#### 総務省 「電気通信事業者におけるフロー情報分析によるC&Cサーバ検知及び共有に関する調査」

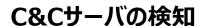
本調査では、「未知のC&Cサーバ検知」と「C&Cサーバリストの有効性評価のためのボットネットの調査」を 目的に、フロー情報から特定したC&Cサーバリストを共有し、電気通信事業者の情報と照合します。本調査を 通じて、ISPによるC&Cサーバの早期発見によるDDoS攻撃等の未然防止・被害極小化の実現を目指します。

### 分析電気通信事業者

- フロー情報の収集・蓄積・分 c&cサーバ 析によりC&Cサーバである可 能性が高い機器の検知
- C&Cサーバである可能性が高 い機器のリスト作成

共有

C&Cサーバ検知手法の改善



# C&Cサーバ調査プロジェクト業務推進G

- 分析電気通信事業者が作成した C&Cサーバリストの精査と詳細分析
- 信頼性の高いC&Cサーバリストの作成



- ボットネット可視化による全体像観測
- ボットネット影響度分析

C&Cサーバリストの分析・評価

## C&Cサーバリスト利活用共有-WG

- C&Cサーバリストの共有検討
- C&Cサーバリストの利活用検討
- ボットネット対策の検討



#### ICT-ISAC事務局

- C&Cサーバリストの共有
- 結果の取りまとめ



### 共有電気通信事業者

- C&Cサーバリストとフロー情報の照合
- C&Cサーバリスト有効性評価

C&Cサーバリストの共有と利活用検討





C&Cサーバ

**ICT-ISAC JAPAN** 

分析結果