2026 年 11 月

日本サイバーセキュリティ・イノベーション委員会（JCIC）　緊急政策提言
「サイバー緊急警報の発令にかかる体制を整備せよ」

サイバー脅威が高まり、被害が急増している。その一因に「発達した AI が既存システムの脆弱性を迅速に見つけること」がある。先般発生した、プログラミング言語 PHP に重大な脆弱性が見つかり、外部からサーバを不正操作されるリスクが懸念されたケースでは、日本国内でも多くの企業が Web サイトやサービスに PHP を利用していることから、政府や企業は対応に追われた。また、高市早苗総理が自身の X アカウントでリスクについて発信し、緊急対応を要請したことにより、セキュリティ関係者のみならず、企業の経営層をはじめ、広く国民全体にその危険性が周知された。

国民の生活に深刻な被害を生じさせうるサイバー攻撃が発生するリスクは急激に高まっている。そのような事態に備え、「サイバー緊急警報」の発令体制の整備をはじめ、以下のとおり日本政府に提言する。

一．サイバー攻撃により広く国民の生命、身体及び財産が脅かされるような事態が想定される際の「サイバー緊急警報」の発令にかかる制度を整備せよ

二．サイバー緊急警報が発令された場合、政府は、企業によるシステム停止やネットワーク遮断などの予防的措置についての要請を含め、国民の安全確保に全力を挙げよ

三．サイバー緊急警報の発令にあたっては、総理を含む官邸からの情報発信も実施し、上記措置の必要性及びそれにより生じる国民生活への影響について国民に十分に説明せよ

四．緊急かつ重大な脆弱性への対応を含め、国民参加型の定期的な模擬訓練を検討せよ

以上