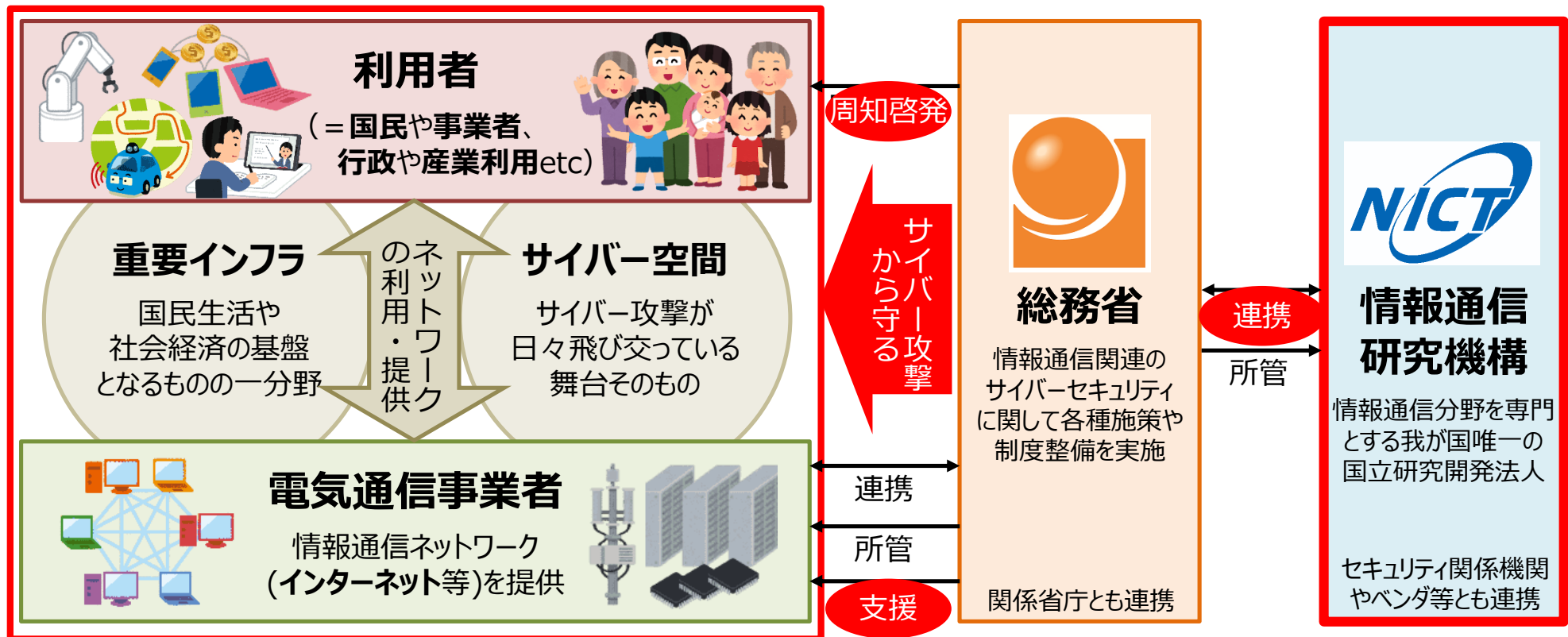


総務省における 国産セキュリティ製品・サービス供給の強化の取り組み

総務省 サイバーセキュリティ統括官室

- 総務省所管である**電気通信事業者 = 情報通信ネットワーク**は、
 - ・ 機能停止すれば国民生活や経済社会に甚大な影響が発生する**重要インフラ**（電力・金融等と同じく防護対象）
 - ・ サイバー攻撃が飛び交う**サイバー空間そのもの**（サイバーセキュリティ確保のための重要な役割）
- **情報通信研究機構(NICT)**は、**サイバー攻撃に関する観測・分析**を長年行い、**高度な技術・人材**を保有
- **総務省**は電気通信事業者やNICTと連携し、**ネットワークや利用者をサイバー攻撃から守る**取組を実施（加えて、脅威情報・技術の国産化プロジェクトを推進し、我が国自らの力で脅威を検知し対抗できる基盤を構築）



我が国では、利用されている**セキュリティ機器・サービスが海外企業に大きく依存**しており、開発に必要なデータの蓄積が困難。また、人材育成に必要なデータ・仕組みが不十分であり、**セキュリティ人材も大きく不足**。

セキュリティ機器・サービス開発の課題



- 情報が集まらないので、実データによる研究開発を行えず、国産技術を作れない。そのため情報が集まらない。
- 海外で分析され**結果の根拠が不明**。 } 経済安全保障上も大きなリスク
- **日本特有の攻撃**に対応できない。

● 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

● セキュリティ人材育成も困難

- ✓ データ不足から海外製の教材に依存せざるを得ない

セキュリティ人材育成の課題

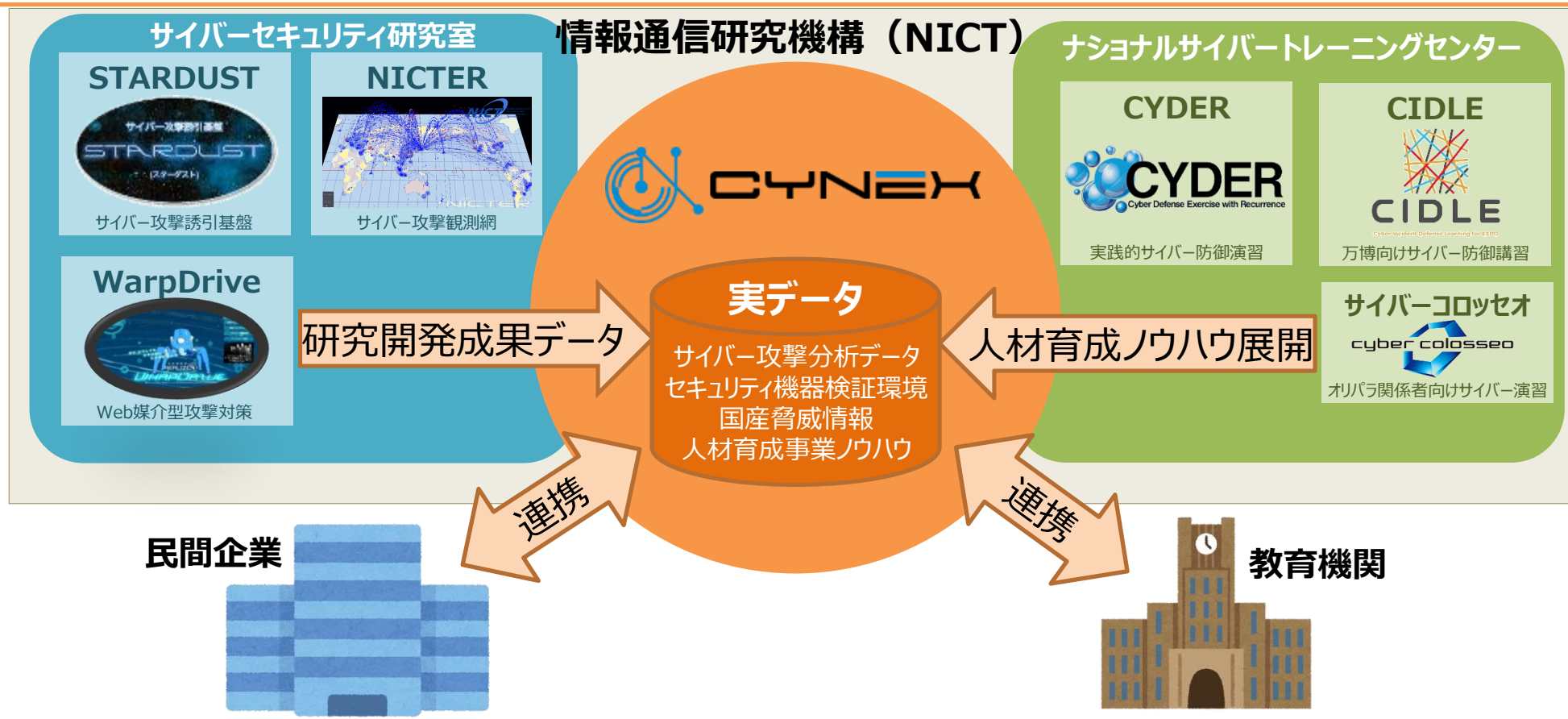
- 演習の実施には、**高度な技術力と計算機環境**が必要
- **海外教材に依存**し、国内組織特有のネットワーク構成の脆弱性を突いた攻撃などを反映できない



国内でサイバーセキュリティ情報を生成・蓄積・提供し、また人材育成にも活かす環境が必要

- データ負けのスパイラルにより、国産セキュリティ技術の開発が低迷。
- サイバー攻撃に関する実データを国内で大規模に収集・蓄積し、活用する仕組み作りが必要。
- 情報通信研究機構（NICT）では、これまで次のような取組を実施
 - ・最先端のサイバーセキュリティ関連技術の研究開発（サイバーセキュリティ研究室）
 - ・実践的サイバー防御演習等による人材育成（ナショナルサイバートレーニングセンター）
- これらのデータ・知見を活用し、サイバーセキュリティに関する産学官の結節点となる先端的基盤として

CY NEX（CYbersecurity NEXus：サイネックス） を構築



- 2023年10月1日、2年半の試行を経て、CYNEXの実施主体として、CYNEXの活動を担ってきた各組織をアライアンス化した「CYNEXアライアンス」（事務局：NICT）を発足。
- 現在、89組織がCYNEXアライアンスに参画し、CYNEXの活動を推進。
- CYNEXアライアンスへの参画等には、参画組織に費用負担を求め、CYNEXの運用費用に充当。



CYNEXアライアンス参画組織による費用負担

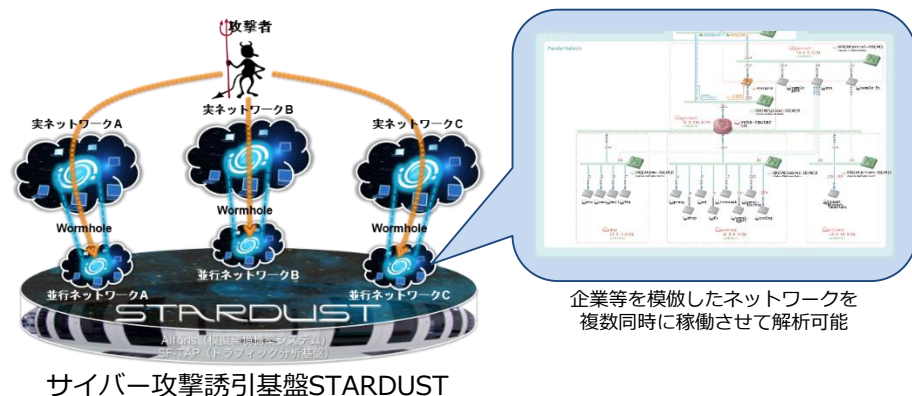
CYNEX参画費	種別	費用（年額）
	大企業	1,000,000円
	中小企業	500,000円
	一般社団法人等	500,000円
	特定非営利活動法人等	50,000円
	教育機関	50,000円
	官公庁等	0円
	有識者等	0円

※ 上記は1つのCo-Nexus（CYNEXのサブグループ）に参画する場合の負担費用。
複数のCo-Nexusに参画する場合は、参画Co-Nexus数に応じて、上記の2倍を上限として負担費用を増額。

CYROP利用費	費用
	CYROP利用に伴う売上高の10%

※ CYNEX参画組織がCYROP（Co-Nexus Cにおいて供用するサイバーセキュリティ演習基盤）を利用した事業により売上を得る場合に、CYNEX参画費とは別に負担を求める費用。

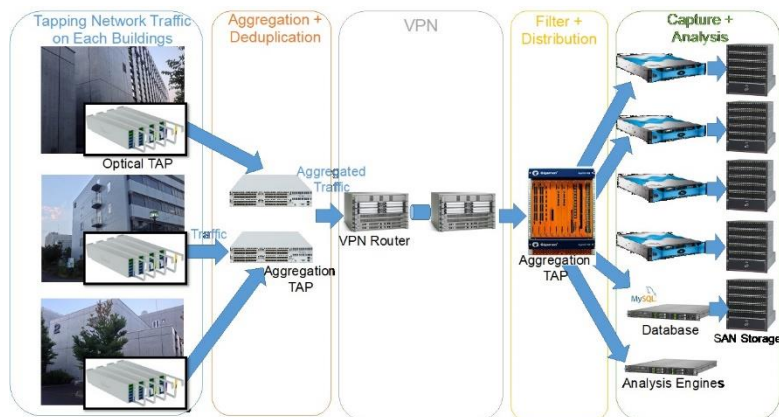
■ サイバー攻撃の共同解析と解析者コミュニティ形成



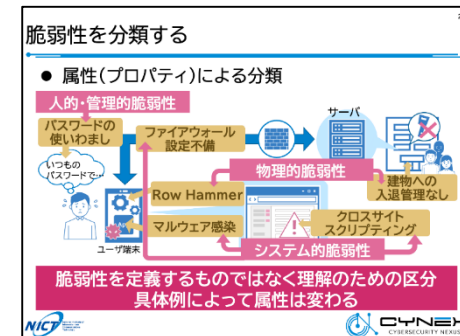
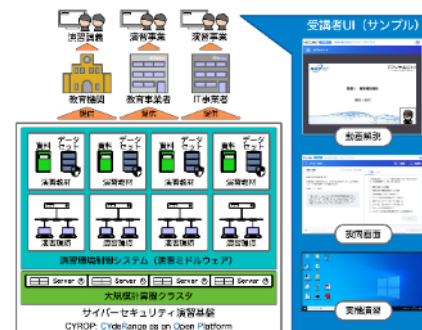
■ 高度な解析者の育成と独自の脅威情報の生成・発信



■ 国産セキュリティ製品のテスト環境提供による実用化支援



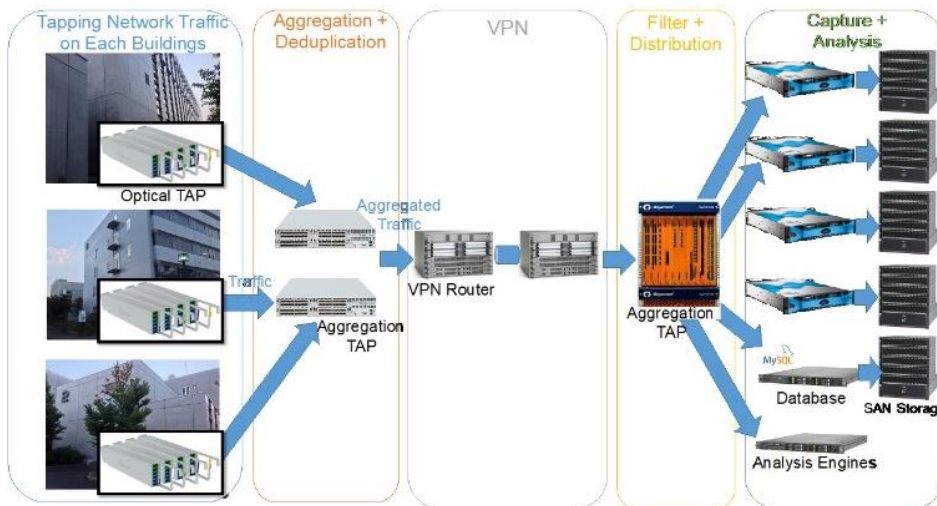
■ 演習基盤開放による国内セキュリティ人材育成事業の活性化



- ✓ 各製品ごとにカスタムした検証環境の構築
- ✓ Walküre (CYNEX Red Team) の模擬攻撃によるセキュリティ機能検証
- ✓ 海外有力製品群との比較検証

国産セキュリティ製品検証リスト（一部抜粋）

製品種別	製品フェーズ	運用・検証の概要
ペネトレーションツール	商用化前技術	ツールの高度化及び長期運用
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
ランサムウェア対策ソフト	商用化済技術	新たなマルウェアへの適応検証

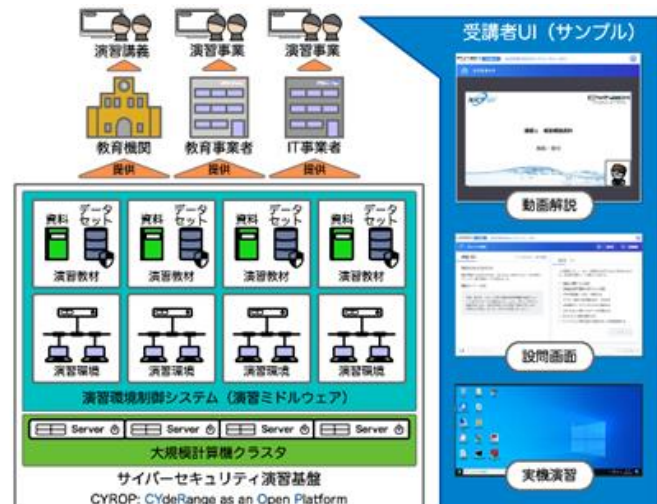


国産セキュリティ製品テスト環境（NICT機構内部ネットワーク観測システム）



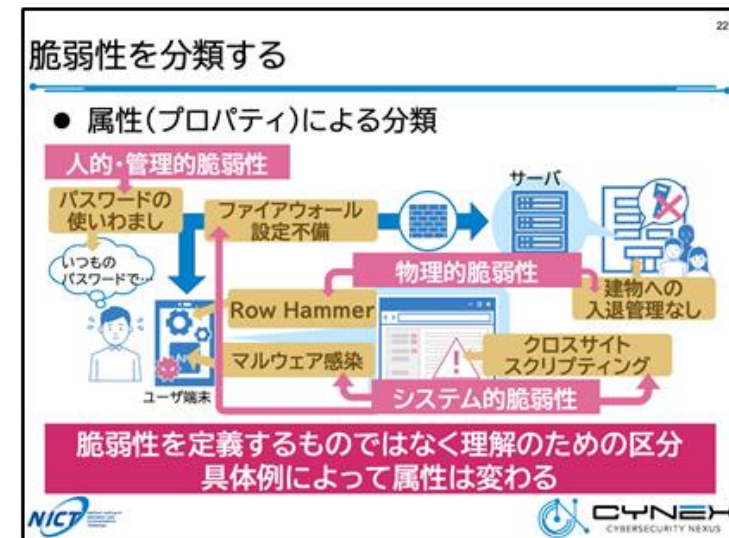
IoT機器検証環境

- ✓ サイバーセキュリティ演習に必要な演習環境と演習教材をオープン化
- ✓ 産学官のニーズに基づき、NIST NICE Frameworkに沿って演習教材整備



サイバーセキュリティ演習基盤
CYROP (Cyber Range Open Platform)

大学・民間企業等**35組織**が参画



CYNEXオリジナル演習教材

新規演習教材の共同開発を実施

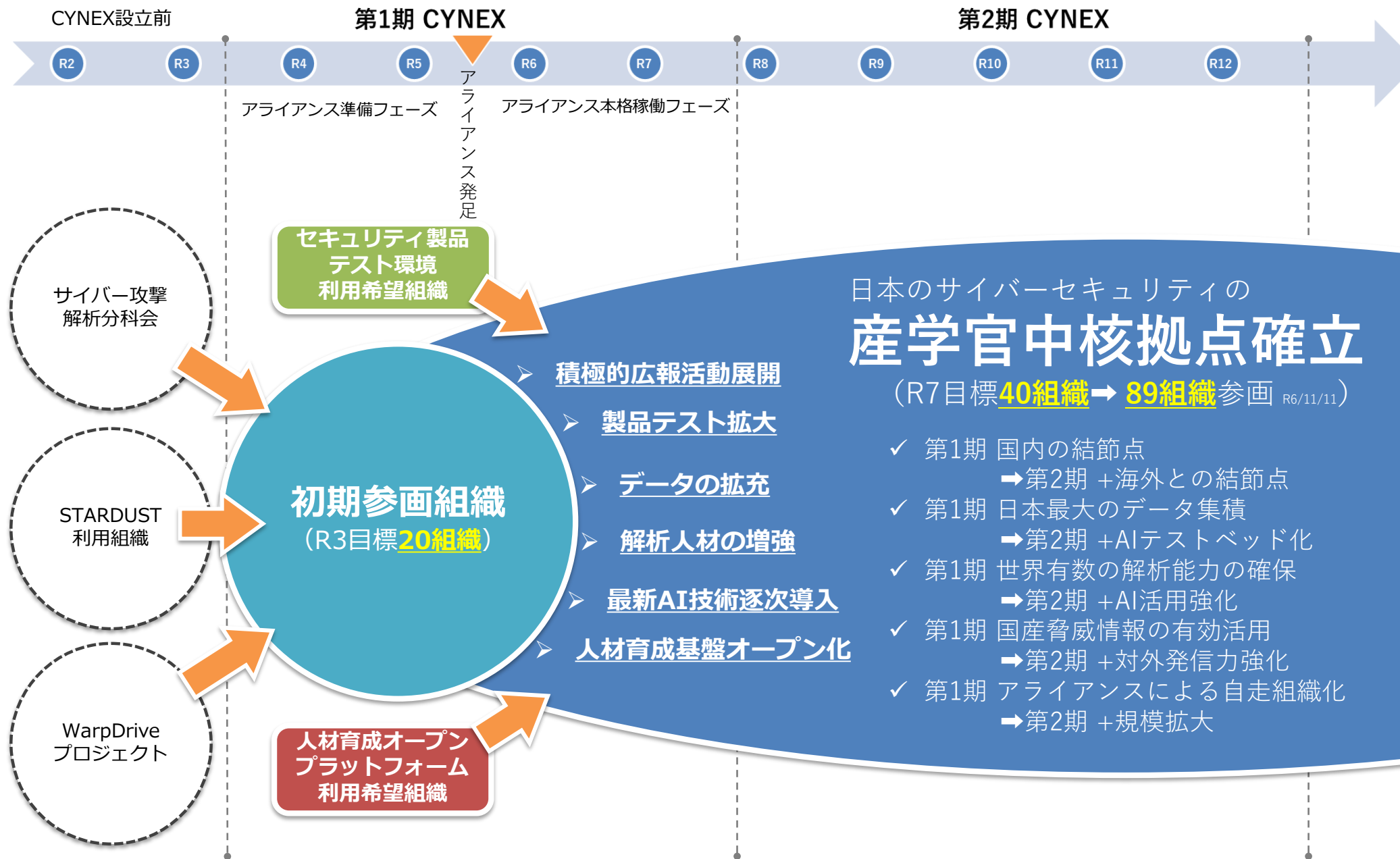
2021年：CYDERコンテンツ、パケット解析等（18種）

2022年：セキュリティ管理、ペネテスト等（18種）

2023年：**フォレンジック、ログ収集・分析等（14種）**

➡ 合計74種に拡充 NICE Framework KSA充足率49%

➡ 2022年度までに作成した教材のうち71%が実利用される



- 総務省では、NICTのデータ・知見を活用したサイバーセキュリティに関する産学官の結節点・CYNEXの構築を支援。CYNEXの活動は令和5年10月から本格的に始動
- 今後もCYNEXの機能を拡大し、海外との結節点機能やAIの利活用の強化などを予定。これらを通じて、さらなる国産セキュリティ製品・サービス供給への貢献を目指していく