産・学・官、それぞれの未来

CYNEX Allianceの共創から見えてきたこと

サイバーセキュリティ研究所 サイバーセキュリティネクサス
CYNEX研究開発運用室長 安田 真悟

CYNEX
CYBERSECURITY NEXUS

NICT 国立研究開発法人 情報通信研究機構

CYNEX Allianceとは

発足理由と価値をもう一度紐解いて考える

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？**（国産で思いつく製品名は…？）

つまり…
官の危機感による産・学の立て直し

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**

結果の因果関係説明にすぎない

解決の為の提案がなぜ

NICTを中心としたアライアンス

なのか

産学官連携とは

＝ 産学官連携の目的 ＝

同じ目的に向けて、役割と成果物の受け渡しを設計すること

“良い成果”の定義、“時間軸”が異なるので足並み（回転数）が揃わない

官

- 目的：社会的要請に基づく課題解決
- 強み：公共目的を定義し、全体を動かす力
  - 制度設計・予算配分による方向性決定
- 制約：手続と合意形成に時間が必要
  - 透明性と正当性が求められる
  - 現場の速度に合わせた試行錯誤が困難

産

- 目的：市場で勝つ、早く回収する
- 強み：意思決定（リソース投下）と実装力
  - 市場を取り込み、プロダクトとして実現
- 制約：採算と競争が前提
  - 投資にはリターン、長期的な取組は苦手
  - 共有は優位性リスク、中立的になれない

学

- 目的：新規性、再現性のある研究と教育
- 強み：独立性が高く本質を時間をかけて研究
  - 短期成果に縛られず普遍的な知を追究
- 制約：現場接続と組織力に課題
  - 実データや現場へのアクセスが限定的
  - 研究は人に依存、体制の継続が困難

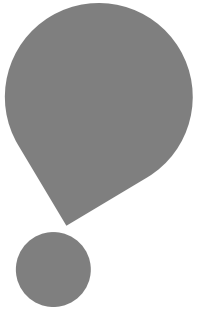
国立研究開発法人とは　3【産学官】＋1【研】

研

- 目的：基礎研究と政策に基づく応用
- 強み：産学官の補完的性質を併せ持つ
  - 採算に縛られず“空白領域”に投資可能
  - 制度を“技術で成立させる”事が可能
  - 持続的な体制構築が可能
- 制約：人手が足りない（笑）

三段歯車

NICT の強み



足並み（回転数）を揃えられる

CYNEX CYBERSECURITY NEXUS

This is

CYNEX

CYBERSECURITY NEXUS

Alliance

CYNEX Allianceと４つの Co-Nexus

CYBERSECURITY Laboratory

研究開発成果

サイバーセキュリティ研究室

人材育成ノウハウ

ナショナルサイバー
トレーニングセンター

National Cyber Training Center

Co-Nexus A

- サイバーセキュリティ情報の大規模収集
- 定常的分析と国内解析者コミュニティ形成

Co-Nexus S

- 高度SOC人材育成
  (Online 自主学習&OJT)
- 説明可能な国産脅威情報の生成･提供

Co-Nexus E

- 国産セキュリティ技術の長期運用･検証
- 国産セキュリティ製品へのフィードバック

Co-Nexus C

- 人材育成基盤のオープン化による事業促進
- オリジナル演習コンテンツの開発

CYNEX
CYBERSECURITY NEXUS
Alliance
アライアンス

民間企業
官公庁

共同解析、育成人材投入、人材育成基盤の
商用利用、製品プロトタイプ導入などの支援

教育機関

共同解析、育成人材投入、
人材育成基盤利用などの支援

CYNEX Allianceと４つの Co-Nexus

CYBERSECURITY Laboratory

研究開発成果

サイバーセキュリティ研究室

人材育成ノウハウ

ナショナルサイバー
トレーニングセンター

National Cyber Training Center

Co-Nexus A

コミュニティ
実データを集め人と繋ぐ

Co-Nexus S

実データを使う人を育てる

Co-Nexus E

実データを使って試す

Co-Nexus C

人材育成の裾野を広げる

集める➡使う➡試す➡広げる

4つのCo-Nexusで循環を作る

CYNEX CYBERSECURITY NEXUS

４つの Co-Nexusの体制

CYBERSECURITY Laboratory

研究開発成果

サイバーセキュリティ研究室

田辺 瑠偉　吉岡 克成　山内 利宏

順天堂大学　横浜国立大学　岡山大学

WARPDRIVE

安田 真悟

Co-Nexus A

- サイバーセキュリティ情報の大規模収集
- 定常的分析と国内解析者コミュニティ形成

参画組織数：45

毛利 公一
立命館大学

佐藤 隆行
日立製作所

Co-Nexus E

- 国産セキュリティ技術の長期運用･検証
- 国産セキュリティ製品へのフィードバック

参画組織数：7

安部 小百合

Walküre
CYNEX Red Team

CYNEX
CYBERSECURITY NEXUS

Alliance
アライアンス

108組織
参画中

民間企業
官公庁

教育機関

共同解析、育成人材投入、人材育成基盤の
商用利用、製品プロトタイプ導入などの支援

人材育成ノウハウ

ナショナルサイバー
トレーニングセンター

National Cyber Training Center

Co-Nexus S

- 高度SOC人材育成
  (Online 自主学習&OJT)
- 説明可能な国産脅威情報の生成･提供

参画組織数：17

久保 正樹

piyokango
セキュリティインコ

Co-Nexus C

- 人材育成基盤のオープン化による事業促進
- オリジナル演習コンテンツの開発

参画組織数：86

佐藤 公信

角田 玄司
ネットワン
システムズ

和山 正人
一関高専

共同解析、育成人材投入、
人材育成基盤利用などの支援

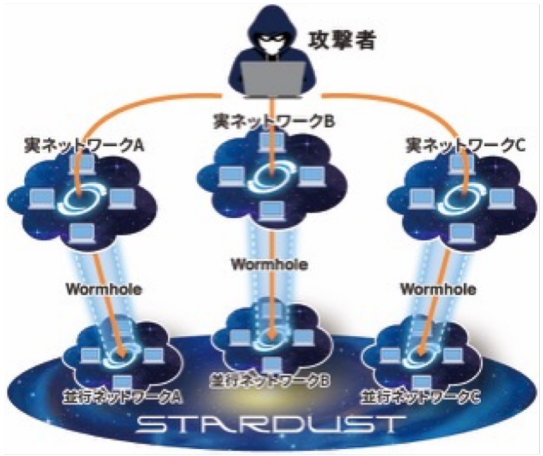
CYNEX CYBERSECURITY NEXUS

Co-Nexus A【実データを人と繋ぐ】

●研究開発成果活用と実データの協創

WarpDrive

CURE Web



サイバー攻撃誘引基盤
STARDUST NxtGen

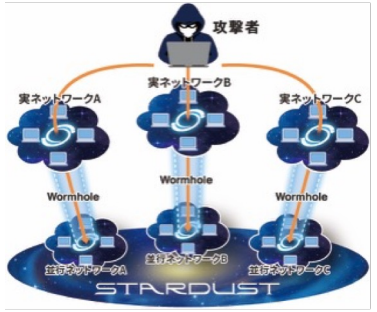
• 解析者コミュニティ形成

CYNEX CYBERSECURITY NEXUS

Co-Nexus Aの活動【実データを人と繋ぐ】

●研究開発成果活用と実データの協創

- 【基盤貸与】STARDUST
  - 標的型攻撃を中心としたサイバー攻撃の分析基盤を提供
    - 実績：33組織に貸与中
- 【基盤貸与】STARGAZER［NEW］
  - マルウェア検体分析、ネットワークIoC情報監視【日本版VTの原型へ】
    - 実績：2026年度貸与開始予定
- 【情報共有】CURE
  - CSL/CYNEX等のNICTが収集した情報の提供基盤
    - 実績：31組織に貸与中
- 【基盤貸与】【情報共有】WarpDrive
  - Webアクセス、ユーザー端末の脅威に関わる情報を収集共有
  - アクセス遷移の復元など汎用的な一次解析支援機能を提供
    - 実績：20組織に貸与中
      700万URL/日の大規模データの共有



サイバー攻撃誘引基盤
STARDUST NxtGen


CURE Web


タチコマSA

CYNEX CYBERSECURITY NEXUS

Co-Nexus Aの活動【実データを人と繋ぐ】

●解析者コミュニティ形成

- 【情報共有】Co-Nexus A 解析者コミュニティ
  - 解析結果、解析ノウハウの共有と信頼関係の醸成
    - 実績：年4回のCo-Nexus A会合（参加者 100名規模）
- 【情報共有】WarDrive コミュニティ
  - 研究(論文)成果、ノウハウの共有、共同研究
    - 実績：WarpDrive Workshop（参加者 40名規模）
- 【知見共有】【情報共有】LETTICE
  - 参画組織の解析者でチームを構成し共同分析
    - 実績：パリ五輪 / 大阪万博に関連するサイバー攻撃を分析・公開

Co-Nexus A会合

```
① attrib +h +s "C:¥Users¥ ¥(ユーザ名)¥ ¥AppData¥Local¥Temp¥wDYCOB82zjvY.exe"
② powershell -Command Add-MpPreference -ExclusionPath 'C:¥Users¥(ユーザ名)¥AppData¥Local¥Temp¥wDYCOB82zjvY.exe'
③ powershell Set-MpPreference -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -
DisableRealtimeMonitoring $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -
EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend && powershell
Set-MpPreference -SubmitSamplesConsent 2 & "%%ProgramFiles%%¥Windows Defender¥MpCmdRun.exe" -
RemoveDefinitions -All
```

共有事例：三次検体(QuasarRAT)が実行したコマンド

Co-Nexus A会合 共有事例(一部)	QuasarRATの観測	大阪関西万博編脅威調査 LETTICE
	Phantom Stealerの解析	パリ五輪におけるサイバー攻撃の調査 LETTICE
	STARDUSTを用いたDDoS攻撃の観測	日本国内のDVR機器を狙うボットネットの解析

Co-Nexus Aの活動【実データを人と繋ぐ】

●対外的情報発信

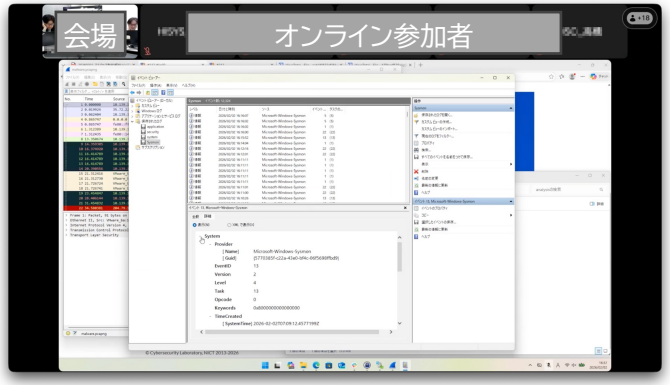
- 【情報共有】解析情報公開
  - STARDUST 解析Blog 公開
    - 実績:これまで4本
- 【情報共有】その他調査報告等
  - ホワイトペーパー
    - 実績:1件(2/13公開予定)【NEW】

Co-Nexus A 解析Blog 記事一覧	
2026/01/28	STARDUSTを用いたAsyncRATの解析
2025/09/17	STARDUSTを用いたLazarus Groupの攻撃の解析
2025/07/18	STARDUSTを用いたRemcosの解析
2025/07/17	STARDUSTを用いたCrySISの解析

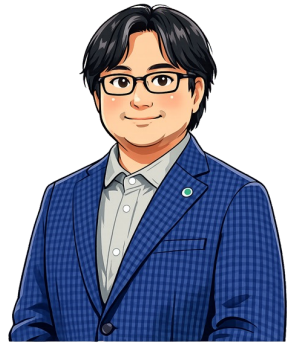
https://cynex.nict.go.jp/library/2504_report_blogs.html

●様々な活動支援活性化策

- 【知見共有】【共同作業】CTFチャレンジ部
  - 国内外のCTFに有志で挑戦
- 【活動支援】STARDUST講習会
  - ハンズオン形式講習による利用支援



STARDUST講習会(オンライン)



CTFチャレンジ部 技術顧問
日立製作所 鬼頭 哲郎 氏
Tetsuro Kito
SANS NetWars 最高位1位の実績

Co-Nexus S【実データを使う人を育てる】

●国産脅威情報提供

- 【情報共有】CSL/CYNEX等のNICTが収集した生データの提供
  - 実績:ダークネットデータを中心に生データを5組織に提供中
  - Alliance Slackへの脅威情報提供(週2回程度 @a_sec_topic)

データ利用事例
横国:am I infected

●高度SOC人材育成

- 【人材育成】オンラインコース / OJTコース
  - オンラインコース 年間最大40名程度 / OJTコース　最大6名程度
  - 実績:オンラインコース 延べ81名修了 / OJTコース 延べ9名修了

CYNEX解析チームでのOJTの様子

●対外的情報発信

- 【情報共有】NICTER 観測レポート/Blog/X

Co-Nexus E【実データを使って試す】

●国産製品・技術の検証

- 【製品評価】参画組織の研究開発技術・製品の長期検証
  - 実績：9製品・技術（7社）の検証・評価を平均200日/年以上実施
- 【基盤貸与】技術検証環境の提供
  - 実績：1社（IoT機器ファジング環境提供）
- 【製品認証】製品カテゴリごとの機能認証【NEW】
  - WAF製品の性能認証

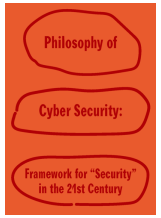
国産セキュリティ製品検証リスト

製品種別	製品フェーズ	運用・検証の概要
ファジングツール	商用化前技術	アルゴリズムの精度検証
IPレピュテーションサービス	商用化済技術	運用されている製品の精度検証新たな分析軸の検証
マルウェア対策ソフト	商用化済技術	新たなマルウェア、亜種への適応検証
機密情報保護ソリューション	商用化済技術	各種情報持ちだし手法の抑止効果の検証
セキュリティ対策SDK	商用化済技術	SDKによる取得ログのセキュリティ対策有効性検証
WAF製品	商用化済技術	2製品目のWAF製品として検証

Co-Nexus C【人材育成の裾野を広げる】

- 国内セキュリティ人材育成事業活性化
  - 【人材育成】【情報共有】標準的サイバーセキュリティ人材育成教材の開発
    - 実績：**提供可能**コンテンツは90種類(NICE Framework KSAカバー率50%以上)
    - 実績：重要インフラ・基幹インフラ向け教材の開発・提供【NEW】
    - 高度人材育成基盤の開発中【NEW】
  - 【人材育成】【基盤貸与】サイバー演習基盤開放
    - 参画組織の社内研修・演習講義・商用演習への活用
    - 実績：R6年度85種類の演習実施（受講者数2,698）
    - 講師育成：CYROP認定講師制度（講習＋認定）開始【NEW】
    - ASEAN（AJCCBC）への演習提供【NEW】
- 対外的情報発信
  - 【情報共有】各種調査報告等
    - 実績：CYNEX新書 2件公表

教育機関での演習教材利用事例

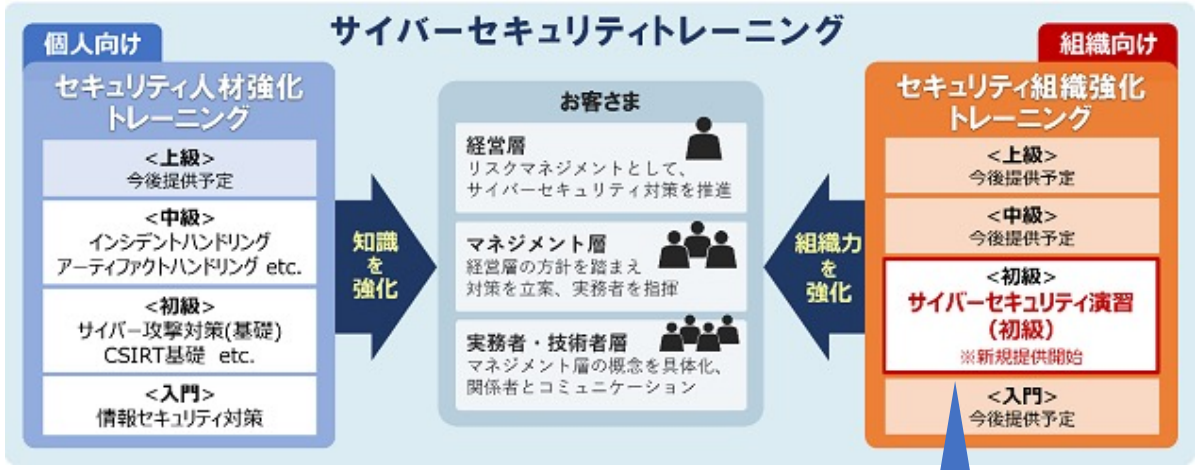


「サイバーセキュリティの哲学」「サイバーセキュリティと民主主義」

商用利用事例(一部)

i-Learning様
「ネットワークセキュリティ対策」

日立ソリューションズクリエイト様
サイバーセキュリティ演習<初級>



自社教材にCYROPを加えてラインアップ強化

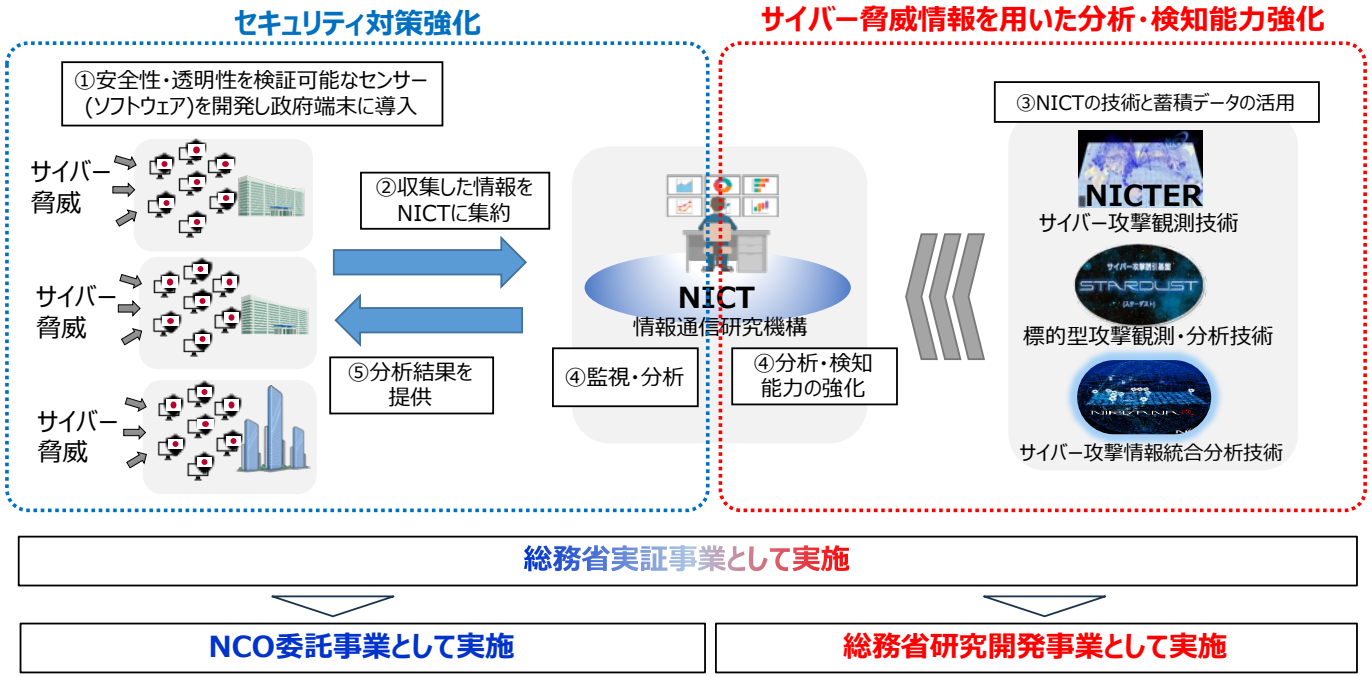
その他:トレノケート様、SAJ様、NEC様など

サイバーセキュリティ情報の収集・分析に係る実証事業

- 安全性や透明性の検証が可能なセンサーをCYNEXで研究開発
  - 政府端末に導入し、得られた情報等を横断的に分析し情報提供

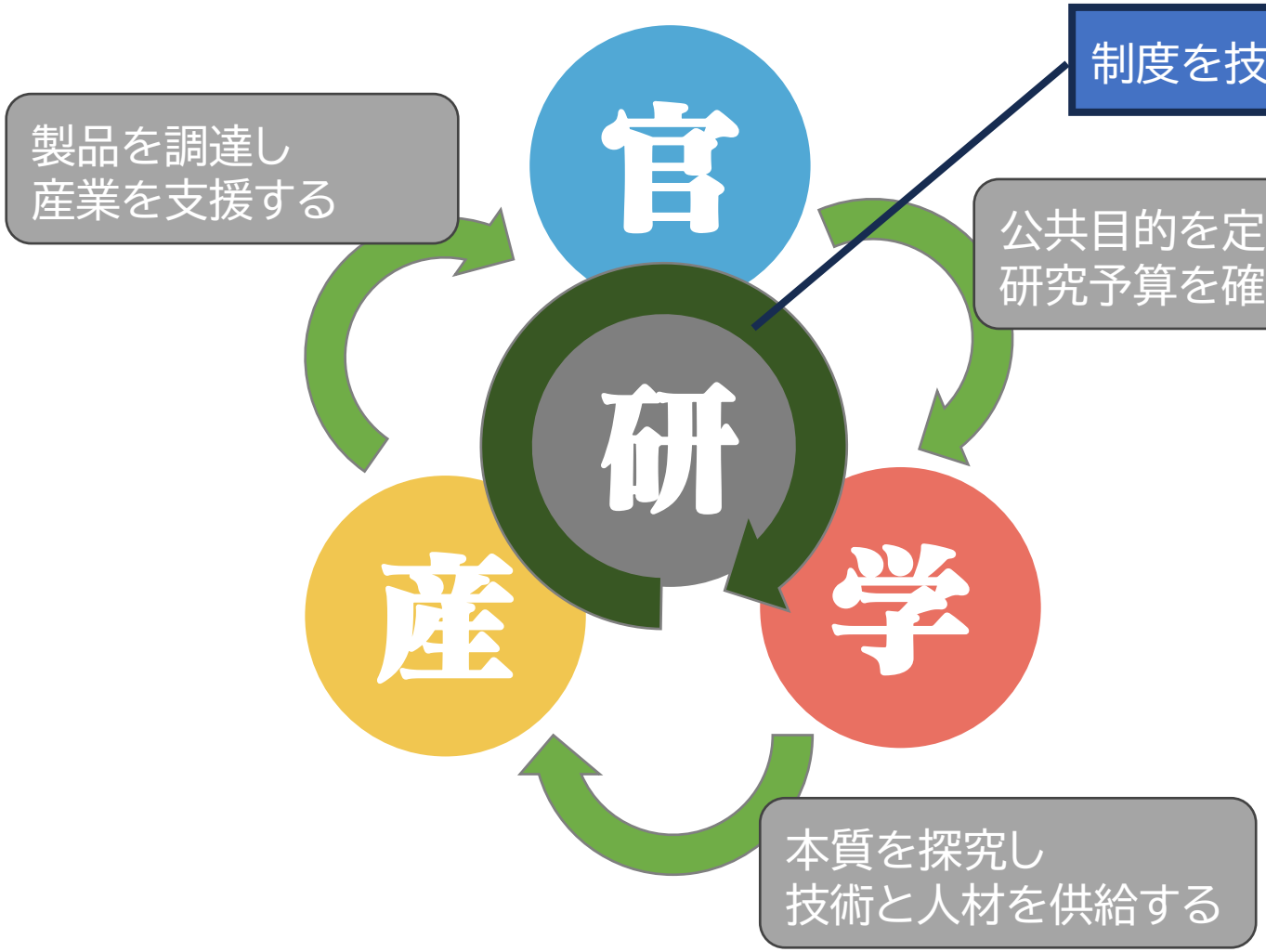
➡ NICT開発センサー『CYXROSS Agent』を政府端末に導入開始

➡ 政府内のマルウェアや指令サーバ等の情報収集可能(関係省庁の協力が重要)



技術で政策を実現している事例

次期中期計画を見据えた提言 NEXT STEP



連携と協創は【善意】ではなく【設計】

官 × 研：政策を“制度仕様”に落とす
学 × 研：本質を“使える形”にする
産 × 研：実装（製品化）を早める

CYNEXはCYNEX Allianceで実現します


CYNEX
CYBERSECURITY NEXUS


NICT
国立研究開発法人
情報通信研究機構