資料3

サイバーセキュリティ分野における研究開発の取組み

令和２年２月７日

総務省

NICTにおけるサイバーセキュリティ分野の研究マップ

- 急増するサイバー攻撃から社会システム等を守るサイバーセキュリティ分野の技術の高度化が不可欠となっていることを踏まえ、 国立研究開発法人情報通信研究機構(NICT)において研究開発を推進。

インシデント分析センター（ニクター）

NICTER

対サイバー攻撃アラートシステム（ダイダロス）

DAEDALUS

Passive

サイバー攻撃統合分析プラットフォーム
（ニルヴァーナ・カイ）

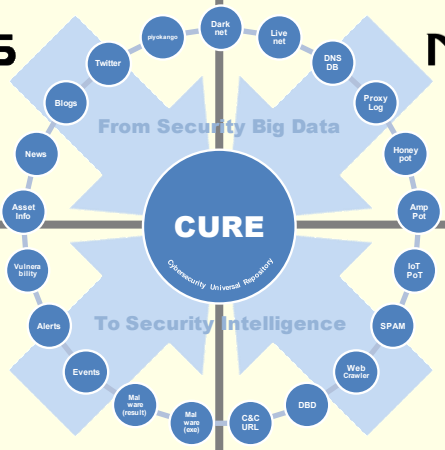
NIRVANA改

脆弱性管理プラットフォーム
（ニルヴァーナ・カイ・ニ）

NIRVANA改弐

Global

Local



リフレクション攻撃専用ハニーポット

AmpPOT

IoTマルウェア専用ハニーポット

IoTPOT

サイバーセキュリティ
ユニバーサル・リポジトリ

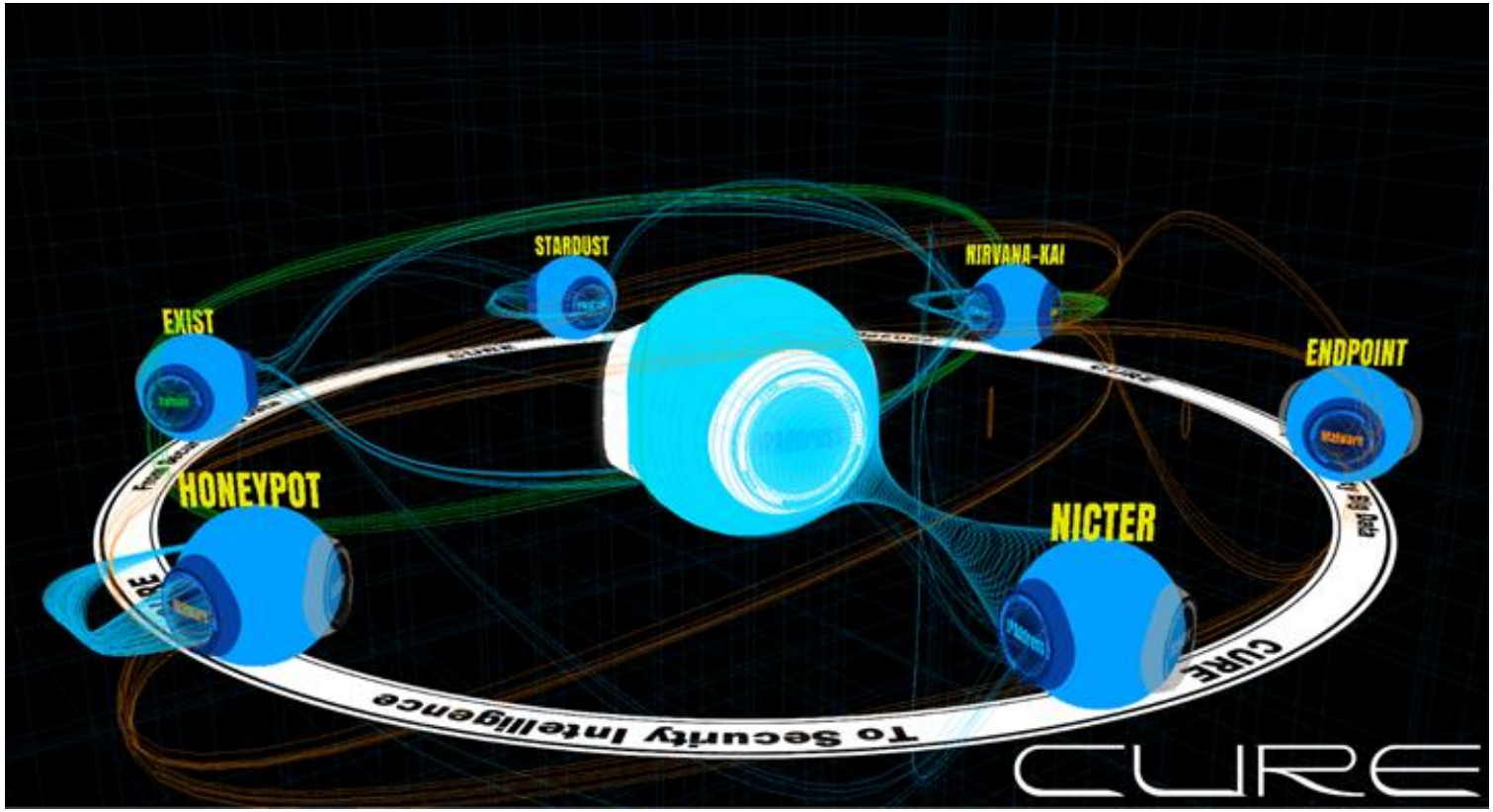
CURE

Active

AIを活用したサイバーセキュリティの高度化

CURE ～サイバーセキュリティ関連情報の大規模集約・横断分析～

- NICTでは、サイバー攻撃の観測情報や脅威情報等、異なる情報源から得られるサイバーセキュリティ関連情報を一元的に集約してつなぎ合わせることで、これまで把握が困難であったサイバー攻撃の隠れた構造を解明し、リアルタイムに可視化。
- 例えば、自組織内のアラートと外部の脅威情報とを関連付けることで、最新の脅威が組織に及ぼす影響について迅速な把握を可能とし、組織のセキュリティ・オペレーションを効率化。



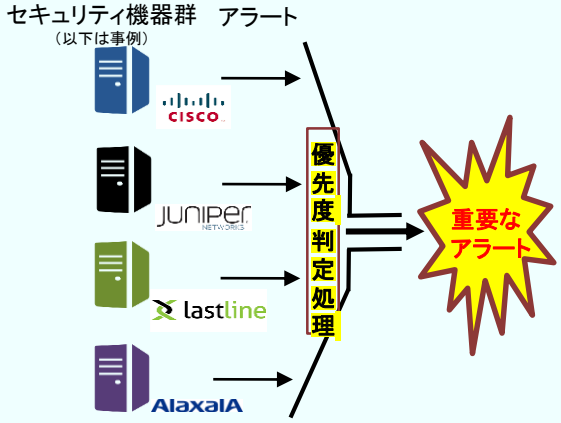
※ CURE（**C**ybersecurity **U**niversal **RE**pository）

AI x Cybersecurity ～AIを活用したサイバーセキュリティの高度化に関する研究～

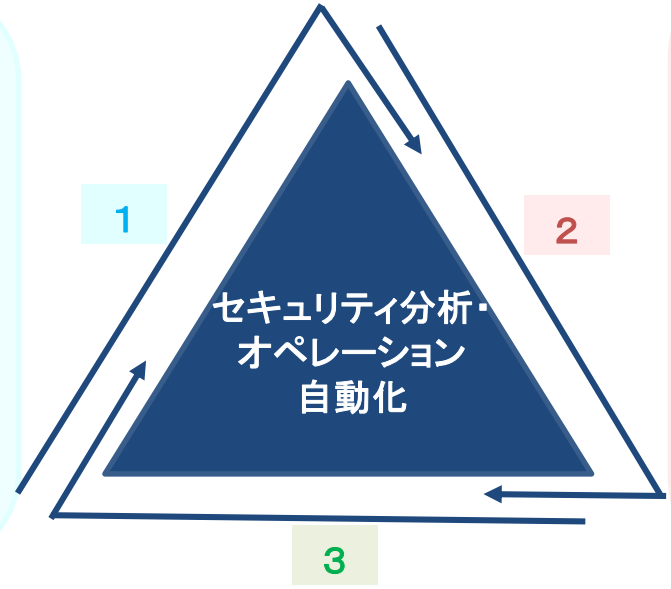
- NICTでは、ダークネット、ハニーポット等の攻撃観測環境を用いて得られた、マルウェアやサイバー攻撃手口などのサイバー攻撃に関連する多種多様かつ大量な情報を保有。
- これらの情報に基づく各種自動分析技術やセキュリティオペレーションの自動化・高精度化に向けて、AI技術を最大限に活用した研究開発を推進。

1. インシデントの優先順位判定

・アラートスクリーニング※
・脆弱性のインパクト分析

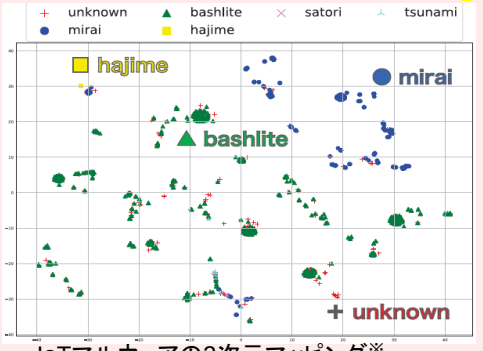


※各種警報を需要度等に応じて選別



2. マルウェア機能分析自動化

・Androidアプリおよびマーケット分析
・IoTマルウェア分析、自動分類
・マルウェア自動分析ツール化

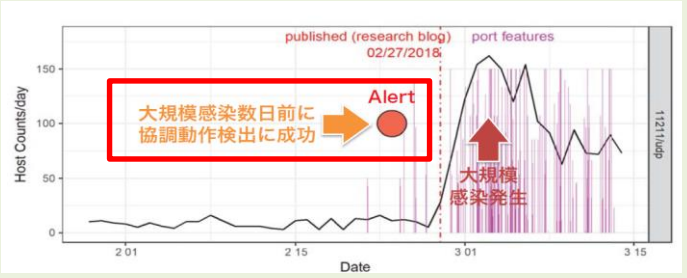


IoTマルウェアの2次元マッピング※

※あるマルウェアを捕獲したときに、Miraiなのかhajimeなのかといった情報がすぐに分かれば、その後のマルウェア解析を効率的に行うことが可能。その類似度を表している。

3. 攻撃の検知・脅威予測・予兆把握

・攻撃初期挙動検知
・ユーザトラフィックの異常検出
・脅威予測
・予兆検知
・影響度評価（攻撃インパクト分析）
・早期警戒情報の導出



設計・製造におけるチップの脆弱性検知手法の研究開発

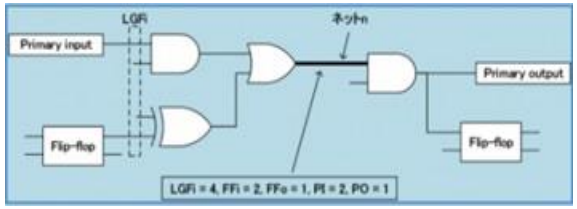
- 電子機器のハードウェア上に組み込まれた不正なチップは、製品出荷後に交換･修正することが難しく、その影響は極めて深刻になる可能性があることから、サプライチェーン上の脅威となっている。
- 総務省ではハードウェアチップの設計・製造における脆弱性検知手法に関する研究開発を実施中。

回路情報を用いて不正回路を検知する技術

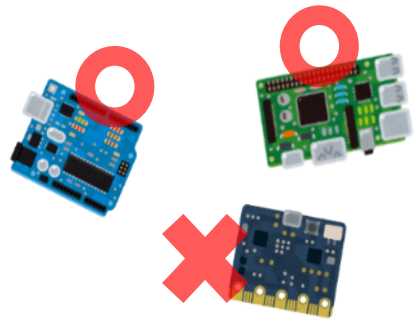
外部から調達した設計ツールや設計部品を用いたチップ設計全体の安全性を担保するために、回路情報の中に不正に改変された回路が含まれるか、機械学習等のAI を活用して検知する技術を確立

電子機器の外部から観測される情報を用いて不正動作を検知する技術

市販の組込みマイコン等の安全性を担保するために、不正回路が組み込まれたチップにより構成される電子機器に対し、電力波形の特定部分の電力量や継続時間等、電子機器の外部から観測される情報を用いて、不正動作を機械学習等のAI を活用して検知する技術を確立



AIにより不正回路を検出



AIにより不正動作を検出