資料３－１

サイバーセキュリティ研究開発等について

平成２８年１０月３１日

総務省　情報流通行政局

情報セキュリティ対策室

国立研究開発法人 情報通信研究機構（NICT）の概要

国立研究開発法人 情報通信研究機構 National Institute of Information and Communications Technology

※NICT：National Institute of Information and Communications Technology

●ICT分野を専門とする我が国唯一の公的研究機関

●役職員数：理事長　坂内正夫（前国立情報学研究所所長）
理事5名、監事2名、常勤職員　415名（H28.10.1現在）

●平成28年度 予算額：270.7億円
（平成27年度当初 予算額：274．4億円、補正 予算額： 23.0億円）

●所在地：本部　東京都小金井市
研究所等　神奈川県横須賀市、兵庫県神戸市、京都府相楽郡精華町、大阪府吹田市、宮城県仙台市
技術センター等　茨城県鹿嶋市、石川県能美市、沖縄県国頭郡恩納村　等

●主な業務：

・情報通信分野の研究開発
- 電波から光までの電磁波を利用し、突発的大気現象の早期補足や宇宙環境の計測を行う**センシング基盤分野**
- 無線や光などの通信技術により、社会のあらゆるものを繋ぐ次世代ネットワークを実現する**統合ICT基盤分野**
- 膨大な言語情報や人の脳情報をICTの観点から解析し、実社会に新たな価値を創造する**データ利活用基盤分野**
- AI技術を利用した次世代のサイバー攻撃分析技術でサイバー攻撃に対応する**サイバーセキュリティ分野**
- 量子情報技術や新規ICTデバイス開発で、既存社会基盤に新しい概念や枠組みを提供する**フロンティア研究分野**

・技術実証と社会実証の一体的推進が可能なテストベッド構築・運用

・産学／地域／グローバル連携等、幅広いネットワークを活用したオープンイノベーション創出に向けた取組

・日本標準時の維持/標準電波の送信、磁気圏の様子を観測予報する宇宙天気予報、
サイバーセキュリティに関する演習、無線機器の型式検定　など

・民間、大学等が行う情報通信分野の研究開発の支援　など

NICTのサイバーセキュリティ研究体制

2011年～ ＋ 2013年～

ネットワークセキュリティ研究所（NSRI）

サイバーセキュリティ研究室

世界最先端のサイバー攻撃観測・分析・対策・予防を実現する技術基盤を構築し、社会課題の解決に貢献

サイバー攻撃対策総合研究センター（CYREC）

サイバー防御戦術研究室

NICTERで培った基盤技術を用い、標的型攻撃等に対する根源的な防御戦術を立案・実現

サイバー攻撃検証研究室

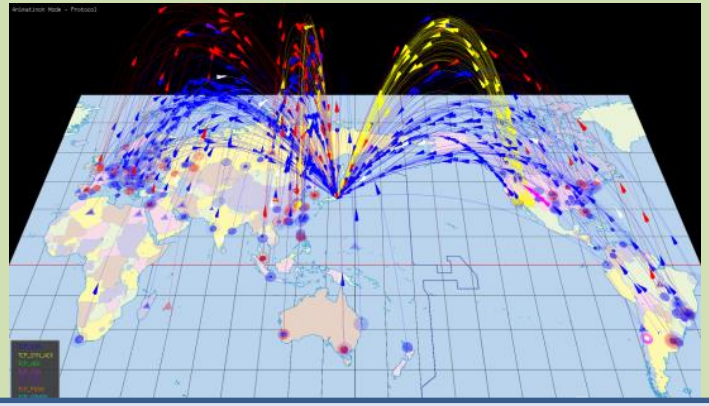
StarBEDで培ったエミュレーション技術を用い、セキュリティ実験環境を容易に構築・活用する技術を確立

情報通信研究機構（NICT）におけるサイバーセキュリティ技術の成果展開

■　国立研究開発法人　情報通信研究機構（NICT）では、研究開発の一環として、サイバーセキュリティ技術の成果展開を実施。無差別攻撃型（マルウェア）対策技術については、多くの自治体に導入が進むとともに、年金機構に対しても使用された標的型攻撃対策についても、早期導入に向けた取り組みを推進。

◆NICTER（ニクター）【無差別型攻撃対策】

- ダークネット（未使用IPアドレス）への通信をセンサーで観測することで、サイバー攻撃の地理的情報や攻撃量、攻撃手法等をリアルタイムに可視化。
- 本技術を応用して、地方公共団体情報システム機構（J-LIS）との協力により、マルウェアに感染した自治体へアラートを提供。



602自治体に導入済み（本年9月時点）

◆NIRVANA改（ニルヴァーナ・カイ）【標的型攻撃対策】

- NICTERの技術を応用し、組織内にセンサーを設置して組織内の通信状況をリアルタイムに可視化するとともに、本技術について2015年6月から技術移転開始。
- さらに、本技術と組み合わせ、ネットワーク内での異常検知時に通信を自動遮断する技術等を開発中。

技術移転を開始（昨年6月）

アドバンスト・サイバーセキュリティ技術

● より能動的・網羅的なサイバー攻撃観測技術の確立

- ✓ Passive（第2期）→Flexible（第3期）→Active（第4期）
- ✓ “目”の拡張（IoT機器用センサ、Smart Phone用センサ、Home Network用センサ　etc.）

● AI技術のサイバーセキュリティ応用

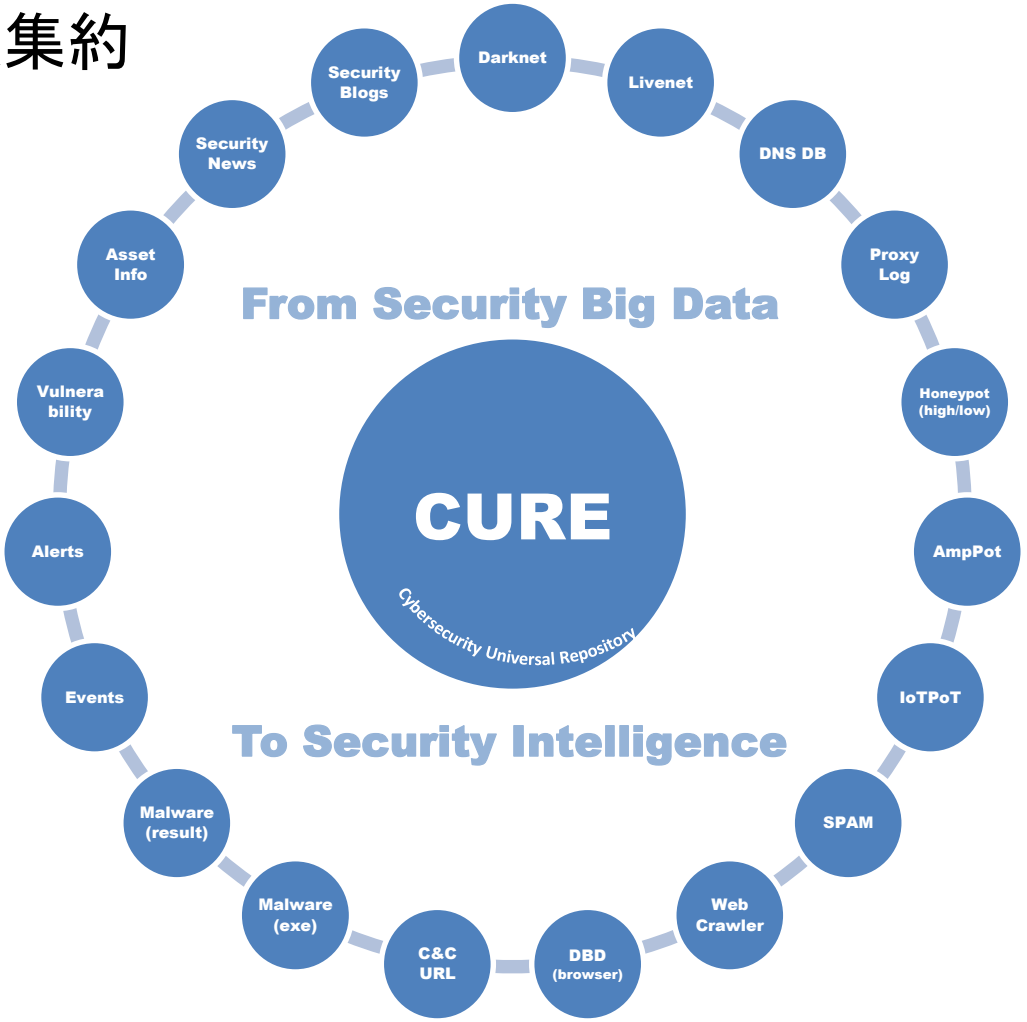
- ✓ 観測の自動化：予測型動的観測、AIクローリング　etc.
- ✓ 分析の自動化：マルチモーダル自動分析、学習型マルウェア自動分析　etc.
- ✓ 必要なブレークスルー
  - リアルタイム性（現状：高次元の特徴量を扱うリアルタイム分析は不可）
  - 教師あり学習から教師なし学習へ（現状：要教師データ、未知の攻撃検知は不可）
  - チューニング問題の克服（現状：組織ごとの精緻なカスタムチューニングが必須）
  - 原因への遡及（現状：機械は攻撃検知の原因を表現不可）

● 可視化ドリブンなセキュリティオペレーションの確立

- ✓ 第2期：サイバー攻撃を可視化
- ✓ 第3期：アラートを可視化
- ✓ 第4期：可視化エンジンでオペレーションを完結
  - UIのユーザビリティ向上
  - 検索、フィルタ機能の強化
  - セキュリティ機器との連携強化
  - マルチプラットフォーム化（WebGL化）　etc.

サイバーセキュリティ・ユニバーサル・リポジトリ技術

- セキュリティ関連情報を大規模集約
  - ✓ 各種観測情報
  - ✓ マルウェア検体/解析結果
  - ✓ セキュリティ機器のアラート情報
  - ✓ 脆弱性情報、資産情報
  - ✓ セキュリティNews/Blog etc…
- マッシュアップと自動対策
  - ✓ 複数情報源の紐付け
  - ✓ 攻撃キャンペーンの解明
  - ✓ 組織やユーザへの自動対策展開
- セミ・オープン研究基盤
  - ✓ CURE格納情報の外部研究利用
  - ✓ 機微情報への階層的アクセス制御
  - ✓ CUREを核にしたAll Japan体制のサイバーセキュリティ研究基盤創立



サイバーセキュリティに関する研究開発の推進

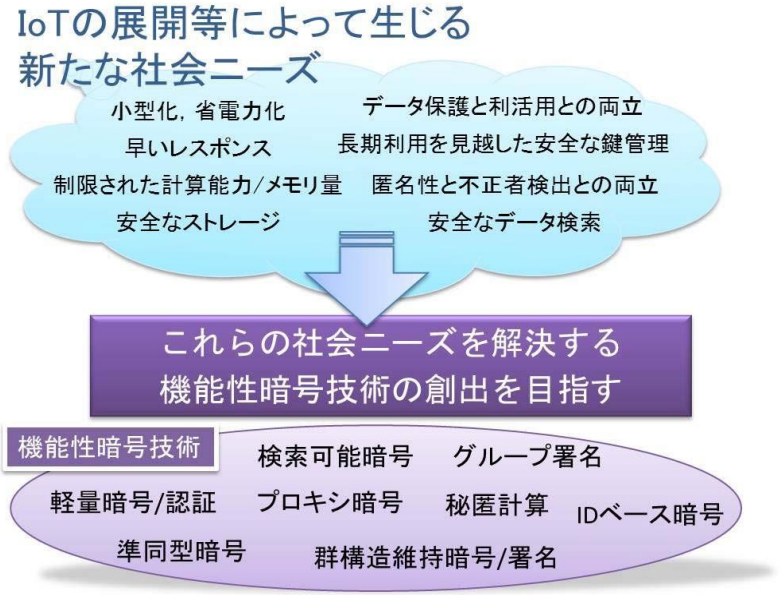
IoT時代に向けた研究開発の推進

様々なモノが通信ネットワークに接続されるIoT時代においては、小規模なセンサーをはじめとする、電子回路の規模や消費電力に制限があり単体ではサイバー攻撃に対して十分な防御手段を持たない機器を防御するための技術が必要となる。

［総務省事業（平成28年度第2次補正予算）］

IoT機器に実装可能な軽量な暗号・認証技術の開発等

IoTの展開に伴って生じる新たな社会ニーズに対応するため、新たな機能を備えた機能性暗号や軽量暗号・認証技術の研究開発に取り組む



IoT時代におけるサイバーセキュリティ総合対策実証事業

IoT機器とインターネットの境界上にセキュアなゲートウェイを設置し、低機能なIoT機器の セキュリティを確保するための取組