わかる！CYNEX

～ つながる日本のサイバーセキュリティ ～

サイバーセキュリティ研究所 副研究所長
|-- サイバーセキュリティネクサス ネクサス長
|-- サイバーセキュリティ研究室 室長

井上 大介

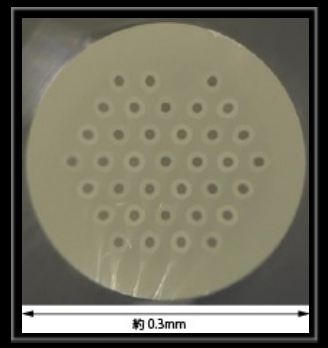
CYNEX
CYBERSECURITY NEXUS

NICT 国立研究開発法人 情報通信研究機構

国立研究開発法人 情報通信研究機構とは？

- 情報通信分野を専門とする日本で唯一の公的研究機関

日本標準時の生成・配信
（うるう秒挿入）

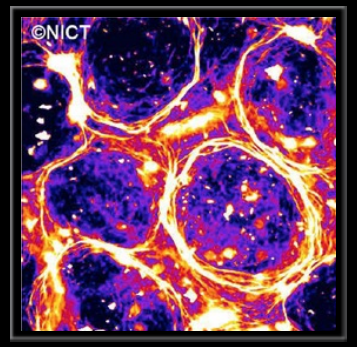


光通信システム
（ペタbps級 マルチコアファイバ）

宇宙通信システム
（超高速インターネット衛星きずな）

サイエンスクラウド
（ひまわり8号リアルタイムWeb）

電磁波センシング
（Pi-SAR2による3.11直後の仙台空港）



バイオ・ナノICT
（生体分子の自己組織化）

脳情報通信融合
（ブレイン・マシーン・インターフェイス）

多言語音声翻訳
（多言語音声翻訳アプリVoiceTra）

超臨場感コミュニケーション
（初音ミクさんの電子ホログラフィ）

サイバーセキュリティ
（対サイバー攻撃アラートシステムDAEDALUS）

NICT サイバーセキュリティ分野の体制図

【第5期中長期計画　サイバーセキュリティ分野】

(1)　サイバーセキュリティ技術
(ア) データ駆動型サイバーセキュリティ技術
(イ) エマージングセキュリティ技術

(2) 暗号技術
(ア) 安全なデータ利活用技術
(イ) 量子コンピュータ時代に向けた暗号技術の安全性評価

(3) サイバーセキュリティに関する演習

(4) サイバーセキュリティ産学官連携拠点形成

(5) パスワード設定等に不備のあるIoT機器の調査

サイバーセキュリティ研究所


盛合 志帆
所長


井上 大介
副所長


中尾 康二
主管研究員

セキュリティ基盤研究室


篠原 直行 室長

サイバーセキュリティ研究室


井上 大介 室長

CYNEX サイバーセキュリティネクサス


井上 大介 ネクサス長

ナショナルサイバートレーニングセンター


園田 道夫
センター長

サイバートレーニング研究室


花田 智洋 室長

サイバートレーニング事業推進室

ナショナルサイバーオブザベーションセンター


衛藤 将史
センター長

サイバーオブザベーション運用室


衛藤 将史 室長

サイバーオブザベーション事業推進室

総合企画室

サイバーセキュリティあるある（1）

セキュリティ担当者

彼の国のセキュリティ製品は
検知率100%で凄いじゃないか！

社長…
セキュリティの世界で100%は
ほぼ嘘なんですって…

社長

サイバーセキュリティあるある（2）

セキュリティ担当者

この侵入検知システムのアラート…
何でずっと出続けてるんですかね？

お任せください！本国の開発部隊に
問い合わせてみます！

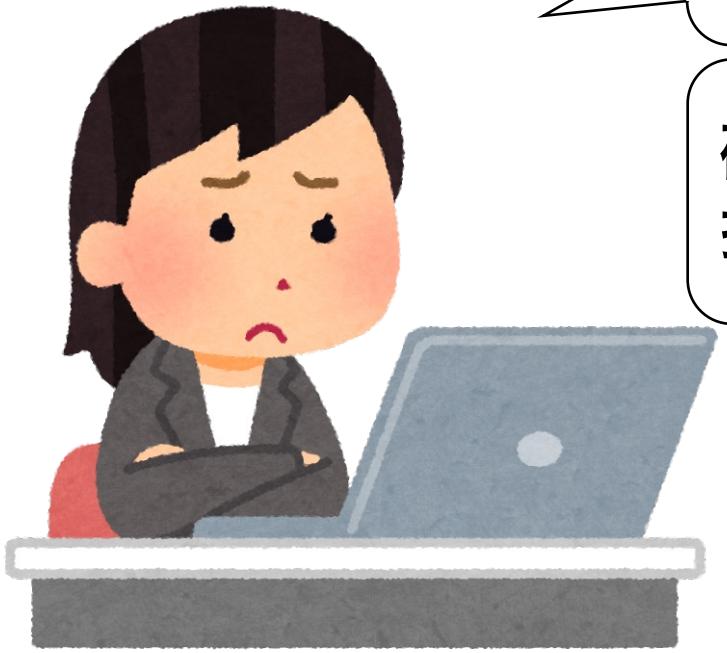
・
・　数週間後
・

検知ロジックのコアに当たるため
開示不可だそうです！

セキュリティベンダ
日本代理店

サイバーセキュリティあるある（3）

機械学習の検知エンジン作ったけど
どこかで試せないかなぁ…



セキュリティ研究者

研究部門には事業部の顧客データは
指一本触れさせません！

事業部

サイバーセキュリティあるある（4）

今度うちの学科で、サイバー演習をすることになって…

准教授

お任せください！本国の営業部隊に問い合わせてみます！

・
・　数日後
・

サイバー演習BOX（ハーフラック）が破格の8億円ポッキリです！

セキュリティベンダ
日本代理店担当者

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…？）

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**

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

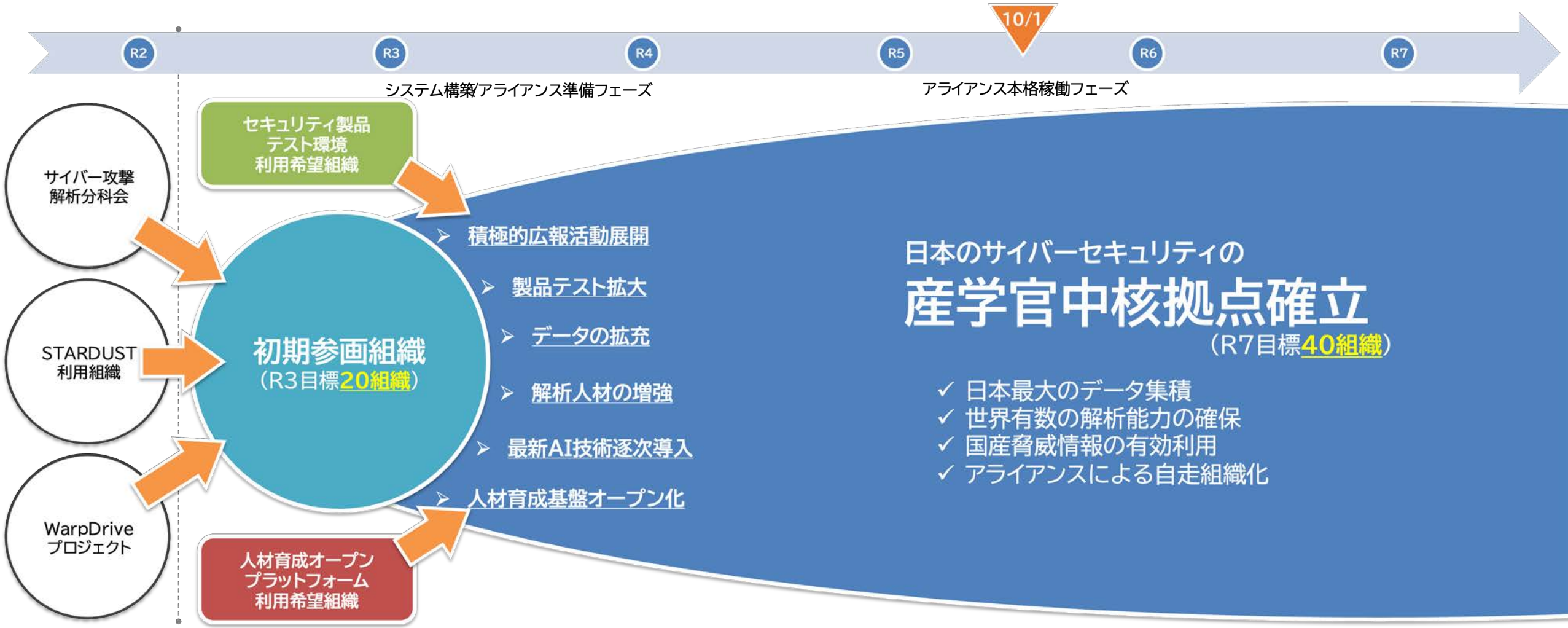
- 実データを**大規模に収集・蓄積**する仕組み
- 実データを**定常的・組織的に分析**する仕組み
- 実データで**国産製品を運用・検証**する仕組み
- 実データから**脅威情報を生成・共有**する仕組み
- 実データによる**人材育成をオープン化**する仕組み

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

CYBERSECURITY NEXUS

CYNEXの事業展開のタイムライン



2023年10月1日 CYNEXアライアンス 発足

CYNEX CYBERSECURITY NEXUS

4つの “Co-Nexus” によるプロジェクト推進

CYNEX ALLIANCE

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

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・情報発信

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

Co-Nexus C (CYROP)

- ✓サイバーセキュリティ演習基盤のオープン化
- ✓演習環境の運用と演習教材の継続的開発

*CYROP: Cyber Range Open Platform

Co-Nexus Chairs


安田 真悟
NICT


毛利 公一
立命館大学


佐藤 隆行
日立製作所


久保 正樹
NICT


piyokango
セキュリティインコ

Walküre
CYNEX Red Team


安部 小百合
NICT


佐藤 公信
NICT


島 成佳
長崎県立大学


井田 純
トリノケート

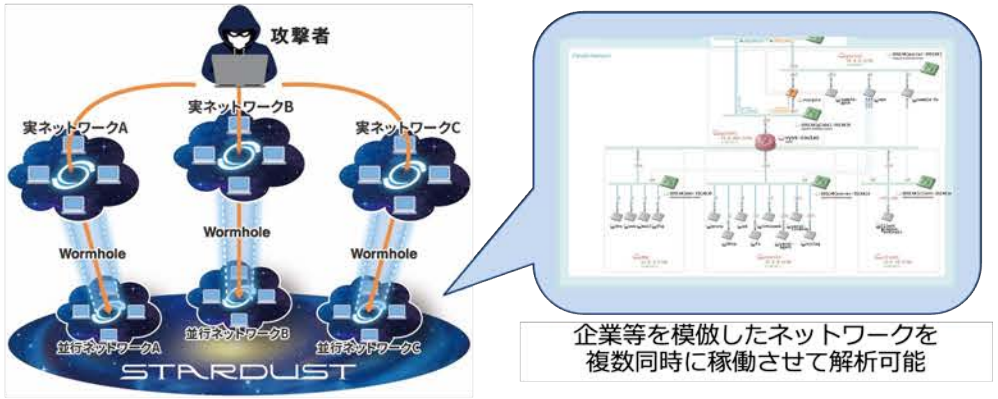
各Co-Nexusの概要と参画組織数（2024年2月29日現在）

60組織参画中

Co-Nexus A (Accumulation & Analysis)

参画組織数：32

- 目的：STARDUSTを核とした共同解析と解析者コミュニティ形成



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

サイバー攻撃誘引基盤STARDUST

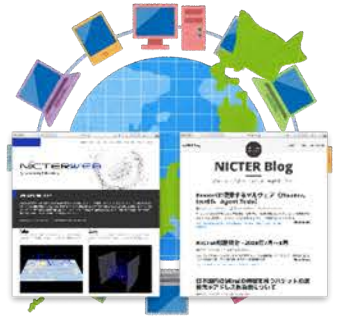
Co-Nexus S (Security Operation & Sharing)

参画組織数：14

- 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

自主学習型
オンラインSOC研修

OJTでのSOC業務従事

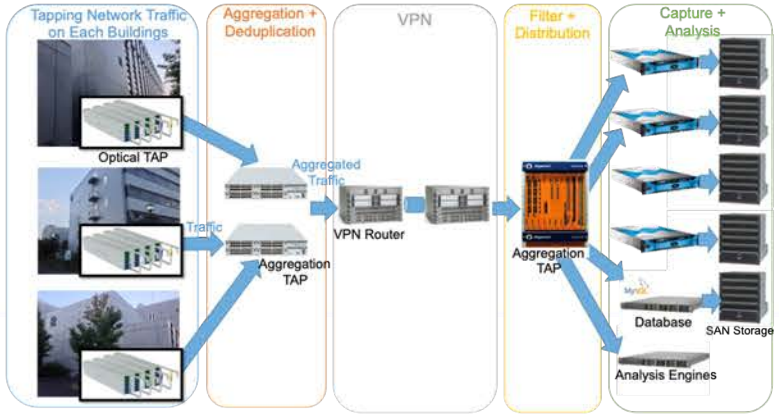


国産脅威情報発信/提供

Co-Nexus E (Evaluation)

参画組織数：5

- 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



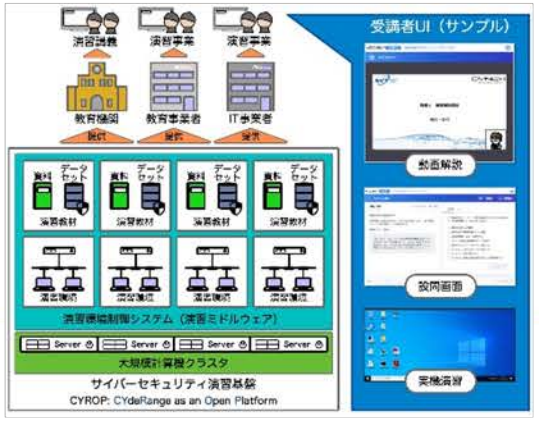
国産セキュリティ製品テスト環境（機構内部ネットワーク観測システム）

Co-Nexus C (CYROP*)

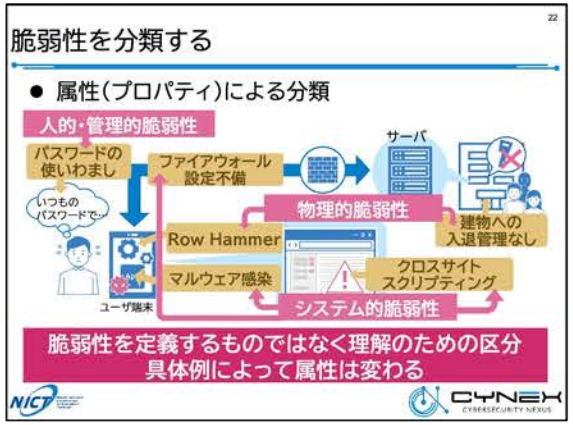
*CYROP: Cyber Range Open Platform

参画組織数：34

- 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基盤CYROP



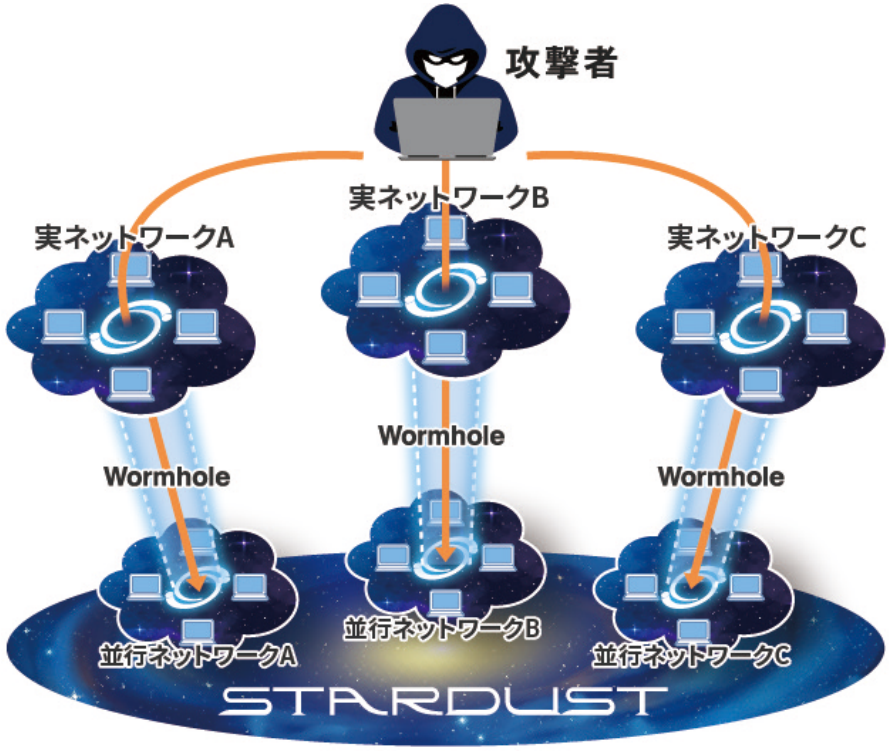
CYNEXオリジナル演習教材

Co-Nexus A

Accumulation & Analysis

STARDUST&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**
- **最新の攻撃事例や解析ノウハウを共有する解析者コミュニティの形成**



サイバー攻撃誘引基盤STARDUST NxtGen

● 活動状況

✓ **STARDUST NxtGen**貸与開始
- 参画組織が並行してHuman-operatedな攻撃観測

✓ 年間**300日以上**の攻撃誘引実験
- NICTの解析結果は積極的にコミュニティへ共有

✓ **解析者コミュニティ会合**定期開催
- 毎回**90名**規模の解析者や研究者が参加
  - ✓ STARDUST 標的型攻撃/ランサムウェア観測事例
  - ✓ ロシア・ウクライナ情勢関連の観測情報
  - ✓ 脅威情報/OSINT収集ノウハウ共有
  - ✓ アトリビューションのためのアーティファクト分析事例
  - ✓ 医療業界のインシデント対応事例　etc.

解析ノウハウ例：STARDUST観測失敗事例

●攻撃者がすぐに去ってしまった原因

✓一般ユーザでないと（解析環境と）判断？

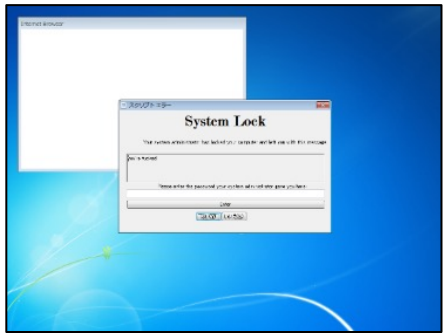
- メールの受信トレイ、送信済みアイテム、**下書きが空**
- **ブラウザの閲覧履歴がない**
- systeminfoコマンドを使用して動作環境を確認 etc.

✓そもそもターゲットが日本ではなかった？

- 平日の 9:00~18:00（UTC+9）に実験を実施
- OSの言語設定やファイルなどすべて日本語
- **日本語環境に戸惑っている攻撃者を何人か確認**

攻撃者が解析環境と気づいた後の行動:

シャットダウン



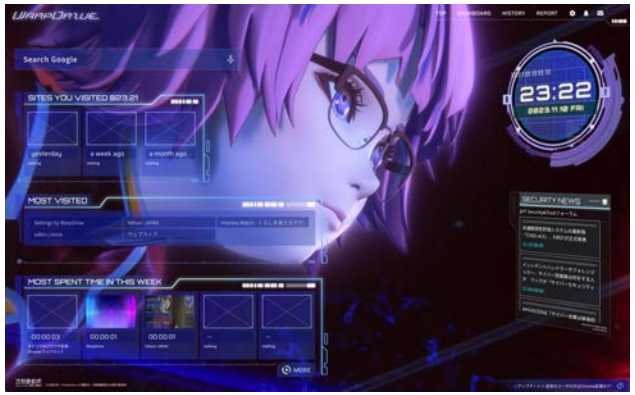
画面ロック

チャットで話しかけてくる

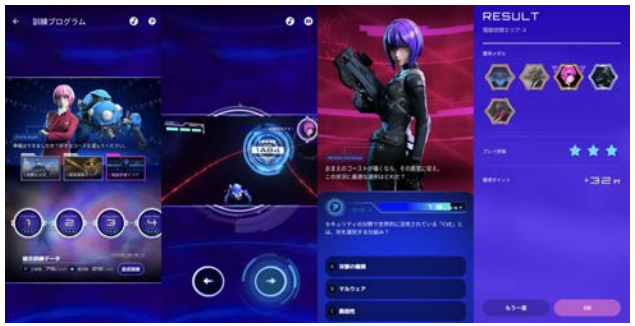
WarpDriveプロジェクト

●ユーザ参加型のWeb媒介型攻撃大規模観測プロジェクト

- ✓Web媒介型攻撃の対策確立のためのデータ収集・分析
- ✓**タチコマ・セキュリティ・エージェント**（PC/Android版）を無償配布



PC版
タチコマSA



Android版
タチコマモバイル

©士郎正宗・Production I.G/講談社・攻殻機動隊2045製作委員会

● 活動状況

- ✓ **第2弾アップデート**（2023/10/16 リリース）
  - Android向けタチコマモバイルに**ゲーム機能を開発**
  - クイズゲームでセキュリティやITの知識を反復学習
- ✓ **第3弾アップデート**（2024/2末 リリース）
  - PC向けタチコマSAにゲーム機能を追加
  - Android向けに**ローカルスキャン機能を開発**
    - ➡ 家庭内のネットワークデバイスを発見可能に
- ✓ **WarpDriveコミュニティ発足**
  - 産学の研究機関が複数参画
  - データ解析や対策展開を加速

Co-Nexus S

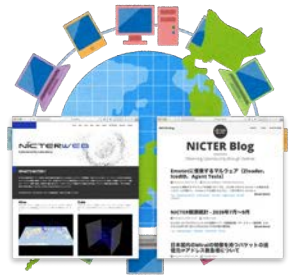
Security Operation & Sharing

高度SOC人材育成と国産脅威情報発信

- **自主学習型オンラインSOC研修と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とデータの外部提供**

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

フロー情報分析による
C&Cサーバ検知

● 活動状況

✓ **オンラインコース＆OJTコース**
- オンラインコース：3期生6名 修了、**4期生16名 研修中**
- OJTコース：CYNEX解析チームで2名修了、**2名育成中**

✓ **NICTERレポート, Blog, Twitter**
- NICTER観測レポート2023（2024/2/13 公開）
- NICTER Blog：5件、Twitter 随時更新

✓ **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

✓ **C&Cサーバ検知に関する調査***への情報提供

* 電気通信事業者おけるフロー情報を用いたC&Cサーバ検知に関する手法や有効性の調査

CYNEX CYBERSECURITY NEXUS

高度SOC人材育成の各種コース

● 高度SOC人材育成 コースメニュー

コース名		期間	内容
オンラインコース		半年	●オンライン自主学習プラットホームによる学習 ●学習した知識を使った調査実施 ●成果発表
OJT	ダークネット分析コース	2年～	●ダークネット分析の概要説明 ●ダークネットデータの取得 ●分析アプローチの検討と分析実施 ●成果発表
	ライブネット分析コース	2年～	●ライブネットオペレーションの概要説明 ●機構内セキュリティオペレーション ●分析アプローチの検討と分析実施 ●成果発表
	アーティファクト分析コース	2年～	●マルウェア解析の概要説明 ●解析環境構築 ●マルウェア表層解析/動的解析/静的解析 ●成果発表

● オンラインコース（半年間）

SecBokベースのスキル評価

オンライン自主学習プラットホームによる学習
（CYNEX解析チームによるサポート、進捗ミーティングx3回）

学習した知識を使った調査実施
（テーマ選定、 CYNEX解析チームによるサポート）

成果発表 → 修了証発行

CYNEX高度SOC人材育成修了証

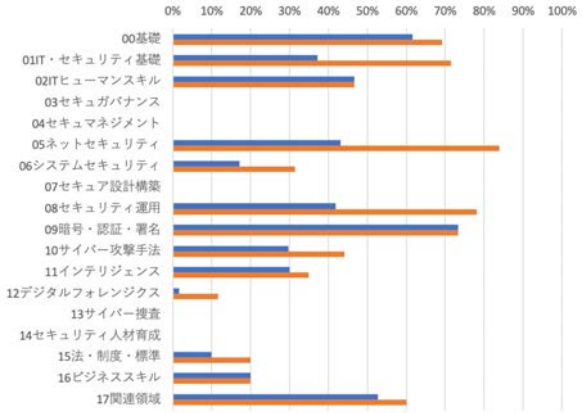
● OJTコース（2年間）

- ✓ CYNEX解析チームの一員として観測・分析業務に従事
- ✓ 世界中のセキュリティアプライアンスを用いた統合分析

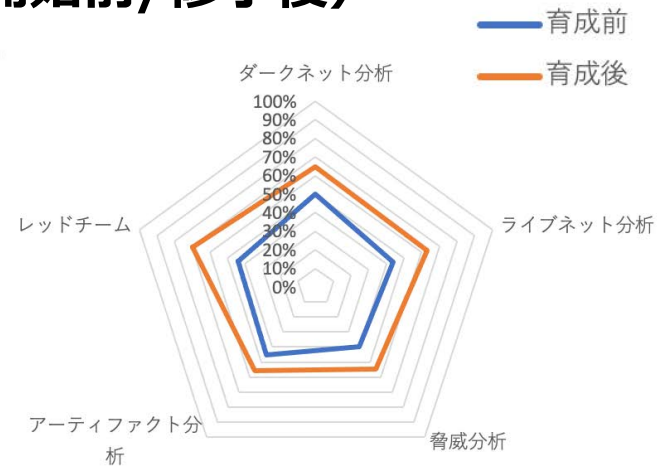
CYNEX解析チームでのOJTの様子

NISCコラム（OJTコース第1号）
https://security-portal.nisc.go.jp/cybersecuritymonth/2023/columns/column-kaneshiro.html

● スキル評価（コース開始前/修了後）



分野別適合率



スコープ別適合率

自主学習型オンラインSOC研修システム

Co-Nexus E

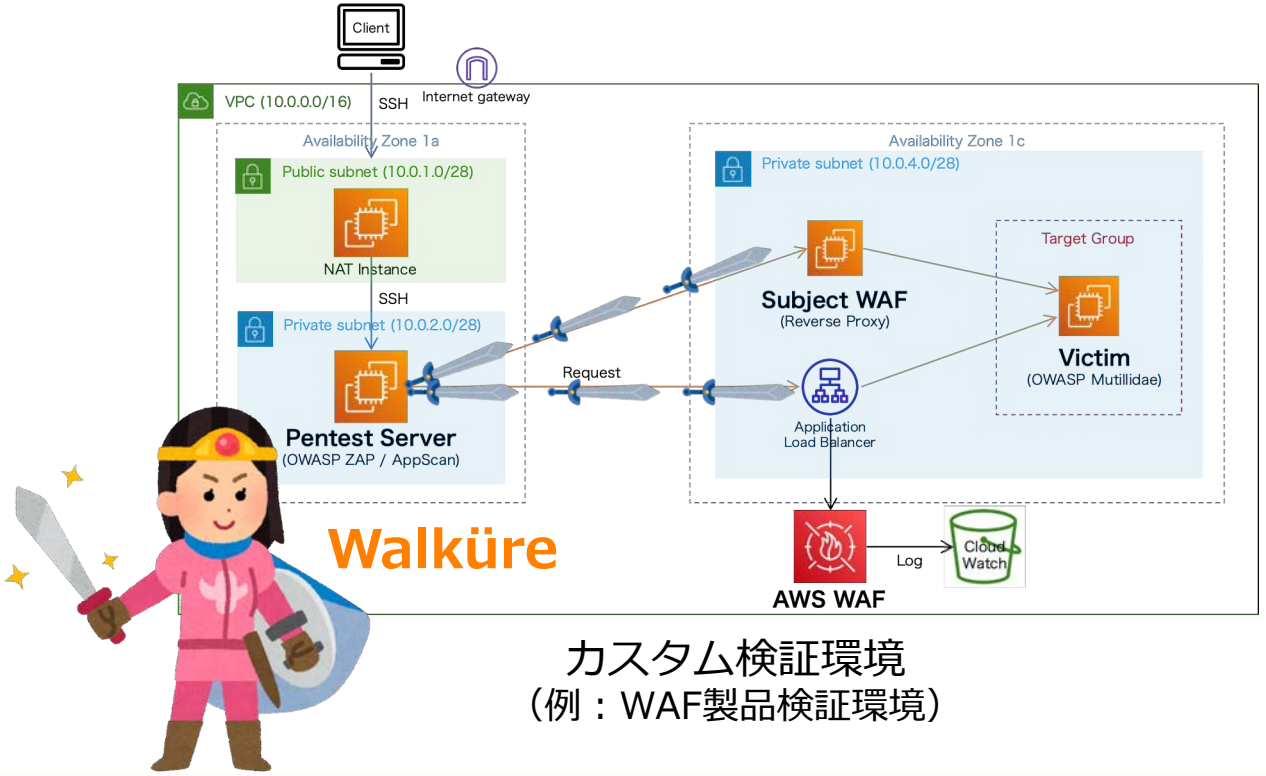
Evaluation

国産セキュリティ製品の運用・検証

●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

✓**Walküre（CYNEX Red Team）**の模擬攻撃によるセキュリティ機能検証



カスタム検証環境
（例：WAF製品検証環境）

● 活動状況

✓ **国産製品の長期運用・検証**を実施

✓ 各製品ごとに**カスタム検証環境構築**
- WAF製品検証環境
- IoT機器検証環境 etc.

✓ **Walküre**による模擬攻撃の実施

✓ 海外有力製品群との**比較検証**

✓ 開発企業への**フィードバック**

検証事例：IoT機器のファジング技術

●IoTファジング技術

- ✓リチェルカセキュリティ社が開発
- ✓様々な入力データを機器に与えてバグや脆弱性を検出
- ✓IoT機器の特性を踏まえた技術（ソフトウェアの状態を確認しづらいなど）

●IoTファジングを実機検証する環境を構築

- ✓NICTで培ってきたIoT機器向けのマルウェア研究や脆弱性対応のノウハウを活用

●12機種20台の機器を接続

- ✓ホームルータ、カメラ等
- ✓2022/8より検証継続中
- ✓リモート操作可能

IoTファジング検証環境

Co-Nexus C

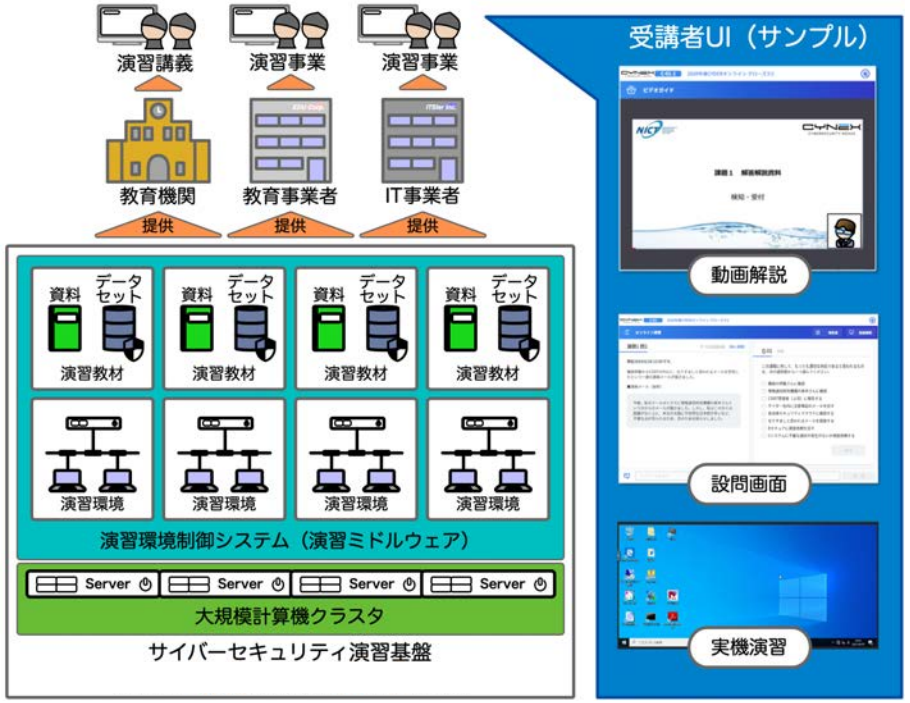
CYROP: Cyber Range Open Platform

人材育成オープンプラットフォーム

●サイバー演習基盤開放による国内セキュリティ人材育成事業活性化

✓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**

✓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

● 活動状況

✓ **CYROP基盤本格稼働開始**

- CYROP：Cyber Range Open Platform

✓ **３組織**が商用演習サービスを開始

- CYDER Aコース由来 演習教材（順次受け入れ）
- CYDER Bコース由来 演習教材（順次受け入れ）
- CYNEX オリジナル 演習教材（拡充中）

✓ **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、ペンテスト等（18種）
- 2023年：**フォレンジック、OTセキュリティ（29種）**

演習教材一覧（~2022年度）

CYDERからの継承コンテンツ

- ✓ 2019年 Aコース（初級）
- ✓ 2020年 B-1コース（中級）
- ✓ 2020年 B-2コース（中級）
- ✓ 2021年 B-2コース（中級）

パイロットコンテンツ

- ✓ IoTを含むセキュリティ問題検出とその防御
- ✓ パケットキャプチャとパケット解析
- ✓ OSコマンドインジェクションとその防御
- ✓ SQLインジェクションとその防御
- ✓ XSSとその防御
- ✓ クロシュサイトリクエストフォージェリとその防御
- ✓ マルウェア挙動およびその防御
- ✓ マルウェアキャプチャ
- ✓ ソケットプログラミング（バッファオーバーフロー）
- ✓ ノンテクスキル演習

1.1 講義を受講するために必要な事前 KSA

本講習を受講するために必要な前提知識および対応する NIST NICE Framework の K(Knowledge)・S(Skill)・A(Ability)を「表 1 講義を受講するために必要な事前 KSA」に示します。アンダーバーの後の数字は認知プロセスの次元を示します。例として、「Linux の基本操作」の場合、「K0060: Knowledge of operating systems.」に該当するナレッジが、認知プロセス「1 知識・記憶レベル」の次元で必要であることを示します。

表 1 講義を受講するために必要な事前 KSA

前提知識	Knowledge	Skill	Ability
Linux の基本操作	K0060_1	-	-
TCP/IP の基本知識	K0001_1	-	-
明確かつ簡潔な方法で質問に答える能力	-	-	A0011_1
明確な質問をする能力	-	-	A0012_1
小グループでの議論を促進する能力	-	-	A0016_1

1.2 講義を受講して得られる KSA

本講習を受講することで得られる知識および対応する NIST NICE Framework の K(Knowledge)・S(Skill)・A(Ability)を「表 2 講義を受講して得られる KSA」に示します。アンダーバーの後の数字は認知プロセスの次元を示します。例として、「検査ツール」の章を受講した場合、「K0177: Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).」に該当するナレッジが、認知プロセス「3 適用レベル」の次元で得られることを示します。

表 2 講義を受講して得られる KSA

章	Knowledge	Skill	Ability
脆弱性とは	K0005_2 K0009_2 K0296_2	S0001_2	A0015_2
脆弱性診断（セキュリティ診断）	K0013_2 K0290_2 K0046_2 K0339_2 K0342_2	S0001_2	A0015_2

NIST NICE FrameworkのKSA（Knowledge, Skill, Ability）に基づく教育コンテンツの事前スキル/取得スキル

情報セキュリティ基礎

- ✓ OS基礎
- ✓ OSコマンド基礎
- ✓ セキュリティ情報発信演習
- ✓ ネットワーク基礎
- ✓ ルーティング演習

情報セキュリティ管理

- ✓ 情報セキュリティ管理基礎
- ✓ セキュア開発
- ✓ セキュリティ規格
- ✓ セキュリティ対策技術
- ✓ クラウドセキュリティ
- ✓ スレッドインテリジェンス
- ✓ ハニーポット演習

各コンテンツには講師用解説として全ページ「目標」「説明の流れ」「ポイント」を記載

ペネトレーションテストおよび検証コード検証

- ✓ ペネトレーションテストの概要
- ✓ ペネトレーションテストの種類
- ✓ サイバーキルチェーン・ATT&CK
- ✓ ペネトレーションテストハンズオン
  - 公開サーバーテスト
  - AD侵入テスト

ハードニング演習

- ✓ ハードニング Bule Teams演習

※オレンジ色のコンテンツはハンズオン有り

2023年度新規開発演習教材

- **メールシステム**
  - ✓ SMTP
  - ✓ POP3　IMAP
  - ✓ メールの構造
  - ✓ MIME
- **無線LANとそのセキュリティ**
  - ✓ 無線LANの方式
  - ✓ 無線LANへの攻撃
  - ✓ 無線LANのアクセス制限
  - ✓ Bluetooth
  - ✓ Bluetoothへの攻撃
- **ソーシャルエンジニアリング**
  - ✓ フィッシング
  - ✓ 標的型攻撃
  - ✓ 水飲み場攻撃
- **暗号技術**
  - ✓ TMP HSM
- **基本的な攻撃**
  - ✓ クリスマス攻撃
  - ✓ エクスプロイト攻撃
  - ✓ ゼロデイ攻撃
- **物理セキュリティ**
  - ✓ セキュアエリア
  - ✓ ビデオ監視
  - ✓ クリアデスク
- **フォレンジック**
  - ✓ メモリ
  - ✓ HDD
- **セキュアプログラミング**
  - ✓ 入力検証とサニタイジング
  - ✓ エラー処理のコーディング規則
- **インシデント対応演習**
- **組込・OT**
  - ✓ SCADA
  - ✓ Stuxnet
  - ✓ IEC62443
- **ログ収集・分析**
  - ✓ Splunkなどを利用した相関分析
- **インストラクショントレーニング**

大学での演習教材利用事例

Future Works

今後の活動予定

Project> LETTICE

Leading Expert Team for Threat Intelligence Collection and Evaluation

Project> LETTICE

●Co-Nexus Aに脅威情報分析チーム “LETTICE” を設置

- ✓ CYNEXアライアンスメンバーより構成される脅威情報分析チーム
- ✓ Slackでの情報共有＋リアル会合でのコミュニケーション

●LETTICE会合参加ルール

- ✓ 開催頻度は月1回程度、リアル開催@NICT日本橋、チャタムハウスルール適用
- ✓ 発表は輪番形式、独自情報はTLP:RED扱い（発信者が許せばAMBER＋STRICT可）

●LETTICE会合で取り上げる内容

- ✓ インシデント公表された情報の整理、深堀、自身の知見に基づく評価
- ✓ 脆弱性情報の分析（深刻度、被害情報など）、悪用された脆弱性の一覧作成
- ✓ 観測情報の分析
- ✓ レポート・書籍を持ち寄り、概要紹介、書評
- ✓ 脅威アクターの分析（新しく登場したアクター、確認された手口など）
- ✓ 新たに脅威分析の検討が必要な動き etc.

プロジェクトイメージ

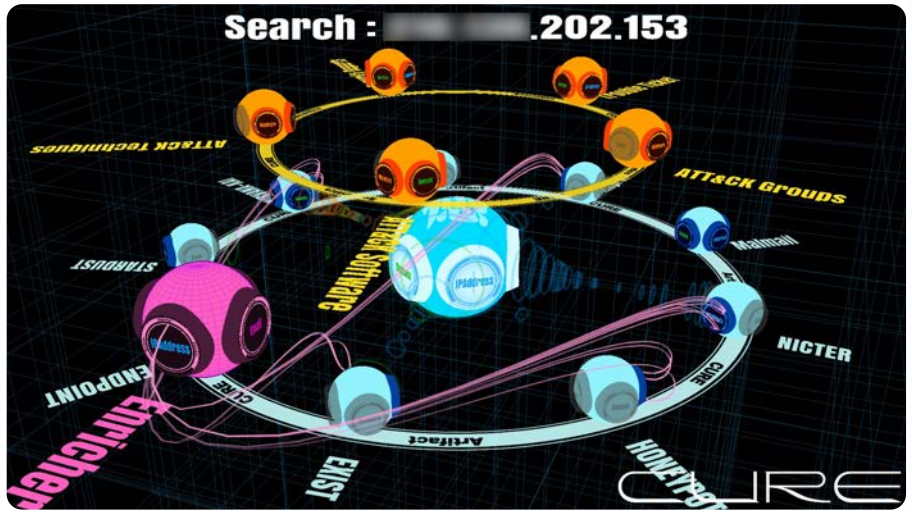
● 将来構想

- ✓ アライアンス参画組織への脅威分析結果の共有
- ✓ アライアンス参画組織からの要請による調査対応
- ✓ CYNEXの発信チャネル経由での情報発信
- ✓ スキルセットを整理し Co-Nexus Sへ展開
  （教育・訓練コンテンツの開発）

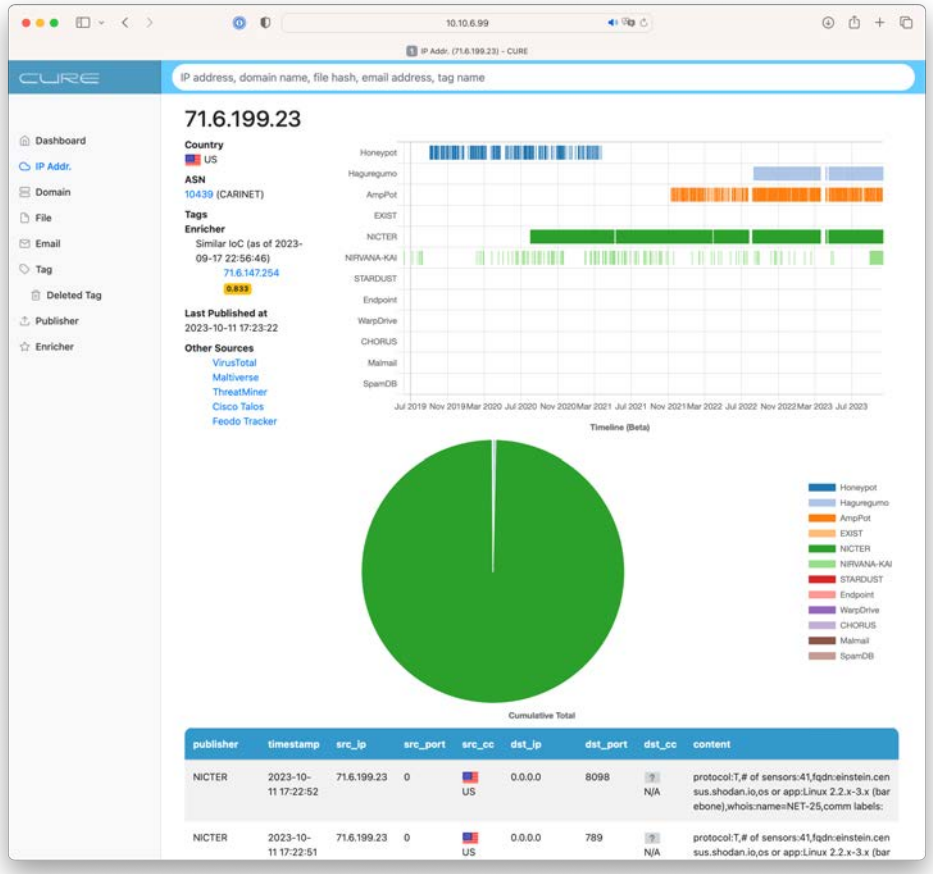
2024年2月初期メンバーで活動開始

セキュリティ情報融合基盤CURE 開放

- **CURE：NICTの収集データを統合する大規模DB**
- **Co-Nexus A/S向けに2023年度末開放**
- **検索可能データセット（予定）**
  - ✓ Honeypot
  - ✓ Haguregumo
  - ✓ AmpPot
  - ✓ EXIST
  - ✓ NICTER
  - ✓ STARDUST
  - ✓ CHORUS
  - ✓ SpamDB
  - ✓ ATT&CK
  - ✓ Security Reports
  - ✓ Social Media



CURE



CURE Web

CYNEX CYBERSECURITY NEXUS

How to Join CYNEX?

CYNEX参画方法

CYNEXアライアンス参画費用

●参加組織の種別、参画するCo-Nexus数に応じて参画費を設定

参画組織の種別	参画するCo-Nexus数と参画費の金額（年額、単位：千円）			
	1	2	3	4
大企業	1,000	1,500	1,800	2,000
中小企業	500	750	900	1,000
社団法人等	500	750	900	1,000
NPO法人	50	75	90	100
教育機関	50	75	90	100
官公庁	0	0	0	0
専門委員	0	0	0	0
特別会員	0	0	0	0

CYNEX参画申し込み・お問い合わせ先

CYNEX事務局

cynex@ml.nict.go.jp

つながる日本のサイバーセキュリティ

- 官：国産のセキュリティ製品を使う！
- 産：国産のセキュリティ製品を創る！
- 学：イノベーターを輩出する！