わが国の防衛に関係する空港システム、電力システム、交通システムなどに係るサイバーセキュリティ対策に関する質問主意書

右の質問主意書を国会法第七十四条によって提出する。

平成二十八年三月一日

藤末健三

参議院議長山崎正昭殿

わが国の防衛に関係する空港システム、電力システム、交通システムなどに係るサイバーセキュリティ対策に関する質問主意書

防衛省及び自衛隊のインターネットサイトにおける「自衛隊のサイバー攻撃への対応について」の記述では、「Ｑ２　防衛省・自衛隊はどのように対応しているのですか。」という問いに対して「Ａ２　自衛隊の任務遂行上、サイバー空間の安定的な利用の確保は不可欠な前提となっています。官民における統一的・横断的な情報セキュリティ対策については内閣官房を中心とする取組が進められる一方、防衛省・自衛隊では、自らのシステム・ネットワークの防護に取り組んでいます。昨年９月には、取り組むべき施策を一体的かつ整合的に推進していくための指針として、「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」（「サイバー指針」）をとりまとめるなど、必要な取組を進めているところです。」と回答している。

しかしながら、自衛隊が国土防衛のために活動するには、自衛隊のシステム以外の高度なサイバーセキュリティが重要である。例えば、航空自衛隊が民用と共用している滑走路を管制するシステムのサイバーセキュリティ、自衛隊が駐屯している地域の電力システムのサイバーセキュリティ（電力が完全に独立して供

給できる駐屯地はほぼないはず。海外のサイバー戦の事例を見ると、攻撃の前に電力システムをサイバー攻撃することが常套手段）、陸上部隊が移動する際の交通システムのサイバーセキュリティ（交通信号などは高度な技術を有するハッカーには容易に操作される。陸上自衛隊などが地上交通で移動する際に人為的に交通渋滞を起こすことは容易である）など防衛に関係する防衛省・自衛隊以外のシステムのサイバーセキュリティの強化を行う必要があると考えるが、政府の見解を示されたい。ちなみに内閣サイバーセキュリティセンター（ＮＩＳＣ：National center of Incident readiness and Strategy for Cybersecurity）は民間のハッカー対策を行うレベルであり、海外からのサイバー攻撃に対応するだけのサイバーセキュリティを進める役割を持っていないと考えるが、政府の所見如何。

右質問する。