経済産業省

資料3

事務局説明資料

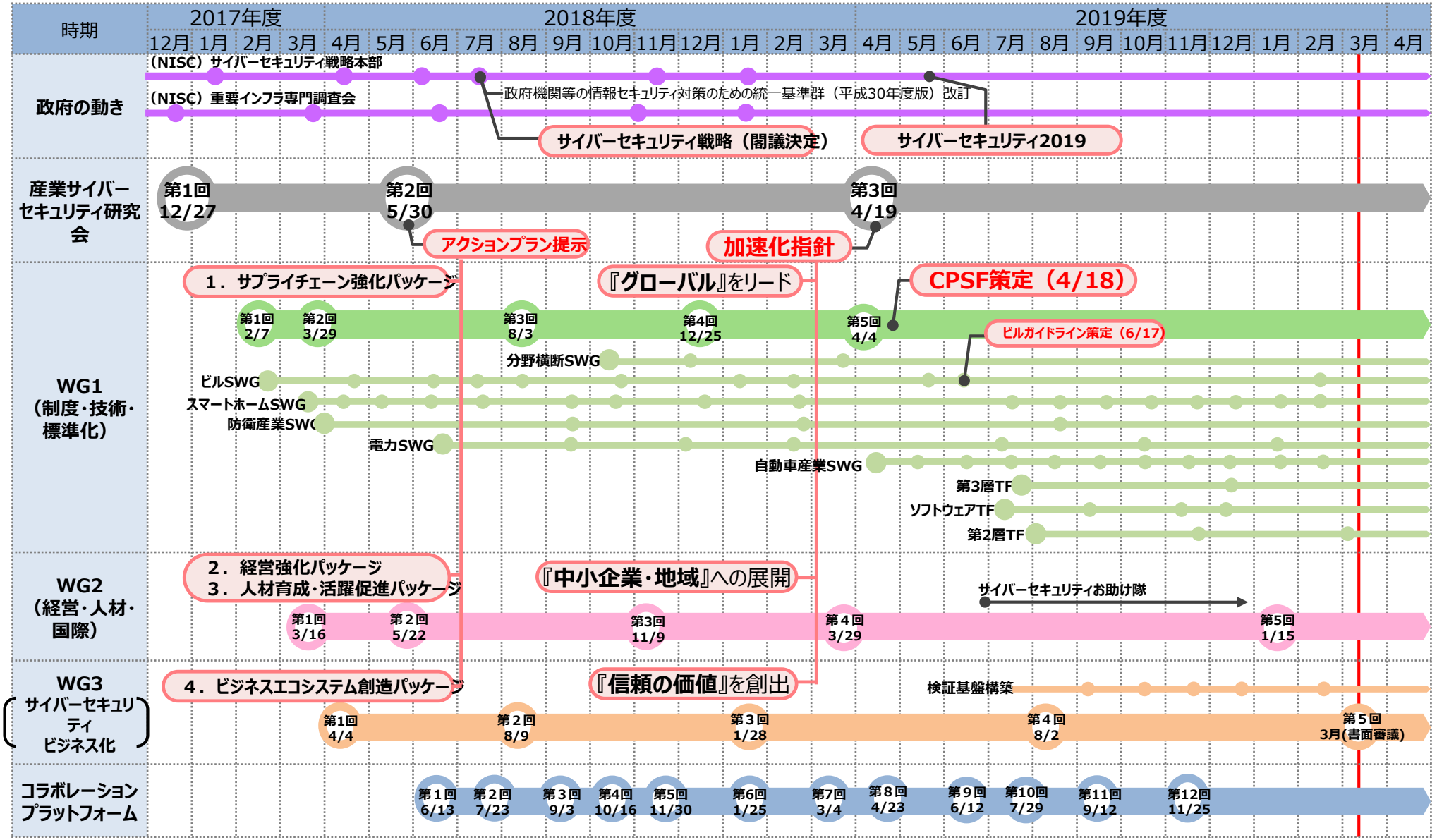
産業サイバーセキュリティ研究会WG3
（サイバーセキュリティビジネス化）
第５回

令和２年３月

経済産業省　商務情報政策局

サイバーセキュリティ課

産業サイバーセキュリティ研究会関連の動き



セキュリティのエコシステムを実現するための課題全体像

前回WG3資料の再掲

- 信頼できる製品・サービスと隠れたニーズを掘り起こし、ビジネスマッチングの場を提供することにより、セキュリティ産業の発展を目指す。

安心して製品・サービスを利用できる基盤を構築

1．Proven in Japan（検証基盤）

2．情報セキュリティサービス審査登録制度

3．セキュリティに関する契約の在り方の検討

&

隠れたニーズに対応したビジネスの創出

4．サイバーセキュリティお助け隊

5．中小企業向け製品・サービスの検証

市場への展開

ビジネスマッチング

6．コラボレーション・プラットフォーム

1．Proven in Japan（検証基盤）
2．情報セキュリティサービス審査登録制度
3．セキュリティに関する契約の在り方の検討
4．サイバーセキュリティお助け隊
5．中小企業向けセキュリティ製品の検証
6．コラボレーション・プラットフォーム

包括的なサイバーセキュリティ検証基盤を構築し、『Proven in Japan』を促進

研究会資料の再掲

- 「Proven in Japan」では、2つの方向を追求し、**セキュリティビジネスの成長を促進**。

① 有効性確認等を通じ、日本発のサイバーセキュリティ製品のマーケット・インを促進

② IoT機器等の信頼性を高度に検証するハイレベル検証サービスの拡大

1．セキュリティ製品の有効性検証

2．実環境における試行検証

3．攻撃型を含めたハイレベルな検証サービス

信頼できる
セキュリティ製品・サービス

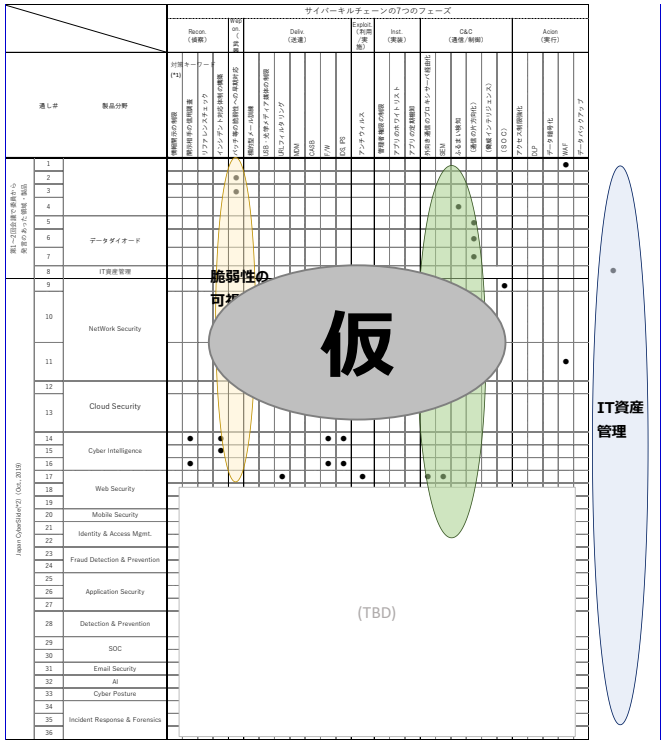
世界に貢献する
高水準・高信頼の検証サービス

緑 青

今年度の議論・検討の流れ

- 有識者会議を開催し、重要分野の選定、該当分野の製品の公募、検証作業を実施。
- 有効性検証、実環境における試行検証それぞれのアウトプットを取りまとめ、次回コラボレーション・プラットフォームで発表する。

有識者会議でセキュリティ領域の全体マップを作成し、**重要分野**を選定（市場性、日本発の製品が強味を発揮可能か等の観点から）



重要分野に該当する**製品を公募で選定**
有効性評価、実環境における試行**評価を実施中**

有効性検証 → 検証環境

yamory
（OSSの脆弱性可視化）
VISIONAL

お試し製品提供と検証 → 実環境

AX-Network Visualization
（ネットワーク脅威可視化）
AlaxalA

第13回コラボレーション・プラットフォームで発表、**ビジネスマッチング**を実施する。

日本発製品・サービスのプロモーションに資するため、主に以下の内容を公表する。

有効性検証

製品のストロングポイント

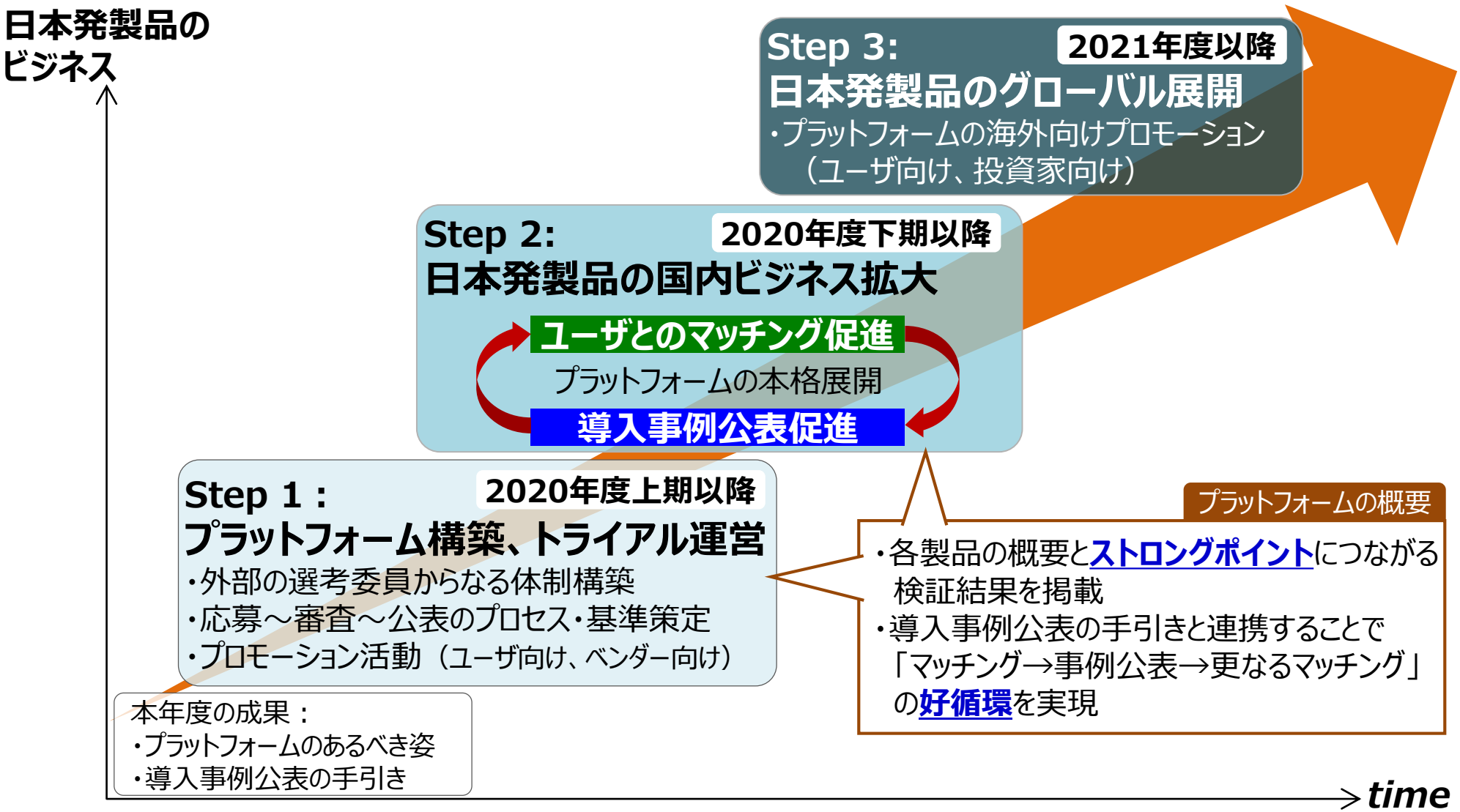
実環境における試行検証

導入事例公表の手引き

骨子(案):
- 公表のメリット／デメリット
- 公表可否判断のポイント
- 公表内容
- ステークホルダーとの調整 等

来年度以降方針

本年度の成果を基に、マッチングプラットフォーム構築、日本発セキュリティ製品の国内ビジネス拡大、更に海外展開を目指す。



赤

Society5.0時代の信頼性確保のために必要となる攻撃型手法を含むハイレベルな検証サービスの普及展開へ向けた実証

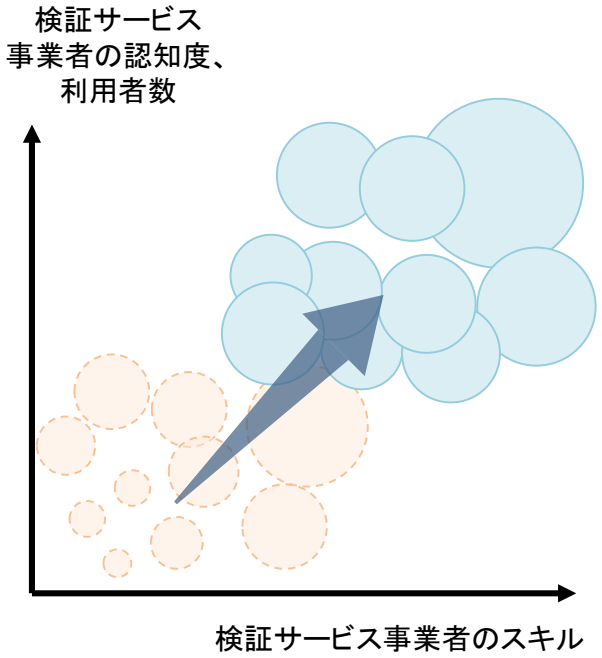
- 2019年度は、IoT機器等についてホワイトハッカー等を有する実力のある検証事業者による攻撃的手法を含むハイレベルな検証を通じて、信頼できる事業者を確認する仕組みや、事業者と利用者間のコミュニケーション、機器ごとの効果的な検証手法等の考え方を第一弾の**手引きとして整理**。
- 2020年度は、昨年度実施した機器とは異なる機器を対象として事業を実施すると共に、将来的に検証事業に活用でき得る技術等に関する調査を通じて、手引きの充実を図る。

検証事業者

検証

・IoT機器等
＜2019年度＞
ルータ、UTM、タブレット、スマートロック
＜2020年度＞
R1年度とは異なる機器

①様々な検証手法を用いた機器・システムごとの検証結果
→IoT機器等ごとに効果的な検証手法の考え方を整理
②検証事業者に求められる信頼性等の考え方の整理
→適切な情報管理を行う主体としての信頼性や、質の高い検証を行うことができる事業者としての信頼性について検討
③検証事業者と利用者間のコミュニケーション手法の整理
→検証サービスへの認知及び利用者の増加



手引きの概要

- 今年度作成中の手引きにおいては、検証サービスの高度化に向け、検証サービス事業者と検証依頼者の双方が参照する手引きを作成中。

手引きの目的・対象機器・対象者について

項目	概要
目的	• 検証サービス事業者のサービス高度化に向け、技術や情報管理等の観点において、信頼できる検証サービス事業者を判断するための基準を示すこと。 • 検証サービス事業者・検証依頼者間の共通言語となりうることを目的として、検証の準備段階で検証依頼者が伝えるべき情報や、検証結果の報告時に検証サービス事業者が伝えるべき情報など、二者が適切なコミュニケーションを行うための留意事項等を示すこと。
対象機器	• IoT機器をはじめとするネットワークに常時接続する機器、及びその関連サービス
対象者	• 機器検証を実施する検証サービス事業者 • 事業者に対して検証を依頼する者（機器の開発者やPSIRT担当者等）

手引きの目次（案）

章	項
1 背景と目的	1.1 背景
	1.2 本手引きの目的
	1.3 本手引きで対象とする機器
	1.4 対象者
	1.5 本手引きの構成
	1.6 本手引きの活用方法
2 機器検証とは	2.1 検証の目的
	2.2 一般的な検証手法
3 機器検証の実施	3.1 検証手順
	3.2 検証に向けた準備
	3.3 検証計画の策定
	3.4 検証実施
	3.5 検出における留意点
4 機器検証の報告	4.1 検証結果の分析
	4.2 検証結果の報告
5 付録	5.1 用語集
	5.2 参考文書

1．Proven in Japan（検証基盤）
2．情報セキュリティサービス審査登録制度
3．セキュリティに関する契約の在り方の検討
4．サイバーセキュリティお助け隊
5．中小企業向けセキュリティ製品の検証
6．コラボレーション・プラットフォーム

情報セキュリティサービス審査登録制度の概要

- **一定の技術・品質管理要件を定めた「情報セキュリティサービス基準」**を策定し、基準に適合するサービスのリストを2018年6月よりIPAが公開。

＜情報セキュリティサービスにおける課題＞

どの事業者のサービスを選べば良いか分からない

信頼できるサービス事業者にお願いしたい

ユーザ
（企業、政府機関等）

選定時に活用

我が社のサービスをもっと見つけて欲しい

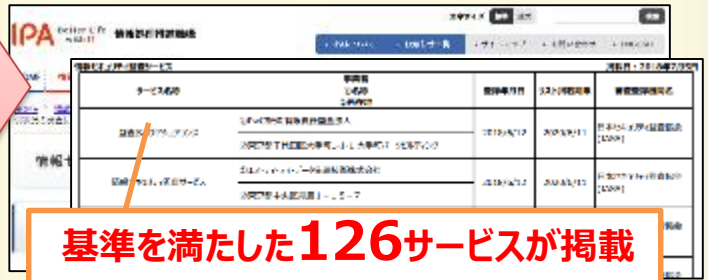
我が社の技術力、サービス品質をアピールしたい

ベンダー
サービス提供事業者

審査を受けてリストに掲載

○情報セキュリティサービス基準適合サービスリスト（IPA）

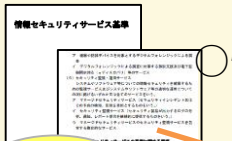
審査登録機関による審査で基準を満たすと認められたサービスをリストとして公開



基準を満たした126サービスが掲載

- 情報セキュリティ監査（27サービス）
- 脆弱性診断（50サービス）
- デジタルフォレンジック（19サービス）
- セキュリティ監視・運用（30サービス）

2020年1月現在



○情報セキュリティサービス基準（METI）

技術

品質

上記４サービスに関して技術要件・品質管理要件を定めた基準

本制度を通じて目指す社会

専門的知識を持たないユーザでも、自社に最適かつ品質を備えたサービスを選択できる

技術と品質を備えた情報セキュリティサービスの普及・発展

制度の普及・浸透

情報セキュリティサービス審査登録制度の今年度取組

- 2019年度は**制度の認知度向上と登録サービス数増加**を目指し、全国各地のセミナーでの制度紹介や個別ベンダへの働きかけ等を実施。登録サービス件数は**約170件**になる見込み（申請・審査中含む）。次回申請期間は3/23～。

今年度の取組

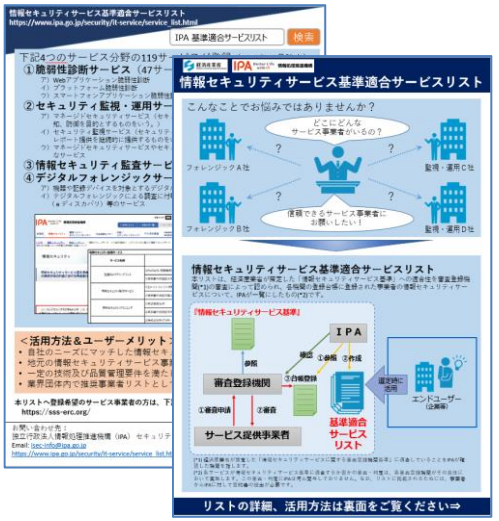
登録サービス数増加に向けた各種施策：

- 全国の**セミナーでの制度紹介**（50回程度）
- 業界団体や地方経産局等と連携して**個別ベンダへの周知実施**
- **制度紹介パンフレット**の作成・配布※
- 経産省**入札案件への引用**（ベンダーメリットの明確化）

制度の信頼性確保（昨年度から継続）

- リストに掲載されたサービスに対しての**サーベイランス実施**

※ユーザ向けパンフレット



＜参考＞登録ベンダーの所在地

- **情報セキュリティ監査**（27サービス）　**東京22**、京都1、広島1、埼玉1、神奈川2
- **脆弱性診断**（50サービス）　**東京40**、新潟1、兵庫1、大阪1、大分1、茨城1、神奈川5
- **デジタルフォレンジック**（19サービス）　**東京15**、兵庫1、神奈川1
- **セキュリティ監視・運用**（30サービス）　**東京23**、大阪1、大分1、神奈川5

⇒ **登録サービスの約８割が東京に集中。本制度を地方にも普及・浸透させるため、地方に所在するベンダーの登録数を増やす取り組みも続ける。**（特に、ユーザ環境での作業が必要になる情報セキュリティ監査と脆弱性診断）

情報セキュリティサービス審査登録制度の来年度方針

- 2020年度は、本制度の普及活動を引き続き実施するとともに、ユーザ・ベンダ双方への**活用状況・ニーズ調査**を実施し、対象サービスの追加等を検討していくことで、制度の更なる改善を図っていく。

＜来年度の取組＞

ユーザ調査

ユーザ
（企業、政府機関等）

- 制度の認知度、活用状況
- 情報セキュリティサービス活用における課題
- リストの改善要望

等

ベンダー調査

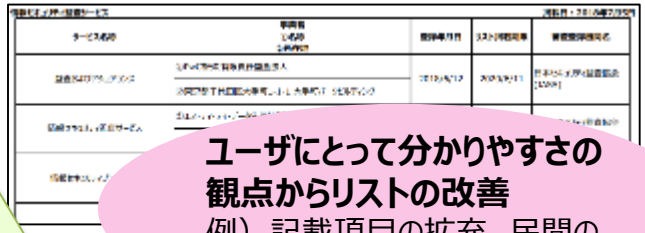
ベンダー
サービス提供事業者

- 制度の認知度、登録検討状況
- 登録によるメリットの明確化

等

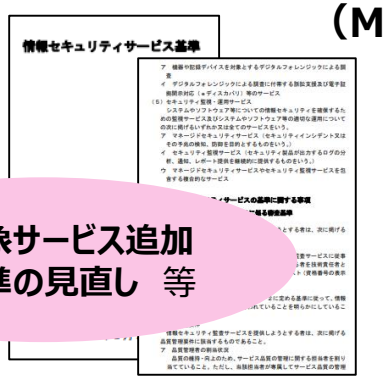
実地調査により、ニーズ視点で制度の改善

○情報セキュリティサービス基準適合サービスリスト（IPA）



ユーザにとって分かりやすさの観点からリストの改善
例）記載項目の拡充、民間のサービスリストとの連携　等

○情報セキュリティサービス基準（METI）



- **対象サービス追加**
- **基準の見直し**　等

（参考）情報セキュリティ監査企業台帳の廃止

- 情報セキュリティ監査の普及を図ることを目的とした情報セキュリティ監査企業台帳を**2020年3月末日をもって廃止**予定。
- 今年度をもっての台帳廃止については、本WG第３回会合（2019年1月28日開催）において了承され、同年3月25日に当省ホームページ※において周知済み。
- 今後は、より信頼性の高い情報を提供する**情報セキュリティサービス審査登録制度（情報セキュリティ監査サービス）が、当該台帳が担ってきた役割を代替**する。
- なお、システム監査企業台帳制度は、現状では同様の制度が存在しないことなどを踏まえ、来年度以降も継続し、その在り方について引き続き検討していく。

※https://www.meti.go.jp/policy/netsecurity/is-kansa/audit_is_list_notice.html

＜両制度の概要＞

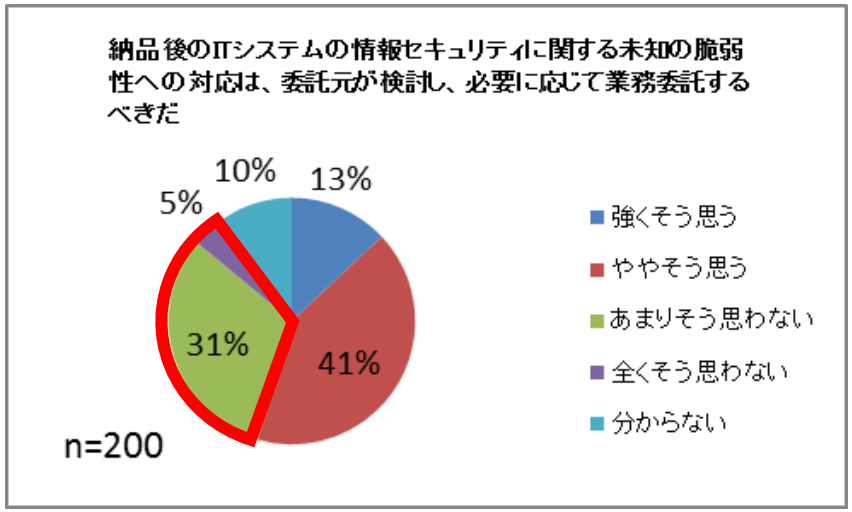
	情報セキュリティ監査企業台帳制度	情報セキュリティサービス審査登録制度（情報セキュリティ監査サービス）
根拠	情報セキュリティ監査企業台帳に関する規則（告示）	• 情報セキュリティサービス基準 • 情報セキュリティサービスに関する審査登録機関基準
目的	情報セキュリティ監査の普及	情報セキュリティサービス業の普及促進等
登録方法	申告書の提出（申告があれば原則掲載）	審査登録機関による情報セキュリティサービス基準への適合審査

1．Proven in Japan（検証基盤）
2．情報セキュリティサービス審査登録制度
3．セキュリティに関する契約の在り方の検討
4．サイバーセキュリティお助け隊
5．中小企業向けセキュリティ製品の検証
6．コラボレーション・プラットフォーム

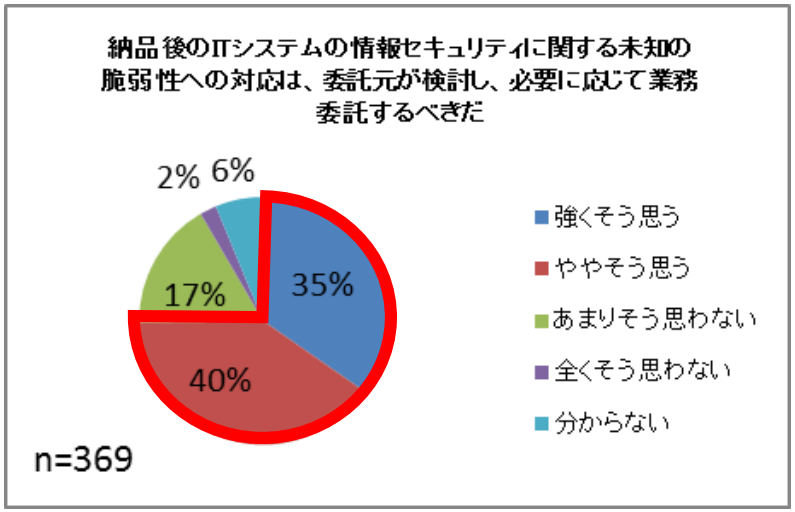
セキュリティに関する契約の課題

- 契約においてセキュリティの責任範囲が不明確であることが調査から明らかに。
  実際に訴訟問題に発展する事例も発生。

委託元の認識



委託先の認識



民法改正を踏まえた「情報システム・モデル取引・契約書」の見直しの検討と併せて、セキュリティについてもユーザ・ベンダ間でのセキュリティ仕様の検討プロセス、検討が必要と考えられる対応項目等について以下の場で検討中。

セキュリティ検討PT（民法改正対応モデル契約見直し検討WGの下に設置）：

第１回（2019/ 9/20） 検討の進め方等
第２回（2019/10/18） 論点についての議論（OSの標準機能を使った攻撃、クラウドのセキュリティ等）
第３回（2019/11/15） 論点についての議論（ソフトウェア・サプライチェーンでのセキュリティの確保等）
第４回（2019/12/20） 中間まとめ
第５回（2020/ 1/17） セキュリティ仕様策定プロセスに関する議論、スケジュール確認

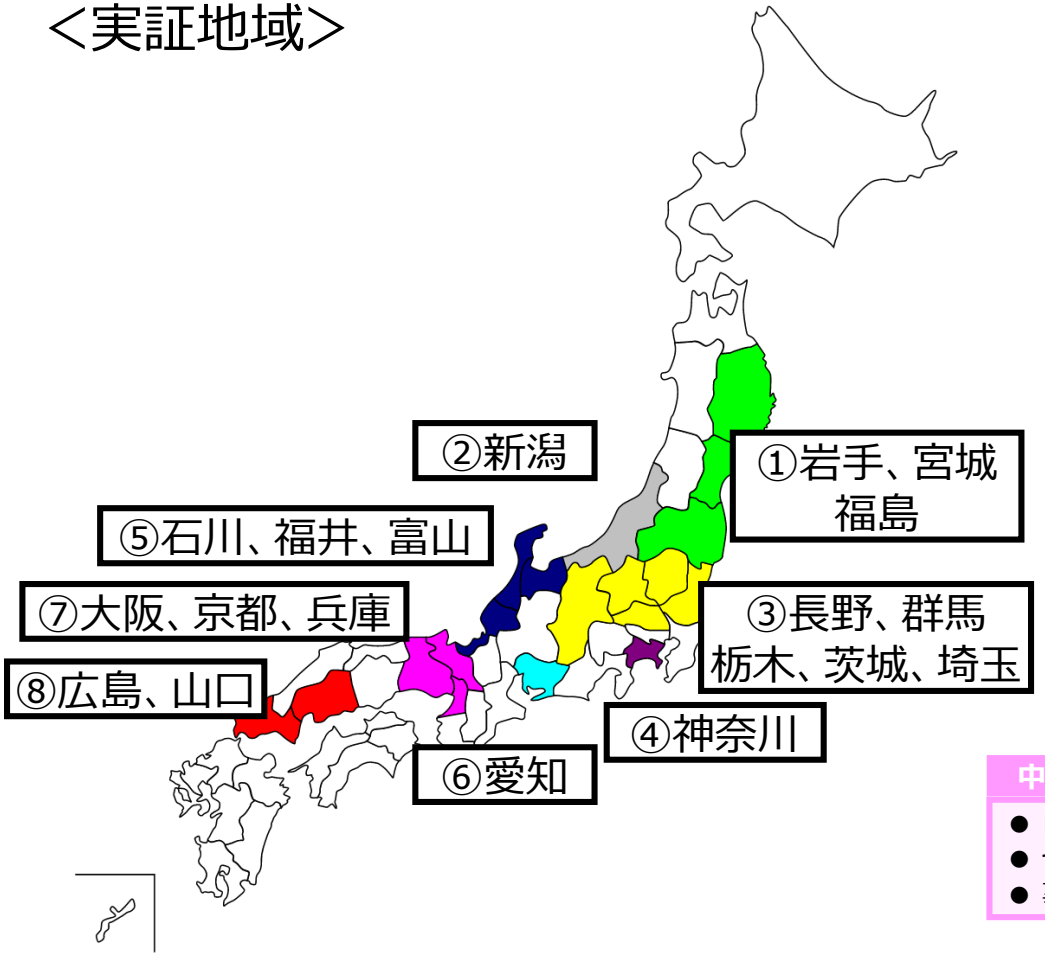
https://www.ipa.go.jp/ikc/about/committee-01.html

1．Proven in Japan（検証基盤）
2．情報セキュリティサービス審査登録制度
3．セキュリティに関する契約の在り方の検討
4．サイバーセキュリティお助け隊
5．中小企業向けセキュリティ製品の検証
6．コラボレーション・プラットフォーム

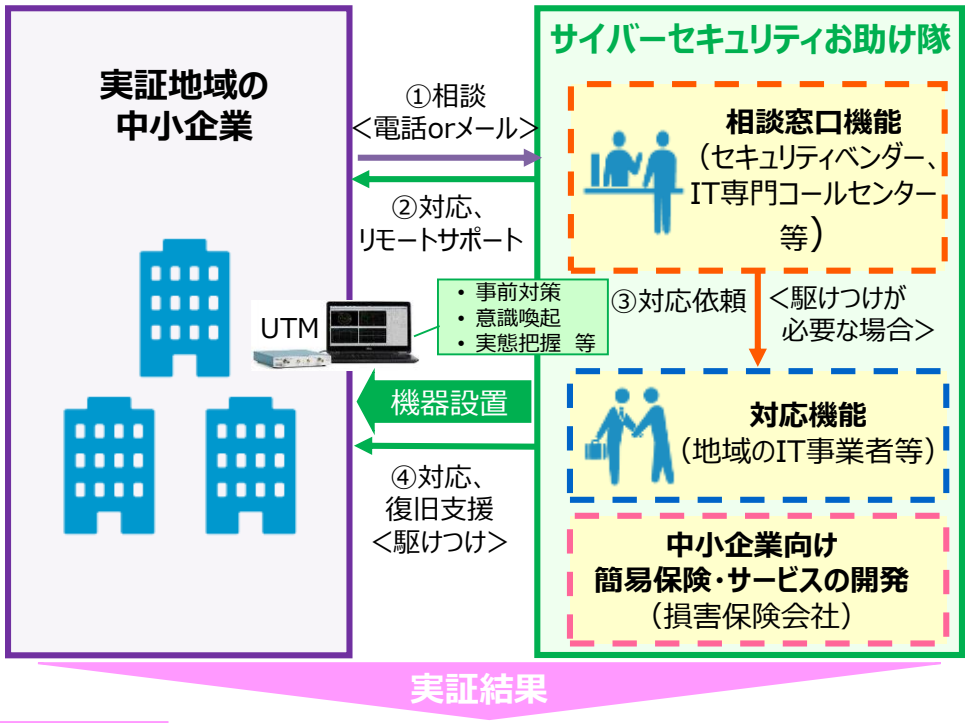
サイバーセキュリティお助け隊実証事業

- 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	参加 中小企業数
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	**111**
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	**148**
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**	**112**
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	**150**
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	**120**
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	**201**
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	**112**
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	**110**

計**1,064**社の
中小企業が参加

サイバーセキュリティお助け隊　今年度実証事業の結果

- 全国８地域でインシデント対応を計128件実施、そのうち駆けつけ対応は18件実施。

＜コールセンター稼働及び駆け付け支援状況（全国８地域合計／１月末時点）＞

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	741件	実証参加に関する問い合わせ	64件
		セキュリティ機器設置等の問い合わせ	432件
		セキュリティ対応の相談	113件
		その他	132件
インシデント等対応	196件	**電話およびリモートによるインシデント対応** ※	**110件**
		訪問によるインシデント対応	**18件**
		機器設置等のトラブル対応	19件
		その他	49件

※電話およびリモートによるインシデント対応には、訪問によるインシデント対応の一次対応を含む

＜駆けつけ支援例＞

事例１

お助け隊事業で設置のUTMで不審な通信を検知し、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**したことであった。駆けつけ支援を実施し、対処した。

お助け隊による対処が行われず放置した場合の被害想定額は約4,925万円※

※マルウェアが社内の全PCに感染し、業務停止や情報漏えいが発生した場合の初動対応、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

事例２

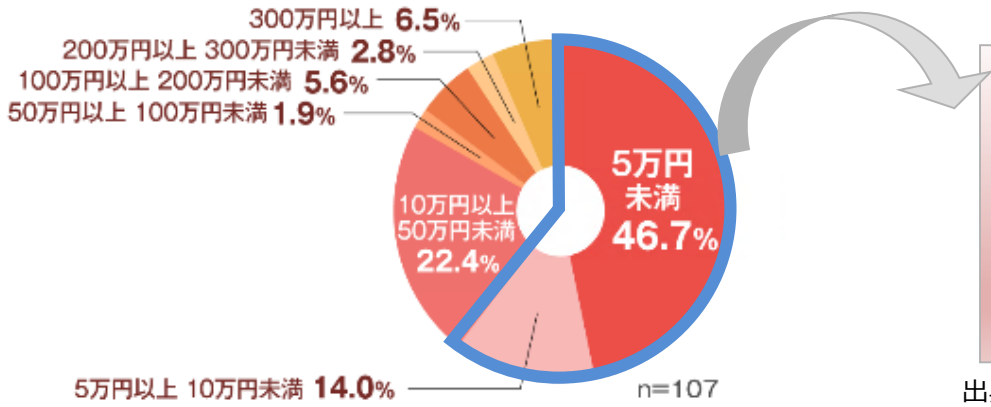
お助け隊の参加企業から送付されたなりすましメールをきっかけに、同企業の従業員の端末のEmotet 感染を確認。駆けつけ支援を実施し、対処した。なお、本件は、出張先ホテルの wifi 環境において感染したため、お助け隊事業で設置した監視センサーでは検知されなかった。

（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

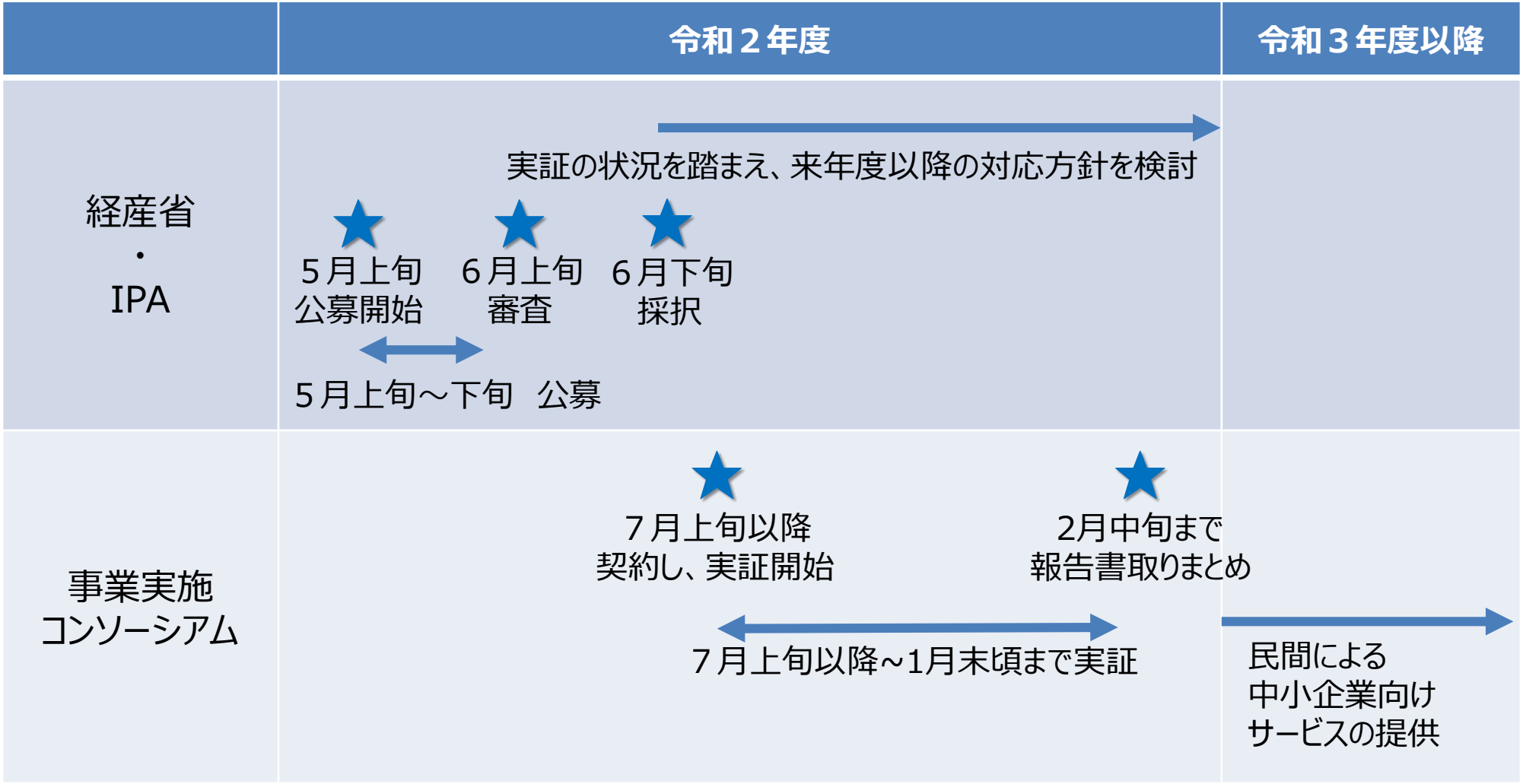
令和２年度事業概要

- 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

令和２年度事業のスケジュール（案）

- 令和２年度もIPAが事務局となり、５月上旬より公募開始予定。



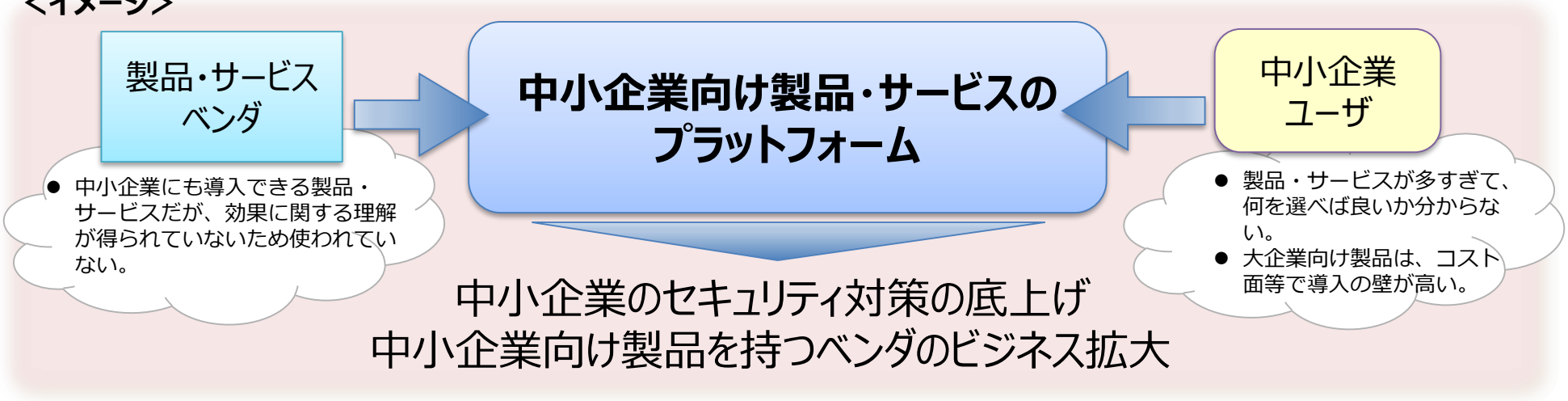
1．Proven in Japan（検証基盤）
2．情報セキュリティサービス審査登録制度
3．セキュリティに関する契約の在り方の検討
4．サイバーセキュリティお助け隊
5．中小企業向けセキュリティ製品の検証
6．コラボレーション・プラットフォーム

中小企業向けセキュリティ製品・サービスの検証事業

前回WG3資料の再掲

- 市場に流通しているセキュリティ製品・サービスは、中小企業から見て過度に高機能、運用コストが高い等、中小企業のニーズにマッチしていないとの声がある。
- 中小企業をターゲットとしたセキュリティ製品・サービスが、真に中小企業のニーズにマッチしているか検証することで、中小企業向け製品のビジネスの確立を促し、中小企業のセキュリティ対策の底上げを図る。

<イメージ>



検証対象製品・サービスが満たすべき要件

- 大規模なシステム改修を伴わず**実装が容易**であること（導入のし易さ）
- 社内に専門人材がいなくても使えること（**運用のし易さ**）
- 導入時や運用時の**コストが安価**であること

今年度の検討経緯と評価結果サマリ

- 有識者による検討委員会を開催し、評価項目のたたき台作成、トライアルに協力するベンダーの公募と選定、ユーザ環境への製品導入・運用を実施。
- ユーザ及びベンダーへのヒアリング結果をまとめ、評価項目(案)を作成した。

公募でベンダー３社選定

イージス株式会社
EDR+EDR運用サービス「セキュリティドクター」

NTTコミュニケーションズ株式会社
・簡易**SOC**サービス「セキュリティサポートデスク」
・**エンドポイント**セキュリティ「マイセキュアビジネス」
・**クラウド**アプリセキュリティ「Cloud App Security」

株式会社Blue Planet-works
エンドポイントセキュリティ
「AppGuard Enterprise」「AppGuard Solo」

実ユーザ環境に導入・運用

Ａ社（**製造業、45名**）
Ｂ社（**製造業、15名**）
Ｃ社（**SI業、121名**）
Ｄ社（**ガス供給業、158名**）
Ｅ社（**NI業、18名**）
Ｆ社（**卸売業、14名**）

各社2回ずつヒアリング

評価項目(案)と、中小企業向け情報提供のポイント

ユーザが特に重視する評価項目

・導入及び運用のコスト
・製品性能の客観的な根拠
・オールインワン
・未知の脅威への対応　等

中小企業向けに情報を提供する際のポイント

・ユーザ目線の解説情報
・掲載情報の信頼性確保
・自社のニーズにマッチした情報を検索可能 等

中小企業向けセキュリティ製品・サービスに関する評価項目(案)

- 中小企業ユーザ６社のヒアリング結果から、評価項目(案)を作成した。
- 今後、各項目のユーザ目線でのブラッシュアップや重要度に応じた優先度付け等を行い、中小企業の適切な製品選定をサポートするものに仕立てる。

評価項目の観点		詳細な評価項目	
1	導入のし易さ	1.1	大規模なシステム改修の必要性がない
		1.2	必要となる機能を自由に選択することができる
		1.3	インストールや設定の手間を省くことができる
		1.4	必要最小限の知識で簡単にインストールや設定を行うことができる
		1.5	PCのシステムパフォーマンスへの影響が最小限である
		1.6	PCにインストール済みのソフトウェアへの影響が最小限である
		1.7	本格的に導入する前に、有償、無償を問わず、お試し利用ができる
		1.8	導入に関してのサポート対応がある
2	運用のし易さ	2.1	運用に関しての専門的な知識の習得の必要性がない
		2.2	さまざまな状況に応じた適切なサポートツールが充実している
		2.3	問合せ・相談窓口を設置している
3	導入時や運用時に要する費用	3.1	導入コストが安価である
		3.2	運用コストが安価である
4	導入や運用における課題の解決	4.1	製品・サービスの性能・スペックについて、客観的な根拠が明示されている
5	製品・サービスのセキュリティ性能	5.1	既知の脅威・インシデントに対応することができる
		5.2	未知の脅威・インシデントに対応することができる
		5.3	ユーザ側の人為的なミスや内部不正による脅威・インシデントに対応することができる
		5.4	サービス提供者側の悪用等の悪意がある行動を防止することができる
6	製品・サービスに付帯するオプションサービス等	6.1	サイバー保険等の補償サービスの利用ができる
		6.2	リスク評価(リスクアセスメント)やコンサルティング等のサポートサービスの利用ができる
		6.3	インシデント対応等の緊急対応サービスの利用ができる
		6.4	勤務時間外対応のサポートサービスの利用ができる

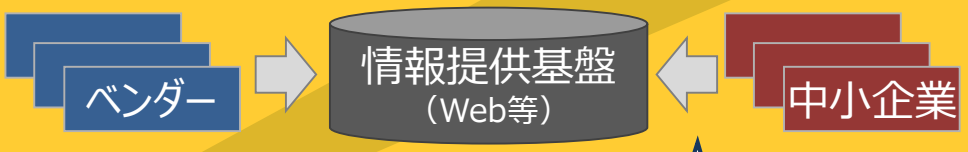
来年度以降方針

本年度の成果を基に、中小企業向けセキュリティ製品の特長等の情報を、中小企業に対し、分かりやすく信頼性の高い状態で提供する仕組みを構築することで、中小企業向けビジネスの拡大及び中小企業のセキュリティ対策底上げを目指す。

・中小企業向け製品のビジネス
・中小企業のセキュリティ対策

Step 3: **2021年度以降**
中小企業のセキュリティ対策底上げ
・サイバーセキュリティお助け隊、
SECURITY ACTION等の施策との連携

Step 2: **2020年度下期以降**
中小企業向けセキュリティ製品ビジネスの拡大
・参加ベンダー、利用ユーザ企業の本格募集



Step 1： **2020年度上期以降**
情報提供基盤の要件具体化と構築、トライアル運営
・評価項目のブラッシュアップ
・体制構築（事務局と評価会議）、ルール策定
・プロモーション活動（ユーザ向け、ベンダー向け）

情報提供のポイント
中小企業の適切な製品選定・導入を支援するための各種工夫
- 独自の解説情報の掲載
- インデックス付けによる容易な検索 等

本年度の成果：評価項目(案)、情報提供のあるべき姿・ポイント

time

1．Proven in Japan（検証基盤）
2．情報セキュリティサービス審査登録制度
3．セキュリティに関する契約の在り方の検討
4．サイバーセキュリティお助け隊
5．中小企業向けセキュリティ製品の検証
6．コラボレーション・プラットフォーム

コラボレーション・プラットフォームの開催状況

- サイバーセキュリティ対策に関する情報交流の場として2018年6月より開催開始。
- 各回、予定定員以上の申込みがあり、参加者からは政府との意見交換、最新動向の情報収集、人脈形成等、様々な視点で有益との声。

	開催日		参加人数(*)	テーマ
2018年	6月13日	第一回	179名（99名）	経済産業省の政策動向
		〜		
2019年	1月25日	第六回	108名（48名）	サイバー・フィジカル・セキュリティ対策フレームワーク
	3月4日	第七回	114名（42名）	IoTの製造現場のセキュリティ対策
	4月23日	第八回	97名（51名）	サイバーセキュリティ経営、検証基盤
	6月12日	第九回	133名（34名）	データ利活用
	7月29日	第十回	112名（42名）	クラウド
	9月12日	第十一回	98名（42名）	経済産業省の来年度政策
	11月25日	第十二回	127名（49名）	中小企業
	未定	第十三回	ー	検証基盤と中小企業向け製品検証

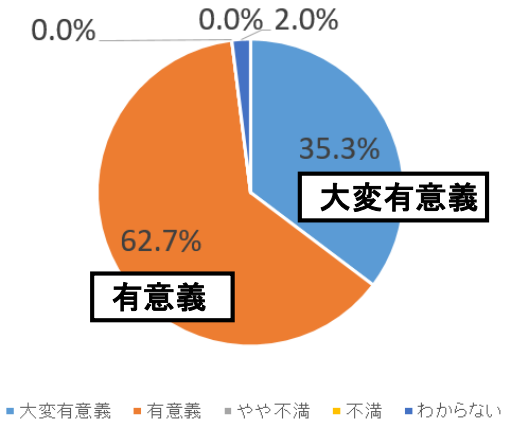
(*)括弧内の人数はコラボレーション・プラットフォーム後に開催した情報交換会の出席者数

富田理事長(IPA)ご挨拶

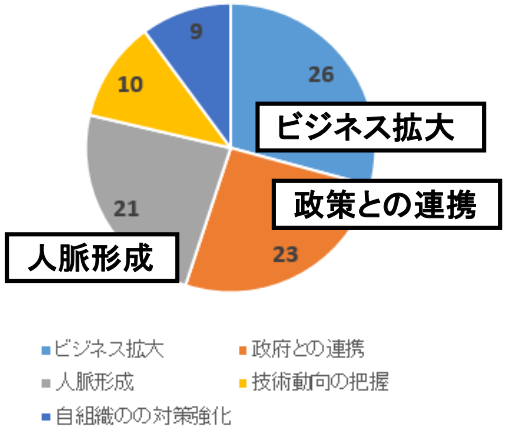
三角審議官(経済産業省)ご挨拶

グループディスカッション(第二回)

Q.コラプラの満足度は？



Q.コラプラに参加して良かったことは？



※第五回コラボレーション・プラットフォームアンケートより

（詳細はIPAのサイトを参照） https://www.ipa.go.jp/security/announce/collapla_index.html

コラボレーション・プラットフォームの目指す姿と来年度方針

- 業種・業界ごとのユーザニーズに対応する内容を検討する等の工夫をしつつ、様々なコラボレーションが行われる場を目指して来年度も継続開催していく。

コラプラの目指す姿

情報交換・交流の場

ビジネスマッチングの場
出会いの場

参加者からの意見を
政策に反映させる

2018年6月から**12回**開催し、各回**約100名**に参加いただいた。

来年度開催方針

【政策とのコラボレーション】

政策に関する意見交換の機会を設定し、**参加者からのご意見を着実に政策に反映**。

⇒政策紹介、グループディスカッション、情報交換会を通じて、意見交換を継続実施。

【シーズサイドのコラボレーション】

ベンダー企業間で連携を図り、**より大きなソリューションを市場に流通。**

⇒ベンダー、SIer等幅広い方々に参加いただき、参加者同士での連携検討を期待。

【ニーズサイドのコラボレーション】

ユーザ企業や大学等の間で課題を共有し、**セキュリティに関するニーズを具体化**。

⇒業界ごとのユーザニーズをプログラムに反映させるため、業界団体との連携等を検討。

【ニーズとシーズのコラボレーション】

ニーズサイドとシーズサイドの連携を図り、**ビジネスマッチング**につなげる。

⇒製品検証事業等の協力ベンダに登壇いただく等、ベンダ側とユーザ側とのパスとなるプログラムを検討。

（参考）次回コラボレーションプラットフォームの開催内容

- 次回コラプラでは、検証基盤構築（我が国発セキュリティ製品の有効性検証と実環境への試行導入）事業及び中小企業向け製品の検証事業について紹介するとともに、**今年度事業に協力いただいた製品を展示・紹介することで参加者とのマッチングの機会**を提供。

◆日時：未定
◆IPA（東京都文京区）

◆プログラム（予定）
14:00～14:05　開会挨拶（IPA）
14:05～14:20　検証基盤構築と中小企業向け製品検証事業の紹介（経済産業省）

14:20～14:50　＜緑青＞ベンダからの製品紹介（ユーザの声含む）
14:50～15:05　休憩
15:05～15:50　＜中小＞ベンダからの製品紹介とユーザの声
15:50～16:05　休憩

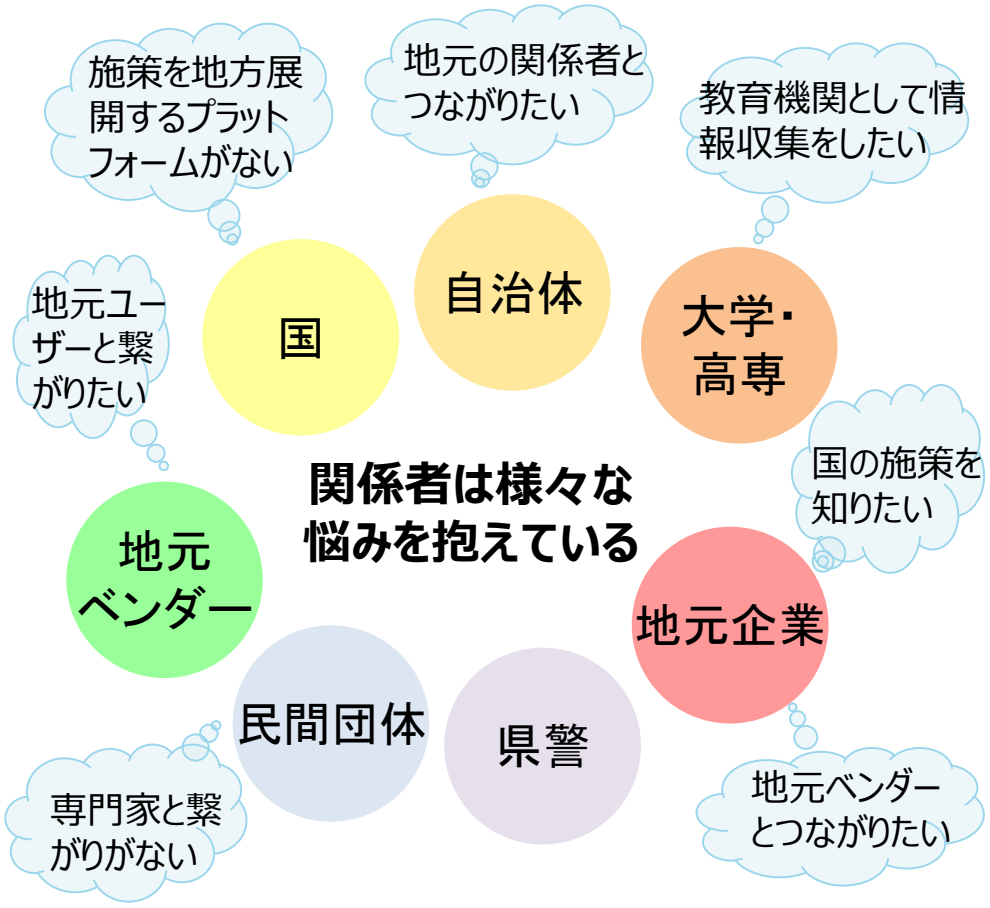
16:05～17:10　ブースでの展示　又は　グループディスカッション

17:30～　　情報交換会

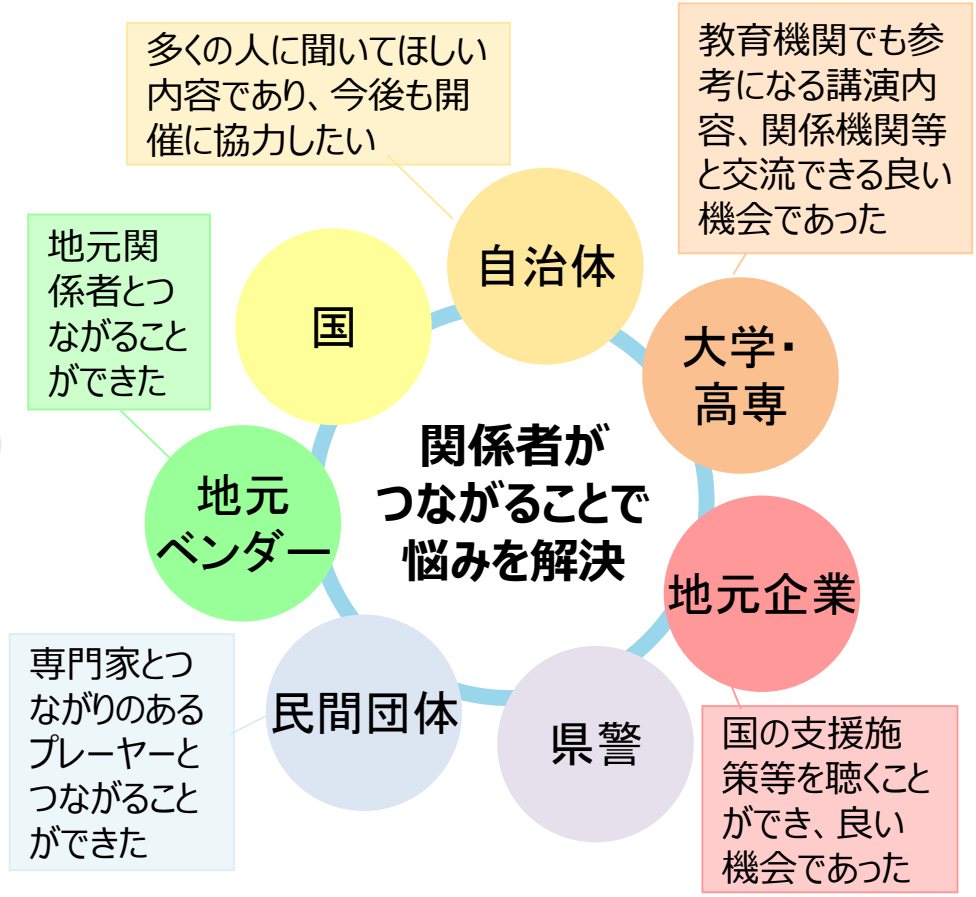
地方版コラボレーション・プラットフォームのコンセプト

- 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）各地域でのセキュリティ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、更に取組み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 岩手、秋田、宮城、青森

（東北経産局、IPA、MISEC※1、TiSA※2、自治体他）

令和元年10月に岩手にて地方版コラボレーション・プラットフォーム第１弾を開催。その後、秋田、宮城、青森で順次開催し、セミナーと合わせ懇親会、個別相談会や名刺交換会等を実施

岩手でのセミナーの様子

宮城でのセミナーの様子

青森でのセミナーの様子

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

関東サイバーセキュリティセミナー

（関東経産局、関東総通局、
一般社団法人テレコムサービス協会　関東支部）

令和2年に東京で関東総通局と連携し、初開催し、セミナーと合わせ名刺交換会を実施

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月に岡山、広島で開催

平成31年2月広島開催の様子

令和２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

地域に根付いたセキュリティコミュニティ形成の形態

- 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。

自治体

県警

地方経産局

大学・高専

地元民間団体

商工会議所

＜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

地域に根付いたセキュリティコミュニティ形成促進に向けた来年度の取組

- 全国各地で地域に根付いたセキュリティコミュニティの形成を促進するために、**「地域セキュリティコミュニティ形成促進のためのプラクティス集」の開発**や、**専門家派遣制度・団体等のリスト化**を行う。

＜来年度の取組＞

各地域の
セキュリティコミュニティの
プラクティス
をヒアリング調査

各地域に専門家を
派遣可能な制度・
団体等※を調査

※例えば、セキュリティプレゼンター制度や叶会等

インターネット等に掲載

「地域セキュリティ
コミュニティ
形成促進のための
プラクティス集」
を開発

※イメージ

専門家派遣
制度・団体等
を**リスト化**

各地域に専門家を
派遣可能な制度概要
及び
専門家・団体の
連絡先リスト

参照

新たにセキュリティコミュニティを形成する団体・
取組を拡充したいセキュリティコミュニティ等