資料２

関係省庁の取組状況について

総務省　　電気通信事故に関する取組等について（資料２－２）

厚生労働省　重要インフラ分野における予算概算要求の
状況について

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（第二案）について　（資料２－３）

国土交通省　交通ＩＳＡＣの進捗状況

資料２－２

電気通信事故に関する取組等について

総務省

「平成29年度　電気通信事故に関する検証報告」について

■通信工学、ソフトウェア工学、システム監査、消費者問題の有識者で構成される「電気通信事故検証会議」において、平成29年度に発生した電気通信事故に関し、電気通信事故の再発防止に寄与することを目的として検証を行った内容を取りまとめたもの。

【電気通信事故検証会議構成員】
相田　仁　（東京大学大学院工学系研究科　教授）【座長】
阿部　俊二（国立情報学研究所アーキテクチャ科学研究系　准教授）
内田　真人（早稲田大学基幹理工学部情報理工学科　教授）【座長代理】
福井　晶喜（(独)国民生活センター相談情報部相談第2課　課長）
森島　直人（EYアドバイザリー・アンド・コンサルティング株式会社シニアマネージャー）
矢入　郁子（上智大学理工学部情報理工学科　准教授）

（１）平成29年度検証案件の概要

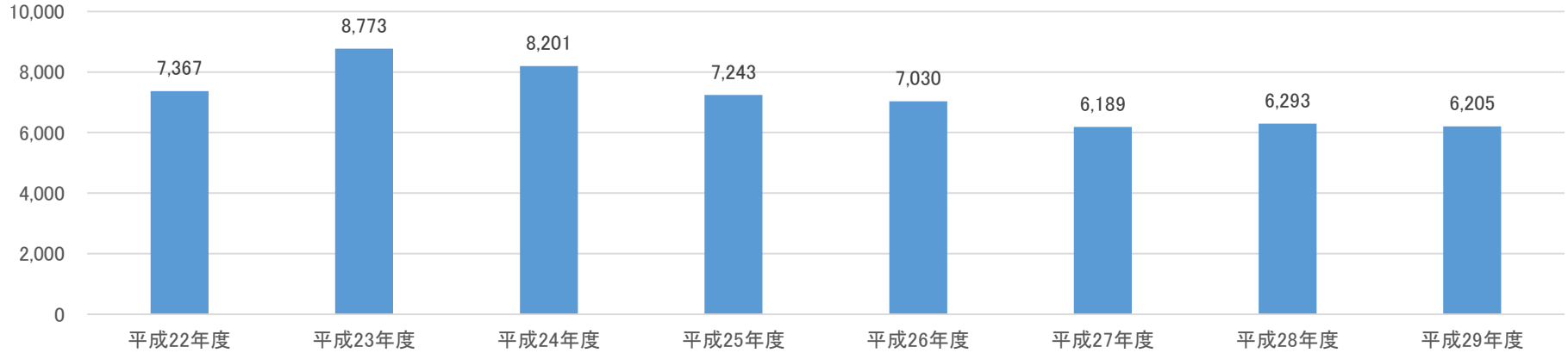
○平成29年度に報告された電気通信事故

（括弧内は平成28年度の数値。）

	報告事業者数	報告件数
重大な事故	６社※ （４社）	４件 （５件）
四半期報告事故		
詳細な様式による報告	132社 （128社）	6,205件 （6,293件）
簡易な様式による報告	21社 （28社）	68,849件 （65,670件）

※卸提供元事業者において発生した事故を含むため、報告事業者数には卸提供元事業者及び卸提供先事業者の両方が含まれており、報告件数よりも多くなっている。

○事故発生件数の年度ごとの推移



「平成29年度　電気通信事故に関する検証報告」について

（２）平成２９年度に発生した事故から得られた教訓等（一部抜粋）

他の電気通信事業者においても同様な事故が発生しないよう、平成29年度に発生した事故の検証から得られた教訓等を整理。概要は以下のとおり。

1　事故の事前防止の在り方

○　**ソフトウェア不具合への対応**
- ソフトウェアのバージョンアップに際しては、重要度・緊急度を考慮の上、導入要否を判断する必要。
- 導入に当たっては、運用環境に近い環境で、試験･検証を行うことが重要。

○　**設備・ソフトウェアの仕様・設定の誤認防止および設定前後の動作確認**
- 設備・ソフトウェアの仕様等の変更の内容、時期等については、関係する部署間で情報共有等を図ることが望ましい。
- インターネットの安定性を確保するため、不要な経路情報をルータでフィルタする仕組み等は有効。

○　**組織外の関係者との連携**
- 接続先事業者の設備に関する情報については、可能な範囲で運用に従事する関係者間で情報共有を図ることが望ましい。

○　**教育・訓練**
- アナログ設備からインターネット設備まで広い範囲の技術の継承に努め、疑似環境による実習等実際の現場に近い環境における教育・訓練が重要。

2　事故発生時の対応の在り方

○　**速やかな故障設備の特定**
- 設備の冗長化対応に当たっては、経路によって機器の動作に差が生ずることがないよう、設計ポリシーはなるべく同一のものとすることが望ましい。
- 日常的に主な接続ポイント等での稼働状況等を計測することは有効。

○　**事故情報共有マニュアル等の作成**
- 事故の規模に応じて、社内外の情報提供についての手続き、内容等についてマニュアルを作成すること等が望ましい。

○　**利用者への情報提供のための社内体制**
- 事故対策本部等へは広報や渉外の担当も参加し、障害等の詳細をリアルタイムに共有することで、継続した利用者への情報提供ができる体制とすることが望ましい。

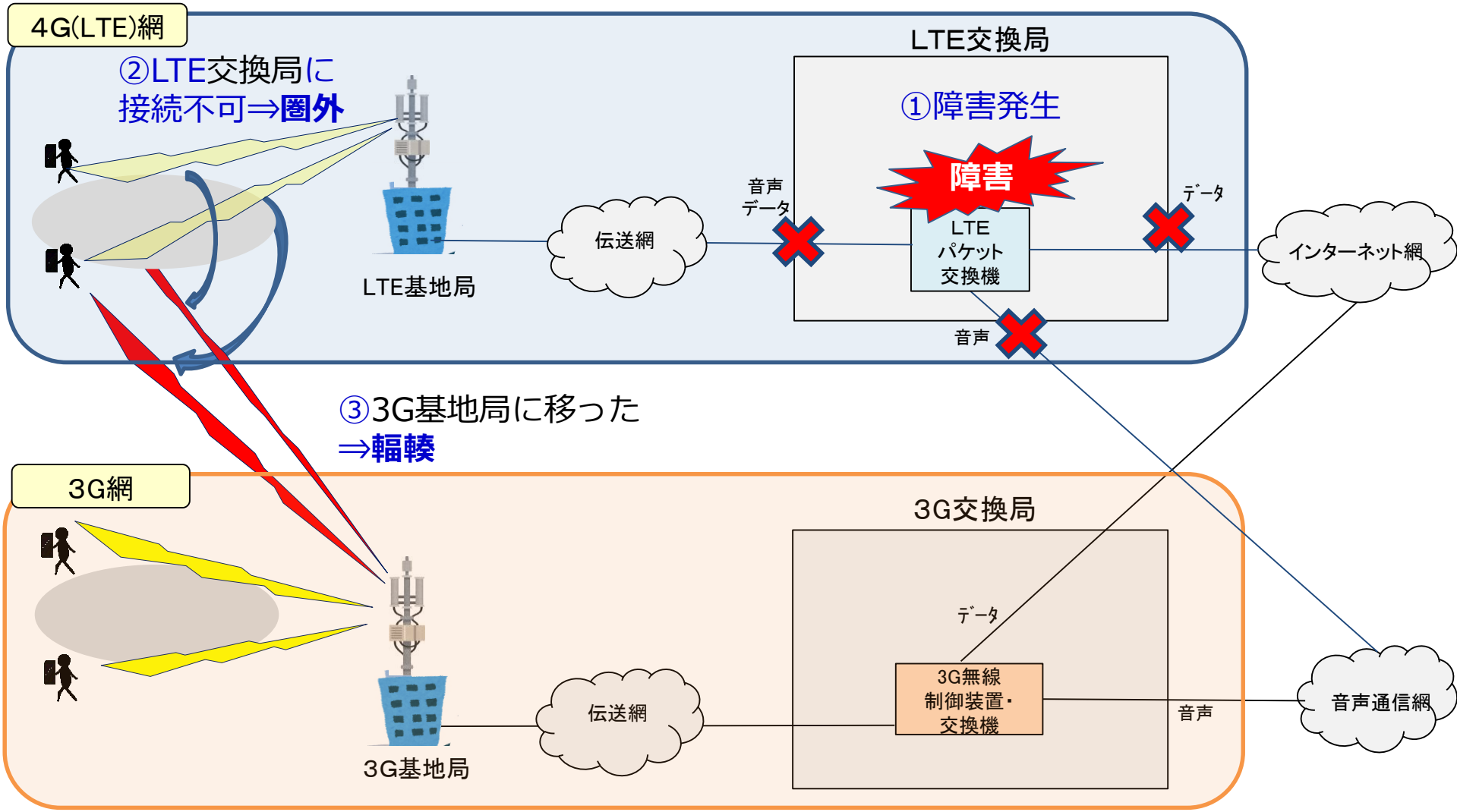
ソフトバンクの携帯電話（LTE）サービスにおける通信障害の概要

○　ソフトバンクの携帯電話（LTE）サービスの通信障害は、緊急通報を取り扱う音声通話サービスの障害であり、影響時間が１時間以上かつ影響利用者数が３万人以上であることから、電気通信事業法上の重大な事故に該当。

発生・復旧日時	発生：平成30年12月6日(木)　13時39分　（影響時間：４時間25分） 復旧：平成30年12月6日(木)　18時04分
影響利用者数等	約3,060万回線・全国
影響があったサービス	＜サービス分類＞ 携帯電話（緊急通報を取り扱う音声通話サービスを含む） インターネット接続サービス ＜具体的なサービス＞ ソフトバンク及びワイモバイルの携帯電話サービス(LTE) ソフトバンク「おうちのでんわ」及び「SoftBank Air」
具体的な障害内容	携帯電話（LTE）の音声通話・データ通信が利用できない状況に ⇒　本障害の影響で、一時、3G網で輻輳が発生
障害原因	首都圏及び関西圏のネットワークセンターの エリクソン社製LTEパケット交換機全台のソフトウェア異常 ※ソフトウェアに組み込まれた証明書の期限切れによる機能の停止

通信障害の状況

○ 今回の通信障害は、①中核設備である**LTEパケット交換機での障害**発生 ⇒ ②全４Gユーザーの端末が**LTE交換局に接続不可** ⇒ ③全４Gユーザーが3G基地局に移ったことにより、**3G網で輻輳**が発生。
その結果、**音声通話もインターネット接続もほぼ不可**に。



経済産業省

資料２－３

サイバー・フィジカル・セキュリティ対策フレームワーク（第二案）について

平成31年 1月17日

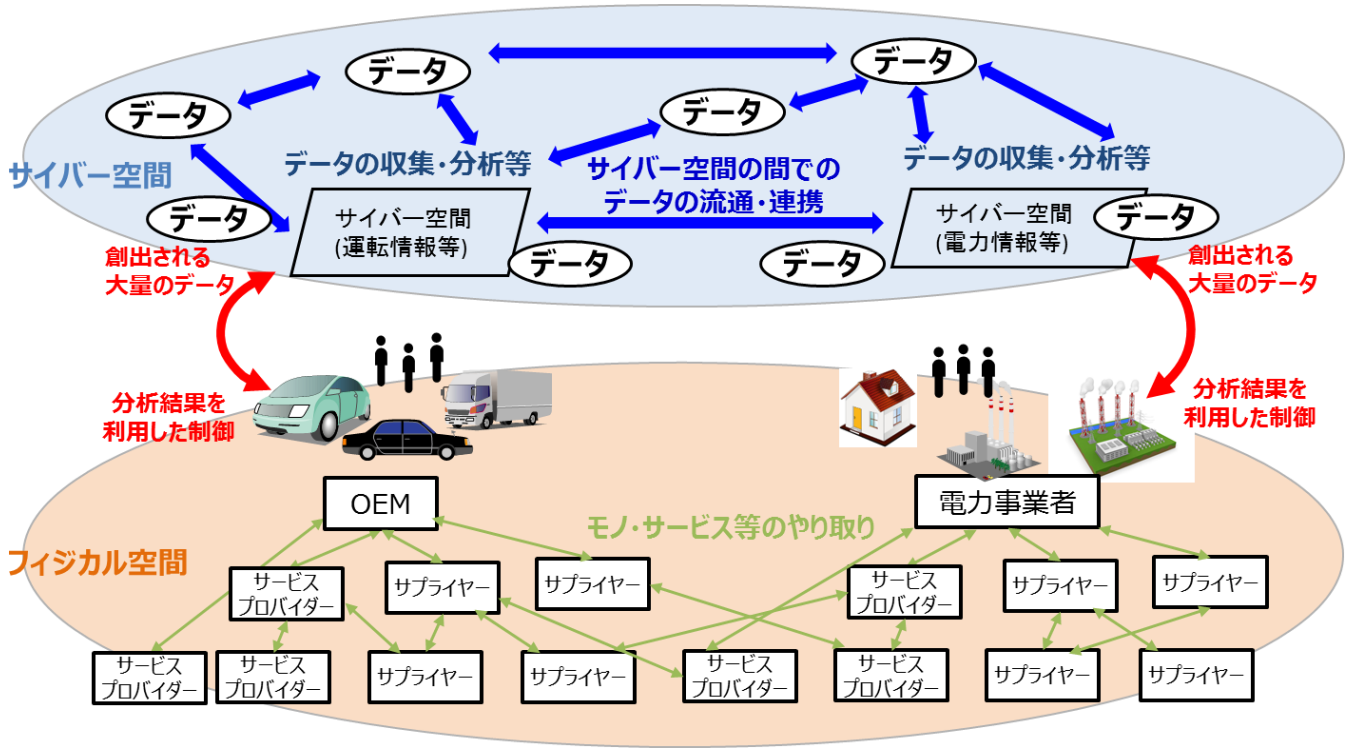
経済産業省　商務情報政策局

サイバーセキュリティ課

背景：サイバー攻撃の脅威の拡大

- 「Society5.0」における産業社会では、**サイバー攻撃の起点が拡大**するとともに、**複雑につなが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』の中で影響を受ける範囲が拡大。**
- サイバー空間とフィジカル空間が高度に融合するために、**サイバー攻撃がフィジカル空間まで到達。**
- IoTから得られる**データの転換処理の信頼性確保、大量のデータの正確性・流通・連携を支えるセキュリティ対策**も課題。

Society5.0の社会におけるモノ・データ等の繋がりのイメージ



大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

フィジカル空間とサイバーの融合
⇒フィジカル空間までサイバー攻撃が到達

複雑につながるサプライチェーン
⇒影響範囲が拡大

フレームワークを作成する目的と適用範囲

- 「Society5.0」、「Connected Industries」の実現へ向けて、**産業構造、社会の変化に伴うサイバー攻撃の脅威の増大に対応することが必要。**
- このため、**バリュークリエイションプロセスのリスク源を適切に捉えるためのモデルを構築し、求められるセキュリティ対策の全体像を整理**し、**産業界が自らのセキュリティ対策に活用できる対策例を『サイバー・フィジカル・セキュリティ対策フレームワーク』**として取りまとめる。
- 本フレームワークは、**従来型サプライチェーンにおいても適用可能な対策に加え、新たな産業社会に変化したからこそ新たに対応が必要なものを整理**している。このため、それぞれの組織の状況に応じてセキュリティ対策を選定することが可能。

サイバー・フィジカル・セキュリティ対策に含まれる対策

従来型サプライチェーンにおいても適用可能な対策	新たな産業社会に変化したからこそ新たに対応が必要な対策

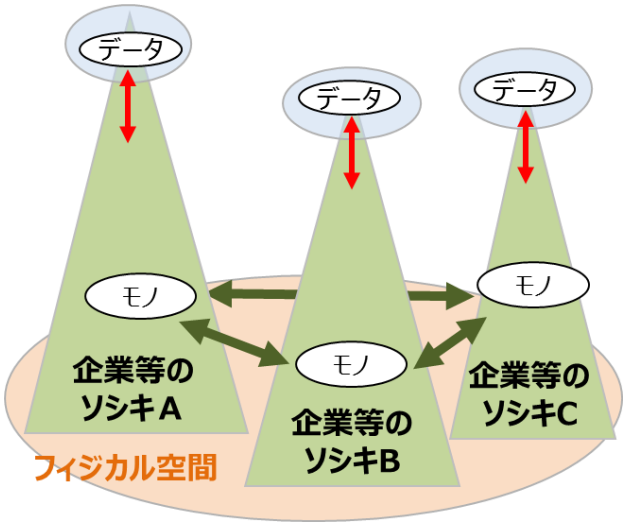
・**新たな産業社会における**バリュークリエイションプロセス全体が適用範囲
・それぞれの組織の状況に応じてセキュリティ対策を選定することが可能

「Society5.0」型サプライチェーン
”価値創造過程”（バリュークリエイションプロセス）への対応

- 従来のサプライチェーンでは、セキュリティを確保した組織間の取引であれば、プロセス全体のセキュリティも確保される。
- 「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、自組織のセキュリティ確保だけではバリュークリエイションプロセスのセキュリティを確保することは困難。**
- バリュークリエイションプロセス全体のセキュリティ確保に必要な、**信頼性の基点を明確にするに新たなモデルが必要。**

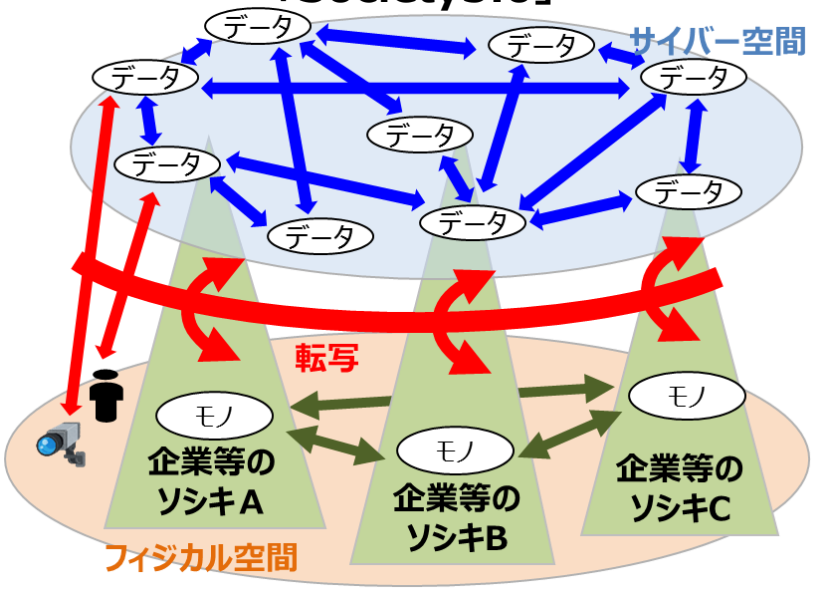
サプライチェーン構造の変化のイメージ

「Society5.0」以前



- **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ソシキが明確**

「Society5.0」



- **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ソシキ・ヒトが不明確**

三層構造アプローチ

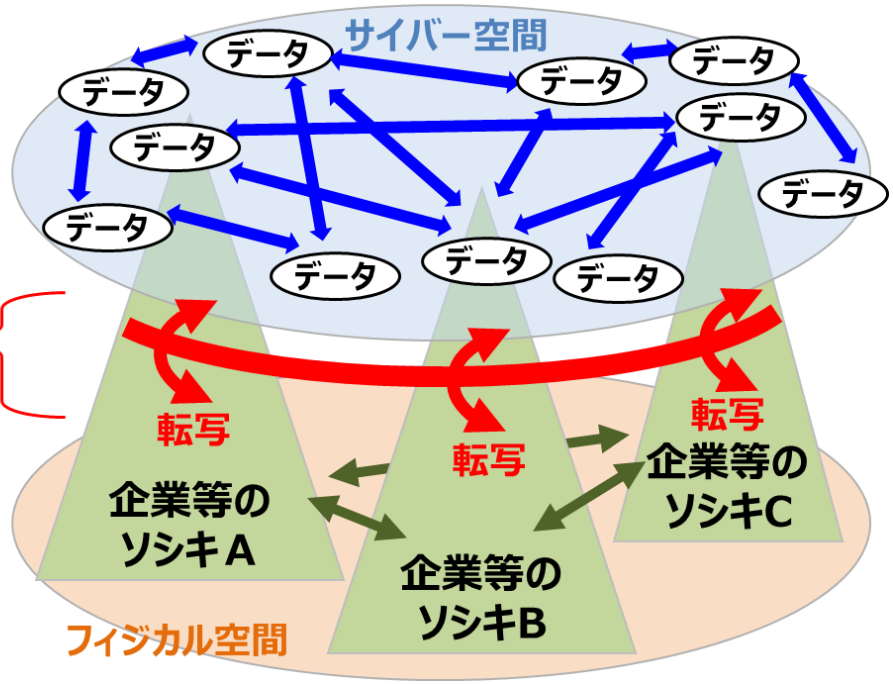
～バリュークリエイションプロセスのセキュリティを確保するための信頼性の基点を設定するためのモデル～

- **本フレームワークでは、バリュークリエイションプロセスが営まれる産業社会を、３つの層に整理**して捉え、**信頼性の基点を明確にする。**
- それぞれの層には、バリュークリエイションプロセスにおいて、信頼性が確保されなければならない機能・役割が存在する。
  - **第１層**では、企業間のつながりにおける、**企業（組織）のマネジメントの信頼性**
  - **第２層**では、サイバー空間とフィジカル空間のつながりにおける、**要求される正確性に応じて適切に情報が変換される“転写”機能**
  - **第３層**では、サイバー空間のつながりにおける、**データの信頼性**

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

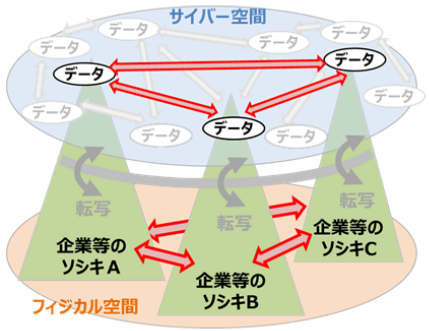
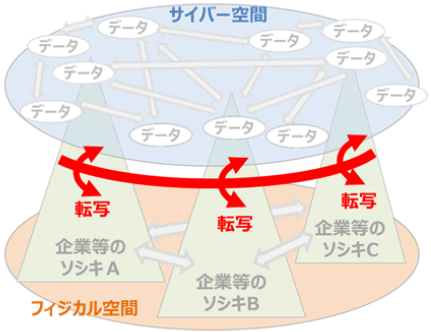
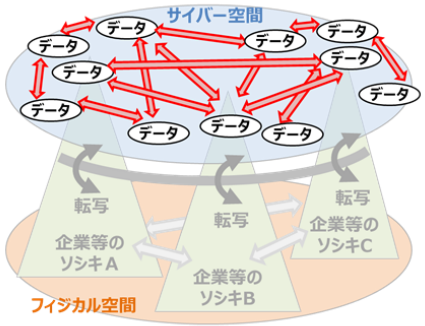
フィジカル空間とサイバー空間のつながり
【第２層】
- フィジカル・サイバー間を正確に“転写“する機能の信頼性を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

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



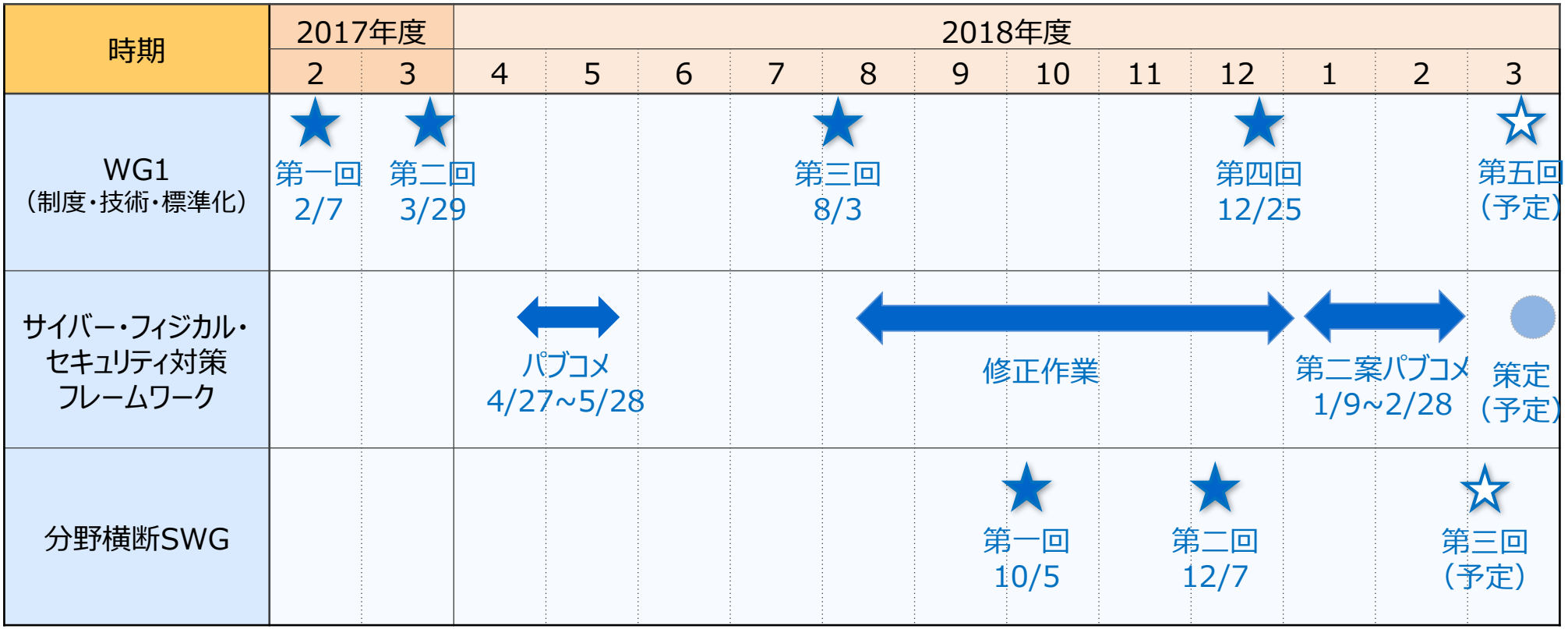
【本フレームワークの全体像】
バリュークリエイションプロセスにおけるリスク源と対応する方針の整理

- 各層ごとに守るべきもの、セキュリティ事象、リスク源を整理し、どのような対策を講じるかを整理。

	企業間のつながり【第１層】	フィジカル空間とサイバー空間のつながり【第２層】	サイバー空間におけるつながり【第３層】
新たなサプライチェーン構造の整理			
機能（守るべきもの）	• 平時及び緊急時のリスク管理・対応体制の構築と運用 • 企業内及び企業間のリスク管理・対応体制の構築と運用	• フィジカル空間とサイバー空間の境界における情報の正確な転写	• データの加工・分析 • データの保管 • データの送受信
セキュリティ事象	• 保護すべき資産の棄損 • 他組織のセキュリティ事象発生に起因する事業停止	• 不正確なデータの送信 • 安全に支障をきたす動作	• 保護すべきデータの漏えい • なりすまし等による不正な組織からのデータ受信
リスク源	• セキュリティリスクに対するガバナンスの欠如 • 他組織との連携状況の未把握	• 不正なIoT機器との接続 • 許容範囲外の入力データ	• 通信経路が保護されていない • 通信相手を識別していない
対策要件（構成要素ごとに整理）	■ マネジメントルールの徹底 ■ 関係者との役割分担	■ 接続相手の認証 ■ 安全なIoT機器の導入	■ 暗号化によるデータ保護 ■ データの提供者の信頼性確認

これまでの取組と今後のスケジュール（案）

- **『サイバー・フィジカル・セキュリティ対策フレームワーク』（第二案）**について、国内外から広く意見を募るため、日本語・英語にて**パブリック・コメントを2月28日まで実施中**。

＜意見公募ページ＞電子政府の総合窓口
「サイバー・フィジカル・セキュリティ対策フレームワーク(案)」に対する意見公募
http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595219001

今後のスケジュールのイメージ