サイバーセキュリティ戦略の概要

平成30年７月27日
閣 議 決 定

◆ 新たなサイバーセキュリティ戦略(2018年７月)は、サイバーセキュリティ基本法に基づく２回目の「サイバーセキュリティに関する基本的な計画」。2020年以降の目指す姿も念頭に、我が国の基本的な立場等と今後３年間（2018年～2021年）の諸施策の目標及び実施方針を国内外に示すもの

◆ サイバーセキュリティ2018は、同戦略に基づく初めての年次計画であり、各府省庁はこれに基づき、施策を着実に実施

＜新戦略(2018年戦略) （平成30年7月27日閣議決定）の全体構成＞

1 策定の趣旨・背景

- サイバー空間がもたらす人類が経験したことのないパラダイムシフト（Society5.0）
- サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会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

- 人工知能（AI）、IoTなど科学的知見・技術革新やサービス利用が社会に定着し、人々に豊かさをもたらしている。
- 技術・サービスを制御できなくなるおそれは常に内在。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、多大な経済的・社会的損失が生ずる可能性は指数関数的に拡大

3 本戦略の目的

- 基本的な立場の堅持（基本法の目的、基本的な理念（自由、公正かつ安全なサイバー空間）及び基本原則）
- 目指すサイバーセキュリティの基本的な在り方：持続的な発展のためのサイバーセキュリティ（サイバーセキュリティエコシステム）の推進。３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）からの取組を推進

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

～新たな価値創出を支えるサイバーセキュリティの推進～

- 新たな価値創出を支えるサイバーセキュリティの推進
- 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
- 安全なIoTシステムの構築

国民が安全で安心して暮らせる社会の実現

～国民・社会を守る任務を保証～

- 国民・社会を守るための取組
- 官民一体となった重要インフラの防護
- 政府機関等におけるセキュリティ強化・充実
- 大学等における安全・安心な教育・研究環境の確保
- 2020年東京大会とその後を見据えた取組
- 従来の枠を超えた情報共有・連携体制の構築
- 大規模サイバー攻撃事態等への対処態勢の強化

国際社会の平和・安定及び我が国の安全保障への寄与

～自由、公正かつ安全なサイバー空間の堅持～

- 自由、公正かつ安全なサイバー空間の堅持
- 我が国の防御力・抑止力・状況把握力の強化
- 国際協力・連携

横断的施策

- 人材育成・確保
- 研究開発の推進
- 全員参加による協働

5 推進体制

内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図るとともに、同センターが調整・連携の主導的役割を担う。

現状認識と将来像（サイバー空間と実空間の一体化に伴う脅威の深刻化）

中長期

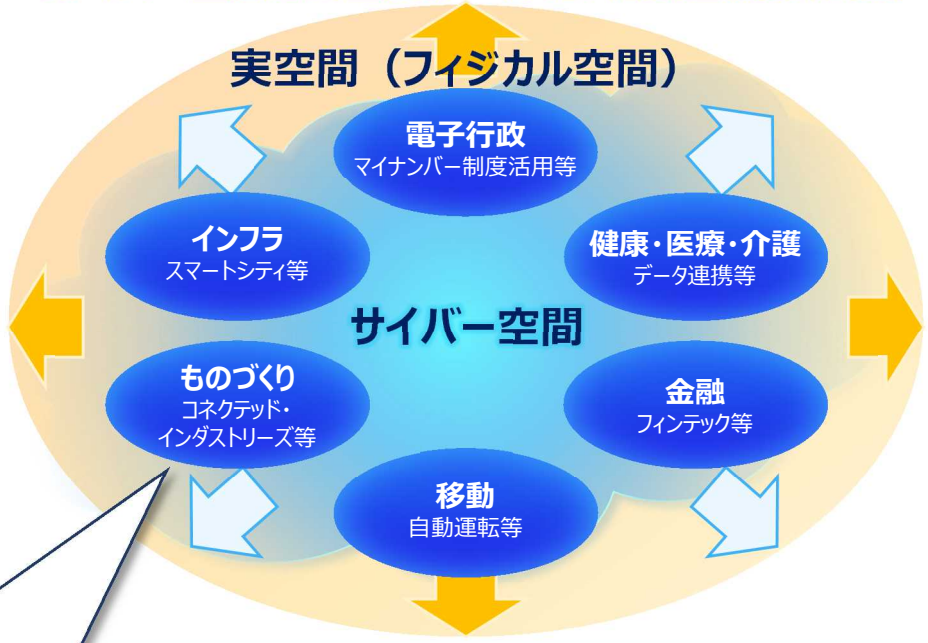
策定の趣旨・背景

【（2015年戦略策定時）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】



サイバー空間に係る認識

・AI、IoT 、Fintech 、ロボティクス、３Dプリンター 、AR/VR など、**サイバー空間における知見や技術・サービスが社会に定着し**、経済社会活動・国民生活の既存構造に変革をもたらす**イノベーションを牽引する一方で、不確実さは常に内在**

サイバー空間がもたらす恩恵

・サイバー空間における技術・サービスが**制御され、様々な分野で当然に利用されており、人々に豊かさをもたらしている**。

・深層学習による**AIの進化**により、既に幅広い産業に応用され始めている。

・**IoT機器で得られるデータ**を利活用した新たなビジネスやサービスが創出されつつある。

サイバー空間における脅威の深刻化

・サイバー空間における技術・サービスを**制御できなくなるおそれは常に内在しており、多大な経済的・社会的な損失が生じ得る。**

・重要インフラサービスの障害やIoT機器の意図しない作動により、様々な**業務・機能・サービス障害が生じた場合、社会に大きな影響が生じ、国家安全保障上の問題**に発展する可能性

・サイバーセキュリティ対策の不備が、**金銭的な損害を直接引き起こし**、拡大することが予想される。

目指す姿（持続的な発展のためのサイバーセキュリティ　–「サイバーセキュリティエコシステム」の実現- ）

○　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※）の実現に寄与するため、実空間との一体化が進展しているサイバー空間の持続的な発展を目指す（「サイバーセキュリティエコシステム」の実現）。

○　このため、これまでの基本的な立場を堅持しつつ、３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）から、官民のサイバーセキュリティに関する取組を推進していく。

※　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）

＜サイバーセキュリティの基本的な在り方のイメージ＞

①サービス提供者の任務保証
- 業務・サービスの着実な遂行 -
Mission Assurance

- 自らが遂行すべき業務やサービスを「任務」と捉え、これを着実に遂行するために必要となる能力及び資産(*)の確保
- 一部の専門家に依存するのではなく、「任務」の遂行の観点から、その責任を有する者が主体的にサイバーセキュリティ確保に取り組む

＊：人材、装備、施設、ネットワーク、情報システム、インフラ、サプライチェーンを含む

持続的な発展のためのサイバーセキュリティ
-「サイバーセキュリティエコシステム」の実現–
Cybersecurity Ecosystem

全ての主体が、サイバーセキュリティに関する取組を自律的に行いつつ、相互に影響を及ぼし合いながら、サイバー空間が進化していく姿を、持続的に発展していく一種の生態系にたとえて、「サイバーセキュリティエコシステム」と呼称する。

②リスクマネジメント
- 不確実性の評価と適切な対応 -
Risk Management

- 組織が担う「任務」の内容に応じて、リスクを特定・分析・評価し、リスクを許容し得る程度まで低減する対応

③参加・連携・協働
- 個人・組織による平時からの対策 -
New　Cyber Hygiene

- サイバー空間の脅威から生じ得る被害やその拡大を防止するため、個人又は組織各々が平時から講じる基本的な取組
- 平時・事案発生時の、各々の努力だけでない、情報共有、個人と組織間の相互連携・協働を新たな「公衆衛生活動」と捉える

【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」に係る諸施策の目標及び実施方針のポイント
新たな価値創出を支えるサイバーセキュリティの推進

・全ての産業分野において、企業が事業継続を確固なものとしていくとともに、新たな価値を創出していくための動きを支えるための基盤として、一体的にサイバーセキュリティの確保に取り組む
・その際には、サイバーセキュリティ対策をリスクマネジメントの一環として捉え、取り組むことが重要

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

- 経営層の意識改革の促進（「費用」から「投資」へ）
- 企業のサイバーセキュリティ対策に関する積極的な情報発信・開示の促進
- 官民が連携してサイバーセキュリティ保険の活用を推進
- セキュリティビジネス強化に向けたガイドライン策定、リスク分析、研究開発等

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

- 脅威を明確化し、運用レベルでの対策を実現する業種横断的指針の作成
- 産業分野ごとの具体的対応策の提示
- 中小企業の取組の推進

３．安全なIoTシステムの構築

- IoTシステムに関するサイバーセキュリティの体系整備と国際標準化
- IoT機器の脆弱性対策モデルの構築・国際発信

国民・社会を守る任務を保証

国民が安全で安心して暮らせる社会を実現するためには、政府機関、地方公共団体、サイバー関連事業者、重要インフラ事業者等、教育研究機関、そして国民一人一人に至るまで、多様な関係者が連携して多層的なサイバーセキュリティを確保することが重要であり、これらの業務やサービスが安全かつ持続的に提供されるよう「任務保証」の考え方に基づく取組を推進していく。

１．国民・社会を守るための取組

- 「積極的サイバー防御」の構築
  （脅威情報の共有・活用の促進、脆弱性情報の提供等）
- サイバー犯罪への対策

２．官民一体となった重要インフラの防護

- 重要インフラ行動計画に基づく取組の推進
- 地方公共団体の取組強化

３．政府機関等におけるセキュリティ強化・充実

- 情報システムの状態のリアルタイム管理の強化（新たな統一基準群に基づく取組等）

４．大学等における安全・安心な教育・研究環境の確保

- 各層別研修及び実践的な訓練・演習の実施

５．2020年東京大会とその後を見据えた取組

- サイバーセキュリティ対処調整センターの構築

６．従来の枠を超えた情報共有・連携体制の構築

- 多様な主体の情報共有・連携の推進

７．大規模サイバー攻撃事態等への対処態勢強化

- サイバー空間と実空間の双方の危機管理に挑むための対処態勢の強化

国民が安全で安心して暮らせる社会の実現

任務保証の実現（サービスの安全かつ持続的な提供）

情報共有・連携
（サイバーセキュリティ協議会、政府オリパラCSIRT等）

自由、公正かつ安全なサイバー空間の堅持

国際社会の平和・安定及び我が国の安全保障のために、自由、公正かつ安全なサイバー空間は必要不可欠である。自由、公正かつ安全なサイバー空間を堅持するため、国際場裡において我が国の立場を発信し、我が国の安全の確保に取り組み、国際協力・連携を進める。

１．自由、公正かつ安全なサイバー空間の堅持

- 自由、公正かつ安全なサイバー空間の理念の発信
  (我が国の意見表明や情報発信、サイバー空間の発展を妨げる取組への対抗等)
- サイバー空間における法の支配の推進
  (国際法の適用、規範の形成・普遍化についての議論への関与等)

２．我が国の防御力・抑止力・状況把握力の強化

- 国家の強靭性の確保
  (関係機関の任務保証、先端技術等の防護等)
- サイバー攻撃に対する抑止力の向上
  (実効的な抑止のための対応、信頼醸成措置等)
- サイバー空間の状況把握の強化
  (関係機関の能力向上、脅威情報連携等)

３．国際協力・連携

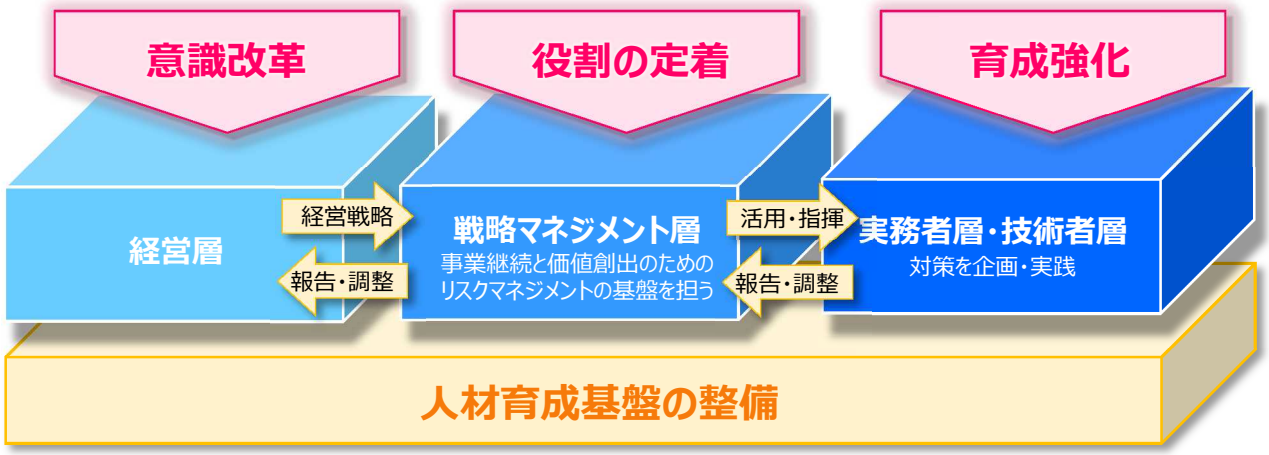
- 知見の共有・政策調整
- 事故対応等に係る国際連携の強化
- 能力構築支援

サイバーセキュリティに関する共通基盤的な取組の推進

サイバーセキュリティを支える基盤的取組として、横断的・中長期的な視点で、人材育成・確保や研究開発に取り組むとともに、
サイバー空間で活動する主体としての国民一人一人が、サイバーセキュリティに取り組むような全員参加による協働を推進

１．人材育成・確保

- 「戦略マネジメント層」の育成・定着
- 実務者層・技術者層の育成
- 人材育成基盤の整備、国際連携の推進
- 各府省庁のセキュリティ人材の確保・育成強化

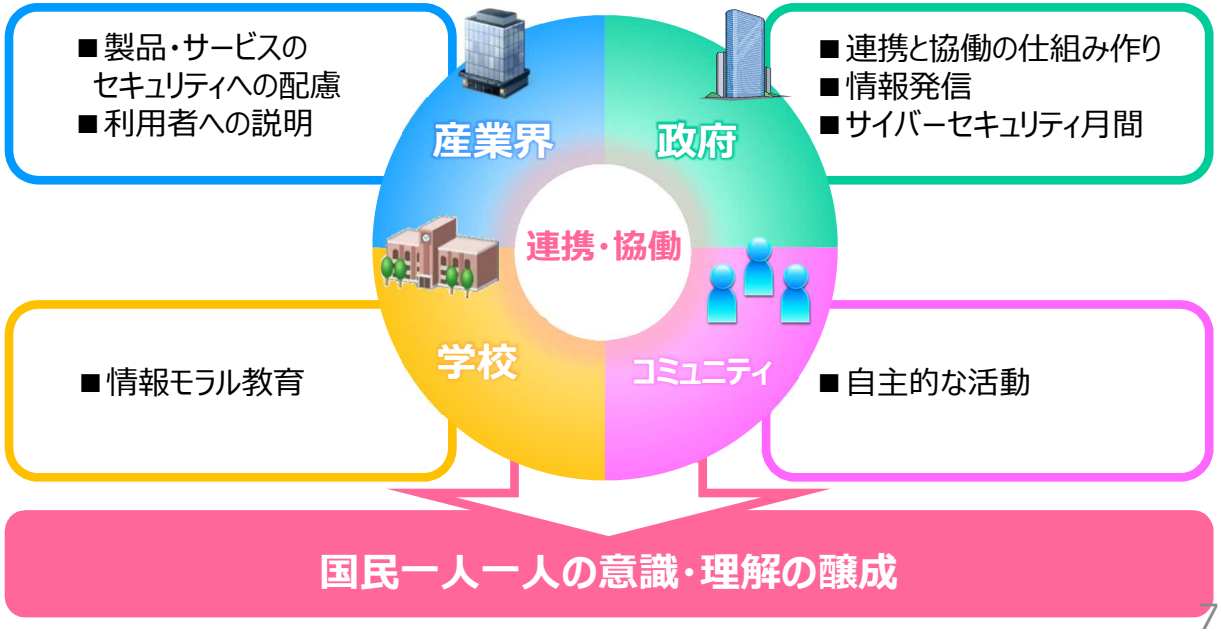


２．研究開発の推進

- 実践的な研究開発の推進
  （検知・防御等の能力向上、不正プログラム等の技術的検証を行うための体制整備等）
- 中長期的な技術・社会の進化を視野に入れた対応

３．全員参加による協働

- サイバーセキュリティの普及啓発に向けたアクションプランの策定とそれに基づく連携・協働
- 「サイバーセキュリティ月間」などを通じた情報発信



【５．推進体制】

推進体制のポイント

○　サイバーセキュリティの確保を通じて、情報通信技術及びデータの利活用を促進し、経済・社会活動の基盤とすること、我が国の安全保障を万全のものとすることは、従来からの方針。サイバーセキュリティ戦略本部の事務局であるNISCを中心に関係機関の一層の能力強化を図るとともに、各府省庁間の総合調整及び産学官民連携の促進の要となる主導的役割を担う。

○　各府省庁の施策が着実かつ効果的に実施されるよう、必要な予算の確保と執行を図る。別紙の担当府省一覧を含む各年度の年次計画を作成する。