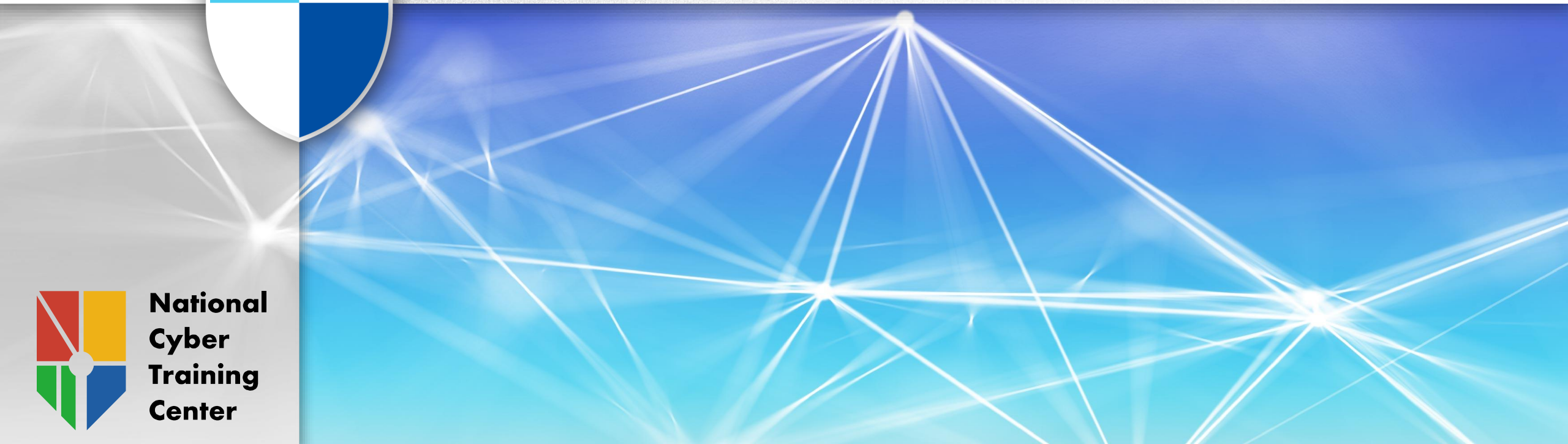
国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所
ナショナルサイバートレーニングセンター

第4回サイバーセキュリティ対策等についての説明会

体験型の実践的サイバー防御演習CYDERとは

花田 智洋



National Cyber Training Center

スピーカー

- 氏名: 花田 智洋 (Tomohiro Hanada)
- 勤務先: 2017年1月～現在
  - NICT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(通称: ナショトレ)
  - CYDER, RPCI, SecHack365, CIDLE,
    CYDERANGE開発等の事業に携わる
- 前職: ～2016年12月末
  - 銀行システム担当のプロジェクトマネージャー
- 業務外活動:
  - 情報セキュリティコミュニティ運営(2006-現在)
  - SECCON実行委員長(2018-2022), 副実行委員長(2023-現在) 他

PMP CISSP CompTIA CTT+ CERTIFIED

エヌアイシーティー

NICT: 国立研究開発法人情報通信研究機構

情報通信分野を専門とする我が国唯一の公的研究機関

重点5分野

- ✓ 電磁波先進技術
- ✓ 革新的ネットワーク
- ✓ **サイバーセキュリティ**
- ✓ ユニバーサルコミュニケーション
- ✓ フロンティアサイエンス
  ＋オープンイノベーション

足りない

日本のサイバーセキュリティ人材数

約11万人

ISC2 Cybersecurity Workforce Study (https://www.isc2.org/Research), 2023

National Cyber Training Center

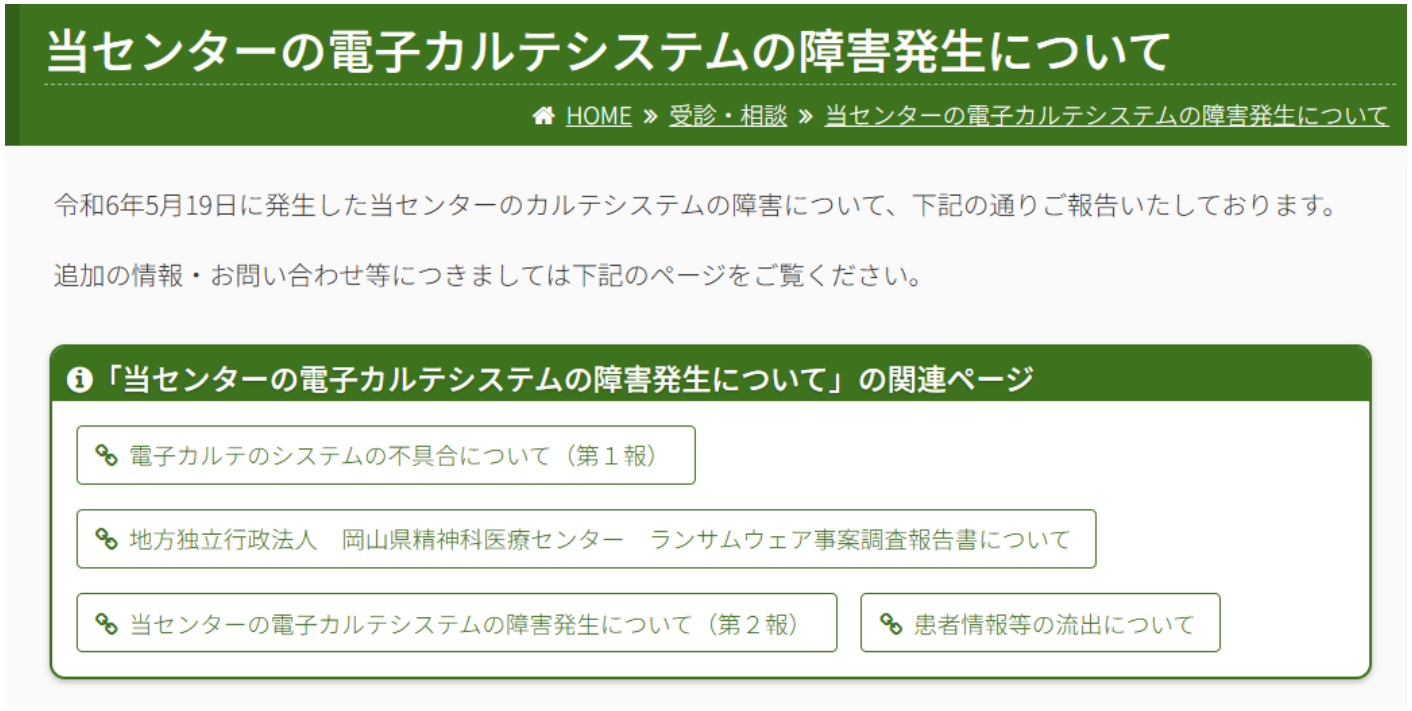
人材育成

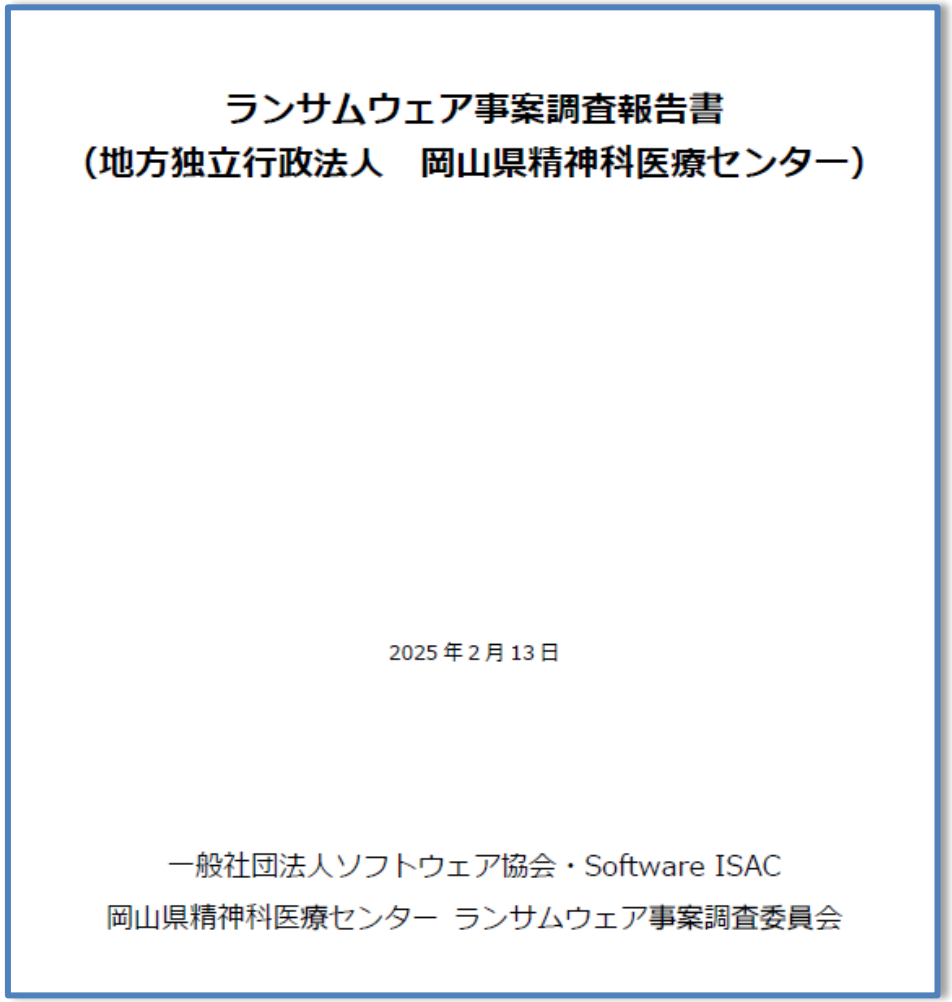
ところで

業界の情報をタイムリーにキャッチアップできていますか？

業界の情報をタイムリーにキャッチアップできていますか？

今年2025年2月公開の報告書




ランサムウェア事案調査報告書
（地方独立行政法人　岡山県精神科医療センター）

2025 年 2 月 13 日

一般社団法人ソフトウェア協会・Software ISAC
岡山県精神科医療センター ランサムウェア事案調査委員会

当センターの電子カルテシステムの障害発生について – 地方独立行政法人 岡山県精神科医療センター

https://www.okayama-pmc.jp/home/consultation/er9dkox7/

事案概要

- 岡山県精神科医療センターで2024年5月に**ランサムウェア攻撃**が発生。

- **国内病院で15件目**、精神科病院では初の事例。
※公表されていない/できていない事例の可能性有

- 電子カルテを含む**情報システムが機能停止、個人情報漏洩。**

攻撃と被害

2024年5月13日初期侵入、19日電子カルテ等が完全暗号化。

仮想サーバー23台、物理サーバー9台、端末244台が暗号化、
共有ストレージの**データ全損**。

推定40,000人分の個人情報漏洩。

なぜ攻撃が成功したのか

保守用SSL-VPN装置の**脆弱性放置**。
※2018年以降アップデートせず

推測しやすい管理者パスワードの使いまわし。
ID: administrator, Password: P@ssw0rd

全ユーザーへの管理者権限付与。

「**閉域網神話**」による思考停止。
※オオカミ少年的な正常性バイアスも

対応と復旧

インシデント発覚後、迅速に**紙カルテ運用**を開始し診療継続。

外部の専門家の協力を得て3ヵ月でシステムを完全復旧。
※復旧のための追加キャッシュアウトが発生

情報漏洩に関する**記者会見**の実施、患者への説明と**相談窓口**の設置。

再発防止策

ソフトウェアの定期的アップデートの徹底。
※Windows Update等

長いパスフレーズの採用。

管理者権限を厳格に制限し、個別のID/パスワードを設定。

オフライン・バックアップの定期的取得・確認。
※本件では、オフライン・バックアップを適切に取得できていなかったことが
復旧時に発覚

教訓と提言

サイバーセキュリティ対策の継続的な啓発・教育が不可欠。

過去の攻撃事例から学び、セキュリティ対策を迅速に適用することが重要。

「あろうことか、私たちは過去の事例に十分学んでいませんでした。
　報告書が公表されている病院で発生した事例とまったく同じである。」
※耳の痛い話

病院業界全体で管理者権限の適正化を推進。

注目

過去の攻撃事例から学び、セキュリティ対策を迅速に適用することが重要。


誰かがなんとかしてくれるって、
みんなが思ってた。

注目

過去の攻撃事例から学び、
セキュリティ対策を迅速に
適用することが重要。

Next action: 再発防止策、勤務先で対策済みですか?

[再掲]教訓と提言

- サイバーセキュリティ対策の継続的な啓発・教育が不可欠。
- 過去の攻撃事例から学び、セキュリティ対策を迅速に適用することが重要。
- 病院業界全体で管理者権限の適正化を推進。

[再掲]教訓と提言

- **サイバーセキュリティ対策の継続的な啓発・教育が不可欠。**
- 過去の攻撃事例から学び、セキュリティ対策を迅速に適用することが重要。
- 病院業界全体で管理者権限の適正化を推進。

ナショナルサイバートレーニングセンター2025

実践的サイバー防御演習
「CYDER」（サイダー）

国の機関、地方公共団体、重要社会基盤事業者等を対象とする実践的なサイバー防御演習

実践サイバー演習
「RPCI」（リプシィ）

情報処理安全確保支援士向け特定講習。CYDERのノウハウを活かした、リアリティの高い実践的なインシデントハンドリング演習

「SecHack365」
（セックハック サンロクゴ）

セキュリティイノベーター育成を目的として、NICTが若年層のICT人材を対象に、セキュリティの技術研究・開発を本格的に指導する新規プログラム

実践的サイバー防御演習「CYDER」の概要

- 情報通信研究機構（NICT）ナショナルサイバートレーニングセンターでは、2017年度から**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。
- 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、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**。

概要（2025年度）

【受講対象】 国の機関、指定法人、独立行政法人（無料）
地方公共団体の職員（プレCYDERとAコースは無料）
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
プレCYDER	オンライン演習	-	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	全組織共通

CYDER受講者数の推移（累積数）

実践的サイバー防御演習 CYDER は選べます

オンライン演習

プレCYDER 1期・2期 ケーススタディ
プレCYDER 3期 ドリル

集合演習

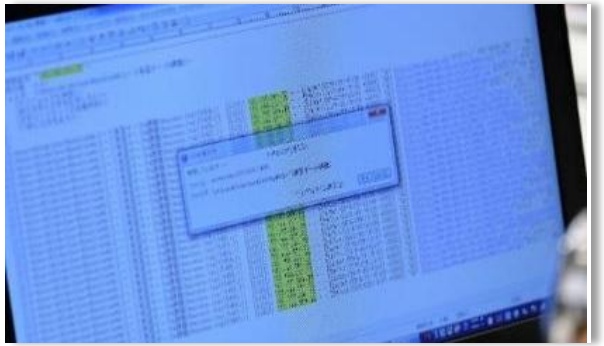
Aコース 初級
B-1・B-2コース 中級
Cコース 準上級

集合演習風景

オリエンテーション

演習フロー説明

インシデント発生～事実確認

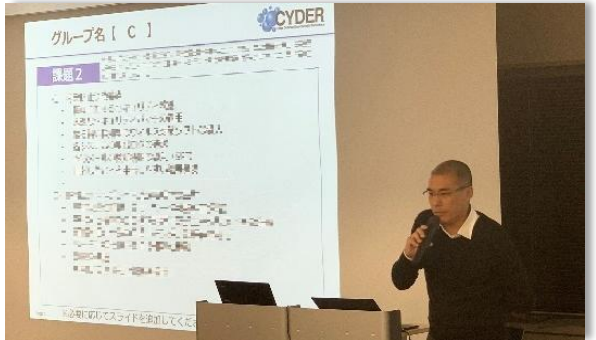


チューターによるサポート

マルウェア挙動調査

グループワーク

発表



報告書作成

確認テスト

あなたにぴったりの受講スタイルは？

積み重ねてきた経験や業務上の立場によって異なる受講スタイルの例をご紹介します。

情報システム担当者として経験が長く、より高度な分析・判断スキルを習得したい方

部門リーダースタイル

例1：部下への教育導入判断のためにプレCYDER（1期・2期：ケーススタディと3期：ドリル）、その後自分のスキル維持のためにCコースを受講。

- プレCYDER 1期 / ケーススタディ（5～8月）
- プレCYDER 2期 / ケーススタディ（9～11月）
- プレCYDER 3期 / ドリル（11～1月）
- 集合演習 Cコース（11～1月）

例2：プレCYDER（1期：ケーススタディと3期：ドリル）の後に部下と同じグループでB / Cコースを受講し、組織としての体制を強化。

- プレCYDER 1期 / ケーススタディ（5～8月）
- プレCYDER 3期 / ドリル（11～1月）
- 集合演習 Bコース（10～1月）
- 集合演習 Cコース（11～1月）

CSIRTの中心となってインシデント対応作業を担う立場であり、スキルアップしたい方

チームリーダースタイル

例1：知識のアップデートのために、プレCYDER（1期：ケーススタディと3期：ドリル）を受講し、その後にB / Cコースで実践を積む。

- プレCYDER 1期 / ケーススタディ（5～8月）
- プレCYDER 3期/ドリル（11～1月）
- 集合演習Bコース（10～1月）
- 集合演習 Cコース（11～1月）

例2：プレCYDER（1期：ケーススタディ）/ Bコースを受講後に、プレCYDER（3期：ドリル）を挟んでCコースで知識を深める。

- プレCYDER 1期 / ケーススタディ（5～8月）
- 集合演習 Bコース（10～1月）
- プレCYDER 3期 / ドリル（11～1月）
- 集合演習 Cコース（11～1月）

情報システム担当の経験が2年以内で、インシデント発生時の対応の流れを理解したい方

チームメンバースタイル

例1：プレCYDER（1期：ケーススタディと3期：ドリル）で基礎を固めた後に、A / Bコースで実践を積む。

- プレCYDER 1期 / ケーススタディ（5～8月）
- プレCYDER 3期 / ドリル（11～1月）
- 集合演習 Aコース（7～1月）
- 集合演習 Bコース（10～1月）

例2：プレCYDER（1期：ケーススタディ）/ Aコースを受講後に、プレCYDER（3期：ドリル）を挟んでBコースで応用力を強化する。

- プレCYDER 1期 / ケーススタディ（5～8月）
- 集合演習 Aコース（7～1月）
- プレCYDER 3期 / ドリル（11～1月）
- 集合演習 Bコース（10～1月）

CSIRT/情報システム課1年目、IT/DX推進リーダー、個人情報業務担当、幹部/経営層の方

ビギナースタイル

例1：プレCYDER（1期：ケーススタディ）で最初の一歩を。その後プレCYDER（2期：ケーススタディ&3期：ドリル）で更に1歩。

- プレCYDER 1期 / ケーススタディ（5～8月）
- プレCYDER 2期 / ケーススタディ（9～11月）
- プレCYDER 3期 / ドリル（11～1月）

例2：プレCYDER（1期・2期：ケーススタディ）とプレCYDER（3期：ドリル）で基礎を固め、Aコースで実践力を磨く。

- プレCYDER 1期 / ケーススタディ（5～8月）
- プレCYDER 2期 / ケーススタディ（9～11月）
- プレCYDER 3期 / ドリル（11～1月）
- 集合演習 Aコース（7～1月）

国の機関(31組織)

内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、警察庁、個人情報保護委員会、カジノ管理委員会、金融庁、消費者庁、こども家庭庁、デジタル庁、復興庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省、防衛省、会計検査院、衆議院事務局、参議院事務局、国立国会図書館、最高裁判所、日本銀行

独立行政法人(86組織)

国立公文書館、北方領土問題対策協会、日本医療研究開発機構、国民生活センター、情報通信研究機構、統計センター、郵便貯金簡易生命保険管理・郵便局ネットワーク支援機構、国際協力機構、国際交流基金、酒類総合研究所、造幣局、国立印刷局、国立特別支援教育総合研究所、大学入試センター、国立青少年教育振興機構、国立女性教育会館、国立科学博物館、物質・材料研究機構、防災科学技術研究所、量子科学技術研究開発機構、国立美術館、国立文化財機構、教職員支援機構、科学技術振興機構、日本学術振興会、理化学研究所、宇宙航空研究開発機構、日本スポーツ振興センター、日本芸術文化振興会、日本学生支援機構、海洋研究開発機構、国立高等専門学校機構、大学改革支援・学位授与機構、日本原子力研究開発機構、勤労者退職金共済機構、高齢・障害・求職者雇用支援機構、福祉医療機構、 国立重度知的障害者総合施設のぞみの園、労働政策研究・研修機構、労働者健康安全機構、国立病院機構、医薬品医療機器総合機構、医薬基盤・健康・栄養研究所、地域医療機能推進機構、年金積立金管理運用独立行政法人、国立がん研究センター、国立循環器病研究センター、国立精神・神経医療研究センター、国立成育医療研究センター、国立長寿医療研究センター、農林水産消費安全技術センター、家畜改良センター、農業・食品産業技術総合研究機構、国際農林水産業研究センター、森林研究・整備機構、水産研究・教育機構、農畜産業振興機構、農業者年金基金、農林漁業信用基金、経済産業研究所、工業所有権情報・研修館、産業技術総合研究所、製品評価技術基盤機構、新エネルギー・産業技術総合開発機構、日本貿易振興機構、情報処理推進機構、石油天然ガス・金属鉱物資源機構、中小企業基盤整備機構、土木研究所、建築研究所、海上・港湾・航空技術研究所、海技教育機構、航空大学校、自動車技術総合機構、鉄道建設・運輸施設整備支援機構、国際観光振興機構、水資源機構、自動車事故対策機構、空港周辺整備機構、都市再生機構、奄美群島振興開発基金、日本高速道路保有・債務返済機構、住宅金融支援機構、国立環境研究所、環境再生保全機構、駐留軍等労働者労務管理機構

指定法人(サイバーセキュリティ基本法第13条の規定に基づき、サイバーセキュリティ戦略本部が指定する9法人)

地方公共団体情報システム機構、地方公務員共済組合連合会、地方職員共済組合、東京都職員共済組合、全国市町村職員共済組合連合会、国家公務員共済組合連合会、日本私立学校振興・共済事業団、公立学校共済組合、日本年金機構、国立健康危機管理研究機構

地方公共団体

都道府県、市区町村　　※2025年度から地方公共団体の方は集合演習BコースとCコースが有料となりました。

CYDERをお勧めする理由

- CYDERは、**豊富なコースラインナップ**で、初学者から上級者までサポートします。
- サイバー攻撃は日々進化しています。知識のアップデートのために、繰り返し受講をお勧めします。

初級、 中級、準上級、オンライン(プレCYDER)

- 最大4名のグループワーク、ハンズオン　等
- 国の機関の方は受講料が無料
- 新作シナリオ続々、繰り返し受講やステップアップをオススメ
- 受講後に発生した**インシデント対応に役立った**例

演習環境CYDERANGE

- 各グループに専用の演習環境を提供
- NICTの強み① 大規模計算機環境＆StarBED

そのときどきの旬なシナリオの提供

- NICTの強み② 研究実績と攻撃観測データの蓄積


今からでも、遅くない。
何かあってからじゃ、遅い。

National Cyber Training Center

CYBERSECURITY
Research Institute


NICT
国立研究開発法人
情報通信研究機構