

参加費無料

# セキュリティの インシデント対応を 体験しませんか？



In 東海

会場開催！

中小企業・団体の経営層や責任者の方へ

## サイバーインシデント演習

日程 令和 3 年 11 月 11 日 (木)

※受付開始 13:30 ~

14:00 ~ 17:00



参加

会場参加：TKP名古屋駅前カンファレンスセンター 8F  
(名古屋市中村区名駅2-41-5 CK20名駅前ビル)

(※お申込み後に事務局より参加方法等をご案内いたします。)

定員

50名 ※定員になり次第、受付を終了

■対象者：中小企業、団体等の経営層、セキュリティ責任者及び情報システム運用担当者の方

近年、世界的にサイバー攻撃を起因としたセキュリティインシデントが増加しており、攻撃の手法も高度化・巧妙化しております。また攻撃対象も大企業に留まらず、中小企業に対するサイバー攻撃も増加しております。万が一、サイバー攻撃を受けた場合には、迅速な対応により被害拡大を抑止することが極めて重要であり、迅速な対応を行うためには、全社的な体制構築、対応手順の準備等、日頃のインシデントへの備えが不可欠となります。

本演習では「事業経営の観点からみるサイバーセキュリティリスクの特定と対応戦略」に関する講義並びに擬似的なインシデント対応を体験いただく「サイバーインシデント演習」を開催いたします。

講義パートでインシデント対応の基本的なプロセスについて理解いただいた後に、演習パートで疑似的にインシデント対応を体験いただくことで、効果的にインシデント対応に関するノウハウを学習することが可能となります。是非ともご参加を検討ください！

プログラム、参加申込方法は裏面へ

# プログラム

## > 第1部 サイバーセキュリティ講義 [14:10~14:40]

### ■ 「事業経営の観点からみるサイバーセキュリティリスクの特定と対応戦略」

- ・最近のサイバー攻撃の情勢などをご紹介しつつ、被害拡大を最小限にとどめるためのインシデント対応の基礎に関する講義をいたします。

## > 第2部 サイバーセキュリティ演習 [14:40~17:00]

### ■ 「セキュリティインシデント発生時の効果的な対応について」

- ・第1部の内容を踏まえて、疑似的なインシデント対応を体験していただきます。
- ・チームに分かれて、疑似的に発生するインシデントについて議論していただきます。その後、各チームの代表者による発表及び講師による簡単な講評・解説を予定しております。



事態発生

対応検討

対応評価



※会場参加者は、新型コロナウイルス対策を行った上で机上演習の要素を取り入れたグループワークを予定

☆講師： 東京工業大学サイバーセキュリティ経営戦略コース 講師  
株式会社NTTデータ経営研究所  
パートナー 大野 博堂 氏

### 【※会場参加でお申込みの方へ】

開催にあたりましては、新型コロナウイルスの感染予防対策（会場入り口での検温及びアルコール消毒の設置）を十分に取りますが、次のことにつきましてご協力をいただきますようよろしくお願いいたします。なお、新型コロナウイルス感染状況により「オンライン」のみの開催となる場合がございます。

- ・発熱や咳等の風邪症状など体調不良がみられる場合は、参加をお控えください。
- ・手洗いや咳エチケットの徹底をお願いします。また、会場入り口のアルコール消毒をご活用いただくとともに、マスクの着用をお願いします。

### 「サイバーインシデント演習」参加申込

- 参加ご希望の方は、以下URLから参加申込をお願いします。なお、参加費は無料です。

申込期限：11月4日(木)17時

参加申込用URL：[https://soutsu-cyber.com/f/4515/application\\_tokai](https://soutsu-cyber.com/f/4515/application_tokai)

アクセス時にパスコードの入力が必要です。

パスコードは「soutsu\_cyber5986」を入力してください。



※本イベントの申込受付及びご案内等は、請負事業者である株式会社NTTデータ経営研究所が行います。  
お申込みの際にお知らせいただいた氏名等の個人情報は、当該演習への参加集約にのみ使用し、演習終了後廃棄します。

【本件お問い合わせ】総務省東海総合通信局 電気通信事業課

TEL：052-971-9114 / e-mail：tokai-jigyo-jigyo@soumu.go.jp