

中長期的

## 1 策定の趣旨・背景

1. 1. サイバー空間がもたらすパラダイムシフト（サイバー空間では、創意工夫で活動を飛躍的に拡張できる。人類がこれまでに経験したことのないSociety5.0へのパラダイムシフト）
1. 2. 2015年以降の状況変化（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<sup>\*</sup>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、既存構造を覆すイノベーションを牽引。**様々な分野で当然に利用**され、人々に豊かさをもたらしている。  
※: Internet of Thingsの略
2. 2. サイバー空間における脅威の深刻化
  - ・技術等を**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・社会的な損失が生ずる可能性は拡大

## 3 本戦略の目的

3. 1. **基本的な立場の堅持**
  - (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. 目指すサイバーセキュリティの基本的な在り方
  - (1) 目指す姿（**持続的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**） (2) 主な観点 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**

## 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	国民が安全で安心して暮らせる社会の実現	国際社会の平和・安定及び我が国の安全保障
<ol style="list-style-type: none"> <li>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                &lt;施策例&gt;・<b>経営層の意識改革の促進（「費用」から「投資」へ）</b>                ・投資に向けたインセンティブ創出（情報発信・開示による市場の評価、保険の活用）                ・セキュリティ・バイ・デザインに基づくサイバーセキュリティビジネスの強化</li> <li>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                &lt;施策例&gt;・<b>中小企業を含めたサプライチェーン（機器・データ・サービス等の供給網）におけるサイバーセキュリティ対策指針の策定</b></li> <li>3. 安全なIoTシステムの構築                &lt;施策例&gt;・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                ・<b>IoT機器の脆弱性対策モデルの構築・国際発信</b></li> </ol> <p style="text-align: right;">等</p>	<ol style="list-style-type: none"> <li>1. 国民・社会を守るための取組                &lt;施策例&gt;・脅威に対する事前の防御（<b>積極的サイバー防御</b>）策の構築                ・サイバー犯罪への対策</li> <li>2. 官民一体となった重要インフラの防護                &lt;施策例&gt;・安全基準等の改善・浸透（サイバーセキュリティ対策の<b>関係法令等における保安規制としての位置付け</b>）                ・地方公共団体のセキュリティ強化・充実</li> <li>3. 政府機関等におけるセキュリティ強化・充実                &lt;施策例&gt;・<b>情報システムの状態のリアルタイム管理の強化</b>                ・先端技術の活用による先取り対応への挑戦</li> <li>4. 大学等における安全・安心な教育・研究環境の確保                &lt;施策例&gt;・<b>大学等の多様性を踏まえた対策の推進</b></li> <li>5. 2020年東京大会とその後を見据えた取組                &lt;施策例&gt;・<b>サイバーセキュリティ対処調整センターの構築の推進</b>                ・成果のレガシーとしての活用</li> <li>6. 従来の枠を超えた情報共有・連携体制の構築                &lt;施策例&gt;・<b>多様な主体の情報共有・連携の推進</b></li> <li>7. 大規模サイバー攻撃事態等への対処態勢の強化                &lt;施策例&gt;・<b>実空間とサイバー空間の双方の危機管理に臨むための大規模サイバー攻撃事態等への対処態勢の強化</b></li> </ol> <p style="text-align: right;">等</p>	<ol style="list-style-type: none"> <li>1. 自由、公正かつ安全なサイバー空間の堅持                &lt;施策例&gt;・<b>自由、公正かつ安全なサイバー空間の理念の発信</b>                ・サイバー空間における法の支配の推進</li> <li>2. 我が国の防御力・抑止力・状況把握力の強化                &lt;施策例&gt;・<b>国家の強靱性の確保</b>                (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<b>抑止力の向上</b>                (①実効的な抑止のための対応、②信頼醸成措置)                ・サイバー空間の<b>状況把握の強化</b>                (①関係機関の能力向上、②脅威情報連携)</li> <li>3. 国際協力・連携                &lt;施策例&gt;・<b>知見の共有・政策調整</b>                ・事故対応等に係る国際連携の強化                ・能力構築支援</li> </ol> <p style="text-align: right;">等</p>

### 横断的施策

- 人材育成・確保** <施策例> **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（**高度人材**含む）、人材育成基盤の整備、**政府人材**の確保・育成の強化、国際連携の推進
- 研究開発の推進** <施策例> 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）、**AI**等中長期的な技術・社会の進化を視野に入れた対応
- 全員参加による協働** <施策例> 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**、**国民への情報発信**（サイバーセキュリティ月間の充実等）、サイバーセキュリティ教育の推進

## 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、各府省庁間の総合調整、産学官民連携の促進の要となる主導的役割を担う。また、危機管理対応についても一層の強化 等

戦略期間