「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 第二次とりまとめ（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、第二次とりまとめ（案）を参照

○　第一次とりまとめ以降に発生したサイバー攻撃の動向等を踏まえ、下記の課題に係る対策について、通信の秘密及び不正アクセス行為との関係を整理

①　C&Cサーバ※等との通信の遮断

→　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

※　Command and Controlサーバの略であり、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者からの指令を送り、制御を行うサーバコンピュータのこと。

②　他人のID・パスワードを悪用したインターネットの不正利用への対処

→　ISPが契約者に振り出している、インターネットを利用するためのID・パスワードを悪用したインターネットの不正利用への対処として、当該IDの一時停止や、正規の利用者へパスワードの変更依頼を行うことは、電気通信役務の円滑な提供を確保す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。

③　脆弱性を有するブロードバンドルータ利用者への注意喚起

→　不正送金や情報窃取、大量通信等のサイバー攻撃につながるおそれのある脆弱性※を有するブロードバンドルータを調査するために、インターネット側からブロードバンドルータに対して名前解決要求等を行い、これへの応答の有無を確認することは、不正アクセス行為の禁止等に関する法律に定める不正アクセス行為に該当しない。

※　情報通信機器やソフトウェア等において、プログラムの不具合や設計上のミスにより発生した、不正アクセスやウイルス感染等の原因となり得る情報セキュリティ上の欠陥のこと。

→　また、調査により得られた通信履歴から利用者を特定し、注意喚起を実施することは、電気通信役務の安定的提供等を図るための正当業務行為として許容される。

④　DNSの機能を悪用したDDoS攻撃に用いられている名前解決要求に係る通信の遮断

→　DNSの機能を悪用したDDoS攻撃である、DNSAmp攻撃やランダムサブドメイン攻撃を防止するため、当該攻撃に用いられている名前解決要求に係る通信を割り出し、これを遮断することは、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。