

サイバー攻撃に対する防御演習の実施支援

- 総務省は、サイバー攻撃による被害の拡大を踏まえ、情報通信研究機構（NICT）を通じ、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を対象とした体験型の実践的サイバー防御演習（CYDER※）を全国の総合通信局・所の管内（全国11地域）において2017年から実施。
- 四国総合通信局では、四国管内で開催される演習についての周知や参加の働きかけなどを継続して実施。

※ CYDER：CYber Defense Exercise with Recurrence（参加申込：<https://cyder.nict.go.jp/>）

令和4年度の実施概要

■ 開催形式

集合形式：全国各地で計100回程度開催（A～Cコース）
 オンライン形式：標準コースは5月24日～7月19日まで開催
 入門コースは令和5年1月開講予定

■ 演習内容

受講者は、振り分けられたチーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機を操作しながらサイバー攻撃によるインシデントの検知から対応、報告、回復までの一連の対処方法を体験する。

■ 対象者

情報システム担当者、セキュリティ管理者、CSIRT（コンピュータセキュリティに関する事故対応チーム）要員等

コース名	レベル	主な対象組織	期間		開催エリア
			事前学習	演習	
Aコース ※	初級	すべての組織	2～5時間程度	1日間	全国47都道府県
B-1 コース	中級	地方公共団体			全国11地域
B-2 コース	中級	国の機関、指定法人、独立行政法人、重要社会基盤事業者等		東京・大阪・名古屋・つくば	
Cコース	準上級	すべての組織		2日間	東京
オンライン標準コース	初級	すべての組織		1日間	全国（職場・ご自宅等）
オンライン入門コース	入門	すべての組織			

演習の流れ（実施例）

講義

- ・最新のサイバー攻撃事例紹介
- ・攻撃に利用されるツールや技術の紹介
- ・演習で利用するネットワーク管理ツールや解析ツール等の説明



演習

- ・異常の検知、職員への注意喚起
- ・不審なファイル解析、現状把握
- ・状況のエスカレーション
- ・内部感染の端末、原因の調査
- ・情報漏洩報告
- ・これら一連の作業を実機を用いて演習



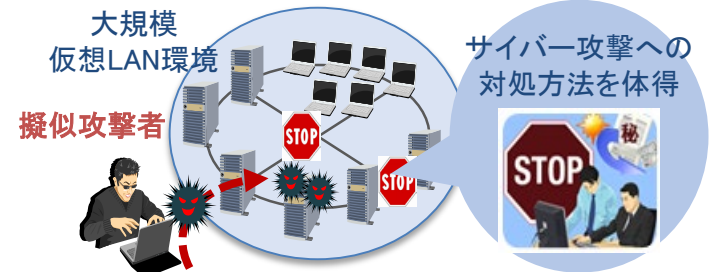
振り返り

- ・演習の振り返り、実機による作業確認
- ・管理する際のポイントやベストプラクティス紹介
- ・演習で学んだ結果や自組織へのフィードバックについてグループ発表



1日にわたるプログラム

演習のイメージ



※今年度の新たな取組として、北海道（幌加内町）及び高知県（須崎市）にて周辺の地方公共団体を対象とした「出前CYDER」（Aコース（初級）の内容）を実施予定。また、近畿総合通信局にて、複数会場を結んで同時開催する「CYDERサテライト」を11月頃に実施予定。