別紙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

第四次とりまとめの概要

令和３年11月
事　　務　　局

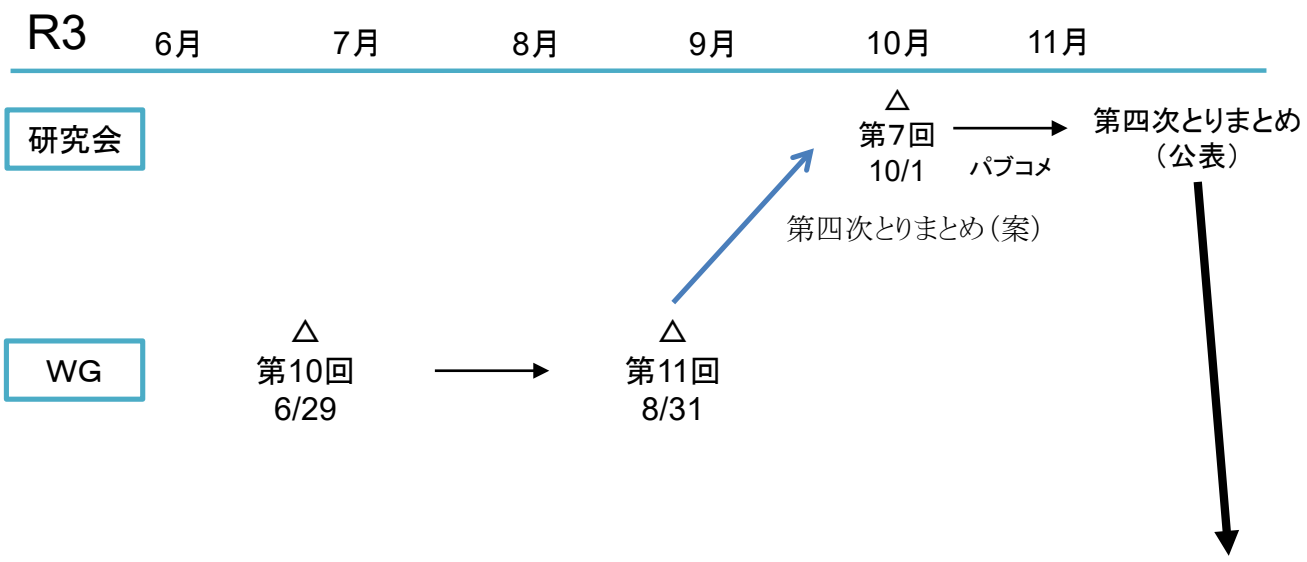
「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」 概要

○ サイバー攻撃が巧妙化・複雑化する中で、電気通信事業者が、通信の秘密等に配慮しつつ、新たな対策や取組を講じていくことが可能となるように、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ついて検討を行うことを目的として開催している。

○ 同研究会における議論を取りまとめた結果については、第一次とりまとめが平成26年４月に、第二次とりまとめが平成27年９月に、第三次とりまとめが平成30年９月に公表されている。

○ 第四次とりまとめについては、令和3年10月１日の同研究会会合で案をとりまとめ、パブコメを経た上で、同年11月公表。

スケジュール



「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」(事業者団体作成)に反映（見込み）

検討事項

（１）平時におけるフロー情報※1の収集・蓄積・分析によるC&Cサーバ※2である可能性が高い機器の検知について

（２）フロー情報を収集・蓄積・分析して検知したC&Cサーバに関する情報についての共有について

（３）その他

※1 IPアドレス及びポート番号等のヘッダ情報並びにルータでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報

※2 Command and Control サーバの略であり、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者から指令を送り、制御を行うサーバコンピュータ

（参考）「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」構成員

構成員

＜本会合＞

（座長）	鎮目　征樹	学習院大学法学部　教授
（座長代理）	宍戸　常寿	東京大学大学院法学政治学研究科　教授
	木村　孝	一般社団法人日本インターネットプロバイダー協会　事務局長
	木村　たま代	主婦連合会　事務局長
	小山　覚	一般社団法人ICT-ISAC　ステアリング・コミッティ　運営委員長
	中尾　康二	国立研究開発法人情報通信研究機構　サイバーセキュリティ研究所　主管研究員
	藤本　正代	情報セキュリティ大学院大学　教授
	森　亮二	英知法律事務所　弁護士
	吉岡　克成	横浜国立大学大学院環境情報研究院／先端科学高等研究院　准教授

＜WG＞

（主査）	宍戸　常寿	東京大学大学院法学政治学研究科　教授
（主査代理）	森　亮二	英知法律事務所　弁護士
	井上　大介	国立研究開発法人情報通信研究機構　サイバーセキュリティ研究所 サイバーセキュリティネクサス　ネクサス長
	木村　孝	一般社団法人日本インターネットプロバイダー協会　事務局長
	小山　覚	一般社団法人ICT-ISAC　ステアリング・コミッティ　運営委員長
	齋藤　衛	株式会社インターネットイニシアティブ　セキュリティ本部長
	鎮目　征樹	学習院大学法学部　教授
	丸橋　透	明治大学法学部　教授
	吉岡　克成	横浜国立大学大学院環境情報研究院／先端科学高等研究院　准教授

第四次とりまとめのポイント

ポイント

（1） 平時におけるフロー情報の収集・蓄積・分析によるC&Cサーバである可能性が高い機器の検知について

→ **正当業務行為として許容される**

〈考え方〉

ISP※が平時において、自らのネットワーク内のルータ等の電気通信設備を通過するユーザの通信トラフィックに係るデータのうち、IP アドレス等のフロー情報を収集・蓄積・分析して未知のC&Cサーバを検知することは、必要最小限の範囲でフロー情報を収集・蓄積し、そのフロー情報をC&Cサーバ検知以外の用途で利用しない場合に限り、正当業務行為として許容される。

（2） フロー情報を収集・蓄積・分析して検知したC&Cサーバに関する情報についての共有について

→ **通信の秘密の保護規定に抵触しない**

〈考え方〉

一のISPが、（1）の取組により得られたC&Cサーバに関する情報（IPアドレス、ポート番号）を取りまとめてリスト化したものを、サイバーセキュリティ対策を行うために適切な事業者団体等に提供することは、通信の秘密の保護規定に抵触しない。

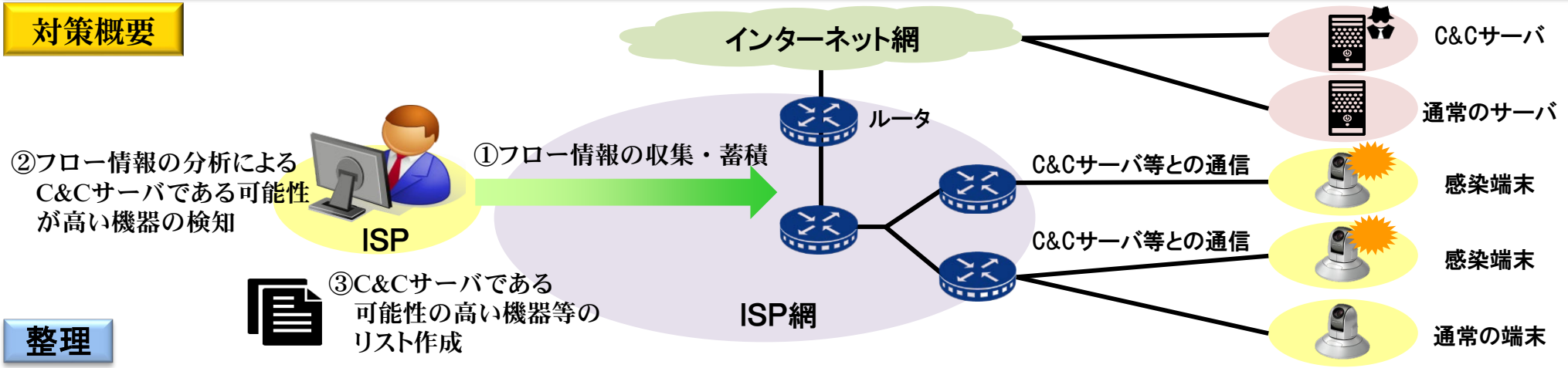
※ Internet Service Provider の略であり、インターネット接続サービスを提供している事業者のこと

検討課題（１）平時におけるフロー情報の収集・蓄積・分析によるC&Cサーバである可能性が高い機器の検知

論点

ISPがサイバー攻撃に予防的に対処するため、平時から、ISPが、自らのネットワーク内の通信トラフィックに係るデータを収集・蓄積・分析し、C&Cサーバである可能性が高い機器の検知を行うことが考えられる。具体的には、現状多くのISPにおいて、自らのネットワーク内のルータ等の電気通信設備を通過するユーザの通信トラフィックに係るデータのうち、IPアドレス及びポート番号等の情報（フロー情報）を、通信の傾向把握のために収集・活用しているところであるが、これを分析して未知のC&Cサーバの検知を行うことが考えられる。このような取組は、通信の秘密との関係上どのように整理が可能か。

対策概要



整理

以下のことから、本件対策は、正当業務行為として違法性が阻却される。

「目的の正当性」：本件対策は、DDoS攻撃等のC&Cサーバを起点とするサイバー攻撃が発生する前から未知のC&Cサーバ等を検知し、その検知した情報をもとに、各ISPにおいて適切な対処ができるようにすることにより、自己の電気通信役務の提供への重篤な支障の発生を未然に防止し、または、その被害の拡大を最小限に抑え、電気通信役務の円滑な提供を確保するための措置であり、目的の正当性を認めることができる。

「行為の必要性」：サイバー攻撃の複雑化・巧妙化が進んで攻撃の頻度は高まり、ISPの提供する電気通信ネットワークに対するC&Cサーバを起点としたサイバー攻撃がいつ行われてもおかしくない状態にさらされている等、現在の電気通信ネットワークを取り巻く状況においては、行為の必要性が認められる。

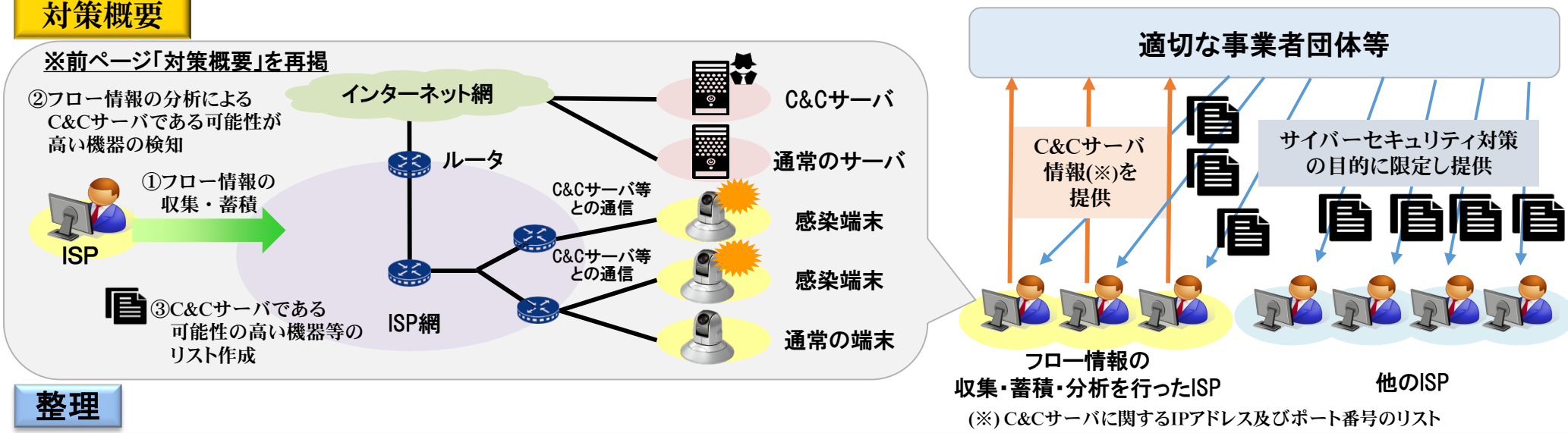
「手段の相当性」：必要最小限の範囲でフロー情報を収集・蓄積し、そのフロー情報をC&Cサーバ検知以外の用途で利用しない場合には、手段の相当性が認められる。

検討課題(２)フロー情報を収集・蓄積・分析して検知したC&Cサーバに関する情報についての共有

論点

各ISPがサイバー攻撃に対処できるようにする観点から、一のISPが自らの電気通信ネットワーク内のフロー情報の収集・蓄積・分析によって検知したC&Cサーバに関する情報（IPアドレス、ポート番号）を、適切な事業者団体等に提供することが考えられる。このような取組は、通信の秘密との関係上どのように整理が可能か。

対策概要



整理

本件において対象とされるC&Cサーバに関する情報は、必要最小限のフロー情報について、C&Cサーバを検知する目的のみのために集合的に分析した結果として得られたC&Cサーバに関するIPアドレス及びポート番号を取りまとめてリスト化したものである。すなわち、個別の通信と切り離され、個々の通信がいつ誰に対して行われたかといった個々の通信の構成要素を明らかにすることにつながらないものである。

したがって、このように、C&Cサーバに関するIPアドレス及びポート番号のリストの情報のみを、サイバーセキュリティ対策を行うために必要最小限の情報として、適切な事業者団体等に提供することは、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 。