電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会
ワーキンググループ（第 10 回）議事要旨

１．日時

令和３年６月 29 日（火）17:00～19:00

２．場所

Web 開催

３．出席者

（１） 構成員

宍戸主査、森主査代理、井上構成員、木村孝構成員、齋藤構成員、鎮目構成員、丸橋構成員、吉岡構成員

（２） 総務省

今川電気通信事業部長、藤野官房審議官、小川消費者行政第二課長、中溝サイバーセキュリティ統括官室参事官、高田消費者行政第二課企画官、伊藤消費者行政第二課課長補佐、廣瀬サイバーセキュリティ統括官室参事官補佐

（３） その他（主査により参加が認められた者）

則武　智　一般社団法人 ICT-ISAC　事務局次長

４．議事模様

（１） 開催要綱（案）について

事務局から、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会ワーキンググループ　開催要綱（案）」について説明が行われ、案のとおり了承された。

（２） 「サイバー攻撃に関する最近の動向」及び「第四次とりまとめ（案）」について

事務局から、「サイバー攻撃に関する最近の動向」及び「第四次とり

まとめ（案）」について説明が行われた。

主なやり取りは以下のとおり。

・ 今回の対策として取り上げる C&C サーバの検知について、具体的にどのような方法で検知することを想定しているのか、それによってどの程度の精度が得られる想定であるのか、事例や評価検証はあるのか等の説明が必要。
・ 仮に、今回の対策が試行的な効果検証を実施するということになると、手段の相当性があるというのは難しいのではないか。
・ フロー情報自体は、設備投資の判断やネットワーク運用のため、常時分析を日常的に行っているもの。一方で、その中から C&C サーバの通信を見つけることは難しい行為であり、また、フロー情報はサンプリング情報であるため、実際の通信ログより不確実な情報をもとにするという点でも難しいのではないか。さらに、C&C サーバの情報が見つかったとして、それが実際にどういうマルウェアや攻撃と紐付いているのか分からなければ次の一手ができないことが懸念される。
・ プロバイダの中で閉じた対策ではなく、先を見据えた意見としては、研究者やセキュリティベンダーの力を借りられることが必要。
・ C&C サーバの検知が確実なものではなく試行的なものだとすると、今回の措置が電気通信の安定的かつ円滑な提供の維持という究極の目的にどの程度資するのかということの説得的な説明が必要。
・ 欧州やあるいは米国等で C&C サーバ等のテイクダウンが非常に大きな成果を上げている中で、日本も追随できるよう、研究機関に対する情報提供を可能とすること等の整理も含め、対策を検討することが必要。
・ C&C サーバを放っておくと電気通信役務の提供に重篤な支障が生じるという整理をしているが、ネットワークへのリスクについて根拠となる材料が足りないのではないか。
・ 例えば、オリパラのサーバに対する DDoS 攻撃等により、特定のサーバへの支障というのは十分起こり得るので、それをもって ISP による電気通信役務の提供が重篤な支障を生じ得るといえることはできないか。

・ フロー情報の集合的分析の結果、検知される C&C サーバである可能性が高い機器の IP アドレス及びポート番号について、通信の秘密に該当しないとしてよいか、考え方について議論の余地があるのではないか。
・ 論点を整理すると、次の４つである。
  ① フロー情報の収集・蓄積、解析、C&C サーバの検知、という一連の行為について分解して検討することが必要。（単に試行的な対策であれば、C&C サーバ検知との相関性がなく、正当業務行為としての整理が難しくなってしまう。）
  ② 目的の正当性に関し、ネットワーク全体に問題が起きることで、個々の ISP の電気通信役務の安定的かつ円滑な提供の確保に重篤な支障が生じる事態になっているといえるか、丁寧な立論が必要。
  ③ 手段の相当性に関し、具体的な行為との関係で、それが手段として相当かを整理することが必要。必要最小限というために、具体的にどの範囲でデータを抽出して分析する等、一定の制約が必要かどうかについても整理が必要。
  ④ フロー情報を収集・分析して、最終的に外に提供されるところの C&C サーバである可能性が高い機器の IP アドレスおよびポート番号の情報は、通信の秘密との関係で、特定の個々の通信とは関係のないものになっているのかどうか、整理が必要。
・ 上記③に関し、ネットワークの個々の ISP の電気通信役務の安定的な提供のためにできる手段が、侵害が現実化した段階だと限られているので、多少法益侵害の点で問題があっても正当化される、という方向の議論もあり得るのではないか。
・ サイバー攻撃の複雑化・巧妙化は右側上がりで進んでいく一方であり、本筋からすると、将来的には、法律を整備して、時流に応じたサイバー攻撃対策を行えるようにすることが必要ではないか。

（３） 閉会