STEP 3

サイバーインシデント演習 in 北海道

開催概要

　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。

　そのためサイバー攻撃を受けた場合に備えて、社内意識の醸成、組織内の基本方針や体制の構築、対応方法や手順などの共有が重要となっています。

　本演習では、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、インシデント発生から対応検討、評価までのサイクルを机上演習いただきます。

※本演習は、「3ステップで学ぶ情報セキュリティ支援パッケージ」の**<STEP3 実行>** として開催します。

主催

総務省北海道総合通信局・経済産業省北海道経済産業局・
北海道地域情報セキュリティ連絡会（HAISL）

イベント詳細

2026年
1月23日(金)　13:00~17:00
（12:30受付開始）

ACU-A 中研修室1206
(札幌市中央区北4条西5丁目アスティ45
/JR札幌駅 徒歩5分)

※講演・演習はオンラインによる聴講が可能ですが、
　実機演習はできません。
※オンラインでの聴講にあたっての注意事項は、
　申込ページをご確認ください。

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

会場定員：40 名
※定員に達し次第、受付を終了いたします

参加費無料

右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=266

[申込期限]2026年 1月15日(木) まで

Cyber incident exercise

プログラム

第１部サイバーセキュリティ講演
［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部サイバーセキュリティ演習
［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」
・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、グループごとにパソコンを使用して、インシデントとなりうるリスクを疑似体験し、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、インシデント発生から対応検討、評価までのサイクルを机上演習します。

※講演・演習は日本語で行います。
※昨年度（2025.1.15）に実施した演習とは異なるテーマで実施しますので、既参加の方も是非、今年度もご参加ください。
※会場ではグループワークを実施しますので、本演習に参加される皆様での名刺交換の機会もございます。必須ではありませんが、名刺の持参をお勧めいたします。

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。

お問い合わせ

●演習全般について

総務省 北海道総合通信局
サイバーセキュリティ室
011-709-2311(内線4767)
security-hokkaido@soumu.go.jp

●お申込みについて

一般財団法人関西情報センター
イノベーション創出支援グループ
06-6809-2142
rstaff@kiis.or.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