

# 関西サイバーセキュリティ・ネットワーク (地域SECURITY)の取組について

2023年2月1日

近畿総合通信局 サイバーセキュリティ室

1. セキュリティコミュニティ(地域SECURITY)について
2. サイバーセキュリティ・カフェ
3. サイバーセキュリティ・スクール
  - 3-1.ゲーム編
  - 3-2.CTF編
  - 3-3.来年度西日本地域連携若者向けイベント
4. 最後に

# 1. 地域に根付いたセキュリティコミュニティ(地域SECURITY)の形成促進

■ 総務省、経済産業省が互いに連携しつつ、地域単位の事業者のセキュリティ対策の強化のため、地域に根付いたセキュリティコミュニティ(地域SECURITY)の形成の促進を図る。

● 全国規模で事業展開する企業に比べ、地域の企業や地方公共団体などについては、有効なサイバーセキュリティ対策をとるための人材育成・普及啓発の機会や情報共有の枠組みなどが不足しているおそれ。



● 地域の企業や地方公共団体については、各者とも単独で有効なサイバーセキュリティ対策をとることは困難であり、地域レベルでの**コミュニティを形成**して情報共有等を強化する必要がある。

## 地域に根付いたセキュリティコミュニティ



## セキュリティコミュニティの形成の促進

- ①当該地域における大手事業者、②業界団体（地方支部など）、③都道府県警、④サイバーセキュリティ関係事業者・機関、⑤地方公共団体、⑥有識者などによる地域のサイバーセキュリティ向上のための推進体制を構築する。なお、情報共有体制がすでに存在している地域においては、既存の体制を活用していくことが望ましい。
- 地域の企業等向けに①定期的なセミナーやインシデント演習※の実施、②セキュリティ関連の情報共有の枠組みなどを構築。

# 1. 各地域におけるセキュリティコミュニティ

- 全11地域において、セキュリティコミュニティの設立が完了。今後は、地域全体への活動の展開や、セミナー等の開催に加えて幅広い層への普及啓発を推進。



# 1. 全国総合通信局の令和4年度の取組(本省支援分・見込み)

令和4年度は、各総合通信局等への要望調査の結果を踏まえ、サイバーセキュリティに関するセミナー（計17回）、インシデント対応演習（計11回）及び若年層向けのCTF（計5回）の開催を支援。

支援施策名	管区	支援内容(令和4年度)
地域のセキュリティコミュニティが関与するセミナーの開催支援 (計17回)	北海道(3日間)、 東北、 北陸、 東海(2日間※1)、 近畿(4日間※2)、 中国(2日間)、 四国、 九州、 沖縄(2日間)	<ul style="list-style-type: none"> <li>地域で開催するセミナーの運営補助</li> </ul> <p>※1 東海管区における2日間の内、1日間は地域のセキュリティコミュニティに参画する事業者や有識者が参加する会合の開催</p> <p>※2 近畿管区における4日間の内、計3日間は座談会(セキュリティカフェ)及びイベント(セキュリティ・スクール)の開催</p>
地域のセキュリティコミュニティ参加事業者に対するインシデント対応演習の実施 (計11回) ※インシデント対応演習:インシデント発生時の一次対応や情報連携のグループワーク	北海道、東北、北陸、 信越、関東、東海、 近畿、中国、四国、 九州、沖縄 (各1回)	<ul style="list-style-type: none"> <li>インシデント対応演習の企画・内容検討</li> <li>インシデント対応演習の開催に係る支援全般</li> </ul>
若年層向けCTFの実施 (計5回) ※CTF:Capture The Flagの略で、ゲーム形式でセキュリティの実践的スキルを競うコンテスト	東北、 北陸(2日間)、 近畿、 中国	<ul style="list-style-type: none"> <li>若年層を中心としたサイバーセキュリティ初学者向けのCTFの企画・運営</li> </ul>

※ このほか、令和5年1月以降にメールマガジン用のコンテンツを作成し、発信予定。

## 2. はじめに

前提：組織規模や立場によって、求めている情報が異なる

(例えば、経営層や一般社員はフォレンジックの技術内容の講義を求めているいない。)

○関西サイバーセキュリティネットワークにおける取組の対象について

	大企業	中小企業	個人事業	学生
経営層		サイバーセキュリティ・カフェ サイバーインシデント演習		
情報管理 担当者	サイバーインシデント演習 セキュリティ・リレー講座 セキュリティアドバイザ派遣事業	サイバーセキュリティ・カフェ サイバーインシデント演習 セキュリティ・リレー講座 セキュリティアドバイザ派遣事業	サイバーセキュリティ・カフェ サイバーセキュリティ・スクール セキュリティ・リレー講座	サイバーセキュリティ・スクール 情報セキュリティセミナー
一般社員	サイバーセキュリティ・スクール 情報セキュリティセミナー	サイバーセキュリティ・スクール 情報セキュリティセミナー		

本日も説明する

- ・サイバーセキュリティ・カフェ
- ・サイバーセキュリティ・スクール

⇒これからサイバーセキュリティを学ぶ方やセキュリティ強化を検討する初級者が対象

## 2. サイバーセキュリティ・カフェ

イベント開催回数が多い大都市圏ではなく、「地方都市」において中小企業等のサイバーセキュリティ担当者を対象に、サイバー攻撃の現状やセキュリティ対策などの【ミニ講演】とあわせ、質問や相談を気軽にできる【座談会】を会場とオンラインのハイブリッドで開催。

開催実績

令和2年12月 カフェin福知山(京都府福知山市):15名  
 令和3年11月 カフェin奈良(奈良県大和郡山市):30名  
 令和4年12月 カフェin紀南(和歌山県田辺市):32名

令和3年 3月 カフェin彦根(滋賀県彦根市):7名  
 令和4年 1月 カフェin但馬(兵庫県豊岡市):38名

### サイバーセキュリティ・カフェ in 紀南 プログラム

#### ●ミニ講演1

「ネット犯罪等の防止について」

和歌山県田辺警察署 地域課 巡查部長  
 神保 元希 氏

#### ●ミニ講演2

「サイバー攻撃の現状と最新のセキュリティ対策」

クオリティソフト株式会社 営業本部  
 アカウントマネージャー 小山 裕輔 氏

#### ●座談会

モデレーターNPO情報セキュリティ研究所  
 代表理事 臼井 義美 氏

パネリスト 神保 元希 氏 ・ 小山 裕輔 氏

#### ●対象者

主に田辺市、田辺市周辺地域の中小企業、団体等のサイバーセキュリティに関心のある方やサイバーセキュリティ担当者など。

## サイバーセキュリティ・ カフェ

in 紀南

参加費無料

～まだ他人事だと思っていますか？  
危険はすぐそこまで来てますよ！～

「サイバーセキュリティ、なんやそれ？」

そんなあなたの疑問にお答えします。  
 難しい用語を使わず簡単に解説！  
 お気軽にご参加下さい！

日時

令和4年12月15日(木)

14:30～16:40(終了予定)

開催形式

会場(定員20名)及びオンライン(Webex)

## 気軽に相談!企業情報の守り方 ~奈良の最強講師と考えるセキュリティ対策~



### サイバーセキュリティ・カフェ in 奈良

日時: 令和3年11月15日(月) 13:30~16:00

会場: HARUHI (JR郡山駅より徒歩1分/無料駐車場あり)  
<https://haruhi-nara.com/>

対象者: 奈良県周辺地域の中小企業、団体のサイバーセキュリティに関心のある方、サイバーセキュリティ担当者など。  
※初級者向け内容で興味のある方ならどなたでも参加いただけます!

総務省 近畿総合通信局 経済産業省 近畿経済産業局 KiiS 関西情報センター

## サイバーセキュリティ・カフェ in 但馬

令和4年1月18日(火) 14:30~17:00



### 荒波ウイルス襲来!!! 今こそ、最強講師と打ち砕け!!!

参加費  
無料

対象者: これからサイバーセキュリティ対策をお考えの方、既に対策済みで対策強化方法や最新事情を知りたい方。(初級者向けです)  
※中小企業・団体・個人など、興味のある方ならどなたでも参加いただけます!  
会場: アールベルアンジェ豊岡 (JR豊岡駅より徒歩5分/無料駐車場あり)

## ○過去の取組一覧

### 3. 主な取組

#### ○令和4年度

- 令和5年1月13日  
[「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？」](#)
- 令和4年12月19日  
[学生向け「CTFワークショップin大阪」を開催](#)  
[「ゲーム形式でサイバーセキュリティを体験してみよう」](#)
- 令和4年11月7日  
[「サイバーセキュリティカフェin紀南」を開催](#)  
[「まだ他人事だと思っいていますか？危険はすぐそこまで来てますよ！」](#)  
**【トピックスに開催結果を掲載しました】**
- 令和4年8月10日  
[第2回サイバーセキュリティスクール\(CTF編\)](#)  
[「サイバー空間からの挑戦状！仲間とともに立ち向かえ！」](#)  
**【トピックスに開催結果を掲載しました】**
- 令和4年8月1日  
[Who is Secwre Wolf?](#)  
[「第1回サイバーセキュリティスクール\(ゲーム編\)」を開催」](#)  
**【トピックスに開催結果を掲載しました】**

#### ○令和3年度

- 令和4年3月17日  
[「のぞいてみよう！ITエンジニアの世界](#)  
[「若者向けCTFワークショップを開催」](#)  
**【トピックスに開催結果を掲載しました】**

## ○開催結果の掲載

### サイバーセキュリティ・カフェin紀南を開催(2022.12.15)

2023年1月12日 掲載

関西サイバーセキュリティ・ネットワーク事務局<sup>※</sup>は、令和4年12月15日(木)、和歌山県田辺市内の会場及びオンラインにより、地元の企業や団体等のサイバーセキュリティ意識の醸成や、セキュリティ対策レベルの向上を目的として、「サイバーセキュリティ・カフェin紀南」を開催しました。本イベントでは、サイバー攻撃の現状やサイバーセキュリティ対策をより身近な問題として感じていただけるよう、分かりやすく説明するミニ講演と、素朴な質問や相談ができる座談会を実施しました。

冒頭、主催者を代表し、近畿総合通信局長の井上が挨拶を行い、「大阪府内の病院において、サイバー攻撃により電子カルテシステムが障害を受け通常診療ができなくなるなど、業務に深刻な影響を及ぼす事例が発生している。サイバー空間は利便性の向上をもたらす反面、攻撃を受けた時の影響は計り知れず、非常に大きなものとなる。セキュリティ対策を確実に行うことはいうまでもなく、事業継続の観点からサイバー攻撃からの復旧について日頃から備えておくことも重要である。」と指摘しました。



主催者挨拶(井上局長)

#### ミニ講演

##### 「ネット犯罪等の防止について」

まず、和歌山県田辺警察署 地域課 巡査部長の神保元希氏から、サイバー犯罪の動向や和歌山県内での被害・相談状況、実際のトラブル事例などについて説明がありました。偽サイトや詐欺サイトによる被害に関する相談が特に増加しており、近年偽サイトの作りが精巧になっていることから、複数の特徴をチェックし慎重に見極めることが必要であるとお願いいただきました。そのほか、増加している手口としてランサムウェアや標的型攻撃メール、サポート詐欺、SNSのID(アカウント)不正利用などについて解説があり、日頃から注意することとして、ID・パスワードの管理徹底や各々のセキュリティの意識・知識の向上が特に大切であると呼び掛けました。

##### 「サイバー攻撃の現状と最新のセキュリティ対策」

次に、クオリティンフト株式会社 営業本部 アカウントマネージャーの小山裕輔氏から、企業・団体など組織における被害が増加しているサイバー攻撃の現状やその対策について説明がありました。ランサムウェア・標的型攻撃のほか、近年、セキュリティ意識の高い大企業を直接標的とせず、取引先や傘下の企業など対策の甘い組織を攻撃の足掛かりとして狙う「サプライチェーン攻撃」が増加しており、中小企業等においても十分な対策が必要であると注意喚起しました。また、セキュリティ対策として、既知のマルウェアをパターンマッチングにより防ぐウイルス対策ソフトに加え、未知の脅威への対策として、プログラムの振る舞いにより悪意のあるマルウェアかどうか判断する検出方法(ビヘイビア)が可能な製品などを組み合わせた「多層防御」が重要であること、組織内における脆弱性の適切な把握と是正が大切であることをお願いいただきました。

## 2. サイバーセキュリティ・カフェ

### ①期待

1. 地元企業の経営者層や病院関係の積極的な参加。  
→地元商工会議所や県商工会連合会に周知依頼。  
→令和4年度から医師会に周知依頼。
2. 座談会で講師と参加者の相互コミュニケーションを図る。

### ②結果

1. 参加者が少ない。(会場12名、オンライン20名)  
→病院関係の申込みは、全体の約33%と非常に高い。
2. 講演内容や座談会での質問において、メイン対象者とのギャップが発生。  
→講師の専門分野に講演内容が集中したり、座談会では一部参加者の個人的な興味に基づく質問が行われて、他の参加者が議論について行くことができないことがあった。

### ③改善点

1. ターゲットの明確化と周知方法の検討  
→半田病院や大阪急性期・総合医療センターへのサイバー攻撃で病院関係者の関心高い。  
ただし、サイバー攻撃は無差別であるため、関心が薄い地域や業界ほど参加して欲しい。
2. 講師陣やファシリテーターへ対象者レベルや開催意図の正確な共有  
→メインの参加者が求めている情報の適切な提供を行う。

カフェin紀南 講演の様子



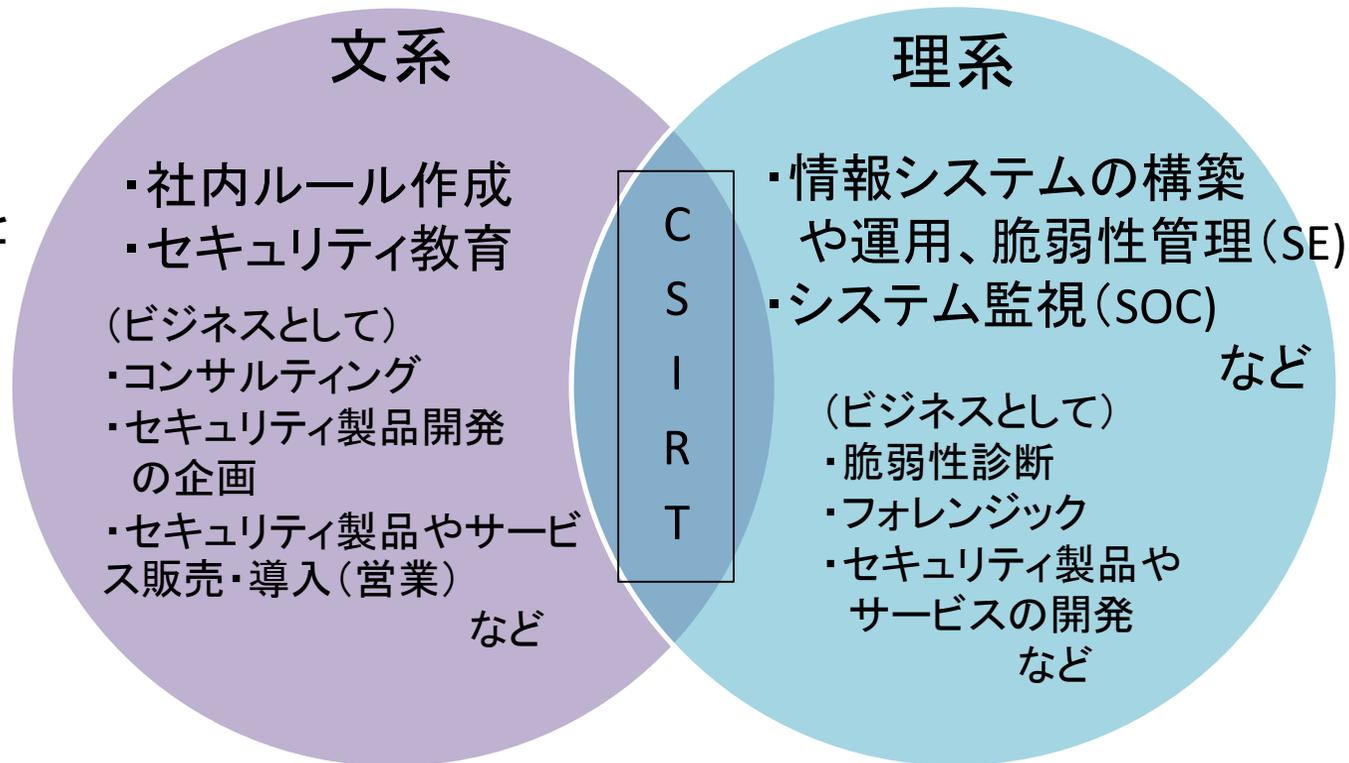
### 3. はじめに(サイバーセキュリティ・スクール)

背景: 日本で不足しているサイバーセキュリティ人材数は、およそ5万6千人  
(2022年版「(ISC)<sup>2</sup> Cybersecurity Workforce Study」より)

#### ○サイバーセキュリティに関する仕事(当局によるイメージ)

サイバーセキュリティと聞くと理系の仕事であると思われるが。。。

実は、文系の仕事も多いのではないか。



⇒学生や若年層にセキュリティの仕事のイメージを持ってもらうことが人材の裾野拡大に重要

# 3-1. サイバーセキュリティ・スクール(ゲーム編)

セキュリティを専門に学ぶ学生以外にもサイバーセキュリティへの関心を高め、地域のセキュリティ人材の裾野を広げるため、二つのゲームを通してサイバーセキュリティを学べるイベントを開催。

対象者は、サイバーセキュリティに興味はあるけど、これまで学んだことない学生など。

開催日: 令和4年9月1日 参加人数: 11名(会場)

## プログラム

1. カードゲーム『セキュリティ専門家 人狼』  
若者の間で人気のある「人狼ゲーム」題材にしたセキュリティ教材。

2. ボードゲーム『Malware Containment』  
参加者がCSIRTの一員となって、それぞれの役割に応じた行動を行い、マルウェアに感染した端末を封じ込めるゲーム。

※いずれもJNSAゲーム教育WGが開発

## 講師

日本ネットワークセキュリティ協会(JNSA)

ゲーム教育WG

長谷川氏 杉野氏 青木氏



### ①期待

1. 「サイバーセキュリティに興味はあるけど、これまで学んだことのない」学生が対象。  
→知識などを習得することを目的としたイベントではなく、ゲームを通して楽しくサイバーセキュリティやそれを守る仕事のイメージを持ってもらうことが目的。
2. 大学生などが授業のない夏休み中(9月)に開催することで、多くの参加者を期待。

### ②結果

1. 参加者が少ない。(11名)  
→ただし、群馬県から参加した学生がいた。  
(全国的にも珍しいイベントであったと考えられる)
2. 8月に募集開始で、すでに学生は夏休みに入っていた。

ボードゲーム様子



### ③改善点

1. サイバーセキュリティに興味を持っていない学生も参加しやすい工夫が必要。  
→大学の教務課や学務課などとの事前調整を検討。
2. 適切な時期のイベント開催及び周知・募集期間の設定。  
→例えば大学生の場合、7月までに募集を開始して、8月や9月にイベントを開催など。

## 3-2. サイバーセキュリティ・スクール(CTF編)

「サイバーセキュリティに興味はあるけど、これまで学んだことがない大学生、院生、高専生、短大生、専門学生や入社約1～3年目の若手社員」を対象に、現役ITエンジニアによる講演とCTFを組み合わせたイベントを開催。「8割解けるCTF」を掲げるWEST-SECの協力。

開催日: 令和4年9月15日 参加人数: 85名

### プログラム

#### 1. 講演

- ・「海外大学院(米国カーネギーメロン大学)での世界に通用するセキュリティエンジニア教育」  
→学習環境やカリキュラムなどに加え、学生の国別構成や卒業生の進路・待遇などを説明。
- ・「セキュリティ業務の現状と魅力」  
→セキュリティ業務がエンジニアだけのものではなく、幅広い分野、業種の業務に渡っていることや常に新しい課題にチャレンジできる点などの魅力を説明。

#### 2. CTF

3～4人のチームに分けて、サイバーセキュリティに関するクイズを解き、合計点数を競う。

#### 3. 解説・表彰



## 第2回 サイバーセキュリティ・スクール CTF編

令和4年9月15日(木)  
14:00～18:00



参加費無料

「サイバー空間からの挑戦状!仲間とともに立ち向かえ!」

Challenge 0 Solves

**Q1** ANIMAL 80

ANIMAL.png

Submit

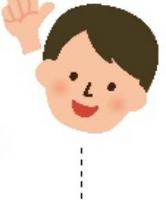
Challenge 0 Solves

**Q2** 証拠写真 [tech] 150

内閣不正電報の証拠画像を写す中、感度の付け・特定人物を写っていたことを露骨に示す写真を入力した。だが、残念ながらこの写真からはどの人物も写っていない。7枚に等しい証拠写真が用意されている。なんと、この写真に秘訣隠されてきた。お答えを。

Submit

あなたにはこの問題が解けますか?



だいちにてんちり



**CTFとは**

Capture The Flagの略で旗取りゲームのことです。専門知識や技術を使って、隠されている答えを見つけ出し、獲得した合計点数を競います。丁寧な解説と演習を通していろいろなセキュリティ技術を体験できます。CTFが初めての方を対象としておりますので、安心してご参加下さい。

### ①期待

1. 通常のCTFイベント(セキュリティの専門的な知識を駆使して、高度な問題を解く)ではなく、参加者がチームメンバーと協力して、回答を探し出して「学習」することが目的。
2. 地元大阪大学のCTFサークル「Wani Hackase」の作問協力。

### ②結果

1. 合計20チーム以上が参加。(参加者85名)  
→コミュニケーションが活発なチームは、点数が高い。
2. 一部出題レベルが高い問題があった。  
→作問者にレベルが低めの問題をお願いしていたが、趣向を凝らした問題がみられた。

### ③改善点

1. チーム毎にコミュニケーション差が大きい。  
→事前のウォーミングアップの時間を確保。
2. 解説時間の確保  
→点数を競うイベントであるため、点数に差が出る問題が必要ではあるが、解説がなかった問題に対しては疑問が残ったままイベントが終了した参加者もいた。  
競技と解説の時間のバランスが大切。

CTFの様子



## 現状

1. 全国11の総合通信局において地域コミュニティ(SECURITY)が設立
2. 地域内でのイベントのマンネリ化(講師選定など苦戦)
3. 近年インシデント事案が増加し、セキュリティ人材の裾野拡大が急務



## 目的

1. 次のステップとして各コミュニティ間連携
2. 地域の枠を超えたセミナー講師派遣・新たな形式のセミナーを横展開
3. 講演を聴講するだけでは、参加者と企業にメリットになるイベント

## コンセプト

1. 西日本地域の総務省総合通信局が連携して大規模開催！
2. 参加者:「講演」と「競技」でセキュリティ知識を学ぶ場だけでなく、  
→今後の就職や転職活動の参考に
3. 企業:各地域のセキュリティベンダが協力機関として参画  
→人材確保やサービス宣伝のためのPRの場

## 概要案

※未確定

- 参加地域 北陸、近畿(代表事務局)、中国、四国、九州総合通信局
- 開催方法 ハイブリッド開催(メイン会場(大阪)+サテライト会場+WEB)
- 開催時期 令和5年6月中旬頃予定
- 対象者 学生(大学生、院生、専門学校生、高専生など)と若手社員
- 協力 WEST-SEC

## プログラム案

- ①各局(各会場)紹介  
各地の話(名産、セキュリティの取組など)を交えて紹介
- ②講演
- ③競技(チーム戦)
  - ・二択形式:チーム内フォーミングアップ(○×問題など)
  - ・CTF形式:参加者レベルの公正性のため一般教養問題
- ④LT(Lightning Talks)大会  
各会場に地域のセキュリティベンダなどを招いて、2分のLT
- ⑤まとめ、表彰
- ⑥交流会(自由参加)  
各セキュリティベンダのブースを用意、参加者が自由に話を聞ける場。  
→参加者はLTで気になったセキュリティベンダのブースを訪問。

### ・イベントの評価方法について

評価の一つとして、「参加者数」が考えられるが、これを重視して対象者の範囲を広くすると、イベントの内容と参加者のレベルや求めている情報との乖離が発生する。

⇒参加者が少数になることを恐れずに、メインターゲットを明確に絞り、参加者が求めている情報をピンポイントで届けることが重要ではないか。  
ただし、周知方法等の工夫は必要。

# ご静聴ありがとうございました

連絡先

近畿総合通信局 サイバーセキュリティ室

Tel.06-6942-8546

[E-mail.kansai-seminar@ml.soumu.go.jp](mailto:E-mail.kansai-seminar@ml.soumu.go.jp)