NICT 国立研究開発法人 情報通信研究機構

総務省 Ministry of Internal Affairs and Communications

実践的サイバー防御演習 2023

CYDER
Cyber Defense Exercise with Recurrence


ウワーッ!
さいたま市役所
どうかしたのか?
課長! 社内のPCが大変なことに!
もうなんだこれ忙しいときにかぎって
おつかれさまでーす
あっ
ベンダーさん! 助かったー!
まずは状況をご説明いただけますか
全PCに突然警告が出てきてしまいまして…
……これは、個人情報漏洩のリスクにさらされていますね
ええー!
お役に立ちたいのですが、そういう契約は結ばれていませんので。
どどどうすれば良いんですか!?
ええ!?
課長、どうなってるんですか!
あれ、どういう契約にしてたっけ…。
そ
と、とにかくなんとかするんだ!
何をするかは自分で考えろー!
そんな契約はしてないんだけど…
そんな~!
数か月後
ようやく完全復旧しました。
ご苦労だった。無理をさせてしまったな。
君達にCYDER受講させておけばよかったなぁ
どんなに忙しくても、もっといろいろ備えておくべきだった……
はい

大事なのは、被害直後の行動です。

被害に遭うのは、仕方がない。今やそう言ってしまっても過言ではないほど、
毎日多くのセキュリティインシデント※が発生しています。いざあなたの組織に降りかかったとき、
被害を最小限に抑えるためには、対処の「速さ」と「正確さ」、そして「組織内外の連携」が欠かせません。
まずはCYDER（サイダー）を通して被害直後の対応を実践的に学び、
手順や準備を見直すことで、来たるべき「そのとき」に備えましょう。

※コンピューターの利用や情報システムを運営する上で、
セキュリティ上の脅威となる事象や、業務に影響を与える事件・事故のこと。

**こんなことが
起きないって
言い切れますか？**

インシデント発生による被害の実例

市のメールマガジン管理サーバーにて発生

不正アクセスによる個人情報漏洩

市の委託業者が管理していたメールマガジンの管理サーバーが不正アクセスを受け、登録者約200人の個人情報が閲覧可能となり、迷惑メールが約8万件送信された。

町立病院にて発生

ランサムウェア被害による大幅な診療制限

電子カルテシステムなどがランサムウェアに感染し、医療業務の提供に必要な情報が暗号化され、通常診療に戻るまで2か月強の時間を要した。

市のシステム運用委託先にて発生

業務委託先の人為的ミスによる情報漏洩未遂

システム運用を請け負っていた事業者の作業員が、住民情報を含んだUSBを紛失し、約50万人の個人情報漏洩に関する騒動が発生した。

市が管理するWebサイトにて発生

Webサイト改ざんによる公開停止

市が管理する買い物支援に関する情報を紹介するWebサイトが何者かにより改ざんされ、児童ポルノへのリンク情報が掲載されていたため市はサイトの公開を停止した。

**初動対応を誤ると多大な損失を被ります。
費用の他に時間や労力なども奪われ、組織の信用失墜も免れません。**

CYDERってなに？

**CYDERは、組織がサイバー攻撃を受けた際の
インシデント対応をロールプレイ形式で学ぶ演習です。
対応手順を学び、具体的な対処を体験することで、
組織としての平時の備えや被害を抑えるための組織的な
対応方針などの実務に応用できる気づきや知見が得られます。**

集合演習

集合演習に向けて、「事前学習サイト」でセキュリティに関する基礎的な知識や考え方を自習します。
初学者の方も学習が進められるよう、詳しい解説資料や用語集をご用意しています。

演習当日は組織のネットワーク環境を模した仮想環境で、擬似的に発生させたサイバー攻撃に対するインシデント対応の5つの手順を実践します。

マルウェア感染や情報漏洩等のインシデント対応において求められる分析・判断・報告等に必要なスキルが身につきます。

多様な視点に気づくグループ課題

最大4人のグループで、実際のインシデント対応のように協力して課題に取り組みます。意見を出し合って対応を進め、最後に振り返りを行う中で、他組織の受講者の様々な考え方に触れ、自組織に活かせる気づきが得られます。

経験豊富な講師・チューターがサポート

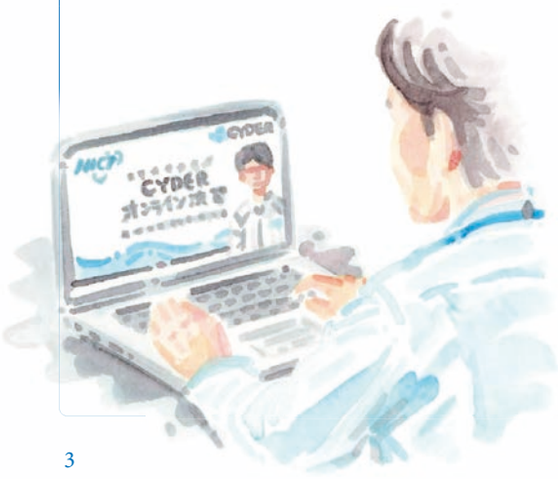
ご質問やお困りごとに迅速に対応します。遠慮なくお声がけいただけるように、実習中は数人が会場を巡回しており、小さな疑問もその場で解決できます。

ツールを操作し実践課題に挑戦

外部ベンダーへの委託内容の理解を深め、円滑に連携できるように、実際のサイバー攻撃事例に基づいた攻撃シナリオを体験する中で、ツールの使用シーンと具体的な操作方法を学びます。

オンライン演習

知識面で集合演習の受講にご不安のある方は、個人向け独習型のオンライン演習をご活用ください。マルウェア感染や情報漏洩等のインシデント対応において前提となる知識やトレンド等が学べます。



オンライン入門コース
（5～7月開講予定）

ログ解析等の実践課題も含めビデオガイド付e-learningにてインシデント対応の前半（証拠保全まで）を学習します。Webブラウザだけで、ご都合の良い時間や場所での受講が可能です。

プレCYDER※
（12～1月開講予定）

さらに短時間でインシデント対応の基本中の基本を学習します。

※2023年度のプレCYDERは、受講対象を国の機関、地方公共団体にご所属の方に限って実施します。予めご了承ください。

**受講後は、CYDERで学んだ内容を職場でも共有し、
自組織のインシデント対応力の向上に活用しましょう。**

CYDERで学べる5つの手順

インシデントの被害を最小限に抑えるには、組織内に限らず外部ベンダーとも連携し、迅速かつ的確に初動対応を行うことが重要です。CYDERでは、課題を通じて5つの対応手順と具体的な対処方法を実践します。

演習シナリオ例

ある日、さいだ市の職員Aさんが、取引業者から納品されたUSBメモリを自分の業務用パソコンに挿入し、USBメモリに入っていたファイルをクリックしました。

step 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。

対処の具体例：ネットワーク監視会社からの連絡「さいだ市職員の業務用パソコンから不正な通信を検出した」の事実確認を行う。

step 2

トリアージ（優先順位付け）

ログ調査、ファイルの解析などを外部ベンダーに依頼し、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。

対処の具体例：不正な通信の内容を確認・分析し、発信源となったパソコンとその利用者を特定する。

step 3

インシデントレスポンス（対応）

組織としての具体的な対応や、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。

対処の具体例：影響範囲を特定し、被害拡大を防ぐため必要であれば専門ベンダー・警察等に協力を仰ぐ。

step 4

報告・公表

被害の度合いや影響範囲に応じて、時には組織内部だけでなく、被害者、監督官庁などの外部関係者にも報告・公表を行います。

対処の具体例：一連の対応を時系列にまとめ、報告書を作成する。

step 5

事後対応

インシデント対応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。

対処の具体例：対応の中で得られた経験や気づきを共有し、現状へのフィードバックを検討する。

もしもCYDERを受講していたら？

実際に起きたあの事例。
インシデント被害に遭った組織にCYDER受講者がいたとしたら、
迷わず対処できたかもしれません。
CYDERで学べる準備や手順がいざという時にどう活きるのか、
昨今のインシデント事例と共にご紹介いたします。

case 1

重要インフラ関連事業者、4か月間メールも使えず

2022年4月、ある重要インフラ関連事業者が外部からの不正アクセスを受け、業務用サーバーおよびバックアップサーバーがランサムウエア（身代金要求型ウイルス）に感染。データが暗号化された結果、同日朝から業務のほとんどができなくなった。辛うじてネットワークに未接続だった25台のパソコンを用いて、大幅に機能制限された中での業務再開となり、職員のメールは復旧までに4か月を要した。

もしもCYDERを受講していたら

想定される最悪の事態に備え、
BCPを策定できていた

あり得る脅威を具体的に知り、
バックアップを十分保護できていた

各機能の復旧までの時間を
大幅に短縮できていた

検知の重要性を理解しているので、
予兆の段階でリスク検知できていた

case 2

病院の電子カルテが長期使用不能に

ある病院で深夜、多数のコンピューターが一斉に使えなくなり、プリンターからは紙が尽きるまで脅迫状が吐き出された。被害に遭った電子カルテシステムは即座に隔離するも、各種システム、コンピューターの総点検を余儀なくされる。ベンダーと協議の上、各社にエンジニアの派遣を依頼したが叶わず、解析のためコンピューターを送付することに。同時に別ベンダーに電子カルテの新規構築を依頼し、復旧に2か月を要した。

もしもCYDERを受講していたら

有識者や警察に相談できる体制を早期に整え、
復旧を早めることができた

攻撃手法を理解しているため、
対応の道筋が見え、
適切な予算投下ができた

初動のスピード感を重視し、
ベンダーとの契約にインシデント対応を
盛り込んでおくことができた

安全なバックアップにより、
復旧の大幅な遅れを避けられた

運命の分かれ道は、CYDER受講を検討している「いま」かもしれません。

実践的サイバー防御演習「CYDER」2023年度コース概要

CYDERでは、受講目的やスキル等に合わせてご自身に合ったコースをお選びいただけます。

集合演習の受講対象者と身につくスキル

マルウェア感染や情報漏洩等のインシデント対応において求められる分析・判断・報告等に必要なスキルが身につきます。

コース名	受講対象者	身につくスキル
Aコース（初級）	・情報システム担当の経験2年以内相当の知識をお持ちの方 ・CSIRTにおいて関係部署や他組織との連絡調整、分析や対応方針検討等のインシデント対応作業を補助する役割を担う方	・インシデント発生時の対応の流れを理解できる ・ベンダーからの報告書を読み解き、ベンダーとの円滑な情報連携ができる ・事前の備えとして何をすれば良いかを理解できる
Bコース（中級）	・情報システム担当の経験2年以上相当の知識をお持ちの方 ・Aコースを受講済みの方 ・CSIRTにおいて関係部署や他組織との連絡調整、分析や対応方針検討等のインシデント対応作業を担う方	・CSIRTの他のメンバー、上司、ベンダー等と適切に情報共有し、インシデント発生時に自らすすんで対応ができる ・パソコン、サーバー、ネットワーク機器等のログを監査できるもしくは監査作業の内容を把握できる ・自組織のセキュリティポリシーを見直すことができる
Cコース（準上級）	・情報システム担当の経験3～4年以上相当の知識をお持ちの方 ・Bコースを受講済みの方 ・インシデント分析や対処法および予防策の検討に必要な知識・スキルを深掘りしたい方	・インシデント対応時に集まる情報を、その背景を含めて読み解くことができる ・インシデント対応時やその前後に、CSIRTの他のメンバー、上司、ベンダー等へ適切な指示・報告・調整を行うことができる ・自組織のセキュリティポリシーを策定し、適切な対策を導入することができる

※集合演習を受講すると、CISSP、SSCP、CCSP等の資格試験を実施する（ISC）²のCPEクレジットを取得することができます。

オンライン演習の受講対象者と身につくスキル

マルウェア感染や情報漏洩等のインシデント対応において前提となる知識やトレンド等が学べます。

コース名	受講対象者	身につくスキル
オンライン入門コース	・情報システム担当の経験1年未満の方 ・情報システム担当経験1年以上でも知識のアップデートをお考えの方 ・集合演習Aコースを受講予定で予習したい方 ・過去に集合演習Aコースの内容が難しく感じたため復習したい方 ・過去にCYDERを受講したことがない方	・集合演習Aコースの受講に必要な最低限の知識（基本的な情報システムや情報セキュリティに関する知識）が習得できる
プレCYDER	・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 ・情報システムに携わり始めたばかりの方 ・過去にCYDERを受講したことがない方	・CSIRT担当者として知っておきたい基礎的な事項を短時間で習得できる（開発中）

※オンライン演習は、CPEクレジット付与対象外となります。

CYDER
Cyber Defense Exercise with Recurrence

コースの種類

演習形式	コース名	レベル	主な対象組織	期間※2		開催エリア
				事前学習	演習	
集合演習	Aコース	初級	全ての組織	2～5時間程度	1日間 (9:30～17:00)	全国47都道府県
	B-1コース※1	中級	地方公共団体		1日間 (9:30～17:30)	全国11地域
	B-2コース※1		国の機関 重要社会基盤事業者等			東京・名古屋・大阪
	Cコース	準上級	全ての組織		2日間 (各日10:00～17:00)	東京
オンライン演習	オンライン入門コース	入門	全ての組織	なし	最短3時間30分程度	全国 (職場・ご自宅等)
	プレCYDER	—	国の機関 地方公共団体等		2～3時間程度	

(※1) B-1コースでは、地方公共団体特有のシステム環境を、B-2コースでは、省庁・企業の一般的なシステム環境を模した仮想環境で演習を行います。ご所属の組織に関係なく、どちらのコースもご受講可能です。ご希望に合うコース、開催地をお選びください。(※2) 申込期限について：いずれの演習形式も受講席数に限りがございますので、早めのお申し込みをお勧めします。(集合演習) Webから申し込む場合の期限は開催日の5営業日前までです。以降に申込をご希望の方は、事務局までお問い合わせください。(オンライン演習) 空席があれば、演習当日でもお申し込みいただけます。

2023年度開催スケジュール予定

演習形式	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
集合演習				Aコース								
							B-1コース					
										B-2コース		
								Cコース				
オンライン演習		オンライン入門コース							プレCYDER			

※予定は変更となる可能性がございます。詳細は決定次第Webサイトにて随時お知らせいたします。

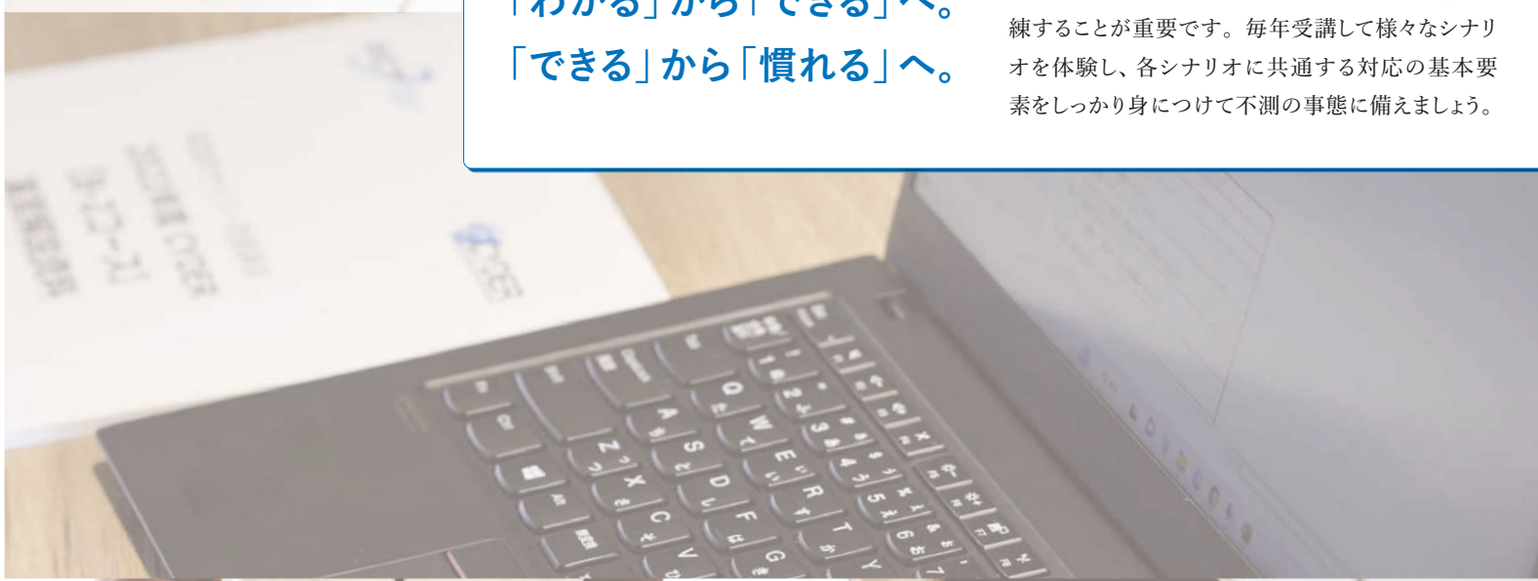
受講費用

所属組織	対象コース	費用(税込)
国の機関、地方公共団体等の情報システム担当者	全コース	無料 ※年度内に複数回受講の場合、一部有料
上記以外の法人・団体に所属されている方 (重要インフラ事業者等の情報システム担当者)	Aコース／Bコース／オンライン入門コース	1受講　77,000円／人
	Cコース	1受講　121,000円／人

※2023年度のプレCYDERは、受講対象を国の機関、地方公共団体にご所属の方に限って実施します。予めご了承ください。

「わかる」から「できる」へ。
「できる」から「慣れる」へ。

防災訓練と同様に、インシデント対応も繰り返し訓練することが重要です。毎年受講して様々なシナリオを体験し、各シナリオに共通する対応の基本要素をしっかり身につけて不測の事態に備えましょう。



CYDER受講者の声

演習を受講して実際に得られた学びについてご紹介します。

自分自身や組織の課題が明確になりました

Aさん／集合演習を受講

これまでインシデント対応を体系的に学んだことがなく、経験から推測して対処していましたが、CYDERで実際に手を動かして一通りの対応を擬似体験したことで、自分自身や組織の課題が明確になりました。

知識に自信が無くても大丈夫

Bさん／集合演習を受講

初学者のためグループ課題が不安でしたが、Aコースは1手順ずつ学ぶので、講義や教材の内容を踏まえて課題に取り組み、グループの方と回答を検討することができました。

自組織のCSIRT設置にも役立ちました

Cさん／集合演習を受講

CYDERの受講により対応や準備のイメージがわき、自組織のCSIRT設置にもつながりました。いざという時のための経験が大切と実感しており、情報システム担当が毎年受講できるよう調整しています。

自分一人では得られない気づきがありました

Dさん／集合演習を受講

自分の視点だけでは気づけないことを、グループ課題や講師の言葉で気づくことができました。また、課題で行き詰まった時も、チューターが積極的に話しかけてヒントを出してくれたのでよかったです。

「委託業者任せ」を見直す機会になりました

Eさん／集合演習を受講

演習でログ解析等を体験して、委託業者に任せている業務について知ることができ、有事の際の委託業者との連携や、自組織の職員が対応するべきことなどを考えるよい機会になりました。

集合演習の復習にオンライン演習を活用しました

Fさん／オンライン演習を受講

今年は業務都合で集合演習を受講できず、オンライン演習を昨年のAコースの復習として受講しました。期間が空いて忘れてしまっていた部分も多くあったため、繰り返し受講することが大切だと感じました。

受講した人が続々と、実践演習の重要性に気づいています。

ナショナルサイバートレーニングセンターについて

情報通信分野を専門とする我が国唯一の公的研究機関である、国立研究開発法人情報通信研究機構（NICT）では、急増かつ巧妙化するサイバー攻撃から我が国を守るため、長年にわたりサイバーセキュリティ技術の研究開発を行っています。ナショナルサイバートレーニングセンターは、それらの研究で得られた技術的知見を活用し、実践的なサイバートレーニングを企画・推進している組織です。

お問い合わせ：国立研究開発法人情報通信研究機構（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
Tel：042-327-5612　Mail：cyder@ml.nict.go.jp　Web：cyder.nict.go.jp
受付時間：9:00–12:00／13:00–17:00　※土日・祝日・年末年始を除く

CYDER

ナショナルサイバートレーニングセンター

WEB検索からもご確認いただけます ▶ CYDER 検索