資料43－2－2

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）

2022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

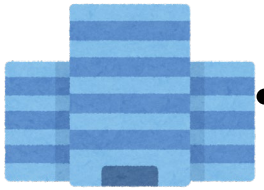
説明可能な国産脅威情報の生成・提供

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.

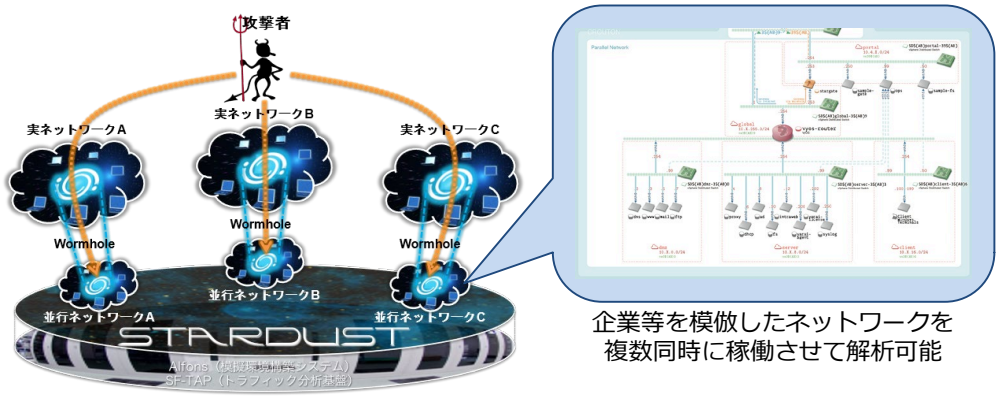
教育機関

4つの “Co-Nexus” によるプロジェクト推進

Co-Nexus A (Accumulation & Analysis)

参画組織数：37

- 目的：STARDUSTを核とした共同解析と解析者コミュニティ形成



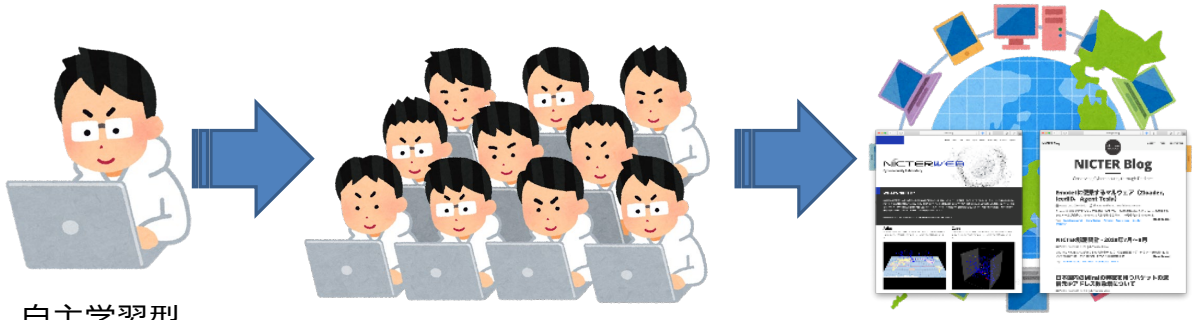
企業等を模倣したネットワークを
複数同時に稼働させて解析可能

サイバー攻撃誘引基盤STARDUST

Co-Nexus S (Security Operation & Sharing)

参画組織数：9

- 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

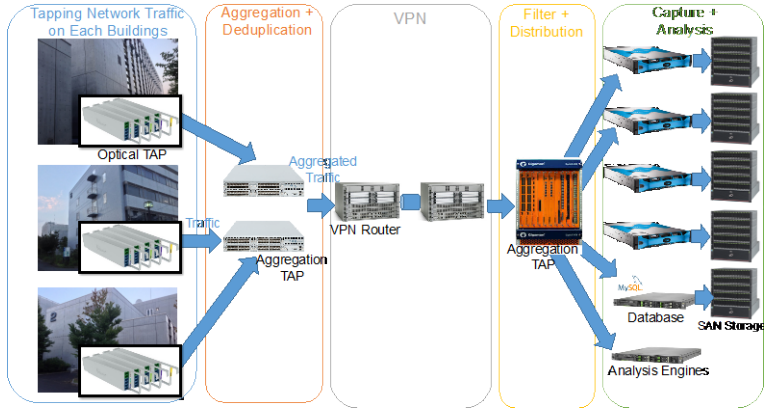
OJTでのSOC業務従事

国産脅威情報発信/提供

Co-Nexus E (Evaluation)

参画組織数：7

- 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



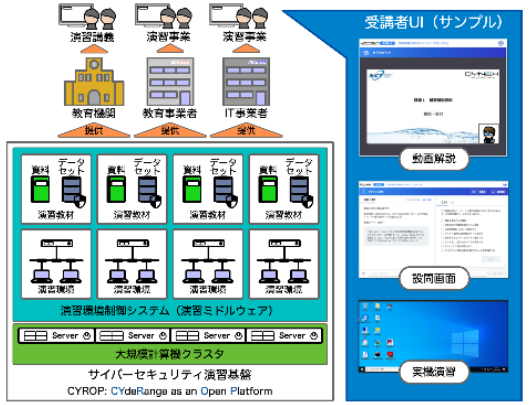
国産セキュリティ製品テスト環境（機構内部ネットワーク観測システム）

Co-Nexus C (CYROP*)

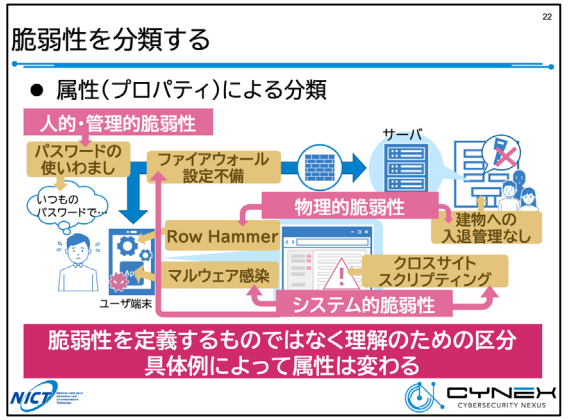
*CYROP: CYDERANGE as an Open Platform

参画組織数：16

- 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



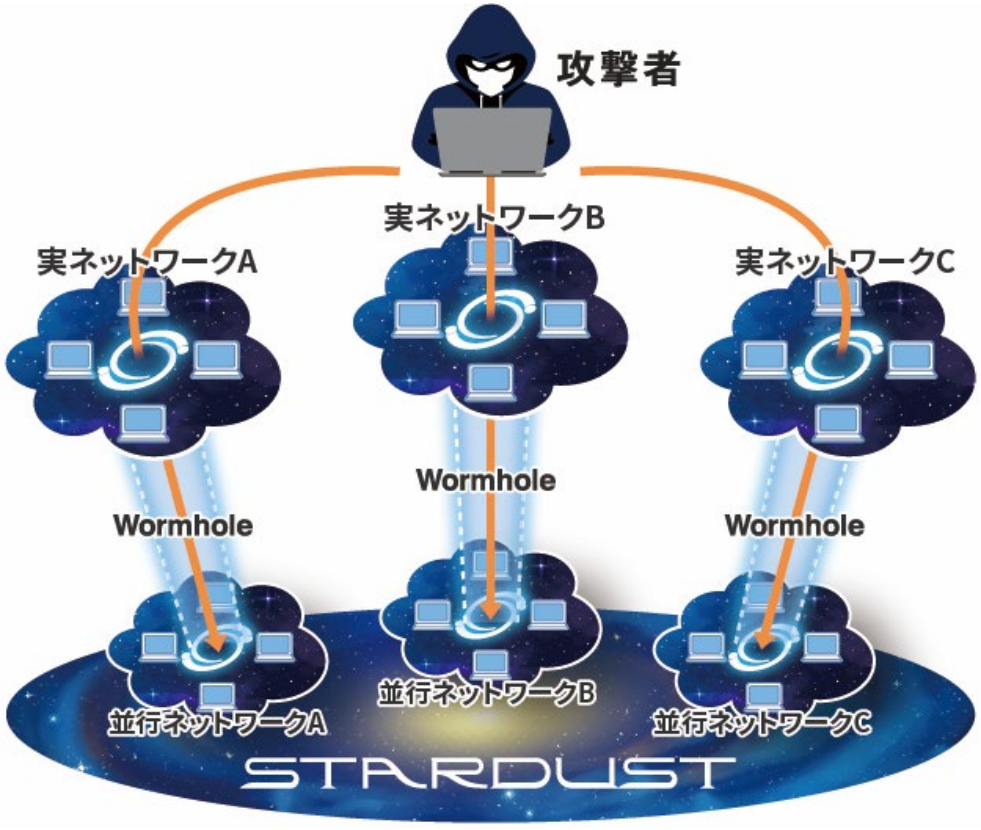
CYNEXオリジナル演習教材

Co-Nexus A：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**



サイバー攻撃誘引基盤STARDUST

● 2022年活動状況

✓ **37組織**から**70名以上**の解析者参画

✓ 年間**400件以上**の攻撃活動観測

✓ **解析者コミュニティ会合**定期開催

- 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
- DVRの脆弱性発見と対応事例
- EDRバイパス攻撃事例　　etc.

✓ **常時情報共有環境**の整備

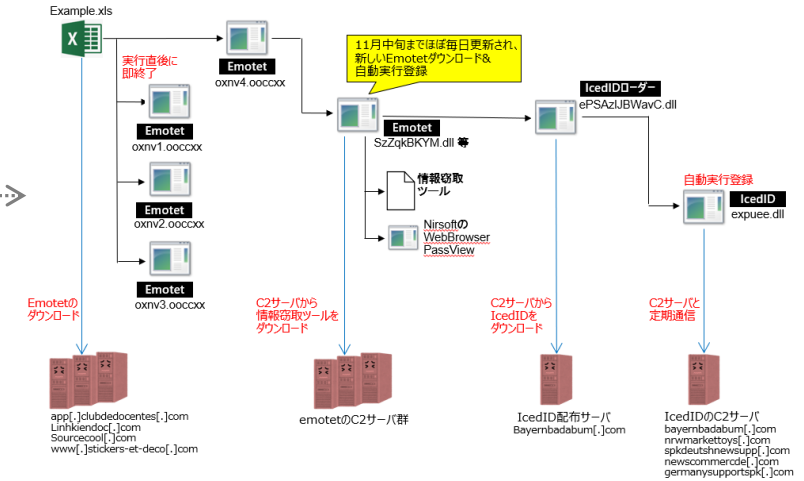
Co-Nexus A：攻撃活動観測・解析事例

● 攻撃活動観測 概要レポート（一部抜粋）

Case	実施期間		検体名称	進行度								実施結果
	開始	終了		1	2	3	4	5	6	7	8	
220810_CL12_001	2022/9/20	2022/9/20	Remcos								1	実行後、transfer.sh への接続を行っていたが、その他の動きが無かったため観測を終了
220828_CL12_002	2022/8/28	2022/8/29	OilRig		1							検体を実行するも、通信が発生せず、観測を終了
220819_CL12_003	2022/8/19	2022/8/19	Lazarus (Job Offer)					1				Coinbase のデコイを用いた Lazarus の転職希望者を狙う。接続先との通信が成立せず観測を終了。
220829_CL12_004	2022/8/29	2022/8/30	Lokibot		1							検体に解析環境検知機能があり、通信が発生せずにプロセスが即終了
220902_CL12_005	2022/9/2	2022/9/6	Lazarus (Dangerouspassword)									lnk ファイル実行後、子プロセスから C2 サーバーへの通信が発生したものの、以降は不審な通信や挙動が発生しなかったため、観測を終了
220905_CL12_006	2022/9/5	2022/9/6	Lokibot		1							検体に解析環境検知機能があり、通信が発生せずにプロセスが即終了
220907_CL12_007	2022/9/7	2022/9/9	Nanocore								1	1 次検体で nanocore、2 次検体で Formbook に感染し、C2 サーバーへの通信などを確認されたが、その後の継続的な攻撃が見られず観測を終了
220907_CL12_008	2022/9/7	2022/9/7	Formbook								1	SUTARDUST 環境ではプロセスインジェクションに失敗して終了
220914_CL12_009	2022/9/14	2022/9/14	Kimsuky			1						接続先に名前解決できず終了
220916_CL12_010	2022/9/16	2022/9/16	Kimsuky					1				C2 サーバーからエラーメッセージ(404)が返ってきて通信終了、以降不審な挙動も無し
220926_CL12_011	2022/9/26	2022/10/28	AgentTesla								1	途中から動きが見られなくなった。ディスク容量が足りなくなったため、攻撃が見られなくなった可能性も
220928_CL12_012	2022/9/28	2022/9/30	Konni									C2 サーバーへ端末情報を送付。その後、不審な挙動無し
221004_CL12_013	2022/10/4	2022/10/4	Kimsuky					1				2022/10/4 14:45 の時点で通信先が 404()
221012_CL12_014	2022/10/12	2022/10/12	Kimsuky			1						接続先に名前解決できず
221024_CL12_015	2022/10/24	2022/11/1	Royalroad sharppanda								1	観測初日のみ別の C2 サーバーと通信を行い、情報収集結果を送付
221104_CL12_016	2022/11/4	2022/11/9	Emotet									C2 サーバーとの定期通信のみを観測
221104_CL12_017	2022/11/4	2022/12/2	Emotet								1	情報窃取と外部メールサーバーへのメール配信試行(FW でブロック済),二次検体のダウンロードを観測
230117_CL12_018	2023/1/17	2023/2/17	Emotet								1	Emotet の検体更新と情報窃取は定期的に観測できたが、メール配信は観測できなかった。また、ダウンロードされた Emotet も前回キャンペーンとの差異は見られなかった。その後、不審な通信や挙動が発生しなかったため、観測を終了した。

STARDUSTで観測した攻撃の進行度
（1：検体実行不可 ～ 8：継続的に攻撃発生）

● 攻撃活動観測 詳細レポート（一部抜粋）



● NanoCore RATの攻撃者の挙動一覧

分類	行動
メール	Outlook を開く
	受信トレイを確認する
	送信済みアイテムを確認する
	下書きを確認する
	ユーザのアカウント情報を確認する
	特定のメールを検索する
	メールの送信を試みる
ブラウザ	Chrome や Internet Explorer を開く
	Google アカウントへのログイン状況を確認する
	言語設定を英語に変更する
	ブックマークを確認する
	ブックマークされたページを開く
	特定のページを開く（PayPal，Alibaba，xvideos など）
	閲覧履歴を確認する
	特定のツールをダウンロードする
	よくアクセスするページや最近閉じたタブを確認する
権限昇格	管理者権限を要求する

分類	行動
ファイルアクセス	デスクトップ上のファイルやフォルダを開く
	最近表示した場所を開く
	ファイルを圧縮する
	ネットワークドライブを確認する
	ファイルを C2 サーバにアップロードする
	他のマルウェアを実行する
	NanoCore クライアントを更新する
	NanoCore クライアントをアンインストールする
	スタートメニューからアプリやファイルを検索する
アカウント情報	ブラウザに登録されたパスワードを窃取する
	メーラーに登録されたアカウント情報を窃取する
ネットワーク接続	タスクバーのネットワークアイコンから通信状況を確認する
	コントロールパネルのネットワークと共有センターを確認する
コマンド	ipconfig，net view コマンドを実行する
	systeminfo コマンドを実行する
その他	NjRAT チャット機能で話しかけてくる
	操作できないようにするために画面をロックする

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

✓自主学習型オンラインコースとCYNEX解析チームでのOJTコース

✓サイバーセキュリティ関連情報の発信機能のCYNEXへの集約と強化

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

● 2022年活動状況

✓ **オンラインコース&OJTコース**
- オンラインコース：1期生6名、2期生8名 修了
- OJTコース：CYNEX解析チームで1名育成中（2年間）

✓ **NICTERレポート**, **Blog**, **Twitter**
- NICTER観測レポートQ1, Q2, Q3, Q4, 2022
- NICTER Blog：8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

✓ **DVR製品の脆弱性***報告・公表

* 脆弱性：CVE-2022-35733

Co-Nexus S：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

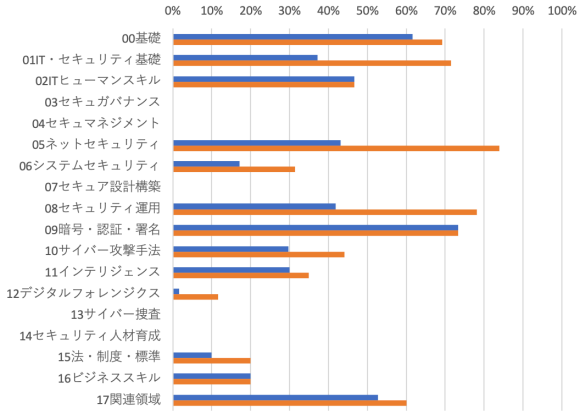
● OJTコース（2年間）

- ✓ 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

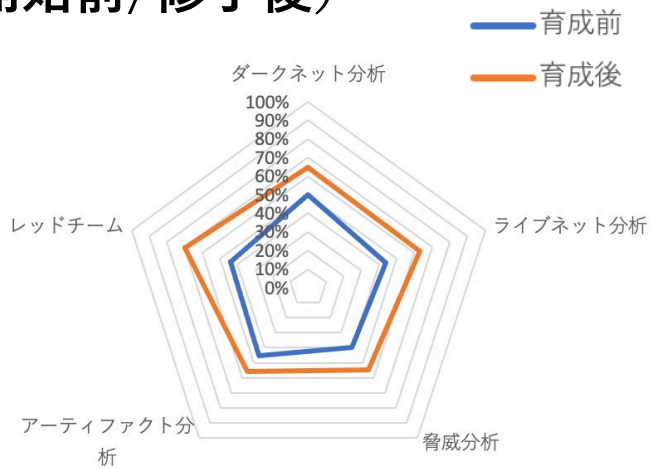
CYNEX解析チームでのOJTの様子

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

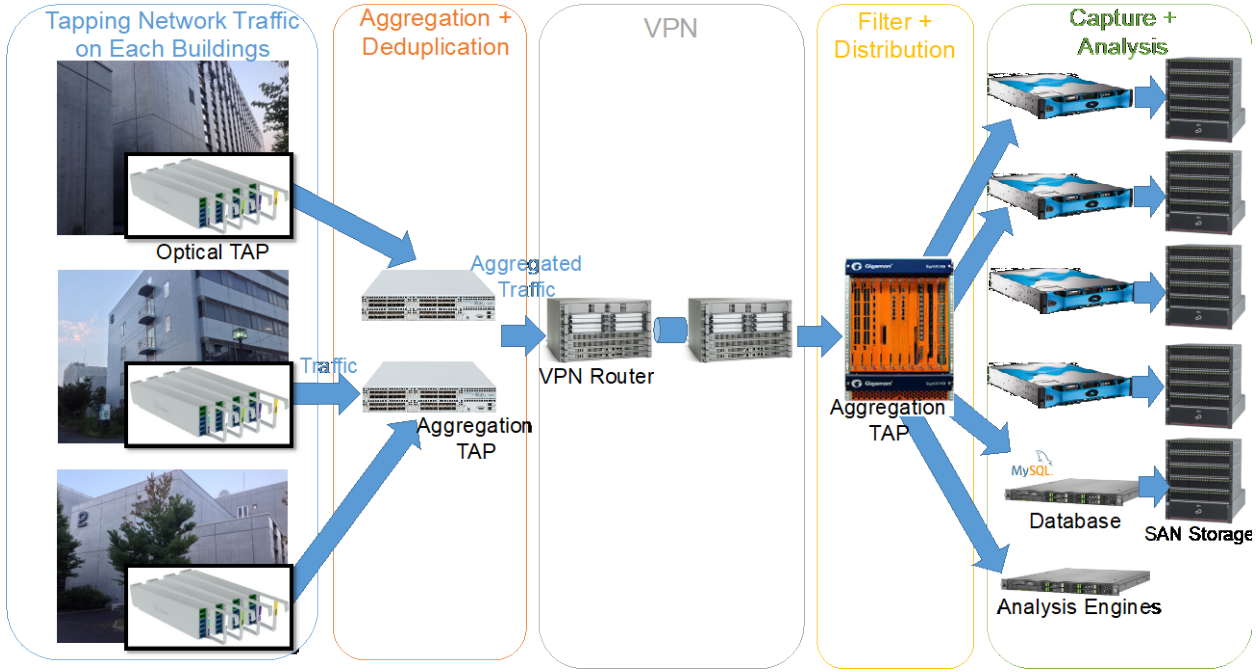


スコープ別適合率

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**（攻撃チーム）による模擬攻撃を用いた機能検証



Co-Nexus E セキュリティテスト環境（機構内ネットワーク）

● 2022年活動状況

- ✓**7企業の製品の長期検証**を開始
- ✓各製品ごとに**カスタム検証環境構築**
- ✓**CYNEX Red Team**による模擬攻撃
- ✓海外有力製品との**比較検証**
- ✓民間企業への**フィードバック**

Co-Nexus E：運用・検証事例

● 検証の流れ

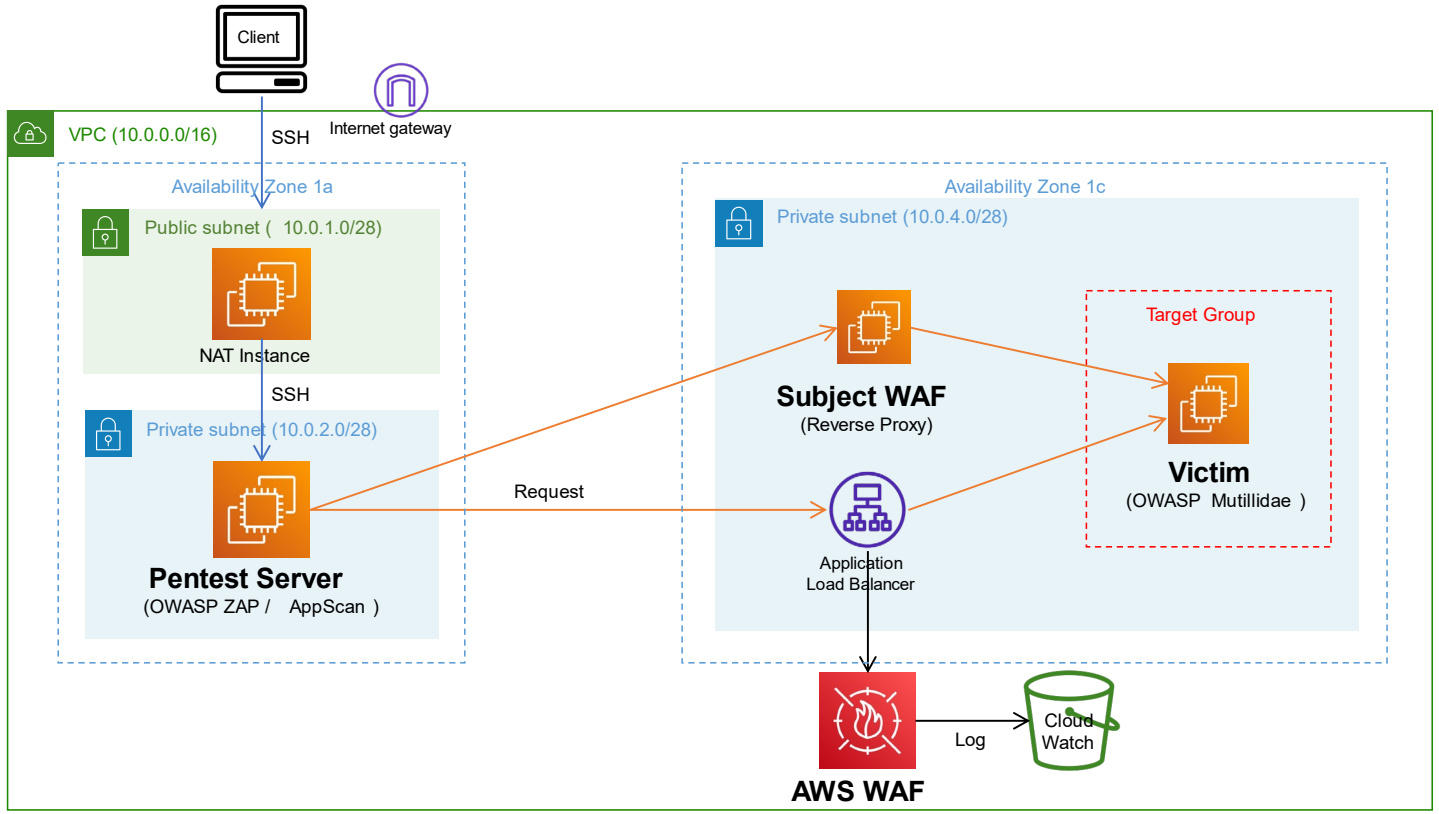
- 共同研究契約（NDA）
- 検証要件のヒアリング
- カスタム検証環境構築
- CYNEX Red Team による検証
- 検証結果のフィードバック

● 検証中の製品種別

製品種別	運用・検証内容
WAF（Web Application Firewall）	運用されている製品の精度検証
ペネトレーションツール	ツールの高度化及び長期運用
ファジングツール	アルゴリズムの精度検証
統合分析ソリューション	新たな分析軸の検証
IP レピュテーションサービス	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	新たなマルウェアへの適応検証

● カスタム検証環境での運用・検証事例（WAF）

- ✓ AWS上にWebアプリケーション攻撃検証のための仮想環境を構築
- ✓ 脆弱性を持つWebアプリケーションを稼働（OWASP Mutillidae）
- ✓ 検証対象となるWAF製品を導入（Subject WAF）
- ✓ 各種ペンテストツールを用いた攻撃（OWASP ZAP/AppScan等）
- ✓ 既存のWAF製品（AWS WAF等）との比較検証

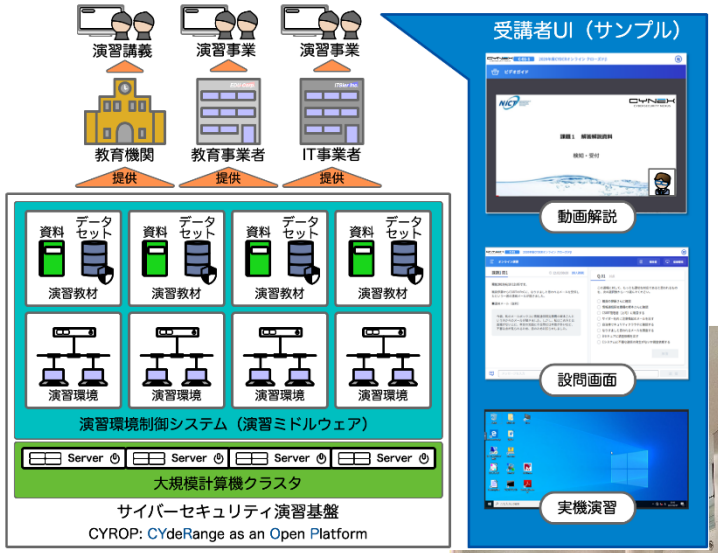


Co-Nexus C：人材育成オープンプラットフォーム

●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

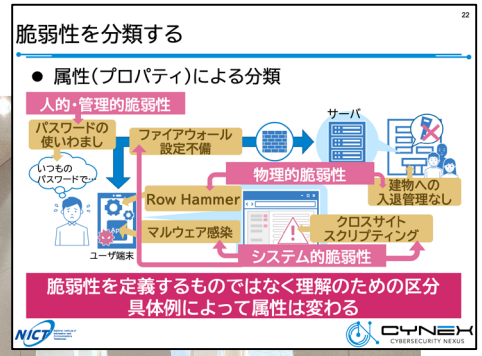
✓サイバーセキュリティ演習に必要となる**演習環境と演習教材をオープン化**

✓米国NIST NICE Frameworkに基づいた演習教材の段階的整備



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



大学での
演習教材利用事例

● 2022年活動状況

✓大学/民間企業など**16組織**が参画

✓**CYROPオープン化トライアル中**

- CYDER Aコース由来 演習教材
- CYDER Bコース由来 演習教材
- CYNEX オリジナル 演習教材

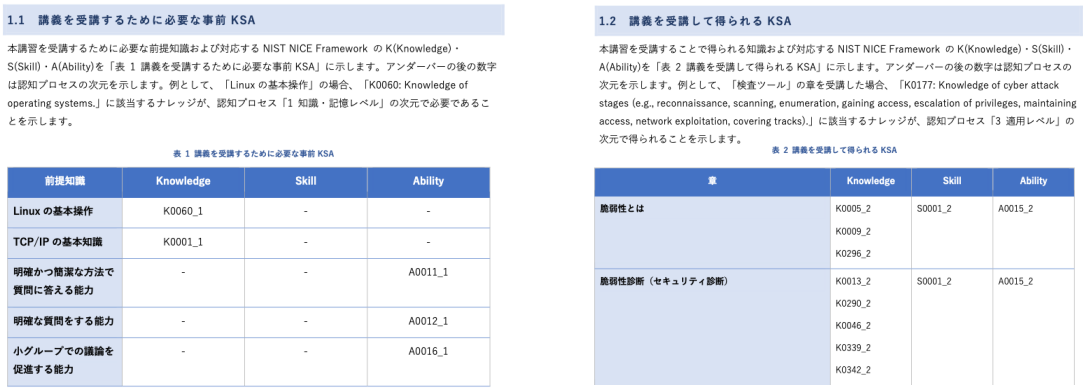
✓教育機関向け人材育成教材など
新規演習教材の共同開発を継続

CYNEX

Co-Nexus C：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

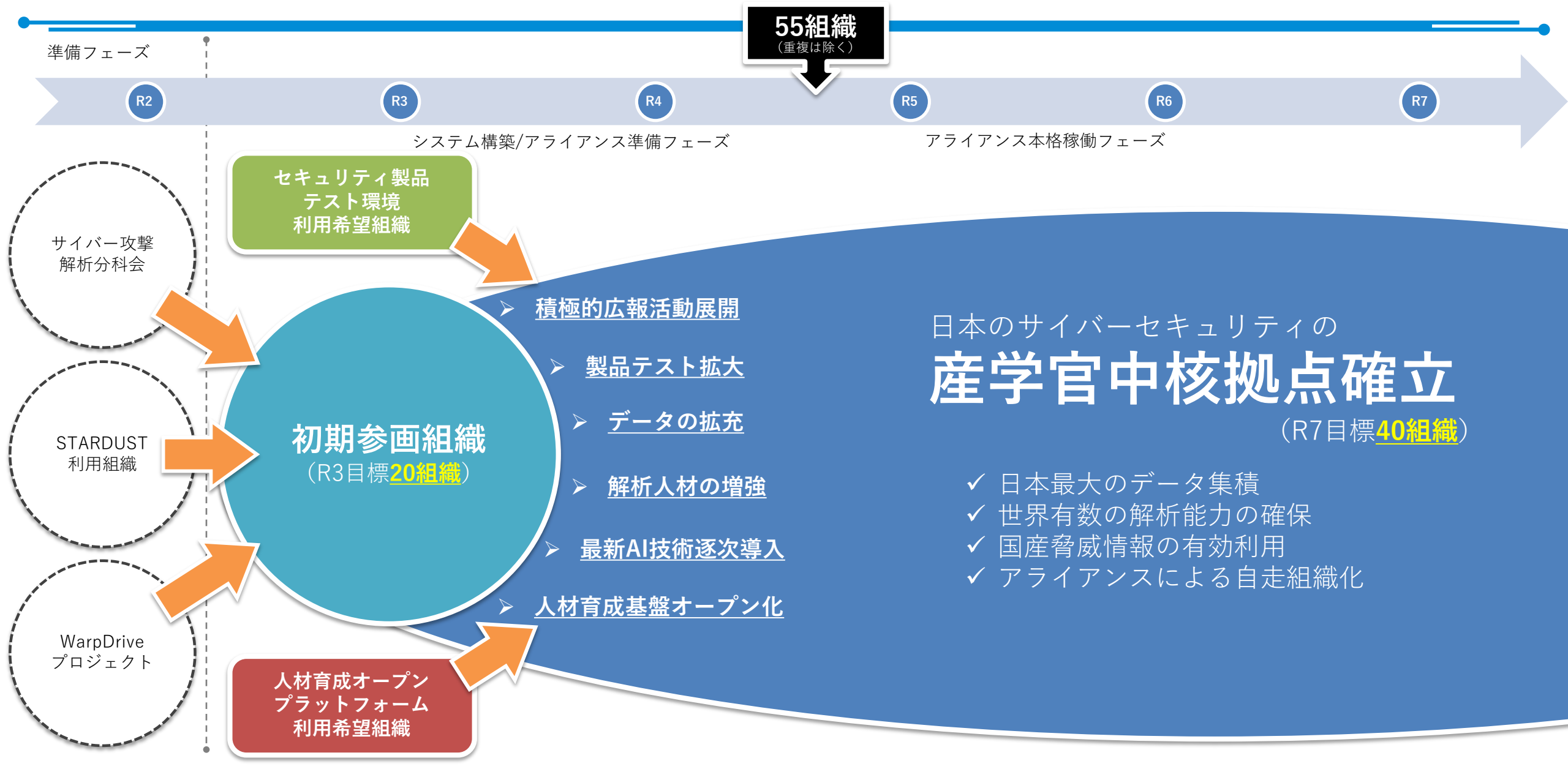
各コンテンツには講師用解説として全ページ「目標」「説明の流れ」「ポイント」を記載

- **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

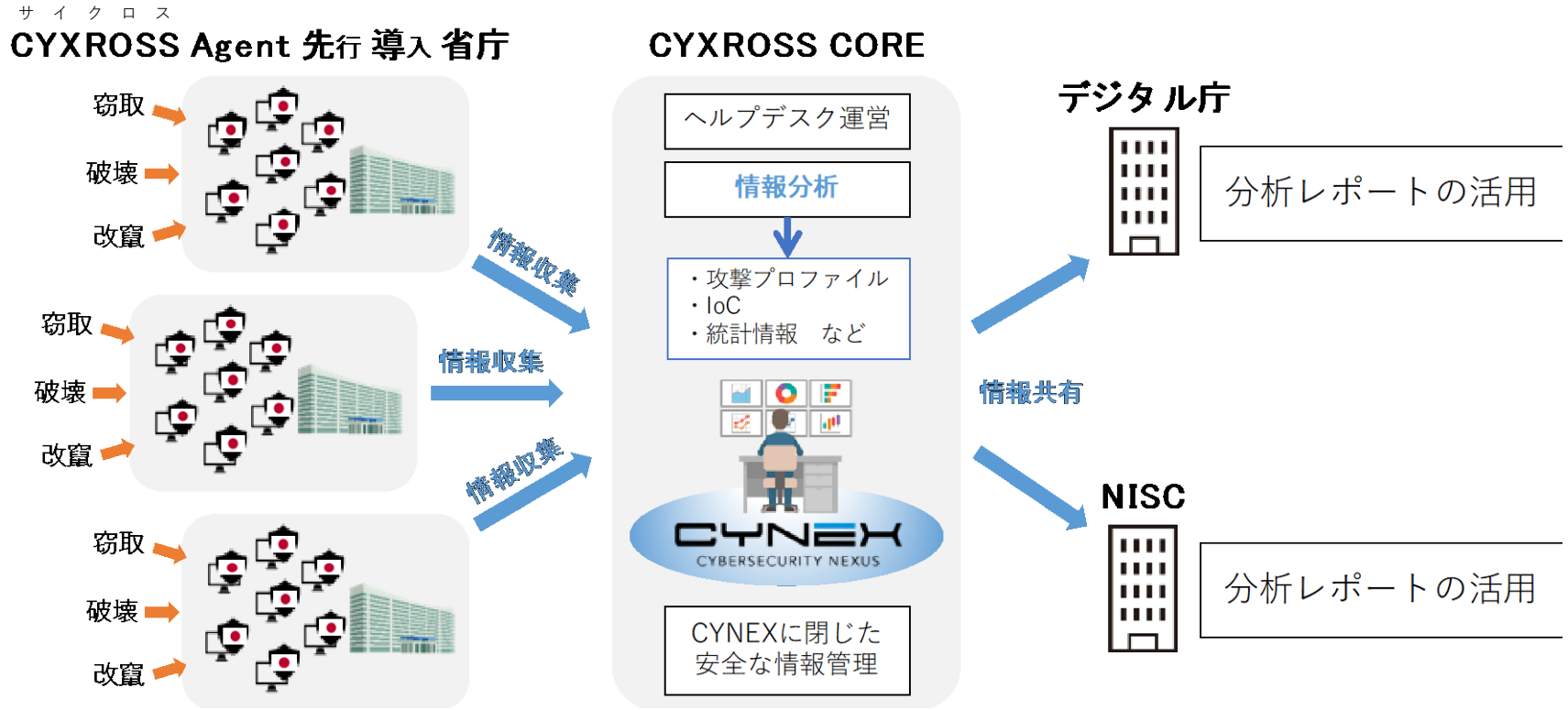
- **ハードニング演習**
  - ✓ ハードニング Bule Teams演習

※オレンジ色のコンテンツはハンズオン有り

CYNEXの事業展開のタイムライン



- **安全性や透明性の検証が可能な国産セキュリティソフト**を政府端末に導入し、得られたマルウェア情報等をCYNEXにおいて集約・分析する実証事業を実施



✓ 国産セキュリティソフト『CYXROSS Agent』（仮称）を政府端末に導入し情報収集
✓ NICT CYNEXで**組織横断的情報分析**を行い、デジタル庁やNISC等に情報共有

CYNEX参画申し込み・お問い合わせ先

CYNEX事務局

cynex@ml.nict.go.jp