National Cyber Training Center

ナショナルサイバートレーニングセンター

CYDERオンライン演習への挑戦

中川 哲也 (Tetsuya Nakagawa)

国立研究開発法人 情報通信研究機構

自己紹介

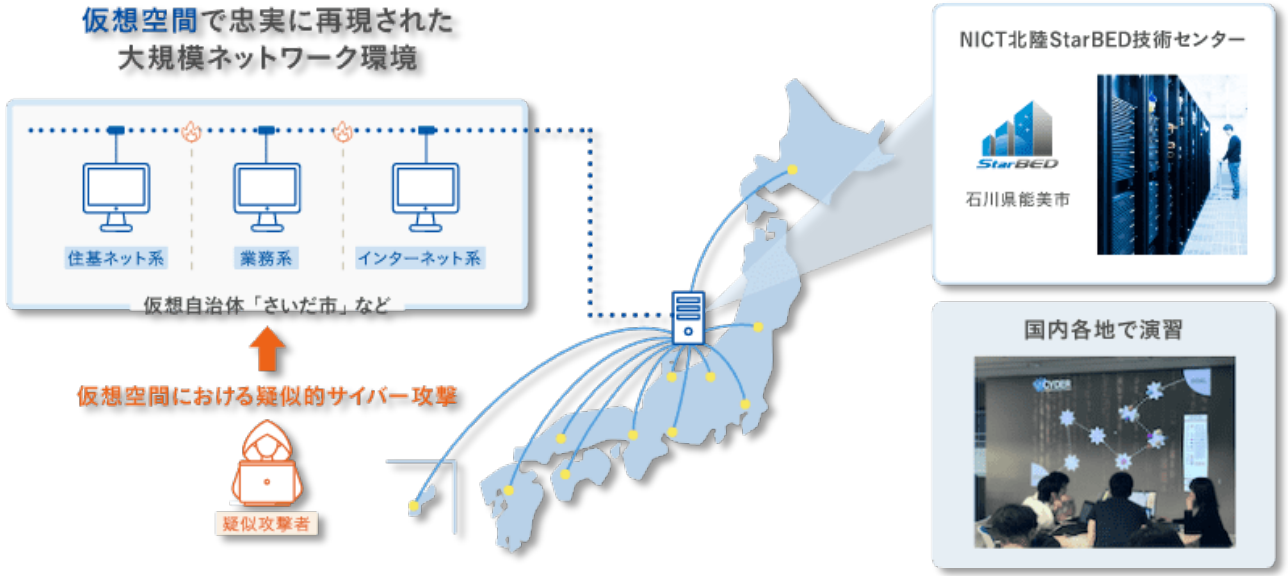
- 氏名: 中川　哲也(Tetsuya Nakagawa)
- 勤務先: 2018年10月-現在
  - NICTサイバーセキュリティ研究所
    ナショナルサイバートレーニングセンター(通称: ナショトレ)
  - 演習システム**CYDERANGE**の研究開発、**演習シナリオ**開発、演習企画・運営を担当
- （ナショトレ以外の）携わった仕事
  - 暗号モジュールなどの組込みシステムの研究開発やプロジェクトマネージメント業務
- 保有資格など:
  - 情報処理安全確保支援士、ネットワークスペシャリスト

CYDERとは

CYDERとは

CYDER(Cyber Defense Exercise with Recurrence)

- ✓**サイバー攻撃を受けてしまった時にどのように対応したらよいかを PCを操作しながらロールプレイ形式で体験できる演習。**
- ✓全国で年間100回以上開催、受講者数約4,000人の**国内最大規模のサイバーセキュリティ演習。**
- ✓主に官公庁、独立行政法人及び**地方公共団体**向け演習。



CYDERオンライン演習への挑戦

CYDERのオンライン演習化

●地理的・時間的要因でCYDERを受講できない方への対応として

–指定された演習日でなく、自分の**都合のよい日時**に受講したい

–わざわざ演習会場に行かずに、自分の**都合のよい場所**から受講したい

●2021年当時のコロナ禍の感染症拡大防止対策のために

–演習会場に行くための**外出は控えたい**

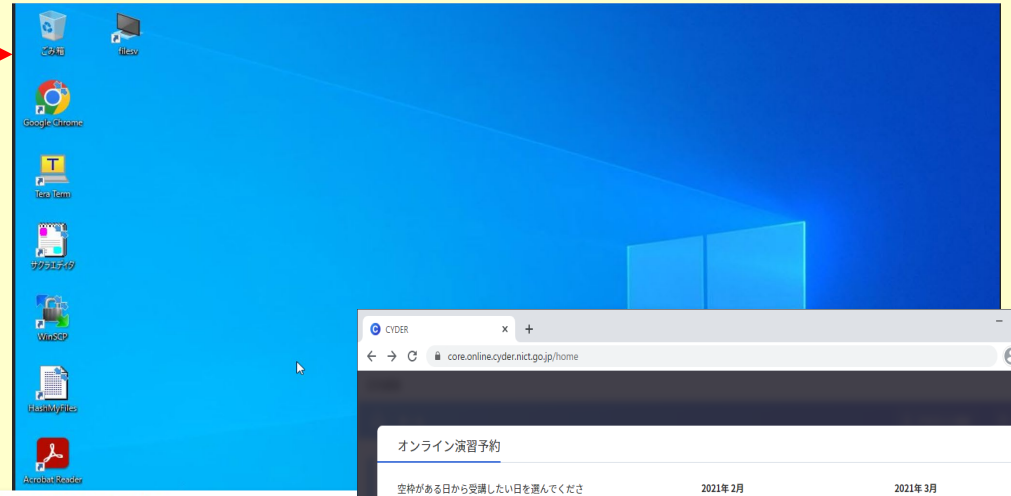
–演習会場での他の受講者や講師・チューターの**物理的な接触はさけたい**

→講師・チューターなし受講者だけのCYDERオンライン演習

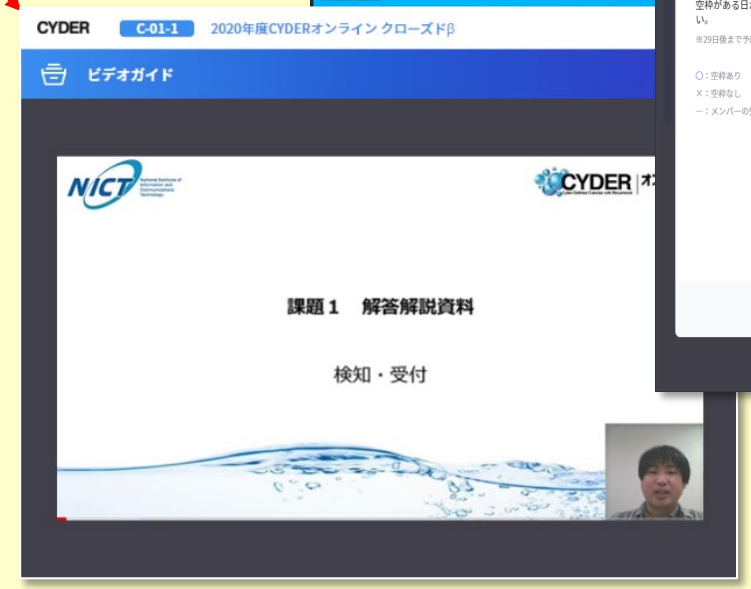
Webブラウザで予約から受講まで完結

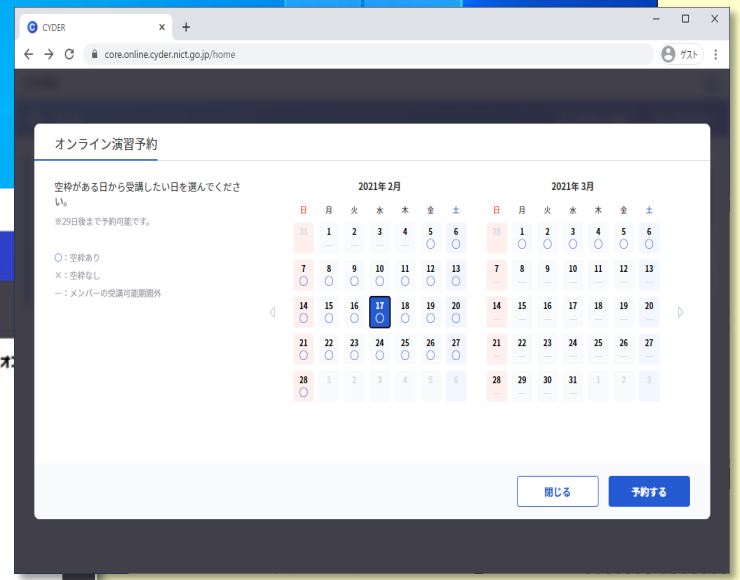
LMS（学習管理システム）

仮想演習環境



ビデオ配信



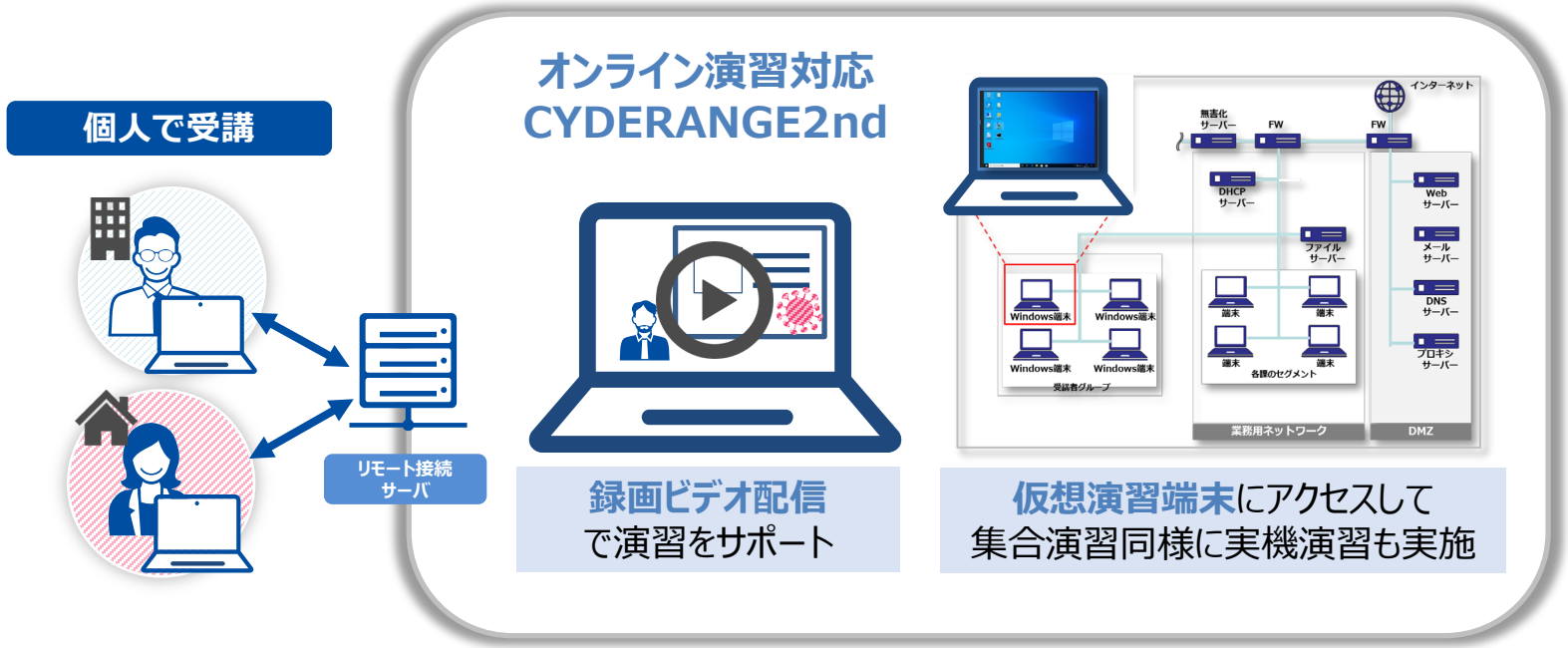


予約画面

オンライン演習対応
CYDERANGE2nd

最初の挑戦：オンラインAコース（正式サービス概要）

- 2021年度**Aコースシナリオ**を個人向けに再構成
  - 講師・チューターの役割のビデオ配信
  - 仮想演習端末を用いた実機演習
  - 記述式ディスカッション課題の自己採点、集合演習の回答例を紹介



コース名	オンラインA
受講対象組織	全組織共通
対象者	システムの運用担当者
開催地	リモート受講
実施時期	2021年11月～2022年2月
受講者数	641名

最初の挑戦：オンラインAコース（アンケート結果）

【ポジティブな感想】

- オンラインでは**自分のペース**で学ぶことができよかった。少なくとも基本的なことをじっくり学ぶべきAコースに関しては，オンラインの方が**集合演習より学習効果が高い**と思う。

- **仮想環境の提供**などすばらしい研修でした。**自分のペース**でできますし、通信内容の把握などさらに実践的なハンズオンも可能ではないかと思います。

- **個人向け演習に再構成した結果、一定の評価をいただいたが。。。**

最初の挑戦：オンラインAコース（アンケート結果）

【ネガティブな感想】

- 情報システムに携わっている人にとってはわかりやすいと思うが、他の部署から人事異動できた初心者にとっては**言葉からわからない**。

- **直ぐに質問できない**。不明な点などその場で解決できないので，向学意欲が低下しかねない。

- デメリットとしては、やはり**グループで討議ができない**ことです。また、**チーム内で分担**するようなよりリアルに近い対応ができないこともデメリットと考えます。

→**まだまだ難しいとの苦言や、オンラインでもチューターサポートやグループ課題が必要とのご意見もあり！**

新たなる挑戦（要件の見直し）

●根本的な目標は何か？

–誰も取り残さないサイバーセキュリティ人材育成

–CYDER**未受講の地方自治体の数をゼロ**にする

●主な受講対象者は誰か？

–**地理的な理由**や兼務による**時間的な制約**でCYDERを受講できていない国の機関や**地方自治体の方**

●CYDER演習の本質とは何か？

✓サイバー攻撃を受けてしまった時にどのように対応したらよいかをPCを操作しながら**ロールプレイ形式で体験できる**演習

–ただし、CYDERを受ける準備のための**最低限の知識を得る演習**も必要

新たなる挑戦その１

- 受講対象者：CSIRT／情報システム課に配属されたばかりで**基本的なIT知識をお持ちでない方**やいろいろな業務を兼務されて**時間のとれない方**

- 演習要件：受講時間が**3時間程度**で**分割受講**が可能でインシデント対応に**最低限必要なこと**を学べる、かつ、**向学心をそそる**オンライン演習

→プレCYDER

2. プレCYDERとは

プレCYDERとは

- 受講時間が**3時間程度**で**分割受講**が可能
  - –約15分単位の分割受講可能で合計2～3時間
  - –動画視聴とクイズ形式の課題を組み合わせたコンテンツ

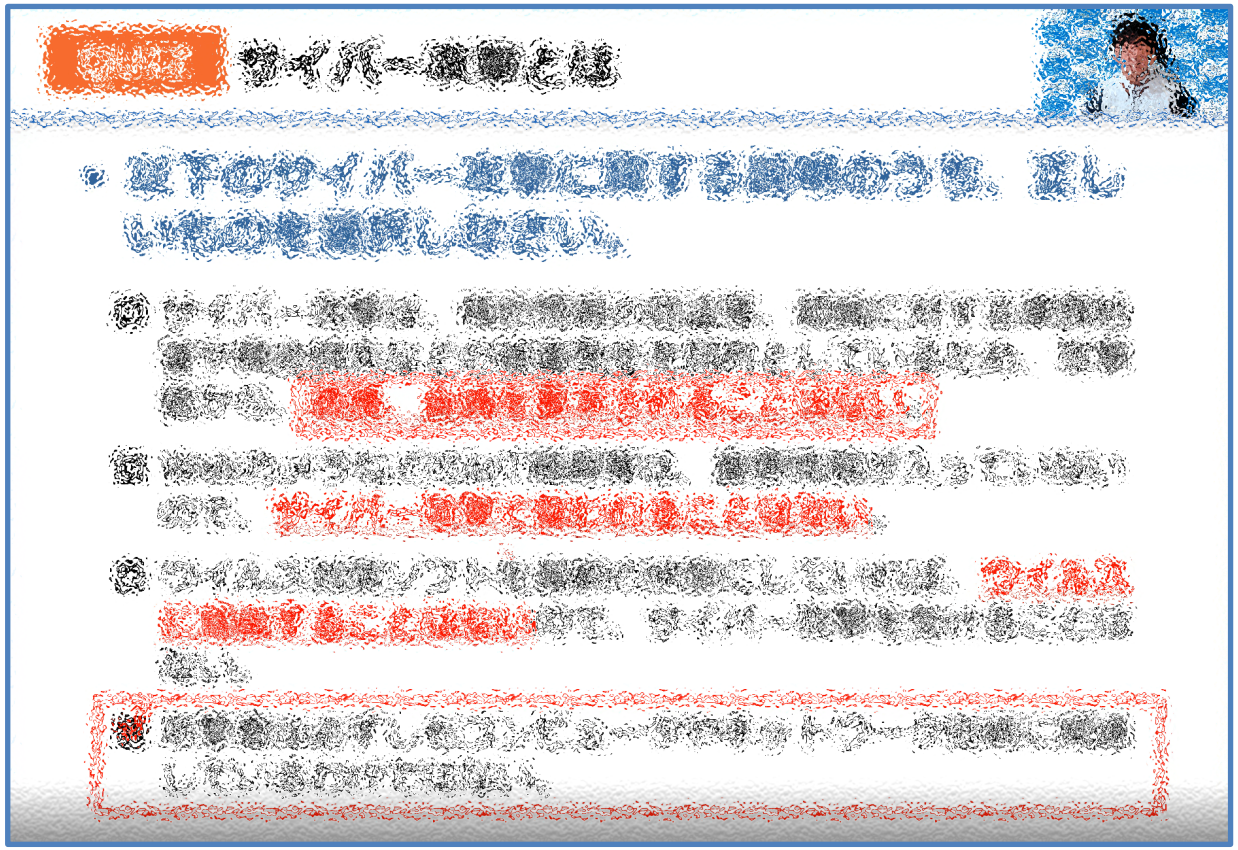
目次

CYDER Cyber Defense Exercise with Recurrence

内容		時間
第1部　オリエンテーション	本コースについて	5分
第2部　講義	サイバー攻撃について ×3本※	40分
	インシデントレスポンスについて ×5本※	65分
第3部　後続コースのご案内	CYDERの紹介 ×1本※	15分
第4部　本コースを通して	確認テスト	10分
	アンケート	15分
合計時間		150分

※ 動画説明あり。動画は複数本に分かれていますので、分割受講可能です。

Page 6



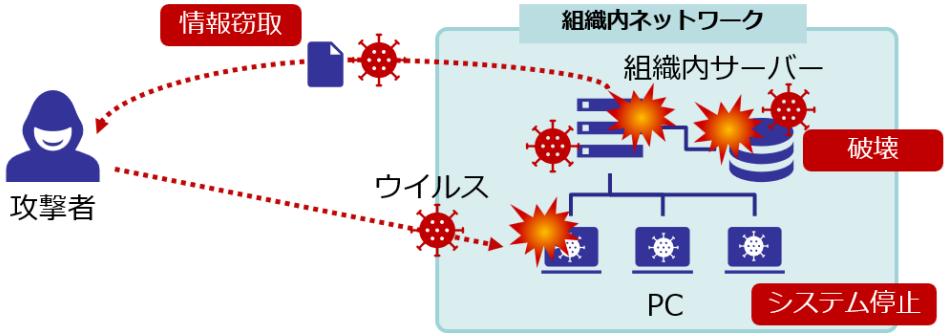
新たなる挑戦：プレCYDERとは

- インシデント対応に**最低限必要なこと**を学べる
  - –サイバー攻撃の仕組みとトレンド
  - –インシデントハンドリング概要

サイバー攻撃とは

CYDER Cyber Defense Exercise with Recurrence

- ネットワークやシステム、PCに対して行われる不正な活動のこと
- システムの停止、データの破壊、情報の窃取などが行われる



Page 20

インシデントマネジメント（2/2）

CYDER Cyber Defense Exercise with Recurrence

	ステップ	内容	事例の場合
準備	インシデント発生前	• インシデント対応手順・体制の整備、訓練 • 脆弱性対応	・セキュリティに対する知識や経験の不足 ・インシデント対応の準備が不十分だった。 ・脆弱性が放置されていた
インシデントハンドリング	検知・連絡受付	• インシデントが発生した旨の連絡を受領 • 関係各所に報告	・異常事態が明確にわかりやすかった。 ・システム担当者、幹部、関係各所に迅速に報告されていた。
	トリアージ	• 事実関係や状況を確認 • インシデントか否かの判断 • 対応の優先順位付け	・基本方針は明確に打ち出していた ・知識や経験不足から、初動対応に戸惑いや遅れが生じている
	インシデントレスポンス	• 対応方針の検討 • 被害の原因を取り除き元の状態に復旧	・基本方針を明確に打ち出していた ・ベンダーとの協力体制に不備があり、対応が遅れてしまった。
	報告公表	• 被害状況や影響範囲に応じて組織内外に対して報告・公表	・被害発生直後に記者会見を開いたことが奏功。多方面からの協力を得られた。
	事後対応	• 報告書の取りまとめ • 振り返りの実施	・調査報告書を作成し、自組織だけでなく、他の病院や事業所のセキュリティ強化に貢献

Page 49

プレCYDERとは

●向学心をそそるオンライン演習

– 実際に起こった最新事例のケーススタディ課題

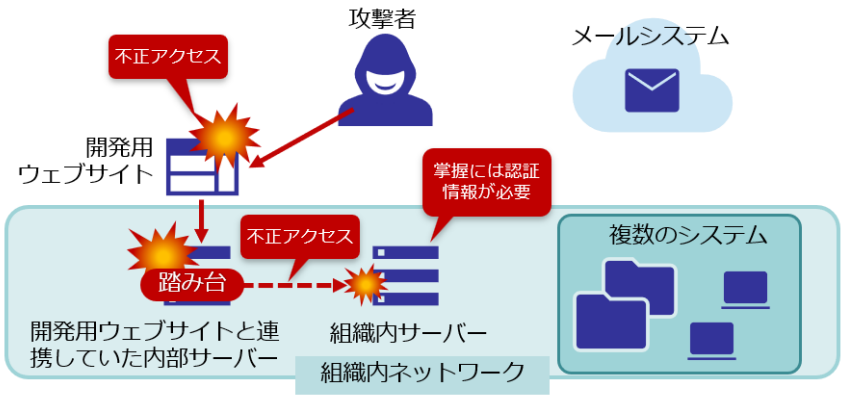
– 事例のインシデント報告書をやさしく説明

不正アクセスの手口２

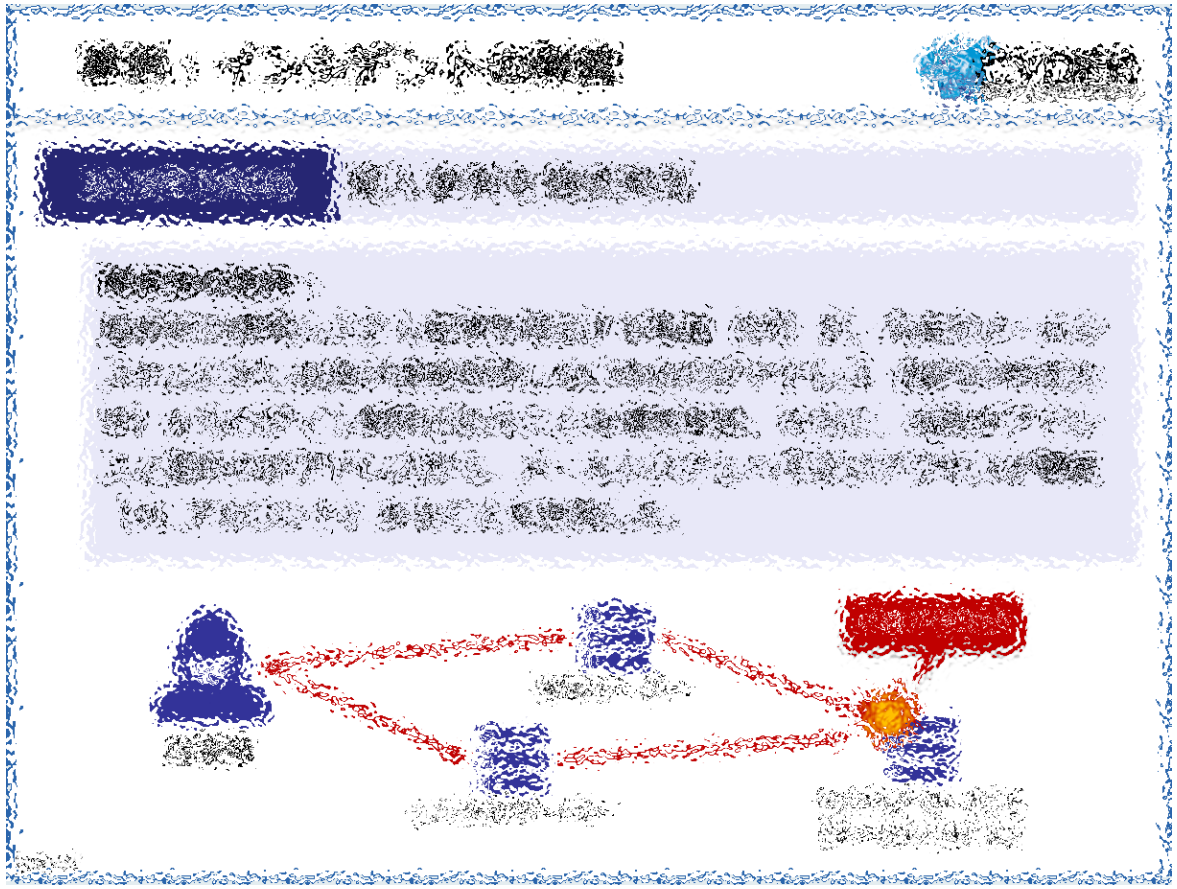
CYDER Cyber Defense Exercise with Recurrence

12月15日～　内部サーバーへの不正なアクセス１

- ✓ **内部に侵入し、更に別の組織内サーバーを攻撃**
- ✓ 組織内サーバーを掌握するためには、サーバーの認証情報が必要



Page 46



プレCYDER（実施結果）

- 初年度の2023年は実施期間2か月程度で**1000人を超える受講者数を達成！**
- 受講者アンケート結果も**好評！**
  - **今年度よりセキュリティ関係の担当となり**右も左もわからない状況であったが、今回の研修を受講し、攻撃の種類や対応の流れを学ぶことができ、**とても有意義な研修**だと感じた。
  - CYDERの重要性を理解。また、CSIRTの教育の強化の必要性も認識した。**平時におけるベンダーとの連携**及び契約当初における**運用保守契約内容の熟知**が組織全体として必要であることが理解できた。

- 2024年度以降も取り上げる事例を変えて**継続実施中**。

新たなる挑戦その２

●受講対象者：基本的なIT知識はお持ちだが、**地理的・時間的要因**が理由でCYDERの受講機会を逃している方

●演習要件：グループディスカッションやチューターサポートがあり、**集合演習と同等の演習効果のある**オンライン演習

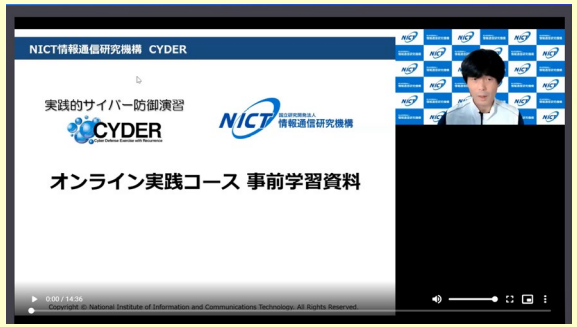
→オンライン実践コース

2. CYDERオンライン実践コースとは

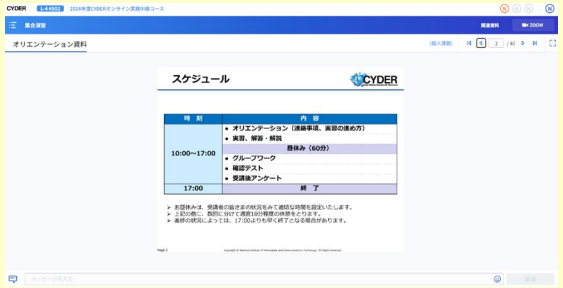
オンライン実践コース（概要）

CYDERANGE2nd

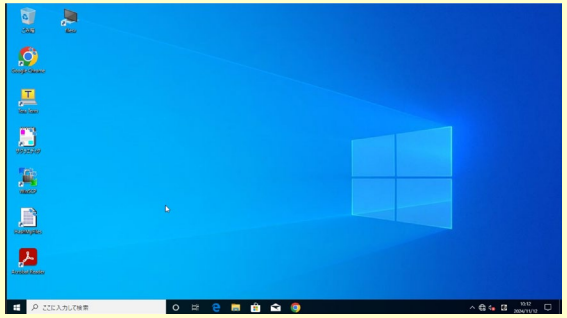
演習日前に講義ビデオを視聴（反転学習）



LMS（学習管理システム）



仮想演習環境



ブラウザでアクセス
LMSで承認、採点などを実施

ブラウザアクセス

Zoom配信

グループA

自治体A職員 自治体A職員 自治体A職員 自治体A職員

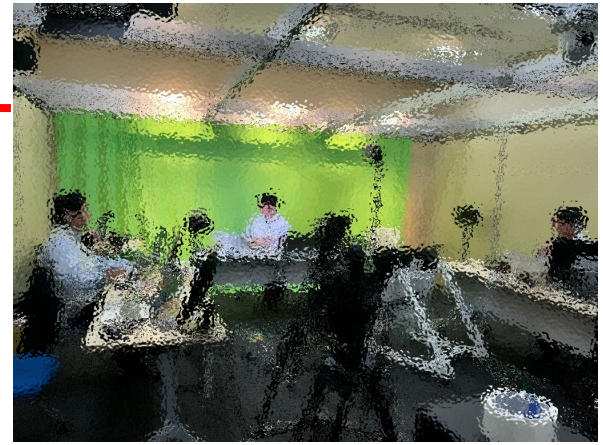
グループB

自治体E職員 自治体E職員 自治体F職員 自治体F職員

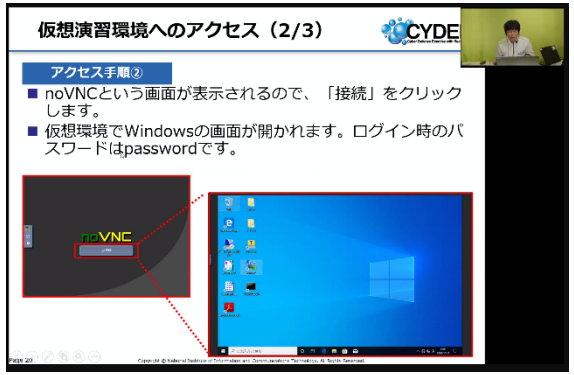
グループC

自治体I職員 自治体J職員 自治体K職員 自治体L職員

日本橋配信室



講師によるリアルタイム講義



ブレイクアウトルームでチューターがサポート

グループ課題をブレイクアウトルームでサポート

グループA

自治体A職員 自治体A職員 自治体A職員 自治体A職員

グループB

自治体E職員 自治体E職員 自治体F職員 自治体F職員

グループC

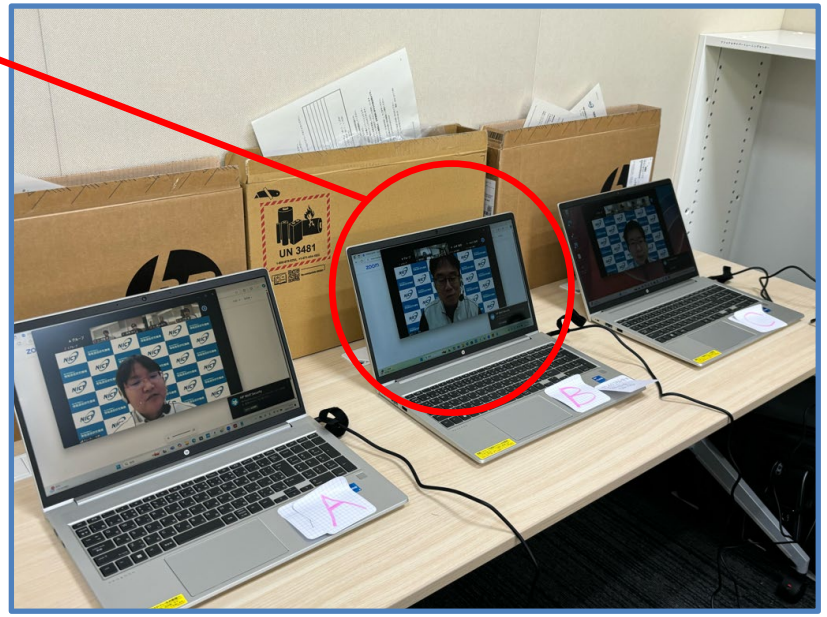
自治体I職員 自治体J職員 自治体K職員 自治体L職員

Zoom接続

同じ
ブレイクアウトルーム
に参加

チューターがサポート

講師・チューター全員でグループを監視



オンライン実践コース（実施結果）

●以下の工夫で集合演習と同等の効果を達成できる見込みがついた。

–講義部分を**ビデオガイド付き事前学習**として当日の演習から分離。

–**解き方が一本道**になるように演習の**課題の量と粒度**を調整。

●受講者アンケート結果もポジティブなものが増加！

–本研修は数年に１回くらいの頻度で**定期的に受講したい内容**であるため，次年度以降も受講を希望する。

–オンライン実践コースは**非常に有用**でした。今後も継続して事業化されることを期待します。

しかし。。。

オンライン実践コース（新たに見つかった課題）

【受講環境】

- 仮想演習環境アクセスを**自治体セキュリティクラウド**がブロック。
- ノートPC1台だと**画面が足りない**。
  - （**3画面必要**：講師Zoom画面、仮想演習環境画面、LMS画面）

【演習内容】

- 集合演習より**内容や分量が物足りない**。
- 報告書の文量が多く、読み込むのに時間がかかったため、メンバー同士で**ディスカッションする時間があまり取れなかった。**

- **さらなる改善が必要！**

CYDERオンライン演習への挑戦は
まだ続いています！