資料５－２

安全なIoTシステムの創出に向けた意見交換会　とりまとめ

平　成　３　０　年　３　月　１　２　日
内閣官房 内閣サイバーセキュリティセンター

平成27年9月のサイバーセキュリティ戦略決定を受け、サイバーセキュリティ戦略本部研究開発戦略専門調査会による審議（平成28年3月、6月、10月）を経て、安全なIoT（Internet of Things, いわゆるモノのインターネット）システムの具体化に向けた検討が開始された。

官民連携の検討体制の検討を経て、平成29年3月から4回にわたって有識者、内閣サイバーセキュリティセンター（以下「NISC」という。）、関係省庁が協働し、多様な主体の連携を必要とするIoTシステムのサイバーセキュリティの在り方について、種々、検討を行ってきたところである。

現行サイバーセキュリティ戦略の終期に当たるため、これまでの検討結果を取りまとめるとともに、これまでの知見を踏まえ、新たな取組方針を導き出すものとする。

1.　現行戦略の要求事項

平成27年9月に閣議決定された「サイバーセキュリティ戦略」において、安全なIoTシステムに関する記載の概要を以下に示す。

> IoTシステムにおける高いレベルでのセキュリティ品質を確保するため、産学官が一体となって先んじて投資を行うことは、多くのIoTシステムの利活用が見込まれる2020年の東京オリンピック・パラリンピック競技大会の成功はもとより、我が国企業によるIoTシステムを活用した新たなビジネス・新規雇用等の創出のため必要不可欠。

1.1. 安全な IoT システムを活用した新規事業の振興

- IoTシステムに係る新たな事業を成功させるためには、競争力の源泉となる高いレベルでのセキュリティ品質の実現が不可欠。連携される既存システムを含めて、IoTシステム全体の企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン(Security By Design)の考え方を推進する。

1.2. IoT システムのセキュリティに係る体系及び体制の整備

- IoTシステムに係る大規模な事業について、業態横断的に産学官の主体が適切に連携

することで、ビジネスイノベーションを巻き起こしていく。関係主体間において相互信頼に基づく連携と各主体の自律的な取組による協働を実現するため、当該事業に求められるセキュリティ対策に係る基本理念、目標、方法、期限等について共通認識を醸成し、各関係主体の任務を明確化する。

- 経済社会への影響が大きいと考えられるものについては、サイバーセキュリティ戦略本部が、横断的な対策のために必要な企画・立案・総合調整を行い、関係府省庁や関係機関の間における有機的・一体的な連携を働きかけるなど、必要な取組が整合的かつ遺漏なく実施されるよう促していく。

2. 現行戦略を踏まえたこれまでの施策の展開

サイバーセキュリティ戦略策定直後、総務省、経済産業省、IoTコンソーシアムが協働し、平成28年7月にIoTセキュリティガイドラインを策定した。

その際、NISCは同ガイドの策定に協力しつつ、サイバーセキュリティ戦略を踏まえた今後の検討事項を明記した「安全なIoTシステムのセキュリティに関する一般的枠組」を平成28年8月に策定し、国内外に発信した。

2.1. NISC の取組

NISCは、「安全なIoTシステムのセキュリティに関する一般的枠組」を基に官民の自律的な連携体制の整備を具体化すべく、体制の検討を民間とともに行った。多様な主体の連携は、異なった価値観、異なった慣習、文化等を背景とした主体の連携を意図する。こうした取組はサイバーセキュリティの分野では、初めての試みであり、試行錯誤を伴うものであった。結果として、NISCが主導する形で平成28年3月に「安全なIoTシステムの創出に向けた意見交換会」を開始し、現在に至っている。

第1回目では、インターネット空間をどう捉えるかといった根本的な課題の提起に始まり、検討に参加している者のインターネットの捉え方が多種多様であることが明らかになった。また、家電製品のセキュリティの国際電気標準会議(IEC)での検討状況、NIST CPS Framework を利用したリスク対策モデル、サイバー分野と保安管理分野の違い等が検討された。

第2回検討会では、IoTの阻害要因、国際標準の現状、具体化に向けた課題と方向性の検討が行われた。

第3回検討会では、IoTセキュリティに関する国際標準化動向、各産業分野におけるIoTセキュリティに関する先進的な取組事例の紹介、各省庁におけるIoTセキュリティに関する政策の紹介が行われた。

これと並行して、米国NISTとの協力関係を構築し、IPAや関係者の協力の下「「安全なIoTシステムのセキュリティに関する一般的枠組」を国際標準化すべく検討を行い、ISO/IEC JTC1 SC41において、日本提案によるNWIP(New Work Item Proposal)が投票される見込みとなった。

2.2. 各府省の取組

現行戦略策定から2年半経過した現時点において、NISC及び各府省では、様々な施策の進展がみられている。

2.3. IoT を取り巻く状況の変化

現行サイバーセキュリティ戦略策定以降、国内においては、「IoTセキュリティガイドライン」、「安全なIoTシステムのセキュリティに関する一般的枠組」、海外においては、NISC CPS Framework, IIoT、Industry 4.0等、IoTに関係する取組が世界規模で急速に広がりを見せてきている。

こうした状況から、現行サイバーセキュリティ戦略が決定された平成27年9月当時と現時点との約2年半の間、加速的に関係各層の問題認識の高まりとともに、具体的取組が前進してきているところ。関係者間での具体的な議論が効果的に行うことが出来る環境が醸成される状況となってきている。

3. 課題の整理と今後の方向性

多様な主体が相互に理解し、主体間の新たな連携を目指す立場をとるNISCの取組は相応の時間を必要とするものである。他方、日進月歩するICT環境に適時的確に対応する立場である担当府省庁は、スピード感をもってIoTを取り巻く諸課題に取組む必要がある。こうしたことから、NISCと担当府省庁との施策の展開のスピード感には必然的な開きが生じ、政府内での調整が後手に回ってしまったことは否めない。また、官民の調整については、体系的なコミュニケーションの場を一層有効に活用していく必要がある。

さらに、Society5.0の実現が具体的に視野に入ってきたことから、サイバー分野とフィジカル分野の一体化の必然性についての関係者の理解が深まってきたところ。こうした状況を踏まえ、我が国一体となって安全なIoTシステムを一層効果的に発展させていくため、現行サイバーセキュリティ戦略に示された方針に基づき、サイバーセキュリティ戦略本部による横断的な対策のために必要な企画・立案・総合調整を一層充実させ、関係府省庁や関係機関の間における有機的・一体的な連携を働きかけるとともに、関係する多様な主体の相互信頼に基づく体系的な体制の整備、各関係主体の任務の明確化等を促進していくことが求められる。

3.1. 基本的考え方

3.1.1 共通認識の下での関係主体の協働

Society5.0の実現に向けて、これまで慣習やビジネスモデルの異なる様々な分野のIoTシステムに関わる主体が連携して価値を生み出すことが期待されている。その際、各分野・各主体の多様性を尊重し、自律的な取組を推進しつつも、一定の整合性、一貫性を持って安全・安心なIoTシステムを実現していくための体系の構築が必要となる。

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」に示される検討項目を踏まえ、関係主体間でセキュリティ対策に係る基本理念、目標、方法、期限等についての共通認識の醸成と、各分野・各主体の役割(機能)の明確化を図った上で、自律的にサイバーセキュリティに関わる取組を進めつつ、関係者が協働した取組を推進するものとする。このため、協働を促進する仕組みを具体化する。

3.1.2 グローバルな視野を持った取組

安全なIoTシステムの創造によって国際貢献を通じたリードができるよう、グローバルな視野を持ってIoTシステムに関するサイバーセキュリティの取組を推進する。特に、国際標準化活動を積極的に推進するとともに、国内外における関連する既存の規格等を意識した取組を行う。

3.1.3 発展期に向けた取組

この2年半でIoTに関する種々の検討が様々な分野で行われてきたところ。これまでリーダー的な主体が中心となって活動してきたところであるが、今後は、ユーザとなるべき主体の参画(府省庁、業界、学術団体等)を一層広く求めていき、安全なIoTセキュリティシステムの実現の加速化を図る。

3.1.4 機能保証(任務保証)～着実なサービスの提供～を基本とした取組

IoTシステムがそれに関わる利益とコストのバランスを含め、適切にその機能を全うすること(機能保証)を基本とし、そのサイバーセキュリティは、IoTシステムの機能を全うするために検討が必要な項目の一つとして位置付けるものとする。

3.2. 重点的に取り組むべき領域

3.2.1 関係者間における共通認識の一層の醸成及び役割の明確化

多様な主体が体系的に安全なIoTシステムを効率的に推進していくためには、関係主体間でセキュリティ対策に係る基本理念、目標、方法、期限等についての共通認識を醸

成した上で、競争領域を除き、官民を含む関係主体間での相互信頼に基づく情報共有によって、できるだけ競合を排除し、相互に力を合わせることを基本として、各主体の取組をマッピングし、情報共有を行うことなど検討する。

その際、関係者が多数存在することも考慮し、定期的な会合に加え、ITを活用し、リアルタイムでどのような取組が、いつ、どこで行われるかを共有できる仕組みを構築することも検討する。

3.2.2 検討すべき課題の関係者間での共有

IoTシステムにおいて具体的に検討すべき課題(応用分野、基礎検討分野等)が時々刻々と変化していくことを踏まえ、関係者間で課題のマッピングを行い、その課題に関係する主体間で、方針、期限、役割分担を決定する。

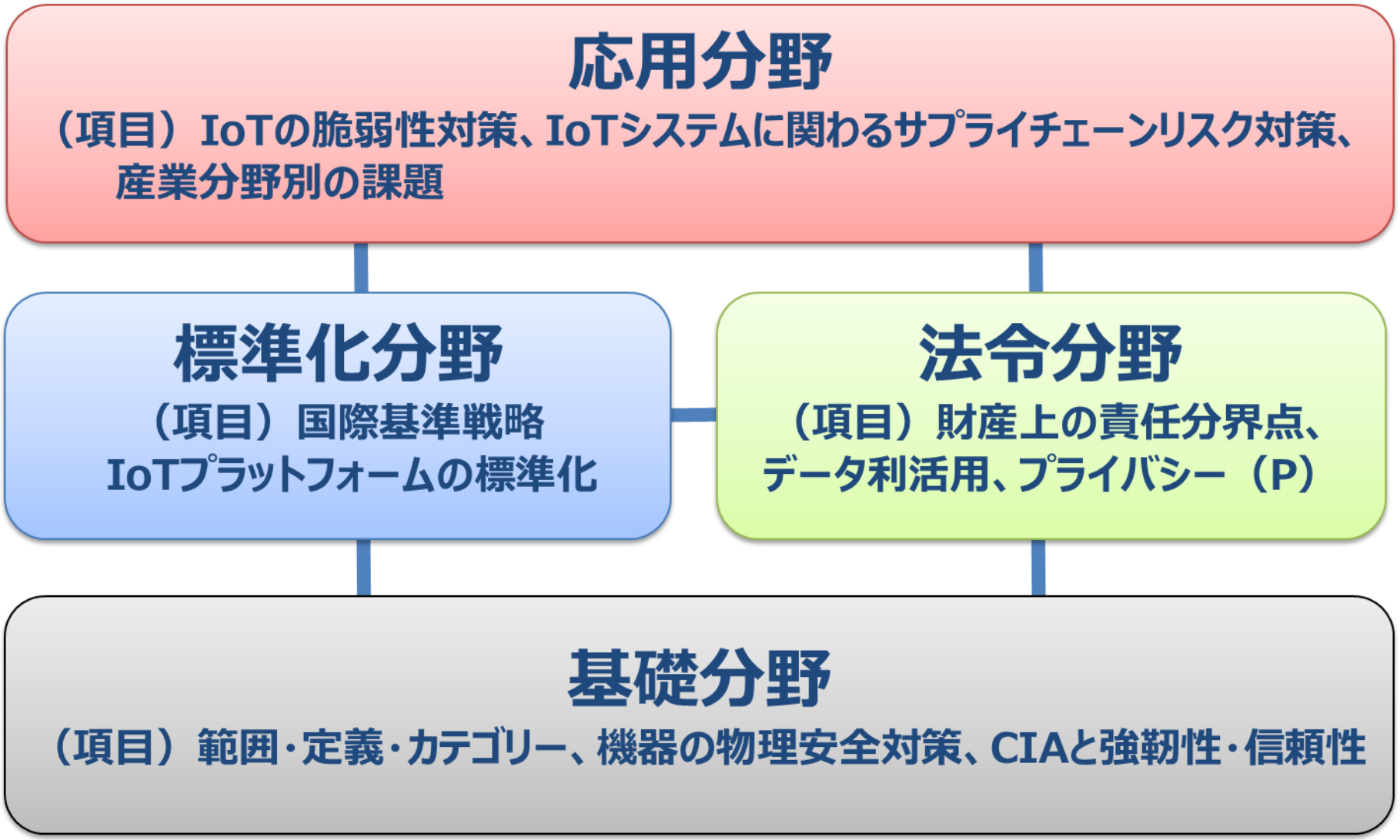
現時点で考えられる課題(分野)の例(※要検討)

- 応用分野（喫緊の対策が必要な分野）
  - IoTの脆弱性対策（ボット対策等）
  - IoTシステムに関わるサプライチェーンリスク対策

- 標準化分野
  - 国際基準戦略(国際標準・海外標準の活用)
  - IoTプラットフォームの標準化

- IoTセキュリティ基礎分野
  - IoTの範囲、定義、カテゴリー
  - IoT機器の物理安全対策
  - IoT機器の機密性、完全性、可用性、強靭性、信頼性等の検討

- 法令検討分野
  - 財産上の責任分界点の検討
  - データ利活用の検討
  - プライバシー(P)


応用分野
（項目）IoTの脆弱性対策、IoTシステムに関わるサプライチェーンリスク対策、
産業分野別の課題
標準化分野
（項目）国際基準戦略
IoTプラットフォームの標準化
法令分野
（項目）財産上の責任分界点、
データ利活用、プライバシー（P）
基礎分野
（項目）範囲・定義・カテゴリー、機器の物理安全対策、CIAと強靭性・信頼性

4. 今後の取組

NISCは、IoTシステムのサイバーセキュリティに関し、行政各部の施策の統一保持上必要な企画及び立案並びに総合調整を行う立場として、各府省及び民間の役割と取組の明確化を図りつつ、体系的な体制の整備を行い、我が国一体となって推進の加速化を行うものとする。

このため、競争領域を除き、安全や相互運用の円滑化、開発期間の効率化の観点からは、官民を含む関係主体間での相互信頼に基づく情報共有によって、できるだけ重複を排除し、相互に助け合うことを基本として、各主体の取組をマッピングし、情報共有を行うなどの検討を行うことを検討する。その際、民間との連携についての加速化の検討を行うものとする。

このため、ボット対策、サプライチェーンリスク対策などを含めたIoTシステムのサイバーセキュリティ対策の検討を行っていくものとする。