

# 安全なIoTシステムの創出

2016年3月2日

内閣サイバーセキュリティセンター（NISC）

<http://www.nisc.go.jp/>

# 新たな「サイバーセキュリティ戦略」について（全体構成）



**1 サイバー空間に係る認識**

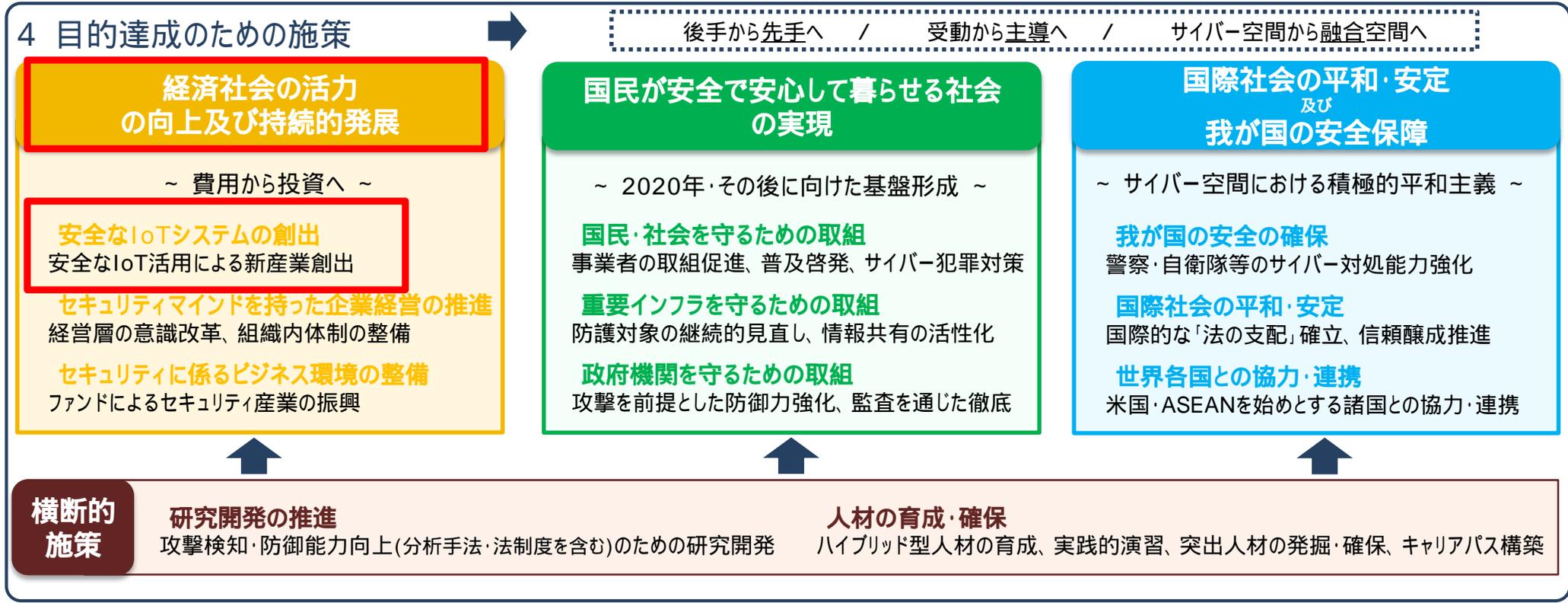
- サイバー空間は、「無限の価値を産むフロンティア」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに接続され、実空間とサイバー空間との融合が高度に深化した「接続融合情報社会（連融情報社会）」が到来同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

**2 目的**

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「**経済社会の活力の向上及び持続的発展**」、「**国民が安全で安心して暮らせる社会の実現**」、「**国際社会の平和・安定及び我が国の安全保障**」に寄与する。

**3 基本原則**

情報の自由な流通の確保      法の支配      開放性      自律性      多様な主体の連携



**5 推進体制**

- 官民及び関係省庁間の連携強化、オリンピック・パラリンピック東京大会等に向けた対応

## 5.1 経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

### サイバーセキュリティ戦略の「安全なIoTシステムの創出」の構成

#### 5.1.1 安全なIoTシステムの創出

安全なIoTシステムを活用した新規事業の振興

セキュリティ・バイ・デザインの考え方を推進する

IoTシステムのセキュリティに係る体系および体制の整備

IoTシステムに係る大規模な事業について

業態横断的に産学官の主体が適切に連携することが重要

IoTシステムのセキュリティに係る制度整備

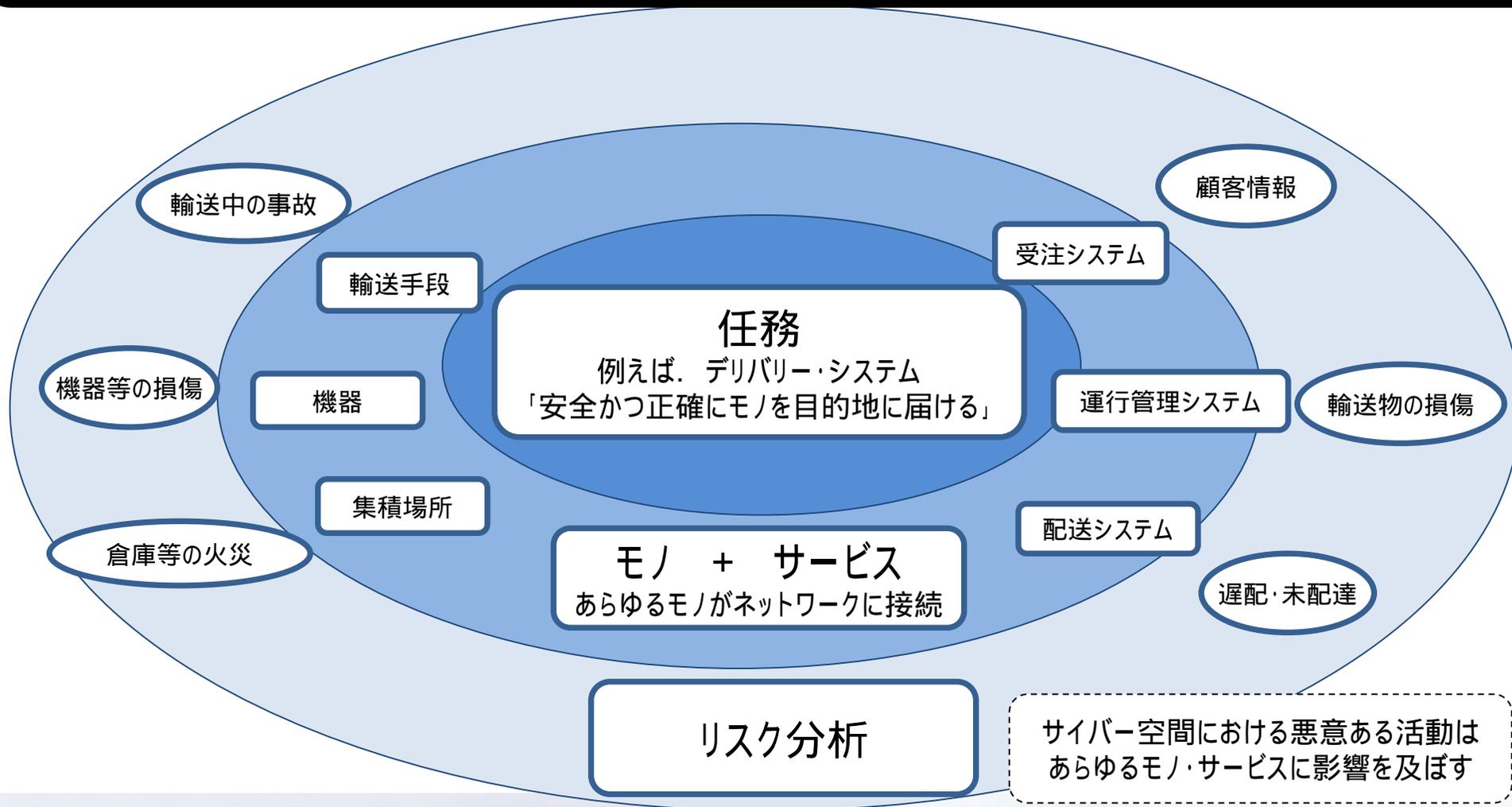
IoTシステムのセキュリティに係るガイドラインや基準の整備を行う

IoTシステムのセキュリティに係る技術開発・実証

「設計から廃棄までのライフサイクルが長い」、「処理能力に制限がある」といった、従来の情報通信機器とは異なるIoTシステムのセキュリティに係る技術開発・実証

# 任務保証の考え方について

業務責任者（任務責任者）がシステム責任者（資産責任者）と、機能やサービスを全うするという観点からリスクを分析し、協議し、残存リスクの情報も添えて経営者層に対し提供し総合的な判断を受ける「機能保証（任務保証）」の考え方に基づく取組が必要

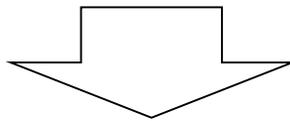
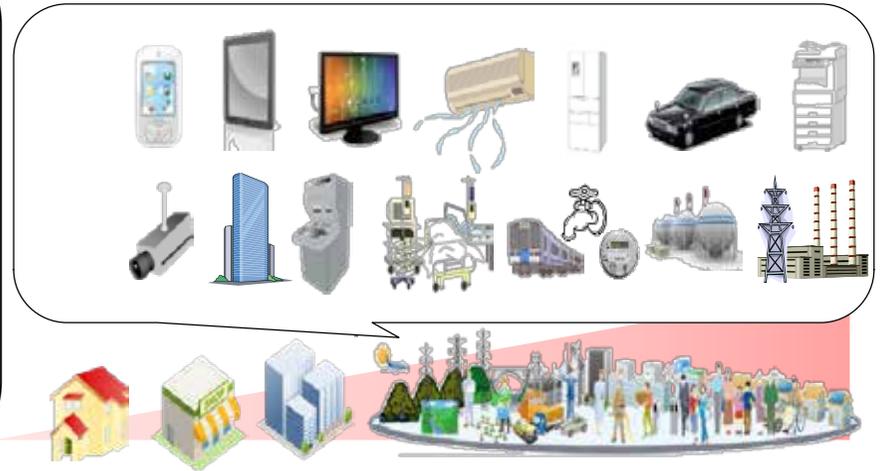


# セキュリティ品質の実現が企業価値に

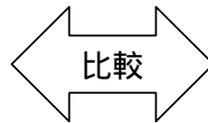
## 【IoTシステム】

- ・様々なモノがネットワークに接続（IoT）
- ・サイバー空間と実空間が融合
- ・IoTシステムを通じて新たなサービスを提供

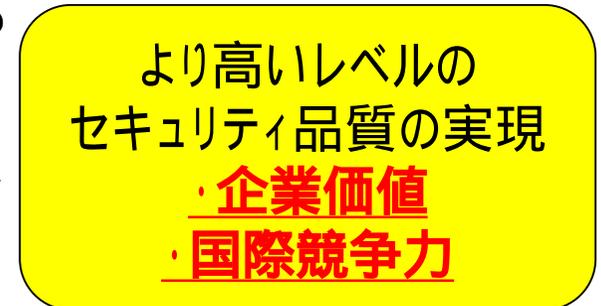
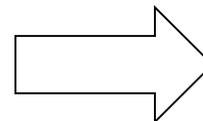
**セキュリティ品質（安全、セキュリティ）の保証が前提**



- ・IoTシステムのサービスの効用と比較してセキュリティリスクを許容し得る程度まで低減
- ・高いレベルのセキュリティ品質の実現が**企業価値や国際競争力の源泉に**



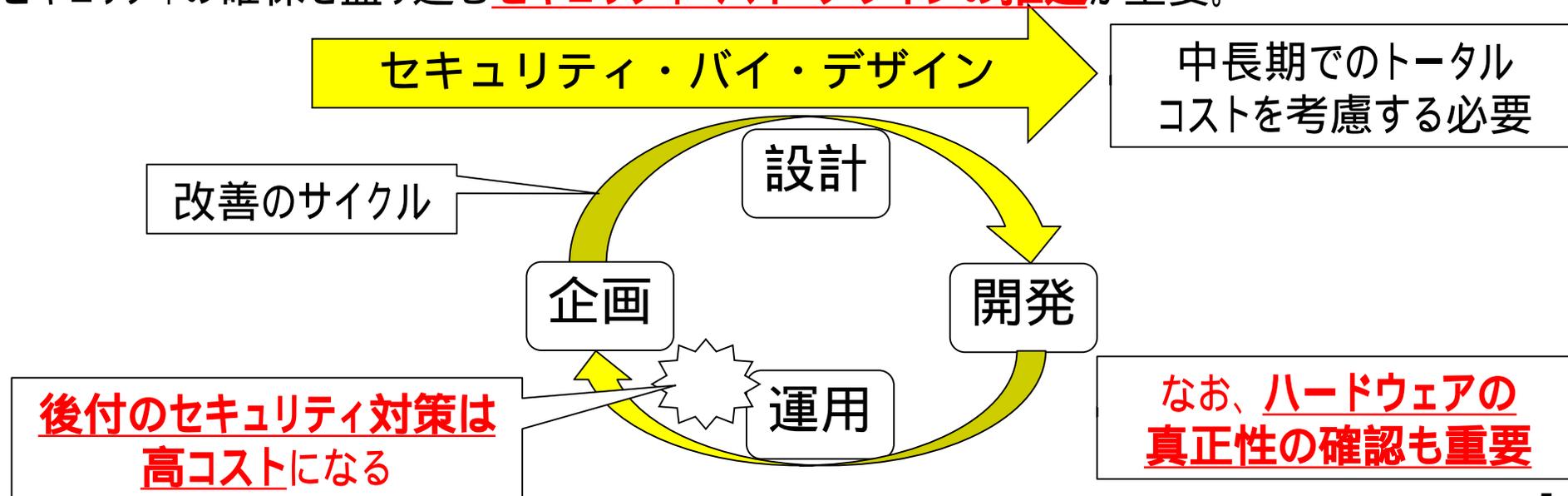
「費用」から  
「投資」へ



## ・IoTシステムの特徴（例）

- 設計から廃棄までの長いライフサイクル、処理能力の制限
- セキュリティ監視、パッチ適用・アップデートの仕組み、拡張性の考慮
- IoTシステムの実現には、多数の関係者が関与することとなり、サプライチェーン全体で適切な対策が講じられていることが求められる

・連携される既存システムを含めて、IoTシステム全体の企画・設計段階からセキュリティの確保を盛り込む**セキュリティ・バイ・デザインの推進**が重要。



# IoTシステムの階層構造とセキュリティ確保

サービス利用者



脅威例

利用者が期待するセキュリティ品質

対策例

なりすまし攻撃  
DoS攻撃・脆弱性攻撃

サービス

アクセス制御  
脆弱性対策

データ改ざん  
情報漏えい

プラットフォーム

アクセス制御  
ログ管理・監視

盗聴  
情報漏えい

ネットワーク

暗号化  
ネットワーク監視

データ改ざん  
信頼のおけない機器

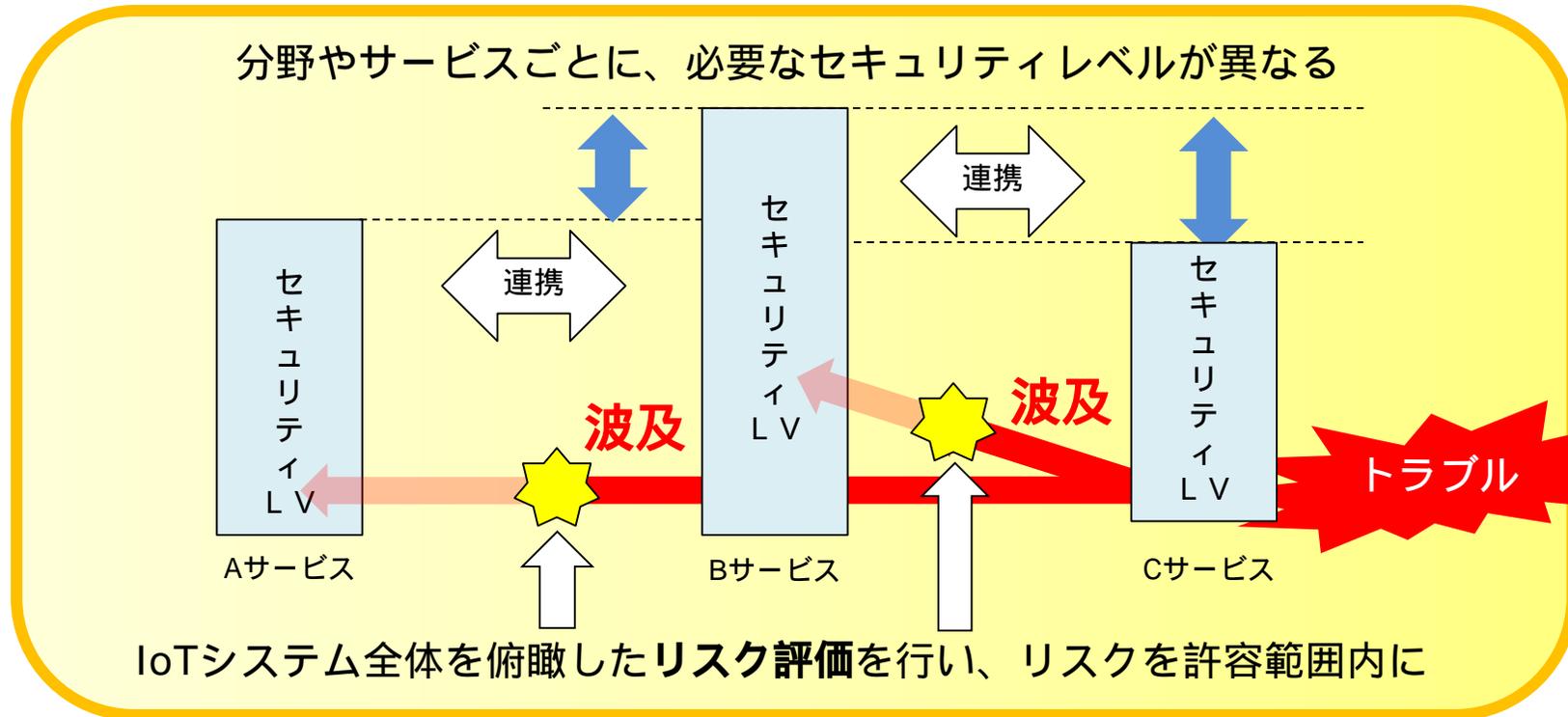
機器

ユーザ認証・暗号化  
HWの真正性検証

リアル空間とサイバー空間を結ぶ  
データの循環システム

任務達成の観点から  
ICT以外も含めて検討が必要

IoTシステムはデータの流通プラットフォーム。  
データとシステム全体のセキュリティ確保を行う必要がある。



レベルの異なるIoTシステムを相互連携させる場合は、  
残存リスクを客観的に評価し、  
許容範囲内に収めるための**リスク評価**が必要

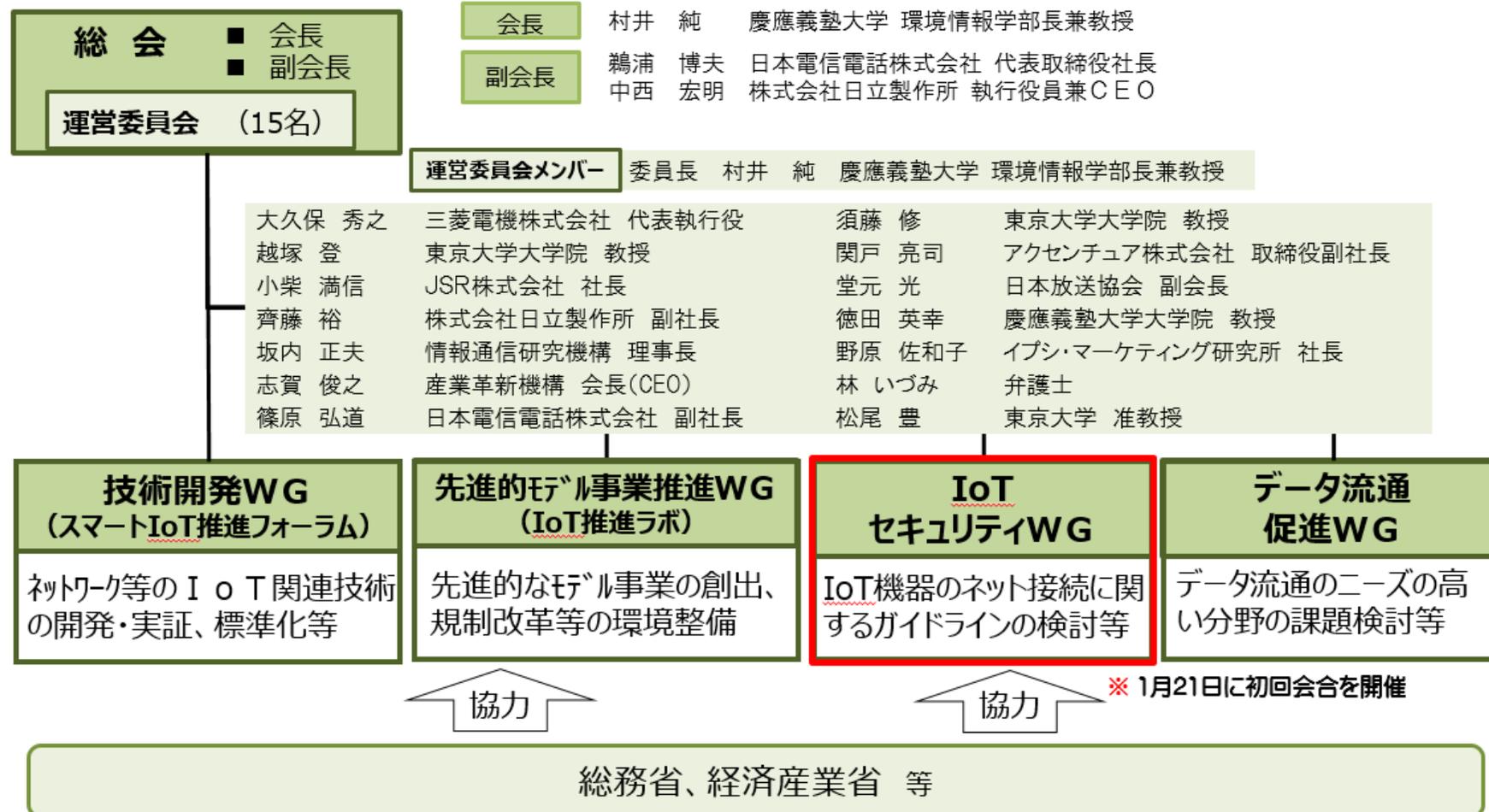
【まとめ】

安全なIoTシステムの創出にあたっては、以下のような取組・考え方が必要

- 任務保証の考え方に基づく取組
- セキュリティ品質の実現が企業価値
- セキュリティ・バイ・デザインの推進
- データとシステム全体のセキュリティ確保
- システム間の相互連携の際のリスク評価

## IoT推進コンソーシアム

- IoT/ビッグデータ/人工知能時代に対応し、企業・業種の枠を超えて産学官で利活用を促進するため、民主導の組織として「IoT推進コンソーシアム」を設立。(平成27年10月23日(金)に設立。)
- 技術開発、利活用、政策課題の解決に向けた提言等を実施。



## IoTセキュリティワーキンググループで検討するガイドラインの対象と内容について

IoTセキュリティワーキンググループでは、以下の議題について、サブワーキンググループを設置して検討を行う。

【議題1】IoT機器等の設計・製造・構成・管理に求められるセキュリティガイドライン

【議題2】IoT機器の通信ネットワークへの接続に係るセキュリティガイドライン

		供給者		利用者	
		機器メーカ	サービス提供者 (Sier、インストラ)	企業利用者	一般利用者
プラットフォーム (データセンタ、データ分析)		総務省ガイドライン      経産省ガイドライン <b>クラウドセキュリティガイドラインと連携</b>			
ネットワーク	インターネット	<b>【議題2】</b> IoTサービスの提供者・利用者が機器をネットワークに接続する際、遵守もしくは留意すべき事項		<b>【議題1】</b> セキュリティ対策を行う上での、組織的改善事項 (CSMSをベースに検討)	<b>【議題2】</b> 一般利用者がIoTサービス・機器を利用する際に最低限留意すべき事項
	狭域ネットワーク				
機器	通信機能	<b>【議題1】</b> IoT機器が満たすべきセキュリティ・セーフティ・リニアビリティに関して、設計・開発時に留意すべき推奨事項			
	ハードウェア				
	ソフトウェア(OS、ミドルウェア、アプリ等)				
	本来機能				