「次期サイバーセキュリティ戦略」（骨子）の概要

参考資料１－１

中長期的

戦略期間

１　策定の趣旨・背景

１－１　サイバー空間がもたらす変革の潮流（自律・分散・協調によるサイバー空間の急速な拡張及び発展、人類がこれまでに経験したことのないパラダイムシフト（Society5.0））

１－２　2015年戦略策定とそれ以降の状況変化等（サイバー空間と実空間の一体化に伴う脅威の深刻化・巧妙化、2020年東京大会等を見据えた新たな戦略の必要性）

２　サイバー空間に係る認識

２－１　サイバー空間がもたらす恩恵

・人工知能（AI）、IoT※等による技術革新やサービス利用が社会的に定着し、経済社会活動・国民生活の既存構造を覆すイノベーションを牽引、あらゆる領域で利用拡大

※：Internet of Thingsの略

２－２　サイバー空間がもたらす脅威

・IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、脅威は深刻化・巧妙化。経済的・社会的損失のリスクも指数関数的に拡大

３　目的

３－１　我が国の基本的な立場

（１）基本法の目的（２）基本的な理念（自由、公正かつ安全なサイバー空間）（３）基本原則（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）

３－２　サイバーセキュリティの基本的な在り方（別紙）

（１）目指す姿（「サイバーセキュリティエコシステム」（仮称）（持続的な発展のためのサイバーセキュリティ）の推進）（２）主な観点（①任務保証、②リスクマネジメント、③参加・連携・協働）

４　目的達成のための施策

経済社会の活力の向上及び持続的発展

１．新たな価値創出を支えるサイバーセキュリティの推進

＜施策例＞・経営層の意識改革
・サイバーセキュリティに対する投資の推進
・先端技術を利用したイノベーションを支えるサイバーセキュリティビジネスの強化

２．多様なつながりから価値を生み出すサプライチェーンの実現

＜施策例＞・セキュリティ対策指針の策定
・サプライチェーンにおける機器・サービスのセキュリティを確認できる仕組の構築
・中小企業の取組の促進

３．安全なIoTシステムの構築

＜施策例＞・IoTシステムにおけるセキュリティの体系の整備と国際標準化
・脆弱性対策に係る体制の整備

等

国民が安全で安心して暮らせる社会の実現

１．国民・社会を守るための取組

＜施策例＞・安全・安心なサイバー空間の利用環境の構築

２．2020年東京大会とその後を見据えた取組

＜施策例＞・2020年東京大会に向けた態勢の整備
・未来につながる成果の継承

３．官民一体となった重要インフラの防護

＜施策例＞・サイバー攻撃発生時における関係主体の冷静かつ適切な対応を促進する取組
・地方公共団体のセキュリティ強化・充実

４．政府機関等におけるセキュリティ強化・充実

＜施策例＞・情報システムのセキュリティ対策の高度化・可視化
・クラウド化の推進によるセキュリティ施策の集約等
・先端技術の活用による先取り対応への挑戦

５．大学等における安全・安心な教育・研究環境の確保

＜施策例＞・大学等の多様性を踏まえた対策の推進

６．従来の枠を超えた情報共有・連携体制の構築

＜施策例＞・多様な主体の情報共有・連携の推進
・情報共有・連携の新たな段階へ

等

国際社会の平和・安定及び我が国の安全保障

１．「自由、公正かつ安全なサイバー空間」の堅持

＜施策例＞・「自由、公正かつ安全なサイバー空間」の理念の発信
・サイバー空間における法の支配の推進

２．我が国の防御力・抑止力・状況把握力の強化

＜施策例＞・国家の強靭性の確保
（①任務保証、②我が国の先端技術・防衛関連技術の防護、③サイバー空間を悪用したテロ組織の活動への対策）
・サイバー攻撃に対する抑止力の向上
（①対応措置、②信頼醸成措置）
・サイバー状況把握（CSA）の強化
（①対処機関の能力向上、②サイバー攻撃対処能力向上のための脅威情報連携）

３．国際協力・連携

＜施策例＞・知見の共有
・事故対応等に係る国際連携の強化
・能力構築支援

等

横断的施策

研究開発の推進　＜施策例＞実践的な研究開発の推進、研究開発環境の整備、国内外への積極的な発信

人材育成・確保　＜施策例＞戦略マネジメント層の育成、実務者・専門家層の育成、人材育成基盤の整備、国際連携の推進

全員参加による協働　＜施策例＞政府による取組、関係団体等の連携、安全・安心な利用環境の構築

５　推進体制

本戦略の実現に向け、サイバーセキュリティ戦略本部の下、内閣サイバーセキュリティセンターが主導的役割を担いつつ、政府一体となった対策、官民及び関係省庁間の連携強化を推進。また、危機管理対応についても一層の強化　等

（別紙）次期戦略におけるサイバーセキュリティの基本的な在り方のイメージ（案）

○　サイバー空間と実空間の一体化が加速的に進展する中、現行戦略で「無限の価値を産むフロンティア」とされたサイバー空間が持続的に発展し、新しい価値やサービスが次々と創出されて人々に豊かさをもたらす社会（Society5.0※）を実現させるため、官民のサイバーセキュリティに関する取組を、３つの観点（①任務保証、②リスクマネジメント、③参加・連携・協働）から、推進する。

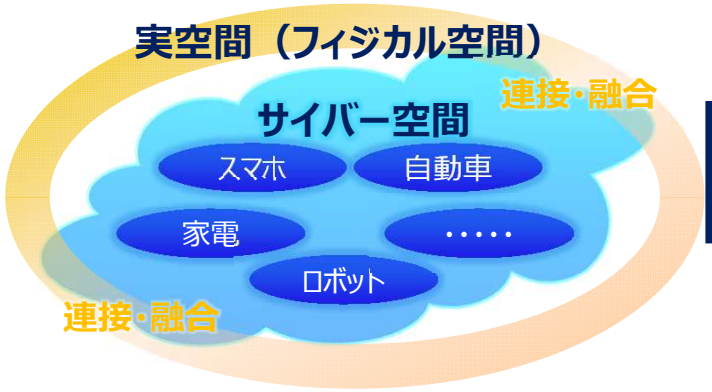
※　狩猟社会、農耕社会、工業社会、情報社会に続く、人類史上５番目の新しい社会。新しい価値やサービスが次々と創出され、社会の主体たる人々に豊かさをもたらしていく。（未来投資戦略2017より）

（参考）サイバー空間の認識に関する変化のイメージ

中長期

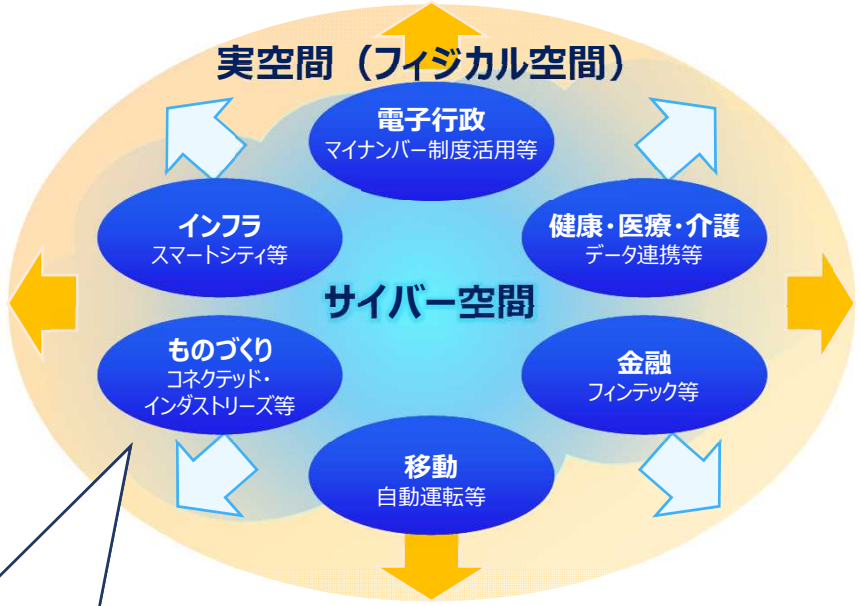
現行戦略策定時（2015年9月）から現在における変化

【（現行戦略策定時）連接融合情報社会の到来】
～実空間のヒト・モノがネットワークに**連接**され、
実空間とサイバー空間の**融合**が高度に深化～



一体化

【サイバー空間と実空間の一体化、活動空間の拡張】



サイバー空間がもたらす恩恵

・技術革新（AI、IoT、Fintech等）やサービスの利用拡大に支えられ、**経済社会活動・国民生活の**様々な分野で、既存社会の構造を根底から覆すような**イノベーションを牽引**。

・これにより、**サイバー空間と実空間の一体化が進展し、必須インフラ化**。

・**人間社会全体の活動空間自体も急速に拡張**。
この恩恵を最大限享受できるようにすべき。

サイバー空間がもたらす脅威

・サイバー空間における**脅威は深刻化・巧妙化**（例：ゼロディ攻撃、ダークウェブ、AI活用）。

・サイバー空間と実空間の一体化の進展に伴い、**実空間での経済的・社会的損失のリスクが指数的に拡大するおそれ**。

・こうした影響拡大の可能性も踏まえて、国家の関与が疑われる事案が増加し、**被害の深刻化が懸念される。**

・**もはや特定の主体による対策だけではサイバーセキュリティは守れず**、イノベーションに支障が生ずるおそれ。