資料28－1

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)

の構築について

令和３年２月８日

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

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NICTに構築し、産学官の**結節点**として開放することで、サイバーセキュリティ対応能力の向上を図る。

（令和２年度三次補正予算：85.2億円／令和３年度当初予算案：7.0億円）

STARDUST
サイバー攻撃誘因基盤

NICTER
サイバー攻撃観測網

各種外部情報

CYDER
実践的サイバー防御演習

サイバーコロッセオ
オリパラ関係者向けサイバー演習

民間が有する各種演習教材

成果展開

成果展開

教材変換インタフェースの開発・標準化

サイバー攻撃分析環境

情報

大規模集約データベース

情報

セキュリティ機器テスト環境

最新の攻撃情報（演習教材に反映）

相互補完

受講者の挙動（攻撃分析に活用）

演習教材提供環境

演習用大規模計算機環境

受講者挙動DB

AIを駆使した大規模横断分析＋付加価値の付与

根拠・背景等が
説明可能な国産セキュリティ情報

提供

政府機関・セキュリティ機関等

- マルウェア情報
- 指令サーバ情報
- 攻撃元IPアドレス情報
- 攻撃者/攻撃手法情報 等

コミュニティ形成による連携

人材育成事業者　教育機関　ICTベンダ

サイバーセキュリティに関する産学官の結節点『CYNEX』

- 情報通信研究機構（NICT）では、これまでも次のような取組を実施
  サイバーセキュリティ研究所・・・最先端のサイバーセキュリティ関連技術の研究開発を実施
  ナショナルサイバートレーニングセンター・・・実践的サイバー防御演習等による人材育成を実施
- これらの知見を活用し、サイバーセキュリティに関する産学官の巨大な結節点となる先端的基盤として
  ＣＹＮＥＸ（Cybersecurity Nexus：サイネックス） を構築予定

サイバーセキュリティ統合知的基盤

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戦略本部 研究開発戦略専門調査会（2019年5月17日）

● データ負けのスパイラル

✓ データが集まらない → 研究開発できない → 技術を作れない
→ 技術が普及しない → データが集まらない → …

● 今、日本に必要なこと

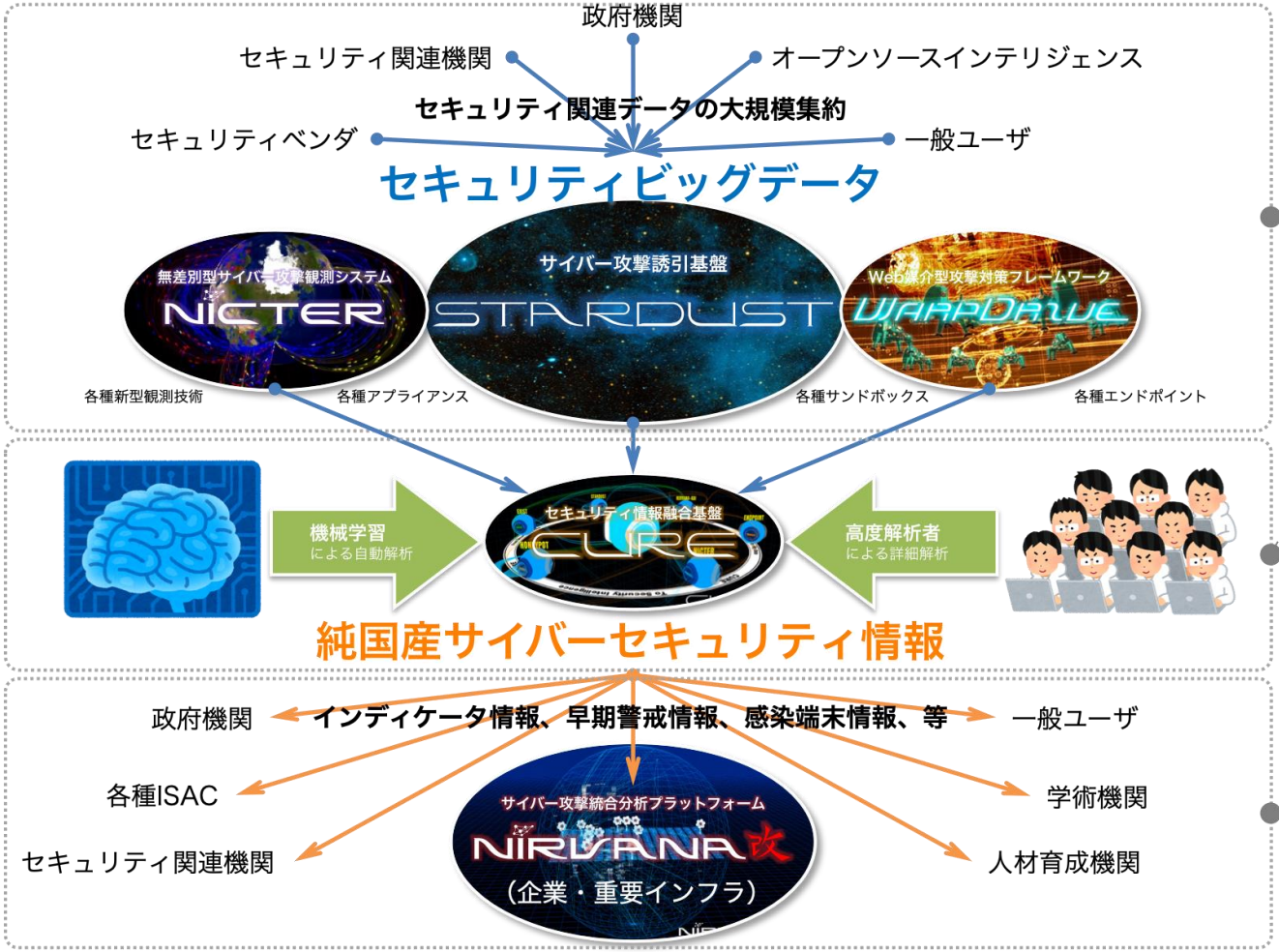
✓ 実データを大規模に収集・蓄積する仕組み
✓ 実データを定常的・組織的に分析する仕組み
✓ 実データで国産製品を運用・検証する仕組み
✓ 実データから脅威情報を生成・共有する仕組み

これらの仕組みの実現を目指す産学官の結節点

CYNEX を構築
Cybersecurity Nexus

サイバーセキュリティ統合知的基盤の構想

NICTER、STARDUST、WarpDrive等の観測機構を活用し、**セキュリティビッグデータ**を収集。
人と機械との連携による定常的・組織的な分析を行い、**純国産サイバーセキュリティ情報**を生成。
加えて、実データを用いた**国産セキュリティ製品の運用・検証**や、**高度SOC人材育成**を実施。



大規模収集・蓄積

- 産学官から情報集約
- OSINTの大規模収集
- NICTの研究成果を活用
  ➡ NICTER, STARDUST, WarpDrive

定常的・組織的分析

- 高度解析者の結集・育成
- 機械学習技術の定常運用
- NICTの研究成果を活用
  ➡ CURE, AI x Cybersecurity

国産製品運用・検証

- 国産製品のプロトを長期運用
- 海外製品群との比較検証
- NICTのLANをテストベッド化
  ➡ NICTER解析チーム

脅威情報生成・共有

- 高度解析者による脅威情報生成
- 産学官への迅速な共有
- NICTの研究成果を活用
  ➡ NIRVANA改

サイバーセキュリティ統合知的基盤の活動内容

大規模収集・蓄積

1. STARDUST等のセミオープン※化

- ✓ STARDUSTを産学に半開放し大規模並列解析
- ✓ 共同分析を通して国内解析者コミュニティを醸成

※セミオープン：信頼できるCYNEXの参画機関にSTARDUSTを開放

定常的・組織的分析

2. 高度SOC人材育成

- ✓ 産学官から高度解析者を集結
- ✓ 高度SOC人材育成プログラムによる教育

国産製品運用・検証

3. 実環境での国産製品の長期運用・検証

- ✓ 実ネットワークのデータ利用による検証環境
- ✓ 国産製品を長期運用・機能検証

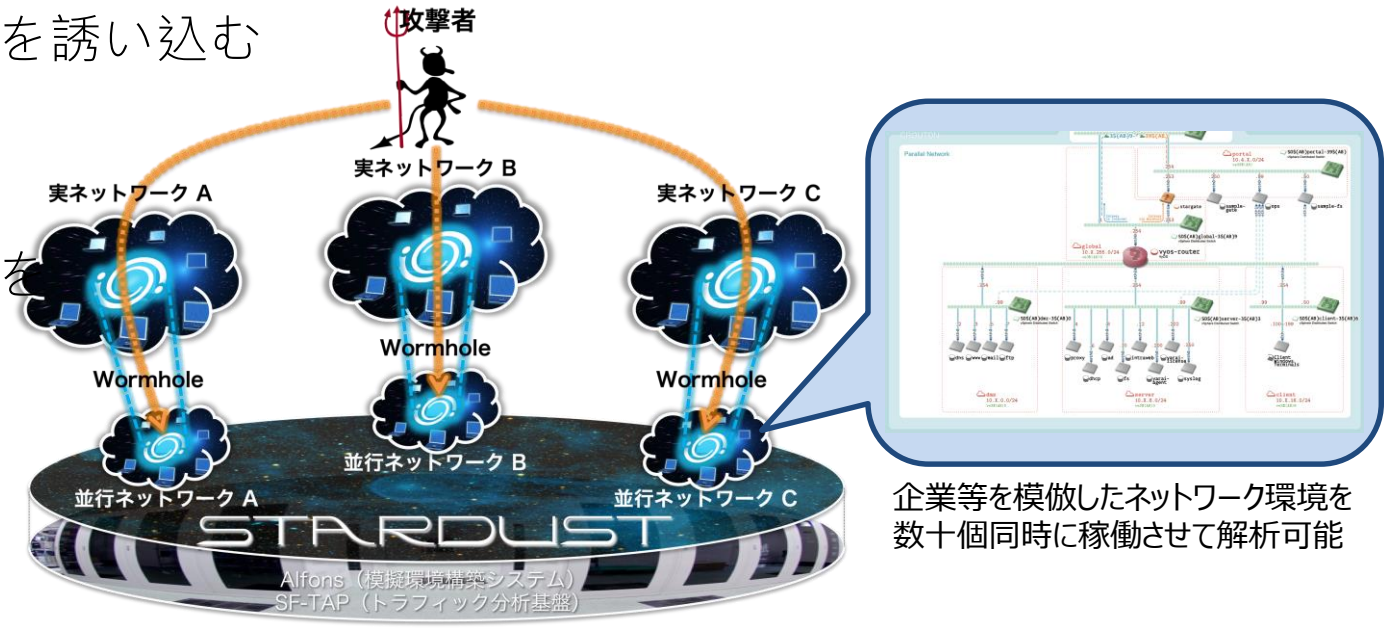
脅威情報生成・共有

4. 純国産サイバーセキュリティ情報の生成

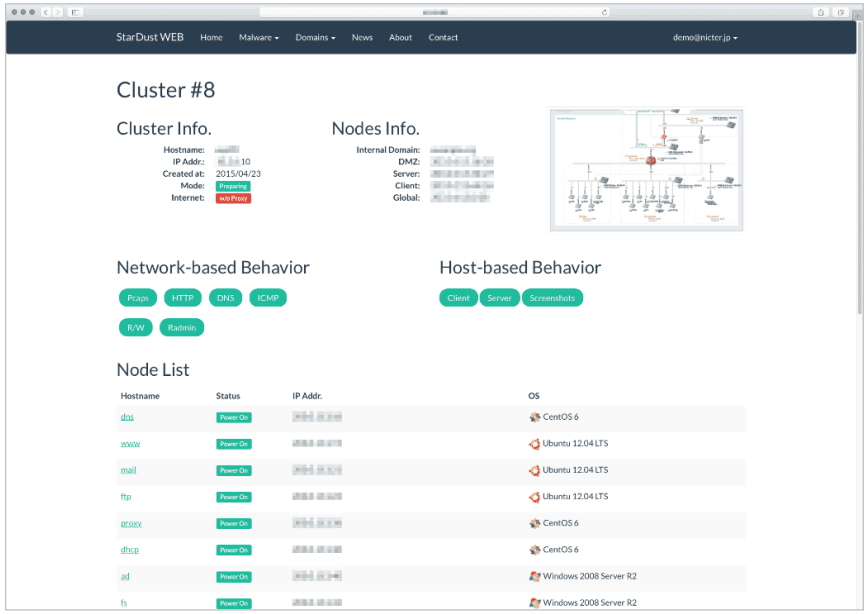
- ✓ 各種データを機械学習等と高度解析者により統合分析
- ✓ 説明可能かつ即時的な純国産IoCを生成・発信

STARDUSTのセミオープン化

- 標的型攻撃等の攻撃者を誘い込む<u>サイバー攻撃誘引基盤</u>
- 組織を精巧に模擬した“<u>並行ネットワーク</u>”を高速・柔軟に自動生成
- 並行ネットワーク中で攻撃者を長期誘引し、<u>ステルスに挙動を解析</u>



企業等を模倣したネットワーク環境を数十個同時に稼働させて解析可能



STARDUST Web

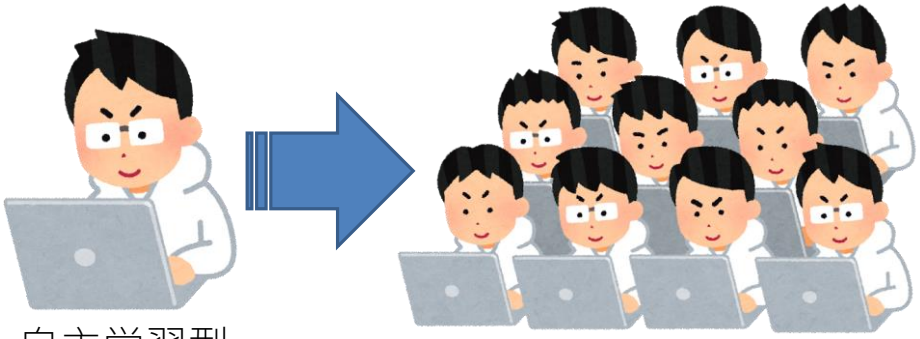
■ <u>STARDUSTのセミオープン化</u>

- ✓ 参画組織ごとにカスタマイズされた<u>並行ネットワークを貸し出し</u>
- ✓ STARDUST Web経由の遠隔解析
- ✓ 定期的な解析情報の交換を通した<u>解析者コミュニティの醸成</u>
- ✓ <u>All Japanでの共同解析</u>を実現する大規模並行ネットワークの構築

高度SOC人材育成

- NICTER解析チームにおいて
  定常的分析業務を実施
- ダークネット分析（Global観測）
- ライブネット分析（Local観測）
- 機構内インシデント対応
- 研究開発成果のテスト稼働

NICTERオペレーションルーム



自主学習型
高度SOC研修

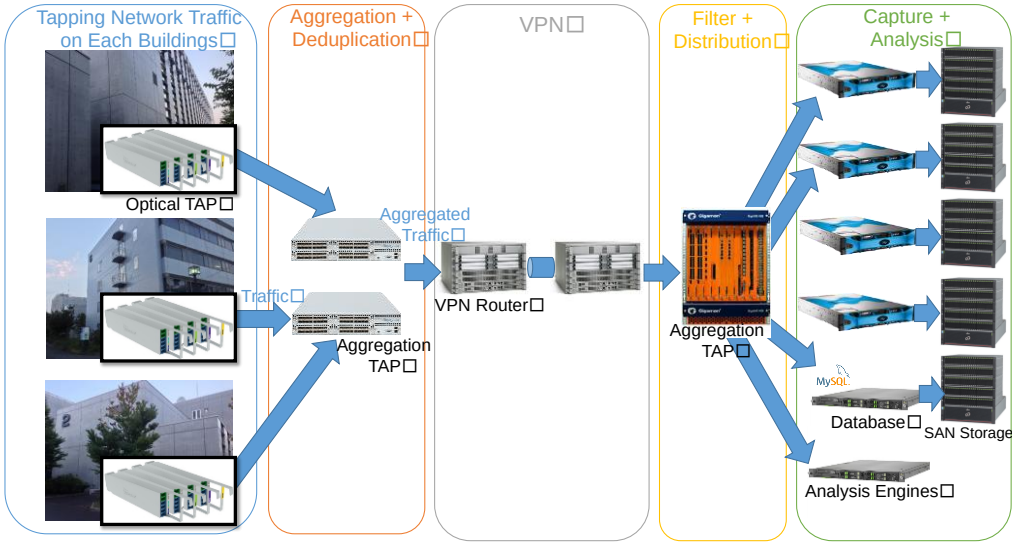
OJTでのSOC業務従事

■ 高度SOC人材育成

- ✓ NICTER解析チームでの人材育成
- ✓ 参画組織からの育成人材受け入れ
- ✓ 自主学習型高度SOC研修
- ✓ OJTでのSOC業務従事
- ✓ 多数の海外製/国産製品を用いた
  複合的オペレーションを経験可能に

国産セキュリティ製品の運用・検証

- 実ネットワークのデータ利用による<u>セキュリティ製品テスト環境化</u>
- ネットワークトラフィックを<u>リアルタイムにキャプチャ</u>し大規模DBに数年分の通信を蓄積
- PC数百台に観測エージェント導入
- <u>海外製有力セキュリティ製品</u>を複数機種稼働（比較評価用）



NICT内部ネットワーク観測システム

富士通 標的型攻撃発見サービス

AlaxalA AX-3D-View

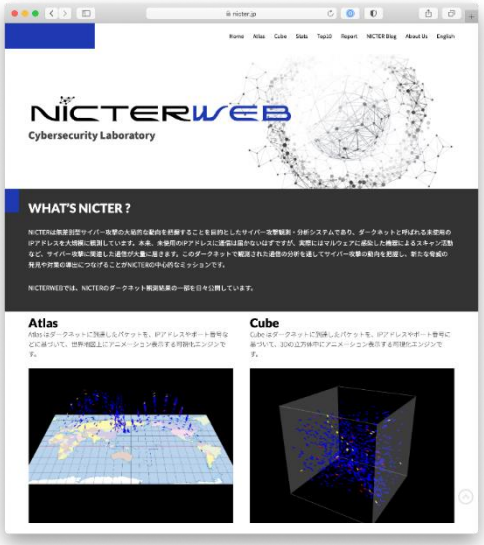
NICTにおける製品運用・検証の先行事例

■ <u>国産セキュリティ製品運用・検証</u>

- ✓ 参画組織による製品プロト持ち込み
- ✓ 参画組織からの技術者受け入れ
- ✓ <u>NICT-CSIRTでの製品長期稼働</u>
- ✓ <u>実攻撃および模擬攻撃によるテスト</u>
- ✓ テスト結果のレポーティング

純国産サイバーセキュリティ情報の生成

- NICTから<u>サイバー攻撃関連の情報を様々な形態で発信・共有中</u>
- <u>NICTER Web</u>
  - ✓ ダークネット観測結果を自動配信
- <u>NICTER観測レポート</u>
  - ✓ ダークネット等の詳細分析結果を定期公開
- <u>NICTER Blog</u>
  - ✓ 様々な分析結果についてタイムリーに発信



NICTER Web と NICTER Blog

<u>サイバーセキュリティ情報の生成</u>

- ✓ 機械学習エンジンと解析チームによるサイバー攻撃の自動解析/詳細解析
- ✓ <u>情報源が明確で説明可能性の高い純国産インディケータ情報（IoC）生成</u>
- ✓ <u>CYNEX参画組織内での情報共有</u>
- ✓ CYNEX外への情報共有・情報発信

サイバーセキュリティ人材育成基盤

セキュリティ人材育成に関する課題 （NICTによる国内有識者へのヒアリング結果より）

我が国はサイバーセキュリティ自給率が他国に比べて低く、サイバー演習においても海外製の演習環境やシナリオに依存しがち。日本特有のインシデント事例等が活用されていないことが、安全保障の観点において大きな課題

セキュリティ関連団体

民間の教育事業者

演習用の環境構築やシナリオ開発には高度な知識や技術力が必要となるが、これらに単一組織だけで取り組むのは非常に効率が悪いため共同開発体制が必要。それと並行して教材フォーマット等の標準化も重要

演習事業の実施にあたっては、その基盤となる計算機環境や演習システムが必要となるが、その構築と維持には高い技術力が必要であり、単一組織での構築・長期的運用は困難

教育機関

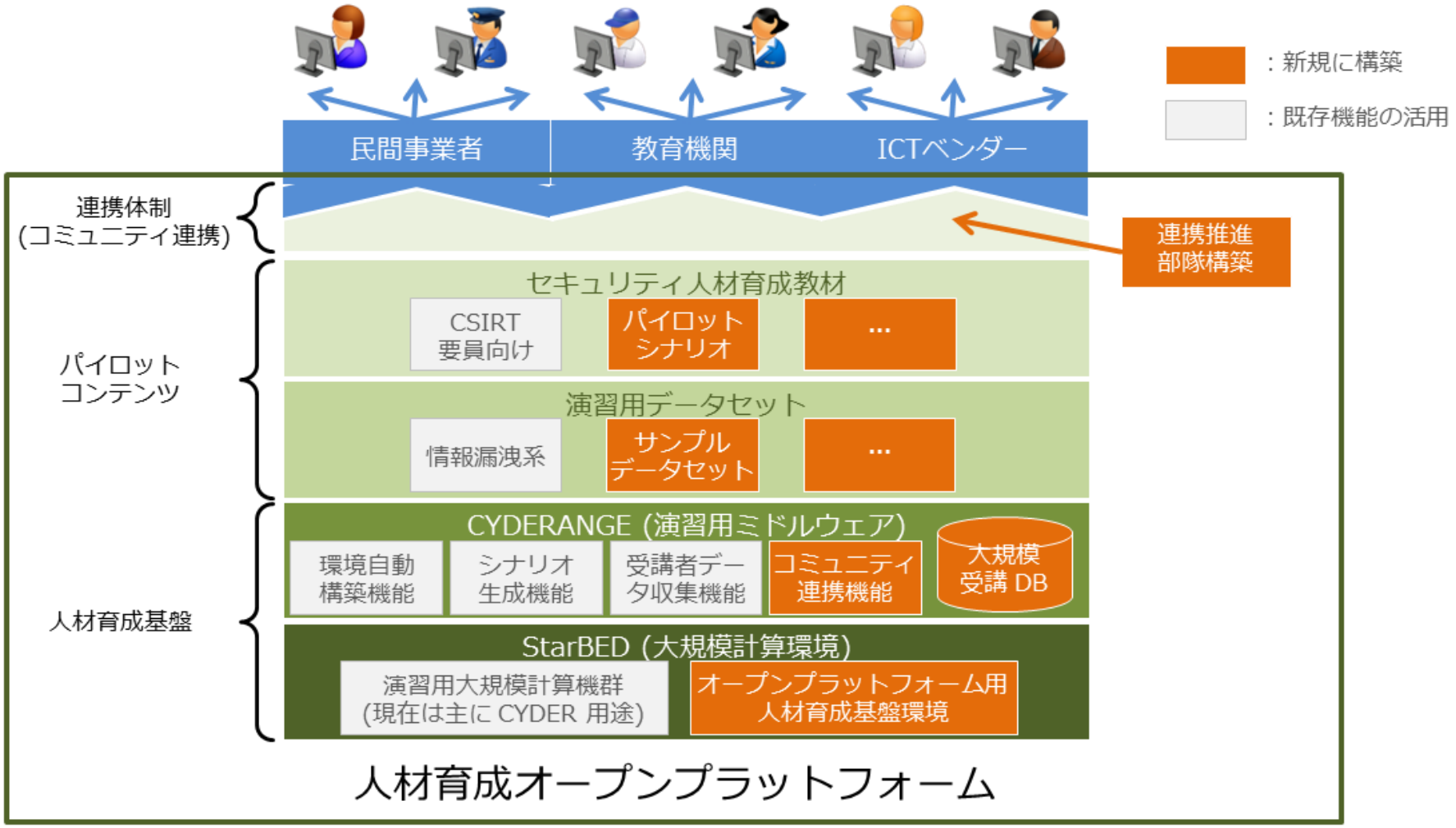
よりオープンな人材育成環境と協力体制の必要性

- ✓ 我が国ならではの演習コンテンツ開発体制の実現
- ✓ 各組織が持つ既存の演習コンテンツの共有や、相互活用と共同開発を実施
- ✓ 産学官が連携して教材・環境の標準化を進め、社会全体での開発効率を向上
- ✓ 基盤となる計算機環境についても産学官が (相応の対価の下で) 共同利用

これらの仕組みを実現する
産学官の結節点
CYNEX を構築
Cybersecurity Nexus

サイバーセキュリティ人材育成基盤の構想

- ナショナルサイバートレーニングセンターで構築した CYDERANGE、演習シナリオ等の人材育成基盤をオープン化し、民間事業者や教育機関における人材育成事業を促進する。
- このための基盤を、人材育成オープンプラットフォームとして整備。



サイバーセキュリティ人材育成基盤の活動内容

1. 人材育成コミュニティ（連携体制）の慫慂

- ✓ 民間事業者や教育機関等のヒアリング（ユーザニーズ調査）
- ✓ 連携先機関が活用し易いライセンス形態の整理
- ✓ 大規模受講データベース等を活用した民間事業者や教育機関等との共同研究開発

2. 人材育成基盤の開発、構築

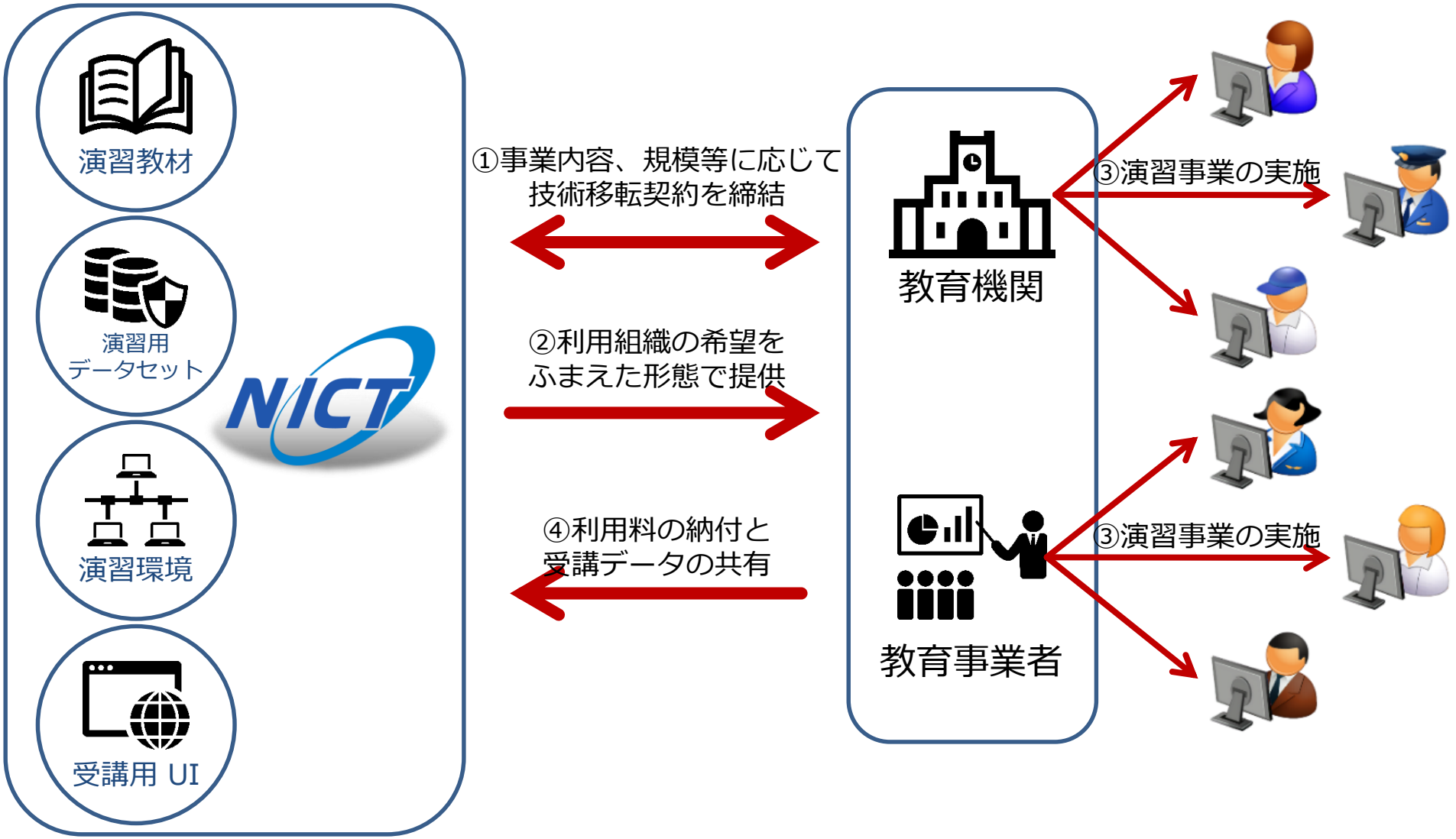
- ✓ 接続用API、オンライン演習用ユーザインターフェイス等のCYDERANGE (演習用ミドルウェア) の高度化
- ✓ 受講データを収集する大規模受講データベースの構築
- ✓ 演習用ミドルウェアを支える大規模計算環境の構築

3. 人材育成基盤利用促進のためのパイロットコンテンツ開発

- ✓ 既存コンテンツをベースに、よりユーザニーズに適合したパイロットコンテンツ (パイロットシナリオ・サンプルデータセット等) を開発
- ✓ 社会的な需要に応じ、システム構築技術者、システム開発者、一般の SOC 担当者等のセキュリティ対応力向上を目的としたコンテンツを開発予定

人材育成オープンプラットフォームのサービス提供イメージ

- 利用希望組織は、事業内容、事業希望等に応じて、プラットフォーム利用のための技術移転契約を NICT と締結
- NICT は利用組織の希望をふまえて、演習教材、演習用データセット、演習環境、受講用ユーザーインターフェース (UI) 等のすべて、または一部を提供



CYNEXの事業展開のタイムライン

CYNEXの事業展開のタイムライン