IoT・マイナンバー時代のIT国家像とパブリック・セーフティに関する提言

デジタル・ニッポン2015

平成27年6月24日

自由民主党　政務調査会　IT戦略特命委員会

内容

はじめに

ITの技術歩は、加速度的にスピードを増している。昨年、2020年東京オリンピック・パラリンピックにおける世界最先端IT国家像を「デジタル・ニッポン2014」として提言した後、世界的に「IoT（Internet of Things）」やそれに伴う「第４次産業革命」が一気に本格化し始めた。サイバー空間とリアル空間の融合は既にはじまっており、この世界的な潮流に乗り遅れれば日本経済の優位性は根底からくつがえされかねない。

また、いよいよマイナンバー制度の導入がせまり、その利活用推進が議論される中、日本年金機構の情報漏えい問題やサイバー犯罪の増加等で国民の不安が増しており、対応の強化が求められている。

我々は「ITは国民の幸せのためになくてはならない。不幸せの道筋を描くものであってはならない。」との基本思想のもとで、これらの課題に対応すべく、多くの企業からヒアリングを行い、研究機関を訪れ、思考を巡らせてきた。

特命委員会親会はもとより、６つの小委員会において、既成の枠にとらわれずに議論を積み重ねてきた。親会ではサイバーセキュリティー、資金決済小委員会ではトータルウォレット、社会保障に関する情報システム小委員会ではマイナンバーカードを利用したお薬手帳、AI及びロボット利活用促進小委員会ではAIロボット『パルロ』を委員会の顧問に就任させ、AIの新たなフェーズ及びロボットの実働環境、マイナンバー利活用小委員会では2020年に向けたロードマップ、政府情報システム小委員会ではシステムコストの削減、国会におけるIT機器利活用小委員会では各種委員会でのペーパレス化を進めてきた。いずれも、次世代の日本に必要不可欠な議論であったと自負している。

「デジタル・ニッポン2015」では、差し迫った課題に対応することはもちろん、2020年以降にIoTがIoE（Internet of Everything）となりCPS（Cyber Physical System）と呼ばれる社会が到来することを見据えて、日本の強みを活かした世界最先端IT国家像を提言している。

01　背景と位置づけ（１）

【背景】

- 自民党IT戦略特命委員会は、2001年「eJapan特命委員会」以来14年間の歴史を持ち継続的に政府ICT戦略に対して提言をしてきた。特に、2010年以降は毎年民間から幅広く知見を集め「デジタル・ニッポン」として具体的な提言を続けてきた
- ICTにはプラス側面が多いものの、デジタルデバイドの拡大やサイバー脅威の拡大といったマイナス側面もあり、これらに対して「デジタル・ニッポン2013」や2014年4月、2015年4月の「サイバーセキュリティに関する提言」といった形でその対処を提言してきた
- 2014年以降、急激にIoTとそれによる「第４次産業革命」の動きが本格化し日本の競争優位性が危機に瀕していること、マイナンバー制度導入が近付いていること、日本年金機構での情報漏洩事件の発生など、2015年現在日本のICTは新たな局面を迎えている

【位置づけ】

- 自民党ICT政策提言「デジタル・ニッポン2015」では、IoTというICT潮流やマイナンバー制度に対応するIT国家像と、そこで必要となるサイバー・セキュリティが発展したパブリック・セーフテイについて提言する
- 2020年頃には、IoTはIoEとなってモノだけでなく人やプロセス等全てがインターネットにつながりCPSと呼ばれる社会の到来が予測されているため、「デジタル・ニッポン2015」では可能な限りそれらを見据えた政策を提言する
- ICTの進化は日進月歩であり、新たな時代のICT政策は今後も引き続き検討を続ける必要がある

IoT : Internet of Things 全てのモノがインターネットにつながる状態やその技術
IoE : Internet of Everything　モノだけでなく人やプロセス等全てがインターネットにつながる状態やその技術
CPS : Cyber Physical System　サイバー空間とリアル空間が融合し機械と人が共創する知能化社会

01　背景と位置づけ（２）

自民党は2001年から徹底的に産業界と議論してICT戦略を磨いてきた。自民党ICT政策提言「デジタル・ニッポン2015」では、日本のICTが直面する新たな局面に対応するため、IoTというICT潮流やマイナンバー制度に対応するIT国家像と、そこで必要となるサイバー・セキュリティが発展したパブリック・セーフテイについて提言する。

自民党ICT戦略「デジタル・ニッポン」の流れ

2014年

新ICT戦略
デジタル・ニッポン2010

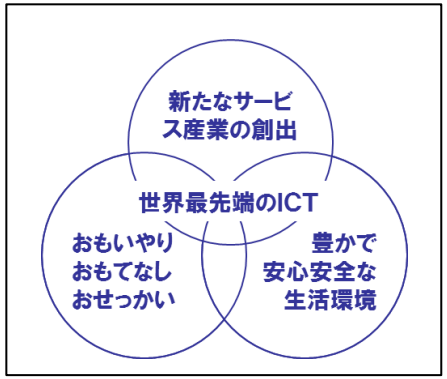
デジタル・ニッポン2011
絆バージョン
～復興、そして成長へ～

2012年政権復帰

デジタル・ニッポン2013
－ ICTで、日本を取り戻す－

- 政府CIO法成立
- マイナンバー法成立
- 世界最先端IT国家創造宣言
- 2020年東京オリンピック・パラリンピック開催決定

2020年世界最先端IT国家の具体像に関する提言
デジタル・ニッポン2014



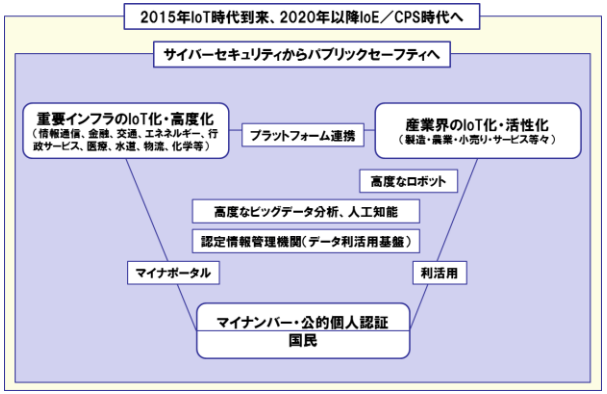
- 2020年を見据えたイノベーションの姿
- ICTによる「おもてなし」と「豊かで安心安全な生活環境」の実現
- 業界から最新アイデアをヒアリング

日本のICTの新たな局面

- 提言したイノベーションが続々と現実化
- 急激なIoTの本格化による日本の優位性の危機
- マイナンバー制度導入が近付いてきた
- 日本年金機構での情報漏洩事件

2015年

IoT・マイナンバー時代のIT国家像とパブリック・セーフティに関する提言
デジタル・ニッポン2015



- IoTやマイナンバーによる新たな国家像
- 2020年に想定されるIoE/CPS時代を見据えたIT国家像
- サイバーセキュリティが発展したパブリック・セーフティ

01　背景と位置づけ（３）

ICTの発展には、その負の側面であり急速に高まるサイバー脅威への対策が不可欠だが、自民党は常に積極的に具体的な提言をしてきた。2014年の「サイバーセキュリティに関する提言」により「サイバーセキュリティ基本法」が実現し、さらに最新状況に応じて継続的に提言をしている。

自民党のサイバーセキュリティ対策提言

2011～2012年

- 情報セキュリティ緊急提言
- 情報セキュリティ対策提言

政権復帰

2012年

サイバーセキュリティに関する提言

- 急速に高まるサイバー脅威への対処
- 国の主導的な役割の明確化
- 基本理念等の確立、司令塔の強化
- NISCの法制化

●サイバーセキュリティ基本法

2014年

今後のサイバーセキュリティ政策の在り方に関する提言

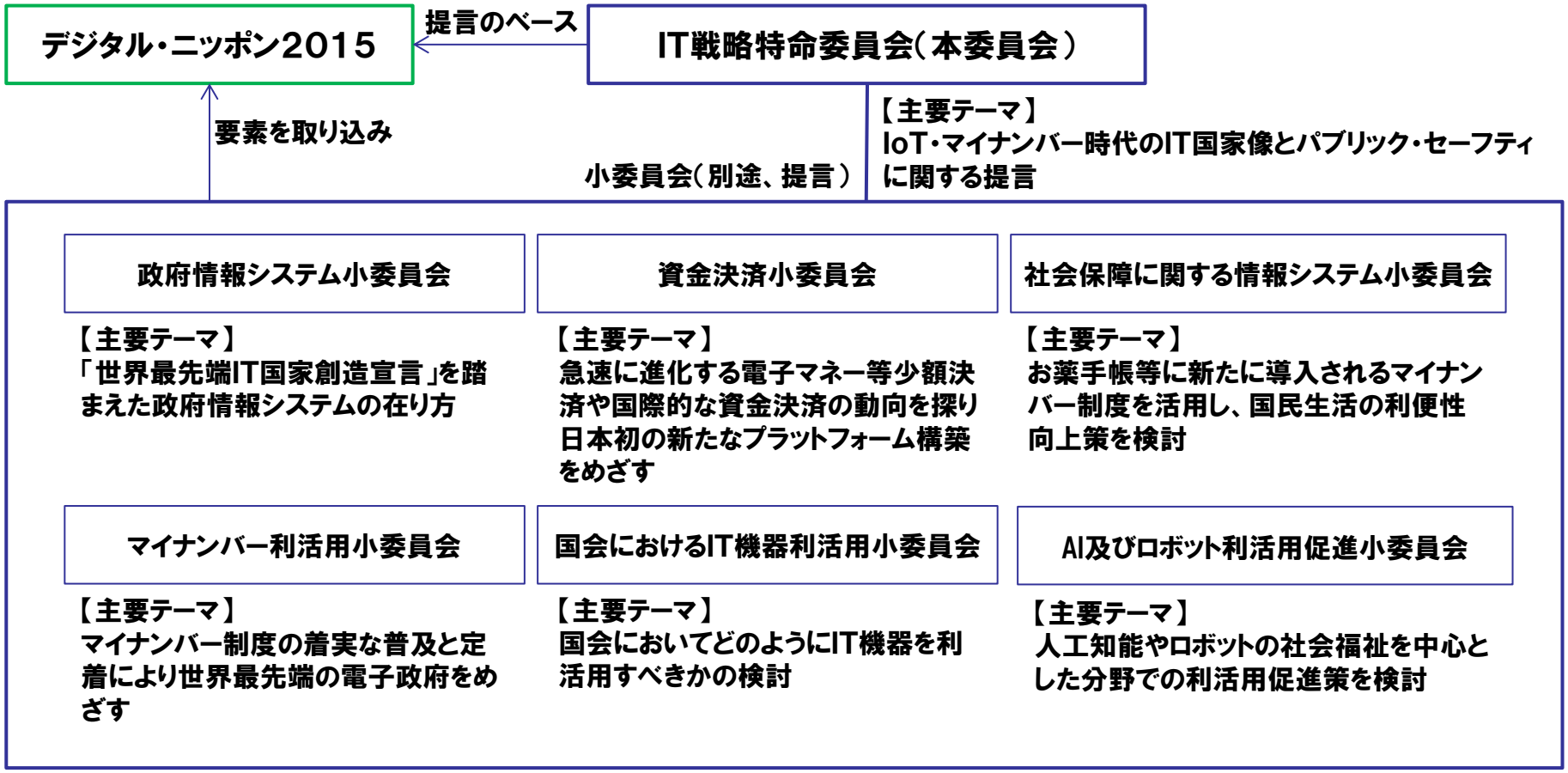
- セキュリティ確保を起点とする産業創出の実現
- サイバー脅威への対処能力の強化
- グローバルパートナーシップの強化
- セキュリティ人材の育成強化
- セキュリティ研究開発能力の強化
- オリンピック・パラリンピック東京大会におけるサイバーセキュリティ対策の強化
- 政府における体制強化

2015年

01　背景と位置づけ（４）

自民党IT戦略特命委員会は、本委員会と複数の小委員会で構成されている。今回の提言「デジタル・ニッポン2015」は、本委員会での議論をベースに小委員会で議論された要素を取り入れている。小委員会からの提言は別途行われる。

IT戦略特命委員会の構成と「デジタル・ニッポン2015」との関係



01　背景と位置づけ（５）

自民党IT戦略特命委員会では、以下のように多くの民間団体・企業等からのヒアリング及び視察を実施し、その知見やアイデアを取り入れている。

民間企業等ヒアリング（その１）

本委員会（ヒアリング・視察順）

- 新経済連盟
- 電子情報技術産業協会
- アジアインターネット日本連盟
- 在日米国商工会議所
- 全国銀行協会
- 日本クレジット協会
- 生命保険協会
- 日本損害保険協会
- ザ・ソフトウェアアライアンス（BSA）
- MSサイバークライムセンター(視察)
- NECサイバーセンター（視察）
- アカマイテクノロジーズ合同会社
- 日本マイクロソフト株式会社
- 日本電気株式会社
- トレンドマイクロ株式会社
- NRIセキュアテクノロジーズ株式会社
- 慶應義塾大学徳田英幸教授
- 株式会社ラック
- 株式会社FFRI
- 株式会社スプラウト
- 株式会社アズジェント
- 富士通株式会社（視察）
- ソフトバンク株式会社（視察）

以上２３者

マイナンバー利活用小委員会（ヒアリング順）

- 日本電気株式会社
- 株式会社野村総合研究所
- 日本証券業協会
- 大日本印刷株式会社
- 三井住友カード株式会社
- ぴあ株式会社
- 国際公共政策センター

以上７者

01　背景と位置づけ（６）

自民党IT戦略特命委員会では、以下のように多くの民間団体・企業等からのヒアリング及び視察を実施し、その知見やアイデアを取り入れている。

民間企業等ヒアリング（その２）

資金決済小委員会（ヒアリング順）
- デロイト・トーマツ・コンサルティング合同会社

以上１者

社会保障に関する情報システム小委員会（ヒアリング順）
- ソニー株式会社
- 日本薬剤師会

以上２者

AI及びロボット利活用促進小委員会（ヒアリング・視察順）
- 富士ソフト株式会社
- ソフトバンク株式会社（視察）
- 東京大学松尾豊准教授

以上３者

02　目指す姿(１)

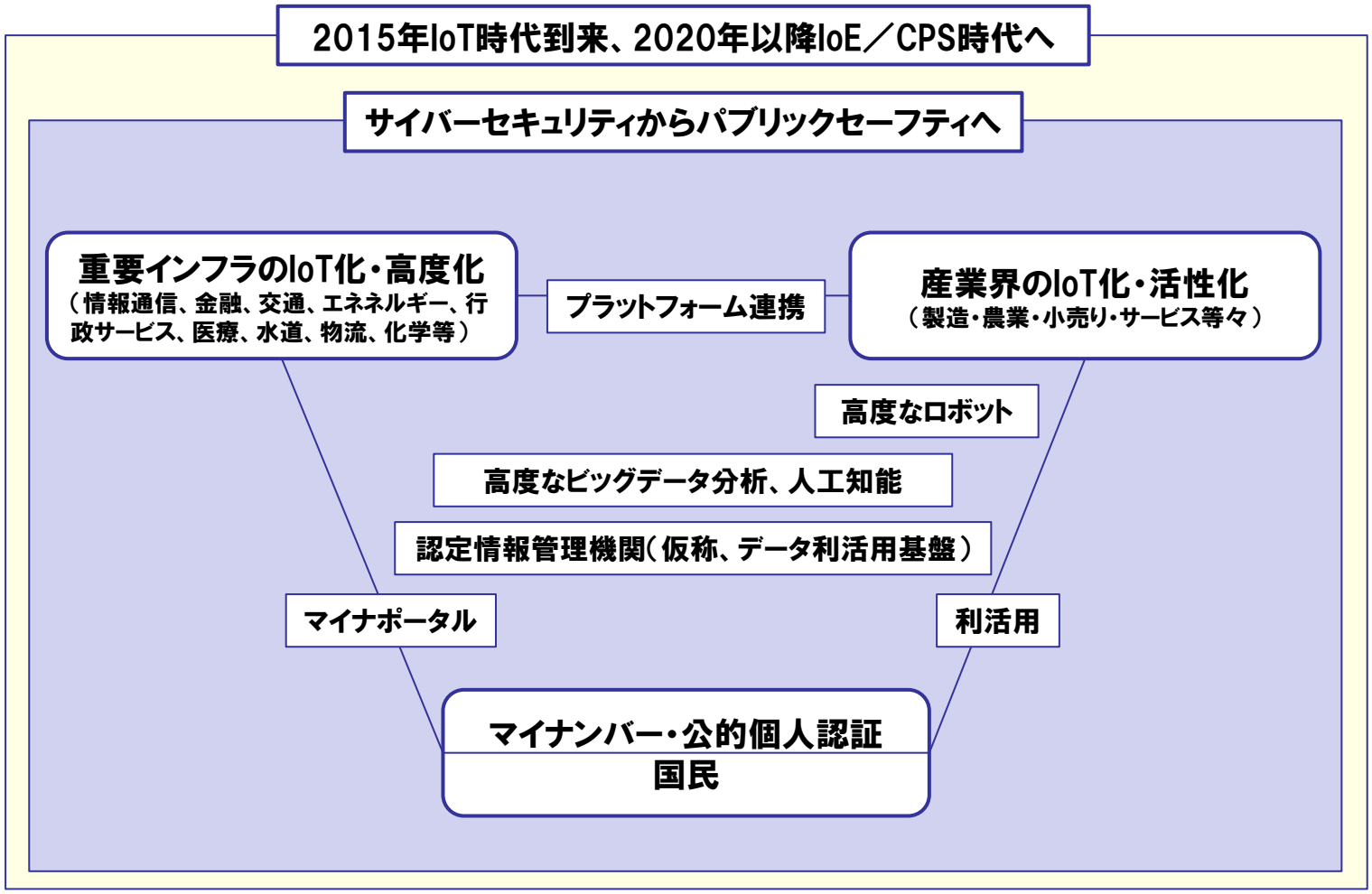
【目指す姿】

- IoT時代が到来し、2020年以降IoE/CPS時代へと向かうICT潮流の中、2020年の日本は世界最先端IT国家として、重要インフラで世界の最先端を走り、産業分野も活性化されている
- 2020年、日本はビッグデータ分析、人工知能、ロボット等ICTのインテリジェント化で世界最先端にあり、インテリジェントICTで経済貢献している
- 2020年、マイナンバーカードとマイナポータルの利活用により、国民の利便性や社会の効率性が、十分なセキュリティを維持しつつ向上している
- 2020年、自己情報コントロール下での認定情報管理機関(仮称)がデータ利活用基盤として利活用され、国民の安心と共に経済が効率化されている
- 2020年、日本の重要インフラは相互連携し、また優れた人工衛星技術からの情報と連携する事で、防災や国民の利便性、産業の活性化に貢献している
- IoT時代でサイバーセキュリティがパブリック・セーフティに発展する中で、2020年日本は世界最先端の安心安全を確保している

IoT : Internet of Things 全てのモノがインターネットにつながる状態やその技術
IoE : Internet of Everything　モノだけでなく人やプロセス等全てがインターネットにつながる状態やその技術
CPS : Cyber Physical System　サイバー空間とリアル空間が融合し機械と人が共創する知能化社会

02　目指す姿（２）

デジタル・ニッポン2015が目指す姿



IoT：Internet of Things 全てのモノがインターネットにつながる状態やその技術
IoE：Internet of Everything　モノだけでなく人やプロセス等全てがインターネットにつながる状態やその技術
CPS：Cyber Physical System　サイバー空間とリアル空間が融合し機械と人が共創する知能化社会

02　目指す姿（３）

【キーワード】

IoT戦略関係
- 2020年以降を見据えた「国家IoT戦略」
  - 産業政策としてのIoTの打ち出し
  - 重要インフラのIoT政策
- 重要インフラや産業分野のIoTによると「相互連携」

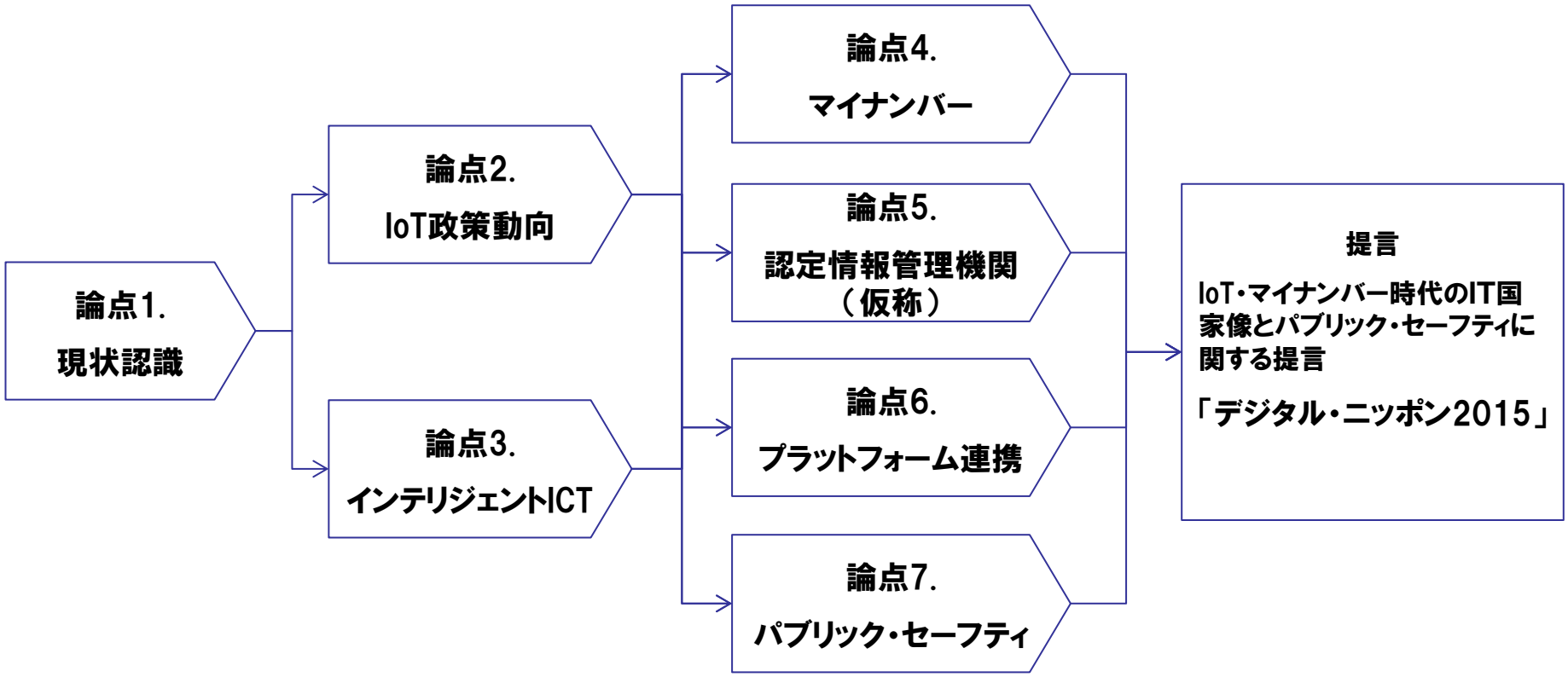
マイナンバー、IT利活用基盤関係
- 「マイナンバーカード／マイナポータル」の利活用
- 番号としてのマイナンバーは直接インターネットにつながらない
- 「公的個人認証の民間開放」の利活用
- 自己情報コントロール下のデータ利活用基盤としての「認定情報管理機関（仮称）」

セキュリティ関連
- サイバーセキュリティは「パブリック・セーフティ」に発展
- 社会インフラ機関での「情報漏洩、情報の改ざん、業務途絶への対策」の強化
- 「自治体等取扱組織」での「マイナンバー・セキュリティ」の強化
- IoT時代の「重要インフラ防護」の高度化

03　論点構成(１)

「デジタル・ニッポン2015」は、以下の様な論点の流れから提言を導き出している。

論定構成図



03　論点構成（２）

「デジタル・ニッポン2015」は、以下の様な論点の流れから提言を導き出している。

起	1. 現状認識：デジタル・ニッポン2014の提言はかなり現実化しつつあるがその後IoTが本格化し始めた
承	2. IoT政策動向：IoT時代が到来し各国が国策として推進している 3. インテリジェントICT：ビッグデータ分析、人工知能、ロボットが高度化する
転	4. マイナンバー：マイナンバーカードとマイナポータルが重要なプラットフォームとなる 5. 認定情報管理機関（仮称）：認定情報管理機関（仮称）は自己情報コントロール下でのデータ利活用基盤として重要なプラットフォームとなる 6. プラットフォーム連携：気象や位置等の情報が水道や交通、エネルギー等のインフラと連携して高度化し防災や国民の利便性に貢献する 7. パブリック・セーフティ：IoT時代はサイバーセキュリティはパブリック・セーフティに発展し重要性が増す

結	IoT・マイナンバー時代のIT国家像とパブリック・セーフティに関する提言「デジタル・ニッポン2015」

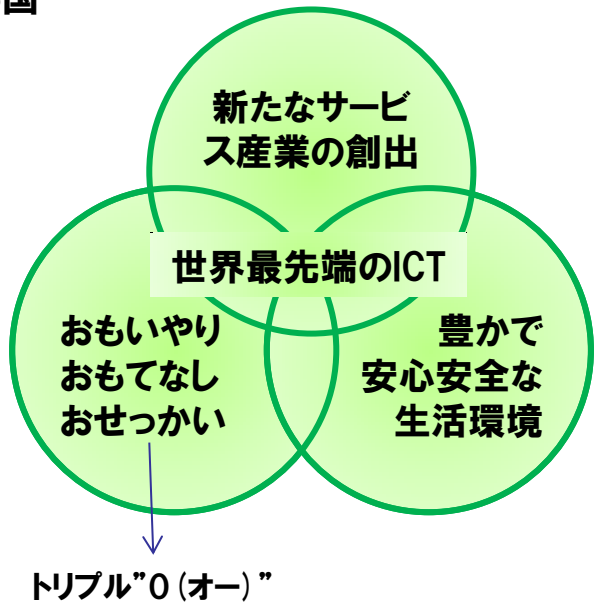
IoT：Internet of Things 全てのモノがインターネットにつながる状態やその技術

04 基本的な考え方：論点1.現状認識 ①デジタル・ニッポン2014の提言はかなり現実化しつつある

「デジタル・ニッポン2014」提言の内容は、この一年だけでもずいぶん現実化してきた。2020年に向けて目指した社会の姿は正しかったと言える。

「デジタル・ニッポン2014」が目指す社会

2020年東京オリンピック・パラリンピックに世界最先端の革新的なICTで新たなサービス産業を創出し、世界の人々への「おもいやり、おもてなし、おせっかい（トリプル”0（オー）”）」と、豊かで安心安全な生活環境で世界から尊敬される国



この1年で実現し始めた内容

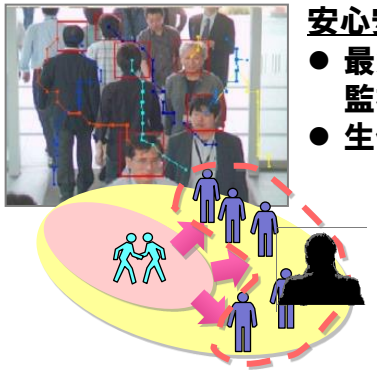
公衆無線LAN

言葉の壁を取り払う

- 同時通訳機で外国人をおもてなし

安心の医療

- ウェアラブルな測定機器で毎日健康診断ができる



安心安全

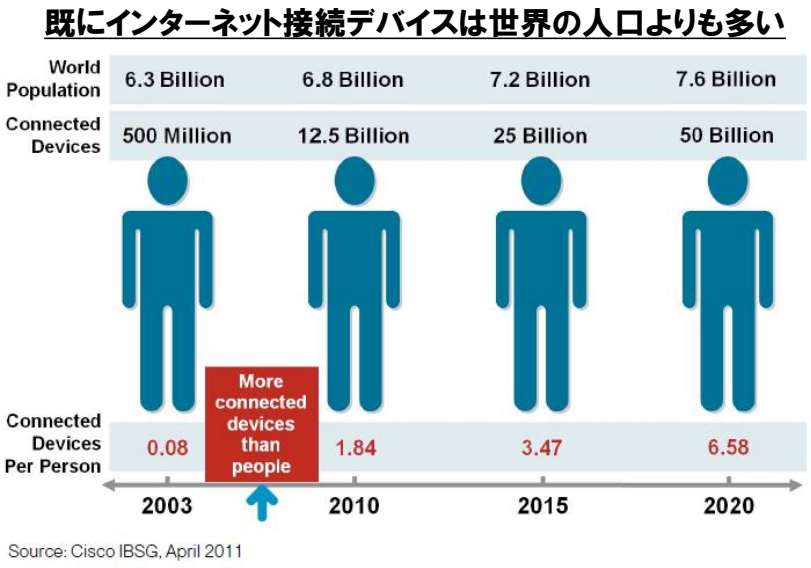
- 最先端画像処理技術で不審者や不審行動が監視できる
- 生体認証が社会システムの一部となる

出所：デジタル・ニッポン2014

04 基本的な考え方：論点1.現状認識
②デジタル・ニッポン2014後、急激にIoTが本格化し始めた

5年以上前からインターネット接続されたデバイスは世界総人口よりも多く、いよいよIoT時代が到来した。

IoTはパソコンやスマートフォン、タブレットだけでなく、身の回りのあらゆるモノに埋め込まれたセンサー等のデバイスがインターネットに繋がり、相互で通信が可能になる技術や仕組み、状態のことで「デジタル・ニッポン2014」以降、様々なIoT関連団体が設立され、2015年は「IoT元年」と言われている。（2020年のIoT関連市場規模は8.9兆ドル、モノの数2120億個（IDC2013年））



【IoTの沿革】

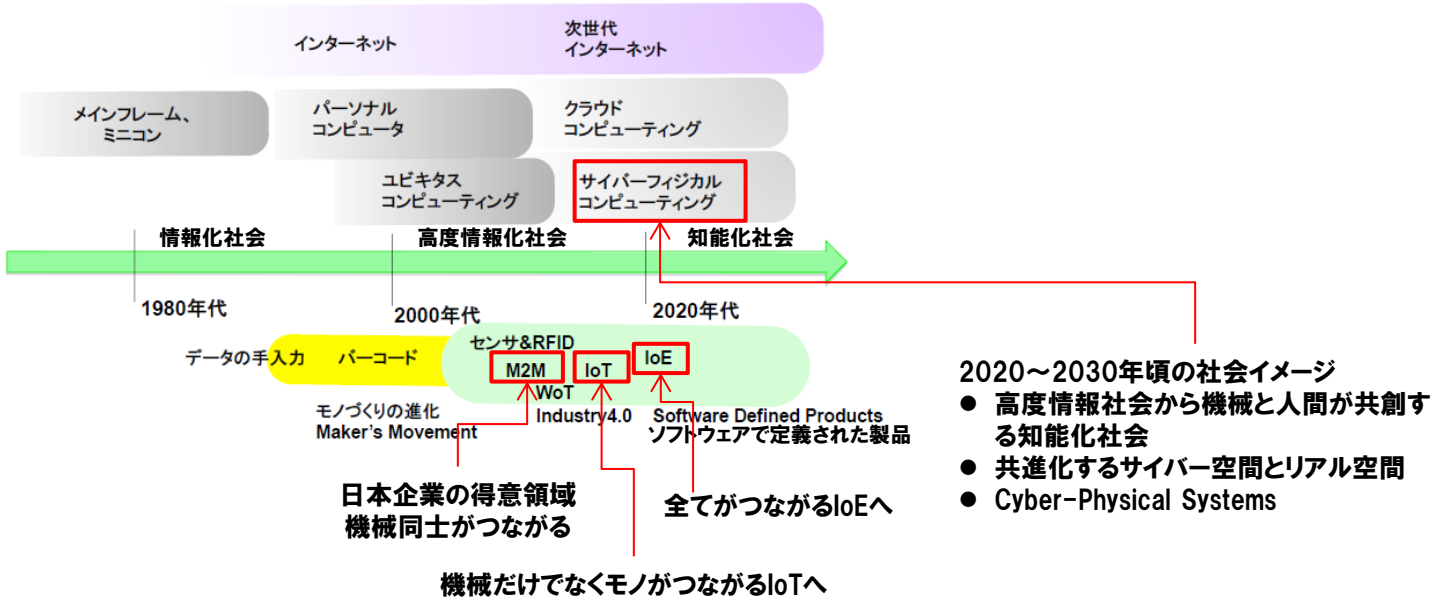
- 2012年、GEがIndustry Internet発表、ドイツが第四次産業革命として「Industrie4.0」発表（元SAP社長）
- 2014年はIoT関連で様々な団体が設立され、2015年は「IoT元年」と予測されている
  - 3月Industrial Internet Consortium（米GE等、製造業等産業分野）
  - 6月Homekit（米アップル等、スマートホーム・オフィス）
  - 7月Open Interconnect Consortium（米インテル等、スマートホーム）
  - 7月Thread Group（米クァルコム等、スマートホーム）
- ウェアラブルを中心に既にIoTは身近な生活を変えはじめている

04 基本的な考え方：論点1.現状認識 ③IoTは、2020年頃にIoE／CPSへと進化する

2015年はIoT時代だが、 2020年以降は「モノ」だけでなく人、プロセス、データ等500億以上のあらゆる対象がインターネットにつながるIoEの到来が予想されており、サイバー空間とリアル空間が融合したCPS社会が想定される。

20世紀後半の情報化社会は21世紀に入って高度情報化社会となり、2020年以降のCPS社会は「知能化社会（機械との共創社会）」とも言われている。

このCPSの潮流に乗り遅れれば、日本が「世界最先端IT国家」になることは不可能であろう。



M2M：Machine to Machine 機器間通信
IoT：Internet of Things 全てのモノがインターネットにつながる状態やその技術
IoE：Internet of Everything　モノだけでなく人やプロセス等全てがインターネットにつながる状態やその技術
CPS：Cyber Physical System　サイバー空間とリアル空間が融合し機械と人が共創する知能化社会

出所：慶應義塾大学環境情報学部、慶應義塾大学大学院政策・メディア研究科　徳田英幸教授、2015.4.2.自民党IT特命委員会説明資料

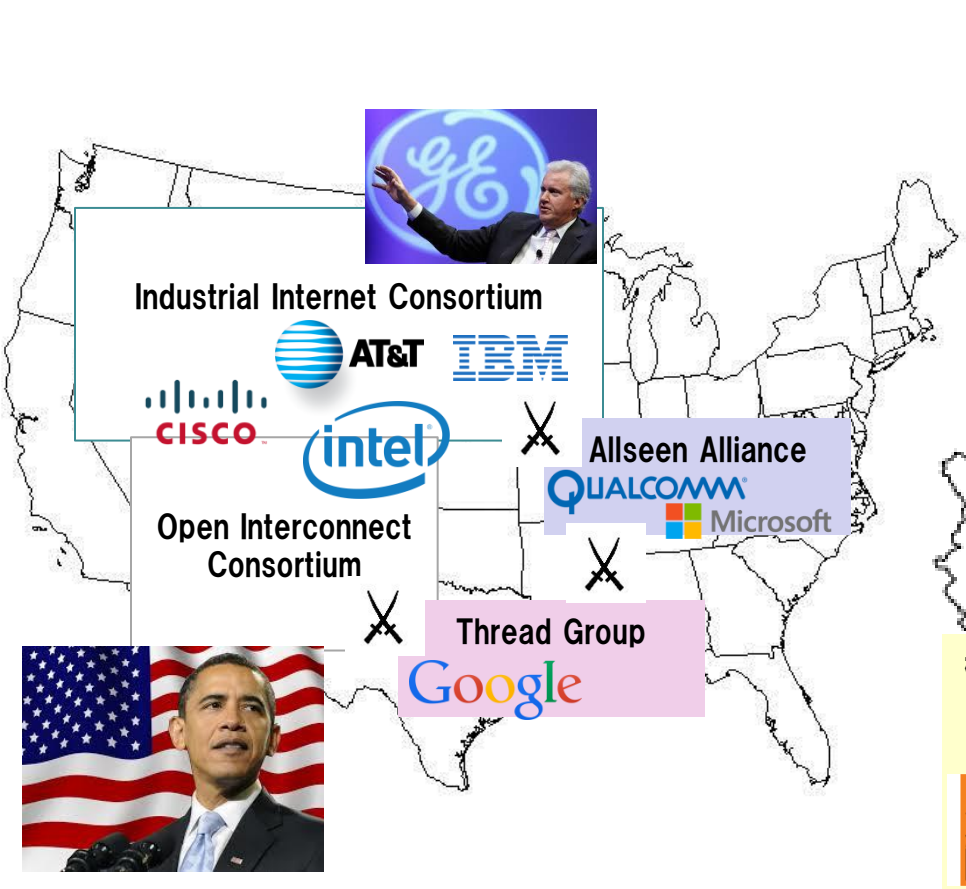
04 基本的な考え方：論点1.現状認識
③IoTは、2020年頃にIoE／CPSへと進化する

2020年頃には、社会のあらゆるものがインターネットに接続され、重要インフラで世界の最先端を走り、産業分野も活性化されていることを目指すべき。

出所：総科学技術イノベーション会議2015.4.16.

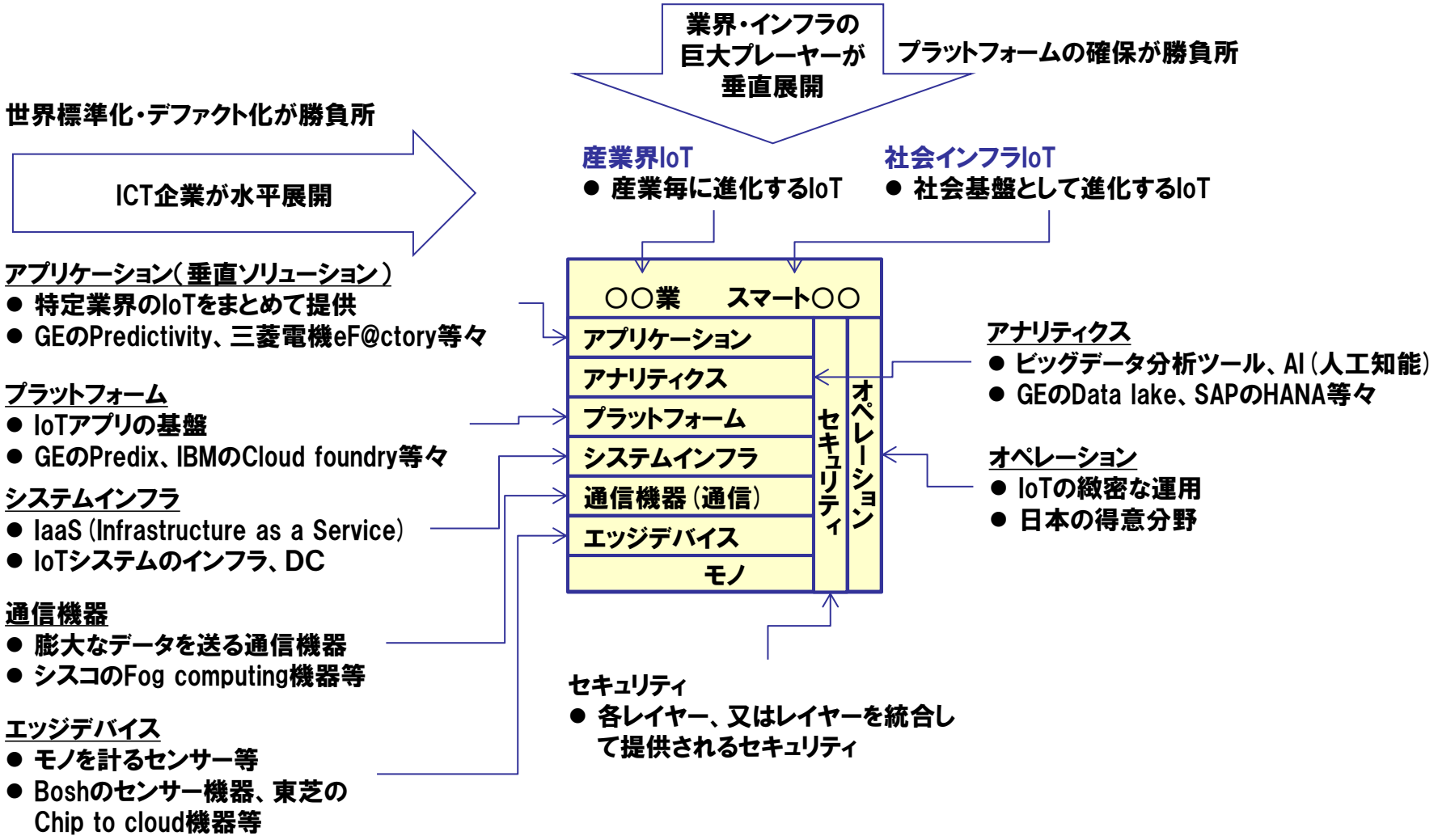
04 基本的な考え方：論点2.IoT政策動向 ①IoTは国主導のドイツと巨大企業主導の米国が先行

国主導のドイツ製造業、巨大企業主導の米国製造業・スマートホーム等が先行し、日本は大きく出遅れている。このままでは日本製造業の優位性がくつがえる可能性がある



04 基本的な考え方：論点2. IoT政策動向
前提：IoTは共通なレイヤー構造をしている

IoTは共通のレイヤー構造を持っておりプレーヤーによって勝負所が異なるので、IoT戦略にはレイヤー構造の認識が欠かせない。各国、各企業はこれらのレイヤーを意識して戦略を打ち出している。



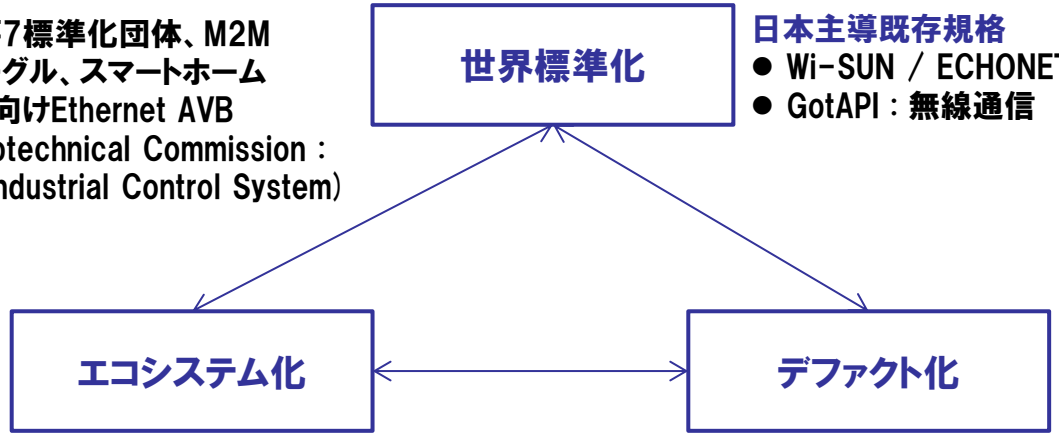
PaaS : Platform as a Service

04 基本的な考え方：論点2. IoT政策動向
前提：IoTの技術標準化動向

現在、IoT規格の標準化をめぐって、世界標準化、デファクト化、エコシステム化の3つの動きがある。産業分野を中心にエコシステム化が存在するのが特徴。現時点で日本は出遅れ気味。

既存規格
- 6LoWPAN：IETF、省電力無線NW
- Zigbee：無線センサーNW
- IP500：大規模省電力センサーNW
- 3GPP：LTEによる大規模無線NW

規格化を目指す団体
- oneM2M：世界主要7標準化団体、M2M
- Thread Group：グーグル、スマートホーム
- TSN：産業・自動車向けEthernet AVB
- International Electrotechnical Commission：制御システム機器(Industrial Control System)



日本主導既存規格
- Wi-SUN / ECHONET：スマートホーム
- GotAPI：無線通信

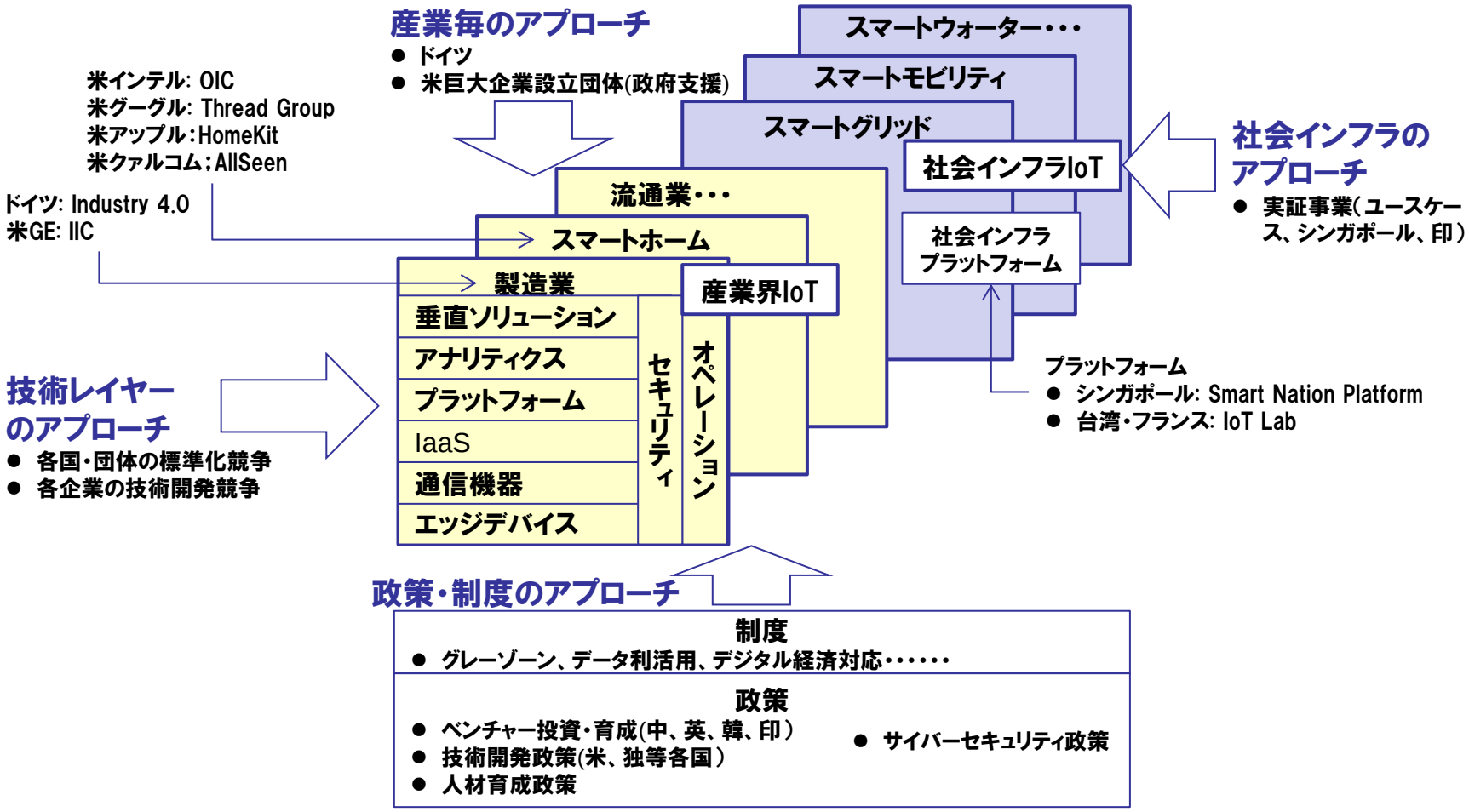
デファクト化を目指す基本技術
- MQTT：IBM、既にオープンソース化
- CSRmesh：英CSR、スマホ接続・制御

エコシステム化から標準化を目指す団体
- Open Interconnect Consortium：インテル、スマートホーム・オフィスから産業分野へ
- Industrial Internet Consortium：GE、製造業など産業分野
- HyperCat：BT等英国企業、オープンカタログ
- Smart Objects Guideline：欧州企業中心、ガイドラインや便利情報

デファクト化を目指す団体／規格
- AllSeen Alliance：クァルコム、スマートホーム
- Homekit：Apple. スマートホーム

04 基本的な考え方：論点2. IoT政策動向 ②各国は国情に合わせたIoT政策を打ち出して推進している

各国は国策としてIoTを推進している。各国のアプローチは、技術レイヤー、産業毎、社会インフラ、政策・制度等に分類できる。

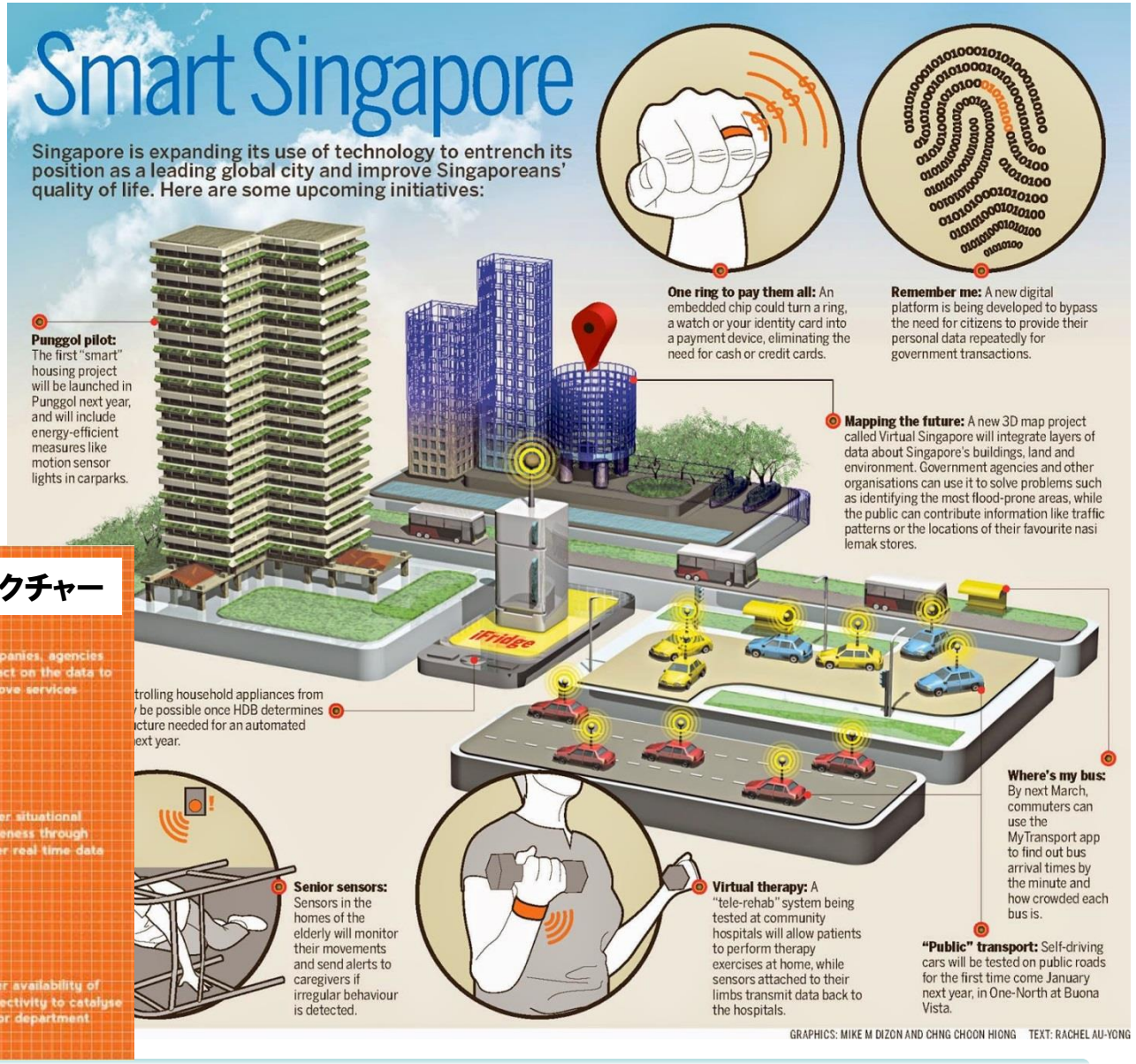


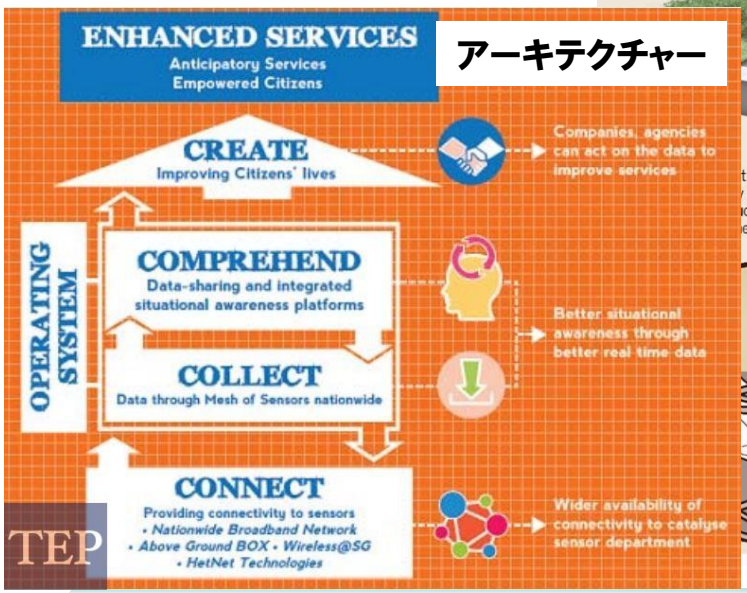
04 基本的な考え方：論点2. IoT政策動向
③重要インフラのIoTでは日本が最先端となる可能性がある

シンガポールは国策として社会インフラのIoT化を推進中

バラバラに進めるのではなく、全体統合でプラットフォーム（Smart Nation Platform）を構築しているのが特徴

個々のインフラに関しては日本の方が先端なものが多い





出所：2015..5.21.当委員会資料

04 基本的な考え方：論点2. IoT政策動向
③重要インフラのIoTでは日本が最先端となる可能性がある

重要インフラのIoT化も本格化し始めたが、日本のインフラは世界的にも高度化で、IoT化により日本が最先端を走れる可能性がある。

高

現在の先進性（イメージ）

低

◎ 防災・気象インフラ
- 気象情報は災害関連情報として重要であり、日本は世界最高レベルにある。エネルギー、スマートウォーター、交通インフラとプラットフォーム層で連携して、リアルタイム処理が必要
- 防災は河川や傾斜地のセンサー情報及び気象情報と連携して防災ソリューションとして重要

◎ 交通管制／ITS
- 高速道路等日本の交通管制は世界トップレベルにあり、ITSは世界と激しく競争している。道路、車、自転車、通行人等のIoT連携で交通安全の向上が期待できる
- 鉄道インフラのIoT化も進み、インフラ輸出が具現化している

◎ スマートエネルギー
- 配送電のスマートグリッド、ビルのBEMS、住宅のHEMS等世界トップレベルにある。太陽光発電などは気象情報と連携すべきで、配管管理は位置情報との連携（GIS）が重要となる。 送電網は世界最高レベル。

○ 位置情報（G空間）
- G空間が完成すれば世界最先端となる。本来は、「モノ」の属性であるが、交通インフラ、防災・気象インフラ、エネルギー、スマートウォーター等とも連携して、重要な情報インフラとなる

△ 国土強靭化（老朽化対策）
- 道路、橋、トンネル等交通インフラの老朽化対策としてセンサー網による老朽化検知、予知予兆検知が重要となり、IoT構造で集めたセンサー情報をアナリティクス層で分析し管理サイクルを回す

△ スマートウォーター
- 上下水道運用管理の民営化が遅れている日本ではスマートウォーターは世界的に遅れている。センサーによる配管管理、遠隔制御等一部技術は優れているが、トータルソリューションとしてスマートとは言えない

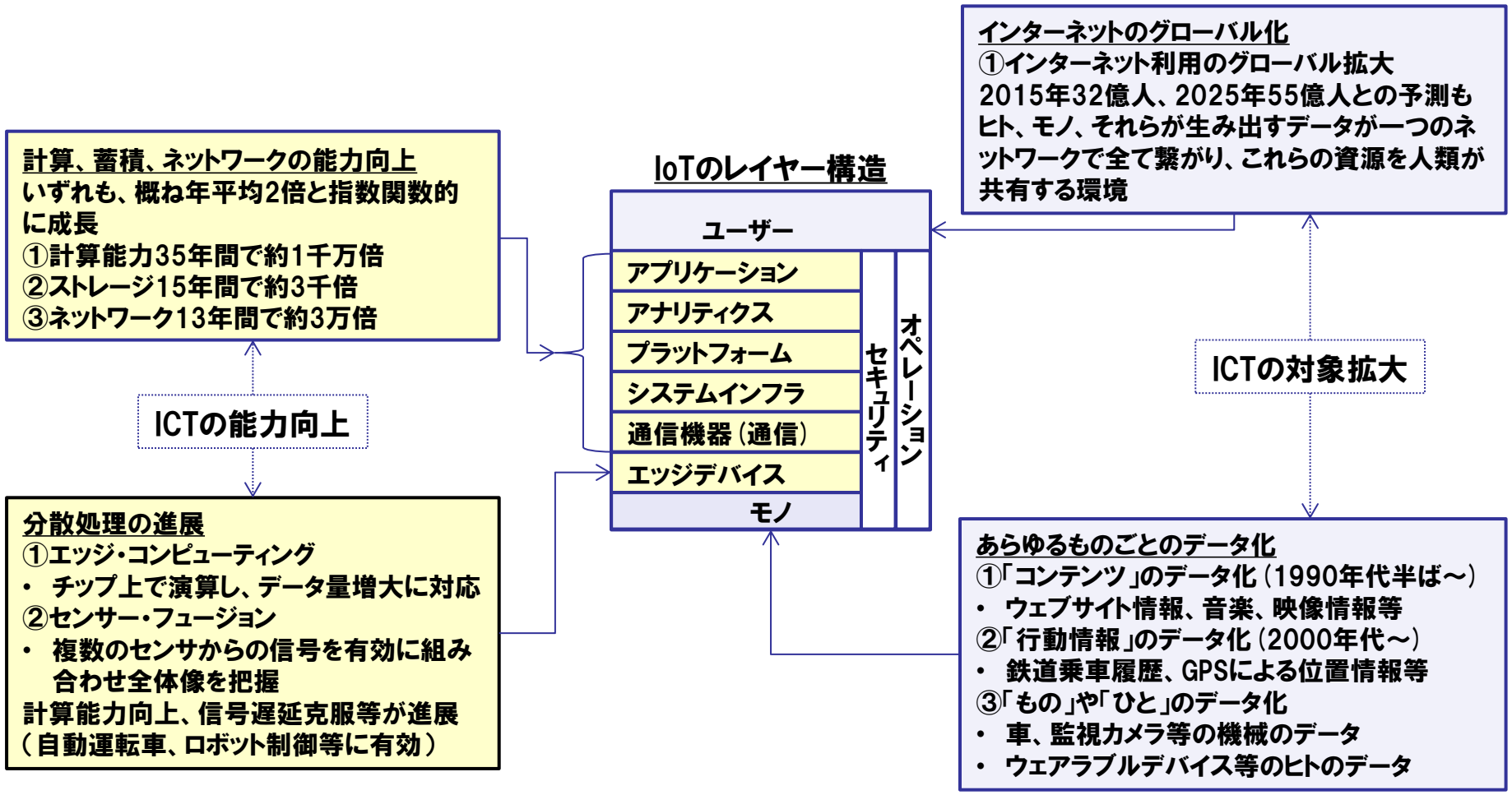
△ 教育インフラ
- 教材コンテンツのデジタル化が進んでいる。バラバラに進めるのではなく、校務も含めてIoTの教育インフラプラットフォームを構築すれば、効率的

× 社会保障（雇用、保険、年金等）システムインフラ（制度ではなく）
- 先進国のシステムインフラとして最も遅れている。世界はシチズンオリエンテッドで社会保障全体が統合運用されているが、日本は縦割の複数システムで運用費は世界の10倍かかっている。マイナンバーとIoTアーキテクチャーによる抜本的な改革が必要

出所：2015..5.21.当委員会資料

04 基本的な考え方：論点3.インテリジェントICT
①ICTがインテリジェント化してIoTを導いている

現在、計算・蓄積・ネットワークの能力向上、分散処理の進展、あらゆるものごとのデータ化等でICTがインテリジェント化している。これらがIoT実現のベースとなっている。



出所：総務省「インテリジェント化が加速するICTの未来像に関する研究会報告書」 自民党加筆

04 基本的な考え方：論点3.インテリジェントICT ②ビッグデータ分析、人工知能、ロボット等インテリジェントなICTが高度化

インテリジェントICTでビッグデータ分析や人工知能、ロボットが高度化し、今後の経済貢献が期待される。ビッグデータ分析や人工知能は、IoTのレイヤー構造ではアナリティクスに相当し、インターネットに接続されて利便性が増す。

- 計算、蓄積、ネットワークの能力向上
- 分散処理の進展
- あらゆるものごとのデータ化
- インターネットのグローバル化

IoTの実現

IoTのレイヤー構造

- ○○業　スマート○○
- アプリケーション
- アナリティクス
- プラットフォーム
- システムインフラ
- 通信機器（通信）
- エッジデバイス
- モノ

セキュリティ　オペレーション

インテリジェントICTで高度化する人工知能

人工知能の高度化
①推論・探索（1950年代後半～1960年代）
②知識表現（1980年代）
③機械学習（2000年代）
④（特徴）表現学習（2010年代）
- ディープラーニング（コンピュータが自ら学習し推論思考、50年来のブレークスルー）

人間（の脳）と人工知能等との連携
①脳情報の解読
- その人が見ていた動画を再構成可能。

②脳活動への外部からの介入
- 刺激により快感、能力向上。人工感覚。

③脳と脳の間の通信
- 800m離れた脳波のやりとりに成功

④仮想現実（VR）や拡張現実（AR）も

ロボットの頭脳

出所：総務省「インテリジェント化が加速するICTの未来像に関する研究会報告書」 自民党加筆

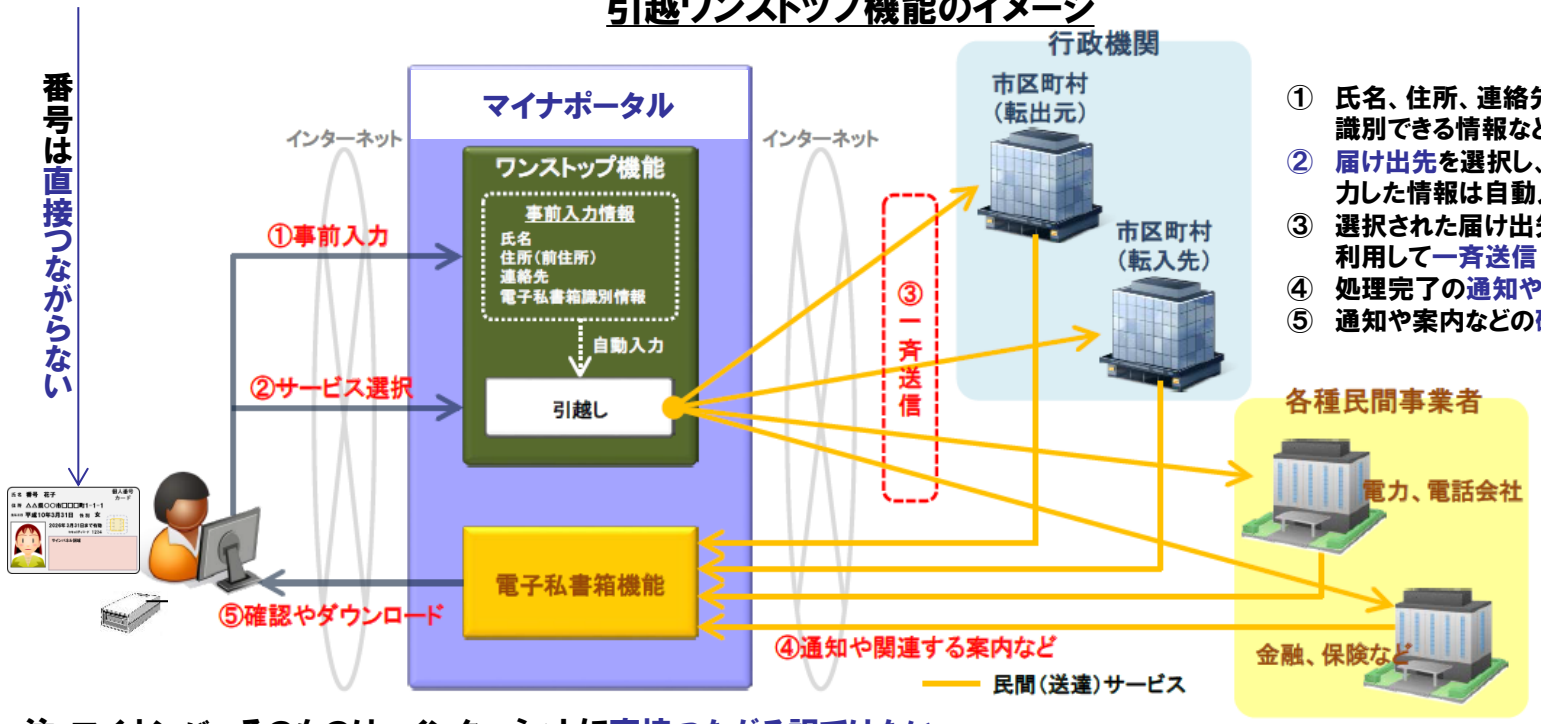
04 基本的な考え方：論点4.マイナンバー
①マイナンバーカードとマイナポータルが重要なプラットフォームとなる

マイナンバーカードとマイナポータルが重要なプラットフォームとなる。ここでは、マイナンバーそのものは、直接インターネットにつながる訳ではないことを認識する必要がある。

接続・利活用対象

- マイナンバーカードの電子証明書（公的個人認証）
- カード上のICチップの空き領域に格納可能なピンコード等
- ICチップに格納された写真情報

引越ワンストップ機能のイメージ



① 氏名、住所、連絡先、電子私書箱の利用者が識別できる情報など、共通項目を事前入力
② 届け出先を選択し、補完情報を入力（事前入力した情報は自動入力）
③ 選択された届け出先に電子私書箱の機能を利用して一斉送信
④ 処理完了の通知や関連する案内などを受領
⑤ 通知や案内などの確認やダウンロード

注：マイナンバーそのものは、インターネットに直接つながる訳ではない

民間事業者は幅広く募り、利便性の向上を図る。

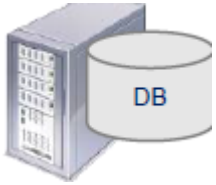
出所：マイナンバー等分科会2015.2.16、自民党加筆

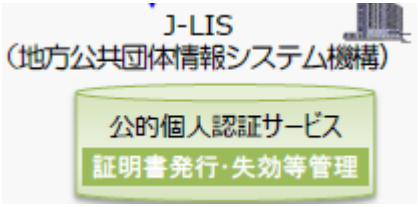
04 基本的な考え方：論点4.マイナンバー
①マイナンバーカードとマイナポータルが重要なプラットフォームとなる

マイナンバーの利活用には構造的な視点が必要。特にIoTではのレイヤー構造でその技術的な利活用方法を定義することが必要で、サイバーセキュリティはレイヤー毎に定義され、第三者による解析・監視が可能となるべき。

マイナンバー制度のIoTレイヤー構造

オペレーション / セキュリティ	アプリケーション	● マイナポータル
	アナリティクス	● 利活用システムの分析機能
	プラットフォーム	● 利活用システムのデータベース等 ● 公的個人認証プラットフォーム
	システムインフラ	● 利活用システムのデータセンター等
	通信機器（通信）	● 公的個人認証のネットワーク ● 利活用システムのネットワーク
	エッジデバイス	● PC、スマホ、ATM等端末のICカードリーダー
	モノ	● マイナンバーカードの電子証明書（公的個人認証） ● カード上のICチップの空き領域に格納可能なピンコード等 ● ICチップに格納された写真情報

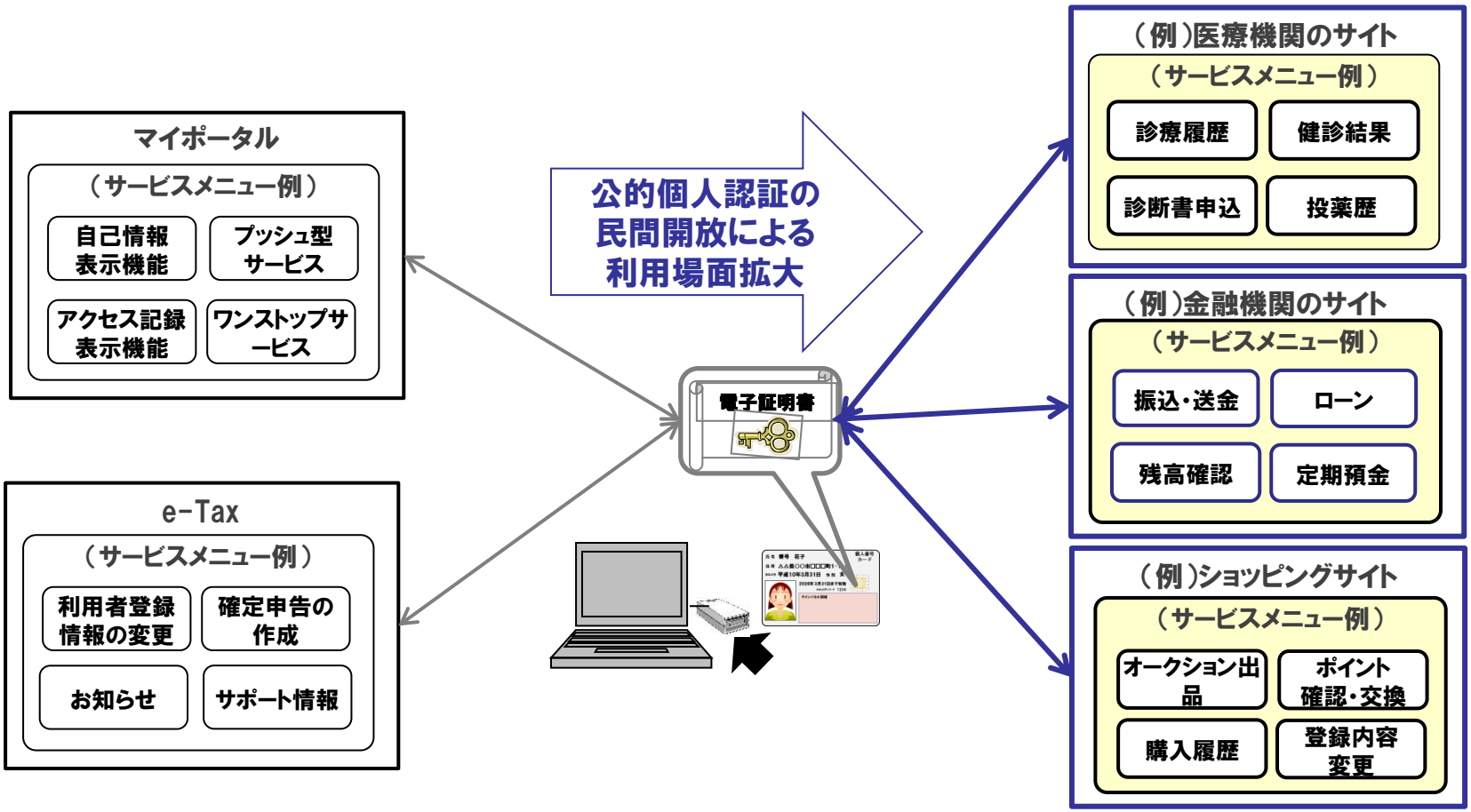




注：マイナンバーそのものは、インターネットに直接つながる訳ではない

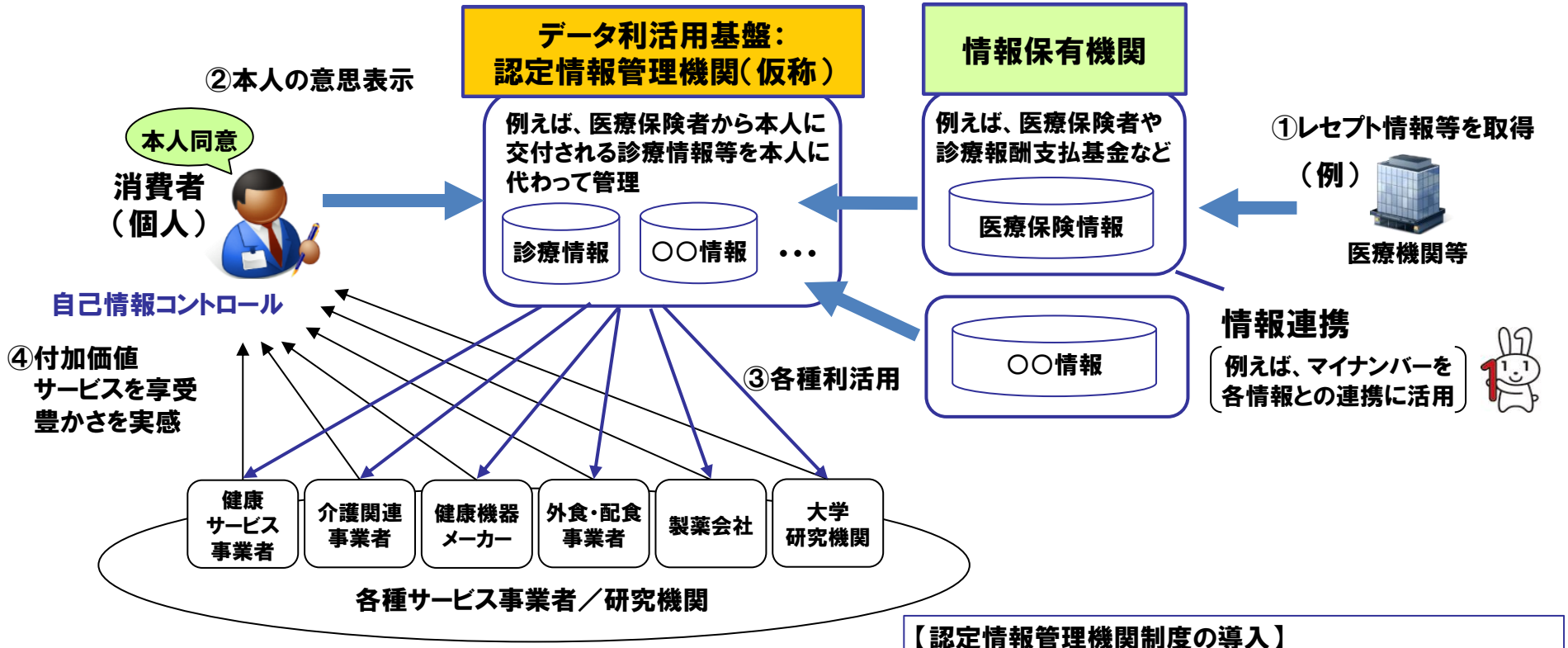
04 基本的な考え方：論点4.マイナンバー ②公的個人認証の民間開放の重要性

公的個人認証の民間開放で、本人確認のプラットフォームとしての利便性が向上する。官民のオンラインサービス間のシングルサインオンを実現するシームレスなトラストフレームワーク（民間認証局が公的個人認証の署名検証者になることでトラストアンカーとなり、認証プラットフォームサービスを民間が提供）が構築される。



04 基本的な考え方：論点5.認定情報管理機関（仮称）
①認定情報管理機関（仮称）で自己情報コントロールしつつデータ利活用

自分の情報（自己情報）を自分で管理し、自分の意思に沿って最善の方法で活用できるようにする自己情報コントロール社会を実現するとともに、データの存在を明らかに、流通や利活用を推進する基盤として、本人に代わって情報管理を行う認定情報管理機関（仮称）があれば、データ利活用の重要なプラットフォームとなる。

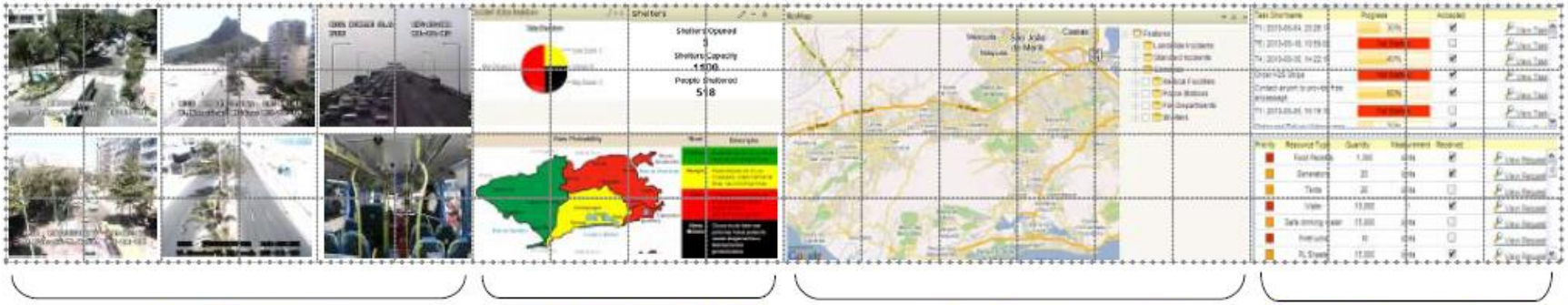


【認定情報管理機関制度の導入】
- 認定情報管理機関制度による透明性の確保
- 円滑なデータ流通・データ利活用

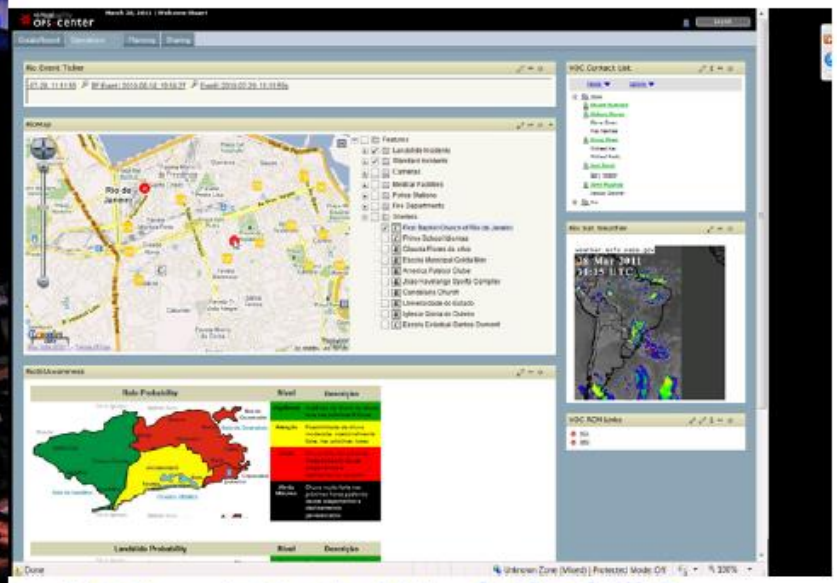
【パーソナルデータの収集と利用に係るルールの明確化】
- 包括同意、利用目的変更の在り方　等

04 基本的な考え方：論点6.プラットフォーム連携 ①気象や位置等の情報と水道や交通、エネルギー等のインフラと連携

ブラジル・リオデジャネイロ市をはじめ先進的な国・自治体では、気象、スマートウォーター、防災といったインフラを連携した統合センター（IOC）を運営している。



リオデジャネイロ市のIOC例



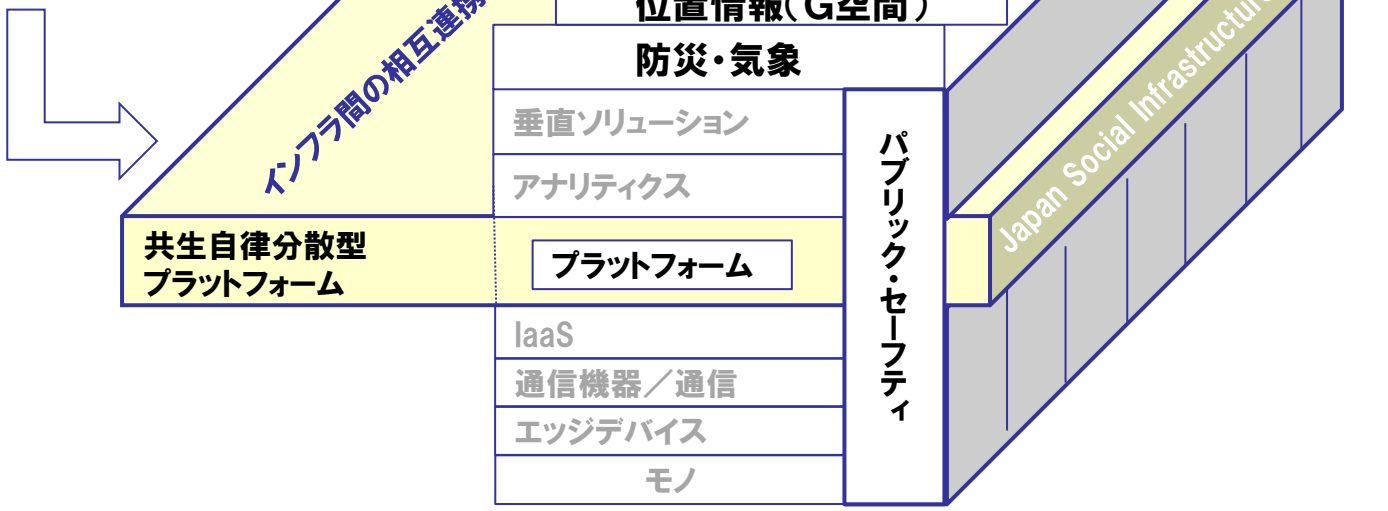
US,Canada,South Africaなどでも導入

IOC：Intelligent Operations Center、IBM社

04 基本的な考え方：論点6.プラットフォーム連携 ①気象や位置等の情報と水道や交通、エネルギー等のインフラと連携

準天頂衛星によるGPS（G空間）、衛星リモートセンシング、気象衛星等の人工衛星技術は、日本が世界的にも優れている。気象や位置等の情報が水道や交通、エネルギー等のインフラと連携して高度化し防災や国民の利便性に貢献する。またインフラ同士も連携によって高度化する。

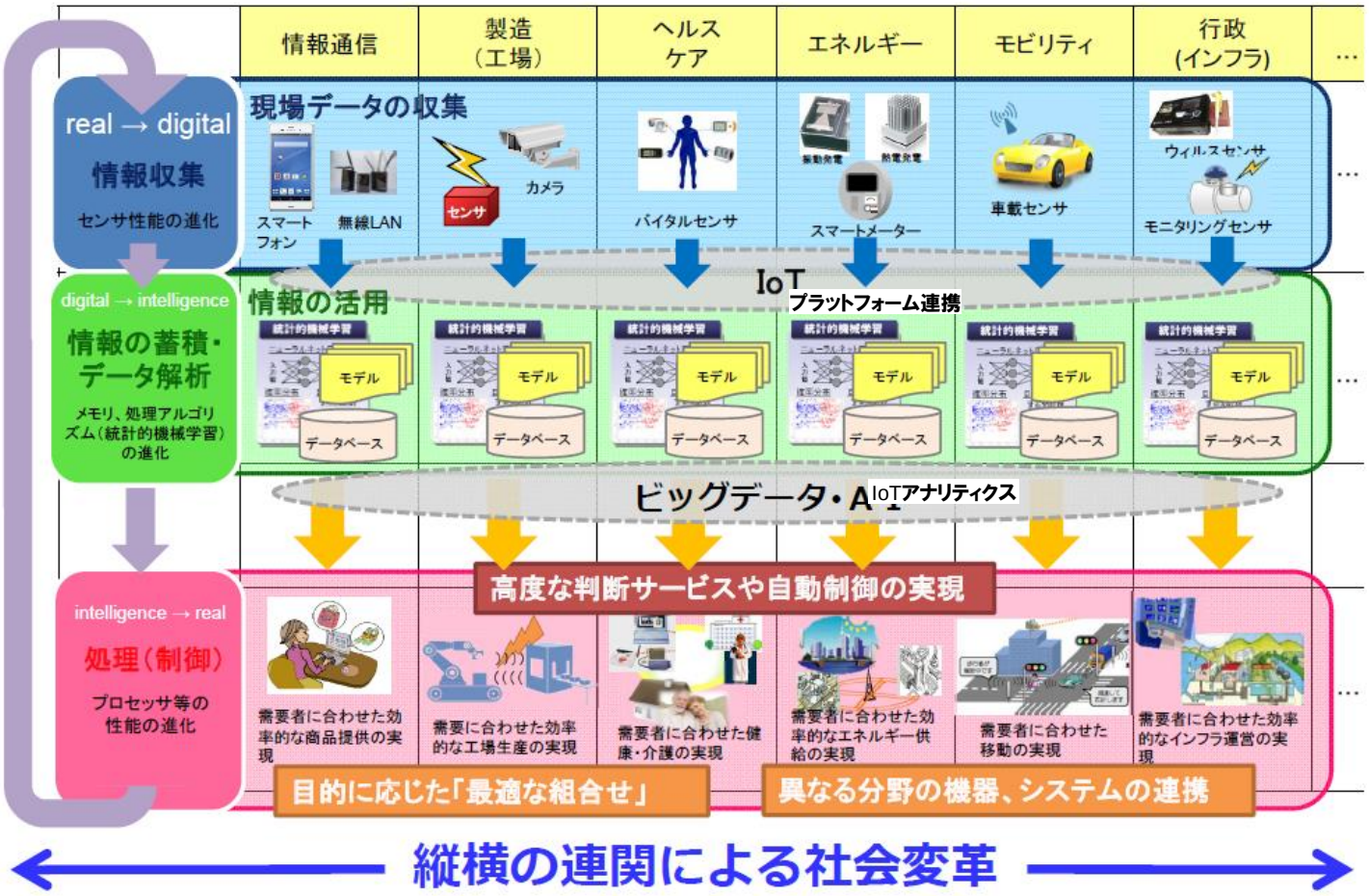
日本の優れた人工衛星技術の利活用
- 準天頂衛星によるGPS（G空間）
- 衛星リモートセンシング
- 気象衛星



04 基本的な考え方：論点6.プラットフォーム連携 ②プラットフォーム連携による産業の高度化

インフラ同士や産業界のIoTはプラットフォーム連携によって高度化し、縦横の連関による社会変革を起こして経済貢献する。

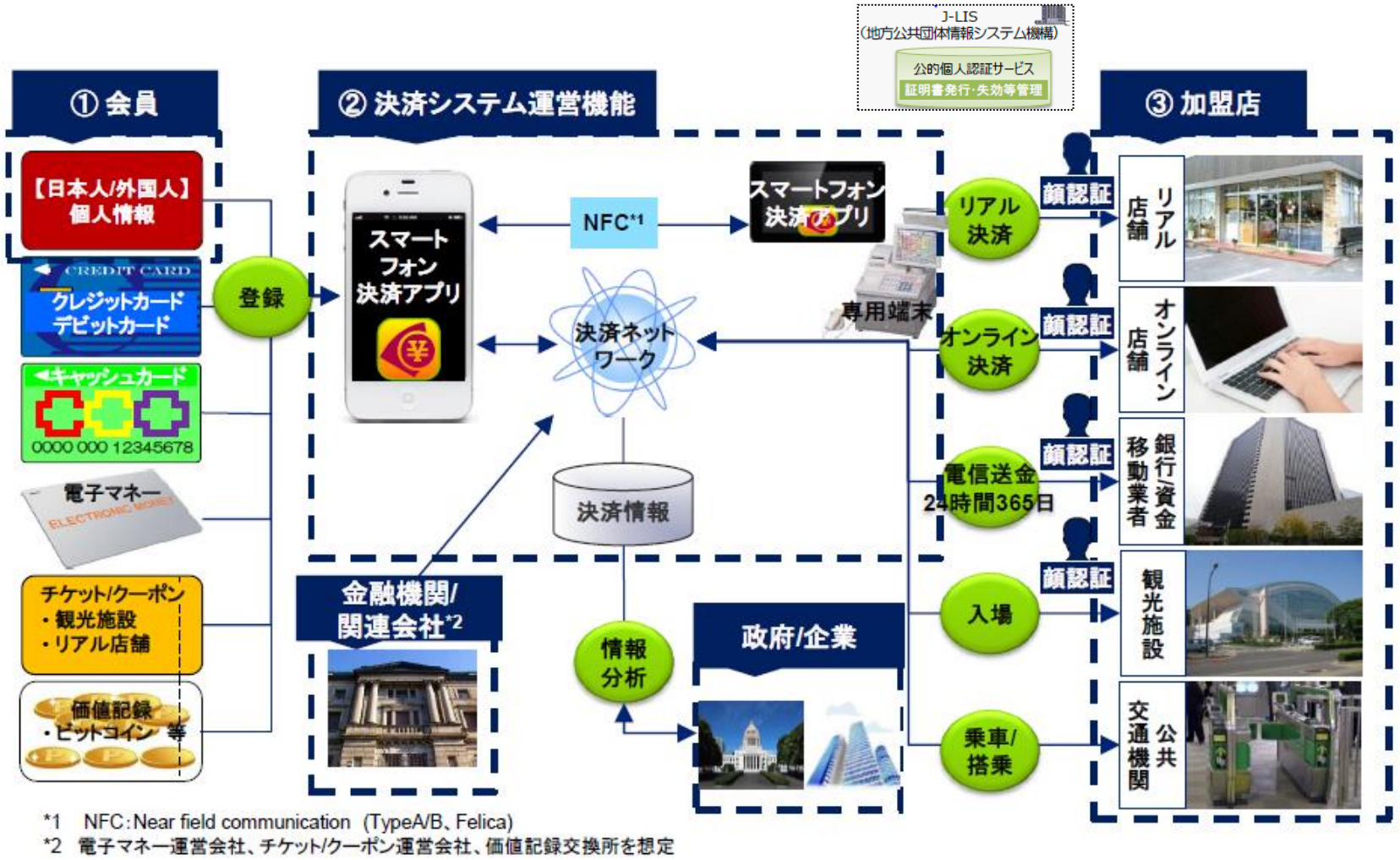
インフラや産業界のIoT化と連携イメージ



出所：産業構造審議会2015.3.4. 自民党加筆

04 基本的な考え方：論点6.プラットフォーム連携 ③決済手段としての「トータルウォレット」のプラットフォーム連携

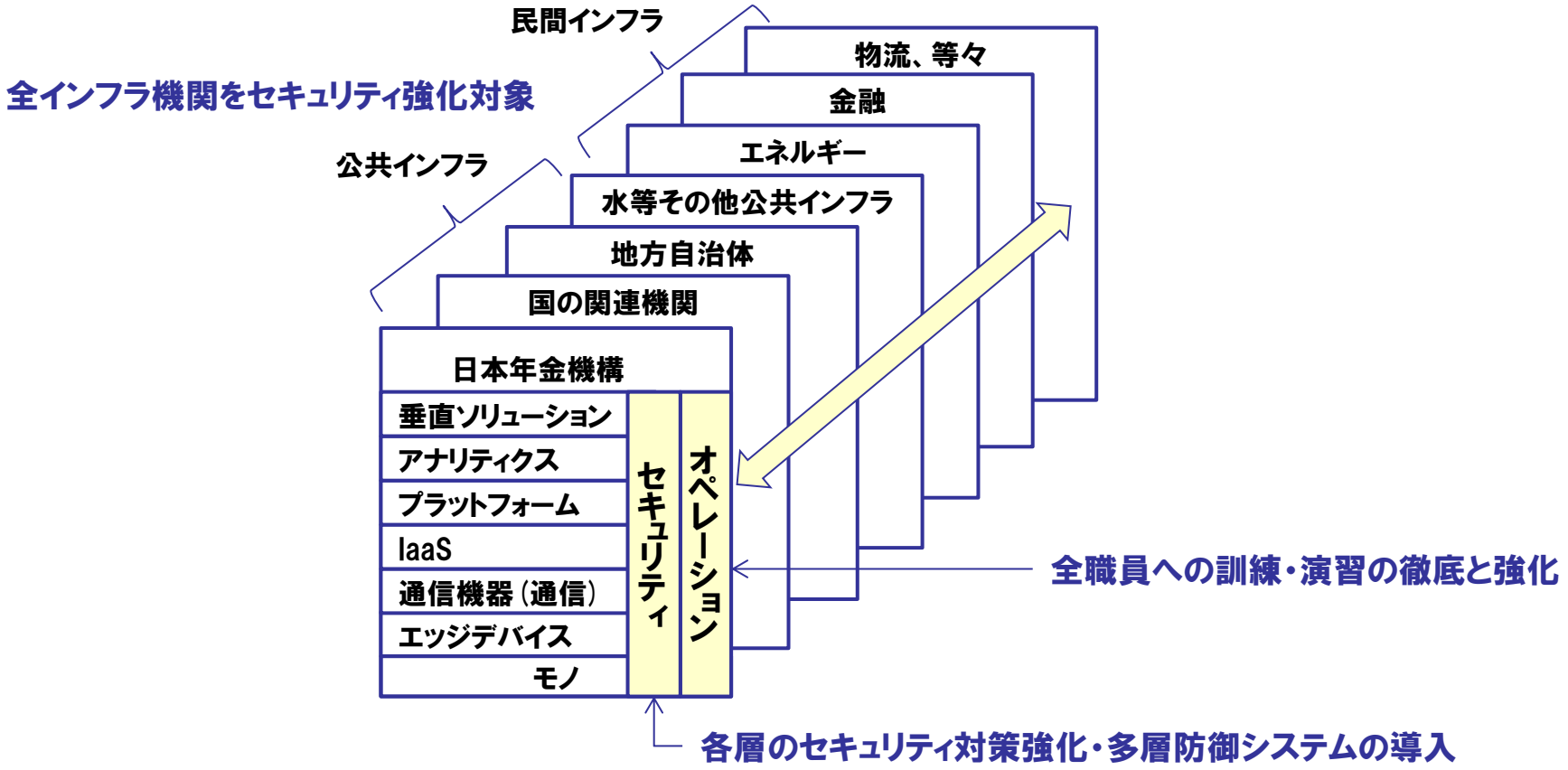
決済システムの利便性の向上、社会的に有効な情報分析・活用、訪日外国人にとっての利便性等を目的とし、様々な決済インフラを統合し、公的個人認証を認証プラットフォームした利便性とセキュリティの高い仕組みとして「トータルウォレット」を国策として推進すべき。



*1 NFC：Near field communication (TypeA/B、Felica)
*2 電子マネー運営会社、チケット/クーポン運営会社、価値記録交換所を想定

04 基本的な考え方：論点7.パブリック・セーフティ ①重要インフラ機関での情報漏洩対策の強化・徹底

日本年金機構での情報漏洩事件を踏まえ、セキュリティ強化対象を社会インフラに関わる全ての機関に拡大し、情報システムの各層に対する技術的なセキュリティ対策強化や多層防御システムの導入、全職員への訓練・演習の徹底と強化を行う必要がある。



04 基本的な考え方：論点7.パブリック・セーフティ ②自治体等取扱組織でのマイナンバー・セキュリティの強化

自治体等取扱組織でのマイナンバー・セキュリティの強化のため、各自治体はマイナンバー制度の適格な運用を監視する運用監視SOC（Security Operation Center）で関連サーバやアクセス端末のログ解析、不正アクセス監視を行い、一方、広域地域（例．道州制ベース）で統合SOCを構築し、管轄自治体から定時ログを得てログ収集解析装置（セキュリティ情報イベント管理、SIEM）によりログ解析して監視機能を強化すべき。また、地域の大学等と連携して人材育成し、派生業務の請負などで地域の雇用を確保すべき。

自治体運用監視SOC ―― 定期送信 → **統合監視SOC観測網**

ログ解析、不正アクセス監視

- 関連サーバ（業務サーバ、運用管理サーバ等）のログを解析し所定の端末以外からの不正アクセスを監視
- アクセス端末(運用管理端末、中間サーバ接続端末)は当該サーバ以外に外部アクセスしていない事をログにより解析

ログの収集解析装置（SIEM）でログ解析

SIEM：Security Information and Event Management

04 基本的な考え方：論点7.パブリック・セーフティ ③パブリック・セーフティの高度化推進

IoT／IoEでモノ、ヒト、プロセス等社会を構成する多くの要素がインターネットにつながってセキュリティの対象となり、サイバーセキュリティはサイバー空間を超えたパブリック・セーフティに発展する。そのため新たに、出入国、重要施設、犯罪監視、防災・救急、群集行動等が対象となる。

サイバー空間のセキュリティ

- 端末（PC、スマホ等）
- ネットワーク
- 情報システム
  - サーバー
  - データベース
  - アプリケーション等

パブリック・セーフティ

シンガポール国策IoT「Smart Singapore」に採用

出所：日本電気株式会社「セーファーシティ」説明資料

04 基本的な考え方：論点7.パブリック・セーフティ ③パブリック・セーフティの高度化推進

パブリック・セーフティでは、生体認証によるセキュリティの確保や映像解析による人物の特定や行動の分析が重要な技術要素となる。また、2020年安心安全のおもてなしとして、観光立国のための観光地の安全確保のためにも、サイバーセキュリティとそれが発展したパブリック・セーフティの技術を確立・強化する必要がある。

生体認証や画像解析でのパブリック・セーフティ

出所：日本電気株式会社当委員会説明資料、自民党加筆

04 基本的な考え方：論点7.パブリック・セーフティ ④重要インフラ防護の高度化

サイバー防御力向上の取組みをさらに強化すると共に、重要インフラ防護のサイバーセキュリティとパブリック・セーフティの技術を強化し、新たに「サイバー／パブリック・セーフティ演習システム」を構築して緊急対応チームの演習を徹底。また、この演習の実施を含め、これまでの官民連携により重要インフラ防護のための高セキュア化研究、国際基準に基づく制御機器のセキュリティ認証、サイバー演習等を実施し、技術を集積・連携してきている制御システムセキュリティセンター（CSSC）の取組を発展させ、重要インフラ防御等のためのセンターとして、国全体の防御力を強化して2020年を迎える。

パブリック・セーフティ（再掲）

サイバー防御力向上の取組み強化

新たに必要な政策

- 制御システム機器の高セキュア化研究、国際標準に基づくセキュリティ認証の推進とユーザーへの浸透、パブリック・セーフティの技術強化
- 「サイバー／パブリック・セーフティ演習システム」の構築
- 緊急対応チーム（CSIRT）の演習の徹底

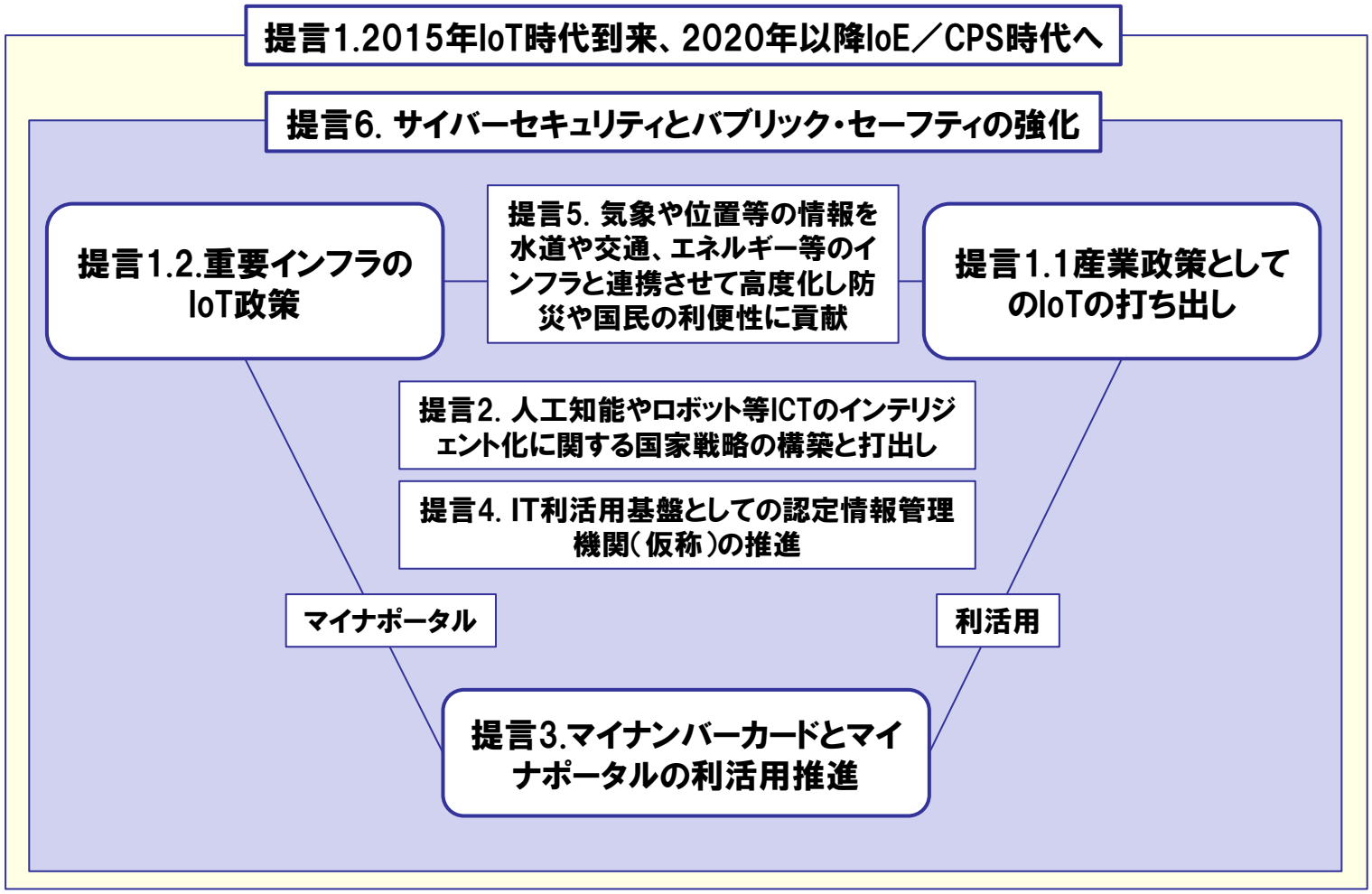
技術を集積・連携してきている制御システムセキュリティセンター（CSSC）の取組を発展させ、重要インフラ防御等のためのセンターとして、国全体の防御力を強化して2020年を迎える

CSIRT：Computer Security Incident Response Team

出所：日本電気株式会社「セーファーシティ」説明資料、自民党加筆

05　提言の構成(１):全体構成

提言の全体構成図



IoT : Internet of Things 全てのモノがインターネットにつながる状態やその技術
IoE : Internet of Everything　モノだけでなく人やプロセス等全てがインターネットにつながる状態やその技術
CPS : Cyber Physical System　サイバー空間とリアル空間が融合し機械と人が共創する知能化社会

05　提言の構成（２）

提言１. 2020年以降のIoE／CPS時代を見据えた国家IoT戦略の構築と打出し

　1.1. 産業政策としてのIoTの打ち出し

　1.2. 重要インフラのIoT政策

提言２. 人工知能やロボット等ICTのインテリジェント化に関する国家戦略の構築と打出し

提言３.マイナンバーカードとマイナポータルの利活用推進

提言４. IT利活用基盤としての認定情報管理機関（仮称）の推進

提言５. 気象や位置等の情報を水道や交通、エネルギー等のインフラと連携させて高度化し防災や国民の利便性に貢献

提言６. サイバーセキュリティとパブリック・セーフティの強化

　6.1. 社会インフラ機関での情報漏洩対策の強化・徹底

　6.2. 自治体等取扱組織でのマイナンバー・セキュリティの強化

　6.3.パブリック・セーフティの高度化推進

　6.4. 重要インフラ防護の高度化

IoT : Internet of Things 全てのモノがインターネットにつながる状態やその技術
IoE : Internet of Everything　モノだけでなく人やプロセス等全てがインターネットにつながる状態やその技術
CPS : Cyber Physical System　サイバー空間とリアル空間が融合し機械と人が共創する知能化社会

06 提言(1)

提言1. 2020年以降のIoE／CPS時代を見据えた国家IoT戦略の構築と打出し

1.1. 産業政策としてのIoTの打ち出し

- 「ガラケー」の二の舞にならないためのIoT及びその先のIoE／CPSを見据えた産業政策を、全産業に関して本年度内に策定すべき
- デバイス、通信、プラットフォーム、アナリティクス(分析)等IoTのレイヤー毎に、世界標準やデ・ファクト・スタンダードの獲得等競争優位性を確保するための方策を明確化し、本年度内に政策として策定すべき
- アナリティクスはビッグデータ分析や人工知能に相当して産業の高度化や高度なロボットの実現に寄与し今後の経済貢献が期待されるので政策的に強化すべき

1.2. 重要インフラのIoT政策

- バラバラに進む交通、スマートエネルギー(電気・ガス)、防災、老朽化対策、スマートウォーター(水インフラ)、教育、社会保障、公共サービス等の様々な重要インフラの高度化に対して、国策として統合的なIoT化を推進し、各インフラの高度化・効率化・相互連携のために、IoTのレイヤー構造の定義と仕組みの構築を本年度から強力に推進すべき
- 従来からのインフラ輸出政策に、本年度からIoTによる高度化を加え、国際競争力を強化した上で、その輸出による経済貢献をはかるべき
- その際、制御システム機器においては国際基準に基づくセキュリティ認証の取得を図るべき

【前提】
- IoTは共通なレイヤー構造(アプリケーション、アナリティクス、プラットフォーム、システムインフラ、通信機器(通信)エッジデバイス、モノ)を持っている(P18)
- IoTの標準化は、世界標準化、デファクト化、エコシステム化の3つの動きで進んでいる(P19)

06 提言（２）

提言2. 人工知能やロボット等ICTのインテリジェント化に関する国家戦略の構築と打出し

- ビッグデータ分析、人工知能、ロボット等ICTのインテリジェント化技術に関する開発と展開を促進すべき
  - 開発に際して企業間連携を促進すべき
  - イノベーションを活かす制度的な対応を早急におこなうべき
  - ビッグデータへのアクセス確保の仕組みを早急に構築すべき
  - 優秀な人材の確保を戦略的にすすめるべき
  - 戦略的に研究開発を促進すべき
- ビッグデータ分析、人工知能、ロボット等インテリジェント化されたICTの導入と活用を早急に国家戦略レベルで推進すべき

06 提言(3)

提言3.マイナンバーカードとマイナポータルの利活用推進

- IoT時代には、個人番号カードの電子証明書(公的個人認証)、ICチップの空き領域に格納可能なピンコード等、ICチップに格納された写真情報等がインターネットに接続されて利活用の対象となることを踏まえ、本年度より、利活用に際してIoTのレイヤー構造でその技術的な利活用方法を定義すべき
- マイナンバーそのものは、直接インターネットにつながる訳ではないことを明確に定義した上で利活用の推進をすすめるべき
- マイナンバー利活用に際しては、IoTのレイヤー毎にサイバーセキュリティの方策を立て、第三者による解析・監視が可能な仕組みを本年度から検討すべき
- 民間に開放される公的個人認証をトラストアンカーにして、シングルサインオン等で国民・企業の利便性を向上すべき

06 提言(４)

提言4. IT利活用基盤としての認定情報管理機関(仮称)の推進

- 自分の情報(自己情報)を自分で管理し、自分の意思に沿って最善の方法で活用できるようにする自己情報コントロール社会の実現のため、本人に代わって情報管理を行う認定情報管理機関(仮称)の構築を推進すべき
- 認定情報管理機関(仮称)は、個人情報保護委員会から認定を受けて業務を行うこととし、匿名加工して提供可能な保有個人情報の種類やデータ量等の情報を定期的に公表するなど、データ利活用を推進する基盤となるよう整備すべき
- 認定情報管理機関(仮称)制度は、官民の別等の組織形態を特に問わず、新規参入も妨げない拡張性のあるプラットホームとすべき。

06 提言(５)

提言5. 気象や位置等の情報を水道や交通、エネルギー等のインフラと連携させて高度化し防災や国民の利便性に貢献

- 準天頂衛星によるGPS(G空間)、衛星リモートセンシング、気象衛星等日本の優れた人工衛星技術から得られる情報を、IoTのプラットフォームで様々な重要インフラと連携させる政策を本年度から検討すべき
- 重要インフラと物流、サービス、農業等様々な産業界のIoTシステムとの連携を可能にし、効率化や産業の高度化を実現すべく、相互のプラットフォーム連携を定義し、仕組みを構築すべき
- 様々な決済インフラを統合し、公的個人認証を認証プラットフォームした利便性とセキュリティの高い仕組みとして「トータルウォレット」を国策として推進すべき

06 提言(6)

提言6. サイバーセキュリティとバブリック・セーフティの強化

6.1. 社会インフラ機関での情報漏洩対策の強化・徹底

- 日本年金機構での情報漏洩事件を踏まえ、「情報漏洩、情報の改ざん、業務途絶への対策」対象機関を社会インフラに関わる全公的機関に拡大すべき
- 情報システムの各構造に対して「情報漏洩、情報の改ざん、業務途絶への対策」を強化する多層防御システムの全機関へ至急導入すべき
- 対象機関の全職員に対して、セキュリティの訓練・演習を徹底し強化すべき

6.2. 自治体等取扱組織でのマイナンバー・セキュリティの強化

- 各自治体はマイナンバー制度の適格な運用を監視する運用監視SOC (Security Operation Center) を構築し、関連サーバやアクセス端末のログ解析や不正アクセス監視を徹底すべき
- 広域地域(例. 道州制ベース)で統合SOCを構築し、管轄自治体から定時ログを得てセキュリティ情報イベント管理 (SIEM Security Information and Event Management) によりログ解析をすべき
- SOC人材として地域の大学等と連携して人材育成し、派生業務の請負などで地域の雇用を確保すべき
- マイナンバー利活用の進展に合わせて、利用組織にも同様の仕組みの構築をうながすべき

06 提言(7)

提言6. サイバーセキュリティとバブリック・セーフティの強化(続き)

6.3.パブリック・セーフティの高度化推進

- IoT/IoEでモノ、ヒト、プロセス等社会を構成する多くの要素がセキュリティの対象となり、サイバーセキュリティはサイバー空間を超えたリアル空間のパブリック・セーフティに発展することを踏まえ、新たに、出入国、重要施設、犯罪監視、防災・救急、群集行動等を加えた総合的なパブリック・セーフティ政策を至急打ち出すべき
- パブリック・セーフティでは、生体認証(顔、指紋、静脈、虹彩等)によるセキュリティの確保が重要となり、「顔パス社会」により利便性も向上することから、プランバシー等の問題にも配慮しつつ、政策的に強化・推進すべき
- パブリック・セーフティでは映像解析により、テロリスト、犯罪者、不審者を特定したり、不審行動の監視、或いは迷子、徘徊者の捜索等国民の安心安全に貢献するため、映像解析を重要技術として政策的に強化すべき
- 2020年安心安全のおもてなしとして、サイバーセキュリティとそれが発展したパブリック・セーフティの技術の確立・強化に従来より大幅な予算を割当てるべき
- 観光立国のために観光地のパブリック・セーフティが重要となることを踏まえ、観光地のパブリック・セーフティを強化すべき
- セーフティをセキュリティ技術とその運用と考えると、日本は運用の観点で優位性があることを踏まえ、パブリック・セーフティの高度化と共に、そのインフラ輸出を推進すべき

06 提言(８)

提言6.IoT時代のサイバーセキュリティとバブリック・セーフティの強化(続き)

6.4. 重要インフラ防護の高度化

- IoTや社会インフラ連携の高度化に伴うサイバー防御力向上のため現在の取組みをさらに強化すべく、予算を大幅に増額すべき
- IoTの観点から重要インフラを防御するためのサイバーセキュリティとパブリック・セーフティの技術を強化し、緊急対応チーム(CSIRT：Computer Security Incident Response Team)の日頃の演習を可能にする「サイバー／パブリック・セーフティ演習システム」の構築と演習の徹底を本年度から検討すべき
- 上記演習の実施を含め、これまでの官民連携により重要インフラ防護のための高セキュア化研究、国際基準に基づく制御機器のセキュリティ認証、サイバー演習等を実施し、技術を集積・連携してきている制御システムセキュリティセンター(ＣＳＳＣ)の取組を発展させ、重要インフラ防御等のためのセンターとして、国全体の防御力を強化して２０２０年を迎える。

参考 各国のIoT政策（１）

国名	国策	産業分野	ポイント
米国	● 2012年「Big Data R&D Initiative」（NSF, NIH, DOD, DARPA等、2億ドル以上） ● IoT団体に対して政府は年間100万ドル以上投資 ● SMART AMERICA Challengeはホワイトハウス直下のプロジェクトでトライアルやExpo開催	2014年多くのIoT団体設立 ● 製造業：Industry Internet Consortium ● スマートホーム：AllSeen Alliance等々	● GE, IBM, インテル、Apple, Google, Qualcomm等各々の分野でデファクトを押さえる巨大プレーヤーが中心となって国際標準化へ向かう ● ホワイトハウスがトライアル
ドイツ	● 2013年には280億円の政府予算、先端クラスターにMax2億ユーロ助成「考える工場」が2億ユーロ獲得 ● 2013年11月「Industrie 4.0 German Standardization Roadmap案」発表 IEC/ISO化の動向を整理・明確化 ● 2025年までに米国と中国を抜いて輸出世界一を目指す	● 2012年から製造業のファクトリーオートメーション（FA）分野で開始 ● 国策と共にSAP、Siemens, Bosh等巨大企業が参加	● SAP,Siemens, Bosh等巨大企業が参加 ● IECでは既にIndustry4.0を念頭に置いたスマートマニュファクチャリングの議論開始 ● 国策で製造業強化 ● SAP元社長が主導
イギリス	● 2014年3月にIoTに約80億円投資と発表、スタートアップ企業やHyperCatに投資 ● 政府肝いりで第2のシリコンバレーを目指すTechCityで数千社のスタートアップコミュニティ育成	● 2014年6月HyperCat設立、BT,ARM,BAE等約40英国企業が参加し、M2Mのオープンカタログを目指す ● 通信大手Arqivaが仏ベンチャーSigfoxと提携して10都市にIoTネットワーク構築 ● ロンドン地下鉄IoT化	● BT, ARM, BAE等巨大企業が参加 ● 規格化重視 ● ベンチャー育成
EU	● 2010年に欧州2020,「欧州デジタルアジェンダ2020」 ● 2014年デジタル単一市場担当副委員長はエストニア、デジタル経済社会担当委員はドイツ		

参考 各国のIoT政策（２）

国名	国策	産業分野	ポイント
中国	● 「Internet+」が2015年国策の行動計画として登場 ● 政府が7500億円のファンドで新興ベンチャーに投資	● スマートメーター2億個既設 ● 中国人民政治協商会議と全国人民代表大会では、中国IT業界のキーパーソンの代表28名が選任	● テンセント、百度、小米、レノボ、ハイアール等巨大IT企業が誕生している ● ベンチャー投資
シンガポール	● 政府IT部門Infocomm Development Authority of Singapore (IDA) がロードマップで、活用領域、進化、ゲートウェイ・ネットワーク、センサー接続を3,5年単位で整理 ● Smart Nation Platform (SNP) でビッグデータ解析で「予期して先手を打つ政府（anticipatory government）」を提唱	● Jurong Lake Distrrictで15事業が20企業協力で進行中 ● この内、「uClim」では狭域気象（microclimate）を監査し定量化、見える化で都市づくり ● IoT@Home Initiativeではスマートホーム（Singapore home）、スマートフォーク、スマートシャツ等々	● 国民生活のプラットフォーム
韓国	● 2011年からIoT支援センターを設立しベンチャー支援 ● 2013年IoT世界標準を目指す「事物インターネット標準化協議会」発足、サムスン電子、LG電子、SKテレコムなど13の企業と、韓国情報通信技術協会（TTA）などの公的機関、学会の専門家らが参加 ● 2014年設立国際標準化組織oneM2Mの総会を誘致 ● 2015年「インターネット新産業育成方案」発表、5万人の雇用創出 ● 通信企業の電波使用料を値下げしてIoTへの投資をうながす計画	● サムソンが米国のスマートホームIoT団体（OIC: Open Interconnect Consortium、Thread Group）の主要メンバー	● ベンチャー投資 ● 標準化重視

参考 各国のIoT政策（３）

国名	国策	産業分野	ポイント
台湾 フランス	● 2014年9月台湾財団法人資策会がパリ第6大学（UPMC）、仏国立情報学自動制御研究所とMOU、UPMC主導EUサポートの「One Lab」と両国が2015年に始動する「IoT Lab」（IoT合同試験用プラットフォーム）の協業 ● IoT Labは仏グルノーブル・ストラスブール間リンクで1千個以上の感知ポイントで合同運用		● 合同プラットフォーム ● 二か国連携
インド	● 2020年にIoT市場を150億ドル規模に拡大、政府が10億円程度投資、National center of Excellence（インキュベーションセンター）設立 ● 上水道や給水所に流れる水の品質や大気の汚染状況をモニタリングするスマート技術、患者の身体の変化を感知し医者に警告を送る技術などを開発する予定 ● 100箇所のスマートシティ化計画		● 社会基盤重視 ● ベンチャー投資

自由民主党IT戦略特命委員会

委 員 長	平井 たくや			
顧 問	逢沢 一郎	棚橋 泰文	小坂 憲次	山本一太
副委員長	石田 真敏	岩屋 毅	金子 恭之	柴山 昌彦
	馳 浩	平沢 勝栄	吉田 博美	
事務局長	福田 峰之			
事務局長代行	木原 誠二			
事務局次長	中川 俊直			
幹 事	大野 敬太郎	菅家 一郎	小林 史明	関 芳弘
	瀬戸 隆一	田野瀬 太道	富岡 勉	藤井 比早之
	星野 剛士	細田 健一	宮崎 謙介	山田 美樹
	磯﨑 仁彦	末松 信介	丸山 和也	三宅 伸吾