# セキュリティ情報の自給に向けた サイバーセキュリティ知的基盤構想

井上 大介
国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所
サイバーセキュリティ研究室

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

# サイバーセキュリティ自給率の低迷

## ● サイバーセキュリティ研究・技術開発取組方針

サイバーセキュリティ戦略本部 研究開発戦略専門調査会（2019年5月17日）

**３．取り組むべき課題**
**(2) サイバーセキュリティ自給率の低迷**

我が国のベンダー企業においては、**海外のセキュリティ技術を導入・運用する形態が主流**となっている。このようなビジネスモデルは、**研究開発投資を抑え**、事業上のリスクを極小化することができる一方で、利益率が低く、また、**コア技術に係るノウハウ・知見を蓄積することが難しい**側面がある。（P5）

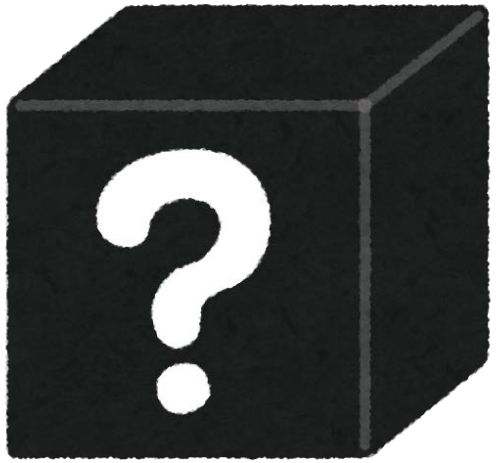
我が国企業の国際競争力強化はむろんのこと、政府機関や重要インフラ事業者等のサービスを支える**セキュリティ技術が過度に海外に依存する状況を回避・脱却**する観点から、コア技術の開発・運用を中心に、国産技術・産業の育成を進めていくことが重要である。（P6）

## ● 実際、日本のセキュリティ自給率はどのくらい？

- ✓ 具体的な自給率の算出は容易ではない（そのような調査結果は見たことがない）
- ✓ **体感では自給率10%を切っているのでは？**（国産で思いつく製品名は…？）

# なぜ国産セキュリティ製品は少ないのか？

- **日本の失われた20年でセキュリティのR&Dは後回し**
  - ✓ バズワード駆動の研究開発（マルチメディア、ユビキタス、クラウド、ビッグデータ、AI、etc. etc... ）
  - ✓ 「セキュリティはお金にならない」を信じたトップマネジメント層



- **海外では着々と研究開発➡製品の普及**
  - ✓ 製品（＝センサ）を世界中に展開し大規模観測網を構築
  - ✓ 観測したデータが次の研究開発を進める正のスパイラル

- **国内ではブラックボックスSIerの台頭**
  - ✓ ブラックボックスの海外製品を組織の入り口に設置する『壺ビジネス』
  - ✓ 技術詳細は「製造元に確認」➡（数週間後）➡「技術のコアのため開示不可」

➡ **国内にコア技術が育たず、データも集積せず**

# データ負けのスパイラル

- **国内業界はデータ負けのスパイラル**
  1. 国産のセキュリティ技術が普及しない
  2. サイバー攻撃の実データが集まらない
  3. 実データを使った研究開発ができない
  4. 良い国産セキュリティ技術を作れない

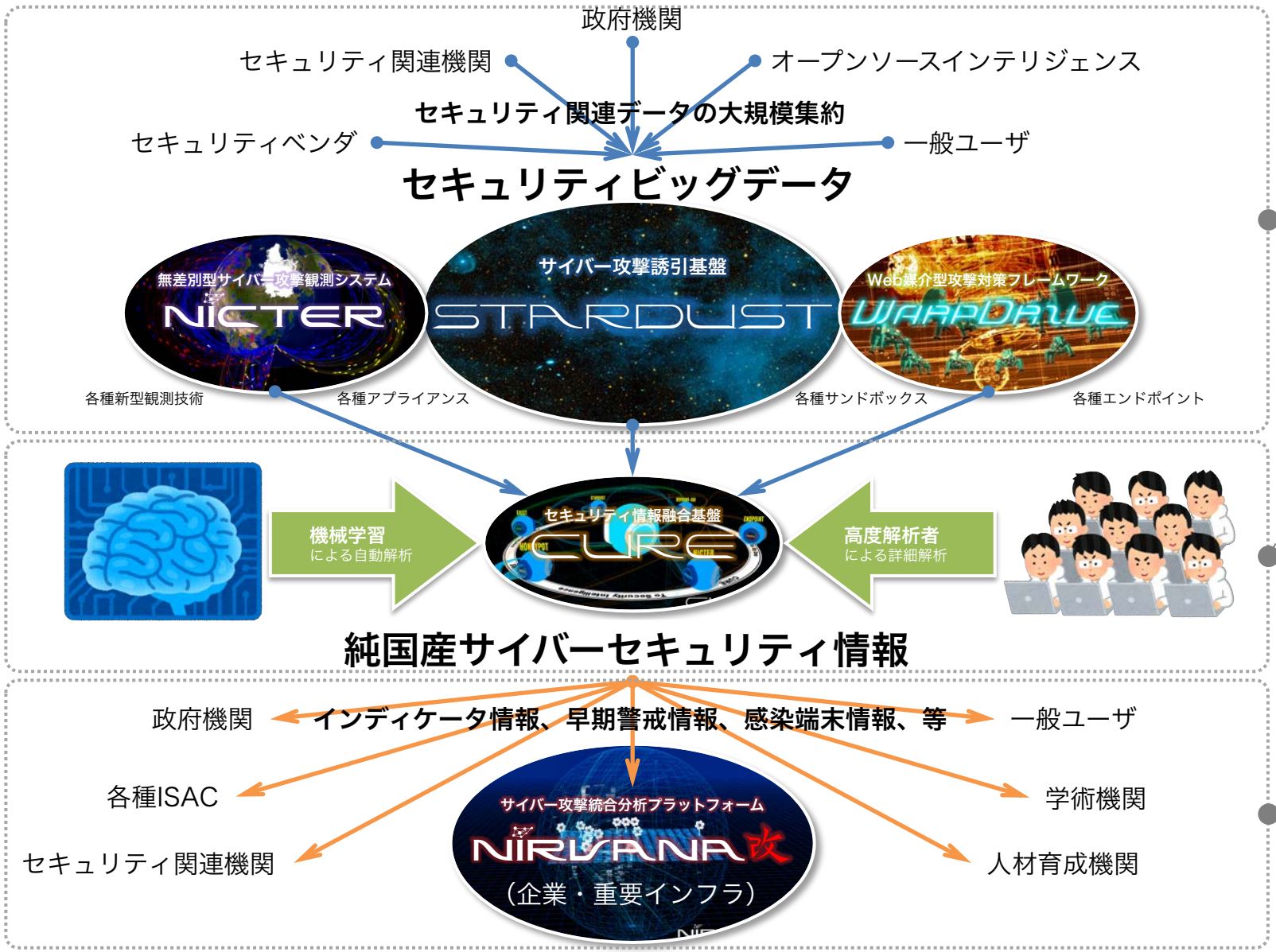
- **高騰するサイバーセキュリティ情報**
  - ✓ 国内のデータが海外に流れ、海外で分析
  - ✓ 海外で生成された脅威情報を高額で購入


➡ **国内でサイバーセキュリティ情報を生成・蓄積・提供できる環境が必要**

# 今、日本として何が必要か？

- **実データを大規模に集約・蓄積する仕組み**
  - ✓産官学が連携し各種観測情報やOSINTを大規模集約・蓄積
- **実データを定常的・組織的に分析する仕組み**
  - ✓高度解析者の結集・育成と機械学習技術の適用による定常分析
- **実データで国産製品を運用・検証する仕組み**
  - ✓国産製品のプロトタイプ群を長期運用・機能検証できる環境
- **実データから脅威情報を生成・共有する仕組み**
  - ✓国産IoCを生成しActionable Informationを国内で共有

# サイバーセキュリティ知的基盤構想




## 大規模収集・蓄積

- 産学官から情報集約
- OSINTの大規模収集
- NICTの研究成果を活用
  - ➡ NICTER, STARDUST, WarpDrive

## 定常的・組織的分析

- 高度解析者の結集・育成
- 機械学習技術の定常運用
- NICTの研究成果を活用
  - ➡ CURE, AI x Cybersecurity

## 国産製品運用・検証

- 国産製品のプロトを長期運用
- NICTのLANをテストベッド化
- 海外製品群との比較検証

## 脅威情報生成・共有

- 高度解析者によるIoC生成
- 産学官への共有
- NICTの研究成果を活用
  - ➡ NIRVANA改

# サイバーセキュリティ知的基盤を活用した各種活動内容

## 1. STARDUSTのセミオープン化と大規模並列化

✓ STARDUSTを民間企業、学術機関等に開放し、大規模並列解析

## 2. 国産セキュリティ製品の運用・検証

✓ NICTのLANをテストベッドとして国産製品を長期運用・機能検証

## 3. 高度SOC人材育成

✓ 産学官から高度解析者を集結し、SOC人材育成プログラム構築

## 4. 純国産サイバーセキュリティ情報の生成

✓ 各種観測網等のデータを機械学習等を駆使して統合分析

✓ 説明可能（explainable）かつ即時的な純国産IoCを生成・発信

## 5. 国内解析者コミュニティの醸成

✓ データの共同分析・情報共有を通して国内解析者コミュニティを醸成

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response