重要インフラのサイバーテロ対策に係る特別行動計画
(概要)

1　目的

いわゆるサイバーテロなど、情報通信ネットワークや情報システムを利用した、国民生活や社会経済活動に重大な影響を及ぼす可能性があるいかなる攻撃からも重要インフラを防護する。

2　対象とする重要インフラ分野

情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む。）

3　官民におけるサイバーテロ対策

(1) 被害の予防（セキュリティ水準の向上）

被害を予防するため、その前提として、対象となる重要インフラの情報システムのリスク分析を行い、情報システムの重要度に応じた対策を講ずることによって、恒常的に各重要インフラ分野のセキュリティ水準の向上を図る。

(2) 官民の連絡・連携体制の確立・強化

セキュリティ情報（セキュリティ改善に必要な情報）及び警報情報（サイバー攻撃の発生情報等の警戒や緊急対処に必要な情報）の共有、予防・対処等を連携して行うための官民における体制の確立・強化を図る。

(3) 官民連携によるサイバー攻撃の検知と緊急対処

各重要インフラ分野においてサイバー攻撃を受けた場合又はそのおそれがある場合の対応策を定めるとともに、官民全体で対処能力の強化を行う。

(4) 情報セキュリティ基盤の構築

サイバーテロ対策を進めていくため、人材の育成、研究開発、普及啓発、法制度の整備等の情報セキュリティ基盤の構築を推進する。

(5) 国際連携

サイバー攻撃は、国境を越えて行われる可能性があることから、このような攻撃に適切に対処するため、国際的な連携を推進する。

4　行動計画の見直し

この行動計画は、官民の連絡・連携体制の確立を中心としてとりまとめた初めてのものであり、政府は、この進捗を踏まえ、定期的及び必要に応じ見直しをする。