリクルーティング方法 [SEC'22]
  - 研究者のコネクション活用(e.g., 個人的な連絡先、スノーボールサンプリング、MLでのCS学生募集)
  - 有料サービス(e.g., Prolific, Upwork, Freelancer)
  - ソーシャルメディア(e.g., Twitter, Facebook Groups)
  - オンラインフォーラム/ブログ (e.g., Reddit)
  - ネットワーキング(e.g., LinkedIn)
  - メール募集(e.g., Github, Google Play)

過去にやってる研究はあるが)
GitHubやGoogle Play 経由の開発者の
募集はサービスの利用規約違反のため
非推奨 [CHI'22]

Tahaei et al. *Recruiting Participants With Programming Skills: A Comparison of Four Crowdsourcing Platforms and a CS Student Mailing List* (CHI'22)
Kaur et al. *Where to Recruit for Security Development Studies from: Comparing Six Software Developer Samples* (SEC'22)

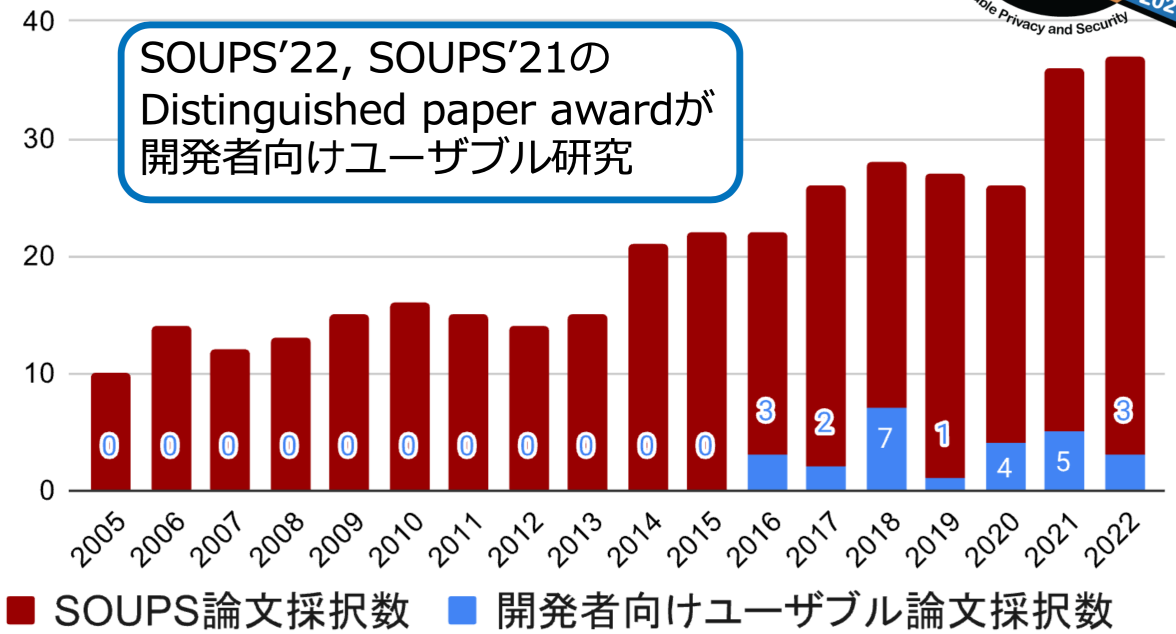
論文数から見る開発者向けユーザブルセキュリティ研究

開発者向けユーザブルセキュリティ
研究に関する論文件数*



2016年頃から急速に論文件数が増加

難関国際会議SOUPSにおける開発者向け
ユーザブルセキュリティ論文

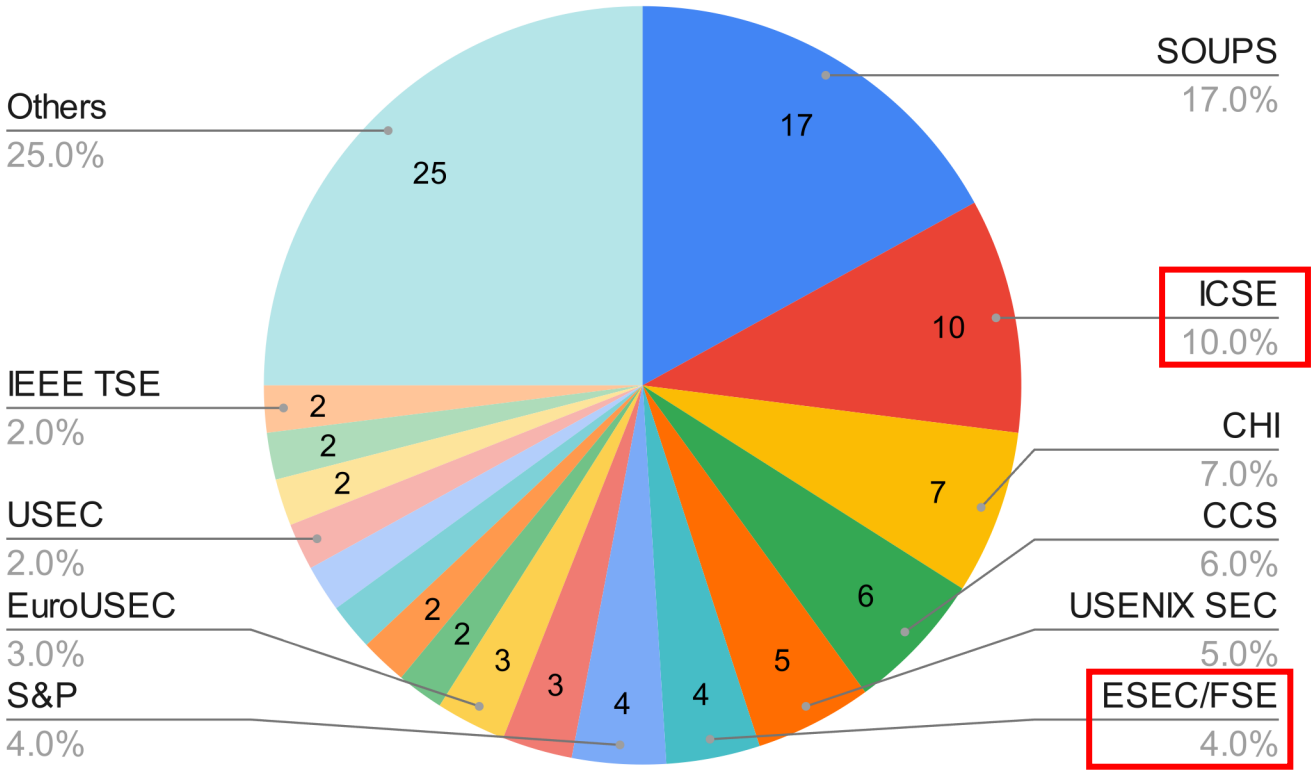


近年のSOUPSにおける論文における1～2割が
開発者向けユーザブルセキュリティ研究

*参考元: Mokhberi et al. *SoK : Human , Organizational , and Technological Dimensions of Developers ' Challenges in Engineering Secure Software*, (EuroUSEC'21)
Kaur et al. *Where to Recruit for Security Development Studies: Comparing Six Software Developer Samples*, (SEC'21)
Tahaei et al. A *Survey on Developer-Centred Security*,(EuroUSEC'19)

国際会議ごとに見てみると...

国際会議/論文誌ごとの開発者向け
ユーザブルセキュリティ論文の発表件数*



- ソフトウェア高額分野でも
  ユーザブルセキュリティに関連する
  論文が増加中
  - ICSE, ESEC/FSE, ASE（SW工学分野Tier1会議）で、数年前からHCIのセッションが新設
- IEEE SecDevが2016年から開始
  - セキュアなシステム開発に関する研究に特化した国際会議

*参考元: Mokhberi et al. *SoK : Human , Organizational , and Technological Dimensions of Developers ' Challenges in Engineering Secure Software*, (EuroUSEC'21)
Kaur et al. *Where to Recruit for Security Development Studies: Comparing Six Software Developer Samples*, (SEC'21)
Tahaei et al. A *Survey on Developer-Centred Security*,(EuroUSEC'19)