サイバーセキュリティ統合知的・人材育成基盤

CYNEX（サイネックス）

2021年度活動状況報告

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ネクサス

NICT National Institute of Information and Communications Technology

CYNEX CYBERSECURITY NEXUS

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

サイバーセキュリティ研究室

研究開発成果展開

人材育成ノウハウ展開

ナショナルサイバートレーニングセンター

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

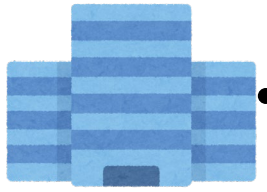
説明可能な国産脅威情報の生成・提供

高度SOC人材育成（Online自主学習＆OJT）

国産セキュリティ技術の検証環境構築

人材育成基盤のオープン化による事業促進

CYNEX
CYBERSECURITY NEXUS



民間企業・政府機関

共同解析，育成人材投入，
人材育成基盤利用，
製品プロトタイプ導入，etc.

共同解析，育成人材投入，
人材育成基盤利用，etc.

教育機関

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

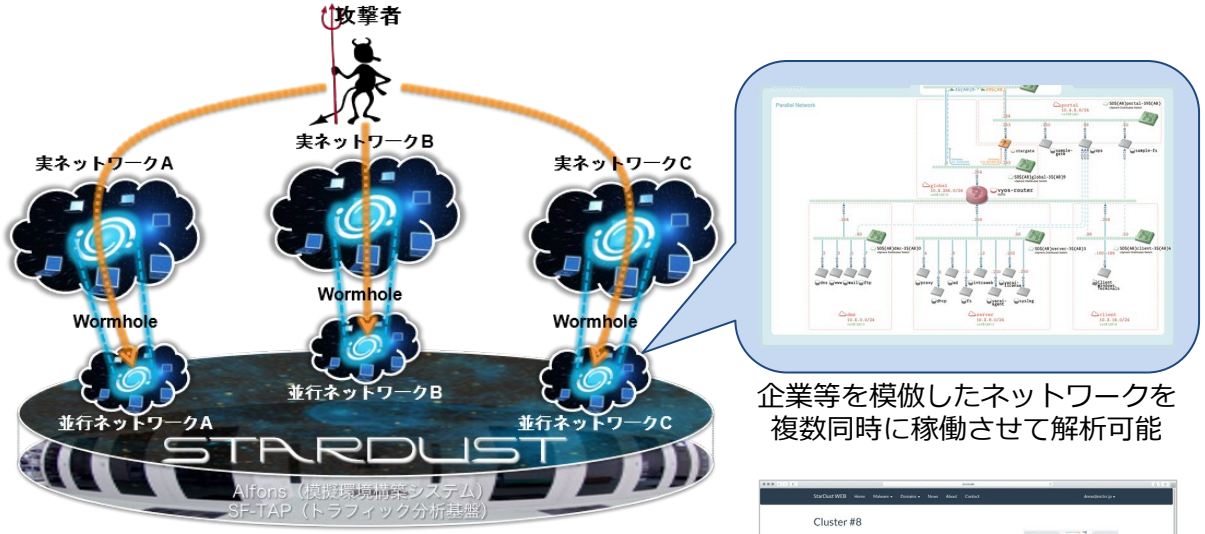
Co-Nexus C (CYROP*)
- ✓人材育成基盤のオープン化
- ✓パイロットコンテンツ開発

*CYROP: CYDERANGE as an Open Platform

Co-Nexus A：STARDUST＆解析者コミュニティ形成

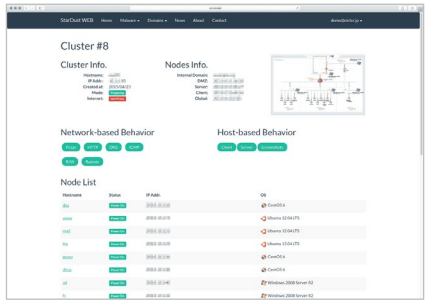
●目的：STARDUSTを核とした共同解析と解析者コミュニティ形成

- ✓ STARDUST：人間の攻撃者を誘い込む**サイバー攻撃誘引基盤**
- ✓ 定常的な攻撃誘引の試行と解析結果を共有する解析者コミュニティの形成



CYNEX専用STARDUST構築中

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

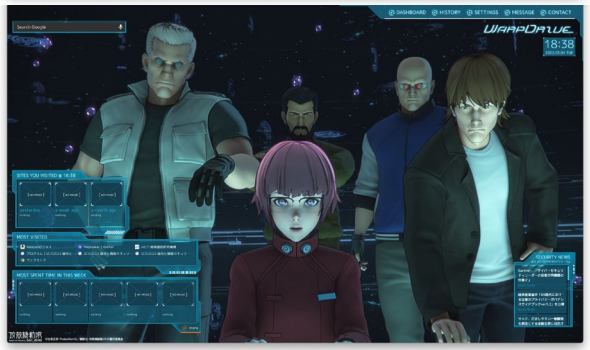
● 2021年度活動状況

- ✓ **30組織**からの参画申し込み
- ✓ 延べ**300日以上**の攻撃誘引試行
- ✓ Co-Nexus Aミーティングを複数回開催し解析結果やノウハウを共有

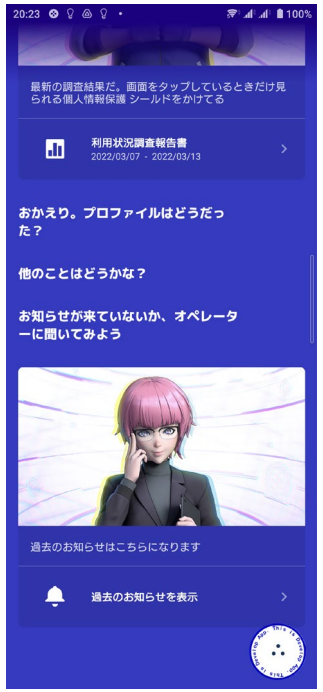
Co-Nexus A：WarpDriveプロジェクトの継承と進化

●目的：Web媒介型攻撃の対策確立のためのデータ収集・分析

- ✓ WarpDrive：ユーザ参加型の**Web媒介型攻撃大規模観測プロジェクト**
- ✓ NICT委託研究（2016～2020年度）の成果をCYNEXに継承・進化



新Windows/Mac版タチコマSA



新Android版タチコマSAモバイル

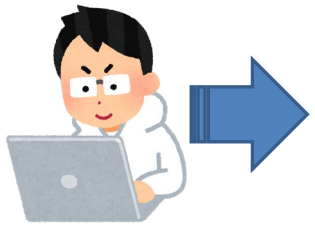
● 2021年度活動状況

- ✓ WarpDrive関連システムの**CYNEXへの完全移管を完了**
- ✓ さらなる参加ユーザ獲得に向けた**タチコマセキュリティエージェント**第一弾アップデート完了

Co-Nexus S：高度SOC人材育成と国産脅威情報発信

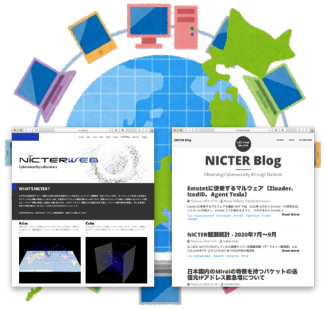
●目的：高度な解析者の育成とCYNEX独自の脅威情報の生成・発信

- ✓ オンラインSOC研修（自主学習型）とCYNEX解析チームでのOJT
- ✓ サイバーセキュリティ関連情報の発信機能のCYNEXへの集約



自主学習型
オンラインSOC研修

OJTでのSOC業務従事



国産脅威情報発信/提供

自主学習型オンラインSOC研修システム

am I infected

● 2021年度活動状況

- ✓ 6組織からの参画申し込み
- ✓ オンラインSOC研修システム始動
- ✓ am I infected?*への情報提供

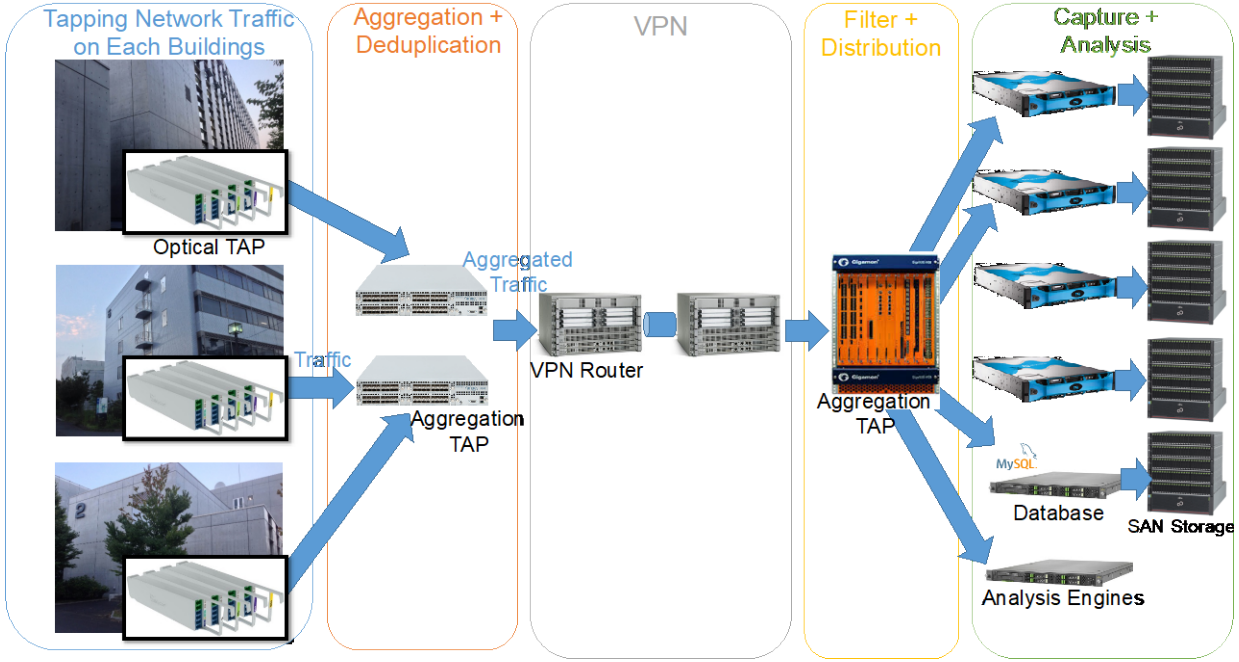
*横浜国立大学 情報・物理セキュリティ研究拠点が運営するマルウェア感染・脆弱性診断サービス

- ✓ NICTER観測レポート2021公開

Co-Nexus E：国産セキュリティ製品の運用・検証

●目的：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

- ✓ NICT内部ネットワークにおける国産セキュリティ製品の長期運用・検証
- ✓ CYNEX Red Teamによる模擬攻撃を用いたセキュリティ機能検証



NICT内部ネットワーク観測システム

● 2021年度活動状況

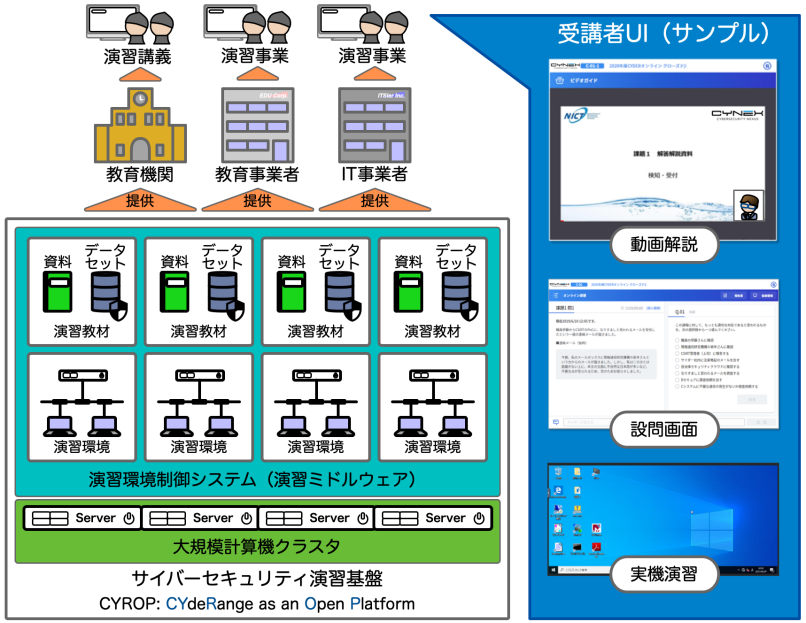
- ✓ 4組織からの参画申し込み
- ✓ CYNEX Red Team（攻撃チーム）の立ち上げ開始
- ✓ 模擬攻撃再現ツールを運用・検証し民間企業へフィードバック実施中

Co-Nexus C：人材育成オープンプラットフォーム

●目的：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

✓サイバーセキュリティ演習に必要となる**演習環境と演習教材をオープン化**

✓米国NIST NICE Frameworkに基づいた教育教材の段階的整備



サイバーセキュリティ演習基盤CYROP

CYROP利用第一号

● 2021年度活動状況

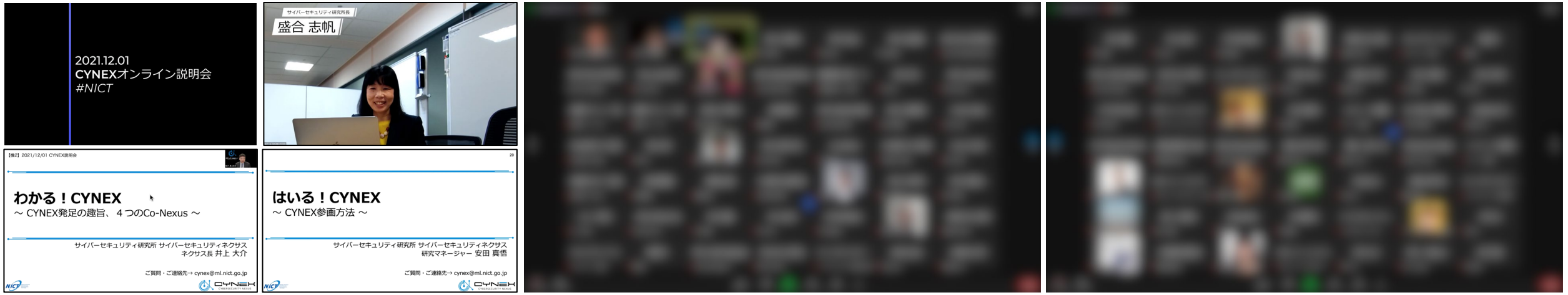
✓ **8組織**からの参画申し込み

✓ サイバーセキュリティ演習基盤
CYROPオープン化トライアル開始

✓ 教育機関向け人材育成教材など
新規演習教材の共同開発開始

CYNEX参画スキームの整備とオンライン説明会開催

4つのCo-Nexus	参画内容	手続き
Co-Nexus A	解析情報の共有（旧解析分科会）	**委員委嘱**
	STARDUST利用	**共同研究契約**
	WarpDriveプロジェクト	**共同研究契約**
Co-Nexus S	高度SOC人材育成（オンライントレーニング）	**研修員**
	高度SOC人材育成（OJT）	**出向**
Co-Nexus E	国産セキュリティ製品の運用・検証	**共同研究契約**
Co-Nexus C	セキュリティ人材育成の社会展開（事業化）	**覚書 + α（機材貸与契約等）**
	セキュリティ人材育成コンテンツ開発	**共同研究契約**



2021年12月1日 CYNEXオンライン説明会の模様（40組織69名の外部参加者）

CYNEXの事業展開のタイムライン