『コネクテッドカー＋MaaS時代のサイバーセキュリティ』

2019年12月9日

藤原　洋

（株）ブロードバンドタワー代表取締役会長兼社長CEO
一般財団法人インターネット協会理事長/IoT推進委員長

5G Innovations

目次

1．コネクテッドカーとCASE時代とは？

●「CASE」の意味

○2016年パリモーターショー：
　独ダイムラーのディーター・ツェッチェCEOが発表した中長期戦略

⇒「Connected：コネクティッド化」

⇒「Autonomous：自動運転化」

⇒「Shared/Service:シェア/サービス化」

⇒「Electric：電動化」

●「CASE」＝自動車から全産業に大変革期をもたらすキーワード

①商品構造=サプライチェーンの変化

②バリューチェーンからサービスバリューWebへの変化

③製品販売から機能提供へのビジネスモデルの非連続的に変化

●CASEがデータセンターなど情報通信インフラとどう関わるか？

C⇒インターネットと常時接続される「コネクティッド化」クルマの
状態や周囲の道路状況などのビックデータを生み出し、
蓄積・分析することによって新しい価値を創造する

A⇒自動運転化には低遅延の5G（第5世代モバイル通信システム）
が効力を発揮する

S⇒クルマビジネスや社会を大きく変えるのは「シェア/サービス化」

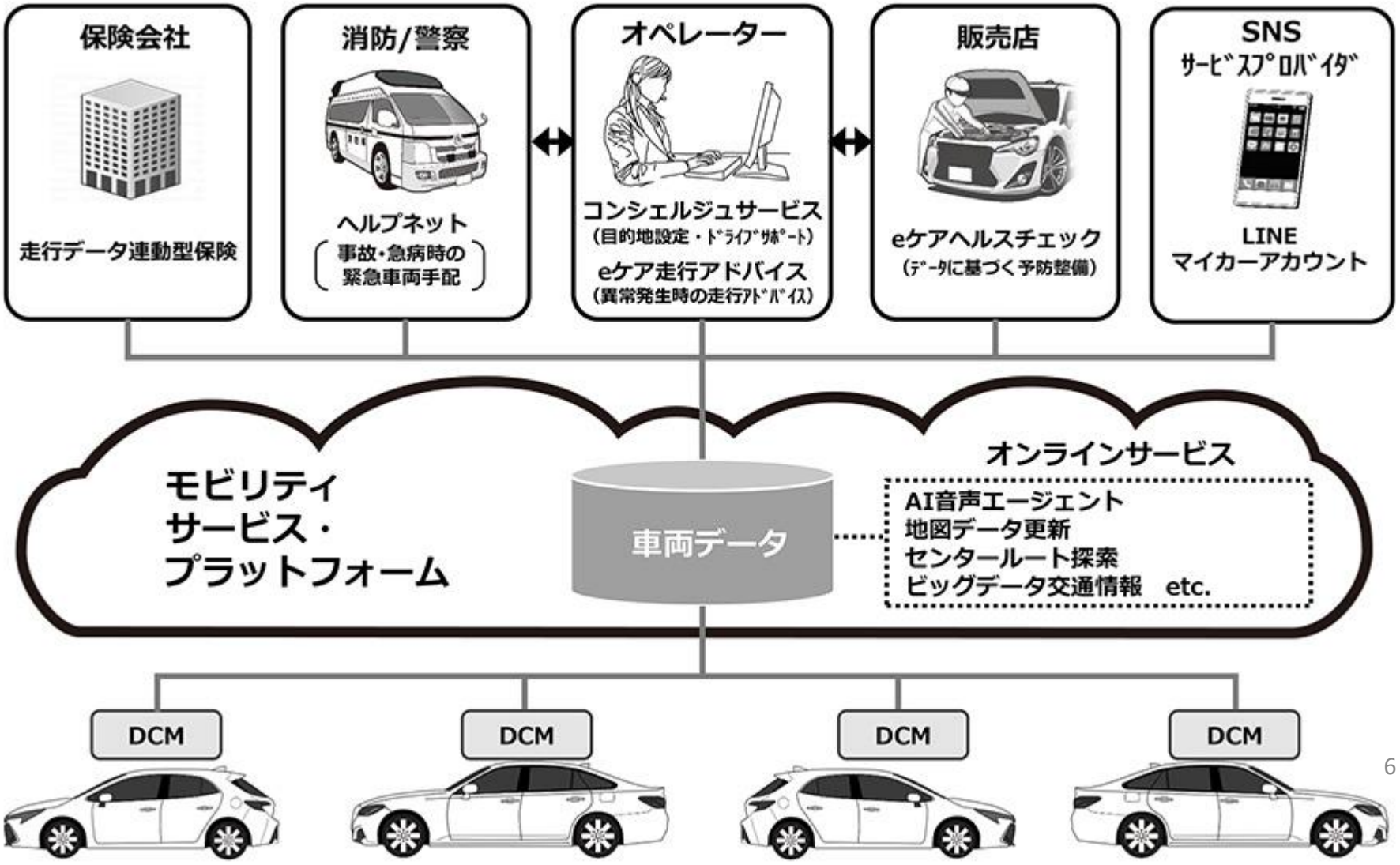
E⇒国連の2030年の持続可能性SDGsに「電動化」という新しい潮流

特に後で述べるデータセンターに直接影響するのが
C（Connected）　A（Autonomous）　S（Shared/Service）

●日本企業の取り組みトヨタ自動車

C=Connected

2018年6月26日から、車両の制御ネットワーク（CAN）に接続する車載通信機（DCM）を全グレードに標準搭載したコネクティッドカー、新型クラウン、新型車カローラ スポーツの販売を開始



運転支援と自動運転による自動走行

システムが自動的に実行！

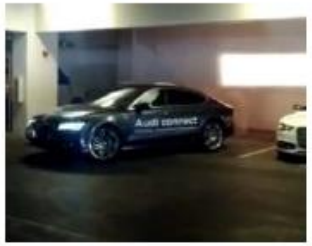
走行速度や交通環境等に応じ、さまざまな自動走行が想定される。

さまざまな走行状態

高速走行

低速走行、渋滞

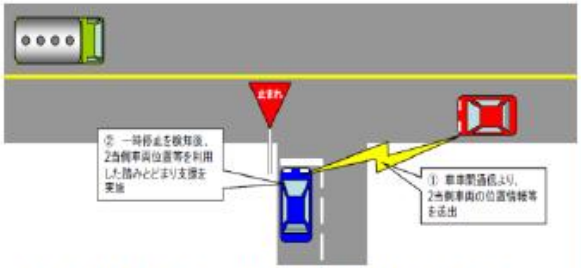
駐車



電波による「認知」

レーダによる車間距離測定（イメージ）

レーダによる周囲監視（イメージ）



車車間通信等による情報入手（イメージ）

「判断」

「操作」

【さまざまな“自動走行”（例）】

■高速道路において
- 高速走行状態での自動走行
- 低速走行状態での自動走行
- 渋滞状況下での自動走行
- 隊列走行

■一般道（混合交通）において
- 市街地での自動走行（歩行者、自転車と共存）

■駐車場において
- 自動駐車

■あらゆる状況下で
- さまざまな走行状態に柔軟に対応する汎用的な自動走行

出典：総務省電波政策2020懇談会

自動車の自動走行　A=Autonomous

自動運転のレベル0～5とは？　A=Autonomous

レベル0:　ドライバーがすべてを操作

レベル1 :システムがステアリング操作、加減速のどちらかをサポート【運転支援】

⇒・車線の逸脱を検知するとステアリングを補正、
・先行車との距離を一定に保つために自動でスピード調整をするACC（ **Adaptive Cruise Control** ）

レベル2: システムがステアリング操作、加減速のどちらもサポート【運転支援】】

自動運転システムが対応⇒ﾃﾞｰﾀｾﾝﾀｰ連携へ

レベル3 :特定の場所でシステムが全てを操作、緊急時はドライバーが操作【自動運転】

レベル4 :特定の場所でシステムが全てを操作【自動運転】

レベル5 :場所の限定なくシステムが全てを操作【完全自動運転】

２．MaaS時代とは？

●MaaS とは？

MaaSとは、Mobility as a Serviceの略で、「サービスとしての移動」

MaaS は、ICT を活用して交通をクラウド化し、公共交通か否か、またその運営主体にかかわらず、マイ カー以外のすべての交通手段によるモビリティ（移動）を 1 つのサービスとしてとらえ、シームレスにつなぐ 新たな「移動」の概念。

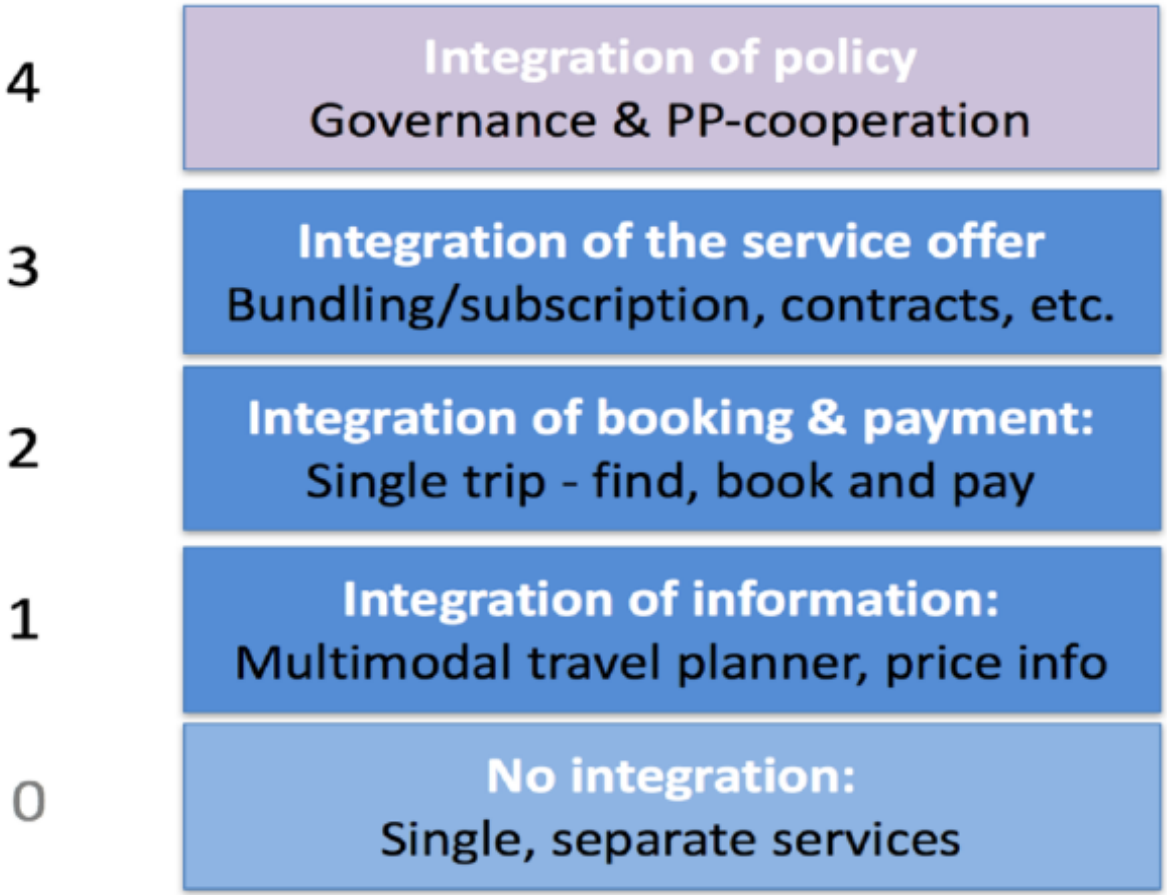
利用者はスマートフォンのアプリを用いて、交通手段やルートを検索、利用し、運賃等の決済を行う。

MaaS の定義は、発達中の新しいサービスであることから、先行している海外においても定まったものが ないのが現状で、国や研究者によっても定義内容や含まれる範囲に違いがある。

2015年のITS世界会議で設立されたMaaSAllianceでは、「MaaSは、色々な種類の交通サービスを、需要に応じて利用できる一つの移動サービスに統合することである」とされている。

●スウェーデンのチャルマース大学の研究では4段階に分けている。

レベル4 政策の統合（データ分析による政策）
レベル3 サービス提供の統合（公共交通に加えてレンタカー等も統合）
レベル2 予約、決済の統合（1トリップの検索、予約、支払）
レベル1 情報の統合（複数モードの交通提案、価格情報）



出典：https://www.mlit.go.jp/pri/kikanshi/pdf/2018/69_1.pdf

●欧州におけるMaaS の事例

○フィンランド
首都ヘルシンキで、MaaS Global 社によりMaaS アプリ「Whim」のサービスが2016 年に開始。

運輸通信省は、デジタル化、試行、規制緩和を進める目的で、交通サービス法（Act on TransportServices）を3 段階に分けて施行を予定しており、最初の道路交通分野については2018 年7 月施行。

（2017 年10 月に国会提出の第2 段階では、航空、海運、鉄道交通分野が追加される。第3 段階は、交通システム及び関連デジタルサービスを対象に予定。）

〇ドイツ
ダイムラー社の子会社Moovel が、ドイツ全土でモバイルアプリ「moovel」のサービス（予約、決済は除く）を2012 年に開始。

ドイツ鉄道（DB）が、多モードのルート･運賃情報の検索アプリ「Qixxit」を2013 年より提供。

〇イギリス
ウェストミッドランドにおいて、MaaS Global 社のアプリ「Whim」のサービスが2018 年4 月に開始。

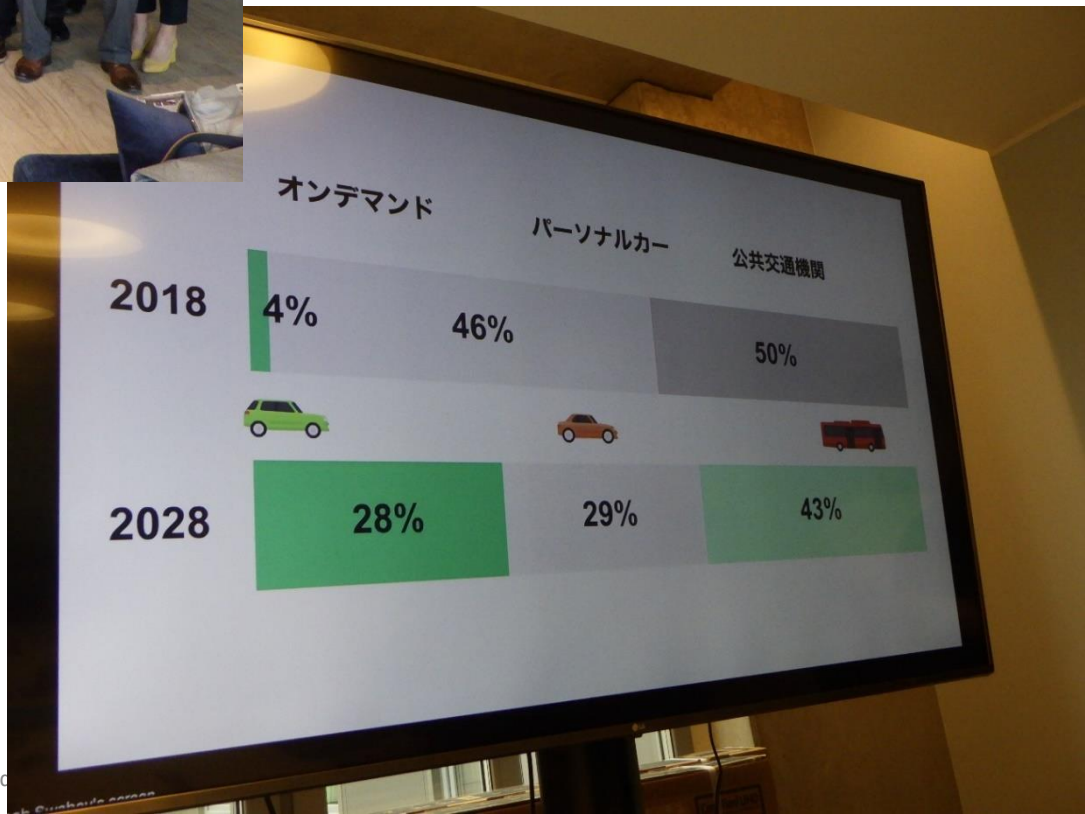
なお、上記の他にも、欧米等におけるMaaS の事例は多くある。

●2019年9月北欧調査団（エストニア発ライドシェアの雄Bolt社を訪問）
～UberやLyftと異なるエストニア流のモビリティサービス～

エストニア発ライドシェア・ベンチャー企業＝Bolt社の急成長の秘密を探る。

〇Hannah Swabey氏（法務部門・弁護士）のプレゼンテーション
Martin Villig(Founder)、Sandra Sarav（Public Policy Manager、前経済通信省）

〇かつてタリンでタクシーを捕まえるのは大変だった（今でも）
〇現在2500万人、90以上の都市、30か国以上。
〇ユニコーン（時価総額1000億円以上の未上場）の仲間入り
〇世界の交通機関の売上は12兆ドル以上（1300兆円）
〇交通機関は世界の30%の二酸化炭素を排出
〇ヨーロッパの人々は38分かけてクルマで通勤
〇人口1000人当たりエストニア534台クルマ保有/アメリカ910台保有
⇒乗っているのは5%時間だけで、95%は駐車場に停車⇒あなたは車は必要？
⇒世界のある町ではクルマの8倍の駐車場
〇オンデマンド・カー：　2018年4%→2019年28%
〇ライドシェア資金調達$：Uber=30B, DiDi21B, Grab9B, Lyft5B, OLA4B, Bolt175M
〇Boltの3年の成長：　利用者数300万→2500万、100→1000チーム、11→30か国
〇Boltはコスト競争力が高い：ドライバー収入が多い、Boltは利益を取り過ぎない
〇Boltはライドプーリング、レンタル、データビジネスへと拡大
〇Boltは歩く、ライドプーリング、電動スクータ（電動キックボード）をコーディネート



●Q&A
○なぜBoltは成功したのか？
【回答】Sandra Sarav女史
　欧州にユニコーンは、14社しかいない。ここも間もなくユニコーン。より高効率、より人員少。よりコミッション少。Back-Endの強さだ。

○競争力はどこにあるのか？
【回答】Martin Villig氏
　勤勉で優秀なエストニアで事業をタイミングよく始めたから。

○UberやLyftは、事業拡大で赤字が続いているが、Boltは？
　赤字と黒字の地域があり、うまくいっているのは、南アフリカ

○入賞は？
　フィナンシャルタイムズの急成長会社ベスト3に選ばれた。Spotifyは、企業価値で30位以内に入っている。BoltもSpotifyが見えてきた。CFOもSpotifyから来た。

●おわりに
　Boltの強みは、正にエストニアのIT分野の技術力の高さとシリコンバレーと比較して負けるとも劣らない研究開発エンジニアの優秀さと勤勉さにあると感じた。
Boltは、今後世界のライドシェア市場で目を離せない存在となるだろう。

●フィンランドのSensible4社による電気自動車自動運転バス搭乗記
～公道を自動運転車が走る時代は、もう直ぐここまで来ている！～

フィンランドは、5G分野で滅法進んでいる国に続き
自動運転の話題を提供します。そもそもフィンランドが、
MaaS（Moblity as a Service）発祥の地＊だということは、
あまり知られていない。
＊MaaS は、MaaS Global社CEOの
Sampo Hietanen氏が提唱した概念。

Sensible4社がどのような自動運転EVバスを運行し、
次なる可能性を示せるかを探る。
●自動運転車を開発するSensible4（フィンランド）
○無印良品を展開する良品計画は2018年11月1日、
フィンランドにおいて2020年の実用化を目指す
自動運転バス「Gacha（ガチャ）シャトルバス
（仮称）」に車体デザインを提供したことを発表。

○Gachaシャトルバスは、自動運転技術の研究開発を行なうフィンランドの企業
「Sensible 4」がヘルシンキ周辺の3都市「エスポー」「ヴァンター」「ハメーンリンナ」
のサポートを受け開発を進めている、あらゆる気象条件下でも機能する世界初の
自動運転バス。

〇世界でも大雨や霧、雪の気象条件下での自動運転車両の実用化には至っていないのが現状。

〇「すべての自動運転車は、実用化の前にあらゆる気象条件での走行が可能であることを証明する必要があることは明白である」として、Sensible 4は北極圏のラップランドにおいて技術テストと検証中とのこと。

●Gachaシャトルバス
〇全天候型という特徴
〇個人所有のクルマではなく地域でシェアする
　公共交通機関としての実用化をターゲット
⇒無印良品の考え方と合致するとしてSensible 4
　との共同プロジェクトを2017年からスタート。
〇前後のないミニマルでフレンドリーな形
〇照明とコミュニケーションスクリーンが一体となったLEDのライトベルト
〇内装に沿ったラウンド型のベンチシート

●フィンランドは、法律上公道を走る乗り物に必ずしも運転手が乗車している必要がなく、自動運転車の実用実験のしやすい環境にあります。

〇2019年3月実働車両のプロトタイプをヘルシンキ近郊で一般公開
〇2019年上半期内にヘルシンキ周辺の3都市「エスポー」「ヴァンター」「ハメーンリンナ」での実用試験運行を開始

●「Gachaシャトルバス」概要
サイズ：2.5×2.8×4.5m（幅×高さ×奥行き）
定員：16名（座席数10席、立ち乗り6名）
自動運転での最高速度：40km/h
駆動装置：電動（4WD）
走行距離：急速チャージで100km以上
（オプションとしてワイヤレスチャージも可能）
自動運転用のセンサー情報は、カメラ映像ではなく、
多数配置しているレーダー情報によるとのこと。

●おわりに
　初めて公道を走る自動運転車に乗車。なかなかのスグレモノ。
前方の交通状況に応じて、おとなしく運転している安全自動運転車。
Sensible4社は、フィンランドの会社らしく、社会福祉的な観点からではなく、収益事業として挑戦している。新しいテクノロジーの持っている本質を
「勝負」ではなく「意義」の中に見出そうとする人々なのだと感じた。
日本では、雪国の感じ。雪国に夏だけではなく冬に訪れると少しその土地の風土が理解できる気がする。私は、かつて2月上旬にヘルシンキに行ってマイナス30度を超える寒さを体験したことがあるが、雪国の人々が創り出したこの電気自動車バスは、日本の地方で色々展開ができそうな気がした。

●電気自動車 自動運転オペレータのRoboride社と
MaaSプラットフォーマのKyyti（クーティ）社との会合
【先端を走るフィンランドのコネクテッドカー技術】
～工場内の自動運転サービスを始動したRoboride社とは？～

MaaSの発祥の地フィンランドで自動運転をはじめとする「乗り物ビジネス」各社がどのようなビジネスモデルや分業体制のエコシステムを確立しようとしているかを探る。

そこで、今回2社を選んで会合を持った。MaaS（Mobility as a Service）とは、インターネットとモバイル通信を活用して交通をクラウド化し、公共交通か否か、またその運営主体にかかわらず、マイカー以外のすべての交通手段によるモビリティ（移動）を1つのサービスとしてとらえ、シームレスにつなぐ 新たな「移動」の概念。このMaaS分野で新たな挑戦を始めた2社。

この新たな市場には、いくつものビジネスチャンスがあるが、ここで紹介する2社の1社は、自動運転オペレータ会社でRoboride社。

もう1社は、相互に提携関係にあるKyyti社です。
今回は、Roboride社CTOのMikko Hurskainen氏とKyyti社CEOのPekka Möttö氏。
http://roboride.fi/
https://www.kyyti.com/

●ミッコ・ハルスカイネン（Mikko Hurskainen）氏プレゼンテーション概要

ハルスカイネン氏は、組み込み系技術、通信技術、ソフトウェア技術に関する研究者でソフトウェア工学の修士号を取得し、多くのアーリーフェイズのアイデアを市場に出すことが得意とのこと。

出典：http://roboride.fi/

○Roboride社のサービス

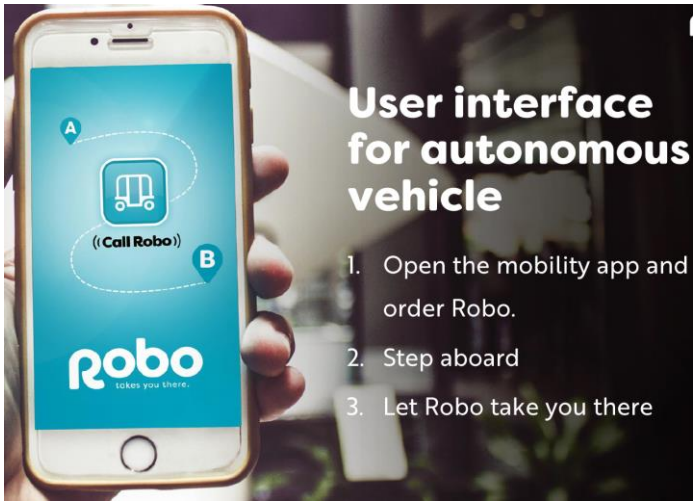
ラスト1マイルの輸送サービスで、都市化と気候変動が続く中で、化石燃料ではなく電動化が求めれている。そこで、当社は、顧客に対して1stとラストマイルの電気自動車自動運転のターンキーソリューション＊を展開。

＊ターンキー：「鍵を回せばすぐに使える」という意味の英語表現で、製品をすぐに稼働できる状態で顧客に納品すること。

我々は、顧客ニーズに対応し、特定のメーカーに束縛されずにベストなソリューションを提供する。ソリューションは、以下の構成。

出典：http://roboride.fi/

①Robo Vehicles
⇒Nice and easy to travel, Four seats, No noise, No exhaust fumes(排気ガスなし), No driver, Arrive on order and takes, 40km/h,
Personal yet public, Inexpensive, Safe
②Remote control and reacting to malfunction situations
③Maintenance and service of the vehicles
④End user application
⑤Management of payment transactions and integration of ticket



出典：http://roboride.fi/#3

〇サービス地域
世界中、最初の市場は、欧州、中国、インド

〇適用分野（対象）
①大学キャンパス⇒インドの大学の話を進めているところ
②工場⇒Pori市の銅製造所で商用パイロット実証実験を始動。世界初の自動運転サービス。
③ホリデーリゾート⇒中国の2022年北京冬季オリンピック会場の近くのHaituo Valleyのホリデーリゾートで車体数10（Fleet size 10pods）でプロジェクトを開始
⇒本プロジェクトだけでサービスエリア＝18㎞
④大病院

〇投資家へ向けてのメッセージ（モビリティ革命へようこそ）
⇒グローバルマーケット
⇒グローバル・メガトレンドが成長を支援
⇒強力な専門家集団
⇒多様なバックグランド集団
⇒スケーリングなビジネスモデル
⇒有能なサービス軌道
（competent service trajectory）

〇Robo対象車
L7タイプ
（EU規制で最大重量と乗員数に規定）
⇒現在はイギリスのメーカーから調達

〇安全テストパートナー
VTT（Technical Research Center in Finland）

●Kyyti Group(クーティグループ)CEOのPekka Möttö氏(ペッカ・モットー氏)のプレゼンテーション
日本国内のMaaS市場が活発化する一方で、MaaS発祥の地・フィンランド発の企業Kyyti Group(クーティグループ)CEOのPekka Möttö氏(ペッカ・モットー氏)が、世界で事業展開を行うKyytiグループの数々の取り組みについて話してくれた。

〇KyytiはMaaSが生まれた地であるフィンランド発の企業で、 オンデマンドのライドシェアリングサービス、フィンランド最大の自動車メーカーへの通勤サービス、公共交通機関のチケット販売の統合といった幅広い分野でプラットフォームサービスを提供しています。Business Finland＊から500万ユーロの資金援助を受け、地方の公共交通問題の解決を目指した全国規模のプラットフォーム構築を進めています。
＊Business Finland：スタートアップ支援や投資誘致などを行うフィンランド経済・雇用省傘下の政府機関。

○人材

モットー氏はKyytiについて「運輸・IT業界の経験がある人材をそろえ、輸送システムの運営やデータのモデリングについての経験を最大限高いレベルで融合させた企業だ」とし、プラットフォームを提供する企業で、MaaSプレイヤーではないとのこと。

出典：http://www.truck-x.com/wp/wp-content/uploads/2019/06/NextVehicle19.pdf

○海外展開

Kyytiはフィンランド国内で郊外でのMaaS事業支援に取り組んでいるほか、オランダでは運輸省と連携して総額4,000万ユーロ（50億円）の大規模なパイロット事業を展開。

Kyytiのビジネスを行う地として注目しているのは欧州だけではなく、アメリカ・カリフォルニア州で2019年にMaaS & DRT(デマンド型交通)プロジェクトを立ち上げ、MaaS関連のテクノロジーを活用する事業を展開。注目すべき市場として日本を取り上げ、フィンランドを除けば、MaaSに一番関心を寄せているのは日本だとし日本市場への進出に強い意欲を見せていた。

〇なぜMaaSか？

フィンランドでも人口密度の低い地方では路線バスのような公共交通が整備されておらず、通学、通院、介護施設への往復など、生活維持のために必要となる移動については国や地方政府の負担で必要最低限の移動サービスが提供されている。しかし、多くの車両が乗客1名という非効率で、
国や地方政府の財政負担が重く、MaaS（Mobility as a Service）などを
活用した新しい社会システムによる課題解決が求められている。

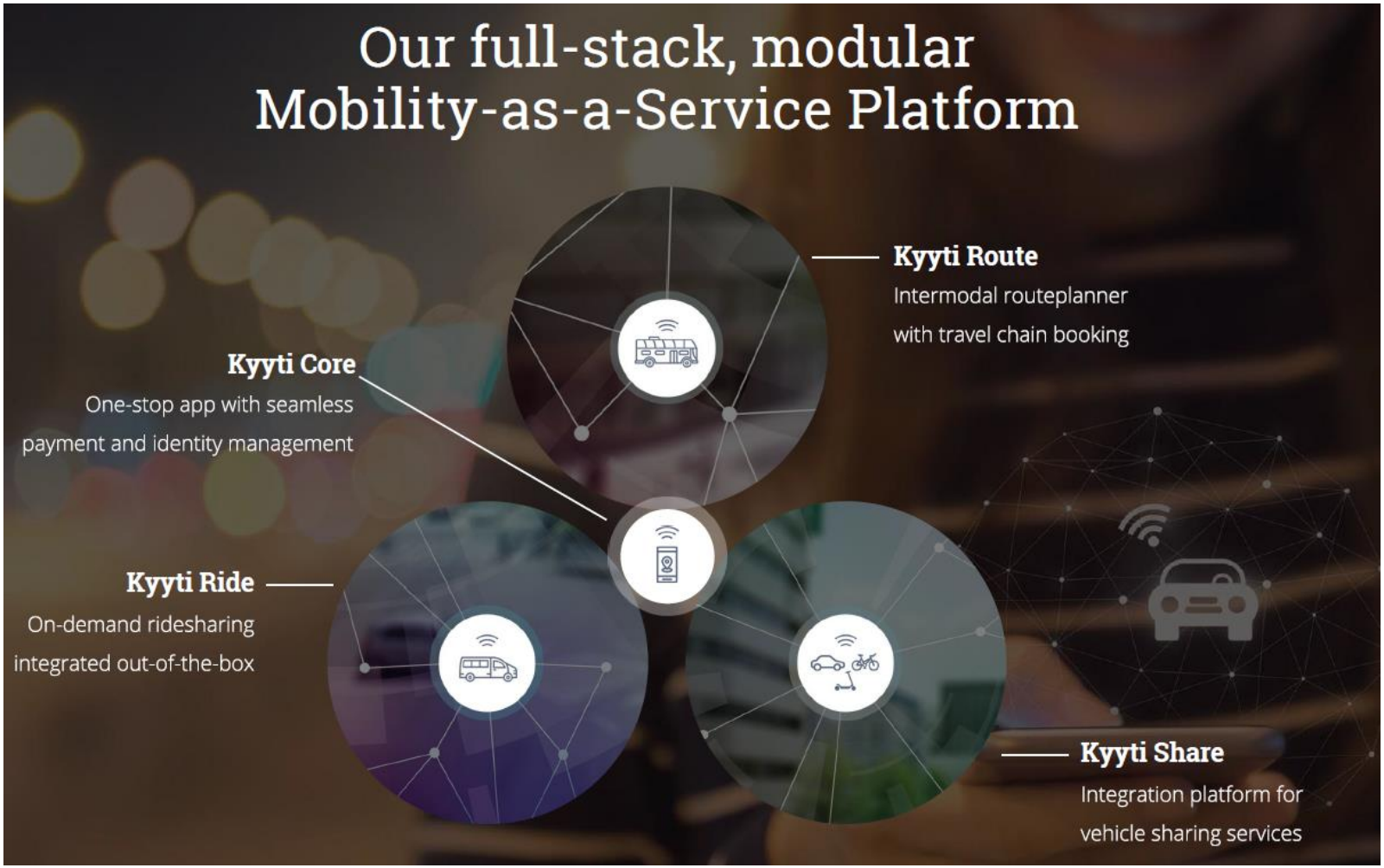
〇沿革

Kyyti社は2016年からフィンランドでモビリティサービスのプラットフォームを提供しているスタートアップ企業、同社が提供する地方版MaaS（rural MaaS）プラットフォームは、完全に自動化された配車システムを
交通事業者に提供し乗客はスマホまたは電話で乗車予約ができる仕組み。

フィンランドでは、病院、学校、介護施設などの送迎客は税金で移動費の大半が賄われることから約5€（500～600円）でタクシーに乗車できるが、一般客は同社のシステムを使うことで送迎客とのライドシェアが可能となり、安価でタクシーを利用できるようになった。交通手段が限られている地方において、異なる目的の利用客を統合することで効率的な交通システムを実現した画期的なサービスで、地方版MaaSの導入で、タクシーの一人乗り乗車が減少し、国や地方政府の財政負担が抑制されるとのこと。

○Kyyti社のプラットフォームの概要（4つから構成）

- Kyyti Core：ワンストップ・シームレス決済、ID管理
- Kyyti Ride：オンデマンドライドシェア
- Kyyti Route ：トラベルチェーンに基づくモーダル内のルーティング
- Kyyti Share：ライドシェア用の統合プラットフォーム



出典：Kyyti社

●Q&A
Q:Roboride社の仕組みを1台導入するとコストは？
A:10000€（120万円）/月と高いが、バスと運転手を雇うより安い

Q:事故が起こった時の責任は？
A：Roboride社の責任

Q:銅工場の例では客は乗るだけで何もしなくてよいのか？
A:受付があって受付がロボを呼んでくれる。元来エスコートなしでは動けなかった客への対応が便利になったと評判

Q:電気自動車はどこから買っている？
A：イギリスのアウリゴ（Aurrigo）社製造https://aurrigo.com/

Q:クルマは購入？リースにしないのか？
A：今は購入している。

Q:日本の高齢化・過疎化地域に向いていないか？
A:日本もフィンランドも過疎化問題は同じ。運転手なしが重要。タクシーは運転手がいるので人件費で難しい。自動運転は、公道がまだ現実的ではない。だから工場などに市場を絞っている。

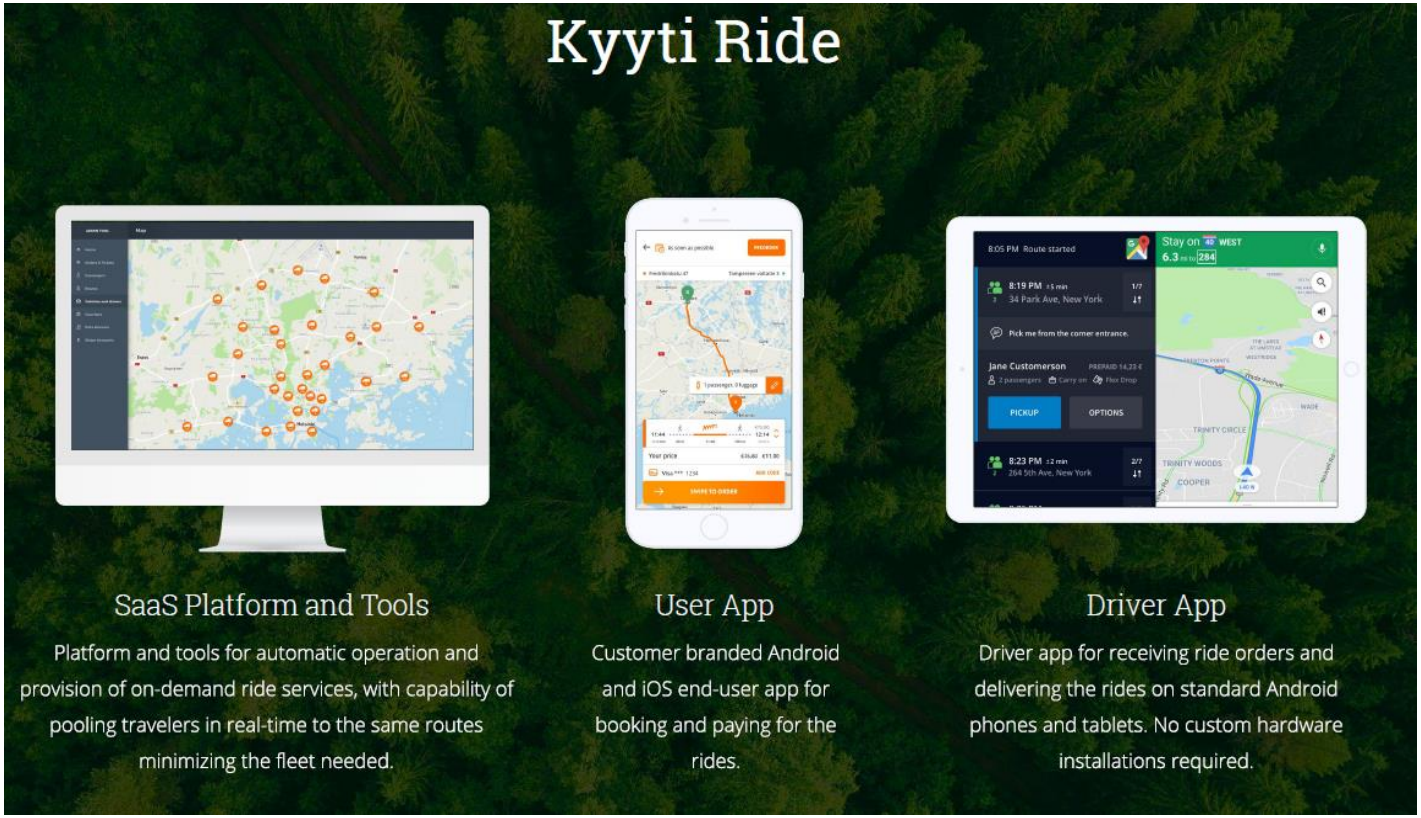
Q:Sensible4はライバルか？
A:競争ではなく共存だと考える。プラットフォームを共通化し市場を分けるなどできる。フィンランドは、規制緩和があり、MaaSは、やり易い国。

Q:Roboride社の強みは？
A：以下の3点
① 車両の検討能力・知識がある。
② 中身を作れる
⇒自動運転ソフトウェアをロボクラウドに置いておく
⇒モニタリング
⇒フリート管理（艦隊の意味、ひいては車両管理）。
③ 自動運転検討能力
⇒自治体のニーズが高いがテクノロジーがない。

Q:制御システムのノウハウは特許化しているのか？ディープラーニングを適用しているのか？
A:全体のパッケージを作っているのが強み。MaaSプラットフォームは、Kyyti社製。自動運転のノウハウはフィンランドにたくさんあり、パートナー企業と協力している。深層学習まではやっていない。

Q:Kyyti社は、何でビジネスをするのか？
A:MaaSプロバイダーではない。プロバイダー用のプラットフォームの提供が仕事。自治体や市に使ってもらう。でも1社独占はよくない。

Q:マルチモーダルとは？
A:路面、天気、年齢に応じたり、景色の良いルートを選ぶなど。よりパーソナライズされたもの。オランダでは、気象条件と組み合わせたところ。現状は、時刻と地図情報が主体でモードを選ぶ。



出典：Kyyti社

●おわりに

MaaS プラットフォームの位置づけが2人の話から明確になった。すなわち、路線検索機能、サービスの統合、決済の機能。現在世界各国で交通システムの見直し要求。その方向性の１つが、公共交通とタクシーの間を埋めるオンデマンドシェアライドシステム。そこには、情報収集とデータ分析が必須となる。日本では、自動車のことは自動車会社の仕事だと思われがちだが、クルマを作ることとクルマを使うことは全くの別物だ。

KyytiのCEOのペッカ・モット一氏は、MaaS 分野に進出する前に都市間 のバスサービスでの成功体験。かつてフィンランドでは鉄道もバスも高価で都市間の公共交通を使うよりも自家用車移動の方が圧倒的に安価だった。

2012 年に規制緩和が行われたことを契機に、新しいバスサービスに参入することとし、ONNI BUSという柔軟な価格設定でイン ターネットにて予約可能なフィンランド初のバスサービスを導入。モット一氏の尽力で、ONNI BUSは結果として市場の50%以上を占有することができ、長距離バス会社の独占を覆すことに成功。今では大都市間を自家用車よりも鉄道やバスで移動するほうが安価に。新しいモビリティサービスが、世の中に実際に変化をもたらすことが可能であることことがわかってきた。

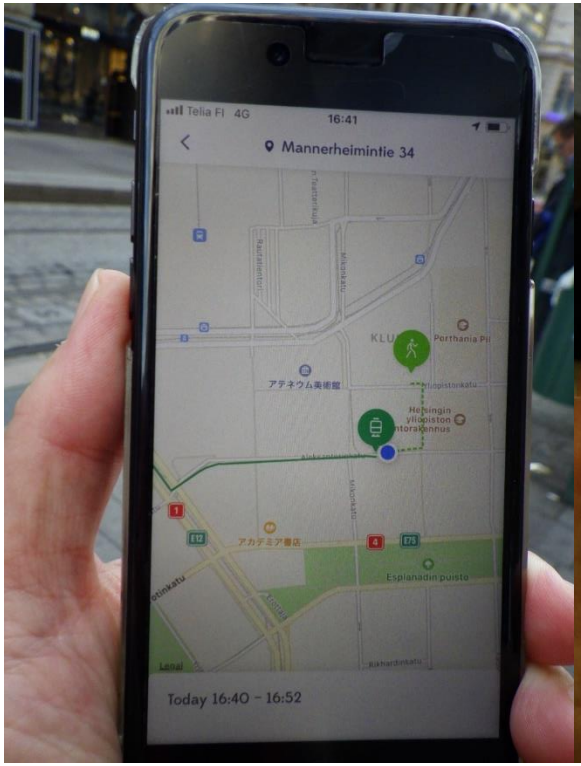
かつての ビジネスモデルでは旅行代理店や切符売り場などの物理的な場所を保有していないと顧客との接点を持つことができなかったが、ITを活用すれば、顧客との接点を持つことが可能になったことでMaaSの未来へつながるだろう。

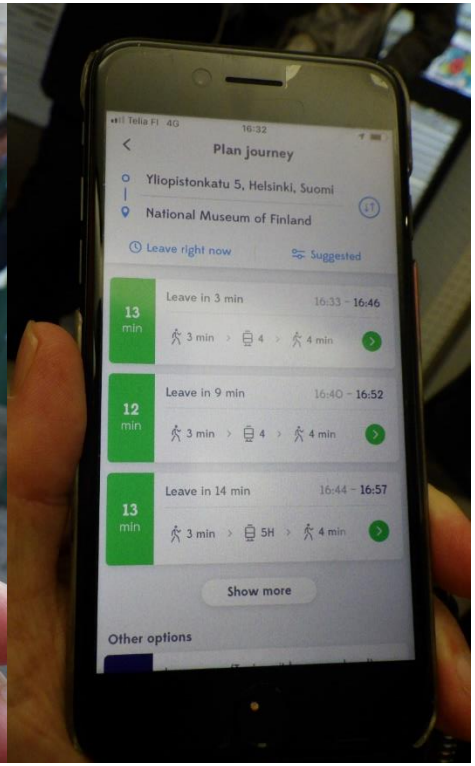
●ヘルシンキ名物MaaSアプリWhimで路面電車に乗って市立図書館へ

iPhoneアプリWhimをダウンロードして路面電車代を支払うと電車にも乗れて目的地までの交通手段を徒歩も含めて所要時間と時刻表も併せて教えてくれる。そして目的地の何ともモダンなヘルシンキ市立図書館を訪ねてWhimのアドバイス通りに次は、7番の路面電車に乗って帰ってきた。

Whimは、私たちの生活を根本から変えてしまう自家用車をなくしてしまう世界初の先進的なMaaS（Mobility as a Service）で、ベンチャー企業「MaaS Global」がサービスを提供している。

Whimは、2016年にヘルシンキにて実証実験を行った後、正式にサービスを開始。毎月定額もしくはその都度お金を払ってポイントに換え利用することで、いくつかの交通手段から最適な移動ルートを自動検索し、私たちを目的地まで運んでくれる。予約から決済まで一括して行え、利用できる交通手段は、電車やバスのほか、タクシー、バイクシェアなど。ユーザーがスマホアプリを提示するだけで、交通手段を利用できる。





●日本国内

○JR東日本

2017 年9 月、交通事業者、国内外メーカー、大学、研究機関などが参加、連携し、社会課題の解決に取り組むことを目的に、「モビリティ変革コンソーシアム」を設立。3 つのワーキング・グループ（WG）を設置し、Door to Door 推進WG において都心地域等におけるマルチモーダル・サービスを検討。

○小田急

2018 年4 月、「中期経営計画」で、次世代モビリティを活用したネットワークの構築で将来像に「多様なモビリティサービスを1 つのサービス（MaaS）として利用者に提供」との文言を盛り込む。MaaS の発展に、基本サービス（経路案内、運行情報、予約・決済）＋付加的サービス（ホテル・商業などの情報・手配）を記載。

●MaaS に関連する要素とは？
MaaS に必要な要素としては、交通機関の運行等の情報や、運賃・料金の設定及び決済があげられる。

〇公共交通機関の運行情報等
　MaaS では、ICT により鉄道、バス等の経路、時刻表等のデータを検索し組み合わせ、利用者のニーズに合うサービスが提案される。

⇒検索対象となる交通機関の運行情報や、駅等の地理的情報等のデータを利用できる必要があり、欧米ではオープンデータとして整備されている。

⇒日本では2015 年9 月に公共交通オープンデータ協議会が設立され、「公共交通分野におけるオープンデータ推進に関する検討会」が検討を進めている。

⇒同検討会の「中間整理」（2017 年5 月）において、「諸外国においては、ICT 技術の進展、MaaS（モビリティ・アズ・ア・サービス）の考え方の広まり等から、公共交通分野におけるオープンデータが推進されている。我が国もこうした動きをとらえ、2020 年東京オリンピック・パラリンピック競技大会を見据え、積極的にオープンデータ化に取り組むべきであり、データを保有する交通事業者は、オープンデータの推進を自らの成長戦略の大きな柱と位置づけ、率先して取り組むことが望まれる。」とされている。

〇運賃・料金の設定、決済

MaaS の運賃・料金支払は、欧米ではキャッシュレス決済されている例が多い。

運賃・料金の体系も、利用都度毎の決済の他に、定期券のように月単位の定額料金制プランを設定しているサービスもある。

⇒日本では、2001 年のJR 東日本によるSuica をはじめとして交通系IC カードが普及。

⇒「交通政策基本計画」（2015 年2 月13 日閣議決定）においても、「交通系IC カードの利用エリアの拡大や事業者間での共通利用、エリア間での相互利用の推進策を検討する」とされており、IC カードの普及・利便拡大に取り組んでいる。

⇒サービスが提供されるエリアは交通状況に応じ様々な範囲が考えられるので、交通系IC カード利用について検討が必要となる。

● 日本政府の取組方針

2018 年6 月15 日に閣議決定された「未来投資戦略2018」中で、MaaS は自動運転とともに以下のように記述されている。

（1）「自動化」：次世代モビリティ・システムの構築<公共交通全体のスマート化>
「MaaS（Mobility as a Service）などの施策連携により、利用者ニーズに即した新しいモビリティサービスのモデル都市、地域をつくる。」

（2） 政策課題と施策の目標
「自動運転及び交通全体の統合サービス・プラットフォームを含む「次世代モビリティ・システム」の実現に向け、施策を展開していく」
「自動運転のみならず様々なモビリティ手段の在り方及びこれらを最適に統合するサービス（MaaS（Mobility as a Service））について検討を進める。」

（3） 新たに講ずべき具体的施策（次世代モビリティ・システムの構築に向けた取り組み）
「・地域の公共交通と物流について、オープンデータを利用した情報提供や経路検索の充実、スマートフォンアプリによる配車・決済等のICT、自動走行など新技術の活用、見守りサービスや買い物支援の導入、過疎地域での貨客混載、MaaS の実現など多様な分野との施策連携により、都市と地域の利用者ニーズに即した新しいモビリティサービスのモデルを構築する。」

「・様々な交通サービスをデータでつなげて新たな付加価値を生み出すモビリティサービス等（MaaS）の促進について、オンデマンドなどのサービス高度化、API 等によるデータ連携・プラットフォーム、対応する制度の在り方などについて、検討を行う。」

●クルマの需要は個人中心から法人中心に【モビリティサービス】

○クルマを所有するという形態ではなく、安くて便利に利用できるサービス（ライドシェアや配達代行サービス）が広がる

○ライドシェア用アプリで素人がプロドライバー並みの仕事へ

⇒どこに行けば乗客がいるのか

⇒どのルートで走れば目的地に効率的に行けるのか

⇒料金計算や支払い手続きを短期間で習得

⇒コネクティッド化や自動運転化、電動化の進展によって運転手の機能を補完・代替し、コスト優位性と付加価値増大

○ネットワーク外部性（ネットワーク型のサービス利用者が増えると、より多くの相手と連絡をとれるようになり便利に）により、安くて便利なサービスを利用する人が増えれば増えるほど、利便性が向

○所有から利用でクルマ自体の需要は個人中心から法人中心へ

○移動コスト：4$/mile（所有）⇒0.4$/mile（2030年） Shared/Service

●クルマの需要は個人中心から法人中心に【モビリティサービス】

ネットワーク外部性（ネットワーク型のサービス利用者が増えると、より多くの相手と連絡をとれるようになり便利に）により、安くて便利なサービスを利用する人が増えれば増えるほど、利便性が向上

多方面で多様な市場が生まれ、それらが結びついていくことによってネットワーク外部性がさらに高まる「マルチサイドプラットフォーム型モビリティサービス」へと進化

モビリティサービスが普及すると、安くて便利なタクシーやバスが増えていくため、クルマ自体の需要主体は個人中心から法人中心へ変化

クルマの販売台数や利益が減る方向に構造変化

収益源も車両の製造・販売からサービス側にシフトし業界構造や交通・社会インフラにも影響を与えるほどの破壊的変化を引き起こす。

●モビリティビジネスのグローバル市場規模は約550兆円の変化

⇒車両販売による収益＝約330兆円

⇒各サービスの収益（平均利用年数10年）＝約220兆円

⇒保険、ファイナンス、メンテナンス、リユース、エネルギー管理

⇒コネクティッド化が先行し、保険、メンテナンス、ファイナンスなど新しいビジネスが生まれ、既存のクルマもコネクティッド化し、2030年頃には世界で10億台規模へ

CASE時代に対応した5Gデータセンターにおいて
MaaS（Mobility as a Service）サービス事業者
・付加サービス事業者が相互接続へ！

３．CASE/MaaS時代のサイバーセキュリティとは？

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）

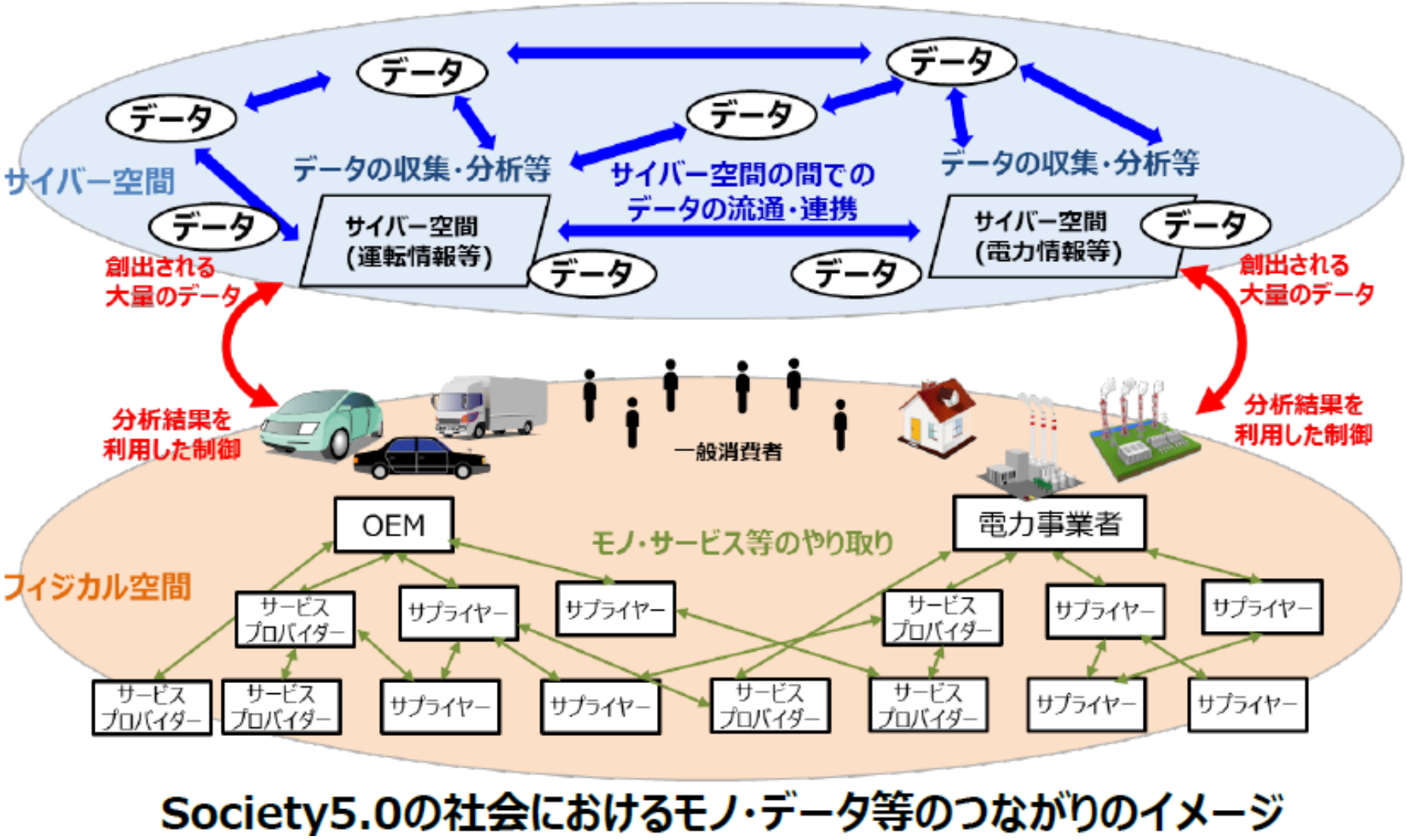
⇒2019年4月経済産業省商務情報政策局サイバーセキュリティ課

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）の概要

サイバー空間とフィジカル空間が高度に融合した「Society5.0」の到来

- 我が国では、**サイバー空間とフィジカル空間を高度に融合**させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会**「Society5.0」**の実現を提唱。
- **「Society5.0」では、付加価値を創造するための一連の活動（サプライチェーン） の形態が、より柔軟で動的なものに変化。**この**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。
- 一方で、**サイバー空間とフィジカル空間の融合により、サイバー攻撃の脅威が増大。**

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf



Society5.0の社会におけるモノ・データ等のつながりのイメージ

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

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
サイバー空間の融合
⇒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

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

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）の目的と適用範囲

- 「Society5.0」の実現へ向けて、**産業構造、社会環境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**するとともに、産業界が自らの対策に活用できる**セキュリティ対策例をまとめた、『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）』を策定する。**
- 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。

CPSF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

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

CPSFの想定読者、全体構成

- CPSFは、産業社会の全体像を捉えたものであるため、**バリュークリエイションプロセスに取り組むすべての主体が適用対象。**
- **技術等の変化に伴う見直し等も考慮し、三部構成（コンセプト、ポリシー、メソッド）を採用。**

想定読者	第Ⅰ部【コンセプト】	第Ⅱ部【ポリシー】	第Ⅲ部【メソッド】
• CISO（Chief Information Security Officer; 最高情報セキュリティ責任者）	○	○	
• サプライチェーンマネジメントに関わる戦略・企画部門の担当者	○	○	
• バリュークリエイションプロセスに関わる企業・団体等のセキュリティ担当者		○	○
• 情報関連機器、制御系機器の開発・品質保証、システム設計・構築・検証担当者		○	○
• データマネジメントの担当者		○	○
• 各産業分野におけるセキュリティ対策のガイドライン等を策定する業界団体等の担当者	○	○	○

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

CPSFに期待される効果・特徴、使い方

- CPSFを活用することで期待される効果。
  - セキュリティ対策の実行による**バリュークリエイションプロセスの信頼性の確保**
  - 製品・サービスのセキュリティ品質を差別化要因（価値）にまで高めることによる**競争力の強化**
- CPSFは、「Society5.0」という新たな産業社会において、付加価値の創造に取り組む主体が、その活動に必要なセキュリティ対策を講じようとする際に参照されることを想定。
- 一方、業界や企業により、**守るべき資産、人的・資金的リソース、又は許容できるリスク等は異なる**ため、以下の内容を参考に本フレームワークを利用することを期待。

リスク源の洗い出し

第Ⅱ部、添付A、添付B

- 三層構造モデルを参考にし、企業等の付加価値の創造活動におけるモデルを構築
- 企業等のリスク源の明確化

企業等におけるセキュリティポリシーの策定及び対策の実装

第Ⅲ部、添付C

- 第Ⅲ部、添付Cを参考に、自組織におけるセキュリティポリシーの策定及びセキュリティ対策の実装
- 国際標準等との比較

企業等、業界等における信頼のチェーンの構築への活用

- リスク源を洗い出し、セキュリティ対策を実施することで、一つ一つのバリュークリエイションプロセスの信頼性を確保
- 上記取組をつなげることで信頼のチェーンを構築。

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

第Ⅰ部　コンセプト：

サイバー空間とフィジカル空間が高度に融合した産業社会における産業分野のサイバーセキュリティの在り方

”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
～三層構造と６つの構成要素～

- 従来のサプライチェーンでは、セキュリティ対応をしっかりと行った主体間で行われる取引であれば、そのプロセス全体のセキュリティが確保される。
- 一方、「Society5.0」では、従来のサプライチェーンのように、**組織のマネジメントの信頼性にのみ基点を置くことでバリュークリエイションプロセスの信頼性を確保することは困難。**
- こうした、従来のサプライチェーンの活動範囲から拡張された付加価値を創造する活動のセキュリティ上のリスク源を的確に洗い出し、対処方針を示すためのモデルが必要。

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

三層構造モデル

バリュークリエイションプロセスが発生する産業社会を、３つの「層」で整理。

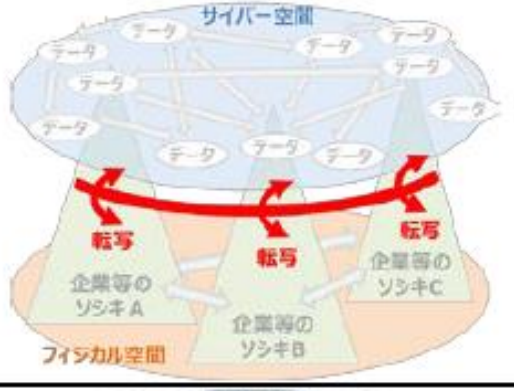
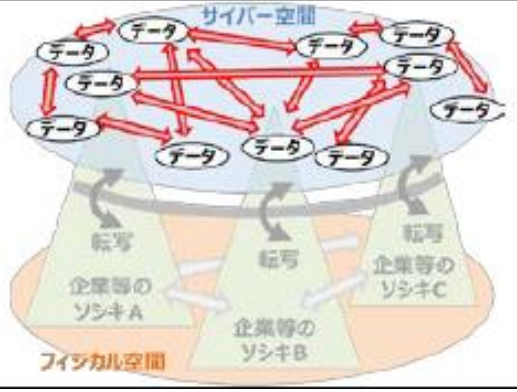
第1層：企業間のつながり
第2層：フィジカル空間とサイバー空間のつながり
第3層：サイバー空間におけるつながり

６つの構成要素

バリュークリエイションプロセスに関与する構成要素を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

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

三層構造	概念図
第1層	
第2層	
第3層	

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

三層構造アプローチの意義

～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の設定～

- **三層構造モデル**では、『Society5.0』における新たなサプライチェーン、**バリュークリエーションプロセスの信頼性の基点を的確に設定するために、産業社会を３つの「層」で整理。**
- 各層における信頼性の基点は以下のとおり。
  - **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、**要求される情報の正確性に応じて適切な正確さで情報が変換される“転写”機能の信頼性**
  - **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**

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

サイバー空間におけるつながり
【第３層】

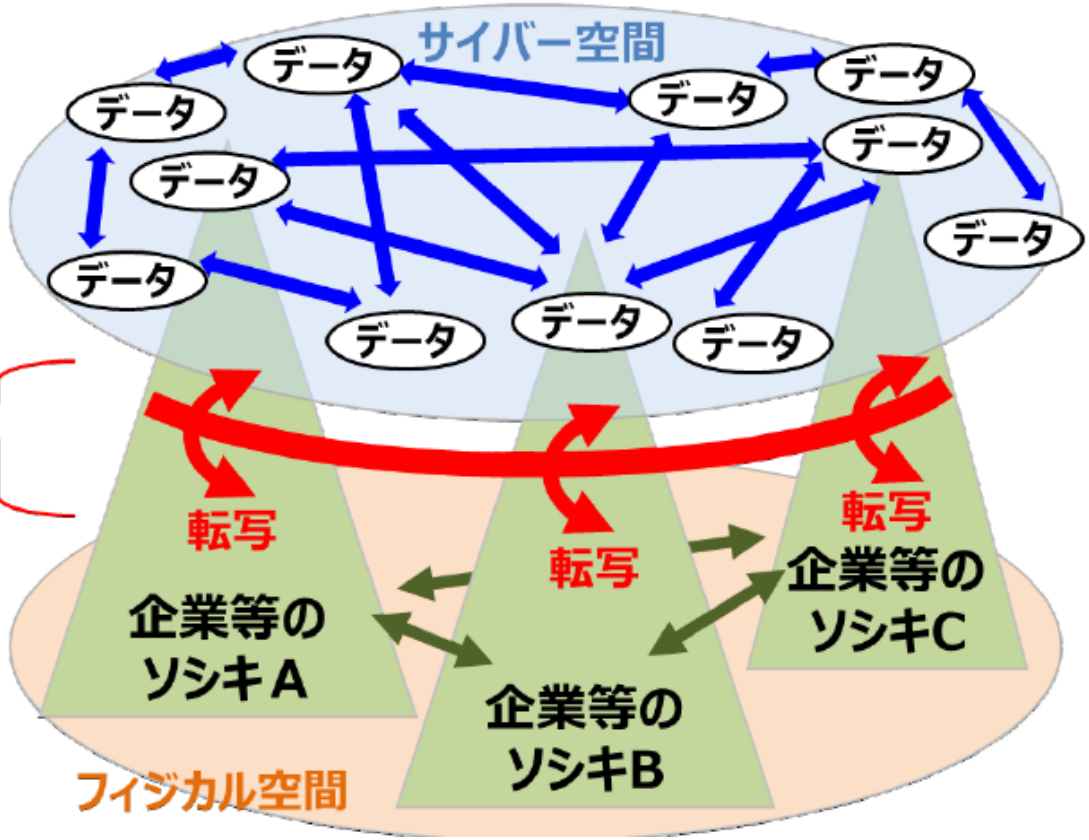
- 自由に流通し、加工・創造されるサービスを創造するためのデータの信頼性を確保

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



出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

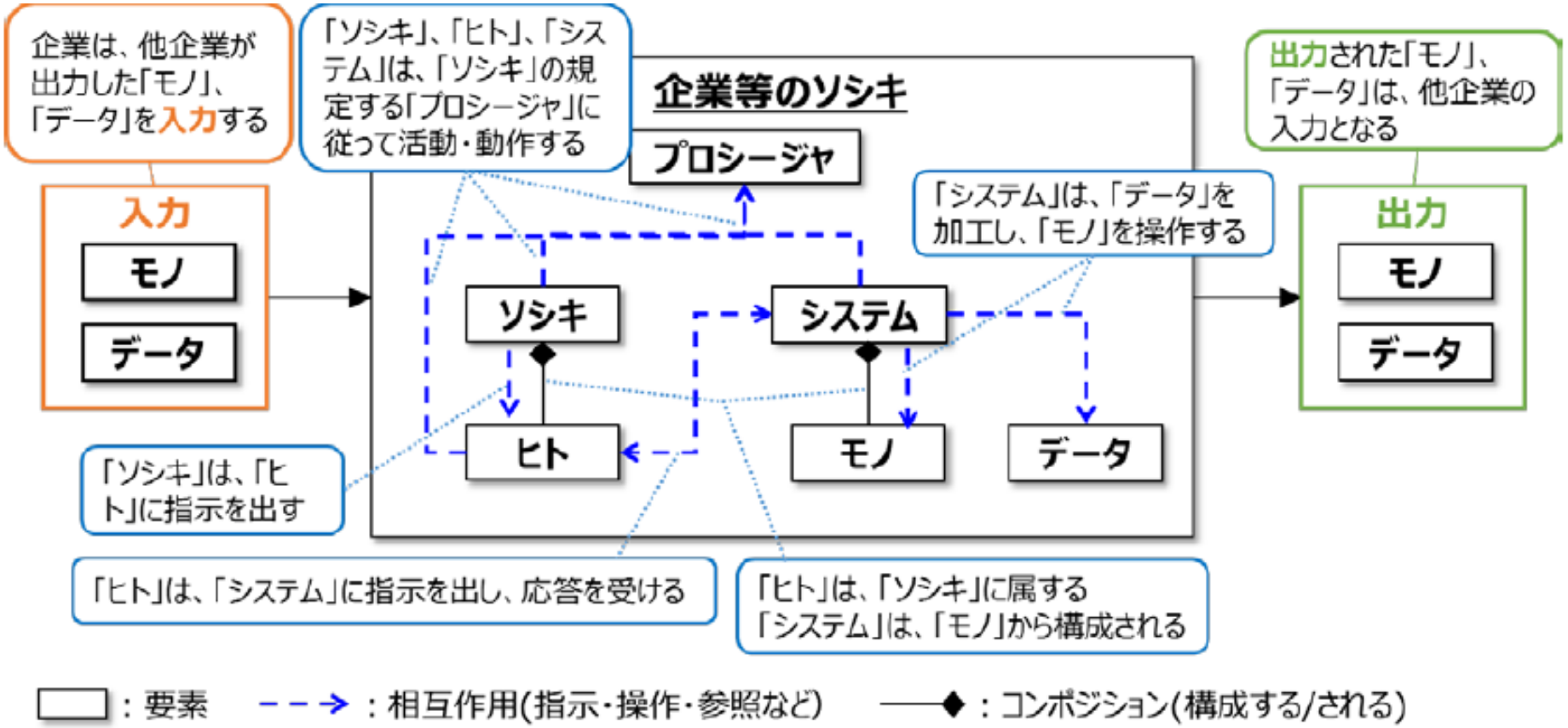
６つの構成要素

～動的で柔軟なバリュークリエイションプロセスを捉えるための構成要素～

- バリュークリエイションプロセスは、**動的に柔軟に構成されることから、資産を固定的に捉えることが難しく、構成要素について一定の抽象化を行って捉えることが必要。**
- このため、セキュリティ対策を講じる上で最適な最小単位として、**６つの構成要素で整理。**

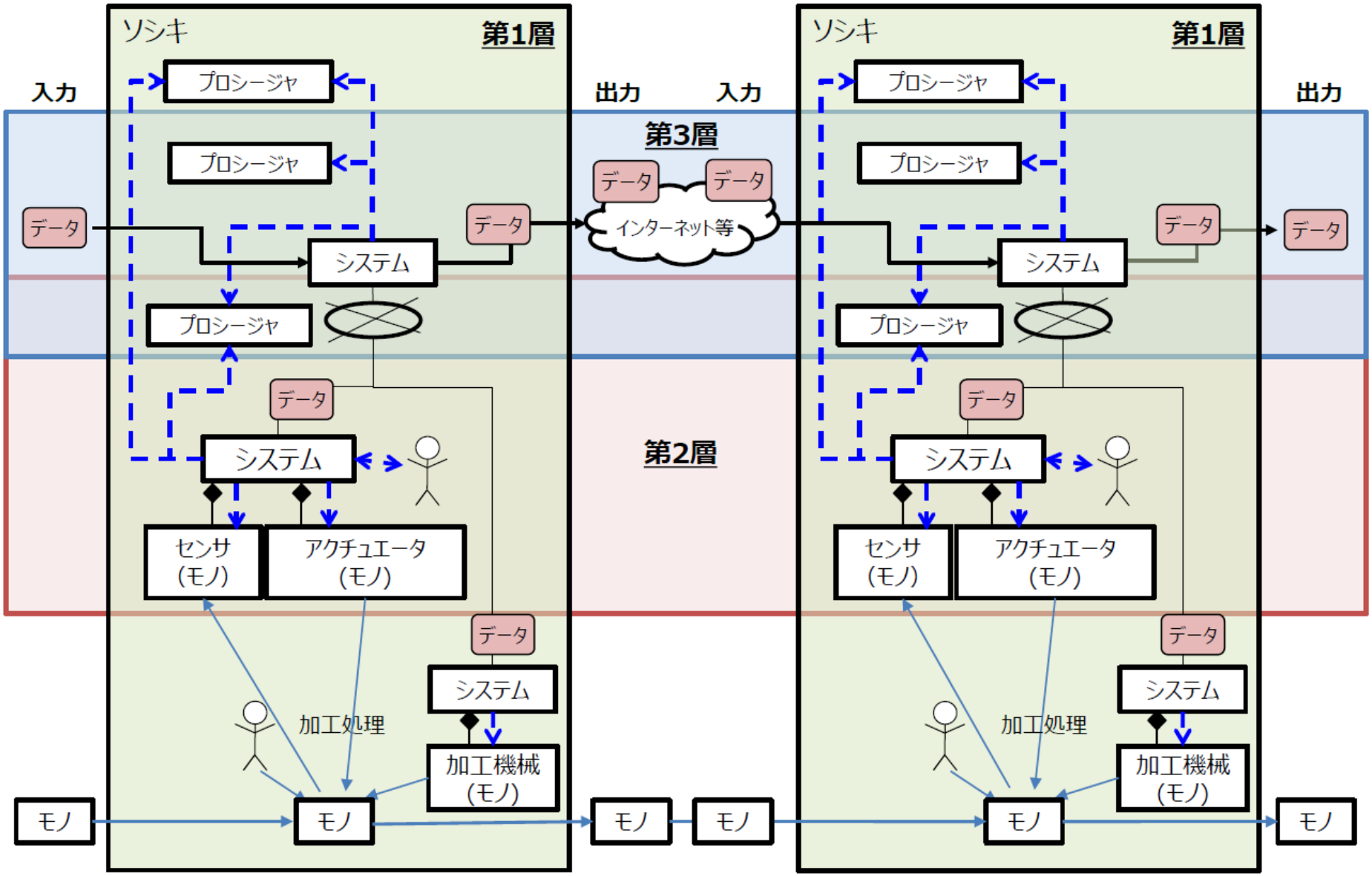
構成要素	定義	構成要素	定義
ソシキ	• バリュークリエイションプロセスに参加する企業・団体・ソシキ	**データ**	• フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
ヒト	• ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人	**プロシージャ**	• 定義された目的を達成するために一連の活動を定めたもの
モノ	• ハードウェア、ソフトウェア及びそれらの部品操作する機器を含む	**システム**	• 目的を実現するためにモノで構成される仕組み・インフラ

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf



出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

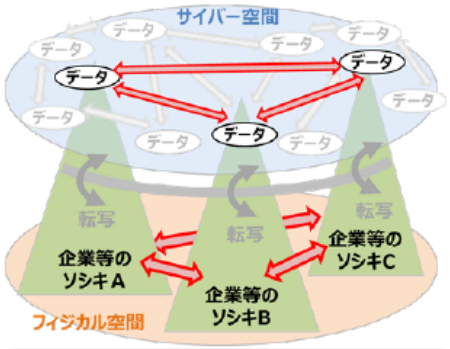
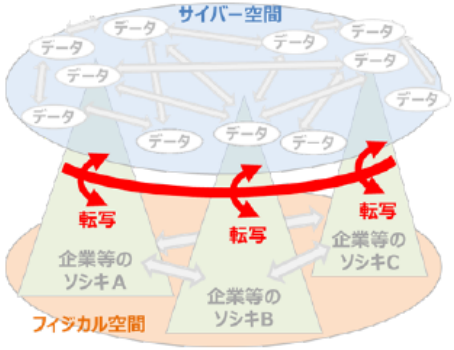
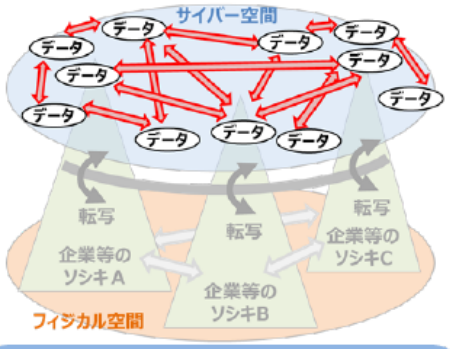
三層構造における6つの構成要素の関係



出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

CPSFの全体概要（リスク源と対応する方針の整理）

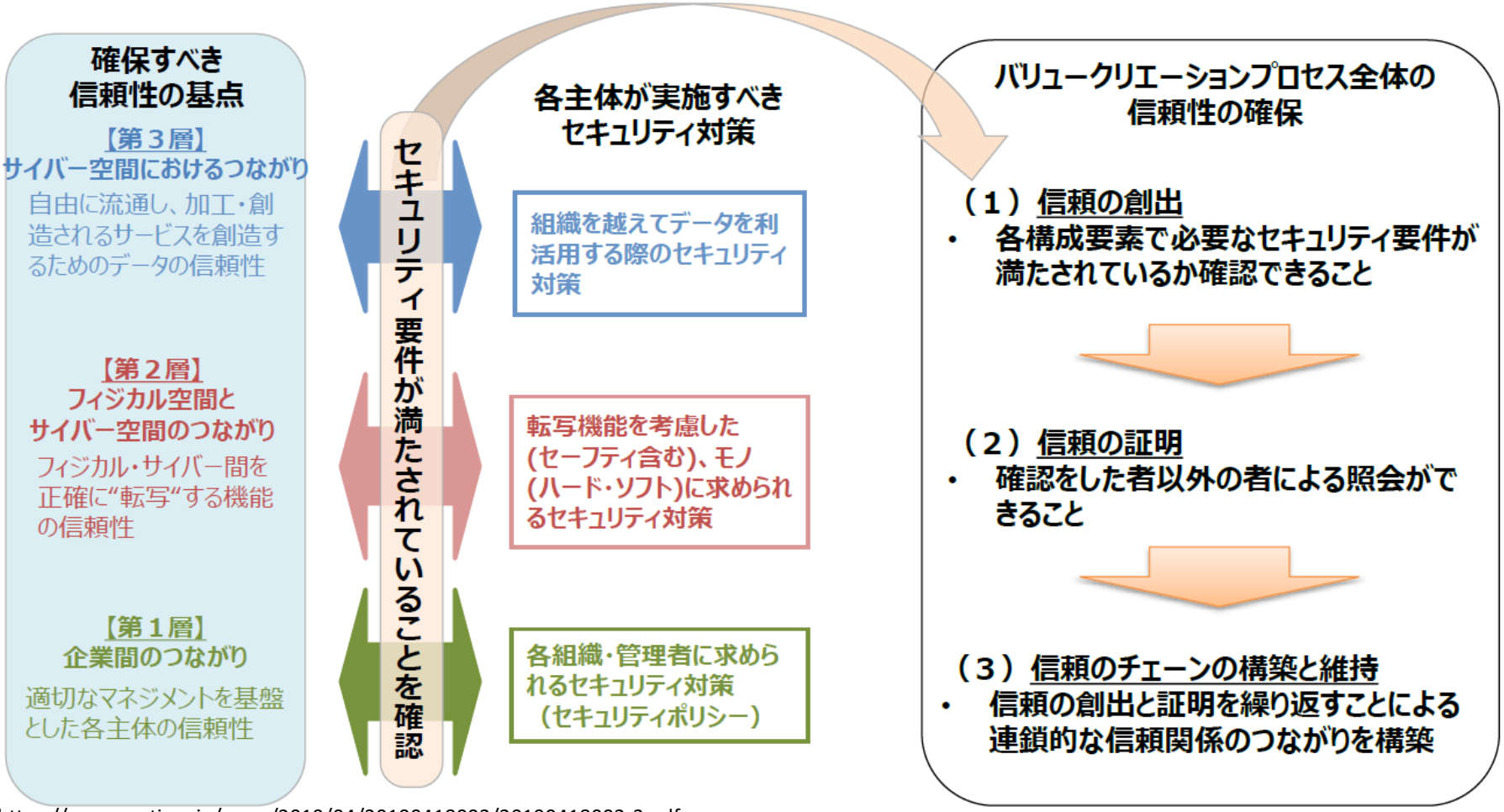
- 各層における機能、セキュリティインシデント、リスク源、対策要件を整理。

	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
セキュリティインシデント	• 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（構成要素ごとに整理）	• 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	■ 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

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

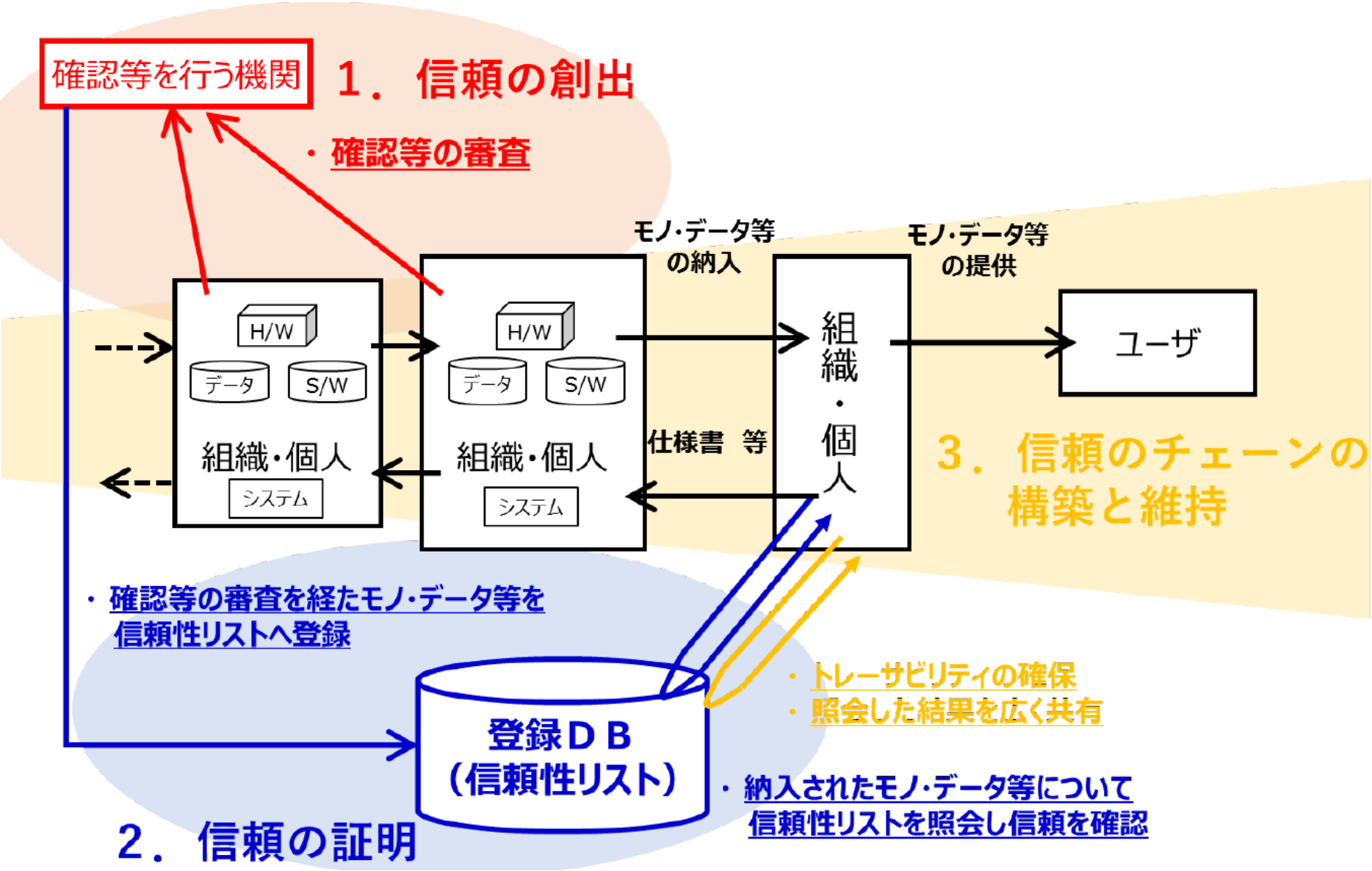
CPSFにおける信頼性の確保の考え方

- 各構成要素について必要なセキュリティ要件が満たされていることを確認し(**信頼の創出**)、確認した主体以外の者による照会ができるようにし(**信頼の証明**)、それを繰り返し行い、広く共有して**信頼のチェーンを構築、維持**することで、**バリュークリエイションプロセス全体のセキュリティを実現**することになる



出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

信頼の創出、信頼の証明、信頼のチェーンの構築と維持の関係のイメージ



出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

第Ⅱ部　ポリシー：　リスク源の洗い出しと対策要件の特定
三層構造モデルと６つの構成要素を活用したリスクマネジメント

- リスクマネジメントにおける標準的なプロセス（例：JIS Q 31000:2010, JIS Q 27001:2014）も踏まえ、**CPSFに基づくセキュリティリスクマネジメントの流れを整理。**
- **三層構造モデル、6つの構成要素の考え方を活用し、バリュークリエイションプロセスの特徴をとらえたセキュリティリスクマネジメントが可能。**

セキュリティ・リスクマネジメントの流れ

1. 分析対象の明確化
2. 想定されるセキュリティインシデント及び事業被害レベルの設定
3. リスク分析の実施
4. リスク対応の実施

CPSFの考え方を踏まえたリスクマネジメントで考慮すべき観点

① バリュークリエイションプロセスに関わるステークホルダーとの関係

② IoT機器を介したサイバー空間とフィジカル空間の融合

③ 組織を跨がるデータの流通

④ 各層における信頼性の基点の確保

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

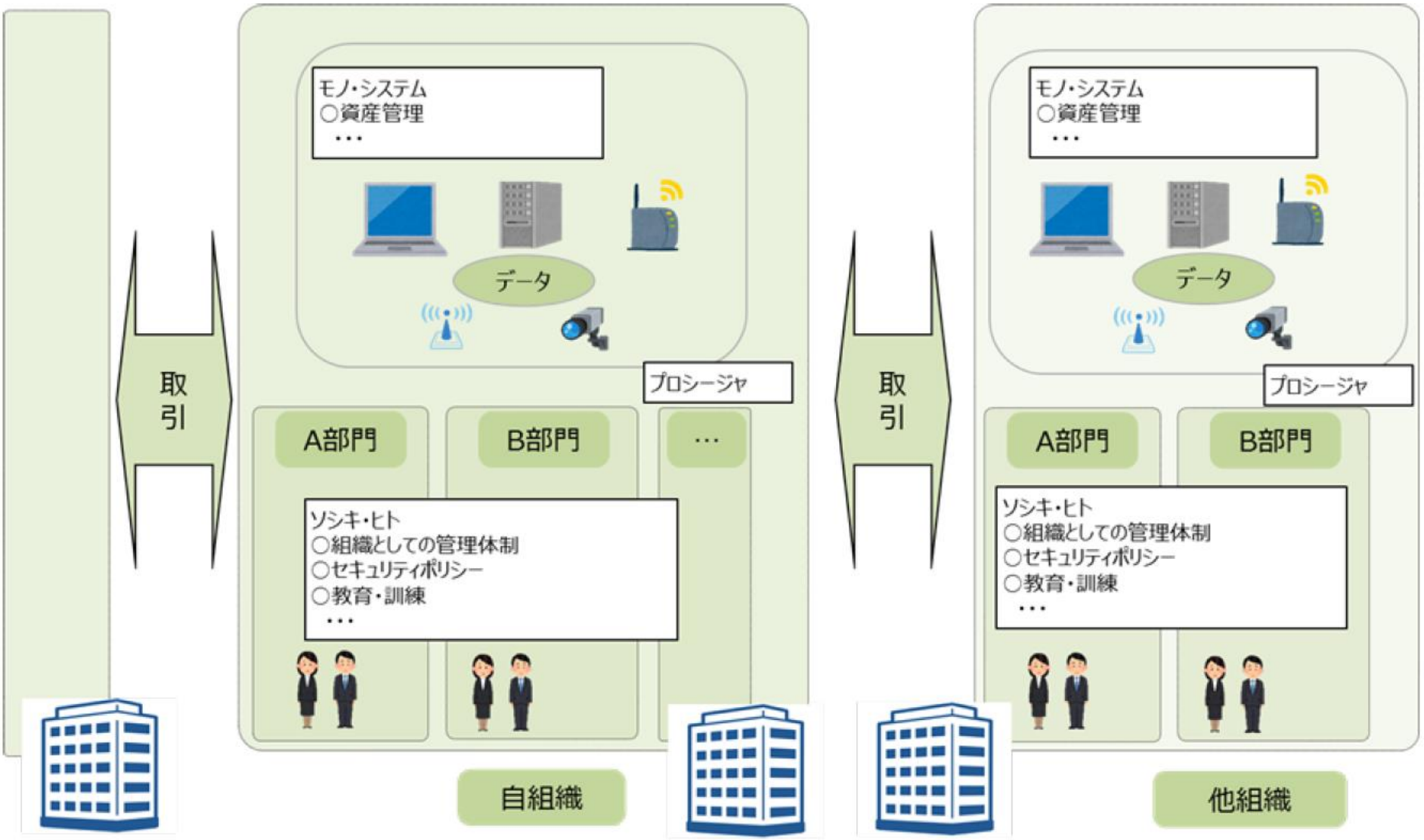
分析対象の明確化（三層構造モデルへの落とし込み）

- 各層の特性及び機能・役割を理解した上で**分析範囲及び資産を整理**。
- 分析対象のシステムによっては第２層の機能と第３層の機能を併せ持つモノもあることに留意。

階層	特性	機能・役割	分析対象	分析対象の具体的イメージ
第1層	各組織の適切なガバナンス・マネジメント	• 各組織のセキュリティマネジメント 【信頼性の基点】組織・マネジメント	• 組織で管理されるモノ・システム等 • 組織内で流通するデータ 等	• 社員、従業員 • 企業のIT資産 等
第2層	フィジカル空間とサイバー空間のつながり拡大	• フィジカル空間とサイバー空間との間のデータのやりとり 【信頼性の基点】ルールに沿って正しくフィジカル空間とサイバー空間とを転写する機能	• データを転写するモノ・システム • 転写されるデータ 等	• センサ • アクチュエータ • 3Dプリンタ • 監視カメラ 等
第3層	サイバー空間で組織を超えた多様・大量のデータの流通・処理	• データの送受信、加工・分析、保管 【信頼性の基点】データ	• データを送受信／加工・分析／保管するモノ・システム • 組織を超えて流通するデータ 等	• サーバ • ルータ • スマートメータ • オープンデータ 等

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

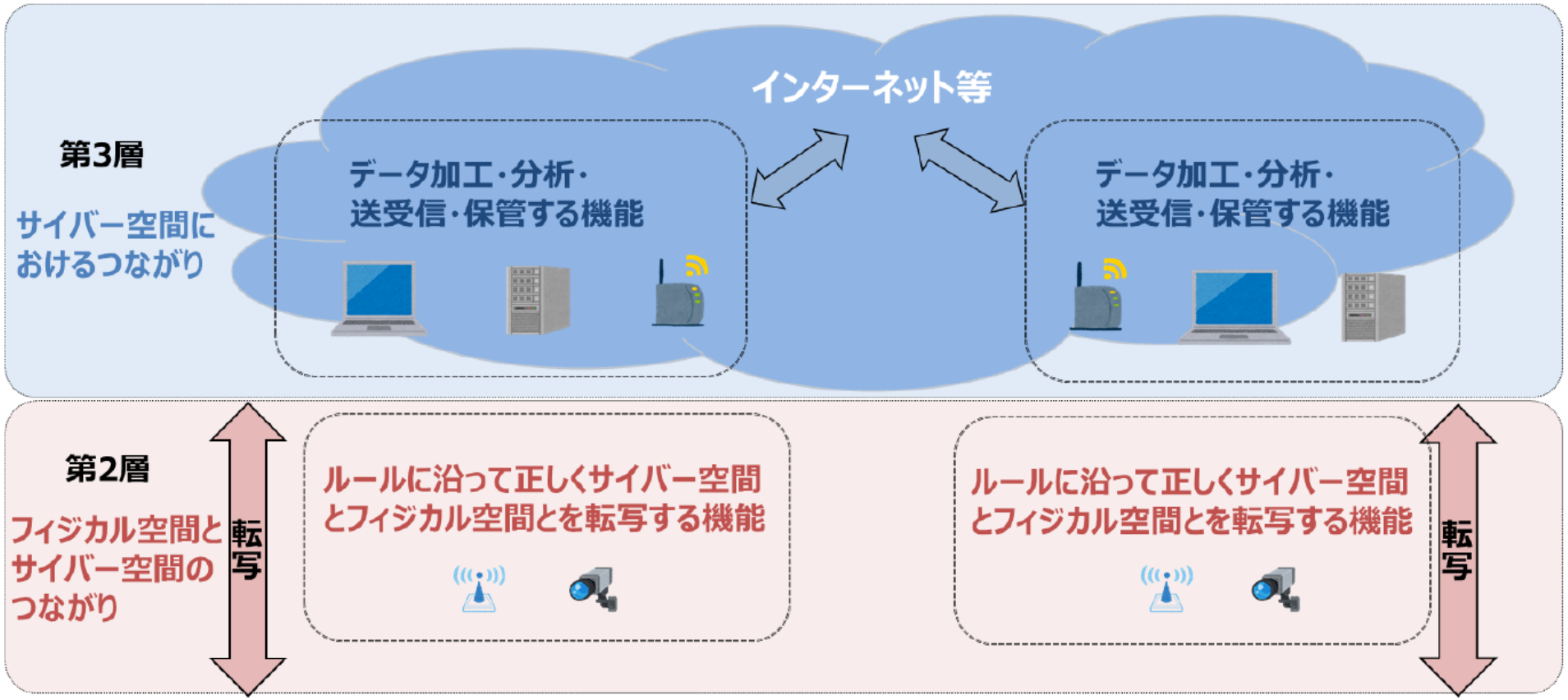
第1層の分析対象及び分析対象の具体的イメージ



第1層 企業間のつながり

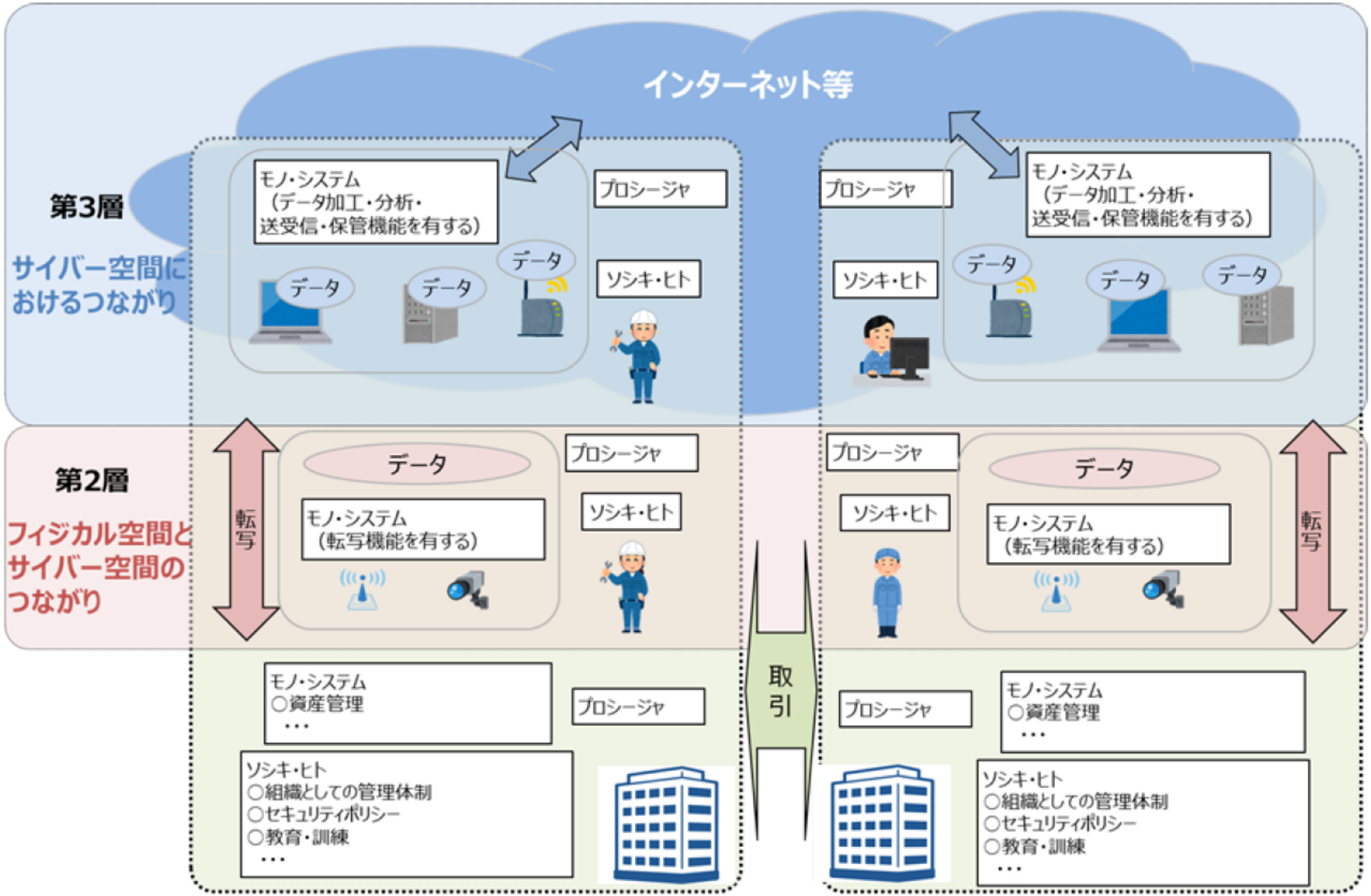
出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

第2層及び第3層の機能・役割及び分析対象の具体的イメージ



出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

三層構造モデルと6つの構成要素を活用した分析対象の具体的イメージ



出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

想定されるセキュリティインシデント及び事業被害レベルの設定①
～各層の機能に対する悪影響のイメージ～

- 三層構造モデルにおける各層の特性などを踏まえ、**各層の機能（守るべきもの）とそれに対する悪影響のイメージを整理。**

階層	各層の機能（守るべきもの）	機能（守るべきもの）に対する悪影響のイメージ
第1層	• 各組織のセキュリティマネジメント	• **セキュリティインシデントの発生**（営業秘密の漏えい） • **セキュリティインシデントによる影響の拡大**（被害拡大による事業影響）
第2層	• フィジカル空間とサイバー空間との間のデータのやりとり	• **機器の機能停止**（IoT機器の稼動停止） • **信頼性の低い稼動**（IoT機器の意図しない稼働）
第3層	• データの送受信、加工・分析、保管	• **データ保護に係る法制度等への不準拠** • **セキュアでない稼動**（データ処理側での情報資産の棄損） • **信頼性の低い稼動**（データ関連サービスの意図しない稼動）

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

想定されるセキュリティインシデント及び事業被害レベルの設定②
～想定されるセキュリティインシデントの設定～

- 各層の機能及び機能に対する悪影響の観点を踏まえ、**三層構造の各層で発生を回避すべき一般的なセキュリティインシデントを整理。**

階層	想定されるセキュリティインシデントの例
第1層	• セキュリティインシデントによる被害が拡大し、**適切に事業継続できない** 等
第2層	• 内部に不正アクセスされた**IoT機器が意図しない動作** • 改ざんされた**IoT機器による正確でないデータの送信等**が発生 等
第3層	• サイバー空間にて取り扱われる**保護すべきデータの漏えい** • なりすましされた機器等から**不適切なデータを受領** 等

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

リスク分析・リスク対応の実施（添付Ｂの活用）

- 添付Bでは、**抽出したセキュリティインシデントに対して**、当該インシデントの発生を助長、あるいは発生した**インシデントの被害を拡大させる可能性がある脅威及び典型的な脆弱性を整理。**
- 脆弱性を**6つの構成要素で捉えることで、新たなサプライチェーンにおけるリスク源の洗い出しへ対応可能。**実際のリスク分析を実施する際にも、検討するリスク源の抽出及び過不足のチェック等に活用可能。
- 添付Ｂには、さらに対応するセキュリティ対策要件も整理。**リスク対応として低減を実施する場合は、これらを参照することで対策要件の選択が可能。**

＜添付B＞　リスク源と対策要件の対応関係

機能	想定されるセキュリティインシデント	リスク源			対策要件	対策要件ID
		脅威	脆弱性ID	脆弱性		
下記すべてに関わる • データを加工・分析する機能 • データを保管する機能 • データを送受信する機能	サービス拒否攻撃により、関係する他組織における自組織のデータを取り扱うシステムが停止する	システムを構成するサーバ等の電算機器、通信機器等に対するDoS攻撃	L3_3_b_ORG	[ソシキ] ・データの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない	サービスやシステムの運用において、サービスマネジメントを効率的、効果的に運営管理するサービスサプライヤーを選定する	CPS.SC-2

脆弱性は、６つの構成要素別に記載。

対策要件IDで添付Cの詳細な対策例を参照可能。

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

第Ⅲ部　メソッド：　セキュリティ対策要件と対策例集
対策要件及び対策例集を活用したリスク対応

- 添付Ｃでは、添付Ｂで示した対策要件を**NIST Cybersecurity Frameworkを参考にカテゴリー分けを行い整列**（次スライド参照）。更に、各対策要件について、**具体的な参考となる対策例を記載。**
- 企業等はリスクアセスメントの結果に応じて、第Ⅲ部に記載された対策要件および、**添付Cに記載されたセキュリティ対策例**を実装し、リスクマネジメントプロセスを適切に実施することで、自組織のセキュリティマネジメントを改善することが可能。

＜添付Ｃ＞　対策要件に応じたセキュリティ対策例集

添付Bの脆弱性に対応。

他の国際規格等との対応関係。（説明後掲）

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	NIST SP800-171	NIST SP800-53	ISO/IEC 27001 付属書A
CPS.AM-1	・・・	L1_1_a_COM L1_1_b_COM L1_1_c_COM L2_1_a_ORG L2_3_b_ORG	<H-Advanced> ・・・	O/S	○	○	－
			<Advanced> ・・・	O/S	○	○	○
			<Basic> ・・・	O			

・添付Bの対策要件をNIST CSFを参考に整列。
・対象要件IDで添付Bの記載へ参照が可能。

対策例は３つのレベルに分けて記載。
High Advanced, Advanced, Basic

対策例を実施する主体を記載。
S:　システムに実装される対策
O:　組織に実装される対策

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

- 対策要件のカテゴリーは、**NIST Cybersecurity Framework に対応**する形で整理。

カテゴリー名称	略称	NIST Cybersecurity Framework v1.1 の対応カテゴリー
資産管理	CPS.AM	ID.AM (Asset Management)
ビジネス環境	CPS.BE	ID.BE (Business Environment)
ガバナンス	CPS.GV	ID.GV (Governance)
リスク評価	CPS.RA	ID.RA (Risk Assessment)
リスク管理戦略	CPS.RM	ID.RM (Risk Management Strategy)
サプライチェーンリスク管理	CPS.SC	ID.SC (Supply Chain Risk Management)
アイデンティティ管理、認証及びアクセス制御	CPS.AC	PR.AC (Identity Management and Access Control)
意識向上およびトレーニング	CPS.AT	PR.AT (Awareness and Training)
データセキュリティ	CPS.DS	PR.DS (Data Security)
情報を保護するためのプロセスおよび手順	CPS.IP	PR.IP (Information Protection Processes and Procedures)
保守	CPS.MA	PR.MA (Maintenance)
保護技術	CPS.PT	PR.PT (Protective Technology)
異変とイベント	CPS.AE	DE.AE (Anomalies and Events)
セキュリティの継続的なモニタリング	CPS.CM	DE.CM (Security Continuous Monitoring)
検知プロセス	CPS.DP	DE.DP (Detection Processes)
対応計画	CPS.RP	RS.RP (Response Planning) RC.RP (Recovery Planning)
伝達	CPS.CO	RS.CO (Communications) RC.CO (Communications)
分析	CPS.AN	RS.AN (Analysis)
低減	CPS.MI	RS.MI (Mitigation)
改善	CPS.IM	RS.IM (Improvements) RC.IM (Improvements)

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

CPSFにおける他の国際規格等との対応関係

- 第Ⅲ部、添付C及び添付Dにおいて、主要な国際規格等との対応関係を記載。
- NIST Cybersecurity Framework、NIST SP800-171、ISO/IEC 27001付属書Aについては、**各規格等から見た場合の対応関係も整理。**

<添付C> CPSF ⇒ 他の国際規格等

対策要件ID	対策要件	対応する脆弱性	対策例	対策例を実行する主体	NIST SP800-171	NIST SP800-53	ISO/IEC 27001 付属書A
CPS.AM-1	・・・	L1_1_a_COM, L1_1_b_COM, ・・・	<H.Advanced> ・・・	O/S	○	○	―
			<Advanced> ・・・	O/S	○	○	○

<添付D> 他の国際規格等 ⇒ CPSF

NIST Cyberseucurity Framework v1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
特定(ID)	AM-1	・・・	CPS.AM-1	・・・

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク		
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例
アクセス制御	3.1.1	・・・	・AC-2 アカウント管理 ・・・	CPS.AC-9	・・・	・・・

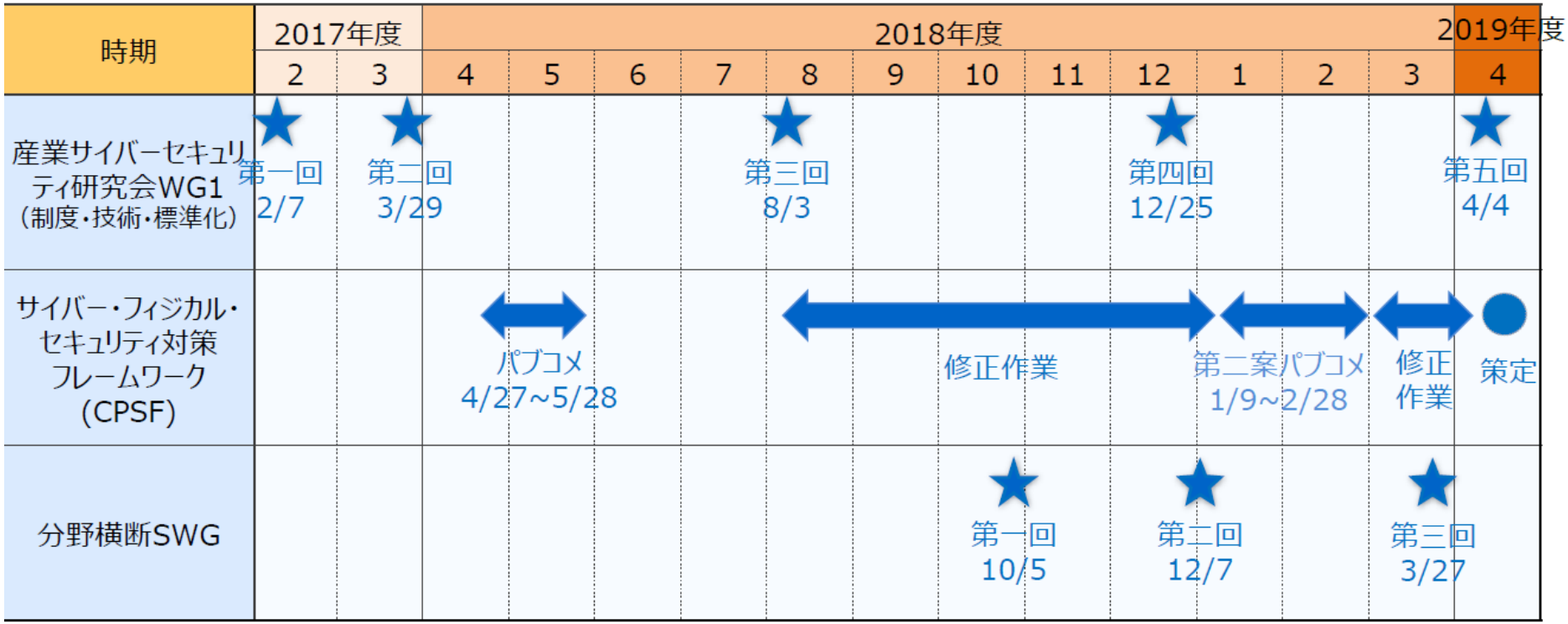
ISO/IEC 27001:2013 附属書A		サイバー・フィジカル・セキュリティ対策フレームワーク		
管理策ID	要求事項	対策要件ID	対策要件	対策例
A.5.1.1	・・・	CPS.BE-2	・・・	・・・

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

これまでの取組について

- **『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）』を4月18日に策定。**
- 今後、CPSFを主要な産業分野に展開し、各産業分野で求められる具体的なセキュリティ対策の検討を推進。

これまでの取組の経緯



出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

産業分野ごとの検討の促進：分野別のSWGの設置

- 産業サイバーセキュリティ研究会WG1（技術・制度・標準化）で検討してきたCPSFを、**産業分野別に順次展開**し、具体的適用のためのセキュリティポリシーを検討。

［2018年2月～（５回開催）］
2019年４月　CPSFの決定・公表

［2018年２月～（８回開催）］
2018年9月　ガイドライン（β版）を公開
2019年3月　ガイドライン第1版（案）のパブコメを実施

［2018年6月～（４回開催）］

［2018年３月～（８回開催）］
（防衛装備庁 情報セキュリティ官民検討会）

2019年４月　第1回会合開催

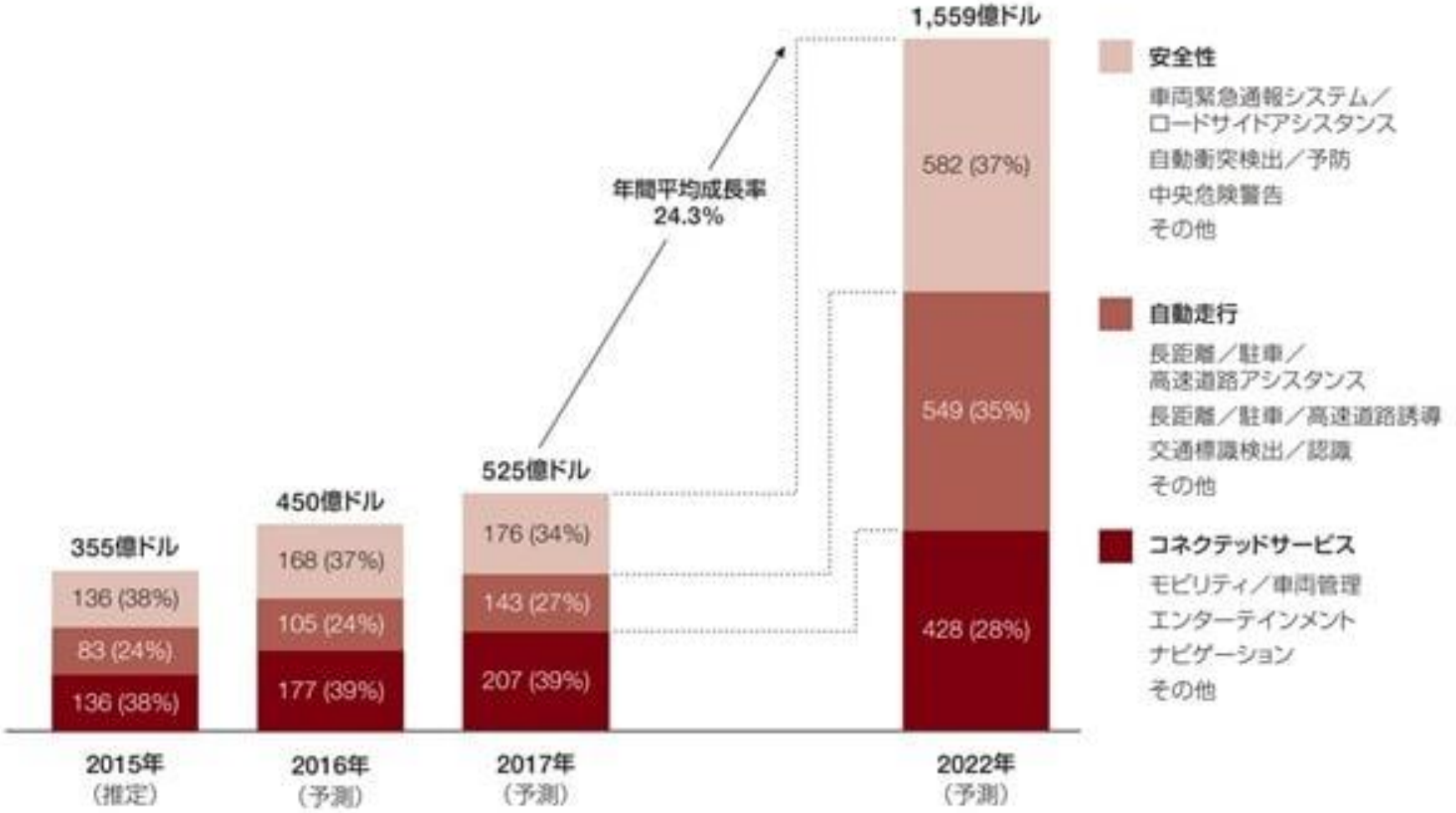
［2018年３月～（８回開催）］
(JEITA スマートホーム部会 スマートホームサイバーセキュリティWG)

出典：https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

４．コネクテッドカーのサイバー攻撃リスクとその対策

●コネクテッドカーへのサイバー攻撃

コネクテッドカーの市場拡大に追いついていないセキュリティ対策



出典：PWCレポート

●サイバー攻撃対象となるCANとは？

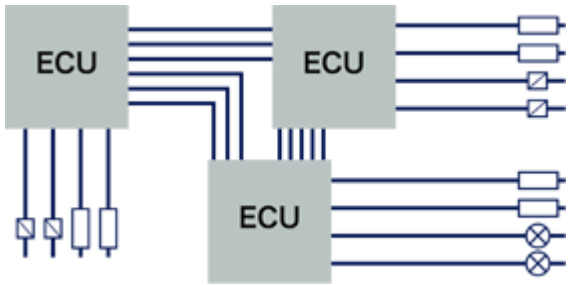
CANとは、「Controller Area Network」の略で、ドイツのBosch社が開発したシリアル通信プロトコル。完成したのは1985年、実際に量産車に採用されたのは1990年。その後、1994年に国際標準化機構（ISO）により標準規格（ISO11898/ISO11519）へ。現在では、ほぼすべての自動車に採用。

●CANの必要性

自動車の高性能化によって増える電子制御ユニット（ECU：Electronic Control Unit）への対応。制御内容が複雑になれば入出力も増えてECUは大型化し、複数のECU間でデータを共有し配線が増加。それによって複雑化し、重量や部品点数も増え、製造コストが跳ね上がってしまいます。その解決策が少ない配線でも高速かつ確実な通信ができる、シリアル通信プロトコル。

●従来型の通信方式からCANへ進化

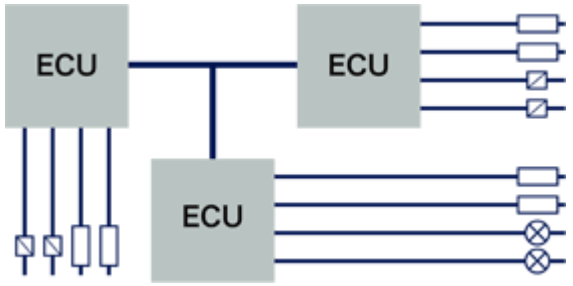
配線の本数が多い、重量が増加
配線スペースの増大



出典：キーエンスCAN計測器教科書

●CANを活用した通信方式

少ないハーネスで接続できる
ECU同士の通信が容易に行える
拡張性が高い
1つの情報を複数のECUで共有できる
ネットワーク全体の故障診断や処理が1ヶ所でできる



出典：キーエンスCAN計測器教科書

●通信プロトコルの種類

車載ネットワークには「CAN」のほか、「LIN」「FlexRay」「MOST」などの通信プロトコルも利用。「LIN」はCANのサブネットワークとしての利用を想定し、低コストでシリアル通信が行える規格。そして次世代車載ネットワークとして注目されているFlexRayは、CANよりも高速な通信が可能。CAN・LIN・FlexRayはエンジン制御などの通信に利用されるが、「MOST：Media Oriented Systems Transport」は、マルチメディア系の通信を想定。

通信プロトコル	最大通信速度
CAN	1Mbps
LIN	20kbps
FlexRay	10Mbps
MOST	24.8Mbps （50Mbps/150Mbpsの規格もあり）

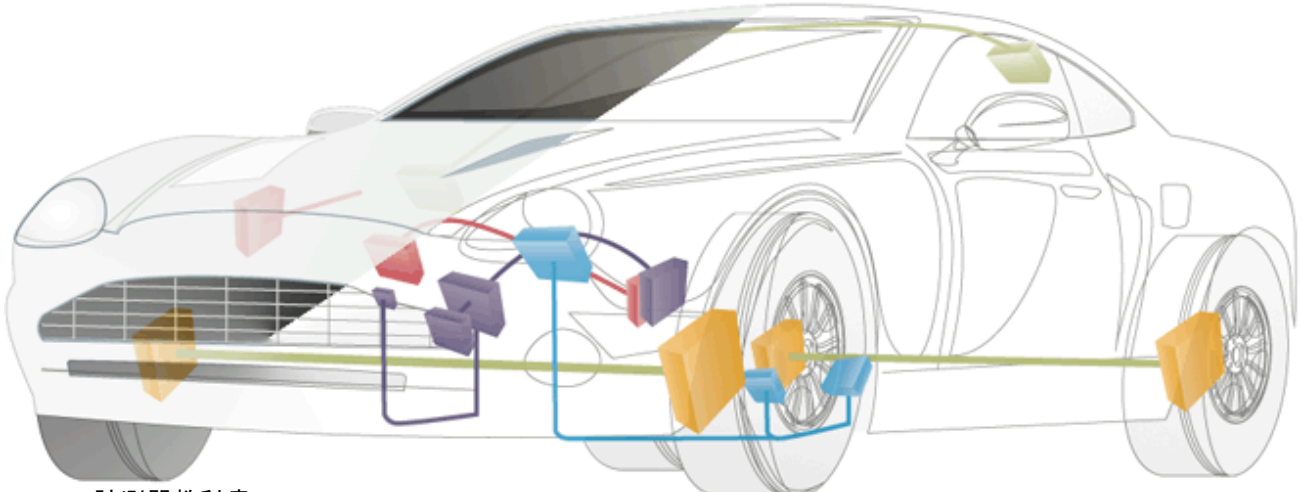
出典：キーエンスCAN計測器教科書

●CANの種類

CANは通信速度によって高速CAN・低速CAN「CAN-B」のように分類

⇒SAE（Society of Automotive Engineers）では通信速度で分類

クラス	通信速度	用途
クラスA	～10kbps	ライト類、パワーウィンドウ、ドアロックなど
クラスB	10～125kbps	メーターやオートエアコン、故障診断などのステータス情報系
クラスC	125kbps～1Mbps	エンジンやトランスミッション、ブレーキの制御などのリアルタイム制御系



出典：キーエンスCAN計測器教科書

●自動車のIoT化によるリスク

⇒コネクテッドカーの市場が広がるにつれて、CANの外部から
ハッカーが車両システムを乗っ取るリスクなどが顕在化

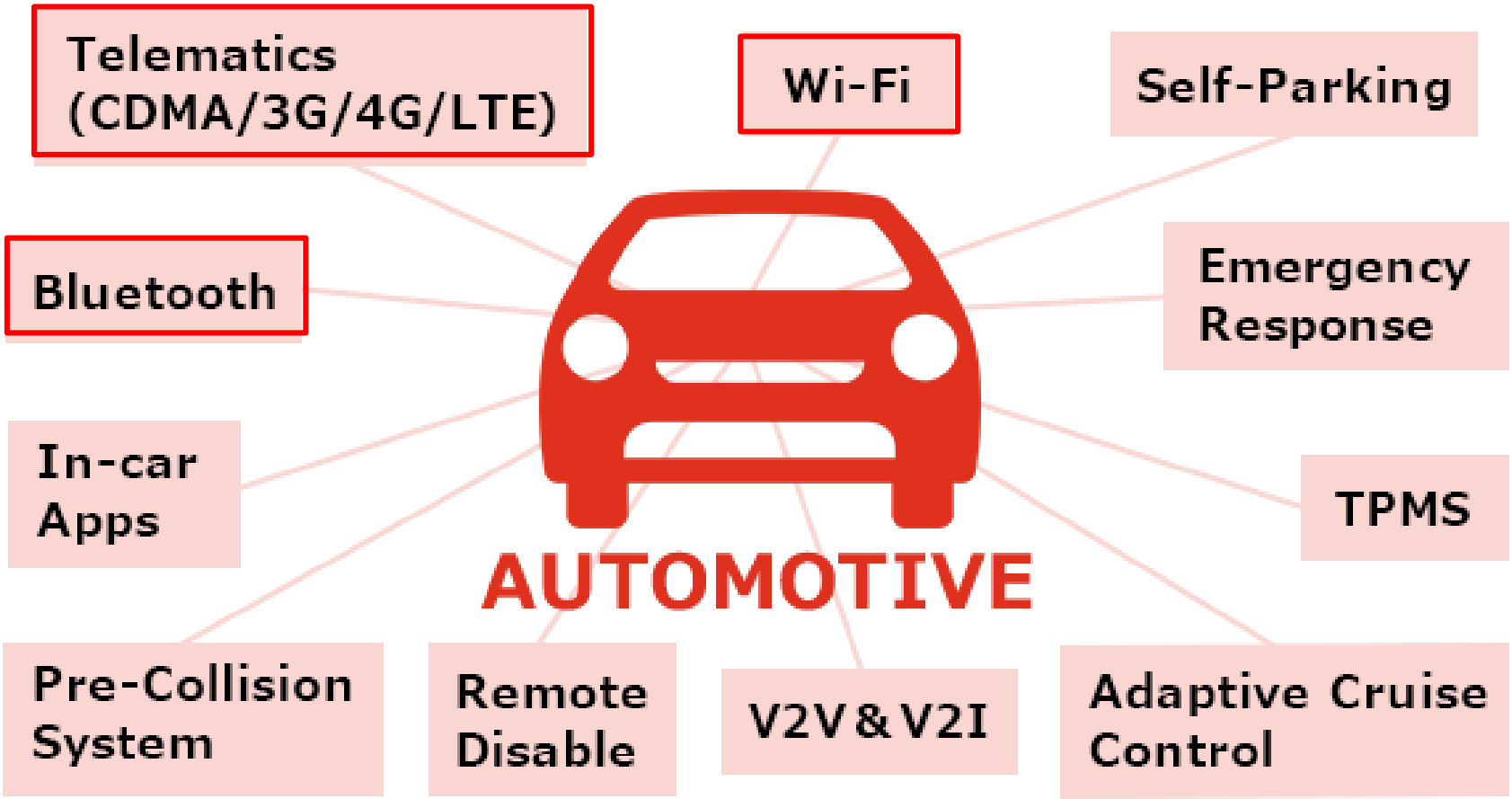
⇒コネクテッドカーには無線通信機器、車間通信システム、
車両制御機器など、数多くのシステムモジュール（IoT機器など）
が搭載されサイバー攻撃のリスク

⇒操舵システムに外部からアクセスされ、勝手にハンドル操作

⇒車の無線通信機能に脆弱性が存在し、車内制御システムが携帯電話からハッキングされ盗難防止アラームの無効化や、エアコン、ライトなどの車載機器を自由にコントロール

⇒コネクテッドカーは、多くのサプライヤーの部品で完成車となるため、サプライチェーンのビジネスパートナーを含めたセキュリティ管理体制が必要

コネクテッドカーのハッキング対象・経路



出典：PWCコネクテッドカーレポート

車両への直接攻撃とコネクテッドカークラウドなどへの攻撃リスクあり

出典：PWCコネクテッドカーレポート

●MaaSが本格普及したときに生まれる最大のリスクと保険

⇒サイバー攻撃

⇒コネクテッド・MaaS車両には通信機能が必須

⇒MaaS車両が自動運転機能の場合、サイバー攻撃被害は重大

⇒ドアをロック/運転操作に割り込まれる危険

⇒サイバーセキュリティ保険のニーズ

⇒MaaS向けの保険の一例：「オンデマンド保険」
　あらゆるものを対象に、適用期間を限定するタイプの損害保険

⇒ウェイモ社は、自動運転車に対する不安を緩和することを目的に、「オンデマンド保険」を提供する米トロブ（Trov）社と提携

●損保ジャパンのMaaS対応

SOMPOリスクマネジメント

2019年6月に発表された「成長戦略2019」では、少子高齢化やドライバー不足といった課題を解決するために目指す社会として「新たなモビリティサービス（MaaS）が組み込まれ、都市空間の在り方を変え、都市自体が高度にサービス化するスマートシティへ」が掲げられました。

それを受け、官民一体となったMaaS実現に向けての実証実験が加速されています。

損保ジャパンではMaaS実現に向けて、様々な角度からリスクソリューションを提供いたします。

●コネクテッドカーへのサイバー攻撃対策

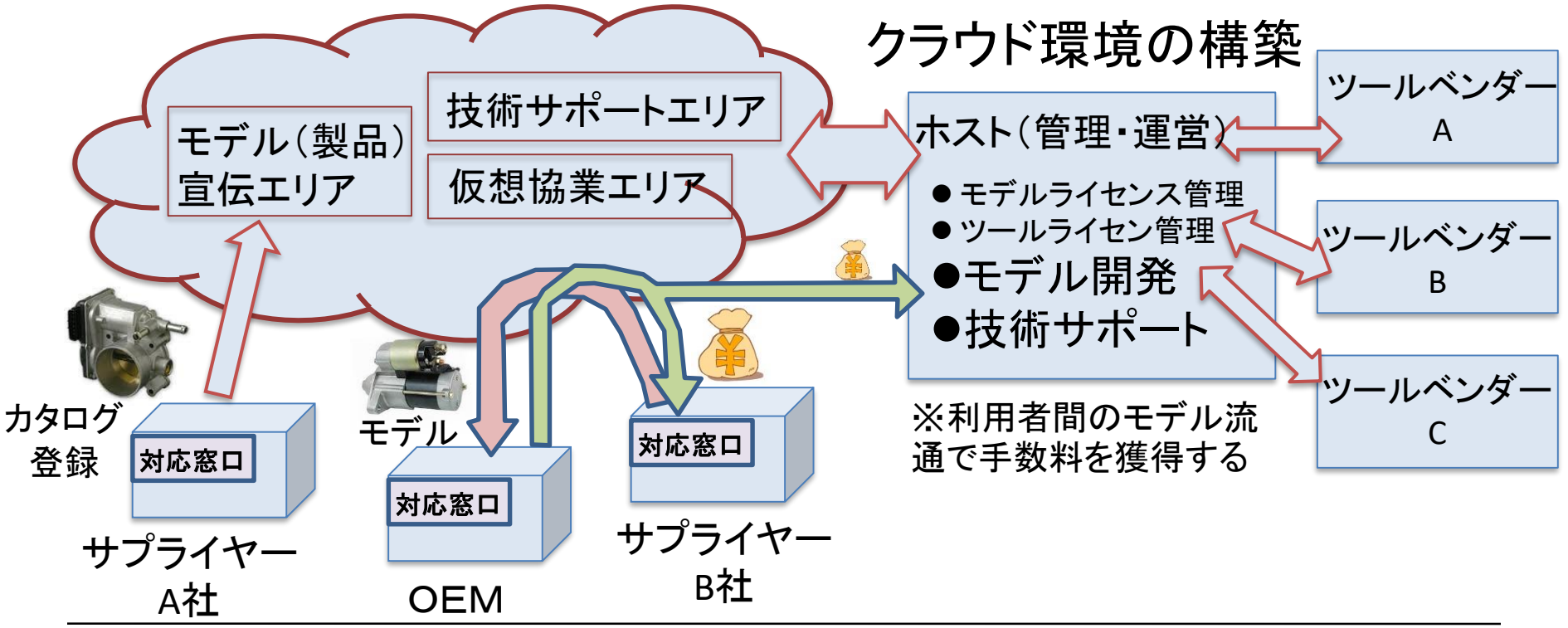
①セキュアプロセスの確立

②組み込み機器へのハードウェア・ソフトウェアの脆弱性テスト

③通信機能/テレマティクス脆弱性診断テスト

OICでの新たな取り組み
「次世代サプライチェーンの構築」

- モデル流通環境の提供 （盤石な流通）
- ソフト導入・維持に係る経費の削減 （中小企業の呼び込み）
- モデルによる製品宣伝のカタログ （市場の拡大）
- 仮想協業空間の提供 （協業の活性化）



出典：IoT/AI時代におけるオープンイノベーション推進協議会

OICでの新たな取り組み
～クラウド仮想協業空間（自動車のMBDを軸に）の立ち上げ～

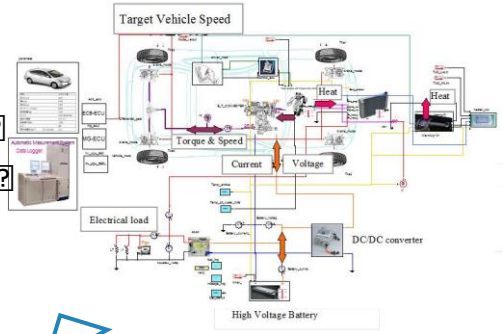
MBD: Model Based Development

仮想協業エリア□

ツール依存の無い国際標準によるサンプルモデルを置く□

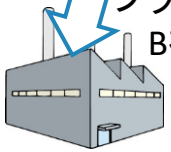
□

- 車1台分全体を表現できるモデル□
- OEMサプライヤー連携が可能な、□エンジンモデル□
- 電装品モデル□



サプライヤー□
A社□

プライヤー□
B社□



サプライヤー□
C社□

OEM□
A社□

大学□

出典：IoT/AI時代におけるオープンイノベーション推進協議会

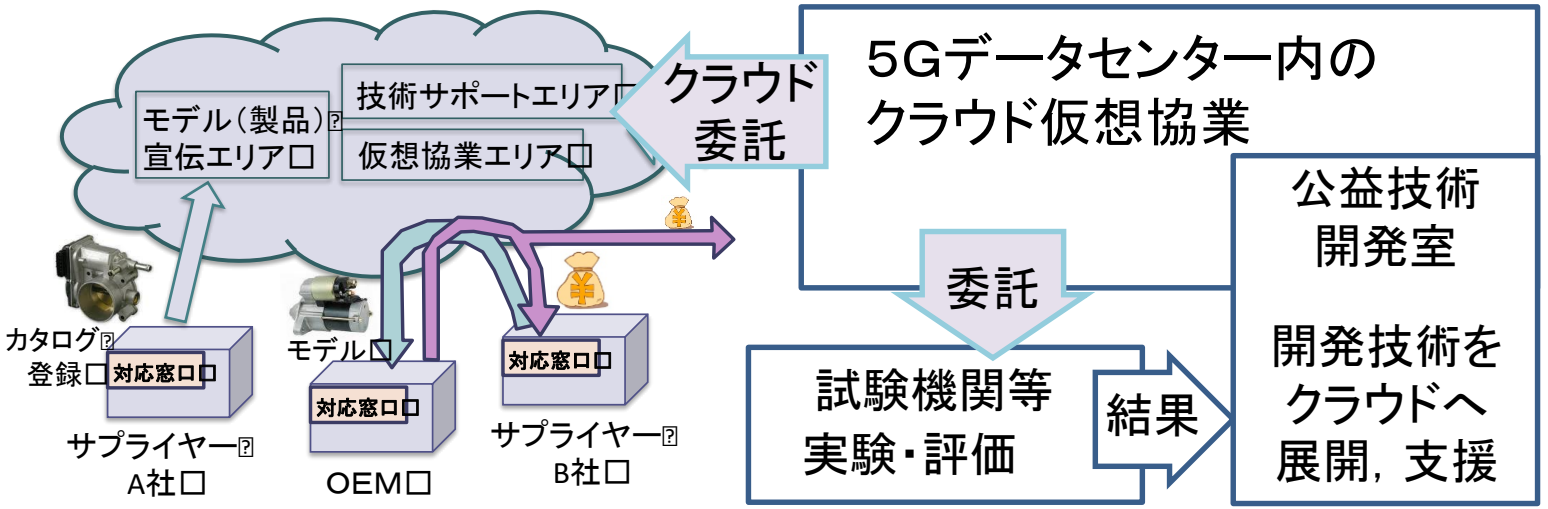
OICでの新たな取り組み
～次世代サプライチェーンプロジェクト（自動車を軸に立ち上げ）～

要件　① 競争優位性の構築

- モノづくり環境のデジタル化

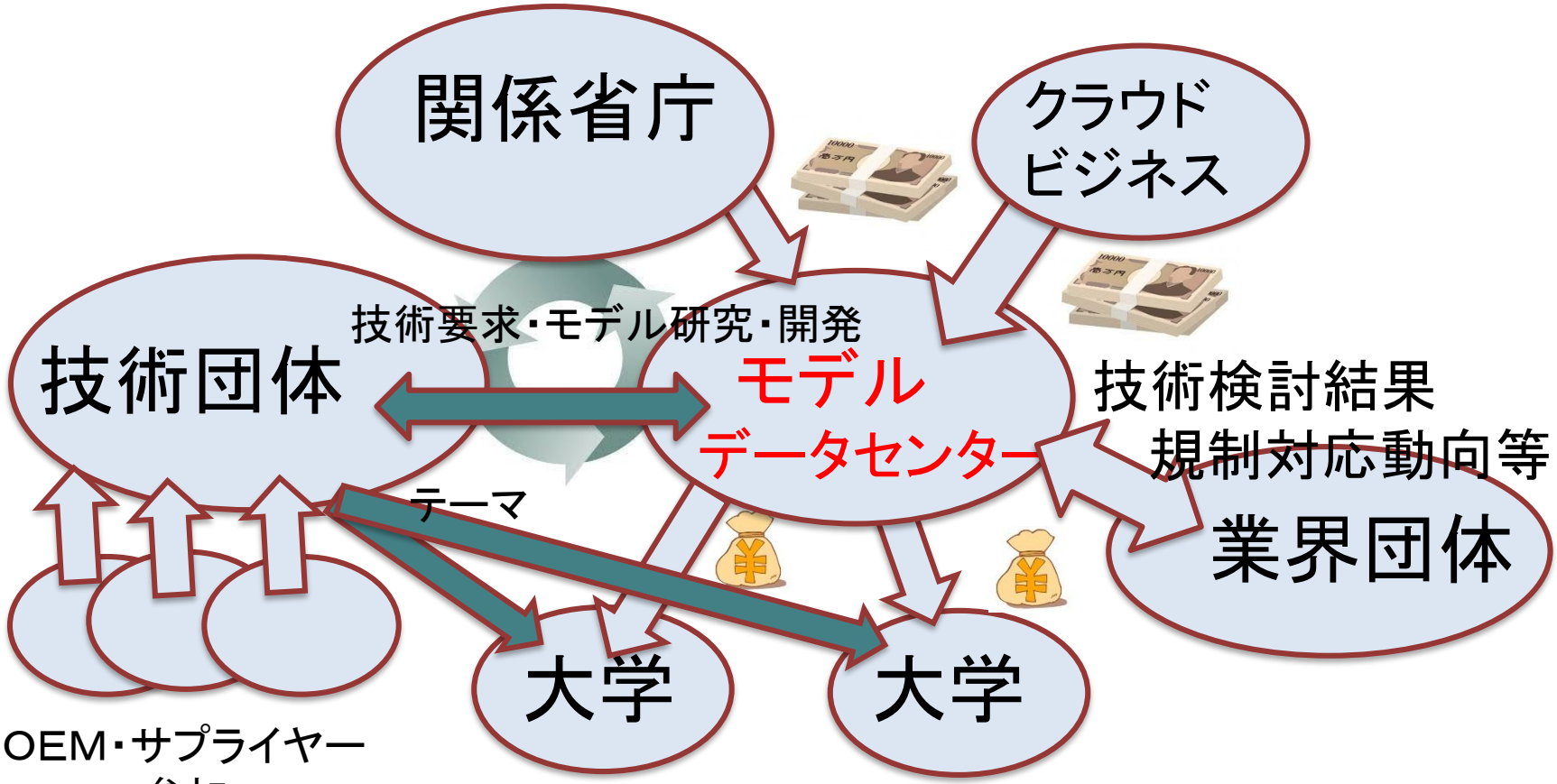
② 波及性

- クラウド内で新たな企業の起業や、
  モノづくりに関わる経済の発展が望める
- MBD以外CAD、制御ソフト等、多くの分野・産業で
  同じ仕組みの利用が可能



出典：IoT/AI時代におけるオープンイノベーション推進協議会

OICでの新たな取り組み
～次世代サプライチェーンプロジェクト関係機関および産学連携～



企業のニーズに近い研究で産学の活性化

大学研究者・大学院生（企業との共同研究・開発），即戦力の人材育成

出典：IoT/AI時代におけるオープンイノベーション推進協議会

ご清聴ありがとうございました