Internet Week 2007

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？

「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（第1版）」について

2007年11月21日
ニフティ株式会社 経営補佐室
木村 孝

本資料は当日のプレゼン資料に後日追加修正を施したものです。

通信の秘密についての最近の報道

2006年5月の各種報道
某大手ISPによるWinnyの完全遮断について

ニュース、新聞での報道（5／18）
「Winny通信遮断、国の判断受け中止」

総務省 「憲法抵触の恐れ」、、、、、

2007年8月15日 某大手新聞1面の記事

ウイルス感染パソコン、ネット強制切断可能に・官民で指針

総務省は、、、、、

「通信の秘密」とは

日本国憲法 第21条2項 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

電気通信事業法
（検閲の禁止）
第3条　電気通信事業者の取扱中に係る通信は、検閲してはならない。
（秘密の保護）
第4条　電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。
2　電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。

罰則　（事業法第179条、　2年以下の懲役又は百万円以下の罰金、第2項　電気通信事業に従事する者の場合は3年以下の懲役又は二百万円以下の罰金。未遂も罰）

個人情報の漏えいと通信の秘密漏えい

- 個人情報の漏えいよりも通信の秘密の漏えいの方が重大と考えられている。
- 通信の秘密漏えい事故

電気通信事業法　第28条　電気通信事業者は、第8条第2項の規定により電気通信業務の一部を停止したとき、又は電気通信業務に関し通信の秘密の漏えいその他総務省令で定める重大な事故が生じたときは、その旨をその理由又は原因とともに、遅滞なく、総務大臣に報告しなければならない。　(30日以内)　施行規則57条　罰則30万円以下の罰金(188条)

- 個人情報漏えい事故

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

第22条　電気通信事業者は、個人情報の漏えいが発生した場合は、速やかに、当該漏えいに係る事実関係を本人に通知するものとする。2　電気通信事業者は、個人情報の漏えい等が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り、当該漏えい等に係る事実関係その他の二次被害の防止、類似事案の発生回避等に有用な情報を公表するものとする。3　電気通信事業者は、個人情報の漏えい等が発生した場合は、当該漏えい等に係る事実関係を総務省に直ちに報告するものとする。

(追加) 日米における通信の秘密の違い

- アメリカの憲法においては「通信の秘密」を規定するような条文はない。
- そもそもアメリカではインターネットは情報サービスとして取り扱われており、「通信」としては取り扱われていない。
- 世界的にも憲法上で通信の秘密を規定するのは珍しいかも。

インターネットと通信の秘密

総務省　電気通信サービスFAQから　http://www.soumu.go.jp/joho_tsusin/d_faq/

5-4「通信の秘密の保護」に関する法律と「通信の秘密」として保護される範囲

(前略) **通信内容だけでなく、通信当事者の住所、氏名、通信日時、発信場所等通信の構成要素や通信の存在の事実の有無を当然に含む**(後略)

5-5 インターネット上の通信も「通信の秘密」として保護されるのか

インターネットを利用して行われる通信であっても、インターネット接続事業者のサービスを利用して行われるような場合には、電気通信事業者の取扱中に係る通信の秘密に該当し、電気通信事業法に定める保護が与えられることになります。それ以外の場合であっても、必要に応じて有線電気通信法、電波法等の保護が与えられることになります。

機械的な処理あっても「通信の秘密」を侵害したことには変わりはないとされる。

ということはISPの業務はほとんど全て「通信の秘密」を侵害していることになる。

通信の秘密を侵すということとは？

- 知ること，漏らすこと，使うこと
  - 積極的に知る(聞く)行為(知得)
    - 漏らさなくても知るだけでアウト
    - 機械が収集するのも知得なのでアウト
  - 他人に漏らす行為(漏えい)
    - 他人に知らせたらアウト
    - 他人に知り得る状態においてもアウト
  - 悪用する行為(窃用)
    - 当事者の意に反して利用するのはアウト

しかし、「通信の秘密」の侵害によりによりすべて法的責任が生じるわけではない。

通信の秘密で法的責任を負わないための3つの条件

下記のいずれか一つを満たす必要がある

1. **当事者の同意がある**
2. **刑法35条*でいう「正当業務行為」**
3. **刑法37条*2でいう「緊急避難」に該当する**

2と3を「違法性阻却事由」と言う。

1．当時者の同意

当時者の同意があれば、秘密性はないので、違法性がない。利用者の申し込みに基づきフィルタリングを行なう場合は当事者の同意があったとされる。当事者は電話の場合、End-Endの両当事者の同意が必要とされるが、メールの場合は送信した時点で送り手の手は離れているという解釈から、メールの受信者の同意（委託）があればチェックして良いとされる。ただし、約款(利用規約）による包括的な同意では駄目で、個別の明示的な同意が必要とされる。

2．正当業務行為

- 配送のためにメールの宛先などをメールサーバーが振り分けのために見る事などのように、それを行なわなくては業務がなしえないもの。これは「通信の秘密を侵害しているが違法ではない」とされる
- 令状による開示

***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．緊急避難

正当行為と同じように「通信の秘密は侵害されているが違法ではない」
迷惑メールが受信元ISPのサーバーに大量に送信され、サーバーがダウンするような場合に、そのメール送信元からのメールを遮断する場合など。「現在の危難」が要件とされるため、その危難が発生している間しか認められない。迷惑メールが送信されていると分かっていても量的にサーバーがダウンする程度に至らない場合は「やむを得ず」とは言えないので、緊急避難にならない。

*2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。

(追加) 故意と過失

- 基本的に刑法で処罰されるのは故意
- 過失で処罰されるのは例外的 (過失を処罰することが予め条文で規定されている。)
- 通信の秘密の侵害についても、過失による場合(漏えい) は通常処罰されない。(重過失によるような場合は除かれる)
- 過去の例で、通信の秘密の侵害として処罰された例は、電話の盗聴を行なった場合など、故意性が強い場合。インターネットの業務のように微妙な事例はまだ無いと思われる。

緊急避難の例

電子掲示板における自殺予告の書き込みや自殺予告を内容とする電子メールに係る発信者情報は、個別の通信の構成要素であり通信の秘密に当たるため、プロバイダ等がその取扱中に係る発信者情報を知得し、又は発信者以外の第三者に開示することは、原則として通信の秘密の侵害に当たり許されない。しかしながら、当該発信者情報の開示が緊急避難 (刑法第３７条第１項本文) の要件を満たす場合には、開示行為の違法性が阻却されることになる。

「インターネット上の自殺予告事案に対するガイドライン」

その他、法律や解釈で認められた場合

・特定電子メール法　平成17年改正

（電気通信役務の提供の拒否）
第十一条 電気通信事業者は、一時に多数の架空電子メールアドレスをそのあて先とする電子メールの送信がされた場合において自己の電子メール通信役務の円滑な提供に支障を生ずるおそれがあると認められるとき、その他電子メールの送受信上の支障を防止するため電子メール通信役務の提供を拒むことについて正当な理由があると認められる場合には、当該支障を防止するために必要な範囲内において、当該支障を生じさせるおそれのある電子メールの送信をする者に対し、電子メール通信役務の提供を拒むことができる。

・プロバイダ責任制限法に基づき発信者情報開示をする場合

・解釈で認められる場合　例：「Outbound Port 25 Blocking導入に関する法的な留意点」

- OP25Bは、当事者の同意がない限り、通信の秘密を侵す行為に該当する
- OP25Bは、「目的の正当性、行為の必要性」及び「手段の相当性」を満たしており、正当業務行為と解釈できる
- OP25Bは、電気通信事業法第6条に規定する「不当な差別的取扱い」にも該当しない

「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」http://www.soumu.go.jp/joho_tsusin/d_syohi/jigyosha.html

インターネットにおける「通信の秘密」の侵害のケース

こういうのは？

大量のspamメールを送信するユーザの通信内容を調べ、メールの送信量を絞る

DDoS攻撃者の発信元をISP(A)が調べる

ISP(B)がユーザのメールを届ける（媒介する）

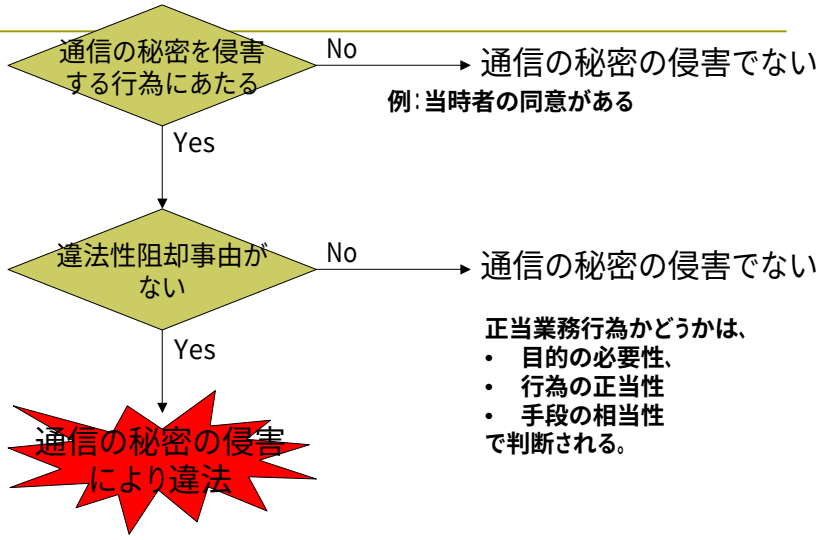
その他にも・・・

- 自ISPの契約者から、「自社のホームページが攻撃を受けているので、攻撃パケットをブロックしてほしい」との依頼があった
- 特定のユーザ宛の大量通信によって、事業者設備に支障が生じている
- ウイルスに起因する大量通信が不特定多数の送信元から送信され続けている
- 送信元詐称パケットが送信されている

・・等

事業者が対処措置の実施可否を判断しなければならない

通信の秘密の侵害で違法となる判定フロー



以下、P2Pに対する帯域制限を例に取ってみると。

まず「通信の秘密」「侵害行為」構成要件該当性

1.「通信の秘密」該当性

「通信の秘密」とは、(1)個別の通信に係る通信内容のほか、(2)個別の通信に係る通信当事者の住所、氏名、発信場所、通信日時等の構成要素を含む。

個別の通信に係るパケットの中身（ウィニーに特有のパケットのパターンであるかどうかを含む）は通信の秘密の保障を受ける。

2.「侵害行為」該当性

通信の秘密を「侵害する行為」には、「発信者又は受信者の意思に反して通信の内容等を利用すること」（窃用すること）も含む。

電気通信事業者が、自己のネットワークを通過するすべてのパケットをチェックした上、ウィニーがやり取りするパケットを検知して、これを破棄することは、通信の秘密の侵害に当たる。

通信当事者の同意がない限り、「通信の秘密」を「侵す行為」に該当する。

15

次に違法性阻却事由についての検討

問題の所在

通信の秘密侵害行為に該当する場合であっても、違法性阻却事由があれば（正当業務行為等に該当すれば）、当事者の同意の有無に関わりなく、許されることになる。

正当業務行為該当性

(1) 目的の正当性

電気通信事業者は、通信内容をそのまま伝達することが予定されており、本来の業務の範囲を超える。

(2) 手段の相当性

「通信当事者の同意を得ないで、ネットワークを通過するすべてのパケットをチェックし、ウィニーがやり取りするパケットを検知し、これを破棄する」行為は、
① 個人情報や機密情報等以外の問題のない情報の通信も遮断されてしまう
② ウィニーを用いた通信以外の通信を誤って遮断する可能性がある
ことから、目的達成のための手段として過大であり、手段の相当性を欠く

正当業務行為（違法性阻却事由あり）と判断できない。

16

目的の正当性の検証

- P2Pによりバックボーン回線が過度に専有され、他の全ての通信に影響がでていることから、通信設備の正常な運営を確保するため。
- (上り下りにより異なるが、P2Pによりバックボーンの5割から9割が占められ、全体で帯域の100％近くまで利用されているのはネットワークとして異常的な状態であり、例えばメールの受信がうまく行かない、ストリーム配信の映像が途切れる、Webの表示が遅いなど、全ての通信で減速するなど影響がでる。) 回線を増強すれば一時的には回避できるが、しばらくすると直ぐにまたP2Pで専有されてしまう。
- P2Pを介した情報流失を防止するため、というのは駄目のよう。

目的2：利用の公平性の確保

- 特定の利用者の通信だけを差別するのではなく、全ての利用者について行う。
- 現状では一部の利用者がネットワーク資源を大量に使い、その結果回線を共有するほかの利用者が圧迫を受ける可能性があり、その点ではそのような使い方を何らかの形で制御しないと、かえって利用が公平ではない。
- 会員（利用者）に対し、ポリシーを事前に提示し、利用規約で合意してもらうことで、公平性の確保は図れるのではないか。
- 現状を放置すると、一部の利用者の利用が全体としてネットワークを圧迫し、コストの上昇、ひいては利用料金の値上げにつながりかねない懸念がある。多くの利用者に安価にブロードバンドを提供するという観点から、一部のP2Pの利用についてはある程度の制限がかかるのは全体としては合理的と考えられる。

設備の適正な管理を理由にすると、目的としては受け入れられやすい？

- 平均を著しく超える大量のトラフィックを送受信するによりネットワーク設備・帯域を専有するような利用を行うことにより、他の多くのお客様が通信速度の低下・通信品質の悪化等の影響を被る事態が発生している
  - ■設備の適正な管理のためトラフィックの内容をより 的確に把握するため装置を導入
- 少数のユーザーがトラフィックの大半を使ってしまうのは 利用者間で公平とは考えられない。それを平準化するため一部の特殊な 使い方に制御を加える

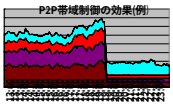
多くのお客様が安心・安全にインターネットを利用できるように
ネットワークの維持／管理業務の一部として帯域制御を実施

目的の正当性を検証するためのデータが必要

- 特に最初に行う2，3社
- 一旦正当とされれば同じ方式については以降の事業者はデータの提出は必要なくなる。総務省に届出のみで可（OP25Bの経験）
- 上りと下りに分けて検証したデータと分析結果を提出

(上りの例)

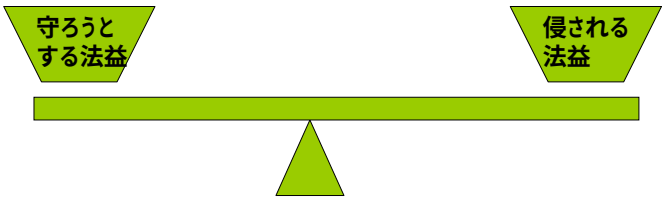
- ファイル交換ソフトのトラフィックに帯域制限をかけない場合、上りのトラフィックは能力のnn％で推移
- そのうち、P2Pと思われる利用が全体の約9割を占めている。
- 装置を用いてファイル交換ソフトのトラフィックをxxx Mbpsに帯域制限をかけた場合、トラフィック量はネットワーク能力のyy％からzz％となる。
- 結果的に、その中でフィル交換ソフトと思われる利用は全体の約半分になる。
- ファイル交換ソフトのトラフィックに帯域制限をかけない場合に比べ、ファイル交換ソフトのトラフィックに帯域制限をかけた場合には、ファイル交換以外のトラフィックがn割程度増える。



手段の相当性
遮断と制限(帯域制限は同一ではない)

- 通信の秘密の侵害については同様だが、行為が異なることで、正当性を判断する場合の法益の権衡の際の判断に影響がある。
- 遮断の場合は、帯域制限に比べ侵害される法益はより大きいと考えられる。
- 帯域制限であれば、速度は抑えられるものの、使えない訳ではないので、侵害される法益はより少ないと考えられるよう。

遮断と制限の差はここ！！



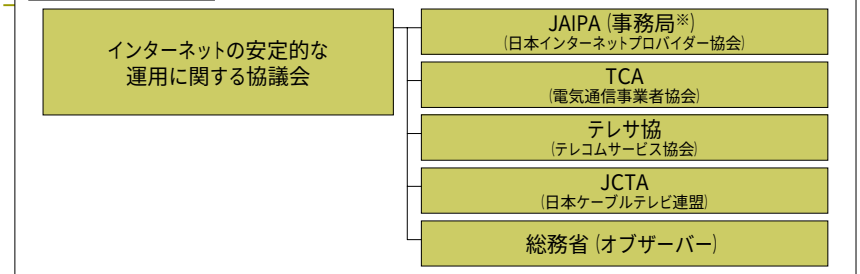
ガイドラインについて

- 電気通信関連の4団体*は、2007年5月30日に「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（第1版）」を策定し、その概要について報道発表
  http://www.jaipa.or.jp/info/2007/info_070530.html
- ガイドライン本文は、原則として電気通信事業者限りの開示なので、取扱いには注意すること。非公開とした理由は、公開すると攻撃者へISPが対処できない攻撃方法発案のヒントを与えかねない為。
- (追加)ガイドラインは加盟する団体事務局から配布。団体非加盟の事業者はJAIPAに照会。
- 業界の自主基準としての位置づけ（総務省はオブザーバとして協議会に参加）
- 業界の自主ガイドラインとしての性質上、ガイドラインに沿った対応をすれば必ず免責されるといった効果までは無いが、仮に法的な紛争があった際にはガイドラインに沿った対応を行っていることが考慮されるものと期待される
- (追加) ガイドライン協議会では、新しい事例を募集しているので、事例の相談があれば事務局（JAIPA）に寄せて欲しい。

*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

「インターネットの安定的な運用に関する協議会」

協議会構成メンバー



活動内容

- 2006年5月～
- 前述のようなケース（1～6）のような場合において、「通信の秘密の侵害」にあたるのか、そうでないのかについての類型化とその考え方を整理
- ガイドラインの作成とISP業界における情報共有

23

フィルタリングについて

P2Pによる遮断（ぷらら）、ホームページのフィルタリングサービス、電子メールの迷惑メールフィルタリングについて以下のような考え方がされている。

＜初期設定をフィルタリングオンの状態で提供するための条件＞

1. 利用者が、いったんフィルタリングサービスの提供に同意した後も、随時、任意に同意内容を変更できる状態（設定変更できる状態）であること
2. フィルタリングサービス提供に対する同意の有無にかかわらず、その他の提供条件が同一であること
3. フィルタリングサービスの内容等が明確に限定されていること
4. 通常の利用者であれば当該サービスの提供に同意することがアンケート調査結果等の資料によって合理的に推定されること
5. 利用者に対し、フィルタリングサービスの内容等について、事前の十分な説明を実施すること（事業法第26条に規定する重要事項説明に準じた手続により説明すること）

平成18年1月23日電気通信事業分野におけるプライバシー情報に関する懇談会（第18回会合）議事要旨
http://www.soumu.go.jp/joho_tsusin/d_syohi/060123_1.html

24

では、こういうのはどうなんでしょう？

- LAN型のアーキテクチャで提供するISPで TCP/UDPでポートの135番、137番、138番、139番、445番をマスクする。
- ポートを全て閉じた上で、いわゆるウェルノーンといわれるポートのみをオープンする。
- メールとWebのポートのみ利用可能とする。