資料21－1

地域のセキュリティコミュニティの形成について

令和２年２月

サイバーセキュリティタスクフォース事務局

地域のセキュリティ対策の強化

【IoT・5Gセキュリティ総合対策からの抜粋】

Ⅲ 情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策

（８）地域の情報通信サービスのセキュリティの確保

我が国の情報通信サービス・ネットワークの安全性や信頼性の確保の観点からは、全国規模や首都圏でサービスを提供している事業者だけでなく、地域単位で情報通信サービスを提供している事業者におけるサイバーセキュリティの確保も重要な課題である。

他方、**地域においては、首都圏と比較してサイバーセキュリティに関する情報格差が存在するほか、経営リソースの不足等の理由により、セキュリティ対策が十分でないケースが存在するおそれ**がある。

そのため、**業界団体やセキュリティ関係機関等と連携しつつ、地域の事業者のサイバーセキュリティ対策の質の向上に向けた連絡体制を構築することが必要**である。

なお、当該施策の展開に当たっては、Ⅲ－（６）の公衆無線LANのセキュリティの確保やⅣ－（２）－①の実践的サイバー防御演習（CYDER）の実施、Ⅳ－（２）－④の地域のセキュリティ人材育成の取組等との連携を図り、効果的に地域の情報通信サービスのセキュリティ対策の質の向上を図ることが重要である。

地域に根付いたセキュリティコミュニティの形成促進

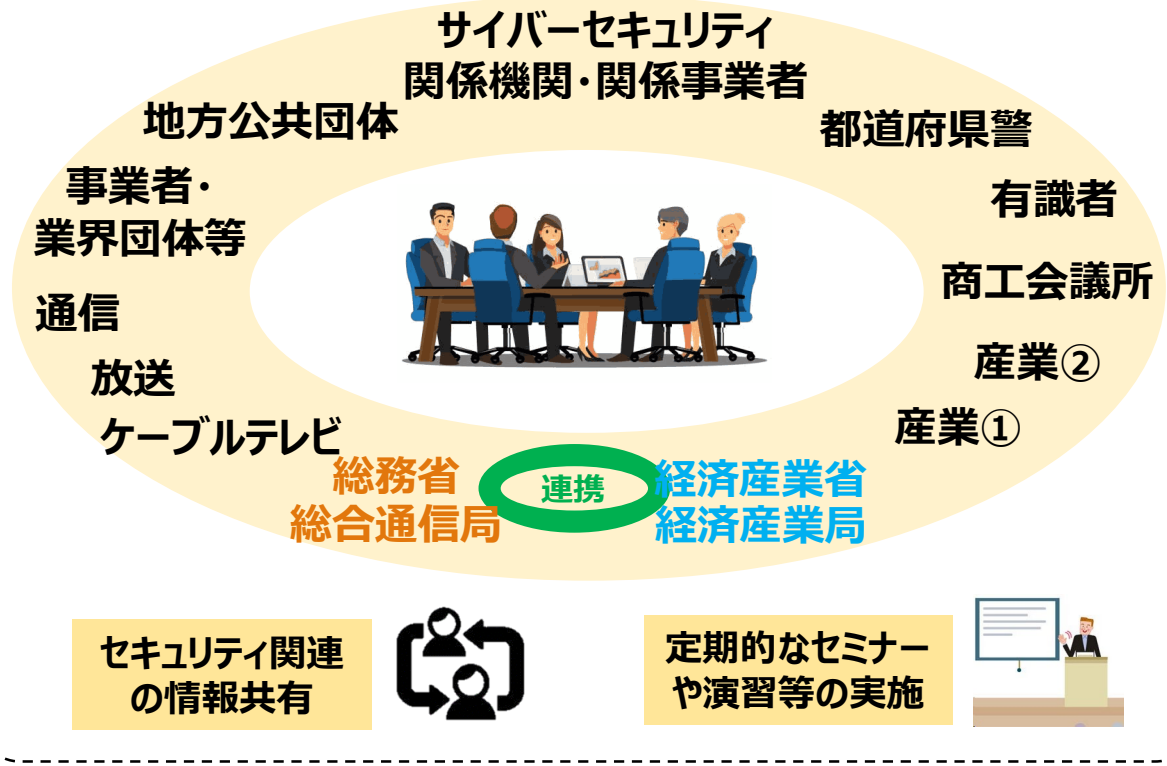
■ 総務省、経済産業省が互いに連携しつつ、地域単位の事業者のセキュリティ対策の強化のため、地域に根付いたセキュリティコミュニティの形成の促進を図る。

● 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。

※インシデント演習については構成員限りとしてスライド10に詳細を記載

令和元年度の取組の例

■ 令和元年度は北海道、近畿、中国においてセキュリティコミュニティ形成に向けた取組を促進。令和２年度はさらに複数の地域において取組を促進する。

東北
（地方版コラボレーションプラットフォーム）

経済産業省では各地域において、地方自治体、教育機関、地元企業、地元ベンダー、地元関係団体等によるセキュリティコミュニティの形成を促すための取組を実施。東北地方では各県ごとにサイバーセキュリティセミナーを開催。

令和元年10月23日　岩手　　令和２年2月12日　青森
令和元年12月 6日　秋田　　令和２年2月28日　山形（予定）
令和元年12月10日　宮城

北海道

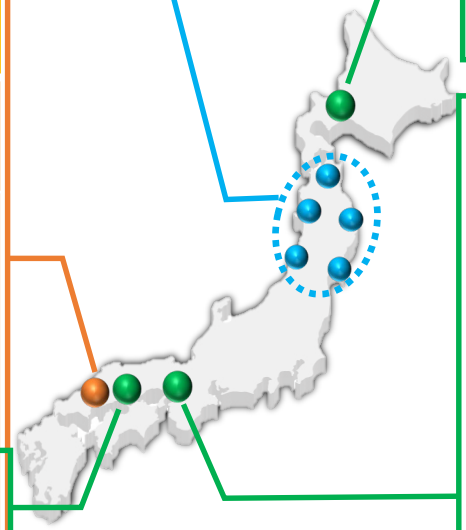
平成26年より、北海道地域情報セキュリティ連絡会**（HAISL）が既に稼働**
【事務局】 北海道総合通信局、北海道経済産業局、北海道警察本部

✓ 令和２年3月10日に北海道総合通信局主催で「サイバーセキュリティフォーラム北海道２０２０」を開催予定。本イベントにおいて、セミナーとインシデント演習の要素を一つのフォーラムに集約する予定（共催としてHAISLも参加）

中国

各県において都道府県警が中心となった連絡会があり、**これらの体制との連携を模索**

✓ 令和元年10月3日 **「中国四国民放技術責任者会議」**にて、放送事業者の技術部門責任者等に対して総務省職員が講演。
✓ 令和元年11月7日 **「日本ケーブルテレビ連盟中国支部例会」**にて、ケーブルテレビ事業者経営層に対して総務省職員が講演。
✓ 令和２年2月５日 **「サイバーセキュリティセミナー岡山」（中国経済産業局との共催）**にて総務省職員が講演。
✓ 令和２年3月中旬　経営者及びシステム担当者等を対象とした**インシデント演習**を広島にて実施予定。



総務省・経済産業省合同の取組
総務省の取組
経済産業省の取組

近畿

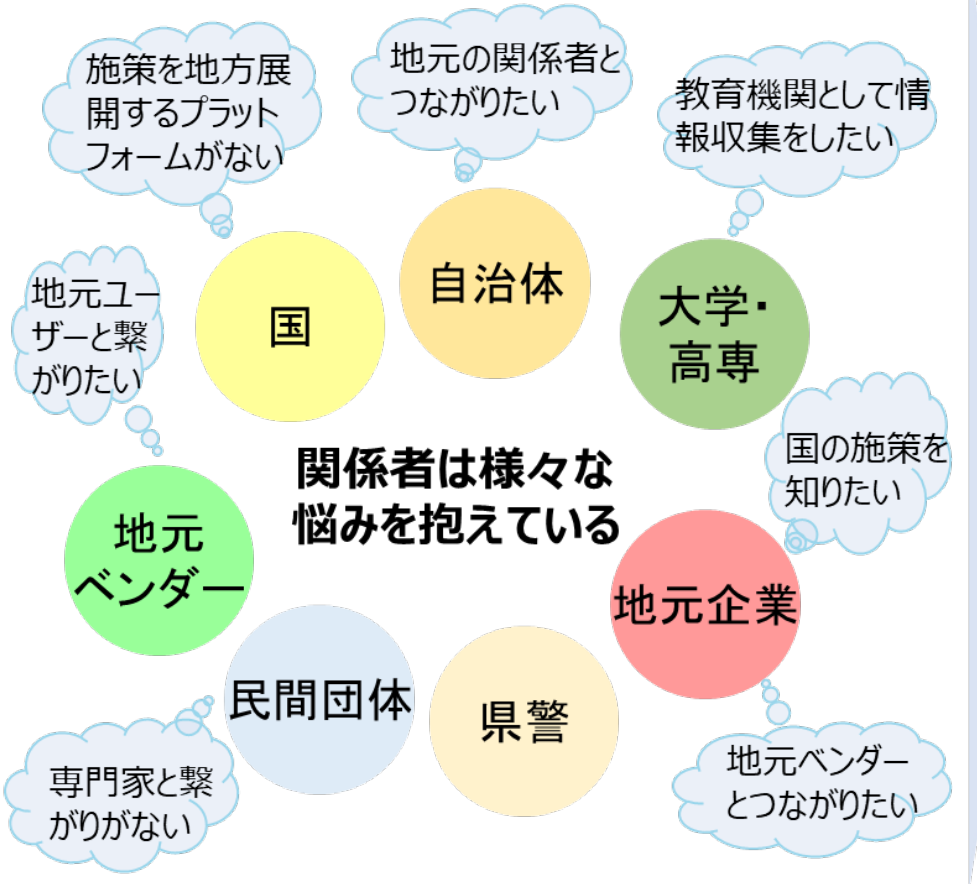
平成30年より、関西サイバーセキュリティ・ネットワーク**（関西SEC-NET）が既に稼働**
【事務局】 近畿総合通信局、近畿経済産業局、（一財）関西情報センター

✓ 令和２年1月31日 「中小企業等向け「業種横断的」セキュリティ戦略セミナー」を実施。
✓ 令和２年2月25日 「サイバーセキュリティフォーラム in 大阪」を開催予定。異業種の中小企業がユーザー企業目線で議論するパネルディスカッションを予定。
✓ 令和２年3月17日　経営者及びシステム担当者等を対象としたインシデント演習を大阪にて実施予定。

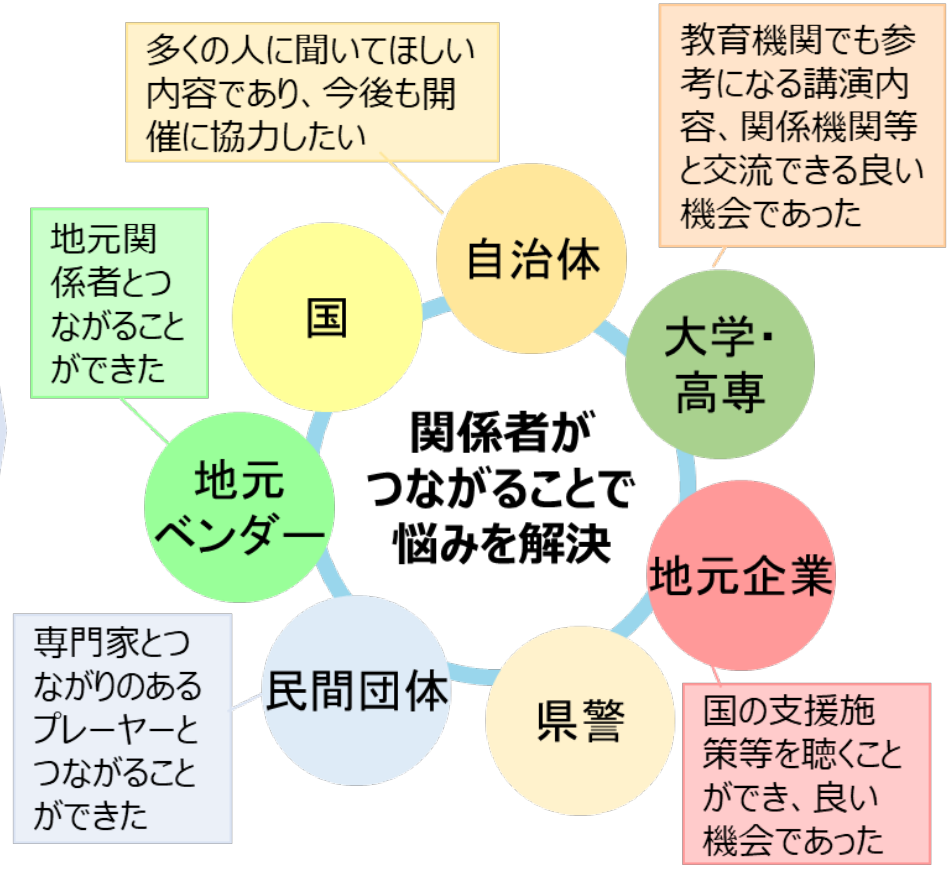
地方版コラボレーション・プラットフォームのコンセプト

- 各地域において、地方自治体、教育機関、地元企業、地元ベンダー、地元関係団体等による**セキュリティコミュニティの形成を促すことを目的に開催。**

【サイバーセキュリティセミナー in 岩手の例】



＜イベント開催後の声＞



出典：「経済産業省　第5回 産業サイバーセキュリティ研究会 WG２　資料３　事務局説明資料」より抜粋
(https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/005.html)

（参考）各地域でのコミュニティ形成に向けた取組状況

- コミュニティ形成に向けた取組を実施している地域が増えてきているが、更に取組を広める必要がある。

＜各地域の主な取組状況＞

サイバーセキュリティセミナー in 秋田

（東北経産局、IPA、秋田県、
秋田デジタルイノベーション推進コンソーシアム）

令和元年12月に、秋田県が中心となり、地方版コラボレーション・プラットフォームの第2弾として開催

サイバーセキュリティセミナー in 宮城

（東北経産局、IPA、MISEC※1、TiSA※2）

令和元年12月に、地方版コラボレーション・プラットフォーム第3弾として開催し、セミナーと合わせ個別相談会を実施

北海道地域情報セキュリティ連絡会（HAISL）

（北海道経産局、北海道総通局、北海道警察）

平成26年9月に発足し、年３回程度セミナー開催（計14回）

一般向けセミナー(令和元年9月)

会員向け勉強会の様子

サイバーセキュリティセミナー in 岩手

（東北経産局、IPA、岩手県、滝沢市、
いわて組込技術研究会）

令和元年10月に、地方版コラボレーション・プラットフォームの第1弾として開催

2/18 東京

3/18 大分

サイバーセキュリティセミナー広島・岡山

（中国経産局、中国総通局、広島県警、岡山県警）

平成31年2月に広島で、3月に岡山で初開催し、令和元年度も2月5日に岡山、6日に広島で開催予定

平成31年2月広島開催の様子

関西サイバーセキュリティ・ネットワーク

（近畿経産局、近畿総通局、KIIS※3）

平成30年10月に発足し、人材育成、機運醸成等に取り組む

サイバーセキュリティソリューション
地域別講座(令和元年7月
京都、大阪、神戸にて開催)

関西を代表する研究者8名によるリレー講義（令和元年8～9月 計8回）

※1 MISEC・・・特定非営利活動法人みちのく情報セキュリティ推進機構
※2 TiSA・・・東北地域情報サービス産業懇談会 ※3 KIIS・・・一般財団法人関西情報センター

出典：「経済産業省 第5回 産業サイバーセキュリティ研究会 WG２ 資料３ 事務局説明資料」より抜粋
（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/005.html）

北海道地域情報セキュリティ連絡会（HAISL）

■　平成26年９月、インターネットが広く普及し、サイバー攻撃や情報漏洩等のリスクへの情報セキュリティ対策が重要となっている中、国、地方公共団体、企業、団体及び教育関係者等が連携や協力を進めやすい環境を整え、関係者が情報セキュリティに関する情報を共有するとともに、情報交換や勉強会を通じた交流を深めることで北海道地域の情報セキュリティ向上することを目的に設立。

＜連絡会の概要＞

■運営体制

会長　　北海道大学　情報基盤センター長　高井　昌彰　教授
副会長　北海道情報セキュリティ勉強会　会長代理　三谷　公美（道警関係）
　　一般社団法人北海道IT推進協会　副会長　河瀬　恭弘　（経済産業局関係）
　　一般社団法人テレコムサービス協会　北海道支部長　佐々木　浩一　（総合通信局関係）
事務局　**北海道総合通信局**、北海道経済産業局、北海道警察本部

■取り組み

１　相互協力

参画機関・団体が実施する情報セキュリティ関連行事の告知や相互協力依頼、人材育成に係る環境整備など、連絡会会員間での連携を図り、各事業の効果的かつ効率的な実施に繋げる。

２　勉強会

参画機関から講師を招き、情報セキュリティインシデントのトレンドやその対策等について勉強会を行う。

３　情報発信

情報セキュリティに関する注意喚起や連絡会会員が実施する情報セキュリティ関連行事等を随時メール等により、広く情報発信する。

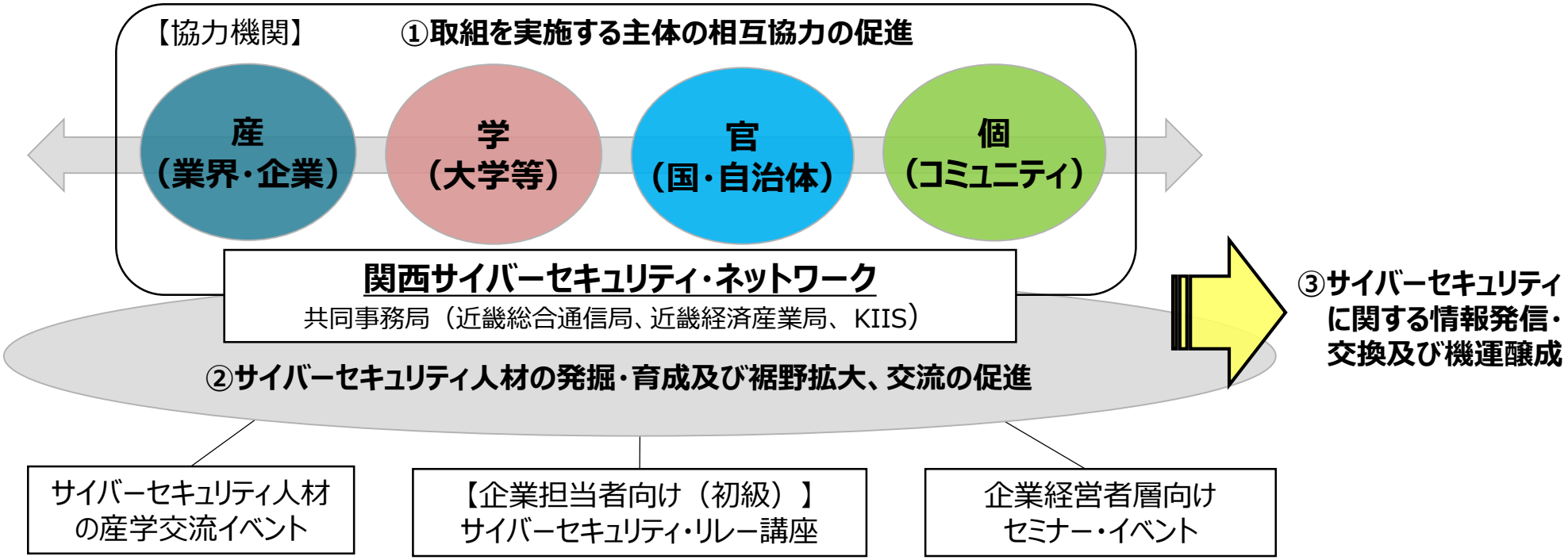
■参加機関

道内の情報セキュリティ関係機関（産学官）３９機関、事務局３機関

関西サイバーセキュリティ・ネットワーク（関西SEC-net）

■ 2018年10月、近畿総合通信局、近畿経済産業局、（一財)関西情報センター(KIIS)が共同事務局となり、サイバーセキュリティ分野における関西の産学官等の相互協力を促進するため、「関西サイバーセキュリティ・ネットワーク」（関西SEC-net）を発足。

■ 関西におけるセキュリティの推進基盤として、人材発掘・育成、情報交換、機運醸成の場を提供。サイバーセキュリティで重要な、「知る」ための取組を進める。



※原則として、産学官個の各主体が実施していない領域の取組を補完的に実施する

出典：関西SEC-net事務局（近畿経済産業局、近畿総合通信局、関西情報センター）資料より総務省作成

関西サイバーセキュリティ・ネットワーク体制

【協力機関】 ※平成30年10月17日発足時（40機関）より順次拡大中。　（順不同）65機関（令和2年2月1日時点）

カテゴリ		主な機関等
産	業界団体・経済団体	関西経済連合会、関西経済同友会、大阪商工会議所、神戸商工会議所、京都商工会議所、関西ものづくりIoT推進連絡会議関係団体（18団体：IT・電気計測器・電子電機・電子部品）、近畿情報通信協議会、日本ネットワークセキュリティ協会（JNSA）西日本支部、ISACA（情報システムコントロール協会）大阪支部、産業横断サイバーセキュリティ人材育成検討会（CRIC CSF）、日本ケーブルテレビ連盟近畿支部、テレコムサービス協会近畿支部
	セキュリティベンダー	神戸デジタル・ラボ、ファイア・アイ、ラック、エムオーテックス、大日本印刷、日本シノプス
	情報通信企業	NTT西日本、オージス総研、NEC、富士通、日立製作所、さくらインターネット、ケー・エス・ディー、日商エレクトロニクス、NTTデータ先端技術、さくらケーシーエス
	ユーザー企業	パナソニック、関西電力、大阪ガス、西日本旅客鉄道、ダイキン工業、日本放送協会大阪放送局、毎日放送、朝日放送テレビ、関西テレビ、読売テレビ放送
	その他企業	NHKテクノロジーズ大阪総支社、双日インシュアランス、SOMPリスクマネジメント、トーマツ、
学	大学・大学院	神戸大学、兵庫県立大学、和歌山大学、大阪経済大学、立命館大学情報理工学部上原研究室、奈良先端科学技術大学院大学サイバーレジリエンス構成学研究室、近畿大学、福井大学
	研究機関	産業技術総合研究所（AIST）、情報通信研究機構（NICT）
	その他	OCA大阪デザイン＆IT専門学校
官	国関係機関	内閣官房内閣サイバーセキュリティセンター（NISC）、情報処理推進機構（IPA）
	自治体	大阪府、兵庫県、滋賀県、大阪市、神戸市、堺市、京都市
個	セキュリティコミュニティ	総関西サイバーセキュリティLT大会、OWASP Kansai、tktkセキュリティ勉強会

【共同事務局】　近畿総合通信局、近畿経済産業局、一般財団法人関西情報センター（KIIS）

出典：関西SEC-net事務局（近畿経済産業局、近畿総合通信局、関西情報センター）資料より総務省作成

構成員限り

中国地方のサイバーセキュリティ関係協議会

名称	鳥取県サイバーセキュリティ対策ネットワーク	安全・安心なサイバー空間を構築するための島根県官民連携協議会	岡山県情報セキュリティ協議会（OISec）	広島県インターネットセキュリティ対策推進協議会（HISEC）	山口県ネットワークセキュリティ協議会

個別の会員情報等を含むため
非公開といたします

構成員限り

インシデント演習について

- 地域の企業のサイバーセキュリティ対策の向上には、**社内方針・ルールの策定や予算の確保等に責任を持つ経営層等の意識改革**、さらには**セキュリティの理解を持って高度な経営判断を補佐する戦略マネジメント層の育成**が必要不可欠である。
- 本施策のインシデント演習は経営層及び戦略マネジメント層を主な対象として実施する。

受講効果の維持のため、
受講者以外には非公開といたします

経営層や戦略マネジメント層を対象とした演習としてシナリオの内容が適切か御意見をいただきたい。

地域に根付いたセキュリティコミュニティの形成に関する論点

■ 本取組は、地域においてセキュリティコミュニティの形成に向けて一定の**自発的な動きがあることを前提**に、それを支援していくものとする。

- **地域のセキュリティコミュニティの立ち上げ**
  - ✓ セキュリティコミュニティが自発的に立ち上がるためにどのような要素が必要か？政府が支援できることはあるか？
- **自立的なセキュリティコミュニティの維持**
  - ✓ 平時・有事における情報共有を可能にする信頼関係はどのように構築されるのか？
  - ✓ 立ち上がったセキュリティコミュニティの自立的な在り方を損なわないような政府の支援策としてはどのようなものがあるか？

上記の論点について、御意見、コメントなどをいただきたい。

いただいた御意見を踏まえ、令和２年度の施策について関係主体と連携しながら取り組んで参りたい。