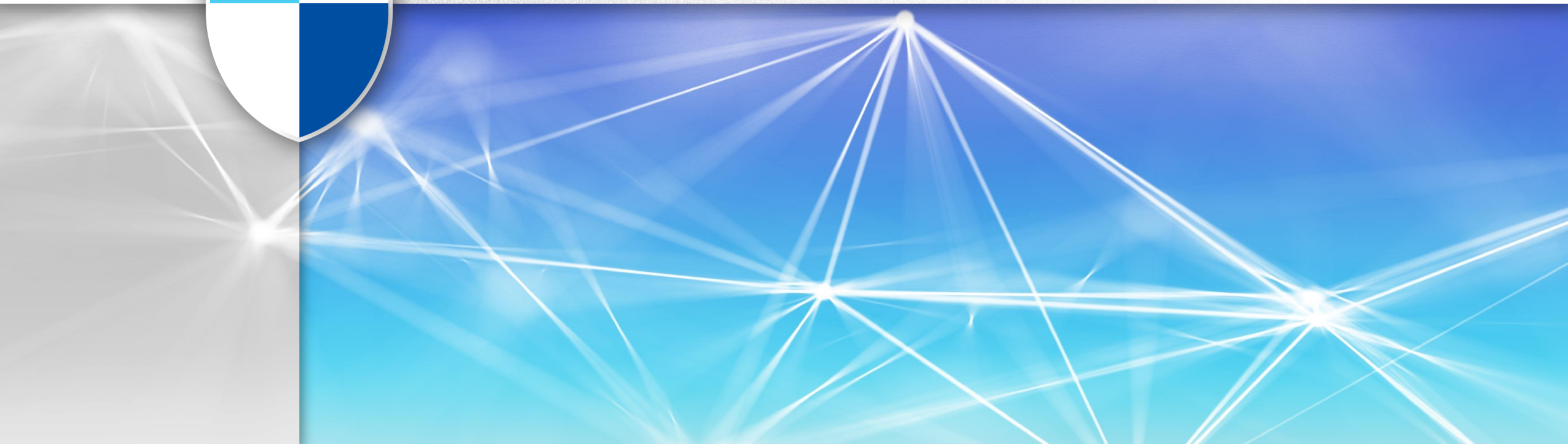
国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所
ナショナルサイバートレーニングセンター

資料４－１
※一部非公開※

実践的サイバー防御演習「CYDER」
2023年度結果と2024年度の実施予定について

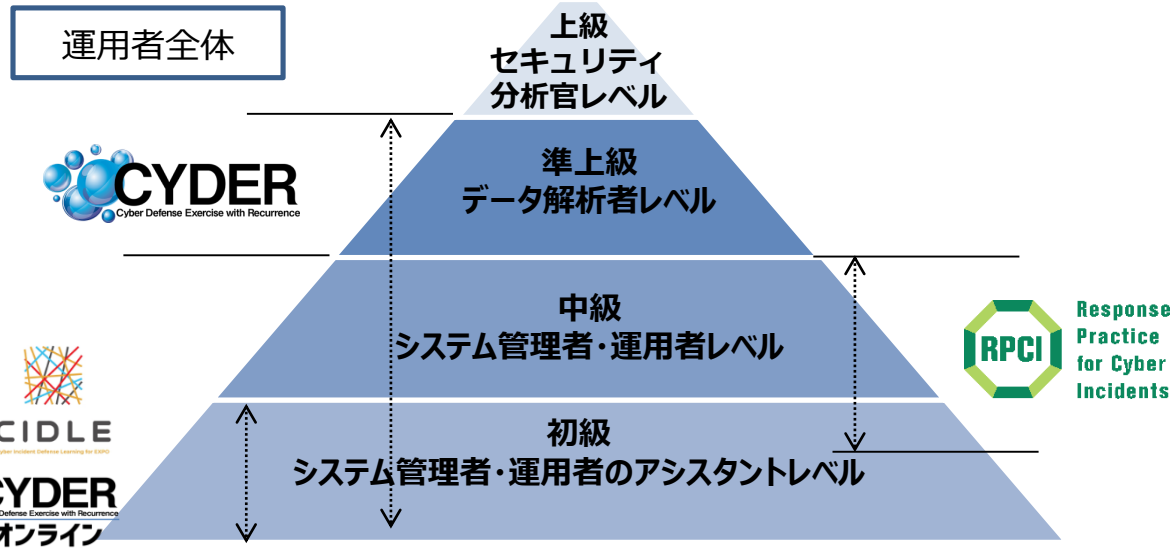


「ナショナルサイバートレーニングセンター」の概要

- **NICTの技術的知見、研究施設等を最大限に活用し、実践的なサイバートレーニングを企画・推進**する組織として設置（2017年4月1日）
- 日本全体のサイバーセキュリティエコシステムの能動的な発展のため、**インシデント対応の実務に携わる運用者**及び**革新的なセキュリティサービス等を開発するハイレベルな人材**の育成を実施

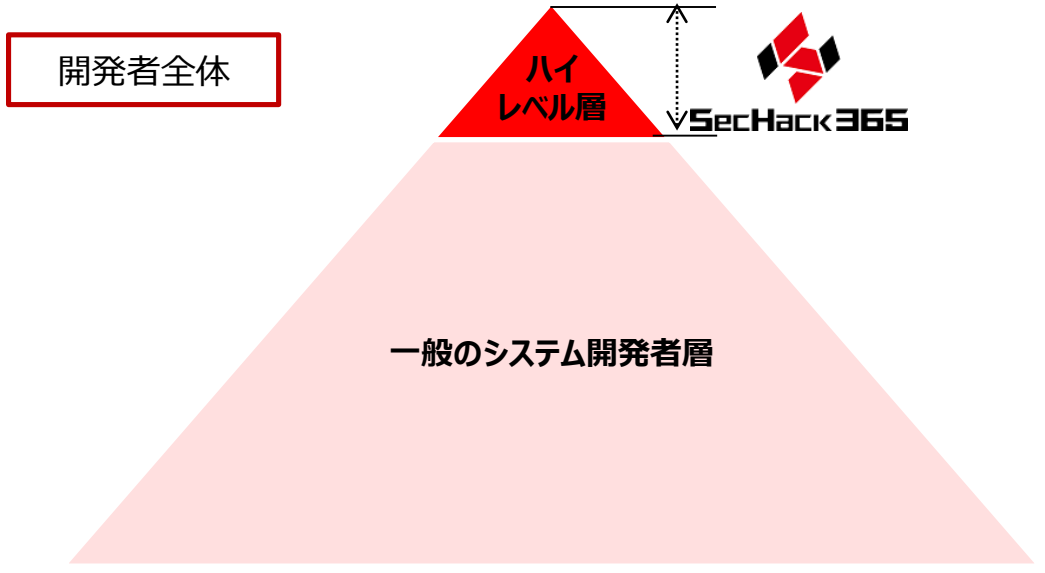
セキュリティオペレーター（実践的運用者）の育成

- **行政機関や民間企業等の組織内のセキュリティ運用者（情報システム担当者等）を対象**
- **年間約3000名の規模で、所属組織がサイバー攻撃を受けた段階等（＝「有事」）における実践的なインシデント対応能力を育成**



セキュリティイノベーター（革新的研究・開発者）の育成

- **単なる「ユーザー」として既存ツールを利用するだけではなく、セキュリティマインドを持ち、革新的なセキュリティソフトウェア等を自ら「研究・開発」していくことができるハイレベルな人材を育成（年間約40名）**



実践的サイバー防御演習「CYDER」の概要

CYDER Cyber Defense Exercise with Recurrence

NICT National Institute of Information and Communications Technology

- 国の機関、地方公共団体及び重要インフラ事業者等を対象に、**NICTの技術的知見を活用**し、仮想空間上に組織のネットワーク環境を再現し、一連のインシデント対応を模した実践的な防御演習を行うプログラム。
- 自治体、関係府省庁、警察、自衛隊、重要インフラ事業者等多くの組織が毎年受講

概要（2023年度）

【受講対象】 国の機関、指定法人、独立行政法人、地方公共団体の職員 **（無料）**
重要社会基盤事業者、民間企業等（有料）
【開催形式】 集合演習 **（全都道府県で100回程度）**
オンライン演習

コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織
A	集合演習	初級	システムに携わり始めたばかりの方 (事案発生時の対応の流れ)	全組織共通
B-1		中級	システム管理者・運用者 (主体的な事案対応・ｾｷｭﾘﾃｨ管理)	地方公共団体
B-2				地方公共団体以外
C		準上級	セキュリティ専門担当者 (高度なセキュリティ技術)	全組織共通
入門	オンライン演習	入門	情報システム担当経験1年前後で 知識のアップデートをお考えの方	全組織共通
プレCYDER		-	インシデント発生時の対応の学習を これから始める、又は始めたばかりの方	国の機関等、 地方公共団体

CYDER受講者数の推移（累積数）

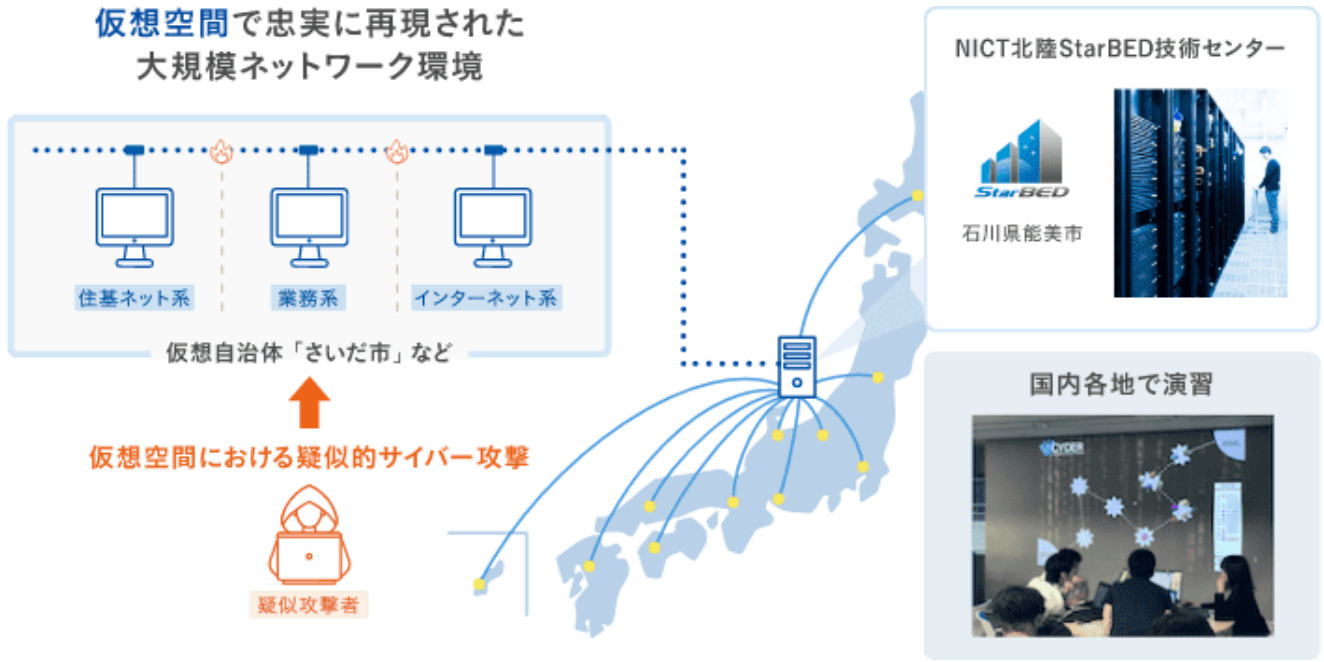
CYDERのトレーニング内容（集合演習）

- 自治体等のネットワーク環境を仮想空間上に再現し、インシデントハンドリングをロールプレイ形式で体験
- 最近のサイバー攻撃事例分析に基づいた、リアリティある演習シナリオ
- 経験豊富な講師・チューターによるサポートや、受講者間のグループワークによる高い学習効果

演習シナリオの例

- **標的型攻撃**
  職員が標的型メール（Emotet）を開き感染が拡大し、Web管理者の端末からWebが改ざんされる
- **踏み台攻撃**
  リモートワーク端末を踏み台としてLGWAN内に侵入され、情報を窃取される
- **ランサムウェア攻撃**
  乗っ取られた外部アカウントからのメールを職員が開き、そこを踏み台に組織内システムがランサムウェアに感染

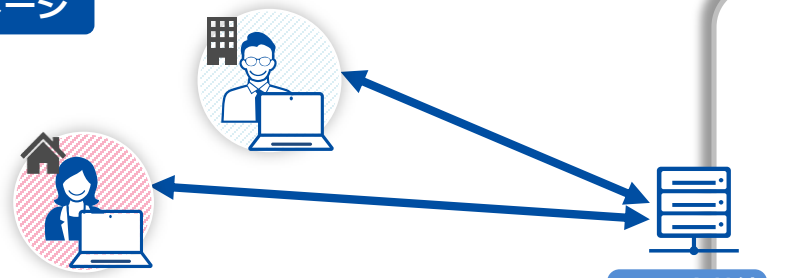
演習舞台設定演習イメージ



CYDER オンライン演習

- 地理的・時間的要因等によりCYDER集合演習が受講できない方への対応として、職場や自宅のパソコンのWebブラウザから演習環境に接続し、受講可能なオンライン演習を提供
- 令和5年度は、国の機関等、地方公共団体を対象として、**CSIRT担当者として知っておきたい基礎的な事項を短時間で習得できる「プレCYDER」を新設実施。**

受講イメージ



スライド資料を用いた学習

クイズフォーマットの課題

録画解説ビデオで演習をサポート

仮想演習端末にアクセスして
集合演習同様に実機演習も実施

令和5年度のオンラインコース

入門	• 集合演習Aコース受講に必要な最低限の知識レベル • 個人課題のみで構成 • 集合演習の予習として活用
プレCYDER	• CSIRT担当者として知っておきたい基礎的な事項を短時間で習得可能

CYDERオンライン演習 令和5年度の実施

4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
	オンライン入門コース							プレCYDERコース			

2023年度CYDER演習実施結果

赤枠内取扱注意

- 全都道府県で集合演習を106回開催。目標3,000名に対し過去最多の**3,742名**が受講修了
- オンライン演習は**1,963名**が受講修了
- 新たに試行した短時間でCSIRTとして備えるべき基礎的事項が学べるプレCYDERには、想定を上回る申し込みがあり、**こうした内容・方式での演習ニーズの高さが示された**。未受講自治体からも受講されており、**これまで集合演習を受講してこなかった組織の底上げに貢献**

国の機関等の受講状況

赤枠内取扱注意

- 各種周知やデジタル庁との連携が奏功し、国の機関では**約９割以上の組織**が集合演習を受講し、受講者数は前年度から1.3倍増

地方公共団体の受講状況

赤枠内取扱注意

- 各方面からの周知等により、市町村の受講が進み、主指標未受講自治体数が**昨年比約４割減少する等、**地方公共団体での受講が進んだ。
- 主指標未受講組織の内、**約2.5割の組織がオンラインコース**を受講する等、受講機会の提供に貢献した。

CYDER受講者の声

赤枠内取扱注意

- CYDERで得た知識が**実際にインシデントが発生した際に役立った**、受講をきっかけに**ベンダーとの連携体制を見直した**、**自組織のネットワーク構成・セキュリティポリシー等の見直しのきっかけとなった**等、CYDERの受講が組織におけるインシデント対応や準備に生かされている。

プレCYDER実施概要

赤枠内取扱注意

- CSIRT担当者として最低限知っておきたい事項を短時間で習得できる**「プレCYDER」**を、国・自治体向けに試行実施（2023/12/5～2024/1/31）
- 動画視聴とクイズ形式の課題を組み合わせ、受講対象者が理解し易い構成になるよう工夫

- 動画視聴とクイズ
  - 動画視聴とクイズ形式の課題を組み合わせたコンテンツ
  - 2～3時間で受講可能
  - 約15分単位の分割受講可能
- 最新事例のケーススタディ
  - 最新事例に基づくケーススタディ課題
  - 選択式の問題に解答するクイズ形式の課題
- サイバー攻撃の仕組みとトレンド
  - サイバー攻撃の説明
  - 手口とメカニズム
  - 攻撃が成功するとどうなるか
  - サイバー攻撃への対策
- インシデントハンドリング概要
  - インシデントとは何か
  - インシデント発生時の対応
  - CSIRTの必要性

プレCYDER受講者の声

赤枠内取扱注意

- セキュリティ担当となったばかりで何をしてよいか分からなかったが、基礎を学ぶことができてよかった、 CSIRTの教育の強化の必要性を認識できた、オンライン形式で分割受講できたのが良かった、事例からインシデント発生時の体制や対応を学べてよかった、といった声が寄せられる等、**オンライン形式、複数動画で分割受講可能な構成、基礎から学ぶプログラム、事例に基づいたリアルな内容**が受講者のニーズにマッチ
- **庁内の研修として活用**した自治体も複数存在。

→ **2024年度は、開講期間を拡大して受講機会を増やすとともに、新コンテンツで更なる知識の習得機会を提供予定**

周知・意識啓発に関する取組

➢主な取組

- ✓**パンフレット・チラシ発送**
  - ✓全国の自治体、都道府県警察、独立行政法人、指定法人、広域連合等への発送
- ✓**各総合通信局等**を通じた周知
- ✓**メルマガ**（サイバートレーニング通信）での演習の周知
- ✓**SNS**（Twitter・Facebook・Instagram）・**機構Webサイト**での周知
- ✓**対面イベント**（白浜シンポジウム、Interop等）での周知
- ✓**各総合通信局主催サイバーセキュリティイベント、各種説明会**等における周知
  - ✓省庁関係機関CSIRT向け勉強会、医療関係者向け説明会、自治体のCSIRT担当者会議等
- ✓**NISC、J-LIS、デジタル庁、自治大学校等との周知連携**
  - ✓各種研修・勉強会での周知、メールを通じた周知等