資料5

安全なIoTシステムのセキュリティに関する一般的枠組についての素案（今後の取組）

平成２８年１０月３１日

内閣サイバーセキュリティセンター

○概要

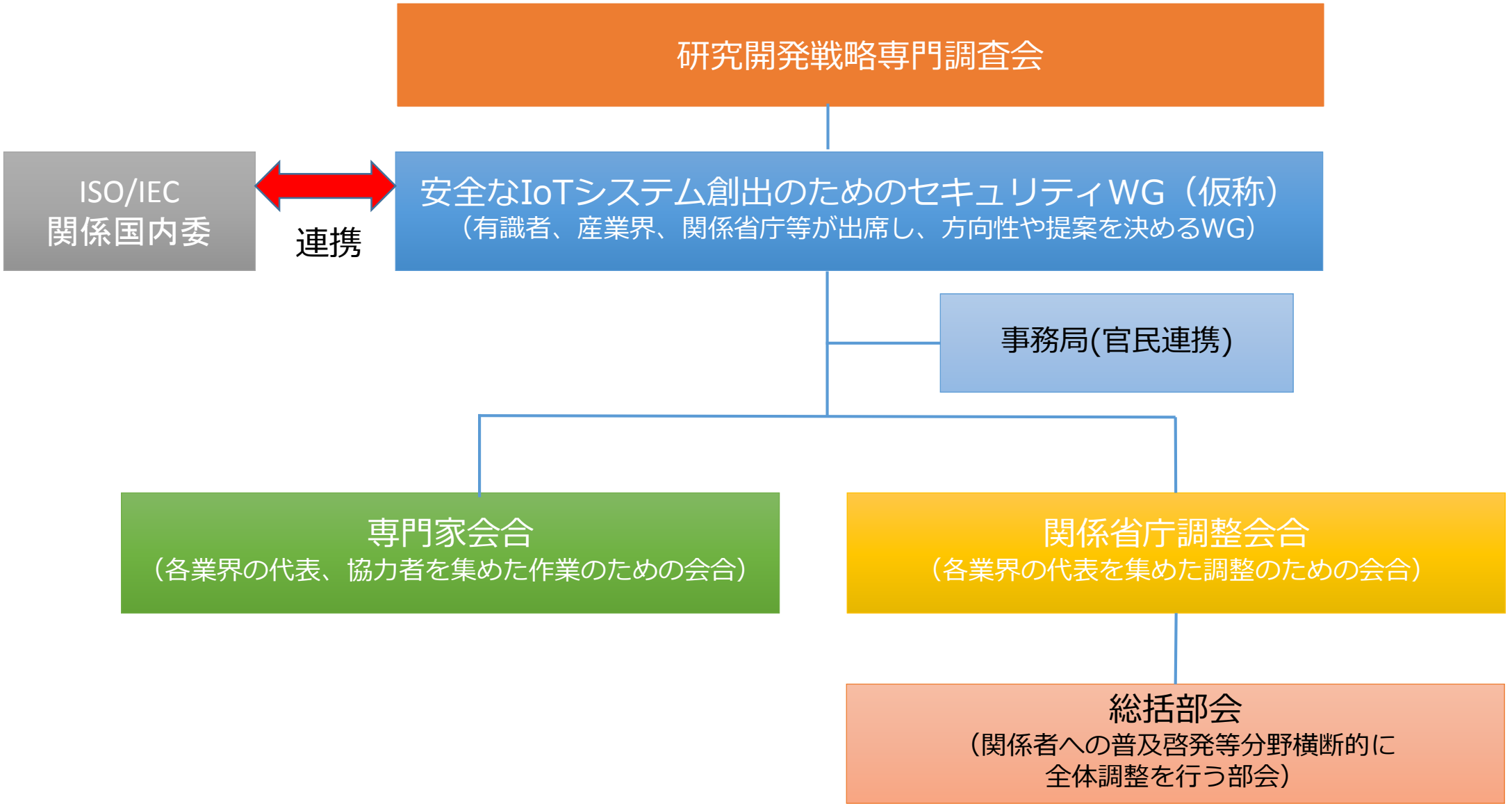
（1）目的

- 我が国では、IoTブームに伴い、セキュリティ対策の事例集が多数策定されているが、情報系のセキュリティの延長線で作成されているところ。
- 今後はこうした取り組み加え、我が国の強みである安全や機能が提供する品質の高さの確保と関連付けていく取り組みが必要と思われる。
- このため、「安全なIoTシステムのためのセキュリティに関する一般的枠組」を基礎とした我が国発のIoTシステムセキュリティの国際標準化に貢献する。
- こうした取り組みを通じて、**我が国の高い製品の品質を「セキュリティ」の局面においてもブランド価値として、国際競争力強化に活かし**、**セキュリティ対策の強化を推進**していく。

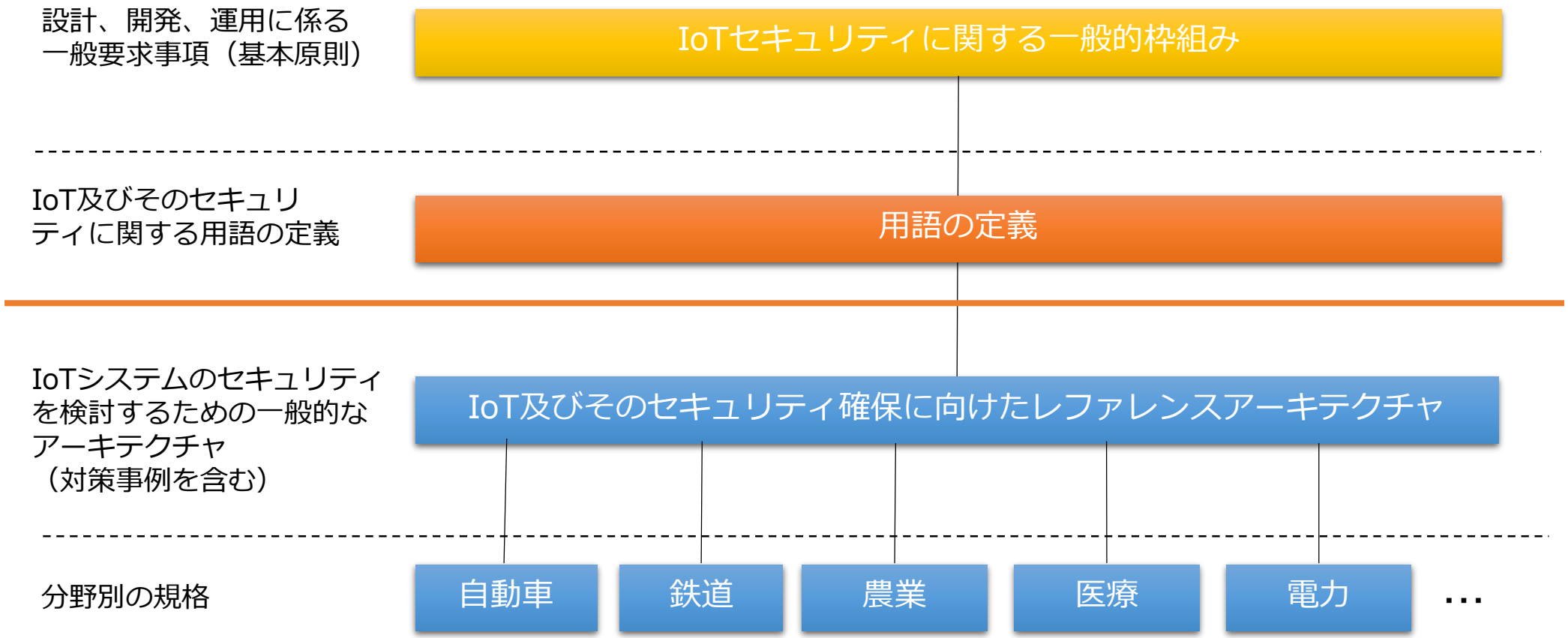
（2）当面のアウトプット

- **IoTセキュリティのフレームワークの国際標準化に向けた日本案の策定**
  → 一般的枠組をベースにしつつ、国内で議論・調整を行い国際標準を目指す
- **フレームワークを各分野に適用するための関係者の理解促進やアクションプランの策定**
  → IoTセキュリティのフレームワークをベースとした**関係者への普及・啓発**
  →具体的なサービスインに向けた**分野別の規格等の策定**(製品や事業に対する規制法におけるIoTセキュリティに関するセキュリティ基準策定)**の方向性検討**

○検討体制(素案)


研究開発戦略専門調査会
ISO/IEC
関係国内委
連携
安全なIoTシステム創出のためのセキュリティWG（仮称）
（有識者、産業界、関係省庁等が出席し、方向性や提案を決めるWG）
事務局(官民連携)
専門家会合
（各業界の代表、協力者を集めた作業のための会合）
関係省庁調整会合
（各業界の代表を集めた調整のための会合）
総括部会
（関係者への普及啓発等分野横断的に
全体調整を行う部会）

規格体系(素案)


設計、開発、運用に係る
一般要求事項（基本原則）
IoTセキュリティに関する一般的枠組み
IoT及びそのセキュリ
ティに関する用語の定義
用語の定義
IoTシステムのセキュリティ
を検討するための一般的な
アーキテクチャ
（対策事例を含む）
IoT及びそのセキュリティ確保に向けたレファレンスアーキテクチャ
分野別の規格
自動車
鉄道
農業
医療
電力
…

（参考１）国内外の取組

○主な国内の民間の取組

・　本年２月、日本クラウドセキュリティアライアンス（米国発のクラウドコンピューティングのセキュリティを確保するための業界団体(CSA)の日本版非営利法人。セキュリティ対策機器関係の企業、認証機関等から構成）が、IoTシステムのセキュリティを確保するために、脅威のとらえ方や、対策に向けたポイントをまとめたガイダンス（CSAが策定したものの和訳）を発行。また、本年４月には、IoTシステムへの脅威に対する影響評価の方法についてまとめた文書も発行。

・　本年６月、JNSA（セキュリティベンダーの業界団体）がコンシューマ向けIoTセキュリティガイドを発行。IoTシステムに対するサイバー攻撃の脅威の具体例を示したうえで対策例を提示。

○海外における主な動き

・　昨年９月より、IIC（Industrial Internet Consortium、米国企業（Cisco, Intel, IBM, GE, AT&T）が中核となって設立）がIoTシステムへのセキュリティを組み込むためのフレームワークを策定中。

・　本年２月、GSMA（移動体通信事業者の国際的な業界団体）が、IoTの脅威と対策方法に関するガイドラインを発行。

・　本年５月、米国商務省傘下のNISTがCPSフレームワークを策定。任務保証の考え方に基づき、IoTのシステムのサービス品質を確保するための基本的な考え方と考慮すべき重要なポイントを提示。

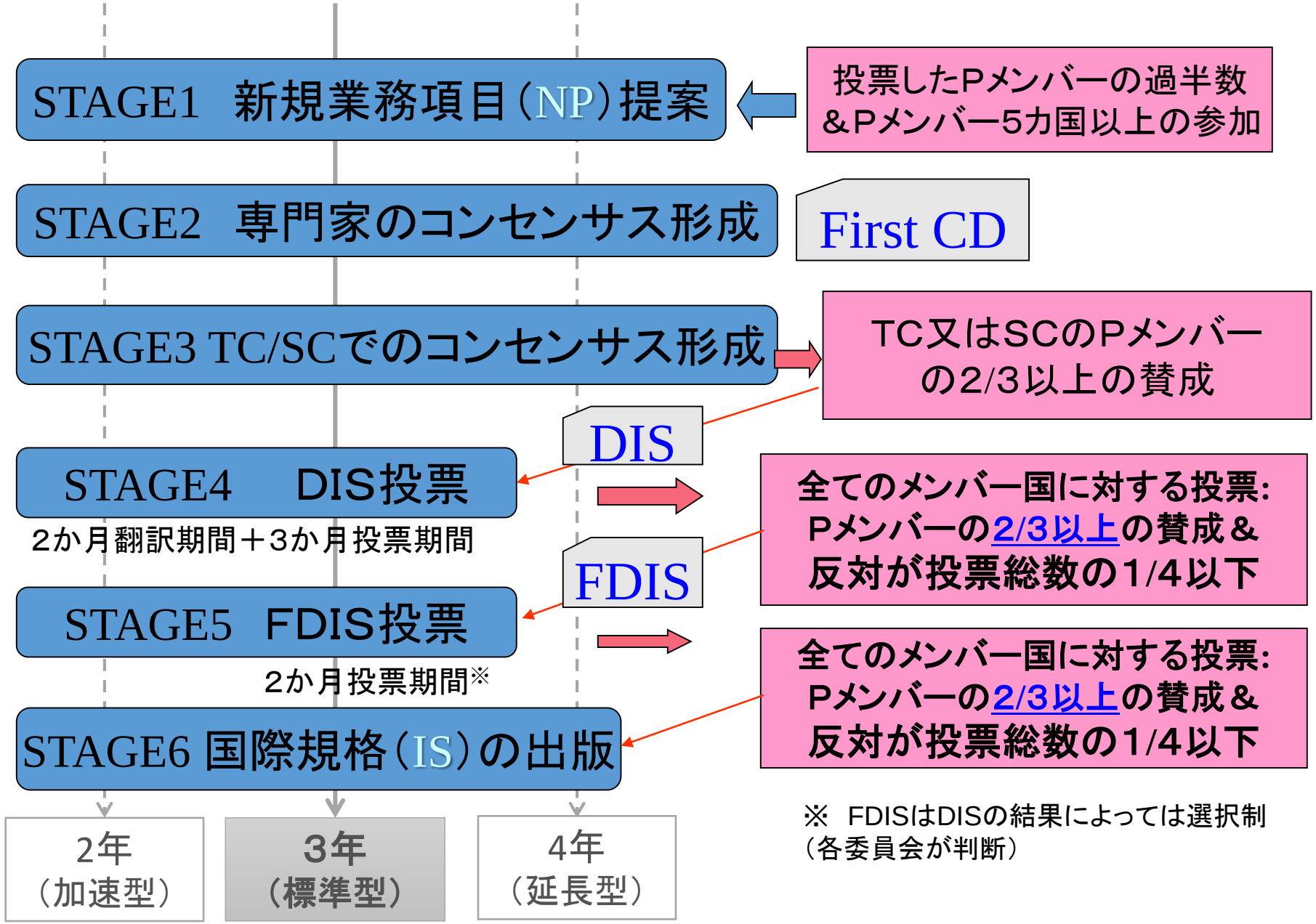
・　本年８月２日、米国商務省国家通信情報局が、IoTの利益・課題・政府の役割についてのパブリックコメント実施結果を公表（別添参照）

○国際標準化の動き

・　ISO/IEC JTC1 SC27 において、IoTシステムにおける安全性・信頼性（セキュリティを含む）を実装するための標準策定に向けた検討が行われている。ワーキンググループで内容を検討している状況。（WDステージ）

・　ITU-T　CG-IoTSEC（SG17とSG20の合同グループ）において、IoTセキュリティおよびプライバシーに関する標準化の検討が行われており、報告書のとりまとめ作業を行っている。

（参考）ISOにおける一般的な国際規格(IS)開発の流れ



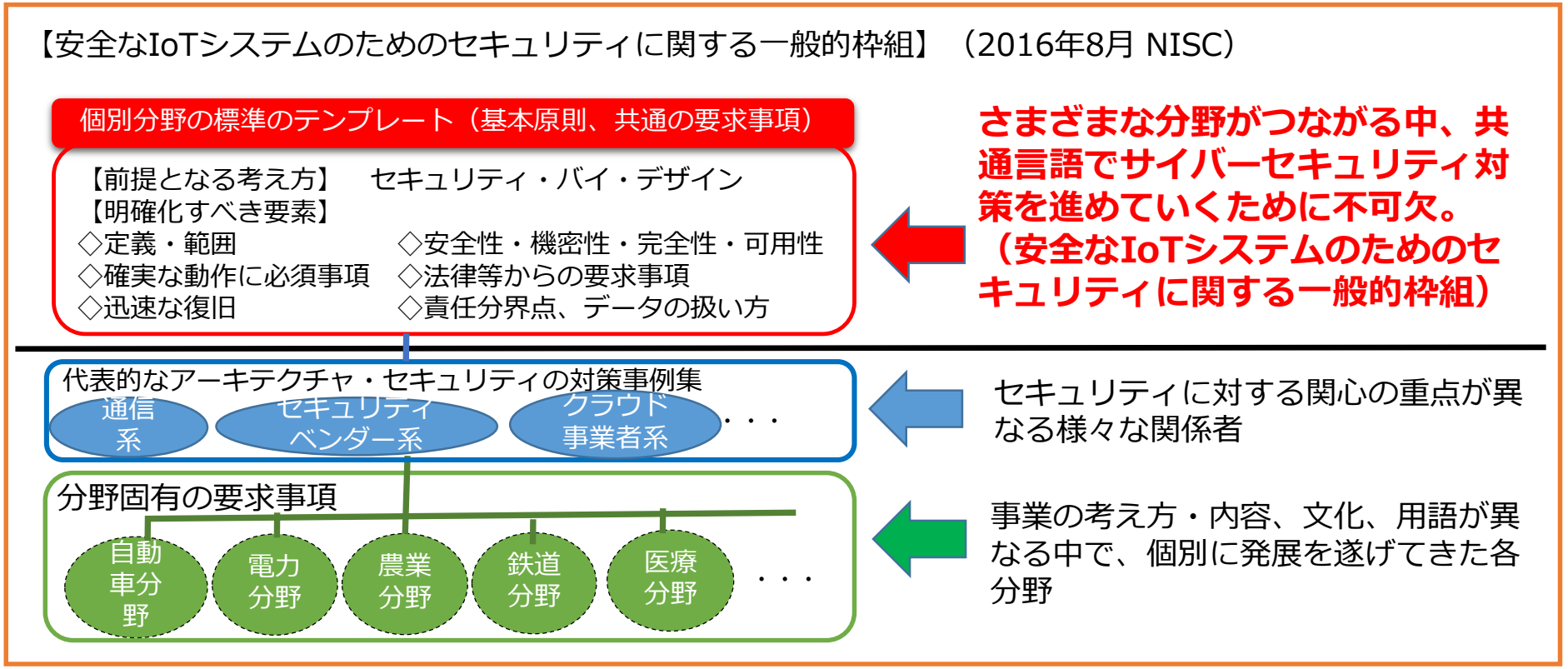
※　FDISはDISの結果によっては選択制
（各委員会が判断）

（参考）ISOにおける国際規格開発プロセス

ステージコード	段階（Stage）	関連文書の名称	文書の略称	省略の可否	Directives掲載箇所
(00)	（予備段階） (Preliminary stage)	（予備作業項目） (Preliminary work item)	PWI		Part1-2.2
10	提案段階 Proposal stage	新業務項目提案 New work item proposal	NP	（※）	Part1-2.3 Part1-AneexF
20	作成段階 Preparatory stage	作成原案 Working draft	WD	○	Part1-2.4 Part1-AneexF
30	委員会段階 Committee stage	委員会原案 Committee draft	CD	○	Part1-2.5 Part1-AneexF
40	照会段階 Enquiry stage	国際規格案 Draft International Standard	DIS		Part1-2.6
50	承認段階 Approval stage	最終国際規格案 Final draft International Standard	FDIS	○	Part1-2.6.1 Part1-2.7
60	発行段階 Publication stage	国際規格 International Standard	IS		Part1-2.8
90	見直し段階 Review stage	※IS発行後、5年ごとに定期的な見直し（Systematic Review, SR）を行う。			Part1-2.9 Sup. 2.9
95	廃止段階 Withdrawal stage	※規格の見直しの結果、①確認、②追補・改訂、③廃止の選択肢がある。			Part1-2.9 Sup. 2.9

→このプロセスとはまた別に迅速法による手順（Fast-track procedure）も存在。（Dir. Part1 Annex F参照）
※基本的にNP投票は必要。迅速法など、特殊な場合のみNP投票が不要となる。

（参考）安全なIoTシステムの創出に向けた取組



上記体系でサイバーセキュリティ対策を進めるために今後必要な取組例

【国際標準化に向けた取組】
米国等の主要国と連携し、ISOなどの国際標準への提案に向けた取組を検討。今後策定される各分野固有の国際基準等について、標準のテンプレートを踏まえたものにし、我が国の強みを国際標準に反映していく。

【日本国内の基準等への適用】
日本国内の様々な関係者が策定する基準やガイドラインについて、標準のテンプレートをベースとしたものとなるよう促し、展開を図ることで我が国のIoTシステムの国際競争力を高めていく。

別添

米国商務省国家通信情報管理局
IoT の利益・課題・政府の役割についてパブリックコメント実施

米国商務省(DEPARTMENT OF COMMERCE:DOC)の国家通信情報管理局(National Telecommunications and Information Administration: NTIA)は、2016 年 4 月 6 日に「IoT の進展を促進するための利益、課題及び政府に求められる役割に関するコメント要求」(Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things)(以下「IoT のための RFC」という。)を Federal Register (連邦官報) に告示し、2016 年 6 月 2 日までの期間で意見を募集しました[1]。2016 年 8 月 2 日に寄せられた意見が公開された[2]ことから、NTIA が質問を行った 28 項目と様々な団体・企業からの回答の概要をまとめています。IoT にどのような課題があるのか、IoT 政策について米国政府機関はどうあるべきか、に関する主要な米国企業の意見を報告します。

コメント全般を通じてみると、IoT の進展によって様々なモノが連接されることによるセキュリティ上の懸念やプライバシー保護に関する懸念が課題としてあげられており、これを解決するために、政府は縦割りではなく統一的なアプローチをとること、その際過度な規制によってイノベーションを阻害することのないよう留意することが求められています。IoT は今後ますます社会システムそのものから切り離して考えることはできなくなっており、IoT セキュリティは IT セキュリティの域を超えて社会セキュリティともいうべきものとなっていくことを示唆するコメントが多数見受けられました。

1. 告示の背景

連邦官報によると、商務省は、デジタルエコノミーの発展を促進し、インターネットがイノベーションのためにオープンであり続けることを確保することを最優先とした施策を行ってきた。NTIA は、現在の技術及び政策の見直しをするために、IoT のための RFC を行うこととしたと説明している。NTIA はコメントを踏まえて、技術発展に影響を及ぼす課題を特定し、潜在的な利益を課題及び民間セクターとともに IoT 技術の発展を促進するために連邦政府が担うに望ましい役割を明らかにした報告書[3]を公表するとしている。また、2016 年 8 月 2 日 NTIA のブログページで NTIA 副次官補アンジェラ・シンプソンが寄せられたコメントの公開[4]を行い、次のように説明している。

「IoT は様々な利益を消費者へ提供するが、IoT のユーザにとっては、IoT 機器とアプリケーションは安全であるという保証が必要になる。そのためには、IoT 機器またはアプリケーションの潜在的なセキュリティ上の脆弱性へ対応しなければならず、パッチを当てて、セキュリティのアップグレードをする必要がある。しかし、現時点でセキュリティアップグレードをサポートする共通で広く受け入れられた定義はないため、ユーザはサポート内容を知ったうえで製品やサービスを購入するという選択肢がない。IoT 製品について利用者がより良い理解をできるように、新しいマルチステークホルダープロセスを

---

[1] *http://www.ntia.doc.gov/print/press-release/2016/us-department-commerce-seeks-comment-potential-policy-issues-related-internet-thi, http://www.ntia.doc.gov/federal-register-notice/2016/rfc-potential-roles-government-fostering-advancement-internet-of-things, http://www.ntia.doc.gov/files/ntia/publications/fr_rfc_iot_04062016.pdf, 当初は5 月 23 日までの期限でしたが、その後5 月 11 日に期限を6 月 2 日まで延長することとされました。(http://www.ntia.doc.gov/federal-register-notice/2016/extension-comments-period-potential-roles-government-fostering-advancement-iot)*

[2] *http://www.ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fostering-advancement-internet-of-things*

[3] *http://www.ntia.doc.gov/files/ntia/publications/fr_rfc_iot_04062016.pdf,「green paper」とされており、議論を促進するための文書としての位置づけになります。*

[4] *http://www.ntia.doc.gov/blog/2016/increasing-potential-iot-through-security-and-transparency*

計画している。」

NTIA は IoT の利益・課題・政府の役割についてパブリックコメントで集まった情報を参考に、2016 年 10 月の第 3 週にマルチステークホルダープロセスを立ち上げとしている[5]。

2. NTIA の質問項目の概要と寄せられた回答の概要

IoT のための RFC は、IoT 全般、技術、経済、政策課題、国際関係及びその他の論点の 6 項目、計 28 の質問に対するコメントを求めるものである。

(1) IoT 全般に関する質問
既存の技術とIoTが進展していくために必要な技術との相違やそれに対する課題、既存の法令や政策等との整合性をどのように図っていくのか、IoT 社会全般の規律をどのように考えていくべきかといったことが中心となっている。

(2) 技術に関する質問
技術的課題がどのような性質のものであり、政府が当該課題を克服していくためにできることがあれば、それを把握することが重要であるとの認識から質問が作成されている。

(3) 経済について
IoT が米国経済に与える影響を見積もることを目的としており、特に米国経済社会における IoT の役割及び経済社会に対する IoT の影響を数値化することを行っていくことに関する質問となっている。

(4) 政策課題
重要なサービスに関する機密性、完全性、可用性及びレジリエンス、個人情報保護やプライバシーの観点からの質問となっている。

(5) 国際関係
標準化組織や国際組織等、諸外国や国際機関によって IoT を前提とした取組を背景に、こうした機関等とどのように協力していくかという観点から質問がなされている。

28 の質問に対して 138 の団体・企業・個人から回答が寄せられたところ、NISC が発行した「安全な IoT システムのためのセキュリティに関する一般的枠組み」[6]に基づき有益と思われるものを以下の 6 項目に集約し、それに対する主要な団体・企業[7]から寄せられたコメントをまとめました。NISC が発行した上記一般的枠組みは、特に下線部で示したように米国における連邦政府への期待を先取りしたものと評価でき、今後の日本政府の積極的な活躍が期待されます。

[5] *http://www.ntia.doc.gov/speechtestimony/2016/remarks-angela-simpson-fostering-advancement-internet-things-workshop*
[6] *安全な IoT システムのためのセキュリティに関する一般的枠組(http://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf)*
[7] *米国の主要な団体(自動車連盟、民生技術協会、消費者連合)や主要な IT 系企業(IBM、Microsoft、Verizon、ARM)や著名なコンサルティング会社(Booz-Allen-Hamilton)の 10 組織の回答をまとめた*

① IoT の課題についての質問(No.1,4,18) 「IoT によって引き起こされる課題や新たなチャンスは、我々がこれまでに経験してきたことと違うか、違うならどのように違うのか？」	
Consumer Technology Association（全米民生技術協会）	● 現在、IoT に関する最大の課題は、連邦政府がバラバラに推進していることである。例えば、National Highway Traffic Safety Administration(NHTSA)や Food and Drug Administration(FDA)は、既に車や医療デバイスのインターネット接続によって生じるセキュリティや安全性の問題に取り組んでいる。また、Federal Trade Commission(FTC)は IoT に関連した消費者のプライバシー問題やサイバーセキュリティを識別していて、現時点で可能なベストプラクティスを提供している。 ● 連邦政府が別々に対策を進めることは、IoT の発展に大きなダメージを与える。例えば、FDA の規則である HIPPA は、医療健康器具ベンダが提供するウェアラブル端末に適用されるが、それらの器具は小売店で販売されることから FTC の規則で異なった要求をされることもある。消費者向け IoT はケースバイケースの法制度を適用される。従って、特定の IoT 機器またはアプリケーションに適用される具体的な法律、規則及び規制はいつも明らかなわけではないかもしれず、重複するか、矛盾しさえするかもしれない。
Consumer Federation of America（全米消費者連合）	● IoT の課題は、プライバシー、セキュリティ、透明性、知的財産権、継続性、選択権、救済制度の整備である。 ● IoT は個人のプライバシーを守る権利に新たな課題を突き付けている。デバイスに埋め込まれたセンサーによって、人の日常の行動に関する情報が追跡されるようになる。家で何をしているのか、交通機関を使ってどこに行こうとしているのか、健康状態や娯楽などを瞬時に分析し入手することができる。また、IoT による情報収集は、見えないところで個人がコントロールできない形で広がってしまう。 ● IoT のセキュリティは大きな課題であり、相互接続される性質上、脆弱性の影響は大きくなる。 ● IoT によって、どのようなサービスが他のサービスと繋がっていて、機能しているかが明確でなく、透明性が確保されていないことは消費者にとって大きな課題である。製品やサービスは、正確な情報を消費者へ提供することが常に課題となっている。IoT によって製品とサービスが複雑になれば、消費者が理解することは困難となる。IoT については専門的でない容易な用語で情報を開示することが重要である。 ● IoT により消費者はデジタル著作権の問題に直面する。複数のデバイスでデジタル音楽を使用することができるのか、購入した電子書籍を転売できるのか。また、消費者の個人情報(例えば、電力消費量、フィットネス履歴など)をプロバイダー間で転用することは消費者が申し出れば防ぐことはできるが、転用が拒否された場合に、そもそも IoT 業界はサービスを提供するのだろうか。 ● 誰もが製品やサービスが永遠に続くとは思っていないが、IoT デバイスの性質を考えると、長年使用したコンポーネントがいまだにサポートされているのか、それとも単に機能停止しているのかなど、IoT サービスの継続性が消費者へ影響を及ぼすことになる。 ● 消費者が IoT に参加しないことを選択できるかどうかも重要な課題となる。
IBM	● IoT の課題で、既存の IT 環境と同様に課題であるものは、以下のものである。 ➢ システムの相互運用性 ➢ セキュリティ ➢ プライバシー ➢ 法的責任 ● IoT で現在とは異なる課題は、セキュリティである。IoT の進展によってセキュリティの問題はこれまでよりも明らかに増大する。新たに想定される課題は、 ➢ より多くの機器が攻撃対象となる ➢ 機器は様々な特徴をもっており複雑化する ➢ より多くのデータと新しい種類のデータが生じる ➢ 機器は直接接続されており、物理的な環境を変更することが可能となる
ARM	● IoT の課題は、以下に挙げることができる。 ➢ エネルギー効率 IoT 機器に搭載されるセンサーなどの部品には長いバッテリー寿命又は環境からエネルギーを取得する技術が必要となる。これらを解決するためには、新しいバッテリー技術が必要となる。

	➢ 制約された環境におけるコンピュータパワー IoT センサーは非常に小さい。IoT には単純な処理を行うものや、洗練された端末データ処理を行うものもある。また適切なセキュリティを確保するためにソフトウェアのアップデートを行うことができる処理能力も必要になる。 ➢ セキュリティ セキュリティは最大の課題となることは確実である。 ➢ 通信 IoT は適切なローカルエリアネットワークと広範なエリアでの通信能力が必要となる。

② IoT の定義についての質問(No.2) 「“もののインターネット(IoT)”という言葉は、複数の組織で定義されており、例えば米国政府であれば NIST や FTC において、政策の説明やアーキテクチャーのリファレンスの中で定義されている。我々が IoT ﾗﾝﾄﾞｽｹｰﾌﾟ(IoT の展望)を調査する際に、どの定義を使用すれば良いと思うか？」	
Booz-Allen-Hamilton	● 連邦政府が IoT へ取り組むには、まず IoT の定義を考慮すべきである。様々な関係者がいろいろな定義を提案している。サイバーフィジカルシステム、物理的なインターネット、ユビキタスコンピューティング、環境インテリジェンス、広がるインターネット、物の WEB 化、ワイヤレスセンサーネットワーク、物理的コンピューティング、M2M、インダストリアルインターネット、などの IoT に関連する様々な言葉を反映したものになると予想される。 ● 適切な IoT の定義は、エコシステム全体を考慮したものになるべきである。ブーズアレンハミルトンとしては、IoT はデジタル世界と物理世界を融合するデバイス、センサーその他の機器が相互接続されたエコシステムと定義する。 ● IoT は、サイバーフィジカルソリューションにおいて安全性、セキュリティ、運用の効率性を高める機会をもたらす。
Consumer Technology Association（全米民生技術協会）	● CTA としては、企業、商用、産業用とは別に、消費者向けの IoT(消費者 IoT)という定義を考慮することを提案する。政策立案者にとって特に重要になることは、産業用と消費者向けの IoT の違いを理解して、IoT の進展が規制によって制限されないようにすることである。

③ IoT セキュリティについての質問(No.16,25) 「IoT のサイバーセキュリティの懸念事項に対して、政府はどのように取り組めばよいか？IoT によってどのようなサイバーセキュリティ上の懸念事項が生じるか？他のサイバーセキュリティの懸念事項とどのように異なるか？」	
Booz-Allen-Hamilton	● メジャーな IoT リスクは、セキュリティとプライバシーである。従来のサイバーセキュリティは、ファイアウォールの内側と外側の 2 面を見ていればよかったが、IoT では新たな第 3 の局面が出てくる。従業員が身に着けているウェアラブル端末や駐車場に停めてあるコネクティッドカー等が新たなサイバーリスクをもたらす。 ● IoT では新たなセキュリティモデルを作らなければならない。連邦政府が行う標準化は重要である。NIST がこれまでも行っている活動を継続し、IoT セキュリティに関しても調査研究や標準化、教育支援などガイドラインの策定をおこなっていくべきである。 ● 連邦政府は、IoT サイバーリスクを分類する際には、例えば次のカテゴリを考慮するとよい。 ➢ コンシューマデータシステム(データ漏えいリスク) ➢ パブリックインフラシステム(重要インフラ停止リスク) ➢ 民間産業システム(人命にかかわる事故、例えばプラント爆発、航空機墜落など) ➢ 軍事産業システム(戦術や諜報活動を脅かされるリスク)
IBM	● 政府は新しい規則を策定することに集中するのではなく、代わりにテクノロジーとセキュリィの両方ために、イノベーションを促す柔軟なモデルを醸成するべきである。政府はサイバーセキュリティ情報共有のためのコミュニティを支援し続け、適切なセキリティ研究機関と調整し、クリアなガイドランを策定するように民間と連携するべきである。政府は潜在的な攻撃を前にして、サイバーセキュリティの研究とイノベーションを育てるべきである。
Microsoft	● IoT のサイバーセキュリティに関する政策では、主要な IoT プレーヤーに役割を課し、それぞれの役割に適切なセキュリティ施策を決定すべきである。IoT の上位では、メーカ、インテグレータ、開発者、設置者、運用者に依存する。マイクロソフトの知見では、各人の役割は、以下のように説明できる。 ➢ IoT ハードウェアメーカー/インテグレータ ① IoT へは最小の要件、操作に必要な最小の機能だけを含むように設計する。 ② ハードウェアの改変を検出し、不正な改変がないことを保証する。 ③ 暗号化されたストレージと信頼あるブート機能で安全なハードウェアを作る。 ④ アップグレードを安全に実施できるよう、ファームウェア暗号化などを実施する。 ➢ IoT ソリューション提供者 ① セキュアな開発方法を利用する。 ② オープンソースソフトウェアを利用する際には細心の注意を払う。 ③ ソフトウェアのライブラリや APIs(Application Programming Interfaces)を利用する際は最新の注意を払う。 ➢ IoT 導入者 ① ハードウェアをセキュアに(パラメータなどの設定を適切に)導入する。 ② 認証キーはセキュアに保管する。 ➢ IoT 運用者 ① システムを最新に保つ。 ② 悪意ある攻撃を防ぐ。 ③ 監査を頻繁に行う。 ④ 物理的な IoT インフラを保護する。 ⑤ クラウドコンピューティングを保護する。

④ IoT プライバシーについての質問(No.17,18,25) 「IoT に関するプライバシーの懸念事項へ政府はどのように取り組めばよいか？IoT によってどのようなプライバシーの懸念事項が生じるか？他のプライバシーの懸念事項とどのように異なるか？」	
Consumer Technology Association（全米民生技術協会）	● 時として、政府の行動は市場に不確実性を作り、技術革新を抑制し、最終的に消費者へ害を与えてしまう。法律や規制はしばしば、進化し続ける技術に追いついていけない。また政府が仮定するシナリオは、消費者の要望や市場がどこへ向かっているかを、ある一定時点における静的な観測に基づいている。一方、業界の自主規制は、より容易に市場の変化や技術の進化に対応することができる。また、業界の自主規制は社会規範に基づくトップダウンのルールである。IoT の達成には自主規制のルールが最も適しているかもしれない。さらに、IoT 業界では、既に積極的に IoT のプライバシーの課題に取り組んでいることを考慮すべきである。
Consumer Federation of America (全米消費者連合)	● これまでの米国政府のプライバシーへのアプローチは、分野別の個別法と自主規制で成り立っており、業界毎に巨大なギャップを残し、個人に対して効果的な保護を提供できていない。
Verizon	● NTIA は、連邦政府や他の政府機関とは別に、IoT に特化したプライバシー政策や法案を策定することを抑制すべきである。IoT 固有のプライバシー法や規則をパッチワークのように策定することは、IoT の発展を遅らせ、紛らわしい法体系となってしまう。もっと言えば、現行法を IoT 環境へ適用すればよく、新しい法律は不要である。
Microsoft	● IoT を促進させるためには、伝統的な、Notice(通知)と Consent(同意)によるプライバシーの保護から、透明性とユーザコントロールへ発展させるべきである。IoT システムでは、利用者が個人情報の利用に関して、同意を行うボタンがない。
IBM	● 政府は、情報の自由な流れを保証し、デジタル経済のグローバル化を認識すべきである。権利と情報の使用は、既存の法体系の下で、契約上の問題として取り扱われるべきであり、革新と競争を促し、市場が個人情報の適切な取り扱いを決定していくようにすべきである。政府は「プライバシーバイデザイン」を宣伝すべきである。

⑤ IoT の技術的季題についての質問(No.6,7) 「どのような、技術的問題が IoT の開発を阻害しているか？」	
Auto-alliance (自動車連盟)	● 相互運用性で最も重要なのは、車が他車メーカの車と通信できることであり、現在の車と何年も後に売り出される車が通信できることを保証しなくてはいけない。
Booz-Allen-Hamilton	● 技術的な課題としては、技術標準が整備されていないこと。例えば、エッジコミュニケーションプロトコルや非構造化データストレージなどがある。 ● 新しいバッテリー技術や既存のレガシーシステムとの統合も課題である。
Verizon	● NTIA は、連邦政府や他の政府機関とは別に、IoT に特化したプライバシー政策や法案を策定することを抑制すべきである。IoT 固有のプライバシー法や規則をパッチワークのように策定することは、IoT の発展を遅らせ、紛らわしい法体系となってしまう。もっと言えば、現行法を IoT 環境へ適用すればよく、新しい法律は不要である。
Consumer Technology Association (全米民生技術協会)	● 相互運用性と確かなレベルの標準化が IoT エコシステムの成功には不可欠である。政府は、Industry Internet Consortium や Open Connectivity Foundation などが技術的なベストプラクティスや標準を開発し、オープンな参加で国際標準を策定できるよう、後押しすべきである。政府は、商用の利用可能なソリューションを活用すべきである。**連邦政府は、IoT が広まっていく際に唯一国全体を把握できる立場であることを認識**し、**透明性を持って情報を共有し、産業界が IoT 全体の広がりを理解できるようにすることが IoT の発展に寄与**できる。NTIA は、IoT の様々な利用形態を考慮し、ニュートラルなアプローチで IoT の政策を作るべきである。
Verizon	● 有線・無線のネットワークの双方が、IoT 通信のバックボーンとなる。IoT の発展には、ネットワークが消費者や企業の要求に応えられる強固で利用可能なものでなければならない。IoT ソリューションの成長はワイヤレスネットワークの負荷を指数関数的に増加させている。

⑥ IoT における政府の役割についての質問(No.3,15,20,21,26,27) 「IoT によって影響を受ける主要な政策課題は何か？政府はその課題に対してどのように対応すべきか？連邦政府と共に商務省は、IoT の課題と機会を支援する場面において、どのような役割を演じればよいか？」	
Auto-alliance (自動車連盟)	● 現在および将来の IoT 政策は結果として、自動車業界や他の業界にとって、サイバーセキュリティ、データプライバシー、V2V 及び V2I[8]の利用を適切に保護し、また連邦および州の法律や規制と競合、矛盾せず、重荷とならないようなものにしてほしい。
Consumer Technology Association (全米民生技術協会)	● 政府は技術革新を促進するために、既定の法令ではなく市場に根ざした政策を検討すべきである。政府の規制は、公共の利益がある場合に適用されるべきである。 ● 政策立案者は、消費者や企業が生活の中で技術をどのように採用しようとするかを安易に推測すべきではない。政策立案者は、仮説を立てた場合には、実証分析を行い、費用対効果を総合的に考慮して検証すべきである。 ● IoT の主要な政策の目的は、イノベーションを促進することである。
Consumer Federation of America (全米消費者連合)	● これまでの米国政府のプライバシーへのアプローチは、分野別の個別法と自主規制で成り立っており、業界毎に巨大なギャップを残し、個人に対して効果的な保護を提供できていない。
Verizon	● 政策立案者は、IoT ソリューションを制御するために広範な新しい規則を採用するのを避けるべきである。既にいくつかの IoT フレームワークは存在している。これらのフレームワークをスタートポイントとして、IoT 政策を考慮すべきであり、新たな IoT 制度を導入するべきではない。 ● 米国はプライバシーとセキュリティなどの大きな問題についての方針を策定する際は、全ての IoT ソリューションを横断的に、産業界毎ではなく、全体的なアプローチを取るべきである。 ● 特定の産業固有の IoT 政策があるかもしれないが、全体的な IoT 政策へ支障となるような制度設計は避けるべきである。 ● 政策立案者は、消費者向けと産業向けの IoT の重要な違いを認める必要がある。産業向けの IoT では個人情報を扱わないため、消費者保護法を適用することは誤りである。IoT 創世記には、「害を与えない」アプローチを採用するべきである。次期尚早の規制を避けるべきである。規制という手段をとるよりも、関係者との合意形成からベストプラクティスや原則を引き出すような介入を行うべきである。
CISCO	● 政府機関および政策立案者は、 ➢ サイバーセキュリティリスクの管理のために民間企業と協力することができる。 ➢ IoT の相互運用性を促進するために、ステークホルダーと協力することができる。 ➢ IoT の利用可能性を促進するために周波数帯域の適切な政策を設計することができる。 ➢ IoT に関連した教育政策を推進することができる。
Microsoft	● 政府には以下の事項を期待する。 ➢ IoT サイバーセキュリティフレームワークのベストプラクティスを策定すること。 ➢ 伝統的な「通知と同意」ベースのフレームワークを、透明性、文脈に応じた、消費者の期待に焦点を当てたフレームワークへ近代化すること。 ➢ IoT 業界が自発的に、オープンでコンセンサスベースの開発を支援すること、また技術革新を促進し、相互運用性を確保するための世界的な規格化を支援すること、レガシーシステムと IoT システムが共存可能にすること。 ➢ 国際貿易公約と同様に、IoT についても他国の戦略や取組において国際的な連携を行うこと。 ➢ 政府機関をまたぐ IoT タスクフォースを立ち上げること。少なくとも、DOC、DOD、DHS、DOT、FCC、米国通商代表を含めたタスクフォースにすること。タスクフォースでは、以下を検討すること。 ① 連邦政府の戦略的な政策文書に、IoT デバイスによってセキュリティリスクが増大している側面を記述するように指示すること。

[8] *vehicle-to-vehicle and vehicle-to-infrastructure*

	② IoT による便益とリスク双方に関する気づきと教育プログラムを実施すること。 ③ IoT に関連したセキュリティの課題、IT と OT の融合、将来の IT と OT の専門家の育成、について学界と共に推進すること。 ④ 標準化と政策策定のために適切な国際フォーラムと連携を促進すること。 ⑤ サイバーセキュリティの意義とリスクを管理するために IoT 展開ガイドランを策定し、アップデートし、維持するために、様々な産業界の IoT コンソーシアムを開催し、支援すること。
IEEE	● ステークホルダコーディネーション 連邦政府は産業界、学界、専門家及び一般大衆間のコミュニケーションを良くする有益な役割を果たすことができる。IoT においては、技術格差を識別し評価し、セキュリティ、プライバシー、市民の自由を確保するために、技術が発展するために、すべてのステークホルダーを横断的にコーディネートする必要がある。 ● 標準化 **IoT の基礎は接続性**にある。IoT 機器は、異なるメーカが作成した IoT 機器と繋がらなければならない。またその繋がりは、シームレスに、ユーザフレンドリーに、セキュアでなければならない。連邦政府は、標準開発組織と連携して、標準化の開発を促進し、開発プロセスを支援し、関連するステークホルダーのコーディネートを行うこと。 ● セキュリティ・プライバシー IoT を利用するユーザのプライバシーの問題はエンジニアリングの問題ではなく、政策の課題である。IoT でセキュリティやプライバシーをどのように確保すればよいかは公的なフォーラムで議論されるべきである。一般大衆は IoT を信頼しなければ、IoT を使わない。政府は、セキュリティ、プライバシー、安全上に関して透明性の高いプロセスを通じて規則を策定することで、人々が IoT システムを信頼するようになる。 ● 国際関係 IoT は可能な限りグローバルなネットワークであるべき。政府機関は、米国を代表し、ITU や WIPO の組織で重要な役割を担っている。