資料２

関係省庁の取組状況について

総　務　省：　放送設備のサイバーセキュリティ確保に関する検討（資料２－１）

経済産業省：　経済産業省におけるサイバーセキュリティ対策強化のための各種取組（資料２－２）

放送設備のサイバーセキュリティ確保に関する検討

資料２－１

■ 総務省において、放送設備のサイバーセキュリティ確保に関する検討を開始。

- 「重要インフラの情報セキュリティ対策に係る第4次行動計画」（平成30年7月25日 サイバーセキュリティ戦略本部決定）において、重要インフラ分野おけるセキュリティ対策について、安全等を維持する観点から情報セキュリティ対策を関係法令等における保安規制として位置付けることなど、制度的枠組みを適切に改善する取組の継続的な実施が明記されている。

- サイバー攻撃の多様化、2020年東京オリンピック・パラリンピック競技大会への対応等を見据え、令和元年6月に情報通信審議会に放送設備のサイバーセキュリティ確保に関する技術的条件について諮問し、７月より情報通信審議会放送システム委員会（※）で検討を開始。

（※）放送システム委員会の下に、放送事業者、電気通信事業者、放送関係団体、メーカ、研究機関等の関係者で構成する作業班を設置し検討。

放送システム委員会

放送設備安全信頼性検討作業班

（作業班１）地上放送・衛星放送関係

主　任　甲藤二郎 早稲田大学基幹理工学部 教授

構成員　放送事業者（地上放送(テレビ・ラジオ)、衛星放送）、電気通信事業者、メーカ、放送関係団体関係者、研究機関関係者、学識経験者（21名）

（作業班２）有線放送関係

主　任　上園一知 一般社団法人日本ケーブルラボ主任研究員

構成員　放送事業者、電気通信事業者、メーカ、放送関係団体関係者（14名）

総務省令の改正イメージ

■ 総務省において、放送設備のサイバーセキュリティ確保に関する省令改正を令和2年度春頃に予定。

- 放送法第121条等において、放送設備の技術基準への適合を義務付け。
- 技術基準は、その発生を未然に防止するための措置及び発生した際の復旧を目指した措置として、設備故障、自然災害、停電その他12項目の措置事項を省令（放送法施行規則）で規定。

・予備機器等
・故障検出
・試験機器及び応急復旧　機材の配備
・機能確認

・誘導対策（アンテナからの電磁誘導影響への対策）
・耐震対策
・耐雷対策
・防火対策

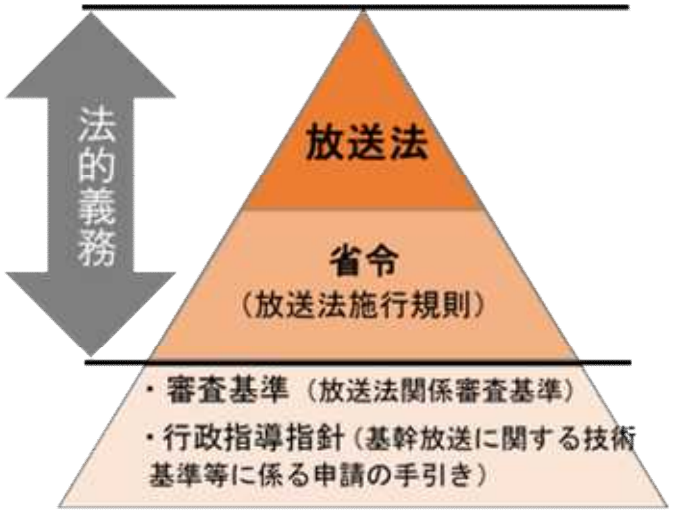
・屋外設備
・収容する建築物
・停電対策
・宇宙線対策
・サイバーセキュリティの確保【追加】

- 今般、この技術基準にサイバーセキュリティの確保の規定を追加

○ 条文イメージ

放送設備又は当該放送設備を維持若しくは運用するために必要な設備は、当該放送設備によって行われる放送の業務に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（サイバーセキュリティ基本法第２条に規定するサイバーセキュリティをいう。）の確保のために必要な措置が講じられていなければならない。

※ 措置の具体的な内容については、放送法関係審査基準にその具体的措置を例示し、事業者ごとの対策内容を確認。



経済産業省

資料２－２

経済産業省におけるサイバーセキュリティ対策強化のための各種取組

経済産業省　商務情報政策局
サイバーセキュリティ課

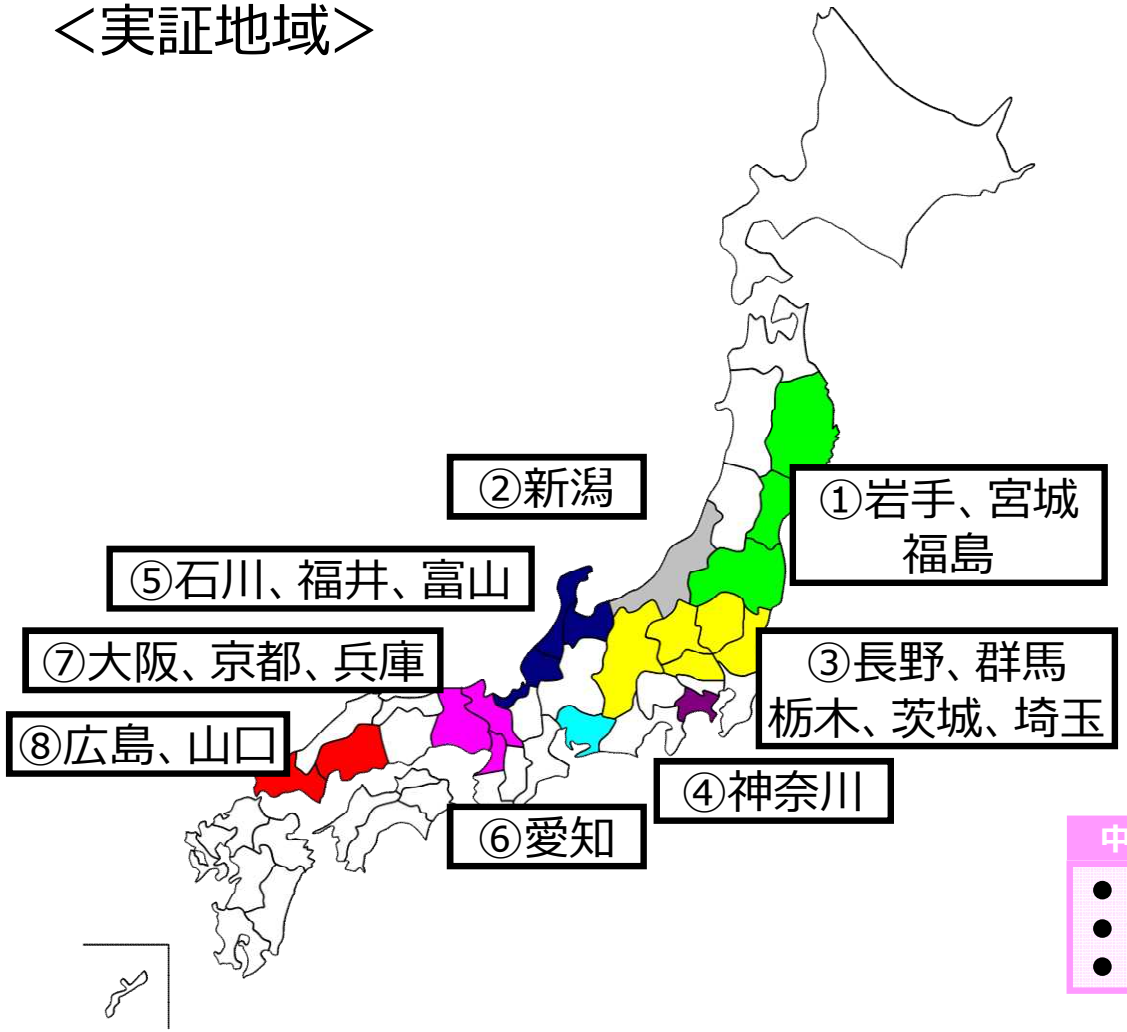
１．サイバーセキュリティお助け隊実証事業

２．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

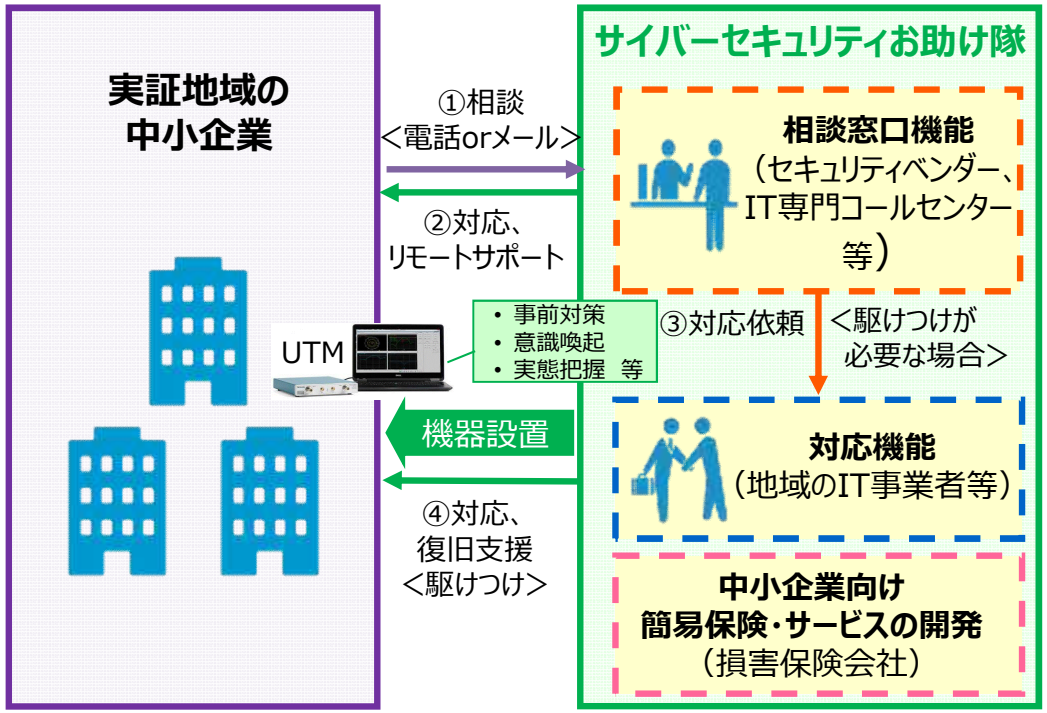
1．サイバーセキュリティお助け隊実証事業

- 全国**8地域**において、地域の団体、セキュリティ企業、保険会社がコンソーシアムを組み、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした**実証事業**を実施。
- 本事業により、中小企業の事前対策の促進や意識喚起、攻撃実態や対策ニーズの把握を行い、**民間による中小企業向けのセキュリティ簡易保険サービスの実現を目指す。**

＜実証地域＞



＜実証のイメージ＞



実証結果

中小企業　側

- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上　　等

保険会社、セキュリティベンダー　側

- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握　　等

（参考）サイバーセキュリティお助け隊コンソーシアムリスト

地域名	実施主体	実施体制
宮城、岩手、福島	株式会社デジタルハーツ	**損害保険ジャパン日本興亜株式会社** 株式会社アライブ 地元関係団体多数
新潟	東日本電信電話株式会社	**東京海上日動火災保険株式会社** 東京海上日動リスクコンサルティング株式会社
長野、群馬、栃木、茨城、埼玉	富士ゼロックス株式会社	**東京海上日動火災保険株式会社**
神奈川	SOMPOリスクマネジメント株式会社	**損害保険ジャパン日本興亜株式会社** 日本PCサービス株式会社 株式会社コムネットシステム 株式会社サイバーセキュリティクラウド 株式会社ラック 学校法人岩崎学園
石川、福井、富山	株式会社PFU	アイパブリッシング株式会社 **損害保険ジャパン日本興亜株式会社**　金沢支店 北陸先端技術大学院大学 PFU西日本株式会社
愛知	MS&ADインターリスク総研株式会社	**三井住友海上火災保険株式会社** **あいおいニッセイ同和損害保険株式会社** NTTアドバンステクノロジ株式会社 綜合警備保障株式会社 デロイトトーマツサイバー合同会社
大阪、京都、兵庫	大阪商工会議所	**東京海上日動火災保険株式会社** 日本電気株式会社 キューアンドエー株式会社
広島、山口	株式会社日立製作所	**損害保険ジャパン日本興亜株式会社** SOMPOリスクマネジメント株式会社 株式会社日立システムズ 広島県情報産業協会

サイバーセキュリティお助け隊　今年度実証事業の状況①

- 多くの中小企業に参加いただき、駆けつけ事例も発生している状況。

受託事業者	地域	参加 中小企業数
株式会社デジタルハーツ	宮城県、岩手県、福島県	111
東日本電信電話株式会社	新潟県	148
富士ゼロックス株式会社	長野県、群馬県、栃木県、茨城県、埼玉県	112
SOMPOリスクマネジメント株式会社	神奈川県	150
株式会社PFU	石川県、富山県、福井県	120
MS&ADインターリスク総研株式会社	愛知県	201
大阪商工会議所	大阪府、京都府、兵庫県	112
株式会社日立製作所	広島県、山口県	110

計**1,064**社
の
中小企業が
参加

(2020年1月10日時点)

お助け隊で観測されたサイバー攻撃の実例

お助け隊設置のUTMが不審な通信を観測。ボットネットへの通信が疑われた。
原因は、従業員がマルウェア感染が疑われる**私物のスマートフォン**を社内の無線アクセスポイントに接続したこと。
お助け隊が**駆けつけ対応を実施し、対処した**。

お助け隊による対処が行われず放置した場合・・・
スマートフォンに感染しているマルウェアがWi-Fiを経由して社内LANに侵入し、社員全員の業務用PC全25台に感染、業務停止や機密情報が漏洩する事態が考えられた。
この場合の保険会社算出の被害想定額※は、

約**4,925万円**

※初動対応、調査対応、復旧費用、事業停止による損失等。

出典：MS&ADインターリスク総研株式会社　2019年10月16日「サイバーセキュリティお助け隊実証事業（愛知県）」中間報告会資料

サイバーセキュリティお助け隊　今年度実証事業の状況②

- 全国８地域合計でインシデントが48件既に発生しており、そのうち駆けつけ対応が17件発生している状況である。（12/6時点）

＜コールセンター稼働及び駆け付け支援状況＞

対応種別	総数	アラート種別	発生件数
コールセンター対応	545件	実証参加に関する問い合わせ	125件
		セキュリティ機器設置等の問い合わせ	294件
		セキュリティ対応の相談	70件
		その他	56件
インシデント等対応	74件	**電話およびリモートによるインシデント対応**	**31件**
		訪問によるインシデント対応	**17件**
		機器設置等のトラブル対応	22件
		その他	4件

令和２年度事業概要

- 今年度事業で明らかになった中小企業の実態やニーズを踏まえつつ、次年度も「サイバーセキュリティお助け隊」の実証事業を各地で実施予定。

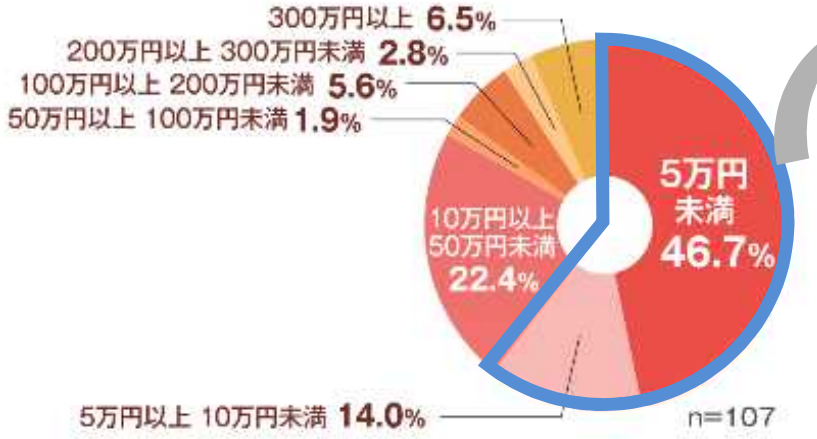
今年度事業で明らかになった課題等	次年度事業の方針
マーケティングには地域特性、産業特性等の考慮が必要	**地域特性や産業特性等を一定程度考慮した単位**での実証
無償の実証事業でも参加の必要性を感じない中小企業が多い	今年度事業で明らかになった各地域の攻撃実態等のデータ等を用い、参加募集説明会等を通じて**各地で普及啓発を実施**
実証事業に参加したくても、人手不足により、機器設置等に対応できない	セキュリティサービスの**導入・運用負荷を下げる**方法を検討
同規模サービスを有償提供する場合、年間10万円以下での提供は厳しい	**サービス内容のスリム化、事前サービス等とのセットによるリスク低減**方法を検討

（参考）中小企業の実態調査結果

- 中小企業の中でも比較的サイバーセキュリティ意識の高いSECURITYACTION宣言企業やお助け隊参加企業でも、セキュリティ対策にかける費用について非常にシビアであるのが実態。

＜SECURITYACTION宣言企業へのアンケート調査＞

Q13 情報セキュリティ対策費はどれくらいかかりましたか？
（ひとつだけお選びください）※貴社・貴団体の職員の人件費は含まず、セキュリティ対策ソフト等の導入や社外の専門家に支払った費用等



サイバーセキュリティの意識が高い中小企業でも年間10万円もかけられない。

- セキュリティアクション宣言企業の60.7%が、「セキュリティ対策に掛けた費用は10万円未満」と回答。

出典：2018年3月2日東洋経済新報社 SECURITY ACTION実態調査結果

＜お助け隊説明会@大阪で実施したアンケート結果（n=69社）＞

Q.サイバーセキュリティ対策に年間どれくらい経費をかけていますか？
（正社員情シス担当者の人件費除く）

5万円以内	31
6～10万円	10
11～15万円	7
16～20万円	2
21～50万円	5
51～100万円	2
101万円～	4

Q.お助け隊サービス（有償サービスとなった場合）に年間いくらなら出せますか？ ※アンケート結果を月額から年額へ換算

1.2万円未満	3
2.4万円未満	7
3.6万円未満	11
4.8万円未満	5
6.0万円未満	24
7.2万円未満	4
8.4万円未満	0
8.4万円以上	3

（参考）中小企業向けサービスの開発状況

- お助け隊受託事業者の中から中小企業向けのサービスが開発され始めている。

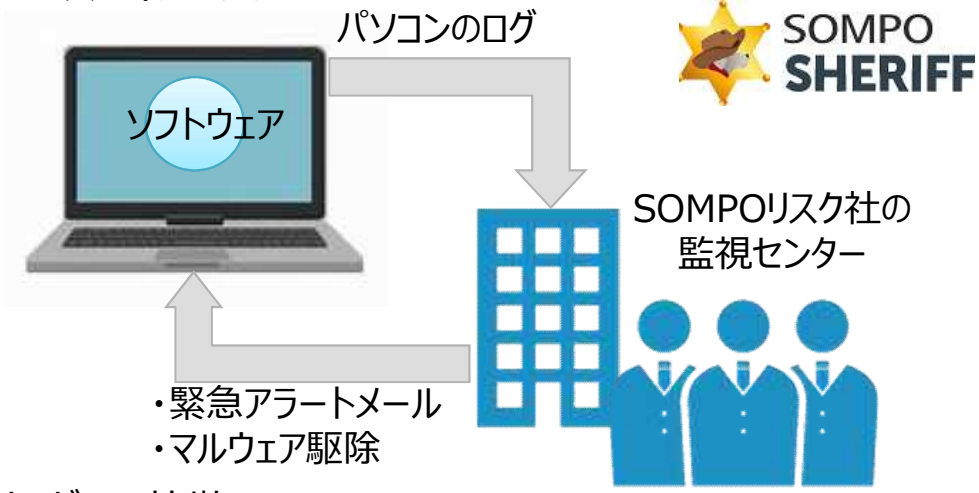
例）SOMPOリスクマネジメント社の新サービス「SOMPO SHERIFF」

同社が神奈川県での実証事業で感じた中小企業の課題

通信機器を設置する作業において、中小企業では自社の社内ネットワークの状況が分かる人がいないことが多く、設置作業が難航。

- 新サービス「SOMPO SHERIFF」では、顧客企業が保護したいパソコンに専用ソフトウエアをインストールするだけで利用できるようにした。
- パソコンのログを収集し、監視センターに送る仕組みのため、ソフトの動作設定など顧客側の負担になる作業はほぼ発生しない。

＜サービスのイメージ＞



＜サービスの特徴＞

運用
監視センターから遠隔でマルウェアを検出、早期駆除

導入
ソフトウェアをインストールするだけ

コスト
初期費用35,000円、月額1台あたり1,800円(税抜)

保険
サイバー保険を自動付帯

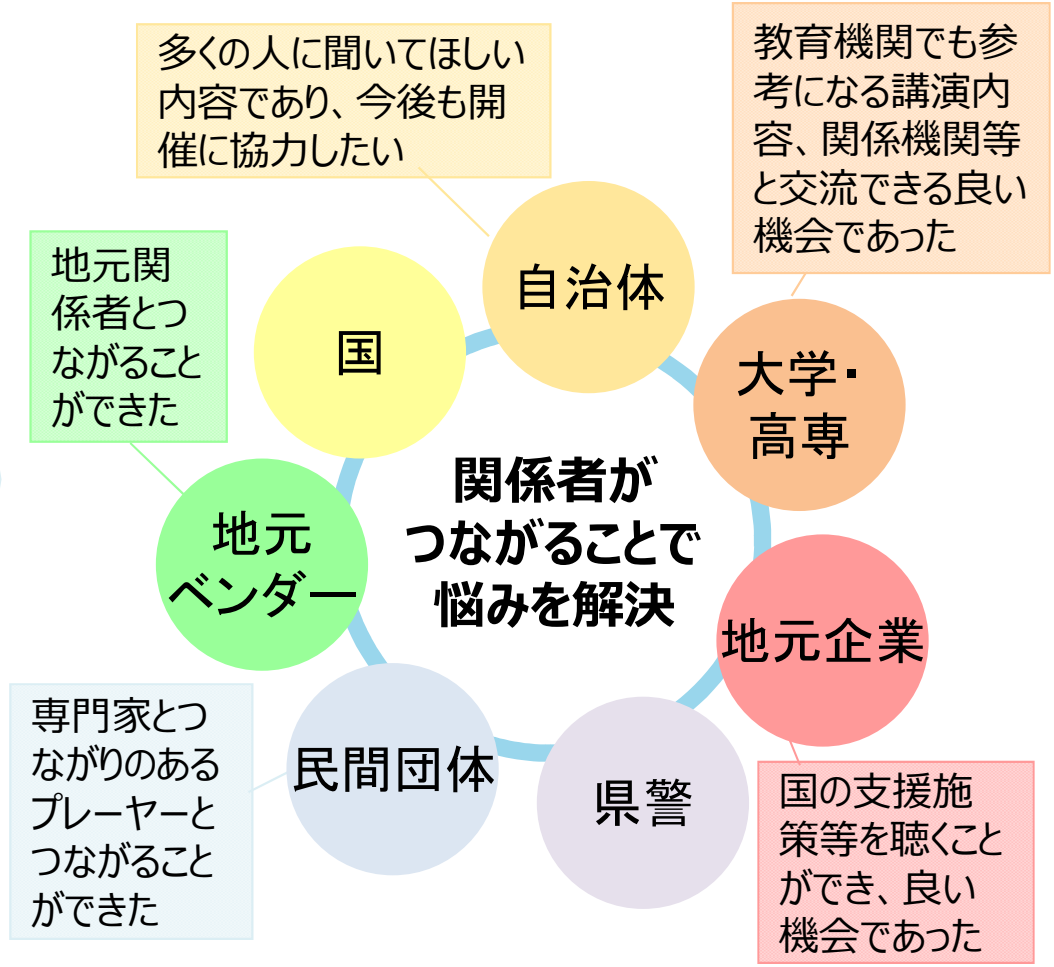
出典：SOMPOリスクマネジメント株式会社の2019年11月21日ニュースリリースを基に経済産業省で作成

2．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＞



（参考）ニーズとシーズをマッチングする『コラボレーション・プラットフォーム』

- ニーズとシーズをマッチングする“場”となる『**コラボレーション・プラットフォーム』をIPAに設置し、2018年6月から活動を開始**。2019年12月までに12回開催。

（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

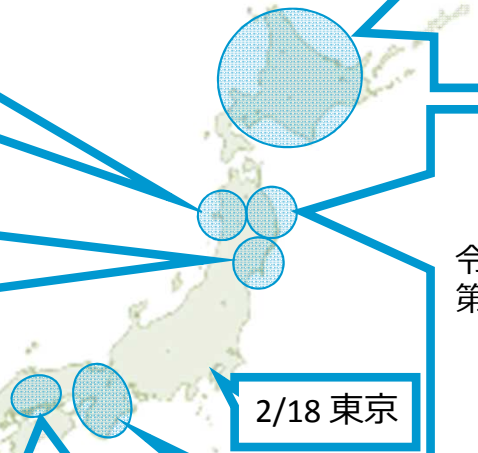
（東北経産局、IPA、秋田県、
秋田デジタルイノベーション推進コンソーシアム）

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



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

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）

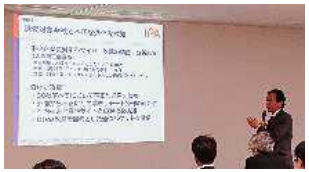
一般向けセミナー(令和元年9月)

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



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

地方版コラボレーション・プラットフォームの開催形態

- セキュリティコミュニティの中心になり得る団体は、**地域によって様々なパターン**（都道府県警、地方経産局／総通局、自治体、民間団体、高専等）が考えられる。
- 地域特性、中心的団体、物理的距離等も考慮しつつ、関係省庁等とも連携し、**地域・都道府県単位でのセキュリティコミュニティの形成を目指したい。**

＜想定される中心的な団体＞

➢ 地域の特性や既存の取組によって、セキュリティコミュニティの中心になる組織としては例えば下記が考えられる。

＜コミュニティの継続性に必要な条件＞

① **中心的団体の活動エリア単位での実施**
⇒ 中心的団体の活動エリアは地域単位・都道府県単位が多い

② **物理的距離の近さ**
⇒ 地域単位での集客が難しい地域もある
（例：青森-仙台間　車で約4時間半）

③ **地域特性に応じた内容**
⇒ 実施単位が小さい方が、地域特性を考慮しやすい

地域・都道府県単位での
セキュリティコミュニティ形成を目指す

必要と考えられる取組

- 全国各地で地域に根差したセキュリティコミュニティの形成を推進するために、以下の取組を開始する。

＜コミュニティ形成に必要な取組＞

①セキュリティコミュニティを形成するためのモデル及びプラクティスの共有

- 新たにコミュニティを形成する際にアプローチ先として想定される関係機関（自治体、商工団体、県警、大学 等）をリスト化。
- 他地域でのコミュニティの取組を参考にできるよう、各コミュニティのプラクティスを共通のフォーマットでとりまとめ、横展開。
- 課題なども共有することで、ソリューションを有するプレイヤーとの更なる連携を促進。

＜イメージ＞

②各地域に駆けつけ可能な専門家や、専門家派遣制度等の情報・問合せ先リストの作成・共有

- 連携できる可能性のある専門家やイベント（例．JNSA全国横断セミナー）、活用可能な制度（例．IPAセキュリティプレゼンター制度）等の情報・問合せ先リストを作成・共有。

＜イメージ＞

活用可能な制度

組織名	担当部署	連絡先
IPA セキュリティプレゼンター	××課	XX-XXXX
IPA 講師派遣制度	○○課	XX-XXXX

セキュリティ専門家

組織名	氏名	連絡先	専門等
JUAS	○○	XX-XXXX	経営層向け
JPCERT	△△	XX-XXXX	最新攻撃事例