

# クラウド化推進社会と 我が国のサイバーセキュリティ戦略

**MPOWER**  
CYBERSECURITY SUMMIT

開催日: 2018. 11. 8 (木)  
会場: ザ・プリンスタワー東京  
登録受付中 >



MPOWER2018 講演資料 of McAfee

日本銀行



銀行



箆筒

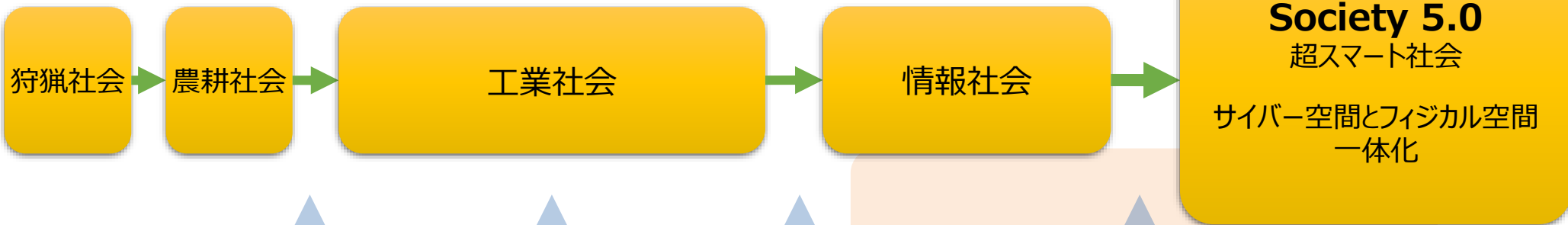


平成30年11月8日

内閣官房内閣サイバーセキュリティセンター(NISC) 内閣審議官  
経済産業省(METI) サイバーセキュリティ・情報化審議官  
三角 育生

# Society 5.0では

## <社会の変化>

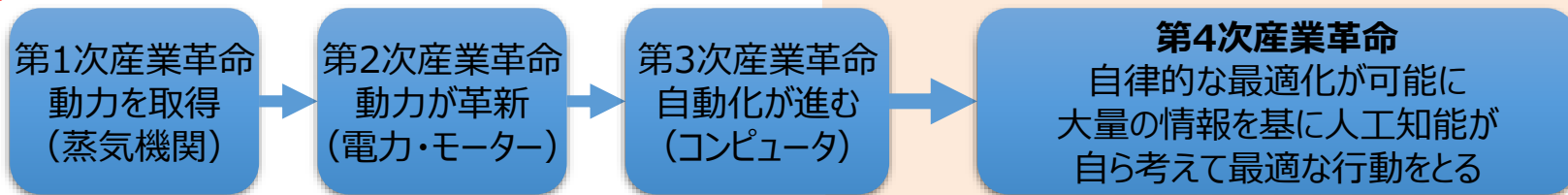


## <産業の在り方の変化>

個々の産業ごとに発展



## <技術の変化>



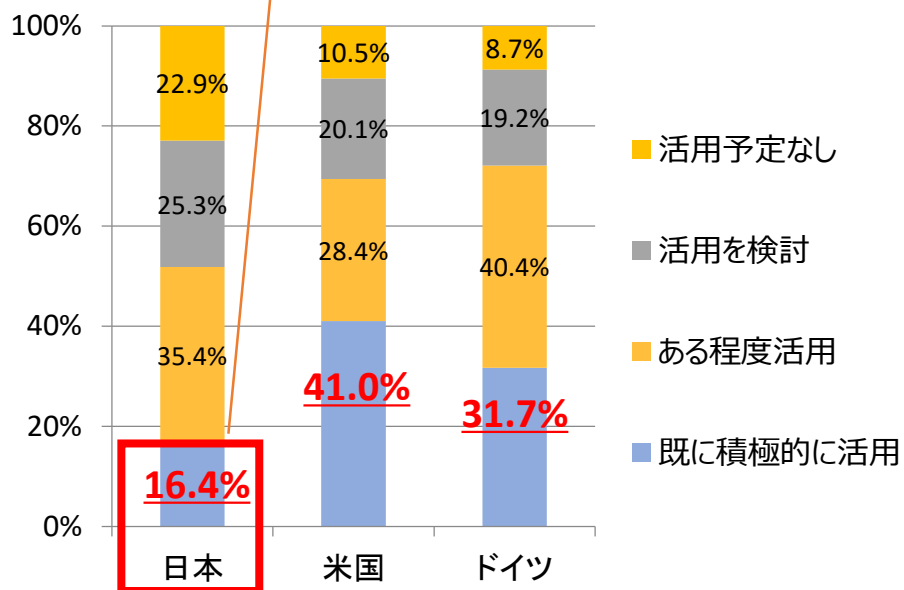
# 我が国のデータ利活用の現状

日本では、諸外国に比べるとデータ利活用の遅れをとっている

しかし、製造現場(工場内)においてデータを取得している企業の割合は増加している

## 諸外国比較（データの利活用状況）

欧米諸国に比べてデータを利活用している企業が少ない

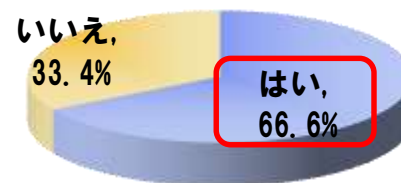


(出典) 総務省「安心・安全なデータ流通・利活用に関する調査研究」(平成29年) から経済産業省作成

## 【国内工場で何らかのデータ収集を行っているか】

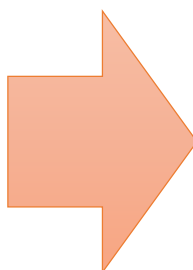
2016年

(n=4566)



資料：経済産業省調べ（16年12月）

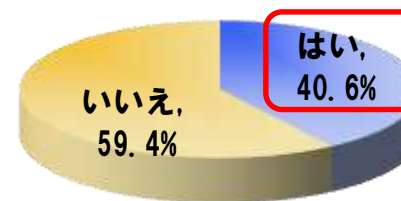
日本においても  
データ取得企業は  
増加している



しかし...

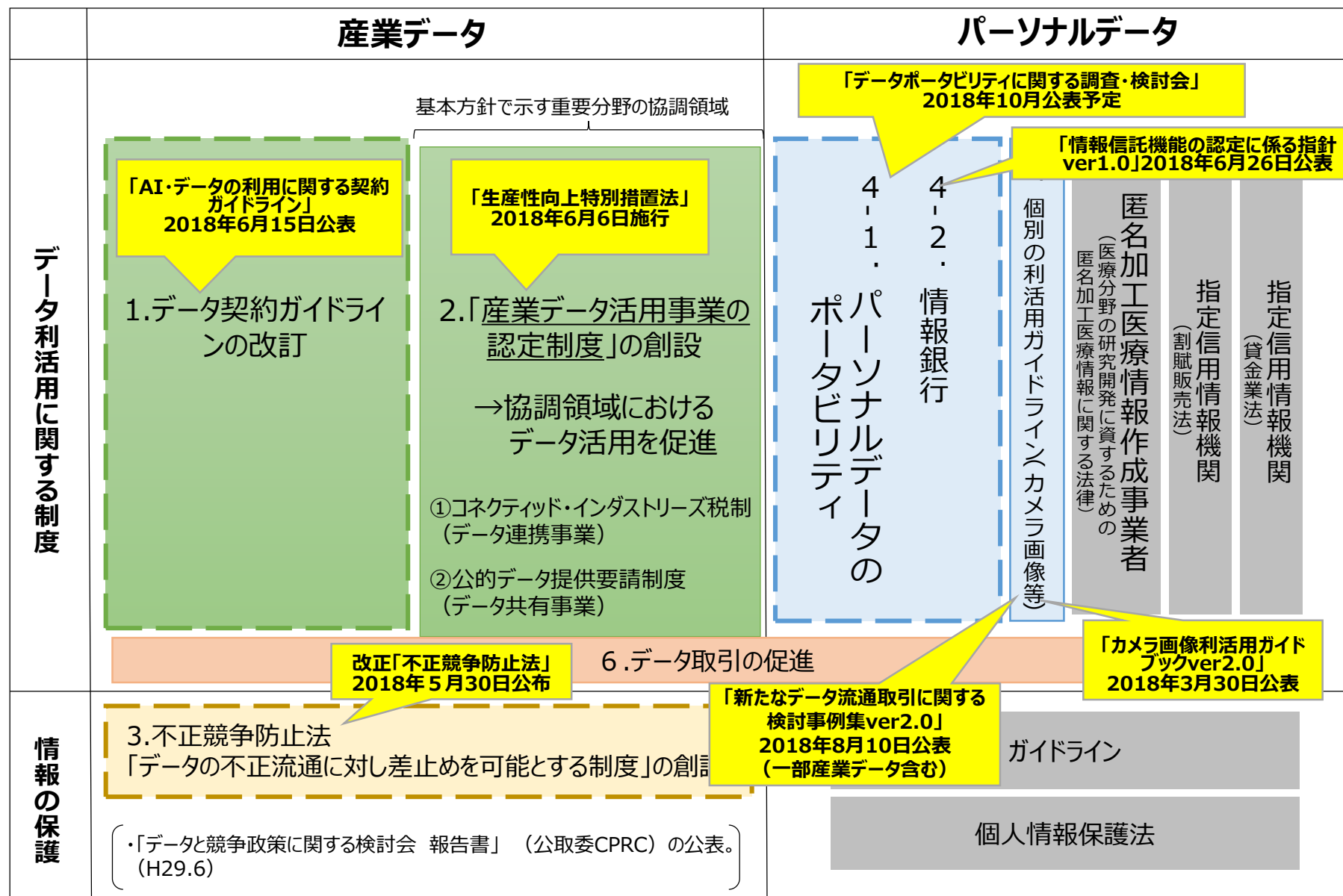
2015年

(n=3751)



資料：経済産業省調べ（15年12月）

# Connected Industries実現のためのデータ関連制度の整備



# サイバーセキュリティ戦略

平成30年7月27日閣議決定

## 1 策定の趣旨・背景

- Society5.0
- サイバー空間と実空間の一体化の進展

## 2 サイバー空間に係る認識

- 人工知能（AI）、IoTなど→人々に豊かさ
- 多大な経済的・社会的損失が生ずる可能性は指数関数的に拡大

## 3 本戦略の目的

- 自由、公正かつ安全なサイバー空間
- 持続的な発展のためのサイバーセキュリティ（サイバーセキュリティエコシステム）  
← ①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働

## 4 目的達成のための施策

### (1)経済社会の活力の向上 及び持続的发展

～新たな価値創出を支える  
サイバーセキュリティの推進～

- 新たな価値創出を支えるサイバーセキュリティの推進
- 多様なつながりから価値を生み出すサプライチェーンの実現
- 安全なIoTシステムの構築

### (2)国民が安全で安心して 暮らせる社会の実現

～国民・社会を守る任務を保証～

- 国民・社会を守るための取組
- 官民一体となった重要インフラの防護
- 政府機関等におけるセキュリティ強化・充実
- 大学等における安全・安心な教育・研究環境の確保
- 2020年東京大会とその後を見据えた取組
- 従来の枠を超えた情報共有・連携体制の構築
- 大規模サイバー攻撃事態等への対処態勢の強化

### (3)国際社会の平和・安定及び 我が国の安全保障への寄与

～自由、公正かつ安全なサイバー空間の堅持～

- 自由、公正かつ安全なサイバー空間の堅持
- 我が国の防御力・抑止力・状況把握力の強化
- 国際協力・連携

### (4)サイバーセキュリティに関する共通基盤的な取組の推進

■ 人材育成・確保

■ 研究開発の推進

■ 全員参加による協働

## 5 推進体制

- 内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化



# (1)経済社会の活力の向上及び持続的发展

## 1. 新たな価値創出を支えるサイバーセキュリティの推進

経営層の意識改革の促進  
（「費用」から「投資」へ）

## 2. 多様なつながりから価値を生み出す サプライチェーンの実現

脅威を明確化し、運用レベルでの対策を実現  
する業種横断的指針の作成

中小企業の実組の推進

## 3. 安全なIoTシステムの構築



# セキュリティに関する経営層の関わり

海外と比較すると日本の企業は情報セキュリティに関する意思決定において経営層の関わりが薄い

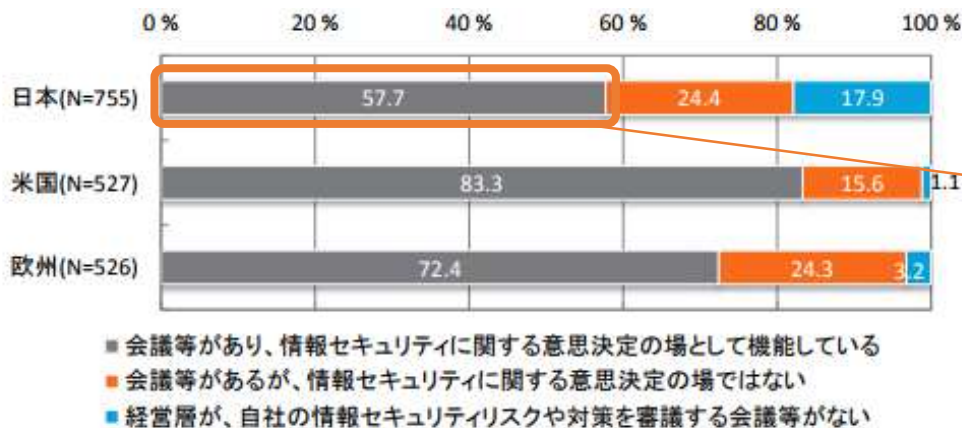


図 5.3-2 経営層の情報セキュリティに対する関与

経営層が積極的にセキュリティに関与している企業は6割弱

セキュリティが経営上のリスクの1つであることを上司から説明を受けている企業は7割弱 (米国は9割強)

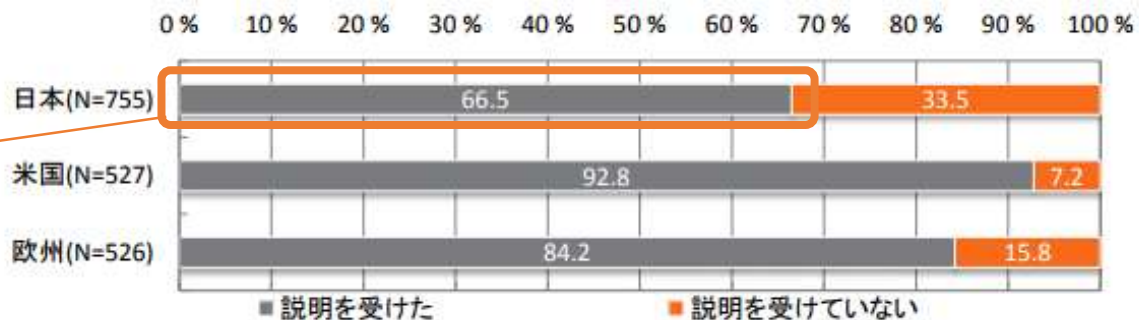


図 5.3-1 経営層または上司からの説明状況

出典：企業のCISOやCSIRTに関する実態調査2017(IPA)

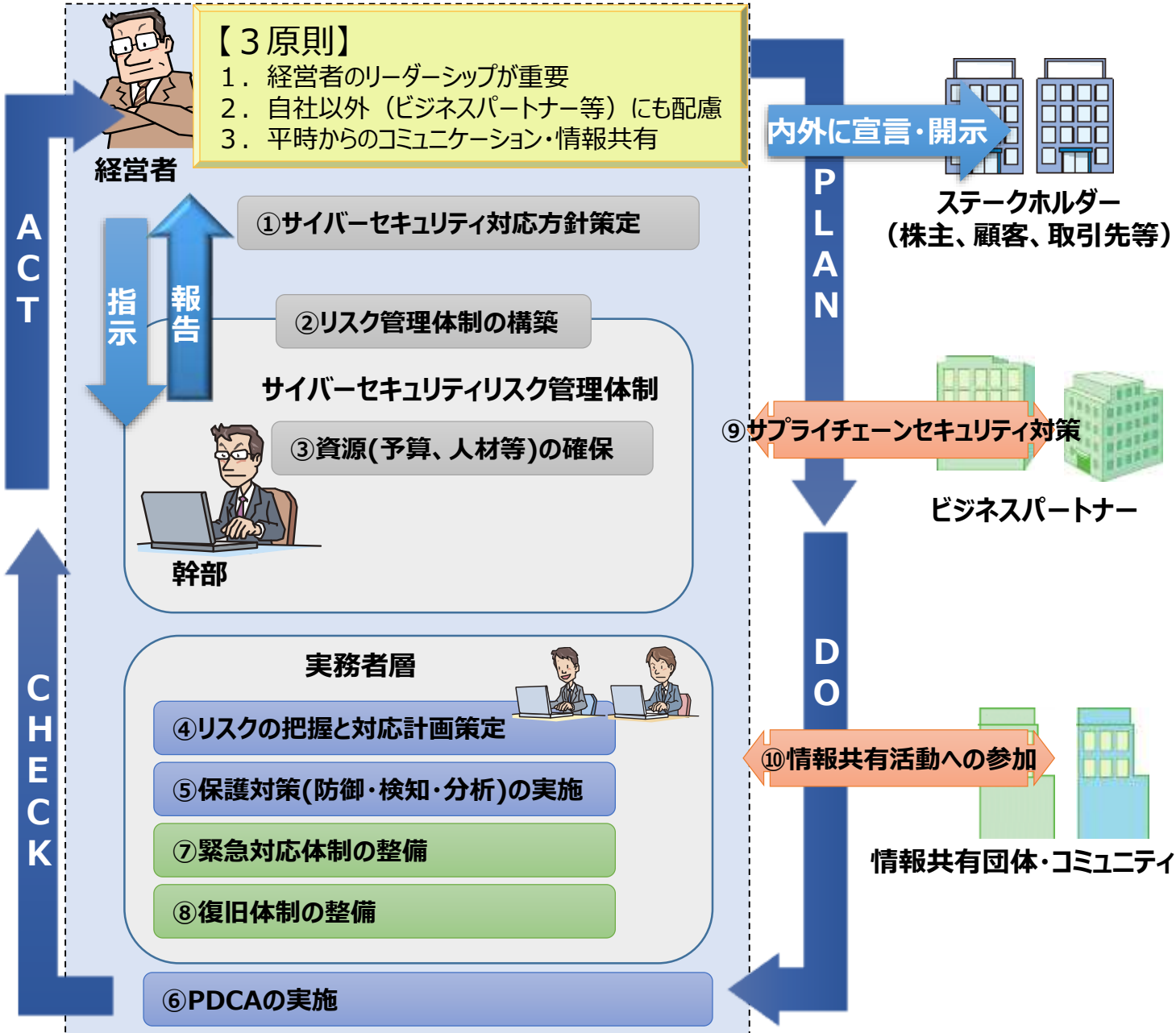
# NIKKEI225企業の情報提供

平成27年度 日経225社業種別サイバーセキュリティ情報開示状況

日経業種分類				開示 企業数	開示企業%	
大分野	社数	中分野	社数		中分野	大分野
A 技術	58	01 医薬品	8	5	62.5%	74.1%
		02 電気機器	29	22	75.9%	
		03 自動車	10	7	70.0%	
		04 精密機器	5	3	60.0%	
		05 通信	6	6	100.0%	
B 金融	21	06 銀行	11	11	100.0%	100.0%
		07 その他金融	1	1	100.0%	
		08 証券	3	3	100.0%	
		09 保険	6	6	100.0%	
C 消費	31	10 水産	3	1	33.3%	87.1%
		11 食品	11	10	90.9%	
		12 小売業	8	8	100.0%	
		13 サービス	9	8	88.9%	
D 素材	66	14 鉱業	1	0	0.0%	42.4%
		15 繊維	5	1	20.0%	
		16 パルプ・紙	5	0	0.0%	
		17 化学	18	7	38.9%	
		18 石油	2	2	100.0%	
		19 ゴム	2	1	50.0%	
		20 窯業	9	3	33.3%	
		21 鉄鋼	5	1	20.0%	
		22 非鉄・金属	12	7	58.3%	
E 資本財 ・その他	36	23 商社	7	6	85.7%	52.8%
		24 建設	9	5	55.6%	
		25 機械	16	8	50.0%	
		26 造船	2	2	100.0%	
		27 その他製造	3	3	100.0%	
F 運輸 ・公共	20	28 不動産	6	1	16.7%	90.0%
		29 鉄道・バス	8	8	100.0%	
		30 陸運	2	2	100.0%	
		31 海運	3	1	33.3%	
		32 空運	1	1	100.0%	
		33 倉庫	1	1	100.0%	
		34 電力	3	3	100.0%	
合計	232	232		156		



# サイバーセキュリティ経営ガイドライン

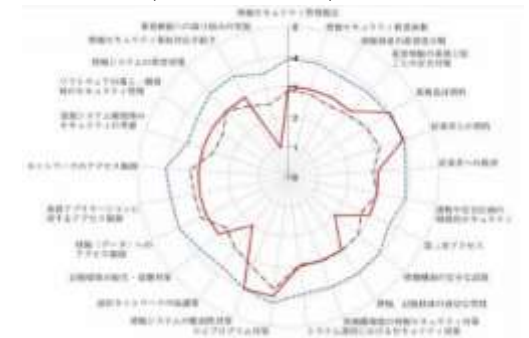


『対策事例集』と  
『可視化ツール』の整備

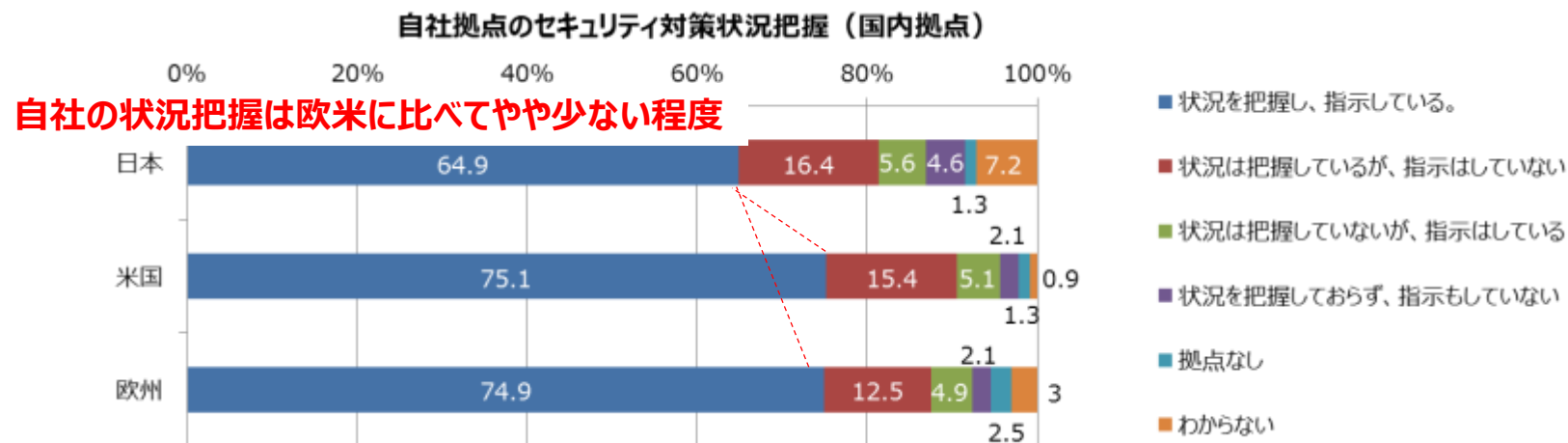
業界団体（ユーザ企業）  
と連携して

10項目に対応した  
プラクティス集

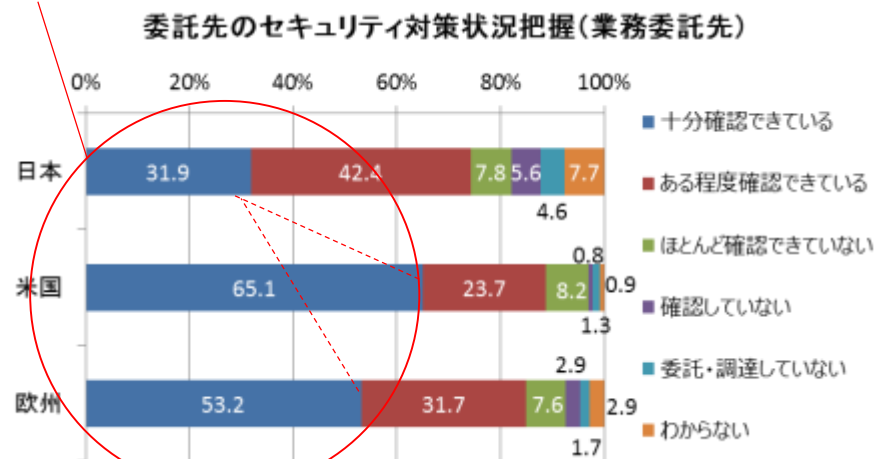
可視化ツール  
(イメージ)



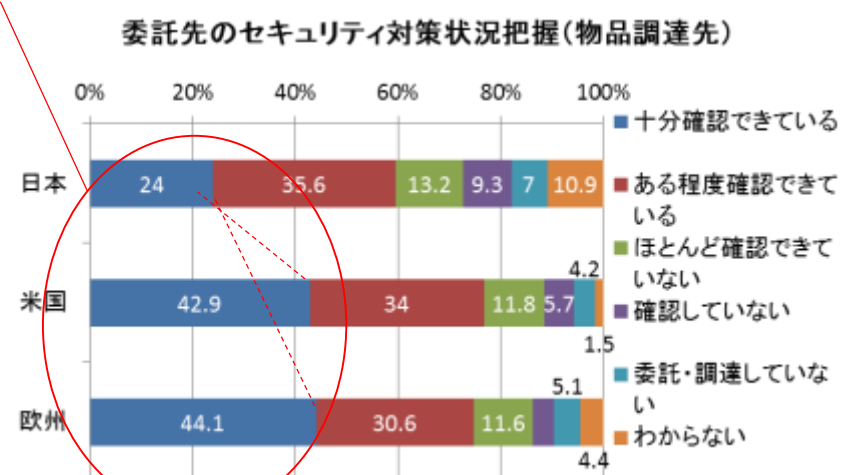
# 現状： 日本企業は、委託先等の取引先への対策が欧米に比べて遅れている



## 委託先の状況把握は米国の半分以下、欧州の2/3



## 調達先の状況把握は欧米の6割以下



出典：独立行政法人情報処理推進機構「企業のCISOやCSIRTに関する実態調査2017-調査報告書-」（2017年4月13日）

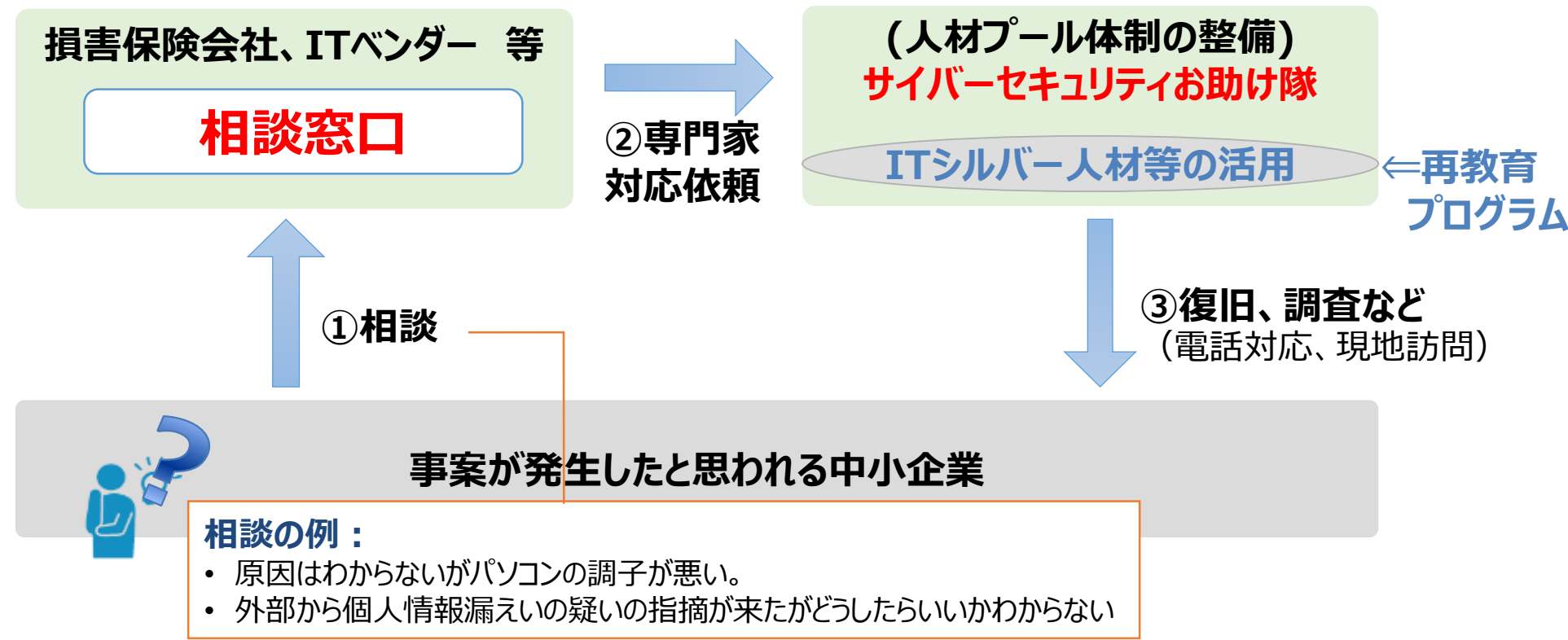
\* 日本・米国・欧州（英・独・仏）の従業員数300人以上の企業のCISO、情報システム／情報セキュリティ責任者／担当者等にアンケートを実施（2016年10～11月）

\* 回収は日本755件、米国527件、欧州526件

# 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



# サプライチェーン構造の変化を踏まえ、新たな枠組みを提唱

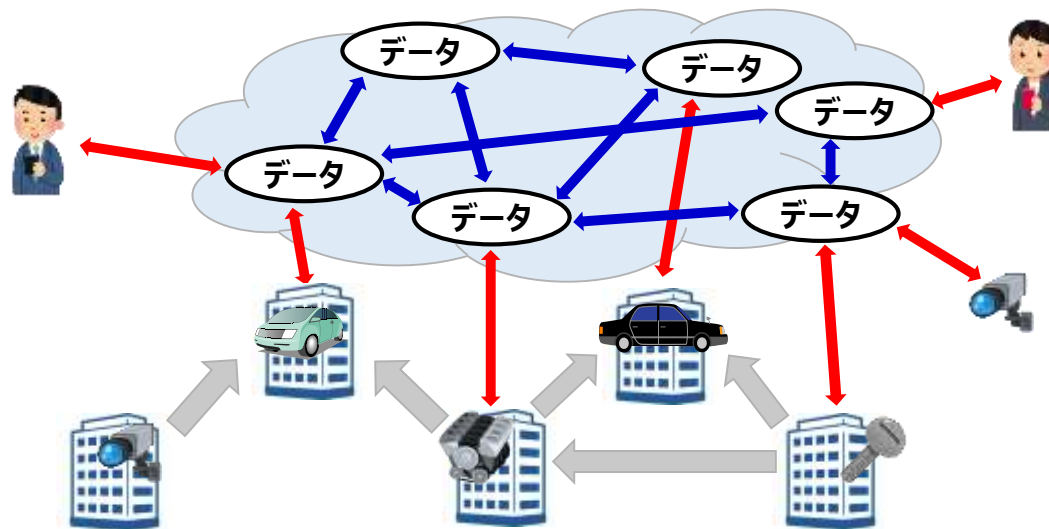
「Society5.0」では、データの流通・活用を含む、より柔軟で動的なサプライチェーン『バリュークリエーションプロセス』へと、サプライチェーンの構造が変化

「Society5.0」以前  
(従来のサプライチェーン)



個々の企業主体の定型的なつながり  
(従来のサプライチェーン)で価値を  
生み出す

「Society5.0」  
(より柔軟で動的なサプライチェーンへ)



様々な企業や個人等のより柔軟で動的な  
つながり、『バリュークリエーションプロセス』が  
価値を生み出す

「Society5.0」におけるセキュリティを確保す  
るためには、**従来とは異なる新たな視点が必要**

『サイバー・フィジカル・セキュリティ対策  
フレームワーク』の策定へ

## (2)国民が安全で安心して暮らせる社会の実現

### 1. 国民・社会を守るための取組

「積極的サイバー防御」の構築

サイバー犯罪への対策

### 2. 官民一体となった重要インフラの防護

重要インフラ行動計画に基づく取組の推進

地方公共団体の取組強化

### 3. 政府機関等におけるセキュリティ強化・充実

情報システムの状態のリアルタイム管理の強化

### 4. 大学等の多様性を踏まえた対策の推進

各層別研修及び実践的な訓練・演習の実施

### 5. 2020年東京大会とその後を見据えた取組

サイバーセキュリティ対処調整センターの構築

### 6. 従来の枠を超えた情報共有・連携体制の構築

### 7. 大規模サイバー攻撃事態等への対処態勢強化

サイバー攻撃と実空間の双方の危機管理に挑むための  
対処態勢の強化



任務保証の実現（サービスの安全かつ持続的な提供）

情報共有・連携

（サイバーセキュリティ協議会、政府オリパラCSIRT等）



リスクマネジメントの  
促進



安全基準等の  
策定・改善



演習・訓練の  
実施・参加



セキュリティ人材の  
育成



情報収集・分析



# サイバーセキュリティ基本法の一部を改正する法律案の概要

## 趣旨

サイバーセキュリティに対する脅威が一層深刻化する中、我が国におけるサイバーセキュリティの確保を促進し、2020年東京オリンピック・パラリンピック競技大会の開催に万全を期すため、**官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行う**ための協議会を創設する等の措置を講ずる

## 概要

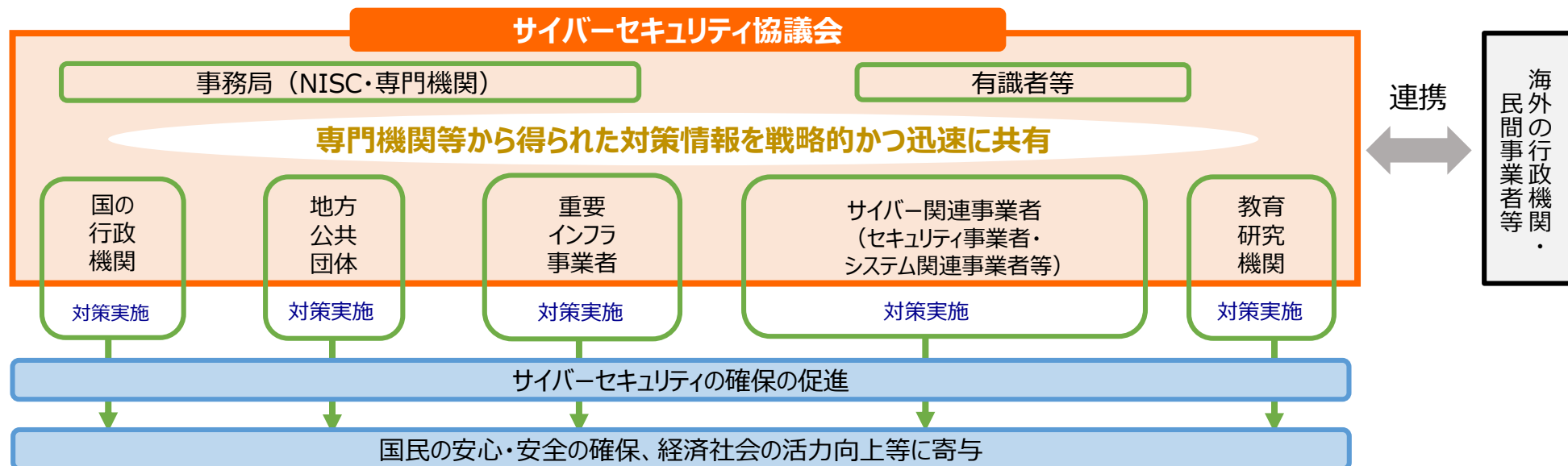
### ● サイバーセキュリティ協議会の創設

官民の多様な主体が相互に連携して情報共有を図り、必要な対策等について協議を行うための協議会を、サイバーセキュリティ戦略本部長等が創設するとともに、構成員に対して遵守事項（秘密保持、情報提供の協力）等を定める

### ● サイバーセキュリティ戦略本部による連絡調整の推進

本部の所掌事務に、事象が発生した場合における国内外の関係者との連絡調整に関する事務を追加し、当該事務の一部を政令で定める法人に委託することができることとするとともに、当該法人に対して秘密保持義務等を定める

【施行期日】 公布の日から起算して一年を超えない範囲内において政令で定める日





# 政府のビジョンとクラウドの位置づけ

- ・クラウド・バイ・デフォルト原則を採用
- ・成長戦略、サイバーセキュリティ戦略等において、安全性評価の検討を位置づけ

## 政府情報システムにおけるクラウドサービスの利用に係る基本方針(2018 年6月7日 C I O連絡会議決定)

### 2 基本方針

#### 2.1 クラウド・バイ・デフォルト原則

政府情報システムは、クラウド・バイ・デフォルト原則、すなわち、**クラウドサービスの利用を第一候補**として、その検討を行うものとする

## 未来投資戦略2018(2018 年6月15日 閣議決定)

### Ⅱ. 経済構造革新への基盤づくり

#### [ 1 ]データ駆動型社会の共通インフラの整備

##### 1. 基盤システム・技術への投資促進

##### (3) 新たに講ずべき具体的施策

##### ii) サイバーセキュリティの確保

クラウドサービスの多様化・高度化に伴い、官民双方が一層安全・安心にクラウドサービスを採用し、継続的に利用していくため、情報資産の重要性に応じ、信頼性の確保の観点から、**クラウドサービスの安全性評価について、諸外国の例も参考にしつつ、本年度から検討を開始する**

## サイバーセキュリティ戦略(2018年7月27日 閣議決定)

### 4. 目的達成のための施策

#### 4.2. 国民が安全で安心して暮らせる社会の実現












##### 4.2.3 政府機関等におけるセキュリティ強化・充実

##### (2) **クラウド化の推進等による効果的なセキュリティ対策**

各府省庁において情報の特性に応じて適切な情報システムの形態を選択するとともに、政府全体としてセキュリティ施策を効率的・効果的に実施できるよう、システムの構築と運用の集約及びセキュリティ水準向上の利点を活かすことができる、政府プライベートクラウドとしての政府共通プラットフォームへの移行を含む**クラウド化を推進する。クラウド化の推進に当たっては、安全性評価など、適切なセキュリティ水準が確保された信頼できるクラウドの利用を促進する方策について検討を進める**

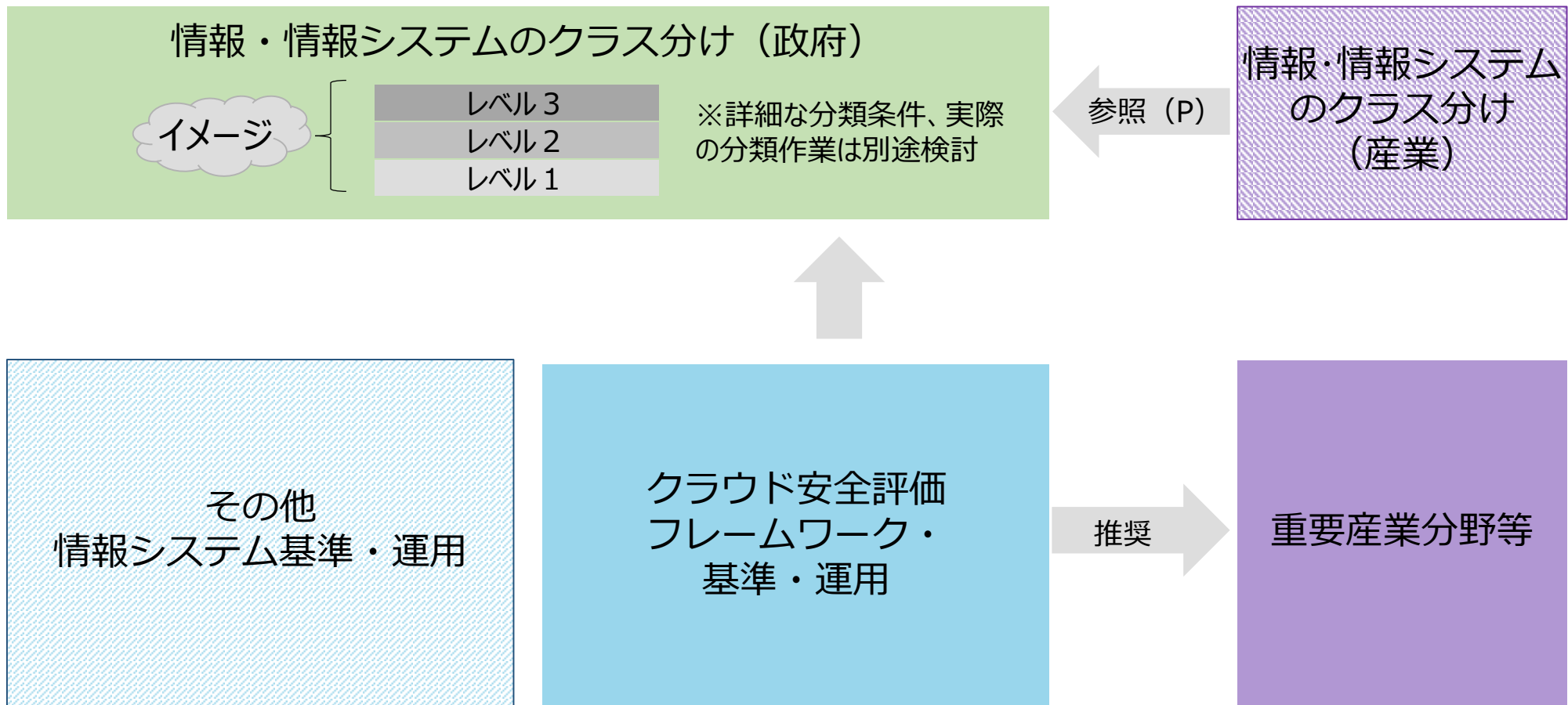
# クラウドサービスに係る世界の潮流（海外政府調達について）

- 海外の政府調達では、多くが①クラウドファーストを掲げ、②その直後にクラウドサービスの政府調達に係る認証制度を導入
- 日本では、2018年6月にクラウド・バイ・デフォルト原則を採用したところ、安全性評価の仕組みの検討が必要

	クラウド利用の方針	政府のクラウド認証制度	主な関連機関
	<b>2010年</b> 「25 POINT IMPLEMENTATION PLAN TO REFORM FEDERAL INFORMATION TECHNOLOGY MANAGEMENT」 →クラウドファースト(cloud first)	<b>2011年～</b> Federal Risk and Authorization Management Program 	General Services Administration （※独立政府機関） 
	<b>2014年</b> 「Australian Government Cloud Computing Policy」 →クラウドファースト(cloud first)	<b>2014年～</b> Information Security Registered Assessors Program 	Australian Signals Directorate （※防衛省管轄） 
	<b>2011年</b> 「Government Cloud Strategy」 →クラウドファースト(a public cloud solution first policy)	<b>2013年～</b> G-Cloud framework	Government Digital Services （※内閣府管轄） 
	<b>2011年</b> 「e-Government masterplan 2011-2015」 →政府プライベートクラウドの構築、移行（G-Cloud）	<b>2013年～</b> Multi-Tier Cloud Security（MTCS:SS584）	Infocomm Media Development Authority （※情報通信省管轄） 
	<b>2018年</b> 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」 →クラウド・バイ・デフォルト	<div style="border: 2px dashed red; padding: 10px; display: inline-block;"> <b>存在せず ※</b>  <b>（各種基準やガイドラインのみ）</b>  <small>※民間による認証制度は存在するが、政府が統一的に見る仕組みは存在しない</small> </div>	<b>存在せず</b> <div style="border: 1px solid red; padding: 5px; display: inline-block;"> IT室が助言し、  各省庁が独自に調達 </div>

# クラウドサービスの安全性評価に関する検討会におけるスコープ

- ①基準活用の前提となる情報・情報システムのクラス分けに関する議論と、  
②クラウド調達基準等に関する議論を行う
- 上記に加えて検討すべき事項については、継続的な検討事項として項目整理を行う



# (3) 国際社会の平和・安定及び我が国の安全保障への寄与

## 1. 自由、公正かつ安全なサイバー空間の堅持

## 2. 我が国の防御力・抑止力・ 状況把握力の強化

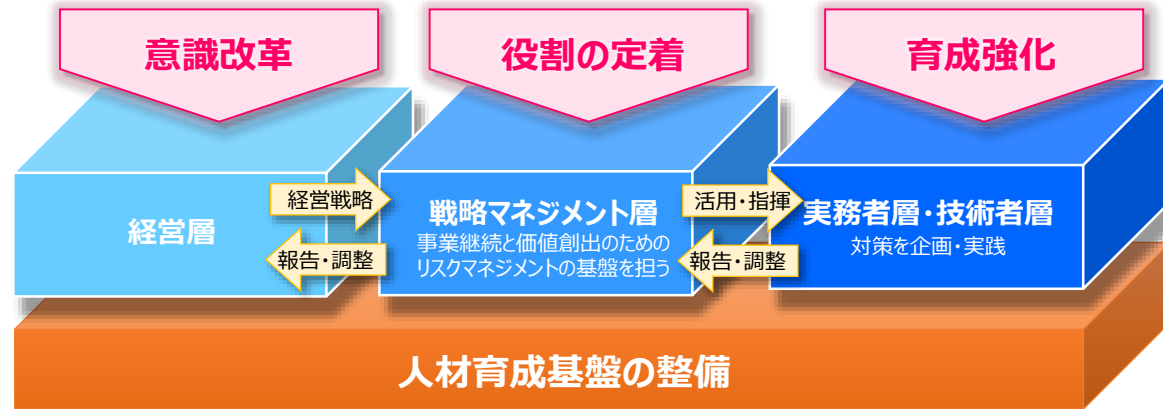
## 3. 国際協力・連携



# (4)サイバーセキュリティに関する共通基盤的な取組の推進

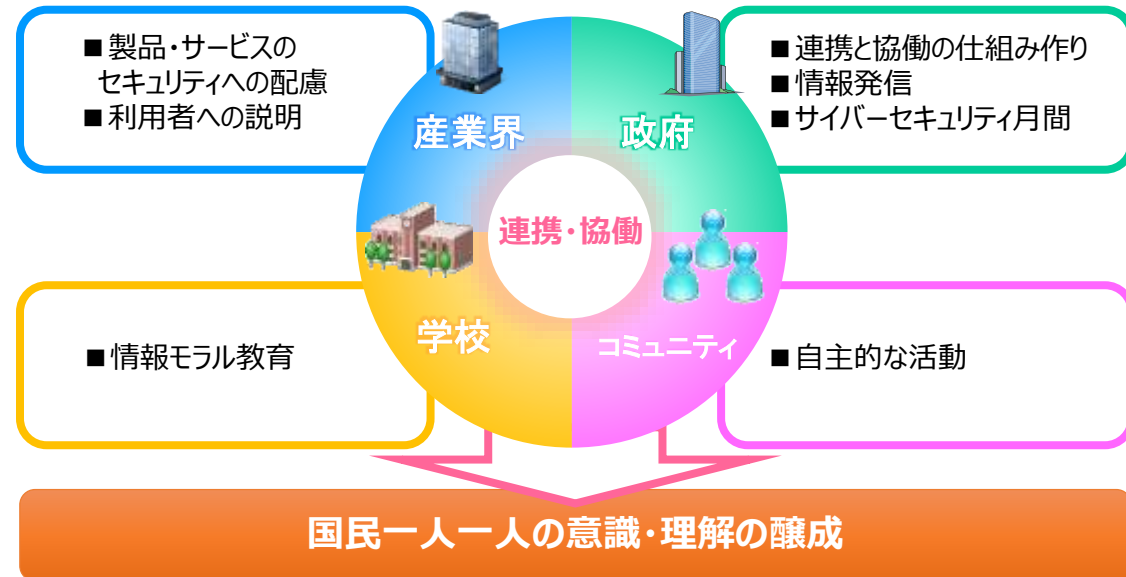
## 1. 人材育成・確保

「戦略マネジメント層」の育成・定着  
実務者層・技術者層の育成  
人材育成基盤の整備、国際連携の推進



## 2. 研究開発の推進

実践的な研究開発の推進  
(検知・防御等の能力向上、不正プログラム等の技術的検証を行うための体制整備等)  
中長期的な技術・社会の進化を視野に入れた対応



## 3. 全員参加による協働

サイバーセキュリティの普及啓発に向けたアクションプランの策定とそれに基づく連携・協働  
「サイバーセキュリティ月間」などを通じた情報発信

# 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**の育成の例

- 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＞

## 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＞



- 次世代の経営人材を集中的に育成するプログラム(2018年9月開講)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11月から開始。

- 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**

### 対象人材像

- 現在CISOやその補佐を務めている方や、**戦略企画層の方**

- 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

### カリキュラム ・期間

- 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20名**程度を加え、**合計100名程度**を対象として開始予定



# サプライチェーンサイバーセキュリティの実現に必要な研究開発 (SIP第2期)

## A.信頼の創出・証明

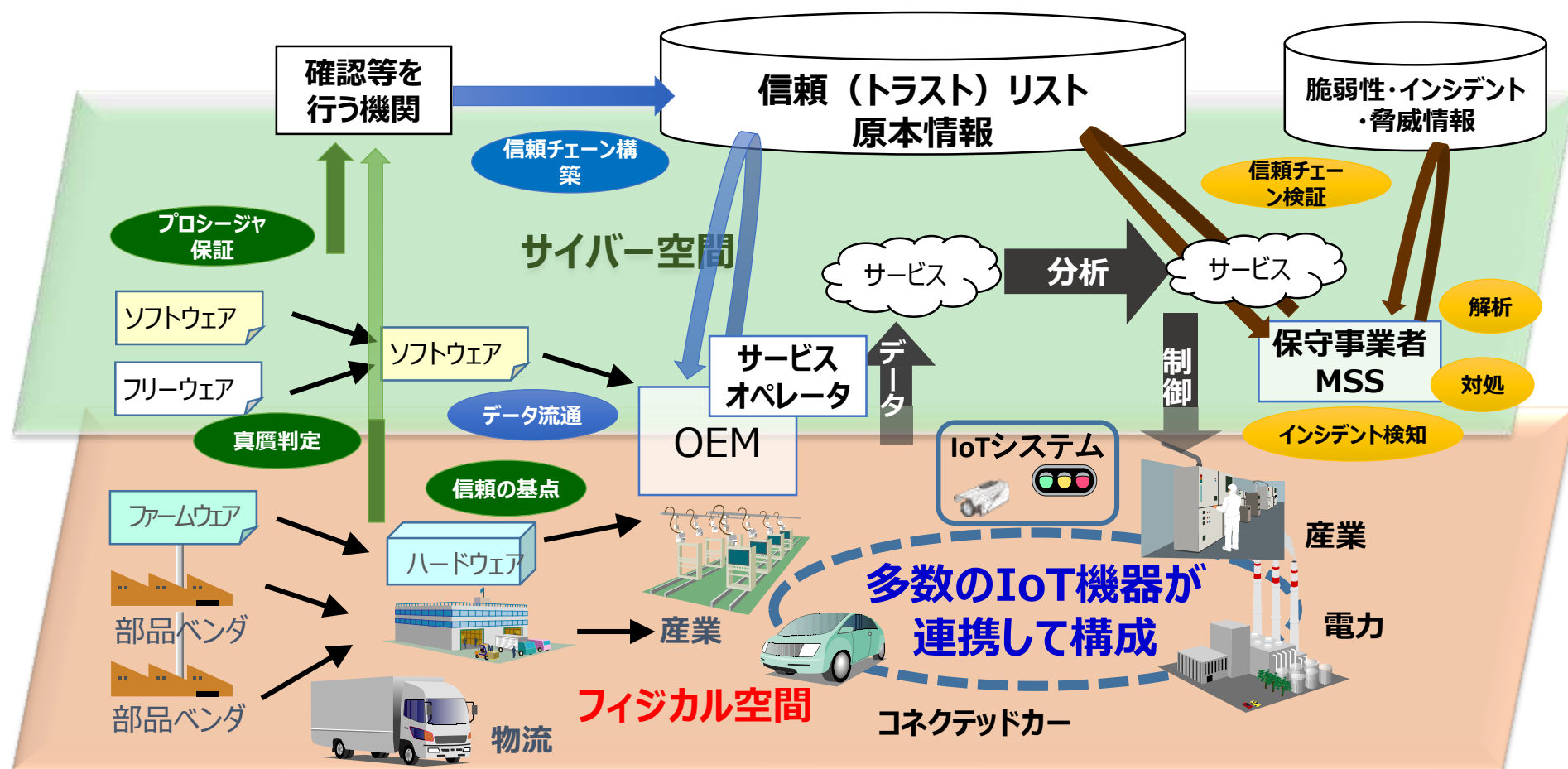
多様なIoTシステム・サービスやサプライチェーン全体のセキュリティ確保に必要な信頼の創出・証明技術

## B.信頼チェーンの構築・流通

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

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





MPOWER2018 講演資料 of McAfee

ご清聴ありがとうございました。

内閣官房内閣サイバーセキュリティセンター(NISC) 内閣審議官  
経済産業省 サイバーセキュリティ・情報化審議官  
三角 育生