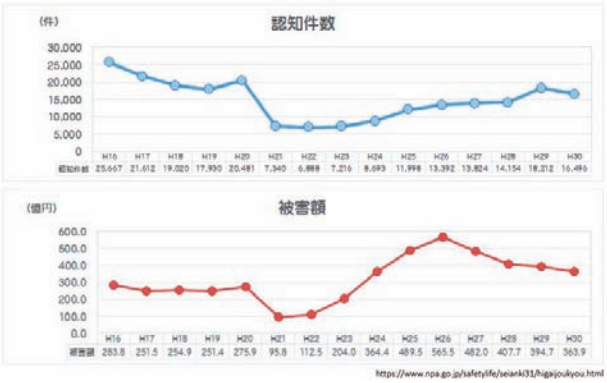
迷惑電話対策に関する標準化動向

NTTネットワークサービスシステム研究所　永徳（えいとく）　はるか

1. はじめに

近年、日本国内における迷惑電話の被害が拡大している。迷惑電話の種類としては、いたずら目的の電話やしつこい勧誘の電話、機械的に多数のユーザへ発信を行うロボコールや、近親者や公的機関を騙った特殊詐欺電話など多岐にわたっている。特に特殊詐欺については、年々手口が複雑化・巧妙化しており、現在も年間400億円程度の被害が発生するなど社会問題化している（図1）。

このような迷惑電話被害は日本独自のものではなく、海外においても深刻な社会問題として扱われており、米国を中心に迷惑電話ソリューションサービスを展開しているFirst Orion社の調査によると、米国内の携帯電話で2017年に3.7%だった迷惑電話が2018年には29.24%に達した。このような事態を受け、米国のFCC（Federal Communications Commission）は2017年11月に、ロボコールの可能性がある電話をキャリアの判断で切断できる新たな規則を発表した。具体的には、無効な番号（偽の市外局番の番号など）やサービスプロバイダとつながりのない番号、料金を現在請求されていない番号及び受信しか行わない設定の番号から発信された通話を切断することが認められている。また、



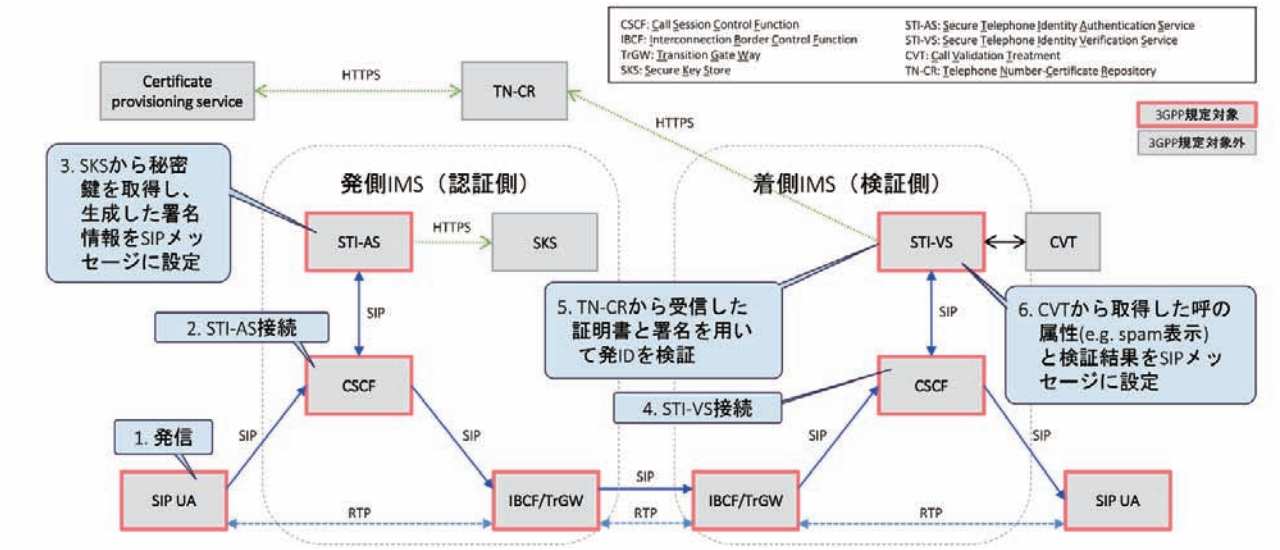
■図1. 特殊詐欺被害の状況（警察庁ホームページより抜粋）

2019年には、SHAKEN（Signature-based Handling of Asserted information using toKENs）と呼ばれる署名ベースの発信者ID検証システムへの対応を全米キャリアに義務付けることがFCCによって発表されるなど、国を挙げて迷惑電話対策に取り組んでいる。ヨーロッパにおいても迷惑電話被害の増加は深刻な問題であり、ユーザは迷惑電話番号データベースへの問合せ機能を持つアプリなどを利用して、迷惑電話への対策を行っている状況である。

表1に示すように、多くの標準化団体が迷惑電話対策に

■表1. 各標準化団体での検討状況

標準化団体	対策種別	サービス名、検討名、仕様タイトルなど	参考文献
IETF	発ID検証	発ID検証方式：In-band方式	RFC 8224
		転送呼向け発ID検証	draft-ietf-stir-passport-divert
		発ID検証方式：Out-of-band方式	draft-ietf-stir-oob
	着信者へ発ID情報通知	SIP Call-Info Parameters for Labeling Calls	draft-ietf-sipcore-callinfo-spam
	受信拒否通知	A SIP Response Code for Unwanted Calls	RFC 8197
		A SIP Response Code for Rejected Calls	RFC 8688
3GPP	発ID検証	署名を用いた発ID検証 SPECTRE（eSPECTRE）	TS 24.229
	着信者へ発ID情報通知	着信者への発信者情報提供（eCNAM）	TS 24.196
		Call Whisper	TS 22.173
ITU-T	詐欺電話対策	詐欺電話対策フレームワーク	X.1231 Supplement 33
	IPマルチメディアスパム対策フレームワーク	マルチメディアスパム対策フレームワーク	X.1245
		VoIPスパム対策フレームワーク	X.1245 Supplement 11
		発ID偽装対策	X.1245 Supplement 28
	CS迷惑電話対策	CS発呼シナリオにおける迷惑電話対策	X.1246
ETSI	着信者へ発ID情報通知	着信者への発信者情報提供（eCNAM）	ETSI TS 124 196（3GPP TS 24.196）
ATIS	フレームワーク	Signature-based Handling of Asserted information using toKENs (SHAKEN)	ATIS-1000074
	SHAKEN運用	Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management	ATIS-1000080



■図2. SHAKENアーキテクチャ

関する検討を行っており、これらは時系列的に、スパム電話への対策、発ID偽装対策、発信者情報通知によるロボコール対策、特殊詐欺電話対策、の4つに大別できる。本稿では、迷惑電話対策に関する標準化の状況と規定内容について説明する。

2. スパム電話対策に関する標準化状況

スパム対策については、2010年頃からITU-TのSG17がIPマルチメディアアプリケーション（email、インスタントメッセージ、VoIP等）におけるスパム対策方式を検討しており、X.1245としてフレームワークが規定されている。X.1245では、スパムの分析方式としてSource analysis method、Characteristics analysis method、Content analysis methodの3つを提唱している。Source analysis methodは、評価情報やスパム履歴などの送信元情報を分析してスパムを識別する方式であり、送信元識別子にはIPアドレスやドメイン名、電話番号、ユーザ識別子を利用可能である。Characteristics analysis methodは、通信の特性（同時大量配信メールやインタラクティブ性のない通信など）からスパムの可能性を検知する方式であり、チューリングテストやグレイリスティングが最も一般的な対策技術である。最後のContent analysis methodは、通信のコンテンツ（テキスト、音声、画像等）の分析によりスパムを識別する方式である。またX.1245では、スパム対策フレームワークをCASF（core anti-spam Functions）、SASF（sender-side anti-spam Functions）、RASF（recipient-side anti-spam Functions）、SRF（spam recipient Functions）の4つの機能群の組合せによって定義している。CASFは、スパム対策ポリシの管理やSASF／RASFの制御、プロトコル/コンテンツの特性分析によるスパムの識別とフィルタリング／ブロックの機能を有する。SASF／RASFはメッセージの送信者側／受信者側のスパム分析機能及びスパムフィルタリング／ブロック機能で構成され、CASFより取得したスパム対策ポリシを適用してスパム対策機能を実行する。SRFはメッセージ受信端末におけるスパム対策機能を指し、プロトコル／コンテンツ分析機能、フィルタリング／ブロック機能、ローカルのスパム対策ポリシで構成されている。SRFはユーザ自身、もしくはサービスプロバイダから提供される情報に従ってスパム対策を実施する。

3. 発ID偽装対策に関する標準化状況

その後、VoIP（Voice over IP）サービスの普及に伴い、発IDを偽装したスパムや詐欺が増加したことを受けて、2017年頃から各標準化団体では発ID偽装対策に関する検討が盛んに行われてきた。

3.1 ATISの検討状況

発ID偽装対策のためのフレームワークはATIS（The Alliance for Telecommunications Industry Solutions）がSHAKENとして規定している（図2）。このSHAKENフレームワークでは、発側IMS（IP Multimedia core network Subsystem）網が署名を発行し、着側IMS網が署名の検

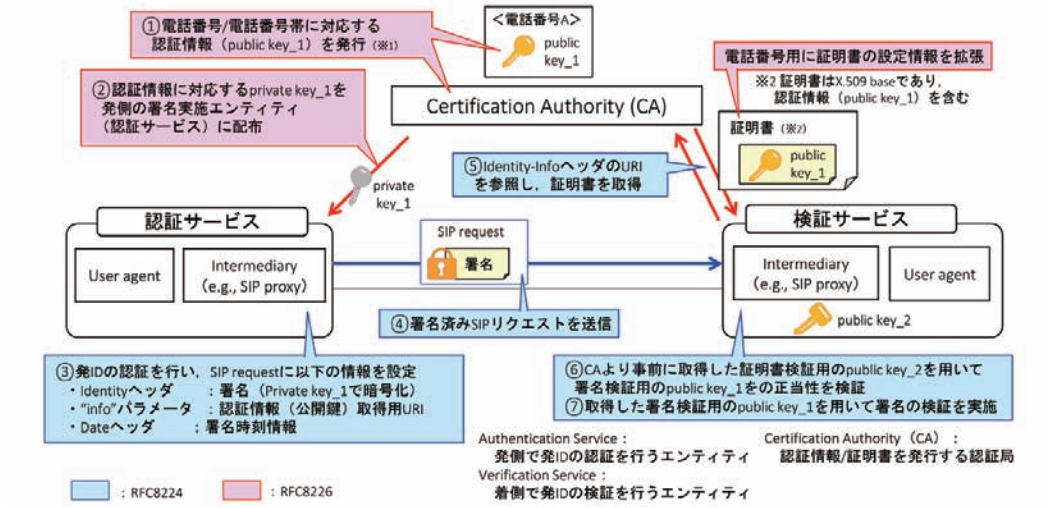
証を行うことで発ID偽装対策を可能としている。

3.2　IETFの検討状況

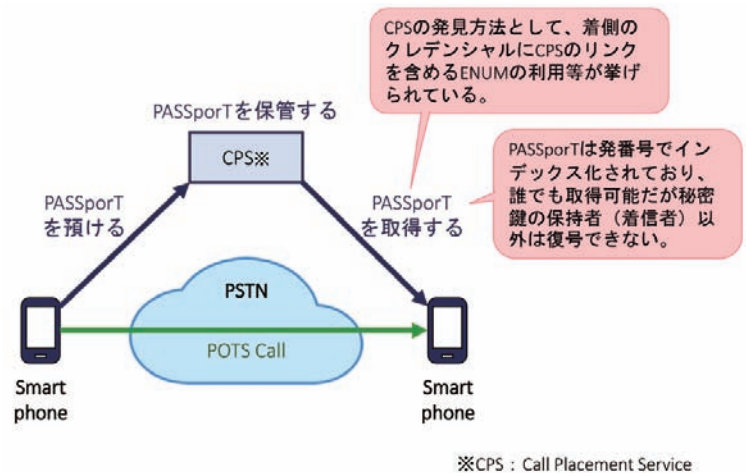
IETFのSTIR WGでは、RFC 8224においてIdentityヘッダを定義しており、このヘッダに署名情報を設定し、発側IMS網から着側IMS網へ署名情報を送信して発ID偽装対策を行う方式（in-band方式）を規定している（図3）。この時、Identityヘッダに設定される発信者の署名情報の形式はPASSporT（Persona Assertion Token）としてRFC 8225で規定されている。PASSporTはJSON Web Token及びJSON Web Signatureを用いた署名情報として定義されており、この署名情報は発端末が送信するSIPリクエストのToヘッダ、FromヘッダもしくはP-Asserted-Identityヘッダ及びDateヘッダから生成される。また、IETFでは、中継網で呼設定信号に付与されたメタデータを削除するような場合であっても端末間で認証情報を交換するため、外部データベースを用いて署名情報を取得する方式（out-of-band方式）に関しての検討も行っている（図4）。この方式では署名を実施するIMS網が外部のCPS（Call Placement Service）にPASSporTを預け、検証を実施するIMS側がCPSからPASSporT情報を取得して検証を行う。out-of-band方式は現在WGでの検討が終わり、IESGレビュー中である。

3.3　3GPPの検討状況

3GPPでは、迷惑電話の防止に取り組む米国の強い要請によってIMS網における発ID偽装対策が検討され、IMS信号仕様であるTS 24.229にSPECTRE（リリース14）／



■図3．in-band方式概要



■図4．out-of-band方式概要

eSPECTRE（リリース15）として導入されている。3GPPにおける検討は米国主導であったため、ATISとSIP Forumが共同で検討したSHAKENアーキテクチャをベースとしている。

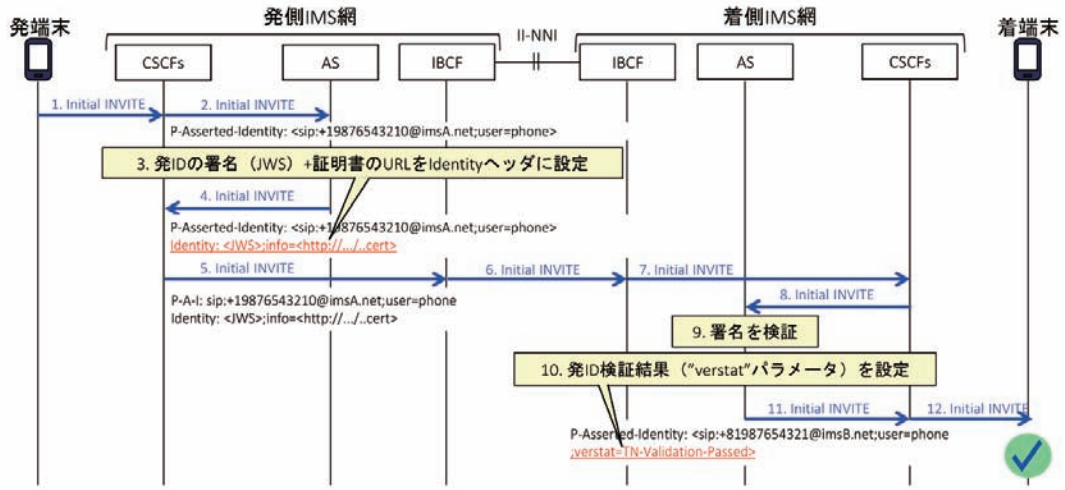
SPECTRE／eSPECTRE仕様では、端末への機能通知や発IDの署名情報の設定機能と発ID検証機能、また、着端末における網へのスパム呼通知機能等の信号仕様が規定されている。

端末への機能通知機能に関しては、端末がIMS登録を行う際に、IMS網がREGISTERに対する200レスポンスのFeature-Capsヘッダに“+g.3gpp.verstat”を設定することで発ID検証機能をサポートしていることを通知する。

発ID署名と検証に関して、3GPPリリース14では**図5**の手順が規定されている。発端末がInitial INVITEリクエストもしくはMESSAGEリクエストを送出した時、発側IMS網のCSCF（Call Session Control Function）はAS（Application Server）に対して発IDの署名を要求し、署名を要求されたASは、発ユーザの証明を行い、署名情報と証明書の取得先URIを設定したIdentityヘッダを返送する。発側IMS網のCSCFはこのIdentityヘッダを含めたリクエストを送信し、当該ヘッダが設定されたリクエストを受信した着側IMS網のCSCFは、自網のASに対して署名の検証を要求する。ASはIdentityヘッダの情報から証明書を取得して、署名情報を用いて発IDの検証を実施し、P-Asserted-Identityヘッダもしくは Fromヘッダに、検証結果を設定した“verstat” tel URIパラメータを設定する。この時、検証成功の場合は“TN-Validation-Passed”、検証失敗の場合は“TN-Validation-Failed”、未検証の場合は“No-TN-Validation”をverstat tel URIパラメータに設定し、その後、検証結果を着端末へ通知する。

リリース14では主にASによる発IDの署名及び検証に必要な機能が規定されたが、リリース15では発IDの検証機能を強化することを目的として、発ID検証時の発IDの認証（attestation）レベルの識別、IBCF（Interconnection Border Control Function）における発ID署名情報の設定及び検証、着信転送時の転送元電話番号の検証、の3つを可能にすべく機能拡張が実施された。

着端末における網へのスパム呼通知機能に関して、SPECTRE／eSPECTREでは、着信者が受信した呼を迷惑電話だと判断した場合に、それを着IMS網に通知するレスポンスコードとして“607（Unwanted）”を規定している。“607（Unwanted）” はINVITE／CANCEL／BYE／SUBSCRIBE／NOTIFY／MESSAGEリクエスト等に対するレスポンスとして設定可能であり、“607（Unwanted）”を受信したサービスプロバイダは、着信者が管理するブラックリストに、報告された発IDを登録し、再度受信した際にブラックリストの情報を利用してトレースバックや政府への通知に利用することができる。また、中間エンティティ（分析エンジン等）で迷惑呼と判断された場合に利用されるレスポンスコードとして、“608（Rejected）”が現在IETFにて検討されている。“608（Rejected）” はIMS網による切断となるため、クレームの連絡先を含めたCall-Infoヘッダを設定することが想定されている。



■図5. SPECTRE仕様における署名情報の設定手順及び検証結果の通知手順

4. 発信者情報の通知に関する標準化状況

北米ではFCCの要請により迷惑電話対策の検討が進められており、3GPPリリース14では北米のATIS SHAKENアーキテクチャをベースに発ID検証及び迷惑呼の報告機能が規定された。その後、北米でのロボコール対策要件に、ユーザが発信者を識別するための「電話番号以外の発信者情報の着信者への通知」が含められたことを受け、3GPPにおいても当該サービスをIMS付加サービスとして検討することとなった。

3GPPでは、着側IMS網が外部データベースから発信者情報を取得して着ユーザへ提供するeCNAM Enhanced Calling NAMe）サービスをTS 24.196に規定している。

eCNAM仕様では、SPECTRE／eSPECTREによって発IDの検証が成功し、P-Asserted-Identityヘッダの“verstat” tel URIパラメータに“TN-Validation-Passed”が設定されている場合、着側IMS網のeCNAM ASが外部データベースに問い合わせを実施し、取得した発信者情報をリクエストのFromヘッダ、P-Asserted-Identityヘッダ、Call-Infoヘッダに設定して着端末へ通知する。

IETF draft-ietf-sipcore-callinfo-spamでは、着IMS網や着ユーザが迷惑電話を判別するための情報（発信者や呼のタイプ、信頼度、補足説明等）を通知することを目的としてCall-Infoヘッダの拡張が現在も検討されている。

5. 詐欺電話対策に関する標準化状況

2019年になって、ITU X.1231 Supplement 33では、詐欺電話に対するセキュリティフレームワーク及び詐欺電話に対する最適解を提供することを目的として詐欺電話の事例収集・特性分析を実施し、必要機能を明確化した上で詐欺電話対策システムの機能構成と対策プロセスを提示している。

このフレームワークにおいて、通信ネットワークを利用した詐欺では、可能な限り多くの対象者に電話をかけること及び無登録の発信者番号や非通知着信等を用いて警察の捜査の手が及ばないようにする傾向があることが示されている。また、物理的特性、発信者番号の特性、着信時の特性については**表2**の傾向があることが示されている。

6. おわりに

電話サービスは今や社会に十分普及したが、スパムや詐欺などの迷惑電話被害の増加が近年社会問題となっている。2010年頃から、多くの標準化団体が迷惑電話対策に関する検討を行い、スパム対策、発ID偽装対策、発信者情報通知に関しては信号手順を規定している。詐欺電話対策に関してはフレームワークの規定が完了しており、今後の更なる検討が期待される。

■表2. 特殊詐欺電話の特徴

No.	通話の物理的特性	概要
1	架電の頻度	数を撃てば当たる狙いで，詐欺師の電話番号からの発呼頻度は，正当なユーザーに比べ高い．
2	着信の分散	正当なユーザーの平均値を上回る呼出し番号数や初回着信の多さから，詐欺師の発呼先は散らばりがち．
3	通話時間	正当なユーザーの通話時間に比べ，詐欺電話は受信者に認識されがちで，平均数秒で終了する通話が多い．

No.	発信者番号の特性	概要
1	特定の公共番号	公によく周知された番号は受信利用が主目的であり，当該番号は詐欺師のなりすまし発信の可能性が高い．
2	番号の非通知	特殊な方法で発信者番号を隠蔽し，ブロック機能の回避および受信者側に証拠が残らないようにする．
3	異常信号	位置情報を隠蔽する異常信号の発生は，発信者の違法行為への関与が疑われる．(例) 国番号・番号桁違い

No.	着信時の特性	概要
1	キーボードの使用	受信者側における電話機のキーボード(キーパッド)使用の有無が，詐欺電話を判別する重要な特徴となる．
2	録音済み音声	事前録音した音声ファイルを使用し人件費を減らす詐欺師もいる．開始数秒の音声サンプルが判別に有効．
3	通信手段の組合せ	多くの詐欺師は電話を通信手段にしない．複数の詐欺対策技術の組合せと更新により，障害を減らせる．