CYDER
Cyber Defense Exercise with Recurrence

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

誰かがなんとかしてくれるって、
みんなが思ってた。

CYDER

2025

It is no wonder that we are being victimized. It is no exaggeration to say that many security incidents occur every day.
When an incident occurs in your organization, speed, accuracy, and coordination within and outside your organization are essential to minimize the damage.
First, learn how to respond immediately after a disaster through CYDER,
and then review your procedures and preparations to be ready for the coming “when the time comes.”

実践的サイバー防御演習

さいだ市役所 情報システム担当

才羽まもる

私はIT関連の業務を担う公務員。
世間ではサイバー被害が急増中らしいが、
防御演習を経験済みの私にとっては
恐れることではない。

はあ――
それじゃ
事後対応に
取りかかると
するか。

トホホ…

…ん？
こんなボタン
あったか？

ポチッ

ズドドドド

そうとわかれば
やるしかない！

まずは
プレCYDER！

そして
集合演習！

そうか、一回受けて
満足してちゃ
だめなんだ。

あの日以降
CYDERボタンが
現れることは
なかったが、
定期的な防御演習を
心に誓った
才羽なのであった。

繰り返し受講は

つづく

あのー
すみません

ちょっと変な
メールが届いて
しまって…

OK！
それじゃあ
まずベンダーさんに
連絡してと…

つぷるるる…

ついにうちにも
やって来たか。
どれどれ。

……あれ？
まずどう
するんだっけ？
というか、
なんか手口が
進化してない？

そういえば
演習受けたの、
3年くらい
前だったっけ。
ヤバい、
わからん!!

数日後

初動のミスが
響いたことで
大騒動に発展。

……はっ！

ガバッ

これは
もしかして…

7月
8

まちがいない！
情報漏洩が起きる
ちょうど一週間前だ！

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

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ヶ月強の時間を要した。

県の業務委託先にて発生

USBメモリ紛失により情報漏洩

県の業務委託先によるUSBメモリ紛失で、全市民の住民基本台帳の情報や住民税の情報など重要情報が漏洩。損害賠償請求に至ったが、県も管理責任を問われた。

県などの自治体にて発生

大規模アクセス集中攻撃によりWeb閲覧不可に

県などの自治体が利用するセキュリティクラウドの未対策サーバーに対しDDoS攻撃が行われ、Webサイト閲覧やメールの送受信に障害が発生した。

市の受託先にて発生

マルウェア感染によりメール情報が流出

約800自治体が採用する電子申請のヘルプデスクがマルウェアEmotetに感染し、ヘルプデスクで扱ったメール情報が外部に流出した。

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?

事前学習

充実した事前学習で基礎固め

集合演習に向けて、オンライン形式の事前学習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。

集合演習

インシデント対応を体験し実践的なスキルを身につける

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。

CYDERで学べる5つの手順

演習シナリオ例

ある日、さいだ市の職員Aさんのパソコンに巨大なメッセージが表示され、「データを人質にとった。身代金を仮想通貨で払え」と言われてしまいました。

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：メッセージ表示の通報を受け、表示のきっかけとして思い当たることが無いか等を確認する。

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：他のパソコンに同様の表示が無いかを周知確認し、感染・隔離範囲を見積もる。

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、実務に応用できる知見が得られます。

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。

あなたはどちら派?

所属組織のCSIRT※メンバーと同一グループで受講して体制を確認するか、あえて違うグループで他組織の方と交流するか、目的に合わせて選択してください。（可能な限りご希望に沿うよう配慮いたします）

※「Computer Security Incident Response Team」の略。情報セキュリティに関わるインシデントに対処する組織のこと。

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。

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：専門ベンダー・警察等に連絡、アドバイスに従いネットワークの隔離等を実施する。

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、必要に応じて第三者機関の協力のもと報告書を作成する。

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。

プレCYDERってなに?

オンライン演習

スキマ時間の動画視聴で
セキュリティの基礎知識を身につける

これまで、業務や地理的なご都合により
集合演習への参加が難しかった方や、
セキュリティの基礎の基礎からじっくり学びたい方に最適です。

実際の事件に学ぶケーススタディ＋基礎知識

実際に起きた事例をもとに具体的にポイントを説明しているため、事件の内容を確認しながら、適切な対処方法だけでなく、CSIRT※や一元的な窓口の設置、外部委託事業者への依頼内容等、自組織で必要な備えについても学べます。

※「Computer Security Incident Response Team」の略。情報セキュリティに関わるインシデントに対処する組織のこと。自組織のインシデント（事件や事故のこと）に対処する以外にも、インシデント情報、脆弱性情報、攻撃予兆情報の収集・分析、対応方針や手順の策定などを行う。

短時間で要点を押さえられる演習プログラム

10分程度の複数動画で構成。分割受講が可能なため、スキマ時間に少しずつ学習いただくことができます。

経験豊富な講師の丁寧な解説

理解が曖昧だったことや、今更聞けない基本的なことを分かりやすく説明。動画内のクイズでテンポ良く理解が深まります。

開講期間内なら「いつでも」「どこでも」受講可能

Webブラウザとインターネット接続環境があれば、申込みが完了したその日のうちに受講可能。思い立ったらすぐに学べます。

毎年受講することで知識をアップデート

最新事例に基づいた新しいコンテンツを毎年提供予定。受講することで、知識の定着・最新化ができます。

**プレCYDERの
シナリオをご紹介**

“たったひとつの冴えないパスワード編”（5月～7月開講予定）

1人の油断が大惨事に。冴えないパスワードが招いた大量の情報漏洩。さらにはどの業務にもつきものである外注管理などをテーマに、巨大研究機関を揺るがした大事件について詳しく解説します。

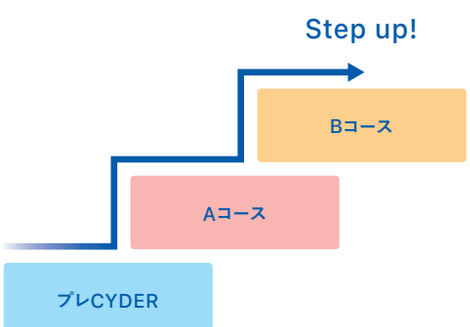
プレCYDERは、サイバー攻撃を受けた際のインシデント対応について、基礎の基礎から学べるオンライン演習です。
DX化が進む昨今において、組織人が最低限知っておくべきセキュリティ知識が身に付きます。

プレCYDERのおすすめ活用方法

その 1

CSIRT / 情報システム課に配属された方の最初の一歩として

CSIRT / 情報システム課に配属されたら、まずはプレCYDERから。CSIRT / 情報システム担当者として最低限知っておきたい知識を習得し、集合演習Aコースへステップアップしましょう。



その 2

一般職員の教育ツールとして

DX化が進む昨今、情報システム担当者でなくともセキュリティの知識は必要となってきています。一方で、職員のセキュリティに対する意識にバラつきがあり、更なる教育が必要という声も耳にします。スキマ時間に動画視聴をすることでセキュリティの基礎知識を習得できるプレCYDERなら、本来の業務で忙しい一般職員の皆さまの負担を最小限に抑えることができます。2024年度も複数の自治体様がこの方法で活用され、「自分たちに直結する内容で危機感を感じた」とコメントいただいています。

その 3

組織幹部層や経営層のセキュリティインシデント情報アップデートツールとして

組織をまとめる幹部層や経営層の皆さまが最新のセキュリティ事情を理解することで、「組織としてどんな対策が必要か」が見えてきます。優秀な情報システム担当者やCSIRT要員がいても、その声を聴きその意味を理解できる幹部層・経営層がいなければ、十分な対策をとることはできずインシデントに巻き込まれてしまいます。実際に起きた事件を元に詳しく説明をしているプレCYDERを受講いただくことで、サイバー攻撃のビジネスインパクトを実感し、自組織の体制はどうなっているのか、自組織に不足しているものは何かを考えるヒントを得られます。

NEWS

プレCYDER 3期 ドリル編

2025年11月～2026年1月開講予定

プレCYDER（3期：ドリル）は、自信をもって集合演習を受けるための準備ができるコースです。Aコースを受講したいけどちょっと自信がない方、プレCYDER（1期・2期：ケーススタディ）受講後にもう少し基礎固めをしたい方にお勧めします。

あなたはどれを受講しましたか？

プレCYDER 基礎から学べるオンライン演習

Aコース 初級レベルの集合演習

1 受講済みならチェック ☐

地方公立病院を襲ったランサムウエアの猛威と診療継続の苦闘

2 受講済みならチェック ☐

たったひとつの弱いパスワードが招いた巨大研究機関の情報漏洩

3 受講済みならチェック ☐

職員が標的型メールを開きウイルスに感染し、その後感染拡大

15 受講済みならチェック ☐

ダークWeb情報をもとにクラウドサービスにログイン、仕込まれたマルウェアが発火

14 受講済みならチェック ☐

攻撃者に乗っ取られたメールアドレスから送られた添付ファイルから感染、その後拡大

13 受講済みならチェック ☐

悪意のある広告を含んだサイトにアクセスしマルウェアに感染、組織内で感染拡大

12 受講済みならチェック ☐

CMSの脆弱性を用いて侵入・改ざんされたWebサイトを発火点とするインシデント

16 受講済みならチェック ☐

VPN接続中にLGWAN系用のサーバーに保存したファイルからマルウェアが発火

17 受講済みならチェック ☐

乗っ取られたメールアドレスから送られた添付ファイルを開き感染、その後感染拡大

18 受講済みならチェック ☐

委託業者端末が攻撃され、窃取された情報をもとに委託元組織情報が窃取される

19 受講済みならチェック ☐

VPN接続中に基幹系用のサーバーに保存したファイルからマルウェアが発火

20 受講済みならチェック ☐

ドッペルゲンガードメインのメールサーバーへのメール誤送信が招いた踏み台攻撃

CYDERシナリオ年表

あなたが受講したのはいつですか？

2017年	2018年	2019年
3 | 8 | 9	4 | 10 | 11	3 | 12 | 13

CYDERは、様々な攻撃手法を取り入れて演習シナリオを作成しています。
あなたはどのシナリオを体験済みですか？ 早速チェックしてみましょう。

4 受講済みならチェック ☐
マルウェア感染したUSBメモリを端末に接続してしまい、感染

5 受講済みならチェック ☐
標的型メール（Emotet）の添付ファイルを開き感染、関係者にマルウェア付きのメールを送付

6 受講済みならチェック ☐
標的型メール（Emotet（亜種））の添付ファイルを開き感染、住民へマルウェア付きのメールを送付

7 受講済みならチェック ☐
標的型メール（Emotet（亜種））の添付ファイルを開き感染、マルウェアを通してWebが改ざん

Bコース 中級レベルの集合演習

11 受講済みならチェック ☐
標的型メールを発火点とし、DNSを利用してC&Cと通信、情報漏えい

10 受講済みならチェック ☐
攻撃者により不正改造されたアプリケーションを発火点とするインシデント

9 受講済みならチェック ☐
持ち出しPCで外部からインターネットにアクセスしマルウェアに感染、組織内で拡大

8 受講済みならチェック ☐
Webサイトの脆弱性を突かれ、管理者ページの改ざんが発生

Cコース 準上級レベルの集合演習

21 受講済みならチェック ☐
委託業者のクラウドサービスでの設定不備が招いた、職員端末でのランサムウェア感染

22 受講済みならチェック ☐
攻撃ツールを用いた脆弱なWebサイトへの攻撃体験と攻撃解析による防御方法の検討

23 受講済みならチェック ☐
組織のVPN装置を経由した、ドメインコントローラーを通したランサムウェア感染

2020年	2021年	2022年	2023年	2024年
5 | 14 | 15	6 | 16 | 17 | 22	6 | 18 | 19 | 22	1 | 6 | 18 | 20 | 22	1 | 2 | 7 | 20 | 21 | 23

あなたにぴったりの受講スタイルは?

A

合計　　個

- ☐ 情報システム担当として3〜4年以上の経験を有し、実務レベルでのインシデント対応を強化したい
- ☐ Bコースを修了していて、より高度な分析・判断スキルを習得したい
- ☐ インシデント発生時の分析・対処・予防策を深く理解し、組織のセキュリティ強化に貢献したい
- ☐ grepなどのコマンドを活用したログ解析の経験があり、実践的なインシデント分析力を強化したい
- ☐ コミュニケーションを取りながらチームで問題を解決し、積極的にディスカッションや意思決定に参加できる

Aのチェックマークが最も多い
あなたにぴったりの受講スタイルは

部門リーダースタイル

例1：部下への教育導入判断のためにプレCYDER（1期・2期：ケーススタディと3期：ドリル）、その後自分のスキル維持のためにCコースを受講。

プレCYDER 1期 / ケーススタディ（5〜8月）
↓
プレCYDER 2期 / ケーススタディ（9〜11月）
↓
プレCYDER 3期 / ドリル（11〜1月）
↓
集合演習 Cコース（11〜1月）

例2：プレCYDER（1期：ケーススタディと3期：ドリル）の後に部下と同じグループでB / Cコースを受講し、組織としての体制を強化。

プレCYDER 1期 / ケーススタディ（5〜8月）
↓
プレCYDER 3期 / ドリル（11〜1月）
↓
集合演習 Bコース（10〜1月）
↓
集合演習 Cコース（11〜1月）

B

合計　　個

- ☐ 情報システム担当の経験2年以上相当の知識を持っている
- ☐ 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立場である
- ☐ コンピューターとネットワーク（特にWindowsとTCP / IP）及びサイバーセキュリティに関する基礎知識を持っている
- ☐ 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できるようになりたい
- ☐ 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ようになりたい

Bのチェックマークが最も多い
あなたにぴったりの受講スタイルは

チームリーダースタイル

例1：知識のアップデートのために、プレCYDER（1期：ケーススタディと3期：ドリル）を受講し、その後にB / Cコースで実践を積む。

プレCYDER 1期 / ケーススタディ（5〜8月）
↓
プレCYDER 3期/ドリル（11〜1月）
↓
集合演習Bコース（10〜1月）
↓
集合演習 Cコース（11〜1月）

例2：プレCYDER（1期：ケーススタディ）/ Bコースを受講後に、プレCYDER（3期：ドリル）を挟んでCコースで知識を深める。

プレCYDER 1期 / ケーススタディ（5〜8月）
↓
集合演習 Bコース（10〜1月）
↓
プレCYDER 3期 / ドリル（11〜1月）
↓
集合演習 Cコース（11〜1月）

積み重ねてきた経験や業務上の立場によって、受講スタイルは異なります。自分には、どのコースがぴったりなのかチェックしてみましょう。

C

合計　　個

- ☐ 情報システム担当の経験2年以内相当の知識を持っている
- ☐ 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立場である
- ☐ インシデント発生時の対応の流れを理解できるようになりたい
- ☐ 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ようになりたい
- ☐ インシデントへの備えとして、事前に何をすれば良いかを理解できるようになりたい

Cのチェックマークが最も多い
あなたにぴったりの受講スタイルは

チームメンバースタイル

例1：プレCYDER（1期：ケーススタディと3期：ドリル）で基礎を固めた後に、A / Bコースで実践を積む。

プレCYDER 1期 / ケーススタディ（5〜8月）
↓
プレCYDER 3期 / ドリル（11〜1月）
↓
集合演習 Aコース（7〜1月）
↓
集合演習 Bコース（10〜1月）

例2：プレCYDER（1期：ケーススタディ）/ Aコースを受講後に、プレCYDER（3期：ドリル）を挟んでBコースで応用力を強化する。

プレCYDER 1期 / ケーススタディ（5〜8月）
↓
集合演習 Aコース（7〜1月）
↓
プレCYDER 3期 / ドリル（11〜1月）
↓
集合演習 Bコース（10〜1月）

D

合計　　個

- ☐ CSIRT / 情報システム課に配属されたばかりだ
- ☐ IT / DX推進リーダー、個人情報を取り扱う業務、パソコン作業を伴う業務に携わっている
- ☐ 組織の幹部層、経営層であり、インシデント対応への組織的な備えの重要性を理解したい
- ☐ 集合演習の受講へ向けて、インシデントハンドリングの基礎を学びたい
- ☐ 基礎的なセキュリティ用語や、ベンダーの報告書内の用語を理解したい

Dのチェックマークが最も多い
あなたにぴったりの受講スタイルは

ビギナースタイル

例1：プレCYDER（1期：ケーススタディ）で最初の一歩を。その後プレCYDER（2期：ケーススタディ&3期：ドリル）で更に1歩。

プレCYDER 1期 / ケーススタディ（5〜8月）
↓
プレCYDER 2期 / ケーススタディ（9〜11月）
↓
プレCYDER 3期 / ドリル（11〜1月）

例2：プレCYDER（1期・2期：ケーススタディ）とプレCYDER（3期：ドリル）で基礎を固め、Aコースで実践力を磨く。

プレCYDER 1期 / ケーススタディ（5〜8月）
↓
プレCYDER 2期 / ケーススタディ（9〜11月）
↓
プレCYDER 3期 / ドリル（11〜1月）
↓
集合演習 Aコース（7〜1月）

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。

初学者にもわかりやすく充実の内容でした

Aさん / 集合演習を受講

私は経験が浅く非常に心配していましたが、講義を終えた時には、インシデント発生から解決に至るまでの工程を具体的にイメージできるようになっていました。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。

毎年受講して知識をUpdateしています

Bさん / 集合演習を受講

情報システム部門に配属されてから毎年受講しています。実際にインシデントに至らずとも通常業務でヒヤッとすることは多々あり、その時に手順を追って対応していく流れはCYDERを受講することで身に付いたと思います。

委託業者さんと対等に話ができるようになりました

C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、今までの「委託業者任せ」の体制から、「対等に議論できる関係性」に変化しました。

ひとり情シスだからこそCYDERは必要だと思います

Dさん / 集合演習を受講

情報システム課は自分ひとりですが、だからこそきちんとした知識を身に付ける必要があると思い、毎年集合演習を受講しています。知識があるからこそ、委託業者との連携もうまくいき、安心して不在にできます。

スキマ時間に受講できて助かりました

Eさん / プレCYDERを受講

業務都合に合わせて、毎日少しずつ受講できたのでとても便利でした。動画では、実際に起きた事件の真相に触れながらセキュリティの基礎についてわかりやすく説明しているので、理解が進みました。

一般職員向けの研修として活用しました

Fさん / プレCYDERを受講

兼ねてより職員のリテラシーの低さが悩みの種で、プレCYDERを一般職員の研修として活用しました。動画を視聴することでセキュリティの基本を効率よく学べること、身近な事例が題材ということで「自分たちに直結する内容で危機感を感じた」と好評でした。

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

National Cyber Training Center

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

実践的サイバー防御演習「CYDER」2025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）	• 情報システム担当として3〜4年以上の経験を有し、実務レベルでのインシデント対応を強化したい方 • Bコースを修了し、より高度な分析・判断スキルを習得したい方 • インシデント発生時の分析・対処・予防策を深く理解し、組織のセキュリティ強化に貢献したい方 • grepなどのコマンドを活用したログ解析の経験があり、実践的なインシデント分析力を強化したい方	• 攻撃者の手法を理解し、ログ解析やネットワークトラフィック分析を通じて、既知・未知の攻撃を識別し、早期検知のための分析フローを確立する「高度なインシデント分析スキル」 • インシデント対応時に収集した情報を適切に解釈し、自組織のセキュリティポリシーに基づいて、迅速かつ的確な判断を下し、適切な対策の検討・導入・運用ができる「対応力」 • CSIRTメンバーや関係者と円滑に連携し、適切な指示・報告・調整を行う「協調力」

※いずれかを満たす方であることが望ましい
●集合演習を受講すると、CISSP、SSCP、CCSP等の資格試験を実施するISC2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
プレCYDER	1期・2期 ケーススタディ	• CSIRT / 情報システム課に配属されたばかりの方 • IT / DX推進リーダー、個人情報を取り扱う方、一般職員 • 組織の幹部層、経営層の方	• 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 • 基礎的なセキュリティ用語やベンダーの報告書内の用語を理解できる • インシデント対応への組織的な備えの重要性を理解できる
	3期 ドリル	• プレCYDER（1期・2期）を受講済みの方 • インシデント対応の流れや基本を押さえたい方 • Aコース受講の準備をしたい方	• セキュリティやインシデントハンドリングの基礎知識を身に付けることができる • インシデント発生時の対応の流れを理解できる

※オンライン演習は、CPEクレジット付与対象外となります。

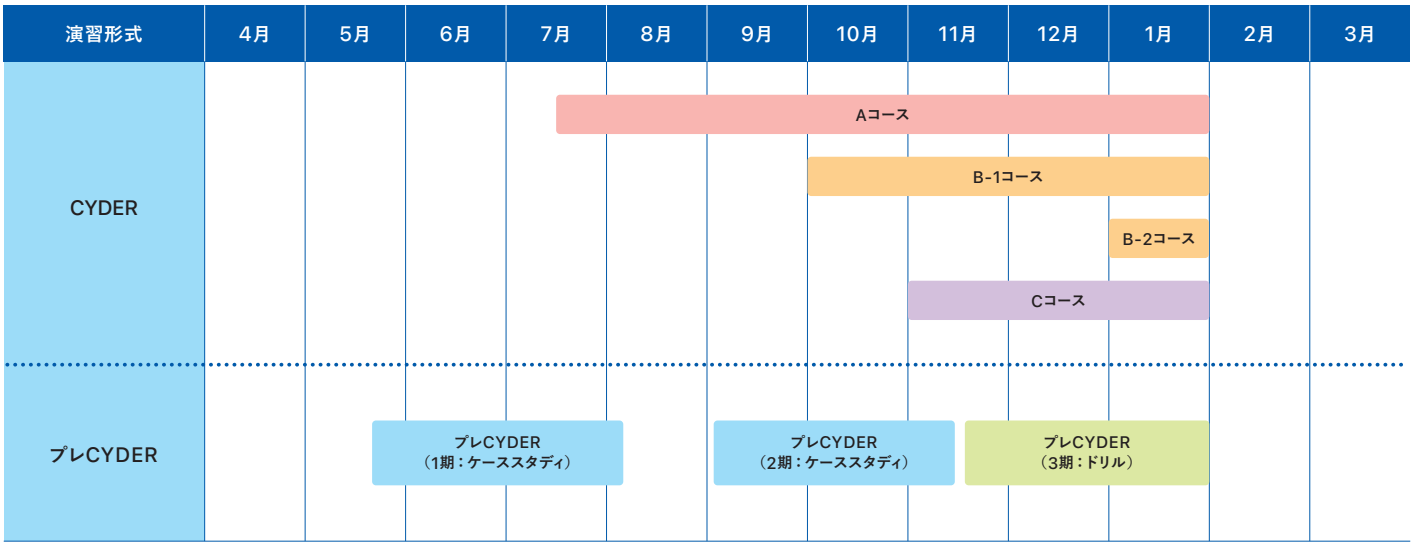
CYDER
Cyber Defense Exercise with Recurrence

コースの種類

コース名		演習形式	レベル	主な対象組織	期間※2		開催エリア
					事前学習	演習	
CYDER	Aコース	集合演習	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8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・大阪
プレCYDER		オンライン演習	—	全ての組織	なし	2～3時間程度※3	全国(職場・ご自宅等)

[※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：(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。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。(プレCYDER)演習当日でもお申し込みいただけます。[※3]プレCYDER(3期：ドリル)は開発中のため演習時間は未定です。

2025年度開催スケジュール予定



※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(税込み)
国の機関等	全コース	無料※
地方公共団体	Aコース / プレCYDER	無料
	Bコース	1受講 77,000円 / 人
	Cコース	1受講 121,000円 / 人
上記以外の法人・団体に所属されている方	Aコース / Bコース	1受講 77,000円 / 人
	Cコース	1受講 121,000円 / 人
	プレCYDER	1受講 11,000円 / 人

※年度内に、複数コースを受講する場合有料となる組合せがあります。詳しくはWebサイトでご確認ください。