経済産業省

資料７

# サイバー・フィジカル・セキュリティの確保に向けた取組

平成31年3月1日

経済産業省　商務情報政策局

サイバーセキュリティ課

# 【経済産業省におけるサイバーセキュリティ政策の方向性】
# 産業サイバーセキュリティ研究会とWGの設置による検討体制

## 産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催

→ 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（４つの柱）**を提示

**構成員**

※第2回開催時点

| | |
|---|---|
| **石原　邦夫** | 日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、東京海上日動火災保険株式会社相談役 |
| **鵜浦　博夫** | 日本電信電話株式会社代表取締役社長 |
| **遠藤　信博** | 日本経済団体連合会情報通信委員長、日本電気株式会社会長、サイバーセキュリティ戦略本部員 |
| **小林　喜光** | 経済同友会代表幹事、株式会社三菱ケミカルホールディングス取締役会長 |
| **中西　宏明** | 株式会社日立製作所会長、(日本経済団体連合会会長) |
| **船橋　洋一** | アジア・パシフィック・イニシアティブ理事長 |
| **宮永　俊一** | 三菱重工業株式会社社長 |
| **村井　純(座長)** | 慶應義塾大学教授、サイバーセキュリティ戦略本部員 |
| **渡辺　佳英** | 日本商工会議所特別顧問、大崎電気工業株式会社取締役会長 |

**オブザーバー**

NISC、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省

---

**サイバーセキュリティ基本法改正（NISC）にて対応**

平成30年3月9日　閣議決定
平成30年12月5日　成立

**WG１（制度･技術･標準化）**

第１回　平成30年2月7日
第２回　平成30年3月29日
第３回　平成30年8月3日
第４回　平成30年12月25日

**１．サプライチェーン強化パッケージ**

**WG２（経営･人材･国際）**

第１回　平成30年3月16日
第２回　平成30年5月22日
第３回　平成30年11月9日

**２．経営強化パッケージ**

**３．人材育成・活躍促進パッケージ**

**WG３（サイバーセキュリティビジネス化）**

第１回　平成30年4月4日
第２回　平成30年8月9日
第３回　平成31年1月28日

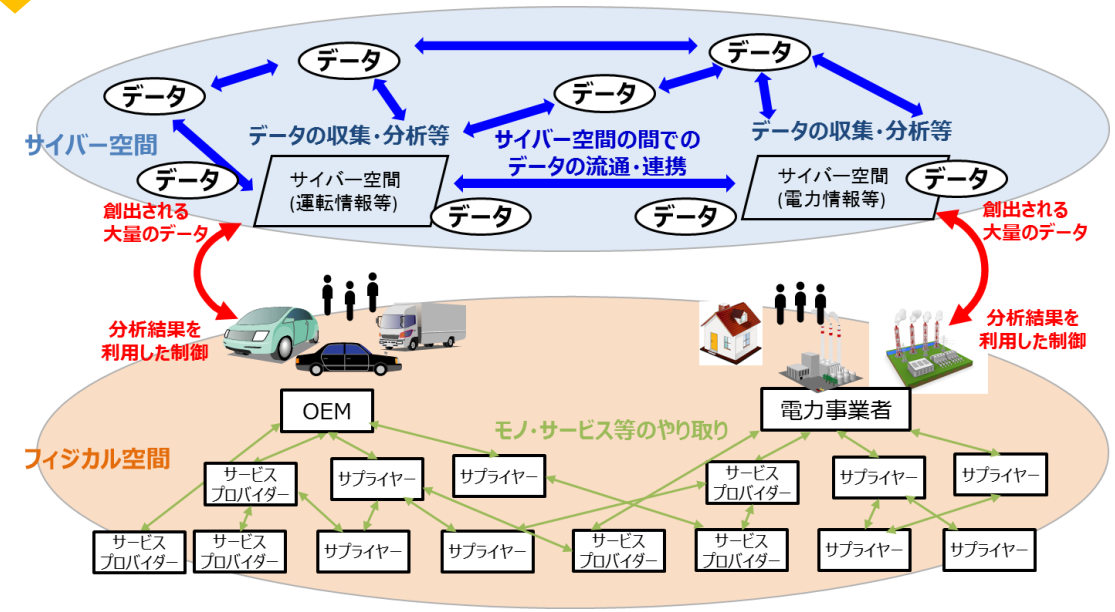
**４．ビジネスエコシステム創造パッケージ**

# 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
## ＜サプライチェーン構造の変化＞

- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能となる。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要**となる。

**「Society5.0」以前**

**個々の企業主体の定型的なつながりで価値を生み出す**




**Society5.0の社会におけるモノ・データ等の繋がりのイメージ**

**サイバー空間で大量のデータの流通・連携**
**⇒データの性質に応じた管理の重要性が増大**

**フィジカル空間とサイバー空間の融合**
**⇒フィジカル空間までサイバー攻撃が到達**

**企業間が複雑につながるサプライチェーン**
**⇒影響範囲が拡大**

# サイバー・フィジカル一体型社会のセキュリティのために フレームワークで提示した新たなモデル：三層構造と６つの構成要素

- フレームワークでは、産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するための新たなモデルを提示。

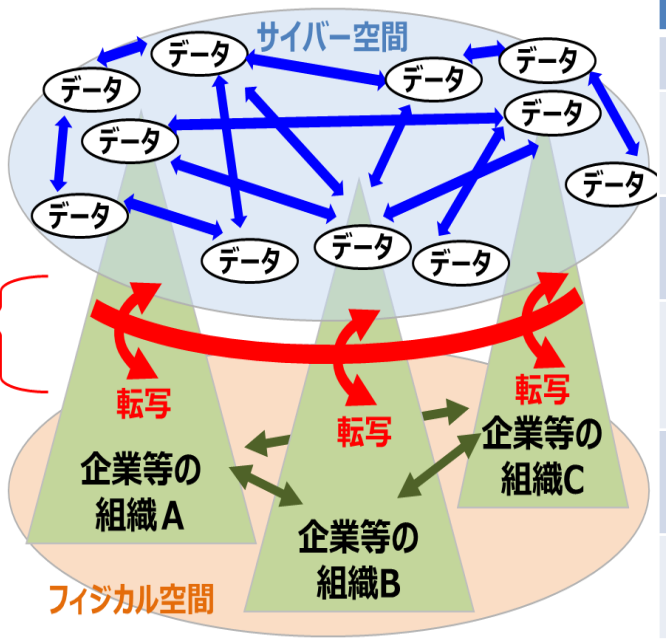
## 三層構造アプローチ

「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

### サイバー空間におけるつながり
**【第３層】**
自由に流通し、加工・創造されるサービスを創造するための**データの信頼性**を確保

### フィジカル空間とサイバー空間のつながり
**【第２層】**
フィジカル・サイバー間を正確に**“転写”する機能の信頼性**を確保（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

### 企業間のつながり
**【第１層】**
適切な**マネジメントを基盤に各主体の信頼性**を確保




## ６つの構成要素

対策を講じるための単位として、**サプライチェーンを構成する要素を６つに整理**

| 構成要素 | 定義 |
|---|---|
| ソシキ | • 価値創造過程に参加する企業・団体 |
| ヒト | • 組織に属する人、及び価値創造過程に直接参加する人 |
| モノ | • ハードウェア、ソフトウェア及びそれらの部品<br>• 操作する機器を含む |
| データ | • フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報 |
| プロシージャ | • 定義された目的を達成するために一連の活動を定めたもの |
| システム | • 目的を実現するためにモノで構成される仕組み・インフラ |

## 1. 研究開発

- 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」
- 中核的な研究開発拠点の設置
  ～ 産総研 サイバーフィジカルセキュリティ研究センター
- 高度なIoT社会の実現に向けた技術開発

## 2. サイバーセキュリティビジネスの強化

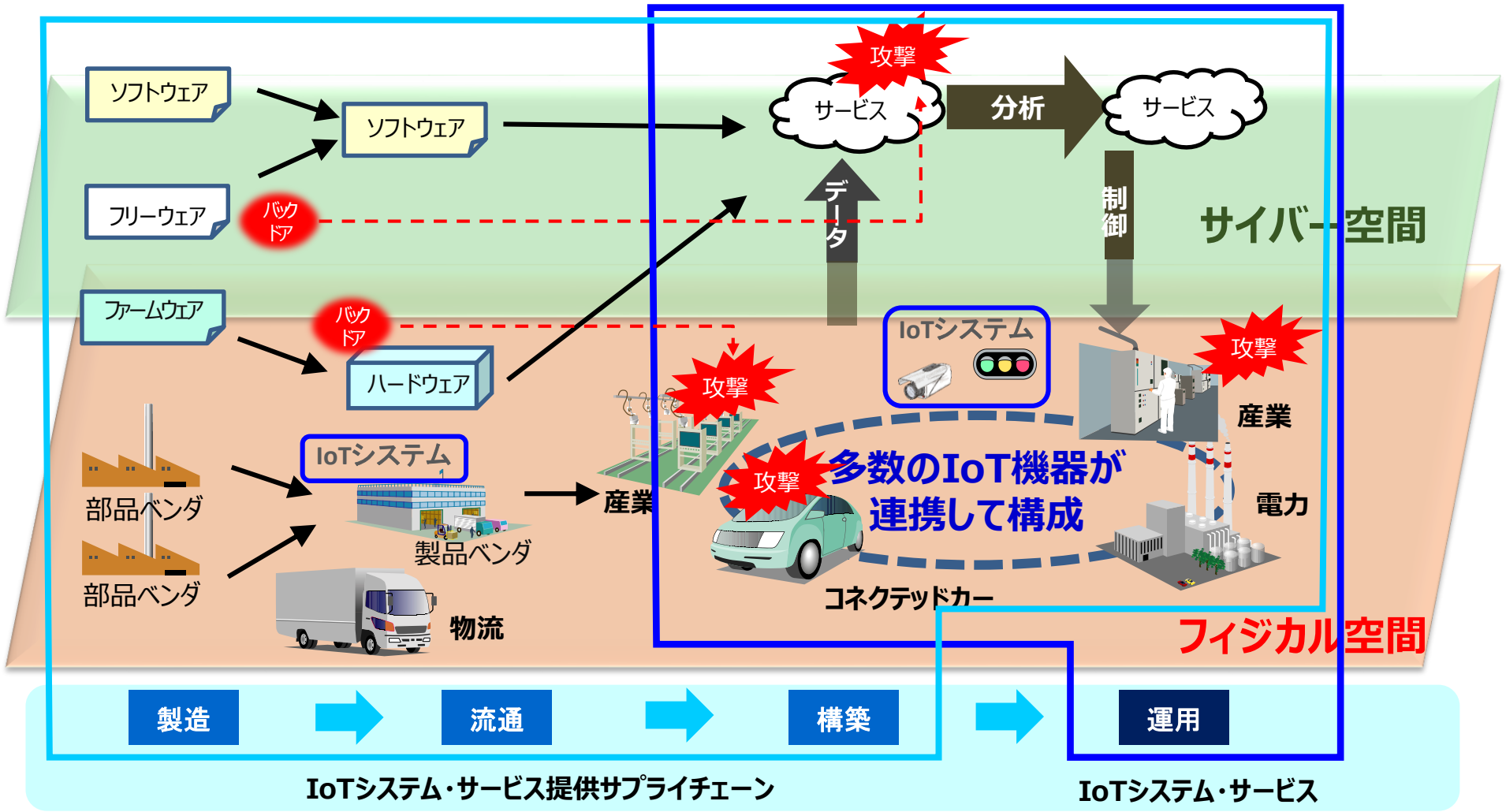
- サイバーセキュリティ検証基盤の構築に向けた検討
- サイバーセキュリティお助け隊
- コラボレーション・プラットフォーム

# 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」

**複雑につながるサプライチェーン**
**⇒ 影響範囲が拡大**

**フィジカルとサイバーの融合 ⇒**
- **サイバー攻撃がフィジカル空間まで到達**
- **フィジカルから侵入しサイバー空間への攻撃も**
- **フィジカルとサイバーの間の情報伝達への攻撃**

**大量のデータの流通・連携**
**⇒ データ管理の重要性が増大**



# SIP第2期 - 研究開発の取組内容・実施体制

## A.信頼の創出・証明

**ECSEC, 産総研, NTT, NEC, 日立製作所, KDDI総研 等**

多様なIoTシステム・サービスやサプライチェーン全体のセキュリティ確保に必要な信頼の創出・証明技術

## B.信頼チェーンの構築・流通

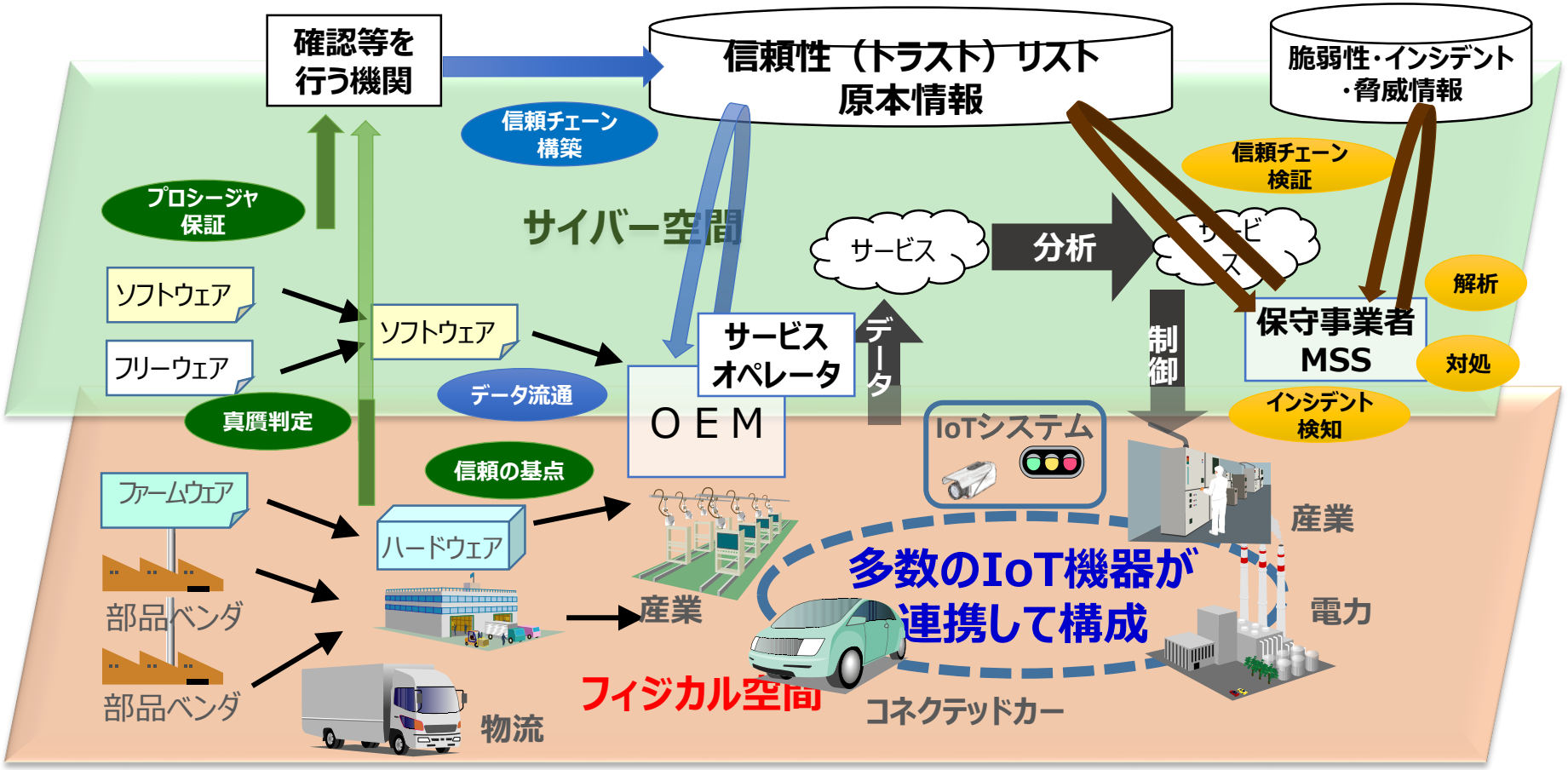
**日立製作所, NEC, KDDI総研, 富士通 等**

信頼チェーンを構築し、必要な情報をセキュアに流通させる技術

## C.信頼チェーンの検証・維持

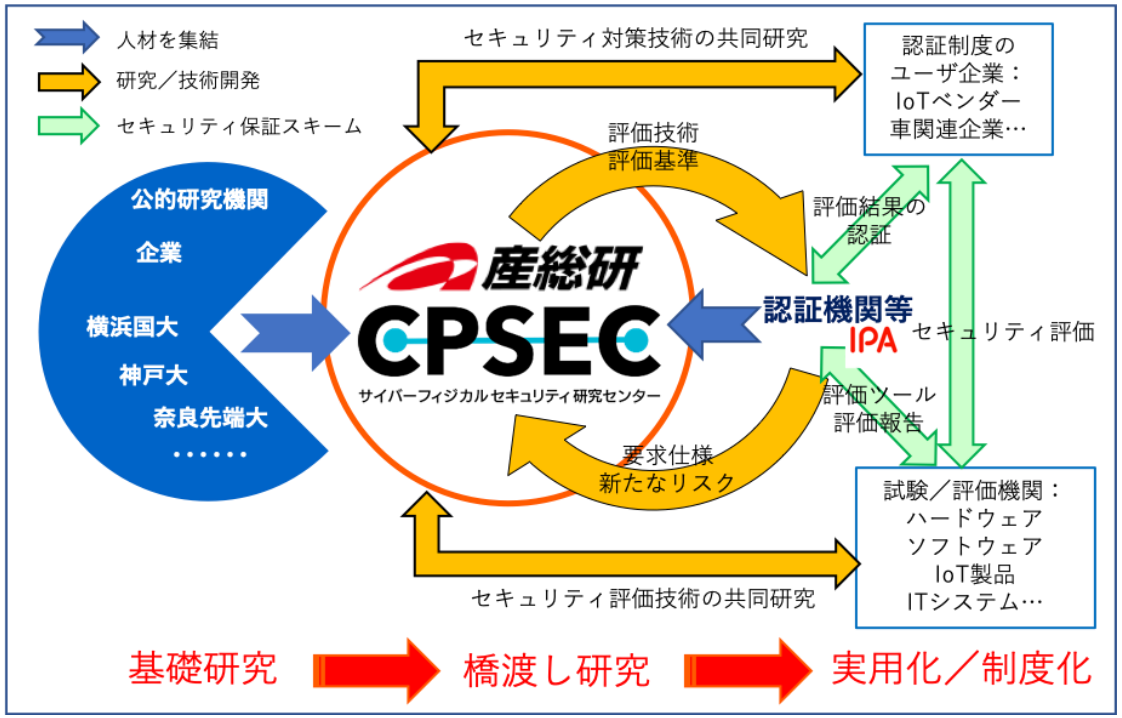
**日立製作所, NEC, KDDI総研, NTT, 三菱電機 等**

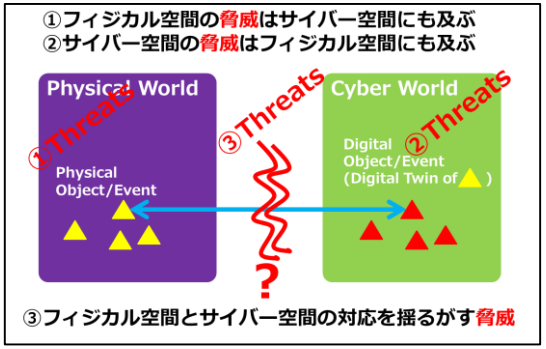
信頼チェーンが安全に運用されていることを検証し、維持することを可能にする技術



# 中核的な研究開発拠点の設置
# ～ 産総研 サイバーフィジカルセキュリティ研究センター（CPSEC）

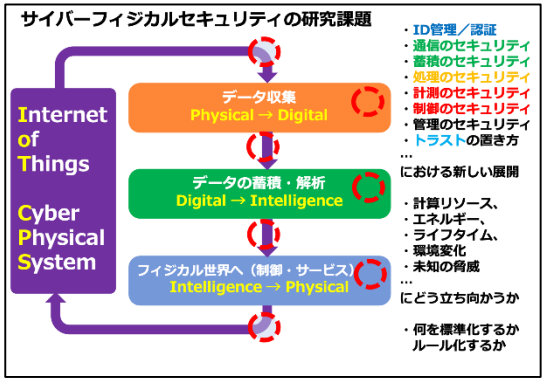
- サイバーフィジカルセキュリティの研究拠点として設置（2018年11月～2025年3月）
- 研究センター長　松本　勉（横浜国立大学とクロスアポイントメント）
- 産総研、企業、大学、試験／評価機関等から研究者や技術者をセンターに集結
  総員121名 = 職員等(産総研の身分を有する者)90名+外来研究員等(含む学生)31名（2月19日時点）
- ７研究チーム（**セキュリティ保証スキーム／高機能暗号／暗号プラットフォーム／ハードウェアセキュリティ／インフラ防護セキュリティ／ソフトウェア品質保証／ソフトウェアアナリティクス**）及び企業との連携研究室で構成
- バリューチェーンにおけるセキュリティで必要となる「研究開発」～「評価制度」までを技術面からサポート
- セキュリティを測定可能とする研究、継続的な最新技術／知見の蓄積




サイバーフィジカル
セキュリティとは

セキュリティを
考慮すべき対象と
研究課題

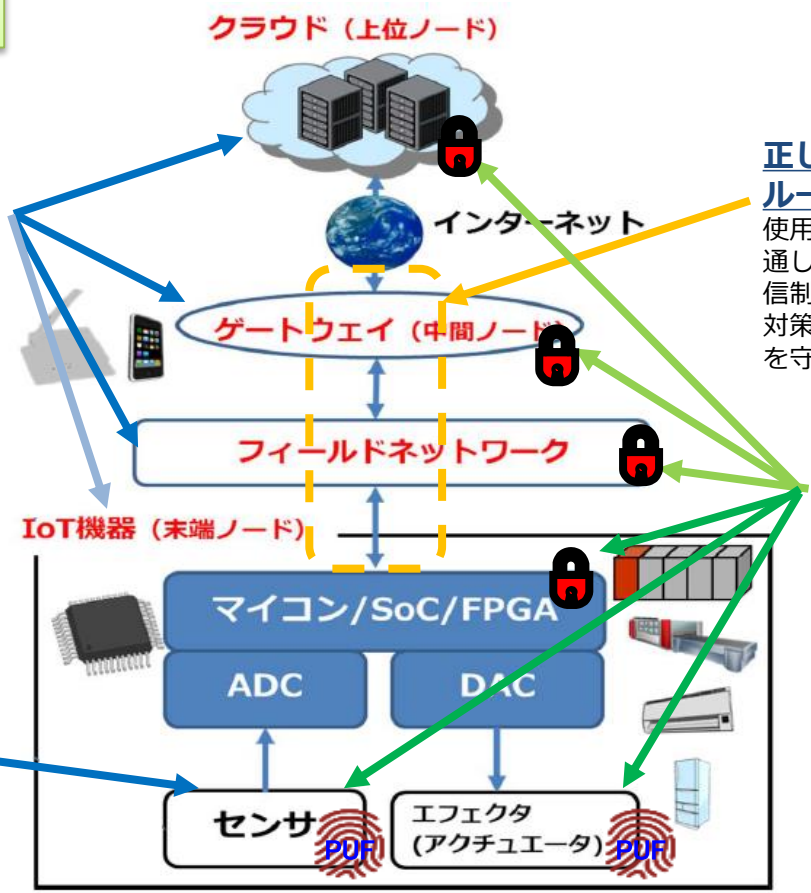


# （参考）高度なIoT社会の実現に向けた技術開発（経済産業省）

- 高機能暗号や計測セキュリティ、通信制御機器、複製不可能デバイスなどの**ハードウェアセキュリティ基盤を構築することで、多様なIoT機器からクラウドまでセキュアな環境を実現。**

**IoT時代における**
**ハードウェアセキュリティ基盤の構築**

**高機能暗号**
クラウドからフィールドネットワークまでのセキュリティ課題を解決する為の、高機能暗号を高速・低消費エネルギーで実現するチップとソフトウェアの要素技術の開発。




**正しい通信だけを許可するルータ等の通信機器**
使用するサービスを元に自動で通してよい通信のみを通す「通信制御」により、セキュリティ対策を個別に実施できない機器を守る。

**複製不可能デバイス**
製造プロセス中のゆらぎなど複製困難な特性(PUFなど)を利用して実現。デバイス固有のIDや暗号鍵に利用することで、安価に機器認証・偽造品防止する要素技術の開発。

(PUF: Physical Unclonable Function)

**計測セキュリティ**
センサ等による情報取得に対する脅威への対策に関する要素技術の開発。

## 1. 研究開発

- 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」
- 中核的な研究開発拠点の設置
  ～ 産総研 サイバーフィジカルセキュリティ研究センター
- 高度なIoT社会の実現に向けた技術開発

## 2. サイバーセキュリティビジネスの強化

- サイバーセキュリティ検証基盤の構築に向けた検討
- サイバーセキュリティお助け隊
- 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ビジネス化に関する政策の方向性

- ビジネス環境を整え、コラボレーション・プラットフォームを軸とした市場展開によりセキュリティ産業の振興・活性化を目指す

## 安心して製品・サービスを利用できる基盤を構築

- サイバーセキュリティ検証基盤
- 情報セキュリティサービス審査登録制度

&

## 隠れたニーズに対応したビジネスの創出

- サイバーセキュリティお助け隊

市場への展開

## ビジネスマッチング

- 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、『Checked by Japan』による競争力創出を促進

- 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等を目的として、**包括的なサイバーセキュリティ検証基盤を構築し、『Checked by Japan』による信頼できる製品の開発の普及促進を図るとともに、検証事業を活性化。**
- 来年度の予算事業を効果的に実施するために、今年度は事前調査を実施。

## 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、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。**

セキュリティ製品のマーケットインの促進

検証ビジネスの活性化

# 【実環境における試行検証①】セキュリティ製品導入組織との意見交換

- 自組織へのセキュリティ製品導入を事例として公表している組織と、製品導入における課題等について意見交換を実施中（～2019年2月まで）。
- セキュリティ製品については導入事例の公表を認めない組織が多い中、公表を認めている理由についても確認。

製品導入

導入実績の公表

ベンダー視点

製品が実環境でも問題なく動作することを検証

導入実績の公表により次のビジネスへつなげる

ユーザーとの意見交換

ユーザー視点での課題抽出

**政策的な方向性の明確化**

コラボレーション・プラットフォームを軸としたベンダーとユーザーのマッチング促進

ベンダー　　ユーザー（企業、大学等）

# 【ホワイトハッカーの実攻撃検証】検証の目的と枠組みの考え方

- Society5.0の進展に伴い、サイバー攻撃の影響範囲は末端のIoT機器まで及ぶことになった。これに伴い、影響が大きなIoT機器等についてはセキュリティの検証を行うことが必要。
- このため、製造者の過失によるIoT機器等の脆弱性に加え、製造者による意図的な脅威（機器が収集した個人情報等の外部への漏洩やバックドアの埋込など）が含まれていないかについて検証を行うための基盤を構築する。

## 検証基盤構築へ向けた考え方

1．IoT機器・システム等の重要性等を考慮した**検証対象の特定**

＋

2．対象機器のライフサイクルへの対応も考慮した**検証手法の選定**

＋

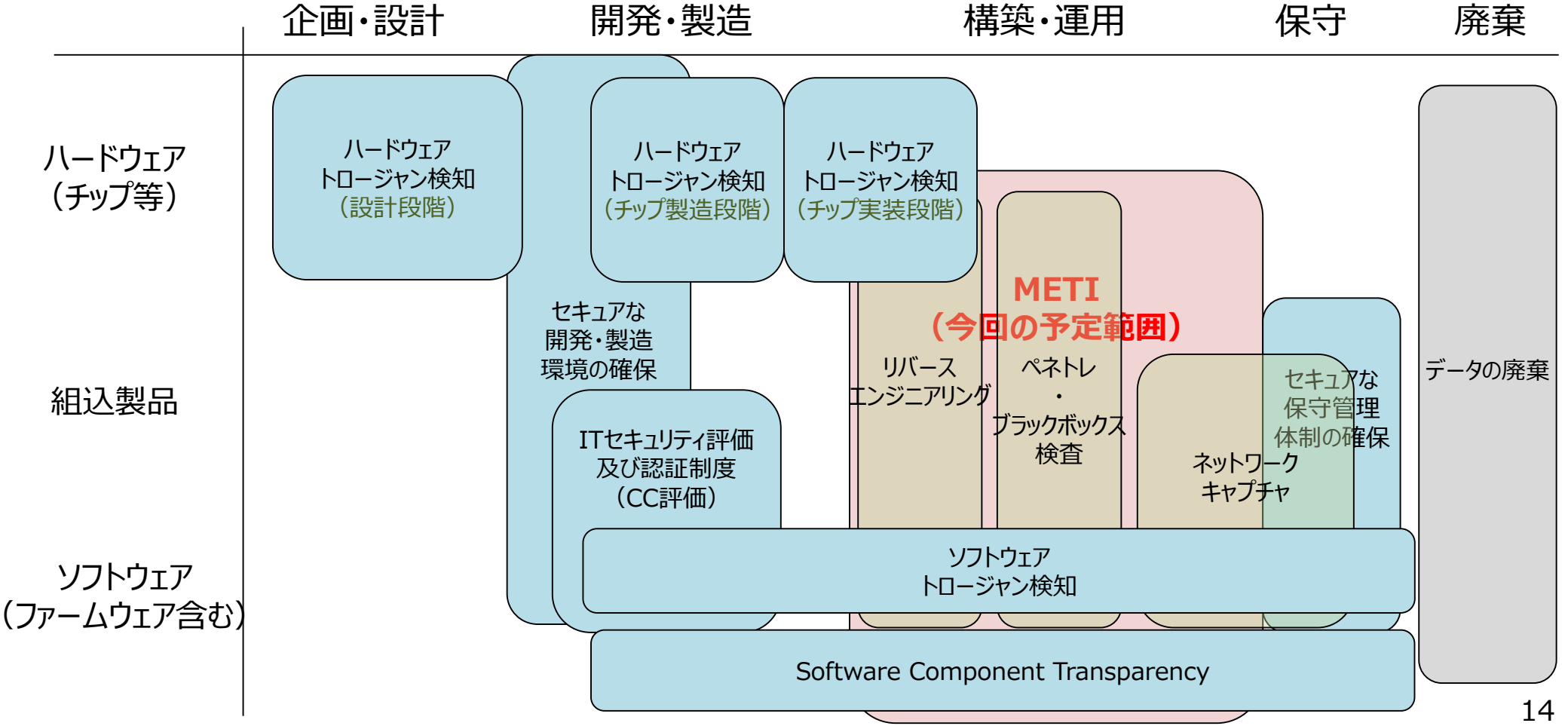
3．技術的・組織的な観点から信頼できる**検証主体の確保**

平成30年度予算を活用し、事前調査を実施

平成31年度予算を活用して、考え方を整理し、検証基盤を構築

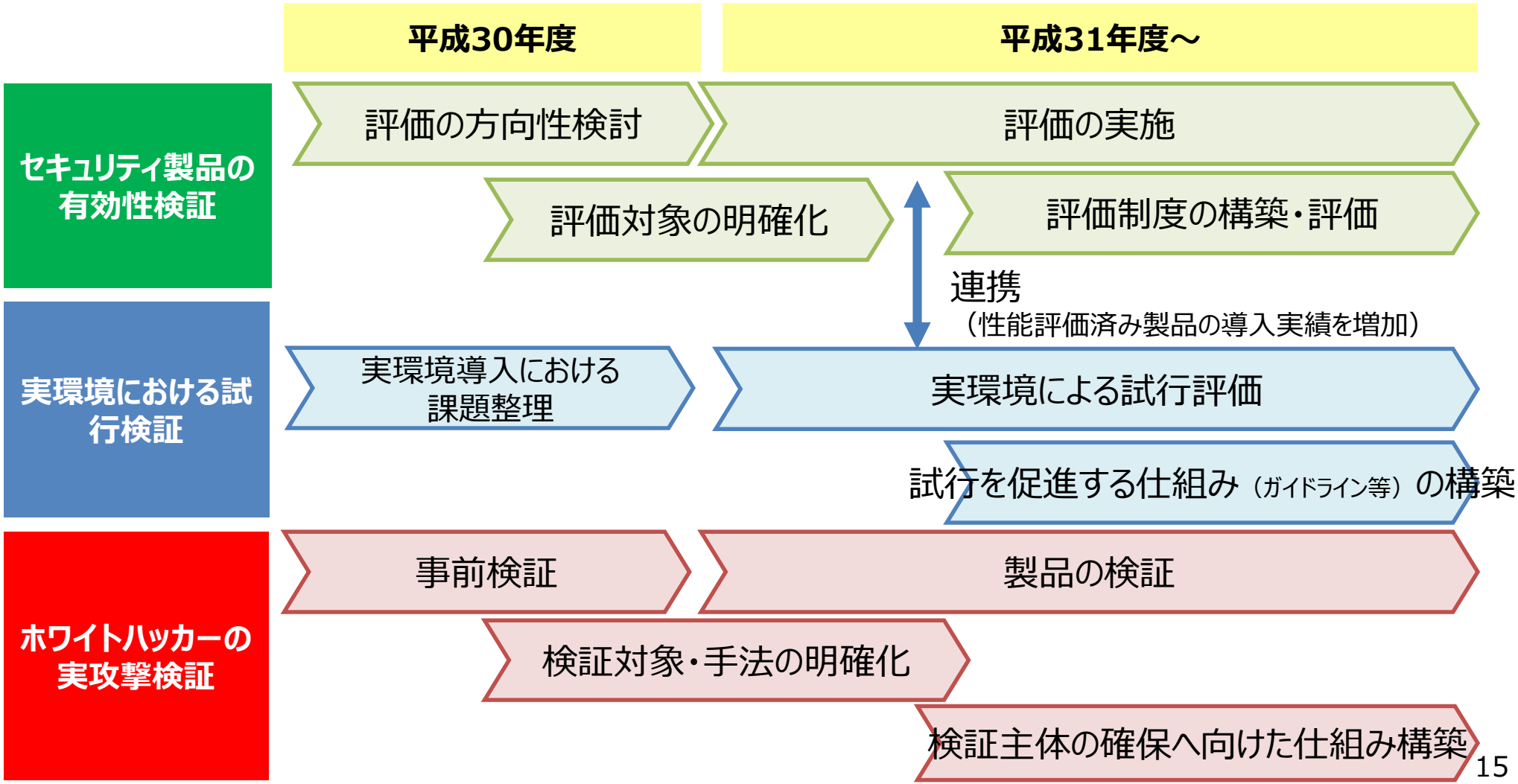
# 【ホワイトハッカーの実攻撃検証】
# 対象機器のライフサイクルへの対応も考慮した検証手法の選定

- 製品のセキュリティ検証の実施に当たっては、製品のライフサイクルも考慮し、検証方法を選択する必要がある。
- IoT機器等を対象とした本検証では、構築・運用段階における検証手法について、その有効性等について確認するとともに、その他の検証手法との関係も整理する。



# 包括的なサイバーセキュリティ検証基盤の構築へ向けた今後の取組

- 今年度中に事前調査を行い、評価の方向性や対象等を明確化。
- 来年度、検証を実施し、対象製品の決定、構築し、評価を開始予定。



# サイバーセキュリティお助け隊

- 平成30年度第二次補正予算、中小企業強靭化対策事業の中の１事業として「サイバーセキュリティお助け隊」の実証事業を全国8地域程度で実施。
- IPAが事業実施主体となり、本年度内に公募開始予定。

## 中小企業等強靭化対策事業

**平成30年度第2次補正予算案額 15.0億円**

中小企業庁 経営安定対策室
03-3501-0459
中小企業庁 技術・経営革新課
03-3501-1816
商務情報政策局 サイバーセキュリティ課
03-3501-1253

### 事業の内容

**事業目的・概要**

- BCP（Business Continuity Plan：事業継続計画）の取組事例や早期復旧事例などを広く紹介するとともに、サプライチェーンに位置づけられる中小企業等のBCPの策定を支援し、そうした取組を横展開することによって、中小企業の防災意識の啓発、強靭化に向けた取組の促進を図ります。
- サイバー攻撃に備えて、中小企業等のセキュリティ対策の普及啓発、マネジメント指導のほか、トラブル時の相談対応・現場派遣体制構築等の実証事業を行います。

**成果目標**

- 延べ2万者の中小企業者に対し、BCPの重要性等について啓発を行います。
- BCPのモデルとなる取組（例：サプライチェーン、地域の中核企業）を支援し、これら支援成果をとりまとめて事例集として公表し、BCP策定を促進します。
- 8地域で、サイバーセキュリティ対策の啓発を行うとともに、トラブル時の相談体制等の実証を行い、必要な人材、体制等を明らかにすることを目指します。

（１）BCP等普及啓発事業

国 → 民間団体等 → 中小企業・小規模事業者

委託・補助（10/10）　説明会・訪問・相談会、指導等

（２）BCP策定・対策支援事業

国 → 民間団体等 → 中小企業・小規模事業者

委託・補助（10/10）　支援・実証

### 事業イメージ

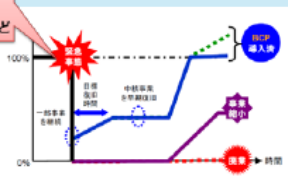
**１．BCP等普及啓発事業**

- 中小企業に、自社の災害リスクやサプライチェーンに対するサイバー攻撃のリスクを認識してもらうとともに、BCPの策定・取引先も含めた対策状況の点検や保険を含めた対応等について、啓発を図ります。
- 具体的には、商工団体等を通じて、会員企業等への周知を行うとともに、全国各地において、シンポジウム等を開催します。

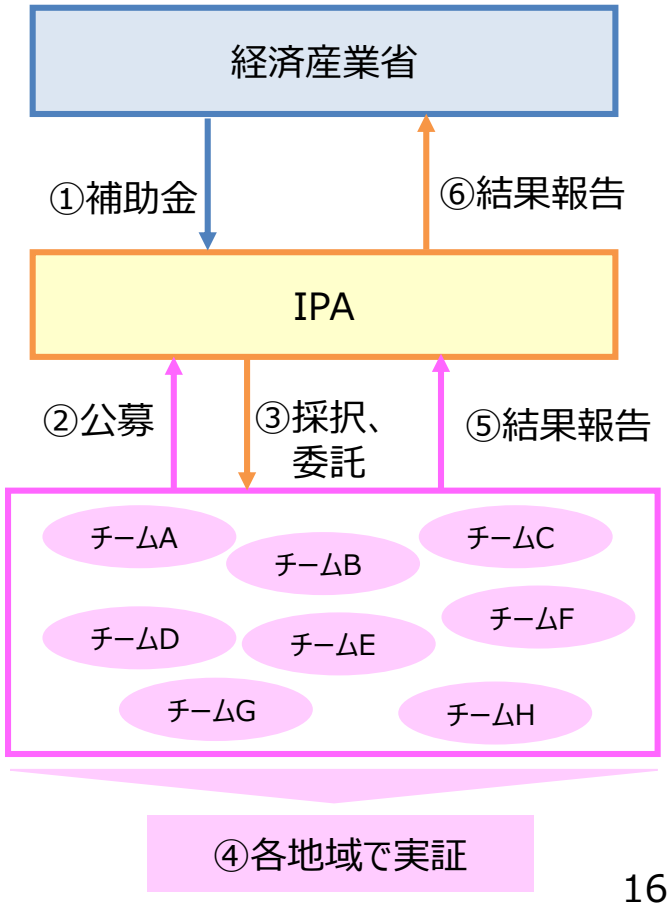
**２．BCP策定・対策支援事業**

- サプライチェーンに位置づけられる中小企業等について、各企業が直面するリスクに応じたBCPの策定をハンズオンで支援します。
- 全国各地において、ワークショップを開催し、参加する中小企業に対し、BCPの必要性について啓発を図るとともに、その策定に向けた試行的取組を支援します。
- サプライチェーン全体のサイバーセキュリティ対策の普及啓発に取り組むとともに、サイバー攻撃によるトラブル時の相談対応・現場派遣などの支援サービス提供体制を整備するなど、中小企業のニーズに沿ったセキュリティ技術・サービスの実証事業を地域単位で実施します。

例えば、
・大地震等の自然災害
・テロ等の事件、大事故
・突発的な経営環境の変化
など




＜事業実施体制＞

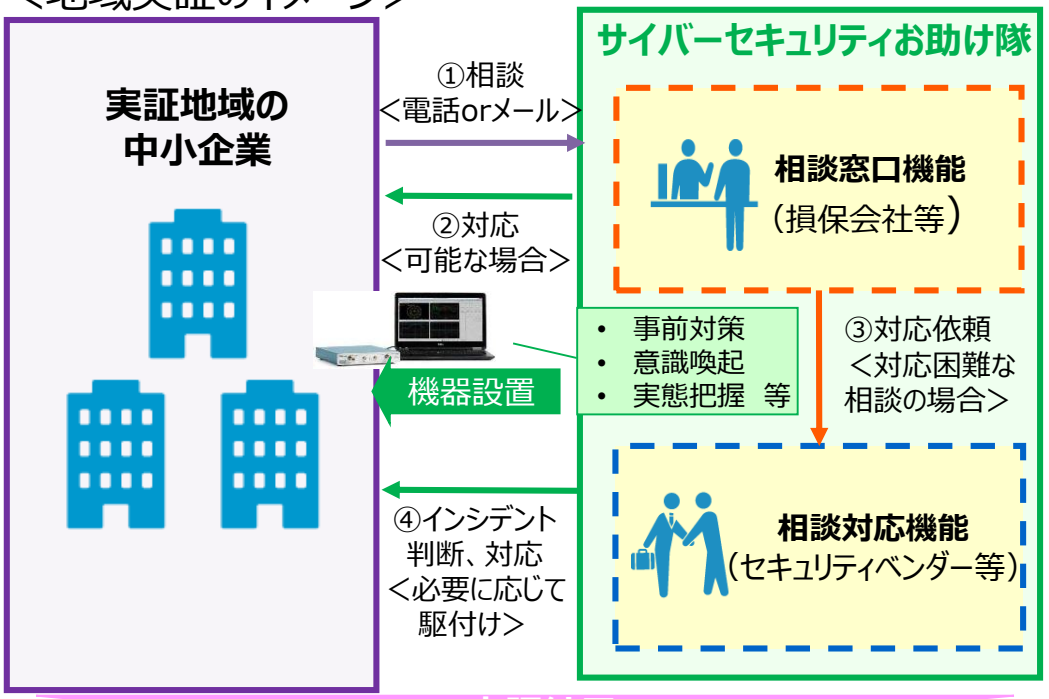



経済産業省　平成30年度第２次補正予算案の概要（ＰＲ資料）

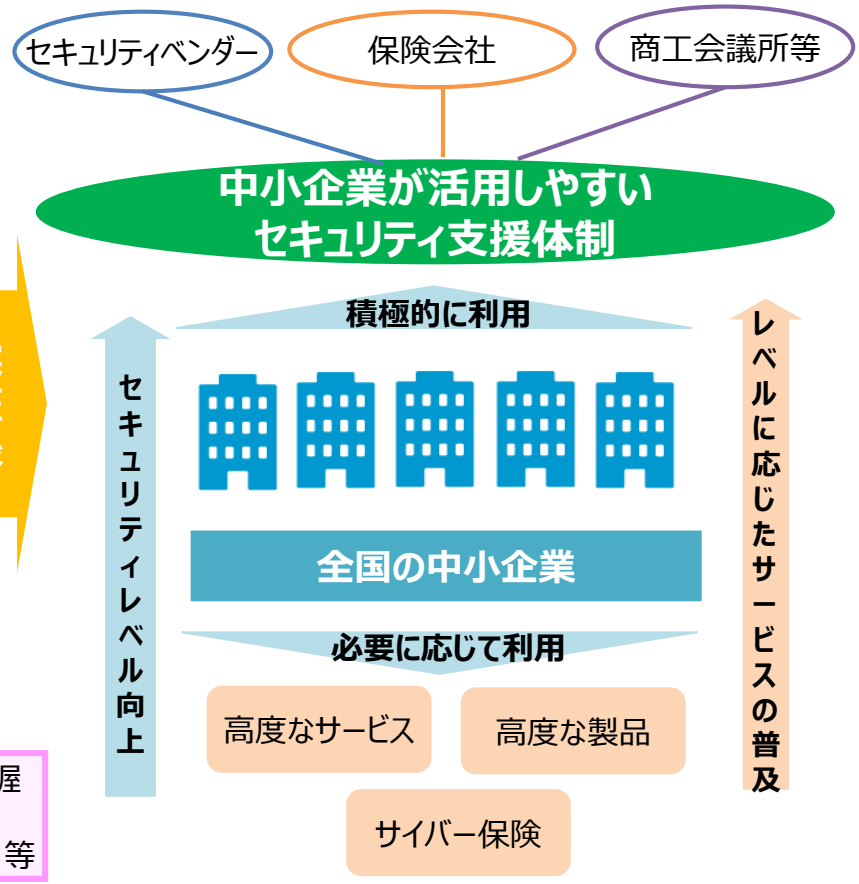
# サイバーセキュリティお助け隊の実証

- 中小企業向けにサイバーセキュリティに関する支援の仕組みを新たに構築し、全国最大8地域を対象に地域の団体、企業等と連携した実証を行い、サイバー攻撃の実態や対策のニーズを把握するとともに、中小企業の事前対策の促進、意識喚起を図る。
- 実証後は、保険機能とも連動した中小企業が利用しやすい支援体制の構築を目指す。

＜地域実証のイメージ＞




実証後




実証結果

**中小企業　側**

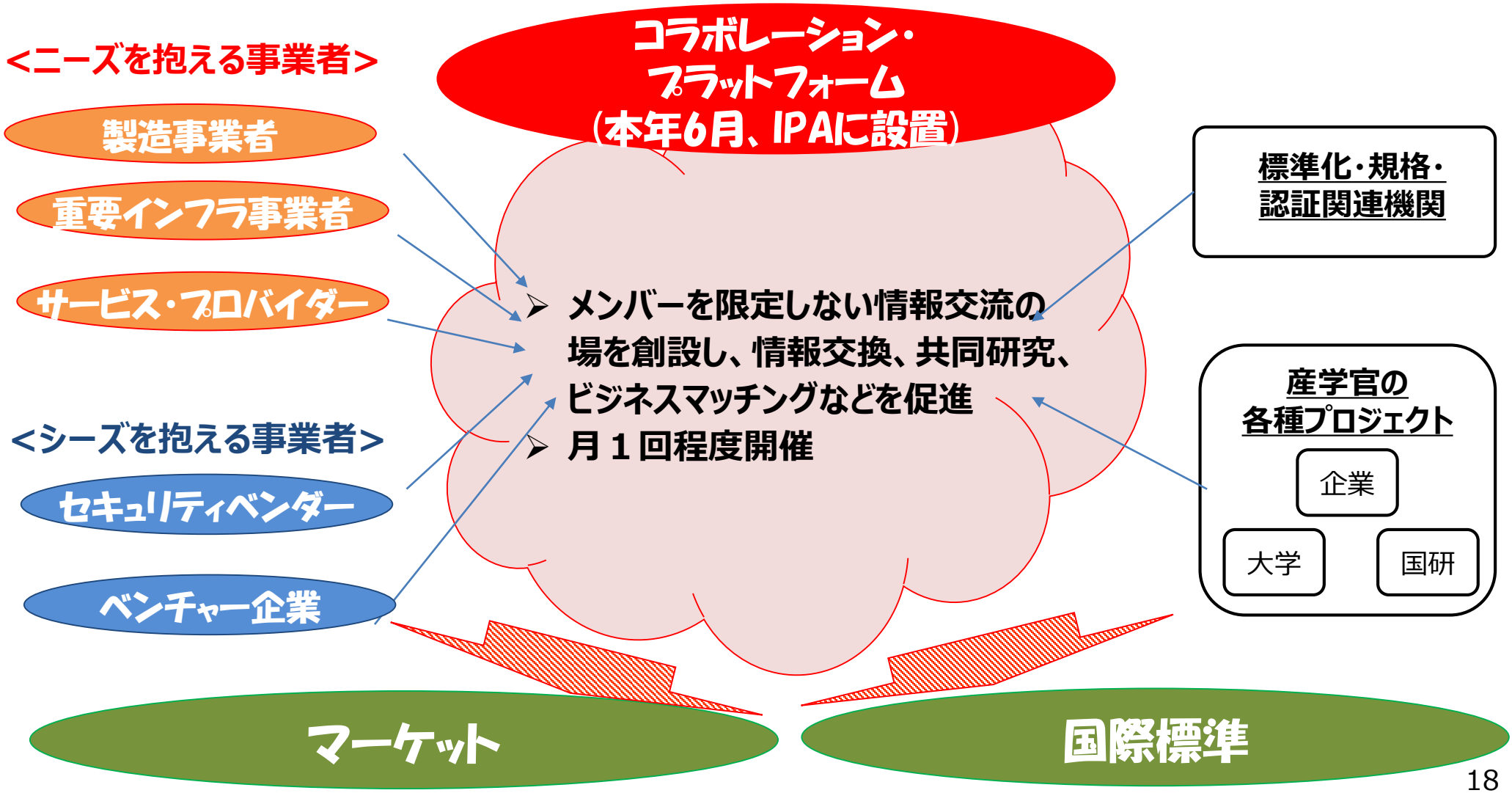
- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上　　等

**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

# 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。**



# コラボレーション・プラットフォームの開催状況

- 各回、予定定員以上の申込みがあり、参加者からは政府との意見交換、最新動向の情報収集、人脈形成等、様々な視点で有益との声も。

| | 開催日 | 参加人数(*) | 主なテーマ |
|---|---|---|---|
| 第一回 | 6月13日 | 179名（99名） | 経済産業省の政策動向 |
| 第二回 | 7月23日 | 104名（74名） | サプライチェーン対策、人材育成、つながる世界の脅威と対策 |
| 第三回 | 9月3日 | 132名（69名） | 業界別のセキュリティ対策、セキュリティ検証基盤、サイバーセキュリティ経営 |
| 第四回 | 10月16日 | 151名（56名） | 中小企業のセキュリティ対策 |
| 第五回 | 11月30日 | 98名（40名） | IoTの技術・標準化動向 |
| 第六回 | 1月25日 | 108名（48名） | サイバー・フィジカル・セキュリティ対策フレームワーク |
| 第七回 | 3月4日 | 100名超の予定 | IoT等のIoTの導入時等におけるセキュリティの強化 |

(*)括弧内の人数はコラボレーション・プラットフォーム後に開催した情報交換会の出席者数


富田理事長(IPA)ご挨拶


三角審議官(経済産業省)ご挨拶


パネルディスカッション(第一回)


グループディスカッション(第二回)

# コラボレーション・プラットフォームの今後の方向性

- 新規参加企業の増加を促し、人脈形成の機会を強化するとともに４つの観点でのコラボレーションの実現を目指す。

## 【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増やし、**参加者からのご意見を着実に政策に反映**。

※ コラボレーション・プラットフォームだからこそ実現可能。

## 【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**。

※ ベンダー同士でチームを組むことにより、解決できる課題や販売網の拡大を期待。

## 【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**。

※ セキュリティ担当者が少ない企業からは、悩みを共有できる仲間がいなくて困っているとの声も。

## 【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。

※ 規模の小さな企業からはユーザ企業等とのパスがなく事業拡大が困難との声も。