

電気通信事業における ガバナンス強化の必要性

通信手段多様化・複雑化の時代、ユーザを守る為に

一般社団法人日本インターネットプロバイダー協会

副会長兼専務理事

立石 聡明

JAIPA概要

- 沿革：
 - 1997年地方のISP100社余りで任意団体を設立(JLAP)
 - 大手ISPも参画し日本インターネットプロバイダー協会を任意団体として1999年12月設立
 - 2000年12月に社団法人となる。（現在一般社団法人）
- 会員数：145社（正会員140・賛助会員5）
- ロケーション：代々木駅前ビル
 - 会員企業様が参集しやすい場所に
 - 住所：東京都渋谷区代々木1-36-1 オダカビル6F

JAIPAとは

インターネットプロバイダーからなる日本で唯一の業界団体です。

具体的には

- 大手ISPだけでなく地方の中小ISP約100社が加盟するインターネット接続サービス(ISP) 事業者
 - 地方ISPは地域におけるIT関連の各種事業を提供していることが多く、自治体のシステムやインフラ(光ファイバー、ADSL~IoT・M2MX)も独自に展開している事業者も少なくない
 - 今後、DXを促進していく上で、地域の自治体等からの信頼も厚い
 - それぞれ街づくりなどの事業と一体的に地域に根ざした事業展開を行っている
- クラウド、ホスティング事業者
- 上記に対して各種サービス（セキュリティや技術など）を提供する事業者などインターネット関連事業者で構成されています

ユーザが安心して通信を利用できる環境の構築を

- 新型コロナ感染症が広まって以来、それまで遅々として進まなかったデジタル化の波が世界的に押し寄せてきた
- DXの推進、ポストコロナ時代において、インターネットが国民生活においても、社会経済基盤としてもより一層重要性が増している
- このような時代において、利用者が安心してインターネットを利用できる環境を維持していくことが極めて重要である
- 一方、重要性の高まり、大量の情報集積、サイバー攻撃などにより、リスクが高まっており、このリスクに業界全体として対応するためのガバナンスを高めていくことが重要

通信事業者はユーザを守る立場

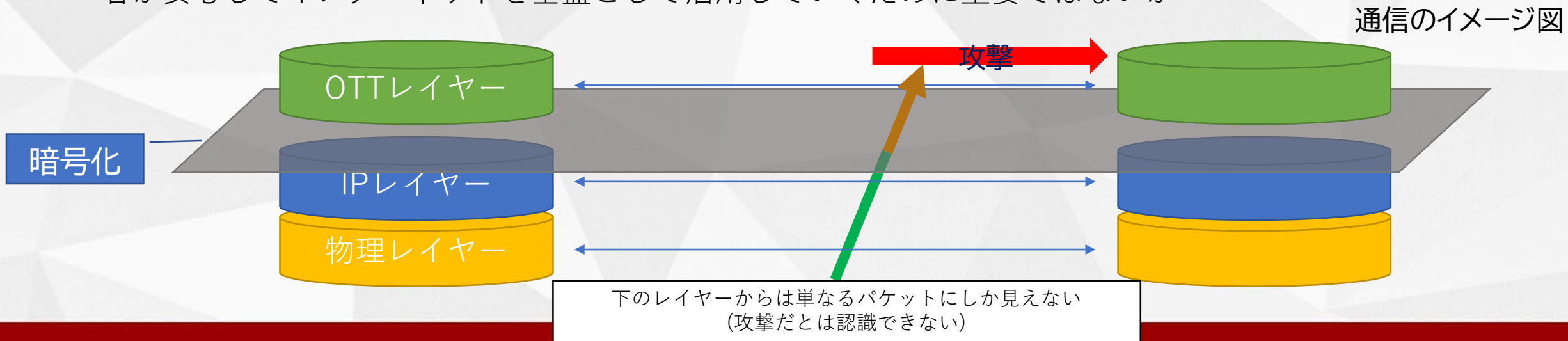
- ISP等の通信事業者(IPレイヤー、物理レイヤー)は、通信の秘密を保護しつつも、業界ガイドラインの策定、運用を通じ、サイバー攻撃から通信網や利用者を守る役割を担ってきた
- その上に乗って暗号化した通信を大量に流通させるOTTの登場により、ユーザを適切に守るにはISP等だけでなく、OTTに対するガバナンスも視野に入れることが求められる
- (今回検討されている内容について) 電気通信事業者として従来から行ってきたことであり、特段問題がある内容ではなく当然果たすべき役割と考える

通信のイメージ図



SSLやアプリ内通信等は通信事業者からその内容が見えない

- SSLやアプリ内通信等が「普及することにより」「電気」通信事業者のみでは利用者を守り切れない環境変化が起こっている
- 暗号化等がされたレイヤーの通信はISPからは単なるパケットにしか見えないため、行われている通信が攻撃かどうか不明
- ISP（電気通信事業者）としても、「通信の秘密に関する情報を守る」、「サイバー攻撃から守る」努力を続けるものの、OTTレイヤーにおいてもこれを守らないとユーザーを守り切れない
- ISPとOTTレイヤーそれぞれが、その役割を共同して果たす体制を整えていくことが、日本の利用者が安心してインターネットを基盤として活用していくために重要ではないか



サイバーセキュリティ

- 2007年より「インターネットの安定的な運用に関する協議会」を業界団体を構成し、総務省のオブザーバー参加のもと、「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」を策定し、数年おきに計5回に渡り改訂を行って運用してきた
- このガイドラインは民間のものであるが、電気通信事業者がDoS 攻撃等のサイバー攻撃、マルウェアの感染拡大及び迷惑メールの大量送信及び壊れたパケット等を識別しその通信の遮断などの対処を実施するにあたって、電気通信事業法等の関係法令に留意し適法に実施するための参考資料として作られ、一種の共同規制的な役割を果たしている
- 複雑化・巧妙化したサイバー攻撃等に適切に対処するために、DDoS攻撃などの攻撃元、指令元、攻撃先情報等についてISP事業者間の連携協力を促進する仕組みが可能になると、ユーザを攻撃から守るだけでなく、インターネットの安定的な運用という面からも通信事業者にとって有益である
- よって今回の法改正で実現しようとしていることについて賛同する

端末IDやCookie:「グローバルな調和の必要性」

- EU ePrivacy指令については、10年以上前に施行されており、cookie等端末情報を取得する際には原則として同意取得が原則となっている
 - そもそもEUの求めるCookieのオプトアウトとはほど遠い方法で同意を求めようとしていることが既に問題となっている
- 米国においても従来から端末情報取得についてオプトアウトが行われてきており、CCPAにおいてもオプトアウトを導入することが義務付けられている
 - ⇒ 端末IDやCookie等の端末情報について、取得しようとする際には、利用者の確認の機会を適切に与えないと、むしろグローバルな規制との調和が図られないのではないか
 - ⇒ 電気通信事業者が適切に利用者情報の保護を行うこと、サイバーセキュリティ対策を確保していくことが、我が国がグローバルに提唱・推進するDFFTを確保する観点からも重要ではないか
- これは今後GDPRの十分性認定に影響する可能性が出てくれば、日本企業にとって大きな損失となり得ることが懸念される。

ユーザが安心して通信を利用できる環境の構築を

- これまでもISPなどの（登録・届出）電気通信事業者は、通信の秘密の保護、利用の公平、電気通信事業者における個人情報保護などを順守してきた
- インターネットの仕組みが従来の通信の枠を超えて複雑化し、新たな事業者が登場、各種サービスを提供する中、それらに対する一定の規律を検討することが求められている
 - レイヤーが違ってユーザの保護は同レベルで必要な措置であり、暗号化やアプリ内通信が一般的になりつつある現状を考えれば必要
 - 特に「通信の秘密」等に関しては憲法が保障する国民の権利であり、これはいかなる「力」からも守られるべきであって通信事業者はその最後の砦とも言える存在ではないかと考える
- 複雑化、巧妙化したサイバー攻撃に対処するためには、DDoS攻撃などの攻撃元、指令元、攻撃先情報等についてISP事業者間の連携協力を促進する仕組みが可能になると、ユーザを攻撃から守るだけでなく、インターネットの安定的な運用という面からも有益である
- 検索サービスや大手プラットフォームが上記の様な体制を取ることは極めて重要な環境整備であり、ユーザの情報を保護することは基本的には規模に関係なく必要な措置ではないか
- 適切に利用者情報の保護を行うこと、サイバーセキュリティ対策を確保していくことが、我が国がグローバルに提唱・推進するDFFTを確保する観点からも重要