# つなげるセキュリティトレーニング

サイバーセキュリティネクサス
佐藤公信

# 博士（工学）CISSP 佐藤公信

肩書き
・国立研究開発法人情報通信研究機構（NICT）サイバーセキュリティネクサス主任研究員
・SEC道後プログラム検討会委員
・情報処理安全確保支援士実践講習講師
・SecHack365表現駆動コースコースマスター

資格
・(ISC)² CISSP
・CompTIA CTT+

経歴
・高知工科大学大学院　博士（工学）
・高知工科大学　地域連携機構　助教
・高知工業高等専門学校　電気情報工学科　助教
・高知工業高等専門学校　ソーシャルデザイン工学科　准教授

研究
・Deep Learningによるパターン認識，産業応用

# 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

## 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


安部 小百合
NICT


佐藤 公信
NICT

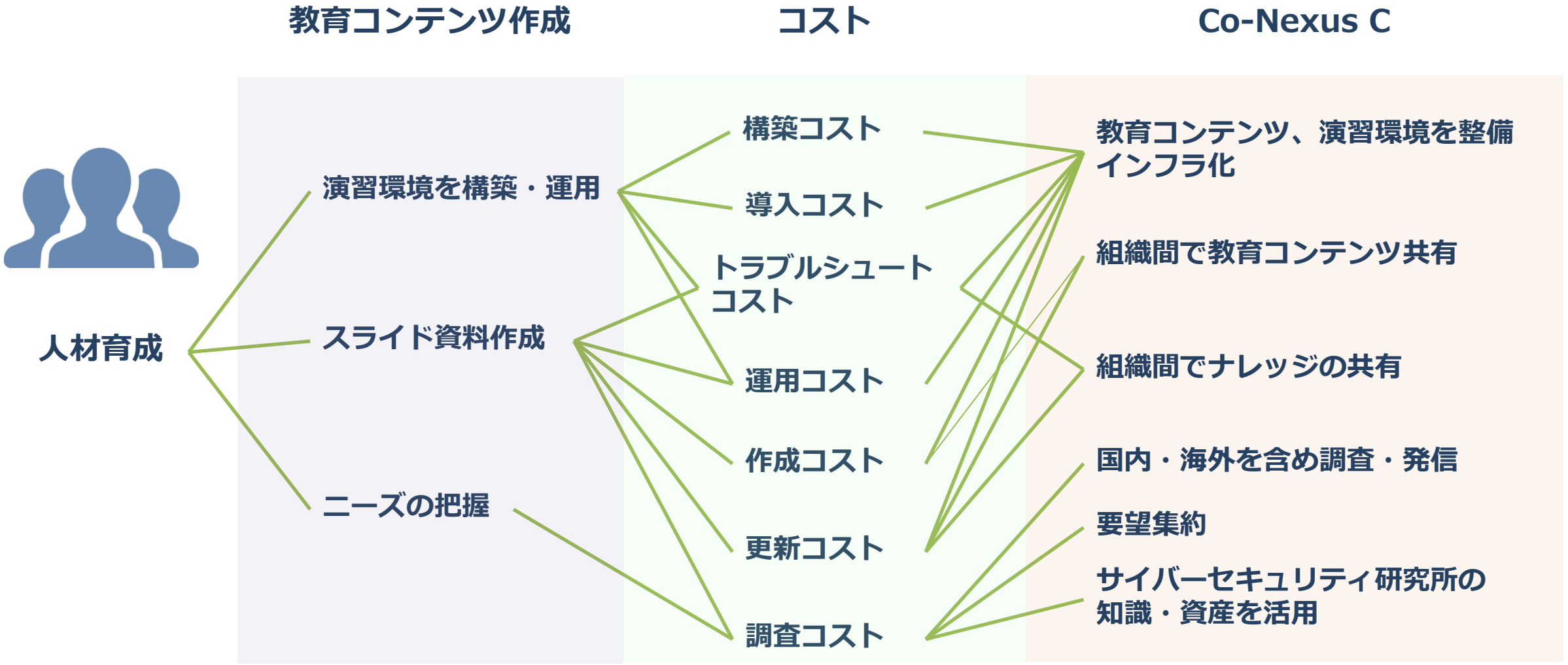

島 成佳
長崎県立大学


井田 潤
トレノケート

NICT National Institute of Information and Communications Technology

CYNEX CYBERSECURITY NEXUS

# Co-Nexus Cの活動




コンテンツをつなげる

# Co-Nexus Cロードマップ

R2 R3 R4 R5 R6 R7

**教材ニーズ調査**
トレーニングベンダーやセキュリティ教育および制度設計有識者等へのヒヤリングを実施し、我が国で必要とされる教材のニーズを明らかにする。

**教育調査**
CVID-19がもたらしたセキュリティ教育への影響を調査し、今後のセキュリティ教育のありかたを明らかにする。

**教育調査**
フレームワークと社会展開について調査し、Co-Nexus Cでの最適なフレームワーク実装方法を考察する。

**教育調査**
Co-Nexus C提供教育コンテンツによるカリキュラムの作成を目指す。

調査の結果を踏まえてR4以降に作製する教材KSAのプライオリティを決定

## 教えたいを叶える

✓教材ニーズの調査
✓教材の整備

教材整備

順次、教材がカバーするKSAを拡大

R3作製教材
オリジナルコンテンツ

OC

トレーナー育成に向けてのコンテンツ開発

TT

教材テーマを選べばKSAをどの深さで学べるなど、教材テーマとKSAを紐付けて整理。教えたいKSAからテーマを選ぶことも可能

アウトプット
・教材パワーポイント
・講師用マニュアル
・演習環境(VM等)
・環境構築マニュアル

**CYDERANGEへの実装**
利用者が、環境整備などの事前準備工数が少なく、トレーニングを開始できる環境の整備

CYDER Cyber Defense Exercise with Recurrence
cyber colosseo

ナショナルサイバートレーニングセンターが開発した過去の演習教材を利用可能

FREE 無償利用期間

INFINITY CHAMBER

Co-Nexus C Alliance加盟の組織間での教材シェア
StarBEDの豊富な計算リソース上に構築されたLMSと共に教材パワーポイントやLMS上に展開された演習環境を利用できる。

Co-NexusC Alliance（仮称）

有償利用

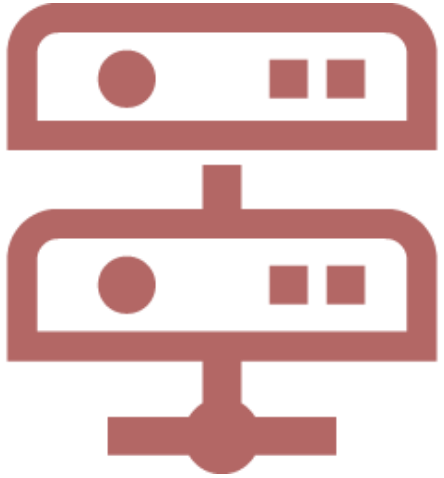
NICT National Institute of Information and Communications Technology

CYNEX CYBERSECURITY NEXUS

# 仕事,タスクをつなげる NIST NICE Framework

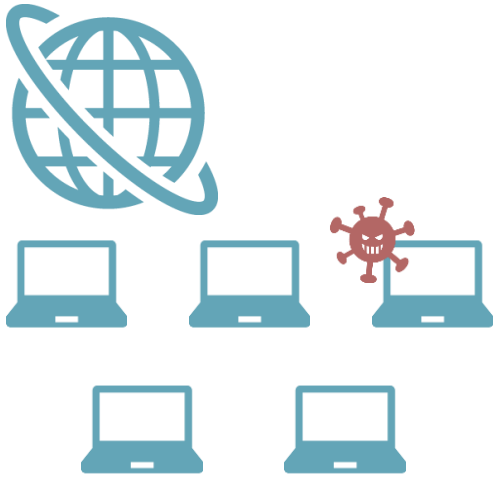
NIST NICE Framework は、世界的に知名度が高く、ITSS+やSecBokと相互に読み替えが可能なため、国内のフレームワークと互換性をとることができる。
Co-Nexus C Allianceでは、人材育成基盤のオープン化を目指し、産学官でのセキュリティ教育教材やノウハウの共有を行う。

# CYROP　～教えたいを叶えるために～



計算資源

演習環境



Learning
Management
System

教育コンテンツ

# 演習環境

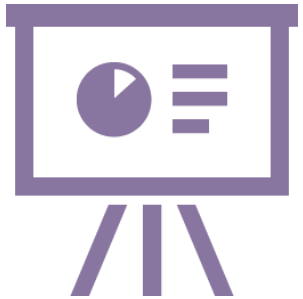
## 演習環境の利用イメージ

Step1 サービスの洗い出し 2 3 4

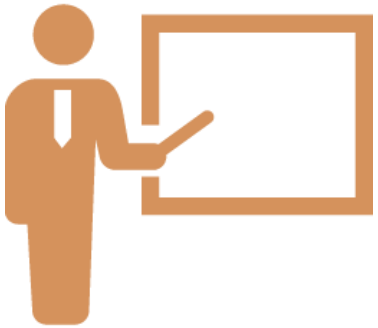
# 教育コンテンツの特徴

フレームワークの利用
NIST　NICE Framework を利用して、受講者が身につけられる知識、スキルが整理

前提知識
受講者が受講に際して必要な知識を明示



解説
講義用スライドには、スライド毎に、「目標」「説明の流れ」「ポイント」を記載



講師知識
コンテンツを利用する講師は、情報処理安全確保支援士以上の知識とスキル保持者として教育コンテンツを作製

# 講師とコンテンツをつなげる

# 教育コンテンツ
## 解説例


スライドノート部分には、全ページにわたり
「目標」
このスライドで伝えたいことはなにか
「説明の流れ」
説明の流れの例
「ポイント」を記載
このスライドで重要な部分はどこか
を記載している

NICT National Institute of Information and Communications Technology

CYNEX CYBERSECURITY NEXUS


知識をつなげる

# 教育コンテンツ
## 事前知識例

### 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 |

受講にあたって受講者が必要とする前提のKSAを示しています。ここに記載されたKSAを受講者が身につけていることを前提として講義スライド等の資料がつくられています。

KSAの「_」以下は、認知プロセスの次元を表します。

1=知識・記憶レベル
2=理解レベル
3=応用レベル

# 教育コンテンツ
## 身につけられる知識例

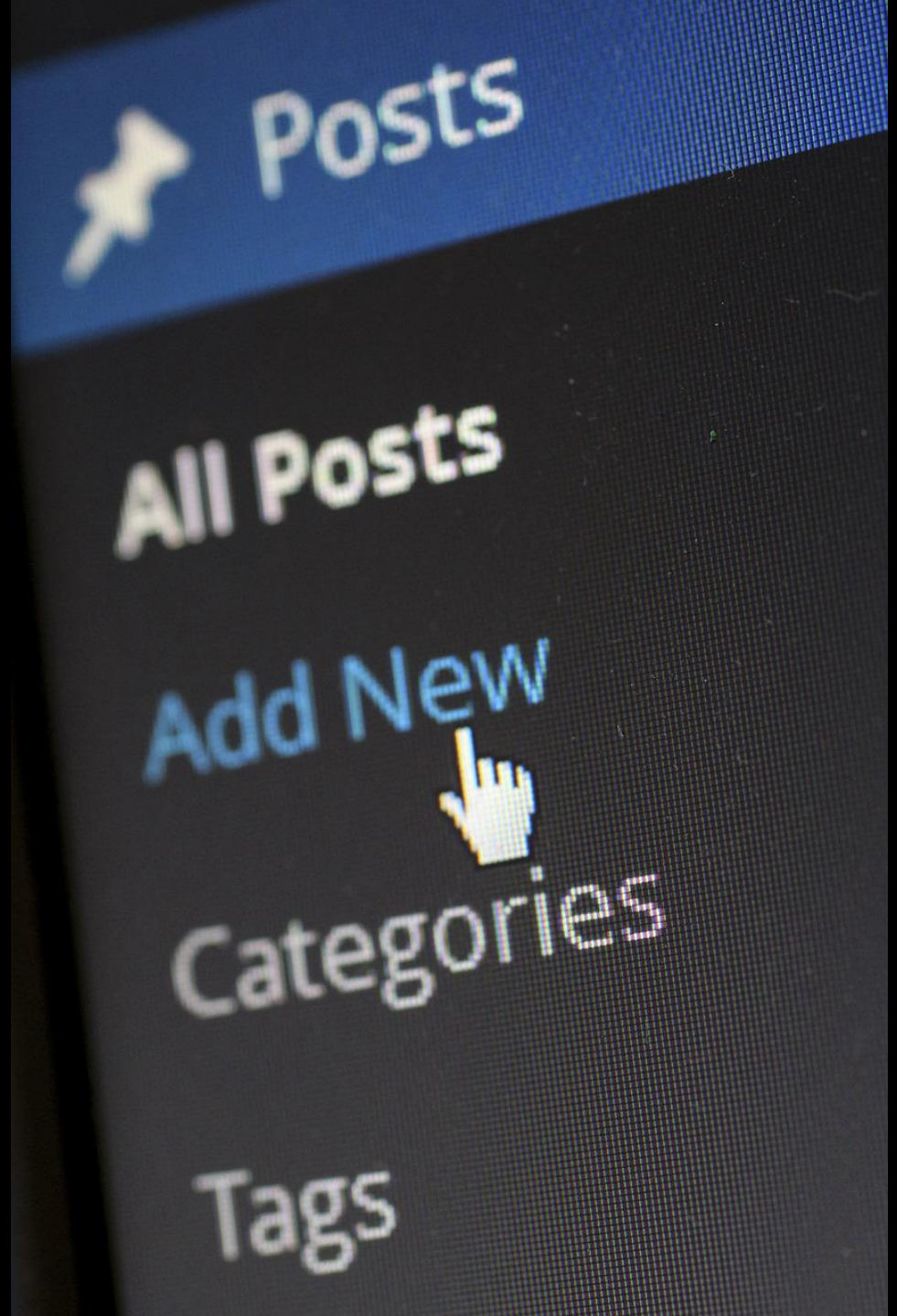
### 1.2　講義を受講して得られる KSA

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<br>K0009_2<br>K0296_2 | S0001_2 | A0015_2 |
| 脆弱性診断（セキュリティ診断） | K0013_2<br>K0290_2<br>K0046_2<br>K0339_2<br>K0342_2 | S0001_2 | A0015_2 |
| 対策 | K0005_2<br>K0007_2<br>K0009_2 | - | - |

受講すると身につけられるKSAが記載されています。KSAは章ごとに記載され、講師によって構成変更が容易にできるようにされています。




組織とコンテンツをつなげる

# アライアンスでトレーニングを共有する

開発したセキュリティトレーニングを共有する
アプライアンスのトレーニング
専門性の高いこと
知って欲しいこと

# CYDERからの教育コンテンツ

- CYDER
  - ✓2019年　A
  - ✓2020年　B1
  - ✓2020年　B2
  - ✓2021年　B1
  - ✓2021年　B2
  - ✓2022年　B2
  - ✓2023年　A
  - ✓2022年　B1
  - ✓RPCI　（受け入れ準備段階）
  - ✓Gコース（受け入れ準備段階）

CYDERおよびパイロットコンテンツはNIST NICE Framework に基づき受講者が身につけられるKSA、Knowledge Skill Abilityが整備されています。

CYDER においては、NIST NICE Framework の定義する Incident Responderの役割が身につけておくべきKSAを基に、より日本の現状に特化するようKSAを設定しています。

＊ハンズオンを含むコンテンツ

# 2021年度開発コンテンツ

- 2021 オリジナルコンテンツ
  - ✓ 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
  - ✓ クロス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）
  - ✓ ノンテクニカルスキル演習（ロールプレイ）

オリジナルコンテンツは、章ごとに受講者が学ぶことができるKSAを設定しています。章ごとにKSAを整理している理由は、教育プログラムを設計する際に、容易にコンテンツを組み替えながら、1つの教育プログラムをつくることができるためです。

＊ハンズオンを含むコンテンツ

# 2022年度開発オリジナルコンテンツ

- 情報セキュリティ基礎
  - ✓ OS基礎
  - ✓ OSコマンド基礎 （ハンズ有り）
  - ✓ 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（ハンズ有り）

- 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 （ハンズオン有り）

- 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（ハンズ有り）
    AD侵入テスト（ハンズ有り）

- ハードニング演習
  - ✓ ハードニング Bule Teams演習（ハンズオン有り）

＊ハンズオンを含むコンテンツ

NICT National Institute of Information and Communications Technology

CYNEX CYBERSECURITY NEXUS

# 2023年度開発コンテンツ

- ネットワークセキュリティ
  - ✓ DNSセキュリティ（ハンズ有り）
  - ✓ VPNセキュリティ
  - ✓ メールセキュリティ
  - ✓ 脆弱性診断（ハンズ有り）
  - ✓ 無線LANセキュリティ

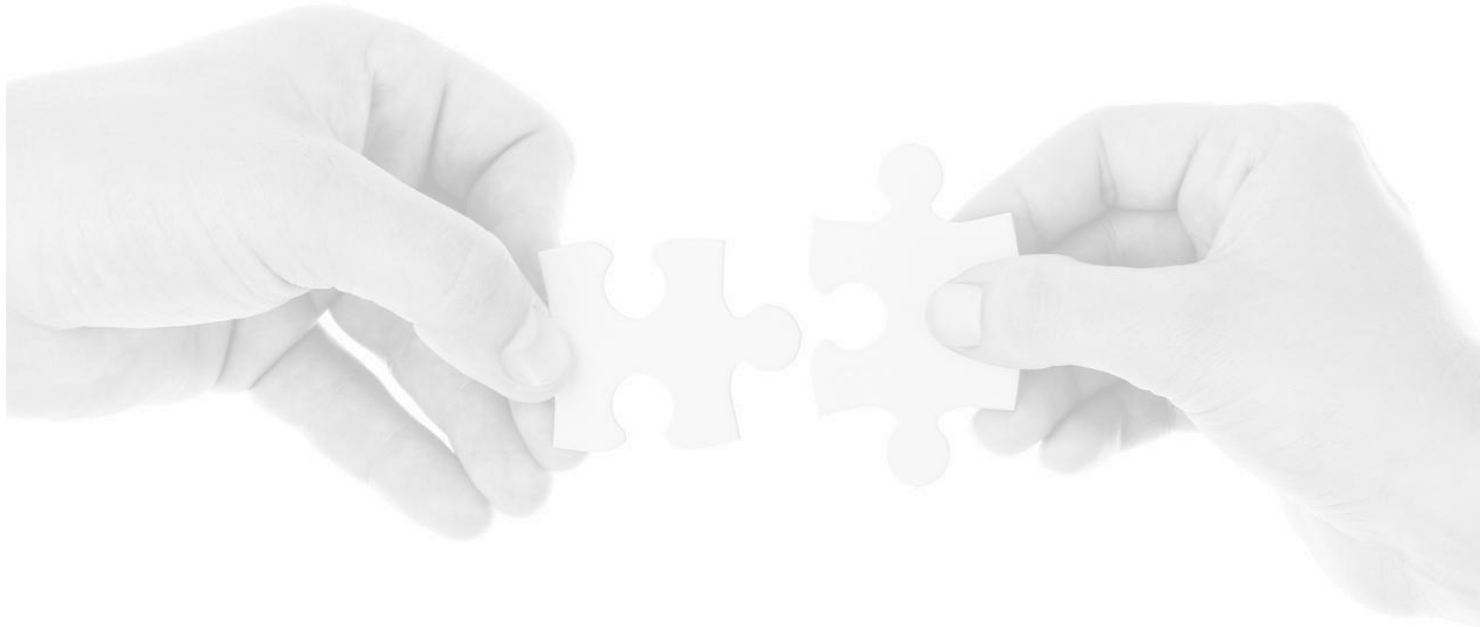
- 経営層から現場まで取り組めるセキュリティ演習_演習
  - ✓ インシデントレンスポンス（ハンズ有り）
- 認証と認可
- 暗号基礎
  - ✓ 暗号基礎（ハンズ有り）
- フォレンジック解析
  - ✓ メモリフォレンジック（ハンズ有り）

- ログ分析演習
  - ✓ ログ分析演習（ハンズ有り）

- OTセキュリティ
  - ✓ OTセキュリティ演習（ハンズ有り）
- トレーナーズトレーニング

# 2024年度開発コンテンツ

- 初心者向けリテラシー教育
  - ✓ 初心者向けリテラシー教育 座学
  - ✓ 初心者向けリテラシー教育 演習
- RedTeam&BlueTeam演習
  - ✓RedTeam&BlueTeam演習（ハンズ有り）
- 仮想化セキュリティ
  - ✓仮想化セキュリティ 座学
  - ✓仮想化セキュリティ 演習（ハンズ有り）
- ネットワークセキュリティ
  - ✓メールセキュリティ演習（ハンズ有り）
- スレッドハンティング
  - ✓スレッドハンティング



# End