DNP

販売元 ： 大日本印刷株式会社　ABセンター DX事業開発本部
サイバーセキュリティ事業推進ユニット 営業部
TEL 050-3753-5900

運　営 ： 株式会社サイバーナレッジアカデミー

※株式会社サイバーナレッジアカデミーは大日本印刷株式会社（DNP）のグループ会社です

担当 ：

2021.10

DNP

世界有数のサイバーセキュリティ技術を持つ
イスラエル IAI社※の訓練システム「TAME Range」を活用

サイバー・インシデントレスポンス・マネジメントコース

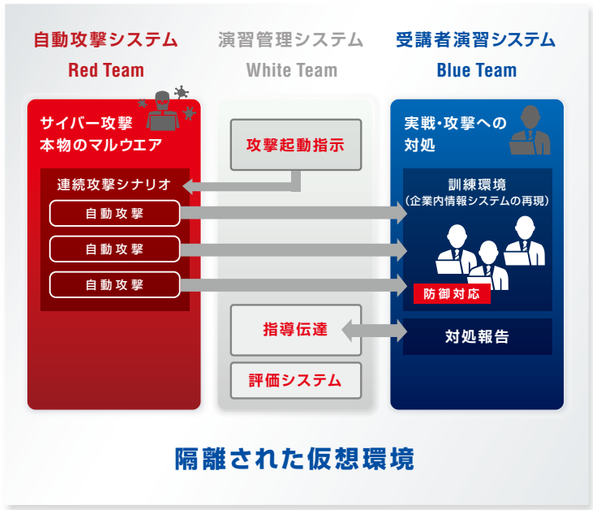
CYBER KNOWLEDGE ACADEMY サイバーナレッジアカデミー

※ IAI　イスラエル・エアロスペース・インダストリーズ

サイバー・インシデントレスポンス・マネジメントコースは、
日々進化するサイバー攻撃への対応を体験型実践演習（ハンズオン）で学習することで、
未知の攻撃にも対応できる**スキルを修得**することができる**トレーニングサービス**です。
受講者は**チーム形式**で、インシデント対応についての基礎的な知識・対処方法から
応用実践までを学習します。本トレーニングを受講することで、複雑化・高度化する
サイバー攻撃に対し、チームで対応することの有用性を認識し、**チーム力の醸成**と
向上を体感することができます。個人のスキルアップはもちろんのこと、
チームリーダーも養成するカリキュラムをご提供いたします。

サイバー・インシデントレスポンス・マネジメントコースの特長

本物のサイバー攻撃を再現した「体験重視のアカデミー」



体験重視の実践演習
・座学中心の講習とは異なり、全体の７割におよぶ実践演習を実施

チーム力とチームリーダーの養成
・リーダーと複数メンバーで構成されるチーム形式での演習
・個人のスキルアップに加え、チーム力とリーダーシップを醸成

攻撃シナリオを用いて隔離された仮想環境上で演習を実施
・実際に発生しているサイバー攻撃事案をリアルに再現した攻撃シナリオを、訓練環境で繰り返し体験し、インシデント対応の考え方を身につけることが可能
・チームメンバー間で連携しながら防御能力の向上を図る
・典型的な企業内情報システムを再現した訓練環境には業務サーバー群、従業員ワークステーション群に加えて、IPS/IDS,SIEM,エンドポイント・セキュリティツールなどを配備済み

受講者の理解度と対処状況を評価・採点
・受講者の演習結果から、課題を抽出して解決を図る

世界有数のセキュリティ技術を持つ イスラエルIAI※社の訓練システムを導入

本トレーニングでは、イスラエルIAI社※製品「TAME Range」を導入しています。TAME Rangeは現実の脅威に対抗できるレベルまで能力向上が見込める訓練システムです。

TAME Rangeの特長:
- 多様なサイバー攻撃に対応可能なサイバーセキュリティチームの組織力、リーダー指揮能力の向上
- 標的型攻撃などの実例に基づく攻撃シナリオによるリアルな防御トレーニングを実施
- 隔離された仮想環境上で繰り返し訓練可能
- 受講者の理解度、対処状況、チームの訓練達成状況を客観的に評価する進捗管理システム
- GUI操作で攻撃パターンを変更可能（既存攻撃パターンによる構成）

※ IAI：イスラエル・エアロスペース・インダストリーズ（イスラエル政府100％出資の主力航空機メーカー）

受講の効果

- チームでの対応を行うことで、担当毎の役割（F/W担当、エンドポイント担当、ログ監視担当等）、業務内容を理解し、自社内で応用することができる。
- FireWallやIPS/IDSのルール設定、SIEMの相関分析ルール設定について、実際のサイバー攻撃に対処するための適切な設定方法を習得できる。
- **ISACA CPE（継続教育）申請可能**
  ISACA（情報システムコントロール協会）CPE ポリシーに基づき受講時間をCPEとして申請することができます（50分＝1CPE 換算）。
- サイバー攻撃を受けた際の対応プロセス（調査、分析、対処、報告）の流れを理解し、必要なツールの使い方を習得できる。

基礎演習 5日間コース内容

区分	講義・演習名	講義・演習概要とねらい
講 義	サイバーセキュリティ概論	サイバーセキュリティの動向と最近の事故事例について説明します。
講 義	演習環境について	演習環境上の仮想企業ネットワーク（DMZ・社内）について説明します。
演 習	防御ツールについて	防御ツールについて解説後、実際に攻撃を防御する演習を行います。 ①統合ログ管理システム（SIEM）　②ファイアーウォール・侵入防御システム（IPS） ③統合エンドポイントセキュリティ　④ディレクトリサービス、集中稼動管理システム
演 習	調査・分析について	実際に攻撃を調査・分析する演習を行います。 ①Web・FTPサーバログ／イベントログ　②マイクロソフト社などの提供する調査・分析ツール ③ネットワークパケットキャプチャー・調査・分析ツール
演 習	サイバー防御演習（社内攻撃1）	演習環境上の社内ネットワークへの攻撃に対して、チームで防御する演習を行います。
演 習	サイバー防御演習（DMZ攻撃）	演習環境上のDMZへの攻撃に対して、まず講師が防御の実演を行います。 その後、受講生がチームで防御する演習を行います。（※演習の進み具合により、説明のみの場合もあります。）
演 習	サイバー防御演習（社内攻撃2）	演習環境上のDMZ及び社内ネットワークへの攻撃に対して、チームで防御する演習を行います。
演 習	サイバー防御演習（社内攻撃3）	演習環境上の社内ネットワークへの攻撃に対して、チームで防御する演習を行います。

推奨受講対象　以下の基礎知識を有する方の受講を推奨します。
・Windowsサーバ・クライアントの基礎知識　・ネットワークの基礎知識　・マルウェア対策の基礎知識

株式会社サイバーナレッジアカデミー
CYBER KNOWLEDGE ACADEMY
〒141-8001
東京都品川区西五反田3-5-20
DNP五反田ビル3F
https://www.dnp.co.jp/cka/