TTC技術レポート
Technical Report

TR-1104

ECC Report 338
CLI Spoofing

Technical Report on CLI Spoofing
published by ECC NaN

第 1.0 版

2023 年 9 月 4 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

目　　次

I. はじめに

近年の電気通信網の IP 化にともない、従来、加入者線に対応して固定的であった CLI（Calling Line ID）は柔軟に設定することが可能となり、利便性の向上とともに、その反面、CLI Spoofing（発番号なりすまし）が国内でも、国際的にも問題となり、活発に議論されている。CEPT（欧州郵便電気通信主管庁会議）においても、その配下の ECC（Electronic Communications Committee）で CLI Spoofing の検討が進められ、CLI Spoofing について、欧州各国の対応の調査、及び、米国で導入されている STIR/SHAKEN を含む技術的な解決についてまとめたレポートを 2022 年に発行した。

CLI Spoofing の問題に対し、現状問題や各国の対応、また論点をより広く理解していただくために、番号計画専門委員会では、CEPT ECC 発行の ECC report 338 を翻訳し、本テクニカルレポートとして発行する。これらの内容は、CLI Spoofing に関する検討に資する情報として活用いただくことにより、現代社会における電気通信番号の理解に大いに役立つものと思われる。

本レポートの冒頭にあるように、現在は音声通信を中心に進められているが、今後はテキストメッセージング等への適用に議論は発展していくものと考えられる。今後の展開を想定しつつ、一読いただければ、今後の更なる検討のための一助になればと考えている。

(*1)原文は ECC NaN の発行ドキュメントとして公表されている。また、翻訳文では、担当者が重要と思われる箇所を**太字**にしている。

https://docdb.cept.org/document/28558

II. 作成担当

番号計画専門委員会

III. 改訂の履歴

版　数	制　定　日	改　版　内　容
第 1 版	2023 年 9 月 4 日	制定

ECC Report 338

CLI スプーフィング

2022 年 **6** 月 **7** 日に承認

0　エグゼクティブサマリー

近年、Calling Line Identification (CLI) スプーフィングが増加している。IP ベースのネットワークへの移行によって、そのような行為が容易になったことが主な要因の 1 つである。それにもかかわらず、多くの国では依然として従来のネットワークと IP ベースのネットワークが共存しており、そのため CLI スプーフィングのすべての問題を解決する唯一の解決策を見出すことは困難な状況である。このレポートでは、この点に関し CLI スプーフィングに対抗するため、複数の管轄区域における現在の規制とさまざまな技術的実践をレビューする。続いて、検討可能な解決策を展開するための 2 段階または 3 段階のアプローチを提案する。

短期的には、トラフィックのパターン分析により、問題の一部が軽減される可能性があるが、その方法は一般的にリアルタイムの解決策ではない。国レベルでも、ITU や BEREC などの国際/地域フォーラムでもその両者において、CEPT 行政は、業界団体が CLI スプーフィングと戦うためのトラフィック分析と情報共有に関する議論を促進するよう対応していく必要がある。また、たとえば CLI が上書きされるのか、または、通信をブロックするのかどうかを確認するために、ユーザが提供した CLI が発信元のサービスプロバイダによって検証されることを、規制要件として要求する必要がある。中継サービスプロバイダには他の要件も課される場合がある。

中期的には、最低限として、国内通話が現在よりも信頼できることを要求する、国レベルでの解決策が導入される可能性がある。しかしながら、EU 外から発信された通話が EU 内で終端する場合の料金が通常より高いため、より低い料金となるために、実際には外部から発信された通話が EU 内から発信されたように表示されることを防ぐメカニズムが必要である。これは、EU の通信事業者の収益に影響を与えている。

長期的な解決策として、Secure Telephone Identity Revisited (STIR)/Signature-based Handling of Asserted information using toKENs (SHAKEN) などの技術、またはその他の技術を実装することができる。 STIR は、電話番号が通話開始時に証明および署名され、通話着側で検証されるという点で、特定の番号を使用する発信者の承認の検証を容易にすることを目的としている。ただし、このような技術には一般にオール IP 環境が必要であり、ネットワークがそこに到達するには今から数年かかることが予想される。

略語	説明
A2P	Application-to-Person
ARCEP	フランス電気通信・郵便・出版流通規制機関
ATIS	米国電気通信産業ソリューション連合
BEREC	欧州電気通信規制当局
BIPT	ベルギー郵便電気通信庁
CEPT	欧州郵政電気通信行政会議
CLI[1]	発信回線識別子
CPN	発信者番号
CRL	証明書失効リスト
CVT	通話検証処理
DDI	直接ダイヤルイン
DLT	分散型台帳技術 (ブロックチェーンなど)
ECC	電気通信委員会
ECNO	電気通信網事業者
ECSP	電気通信サービスプロバイダ
EECC	欧州電子通信コード
ePR	e プライバシー規制
ETSI	欧州電気通信標準化機構
EU	欧州連合
FCC	米国連邦通信委員会
GDPR	一般データ保護規則
GMSS	全地球移動衛星システム
GW	ゲートウェイ
HTTP	HyperText Transfer Protocol

[1]このドキュメントでは、CLI は発信元の他種類の識別子を参照するためにも使用される。

略語	説明
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Service Digital Network
ITAKT	ノルウェー国家電気通信産業犯罪防止組織
ITU-T	国際電気通信連合電気通信標準化部門
LEA	法執行機関
Nkom	ノルウェー通信庁
NP	番号ポータビリティ
NRA	国家規制当局
PBX	構内交換機
P2P	Person-to-Person
PSTN	公衆交換電話網
RFP	提案依頼書
ROA	電気通信事業経営を政府から認可された政府以外の機関。国際電気通信条約上のキャリア（電気通信事業者）
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SMPP	Short Message Peer-to-Peer
SMS	Short Message Service
SPC	Service Provider Code
SOLID	Social Linked Data
SS7	ITU-T 共通線信号 No.7
STI	Secure Telephone Identity
STI-AS	STI - 認証サービス
STI-CA	STI - 認証局
STI-GA	STI - 統治当局
STI-PA	STI - ポリシー管理者
STI-VS	STI - 検証サービス

略語	説明
STIR	Secure Telephone Identity Revisited
TKG	Telekommunikationsgesetz、ドイツ電気通信法
USD	ユニバーサルサービス指令
VoIP	Voice over IP

1　序章

従来、公衆交換電話網 (PSTN) における発信、転送、及び、発信回線識別子 (CLI)の表示は、電気通信事業者 (ECNO) の単独の責任と管理であり、 CLI を操作する場合は遠隔からの特殊な機器が必要であった。このような安全な環境では、音声およびメッセージングサービスでエンドユーザに表示される CLI の信頼性が高く、必要に応じて中継ネットワークを介し、発信元ネットワークから終端ネットワークまでのサプライチェーンが構築されている。

レガシーネットワークからの移行により、インテリジェンスがネットワークエッジに移行し、より洗練されたエンドユーザデバイスとアプリケーションにより、エンドユーザは　CLI を操作できるようになり、従来のプレーヤーに加え、更に新規のプレーヤーが参入するサプライチェーンに拡張された。同時に、 CLI の概念を熟知しない、一般的には小規模である新規参入通信事業者の多くが市場に登場し、インターネットプロトコル (IP) に基づいた音声およびメッセージング サービスも提供している。

これらの発展により、**発信者から着信者までの通話/メッセージを処理するための「チェーン」が長く複雑になり、CLI の整合性を維持することがより困難**になっている。

CLI のルールを明確にすることは市場にとって重要である。ECC 勧告 (19)03「発呼側識別および発信側識別における信頼性を高めるための措置 (Measures for increasing Trust in Calling Line Identification and Originating Identification) 」 [1]

ECC レポート 248「CLI 使用の進化 – サービス提供から番号の使用権の切り離し(Evolution in CLI usage – decoupling of rights of use of numbers from service provision) 」 [2]には、**悪意のある目的で使用されない場合は、エンドユーザにとって利点となる、柔軟な CLI の使用に関する詳細情報が含まれている。**このレポートは、 CLI 検証技術を必須にすることを推奨している。代替のオペレータは、エンドユーザが　CLI として提示された番号を使用する権利を持っていることを保証するための検証手段を提供する必要がある。

ECC レポート 275「電気通信サービスの国際詐欺と悪用における E.164 番号の役割 (The role of E.164 numbers in international fraud and misuse of electronic communications services) 」 [3]では、 **CLI スプーフィングを、発信者、発信側ネットワーク、および/または中継ネットワークが表示される情報を操作できるようにする技術**と説明している。着信者を騙して、通話/メッセージが別の人、組織、または場所から発信されたものであると思わせることを目的として、 CLI フィールドに使用する。 CEPT 諸国では、CLI スプーフィングによる消費者被害の事例がますます増加している。　CLI スプーフィングに基づくさまざまな詐欺事件については、ECC レポート 275 で説明されている。詐欺師は、エンドユーザが従来から CLI 情報は正しいと信頼している点を利用し、CLI スプーフィングを行う。。通常、表示される　CLI は、着信者が使い慣れている形式の地理的識別番号またはモバイルの E.164 番号である。　CLI スプーフィングでは、表示される番号は、割り当てられた番号、未割り当ての番号、または国内番号計画に存在しない番号である可能性がある。

より最近では、 EU 内の携帯電話および固定電話の着信料の低下の傾向に関連し、高い着信料を逃れるため、**EU 内の通信時に適用される低い着信料を利用する目的**で、**非 EU 国の番号から発信**された通話またはメッセージで、**非 EU 国の通信事業者や EU の中継事業者により CLI 操作**が行われている。

ルールの明確化は重要であるが、エンドユーザを誤解させるため、意図的に CLI を操作する一部の攻撃者を阻止するには十分ではない。国際音声電話およびメッセージングシステムは複雑であるため、これらの

悪者を特定して制裁することは困難である。したがって、追加の対策を検討する必要がある。

このレポートでは、さまざまな**解決策の長所と短所、スプーフィングの影響を軽減するためのさまざまな解決策の運用への影響、展開の側面、および国際的な側面**について取り上げる。これらの内容は、ECC レポート 275、セクション 11.1 と整合している。

最後に、理解のために補足すると、一般的なユーザは、「正しい」（つまり、有効で正当な） CLI による通話またはメッセージと、「信頼できる」通話またはメッセージとの違いを必ずしも認識しているわけではない。技術を使用すると、 CLI が一定レベルの信頼を確保できるようになるが、それは発信者が必ずしも善意を持っていることを意味するわけではない。

2　スコープ

ECC レポート 275 の検討範囲は、エンドユーザが被害者となる CLI スプーフィングのケースに限定されている。**CLI スプーフィングは、ECC は通信事業者にも悪影響が及ぶ可能性**があり、発生する問題は音声通話やメッセージング サービス (SMS など) にも関連しており、このレポートではその点に関して認識している。

実際、ショートメッセージサービス (SMS) などのメッセージングサービスでは、CLI としての E.164 番号とショートコードの使用も出現しており、さらに増加している。 CLI 情報のルーティングと送信のために、SMS サービスプロバイダは通常、ITU-T 共通線信号 No.7 (SS7) と IP ベースのプロトコル (ショートメッセージ peer to peer (SMPP) など) の両方を利用しており、それにより、サプライチェーンの中で、CLI フィールドを変更できるアクターの数が増加している。近年、特にビジネス関連の SMS サービスの分野で、SMS の革新的な使用が増加している。 CLI フィールドで使用する英数字は大幅に増加している。スマートフォンでは、SMS やその他の種類のメッセージングにハイパーリンクが含まれる可能性があり、これがフィッシング詐欺の増加や、高額な料金の電話番号へのコールバックを招く可能性がある。

上記を理解した上で、このレポートでは、**音声通話にのみ関連する CLI スプーフィングに対処するための規制上の取り組みと、技術的解決策を調査および評価する**。

3　定義

用語	意味
CLI スプーフィング	通話やメッセージの処理に介入する着信側やネットワークオペレータを騙す目的で、通話やメッセージを処理する発信側やネットワークオペレータが CLI フィールドに表示される情報を、通話またはメッセージが別の人、団体、または場所から発信されたものであるかのように操作可能にする技術。
発信者	通信 (通話またはメッセージ) を開始する当事者。
着信者	通信（通話またはメッセージ）を受信する当事者。
認定オペレータ	公共通信サービスまたは放送サービスを運営し、当該機関の本部がその領域内に位置する加盟国、または、このオペレータに自国の領域内で電気通信サービスを確立および運営する権限を与えた加盟国によって ITU 規約第 6 条に規定された義務が課されるオペレータ。
ワンギリ	通常、自動化された手法にて、詐欺師が広い範囲の番号に対して大量の非常に短い通話を試みる手法。通話による攻撃の場合、これらの通話は 1 ～ 2 回の呼び出し音の後に切断されるため、エンドユーザのディスプレイには不在着信として表示される。

4　CLI スプーフィングに対抗するための現行規制の実践

多くの国では、CLI スプーフィングの阻止と対抗を目的とした規制を導入している。下記にいくつかの実践を示し、それらを考察する。

4.1　ベルギーの取り組み

4.1.1　CLI ガイドライン

2020 年 12 月 4 日、ベルギー郵便電気通信庁 (BIPT) は CLI ガイドラインを発行した。 BIPT は、このガイドラインの発行により不正行為を減らすことに加えて、通話が開始された瞬間から通話が終了するまで、CLI の使用と表示に関し、業界とエンドユーザにさらに明確な情報を提供したいと考えている。そのため、 CLI の正確性を保護し CLI の信頼性を高めることを目的として、コールルーティングを管理する 4 つの原則を BIPT は提唱している。

1 番目の原則は、**各通話は、ネットワーク番号に関連付けられる必要があるということである**。ネットワーク番号は通話の発信元を識別するものであり、ユーザと公衆電気通信ネットワークの間の、回線(固定ネットワークの場合) または、接続 (モバイル ネットワークの場合) に対応する電話番号である。ユーザが生成する CLI で発信者を識別することもあるが、これはオプションである。必要に応じて、 CLI はネットワーク番号と同じである必要がある。

2 番目の原則は、**ネットワーク番号が(個人または組織の)発信接続を一意の方法で識別するというものである**。この番号は、通話を発信したオペレータによって発信者に割り当てられたものであるため、発信者はこの番号を使用する権利を持っている必要がある。

3 番目の原則は、**プレゼンテーション番号がダイヤル可能である必要がある**ということである。これは、このような CLI を受信するエンドユーザが自分でこの番号にダイヤルして、実際に通話を設定できる必要があることを意味する。

4 番目の原則は、**ネットワーク番号とプレゼンテーション番号が有効である必要があるということである**。有効な番号とは、国際公衆電気通信番号計画 (ITU-T E.164 勧告) に準拠した番号であり、ベルギー番号の場合は、番号に関する王政令 (Numbering Royal Decree) 第 4 条の条項に従い、BIPT によって割り当てられた番号ブロックからの番号である。BIPT は、オペレータに割り当てていない番号ブロックの電話番号を使用することは許可していないことをここで明記する。

4.1.2　ブラックリスト

特定(例えば銀行など)の地理的な番号は、フィッシング詐欺などを目的とする CLI スプーフィングに対して特に警戒が必要である。海外からの CLI スプーフィングに対抗するため、BIPT は詐欺の影響を受けやすい地理的番号のリスト「ブラックリスト」の作成と保管を進めている。このリストのエンドユーザ (銀行など) は、リストに番号を載せることを、積極的に要求することができる。このような**「ブラックリスト」を使用して、ベルギーの主要な通信事業者は、海外から発信される通話を CLI によってブロック**する。実際の契約条件と手順は、BIPT 不正防止ワーキング グループ内でさらに策定が検討されている。

4.2　フランスの取り組み

フランスの電気通信・郵便・出版流通規制機関(ARCEP) は、 CLI スプーフィングの対策のために、長年にわたり複数の決定を下してきた。最初に、ワンギリでのプレミアム料金番号の使用を防ぐために 2012 年に採用され [13]、CLI としてのプレミアム料金番号 (フランスでは 089 までに始まる) の使用を禁止された。[13]

その後、ARCEP は 2018 年 及び 2019 年 に、現在のフランスにおける番号計画の決議の修正を行った。これらの決議では、 CLI スプーフィングを使用した不正な通話を減らす目的で、いくつかの勧告を作成している。

- ARCEP は、国際相互接続（EU 域外）を通じて着信したフランスの地理的または非地理的番号を伴う通話またはメッセージについて、**通信事業者がそれらの通話またはメッセージのルーティングをブロックすることが許可されることは正当である**と結論付けた。
- **自動システム (国内および国際) から送信される通話またはメッセージについて**は、2019 年 8 月 1 日から**携帯電話番号を CLI として使用することが禁止**された。**同様の禁止が、地理的番号および非地理的固定番号に対し**ても 2021 年 1 月 1 日から実施された。自動システムからの通話とメッセージには専用の番号帯では利用可能である。
- CLI として使用される電話番号は、**ARCEP によって割り当てられた範囲**である必要があり、また、**オペレータによってエンドユーザに割り当てられた番号**であり、その番号は、電話番号の割り当てられている期間中に、電話またはメッセージを**発信したユーザに繋がる必要**がある。

また、ARCEP は同決議により、2018 年 8 月 1 日以降、**非地理的番号および携帯電話番号への新しい番号の二次割り当てを禁止しており (地理的番号については 2023 年 1 月 1 日から禁止)**、フランスのすべての通信事業者に対して毎年、サブ割り当て (2 次割り当て、3 次割り当て等) されたすべての番号リストの提出を求めている。

これらの勧告の実装を確認するために、ARCEP は通信事業者に対し、間違った実装の状況や、ブロックされた通話の数とその発信元に関する情報を定期的に提供するよう呼びかけている。たとえば、2019 年 12 月、フランスの既存通信事業者（Orange）は、2019 年 9 月から 2019 年 11 月までの期間に、海外からの 1 億 1,100 万件の通話をブロックしたことを公に示した [14]。

2019 年のフランスの決議[15]も、**長期的な解決策として STIR/SHAKEN を視野**に入れている。その試験として、ARCEP は、認証される番号専用に確保された、特定の番号帯域 (地理的番号、モバイル番号、非地理的番号用) をすでに導入してきた。さらに、約 2 年間にわたる取り組みの成果として、詐欺電話に取り組むことを目的としたフランスの法律が 2020 年 7 月 24 日に制定された。この規定では、**欧州のエンドユーザに電気通信サービスを提供しない通信事業者との相互接続を通じ受信した通話とメッセージがフランスの CLI のものは、2020　10 月 24 日までにブロックすることを、通信事業者に義務付けている**。国際ローミングやトールフリーダイヤル番号の特定範囲の一部には例外が適用される。この規定は、**すべての通信事業者に対し、CLI 情報を認証し、通話のなりすましを防止する技術を 36 ヶ月以内に導入することを義務付けている。**この法的枠組みに基づき、ARCEP は事業者とのワークショップを開催し、フランスで STIR/SHAKEN フレームワークを展開する機会と最善の方法について検討を進めている。

ARCEP は、STIR/SHAKEN が IP 相互接続を通じてのみ機能することを認識しているが、市場 1 および 2 に関する最新の市場分析決定において、首都圏では 2015 年 7 月 1 日以降[16]、海外領土では 2018 年 7 月 1 日以降[17]、発信元オペレータからの IP 相互接続の要求は必然であり、合理的であるとみなされると

述べている。したがって、ARCEP の観点からは、レガシー ネットワーク サポートの進捗状況を監視しながら、IP 相互接続のみを介して機能する長期的なメカニズムに取り組むことが合理的である。さらに、フランスの既存通信事業者はすでに、数年内に **PSTN および総合デジタル サービス網 (ISDN) ネットワークの廃止を計画しているため、ARCEP は、SS7 相互接続を介して送信されるトラフィックが急速に減少すると予想している。**

4.3 ドイツの取り組み

4.3.1 2021 年 12 月 1 日以前の法的状況

ドイツの法律には、以前、電話の発信コールを設定する際の番号の送信に関し、それぞれの権利と義務を規制する条項が含まれていた。

関連規定のサブセクション 1（ドイツ電気通信法 (Telekommunikationsgesetz – (TKG)) のセクション 66k ）は、ネットワークで生成された番号と、通話に関与する電気通信サービスプロバイダの義務について規定している。サブセクション 2 では、ネットワークで生成された番号に追加し発信者が送信できる「汎用番号（Generic Number)」について説明している。 TKG セクション 66k(2) の規定に違反して汎用番号（Generic Number）を伝達すことは、「発信者 ID のスプーフィング」とされている。

ドイツ連邦ネットワーク庁 Bundesnetzagentur は、国家規制当局として、第 67 条第 1 項第 1 条 TKG によって付与された権利を行使する権利を有しているが、必要な是正措置を講じることはほとんど不可能であった。この特定の種類の詐欺では、違反を是正するために詐欺の責任者を特定する必要がある。しかし、**Bundesnetzagentur は TKG セクション 66k の規定の実施と強制を担当する機関であったにもかかわらず、そのために必要な手段と権限がなかった。何よりも、調査を行って責任者を特定する権限が与えられていなかった。**

4.3.2 現在の法的状況

2021 年 12 月 1 日に改訂され発効した TKG は[18]、ドイツの立法者により、とりわけ発信者 ID のなりすましに関する状況を改善するために、番号の送信に関連する義務と義務を規制するための新しいアプローチが選択された。

関連規定は、新しい **TKG のセクション 120 およびセクション 123(3) に記載**されている。

特に、この法律は多くの新しい技術的保護メカニズムを規定している。たとえば、**海外のネットワークからの通話の発信者の番号がドイツの番号である場合、その番号 (携帯電話番号を除く) を表示してはならず、**ドイツのネットワークへの通話の進入経路を識別する必要がある (新規セクション 120(4) TKG)。**なりすましの発信者番号による通話の大部分が、外国のネットワークから発信**されているか、**外国のネットワークを介してルーティングされているという調査結果**により、この規定が促進された。新しい条項の主な目的は、表示されるドイツの番号の有効性に対する信頼を再構築することである。

この法律には、**発信者の番号として「禁止された」番号が表示される通話を切断する**ための新しい義務も含まれている (新しいセクション 120(3) TKG)。このことにより、特に高額を請求する番号が発信者の番号として表示されるのを防ぐことができる。現在、「禁止」番号のリストには、緊急通報番号 110 と 112 も含まれている。これは、詐欺師が、緊急通報番号が持つ影響力とこれらの番号に関連する一般の信頼を悪用することを防ぐことを目的としている。過去には、発信者が、着信者に 110 を表示して、警察を装う電話が

頻繁に発生していた。

最後に、Bundesnetzagentur は、初めて**通話データに関する情報を要求する権利を与えられたため、番号操作に関する規定に対する違反を訴追する権限を持つことができるようになった** (新しいセクション 123(3) TKG)。

新しい対策のパッケージ、特に技術的に保護するメカニズムは、発番号が操作された通話の数が大幅に減少すると期待されている。このような立法による改善は、技術的な対策に焦点を当てている。重大な理由により、悪用事件の捜査が非常に困難であることが多い分野では、加害者に対して事後的に講じる対策より、未然に悪用を防ぐ技術的対策は効果的である。

この法律は部分的に最長 1 年の実施期間が規定されており、これは次年度末以降、状況の大幅な改善が期待できる。

政府により考えられる措置は次のとおりである。

- 実施期間終了後は、なりすましの番号、特にドイツの番号が発信者の番号として表示される電話に関する苦情は大幅に減少すると予想される。それにもかかわらず、**番号が操作された場合、連邦政府は適切な場合に、加害者に対する具体的な調査を開始し、行動を起こすことができる。このような場合に考えられる措置には、実際に通話に使用されていた番号を切断すること（新規第 123 条（1）TKG）や、行政罰金手続きにおいて違反を慣習法ではなく制定法により罰せられる犯罪として処罰**する(新規第 228 条（2）第 29 項以降 TKG）が含まれる。

4.4 ラトビアの取り組み

ラトビアでは、正式な規制を利用し、エンドユーザに A ナンバー(訳者コメント：発番号)を使用する権利がない場合や A ナンバーがルーティングできない場合など、A ナンバーが操作された通話をブロックすることを通信事業者に義務付けている。

ラトビアでは、**A ナンバーの部分的置換または完全な置換を含む CLI スプーフィング**は、**番号の悪用および詐欺とみなされる**[9]。ラトビア国家規制当局（NRA）は、番号を使用した不正行為の排除に関する手順を策定している。

番号の不正使用が検出された場合、電気通信サービスプロバイダ (ECSP) は通話のルーティングと関連する番号へのアクセスを直ちにブロックする必要があるとラトビア規制当局は予測している [10 [10]。ラトビアの法律は、ECSP が相互接続契約に適用される支払い手順と詐欺の場合にとるべき措置への言及を含めるべきであることも予見しており[11]詐欺や番号の不正使用を防止する措置を講じるべきである[12]。

電気通信法では、規制当局が、その活動において番号を使用して行われた不正行為または番号の不正使用を検出した ECSP に対して、番号を使用する権利を付与しない、または取り消す権利を有することも定義されている。

4.5 ノルウェーの取り組み

ノルウェーでは、2013 年から正式な規制[4]が施行されており、**技術的に可能で経済的に実現可能であれば、エンドユーザが A ナンバーを使用する権利を持たない場合や、A ナンバーでルーティングできない場合、通話をブロックすることを通信事業者に義務付けている。**

ノルウェー通信庁 (Nkom)も、顧客の経済的損失や消費者被害を防ぐために通話をブロックする権利を明確にする法的ガイダンスを利害関係者に提供した。

Nkom の主導により、ナンバーディスプレイ/ CLI に関する業界ガイドラインを、ノルウェーの番号割り当てワーキンググループの関係者と協力して作成した。

さらに、Nkom は、CLI スプーフィングと Wangiri を防止する対策を開発するための業界専門家グループを設立した。この取り組みは進行中であるが、現状、通話フィルタリング (トラフィック監視や位置確認を含む) と、なりすましの被害者、つまり、なりすましに番号が悪用された顧客に対する臨時の解決策に力を注いでいる。

また、ケースに応じ、SMS スプーフィングを削減するための通信事業者の取り組みも限定的な範囲で進められている。

Nkom はまた、警察当局や通信事業者との共同ワークショップを企画し、国家電気通信産業犯罪対策機関 (ITAKT [2]) とも交流している。

4.6 英国の取り組み

英国 (UK) は、発信者に提示される CLI データが正しいことを保証するため、現在および将来にむけた取り組みを進めており、**CLI への信頼を促進と、消費者利益の保護を目指**している。これらの措置は、**規制やガイドラインの策定と遵守、情報共有など、業界と規制当局との協力**に基づいている。

IP テクノロジーの発展により、通話に関連する CLI データの変更が容易になった。ネットワークの IP 化により、CLI が正しく、信頼できるものであることを確認するために、さらに多くの対策を講ずる必要がある。正確な CLI データがエンドユーザに確実に提供されるようにするために、実現可能な範囲でオペレータはより大きな役割を担っている。

4.6.1 CLI の義務とガイドライン

Ofcom (英国通信規制当局) は、オペレータ[5]に対し、CLI 機能を提供し、通話で提供される CLI データに、発信者を一意に識別する有効なダイヤル可能な電話番号が含まれていることを確認することを要求している。

- 有効な番号とは、**国際公衆電気通信番号計画 (ITU-T E.164 勧告) [6]で**ある。英国の番号を使用する場合、その番号は英国の電話番号計画[7] において割り当てが可能な番号であって、Ofcom によってオペレータに割り当てられる番号である必要がある。
- ダイヤル可能な番号は、**使用中であり、折り返しまたはその後の通話に使用できる番号**である必要がある。
- ユーザに割り当てられた番号であるか、あるいは、その番号を割り当てられた第三者からその番号を使用する許可が (直接的または間接的に) ユーザに与えられているため、ユーザが使用する権限を持っているものである場合、**番号は発信者 (個人または組織) を一意に識別**する。

[2]http://itakt.no/

Ofcom は、CLI 情報の信頼性を向上させるための、有効性、プライバシー、完全性の基本原則を定め、CLI 要件を実装するためにオペレータが期待されることを明確にするために、 CLI ガイドラインも公開した [8]。 CLI データの伝達は 2 者以上の ECNO 間の協力に依存することが多く、一貫性のある伝達基準が必要であり、ガイダンスが必要である。

CLI ガイドラインは、現在、技術的に可能なものに基づき、電話コール（または呼）のさまざまな部分でオペレータ向けに有効でダイヤル可能な CLI の定義を定めている。**発オペレータは、正確な CLI データが呼で提供されることを保証する責任があり、中継/着信オペレータは、提供された番号が有効な番号範囲のものであることを確認することが要求される。**

CLI ガイドラインでは、次のことも確認している。

- **すべての通話は、通話の発信元を識別するネットワーク番号に関連付けられている必要**がある。ただし、発信者を識別するために着信側に表示される CLI (プレゼンテーション番号) は、発信者を一意に識別する別の有効なダイヤル可能な番号に正当に変更される場合がある。 CLI ガイドラインでは、顧客のさまざまな通話要件 (たとえば、コールセンターが複数のクライアントに代わって電話をかけるなど) を満たすために、プレゼンテーション番号が商用サービスとして提供されるシナリオを定めている。
- **表示される CLI** は、過剰な通話料金、または予期しない通話料金が発生する、**プレミアム料金サービスに接続する番号や、収益分売番号**（収益を分配する場合に使用する番号）**であってはならない**。

ユーザのプライバシーを尊重し、信頼できる CLI データをエンドユーザへ送信することは、元のデータが正しいことと、この情報を正しく伝えるために呼の伝達に関与するすべての 電気通信ネットワークオペレータ/電気通信サービスオペレータが協力することに依存する。 CLI の義務により、オペレータは CLI データがより正確に交換され、有効な CLI データのみがエンドユーザに利用可能になる必要がある。

4.6.2 CLI が無効な場合のオペレータのアクション

オペレータが、通話で提供された CLI に無効またはダイヤル不可能な CLI データが含まれていると判断した場合、技術的に可能な場合は、通話が着信側に接続されないようにする必要がある。これには、通話をブロックまたはフィルタリングすることが考えられる。

英国外 (英国が設定する要件の範囲外のネットワーク) から発信される通話の場合、最初のエントリーポイントのオペレータは次の責任を負う。

- **有効な CLI データが入力されていることを確認**する。有効な CLI データでない場合は、
- **無効または欠落している CLI データ**を、この目的のために割り当てられた**番号に置き換える**。こうした状況を容易にするために、Ofcom は**特定の範囲のネットワーク コード (「0」と 08979 で始まる 10 桁の番号)** を利用可能とした。

以前の業界の慣例では、オペレータは割り当てられた範囲から乱数を挿入していたが、この方法は業界全体に統一的に適用されていなかった。 08979 の番号帯を挿入すると、(i) CLI が挿入されたことが明確に示され、 (ii) (08979 の後の 2 桁は、挿入を行ったオペレータを識別するため)その番号を挿入した英国 電気通信ネットワークオペレータを特定できるため、コール トレース プロセスが簡素化され、高速化された。

4.6.3　規制当局と業界の調整

Ofcom はまた、オペレータと協力して、信頼できる CLI を使用しない通話のブロックを支援している。これには次のようなものがある。

- 迷惑電話に関する業界検討グループを招集し、メンバーは**詐欺や悪用のためにブロックされた番号について規制当局を通じて情報を共有可能とする。**
- Ofcom が提供する**「保護された」番号のリスト**は、英国の電話番号計画で使用が指定されていない番号であり、有効な番号ではないため、使用すべきではない。オペレータは、このリストを**参照ツールとして使用して、これらの CLI による通話をブロック可能**とする。
- **「発信禁止」番号リストの編集**。詐欺師による番号なりすましの最も悪質なケースの一部は、金融機関や政府機関が使用するものに関連していることから、「発信禁止」リストには、組織が発信通話に使用しない番号 (着信専用の顧客連絡先番号など) が含まれている。Ofcom はさまざまな団体と協力して、発信に使用すべきではない番号に関する情報を通信事業者と共有している。
- モバイルネットワークや警察と協力して、偽番号への折り返し電話を促す**テキストメッセージ詐欺に対する革新的な技術的解決策を検討**している。

4.7　情報の共有

情報共有の取り組みは、傾向の発見など、番号の不正使用やスプーフィングの研究や理解に役立つ可能性がある。ただし、このような対策は本質的にリアルタイムではないため、CLI スプーフィングの発生を阻止するのにそれほど効果的ではない。これには、リアルタイム、または、ほぼリアルタイムの情報とアクションが必要であり、これらの取り組みは短期間で実施できる。情報共有の例を以下に示し、これらがどのような利点をもたらすかを考察する。

4.7.1　BEREC の協力プロセス

2013 年、BEREC は USD ユニバーサルサービス指令第 28 条第 2 項に関する報告書を発表した。調和された **BEREC 協力プロセス[32] は、詐欺や悪用が確認された際の、NRA またはその他の関連国内当局による介入における国境を越えた協力プロセスを概説**しており、これには CLI スプーフィングが含まれる可能性がある。調和の取れた BEREC 協力プロセスは、NRA を支援するために、EU 加盟国に「関連する事項を確保すること」を要求する権限（旧 USD 第 28 条第 2 項、現在は EECC 第 97 条第 2 項）の効果的な適用についてまとめている。 各国当局は、公衆通信ネットワークや公的に利用可能な電気通信サービスを提供する事業者に対し、詐欺や悪用の理由で正当化される、番号やサービスへのアクセスを遮断をすることについて、ケースバイケースで要求することができる。 このような場合、電気通信サービスのプロバイダは、関連する相互接続またはその他のサービスの収益を差し控えている。**BEREC の協力プロセスは、詐欺や悪用と阻止するための国家プロセスを補完するための協力および情報共有ツールとして最もよく理解**されている。ただし、**このプロセスは比較的少数しか適用されておらず、ほとんど試験されていない**。経験上、通信事業者間の相互接続支払いの転送速度を考慮すると、このプロセスは長すぎるためあまり効果的ではないことが明らかになった。「ベスト プラクティス ガイドライン」を適用して、EU 全体でより頻繁に、より迅速に、調和のとれた方法を使用することにより、CLI スプーフィングを含む詐欺や悪用の傾向を理解し、それに対抗する効果が向上する可能性がある。

4.7.2 ITU-T ガイダンス

4.7.2.1 勧告 ITU-T E.156 - ITU-T E.164 番号リソースの不正使用の報告に対する ITU-T の措置に関するガイドライン

これは、ITU-T Study Group 2 により発行された、**E.164 電話番号リソース不正使用の申し立ての報告に関する勧告**である。

対象となる E.164 番号リソースは以下のとおりである。

- 地理的地域の国コード
- インマルサット (+870) および国グループ (+388) のコード
- ネットワークのための国コード (+882、+883)
- グローバルサービスのための国コード (例: +800、+878 など)
- GMSS(Global Mobile Satellite Services) オペレータのための国コード (例: +881)
- トライアルのための国コード (+991)
- 未割り当ての国コード

加盟国または認定オペレータ (ROA：Recognised Operating Agencies) は、ITU Web サイトにあるフォームを使用して不正使用の申し立てができる。

報告に基づいて、勧告 ITU-T E.156 に関連するデータベースがあるが[3]、2005 年以降、通知は僅か 242 件で、それに対する返答を得たのは僅か 31% であった。[4]

データベースに含まれるデータの例は、下表の悪用の種類を分類することができる。

表1: 不正使用の種類と報告数

誤用の種類	レポート数
プレミアム料金サービスで使用するコード	105
意図と異なるコード	105
その他	13

[3] https://www.itu.int/net/ITU-T/misuse/table.aspx - TIES アカウントを使用してのみアクセス可

[4] 2022 年 3 月 16 日の情報に基づく

誤用の種類	レポート数
Web ダイヤラーに使用されるコード	5
未割り当てのコード	5
誤ってルーティングされたコード	3
上記以外	3
予約済みコード	2
費用分配型サービスで使用するコード	1

4.7.2.2 勧告 ITU-T E.157 - 国際発呼者番号の送信

勧告 ITU-T E.157 は、セキュリティを向上させ、詐欺や技術による被害を最小限に抑えるために、さまざまな国に発信者番号 (CPN - A パーティ番号/CLI に相当) を送信するためのガイダンスを提供するために開発された。

勧告 ITU-T E.157 に示すガイドラインでは主に、送信される発信者番号は、発信の国から受領（後続）国に送信されるまでは、通話が発信された国、または、ネットワークを識別するために国コードを先頭に付けた発信者番号で構成される必要があること(国際ローミングまたはノマディック通話は含まない)を述べている。さらに、送信される発信者番号には、国コードに加えて、各国の宛先コード、または通話ごとに適切な請求と精算を可能にする十分な情報が含まれている必要がある。

5　CLI スプーフィングに対抗するためのさまざまな技術的解決策の分析

この章では、CLI スプーフィングへの対抗措置として、長期的な対応となる可能性のある解決策をいくつかを紹介する。その中には、**STIR/SHAKEN** など、すでに部分的に実装されているもの、**SOLID** や **DLT** など、まだ技術的な安定にむけた過程段階のものが含まれる。

一方、この章では、CLI スプーフィングとネットワーク間の信頼を扱う多くの **ITU-T Study Group (SG) で開発されている解決策/勧告については分析しない**。たとえば、ITU-T SG2 は 2021 年にスプーフィング対策施策の実施を支援できるテクニカルレポート[34] を発行した。プロトコルを扱う ITU-T SG11 は既存および将来ネットワークを対象に、信頼できるネットワークエンティティ間での信号アーキテクチャと要求条件を提示するテクニカルレポート[35] を発行した。ITU-T SG17 など、セキュリティを扱う他の SG は、スプーフィングに関する側面にも取り組む可能性がある。

5.1　米国における STIR/SHAKEN の導入に関する概要説明

この章では、米国で導入されている STIR/SHAKEN について、米国で採用されているガバナンス構造も含め説明する。米国以外の国では、異なるガバナンスのアプローチを採用しながら、STIR/SHAKEN を実装し、グローバルな相互運用性をサポートする可能性がある。たとえば、個別の国レベルではなく欧州レベルでガバナンスを導入することも可能であろう。

SS7 ベースのネットワークでは、発側オペレータがネットワーク シグナリングに CLI を挿入し、信頼できるオペレータのチェーンを介して、正確な(固定およびモバイルの)CLI を使用して宛先オペレータにて呼は終端する。たとえば、PBX が番号 (内線番号) を挿入するなどの例では、2 つのオプションが許容される。1 つは検証無しでそのまま伝達する方法、もう 1 つは(番号が DDI 範囲に属さない場合は、オペレータが CLI としてメイン番号を挿入し）検証し、伝達する方法の 2 つのオプションが許容される方法。

現在では、IP 技術により任意の番号を CLI として挿入できるようになり、さらに多くのオペレータが最終宛先へのコール（または、呼）の処理に介入するため、チェーンの信頼性が低下している。

5.1.1　SHAKEN の背景にある重要な洞察

SHAKEN プロトコルでは、発信側オペレータが常に通話の発信について何らかの情報を知っているという前提が基本にある。

a)　CLI の番号を知っている場合。（たとえば、ネットワークによって行われるモバイル認証や、交換機によって制御される固定番号）

b)　顧客を知っており、別の CLI (PBX、受付係、市内コールバック番号) の挿入を許容する場合

c)　ネットワークへのエントリーポイント (ゲートウェイ) のみを知っている場合

SHAKEN は、発側オペレータがこの情報を着側オペレータに安全に伝達するためのメカニズムを提供する。言い換えれば、**SHAKEN により発信事業者が知っている内容を着信事業者に安全かつ確実に伝達することを保証する**ことができる。

したがって、**発側オペレータは、通話の発信について知っている情報** (顧客とその番号を使用する権利、または顧客 (番号ではない)、または電話の自社のネットワークへのエントリーポイント) に基づいて**デジタル署名を作成**する。そして、それを**シグナリング部分に挿入して、着側オペレータに転送**する。着側オペレータは**デジタル署名を検証**し、発側オペレータと着側オペレータの間で通信に関与するものが CLI を変更した場合、検証プロセスで変更フラグが立てられる。

また、**発信識別子 (「 origid 」) と呼ばれる特別な番号**は、通話の発信を一意に識別し、通話ごとに生成され、**通話のトレースバックと評判を判断する目的で使用されるシグナリング部分に挿入**される。「 origid 」は、オペレータに対応し、グローバルに一意であるが、実態は不明な識別子であり、通話、顧客、デバイスのクラス、またはオペレータの評判の判断や、トレースバックするために使用する可能性のある、顧客やゲートウェイの識別情報が含まれる場合がある [5]。

SHAKEN は、IETF によって開発され、エンドツーエンドのメカニズムとして設計されたプロトコルである STIR に基づいている。 STIR クライアントは、発側と着側の両方に存在する。**発信オペレータによるデジタル署名の作成**と、その後の**着信オペレータによる検証**は、**通話に関与するユーザによって処理される通話レベルのタスク**であるため、オペレータはそのプロセスにおいてトランスペアレントである。 **SHAKEN** は STIR に基づいているため、**証明書管理システムが必要**であり、**実装のこの部分はオペレータ レベル**で行われる。

STIR/SHAKEN は、スプーフィングされた CLI による呼を直接ブロックはしない。 SHAKEN からの**検証結果は**、着側のエンドユーザに直接表示されるか、本質的に良好な通話、疑わしい通話、または詐欺の可能性がある通話を識別する**評価システムを提供する「通話ブロック アプリ」に入力される可能性**がある。通話ブロックアプリは、着信者に代わって、好ましからざる通話の着信を阻止することができる。通話ブロックアプリが使用されない場合は、着側のエンドユーザが通話ごとに決定することができる。

要約すると、SHAKEN は、発信者番号の署名と検証に必要なツールをオペレータに提供するのみでなく、電話に応答する前に、発信者を信頼するかどうかについて一定レベルの安心をエンドユーザに提供する。

5.1.2 認証要求 (さまざまなレベルの認証)

SHAKEN では、次に示す異なる認証 3 レベルが定義されている。

- 完全認証 （Full attestation）
- 部分認証 （Partial attestation）
- ゲートウェイ認証 （Gateway attestation）

5.1.2.1 完全認証（Full attestation）

署名するオペレータは次の条件をすべて満たす。

a) 通話の発信の責務を有する。

---

[5]ある識別子が、ランダムな文字列または数値であること以外に、それが識別するものについての情報の提供がない場合、それは不明な識別子である。

b) ユーザを直接認証する関係にあり、ユーザを識別できる（法執行機関（LEA：Law Enforcement Agency）にとって重要)。

c) 通話に使用された電話番号との検証の関係を確立している。

完全認証（Full attestation）では、署名オペレータは、ユーザが CLI として表示される番号を正当に使用できると主張するが、その通話が実際に発呼者として表示される番号からのものであるとは主張しない。(「正当な」スプーフィングは許可される)。 最終的には、何が「電話番号を主張する正当な権利」を構成するかを決定するのは通信事業者のポリシー次第であり、それは通信事業者の「評判」に影響を与える。**STIR では、このような「正当な」なりすましは許可されてないが、SHAKEN では許容される。**

5.1.2.2 部分認証（Partial attestation）

署名するオペレータは次の条件をすべて満たす。

a) 通話の発信の責務を有する。

b) ユーザを直接認証する関係にあり、ユーザを識別できる（法執行機関（LEA：Law Enforcement Agency）にとって重要)。

c) 通話に使用された電話番号との検証関係付けが確立されていない（チェックが行われていないか、肯定的な応答が得られていない)。

重要:**部分認証は**、通話がこの番号から発信されていないことを意味するのではなく、これが「チェックされなかった」(つまり、**署名するオペレータが知らない**) ことを意味するのみである。各ユーザには依然として**一意な識別子が割り当て**られ、データ分析に基づいて評判プロファイルの確立と、そのような一意な識別子を割り当てられた**ユーザによって主張される情報の信頼性について評価することが可能**である。 (識別子や署名だけからユーザの身元をリバースエンジニアリングすることは不可能であり、それによってユーザ情報のプライバシーが保護される)。

5.1.2.3 ゲートウェイ認証 （Gateway attestation）

署名するオペレータは次の条件をすべて満たす。

a) VoIP ネットワークへの通話のエントリ ポイント。

b) 通話を開始したユーザとの関係がない。

基本的に、**ゲートウェイ認証は、オペレータがそのネットワークへの通話のエントリ ポイントのみを知っていることを示すのみ**である。ゲートウェイ認証は、「 origid 」が発側のノードまたはトランクを指すため、トレースバックに使用できる。

5.1.2.4 原則

Full attestation の場合、VoIP ネットワーク上でオペレータが直接関与し開始したすべての通話に、唯一の識別子が使用されるが、オペレータは地理的地域や顧客のクラスを区別するために予備の識別子を持つことを選択することも可能である。

Partial attestation の場合、トレースバックと評判のセグメンテーションの両方で呼を区別するために、顧客ごとに 一意の識別子が必要である (あるユーザの評判が同じオペレータの他のユーザの評判に影響を与えないようにするため)。

ゲートウェイ認証の場合、ベスト プラクティスでは、トレースバック識別と評判による評価を可能にするために、発信元のノードまたはトランクを識別するために「 origid 」は十分に粒度が高い必要があると規定している。

信頼のレベルを反映するため、このような認証レベルを設定している。また、トレースバックと不正な通話の識別に関するベスト プラクティスも開発されている。 「 origid 」を使用することで、「origid 」を使用した呼で問題が検出されると、その後に迅速なトレースバックが可能になるが、「不正な呼び出し」を特定するにはデータ分析が必要である。

現在、CLI は簡単になりすましができるため、オペレータは不正行為を検出するためにデータ分析に依存する必要があり、誤検知のリスクが常に存在するため、固有の制限を認識する必要がある。 「 origid 」と SHAKEN メカニズムの導入により、この (分析) パラメータはより広範囲で信頼できるようになった。

5.1.3 ネットワークの実装

5.1.3.1 Session Initiation Protocol (SIP) ベースのネットワーク上のユーザ間通話

SIP ベースのネットワーク (IMS 環境など) 上のユーザ間で通話が行われる場合、認証および検証サービスの処理には、発側のサービス プロバイダで Secure Telephone Identity - Authentication Service (STI-AS)と着側サービスプロバイダで Secure Telephone Identity - Verification Service (STI-VS)が存在する必要がある。

発信者から SIP INVITE を受信すると、**発側のサービス プロバイダは 発信元と発信者番号に基づいて、発信者番号に提供する認証のレベルを決定**する。次に、発側のサービスプロバイダは、**SIP INVITE を STI-AS に送信**する。**STI-AS は、通話の発信時に、認証レベルや「 origid 」を含む発信者情報に署名してトークン (PASSporT) を生成するメカニズムを実装**する。**この情報**と、発側サービスプロバイダの証明書を管理する**リポジトリの場所**を含むその他のパラメータは、**SIP ID ヘッダーに挿入**される[26]。

SIP ID ヘッダーを含む **SIP INVITE を受信**すると、**着側サービス プロバイダはそれを STI-VS に送信**する。 **STI-VS** は、SIP ID ヘッダーに含まれる発側サービス プロバイダの証明書リポジトリの場所を利用して、**公開キーを含むデジタル証明書を取得**し、**SIP ID ヘッダーをデコード**し、**署名を検証**し、**PASSporT を検証**する。**着側のサービス プロバイダは、認証のレベルと検証結果**に応じて表示などの**オプションの処理**を行い、**着信側への通話を完了**する。

このメカニズムは、完全証明および部分証明で機能する。

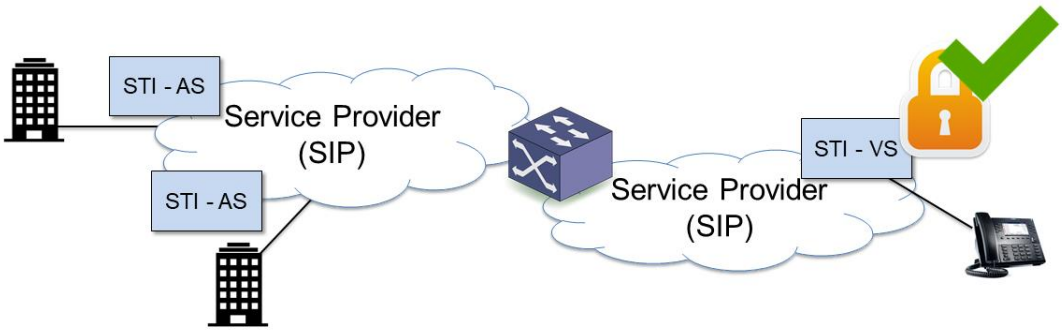

図1: Session Initiation Protocol (SIP) ベースのネットワーク上のユーザ間通話のメカニズム

(出典:ATIS)

5.1.3.2 SS7 ネットワークから発信、SIP ベースのネットワークに着信する通話

このような場合、通話は SIP エンドツーエンドに基づいていない。発側と着側のサービス プロバイダの間には複数の中継事業者が存在する可能性があるため、通話は**最初の SIP ベースのネットワークへのエントリ ポイントで STI-AS によって署名**される。 **STI-AS は、トークン (PASSporT) と証明書リポジトリの場所を挿入した SIP ID ヘッダーを含む SIP INVITE を送信**する。

着側のサービス プロバイダが受信すると、SIP ベースのネットワーク上のユーザ間通話で説明したように、**SIP ID ヘッダーを含む SIP INVITE が検証のために STI-VS に送信**される。ただし、SS7 ネットワークから発信された呼の場合、着側のサービス プロバイダの STI-VS は、呼が SIP ベースのネットワークに入った場所のみを確認できる。したがって、このような場合は、ゲートウェイ認証のみが可能となる。

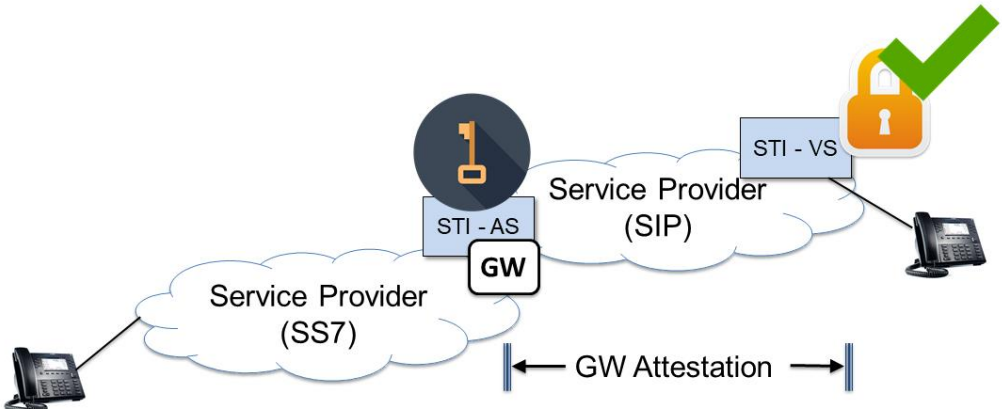

図2: SS7 ネットワークから発信、SIP ベースのネットワークに着信する通話

(出典:ATIS)

5.1.4 SHAKEN のガバナンスモデル

このセクションでは、米国で導入されている STIR/SHAKEN について、米国で採用されているガバナンスの構造と共に説明する。

デジタル署名の作成には STIR/SHAKEN 証明書が必要であり、これらの証明書が悪意のある者の手に渡らないようにする必要がある。

このため、ガバナンス機関 (STI-GA) が設立され、エコシステム全体のルールや事業者が SHAKEN 証明書を取得するためのメカニズムの定義および変更に関する任務をガバナンス機関 (STI-GA)が負っている。**正当なオペレータのみがデジタル証明書を取得し、システムに参加できることを保証することが必要**であるということについて、STI-GA が十分に注意を払うことが重要である。 **STI-GA は、提案依頼書 (RFP) に従って STI ポリシー管理者 (STI-PA) を選択する責任**もある。

FCC は、ガバナンス機関に対して独立した立場での監督機能のみを持っている。システムを迂回する方法など、不正行為が予想されるため、**ガバナンス当局の理事会は、ルールの適応に迅速に対応するために業界関係者のみで構成**されている。

STI-PA は、STI-GA によって作成されたルールを適用することにより、運用上の役割を採用し、オペレータが STI 証明書を取得する権限を持っていることを検証する。彼らは、**「オペレータのトークン」を発行**し、**STI 認証局 (STI-CA) を承認**し、すべての安全で承認された **STI-CA (システム全体の信頼のルートを構成する) のリスト**と**証明書失効リスト (CRL) を管理**する。

STI-CA は、事業者に STI 証明書を発行する。これらは、STIR/SHAKEN に特化した認証局 (CA) である。 CA が SHAKEN システムに参加するには、STI-PA に申請する必要がある。申請では、CA は STI-GA によって定義された基準を満たしていることを証明する必要がある。

これらのシステムへ参加を希望する事業者は、STI-GA が定義する基準を満たしていることを証明する申請書を STI-PA に提出する必要がある。合格すると、STI-PA は「サービス プロバイダ コード」(SPC) トークンを発行する。トークンに基づいて、検証を受けている STI-CA から STIR/SHAKEN 証明書を購入できる。

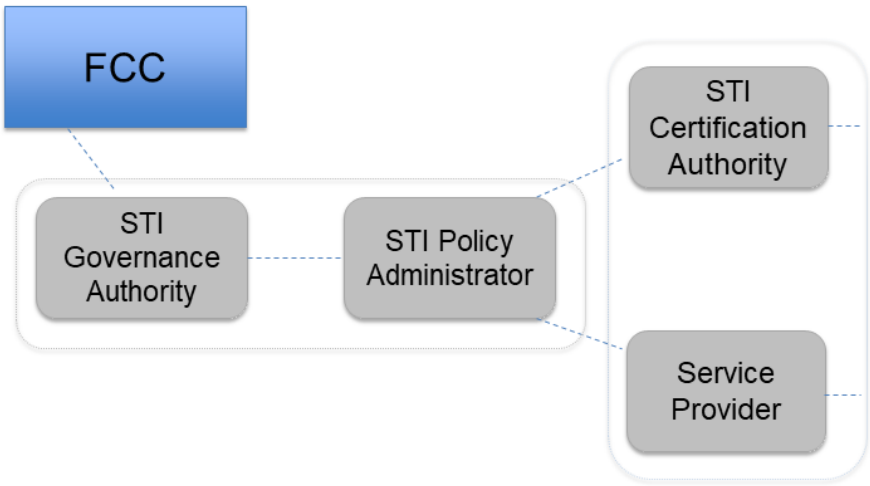

図3: STIR/SHAKEN ガバナンス モデル

(出典:ATIS)

5.1.5 IP および非 IP ネットワーク上で通話認証を実装するための拡張機能

FCC は、米国の電気通信サービスプロバイダ(ECSP)に対し、SS7 ネットワークを用いた通話で CLI を検証するためのメカニズムを実装することを義務付けている。この対策は STIR/SHAKEN アーキテクチャとクエリに基づいており、これらの情報を SS7 シグナリングにて送信することが可能である。この実装は 2022 年あるいは 2023 年に完了すると予想されている。

5.2 INTERNATIONAL STIR/SHAKEN

STIR/SHAKEN に基づく技術による対策は集中型アーキテクチャであり、当初は単一の国、米国向けに設計されていた。カナダとの協定により、異なる 2 つのインスタンスを許可できるようにモデルを更新する必要があったが、両国は現在、同一の国コードを使用し、共通した番号計画の管理を行っており、共通組織を持っている。国境を跨る SHAKEN 標準では、最初に、二国間協定に基づいて、国家間で STIR/SHAKEN が機能することを可能にするメカニズムを定義する。一方で、調整された地域での実施（例：ヨーロッパ全体のガバナンス）、業界フォーラム、または「利益共同体」など、国境を越えた取り組みに役立つ可能性のある戦略は数多くある。これらの初期的なアプローチは、最終的にはスケーリングが問題となるが、今後数年間の展開においては、容易に拡張が可能である。

しかし、詐欺や番号の悪用を軽減するために CLI 検証メカニズムを導入したいと考えている国が増えている。そのため、この新しい要件を満たすために、STIR/SHAKEN 技術による解決策を拡張する必要がある。

最も顕著な課題は、以下の関連項目である。

- **正当性を確保するための厳格な審査プロセス**の設定

- **すべての国で審査プロセスを導入することが困難である**こと
- **非常に多くの国との間で、二国間協定が必要になる**ことによる影響

上記の課題はあるが、各国がレジストリに登録し、個々の国/地域で誰を信頼するかを決定する簡潔なプロセスを提供する必要がある。次の図に示すように、登録モデルは国ごとに異なる場合がある。

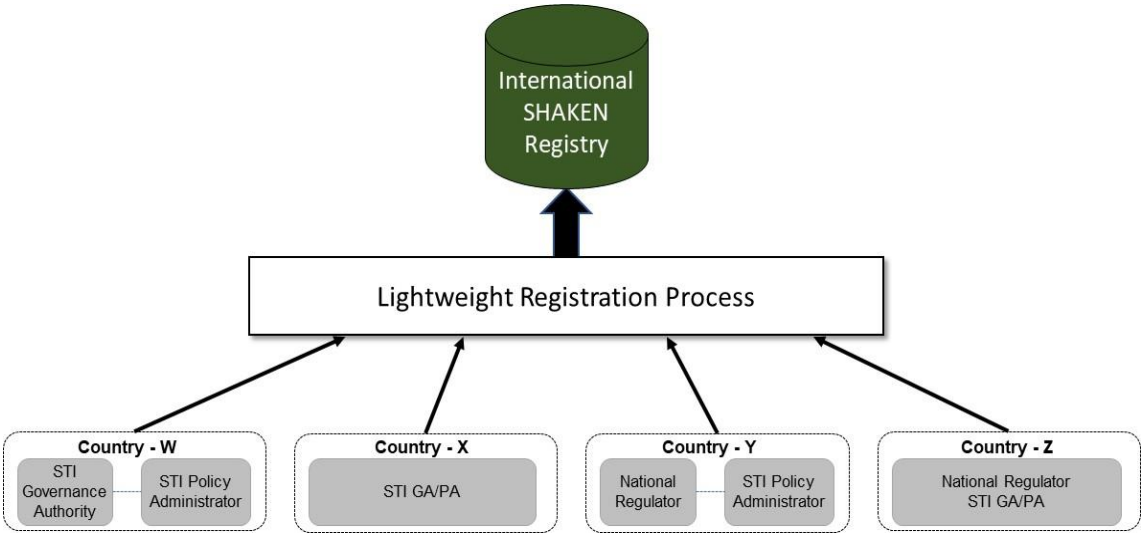

図4:International SHAKENレジストリ

(出典:ATIS)

International SHAKEN レジストリの登録情報の扱い方は、国ごと、地域ごとに独自に決定できる。しかしながら、**国際的に一貫性があることを確認するために、最低限の基準をいくつか定義する必要**がある。

中央レジストリの長期戦略を完全に実装するには追加の作業が必要であり、管理上のいくつかの課題に直面しているため、中央レジストリの実用化前に STIR/SHAKEN を大規模に導入する必要がある可能性がある。

International STIR/SHAKEN モデルのより一般的な図を図 5。

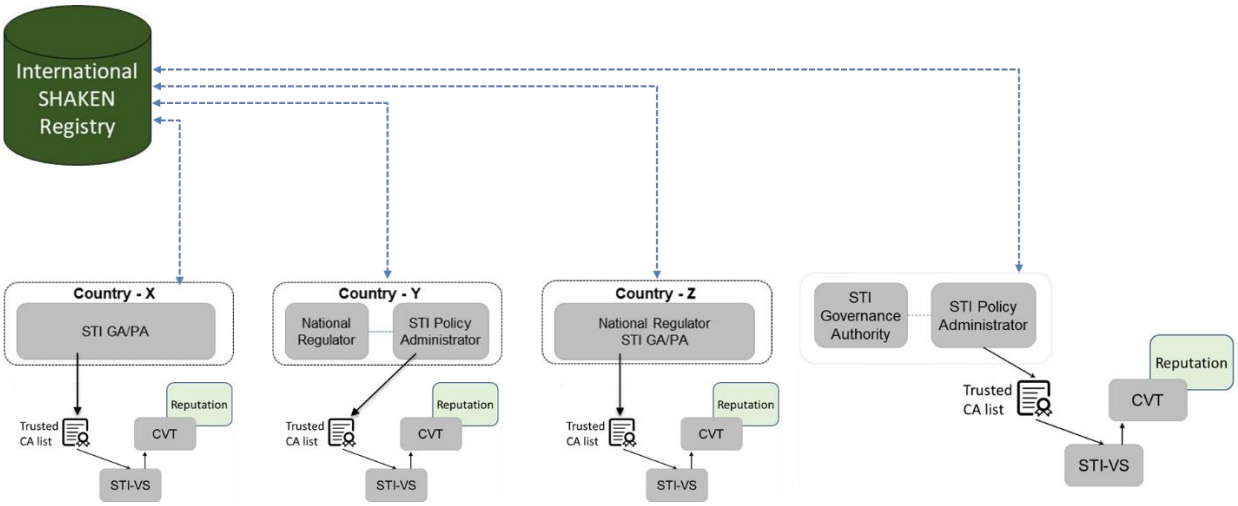

図5:国際SHAKENフォーラム

(出典:ATIS)

5.3 SOCIAL LINKED DATA (SOLID)

SOLID (Social Linked Data) は、**Linked Data の原則**[6]**に基づく分散型アプリケーションを構築するために提案された一連の規則であり、ツール**である。 SOLID フレームワークを使用すると、個々のエンティティがデータをプライベート データ ストアに利用するシステムやアプリケーションから分離可能となる。SOLID はモジュール式で拡張可能であり、既存の W3C 標準およびプロトコル[7]に可能な限り依存している。

SOLID を使用すると、個々のエンティティは、データをプライベート データ ストア あるいは「ポッド」に活用するシステムやアプリケーションからデータを分離できる。個々のエンティティは、そのポッド内のデータを制御し、そのデータを共有する他のエンティティを選択する。これは、HTTP の上に構築されており、一連のオープン標準とプロトコルを通じて拡張されている。

SOLID の分散型アーキテクチャは、分散型 peer to peer 不正防止ネットワークの基盤を提供する。 Web 上に構築されているため、新しいプロトコルやインフラストラクチャ要件は導入されず、複雑性が増加することが制限され、Web トラフィックを促進するためにすでに設置されている既存のインフラストラクチャを再利用できる。

SOLID は、分散型 ID およびセキュリティ モデルが peer to peer 認証、認可、および暗号化を提供する A-party Number 検証のための通信エコシステムに適用できる。

---

6 https://www.w3.org/DesignIssues/LinkedData

7 https://w3.org/

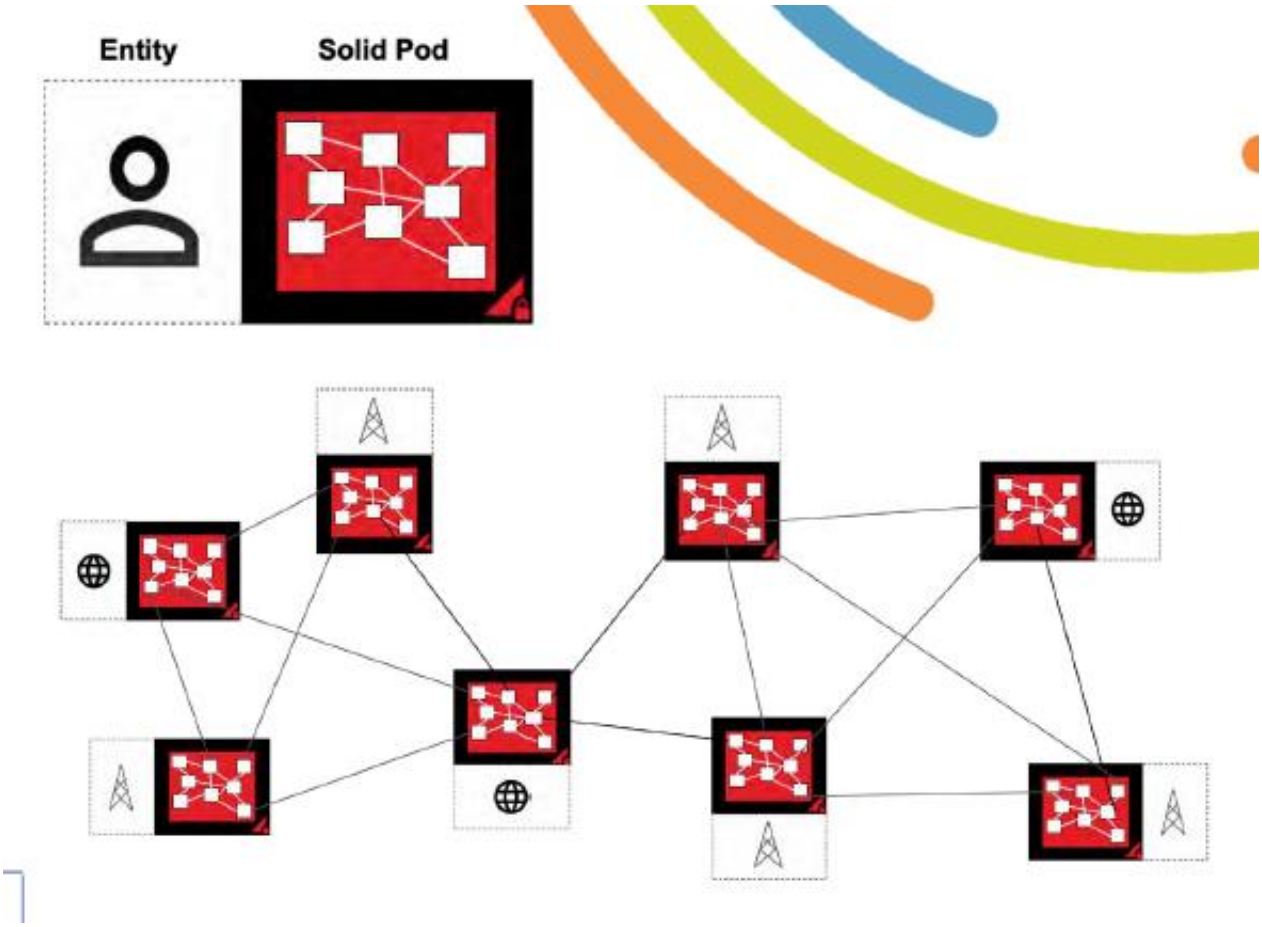

図6: アーキテクチャ

(出典: I3フォーラム)

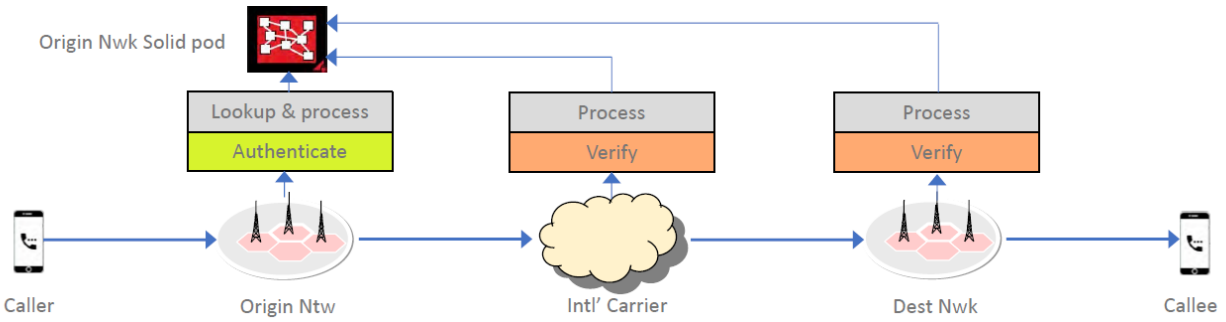

図7: プロセス

(出典: I3フォーラム)

SOLID は、分散型 peer to peer ネットワークを介したインターネットワーク通話詐欺を軽減するために、特に Secure Telephone Identity Revisited (STIR) と組み合わせて議論されている。 STIR は、発信元の検証と、発信元ネットワークと宛先ネットワーク間の通話メタデータの安全な転送に使用できる。 SOLID は、同じ間での柔軟かつ安全なデータ共有に使用できる。この理論的なアプローチは、オペレータ、通信事業者、発信者、着信者の正当なエコシステムを中断することなく、不正行為を対処する。

このアプローチでは、参加している各ネットワークに、自身がホストする、関連付けされた SOLID Pod が存在する。参加している異なる宛先ネットワークへの通話が開始される毎に、発信元ネットワークは、その宛先ネットワークのみがアクセスを許可されているエリアの SOLID ポッドに通話レコードを作成する。発信側のネットワークは、通話開始時刻、発信者番号、着信者番号、通話状態などの重要なメタデータを通話記録に保存する。通話記録の URL を SIP ID ヘッダーに保存し、宛先ネットワークで「To」ヘッダーを匿名の着信者識別子に変更する。宛先ネットワークが通話を受信すると、SIP ID ヘッダーに保存されている URL で SOLID Pod 内の通話記録を検索し、「To」ヘッダーをそこに保存されている実際の着信者番号に更新する。また、通話記録を更新して、通話が目的の宛先ネットワークで受信されたことを発信元ネットワークに知らせる。

この対策では、STIR を使用して呼び出し元を検証し、ワークフローの整合性に不可欠な発信側ネットワークの ID を証明する。 STIR では、発信元ネットワークが通話記録の URL を宛先ネットワークに渡すために使用する SIP ID ヘッダーが導入されている。 STIR により、宛先ネットワークは、アイデンティティヘッダー (したがって通話記録の URL) が転送中に改ざんされていないことを確認できる。

現在、SOLID を実際に実装しているオペレータはいない。 SOLID 技術仕様のドラフトは https://github.com/solid/solid-spec より入手可能である。

5.4 分散型台帳技術 - ブロックチェーン

分散台帳テクノロジー (DLT) は、**複数のノードにわたる複数の参加者による分散データベース管理を可能にするプロトコル**である。DLT のプラットフォームは、電話番号データベースの確立において、下記 3 項目に示す特徴により、特に適している。

- プロセス内で信頼と保証を提供
- 安全な不変資産を作成(この場合、数値はデジタル資産)
- 「スマート コントラクト」 (特定の条件によって検証およびトリガーできる方法で、特定の種類のトランザクションルールをエンコードするプログラム) を提供

ブロックチェーンは分散型台帳の一種である。これは、連続的に成長するブロックのチェーンとして配置され、デジタルに記録されたデータで構成されており、各ブロックは暗号でリンクされ、改ざんや改訂に対して強化されている。ブロックチェーンを番号管理に適用すると、メンバー間で分散ノードを介して分散されるプラットフォームを使用して、デジタル資産としての電話番号の使用権とステータスに基づく一種の分散台帳を提供できる。 (プライベートなプラットフォーム、あるいは、パブリックなプラットフォームと対照的に)、「許可されたブロックチェーン」プラットフォームは、番号管理に関与するすべての当事者の機能を保証するが、特定の識別可能で許可された参加者のみがアクションを実行できるようにするアクセス制御レイヤーの追加のセキュリティ手段を備えている。したがって、データは安全かつ透過的に交換できる。

通信分野における DLT の影響と応用に関する実質的な作業は、さまざまな組織、特に ITU によって着手されている[33]。

ブロックチェーンは、ユーザの身元を確認するために公開鍵証明書を共有

- ブロックチェーンは、2 パーティ間のトランザクションを記録できる分散型台帳である。当事者は効率的かつ検証可能かつ永続的な方法で参加する
- オペレータが加入者の身元情報と証明書の情報を共有するというユースケース
- ブロックチェーンエコシステムは国際的な通信事業者間だけでなく、 国内通信事業者でも構築される
- ガバナンス、ポリシー、認証は今後さらに分析
- 証明書管理に関しては Solid と比較

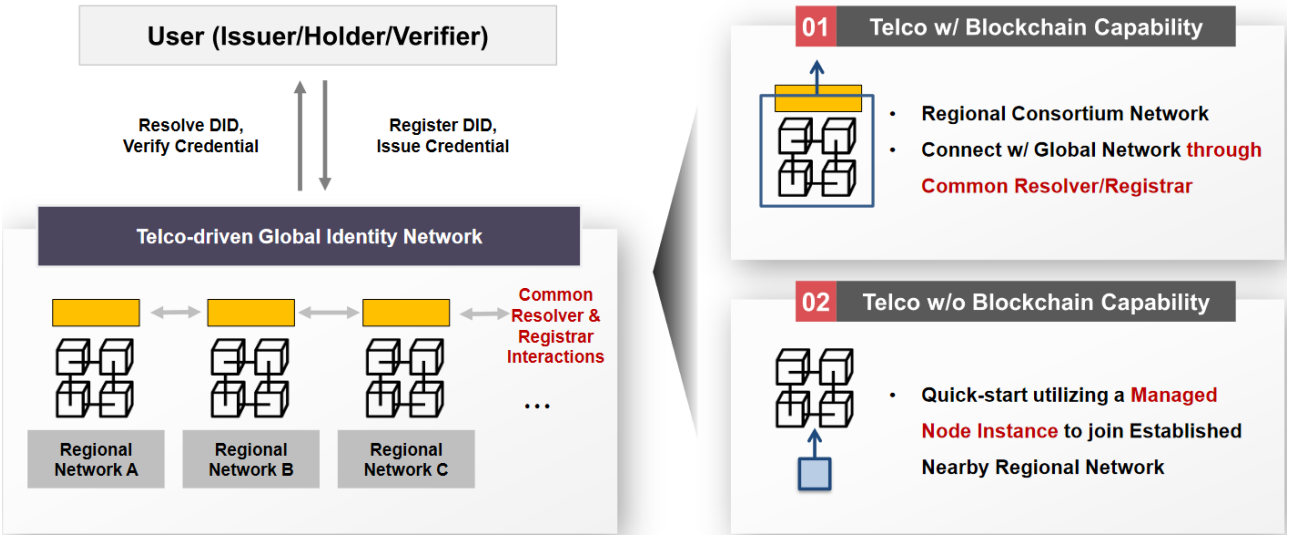

図8: ブロックチェーンのグローバル ネットワーク アーキテクチャ

(出典:SKテレコム)

5.5 AB ハンドシェイク

AB ハンドシェイクは、**オペレータ間の協力に基づいてリアルタイムで不正行為を検出し、ネットワーク間のトラフィックを検証することで、オペレータ グループ内の不正行為を排除する目的で使用されるソリューション**である。

AB ハンドシェイクは、特定の国や一連の規制に関係のない中立的なソリューションとして開発された。現在、さまざまな地理的地域にある通信事業者のライブ トラフィックを検証している。通信事業者は、同じ国内の他通信事業者の決定に関係なく、個別にオプトインしてサービスに接続できる。

スプーフィングの場合、詐欺師は発信通話の A E.164 番号を変更して、着信者がよく知っている番号を模倣する。 AB ハンドシェイクを使用すると、発信側スイッチは通話データを発信側コール レジストリに送信し、その後、インターネット (帯域外の並列 HTTP サイド パス) 経由で着信側コール レジストリへの検証要求が開始される。着信交換機は (オペレータ A からの通話を着信した後) 通話データを着信通話レジス

トリに送信する。着信コール レジストリは、A E.164 番号データに基づいて、着信側で着信した A E.164 番号が割り当てられているオペレータに検証要求を送信する。 A E.164 番号がスプーフィングされた場合、応答は通話が開始されないか (システムに参加しているオペレータの場合)、完全に応答しない。 B オペレータは、通話が不正であることをリアルタイムで検出し、通話をブロックする、あるいは、通話に詐欺のラベルを付けることが可能である。すべての通話の詳細は、調査や紛争に使用するために通話記録に収集される。A E.164 番号がスプーフィングされていない場合、オペレータ A は終了確認要求を着信し、通話が確認されたと応答する。 A E.164 番号がスプーフィングされた場合、オペレータ A は、コールが別の CLI を使用してオペレータ B に到達したという通知を受け取る。

どちらかの側からも応答がないために通話の検証が不可能な場合、通話は中断されることなく続行される。対応する通知が他の参加オペレータに送信されるため、誤検知の詐欺アラートは生成されない。通話の検証は、オペレータによって制御される通話レジストリ ノード間で直接実行され、中央データベースはこのプロセスには関与しない。通話ログは、参加しているオペレータの個別の通話レジストリに保存される。中央データベースには、参加する番号範囲とコール レジストリ ノードの IP アドレスのリストが保持される。この情報は、通話検証要求をルーティングする目的で、個々の通話レジストリに配布される。

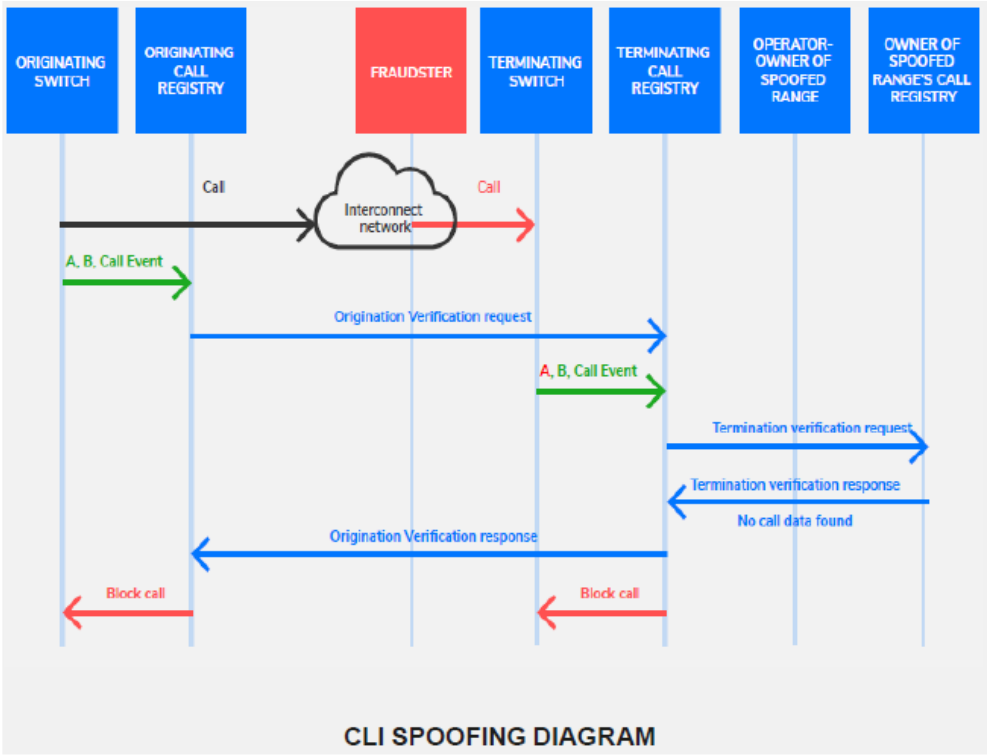

図9: CLI スプーフィング検出のための CLI 検証

（出典：ABハンドシェイク）

AB ハンドシェイクは、営利団体である AB Handshake Corporation によって推進されている。システムは帯域外検証方式を使用しており、通話確立プロセスに干渉しない。このようなアーキテクチャにより、オペレータのネットワークとの非侵襲的な統合が可能になり、IP ネットワークとレガシー オペレータ ネットワ

ークの両方をサポートできる。国際通話または市内通話フローは、この検証方法の追加による影響を受けない。

AB ハンドシェイク方式では、発信側と着信側の間のすべての通話パラメータが検証されるため、CLI スプーフィング以外の他のタイプの音声詐欺を検出してブロックできる。

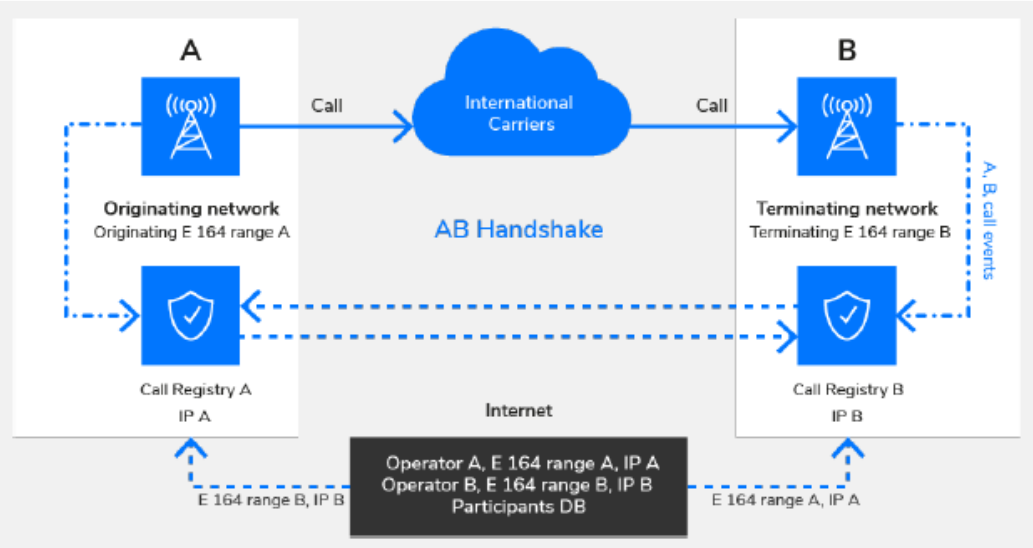

図10: AB ハンドシェイク アウトオブバンド システム アーキテクチャ

（出典：ABハンドシェイク）

同じ帯域外ハンドシェイクは、P2P および A2P SMS トラフィックの検証にも適用できる。 AB Handshake はこのサービスのトライアルを発表した。 SMS 検証ソリューションのアーキテクチャとロジックは、上記の原則に沿ったものになる。

どのオペレータが特定のアクティブな E.164 番号にサービスを提供するかについて、詳細でリアルタイムの知識が必要であるが、電話番号のサプライ チェーンの複雑さ (番号ポータビリティと再割り当て) を考慮すると、これは大きな課題である。 AB ハンドシェイク エコシステム内では、これはネットワーク レベルでのナンバーポータビリティ(NP) データベースとの統合、または認可された番号計画管理者との統合によって処理される。中立的な中央レジストリを作成して管理する必要があるようである (呼び出しレジストリをサポートするための IP アドレスも使用する)。これは国際的な観点では慎重を要する。

5.6 通話パターン分析

主な国際的ななりすましは、特定の宛先または地域への複数の通話で構成される場合がある。関連パラメータが設定されていれば、**理論上、トラフィック パターン分析により、なりすましのトラフィックを実際のトラフィックから分離できる。**特に、各国でトラフィックを受信するプロバイダは、通常、SS7 シグナリングが使用される場合に Q.708 国際シグナリング ポイント コードを保持することで、分離を行うためにトラフィックの分析を実行できる立場にある。分析の種類はすでに実装されているか、短期的に検討できるものである。

また、国際トラフィックを終端または中継する大手国際通信事業者は、不審なアクティビティを検出する必然的な立場にある。ただし、これらの関係者の主な役割は、コンテンツや CLI の使用とは関係なく、トラフィックが確実に通過するようにすることである。したがって、バリューチェーン全体の利益のために、前述の利害関係者が特定の基準を満たさないトラフィックをブロックまたはマークするという、より積極的な役割を想定することもできる。

通話パターンのトラフィックが、明らかに悪意のあるものであることを示している場合のパラメータを設定することによって契約当事者が基準を設定しサービス品質を向上させることができる。 通話パターン分析のパラメータは、正式な番号の起源の分析と組み合わせ、特定の番号またはチャネルから発生する通話量の分析に関連する可能性がある。たとえば、分析の入力として、発信元が Z の Y ゲートウェイの番号からコール数がレベル X を超えた場合、そのコールはおそらく、なりすましである可能性があるとする。

通話のブロックにはリスクが伴うため、中程度の方法としては、CLI を削除して不明な発信者としてマークを付けることが考えられる。

卸売業者は、悪者を特定するために、グループとしてこの問題に取り組む必要がある。これには、業界内および公的機関との長期にわたる協力的なサポートが必要である。情報の共有はデリケートな作業であり、一部の当事者が「機密保持」条項を悪用してこれを不可能にすることを避けるために、業界内の契約を見直す必要がある。

不正なトラフィックを助長する利害関係者を特定した後､この情報を使用して他の ECNO/ECSP に警告し、十分な措置を講じることができる。

ただし、これらのソリューションの影響によって、偽装通話の通過が必ずしも阻止されるわけではない。実際、なりすましを行う者は自身で戦略を立て、バリューチェーン内のさまざまな利害関係者がとるべきアクションを決めるさまざまなパラメータを持っている可能性がある。さらに、実装されたブロック対策で誤検知が発生し、実際の通話がブロックされる、あるいは、制限される可能性がある。しかしながら、現在のキャリアのみによるアプローチよりも積極的なアプローチが依然として望ましい。

STIR/SHAKEN では、「origid 」によって発信元が一意に識別できるため、トレースバックが可能になる。特定の発信元オペレータが信頼できない場合 (たとえば、アテステーションの不正な操作など)、これはデータ分析によって検出できる。この結果、着信側のオペレータは、CLI を削除したり、発信側のオペレータからの通話をブロックしたりするという形で措置を講じることができる。

5.7　ゲートウェイ制御

相互接続中の携帯電話通話が国の管轄区域に入ると、国際ゲートウェイを通過する。このような通話の CLI として国内の携帯電話番号が使用される場合、ネットワーク オペレータは、場合によってはサードパーティを通じて、**問題の番号に関連付けられた SIM が実際に国外にあるかどうかをゲートウェイ レベルで確認**することができる。逆の場合、つまり**国際電話が国際ゲートウェイに着信するが、CLI として使用される番号に関連付けられた SIM が実際には国内にある場合、その通話はなりすましである可能性が高いため、ブロックまたは制限される可能性がある**。このような「地理チェック」[8]により、なりすましの量を減らすことができる。

[8]必要な情報の処理には、特に e プライバシー法の観点から、さらなる分析が必要

さらに、国内通話を装った、国外から発信される国内の地理的番号による相互接続通話をブロックまたは制限することで、なりすましが減少する事が予想できる。ただし、各国の地理的な番号からの国際着信通話が許可されるかどうかは、国の政策によって異なる。

6 法的/規制的側面

EU では、CLI に関連する法がいくつか規定されている。これらの規定は主に、欧州電子通信コード指令 (EECC) の指令 (EU) 2018/1972 [36]、プライバシーと電気通信に関する指令 2002/58/EC [37]である。これらは CLI の導入に関することが中心であり、 CLI スプーフィングへの対処が目的ではない。

EECC によると、NRA は、発信側の番号が着信側に提示される CLI 機能 (EECC の第 115 条および附属書 VI パート B)を、通話が確立される前にエンドユーザが利用可能にすることを、公的に利用可能な番号ベースの対人通信サービスを提供するすべてのプロバイダに要求している可能性がある。この機能は、個人データとプライバシーの保護に関する関連法、特に e プライバシー指令に従って提供される。ただし、この義務は技術的な実現の可能性に依存する。

EECC は、以前の、電気通信部門に関するする EU 指令の大部分を置き換えたが、e プライバシー指令を廃止せず、その規定は現在も有効な状態である。

e プライバシー指令の原則と主な規定は全般的に維持された状態であり、この指令は技術的および市場の現実の進化に完全に追従していないため、電気通信に関連したプライバシーと機密性の効果的な保護と一貫性がなく、不十分な状況になっている。したがって、この指令は、提案されている e プライバシー規則 (ePR) [38]に置き換えられることになるが、これは、EECC とは異なり、加盟国の国内法の一部となる。現在の指令の国レベルでの実施により、サービスプロバイダに対する義務やユーザの権利に関してわずかな違いが生じる可能性があるが、次の規制ではおそらくこの観点で完全に調和がとれると考えられる。

したがって、適切な実施を確保できるかは、国内法が現在の指令に準拠しているかに依存する部分もあるが、現在の指令に対応する次の規制の範囲と影響にも依存する。

いずれの場合も、言及される法規定は EU 加盟国に関係するものであり、CEPT には EU 加盟国以外の欧州諸国も含まれることを考慮する必要がある。

以下のセクションでは、CLI の実装と可能な操作に関して、現在の指令および提案されている ePR において考慮する必要がある規定の概要を簡単に説明している。

6.1 欧州電子通信コード (EECC)

EECC の第 40 条 (ネットワークとサービスのセキュリティ) と第 115 条 (追加機能の提供) は、CLI スプーフィングへの対策に何らかの影響を与える可能性がある。

EECC 第 40 条によると、EU 加盟国は、公共電気通信ネットワークまたは公的に利用可能な電気通信サービスのプロバイダが、ネットワークおよびサービスのセキュリティリスクを管理するために、適切かつ相応な技術的および組織的措置を講じることを保証するものとする。最先端技術を考慮して、これらの対策は、提示されたリスクに適切なレベルのセキュリティを確保する必要があり、その他のネットワークユーザまたは他のネットワークおよびサービスへの悪影響を防ぐ対策が含まれるが、これらに限定されない。ネットワーク自体がセキュリティの危険にさらされている場合、EECC の第 40 条自体は、CLI スプーフィングに対抗するための十分な法的根拠を提供していない可能性がある。

さらに、EECC の第 115 条では、EU 加盟国は、関係する規制当局と連携して、公的に利用可能な番号ベースの対人通信サービスを提供するすべてのプロバイダに対して、CLI の機能の全て あるいは一部を無料で利用できるように要求できることを確保しなければならないと規定している。 ここで、CLI 機能とは、EECC で定義する、(音声通信のみに限定した)通話が確立される前に、受信側に提示する発信者の番号を表示する機能である。

6.2 e プライバシー指令の存在

現在の e プライバシー指令では、第 8 条 (通話および接続回線識別の表示と制限) および第 10 条 (例外) が CLI に関連している。

第 8 条

- 1. 発回線 ID の表示が提供される場合、サービスプロバイダは、発側ユーザに対し、簡易な手段で、通話ごとに発回線 ID を非表示とする機能を無料で提供しなければならない。発側加入者へは、回線ごとにこの機能の提供が可能でなければならない。
- 2. 発回線 ID の表示が提供される場合、サービスプロバイダは、この機能を合理的に使用するために、簡易な手段で、着信通話の発回線 ID を非表示とする機能を無料で着加入者に提供しなければならない。
- 3. 発回線 ID の表示が提供される場合、および通話が確立される前に発回線 ID が表示される場合、サービスプロバイダは、発回線の識別が、発側ユーザまたは加入者によって非表示の場合、簡易な手段を使用して、着呼を拒否する機能を着加入者に提供しなければならない。
- 4. 接続回線 ID の表示が提供される場合、サービスプロバイダは、簡易な手段を使用して、発側ユーザへの接続回線 ID を非表示とする機能を無料で着加入者に提供しなければならない。
- 5. 第 1 項は、EU 内の第三国への通話にも適用される。第 2 項、第 3 項および第 4 項は、第三国からの着信にも適用される。
- 6. ECC 加盟国は、発呼者および/または接続回線の ID の表示が提供される場合、公的に利用可能な電気通信サービスのプロバイダがそのことと、第 1 項、第 2 項、第 3 項および第 4 項に定める可能性について公衆に通知することを保証するものとする。

第 10 条

- ECC 加盟国は、公衆通信ネットワークおよび/または公的に利用可能な電気通信サービスのプロバイダが以下の行為を無効にする方法を、管理する明確な手順があることを保証するものとする。
- (a) 悪意のある電話または迷惑電話の追跡を要求する加入者の申請に応じ、一時的に発回線 ID の提示を排除すること。この場合、国内法に従って、発加入者の識別情報を含むデータは保存され、公衆通信ネットワークおよび/または公的に利用可能な電気通信サービスのプロバイダによって利用可能になる。
- (b) 法執行機関、救急車サービス及び消防を含む緊急電話および、国家機関によって同様に認識されている組織に対して、回線ごとに、発回線 ID の表示と、位置データの処理に対する加入者またはユーザの同意の一時的な拒否または欠如を排除すること。

CLI の有効化と無効化に関する規定を実装する場合、プロバイダは、その際に発生する可能性のある脅威を考慮する必要がある。特に言及されていないが、不正な CLI のプレゼンテーションは、着側のエンドユーザによる番号の信頼性を低下させる可能性があり、その結果、EECC 第 115 条の有効性が減少する可能性がある。

6.3 e プライバシー規制（ePR）案

提案されている ePR の第 12 条と第 13 条が CLI に関連しており、現在の指令の第 8 条と第 10 条の義務を反映している。提案された ePR の第 5 条 (電気通信データの機密保持) と第 14 条 (望ましくない、悪意のある、または迷惑な通話のブロック) が CLI スプーフィングに関連している。

- 第 5 条、電気通信データは機密とする。電気通信データの盗聴、盗聴、保存、監視、スキャン、またはその他の種類の傍受、監視および処理を含む、関係するエンドユーザ以外の者による電気通信データへの干渉は、本規約で許可されている場合を除き、禁止される。
- 第 14 条 14.1、番号ベースの対人通信サービスのプロバイダ は、エンドユーザによる不要な電話、悪意のある電話、または迷惑電話の着信を制限するための最新の対策を導入する。
- 第 14 条 14.1a、エンドユーザ、望ましくない、悪意のある、または迷惑な通話の追跡を要求する場合、ECC 加盟国は、明確な手順の確立と、番号ベースの対人通信サービスのプロバイダが、一時的な発信者番号の削除を無効にするか、そうでなければ対処する状況に関して、より具体的な規定を確立する。

電気通信データは機密であり、十分に広範かつ技術中立的な方法で定義される必要がある。これには、いわゆる通信メタデータが含まれる。たとえば、A 側の番号や B 側の番号など、通信の送信元と宛先を追跡および識別するためのデータである。 ePR 案の第 5 条では、なりすましについては特に言及されていないが、関係するエンドユーザ以外の者による同意のない、電気通信データへの干渉 (これらのデータの操作を含む) は禁止されると記載されている。このことから、電気通信サービスプロバイダはこれらのデータの信頼性に関して(共同)責任を負っていることが理解できる。

それにもかかわらず、詐欺師が CLI のスプーフィングの背後にいる場合が多く、エンドユーザが CLI スプーフィングの発信元であるようなケースは、これらの規定で直接カバーされていない。

さらに、提案された ePR の第 14 条 14.1 および 14.1a では、望ましくない、悪意のある、または迷惑な通話に関して、プロバイダは、エンドユーザによる望ましくない、悪意のある、または迷惑な通話の着信を制限するための最新の対策を導入する必要があると規定している。 第 14 条は、なりすましによって促進される可能性のある消費者問題を対象としている。前文 29 (ePR) から、番号ベースの対人通信サービスのプロバイダは既存のテクノロジーを導入し、番号計画に存在しない番号、番号ベースの対人通信サービスのプロバイダに割り当てられていない有効な番号、割り当てられているがエンドユーザには割り当てられていない有効な番号などの無効な番号から発信される通話など、望ましくない、悪意のある、または迷惑な通話からエンドユーザを無料で保護する必要があることがわかる。これは、提案されている ePR の第 5 条および EECC の第 40 条に沿って行われるべきである。

総括

EU では、**EU 加盟国に対し、公的に利用可能な番号ベースの対人通信サービスのプロバイダに発回線 ID の表示を義務付ける国内規定を確立することを奨励**している。この規定の目的は、**発信者番号を識別し、電気通信サービスのユーザが公衆音声通信におけるプライバシー保護のレベルを選択できる**ようにすることである。 CLI の情報が信頼できない場合、この目標は損なわれる。その場合、EECC 第 115 条に基づいて電気通信プロバイダによって実装された機能の有効性は、意図した効果の一部 (またはすべて) を失うことになる。

公的に利用可能な番号ベースの対人通信サービスのプロバイダが自発的または国レベルでの義務付けで CLI を提供する場合、EU の法律から、そのプロバイダは、その結果として、着信側に正しく配信される情報はネットワーク内で確実に保持されるように措置を講じる責任を負っていることが理解できる。ただし、この点に関しては、相応な技術的および組織的措置の原則が、EECC および、ePR からは、最先端技術を使用するという原則が適用される。この法的状況は、電気通信サービスプロバイダがあらゆる場合において EECC 第 115 条の目標に完全に貢献するための十分な手段を持っていない可能性があることを考慮していると思われる。このようなケースは通常、通話が終了する国の国外ネットワークから信頼できない CLI が発信された場合に発生する。

前述の **EU の規定に欠けている要素は、これらの要件が公共の電気通信ネットワークおよびサービスのプロバイダのみに向けられているということ**である。 **CLI スプーフィングの実践におけるエンドユーザの役割は、VoIP テクノロジーの成長とともに増大**しており、これらの**当事者を CLI スプーフィングを禁止する条項の共同の対象として含めない理由はない**。

提案されている ePR の立法プロセスの結果次第では、特に第 5 条と第 14 条は、CLI スプーフィングをさらに防止するための国家的措置の議論に影響を及ぼす可能性がある。

[38]に沿ったものである必要があり この措置には、ECSP/ECNO がサービスに入れる CLI 情報を検証する合理的な手段がない場合に、CLI 情報をマスクしたり、通話をブロックしたりする許可または義務が含まれる場合がある。

規制措置が講じられているにもかかわらず、多くの責任は依然としてプロバイダとエンドユーザ自身にある。このような規制と合わせて、CLI スプーフィングを最小限に抑えるには、迅速かつ効果的な措置が不可欠である。

6.4 2020 年 12 月 18 日の欧州委員会の委任規則 (EU) 2021/654

欧州委員会委任規則 (EU) 2021/654 [39] は、ユーロ レートと呼ばれる単一の欧州連合全体の最大モバイル音声終端レートと単一の最大欧州連合全体の固定音声終端レートを設定している。この規制により、通信事業者は、CLI が欠落している場合、無効である場合、または不正である場合、通話において、連合全体で、呼終端料金を適用しない権利が与えられている ([39]の備考 15 を参照)。

このアプローチでは、不正行為は報われない。さらに、オペレータがなりすましの CLI トラフィックを着信しようとする場合、着側オペレータに追加の相互接続料金を請求できるようにすることは有益かつ適切である。これらの追加料金は、なりすましトラフィックの防止と検出のために、これらの着側事業者が負担するコストをカバーする必要がある。

何が CLI スプーフィングとみなされるか、何がみなされないかについて明確な検証可能なルールを定義する必要がある。定義をしない場合、着側事業者がこの権利を利用して、通話の伝達に関係する他のネットワーク オペレータからは法外とみなされる料金を請求される可能性があるからである。

7　さらなる分析と考察

欧州のすべての通信事業者が、規制介入なしに自主的に CLI スプーフィングに対抗するシステムを導入する可能性は低い。その意味では、対応する法律の施行後に事業者が初めて STIR/SHAKEN を大規模に導入する米国の状況と類似している。

この規範の既存の規定と、現行の e プライバシー指令は法的根拠が弱く、CLI スプーフィングを防止するテクノロジーを義務付けるには不十分である可能性がある。提案されている e プライバシー規則は、第 14 条 14.1 および 14.1a でより強固な法的根拠を提供しているが、これらのサブ条項は原則に限定されており、重要であるが、おそらく十分ではない。

本質的に国際的な問題に対して非効率な国家的解決策につながる断片的なアプローチには明らかにリスクがある。

番号の悪用や不正使用を目的とした CLI スプーフィングを禁止するには、EU の法律に含める必要がある。さらに、相互運用性を確保するために、各国が遵守しなければならない一連の共通原則と調和のとれた技術を設けることが推奨される。

短期的には、トラフィック パターン分析により問題の一部が軽減される可能性があるが、一般にリアルタイムの解決策ではない。**国レベルでも、ITU や BEREC などの国際/地域フォーラムでも、CEPT 行政は業界団体が、CLI スプーフィングと戦うためのトラフィック分析と情報共有に関する議論を促進するように対応する必要**がある。

おそらく、着信側番号と発信側番号の両方が米国の番号である通話を終端したいすべてのヨーロッパの通信事業者は、いずれ STIR/SHAKEN を実装する必要があるであろう。明らかに、このテクノロジーには先行者利益がある。非リアルタイム ソリューションでは問題は解決されないため、リアルタイム ソリューションが必要である。ブロックチェーンや SOLID など、CLI スプーフィングに対抗する他のテクノロジーは、非常に未熟な段階にあるか、非リアルタイム ソリューションとしてのみ使用できる。したがって、**ヨーロッパが STIR/SHAKEN を、CLI スプーフィングとの戦いを支援する大きな可能性を備えた強力な候補として考慮するのは適切である。ただし、さらなる研究が必要な側面もいくつかある。**

STIR/SHAKEN または欧州版の STIR/SHAKEN とその実装が GDPR および将来の e プライバシー規制に準拠していることを確認する必要がある。それは行われなければならない分析である。 STIR/SHAKEN では、悪意のある者による不正行為を検出するために、通話のトレースバックが不可欠である。したがって、これらの目的で GDPR/e プライバシー規制に従って CDR (通話詳細記録) を使用できるかどうかを評価する必要がある。また、競争の観点から、扱いに細心の注意が必要である評価システムを「養う(構築していく)」ためには、関係者全員による情報共有の協力が必要である。

欧州で調和のとれた展開とさまざまな国でそれに関連するガバナンス システムの展開があれば、優位となるであろう。 そのため、アプローチは「可能な限り国際的」である必要がある。 EU/CEPT の共通アプローチが最低限であり、世界的なアプローチが理想である。したがって、STIR/SHAKEN 業界フォーラムを設立するというアイデアは、現実的な前進である。ただし、ヨーロッパ諸国では重要な機能を維持することが推奨されるべきである。

全ヨーロッパへの展開は、規模と調和の点で利点をもたらす。 WG NaN の要請に応じて、EC は、新しいアクション (8)「SDO は、CLI スプーフィングを軽減、防止、および/または検出するための対策に関す

る報告書を作成する。報告書は、技術的、運用的、標準化および欧州の観点から、考えられるさまざまなソリューション(STIR/SHAKEN、ブロックチェーン、SOLID など)のコスト面を検討する必要がある。また、そのようなソリューションを欧州レベルでどのように展開し、管理できるかについても検討する必要がある」と EU ローリングプラン 2021 にまとめた。

ガバナンス構造と展開に関連するコストは、選択したソリューションによって異なり、EU またはより大規模な CEPT ソリューションに基づく可能性がある。いずれの場合も、ソリューションは他の同様のシステムと相互運用できる必要がある。

オペレータが世界的なシステムに参加できるように、満たすべき基準 (たとえば、番号リソースに直接アクセスできるエンティティのみ、おそらくより厳格な基準) を調和させることは不可能である。この点に関して、将来の研究では、基本層（最小レベル）と第 2 レベルの 2 層で構成されるハイブリッド モデルを採用するメリットも調査される可能性がある。基本レベルの場合、最小基準は次のようになる。番号リソースが直接割り当てられている当事者のみ、およびユーザの認証に関する最小限のルールを満たす当事者のみがデジタル証明書を取得できる。 2 番目のレベルは、経験から得られたデータから導き出された「評判」に基づいている可能性がある。

また、AB ハンドシェイクなどは他のタイプの詐欺 (ワンギリ、通話ハイジャックなど) に直接適用できることに注意することも重要であるが、ハンドシェイクは独自のソリューションであり、STIR/SHAKEN などのソリューションのようなオープンな対策と比較して幅広い適用性の点で不利と見なされる可能性がある。

STIR と組み合わせた SOLID の実用化は GSMA で議論され、 STIR/SHAKEN/ が FCC によって施行され、北米の通信事業者全体に広がっていることを考慮すると、STIR/SHAKEN/ と比較した場合、限定的な追加のメリットしか得られないことが判明した。そうは言っても、両方のフレームワークには互換性があり、SOLID は STIR/SHAKEN よりも幅広い詐欺防止範囲に対応している。

8 結論

CLI スプーフィングによって引き起こされる被害を考慮すると、CEPT 管理者が次のアプローチを取ることは適切である。

1 国内法で、オペレータだけでなくユーザも含めた CLI スプーフィングを明示的に禁止する。

2 特に CLI への対処方法に関する CEPT 諸国における調和された規制ガイドラインおよび/または強制規則をさらに詳細化する:

- どのようなトラフィックがスプーフィングとして認定されるかを決定するための明確な技術的ルールを定義する。
- なりすまし通話を処理するさまざまなオペレータのそれぞれの責任を明確に決定する。
- CLI スプーフィングに責任のあるエンティティおよび/または個人に制裁を課す。
- 必要に応じて、CLI スプーフィング活動の疑いによりトラフィックをブロックする事業者に対して、より明確な法を提示する。
- オペレータ間の CLI スプーフィングに関する情報共有イニシアチブのサポートを奨励する。
- 人工知能に基づく通信パターン分析ツールのオペレータによる設置を奨励する。
- ユーロレートを設定する委任規制（EU）2021/654 に完全に準拠して、着側事業者または通信事業者が「相互接続追加料金」を課すことができる範囲に対処するための解決策を検討または提案する。

3 呼のトレースバックについてヨーロッパの調和されたアプローチの展開を検討し、開発する。

4 なりすましの疑いのある国内 E.164 番号から発信された着信トラフィックに対して、国際ゲートウェイで実装するブロック メカニズムに関する ECC 勧告を検討する。

5 以下の基準を考慮して、CLI スプーフィングを排除することを目的とした、STIR/SHAKEN、AB ハンドシェイク、SOLID、分散台帳テクノロジー (ブロックチェーンなど) などの技術的手法のさらに分析する。

- 国家の分断を可能な限り回避する。
- ネットワーク(非 IP ネットワークなど)への影響と実装と管理のコストを最小限に抑える。
- 国内法の遵守。
- その他の地政学上の地域における開発状況。
- 他の種類の詐欺や不正行為と戦うための選択肢の将来を見据えた可能性。

6 選択されたアプローチを CEPT 諸国で調整して展開する。

ANNEX 1: 参考文献のリスト

[1] ECC 勧告 (19)03 :「発呼側識別および発信側識別の信頼性を高めるための措置 (Measures for increasing Trust in Calling Line Identification and Originating Identification) 」 、2019 年 11 月承認

[2] ECC レポート 248 : 「CLI 使用法の進化 – 番号の使用権とサービス提供の切り離し (Evolution in CLI usage – decoupling of rights of use of numbers from service provision) 」 、2016 年 4 月承認

[3] ECC レポート 275 :「電気通信サービスの国際詐欺と悪用における E.164 番号の役割」、2018 年 5 月承認

[4] 電気通信ネットワークおよび電気通信サービスに関するノルウェー規制 (Ecom 規制) (ノルウェー語のみ)

[5] Ofcom UK - General Conditions of Entitlement - 非公式統合版。

[6] 勧告 ITU-T E.164:「国際公衆電気通信番号計画」、2010 年 11 月

[7] 英国 全国電話番号計画

[8] Ofcom UK:「発信者回線識別機能およびその他の関連サービスの提供に関するガイダンス」、2018 年 7 月 30 日。

[9] ラトビア公共事業委員会理事会決定第 1/20 号-番号付けを使用した詐欺行為の排除に関する規則- 2015 年 12 月 3 日に採択

[10] ラトビア 電気通信法

[11] 2017 年 3 月 30 日、リガの公益事業委員会評議会決定第 1/13 号 (議定書第 13 号、項目 6)。電気通信ネットワーク相互接続サービスの技術および運用規定。

[12] 2018 年 12 月 20 日、リガの公益事業委員会評議会決定第 1/35 号 (議定書第 54 号、項目 7)。電気通信分野における一般認可規則

[13] 決定番号 2012-0856 号 （2012 年 7 月 17 日）電気通信および郵便規制庁は、 2005 年 12 月 15 日の決定番号 05-1085 (35 ページ) で規定されている 08 で始まる番号範囲と短縮番号の構成を修正。（フランス語のみ）

[14] ニュース記事: 「暴力的な訪問販売との戦いの原動力である Orange は、1 億 1,100 万件のスパム電話をブロックした」、2019 年 12 月 12 日 (フランス語のみ)

[15] 決定番号 2019-0954 (2019 年 7 月 11 日) 国内番号計画とその管理規則を確立する決定を修正。 (フランス語のみ)

[16] 決定番号 2014-1485（2014 年 12 月 9 日）電気通信および郵便規制庁における、フランスの固定ネットワーク上の音声通話の終了およびフランスのモバイル ネットワーク上の音声通話の終了に関連する市場の決定。市場に重大な影響を与える事業者の指定と、2014 年から 2017 年の期間にこのタイトルに課せられる義務。 (フランス語のみ)

[17] 決定番号 2017 1453（2017 年 12 月 12 日）電気通信および郵便サービスの規制当局における、フランスの固定ネットワークでの音声通話の終了およびフランスでの音声通話の終了

に関連する関連市場の決定。フランスのモバイル ネットワーク、これらの市場に重大な影響を与える通信事業者の指定、および 2017 年から 2020 年の期間にこのタイトルに課せられる義務について説明。_(フランス語のみ)

[18] ドイツ電気通信近代化法 (TKMG)、2021 年 6 月 23 日。(ドイツ語のみ)

[19] 勧告 ITU-T E.156:「E.164 番号リソースの不正使用の報告に対する ITU-T の行動に関するガイドライン」

[20] 勧告 ITU-T E.157:「国際発呼者番号の配信」

[21] IETF RFC 7340: 「安全な電話 ID に関する問題の声明と要件」

[22] IETF RFC 7375: 「安全な電話 ID 脅威モデル」

[23] IETF RFC 8224: 「SIP における認証されたアイデンティティ管理」

[24] IETF RFC 8225: 「PASSporT: 個人アサーション トークン」

[25] IETF RFC 8226: 「安全な電話 ID 認証情報: 証明書」

[26] ATIS 1000074: Signature-based Handling of Asserted information using toKENs (SHAKEN)」

[27] ATIS 1000080 : 「Signature-based Handling of Asserted information using toKENs (SHAKEN): ガバナンス モデルと証明書の管理」

[28] ATIS 1000081: 「確認済みの発信者 ID を表示するためのフレームワークに関する技術レポート」

[29] ATIS 1000082: 「集中署名および署名検証サーバー用の SHAKEN API に関する技術レポート」

[30] ATIS 1000084: 「SHAKEN STI 認証局およびポリシー管理者向けの運用および管理上の考慮事項に関する技術レポート」

[31] ATIS 1000085: 「SHAKEN の「div」PASSporT のサポート」

[32] 「第 28 条 (2) USD ユニバーサル サービス指令: 調和された BEREC 協力プロセス - BEREC ガイダンス ペーパー」に関する BEREC BoR (13)37

[33] ITU-T 技術仕様 FG DLT D1.1:「分散台帳技術の用語と定義」、2019 年 8 月

[34] ITU-T テクニカルレポート TR.spoofing (06/2021): 「スプーフィングへの対策」

[35] 勧告 ITU-T Q.3057 (04/2020): 「信頼できるネットワーク エンティティ間の相互接続のためのシグナリング要件とアーキテクチャ」

[36] 2018 年 12 月 11 日の欧州議会および理事会の欧州電気通信規約を確立する指令 (EU) 2018/1972。

[37] 電気通信部門における個人データの処理とプライバシーの保護に関する、2002 年 7 月 12 日の欧州議会および欧州理事会の指令 2002/58/EC (プライバシーおよび電気通信に関する指令)。

[38] 電気通信における私生活の尊重と個人データの保護に関する欧州議会および欧州理事会の規制、および指令 2002/58/EC (プライバシーおよび電気通信に関する規制) の廃止に関する提案

[39] 欧州議会および欧州理事会の指令 (EU) 2018/1972 を補足する、2020 年 12 月 18 日の欧州委員会委任規則 (EU) 2021/654。単一の最大連合全体のモバイル音声終了レートと単一の最大連合全体の固定音声終了レートを設定 (EEA 関連のテキスト)。