

電気通信事故検証 報告書
（令和4年7月2日発生した
KDDI 株式会社及び沖縄セルラー電話株式会社
による重大事故）

令和 4 年 10 月
電気通信事故検証会議

目次

1. 重大事故の概要等

1.1 重大事故の概要	-----2
1.2 重大事故の検証	-----3

2. 検証結果

2.1 発生状況	-----4
2.2 発生原因	-----16

3. 再発防止策

3.1 報告のあった主な再発防止策	-----20
3.2 追加的再発防止策	-----22

4. 今後について -----26

《参 考》

本報告書本文中に用いる用語の取扱いについて、本報告書の本文中用いる検証の結果を表す用語は、次のとおりとする。

- ① 断定できる場合 ・ ・ ・ 「認められる」
- ② 断定できないが、ほぼ間違いのない場合 ・ ・ ・ 「推定される」
- ③ 可能性が高い場合 ・ ・ ・ 「考えられる」
- ④ 可能性がある場合 ・ ・ ・ 「可能性が考えられる」

1. 重大事故の概要等

1.1 重大事故の概要

令和4年7月2日、KDDI 株式会社及び沖縄セルラー電話株式会社の多摩ネットワークセンターに設置されている全国中継網コアルータ¹のメンテナンス作業において、ルーティングの誤設定により、当該コアルータを経由する一部のトラフィックが通信断となった。これにより、利用者の端末が送信する位置登録要求信号が繰り返し再送され、全国の VoLTE 交換機²および加入者データベースが輻輳状態となった。

この輻輳によって、全国的に音声通信、SMS が利用しづらい状況となり、一部の端末では音声通信に必要な位置登録がしづらいことでデータ通信にも影響が発生した。

VoLTE 交換機および加入者データベースの輻輳を解消させるために、無線設備および VoLTE 交換機での流量制御等を実施すると共に、過剰な信号の発生原因となっていた VoLTE 交換機（呼制御機能）6 台を切り離すことで、輻輳が解消した。なお、同社の回線を利用する MVNO においても同様のサービス影響が発生した。

当該事故の影響時間は、7月2日（土）1時35分から7月4日（月）15時までの合計 61 時間 25 分、影響エリアは全国、影響数は音声（VoLTE）サービス約 2,316 万人、データ通信（4G/5G）サービス 775 万人以上、合計のべ 3,091 万人以上（いずれも推計値）であり、当該利用者には、物流関連、自動車関連、行政サービス、銀行関連、交通関連等、多岐にわたる法人の利用者も含まれており、長時間にわたり全国の利用者に大きな影響があった。

¹ モバイルネットワークと全国中継網を接続するルータ

² モバイルネットワーク上で音声サービスを提供するための電話交換設備

影響時間	7月2日(土)1:35 ～ 7月4日(月)15:00 (61時間25分)
影響エリア	全国

＜影響数＞

音声(VoLTE)	約2,316 万人
データ(4G/5G)	775万人以上
合計	のべ 3,091万人以上

※影響規模は通常時(通信障害の1週間前の同時間帯)と通信障害時の差分(呼数や位置登録数)をもとに推計し算出

図 1-1 事故の影響の概要

1.2 重大事故の検証

当該 KDDI 株式会社及び沖縄セルラー電話株式会社による重大事故について、電気通信事故検証会議は、令和4年8月より、事故の原因を検証し、事故の防止に寄与することを目的として検証を行った。

本報告書は、電気通信事故検証会議（令和4年度第1回～第3回）において、当該重大事故の検証を行った結果を取りまとめたものである。

2. 検証結果

2.1 発生状況

(1) 全国中継網コアルータの一部トラヒックで通信断発生

KDDI 株式会社の全国中継網コアルータにおける多摩ネットワークセンターに設置のコアルータのソフトウェアバージョンアップにおいては、通常、サービス影響を回避するために、バージョンアップ対象のコアルータに流れるトラヒックを他のコアルータへ片寄せし、商用ネットワークから切り離して、予備のコアルータにケーブルを切り替えた上で、バージョンアップを実施することとしている（図 2-1①から⑤参照）。コアルータのソフトウェアバージョンアップ後に、予備のコアルータから元のコアルータに戻す場合も、一度予備のコアルータに流れるトラヒックを他のコアルータへ片寄せし、予備のコアルータを商用ネットワークから切り離れた上で、元のコアルータへ切り替えることとしている（図 2-1⑥から⑧参照）。

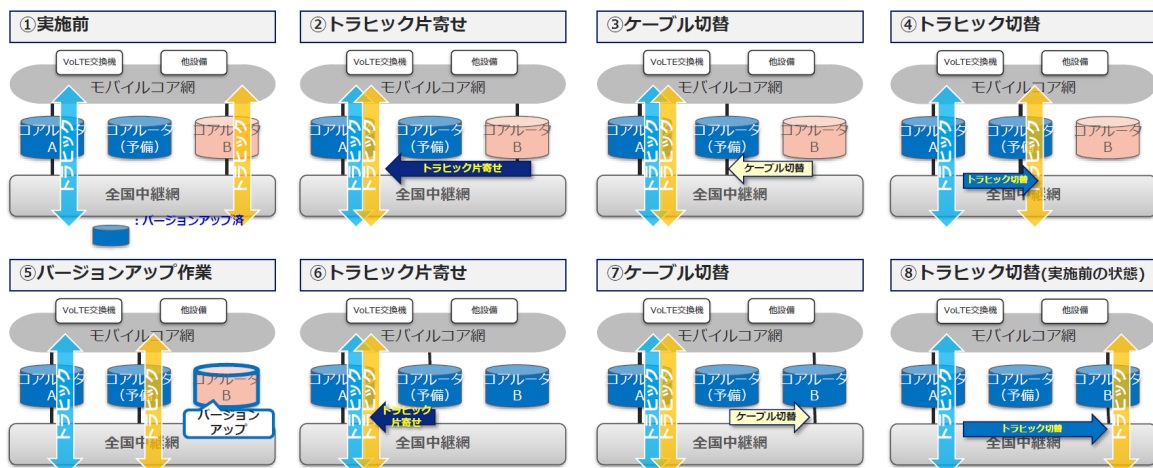


図 2-1 全国中継網コアルータの通常作業

このため、KDDI 株式会社の 100%子会社である KDDI エンジニアリング株式会社において、全国中継網コアルータのメンテナンス作業として、上記図 2-1⑥のとおり、多摩ネットワークセンターに設置の 2 台の運用中ルータに対して、コアルータ B のソフトウェアバージョンアップ後、予備のコアルータからコアルータ B に切り替えるため、予備のコアルータのトラヒックをコアルータ A に片寄せする作業を実施した。しかしながら、今回、当該作業において、作業員が誤った作業手順書（本来、使用すべきではない古い手順書）を用いて片寄せ作業を行い、当該作業手順書には、VoLTE 交換機のルーティング変更設定の手順が指示されておらず、VoLTE 交換機には予備のコアルータ向けのルーティング設定（静的ルート）が残ったため、当該予備のコアルータに流れるトラフィックは途絶し、同確率でコアルータ A に流れるトラフィックは正常に機能したと推定される（図 2-2 参

照)。このため、当該 VoLTE 交換機を経由する信号について、1/2 の確率で失敗する状態が生じたと推定される。

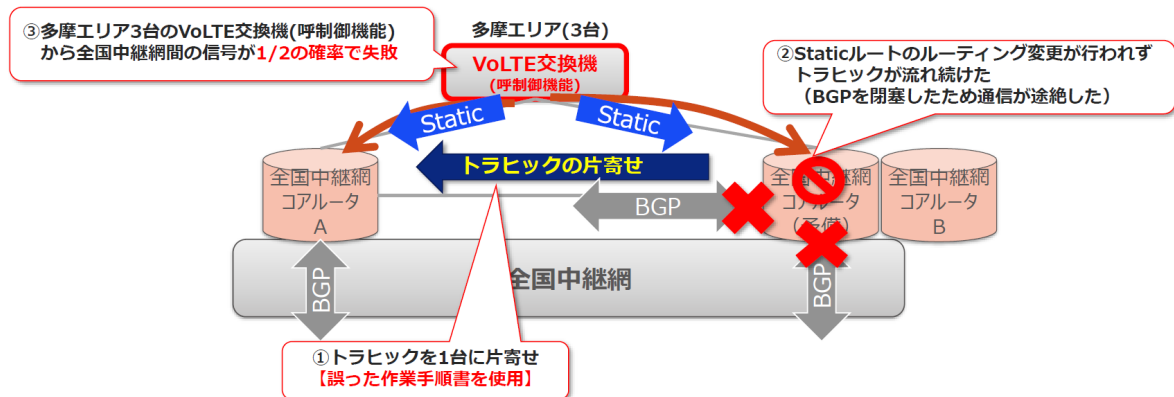


図 2-2 全国中継網コアルータでの通信断

(2) VoLTE 交換機の輻輳

音声通話 (VoLTE) を利用するには、まず利用者の端末は、電源オン、エリアが圏外から圏内になるタイミング、または定期的な更新のタイミングなどで、利用可能な契約状態なのか、加入者 DB に問い合わせする。利用可能な場合は、どのエリアに在圏しているのか、全国中継網コアルータを経由して VoLTE 交換機に位置登録を行う。これにより、音声発信や着信が可能となる (図 2-3 参照)。

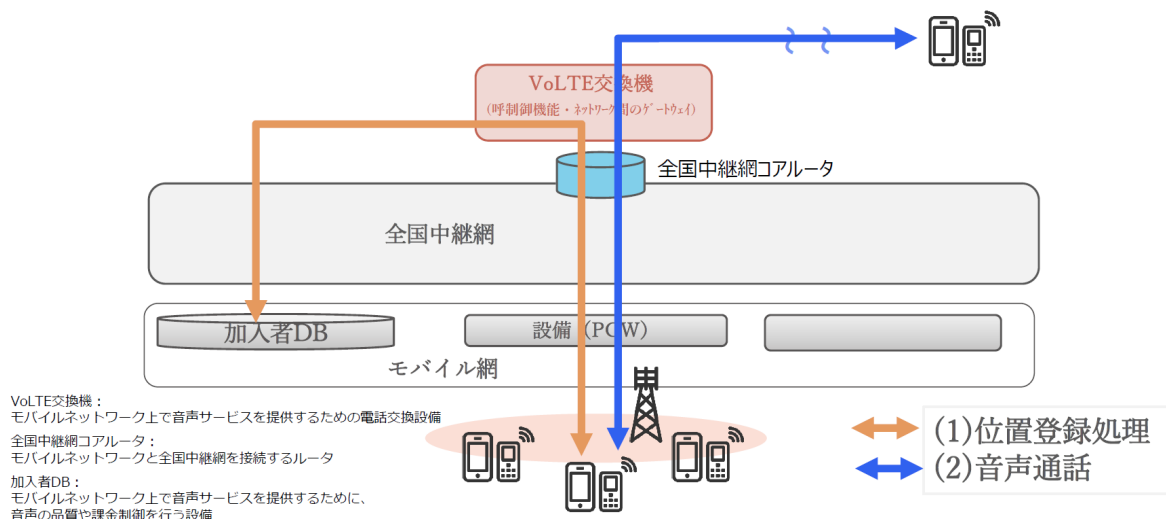


図 2-3 正常時の通信の流れ

このため、端末から VoLTE 交換機に対して位置登録要求の送信が定期的になされているが、上記 (1) の事象により、多摩ネットワークセンター設置の VoLTE 交換機 (以下、「多摩エリアの VoLTE 交換機」という。) では、上り方向 (利用者端末から VoLTE 交換機) の信号は通るが、下り方向 (VoLTE 交換機から端末) の信

号が1/2の確率で届かない状況が発生したため、端末は位置登録処理が完了せず失敗したと判断し、位置登録要求信号の再送を繰り返したと推定される（図2-4参照）。

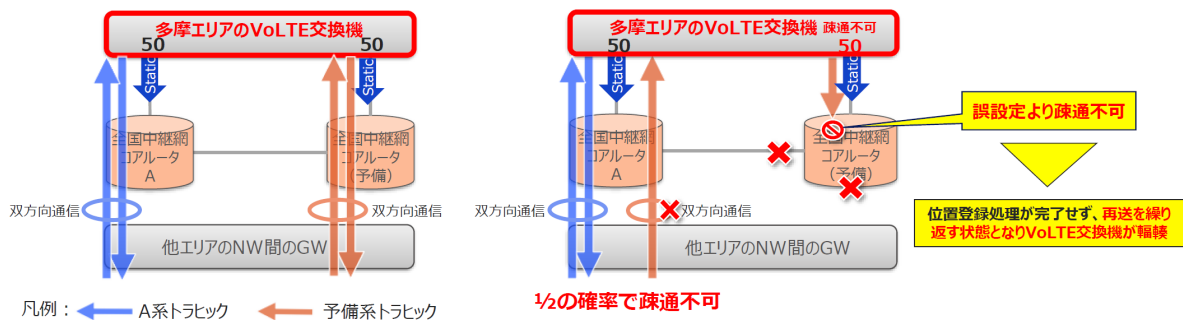


図 2-4 全国中継網コアルータでの通信断の詳細

また、VoLTE 交換機はネットワーク間のゲートウェイ³と呼制御機能⁴で構成されるが、呼制御機能の負荷分散のため、VoLTE 交換機内にあるネットワーク間のゲートウェイを通じて全国の呼制御機能に均等分散される設計となっており、全国の利用者からの位置登録要求信号も、最寄りのネットワーク間のゲートウェイを経由した後、均等の確率で、多摩エリアの VoLTE 交換機の呼制御機能へ向かう設計となっていた。さらに、全国の VoLTE 交換機内にある各ネットワーク間のゲートウェイから多摩エリアの VoLTE 交換機の呼制御機能への位置登録要求信号は、異常状態となっていた多摩ネットワークセンター設置の全国中継網コアルータを経由する（また多摩エリアの呼制御機能から当該ネットワーク間のゲートウェイへ応答を返す）設計となっていた。このため、全国の VoLTE 交換機内にある各ネットワーク間のゲートウェイは、均等の確率で多摩エリアの VoLTE 交換機の呼制御機能へ位置登録要求信号を送信し、1/2 の確率で応答信号が返らない状況であったが、1/2 の確率で応答していたため異常と認識せず、再送機能により多摩エリアの VoLTE 交換機の呼制御機能へ信号の送出を繰り返したと推定される。

さらに、VoLTE 交換機内にある呼制御機能には、過去に端末が位置登録した情報が残っており、当該位置登録情報の更新のため、全国の VoLTE 交換機の呼制御機能から多摩エリアの VoLTE 交換機の呼制御機能へ向かう位置登録要求信号もあり、当該位置登録要求信号も、多摩ネットワークセンター設置の全国中継網コアルータを経由したため、ここでも 1/2 の確率で応答信号が返らない状況となり、呼制御機能の再送機能により信号の送出を繰り返したと推定される（図2-5参照）。

結果、多摩エリアの VoLTE 交換機の呼制御機能に位置登録要求が急増し、輻輳

³ 端末(モバイルコアネットワーク)との接続を提供し、VoLTE 交換機の最初の接続箇所として負荷分散の機能等を有する

⁴ ユーザの登録やセッション設定の制御を実施する機能を有する

状態となり、通常時の約7倍の負荷が発生したと考えられる。

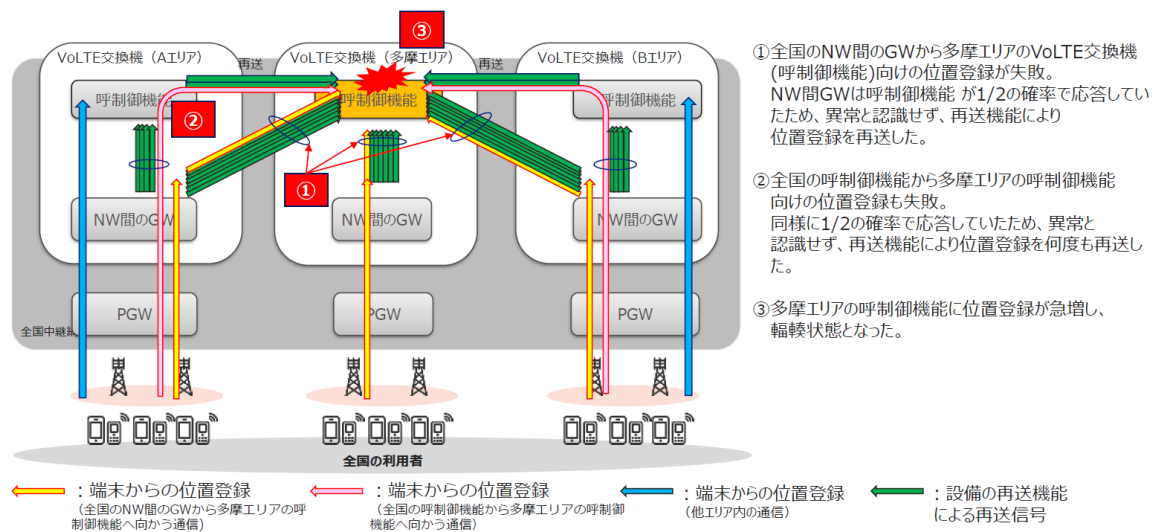


図 2-5 多摩エリアの VoLTE 交換機の輻輳

また、他エリアの VoLTE 交換機でも、多摩エリアの VoLTE 交換機の呼制御機能へ同様の信号の再送を繰り返したことに加え、全国のネットワーク間のゲートウェイは、多摩エリアの VoLTE 交換機の呼制御機能向けの再送タイマー満了により、位置登録信号の送信先を他エリアの呼制御機能に変更したことにより、他エリアの呼制御機能も同様に輻輳に至り、全国に輻輳状態が波及、他エリアの VoLTE 交換機（呼制御機能）は各々通常時の約 6.5 倍の負荷が発生したと考えられる（図 2-6 参照）。

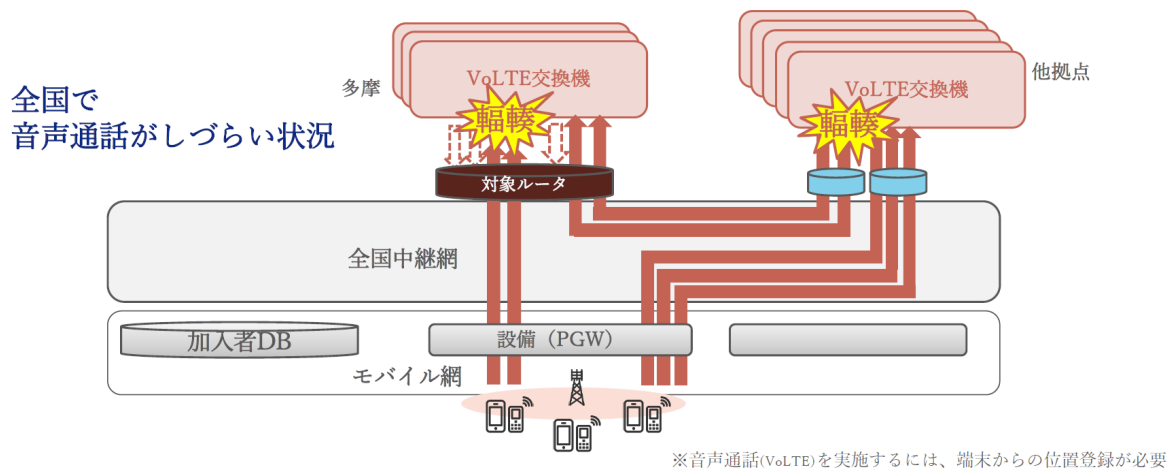


図 2-6 全国の VoLTE 交換機の輻輳

（３）加入者データベースの輻輳

通常、端末から VoLTE 交換機向けの位置登録要求（再送を含む）の度に、加入者データベース向けにも位置登録要求が送信される。上記（２）の事象により、

全国の VoLTE 交換機で輻輳が発生し、これが起因となり、端末から加入者データベース⁵向けの位置登録要求の再送信号が増加することにより、加入者データベース⁵も輻輳状態となったと推定される（図 2-7 参照）。

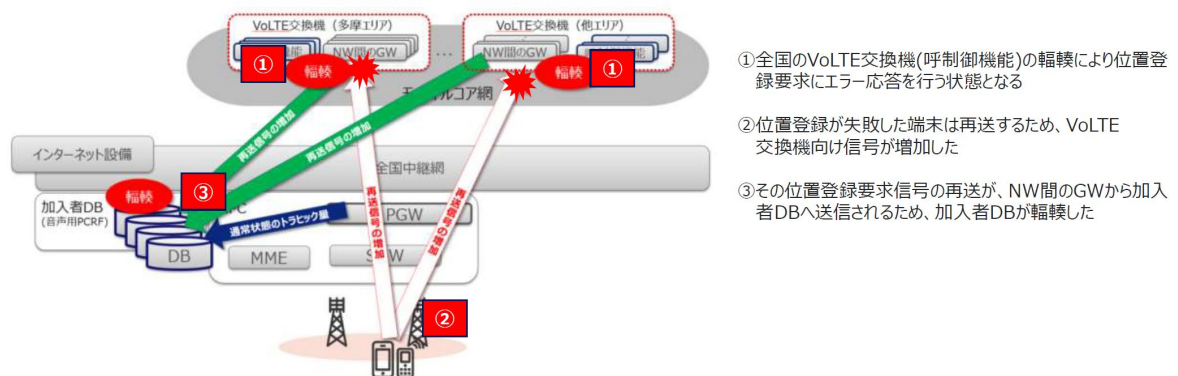


図 2-7 加入者データベースの輻輳詳細①

また、加入者データベースの輻輳により、パケットネットワークのゲートウェイ装置（PGW）からのセッション要求に対して、加入者データベースがエラー応答を行う状態となり、エラー応答を受けた端末から加入者データベースへ信号が再送されることにより、加入者データベースの輻輳がさらに悪化及び継続したと推定される（図 2-8 参照）。

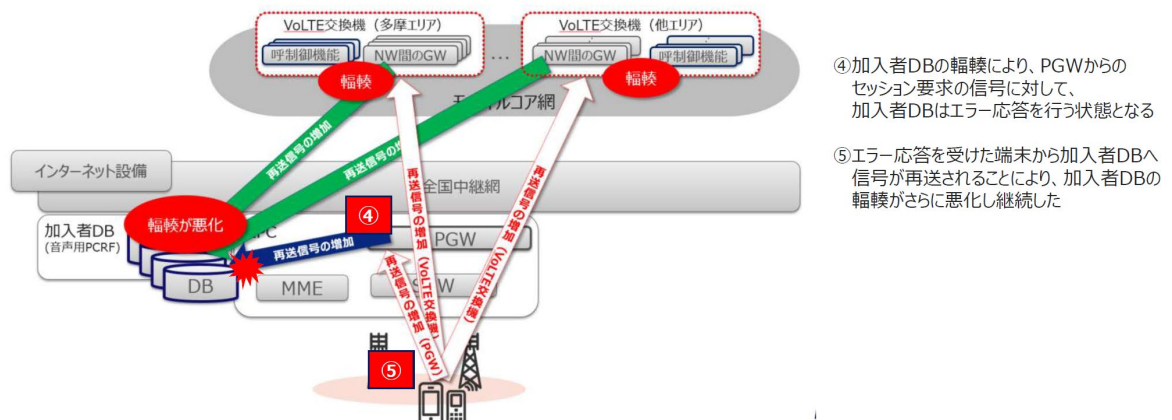


図 2-8 加入者データベースの輻輳詳細②

これにより、全国的に位置登録および音声通信が接続しづらい状態となり、また、一部の端末では音声通信に必要な位置登録がしづらいことでデータ通信にも影響が発生したと考えられる。

⁵ 加入者の位置情報や回線情報等を管理するデータベース。モバイルネットワーク上で音声サービスを提供するために、音声通話のサービス品質（Quality of Service (QoS)）ポリシーの決定や課金制御を行う設備等が含まれる。

具体的には、今回、データ通信向けの加入者データベースには輻輳が見られず、データ通信に関しては、ネットワークの負荷軽減のための流量制御を除いて、原則として影響はないものと思われたが、端末仕様によりアンテナピクトの表示及びデータ通信の動作が異なり、一部の端末においては、音声用のセッション確立失敗時に、一定時間毎に圏内、圏外を繰り返す（圏外時はデータ通信の利用不可）動作がみられ、一部の利用者にはデータ通信にも影響が発生したと考えられる（図 2-9 参照）。

端末仕様	音声	データ	アンテナピクト	端末の状態
A	×	○	グレーアウト	データ通信のみ可
B	×	△	圏内⇄圏外	一定時間毎に圏内、圏外を繰り返す（圏内時はデータ通信可能）

補足1：SMSは音声用のセッション(PDN)のステータスに依存
補足2：+メッセージ、iMessageはデータ用のセッション(PDN)に依存



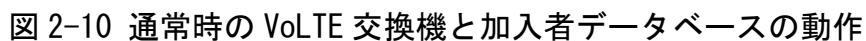
図 2-9 端末仕様による動作の違い

（４）一部 VoLTE 交換機の異常状態による加入者データベース輻輳の長期化

通常、図 2-10 のとおり、端末から位置登録要求があると（①-1）、VoLTE 交換機のネットワーク間のゲートウェイは加入者データベースの通信ポリシー及び課金ルール機能（PCRF）⁶に位置登録開始通知を行い（①-2）、また VoLTE 交換機の呼制御機能に対して認証要求を行う（①-3）。呼制御機能は加入者データベースの加入者管理サーバー（HSS）⁷と複数の認証セッションを常時確立し認証処理を行う（②）。認証に成功すると呼制御機能はネットワーク間のゲートウェイに通知（③-1）。ネットワーク間のゲートウェイは加入者データベース（通信ポリシー及び課金ルール機能（PCRF））に認証成功を（③-2）、また端末に位置登録完了を通知する（③-3）。また、呼制御機能は、加入者データベースの加入者管理サーバー（HSS）との認証セッションの状態を常に内部データベースに同期しており、内部データベースは6時間毎に定期的にバックアップする仕様であった（④）。

⁶ Policy and Charging Rules Function。モバイルネットワーク上で音声サービスを提供するために、音声通話のサービス品質（Quality of Service (QoS)）ポリシーの決定や課金制御を行う設備

⁷ Home Subscriber Server。加入者情報を管理するサーバーであり、ユーザーの位置管理、認証、サービスの起動状態の管理等を行う。



しかしながら、今回、図 2-11 のとおり、VoLTE 交換機の輻輳により、呼制御機能の中央処理装置（CPU）が高負荷となり（①-1）、VoLTE 交換機の呼制御機能と加入者データベース（加入者管理サーバー（HSS））間の認証セッションにおいて確立と停止（Up/Down）が繰り返し発生する異常が発生し（①-2）、VoLTE 交換機において、認証セッションの状態の内部データベースへ同期処理が正しく行えず（②）、データの不整合が発生したと推定される。仕様にに基づき、VoLTE 交換機は内部データベースの定時バックアップを行ったが（③）、6 台の VoLTE 交換機⁸においてはデータ不整合が発生しているタイミングでバックアップが行われたため、データ不整合があるバックアップファイルが生成されたと推定される。



10

こうした中で、VoLTE 交換機の輻輳を解消させるため、VoLTE 交換機（呼制御機能）のリセットを実施したが、最新のバックアップファイル（6 台の VoLTE 交換機においてはデータ不整合があるバックアップファイル）に基づきリセットを実施したため、データ不整合があるバックアップファイルで起動した 6 台の VoLTE 交換機（呼制御機能）は異常状態が継続し、図 2-12 のとおり、VoLTE 交換機（呼制御機能）と加入者データベース（加入者管理サーバー（HSS））間の認証セッションに不良が継続して発生（①）、当該 6 台の VoLTE 交換機の呼処理機能に收容されている全ユーザにおいて、位置登録時の認証失敗となり（②-1～3）、端末からの位置登録要求が繰り返し再送された（②-4）と推定される。その結果、加入者データベース（PCRF）に対して、ネットワーク間のゲートウェイから不要な過剰信号が繰り返し送信され（③-1）、加入者データベース（PCRF）の中央処理装置（CPU）使用率が高負荷となった（③-2）と推定される。加入者データベースの輻輳が解消せず、影響が長期化したと考えられる。

図 2-12 リセット後の VoLTE 交換機と加入者データベースの動作

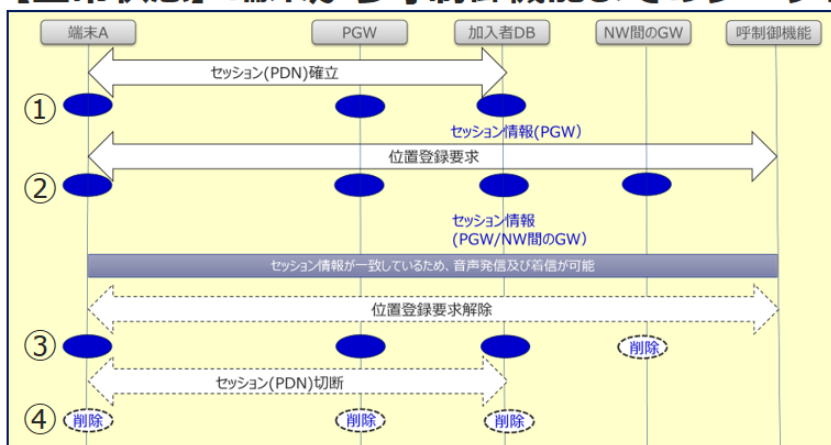
また、セッション情報のデータ不一致の発生も、影響が長期化した要因と考えられる。音声通話 (VoLTE) を実施するには、VoLTE 交換機、加入者データベース、パケットネットワークのゲートウェイ装置 (PGW)⁹ の3つの設備間でユーザのセッション情報 (加入者識別子、IP アドレス等) が一致している必要があり、図 2-13 の上図とおり、正常時においては、①端末から加入者データベース間のセッション (PDN) を確立する、②位置登録要求の信号処理が完了して、音声発着信が可能となる (完了すると、端末ごとにセッション情報 (加入者識別子、IP アドレス等) が生成される)、③位置登録要求解除により VoLTE 交換機 (ネットワーク間のゲートウェイ) においてセッション情報が削除される、④セッション (PDN) の

切断により、端末、加入者データベース、パケットネットワークのゲートウェイ装置（PGW）においてセッション情報が削除される、といった工程でセッション情報のやり取りが行われる。

しかしながら、今回、セッション情報のやり取りが正常に行われず、セッション情報のデータ不一致が発生した。具体的には、図 2-13 の下図のとおり、⑤正常状態①、②と同様にセッション情報を生成したものの、⑥加入者データベースの輻輳により、セッション(PDN)切断・位置登録解除時に情報削除要求が処理できず、端末 A のセッション情報が加入者データベースに残存したため、⑦別の端末 B のセッション情報が新たに生成された際、加入者データベースにおいて端末 A で利用していたものと同じ IP アドレスが割り当てられ、⑧端末 A の残存セッション情報の削除契機（端末のセッション生成から 25 時間経過、かつ、パケットネットワークのゲートウェイ装置（PGW）セッション情報なしの場合）に、端末 B のセッション情報も端末 A の情報とともに削除される事態が発生したと推定される。結果、VoLTE 交換機、加入者データベース、パケットネットワークのゲートウェイ装置（PGW）でユーザのセッション情報が一致せず、その後の音声通話が不可となる事態が発生した。

当該セッション情報のデータ不一致の修正にも多くの時間を要したと考えられる。

・ 【正常状態】 端末から呼制御機能までのシーケンス



・ 【不一致状態】 端末から呼制御機能までのシーケンス

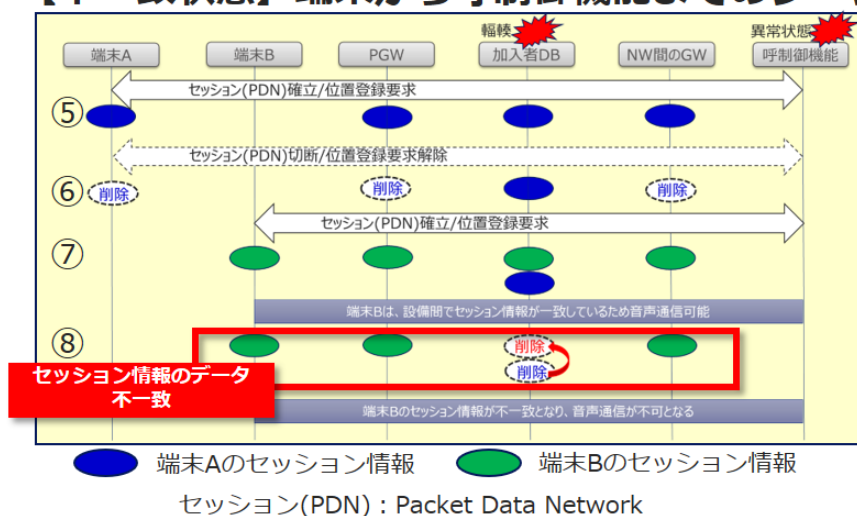


図 2-13 セッション情報のデータ不一致

(6) 措置模様 (事故対応状況)

事故の対応に係る措置としては、図 2-14 のとおり、大きく 5 つの措置が行われた。

まず、①信号接続要求の流量制御、VoLTE 交換機の流量制御及び呼制御機能リセットなど VoLTE 交換機の負荷低減¹⁰、②加入者データベースの負荷低減に向けた一部パケットネットワークのゲートウェイ装置 (PGW) の切り離し、③セッション情報のデータ不一致を修正するための全パケットネットワークのゲートウェイ装置 (PGW) のセッションリセット、④加入者データベースの負荷均等化に向けたパケットネットワークのゲートウェイ装置 (PGW) から加入者データベー

¹⁰ VoLTE 交換機を切り離すために、VoLTE 交換機の閉塞も実施したが、異常状態が継続していた 6 台の VoLTE 交換機については、異常状態であったために閉塞処理が正常に完了しなかったと推定される。

スの収容変更、⑤最終的には、異常状態が継続していた6台の VoLTE 交換機を切り離したことで、端末からの再送が収束し、輻輳が解消したと認められる。

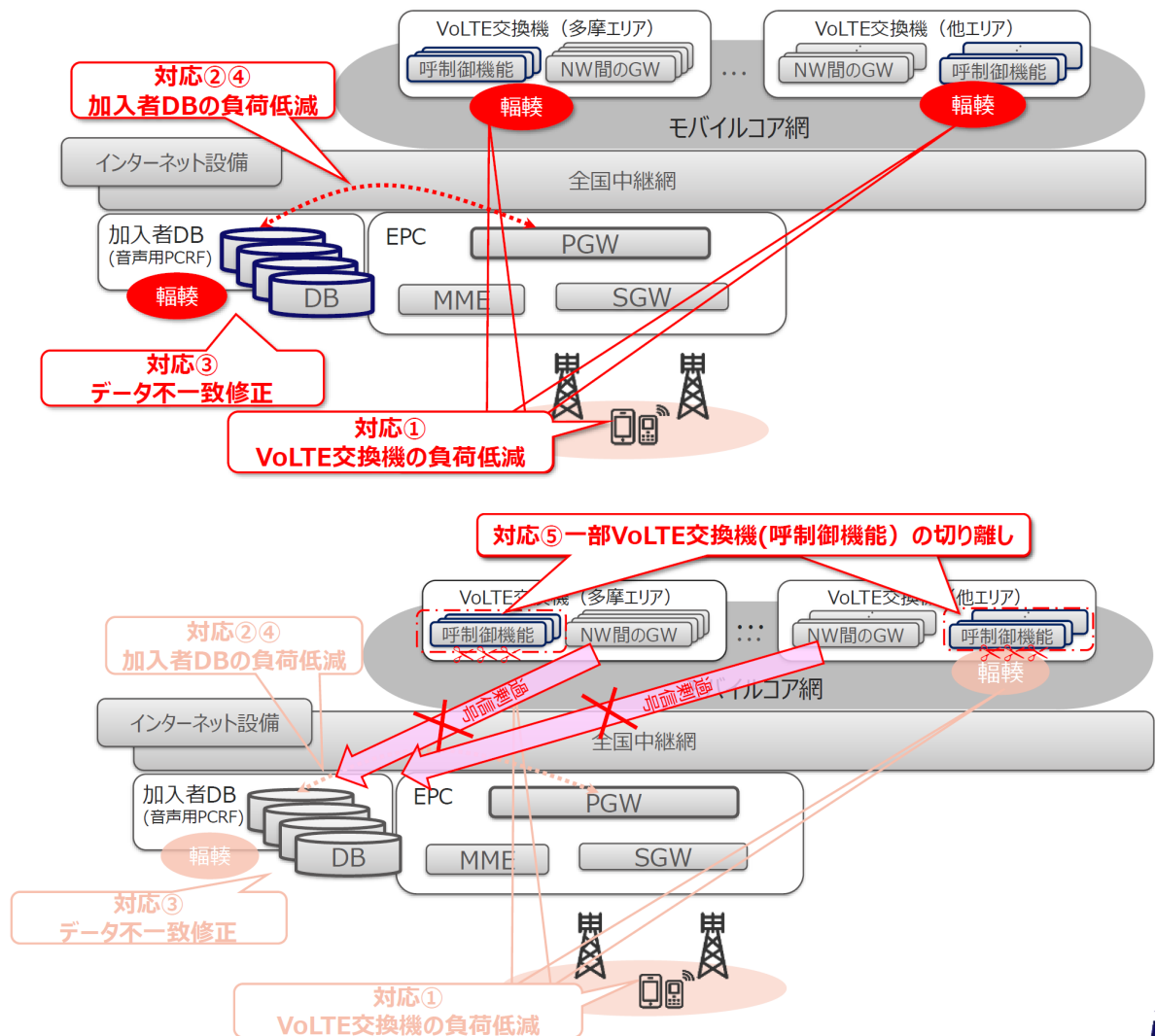


図 2-14 事故対応に係る措置

(7) 利用者への情報発信

KDDI 株式会社によると、今回の事故に関して、利用者から KDDI 株式会社に対して約 13 万件の電話又はメールによる問い合わせがあったとされる(7月8日 12 時時点)。その主な内容は、「電話が繋がらない、使えない」、「ネットが繋がらない」、「ホームプラス電話が使えない」、「どれくらいで(いつ)復旧するのか」、「補償について確認したい」、「通話ができるようにするにはどうしたらよいか」、「障害について確認したい」、「障害の原因は何か」等であったようである。

KDDI 株式会社及び沖縄セルラー電話株式会社は、自社のホームページで、通信状況、復旧作業の状況、復旧見通し等の情報を掲載するとともに、7月2日、3日、4日の合計3回記者会見、販売代理店において店頭での周知等を行ったと認められる。しかしながら、事故発生直後のみならず、2日目、3日目においても、利用者から多くの問い合わせ

せがあった状況に鑑みると、利用者に対して必要な情報が十分に提供できていなかったと推定される(図 2-15 参照)。

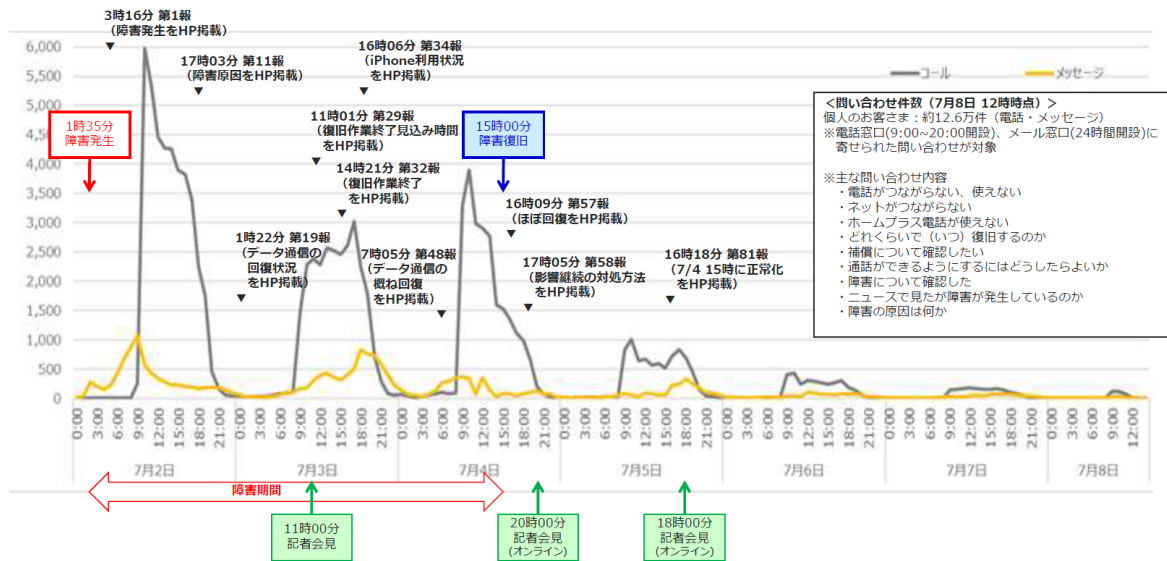


図 2-15 利用者からの問い合わせ件数の推移

2.2 発生原因

(1) メンテナンス作業時の原因

①作業管理者による手順書の指示誤り

KDDI 株式会社及び沖縄セルラー電話株式会社によると、メンテナンス作業の実施にあたり、作業管理者が作業実施者に対し、作業フォルダにある手順書で作業の準備を指示することとされていた。しかしながら、当該作業管理者が誤った作業フォルダを指示し、指示した作業フォルダに誤った作業手順書が保存されていたことで、誤った作業手順書を用いて作業が実施されたと認められる。この背景には、最新の作業手順書を保管するフォルダの場所に関するルールがなく、人為的なミスによる手順書の参照誤りが発生しうる状態となっていたこと、また過去の手順書を無効化する等の管理方法に関するルールがなかったこと等が考えられる。

②作業承認者における手順書内容の確認不足

KDDI 株式会社及び沖縄セルラー電話株式会社によると、作業承認プロセスに従い、作業の準備および不測の事態への対応等については、決められた作業承認者が確認を行うこととされていた。しかしながら、本作業について、当該作業承認者において適切な確認ができていなかったと認められる。

③作業実施者によるサービス正常性の確認不足

KDDI 株式会社及び沖縄セルラー電話株式会社によると、運用中の2台のルータから、1台へトラヒックを片寄せする作業を実施する際には、作業実施者が手順書に従いサービスの正常性確認を行うこととされていた。しかしながら、当該作業実施者において、サービスの正常性について適切な確認ができていなかったと認められる。

⑤ 切戻し時間の考慮不足

KDDI 株式会社及び沖縄セルラー電話株式会社によると、メンテナンス作業における切戻し（トラヒック切替え作業中に重大なトラブルが発生して新しいシステム等の稼働が見込めなくなったとき、切替えを中止して元の状態に戻すこと）によるサービス影響の見積もりは15分以内と想定していた。しかしながら、VoLTE交換機および加入者データベースの輻輳を考慮した事前評価が実施されておらず、適切な切戻し時間が設定されていなかったと認められる。

⑤作業承認プロセスにおける問題

KDDI 株式会社及び沖縄セルラー電話株式会社によると、作業承認プロセスにおいて、事前に想定した作業影響度においてリスクの大きな作業については、作

業承認会議にて各本部長レベルでの合同審議を実施している。しかしながら、今回の作業については、誤った作業手順の影響による全国的なモバイル網の輻輳影響が発生することを想定できていなかったため、作業承認会議への付議がされていなかったと認められる。

（２）大規模化した原因

①輻輳制御の設計ミス

KDDI 株式会社及び沖縄セルラー電話株式会社によると、輻輳耐性の点検を実施しており、ルータが故障した際には、端末から一斉に要求信号が送信されても、輻輳制御機能により自動的に解消できることを確認していたとしている。しかしながら、今回の事故では、多摩ネットワークセンター設置の VoLTE 交換機向けの信号が 1/2 の確率で応答するが、1/2 の確率で返らない状態となったため、異常と認識せず、自動的な輻輳解消ができなかったと認められる。こうしたネットワーク状態を異常と認識できていれば、障害を最小限に抑えることができたとも考えられ、輻輳制御の設計について課題があったと推定される。

②装置の動作に関する想定不足

また、こうした VoLTE 交換機向けの信号が 1/2 の確率で応答するが、1/2 の確率で返らないネットワーク状態時においては、装置自身が再送し大規模な輻輳が発生する可能性があることや、再送を抑止する状態管理機能が適切に機能しないことについて想定できていなかったと認められる。

③影響が全国へ波及するリスクの評価不足

KDDI 株式会社及び沖縄セルラー電話株式会社では、特定の拠点で発生する輻輳を早期に収束させるために全国フルメッシュ構成を採用していたとしているが、影響が全国に波及するリスクについての評価が不足していたと認められる。

（３）長期化した原因

①複雑な輻輳状態における復旧手順の考慮漏れ

「2.1 発生状況（４）一部 VoLTE 交換機の異常状態による加入者データベース輻輳の長期化」及び「同（５）セッション情報のデータ不一致」で記載のとおり、今回、VoLTE 交換機の輻輳状態を解消させる手順として、呼制御機能のリセット手順を実行したが、6 台の VoLTE 交換機は輻輳によって壊れたバックアップファイルを読み込み、起動したことで、位置登録要求信号の再送が繰り返されたと認められる。加入者データベースの高負荷により、すべての VoLTE 交換機から大量のエラーが発生したため、異常がある VoLTE 交換機の特定にも時間を要したと考えられる。また、当該 VoLTE 交換機を切り離すために閉塞を実施したが、異常状態が継続していたために閉塞処理が正常に完了せず、この事象に気づくのも時間

を要したと認められる。さらに、加入者データベースの輻輳を契機に、加入者データベースにおいて一部のセッション情報の削除処理が失敗し、VoLTE 交換機、加入者データベース、パケットネットワークのゲートウェイ装置（PGW）との間でセッション情報のデータ不一致が発生し、VoLTE 交換機を利用する全ユーザのセッションについて設備容量を超過しない範囲でリセットを実施したため、時間を要したと認められる。加えて、音声の発着信の成功率、端末から VoLTE 交換機への接続数等は正常値に戻った後も、高負荷状態が長時間継続していたため、音声サービスを提供するすべての設備の点検、安定動作の確認を行うため時間を要したと認められる。

上記に鑑みれば、KDDI 株式会社及び沖縄セルラー電話株式会社において、このような VoLTE 交換機や加入者データベースにおいて異常状態が生じることを考慮できていなかった、また、今回のような特異な事象に陥った際に VoLTE 交換機 1 台 1 台の装置状態を正確かつ速やかに把握する手順が十分ではなかったなど複雑な輻輳状態を復旧させる手順が確立できていなかったと推定される。

②VoLTE 交換機の動作検証及び動作確認不足

今回、KDDI 株式会社及び沖縄セルラー電話株式会社において、輻輳等により高負荷状態となった場合に VoLTE 交換機のバックアップファイルが壊れる可能性があること、VoLTE 交換機が壊れたバックアップファイルに基づき起動した場合に正常にリセットがなされず異常状態が継続する可能性があること、また加入者データベースの輻輳を契機に加入者データベースにおいて一部のセッション情報の削除処理が失敗し、ユーザのセッション情報が削除される事態が発生する可能性があることについて、十分に認識していなかったと考えられる。

特に、KDDI 株式会社によると、障害の対応においては、過去の商用の高負荷状態からの復旧経験に基づき、運用手順としてリセットを実施することとしていたが、テストベッドにおける検証は不十分であったと認められる。具体的には、システム開発・設計ガイドラインには「性能諸元値の限界以上（諸元値単体、組合せの両方）の負荷をかけ、システムのボトルネック、振る舞いを把握する」となっていたが、振る舞いの把握として明示的にシステムリセット等の考慮が不足しており、高負荷時の動作については、呼処理を中心に実施しており、高負荷下でのシステムリセットの挙動については検証をしていなかったと認められる。

VoLTE 交換機や加入者データベースに関して、正確な情報の取得、高負荷状態等の異常状態における動作検証及び動作確認について不足があったと推定される。

③事故対応訓練の不足

KDDI 株式会社及び沖縄セルラー電話株式会社によると、複数システムの監視担当者が連携して対処する様な複雑な訓練も実施していたとのことであるが、今

回のような、輻輳の自動制御が機能せず復旧のシナリオが立てられないような事象まで想定した訓練は実施できていなかったと認められる。

（４）利用者への情報発信が不十分だった原因

①利用者が必要とする情報を収集・整理する障害時の社内体制

KDDI 株式会社及び沖縄セルラー電話株式会社によると、障害発生当初においては、利用者へ発信できる情報がほとんどなかったこともあり、7 月 2 日（土）3:16 に障害報（第一報）を掲載後、14 時間の間、情報のアップデートがなされず、長時間に渡り、障害の状況などを的確に情報発信することができていなかったと認められる。また、障害報（第一報）では、タイトル・日時・対象サービス/影響・影響エリアの 4 項目であり、利用者が必要とする情報の種類（項目）や内容が不十分であったと認められる。さらに、利用者が見つけやすく、分かりやすい情報提供が出来ていなかったと認められる。

これは、障害時に利用者が必要とする情報を収集・整理する社内体制や仕組みが整備できていなかったことが原因と考えられる。

②分かりづらい表現・用語による情報発信

KDDI 株式会社及び沖縄セルラー電話株式会社によると、「復旧作業終了」と「本格再開」という表現について、同社としては、復旧作業終了後に流量制御等の解除および正常性の確認を経て本格再開（回復）を想定し案内していたが、利用者やマスコミからは「復旧作業終了」を「本格再開（回復）」と同義ととらえられたとしている。実際は復旧作業終了後も輻輳が解消せず流量制御を継続実施したことから、結果として利用者に大きな混乱を与えることとなった。利用者やマスコミにとって分かりづらい表現や用語の定義が不十分な状態で情報発信を行ったことも、利用者の混乱を招いた要因と考えられる。

3. 再発防止策

3.1 報告のあった主な再発防止策

（１）手順書管理のシステム化と社内ルールの見直し

今回の事故の発端は、上記「2.2 発生原因（１）メンテナンス作業時の原因」に記載のとおり、①作業管理者による手順書の指示誤り、②作業承認者における手順書内容の確認不足、③作業実施者によるサービス正常性確認不足 という３つのヒューマンエラーが重なったことによるものと認められる。また、KDDI 株式会社によると、当該確認作業は、すべて人手で確認する仕組みとなっていたとされている。

このため、KDDI 株式会社は、過去の手順書は無効化する等、誤った手順書が選択されること及び誤った手順書で作業が実施されることの徹底した防止や、ヒューマンエラーによるミスを防止し人手による確認をサポートする観点から手順書の管理・承認・利用を一元的に管理するためのシステムの構築を行うとともに、手順書の確認方法、確認手順、確認体制の見直し、設備の重要度を考慮した作業合同審議付議基準の見直し等を含め、必要となる社内ルールの見直しを行うこととしている。

（２）切り戻し設定時間の基準見直し

上記「2.2 発生原因（１）メンテナンス作業時の原因 ④切戻し時間の考慮不足」で記載のとおり、今回、VoLTE 交換機および加入者データベースの輻輳を考慮した事前評価が実施されておらず、適切な切戻し時間が設定されていなかったと認められる。

このため、KDDI 株式会社は、当該設備に対して作業を行う場合は、設備の処理限界や様々な挙動を考慮した事前のリスク評価を行った上で、作業ごとに切戻し時間を設定するとともに、作業にあたっては、万一の輻輳発生に備えた「輻輳時の復旧手順」を準備し作業に臨むとしている。

（３）輻輳制御の設計見直し

上記「2.2 発生原因（２）大規模化した原因 ①輻輳制御の設計ミス」で記載のとおり、今回の障害では、VoLTE 交換機向けの信号が 1/2 の確率で応答が返らない状態となったため、異常と認識せず、自動的な輻輳解消ができなかった可能性が考えられる。このため、KDDI 株式会社は、信号が 1/2 の確率で応答が返らない状態についても、異常性を認識させ、自動的な輻輳解消が実現できるように輻輳制御の設計見直しを行うとともに、サービス影響を局所化する対策を行うこととしている。また、影響が全国に波及するリスクを低減させるべく、VoLTE 交換機のネットワーク構成を全国フルメッシュ構成から、東西分散構成に変更すると

している。

（４）異常設備の検知ツールの開発・導入

今回、ネットワークの監視としては、エンドツーエンドのサービス健全性の監視やノード監視（リソース異常等、プロセス異常等）を行っていたが、この二つの監視では異常状態となっている VoLTE 交換機を特定できなかったとされている。このため、KDDI 株式会社は、事故の大規模化を防止するためには、VoLTE 交換機への要求の成功率を確認する等により、異常設備を早期に検知できる検知ツールの開発・導入を行うこととしている。

（５）復旧対処の自動化

上記「2.2 発生原因（３）長期化した原因①複雑な輻輳状態における復旧手順の考慮漏れ」で記載のとおり、VoLTE 交換機の輻輳状態を解消させる手順として、呼制御機能のリセット手順を実行したが、異常状態で起動したことで、位置登録要求信号の再送が繰り返され、さらに、加入者データベースでセッション情報のデータ不一致が発生するなど、複雑な輻輳状態が継続したと考えられる。

総務省では平成 30 年度から令和 2 年度に「革新的 AI ネットワーク統合基盤技術の研究開発」の「AI によるネットワーク運用技術」において、学習データに基づいた AI による障害検知・原因特定・復旧手順作成・復旧対処の研究開発を実施しており、現在、KDDI 株式会社において、技術開発を継続し、5G スタンドアローン方式のコアネットワーク設備を対象としたオープンソースソフトウェアによる障害分析 AI モデルを用いた障害発生検知と障害原因特定の実現性を検証中としている。KDDI 株式会社は、通信障害の長期化を防止するため、こうした復旧対処の自動化についての取組を進めるとしている（図 3-1 参照）。

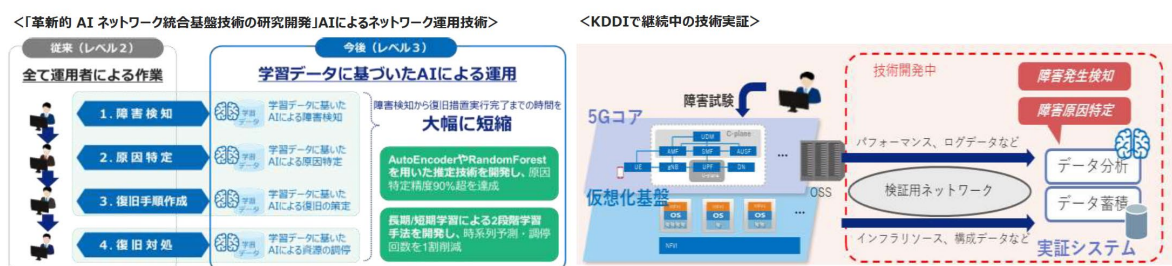


図 3-1 AI によるネットワーク運用技術

（６）輻輳発生時の復旧手順の見直し

上記「2.2 発生原因（３）長期化した原因①複雑な輻輳状態における復旧手順の考慮漏れ」で記載のとおり、今回、複雑な輻輳状態を復旧させる手順が確立できていなかった可能性が考えられる。

このため、KDDI 株式会社は、VoLTE 交換機を異常状態で起動しても、VoLTE 交換機の呼制御機能をリセットすることができる方法等、輻輳発生時の復旧手順の見直しを行うこととしている。

（７）利用者目線での分かり易い情報の定期的発信

今回の事故では、利用者が必要とする十分な情報が得られず、各地の販売代理店において説明を求める利用者であふれる等、多くの混乱が生じた。

このため、KDDI 株式会社は、改めて、利用者目線で、影響が想定されるサービス及び機種等の種類、影響の具体的な内容（状況が明らかになったら出来る限り具体的に表現）、復旧の進捗及び復旧予定時刻を含む復旧の見通し、復旧に時間を要する場合は代替手段（可能な場合）、原因、場所等が特定できる場合は原因と場所等の概要（セキュリティ上の観点から問題があると判断した事項は除く）等について、知り得る限りの情報を平易な用語を用いて定期的かつ速やかに情報発信することとしている。

（８）大規模障害時における広報部門を中心とした对外情報発信班の新設

今回の事故では、多摩ネットワークセンター設置の全国中継網コアルータ及び VoLTE 交換機だけでなく、全国の VoLTE 交換機や加入者データベースにまで輻輳が生じ、複数のシステムにまたがる複雑な輻輳状態が継続したと考えられる。

このため、KDDI 株式会社は、適切な復旧作業及び情報発信を行うためには、責任者を中核として全社横断的に対策を行う組織（「全社重大事故対策本部」）の立ち上げとともに、広報部門、運用管理部門、マーケティング部門、カスタマーサービス部門、個人・法人営業部門等、様々な部門が横断的に利用者影響・声を収集し、大規模障害時において適時適切な情報発信を行う对外情報発信班として、「お客さま広報班」を新設することとしている。

3.2 追加的再発防止策

上記「3.1 報告のあった主な再発防止策」に記載の、KDDI 株式会社及び沖縄セルラー電話株式会社から報告のあった再発防止策に加え、以下の再発防止策を行うべきである。

（１）人為的ミス防止する品質管理体制の強化

上記「2.2 発生原因 2.2 発生原因（１）メンテナンス作業時の原因」で記載のとおり、今回の事故の発端は人為的なミスによるものである。KDDI 株式会社では、人為的ミスの防止を含む、組織横断での品質向上活動の改善を検討するため、技術部門を中心とする品質改革担当（CQO）が任命されており、当該 CQO を筆頭と

する品質改革会議にて、技術統括本部横断で設備や作業の品質改善に取り組む品質向上活動を行なっているとしている。他方、手順書の保管フォルダ場所に関するルールがなく、人為的なミスによる手順書の参照誤りが発生しうる状態となっていた、過去の手順書についても無効化する等の処理方法に関するルールがない等、人為的ミスを防止する体制が十分であったとは言えない。改めて、人為的ミスを防止するための品質管理体制の強化を行うべきと考えられる。

(2) VoLTE 交換機及び加入者データベースの動作検証及びリスク評価の徹底
上記「2.2 発生原因(3) 長期化した原因②VoLTE 交換機の動作検証及び動作確認不足」で記載のとおり、今回、KDDI 株式会社及び沖縄セルラー電話株式会社において、輻輳等により高負荷状態となった場合に VoLTE 交換機のバックアップファイルが壊れる可能性があること、VoLTE 交換機が壊れたバックアップファイルに基づき起動した場合に正常にリセットがなされず異常状態が継続する可能性があること、また加入者データベースの輻輳を契機に加入者データベースにおいて一部のセッション情報の削除処理が失敗し、ユーザのセッション情報が削除される事態が発生する可能性があることについて、検証の実施を含め、十分に認識していなかった可能性が考えられる。

改めて、VoLTE 交換機及び加入者データベースについて、ベンダーから必要となる情報の取得、高負荷状態等の異常状態における動作検証及び動作確認を徹底するとともに、それに基づくリスク評価を適切に実施する等、VoLTE 交換機及び加入者データベースのリスク管理の徹底を行うべきと考えられる。また、運用手順として高負荷時のリセットが存在する場合には、高負荷時のリセットの検証を行うよう他設備も含めて点検を行うべきと考えられる。VoLTE 交換機等の高負荷状態の検証に関するテストベッドの規模に関して、自社単独で高負荷検証が実施できない場合は、ベンダーと連携しベンダーのテストベッド環境の下で自ら検証を実施することも含め、十分な検証を実施していくべきと考えられる。

(3) 輻輳の自動制御が機能しない事故への対応訓練

今回の事故では、VoLTE 交換機向けの信号が 1/2 の確率で応答が返らない状態においては、当該 VoLTE 交換機(呼制御機能)に対して信号の送出を何度も繰り返し、大規模な輻輳が生じる可能性があることを考慮できていなかった等、設備の動作確認の徹底と設備のリスク管理が課題としてあるのは前述のとおりである。加えて、平時から様々な異常状態の発生を想定し、事故対応訓練を怠ることのないようにすることも極めて肝要である。KDDI 株式会社では、1 時間未満復旧訓練を年間 15 回、実際の障害を題材とした訓練を年間 10 回実施する等、重大事故対応訓練を実施しているとしているが、改めて、輻輳の自動制御が機能しないよう

な事象まで想定した訓練を実施すべきと考えられる。¹¹

（４）端末仕様の改善に向けた取組

上記「2.1 発生状況（３）加入者データベースの輻輳」で記載のとおり、今回、端末仕様によりデータ通信の動作が異なり、一部の端末においては、音声用のセッション確立失敗時に、一定時間毎に圏内、圏外を繰り返す（圏外時はデータ通信の利用不可）動作がみられ、一部の利用者にはデータ通信にも影響が発生したと考えられる。音声用のセッション確立失敗時に、データ通信にも障害が及ぶ可能性がある端末については、端末メーカーと協力して、利用者にその旨を周知していくことが期待される。また、利用者にとってより使いやすい動作となるよう、音声のみ、データ通信のみでも通信できるサービスは利用できるようにするとともに、それが分かる表示にすることを含め、端末メーカーと協力して、ソフトウェアのアップデート等により仕様の見直しを行うことが期待される。

（５）代替手段の確保

携帯電話サービスは、国民生活や経済活動に不可欠なライフラインとなっている。自然災害や通信障害等の非常時においても、継続的に通信サービスを利用できる環境整備に向けて、総務省では令和４年９月から「非常時における事業者間ローミング等に関する検討会」を開催し、携帯電話利用者が臨時的に他の事業者のネットワークを利用することができる「事業者間ローミング」を始め、Wi-Fiの活用などの幅広い方策について検討を行うこととしている。今回の事故による影響等に鑑み、こうした代替手段の確保に向けた検討に積極的に貢献していくべきと考えられる。

（６）他通信事業者と連携した業界全体の情報発信の改善

携帯電話サービスが国民生活等の重要なインフラとなっている状況を踏まえ、事故発生時には、適時に具体的かつ分かりやすく利用者が必要とする情報を提供できるよう、周知広報の業務方法を改善し、非常時のリスクコミュニケーションを確実なものにすることが求められる。また、事故発生時の関係機関（緊急通報機関、政府、指定公共機関、報道機関等）や法人顧客等への連絡体制を強化し、非常時における電気通信事業者からの連絡を徹底することが求められる。

このため、本電気通信事故検証会議の下に「周知広報・連絡体制ワーキンググループ」を設置し、通信障害時に利用者が必要とする情報を利用者目線で丁寧かつ適時に提供できるよう、携帯電話事業者が行う周知広報の内容・頻度等につい

¹¹ なお、KDDI 株式会社及び沖縄セルラー電話株式会社によると、令和４年９月２３日に両社社長も参加した全社重大事故対策本部訓練を実施し、平時からの事故対応に備えたとされている。

て、具体的な業界ルールの検討を行うことが適切である。具体的には、利用者が必要とする情報の種類（事故状況、緊急通報への影響、その代替手段、復旧見通し等）の特定、周知広報で使用する用語（「復旧作業」「本格再開」「利用しづらい状況」「流量制御」「輻輳」等）の意味や使用方法等の定義について検討を行い、リスクコミュニケーションの一環として、それらを報道機関等と共有すべきと考えられる。また、そもそも携帯電話が使えない状態の利用者に対して、障害に関する情報が確実に伝わるよう、報道機関や販売代理店とタイアップを含む情報伝達手段の多様化、事故発生時に携帯電話事業者から関係機関（緊急通報機関、政府、指定公共機関、報道機関等）や法人顧客等に対する緊急の連絡体制を確実なものとする方策、災害時・障害時における通信の障害状況に関するデータの提供方法等についても検討するべきと考えられる。併せて、当該内容については、業務上の標準モデルを策定し、各携帯電話事業者の管理規程（電気通信事業法 44 条）や社内のコンティンジェンシープラン等に反映することも検討すべきと考えられる。こうした検討に積極的に貢献していくべきと考えられる。

4. 今後について

上記「3.2 追加的再発防止策」において追加の再発防止策について検討したが、（VoLTE 交換機及び加入者データベースに限らない）通信設備が抱える潜在リスクの洗い出しの不足（ベンダーとの情報連携や動作検証の不足含む）、システムの保守・管理態勢及び社内情報共有体制の不備、平時からの教育・事故対応訓練の不足、利用者への周知広報の不足、事業者間連携による対策の不足等、事故の背景にある構造的な問題については、他の通信事業者にも共通する課題であると考えられる。

こうした業界に共通する構造的な課題については、今後、本電気通信事故検証会議において、検証を深めていくことが必要である。

(参考) 電気通信事故検証会議 構成員一覧

(五十音順、敬称略)

- 相田 仁** 東京大学大学院 工学系研究科 教授
- 阿部 俊二** 国立情報学研究所 アーキテクチャ科学研究系 准教授
- 内田 真人** 早稲田大学 理工学術院 教授
- 加藤 玲子** 独立行政法人国民生活センター 相談情報部相談第2課長
- 黒坂 達也** 株式会社企 代表取締役
- 妙中 雄三** 奈良先端科学技術大学院大学 先端科学技術研究科
情報科学領域 准教授
- 中田 雅行** EY ストラテジー・アンド・コンサルティング株式会社マネージャー
(第2回会合から)
- 堀越 功** 株式会社日経BP 日経クロステック先端技術副編集長
- 森井 昌克** 神戸大学大学院工学研究科 教授
- 森島 直人** EY ストラテジー・アンド・コンサルティング株式会社パートナー
(第1回会合まで)
- 矢入 郁子** 上智大学 理工学部 情報工学科 准教授