

3 月の韓国政府機関等に対するサイバー攻撃への対応について

1 事案の概要

平成 23 年 3 月 3 日から 5 日にかけて、韓国政府機関等 40 のウェブサーバに対し、サイバー攻撃（DDoS 攻撃）が行われ、一部のウェブサイトの閲覧に支障が生じたもの。

韓国当局は、所要の捜査の結果、平成 21 年 7 月に発生した米韓サイバー攻撃事案と同一犯（北朝鮮）による犯行と発表した。

（注）DDoS 攻撃：攻撃目標のサーバに対して、複数のサーバやパソコンから同時に大量のデータを送り付け、その機能を停止させる電子的攻撃。

2 韓国当局と連携した警察の対応

(1) 攻撃元の捜査

攻撃指令サーバとみられる 4 つの IP アドレスについて、我が国所在のものとして、韓国当局から ICPO を通じ、捜査協力要請があったもの。

警察が所要の捜査を行った結果、3 台のコンピュータは攻撃の踏み台となっていた可能性が高いことが判明。うち 2 台からは、外部の IP アドレスと不審な通信を行う不正プログラムが検出された。

踏み台となっていたコンピュータのうち 1 台は、個人が家庭用に使用していたパーソナル・コンピュータが、何者かに攻撃指令サーバとして仕立てられ、サイバー攻撃を敢行していたとみられる。

(2) 韓国当局との協議

韓国当局との協議の結果、国境を越えて敢行されるサイバー攻撃への対応については、海外の捜査機関との連携が不可欠であり、攻撃者の追及に係る緊密な捜査協力等、連携を強化することで合意。

3 情報セキュリティ対策に係る広報啓発活動の推進

本件では、事業者等がサーバとして使用しているコンピュータだけでなく、家庭用のパーソナル・コンピュータも攻撃者に利用されていたことから、企業・業界団体等のみならず、個人利用者に対しても、本事案を踏まえた注意喚起を行うとともに、ウイルス対策ソフトの適切な導入等の情報セキュリティ対策に関する広報啓発活動を推進。