「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）に対する意見募集の結果について

別紙３

1　概要

これまでの議論の内容をまとめた第四次とりまとめ（案）について、総務省ホームページ及び電子政府の総合窓口を通じ幅広く国民より意見募集を実施。

2　意見募集期間

令和3年10月6日（水）～11月4日（木）

3　意見募集の結果

7件の意見提出

4　意見提出者（計7者）

- 株式会社ラック
- パロアルトネットワークス株式会社
- 個人（5件）

※意見提出数は、意見提出者数としています。

「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)」に対して提出された御意見
【意見募集期間:令和3年 10 月6日(水)～同 11 月4日(木)】

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
1	p. 11	2	2	（2）	第２章第２節（２）の丸２において、「５Gの進展によりIoT機器の利用が増加するに伴って(中略)調査対象となるIoT機器のIPアドレスが膨大になる」との記載があるが、調査対象の機器となるIPアドレスの増加に対し、直接的な影響を与える「IPv6対応の普及も併記してはどうか。 ５Gに関する記載にも異論はないが、IPv6に対応した回線やサービスが多く提供され、様々なIoT機器がグローバルなIPアドレスを有するようになったことも、重要な要因である。	調査対象となるIoT機器のIPアドレスの膨大化は、IoT機器の増加が主たる原因と考えられるため、原案のとおりとすることが適当と考えます。	個人①
2				とりまとめ（案）全体	この２点についての考え方に異論はありませんが、これ以外にも、サイバー攻撃の防御に資するような対策はどんどん講じてください。	本とりまとめ（案）への賛同の御意見として承ります。 いただいたご意見については、今後検討を進めていく上での参考とさせていただきます。	個人②
3				とりまとめ（案）全体	この度、IoT 機器の普及・利用の急速な拡大や5G サービスの開始など、新たな技術やビジネスが進展する中、IoT 機器を悪用したサイバー攻撃のリスクなどに対応した「第四次とりまとめ(案)」が提示されたことは、誠に時期を得たものであります。今回の取りまとめにより、C&Cサーバーの検知と関係者による情報共有が促進され、サイバーセキュリティ対策が一層進展いたしますので、本案に賛同いたします。	本とりまとめ（案）への賛同の御意見として承ります。	株式会社ラック

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
4	p.9	2	2	（１）	本検討は、事業者として過度な負担をすることなく効率的な通信サービスを提供することが可能となるため大変歓迎すべき内容だと考えます。	本とりまとめ（案）への賛同の御意見として承ります。	パロアルトネットワークス株式会社
5	p.12	2	2	（２）	「利用者に対し、サイバーセキュリティ対策に活用する目的で必要最小限の範囲で行っていることについて、わかりやすく周知することが適当」については、同意できます。また、ご指摘の通りこれらの対策について利用者に理解してもらうことが大事だと思います。その上で、「わかりやすく周知」という具体的な方法ですが、Webも含めカタログや販促資料等に当該機能や対策を紹介することでよいか、具体例を示していただければ、事業者として実務的に助かります。	電気通信事業における個人情報保護に関するガイドラインの解説（平成29年９月（平成31年２月更新））2-12「公表」における事例などを参考に、合理的かつ適切な方法で周知を行うことが適当と考えられます。	パロアルトネットワークス株式会社
6	p.13	2	3	（１）	高度なサイバー攻撃を早期に察知し、未然防止あるいは影響範囲を限定/特定するためには単純な「IPアドレス、ポート番号」のみの情報共有ではなく、例えば、IoC(Indicator of Compromise)フォーマットの標準仕様「STIX(Structured Threat Information eXpression)」に基づいた情報共有を検討するべきと考えます。 脅威は海外発であることが多い為、提供先の事業者団体については海外関係機関も念頭におくべきであり、その意味でもグローバルの標準仕様であるSTIXに基づいた情報共有は重要ではないでしょうか。	本とりまとめ（案）では、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必要最小限の情報に限って C&C サーバに関する情報を共有することとしており、STIX 形式で共有される情報のように、攻撃手口や対処方法なども含む網羅的な情報を共有するものではないことから、原案のとおりとすることが適当と考えます。	パロアルトネットワークス株式会社

番号	項目 頁	章	節	該当部分	提出された御意見	御意見に対する考え方	意見提出者
7	p.13	2	3	（１）	また、一度C&Cサーバとして検知したIPアドレスについては、一定期間後IPアドレスが変更される可能性もあるため、定期的にメンテナンスすることも併せて実施すべきと考えます。	本とりまとめ（案）で示した取組が電気通信事業者により継続的に実施される場合においては、C&Cサーバとして検知した IP アドレスについて、定期的なメンテナンスが行われることが適当と考えます。	パロアルトネットワークス株式会社
8	p.13	2	3	（１）	最後に、今後将来的な対策の強化を行う為、IPアドレスベースの検知に加えて、URLやDNS情報を収集対象とする事も影響に合わせて検討すべきと考えます。 通信の秘密の保護規定に抵触しないよう、サービス提供時にユーザへ了承を頂く前提において、そのようなセキュリティ対策も求められる状況が将来的には想定されます。	御指摘のセキュリティ対策は、ユーザからの有効な同意を取得した上であれば実施可能と考えます。 なお、ISP が、有効な同意に基づく通信遮断を目的として C&C サーバである可能性が高い機器の FQDN 等を検知する場合における有効な同意については、「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 第三次とりまとめ（以下「第三次とりまとめ」という。）」の第２章第４節において整理が行われています。	パロアルトネットワークス株式会社
9	p.14	2	3	（２）	「十分な信頼・協力関係が構築されているISP」に加え、十分な情報管理体制を構築しているISPであることも必要ではないかと思料いたします。	第２章第３節（２）にお示ししたとおり、「不当にサイバー攻撃者側に漏えいすることのないよう十分な信頼・協力関係が構築されている ISP」は十分な情報管理体制を構築している ISP であると考えます。	パロアルトネットワークス株式会社
10	p.14	2	3	（２）	また、上記コメントと同様、「わかりやすく周知」については、具体例を挙げていただきたく、ご検討のほどよろしくお願い申し上げます。	番号５の考え方のとおりです。	パロアルトネットワークス株式会社
11	p.4 p.6	1		（１）	「インターネット・サービス・プロバイダ（ISP）の提供する電気通信ネットワークに対するサイバー攻撃が複雑化・巧妙化」「こうした複雑化・巧妙化したサイバー攻撃が ISP の提供する電気通信ネットワークに対していつ行われてもおかしくない状態」 ほとんどのサイバー攻撃の対象は ISP が提供する電気通信ネットワークに接続された電子計算機であって、電	「電気通信ネットワーク」という表現は、ISP のネットワーク回線のみを指したものではなく、ISP のネットワーク機器やサーバなども含めたものとして使用しています。	個人③

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
					気通信ネットワーク自体ではないはずである。ISP が提供する電気通信ネットワーク自体にサイバー攻撃が行われた事例が存在するのであれば、示してほしい。		
12	p.5	1		図２	図 2 中「仮想通貨」 cryptocurrency の訳語としては「暗号通貨」がより適切ではないか。	資金決済に関する法律（平成二十一年法律第五十九号）の表現に倣い、「暗号資産」と修文させていただきます。	個人③
13	p.6	1		（２）	IP アドレス及びポート番号等のヘッダ情報並び(中略)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。 TCP SYN Flood 攻撃等の DDoS 攻撃では、送信元 IP アドレスを詐称することが可能であるため、分析に使用するには信頼度が低いのではないか。	フロー情報分析による C&C サーバの検知の精度については、参考資料「C&C サーバ検知のためのフロー情報分析」中「フロー情報分析による C2 サーバ検知の精度について」(p.22 下段）のとおり、一定の高い精度が示されていますが、今後、分析を実施する ISP において、更なる精度向上に努めることが適当と考えます。	個人③
14	p.6	1		（２）	既知の C&C サーバを教師データとして機械学習を行う手法 「既知の C&C サーバ」に関するデータは、どのように取得されたものか。このデータの品質は、機械学習の結果に影響を及ぼすと考えられるため、明確化が必要である。	例えば、「第三次とりまとめ」注釈４の「信頼性の高い C&C サーバに関するレピュテーションデータベースに含まれる情報のうち、C&C サーバであることの確度が高い機器に関する情報」が考えられます。	個人③
15	p.11	2	2	（２）	ISP によって収集・蓄積・分析されるフロー情報は、現状多くの ISP において通信の傾向把握のために既に収集・活用されているものであり この収集・活用は、通信当事者の有効な同意に基づくものではないのか。その場合は、正当業務行為の例としては適切ではない。	本とりまとめ（案）の第２章第１節（１）のとおり、通信のヘッダ情報を用いて経路制御を行う等の通信事業を維持、継続する上で必要な行為については正当業務行為として整理されています。	個人③

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
16	p.14	2	3	（２）	提供先の ISP においてサイバーセキュリティ対策に活用する目的に限定して用いること 具体的にどのような対策か明らかにしてほしい。たとえば、この情報を用いて通信遮断を行うことは、目的の範囲内か。	例えば、通信当事者の有効な同意に基づいて C&C サーバとの通信遮断を行うことは、提供された C&C サーバに関する情報の利用目的の範囲内と考えます。	個人③
17	p.22			参考資料 「C&C サーバ検知のためのフロー情報分析」 ２）フロー情報の分析・C2 サーバの検知①	端末等の感染対策を目的とする市販のソフトウェアのブラックリストにはこの初期接続先サーバが登録されており、 「ブラックリスト」の語は、黒人差別を連想させるとして海外にて使用を控える傾向があるがが、代替の用語を使用すべきではないのか。	「第三次とりまとめ」注釈４中の「レピュテーションデータベース」という表現に倣い、「レピュテーションリスト」と修文させていただきます。	個人③
18	p.22			参考資料 「C&C サーバ検知のためのフロー情報分析」 ２）フロー情報の分析・C2 サーバの検知①	端末等の感染対策を目的とする市販のソフトウェアのブラックリストにはこの初期接続先サーバが登録されており、C2 サーバが網羅されているとはいえないため、 C2 サーバが網羅されていない理由を詳しく検討すべきだ。例えば、当該ソフトウェアがウェブブラウザーに組み込む形で動作するためウェブブラウザーが直接アクセスしない C2 サーバを登録する必要はないため、などの理由ではないのか。	市販のレピュテーションリストで C&C サーバが網羅されていない理由については、御指摘の理由のほかにも、多くが海外での調査をもとに作成されていること等が想定されるため、本文において断定的に記載することは避けるべきと考えます。	個人③
19	p.22			参考資料 「C&C サーバ検知のためのフロー情報分析」 ２）フロー情報の分析・C2 サーバの検知②	フロー情報(既知 C2 サーバに関するもの) これをどうやって取得し、また既知の C2 サーバに関するものと判断すべきかを明記すべきだ。	番号 14 の考え方のとおりです。	個人③

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
20	p.3	序章			３ページの１９行目の半角の「5G」と、６ページの１行目の全角の「５Ｇ」とは、どちらかに字句を統一したほうがよい。	御指摘の修正意見を踏まえ、「５Ｇ」に修文させていただきます。	個人④
21	p.11	2	2	（２）	１０ページの脚注の５行目「はじめ」と、１１ページの１３行目「始め」とは、どちらかに字句を統一したほうがよい。	御指摘の修正意見を踏まえ、「はじめ」に修文させていただきます。	個人④
22	p.11	2	2	（２）	１１ページの脚注１２の冒頭「平成30年度」は「2018年度（平成30年度）」のほうがよい。他の箇所の例と同様に。	御指摘の修正意見を踏まえ、「2018年度（平成30年度）」に修文させていただきます。	個人④
23	p.3	序章		序章全体	＞序章 セキュリティについては大問題であるのに、ISP・VNE等においての、アクセスポイントにおけるSPI（ステートフルパケットインスペクション）技術を用いたフィルタが一般に利用可能になっていない事については非常に訝しむべきものであるし（これだけでTCPプロトコル（DNSoverTLS等以降は名前解決もTCPが主流として用いられるであろう。UDPの方が高速化には有用ではあろうが。）でのサイバーセキュリティ問題は激減が達成されると思われるのであるが。なぜどこも行わないのだ？）、またインターネット上を通信される電子メールのTLSでの送信・受信双方の保護（SMTPoverTLS、STARTTLSによる）が行われていないのも遺憾である（サイバーセキュリティ基本法、個人情報保護法、電気通信事業法等の法令解釈でそうなるべきはずであるし（そうでないなら、各種の個人情報が含まれる事になるような問い合わせや利用者情報ページのhttps化は何なのか、	本とりまとめ（案）は、既にISPが通信傾向の把握のために収集・活用しているヘッダ等のフロー情報をC&Cサーバを検知する目的で活用することについて検討するものであり、御指摘のSPI技術のようにヘッダ以外の情報を利用者の同意なく活用することについては、通信の秘密との関係で慎重な検討が必要であると考えます。	個人⑤

番号	項目 頁	章	節	該当部分	提出された御意見	御意見に対する考え方	意見提出者
					という話である。)、国総務省は法定の電気通信事業者くらいには電子メールのTLSでの保護が可能なように指導・義務化すべきである。行っていないのは懈怠の事態であろう。)。 特に、上で述べた前者の、ISP・VNE等においての、アクセスポイント的端点におけるSPI（ステートフルパケットインスペクション）技術を用いたフィルタリングについては、本件でも非常に有用なはずであるが、国、あるいは業界は、ISP・VNEのアクセスポイント的な端点において、通信契約者がSPIフィルタを適用出来るようにした方が良いのではないかと考える。 「難しい話」をするより、単純にその方が悪を一気に叩き潰すのに効果があると考えるが（何故しないのだ？)、検討を行っていただきたい。(善意はあるのか？と国民は政府等に訊いているのである。分かるであろうか？話が難しすぎるであろうか？）		
24	p.4	1		（１）	＞第１章　最近のサイバー攻撃に係る課題と対策例 ＞4頁 なお、DDoSについては、その発信者を偽る事も多いであろう事について意識しておくべきであると考える。 誤った措置を取ると、無実の人に反射的なDoSが成功してしまう事について、認識するようにされたい。(もちろん、上記の序章に対しての意見で述べたSPIフィルタはそんな事は無いのであるが。NICT等もISP等の端点におけるSPIフィルタの実施について意見してもらいたいものである。(しかし学者達は、簡単に行える害性の	いただいた御意見については、今後検討を進めていく上での参考とさせていただきます。	個人⑤

番号	項目 頁	章	節	該当部分	提出された御意見	御意見に対する考え方	意見提出者
					低い有効な対策より、副作用の強い手段を好むのであろうか？何のために？多くのITエンジニアが認めるであろう情報工学的に適切な害性の低い有効な対策より、危険を好むのであろうか？))		
25	p.5	1		（１）	＞5頁 SPIフィルタ（穴を開けれる必要があるが）を通信事業者が端点で適用する事で、大幅に減るのではないかと思われる。 より集中的な対処が可能な程度に減少するのではないか。 （ルータ等には非常に多数のSPIフィルタ（ああ、そうそう、Google社のアップストアなどにアクセスすると、TRACEROUTEを打ってくるようなので（何でインターネットでのグローバルIPが所在するISP等で止まっていないのだ、という疑問がある。)、引っかかるようですね。）で弾いた不適切なアクセスの記録があるのであるが、それらは膨大な数である。） （というか、その様な状況が分かるのであれば、それこそSPIフィルタを用いれるようにせよ、と言いたいのであるが。）	番号 23 の考え方のとおりです。	個人⑤
26	p.5	1		（２）	＞6頁 全てについて副作用がある事についてちゃんと認識されたい。 内部の機構（内部情報あるいは一般的知識）について想定しての、対策の回避・規制対象のなすりつけ、の様な事がされる事態の危険性については常に想定された	いただいた御意見については、今後検討を進めていく上での参考とさせていただきます。	個人⑤

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
					い。		
27	p.8	2	1	第１節全体	＞第２章　具体的検討 ＞第１節　通信の秘密の利用等に関する違法性阻却事由等について そんな事より、まずは、ISP・VNE等においてSPIフィルタの利用が行えるようにされたい。	番号 23 の考え方のとおりです。	個人⑤
28	p.9	2	2	第２節全体	＞第2節　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 そんな事より、まずは、ISP・VNE等においてSPIフィルタの利用が行えるようにされたい。 それをしていないのであれば、違法性阻却事由はそう高くないのではないかと考える。 まず、行うべき事をされたい。	番号 23 の考え方のとおりです。	個人⑤
29	p.12	2	3	第３節全体	＞第3節　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 情報の詐称や誤りが発生する危険性については常に想定されたい。 また、説明責任について負うようにされたい。	いただいた御意見については、今後検討を進めていく上での参考とさせていただきます。	個人⑤
30	p.15	3		第３章全体	＞第３章　おわりに まずは、ISP・VNE等においてSPIフィルタの利用が行えるようにされたい。	番号 23 の考え方のとおりです。	個人⑤