

サイバーセキュリティの確保に関する件

政府は、サイバーセキュリティ基本法の施行に当たっては、次の諸点について法的措置も含めて検討を加え、その遺憾なきを期すべきである。

一 具体的な施策

1 サイバーセキュリティ戦略本部は、国家安全保障会議、高度情報通信ネットワーク社会推進戦略本部、内閣危機管理監等と緊密な連携を図ることとするほか、サイバーセキュリティに関する幅広い分野の有識者の意見を十分に取り入れ、施策に反映させるよう努めること。

2 サイバー攻撃関連情報の集約、予防策の構築並びにサイバー攻撃に対応するため
の演習及び訓練の企画及びその実施については、内閣官房情報セキュリティセンタ
ーを中心として総合的に実施すること。

3 内閣情報通信政策監と連携して、サイバーセキュリティに関する施策の評価を定
期的に実施すること。

4 政府の各機関、重要社会基盤事業者及びサイバー関連事業者その他の事業者等
における情報通信関連機器等の安全性に関する基準等については、未知の攻撃手法や

想定外の攻撃対象への攻撃にも柔軟に対応できるよう、防護対象の重要性の段階に応じたものとするなど、総合的かつ有機的な視点から策定すること。

5 大規模サイバー攻撃への対応要領を作成し、関係者の協力の下に行われる定期的な演習及び訓練を通じて実効性のある対応策の構築に努めること。

6 サイバーセキュリティ確保のため、サイバーセキュリティに関する技術の向上のための研究開発予算の充実等の取組を積極的に推進すること。

7 中小企業者その他の民間事業者におけるサイバーセキュリティの確保のための自発的な取組を積極的に促進すること。

8 国民一人一人が自発的にサイバーセキュリティの確保に努めることができるよう、必要な情報の提供及び助言その他の施策を積極的に推進すること。

9 地方公共団体が自主的な施策の策定及びその実施を推進できるよう、積極的な支援を行うこと。

10 内閣官房情報セキュリティセンターについては、サイバーセキュリティ対策を着実に実施するために必要かつ十分な人員、予算を継続的に確保し、サイバーセキュリティ戦略を積極的に実施すること。

11 サイバーセキュリティ戦略本部の事務のうち、監査、原因究明のための調査、府省横断的な計画及び関係行政機関の経費の見積り方針等の作成等について、迅速か

つ効果的に行う体制を整備すること。

二 人材の育成及び登用

1 サイバーセキュリティに関する高度かつ専門的な知識を有する人材の育成に早急に取り組むとともに、人材を関係行政機関及び民間企業等から幅広く登用するよう努め、官民の連携体制を整備すること。

2 国の行政機関等でサイバーセキュリティに係る事務に従事する者の関係府省庁及び民間企業等との積極的な人事交流を推進するとともに、過去の人事慣行にとらわれない人事評価の在り方を検討すること。

三 連携体制の整備

1 サイバー攻撃のもたらす被害の重大性に鑑み、国家安全保障会議等との連携の下、安全保障上の観点から迅速かつ実効性のある措置を講ずることを検討した上で、必要な措置を講ずること。その際には、平素から危機管理、安全保障までを連続的に対応できる体制を整備すること。

2 サイバーセキュリティに関する国際的な連携を推進するため、サイバーセキュリティに関する諸外国の政策や国内外における情勢等の分析、国際的な会議への対応等に関する十分な人員体制を確保し、迅速な情報共有と協力体制の構築を実現すること。

四 サイバー攻撃を組織的に行う集団等の動向を分析し、捜査機関等との情報の適切な共有を図ること。

五 二〇二〇年オリンピック・パラリンピック東京大会におけるサイバーセキュリティに関する事象に対処するための国内外の関係機関との連絡調整等を行う組織の在り方について、将来の推進体制を見据えて検討した上で、必要な措置を講ずること。

六 国民の基本的人権について十分に配慮しつつ、サイバーセキュリティの確保を図るため、インターネットその他の高度情報通信ネットワーク上の通信における実効ある帯域制御の在り方について検討すること。

七 立法機関及び司法機関におけるサイバーセキュリティの確保について、それらの機関からの要請に応じ、必要な協力を行うよう努めること。

右決議する。