経済産業省

資料７

電力分野を巡るサイバーセキュリティ政策の動き

経済産業省　商務情報政策局

サイバーセキュリティ課

１．はじめに
～サイバー攻撃の脅威レベルの向上と海外の動き

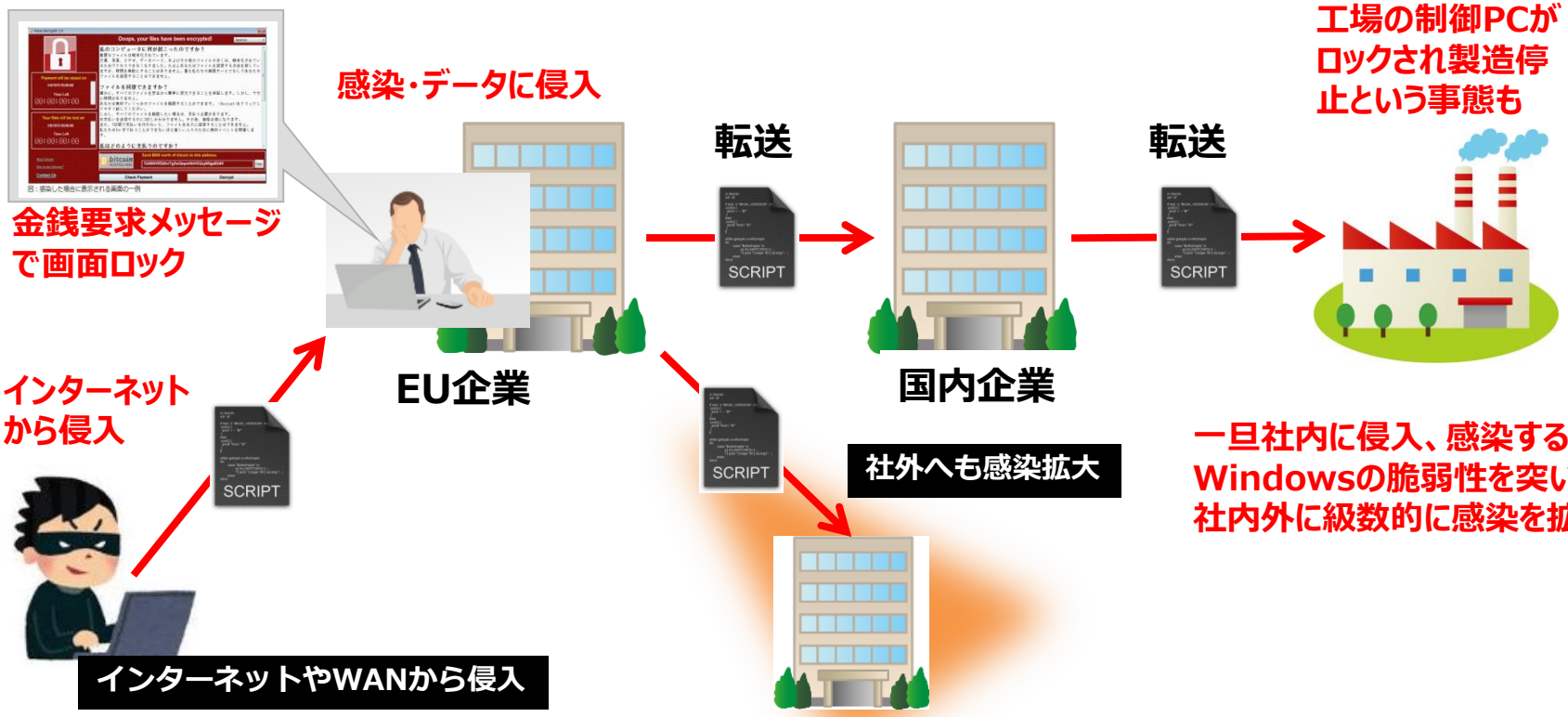
２．「Society5.0」において必要なセキュリティ対策
～サイバー・フィジカル・セキュリティ対策フレームワークの策定

３．サイバー攻撃の脅威レベルの向上を踏まえた海外における電力サプライチェーンの強化の動き

４．電力分野におけるサプライチェーンサイバーセキュリティ対策

サイバー攻撃の脅威レベルの増大（サプライチェーンを通じた攻撃（水平的脅威））
ランサムウェア"WannaCry"の猛威

- 平成29年５月、世界の少なくとも約150か国において、Windowsの脆弱性を悪用したランサムウェア「WannaCry」に感染する事案が発生。
- **感染した欧州企業から、サプライチェーン経由で国内企業も感染**。



サイバー攻撃の脅威レベルの増大（サプライチェーンを通じた攻撃（水平的脅威））
台湾積体電路製造（TSMC）のランサムウェア感染事案

- 2018年8月3日、半導体受託生産の世界最大手である**台湾積体電路製造（TSMC）※において、主力工場内ネットワーク機器がマルウェア感染**。6日午後に復旧するまでの間、**生産が一時停止**。
- 生産停止による**損害額は最大190億円**（営業利益ベース）。

※台湾TSMC社：台湾新竹市に本拠を置く世界最大の半導体製造企業。2014年の市場シェアは53.1%。
顧客企業は米アップル、クアルコム、NVIDIA等、数百社に上る。

本事案の詳細（原因等）

- 感染したマルウェアは、2017年5月に世界中で猛威を振るった「WannaCry」の亜種（金銭要求画面が出ずに機器を停止）。
- 感染した新規追加機器を工場内ネットワークに接続したことで、ネットワーク内感染が発生。
- 本来、接続前に閉鎖環境でウィルススキャンする手順であったが、内部の作業ミスにより実施されなかった。
- 加えて、ネットワーク内機器がWindows7端末であったため、ネットワーク内で感染が拡大。

３日間の生産停止により、損害額１９０億円

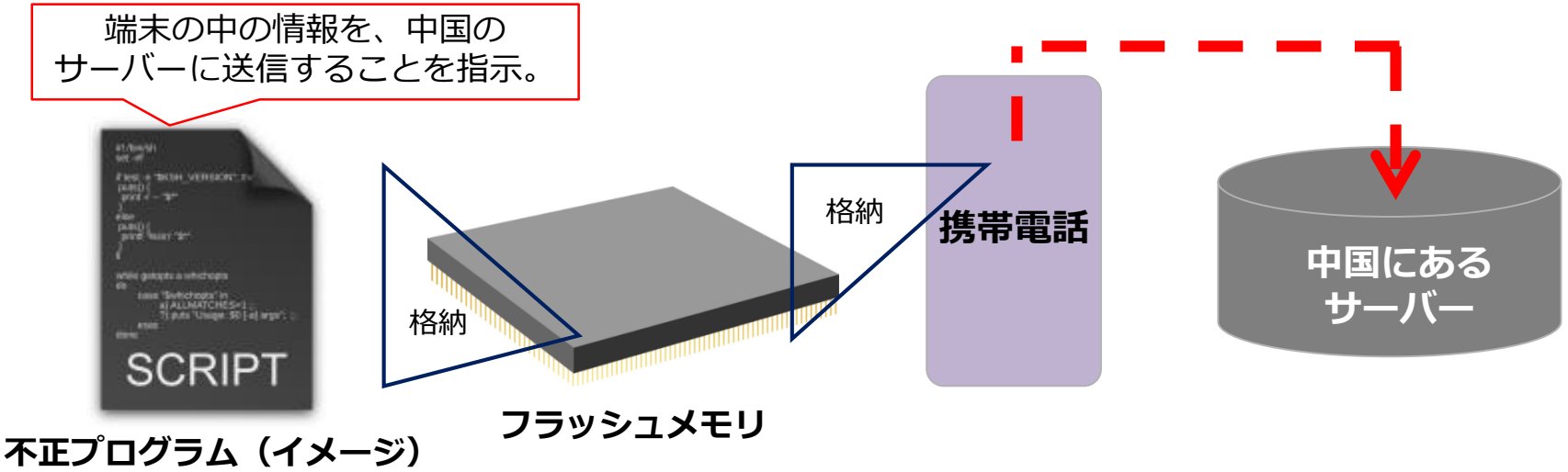
感染イメージ

サイバー攻撃の脅威レベルの増大（サプライチェーンを通じた攻撃（水平的脅威））
携帯端末に不正プログラムが仕掛けられた事例

- メモリに不正プログラムが仕掛けられ、保存されている情報の不正送信や改ざんを受けるリスクが顕在化。
- **製造時に物理的に組み込まれた不正プログラムは検知や削除が容易ではない**。

フラッシュメモリに不正プログラムが仕掛けられた事例

- 2016年、**米国セキュリティ会社が携帯電話のフラッシュメモリのファームウェアに仕込まれている不正プログラムを発見**。
- 中国企業が開発・製造したもので、ユーザーの同意なしに、72時間おきに携帯電話内の情報が中国のサーバーに送信される。



電力分野における事例

サイバー攻撃の脅威レベルの増大
（情報システムを越えて制御システムに達する攻撃（垂直的脅威））
制御系にまで影響が波及

- 米国ICS-CERTの報告では、**重要インフラ事業者等において、制御系にも被害が生じている**。
- ウクライナでは、2015年と2016年にサイバー攻撃による停電が発生。**2016年の攻撃(CrashOverRide)**では、**サイバー攻撃のみで、停電が起こされた**。

米国の重要インフラへのサイバー攻撃の深さ

攻撃のうち約一割は、制御系までサイバー攻撃が到達

（出典）NCCIC/ICS-CERT Year in Review FY2015
Homeland Security より経済産業省作成

2016年に発生したウクライナの停電に係る攻撃（CrashOverRide(Industryoyer)）

(出典)https://www.jiji.com/jc/v2?id=20110311earthquake_25photo
(出典)www.chuden.co.jp/hekinan-pr/guide/facilities/thermalpower.html

（参考）米国電力事業者を標的とした北朝鮮によるサイバー攻撃

- 2017年9月22日、北朝鮮のハッカー集団「TEMP.Hermit」が**複数の米電力事業者を標的にスピアフィッシングメール攻撃**を行った（FireEye報告書より）。
- 今回の攻撃は、検知・阻止されたものの、**電力事業者のシステムに致命的な打撃を与えるための偵察活動**であったと見られている。

本攻撃による脅威の詳細

偵察活動

① 資金調達パーティへの招待状を偽装したメールが複数の米電力事業者宛に届く
② マクロが含まれている添付ファイルを開封すると、バックドア型マルウェア「PEACECOFFEE」がインストールされ、ポート443を通じてC&Cサーバとの通信を開始
③ 攻撃者は、 C&Cサーバを介し、ファイルのアップロードやダウンロード、ファイルリストの作成等、任意のコマンドを実行

電力制御系システムの防御対策等の情報漏えい → さらなる攻撃による電力供給停止

欧米において強化される『サプライチェーン』サイバーセキュリティへの要求

- **米国、欧州は、サプライチェーン全体に及ぶサイバーセキュリティ対策を模索。**

【米国】

- 2018年4月16日、**サイバーセキュリティフレームワーク**（NIST策定のガイドライン）**に、『サプライチェーンのリスク管理』及び『サイバーセキュリティリスクの自己評価』を追記**
- 2017年末、**防衛調達に参加する全ての企業に対してセキュリティ対策（SP800-171の遵守）を義務化**

【欧州】

- 2018年5月10日、**エネルギー等の重要インフラ事業者に、セキュリティ対策を義務化（NIS Directive）を施行**
- 2017年、**単一サイバーセキュリティ市場を目指し、ネットワークに繋がる機器の認証フレームの導入検討を発表**
- 2018年5月25日、**EUの顧客データを扱う企業に対するデータ処理制限等の新たな義務（GDPR）を施行**
- **ドイツにおいてルーターのテクニカルガイドラインを作成中**

セキュリティ要件を満たさない事業者、製品、サービスは

グローバルサプライチェーンからはじき出されるおそれ

１．はじめに
　～サイバー攻撃の脅威レベルの向上と海外の動き

２．「Society5.0」において必要なセキュリティ対策
　～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

３．サイバー攻撃の脅威レベルの向上を踏まえた
　海外における電力サプライチェーンの強化の動き

４．電力分野におけるサプライチェーンサイバーセキュリティ対策

Society5.0を3層構造の社会モデルで捉えた背景①
～従来型のサプライチェーンからSociety5.0型のサプライチェーンへの変化

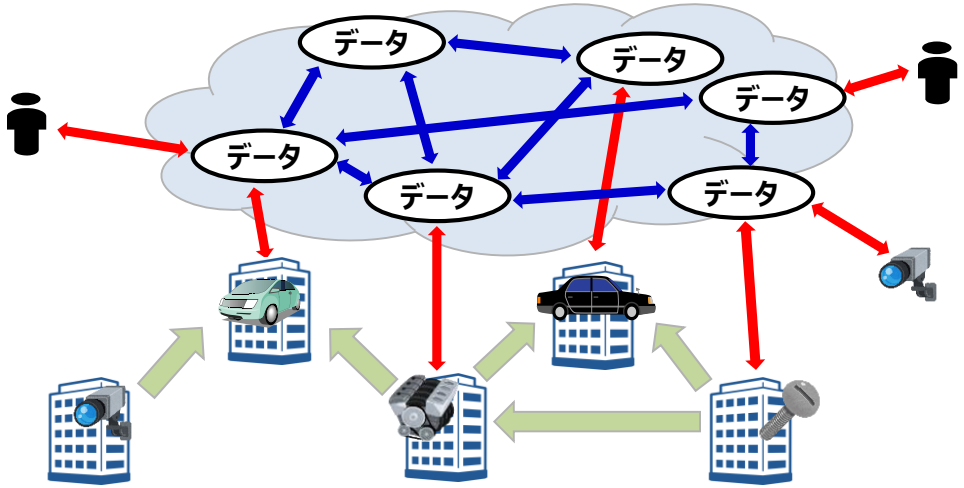
- 「Society5.0」では、企業間・産業間のネットワークが急拡大し、これまで取引を行うことがなかった**主体を新たに巻き込んだ、より柔軟で動的なサプライチェーン**の構成が可能。
- 本フレームワークでは、「Society5.0」におけるサイバー空間とフィジカル空間の相互作用で新たな付加価値を生み出す新たな形のサプライチェーンを**価値創造過程（バリュークリエイションプロセス）**と定義。

「Society5.0」以前（従来のサプライチェーン）

部品メーカ　　組立メーカ　　完成メーカ

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」（価値創造過程（バリュークリエーションプロセス））

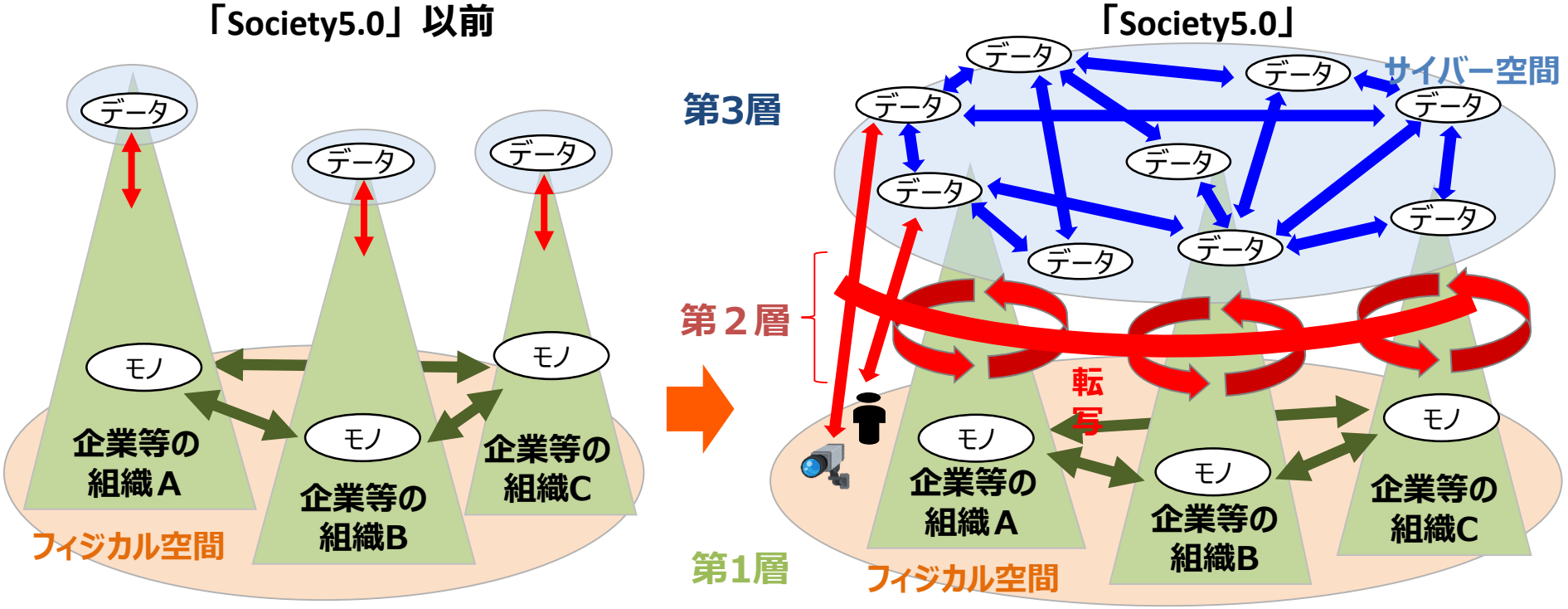


様々な企業や個人等のより柔軟で動的なつながり（バリュークリエーションプロセス）が価値を生み出す

バリュークリエーションプロセスのリスク源を適切に捉えるために、今までと違う新たなモデルが必要

Society5.0を3層構造の社会モデルで捉えた背景②
～信頼を確認する対象の多様化

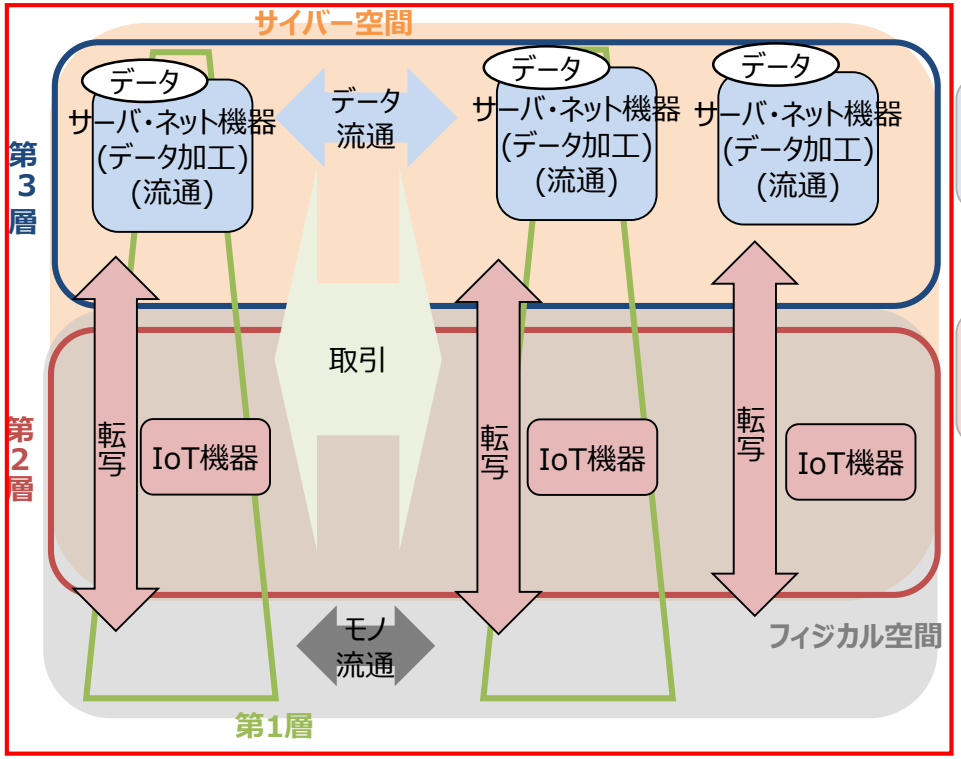
- 「Society5.0」というサイバー空間とフィジカル空間が一体化した産業社会においては、組織のセキュリティ確保だけでは社会全体の信頼が確保できない。
- このため、信頼を確認する対象の機能で3層構造に分けて社会モデルを構築。



- 信頼できる組織間のモノ・データの交換が中心であり、モノ・データ等の責任をとる組織が明確
- 信頼が確認できないヒト・モノとのデータの交換が行われる等、モノ・データ等の責任をとる組織・ヒトが不明確

Society5.0における信頼確保を目指したセキュリティ対策
～各機能に着目したマルチステークホルダーによる対策

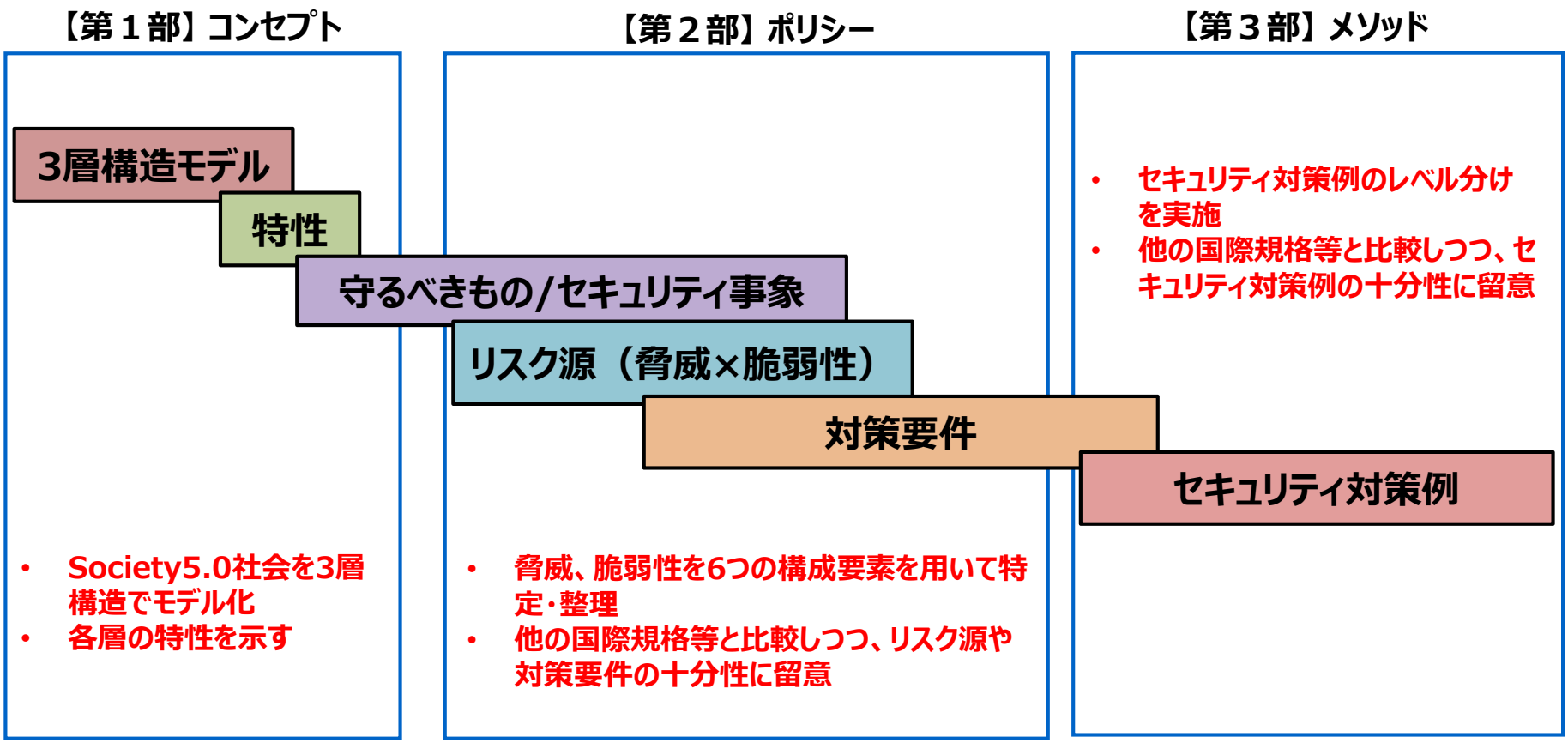
- 各層や各主体が相互に密接に関係する**「Society5.0」のセキュリティを確保するため**には、従来の個々の組織主体のセキュリティ対策だけでは不十分であり、各層において、**マルチステークホルダーによる対応も含めたセキュリティ対策**が必要。



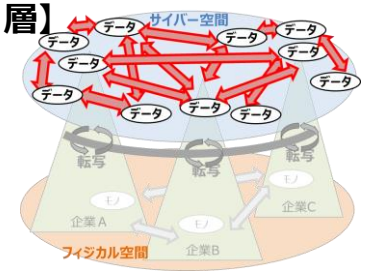
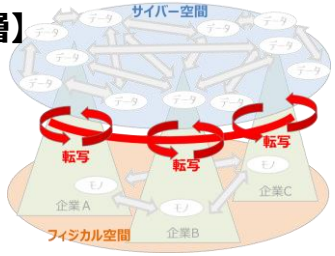
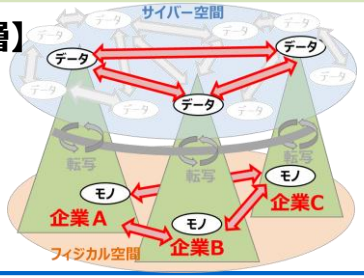
信頼を確保すべき対象	各主体が実施すべきセキュリティ対策	相手の信頼の確認
自由に流通し、加工・創造されるサービスを創造するためのデータの信頼	データ加工・流通時のセキュリティ対策	データの信頼の確保
フィジカル・サイバー間を正確に“転写“する機能の信頼	転写機能を考慮した(セーフティ含む)、モノ(ハード・ソフト)に求められるセキュリティ対策	転写機能の信頼の確保
適切なマネジメントを基盤に各主体の信頼	組織・管理者に求められるセキュリティ対策(マネジメント規格)	主体の信頼の確保

【参考】
フレームワークの全体構成の見直し

- 『サイバー・フィジカル・セキュリティ対策フレームワーク』を**リスク評価に活用するためには、脅威と脆弱性（リスク源）の明確化**が必要。
- また、**企業等が実施する対策の十分性・コストを検討するためには、対策例のレベル分け**が必要。
- こうした観点から、フレームワークの構成を以下のとおり**3部構成に再構成**する。



【参考】
（第1部）フレームワークの構成
~フレームワークが提示する3層構造モデルと特性

3層構造モデル	特性	守るべきもの/セキュリティ事象
サイバー空間におけるつながり 【第３層】  **信頼を確保すべき対象** 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	サイバー空間にて自組織のデータだけでなく、組織を超えて多様かつ大量なデータを収集・蓄積・加工・分析	**【守るべきもの】** • ライフサイクル全体に渡る、データの適切な保護 **【セキュリティ事象（例）】** • サイバー空間にて保管された保護すべきデータが漏洩する
フィジカル空間とサイバー空間のつながり 【第2層】  **信頼を確保すべき対象** フィジカル・サイバー間を正確に“転写“する機能の信頼	IoT機器を介して、フィジカル空間とサイバー空間とのつながりが増大	**【守るべきもの】** • サイバー空間/フィジカル空間の間における転写機能 • 転写機能を支えるモノ、システムの信頼性 **【セキュリティ事象（例）】** • IoT機器の意図しない動作による機器の破損、従業員への物理的危害、業務への悪影響
企業間のつながり（従来型サプライチェーン） 【第1層】  **信頼を確保すべき対象** 適切なマネジメントを基盤に各主体の信頼	個々の組織の適切なガバナンス・マネジメントによって信頼が維持	**【守るべきもの】** • 組織の信頼 • 組織間における取引の信頼性 **【セキュリティ事象（例）】** • セキュリティインシデントによる被害が拡大し、自組織および関係する他組織が適切に事業継続できない

【参考】
（第2部）フレームワークの構成
~リスク源（脅威×脆弱性）と対策要件

守るべきもの/セキュリティ事象 → リスク源（脅威×脆弱性） → 対策要件

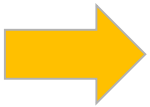
階層	守るべきもの/セキュリティ事象	リスク源		対策要件
		脅威	脆弱性	
第3層	**【守るべきもの】** • ライフサイクル全体に渡る、データの適切な保護 **【セキュリティ事象（例）】** • サイバー空間にて保管された保護すべきデータが漏洩する	サイバー空間におけるデータの安全な利活用に対する脅威	サイバー空間における資産または管理策の弱点	（例） 適切なデータの機密区分および区分に応じた管理策を実施する
第2層	**【守るべきもの】** • サイバー空間/フィジカル空間の間における転写機能 • 転写機能を支えるモノ、システムの信頼性 **【セキュリティ事象（例）】** • IoT機器の意図しない動作による機器の破損、従業員への物理的危害、業務への悪影響	フィジカル空間とサイバー空間の間の転写機能に対する脅威	転写機能を実現するための資産または管理策の弱点	（例） 受容できない既知のセキュリティリスクの有無を企画・設計の段階から確認し、適宜対策を講じる
第1層	**【守るべきもの】** • 組織の信頼 • 組織間における取引の信頼性 **【セキュリティ事象（例）】** • セキュリティインシデントによる被害が拡大し、自組織および関係する他組織が適切に事業継続できない	サプライチェーン全体での事業継続に対するセキュリティに係る脅威	フィジカル空間における資産または管理策の弱点	（例） 関係する外部組織に対して、契約内容遵守状況を定期的に評価する

【参考】
（第2部）3層構造における６つの構成要素
～脅威・脆弱性・セキュリティ対策例等の特定・整理に利用

- 3層構造に基づく社会モデルにおける構成要素を6つに分類・一般化。

「Society5.0」以前

組織が中心となってモノ・データを管理してサプライチェーンを構成



「Society5.0」

組織に所属していないヒト・モノ・データ等も価値創造過程に直接参加可能

構成要素	定義	具体例
組織	価値創造過程（特に、従来型サプライチェーン）に参加する企業・団体	企業、企業の事業部/本部/部、政府機関、学校
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	従業員、職員、パートタイマー、個人事業主、個人
モノ	ハードウェア、ソフトウェア、及びそれらの部品 操作する機器を含む	PC、サーバ機器、IoT機器、通信機器、スイッチングハブ、ルータ、ネットワークケーブル、CPUとメモリ付きの基板、CPU、メモリ、 ソフトウェア、モータ、アクチュエータ、発電機
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	文字データ、数値データ、静止画像データ、動画像データ、 システム設定値
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	マニュアル、ルール、規則、ポリシー
システム	サービスを実現するためにモノで構成される仕組み・インフラ 【参考】 情報システム：アプリケーション，サービス，IT 資産，及び情報を取り扱う他の構成要素。JIS 27000:2014	

※赤字はパブコメ版から追記した個所

【参考】
（第3部）セキュリティ対策例の作成

- 対策要件に基づき、セキュリティ対策例を作成。

対策要件 → **セキュリティ対策例**

＜イメージ＞

対策要件
・・・
• 暗号化機能、アンチウイルス機能等をIoT機器側で実装することが難しい場合、システム側で"転写機能"を守るためのセキュリティ対策を実装する必要がある。
・・・
• IoT機器、サーバ等のソフトウェア構成情報、パッチ適用状況等を把握し、適宜対応する必要がある。
・・・

セキュリティ対策例
【対策例】 ・・・
(L2.017) (L3.014) IoT機器で構成する組織内のネットワークを、他のネットワークと物理的又は論理的な手法で分離する。
(L2.018) ネットワーク監視によるサイバー攻撃検知
(L2.018) ファイアウォール、IDS(不正侵入検知システム)、IPS(不正侵入防止システム)の導入
(L2.015) セキュリティルールに従って、ソフトウェアの追加/削除/更新を監視し、その作業履歴や監査ログを残し、定期的にレビューする
(L2.020) IoT機器の稼働状況、監査ログ、IoT機器の設定、ソフトウェアの構成等を遠隔地から集中管理する。これにより、稼働状況の把握やセキュリティインシデントの検知を迅速に実施する。

＜作成中＞

並び順は、国際規格等を参照しつつ検討

１．はじめに
　～サイバー攻撃の脅威レベルの向上と海外の動き

２．「Society5.0」において必要なセキュリティ対策
　～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

３．サイバー攻撃の脅威レベルの向上を踏まえた
**　海外における電力サプライチェーンの強化の動き**

４．電力分野におけるサプライチェーンサイバーセキュリティ対策

米国の電力業界におけるサイバー攻撃の懸念を踏まえた動向①

- 7月31日、米国連邦エネルギー規制委員会(FERC)※1は北米電力信頼度評議会(NERC)※2に対し、インシデント報告に係る要求基準の強化を指示。NERCは10月1日にまでに基準を改定。
- 8月16日、NERCは大規模電力システム※3制御センター間の通信の保護に係る新基準を決定。

※1 FERC：米国エネルギー省（DoE）の管轄下の機関。
※2 NERC：FERCが電力信頼度機関（ERO）として認定。FERCの監督の下、NERCは電力セクターのセキュリティ基準の作成・監査を実施。違反には罰金。
※3 大規模電力システム：大規模発電設備、送電・配電設備のうち大きな停電につながる可能性がある設備の総称（NERCが定義）

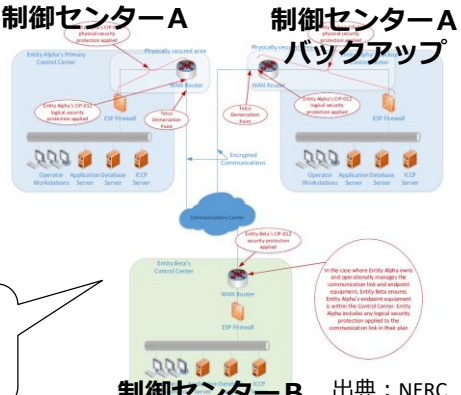
インシデント報告に係る要求基準強化の指示（7/31 FERC）

- 2015-2016年にインシデント報告が無かったことを踏まえ、攻撃が失敗（attempt to achieve）した場合のインシデント報告も義務化（※ 現行のNERC基準CIP-008-5では、被害があった場合のみ報告を義務化）
- インシデント報告に求められる最低限の情報を標準化（※ 機能的影響（示せる場合）、攻撃経路、侵入のレベルを報告に含める。）
- インシデントの深刻度に応じた報告タイムラインを設定（※ 重大事象ほど迅速な報告が求められる。）
- E-ISACに加え、DHSのNCCIC ICSに対してもインシデント報告を義務化

大規模電力システム制御センター間の通信の保護に関する基準（8/16 NERC）

- 新たなCIP（Critical Infrastructure Protection）標準であるCIP-012-1を策定。
（※ NERCはこれまでセキュリティ関連の主なもので約10の基準を策定。）
- 電力システムのリアルタイム監視データ等を大規模電力システム制御センター間で通信する際に必要となるセキュリティ対策の策定・実施や役割分担の明確化を求めている。

CIP-012-1基準の履行ガイドラインの草案では、制御センター間で通信をする際に必要となる対策の例として、拠点間の通信の暗号化や通信機器の物理セキュリティ対策など、具体的に記述。



出典：NERC

米国の電力業界におけるサイバー攻撃の懸念を踏まえた動向②

- 10月31日、米国連邦エネルギー規制委員会(FERC)は、**新たなサプライチェーンリスク対策**として、北米電力信頼度評議会(NERC)が新たに作成・更新したCIP-013-1,CIP-005-6,CIP-010-3を承認。
- さらに同日、FERCは、NERCに対するOrder 850を発行。

CIP-005-6 （Cyber Security - Electronic Security Perimeters）

影響度「中」又は「大」の大規模電力システムにおいて、ベンダーからのリモートアクセスのセッションを把握する手段を１つ以上持つこと（Requirement 2.4）及び無効化する手段を１つ以上持つこと（Requirement 2.5）という要求事項が追加。

CIP-010-3 （Cyber Security - Configuration Change Management and Vulnerability Assessments）

影響度「中」又は「大」の大規模電力システムにおいて、ソフトウェアのソースのidentityとintegrityを検証することという要求事項が追加。

CIP-013-01 （Cyber Security - Supply Chain Risk Management（新規））

影響度「中」又は「大」の大規模電力システムにおいて、サプライチェーン・サイバーセキュリティ・リスクマネジメント計画として、ベンダーのサイバーインシデントの報告、ベンダーの脆弱性公表、ソフトウェア検証等に関するプロセスの策定等を要求。

Order 850

監視制御システム（EACMS）（FW、認証サーバ、IDS、SIEM等）についてもNERCのサプライチェーン対策のスコープに含むよう指示。

出典ITTA

いずれも米国の電力業界（The Edison Electric Institute, Electronic Power Supply Association, the Electricity Consumers Resource Council）から反論を受けている模様

１．はじめに
　～サイバー攻撃の脅威レベルの向上と海外の動き

２．「Society5.0」において必要なセキュリティ対策
　～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

３．サイバー攻撃の脅威レベルの向上を踏まえた
　海外における電力サプライチェーンの強化の動き

４．電力分野におけるサプライチェーンサイバーセキュリティ対策

海外の動向も踏まえたセキュリティ対策の重要性

- サイバー攻撃の脅威の高まりに伴い、**米国やイスラエルでは、特にサプライチェーンリスクマネジメントに関する対策が進められている**。
- IoTの進展とともに、電力自由化等の進展に伴い、**新たな電力供給構造の中でのサプライチェーンリスクマネジメントの必要性が高まっている**。

電力を取り巻く環境の変化

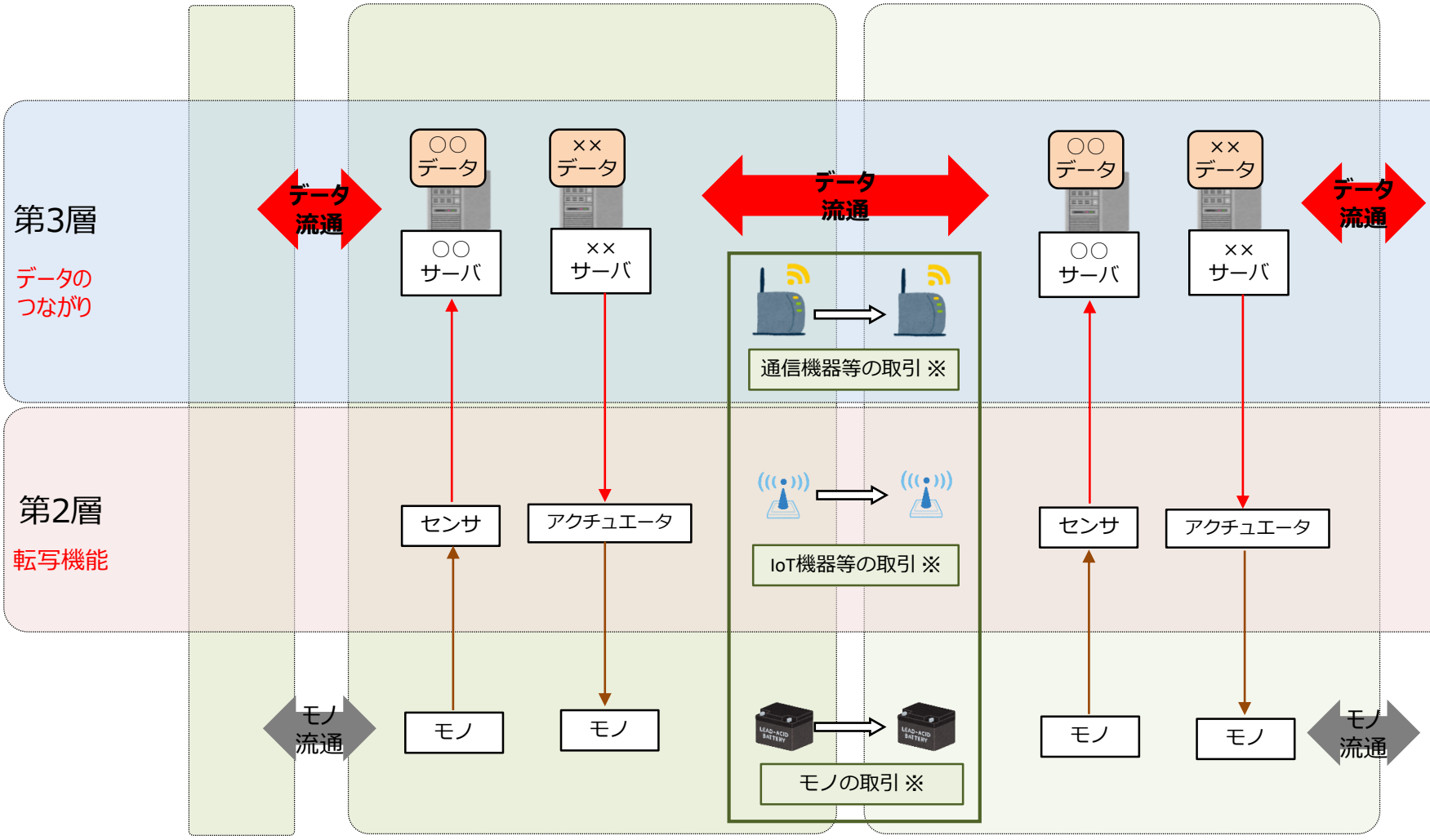
・ＩＰ化・国際標準プロトコルの活用
・ＩｏＴ機器の増加
・発送電に関わるプレイヤーの増加（アグリゲーター、新電力、スマートメーター）

重要性が高まったセキュリティ対策の考え方

①発送電に関する機能を確保するためのセキュリティの確保
- 発送電設備の信頼性確保
- 常時監視体制の構築
- メンテナンスまで含めた信頼性確認体制確保
- データの暗号化機能の追加

②発送電に伴うデータのやり取りに関するセキュリティの確保
- サプライチェーン全体でのセキュリティ対策

3層モデルでの整理



※ モノの調達、取引の際は、第1層の対策を基本に、機能に応じて、第2層（or第3層）の対策も追加で必要。