ITシステムの安定運用を実現するマネージドサービスを支える技術

Managed Services Allowing Customers to Secure Stable Operation of Information Technology Systems

熊崎　裕一郎 KUMAZAKI Yuichiro　　今井　　聡 IMAI So

コンピューターシステムの保守においては，IoT（Internet of Things）の普及に伴い，監視対象機器数が飛躍的に増加しており，その安定運用に有効なマネージドサービスが注目を集めている。

東芝ITサービス（株）は，技術者が長年にわたって積み重ねたノウハウや仕組みを活用したマネージドサービスを提供しており，リモート監視サービスでは，警報処理の96％を自動化して，措置が必要な案件を絞り込むことで，顧客のIT（情報技術）システムの安定運用を実現している。

Managed services for the maintenance of computer systems, which can effectively analyze large volumes of data, have been attracting increasing attention in recent years in line with the expanding number of monitored devices accompanying the dissemination of the Internet of Things (IoT).

With this trend as a background, Toshiba IT-Services Corporation has been providing managed services based on its know-how acquired through the accumulated experience of its engineers. In the field of remote monitoring services, we are contributing to the stable operation of customers' systems by providing an incident management system that automatically classifies alarms and extracts critical incidents needing specific actions for system recovery. Our incident management system has achieved a 96% reduction in the number of manual operations required for such incidents.

1. まえがき

東芝ITサービス（株）は，設立時から現在に至るまで，コンピューターの保守サービスの提供を事業の柱としているが，昨今，マネージドサービスと呼ばれているコンピューターシステムの運用サービスも1980年代から提供してきた。この約40年の間に，マネージドサービスを取り巻く環境は変化してきたが，サービスの提供にあたって，技術者の継続的な取り組みによって得られたノウハウの蓄積と，仕組み作りが重要であることは変わらない。

ここでは，当社におけるマネージドサービスの提供を支える技術と体制について述べる。

2. マネージドサービスへの取り組み

当社は，1980年代に東芝が導入したスーパーコンピューターのオンサイト運用サービスの受託に始まり，リモート監視サービス，リモート運用サービス，リモートセキュリティー監視サービスと，マネージドサービスの提供を拡大してきた。現在では，マネージドサービスに従事する技術者は800名を超える規模となり，当社における事業の柱の一つへと成長した。

当社では，提供するマネージドサービスを，大きく二つに分類している。その一つがオンサイトマネージドサービスで，顧客の拠点又はコンピューターの設置拠点に駐在した技術者が，サービスを提供するものである。もう一つは，リモートマネージドサービスで，当社の拠点であるリモートマネージドサービスセンター（RMC：Remote Managed Service Center）に常駐する技術者が，ネットワーク経由で顧客のコンピューターなどを監視・操作してサービスを提供するものである。

マネージドサービスは，システムの導入から廃止までの長期間のライフサイクルを継続してサポートするサービスであることから，当社では，効率の良い安定したシステム運用により，安心を提供することが，顧客にとって最大の価値になると考えている。

3. マネージドサービスの安定運用を支える技術

当社では，マネージドサービスを提供する技術者自らが日々の業務から得たノウハウを体系化し，その知見を基に業務の自動化を推進し，生産性と品質の向上を実現してきた。

3章では，マネージドサービスの中でも重要な要素である障害監視と，定常的に行う必要がある運用作業の管理に関する自動化技術について述べる。

3.1 インシデント管理システムによる自動化

RMCでは，幅広い顧客へリモート監視サービスを提供している。このサービスは，**図1**に示すとおり，顧客が利用し

ている各種機器の状態を常に監視し，障害が発生した場合は直ちに顧客に連絡するというものである。契約によっては，定型化された障害復旧措置も含まれる。

RMCでは，監視対象の機器から，合計で1か月当たり平均約10,000件（2020年度実績）の警報を受信している。この大量の警報を誤りなく効率的に処理するため，**図2**に示すインシデント管理システムを開発し，運用している。

一般に，インシデントは，顧客の機器に何らかの影響を与える事象である。RMCでは，これを拡張して，インシデントを，何らかの警報を認知して，内容を判別し，顧客への通報など必要な措置を実施するまでの一連の流れと捉えている。

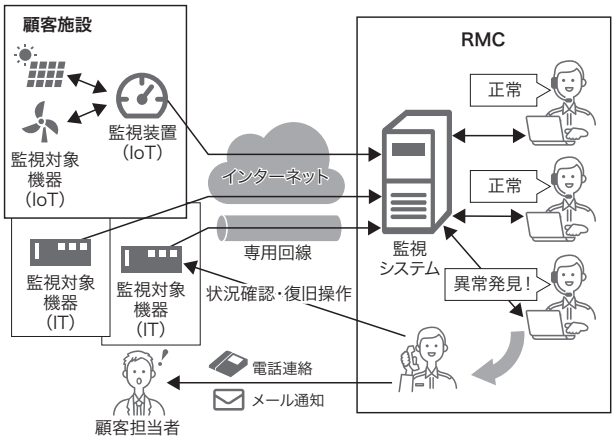

図1. リモート監視サービスの概要

RMCでは，顧客の保有する幅広い機器に対して，その状態を常に監視し，障害が発生した場合には直ちに連絡するといったリモート監視サービスを提供している。

Overview of remote monitoring service

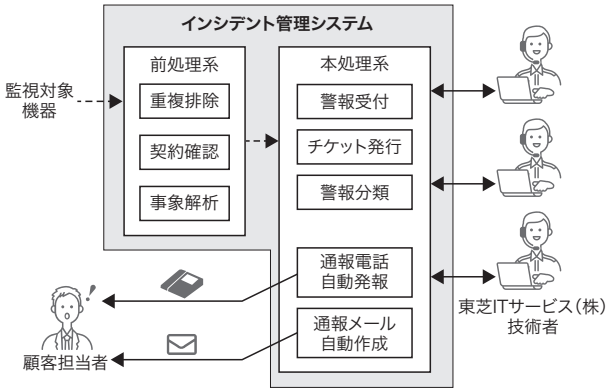

図2. インシデント管理システムの概要

警報処理の自動化によりIoTへの対応で監視対象機器数が飛躍的に増加しても，インシデントの見逃しを防ぐことができ，顧客への適切な連絡や障害復旧措置が可能となった。

Incident management system to extract critical incidents needing specific actions for system recovery

インシデントの発端は，監視装置や監視対象機器から出力される警報メール又はログ（動作や状況の記録）である。インシデント管理システムの前処理系では，技術者が蓄積したノウハウを結集したルールと，監視計画で顧客と合意したルールを，データベースに登録して，そのデータベースを参照することで警報メールやログのふるい分けを行う。ふるい分けの結果，技術者による対応が必要と判定したものだけをインシデントとして本処理系に登録して，適切に対応できるようにした。

前処理系で行っている具体的な処理は，次のとおりである。

⑴ 重複排除　障害が継続している場合など，同一の原因で警報などが連続して発生する場合，これを自動的に判定し，一つの警報にまとめる。

⑵ 契約確認　契約に応じて通知や措置を行うため，警報などと顧客名のひも付けを行う。

⑶ 事象解析　警報などの内容を基に，重要度を判定するとともに，顧客への通知電話・通知メールのテンプレートを選択した上で，本処理系へインシデントとして登録する。

インシデント管理システムの本処理系では，インシデントの登録，インシデントの対応状況の確認など，技術者の支援を行う。更に，RMC独自の機能として，重要度に応じて顧客への通知メールを自動生成し，自動送信する。

この仕組みにより，警報処理の96％が自動化され，技術者による対応を1か月当たり約400件に削減できた。IoTへの対応で監視対象機器数が飛躍的に増加しても，インシデントの見逃しを防ぎ，いざというときは，顧客への適切な連絡や障害復旧措置が可能となった。

3.2 運用作業管理システムによる自動化

RMCでは，顧客との契約で定められた定期作業，顧客から随時依頼される臨時作業，及び障害予防のための運用作業など，1か月当たり約3,200件の作業を，計画に沿って実施している。この大量の作業を確実に実施するため，当社では運用作業管理システムを開発し，活用している。このシステムは，技術者に向けて所定の時刻に作業の実施を促す機能，及び管理者に向けて各作業の進捗状況をまとめて報告する機能を提供する。

システムの構成図を，**図3**に示す。RMCでは，このシステムに，月次，週次，日時，臨時などの種別を指定して，管理者が作業予定を登録している。実施すべき作業の予定時刻近くになると，作業状況を表示している大型モニターの該当行が黄色となり，更に作業予定時刻を超過すると，警

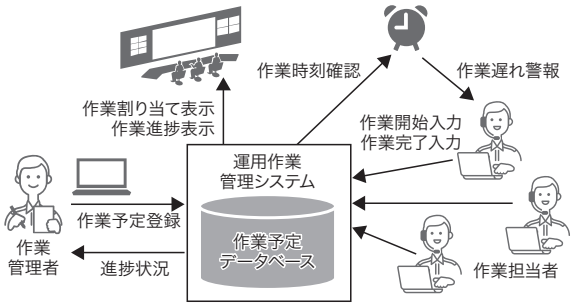

図3. 運用作業管理システムの概要

作業予定が一目で把握できるこのシステムを導入して以来，作業漏れは発生していない。

Job operation management system for notification of job schedules

報を発出することで，作業担当者に作業開始を促す。作業担当者は，作業の予定時刻が近づいてきたことを一目で把握できるので，漏れなく作業に着手できる。同時に，作業管理者は，全ての作業の進捗状況を把握できるので，確実に作業の管理ができる。また，交代勤務に伴う交代時の引き継ぎ時にも役立つ。

2010年8月にこのシステムを導入して以来，作業漏れは発生しておらず，最小限の機能により，大きな効果を上げている。

3.3　きめ細かい監視を実現するログ監視

監視対象であるコンピューターシステムの仮想化やクラウドシステム化が進むにつれて，専用の監視サーバーによる監視に代わり，ソフトウェアが出力するログを基にした監視が主流となりつつある。当社では，この状況に対応するため，SIEM（Security Information and Event Management）製品を導入して，障害の検知に役立てている。SIEMを用いたログ監視の高度化について，**図4**を用いて述べる。

従来のログ監視では，ログの中に事前に登録した文字列

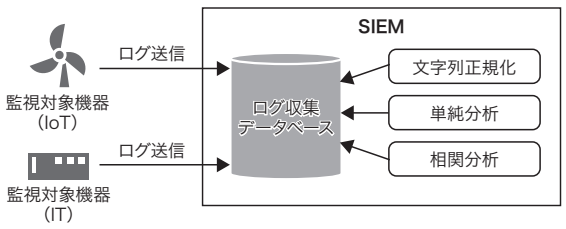

図4. SIEMを用いたログ監視の高度化

従来法の単純なログの分析だけでなく，文字列正規化と相関分析により，ひそかに進行する情報セキュリティー上の障害の予兆を検知できる。

Log monitor with further strengthened functions using security information and event management (SIEM)

が出現したら障害検知とする，という単純な検索しかできなかった。SIEMであれば，文字列正規化と相関分析により，ログの出現順序など時系列に依拠した検索や，サーバーAで何らかの文字列αが出力され，なおかつ，サーバーBでも同じ文字列αが出力された場合に障害とするなど，サーバーをまたがる検索が可能となる。この検索は，巧妙に痕跡を隠蔽するサイバー攻撃の検知に寄与する。また，複雑な障害時など，技術者が大量のログを調査する場合にも，SIEMにより検索作業を効率化できる。

更に，将来は，ログの出力パターンの変化を見定めるなどの手法で，障害が発生する前の予兆を検知して，障害を未然に防止する，いわゆる予防保守の実現へとつなげ，SIEMによるログ監視を利用して，高付加価値サービスを提供していく。

4. マネージドサービスを支える技術の向上

マネージドサービスを提供するためには，障害監視・運用を行う拠点の整備と技術者の育成が必要である。ここでは，マネージドサービスを支える体制や人材，及びそれらの運営に関する仕組みについて述べる。

4.1　マネージドサービスの提供体制

コンピューターシステムがビジネスそのものとなった今日，マネージドサービスを利用する顧客は，1日24時間，週7日，途切れることのないサービスの提供を期待している。その期待は，大規模災害が発生した場合でも変わらない。

RMCでは地震・停電などの災害に備えて，サービス拠点を国内の東西3か所に分散配置している。平常時は三つの拠点で分散してサービスを提供している。いずれかの拠点が被災した場合は，顧客との契約条件に応じて，残る二つの拠点だけでサービスを提供できる体制を整えている。また拠点を置くだけでなく，災害を想定した切り替え訓練を行い，切れ目のない運用を実現している。

災害対策のため，コンピューターシステムを複数箇所のデータセンターに分散配置することは一般的となっているが，当社では更に，技術者を含めてマネージドサービスの拠点を分散配置して顧客に提供することで，信頼性を高めている。

4.2　技術者の育成

マネージドサービスの事業規模拡大に伴い，直近10年間で当社の技術者数は約1.5倍となった。この技術者を育成することが，マネージドサービスの提供にあたって最も大切であると考え，継続的に技術者育成に努めている。育成カリキュラムは，監視サービスの障害事例を基に組み立てており，短期間で技術者を育成して，今後のサービス需要の拡大に備えている。

4.3　顧客の声やノウハウの共有

マネージドサービスを提供している技術者は，日常的に顧客との接点を持ち，貴重な経験を積む機会があるものの，駐在拠点の地理的な制約や交代制勤務による制約により，経験で得た知見の共有が難しいという問題があった。

この問題を解決するため，当社では，顧客の声と対応事例の共有を進める活動を推進している。2020年度から，専用のデータベースを用意して，情報の登録を開始した。今年度は，十分なデータが蓄積できたことから，テキストマイニング技術を適用して，具体的な声として現れることのない，潜在的な顧客ニーズを掘り起こす仕組みを整え，サービス向上に役立てる取り組みを開始した。

この活動は，技術者の意識向上や部門内のコミュニケーション向上といった内部的な効果だけでなく，サービスの品質向上や顧客への提案件数の増加という形で，顧客へ提供する価値の向上に寄与している。

4.4　ISO/IEC 20000の認証取得

当社は，高品質なマネージドサービスを提供するため，ITサービスマネジメントに関しての国際標準であるITIL（Information Technology Infrastructure Library）に基づいて，サービス提供と品質管理の体制を整え，2011年に主要なサービスについて，ISO/IEC 20000（国際標準化機構／国際電気標準会議規格 20000）の認証を取得した。認証の取得により，当社のマネージドサービスが適切な体制で提供されていることを証明できた。

5. ユニファイドサービス

当社は，新しいマネージドサービスとして，包括的なサービスが特徴であるユニファイドサービスを提案している。ユニファイドサービスとは，オンサイトマネージドサービス，リモートマネージドサービスに加えて，当社が提供している，全国108拠点から現地駆け付けを行う保守サービス，及びIT機器の構築や初期設定作業を行うプラットフォームインテグレーションサービスを組み合わせて，顧客のニーズに包括的に対応するサービスである。フィジカル領域で得たデータを，サイバー領域で付加価値のある情報に変換し，フィジカル領域に戻して活用するサイバーフィジカルシステム（CPS）の考え方に基づき，フィジカル領域にある機器の状態を維持・復旧する機能を提供している。

例えば，次のようにサービスを有機的に組み合わせたユニファイドサービスによって，新たな価値を提供している。

⑴　オンサイトマネージドサービス　　顧客の業務知識に精通した技術者が常駐して，日々のシステム運用や業務支援を行う。

⑵　リモートマネージドサービス　　システムが発する警報やユーザーからの問い合わせに対して，夜間休日を含め，当社拠点に常駐した技術者が対応する。

⑶　保守サービス　　警報の原因が装置の故障と判断した場合は，保守員を現地に派遣して修理を行う。

6. あとがき

当社では，40年以上にわたり，個々の技術者がサービスの現場で経験を積み，それぞれの役割において責任を持ち，常に改善を繰り返しながら顧客に寄り添ってきた。ここで述べた技術や体制も，このような技術者の取り組みによって作り上げたものである。

今後，AIなどの新しい技術を取り入れて駆使するとともに，これまでどおり顧客との接点を大切にして，より高品質なマネージドサービスを提供していく。

熊崎　裕一郎　KUMAZAKI Yuichiro
東芝 IT サービス（株）
サポート & ソリューション統括部 ソリューション推進部
Toshiba IT-Services Corp.

今井　　聡　IMAI So
東芝 IT サービス（株）
マネージドサービスセンタ 第二マネージドサービス部
Toshiba IT-Services Corp.