69

平成二十三年十一月二十五日提出
質問第六九号

サイバーテロ攻撃対策に関する質問主意書

提出者　山内康一

サイバーテロ攻撃対策に関する質問主意書

一　先般、衆議院や総務省のウイルス感染事象に関して、議員端末より実際に端末ＩＤやパスワード、証明書が窃取・悪用された可能性があるという事実は、その情報自体の重要性の観点のみならず、国家の中枢を狙ったサイバーテロ攻撃と同義であり、単純なウイルス感染で片付けられる事ではない。

①　サイバーテロ攻撃対策の組織体制上、国家としての主管はどこか。また国会や省庁間の連携体制や対策予算の編成についての方針はあるのか。

②　多くのサイバーテロ攻撃の発信元は海外からであることが指摘され、その対策には国家間の連携・協力も必要である。他国との国際協力に関する具体策はあるのか。

二　民間企業を狙ったサイバーテロ攻撃による被害も一部メディアで報道されており、その結果、企業が守るべき情報資産（個人情報や知的財産）の漏えいに至っている。サイバーテロ攻撃に対しては旧来よりウイルス対策専門ベンダーが提供するウイルス対策ソフトウェアによる対処が一般的である。しかし、昨今のサイバーテロ攻撃は既存の対策をすべて超えて行われており、末端のウイルス対策ソフトウェアでは防御が不十分で、ネットワーク全体での対策が急務である。内閣官房情報セキュリティセンター（ＮＩＳ

C）をはじめ、各種サイバーセキュリティに関わる指針やガイドラインを提供する団体のオブザーバー（アドバイザー）は、昨今のサイバーテロ攻撃から十分に防御できたとは言えないウイルス対策ベンダーの識者が中心であり、基本メンバーもほとんど変わらない。既に世界ではネットワーク全体を含めたサイバーセキュリティが常識となっている。

① オブザーバー（アドバイザー）として今求められるのはネットワークセキュリティに精通したベンダーや識者であると考えるが、具体的な対策はあるか。

② サイバーテロ攻撃に対して、国家として具体的にガイドラインや指針を提示する必要があると考えるが如何。

③ 国防の観点からも、サイバーテロ攻撃対策に関して政府横断に、民間企業に対しても強制力を持つ組織が必要であると考えるが如何。

右質問する。