内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

参考資料

次期サイバーセキュリティ戦略（案）について

令和３年８月３日

内閣サイバーセキュリティセンター
重要インフラグループ

次期サイバーセキュリティ戦略の課題と方向性

2020年代を迎えた日本を取り巻く時代認識　：　「ニューノーマル」とデジタル社会の到来

- デジタル経済の浸透、**デジタル改革**の推進
- **新型コロナウイルス**の影響・経験
テレワーク、オンライン教育等の進展
- 厳しさを増す**安全保障**環境
- **SDGｓ**への
デジタル技術の貢献期待
- **東京オリンピック・パラリンピック**
に向けた取組

サイバー空間をとりまく課題認識　：　国民全体のサイバー空間への参画

- サイバー空間は、国民全体等**あらゆる主体が参画し公共空間化**
サイバー・フィジカルの垣根を超えた各主体の相互連関・連鎖の深化
攻撃者に狙われ得る弱点にも
- 地政学的緊張を反映
国家間競争の場に
安全保障上の課題にも
- 不適切な利用は
国家分断、人権の阻害へ
- 官民の取組の
活用

あらゆる主体にとってサイバーセキュリティの確保は自らの問題に
５つの基本原則※は堅持

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進

安全保障の観点からの取組強化

公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

「自由、公正かつ安全なサイバー空間」の確保

※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

次期サイバーセキュリティ戦略（案）の構成

中長期的

1　2020年代を迎えた日本をとりまく時代認識

1－1　デジタル経済の浸透・デジタル改革の推進、SDGsへの貢献に対する期待、安全保障環境の変化、新型コロナウイルスの影響・経験、東京大会に向けた取組の活用

2　本戦略における基本的な理念

2－1　確保すべきサイバー空間は「自由、公正かつ安全な空間」

2－2　基本原則は従来の戦略で掲げた５つの原則を堅持（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　サイバー空間をとりまく課題認識

環境変化からみたリスク、国際情勢からみたリスク、近年のサイバー空間における脅威の動向

戦略期間

4　目的達成のための施策

＜3つの方向性＞　（１）デジタル改革を踏まえたデジタルトランスフォーメーション とサイバーセキュリティの同時推進
（２）公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保
（３）安全保障の観点からの取組強化

経済社会の活力の向上及び持続的発展

1．経営層の意識改革

2．地域・中小企業におけるDX with Cybersecurity の推進

3．新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

4．誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

国民が安全で安心して暮らせるデジタル社会の実現

1．国民・社会を守るためのサイバーセキュリティ環境の提供

2．デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

3・4・5．経済社会基盤を支える各主体における取組
①(政府機関等)
②(重要インフラ)
③(大学・教育研究機関等)

6．多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用

7．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

1．「自由、公正かつ安全なサイバー空間」の確保

2．我が国の防御力・抑止力・状況把握力の強化

3．国際協力・連携

横断的施策

研究開発の推進　／　人材の確保・育成・活躍促進　／　全員参加による協働・普及啓発

5　推進体制

「自由、公正かつ安全なサイバー空間」を確保するための政府一体となった推進体制

４.２.４ 経済社会基盤を支える各主体における取組②（重要インフラ）

我が国の経済や社会は、様々な重要インフラサービスの継続的な提供に依存しているが、重要インフラ間の相互依存性の高まりやサプライチェーンの複雑化・グローバル化を踏まえると、安全で安心な社会の実現には、**脅威が年々高まっている重要インフラのサイバーセキュリティを確保し、強靭性を高めることが不可欠**である。

平成26年に公布・施行されたサイバーセキュリティ基本法では、重要インフラ事業者の責務を明確に定めるとともに、国は、重要インフラ事業者等のサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他自主的な取組の促進その他必要な施策を講ずるよう規定されている。

こうしたことを踏まえ、**重要インフラに関わる各主体がそれぞれの責務を認識し、官民が一体となって堅牢な重要インフラの実現に向けた取組を推進**する。

（１）官民連携に基づく重要インフラ防護の推進

国民生活及び社会経済活動の基盤である重要インフラサービスの安全かつ持続的な提供のため、**重要インフラ防護に責任を有する国と自主的な取組を進める事業者等との共通の行動計画を官民で共有し、これを重要インフラ防護に係る基本的な枠組みとして引き続き推進**する。

重要インフラを取り巻く脅威は年々高度化・巧妙化しているが、その一方で、重要インフラ分野ごとにシステムの利用形態が異なることから、各組織における脅威の差異が拡大してきている。このことを踏まえ、重要インフラ防護のよりどころとなる現行の「重要インフラの情報セキュリティ対策に係る第４次行動計画」を基本としつつ、**重要インフラ分野が全体として今後の脅威の動向、システム、資産を取り巻く環境変化に柔軟に対応できるようにするため、行動計画を積極的に改定**し、**官民連携に基づく重要インフラ防護の一層の強化**を図る。

重要インフラサービスの安全かつ持続的な提供において、デジタル技術は大きな役割を果たすものであり、サイバーセキュリティの確保は経営の根幹に関わるものである。この認識の下、ビジネスとセキュリティのバランスが取れ、先進的でセキュリティ対策が適切に講じられた重要インフラサービスの実現を確実なものとするため、各組織が先行事例で得られた教訓を有効に生かせるよう、重要インフラ事業者等による情報収集を円滑にするための横断的な情報共有体制の一層の充実を図るとともに、セキュリティ対策は組織一丸となって取り組むことが重要であることから、**経営層のリーダシップが遺憾なく発揮できる体制の構築**を図っていく。

（２）地方公共団体に対する支援

地方公共団体は、個人情報等の多数の機微な情報を保有し、**国民生活に密接に関係する基礎的なサービスを提供していることに鑑み、国は、地方公共団体において適切にセキュリティが確保されるよう、国と地方の役割分担を踏まえつつ必要な支援を実施**する。

「地方公共団体における情報セキュリティポリシーに関するガイドライン」（以下「ガイドライン」という。）に基づくセキュリティ対策が着実に実施されるよう、人材の確保・育成及び体制の充実並びに必要な予算を確保するための取組を支援する。

地方公共団体情報システムの標準化、行政手続のオンライン化、「クラウド・バイ・デフォルト原則」等を受けたクラウド化、働き方改革や業務継続のためのテレワークの導入等、新たな時代の要請に柔軟に対応できるよう、ガイドラインの継続的な見直し等、必要な諸制度の整備を推進する。

地方におけるデジタル改革（デジタル・ガバメントの実現）を促進するため、国は、「デジタル社会の実現に向けた改革の基本方針」（令和２年12月閣議決定）を踏まえ、整備方針において、地方公共団体のセキュリティについての方針を規定する。

国民生活・国民の個人情報に密接にかかわるマイナンバーについて、利便性とセキュリティの調和を考慮して対策を強化し、安全・安心な利用を促進する。