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
（第７回）議事要旨

１．日時

令和３年 10 月１日（金）15:00～17:00

２．場所

Web 開催

３．出席者

（１） 構成員

鎮目座長、宍戸座長代理、木村孝構成員、木村たま代構成員、小山構成員、中尾構成員、藤本構成員、森構成員、吉岡構成員

（２） 総務省

二宮総合通信基盤局長、巻口サイバーセキュリティ統括官、北林電気通信事業部長、山内大臣官房審議官、林総務課長、木村事業政策課長、小川消費者行政第二課長、梅村サイバーセキュリティ統括官室参事官、海野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、安藤サイバーセキュリティ統括官室企画官、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（座長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．議事要旨

（１） 開会

開会にあたり、二宮総合通信基盤局長及び巻口サイバーセキュリティ統括官から挨拶が行われた。

（２） 議事

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　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「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第四次とりまとめ（案）」について

事務局から、「C&C サーバ検知のためのフロー情報分析について」及び「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第四次とりまとめ（案）」について説明が行われた。

③　自由討議

事務局からの説明を踏まえ、自由討議が行われた。

主なやり取りは以下のとおり。

・ 今回の取組でいう「フロー情報分析サーバ」とは、各 ISP が、これまでフロー情報分析・収集を行っているサーバに、C&C サーバ検知の分析ロジックを追加したものという理解でよいか。

⇒（事務局）そのような理解でよい。

・ フロー情報分析の目的について、未知の C&C サーバを見つけるという目的も重要だが、既知の C&C サーバの確認という目的も重要になるのではないか。

⇒（事務局）結果的には両方見つけることができるという理解でよい。

・ C&C サーバの検知の精度については、ハニーポット等別の分析手法を用いた答え合わせを行う必要があると思う。また、各 ISP が検知した情報は、その信憑性によって本当に使えるかどうかが決まると思う。

⇒（事務局）検知の精度を上げていくという取組は大変重要であり、今回のとりまとめが認められれば今後その点も検証していきたいと考えている。

・ 今後、ISP の中で C&C サーバを検知した後にそれをどう活用するのかについては、ISP の自主的な検討に委ねるということか。

⇒（事務局）ISP の中での検証も必要であるし、また ICT-ISAC 等に情報を共有して外部の知見をフィードバックしてもらうなど、コミュニティの中で検証していくということも重要と考えている。

・ C&C サーバの通信の遮断について、実際の事例から、遮断要請元の情報のみに基づき機械的にやるというより、関係者の知見を重ねて遮断するという段取りが必要だと思った。ICT-ISAC は認定協会という役割もあるため、中心的な役割を果たしつつ、NICT などの研究機関とも協力することによって、答え合わせの精度を高めていくということをしていきたい。
・ 今後取組を継続していくにあたっては、最初に条件等（サンプリングレートなど）を設定したときに考慮された事項の引継ぎが組織的に行われることが重要である。
・ 上述の「最初に条件等を設定したときに考慮された事項の引継ぎ」に配慮した上で、技術や背景の変化に対応した運用をお願いしたい。
・ ハニーポットやマルウェア解析では末端を検知できるが上位にある C&C サーバやボットマスターは検知できないので、これらまで検知できるフロー情報分析という手法には独自の意義がある。ハニーポット等の別の手法とうまく補完・連携しあうことが重要である。
・ フロー情報の分析ロジックについて研究機関等と情報共有できるとさらに検知の精度が上がっていくのではないか。
・ とりまとめ（案）について、修正意見を述べるものではないが、次の４点を意見として述べておきたい。

ア　フロー情報はあくまで通信の秘密に該当するものであって、今回の取りまとめ案は、C&C サーバの検知を目的としてフロー情報を分析することを適法化しているものである。

イ　既に取得済みのフロー情報を利用する点で通信の秘密への新たな侵襲がないこと、及び、サンプリングは１万分の１程度のレートで無作為に行われていることが、手段の相当性を基礎づける事実に該当する。

ウ　C&C サーバに関するリストについて、完全に通信の秘密と切り離されているわけではない。本とりまとめ案の「通信の秘密の保護規定に直ちに抵触するとまではいえないと考えられる。」旨の記述（13 頁）

は、無理に通信の秘密との関係を整理しない趣旨であると理解。

エ　サイバーセキュリティ対策について、今回のような正当業務行為で整理することは限界があるため、電気通信事業者によるサイバーセキュリティ対策に関する法律を作って法令行為として通信の秘密の侵害に関して違法性阻却をするという方向を目指してほしい。

⇒（事務局）今回はあくまでも一つの ISP の中で分析するということになっているが、ISP 間の連携・協力の可能性も見据えつつ、必要な制度的検討をしてまいりたい。

・ 利用者に対する適切な情報提供が重要。情報の取扱いを透明化して利用者に説明することで、事業者と利用者との信頼関係につながるのではないか。

④　議論の取りまとめ

「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第四次とりまとめ（案）」についての修正意見はなかった。

同とりまとめ（案）については、意見募集手続を実施した後で最終的なとりまとめとして公表することについて合意され、提出された意見の採否については鎮目座長に一任された。

（３）　閉会

以上