IPA Better Life with IT

第24回コラボレーション・プラットフォーム

2021年度 サイバーセキュリティ検証基盤

2022年12月20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

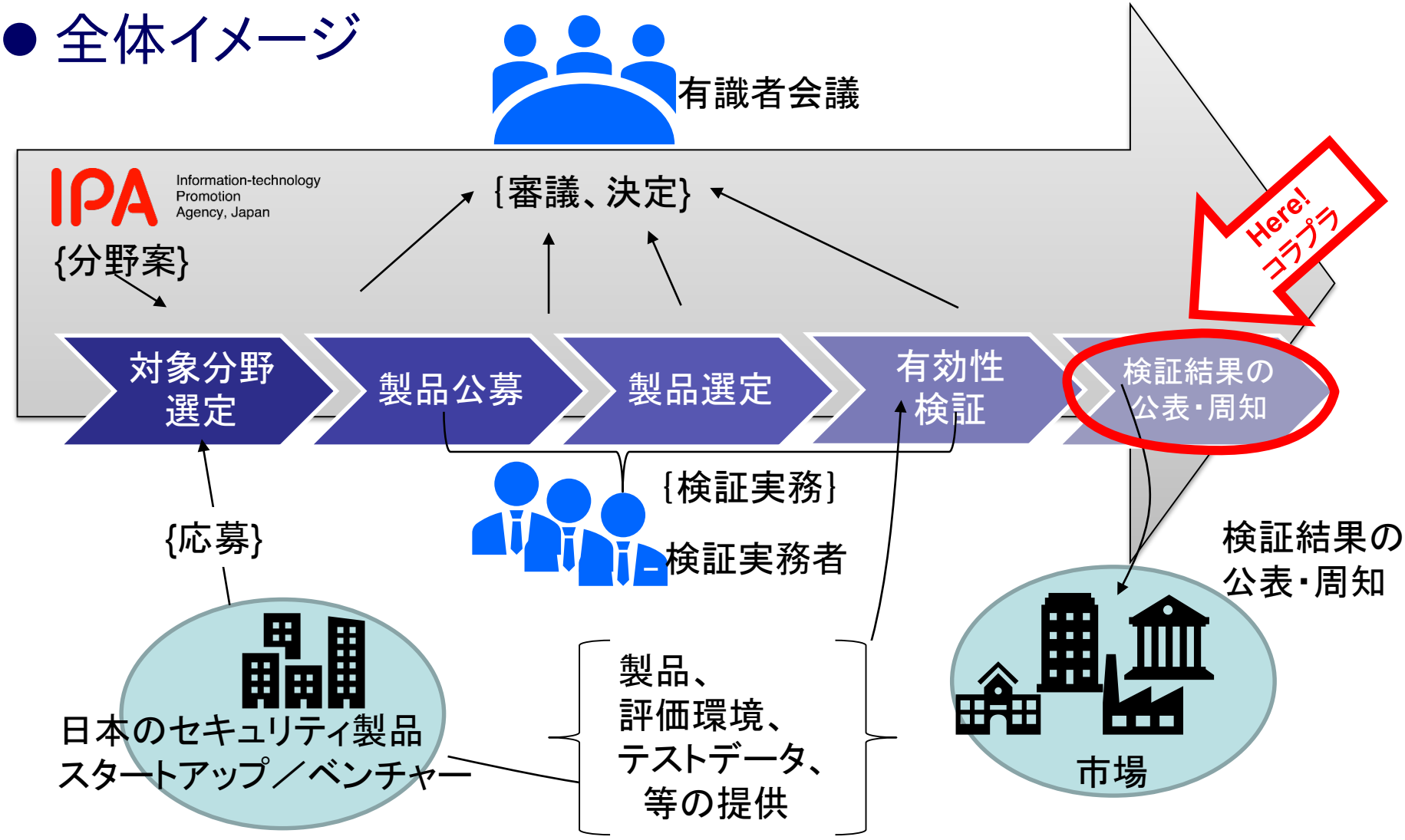
- 目的

  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)

● 2021年度(3か年目)の事業(抜粋)

2020年度の事業で作った、製品選定～有効性検証の仕組み(手順・基準等)に基づき、有効性の検証を実施

- ✓ 「セキュリティ製品・サービス重要分野マップ」の更新、2021年度の対象製品分野の選定
- ✓ 対象製品の公募・選定
- ✓ 検証を実施
- ✓ 2020年度版「試行導入・実績公表の手引き」の評価

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

講演(2)にて説明

	実施概要
1. 重要分野選定	• 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。
2. 製品公募	• 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。
3. 製品選定	• 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。
4. 有効性検証	• 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。
5. 検証結果公表	• 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。

コラボレーション・プラットフォーム

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
    - 次ページの表（マップ）参照
    - 横軸：　対策が必要なプロセス
    - 縦軸：　組織に対するサイバーセキュリティ脅威
      (IPAの「情報セキュリティ10大脅威 2021」の組織編にランクインした脅威に、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）
  - 脅威の状況、ユーザ企業の対策等状況、セキュリティ技術、これらの変化等を踏まえて見直し

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リスクの可視化・緩和**、 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、**⑨データ保護、⑩ID/アクセス管理**

<対策が必要なプロセス>

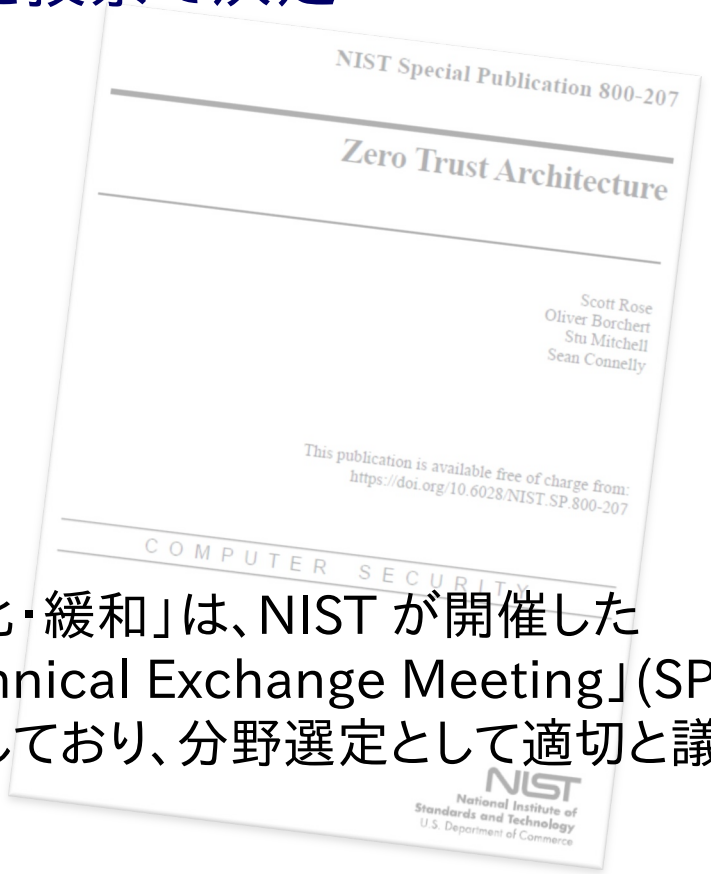
^組織に対するサイバーセキュリティ脅威v

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・緩和				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	リスクアセスメント	リスク緩和	テスト(ペネトレーションテスト等)	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	
標的型攻撃による機密情報の窃取			○	○					○			○		○				○
内部不正による情報漏えい		○							○	○		○		④	○			⑥
ランサムウェアによる被害			○									○	○	○			○	○
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	○		○	○	○					○			⑤				○	
テレワーク等のニューノーマルな働き方を狙った攻撃	○		○		○				○			○						○
ビジネスメール詐欺による金銭被害					○							○		○			○	○
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								⑨							○	○	○
不注意による情報漏えい	○	⑩	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					○			○		○	○					○		
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	○			○	○								○	○				
IoT機器のBot化などの不正利用、情報漏えい	○		○	○	○		○ ⑦						○					
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	○	○	○		○					○			○					
インターネット上のサービスへの不正ログイン		○		○	○						○						○	

※ 詳しくは「2021年度サイバーセキュリティ検証基盤の運用」付録A参照
https://www.ipa.go.jp/files/000097009.pdf

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“重要分野マップ”に基づき審議のうえ、
  2021年度に取上げる分野を投票で決定
  - 脅威の可視化
  - リスクの可視化・緩和
  - データ保護
  - ID/アクセス管理
- (参考)
  有識者会議にて、
  「脅威の可視化」「リスクの可視化・緩和」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、分野選定として適切と議論



IPA Better Life with IT

～ ご清聴ありがとうございました ～