資料2-1

重点領域・テーマについて

横浜国立大学　吉岡克成

研究・産学官連携戦略WG 資料（2020.08.06）

本日のトピック

- サイバーセキュリティ研究とその変遷
- 最近のサイバーセキュリティ研究に共通する重要な観点
- 日本の強みについて
- 事例紹介：米国・欧州と伍していくための交流

サイバーセキュリティ研究とその変遷

10年以上前から実施されている典型的研究アプローチの例

- 攻撃の観測
- マルウェア収集
- 攻撃コードの解析
- マルウェア解析・分類
- 可視化
- 検知・防御手法
- 駆除・隔離手法
- セキュリティ強化手法

研究アプローチ自体に新規性が無くても、社会・技術トレンド、脅威の変遷等により、研究対象に新規性があるケースも多い
（例：IoT・AI・DXの普及・進展、標的型攻撃、ランサム、制御システム攻撃、コネクテッドカーへの攻撃、など）

参考：付録（スライド１４－１５）

サイバーセキュリティ研究とその変遷

10年以上前から実施されている典型的研究アプローチの例

- 攻撃の観測
- マルウェア収集
- 攻撃コードの解析
- マルウェア解析・分類
- 可視化
- 検知・防御手法
- 駆除・隔離手法
- セキュリティ強化手法

新しい研究アプローチの例

- 広域スキャン、大規模調査による実態把握
- 脆弱性の発見、攻撃の提案

広域スキャンや大規模調査により新たな脅威、問題を発見する研究の増加（正確な実態把握の重要性）

参考：付録（スライド１６、１７）

サイバーセキュリティ研究とその変遷

10年以上前から実施されている典型的研究アプローチの例

- 攻撃の観測
- マルウェア収集
- 攻撃コードの解析
- マルウェア解析・分類
- 可視化
- 検知・防御手法
- 駆除・隔離手法
- セキュリティ強化手法

新しい研究アプローチの例

- 広域スキャン、大規模調査による実態把握
- 脆弱性の発見、攻撃の提案

参考：付録（スライド１８，１９）

実際に発生する前に攻撃を発見し、インパクト等を検証する研究（攻撃研究）の増加.「責任ある情報開示」など研究倫理対応がスタンダードに

サイバーセキュリティ研究とその変遷

10年以上前から実施されている典型的研究アプローチの例

- 攻撃コードの解析
- マルウェア解析・分類
- 可視化
- 検知・防御手法
- 駆除・隔離手法

システムだけでなく人の振る舞い、判断が脅威の源泉となるという発想

新しい研究アプローチの例

- ユーザの振る舞いの分析・理解
- 開発者の振る舞いの分析・理解
- 攻撃者の振る舞いの分析・理解・経済的要素

脆弱なシステム、アプリを作る開発者の振る舞い、傾向、周辺環境の分析・改善が重要という発想

攻撃の実態や特徴の把握、アトリビューション.脅威インテリジェンス収集など

マネタイズ等、経済的背景等の理解と対策の実効性向上

参考：付録（スライド２０）

サイバーセキュリティ研究とその変遷

10年以上前から実施されている典型的研究アプローチの例

- 攻撃の観測
- マルウェア収集
- 攻撃コードの解析
- マルウェア解析・分類
- 可視化
- 検知・防御手法
- 駆除・隔離手法
- セキュリティ強化手法

新しい研究アプローチの例

- 広域スキャン、大規模調査による実態把握
- 脆弱性の発見、攻撃の提案

新しい研究アプローチの例

- ユーザの振る舞いの分析・理解
- 開発者の振る舞いの分析・理解
- 攻撃者の振る舞いの分析・理解・経済的要素

新しい研究アプローチの例

- セキュリティ通知

検知・発見した攻撃・脆弱性をどう関係者に伝え対策の実効性を向上させるかという観点

参考：付録（スライド２１）

最近のサイバーセキュリティ研究に共通する重要な観点

- **技術・社会・脅威の正確な現状把握**
  - サイバーセキュリティは応用分野．社会的・産業的観点、要請を忘れてはタコツボ研究になってしまう
  - 「この脅威は終わった」という根拠のない噂に流されずデータのみを信じる．
- **ヒューマンファクター**
  - システムを使うのも、攻撃を行っているのも結局は人間
  - 人の振る舞いに影響を与える経済的、社会的、政治的な背景
  - AI普及が進む社会ではどうなるか？（誰が判断するのか？）
- **プロアクティブ**
  - 調査研究、攻撃研究で先回りし、後追い対策から脱却
  - 脅威の予測による選択的集中と対策
  - 意味のある予測には正確な状況把握が必要

（米国、欧州等と伍していくための）海外との交流について

- **留学等（日本研究者→海外）**
  - 訪問（スポット）
  - 短期留学

    ← こちらが現実的
  - 現地で学位取得
  - 現地の大学に採用
  - 出身国から人材受入（橋渡し）

    ← こちらが望ましいが
  - （出身国に戻り優遇）

- **招へい・雇用（海外研究者→日本）**
  - 招待講演等（スポット）

    ← こちらが現実的
  - 短期招へい、雇用
  - 長期招へい、雇用

    ← こちらが望ましいが

横浜国立大学先端科学技術高等研究院
情報・物理セキュリティ研究ユニット

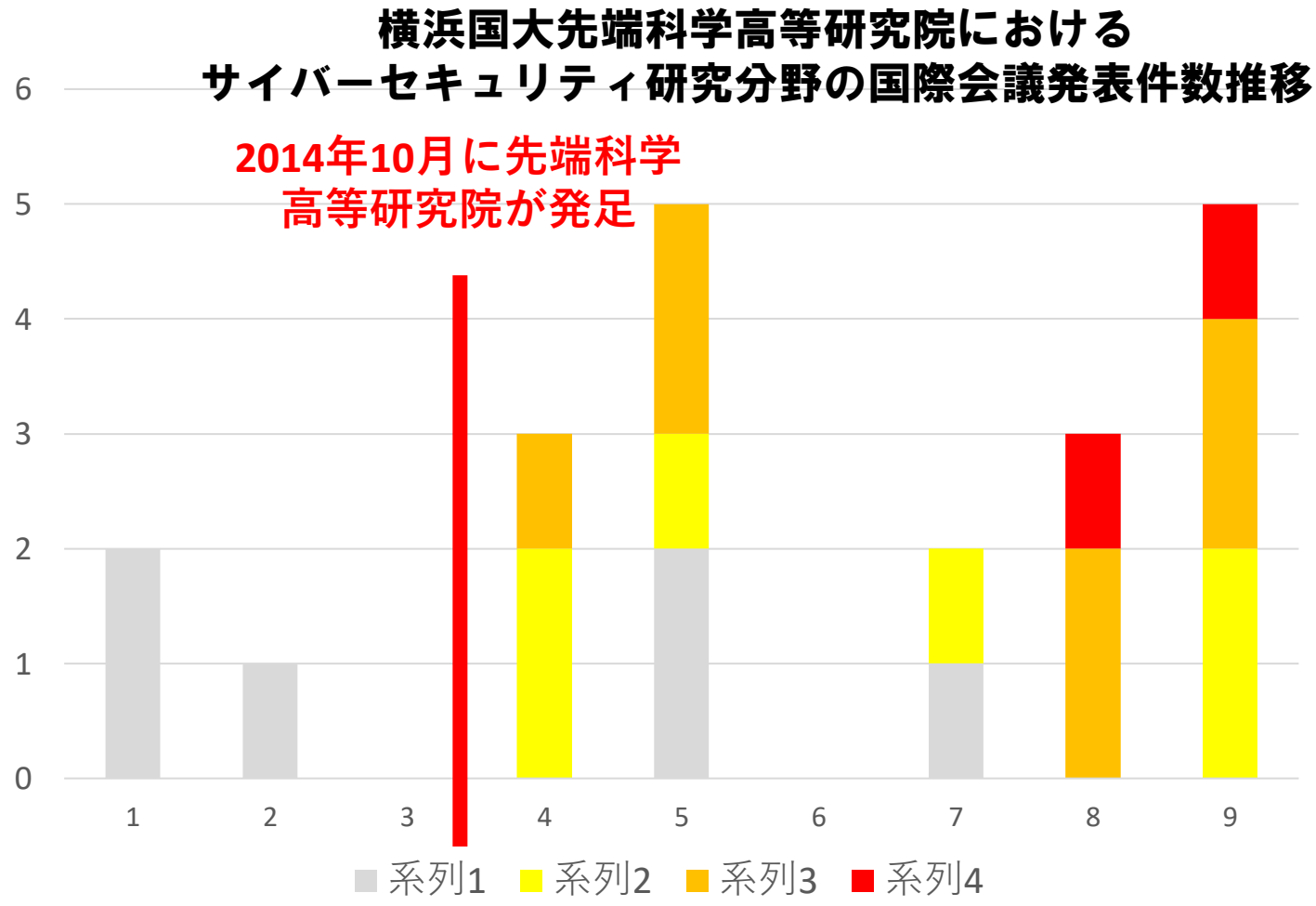
- 文部科学省「国立大学改革強化推進事業」を基に設立された
- 海外（米国、ドイツ、オランダ）から著名研究者を短期雇用・招へい（1週間~2ヶ月／年）し、国際共同研究を実施
- 多数の国内研究組織との共同研究

  情報通信研究機構、NTTセキュアプラットフォーム研究所、富士通研究所、NEC、トレンドマイクロ、セキュアブレイン、三菱電機、KDDI総合研究所他

横浜国立大学
先端科学高等研究院

招へいしたトップ研究者からの学び

年に１週間～１か月トップ研究者を大学に招いて集中的に議論を実施し（×２大学）、この分野の論文の書き方（通し方）を学んだ



短期留学による学び

- 2019年3月、UCSBの招へい研究者から若手研究者をUCSBに寄こさないか、と聞かれる

- 希望者を大学で探すも見つからず。共同研究をしているNICTから１名の希望があり、短期留学（半年間）を実施して頂いた。

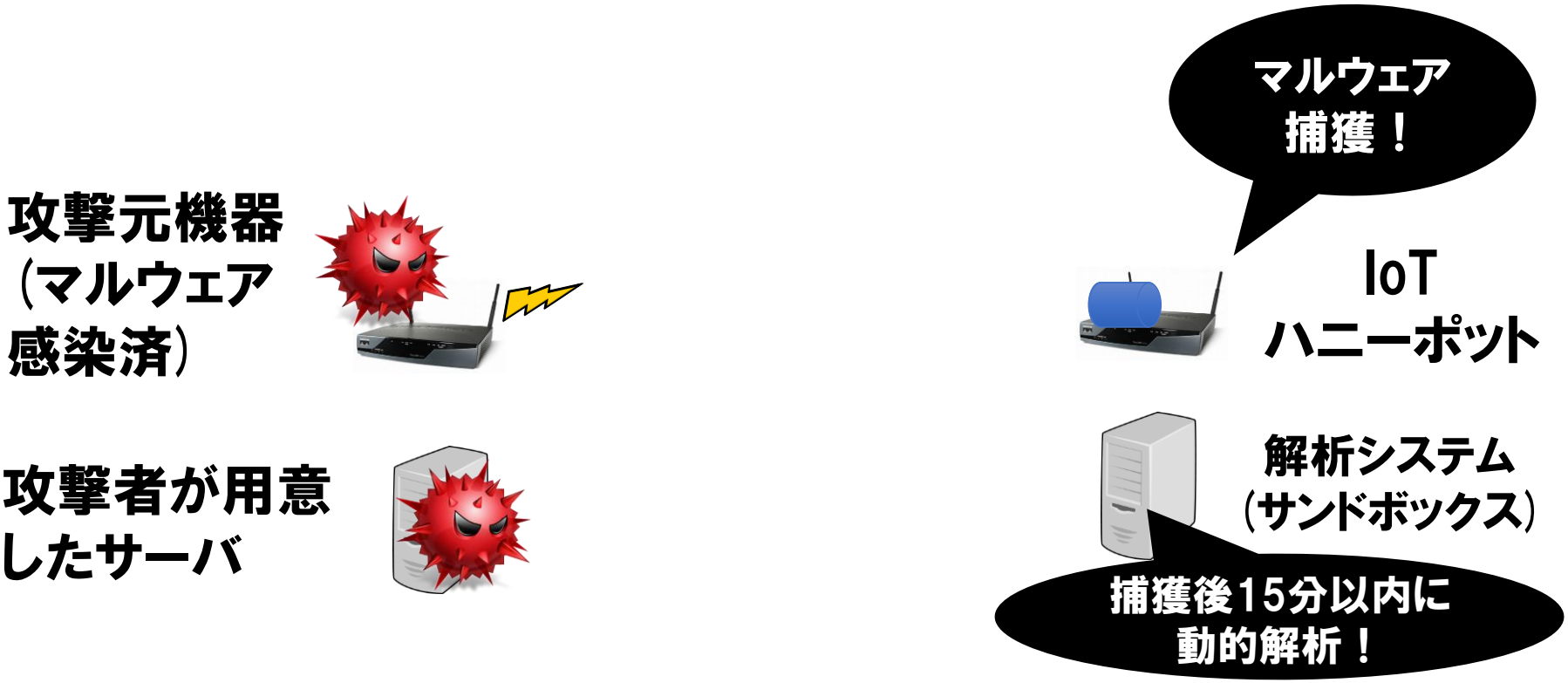
- 先日、留学当時の研究成果がRAID2020（T2）に採録となった。

流動性や海外志向の小さい現状では、短期留学、短期招へいが現実的かもしれない。（自らの経験から、それでも大きな効果があるように思われる）

付録

事例：ハニーポットによるIoTサイバー攻撃の観測と詳細分析

脆弱なIoT機器を模擬した**囮システム（ハニーポット）**により
IoTにおける大規模サイバー攻撃の詳細解析を行った[1].



[1]Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, and Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," 9th USENIX Workshop on Offensive Technologies (USENIX WOOT 2015), 2015.

事例：ハニーポットによるIoTサイバー攻撃の観測と詳細分析

- ハニーポットは「古い」研究テーマ。でもIoTなら「タイムリー」？
- 30か国100以上の研究機関、公的対策機関等にIoTマルウェア検体などのデータを提供
- 発表論文2件の合計参照件数は330件超 [2]
- 最初の研究論文発表の約1年後に、IoTマルウェアMiraiによる当時史上最大のサイバー攻撃が発生し注目された（偶然）
- 後述するユーザへの感染状況通知の研究 [NDSS2019] のベースになった

[2] https://scholar.google.com/citations?user=HlEM1f4AAAAJ&hl=en

広域スキャン・大規模調査を行った研究事例

Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer,Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey, and J. Alex Halderman, “The Matter of Heartbleed,” ACM Internet Measurement Conference (IMC), November 2014.

Zakir Durumeric, Eric Wustrow, and J. Alex Halderman, “ZMap: Fast Internet-Wide Scanning and its Security Applications” USENIX Security Symposium, August 2013

Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman, “Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices” USENIX Security Symposium, August 2012

大規模調査に関する国内研究事例

Voice Assistant アプリの大規模実態調査 (CSS2019最優秀論文賞)

刀塚 敦子(早稲田大学)、飯島 涼(早稲田大学, 情報通信研究機構)、渡邉 卓弥(早稲田大学, NTTセキュアプラットフォーム研究所)、秋山 満昭(NTTセキュアプラットフォーム研究所)、酒井 哲也(早稲田大学)、森 達哉(早稲田大学, 情報通信研究機構, 理研 AIP)

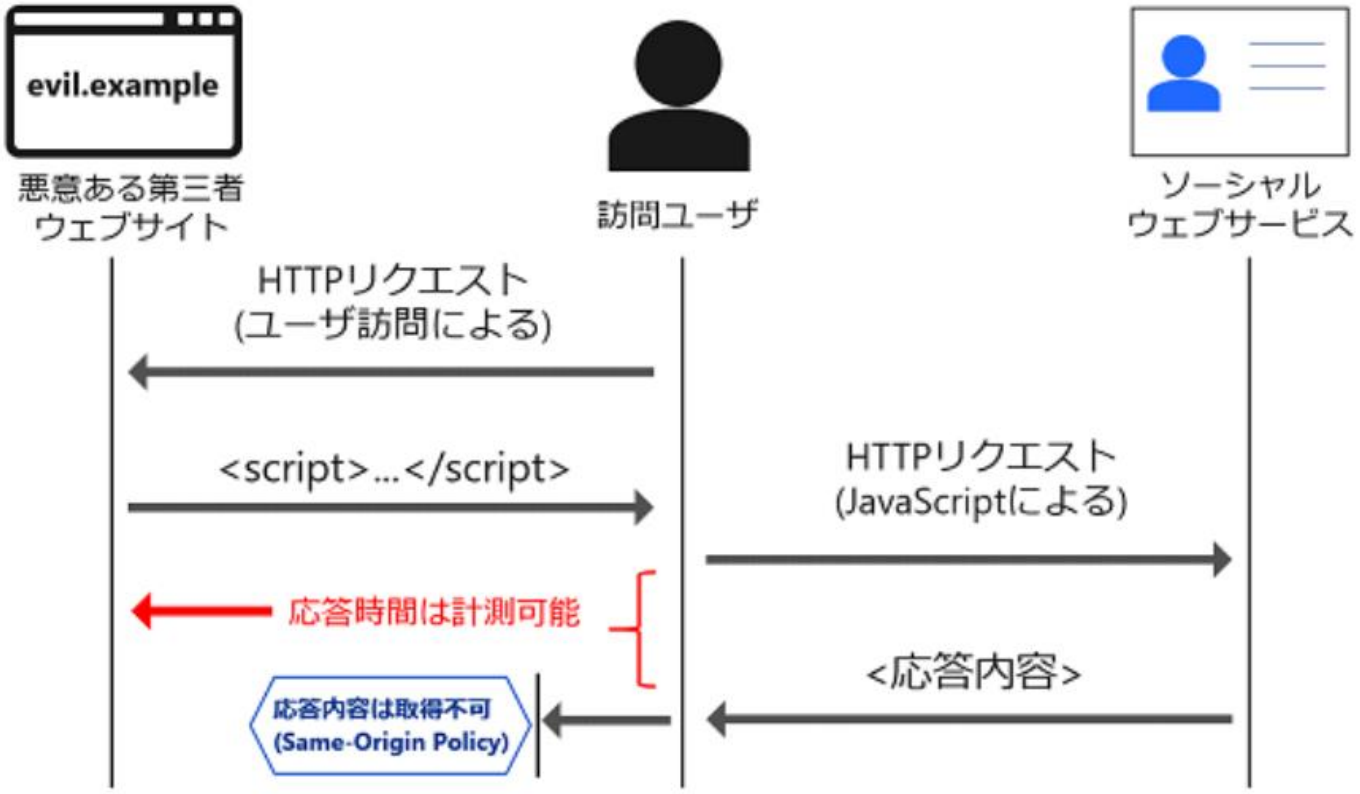
Androidアプリケーションにおける電子署名の大規模調査 (CSS2016学生論文賞)

吉田 奏絵 (東邦大学)、今井 宏謙 (東邦大学)、芹沢 奈々 (早稲田大学)、森 達哉 (早稲田大学)、金岡 晃 (東邦大学)

クラウドサービス悪用攻撃の大規模実態調査 (CSS2019学生論文賞)

福士 直翼(早稲田大学)、千葉 大紀(NTTセキュアプラットフォーム研究所)、秋山 満昭(NTTセキュアプラットフォーム研究所)、内田 真人(早稲田大学)

訪問ユーザとSNSアカウントを結び付けるプライバシ攻撃



クロスサイトリクエストフォージェリによるタイミング情報の計測

https://www.ntt.co.jp/sc/project/cybersecurity/silhouette.html

T. Watanabe, E. Shioji, M. Akiyama, K. Sasaoka, T. Yagi, and T. Mori, “User Blocking Considered Harmful? An Attacker-controllable Side Channel to Identify Social Accounts,” Proceedings of the 3rd IEEE European Symposium on Security and Privacy (Euro S&P 2018), April 2018

実世界への対策の適用

影響を受けるサービス事業者やブラウザベンダに対し、被害が発生する前に事前の情報共有を行うとともに、Twitterなどの実際のウェブサービスやMicrosoft Edge、Internet Explorer、Mozilla Firefoxといったウェブブラウザの対策実施に対し評価手法を用いて協力することで、本脅威による第三者からのアカウント名特定を不可能とする対策を実施.

https://www.ntt.co.jp/news2018/1807/180718a.html

企業

プライバシー脅威「シルエット」への対策

投稿者 @kpk および @equanimityhow
水曜日, 2018年9月19日

利用者の皆さんのセキュリティとデータを守ることはとても大切なことです。一つの側面として、他のサイトを訪問する際にTwitterの個人情報を守ることが挙げられます。

メール、ツイート、他のサイトの広告、またはハッキングされた馴染みのあるサイトからのリンクを介して、誤って悪質なウェブサイトへアクセスする可能性があります。そのウェブサイトは利用者にわからないように秘密裏で通信を行うため、そのサイトが悪質な性質を持っているかどうか明らかではないかもしれません。

もし、ウェブサイトが皆さんのTwitterの個人情報を特定できた場合、その情報を追跡や他の紐づいているアカウントにも使用する場合があります。これにより、利用者のオンラインの情報を特定させることができるかもしれません。地域によっては、利用者に大きな

https://blog.twitter.com/official/ja_jp/topics/company/2018/twitter_silhouette_JPN.html

ユーザの振る舞いに関する国内研究事例

ユーザのセキュリティ対策行動における心理的な要因の影響評価（CSS2019優秀論文賞）

佐野 絢音（株式会社KDDI総合研究所）、澤谷 雪子（株式会社KDDI総合研究所）

山田 明（株式会社KDDI総合研究所）、窪田 歩（株式会社KDDI総合研究所）

I Know What You Did Last Login: Inconsistent Messages Tell Existence of a Target's Account to Insiders

Ayako Akiyama Hasegawa, Takuya Watanabe, Eitaro Shioji, Mitsuaki Akiyama

Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC 2019) 2019年12月

事例：IoTマルウェア感染ユーザへの効果的なセキュリティ注意喚起

O. Cetin, C. Gañán, L. Altena, D. Inoue, T. Kasama, K. Tamiya, Y. Tie, K. Yoshioka, M. van Eeten, "Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai," The Network and Distributed System Security Symposium (NDSS 2019), 2019.