経済産業省

資料３

産業サイバーセキュリティ強化へ向けた アクションプラン

経済産業省

商務情報政策局

アクションプランの4つの柱

１．サプライチェーンサイバーセキュリティ強化パッケージ

２．サイバーセキュリティ経営強化パッケージ

３．サイバーセキュリティ人材育成・活躍促進パッケージ

４．セキュリティビジネスエコシステム創造パッケージ

１．グローバルサプライチェーンに対応した **サプライチェーンサイバーセキュリティ強化パッケージ**

(１)サイバー・フィジカル・セキュリティ対策フレームワークの策定

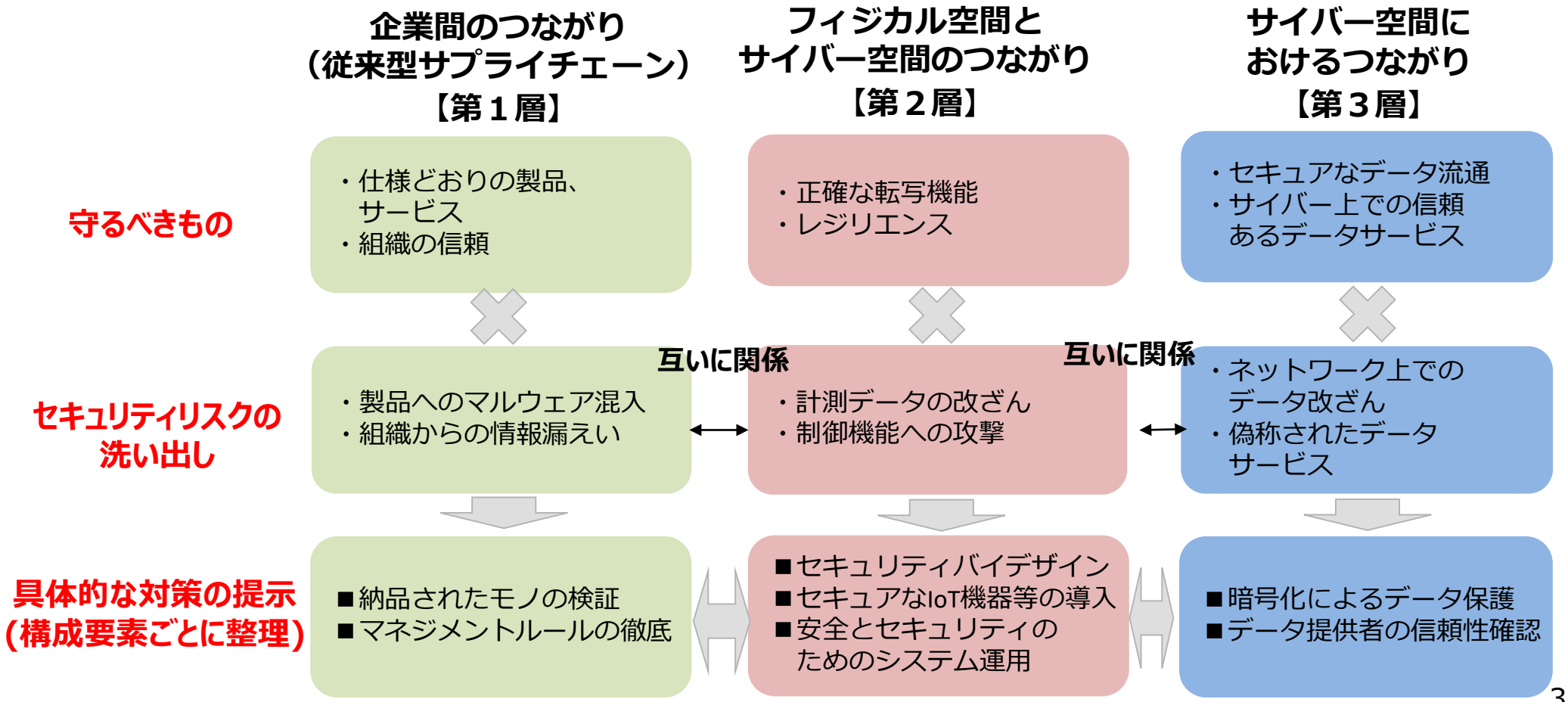
(２)サイバー・フィジカル・セキュリティ対策フレームワークの国際化の推進

(３)サプライチェーンを共有するＡＳＥＡＮへのアウトリーチの強化

(４)サプライチェーンサイバーセキュリティに係る研究開発の推進

Society5.0/Connected Industriesの進展に対応した『サイバー・フィジカル・セキュリティ対策フレームワーク』の策定

- Society5.0、Connected Industriesの進展によって**複雑化していくサプライチェーンのサイバーリスクに対応する新たな対策フレームワーク**の原案を作成。
- IoTやビッグデータの活用などに伴う新たなリスクに対応するため、**産業社会を三層（企業間、フィジカル-サイバー、サイバー空間）に分類した新たなアプローチ**を提示。



グローバルサプライチェーンに対応するため
『サイバー・フィジカル・対策フレームワーク』の国際化を推進

- グローバルサプライチェーンにそのまま適用できるフレームワークとするため、国際標準（ISO27001等）や米国規格（NIST Cybersecurity Framework等）と連動。
- 国外からも積極的に意見を募るため、**英語版パブリックコメントを実施**。
- **国外の会議などでフレームワークを積極的に紹介**。今後、国際標準化についても検討。

パブリックコメント（4/27-5/28）

■ 国内23、海外9の組織・個人より300件強の意見提出あり。肯定的な意見が9割弱。

■ 海外からの主なコメント

- 各産業への「行動の呼びかけ」として有用（米国企業）
- 中小企業でも利用しやすいフレームワークとすると良い（米国産業団体）
- 国際標準や海外規格に留意して進めてほしい（欧州企業 他）

海外における周知活動

- TechGlobal (米国・ワシントンDC）4月
- 日ASEANサイバーセキュリティＷＧ（インドネシア・バリ）5月
- Securing Global Industrial Value Networks（ドイツ・ベルリン）5月
- OECD・SPDE（フランス・パリ）5月

サプライチェーンを共有するASEANへのアウトリーチの強化

- 多くの日本企業がサプライチェーンを共有するASEAN各国のサイバーセキュリティ対応能力の向上のため、米国と連携し、**ASEAN向け日米共同演習を今年から開始。**

ASEAN向け日米共同演習

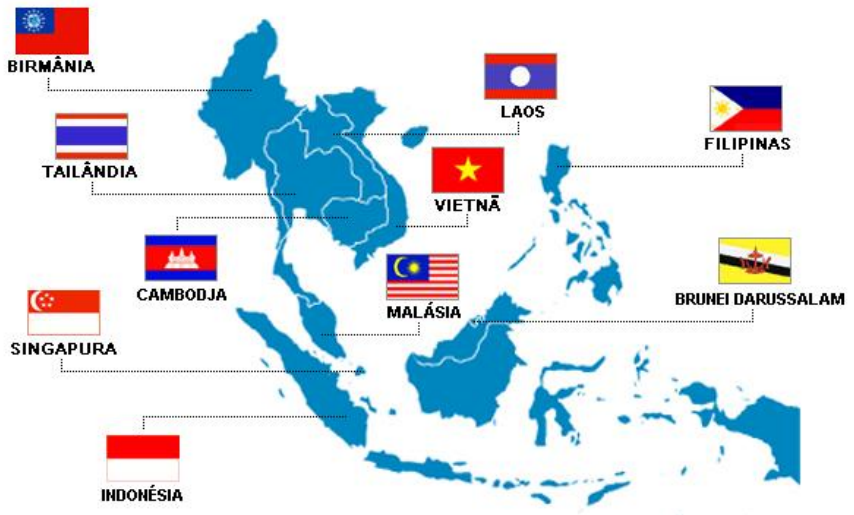
- **開催時期：2018年秋(以降毎年開催)**
- **開催場所：東京**
- **参加国　：ASEAN各国(マレーシア、タイ、ベトナム等)等が参加**

METI Ministry of Economy, Trade and Industry

Homeland Security

asean

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM



サプライチェーンサイバーセキュリティに係る研究開発の推進

- 総合科学技術・イノベーション会議の**研究開発プログラム（SIP）に「IoT社会に対応したサイバー・フィジカル・セキュリティ」プログラムを設置など**(※) 研究開発事業を拡充。
- 更に、**拠点化による中核的な研究開発体制の整備**や、研究成果の実装のための**認定・認証体制の強化**を推進。

SIP第2期 「IoT社会に対応したサイバー・フィジカル・セキュリティ」

平成30年3月30日：
総合科学技術・イノベーション会議にて**課題決定**

平成30年4月12日：
プログラムディレクター(PD)決定
後藤 厚宏 情報セキュリティ大学院大学 学長

平成30年度下半期：
研究開発開始を予定

研究開発の内容

■サプライチェーンのセキュリティ確保

（例）
- IoT等の**エッジデバイスのセキュリティ確保**技術
- **取引先のセキュリティの確保状況を確認**するための基盤技術
- **AIを活用したサイバー攻撃の検知・解析**技術

※ AIチップ・次世代コンピューティングの技術開発においてもセキュリティ技術の研究開発を推進

２．経営・現場双方の課題に応える
サイバーセキュリティ経営強化パッケージ

(１) サイバーセキュリティ経営実現に向けた体系的政策アプローチ

①経営層向け：サイバーセキュリティ経営を促す仕組みの構築

②現場の実務者向け：具体的な対策の導入を促す事例集と可視化ツールの整備

③中小企業向け：サイバー保険等と連携した『サイバーセキュリティお助け隊』の創設

(２)情報共有の仕組みの強化

①経営層向け：
経営者にサイバーセキュリティ経営を促す仕組み『３STEPアプローチ』

1st Step

サイバーセキュリティ経営の在り方の明確化

- **サイバーセキュリティ経営ガイドラインの普及・定着**

2nd Step

サイバーセキュリティ経営を求める仕組みの構築

- **コーポレート・ガバナンス・システム（CGS)に関するガイドライン**のとりまとめに向け、**サイバーセキュリティを位置付け**
- **『取締役会実効性評価』の項目**にサイバーリスクを組み込むことを促進
- サイバーセキュリティが経営リスクであることの投資家に対する啓発

3rd Step

市場（投資家）に対するサイバーセキュリティ経営の可視化

- セキュリティの高い企業であることを投資家が評価できるようにするための、**サイバーセキュリティ経営に関する情報の開示の在り方**の検討

サイバーセキュリティ経営を求める仕組みの構築

1．CGSに関するガイドラインのとりまとめに向け、サイバーセキュリティを位置付け

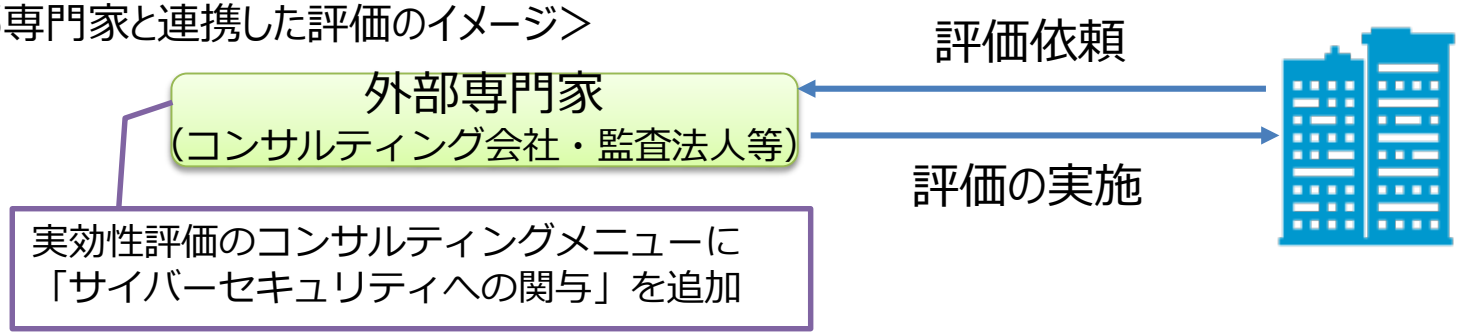
・**コーポレート・ガバナンス・システムに関する議論**の中で、「守り」のリスク管理の一環として、**サイバーセキュリティ対策を位置付け**、**コーポレート・ガバナンス・システム（CGS）に関するガイドライン**のとりまとめに向け、**サイバーセキュリティを位置付け**ることを検討。

2．サイバーセキュリティを考慮した取締役会の実効性評価の促進

・**サイバーセキュリティへの経営層の関与を、上場企業で行われている『取締役会の実効性評価』の評価項目へ組み込むことを促進**。

・**投資家に対するサイバーセキュリティの啓発を実施**。

<外部専門家と連携した評価のイメージ>



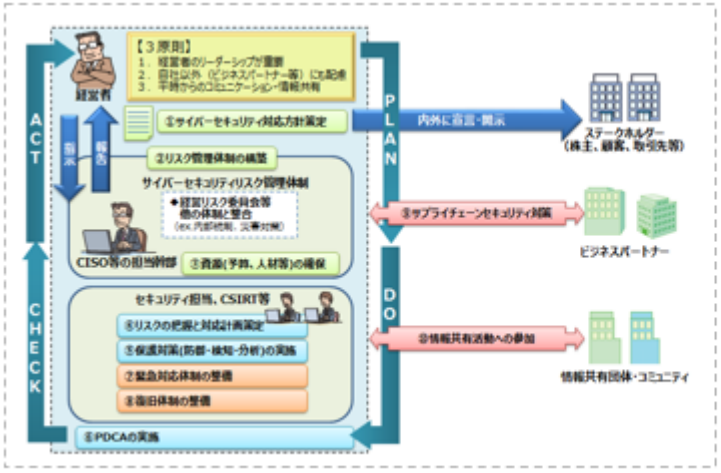
②現場の実務者向け：
サイバーセキュリティ対策の導入を促す対策事例集と可視化ツールの作成

- 企業現場での対策導入を促すべく、**具体的な対策の参考となる『対策事例集』と自社の状況（成熟度）を把握するための『可視化ツール』**の整備に着手。
- ツール整備・活用推進のため、**『サイバーセキュリティ経営プラクティス検討会』を発足。**

サイバーセキュリティ経営プラクティス検討会(本年6月設置予定)
(事務局：IPA、経産省)

損保会社 | 産業横断サイバーセキュリティ人材育成検討会 | JUAS | 日本商工会議所

「対策事例集」の作成



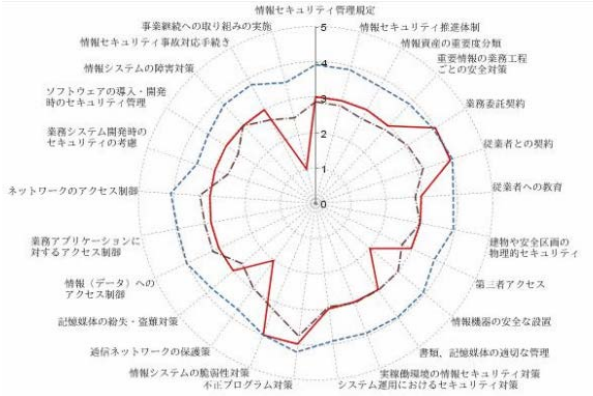
サイバーセキュリティ経営ガイドライン

連携 業界団体（ユーザ企業）

作成


重要１０項目ごとのプラクティス

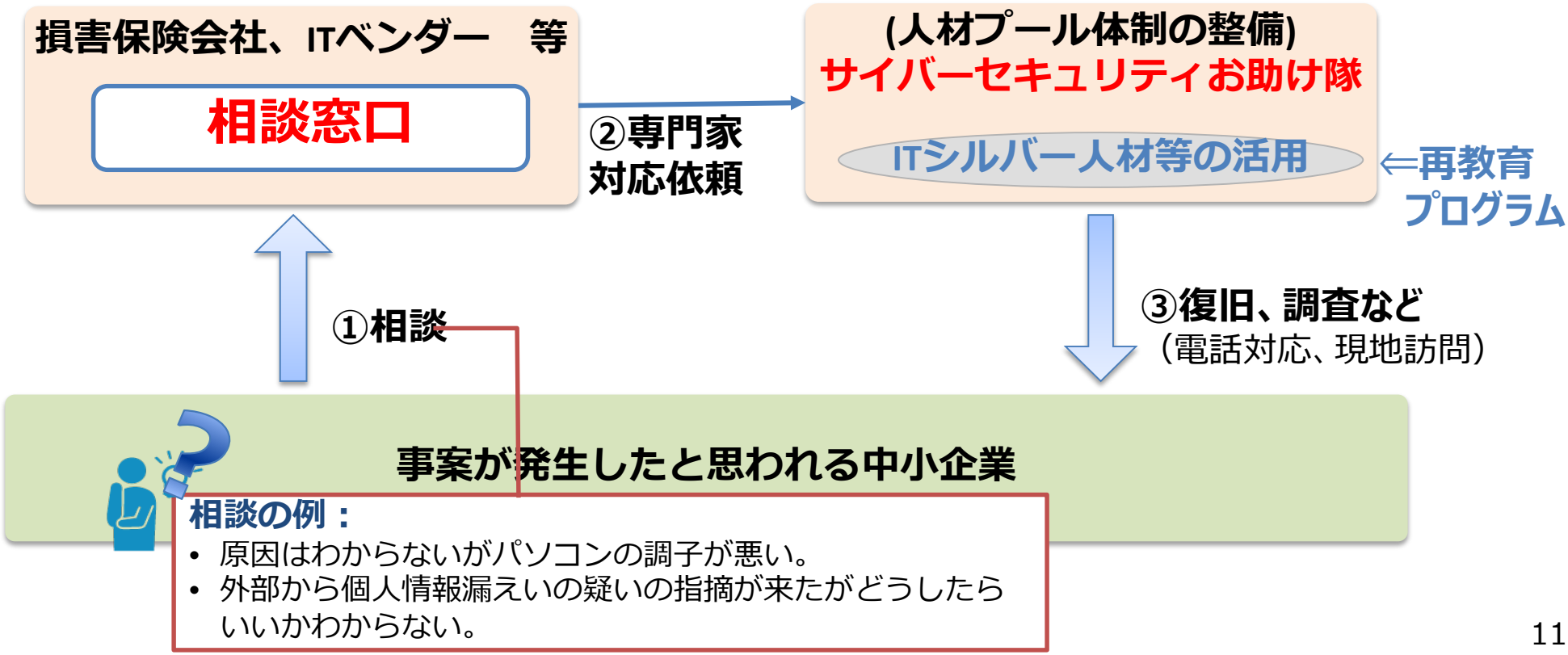
『可視化ツール』のイメージ
(米国NPOとも協力)



②中小企業向け：
サイバー保険等と連携して中小企業を支援する『サイバーセキュリティお助け隊』の創設

- 24時間相談窓口などの体制を持つ損保会社等と連携して、中小企業のサイバーセキュリティに関するトラブル対応を支援する『**サイバーセキュリティお助け隊』を創設。**
- ITに従事してきたシルバー人材の再教育などを通じて人的リソースを確保。

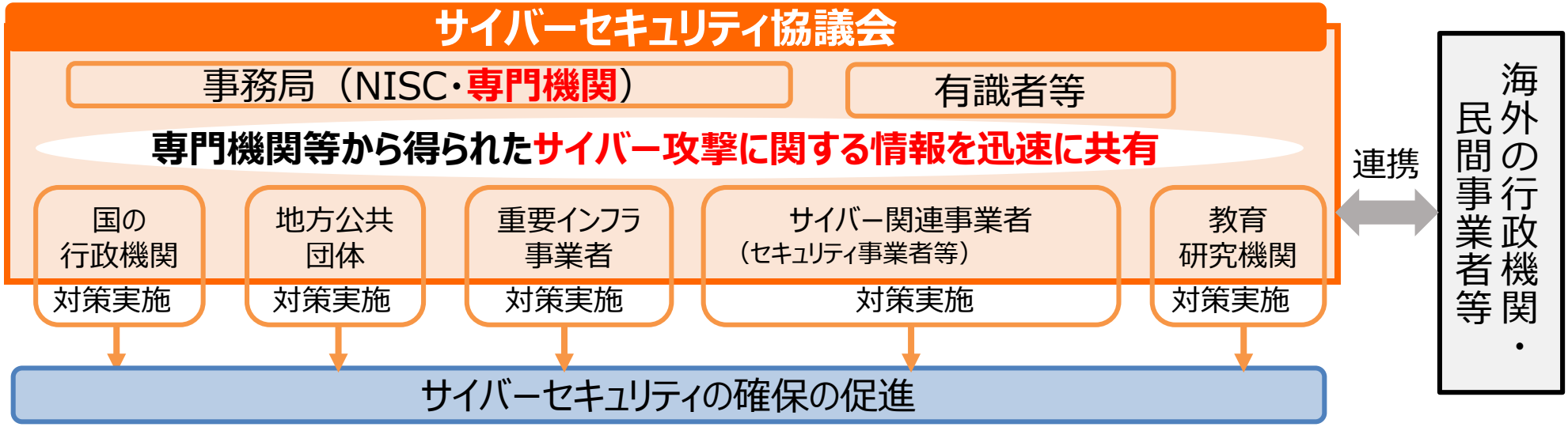
サイバーセキュリティ保険等と連携した『サイバーセキュリティお助け隊』のイメージ



(２)サイバーセキュリティに関する情報共有の強化

- 事業者が、**分野を超えて横連携で情報共有を図り、必要な対策等について協議を行うための協議会を創設**するためのサイバーセキュリティ基本法の改正案を閣議決定。
- WGの活動なども通じ、分野の中で**縦連携で情報共有を深める枠組み作り**を促進。

①分野を超えた横連携の強化：サイバーセキュリティ基本法の改正



②産業分野ごとの縦連携の強化

- **民間事業者によるISAC**や、**J-CSIP**の取組が進められている。
- **本研究会の下に設置したSWGにおいて、具体的な対策レベルでの情報共有を促進。**
- **電力分野**については、**次期エネルギー基本計画の中で情報共有の強化を位置付ける方向で検討。**

３．サイバーセキュリティ対策を支える基盤となる **サイバーセキュリティ人材育成・活躍促進パッケージ**

(１)『セキュリティ人材活用モデル』の作成

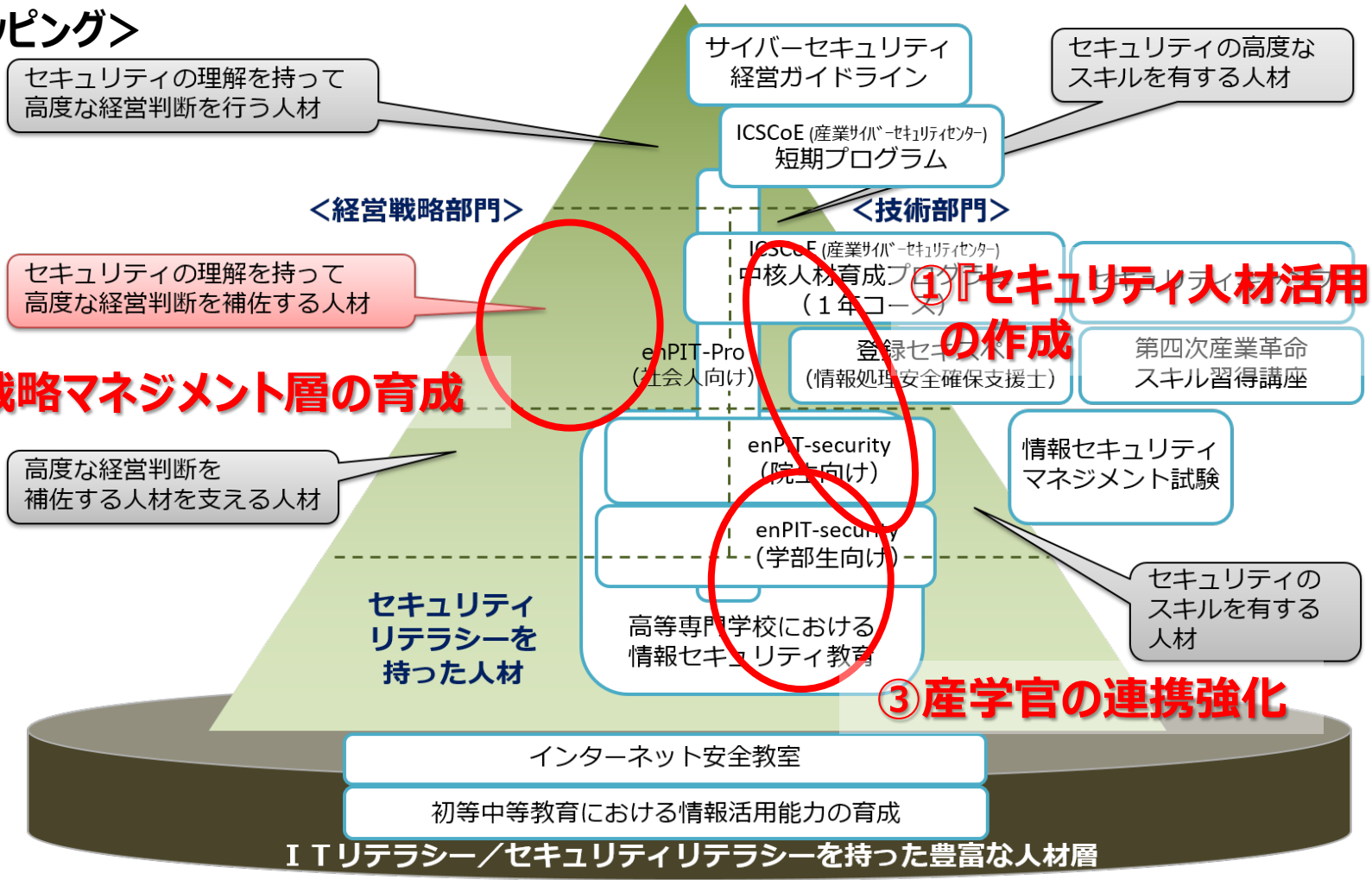
(２)サイバーセキュリティ経営を進める『戦略マネジメント層』の育成

(３)産学官連携の促進

サイバーセキュリティ人材育成・活躍促進パッケージの全体像

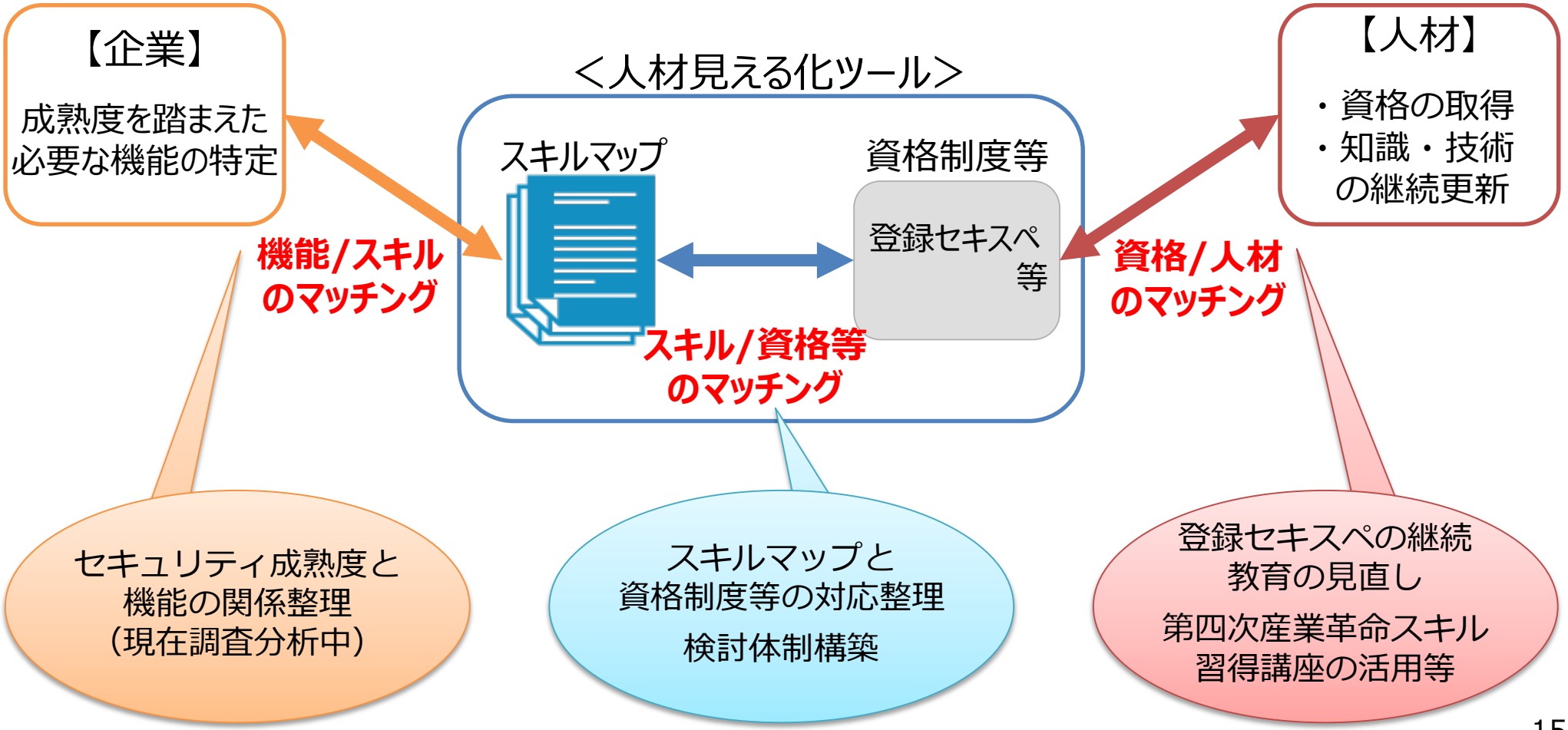
- ユーザー企業において必要となる**セキュリティ人材の定義、評価指標が不明確。**
- **「セキュリティの理解を持って高度な経営判断を補佐する人材」の育成が不十分。**
- 教育プログラム策定への貢献など、**産業界の教育への取組の強化が期待される。**

＜政策マッピング＞



セキュリティ人材の流動化に対応できる『セキュリティ人材活用モデル』の構築

- サイバーセキュリティ経営の実現を目指す**企業と求められるスキルを持つセキュリティ人材をマッチングするモデルの構築**を目指す。
- セキュリティ人材の最適活用、処遇改善につなげ、流動化に対応した人材市場を実現。



サイバーセキュリティ経営を進める戦略マネジメント層の育成

- セキュリティの理解を持って高度な経営判断を補佐する人材『**戦略マネジメント層**』を育成するために、**産学官連携やICSCoEを拠点としたプログラムを開始。**

サイバーセキュリティ経営を含む『次世代経営人材の育成プログラム』の開始 ＜産学官連携＞

- 次世代の経営人材を集中的に育成するプログラム**(2018年秋開講)**の中で、**経営視点で見たサイバーセキュリティ課題の講義も実施**予定。

CISO人材の育成プログラムの開始 ＜IPA産業サイバーセキュリティセンター＞

- **CISOや戦略マネジメント機能を担う人材に必要なセキュリティ対策に関するトレーニング**を行うプログラムを**2018年秋から開始。**

対象人材像

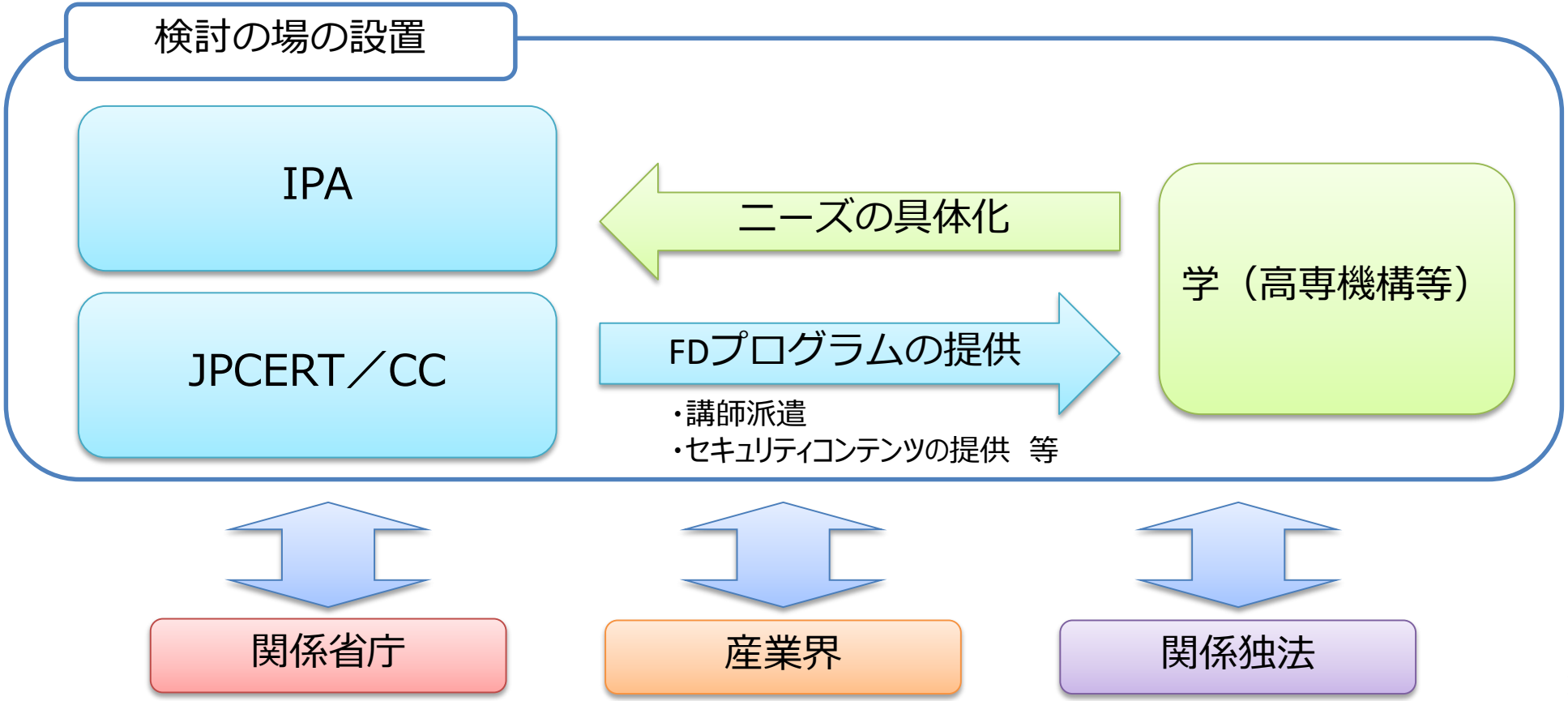
- **次世代の経営を担うことを期待**されている**戦略企画層の方**
- **現在CISOやその補佐を務めている方や、戦略企画層の方**

カリキュラム・期間

- **デジタル経営の講義を、4か月程度かけて実施。**
- その中で、**サイバーセキュリティの必要性・位置づけ**についても講義を実施。
- **サイバーセキュリティのリスク管理や、インシデント対応等**のプログラムを、**2~3か月の間集中して実施。**
- 「中核人材育成プログラム」の受講者80名に、**戦略マネジメント層10~20名を加え、合計100名程度を対象として開始予定。**

産学官連携の促進 「学」向けのトレーニングの提供

- セキュリティ教育の機会を提供するため、教える側の質的向上・量的拡充が必要。**「学」の教員向けにIPA、JPCERT/CCにより、FD（Faculty Development）等の研修機会を提供。**
- 当初は、IPA、JPCERT/CC、高専機構等の「学」による検討の場を設置し、今後、産業界、関係省庁、関係独法等の参画を求めながら課題の洗い出し・解決を図る。



４．ニーズとシーズをマッチングしてビジネスにつなげる **セキュリティビジネスエコシステム創造パッケージ**

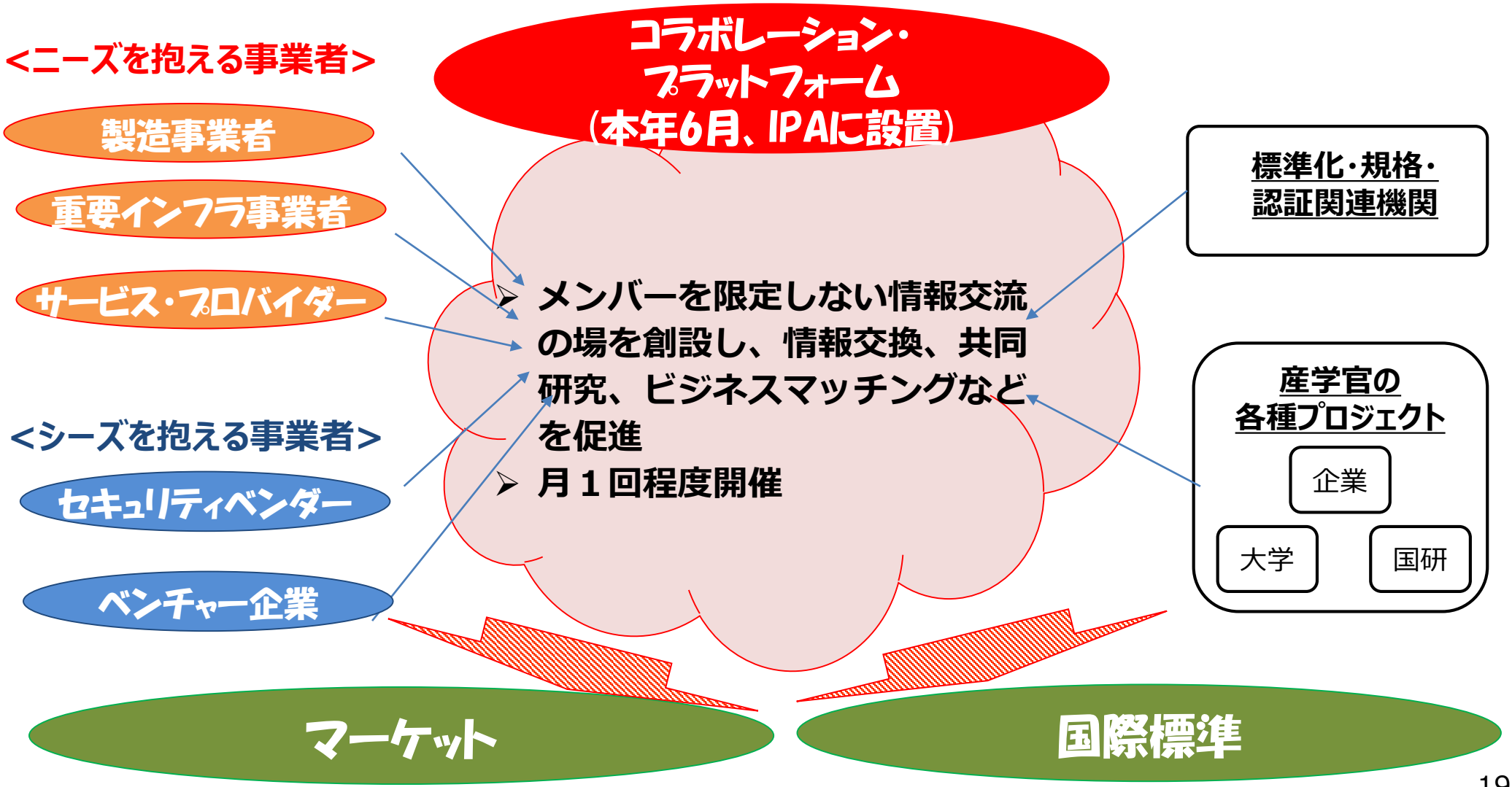
(1)『コラボレーション・プラットフォーム』の設置

(2)『実戦的サイバーセキュリティ検証基盤』の構築

(3)「質の高いインフラ輸出戦略」にサイバーセキュリティの位置付けを明確化

ニーズとシーズをマッチングする『コラボレーション・プラットフォーム』の設置

- 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、6月から活動を開始。**



日本特有のセキュリティ要求に応えた製品・サービスの活用を進める『実戦的サイバーセキュリティ検証基盤』の構築

- 日本のセキュリティニーズに応じた日本発の**サイバーセキュリティ製品の有効性等を実機を通じて検証するための『実戦的サイバーセキュリティ検証基盤』**を構築。

実戦的サイバーセキュリティ検証基盤の全体像

1．セキュリティ製品の有効性検証 ＜性能評価＞

＜イメージ＞

・検証機関が、**セキュリティ製品の有効性を検証し、お墨付きを与えることで、マーケットインを促進。**

2．実環境における試行検証 ＜信頼性評価＞

＜イメージ＞

・ベンチャー等が、**製品の信頼性等を検証するために、製品を民間事業者等へ提供し、実績を作る。**

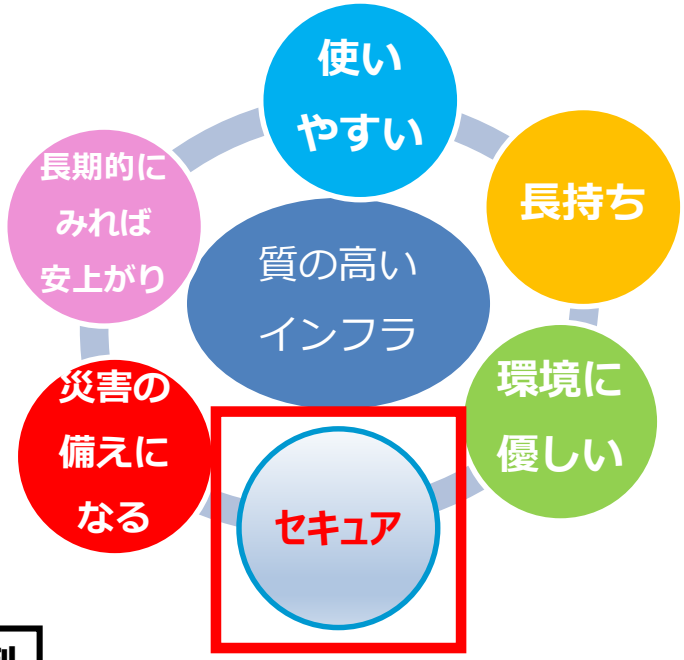
3．ホワイトハッカーの実攻撃検証 ＜ハイレベルなリスク評価＞

＜イメージ＞

・**ホワイトハッカーによる自由な攻撃**を通じて、**実際の制御系システムのセキュリティを検証。**

「質の高いインフラ輸出戦略」に基づき
サイバーセキュリティ品質が高いインフラ輸出を進める

- APECの「**質の高い電力インフラのガイドライン**」に**セキュリティ要求を反映済。**
- 今後、ガイドライン等を踏まえ、セキュリティ品質が高いインフラ輸出を促進。



Cybersecurity

APEC Guideline for Quality Electric Power Infrastructure

1.3.5 安全性
(2) 情報セキュリティ

取組例

- ASEANにおいて**セキュリティ対応した制御系システムのフィージビリティスタディ**を実施。
- インフラシステム輸出へつなげる。

AOTS