マネージドサービスを実現するための システム開発と運用プロセスの標準化

Standardization of System Development Guidelines and Checklists for Each Phase of Development of Managed Services

雑賀　翼 SAIKA Tsubasa　村田　尚彦 MURATA Naohiko

社会インフラを支えるCPS（サイバーフィジカルシステム）には高い業務継続性が求められる。システム障害が生じないように運用するとともに，万一障害が生じても，即時にシステムを復旧して顧客の業務継続性を保証しつつ，その障害の根本原因を特定して対策を施す必要がある。

東芝デジタルソリューションズ（株）は，これらの要求を満たすマネージドサービスの実現に向けて，システムの障害対策の組み込み方や，システムの運用・保守に必要な設計手法などを記述したシステム開発ガイドライン及びチェックリストを開発した。これにより，継続的な改善が可能なマネージドサービスを提供できる。

Cyber-physical systems (CPS) for social infrastructure must provide a high level of business continuity management. The need has consequently arisen for managed services to secure the stable operation of systems while ensuring customers' business continuity through rapid recovery, identification of the main cause, and implementation of measures to prevent a recurrence in the event of a problem occurring in their systems.

As a managed service provider (MSP), Toshiba Digital Solutions Corporation has developed system development guidelines and checklists for use in each phase of development of managed services. These guidelines and checklists provide standardized methods including methods for incorporating countermeasures against problems into a system and methods for preparing the various documents necessary for operation and maintenance services, making it possible to offer CPS services capable of being continuously updated.

1. まえがき

東芝グループは，電力システムをはじめ公共・交通・放送などの社会インフラを支えるCPSを提供している。これらのシステムに障害が発生すると，社会的な混乱を引き起こすおそれがある。

そこで，システム障害の発生を低減するために，これまでも開発プロセスや設計テンプレートの標準化などを行い，システムの品質向上を図っているが，それでもシステム障害が発生するケースが多々ある。

また，近年，CPSの一部にパブリッククラウドなど第三者が提供するサービスが採用されている場合があり，それらについても障害が発生することを前提として，その対策を施しておくことが重要である。

万一，システム障害が発生した場合，障害発生による社会的影響を低減するために，次の対応を行わなければならない。

⑴　システムを監視し，障害を即時に検知

⑵　障害からの速やかな復旧

⑶　障害の根本原因を特定し，それを除去

通常，上記の対応において，障害発生を検知してからの復旧はシステムの運用担当者が行うことが多いが，人手を介することで復旧までに時間が掛かる傾向がある。また，人手による作業は操作・手順ミスなどのヒューマンエラーも避けられない。したがって，可能な限り人手を介さずに自動復旧した方がシステムダウンの時間を短縮でき，顧客の業務への支障を低減できる。更に，システム障害の検知・復旧及び根本原因の特定のためには，システム設計書などが必要になる。このため，運用担当者及び関係者に対して，開発フェーズで作成したシステム設計書を確実に引き継いでおかなければならない。

復旧の自動化及び設計書の整備は，運用フェーズへの移行前の開発フェーズで開発担当者が行い，運用担当者に引き継ぐ必要がある。そこで，東芝デジタルソリューションズ（株）は，障害発生を前提としたシステム設計，及び漏れのない引き継ぎを行うために，“MSP（マネージドサービスプロバイダー）対応システム開発ガイドライン”及び“MSP対応確認チェックリスト”を開発した。ここでは，そのシステム開発ガイドラインと確認チェックリストの概要について述べる。

2. MSP対応システム開発ガイドライン

システムの運用・保守を含めた総合的なサービスを提供することを，マネージドサービスと呼ぶ。また，マネージドサービスを提供する事業者は，MSPと呼ばれている。

MSPは，顧客との間で，サービスの品質を保証する契約を結ぶことが一般的である。この契約はSLA（サービスレベル合意書）と呼ばれ，一般にサービスの定義・範囲・内容や，品質目標とそれに違反した場合の補償などを規定する。例えば，“サービス提供者はサービスの月間稼働率99.9％を保証し，違反時には顧客へサービス利用料金の10％を返金する。”といった条項が，SLAに含まれる。

SLAを満たした運用を行うためには，SLAに対応する品質指標を常に計測し，品質目標に対して違反が発生した場合には一次的な対策を施して，早急に品質を回復する必要がある。そして，違反の原因となった品質上の問題を解消し，更に恒久的な対策としてその問題の根本原因を調査して改善することが重要である。

これらを実現するためには，サービス開発時から品質目標の達成を考慮して設計・実装をするとともに，品質指標の計測，問題の検知，原因調査が可能な仕組みを用意しておく必要がある。

これらの仕組みを備え，マネージドサービスとして運用可能なシステムを開発するために実施すべきことを，MSP対応システム開発ガイドラインとして標準化した。

実施すべき項目は，当社でのシステム運用経験，更に社外事例[1]や業界標準など[2, 3]も加えて洗い出した。現在，10カテゴリー，84項目をこのガイドラインに掲載している。**表1**にカテゴリーの一覧を示す。

このガイドラインでは，項目ごとに実施する目的の解説と，社内の開発標準に基づいた具体的な実現方法，コード例を示している。利用するツールやフレームワークを共通化することで，システムの開発・運用・保守の品質向上と効率化を図ることができる。また，開発段階から運用の自動化，定型化を行うことで，複数のサービスを同じ手順でまとめて運用することにより一層の効率化も期待できる。

2.1　システムの可用性

システムの可用性について，ガイドラインの内容の一部を説明する。可用性とは，システムが正常な状態で継続して稼働できる能力のことである。マネージドサービスのSLAの中に示されている可用性を保証する場合，システムの稼働状態の監視や障害の検知，障害の管理者への通知，障害からのシステムの自動復旧，障害部分の切り離しを行うために，システムのモニタリングの仕組みが必要になる。

パブリッククラウドでは，可用性の実現方法が従来のオンプレミスとは異なる。オンプレミスでは，ハードウェアの信頼性を高めるなど，障害を回避することで可用性を高めていた。一方，パブリッククラウドでは，障害を回避するのではなく，発生する障害の影響を抑えることで可用性を高めている。また，パブリッククラウドの責任分担では，サービスの可用性はクラウドサービスプロバイダーが担保するため，ユーザーは関与できない。このため，パブリッククラウドを用いたマネージドサービスでは，クラウドサービスプロバイダーが提示する可用性をベースに，ユーザーの責任範囲であるアプリケーションを加えて，サービス全体の可用性を設計することが求められる。

2.2　システムの状態監視

一般に，サーバーやコンテナの稼働状態の確認手段は，パブリッククラウドの機能として提供されている。しかし，サーバーやコンテナが稼働していても，アプリケーションが正常に稼働していなければ，システムとしては利用不可の状態にある。したがって，システムの状態監視には，アプリケーションの稼働監視まで含める必要がある。

アプリケーションが正常に稼働していることを確認するには，確認手段をアプリケーション自体が備えている必要がある。

例えば，アプリケーションに**図1**のような健全性チェック用のエンドポイントを用意し，定期的に当該エンドポイントへ接続することで監視を行う。ガイドラインでは，この健全性

表1．MSP対応システム開発ガイドラインのカテゴリー一覧
List of categories of system development guidelines for managed services

カテゴリー	項　目	カテゴリー	項　目
A	システムとネットワーク	B	コードとドキュメント
C	設定情報	D	開発ライフサイクル
E	クラウドネイティブなアプリケーション実装	F	可用性の確認
G	セキュリティー	H	モニタリングとログの管理
I	パフォーマンスとキャパシティー	J	運用

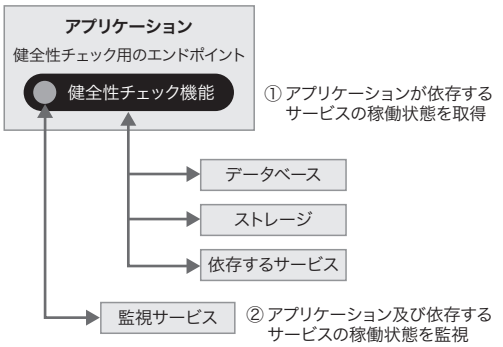

図1．アプリケーションの健全性のチェック方法
アプリケーションが正常に稼働していることを監視するために，エンドポイントを用意し，定期的に接続することで監視を行う。
Checkpoints to evaluate soundness of application in development and operation phases

チェック用のエンドポイントの実装方法を，具体的に示している。

2.3　自動障害復旧

システムダウンの時間を短縮するには，システムが障害から自動的に復旧できることが必要である。近年，パブリッククラウドが提供するサービスにより，障害からの復旧の自動化が容易になっている。

また，クラウドサービスでは計算機リソース（CPUや，メモリー，ストレージなど）の調達が容易なため，システムの一部に障害が発生してもサービスを継続できるように計算機リソースの冗長化が推奨されている。ただし，それには，システムの設計段階で冗長化に対応しておく必要がある。

ガイドラインでは，一般的なシステム障害に対し，これらの自動復旧方法を示している。

2.4　原因特定

障害の原因を特定するには，システムの状態監視で異常のあるコンポーネントを特定できるようにすること，及び各コンポーネントで必要な情報をログなどに保存しておくことが必要である。また，原因調査を効率的に行うには，各コンポーネントのログを集約して分析可能にすることが求められる。ガイドラインでは，原因調査のために収集すべきログの種類や，ログの集約・分析のためのアーキテクチャーを示すことで，様々なCPSにおいて統一的・効率的に原因特定が行えることを目指している。

3.　MSP対応確認チェックリスト

運用時に必要なドキュメント（運用マニュアルや，各種設計書など）や運用に必要な環境が，開発担当者から運用担当者に引き渡されることで，初めて運用フェーズに移行できる。ただし，システムの規模や運用の範囲などにより，運用に向けて準備するものが異なる。例えば，システムのインフラをマネージドサービスとして提供する場合は，アプリケーションの監視，対応などが不要となるため，アプリケーションを対象とした運用マニュアルがいらなくなる。このことから，システム開発時に，対象となるシステムの運用業務範囲を確認し，必要なドキュメントを確実に運用担当者に引き渡すことが必須となる。

また，運用効率化のための仕組みをシステムのアプリケーションに作り込むことについても同様であり，システムの特性により，どこまで作り込むかを判断することが重要になる。

これらのことから，運用の対象となるシステムに対して，何をどこまで作成するかを，システムを開発する前に開発者と運用担当者の双方で検討し，合意しておくことが重要である。この合意作業をサポートするために，MSP対応確認チェックリストを開発した。

MSP対応確認チェックリストは，MSP対応システム開発ガイドラインで示した84項目に対し，**表2**に示す例のようにまとめている。

ここで，このチェックリストを，提案～設計・構築～リリース～運用といった一連のプロセスにおいて，どのように活用しているかについて述べる。チェックリストに基づいて確認を行うタイミングを**図2**に示す。

提案・見積もり段階（図2の①）では，開発担当者と運用担当者の双方で，開発対象となるシステムの運用に必要なドキュメントやアプリケーションの作り込み範囲の選定を行い，サービス開発の見積もりに反映する。要件定義段階（図2の②）では，サービスの運用要件の変更などによる見直しを行う。また，設計・構築・テスト段階（図2の③）では，開発担当者により作成されたドキュメントについて，不備がないことを運用担当者と逐次確認する。運用テスト段

表2.　MSP対応確認チェックリストの項目例

Examples of checklists for managed services

No.	チェック項目	ルール
A.1	システムの構成は明確か	利用するクラウドサービスとその構成が明確であること。
A.2	ネットワークの構成は明確か	利用するクラウドサービスの通信経路，プロトコル，ポートなどが明確であること。
⋮	⋮	⋮
E.8	ボトルネックになる処理は明確か	アプリケーション内の，ボトルネックになる処理が明確であること。
⋮	⋮	⋮
F.1	アプリケーションは安全に終了するか	アプリケーションがスケールインなどで停止する場合，アプリケーションは安全に停止し，再度起動された場合にも問題なく動作すること。
⋮	⋮	⋮

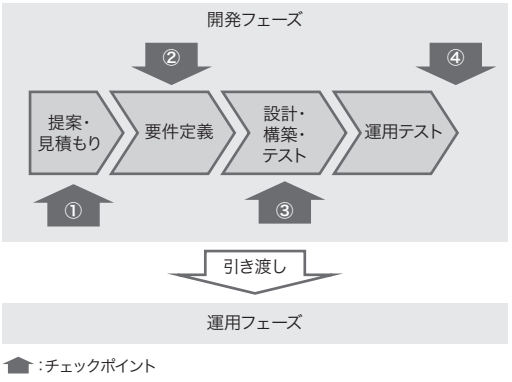

図2.　チェックリスト利用のタイミング

サービスの開発・運用プロセスの様々な段階で，MSP対応確認チェックリストを利用する。

Timing of use of checklists

階（図2の④）では，運用マニュアルなどの作成ドキュメントを基に運用テストを実施し，各ドキュメントなどに対して開発担当者及び運用担当者の双方で最終確認を行い，問題がなければ運用フェーズへ移行する。

4. あとがき

現在，当社は，顧客向けにパブリッククラウドを対象としたマネージドサービスを，“東芝マネージドサービス Albacore™”[4]として提供している。該当する案件には，MSP対応システム開発ガイドライン及びMSP対応確認チェックリストを適用しており，運用後に発覚するような運用環境の不備を事前に確認することで，効果を上げている。

運用において，事前検討漏れの低減は，チェックリストの項目を増やし，細部まで確認することで実現できるが，確認するための手間が多くなり担当者への負担が増すことになる。この点については，設計標準と併用することで負担を軽減している。例えば，システム設計書や運用設計書などに必要な項目が記載されているかの確認は，標準の設計テンプレートを用いることで確認作業を省略している。

また，MSP対応システム開発ガイドライン及びMSP対応確認チェックリストを継続的に強化させていくことが重要である。例えば，クラウドサービス技術の進化により，確認する項目が変わってくる可能性がある。クラウドサービスが提供された当初は，バーチャルマシンなど計算機リソースを意識しなくてはならなかったが，現在では，サーバーレス技術のように，計算機リソースを意識しなくてもシステム構築が可能になってきているものもある。従来の運用フェーズでは，計算機リソースのキャパシティー管理・性能管理が必要だったが，サーバーレス技術では計算機リソースの管理は不要になる。このように，技術の進化に合わせて確認項目の継続的な見直しが必要になる。

今後も，MSP対応システム開発ガイドライン及びMSP対応確認チェックリストの更新を継続し，高品質なマネージドサービスを顧客に提供していく。

文　献

(1) Beyer, B. et al., eds. Site Reliability Engineering: How Google Runs Production Systems. O’Reilly Media, 2016, 552p.
(2) 情報処理推進機構（IPA）技術本部 ソフトウェア高信頼化センター. “システム構築の上流工程強化（非機能要求グレード）”. 社会基盤センター. <https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html>,（参照 2020-06-22）.
(3) 電子情報技術産業協会 ソリューションサービス事業委員会編. 民間向けITシステムのSLAガイドライン. 第4版, 日経BP社, 2012, 328p.
(4) 東芝デジタルソリューションズ. “東芝マネージドサービス Albacore™ ビジネスと，その進化をとめない”. Albacore（アルバコア）. <https://www.toshiba-sol.co.jp/pfsol/agcloud/albacore.htm>,（参照 2020-06-22）.

雑賀　翼　SAIKA Tsubasa
東芝デジタルソリューションズ（株）
ソフトウェアシステム技術開発センター
IT モダナイゼーション推進部
Toshiba Digital Solutions Corp.

村田　尚彦　MURATA Naohiko
東芝デジタルソリューションズ（株）
ソフトウェアシステム技術開発センター
IT モダナイゼーション推進部
Toshiba Digital Solutions Corp.