「これからのMVNO」の転ばぬ先の杖

~ 端末側から見える情報と具体事例のご紹介 ~

2016/01/21（木） JANOG37 Meeting in NAGOYA

株式会社メリテック
技術サポート部　品質保証エンジニア
木野　純武
skino@meritech.co.jp

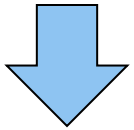
MVNOに関わるきっかけ

■株式会社メリテックとは

- 公式サイト
  - *http://www.meritech.co.jp/About_Company.html*
  - 端末から取得できる無線区間の情報をログ化するツールや、これらのログに含まれるデータを整理して解析するツールを提供している。
  - モバイル網の電波伝搬シミュレータも取り扱っている。
- 基本的にお客様はMNO様や通信機器ベンダ様
  - エリア品質の改善や商用NWの動作検証でご利用頂いている。
- では、なぜMVNOとの関わりが生まれたのか？

■関わりのきっかけ

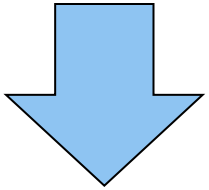
- 製品検証でよくMVNO回線を利用していた
  - MVNO回線は、安価にモバイル網が使える回線契約もあるので、製品検証におけるフィールドテストの良い友だった。
- IIJmioミーティングへの参加（2回目から）
  - 4回目の開催後、2014年9月17日から提供されはじめたiOS 8のアップデートで、KDDI回線MVNOがiPhoneで利用不能になった話題がホットに。
  - また、ドコモ回線のMVNOでも3Gでセッションが確立されてからLTEに上がる形で繋がってくる端末が多い旨の話を伺っていた。



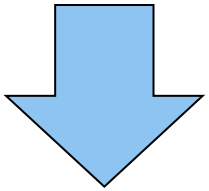
実はどちらの話題についても、どの辺りで問題が発生しているのかを、メリテックではある程度推測できていた。

■その後の流れ

- 端末接続性の問題に悩むMVNOは今後増える。
（Nexusしかり、iPhoneしかり）



- 「無線区間でやり取りされている制御信号」をMVNOが確認できる手段を持つことは、特有の接続問題を究明するための一手になり得る。



- 弊社ツールはその「情報」を提供できる。

「無線区間での制御」を見る意味

■モバイル網もひとつの小宇宙

- 端末がIP reachableとなるまでには、モバイル網の中でも多くのプロセスを経る必要がある。

- 端末から見える分だけでも…
  - 通信できる基地局を探す
  - 必要な無線リソースを基地局から割り当てられる
  - コアネットワークにサービス開始を要求
  - 認証・セキュリティのチェック
  - 使用APNの通知
  - 端末能力の通知
  - IPアドレス受領・DNS確認
  - 時刻補正情報の受領

■端末から得られる制御情報は宝の山

- 端末は、モバイル網にとって「終端」ノード。
  終端ノードは実ユーザとの接点。

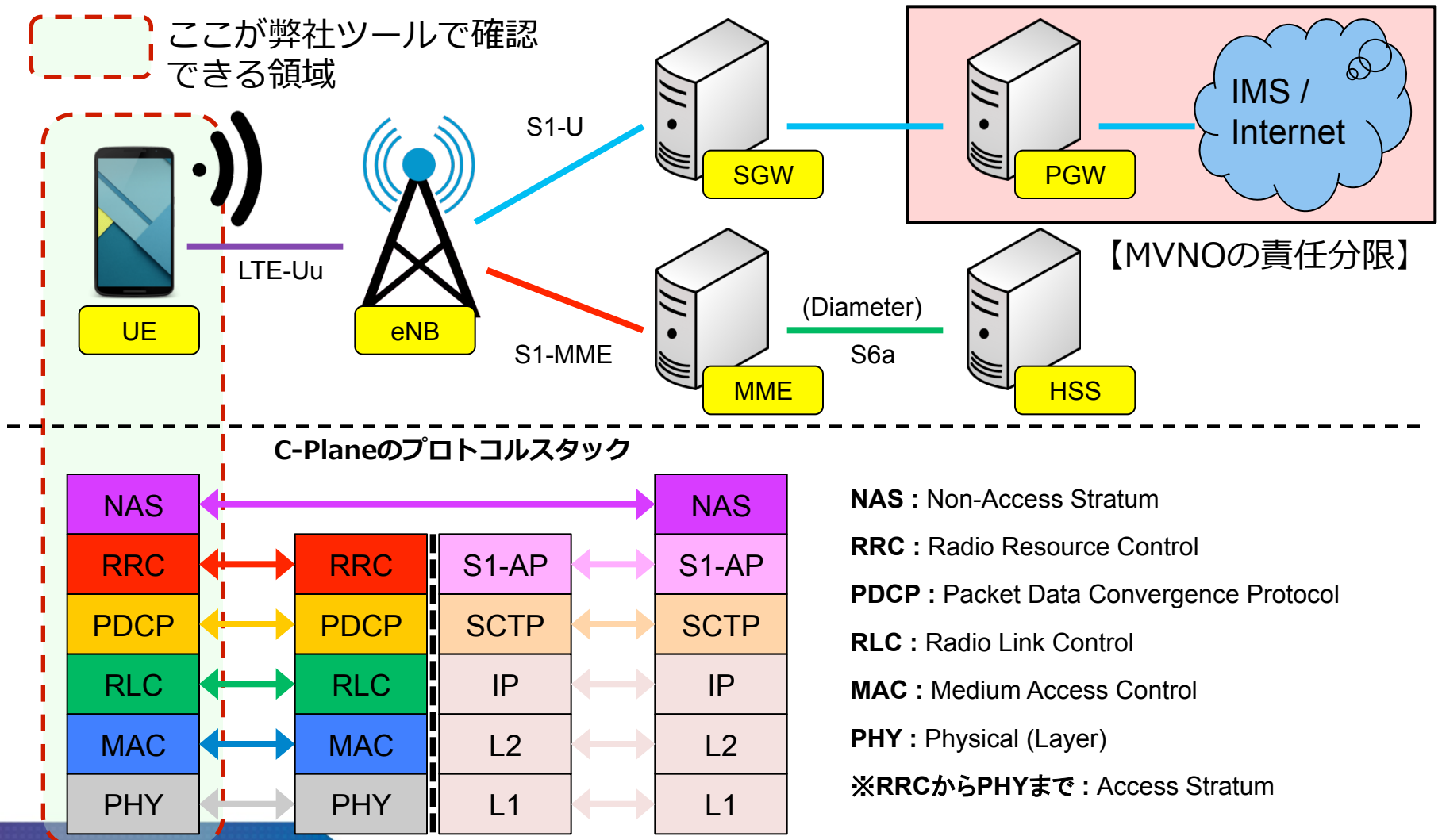
- MVNOからは「見えない」MNO網内の制御を
  垣間見できる唯一のポイントが、端末側。

- 端末からの情報を確認するためのツールは複数
  存在する。（弊社製品もその1つ）

- 市販端末（の一部）を使用して確認が可能。

弊社ツールが見ている領域

■ノード構成図とプロトコルスタック（一部省略）



NAS : Non-Access Stratum

RRC : Radio Resource Control

PDCP : Packet Data Convergence Protocol

RLC : Radio Link Control

MAC : Medium Access Control

PHY : Physical (Layer)

※RRCからPHYまで : Access Stratum

※EPC/E-UTRANのアーキテクチャの一部を抜粋

■端末側C-Planeプロトコルスタック概要

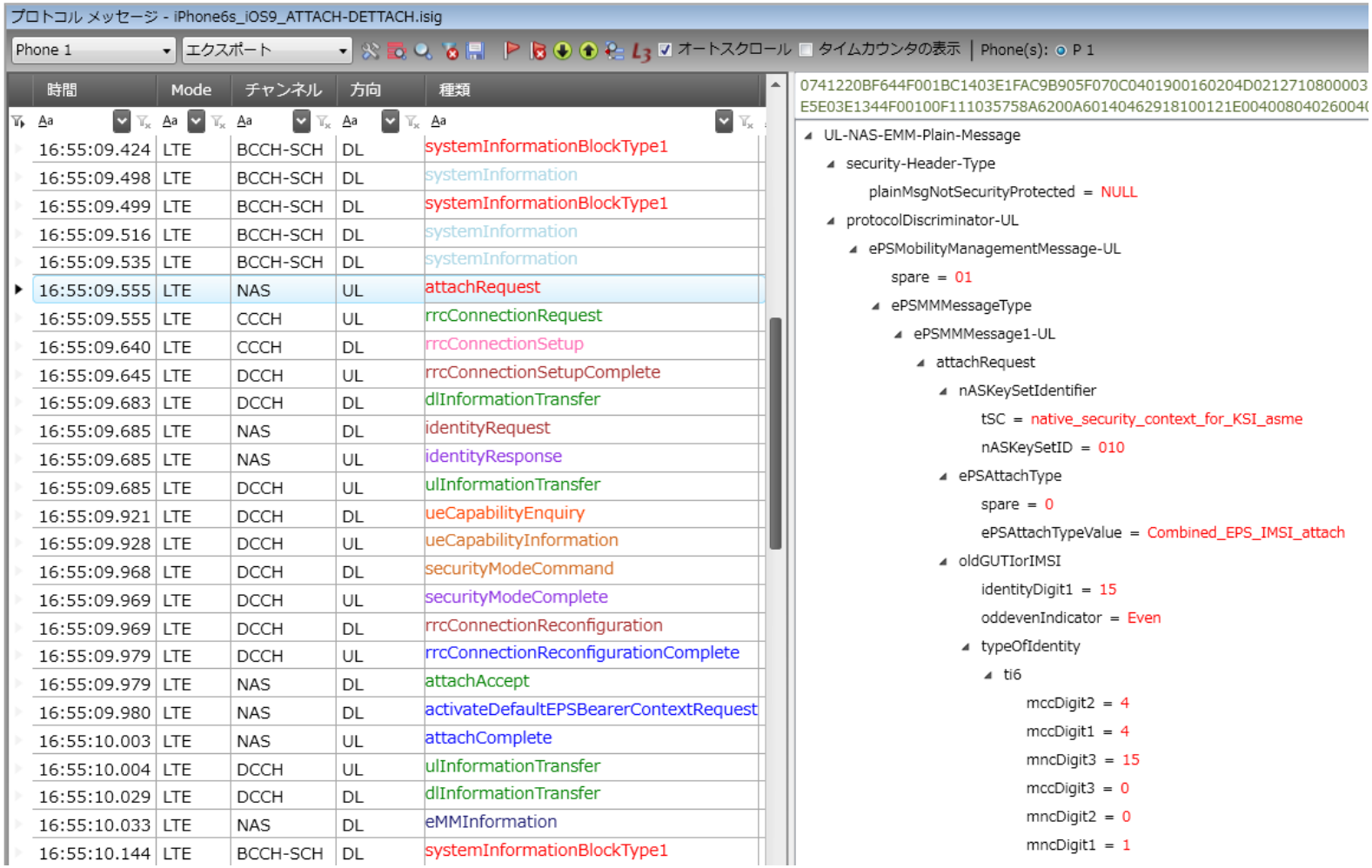
- **PHY** (Physical layer)
  - いわゆる物理層。フレーム同期や変復調など。
- **MAC** (Medium Access Control sublayer)
  - HARQによる再送制御やリソースのスケジューリング管理が行われるレイヤ。
- **RLC** (Radio Link Control sublayer)
  - PDU単位での再送制御(ARQ)や並べ替えなどが行われるレイヤ。
- **PDCP** (Packet Data Convergence Protocol sublayer)
  - PDUに対して秘匿化・完全性チェックを行うレイヤ。
- **RRC** (Radio Resource Control)
  - 無線区間の接続手順やハンドオーバなどの制御を行うレイヤ。
    下位レイヤのConfigurationもここの管轄。
- **NAS** (Non-Access Stratum control protocol)
  - サービス認証やベアラ管理、セキュリティ設定、在圏位置管理を行うレイヤ。
    いわゆるAttach/DetachやIPアドレス割り当てが行われるのはここ。

■シグナリング（制御信号）は

- RRCとNASを確認すべし
  - モバイル網で俗にLayer 3と呼ばれているグループ。
    無線区間の制御はRRCレイヤで。
    コアネットワークの制御信号はNASレイヤで。
    - MNOのコアネットワークと接続しているMVNOは、MMEやPGWに関係するNASレイヤの制御信号を見るのが特に有用。
  - NASレイヤの制御信号は以下のカテゴリがある(※)
    - EMM（EPS Mobility Management）
      - 端末の位置管理・認証・制御信号のセキュリティに関する制御を行うシグナリング群で、その性質上MME/HSSが関係する。
    - ESM（EPS Session Management）
      - 端末のベアラ管理やIP接続（IPアドレス割り当てやQoS管理など）の制御を行うシグナリング群で、その性質上PGW/PCRFが関係する。

※W-CDMAもモデルとしては同じ。MM、GMM、SM等がある。

■弊社ツールでの表示サンプル (Sigma-PA)



成果と今後の意義

■これまでの成果

- Internet Initiative Japan様
  - IIJmioミーティングでのIIJ大内様の発表
    - 第7回の発表　：　MVNOとSIMフリー端末の問題について
      - *http://techlog.iij.ad.jp/archives/1501*
    - 第8回の発表　：　続、MVNOとSIMフリー端末の問題について (iOS編)
      - *http://techlog.iij.ad.jp/archives/1578*

- ケイ・オプティコム様（mineoブランド）
  - 公式ファンサイト「マイネ王」での技術関連記事
    - 2015年8月31日の記事　：
      iPhone・iPadのAPN構成プロファイルの変更による現時点での動作解析の結果共有
      - *https://king.mineo.jp/magazines/special/150*

基本的にメリテックは裏方（解析ツールの提供者）として貢献。
解析・原因究明は個々のMVNO様が尽力された成果。

■「これからのMVNO」にとっての意義

- 自前で端末を調達・供給する時の動作検証手段として。
  また、SIMロック解除後の端末を使うユーザも今後増えてくる。
- 問題事象発生時の調査材料・要素の確保。（特にiOS端末…）
- HLR/HSS開放で端末接続性に関するMVNOの責任範囲が広がる。
  海外ローミングも独自で行うようであれば、その動作検証も必要。
- IMSも具備するようなFull MVNOを目指すなら、SIPセッションの確認も必要になってくるかもしれない。
- MVNOとして機能的に高度化するほど、モバイル網との関係性が深くなる。言い換えれば「MNOに近付く」ことでもあり、その分問題に対する調査能力もより深く・広く必要となってくる。

「繋がった後の通信品質」だけではなく
「繋がるまでのサポート」も重要になる

そのための【転ばぬ先の杖】

事例のご紹介

■概要（SORACOM Air）

SORACOM Air 開発者ドキュメント [SORACOM Air SIMの各状態] より引用。
https://dev.soracom.io/jp/docs/subscriber_status/

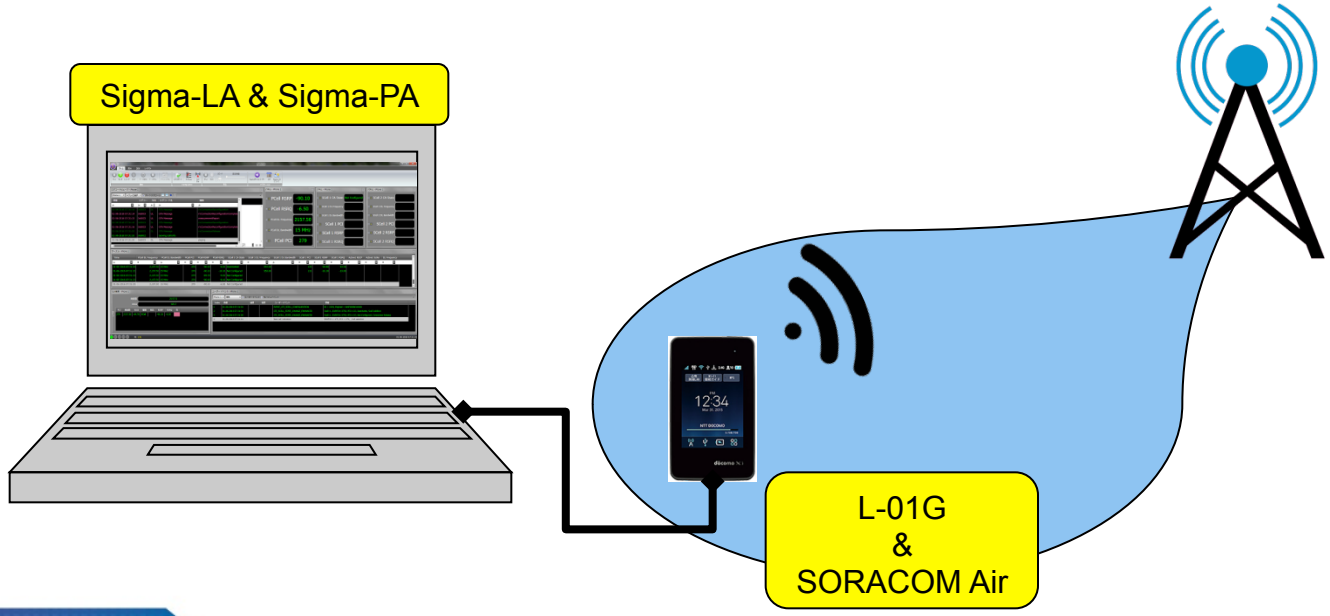
- 休止中 (inactive) 状態
  - ご購入後、アカウントへの登録が完了したSIMについて、データ通信のためのセッション確立要求を一時的に拒否するように設定した状態を意味します。端末がこの状態にあるSIMでデータ通信を行おうとしても、セッションを確立できないことから、データ通信を行うことは出来ません。何らかの理由で一時的に端末からの通信を禁止したい場合等にご活用頂けます。 なお、休止中のSIMにつきましても、SMS対応のSIMの場合、SMSの送受信は可能であり、基本料金およびSMS送信にあたっては課金が発生します。

  - 本状態においても、端末と無線基地局との間の3G/LTE通信リンク自体は確立可能な状態にあることから、端末側の実装によってはデータ通信セッション確立のための要求が繰り返し送られる可能性があります。その場合、端末側の電力消費が継続してしまうことも考えられることから、長時間にわたって休止中のSIMを端末に挿したままにする場合には、予め端末側の再接続処理の調整を行っておくことを推奨します。

→ 赤色の部分では実際にどのように動いているか、弊社ツールにて確認を行ってみた。

■確認環境

- 使用機材
  - 使用端末：L-01G（LG社製モバイルWi-Fiルータ）
  - 使用回線：SORACOM Air（データ通信only契約）
  - 取得ツール：Sigma-LA
  - 解析ツール：Sigma-PA



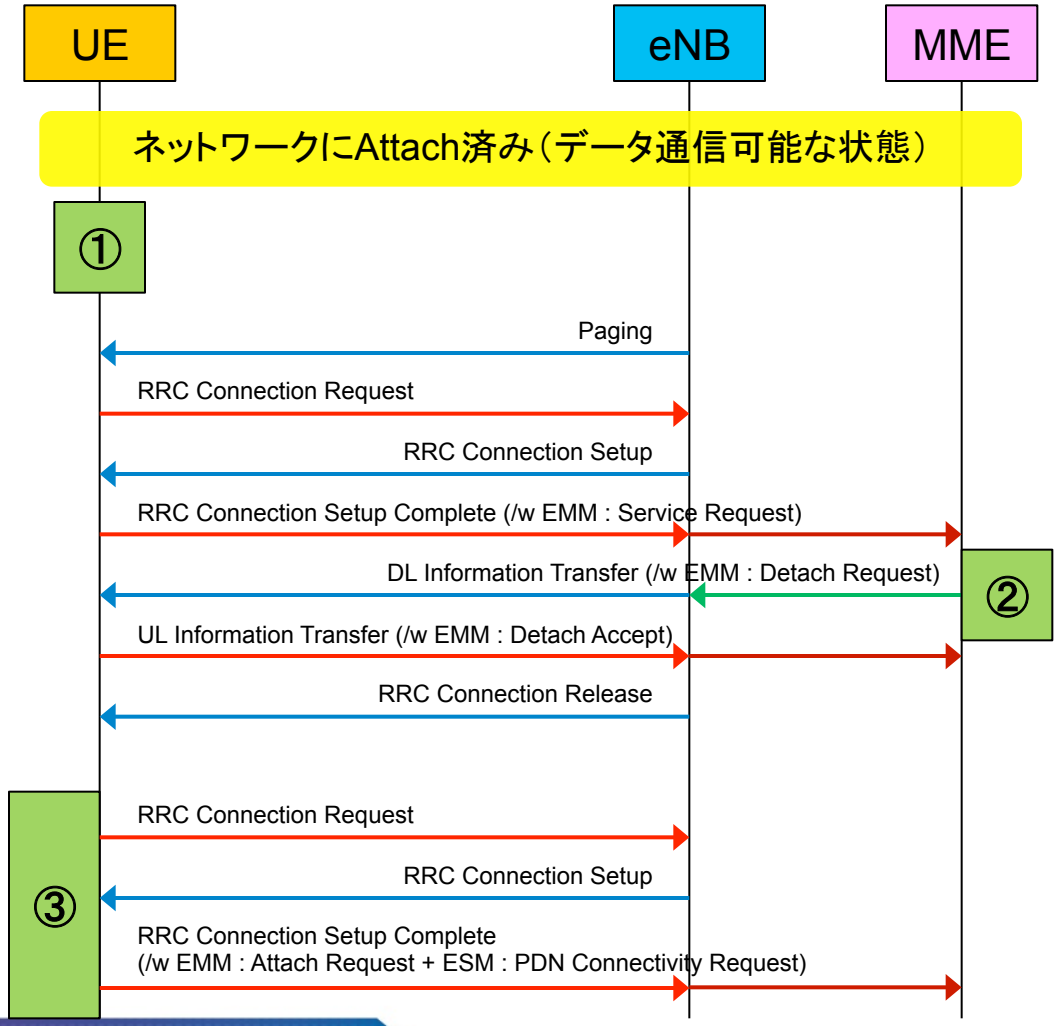
■確認できている内容

【注意】下記は、2016年1月3日時点で確認できている事例です。

- ユーザーコンソールから回線状態を「休止中」にしても端末から一定間隔でPDP接続要求が上がり続ける。
  - 状態を「休止中」に変更すると回線は切断されるが、ネットワークから送信される切断要求には、再登録を要求するパラメータが含まれているため、端末はネットワークに登録要求を再送信するが弾かれる。
  - その後、3Gに遷移して位置登録は完了するが、データ通信ベアラの確立要求は弾かれて、端末は再度要求する……という動作が繰り返される。

- この状態ではPingも通らずIPアドレスも割り当てられていないなので、通信していないように見える。
  - しかし実際には、モバイル網内で制御信号のやり取りが間欠的に発生している。（端末やチップの実装依存だが10～30分間隔）
  - 登録要求の発生によりモデムチップが稼働するため、バッテリー消費が増える。特にIoT機器への影響が大きいポイント。

■事例発生の流れ（１）



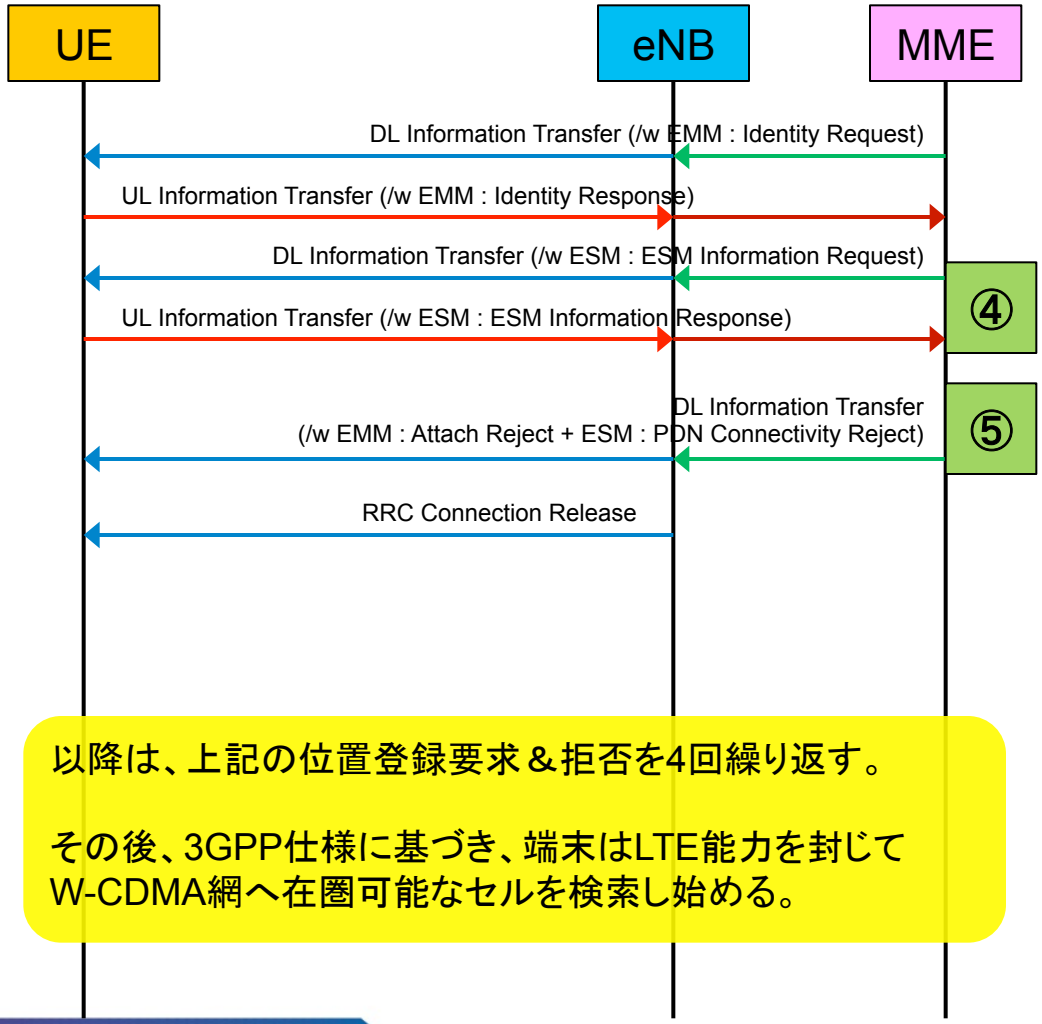
①SORACOMのユーザーコンソールで回線状態を「使用中」から「停止」に変更。

②ネットワークから切断要求（EMM ： Detach Request）を受信するが、Detach Typeが「Re-attach required」となっている。

③端末は「Re-attach required」の指示に従いDetach手順完了直後、位置登録要求（EMM ： Attach Request）を改めて送信する。

事例発生の流れ（２）に続く

■事例発生の流れ（２）



以降は、上記の位置登録要求＆拒否を4回繰り返す。

その後、3GPP仕様に基づき、端末はLTE能力を封じて
W-CDMA網へ在圏可能なセルを検索し始める。

④ネットワークから通信ベアラ情報を送るよう
要求され、端末はAPN（soracom.io）を送る。

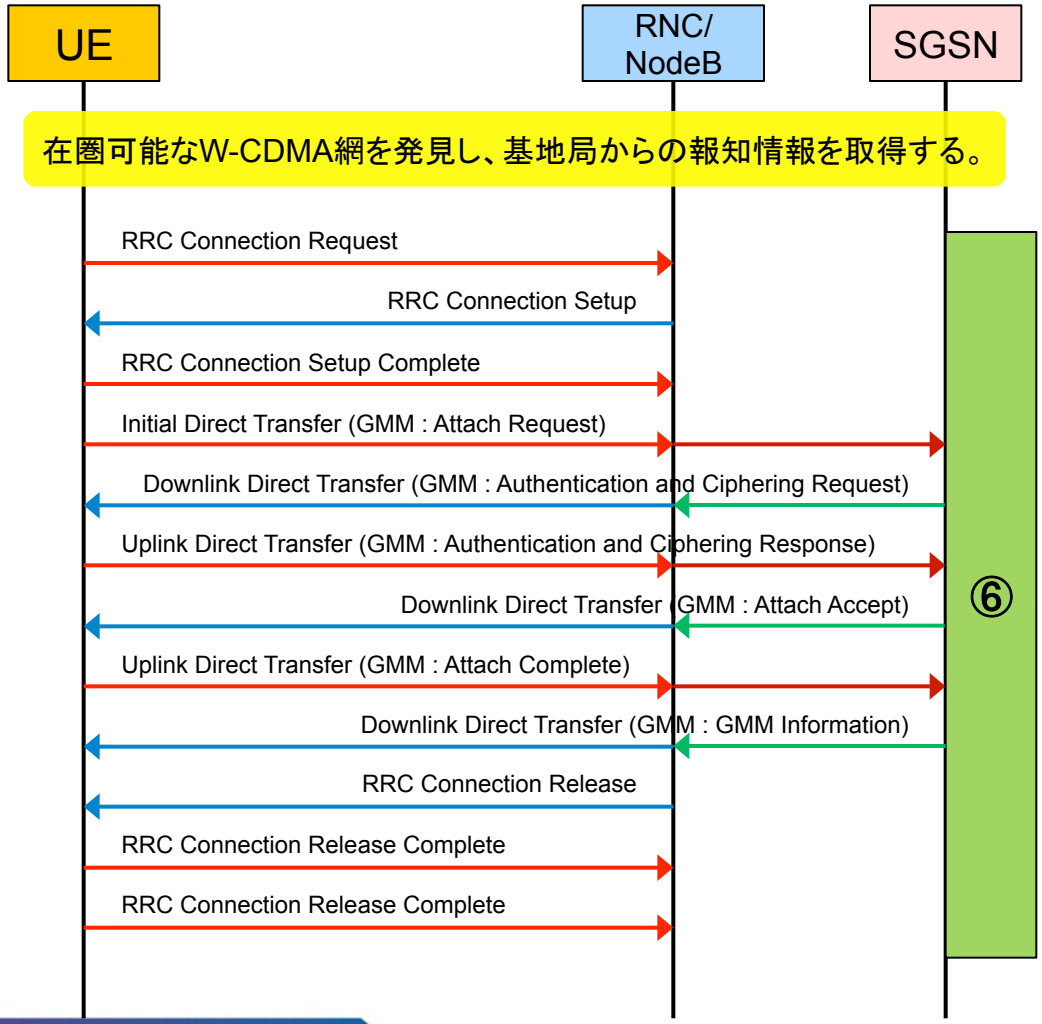
⑤端末はネットワークから位置登録の拒否
（EMM : Attach Reject）を受信する。
Cause値として下記の結果が含まれている。

■EMM : Attach Reject
→ EMM Cause 19 ESM failure
■ESM : PDN Connectivity Request
→ ESM Cause 29 User Authentication Failed

P-GW方面でユーザ認証に失敗したことが原因と
判別できる。SORACOMコンソール上で「停止」
したことが反映されている模様。

事例発生の流れ（３）に続く

■事例発生の流れ（３）



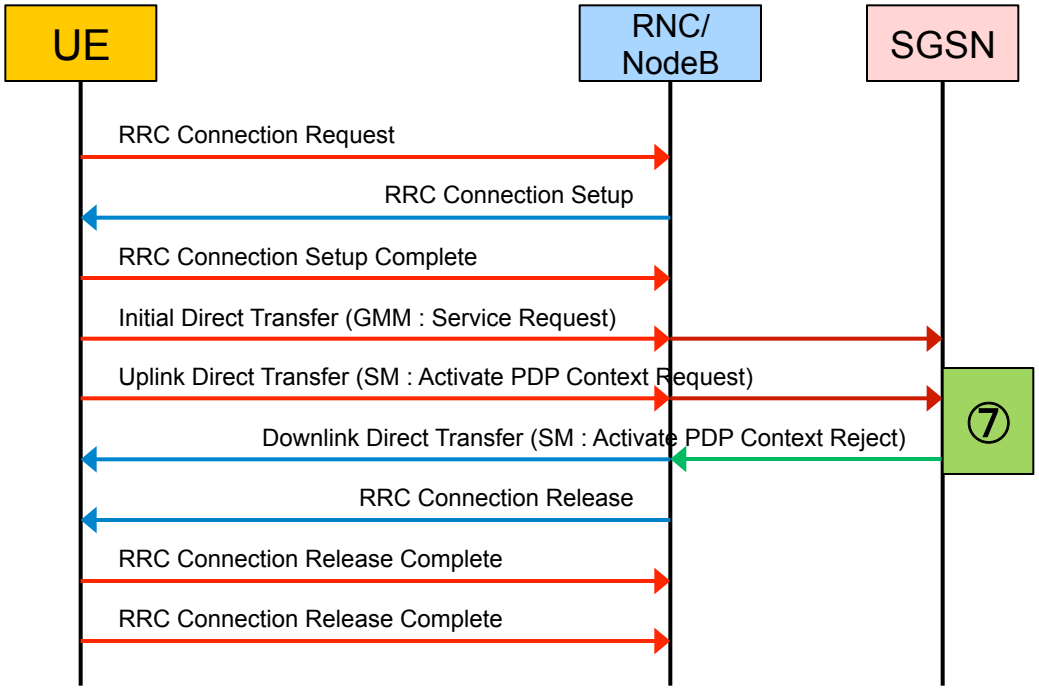
⑥端末は3G（W-CDMA）に移った後、3Gの位置登録手順を開始し、完了する。

ただし、この時点ではデータ通信ベアラが確立されておらず、あくまで「MNO網で位置管理ができるようになった」だけの段階。

LTEと異なり、データ通信ベアラの確立は位置登録手順に包含されておらず、この後に改めて別途実施される。

事例発生の流れ（４）に続く

■事例発生の流れ（４）



⑦APNを載せたデータ通信ベアラの確立要求を実施するが、SM ： Activate PDP Context Rejectを受信し、弾かれる。
Cause値として下記の結果が含まれている。

■SM ： Activate PDP Context Reject
→ SM Cause 29 User Authentication Failed

LTE時のCauseと同じであり、コンソールからの「停止」が引き続き機能しているのが伺える。

- この後、上記動作を10～30分間隔で繰り返す。
  - 試行間隔は端末依存のようだが、3GPPの仕様上はこの確立要求動作を繰り返すことが許容されている。
  - ベアラ確立手順でRejectされているため、GGSN/P-GWにReject履歴が残っていると思われる。なお、本動作が数百台規模で同時発生したらと想像すると…

参考資料

■参考資料

- 3GPP Technical Specification (Release 12)
  - TS 36.300 E-UTRA and E-UTRAN Overall description
  - TS 36.331 E-UTRA RRC protocol specification
  - TS 25.331 RRC protocol specification
  - TS 24.008 Core network protocols
  - TS 24.301 NAS protocol for EPS
  - TS 23.401 GPRS for E-UTRAN access
  - TS 29.061 Interworking between the PLMN supporting packet based services and PDN
- IIJのエンジニアによる公式blog「てくろぐ」
  - http://techlog.iij.ad.jp/
- mineo公式ファンサイト「マイネ王」
  - https://king.mineo.jp/
- SORACOM Air
  - https://soracom.jp/services/air/

Meritech
Your efficiency, Our passion

Meritech Co., Ltd.
Japan
+81-3-3552-1131
www.meritech.co.jp

Meritech Software Pvt. Ltd.
India
+91-172-462-6600
www.meritechsolutions.com

Meritech Systems PTE Ltd
Singapore
+65-6521-3780
www.meritech.sg