「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 第一次とりまとめ（案）」概要

（別紙2）

検討された課題とその対策

詳細については、第一次とりまとめ（案）を参照

最近のサイバー攻撃の動向を踏まえ、主として下記の課題に係る対策に関し、通信の秘密との関係等を整理

① マルウェア配布サイトへのアクセスに対する注意喚起

→ 利用者が、一旦契約約款に同意した後も、随時、同意内容を変更できる（オプトアウトできる）こと等を条件に、契約約款に基づく事前の包括同意であっても有効な同意と整理

② マルウェア感染駆除の拡大

→ C&Cサーバ※1に蓄積されている、同サーバとマルウェアに感染したPC等の端末に係る通信履歴からマルウェアの感染者を特定し、注意喚起を実施することは、当該端末が正常かつ安全に機能することに対する現在の危難を避けるための緊急避難※2として許容される。

※1 Command and Control serverの略。マルウェアに感染してボットと化したコンピュータ群（ボットネット）に、情報漏えいやデータ破壊等に係る指令を送り、制御の中心となるサーバ。

※2 刑法第37条 自己又は他人の生命、身体、自由又は財産に対する現在の危難を避けるため、やむを得ずにした行為は、これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない。ただし、その程度を超えた行為は、情状により、その刑を減軽し、又は免除することができる。

③ 新たなDDoS攻撃であるDNSAmp攻撃の防止

→ 利用者が設置しているブロードバンドルータ等のゲートウェイに対するインターネット側からの名前解決要求に係る通信を遮断することは、電気通信役務の安定的提供を図るための正当業務行為※として許容される。

※ 刑法第35条 法令又は正当な業務による行為は、罰しない。

④ SMTP認証の情報（ID及びパスワード）を悪用したスパムメールへの対処

→ 他人のID・パスワードを悪用して送信されるスパムメールへの対処として、当該IDの一時停止や、正規の利用者への注意喚起等を実施することは、電気通信役務の安定的提供を図るための正当業務行為として許容される。