資料８

令和７年５月12日

サイバーセキュリティ戦略本部への提言

日本電信電話株式会社　松原実穂子

日本を取り巻く安全保障環境は厳しさを増し、サイバー脅威環境もまた悪化している。ボルト・タイフーンやソルト・タイフーンは、現時点で日本国内の重要インフラ企業において見つかっていないものの、攻撃者の目的から鑑みるに、日本が狙われてもおかしくない。また、昨年末から日本の基幹インフラに対して続いた大規模DDoS攻撃は、DDoS攻撃だけでも十分に経済安全保障を脅かせると証明した。加えて、日本企業に対するランサムウェア攻撃を見ても、海外の子会社から侵入される事案や、サービス提供が中断され、顧客組織でも業務の遅延が発生する事案が昨年以降目立つ。

こうした脅威認識のもと、下記の２点について提言する。

- 新司令塔から重要インフラ企業への防御に役立つ脅威インテリジェンスの提供

今後、能動的サイバー防御法が成立すれば、日本政府に対し、今まで以上に重要インフラ企業からインシデント情報など知見が集約されることになる。新司令塔は、その知見と政府でしか得られない情報をまとめ、重要インフラ企業の経営と運用現場においてサイバー防御と被害拡大防止に役立つ脅威インテリジェンスを速やかに提供すべきである。セキュリティ・クリアランス保持者への機密情報提供と、非保持者へのサニタイズ情報の提供の二通りが考えられる。このインテリジェンスは、脅威ハンティングにも役立つはずだ。

また、官民間の双方向の情報共有が運用現場に過度な負担をかけず、かつ被害最小化に役立つようにするため、定期的・継続的に官民間で意見交換し、過去の教訓を活かせる機会をもっていただきたい。

- 実践的な官民合同のサイバー演習の実施

NISC主催の全分野一斉演習やNATOサイバー防衛センター主催のロックド・シールズ演習は、能動的サイバー防御法が成立すれば、日本のインシデント対応総合力を一層強化する上で役立てられるはずのものである。こちらについても、参加した官民関係者の間で反省点と教訓について洗い出す機会を事後に設けていただきたい。

以　上