Cisco Customer Experience

やわらかいインフラ

ホワイトペーパー SP 版

---シスコが考える運用の課題とあるべき姿---

Version 1.0

Cisco Systems, Inc.
Corporate Headquarters

170 West Tasman Drive
San Jose, CA 95134-1706 USA

Phone: +1 408-526-4000
Toll Free: +1 800-553-NETS (6387)
Fax: +1 408-526-4100

目次

図目次

本書について

著者

Name	Title
Kazuhide Inokuchi	Principal Architect, Cisco Customer Experience
Masanori Iwamoto	Customer Delivery Architect, Cisco Customer Experience
Shuji Nakano	Consulting Engineer, Cisco Customer Experience
Toshiki Hayashi	Customer Delivery Architect, Cisco Customer Experience
Yuhei Otsuka	High Touch Engineering Technical Leader, Cisco Customer Experience
Joon Sim	Consulting Engineer, Cisco Customer Experience
Teru Sato	Leader, Cisco Customer Experience

履歴

Version	Date	Status	Reason for Change
1.0	June 2024	Release Version	Initial Release

参考文献

1. (2018). 2050 年までの経済社会の 構造変化と政策課題について. 参照先: https://www.meti.go.jp/shingikai/sankoshin/2050_keizai/pdf/001_04_00.pdf
2. (2023). 重大な事故の報告. 参照先: https://www.soumu.go.jp/menu_seisaku/ictseisaku/net_anzen/jiko/judai.html
3. (2023). Gartner、IT 運用担当者はキャリア・パスに不安を抱えているとの調査結果を発表. 参照先: https://www.gartner.co.jp/ja/newsroom/press-releases/pr-20230914
4. (2018). D X レポート ～IT システム「2025 年の崖」の克服と DX の本格的な展開～. 参照先: https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation/pdf/20180907_01.pdf

1. はじめに

このホワイトペーパーでは、シスコがビジネスや環境の変化に合わせて動的にインフラを拡張・運用できる「やわらかいインフラストラクチャ」（以下、やわらかいインフラ）について、必要とされる機能や特徴、利用方法などについて解説します。やわらかいインフラとは、シスコのカスタマーエクスペリエンス部門（CX）のエンジニアが社内で使用してきた用語で、クラウド時代の DX プラットフォームを意味しており、ネットワーク業界のみならず IT 全体における将来の課題に備えリスクに対応可能な概念を表現しています。

本ホワイトペーパーでは、通信事業者を対象に技術部門の責任者の方や、ネットワーク運用に携わる方々に向けて、やわらかいインフラにおける運用がどのような課題によって必要とされ、今後どのような運用の高度化を行っていくと良いのかを様々な視点から考察しています。本ホワイトペーパーを通じて、やわらかいインフラについてより深く理解し、やわらかいインフラを導入することで得られるメリットや効果について、共通のイメージを持っていただければ幸いです。

2. 通信事業者の運用課題

現在の状況から見た 2030 年以降の要件

運用は、通信事業者にとっては単なるバックエンド業務ではありません。これはサービスを提供し、顧客との接点を持つ、事業の心臓部とも言える領域です。運用は利益を生み出し、エンドユーザーとの絆を強化し、企業のブランドを形成します。ところが近年、通信事業者の運用は、複雑化と低廉化によって、労働に頼った品質管理と過度なコスト削減の要求に挟まれ、身動きできない状態に落ちいってしまう傾向があります。今後、通信事業者は、より効率的で、顧客に対してより価値を提供できる方法を見つけていく必要があります。

労働人口の確保

日本の労働人口は、今後も厳しい状況が予想されますが、見方を変えれば通信事業者にとって、人材の質を高め、より生産的な運用へと変革を推進する絶好の機会ともいえます。運用部門における人材を確保し、定着させるためには、魅力的なキャリアパスの提供が必要です。また、より少ない人数で高品質なサービスを維持するための技術的なイノベーションにも目を向けていくことが大切です(*図 1*)。

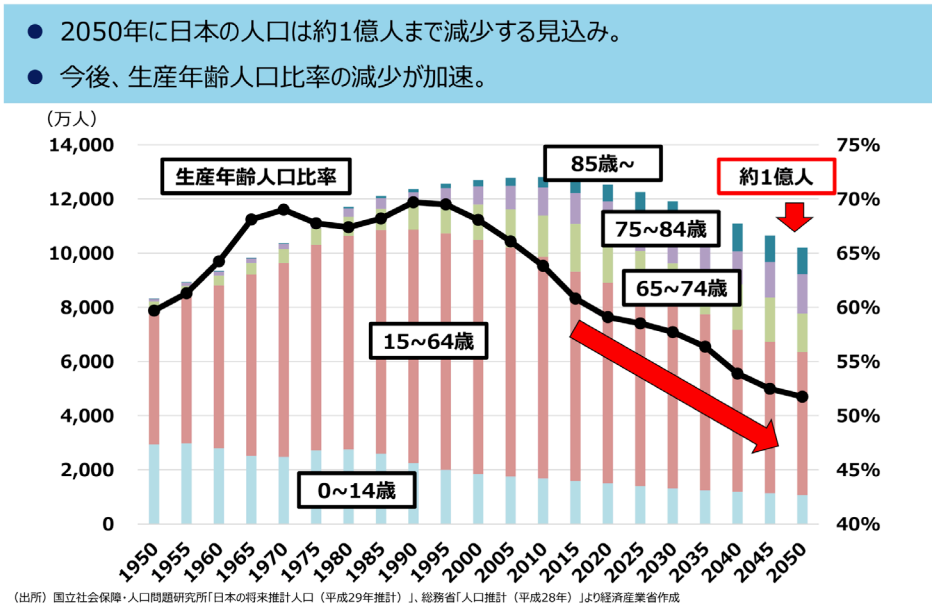


図 1：人口統計 [1]

新たな要求と競争

通信の重要性は今後も増加していきます。サービスの料金や品質は社会から透明性を要求され、障害発生時にはよりタイムリーで正確な報告を求められます。正確な状況をいち早く周知することが当然となり、消費者はそれを基に事業者を比較するでしょう。今、品質と価格に加えて、新たに透明性という競争が生まれています。

技術者の変化する価値観

今の技術者たちには、特定のネットワーク内での経験だけでなく、ジョブ型の雇用に適応する多様なプロフェッショナルスキルを身につけ、自らのキャリアを能動的に築いていくことが求められています。この変化に対応するためには、職場で技術者が成長しやすい環境を提供することによって、優秀な人材を引きつけ保持することが重要になります。

3. 通信事業者における安全性と信頼性

安全・信頼性は通信事業者の生命線

電気通信サービスには、高い安全性と信頼性を確保することが求められています。安全性と信頼性とは、ネットワークの高稼働率の維持、重大な事故が発生しないような安定した通信サービスの提供、および通信の不正使用を防止することを意味します。通信事業者にとって、安全性と信頼性は、社会的な責任と収益性という 2 つの観点から、企業価値に大きく影響を及ぼす要素となっています。

社会的な責任の面において、通信インフラは、日常生活やビジネス、さらには災害時の緊急通報や伝言板サービスなど、現代社会の基盤として不可欠です。このため、社会に対する責任はとても重大なものであり、責任を果たすことは企業価値の向上に直結しています。また一方で、責任を果たせない場合には、総務省報告や行政指導といった説明責任や是正責任が発生します (*図 2*)。

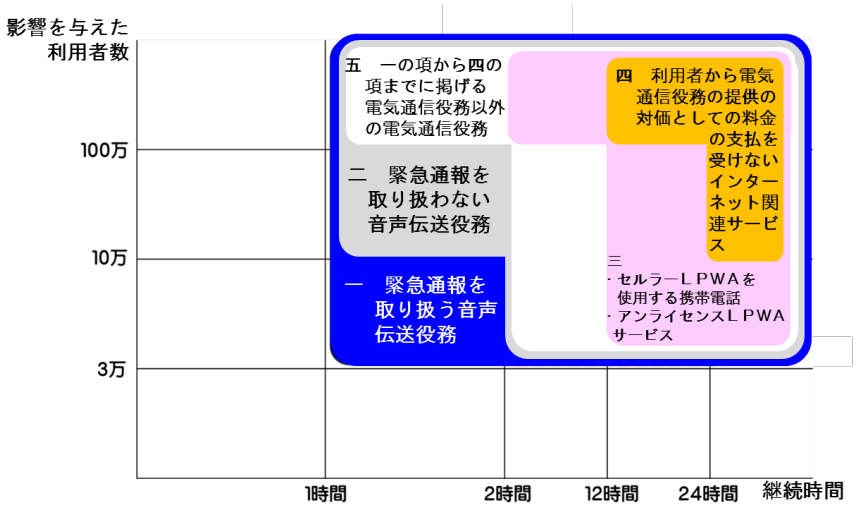


図 2 : 重大事故の総務省報告基準 [2]

収益性の面では、安全性と信頼性が顧客に選ばれる最も重要な理由の 1 つであることから、顧客が競合他社に流出するのを防ぐための大切な要素となっており、収入の増加にも繋がります。加えて、通信障害を減少させることは、障害復旧や事後対応にかかる運用コストの削減に加えて、重大な障害発生時の顧客への補償にかかる通信料などのコスト削減にもつながります。

障害前提の運用

安全性と信頼性を確保するためには、障害が発生しないように予防することも重要ですが、障害の発生を完全に防ぐことは不可能であり、障害が発生したときの対応を前提にした運用が非常に重要です。

障害を前提にした運用では、サービスに影響が出ないようなインフラ設計、信頼性の向上、そして障害が発生した後に迅速に復旧できる体制を整えることが大切です。

信頼性を高めるためには、制御カード、回線、地域レベルでの冗長性を確保し、障害時にはこれらを切り替えてサービスを継続できるようにする必要があります。しかし、この切り替えを確実に行うことが課題となります。多重障害を考慮に入れると、障害パターンは無数に存在し、設計や検証が非常に困難です。また、不具合や故障が原因で切り替えが行われない可能性もあります。

障害の復旧には、障害の検知、切り分け、復旧対応の 3 つのステップが必要で、迅速な復旧にはこれらのステップを素早く実行できることが求められます。しかし、マニュアルによる障害対応では、機器からのアラームがなければ障害を検知できない、切り分けが運用者の経験や知識に依存している、機器に CLI でログインして復旧作業を行う必要があるなど、運用者の対応に依存しており、結果として不確実かつ遅い対応になりがちです。これらの問題を改善するためには、システムを用いた自動化を積極的に導入していくことが必須となります(*図 3*)。

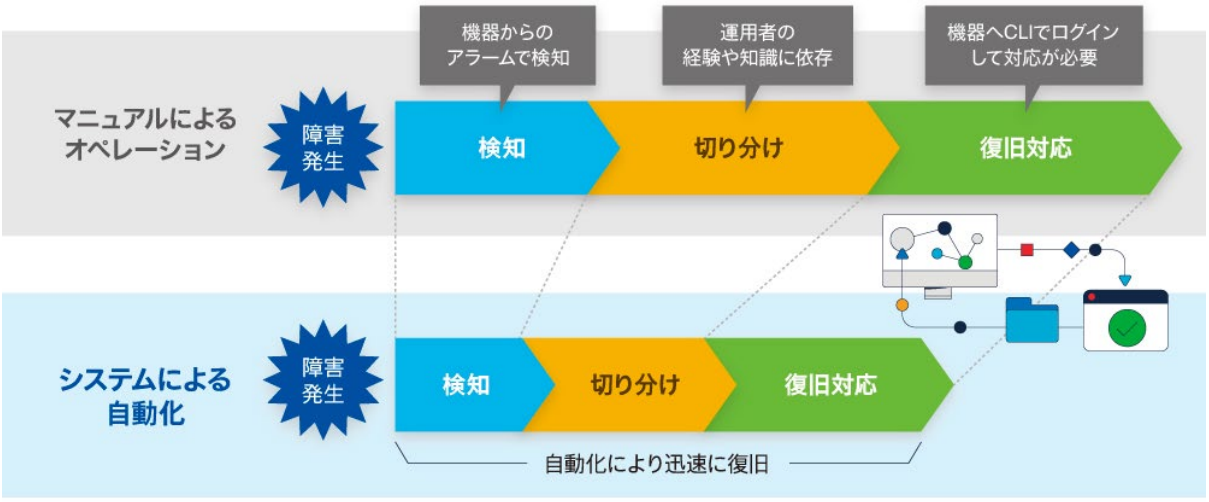


図 3：障害対応のステップ

報告・透明性

障害が発生した際には、顧客や行政機関をはじめとする関係する全ての関係者へ、障害の状況を報告する責務が生じます。

2023 年 3 月に総務省より更改されたガイドラインにて原則 30 分以内に ホームページで初報公表することが明記されるなど、社会的にも重要な課題となっています。

この報告は迅速かつ正確に行うことが求められます。SLA に基づいて、顧客にはホームページでの公開や電話による報告、メールによる自動通知などを通じて情報を伝達します。また、緊急呼に対しては、警察、消防および海上保安庁など緊急通報受理機関への連絡も実施します。このように、人の手によって多くの関係者への報告が行われることになり、多大な時間と労力を要します。加えて、報告する内容は影響を受けるサービスやエリア、復旧の見込み、影響時間、対応状況、根本原因といった複雑かつ多岐にわたる情報を含んでおり、これらを迅速かつ正確に把握して発信することには一層の困難を伴います。さらに、報告を行う担当者は障害対応を行う技術者ではないため、技術者から障害情報を聞き出し、それを理解する過程は、1 分 1 秒を争う状況下において報告者と技術者の両者にとって大きな負担となります。これらの理由から、障害報告のプロセスを改善する必要があると考えられます。

セキュリティ対策

信頼性の高い電気通信サービスを提供するためには、セキュリティ対策が極めて重要です。通信事業者が直面する最大のセキュリティリスクとして、情報の漏洩があります。これまでにも、多くの通信事業者が顧客情報の漏洩により、大きな問題に直面してきました。また通信に関する情報としては、通信内容の漏洩が「通信の秘密」の侵害につながりますし、ネットワーク構成に関する情報の漏洩はサイバー攻撃を受けるリスクを高めます。

情報漏洩以外にも、サイバー攻撃による電気通信サービスの可用性の低下も深刻なセキュリティリスクです。DDoS 攻撃による機器や回線の圧迫、脆弱性を狙った攻撃、作業用 PC のマルウェア感染やソーシャルエンジニアリングによる不正侵入など、様々な脅威に対し、通信事業者は適切な対策を講じて事前に防止する必要があります。さらに、外部からの攻撃だけでなく、契約社員や業務委託先を含む内部関係者による攻撃や意図的な情報漏洩の可能性にも注意を払い、これらを防ぐ措置を講じることも求められます。

未知への耐性

通信事業者は、多種多様な機器を長期間にわたって運用しています。そのため、検証結果や過去の事例とは全く異なる未知の事象が発生する可能性があります。このような事象が発生した場合でも、安定した通信サービスの提供が求められます。未知の事象に対応するためには、多角的なアプローチでの切り分けや詳細な調査を行い、試行錯誤を重ねながら解決策を見つけ出すことが必要です。このプロセスは時間を要し、ネットワークを正常な状態に戻すまでの時間短縮が課題となります。

多くの場合、未知の事象への対応は、高いスキルを持つ熟練の運用者が必要になります。 また、時にはベンダーへのエスカレーションが伴うこともあり、解決策の発見が困難であることが少なくありません。熟練運用者によって発見された対処方法も、それを組織のナレッジとして蓄積し、未知を既知に変えるためには、システム的に適切な管理を行うことが重要です。個人の

記憶に頼る状態では、組織全体としてのナレッジの蓄積がなされず、同様の事象が再発した際に同じ苦労を繰り返すことになるかもしれません。

運用の役割

運用部門は、しばしば「最後の砦」と呼ばれます。これは運用が業務の最終工程に位置し、サービス品質や顧客からの評価に直結する重要な業務だからです。質の高い運用業務は、企業価値の向上に大きく寄与します。加えて、運用部門は商用機器を長期間にわたって扱うことから、実網に関する理解度が最も高い部門と言えます。運用部門が実際のネットワーク運用から得た知見を設計や開発業務にフィードバックしたり、設計・開発と運用が一体となったチームを形成することで、品質改善を促進することができ、より大きな価値を生み出すことが期待できます。運用業務の改善は、ネットワークを最も長く取り扱い続ける役割を担っているため、安全性や信頼性の向上に大きな効果をもたらすことになるのです。真に顧客や社会の利益を考慮し社会責任を果たす企業は、運用に対する継続的な投資を怠りません。高品質な運用業務は、顧客満足度の向上だけでなく、社会全体への信頼性の保証にもつながります。

4. 人材や組織の課題

運用の魅力

昨今の通信インフラは我々の日常生活やビジネスを支える基盤であり、その運用業務は企業や組織の中でも顧客やサービスに近い立ち位置で、エンジニアが各々の技術スキルを駆使しながら日常的な維持管理から大規模障害まで様々な問題や課題を継続的に解決し続けています。

そして、安定した品質でのサービス提供を支え、顧客からの評価などに直結する社会的責任を担う、非常にチャレンジングな業務といえます。そのためエンジニアは絶えず新技術を習得し、組織とともに成長していくことが期待されます。しかし、現実の運用監視現場ではそのようになっていません、何故でしょうか？

運用監視組織の課題とエンジニアの市場価値

多くの場合、通信事業者の運用監視現場では、ある程度の人材を確保できることを前提として、簡単な繰り返し作業に落とし込み、それらを担当者が淡々と行う組織や業務設計となっています。

そのため、あらかじめ作成されたマニュアルに従った作業を繰り返し行うことが多く、逆にマニュアルから外れた機器オペレーションや、プログラミングを活用した効率化などの機会は少なく、業務を通じてキャリアアップしづらい状況があります(*図 4*)。

これにより、現状の運用監視業務は、エンジニアにとって成長しづらくいわゆる非先端 IT 従事者と見なされることさえもあり、総じて市場価値が低い傾向にもあります。また多くの通信事業者運用監視現場では 24 時間 365 日体制をとっていて、深夜勤務を含む輪番などワークライフバランスの負担となることもあるでしょう。

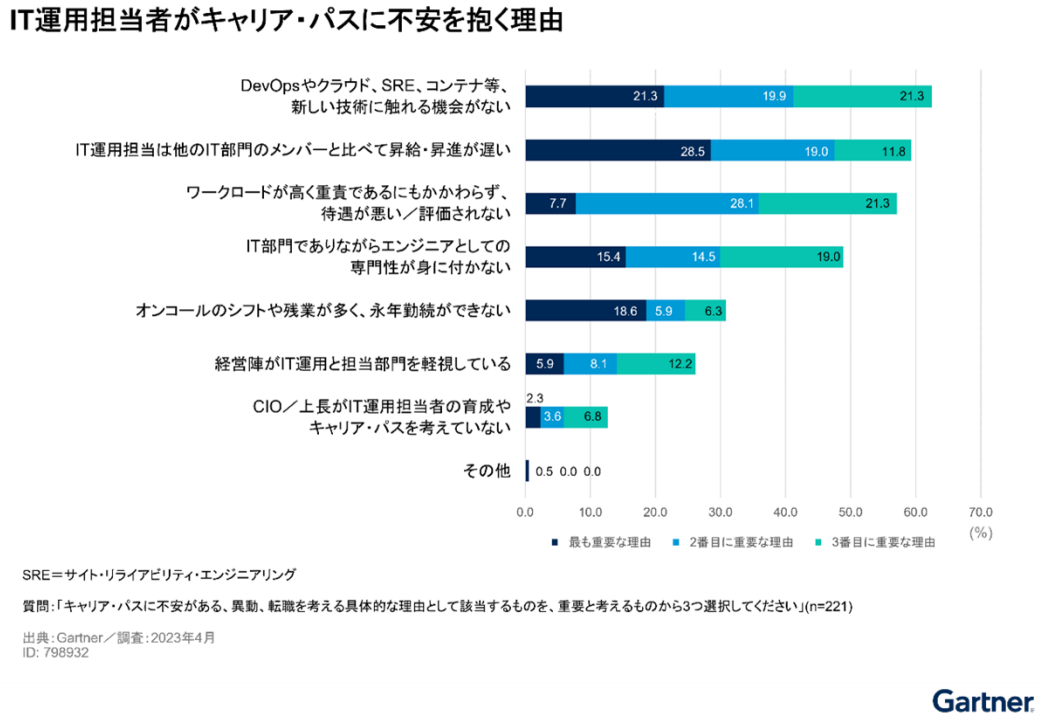


図 4：運用担当者がキャリア・パスに不安を抱く理由 [3]

しかしながら本来、運用監視現場はエンジニアの成長によって顧客に新たな価値を提供し、自社サービスの価値向上など良い影響を及ぼす可能性がある、魅力にあふれる場所であるべきです。

そのためには通信事業者が今後競争力のあるサービスを提供し、企業やサービスの価値を向上するために組織や人材の変革を行う必要があると考えます。

過度な複雑性

昨今、ユーザーニーズに対応するためのトラフィックの増加やサービス自体の多様化、モバイルの発展や IoT の普及に加え、デバイスの多様化やクラウドや仮想化の一般化など、ネットワークの構成要素に様々な要因が絡み合い、複雑化が進んでいます。一方でネットワーク自体が進化あるいは複雑化する中で運用手法は従来通りの手法やポリシーに基づくものを継続しており、これが日々運用現場の頭を悩ませています。このような運用観点における複雑性の課題を以下に示します。

運用管理の複雑性

従来の ネットワーク運用では SNMP や Syslog などデバイスベースの監視により障害検知を行っています。昨今の通信事業者のような大規模かつ仮想化技術によりスライスされたネットワークにおいては従来ベースの監視手法のみで障害を検知することが困難となっており、かつ通信サービスの品質に対する顧客からの要求や期待値が上がるなかで、サービス品質の劣化を検知できずクレームなどの問題へと発展するケースも少なくはありません。

従来のデバイスベースのみの監視からネットワークアーキテクチャに即した監視方法へ移行し、運用上必要な情報を全て取得し、疎通性のみならずユーザー体験など含めたサービス品質の向上を実現する必要があります。

変更管理の複雑性

ネットワーク運用の現場では商用機器の実コンフィグレーションと構成管理 DB 上のデータに差分が生じることがあります。これはコンフィグサーバ等にて厳密な変更履歴管理をしておらず、かつ人手による構成管理 DB の変更におけるオペレーションミスなどに起因し、コンフィグレーションを「いつ」「だれが」「なにを」変えたのか変更履歴を厳密に追跡することが困難という現状があるからです。このことが障害発生時の復旧作業において誤ったオペレーションや対応時間の長期化など影響を及ぼす可能性があります。

ネットワーク機器のコンフィグレーションや構成管理 DB は、常に信頼できる情報源であるべきです。セキュリティ的な観点も含め、ネットワークの変更管理を厳密に行うことは非常に重要であり、そのための仕組みの検討や自動化による解決が有効と考えます。

オペレーションの複雑性

昨今 Software Defined Networking (SDN)の普及、Open Source Software (OSS)やその他ベンダーソリューションの発展などにより、通信事業者の運用現場においても何らかの自動化に関する取り組みが行われ、業務効率化の成果をあげています。

しかしながら業務の全てを自動化できているケースは少なく、人がいることが前提のオペレーションとなっていることが多い状況です。例えばネットワーク運用の障害対応において、ログ収集やトラフィック迂回措置のためのコンフィグレーション投入などは自動的に行うが、障害箇所や要因を特定することについては、まだまだエンジニアの経験や判断に依存しています。

昨今 AI 技術の発展に伴い、ネットワーク運用へ AI 技術を適用することで、従来自動化が困難であり人による判断が必要であったオペレーションを自動化するための検討が活発になっています。通信事業者においてもオペレーションの簡素化やさらなる自動化を実現するための検討が必要となっています。

5. ネットワーク運用におけるレガシー装置の問題とその影響

近年の技術は急速に進化しています。技術が進化することによって、ネットワークを活用したサービスを使う機会も増大し、それによってネットワークに求められる要求も変化しています。それらの要求に対応するため、新しい技術や装置を導入することが一般的に行われていますが、レガシー装置が残ったまま運用されているというケースも珍しくありません(*図 5*)。

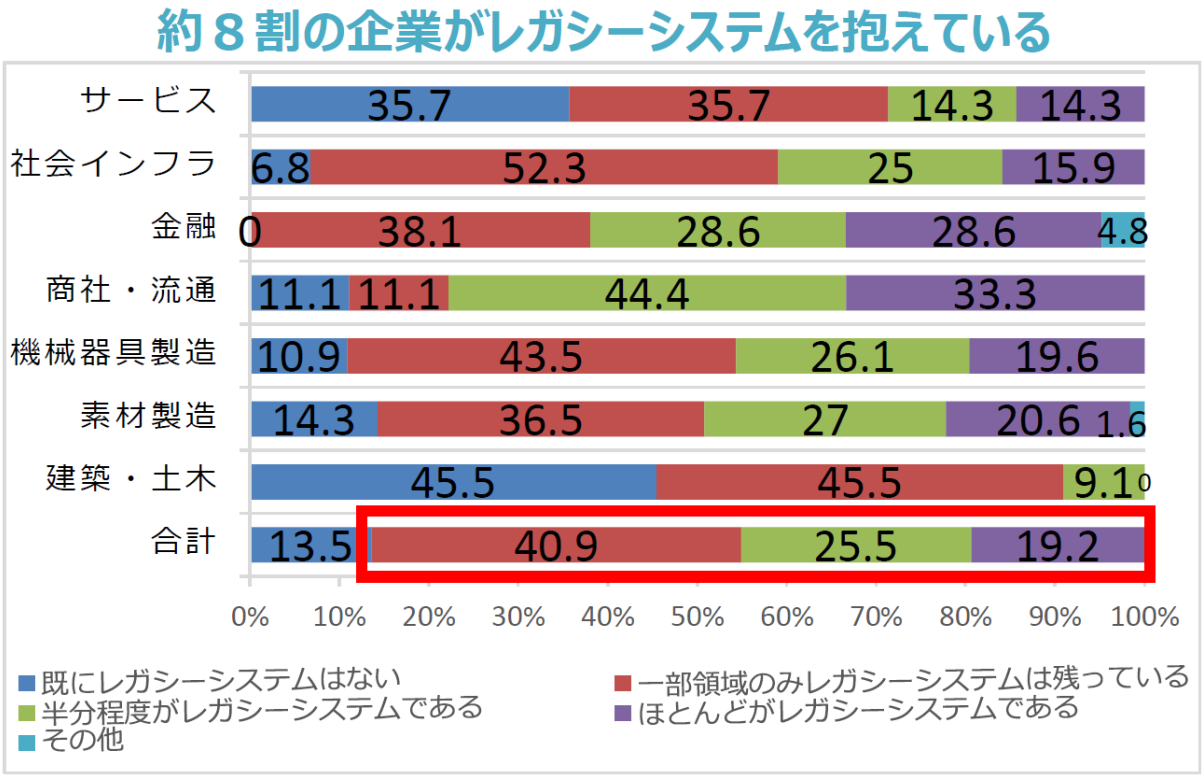


図 5：レガシー装置を抱えている企業の割合 [4]

そのような状況下において抱えられる問題を以下に示します。

新しい技術やアプリケーションとの互換性

新しいプロトコルやデータフォーマットをサポートしていない等の理由で、最新のシステムやソフトウェアとの連携に問題が発生する可能性があります。この不一致は、統合性の問題を引き起こし、全体的な業務効率の低下につながることになります。

拡張性

新しい技術や増加するトラフィックの要求に応じてスケールアップする能力が限られてしまうと、ビジネスの成長に合わせてネットワークを適切に拡張することができなくなる可能性があり、将来的なネットワークの拡張やアップグレード計画に影響を与えます。

パフォーマンス

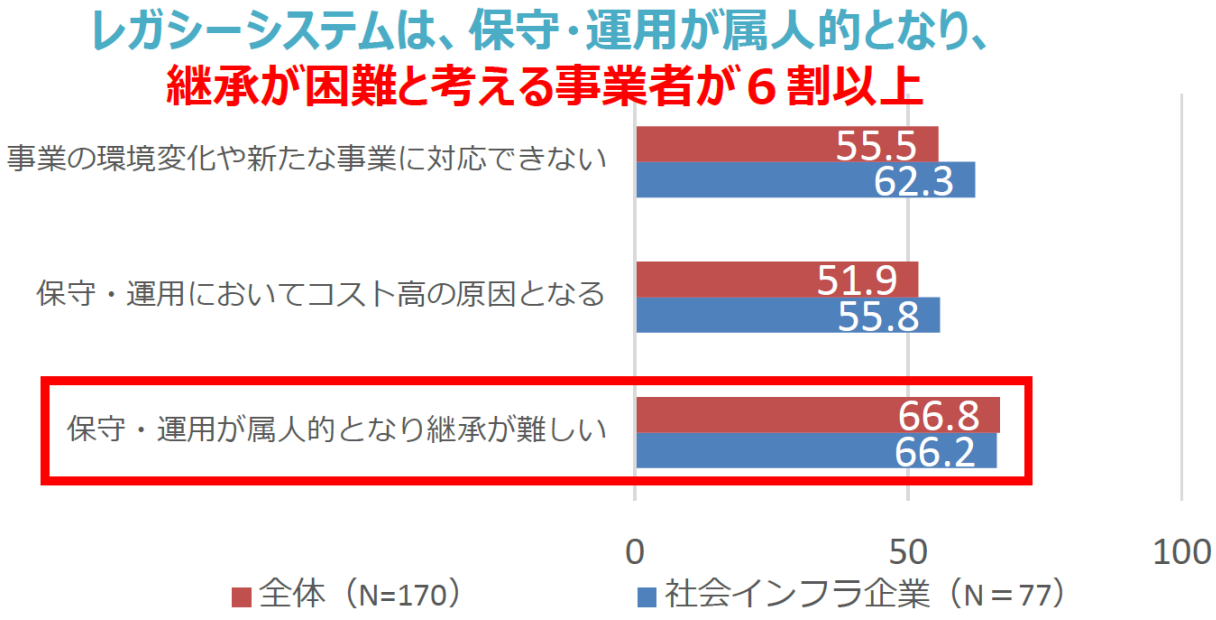
要求に応じたスループット、遅延、ジッターなどのパフォーマンスを提供できなければ、サービスプロバイダの成長や新しいサービスの導入が妨げられることになります。また、ネットワークの遅延やダウンタイムが発生し、ユーザー体験に悪影響を及ぼす可能性があります。

コンプライアンス遵守

多くの業界では、データ保護やネットワークセキュリティに関する法律や規制が定められています。レガシー装置がこれらの基準に準拠していない場合、コンプライアンス違反のリスクに直面し、罰金や信頼性の損失などの重大な結果を招くことになります。

技術者の確保

レガシー装置を維持するためには、古い技術に精通した技術者が必要です。しかし、新しい技術に焦点を当てた教育が主流となっているため、古い技術を理解し、管理できる技術者を確保することが困難になっています。技術者の確保が難しくなると、レガシー装置の適切な管理やトラブルシューティングができなくなり、最終的には運用の効率性や信頼性に影響を与えることになります (*図 6*)。



（出典）「情報システム開発課題アンケート結果」（平成30年2月、経産省委託）を基に作成

図 6：技術者の継承問題 [4]

運用コストの増加

レガシー装置は新しい技術に比べて、パフォーマンスが悪く、エネルギー消費が高い傾向があります。また、古いハードウェアやソフトウェアのメンテナンスには経験や特別な訓練を受けた技術者が必要です。 さらに、旧型の部品が不足していることで、修理や取り替えが高額になったり、入手そのものが困難になっているものもあります。

古い装置の持続的な使用に伴う別の課題として、現行装置に搭載されている新機能の活用不足が挙げられます。これは、最新技術を取り入れずに発生する、必要以上の対処措置や、それに伴う機会損失を引き起こす潜在的な要因となります。これらの要因が運用コストの増加につながります(*図 7*)。

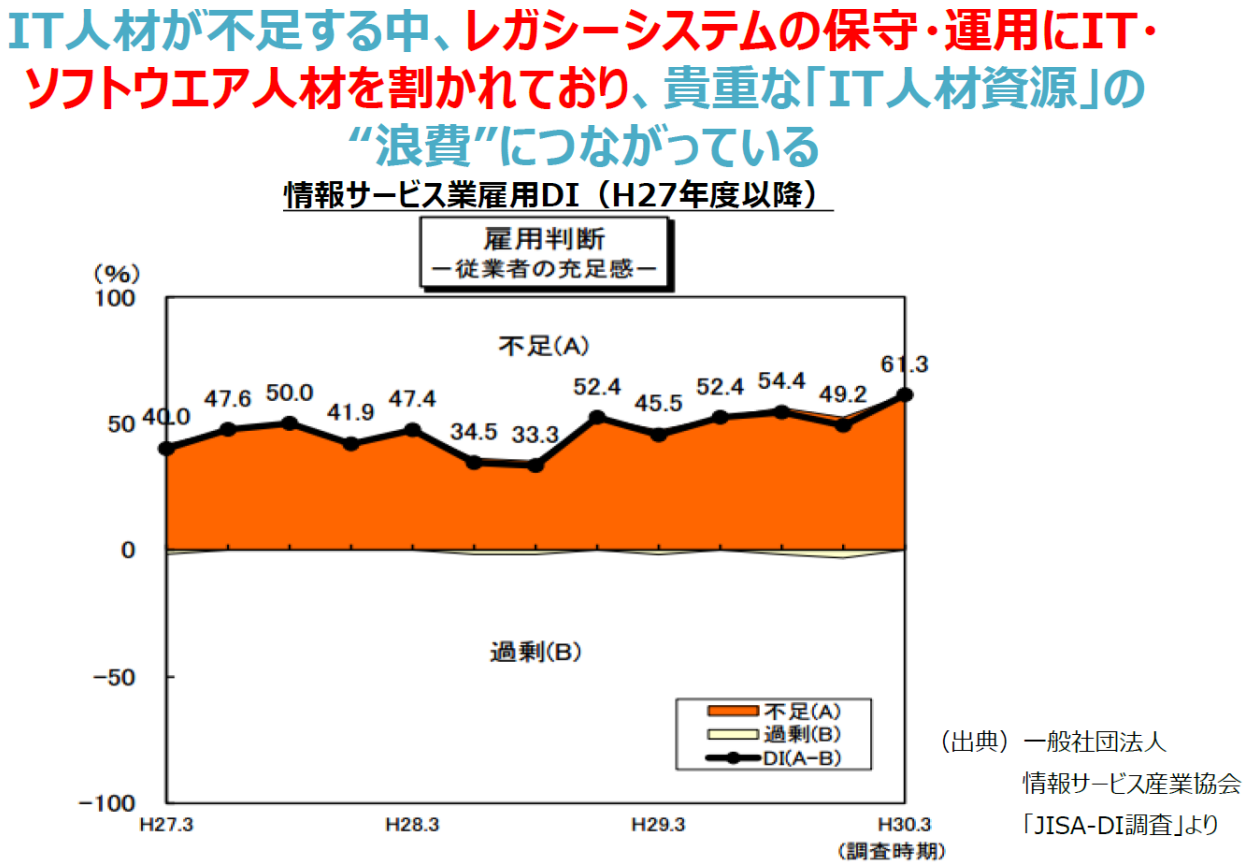


図 7：人材の充足感 [4]

装置のサポート

メーカーによるレガシー装置のサポートは、製品ライフサイクルに合わせて徐々に終了していきます。装置のサポートには大きく分けてハードウェアとソフトウェアがありますが、ハードウェアのサポートが終了する時期には装置の故障率が上がっていることもあり、装置が故障しても対処できなくなるというリスクが発生します。また、ソフトウェアのサポートが終了すると運用に影響を与えるような不具合が発生しても修正不能となり、セキュリティパッチやソフ

トウェアの更新も提供されなくなります。セキュリティパッチの提供が終了したレガシー装置は、新たな脅威に対して脆弱になり、ネットワーク全体のセキュリティレベルが損なわれ、データ漏洩やサービス妨害攻撃などのリスクが増大します。その結果、提供するサービス品質の低下に繋がります。

6. 運用もやわらかく

設備や機器の柔軟性が高度化していく中で、それらを扱い収益を確保していく運用の組織もまた柔軟性が必要となってきています。より少ない人員で、精鋭といえる組織が、より高度で安定したサービスを顧客に届けるためにはどうしたらよいでしょうか。

通信事業者サービスに対して今よりさらに社会的責任が問われる 2030 年において、サービス品質の指標や透明性は常に公表し誰でも参照できる状態が求められます。その上、いつでも新たな社会的な価値を担保するためには、単一の指標では不十分です。あらゆるデータを常に取得し、柔軟に加工し、社会に公表しておく必要があります。これは果たすべき責任であると同時に、トラブル発生時における緊急で綱渡り的なレポート業務からの解放にもなりえるでしょう。社会と運用がつねに同一の品質指標をモニターし、経営と一体化したサービス運用を行っていくことが大切です(*図 8*)。

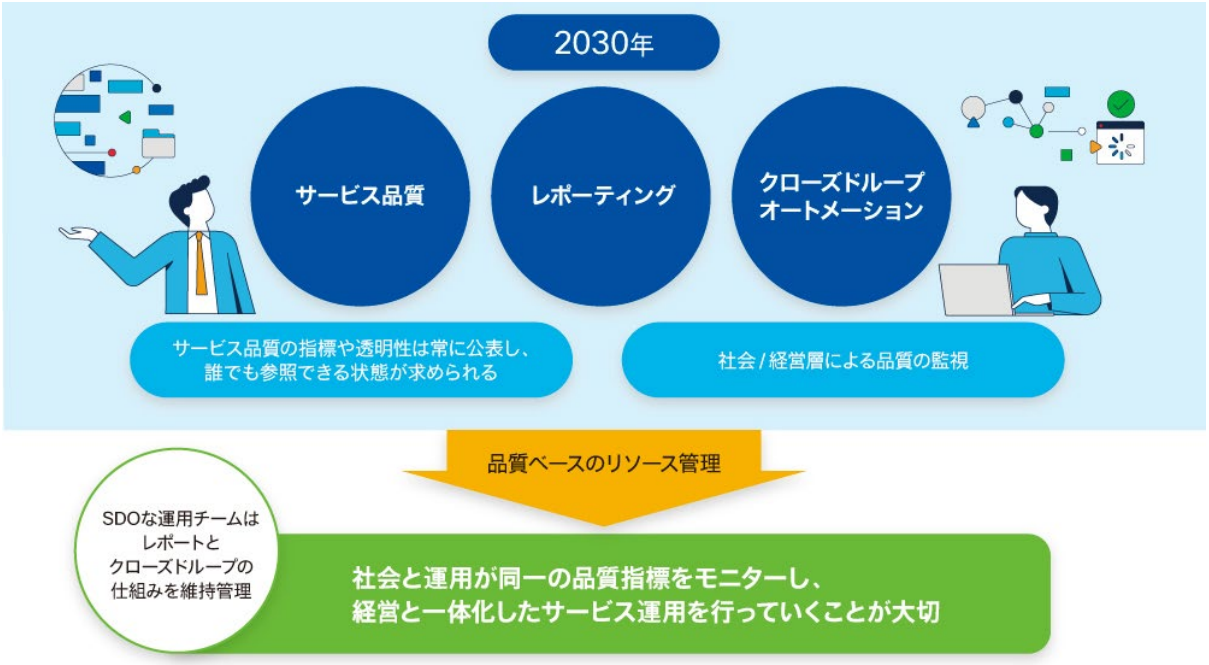


図 8 : 品質の透明化

サービスの品質指標を達成していくことは運用チームの責務ではありますが、24 時間 365 日にわたって人が監視していることが必要かどうかは再考する必要があります。なぜならば第一に、品質指標は人間による監視とアクションで担保されるべきではないからです。複雑化する機器・拡大するサービスに対して限られた、そして貴重な人間による監視はスケールできません。サービス開通や CI/CD は開発・導入時から自動化を計画されているものの、運用については、巨大化していく規模のなかで、新たに見つかる問題の対処と既知の問題の対処を並行していかなければなりません。そのためには運用開発チームとして AI やクローズドループを活用し、人海戦術ではない形でサービスの安定稼働を達成していく SDO: Software Defined Operation（ソ

フトウェア定義された運用）を用いて、運用チームの能力をスケールさせ収益の維持を可能とする必要があります。

第二に 24 時間 365 日、責任を持った組織が監視を行うことは、本来のサービスを安定稼働させることとは別のプレミアムな価値を生みます。ビル監視を例にとると、設備維持と 24 時間 365 日の警備はそれぞれ別の専門チームが担っています。24 時間 365 日監視チームは、社内の全サービスのみならず、顧客のスマートホームセキュリティ、他社、あるいは時差を考慮した他国の監視などもビジネス化し価値を生むプロフィットセンターにもなれる可能性も考えられます。

組織の構成と役割

今よりさらに不確実性の高まった 2030 年という時代において、組織もやわらかくなる必要があると考えます。やわらかい組織とはどのような組織でしょう。ここでひとつの考え方を示します。まず、必要な組織構成を、コアとサテライトの 2 つのグループに分けて考えてみましょう。

コアとなるチームは自社において長期にわたって人とスキルを育てていく組織です。サテライトとなるチームはその時点で必要であるが、長期的には未知数な要素があるチームです。あるいはベンダーや業界の内外からアウトソースしやすい部分を一旦サテライトと区分けすることもできます。

例えば、前述の”運用もやわらかく”で示されたように、データレイクや可視化を開発するチームはコアチームに所属させてみましょう。 このチームは通信事業者のビジネスを可視化し、社会や顧客の変化に応じて柔軟に監視項目を判断することで透明性を常に提供し続けるチームです。同様に戦略や教育を担当するチームもコアチームに所属させます(*図 9*)。

一方でサテライトとなるチームは、ベンダー別の設定や運用、インベントリの管理といった役割が良い例となります。これらはベンダーへのアウトソースがしやすいですし、競合や他国の同一ベンダーを管理するようにスピンアウトさせやすいチームともいえます。また、現在でいう大規模言語モデル（LLM）や突然立ち上がった技術を習得させるチームもサテライトというカテゴリの中では柔軟に立ち上げ可能です。 コア、サテライトどちらに所属するチームも、定期的にどちらが担うべきかを検討し、必要に応じて移動させることも大切です。

たとえば LLM はコアチームに移るかもしれませんし、可視化開発はコアのまま、データレイク管理はサテライトに移すべきかもしれません。 また利益がだせるようになった 24 時間 365 日監視チームはコアに移す、等の検討が考えられます。

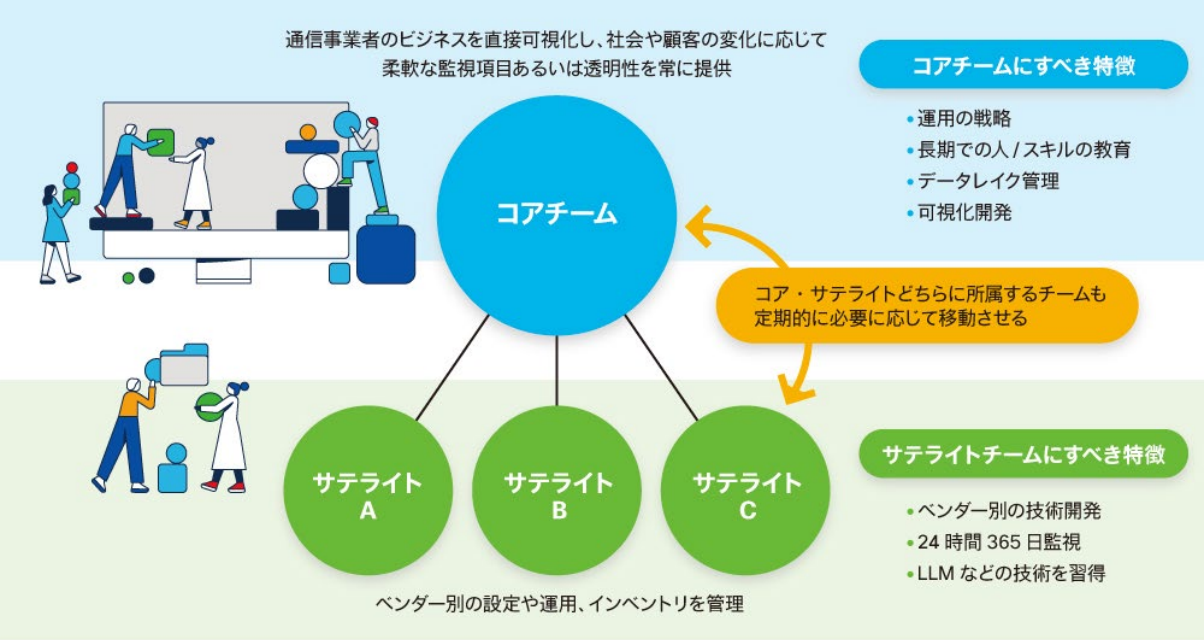


図 9：コアとサテライトの構成

可視化開発をコアチームにおく理由

ベンダーや SIer に依頼することの多い可視化開発をコアチームにおく理由は何でしょうか？実は監視内容は特にサービス立ち上げにおいて、項目の重要度が変化します。想定外の事象や障害を通して対処していくことになるため、外部で開発を行なっていると可視内容の変化に迅速に対応できず、そのまま手動や人員をかけた体制になりがちです。人海戦術は 2030 年には致命的な問題を引き起こします。このことはスキルセットの項目で説明します。

スキルセット

このような運用や組織の柔軟性を高めていくなかで、個々人はどのようにスキルやキャリアを構築していけば良いのでしょうか。 まず、今後のスキルセットの組み立てには、個人の努力はもちろんのこと、組織における役割が大きく影響するようになると考えられます。なぜなら、人口が今よりずっと減っている 2030 年には、組織は「入社してもらう」「必要なスキルを更新してもらう」という考えが大切になるからです。組織のスキルセットポートフォリオを計画し維持することは、組織としてのサービス品質だけでなく、個々人のワークライフバランスや永年雇用に不可欠です。

それでは、2030 年に必要なスキルセットのポートフォリオはどのようなものになるのでしょうか。予測することは難しいですが確実に言えることはあります。 それは現在よりさらに広範囲なスキルセットが運用のエンジニアに求められること、そして、身につけたスキルセットの陳腐化はより早く進むということです。それでは、未知であり、そして有効な寿命の短くなったスキルセットをどのように選択し揃えていくことが必要となっていくのでしょうか。

そこでは、前章で述べたコアグループに置いた戦略・教育チームが有効に機能すると考えます。このチームはエンジニアの稼働について「効率化」にかかっている時間と「障害や問題への対処」にかかっている時間の比率を常にモニターすることが重要です。Google が提案した サイト リライアビリティ エンジニアリング (SRE)に近い考え方ですが、「対処」「手作業」の比率が高まると計画的な業務や学習の障害となり、これが人口減少社会ではサービスの運営に致命的な問題を作り出します。つまり「新たな技術を習得できない」「利益を生まない問題対処に忙殺される」「人が定着しない」と言った問題です。この比率の安定化は運用チームの重要なゴールの 1 つとなるでしょう。

上記を踏まえたうえで、具体的なスキルセットはどのように選定すれば良いでしょうか。ここではスキルセットを必須グループと選択グループに分けて考えます。

組織として利益を生んでいるスキルセット、自動化を行うスキルセットは必須グループに属します。 問題に対処する際に必要なスキルセットは選択グループに属します。組織のコア＆サテライトとおなじように、全てのスキルセットは定期的にレビューされる必要があり、２つのグループを移動可能です。つまり「選択型」であったものが利益を生むようになった場合「必須型」に移動することもできますし、その逆もあり得るということです。

現時点の 2024 年を例にすると、サービス SLA の選定や自動化・可視化を行うためのソフトウェア開発のスキルは必須スキルです。昨今の LLM は選択型に入り将来的に必須スキルになると考えられます。 また、たとえ重要でも外部から調達しやすいスキルセットは選択型に入るかもしれません。

機能としての組織や必須・選択型に分けられるスキルセットのモデルを適切に改善・維持していくことは、売り物であるサービス維持と同じくらい重要なことです。未来は予測できませんが、未知であることだけは確実であり、未知の課題に対応するためには多様性を許容する組織と多様なスキルセットが有効です。繰り返しになりますが、もっとも貴重であるべき私たち労働者が「作業」に忙殺されることはよくありません。

そのためにも組織レベルで「開発」と「対処」の稼働比率を確認・維持していくことが、とても重要になります。

御社の運用状況はどうでしょう？【簡易アセスメント】

第 1 章から第 5 章では社会全般および通信事業者において顕著化されている課題を、第 6 章では運用のあるべき姿について説明しました。あるべき姿を目指す際には「どこから変革を起こすべきか、費用対効果の高いアプローチはあるか」を定める必要があり、そのためには現状を把握する必要があります。そこで、御社での運用課題を明確化するに、運用課題に対して問い掛けを行うための簡易的なアセスメントを作成しました。ぜひ、ご活用ください。

【質問 1】人材の確保・育成方針が体系的に整理されていますか？

1. 職務に必要なスキルセットや経験が具体的に文書化されている
2. 新メンバーのオンボード手順が文書化されている
3. レガシーな機器や仕組みからの移行が予定されている
4. 組織のリスキリングが明文化されてトレーニング等も用意されている
5. 労働市場から調達できるスキルで運用業務の遂行・改善が可能

【質問 2】サービス品質の基準が明確であり、それをもとにサービスの効率化がされていますか？

1. 提供するサービス品質目標が社内的に定義されている。
2. サービス品質が常時可視化され社内でいつでも参照できる。
3. 品質目標の定義見直しと常時可視化のアップデートが可能な体制が整っている
4. 品質目標の達成度合いを元に人員の配置がスケールできる
5. サービス品質が常時可視化、社外に公開され、見直しも定期的に行われている

【質問 3】設計で想定している障害レベルが明確であり、対応プランはありますか？

1. ケーブル故障やトランシーバー故障といったリンク障害を想定し、対応プランがある
2. CPU、ディスク、搭載カード故障といった機器障害を想定し、対応プランがある
3. 明確なハードウェアの故障を伴わない機器の処理異常を想定し、障害時にサービス影響がない
4. 複数リンクの同時障害を想定しているが、手動でのサービス復旧が必要である
5. 複数リンクの同時障害を想定し、対応プランがある

【質問 4】検証効率化・自動化は十分にされていますか？

1. 全く自動化ができていない
2. log 取得まで自動化ができている
3. 試験の判定まで自動化ができている
4. 自動化がシステム化され、一つの検証で作成した自動化項目が他の検証にも移植ができる
5. 上記に加え、検証環境構築の自動化ができている

【質問 5】障害発生時に外部向けに迅速な報告ができますか？

1. 手動で障害状況を把握し、手動で報告を行う
2. システムで障害を検知すると、お客様へ自動的に障害が発生したことが通知される
3. 運用者にシステムの稼働状況が可視化されている
4. AI により報告内容が自動作成できる
5. システムの稼働状況が常時外部に公開されている

【質問 6】障害対応で得られたナレッジがアセット化されていますか？
1. 過去事象のナレッジは各人の記憶の中にのみ存在する
2. ナレッジとして蓄積すべき障害が周知されている
3. ナレッジとして蓄積すべき障害が資料として保存されている
4. 障害対応者がデータベースに入力した対応内容を検索できるデータベースがある
5. 障害対応時には、AI により、自動的に適切な内容がナレッジデータベースから参照される

【質問 7】運用監視における業務が脱属人化されていますか？
1. 人がスキルや経験を活かして非定型的な対応を行う
2. マニュアルに従って決められたオペレーションを人が手動で実施する
3. ソフトウェアやスクリプトを使って既存のオペレーションの一部を効率化している
4. Infrastructure as Code（IaC）を活用し、手順書を廃した SRE 的運用が実現できている
5. AI/ML など先端技術を活用した異常検知やプロアクティブな予測分析からクローズドループオートメーションが実現されている

【質問 8】 レガシー装置の影響を最小化していますか？
1. サポート期間を過ぎている装置があり、メーカーからの HW、SW サポートを受けられない
2. サポート期間を過ぎている装置があるが、メーカーからの HW 及び SW サポートは受けている
3. 全てメーカーのサポート期間内の装置だが、新しいサービスを提供する上で障壁となる
4. 全てメーカーのサポート期間内の装置だが、運用を高度化する上で障壁となる
5. 全てメーカーのサポート期間内の装置で、特に課題は無い

【質問 9】社会全般における変化していくネットワーク上を流れるデータのポリシーやネットワークセキュリティ規制に対応できる環境が準備できていますか？
1. データポリシーやネットワークセキュリティについて気にしていない
2. データポリシーやネットワークセキュリティについて気にしているが、取り扱いされるデータが識別されていない
3. 取り扱いされるデータを手動で識別し、人力で適切なポリシー・セキュリティを適用
4. 取り扱いされるデータを自動で識別しているが、人力で適切なポリシー・セキュリティを適用
5. 取り扱いされるデータを自動で識別し、自動で適切なポリシー・セキュリティを適用

【質問 10】 運用における変更管理基準が定められ、それに基づいて管理されていますか？

1. チーム単位でファイルベースの管理がされている
2. 組織単位でファイルベースの管理がされている
3. 組織単位で変更管理ツールベースの管理が手動でできている
4. 組織単位で変更管理ツールベースの管理が自動でできている
5. 組織単位で変更管理ツールベースの管理が自動でできており、信頼できる唯一の情報源とされている

上記のアセスメントにより、御社の運用はどこから変革を起こすべきか、費用対効果の高いアプローチはあるかをより明確に把握できると思います。やわらかい運用が追求する理想型としては、上記のすべての質問に対して 5 番が選択されることをめざしていくべきでしょう。これらを 1 つずつ実現することが運用高度化の実現、つまり社会的な責任を果たすと同時に価値を高める運用により近づけるためのマイルストーンになっていくはずです。

（※シスコシステムズでは、上記よりさらに広く、深くアセスメントを実施させていただく運用のアドバイザリーサービスをご提供しております。）

The bridge to possible

免責事項

IF THIS DOCUMENT IS PROVIDED AS A DELIVERABLE IN ACCORDANCE WITH THE CISCO TERMS AND CONDITIONS ASSOCIATED WITH A PURCHASED CISCO SERVICE (“TERMS”) THEN THIS DOCUMENT IS PRESENTED SUBJECT TO THOSE TERMS. IN ALL OTHER EVENTS, THIS DOCUMENT IS PROVIDED “AS-IS” WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA 07/24