

平成 31 年 1 月 17 日  
内閣サイバーセキュリティセンター

## 「安全基準等策定指針（第 5 版）の改定」の検討方針

### 1. これまでの取組

「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（平成 29 年 4 月 18 日サイバーセキュリティ戦略本部決定）」は、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきという観点から 13 分野が重要インフラとして指定されていた。今般、これに空港を追加して 14 分野となった（平成 30 年 7 月 25 日サイバーセキュリティ戦略本部決定）。

また、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第 5 版）（平成 30 年 4 月 4 日サイバーセキュリティ戦略本部決定）」が策定され、機能保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供の観点から、安全基準等の継続的な改善に取り組む必要性を明記しており、事業環境等の変化を捉えた改善を行うことが重要である。

### 2. 現状と課題

こうした取組を進める中、各地で複数の自然災害が発生し、重要インフラ事業者等においても、地震や台風によって多大な被害を受けた。また災害による直接的な被害だけでなく、大規模停電に伴う間接的な被害を受ける事態も発生した。こうした状況から、サイバー攻撃だけでなく自然災害に起因する重要インフラサービス障害の発生を可能な限り減らすことが重要である。

また、サイバーセキュリティ戦略（2018）にも記載された通り、重要インフラ事業者等における適切な対応を促進するため、政府が進めるデータの管理の状況に関する調査や国際動向も踏まえた望ましいデータ管理の在り方を含め、安全基準等を改善する取組を継続的に推進する必要がある。

これらの社会動向の変化、新たな知見を踏まえ安全基準等策定指針（第 5 版）を改定することを検討する。

### 3. 改善のポイント

#### (1) 災害による障害の発生しにくい設備の管理

重要インフラサービスの提供に係る情報システムやデータセンターなどの設備は、各種災害等による障害が発生しにくい適切な場所に設置を行うとともに、災害が発生した場合であっても被害を低減する防止対策を図り、適切に保守することを促す内容を追記してはどうか。

#### (2) データ管理の在り方

重要インフラサービスの提供に係る情報システム等のデータ管理については、データを適切に保護するため、現状と課題を整理し、国際動向も踏まえた望ましいデータ管理を行うことを促す内容を追記してはどうか。

#### (3) その他

その他の改定作業として、①空港分野の追加に伴う【別紙1】対象となる重要インフラ事業者等と重要システム例、【別紙2】重要インフラサービスの説明と重要インフラサービス障害の例を修正する。②政府統一基準の改定など参考文献の更新作業に伴い、主に【別紙4】対象項目の具体例等の参照について修正する。

(参考)

### ○サイバーセキュリティ戦略（平成30年7月27日閣議決定）抜粋

#### 4.2.2 官民一体となった重要インフラの防護

##### (1) 行動計画に基づく主な取組

##### ②安全基準等の改善・浸透

重要インフラ事業者等における適切な対応を促進するため、国は、安全基準等を策定するための指針を浸透させる取組を行うとともに、データの管理の状況に関する調査や国際動向も踏まえた望ましいデータ管理や人的要因によるリスク軽減の在り方を含め、業務の内容、組織の規模、システムの使用期間、国際競争力への影響等を考慮して安全基準等を改善する取組を継続的に推進する。