資料9

我が国のサイバーセキュリティ研究の動向について

横浜国立大学　吉岡克成

研究開発戦略専門調査会 資料（2020.02.07）

サイバーセキュリティ研究とその変遷

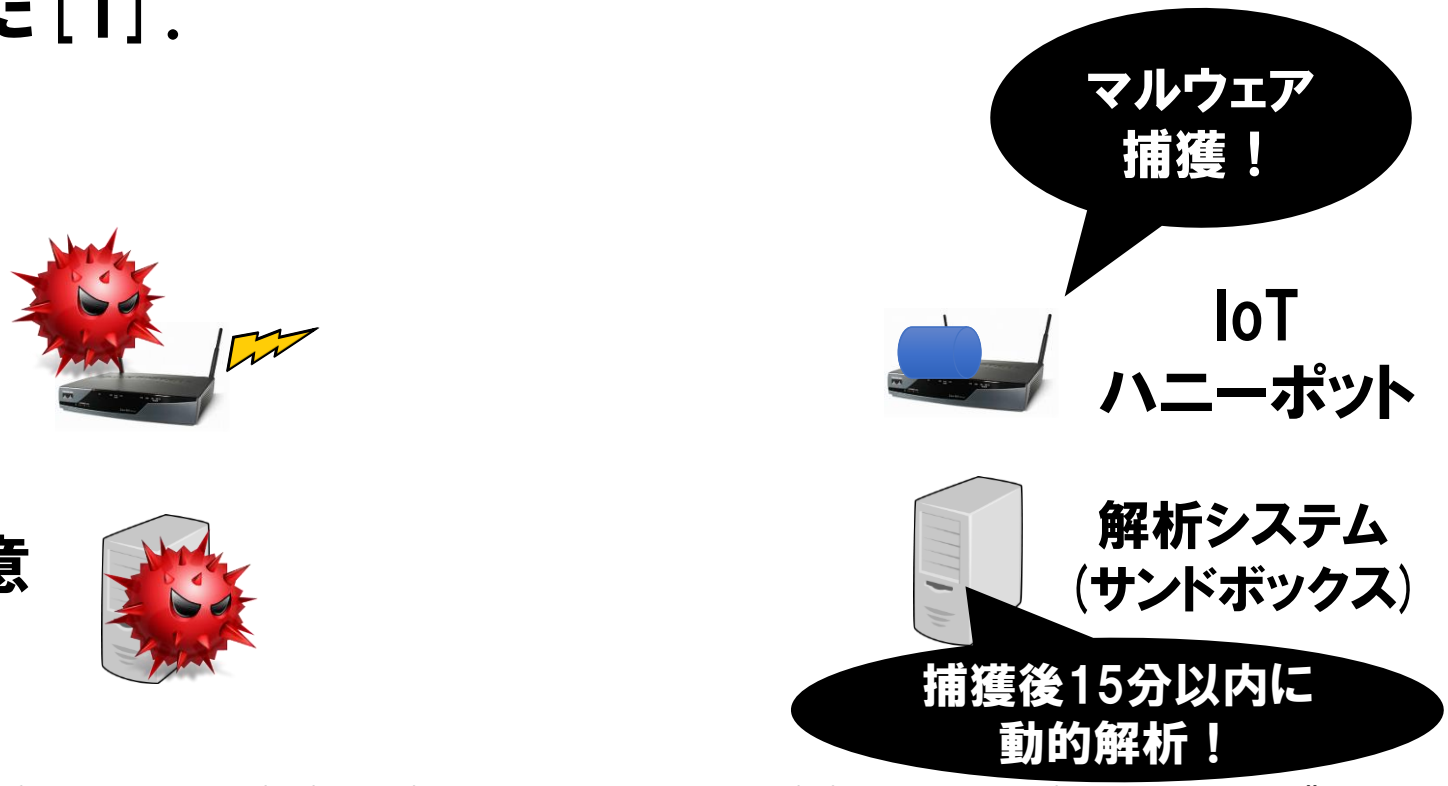
10年以上前から実施されている典型的研究アプローチの例

- 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

社会・技術トレンド、脅威の変遷等により、研究アプローチは同じでも、
対象とする問題の新しさから新規性が生じるケースが多い
（例：スマホ、IoT 、AIの普及、標的型攻撃、ランサム、制御システム
攻撃、実車へのコンセプト攻撃、IoT大量マルウェア感染など）

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）により世界で初めて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

- 30か国90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累計270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

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

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

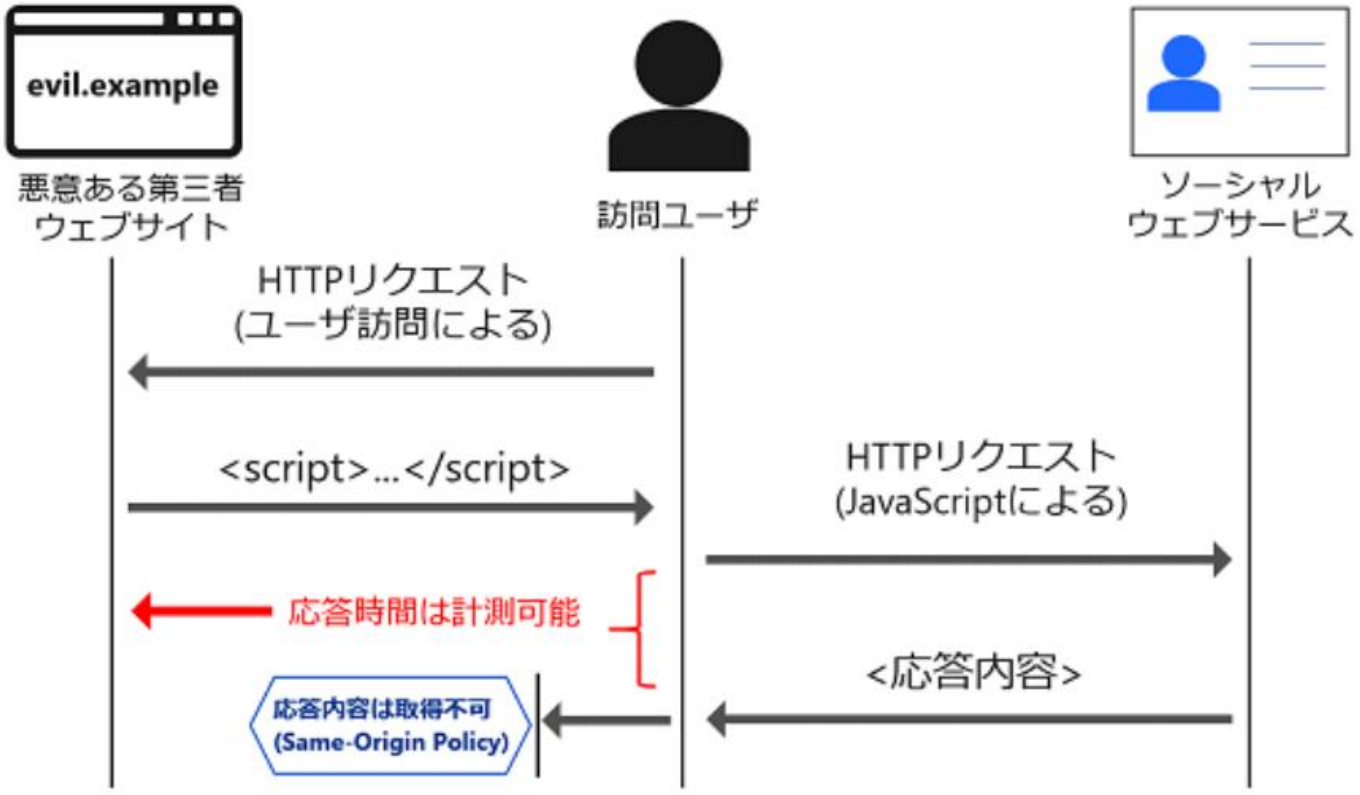
新しい研究アプローチの例

- 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

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

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は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、利用者に大きな危険を及ぼす可能性があります。

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

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

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

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

マネタイズ等、経済的背景等の理解と対策の実効性向上

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

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.

最近のサイバー研究に共通する重要な観点

- **技術・社会・脅威状況の正確な把握**
  - サイバーセキュリティは応用分野．社会的・産業的観点、要請を忘れては独りよがりの研究になってしまう
- **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

我が国の学術系サイバーセキュリティ研究の現状

- 上位のカンファレンスで国内研究が出てこない（投稿すらしない）状況が長く続いてきた
- 7～8年前からTier 2会議（RAID, ACSAC, AsiaCCS, ESORICS等）で少しずつ採録され始める
- 数年前からTier 1会議（Usenix Security, IEEE S&P, ACM CCS, ISOC NDSS）で少しずつ採録され始める

どうしてここまで違うのか？

- **人**
  - （海外有名研究室は）博士課程学生、ポスドク、助教等を中心とする「研究」組織（日本の大学研究室は、学部、修士、博士課程学生からなる研究「教育」組織）
  - （海外有名研究室では）研究室メンバは公募され、高倍率の中、雇用される（ドクター学生は仕事として研究する）.
  - 日本からの海外武者修行、出戻りが少ない
- **社会**
  - （海外では）人材流動性が大きく産業界での実務経験がある人材が博士課程学生として応募する.
  - （海外では）学位取得がキャリアアップに直結し産業界で活躍.
  - （海外では）学術界から産業界への進出（スタートアップ）と産業界からの研究へのフィードバック
- **評価軸**
  - 国内では研究者としての評価はジャーナル投稿数が重要な要素をもつ
  - 米国では、T1等有力会議での発表件数、外部資金獲得などが中心.発行までに年単位で時間がかかるジャーナルよりも国際会議が重視.

注：上記は本資料作成者の主観や伝聞情報を含み、具体的な統計データに基づくものではありません.

我が国の（主に大学での）サイバーセキュリティ研究の活性化に向けて

- 中堅・若手研究者を中心に、国内向け評価軸にとらわれず世界のスタンダードを意識した研究を行う環境・雰囲気が醸成されつつある

- 社会構造、人材流動性、大学に期待される役割など国内と海外で異なる点を認め、日本型の大学研究室モデルで成果を出せるよう模索.
  - 学生の雇用、分担型プロジェクト、社会人ドクター受入、有能なシニア人材の活用など