経済産業省

資料3

事務局説明資料

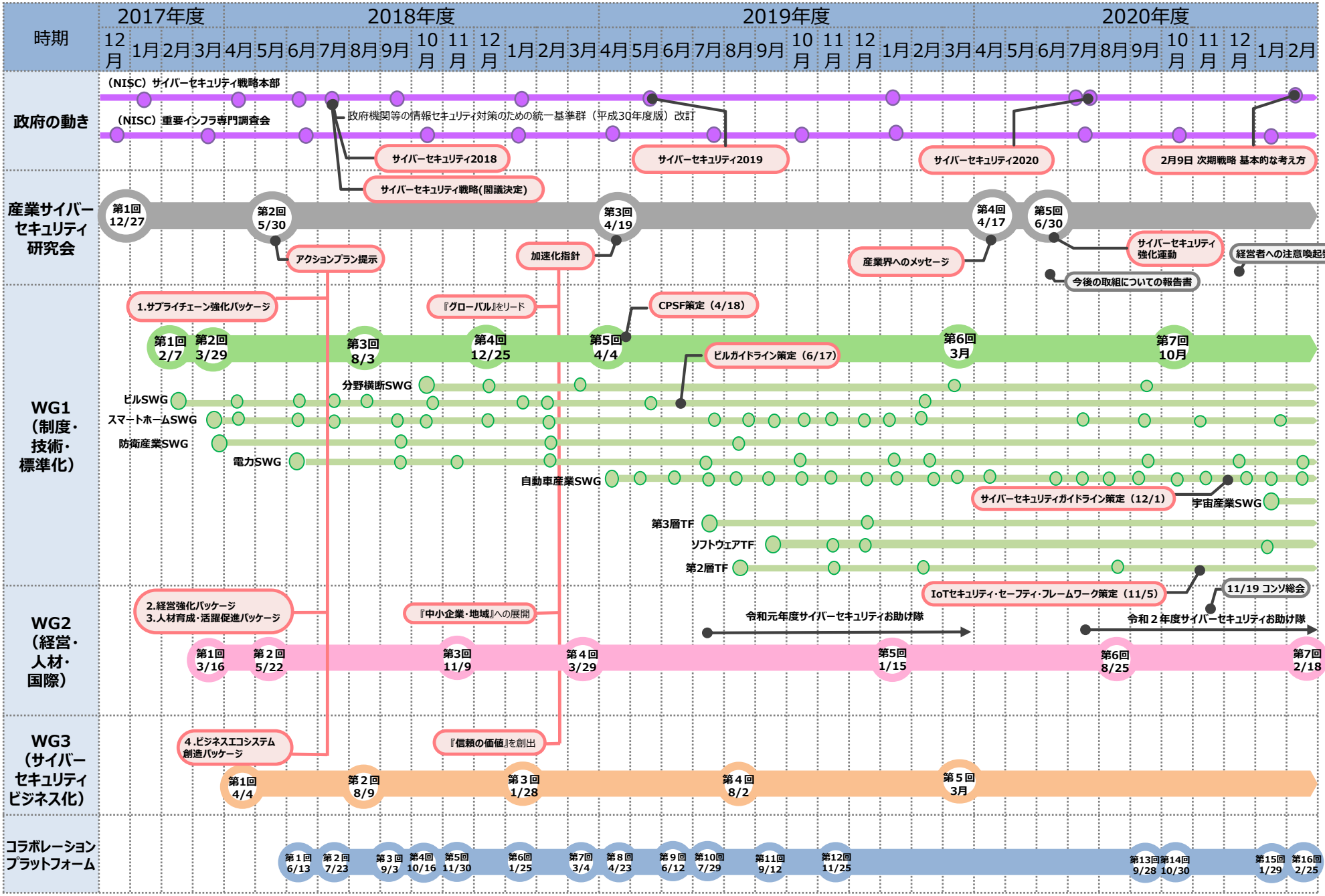
産業サイバーセキュリティ研究会WG3
（サイバーセキュリティビジネス化）
第６回

令和３年３月１０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と予定



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

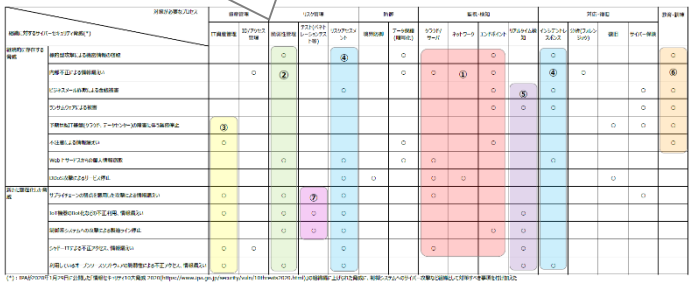
2019年度成果

- 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、コラボレーション・プラットフォームで発表。

累計1,967DL
（2020/4/10～2021/1/31）

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）

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/は省の重篤度判定
⑥ 教育・トレーニング
⑦ ハイレベルセキュリティ検証



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**

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

結果をIPAから公表した他、第13回コラボレーション・プラットフォーム（2020年9月）で発表、**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

2019年度事業の効果

- コラボレーション・プラットフォームで成果発表とビジネスマッチングを実施、90名が参加
- ベンダー各社は有効性検証に参加したことを自社の宣伝活動に活用

コラボレーション・プラットフォームでビジネスマッチングを実施

（第13回、2020年9月28日）

- 「課題解決に役立つ対策技術のご紹介」と題し、検証に参加いただいたベンダーの製品紹介と、個別相談会を実施
- 90名参加

ベンダー各社が有効性検証の成果を自社製品の宣伝に活用

- **Visional社ブログ**
  - 「yamory」が IPA のセキュリティ製品の有効性検証の試行対象として選定
  - 「yamory」の終わりなき技術的挑戦。Visionalの仲間とともに、サイバーセキュリティの未来を創る。
- **アラクサラネットワークス社広報**
  - 「IPAがアラクサラのネットワーク可視化・異常検知ソリューション(AX-NV)の検証結果を公表」
  - 日刊工業新聞、日経新聞、日経産業新聞がアラクサラの広報を転載して紹介


yamory Blog

2020/4/13 お知らせ

「yamory」が IPA のセキュリティ製品の有効性検証の試行対象として選定

編集チーム

オープンソース脆弱性管理ツール「yamory」は、この度、独立行政法人情報処理推進機構（IPA）の「セキュリティ製品の有効性検証の試行」において対象製品に選ばれ、その結果が公表されました。

1. オープンソース脆弱性管理ツール「yamory（ヤモリー）」について
2. 「セキュリティ製品の有効性検証の試行」について
3. 有効性検証の試行結果

オープンソース脆弱性管理ツール「yamory（ヤモリー）」について

yamoryは、オープンソースの利用状況を自動で把握し、脆弱性を検出、管理・対策できるサービスです。

オープンソースに関する最新の脆弱性情報を用いて、yamory 独自の脆弱性データベースを構築しています。


AlaxalA

お問い合わせ

ホーム > 会社情報 > プレスリリース >

IPAがアラクサラのネットワーク可視化・異常検知ソリューション(AX-NV)の検証結果を公表

IPAがアラクサラのネットワーク可視化・異常検知ソリューション(AX-NV)の検証結果を公表

2020年5月25日

アラクサラネットワークス株式会社

アラクサラネットワークス株式会社（本社：神奈川県川崎市　代表取締役社長兼CEO 中川 勝博 ／ 以下、アラクサラ）のネットワーク可視化・異常検知ソリューションAX-Network-Visualization（AX-NV）は、独立行政法人情報処理推進機構（IPA）が行った「セキュリティ製品の有効性検証の試行」において「利用者の実環境における試行検証」の対象製品として選定され、その結果が公表されました。

https://www.ipa.go.jp/security/economics/shikoukekka2019.html

経済産業省の産業サイバーセキュリティ研究会の下に設置したWG3は、日本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に、有効性検証および実環境における試行導入検証を実施し、その内容を発信することで、ユーザが日本発の製品を選定しやすい環境の構築を進めています。

これを受けて「サイバーセキュリティ検証基盤構築に向けた有識者会議(以下、有識者会議)」をIPA内に2019年9月に立ち上げました。そして有識者会議が、日本のユーザ企業の重要課題に対応可能な日本発のセキュリティ製品として、AX-NVを対象にユーザの実環境における試行検証を行いました。

緑 青

今年度の取組（1/2）

有識者会議を６回開催。昨年度成果を踏まえ、検証基盤の構築・運用に関するより踏み込んだ検討を実施。公募を経て２製品を選定し、検証を実施。（緑検証）

緑
サイバーセキュリティ検証基盤の構築
・製品選定～有効性検証の仕組みの構築
・有効な検証結果公表の仕組みの構築

緑
サイバーセキュリティ検証基盤の運用
・製品選定～有効性検証の実施

緑
市場参入支援の仕組み検討
・日本発セキュリティ製品の市場参入を支援する、業界横断の仕組み検討（調査、課題分析、全体図）

青
2019年度成果「試行導入の手引き」改良
・セキュリティ製品のPOCに積極的に取組んでいるユーザ企業にヒアリング等実施

検証基盤運用のプロセス	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、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。 • 検証結果に基づき、当該製品・ベンダーのプロモーションを行う。

公募の結果、独自性、重要分野への該当度合等の観点から以下の２製品を検証対象に選定し、検証を実施：

・GUARDIAX（グレスアベイル社）
SaaS型のWAF（Webアプリケーション・ファイアウォール）

・WiSAS（スプライン・ネットワーク社）
WiFi環境の可視化、最適化、不正利用の防止等

緑 青

今年度の取組（2/2）

- 来年度以降を見据えてスタートアップ等ベンダーの市場参入支援の仕組みの検討も実施（緑検証）
- ユーザ企業の声等から「試行導入の手引き」の改良も実施（青検証）

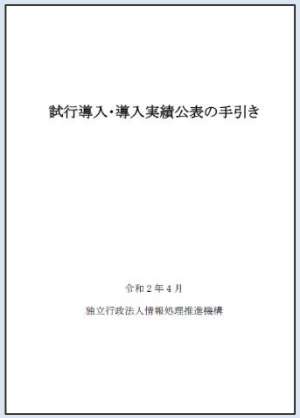
緑
サイバーセキュリティ検証基盤の構築
・製品選定～有効性検証の仕組みの構築
・有効な検証結果公表の仕組みの構築

緑
サイバーセキュリティ検証基盤の運用
・製品選定～有効性検証の実施

緑
市場参入支援の仕組み検討
・日本発セキュリティ製品の市場参入を支援する、業界横断の仕組み検討（調査、課題分析、全体図）

主な論点：
- **ベンチャー成長の各フェーズにおける課題と解決の方向性**
- **関係するプレイヤーと役割の整理**
- **本基盤の目指す所と提供すべき機能**
- **プロモーションの方式・場**
- **投資家による企業評価との連携**
- **公的機関の役割　他**

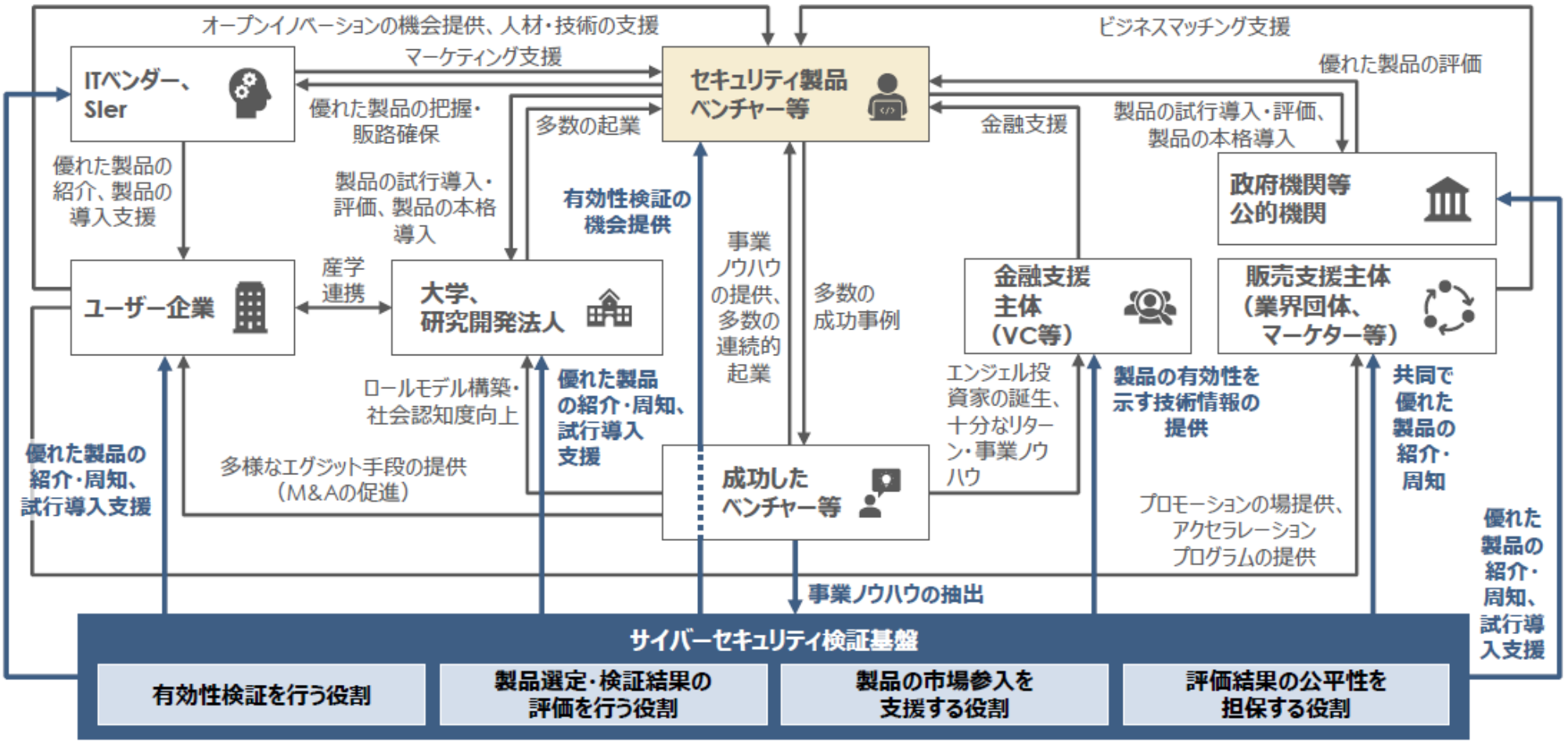
青
2019年度成果「試行導入の手引き」改良
・セキュリティ製品のPOCに積極的に取組んでいるユーザ企業にヒアリング等実施


試行導入・導入実績公表の手引き

令和２年４月
独立行政法人情報処理推進機構

ユーザ企業２社へのインタビュー調査等実施、以下の記述を強化：
- 試行導入結果の公表可否判断のポイント（メリット・デメリット）
- 試行導入をした上で実導入することのメリット（コスト最適化、運用の早期安定化等）
- ベンダー側が準備し、ユーザに提供すべき情報　等

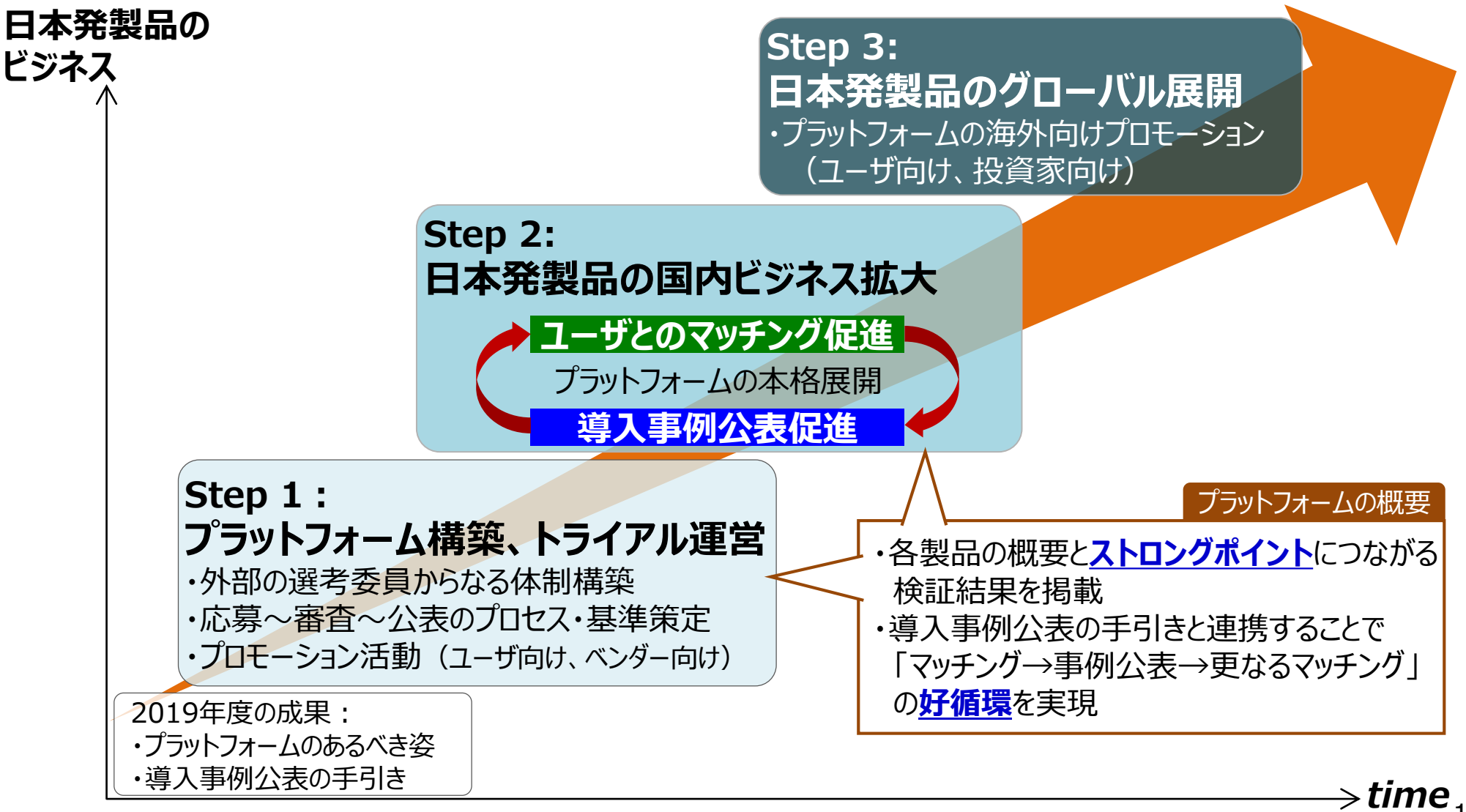
（参考）市場参入支援の仕組みを構成するプレイヤー・役割の関係図（現状案）



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

今後の方向性

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。



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

- 検証サービスの信頼性向上及び検証ビジネスの活性化のために、2019年度に作成した手引きについて、2020年度は**本編を拡充するとともに、検証サービス事業者・検証依頼者それぞれを対象とし、より具体的な記載を行った別冊を作成**。

実証

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＞
ドローン、スイッチ、ロボット掃除機、ノートPC

実証の成果と活用のイメージ

機器のサイバーセキュリティ確保のための セキュリティ検証手引き

検証サービス事業者、検証依頼者の双方が、検証における各フェーズにおいて留意すべき事項等を記載

別冊1：検証サービス事業者向け

本編の記載を検証サービス事業者向けに深掘り
・脅威分析の手法　・実施すべき検証項目　・検証の流れ　等

別冊2：検証依頼者（特に機器メーカ）向け

本編の記載を主な検証依頼者である機器メーカ向けに深掘り
・機器開発における検証の重要
・検証を依頼する際に必要な事項　等

別冊3：検証人材の育成について

検証人材の育成について深掘り
・検証人材に求められるスキル・知識、キャリアデザイン　等

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

赤

（参考）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

- 検証サービスの信頼性向上及び検証ビジネスの活性化のために、2019年度に作成した手引きについて、2020年度は**本編を拡充するとともに、検証サービス事業者・検証依頼者それぞれを対象とし、より具体的な記載を行った別冊を作成**。

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（2019年度作成）

- 検証スキルの向上や検証サービスの高度化を目的とし、検証サービス事業者が実施すべき事項や、検証依頼者が実施すべき事項や用意すべき情報、二者間のコミュニケーションにおいて留意すべき事項等を記載。
- 信頼できる検証サービス事業者を判断・選択するための基準を記載。

別冊1：セキュリティ検証の詳細解説書

- 検証ビジネス全体の底上げのために、検証サービス事業者が実施すべき脅威分析の手法や実施すべき検証項目、検証の流れを詳細に示す。
- 機器全般に汎用的に活用できる整理を目標とするが、対象の例としてIoT機器を例示し具体的な記載も行う。

別冊2： 機器メーカに向けたセキュリティ検証の解説書

- 機器メーカが実施すべき事項や用意すべき情報等、意図した検証を依頼するために必要な事項を詳細に示す。
- 攻撃手法への対策例や、検証結果を踏まえたリスク評価等の対応方針を示す。
- 機器開発におけるセキュリティ検証の重要性を示す。

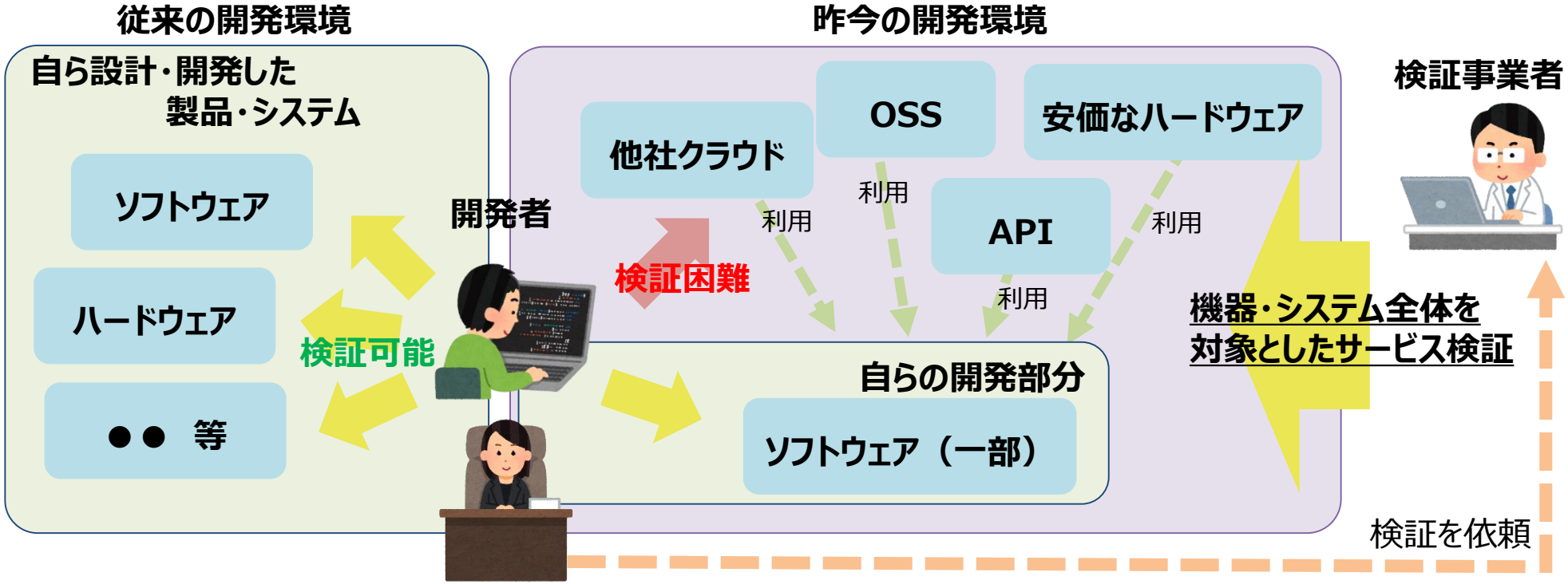
別冊3：検証人材の育成に向けた手引き

- 検証人材に求められるスキル・知識を示し、それらのスキル・知識を獲得するために望まれる取組を示す。
- 検証人材のキャリアを構想・設計する上で考慮すべき観点を示し、検証人材のキャリアの可能性を示す。

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

- クラウドやIoTなどの新しい技術の活用が進み、またオープンAPIやOSSが充実したことで、開発者自身がシステム全体を把握・検証することが困難になりつつある。サービスの品質を保証するために**官民において第三者によるセキュリティ検証の必要性が増大**し、**検証ビジネスの需要が拡大し、産業として重要になっていく**と考えられる。
- 2021年度は、これまで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ともに、検証事業者の信頼性の可視化手法など、機器やサービスを実現するシステムの検証サービスビジネスを更に発展させ利用を促進していくために必要な事項について検討を行う。



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

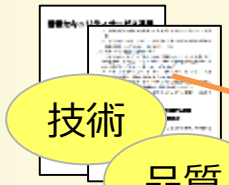
○情報セキュリティサービス基準適合サービスリスト（IPA）

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223サービスが掲載

- 情報セキュリティ監査（62サービス）
- 脆弱性診断（91サービス）
- デジタルフォレンジック（29サービス）
- セキュリティ監視・運用（41サービス）

2020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**（62サービス）　東京47、神奈川6、埼玉3、兵庫2、千葉1、京都1、大阪1、広島1
- **脆弱性診断**（91サービス）　東京73、神奈川6、大阪3、新潟2、兵庫2、宮城1、茨城1、千葉1、大分1、沖縄1
- **デジタルフォレンジック**（29サービス）　東京24、神奈川3、兵庫1、熊本1
- **セキュリティ監視・運用**（41サービス）　東京32、神奈川6、大阪1、兵庫1、大分1

2020年度に実施したアンケート・ヒアリング結果のまとめ

制度の更なる改善を図るため、ユーザ・ベンダ双方への**本制度の活用状況・ニーズ調査**を実施した。

＜制度の認知度・効果＞

- ユーザー企業の半数超が本制度を認知。
- 登録メリットを感じる事業者が存在するほか、登録サービスの利用者による品質評価で「期待未満」が皆無であるなど、制度の目的が満たされていることが観察される。

＜セキュリティサービスの利用動向＞

- **ユーザー企業の約３割がセキュリティサービスを外部に委託**している実態。
- 外部委託における課題として、多くの企業が「サービスが自社の求めている条件を満たしているかどうかの判断ができない」「サービス品質が適切かどうか、使ってみるまで判断できない」と回答。

＜制度において改善すべき事項＞

- ユーザー企業からは登録サービス数の増加を求める意見が最多であるほか、**基準適合サービスリストの改善を求める声**（条件に見合った検索が出来るようリストの記載項目をもっと充実させて欲しい等）があった。
- **地域のベンダーはもっと存在しているはずなのに、登録数としては少ない**印象を受ける。

＜セキュリティサービスの普及方策への期待＞

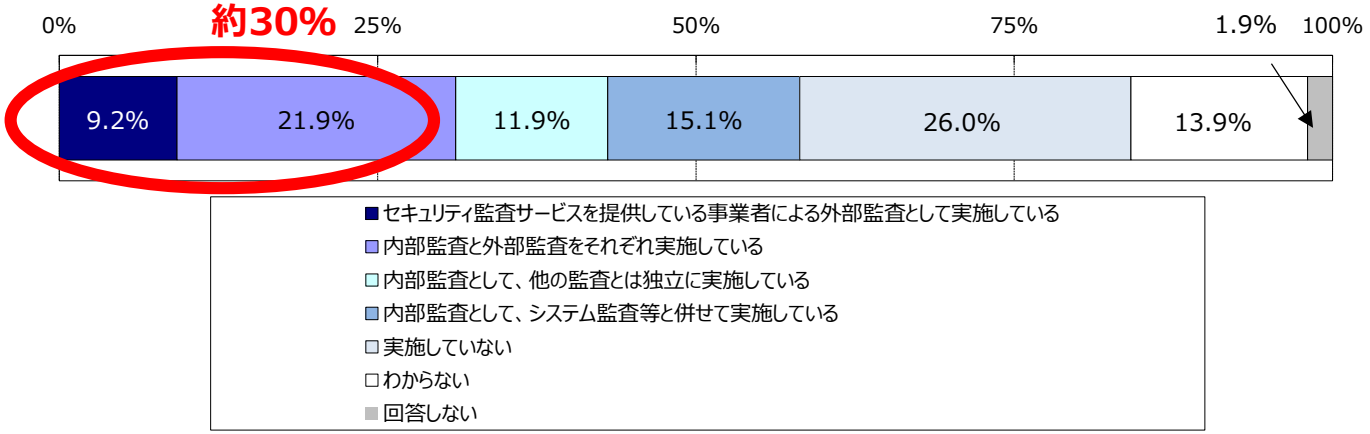
- ベンダーの自己負担で営業活動で認知向上に取り組むには限界があり、**本制度の普及を通じてユーザーへの認知度向上を期待**する意見あり。

※ 全国のユーザー企業でサイバーセキュリティ対策関連業務に従事している方411名を対象にアンケート調査を実施。ユーザー（企業や自治体）、セキュリティサービスベンダー各15社程度を対象にヒアリング調査を実施。

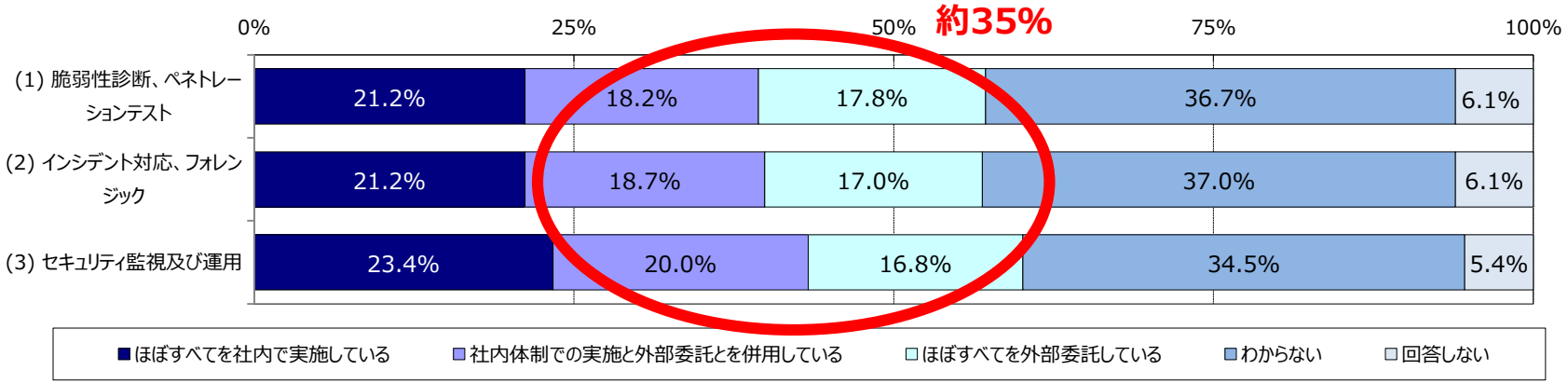
（参考）ユーザーアンケート調査結果①：セキュリティサービスの利用状況

- 企業の約３割が情報セキュリティサービスを外部に委託している。

情報セキュリティ監査サービス



脆弱性診断、デジタルフォレンジック、セキュリティ監視・運用サービス

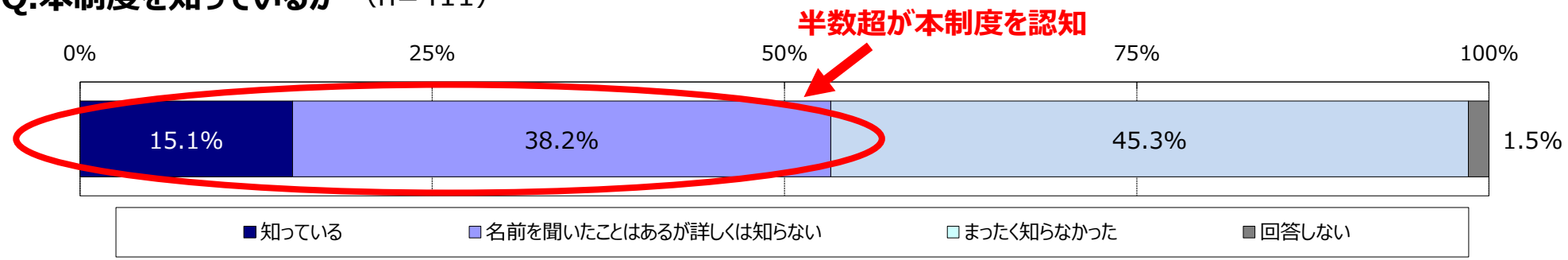


【アンケート概要】 対象：全国のユーザー企業でサイバーセキュリティ対策関連業務に従事している方　411名、 実施時期：2020年11月

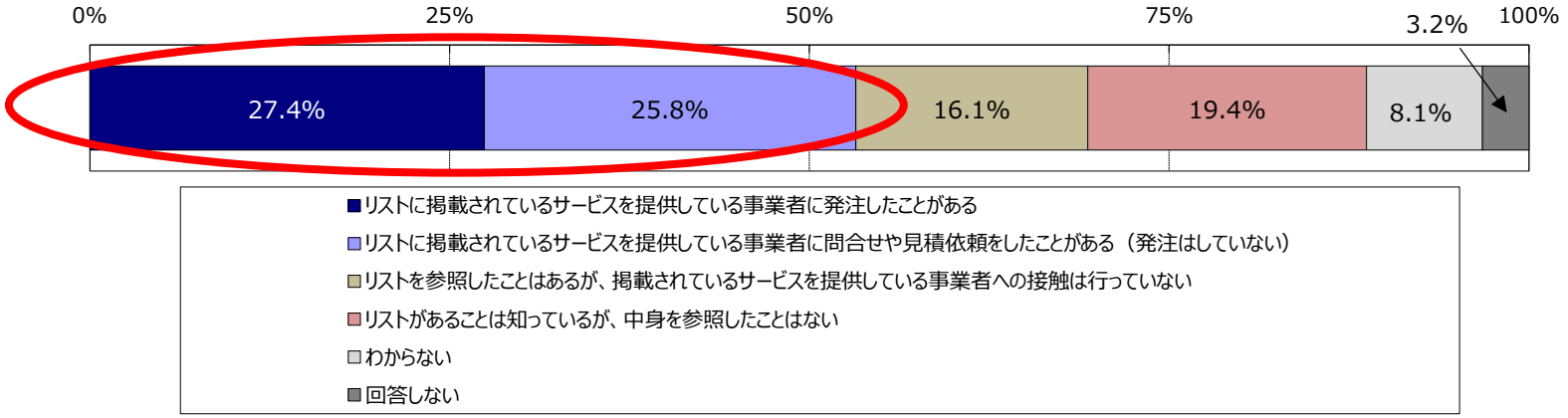
（参考）ユーザーアンケート調査結果②：本制度の認知・利用状況

- アンケート対象企業の半数超が本制度を認知しており、「知っている」と回答した人の約半数が、リスト掲載サービスの提供事業者へ実際に接触（問合せ、見積依頼、発注等）を行ったことがある。

Q.本制度を知っているか （n=411）



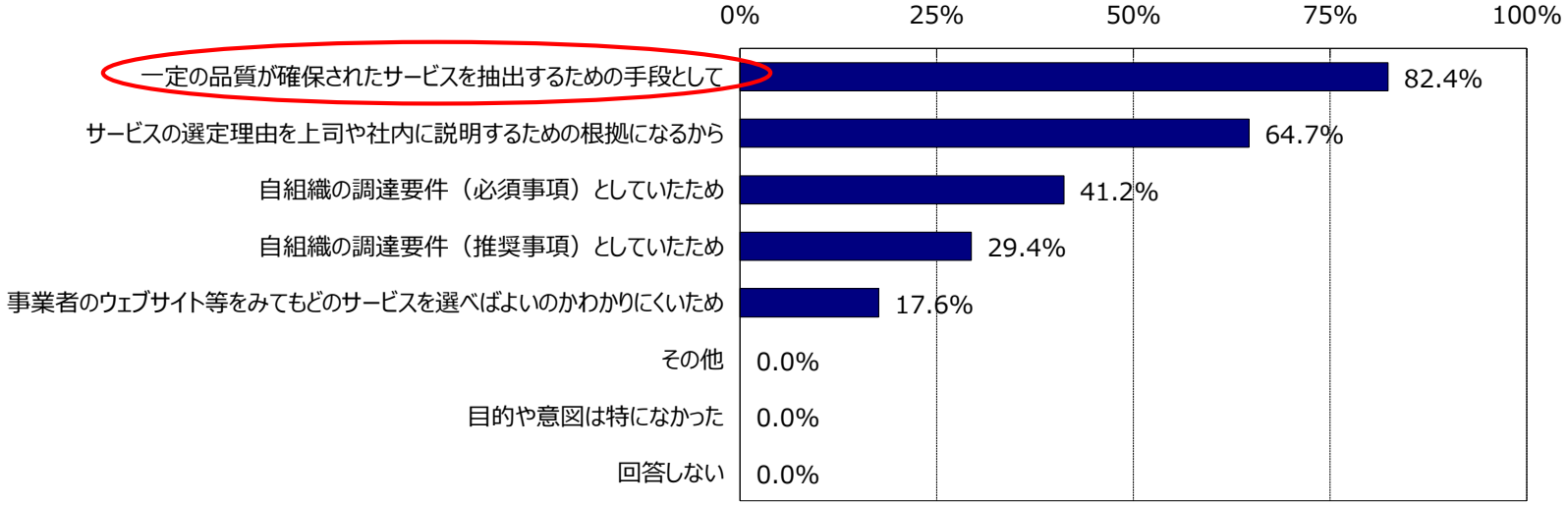
Q.情報セキュリティサービス基準適合サービスリストに掲載されたサービスを利用したことがあるか（n=62）



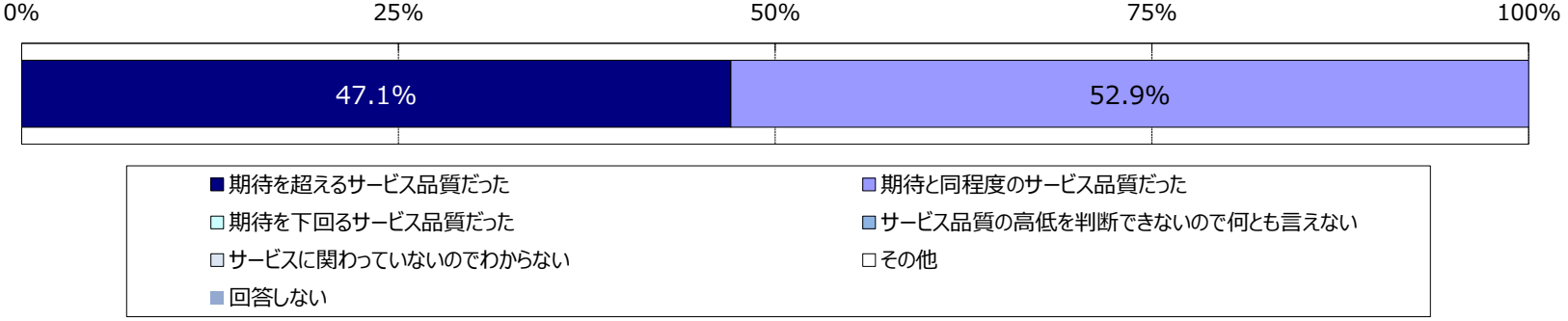
（参考）ユーザーアンケート調査結果②：本制度の認知・利用状況

- 本制度を利用した企業の約８割が、「一定の品質が確保されたサービスを抽出するため」に本制度を利用したと回答。
- 登録サービスの利用者による品質評価で「期待未満」が皆無であるなど、制度の目的が満たされていることが観察された。

Q.情報セキュリティサービス基準適合サービスリストの利用理由　（n=17）



Q.登録サービスを利用した結果（サービス品質）　（n=17）

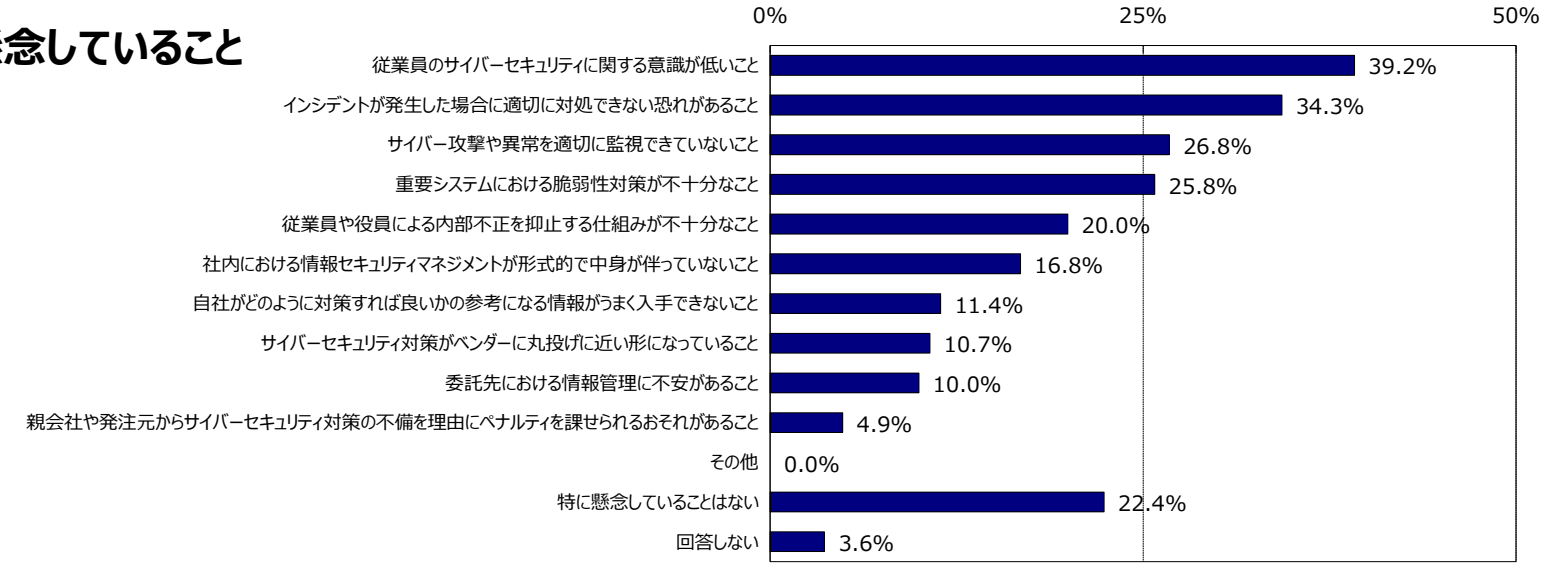


（参考）ユーザーアンケート調査結果③：セキュリティサービスの需要動向

現在の懸念や今後強化したい対策として、多くの企業が従業員教育や社内のセキュリティ管理・運用体制の強化を挙げている。コロナ禍を背景にテレワークやクラウドといったキーワードも注目されている。

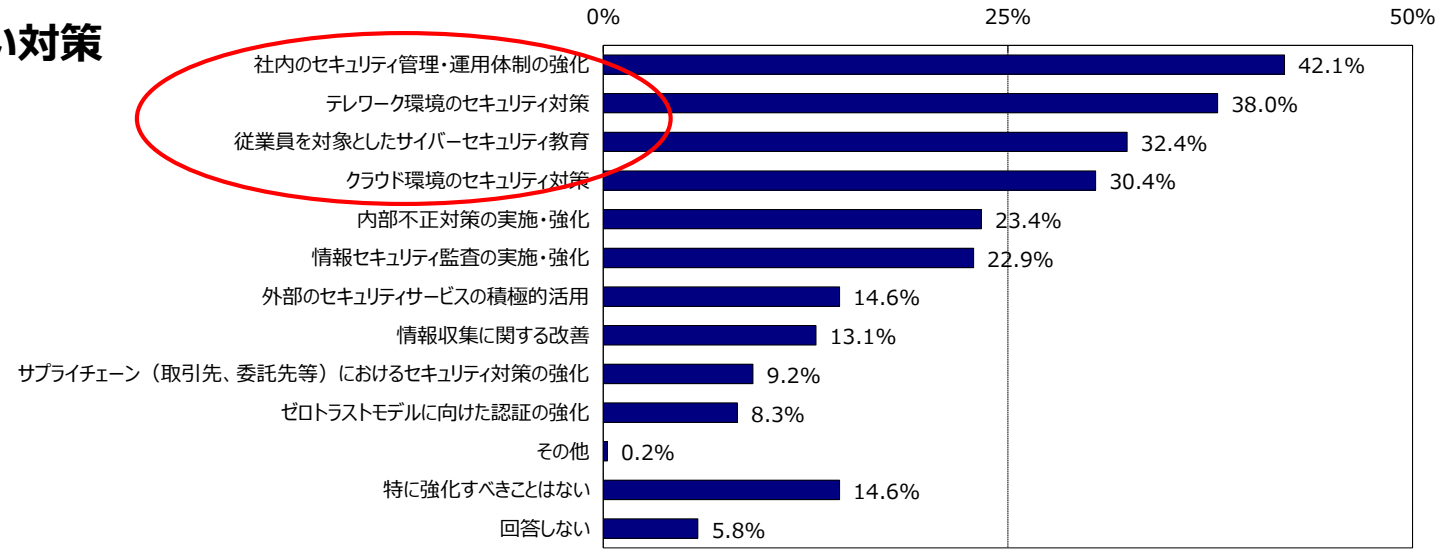
Q.現在懸念していること

（n=411）



Q.今後強化したい対策

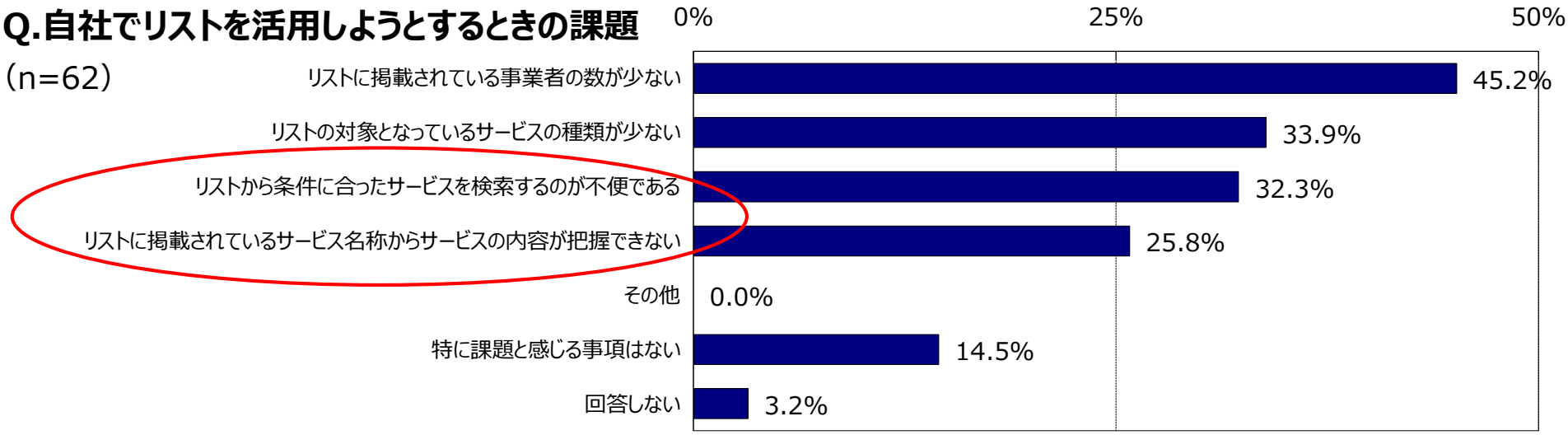
（n=411）



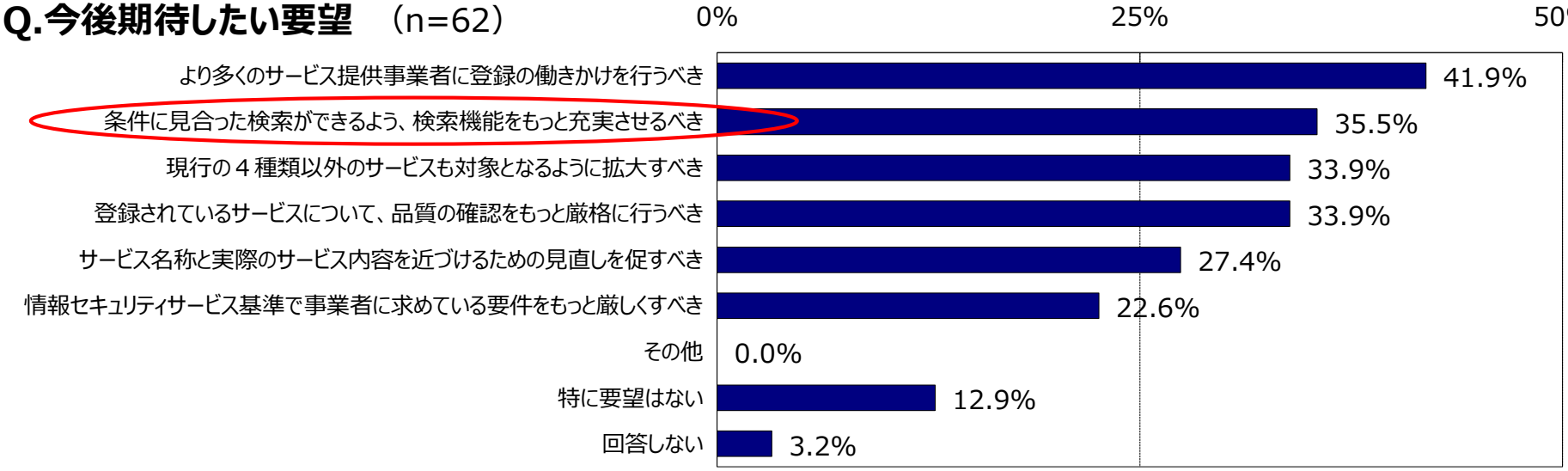
（参考）ユーザーアンケート調査結果④：制度への改善要望

- 登録サービス数の増加を求める意見が最多であり、引き続きセミナーでの制度紹介等、普及活動を継続していく。
- 適合基準サービスリストの改善要望の声を受け、リストの改善を行った。（詳細は次頁）

Q.自社でリストを活用しようとするときの課題



Q.今後期待したい要望　（n=62）



利用者等からのご要望を踏まえた改善状況

- 制度ユーザーからの要望を踏まえ、利用者にとってより分かりやすいものにすべく、基準適合サービスリストを改善。（2021年2月1日公開）
- 官側の利用促進が必要との意見もあるところ、政府統一基準群等への引用も検討中。

ユーザーからの要望

- リストから条件に合った事業者を検索するのが不便である
- リストに掲載されているサービス名称からサービスの内容が把握できない
- 条件に見合った検索ができるよう、検索機能をもっと充実させるべき　等

サービスの概要欄を追加
（どのようなサービスで、どのような手法で行っているか等）

主な顧客の分野・業種欄を追加

事業者のHPへのリンクを追加

サービス提供地域欄を追加

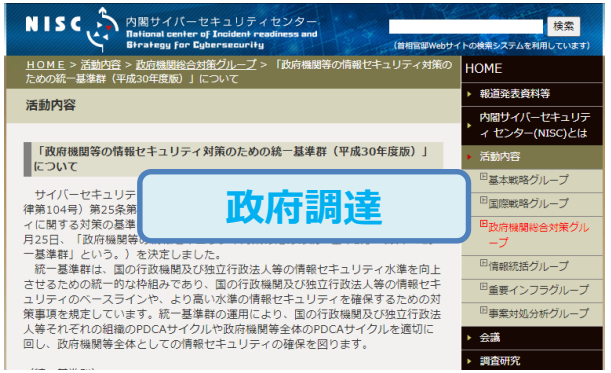
【基準適合サービスリスト（IPA公開）の改善】

サービス名称	事業者名称	事業者所在地	サービスの概要	主たる顧客対象の分野・業種	対象とする地域	登録年月日	有効期限	審査登録機関名
セコムプロフェッショナルサポート	セコムトラストシステムズ株式会社	東京都渋谷区神宮前一丁目5番1号　セコム本社ビル	主にPCのウイルス感染・不正アクセス・情報漏えい等のセキュリティ事案が発生した際の原因調査と早期復旧を目的としたサービスです。本サービスでは、デジタルフォレンジック技術を活用して対象データの保全・解析等を行います。2008年のサービス開始以来、2020年末までに480回のセキュリティ事案対応を行っています。情報セキュリティ担当者がいない中小企業への対応実績もあります。	建設業　化学　機械・電機・精密機器　医薬品・医療関連・化粧品　電気・ガス・熱供給・水道業　マスコミ・出版・印刷・広告　情報処理・ソフトウェア・ＳＩ　運輸・倉庫　商社・流通・卸売・小売業　銀行・証券・保険業　官公庁（官公庁・自治体　等）　その他サービス業　旅行業　銀行・証券・保険業　商社・流通・卸売・小売業　鉄鋼・金属　機械・電機・精密機器　自動車・輸送機器　繊維・アパレル　職業紹介・人材派遣	日本全国	2020/12/20	2022/12/19	日本セキュリティ監査協会（JASA）
インシデントレスポンス	PwCコンサルティング合同会社	東京都 千代田区丸の内2-6-1	企業を脅かすサイバー活動に対応するべく、PwCは専門知識と経験を持つ専門家からなるサイバーセキュリティインシデント対応チームを有しています。PwCのグローバルネットワークを活用し、世界中でインシデント対応アドバイザリーデジタルフォレンジック、ステークホルダーマネジメントといった支援を行います。	公務（官公庁・自治体　等）　その他サービス業　旅行業　銀行・証券・保険業　商社・流通・卸売・小売業　鉄鋼・金属　機械・電機・精密機器　自動車・輸送機器　繊維・アパレル　職業紹介・人材派遣	日本全国	2020/9/23	2022/9/22	日本セキュリティ監査協会（JASA）

有識者からの意見

- 政府調達で本制度が使われる等、官側の利用促進も図っていくべき　等

「政府機関等の情報セキュリティ対策のための統一基準群」等での引用も検討中。



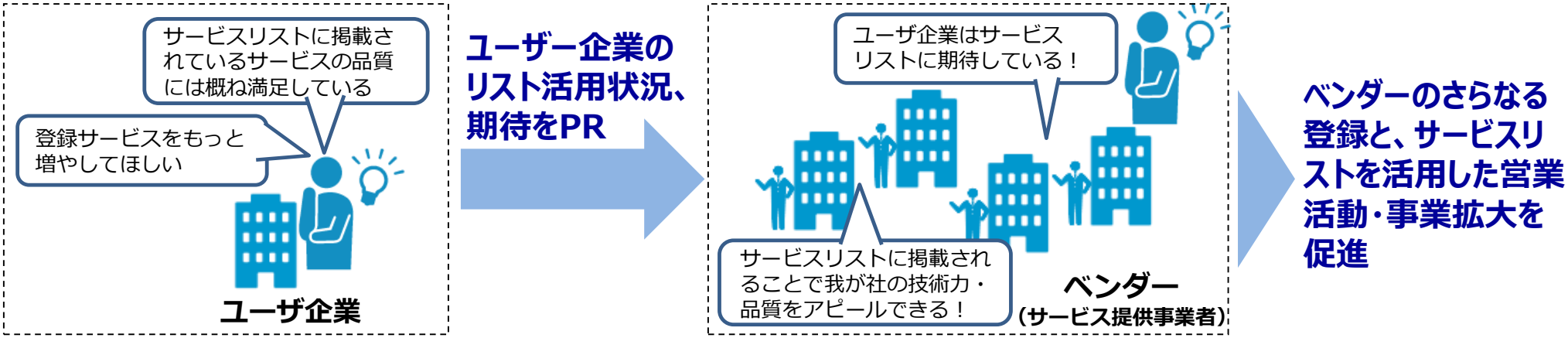
サービス提供事業者へのPR活動・登録の働きかけ

- アンケート結果より、本制度を利用したユーザー企業は登録サービスの品質に対してある一定の満足度を示しており、登録サービス数の増加を期待していることが明らかになった。
- 今後、本制度に寄せられたユーザー企業からの期待の声等を活用し、サービス提供事業者への本制度のPR活動、登録の働きかけを実施していく。

ユーザーからの要望

- リストに掲載されている事業者の数が少ない
- より多くのサービス提供事業者に登録の働きかけを行うべき　等

アンケート結果を活用し、サービス提供事業者へのPR活動・登録の働きかけを行うことで、サービス提供事業者の本制度への登録を促し、ユーザ企業の満足度の向上や、サービス提供事業者の事業機会の拡大につなげる。



地域での普及に向けた今後の方向性

- 地域のセキュリティの取組も重要である一方、本制度に登録されているサービス事業者の多くが東京に集中していることから、本制度の地域への普及も今後進めていくべき。
- セキュリティビジネスを地域に根付かせるべく、地域SECUNITY形成の取組と連携して進めていく。

有識者等からの意見

- 地域のベンダーはもっと存在しているはずなのに、登録数としては少ない印象を受ける　等

＜地域への普及策（案）＞

地域SECUNITY形成活動との連携

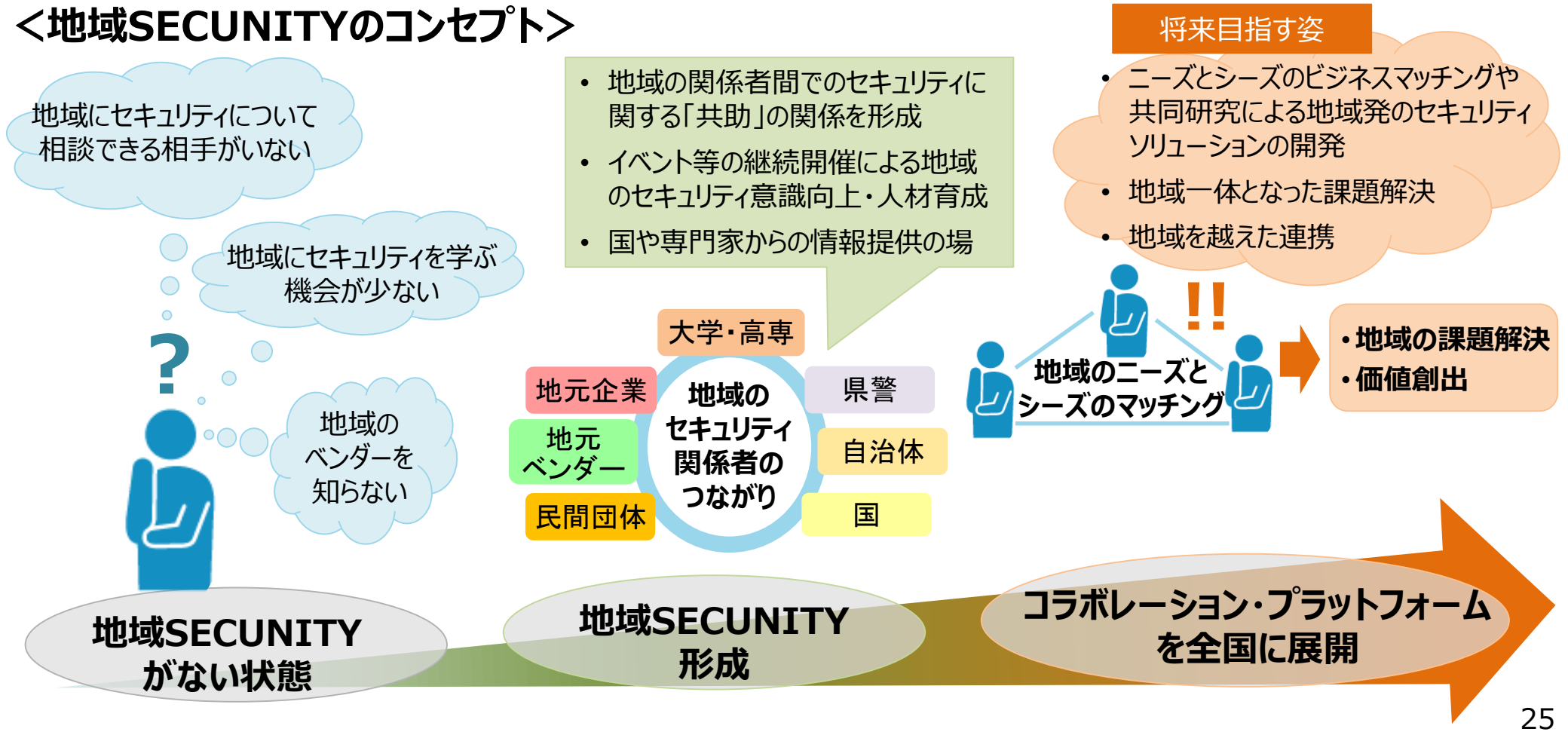
- **各地域のSECUNITYの場を使って、ユーザーに本制度に登録されているベンダーを紹介する。**

- 地元ベンダーが積極的に登録しようとする。（＝サービス基準を満たそうとすることで、サービス提供側の技術・品質力の向上）
- 地元ITベンダーが独力ではサービス基準を満たせない場合、既登録のセキュリティベンダー等と提携することにより、ビジネスマッチングを図るとともに、各地域にセキュリティビジネスを根付かせていく。

（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＞



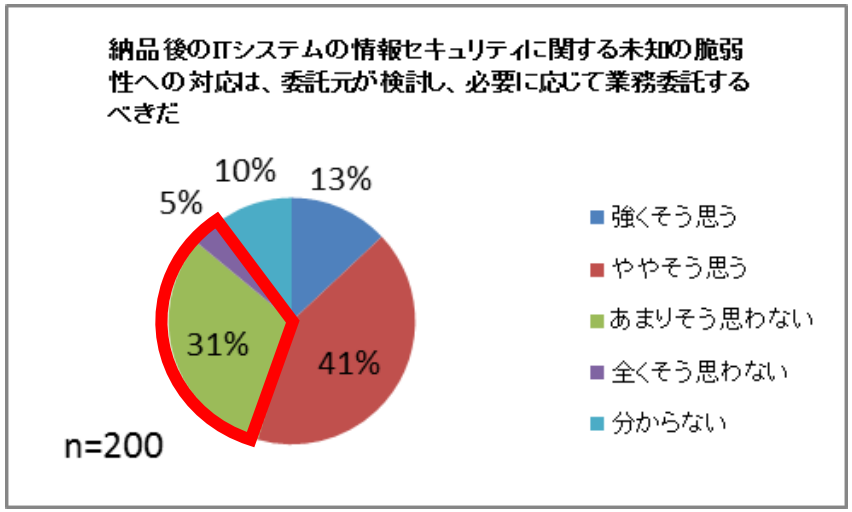
1．Proven in Japan（検証基盤）
2．情報セキュリティサービス審査登録制度
3．セキュリティに関する契約の在り方の検討
4．サイバーセキュリティお助け隊
5．中小企業向けセキュリティ製品の検証
6．コラボレーション・プラットフォーム

セキュリティに関する契約の課題

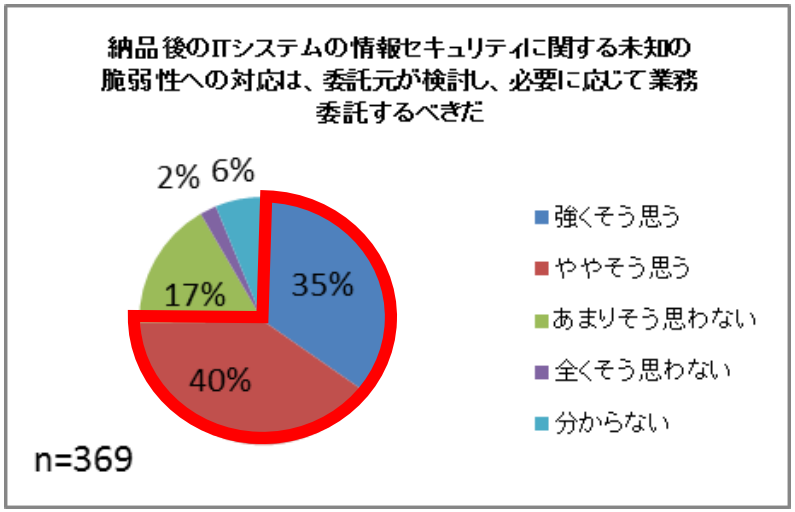
前回WG3資料の再掲

- 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

検討体制

部会

- 主査　平野高志　ブレークモア法律事務所
- 委員　大谷和子　株式会社日本総合研究所
- 〃　松原真弓　富士通株式会社
- 〃　高岡詠子　上智大学
- 〃　坂東直樹　アップデートテクノロジー株式会社
- 〃　三宅　晃　JUAS
- 〃　森田宏樹　国立大学法人東京大学

WG1

- 主査　森田宏樹　国立大学法人東京大学
- 委員　伊藤雅浩　シティライツ法律事務所
- 〃　大谷和子　株式会社日本総合研究所
- 〃　高柳祐治　株式会社日立製作所
- 〃　荻野朋美　東京海上日動火災保険株式会社
- 〃　木内里美　株式会社オラン
- 〃　野々垣典男　プロメトリスト
- 〃　坂東直樹　アップデートテクノロジー株式会社
- 〃　藤田美雄　株式会社大塚商会
- 〃　松島淳也　松島総合法律事務所
- 専門委員　村田和希　東京丸の内法律事務所

セキュリティ検討PT

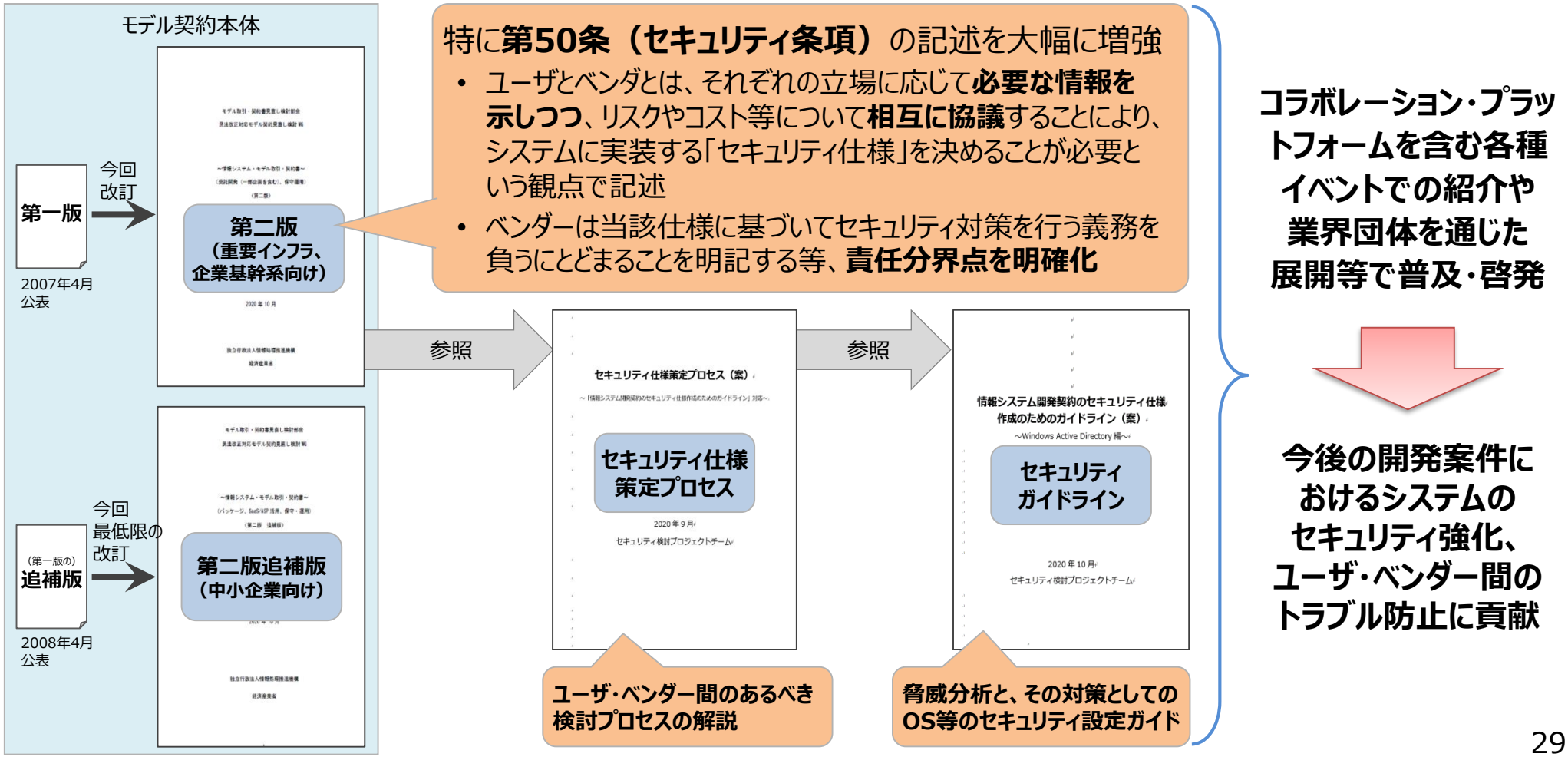
計12回開催（2019年9月～2020年9月）

- 主査　加藤智巳　株式会社ラック
- 委員　阿部恭一　ANAシステムズ株式会社
- 〃　伊藤 昇　株式会社大塚商会
- 〃　江原悠介　PwCあらた有限責任監査法人
- 〃　大谷和子　株式会社日本総合研究所
- 〃　小川隆一　IPA
- 〃　垣内由梨香　日本マイクロソフト株式会社
- 〃　金森直樹　株式会社TKC
- 〃　田上利博　サイバートラスト株式会社
- 〃　坪井正広　株式会社野村総合研究所
- 〃　中尾康二　NICT
- 〃　萩原健太　GSX(株)／Software ISAC
- 〃　板東直樹　アップデートテクノロジー株式会社
- 〃　深津 博　愛知医科大学病院
- 〃　丸山満彦　PwCコンサルティング合同会社
- 〃　山崎文明　情報安全保障研究所合同会社
- 〃　山根義則　三菱自動車工業株式会社

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

セキュリティ関連の成果物概要と今後の普及策

- モデル契約本体はセキュリティ条項（第50条）等の記述を強化（WG1成果）
- セキュリティ仕様策定を支援するための参照文書を２点作成（セキュリティ検討PT成果）
  - 「セキュリティ仕様策定プロセス」
  - 「情報システム開発契約のセキュリティ仕様作成のためのガイドライン（Windows Active Directory編）」
- 各種イベントでの講演や各業界団体を通した展開等により普及・啓発を進める



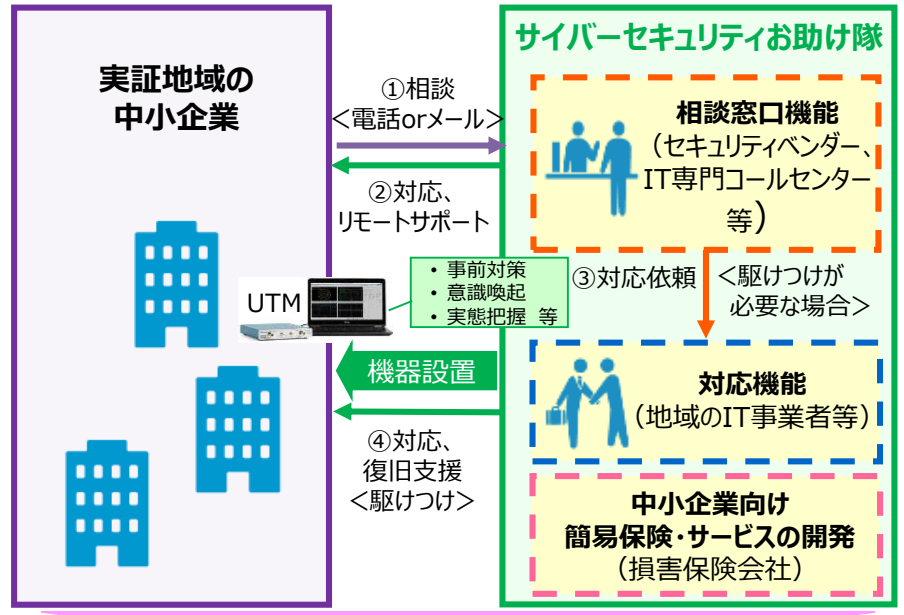
1．Proven in Japan（検証基盤）
2．情報セキュリティサービス審査登録制度
3．セキュリティに関する契約の在り方の検討
4．サイバーセキュリティお助け隊
5．中小企業向けセキュリティ製品の検証
6．コラボレーション・プラットフォーム

サイバーセキュリティお助け隊実証事業(2020年度)

- 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（全国で15件）。
- 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。**

＜2020年度の実証地域＞

＜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

※2019年度実証地域（全8地域、1064社の中小企業が参加）：
①宮城、岩手、福島②新潟③長野、群馬、栃木、茨城、埼玉④神奈川⑤石川、富山、福井⑥愛知⑦大阪、京都、兵庫⑧広島、山口

（参考）サイバーセキュリティお助け隊チームリスト（2020年度）

	対象 （地域／産業分野）	実施体制 ●：実施主体）
①	北海道	●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
②	宮城県、山形県、 秋田県、青森県	●東北インフォメーション・システムズ株式会社 ・ハイテックシステム株式会社 ・秋田システムマネージメント株式会社 ・あいおいニッセイ同和損害保険株式会社
③	岩手県	●富士ソフト株式会社 ・東京海上日動火災保険株式会社
④	岩手県、宮城県、 福島県	●株式会社デジタルハーツ ・損害保険ジャパン株式会社
⑤	千葉県、埼玉県	●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
⑥	千葉県	●SOMPOリスクマネジメント株式会社 ・ちばぎんコンピューターサービス株式会社 ・株式会社千葉銀行　・株式会社ラック ・損害保険ジャパン株式会社
⑦	岐阜県を中心とする 中部エリア	●MS&ADインターリスク総研株式会社 ・中部電力株式会社　・中部電力ミライズ株式会社 ・株式会社中電シーティーアイ ・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
⑧	愛知県、岐阜県、 三重県	●名古屋商工会議所 ・株式会社日立システムズ ・西日本電信電話株式会社 ・東京海上日動火災保険株式会社 ・損害保険ジャパン株式会社
⑨	滋賀県、奈良県、 和歌山県	●大阪商工会議所 ・日本電気株式会社 ・東京海上日動火災保険株式会社 ・キューアンドエー株式会社

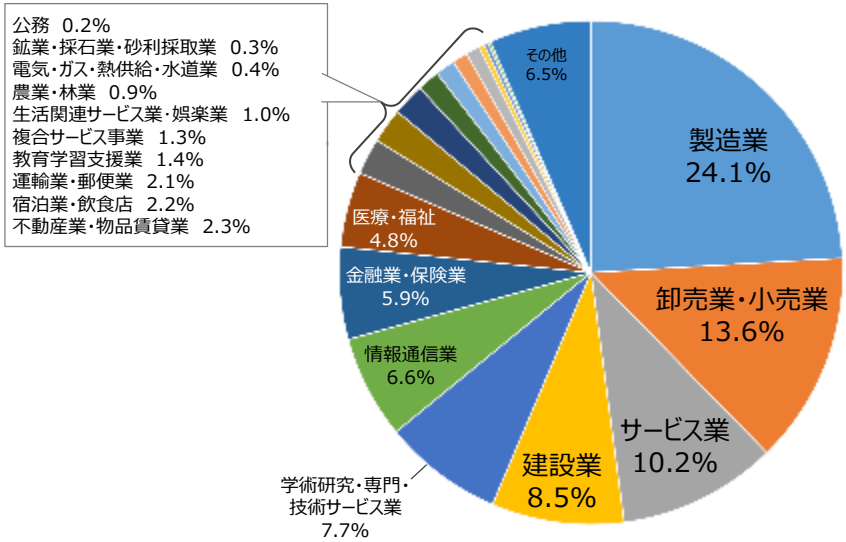
	対象 （地域／産業分野）	実施体制 ●：実施主体
⑩	香川県	●高松商工会議所 ・株式会社STNet ・西日本電信電話株式会社 ・キャノンマーケティングジャパン株式会社 ・損害保険ジャパン株式会社 ・東京海上日動火災保険株式会社
⑪	福岡県を中心とした 九州６県	●株式会社BCC ・日本電気株式会社 ・東京海上日動火災保険株式会社 ・NECフィールディング株式会社
⑫	熊本県	●西日本電信電話株式会社　熊本支店 ・株式会社くまなんピーシーネット ・東京海上日動火災保険株式会社 ・一般社団法人熊本県サイバーセキュリティ推進協議会
⑬	沖縄県	●沖電グローバルシステムズ株式会社 ・株式会社セキュアイノベーション ・ファーストライディングテクノロジー株式会社 ・那覇商工会議所 ・沖縄電力株式会社 ・損害保険ジャパン株式会社
⑭	防衛・航空宇宙 産業	●株式会社PFU ・株式会社エヴァアビエーション ・富士通株式会社 ・ウェブルート株式会社 ・損害保険ジャパン株式会社
⑮	自動車産業	●東京海上日動リスクコンサルティング株式会社 ・東京海上日動火災保険株式会社 ・エヌ・ティ・ティ・コミュニケーションズ株式会社 ・NTTコム ソリューションズ株式会社 ・NTTセキュリティ・ジャパン株式会社 ・ジェイズ・コミュニケーション株式会社

2020年度お助け隊実証事業の結果
①実証参加企業の内訳と中小企業へのサイバー攻撃等の実態

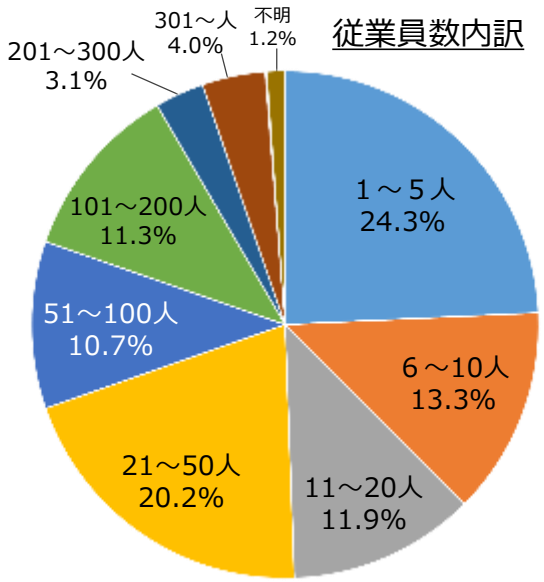
- 1,117社の中小企業が今年度の実証事業に参加。
- 昨年度の実証の結果と同様、内外に向けた不正通信等が数多く検知されるとともに、中小企業の実態や課題が浮き彫りに。

2020年度実証参加中小企業の内訳

業種内訳



従業員数内訳



＜実証における事例（一部）＞

- Webセキュリティ診断において緊急性の高い脆弱性が発見されるなど、中小企業のウェブサイトの多くは、過去に構築後、**脆弱性に対する対応が行われないまま放置されている**例が数多く見られた。
- リスク診断等の簡易ツールを用意しても**自主的に取り組める中小企業は少なく**、個別サポートが必要。
- EDRの検知レポートを送付しても読んでもらえないことが多く、電話で説明すると喜んでもらえる。

商用化においては、コストとの見合いでどこまできめ細かにサポート出来るかが課題。

2020年度お助け隊実証事業の結果　②リモート対処事例

- コロナ禍において、できる限り**リモートでの対処**を実施。

事例１	EDRサービスでブラウザハイジャッカーを確認。駆除方法を案内したが中小企業が自力で対応出来なかったため、お助け隊が**リモートで駆除実施**。
事例２	UTM設置後、**C&Cコールバックとみられる通信を検知**。コールセンターより対象の中小企業に連絡。該当端末は買替となり、その後アラートが出ていないことを確認済み。
事例３	UTMサービスを導入した企業において**「不正なIPアドレスへの通信」**が成立していることが確認されたため、緊急度「高」のアラートを発報し、支援を実施。
事例４	UTMがトロイの木馬を検知。中小企業から相談を受け、お助け隊事業者がリモート支援を実施。**フルスキャンの結果、内在していた別リスクを駆除**。
事例５	**「アドウェア感染」**や、**「フィッシングサイトへのアクセス」**を検知し、対象中小企業と連携の上、リモートでの対処を実施。

2020年度お助け隊実証事業の結果　③産業別実証での気づき

- 2020年度は新たな取組として実施した産業別実証では、業界内での仕組み作りを求める声等があった。

自動車産業

- 外部診断の結果、実証参加企業全体のセキュリティ管理レベルの平均は、**製造業の平均と比べ比較的高かった**。
- 取引先からの要請は高まっているが、セキュリティ対策を行う上でのリソースが全般的に不足。**業界内での人材プールを共有できる仕組み**等の整備が課題。
- **同業他社の状況**を知ることができると、投資判断における経営者への動機付けになる。

防衛・航空宇宙産業

- セルフアセスメント（情報セキュリティ整備状況診断）を実施したところ、今後業界として求められるであろう**レベルに到達していた企業は10%** ※
- **防衛・航空宇宙産業という名目で特別な対策を要求**された企業は**38%**
  要求された対策の中にはアクセス権に関するものもある一方で、セルフアセスメントでは、**秘密情報へのアクセス管理について約半数の企業が実施できていない**と回答。

※CMMC Level 1の17項目全てを達成しているか否かで判定

- 産業別実証事業は、「自動車産業の中小企業サプライヤーを対象とした実証」と、「防衛・航空宇宙産業に関わる中小企業及び今後防衛・航空宇宙産業に参入を検討する中小企業を対象とした実証」を実施。

実証事業から民間サービス化（商用化）の成功のポイント

- 実証事業を経て民間サービスが開発されたり、継続的なサービス展開が図られたりと、お助け隊サービスの民間への移行が進みつつある。
- お助け隊サービスをブランド化し、審査体制を構築すること等により、民間でのサービス展開を支援していく。

実証事業から民間サービスへの移行状況

- 2019年度実証事業後の2020年4月、**「サイバーセキュリティお助け隊サービス」を商用化。**

（大阪商工会議所）

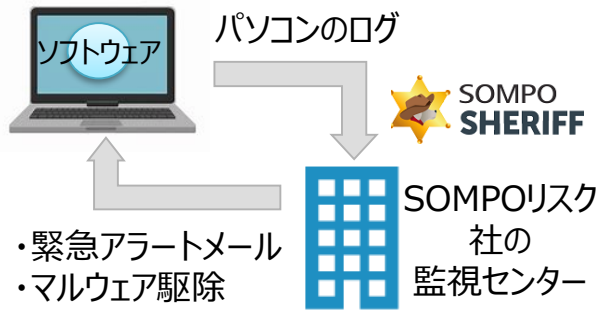
実証を通じて中小企業にとって必要な機能・サービスを精査することで、安価なサービスを実現。

（商工会議所会員月6,600円（年79,200円）
非会員月8,250円（年99,000円））

- 実証事業での経験やノウハウを元に、2019年12月に**新サービスを提供開始。**

（SOMPOリスクマネジメント）

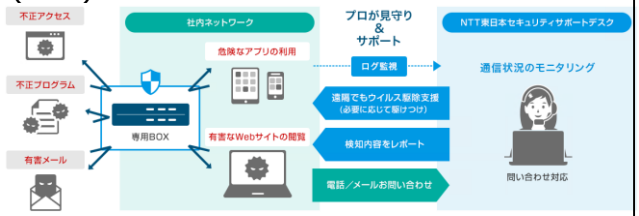
<サービスのイメージ>



- 2019年度実証事業に参加中小企業**148社の内、約4割の61社が有償サービスへ移行。**
※2020年2月17日時点

（NTT東日本）

(参考)同社の提供する「おまかせサイバーみまもり」



実証事業の取組（説明会や標的型メール攻撃の訓練、機器設置による脅威の可視化等）により、約4割の中小企業が民間サービスへの移行を希望。

【有償サービスへの移行時のポイント（一例）】

✓ 脅威状況を簡易レポートにて可視化しつつ、毎月メールで提供する仕組みを用意することで、**中小企業に対して継続的にセキュリティ脅威の訴求と可視化を実施**した。

✓ 実証事業終了時のアンケートと共に、上記レポートを活用しながら、再度**セキュリティ対策の必要性を中小企業へ個別に訴求**して継続勧奨を実施した。 等

実証事業から民間サービスへの移行・普及促進に向けたステップ

- 実証事業で得られた知見に基づき、中小企業向けのセキュリティサービス（お助け隊サービス）が満たすべき基準を整理、パブコメを経て２月末にIPAより公開。
- 2021年3月に第１回審査を行い、４月以降、お助け隊マークが付与された民間サービスが市場に展開される予定。

2019年度（実証１年目）	2020年度（実証２年目）	2021年度以降（民間で自走）

サイバーセキュリティ お助け隊

攻撃実態の把握

ニーズを踏まえたサービスのスリム化

地域特性・産業特性の考慮

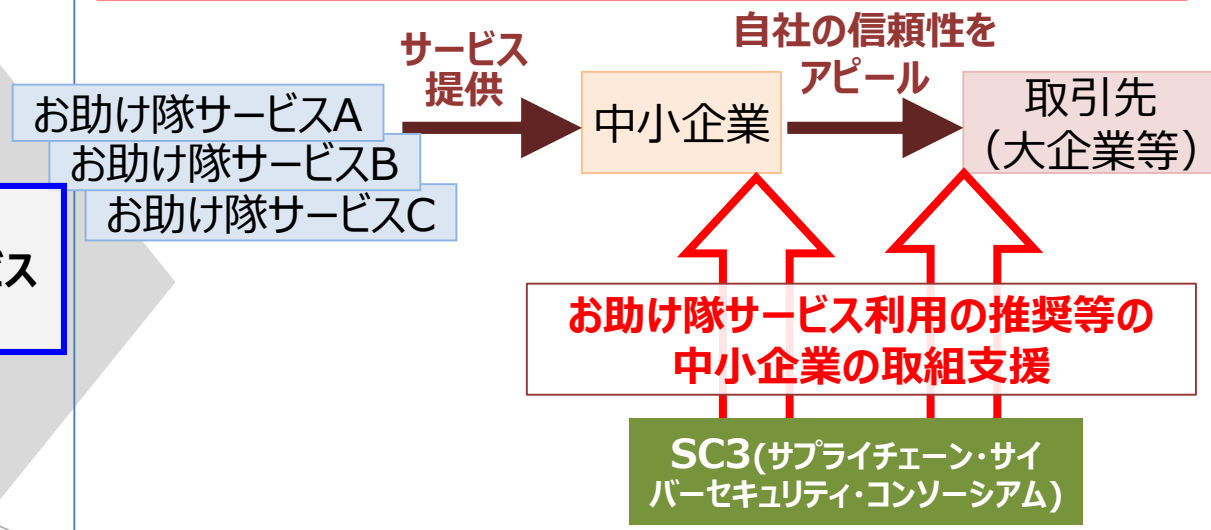
実証事業：
中小企業が利用しやすい安価なセキュリティサービスの開発

意識啓発

事前対策とのセットによるリスク低減

導入・運用負荷を下げる方法の検討

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の商標利用権を付与。



→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）お助け隊サービス基準の概要

大項目	小項目	内容
要件	相談窓口	お助け隊サービスの導入・運用中に関するユーザからの各種相談を一元的に受け付ける窓口を設置すること
	監視の仕組み	・ユーザのネットワークを24時間監視し、攻撃を検知・通知する仕組み（UTM等のツールと監視サービスから構成）を提供すること（ネットワーク一括監視型の場合） ・ユーザの端末（PCやサーバ）を24時間監視し、攻撃を検知・通知する仕組み（EDR等のツールと監視サービスから構成）を提供すること（端末監視型の場合）
	緊急時の対応支援	・営業エリア内であればユーザの指定する場所に技術者を派遣できること ・サービス規約等でユーザと合意した範囲であればリモート対応でも可
	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でも導入・運用できるような工夫が凝らされていること 例：・マニュアルに書かれている通りに数回クリックするだけでインストール完了
	中小企業でも導入・維持できる価格	・月額1万円以下（税抜き）（条件付きで可。PC〇台までなら等） ・最低契約年数は2年以内 ・初期費用、契約年数等の細かな条件もユーザに分かりやすく説明すること
	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保証するサイバー保険が付帯されていること。
	上記機能のワンパッケージ提供	ユーザがお助け隊サービスを購入したり、利用中の問合せ等を行う窓口が一本化されていること（営業窓口と技術支援窓口は別でも可）
	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上記構成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どうしの深いレベルの情報共有に合意し、そのための準備を行うこと
	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（地場のITベンダーは中小企業が多いことも考慮し、緩めの条件とする。）
	更新	2年毎に更新審査を受けること
附則 （推奨事項他）	独自のオプションサービス提供	例：・事前アセスメント等の簡易コンサルティングサービス ・端末監視の仕組み ・デジタルフォレンジック等より広い範囲をカバーするサイバー保険の提供 等
	日本発の技術・製品の活用	日本特有の攻撃に対応するため

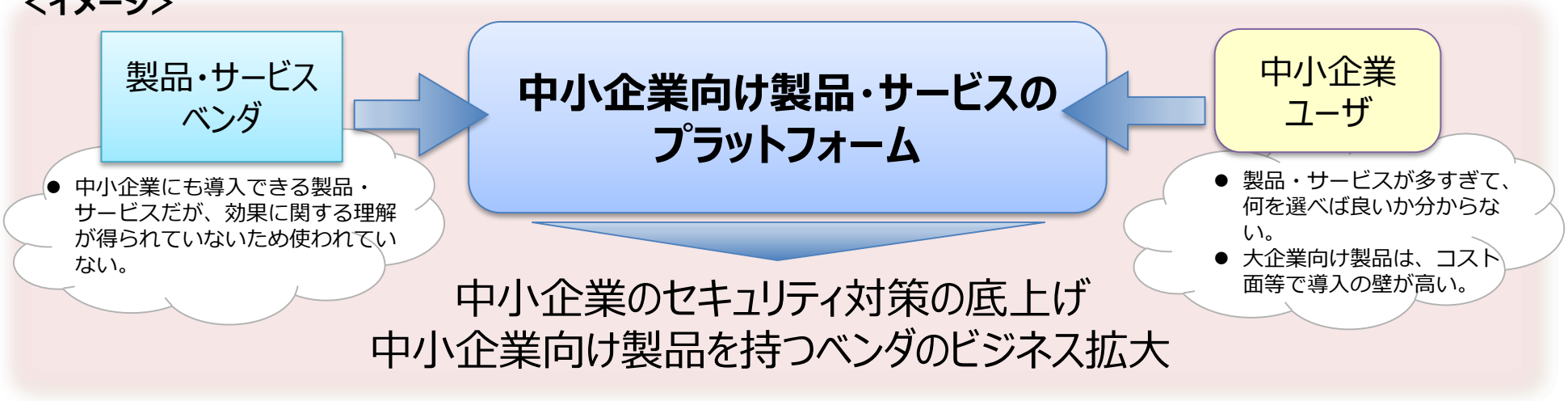
1．Proven in Japan（検証基盤）
2．情報セキュリティサービス審査登録制度
3．セキュリティに関する契約の在り方の検討
4．サイバーセキュリティお助け隊
5．中小企業向けセキュリティ製品の検証
6．コラボレーション・プラットフォームと

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

前回WG3資料の再掲

2019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

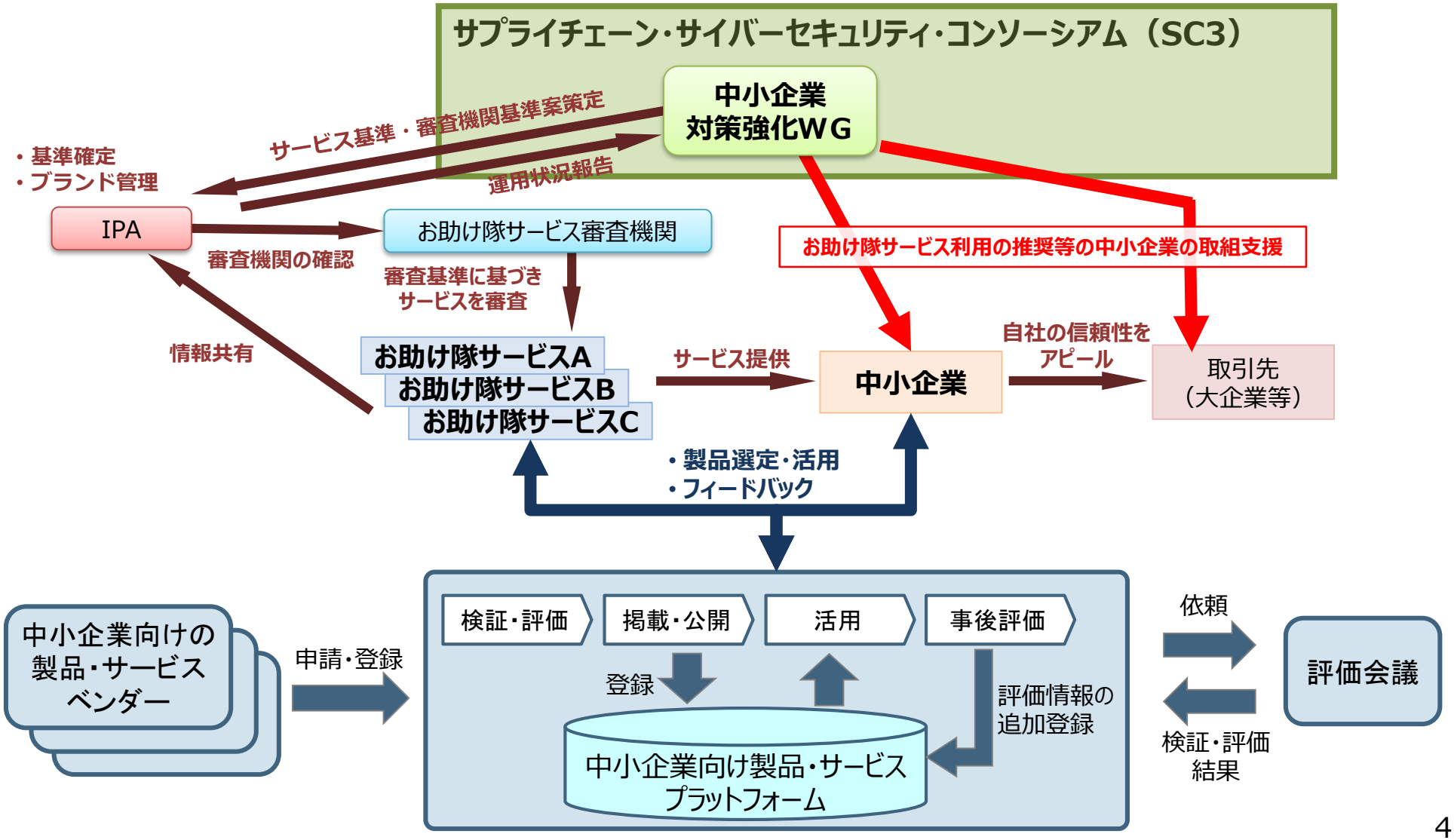
・導入及び運用のコスト
・製品性能の客観的な根拠
・オールインワン
・未知の脅威への対応　等

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

今後の方向性（案）

- 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）2019年度成果：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

- 2019年度の検証事業において、ベンダー３社、中小企業ユーザ６社のご協力をいただき、評価項目を作成した。

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

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2020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**今年度は計４回オンライン開催**。

	開催日	参加人数	テーマ
第13回	**2020年9月28日**	**90名**	**課題解決に役立つ対策技術のご紹介**
	➢ 検証基盤構築事業ならび に中小企業向け製品検証事業の取り組みの紹介 ➢ 事業に参加いただいた製品・ソリューションの個別相談会の実施		
第14回	**10月30日**	**91名**	**テレワークとセキュリティ**
	➢ 前半は講演、後半は⑴テレワークで注意すべきサイバー攻撃、⑵テレワークにおけるガバナンス、⑶テレワークにおけるインシデント対応のあり方をテーマに、解決策や対策のヒントなどをベンダー・ユーザー双方の立場から議論いただくパネルディスカッションを実施。		
第15回	**2021年1月29日**	**123名**	**中小企業との情報共有のあり方**
	➢ 今年度のお助け隊実証事業での事例の紹介 ➢ 中小企業とのサイバーセキュリティ関連での脅威情報やその対策情報の共有のあり方や、課題やその解決策についてあらゆる立場から議論いただくパネルディスカッションを実施。		
第16回	**2月25日**	**172名**	**クラウドシフトのセキュリティ**
	➢ テレワーク、DX等の新しい業務形態やゼロトラスト、データドリブン等のパラダイムの受容が求められる中、クラウド利用におけるセキュリティ課題と対応について講演とパネルディスカッションを実施。		

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。
- コロナの状況を踏まえ、オンラインでの開催を工夫しながら継続しつつ、物理開催の復活を目指して企画の検討等を進めていく。

【参加者からのアンケート結果（第14回の一部抜粋）】

- 政策や他社動向について大変勉強になりました。
- 各パートにつながりがありコンテンツとして大変有意義でした。
- 最後に質疑応答の時間があれば良かったです。
- 取り上げて欲しいテーマ　①クラウド利用におけるセキュリティ　②DXにおけるセキュリティ　③脅威の最新動向
- オンラインより会場での開催が良いですね。

（前回WG3資料の再掲）コラボレーション・プラットフォームの目指す姿

【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。


経済産業省