セキュリティ／データ利活用のための個人情報保護

- 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、また、「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」の考え方を持ち、開発時や運用時においては個々の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。

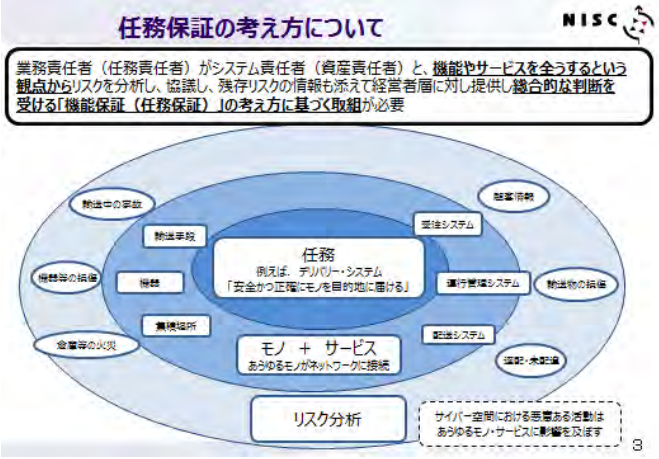
- データ提供者が安心してデータを供出することが新たな価値創出の起点であり、そのためには、プライバシー保護に配慮された制度にもとづいて運用され、安心してデータを供出できることをデータ提供者が認知することが重要であり、改正された「個人情報保護法」の利用推進を図るべきである。

※セキュリティ部分（スライド21～25）の順序に関しては、「サイバーセキュリティ戦略」（平成27年9月 閣議決定）を踏まえて記載

セキュリティ／データ利活用のための個人情報保護

〔任務保証とセキュリティ品質の観点〕

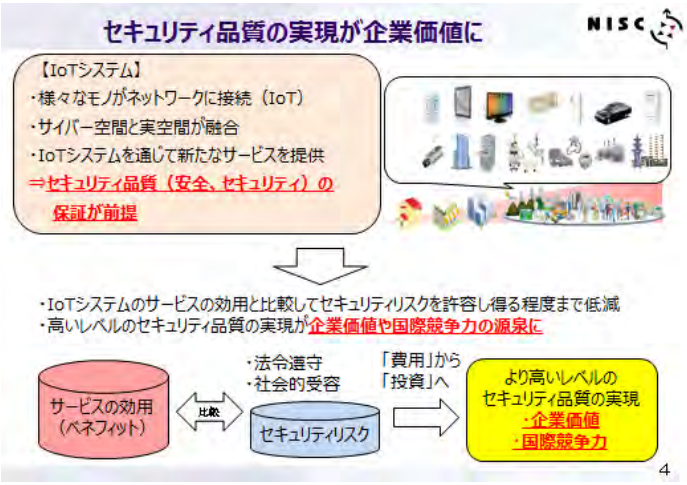
- 機能やサービスを全うするという観点から、リスク分析に基づき経営者層から総合的な判断を受ける、任務保証の考え方に基づく取組が必要である。



※第四回NISCプレゼン資料より抜粋

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。

- サイバーセキュリティを考えるにあたっても、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。



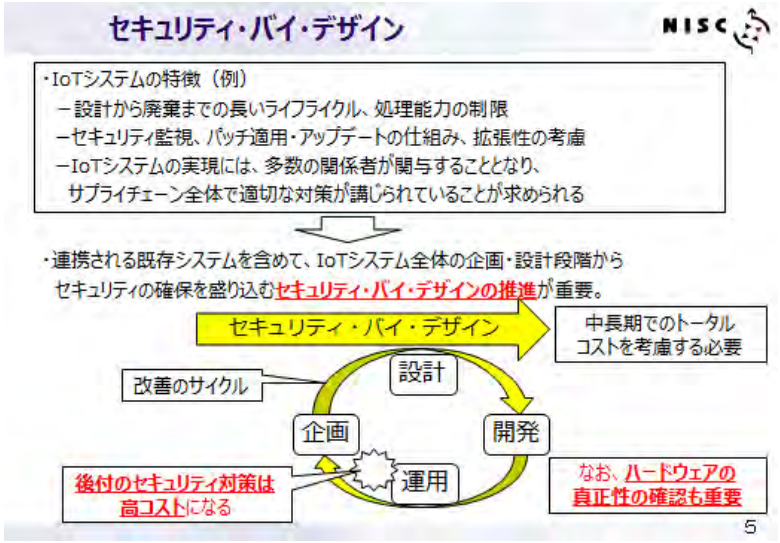
※第四回NISCプレゼン資料より抜粋

- 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／データ利活用のための個人情報保護

〔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。



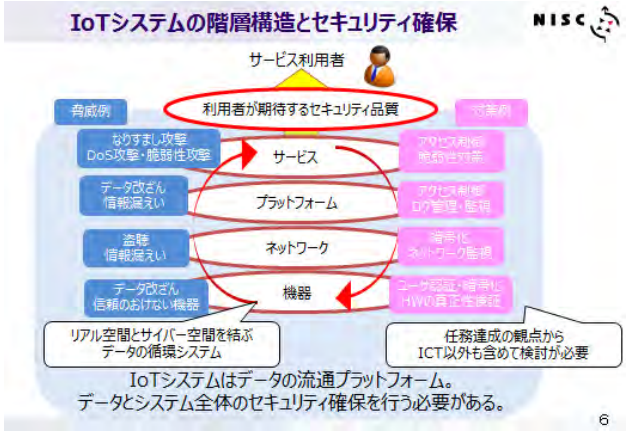
※第四回NISCプレゼン資料より抜粋

- 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（ハードウェアトロジャン検知等）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。



※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」

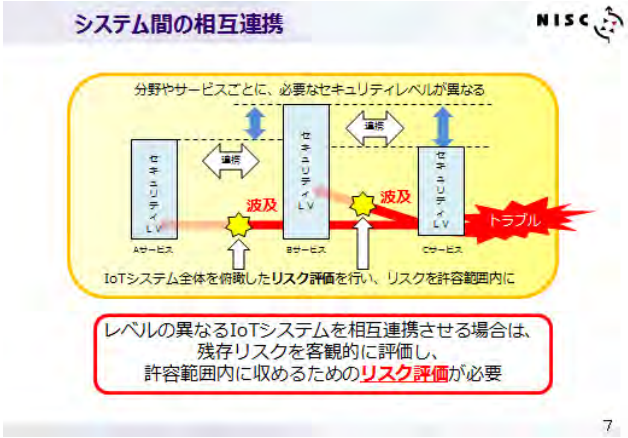
- ネットワークを構成する通信機器等が、仕様通りの構成であり改変されていないこと（完全性）が構築時・運用時に確認でき、また運用中に不正な機器にすり替えられていないこと（真正性）が確認できる戦略的イノベーション創造プログラム（SIP）の重要インフラ等におけるサイバーセキュリティの確保の研究開発成果を最大限活用すべきである。
- IoT時代に相応しい暗号技術等によるトラストの構築が必要である。
  - トラストを構築するために、従来の人や組織に対する認証だけでなく、今後増大することが予測されるIoTデバイスそのものを認証する、いわゆるモノに対する認証※も重要である。
  - トラスト構築のための技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。

セキュリティ／データ利活用のための個人情報保護

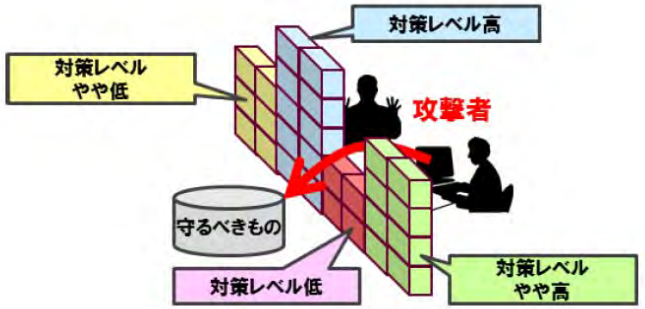
〔IoTシステム間相互連携の観点〕

- 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、ＩＳＡＣ※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。

※ＩＳＡＣ（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。

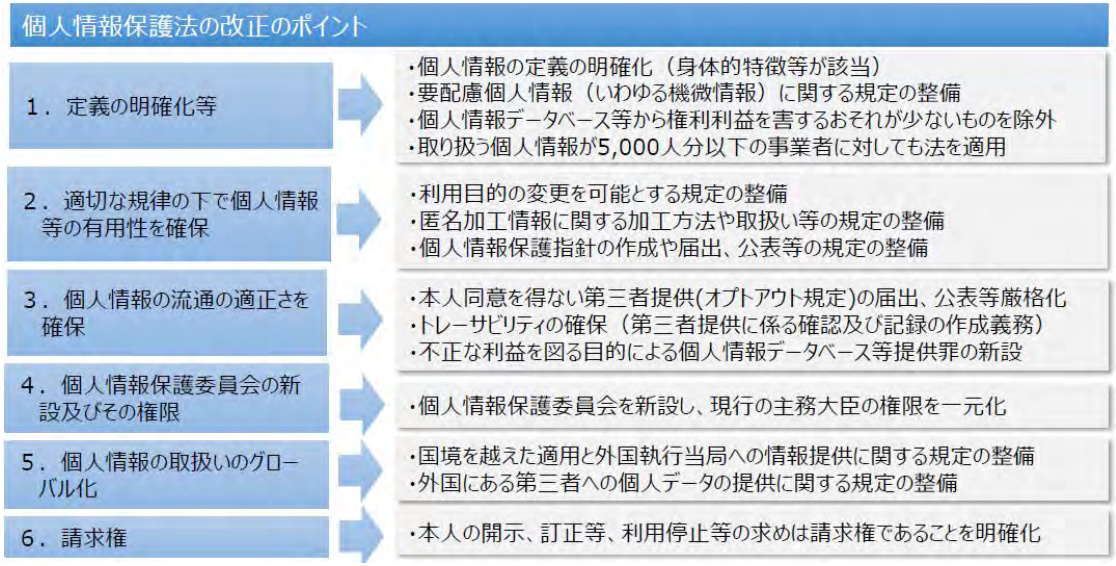
セキュリティ／データ利活用のための個人情報保護

〔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。



※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）

- 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。