資料７－２

総務省におけるサイバーセキュリティ施策の取組状況について

2024年６月

総務省サイバーセキュリティ統括官室

実践的サイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）

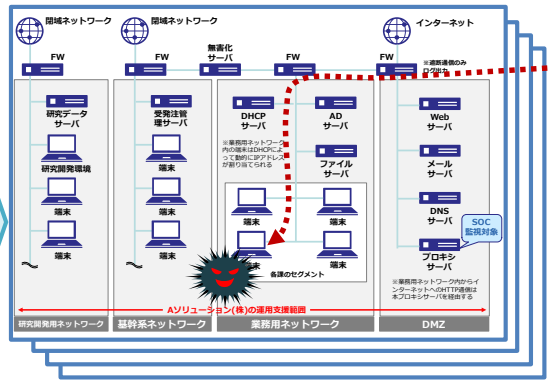
- 総務省は、2017年度から、NICTにおいて、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習**(**CYDER**)を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って、**外部のセキュリティ事業者の支援を受けることを前提としてサイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回・計3,000名規模**で実施(集合コース)。

※ 2017年度:100回・3,009名、2018年度:107回・2,666名、2019年度:105回・3,090名、2020年度:106回・2,648名、2021年度: 105回・2,454名、2022年度: 108回・3,327名、2023年度: 110回・3,742名

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**

演習模様 **専門指導員**による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

2024年度の実施計画

コース名		実施方法	レベル	受講想定者（習得内容）	受講想定組織	実施地	実施回数	実施期間
CYDER	A	集合形式	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	４７都道府県	６４回	７月～翌年１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	１８回	10月～翌年１月
	B-2				地方公共団体以外	東京・大阪・名古屋	１３回	翌年１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・大阪	５回	11月～翌年１月
プレCYDER		オンライン形式	-	全ての情報システム担当者 (最低限必要となる知識の習得と最新化)	全組織共通	(受講者職場等)	-	前半：５月～７月 後半：10月～翌年１月

※プレCYDERは前半と後半で別内容のコンテンツを提供予定

実践的サイバー防御演習（CYDER）受講申込受付開始

- 本年５月、国立研究開発法人情報通信研究機構（NICT）による2024年度の実践的サイバー防御演習（CYDER）について、「集合演習Aコース（７月～９月分）」の受講申込受付を開始。
- 申込みはCYDERのWebサイト（https://cyder.nict.go.jp/）まで。 ※CYDER: CYber Defense Exercise with Recurrence

集合演習Aコースの7～9月開催分について、申込受付を開始しました。

プレCYDERの申込受付開始は、5月21日(火)の予定です。

10月以降開催分の受付開始予定は、こちらをご確認ください。

CYDERパンフレット（2024年度版）

CYDER開催スケジュール（2024年度）

CYDER Aコース（初級、全組織共通）

計64回

地域	実施県	実施日	
北海道	北海道	8/30 札幌	9/6 函館
東北	青森県	9/11 青森	
	岩手県	10/2 盛岡	
	宮城県	7/19 仙台	10/4 仙台
	秋田県	9/27 秋田	
	山形県	10/16 山形	
	福島県	10/8 郡山	
関東	茨城県	7/17 水戸	
	栃木県	7/23 宇都宮	
	群馬県	10/10 前橋	
	埼玉県	10/24 さいたま	
	千葉県	11/21 千葉	
	東京都	7/9 東京	8/9 東京
		8/29 東京	9/3 東京
		10/10 東京	11/27 東京
		12/10 東京	1/10 東京
	神奈川県	8/2 横浜	11/12 小田原
	山梨県	9/5 甲府	
信越	新潟県	9/18 新潟	
	長野県	7/26 長野	10/22 塩尻
北陸	富山県	9/20 富山	
	石川県	9/10 金沢	
	福井県	9/27 福井	
東海	岐阜県	9/10 岐阜	
	静岡県	9/6 静岡	
	愛知県	7/30 名古屋	10/17 名古屋
		11/28 名古屋	
	三重県	10/2 津	

地域	実施県	実施日	
近畿	滋賀県	9/25 大津	
	京都府	9/13 京都	
	大阪府	8/6 大阪	10/24 大阪
		11/13 大阪	12/3 大阪
	兵庫県	10/16 神戸	
	奈良県	9/3 奈良	
	和歌山県	9/13 和歌山	
中国	鳥取県	10/31 倉吉	
	島根県	9/18 出雲	
	岡山県	9/20 岡山	
	広島県	8/30 広島	
	山口県	8/2 山口	
四国	徳島県	10/8 徳島	
	香川県	10/4 高松	
	愛媛県	8/28 松山	
	高知県	9/26 高知	
九州	福岡県	7/31 福岡	12/10 福岡
	佐賀県	11/14 佐賀	
	長崎県	11/1 長崎	
	熊本県	11/12 熊本	
	大分県	11/20 大分	
	宮崎県	11/7 宮崎	
	鹿児島県	7/26 鹿児島	
沖縄	沖縄県	11/26 那覇	

プレCYDER（オンライン形式）

オンライン形式　前半（5月21日から7月19日）、後半（10月から1月末予定）

CYDER B-1コース（中級、地公体向け）

計18回

実施地域	実施日	
北海道	11/8 札幌	
東北	11/15 仙台	
関東	10/9 東京	10/29 東京
	11/1 東京	12/11 東京
信越	11/22 新潟	
北陸	11/26 金沢	
東海	10/18 名古屋	11/29 名古屋
近畿	10/25 大阪	11/14 大阪
	12/4 大阪	
中国	10/29 広島	
四国	11/7 高松	
九州	12/3 熊本	12/11 福岡
沖縄	11/27 那覇	

CYDER B-2コース（中級、国・重ﾌﾗ等向け）

計13回

実施地域	実施日	
関東	1/15 東京	1/17 東京
	1/21 東京	1/22 東京
	1/23 東京	1/24 東京
	1/28 東京	1/29 東京
	1/30 東京	1/31 東京
近畿	1/28 大阪	1/29 大阪
東海	1/24 名古屋	

CYDER Cコース（準上級、全組織共通）

計5回

実施地域	実施日	
関東	11/28~29	東京
	12/12~13	東京
	12/19~20	東京
	1/22~23	東京
近畿	1/30~31	大阪

新しいNOTICEプロジェクトの開始

- マルウェア「Mirai」等に起因する大規模なDDoS攻撃によるネットワーク障害の被害発生等を受け、2019年2月にNOTICEを発足。**ID・管理者パスワードに脆弱性のあるIoT機器**をメインスコープに対処を促進してきた。
- 引き続きID・管理者パスワードに脆弱性のあるIoT機器の乗っ取りが発生しているほか、**ファームウェアに脆弱性のあるIoT機器**の乗っ取りが増加。また、**サイバー攻撃者側も高度に組織化**。

⇒令和6年4月1日「国立研究開発法人情報通信研究機構法の一部を改正する等の法律」施行し、**意識啓発活動を強化**した新NOTICEを発足。※一部規定を除く

【報道発表】IoT機器のセキュリティ向上を推進する新しい「NOTICE」を開始（令和６年３月29日）
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00200.html

目 的

IoT機器のセキュリティ対策向上を推進することにより、

ボットネットによる**サイバー攻撃の発生や被害を未然に防ぐ**

活動内容

活動01 → 脆弱なIoT機器の **観測**

活動02 → IoT機器のリスクと対策への **意識啓発**

活動03 → リスクが高いIoT機器管理者への **注意喚起**

新しいNOTICEプロジェクト（令和６年度からの新たな取組）

観測の強化

IoT機器の乗っ取りにつながる脆弱性を幅広く観測

▼「ID・管理者パスワードに脆弱性のあるIoT機器」を引き続き観測

▼「脆弱性があるファームウェア等を搭載しているIoT機器」、
「既にマルウェアに感染しているIoT機器」も観測対象に追加

意識啓発の強化

IoT機器セキュリティ対策への「必要性に関する気づき」の醸成
IoT機器セキュリティ対策への「心理的ハードル」の低減

▼ロゴ・ホームページの刷新/デジタル広告配信等の広報活動強化

▼ISP/SIer/メーカーなどステークホルダーとの連携を強化

新しいNOTICEプロジェクトの開始　（周知啓発の充実）

HP

https://notice.go.jp/

フライヤー

新しいNOTICEプロジェクトの開始（IoT機器利用者の皆様へのお願い）

➢ 総務省としては、IoT機器の利用者へ、以下のチェック項目における安全管理・対策をしていただけるよう周知・啓発を推進していく。

安全な管理ができているかのチェック項目

設置時

- ☑ 1 推測されにくい複雑な管理者パスワードに変更してください
- ☑ 2 ファームウェアが最新版でない場合はアップデートしてください
- ☑ 3 使用しない機能や設定は無効にしてください

定期的

- ☑ 4 ファームウェアが最新版でない場合はアップデートしてください
- ☑ 5 サポートが終了したルーターやネットワークカメラは買い替えをご検討ください