4）帯域制御ガイドラインと通信の秘密

1.帯域制御ガイドラインから見る通信の秘密の考え方

2009年11月25日

社団法人日本インターネットプロバイダー協会
行政法律部会長　木村　孝

copyright©2009（社）日本インターネットプロバイダー協会

帯域制御ガイドラインとは

- 2008年5月23日に電気通信4団体から報道発表
  - 社団法人日本インターネットプロバイダー協会
  - 社団法人電気通信事業者協会
  - 社団法人テレコムサービス協会
  - 社団法人日本ケーブルテレビ連盟
- 総務省で2007年9月に「ネットワークの中立性に関する懇談会」報告書において、帯域制御の運用基準にかかる必要最小限の運用ルールの策定が望ましいとの指摘うけて、4団体で構成する「帯域制御の運用基準に関するガイドライン検討協議会」が約半年の検討ののち、パブリックコメントを経て策定したもの。
- 具体的にはISPが行なうP2Pファイル交換ソフトなどに対するトラフィック制限や携帯電話会社による大量通信ユーザーに対する通信速度制限について方法や情報開示を規定する民間の自主的ガイドライン
- 2008年から2009年にかけても協議会で検討が行なわれたが、ガイドラインの改定はなく、2009年8月7日に実態調査結果と解説資料（ポイント）のみが公開された。

copyright©2009（社）日本インターネットプロバイダー協会

通信の秘密に関するガイドライン

- 2007年5月30日に同じ電気通信4団体が策定した「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」がありますが、一般には公開されていません。
- 概要がJAIPAのホームページで公開されています。
  http://www.jaipa.or.jp/info/2007/info_070530.html
- Internet Week 2007の「C4 事業者がやってよいこと悪いことを考えよう
- 2)大量通信対策フォーラム～事業者がどこまでやれるのか？」で解説した資料が公開されていますので、参照してください。
  http://www.nic.ad.jp/ja/materials/iw/2007/proceedings/C4/index.html

copyright©2009（社）日本インターネットプロバイダー協会

そのほか通信の秘密に関連する資料

- 総務省　迷惑メール対策技術導入を検討されている事業者の方へ
  （送信ドメイン認証及びOP25B等に関する法的解釈）
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/jigyosha.html

- 総務省　次世代の情報セキュリティ政策に関する研究会（第8回）（平成20年5月23日）配布資料　ISPの活動と「通信の秘密」（高橋郁夫構成員）
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/next_generation/080523_2.html

- Telecom-ISAC Japan　トレースバック研究ポータルサイト
  2009年4月　本トレースバック手法の導入に関する法的問題点の整理
  https://www.telecom-isac.jp/tb/

copyright©2009（社）日本インターネットプロバイダー協会

「通信の秘密」の定義

- 「通信の秘密」の範囲は、個別の通信に係る通信内容のほか、個別の通信に係る通信当事者の氏名、発信場所、通信日時、通信量やヘッダ情報等の構成要素、通信の存否の事実、通信の個数なども含む広範なものである。（後略）

- ISP等が、例えば、特定のP2Pファイル交換ソフトに特有のパケットのパターンを検知して制御する場合のように、自己のネットワークを通過するパケットのヘッダやペイロード情報をチェックすること、特定のアプリケーションに係るパケットを検知すること、その結果を踏まえ当該パケットの流通を制御することは、それぞれの行為が「通信の秘密」の侵害行為に該当することになる。

copyright©2009（社）日本インターネットプロバイダー協会

「通信の秘密」の定義（2）

- また、ISP等が、ユーザのトラヒック量を検知して、特定のヘビーユーザについてはそのパケットの流通を制御することも、個別の通信に係る通信量を把握すること、当該把握に基づき制御を行うことになるため、それぞれの行為が「通信の秘密」の侵害行為に該当することになる。

- たとえ制御装置が自動的に動作するような場合であっても、「通信の秘密」に該当する事項を利用してISP等が制御を行っているのであるから、「通信の秘密」に対する侵害行為に当たらないわけではないことに注意する必要がある。

copyright©2009（社）日本インターネットプロバイダー協会

利用者の同意

- 利用者の同意があれば通信の秘密の侵害にはならない。
- しかし単に契約約款に帯域制御を同意する旨の規定を設けておくだけであったり、ホームページ上で周知しているといっただけでは、当事者の「個別」かつ「明確」な同意があったと見なすことはできないことに注意する必要がある。
- かかる同意があったと見なすためには、例えば、新規のユーザに対しては契約の際に帯域制御に同意する旨の項目を契約書に設けて明示的に確認すること、既存のユーザに対しては個別にメールを送信して帯域制御に同意する旨の返信をもらうことといった方法が考えられる。

copyright©2009（社）日本インターネットプロバイダー協会

違法性阻却事由が必要

- 正当防衛
- 緊急避難
- 正当業務行為

} 違法性阻却事由

- これらのいずれかがあれば、違法性がないということなので、仮に通信の秘密を侵害したとしても、罪に問われない。

copyright©2009（社）日本インターネットプロバイダー協会

正当業務行為とされるかどうかがポイント

具体的事例の検討

① 特定のアプリケーションに対して制御を行う場合

- 特定のP2Pファイル交換ソフトのトラヒックがネットワーク帯域を過度に占有していることにより、他のアプリケーションの通信に支障が生じている又は支障が生ずる蓋然性が極めて高いため、制御装置を利用して帯域を過度に占有しているP2Pファイル交換ソフトに係る通信を識別し、当該アプリケーションによる通信量を制限する場合

② 特定のユーザの利用を制御する場合

- 特定のヘビーユーザの発着信するトラヒックがネットワーク帯域を過度に占有していることにより、他のユーザの利用に支障が生じている又は支障が生ずる蓋然性が極めて高いため、制御装置を利用して当該ヘビーユーザのトラヒックを制御する場合

copyright©2009（社）日本インターネットプロバイダー協会

通信の秘密違反かどうかの判定　①の場合

➢ 目的の正当性、行為の必要性

- 特定のP2Pファイル交換ソフトを用いた通信がネットワーク帯域を一定期間にわたって過度に占有していることにより、他のユーザが通信サービスを利用するに当たって、ウェブページの表示やメールの送受信の遅延等、他のアプリケーションに係る通信速度や通信品質に支障が生じている又は支障が生ずる蓋然性が極めて高いといった客観的状況が発生しており、トラヒックの適正管理によるネットワークの安定的運用を図り、他のユーザの通信品質を確保するために、帯域制御を実施するといった場合には、一般的に目的の正当性及び行為の必要性が認められるものと考えられる。

➢ 手段の相当性

- 上記の目的を達成するために、トラヒックが特に多いアプリケーションに限定して実施していることから、一般的に手段の相当性も認められると考えられる。

copyright©2009（社）日本インターネットプロバイダー協会

通信の秘密違反かどうかの判定　②の場合

➢ 目的の正当性、行為の必要性

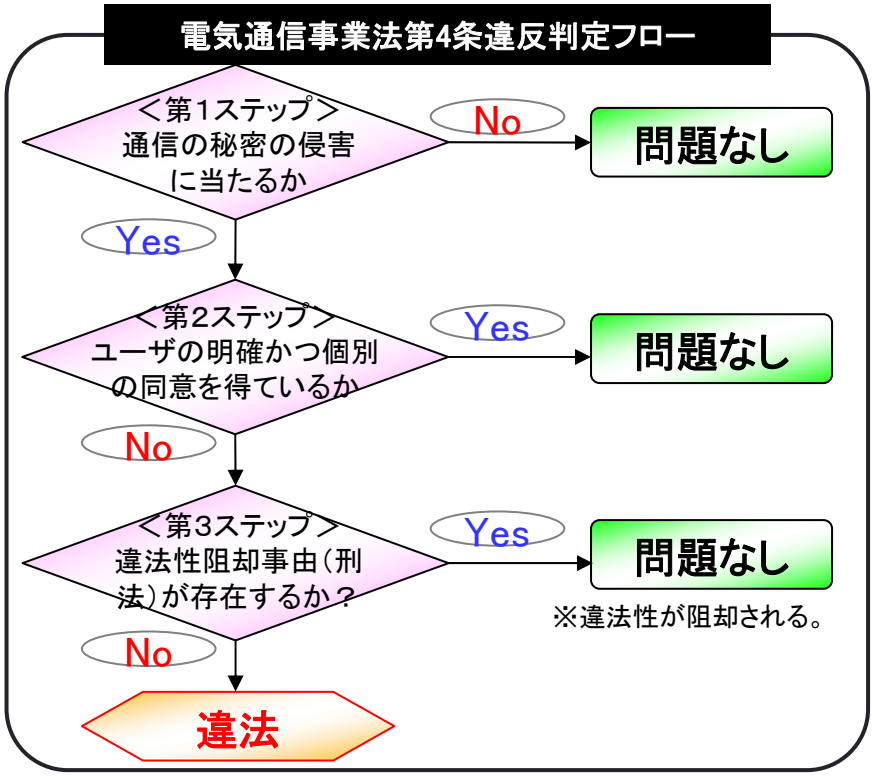
- 特定かつ少数のヘビーユーザが大量のトラヒックを発生させ、当該トラヒックがネットワーク帯域を一定期間にわたって過度に占有していることにより、他の一般ユーザの通信品質に支障が生じている又は支障が生ずる蓋然性が極めて高いといった客観的状況が現れており、トラヒックの適正管理によるネットワークの安定的運用を図り、他のユーザの通信品質を確保するために当該ユーザのトラヒックを制御するといった場合には、目的の正当性及び当該行為の必要性が認められるものと考えられる。

➢ 手段の相当性

- 上記の目的を達成するために大量のトラヒックを発生させている特定かつ少数のヘビーユーザの過度な利用を制限する限りにおいては、一般的に手段の相当性も認められると考えられる。

copyright©2009（社）日本インターネットプロバイダー協会

但し、客観的データが必要



copyright©2009（社）日本インターネットプロバイダー協会