

平成 23 年 7 月の警察庁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 7 月 10 日から 11 日にかけて、警察庁ウェブサーバに対し、複数の攻撃ツールを使用したとみられるサイバー攻撃（DDoS 攻撃）が行われ、警察庁のウェブサイトの閲覧に支障が生じたもの。

分析の結果、中国の大手検索サイトの掲示板（以下「本件掲示板」という。）において、7 月 4 日の尖閣諸島における航空自衛隊の中国偵察機に対する緊急発進のニュース内容とともに、攻撃ツールを使用して日本にサイバー攻撃を呼び掛ける記述があり、攻撃目標として警察庁ウェブサイトに掲示されていたことが判明。

（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 警察の対応

(1) 攻撃元の捜査等

当該期間における警察庁ウェブサーバに対するアクセスを分析した結果、攻撃元である可能性が高い IP アドレスを抽出。

これらは、全て海外所在（そのうち約 9 割が中国所在）のものであったことから、ICPO を通じ、海外の捜査機関に対し、捜査協力要請を実施するとともに、再発防止措置を依頼。

攻撃ツールを使用したとみられるなど、攻撃元と疑われるような発信元は、国内には所在しなかった。

(2) 関係機関との連携

本件掲示板の監視を続けた結果、攻撃者が攻撃目標を警察庁から他の省庁に変更していることが判明したため、当該省庁及び内閣官房に対し、サイバー攻撃の呼び掛けに係る情報を提供するなど、関係機関との連携を図った。