

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

The diagram illustrates the workflow of the C&C Server Investigation Project Business Promotion G. It is organized into three main stages from left to right:

- Stage 1: C&Cサーバの検知 (C&C Server Detection)**
 - 分析電気通信事業者 (Analytical Telecommunications Business Operator)**
 - フロー情報の収集・蓄積・分析によりC&Cサーバである可能性が高い機器の検知 (Detection of devices with high possibility of being C&C servers through collection, accumulation, and analysis of flow information)
 - C&Cサーバである可能性が高い機器のリスト作成 (Creation of a list of devices with high possibility of being C&C servers)
 - C&Cサーバ検知手法の改善 (Improvement of C&C server detection methods)
- Stage 2: C&Cサーバリストの分析・評価 (Analysis and Evaluation of C&C Server List)**
 - C&Cサーバ調査プロジェクト業務推進G (C&C Server Investigation Project Business Promotion 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 (Refinement and detailed analysis of the C&C server list created by the analytical telecommunications business operator)
 - 信頼性の高いC&Cサーバリストの作成 (Creation of a highly reliable C&C server list)
 - ボットネット可視化による全体像観測 (Overall observation of botnet visualization)
 - ボットネット影響度分析 (Botnet impact analysis)
- Stage 3: C&Cサーバリストの共有と利活用検討 (Sharing and Utilization of C&C Server List)**
 - C&Cサーバリスト利活用共有-WG (C&C Server List Utilization Sharing-WG)**
 - C&Cサーバリストの共有検討 (Discussion on sharing the C&C server list)
 - C&Cサーバリストの利活用検討 (Discussion on utilization of the C&C server list)
 - ボットネット対策の検討 (Discussion on botnet countermeasures)
 - ICT-ISAC事務局 (ICT-ISAC Secretariat)**
 - C&Cサーバリストの共有 (Sharing of the C&C server list)
 - 結果の取りまとめ (Summary of results)
 - 共有電気通信事業者 (Shared Telecommunications Business Operator)**
 - C&Cサーバリストとフロー情報の照合 (Cross-referencing the C&C server list and flow information)
 - C&Cサーバリスト有効性評価 (Evaluation of the effectiveness of the C&C server list)

Flow and Data Exchange:

- A red arrow labeled **共有** (Sharing) points from the list creation in Stage 1 to the investigation group in Stage 2.
- A blue arrow labeled **共有** (Sharing) points from the investigation group in Stage 2 back to the detection stage in Stage 1.
- A blue arrow labeled **共有** (Sharing) points from the investigation group in Stage 2 to the sharing WG in Stage 3.
- A blue arrow labeled **共有** (Sharing) points from the sharing WG in Stage 3 back to the investigation group in Stage 2.
- A blue arrow labeled **共有** (Sharing) points from the sharing WG in Stage 3 back to the detection stage in Stage 1.