NISC
National center of Incident readiness and Strategy for Cybersecurity

参考資料５－２

サイバーセキュリティ研究開発戦略 骨子について

平成29年 3月 3日

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

内閣サイバーセキュリティセンター（NISC）

１．策定方針

平成26年７月に、今後３年程度を見据えた基本的な研究開発の方針として、「情報セキュリティ研究開発戦略（改訂版）」を策定した。「サイバーセキュリティ基本法」及び「サイバーセキュリティ戦略」（平成27年9月策定）を踏まえ、「サイバーセキュリティ研究開発戦略」を策定する。

（１）研究開発の目的

①研究開発を通じて国際競争力を強化すること
②研究開発で得られた知見により経済成長につながる新産業を創出すること
③我が国として必要な技術力を獲得・保持すること

（２）対象

- 政府や公的研究機関等のみならず、大学、企業等の取組についても視野に入れる。

（３）時間軸と内容

- 「近い将来」だけでなく「中長期」な社会・経済とITの利活用の進化を視野に入れる。
- 個々の技術的な課題を深掘りするのではなく、将来的なサイバーセキュリティの考え方を踏まえた研究開発の方向性について、ビジョンを示す。

2．状況認識と課題

（1）視点

・ITの進歩は極めて急速であり、数年後の予測は困難。このため、長い人類の歴史を見据えた上で、現在を位置付け、未来に向けたサイバーセキュリティの研究開発を考えていくことが必要

（2）現代の認識

・人類の知的活動に関わる欲求について、これまで「知の継承」（文字と紙の発明）、「知の流通」（活版印刷の発明）、さらには「場所や時間の制約にとらわれない知の共有・活用」（コンピュータとインターネットの発明）を実現

・経済成長のために必要な新しい価値を生むフロンティアの発見が必要

・近代（工業化社会）の終わりとしての情報・知の時代をむかえており、万人が自己の思いやより良い社会の実現をできる転換期に差しかかっているのではないか。

（3）ITの進化と人・社会のかかわり

・専門家のツールとしてのITから、個人のツールとしてのIT、そしてあらゆる個人とその活動・モノがつながるITに変遷。その中で、近年、人と情報の関わり方も大きく変化。

①**「情報の環境化（空気のような存在）」**：インターネットの普及により、多くの情報が身の回りにあふれる時代

②**「環境の情報化」**：IoTによりITが実世界と結びつき、センサーが実世界から収集したデータを基に実世界を変えることができる時代

③**「環境の知能化」**：実世界から収集したデータがビッグデータとして蓄積され、そこから有用な情報を取り出すために人工知能が活用される時代

（4）今後の課題

・サイバー空間の広がりや脅威の深刻化を踏まえ、近い将来のITの利活用に必要なサイバーセキュリティに関する研究開発を推進するとともに、サイバーセキュリティの考え方の変化を含め、中長期を見据えた独自性の高い研究開発を推進していくことが必要。

３．サイバー空間の脅威の深刻化への対応
～近い将来のITの利活用に必要なサイバーセキュリティ技術の開発～

近い将来（５～１０年後）想定されるITの利活用の進化と、セキュリティ研究開発における課題に対応するための取組を推進する。その際、脅威に対する後追いではなく、近い将来の脅威を見越した研究開発を行うことが重要である。

■基本的な考え方

- システム全体（情報システムだけでなく、それを取り巻く環境）を視野に入れることが重要
- サイバー攻撃の防御技術だけでなく、設計・運用・評価分析といったライフサイクルの各段階での技術も重要
- セキュリティ技術だけでなく、マネジメントやリスクコミュニケーションといった社会学的なアプローチも重要

■近い将来のITの利活用の進化(例)

サイバー空間と物理空間の融合(IoT)	AIの高度化・ビッグデータの活用	ネットワーク技術の高度化
• セキュリティの範囲が広がるため、セキュリティ技術のみならず、幅広い技術の知見を統合した研究開発。 • これまで物理空間特有の問題であった安全管理を視野に入れたセキュリティの研究開発。	• ビッグデータの信頼性を確保して活用する技術やプライバシー保護の研究開発。 • AIの脆弱性に対する攻撃対応。 • サイバー攻撃のAI化への対応（防御のAI化）。	• 新しいネットワーク技術におけるセキュリティ・バイ・デザインが必要。 • 暗号の高速化・高度化が必要。 （例：暗号化したまま高速に検索ができる技術の確立など）

■セキュリティ研究開発における課題に対応した方法論（例）

- 産学官の連携と企業経営層のリーダーシップによる研究開発
- 攻撃の実データを活かした実践的な研究開発
- サイバーセキュリティの研究開発に係る制度の検討（海外も視野に入れた対応）
- オープン・クローズド戦略と海外への発信

4．サイバーセキュリティの考え方の再定義
～中長期を見据えた独自性の高い研究開発～

- 超高齢化社会と人口減少社会といった課題に直面する中、サイバー空間を介して人間の能力は拡張し、これまでの生活や労働を代替するにとどまらず、新たな価値を創造していくと考えられる。そして、人々の思いやより良い社会の実現につながっていく可能性がある。
- このように実空間とサイバー空間の融合が高度に深化していく中で、「自由、公正かつ安全なサイバー空間」を創出・発展させるためには、サイバーセキュリティの考え方として、サイバー空間を構成する情報システムへの脅威への対応のみならず、「人間」や「人間が安心して暮らすことのできる社会システム」を守り、強くすることに注目すべき。（サイバーセキュリティの考え方の再定義）

■人間や社会システムを守る視点での研究開発（例）

（人間の脳を守る）

・AIやAR/VR技術により、サイバー空間を介して人間の判断や行動に影響を及ぼすことへの対応が必要ではないか？

（人間の身体を守る）

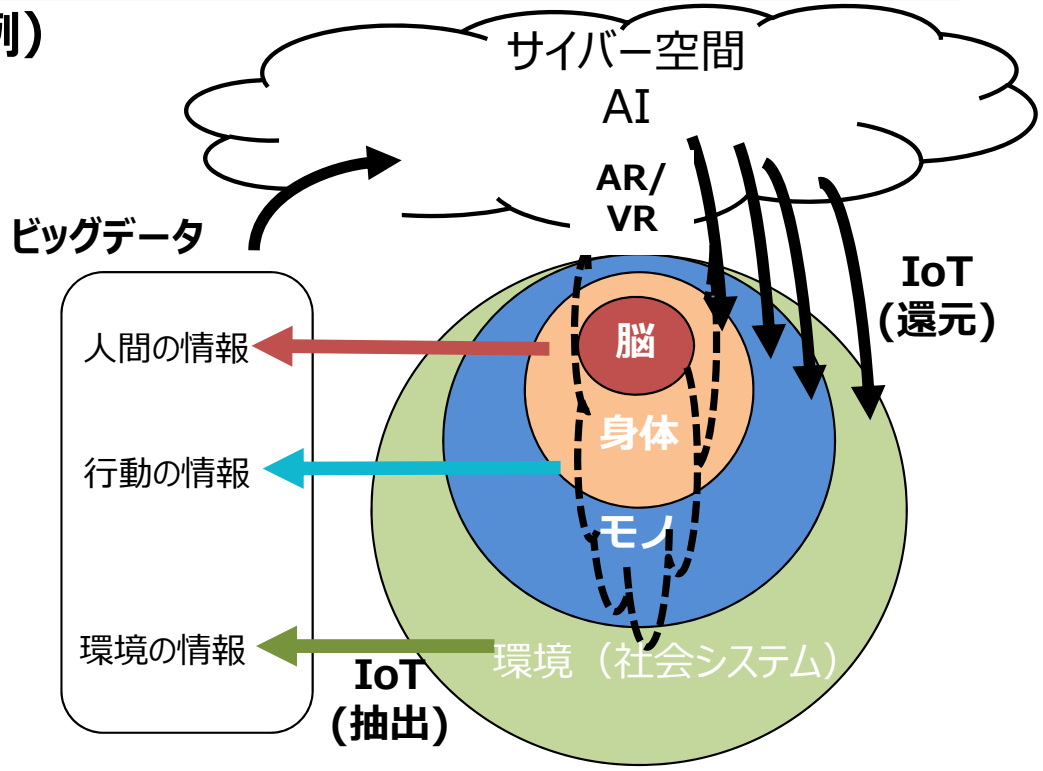
・自動運転やロボットといったIoT技術が身近になるため、サイバー空間からのいかなる影響に対しても、人間の安全を確保することが必要ではないか？

（人間を取り巻く環境（社会システム）を守る）

・「機能保証」の考え方を基本とした研究開発の再構築が必要ではないか？

■システム全体を強くするための方法論（例）

- 異分野（心理学や安全工学だけでなく、脳科学、政治学や社会学などの社会科学、文化人類学など）と連携したアプローチの検討
  - 予測困難な変化に強い仕組とするため、人の生活や社会の許容度など多要素の知見を集積して全体として適切なシステムを構築



サイバー空間は、書類や画像・音声等を電子化した情報が共有されるだけでなく、脳や身体（人間）、身の回りにあるモノ、さらには環境（社会システム）とつながり、人間の能力が拡張するとともに、モノや環境が知能化するなど、実空間に多大な影響を及ぼしうるのではないか。

出典：株式会社NTTデータ経営研究所　Info-Future No.52のレポートを参考にNISC作成