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42－２－２

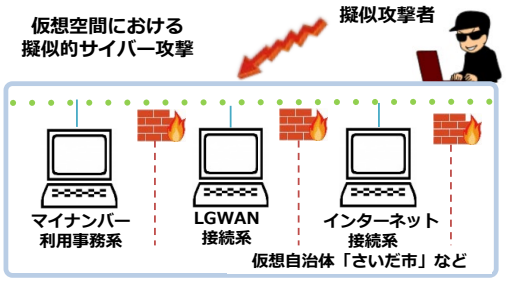
ナショナルサイバートレーニングセンターの取組

2023/2/1

ナショナルサイバートレーニングセンターの概要

セキュリティオペレーターの育成

CYDER
（実践的サイバー防御演習）



対象とする組織
- 国の機関等
- 地方公共団体
- 重要社会基盤事業者
- 民間企業等

Response Practice for Cyber Incidents
（実践サイバー演習）

公的機関初の
情報処理安全確保支援士
向け特定講習

NICTが持つ大規模演習環境を活用
リアリティを高めた
インシデントハンドリング演習

<RPCIの特長>
- **集合演習、グループワークへのこだわり**
- **舞台装置やシナリオのリアリティ**
- **充実したサポート体制**
- **演習後も活用できる教材**
- **各種資格との連携**

大阪万博向けサイバー防御演習

サイバー攻撃に対処可能な万博関連組織の人材育成

万博向け演習プログラムの提供

OSAKA, KANSAI, JAPAN EXPO2025

セキュリティイノベーターの育成

SecHack365
若手セキュリティイノベーター育成プログラム

アイデアソン・
ハッカソンイベント
開催地を変えて複数回実施し、継続的に開発指導

豊富な研究資産
研究開発のノウハウ、攻撃データ等の活用

オンラインでの指導・
遠隔開発実習
自宅などの遠隔地から開発環境へアクセス可能

受講生への支援
長時間の学業との両立についての助言、指導

最先端技術の体験
先端企業の見学による社会体験で発想力を強化

2022年度 実践的サイバー防御演習「CYDER」の概要

（CYDER : CYber Defense Exercise with Recurrence）

国の機関、地方公共団体及び重要インフラ事業者等の情報システム担当者等が、組織のネットワーク環境を模擬した環境で、実践的な防御演習を行うことができるプログラムを提供することにより、数千人規模でセキュリティオペレーターを育成

2022年度コース概要

- 毎年 **約 3,000人が受講、2017年度以降受講者累計19,079人**
- 演習は1日間 (Cコースは2日間)
- 集合 (実地) 演習のほか、オンライン演習(個人学習)を実施
- 組織当たり1名でも複数名でも参加可能
- 重要社会基盤事業者、民間企業等は、受講料が必要

  A/B/オンラインコース … 77,000円 (税込)

  Cコース … 121,000円 (税込)

受講者に身につく主なスキル

レベル	該当コース	主な身につくスキル
入門	オンライン入門	集合演習Aコースの受講に必要な最低限の知識を持って、インシデント発生時の対応に備えることができる
初級	集合A オンライン標準	インシデント発生時の対応の流れを理解し、ベンダーからの報告書を読み解くことができる
中級	集合B	CSIRTメンバー、上司、ベンダー等と適切に情報共有し、主体的にインシデント対応ができる
準上級	集合C	インシデント対応時やその前後において、CSIRTメンバー、上司、ベンター等に適切な指示・報告・調整を行うことができる

2022年度実施内容および対象組織

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	開催地	開催回数	実施時期
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	４７都道府県	６９回	７月～翌年２月
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	全国１１地域	２０回	10月～翌年１月
B-2				地方公共団体以外	東京・大阪・名古屋・つくば	１３回	翌年１月～２月
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	東京	３回	10月～翌年２月
標準	ｵﾝﾗｲﾝ演習	初級	システムに携わり始めたばかりの方	全組織共通	（受講者職場等）	随時	５/24～７/19
入門		入門	インシデント発生時の対応の学習をこれから始める、または、始めたばかりの方				翌年1/17～2/24

※CYDERは、(ISC)² が提供する資格の認定継続に必要なCPEクレジット (継続教育単位) 付与対象の演習

CYDERの実施方式（令和４年度）

出前CYDER、CYDERサテライト概要

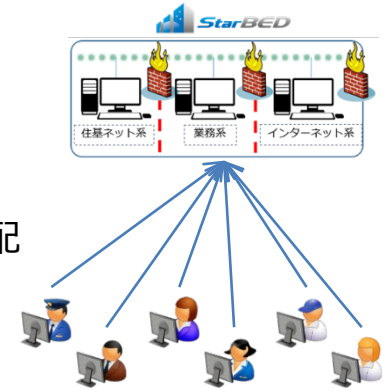
CYDER集合演習 【30人／回】

- 各会場に講師・補助者を手配して、実機演習環境を準備した上で実施

＋

CYDERオンライン演習

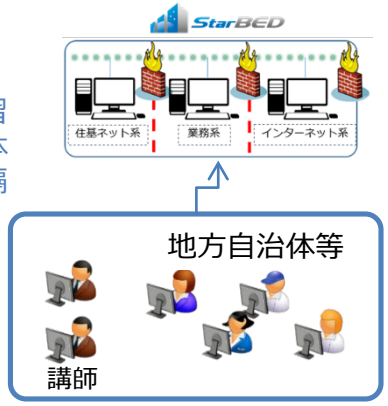
- 形態
  - ✓個人単位での遠隔接続による実機演習
  - ✓録画済み教材
  - ✓機材は受講者手配
- R3年度から本格実施



小規模・柔軟化　　新規実施　　高効率化

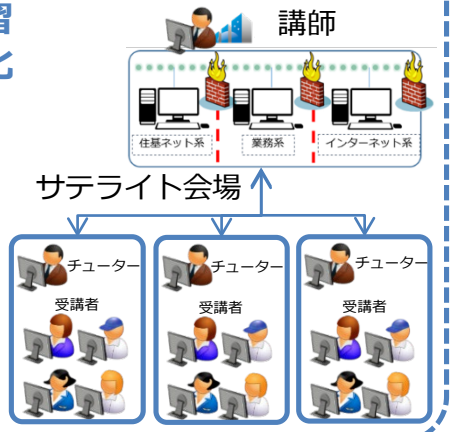
出前CYDER 【10 人／カ所】 2ヶ所

- ✓**未受講自治体の解消**にフォーカス
- ✓ 地理的・時間的要因で集合演習に参加が困難な複数地方自治体等を一か所に集合させた、遠隔接続による実機演習
- ✓ 講師が現地指導にてサポート
- ✓ 自治体等の受講者需要に応じて臨機応変に開催
- ✓ 機材貸与も選択可能



CYDERサテライト 【＋30～人／回】 1ヶ所

- ✓**複数会場での同時演習実施による演習効率化**
- ✓ サテライト会場からの遠隔接続による実機演習
- ✓ 講師は中央に、サテライト会場ではチューターが支援
- ✓ ボトルネックである講師手配の課題を解消
- ✓ 機材貸与も選択可能



CYDERのトレーニング内容・シナリオ

➢ 演習舞台設定

CYDERの演習舞台 (仮想組織のネットワーク) は、コース別に最適化された仮想環境を構築し、実機を用いたハンズオンを通じて実践的なインシデントハンドリングを体験することが可能

➢ 攻撃・対処シナリオ

CYDERの演習で使用されるサイバー攻撃や、それに対処する検知、解析、封じ込め、報告、復旧等の流れは、現実に起きたサイバー攻撃事例の最新動向を徹底的に分析し、コース別に、毎年最新のシナリオを準備。繰り返し受講することにより、最新かつ様々な攻撃に対する対処法を学ぶことが可能

演習シナリオ例

Aコース (2021年度)

① 複数の職員が標的型メール（Emotet）を開き感染し、横展開する
② 展開先の端末がWeb管理者のものであり、Web管理者の端末からWebが改ざんされる

B-1コース (2021年度)

① リモートワーク端末を踏み台として、LGWANへ侵入
② そこから横展開し、展開先で情報を窃取される

B-2コース (2021年度)

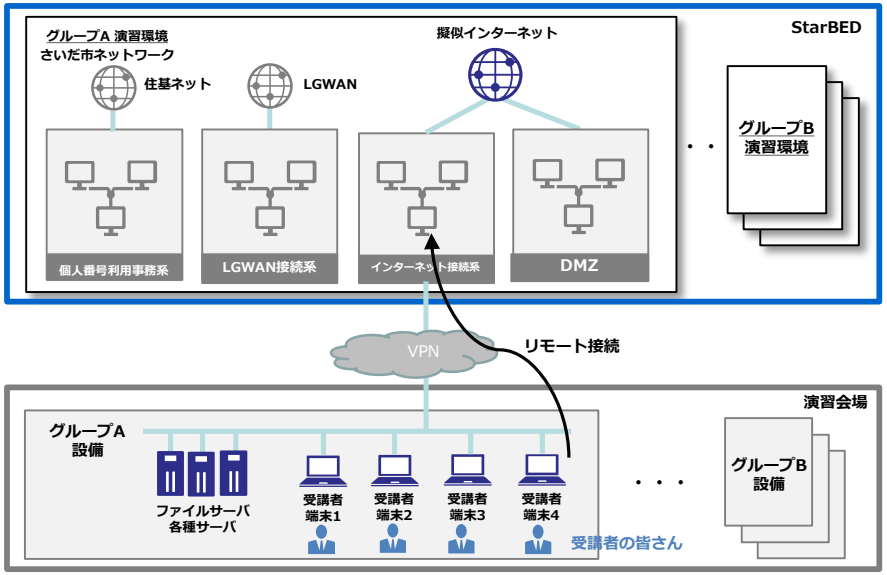
① 国会議員を務める議員のメールアカウントが乗っ取られ、議員がよく連絡を取り合っていたさいだ省職員あてにマルウェア付きメールを送信する
② メールを受信した職員が点府ファイルを開きマルウェアに感染。そこを踏み台とし、省内システムがランサムウェアに感染する

Cコース (2021年度新設)

① 外部公開サーバ経由での侵害を発端とする1つの大規模インシデントを、２日間を通して解き明かす

演習舞台設定例 (B-1コース)

各グループそれぞれに提供するネットワーク構成



非公表

非公表

非公表

非公表

非公表

非公表

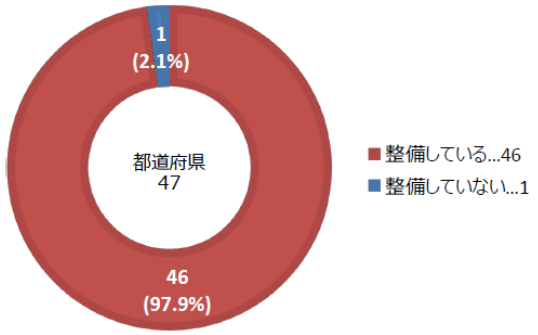
総通局ヒアリングにおいて聴取した課題について

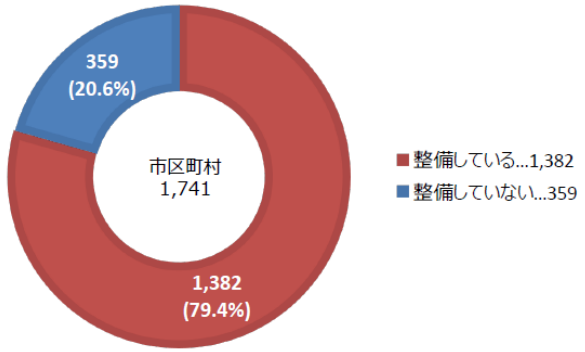
- 特に小規模な自治体は**少人数で兼務しており、時間が取れない**こと、**外部事業者への委託**や危機感の薄さから受講のモチベーションが低い自治体があること等が示された。
- **複数回受講の意欲が低い**こと、**演習時間が長い**ことがネックとなることが示された。
- **オンラインなら小規模自治体でも受講のハードルが下がる**こと等が示された。

- 小規模な自治体は総務課等、担当者が少人数で、議会・災害・コロナ・選挙対応等色々な業務を抱えており、繁忙で参加できない／優先順位が低いという声が多い。
- 担当者が少ない中で1日かけての演習、移動も含めると更に時間がかかることもあり難しいという話を聞く。また、日程が１日だけの設定だと合わせるのが難しい。
- （自治体が連合を作ったり、独自に）システムの一環でセキュリティを外部事業者に委託しており、業者に連絡さえすればいいと思っている。
- サイバー攻撃を身近に感じられない自治体の説得が課題。
- 「未受講だから受けなくてはいけない」と、上から目線で言われるのは抵抗があるという意見があり、演習が必要という基本部分を理解いただけるように工夫する必要がある。
- 一度受けてしまうと、去年受けたからいい、という姿勢になる自治体が多く、複数回受講を勧めているが、なかなか浸透しない。
- 繰り返し受講は大切だと思うが、消防訓練等１～２時間等短時間でできるものと比べると、演習時間がどうしても長い。事前学習も本当にしっかり行うとほぼ1日がかりとなるため、実質2日程度空けるのは難しい。
- オンラインなら受講可能、なぜオンラインが受講済みと評価されないのか、という自治体も多い。受講カウント等、何らかの指標で評価してほしい。
- オンラインを受けたから集合演習は受けなくても良いのではないか、という自治体がある。
- オンライン標準を受講したが内容が難しくて断念したという声もあった。

自治体CSIRTの状況について

- 「自治体DX・情報化推進概要（令和４年３月総務省自治行政局地域情報化企画室）」によると、**都道府県では46団体（97.9%）、市区町村では1,382団体（79.4%）がCSIRTを整備**している。





- 他方で、（各自治体で取組に差はあるものの）**セキュリティ専門人材育成の取組まではできていない**、**全くの別部門から異動して情シス部門へ配属**されることも多い、**外部事業者に委託するケースも多い**等の声も聞いているところ。

- 更なる自治体CSIRTの実態の把握のため、**今年度人材育成需要調査において、以下の点を調査・分析予定**
  - ✓ インシデント対応及び体制の状況/課題
  - ✓ 業務システム・ネットワークの利用状況/課題
  - ✓ インシデント対応に関する外部委託事業者との連携等の状況/課題
  - ✓ インシデント対応関連の訓練・人材育成の要望/課題
  - ✓ CYDER各種コースに対する要望/課題/好事例
  - ✓ CYDERの受講効果・CYDER受講組織のインシデント対応能力（CSIRT の成熟度）の見える化

非公表

非公表

非公表

大阪万博向けサイバー防御演習の新規実施

実施計画(予定)

- 2025年日本国際博覧会（大阪・関西万博）開催に向けて、万博関連組織の情報システム担当者等を対象に、CYDERを基にした人材育成の演習プログラム等を提供する（万博向け演習プログラムの提供）
- さらに高度化・多様化すると見込まれるサイバー攻撃に備えるべく、2025年日本国際博覧会協会側からの要望を踏まえつつ、2025年開催の大阪・関西万博の適切な運営を確保するために、高度な攻撃にも対処可能な人材の育成を、関連組織のセキュリティ担当者等を対象に行う実施できるよう検討。

OSAKA, KANSAI, JAPAN
EXPO2025

サイバー攻撃に対処可能な万博関連組織の人材育成

万博向け演習プログラムの提供

セキュリティイノベーター育成プログラム「SecHack365（セックハックサンロクゴ）」の概要

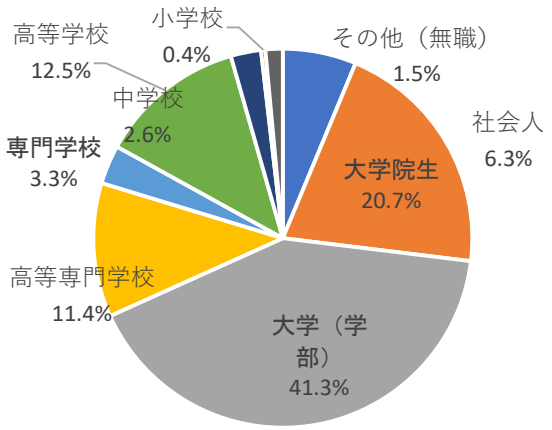
自ら手を動かし、セキュリティに関わる新たなモノづくりができる人材（セキュリティイノベーター）の育成に向けて、若年層のICT人材を対象に、NICTの持つ長年の研究開発のノウハウや、実際のサイバー攻撃関連データとそれらを安全に利用して研究開発が行える環境を活かした、1年をかけて本格的にセキュリティ関連技術の指導を行うプログラム

対象者

- **日本国内に居住する25歳以下の若手ICT人材（学生、社会人、無職等※）**

※2021年度より25歳以下の無職・無収入者へも補助

受講生属性（2017～2022年度）



年間プログラム例(2022年度)

特長

年6回の集合イベント

アイデアソン・ハッカソンのイベントを年6回実施し、継続的に開発指導します。

学生向け支援

学生は受講費用等※を全額補助。学業との両立についての相談や指導も実施。
※旅費等実費相当分

NICTならでは

サイバーセキュリティの研究開発のノウハウや、攻撃データ等を活用できる“NONSTOP”が利用可能。

最先端技術の体験

ゲスト講演や先端企業の見学で発想力やプレゼンテーションスキルを強化。

オンラインでの指導

オンラインで利用可能な開発環境を提供。チャットやタスク管理ツールを活用した継続的な指導。

非公表

非公表