資料５

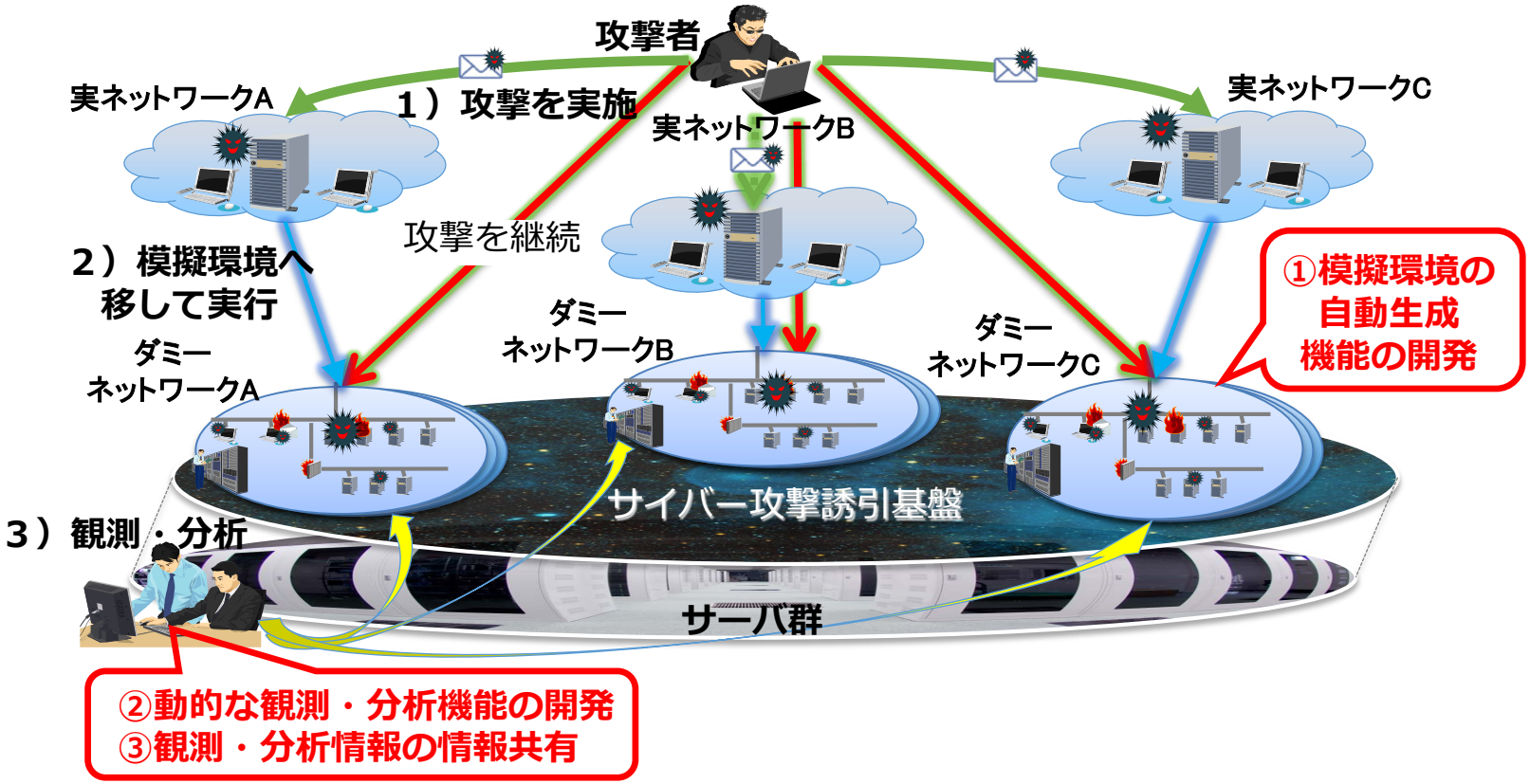
総務省におけるサイバーセキュリティ研究開発の取組み

平成３１年３月１日
総務省
サイバーセキュリティ統括官室

サイバー攻撃誘引基盤の構築（STARDUST）

○　高度かつ複雑なサイバー攻撃に対処するため、政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することが可能な、高度で効率的なサイバー攻撃誘引基盤を構築。

○　攻撃活動の早期収集や未知の標的型攻撃等を迅速に検知する技術等の実証を行うための研究開発環境を、情報通信研究機構（NICT）に整備。分析結果は、セキュリティ対策機関等と連携して情報共有を図り、安全なサイバー空間を実現。



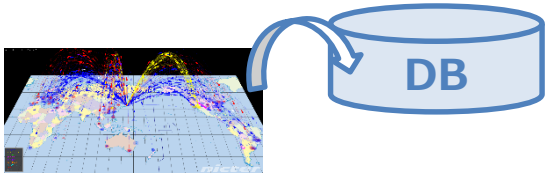
機械学習（AI技術）を活用したサイバーセキュリティの研究開発

○　NICTでは、巧妙化・高度化するサイバー攻撃に対して、機械学習を始めとするAI技術を活用したサイバーセキュリティの研究開発に取り組んでいる。

データセットの構築（例）

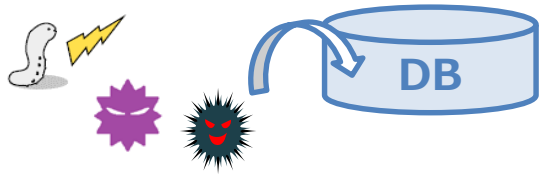
■ダークネット関連データ

未使用IPアドレスへの攻撃関連通信データ等



■マルウェア関連データ

マルウェア検体等、静的・動的解析結果等



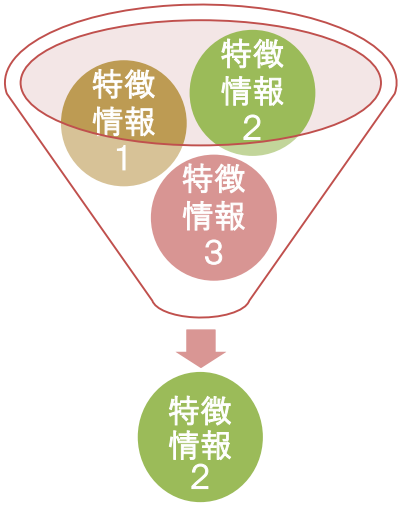
■Android APK関連データ

アプリのカテゴリ情報や説明文等

機械学習の活用（例）

■特徴選択

多様な特徴情報から最も影響力の強い特徴情報を特定



■SVM（サポートベクタマシン）

特徴情報に基づき、機械学習（SVM等）を用いて、データを分類

研究開発成果

攻撃パターンの分析やマルウェアの動作・影響分析等を自動化

（事例１）DDoS攻撃の発生検知

ダークネットトラフィックにおける特徴情報を効果的に特定することで、DDoS攻撃の発生を早期に検知

（事例２）パッカーの特定

マルウェアがどのようなパッカー（難読化ツール（※））を利用しているかを特定

（事例３）Androidアプリ分析

オンラインマーケットで配布されているアプリがマルウェアであるかどうかを判定

（※）難読化ツールとは、実行形式ファイルの機能を損なうことなく、そのソースコードの解析を困難にするツール。

AIを利用してIoT部品のハードウェアのセキュリティの確保を目指した研究

戦略的情報通信研究開発推進事業（SCOPE）：総務省公募研究事業

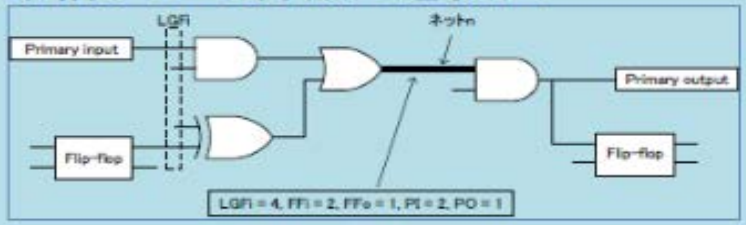
【平成29年度採択案件 ：早稲田大学基幹理工学部　戸川望教授】

IoT機器に悪意ある回路（ハードウェアトロイ）が組み込まれると・・・

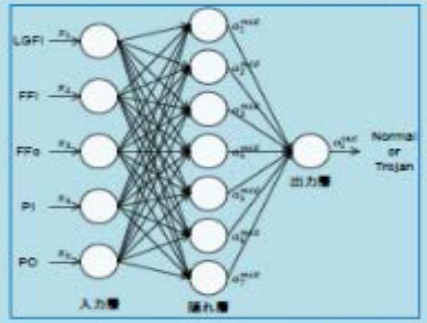
2013年10月（BBC）
ロシアの公営放送局（Rossiya 24)によると、サイバー犯罪者が、アイロンや湯沸かし器の中に、スパムアタックを行うチップを埋め込んでいることが判明。このチップは、勝手にWi-Fiネットワークに繋がってウイルスをばらまく電子回路が組み込まれていた。

http://www.bbc.com/news/blogs-news-from-elsewhere-24707337

回路構造から特徴量を抽出



AIによる学習と判断でハードウェアトロイの検知



→ 未知のハードウェアトロイを誤りなく検知することが目標！

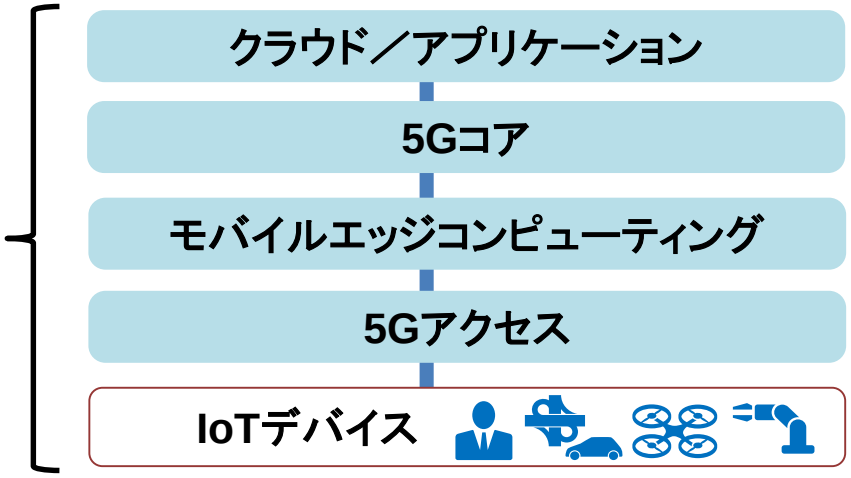
SCOPE課題「設計工程に侵入したハードウェアトロイの検出と耐ハードウェアトロイ設計技術の研究開発」(H26～H28，代表：戸川望)の成果を活用して発展的に研究

5Gネットワークのセキュリティ確保に向けた体制整備と周知・啓発

第5世代移動通信システム（5G）は、IoTシステムの基盤技術であるため、5Gに係る各構成要素（デバイス、クラウド、アプリ等）におけるセキュリティを総合的かつ継続的に担保する仕組みを整備し、対策の共有等を図ることを通じ、5Gを活用する重要インフラ事業者等への周知・啓発を図る。

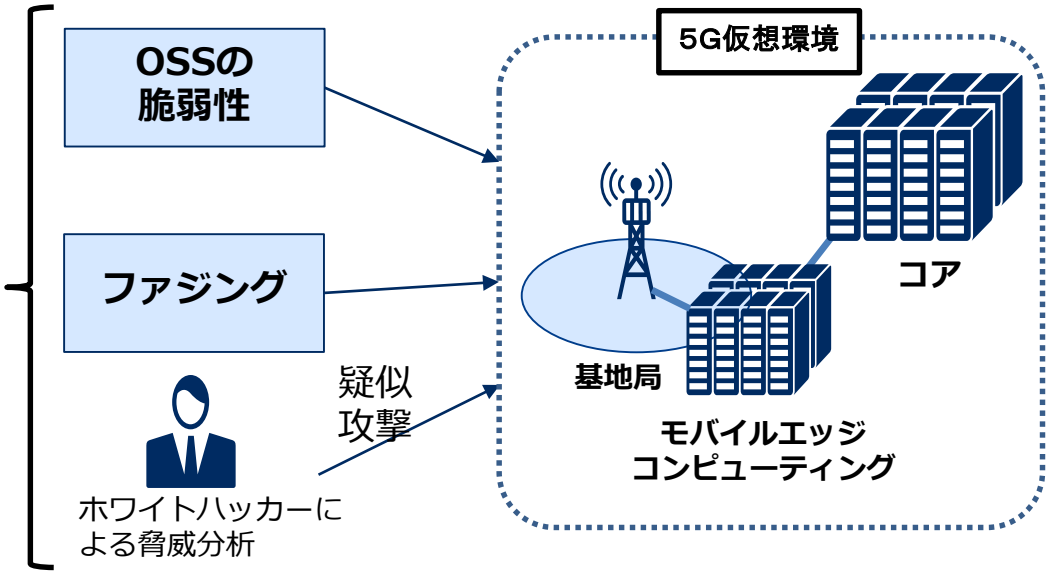
＜基本的考え方＞

- ネットワークインフラとしての機能維持のためには、コア網の機器調達のみに留意すれば良いわけではない。ネットワークのエッジ（基地局の直前）に位置するモバイルエッジコンピューティングのセキュリティが確保されない限り、機能停止/不正動作等のおそれあり。
- 重要通信については、SDN/NFV/スライス等のネットワーク制御技術のセキュリティ対策に加え、5G環境下でのネットワークサービスの各構成要素（デバイス、クラウド、アプリ等）全体を考慮することが必要。



＜平成31年度実施内容＞

- 5Gの仮想環境を構築し、以下の手法により、ネットワークに潜在する脆弱性調査及びセキュリティ課題の洗い出しを実施。
  - ①5Gに実装されるオープンソースソフトウェア等の解析
  - ②多種多様なパターンのデータ送付（ファジング）による異常動作の確認
  - ③ホワイトハッカーによる脆弱性調査、脅威分析
- その結果を踏まえた対応策の策定とその周知・啓発を図る。



その他の取組状況

○ 安全な暗号利用のための研究開発

- 機能性暗号技術や軽量暗号・認証技術、暗号技術の安全性評価、新たな暗号技術の普及・標準化に向けた取組、パーソナルデータの利活用に貢献するためのプライバシー保護技術の研究開発等を実施。

○ 広域ネットワークスキャン技術に関する研究開発

- 脆弱なIoT機器のセキュリティ対策のため、通信量の抑制とスキャンの精度向上を実現する効率的な広域ネットワークスキャン技術の研究開発を平成30年度より実施。

○ 衛星通信における量子暗号技術の研究開発

- 安全な衛星通信ネットワークの構築を可能とし、盗聴や改ざんが極めて困難な量子暗号通信を超小型衛星に活用するための技術の研究開発を平成30年度より実施。

○ 国際標準化活動（ITU-T SG17）

- IoTセキュリティガイドラインをベースとした勧告策定を提案し、2018年9月会合にて新規ワークアイテムとして承認。2020年3月に勧告化合意を目指す。
- 量子暗号通信（量子鍵配送）の鍵管理手法の勧告策定を提案し、2019年1月会合にて新規ワークアイテムとして承認。2020年3月に勧告化合意を目指す。