通信の秘密とは？

～電話１００年の通信から IPの時代の通信への変遷～

テレコムサービス協会　斉藤　衛
日本ｲﾝﾀｰﾈｯﾄﾌﾟﾛﾊﾞｲﾀﾞ協会　甲田　博正
総務省データ通信課　高村　信

電話とインターネットの比較

		電　話　系	インターネット
事　業	主な設備	伝送装置・交換機等（サービス毎に異なる）	WS・PC・PDA・ルータ・スイッチ等多種にわたる（サービスによらない）
	成　長	ゆっくり（現在はマイナス）	非常に速い
	通信料	通話毎課金（時間と距離の概念。みんなのインフラ→公平。）	接続毎・安価（bit単価は約1／1000）（距離・国境を感じない）
プレーヤ	事業者	比較的少数（264事業者 2000/5/1）	非常に多数（しかも急増）（7753事業者 2000/5/1）
	利用者	ほぼ同数（ゆっくり増加→1996年以降ゆっくり減少）	ほぼ同数（急増）
	その他	少数（N・F・O・A等の設備メーカー）	非常に多数（急増）（PC・OS・AP・NW機器のメーカーやベンダ等）
技　術	技術の基盤	仕様化された装置	コンピュータ
	通信方式の特徴	コネクション型・一定品質	コネクションレス型・ベストエフォート型
	サービスの所在	事業者が提供するNW上（端末には限られた機能のみ）	各個人のPC等、事業者のルータ・サーバ等（機能が分散）
	サービスの数（※1）	少数	非常に多数（急増）
	サービスの開発者	事業者と装置ベンダ	個人・企業（わかる者が次々に。）
	IDとその数的制限、付与形態	電話番号・無限（※2）・個人に付与	IPｱﾄﾞﾚｽ・枯渇（※3）・事業者に付与（※4）
特　性	主人公	国・事業者が主体（網中心）（UNI／NNIの概念が存在する。）	（世界中の）個が主体（分散型）（利用者たちが情報発信し、サービスを開発し、ネットワークを造る。）
	リスク等	安定・安全（国・事業者が責任を持って提供）	匿名性・個人主義・様々なリスク
	共通した特性	・クローズ　・トップダウン ・ゆっくり　・スタティック	・オープン　・ボトムアップ ・スピーディ　・ダイナミック　高速で成長する生きもの？！

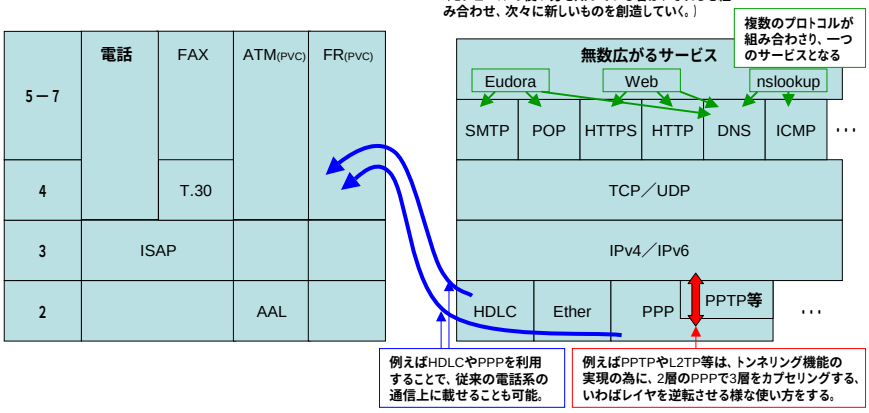
※1．アプリケーションやプロトコル等の数。　※2．桁数を増やすことにより。　※3．動的割当→匿名性を高める原因の一つに。IPv6にて解決。　※4．日本ではJPNICがIPアドレス管理指定事業者に付与。

プロトコル比較

電　話　系　　VS　　**インターネット**

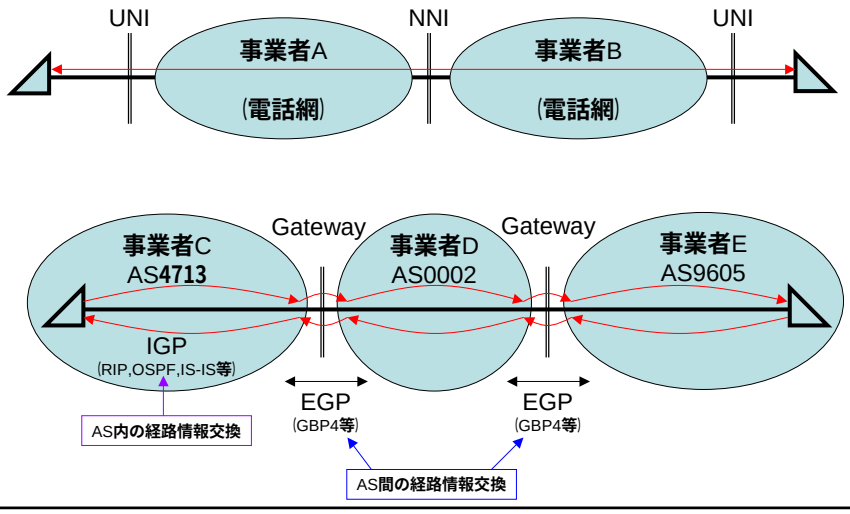
①Vertical。つまりほとんどのプロトコルは、サービス毎に独立している。
②ITUを中心とした国際標準が中心であり、時間をかけて仕様がかためられている。

①ホリゾンタル。つまり、TCP/IP Protocols Suiteを中心に、様々なプロトコルが自由・複雑に関係しあっている。（ソフト開発におけるモジュールの発想）
②自由度が高い為、完成度は低いものもあるが、短期間で開発を重ね、成長していく。
（モジュールの使い方を知っている者が、それらを組み合わせ、次々に新しいものを創造していく。）



通信方式の変化

コネクション型→コネクションレス型



なぜこんな比較をするのでしょうか？？？

通信の秘密として保護すべき部分が、非常に多様化している

通信手順・通信規格・相互接続等

法令についてのおさらい

○電気通信事業法（昭和59年法律第86号）
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　（略）
第１７９条　電気通信事業者の取扱中に係る通信･･･の秘密を侵した者は、２年以下の懲役又は１００万円以下の罰金に処する。
２　（略）

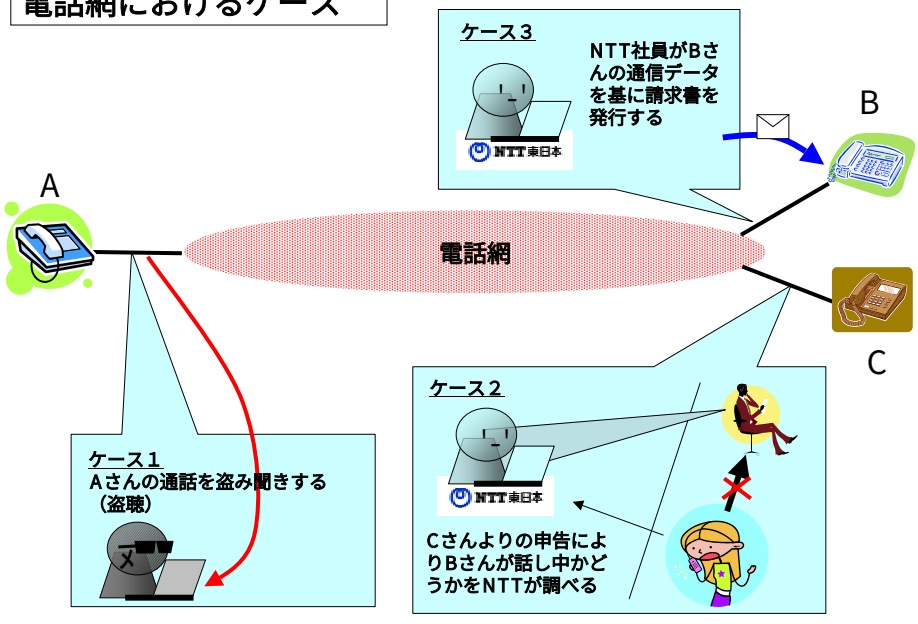
○日本国憲法（昭和22年５月３日施行）
第21条　　（略）
２　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

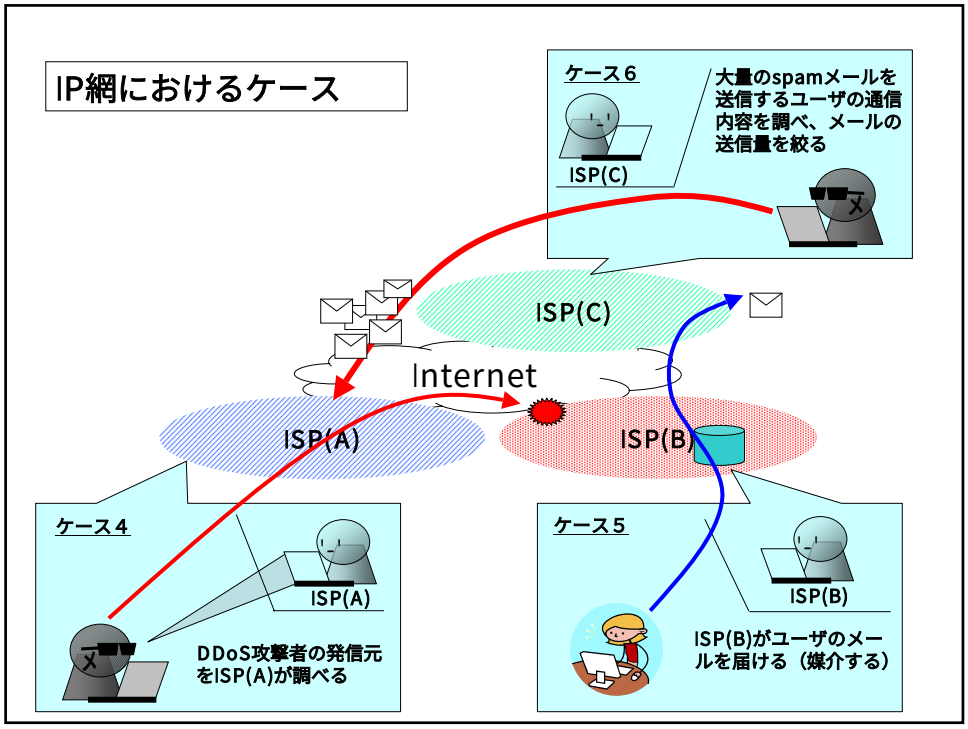
○刑法（明治40年法律第45号）
第３５条　法令又は正当な業務による行為は、罰しない。
第３６条　急迫不正の侵害に対して、自己又は他人の権利を防衛するため、やむを得ずにした行為は、罰しない。
２　防衛の程度を超えた場合は、情状により、その刑を減軽し、又は免除することができる。
第３７条　自己又は他人の生命、身体、自由又は財産に対する現在の危難を避けるため、やむを得ずにした行為は、これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない。ただし、その程度を超えた行為は、情状により、その刑を減軽し、又は免除することができる。
２　（略）

皆さんに質問です！！

次のケースのうち、どれが「通信の秘密の侵害」に当たるか？？
考えてみましょう！！

電話網におけるケース





答　え！！

全部のケースが「通信の秘密の侵害」にあたります。

(((　゜д゜)　　゜゜

１．「通信の秘密」該当性

「通信の秘密」とは、⑴個別の通信に係る通信内容のほか、⑵個別の通信に係る通信当事者の住所、氏名、発信場所等、通信日時等の構成要素を含む。

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構成要素等を利用すること」（窃用すること）も含む。

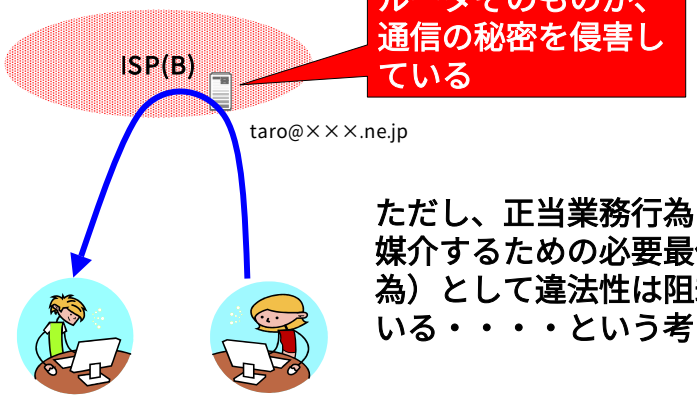
当事者の同意がない限り、通信の秘密を侵害する行為は許されない。

しかしながら･･･

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（正当業務行為又は正当防衛、緊急避難に該当すれば）、当事者の同意の有無に関わりなく、許されることになる。

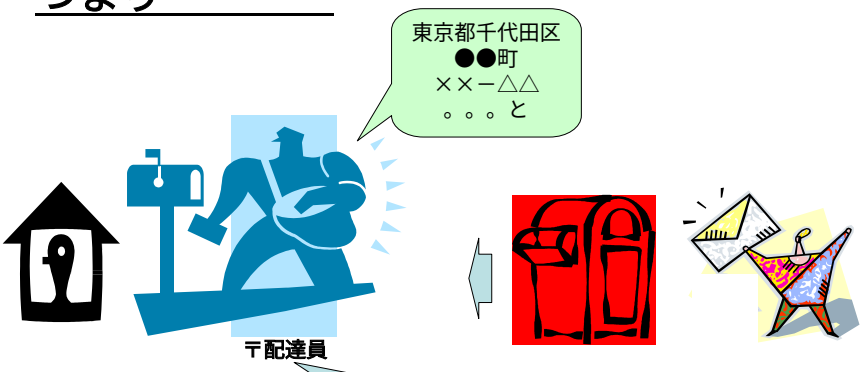
確認までですが。。。。

ケース５



ただし、正当業務行為（通信を媒介するための必要最低限の行為）として違法性は阻却されている・・・・という考え方

つまり・・・・



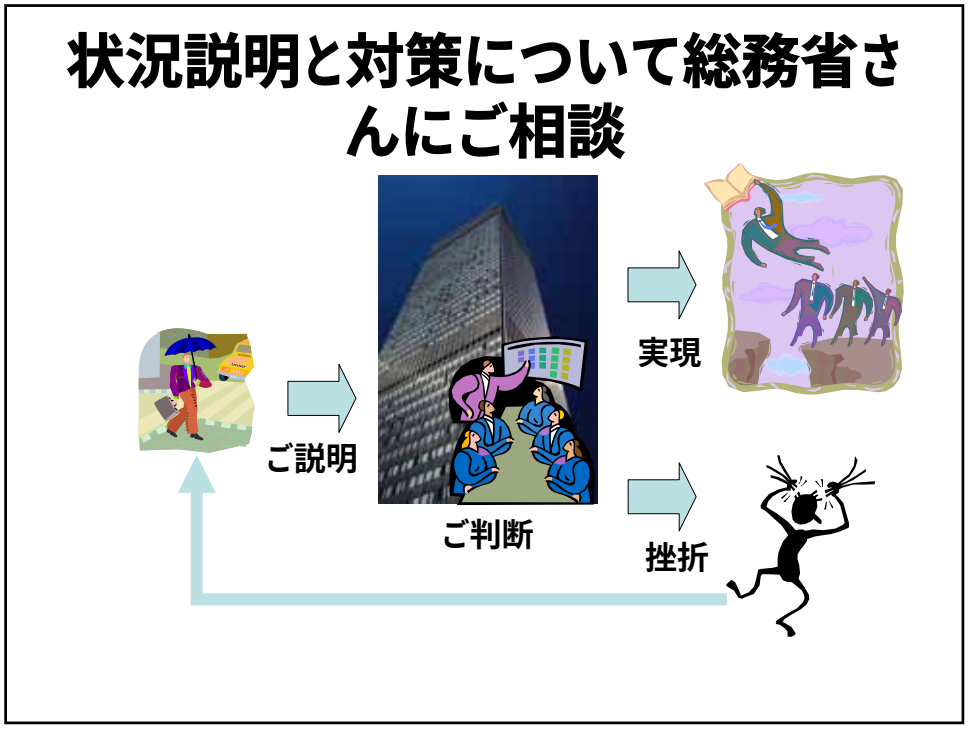
〒配達員は配達するにあたり通信の秘密を常に侵していることになるが、郵便業務の遂行上の正当行為であることから、その違法性は阻却されている

では、具体的にはどんな場合において違法性は阻却されると言えるのか？？？？？

「ケースバイケースですね。個別にご相談ください」　総務省総合通信基盤局消費者行政課談

（　；ω；）


問題は。山積み
DDoS攻撃
フィッシング
Spamメール
ワーム
ウイルス
ボットネット
ターゲッティ
アタック
ソーシャル
エンジニアリング
ゼロデイ
アタック
トラフィック逼迫
脆弱性
情報漏えい
対応コスト


状況説明と対策について総務省さんにご相談
ご説明
ご判断
実現
挫折

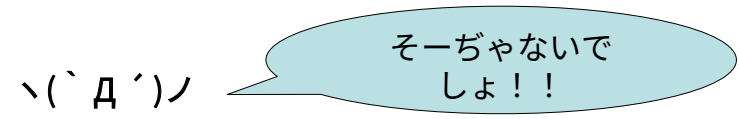
motivation

- 事案はいっぱい、個別のご相談。
- 状況の変化はすばやい。対策には時間がかかる。
- 実は、S務省さんに確認せずにやっている(人たちが居る、らしい)。
- S総務さんって、なんか怖い。

- それぞれの状況に対して何をどこまでしてよいのか、事前に決められないだろうか？
- 状況の変化に応じて毎年アップデートできないだろうか？

私家版S務省語録

- ルータってのはあれですか。IPパケットのヘッダみて送出先を決めるんですか。
  - じゃあ通信の秘密を侵害していますね。
  - 機械で自動的に、でも侵害は侵害ですね。
- それ、やってもいいですが、重要説明事項なので全利用者に十分説明してください。
  - Webに掲載？ダメですね。
- 事業法四条の「電気通信事業に従事する者」というのは、その人がいなければ電気通信が成り立たない人と解釈できます。
  - 今で言えば電話交換手くらいですね。
- …



という声を受けまして、今はこんな営みをしております。

インターネットの安定的な運用に関する協議会

参加団体：日本インターネットプロバイダー協会
テレコムサービス協会
電気通信事業者協会
日本ケーブルテレビ連盟
ｵﾌﾞｻﾞｰﾊﾞｰ：総務省

活動内容は？

●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各ISP間における情報共有

近　日　公　開！！

例えば・・・・・？

問１

大量通信攻撃等、受信した設備に異常を来たす通信（以下「攻撃通信」という。）を受信した受信者から当該攻撃に係る通信の遮断依頼を受けた場合、①遮断依頼が正当なものか否かの判断をするため、ネットワークの適正運営等のために通常時より取得しているトラヒックの統計データと依頼時点の統計データとを機械的に突合せ「異常な状況」であるか否かを判断するとともに、②異常な状況であった場合、当該攻撃にかかる通信がどのような特性を有するものであるかを分析してよいか。

現在検討中

【考え方】
「自社契約者から特定のＩＳＰ別へのトラヒック及びその通信種別情報」及び「特定のＩＳＰ別から自社契約者へのトラヒック及びその通信種別情報」は、個別の通信についてその発信者が自社契約者か否か判別した上で作成された情報であり、通信の秘密に当たる。したがって、これらの情報を攻撃通信への対応のために利用することは、通信当事者の意思に反して行われる場合には通信の秘密の侵害（窃用）に当たりうる。（ただし、当該情報の取得自体については別途）
　この点、受信者又は受信回線の加入者から、「特定の受信回線宛の通信について、その内容等を分析し、一定の攻撃特性を有する通信のみを遮断する（通信の秘密を侵害する）」ことについて個別の同意を取得すれば、通信の秘密の侵害とならない。

問２

網内トラヒックの現状把握
電話網におけるネットワークオペレーションセンターによる流量把握をIP網でも実施。電話網であれば、（通信内容を含まない）共通信号線内の信号から、流量や流束の方向が把握可能であるが、IP通信の場合、パケットヘッダ部の統計データを取得する以外に手段がない。設備増強の必要性の判断や通信設備の障害発生時に障害の原因究明を円滑化などを目的として、網内トラヒックの現状把握をすべく統計データを取得してよいか。

【考え方】
「自社契約者から特定のＩＳＰ別へのトラヒック及びその通信種別情報」及び「特定のＩＳＰ別から自社契約者へのトラヒック及びその通信種別情報」を収集することは、個別の通信に係る送信元及び送信先ＩＰアドレスを検知して利用しているため、通信の秘密の侵害に当たる。
ただし、設備増強の必要性の判断その他の自社業務を適正に遂行する等の業務目的のために、必要な範囲でそれらの情報を収集することは、正当業務行為として違法性が阻却される。

現在検討中

問３

送信元設備の所有者の意思と関係なく送信される攻撃通信の場合
大量通信がウイルス・ワームなどに起因したものであり、不特定多数の送信元から送信され続けている状況下において、これら通信を遮断しない限り通信設備の安定的な運用は困難であるものの、当該遮断がその他の通信も遮断していないことが担保できない状況下において、当該通信の遮断を停止しても安定的な運用が可能となるよう、①遮断した通信パケット及び接続ログから送信元の契約者を特定し、②当該契約者に対しウイルス・ワームなどを駆除するよう要請することを通じ、当該大量通信の漸減を図ってよいか。

現在検討中

【考え方】
　大量通信を送信している契約者を特定するため、個別の通信に関する通信パケット及び接続ログの解析を行うことは、通信の秘密の侵害（知得）に当たりうる。
　しかしながら、大量通信が発生し、これにより事業者設備に生じる侵害を防止するための行為については、通常は、正当防衛又は緊急避難として違法性が阻却される。

現在検討中