「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（案）」に対する意見募集の結果について

（別紙２）

1　概要

これまでの議論の内容をまとめた第三次とりまとめ（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

平成30年8月17日（金）～8月30日（木）

3　意見募集の結果

3者から8件の意見提出

4　意見提出者（計3者）

- 個人①
- 個人②
- 個人③

※個人意見のうち5件は、本意見募集の内容に関する御意見ではないため掲載を割愛しています。

「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 第三次とりまとめ(案)」に対して提出された御意見
【意見募集期間:平成 30 年8月 17 日(金)～同8月 30 日(月)】

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	提出意見を踏まえた案の修正の有無
	頁	章	節					
1				とりまとめ（案）全体	（１）「ISP（インターネット・サービス・プロバイダー)」が、IoT機器から「マルウェアー」に感染し、「DDoS攻撃」等を受けやすくなる事で、ISPの契約時での約款記載すると言う事の内容と考えますが、全く国家主権側が関与する事では無いと考えます。弱体化している「情報技術（IT)」の分野で、ISPのサーバでの運用管理を国家が介入する事では無いと私は考えます。 （２）具体的に言えば、ISPが管理しているサーバーに弱体的な要素が有り、サイバー攻撃に対応でき無いサーバーを運用管理している側に問題が有ります。ISPが管理しているサーバーを強体化をするのであれば、サーバー側のセキュリティー対策を入念に、検証していく事が先決です。	本とりまとめ（案）は、マルウェアに感染している可能性が高い端末の利用者に対する注意喚起等の課題について、電気通信事業者が通信の秘密等に配慮した適切な対応を行うことが可能となるよう、当該課題の解決の方向性について取りまとめたものであり、本とりまとめを参照することにより、電気通信事業者において引き続き自主的に適正なサイバー攻撃への対処が行われることが期待されるものです。 いただいた御意見については本研究会の検討対象ではございませんが、今後のサイバーセキュリティ対策の検討において参考にさせていただきます。	個人②	無
2	p.4	1	ー	（１）	＞4頁目 「C&Cサーバ」についてはそう一般的でない単語と思われるが、何の略なのか、どういうものなのかの説明を行われたい。用語の説明は必要である。 「テイクダウン」も平易・一般的な文言による表現とされたい。(不用意に横文字を使わないでいただきたい。)	御指摘の趣旨を踏まえ、「C&Cサーバ」、「テイクダウン」については、脚注にて用語の説明を追記します。 いただいた御意見については、技術の進歩や新たな対策などサイバー攻撃を取り巻く環境の変化に応じて、引き続き検討させていただきたいと思います。	個人③	有

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	提出意見を踏まえた案の修正の有無
	頁	章	節					
					連絡について、ISP経由のものが記されているが、例えばフレッツのNGN内通信においてなどはISPを介さない形での通信が行われるものであるので、次回からはその場合についての検討も求めたい。			
3	p.5	1	ー	（1）	＞5頁目 ISPが利用者に対しての警告を行う形での対応としている様子であるが、利用者の個人情報保護（電気通信において求められる事である。）の観点からすると、利用者への個別の対応よりも、C&Cサーバである可能性が高いホスト等についての掲示を行うのが適切ではないかと思われる。 利用者個人に対しての対応を行うのは、公平・公正・平等を乱す事もあるので（一部の不法な者はこれを狙っているのではないかと思われるが。電気通信事業において故意に不公正が発生している事態は多く観察されるものである。）、利用者への警告はその希望ある者以外については行わない運用とし、替わりに誰にでも公平な注意喚起サービスとなるものとして、C&Cサーバについての警告や掲示を行うのが適切ではないかと考える。（なお、利用者への警告メール等は、その様なC&Cサーバについての掲示がな	本とりまとめ（案）は、マルウェアに感染している可能性が高い端末の利用者に対する注意喚起等の課題について、電気通信事業者が通信の秘密等に配慮した適切な対応を行うことが可能となるよう、当該課題の解決の方向性について取りまとめたものです。 いただいた御意見については本研究会の検討対象ではございませんが、今後のサイバーセキュリティ対策の検討において参考にさせていただきます。	個人③	無

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	提出意見を踏まえた案の修正の有無
	頁	章	節					
					されている場合は公平・平等を乱さないので可であると考える。）			
4	p.8	1	ー	（４）	＞8頁目 この問題については、各種機器におけるSPIフィルターの搭載・有効化をより一般的に行うようにするとともに、ISP等においてもその様なサービスを提供する事が状況改善に有効ではないかと考える。 （ISPにおいて、世界に対して露になっているIPの各ポートがSPIフィルターにより守られる事になると、セキュリティ危機は大幅に減少するのではないかと思われるのである。） 各ISPがその様なサービスを導入するのはそこまで難しい事ではないと思われるのであるが、検討を行っていただきたく思う。	いただいた御意見については、技術の進歩や新たな対策などサイバー攻撃を取り巻く環境の変化に応じて、引き続き検討させていただきたいと思います。	個人③	無

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	提出意見を踏まえた案の修正の有無
	頁	章	節					
5	p.10	2	1	第２章第１節全体	＞10頁目 違法性棄却理由の濫用がなされないよう、適切に定めを行っていただきたい。（侵害の場合は、通常、必ず利用者に通知を行う等の定めが有効であると考える（侵害の事後でもよいのであるが、事実として発生しているのであれば通知が行われるべきであると考える。）。）	本とりまとめ（案）においては、有効な同意に基づく場合又は違法性阻却事由がある場合に限り、通信の秘密の侵害に該当しないこととして、マルウェアに感染している可能性が高い端末の利用者に対する注意喚起等の課題について整理しています。 本とりまとめ第２章第２節のマルウェアに感染している可能性が高い端末の利用者に対する注意喚起及び第５節のマルウェアに感染し得る脆弱性を有する端末の利用者に対する注意喚起については、利用者に対する適切な情報提供という観点から、違法性阻却事由のうち正当業務行為として注意喚起する場合であっても、注意喚起を行う旨についてあらかじめ契約約款等で明示しておくことが適当と整理しています。	個人③	無
6	p.12	2	2	第２章第２節全体	＞12頁目 上でも記したが、C&Cサーバの掲示等についてを行い、公正性を確保すべきであると考える。	番号３の考え方のとおりです。	個人③	無

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	提出意見を踏まえた案の修正の有無
	頁	章	節					
7				とりまとめ（案）全体	日本においてAndroid端末のアップデートがままならず現在でも中古端末の販売がver5付近のシステムかつメーカー独自の仕様のためアップデートが止まっているものが多くこの状態において中古端末を推奨する場合、Linuxカーネルが古いままかつアプリのアップデートのサポートが終了するため脆弱性を持ったまま使用するケースがあると思われる。貧困層、もしくはアップデートに興味がない老年層において放置されるケースが相次いだ場合、DOS攻撃の攻撃元になったり踏み台として使われる可能性が非常に高い。単体での攻撃であるならば威力はたかが知れているが複数端末による一斉攻撃が予想されます。この対策について端末の回転を早めるか恒久的なサポート体制が必要となります。これについてどうお考えなのかお聞きしたいところです。	いただいた御意見については本研究会の検討対象ではございませんが、今後のサイバーセキュリティ対策の検討において参考にさせていただきます。	個人①	無