ITU-T Workshop報告 −SS7セキュリティ&ICT模倣品対策−

日本電気株式会社　テレコムキャリアビジネスユニット エキスパート　谷川（たにかわ）　和法（かずのり）

1. はじめに

2016年6月下旬から7月上旬にかけて、スイス（ジュネーブ）のITU本部においてITU-T SG11会合が開催された。会合期間中に最近話題となっているSG11の活動に関連する2つのトピック「SS7セキュリティ」と「ICT模倣品*対策」についてのワークショップが設けられていた。両ワークショップとも多くの参加者を集めて活発な議論が行われており、本報告では興味深いワークショップの内容を紹介する。

2. ワークショップ「SS7セキュリティ」

2.1　概要

2014年にドイツの研究者から世界中の携帯通信事業者で用いられているSS7（Common Channel Signaling System No.7：共通線信号No.7）に重大な脆弱性があることが報告されて以来、巷間話題になっているテーマである。ワークショップの概要は以下のとおりである。

- **タイトル**：Workshop on“SS7 Security”（下記URLにプレゼン資料）
  http://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx
- **日時・場所**：2016/06/29, 09：00−12：30、ジュネーブ、ITU本部、POPV1
- **コーディネータ**：Cheng Li氏（Q2/11ラポータ、CAICT、中国）
- **セッション1**：SS7問題の現状
  - Security Aspects in SS7 Networks, Gerhard Ott, Deutsche Telekom, Germany
  - SS7 Security – How to Fill in the Standardization Gap, Giulio Maggiore,TIM, Italy
  - Alternative Solutions for the Improvement of SS7 Security, Minrui Shi, China Telecom, China
  - Observations on SS7 Network Security, Pascal Dejardin, Orange Group, Belgium
- **セッション2**：SS7問題への対策
  - Effective SS7 Protection, Luca Melette, Security Research Labs, Germany
  - Statistics of Vulnerabilities in SS7 Networks and Ways to Make them Secure, Dmitry Kurbatov, Positive Technologies, United Kingdom
  - An Update from GSMA on Interconnect Security and Industry Efforts to Restore Trust, Dominique Lazanski, GSMA

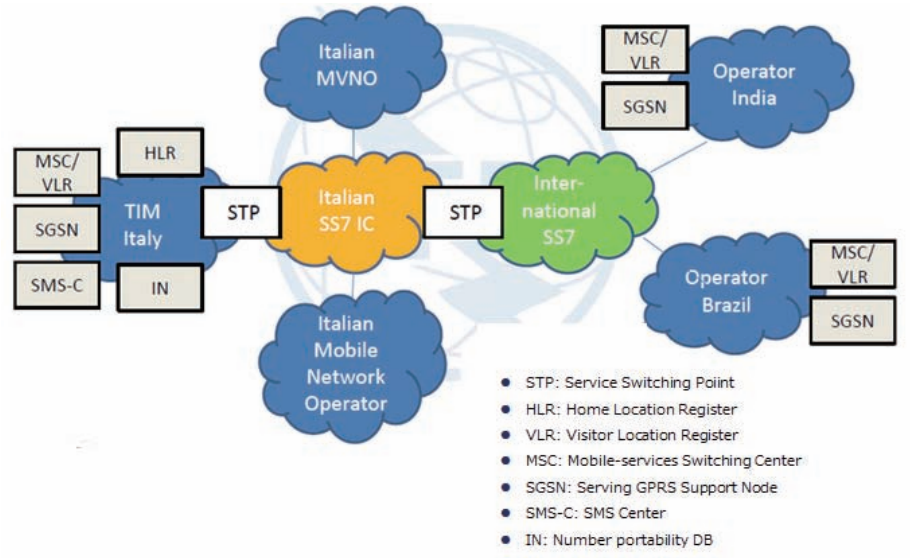
セッション1では、欧州及び中国の4つの通信事業者の取組みが紹介された。イタリアテレコム社からは、世界各国のSS7セキュリティレベルの調査報告（2014年度）が、フランスOrange社からはSS7関連の不正動向のモニタリングについて報告があった。続くセッション2では、セキュリティベンダ2社とGSMA（GSM（Global System for Mobile communications）Association）から不正に関する具体的な手口やその対策について紹介があった。

2.2　SS7ネットワーク

SS7とは、主に電話での制御信号を規定したもので、ほかにも発信者番号通知、プリペイド課金、SMS等の仕様を含む。SS7ネットワークはSTP（Signal Transfer Point：SS7ネットワークのルータ/ゲートウェイへ）により接続され、当初は、音声とは別の専用ネットワークが使われてきた。2G（Second Generation：第2世代移動通信システム（GSM））及び3G（Third Generation：第3世代移動通信システム（W-CDMAやCDMA2000））携帯端末の国際間ローミングはSS7により実現されており、 世界中各国800を超える通信事業者がこれを利用している。

SS7は1975年から開発を始め、1980年にQ.7XXシリーズ勧告としてITU-Tにより国際標準化されている。また、IETF（Internet Engineering Task Force）が、2000年にSIGTRANと呼ばれIPプロトコル上でのSS7の送受信仕様（SS7 over IP）を策定し、ネットワークのIP化に対応している。

＊模倣品は、産業財産権、すなわち、特許権、実用新案権、意匠権、商標権を侵害する物品である。一方、知的財産権のうちでも、著作権や著作隣接権を侵害する物品は海賊版と呼ばれる。



■図1. 国際SS7ネットワークイメージ

携帯電話ネットワークにおけるSS7では、MAP（Mobile Application Part）というリンク間のアクセス（図中の略号装置間の通信）に使われるアプリケーションレイヤーのプロトコルが重要な役割を担っている。

2.3 SS7脆弱性の要因

SS7は、開発時には通信事業者間で閉じた専用ネットワークで用いられることを想定していたことから、認証や正当性検証といった基本的なセキュリティ機能を具備していない。このため、2000年にIP上で処理が可能になると同時にSS7ネットワークはセキュリティの脅威にさらされることになる。

国によっては、SS7ネットワークの接続のために必要なSS7ハブが容易に購入できたり、法的責任内容、セキュリティ措置、監視義務が曖昧なままに通信事業者ライセンスが簡単に発行されてしまったりすることもセキュリティ問題の一因である。SS7ハブへの接続サービスを提供する違法業者さえ出現している。このほか、SS7での転送用アドレス情報となるGT（Global Title）の自由な発行、セキュリティ上の問題を抱えるNW機器の流通、オペレータのネットワーク設定業務のミス等も脆弱性の要因に挙げられる。

昨今のグローバル化に伴う国際ネットワーク間接続の促進、VoIPやデータアプリケーション等の新サービスの登場、通信事業参入の規制緩和による様々な事業者の参入等の時代の変化によってSS7ネットワークへのアクセス数は増加傾向にあり、それに伴いセキュリティリスクも増してきていると言える。

2.4 顕在化するセキュリティ脅威

SS7のセキュリティ脅威に気付いた通信事業者は、P1 Security 社に世界的なSS7のセキュリティ状況の調査を委託しており、2014年12月に164か国の調査内容がWeb上で報告されている（http://ss7map.p1sec.com/）。調査内容は、以下のように大別される。

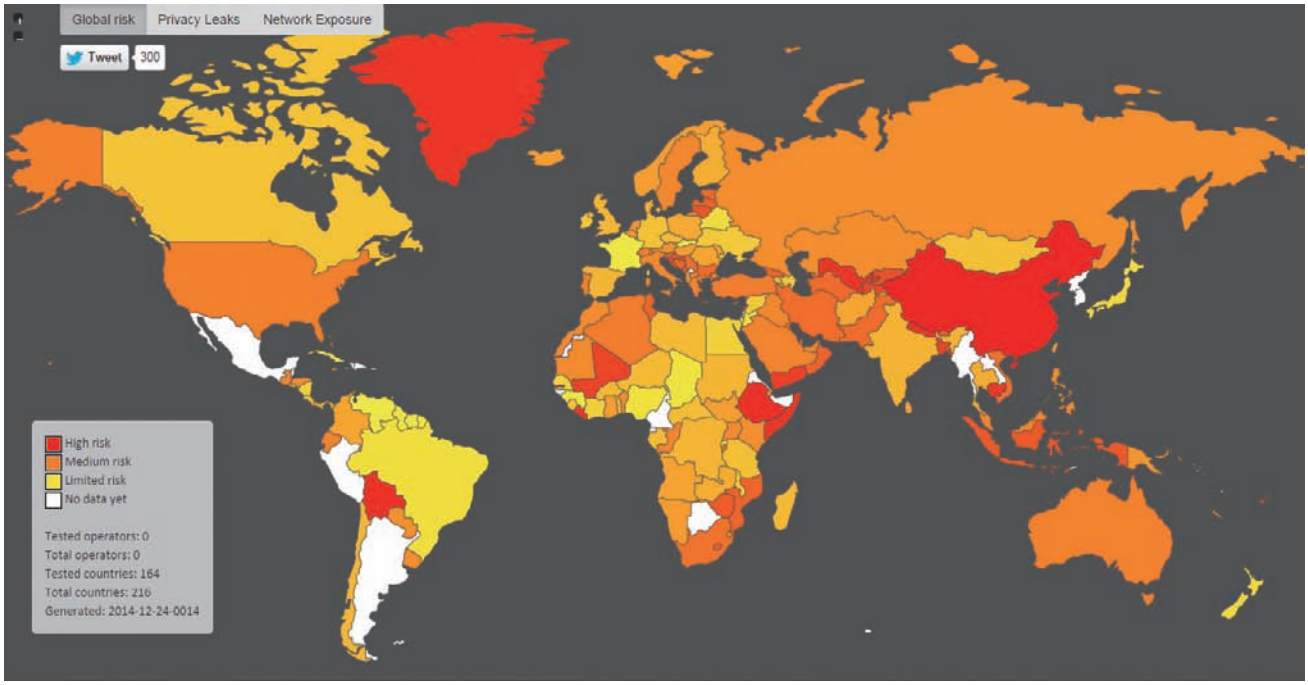
●Privacy Leaks：SS7ネットワークでの個人情報漏えいの危険性
- ・加入者位置情、個人情報（各種ID、暗号キー、支払状況等）、通信の秘匿状況

●Network exposure：ネットワーク関連情報流出の可能性
- ・ネットワークの論理構成、ネットワーク機器のIDの漏えい、NW設定ミス、NWセキュリテイメカニズムを回避される可能性

●Global Risk：上記2項目を組み合わせたリスク状況

調査は、SS7通信のオープンソースソフトウェアを用いて、実際に複数の通信事業者ネットワーク上でGT、MSISDN（Mobile Subscriber Integrated Services Digital Network Number：SIMカードに対応した携帯電話網への加入を一意に識別する番号）等を収集している。

SS7セキュリティ対策は、SS7トラフィック及び国際間通信が多くなればなるほど難しいものとなっており、欧米諸国であってもフランス以外はセキュリティ評価が下位にとどまっている（日本は19位と好評価）。



■図2. SS7セキュリティマップ

SS7による被害は、これまでの調査分析により以下のように分類することができる。

1）情報不正取得
- ・MSISDNやIMSI（International Mobile Subscriber Identity：国際的な加入者識別番号でSIMカードに記録）を不正取得。
- ・MAPコマンドで偽の情報を用いてHLR（Home Location Register：加入者情報の管理データベース）から加入者の位置情報を取得。

2）通信傍受/監視
- ・MAPコマンドの通信転送機能を悪用して、SMSの発信及び着信内容を傍受。

3）窃盗（盗用）/偽造
- ・SMSを悪用してインターネット上のアカウントを乗っ取り。
- ・USSD（Unstructured Supplementary Service Data：携帯でのプリペイドやオンラインバンキング等の金銭を扱うサービスで使われるデータ）を悪用した送金や物品購入の被害。

4）サービス妨害/中断
- ・加入者データベースの加入者情報（加入者識別情報、現在位置等）を書き換えて通信サービスの実施を妨害

各類型におけるMAPコマンドの組合せ例が、各社資料で紹介されている。

2.5 セキュリティ脅威への取組み

DT、Italia Telecom、China Telecom、Orangeから通信事業者各社のSS7セキュリティに関する取組みが紹介されている。各社とも時間と工数をかけて独自のセキュリティ調査を実施しており、分析結果に基づいた個別具体的な対策を実施してきている。

携帯通信事業者や関連事業者の業界団体であるGSMAでは、モニタリングガイドラインやGT発行ガイドラインの作成、リスク対策に向けた要求条件とソリューション検討、携帯事業者間の相互接続における契約締結の支援等を実施している。また、通信事業者間の接続及び通信パケットは必ずしも信用できないということから、国際ローミング協定を結ぶ際にモバイル事業者間で交換する事業者情報データベース（IR.21）の充実を図っている。GSMAでは、自社加入者が他社ローミングパートナーのネットワークに移動した場合のセキュリティを担保するために、Home Routing（他社ネットワークに移動中の自社加入者に対して外部からの着信メッセージがあった場合は、全てのメッセージは自社ネットワークを経由して転送する）を推奨している。また、国際標準の修正として、これまで引きずってきたSS7仕様自体に基づくセキュリティ問題の解決は、

4G（Fourth Generation：第4世代移動通信システム（LTE：long Term Evolution））でのDiameterの採用という形に先送りされることが述べられている。

通信事業者にとってセキュリティ対策の実施の上で悩ましいことの一つには、通信の自由の保障がある。国際間通信では他国での通信サービスの状況によりSS7コマンドやパラメータの組合せは多岐に渡り、疑わしいと思われる通信を一律の条件で全て止める訳にはいかない。また、事業者として、投資対効果の問題もある。セキュリティベンダからも、これまでの調査から違法な通信のバリエーションの洗い出しはほぼ完了しているが、そのセキュリティ対策に容易なケースと難易度が高いケースが存在することが指摘されている。各プレゼンターからは、現在の対策が良好であっても将来に渡って完璧なものではないとして、継続的な問題の監視とその迅速な対処の重要性が各社から繰り返し述べられた。

3. ワークショップ 「ICT模倣品対策」

3.1 概要

本テーマは、本研究会期（2013－2016）においてITU-Tの重要な研究課題としてQ8/11が取り組んできたものである。ワークショップの概要は以下のようなものである。

●**タイトル**：ITU Workshop on “Combating Counterfeit Using Conformance and Interoperability Solutions”（下記URLにプレゼン資料）
http://www.itu.int/en/ITU-T/Workshops-and-Seminars/20160628/Pages/default.aspx

●**日時・場所**：2016/06/28, 14：00－18：00、ジュネーブ、ITU本部、POPV1

●**コーディネータ**：Isaac Boateng氏（Q8/11ラポータ、NCA、ガーナ）

●**セッション1**：現在の政府レベルでの取組みと挑戦

・The Economic Cost of Counterfeiting in EU and the Jointly ITU/BDT-EUIPO Research on Counterfeiting of ICT Devices, Carolina Arias Burgos, EU and Carmen Prado-Wagner, ITU-D

・Combating Counterfeit ICT – Conformity Assessment as a Tool, Joao Alexandre Zanon, Anatel, Brazil

・Overview of National Initiatives and Solutions to Combat Counterfeit Mobile Devices, Dmytro Protsenko, Ukrainian State Centre of Radio Frequencies（UCRF), Ukraine

・Regulatory Proposal in Colombia to control IMEIs in mobile networks（malformed, invalids, duplicated, non-homologated, not registered), Hugo Romero, CRC, Colombia

●**セッション2**：将来的な取組みと既存の技術ソリューション

・Blockchain to Combat Counterfeit Products, Adrian Mccullagh, ODMOB Lawyers and John Flood, ［Biography］Griffith University, Australia

・Combating Grey Devices, Audrey Scozzaro Ferrazzini, Standardization and Industrial Policy Leady, Qualcomm

・Industry Cooperation to Tackle Counterfeiting in Mobile Communications, Thomas Barmueller, Mobile Manufacturers Forum MMF

・A Mutual Benefit of Mobile Operators and Governments to Deploy Device Management Systems, Joseph Eid, Invigo, Lebanon

オープニングセッションで、OECD（Organization for Economic Co-operation and Development）による模倣品動向に関する調査が紹介された。本報告での模倣品の被害状況に鑑みると、模造品対策は開発途上国と先進国双方にとって重要な課題であることが分かる。

セッション1では、ブラジル、ウクライナ等における国家レベルでの携帯電話の模倣品対策が紹介され、模造品対策とともに盗難品の流通対策も重要であることが述べられた。セッション2では、携帯電話における模倣品対策としてのIMEI（International Mobile Equipment Identity：携帯端末識別番号）データベースの活用や、製造番号管理のためのブロックチェーン技術等の対策ソリューションが紹介された。

3.2 ICT模倣品対策の経緯

今研究会期（2013－2016）では、SG11で国際標準化団体間の連携を担当するQ8/11において不正ICT端末対策について具体的な検討を進めてきている。

新興国を中心に不正ICT機器が多く流通しており経済上安全上の懸念から国際的な対策が必要であるとして、2014年、ITU全権委員会議（PP-14）において決議177“ICT端末偽造品対策”（Busan, 2014）が採択され、WDC-14においても同様に決議79“ICT端末偽造品への対処及び扱いにおけるICTの役割”（Dubai, 2014）が採択されている。

同年、Q8/11にて議論中であった模倣品対策の技術レ

ポートTR-Counterfeitingに関連するワークショップが開催され、政府系組織（ウクライナ、ガーナNCA、UAE TRA、ブラジルANATEL、英国BIS、中国MIIT）、国際機関（WIPO、EC、WTO、OECD、WCO、IFPMA）、産業界（MMF、GSMA、Cisco、Microsoft、HP）、非営利研究開発企業（米国CNRI）等の多くの関係団体が参加して意見が交わされている。以来、今回を含めて計4回のワークショップが開催されている。

3.3　OECD調査報告

OECDでは、ICT機器だけではなく観賞用DVDや服飾品といった全ての知財保護商品を対象として、WCO（World Custom Organization：世界税関機構）、TAXUD（Taxation and Customs Union、EC）、米国国土安全保障省が連携して模倣品の被害状況を調査し、以下の報告書が公開されている。

●Trade in Counterfeit and Pirated Goods：Mapping the Economic Impact
http://www.oecd.org/gov/risk/trade-in-counterfeit-and-pirated-goods-9789264252653-en.htm

2013年度の世界規模の被害状況は、4610億USD（貿易総額の2.5%相当）で、その内、EU域内での被害は1160億USD（EU貿易総額の5%）と、知的所有権侵害の被害の深刻さが伝えられている。主な被害国が米国、EU諸国、日本といった先進国であることに驚きはないが、報告書の中では模倣品の製造元が明示されている。

また、模倣品被害全体の傾向や課題として、流通経路の複雑化（海外拠点からの小口配送）、貿易拠点の巨大化（香港、シンガポール、ドバイ等）、政府統制の甘さ（シリア、アフガニスタン等）が挙げられている。

■図3.　模倣品の製造国

3.4　携帯電話模倣品の特徴

ITU-Tが対象とするICT機器の流通は、2013年時点で世界貿易総額の9.8%に昇り、携帯電話の取扱いがその8割を占めている。

犯罪者ネットワークでは、（刑罰が厳しい国でも）他の犯罪に比べて刑が軽い、製造コストの10倍で販売、インターネット経由でグローバルに販路を確保、国の法規制の適用外でのビジネス、拡大するインターネットバンキングやオンラインの支払いで簡単に決済、といった点からローリスク・ハイリターンの安定した収入源と捉えられている。

携帯電話端末製造業者による業界団体MMF（Mobile Manufactures Forum）の調査によると、70%の一般消費者が模倣品端末の品質は正規品と同程度と考えており、これも被害防止の難しい要因である。3GPP（Third Generation Partnership Project）による調査によれば、模倣品では、頻繁な通話断（4回に1回）、ハンドオーバ時の長い遅延時間（平均41%増）、ハンドオーバ失敗（3回ごと）、通話可能な地上局からの距離が正規品の半分程度、データ伝送スピードが表記仕様以下といった問題があることが指摘されている。また、模倣品20端末中11端末に、SMSの不正操作、端末設定やユーザ情報への不正アクセス、アドウェアといった不正ソフトがインストールされていた。

携帯電話の模倣品流通による影響は、関係者ごとに以下のように整理することができる。

●政府：税金・関税逃れによる収入減、国際間の規制の必要性（輸入、販売、認証、IMEI変更等）、公共の安全に脅威（不正IMEIやIMEIデータのない端末からの犯罪やテロ）、雇用機会の喪失
●産業界：正当な権益の喪失（OEM収入の逸失、不正な競争、セールス減、価格変動、知財侵害等）
●通信事業者：提供するQoS低減（カバー率低下、音声orデータ喪失、通信速度低下）、潜在的な電波干渉の可能性、不要な技術的対策の支出（アンテナ設置、基地局、周波数帯利用）
●ユーザ：サービス品質の低下、健康面での危険性（鉛のような危険物質の利用、高い電波の比吸収率（SAR）、バッテリー爆発）、個人情報の漏えい、各種保証やサポートが受けられない

3.5　ICT模倣品への取組み例

セッション1では、国ごとの携帯電話端末模倣品への取組みが紹介されたが、現在の対策の中心となっているのは携帯電話の識別情報IMEIの管理である。IMEIの内、TAC（Type Allocation Code）と呼ばれる機種と製造元の情報はGSMAが管理している。製造事業者は、TACに続く残りの情報を端末に付与する。各国の技術適合認定機関（日本での携帯電話の技術基準適合承認はARIBによる）では、携帯端末の機器認定が済むとそのIMEIを認定済みとして個別データベースに登録することになる。また、携帯事業者は盗難や紛失にあった端末を、EIR（機器識別登録システム：Equipment Identity Register）といった別のデータベースで管理している。

図4は、携帯事業者、ユーザ、機器の適合性認定機関、警察、国内情報管理データベースの関係を表しており、国内データベースに情報が一元化されている事例である。不正なIMEI情報には、形式誤り（Unformatted：桁数が合っていない、値が全て0）、無効ID（Invalid：形式はあっているがGSMAで未承認）、未認可（Non-Approved：国内検査機関で未適合認定）、未登録（Non-Registered：DBにユーザ登録なし）、クローン（Clone：既存IMEIのコピー）がある。これらの不正情報は異なる状況に起因することが想定され（例：明らかな模倣品、情報登録の遅れ・漏れ等）、国の施策ごとに具体的な対応が異なっている（例：Unformattedの場合は即時没収、Non-Registeredの場合は20日間処分留保等）。

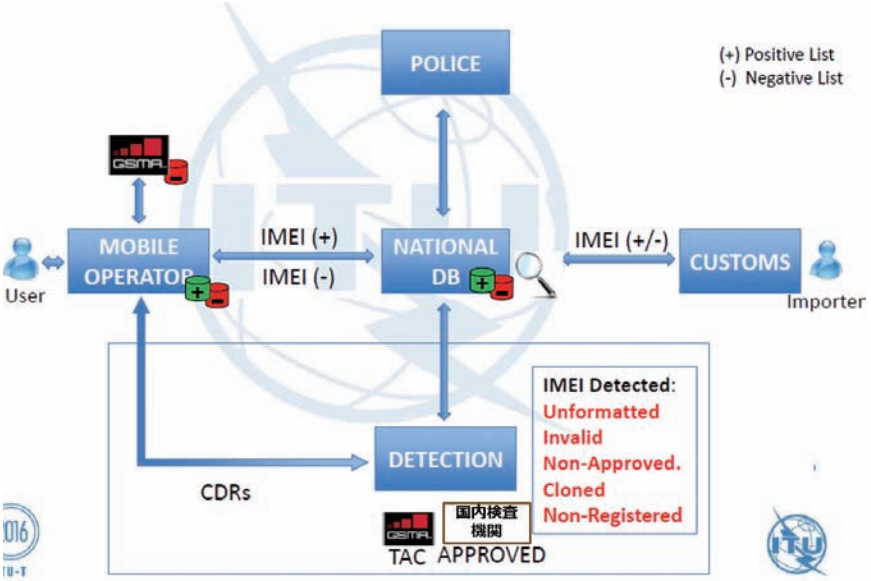
正規流通経路で供給される携帯端末のIMEIは国ごともしくは事業者ごとに管理されており、現状のままでは海外からの盗品や未承認端末への対策が難しくなってきていることが指摘されており、より広域な地域間もしくは国際間での情報共有の在り方が今後の審議テーマの一つである。

3.6　ディスカッション

各セッションを通じて、以下のような点が議論されており、これらは引き続きQ8/11において審議されていく予定である。

- 現在ITU-Tで議論されているICT模倣品の定義が曖昧であり、（無用な議論を避けて）模倣品対策を浸透させるために、国際間で締結済みのTRIPS協定（Agreement on Trade-Related Aspects of Intellectual Property Rights：知的所有権の貿易関連の側面に関する協定）の定義を使うかもしくはITU-Tで新たに作成したほうがよい。
- ICT機器においては非認証端末や盗品の問題も重要であり、これらを包括的に扱う対策の検討が必要である。
- 市場動向や地域ごとの端末の管理政策についてより調査すべきである。
- 国ごとの認証だけではなく、地域ごとの認証に向けた適合性試験機関が有用である。
- 地域内もしくは地域間で協調した標準化を定めるべき（本ワークショップで、GSMAとMMFのような組織間連携は始まっていることが紹介されている）。

（2016年8月31日 情報通信研究会より）



■図4.　IMEIの管理例