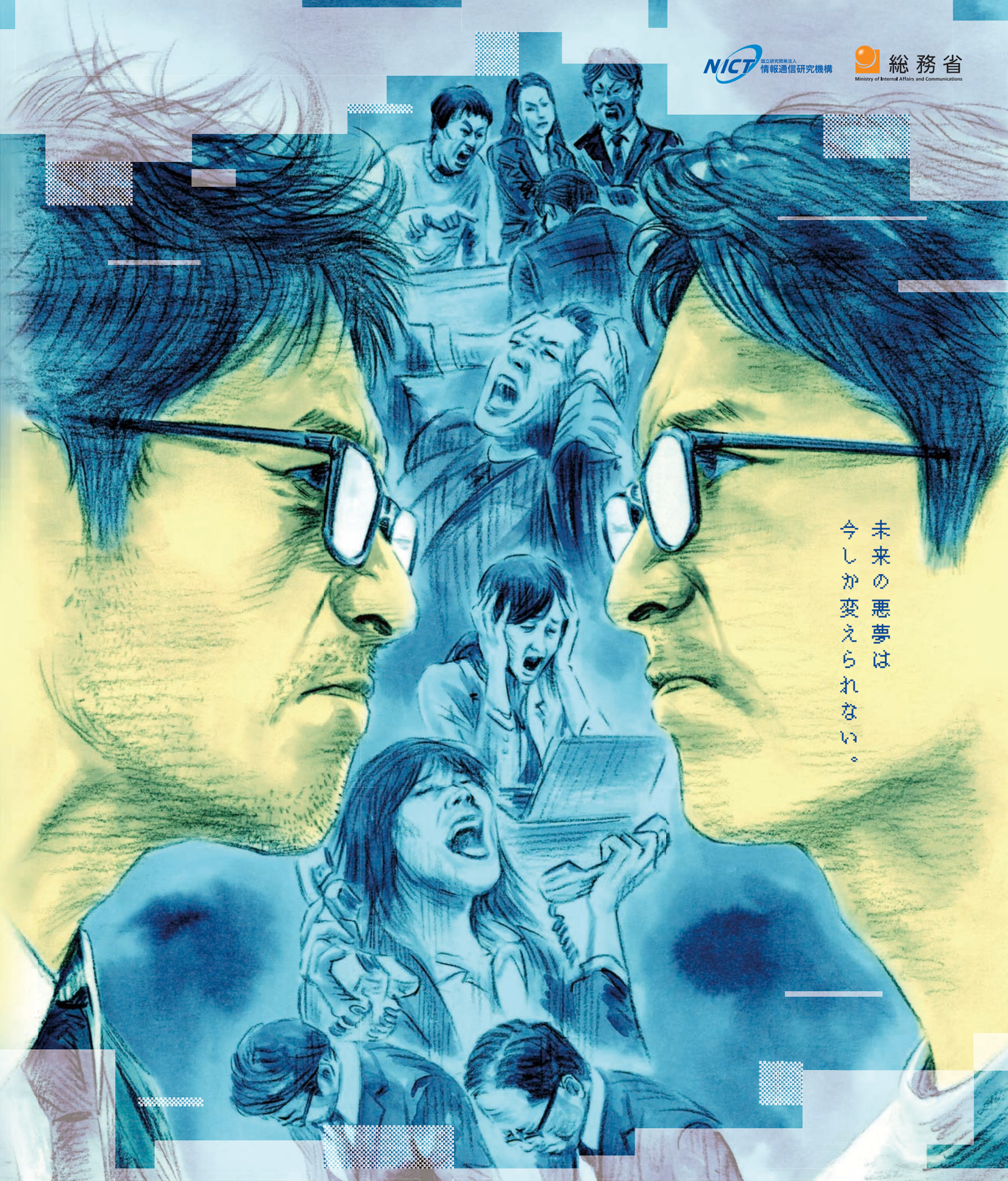


NICT 国立研究開発法人 情報通信研究機構

総務省 Ministry of Internal Affairs and Communications

CYDER 2026

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


わ
なんだ!?
シュウウウ…
さいだ市役所 情報システム担当
才羽まもるの自宅にて
驚かしてすまない
3分だけ時間をくれ
私はCYDERボタンで
1年後の未来から
やってきた君だ
……ほお
SFものでよく見るやつか
む やけに物分かりがいいな
では単刀直入に言おう
君は一年後
サイバー攻撃の
対処に失敗して
大変なことになる
そんなはずはない
ちゃんと本で
勉強しているからな
はぁ～君は
いつもそうだな
自信過剰で傲慢で
そんなだから
友達も少ないんだ!
なんだと
友達が多いと偉いってのか!
とにかく
今のお前に必要なのは
実践経験なんだよ!
なにー?
そんなこといって
過去の自分に責任を
押しつけに来ただけ
なんじゃないの～?
それに経験経験って
インシデント被害に
遭えとでもいうのかよ
バーン
CYDER
そのために
CYDERが
あるんだ!
なんだそれ
俺はコーラ派だ!
ゴクゴク
とにかく
知識だけじゃなく
必ず経験も
積んでおくんだぞ!
シュウウウ…
じゃないと
大変なことに
なるからな!
くそ さすが私だ
まったく聞く耳を
持たない!
ジジジ…
わざわざこんな…
本で勉強すれば
十分さ
CYDER
一年後 さいだ市役所
ザワザワ
才羽
なんとかしてくれ!
このままだと
大変なことになるぞ!
よし
まかせろ!
カタカタ
…ってあれ?
なんでうまく
いかないんだ…?
……
これって
あのときの…
みんなすまん
ちょっと
行ってくる!
えーっ!
わ
なんだ!?
突如出現した
CYDERボタンを押し、
過去の自分に会いに行く
才羽なのであった…
CYDER
ポチッ

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

大手通販会社にて発生

ランサムウェア攻撃を受け、受注・出荷など基幹システムが長期間停止

事業委託先に付与された管理者アカウントのID・パスワードが漏えいし、ランサムウェア攻撃を受けた。約74万件の顧客情報流出の可能性がある。

県の業務委託先にて発生

業務委託先によるUSBメモリ紛失により情報漏えい

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など重要情報が漏えい。損害賠償請求に至ったが、県も管理責任を問われた。

民間企業にて発生

社長なりすましでLINE誘導、8000万円被害

社長を名乗るメールで社員にLINEグループ作成を指示。業務を装い送金を急かし、指定口座へ約8000万円を振り込ませて詐取。

市などの自治体にて発生

偽サポート警告にだまされ、個人情報漏えいの可能性

市の委託先従業員がPCに表示された偽警告にだまされて連絡してしまい、偽サポートセンターの指示に従ってPCを操作したことで個人情報漏えいの可能性。

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えい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「データを人質にとった。身代金を仮想通貨で払え」と巨大なメッセージが表示されました。

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

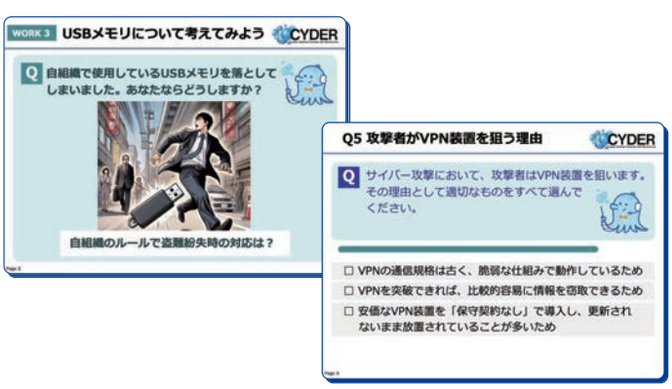
スキマ時間の動画視聴で
セキュリティの基礎知識を身につける

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。

※プレCYDERはセキュリティ学習のはじめの一歩にすぎません。
インシデント対応を習得するには、集合演習の受講が必要です。

ケーススタディ

未経験でCSIRT / 情報システム課に配属されたら、まずはプレCYDERケーススタディから。
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、プレCYDERドリル、
集合演習Aコースへステップアップしましょう。



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。

プレCYDERのシナリオをご紹介

セキュリティ入門者向け ｜ 難易度 ★☆☆

紛失USBメモリが招いた信用失墜編（1期）

膨大な個人情報が記録されたUSBメモリを紛失してしまったら、あなたならどうしますか? 使用する上で欠かせない「USBメモリの適切な扱いに関する知識」や「組織としてのリスク管理」、そして「委託先管理等も含めた日々のインシデント対策の重要性」を、実際にあった事例を紐解きながらわかりやすく説明します。

プレCYDERのシナリオをご紹介

セキュリティ入門者向け ｜ 難易度 ★★☆

閉域網神話の崩壊・甘い認識の代償編（2期）

「インターネット非接続の閉域網だから安全」「うちの委託業者は大丈夫」そんな思い込みはありませんか? 委託業者を起点に発生した医療機関へのサイバー攻撃（サプライチェーン攻撃）の実事例を通じ、侵入経路や運用の弱点、復旧までの全プロセスを追体験することにより、インシデント発生時の意思決定と組織対応を学ぶことができます。

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、組織人として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。

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。

ドリル

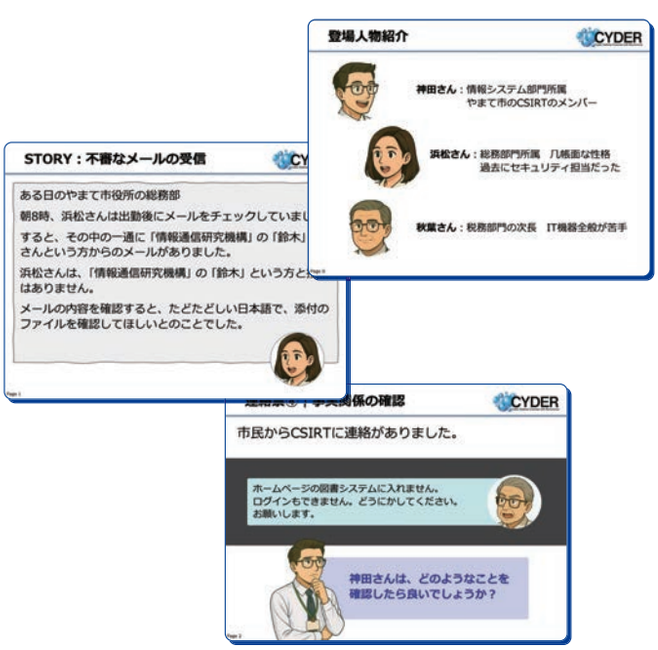
インシデント発生時の初動対応の基本フローについて、ストーリーとクイズを繰り返して反復学習をします。Aコース（初級レベル）受講へのステップアップや、Aコース受講後の知識定着フォローを支援するCSIRT入門コンテンツです。

リアリティ溢れるストーリー展開

やまて市役所を舞台に、CSIRTメンバーの神田さん目線でストーリーが進んで行きます。神田さん目線で考えクイズを解き進めていくことで、まるで本当にインシデント対応を経験しているような感覚を味わえます。

反復練習で応用力が身につく演習プログラム

異なる状況のインシデントハンドリングに繰り返しチャレンジすることで、様々なケースに対応する応用力が身につきます。



プレCYDERのシナリオをご紹介

セキュリティ入門者向け ｜ 難易度 ★★☆

知～ドリル学習1 トリアージ編（1期）

CSIRTメンバーの神田さん（主人公）目線で、次々と起こるインシデントのトリアージ（優先順位付け）に挑みます。職員や市民との会話を織り交ぜながら進むストーリーなので、ちょっとした擬似体験感覚を味わいながら、トリアージの基本が身につきます。

管理者の皆さま、あなたの組織は大丈夫ですか?

近年、サイバー攻撃で業務停止に追い込まれるなど、
大きな被害に繋がる例が増えています。
さまざまな業種や業態が攻撃の対象となり、もはや他人事ではありません。
皆さまの組織は、いざという時にきちんと対応できますか?

CSIRT設置はしたけれど

- ☑ サイバー攻撃が多発する今、
  設置は必須と言われてとりあえず整えた。
- ☑ テンプレートなどを使って必要な文書も整備したが、
  気づけばそのまま何年も経過している。
- ☑ 設置当時からはメンバーも入れ替わり、
  設置当時の経緯を把握しているメンバーはゼロになってしまった。

→ **みなさんの組織は、こんな状況ではありませんか?**

きちんと機能する組織にするには

- ☑ データやシステムのバックアップは大事だと聞き、
  仕組みを整えたが、本番環境で戻したことは一度も無い。
- ☑ インシデント対応の手順を考えて文書化したが、
  通しでの訓練をしたことがない。
- ☑ 文書整備の主担当が抜けてしまい、
  意図や目的がきちんと把握できているか心許ない。

→ **もし、こんな不安があるのなら、
実地に近い訓練を考えてみてはいかがでしょうか?**

新任を素早く立ち上げるには

- ☑ 毎年のように新任が配属されてくるが、
  CSIRTなど専門性が高い分野では
  どうしても立ち上がりが遅くなってしまう。
- ☑ 専門外から来た新任者に独学してもらうにしても、
  良い教材やコンテンツの当てがない。
- ☑ どういう研修に行かせれば良いか、
  どんな研修があるのかがよくわからない。

→ **リアルに近い体験と知識を一気に得られるCYDER演習は、
本番のようにチームで対応し実機にも触れられる集合演習と
オンライン独習型のコンテンツがラインナップされています。**

→ **演習後の生生しい感触を持ち帰り、
自組織の文書や手順に効果的なフィードバックを行えます。
それらによってあなたの組織はより強靭になっていくはずです。**

CYDER活用自治体モデルケース

演習コンテンツの使い方の工夫や自組織内の別演習への応用など、
CYDERをさまざまなアイディアで活用している自治体を
モデルケースとしてご紹介します。

Case 1 組織全体のセキュリティ強化

モデルケース　大阪府島本町 様
人口：3.3万人

CYDER活用による全庁的セキュリティ強化の取組

島本町では、CYDERで使用している報告書を参考に独自の報告書様式を整備するなど、インシデント発生時に備えた準備をしている。各所属からDXなどに前向きに取り組める職員をデジタル化推進委員として選任し、各所属長とともにプレCYDER受講を必須化することにより、全庁的なセキュリティ知識の底上げを図っている。あわせて、仮想ブラウザやファイル送受信サービスの導入、自前のサーバーを構築した標的型攻撃メール訓練、監査の実施やセキュリティポリシーの改訂などを進め、職員の意識改革と組織全体のセキュリティ強化に取り組んでいる。

Case 2 強い情報システム担当者育成

モデルケース　埼玉県庁 様
人口：732.2万人

CYDERで学んだ知識を活かしシステム障害対応訓練を実施

埼玉県庁では、CYDERで学んだ知識を活かしシステム担当者向けの訓練を実施。初学者も参加できるように、CYDERの演習手法を参考にした独自シナリオを作成しているほか、各システムのベンダーにも参加してもらうことで、ベンダー側との意識合わせが可能となり充実したマニュアル改定が可能となっている。

Case 3 全職員のセキュリティ教育

モデルケース　北海道石狩市 様
人口：5.7万人

全職員向け研修として、プレCYDERを活用

石狩市では、プレCYDER「たったひとつの冴えないパスワード編」を、全職員向けの研修として活用。アカウント作成の手順マニュアル、視認性を高めるためのチラシの作成や、受講特設会場を設置し受講しやすい環境を準備する等の工夫で、庁内の全職員の9割以上が受講修了となった。

Case 4 全職員のセキュリティ教育

モデルケース　静岡県吉田町 様
人口：2.8万人

全職員にも実践的なインシデント対応研修を実施

吉田町では、セキュリティ担当課員は全員CYDERのAコースを受講済みで、部門統括は3年前に受講した際の演習テキストを机上に置き読み返し知識の定着化を図っている。

また、委託契約をしているCIO補佐官のアドバイスで、インシデント対応研修を全職員向けに毎年実施している。各課から1名ずつ参加してのグループワークで、インシデントが起きた際に所属する課員としてどう動くべきかをふせんに記入してホワイトボードに貼っていくもので、各課から参加する1名は毎年メンバーを変えることになっているので、年々受講経験者が増えていくことで、万が一の時への備えに厚みを増していくことができている。

関連法規

- 国立研究開発法人情報通信研究機構法（NICT法）
- 個人情報の保護に関する法律
- 行政手続における特定の個人を識別するための番号の利用等に関する法律（マイナンバー法）
- サイバーセキュリティ基本法
- デジタル社会形成基本法
- 重要電子計算機に対する不正な行為による被害の防止に関する法律（サイバー対処能力強化法）

関連法規の詳細は
CYDER公式ウェブサイトから
ご覧いただけます。 →

https://cyder.nict.go.jp/hourei/index.html

あなたはどのシナリオを受講しましたか？

CYDER演習の過去のシナリオをまとめてみました。
ひとつの分類からの学びだけでなく、
複数の分類からの学びで強靭な対応力を身に付けましょう。

メール起点（標的型メール・添付・アカウント乗っ取り・誤送信含む）

［特徴］
- 組織内一般利用者狙い
- AI等によってこれまであった違和感が薄れ、見分けが困難
- 外部に開かれた部門・部署が弱い
- 誤送信は変わらず多発
- メール起点のフィッシング詐欺は増加傾向
- ショートメッセージ、メッセンジャー等も

［過去シナリオ］
- 職員が標的型メールを開封→感染拡大、マルウェア経由でWeb改ざん
- 標的型メール起点→DNSでC&C通信、情報漏えい
- 乗っ取られたメールアドレスからの添付で感染→感染拡大
- ドッペルゲンガードメインのメールサーバーへ誤送信→踏み台攻撃狙い

Web / サーバ侵害起点

［特徴］
- 設定ミス起点はクラウドにも共通する要素
  公開資産（Web / CMS / サーバ）が入口
- 委託先管理的側面も

［過去シナリオ］
- Webサイト脆弱性悪用で侵入→管理者ページ改ざん
- CMS脆弱性で侵入・改ざんされたWebサイトが発火点
- 外部公開サーバの侵害を発端とする大規模インシデント

リムーバブル / 端末持ち出し・Web等閲覧起点

［特徴］
- 組織内一般利用者狙い
- 組織内一般利用者（非専門）のPC等経由
- 従来型境界防御だけでは予防・検知が困難

［過去シナリオ］
- 地方自治体：マルウェア感染USBを接続→感染拡大
- 持ち出しPCの外部での利用時に感染 →組織内感染拡大
- マルバタイジング含むサイト閲覧で感染→感染拡大

ランサム攻撃

［特徴］
- 組織内一般利用者狙いもある
- 近年多発、ビジネスインパクトが大きい
- バックアップの実効性?
- 閉域網の幻想や委託管理の課題、
  サプライチェーン問題等を意識させる

［過去シナリオ］
- 地方公立病院：ランサムウェア被害、頼る先も無く診療継続に苦闘
- 救急病院：委託業者VPN装置経由、閉域網を過信しネットワーク分離不足
- 委託業者のクラウド設定不備→市職員端末でランサム発火
- VPN装置経由→ドメインコントローラー経由でランサム感染狙い

認証情報悪用 / サプライチェーン / 外部経路（クラウド・VPN・委託・改ざんアプリ等）など

［特徴］
- 組織内一般利用者及び設定ミス狙い
- クラウド等新たな基盤への移行を経て
  近年増えつつある複合的な攻撃パターン
- サプライチェーン等、側面からの攻撃も
- ゼロトラスト / ID統制など対抗策も複雑化

［過去シナリオ］
- 国立研究機関：クラウド上の弱いパスワード→研究機関の情報漏えい（認証突破）
- 攻撃者により不正改造されたアプリが発火点（サプライチェーン / 改ざんソフト）
- ダークWeb情報でクラウドログイン
  →マルウェア仕込みが発火点（認証情報漏えい悪用）
- VPN接続中にマルウェア含むファイルを基幹系（LGWAN系）ファイルサーバへ保存
  →感染拡大
- 委託業者端末が攻撃→窃取情報をもとに委託元の情報も窃取（サプライチェーン）

インシデント初動の日ドキュメント
（事例に学ぶ初動対応）

2022年10月31日、大阪急性期・総合医療センターを襲ったランサム攻撃は、
早朝の異変であらわになった

［時刻］	［状況］
5:45	給食事業者の病院配置担当者が電子カルテの不調を最初に発見。
5:50	看護師長も「画面が切り替わるのが遅い」と異変を察知。
6:20	電子カルテが一瞬復活。周囲は安堵するが、 看護師長だけは「これは逆におかしい」と疑念。 
7:10	基幹システムに障害が拡大。朝の回診が混乱し始める。
7:45	医療情報システム担当が通勤電車で「英文メッセージ（暗号化警告）」を知る。
8:20	給食事業者の病院配置スタッフが 病院事業者側のウイルス感染の可能性を病院に伝える。
8:30〜8:50	複数サーバでランサムノート確認。 ベンダーが到着・確認し、ネットワーク遮断実施。 
8:50	幹部会議→「ランサムウェア感染」が公式に認識される。 単なる医療システム障害ではなく災害という認識。 

Check!

なぜ復活したのかは不明だが、システムが一時的に不調になることはそれほど珍しいことではなく、正常性バイアス（災害や事故などの危機的状況に直面した際、「大したことはない」「自分は大丈夫」と都合の悪い情報を過小評価し、正常の範囲内だと思い込む心理メカニズム）も働き、結果として初動開始が遅れてしまうことも珍しくはない。

Check!

この時点でランサム攻撃の被害に遭った確率はかなり高いが、通勤電車という情報共有に不自由する環境でどのように認識を共有できたのか。

Check!

最初に異変を察知してから3時間後に、組織的に被害に遭ったという認識に至った。24時間医療体制を敷く組織としてそれは遅かったのかどうか。潜伏している時点で察知できなかったのはなぜか。初動開始を早めるためにはどんな施策が必要・可能なのか。

V o i c e

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。

Voice 1

住民の情報を守るためには、欠かせないCYDER受講

北海道宗谷郡猿払村役場
西岡 淳 様

インシデントは起きないにこしたことはないですが、いざ発生した時に具体的に何をすればよいのかを演習で学べるところがCYDERのメリットだと感じています。セキュリティベンダーさん等でも似たような研修をやっているのをよく見かけますが、実機・実環境でここまで踏み込んだ内容の研修というのはなかなか見ないと思います。

Voice 2

インシデント検知後、短時間で原因究明に成功

愛知県豊田市役所
桑名 亮佑 様

CYDER受講後に、愛知県の情報セキュリティクラウドでインシデントを検知されたことがありましたが、30分以内に原因を見つけることができました。CYDERの受講時にフォレンジックの手順を学んだので、市のネットワーク、機器構成ではどこから調査すれば良いかを事前に考えることができました。また、CYDERを通して限られた時間の中で課題を解き進める経験ができたことが活かされたと思っています。

Voice 3

限られた情報の中から、優先度を決定する対応力が身に付きました

埼玉県庁
氷見 雄介 様

プレCYDERドリル編は、歯ごたえがありかなり良いと思いました。単元ごとにテストがあり正解しないと次に進めないところや、どんどん問題が複雑になっていきストーリーに引き込まれる感じがとても良かったです。一般的なインシデント対応研修ではその全体像を学ぶことが多いですが、プレCYDERドリル編ではトリアージに特化して深く学ぶことができました。インシデント発生時の一連のプロセスを、入力シートを用いた演習を通じて実践的に習得し、限られた情報の中から、重要度と緊急度を適切かつ迅速に判断し、優先度を決定する対応力が身についたと感じています。また、研修で提示されるシナリオが実際に県内で発生しうる具体的な事案であったため、学びがより一層有意義なものになりました。

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」2026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	想定対象者（例）	身につくスキル
Aコース （初級）	• **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** • 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	• 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）	• **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** • 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）	• **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** • 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 • 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」

※各コースの想定対象者例のいずれかに当てはまれば、そのコースのご受講に適しています。
●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		想定対象者（例）	身につくスキル
プレCYDER	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
	ドリル	• **CSIRT / 情報システム課で、インシデント対応をしている方** • Aコース受講の準備をしたい方 • Aコースの復習をしたい方	• 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。※各コースの想定対象者例のいずれかに当てはまれば、そのコースのご受講に適しています。

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	集合対面	初級	全ての組織	2〜5時間程度	1日間	全国47都道府県
	Bコース※1	集合対面	中級	全ての組織		1日間	東京・名古屋・大阪・福岡
	Cコース	集合対面	準上級	全ての組織		2日間	東京・大阪
プレCYDER	ケーススタディ	eラーニング	入門	全ての組織	なし	2〜3時間程度	オンライン
	ドリル	eラーニング	入門	全ての組織	なし	5時間程度	オンライン

[※1] B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。なお、地方公共団体の方にも取り組みやすいよう、三層の対策の考え方に基づくα′モデル等を参照しつつ演習内容を構成しています。ご所属の組織に関係なくご受講可能です。[※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。

受講費用

所属組織	対象コース	費用（税込み）	備考
国の機関・独立行政法人・指定法人	Aコース / Bコース / Cコース	無料※	AとCの組合せは後で申込したコースが有料
	プレCYDER	無料	他のコースとの組合せに関係なく無料
地方公共団体	Aコース	無料	—
	Bコース	1受講　19,250円 / 人	2026年度に料金改定
	Cコース	1受講　38,500円 / 人	2026年度に料金改定
	プレCYDER	無料	他のコースとの組合せに関係なく無料
民間企業	Aコース / Bコース	1受講　38,500円 / 人	2026年度に料金改定
	Cコース	1受講　77,000円 / 人	2026年度に料金改定
	プレCYDER	1受講　11,000円 / 人	—

※国の機関・独立行政法人・指定法人にご所属の方は、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。