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
ワーキンググループ（第７回）議事要旨

１．日時

平成 30 年３月９日（金）13:00～15:00

２．場所

総務省８階第一特別会議室

３．出席者

（１）構成員

宍戸主査、森主査代理、井上構成員、木村孝構成員、小山構成員、齋藤構成員、鎮目構成員、丸橋構成員、吉岡構成員

（２）総務省

古市電気通信事業部長、竹村事業政策課長、大村消費者行政第二課長、木村サイバーセキュリティ課長、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、冨岡消費者行政第二課課長補佐、高橋消費者行政第二課課長補佐、澤谷サイバーセキュリティ課課長補佐

４．議事要旨

（１）開会

（２）議事

第６回ワーキンググループにおける検討事項の整理状況について

① マルウェアに感染している可能性が高い端末について、当該端末の利用者に対して実施する注意喚起について

・注意喚起に対するオプトアウトについて、システム改造等が必要なため、ISP のハードルは高い。

・マルウェアに感染していて、攻撃の実績が無いかもしれないという段階であっても、結局Ｃ＆Ｃサーバにコントロールされているのでいつ攻撃主体となるか分からない、という状況もあるもと思料。整理状況については、その点を加味した書き方で統一しては。

・マルウェアの機能は、複合的なものが主流になっており、通常は DDoS 攻撃の機能が入っているという状況。

・マルウェアには、ある時点で DoS 攻撃の機能が無くとも、それをダウンロードして、新しい機能を追加した上で、DoS 攻撃をするというものもある。マルウェアに感染にしている時点で、DoS 攻撃の蓋然性があると判断することは現実的と思料。

・正当業務行為の目的の正当性は、電気通信役務の安定的な提供や、業務上の具体的な必要性という点に解釈上絞ってきたと理解。

・マルウェアに感染することは、利用者に被害を及ぼすだけでなく、ネットワークにも被害を生じさせるものと解するのが良いと思料。

② Ｃ＆Ｃサーバである可能性が高い機器と通信している、マルウェアに感染している可能性の高い端末の検知について

・DNS サーバにおけるマルウェアに感染している可能性の高い端末の検知と、ルータにおける同様の検知の取組のうち、後者については、技術的に難易度が高いと思料。

③ Ｃ＆Ｃサーバである可能性が高い機器の検知について

・Ｃ＆Ｃサーバである可能性の高い機器の検知の取組は、Ｃ＆Ｃサーバでない機器との通信も含めて通信全体を保存、分析の対象とするため、プライバシーとの関係も含めて検討すべきと思料。

・Ｃ＆Ｃサーバである可能性の高い機器の検知を希望しない者を検知の対象から外すことは難易度が高いと思料。

・マルウェアには DDoS 攻撃の機能が入っているものが多いし、機能が無いものであっても、即座に機能が追加され得るので、技術的な差はほとんど無いが、以前に DDoS 攻撃に関わったことがログから明らかである等から、差をつけて考えることについて一定の理解は出来ると思料。

・Ｃ＆Ｃサーバの可能性の高い機器の検知の取組について、正当業務行為を検討する場合、何を実現するためなのかという目的の正当性が問題となると思料。

・Ｃ＆Ｃサーバの可能性の高い機器の検知の取組について、正当業務行為を検討する場合、これまでの正当業務行為に関する整理に鑑みて、通信の秘密の侵害が広過ぎるとの印象。

④ 電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律案及び法律案に関する課題の検討について

・パスワード設定に不備のある IoT 機器の利用者に対する注意喚起について、利用者の受容性は高いと思料。実質的なオプトアウトが確保されているということが包括同意との関係で重要。

・オプトアウトは、オプトアウトした人と、していない人の通信履歴を別に保存する方法があるが、ISP にはハードルが高い。

・パスワード設定に不備がある端末への注意喚起について、仕様に含まれる認証については、機器のマニュアルに書いてあるので、ユーザ自身が対応できる可能性があるが、仕様に含まれないものについては、ユーザはどう対処すれば良いか分からないと思料。

・サイバー攻撃の送信元の情報共有や、パスワード設定が不備な端末の調査は、日本全体で一斉に始めていただきたい。

（３）閉会

（以上）