第二一六回

衆第一八号

サイバー安全保障を確保するための能動的サイバー防御等に係る態勢の整備の推進に関する法律案

目次

第一章　総則

（目的）

第一条　この法律は、近年、国内外において国家の関与が疑われるサイバー攻撃（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する攻撃をいう。以下同じ。）その他のサイバー攻撃の脅威が増大していることに鑑み、サイバー安全保障を確保するための能動的サイバー防御等に係る態勢の整備（以下「サイバー安全保障態勢の整備」という。）の推進に関し、基本理念を定め、国の責務等を明らかにするとともに、サイバー安全保障態勢の整備の推進に関する施策の基本となる事項を定めることにより、サイバー安全保障態勢の整備を総合的かつ集中的に推進することを目的とする。

（定義）

第二条　この法律において「サイバー安全保障」とは、外部からのサイバー攻撃の脅威に対して国家及び国民の安全を保障することをいう。

２　この法律において「能動的サイバー防御」とは、外部からのサイバー攻撃について、これによる被害が発生する前の段階から、その兆候に係る情報その他の情報の収集を通じて探知し、その主体を特定するとともに、その排除のための措置を講ずることにより、国家及び国民の安全を損なうおそれのあるサイバー攻撃の発生並びにこれによる被害の発生及び拡大の防止を図ることをいう。

（基本理念）

第三条　サイバー安全保障態勢の整備の推進は、次に掲げる事項を旨として行われなければならない。

一　能動的サイバー防御として講ずる措置（以下「能動的サイバー防御措置」という。）その他のサイバー安全保障を確保するための措置が、サイバー攻撃が発生する前の段階から事態の推移に応じて機動的かつ効果的に実施されるようにすること。

二　能動的サイバー防御措置の実施に当たっては、国民の理解と関心を深めることにより、その協力が得られるようにするとともに、関係機関及び関係事業者（サイバーセキュリティ基本法（平成二十六年法律第百四号）第三条第一項に規定する重要社会基盤事業者（第九条において「重要社会基盤事業者」という。）及び同法第七条に規定

するサイバー関連事業者をいう。以下同じ。）相互の連携協力が確保されるようにすること。

三　日本国憲法の保障する国民の自由と権利が尊重されるべきことに鑑み、能動的サイバー防御措置の実施に際して国民の自由と権利に制限が加えられるときであっても、その制限が、国家及び国民の安全を確保するために必要やむを得ない限度を超えるものとならないようにするとともに、公正かつ適正な手続の下に行われるようにすること。

四　サイバー攻撃の排除のための措置が事態に応じ合理的に必要と判断される限度を超えるものとならないようにすること。

五　我が国の能力を生かしつつ積極的に国際協力を推進するものとし、サイバー安全保障を確保するための措置の実施に際しては、関係する外国との協力を緊密にするとともに、国際社会の理解が得られるようにすること。

（国の責務等）

第四条　国は、前条の基本理念（以下この条において「基本理念」という。）にのっとり、サイバー安全保障態勢の整備の推進に関する施策を総合的に策定し、及び実施する責務を有する。

２　地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバー安全保障態勢の整備の推進に関する施策を策定し、及び実施するよう努めるものとする。

３　関係事業者は、基本理念にのっとり、国又は地方公共団体が実施するサイバー安全保障態勢の整備の推進に関する施策に協力するよう努めるものとする。

（法制上の措置等）

第五条　政府は、サイバー安全保障態勢の整備の推進に関する施策を実施するため必要な法制上又は財政上の措置その他の措置を講じなければならない。

第二章　基本的施策

（能動的サイバー防御措置の機動的かつ効果的な実施のための法制の整備等）

第六条　国は、能動的サイバー防御措置を機動的かつ効果的に実施することができるようにするため、速やかに必要な法制の整備その他の措置を講ずるものとする。

２　国は、前項の法制の整備に当たっては、特に、能動的サイバー防御措置の実施に際して国民の自由と権利に加えられる制限が国家及び国民の安全を確保するために必要やむを得ない限度を超えるものとならないようにしなければならない。

（行政組織の整備等）

第七条　国は、サイバー安全保障を確保するための措置を適切かつ効果的に実施することができるようにするため、必要な行政組織の整備、自衛隊その他の関係機関及び関係事業者の連携協力の確保その他必要な体制の整備を行うものとする。

（人材の確保等）

第八条　国は、サイバー安全保障に係る専門的な知識又は技能を有する人材の確保、養成

及び資質の向上に必要な施策を講ずるものとする。

２　国は、前項の施策を講ずるに当たっては、その漏えいが国家及び国民の安全を損なうおそれのある情報を取り扱う者としての適性を有すると認められた人材が確保されるようにするものとする。

（重要社会基盤事業者に対する支援等）

第九条　国は、国家及び国民の安全を損なうおそれのあるサイバー攻撃による被害の発生及び拡大の防止に資するよう、重要社会基盤事業者に対する必要な助言その他の支援、サイバー攻撃を受けた者に対する相談体制の整備その他の必要な施策を講ずるものとする。

（調査及び研究開発の推進等）

第十条　国は、能動的サイバー防御措置の適切かつ効果的な実施に資するよう、情報通信技術その他の技術に関し、調査及び研究開発の推進その他の必要な施策を講ずるものとする。

（能動的サイバー防御措置に関する国民の理解と関心の増進についての留意）

第十一条　国は、サイバーセキュリティ基本法第二十三条の施策を講ずるに当たっては、広報活動等を通じて、能動的サイバー防御措置に関する国民の理解と関心を深めることに特に留意するものとする。

（能動的サイバー防御に関する国際協力の推進等についての留意）

第十二条　国は、サイバーセキュリティ基本法第二十四条の施策を講ずるに当たっては、能動的サイバー防御に関し国際的な規範の策定への主体的な参画その他の国際協力を推進すること及び我が国が実施する能動的サイバー防御措置に対する諸外国の理解を深めることに特に留意するものとする。

附　則

（施行期日）

１　この法律は、公布の日から施行する。

（検討）

２　政府は、この法律の施行後速やかに、虚偽の情報、不正確な情報その他誤解を生じさせるおそれのある情報の情報通信技術を用いた拡散（以下「虚偽情報等の拡散」という。）が国家及び国民の安全に及ぼす影響について調査及び研究を行い、その成果を踏まえ、虚偽情報等の拡散が国家及び国民の安全を損なうことがないようにするための措置について検討を加え、その結果に基づいて必要な措置を講ずるものとする。

理　由

近年、国内外において国家の関与が疑われるサイバー攻撃その他のサイバー攻撃の脅威が増大していることに鑑み、サイバー安全保障態勢の整備の推進に関し、基本理念を定め、国の責務等を明らかにするとともに、サイバー安全保障態勢の整備の推進に関する施策の基本となる事項を定めることにより、サイバー安全保障態勢の整備を総合的かつ集中的に推進する必要がある。これが、この法律案を提出する理由である。