経済産業省

資料４

サイバーセキュリティビジネスの現状と今後の取組の方向性

経済産業省　商務情報政策局

サイバーセキュリティ課

１．WG３（サイバーセキュリティビジネス化）の位置づけ
２．これまでの取組(セキュリティ産業のビジネス化研究会)
３．サイバーセキュリティビジネスの動向（投影のみ）
４．ビジネス化における課題（仮説）と対策案

産業サイバーセキュリティ研究会WG３の位置づけ

- 昨年12月27日、産業サイバーセキュリティ研究会第1回を開催。**我が国の産業界がサイバーセキュリティに関して直面する課題に対応していくためのＷＧの一つとして、サイバーセキュリティビジネス化を検討するWG３を設置**。

産業サイバーセキュリティ研究会

■政策の方向性を提示

ＷＧ１　制度･技術･標準化

■制度・技術・標準化を一体的に政策展開する戦略を議論

ＷＧ２　経営･人材･国際

■サイバーセキュリティ政策全体の共通基盤となる経営・人材・国際戦略を検討

ＷＧ３　サイバーセキュリティビジネス化

■セキュリティサービス品質向上と国際プレーヤー創出に係る政策を検討

連携

中小企業政策審議会基本問題小委員会等

■中小企業の生産性向上に資するIT利活用支援策とともに検討

WG３（サイバーセキュリティビジネス化）の検討事項

- 産業サイバーセキュリティ研究会で整理した政策の方向性のうち、**３．サイバーセキュリティビジネスの創出支援を中心に検討。**

サイバーセキュリティ政策の方向性

1．産業政策と連動した政策展開	**① 重要インフラの対策強化** －情報共有体制強化　等 **② IoTの進展を踏まえたサプライチェーン毎の対策強化 (Industry by industry)** －防衛関係、自動車、電力、スマートホーム等の分野別検討と技術開発・実証の推進 **③ 中小企業のサイバーセキュリティ対策強化**
2．国際ハーモナイゼーション	**① 日米欧間での相互承認の仕組みの構築** **② 民間主体の産業活動をゆがめる独自ルールの広がり阻止**
3．サイバーセキュリティビジネスの創出支援	**① 産業サイバーセキュリティシステムを海外に展開** **② サービス認定創設、政府調達などの活用**
4．基盤の整備	**① 経営者の意識喚起** **② 多様なサイバーセキュリティ人材の育成（ICSCoE等）** **③ サイバーセキュリティへの過少投資解決策の検討**

１．ＷＧ３（サイバーセキュリティビジネス化）の位置づけ

２．これまでの取組
(セキュリティ産業のビジネス化研究会)

３．サイバーセキュリティビジネスの動向（投影のみ）

４．ビジネス化における課題（仮説）と対策案

セキュリティ産業のビジネス化研究会の取りまとめと進捗

- 平成29年2月～6月にかけて、セキュリティ産業の振興・活性化を行う政策を検討するための研究会を開催。
- 当該研究会では政府調達の拡充、税制の検討など、**需要サイドの政策的出口に関する議論が中心**。
- 今回のWGでは需要サイドもさることながら、**供給サイドにおいて何を強化してビジネス拡大を図るかについても重点的に議論を行うことを期待**。

＜セキュリティ産業のビジネス化研究会の政策的出口＞

政府における需要喚起

民間における需要喚起

①セキュリティに配慮した政府調達の拡大

②投資促進のための税制

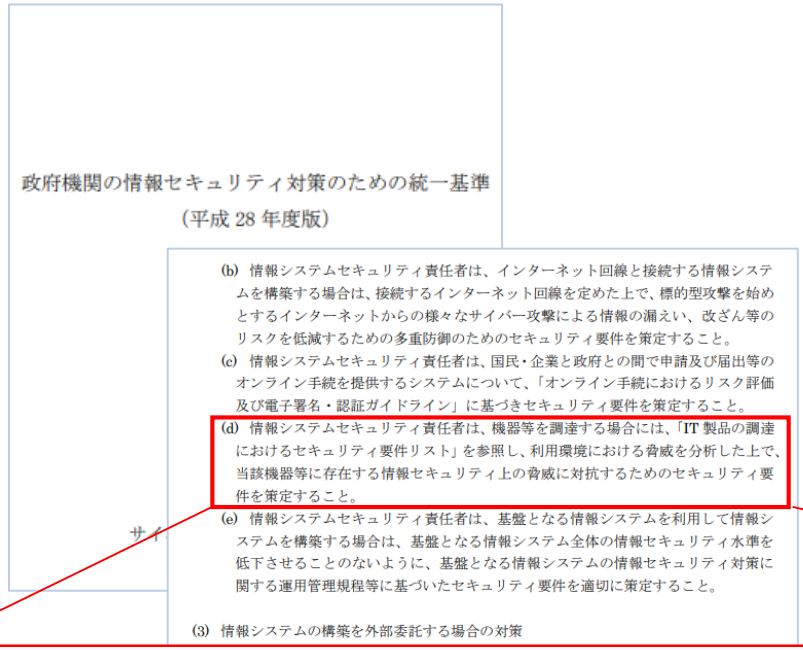
③サイバーセキュリティ経営ガイドラインの改訂

④セキュリティサービス審査登録制度

【セキュリティ産業のビジネス化研究会の政策的出口①】
セキュリティに配慮した政府調達の拡大

- 政府機関等の**情報セキュリティ対策のための統一基準にて参照されている「IT製品の調達におけるセキュリティ要件リスト」を改訂**し、**政府がセキュリティに配慮して調達する製品分野を拡充**（平成30年2月）。

政府機関等の情報セキュリティ対策のための統一基準（NISC）

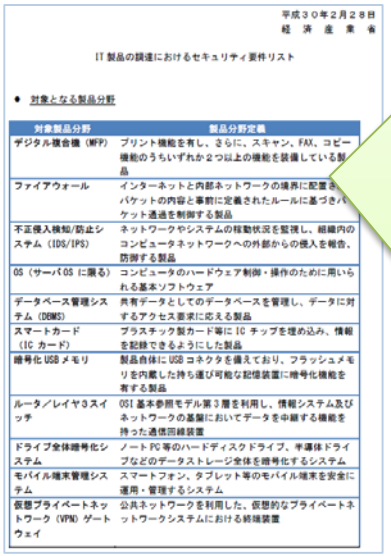

政府機関の情報セキュリティ対策のための統一基準
（平成 28 年度版）

(b) 情報システムセキュリティ責任者は、インターネット回線と接続する情報システムを構築する場合は、接続するインターネット回線を定めた上で、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定すること。
(c) 情報システムセキュリティ責任者は、国民・企業と政府との間で申請及び届出等のオンライン手続を提供するシステムについて、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づきセキュリティ要件を策定すること。
(d) 情報システムセキュリティ責任者は、機器等を調達する場合には、「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。
(e) 情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定すること。

(3) 情報システムの構築を外部委託する場合の対策

参照

IT製品の調達における
セキュリティ要件リスト（経済産業省）


平成３０年２月２８日
経 済 産 業 省

IT 製品の調達におけるセキュリティ要件リスト

● 対象となる製品分野

対象製品分野	製品分野定義
デジタル複合機（MFP）	プリント機能を有し、さらに、スキャン、FAX、コピー機能のうちいずれか２つ以上の機能を装備している製品
ファイアウォール	インターネットと内部ネットワークの境界に配置されパケットの内容と事前に定義されたルールに基づきパケット通過を制御する製品
不正侵入検知/防止システム（IDS/IPS）	ネットワークやシステムの稼動状況を監視し、組織内のコンピュータネットワークへの外部からの侵入を報告、防御する製品
OS（サーバ OS に限る）	コンピュータのハードウェア制御・操作のために用いられる基本ソフトウェア
データベース管理システム（DBMS）	共有データとしてのデータベースを管理し、データに対するアクセス要求に応える製品
スマートカード（IC カード）	プラスチック製カード等に IC チップを埋め込み、情報を記録できるようにした製品
暗号化 USB メモリ	製品自体に USB コネクタを備えており、フラッシュメモリを内蔵した持ち運び可能な記憶装置に暗号化機能を有する製品
ルータ／レイヤ３スイッチ	OSI 基本参照モデル第３層を利用し、情報システム及びネットワークの基盤においてデータを中継する機能を持った通信回線装置
ドライブ全体暗号化システム	ノート PC 等のハードディスクドライブ、半導体ドライブなどのデータストレージ全体を暗号化するシステム
モバイル端末管理システム	スマートフォン、タブレット等のモバイル端末を安全に運用・管理するシステム
仮想プライベートネットワーク（VPN）ゲートウェイ	公共ネットワークを利用した、仮想的なプライベートネットワークシステムにおける終端装置

従来の製品分野(*)に加え、以下の製品分野を追加
- 暗号化USBメモリ
- ルータ/レイヤ3SW
- ドライブ全体暗号化システム
- モバイル端末管理システム
- VPNゲートウェイ

(*)デジタル複合機、ファイアウォール、IDS/IPS、OS、DBMS、ICカード

(d) 情報システムセキュリティ責任者は、機器等を調達する場合には、「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。

【セキュリティ産業のビジネス化研究会の政策的出口②】
コネクテッド・インダストリーズ税制の創設

- **一定のサイバーセキュリティ対策が講じられたデータ連携・利活用**により、**生産性を向上させる取組**について、それに必要となる**システムや、センサー・ロボット等の導入に対して、特別償却30%又は税額控除3%（賃上げを伴う場合は5%）を措置**。
- 事業者は当該取組内容に関する事業計画を作成し、主務大臣が認定。認定計画に含まれる設備に対して、税制措置を適用（適用期限は、平成32年度末まで）。

【計画認定の要件】

①データ連携・利活用の内容

・社外データやこれまで取得したことのないデータを社内データと連携

・企業の競争力における重要データをグループ企業間や事業所間で連携

②セキュリティ面

必要なセキュリティ対策が講じられていることをセキュリティの専門家（登録セキスペ等）が担保

③生産性向上目標

投資年度から一定期間において、以下のいずれも達成見込みがあること

・労働生産性：年平均伸率２%以上

・投資利益率：年平均15%以上

課税の特例の内容

➢ 認定された事業計画に基づいて行う設備投資について、以下の措置を講じる。

対象設備	特別償却	税額控除
ソフトウェア 器具備品 機械装置	30%	3% （法人税額の15%を限度）
		５％ ※ （法人税額の20%を限度）

【対象設備の例】

データ収集機器（センサー等）、データ分析により自動化するロボット・工作機械、データ連携・分析に必要なシステム（サーバ、ＡＩ、ソフトウェア等）、サイバーセキュリティ対策製品　　等

最低投資合計額：5,000万円

※ 計画の認定に加え、平均給与等支給額の対前年度増加率≧３％を満たした場合。

【セキュリティ産業のビジネス化研究会の政策的出口③】
サイバーセキュリティ経営ガイドラインの改訂

- **経営者がリーダーシップを持ってセキュリティ対策を進めるよう普及対策を行うことは、セキュリティ産業の需要喚起につながる。**
- このため、昨今のサイバーセキュリティの状況を踏まえてガイドラインを改訂。

1．経営者が認識すべき３原則

（1）経営者は、**リーダーシップによってセキュリティ対策を進める**ことが必要

（2）ビジネスパートナーや委託先も含めた**サプライチェーンに対するセキュリティ対策が必要**

（3）サイバーセキュリティリスク等について**関係者との適切なコミュニケーションが必要**

2．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築

（指示１）組織全体での対応方針の策定
（指示２）管理体制の構築
（指示３）セキュリティ対策のための資源確保

リスクの特定と対策の実装

（指示４）リスクの把握と対応に関する計画策定
（指示５）**リスクに対応するための仕組みの構築**
（指示６）PDCAサイクルの実施

インシデントに備えた体制構築

（指示７）**緊急対応体制の整備**
（指示８）**被害に備えた復旧体制の整備**

サプライチェーンセキュリティ

（指示９）**サプライチェーン対策及び状況把握**

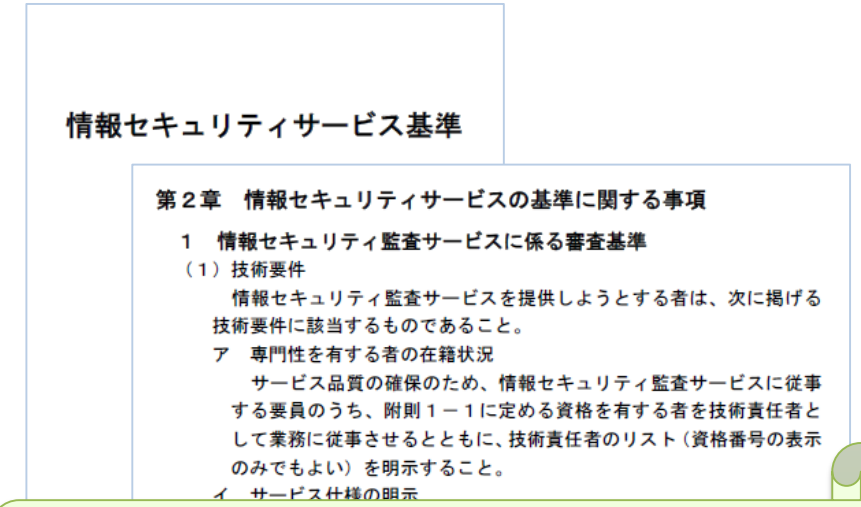
関係者とのコミュニケーション

（指示10）情報共有活動への参加

【セキュリティ産業のビジネス化研究会の政策的出口④】
情報セキュリティサービス審査登録制度

- 情報セキュリティサービスに対する一定の品質を示した基準（情報セキュリティサービス基準）を策定し、当該**基準に適合するサービスが市場にどの程度存在しているかを公表する仕組みを創設。**（調査をIPAに依頼（平成30年2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基準

第２章　情報セキュリティサービスの基準に関する事項

１　情報セキュリティ監査サービスに係る審査基準

（１）技術要件

情報セキュリティ監査サービスを提供しようとする者は、次に掲げる技術要件に該当するものであること。

ア　専門性を有する者の在籍状況

サービス品質の確保のため、情報セキュリティ監査サービスに従事する要員のうち、附則１－１に定める資格を有する者を技術責任者として業務に従事させるとともに、技術責任者のリスト（資格番号の表示のみでもよい）を明示すること。

イ　サービス仕様の明示

調査

News Release　経済産業省

平成30年2月28日

情報セキュリティサービス基準及び

情報セキュリティサービスに関する審査登録機関基準を公表しました

経済産業省は、情報セキュリティサービスを安心して活用することができる環境を醸成するべく、情報セキュリティサービス基準及び情報セキュリティサービスに関する審査登録機関基準を公表しました。また、独立行政法人情報処理推進機構（IPA）に対して、情報セキュリティサービス基準に適合する情報セキュリティサービスの流通状況の調査及びその結果の公表を依頼しました。

1. 背景

昨今、サイバー攻撃は増加傾向にあり、その手口はますます巧妙化してきています。セキュリティ対策は、セキュリティ製品を購入しただけでは十分ではなく、事業者が行う情報セキュリティサービスの利用も含めて検討する必要があります。

【対象となるサービス】
- 情報セキュリティ監査サービス
- 脆弱性診断サービス
- デジタルフォレンジックサービス
- セキュリティ監視・運用サービス

経済産業省はIPAに以下の業務を依頼
- 当該基準に適合するサービスの市場流通状況の調査
- 基準に適合するサービスの台帳作成（6月頃、IPAにて公開予定）

１．ＷＧ３（サイバーセキュリティビジネス化）の位置づけ
２．これまでの取組
(セキュリティ産業のビジネス化研究会)
３．サイバーセキュリティビジネスの動向（投影のみ）
４．ビジネス化における課題（仮説）と対策案

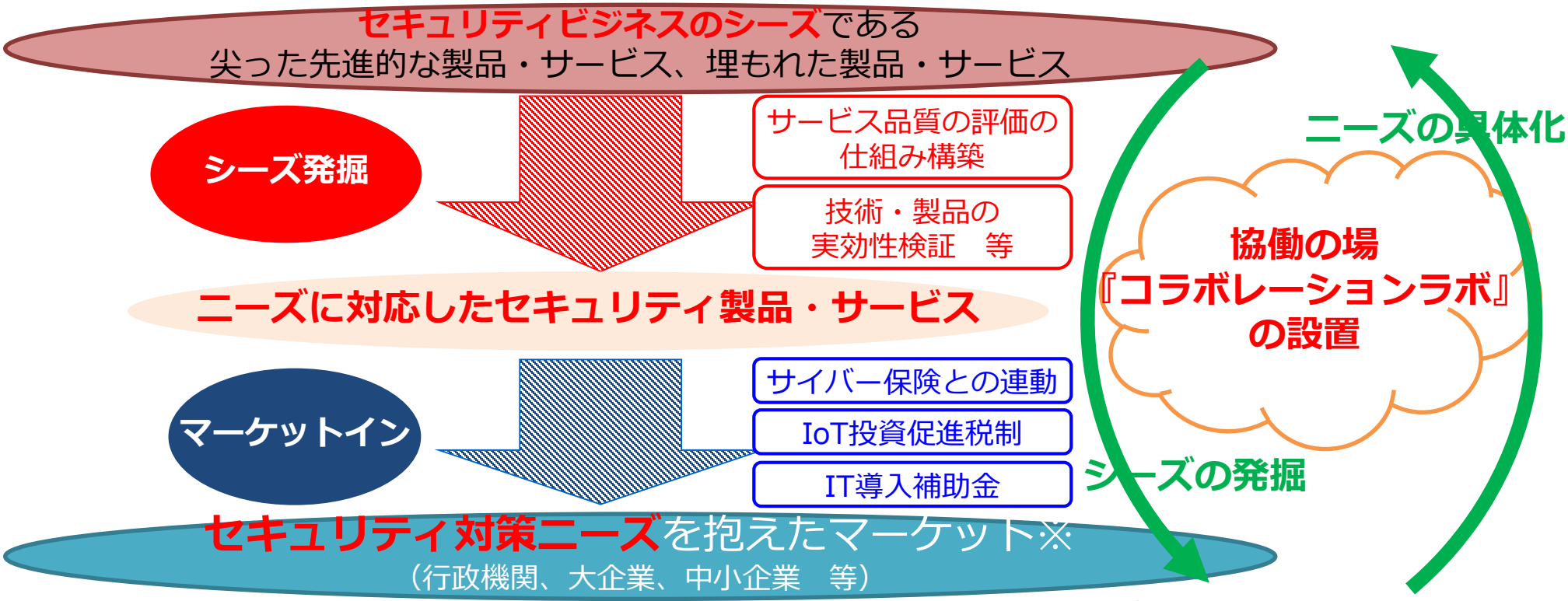
１．ＷＧ３（サイバーセキュリティビジネス化）の位置づけ
２．これまでの取組
(セキュリティ産業のビジネス化研究会)
３．サイバーセキュリティビジネスの動向（投影のみ）
４．ビジネス化における課題（仮説）と対策案

セキュリティ・ビジネス・エコシステムのイメージ

- セキュリティ対策の**ニーズとシーズのマッチング**が、**サイバーセキュリティビジネス化の鍵。**
- **ニーズの明確化・具体化**や、**シーズ発掘の仕組構築**を行うことで、**セキュリティビジネスのエコシステムを構築し、セキュリティビジネスを活性化。**

セキュリティビジネスのエコシステム（イメージ）

※**WG２**において、**セキュリティ人材の育成を検討しセキュリティビジネスのエコシステムを下支え**



※**WG1**において、**各分野に求められる機能を考慮して、必要なセキュリティニーズ等を明確化**
※**政府調達分野も、セキュリティニーズ等を踏まえた活用の検討を継続**

サイバーセキュリティビジネスの2つの観点

- サイバーセキュリティビジネスにおいて、「**for Security**」、及び「**with Security**」の2つの観点で今後の戦略を検討。

for Security（～**で**セキュリティ）

セキュリティ製品・サービスのビジネスの拡大を図る。

＜例＞

- ウイルス対策ソフト
- EDR
- IDS/IPS
- SIEM

with Security（～**の**セキュリティ）

IT/OT製品・システムにセキュリティの価値を加えてビジネスの拡大を図る。

＜例＞

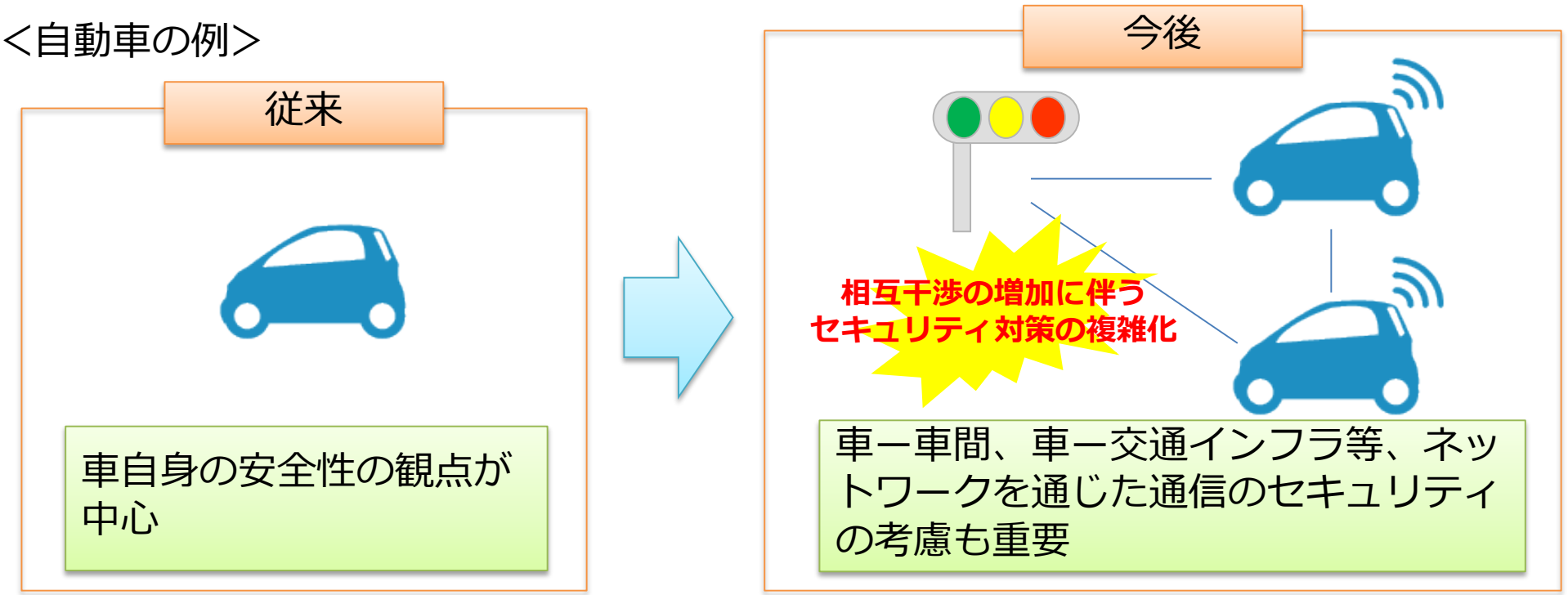
- 自動車
- POS端末
- 家電
- 監視カメラ
- 電力
- 鉄道

それぞれの観点においてビジネス戦略を立てていく必要がある

【セキュリティ産業の将来像（１／３）】
IoT分野における新たなセキュリティ需要の拡大

- Society5.0の実現により、様々なものがつながる時代になる。つながることによりこれまで想定していなかった脅威が出る等、セキュリティ対策がこれまで以上に複雑化することが予想。
- **これまで十分に考えられていなかった脅威への対策をいち早く明確にし、ビジネスとして展開しやすい環境を整えることが重要（IoT分野、エッジコンピュータにおけるセキュリティの需要拡大）。**
- 特に日本の強みである自動車、工作機械等の製造産業においては、セキュリティに十分な配慮ができていないことによって海外での活躍が妨げられ、日本の経済発展にも影響を及ぼす可能性。

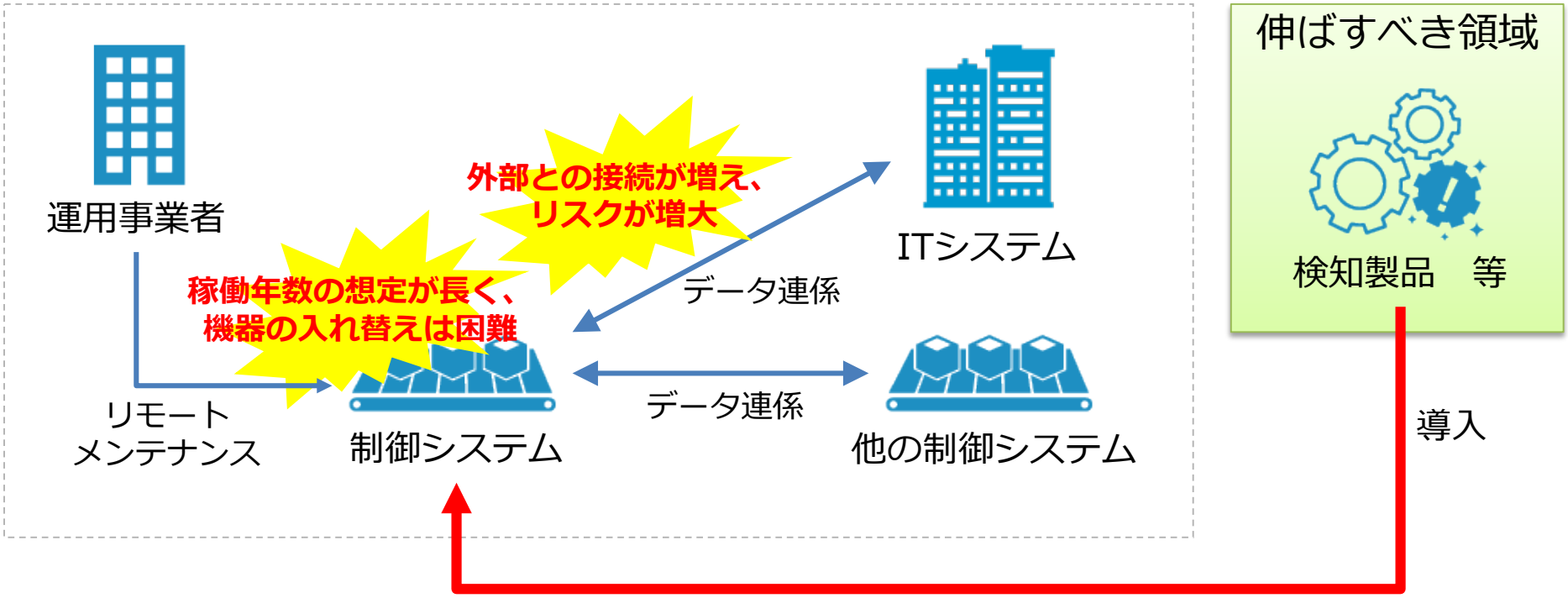
＜自動車の例＞



【セキュリティ産業の将来像（２／３）】

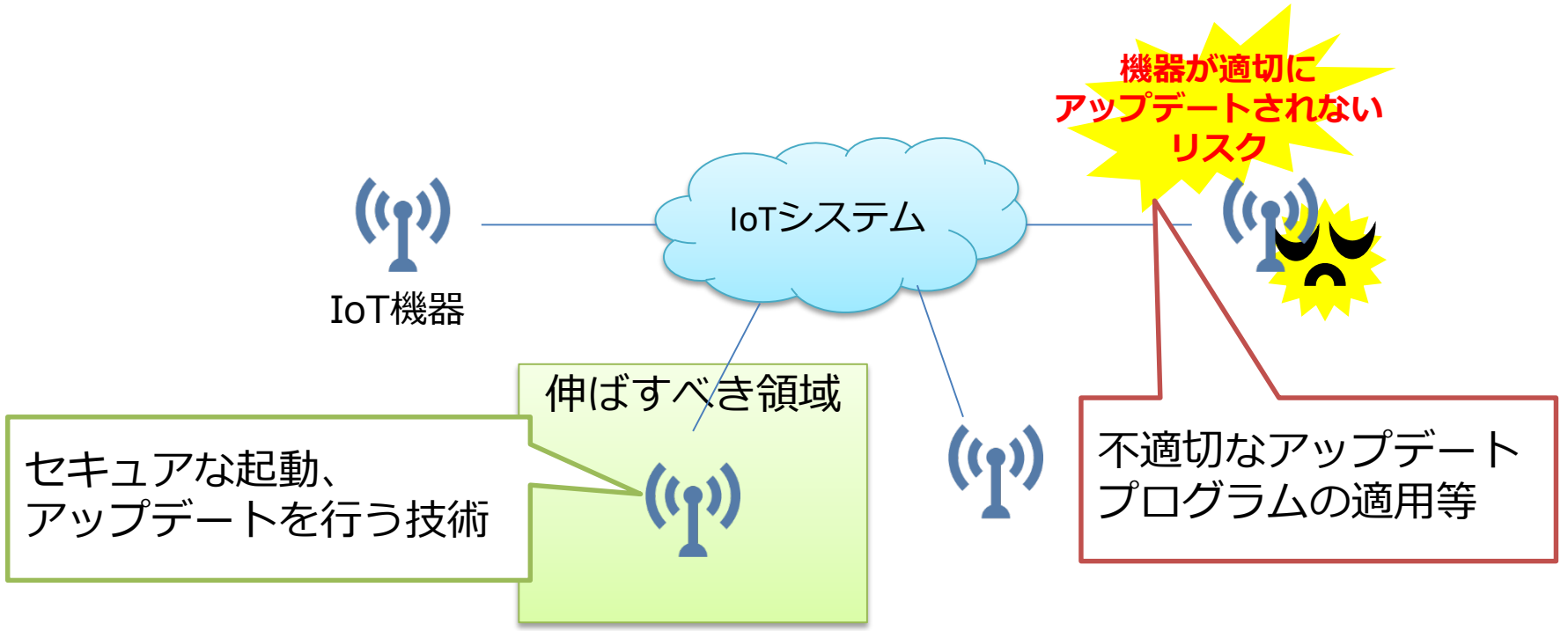
機能保証が求められる制御系システムのセキュリティ対策（特に検知）

- 制御システムはOS・プロトコルの汎用化や他システムとの連携の広がりにより、サイバー攻撃の脅威の増大が予想され、**制御システムにおいても早期に攻撃を検知することが重要。**
- 一般的に制御システムは高い可用性が要求されるため、既存の機器をセキュアな機器に入れ換える等の対応は困難。
- 可用性を損なわずに、**制御システムに後付けで導入できる検知製品等の需要拡大が予想され、この領域にいち早く取り組むことが重要**（**現状、日本にも強みがあると認識**）。



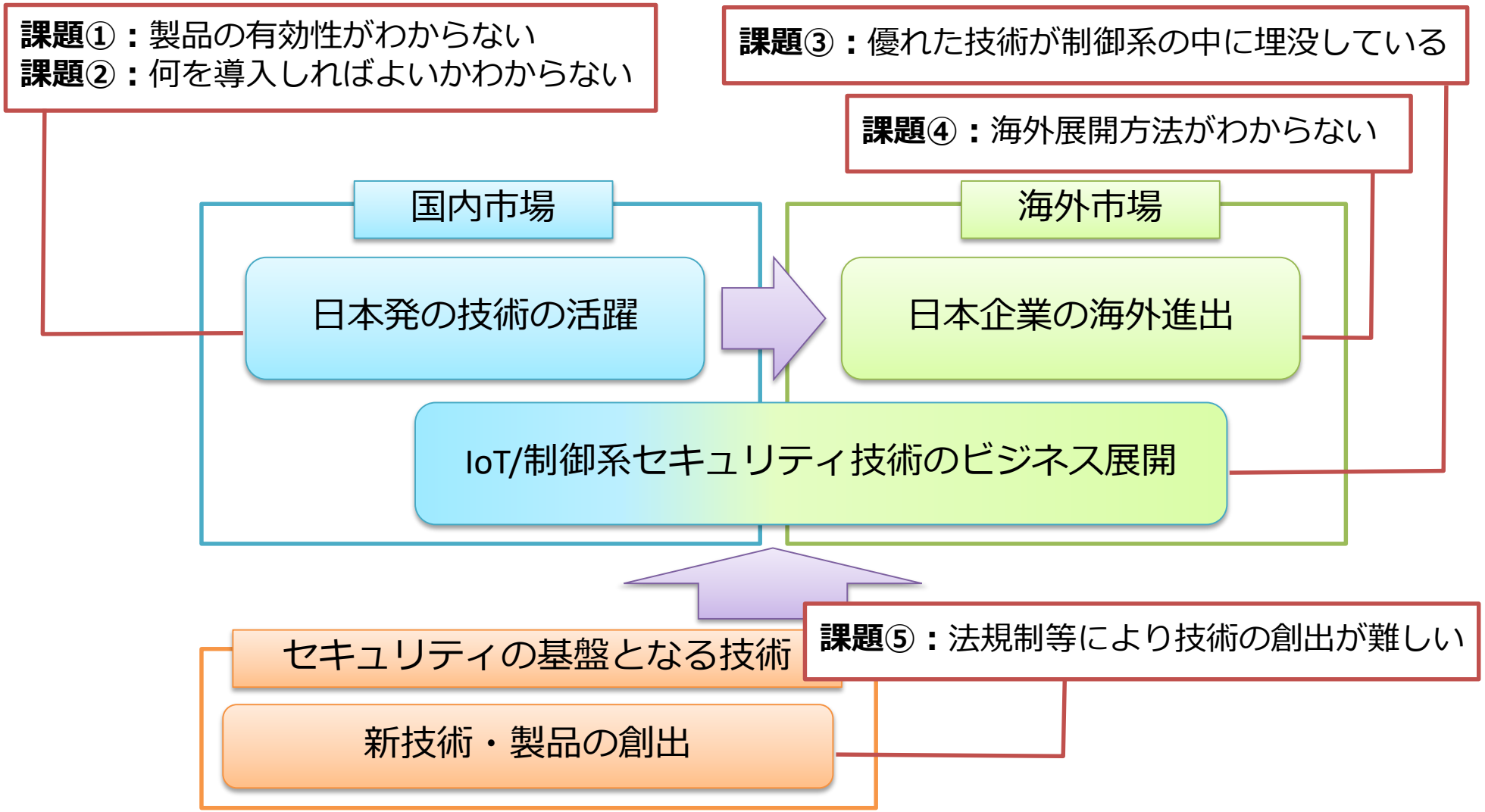
【セキュリティ産業の将来像（３／３）】
つながる機器のセキュリティに対する検証ビジネスの重要性の増加

- IoTの普及により、不特定多数の機器が様々な環境に接続されることが予想。
- 不特定多数の機器が接続できる環境において、悪意のある機器やセキュアでない機器が接続されることにより、当該環境全体が危険にさらされるリスクが増大。
- **接続される機器がセキュアな状態であることを検証する仕組みの重要性が増加（日本としても早期の取り組みが重要）。**



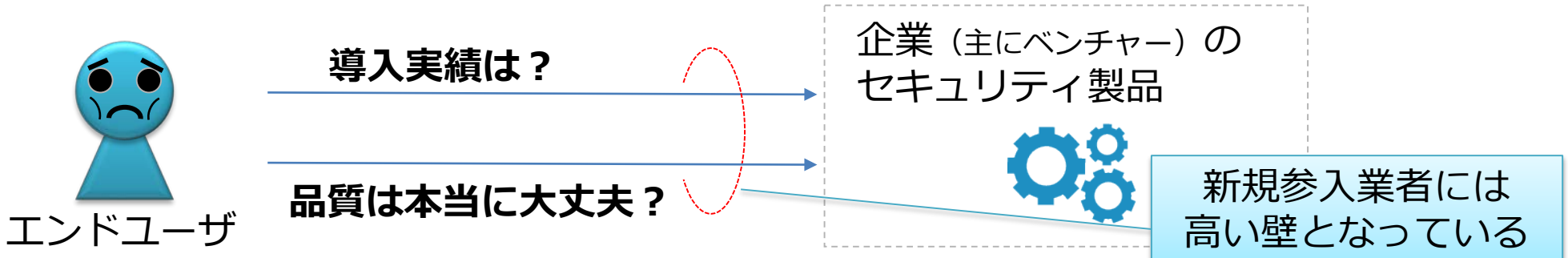
サイバーセキュリティのビジネス化に関する課題（仮説）

- **サイバーセキュリティ産業を取り巻く課題（仮説：下記）を解消する**ことによって、サイバーセキュリティの新技術の創出及びビジネス拡大を期待。



【課題①】製品の有効性が不明確

- **新技術･製品が出てきても、エンドユーザでの導入判断が困難（仮説）。**



＜現場の声＞（経済産業省によるヒアリング）

- 導入実績がないセキュリティ製品を導入するのは不安がある（ユーザ企業）
- 導入実績が豊富な製品は高額であることが多く、導入が難しい（ユーザ企業）
- （特に政府機関から）導入実績として紹介することを禁止されているので、顧客との商談で宣伝できず困ることがある（ベンチャー企業）

解決案

製品の有効性検証制度

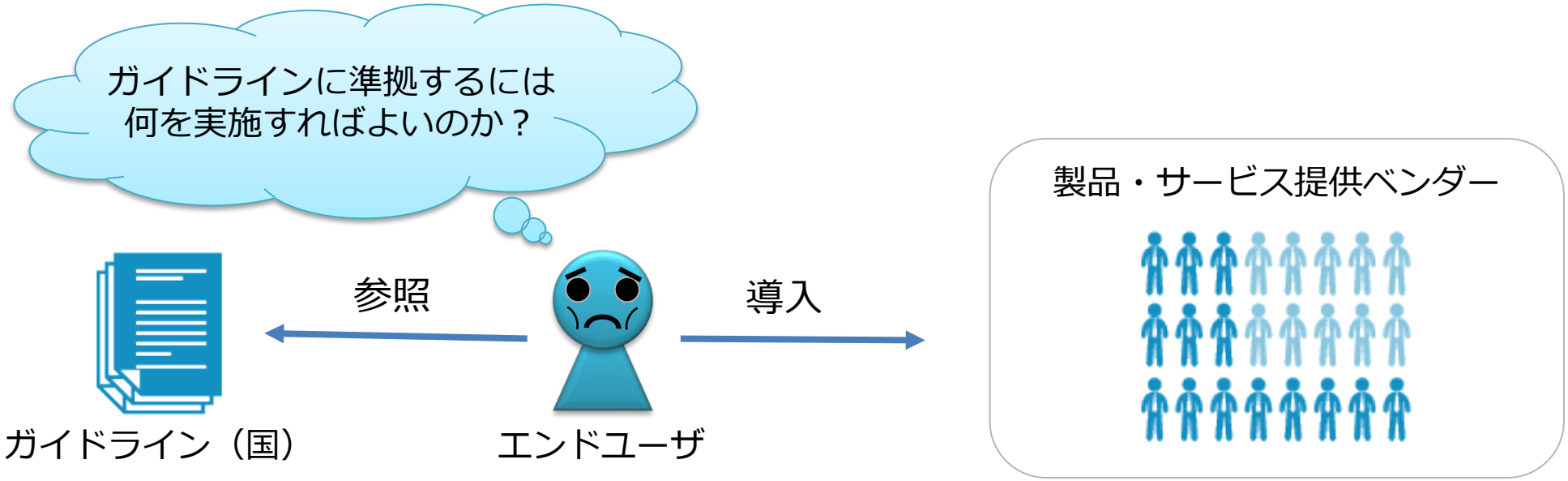
有効性を検証し、ベンチャー等の新技術・製品のマーケットインを促進

製品・サービスのレーティング制度

エンドユーザが利用している製品・サービスの評価（レーティング）を実施し、常に最新の評価を確認できる仕組みを構築

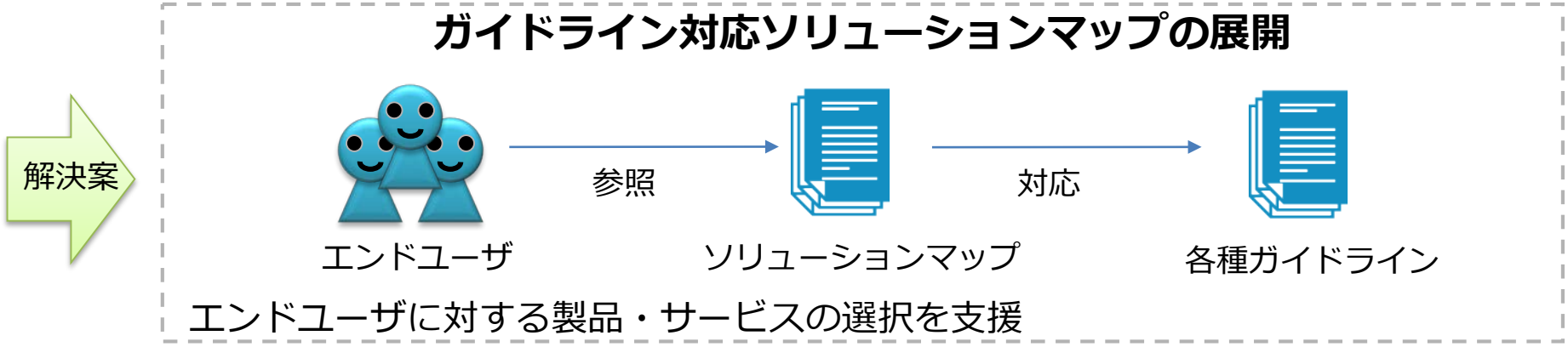
【課題②】何を使えばよいのかの判断が困難

- **セキュリティガイドラインに対応するための具体的な方法が不明**（特に中小）（仮説）。



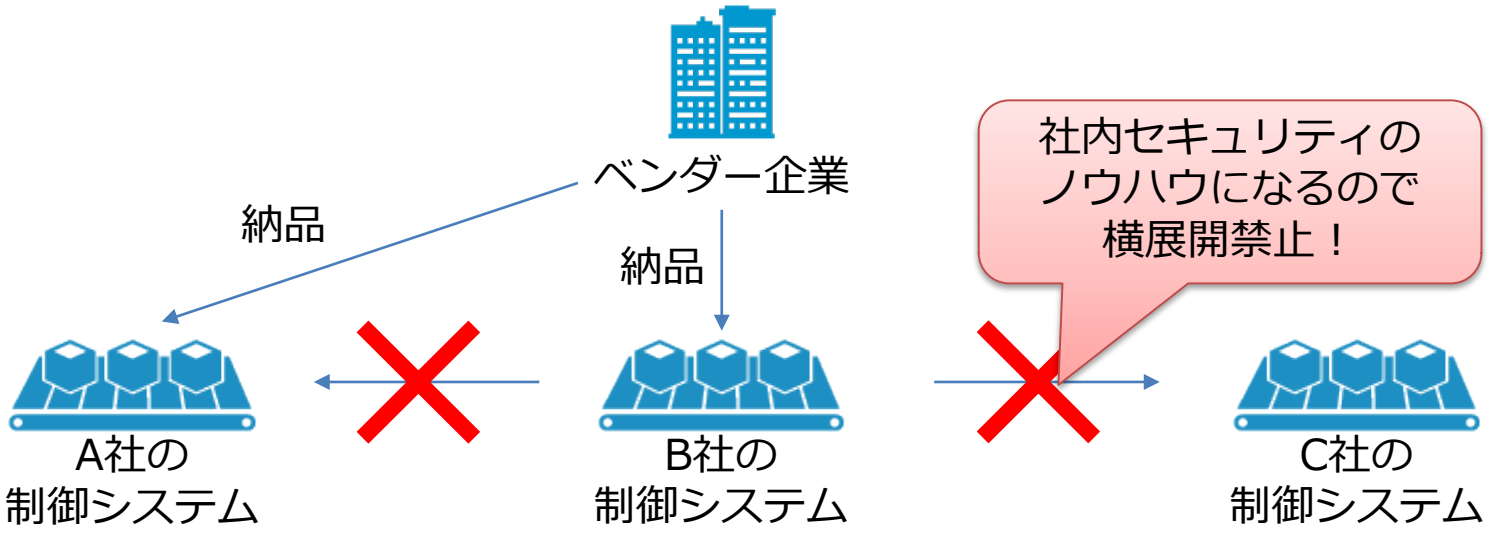
＜現場の声＞（経済産業省によるヒアリング）

- 製品・サービスが多すぎで何を選べばよいかがわからない（ユーザ企業）



【課題③】制御系の中でのセキュリティ技術の埋没

- 制御システムのセキュリティはユーザ企業毎にカスタマイズして設計・実装されており、パッケージ化による販売拡大が困難（仮説）。



＜現場の声＞（経済産業省によるヒアリング）

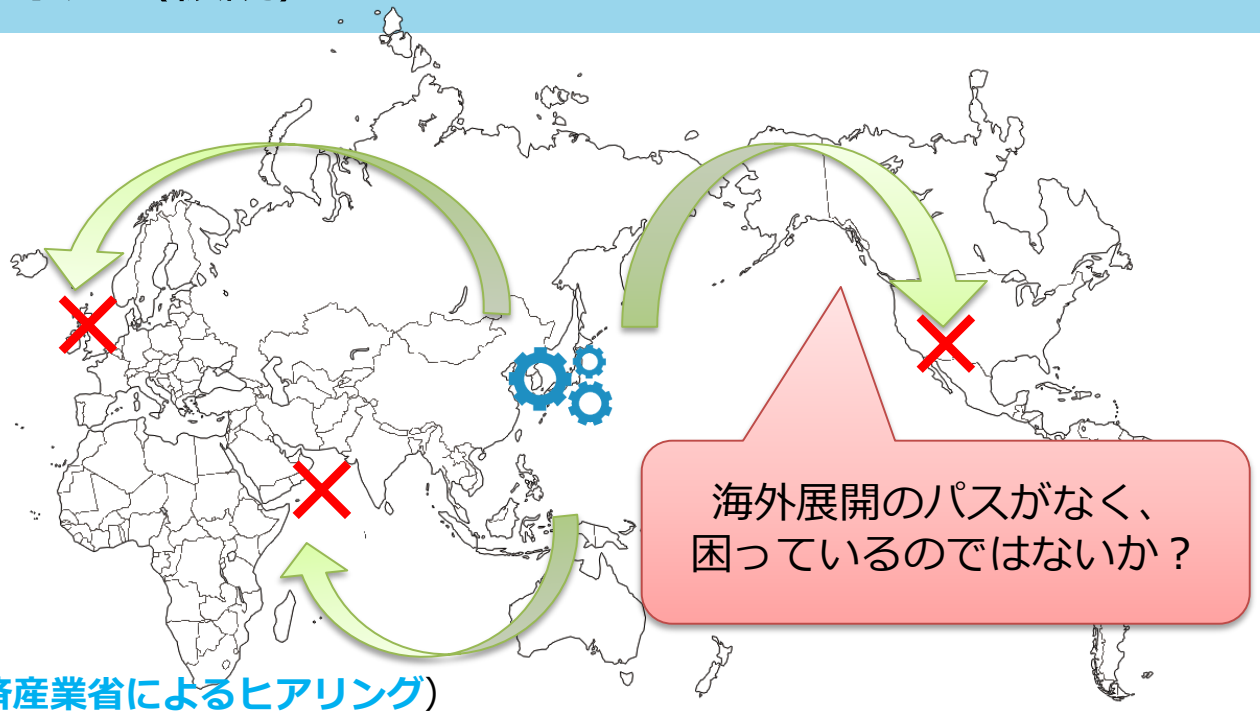
- 特定個社に導入した制御系セキュリティのノウハウをパッケージ化してビジネスを拡大したいが、顧客から禁止されている（ベンダー企業）

解決案

制御系セキュリティのパッケージ化の検討

【課題④】海外展開のパッケージが不足

- 制御系を含めたIoTの個別分野において有益な技術・製品はあるものの、**海外等のビジネス拡大が不十分**（仮説）。



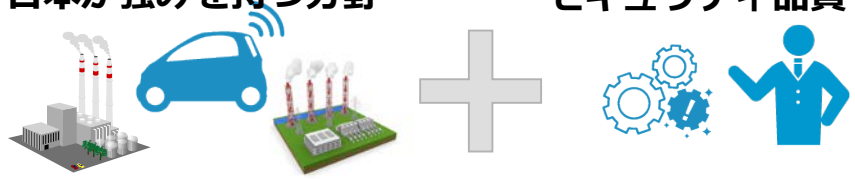
＜現場の声＞（経済産業省によるヒアリング）

- 自社製品の海外展開を図りたいが、どうやって海外展開すればよいかわからない（ベンダー企業）

海外展開支援に向けたパッケージ化の検討

解決案

日本が強みを持つ分野　＋　**セキュリティ品質**



日本が強みをもつ電力等インフラや自動車の分野において、
セキュリティ品質を加えることで競争力を確保

優れたサイバーセキュリティ製品・サービスの展開支援

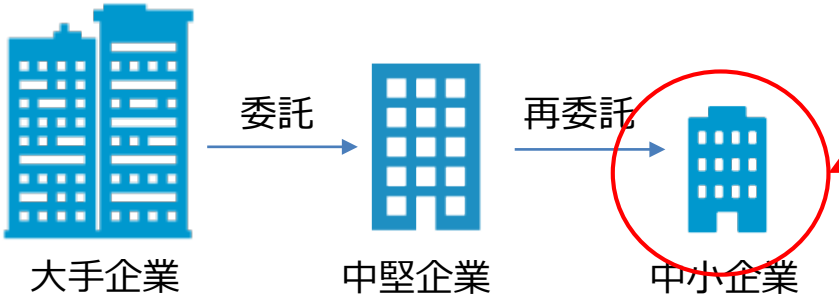
- **優れたサイバーセキュリティ製品・サービスを発掘し、当該技術について海外展開支援等の支援策を検討。**

例：自動車セキュリティの場合

A社
- 機器間のVPN通信により通信経路を保護。
- 「自動車間」や「自動車－交通インフラ間」の通信への活用も期待。

B社
- OSの仮想化を実現。
- 低容量で実現できるため、車載器での活用も期待。

例：サプライチェーンセキュリティの場合



C社
- 端末が保有する情報の秘密分散を図り、情報を保護。
- 安価に導入できるため、中小企業での活用も期待。

【課題⑤】新技術創出に関する法的制約

- 新技術創出やビジネス展開の妨げになるような法規制、法的解釈のグレーゾーンが存在（仮説）。

事例１（ビジネス展開における法的グレーゾーン）：

■セキュリティ監視サービスを提供している某社の社員がウイルス保管容疑により逮捕された。
■本件については、「正当な目的の有無」が論点の一つとなっており、法的な解釈がグレーになっている。

法律：刑法（不正指令電磁的記録に関する罪（ウイルス保管罪））

事例２（尖った技術の創出における課題）：

■CTF（ハッカーコンテスト）の国際大会において、ジャミングを使った問題が問われることがある。日本では法的な制約上、このような技術を習得するのが難しいため、アメリカやイスラエル勢に対して遅れを取ってしまう状況にある。

法律：電波法

事例３（海外ビジネスにおける法律の課題）：

■SOCサービスにおいて、海外の企業のログを日本で解析することがあるが、EUの企業のログを日本で解析した場合、GDPRの影響を受けるのかがよくわからない。

法律：GDPR

解決案

法律の解釈についての整理

専門家/専門機関等と連携し、セキュリティビジネスにおいて影響を受ける可能性がある法律の解釈を整理することを検討。

WG3の今後の進め方(案)

- 新技術の発掘・創出や既存の技術の展開拡充を目的として、**3つのテーマに分け、テーマ毎に本WG委員以外の専門家も招へいして具体的な議論を実施予定。**
- テーマとしては「**IoT（主に自動車）セキュリティ**」、「**制御系セキュリティ**」、「**尖った人材・技術の発掘・創出**」を想定。