資料4

NISC National Information Security Center

技術戦略専門委員会における検討方針（案）について

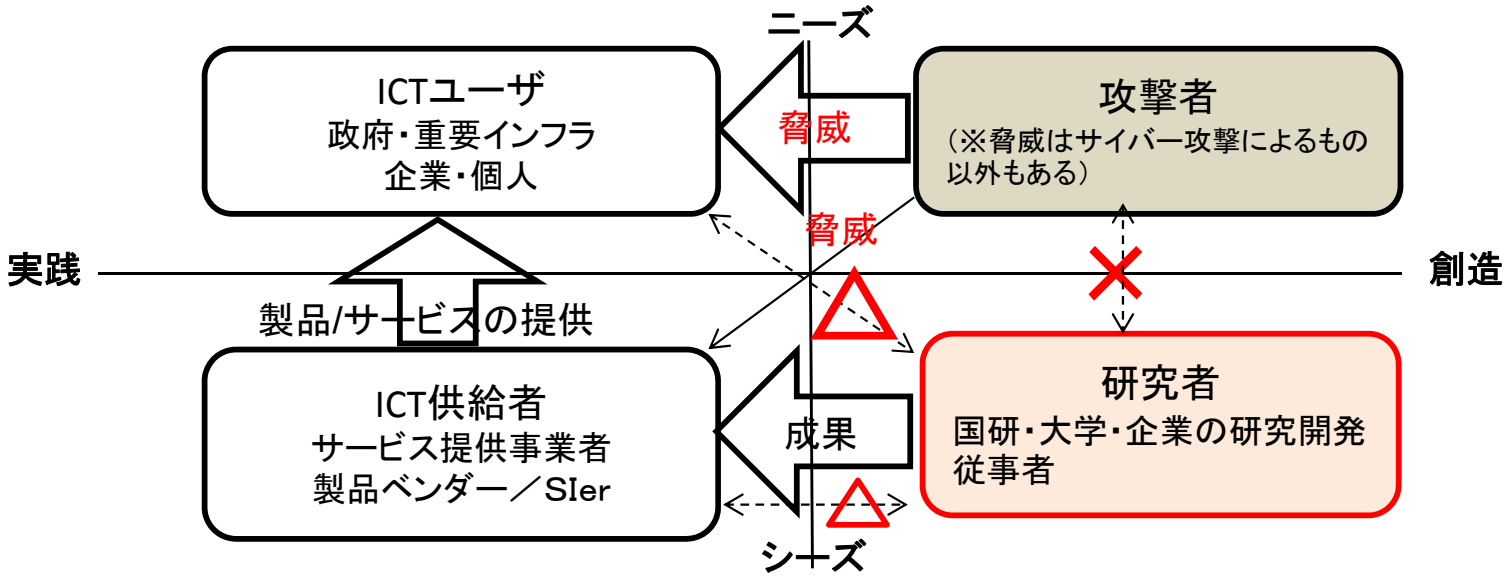
平成26年12月

内閣官房情報セキュリティセンター

「情報セキュリティ研究開発戦略（改定版）」の概要①

1．情報セキュリティ研究開発を巡る課題

- 研究・技術開発に当たっては、現実にどのような脅威があり、具体的なニーズが何であるかということを適時適切に把握して取り組むことが必要。そのため、研究開発をより実践的なものとしていくため以下のような課題を解決する必要がある。（下図）
  - ・研究・技術開発に必要な情報等が十分に循環しない状況であること
  - ・攻撃者の情報を研究開発者において把握することが難しいことなどの課題があること　等



「情報セキュリティ研究開発戦略（改定版）」の概要②

サイバーセキュリティ戦略（2013年6月策定） において示された
○ サイバー攻撃の検知・防御能力の向上
○ 制御システム、ICチップなど社会システム等を保護するためのセキュリティ技術の確立
○ ビッグデータ（パーソナルデータ等）利活用等の新サービスのための技術開発　等

を推進する観点から、**「情報セキュリティ研究開発戦略」を改定**

情報セキュリティ研究開発の推進方針

1. **サイバー攻撃の検知・防御能力の向上**
   - ・分散しているサイバー攻撃情報等の共有のための組織等の連携強化
   - ・研究者等へ政府の有するサイバー攻撃の検体等の提供等を検討
2. **社会システム等を防護するためのセキュリティ技術の強化**
   - ・制御システム等のセキュリティ技術の国際標準化・認証制度等を推進
3. **産業活性化につながる新サービス等におけるセキュリティ研究開発**
   - ・今後発展が期待されるIT利用分野で上流工程からセキュリティ品質の組込を推進
4. **情報セキュリティのコア技術の保持**
   - ・暗号等のコア技術の保持は、我が国の新規産業創出や安全保障等の観点から重要であり維持・強化
5. **国際連携による研究開発の強化**
   - ・各国が「強み」を有する技術を組合せ発展させるため、研究者受入等国際連携を推進

研究開発の効果・成果を高めるための方策等

1. 研究成果の社会還元の推進
2. 必要な研究開発リソースの確保と柔軟性確保
3. 情報セキュリティ技術と社会科学など他分野との融合

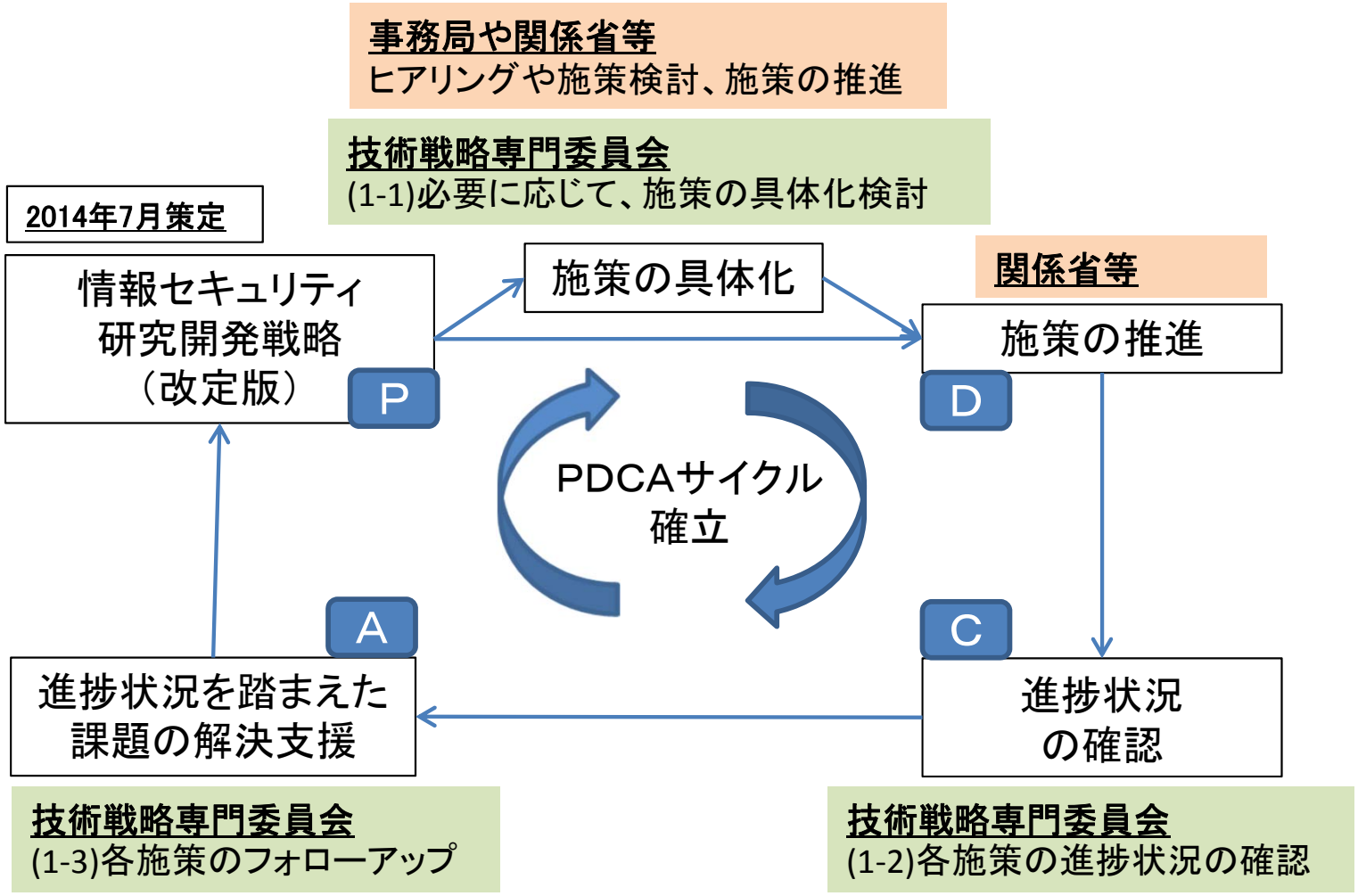
情報セキュリティ研究開発における重要分野

（※　左記の観点を踏まえ、重要分野を整理）

（1）情報通信システム全体のセキュリティの向上
サイバー攻撃の検知、認証、次世代ネットワーク　等
（2）ハード・ソフトウェアセキュリティの向上
制御システム、デバイス、ソフトウェアの安全性確保　等
（3）個人情報等の安全性の高い管理の実現
プライバシー保護、パーソナルデータ利活用　等
（4）研究開発の促進基盤の確立と理論の体系化
理論体系化、調査研究、標準化、評価、暗号技術　等
（5）発展分野でのセキュリティ研究開発
医療健康、農業、次世代インフラ、ビッグデータ、自動車のネットワーク接続　等

技術戦略専門委員会の進め方

【技術戦略専門委員会の進め方】
「情報セキュリティ研究開発戦略（改定版）」の施策の具体化検討、進捗状況確認、フォローアップを行っていくことで、新しいサイバーセキュリティ戦略の策定・検討のインプットにつなげるなど、全体の戦略への反映等につなげていく。



技術戦略専門委員会における検討方針（案）①

■ 本年７月に決定した「**情報セキュリティ研究開発戦略（改定版）**」に基づき施策を推進していくに当たり、専門委員会として定期的にフォローアップを実施していく。（プログラム「おわりに」に記載）

■ 施策ごとに状況や性質等が異なるため、その促進等に当たってはいくつかのアプローチが考えられるが、例えば以下の内容等について専門委員会でのレビューを踏まえ、各施策の推進、評価、総合調整等を進めていってはどうか

【①関係省庁等で既に着手されており、引き続き着実に推進すべき施策】
〇研究開発戦略（改定版）の着実な推進の観点から、専門委員会でも進捗状況等を適時把握し、必要に応じ提言を行う。

- 大学等における研究者又は法人の自主的な研究開発
- 独立行政法人で行われている基礎的研究開発。例えば、CRYPTREC等のわが国として必要な暗号等のコア技術の保持に関するプロジェクト　　等

【②専門委員会として積極的に関与していくべき施策】
〇必要な取組について、専門委員会として関係省庁に働きかける等により、施策を具体化

- サイバー攻撃の検知・防御に関する研究開発
- 政府が保有するサイバー攻撃情報等の共有化の推進
- 制御機器に係る国際標準化、国際的な相互認証に向けた研究開発
- 産業活性化につながる新サービス等におけるセキュリティ研究開発
- 情報セキュリティ技術と社会科学など他分野との融合　　等

技術戦略専門委員会における検討方針（案）②

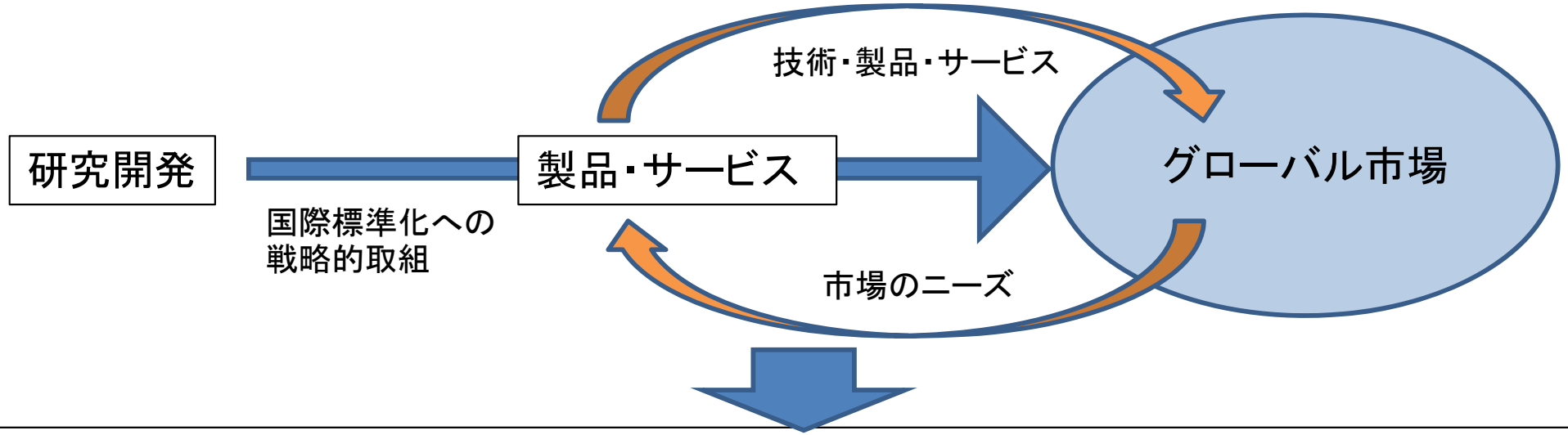
【環境変化】
- モノのインターネット（Internet of Things : IoT）の普及が進み、組込み機器を含む多数のデバイスがネットワークに接続する社会が進みつつある。
- 医療健康、農業、次世代インフラ、家電、自動車などの分野でIT利活用とネットワーク接続が進み、社会インフラに組み込まれ、広がっていく。
- セキュリティ問題が、国民生活や社会・経済活動に重大な影響を与える可能性が高まる。

【推進方針の考え方】
- IoTが普及していくサイバー空間で、セキュリティ確保をすることが重要となる。
- IoT分野は、成長産業領域であり、また日本がリードしていける余地のある領域である。

- **本専門委員会で積極的に関与していく領域の一つとして、成長産業であるIoTの領域を中心としていってはどうか。**

技術戦略専門委員会における検討方針（案）③

【研究開発を通じた目標】
- IoTの普及が進んでいく中、セキュアな技術・製品・サービス（保守・運用を含む）を創り出し、日本発のグローバルIT製品・サービスの実現を目指す。



【実現のために取組が望まれる事項】
- セキュリティ品質を確保するために
  ①上流工程からセキュリティ設計を組み込むこと
- セキュリティ品質が客観的にわかりグローバル市場に受入られるため、
  ②国際標準化や認証（適合性評価）への研究開発段階からの取組
- IoTの機器やサービスは複数の業界・団体にまたがることから、
  ③IoT関連のセキュリティ情報の共有を進める

技術戦略専門委員会における検討方針（案）④　上流工程からのセキュリティ確保

【問題意識】

・医療健康・農業・次世代インフラなどの分野で、IT利活用・ネットワーク接続が進みつつある。
・日本ブランド品質の一つとしてセキュリティを位置づけるために、企画・設計段階の上流工程からセキュリティ品質を組み込むことが重要。

【研究開発の推進の方策（案）】

シーズ側からのアプローチとニーズ側からのアプローチが考えられるが、まずはニーズからのアプローチを主に考えていってはどうか。

（シーズ側からのアプローチ）

- 政府が推進する研究開発プロジェクト等のうち、新たにネットワーク接続を伴うシステム等（例えば、自動車のネットワーク接続等）において、研究・開発・企画の段階から情報セキュリティが組み込まれているかを確認。

（ニーズ側からのアプローチ）

- 製品・サービスとして求められるサービス要件の確保に必要なセキュリティ基準等を設定。（例えば、電力システムであれば、スマートメーターを導入した場合も、電力の安定供給としての本来の目的を達成するものでなくてはならない。）

技術戦略専門委員会における検討方針（案）⑤　標準化・認証

【問題意識】

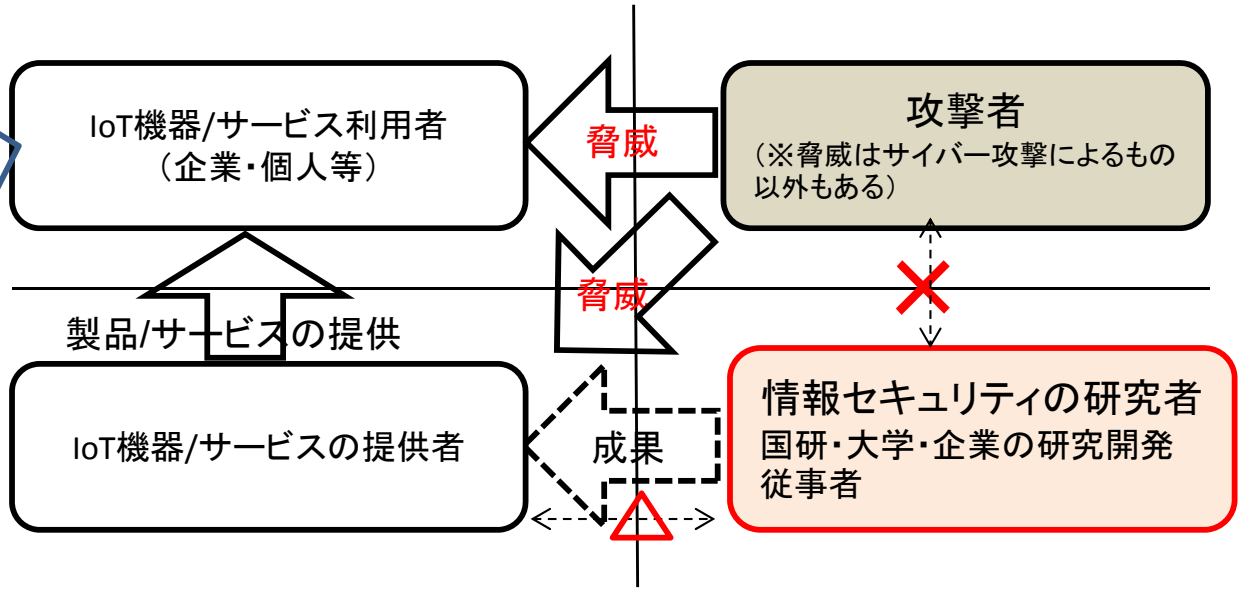
- 国際的に利用されるセキュリティ技術となるには、セキュリティレベルの客観性が必要となり、国際標準化が重要となってくると考えられる。このため、技術開発の際には、国際標準化や認証制度についても並行して考慮していく必要があるのではないか。
- 国際標準化や認証（適合性評価）の取組について、各業界毎に推進しているが、分野間連携が必要ではないか。

【研究開発戦略の推進の方策（案）】

- 政府が推進するセキュリティ研究開発プロジェクトについて、国際標準化や認証（適合性評価）等についての対応が考慮がされているかを評価し、推進していってはどうか。
- また、各業界毎に進めている国際標準化や認証（適合性評価）の取組について後押しするため、政府・公的研究機関として検討の場を設けるとともに、適合性評価等について公的研究機関の活用など必要な支援を行っていってはどうか。

技術戦略専門委員会における検討方針（案）⑥　セキュリティ情報の情報共有

【問題意識】
（1）IoT機器/サービスの提供者は、様々な業界・企業にまたがる。
（2）IoT機器/サービスでは、サイバー攻撃の検知や脆弱性の管理体制が、従来のインターネットサービス関係者と比べて十分でないことが想定される。



【研究開発戦略の推進の方策（案）】
・各業界や企業に分散して蓄積されているセキュリティ情報を共有することが望まれる。
・また、セキュリティ情報が必要な研究者に共有され、必要な研究開発が推進されることが望まれる。
・さらに、事故情報などを集約し、その情報等を活用して製品のアフターフォロー等の継続的なサービスや新製品・サービスに活用されることが望まれる。