経済産業省

資料3

事務局説明資料

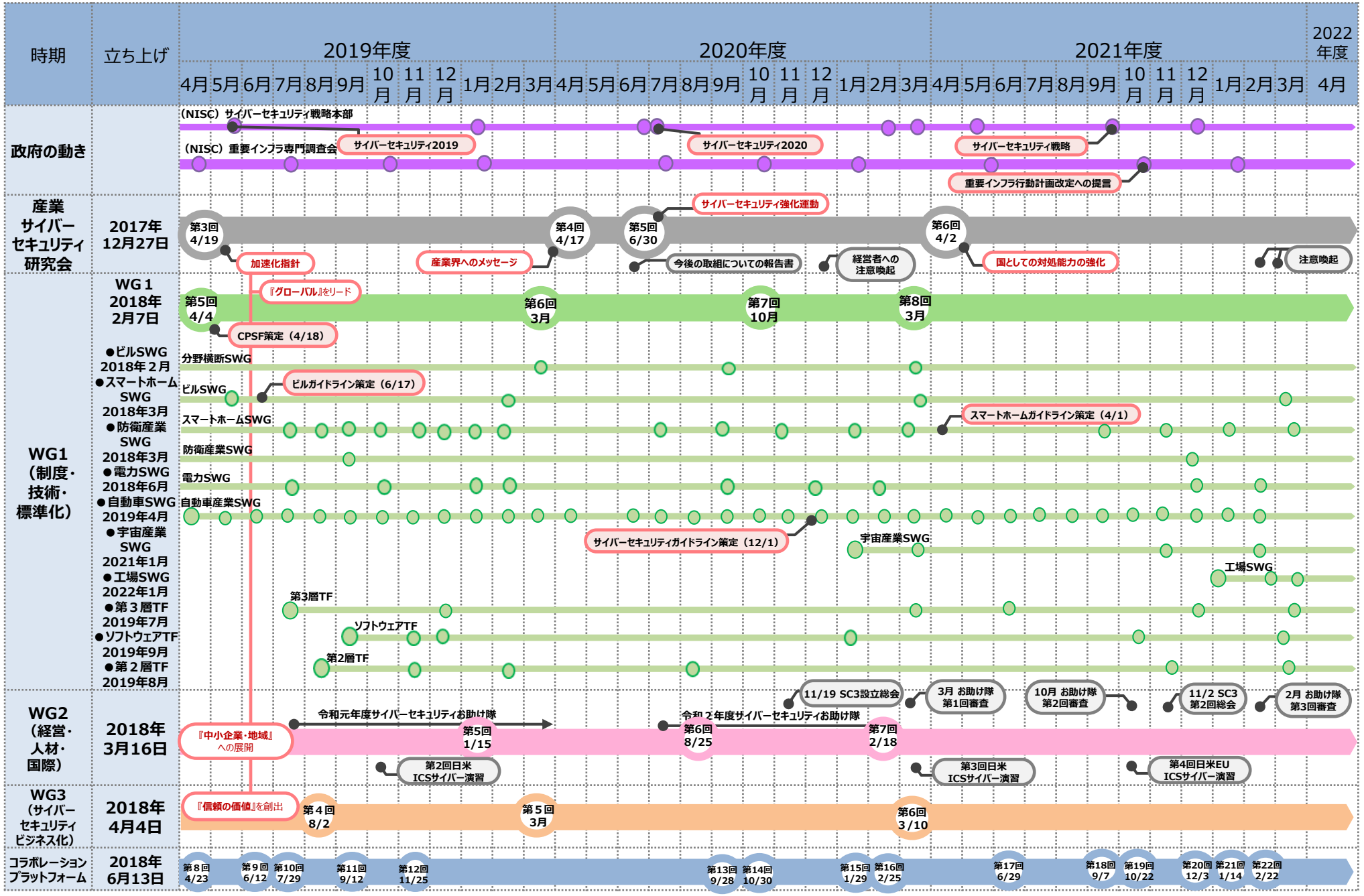
産業サイバーセキュリティ研究会WG3
（サイバーセキュリティビジネス化）
第７回

令和４年４月６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会議の実績



サイバー・フィジカル・セキュリティ対策フレームワークを軸とした各種取組

- **「サイバー・フィジカル・セキュリティ対策フレームワーク」では、Society5.0における産業社会でのセキュリティ対策の全体枠組みを提示。**
- 全体の枠組みに沿って、対象者や具体的な対策を整理し、『サイバーセキュリティ経営ガイドライン』や産業分野別のガイドラインなどの実践的なガイドラインを整備。

＜各種取組の大まかな関係＞

目次

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

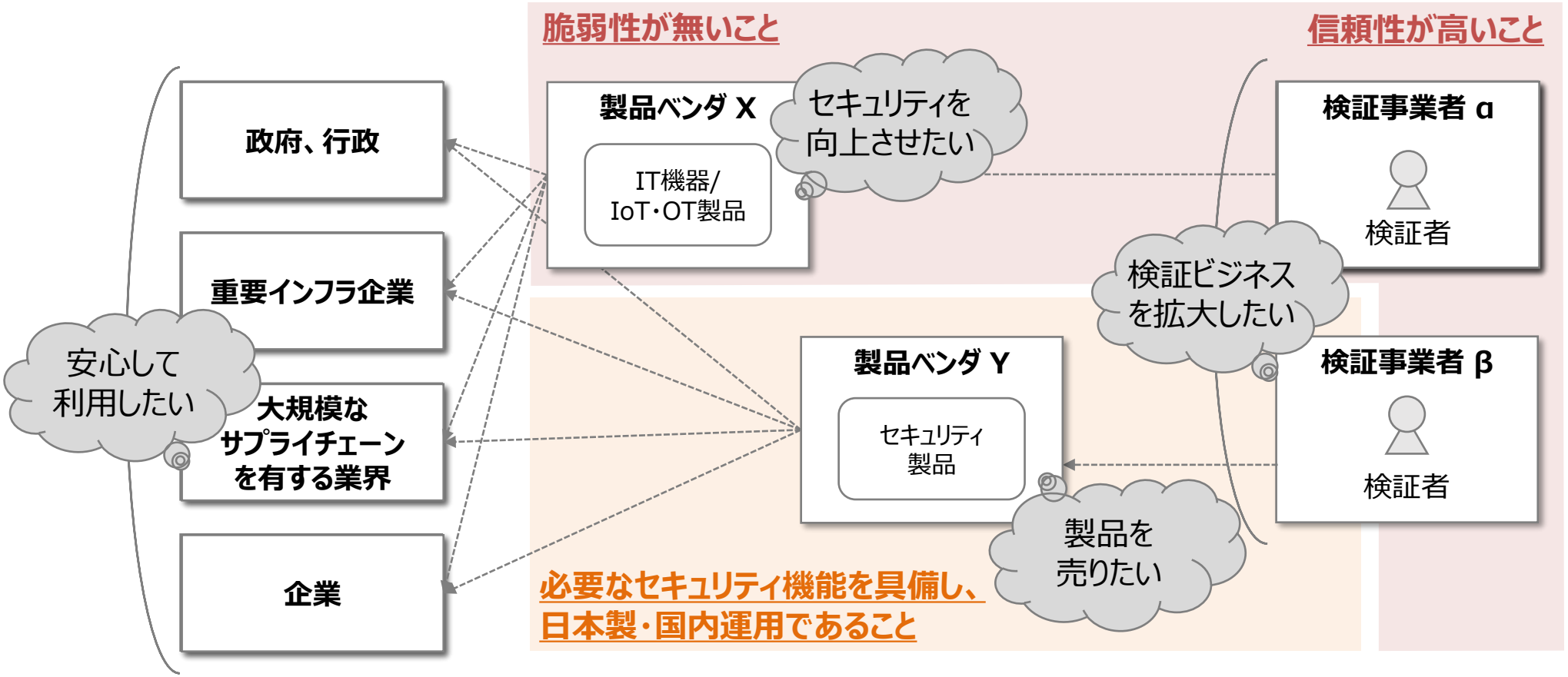
市場への展開

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

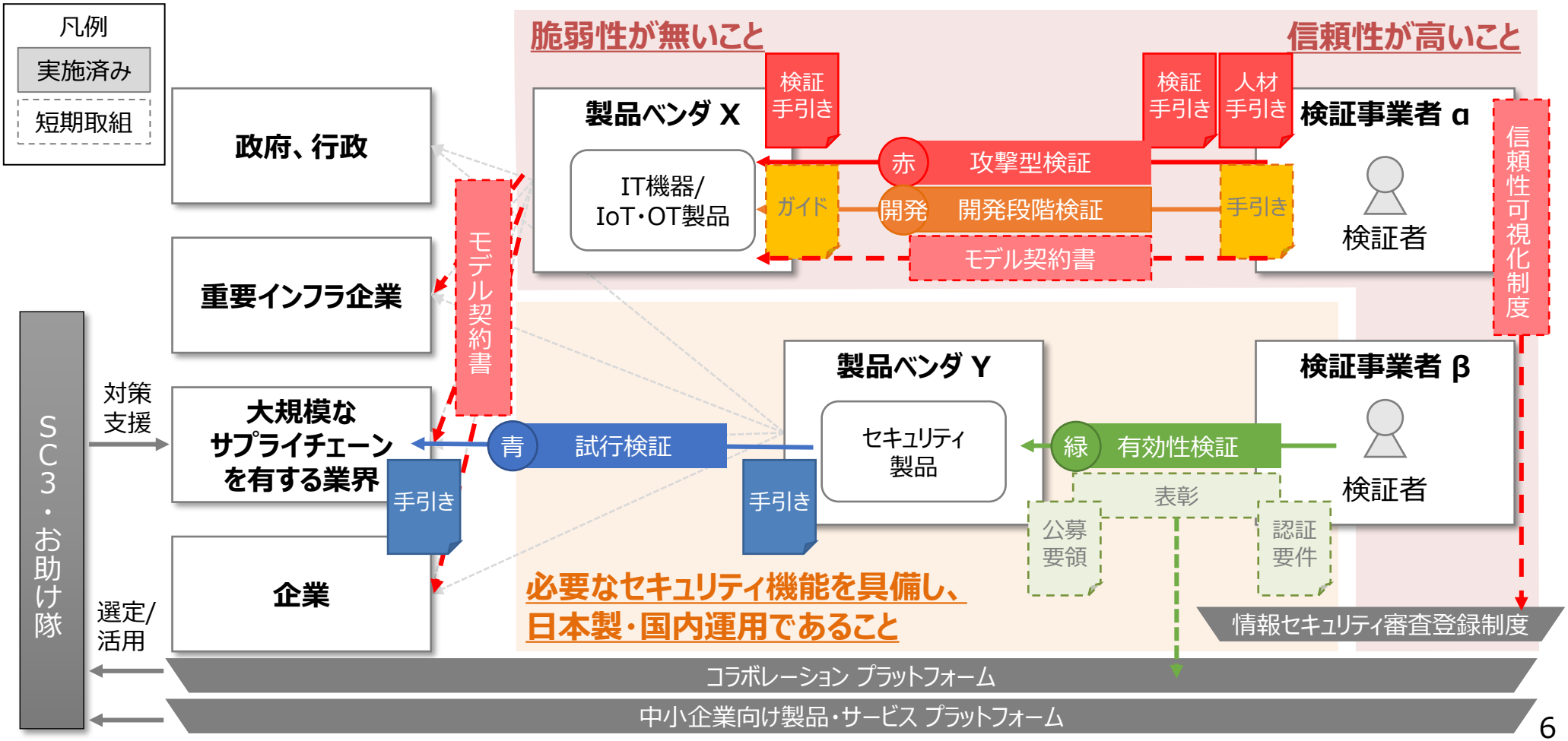
検証基盤に求められる要件

- 安心して製品・サービスを利用できるためには、**信頼できる検証事業者**が、**利用する製品に脆弱性が無いこと**を検証してもらえる仕組みが必要。
- また、**利用するセキュリティ製品が必要な機能を具備し、かつ日本製・国内運用であること**ことが望ましいと考えられる。



検証基盤の全体像

- 産業サイバーセキュリティ研究会WG3(ビジネス化検討)による議論をベースに、セキュリティ検証サービスの産業化に向けて、**セキュリティ製品の有効性検証（緑検証）**や**実環境における試行検証（青検証）**、**攻撃型を含めたハイレベルな検証（赤検証）**を進め、モデル契約やコラボレーションプラットフォーム等と連携してきた。



（参考）『Prove in Japan』 及び関連事業の取組内容（一覧表）

	実施内容	成果物	主な検証対象
緑 セキュリティ製品の有効性検証	サイバー攻撃に対応するセキュリティ製品分野を公表し、その分野に該当する我が国発の製品について、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。	• 試行導入・導入実績公表の手引き • 2019年度版セキュリティ製品・サービス重要分野マップ	• Yamory(VISIONAL社) • WiSAS(Spline Network社) • GUARDIAX(グレスアベイル社)
青 実環境における試行検証	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。		• AX-Network Visualization(Alaxala A社)
赤 攻撃型を含めたハイレベルな検証	2021年4月、機器のハイレベル検証(ペネトレーションテスト)の方法や人材育成の方法を手引きとして公開。2021年度は産業機器に検証対象を広げ、手引きの有効性を確認。 検証事業者の信頼性を可視化するための要件を整理し、情報セキュリティ審査登録制度に「セキュリティ検証」を新設できるか検討中。	• 機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き、解説書 • 検証人材の育成に向けた手引き	• ルータ、UTM、タブレット、スマートロック • ドローン、スイッチ、ロボット掃除機、ノートPC • スマートリモコン・TV、車載器、産業用PC
開発 セキュリティ・バイ・デザインを実現する開発段階検証	開発段階から、設計書とソースコード、実装したプロトタイプで検証を行い、脆弱性を排除した開発を実施することにより、効果的な検証の進め方を整理するとともに、開発段階からの検証の効果を可視化する。これにより、設計段階からセキュリティを意識する「セキュリティ・バイ・デザイン」の考え方を採り入れ、コスト低減を図りつつ、中小企業に検証の必要性を認知してもらうことを目指す。	（今後実施予定）	（予定） IoT家電、産業機器、工場のセンサー、産業用ドローン、NW機器、車載器、モバイル端末、スマートデバイス、等

（参考）『Prove in Japan』 及び関連事業の取組内容（一覧表）

	実施内容	成果物
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に関する情報交換、交流を行っていただける「場」を提供することを目的としたコラボレーション・プラットフォームを開催。	• 2021年度までに20回開催し、のべ2,470名が参加。 • 有効性が確認されたセキュリティ製品のシーズとニーズに係るマッチングの場を提供し、市場展開を促進してきた。
情報セキュリティ 審査登録制度	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。	• 情報セキュリティ監査　67サービス • 脆弱性診断　107サービス • デジタルフォレンジック　28サービス • セキュリティ監視・運用　45サービス 2021年12月現在
モデル契約書	情報システムの信頼性向上・取引の可視化に向けた取引・契約のあり方を整理したもの。2007年に第一版を作成・公開し、その後、民法改正対応及び現在の環境・状況に合わせるべく修正し、2020年にIPAからモデル契約（第二版）を公開。	• モデル契約書のダウンロード数：65,822件 （うち、セキュリティ関連に関わるガイドライン：12,216件）
中小企業向け製品・ サービス PF	中小企業をターゲットとしたセキュリティ製品やサービス選定時のニーズにマッチしているか検証し、適切な製品やサービスを選択できる環境を支援することで、中小企業向けセキュリティ製品の普及を後押しし、中小企業のセキュリティ対策の底上げを図る。	• 中小企業によるセキュリティ製品・サービス選定プロセスの実態・評価基準の見える化 （Security Action登録業者約2,000件からサンプリング）
サイバーセキュリティ お助け隊	中小企業のサイバーセキュリティ対策を支援するための相談窓口、異常の監視、事案発生時の初動対応（駆付け支援等）及び簡易サイバー保険を含む各種サービスを、安価かつ効果的なワンパッケージで確実に提供する。	• 12サービスが全国各地域の中小企業へサービスを展開中。（2022年3月現在）

目次

（２）各施策の現状及び今後の方向性

１．Proven in Japan（検証基盤）
- －緑青検証
- －赤検証
- －開発段階検証（主に中小企業向け）

２．情報セキュリティサービス審査登録制度

３．サイバーセキュリティお助け隊

４．中小企業向けセキュリティ製品の検証

５．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

- 「**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

⇒2021年度は新たに開発段階の製品・設計書等の検証も実施。

1.セキュリティ製品の有効性検証

ベンチャー等のセキュリティ製品

有効性検証

検証環境

2.実環境における試行検証

ベンチャー等

お試し製品提供と検証

実環境

民間事業者等のオフィス

3.攻撃型を含めたハイレベルな検証サービス

検証サービス事業者

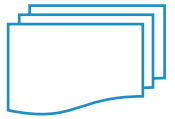
攻撃型検証等

IoT機器・システム等

4.セキュリティ・バイ・デザインを実現する開発段階検証

検証サービス事業者

開発段階検証



設計書・ソースコード等

New

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

緑青検証の立ち上げ背景・概要

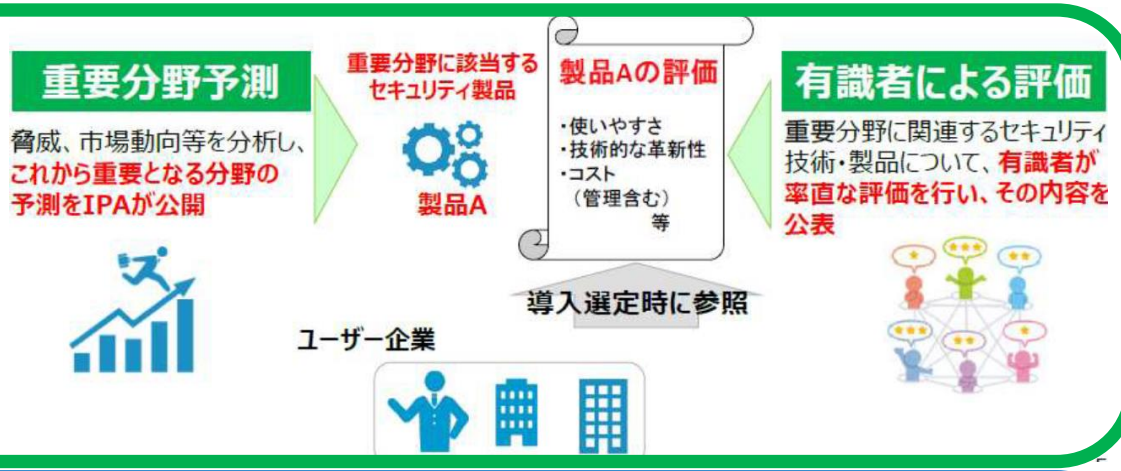
- 産業サイバーセキュリテイ研究会WG3(ビジネス化検討)による議論をベースに、**ベンチャー等のｾｷｭﾘﾃｨ製品/サービスの有効性確認を通じて、国内市場へのマーケット・インを促進。**
- 2019年度より、サイバーセキュリティ検証基盤を整備し、セキュリティ製品の有効性検証(緑検証)/実環境における試行検証(青検証)に着手。

製品の有効性を確認し、発信する仕組み

①国内の脅威・対策動向を踏まえ、**重要性が高い製品分野を設定**

②重点分野に該当する**国内製品**を対象に**有効性検証を実施**

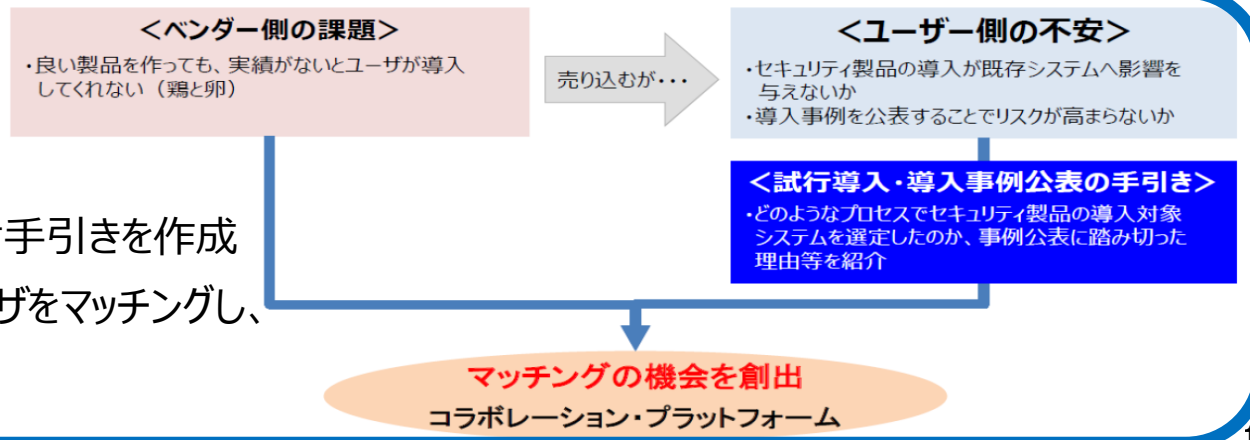
③検証結果を情報発信し、評価製品を選定しやすい環境を構築



実環境への試行導入と実績公表を進める仕組み

①試行導入・実績公表を行う企業向け手引きを作成

②試行導入に関心のあるベンダー・ユーザをマッチングし、国内ベンチャー企業の立ち上げを支援

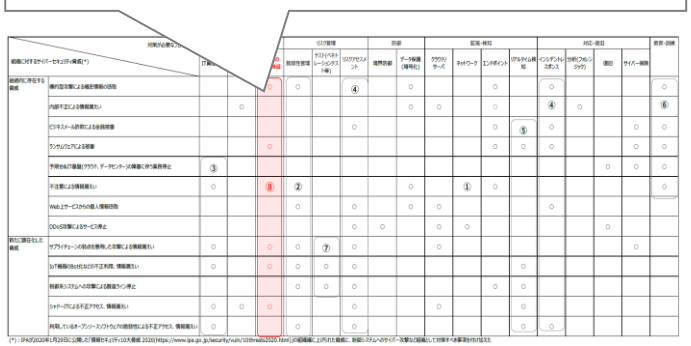


これまでの取組

- 有識者会議を開催し、重要分野の選定と該当分野の国内製品の検証作業を実施。
- また、実環境における試行評価もあわせて実施。
- これらのアウトプットを取りまとめ、コラボレーション・プラットフォームで紹介することでマッチングを後押し。

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）

① 脅威の可視化
② 脆弱性の可視化
③ IT資産管理
④ 脅威インテリジェンスの整理・管理
⑤ マルウェア感染/発症の重篤度判定
⑥ 教育・トレーニング
⑦ ハイレベルセキュリティ検証
⑧ IT資産の認証/検証



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

結果をIPAから公表した他、コラボレーション・プラットフォームにて紹介し、**ビジネスマッチング**を実施

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

有効性検証結果

製品のストロングポイント

実環境における試行検証結果

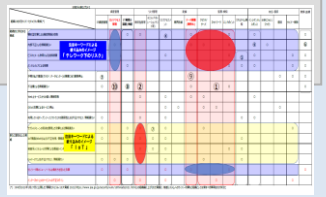
『試行導入・導入実績公表の手引き』
- 公表のメリット／デメリット
- 公表可否判断のポイント
- 公表内容
- ステークホルダーとの調整 等

2021年度の取組・成果

- 検証事業の最終年度に当たる2021年度は、注力すべき重点領域を更新しつつ、製品選定から有効性検証の仕組み(手順・基準等)に基づいた製品検証や実環境での試行を実施し、これを通じ「試行導入・実績公表の手引き」の検討を実施した。
- また、更なるマッチング機会創出に向け、検証結果を活用した表彰制度の立案に向けた検討を行った。

国内外の技術トレンド・製品動向に基づく重点領域の更新

データ保護、ID/アクセス管理の追加



専門家による有効性検証

国内において新規性が高い製品のセキュリティ機能の有効性を有識者にて検証・評価

・Karma（ゼロゼロワン社）
国産IoT検索エンジン

実環境での試行検証

検証事業者環境にて、手引きに従いユーザ企業が実装機能の有効性、操作性等を評価

・AeyeScan（エーアイセキュリティラボ社）
クラウド型脆弱性診断ツール

前年度作成した評価・プロセスの有効性を検証し、「試行導入・実績公表の手引き」に反映

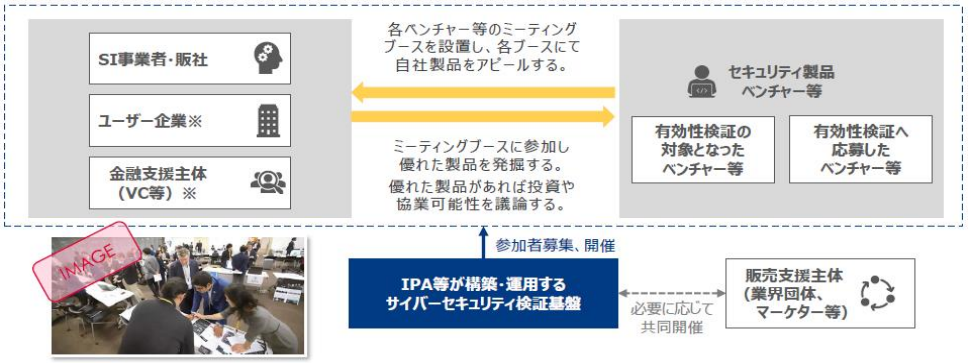
市場参入手法を検討

セキュリティ製品ベンダとSI業者・販社等とのマッチング機会の創出

①マッチングイベントの開催
・商談機会の発掘支援

②表彰の付与・イベント開催
・有効性検証結果に基づく表彰

③ベンチャー等の情報発信サイトの立上げ

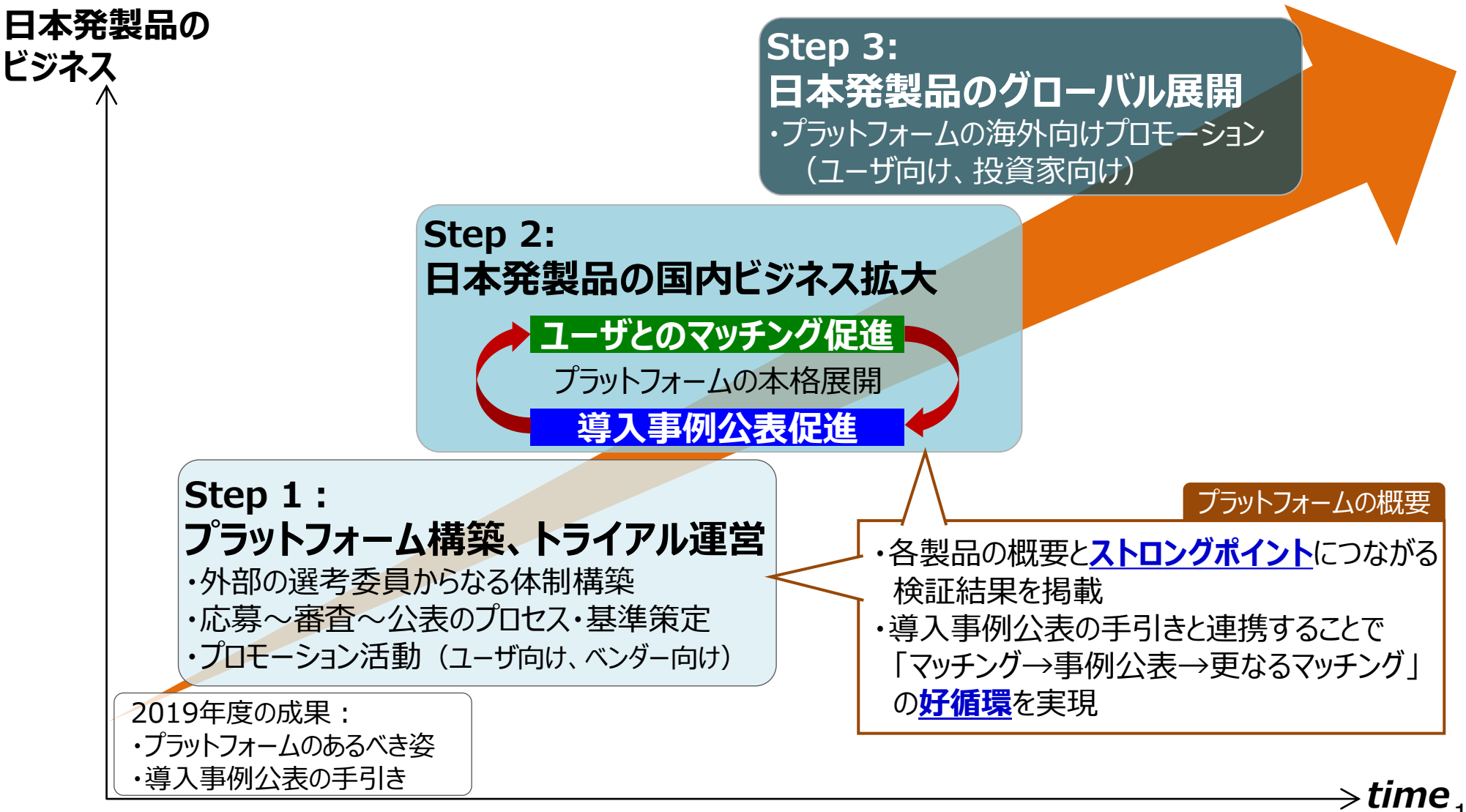


緑青検証の進め方

前回WG3資料の再掲

緑 青

- ２年間に渡る本事業の成果を基に、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。



（参考）製品評価を受けたベンダ企業による評価

- 本検証結果を営業活動に活用し、大手企業２社を含む複数の商談獲得に貢献したが、件数は限定されており　更なる継続的な事業機会・商談発掘の場の拡充を要望。

セキュリティ製品の機能検証

株式会社スプライン・ネットワーク

Spline Network

評価製品：Wifi セキュリティ「WiSAS」
事業概要：セキュリティ監視サービス
　　脆弱性診断サービス

EGセキュアソリューションズ株式会社

EG Secure Solutions

評価製品：次世代クラウド型WAF「GUARDIAX」
事業概要：情報セキュリティ監査、コンサルティング、調査
　　セキュリティ製品の開発、販売、サポート

実環境での有効性/操作性検証

アラクサラネットワーク株式会社

AlaxalA

評価製品：NW可視化・異常検知SL
　　「AX-Network Visualization」
事業概要
　・NW機器の開発・製造・販売・保守
　（企業向け、通信業者・ISP向け）

事業への貢献

■ 受注・商談機会の獲得
- ・重要インフラ/大手企業への採用（大手私鉄グループ、公的機関）
- ・企業からの引き合い・提案依頼を各社とも複数件確認
- ・評価結果を販促ツールとして活用した商談多数・一部は受注

■ 販売チャネルの獲得
- ・代理販売店の獲得（契約前の製品評価にて活用）

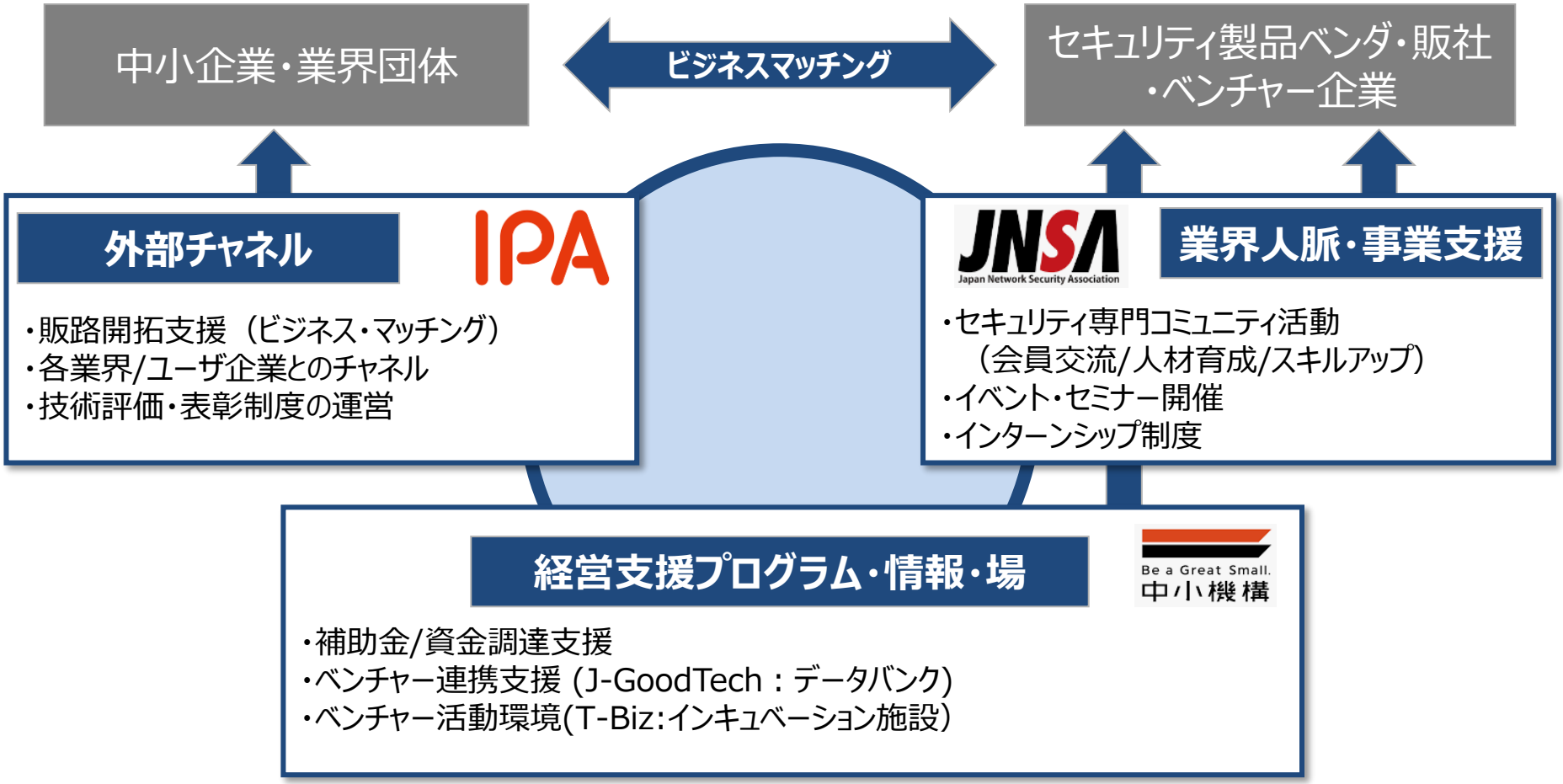
ベンチャー企業からの期待

■ 自社での販促活用に加えて、更なる商談機会の拡大
- ・評価結果の情報掲載、セミナー等による情報発信に加えて、ユーザ・販売店、SI事業者の顔が見える“場”の整備
- ・各種イベントの開催・商談会の開催による紹介機会の拡大

■ 継続的な情報発信、事業支援施策の拡充
- ・情報発信/イベントの継続による、潜在ユーザ企業への訴求
- ・ジャンル別の特集掲載、複数ベンチャー企業共同イベントの開催

実現すべきエコシステム（イメージ）

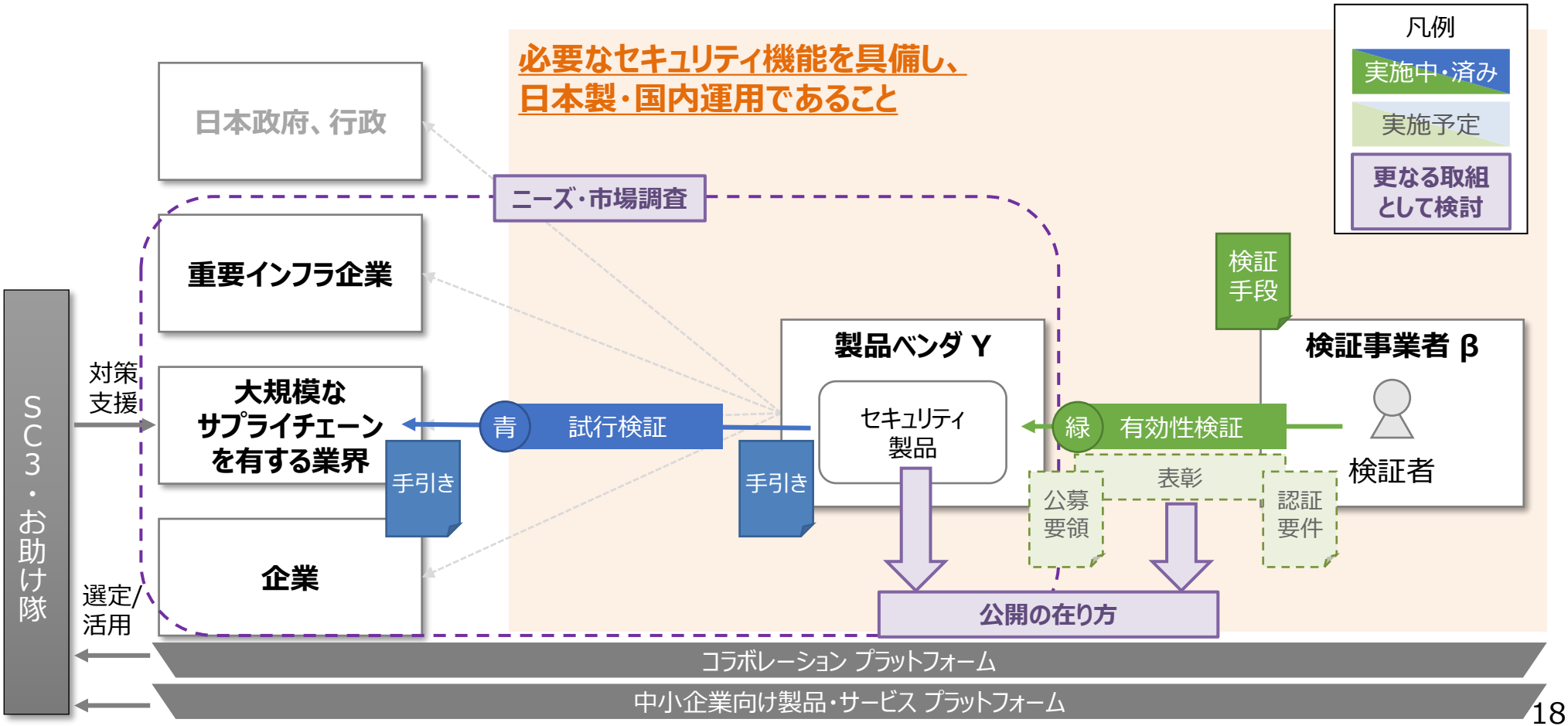
- 今後、関連機関のアセットや既存プログラムを活用し、セキュリティ企業がステージに応じて必要とする支援を、経営/技術/事業の３面から実施する。
- また、IPAによる顧客接点・業界チャネルを活用し、販路開拓・事業化支援を実施する。



今後の方向性

緑 青

- これまで、日本製のセキュリティ製品を対象とし、セキュリティ機能の有効性を確認する手順を整備し、ユーザ企業において試行検証する際の手引き整備した。
- 今後は、市場が求める検証レベルを考慮した機能の有効性検証を実施し、その結果に基づき表彰を行うためのスキームを構築していく予定。
- また、当該表彰結果も含めた有効なセキュリティ製品の公開の在り方や、更なるマッチングに向けたニーズ・市場調査に取り組んでいくことを検討していく。



（２）各施策の現状及び今後の方向性

１．Proven in Japan（検証基盤）

－緑青検証

－赤検証

－開発段階検証（主に中小企業向け）

２．情報セキュリティサービス審査登録制度

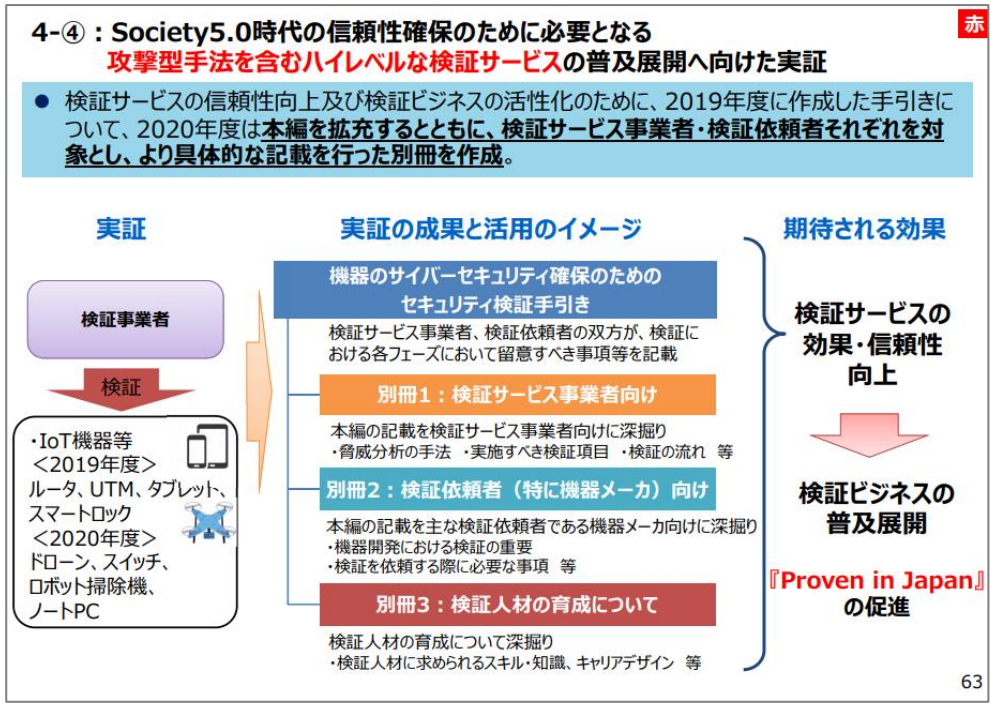
３．サイバーセキュリティお助け隊

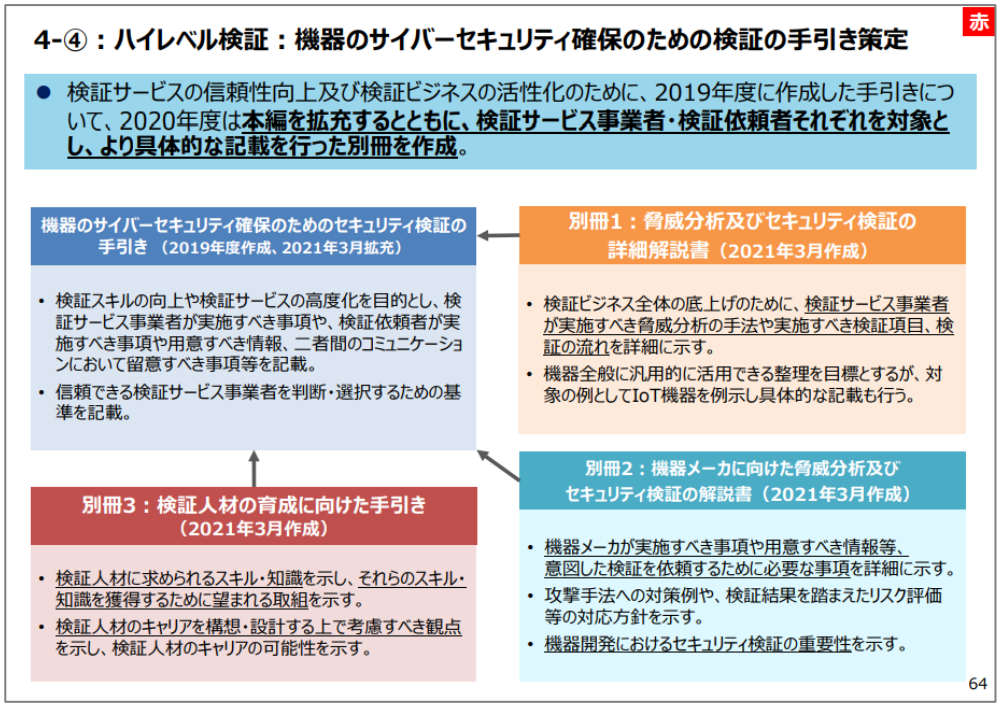
４．中小企業向けセキュリティ製品の検証

５．コラボレーション・プラットフォーム

攻撃型を含めたハイレベルな検証サービスの取組

- 検証サービスの信頼性向上及び検証事業の活性化のために、**本編と3つの別冊によって構成される「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」を策定・公開**した。
- 手引きでは、検証事業者・検証依頼者（機器メーカ）それぞれを対象として、**脅威分析の手法、検証にあたって実施すべき事項、機器メーカが準備すべき事項**等を詳細に記載した。
- また、検証人材の育成に向け、**検証人材に求められるスキル・知識**や、**検証人材のキャリアを構成・設計する上で考慮すべき観点**を整理した。



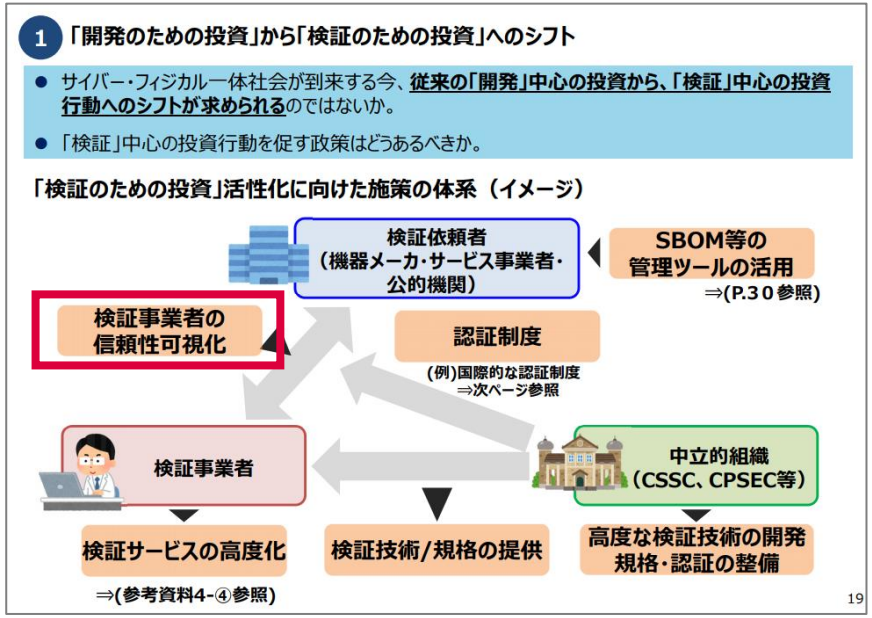


出所）経済産業省「第６回産業サイバーセキュリティ研究会 事務局説明資料」https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/006_03_00.pdf

赤

2021年度の取組

- 検証のための投資を活性化させるためには、**我が国におけるIoT機器等への検証事業の効果・信頼性を向上**し、その**信頼性を可視化**することで、**検証事業の活性化につなげる**ことが必要である。
- これを踏まえ、有識者検討会を設置し、我が国におけるIoT機器等に対する検証事業の効果・信頼性の向上方法や、検証事業者の信頼性を可視化する仕組みについて議論。
- 特に、検証事業者の信頼性を可視化する仕組みの構築に向け、①**検証事業者に求められる信頼性要件、②信頼性可視化方法と信頼できる事業者の選定方法**等に関する論点について、検討会で計3回議論。



2021年度の検討会で議論した5つの論点

1. 「信頼できる検証事業者」に求められる要件は何か。
   また、各要件についてどの程度のレベルが、どの対象に対して求められるか。
2. 構築した仕組みは、どのような目的で、どの依頼者によって活用されるべきか。
3. 検証事業者の信頼性を誰が、どのように確認し、可視化するか。
4. 検証依頼者が、「信頼できる検証事業者」を選定するために必要な仕組みは何か。
5. 「信頼できる検証事業者」に対して、どのようなインセンティブが考えられるか。

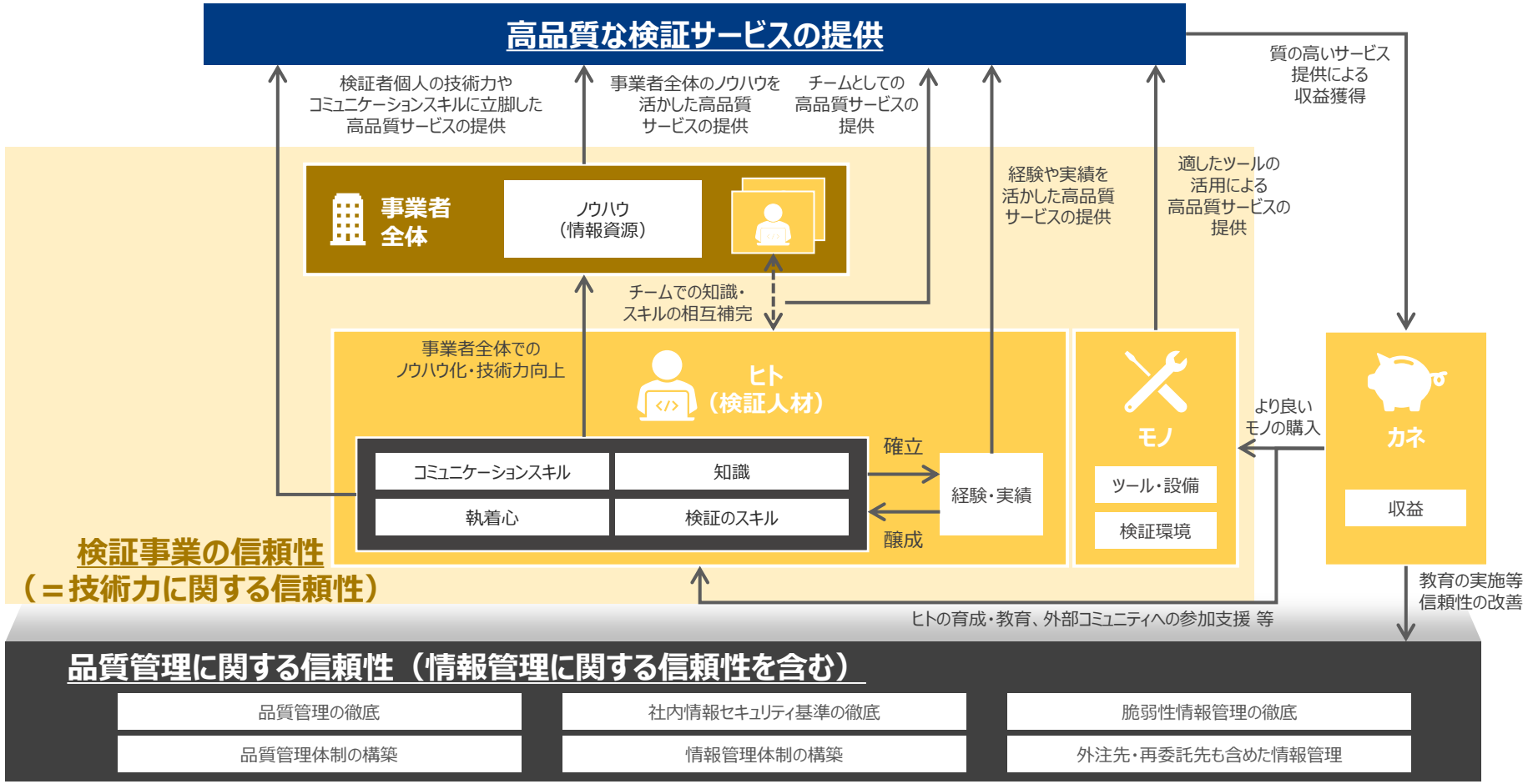
出所）経済産業省「第６回産業サイバーセキュリティ研究会 事務局説明資料」https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/006_03_00.pdf

赤

①検証事業者に求められる信頼性要件

- 信頼できる検証事業者には、**「検証事業の信頼性（＝技術力に関する信頼性）」**、**「情報管理に関する要件」**及びそれらを高い品質で提供する**「品質管理に関する要件」**の**3つの要件区分が求められる。**
- 高品質な検証サービスの提供のためには、「品質管理に関する信頼性（情報管理に関する信頼性を含む）」の基盤の上で、「検証事業の信頼性（＝技術力に関する信頼性）」を確立し、「ヒト・モノ・カネ・情報」の好循環を回すことが必要となる。

検証事業者における信頼性の関係



出所）三菱総合研究所作成

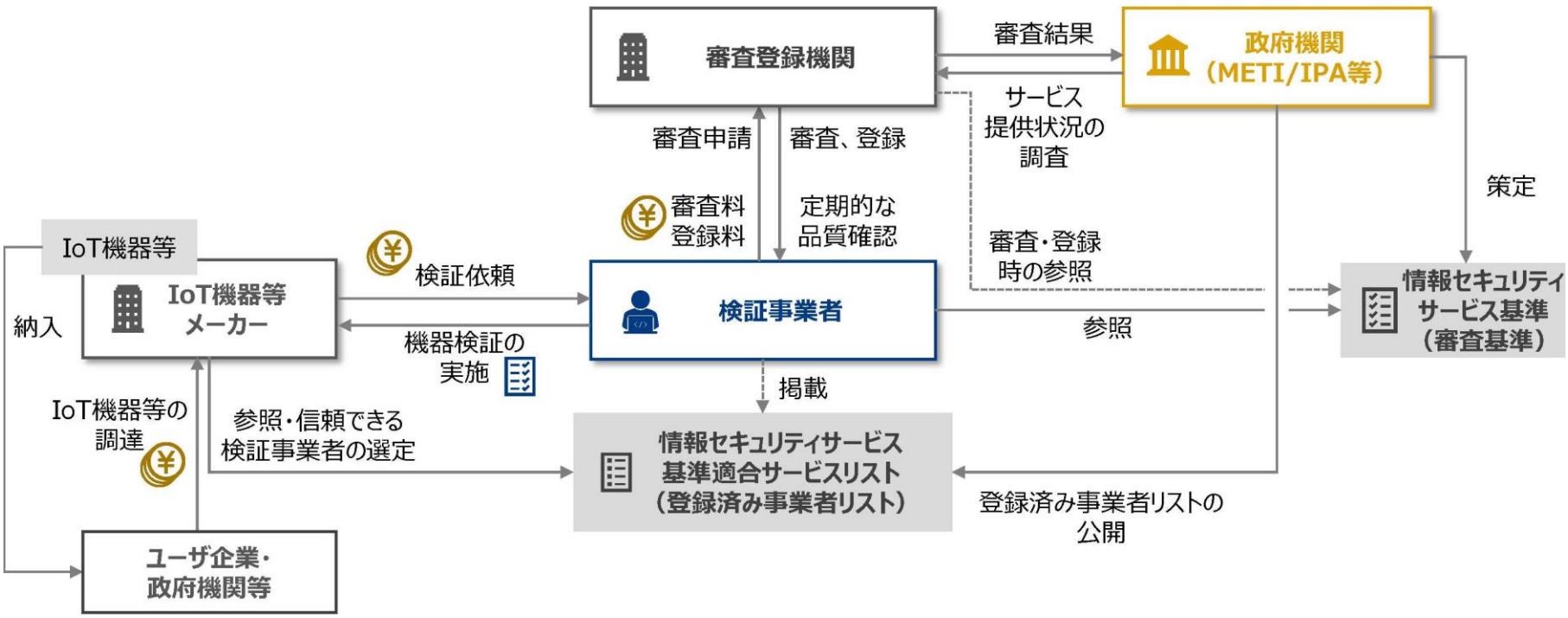
赤

②信頼性可視化方法と信頼できる事業者の選定方法

- 有識者検討会での論点を議論を踏まえ、IoT機器等に対して検証を行う検証事業者の信頼性可視化に当たって、**情報セキュリティサービス審査登録制度に対してIoT機器等に対する「機器検証サービス」を新たに追加できないか検討**を行った。

※審査基準を満たす検証事業者は登録済み事業者リストによって公開される。
検証依頼者はそのリストを参照し、要件に見合う検証事業者を選定することができる。

IoT機器等に対する検証事業者の審査・登録スキーム(案)



※ 本検討では、「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」をIoT機器等とし、このIoT機器等に対して検証を実施する検証事業者の信頼性を可視化することを目的とする。
具体的なIoT機器等として、ネットワーク機器、スマートロック、ドローン、スマート家電、ネットワーク接続するヘルスケア機器等が挙げられる。

赤

（参考）機器検証サービスの審査時に提出を求める書類

- 情報セキュリティサービス審査登録制度の脆弱性診断サービスの審査基準を参考に、機器検証サービスの審査時に提出を求める書類を整理した。

要件区分	要件項目	各要件項目の審査に当たって提出が必要な関連資料
(1) 技術要件	ア　専門性を有する者の在籍状況	• 有資格者リスト（通し番号、氏名、保有資格名称、資格登録番号、有効期限、初登録年、証書の写し） • 研修修了者リスト（通し番号、氏名、研修機関名、研修名、研修終了年月日、証書の写し）
	イ　サービス実施方法の明確化	• サービス内容が明示された資料の写し（HPの写し、サービス仕様が確認できる契約・約款等の写し等） • 機器検証サービスにおける検証結果報告書サンプル
(2) 品質管理要件	ア. 品質管理者の割当状況	• 品質管理者のリスト（通し番号、氏名、所属部署名、役職名、連絡先電話番号、連絡先メールアドレス）
	イ. 品質管理マニュアルの整備	• サービス品質の管理のためのマニュアルや規則等の表紙及び目次 • 審査基準項目の記述箇所が確認できるもの（該当部分のコピー等）
	ウ. 品質の維持・向上に関する手続等の導入状況	• 機器検証サービスに従事するものの教育・研修等の実施又は受講状況リスト（通し番号、氏名、教育・研修等の名称、実施機関名、種別、受講等の時間又はCPEポイント、開始時期、終了時期）

審査の申請及び登録の際に必要となる情報
（審査の対象ではない）

- 申請企業の情報・連絡先
- 機器検証サービスに関するURL、又はホームページの写し
- 審査機関に対する誓約書
- IPAに対する誓約書
- サービス概要
- 主たる顧客対象の分野・業種
- 過去に機器検証サービスにて検証を実施した実績のある機器

赤字は、「脆弱性診断サービス」の「情報セキュリティサービス基準」の要件分類に対して、新たに追加した要件分類、
青字は、同要件分類の内容を一部修正した要件を意味する。

赤

（参考）検証事業者毎に検証実績のある機器の情報を掲載

- 検証依頼者である機器メーカーが自社の製品の検証に適した検証事業者を選定できるよう、情報セキュリティサービス基準適合サービスリストにおいて、登録された各検証事業者の主たる顧客対象の分野・業種や、過去に機器検証サービスにて検証を実施した実績のある機器について記載することを想定。
- 登録済み事業者リストでは、各事業者において実績のある機器に関する情報を示す。
  ただし、審査の実現性の観点より、実施件数割合等を併記せず、機器名称のみを示す。
- また、過去の検証実績は審査対象ではなく、事業者の申告内容に基づき審査登録機関やIPAがリストで明記する形式とする。

情報セキュリティサービス基準適合サービスリストの記載イメージ

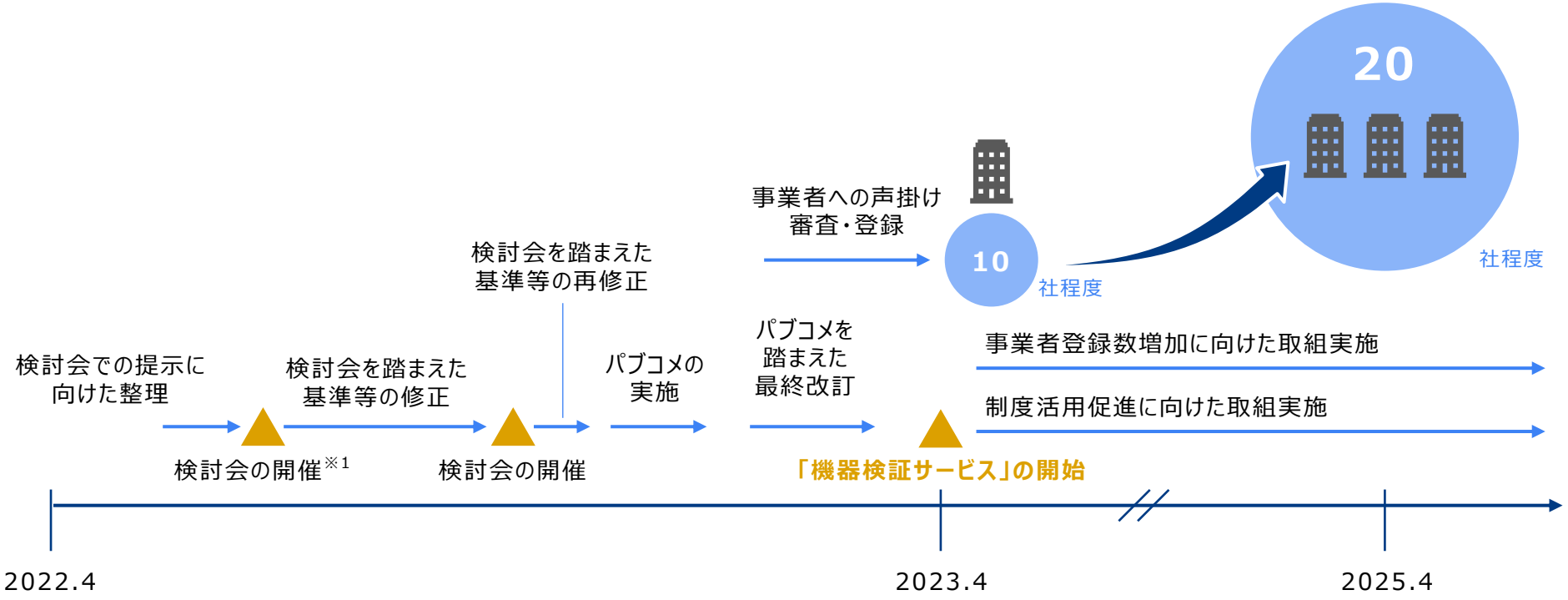
サービス名称	サービス毎のURL	事業者名称	事業者所在地	サービス概要	主たる顧客対象の分野・業種	過去に機器検証サービスにて検証を実施した実績のある機器	対象とする地域	登録年月日	有効期限	審査登録機関名
IoTセキュリティ診断	https://www.example.com	株式会社XXセキュリティ	東京都千代田区Y-Y-Y	IoTセキュリティ診断では、IoTの機器のセキュリティ対策の妥当性や脆弱性有無を確認することで、製品販売前の対策の計画や製品のロードマップ活[illegible]が可能です。	機械・電機・精密機器、自動車・輸送機器、医薬品・医療関連・化粧品	スマートロック、ドローン、Webカメラ、ルーター、ハブ・スイッチ、医療機器、カーナビゲーション	日本全国	2021/10/19	2023/1018	●●

機器メーカーが自社の製品の検証に適した検証事業者を選定できるよう、
登録された検証事業者の主たる顧客対象の分野・業種や、
過去に機器検証サービスにて検証を実施した実績のある機器を明記

今後の方向性①　機器検証サービスの運用開始に向けて

- 2021年度に検討した審査基準に基づき、**今後、情報セキュリティサービス基準に新たに「機器検証サービス」を追加**するとともに、情報セキュリティサービス審査登録制度に基づき、検証事業者の登録及び情報セキュリティサービス基準適合サービスリストの公開を通じて、**機器メーカーが検証を実施する際に信頼性のある検証事業者を確認できる仕組みを構築**する。
- **2023年度より制度運用開始**、2025年度には20社程度が登録することを想定。
- あわせて、製品の信頼性を向上させていくための仕組み（製品ラベル等）も検討。

情報セキュリティサービス審査登録制度へ「機器検証サービス」を追加するプロセス（イメージ）



※1「情報セキュリティサービス普及促進に関する検討会」のこと。情報セキュリティサービスを普及させるための方策及び基準の見直し等に関する検討を行うことを目的として設置。
※2「デジタルフォレンジックサービス」の登録者数について、制度開始後一年以内に16社が登録、制度開始後三年後には28社の登録がなされている。
今回の「機器検証サービス」は脆弱性診断サービスと比較して現状の市場が限定的であるため、登録数は少なくなるが、「脆弱性診断サービス」と同等の伸び率で登録社を増やすことが期待される。

赤

（参考）製品に対するセキュリティラベリング制度

- 諸外国においては、適切なセキュリティ対策が施された製品の導入を促進するための製品に対するセキュリティラベリング制度が検討されている。
- 近年では、**適切なセキュリティ対策が施された製品の導入を促進するために、製品に対するセキュリティラベリング制度が検討**されている。**既にシンガポールやフィンランドで制度が開始**しているほか、**米国においても制度構築が検討**されている。

機器のセキュリティ確保・向上を支援する海外政府機関による代表的な取組

主体	取組名称	概要	目的	時期
NIST	“NISTIR 8259”の策定	IoT機器のメーカーに推奨されるサイバーセキュリティに関連する活動を整理したガイドライン。	IoT機器メーカーが開発する製品の安全性を向上させるための推奨事項を示すこと。	2020年5月29日
NIST	Cybersecurity Labeling for Consumer IoT Products	2021年5月の米国大統領令によって指示された、IoT製品の安全性を確認するためのラベリング制度。これまで、NISTにより、ラベリング制度構築に向けた推奨事項の検討等がなされている。	一般消費者がIoT製品の安全性を判断できるよう、セキュアな製品に対してラベルを付与すること。	2022年2月4日に推奨事項に関する文書が公開
ENISA	Cybersecurity Certification (EUCC Candidate Scheme)	ICT機器を対象とするCommon CriteriaとISO/IEC 18045に基づく欧州サイバーセキュリティ認証フレームワークにおける候補スキーム。	欧州のSOG-IS※4の下で運用されていた既存のCCスキームの後継として機能させること。	2021年5月25日にV1.1.1が公開
DCMS※1	“Code of Practice for Consumer IoT Security”の策定	消費者向けIoT機器及び関連サービスのセキュリティ確保のために機器メーカーが実施すべき13項目を行動規範としてまとめたもの。本規範に基づきEN 303 645が策定。	消費者向けIoT製品の開発、製造、販売に携わる利害関係者を支援すること。	2018年10月14日
DCMS	“Product Security and Telecommunications Infrastructure”法案の提出	インターネットに接続するIoT機器に対して、機器導入時のデフォルトパスワードの禁止等を義務化する法案。遵守しない企業に対する罰金に関する条項も含まれている。	インターネットに接続されるIoT製品に対して、脆弱性の悪用によるサイバー攻撃を防ぐための最低限の対策を求めること。	2021年11月24日庶民院に提出
CSA※2	Cybersecurity Labelling Scheme (CLS)	セキュリティ要件を満足している消費者向けIoT製品（ネットワーク接続する製品）に対してラベリングを行う制度。	消費者がより安全なIoT製品を購入・利用できるようにすること。	2020年10月開始
TRAFICOM※3	Finnish Cybersecurity Label	セキュリティ要件を満足している消費者向けIoT製品（ネットワーク接続する製品）に対してラベリングを行う制度。	製品に対する脅威に対応し、安全な環境で消費者が製品を利用できるようにすること。	2019年11月開始

出所）海外政府機関による取組に関する公開情報に基づき三菱総合研究所作成

※1：英国デジタル・文化・メディア・スポーツ省
※2：シンガポールサイバーセキュリティ庁
※3：フィンランド運輸通信庁
※4：欧州におけるCC加盟国の認証機関間の調整を行う組織

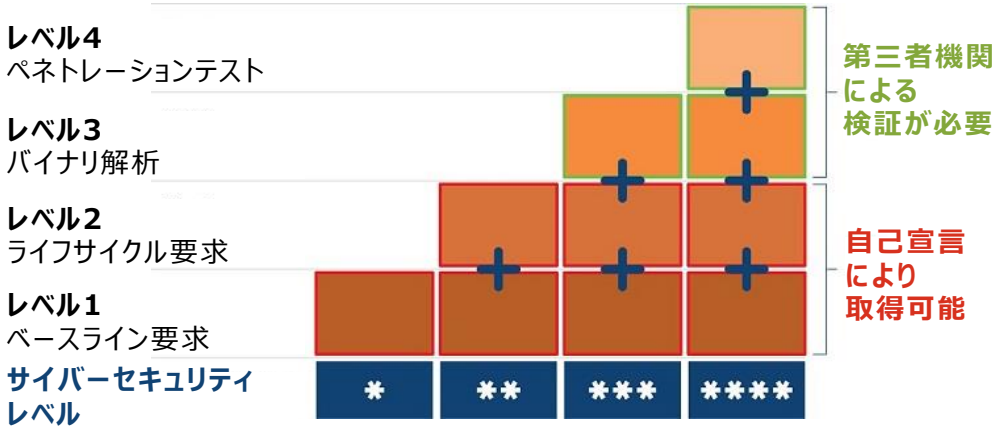
赤

（参考）シンガポールにおけるラベリング制度の事例

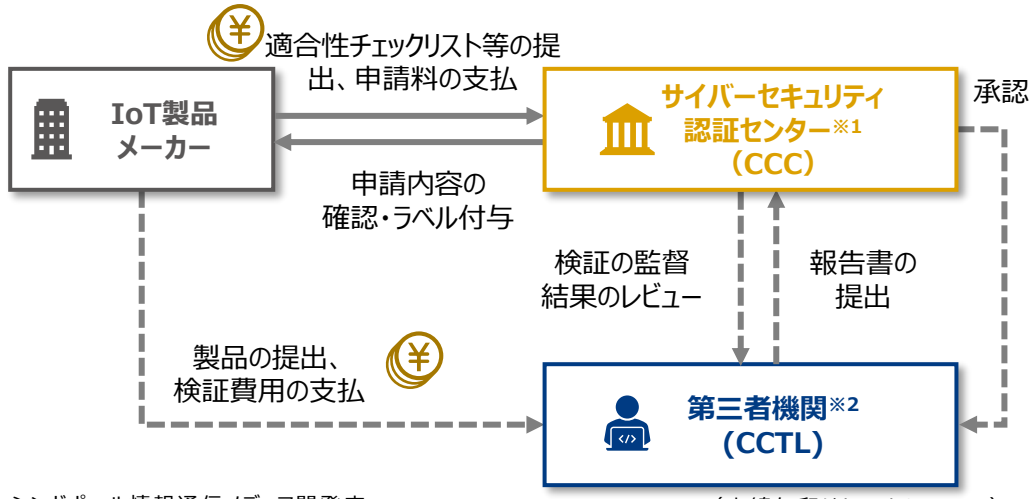
- シンガポールCSAは2020年10月より、サイバーセキュリティ要件を満足している消費者向けIoT製品に対する4段階のラベリング制度を運用している。

- ラベルは4段階に分かれ、**レベル1・2は開発者の自己宣言で取得可能**、**レベル3・4では第三者機関による検証が必要**となる。
- ラベルを取得するためには**ETSI EN 303 645の要件に加え**、**レベル2以降はIMDA※1が策定したガイドラインに基づくライフサイクル要件に満足する必要**がある。そして、**レベル3では第三者機関によるファームウェア及びモバイルアプリに対するバイナリ解析**、**レベル4では機器に対するペネトレーションテスト**にクリアする必要がある。
- ラベルの期間は3年であり、申請料はレベル1でS$53、レベル2でS$418、レベル3でS$1,080、レベル4でS$3,810である。（すべてシンガポールドル。また、レベル3・4は第三者機関に対する検証費用が別途必要となる。）
- **2022年2月時点（制度開始後16ヶ月）で55製品がラベルを取得**している。また、2021年10月には**フィンランドTRAFICOMのFinnish Cybersecurity Labelとの相互運用を発表**した。
- なお、CSAは**IoT製品に対するラベル取得の必須化を検討**している。

企画・設計段階、製造段階でのセキュリティ方針・基準の有無



脆弱性対策の実施状況



※1：シンガポール情報通信メディア開発庁
※2：CSAの一組織である本制度のスキームオーナー。
※3：Common Criteria Test Laboratoryの略で、ISO/IEC 17025の認定を受けている必要がある。

出所）CSA Cybersecurity Labelling Scheme（CLS）に関する公開情報に基づき三菱総合研究所作成

（参考）2022/3/7　赤検証有識者検討会で頂いたご意見

- 2021年度 第3回赤検証有識者検討会で頂いたご意見のなかで、人材確保や検証ラボ、検証センターに関するものは以下の通り。

主なご意見

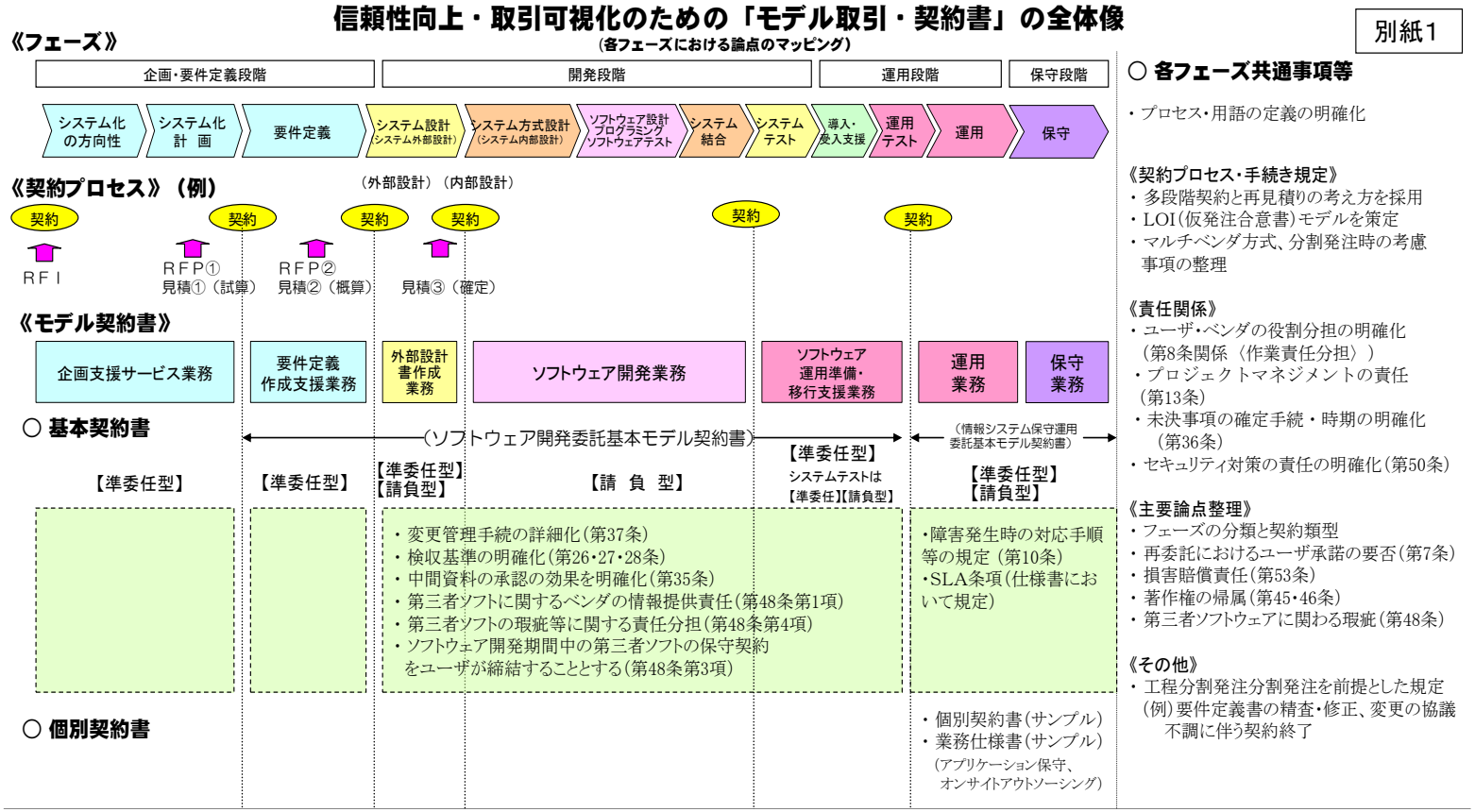
- 人材育成を行ううえでは、知識（座学や動画で学べる教材）と環境（アクセスすれば誰でも自由に攻撃ができるラボやアップデート系やハードコーディング回避などの基本的な実装方法を経験できる場）と経験（攻撃手法と対策方法）が必要である。**知識の形成を促進するほか、攻撃手法やベストプラクティスのような基本的な事項を学べる環境で経験をつけていただくことが重要**である。
- 人材育成において、スキルを表すことは重要だと考えている。JNSAのSecBoKでは、脆弱性診断士に求められるスキルが可視化されている。IoT機器の検証については未対応であるが、今後連携できれば良いと考えている。
- 人材が不足している中で、信頼できる仲間と脆弱性情報といった機微な情報の交換ができるコミュニティ形成を推進していく必要がある。**検証、分析、解析等ができる環境も含めた場づくりが求められる。**
- IPAのICSCoEの中核人材育成プログラムのような若い世代の人材育成を高等教育でも実施していく必要があると感じた。IoTの分野に関する専門教育はまだ存在しない。
- IoTの検証センターは7，8年前から沖縄県で既に運用されている。**検証センターは国内に複数個所あっても良い。**日本国内でも、組み込み系の特定の分野に強い企業が集まっている地域が点在している。**業界や業種ごとに検証センターがあった方が良い**と感じた。
- 中小の機器メーカーが開発を行う際に必要となる検査ツール等を用意したビジネス拠点の設置には、ビルのワンフロア程度のスペースを用意したり、運営を行う事務局を設置したりする必要がある。
- **海外の検証会社は、輸出の関係で港湾都市に集中**している。検証センターは港や製造の拠点に近いところに設置するのが良いと思われる。**安全保障の観点から、日本で検査した製品に、信用性といった付加価値がつくことが考えられる。**

赤

今後の方向性②　機器検証に関するモデル契約書の作成

- 検証事業の発展を見込み、**検証事業者と検証依頼者間の適切な契約を担保するために、脆弱性診断や機器検証に関する内容を含んだ同様の文書を作成**することを検討する。

※現状では脆弱性診断や機器検証に関する契約内容は含まれていない

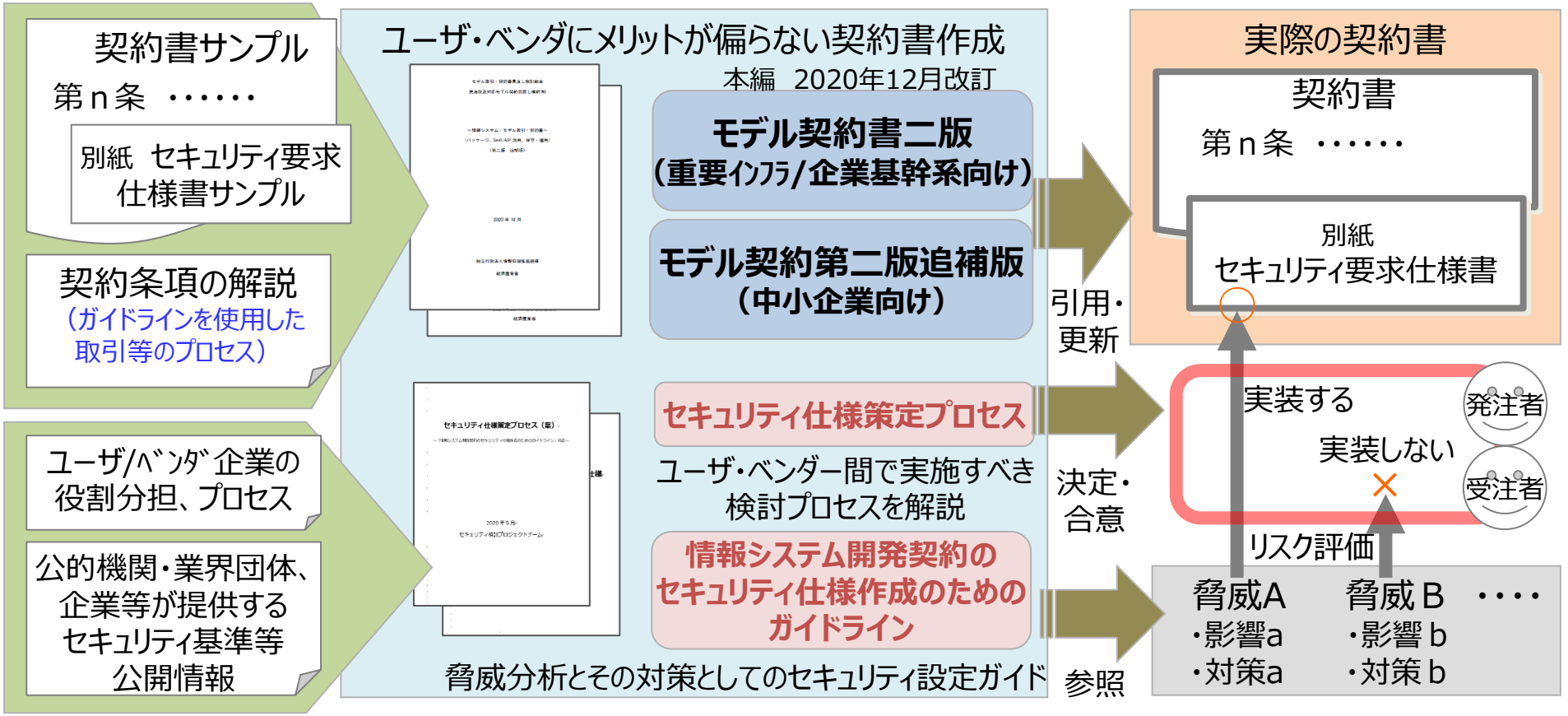


出所）IPA、「情報システム・モデル取引・契約書」
https://www.ipa.go.jp/ikc/reports/20201222.html

赤

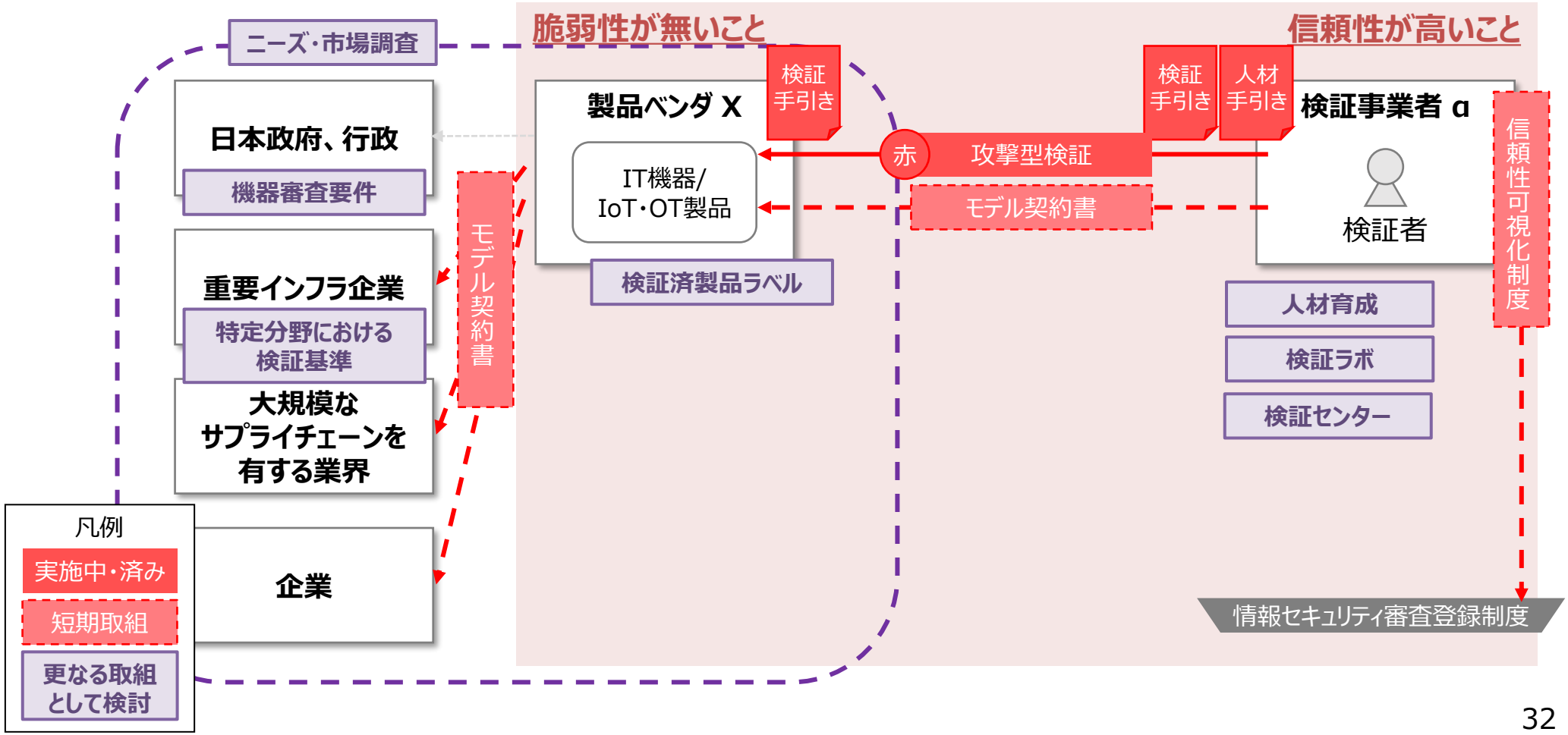
（参考）モデル契約書

- ユーザとベンダの各工程での責務・役割分担等が曖昧である事に起因するシステムトラブルが多発しており、契約の段階から開発・導入手順等の共通理解が重要となっている。
- セキュリティ仕様書の作成プロセスを定義し、想定される脅威と対策、契約書サンプルのチェック項目毎に合意形成をとる為のテンプレートを整備した。



今後の方向性のまとめ

- これまで、主に検証事業者側で必要となる事項（機器検証の実施手順、検証事業者の信頼性可視化制度）の整備に取り組んできた。
- また、信頼性可視化制度の情報セキュリティ審査登録制度への反映等、検証事業者の信頼性向上に向けた取組を引き続き実施していく。
- さらに、更なる検証サービスの普及に向けて、検証サービスを利用する側や検証された機器を使用する側といった**検証サービスの需要を喚起する取組**（ユーザの調達ルールや検証済製品ラベルの検討、等）の検討を行っていく。



（２）各施策の現状及び今後の方向性

１．Proven in Japan（検証基盤）

- 緑青検証
- 赤検証
- **開発段階検証（主に中小企業向け）**

２．情報セキュリティサービス審査登録制度

３．サイバーセキュリティお助け隊

４．中小企業向けセキュリティ製品の検証

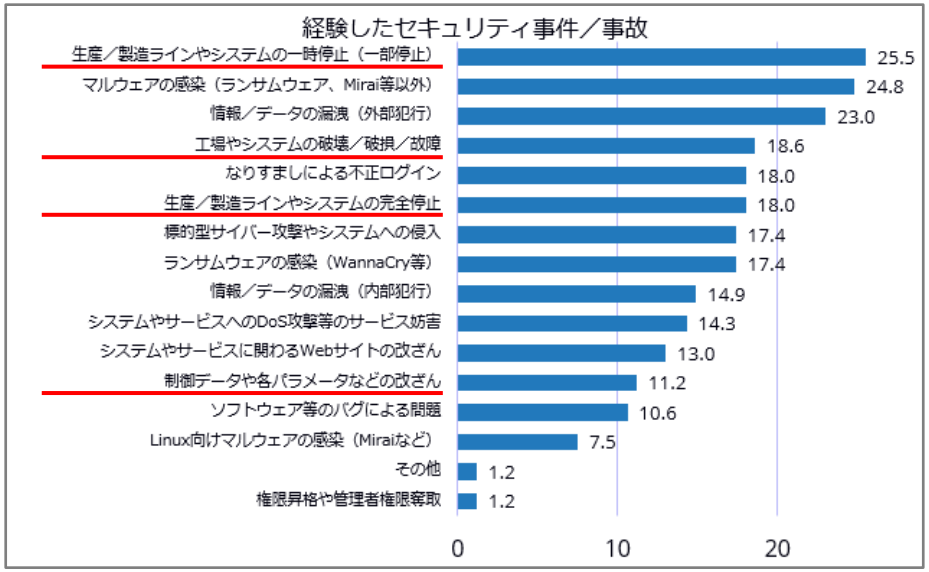
５．コラボレーション・プラットフォーム

開

IoT機器に対するセキュリティ対策の必要性

- DXの進展により、インターネットとIoT機器が繋がり始めたところであるものの、**セキュリティ事件/事故によるIoT機器やOTシステムの一時停止を約25%の企業が経験**しているといった調査結果からも、**こうした機器やシステムでセキュリティ対策を多くの者が導入しているとは言い難い**状況。
- 機器に対する十分なセキュリティ対策が実施されず、脆弱性が残存した場合、悪意ある攻撃者によって不正操作や誤作動が実行され、**機器の利用者へ影響を及ぼす恐れ**がある。
- また、**開発企業は脆弱性の対応に追われる**こととなる。過去には、**脆弱性によりリコールや利用者による訴訟に発展した事例**もあり、最悪の場合、**開発企業の経営に対して影響を与える可能性**もある。
- 今後さらなる脅威の増加・高度化が想定されるところ、**機器に対するセキュリティ対策の具備が不可欠**。

2021年 国内企業のIoT/OTセキュリティ対策実態調査結果



セキュリティ対策の不備により開発企業に影響を及ぼした事例

自動車における脆弱性の検出による140万台のリコール

販売中の自動車に対して外部から不正アクセス可能な脆弱性が公開された。**顧客からの問い合わせが殺到し、開発企業は140万台のリコールを実施**した。**リコールの対応には1,000万ドル以上の費用**を要した。

心臓ペースメーカーにおける脆弱性の検出による46.5万台のリコール

販売中の心臓ペースメーカーに対して心拍リズムを外部から制御可能な脆弱性が公開された。**開発企業は市場に流通している46.5万台を対象にリコールを実施**した。

脆弱な家庭用ネットワークカメラのメーカに対する訴訟

家庭用ネットワークカメラにおいて、認証不備に関する脆弱性が内在し、脆弱性を悪用した不正アクセスが行われた。不正アクセスの被害を受けた複数の利用者により、**開発企業に対して500万ドルを求める集団訴訟**が起こされた。

IDC「2021年 国内企業のIoT/OTセキュリティ対策実態調査」https://www.idc.com/getdoc.jsp?containerId=prJPJ47631521
※ 調査実施：2021年2月、調査対象：国内企業443社

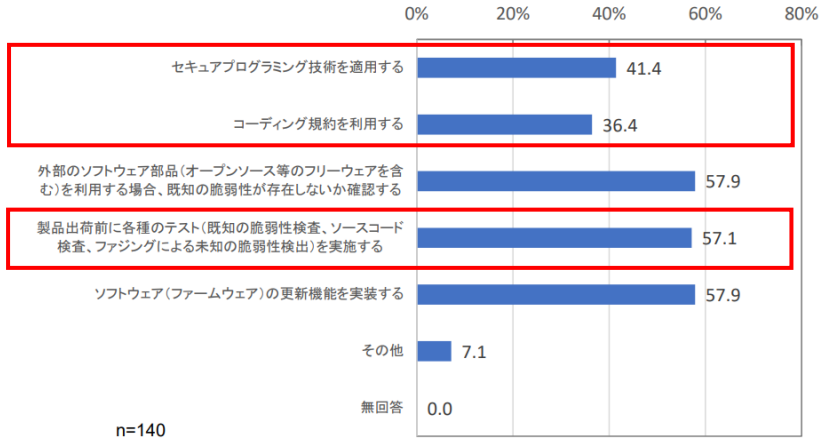
開

IoT機器に対するセキュリティの取組状況・本事業の目的

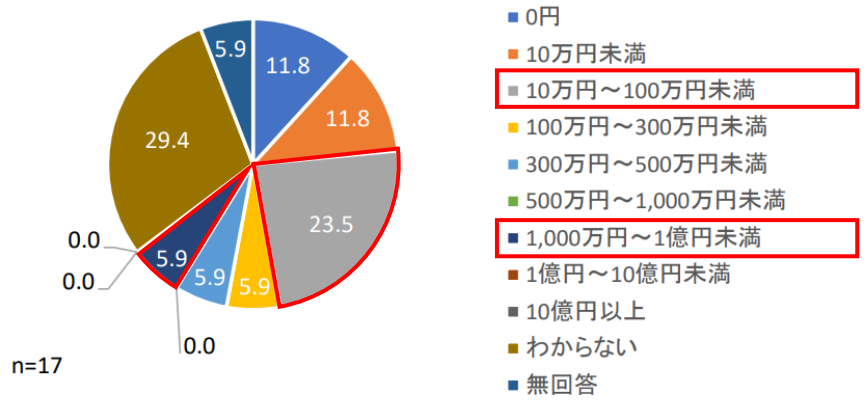
- IoT機器に対するセキュリティの取組においては、「**セキュリティ・バイ・デザイン**」の考えに基づき、設計・開発段階で**セキュリティ対策が適切に導入されていることが必要**。
- 他方で、**開発段階でセキュリティ対策を行っている企業は現状限定的**であり、十分な脆弱性対策が実施されていないことにより、**1,000万円以上の損害に繋がった企業も存在**する。
- 本事業は、セキュリティ・バイ・デザインの考えに立脚し、**開発段階からの脆弱性検証を試験的に実施することで効果的な検証手法を整理する**とともに、**その効果を可視化**し、**中小企業による発売前のIoT機器の脆弱性検証を促進する**ことを目的とする。

IoT機器に対するセキュリティの取組状況

（開発段階の脆弱性対策の考慮内容）



（脆弱性による金銭的な損害）



- **4割以上の企業が機器出荷前に検証を実施していない。**
- **6割程度の企業が開発段階のセキュリティ対策を行っていない。**

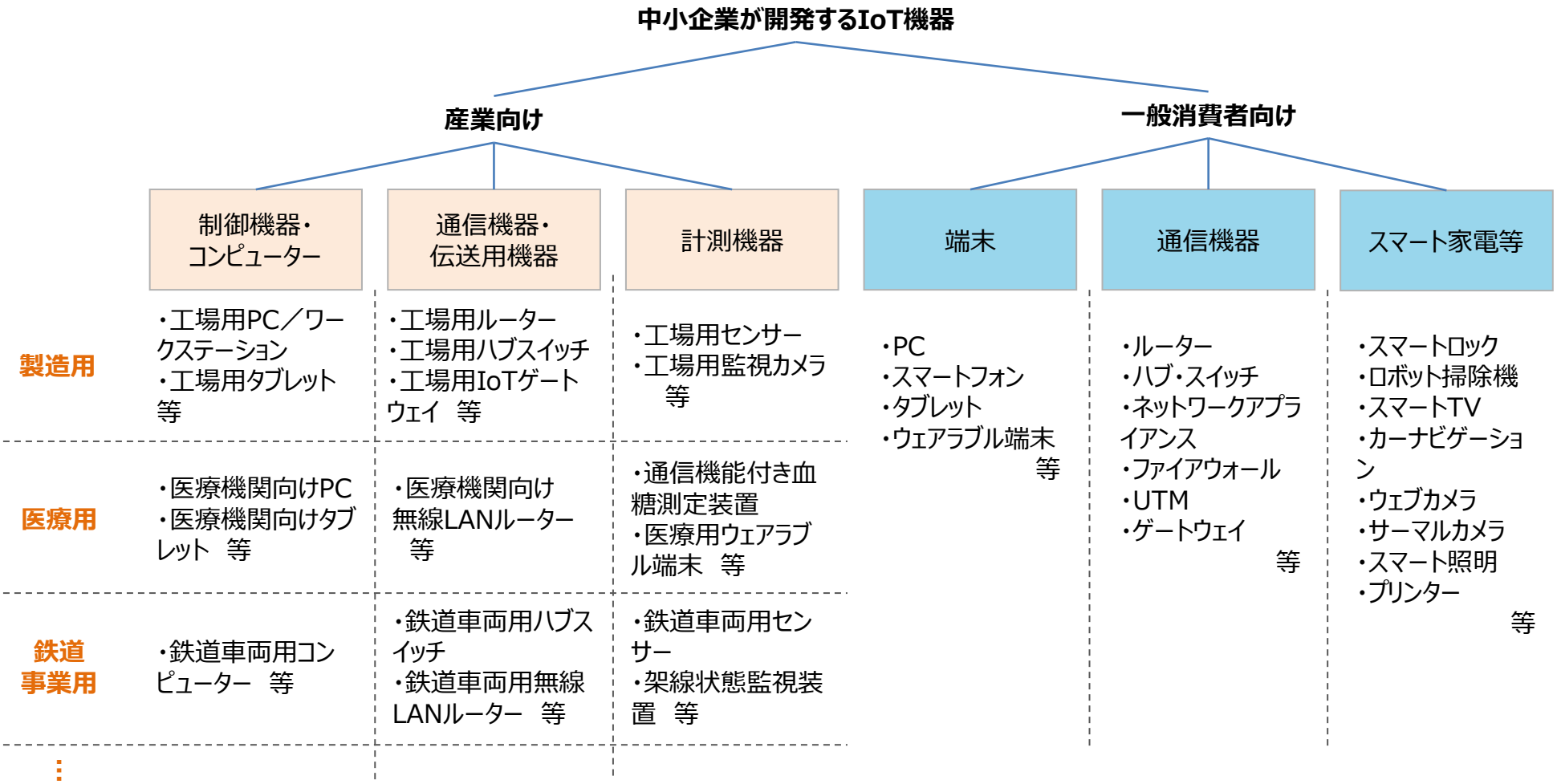
- **10万～100万円未満の損害が最も多いが、1,000万～1億円未満の損害が発生した企業も存在する。**

IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」https://www.ipa.go.jp/files/000065094.pdf
※調査実施：2017年11月、調査対象：国内企業205社

開

本事業で対象とするIoT機器の考え方（類型化）

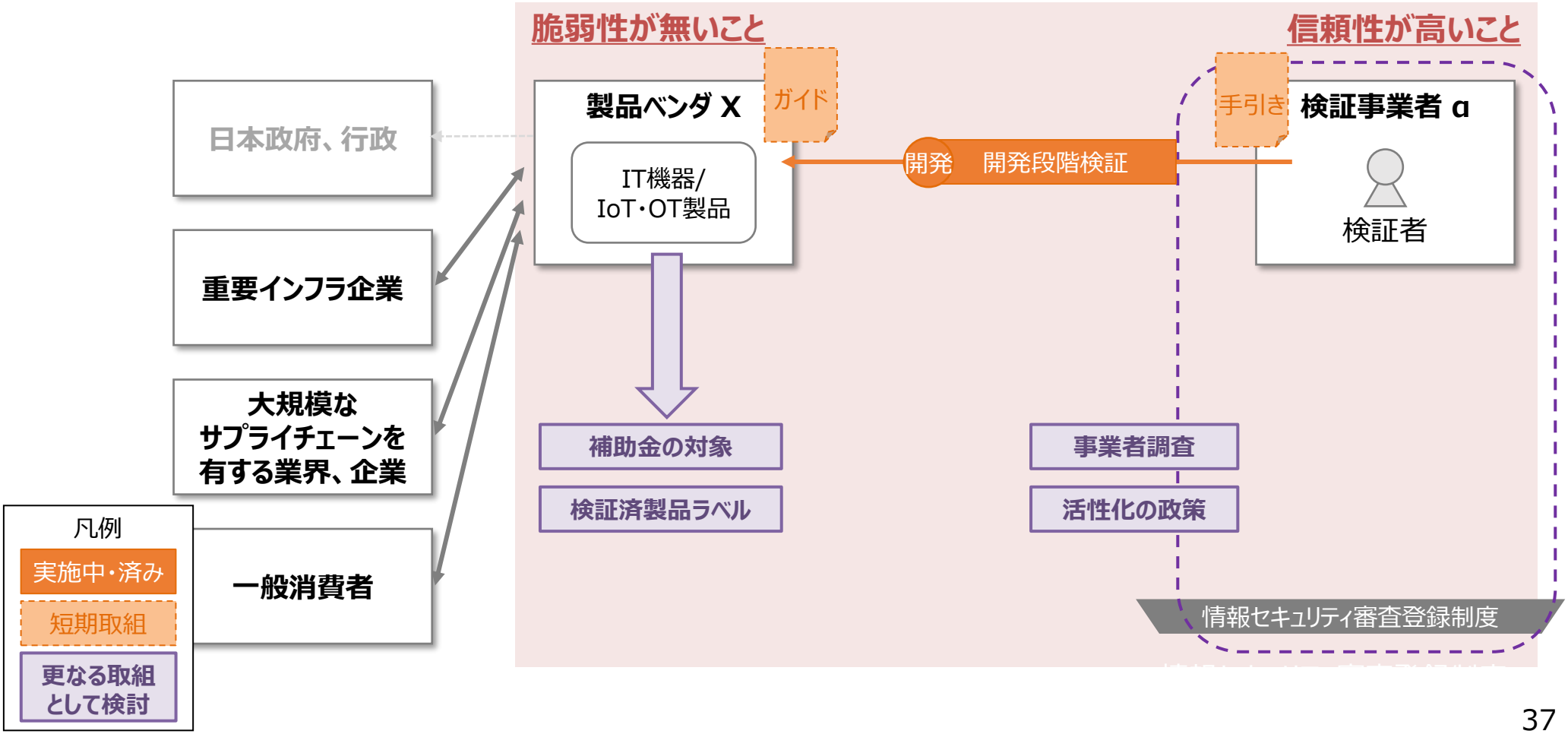
- 中小企業が開発するIoT機器を、**産業向けと一般消費者向けの大きく2つの観点から分類**。
- いずれかに該当するIoT機器に対して、当該機器を開発する中小企業にご協力をいただき、脆弱性検証を実施する。



開

取組まとめ

- 開発段階の製品検証により得られた知見を検証事業者や製品ベンダが参照するための手引きやガイドを整備していく。
- また、製品ベンダのインセンティブとして、検証費用の補助や、検証済製品ラベルの整備等の仕組みを構築することの検討を行っていく。



（２）各施策の現状及び今後の方向性

１．Proven in Japan（検証基盤）
　－緑青検証
　－赤検証
　－開発段階検証（主に中小企業向け）
２．情報セキュリティサービス審査登録制度
３．サイバーセキュリティお助け隊
４．中小企業向けセキュリティ製品の検証
５．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）

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

選定時に活用

審査を受けてリストに掲載

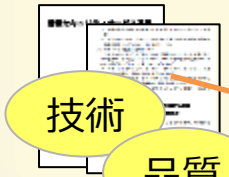
○情報セキュリティサービス基準適合サービスリスト（IPA）

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247サービスが掲載

- 情報セキュリティ監査（67サービス）
- 脆弱性診断（107サービス）
- デジタルフォレンジック（28サービス）
- セキュリティ監視・運用（45サービス）

2021年12月現在



○情報セキュリティサービス基準（METI）

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

（参考）登録サービス事業者の所在地の内訳

- **情報セキュリティ監査**（67サービス）　東京50、神奈川8、埼玉2、兵庫2、千葉1、新潟1、京都1、大阪1、広島1
- **脆弱性診断**（107サービス）　東京84、神奈川7、大阪3、兵庫3、新潟2、福岡2、宮城1、茨城1、千葉1、富山1、徳島1、沖縄1
- **デジタルフォレンジック**（28サービス）　東京23、神奈川3、兵庫1、熊本1
- **セキュリティ監視・運用**（45サービス）　東京36、神奈川5、大阪2、兵庫1、福岡1

「情報セキュリティサービス基準」の改訂

- 関係団体等からの基準見直し要望を踏まえ、2018年6月「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審査登録機関基準」の初版公表以来、**初めての基準改訂を実施。**

＜改訂方針＞

- 主に２点を実施する目的で改訂を実施。
  - 基準中には、頻繁な改定を避けるためツール名などを極力入れない。
  - 審査において、抽象的な定義のみでは判断できないため、具体的な定義とする。
- 現在「附則」になっているもののうち、見直し需要の高い以下の各項を基準から切り離す。
  - ① 資格要件
  - ② 専門家コミュニティ
  - ③ 研修受講実績
  - ④ 参照する基準
  - ⑤ 継続教育
- 切り離した①～⑤は、「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示」の名称にて、IPAの基準適合サービスリストのページに表示し、別途設置する有識者検討会で保守する。

2022年１月31日改訂版公表、2022年４月１日施行

「情報セキュリティサービス基準」 サービス区分毎の主な改訂内容

- 関連団体からの意見、パブリックコメント等を踏まえ、以下の見直しを実施。
- その他、資格を「専門資格」と「汎用資格」に分けて表示。

＜主な改訂内容＞

サービス区分	改訂対象	内容
セキュリティ監査	（なし）	
脆弱性診断	技術要件	●「専門性を有する者の在籍状況」の要件のうち、資格の例示に「OSCP」を追加 ●「サービス提供に用いる基準」の要件のうち、Webアプリケーション及びプラットフォームの脆弱性診断に用いるツールの例示の見直し
デジタル フォレンジック	技術要件	●「専門性を有する者の在籍状況」の要件のうち、資格の例示に「デジタル・フォレンジック資格（CDFP-B、CDFP-P、CDFP-M）」を追加 ●「専門性を有する者の在籍状況」の要件のうち、研修の例示に特定非営利活動法人デジタル・フォレンジック研究会が実施する「IDF講習会」の受講、資格(CDFP)維持に関わる継続的教育の受講を追加
セキュリティ監視・運用	技術要件	●「専門性を有する者の在籍状況」の要件のうち、資格の例示に「CND」を追加 ●「セキュリティ監視・運用サービスの提供において準拠する右に例示する内容及びその明示方法」の例示に、ISOG-J発行の『マネージドセキュリティサービス（MSS）選定ガイドライン（MSS選定ガイドライン）Ver.2.0』P22の記載内容を反映

（注）汎用資格：情報セキュリティ分野の幅広い知識を有することを証する資格の例示
専用資格：当該サービスの提供に関する専門的な知識を有することを証する資格の例示

「情報セキュリティサービスに関する審査登録機関基準」の改訂

＜主な改訂内容＞
下記青文字の追加

第２　用語及び定義
（４）情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示
経済産業省が定めた情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示をいう。

第６　審査手続
１　審査の基準
審査登録機関は，経済産業省が定める**最新の**「情報セキュリティサービス基準」に基づいて審査・登録を行わなければならない。

４　審査
(1) 審査登録機関は，規則において，情報セキュリティサービス基準**並びに審査を行う年度の４月１日時点で有効である情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示**に基づき申請者が必要となる資格要件等について，判断の指針となる内容を定めなければならない。

13　苦情及び異議申立て
(5) 審査登録機関は，利害抵触がないことを確実にするために，**申請日の所属する年度の４月１日より過去**２年以内に申請者にコンサルティングを提供した要員又は申請者に雇用された要員を，この申請者に対する苦情又は異議申立ての解決のレビュー又は承認に従事させてはならない。

2022年１月31日改訂版公表、2022年４月１日施行

今後の取組

	取組	実施予定事項	論点
1	サービス追加、制度普及方策（マッチング等）の検討	**前回のWG3で示されたサービスカテゴリの拡大を踏まえ**、パブコメで意見があった**「インシデントレスポンスサービス」、「ペネトレーションテストサービス」、「IoT脆弱性診断サービス」**、赤検証事業で示された**「機器検証サービス」**などは将来的に登録ニーズが高まると見込まれるが、審査対象にできるようにするためにあらかじめどのような点を明らかにする必要があるか検討する。 また、悪質なサービスを排除する目的の本制度を補完する仕組みの必要要否、実行方法を検討する。	登録可能とするために明らかにすべき項目 ➢ サービスの定義（スコープ） ➢ 技術要件（要員に求めるスキルや経験、仕様として明らかにすべきこと） ➢ 品質管理要件（品質管理マニュアルに記載すべきこと） サービス基準の改訂要否、ユーザー評価等の導入など
2	情報セキュリティサービス基準適合サービスリストの様式等改訂	以下の２点について見直しを実施する。 ① 情報セキュリティサービス基準適合サービスリストに**「再委託によるサービス提供」をしている旨を表示する欄を設ける。** ② IPA及び審査登録機関における情報セキュリティサービス基準適合サービスリストの掲載ページに以下の注釈を表示する。 「本制度はサービス提供事業者の技術的能力と品質管理体制の２つの観点のみについて一定の要件を満たしていることを示すものであり、それ以外の観点（サービスの継続性等）については別の方法で評価を行う必要がある。」	実施時期の目標をどうするか（以下の各点を踏まえる必要がある） ➢ IPA及び審査登録機関における事務対応 ➢ 技術的な仕様変更等の対応に要する期間 ➢ 登録事業者への告知
3	例示の更新要否の検討	● 見直しの頻度：年１回更新の必要性を判断 （更新は不要、という判断でもよい） ● 見直しを行う例： ➢新たなガイドラインや資格制度が整備された ➢サービスで用いられるデファクト標準ツールが変化した ➢オープンソースのツールが更新されなくなった	ー

（２）各施策の現状及び今後の方向性

１．Proven in Japan（検証基盤）
　－緑青検証
　－赤検証
　－開発段階検証（主に中小企業向け）
２．情報セキュリティサービス審査登録制度
３．サイバーセキュリティお助け隊
４．中小企業向けセキュリティ製品の検証
５．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サービス

- 2019年度・2020年度実証事業で得られた知見に基づき、実証参加事業者がサービスを開発。
- サービス普及に向け、2021年度よりサービスブランドを設立。2022年３月時点で12サービスが登録。サービス審査登録制度の運営とともに、中小企業の意識啓発・サプライチェーンによる普及などの施策と一体となった普及施策の展開。

中小企業のサイバーセキュリティ対策に不可欠な各種サービス

- EDR・UTMによる異常監視
- 緊急時の対応支援・駆け付けサービス
- 相談窓口
- 簡易サイバー保険
- 簡単な導入・運用

中小企業でも導入・維持できる価格でワンパッケージで提供

サイバーセキュリティお助け隊サービスウェブページ（2021/11/10公開）
https://www.ipa.go.jp/security/otasuketai-pr/

お助け隊サービス審査登録制度：
一定の基準を満たすサービスにお助け隊マークの商標利用権を付与

お助け隊サービスA
お助け隊サービスB
お助け隊サービスC

サービス提供 → 中小企業 → 自社の信頼性をアピール → 取引先（大企業等）

サイバーセキュリティ お助け隊

お助け隊サービス利用の推奨等の中小企業の取組支援

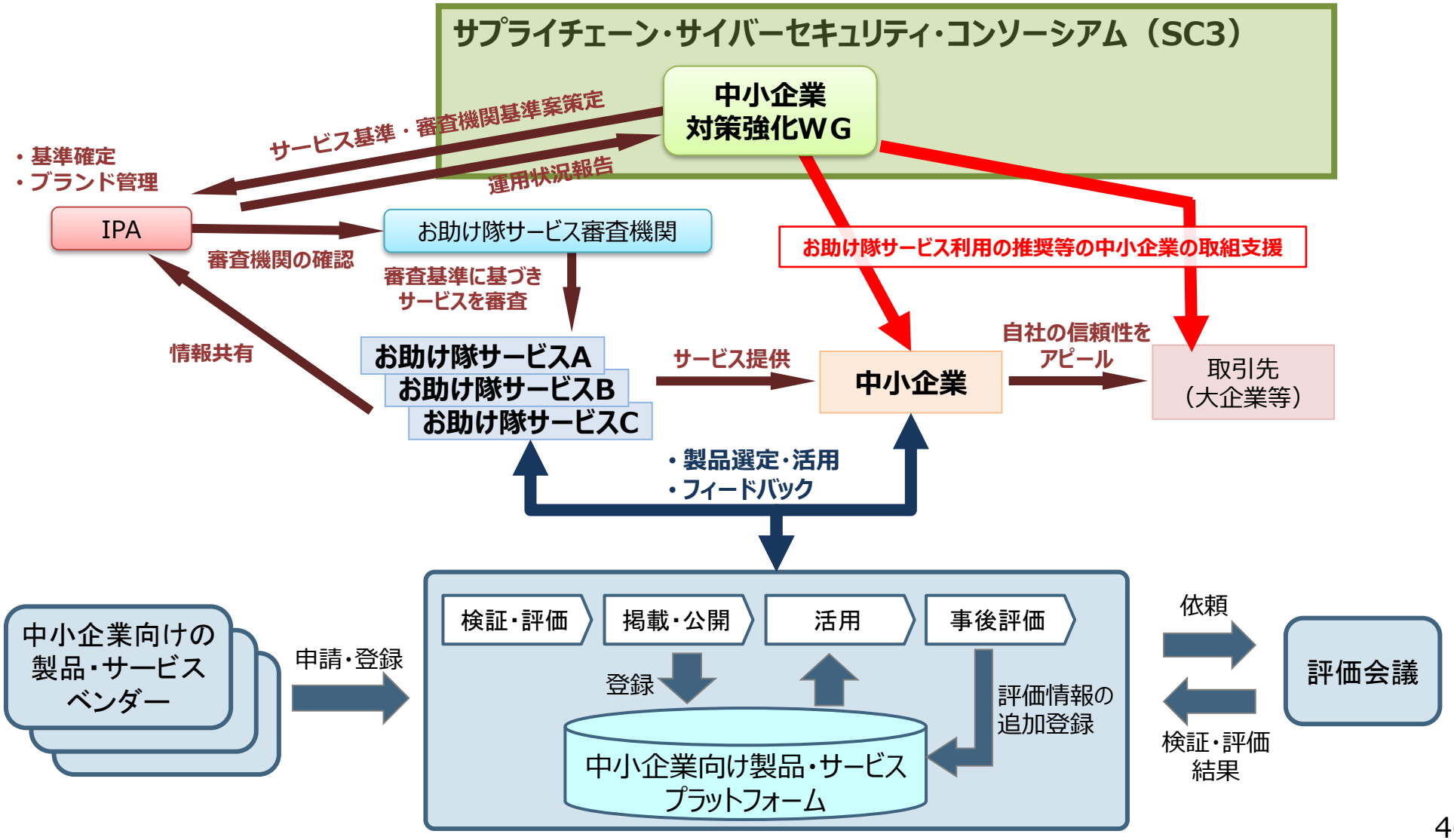
SC3(サプライチェーン・サイバーセキュリティ・コンソーシアム)

→SC3（業種別業界団体が参加）で利用推奨を行うことで、より多くの中小企業がお助け隊サービスを活用し、万が一の際に早急に正しい対処が行える状態を目指す。

（参考）中小企業向け製品・サービスのプラットフォームとの連携

前回WG3資料の再掲

- 本基盤の活用により、お助け隊サービス事業者や中小企業が更なるセキュリティ強化のために適切な製品・サービスを選定できるようにする。
- SC3の中小企業対策強化WGでの議論を期待。



【参考】サイバーセキュリティお助け隊サービス　登録サービスリスト

- 全国各地域の中小企業にとって選択・利用可能な「サイバーセキュリティお助け隊サービス」登録サービスリスト
（第１回審査：5件、第２回審査：４件、第３回審査：３件）

【登録サービスリスト】

	サービス名	事業者名	対象地域
1	**商工会議所サイバーセキュリティお助け隊サービス**	大阪商工会議所	近畿（2府5県）全域、近畿に本社を置く中京圏都市部・福岡県北部の支社・工場、首都圏、長野県　等
2	**防検サイバー**	ＭＳ＆ＡＤインターリスク総研株式会社	全国
3	**PCセキュリティみまもりパック**	株式会社ＰＦＵ	全国
4	**EDR運用監視サービス 「ミハルとマモル」**	株式会社デジタルハーツ	全国
5	**SOMPO SHERIFF（標準プラン）**	ＳＯＭＰＯリスクマネジメント株式会社	全国
6	**ランサムガード**	株式会社アイティフォー	関東地方、中部地方、関西地方、九州地方、沖縄県
7	**オフィスSOCおうちSOC**	富士ソフト株式会社	東北地方（岩手）を中心　※全国展開を計画中
8	**セキュリティ見守りサービス「＆セキュリティ＋」**	株式会社BCC	全国
9	**CBM ネットワーク監視サービス**	中部事務機株式会社	岐阜県（飛騨地方除く）・愛知県（三河地方除く）
10	**中部電力ミライズ　サイバー対策支援サービス**	中部電力ミライズ株式会社	愛知県・岐阜県・三重県・長野県・静岡県（富士川以西）
11	**ＣＳＰサイバーガード**	セントラル警備保障株式会社	東京・神奈川・千葉・埼玉　※順次全国に拡大予定
12	**PCお助けパック　PC定期侵害調査プラン**	沖電グローバルシステムズ株式会社	沖縄県を中心　※全国展開を計画中

【参考】「サイバーセキュリティお助け隊サービス基準」の概要

- 【コンセプト】中小企業に対するサイバー攻撃への対処として**不可欠なサービス**を**効果的**かつ**安価**に、**確実**に提供する。
- 第1回審査(2021年3月)において出た論点を踏まえ、第2回中小企業対策強化WGにおいて、基準改定や基準解釈の目安となるガイドの作成等の方針を議論。**2021年７月に「v1.1版」として公開**した基準の概要は以下のとおり。

主な要件	概要
相談窓口	お助け隊サービスの導入・運用に関するユーザーからの各種**相談を受け付ける窓口を一元的に設置／案内**
異常の監視の仕組み	次のいずれかを含む異常監視サービスを提供すること ・ユーザーのネットワークを24時間見守り、攻撃を検知・通知する仕組み（UTM等のツールと異常監視サービスから構成）（**ネットワーク一括監視型**の場合） ・ユーザーの端末（PCやサーバ）を24時間見守り、攻撃を検知・通知する仕組み（EDR等のツールと異常監視サービスから構成）（**端末監視型**の場合）
緊急時の対応支援	ユーザーと合意したサービス規約等に基づき、ユーザーから要請された場合、ユーザーの指定する場所に**技術者を派遣することにより、緊急時の対応支援を行う**こと（リモートによる対応支援が可能な場合には、リモートによる対応支援も可とする。）
中小企業でも導入・運用できる簡単さ	IT・セキュリティの**専門知識のないユーザーでも導入・運用できるような工夫**が凝らされていること
簡易サイバー保険	インシデント対応時に突発的に発生する各種コストを補償する**サイバー保険が付帯**されていること なお、当該保険は初動対応（駆付け支援等）の費用を補償するものであること
上記機能のワンパッケージ提供	原則として、これら機能をユーザーが個別に契約することなく**一元的に契約可能**であること （例外的に個別契約とする場合にも、ユーザーにおいて手続上の煩雑さを伴わないよう工夫が凝らされていること）
中小企業でも導入・維持できる価格等	**・ネットワーク一括監視型**の場合：**月額１万円以下**（税抜き） **・端末監視型**の場合：**端末１台あたり月額2,000円以下**（税抜き） これらの仕組みを合わせて提供する場合には、この和（**月額１万円に端末１台あたり月額2,000円を加えた価格（税抜き））に相当する価格を超えない価格**であること。端末1台から契約可能であること。 ・最低契約年数は２年以内 **・初期費用、契約年数等の契約にかかる条件をサービス規約等に記載するとともに、口頭又は書面によりユーザに分かりやすく説明**すること
中小企業向けセキュリティ事業の実績	お助け隊実証事業に参加していたこと又は類似のサービスを**中小企業向けに提供・運用した実績**があること
情報共有	お助け隊サービス事業者間の**情報共有（少なくともアラートの統計情報の提供）**に応じること
事業継続性	要員の確保、品質管理等の社内プロセス整備、企業としての安定した財政基盤、経理処理能力等
更新	**２年毎に更新審査**を受けること

（２）各施策の現状及び今後の方向性

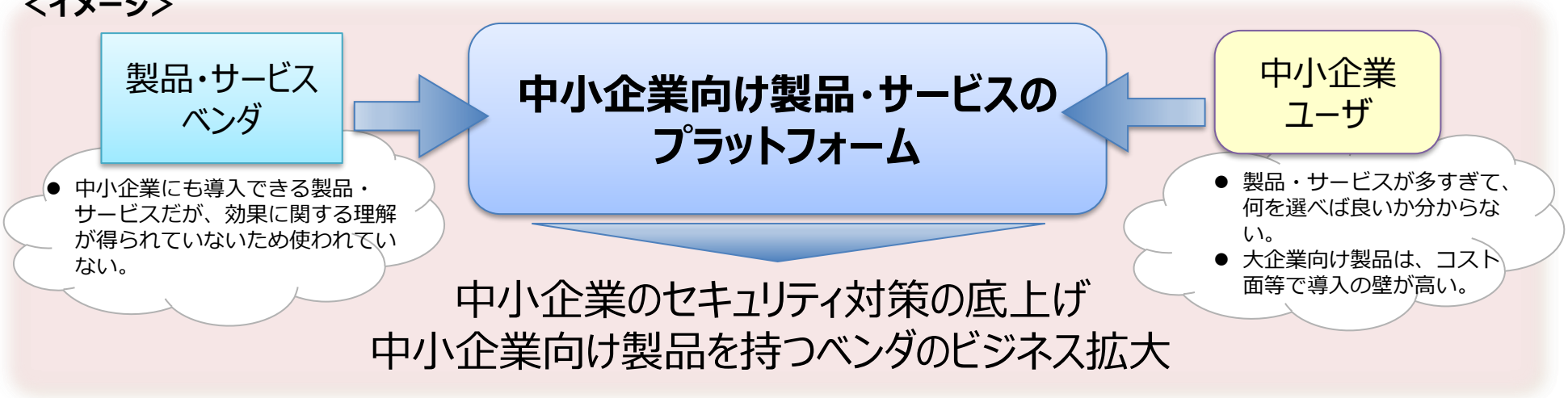
１．Proven in Japan（検証基盤）
　－緑青検証
　－赤検証
　－開発段階検証（主に中小企業向け）
２．情報セキュリティサービス審査登録制度
３．サイバーセキュリティお助け隊
４．中小企業向けセキュリティ製品の検証
５．コラボレーション・プラットフォーム

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

2021年度の検証内容と今後の活動方針

- 2020年度までの成果をもとにセキュリティ製品・サービス情報提要の仮サイトを立ち上げ、SECURITY ACTION登録業者による検索機能をはじめとする有効性評価を行った。
- 中小企業及びベンダーへのヒアリングより、有識者委員会にて事業検証を行った結果、次年度は登録中小企業向けの情報を発信に注力することとなった。

これまでの成果

ユーザ企業が必要とする製品情報項目
（2019年度検証成果）

- セキュリティ製品・サービス選定時の情報収集対象・実態
- 情報提供プラットフォームの潜在ニーズ

ユーザ企業ニーズ調査
（2020年度ニーズ調査）

2021年度の実施事項

申請・登録シート

セキュリティ製品・サービスベンダ

製品・サービス情報
- 製品の仕様・特徴
- 導入/ランニング費用
- 導入ユーザ企業の評価

ユーザ企業
SECURITY ACTION宣言事業者(71,123社)

利用

サンプル SECURITY ACTION セキュリティ対策自己宣言

セキュリティ情報提供プラットフォーム仮検証サイト（IPA）

- セキュリティ製品・サービス情報の掲載
- 問合わせ先/ベンダ情報へのリンク
- 製品リストアップ・検索(価格/カテゴリ)

市場調査（27社）

中小企業ニーズ調査（2,288社）

調査結果 「かなり役に立つ」「役に立つ」といった利用者の声は50%程度あり、中立性のある機関による検証・評価に基づく製品・サービス情報が掲載されていることがその理由と思われる。

活動方針

独自サイトの構築・運用を見送り、ユーザ企業向けコミュニティ形成・情報発信に注力

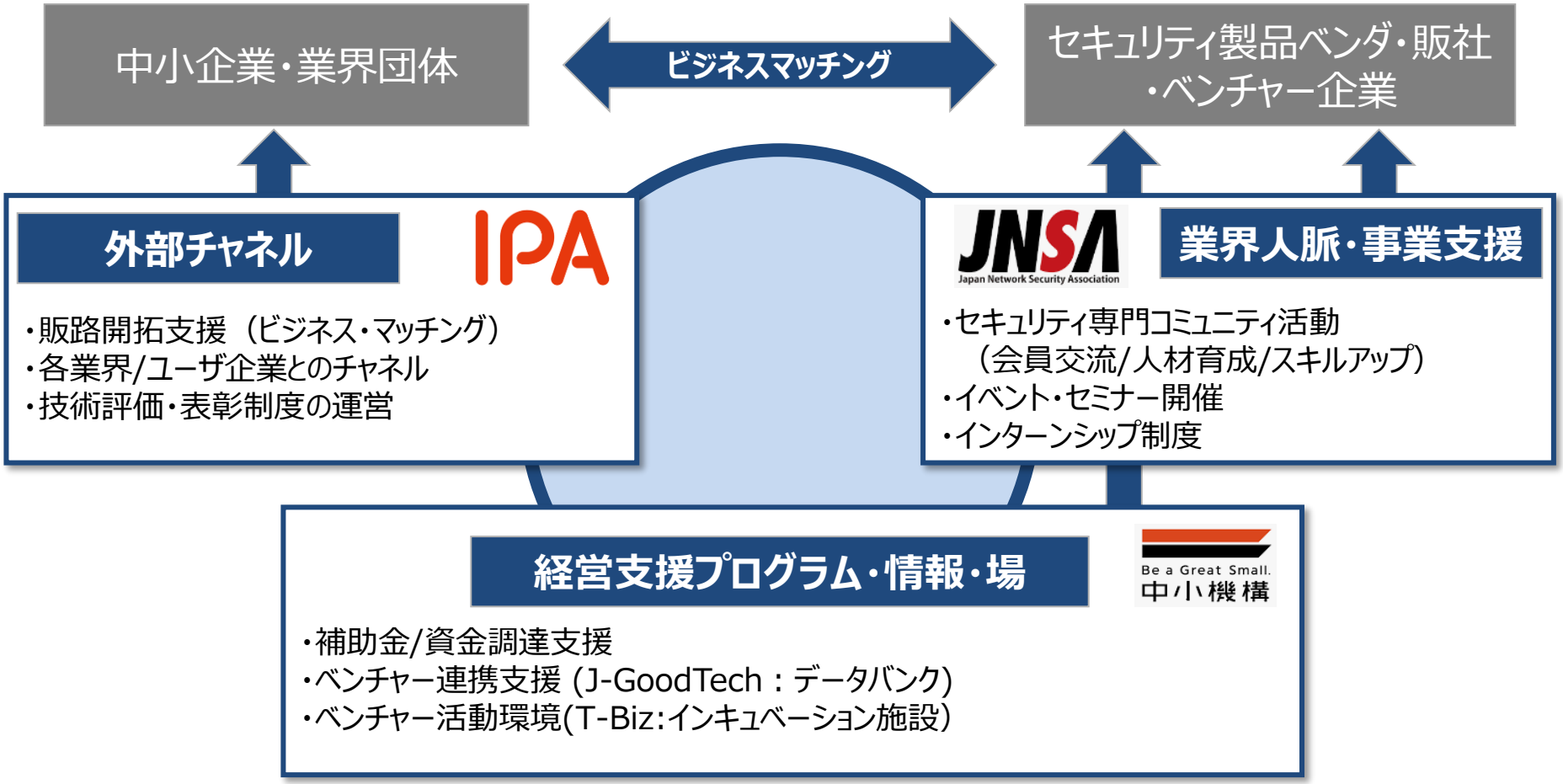
製品情報・リストアップ機能は関連機関へ移管

中小企業向けの情報を発信

実現すべきエコシステム（イメージ）

再　掲

- 今後、関連機関のアセットや既存プログラムを活用し、セキュリティ企業がステージに応じて必要とする支援を、経営/技術/事業の３面から実施する。
- また、IPAによる顧客接点・業界チャネルを活用し、販路開拓・事業化支援を実施する。



【参考】2021年度ユーザ・ベンダ企業調査結果

- セキュリティ製品・サービス情報提供の潜在ニーズと、予算規模による検索機能の有効性を確認した。
- 製品・サービス情報の掲載にあたって、情報の信頼性・公平性の担保といった、製品・サービス品質等に関わる検証・評価を前提とする前提条件があり、ユーザ企業の利用意向を満たす課題が確認された。

ユーザ企業
SECURITY ACTION宣言事業者
(アンケート有効サンプル数：2,288社)

利用

サイトの有用性
選定時に重視した項目
・導入/運用のしやすさ
・導入/運用時の費用

セキュリティ情報提供
プラットフォーム
仮検証サイト（IPA）
・中小企業向け12製品・サービス情報
・製品・サービス別ユーザ企業の評価情報
・注目キーワードの掲載/検索機能の実装

製品・サービス情報

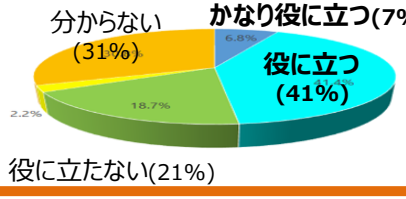
中小企業向け
事業の現状・課題

セキュリティ製品・サービスベンダ
(JNSA会員企業・検証協力ベンダ
企業からの有効回答数：27社)

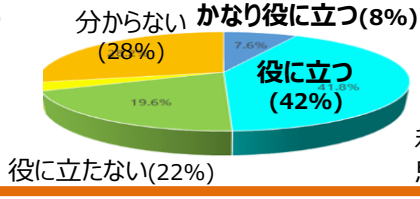
■ 中小ユーザ企業による仮検証サイト評価

主要業種：製造業、建設業、卸・小売業、ｻｰﾋﾞｽ業、学術・技術ｻｰﾋﾞｽ業
利用目的：仮設サイトの内容確認(67%)、製品情報の収集/導入可否検討(22%)

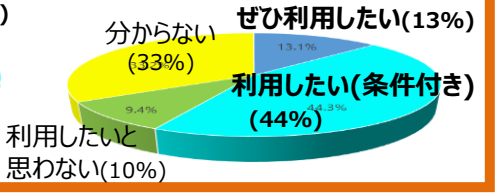
掲載情報の有用性
・製品一覧/概要情報を評価
・**製品特徴/機能比較の拡充を要望**



操作性
・予算/カテゴリ/注目トピック
検索機能を評価



ユーザニーズ
・**掲載製品の検証・評価による情報の信頼性が利用条件**となる



■ 仮検証サイト評価 (2021/12/10-2022/1/14)

・累積アクセス数 40,183件/月、 アクセスユーザ数 6,193人 (ユニークユーザ)
・主要検索条件　製品カテゴリ：UTM,エンドポイントセキュリティ、従業員規模:50名以下、
初期導入コスト：１万円未満、ランニングコスト　10万円未満
・注目キーワード　ランサムウェア対策、テレワークセキュリティ対策、ＧＤＰＲ対応等

■ 中小企業へ導入実績のあるベンダ企業へのアンケート・ヒアリング

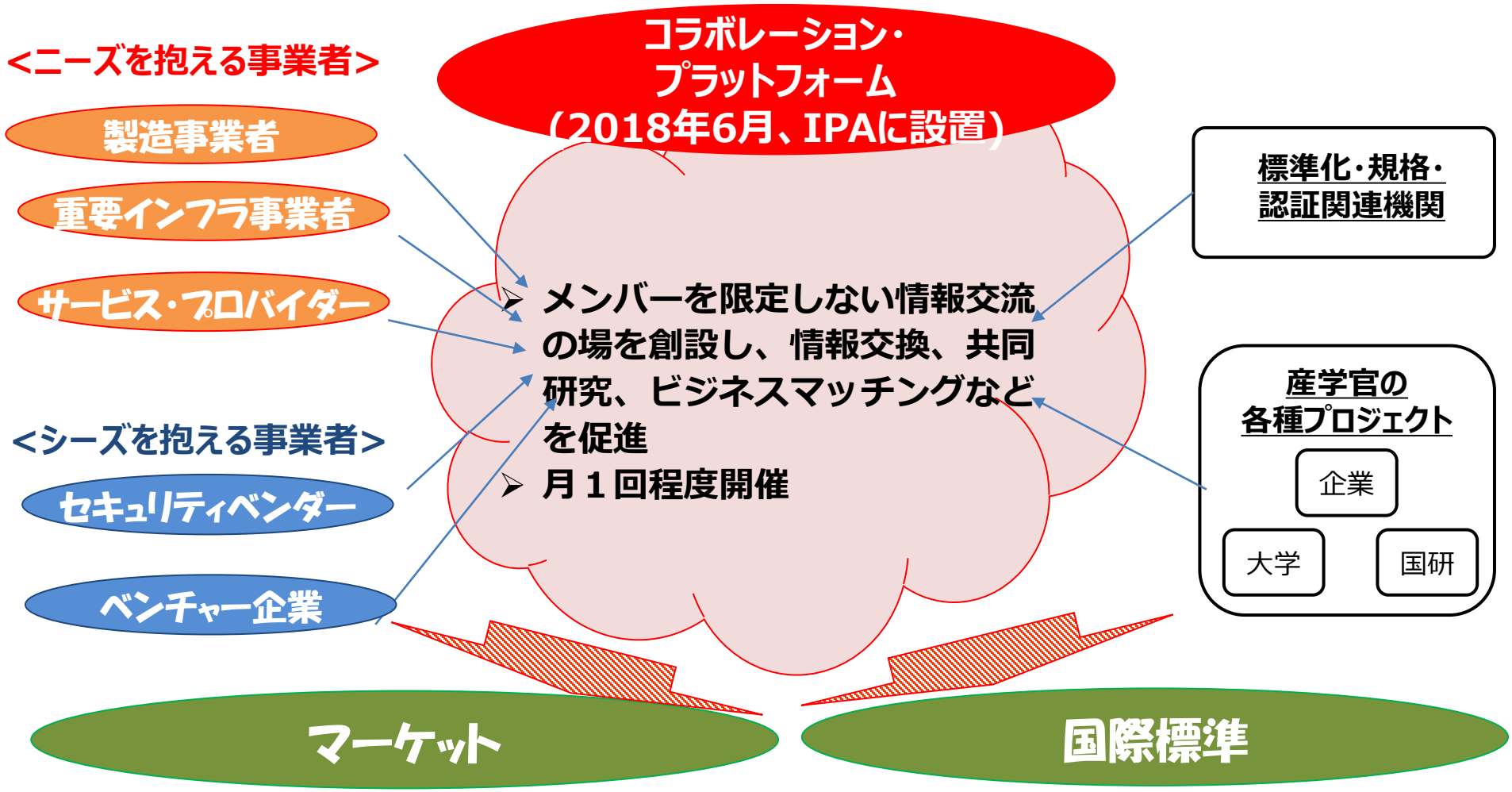
・提供する主要製品：エンドポイント、NWセキュリティ/ログ管理、VPN、ファイル暗号
・導入実績数：100社未満(30%)、100-300社(15%),100名以下の企業(35%)
・ビジネス展開の障壁：提供可能な製品が限定され、商談が小規模
企業数が多く要望が多種多様で、営業活動の効率性が低い

（２）各施策の現状及び今後の方向性

１．Proven in Japan（検証基盤）
　－緑青検証
　－赤検証
　－開発段階検証（主に中小企業向け）
２．情報セキュリティサービス審査登録制度
３．サイバーセキュリティお助け隊
４．中小企業向けセキュリティ製品の検証
５．コラボレーション・プラットフォーム

官民の対話の場としてのコラボレーション・プラットフォームの開催

- 各WGの活動などを通じて顕在化した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。**



コラボレーション・プラットフォームの2021年度開催状況

- サイバーセキュリティに関する情報交換、交流を行っていただける「場」を提供することを目的としたコラボレーション・プラットフォームを2018年6月からIPAを会場として開催してきたが、コロナ禍において2021年度は、時代の潮流にあったテーマを設定し、**計６回オンライン開催**。
- 参加者からは、政府施策の認識、最新動向の情報収集、パネリストのディスカッションによる多方面な議論等、様々な視点で有益との声。

回数	開催日	参加人数	テーマ
第17回	6月30日	133名	サイバーセキュリティ検証基盤事業
第18回	9月7日	145名	フェイクデータなど企業価値を毀損する新たな脅威
第19回	10月22日	120名	K字型(二分化)経済環境下でのセキュリティ投資のあり方
第20回	12月3日	93名	ESG視点でサイバーリスクマネジメントのあり方を探る
第21回	1月14日	171名	サプライチェーンを標的とするサイバーセキュリティリスクへの課題と対応策
第22回	2月22日	146名	事業変革を実現するDXを支えるセキュリティ

コラボレーション・プラットフォームの今後の方向性

- オンライン開催では気軽に参加いただける一方で、コラプラが目指してきた「あらゆるコラボレーションの創出」には、双方向でのコミュニケーションが取りづらい等のオンライン開催特有の障壁あり。
- 2022年度は、聴講主体のオンラインセミナー形式を改め、**少人数参加型でのオンラインワーキンググループ形式**での開催とし、**サイバーセキュリティ検証基盤の結果報告及びビジネスマッチングの場**とするほか、政策やIPAの活動に興味・意見のある方々との間での**課題共有・意見交換を通じてセキュリティ業界の課題解決推進のためのコラボレーションを目指す。**

ワーキンググループ形式によるコラボレーションの推進

【政策・調査活動とのコラボレーション】

政策や調査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・調査紹介、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】

ベンダー企業や大学との連携を図り、**新たなソリューションや技術・手法を市場に流通。**

⇒大学、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。

⇒製品評価事業等の協力ベンダに登壇いただく等、ベンダと市場とのパスとなるプログラムを検討。

目次

論点①　供給サイドの取組の方向性（安心して製品・サービスを利用できる基盤の構築）

- これまで、赤検証の手引き、青検証の手引き、緑検証項目の整理、審査登録制度など、検証事業者の信頼性を向上させていく取組を行ってきた。
- 引き続き、緑検証の表彰制度、信頼性可視化制度の審査登録制度への反映といった取組を進めていくことで、利用者が安心してセキュリティ製品・サービスを利用できる基盤の構築に取り組んでいく。

凡例
- 実施済み
- 短期取組
- 更なる取組として検討

検証サービスの需要サイド

「国民生活や経済活動の基盤としての機能」という観点から主体を区分けし、それぞれに応じた政策を検討

- 日本政府、行政
- 重要インフラ企業
- 大規模なサプライチェーンを有する業界
- 企業

対策支援

SC3・お助け隊

選定/活用

機器審査要件

特定分野における検証基準

青　試行検証

検証サービスの供給サイド

引き続き、信頼性の向上に向けた取組を進めていく

製品ベンダ X
IT機器/IoT・OT製品

製品ベンダ Y
セキュリティ製品

検証済製品ラベル　補助

赤　攻撃型検証
開発　開発段階検証
ガイド
人材育成
検証ラボ
検証センター
緑　有効性検証

手引き

検証事業者 α
検証者

検証事業者 β
検証者

表彰
公募要領
認証要件
公開の在り方

信頼性可視化制度

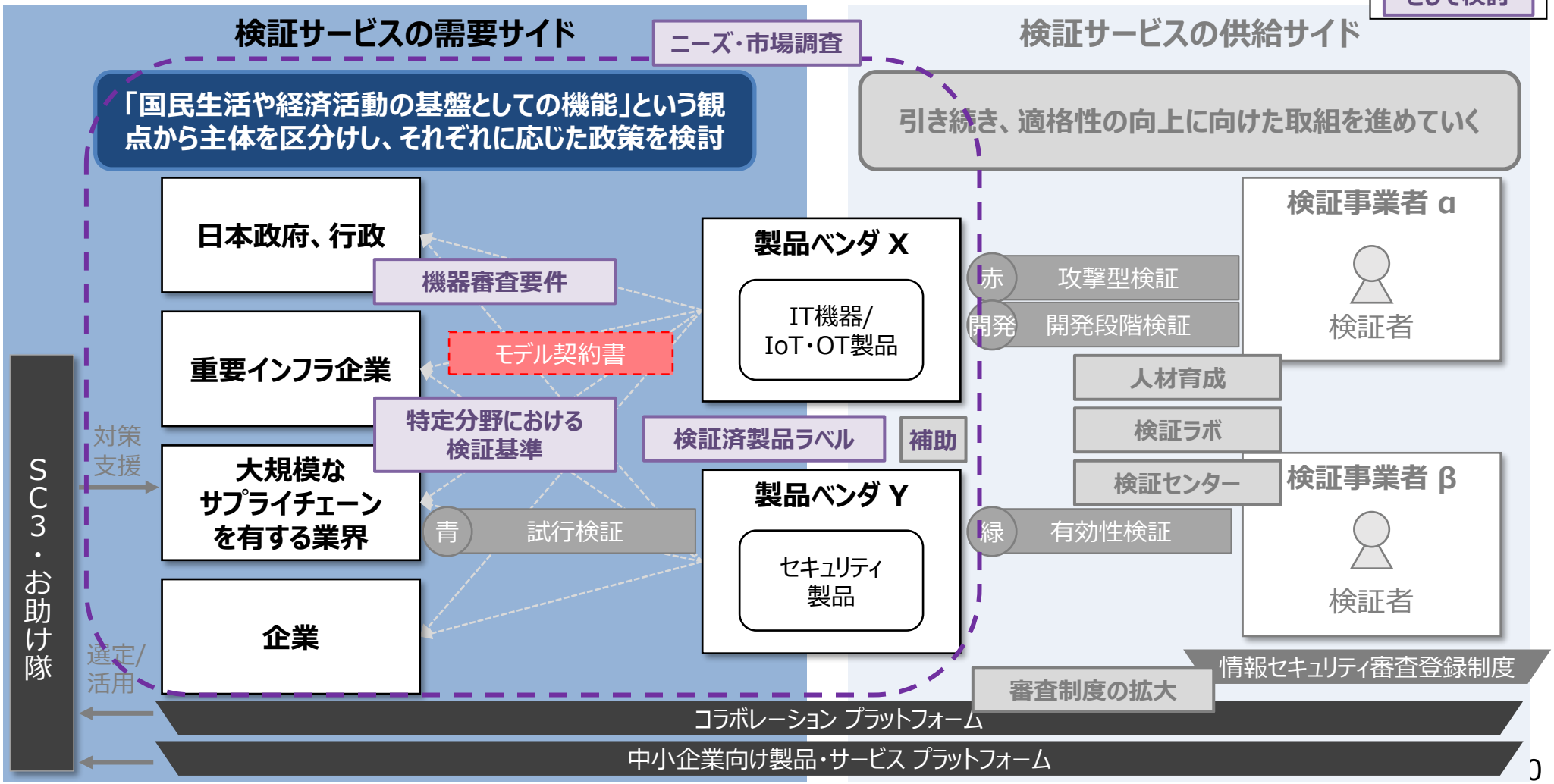
情報セキュリティ審査登録制度

コラボレーション プラットフォーム

中小企業向け製品・サービス プラットフォーム

論点②　需要サイドの取組の方向性（隠れたニーズの掘り起こし）

- また、安心してセキュリティ製品・サービスを利用できる基盤の構築を進めていくと同時に、需要サイドにおけるセキュリティサービスの隠れたニーズを掘り起こしていくことも必要。
- 需要サイドといっても、行政と民間企業、また民間企業の中でも規模や業種は様々であり、どの程度セキュリティ対策を行うべきかも様々であることから、これら全てに一律な政策を課すことが有効とは考え難いことから、需要サイドの区分けを想定し、それぞれの対象に応じた取組を検討していくべきと考えられる。



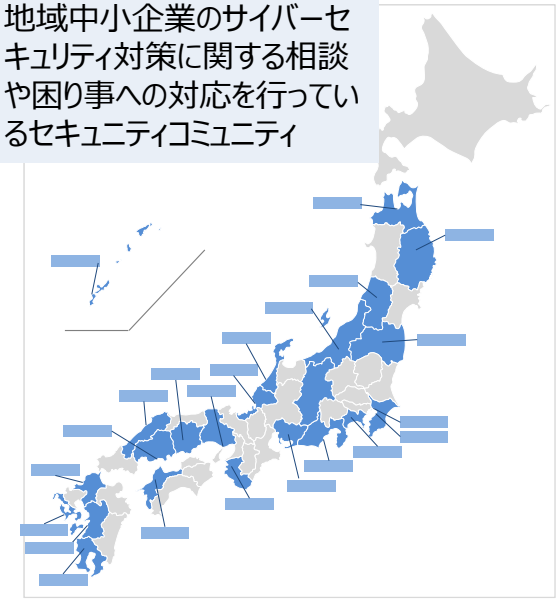
論点③　需要と供給のマッチング

- 検証サービス、セキュリティ製品、デジタルフォレンジック、セキュリティ監視・運用といったセキュリティサービスの市場拡大のためには、供給サイドの信頼性向上、需要サイドのニーズの掘り起こしとともに、供給と需要をマッチさせる取組も必要。
- コラボレーションプラットフォームや地域SECUNITYといった既存の枠組みを活用しつつ、IPA等も活用することで、更なるマッチングに取り組んでいく。また、セキュリティビジネスの需要と供給の関係以外に働きかける取組も検討。
- その他、あらゆる層に向け、セキュリティ意識を醸成させていくために、種々のガイドラインも活用した普及啓発活動や広報に取り組んでいく。

コラボレーション・プラットフォームの活用

地域SECUNITYの活用

地域中小企業のサイバーセキュリティ対策に関する相談や困り事への対応を行っているセキュニティコミュニティ



普及啓蒙・広報活動

関連機関のアセットや既存プログラムを活用

外部チャネル
IPA

業界人脈・事業支援
JNSA
Japan Network Security Association

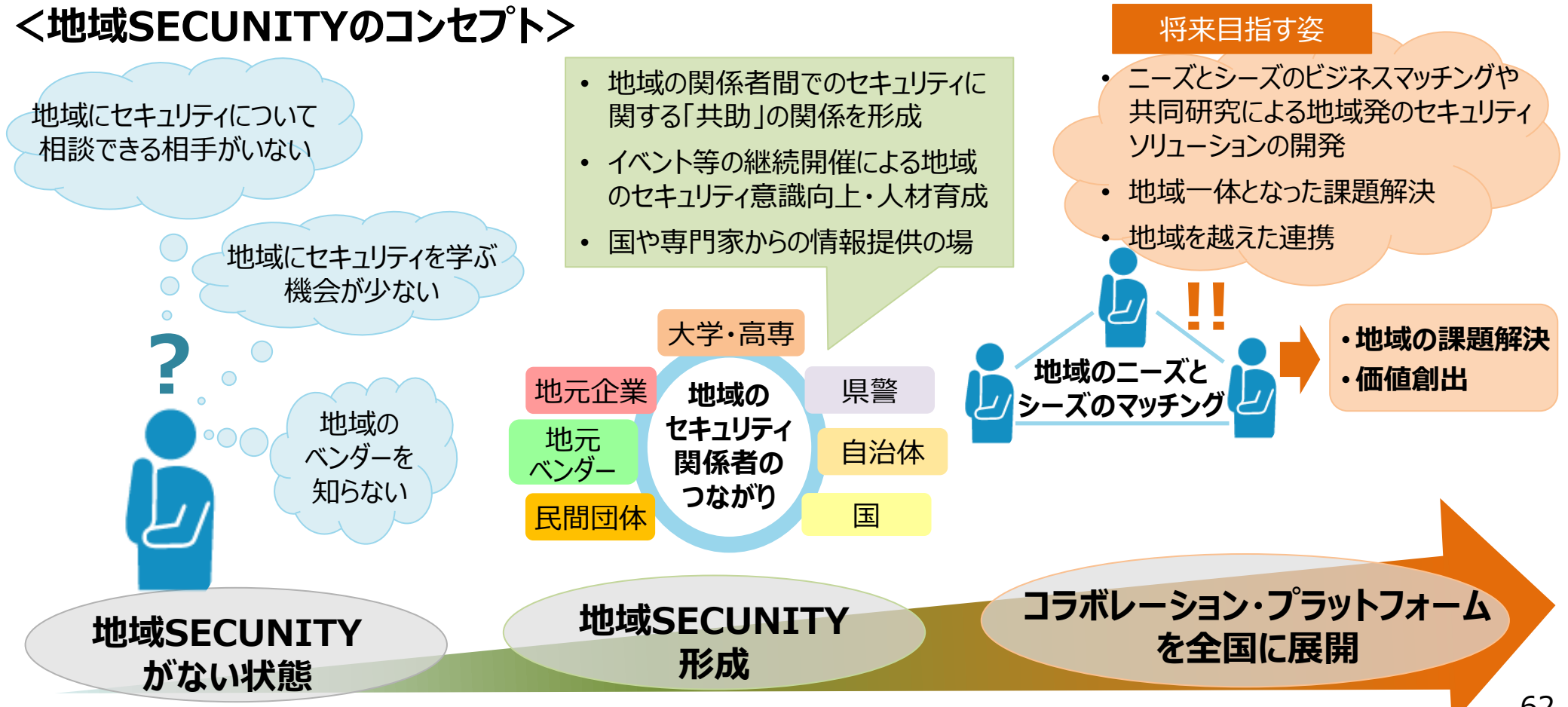
経営支援ﾌﾟﾛｸﾞﾗﾑ・情報・場
Be a Great Small.
中小機構

（注）本図はマッピングのイメージであり、実在するコミュニティに対応するものではない。

（参考）地域に根付いたセキュリティ・コミュニティ（地域SECUNITY）の形成促進

- 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ活動を、「地域SECUNITY」と命名。
- まずは各地域で地域SECUNITYの形成を促進し、将来的には、地域のニーズとシーズのマッチングによる課題解決・付加価値創出の場（コラボレーション・プラットフォーム）へと発展することを目指す。

＜地域SECUNITYのコンセプト＞



（参考）産業サイバーセキュリティセンター（ICSCoE）（2017年4月設置）

- 中核人材育成プログラムでは、電力、石油、ガス、化学、自動車、鉄道分野等の企業から受講者を受け入れ、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ1年程度のトレーニング等を実施。第５期（2021年7月開講）には、48名が参加。修了者は産業サイバーセキュリティエキスパートとして業界内外のサイバーセキュリティの取組に貢献。
- また、短期プログラムとして、経営層が示す戦略の下、事業継続と価値創出に係るリスクマネジメントを中心となって支える立場である、戦略マネジメント層向けのセミナーを実施。

中核人材育成プログラム

- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

卒業プロジェクト（一例）

- **ゼロトラストという戦術の使い方**
  ～情報系・制御系システムへのゼロトラスト導入～

「ゼロトラスト」で用いられる機能について、実際に環境を構築、システムへの導入検証を実施。結果と得られたノウハウを「ゼロトラスト導入指南書」としてまとめた。

- **現場向け制御セキュリティ教育：安全・安定操業を脅かした事例10選**

近年国内外で発生した制御システムへのサイバー攻撃10事例を紹介。事例の紹介に留まらず、発生する可能性がある被害について解説。

https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project.html

修了者コミュニティ「叶会」

- 年１回年次総会（11月）で最新動向と修了者の近況の活躍を発表。
- サイバーセキュリティ情報提供活動：
  情報共有ツール「SIGNAL」を使い、ICSCoEが入手した脆弱性情報等を修了者に提供。

修了者の地域での活躍

- 修了者が卒業プロジェクトの延長としてフレームワーク推進活動を実施。地銀と連携し、中小企業を含めたサプライチェーンのセキュリティ強化に貢献。
- また、商工会議所の会報に地域・中小企業を対象としたセキュリティの取組促進の啓発記事（インシデント事例、SECURITY ACTION制度の紹介等）を執筆（札幌、名古屋、大阪）。地域での繋がりを持たせ、情報発信の場の支援を行う。

戦略マネジメント系セミナー（2018年～）

- 経営層を補佐し、実務者層・技術者層を指揮することでセキュリティ対策を進める戦略マネジメント層向けのセミナー。
- 組織全体のセキュリティレベル向上を目指し、セキュリティ対策を組織横断的に統括する体制及びその責任者の役割について理解を目指す。
- 2021年度は１～２月に対面・オンライン（ハイブリッド形式）で開講。講演・講義・グループディスカッションにより、先進事例・課題や解決策・ノウハウなどを体系的に学ぶプログラムを提供。

（参考）令和３年度地域SECUNITY形成促進の取組（沖縄）

- 沖縄サイバーセキュリティネットワーク（2015年3月発足）など既存の産学官のセキュリティ関連ネットワークを有機的に連携。
- 沖縄地域の自治体、事業者に対し、実態把握のためのアンケート調査を実施し、これを踏まえたセキュリティに関するセミナー開催、相談窓口設置などセキュリティ対策を検討。

【実施団体】沖縄ITイノベーション戦略センター（ISCO）
・SECUNITY事業では、リテラシー向上のためのセミナーの実施やメールマガジンによる情報提供等を行い、総務省、沖縄県事業と連携した取組を展開。
・若手人材の育成のため情報セキュリティマネージメント等の資格者取得支援を実施。
・ビジネスマッチングサイト「インダストリンク」内にサイバーセキュリティ関連コンテンツを作成。

※セキュリティセミナーはコロナ感染対策を考慮してすべてオンライン開催するとともに、動画コンテンツとして提供。

（参考）おかやまAI・セキュアIoT共創コンソーシアム

- 岡山県「大学と連携した地域産業振興事業」の一環として、AI・IoT・セキュリティ関連技術分野において共同研究を目指す企業と大学研究者などが集い、多面的な連携による共同研究の促進を図る「共創の場」として岡山大学に設立。
- IoT機器等を扱う企業が30社、岡山県内5つの学術機関、岡山県等の3団体が参画し、企業間や有識者とのコミュニケーションの場、共同研究組成に向けたワーキンググループや会員企業の課題に応じたワークショップなどの場が提供されている。

https://oasis.okayama-u.ac.jp/wp-content/uploads/2021/03/OASIS.pdf

METI
Ministry of Economy, Trade and Industry

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html