小特集 1.

通信障害と社会

Communication Service Outage and Society

谷脇康彦

Abstract

通信ネットワークの構造変化に伴い，通信サービスの提供に関わるリスク因子の増大と多様化が進み，無謬主義からリスク管理主義への転換が求められる中，リスクの外的要因に対する機能保証と内的要因に対する信頼性向上を2本柱とする統合的なリスク管理・対処の手法の確立が求められている．本稿では通信障害をめぐる環境変化の中で通信事業者が取り組むべき対策の基本的な枠組みについて整理する．

キーワード：SDN/NFV，リスク評価，機能保証，信頼性向上，SRE

1. 問 題 の 所 在

通信ネットワークは社会インフラとして重要な役割を果たしており，通信サービスの停止等は社会経済活動に大きな影響を与える．特に社会経済システムのディジタル化の進展に伴い，通信障害が発生した際の影響は幾何級数的に深刻度を増している．このため，通信障害を防止する観点から電気通信事業法に基づく技術基準の策定・運用が行われているほか，各種ガイドライン(注1)の策定・見直しや所要の技術開発などが行われている．

しかし，通信ネットワークは技術的に大きな構造変化を遂げてきている．そこで本稿においては，こうした構造変化が起きている中にあって通信障害が社会に及ぼす負の影響を最小化するとともに，通信事業者による障害対策の効果を最大化する観点から，リスク評価を軸とする通信障害対策の在り方について整理する．

2. 通信ネットワークの構造的変化

通信ネットワークの構造的変化は多岐にわたるが，最大の変化の一つは回線交換網からIP網への転換である．回線交換網はエンドエンドの通信を回線占有で保証し，サービス品質も通信事業者によって厳密に管理されている中央集権型のネットワークである．これに対し，IP網で提供される通信サービスは，基本的に帯域を複数利用者により共有しつつパケット流通を行う自律分散を基本とするベストエフォート形のサービスである．この回線交換網からIP網への移行過程は完了段階に入りつつあり，NTT東西は2023年末をもって回線交換方式サービスの提供を終了し，IP網への移行を完了する方針を公表している(注2)．

このように，通信ネットワークの構造的変化の第1は「エンドエンドの品質保証形から自律分散のベストエフォート形への移行」である．このため，サービス品質の目指すべき水準を設定・維持するための手法が大きく変わってきている．

次に，通信ネットワークの構造的変化のうち現在進行中なのがハード・ソフトの分離，すなわちSDN（Software Defined Network）/NFV（Network Function Virtualization）技術の実装である．

これまで通信ネットワークを構成するハードは果たすべき機能が機器ごとに固定されてきた．しかし，ハード・ソフトの分離によりハード（機能が定義されていない汎用機器としてのホワイトボックス）の機能がソフトで定義されるSDN技術の実装が進んでおり，例えば米

谷脇康彦　(株)インターネットイニシアティブ
Yasuhiko TANIWAKI, Nonmember (Internet Initiative Japan Inc., Tokyo, 102-0071 Japan).
電子情報通信学会誌　Vol.107 No.1 pp.24-28 2024年1月

(注1)　例えば総務省「情報通信ネットワーク安全・信頼性基準」(1987年郵政省告示第73号)．
(注2)　https://web116.jp/2024ikou/service.html

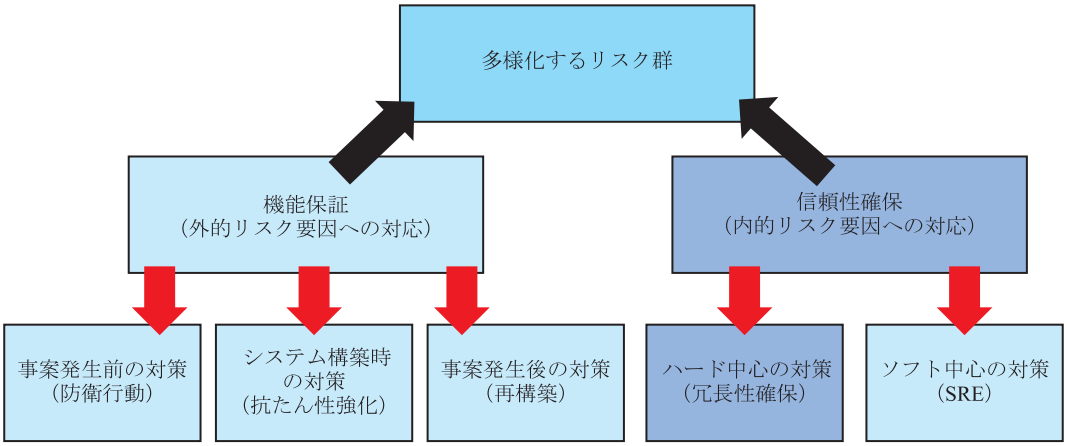

図1　リスクの多様化と対応手法　多様化するリスクへの対応として，機能保証と信頼性確保の二つのアプローチがある．（出典）筆者作成

国で携帯事業に新規参入したディッシュ・ワイヤレスはAWS（Amazon Web Service）でネットワーク運用を行うクラウド実装型のネットワークを構築している(注3)．

すなわち，ネットワーク資源を必要な箇所・時間に仮想的に集めてトラヒックを処理したり，流通するパケットの重要度に応じてネットワークをスライシングした上で帯域制御を行うなど柔軟なネットワーク資源の管理・運用が可能になっていく．しかも，ネットワーク資源の配分を行うオーケストレータの役割がAIによって自動化されることが期待されている．

このように，通信ネットワークの構造的変化の第2は「ハード・ソフト一体型からハード・ソフト分離型への移行」であり，一つの通信ネットワークを機能させるのに必要なプレーヤの数が増加している点が挙げられる．換言すれば，この構造的変化によりリスク因子の数が急速に増加しており，リスク管理が通信サービスの安定提供のために極めて重要な要素となってきていると言える．

このように，回線交換網からIP網への移行，そしてハード・ソフト分離を実現するSDN/NFV技術の実装により，通信障害を生じさせるリスク因子の増加や多様化が進んでいる．このため，伝統的な無謬主義を前提とする通信障害の評価や通信障害への対応策は修正が求められている．

3. リスクの多様化

ネットワークの構造的変化を原因とするリスク因子の増加や多様化が進む中，通信ネットワークの運用に関わるリスク評価について今日的観点から整理し，許容可能な残存リスクを見極めつつネットワークを運用すること（ゼロリスクの達成から残存リスクの管理への転換）が必要になっている（図1）．

まず通信障害を起こす可能性があるリスクには，内的（自律的）要因と外的（他律的）要因がある．このうち内的要因とは，設備の老朽化，ぜい弱性の顕在化，運用ミス，ソフトウェアのバグなどが含まれる．また外的要因とは，自然災害，サイバー攻撃，接続（卸元）事業者における障害，ソフトウェアのサプライチェーンリスク(注4)などが含まれる．外的要因（特にサイバー空間における脅威）はリスク因子としての複雑性が近年増している．その背景には武力攻撃とサイバー攻撃を組み合わせるハイブリッド戦争がウクライナで現実化するなど，国家主体によるサイバー空間への関与が強まっていることが背景の一つとして挙げられる．

4. 機能保証の手法

前章で見たように，通信ネットワークに関わるリスク評価については内的要因と外的要因に分かれる．そのうち，後者の外的要因に関するリスク管理の手法が機能保証（mission assurance）である(注5)．

宇宙政策委員会[2]によれば，機能保証は「事案発生前

（注3）　https://aws.amazon.com/jp/blogs/industries/telco-meets-aws-cloud-deploying-dishs-5g-network-in-aws-cloud/

（注4）　例えば，ライブラリの一部にぜい弱性が含まれていた2021年12月のLog4j2事案等が挙げられる．

（注5）　DoD[1]は，機能保証について「いかなる環境・条件であってもDoDの任務に不可欠な機能（Mission-Essential Functions（MEFs）…人材，機器，施設，ネットワーク，情報および情報システム，インフラおよびサプライチェーン…に不可欠な能力や資産の継続的な機能維持や能力の抗たん性を防御・確保するためのプロセス」と定義しつつ，任務保証の手法によって「DoDがより適切にシステミックなリスク因子，特にDoDの国内・国際における任務遂行を混乱させるDoDの統制外にある要因への依存について戦略的に識別・対処することを可能にする」（下線は筆者による）としている．

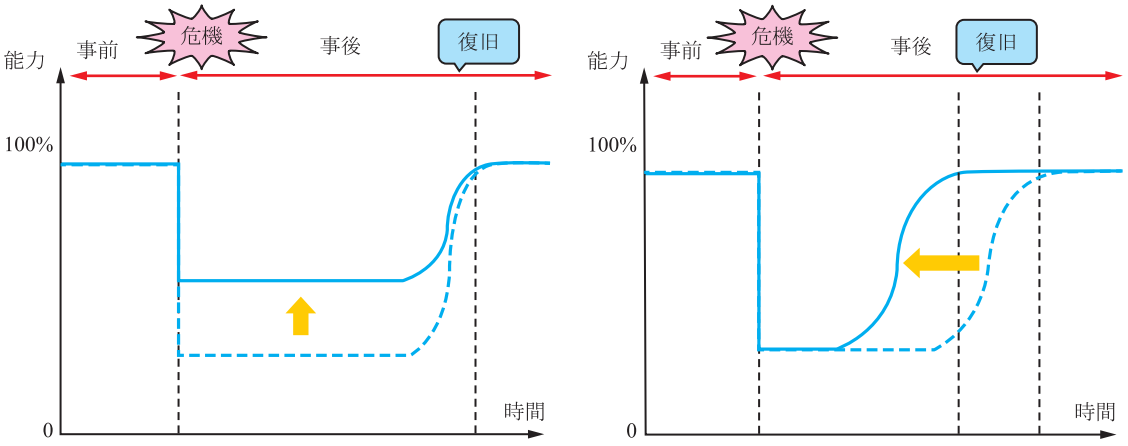

図 2　機能保証の強化による効果　機能保証の強化による効果は，必要な能力の確保（通信障害の範囲を一定の利用者数の範囲内にとどめる）と機能復旧の迅速化（通信障害の時間を一定時間内にとどめる）の二つで計測する．（出典）宇宙政策委員会宇宙安全保障部会「宇宙システム全体の機能保証（Mission Assurance）の強化に関する基本的考え方」（2017 年 4 月，宇宙システムの安定性強化に関する関係府省連絡会議）

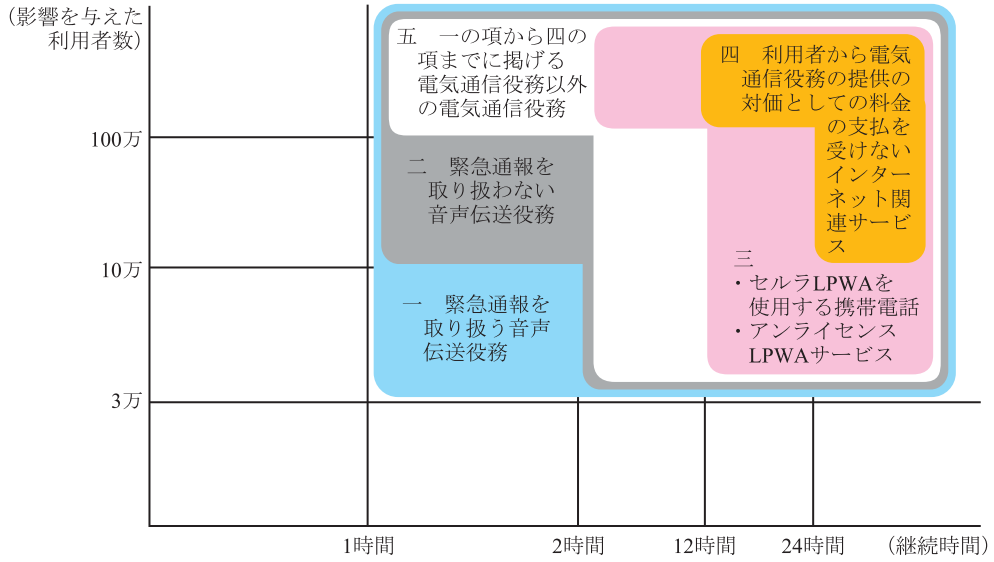

図 3　電気通信事業法に基づく重大事故報告制度（概要）　公的サービスである通信サービスに関わる重大事故は，電気通信事業法第 28 条等の規定に基づき，障害が「影響を与えた利用者数」と障害の「継続時間」で規定されている．（出典）総務省ホームページ「安全・信頼性の向上（重大な事故の報告）」

の対象（防衛行動）」，「システム構築時の対策（抗たん性強化）」及び「事案発生後の対策（再構築）」の三つのフェーズが存在し，必要な施策を講じることで通信ネットワークに求められる「機能（能力）の確保」と「迅速な機能復旧」を確保することが可能となる（図 2）．

通信事業において「機能の確保」と「迅速な機能復旧」を実現する場合，その具体的な水準（しきい値）は電気通信事業法第 28 条等に定める重大事故報告の基準がそれに該当する．具体的には通信障害が発生した場合の影響利用者数と通信障害の継続時間であり，これを上回る通信障害の場合は重大事故として政府に報告（事故後速やかに一報，30 日以内に報告書を提出）する制度がある（図 3）．このため，このしきい値内で障害事案を解消するために機能保証のメカニズムを活用することとなる．

ちなみに機能保証に基づくリスク評価は主としてサイバーセキュリティ分野で採用されている．例えばサイバーセキュリティ戦略本部は，通信，電力，鉄道など 14 分野をサイバーセキュリティ確保のための重要インフラと位置付け，そのリスク管理の手法として，機能保証の考え方に基づくリスク評価を推奨している[(3)]．

その際，本文書では機能保証について，「重要インフラ事業者等が社会経済システムの中で果たすべき役割・機能を発揮するために維持・継続することが必要なサー

ビスを特定し，許容できないリスクがない状態（＝安全）を確保しつつ，そのサービス提供を継続するために必要な業務や経営資源に係る要件を分析・評価した上で，『これに影響する事象の結果からリスク源まで』を演繹的に特定・分析・評価するアプローチ」（注：『』は強調のために筆者追記）であると規定している．

このように，機能保証の考え方は通信事業者ごとに個別に適用するだけでなく，上流から下流に至るサプライチェーンに参加する企業群での取組みや他の業態を含む重要インフラ全体での取組み（例えば重要イベントの開催に向けた業態横断的な防御対策）などの面的な取組みにも有効である．

5. 信頼性確保の手法

次に，信頼性確保の手法としてはハード中心の対策として冗長性確保の観点から対策が講じられてきている．例えば，総務省研究会報告書[4]では，通信障害対策として，ガバナンス強化，外部（第三者）モニタリングの実施，リスク管理の強化，予備系設備への切換不能時の対処のためのリスク管理，著しい高負荷時の動作検証，データ蓄積型設備への定期監視，訓練の実施，ヒューマンエラー防止対策，利用者への周知広報などを主要項目として列挙している．

このうち，外部モニタリングの実施については，金融庁による金融機関への検査・監督や国土交通省による運輸部門の保安監査の例を引きつつ，「（監査の）基本方針に基づき，毎年，（環境の変化等を踏まえ重視する観点や点検対象となる設備等を記載した）実施計画を策定して，実施していくことが考えられる」としている．

このように，総務省研究会報告書は設備面に着目したハード主体のリスク管理，より具体的には冗長性を確保するための信頼性確保のための施策強化に力点が置かれている（図１の濃い色の部分）．これは，設備に着目し設備面を中心に規律を構成してきた電気通信事業法の枠組みの中で合理性を有するものであるが，今後のネットワーク構造の変化に対応した規律の不断の見直しが重要である．

具体的には，前述のとおり SDN/NFV 技術の通信ネットワークへの実装が進むハード・ソフト分離型のネットワーク構造に適用したリスク管理が求められる．この点は前掲の総務省研究会報告書においても視野にとらえており，「仮想化技術等の進展によって，モバイル網のコアネットワークのような電気通信回線設備の伝送交換の制御に係るコア機能を自ら管理せず，外部から当該コア機能の提供を受けて，電気通信サービスの提供を行うことが技術的に可能となっており，（中略）このような場合であっても，外部から提供を受けたコア機能に関しても電気通信サービスの確実かつ安定的な提供のために不可欠なものとなることから，適切にガバナンスを強化していく取組が重要である」と指摘している．

このように総務省研究会報告書ではハード・ソフト分離という構造的変化について「ガバナンス強化」という一般的な記述にとどまっているが，その具体的な運用の在り方について検討を具体化していく必要がある．

その一つの手掛かりがグーグルの提唱する SRE（Site Reliability Engineering）の考え方である[5]．

アプリケーション主体のネットワーク構造になると，ネットワーク運用部門とネットワーク開発（機能追加）部門の連携の在り方が問題となる．機能追加が多数行われると，それだけ運用部門にとっては運用リスクが高まることになる．他方，運用部門の立場を受け入れた安定運用のみを取り入れると機能追加による利便性向上が果たせなくなる．

このため，運用部門と開発部門の間のトレードオフ関係を調整するメカニズムが必要になる．

SRE では，その判断基準として SLO（Service Level Objective）を設定し，スループットなどネットワークの運用に関わる基準値を設定する．その際重要なのが「エラーバジェット」という考え方である．すなわち，エラーによるネットワーク停止時間がエラーバジェットを超える（想定以上のネットワーク障害が発生）場合には運用部門の活動を重視して安定運用を確保することに注力し，開発部門による機能リリースを控えることになる．

このように開発者と運用者を一体的に捉えつつエラーバジェットを基準としてネットワーク管理の力点の置き方を変えるのが SRE の基本的なアプローチである．

加えて，SDN/NFV 技術が実装されたネットワーク運用におけるオーケストレーション機能の自動化を AI に委ねる場合，通信事業者によって設定されたネットワークの運用方針を AI が遵守しているかどうか定期的に確認することを可能にする AI のアルゴリズムのガバナンスや説明責任（アカウンタビリティ）を果たしているかどうかという透明性の視点も重要な検討事項になる．

6. 留意すべき事項

ネットワーク構造の変化に伴い，通信障害が発生した場合の対応の在り方も大きく変わりつつある．その根底にあるのは無謬主義からリスク管理主義への転換であり，他方，発生する障害が社会的に許容範囲内に収まっていると言えるのかどうか，社会全体のコンセンサスを得ながら丁寧なルールづくりを進めていく必要がある．その観点から留意すべき事項として以下の３点を指摘しておきたい．

第１に，無謬主義からリスク管理主義に移行するとし

ても，障害発生時の利用者への情報提供は迅速かつ充実した内容であることが必要になる．総務省ガイドライン[(6)]は，こうした問題意識に立って，復旧の見通し（復旧進捗状況，復旧予定告示等）または復旧日時，代替的に利用可能な通信手段とそれらの利用方法，対象事故等の原因及び場所，掲載事項がいつの時点のものかを示す日時等の情報提供の必要性を指摘している．特に，携帯電話が国民全てのライフラインとなっている今，復旧の見通しに関する情報及び代替的に利用可能な通信手段とそれらの利用方法に関する情報は飛躍的に重要になってきている．

なお，後者の代替手段の提供に関連して，総務省での検討の過程で出てきた携帯電話事業者間のローミングの実現（2025 年度末をめどに実現）や MVNO 事業者等によるマルチプロファイル対応型の SIM（1 枚の SIM で複数事業者の回線を切り換えて利用可能）の提供といった取組みが出てきたことは利用者の視点から見て評価できる．

第 2 に，ハード・ソフト分離の進展に伴って，総務省研究会報告書も指摘しているように，海外のクラウドからソフト機能が提供される事例も今後多数出てくると考えられる．こうした機能提供の在り方は現行法においても可能であるが，かつてインターネットの経路設定問題で日本の通信サービスが混乱した事例[(注6)]などに見られるように，複数事業者・ベンダ間の責任関係の明確化が今後ますます重要になる．一義的には，利用者と直接契約しているサービス提供者が利用者に対して責任を持つべきであるが，リスク管理の切り分け（責任分界点の明確化）など平時から障害発生時に備えた対応策を明確化し，十分な説明責任が果たされるような環境を整えておくことが重要である．

第 3 に，ネットワーク管理者による平時のリスク管理や通信障害発生時の対応については，複雑化してきている一方，対応の迅速化が従来以上に求められるようになってきている．こうした中，規律の在り方について従来以上にソフトローの重要性が高まってきている．例えば，基本的な規律を国が定め，これを実現するための具体的な対応策については各事業者が自主的取組みとして実施し，その成果を国が評価し，必要に応じて規律に盛り込むという共同規制（coregulation）のアプローチなども取り入れ，柔軟かつ多様な取組みを通じたリスク管理を実現していくことが望ましい．

（注 6） 2017 年 8 月に発生した事案．グーグルが誤った経路設定情報を海外プロバイダに誤って発信したことから，一部の回線に過大な負荷によるひっ迫と遅延が生じたが，グーグルがこれを修正したことで問題が解消した．

7. 結　　語

以上見てきたように，通信ネットワークの構造的変化として「エンドエンドの回線交換方式から自律分散のベストエフォート形への移行」が完了間近であるほか，「ハード・ソフト一体型からハード・ソフト分離型への移行」が進行している．こうした変化は通信ネットワークを巡るリスク因子の増加と多様化をもたらし，通信障害の発生リスクに影響を与える．

こうした中，基本的には通信サービスの運用の在り方として伝統的な無謬主義からリスク管理主義に移行する中，包括的なリスク管理の在り方として外的要因を扱う機能保証と内的要因を扱う信頼性向上の二つの取組みが必要になる．特に，機能保証についてはサイバーセキュリティの文脈で語られることが多いものの，リスクの増加や多様化が進展する中，従来のネットワーク信頼性向上のための方策と一体的・包括的に取り組むことが重要になってきている．

また，その際には通信障害発生時の利用者説明の充実，海外からのサービス機能提供への着実な対応，ソフトロー的なアプローチの充実なども図っていく必要がある．

このように，ネットワーク構造が今後も大きく変化していくことが見込まれる中，そうした構造変化に対応しつつ通信障害とそれに関連するリスク評価等の在り方について不断の見直しを行っていくことが求められる．

文　　献

（1） Department of Defense, “Mission assurance strategy,” April 2012.
（2） 宇宙政策委員会宇宙安全保障部会，“宇宙システム全体の機能保証（Mission Assurance）の強化に関する基本的考え方，”宇宙システムの安定性強化に関する関係府省連絡会議，April 2017.
（3） サイバーセキュリティ戦略本部重要インフラ専門調査会，“重要インフラにおける機能保証の考え方に基づくリスクアセスメント（第 1 版），”2018 年 4 月，2019 年 5 月改定.
（4） 総務省電気通信事故検証会議，“電気通信事故に係る構造的な問題の検証に関する報告書，”March 2023.
（5） Google Cloud Blog, “Are we there yet? Thoughts on assessing an SRE team’s maturity,” June 2021.
（6） 総務省，“電気通信サービスにおける障害発生時の周知・広報に関するガイドライン，”May 2023.

（2023 年 7 月 27 日受付　2023 年 8 月 14 日最終受付）

谷脇　康彦（たにわき　やすひこ）

1984 一橋大・経済卒．同年，郵政省（現総務省）入省．内閣サイバーセキュリティセンター（NISC）副センター長，総務省総合通信基盤局長，総務審議官等を歴任．現在，インターネットイニシアティブ取締役副社長．著書に「サイバーセキュリティ」（岩波新書），「教養としてのインターネット論」（日経 BP）など．