

デジタル 主権

統制、依存、イノベーションの
バランスを図る

本資料は、Capgeminiが海外で公開した英語版レポートをもとに作成した日本語翻訳版です。
英語版レポート：Digital Sovereignty - Balancing Control, Dependencies, and Innovation

https://www.capgemini.com/wp-content/uploads/2026/05/27-05-2026-CFT11_Sharad-Sriwastawa_Rakuten-v2.pdf

#11 — 2026 年

Con
ver
sa
tions
FOR TOMORROW



シャラッド・ スリオアストア氏

楽天モバイル株式会社 代表取締役
共同 CEO 兼 CTO
楽天シンフォニー株式会社 代表取締役
社長執行役員



ネットワークの 所有： 「主権」が通信 事業の次の開拓 分野となる理由

シャラッド・スリオアストーア（*Sharad Sriwastawa*）氏は
楽天モバイル株式会社の共同最高経営責任者（CEO）
兼最高技術責任者（CTO）であり、楽天モバイル株式
会社の完全子会社である楽天シンフォニー株式会社の代
表取締役社長執行役員も務め、オープンなクラウドネイ
ティブプラットフォームのグローバル普及を率いています。
シャラッド氏は2018年に楽天モバイル株式会社に入社し、

日本国内における最新かつ最先端の楽天モバイル完全仮
想化クラウドネイティブモバイルネットワークの展開を統括。
現職には2023年に任命されました。これまで、インド、
中東、オーストラリア、米国、アジアにおいて、*Reliance*、
T-Mobile、*Telstra*、*Siemens* や、*RAN* 技術ベンダー
の *Airspan Networks* など、大手携帯電話事業者や
ベンダーでグローバル部門の幹部職を歴任してきました。

楽天のオープンプラットフォームアプローチの起源

Open RAN とは何か、そして楽天モバイルがどのようにネットワークを構築したかについて、簡単にご説明いただけますか？

シャラッド氏：2018 年当時、楽天モバイルは、従来の通信事業者と同じ道を歩み、既存のベンダーを選択し、従来の方法でネットワークを構築することも可能でしたが、実際にはそれとは大きく異なるルートを選択しました。

当社は、次の 4 つの柱に基づいて楽天モバイルネットワークを構築しました。第 1 に、独自の設備ではなく、市販のコモディティサーバーを使用し、ハードウェアとソフトウェアを完全に分離すること。第 2 に、RAN だけでなくコア、BSS、ロードバランシングなど、すべてのワークロードを完全に仮想化しクラウド化すること。第 3 に、初日から AI と自動化を導入すること。当社は日本の既存通信事業者と競争していたため、コスト構造を厳密に統制する必要がありました。そして第 4 の柱として、DevSecOps アプローチを用いて、最初からセキュリティを組み込みました。

Open RAN は、当社の定義によれば、単にソフトウェアを仮想化するだけにとどまりません。ハードウェアスタックとソフトウェアスタックを完全に分離し、ブラックボックスシステムから脱却して、ソフトウェア定義アーキテクチャへと移行することを指しています。そのような変革により、従来よりも優れた柔軟性が得られ、設備投資費、事業費共に大きく削減できました。現在はこの費用削減分を、低価格のコネクティビティという形で、お客様に還元できています。



シャラッド・スリオアストーア氏
楽天モバイル 共同CEO |
楽天シンフォニー
代表取締役社長執行役員

“

2018 年当時、楽天モバイルは、従来の通信事業者と同じ道を歩み、既存のベンダーを選択し、従来の方法でネットワークを構築することも可能でしたが、実際にはそれとは大きく異なるルートを選択しました。

ネットワーク主権について

楽天にとって「ネットワーク主権」とは何ですか？

シャラッド氏：ネットワーク主権とは、インフラストラクチャを自ら所有し、ネットワーク内で何が実行されるかを自ら統制し、その地域の特性やニーズに基づいて独自のソフトウェアロードマップを自ら統制することです。

根本的には、ネットワーク主権は、許可に基づくイノベーションの終わりを意味します。何十年もの間、事業者は新機能を導入するためにベンダーのリリースサイクルを待つ必要がありました。主権を持つことにより、自社ネットワークを自ら運用・管理できるようになります。ただ技術を活用するのではなく、投資した技術の所有者となるのです。

政府もまた、「データ主権」から、「インフラストラクチャ主権」および「ソフトウェア主権」へと重点を移しつつあります。それと並行して、多くの政府は地政学的な問題を受けて、ハイリスクのベンダーや信頼できないベンダーに制限を課し、あるいはそのようなベンダーの排除を義務付けるようになってきました。そうした事情が重なった結果、現在、ネットワークに対する事業者の考え方が根本的に変わりつつあります。

“

ネットワーク主権とは、インフラストラクチャを自ら所有し、ネットワーク内で何が実行されるかを自ら統制することです。

**「Open RAN
によって、
主権は経済的に
実現可能になり、
運用コストの面でも
負担可能になります」**

Open RAN は、技術的な観点で選択すべきものでしょうか、それとも主権の観点で選択すべきものでしょうか？

シャラッド氏：両方です。Open RAN の導入によって、ネットワーク主権の確保が経済・運用面で実現可能となります。主権について語ることはできても、そのコストが高すぎれば、事業者は主権を追求しなくなります。特に、ARPU[1 ユーザーあたり平均収益]の増加や、設備投資費、事業費の削減を求められる状況ではそうなります。

Open RAN は、事業者にとって現実的に手が届く「主権」への道を切り開きます。事業者は、財務の持続可能性を損なわずに自社ネットワークを運用・管理できるようになります。

エグゼクティブによる対談

オープンシステムとクローズドシステムの脆弱性について、どのようにお考えですか？

シャラッド氏：ネットワークの脆弱性の原因は 2 つあります。1 つは単一障害点で、もう 1 つは異常があったときに即座に対応できないことです。

Open RAN はそのいずれの問題も解決します。ハードウェアとソフトウェアが切り離されているため、地政学的な混乱が生じた場合や、特定のベンダーにセキュリティ上の脅威が生じた場合に、ハードウェアコンポーネントを比較的容易に変更できます。しかも複数のオプションから選択できます。

ベンダーロックイン状態のシステムでは、唯一のサプライヤに異常があった場合、その状況から脱却することは極めて困難です。その点で、クローズドシステムこそが脆弱なシステムです。

楽天モバイルは、完全仮想化クラウドネイティブネットワークを大規模に構築した数少ない組織の 1 つですが、その経験から、主権に関して学ばれたことを教えてください

シャラッド氏：Open RAN とクラウドネイティブは関連してはいますが、個別に考えるべき 2 つの概念です。主権の問題に対する関わり方がそれぞれ異なります。Open RAN は基本的には「分離」に関する概念です。クラウドネイティブ、つまりは Kubernetes¹、マイクロサービス、コンテナ化ワークロードを意味しますが、これは Open RAN とは次元が異なります。

クラウドネイティブの考え方は、次の 3 つに基づいています。第 1 に、「スピードと変更のしやすさ」です。従来の通信事業では、エンジニアは今でもメンテナンス時間帯に夜通し作業を行い、アップデートを適用（展開）しています。一方、OTT プロバイダの IT ワークロードの管理方法を見てみると、ダウンタイムがない状態で、日中に変更要求に対応しています。自己修復が可能なアーキテクチャになっているためです。第 2 に、そこから直接、「運用の利便性」が生じます。第 3 に、最も重要な「セキュリティ」です。クラウドネイティブネットワークは不透明ではありません。セキュリティテストの場合でも、セキュリティアルゴリズムを直接 CI/CD[継続的インテグレーション / 継続的デリバリー] パイプラインに組み込む場合でも、クラウドネイティブネットワークにより得られる可視性は、クローズドシステムで提供されるあらゆるものを大きく上回ります。

¹Kubernetes は、コンテナ化されたアプリケーションのデプロイメント、スケーリング、管理を自動化するオープンソースシステムです。



主権を追求する事業者にとって、楽天のアプローチはどのような広範な影響力を持っていますか？

シャラッド氏：Open RAN は今年になって勢いを増しています。現時点で 10 以上の概念実証段階のデプロイメントが稼働しており、2026 年から 2027 年には、そのうち 4 から 5 のデプロイメントがスケーリング段階に進む見込みです。ドイツの通信事業者である 1&1 と共同で構築したネットワークは、Open RAN の規格に基づく欧州初の完全仮想化モバイルネットワークであり、順調に成長しています。米国の Boost Mobile も別の実証事例となっています。

この技術にはもはや疑いの余地はありません。大規模な MIMO[Multiple Input Multiple Output]、電力効率、スケーラビリティに関する懸念が解消されました。足りないのは、移行への商業的な動機だけです。

今後は、あらゆるグリーンフィールドの事業者が Open RAN を選択することになるでしょう。Open RAN のアーキテクチャには、4G から 5G、6G へと移行できる柔軟性があり、独自のクローズドシステムを取り換える必要がないからです。

ドイツの通信事業者である 1&1 と共同で構築したネットワークは、OPEN RAN の規格に基づく欧州初の完全仮想化モバイルネットワークであり、順調に成長しています

AI は通信事業をどのように変えるとお考えでしょうか？また、AI により新たな主権の依存関係は生じますか？

シャラッド氏： 通信事業においては、検討すべき 2 つの明確に異なる側面があります。1 つ目は、ネットワーク運用における AI の活用です。2 つ目は、現状はまだ数少ないのですが、AI ネイティブ製品についてです。BSS[ビジネス支援システム] と OSS[運用支援システム] では、さまざまなものが具体化し始めています。しかし、より大規模なネットワーク資産に対しては、AI は 20 年前に設計された従来のインフラストラクチャの上層に位置付けられています。クラウド化されておらず、アーキテクチャ段階からの AI ネイティブにもなっていません。さらに上層で、ある程度の自動化を実現できますが、基盤のアーキテクチャにより自動化の上限が定められています。

しかし、AI には極めて高いポテンシャルがあります。世界全体の通信事業者の設備投資費と事業費をまとめると膨大な額になりますが、AI はその費用削減につながる、意味のある道筋を示します。事業者はこの分野で協力し始めています。今年の MWC (Mobile World Congress) では、AT&T が独自の小規模言語モデルの取り組みを発表しました。ネットワーク運用には、大規模言語モデルは必要ありません。費用対効果の高い、ドメイン固有の小規模言語モデルが必要なのです。顧客向けアプリケーション、BSS、カスタマーサポート、小売業の接客においては非常に大きなビジネスチャンスがあり、あらゆる企業がその取り組みを進めています。

未来のコネクティビティを所有する

ある国が「未来のコネクティビティの所有を目指す」と言った場合に、それは現実的にはどのような意味になりますか？

シャラッド氏： 近年の地政学的リスクの顕在化により、特定のデータセンターが被災し、銀行システム全体が停止するという事態が発生しました。これにより、限られた数の一元的な資産に過度に依存するリスクが露呈しました。各国は将来を見据えて、レジリエンスの高いネットワークを、多数の小規模な設備を基盤にして構築しようとしています。大がかりな設備投資をしなくてもシームレスなフェイルオーバーを実行できる、自動化機能を備えたネットワークです。

各国は将来を見据えて、レジリエンスの高いネットワークを、多数の小規模な設備を基盤にして構築しようとしています。

そのようなシステムは、国内の人材で運用できる程度に簡易である必要もあります。そうすれば、ネットワークの稼働状態を維持するために、高度な専門性を備えたエキスパートが世界中を飛び回ることもなくなります。インフラストラクチャを所有すれば、そのインフラストラクチャはいつでも自在にアクセスでき、透明性が高く、ブラックボックスのない状態になるのです。



「Open RANでは、
ソフトウェアを取り
込み、独自のハード
ウェアを調達し、
ネットワークを
運用し、特定の
ベンダーへの依存を
排除します」

主権のあるネットワークでもグローバルに展開し、相互に運用できるのでしょうか？

シャラッド氏：「主権」は分断を意味するものではありません。プロトコルは標準化されます。デバイスは、プロトコルに従っていなければ動作しません。Open RANは全体的に3GPPに基づいているため、誰でも、どこでもデプロイできます。アーキテクチャに組み込まれた固有のベンダー依存性というものも存在しません。事業者はソフトウェアを取り込んで所有でき、やがてコードを取り込んで自ら変更できるようになります。それが私の予想する未来です。

これまでの30年から40年の間、ネットワーク事業者は収益を生み、顧客満足を実現することに力を入れてきました。技術ドメインについては他人任せでした。しかし、次世代のCTOは現在、技術の管理だけでなく所有についても検討し始めています。通常の企業が自社のIT資産をどのように扱っているかを見てみると、ただITを管理しているだけでなく、自社で所有しています。そのような所有権を重視する考え方を、通信事業にも取り入れる必要があります。

Open RANでは、ソフトウェアを取り込み、独自のハードウェアを調達し、ネットワークを運用し、特定のベンダーへの依存を排除します。今後はこれと同じロジックがスタック全体に行き渡ることになります。RANの場合にそうであったように、規格がすでにあれば、状況は比較的単純です。一方、インフラストラクチャの可観測性のように、規格がまだ存在しない場合は、対応する規格をまず開発する必要があります。

オープン性とセキュリティ

オープン性はセキュリティリスクを高めると受け止められていますが、それについてはどのようにお考えですか？

シャラッド氏：オープンシステムは本質的にセキュリティが低いというわけではありません。システムを所有していれば、可視化できます。可視化できれば、より高いセキュリティをもたらすことができます。不透明なクローズドシステムでは、何も対策はできません。ブラックボックス内で何らかの異常があったときに、効果的に調査、計測、対応できないのです。単一のベンダーのプラットフォーム内に脆弱性があり、それが世界中の事業者に影響を及ぼし、広い範囲で同時にアップグレードしなければならないというケースはこれまで多く確認されました。これが、不透明な集中型の依存性を持つリスクです。

AI 駆動のセキュリティ機能が驚異的なペースで発展しているのを見ると、これらのツールは、透明性があり調査可能なシステムにおいて最適に動作します。従来のペネトレーションテストの機能は徐々に自動的に処理されるようになっており、その傾向は今後も加速するばかりだと思われます。原則は単純です。クラウドネイティブになる、透明性を備える、そして独自のインフラストラクチャに確実にアクセスできるようにすることです。そのようにアクセスできなければ、セキュリティを高めることはできません。

最高幹部に向けた推奨事項に関するアドバイス

未来型の通信事業ネットワークを構築しようとしている CTO と CIO に向けて、特に推奨することを教えてください

シャラッド氏：第 1 に、国または地域のレベルで主権を追求している場合は、孤立して競争するのではなく、事業者同士で協力しなければなりません。未来に向けて選択すべき技術について、地域全体で標準化する必要があります。そして、事業者は標準化された技術をただ管理するのではなく、協力して創出し、所有しなければなりません。ただし、それには時間がかかります。この業界は何十年もの間、少数のベンダーに依存してきており、必要とされるスキルセットはまだ、広い範囲で獲得できるものにはなっていません。

第 2 に、主権を得るには、技術だけでなくインフラストラクチャの所有権も必要になります。また、その信頼性に対する責任を受け入れる必要もあります。

第 3 に、レジリエンスを設計に組み込む必要があります。その際に課題となるのはコストです。複数の冗長なデータセンターを建設する代わりに、設備投資の負担がなくても冗長性があるかのように振る舞うアーキテクチャの構築を目指す必要があります。それを実現できるのは、クラウドネイティブアプリケーションだけです。



シャラッド・スリオアストーア氏
楽天モバイル 共同 CEO |
楽天シンフォニー
代表取締役社長執行役員

**「国または地域のレベルで主権を
追求している場合は、孤立して
競争するのではなく、事業者
同士で協力しなければなりません」**

キャップジェミニについて

キャップジェミニは、AI を活用してビジネスならびにテクノロジーの変革を支援するグローバルパートナーとして、お客様に具体的なビジネス価値をご提供します。企業の未来を描き、AI・テクノロジー・従業員の力を融合させ、その実現をご支援します。当グループは、約 60 年にわたる確固たる実績を有し、50 か国以上に展開する 42 万人超の使命感あふれる多様性に富んだチームメンバーから成る組織です。深い業界知識と強力なパートナーエコシステムを基盤に、戦略・テクノロジー・デザイン・エンジニアリング・ビジネスオペレーションにおける高度な専門性を活かし、エンドツーエンドのサービスとソリューションをご提供しています。2025 年のグループの売上高は 225 億ユーロです。

Make it real | www.capgemini.com

キャップジェミニ・リサーチ・インスティテュートについて

キャップジェミニ・リサーチ・インスティテュートは、デジタル全般に関するキャップジェミニの社内シンクタンクです。デジタル技術が従来型の大企業に及ぼす影響についての調査レポートを発行しています。キャップジェミニの、グローバルな専門家ネットワークを活用し、アカデミアやテクノロジー企業と緊密に連携しています。インド、シンガポール、英国、米国に研究専門拠点を有します。最近では、独立系アナリスト企業によるリサーチ品質の調査で世界第 1 位にランキングされました。

詳しくは <https://www.capgemini.com/insights/research-institute/> をご覧ください。

本書はキャップジェミニ・グループの所有物であり、秘匿情報または機密情報が含まれている可能性があります。
公開情報。Copyright © 2026 Capgemini. All rights reserved.

