

NEWS RELEASE

報道関係各位

2025年7月31日

【変化する脅威に備える】 Web改ざん、マルウェア、シャドーITに備える新コースを開講 ～ 自己学習型インシデント対応訓練3コースをNet.Campusで提供開始～

アライドテレシス株式会社（本社：東京都品川区、代表取締役社長：サチエ オオシマ）は、教育・研修サービス「Net.Campus」から、自己学習形式のインシデント対応訓練コース3種を新たに開講し、提供を開始したことをお知らせします。

本コースは、当社独自のクラウド型訓練基盤「NetQuest Platform」を活用し、時間や場所にとらわれない柔軟な環境で実践的なインシデント対応訓練を提供し、組織の対応力強化を支援します。

Web改ざん・マルウェア・シャドーITに備える

自己学習型インシデント対応訓練から 3つの新コースが登場！




■ 増えるWeb改ざん、マルウェア、シャドーITに対応する実践力を育成

近年、サイバー攻撃は手口を巧妙かつ多様に変化させながら、業種や規模を問わず企業や組織に被害をもたらしています。中でも以下のようなケースでは、初動対応や連携体制によって被害の拡大に大きな差が生じます。

たとえば、Webサイトの改ざんによる情報の書き換えや悪質なスクリプトの埋め込みは、信用失墜や二次被害を招くリスクがあります。端末のマルウェア感染は標的型攻撃などを通じて水面下で進行し、感染拡大や情報漏えいといった深刻な影響につながります。さらに、IT管理外の端末やクラウドサービス（シャドーIT）を経由した社内感染も、テレワークの普及に伴い実際に報告されるケースが増えています。

もはや特定のシステム部門だけで対応できる時代ではなく、関係部門を含めた連携と判断力の底上げが求められています。一方で、現場の多忙さや人員不足から、計画的な訓練を継続することが難しいという声も少なくありません。

こうした背景を踏まえ、アライドテレシスでは、Webサイト改ざん編、端末マルウェア感染編、シャドーITからの感染編という、現場で実際に起こり得るインシデントをテーマにした3つの自己学習型訓練コースを新たに開発。いつでも・どこでも学習できるクラウド型環境で、実践的な対応力の向上を支援します。

■ 新コースについて

今回新たに開講する3つのコースは、既存の訓練プログラムを基盤に設計された“自己学習型”の新コースです。実際のインシデントを想定したシナリオに沿って、初動対応や関係者との連携、情報共有などの判断プロセスを体系的に学ぶことで、現場で役立つ実践力の向上を支援します。

コース名	期間	内容	標準価格 (税込) / 1名
【自己学習型】 Webサイト改ざん編	3時間	WEBサイト改ざん攻撃におけるインシデント発生時の連携・対応に関する自己学習形式訓練です。本演習では病院のホームページが攻撃の標的になったケースを演習シナリオとします。ビジネスプロセスを意識し、インシデント対応の基本スキルを習得可能です。	44,000円

【自己学習型】 端末マルウェア感染編	3 時間	標的型攻撃からマルウェア感染のインシデント発生時の連携・対応に関する自己学習形式訓練です。マルウェアの影響を小さくするための初動対応や、復旧の為のアクションにどのような外部機関との連携が必要なのかといった点を習得します。	44,000 円
【自己学習型】 シャドーITからの感染編	3 時間	テレワーク作業者がシャドーITにてマルウェア感染し、社内感染が広がるまでにどのようなアクションが適切で、被害を最小限に食い止めるか、自己学習形式訓練を通して習得します。訓練で身につけた内容を社内にて展開することで、急増するテレワーカーのITリテラシーの向上に役立てることができます。	44,000 円

※その他のインシデント対応教育・訓練コースはこちらからご確認ください。<https://www.allied-telesis.co.jp/training/#tc299>

■ 自己学習型コースの特長：受講者が自由に学べる

本コースは、アライドテレシスが独自に開発したクラウド型インシデントレスポンス訓練基盤「NetQuest Platform」を活用しています。ファシリテーターによる進行を必要とせず、PC とインターネット環境さえあれば、時間や場所を問わずに受講可能。多忙な業務の合間でも、自分のペースで無理なく取り組める“自由度の高い”訓練環境を提供します。

- ・時間や場所に縛られず受講可能
出張先や在宅勤務中でもアクセスでき、業務のスキマ時間を活用してスキルアップが可能です。
- ・1 テーマ約 3 時間・分割受講も可能
1 テーマあたりの学習時間はおおよそ 3 時間。途中保存・再開ができるため、空き時間を活用しながら段階的に学習できます。
- ・シナリオベースの実践形式
座学ではなく、インシデント発生時の流れに沿って判断・対応を進めていく実践型の構成です。自ら考え、選択するプロセスを通じて理解と定着を促します。
- ・最新の攻撃トレンドを反映
実際のインシデント事例や最新の脅威情報に基づくシナリオを採用。現場に即した実践力を養えます。

■ NetQuest Platform について

「NetQuest Platform」は、アライドテレシスが独自開発したクラウド型インシデントレスポンス訓練基盤です。事前の準備や調整にかかる時間やコストを抑えつつ、企業の実環境に即した組織全体の訓練を可能にします。

CISO や CSIRT の育成に加え、インシデント対応が求められる複数の部門に同一のシナリオを共有することで、組織全体が同時に訓練を受けることができます。さらに、インシデント対応の一連の流れを実践的に体験できるため、国家サイバー統括室（NCO）をはじめ、多くの企業に採用されています。

● NetQuest Platform の詳しい情報はこちらからご確認ください。

<https://www.allied-telesis.co.jp/security/training/>

アライドテレシスでは、ネットワークインフラの提供にとどまらず、セキュリティを含めた IT 運用の全体最適を支援する取り組みを進めています。現場の知識定着と初動力の向上を目的としたトレーニングサービスの拡充にも注力しており、今後も多様なユースケースに対応した学習コンテンツを順次提供してまいります。

※) 記載されている商品またはサービスの名称等はアライドテレシスホールディングス株式会社、アライドテレシス株式会社およびグループ各社、ならびに第三者や各社の商標または登録商標です。

<<製品に関するお問い合わせ>>
E-Mail: info@allied-telesis.co.jp
<https://www.allied-telesis.co.jp>

<<ニュースリリースに対するお問い合わせ>>
マーケティングコミュニケーション部
Tel: 03-5437-6042 E-Mail: pr_mktg@allied-telesis.co.jp

アライドテレシス株式会社 東京都品川区西五反田 7-21-11 第 2 TOC ビル