

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）

＜宍戸構成員 提出資料＞

- サイバーセキュリティ対策は、インターネットの利用者、関係する機器・端末の供給者等、官民すべての当事者の課題であり、もっぱら電気通信事業者にそのすべての責任や負担を課すようなことは現実的でもなければ、実効的な対策にもならない。

関係する当事者の全体像を見定めた上で、電気通信事業者だからこそ可能で実効的な対策について検討の照準を合わせる必要があると考える。

- 電気通信事業法上の通信の秘密については、憲法上の通信の秘密の趣旨を踏まえ、通信内容だけでなく通信の存在それ自体に関する事実まで広く保護されるものと解した上で、通信の秘密の侵害の違法性阻却事由（本人の同意、正当行為・正当防衛・緊急避難）についての解釈が積み重ねられることで、電気通信事業者による合理的なサイバーセキュリティ対策を可能とする枠組みが取られてきた。

本年の「電気通信事業における個人情報保護に関するガイドライン」の改定に当たっては、IoT時代の到来を踏まえ、「電気通信事業は、通信の秘密と直接関わる事業であって極めて高い公共性を有しており、また、プライバシー保護を必要とする情報を取り扱うことも想定される」と解説に記載された。

上記を踏まえ、常に通信の秘密・プライバシーとの適切なバランスを意識しながら、電気通信事業者によるサイバーセキュリティ対策を可能とする枠組みを検証すべきものとする。

- 大規模なサイバー攻撃に対応するためには、電気通信事業者間での一定の情報の共有・解析が必要である。通信の秘密・プライバシーとの関係で要保護性の程度を整理しつつ、一定の条件を満たす事業者の情報共有を可能とする枠組みを検討すべきものとする。

電気通信事業全体への利用者の信頼を確保するためにも、サイバーセキュリティ対策のために必要な限度で情報が取得・管理される仕組み、さらに不必要・不相当な政府機関等への情報提供等がなされないよう、能力・中立性を確保するための仕組みの検討が必要とする。

- 通信の秘密の保護には、通信事業を利用する公衆の自由（通信の自由）及び社会インフラとしての通信システムの確保の要請が前提されると解される所、サイバーセキュリティの観点から見て問題のある利用者端末への警告や接続の制限は、通信システムの確保のために通信利用を制限する局面として構成され、プライバシーを含めて、問題の所在を整理する必要があると考える。