

# IP電話に関連する諸課題への取り組み

---

平成27年12月  
総務省

# 1. IP電話の普及

- IP電話の利用数は平成26年度末で3,564万件であり、特に0ABJ型IP電話の増加傾向が顕著

## A 050型IP電話

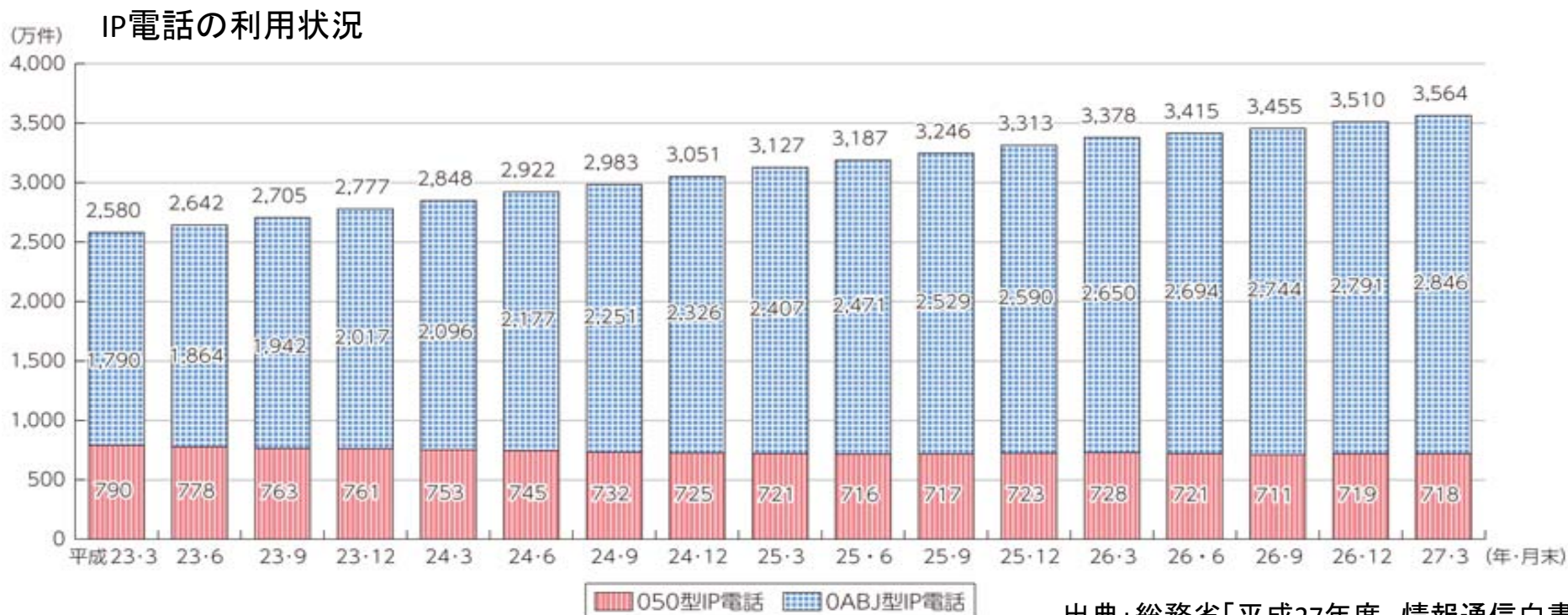
050番号を用い、インターネット接続サービスの付加サービスとして提供され、同じプロバイダもしくは提携プロバイダの加入者間の通話料は無料であることが多い。一方で、緊急通報(110、119等)を利用できない点や、通話品質の基準が加入電話に比べて低いといった点もある。

平成26年度末における利用数は、718万件となっている。

## B 0ABJ型IP電話

0ABJ型IP電話は、加入電話と同じ0ABJ番号を用い、加入電話と同等の高品質な通話や緊急通報(110、119等)を利用できるなどの特徴がある。

平成26年末における利用数は、2,846万件あり、増加傾向が顕著である。

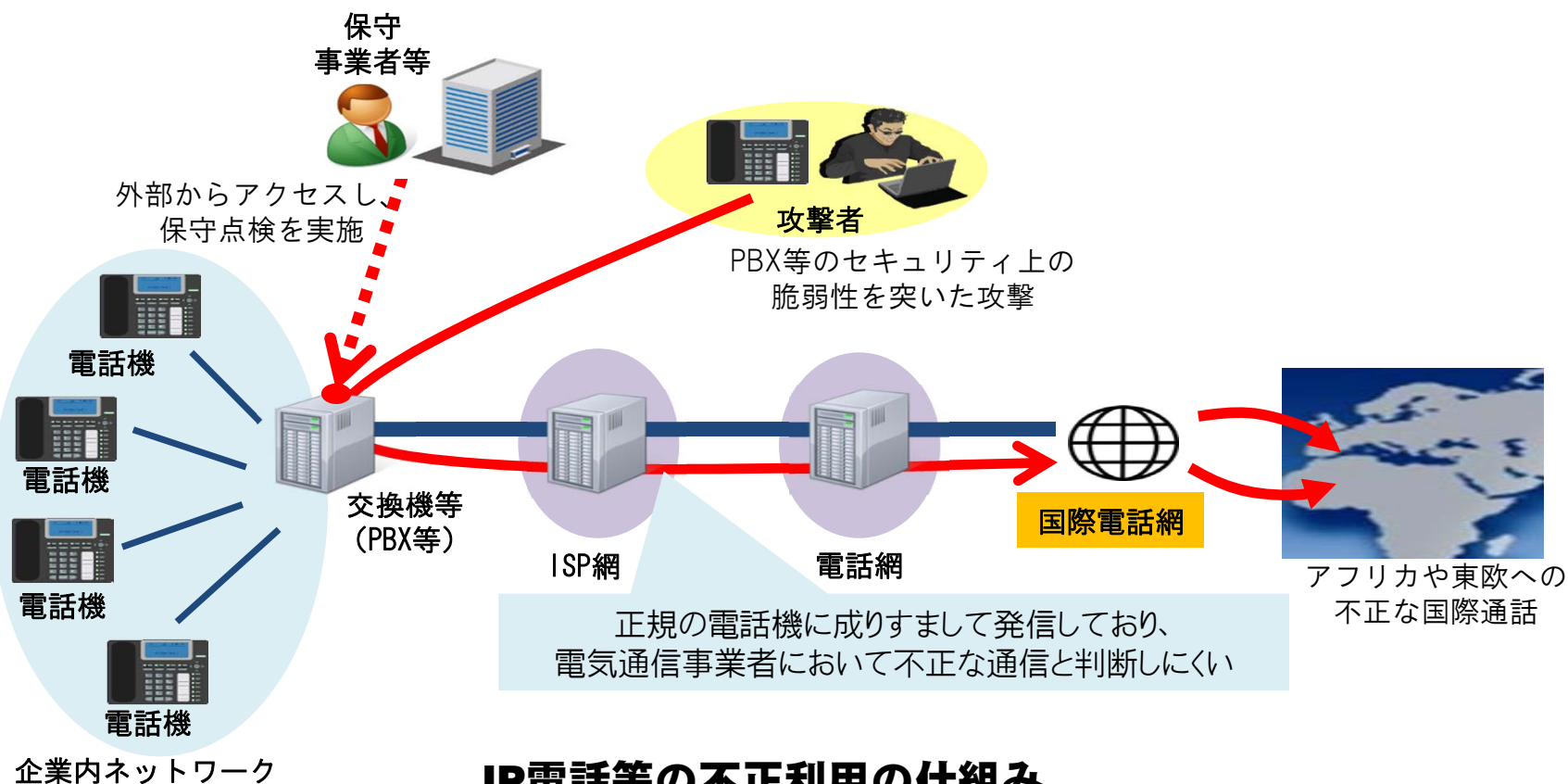


※過去の数値については、データを精査した結果を踏まえ修正している。

出典：総務省「平成27年度 情報通信白書」

## 2. 第三者によるIP電話等の不正利用について①

- 平成22年頃から、多くのIP電話事業者等で不正利用による被害が年間数件～数十件発生。本年3月及び4月、特定の機器販売業者のPBXを導入している利用者において、不正利用による被害が80件程度発生。
- ほとんどは、個人事業主などの中小企業等が利用しているPBX(内線電話を実現するための交換装置)が被害にあったもの。保守等のため外部からのアクセスが可能なPBXがセキュリティの脆弱性をつかれるなどサイバー攻撃を受け、PBXが海外に電話をつなぎっぱなしとなるといった事象。
- 個人ユーザのIP電話ルータは、通常はデフォルトで電話を除けば外部(インターネット)に繋がらない設定だが、自ら外部からアクセス可能とするよう設定変更した個人ユーザが被害にあった事例が少数あり。



## 2. 第三者によるIP電話等の不正利用について②

### 被害状況

※ 平成27年6月22日(月)時点

- 全体的な傾向として、従来より一定の頻度で不正利用による被害が発生しているものの、報道にあったような直近で大規模な不正利用は、事業者横断的に発生しているものではなく、局所的な被害に留まっている模様。
  - 本年3月及び4月に特定の事業者のPBXを導入している利用者において、不正利用による被害が80件程度発生。(A社、B社) ※ さらに当該事業者が提供するPBXのうち、特定の型番の利用者に被害が集中している模様
  - 1か月に5～10件程度の頻度で発生。(C社)
  - 1か月に5件程度の頻度で発生。(D社)
  - 昨年に40件程度発生(E社)
  - 2か月に1件程度の頻度で発生(F社)
  - ここ数年被害は発生していない(G社・H社・I社)

### 被害額

- 本年の被害が総額数千万円程度にのぼる通信事業者もある。利用者の被害額は1件あたり数万円～数百万円程度。

### 被害の傾向

- IP電話の被害はやや減少傾向にある一方で、PSTN(固定電話網)への攻撃が増加傾向にある。
- 法人利用者(特に中小企業)における被害が中心で、個人利用者への被害は比較的少ない。

### 被害の原因

- PBXに不正アクセスが行われ、SIPサーバのIDとパスワードが窃用された。
- PBXに不正アクセスが行われ、任意の端末を組織内の端末になりすまされた、もしくは、特定の番号にかけた場合に国外に転送するよう設定された。
- 利用者サポートとして、ウェブ上でSIPサーバのID・パスワードの案内をしており、そこからID・パスワードが窃用された。
- また、今回報道になっているケースは特定の事業者の特定の型番にPBXに何らかの脆弱性があったものと推測されるが、事業者において調査中であり、詳しい原因までは分かっていない。

## 2. 第三者によるIP電話等の不正利用について③ (機器販売メーカーからの発表:平成27年6月25日・同年9月25日)

### 経緯

3月11日	➤ ある機器を使用している利用者より、通信キャリアから国際電話が頻繁に発信されていることについての確認の連絡があった旨の連絡
	➤ 被害拡大を防ぐため、利用者の了解を得て、リモートメンテナンスにより主装置側での海外発信規制(海外通話は、国際通信識別番号の「010」から始まる番号により発信されることから、「010」で始まる番号については発信できないようにしたもの)などの緊急措置を実施
3月下旬	➤ 被害が再発(不正アクセスを行った者は、「010」で始まる番号の前に「ある記号」を付けて発信していた模様)
	➤ 利用者に対し、通信キャリアに対してキャリア側での国際通話の発信規制をしてもらうよう案内 ➤ 対象機器のファームアップ <ul style="list-style-type: none"><li>● 記号付きの番号も発信できないようにする</li><li>● 一部、インターネット経由での対象機器へのアクセスを物理的に遮断</li></ul>
	➤ 4月3日以降、被害は確認されていない

### 発生原因

対象機器のセキュリティ上に不具合があった(不具合と被害との因果関係については不明)。

## 2. 第三者によるIP電話等の不正利用について④ (注意喚起:平成27年6月)

平成27年6月12日

### 第三者によるIP電話等の不正利用に関する注意喚起

IP電話をはじめとする電話サービスが第三者に不正利用され、利用者に高額な国際電話料金の請求がなされる問題が発生しています。こうした問題は、利用者がIP電話等の電話サービスを利用する際にインターネットに接続している通信機器(PBX(注)、IP電話対応のルータ等)におけるソフトウェアやハードウェアの設定の問題や、セキュリティ上の脆弱性を突いた「なりすまし」や「乗っ取り」による不正利用が原因であることが確認されています。

このため、IP電話等の電話サービスを利用する場合には、第三者による不正利用が行われないよう、ネットワークに接続している通信機器の設定状況を確認し、以下のようなセキュリティ対策を講じるようお願いいたします。

PBX等の通信機器や使用しているソフトウェアの設定状況を確認し、不要に外部からの接続ができる設定になっていないかを確認するとともに、不要な接続環境は削除する。

外部からの接続を許可している場合、「外部から接続する際のパスワード」や「各種設定や管理用のパスワード」について、第三者が推測しやすいパスワードや簡易なパスワードは設定しない。

必要に応じて、通信機器やサービスを提供している事業者、保守ベンダー等に対して次の点を相談する。

- (1)使用するソフトウェアについて、最新のバージョンにアップデートする等のセキュリティ対策を行う。
- (2)通信機器やソフトウェアにアクセスログを記録、保存する機能がある場合には、アクセスログを記録、保存するようにし、不審なアクセスの有無をチェックする。
- (3)電気通信事業者によっては、海外向けの電話番号への発信を規制するサービスを提供している場合があるので、国際通話を利用しない場合は、国際通話発信規制サービスの申込みを行う。
- (4)電気通信事業者によっては、IP電話等が不正利用された場合に通話の宛先となることが多い国／地域を公表していることがあるので、機器やソフトウェアの設定により、これらの国／地域への発信を制限する。

(注)

組織で複数の電話機を設置する場合に、施設内に設置・運用される電話交換機のこと。組織内の電話機同士で内線通話できるようにし、公衆回線との接続を行う目的で利用されるもの。

**【不正利用が確認されたケース】** PBXを利用している利用者において、PBXやこれに導入されているソフトウェアのセキュリティ対策が不十分な場合に、第三者がインターネット経由で利用者のPBX等にアクセスし、利用者になりすまして国際通話を不正に発信している。

IP電話を利用するために接続するルータのセキュリティ対策が不十分な場合に、第三者が接続のためのIDやパスワードを不正に入手し、利用者になりすまして国際通話を不正に発信している。

## 2. 第三者によるIP電話等の不正利用について⑤

### (第三者によるIP電話等の不正利用への電気通信事業者における対策について(要請))

IP電話等が第三者に不正利用され、利用者に高額な国際電話料金の請求がなされる問題が発生する中、総務省では、研究会の議論※1を踏まえ、平成27年7月7日、電気通信事業者に対し不正利用による被害防止のための適切な対応を講じるよう要請※2

※1 「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」(座長:佐伯仁志東大教授)で通信の秘密等との関係を整理

※2 要請は、電気通信事業者協会、テレコムサービス協会、日本データ通信協会テレコム・アイザック推進会議ほかの関係5団体を通じて実施

#### 総務省から電気通信事業者への要請内容

- 一般的なセキュリティ啓発、利用者等への国際電話サービスの利用休止案内、他の事業者との情報共有等に加え、不正利用が行われていると認められる場合に、電気通信事業者の判断により不正な国際電話発信を停止することなどの対策を要請。

#### 【不正な国際電話発信の停止等に関する具体的な対策】

- ① 利用者等に対し、ホームページへの掲載等により、接続・利用環境の確認、セキュリティ対策の強化等を要請する。
  - ※ PBX等の通信機器の設定状況を確認し、不要に外部からの接続ができる設定になっていないかを確認し、不要な場合は削除する。また、国際電話を利用しない場合には端末側で発信制限を行う。等
  - 外部からの接続を許可する場合、「外部から接続する際のパスワード」や「各種設定や管理用のパスワード」について、第三者が推測しやすいパスワードや簡易なパスワードは設定しない。また、使用するソフトウェアについて、最新のバージョンにアップデートする。通信機器にアクセスログを記録・保存する機能がある場合には、この機能を用いて不審なアクセスの有無をチェックする。等
- ② 契約者からの申請を受けた場合には国際電話の利用を速やかに休止する。
- ③ 国際電話をしばらく利用していない契約者回線等について、契約者に必要な案内を行い、国際電話の利用について契約者の意向を確認して国際電話の利用を休止する。
- ④ 不正利用の宛先となっていた国を公表し、契約者側の端末での発信制限を促す。
- ⑤ 国際電話の料金等を検知し、正規の利用者以外の者が利用していた蓋然性の高い場合には、その利用に係る特定の契約者回線からの国際電話の利用を休止する。
  - ※ 休止の措置を取る場合には、契約者に連絡を取り、契約者の同意を得ることが原則であるが、夜間・休日であって連絡を取れない等緊急性が高いと認められる場合には契約者の同意を得ずに国際電話の利用を休止する措置をとった上、速やかに契約者に対して休止した旨を通知
- ⑥ 国際電話の料金等を検知し、正規の利用者以外の者が利用していた蓋然性の高い場合に、正規の利用者以外の者からの国際電話の利用を防止する。
  - ※ 具体的には、不正利用されている発信元IPアドレスからの認証を一時停止することにより措置
- ⑦ 上記対策等では対応困難な場合、特定の国宛ての通信について専ら不正利用に用いられていると認められるときに、不正利用がなされている期間中、当該特定国当ての発信を一時的に規制する。

## 2. 第三者によるIP電話等の不正利用について⑥ (各電気通信事業者における対応状況)

- ▶ NTTコミュニケーションズは、不正な国際電話発信の停止等に関し、要請①～⑦の措置を導入済。
- ▶ NTT東西は、①利用者からの申込み当日に国際通話の発信規制を完了できるよう手続を迅速化、②利用者に連絡がとれなかった場合の緊急的な措置として、NTT東西の判断で利用者の国際通話の発信を一時的に規制する措置(利用者には事後に連絡)等を実施済。
- ▶ その他の事業者においても、総務省からの要請を踏まえ、具体的な対策を実施済又は検討中。



- 「通信の秘密」は、通信が人間の社会生活にとって必要不可欠なコミュニケーション手段であることから、表現の自由の保障を実効あらしめるとともに、個人の私生活の自由を保護し、個人生活の安寧を保障する（プライバシーの保護）ため、憲法上の基本的人権の一つとして、憲法第21条第2項において保障されているもの。
- 日本国憲法の規定を受け、電気通信事業法において、罰則をもって「通信の秘密」を保護する規定が定められており、電気通信事業法上「通信の秘密」は厳格に保護されている。

## 日本国憲法

第21条 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。

## 電気通信事業法

(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。

第179条 電気通信事業者の取扱中に係る通信（第164条第2項に規定する通信を含む。）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。

## 通信の秘密の侵害

通信の秘密を侵害する行為は、以下の3類型に大別されている。

- 知得＝「積極的に通信の秘密を知ろうとする意思のもとで知り得る状態に置くこと」
- 窃用＝「発信者又は受信者の意思に反して利用すること」
- 漏えい＝「他人が知り得る状態に置くこと」

## 通信の秘密の侵害に当たらない場合について

- 一般に、通信の秘密の侵害が許容される場合としては、通信当事者の有効な同意がある場合のほか、下記のような違法性阻却事由がある場合には、通信の秘密の侵害が許容される。

### (1) 正当業務行為に該当する場合

電気通信事業者としての業務を遂行するために必要な場合であって、①目的の正当性、②行為の必要性、③手段の相当性の要件を満たすことが必要。典型的には、課金や料金請求のために必要な場合において、最低限度で通信の秘密を侵す行為は、当該条件を満たすと考えられる。

### (2) 正当防衛、緊急避難に該当する場合

正当防衛の要件（①急迫不正の侵害に対して、②自己又は他人の権利を防衛するために、③やむを得ずした行為）、緊急避難の要件（①現在の危難の存在、②法益の権衡、③補充性）を満たす場合。典型的には、通信施設に対する攻撃に対応したり人の生命身体に対する危険を避けたりするために通信の秘密を侵すことが必要な場合等が挙げられる。

- ⑤ 国際電話の料金等を検知し、正規の利用者以外の者が利用していた蓋然性の高い場合に、その利用に係る契約者回線からの国際電話の利用を休止する。
- ⑥ 国際電話の料金等を検知し、正規の利用者以外の者が利用していた蓋然性の高い場合に、その者からの国際電話の利用を防止する。
- ⑦ その他の対応では困難な場合において、特定国宛ての通信について、専ら不正利用に用いられていると認められるときは、不正利用がなされている期間中、当該特定国宛ての発信を一時的に規制する。

## 1. 通信の秘密の侵害に該当するか

国際電話の料金、通信先の相手国(国番号)、発信元電話番号や発信元IPアドレスは、通信の構成要素として通信の秘密の対象となり得るものであり、これらを分析し通信の規制等の措置を行うことは、通信の秘密の窃用等に該当し得る。

## 2. 正当業務行為として違法性が阻却されるか

「正当業務行為」に該当するといえるには、

(1)目的の正当性、(2)行為の必要性、(3)手段の相当性を満たすことが必要であるところ、

(1)本件対策の目的は、電気通信事業者において、契約に基づく適正な課金・料金請求を行うことにより正規の利用者に対して電気通信役務を提供するとともに、通信事業を維持・継続するため、正規の利用者以外の者が正規の利用者になりすまし、不正に電気通信役務を享受することを防止することにより、電気通信役務の円滑な提供を確保することにあるから、目的の正当性を認めることができると考えられる。

(2)電気通信事業者においては、既に他の対策を実施しているところであるが、利用者の多くは、自ら被害を受けない限り具体的な行動には移りにくいと考えられるため、それら他の対策だけでは十分に対処できず、被害が発生しているため、必要性が認められる。

(3)分析の結果を本件対策以外に利用しない場合であって、必要な期間の対処に限る等上記目的にとって必要最小限の規制にとどまるものであれば、手段の相当性も認められる。

以上から、本件対策は正当業務行為として違法性が阻却されることが考えられる。

## 「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」(平成25年11月～)

サイバー攻撃が巧妙化・複雑化する中で、電気通信事業者が通信の秘密等に配慮しつつ、新たな対策や取組を講じていくことが可能となるよう、電気通信事業におけるサイバー攻撃への適正な対処の在り方について検討を行うことを目的として、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」(総合通信基盤局長及び政策統括官(情報通信担当)の研究会)を開催している。

### 構成員

#### <本会合>

(座長)	佐伯 仁志	東京大学大学院法学政治学研究科教授
(座長代理)	宍戸 常寿	東京大学大学院法学政治学研究科教授
	森 亮二	弁護士
	藤本 正代	情報セキュリティ大学院大学客員教授
	中尾 康二	国立研究開発法人情報通信研究機構 ネットワークセキュリティ研究所 主幹研究員
	木村 たま代	主婦連合会
	木村 孝	一般社団法人日本インターネットプロバイダー協会
	小山 覚	一般財団法人日本データ通信協会 テレコム・アイザック推進会議

#### <WG>

(主査)	宍戸 常寿	東京大学大学院法学政治学研究科教授
	衛藤 将史	国立研究開発法人情報通信研究機構ネットワークセキュリティ研究所 主任研究員
(主査代理)	森 亮二	弁護士
	木村 孝	一般社団法人日本インターネットプロバイダー協会
	小山 覚	一般財団法人日本データ通信協会 テレコム・アイザック推進会議
	齋藤 衛	株式会社インターネットイニシアティブサービスオペレーション本部セキュリティ情報統括室長
	丸橋 透	ニフティ株式会社 理事(法務・渉外担当)(兼)法務部長
	村主 亘	ソフトバンク株式会社 お客様相談室

### これまでの検討

- 平成26年4月……第一次とりまとめ公表
- 平成27年7月……IP電話不正利用対策に関する整理を公表
- 平成27年9月……第二次とりまとめ公表
- 平成27年11月……民間ガイドライン(※)において、本研究会における検討結果を反映

※ 「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」:通信4団体及び一般財団法人日本データ通信協会テレコム・アイザック推進会議から成る「インターネットの安定的な運用に関する協議会」で作成。

### 3. 「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」② (第二次とりまとめについて)

#### 「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」(平成25年11月～)(再掲)

サイバー攻撃が巧妙化・複雑化する中で、電気通信事業者が通信の秘密等に配慮しつつ、新たな対策や取組を講じていくことが可能となるよう、電気通信事業におけるサイバー攻撃への適正な対処の在り方について検討を行うことを目的として、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」を開催している。

平成27年9月9日、同研究会における議論を取りまとめた第二次とりまとめを公表。

#### 「第二次とりまとめ」における検討課題

##### ① C&Cサーバ等との通信の遮断

ISPが自社DNSサーバを通過する利用者のFQDN(※)を検知し、C&CサーバのFQDNの名前解決要求を遮断することについて、どのような場合に通信の秘密に属する情報(アクセス先のFQDN)の利用についての有効な同意と言えるか。

(※ FQDN (Fully Qualified Domain Name) : ホスト名及びドメイン名からなる文字列で、ネットワーク上のコンピュータを特定するもの。)

⇒ 特定の条件下で、約款に基づく包括的な同意であっても有効な同意として整理。

##### ② 他人のID・パスワードを悪用したインターネットの不正利用への対処

PPPoE認証のID・パスワードの不正利用の蓋然性が高いものについて、当該IDからのPPPoE認証を一時停止するとともに、そのID・パスワードを不正に利用されている利用者に対し、個別に連絡を取り、パスワードの変更を依頼することは、通信の秘密との関係上どのように整理が可能か。

⇒ 正当業務行為として整理。

##### ③ 脆弱性を有するブロードバンドルータ利用者への注意喚起

脆弱性を有するルータの利用者に注意喚起することは、不正アクセス禁止法、通信の秘密との関係上どのように整理が可能か。

⇒ 不正アクセス禁止行為には該当しないと整理。

⇒ 正当業務行為として整理。

##### ④ DNSの機能を悪用したDDoS攻撃に悪用されている名前解決要求の遮断

DNSAmp攻撃やランダムサブドメイン攻撃を防止するため、こうした攻撃に利用されるドメイン宛ての通信を遮断することは、通信の秘密との関係上どのように整理が可能か。

⇒ 正当業務行為として整理。

- **携帯電話番号の逼迫状況やM2M等向け番号需要の増大等を踏まえた携帯電話番号制度の在り方**について、平成27年6月18日に情報通信審議会(電気通信事業政策部会)に諮問
- 電気通信番号政策委員会をこれまで5回開催し、10月16日(金)に報告書がとりまとめられた。
- 10月27日の電気通信事業政策部会を経て、答申案について10月28日から11月26日までパブリックコメントを実施。本年中を目処に答申を受け、平成28年4月以降の制度化を予定

・車に搭載するテレマティクスやウェアラブル等、全国の広い範囲を移動し、常態的にネットワークにつながる必要があるような利用には携帯電話ネットワークが用いられる。

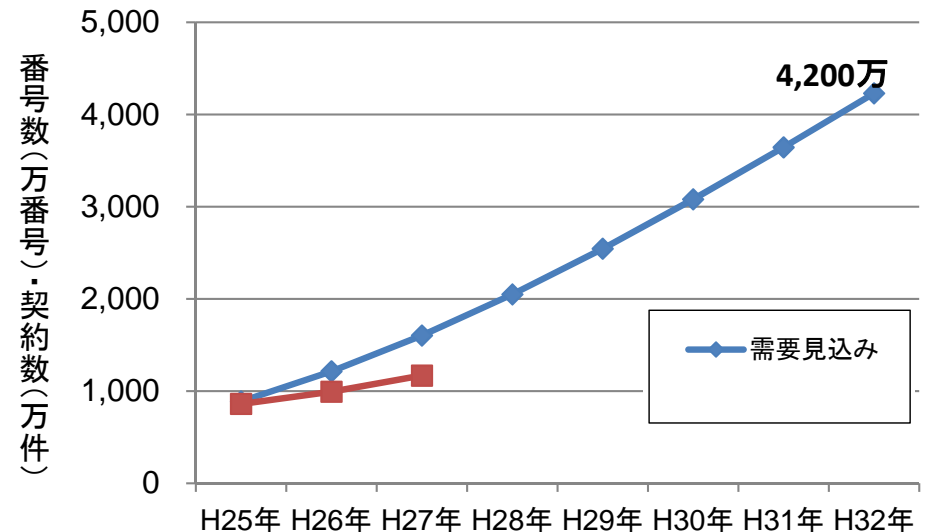
→ 携帯電話ネットワークにおいてM2Mが機能するためには、携帯電話番号が必要。

・宅内や工場内等で固定して用いられる利用(スマートメーターやATM等在庫管理など)の場合、特に都市部では、コストが相対的に小さいWi-Fi等の固定系ネットワークが用いられる場合が多い。

### M2Mの主な活用分野

<p><b>遠隔での使用状況等監視</b></p> <ul style="list-style-type: none"> <li>自動検針                     <ul style="list-style-type: none"> <li>スマートメーター</li> </ul> </li> <li>ビル環境管理</li> <li>構造物ヘルスマonitoring                     <ul style="list-style-type: none"> <li>橋梁モニタリング</li> </ul> </li> <li>遠隔機器監視                     <ul style="list-style-type: none"> <li>重機・工場用機械等の保守</li> </ul> </li> <li>遠隔健康管理・介護                     <ul style="list-style-type: none"> <li>在宅医療機器モニタリング</li> </ul> </li> </ul> <p><b>車両関係</b></p> <ul style="list-style-type: none"> <li>テレマティクス                     <ul style="list-style-type: none"> <li>交通情報・ナビ等の提供</li> <li>運行管理</li> </ul> </li> <li>配送管理                     <ul style="list-style-type: none"> <li>配送状況の把握</li> <li>コンテナ管理</li> </ul> </li> <li>車両位置情報管理                     <ul style="list-style-type: none"> <li>列車位置管理・運転士支援</li> </ul> </li> </ul>	<p><b>見守り・セキュリティ</b></p> <ul style="list-style-type: none"> <li>見守り(屋内)                     <ul style="list-style-type: none"> <li>ペット等の見守りカメラ</li> </ul> </li> <li>見守り(屋外)                     <ul style="list-style-type: none"> <li>子供等の位置情報通知</li> </ul> </li> <li>不正侵入・盗難防止</li> </ul> <p><b>自然環境の監視</b></p> <ul style="list-style-type: none"> <li>自動監視・警報                     <ul style="list-style-type: none"> <li>災害監視センサー</li> </ul> </li> <li>育成環境の最適化                     <ul style="list-style-type: none"> <li>農業センサー</li> </ul> </li> </ul> <p><b>決済関係</b></p> <ul style="list-style-type: none"> <li>在庫管理・決済                     <ul style="list-style-type: none"> <li>自販機・ATM等の在庫管理</li> <li>モバイルPOS</li> </ul> </li> </ul> <p><b>広告表示</b></p> <ul style="list-style-type: none"> <li>デジタルサイネージ</li> </ul>
--	---

M2Mに利用される携帯電話番号の需要予測



出典:「固定電話の番号区画等に関する調査研究 報告書」  
(平成27年3月NTTアドバンステクノロジー株式会社)より作成

## 4. 「携帯電話番号の有効利用に向けた 電気通信番号に係る制度の在り方」について② (電気通信事業政策部会 答申(案)概要)

### □ 「020」番号帯の創設 -IoT社会において、M2M等展開を後押しする等の大きなメリット-

#### 【メリット1】 M2M等向けの大きな番号需要に対応

(背景) M2M等に特化した番号は人が直接使わないため、桁が長くても利用者に不便が生じない。設備改修コスト等を考慮し、当初は11桁とし、近い将来桁増しすることで、大きな番号需要に対応可能(※)。

※ 仮に020番号を090等より2桁長い13桁とすれば最大80億番号を創出可能。

(メリット) 大きな番号空間を生かし、随所で短期間に大きな番号需要が発生するM2Mの特性に余裕を持って対応する番号割当てが可能。

#### 【メリット2】 M2Mの展開加速・コスト削減

(背景) 現在、M2M等向けに使用されている090/080/070番号は、人と人の通話にも使うため、番号を事業者に割り当てるにあたり通話品質の確保や緊急通報の確保などの義務を課しているが、これらを満たすための関係者間調整や設備の手当等に準備 期間やコスト負担が伴っている。

(メリット) 専らデータ通信向けに特化した020番号について、これら音声通話のための要件を設けず、IoT/M2Mの展開加速やコスト削減を促進できる。

#### 【メリット3】 携帯電話利用者の利便性確保

(背景) IoT社会における新しい携帯電話番号需要の多くはM2Mが占めると考えられており、090等をそのまま使っていくと平成30年頃には枯渇することが想定される。

(メリット) 需要が大きいM2M向けに大きな番号空間を持つ020番号を使うことにより、

・携帯電話向けには慣れ親しんだ090/080/070を長く使い続け、

・M2M等端末向けの誤発信による混乱も防止するなど、

利用者の利便性向上に資する。

### □ その他の主な論点

○ 既に090/080/070を使用しているM2M等について、サービス利用者等への過度な負担を防ぐため、サービスや機器の更改時期を捉えたM2M等専用番号への移行を促す。

○ M2M等の専用番号導入により、090/080/070番号のひっ迫は緩和され则认为られるが、隣接する060番号は、将来的に携帯電話番号として使用することも見据え留保する。

### ① 書面の交付義務

(改正後電気通信事業法第26条の2)

電気通信事業者に対し、契約締結後に書面を作成し遅滞なく交付することを義務付け。詳細は省令で規定。対象サービスは総務大臣が指定

### ② 初期契約解除制度

(改正後電気通信事業法第26条の3)

①の書面受領後等の8日間に利用者からの一方的な契約の解除を可能とする制度を導入。対象サービスは総務大臣が指定(①の対象より狭い範囲)

### ③ 不実告知等の禁止

(改正後電気通信事業法第27条の2第1号)

契約の重要事項について、故意に事実を告げず、又は事実でないことを告げる行為を禁止

### ④ 勧誘継続行為の禁止

(改正後電気通信事業法第27条の2第2号)

契約を締結せず又は勧誘を受けないことを希望する利用者に対する再勧誘を禁止。

### ⑤ 代理店に対する指導等の措置義務

(改正後電気通信事業法第27条の3)

電気通信事業者に対し、代理店への指導等の措置を行うことを義務付け。詳細は省令で規定