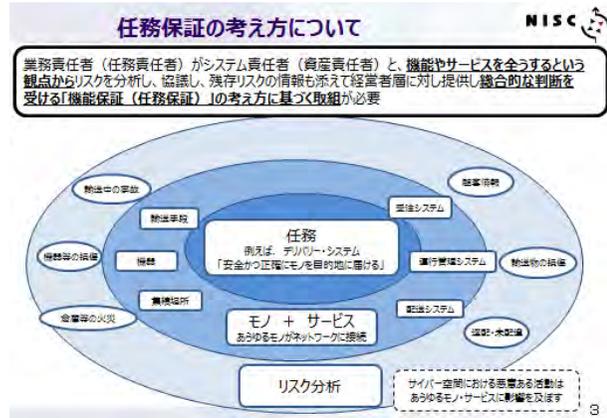


- ICT技術を最大限に活用して超スマート社会の実現を目指すためには、新しく創出される価値が安全・安心に社会実装されるための信頼（インターオペラビリティ、IoTセキュリティ、運用監視、トラスト等）の確保が必要である。プラットフォームにて実現すべき信頼の基盤を構築し、データの利活用を推進していく方向性について議論した。
- 製品やサービスを提供する際には、「**任務保証**」の考え方に基づき取り組むことが重要であり、「**セキュリティ品質**」の実現が欠かせない。セキュリティ品質を確保するための費用はコストでなく価値を生み出すための投資である。その実現には、企画・設計段階からセキュリティ確保を盛り込む「**セキュリティ・バイ・デザイン**」の考え方をもち、開発時や運用時には個々のIoTシステムの階層構造を踏まえた「**データとIoTシステム全体のセキュリティ確保**」を図ること、また、異なる分野を連携協調させる際には「**IoTシステム間の相互連携**」を図り、IoTシステム全体としてのセキュリティを確保することが重要である。さらに、日々進化し高度化するサイバー攻撃に対応するためにはセキュリティ確保のための「**人材育成**」も必要な取組である。
- データ提供者が安心してデータを供出することが新たな価値創出の起点であり、そのためには、プライバシー保護に配慮された制度にもとづいて運用され、安心してデータを供出できることをデータ提供者が認知することが重要であり、改正された「**個人情報保護法**」の利用推進を図るべきである。

## 〔任務保証とセキュリティ品質の観点〕

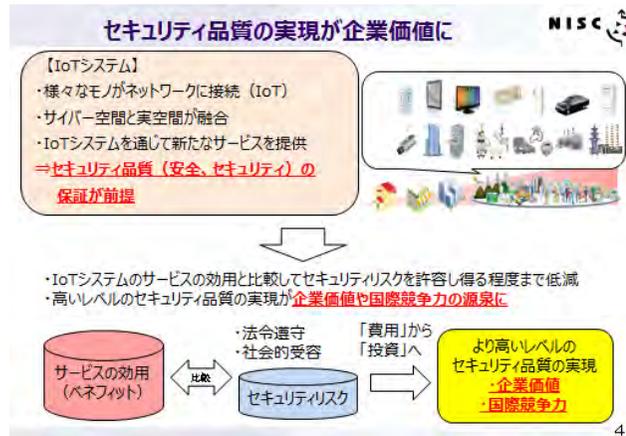
- 機能やサービスを全うするという観点から、リスク分析に基づき経営者層から総合的な判断を受ける、**任務保証**の考え方に基づく取組が必要である。



任務保証の考え方（左図）：  
 デリバリー・システムを例とすると、この場合の任務は「安全かつ正確にモノを目的地に届ける」こと。この任務を達成するには、輸送手段、配送システム、集積場所などの設備・資産、即ち「モノとサービス」を利用・提供することになるが、これらに何らかの不確かな障害などが生じた時に、任務を達成できないというリスクが存在する。特にあらゆるモノがネットワークに接続される社会では、サイバー、すなわちネットワーク越しの悪意ある活動も、モノ・サービスに悪影響を与え、任務を全うできないことが生じる可能性がある。

※第四回NISCプレゼン資料より抜粋

- サイバーセキュリティを考えるにあたっては、パーツや情報システム単体で考えるのではなく、**事業つまり、経営者層が達成すべき任務全体に照らして判断することが必要**である。
- **セキュリティ品質の実現は企業価値や国際競争力の源泉になる**という考え方が重要である。

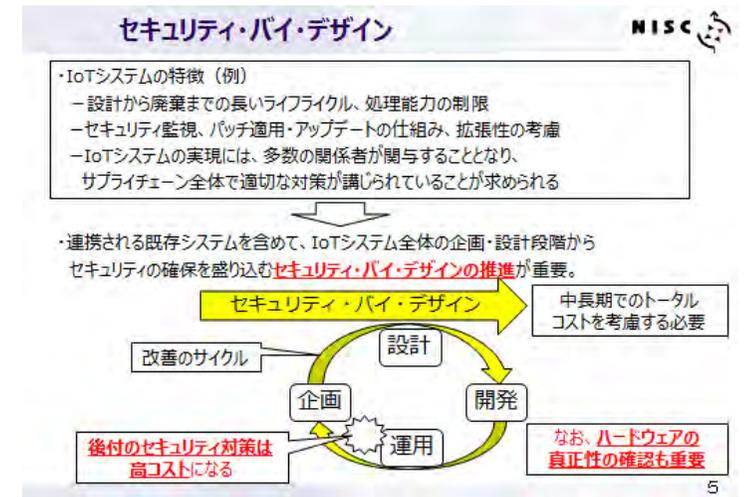


※第四回NISCプレゼン資料より抜粋

- 企業が、IoTシステムを通じて新たなサービスを提供するに当たっては、市場における個人・企業が当該サービスに期待する品質の要素としての安全やセキュリティ、すなわち「**セキュリティ品質**」が保証されていることが前提である。
- 日本の国際競争力の源泉のひとつに品質や安全があるが、IoTシステムにおいてもその**日本ブランドは、維持されなければならない**。サービスの効用を活かすためにはセキュリティの確保が必要であり、**ビジネスにネガティブなものではなく、むしろ高いレベルでのセキュリティ品質の実現は、企業価値や国際競争力の源泉**となり得る。

## 〔セキュリティ・バイ・デザインの観点〕

- 連携される既存IoT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確保を盛り込む、**セキュリティ・バイ・デザイン**の推進が重要である。
- セキュリティ・バイ・デザインの推進を図ることが重要である一方、IoT機器側のセーフティ確保の観点も同様に重要であることから、IoTシステム全体を俯瞰してセキュリティ・バイ・デザインとセーフティ・バイ・デザインとの両立を目指した、**セキュリティ&セーフティ・バイ・デザイン**の推進が重要である。



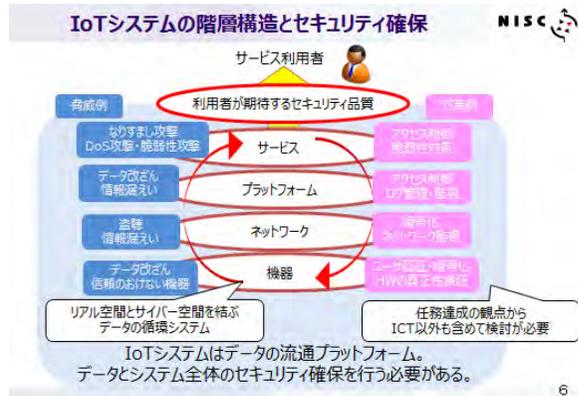
※第四回NISCプレゼン資料より抜粋

- IoTシステムの特徴を踏まえて、セキュリティを担保する技術開発を進める必要がある。
  - Society5.0実現に向け、**既存IoTシステムと新規IoTシステムの混在を想定したセキュリティ技術**が重要である。
  - IoT製品が国内だけでなく海外へ移動するためサプライチェーン全体で適切なセキュリティ対策を講じる必要があるだけでなく、国際的な協力体制、国際的なセキュリティの標準化の動きにも対応すべきである。
  - IoT製品は比較的製品の**ライフサイクルが長い**ものもあり、その特徴を踏まえたセキュリティの考え方（例：脆弱性対処や暗号化強度）が重要である。
  - IoT製品は**不特定多数の者に製品が渡る**ことを配慮した上でのセキュリティの考え方（例：管理できなかったり、利用者により分解して脆弱性を探される）が重要ではないか。
  - **ハードウェアの真正性を担保**するための施策（ハードウェアトロロジアン検知等）が重要である。

# セキュリティ／データ利活用のための個人情報保護

## 〔データとIoTシステム全体のセキュリティ確保の観点〕

- データの流通プラットフォームとしてのIoTシステムの階層構造を踏まえた、データとIoTシステム全体のセキュリティ確保の観点も重要である。



【参考情報③】内閣府 戦略的イノベーション創造プログラム (SIP) NISC

SIP新課題：重要インフラ等におけるサイバーセキュリティの確保  
H27～2015年度～H31、2019年度、予定、H27年度予算 5億円

経緯

- H27年6月18日(第10回CSIT) 新課題候補「重要インフラ等におけるサイバーセキュリティの確保」の承認
- 8月6日 情報セキュリティ大学院大学・情報セキュリティ研究所の内閣府政策参与への任命
- 9月16日～10月5日 研究開発計画パブリックコメントの実施
- 11月10日(第12回CSIT)持ち回り) 実施方針の決定
- H28年1月22日 委託先決定

達成目標

- 重要インフラ等のサイバーセキュリティの確保、意思のある動作を「地理的に異なる」システムの実現
- 重要インフラ等のサイバーセキュリティの確保、意思のある動作を「地理的に異なる」システムの実現
- 重要インフラ等のサイバーセキュリティの確保、意思のある動作を「地理的に異なる」システムの実現

研究開発推進施策

- サイバーセキュリティの確保、意思のある動作を「地理的に異なる」システムの実現
- サイバーセキュリティの確保、意思のある動作を「地理的に異なる」システムの実現

※サイバーセキュリティの確保、意思のある動作を「地理的に異なる」システムの実現

※第四回NISCプレゼン資料より抜粋

## 階層ごとのセキュリティ確保のイメージ SIP：「重要インフラ等におけるサイバーセキュリティの確保」

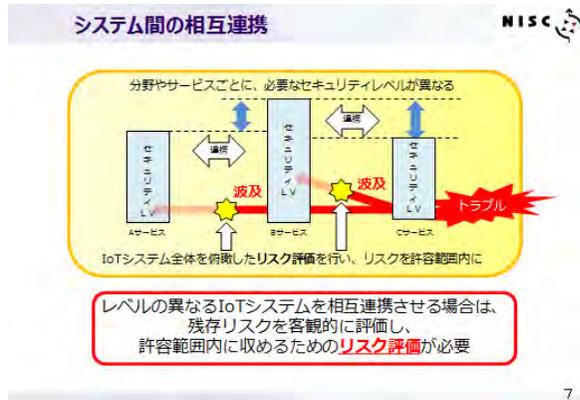
- ネットワークを構成する通信機器等が、仕様通りの構成であり改変されていないこと（完全性）が構築時・運用時に確認でき、また運用中に不正な機器にすり替えられていないこと（真正性）が確認できる戦略的イノベーション創造プログラム (SIP) の重要インフラ等におけるサイバーセキュリティの確保の研究開発成果を最大限活用すべきである。
- IoT時代に相応しい暗号技術等によるトラストの構築が必要である。
  - トラストを構築するために、従来の人や組織に対する認証だけでなく、今後増大することが予測されるIoTデバイスそのものを認証する、いわゆるモノに対する認証※も重要である。
  - トラスト構築のための技術検討を今後も進めていくべきであり、ブロックチェーン※を活用したセキュリティ等、中央集権的に取引（通信）を一括管理する必要がなく、IoTデバイスそれぞれがお互いを監視することで、セキュアな通信を低コストに実現する方式も今後の可能性として検討する必要がある。

※ブロックチェーン 金融審議会 決済業務等の高度化に関するワーキンググループ（第七回）配布資料より

ブロックチェーン（Blockchain）とは、取引履歴を暗号技術によって過去から1本の鎖のようにつなげ、ある取引について改竄を行うためには、それより新しい取引について全て改竄していく必要がある仕組みとすることで、正確な取引履歴を維持しようとする技術。現在、ビットコイン等の仮想通貨などに用いられているが、仮想通貨にとどまらず、様々な利用可能性があることが指摘されており、世界の主要銀行が共同してその利用可能性について研究を開始しているほか、米国ナスダック（National Association of Securities Dealers Automated Quotations：米国の株式市場）は未公開株式の取引にブロックチェーン技術を導入することを公表している。

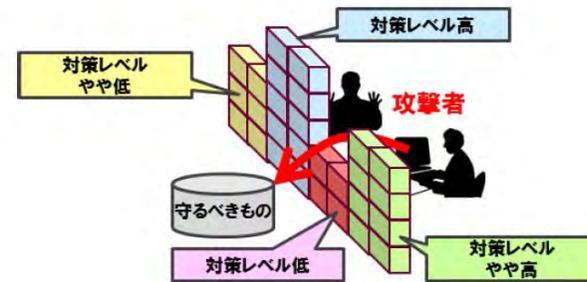
## 〔IoTシステム間相互連携の観点〕

- IoTシステム全体を俯瞰したリスク評価が必要である。安全安心対策のレベルが異なるIoTコンポーネントがつながることで、レベルが低いIoT機器が攻撃の入り口になる可能性があるため、IoT全体に波及するリスクを想定した評価をしていかなければならない。



### IoTシステム間相互連携によるリスク評価の重要性

※ 第四回NISCプレゼン資料より抜粋



### 弱い部分からリスクが発生するイメージ

※ つながる世界の開発指針(独立行政法人情報処理機構(IPA))  
<<http://www.ipa.go.jp/files/000048104.pdf>> (2015/04/04アクセス)

- 業種毎のSOC※および業種間を跨ぐSOCの整備が、インシデントからの早期復旧の観点で重要であり、I S A C※とも一体となった総合的なセキュリティ体制の整備も今後は検討していくべきである。

※SOC (セキュリティオペレーションセンター)

ネットワークやウェブサイトを常時監視し、不正な通信やマルウェアへの感染が疑われる場合には速やかに報告する仕組み。

※ I S A C (インフォメーションシェアリングアンドアナリシスセンター)

サイバーセキュリティに関する脅威を会員企業同士で情報共有し連携して対策に当たる枠組み。

# セキュリティ／データ利活用のための個人情報保護

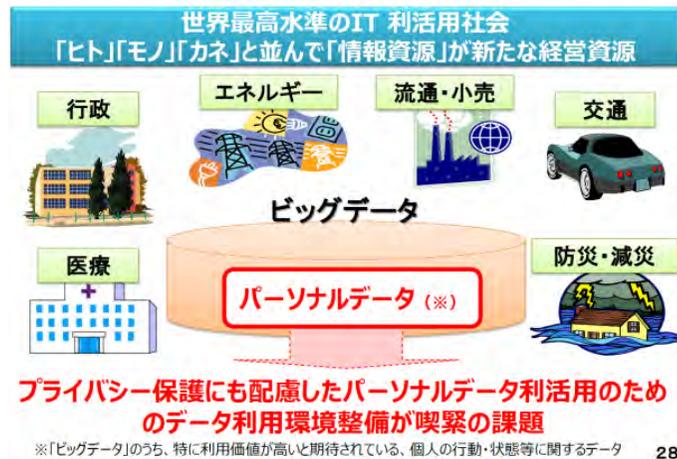
## 〔人材育成の観点〕

- サイバー攻撃の脅威が時代とともに高度化する中、セキュリティ対策も同様に高度化が必要であり、そのための**継続的な人材育成**が急務である。当面の対策としての**運用人材への教育を通じた即戦力の育成**と、将来にわたり安定したセキュリティシステムを構築できる**セキュリティ研究人材の育成**の両側面で検討していくべきではないか。

## 〔個人情報保護の観点〕

- 個人情報の保護を図りつつパーソナルデータの利活用の促進するため、改正個人情報保護法(平成27年9月3日成立)の**匿名加工情報**に関して整備された規定などの活用を進めるべきである。

6-1. 制度改正の背景及び課題



個人情報保護法の改正のポイント

1. 定義の明確化等	→	・個人情報の定義の明確化（身体的特徴等が該当） ・要配慮個人情報（いわゆる機微情報）に関する規定の整備 ・個人情報データベース等から権利利益を害するおそれが少ないものを除外 ・取り扱う個人情報が5,000人分以下の事業者に対しても法を適用
2. 適切な規律の下で個人情報等の有用性を確保	→	・利用目的の変更を可能とする規定の整備 ・匿名加工情報に関する加工方法や取扱い等の規定の整備 ・個人情報保護指針の作成や届出、公表等の規定の整備
3. 個人情報の流通の適正さを確保	→	・本人同意を得ない第三者提供(オプトアウト規定)の届出、公表等厳格化 ・トレーサビリティの確保（第三者提供に係る確認及び記録の作成義務） ・不正な利益を図る目的による個人情報データベース等提供罪の新設
4. 個人情報保護委員会の新設及びその権限	→	・個人情報保護委員会を新設し、現行の主務大臣の権限を一元化
5. 個人情報の取扱いのグローバル化	→	・国境を越えた適用と外国執行当局への情報提供に関する規定の整備 ・外国にある第三者への個人データの提供に関する規定の整備
6. 請求権	→	・本人の開示、訂正等、利用停止等の求めは請求権であることを明確化

※平成27年度個人情報保護法説明会 各回共通資料より抜粋  
([http://www.ppc.go.jp/files/pdf/personal\\_seminar27\\_caa\\_caa.pdf](http://www.ppc.go.jp/files/pdf/personal_seminar27_caa_caa.pdf))

- また一旦匿名化してしまうと、震災等により非匿名化データを利活用したくてもできないといった問題があるため、**データをどのように保管・運用すべきか**に関して、例えば準同型暗号を応用した秘密計算をビッグデータに適用する研究など、**様々な関連研究を支援していくべき**である。

# 新たなサービス創出に向けた推進

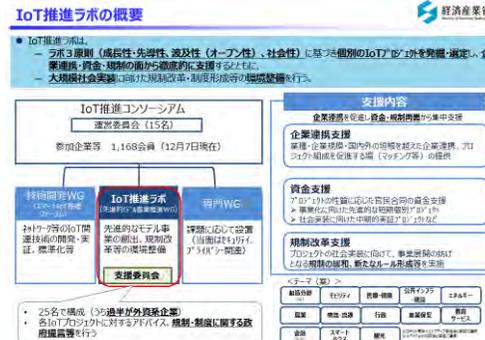
- 超スマート社会サービスプラットフォームでは、新たな価値創出のための取組を加速するための推進方策についても、プラットフォームの具備すべき機能と位置付けており、どのようなものが考えられるかを議論。
- 超スマート社会サービスプラットフォームを社会実装し、新たな価値を生み出すには「システム間連携協調の構築促進」を図ることが重要であり、その実装時期により適切な推進体制を構築する必要がある。例えば、価値が明確で実装時期が早期の場合には、民間企業主体で政府が支援する推進体制が現実的である。また取組については、S I P（戦略的創造イノベーションプログラム）等、政府内で早期社会実装に向け推進している施策を横断的に取り組むことや、早期社会実装可能な連携のユースケースを支援していくことも重要である。
- 一方、規制により超スマート社会サービスプラットフォームの社会実装が阻害されている場合には、「規制の見直し」を図り阻害要因を取り除くことが重要である。一方、将来にわたり持続的にシステム連携による価値創出を可能にするためにも、基礎研究も含めた「共通基盤技術群の検討」※は重要である。そして、常に「価値の受容性」を計測し、超スマート社会に向かっていることを確認していくことが重要である。

※ 「共通基盤技術群の検討」の観点とは、後述の共通基盤技術の議論により特定

# 新たなサービス創出に向けた推進

## 〔システム間連携協調の構築促進の観点〕

- システム連携の社会実装までの時間軸を考えて支援する仕組みを検討していくべきであり、**早期に社会実装可能なケースについては、民間企業の活動を支援していく制度や施策が重要**である。
- 中小企業やベンチャー企業が参画するには参入へのビジネスコスト低減化が必須であり、**先進的なモデル事業に対して政府関係機関やベンチャーキャピタルなどの支援機関と連携し、先進的IoTプロジェクトに対する資金支援や、事業化等に向けたメンターによる伴走支援、規制改革・標準化に関する支援を実施しIoTプラットフォームの発掘・育成を図るべき**である。



第二回システム基盤技術検討会 経済産業省プレゼン資料より抜粋



第一回システム基盤技術検討会 総務省プレゼン資料より抜粋

- 社会実装に向けた検証の場として**テストベットの取組が重要**である。またシステム間連携協調を想定したテストベットの場合には管轄官庁が複数関係することが想定されるため、**複数官庁の管轄する規制を同時に特区化して推進する体制を構築するべき**である。



- 競合企業も含め様々な企業が参画した検証のために、**大学の設備や機能を積極的に活用**するべきである。
- システム連携の社会実装は民間企業の支援だけでなく、政府が主導として進めている**S I Pのプロジェクト**についても**横断的な連携を推進**することが重要である。また、具体的なユースケースを設定し連携の社会実装を図る等、社会実装のための様々なアプローチにより超スマート社会の実現を図るべきである。

## 〔規制の見直しの観点〕

- 超スマート社会サービスプラットフォームの社会実装に向け、**実装の阻害要因となっている規制は緩和**すべきである。
- 社会実装の阻害要因となっている規制については、その時点で緩和が難しい場合でも時代の変化とともに見直しできる場合もあるため、**持続的に見直しを図る**ことが重要である。
- また、実装の前段階として様々な実証試験に関しても**オーナーがコミットメントできる体制**とし、単なる実証実験で終わりとするのではなく、次の検討に反映していくべきである。

## 〔受容性向上の観点〕

- 日本の国民がその価値を享受したかどうかを計測、評価することが重要である。
  - 社会実装の評価は、そのサービス主体である**プレーヤーや顧客ごとに設定して評価**していくことが重要である。
- データを提供する側を配慮したデータ収集に向け、提供者（個人、企業等）は、**どのようなデータを、どのような価値のためであれば提供を受容できるか**について、計測、評価することが重要である。