報道資料

くらしの中に
総務省
MIC Ministry of Internal Affairs and Communications

令和５年１月13日
近畿総合通信局

「サイバーインシデント演習 in 大阪」を開催

－サイバーセキュリティの「インシデント対応」を体験しませんか？－

関西サイバーセキュリティ・ネットワーク事務局※は、中小企業や団体等の経営層、セキュリティ責任者及び情報システム運用担当者の方等を対象に、講演や擬似的なインシデント対応を通じて組織内の基本方針やルールなどを考えていただくことを目的として、令和５年２月21日(火)に「サイバーインシデント演習 in 大阪」を開催します。

※関西サイバーセキュリティ・ネットワーク事務局：
近畿総合通信局、近畿経済産業局、一般財団法人関西情報センター

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は増加しており、攻撃対象も大企業に留まらず、中小企業が攻撃の標的となる事案も目立っていることから、サイバー攻撃への備えとして、社内でセキュリティへの危機意識を共有し、インシデント発生時の対応手順や体制を整えることが重要となっています。

本演習では、組織内の基本方針やルールなどを考えていただく機会となるよう、サイバー攻撃の事例及び対応策に関する講義並びに疑似的なインシデント対応を体験していただきます。

１　日時　令和５年２月21日(火) 14時から17時まで

２　会場　グランフロント大阪　タワーB　カンファレンスルーム B07
（大阪市北区大深町3-1）

３　主催　関西サイバーセキュリティ・ネットワーク事務局

４　プログラム概要

第１部　講演「サイバー攻撃の情勢及び対応策について」

第２部　演習「セキュリティ事件・事故発生時の効果的な対応について」

講師：株式会社川口設計　代表取締役　川口　洋　氏

５　対象者

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

６　定　員　40名（先着順）

７　参加費　無料

８　申込方法等

次の申込フォームからお申し込みください。

・申込フォーム：https://www.kiis.or.jp/form/?id=83
（詳しくは別添「サイバーインシデント演習 in 大阪」チラシをご覧ください。）

・申込期限：令和５年２月15日（水）まで

※参加申込時に取得した個人情報は、本講演への参加申込の受付及び今後の関西サイバーセキュリティ・ネットワークの事業運営に関し必要な場合にのみ使用し、第三者に開示・提供・預託は行いません。
※申込受付業務や受付後のご案内は、請負事業者の一般財団法人関西情報センター（KIIS）が行います。
※新型コロナウイルス感染症の感染状況によりオンラインのみになる可能性があります。

（連絡先）
近畿総合通信局 情報通信部 情報通信連携推進課
／サイバーセキュリティ室
担当：高橋、今宮
電話：０６－６９４２－８６２３

セキュリティのインシデント対応を体験しませんか？

参加費無料

中小企業・経営者やセキュリティ責任者等の方へ

サイバーインシデント演習 in大阪

日 時 令和5年2月21日（火）

※受付開始13:30～

14:00～17:00

病院や教育機関などでもサイバー攻撃が増えてます！

会 場 グランフロント大阪 タワーB カンファレンスルームB07

大阪府大阪市北区大深町3-1

定 員 40名 ※定員になり次第、受付を終了いたします

■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等

中小企業は、サプライチェーンの最前線を担い、多くの取引先や関連企業と日々やり取りを行っていますが、サイバー攻撃を受けた場合に備えて、社内で意識を持ち、体制を構築した上で、セキュリティインシデント発生時の対応方法や手順などを共有しておくことが重要となっています。また、DXの取組等を進める上で、様々なセキュリティインシデントへの対応を求められる機会が飛躍的に増えています。

そこで、最近のサイバーセキュリティインシデントの発生状況や、被害拡大を最小限にとどめるための基本的事項を説明し、擬似的なインシデント発生時対応手順を体験することにより、組織内の基本方針やルールなどを考えていただくことを目的として「サイバーインシデント演習」を開催します。

是非、この機会にインシデント対応の演習をご体験ください。

プログラム・参加申込は裏面へ

総務省 近畿総合通信局

経済産業省 近畿経済産業局

KIIS 一般財団法人 関西情報センター

主催：関西サイバーセキュリティ・ネットワーク事務局
（近畿総合通信局・近畿経済産業局・一般財団法人関西情報センター）

プログラム

＞第１部　サイバーセキュリティ講演［14:00～15:00］

■「サイバー攻撃の情勢及び対応策について」

昨今話題となっているインシデント事例などを紹介しながら、サイバー攻撃による被害拡大を最小限にとどめるインシデント対応の流れを解説します。

＞第２部　サイバーセキュリティ演習［15:00～17:00］

■「セキュリティ事件・事故発生時の効果的な対応について」

・第1部の内容を踏まえ、参加者によるグループワークを実施します。
机上演習として疑似的なインシデント対応を体験いただき、インシデント発生から対応の検討、評価までのサイクルを、参加者が互いにディスカッション・意思決定しながら進めていく形をとります。

事態発生 ⇨ 対応検討 ⇨ 対応評価

※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：株式会社川口設計
代表取締役　川口 洋 氏

2002年 大手セキュリティ会社にて社内のインフラシステムの維持運用業務ののち、セキュリティ監視センターに配属
2013年～2016年 内閣サイバーセキュリティセンター(NISC)に出向。行政機関のセキュリティインシデントの対応、一般国民向け普及啓発活動などに従事。
2018年 株式会社川口設計 設立。Hardening Projectの運営や講演活動など、安全なサイバー空間のため日夜奮闘中。

【新型コロナウイルス感染防止に関するお願い】

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（会場入口での検温およびアルコール消毒の設置等）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」のみの開催になる可能性があります。

・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」 参加申込み

■参加ご希望の方は、QRコードもしくは申込ページよりお申込み下さい。
［申込み期限］：令和５年２月１５日 (水) まで

申込ページURL：https://www.kiis.or.jp/form/?id=83

※本イベントの申込受付及びご案内等は、請負事業者である一般財団法人関西情報センター（KIIS）が行います。

【本件お問い合わせ】総務省 近畿総合通信局 サイバーセキュリティ室
TEL：06 6942 8623／e-mail：kansai-seminar@ml.soumu.go.jp