IPA Better Life with IT

第17回コラボレーション・プラットフォーム

サイバーセキュリティ検証基盤

2021年6月29日

独立行政法人情報処理推進機構
セキュリティセンター　セキュリティ対策推進部
セキュリティ分析グループ

1. サイバーセキュリティ検証基盤

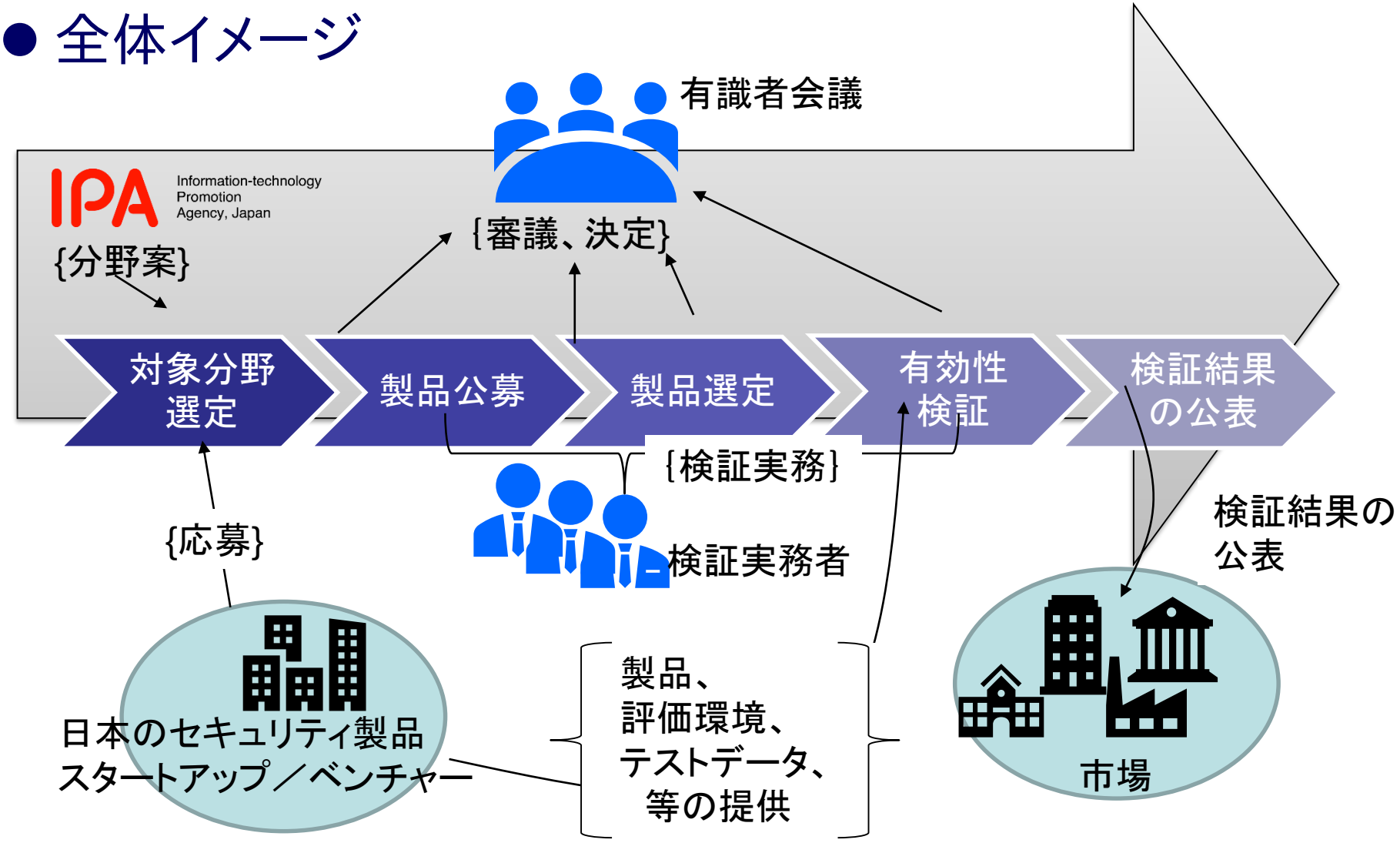
- 目的

  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・サービス（以下、製品）のマーケット・インを促進

- 体制・方法
  - 有識者会議を設置（2019年9月）：以下を審議・決定
    - 検証体制や検証方法の検討、および、仕組み化
    - 検証対象製品の公募、選定製品の検証内容、など
  - 検証の実務は、セキュリティ技術・製品の評価の専門家が、有識者会議の下で実施

1. サイバーセキュリティ検証基盤(2)

- 全体イメージ



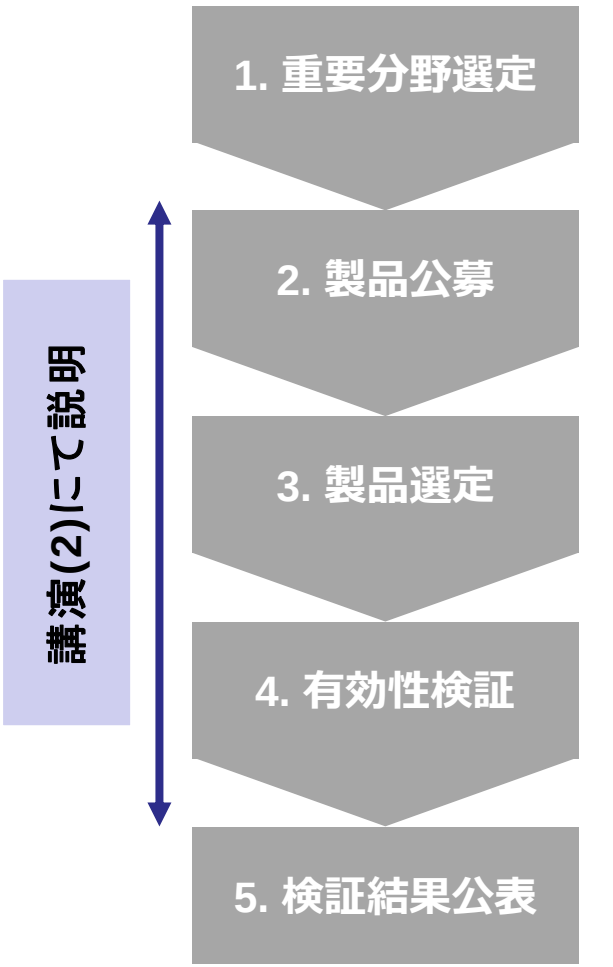
1. サイバーセキュリティ検証基盤(3)

- 2020年度(2か年目)の事業
  - 検証基盤の「仕組み」の構築
    - 製品公募・対象製品選定の仕組み
      ～重要分野マップの修正、重要分野の選定～
    - 効率的な有効性検証の仕組み
    - 検証結果公表等の仕組み、等
  - 上記の運用
    - 製品公募、選定
    - 製品の有効性検証
  - 検証基盤を含む、市場参入促進の仕組み全体像の検討
  - 2018年度成果「試行導入・導入実績公表の手引き」の改良

本項では、この二点をご紹介

1. サイバーセキュリティ検証基盤(4)

● 検証基盤のプロセス



実施概要

- 重要分野マップについて、セキュリティ脅威の状況、ユーザ企業の状況、セキュリティ技術の変化等を踏まえて必要な見直しを行う。
- 製品公募に際しての公募要領・応募用紙を作成し、公募を行う。
- 幅広い製品・ベンダーに応募頂くために、公募の周知を行う。
- 応募された製品・ベンダーの中から、有効性検証の対象となる製品を選定する。
- 製品選定を効率化するために、事前に審査基準を定める。
- 選定された製品の検証を実施する。そのために、製品に対する検証項目、検証環境、検証方法を決定する。
- 製品の特徴的な機能や強みを示す差別化ポイント（ストロングポイント）を調査する。
- 検証結果を文書化し、公表する。
- 検証結果の周知を図る場を提供する。

2. 重要分野マップの修正、分野選定

- 重要分野マップ
  - 重要になると予想されるセキュリティ製品・サービスのマップ
  - 脅威の状況、ユーザ企業の状況、セキュリティ技術の変化等を踏まえて、見直し
  - 検証対象製品を選定する製品分野の基礎とする

- 2020年度の見直し：　議論に挙がった重要分野
  - セキュリティに係る状態の可視化（脅威、脆弱性）
  - IT資産の認証/検証
  - 脅威インテリジェンスの整理・管理

  など

2. 重要分野マップの修正、分野選定(2)

● 重要分野マップ(修正)

<重要分野> ①脅威の可視化、 ②脆弱性の可視化、 ③IT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、**⑧IT資産の認証/検証**

組織に対するサイバーセキュリティ脅威(*) ＼ 対策が必要なプロセス		資産管理			リスク管理			防御		監視・検知				対応・復旧				教育・訓練
		IT資産管理	ID/アクセス管理	IT資産の認証/検証	脆弱性管理	テスト(ペネトレーションテスト等)	リスクアセスメント	境界防御	データ保護(暗号化)	クラウド/サーバ	ネットワーク	エンドポイント	リアルタイム検知	インシデントレスポンス	分析(フォレンジック)	復旧	サイバー保険	
継続的に存在する脅威	標的型攻撃による機密情報の窃取			○	○		④		○			○		○				○
	内部不正による情報漏えい		○						○	○		○		④	○			⑥
	ビジネスメール詐欺による金銭被害						○					○	⑤	○			○	○
	ランサムウェアによる被害			○								○	○	○			○	○
	予期せぬIT基盤(クラウド、データセンター)の障害に伴う業務停止	③														○	○	○
	不注意による情報漏えい	○		⑧	②				○		①	○						○
	Web上サービスからの個人情報窃取				○		○		○	○				○				
	DDoS攻撃によるサービス停止						○	○		○	○					○		
新たに顕在化した脅威	サプライチェーンの弱点を悪用した攻撃による情報漏えい	○		○	○	⑦	○			○							○	
	IoT機器のBot化などの不正利用、情報漏えい	○		○	○	○	○						○					
	制御系システムへの攻撃による製造ライン停止				○	○	○					○	○					
	シャドーITによる不正アクセス、情報漏えい	○	○	○			○			○			○					
	利用しているオープンソースソフトウェアの脆弱性による不正アクセス、情報漏えい	○			○		○						○	○				

(*):IPAが2020年1月29日に公開した「情報セキュリティ10大脅威 2020(https://www.ipa.go.jp/security/vuln/10threats2020.html)」の組織編に上げられた脅威に、制御システムへのサイバー攻撃など組織として対策すべき事項を付け加えた

※ 詳しくは、2020年度成果「サイバーセキュリティ検証基盤の運用に関する報告書」付録B参照
https://www.ipa.go.jp/files/000090567.pdfs

2. 重要分野マップの改良、分野選定(3)

- 分野選定
  有識者会議にて議論、2020年度に取上げる分野を投票
  - 脅威の可視化
  - 脆弱性の可視化
  - IT資産の認証/検証

- (参考)
  有識者会議にて、
  「脅威の可視化」「脆弱性の可視化」は、NIST が開催した
  「Zero Trust Architecture Technical Exchange Meeting」(SP800-207)
  の重要コンセプトに対応(一部)しており、分野選択として適切と議論

3. 市場参入促進の仕組みの検討

● 背景、概要

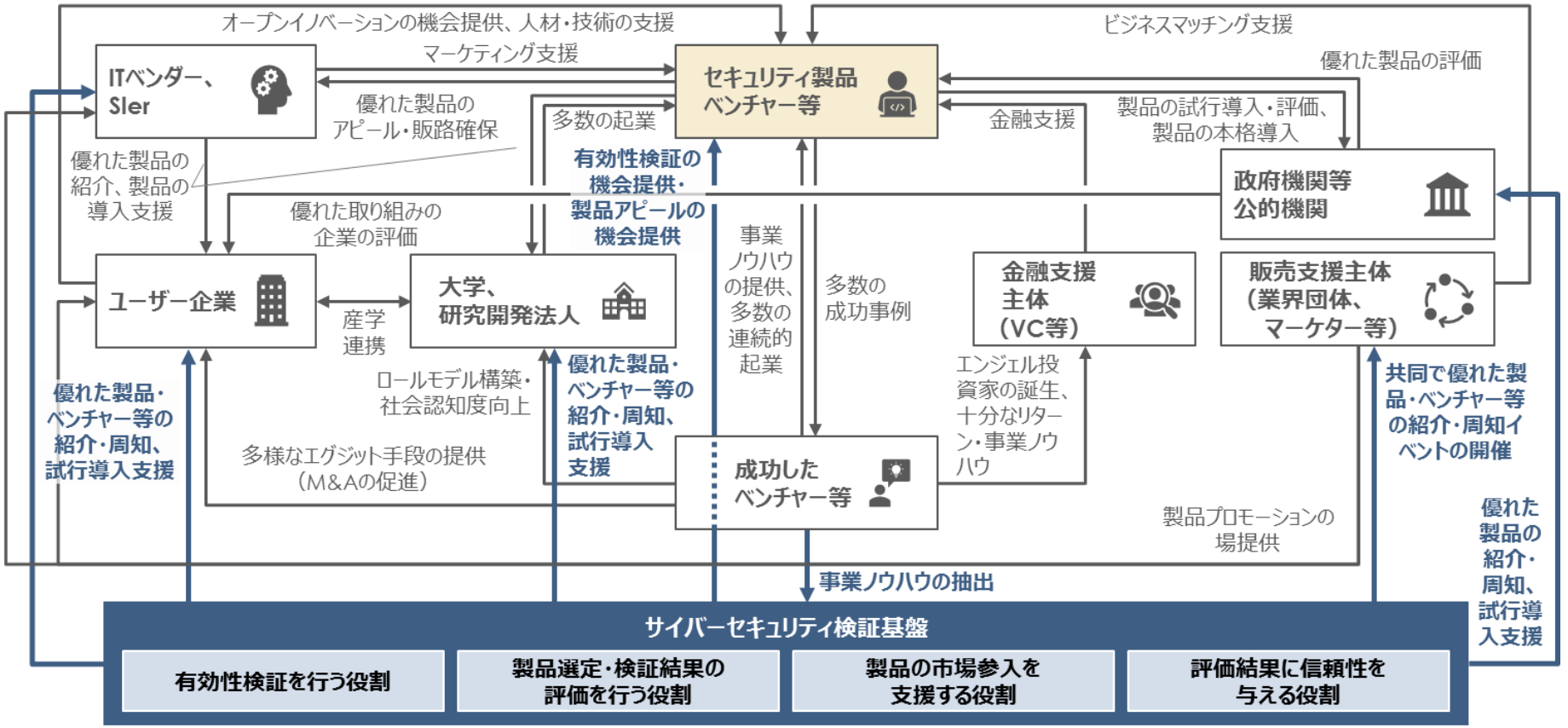
- 日本発のセキュリティ製品に対し、十分な市場参入の機会を提供するには、それを促進する仕組みが重要であることを海外調査で あらためて 確認(2019年度)。

- 市場参入を促進する上で効果的な、社会全体の機能（役割）について検討、全体像を作成(2020年度)。
  - 社会全体の仕組みとして何が必要か
  - 対象製品と潜在的なユーザとをマッチングする機能
  - 検証対象製品を試行導入・評価しその結果の公開に協力する機能
  - 金融支援やマーケターとしての支援を対象製品ベンダーに提供する機能

- 役割の担い手になり得る団体・企業等に、ヒアリング調査、現状分析を実施

3. 市場参入促進の仕組みの検討(2)

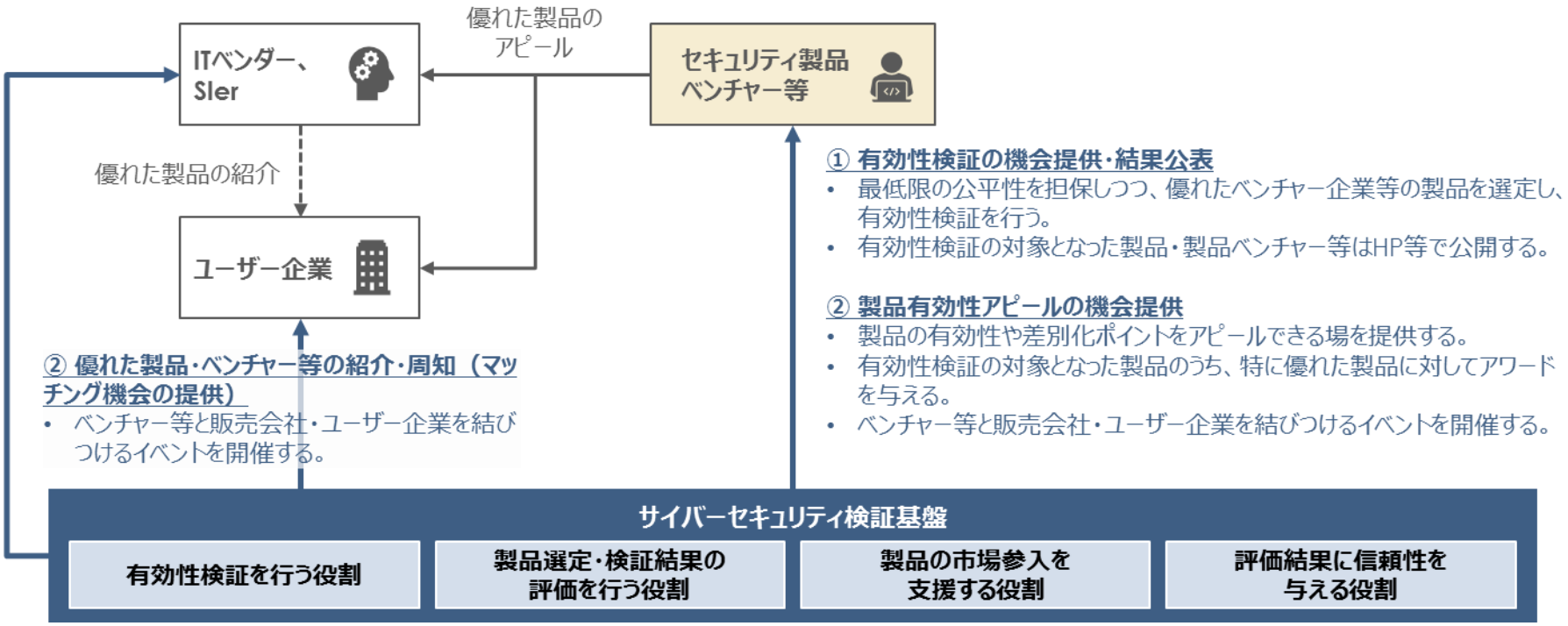
● 全体像・将来像



出所）経済産業省「イノベーション・ベンチャー政策について」に基づき三菱総合研究所作成
http://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/innovation_dai3/siryou4.pdf

3. 市場参入促進の仕組みの検討(3)

- 優先して実施すべき施策案
  - ① セキュリティ製品ベンチャー等に対する有効性検証の機会提供・結果公表
  - ② セキュリティ製品ベンチャー等に対するアピール機会、販売会社・ユーザー企業とのマッチング機会提供



IPA Better Life with IT

～ ご清聴ありがとうございました ～

お問合せは下記まで

isec-kenshoki-info@ipa.go.jp