円滑なインターネット利用環境の確保に関する検討会（第１回）議事要旨

１．日時

平成 29 年 10 月 26 日（木）10:00～11:30

２．場所

総務省 8 階第 1 特別会議室

３．出席者

（１）構成員

佐々木座長、佐伯座長代理、遠藤構成員、宍戸構成員、藤本構成員、森構成員、吉岡構成員

（２）総務省

野田総務大臣、坂井総務副大臣、鈴木総務審議官、武田官房総括審議官、渡辺総合通信基盤局長、谷脇政策統括官（情報セキュリティ担当）、古市電気通信事業部長、木村サイバーセキュリティ課長、柳島参事官（行政情報セキュリティ担当）、小笠原総合通信基盤局総務課長、竹村事業政策課長、荻原電気通信技術システム課長、大村消費者行政第二課長、岡本消費者行政第二課企画官、内藤消費者行政第二課企画官、松井安全・信頼性対策室企画官

（３）オブザーバー

木村 インターネットの安定的な運用に関する協議会主査、小山 ICT-ISAC ステアリング・コミッティ副運営委員長

４．議事模様

（１）総務大臣挨拶

野田総務大臣から冒頭挨拶が行われた。

（２）総務副大臣挨拶

坂井総務副大臣から冒頭挨拶が行われた。

（３）電気通信事業におけるサイバー攻撃等への対策の現状と課題

事務局から、サイバーセキュリティ等に係る現状と課題について説明が行われた。

（４） 自由討議

各構成員、オブザーバーから、電気通信事業者等によるインターネットの障害を防ぐための方策に関する課題と、その検討の方向性について意見陳述が行われ、その後、意見交換が行われた。

出された主な意見は、次のとおり。

○ 今後、C＆Cサーバ対策が大事になっていく。
○ C＆Cサーバ対策として、マルウェアに感染した機器が共通してアクセスする通信先から、C＆Cサーバを特定する方法があるが、この対策を行うにあたって、どのように通信の秘密に配慮していくか議論することが必要。
○ 資料１－３－９の「IoT 機器のセキュリティ対策基準の必要性」について、ネットワーク事業者は、脅威が重大で、機器が脆弱であることを前提として、通信の秘密を勘案しながら対策を講じることとなるが、そもそも機器の脆弱性が放置されないような取組が必要。
○ マルウェアに感染している大量のIoT機器によるサービスを妨害する大規模な攻撃が脅威となっていると言われているが、今後、それが様々な他の攻撃へ応用されることも想定されるため、攻撃を察知する仕組みを作ることが重要。
○ 被害の未然防止を図ることは重要であるが、予測不能なことが起こり得るので、次の事件や事故を防ぐためにどのようにリスク情報を伝達するかなど、二本立てで考えておくべき。
○ 近い将来、AI機能を持ったマルウェアが確実に出てくる。この対策を今から考えていくことが重要。
○ AIや自動化が進んでいる一方、守る側も攻める側も人を配置してコストをかけなければならない部分がある。今は攻撃側の方が自動化に上手く対応している状況。守る側も自動化できるのはどこまでで、どこからは人の判断が必要かという切り分けを行うことが必要。

これらを踏まえ、野田総務大臣、坂井総務副大臣からコメントが述べられた。

（５） その他

第２回会合を 12 月下旬に開催予定としていることが確認された。