お知らせ

くらしの中に 総務省

MIC Ministry of Internal Affairs and Communications

令和８年１月８日
信越総合通信局

サイバーインシデント演習ｉｎ新潟の開催

～　セキュリティのインシデント対応を体験してみませんか？　～

信越総合通信局（局長：鈴木 厚志（すずき　あつし））は、信越サイバーセキュリティ連絡会及び信越情報通信懇談会と共催で、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　新潟」を開催いたします。皆さまのご参加をお待ちしております。

１　概要

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。

２　日時

令和８年２月１９日（木）午後１時から午後５時まで

午後０時３０分から受付開始いたします。

３　会場

アートホテル新潟駅前（会場名：越後）

新潟県新潟市中央区笹口一丁目１番（ＪＲ新潟駅から徒歩１分）

４　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～第３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」

５　募集対象、定員

(1)　対象者

中小企業や団体の経営層、企業団体などのサイバーセキュリティ担当、情報システム運用担当者の皆さま

(2)　定員

先着４０人

６　参加費

無料です。（会場までの交通費等は各自ご負担ください）

７　共催

総務省信越総合通信局、信越サイバーセキュリティ連絡会、信越情報通信懇談会

８　申込方法

別添パンフレットの二次元コード、もしくは以下ＵＲＬ内の申込フォームより、２月１２日（木）までにお申込みください。

https://www.kiis.or.jp/form/?id=270

（一般財団法人関西情報センターのホームページにリンクします）

９　その他

応募に関する個人情報につきましては、今回の開催運営に関する事務手続のみに使用し、終了後は適切に廃棄いたします。また、会場において写真撮影等を実施する場合があり、その際に会場内の参加者が映り込む場合があります。それらは、総務省ホームページ等で掲載される場合がございますので、あらかじめご了承ください。

担当部署　サイバーセキュリティ室
電話番号　０２６（２３４）９９６１

サイバーインシデント演習 in 新潟

セキュリティのインシデント対応を体験しませんか？

開催概要

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。

開催体制

【共催】
総務省信越総合通信局
信越情報通信懇談会
信越サイバーセキュリティ連絡会

イベント詳細

2026年2月19日(木)
13:00~17:00
（12:30受付開始）

アートホテル新潟駅前
(会場：越後)
(新潟県新潟市中央区笹口1-1/
JR新潟駅直結)

中小企業や団体の経営層、企業団体などのサイバーセキュリティ担当、情報システム運用担当者の皆さま

定員：40名
※定員に達し次第、受付を終了いたします

参加費無料

Cyber incident exercise

プログラム

第１部 講演
[13:00～14:00]

■「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・第3部 演習
[14:00～17:00]

■「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。
　第2部では実機演習として、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体験して、意図しない情報漏洩がどのように起きるのか、また不正なサイトからどのように情報が盗まれるのかについて理解を深めます。
　第3部では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。

※2023年に当局が実施した演習とは異なるプログラムを実施します。
※必須ではございませんが、参加者の皆さま同士で名刺交換など交流いただければと存じます
※当日は名刺をご持参いただくことをお勧めいたします。
※講演・演習は日本語で行います。

講師

川口 洋 氏
株式会社川口設計
代表取締役

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

上記二次元コードまたは以下の
申込URLよりお申込みください。
https://www.kiis.or.jp/form/?id=270

[申込期限]2026年2月12日(木)まで

お問い合わせ

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

※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。

Cyber incident exercise