実践的サイバー防御演習

CYDER
Cyber Defense Exercise with Recurrence

CYDER 2024

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


さいだ市役所
みんな、おはよう。
おや、なんだか
騒がしいな…
ガチャ
ちょっときみ、なにか
トラブルでもあった？
それが、今朝
私のパソコンに
脅迫メッセージが
届いたんです…。
なんだこれは！
システム担当のきみ、
なんとかしたまえ！
いや～
こんなの
初めてで…。
いたずらだとは
思いますが、
念のためあとで
調べてみますね。
数日後
はい、さいだ
市役所です。
え!!
怪しいサイトに
個人情報が
貼られている!?
なん
だって!?
個人情報流出
は、夢か！
翌朝
いや～
夢でヨカッタ
いまからでも
遅くないから、
早いとこCYDER
受けてもらっとこ。
ガチャ
ちょっと
大変な
ことが…
あ、
部長！
なに！
これじゃあ
また…
まさか
脅迫メッセージが
届いたなんて
言うんじゃ
ないだろうね？
え、どうして
わかったん
ですか…？
もっと早く
CYDERを勧めて
おくべきだった…
完

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。

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たため、市はサイトの公開を停止した。

県などの自治体にて発生

サイバー攻撃により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?

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。

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。

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。

こんな活用法もあります

所属組織のCSIRTメンバーと同一グループで受講し、有事の際にそれぞれの役割を果たせるか、CYDERの会場で腕試し！本番さながらの環境で自組織のCSIRTの体制を確認することができます。

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。

プレCYDERってなに？

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。

オンライン演習

隙間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。

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。隙間時間に分割受講が可能なため、すき間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。

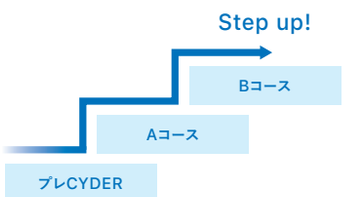
毎年受講することで知識をアップデート

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のおすすめ活用方法

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、基礎知識が身に付いてきたら集合演習Aコースへステップアップしましょう。



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。隙間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。2023年度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。

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。

あなたにぴったりのCYDERは?

リアル会場で実践的な体験ができる集合演習の「CYDER」と、職場から気軽に受講できるオンライン演習の「プレCYDER」から、
ご自身のスキルレベルやご都合に合わせて、ぴったりのコースを見つけてください。

あなたに最適なコースが
きっと見つかります

START

A
インシデントハンドリングについて基礎から学びたい

B
インシデントハンドリングの基礎知識をすでに身につけていて、さらにレベルアップしたい

A

過去にAコースを受けたことがある

Yes

インシデント発生時の対応の流れを思い出すことができる

No

No

ベンダーからの報告書を読み解ける

Yes

B

インシデントハンドリングを俯瞰的に見てチームを統括できるようになりたい

No

攻撃者の心理を知り実践に役立てたい

Yes

A
近くに演習会場がない等、会場での受講が難しく、CYDERを職場やご自宅から体験してみたい

B
異なる役割が付与されたチームメンバーとコミュニケーションを取りながら、実践的に初動対応を学びたい

No

Yes

A

B

プレCYDER
（全ての組織）

基礎から学べるオンライン演習

セキュリティインシデントに関する基礎的な事項について、職場等からオンラインで学べるコース。実際に起きた事例に基づいたリアルな内容で知識の理解が進みます。CSIRTや情報システム課に着任したばかりの方だけでなく組織内の一般職員の方や経営層の方にもお勧めです。

Aコース
（全ての組織）

初級レベルの集合演習

全国47都道府県で受講可能。セキュリティインシデントの発生から報告までの一通りのインシデント対応手順を、実際にパソコンを操作しながらステップ・バイ・ステップで学びます。経験豊富な講師・チューターのサポートを受けながら進めるため初学者でも安心して受講できます。

地方公共団体の職員である

No

Yes

Yes

No

B-1コース
（地方公共団体）

B-2コース
（国の機関・民間企業）

中級レベルの集合演習

仮想のセキュリティインシデントについて、チームで実際にパソコンを操作しながら解決方法を検討し、実践的な対応を学びます。B-1コースでは、自治体のシステム環境を、B-2コースでは、省庁・企業の一般的なシステム環境をそれぞれ模した仮想環境で演習を行います。

No

Yes

Cコース
（全ての組織）

準上級レベルの集合演習

より高いレベルでインシデントハンドリングをコントロールすることを目的としたコース。2日間の演習で、攻撃者の攻撃手法に対する理解を深めその痕跡を追うハンズオンなどに取組みながら、インシデントの全体像の把握に必要なコミュニケーションやポリシーに基づく判断ができる様になることを目指します。

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。

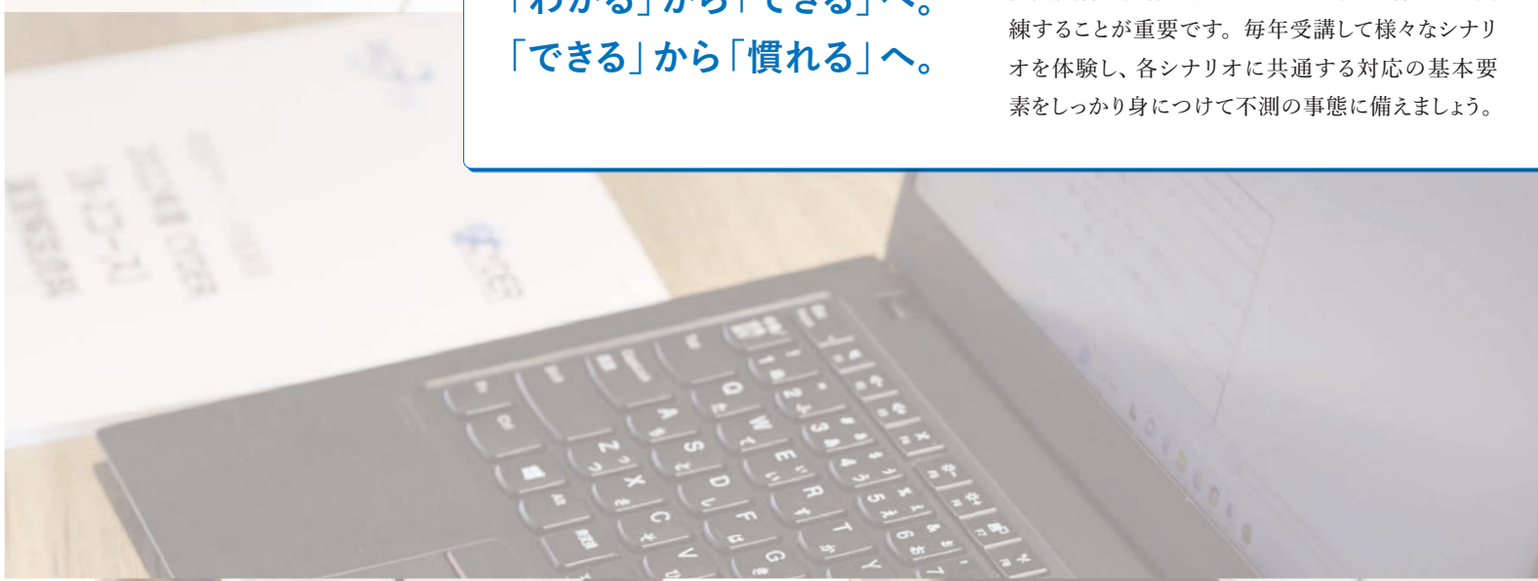
もしもCYDERを受講していたら

- 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。

「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。

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。事前学習で得た知識が、演習を通して自分のものになったと実感しました。

自分一人では得られない気づきがありました

B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。

インシデント対応に役立ちました

Cさん／集合演習を受講

昨年Aコースを受講後、職場内でセキュリティインシデントが発生しましたが、慌てることなく対応することができました。座学とグループワークで実践的に理解を深めることができるので、継続して受講しています。

「委託業者任せ」を見直す機会になりました

D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。

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。

組織内の教育ツールとして活用しました

Fさん／プレCYDERを受講

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から、各課のITリーダーの教育ツールとして活用しました。「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