資料2

# 我が国のサイバーセキュリティ研究開発力の強化に向けて

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
盛合 志帆

NICT National Institute of Information and Communications Technology

# 背景：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？**

# データ負けのスパイラル

- **国内業界は<u>データ負け</u>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


➡ **<u>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</u>**

# データ負けのスパイラルからの脱却に向けて

- 今、日本に必要なこと
  - ✓ 実データを大規模に収集・蓄積する仕組み
  - ✓ 実データを定常的・組織的に分析する仕組み
  - ✓ 実データで国産製品を運用・検証する仕組み
  - ✓ 実データから脅威情報を生成・共有する仕組み
  - ✓ 実データによる人材育成をオープン化する仕組み


これらの仕組みの実現を目指す
**産学官の結節点**を構築

# CYNEX：サイバーセキュリティ統合知的・人材育成基盤

●サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、社会全体で
サイバーセキュリティ人材を育成するための共通基盤を構築し、産学官の結節点として開放

# 4つのサブチーム “Co-Nexus” によるプロジェクト推進


**A** **Co-Nexus A** (Accumulation & Analysis)
- ✓各種観測機構によるデータ収集・蓄積
- ✓解析者コミュニティ醸成と共同分析の実現

**S** **Co-Nexus S** (Security Operation & Sharing)
- ✓高度SOC人材育成（Online自主学習＆OJT）
- ✓国産脅威情報の生成・提供

**E** **Co-Nexus E** (Evaluation)
- ✓国産セキュリティ製品の長期運用・検証
- ✓国産セキュリティ製品へのフィードバック

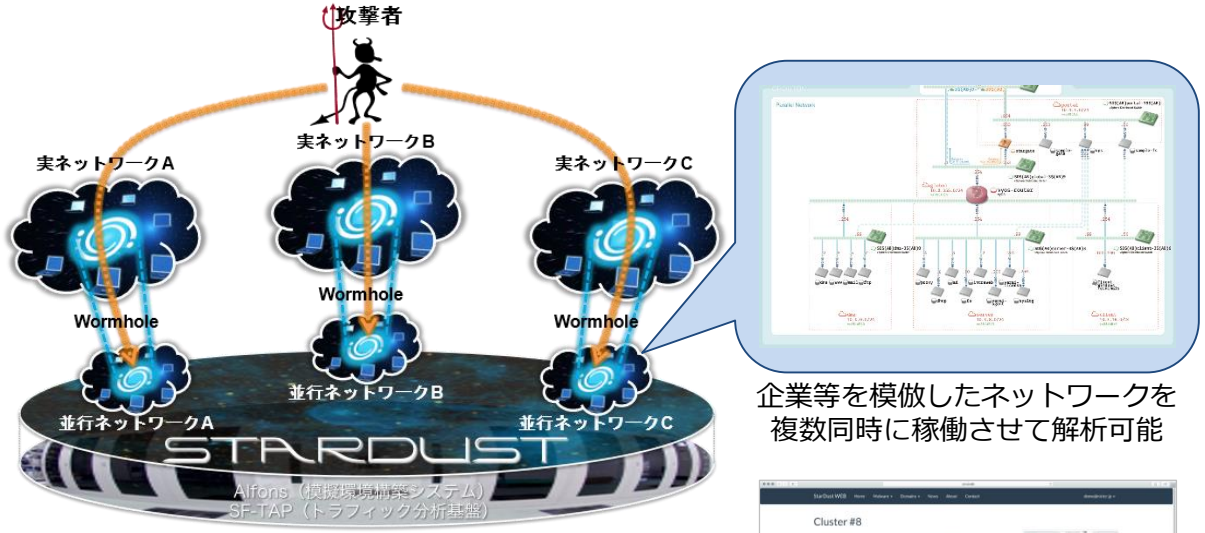
**C** **Co-Nexus C** (CYROP*)
- ✓人材育成基盤のオープン化
- ✓パイロットコンテンツ開発

*CYROP: CYDERANGE as an Open Platform

# Co-Nexus A：STARDUST＆解析者コミュニティ形成

## ●背景：STARDUST

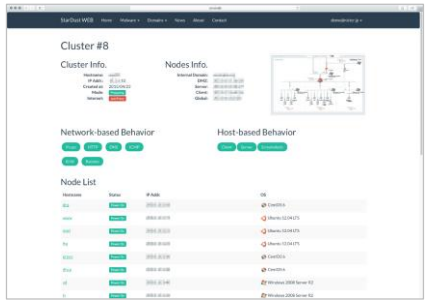
- ✓ 標的型攻撃等の攻撃者を誘い込む**サイバー攻撃誘引基盤**
- ✓ 組織を精巧に模擬した**並行ネットワーク**を高速・柔軟に自動生成
- ✓ 並行ネットワーク中で攻撃者を長期誘引し**ステルスに挙動を解析**




CYNEX専用STARDUST建造中



企業等を模倣したネットワークを
複数同時に稼働させて解析可能




STARDUST Web経由の遠隔解析

## ● STARDUSTの活用と解析能力向上

- ✓ 参画組織ごとに高度化/カスタマイズされた**並行ネットワークを貸し出し**
- ✓ 日常的・定期的な解析情報の共有を通した**解析者コミュニティの形成**
- ✓ **All Japanでの共同解析**を実現する大規模並行ネットワークの構築

# Co-Nexus A：WarpDriveプロジェクトの継承と進化

## ●背景：WarpDrive

- ✓ **Web媒介型攻撃の実態把握と対策確立**に向けたユーザ参加型プロジェクト
- ✓ Windows/Mac/Android版**タチコマ・セキュリティ・エージェント**配布中
- ✓ ユーザのWebアクセスを大規模観測し、**悪性サイトを発見/警告/ブロック**

Windows/Mac版タチコマSA　　Android版タチコマSAモバイル


WarpDriveポータルサイト
https://warpdrive-project.jp/

## ● WarpDriveの継承と進化

- ✓ 委託研究WarpDriveプロジェクトの**CYNEXへの完全移管を完了**
- ✓ さらなる参画ユーザ獲得に向けた**タチコマSAの大型アップデートPJ進行中**
- ✓ **WarpDrive観測情報の大規模解析**と解析者コミュニティへの情報展開

# Co-Nexus S：高度SOC人材育成と国産脅威情報発信

## ●背景：NICTER解析チーム

- ✓ 解析者集団によるダークネット/ライブネット分析
- ✓ **NICT-CSIRT**の片翼として機構内インシデント対応
- ✓ 研究開発成果の1stディプロイメント（SecDevOps）

NICTERオペレーションルーム


自主学習型
高度SOC研修

OJTでのSOC業務従事

国産脅威情報発信

## ● 情報発信力の強化 NEW
## 「NICTER観測レポート2021」の公開 (2022.2.10)

## ● 高度SOC人材育成と情報発信

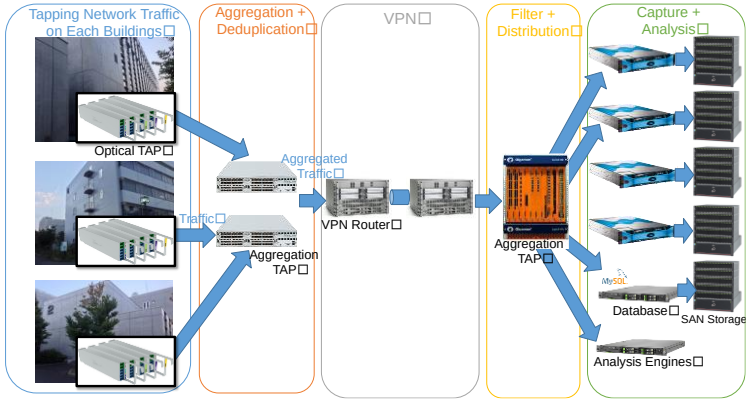
- ✓ **オンライン自主学習型高度SOC研修**と**NICTER解析チーム内でのOJT**
- ✓ 多数の海外製品/最先端研究成果を融合した**次世代セキュリティオペレーション体験**
- ✓ **ヒトとマシンによる国産脅威情報の生成**（高度SOC人材 × 各種機械学習エンジン）とCYNEX内外での情報共有/発信

CYNEX

# Co-Nexus E：国産セキュリティ製品の運用・検証

## ●背景：NICT内部ネットワーク観測システム

- ✓ 機構内**通信をリアルタイムにキャプチャ**
- ✓ 機構内**業務用PC数百台にエージェント導入**
- ✓ **海外有力セキュリティ製品を複数機種並行稼働**




NICT内部ネットワーク観測システム


富士通 標的型攻撃発見サービス


AlaxalA AX-3D-View

NICTにおける製品運用・検証の先行事例

## ● 国産セキュリティ製品運用・検証

- ✓ **参画組織からの製品プロトタイプ持込**と NICT-CSIRTでの長期運用
- ✓ **CYNEX Red Team による模擬攻撃と** 実攻撃を併用したセキュリティ機能検証
- ✓ 運用・検証結果のレポーティングによる **参画組織へのフィードバック**

# Co-Nexus C：人材育成オープンプラットフォーム

## ●背景：セキュリティ人材育成

- ✓ ナショナルサイバートレーニングセンターでのノウハウの蓄積
- ✓ 国や地方公共団体等を対象とするサイバー防御演習：**CYDER**
- ✓ 東京2020大会向け実践的サイバー演習：**サイバーコロッセオ**

実践的サイバー防御演習
CYDER
Cyber Defense Exercise with Recurrence

オリパラ関係者向けサイバー演習
cyber colosseo

## ● サイバーセキュリティ演習基盤CYROPのオープン化トライアルを開始 ～国内のセキュリティ人材育成事業促進に向けて～ (2022.2.3)

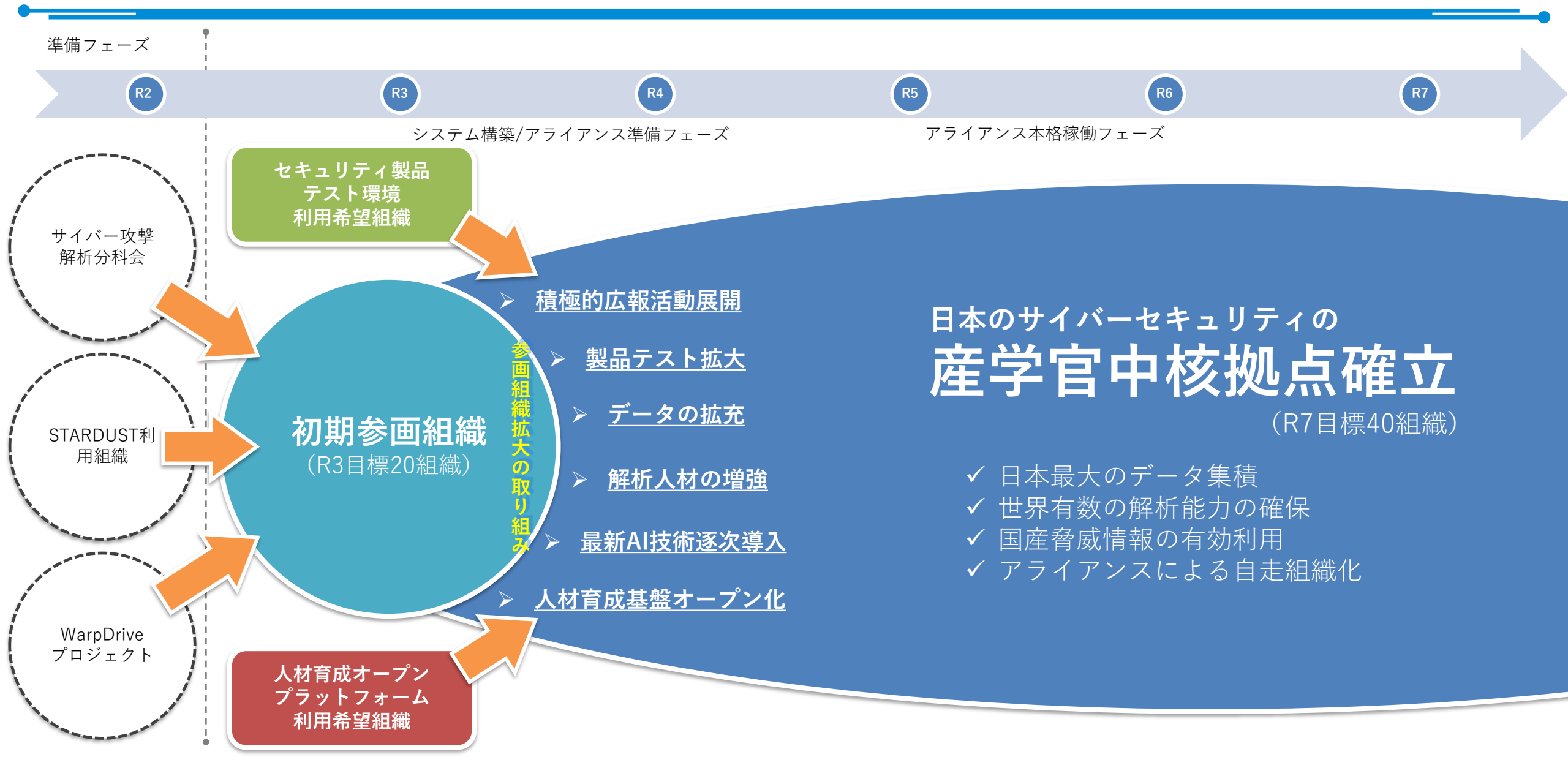
NEW

今回のオープン化の最初のトライアルとして、2022年2月8日から (株)日立ソリューションズ・クリエイトにおいて、CYROPを利用したサイバーセキュリティトレーニングサービスを申込受付開始

## ● 人材育成オープンプラットフォーム

- ✓ **人材育成基盤のオープン化**による国内セキュリティ人材育成事業の活性化
- ✓ 教育機関向け人材育成教材など**新規パイロットコンテンツの共同開発**
- ✓ Co-Nexus A/S/Eからのフィードバックによる**サイバー演習の継続的な最新化**

# CYNEXのタイムライン



# 我が国のサイバーセキュリティ研究開発力の強化に向けて

- 国として保持すべきサイバーセキュリティ研究開発課題（経済安全保障の観点からも）
  - ✓実データの観測・分析に基づく研究は極めて重要。（サイバーセキュリティでもAIの社会実装でも）
  - ✓半導体供給不足を受け、ハードウェアからファームウェアまでのローレイヤー(セキュリティ)を海外依存する危険性を改めて認識。サプライチェーンセキュリティにも直結。
  - ✓暗号技術はコモディティ化しつつあるが、耐量子計算機暗号を含めた次世代暗号技術導入が海外依存とならないよう、研究開発・実装の人材育成が急務。
  - ✓組織横断でのデータ利活用を促進するプライバシー保護データ解析技術は引き続き強化。(次期AI戦略でも議論)
  - ✓１組織で取り組むのが難しい課題が多く、産学官連携がますます重要に。

「サイバーセキュリティ研究・産学官連携戦略WG最終報告」(2021/3/23)でも同様の指摘あり

# 我が国のサイバーセキュリティ研究開発力の強化に向けて (続き)

- 研究開発人材の確保・育成の重要性
  - ✓ 研究技術職離れ（若手研究職の不安定な雇用　e.g., 任期付採用）
  - ✓ 組織としては腹を括って採用し、責任をもって育成
  - ✓ 中長期的視点で研究開発に取り組める公的研究機関が担う役割は大きい
  - ✓ 国としてもっと研究開発人材に投資を！（科学技術立国の復権）