資料２

# 関係省庁の取組状況について

金融庁　　金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅳ）について（資料２－１）

総務省　　実践的サイバー防御演習（CYDER）の開催について（資料２－２）

経済産業省　経済産業省におけるサイバーセキュリティ対策強化のための各種取組について（資料２－３）

# 金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅳ）について

資料２－１

## 金融分野のサイバーセキュリティを巡る状況

- 昨今、世界各国において、大規模なサイバー攻撃が発生しており、攻撃手法は一層高度化・複雑化
- 我が国においても、サイバー攻撃は大手金融機関のみならず、中小金融機関や暗号資産交換業者にまで拡大しており、実効性のあるサイバーセキュリティ対策は急務
- サイバー攻撃の脅威は金融システムの安定に影響を及ぼしかねない大きなリスクとなっており、金融業界全体のインシデント対応能力の更なる向上が不可欠

## これまでの演習の概要

- 過去3回演習を実施。2016年度は77先・延べ約900人、2017年度は101先・延べ約1,400人、2018年度は105先・延べ約1,400人が参加
- 多くの金融機関がコンチプラン等の見直しや社内外の情報連携強化に向けた対応を実施し、演習を通じて対応態勢を改善。一方、インシデント対応時における委託先との連携や顧客対応等が不十分、インシデント対応に必要な人員が確保できていないなどの課題が認められ、対応能力の向上を図っていく必要

## 金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅳ）

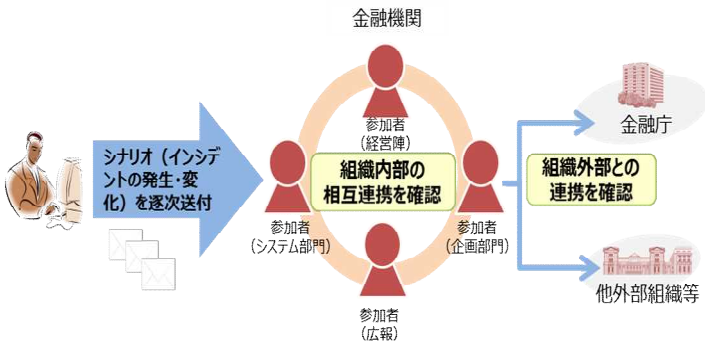
- ◆ 本年10月上旬、2020年東京オリパラ大会に向けた、大規模インシデントの発生に備え、中小金融機関のみならず大手金融機関等も参加して、**金融庁主催による4回目の「金融業界横断的なサイバーセキュリティ演習」（Delta Wall Ⅳ（注））を実施**

  （注）Delta Wall：サイバーセキュリティ対策のカギとなる「自助」、「共助」、「公助」の3つの視点（Delta）＋防御（Wall）
- ◆ 本演習の対象となっていなかった業態（資金移動業者、前払式手段発行者、監査法人等）**を追加**し、**約120社が参加**
- ◆ **2020年東京オリパラ大会の開催時におけるリスク等を想定したシナリオ**とし、預金取扱金融機関・証券会社等向けシナリオとその他業界向けシナリオで実施

### 演習の特徴

- □ インシデント発生時における金融機関内外の情報連携に係る対応体制や手順の確認を目的とした**机上演習**
- □ 経営層や多くの関係部署（システム部門、広報、企画部門等）が参加できるよう、**自職場参加方式**で実施（⇔会場集合方式）
- □ 民間の**専門家の知見や攻撃の実例分析等を参考**にしつつ、金融機関が陥りやすい弱点が浮き彫りとなり、**参加者が「気づき」を得る**ことができる内容
- □ 参加金融機関がPDCAサイクルを回しつつ、対応能力の向上を図れるよう、具体的な改善策を示すなど、**事後評価に力点**
- □ 本演習の結果は、参加金融機関以外にも**業界全体にフィードバック**

### 演習スキーム




【演習シナリオの概要】

**預金取扱金融機関、証券会社等向け**

- ✓ 東京2020大会開催期における、ネットワーク障害の発生及びホームページへのDDoS攻撃
- ✓ 他の金融機関との連携を担うネットワーク機器異常による決済システムの停止
- ✓ システム異常の原因及びDDoS攻撃の種類が判明

**その他業界（生損保、暗号資産交換業者、監査法人等）向け**

- ✓ 東京2020大会に関わるサイバー攻撃についての注意喚起
- ✓ ホームページへのDDoS攻撃、標的型メール攻撃
- ✓ DDoS攻撃の種類及びインシデントの発生原因が判明

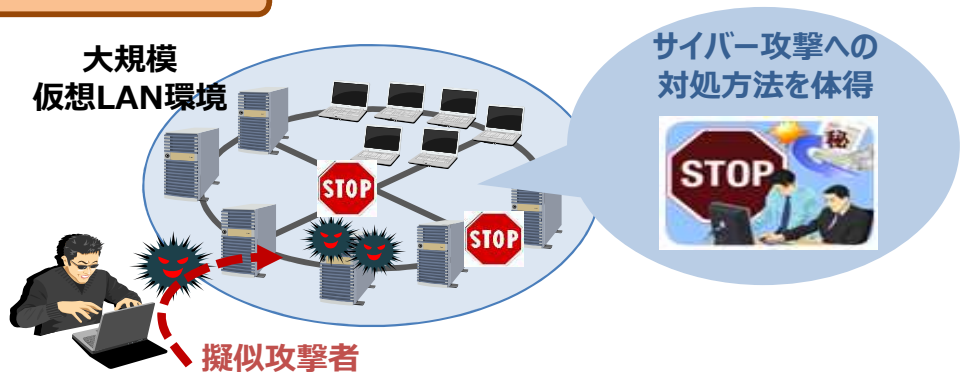
# 実践的サイバー防御演習（CYDER）

資料２－２

- 総務省は、情報通信研究機構(NICT)を通じて、**国の行政機関**、**地方公共団体**、**独立行政法人**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習**（CYDER）を実施。
  ※国の行政機関、地方公共団体、独立行政法人等は無料。重要インフラ事業者等の民間事業者は７万円／回の実費。
- 受講者は、**組織のネットワーク環境を模した大規模LAN環境下**で、**実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- 詳細情報や申込については、**https://cyder.nict.go.jp**

CYDER
Cyber Defense Exercise with Recurrence

## 演習のイメージ



**機材・データ**を使用して
**本番同様の作業**を実施

**グループワーク**での気付き共有

**専門**の**指導員**による補助

**報告書作成**も含めた一連作業

## 令和元年度の実施計画

| コース | 受講対象組織 | 開催地 | 主な開催時期 | 開催状況 |
|---|---|---|---|---|
| Aコース（初級） | （全組織共通） | 47都道府県 | 7～10月頃 | ほぼ実施済<br>（一部地域では申込受付） |
| B-1コース（中級） | 地方公共団体向け | 全国11地域 | 10～11月頃 | 開催中・**申込受付中** |
| B-2コース（中級） | 国の行政機関等、<br>重要インフラ事業者等 | 東京・大阪・名古屋 | 11～１月頃 | 開催中・**申込受付中** |

**令和２年度も実施予定**。インシデント対処能力の向上のために積極的な受講をお願いしたい。

経済産業省

資料２－３

# 経済産業省におけるサイバーセキュリティ対策強化のための各種取組について

経済産業省　商務情報政策局
サイバーセキュリティ課

１．「サイバー・フィジカル・セキュリティ対策フレームワーク」（CPSF）の具体化に係る分野横断的な議論を行うタスクフォースについて

２．情報処理の促進に関する法律の一部を改正する法律案の概要について

# 1．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

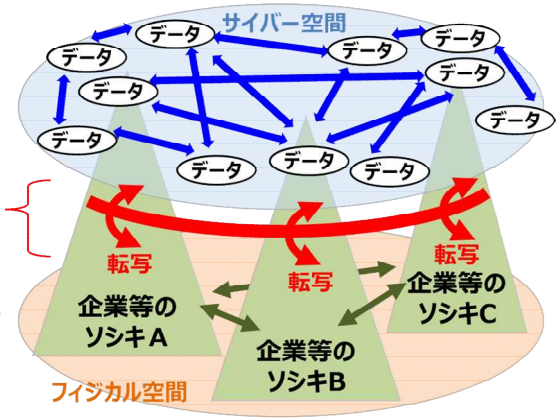
## ～ Society5.0 における新たなサプライチェーン（バリュークリエイションプロセス）の信頼性の確保に向けて ～

- サイバーとフィジカルが高度に融合する**「Society5.0」**では、**より柔軟で動的なサプライチェーンの構成が可能**になる一方、**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**に直面。
- そのため、Society5.0における**新たなリスクに対応するセキュリティ対策の全体像を整理した『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）Ver1.0』を2019年4月18日に公表**。
- 2度にわたるパブコメ（日本語、英語）に対して**国内外から多数のコメント**（合計：約800件、国内51・海外22の個人・組織）が寄せられ、**国際的認知も進展**。

### CPSFが示した『3層構造』

**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




**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

### CPSFが示した『6つの構成要素』

- **リスクベースの対策**につなげるため、動的に構成されるサプライチェーンの**構成要素を6つに整理**

| ソシキ | ヒト | モノ | データ | プロシージャ | システム |
|---|---|---|---|---|---|

### CPSFにおけるリスクマネジメントの考え方

（各層の）機能 → セキュリティインシデント → リスク源（構成要素ごとに整理） → 対策要件 → 対策例（3つにレベル分け）
- High-Advanced
- Advanced
- Basic

### CPSFと国際規格等との整合性確保

- **国際規格等との対応関係を記載**（第Ⅲ部、添付C及び添付D）
- **以下3つの主要な国際規格等から見た対応表も整理**（添付D）
  - NIST Cybersecurity Framework
  - NIST SP800-171
  - ISO/IEC 27001付属書A

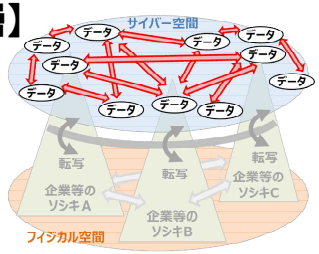
# 1．CPSFに基づく具体化・実装の推進

- CPSFの具体的適用に向け、『**データ区分に応じたセキュリティ対策**』、『**転写機能を持つ機器・システムに求められるセキュリティ対策**』、『**OSSを含むソフトウェアの管理手法等**』について、分野横断的な議論を行うタスクフォース（TF）を設置。
- **分野別サブワーキンググループ(SWG)の議論と連携し、CPSFの産業界における実装を推進。**

**実際の産業活動の内容**

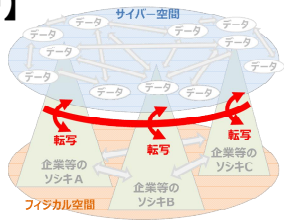
**具体的な対策手法やルールの明確化**

**【第3層】**




サイバー空間におけるつながり

**【第2層】**




フィジカル空間とサイバー空間のつながり

**データを介した連携を行う産業活動**
（分野間の連携 等）

**分野別の産業活動**
- ビル
- 電力
- 防衛
- 自動車
- スマートホーム 等

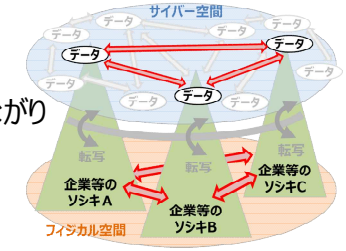
**規模別の産業活動**
- 大企業
- 中小企業 等

**データの信頼性**
（データの完全性、真正性等の確認　等）

**転写機能を持つ機器の信頼性の確認手法**
- 機器・システムのセキュリティ 等

**ソフトウェアの取扱に関するルール・管理手法**
- Software component transparency 等

**【第1層】**
企業間のつながり




**産業サイバーセキュリティ研究会WG 1**

標準モデル（CPSF）

- **ビルSWG**
- **電力SWG**
- **防衛産業SWG**
- **自動車産業SWG**
- **スマートホームSWG**
- **・・・**

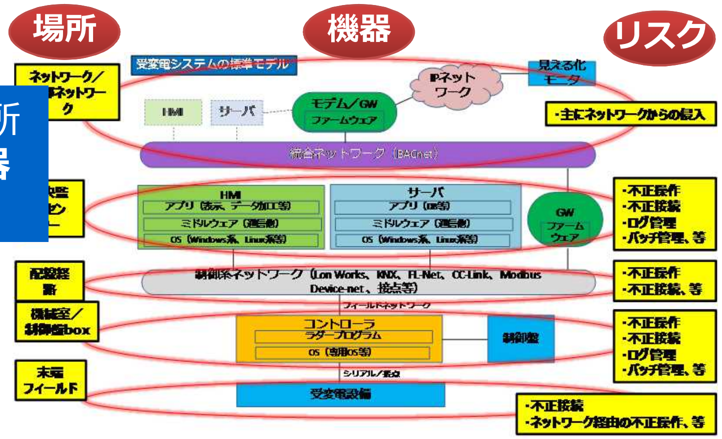
**分野横断SWG**

- **『第3層』TF (⇒ データ区分に応じて適切なセキュリティ対策要件 等)** 7/31第1回
- **ソフトウェア TF （⇒ OSSを含むソフトウェア管理手法 等)** 9/5 第1回
- **『第2層』TF (⇒ 機器毎のラベリング・認証の在り方、安全との一体化への対応 等)** 8/2 第1回

# 【参考】ビルSWG（座長：江崎 浩 東京大学 教授）

- 産業サイバーセキュリティ研究会WG1（制度・技術・標準化）の下の**ビルSWG（ビルオーナー～ベンダまで、ビル関連のステークホルダが参加）**において、ビルの管理・制御システムに係る各種サイバー攻撃のリスクと、それに対するサイバーセキュリティ対策を整理し、ビルに関わるステークホルダーが活用できる**ガイドラインを作成**。**2019年6月17日付で第1版を公開**。

- **場所→場所に置かれる機器→機器に想定されるリスク→対策要件→ライフサイクル別の対応策という流れで整理**




**場所**及びその場所に設置される**機器等**をリストアップ

| | | |
|---|---|---|
| **4.1 全体管理** | | |
| 1. | 構成情報／管理情報 | |
| 2. | バックアップデータ／事業継続 | |
| 3. | 会社／要員の管理 | |
| 4. | 体制構築等 | |
| **4.2 機器** | | |
| 1. | ネットワーク(クラウド、情報系NW、BACnet) | |
| | 10 | ネットワーク |
| | 11 | クラウドサーバ·Webサーバ |
| | 12 | 情報系端末 |
| | 13 | 外部接続用ネットワーク機器（FW、ルータ） |
| | 14 | ビルシステム間相互接続 |
| 2. | 防災センター（中央監視室） | |
| | 20 | 防災センター（中央監視室） |
| | 21 | HMI/HIM |
| | 22 | 保守用持ち込み端末 |
| | 23 | 統合NWにつながるネットワーク機器（FW、ルータ、SW） |
| | 24 | システム管理用サーバ（ビルシステム主装置） |
| 3. | 機械室／制御盤ボックス | |
| | 30 | 機械室 |
| | 31 | コントローラ（DDC、PLC等） |
| | 32 | ネットワーク機器（FW、ルータ、SW） |
| | 33 | ゲートウェイ機器 |
| | 34 | 各種制御盤・分電盤 |
| 4. | 配線経路（MDF室、EPS、天井裏ラック） | |
| | 40 | MDF室／EPS／天井裏ラック |
| | 41 | 内部に置かれたネットワーク機器（SW類） |
| 5. | 末端装置が置かれる場所 | |
| | 50 | 末端装置 |

| | セキュリティインシデント | リスク源 | セキュリティポリシー |
|---|---|---|---|
| 1．構成情報／管理情報 | | | |
| (1) | ビルシステムへの被害発生時に、被害確認が遅れ、復旧作業の支障となる。 | ビルの構成情報が最新状態に管理できておらず、機器の最新の接続関係が把握できない。 | ・構築システム構成図（設計時）に対し、引き渡し時のシステム構成図を竣工引き渡し書類として作成するように"設計仕様"に加える。<br>・システム全体構成（外部接続先を含む）の最新状態を常に把握できるようにする。 |
| 2．バックアップデータ／事業継続 | | | |
| (1) | 適切なバックアップデータがなく、ビルシステムへの被害発生時に復旧作業の支障となる。 | バックアップが取られていない、またはバックアップの範囲や対[illegible]が適切でない。 | ・システムバックアップ方法を運用側と確認の上でバックアップ方法を設計時に仕様を組み込む。<br>・管理ポイントや運転スケジュール等、システムを運用するにあたって必要なデータについては、バックアップを取得する機能を具備する。 |
| (2) | システムの脆弱性をついた攻撃を受ける。 | 脆弱性についての認識が不十[illegible]で脆弱性が残ったままの状態になっている。 | ・既知の脆弱性に対して必要な対策（パッ[illegible]理する。<br>・ただし、他機器および他システムの正常稼動については、担保しなければならない。 |
| 3．会社／要員の管理 | | | |
| (1) | ビルシステムへの被害発生時に、迅速な対応ができず、被害が拡大する。 | ビル管理会社においてセキュリティへの意識醸成、要員教育が十分ではなく、事前対策や対応準備が出来ていない。 | ・システム構築要件に教育訓練について明記する。 |
| (2) | ビルシステムが内部作業員等から攻撃を受ける。 | 作業員等の身元確認や行動監視が不十分で、内部攻撃者が紛れることや攻撃を行うことを防ぐことが出来ていない。 | ・システムの構築・施工・保守にあたって、作業員等の身元確認や行動確認についての要件を明記する。 |
| 4．体制構築等 | | | |
| (1) | 攻撃等への対応が効果的に出来ず、被害が拡大する。 | 十分なリスクアセスメントが出来ていないため、リスク対応の運用計画や体制が十分なレベルで構築できていない。 | ・リスクアセスメントを実施し、その結果を基に監理監査面からの「運用する管理体系」などを運用計画として定義・整備する。 |

ビルシステムの**ライフサイクルの各フェーズ毎に対策**を展開

0.全体管理

| No. | セキュリティポリシー | No. | 設計・仕様(Planning/Procurement)： | No. | 建設(Building) | No. | 竣工検査(Completion inspection) | No. | 運用(Operation) | No. | 改修・廃棄(Reforming) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 00.構成情報／管理情報 | | | | | | | | | | | |
| 001.システムの構成情報が最新になっておらず、機器の接続関係等が把握できないため、被害の確認や復旧のための作業の支障となる。 | | | | | | | | | | | |
| 0011.最新の構成情報の管理が出来ていない。管理運用会社 | | | | | | | | | | | |
| 0011-P1 | 構築システム構成図（設計時）に対し、引き渡し時のシステム構成図を竣工引き渡し書類として作成するように"設計仕様"に加える。システム構成図については※※を参照 システム全体構成の最新状態が常に把握できる様にすること | 0011-P1M1 | 設計図書の特記仕様にシステム構成図を記載する システム全体構成の更新履歴、管理設備毎の稼動履歴等、FMSを利用した運用管理を行う仕様を明記する | 0011-P1M1-B1 | 納品されるシステム構成品（設備）が設計仕様（同等品でも）と異なる場合、その内容を明記してシステム構成図を作成する | 0011-P1M1-B1-C1 | システム構成図と現場機器が合致しているかの確認を行い、引き渡す | 0011-P1M1-B1-C1-O1 | 定期的なシステム構成図の確認を行い外部に漏れないようFMSで管理する | 0011-P1M1-B1-C1-O1-R1 | システム構成が更新や改修時に変更があった部分を最新の情報にシステム構成図を改め、古い構成図は廃棄処理を確認する。 |
| 01.バックアップデータ／事業継続 | | | | | | | | | | | |
| 011.システムのバックアップ等が適切に取得・管理されて[illegible]、被害時の復旧のための作業の支障となる。 | | | | | | | | | | | |
| 0111.定期的なバックアップが取られていない。 | | | | | | | | | | | |
| 0111-P1 | システムバックアップ方法を運用側と確認の上でバックアップ方法を設計時に仕様を組み込む 管理ポイントや運転スケジュール等、システムを運用するにあたって必要がデータについては、定期的にバックアップを取得する機能を有すること | [illegible] | [illegible] | | | 0111-P1M1-C1 | [illegible] | 0111-P1M1-C1-O1 | [illegible] | 0111-P1M1-C1-O1-R1 | [illegible] |
| 012.脆弱性情報等を定期的にチェックしておらず、必要な[illegible]措置をとっていないために、脆弱性を突いた攻撃にあう可能性がある。 | | | | | | | | | | | |
| 0121.適切なアップデート／パ[illegible] | | | | | | | | | | | |
| 0121-P1 | 導入するシステム機器[illegible] パッチの状態を[illegible] ただし他機器[illegible] は、担保[illegible] | 0121-P1M1 | リスクアセスメント実施を踏まえた設計・仕様策定を行い、設計図書の特記仕様にシステムの脆弱性対策について記載する システム全体の接続性を担保した上での、最新のアップデート／パッチが適用されている機器であることを仕様に明記する | | | 0121-P1M1-C1 | システム全体の接続性を担保した上での、最新のアップデート／パッチが適用されている機器であることを確認し引き渡す | 0121-P1M1-C1-O1 | JDCC-19／建物設備システムのセキュリティ脆弱性に関する情報を定期的に入手し、必要に応じてセキュリティパッチを適用すること | | |
| 02.会社／要[illegible] | | | | | | | | | | | |
| 021.[illegible]セキュリティ意識が醸成されておらず、事前のセキュリティ対策が十分に取られず、攻撃を受けた際の対応も遅れる可能性がある。 | | | | | | | | | | | |
| [illegible]セキュリティ意識が低い。 | | | | | | | | | | | |
| [illegible] | システム構築要件に教育訓練について明記する | 0211-P1M1 | リスクアセスメント実施を踏まえた設計・仕様策定を行い、発注主側の運転管理者教育について、明記する。（教育人数・教育テキスト・教育期間・セキュリティー関連教育を含む・教育場所を明記） | | | 0211-P1M1-C1 | 竣工引き渡し時にシステム操作説明を行う際、合わせてセキュリティについても教育を実施すること。 | 0211-P1M1-C1-O1 | BAシステムの運用会社選定（委託先選定）にあたって、その責任範囲を発注要件に組み込む。 管理・運用組織への継続的セキュリティ啓発／監査を実施する ・BAシステム引渡し前に運転要員相当数に十分な操作訓練期間を設ける ・BAシステムの運転権限者の登録情報を発注者と共有できる ・自社（運用会社）の定められた人以外の操作者に対し（保守作業者など）定めた手順を確認し記録する ・発注主に対し運転記録・保管記録類の定期報告要件がある（日常正常時・不具合対応時） | | |
| 022.作業員に内部攻撃者が紛れることを防げず、内部からの攻撃を受ける可能性がある。 | | | | | | | | | | | |
| 0221.作業員の身元管理や行動確認が出来ていない。 | | | | | | | | | | | |
| 0221-P1 | システムの構築・施工に関する要件を明記すると。 | 0221-P1M1 | リスクアセスメント実施を踏まえた設計・仕様策定を行い、システム構築要件を明示する。 就労届や作業員名簿にて、作業員の身元確認を実施すること。また作業実施時は必ず元請社員の立会いを行うこ | 0221-P1M1-B1 | 作業場所が施錠可能な状況から機器の搬入据付を行なう。 やむを得ず、搬入する場合、事前開封が行なわれたかの有無が確認できる梱包をして保管 就労届や作業員名簿にて、作業員の身元確認を実施すること。また作業実施時は必ず元請社員の立会いを行うこ 定期的な現場巡回を行い、不審者や不審行動（不要な撮影等）などを取り締まる | 0221-P1M1-B1-C1 | 元請け社員以外の作業箇所記録を保管し、発注主に報告可能な状態とする | 0221-P1M1-B1-C1-O1 | 保守作業のための来館者は事前届出を行い、入館時に身元確認をし作業域への入室を許可する | | |
| 03.体制構築等 | | | | | | | | | | | |
| 031.設計・構築において、技術者のセキュリティへの知識が不足しており、十分にセキュアなシステムを構築出来ない。 | | | | | | | | | | | |
| 0311.十分なセキュリティ知識と技術をもった設計者が設計をしていない。 | | | | | | | | | | | |
| 0311-P1 | セキュリティ知識を持った有識者の元で設計を実施する体制を整えること。 | 0311-P1M1 | リスクアセスメント実施を踏まえた設計・仕様策定を行い、設計過程で、セキュリティ知識を持った有識者の監修を受けること | | | 0311-P1M1-C1 | 構築後セキュリティ知識を持った有識者の監修を受け、証明を得ること | 0311-P1M1-C1-O1 | 竣工引き渡し時の監査の内容に変化がないか定期的な確認を行う | | |
| 032.作業員のセキュリティ教育が十分でなく、初期対応等に遅れが生じる。 | | | | | | | | | | | |
| 0321.作業員1人1人のセキュリティ意識が低い。 | | | | | | | | | | | |
| 0321-P1 | 入場者教育実施時にセキュリティ教育を実施すること。 | 0321-P1M1 | 設計要件に見積漏れが無いように入場者教育実施時にセキュリティ教育を実施することを明記。 | 0321-P1M1-B1 | 就労届や作業員名簿にて、作業員の身元確認を実施すること また作業実施時は必ず元請社員の立会いを行うこと 定期的な現場巡回を行い、不審者や不審行動（不要な撮影等）などを取り締まる | 0321-P1M1-C1 | 機器設定情報等のドキュメント類については、竣工時に全て回収する | 0321-P1M1-C1-O1 | 保守員の教育を徹底し、訓練を実施し防御のレベルを上げる | | |

**場所・機器別**の想定される**インシデント**と**リスク源**を整理し、その**対策をポリシーレベル**で整理

# 【参考】スマートホームSWG（JEITA スマートホームサイバーセキュリティWG）

- Society5.0の実現を目指し、IT・エレクトロニクス企業のみならず、人々の暮らしに関わる様々なメンバーが、それぞれの知見を結集して、スマートホームのセキュリティ対策の検討を実施。
- マネジメント不在といった**スマートホーム特有の脅威や、製品安全の観点も含めたスマートホーム分野のセキュリティガイドラインを整備する**とともに、運用のあり方についてまとめていく。

＜構成員＞　企業）家電・AV関連、IT・通信関連、車載関連、住宅設備・サービス関連

団体・機関）住宅（戸建て／マンション）・住宅設備分野、電機・通信分野、医療分野、研究機関

経済産業省

**サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）**

**フレームワークと整合**

①三層構造アプローチ
②リスクベース
③国際標準との調和

＋

**スマートホーム特有の脅威を加味**

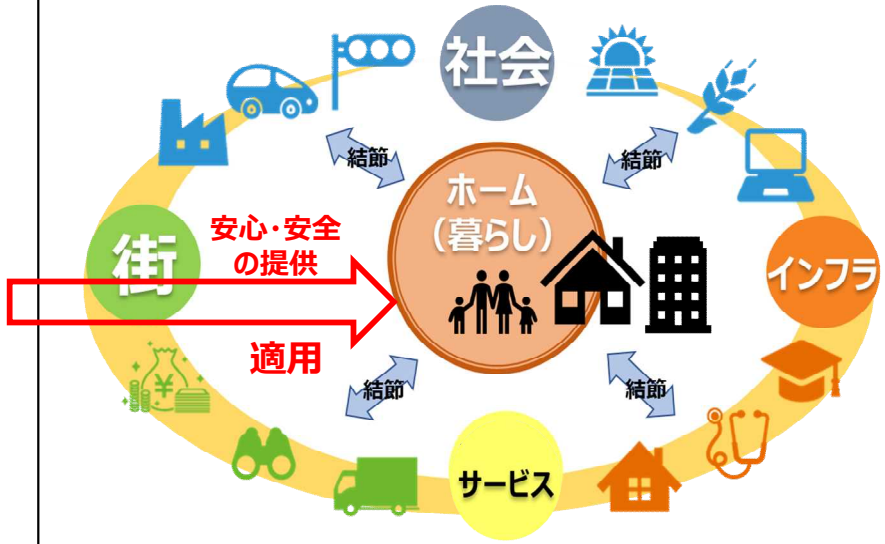
①膨大な対象
②マネジメント不在
③利用者による想定外の事象

JEITA 一般社団法人 電子情報技術産業協会

**スマートホーム実現に向けた サイバーフィジカルセキュリティ対策ガイドライン**

- 定義と説明
  - スマートホームの定義
  - スマートホームを取り巻く環境や状況の変化
  - サイバー攻撃の事例
- スマートホームの住まい手である生活者に向けて
  - 機器やサービスの導入時のリスク
  - 機器やサービスの利用時のリスク
  - 機器やサービスの解約時・機器廃棄時のリスク
  - 利用シーンごとの対策と確認内容の例
- スマートホームを構成する機器やサービスの開発者、提供者に向けて
  - 製品とサービスのライフサイクル全体におけるセキュリティレベルの維持
    - 開発時に考慮を必要とする内容
    - 利用中の製品とサービスにおけるリスクと対策
    - サービス解約や機器廃棄時のリスクとその対策
  - 製品とサービスのサポート停止以降のセキュリティレベルの維持
- ユースケース
- リスク・対策・セキュリティ要件の例
- 国際規格等の各種規格との対応

**2019年度内の策定を目指す**

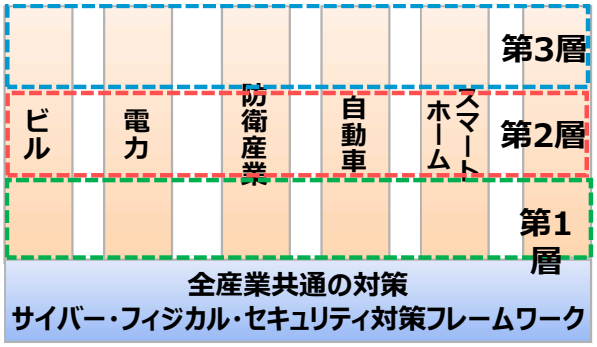



- **Society5.0社会の基盤となるスマートホーム**は、社会インフラや様々な産業、サービスが結節した、住まい手中心のバリュークリエイションプロセスにより構成
- 住まい手の**セキュリティをバリュークリエイションプロセス全体で確保**

# 【参考】『第2層』タスクフォースの検討の方向

- 本タスクフォースでは、諸外国の動向も踏まえながら、サイバー・フィジカル間の**転写機能を持つ機器について、ユーザのリスクや社会に与える被害を考慮した信頼性確保に求められる要件**を整理。
- その整理を踏まえた上で、分野別SWGの検討内容に横串を通すべく、**業界の自主活動を含めた自己適合宣言・認証等の確認の在り方等**を検討するとともに、**産業保安・製品安全も考慮したセキュリティ対策の在り方**について検討を行う。

**分野別ガイドラインにおいて機能の要求を明確化（各SWG）**

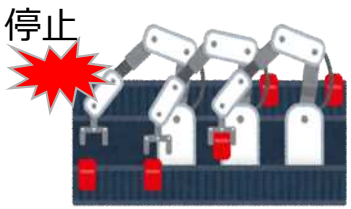



**タスクフォースにおける検討内容イメージ**

**① 業界の自主活動を含めた自己適合宣言・認証等の確認の在り方等の検討**

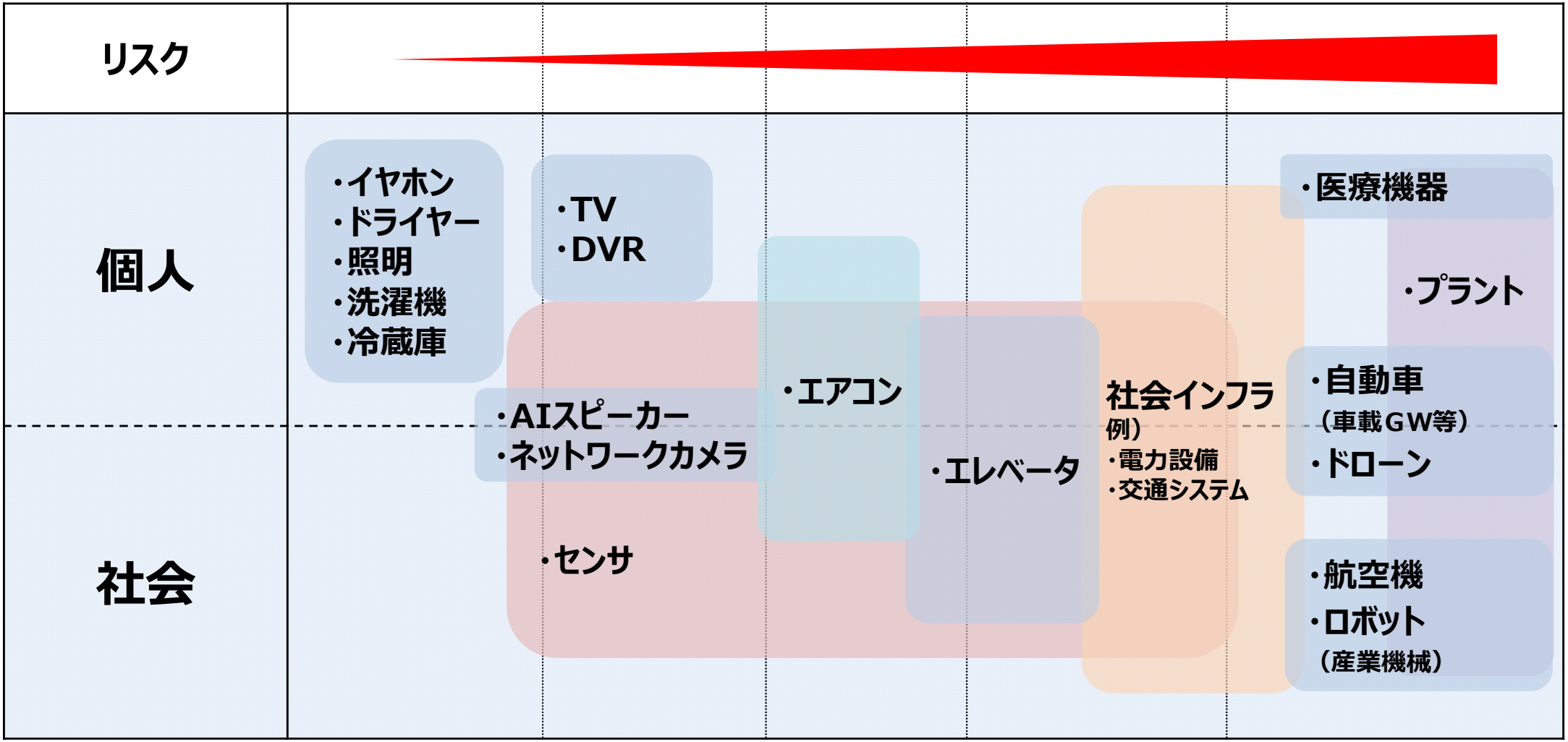
※ 特に高いセキュリティを求める機器に対する要件等を検討

**② サイバーリスクの安全への影響の増大への対応**

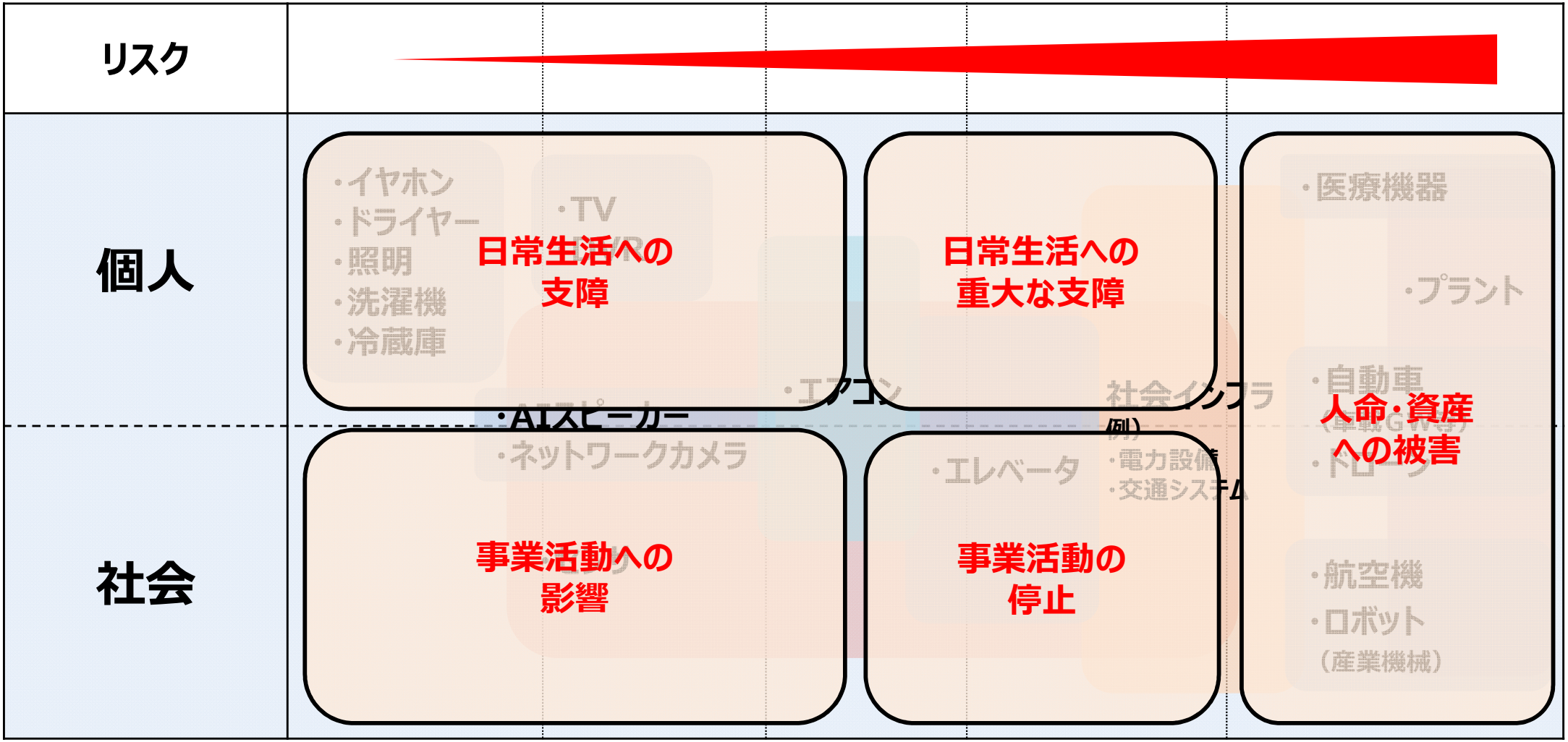



※ 安全も考慮に入れたセキュリティ対策等について検討

# 【参考】サイバー・フィジカル間をつなげる機器に潜むリスクのイメージ



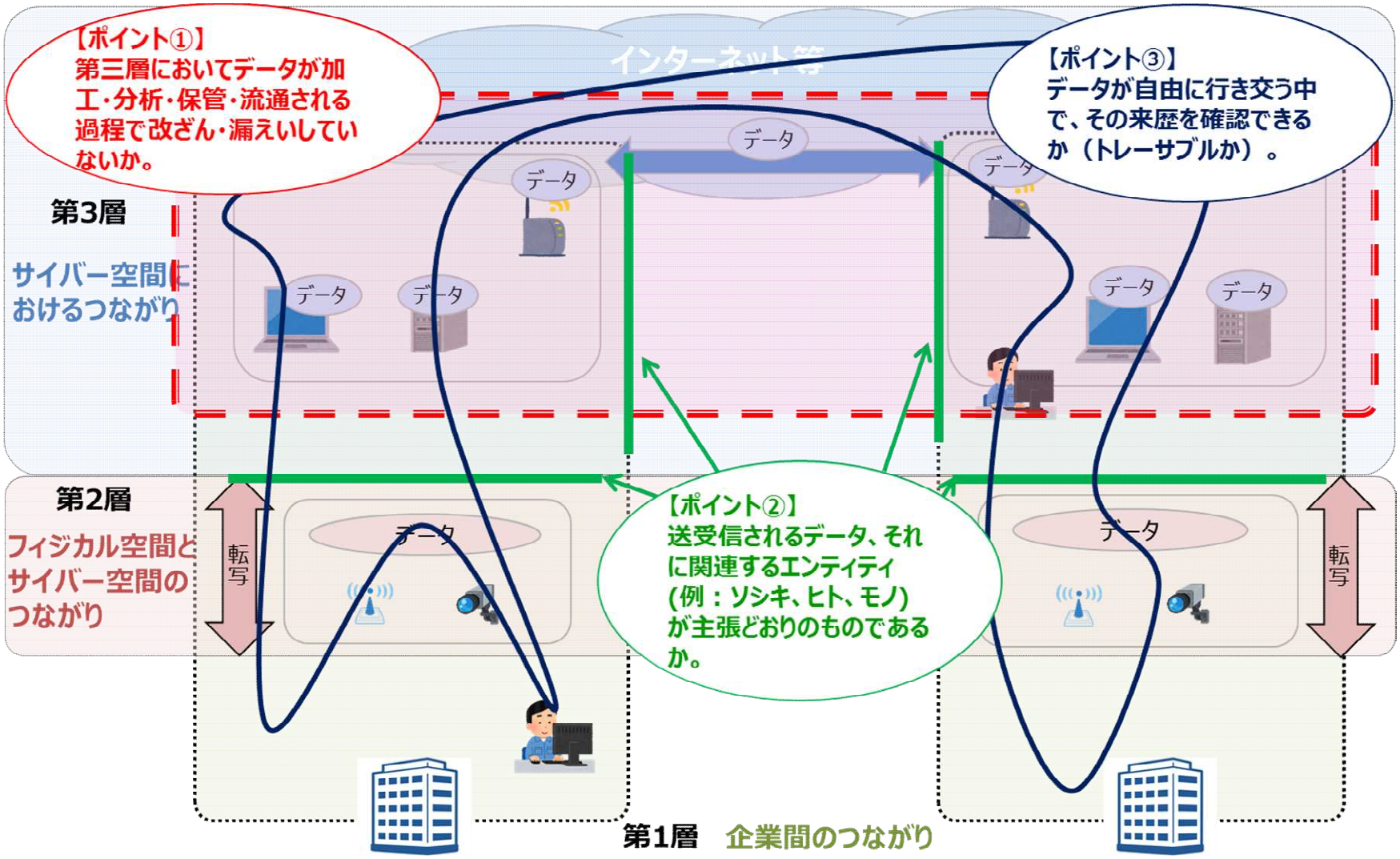
# 【参考】サイバー・フィジカル間をつなげる機器に潜むリスクのイメージ



# 【参考】『第3層』タスクフォースの検討の方向性

- 本タスクフォースにおいて、データの信頼性の考え方を整理し、「**データの区分に応じた適切なセキュリティ対策要件**」及び「**データの信頼性の確認手法**」を検討。

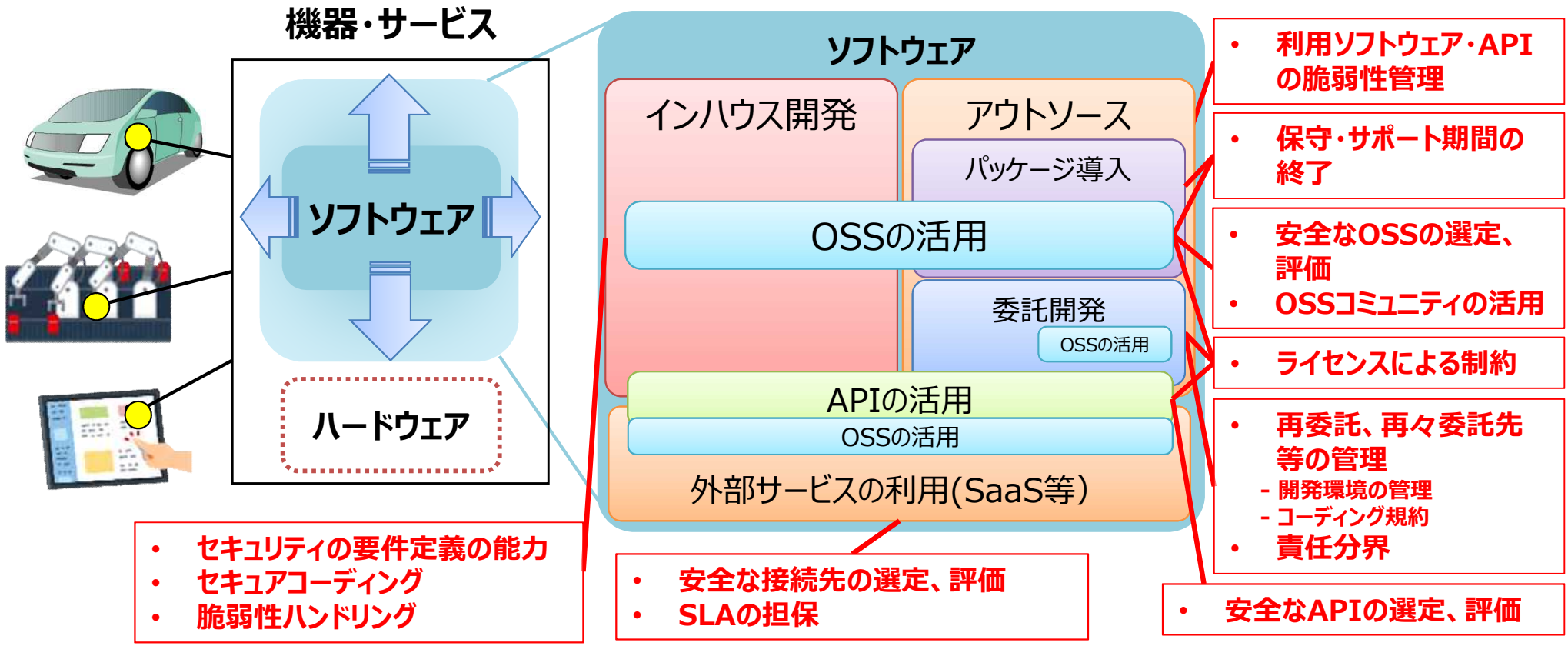
## データの信頼性確保のために考慮すべき3つのポイント



# 【参考】『ソフトウェア』タスクフォースの検討の方向性

- 国際的な動きとも連携しつつ、産業横断的に活用できるソフトウェア管理のあり方について検討を開始する。
- 脆弱性が発覚した際の効果的な対応手法及び既知の脆弱性の管理手法等について検討。
- OSSコミュニティの有効活用も含め、OSS活用のベストプラクティスや、OSS利用時に問題となり得る安全性のリスクやOSSのサポート期間、ライセンスの問題などを整理。

**ソフトウェアの利活用を巡る課題のイメージ**



# 【参考】ソフトウェア管理手法のあり方　～利用者が留意するべき事項～

<table>
<tr><th></th><th>開発中</th><th>運用中<br>（脆弱性情報の収集）</th><th>運用中<br>（脆弱性対応）</th></tr>
<tr><td>HeartBleedの脆弱性</td><td colspan="2" rowspan="2">✓使用中のOSSバージョン把握<br>✓脆弱性情報の確認<br>✓保守・サポート期間の確認</td><td rowspan="2">✓OSSのアップデート<br>✓WAF等による暫定対処<br>✓サービスの一時停止</td></tr>
<tr><td>Strutsの脆弱性</td></tr>
<tr><td>Copayの脆弱性</td><td rowspan="2">✓開発プロセスの確認</td><td rowspan="2">✓使用中のソフトウェアのバージョン把握<br>✓脆弱性情報の確認<br>✓コードサイニング証明書の確認</td><td rowspan="2">✓ソフトウェアのアップデート<br>✓FW等による暫定対処<br>✓ソフトウェアの利用停止</td></tr>
<tr><td>Triadaの脆弱性</td></tr>
<tr><td>ASUSの脆弱性</td><td>✓ パッチ配信サーバの安全性確認</td><td>✓脆弱性情報の確認</td><td>✓マルウェアの削除</td></tr>
<tr><td>OSSのライセンス問題</td><td colspan="2">✓ライセンス内容の確認</td><td>✓ライセンス違反の是正</td></tr>
</table>

JVN等の活用により効率化　SBoM等の活用により効率化

STIX/TAXIIの活用により効率化・自動化

# 2．情報処理の促進に関する法律の一部を改正する法律案の概要

- デジタル技術の急速な発展に伴い、今後、**あらゆる産業活動、国民生活は、リアルタイムに情報やデータが活用・共有されるデジタル社会（＝Society5.0社会）に変貌**。
- デジタル社会においてイノベーションの源泉となる**データ・デジタル技術を活用した新たなビジネスモデル**が、GAFA※1やBAT※2を中心とした**海外企業で誕生**。一方、多くの日本企業では、**事業基盤となるITシステムが技術的に陳腐化（レガシー化）し、データ・デジタル技術を活用した経営の足かせとなるリスクを抱えている**（**2025年の崖**）。 ※1.Google,Apple,Facebook,Amazon ※2.Baidu,Alibaba,Tencent
- こうした状況を打破し、**我が国の産業競争力を向上し、持続的な成長を達成するため**には、①**リアルタイムな変化に即応可能な経営体制の確立、②情報やデータをリアルタイムに扱うシステムの構築**が不可欠。（⇒デジタル・トランスフォーメーション(DX)）

| | 企業のデジタル経営改革 | 産業の基盤づくり | 安全性の確保 |
|---|---|---|---|
| **我が国の現状** | ・新たなデジタル技術を活用した**企業経営**が進んでいない。<br>・**レガシー化したシステムも増加**し、管理に掛かるコストが増大。 | ・**企業ごとに独自のシステム**を作り込んでしまっている。<br>・**組織を超えてデータ連携するシステム**の全体を設計する**専門人材が少ない**。 | ・新技術を活用するための**安全性評価が不十分**。（例：クラウドサービス）<br>・常に最新のサイバー攻撃に関する知識・技能を備えた**専門人材が少ない**。 |
| **課題となる事例** | ・**データ・デジタル技術を活用した新たなビジネスの創出が起こりにくく**、個別企業のみならず、**我が国全体の競争力の低下**をまねく。<br>（例：IT予算に占める既存システムの維持・管理コスト9割超の企業が約4割(民間調査による)。） | ・データを組織横断的に活用する技術の社会実装に向けて、**共通の技術仕様（「アーキテクチャ」という）**を国内で構築できず、**社会的な損失が増大**する。<br>（例：米国では、連邦研究機関（NIST）が電力送電網のデジタル化のアーキテクチャ設計を主導している。） | ・**政府機関等へのサイバー攻撃が発生**した場合、適切な対応がとれず、被害規模が拡大する可能性あり。<br>（例：2015年に、米国の人事管理局がサイバー攻撃を受け、職員の個人情報が流出。） |
| **必要な対応(改正内容)** | ・経営における戦略的なシステムの利用の在り方を提示する**指針を国が策定**。（＝デジタルガバナンス・コード）<br>・上記指針を踏まえた優良な取組を行う**企業を認定**。（＝**DX格付（仮称）**） | ・**アーキテクチャの設計**、**専門家の集約・育成を行う機能**を独立行政法人情報処理推進機構（**IPA**）に**追加**。<br>(産業アーキテクチャ・デザインセンター(仮称)) | ・政府調達におけるクラウドサービスの安全性評価を行う機能を**IPA**に**追加**。<br>・**情報処理安全確保支援士(既存)**の**登録に更新手続き**等を導入し、能力を維持・向上。 |