資料2－5

情報セキュリティ研究開発戦略（改定版）について

（総合科学技術・イノベーション会議　第7回 ICT-WG ご報告資料）

平成27年1月

内閣サイバーセキュリティセンター

情報セキュリティ研究開発戦略の取組状況

【これまでの取組】

①情報セキュリティ研究開発戦略の見直しについて、
平成26年1月の第4回 ICT-WGでご報告後、情報セキュリティ研究開発戦略（改定版）を策定した。（平成26年7月　情報セキュリティ政策会議決定）
策定にあたり、「情報セキュリティ政策会議 技術戦略専門委員会」での検討や有識者ヒアリング、意見公募等を行った。

＜ご参考URL＞
・http://www.nisc.go.jp/materials/index.html　の「情報セキュリティ研究開発戦略（改定版）」
・http://www.nisc.go.jp/conference/seisaku/strategy/index.html（技術戦略専門委員会）

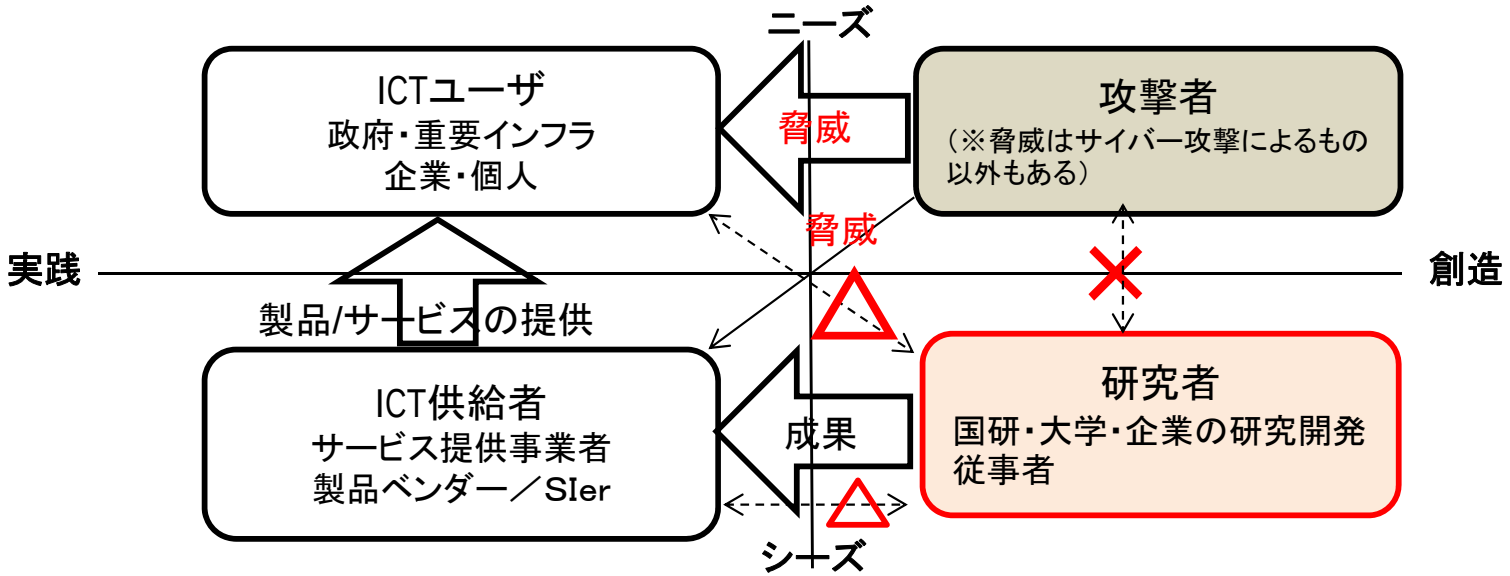
②情報セキュリティ研究開発戦略（改定版）も踏まえ、
関係省庁と連携し、研究開発関連の施策を推進中。

③技術戦略専門委員会（第26回）を平成26年12月に開催し、
今後の技術戦略専門の委員会の進め方や、成長産業であるIoT（Internet of Things：モノのインターネット）領域のセキュリティなどについて議論を行った。

「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における検討方針（案）①

■ 平成26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

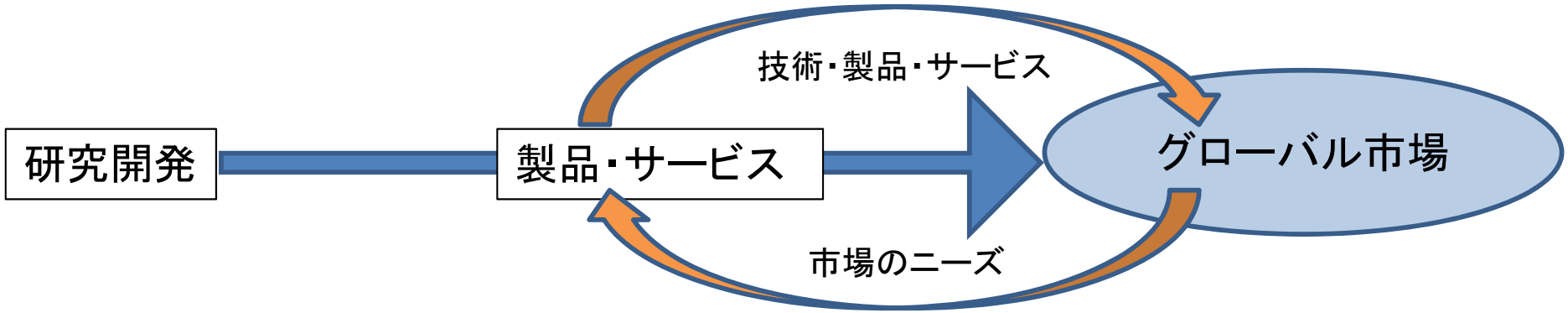
- サイバー攻撃の検知・防御に関する研究開発
- 政府が保有するサイバー攻撃情報等の共有化の推進
- 制御機器に係る国際標準化、国際的な相互認証に向けた研究開発
- 産業活性化につながる新サービス等におけるセキュリティ研究開発
- 情報セキュリティ技術と社会科学など他分野との融合　　等

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。

- 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。

- 技術戦略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**を中心としてはどうか。
- 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して**はどうか。
- IoT領域の研究開発や組織連携が、政府等の組織で十分に取組まれているかを、確認・調整していく予定。



情報セキュリティ研究開発戦略の今後の予定

【今後の予定】

（1）情報セキュリティ研究開発戦略（改定版）も踏まえ、関係省庁と連携し、
研究開発関連施策の状況確認や推進を予定。

（2）技術戦略専門委員会は、今後、年2～3回程度の頻度で開催していく予定。
技術戦略専門委員会では、研究開発戦略（改定版）のフォローアップ、
IoT（モノのインターネット接続）領域のセキュリティに関する議論や、
その他の領域に関する議論などを行っていく予定。

（3）技術戦略専門委員会での議論の結果は、以下のようなものに反映につなげていく想定。
①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（～平成27年夏頃）
など、政府の戦略等への反映
②関係行政機関の経費の見積り方針の作成

内閣サイバーセキュリティセンターのご紹介

ご参考

平成27年1月9日 に
「内閣官房 情報セキュリティセンター」は「内閣官房 内閣サイバーセキュリティセンター」に改組しました。

【旧組織名称】内閣官房 情報セキュリティセンター
National Information Security Center (略称NISC)

【新組織名称】内閣官房 内閣サイバーセキュリティセンター
National center of Incident readiness and
Strategy for Cybersecurity (略称NISC)

「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針（案）」概要

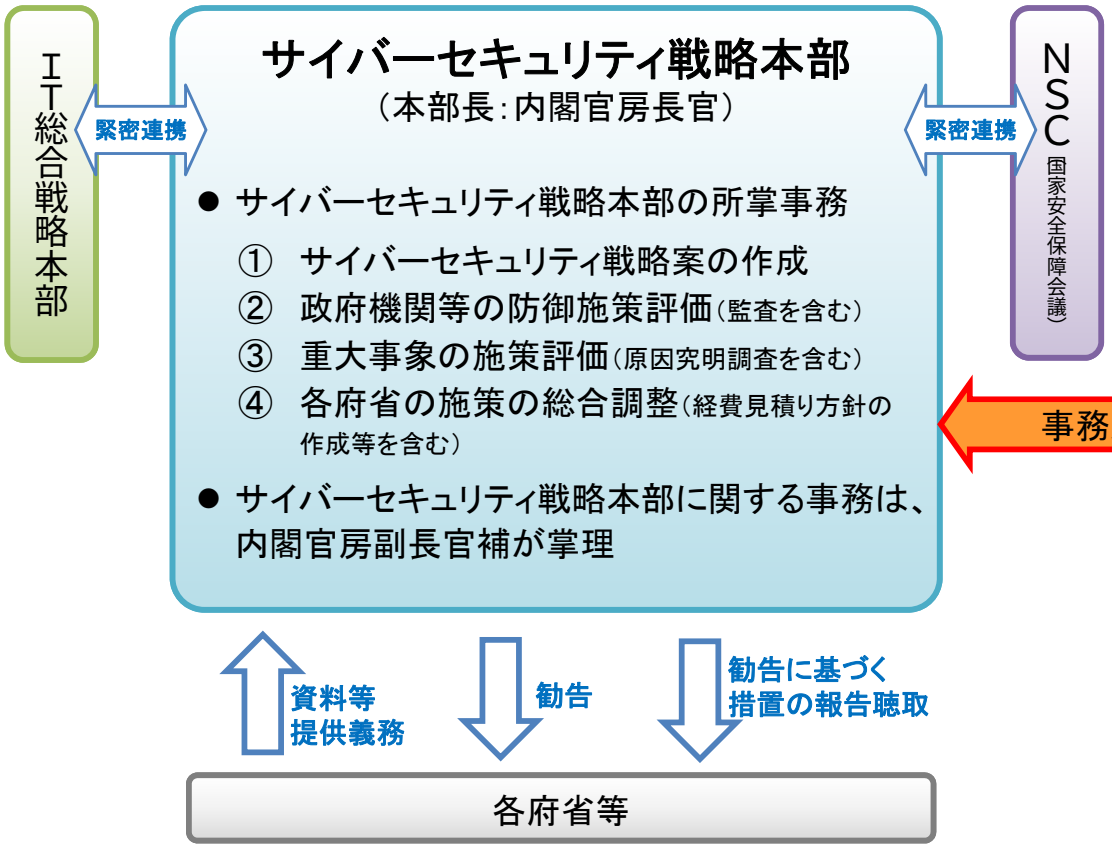
ご参考

1　機能強化の必要性

以下の観点から、我が国の「サイバーセキュリティ」強化のための推進体制の機能強化が不可欠

- あらゆる活動のサイバー空間への依存の高まりにより、リスクが深刻化（甚大化・拡散・グローバル化）
- 「世界最高水準のIT利活用社会」の実現が成長戦略の柱の1つ
- 国際的な連携の強化が必要な諸外国においても、積極的な体制強化を実施
- 2020年東京オリンピック・パラリンピックに向けた対策の強化が必要

2　サイバーセキュリティ基本法の制定



3　我が国の推進体制の機能強化に向けた取組

（1）情報セキュリティ政策会議の担ってきた機能は、サイバーセキュリティ戦略本部が担うこととなる。

（2）内閣官房情報セキュリティセンター（NISC）を以下の組織に法制化（内閣官房組織令）する。

内閣サイバーセキュリティセンター（注）

- 内閣サイバーセキュリティセンターの所掌事務
  - ①GSOCに関する事務
  - ②原因究明調査に関する事務
  - ③監査等に関する事務
  - ④サイバーセキュリティに関する企画・立案、総合調整
- センター長には、内閣官房副長官補をもって充てる

（3）今後、戦略本部の事務の稼働状況、オリンピック・パラリンピック東京大会開催に向けた準備、サイバー空間における脅威の増大等の諸情勢を踏まえつつ、法制の追加的な整備等について引き続き検討。

（注）英名称：National center of Incident readiness and Strategy for Cybersecurity

制度整備を踏まえた内閣サイバーセキュリティセンター（NISC）に関する主な検討事項

ご参考

制度整備を踏まえ、内閣サイバーセキュリティセンター（NISC）に関して、2020年オリンピック・パラリンピック東京大会も見据えつつ、主に以下の項目について必要な措置の検討を行い、可及的速やかに結論を得る。

① GSOC機能の強化

- 新システム（2017年度～）の運用を見据えた体制、機材の整備　等

② 総合的分析機能の強化

- 諸外国の政策、サイバー攻撃の脅威情勢及び攻撃に使用された技術等の総合的な分析
- 高度な専門知識と深い知見を有する専門的人材の確保及び資質の向上

③ 国内外の情報集約機能の強化

インシデント情報の集約機能や助言機能等の強化に向けた、

- 官民連携のスキーム強化・構築
- NISC内の体制・システム整備及び能力向上

④ 国際連携の強化

- 緊急対応関連機関とのパートナーシップ構築等による国際的な窓口機能の強化

⑤ 人材の育成及び登用

- 各省庁からの出向等人材を通じ、NISC内の知見・経験を各省庁に還元
- 任期付任用や人事交流の推進等による技能を備えた人材の確保