経済産業省

資料3

事務局説明資料

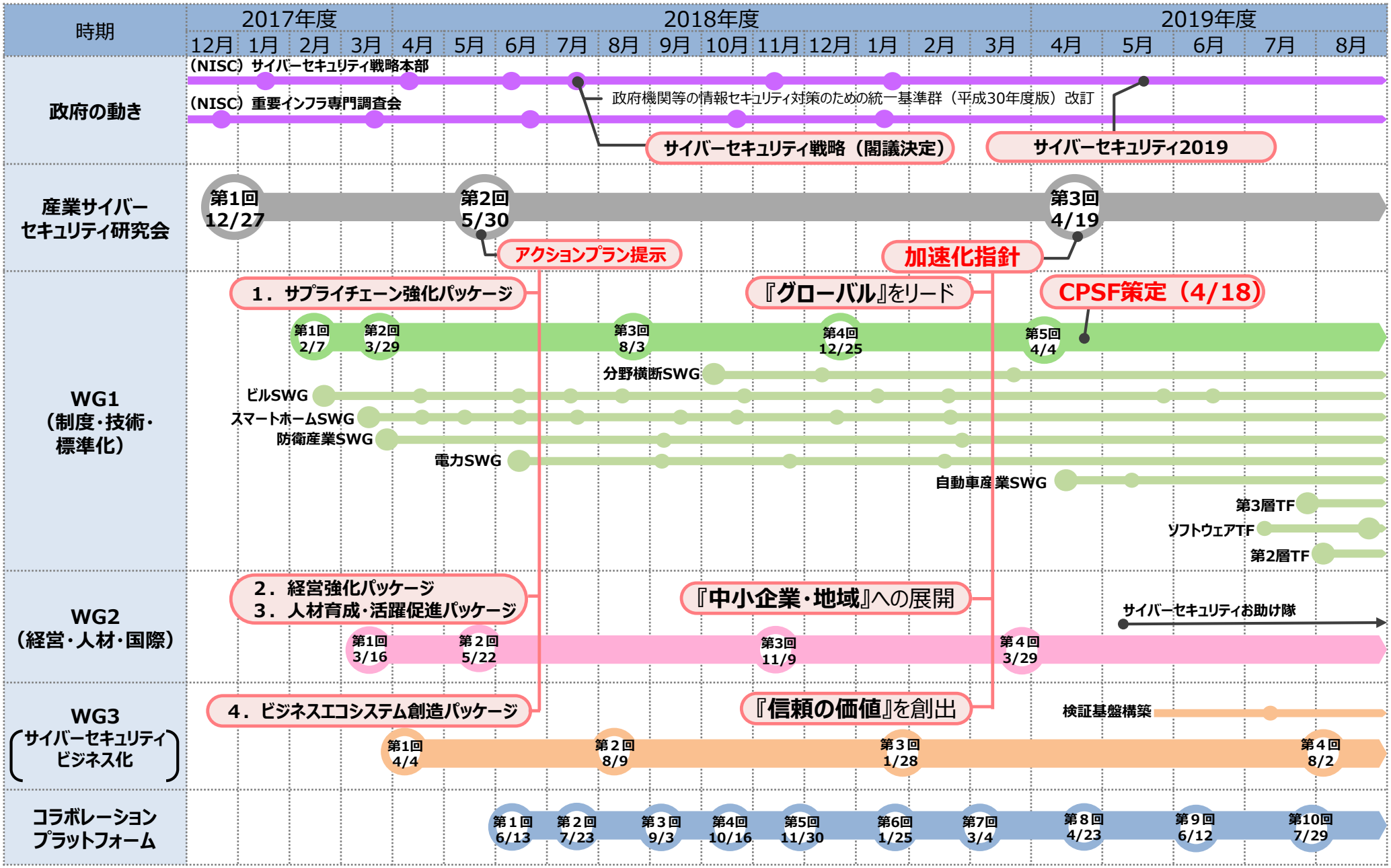
（産業サイバーセキュリティ研究会WG3
（サイバーセキュリティビジネス化）第４回）

令和元年8月2日

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

- 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**。

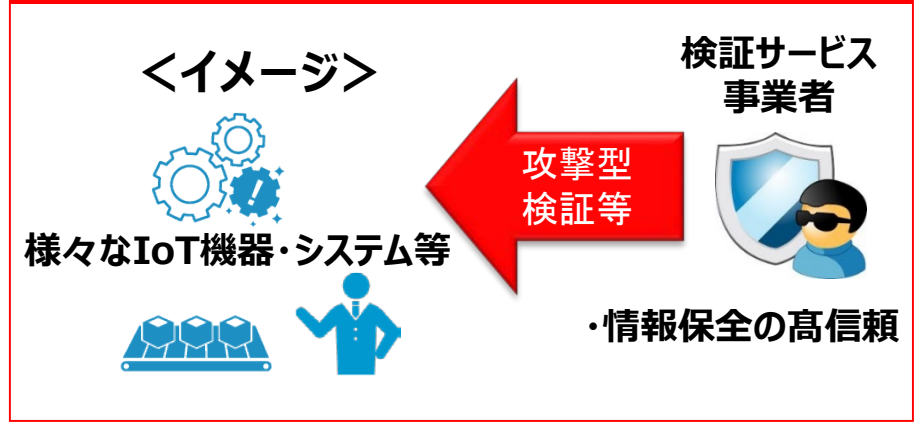
① 有効性確認等を通じ、日本発のサイバーセキュリティ製品のマーケット・インを促進

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

我が国発のセキュリティ製品の普及展開へつなげるため

研究会資料の再掲

重要分野のセキュリティ製品の有効性を確認し、発信する仕組みの構築

- 成熟したセキュリティ製品市場では、海外製の製品が高いシェア。
- **我が国発の新たなセキュリティ製品の市場参入を促進する**ため、サイバー攻撃の脅威や対策動向等を踏まえ、**これから重要性が高くなると考えられる製品分野を公表。**
- その**分野に該当する我が国製品について、専門家による有効性確認を実施**し、その**内容を発信**することで、**ユーザーが我が国発の製品を選定しやすい環境を構築。**

重要分野予測

脅威、市場動向等を分析し、**これから重要となる分野の予測をIPAが公開**

重要分野に該当するセキュリティ製品

製品A

製品Aの評価

・使いやすさ
・技術的な革新性
・コスト
（管理含む）
等

導入選定時に参照

有識者による評価

重要分野に関連するセキュリティ技術・製品について、**有識者が率直な評価を行い、その内容を公表**

ユーザー企業

我が国発のセキュリティ製品の普及展開へつなげるため

セキュリティ製品の実環境への試行導入と実績公表を進める仕組みの構築

- セキュリティ製品等の**選定の決め手の一つは、実環境への導入実績。**
- 実環境への**試行導入・実績公表を行う企業向けの手引きを作成**するとともに、試行導入に関心がある**ユーザーとベンダーをマッチング**し、**我が国発のセキュリティ製品の試行導入・実績公表を促進。**

＜ベンダー側の課題＞

・良い製品を作っても、実績がないとユーザが導入してくれない（鶏と卵）

売り込むが・・・

＜ユーザー側の不安＞

・セキュリティ製品の導入が既存システムへ影響を与えないか
・導入事例を公表することでリスクが高まらないか

＜試行導入・導入事例公表の手引き＞

・どのようなプロセスでセキュリティ製品の導入対象システムを選定したのか、事例公表に踏み切った理由等を紹介

マッチングの機会を創出

コラボレーション・プラットフォーム

セキュリティ製品の実環境への試行導入と実績公表

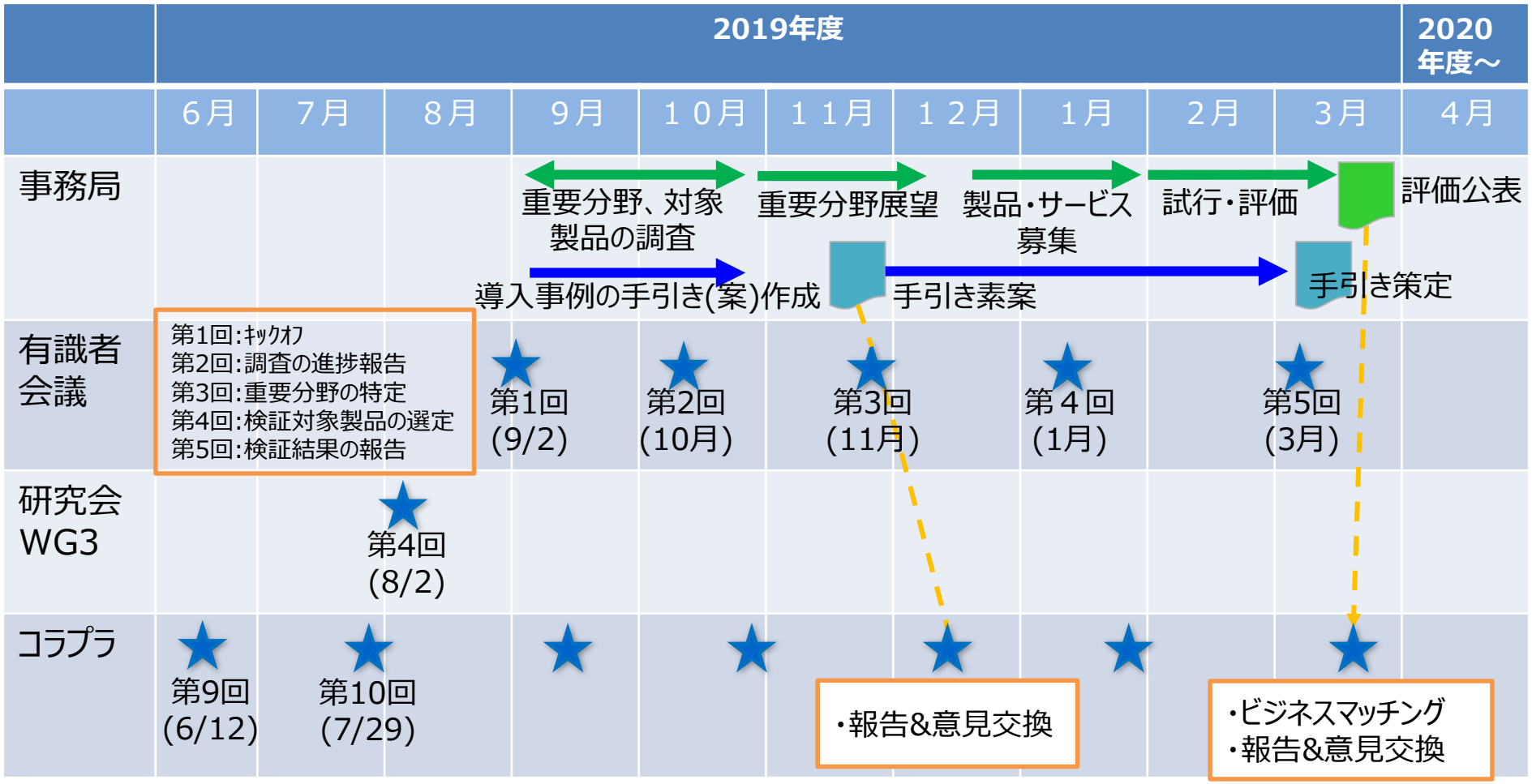
信頼できるセキュリティ製品・サービスの創出のための有識者会議の設立

- 重要分野の展望、当該分野に対応する製品の評価に関する有識者会議を設立。
- 自社で積極的にPoCを行っているユーザ企業の有識者、外部の製品の目利きを行っている有識者、技術評価に知見のあるアナリスト、学識者を中心に構成。
- 年度内に重要分野に対応する製品の評価結果の公表、及び導入事例公表の手引きを作成し、2020年3月のコラボレーション・プラットフォームでのビジネスマッチングを検討。

	名前	組織
1	寺原秀明	日本製鉄株式会社
2	斉藤宗一郎	株式会社資生堂
3	熱海徹	SOMPOリスクマネジメント株式会社
4	佐藤元彦	伊藤忠商事株式会社
5	政本憲蔵	マクニカネットワークス株式会社
6	岩井博樹	株式会社サイント
7	名和利男	株式会社サイバーディフェンス研究所
8	高倉弘喜	大学共同利用機関法人情報・システム研究機構 国立情報学研究所
9	下村正洋	特定非営利活動法人日本ネットワークセキュリティ協会

信頼できるセキュリティ製品・サービスの創出に向けたスケジュール

- ゴール：**①「重要分野予測」で我が国発の製品が活躍できる分野を明らかにし、②製品導入の実績が公表されやすい体制を構築する**ことで我が国発のセキュリティ製品の拡大を図る。
- 今年度の検証・評価方法は自由とし、来年度以降に方法を検討する。



第１回有識者会議（キックオフ）での検討事項(案)

- 重要分野予測
  - 「重要分野」の定義
  - 重要分野予測の作成プロセス
- 有識者による評価
  - 製品・サービスの選定方法・調達先
  - 評価実施者の選定方法
  - 評価項目の選定
    - 例：機能・性能、機能の網羅度、UI・使い勝手、導入コスト、運用コスト、実績（事例）、競合比較 等

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

- IoT機器・システムを中心に、**ホワイトハッカー等を有する事業者による攻撃的手法を含むハイレベルな検証を実施**。
- 実証を通じ、**信頼できる検証主体を確認する仕組み**や、**機器毎に効果的な検証手法等の考え方を整理**し、検証サービスの効果・信頼性を向上させ、ビジネスとして普及展開。

実証

検証対象

・ネットワークに常時接続する端末機器
・サイバー攻撃を受けることにより事故に繋がる可能性があるもの　等

検証事業

検証手法・検証ツール
（リバースエンジニアリング、ネットワークキャプチャ　等）

＋

検証事業者
（ホワイトハッカー　等）

検証技術等の技術開発
（内閣府SIPプロジェクト、AIチッププロジェクト　等）

実証の成果と活用のイメージ

①各検証手法を用いた、対象機器・システムごとの検証結果

⇒IoT機器等毎の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、情報管理体制等の考え方の整理

⇒信頼できる検証主体を確認する仕組みの検討

③技術開発支援などにより、我が国の検証技術の高度化

⇒検証サービスの効果向上

期待される効果

検証サービスの効果・信頼性向上

検証ビジネスの普及展開

『Proven in Japan』の促進

機器の検証に求められる考え方の整理
～機器検証の手引きの策定のイメージ

- **効果的な検証手法を手引きとしてまとめる**ことで、検証の品質の確保を目指す。
- **製品メーカーにおける、製造後だけではなく開発・製造段階での検証活用を促す**ことで、機器・システムのセキュリティレベルの向上を図る。

1．機器の検証に求められる考え方

<イメージ>

機器編

【ルータ編】
- ルータにおける脅威シナリオ
- シナリオに沿った検証項目

【スマートスピーカー編】
- スマートスピーカーにおける脅威シナリオ
- シナリオに沿った検証項目

・・・

【○○編】
・・・
・・・
・・・

共通編

機器の検証における一般的な考え方を整理したもの

- 検証の手順
- 脅威の定義（汎用的な脅威シナリオ　（存在するか））
- （脅威シナリオに沿った検証項目）
- 記録すべき事項、顧客に報告すべき事項
- 検証者が遵守すべき事項　　等

共通編の一部事項については、検証サービス事業者の認定要件とする

2．製品メーカーへの啓発

・IoT機器のベンダが、検証を受けることが望ましい部分を整理。
・製造後だけでなく、開発・製造段階での検証や、セキュアな実装に寄与する考え方を整理。

Proven in Japanにおける検証主体の信頼性確認の方向性 ～情報セキュリティサービス審査登録制度の活用を検討

- 審査登録制度により、「IoT機器向けの検証を行う主体」の「情報管理の信頼性」を確認することを検討。

情報セキュリティサービス審査登録制度

サービスの高度化方策に関する調査報告書

脆弱性診断のカテゴリとして
「ペネトレーションテスト」、
「IoT機器向け脆弱性診断」を追加

カテゴリの導入により、IoT機器向けの脆弱性診断を行う企業の登録が可能。
審査登録制度のコンセプトは「最低限の品質を維持」であるが、Proven in Japanが求める**「高レベルの技術力」を確認する手段を設けるかは要検討**。

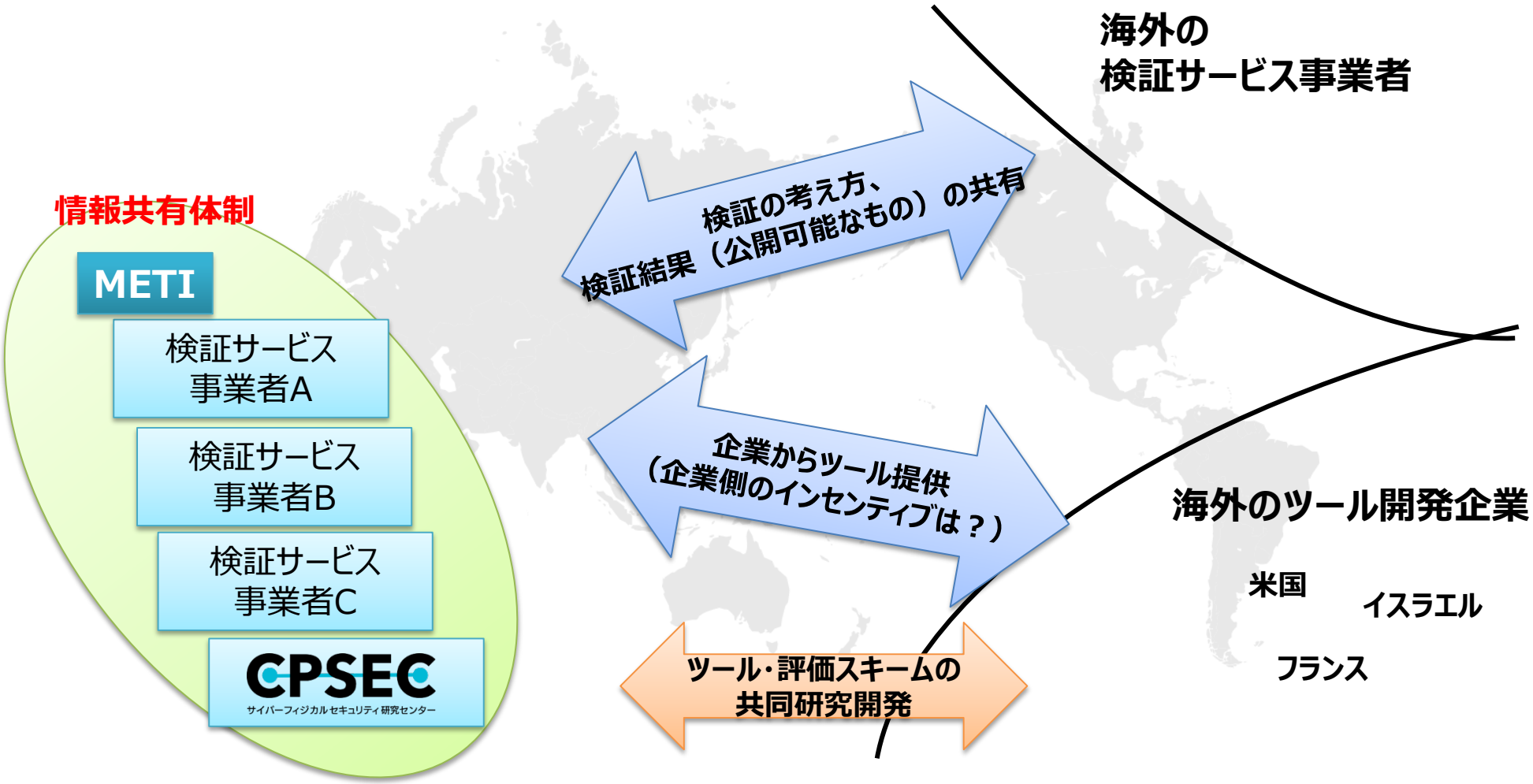
情報セキュリティサービス基準

情報管理に関する基準
- **顧客の情報を保護するための手続を設け**、運用するとともに、当該手続について脆弱性診断サービスを行った案件の担当者以外による監査を実施することにより実効性を確保していること。

現状の基準でも情報管理体制の確認は行われている。
「顧客の情報」に「検証で得られた脆弱性情報」等を明示的に記載するかは要検討

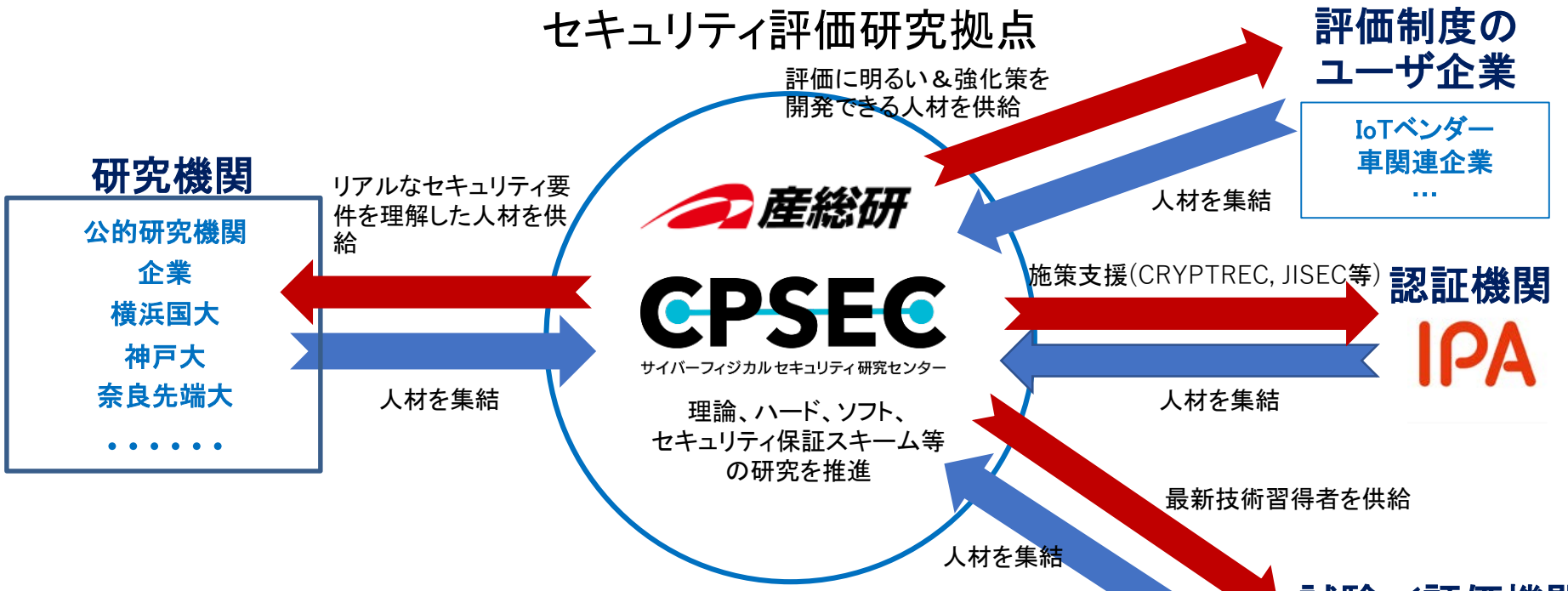
検証PFの海外連携

- 整理した検証の考え方やユースケースを海外の検証サービス事業者とも共有。
- 海外の検証ツール開発企業とも連携し、ツールの試行・フィードバックを通じた連携。



（参考）CPSECの活用

- IPAや試験機関等と密に交流できる場所に人材と設備を集結させ、日本における セキュリティ評価研究の拠点確立を検討。



持続可能な（欧米に並ぶ）セキュリティ評価体制を日本に確立

- 連携による機器の共用＆拠点での人材交流
  - 最新技術の習得（人材育成／確保）
  - 新技術の開発（セキュリティ評価／強化）
- セキュリティ評価事業（制度）へのフィードバック
  - 不正部品混入リスクへの対応
  - 製品のセキュリティを保証することで競争力を強化

（参考）NIST SP800-115※ のテスト項目

- 検証手法の参考となり得るか。ISO/IEC 29119 シリーズも要確認。

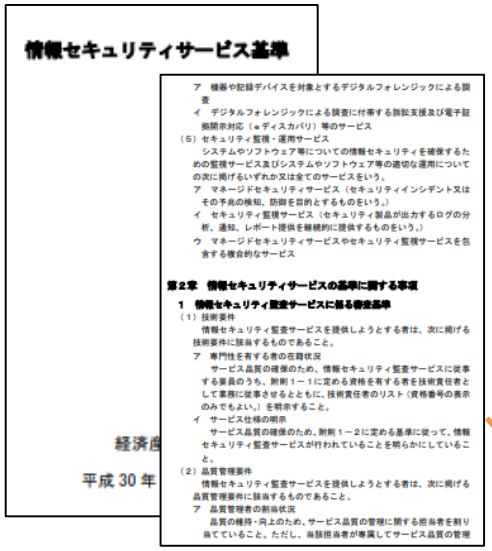
カテゴリ	Technique	Capabilities
Hardware	Testing	
Hardware /Software	Documentation Review	Evaluates policies and procedures for technical accuracy and completeness
	Log Review	Provides historical information on system use, configuration, and modification/Could reveal potential problems and policy deviations
	Ruleset Review	Reveals holes in ruleset-based security controls
	System Configuration Review	Evaluates the strength of system configuration/Validates that systems are configured in accordance with hardening policy
Software	Network Sniffing	Monitors network traffic on the local segment to capture information such as active systems, operating systems, communication protocols, services, and applications/Verifies encryption of communications
	File Integrity Checking	Identifies changes to important files; can also identify certain forms of unwanted files, such as well-known attacker tools
	Network Discovery	Discovers active devices/Identifies communication paths and facilitates determination of network architectures
	Network Port and Service Identification	Discovers active devices/ Discovers open ports and associated services/ applications
	Vulnerability Scanning	Identifies hosts and open ports/Identifies known vulnerabilities (note: has high false positive rates)/Often provides advice on mitigating discovered vulnerabilities
	Wireless Scanning	Identifies unauthorized wireless devices within range of the scanners/Discovers wireless signals outside of an organization’s perimeter/ Detects potential backdoors and other security violations
	Password Cracking	Identifies weak passwords and password policies
	Penetration Testing	Tests security using the same methodologies and tools that attackers employ/Verifies vulnerabilities/Demonstrates how vulnerabilities can be exploited iteratively to gain greater access
Else	Social Engineering	Allows testing of both procedures and the human element (user awareness) Risks

※ NIST Special Publication 800-115 “Technical Guide to Information Security Testing and Assessment”, Sep. 2008

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

- 一定の品質を維持・向上するための要件を定めた「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台帳をIPAより公開。（2018年7月）



情報セキュリティサービス基準

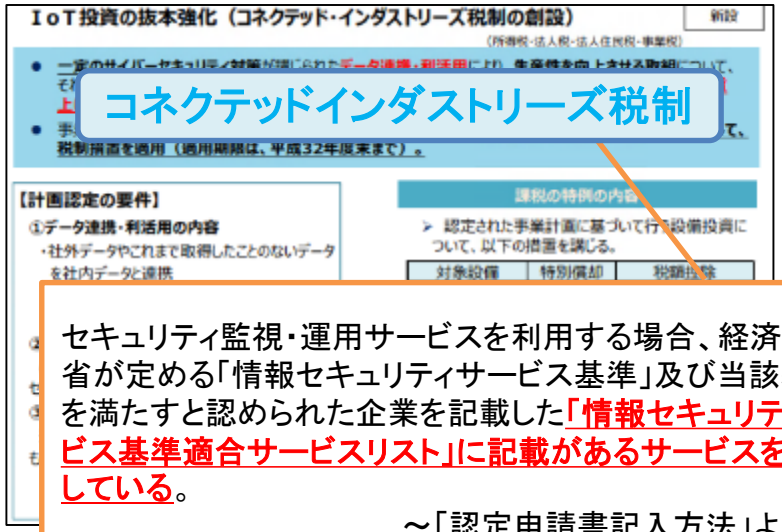
以下の4サービスに関する基準を定める
- 情報セキュリティ監査サービス
- 脆弱性診断サービス
- デジタルフォレンジックサービス
- セキュリティ監視・運用サービス

サービス名称	事業者 ①名称 ②所在地	登録年月日	リスト掲載期限	審査登録機関名
監査およびアシュアランス	①PwCあらた有限責任監査法人 ②東京都千代田区大手町1-1-1 大手町パークビルディング	2018/6/12	2020/6/11	日本セキュリティ監査協会(JASA)
情報セキュリティ監査サービス	①エヌ・ティ・ティ・データ先端技術株式会社 ②東京都中央区月島１－１５－７	2018/6/12	2020/6/11	日本セキュリティ監査協会(JASA)
情報セキュリティプランニング	①株式会社ラック ②東京都千代田区平河町２丁目16番1号平河町森タワー	2018/6/12	2020/6/11	日本セキュリティ監査協会(JASA)
	①株式会社ディアイティ			

107サービスが掲載（2019年7月23日時点）
- 情報セキュリティ監査（23サービス）
- 脆弱性診断（39サービス）
- デジタルフォレンジック（16サービス）
- セキュリティ監視・運用（29サービス）

基準を満たした情報セキュリティサービスの利用促進

- 審査登録制度の利用促進のため、政府調達時や、税制優遇措置や補助金給付を受ける場合に、「情報セキュリティサービス基準適合サービスリスト」掲載企業の活用を推奨。

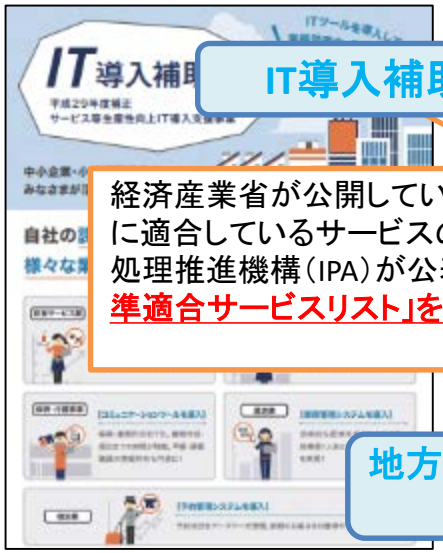


コネクテッドインダストリーズ税制

セキュリティ監視・運用サービスを利用する場合、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を記載した**「情報セキュリティサービス基準適合サービスリスト」に記載があるサービスを利用している**。

～「認定申請書記入方法」より抜粋

※情報セキュリティ監査、脆弱性診断についても同様に記載。

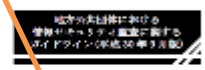


IT導入補助金

経済産業省が公開している「情報セキュリティサービス基準」に適合しているサービスのリストとして、独立行政法人情報処理推進機構（IPA）が公表する**「情報セキュリティサービス基準適合サービスリスト」を参照することが望ましい。**

～「ITツール登録要領」より抜粋

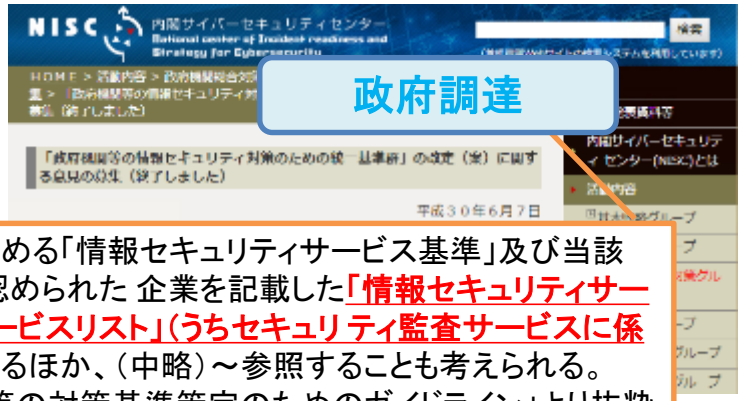
地方公共団体における情報セキュリティ監査に関するガイドライン



ⅰ)組織としての認証資格等

※例えば、ISMS 認証やプライバシーマーク認証、**情報セキュリティサービス基準適合サービスリスト（うちセキュリティ監査サービスに係る部分）**、情報セキュリティ監査企業台帳への登録等

～地方公共団体における情報セキュリティ監査に関するガイドラインより抜粋



政府調達

経済 産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた 企業を記載した**「情報セキュリティサービス基準適合サービスリスト」（うちセキュリ ティ監査サービスに係る部分）を活用**するほか、（中略）～参照することも考えられる。

～「政府機関等の対策基準策定のためのガイドライン」より抜粋

情報セキュリティサービス審査登録制度の充実に向けた取組

- 情報セキュリティサービス審査登録制度の更なる普及・発展のための具体的な施策を検討すべく、「情報セキュリティサービスの高度化方策に関する検討会」を開催。
- ユーザが自社のニーズにマッチしたサービスを提供する企業を探しやすくするために「カテゴリ」の考え方を整備し、今年度審査登録機関にてカテゴリの試行運用を開始。

検討会委員一覧（◎座長）

名前	組織
阿部恭一	ANAシステムズ株式会社
川口洋	株式会社川口設計
小松靖直	日本商工会議所
小屋晋吾	CSAJ
佐藤元彦	伊藤忠商事株式会社
下村正洋	JNSA
◎土居範久	慶應義塾大学
永宮直史	JASA
宮下清	JUAS

サービス名称（現行）	カテゴリ
情報セキュリティ監査	PCIDSS準拠性監査
脆弱性診断	ペネトレーションテスト
	IoT機器向け脆弱性診断
デジタルフォレンジック	不正調査
	インシデント対応
	ファストフォレンジック
	訴訟対応支援
セキュリティ監視・運用	－

情報セキュリティサービス審査登録制度の今後の課題

- 本制度をより普及させていくために、本制度の**登録件数倍増（100件→200件）**を目指し、以下についてさらに検討を進めていく。

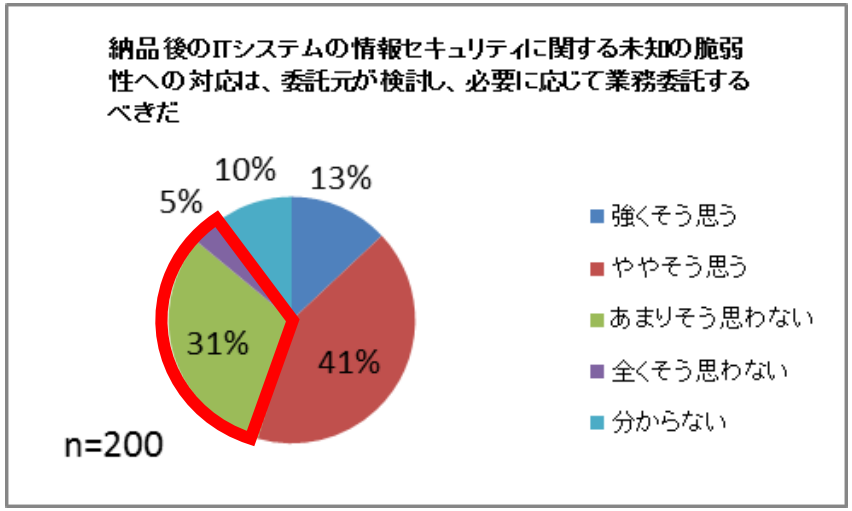
課題	施策
ユーザ企業にとって分かりにくい	• 民間（JNSA等）のサービスリストとの連携強化 • 情報セキュリティサービス表示ガイドラインの導入による、サービス利用企業にとってのわかりやすさの改善
サービス提供企業にとって登録のメリットが不十分	情報セキュリティサービスの利用を促進するため、政府調達時や、税制優遇措置や補助金の支給を受ける場合に「情報セキュリティサービス基準適合サービスリスト」掲載企業の活用を推奨
対象サービスが限定的	現状の４サービスに加え、「セキュリティ教育」や「リスクアセスメント」サービス等についても対象とするよう検討を行うことで、本制度への登録件数の拡大を図る。
制度の認知度が低い	• 全国で開催するセミナー等の機会を活用した普及展開活動 • 登録事業者であることを示す「情報セキュリティサービスマーク」表示の推進
制度自体の信頼性確保	制度自体の信頼性確保のため、昨年度に引き続き情報セキュリティサービス基準適合サービスリストに掲載されたサービスに対してサンプリングでサーベイランスを実施

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

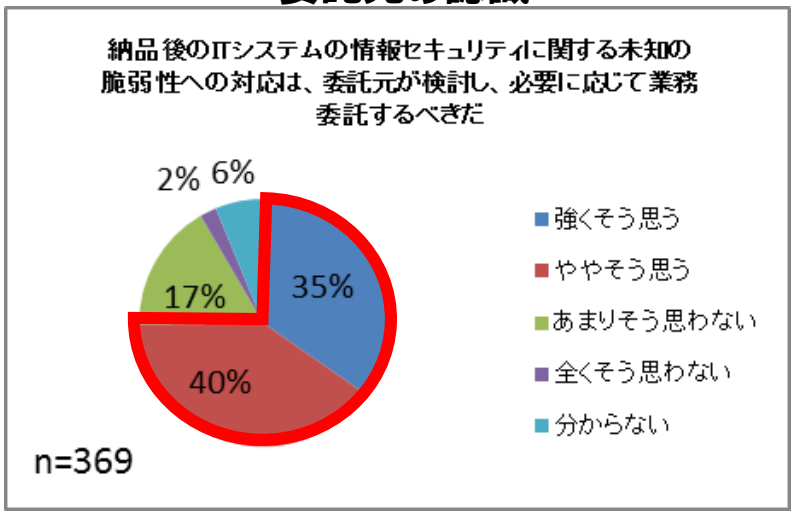
セキュリティに関する契約の課題

- 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



- 多くの企業（委託元：36%、委託先：75%）が納品後の脆弱性対応は自分がやるべきと思っていない。取引相手がやるものと思い込み、脆弱性が放置されるリスクにも繋がる。

裁判例（東京地判平成26年1月23日判例時報2221号71頁）

- インテリア商材を販売する原告X社は、ITベンダーの被告Y社に対し、オンライン受注システムの開発・保守を委託。
- しかしその後、X社のウェブサイトが、Y社から納入されたWebアプリケーションの脆弱性を突かれてSQLインジェクション攻撃を受けたため、X社の顧客情報が漏えいした。
- これについて裁判所は、当時の技術水準に沿ったセキュリティ対策を施したプログラムをX社へ提供すべき債務の不履行が認められるとして、Y社に対し、損害賠償を命じた。

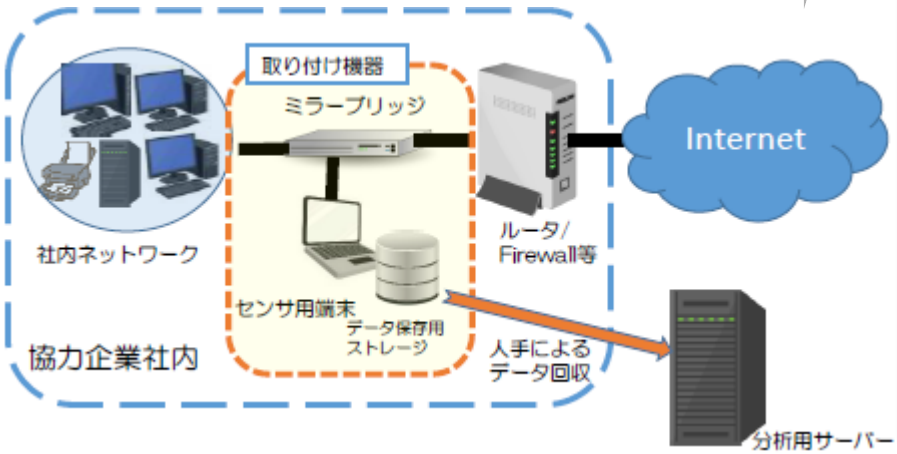
- 民法改正によるモデル取引・契約書見直し検討の中で、セキュリティについても取り組むことを検討中。

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

中小企業に対するサイバー攻撃の調査･分析結果（大阪商工会議所）

- 中小企業の社内ネットワークに出入りするパケットを直接調べた結果、重度な不正アクセスの脅威に晒されている中小企業の実態が明らかになった。

【対象】
大阪市内を中心とした多種他業種の中小企業30社
【期間】
2018年9月～2019年1月の約3～4ヶ月間
【方法】対象企業にセンサーを設置。収集したパケット情報を分析。



✓ **30社すべて**において**不正な通信**が確認された。

✓ アラートログを分析した結果、大きく３つのサイバー攻撃の実態が確認された。

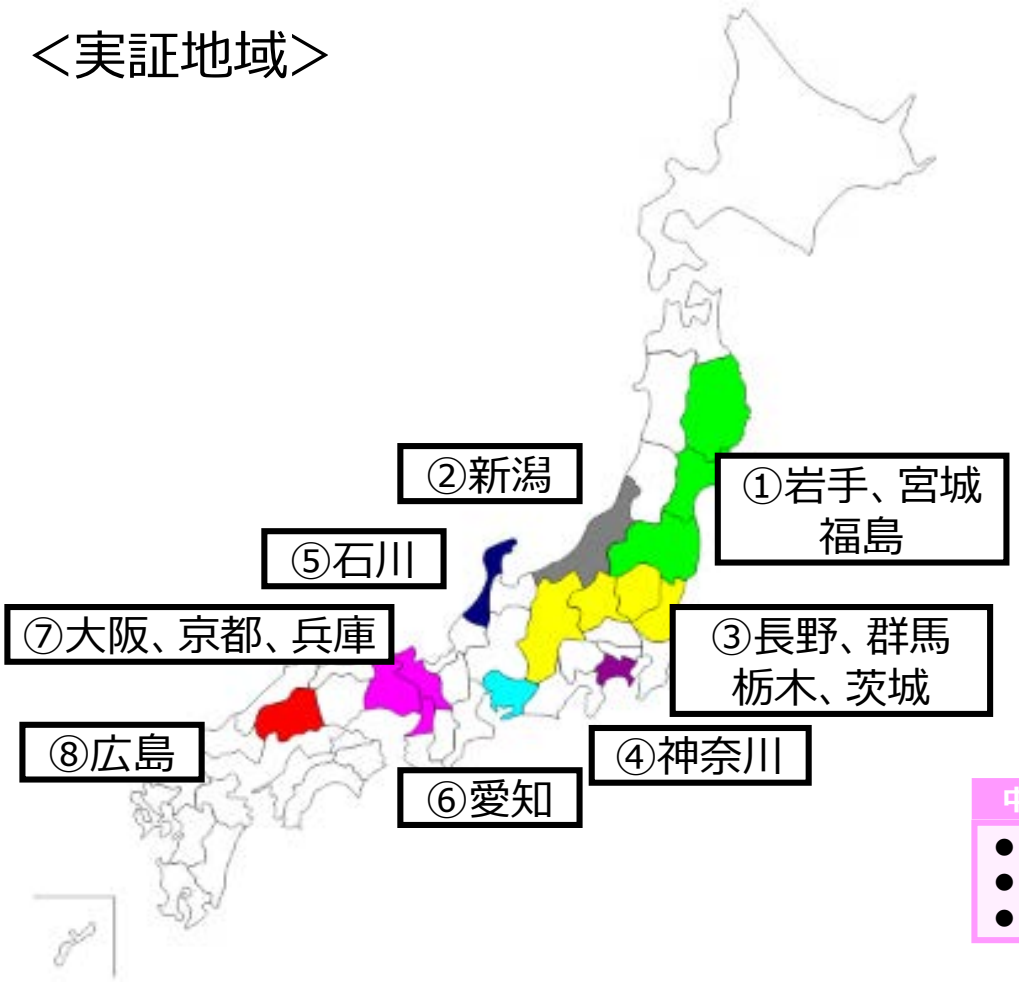
①外部からの社内端末の<u>リモート操作</u>の可能性
②社内端末と<u>悪性サイト</u>との通信
③DDos攻撃を目的としたパケットを受信

出典：大阪商工会議所「平成30年度中小企業に対するサイバー攻撃実情調査（報告）」共同研究実施者：神戸大学、東京海上日動火災保険（株）（2019年7月）

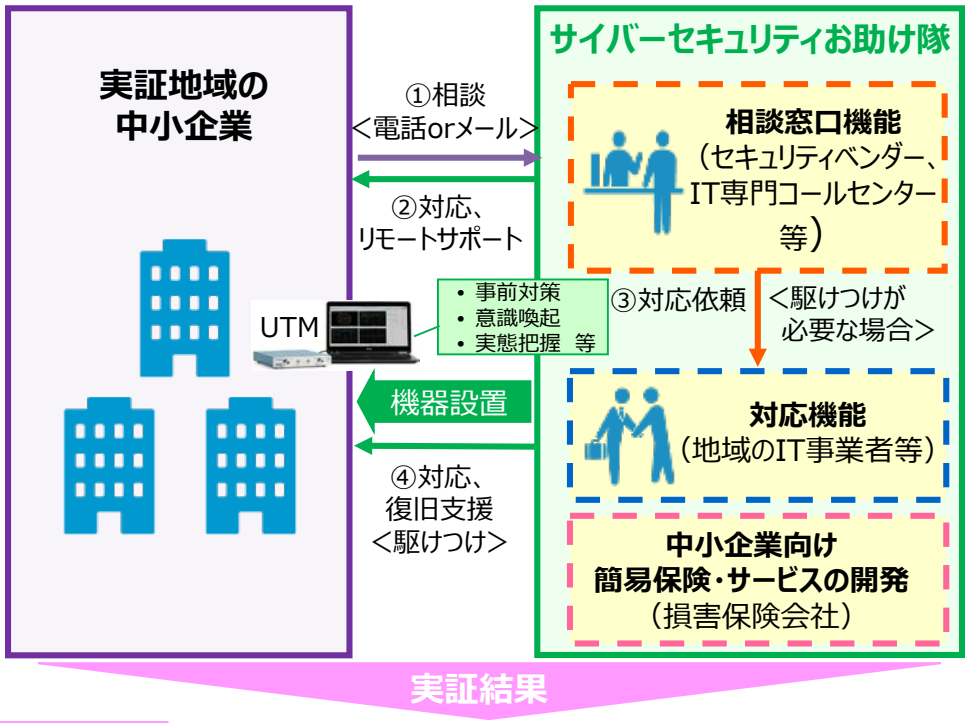
サイバーセキュリティお助け隊

- 全国**8地域**を対象に地域の団体、企業等と連携して、中小企業向けのサイバー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。
- 本事業を通じて、**サイバー攻撃の実態や対策のニーズを把握**するとともに、**中小企業の事前対策の促進、意識喚起**を図る。

＜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

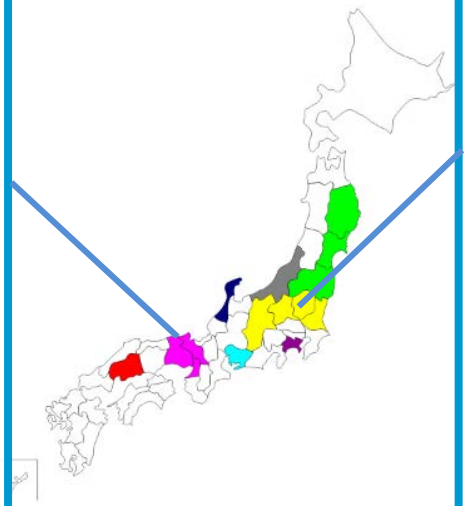
（参考）サイバーセキュリティお助け隊の取組み例

大阪、京都、兵庫 エリア

- 中小企業に“普及・浸透”させるべく、**商工会議所を起点**とした実証事業を実施。
- 実証事業終了後は、全国商工会議所への横展開を検討。

● 調査結果公表とともに記者会見を実施

実証事業開始前に実施した、中小企業の実態把握のための調査結果公表とあわせて、「中小企業のサイバーセキュリティー強化は急務」として「サイバーセキュリティお助け隊」の実証事業に取り組むと発表。



長野、群馬 栃木、茨城 エリア

- 複合機販売の地場企業の**地域密着性**を活用。
- 自社のセキュリティサービスを実証期間中に無償で提供することにより、参加企業にサイバーセキュリティ対策実体験の機会を提供。

● 参加企業確保の工夫

・複合機の営業先企業のUTM導入有無を把握していることが多いため、既存顧客から、実証参加候補をリストアップ。
・説明会を待たずに、参加候補企業へのテルコールで参加企業を募っている。
・自動車メーカーと連携し、自動車サプライチェーンも巻き込んでいく予定。
・商工会議所や県警とも連携。

（参考）各実証地域での事業説明会を開催

- 中小企業のサイバーセキュリティ意識啓発も兼ねたサイバーセキュリティお助け隊の事業説明会を全国８地域で開催。
- IPAのWebページで各事業者の事業内容や事業説明会の詳細を公開中。

実証地域	実施者	開催日
宮城県、岩手県、福島県	株式会社デジタルハーツ	8月下旬頃（調整中）
新潟県	東日本電信電話株式会社	6/25(火)、6/26(水)、6/27(木)
長野県、群馬県、栃木県、茨城県	富士ゼロックス株式会社	7/24(水)、7/26(金)、その他調整中
神奈川県	SOMPOリスクマネジメント株式会社	6/14(金)
石川県	株式会社PFU	7/26(金)、8/28(水)、8/29(木)、8/30(金)
愛知県	MS&ADインターリスク総研株式会社	6/19(水)、6/24(月) ※7/25(木)事業開始説明会
大阪府、京都府、兵庫県	大阪商工会議所	7/5(金)
広島県	株式会社日立製作所	7/24(水)、7/29(月)、7/31(水)、8/1(木)

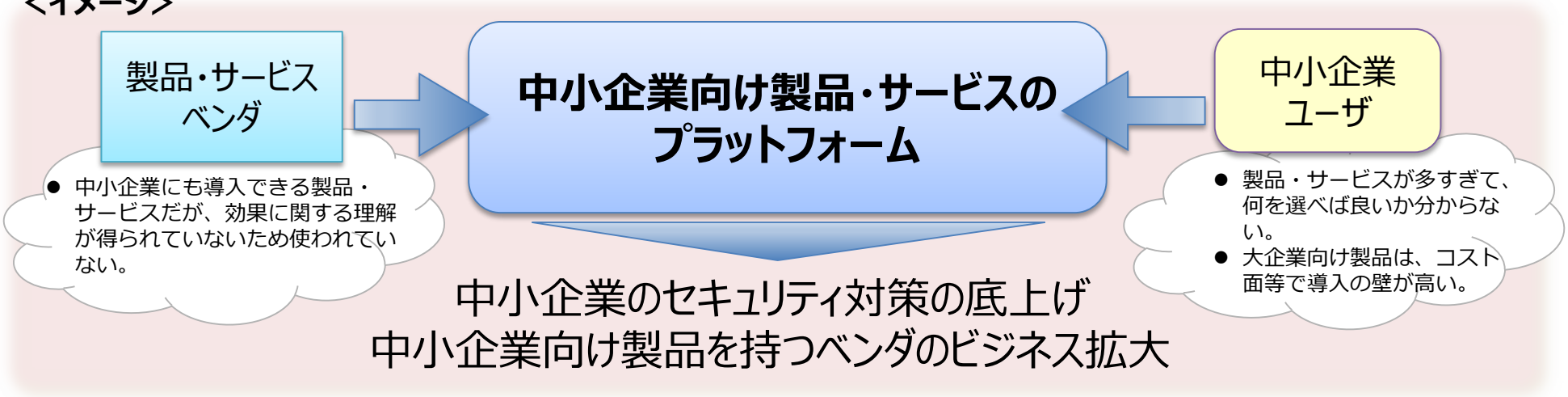
IPAお助け隊Webページ　https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html

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

中小企業向けセキュリティ製品・サービスの検証事業

- 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>

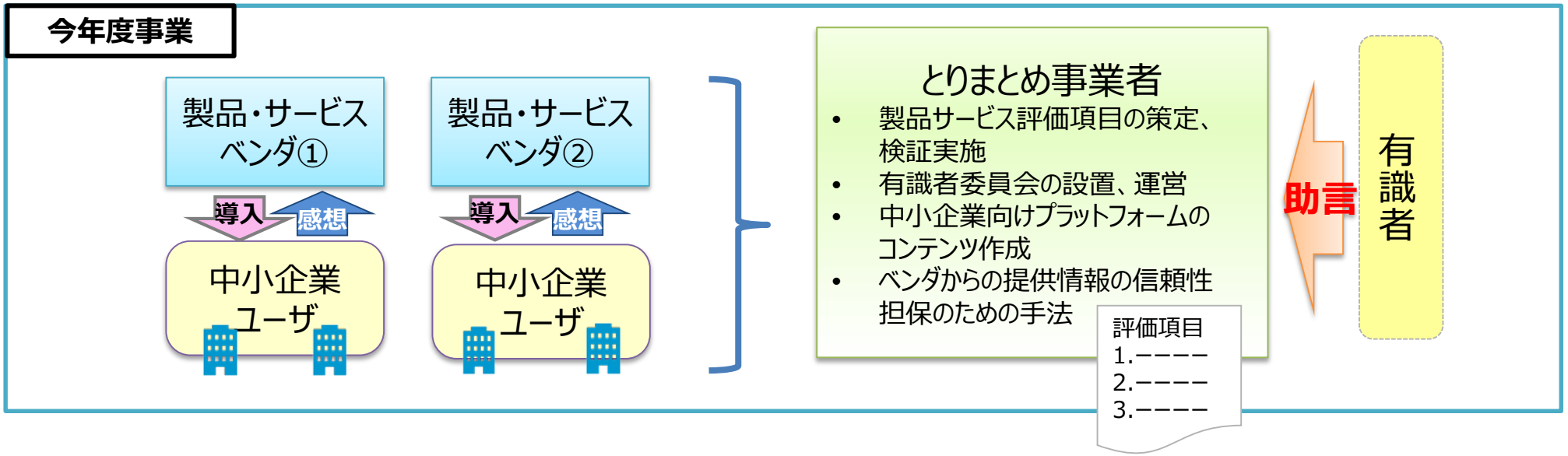


検証対象製品・サービスが満たすべき要件

- 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

今年度検証事業のスケジュールと今後の課題

- 今年度は試行検証として、ベンダ２～３社の協力を得て検証を実施し、評価項目や事業者からの情報提供の在り方を検討していく。



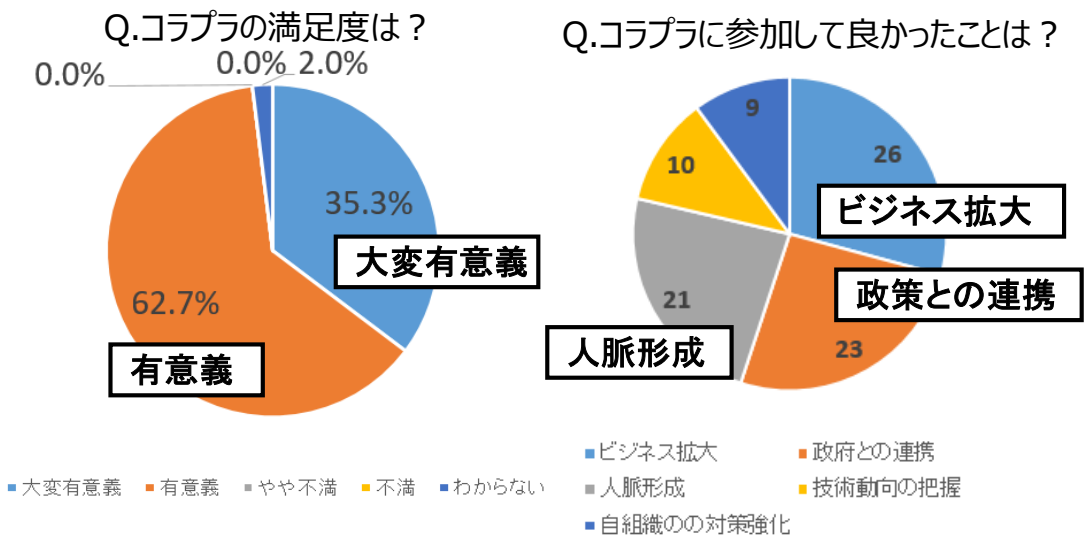
2019年度			2020年度～
▲8月 とりまとめ事業者と 製品・サービス ベンダの採択	**8月～2月　検証**	**▲3月 コラボレーション プラットフォーム 【ビジネスマッチング】**	＜課題＞ プラットフォームの 運営主体をどこにするのか

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

（参考）コラボレーション・プラットフォームの開催状況

- 継続的にコラボレーション・プラットフォームを開催し、各回多数の申込みあり。
- 今後もコミュニティ形成やビジネスマッチングの強化を図るコンテンツを検討。

	日にち		参加人数(*)
2018年	6月13日	第一回	179名（99名）
	7月23日	第二回	104名（74名）
	9月3日	第三回	132名（69名）
	10月16日	第四回	151名（56名）
	11月30日	第五回	98名（40名）
2019年	1月25日	第六回	108名（48名）
	3月4日	第七回	114名（42名）
	4月23日	第八回	97名（51名）
	6月12日	第九回	133名（34名）
	7月29日	第十回	112名（42名）



※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

(*)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


パネルディスカッション(第一回)


グループディスカッション(第二回)

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

（参考）地域での産学官連携による人材育成・コミュニティ形成の促進

- 各地域で不足しがちな**地域を支えるセキュリティ人材の育成**や、実務担当者間の情報交換や相互扶助の基盤となる**地域に根差したコミュニティ形成**のための産学官連携の取組を促す。

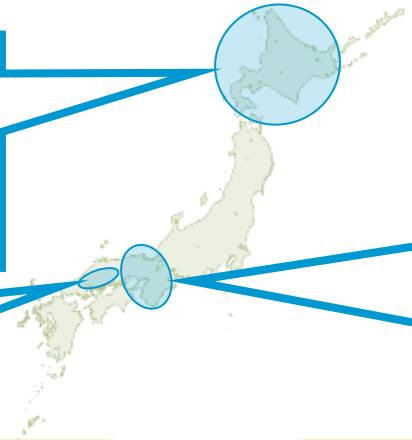
＜各地域の取組の例＞

北海道地域情報セキュリティ連絡会（HAISL）
（北海道局、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13回）


一般向けセミナー(H30.10)


会員向け勉強会の様子

サイバーセキュリティセミナー広島・岡山
・平成31年2月20日@広島（中国経産局、中国総通局）
・平成31年3月5日@岡山（中国経産局、中国総通局）



関西サイバーセキュリティ・ネットワーク
（近畿局、総通局、KIIS※1）

平成30年11月12日
キックオフフォーラム

リレー講義の様子
（計7回実施）

＜取組の方向性＞

１．地域を支える人材の育成

- **産学官連携によるセキュリティ教育の充実**
  ・国立高専機構と産（JNSA※2、CRIC CSF※3 等）や官（IPA、地方局 等）との更なる連携強化　等
- **ICSCoEの地域へのアウトリーチ**
  ・各地域への出張講義　等

両輪で促進

２．地域に根差したコミュニティの形成

- **コミュニティ形成のための働きかけ**
  ・地方版コラボレーションプラットフォームや、シンポジウム（5月28日@大阪）の開催 等
- **ハブとなる人材の活躍促進**
  ・各地域の登録セキスペやICSCoE修了生等との連携強化　等

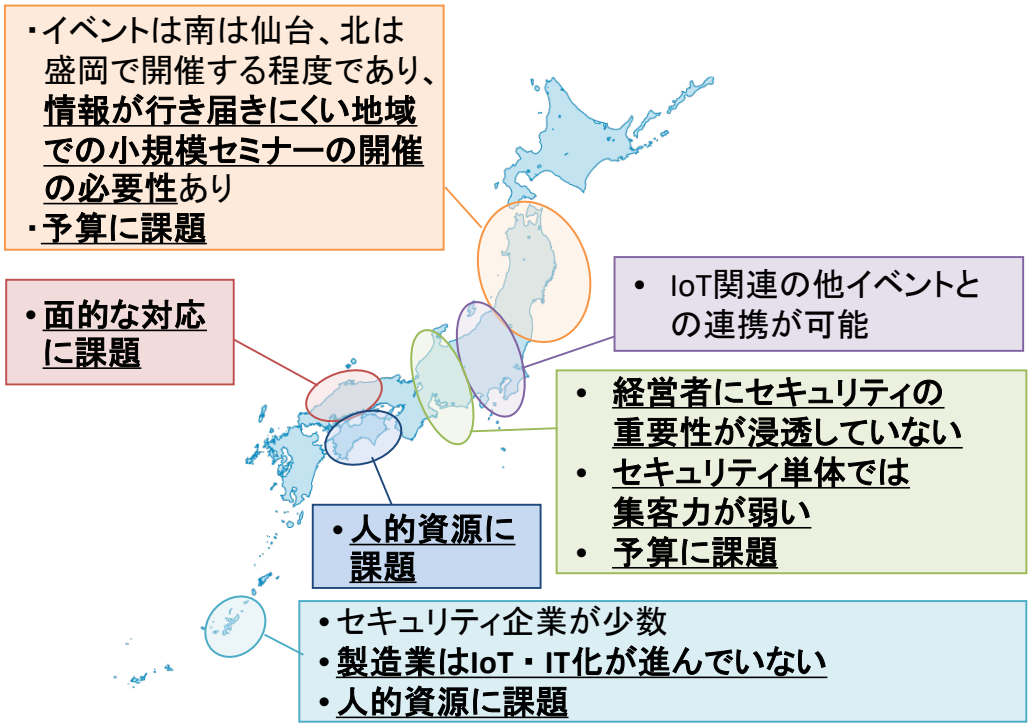
産	学	官
企業・業界団体等 ■CRIC CSF、JUAS、JNSA ■ユーザー企業、ベンダー企業　等	**大学・高専等** ■情報系の学生 ■研究者・教員　等	**関係省庁・独法・自治体等** ■都道府県警、地方局 ■IPA、JPCERT/CC　等

※1 KIIS･･･Kansai Institute of Information Systems、※2 JNSA･･･Japan Network Security Association、
※3 CRIC　CSF･･･Cyber Risk Information Center Cross Sectors Forum

地方版コラボレーション・プラットフォーム開催に向けて

- 地域毎にコラボレーション・プラットフォームを継続的に開催することで、**地域のセキュリティ意識の向上**を図り、**地域内のセキュリティ人材育成**を行うとともに、**セキュリティ担当者同士の企業・業種を跨いだ交流を活発化**を図る。地方ごとのニーズも踏まえたビジネスマッチングの場としての活用も検討。
- 各地方局にヒアリングを実施し、各地域の取組状況や課題が見えてきたところ。
- 今年度、地域のニーズに合った地方版コラボレーション・プラットフォーム開催に向けて、2～3地域で既存の取組みや会議体等との連携を検討中。

＜主な地方局の声（課題等）＞



＜地域の特徴を踏まえて検討中のイベント内容＞

【情報が行き届いていない地域】
各地域のニーズを深堀し、自治体、県警等との連携し、**少人数での勉強会・悩み相談会**開催

【IoT、IT化を推進している地域】
地方版IoT推進ラボ等と連携し、**IoT、ITの導入を検討している方向けにセミナー**を開催

【地域にキーとなる会議体等がある地域】
地域のキーとなる会議体等と連携し、セキュリティイベントを開催