資料2-2

研究・産学官連携戦略ワーキンググループ 第2回

重点化テーマに向けた検討について

秋山満昭

2020.8.6

内容

- 重点化テーマの模索
  - 「学術的に興味深い＋産業的に役に立つ」を充足する分野/領域/軸は何か？
  - 環境的要因：法制度・社会的コンセンサスに関する状況分析
- Top-4論文における産学連携研究の調査
- 成功している他研究分野から学ぶ国際競争・連携の方法
  - 日本のHCIコミュニティ

重点化テーマの模索
「学術的に興味深い＋産業的に役に立つ」を充足する分野/領域/軸は何か？

- **今後社会基盤を支えるであろうICT要素技術のセキュリティ的側面**
  - AIセキュリティ：AIの信頼性が揺らぐと、活用する社会基盤そのものへの影響大
  - 非PC（IoT/OT/CPS等）のセキュリティ：Windows等のPCの解析技術が重要だったのと同様に、モバイルデバイス・IoT/OT/CPSの解析技術はサイバー攻撃対策として必須
- **産業活動を活性化できるセキュリティ技術**
  - データセキュリティ：データは産業活動の源泉。データの保存・交換・処理の安全を確保することでデータ利活用が促進される
  - ユーザブルセキュリティ：人に着目したセキュリティ。セキュリティを担保しつつユーザビリティを向上させる技術はユーザのオンライン活動の活性化に直結。例: FIDO2などのパスワードレス技術等。
- **実データ（臨床データ）の観測・分析と研究へのフィードバック**
  - 実データの観測に基づいたセキュリティ研究：データドリブンアプローチでの研究（医学でいうところの臨床実験・研究）。ネットワーク・システム・サービスの運用時のデータを活用。対策手法の評価検証だけでなく、実態調査に基づいて最新の攻撃情報を把握し、新たな対策技術の研究に活用する、など。
- **未知の脅威を発見する方法の研究（攻撃研究）**
  - オフェンシブセキュリティ：攻撃者の視点に立って未知の脅威を発見、攻撃に悪用される前に対策。水際対策・事後対策から脱却し、事前対策（設計から作り直す、シフトレフト化）によって、根本からの問題解決を目指すもの。対象は低～高レイヤまで対象は広い。日本からのTop-4採択論文の多くが攻撃研究（CCS ‘14, S&P ‘19, NDSS ‘20）。

※これらは完全に独立したものではなく、それぞれにまたがる研究もある

重点化テーマの模索
環境的要因：法制度・社会的コンセンサスに関する状況分析

- プライバシー関連法（欧州GDPR，米国CCPA）
  - 欧州GDPRが2018年施行、米国カルフォルニア州でもGDPRと同等のCCPAが施行。欧米を中心に法制度とサイバーセキュリティの研究（例：法制度とICT設計・運用のギャップの把握や解決に関する研究）が盛んに行われている。
  - 強力なプライバシー保護法が施行されたことを強みに変えて研究を推進していることが欧米の強み
- 米国著作権法にみる「フェアユース」という法理
  - 米国著作権法違反に対する抗弁事由のひとつ、公平な理由があれば侵害に当たらない
  - 米国と同じ研究を日本でやろうとした場合、各種法令違反の懸念が強く、同じことができないと感じる。
  - 日本では、著作権法が2019年に改正されてセキュリティ確保や研究のためのリバースエンジニアリングが認められてはいるが、製品の利用規約はリバースエンジニアリングを禁止しているものが多く、民事訴訟のリスクが懸念される
- 日本の「不正アクセス禁止法」や「不正指令電磁記録罪」の運用について
  - セキュリティ社員逮捕事件や（研究活動ではないが）コインハイブ事件・アラートループ事件などを通じて、多くのセキュリティ有識者から「不透明な部分がある」との指摘がある
  - 研究活動に対する萎縮作用は少なからずあると考えられる
- 日本の学会・研究コミュニティとしては「サイバーセキュリティの研究倫理」に関する取り組みを推進
  - http://www.iwsec.org/mws/ethics.html
  - 革新的研究をサポートする取り組み（啓発活動、チェックリスト、相談窓口）を通じて、学術界・産業界横断的に世論形成が徐々に行われている状況
  - 米国発行のICT/セキュリティ研究の研究倫理指針を示したMenlo Reportの精神に従っている

著作権や不正アクセス関連法に関して米国と比べると日本はまだまだ厳しい状況にあるのではないか。
日本では、企業/研究者と政府機関が協働することが必要ではないか？

Top-4論文における産学連携研究の調査
（実用性を重視しているUSENIX Securityに着目して分析）

- 産学連携論文：ここ10年で増加中
  - 2010: 4/30（13.3%）, 2015: 12/55（21.8%）, 2020: 155本中36本（23.2%）
- 産業のみの論文は非常に少なく、どの年も数件程度
  - GoogleやMicrosoft等が単一組織としての論文多数
- 産学連携の国別比較：US中心だが、中国・韓国も存在感が出てきた
  - 2010: US国内、UK国内、UK+シンガポール、US+中国
  - 2015: US国内5件、US+イスラエル2件、US+ドイツ、US+韓国、US+中国、ドイツ国内
  - 2020: US国内13件、中国国内3件、US+韓国3件、 US+中国2件、 US+スイス2件、US+カナダ、US+ルーマニア、オーストリア国内、US+ベルギー、カナダ+ドイツ、中国+オーストラリア、中国+オーストラリア+US、スウェーデン+ドイツ+オランダ、韓国+オーストラリア

＊組織の国・分類が不明なものがあるので数字は必ずしも正確ではない

Top-4論文における産学連携研究の調査
（実用性を重視している USENIX Security に着目して分析）

- 産学連携で多い企業 (2020年)
  - Google 4件、Samsung 4件、Facebook 2件、IBM 2件、…
  - 中国系企業 7件（Alibaba Group 2件, Ant Financial 2件, SK Hynix, Qi An Xin Technology Research Institute, PWNZEN InfoTech Co., LTD, ByteDance Inc.）
- 産学連携の研究トピック (2020年) *セッション名で分類
  - 4件: 機械学習、ファジング
  - 3件: モバイル、Webセキュリティ＆プライバシー、フィッシング検知、暗号解析/実装、プライバシー保護技術
  - 2件: TEE, Fintech, 認証, データセキュリティ
  - 1件: ネットワーク, ソフトウェア, システム, ユーザブルセキュリティ 1件, 音声アシスタント

・機械学習の脅威、セキュリティを担保する方法
・データのセキュリティを担保しつつ共有・計算する方法
・低〜高レイヤの脅威発見手法

成功している他研究分野から学ぶ国際競争・連携の方法

- 世界的に競争できている研究分野例：ヒューマンコンピュータインタラクション（HCI）分野
  - トップ会議CHIの論文シェアで日本が上位

- HCI分野の第一線で活躍する 山下直美氏 へヒアリングを実施
  - 世界的に競争力を持つためには、世界トップレベルと交流し、世界的と渡り合えるグループ作りが重要
    - 雑務に追い回されずに研究に専念できる環境作りが重要。海外から日本に来たい研究者がいたとしても、雑務やルールが多く、研究活動に幅を持たせたり専念することができないため、逃げていく感じがする。
  - 世界的に競争力のある組織はプロモーション力に長けている
    - CHIなどに参加すると、ある組織（大学や研究機関）がpublishした過去 5 年間の研究成果をまとめたものをbookletにして配っているのを見かける
    - 日本では、個人レベルでSNSで宣伝している人がいるが、組織的な連携はあまりない
    - 予算の使途に制限があり、各研究の範囲を超えた予算執行が許されないのかもしれない
  - 国際学会のローカルチャプター運営による国内HCI研究とトップ会議（CHI/CSCW等）との橋渡し
    - ACM SIGCHI Japan Chapterによって、CHI勉強会・CHI Japan Night等、研究コミュニティを支援している。CHI2021日本開催なども、少しはJapan Chapterの存在が影響したのではないか
    - ただし、こういった国際的な営みを広げる活動（Japan Nightや、シンポジウムなど）を行うための費用の捻出はいつも（他国と比較しても）苦労している
    - Microsoftなどがコミュニティ活動の資金援助をするのは、優秀な人材を集める上で一役買っている。日本でもそうできれば良いのにと思う

成功している他研究分野から学ぶ国際競争・連携の方法

- HCI分野で第一線で活躍する山下直美氏へヒアリングを実施（続き）
  - 国際的なポジションの変化
    - ほんの数年前まで、CHIの採択数は、アジアでは日本がトップだったが、中国・韓国（というより、殆どKAIST）にあっというまに追い越された。
    - 韓国や中国は、米国有名大学で博士を取ると、自国で優遇される模様。日本ではそういうのが全然ない。
    - 日本人の学生から「日本の方が安全で居心地がいいし、海外に行っても優遇されないなら、行くモチベーションが沸きにくい」という意見がでている。
  - 人材交流
    - 海外に人材を送り込む方法について
      - あまりやっていない。
      - たぶん「何か技を学んできて日本で活かす」というものではなく、査読者レベルの研究者と絶えず議論を重ねて研究を改善する機会があることが重要なのではないか。
      - 査読者レベルになるには、数年はかかるので、たとえば数か月や１年行って学んで来ようと思っても、なかなか難しい。
      - HCIの分野に関していえば、短期間（１年程度）でノウハウなどの習得が難しい（日本人の修士学生でCHI・CSCWに論文を通すのはほぼ無理）
    - 海外から優秀な人材を呼び込む方法について
      - 知人の何人かの先生は、向こうの有名な先生と知り合いになり、来てもらって一緒に研究する、という方法をやっている。この方法は、向こうの先生が「日本」に興味を持っている場合は長続きする。ただ、招聘にお金がかかる。
      - 海外から優秀な人に来てもらう方法を考えた方が勝算が大きい。優秀な人を日本に呼ぶ場合、日本は住環境等がよく、日本に来たいと思う人は遥かに多いのではないか。