

中長期的

1. 策定の趣旨・背景

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）
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

1. サイバー空間がもたらす恩恵
 - 人工知能（AI）、IoT※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。
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

※: Internet of Thingsの略

3. 本戦略の目的

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）
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） (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

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> 経営層の意識改革の促進（「費用」から「投資」へ）
 - サイバーセキュリティ対策の情報開示を促進するための手引きの作成
 - 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
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> 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
3. 安全なIoTシステムの構築
 - 「IoTセキュリティガイドライン」の普及展開
 - <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
 - IoT機器の脆弱性対策モデルの構築・国際発信

改正国立研究開発法人情報通信研究機構法に基づくパスワードに不備のあるIoT機器の調査と注意喚起（プロジェクト「NOTICE」）

マルウェアに感染しているIoT機器の利用者への注意喚起

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
 - サイバー攻撃誘引基盤（STARDUST）、改正電気通信事業法に基づく電気通信事業者間のサイバー攻撃に係る情報共有の促進（認定送信型対電気通信設備サイバー攻撃対処協会）
 - <施策例> 脅威に対する事前の防御（積極的サイバー防御）策の構築
 - 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
 - <施策例> 安全基準等の改善・浸透（サイバーセキュリティ対策の関係法令等における保安規制としての位置付け）
 - 地方公共団体のセキュリティ強化・充実
 - 3. 政府機関等におけるセキュリティ強化・充実
 - <施策例> 情報システムの状態のリアルタイム管理の強化
 - 先端技術の活用による先取り対応への挑戦
 - 4. 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
 - 5. 2020年東京大会とその後を見据えた取組
 - <施策例> サイバーセキュリティ対処調整センターの構築の推進
 - 成果のレガシーとしての活用
 - 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
 - 7. 大規模サイバー攻撃事態等への対処態勢の強化
 - <施策例> サイバー空間と実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

サイバー攻撃観測網（NICTER）

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
 - 信頼サービスの在り方の検討
 - 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> 国家の強靱性の確保
 - 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
 - サイバー空間の状況把握の強化
 - ①関係機関の能力向上、②脅威情報連携
3. 国際協力・連携
 - ISAC連携国際ワークショップ、二国間政策協力対話
 - <施策例> 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
 - 「日ASEANサイバーセキュリティ能力構築センター」に係る支援

等

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

地域のセキュリティ人材育成

NICTIにおける研究開発

実践的サイバー防御演習（CYDER）

SecHack365

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

量子コンピュータ時代に向けた暗号の在り方の検討

5Gのセキュリティ対策

AIを活用したサイバー攻撃検知・解析技術の研究開発

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

公衆無線LANの安全な環境整備、e-ネットキャラバン

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。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。等

戦略期間