“守る”テレワークから“攻める”テレワークへ

－テレワーク＆セキュリティセミナーin滋賀－

実践的サイバー防御演習「CYDER」のご紹介

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
研究技術員　有留由記（滋賀出身）

2022/3/3

国立研究開発法人情報通信研究機構（NICT）

CYDER
Cyber Defense Exercise with Recurrence

情報通信分野を専門とする
我が国唯一の公的研究機関

NICTERダークネット観測統計(過去10年間)

CYDER Cyber Defense Exercise with Recurrence

年	年間総観測パケット数	ダークネットIPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2012	約78.0億	190,276	53,206
2013	約128.8億	209,174	63,682
2014	約241.0億	212,878	115,335
2015	約631.6億	270,973	245,540
2016	約1,440億	274,872	527,888
2017	約1,559億	253,086	578,750
2018	約2,169億	273,292	806,877
2019	約3,756億	309,769	1,231,331
2020	約5,705億	307,985	1,849,817
2021	**約5,180億**	**289,946**	**1,747,685**

18秒に1回
攻撃関連通信を受信

出典：NICTER観測レポート2021 https://www.nict.go.jp/press/2022/02/10-1.html

情報セキュリティ10大脅威 2022

■「情報セキュリティ10大脅威 2022」

NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	**1位**	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	**2位**	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**3位**	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	**4位**	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	**5位**	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	**6位**	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	**7位**	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	**8位**	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	**9位**	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	**10位**	不注意による情報漏えい等の被害	9位

出典：IPA「情報セキュリティ10大脅威 2022」2022年2月28日公開 https://www.ipa.go.jp/security/vuln/10threats2022.html

この数字は何?

120社、137件

2021年に個人情報の漏えい・紛失事故を公表した、
上場企業とその子会社の数と事故の件数。

66社、68件

上記数字のうち、不正アクセスなどのサイバー攻撃による事故が起きた社数と、事故件数。

過去最多を記録

出典：東京商工リサーチ「上場企業の個人情報漏えい・紛失事故」調査（2021年）
https://www.tsr-net.co.jp/news/analysis/20210117_01.html

CYDER
Cyber Defense Exercise with Recurrence

「サイバー攻撃？自分には関係ない」

「サイバー攻撃は
大きな組織が受けるもの」

まさかの事態を想定しましょう

CYDER
Cyber Defense Exercise with Recurrence

「自分がサイバー攻撃の加害者に？」

攻撃者に踏み台として利用されれば、
あなたが加害者に。

今できること

CYDER
Cyber Defense Exercise with Recurrence

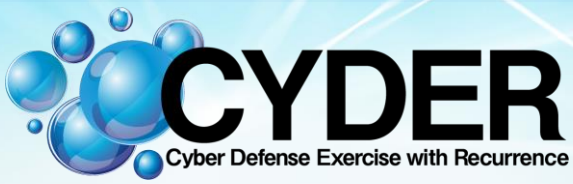
組織がサイバー攻撃を受け事件が発生した時、

「最初にやるべきこと」
「やってはいけないこと」
組織として「事前に準備しておくべきこと」
被害を最小限にするための
「適切な対応手順・方法」

を把握し、一通り訓練しておくこと。

NICT National Institute of Information and Communications Technology

実践的サイバー防御演習
「CYDER」



本演習の目的

CYDER では、サイバー攻撃に対応するため、**自らインシデントハンドリングを実施できるようになること**を目的としています。

サイバー攻撃について理解を深める。対応を学ぶ。

今回の演習でインシデントハンドリングを体験することで、サイバー攻撃について理解を深め、事業継続を脅かす攻撃への対応を学ぶことができます。

サイバー攻撃に対し平時から備え、被害を最小化する。

演習を通じて以下の気づき（ヒント）を得ることができ、みなさんの職務に役立ちます。

- 平時から、どのような備えが必要か。
- 被害を最小化するために、どんな対応をすればよいのか。

一般的なCSIRTの役割

コマンダー（CISO等）

・全体統括　・意思決定
・経営層との情報連携

指示 / 監督　情報提供 / 報告

インシデントマネージャー

・対応状況の把握　・コマンダーへの報告
・対応履歴把握

指示 / 監督　情報提供 / 報告

●記録係（任意）

・インシデントの経緯記録

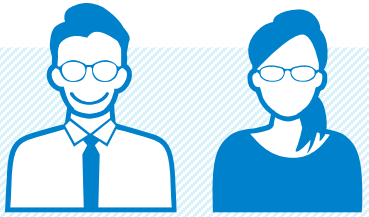
インシデントハンドラー

・インシデント現場監督
・マネージャーへの報告

指示 / 監督　情報提供 / 報告

●PoC、ノーティフィケーション

・組織内、組織外との情報連携
・各関連部署との連絡ハブ、情報発信



●リサーチャー、キュレーター

・インシデントの検知　・情報収集
・分析

CYDER受講生の役割

インシデントハンドリング演習の流れ

CYDER
Cyber Defense Exercise with Recurrence

事前学習（オンライン）

サイバー攻撃の傾向や対策を理解し、集合演習に必要なインシデントハンドリングの心得、基礎知識を学びます。

特徴

① 現実に起きたサイバー攻撃の最新事例を踏まえた**リアルな演習シナリオ**で実践演習を実施。
② 組織の実態に合わせたネットワーク構成で**リアリティのある演習環境**を用意。
③ 講師・チューターの丁寧なサポートがあるので**初学者でも安心！**

集合演習

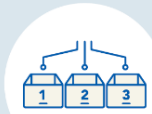
インシデント発生から解決、事後対応までを
グループディスカッションと実機で体験

Flow 1

― 検知・連絡受付

パソコンやサーバーなどの不審な動作を検知。組織内外からの通報を受け付けます。

Flow 2



― トリアージ（優先順位付け）

セキュリティインシデントが疑われる事象に対して、情報収集やログ調査などを行い、事実関係を確認します。インシデントと判断した場合には、被害状況を把握した上で重要度によって対応に優先順位を付けていきます。

Flow 3

― インシデントレスポンス（対応）

組織として、どのように対応すべきか、外部に協力を求める必要があるかなどを検討します。「証拠保全」「封じ込め」「根絶」「復旧措置（暫定対応）」を行います。

Flow 4

― 報告・公表

被害の度合いや影響を及ぼしている範囲に応じて、報告・公表します。組織内部への報告に加えて、被害者、監督官庁や警察機関などの外部関係者にも併せて報告します。

Flow 5

― 事後対応

インシデントに関わったすべての関係者が参加して「振り返り」を実施します。同様のインシデントを防ぐための今後の対応などを含め、最終報告書に取りまとめます。

実践的サイバー防御演習「CYDER（サイダー）」の概要

（CYDER：CYber Defense Exercise with Recurrence）

CYDER Cyber Defense Exercise with Recurrence

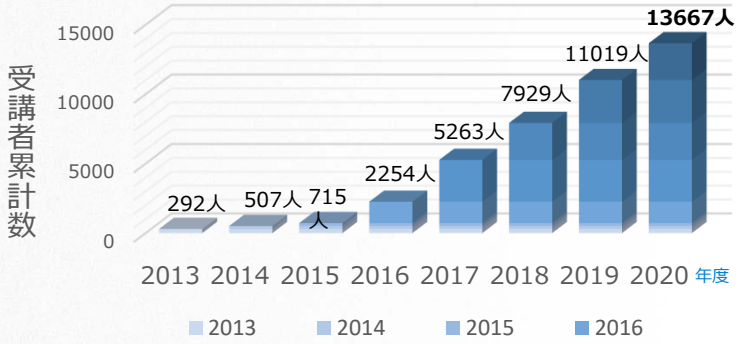
国の機関、地方公共団体及び重要インフラ事業者等の情報システム担当者等が、組織のネットワーク環境を模擬した環境で、実践的な防御演習を行うことができるプログラムを提供することにより、数千人規模でセキュリティオペレーターを育成

2021年度コース概要

- **日本全国で開催**。毎年 **約 3,000人**が受講
- 演習は1日間 (Cコースは2日間)
- 集合 (実地) 演習のほか、**オンライン演習コース (個人演習) を新設**
- 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Aコース … 77,000円 (税込)
Cコース … 121,000円 (税込)

CYDER受講者数の推移 (累積数)



2021年度実施内容および対象組織

コース	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
A	集合演習	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	65回
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	21回
B-2				地方公共団体以外	全国4都市	13回
NEW 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	2回
NEW オンラインA	オンライン演習	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	受講者職場等	-

※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

参 考

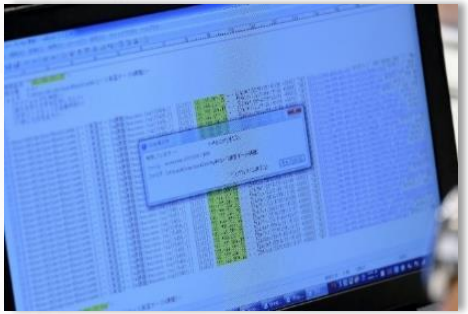
実践的サイバー防御演習「CYDER」の演習風景(2019年度)

CYDER Cyber Defense Exercise with Recurrence

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

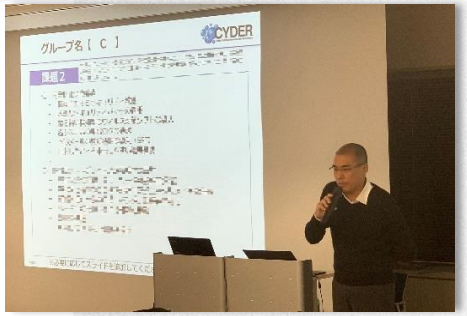


チューターによるサポート

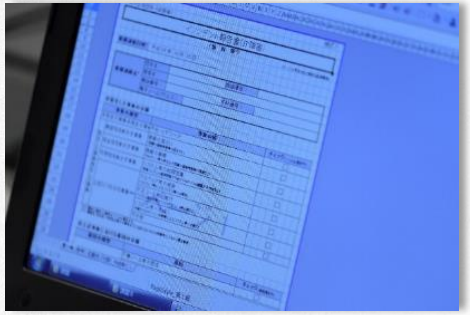
マルウェア挙動調査

グループワーク

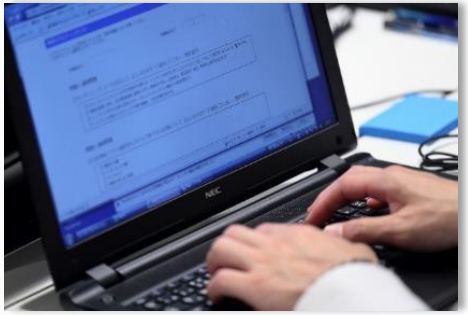
発表



報告書作成



確認テスト



参考

テレワーク環境のリスクと対策

CYDER Cyber Defense Exercise with Recurrence

テレワーク固有のリスクを理解した適切な対応

新型コロナ対応で、十分な準備もできないままリモートワークを実施する組織も多いようです。テレワーク固有のリスクを理解して適切な対応を行う必要があります。

テレワークに関連する事故例

- 大学のリモート授業時に配信したメッセージに、学生の個人情報を誤って添付
- 高校教諭がテレワークのために生徒の個人情報を保存したUSBメモリを紛失
- IT企業が、トラフィック増大等によって障害が多発したため リモートアクセスサービスを終了
- 通信事業者が、リモートアクセスを利用したBYOD端末を経由して VDIサーバーへ不正アクセスを受け、内部情報が流出

テレワークのリスク

- 宅内端末からの情報流出
- 宅内端末を踏み台にした社内への不正侵入
- 宅内端末へのポリシー適用不全による脆弱性の残留
- 宅内端末の通信監視不全による脅威検知の遅延
- 宅内端末への障害対応やインシデント対応の遅延 （遠隔対応、端末の回収、代替機送付等）

テレワークのセキュリティ対策例

- 多要素認証によるVPNアクセス認証の厳格化
- VPNアクセスの監視の強化
- 端末へのエンドポイントセキュリティ(EDR等)の実装による、ネットワークアクセス制限の厳格化、インストール制限、セキュリティパッチ管理の強化、操作監視、インシデント発生時の遠隔分析と隔離
- テレワーク環境の管理と利用の規定の整備

*1:BYOD(Bring Your Own Device)
私有デバイスの業務利用

*2:VDI(Virtual Desktop Infrastructure)
仮想的なデスクトップ環境

事前オンライン学習 サンプル1

第４章　実機演習に必要な知識（使用するツールの紹介）

（標準学習時間：25分）

第４章では、実機演習で必要な知識、使用するツール、使用方法等について紹介します。集合演習当日に利用するツールのためしっかり学んでおきましょう。これからご紹介するソフトウェアは全てフリーです。可能であればソフトウェアをインストールし、触れてみると理解が深まります。

4.1　リモート接続
Windows端末からリモートのLinux端末やWindows端末へアクセスするツールや、ファイルの送受信するツールを学習します。

4.2　メールヘッダ解析
メールヘッダの見方やメールヘッダの詐称の可能性を解説し、不正なメールの見分け方を学習します。

4.3　SPFレコード調査
メールの送信ドメイン認証であるSPFレコードを確認することでメールが詐称されていないことの確認方法を学習します。

4.4　DNS通信ログと出力設定
DNSプロトコルで通信するマルウェアの調査を前提にログ出力の設定方法とログの見方を学習します。

4.5　IOC Finderを使った感染調査
IOCを利用してサイバー攻撃の調査方法の紹介とツールの使い方を学習します。

次ページへ進んで、学習を開始してください。

参考

事前オンライン学習 サンプル2

CYDER Cyber Defense Exercise with Recurrence

参考1.1 最近のセキュリティ事件・事故

日本語のランサムウェアの登場で国内での被害が増加しています。また、ワナクライのように、ワームとして感染拡大できるランサムウェアが出現し、組織への被害が深刻な事例も増えています。

多様化する脅威　～攻撃の傾向（その２）～

ランサムウェアの被害が増加中

- PC内のファイルの暗号化や、スマートフォンの画面のロックを行い、その復元に身代金を要求
- 検出件数が増加、日本語表記のものも確認されており被害が拡大
- Webサイトの脆弱性等を悪用してランサムウェアに感染させるケースが増加中
- 「WannaCrypt(WannaCry、WannaCryptor、Wcry)」（通称：ワナクライ）のように、ワームとして感染拡大する事例が確認された
- 感染したPCだけではなく、共有サーバ等のファイルが暗号化されることも

参考：ランサムウェア「WannaCry(WannaCryptor)」画面

定期的なバックアップと脆弱性対策が重要

参考

集合演習のマイルストーン例

CYDER Cyber Defense Exercise with Recurrence

課題	テーマ	課題概要
1	検知・連絡受付	連絡受付に対する事実確認および対処
2	トリアージ（ログ調査） Hands-on	事実確認のためのログ調査
3	トリアージ（ヒアリング）	現場当事者への指示・依頼
4	対応方針の検討	事実関係の整理、今後の対応方針の検討
5	証拠保全（ディスクイメージ調査） Hands-on	事象の詳細調査（１）
6	証拠保全（マルウェア解析） Hands-on	事象の詳細調査（２）
7	封じ込め・根絶／報告・公表	事実関係の整理、封じ込め・根絶策検討
8	復旧措置・報告書作成	報告書作成
9	再発防止策の検討	改善点の洗い出し

- Hands-on はハンズオン課題、それ以外はディスカッション課題です。
※ディスカッションで検討した内容について、数チームに発表していただきます。その他チームからの質問、助言等の意見交換を行います。

Webサイト https://cyder.nict.go.jp/

次年度の受講をお待ちしております。