NISC National center of Incident readiness and Strategy for Cybersecurity

資料５

サイバーセキュリティ研究開発戦略（案）（概要）

平成29年 5月26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）

サイバーセキュリティ研究開発戦略（概要）

【趣旨】

○情報通信技術（ＩＴ）の進化や、人間と情報の関わり方が変化していることを踏まえつつ、将来的（近い将来、中長期）なサイバーセキュリティ研究開発の方向性についてビジョンを提示

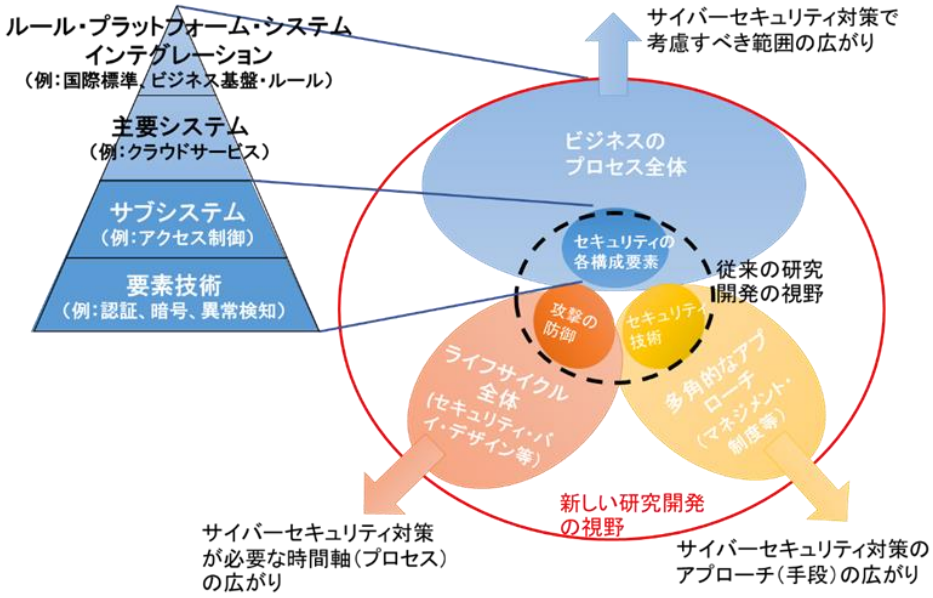
【近い将来】

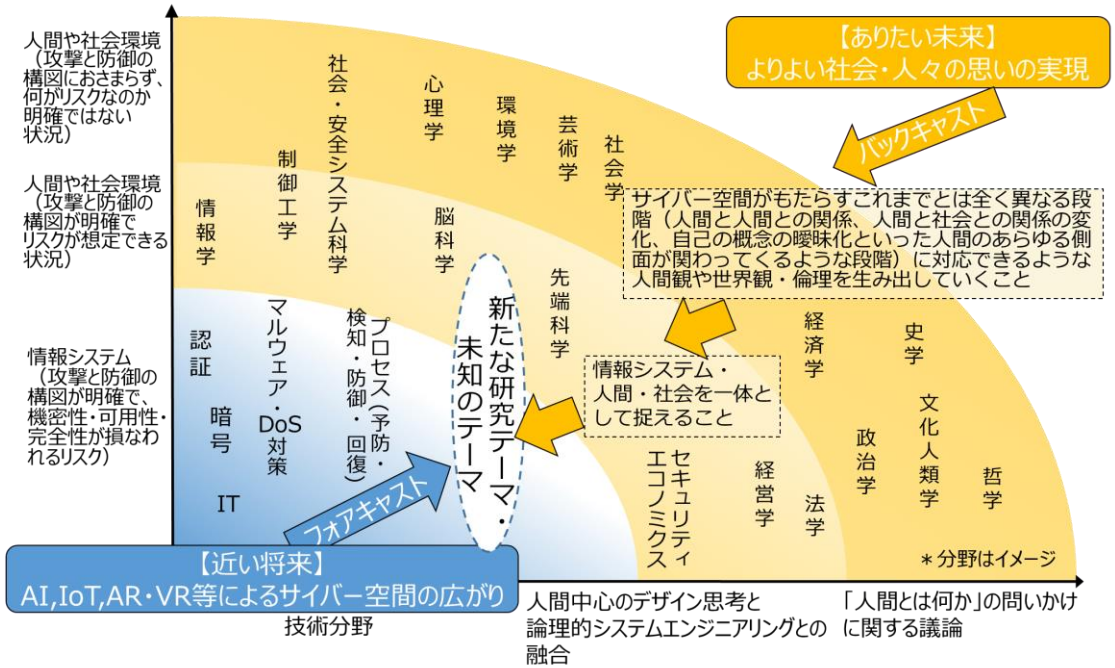
情報システムの進化（つながる（IoT）、知能化する（AI）、広がる(ネットワーク技術)）**を見据え、研究開発の視野を広げることが必要**

IoT、AI、AR・VR等
ITのさらなる進化

【中長期】

サイバーセキュリティの考え方の再定義：情報システムだけでなく、社会や人間を一体として捉えることが必要





【今後の取組】

○人文社会科学分野を含め、本戦略を発信し、具体的な研究分野やテーマについて検討を行うなど、具体化に取り組む。

(参考)サイバーセキュリティ研究開発戦略

【趣旨】

○情報通信技術（ＩＴ）の進化や、人間と情報の関わり方が変化していることを踏まえつつ、将来的（近い将来、中長期）なサイバーセキュリティ研究開発の方向性についてビジョンを提示

○研究開発の目的として、多様な価値観を持つ人間の思いが実現でき、人間が安心して暮らすことのできる社会システムを創造していくことを前提として、研究開発を通じて国際競争力を強化すること、研究開発で得られた知見により新産業を創出すること、我が国として必要な技術力を獲得・保持すること、を意識。

【近い将来】

○基本的考え方：多層防御のサイバーセキュリティだけでは対処が困難な可能性。視野を広げてサイバーセキュリティ対策を捉え、研究開発に取り組んでいくことが期待される。

- セキュリティの各構成要素だけでなく、ｼｽﾃﾑｲﾝﾃｸﾞﾚｰｼｮﾝなどをビジネスプロセス全体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・廃棄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多角的なアプローチも重要

○テーマ：近い将来のＩＴの利活用の変化の流れ（つながる（IoT）、知能化する（AI）、広がる（ネットワーク関連技術））を見据えた研究開発が必要。

○方法論：研究開発の課題に対応した方法論（産学連携、ｵｰﾌﾟﾝ・ｸﾛｰｽﾞ戦略等）も、視野に入れることが必要。

【中長期】

○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、サイバー空間においては、ＩｏＴやＡＩ、ＡＲ・ＶＲ等により、人間の能力は拡張し、実空間とサイバー空間の融合が高度に深化していく。これにより、これまでの労働を代替するにとどまらず、新たな価値を創造し、より良い社会や人々の思いの実現につながっていく可能性がある。

○一方、こうした情報通信技術（IT）は、経済社会の変化をもたらし、現在の経済社会を前提とした将来の技術進歩の外挿（フォアキャスト）によるアプローチのみでは、限界がある可能性。このため、サイバーセキュリティの考え方を再定義（「情報システム」だけでなく、「人間」や「社会」を一体として捉えたセキュリティ）し、ありたい未来から現在すべきことを考えるバックキャストのアプローチも必要。

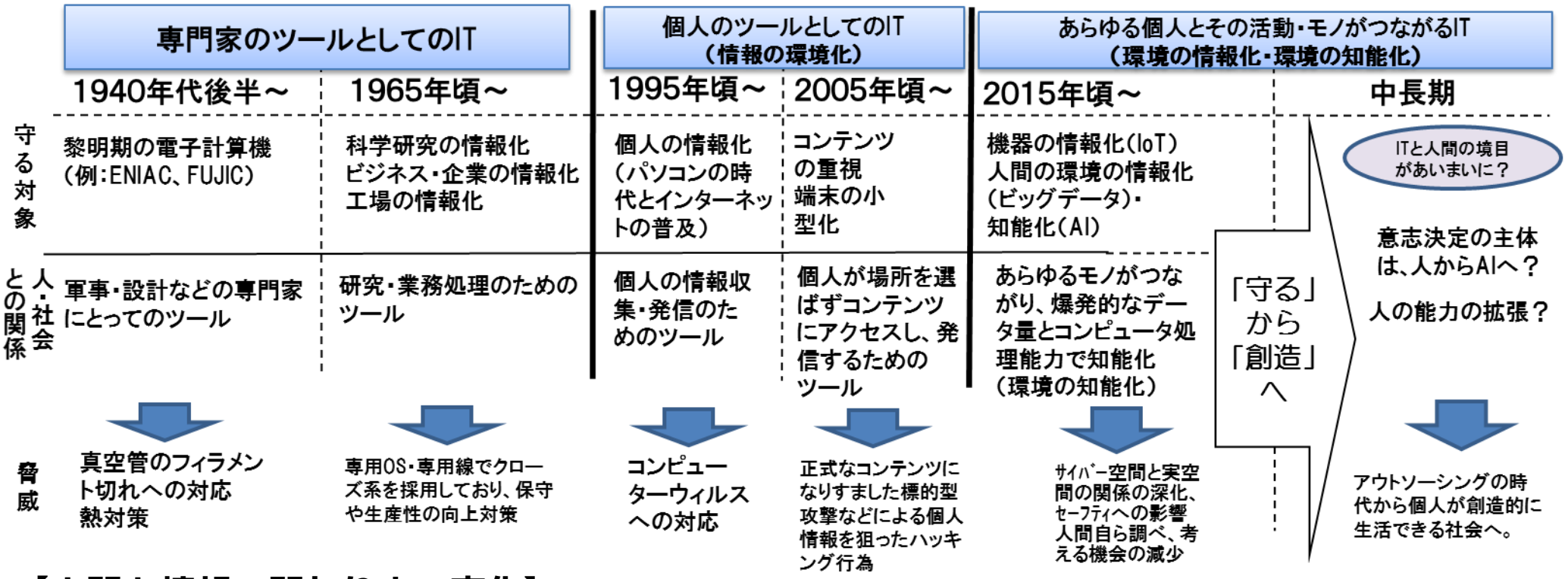
○人文社会科学や情報通信技術（IT）に関連する様々な分野との協業により、「人間」や「社会」を一体で捉えることで、新たなサイバーセキュリティ研究の発見につながる。その際、人間中心のデザイン思考と論理的なシステムエンジニアリングとを融合させるアプローチが有効な可能性。こうしたサイバーセキュリティ研究は、創造的なものであり、人類社会の持続可能性という課題を解決することにつながるもの。

【今後の取組】

○人文社会科学分野を含め、本戦略を発信し、具体的な研究分野やテーマについて検討を行うなど、具体化に取り組む。

（参考）情報通信技術（ＩＴ）の進化/人間と情報の関わり方の変化

【情報通信技術（ＩＴ）の進化】



【人間と情報の関わり方の変化】

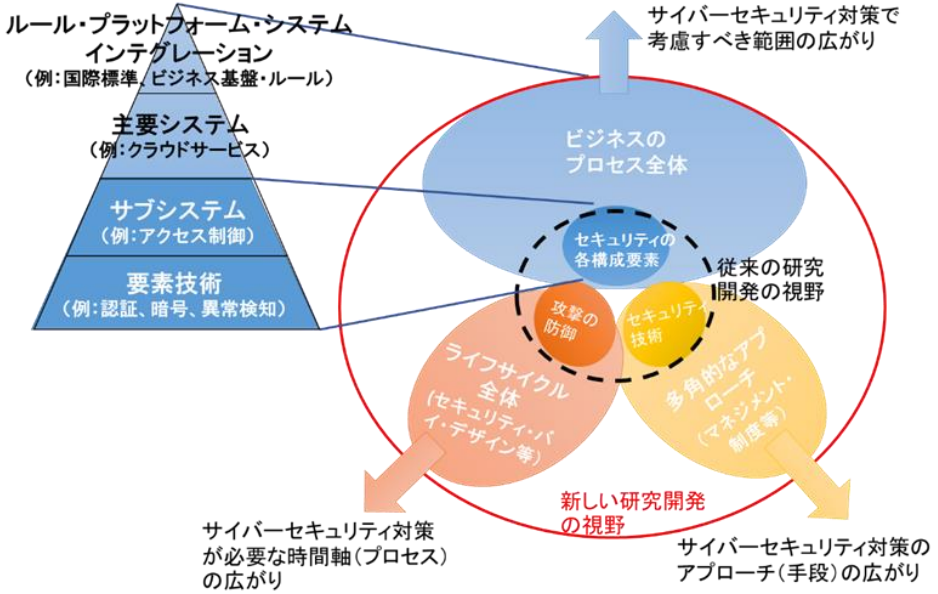
①情報の環境化（インターネットの普及により、多くの情報が身の回りにあふれること）

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こと）

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こと）

（参考）近い将来のＩＴの利活用を想定した研究開発戦略

【研究開発の視野の広がり】



【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
- 脅威に関する情報やユーザー等のニーズを踏まえ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・クローズ戦略の推進と情報発信
- イノベーションの「シーズ」としての研究開発の推進

【近い将来のITの利活用の進化(例)】

つながる
－サイバー空間と物理空間の融合(IoT)－

- IoTシステムは、安全性の要求等従来型の情報システムと異なる特性を持つ。
- 我が国の強み・弱みを捉え、想定されるビジネス自体の目的や戦略に照らし、ビジネスの品質を決定する一要素としてIoTシステムのセキュリティの考え方の整理を前提にした、研究開発が必要。

知能化する
－AIの高度化・ビッグデータの活用－

- AIの普及により、その悪用が公共利益の損失につながる可能性があることから、ガイドラインや倫理指針等を踏まえた対応が必要
- サイバーセキュリティ分野におけるAIの活用（攻撃者の持つ技術の高度化への対応）

広がる
－ネットワーク技術の高度化－

- 新しいネットワーク関連技術（ＳＤＮ、ブロックチェーン等）の発展を踏まえた対応が必要。
- 既存の仕組を根本的に変えるような技術の発展の影響に関する社会学的研究も必要。

（参考）中長期を見据えた研究開発戦略

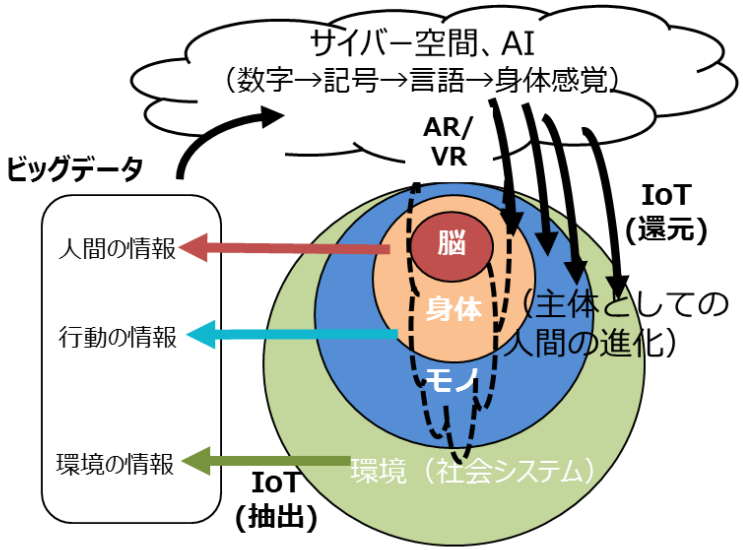
【サイバー空間の広がり】

多様な価値観を承認し、人々の物理的欲求のみならず、精神的な欲求をも満たし、より良い社会を形成する基盤

①ＡＩ（人工知能）
ディープラーニングにより「目を持った機械（認識や運動の上達ができる機械・ロボット）」が誕生

②ＡＲ・ＶＲ（拡張・仮想現実）
VRは、身体を介した一人称の体験をパブリッシュ（本人が知覚可能な体験として、コピー・伝送・再生）することが可能なシステム。

（サイバー空間と人間の関係）



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

【サイバーセキュリティの考え方の再定義】

サイバー空間の広がりによって経済社会の前提が変化する中、現在の経済社会を前提とした将来の技術進歩の外挿（フォアキャスト）によるアプローチのみでは、限界がある可能性

↓

「情報システム」だけでなく、「人間」や「社会」を一体として捉えたサイバーセキュリティ（ありたい未来からのバックキャスト）

人文社会科学や情報通信技術（IT）に関連する様々な分野との協業を図りつつ、人間中心のデザイン思考と論理的なシステムエンジニアリングとを融合させるアプローチによって、人類社会の持続可能性という課題を解決できる可能性。

（サイバーセキュリティ研究の広がり）