

## 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 22 年 9 月、「中国红客联盟」と称する者が、尖閣諸島の中国領有を主張する民間団体「中国民間保釣联合会」のウェブサイト上で、我が国に対するサイバー攻撃を行うよう呼び掛け。

同月 16 日から 18 日にかけて、3 次にわたり、サイバー攻撃（複数種類の D D o S 攻撃（注））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。

（注）D D o S 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のウェブサーバに対する約 2 万に及ぶ発信元を分析し、継続的に頻度の高いアクセスを行った発信元については、サイバー攻撃である可能性が高いことから、I P 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、I C P O 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。

#### (2) 国内における再発防止措置

国内の発信元については、全て所要の捜査をした結果、攻撃の踏み台となっていたコンピュータが我が国に所在することが判明したことから、セキュリティ対策の強化に関する指導等の再発防止措置を実施。

#### (3) 重要インフラ事業者等との情報共有

当該事案においては、中央省庁だけでなく、重要インフラ事業者等も攻撃対象として名指しされたことなどを踏まえ、サイバーテロ対策協議会（43 都道府県で設置済）等の枠組みを通じ、全国の都道府県警察に対し、重要インフラ事業者等と情報共有を図るよう指示。