296

平成二十九年五月十一日提出
質問第二九六号

北朝鮮からと推定されるサイバー攻撃による銀行への不正アクセスと預金強奪に関する質問主意書

提出者　逢坂誠二

北朝鮮からと推定されるサイバー攻撃による銀行への不正アクセスと預金強奪に関する質問主意書

韓国メディアによると、四月二十六日、アメリカを代表するインターネットセキュリティ企業のシマンテックは報告書を公表し、北朝鮮のサイバー攻撃グループが世界各国の銀行から多額の預金を強奪したとする見方を示した。報告書では、バングラデシュやベトナム、エクアドル、ポーランドなどの銀行を狙ったサイバー攻撃について、北朝鮮との関連を示す証拠を見つけたとした上で、「北朝鮮のサイバー攻撃グループが少なくとも九千四百万ドル（約百五億円）を奪い取ることに成功した」としている。

このような事実を踏まえて、わが国の重要インフラに対してサイバー攻撃が行われた場合の政府の対応について、以下質問する。

一　わが国の銀行などの金融機関に他国からサイバー攻撃が行われ、不正なアクセスがなされて、第三国に送金されることで、当該銀行の口座上の預金が強奪された場合、内閣サイバーセキュリティセンターがいうところの「重要インフラ」に対するサイバー攻撃であり、政府の責務として「政府機関は、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して必要な支援を行う」べきものに該当すると考え

てよいか。

二　シマンテックの報告書でいうところの、バングラデシュやベトナム、エクアドル、ポーランドなどの銀行を狙ったサイバー攻撃について、北朝鮮との関連を示す証拠を見つけた事例に関連して、過去五年間、わが国の重要インフラに対して、北朝鮮との関連を示すサイバー攻撃が行われた事例を政府は把握しているか。把握しているとすれば、その数はどの程度か。

三　政府の情報セキュリティ政策会議が平成二十六年五月に決定した「重要インフラの情報セキュリティ対策に係る第三次行動計画（改訂版）」によれば、「各重要インフラ事業者等の対策を通じ、当該重要インフラ事業者等自身のみならず重要インフラ全体の防護能力の維持・向上を目的に、重要インフラ所管省庁及び重要インフラ事業者等は、対策の経験から得た知見等をもとに、継続的に安全基準等を改善する。具体的には、情報セキュリティ対策の運用、内部監査・外部監査、ＩＴに係る環境変化の調査・分析の結果、演習・訓練及びＩＴ障害対応から課題を抽出し、リスク評価を経て、安全基準等の継続的改善に取り組む」と明示されているが、日常的な重要インフラ全体の防護能力の維持・向上を目的とするもので、実際にサイバー攻撃を受け、金融機関から預金等が盗まれた場合の対応策に欠けているように思われる。こ

のような場合、政府のサイバーセキュリティ関係機関は具体的にどのような対応を行うのか。見解を示されたい。

四　わが国の重要インフラに北朝鮮からのサイバー攻撃が行われ、不正なアクセスにより、第三国等に送金されることで、当該銀行の口座上の預金が強奪された場合、どのような罪名に問われるのか。

五　四に関して、このような行為が行われた場合、不正アクセス行為の禁止等に関する法律第二条第四項でいう「不正アクセス行為」に該当するという理解でよいか。

六　シマンテックの報告書が指摘するように、北朝鮮のサイバー攻撃グループが世界各国の銀行から多額の預金を強奪したことを踏まえれば、わが国の重要インフラも同様の被害を受けることを想定すべきであり、政府としてはどのような対策を行っているのか。また、今後、どのように取り組むべきと考えるのか。

七　六に関して、国民の預金保護の関連から、政府は、サイバー攻撃を受けて銀行の預金が大きく失われた場合の対策を何か行っているのか。その根拠法令とともに、政府の対応について、具体的に示されたい。

右質問する。