お知らせ

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

令和７年１月９日
信越総合通信局

サイバーインシデント演習ｉｎ長野を開催

～　セキュリティのインシデント対応を体験しませんか？　～

信越総合通信局（局長：田口　幸信（たぐち　ゆきのぶ））は、信越情報通信懇談会（会長：中野　敬介（なかの　けいすけ））及び信越サイバーセキュリティ連絡会と共催で、中小企業・団体等の経営層、セキュリティ責任者、情報システム運用担当者等の皆さまを対象に、「サイバーインシデント演習　ｉｎ　長野」を開催いたします。多数のご参加をお待ちしております。

中小企業等においては、サプライチェーンの最前線を担い、日頃から多くの取引先や関連企業と情報のコミュニケーションを取られていますが、サイバー攻撃を受けた場合に備えて、平常時から危機管理の意識とともに、体制整備を構築した上で、サイバーセキュリティインシデント発生時の対応方法や手順等を措置しておくことが重要となっています。

本演習では、情報ネットワークにおける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、インシデント発生時対応手順を擬似的に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開催いたします。

１　日時

令和７年２月 17 日（月）午後１時３０分から午後５時まで

午後１時から受付開始いたします。

２　会場

ＪＡ長野県ビル　１２階Ａ会議室

長野県長野市南長野北石堂町 1177 番地３（ＪＲ長野駅から徒歩 10 分）

３　定員

４０人（定員となり次第、受付を終了いたしますので、ご了承ください。）

４　参加費

無料（交通費は各自ご負担をお願いいたします。）

５　応募対象

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等の皆さま

６　共催

総務省信越総合通信局、信越情報通信懇談会及び信越サイバーセキュリティ連絡会

７　講師及びプログラム

(1)　講師

株式会社川口設計　代表取締役　川口　洋　氏

(2)　プログラム

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」

８　申込方法

右記の二次元コード、若しくは以下 URL 内の申込フォームから、２月 10 日(月)までにお申込みをお願いいたします。

https://www.kiis.or.jp/form/?id=175

（本セミナー―請負の一般財団法人関西情報センターの HP にリンクいたします。）

二次元コード

詳細は、別添の案内チラシをご覧ください。

連絡先　信　越　総　合　通　信　局
サイバーセキュリティ室
電　話　０２６－２３４－９９３６

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？

サイバーインシデント演習 in 長野

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。

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。

日時 2025年2月17日(月) 13:30～17:00
（13:00受付開始）

会場 JA長野県ビル　12階A会議室
(長野県長野市大字南長野北石堂町1177番地3/JR長野駅 徒歩10分)

定員 40名 ※定員に達し次第、受付を終了いたします

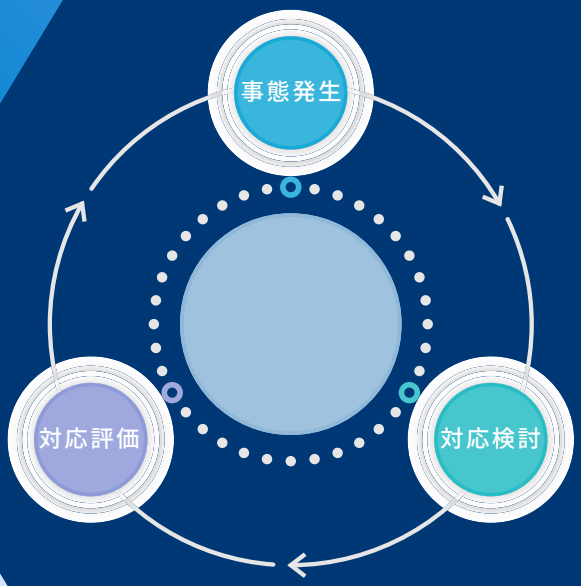
対象 中小企業／団体等の経営層、
セキュリティ責任者及び情報システム運用担当者の方等

共催：信越総合通信局、信越情報通信懇談会、信越サイバーセキュリティ連絡会

プログラム

第１部サイバーセキュリティ講演 [13:30～14:30]

■「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 [14:30～17:00]

■「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。
・またグループごとに配したパソコンを使用してインシデントとなりうるリスクを擬似的体験して、どのようにサイト誘導され、情報が盗まれるのかについて理解を深めます。

※2023年11月1日に実施した演習とは異なるテーマで実施いたします。
※本演習に参加される皆様同士でぜひ名刺交換いただければと存じます。(必須ではございません)
当日は名刺をご持参いただくことをお勧めいたします。

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。

お申込みはこちら

［申込み期限］2025年2月10日(月)まで
[申込みページ]
https://www.kiis.or.jp/form/?id=175

※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。

お問い合わせ先

総務省 信越総合通信局
サイバーセキュリティ室
TEL：026-234-9936
Mail：cyber-shinetsu@soumu.go.jp