NISC

National center of Inoident readiness and
Strategy for Cybersecurity

資料5

安全なIoTシステムの創出

２０１６年３月１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）

NISC

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連接され、実空間とサイバー空間との融合が高度に深化した「**連接融合情報社会**（**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

① 情報の自由な流通の確保　② 法の支配　③ 開放性　④ 自律性　⑤ 多様な主体の連携

4 目的達成のための施策

①後手から**先手**へ　／　②受動から**主導**へ　／　③サイバー空間から**融合**空間へ

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

- **■安全なIoTシステムの創出**
  安全なIoT活用による新産業創出
- **■セキュリティマインドを持った企業経営の推進**
  経営層の意識改革、組織内体制の整備
- **■セキュリティに係るビジネス環境の整備**
  ファンドによるセキュリティ産業の振興

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

- **■国民・社会を守るための取組**
  事業者の取組促進、普及啓発、サイバー犯罪対策
- **■重要インフラを守るための取組**
  防護対象の継続的見直し、情報共有の活性化
- **■政府機関を守るための取組**
  攻撃を前提とした防御力強化、監査を通じた徹底

国際社会の平和・安定及び我が国の安全保障

～ サイバー空間における積極的平和主義 ～

- **■我が国の安全の確保**
  警察・自衛隊等のサイバー対処能力強化
- **■国際社会の平和・安定**
  国際的な「法の支配」確立、信頼醸成推進
- **■世界各国との協力・連携**
  米国・ASEANを始めとする諸国との協力・連携

横断的施策

- **■研究開発の推進**
  攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発
- **■人材の育成・確保**
  ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

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

① 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**

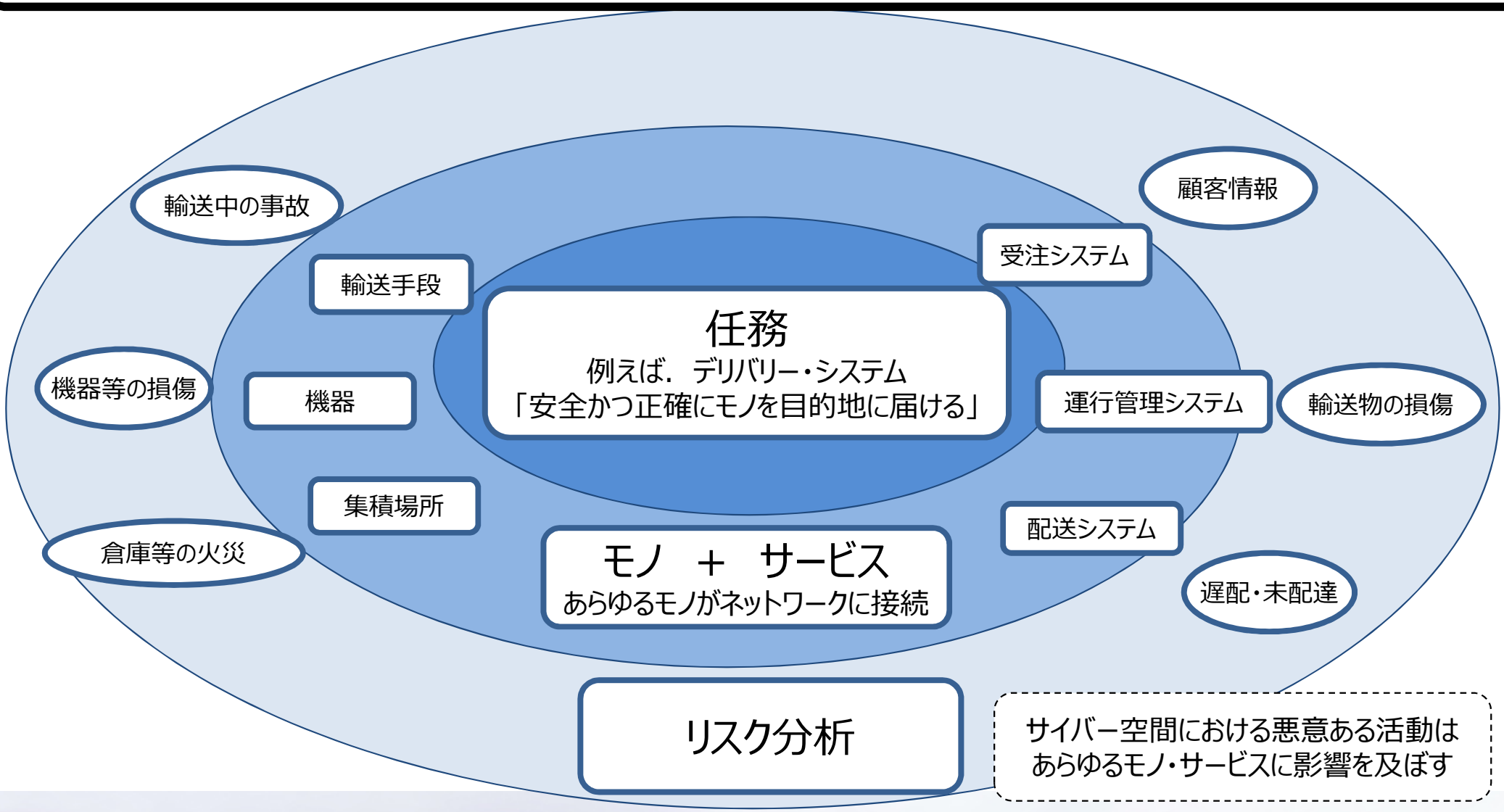
② IoTシステムのセキュリティに係る体系および体制の整備
⇒**ＩｏＴシステムに係る大規模な事業について業態横断的に産学官の主体が適切に連携することが重要**

③ 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**

④ 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**

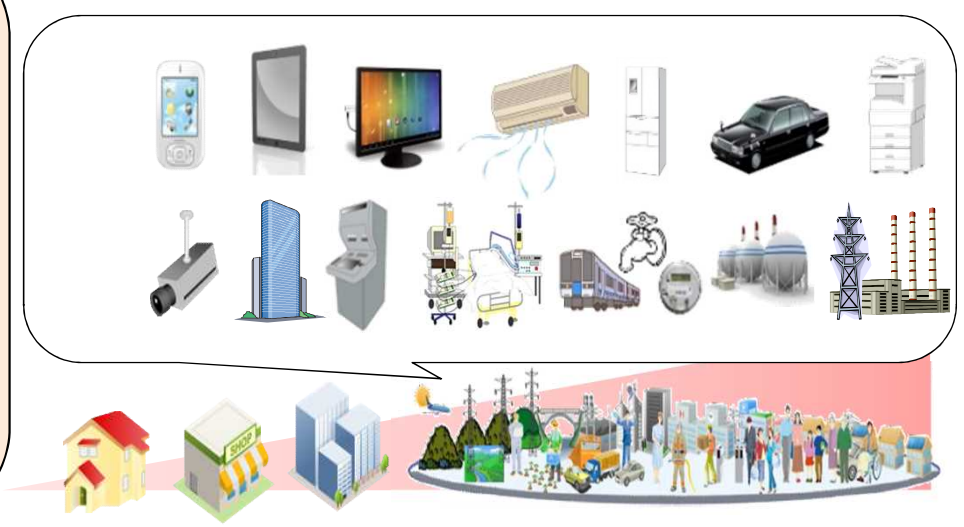
任務保証の考え方について

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

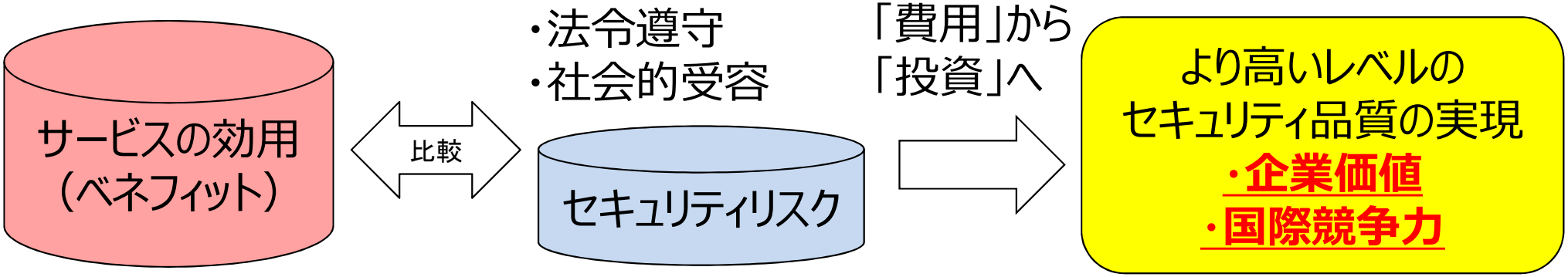


セキュリティ品質の実現が企業価値に

【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**



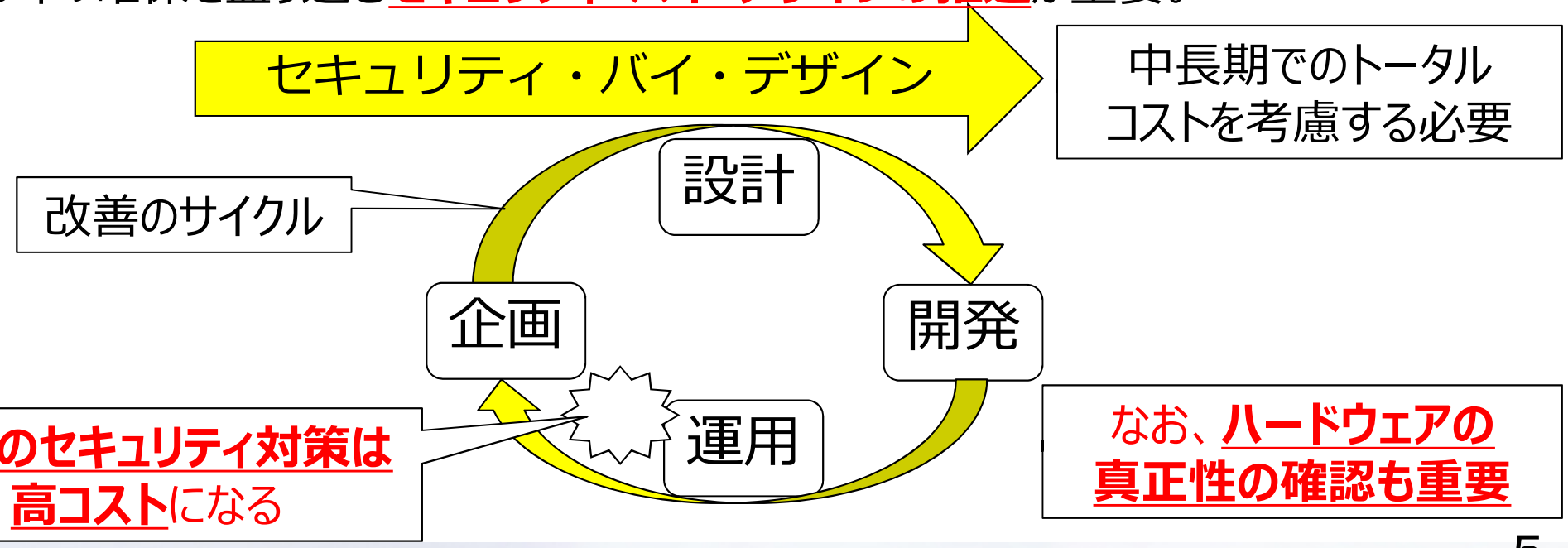
・IoTシステムのサービスの効用と比較してセキュリティリスクを許容し得る程度まで低減
・高いレベルのセキュリティ品質の実現が**企業価値や国際競争力の源泉に**



セキュリティ・バイ・デザイン

・IoTシステムの特徴（例）
　－設計から廃棄までの長いライフライクル、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

利用者が期待するセキュリティ品質

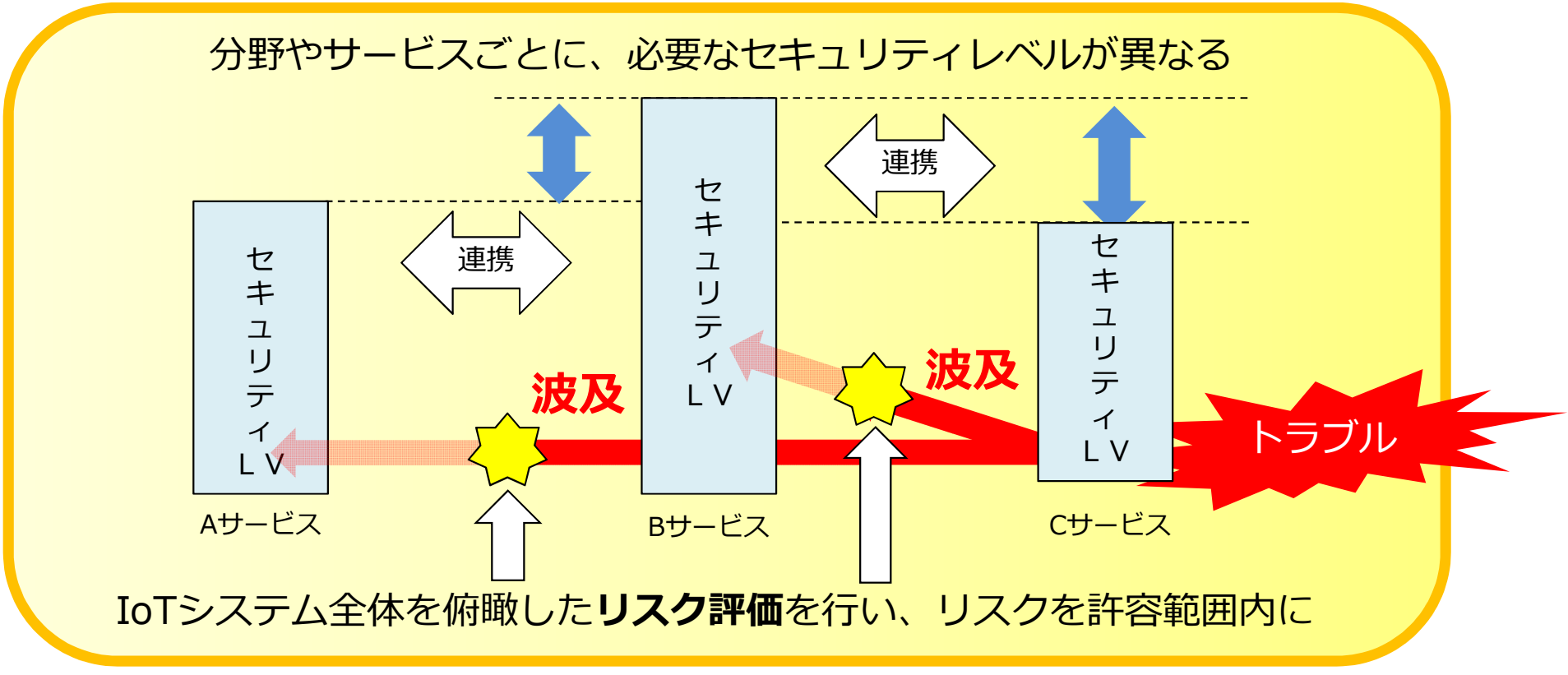
脅威例		対策例
なりすまし攻撃 DoS攻撃・脆弱性攻撃	サービス	アクセス制御 脆弱性対策
データ改ざん 情報漏えい	プラットフォーム	アクセス制御 ログ管理・監視
盗聴 情報漏えい	ネットワーク	暗号化 ネットワーク監視
データ改ざん 信頼のおけない機器	機器	ユーザ認証・暗号化 HWの真正性検証

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。

システム間の相互連携



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

安全なIoTシステムの創出

【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**

内閣サイバーセキュリティセンター

National center of Incident readiness and Strategy for Cybersecurity