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１３日
信越総合通信局

サイバーセキュリティ月間の開催行事等のご案内

信越総合通信局（局長：鈴木 厚志（すずき　あつし））は、政府で定められた毎年２月１日から３月１８日までの「サイバーセキュリティ月間」に、関係機関、団体等と協力して、サイバーセキュリティの普及啓発活動を展開してまいります。
皆さまからのご応募、ご参加をお待ちしております。

１　サイバーセキュリティ月間とは

近年、サイバーセキュリティ上の攻撃が高度化しており、政府、企業等への攻撃は重大な脅威となっています。また、スマートフォンの普及とともに悪質化、巧妙化している不審メール等によって、個人に対する被害が深刻化しています。安心、安全にＩＣＴ（情報通信技術）を利用していくために、国民の一人一人がサイバーセキュリティについて意識するとともに、これら問題に対応する必要があります。

この２月１日から３月１８日までの「サイバーセキュリティ月間」の期間中は、政府機関だけでなく、各種団体と連携したサイバーセキュリティの普及啓発活動が実施されます。

２　信越総合通信局管内で予定されているイベントについて

当局管内では、次のイベントが開催予定です。皆さま方からのご参加をお待ちしております。

(1)　リスク分析ワークショップ

ア　日時

令和８年１月１９日（月）午後１時３０分

イ　会場

ＪＡ長野県ビル　１２階Ｃ会議室

長野県長野市１１７７番地３

ウ　共催

長野県サイバーセキュリティ連絡会（事務局：長野県ＩＴコーディネータ協議会、経済産業省関東経済産業局、総務省信越総合通信局）、独立行政法人情報処理推進機構（ＩＰＡ）

エ　イベントの詳細、参加申込等

以下のホームページ、別添１をご覧ください。

https://nagano-it.jp/news/5485/

(2)　【第１４回】サイバーセキュリティ勉強会 2026 冬 in 塩尻

ア　日時

令和８年２月７日（土）午後１時３０分

イ　会場

塩尻インキュベーションプラザ

長野県塩尻市大門八番町１番２号

ＺＯＯＭウェビナー配信あり

ウ　共催

塩尻市セキュリティ啓発活動実行委員会、塩尻市役所、一般財団法人塩尻市振興公社、クオリティソフト株式会社、有限会社トラストネットワークス

エ　イベントの詳細、参加申込等

以下のホームページをご覧ください。

https://shiojiri-cyber.connpass.com/event/372811/

(3)　第２０回セキュリティセミナー

ア　日時

令和８年２月１３日（金）午後１時

イ　会場

新潟大学駅南キャンパスときめいと

新潟県新潟市中央区笹口一丁目１番地　プラーカ１・２階

オンライン参加もあります。

ウ　共催

特定非営利活動法人新潟情報通信研究所、総務省信越総合通信局、信越情報通信懇談会

エ　イベントの詳細、参加申込等

別添２をご覧ください。

(4)　サイバーインシデント演習ｉｎ新潟

ア　日時

令和８年２月１９日（木）午後１時３０分

イ　会場

アートホテル新潟駅前

新潟県新潟市中央区笹口一丁目１番

ウ　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

エ　イベントの詳細、参加申込等

別添３をご覧ください。

担当部署　サイバーセキュリティ室
電話番号　０２６（２３４）９９６１

リスク分析ワークショップ

参加無料

1.19 月
13:30～16:30

参加形式 集合開催

開催場所 JA長野ビル　12階C会議室
（長野県長野市北石堂町１１７７－３）

対象 県内の中小企業

共催 長野県サイバーセキュリティ連絡会
（事務局：長野県ITコーディネータ協議会　経済産業省関東経済産業局
総務省信越総合通信局）、
独立行政法人情報処理推進機構(IPA)

プログラム

『開会挨拶』

経済産業省関東経済産業局

『情報資産を守る
～リスク分析・対応ワークショップ～』

講師：中小企業診断士/情報処理安全確保支援士
青柳 由多可氏

『閉会挨拶』

長野県サイバーセキュリティ連絡会

お申込み
お問合せ

下記URLまたは右記二次元コードを
読み込みお申込ください。
申込期限：1月14日（水）23:59
https://info.ipa.go.jp/form/pub/application/semi-reg15

〈セミナー運営事務局〉
株式会社船井総合研究所　担当：積山・園田
03-6684-5159
px-isec-seminar@ipa.go.jp

「サイバーセキュリティー月間」記念

第20回セキュリティセミナーのご案内

＊とき　：令和　８年　２月１３日（金曜日）１３：００（１２：３０～接続可能）～１７：３０
＊ところ：ときめいと（現地参加を希望される方（最大100名程度迄（予定））　及び
　　オンラインセミナー（(最大400名程度迄）メールで申込頂いた方に参加ＩＤ等の情報を受け付け処理後発送します。）

＊第一部（１３：１０～１５：１０　１２０分　途中10分の休憩を挟みます。）
　講師　　：総務省サイバーセキュリティ統括官室　参事官補佐　三宅　雅矩（ミヤケ　マサノリ）様
　演題　　：「総務省におけるサイバーセキュリティ政策の最新動向」（仮題）

＊第二部（１５：２０～１７：２０　１２０分　途中10分の休憩を挟みます。）
　講師　　：落合 博幸　先生
　演題　　：「生成AI時代のフェイク情報とダークパターン
　　― サイバー空間で私たちの判断はどう誘導されているのか ―」

＊募集人員　　：500名（リアル講義100名＋リモート講義400名）まで
　（若い方からお年寄りの方まで幅広い年齢層を募集しております。また、リモート講義は国内におけるエリアを問わず受講の応募をお待ちしております。）

＝事前にメールでお申し込みが必要です。＝

＊参加費　　：無料

＊第二部講師　落合　博幸氏　プロフィール

新潟大学人文学部卒
株式会社ラック　サイバー･グリッド･ジャパン　ICT利用環境啓発支援室
新潟県警サイバー犯罪対策アドバイザー
新潟県サイバー脅威対策協議会　幹事
新潟大学　特任教授
開志専門職大学　非常勤講師
敬和学園大学情報メディア研究所　客員研究員
情報セキュリティワークショップin越後湯沢　大会副委員長

＊講演内容
「インターネットやSNSの普及により、フェイク情報や詐欺、誤認を誘う表示や操作が身近な問題となっています。特に生成AIの発展により、文章や画像、音声を本物と見分けがつかない形で作成できるようになり、被害はより深刻化しています。
本講演では、前半にフェイク情報をめぐる国内外の事例を紹介し、生成AIがフェイク情報や詐欺にどのように悪用されているのかを解説します。後半では、利用者を意図せず不利な選択へ誘導する「ダークパターン」について、その歴史や代表的な事例、欧米および日本の法規制の動向を説明します。
日常生活の中で情報を正しく見極め、被害を防ぐために必要な視点や注意点をお伝えします。

＊主催　　：特定非営利活動法人　新潟情報通信研究所、信越情報通信懇談会
＊共催　　：総務省　信越総合通信局
＊後援　　：新潟大学　工学部工学科　知能情報システムプログラム、開志専門職大学

＊参加申し込み（ホームページ　移行中　もご覧下さい）
　メールにてお申し込み下さい、お問い合わせもメールで！
　　メール　　niigata.icl.npo@gmail.com　　（担当　髙橋）

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