Vol.2020-IOT-51 No.3
Vol.2020-SPT-39 No.3
2020/9/4

障害監視システムおよび障害対応業務モデルの提案

波田野裕一 [1]

概要：IT を利用したサービスやシステムの多くにおいて，正常なサービスの提供やシステムの稼動を実現するために 24 時間 365 日の体制で障害監視システムの運用・保守および障害対応業務が行なわれている．従来から監視システム製品・ツールの仕様や利用方法の情報は豊富にあり，近年は障害監視システムの設計に関する情報も増えてきたが，障害監視システムから障害対応業務にわたる障害監視全体にわたってどのように設計するべきかという情報はまだ少なく，各現場において個々人の経験に基づいて非再現的に設計および構築が行なわれているのが現状である．本稿では，障害監視全体を俯瞰し，再現性を持って障害監視システムおよび障害対応業務を設計・構築するためのモデルを提案する．

キーワード：障害監視，障害対応

1. はじめに

多くの IT サービスや IT システムにおいて，サービスの正常な提供やシステムの安定的な稼動を実現するために，監視システムを構築・導入し，早期に障害の発生やその予兆の検知を図っている．そして，障害やその予兆を検知した時に迅速に対応できるように何らかの形で 24 時間 365 日の障害対応体制が敷かれている．

このような障害監視のための製品やツールの仕様および利用方法を解説する情報は従来から豊富にあり，IT エンジニア同士の情報交換が盛んに行われてきた．

更に近年は障害監視システムの設計に関する書籍が発行されるなど，ソフトウェア上の情報も増えてきたが，障害監視システムから障害対応業務にわたる障害監視全体にわたってどのように設計するべきかという情報についてはまだ少なく，各現場において個々人の経験に基づいて非再現的にその設計および構築，運営が行なわれているのが現状であると言える．

本稿では，まず現在の障害監視において抱える課題を明らかにし，障害監視全体を俯瞰し，再現性を持って適切な監視業務を設計･構築するためのモデルについて提案する．

2. 一般的な障害監視センターの障害対応フロー

IT サービスマネジメントのベストプラクティスリファレンスとされている ITIL(v3)では，サービスオペレーションプロセスにおいて，インシデントマネジメントプロセスフローとして以下のようなフローを定義している．[1]

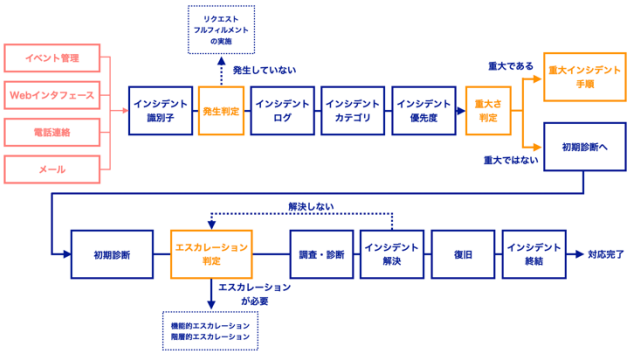
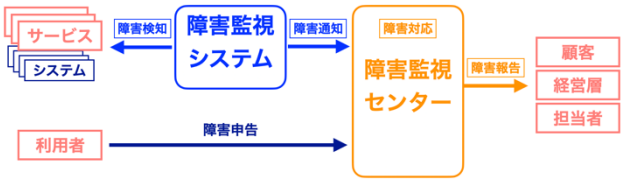


図 1　ITIL Incident management process flow (一部簡略化)

多くの障害監視センターにおいて ITIL のインシデントプロセスフローと類似した障害対応フローが実施されており，数千台のネットワーク機器・サーバ機器を有する IT サービス事業者 A 社においても，ほぼ同様の障害対応フローを実施していた．

A 社においてはメールを主要なインシデント通知媒体とし，イベント管理コンソールや Web インタフェースによる監視を補助的に併用していた．また，障害連絡窓口を社内に公開し，サービス障害を認知した社員からの電話による障害報告にも対応することとなっていた．

このように，一般的な障害監視センターにおいてはインシデント通知の受信を起因としたインシデント対応が主たる業務となっており，インシデント通知を責任分界点として，障害監視システムはシステム管理部署が担当し，障害監視オペレーションは障害監視センターが担当するという分担が行なわれていることが多い．



1 北陸先端科学技術大学院大学
Japan advanced Institute of Science and Technology

Vol.2020-IOT-51 No.3
Vol.2020-SPT-39 No.3
2020/9/4

図 2　障害監視の全体像

これは，障害監視システムに関連する業務が「障害監視システム」というモノに対する専門業務に大きな比重が置かれるのに対し，障害監視センターにおける障害監視オペレーション業務のほとんどが「障害」というコトに対する専門業務であることによる要求技術や勤務体制の差異によって決められた分担であると考えられる．

このように障害監視システムと障害監視オペレーションは障害情報の伝達における上流と下流の関係にあるため，上流側である障害監視システムの仕様やそれ自身の障害に起因する障害通知の増大や検知トラブルに，下流側である障害監視オペレーション業務が直接巻き込まれやすい状態になっている．

実際に A 社においても，事業の拡大とともに監視対象が劇的に増え，監視対応表が数十万セルの規模に肥大化し，受信する障害通知の数が年間数十万件に達するとともに，障害対応フローに存在しない形式の障害通知メールの受信により現場が混乱することも珍しくなくなっていった．

このような状況下において障害監視オペレーション側でできる根本解決策としては，障害監視システムの管理部署に対して障害監視システムの設定変更や改修を要望することだけであり，その設定変更や改修が適切に実施されるまでの間は暫定的にイレギュラー対応フロー追加して凌ぐことになるが，通常であっても負荷が高い状況下においてイレギュラー対応フローが 1 つでも追加されることは現場にとって大きな負担になる．もし，障害監視システム側で根本解決策が実施されなかったときには，現場の負荷状態を軽減するために暫定対応を永続化するために障害監視オペレーション側で障害対応システムの改修を行う場合もあり，元々逼迫している障害監視オペレーションの工数を増大させ，更には障害監視フローが複雑になることにもつながっていくのである．

このように障害監視システムと障害対応オペレーションを上流と下流で分担する体制を取っている場合，以下のように障害アラートの上流側から設計しはじめ下流側に向けて障害監視業務の設計・構築が行われることが多い．

1. 障害監視の対象となるサービスやシステムの確定
2. 障害監視システムの設計，構築，設定の実施
3. 障害対応業務の体制の構築および障害対応フローの策定
4. 障害アラートの通知先の決定，通知設定の実施
5. 障害対応業務の開始

そして，ある程度障害対応業務が安定してくると，障害監視システム側の都合により 3 のフロー策定と 4 の通知設定の順に逆転が生じ，事後承諾の形で障害対応フローが増えることも珍しくはない．このようにして設定された障害監視が，障害対応フローに存在しない形式のアラートを生み出して障害監視オペレーションを混乱に陥れるのである．

このような障害監視システムと障害監視オペレーションの上流・下流という関係は，障害アラート数の増大や障害対応業務の複雑化を招きやすく，障害監視オペレーション側で根本改善をすることが事実上不可能な状態に陥りやすいということができる．

3. 障害監視業務全体を俯瞰する

3.1 なぜ障害監視を行うのか

障害監視は，そもそも何のために行うのか．

ここでは，障害監視を「顧客に提供するサービスやその構成要素である機器などが安定的に稼動していることを継続的に確認し，その稼動が非安定的な状態にある場合には復旧に必要な情報を収集し，対応すること．」と定義する．

上記の定義に従うと，障害監視はサービスの安定的な稼動が最終的な目的であり，そのために必要かつ適切な対応を恒常的に行うことが障害監視オペレーションに期待される役割であり，適切な障害監視オペレーションを行う上で必要な情報を過不足なく伝えることが障害監視システムに期待される役割であることになる．

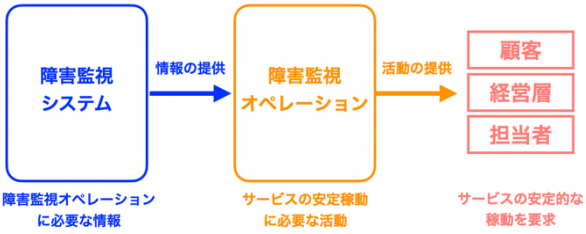


図 3　障害監視の全体像

3.2 障害監視の設計の流れ

このような目的を実現するために障害監視業務を設計するためには，図 2 において最も下流にいる顧客や経営層が考えるサービスの安定稼動をまず明確にする必要がある．次に，顧客たちの求める安定的な稼動を実現するためには，どんな状態のときにどんな対応をするか，どのような情報が必要で，どのように行えばその対応が実現可能になるか，という障害監視オペレーションの設計をする必要がある．更には，顧客達の期待に答える障害監視オペレーションを実現するために必要な情報を得るためには，どのような監視位置からどのような監視を実行して，どのように通知するか，という障害監視システムの設計をする必要がある．

つまり，多くの監視業務においては上流側から設計しているが，障害監視の目的に照らし合わせれば，以下のように下流側から設計するべきであると考えられる．

1. 顧客たちが求める「安定的な稼動」のヒアリング・定義
2. 「安定的な稼動」を実現するための障害対応の設計(どんな事象が起きたら，どんな対応をするべきか)
3. 障害対応に必要な情報の洗い出し
4. 障害対応に必要な情報の取得方法および通知方法の設計，構築
5. 通知設定の実施，障害対応業務の開始

3.3 障害監視の情報の流れ

上記の障害監視設計の観点から，障害監視における情報にはその到達すべき先に応じて 4 つの障害情報レベルを考えることができる．

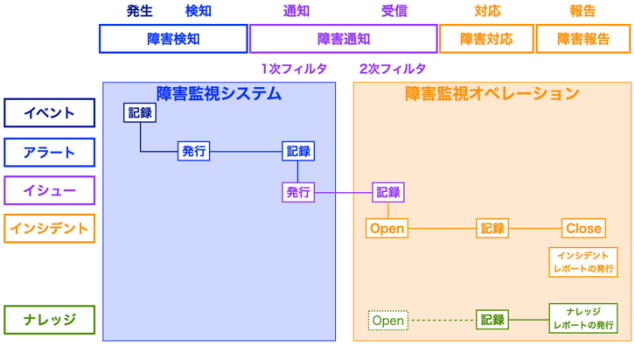


図 4. 到達先に応じた障害情報のレベル

イベント

障害監視システムの監視機能が動作したことを構造的に記録した情報．

アラート

障害監視システムによって安定状態と異なる状態を検知したものを構造的に記録した情報．

自動復旧システムなどによる復旧を試み，復旧した場合は復旧情報を記録して対応完了となる．サービスに影響の無いシステム障害や機器障害は，原則としてアラートの段階で自動復旧を行う．

イシュー

障害監視システムによって自動復旧できないもしくは障害状況が不明なために，人手による確認や障害対応をする必要があると考えられるものを構造的に記録した情報．

障害監視システムにおいて，障害箇所や障害内容によって通知先や通知内容を切り替える一次フィルターを実装する場合がある．(例えば，ベンダや専門部署に直接通知する場合など)．サービス影響の無いシステム障害や機器障害など，障害監視オペレーションが関与する必要が無い場合は障害監視オペレーションにイシュー通知は行われない．

障害監視オペレーションの障害対応システムにおいて，障害箇所や障害内容によって自動処理の実施や担当者の自動アサインを行う二次フィルターを実装する場合がある．(例えば，障害監視システムで未実装の自動復旧を行っている場合や，専門性やシフト勤務によってアサインすべき人員が自動的に決めることができる場合など．)

二次フィルターの自動処理によって復旧した場合は復旧情報を記録して対応完了となる．

障害状況を確認し，顧客たちが求める「安定的な稼動」を満たさない状態が確定した場合は，インシデントの発行を行う．

インシデント

顧客たちが求める「安定的な稼動」を満たさない状態が確定しており，障害監視オペレーションにおいて人の手を介して対応する必要があるものを構造的に記録した情報．

サービスが復旧するまでの活動はインシデントに情報が集約され，全ての復旧活動の軸となる．また，サービス復旧後に顧客に対して発行するインシデントレポートの情報源となる．

インシデントには再発するものもあるため，頻発するものや影響の大きいインシデントの対応記録から知見を抽出し，ナレッジ DB を構築したり，定期的に障害監視センター内でナレッジレポートを発行したりするなどの取り組みを行う例も多い．

4. 障害監視の実例

A 社では，障害監視システムと障害監視オペレーションを別のチームが担当する 2 チーム体制で障害監視を実施しており，障害監視システムの検知するほぼ全てのイベントをメールで障害監視チームに通知し，障害監視チームではメールソフトでの振り分けと人力による振り分けを併用し，振り分け後に対応が必要と思われるメールについてのみ，前述の障害対応表で障害対応方法を確認して対応を実施していた．

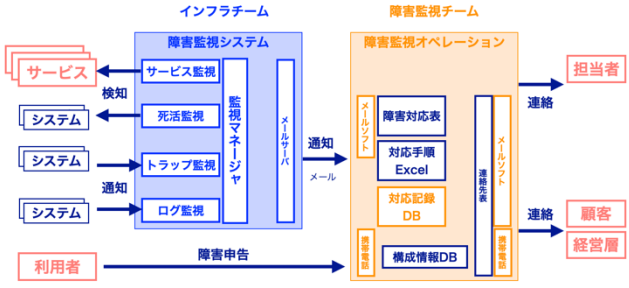


図 5. 障害監視の実例 (2 チーム体制)

Vol.2020-IOT-51 No.3
Vol.2020-SPT-39 No.3
2020/9/4

障害対応表の参照回数は 1 日あたり平均数百回に及び，大規模障害によってアラームストームが発生した場合には数万件のメールを 1 日で処理しなければならなくなったこともある．このような状況下で，ネットワーク機器およびサーバ機器の大規模な増強によるノード数の急増が確実視されていたこともあり，既存の障害監視の枠組みでは障害監視業務が維持できないと判断し，障害監視システムと障害監視オペレーションの全てを一元的に担当する障害監視チームを設置し，以下の施策を行った．

1. 障害連絡を受ける経営層や担当者に，どんな対応を期待しているのかをヒアリングし，障害監視を社内サービスとして再定義した．
2. 現状の障害監視リソースで，実施が可能な監視サービスを定義する一方で，その定義から外れる監視業務については，縮小・廃止を進めた．
3. 再定義した障害監視に必要な情報を洗い出し，構造化した．
4. 障害対応に必要な情報の取得方法や通知方法を構造化し，モデル化を行なった．
5. モデル化，構造化した障害情報の取得方法や通知方法を実装し，障害対応業務を切り替えた．

これらの施策により，従来は障害監視システムの仕様とその設定が障害監視全体を決め，障害監視オペレーションがその枠内で業務を実施するという形から，障害監視オペレーションにおける業務が障害監視の概要を決定し，その概要に従って障害監視システムに対して実装や設定のインプリメンテーションを行うという形へと変わり，障害監視における通知の下流側から上流側へと設計していく流れとなった．

その結果，以下のような変化を生じた．

1. 障害監視システムと障害オペレーションツールの連携

2 チーム体制のときには，別々に設計・構築されていた障害監視システムと障害オペレーションツールについて，マスターデータを共有することでツール間の有機的な連携が可能となった．また，各マスターデータの更新フローを一元化することで新規監視の追加やメンテナンスや障害発生時における機動的な対応が可能となった．更に，障害監視システムの設計意図や挙動をチーム内で随時共有できることによって障害対応フローの設計や見直しが容易になり、各フローの効率性(無駄な確認手順の排除など)や妥当性(効果が不明瞭な手順の見直しなど)が向上することにつながった．

2. アラート数の大幅な抑制

通知ルール DB と通知先 DB の実装により，通知不要なアラートの発生を抑制した．これにより，障害監視チームの受信アラート数が 50 分の 1 以下になり，業務負荷が劇的に低下した．

3. イシュー通知先の多様化

通知ルール DB と通知先 DB の実装により，担当者やベンダーに通知すべきアラートは障害監視チームを経由せずに直接通知するようになった．これにより，障害監視チームの負荷を下げつつ，担当者やベンダーの初動を早めることにつながった．

4. インシデント発行の迅速化

障害対応表を監視マネージャに組み込むことで,イシュー自体に対応ルールを明記できるようにした.これにより,障害監視チームの対応システムにおいてアラートを受信した時点で,障害対応の内容を確定させることが可能となり,インシデント発行の迅速化につながった．

更に，定型化が可能な初動対応については，障害監視システム側で自動対応を実装することで，継続的に障害監視業務の負荷を低減することにつながった．

5. 障害監視業務の拡大

障害監視を社内サービスとして再定義したことにより，従来は障害監視を自前で行っていた事業部署や開発部署から，障害監視の依頼が入るようになった．障害通知への対応負荷が低減していたことにより，新規監視業務の受け入れは十分に可能であり，社内他部署の負荷の低減に貢献するとともに，障害監視チームの存在意義が拡大した．

6. 隠れ監視業務の消滅

障害監視を社内サービスとして再定義し,その定義から外れる監視業務の縮小・廃止を進めるとともに，再定義した障害監視に必要な情報を洗い出し，構造化したことにより，技術的な理由や経緯が不明な障害対応ルールを一掃することが可能になった．これにより特定の監視要員にしかわからない監視業務がほぼ消滅し，定常的な監視業務についてはほぼ全員が実施可能となり，やや特殊性を帯びた業務についても上位の要員であればほぼ全員が実施可能となった．

Vol.2020-IOT-51 No.3
Vol.2020-SPT-39 No.3
2020/9/4

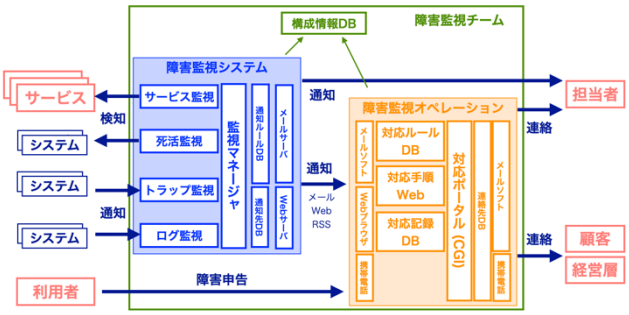


図 6. 障害監視の実例 (1 チーム体制への移行後)

5. おわりに: 障害監視業務の構造化へ

ここまで述べたように，障害監視業務については，障害監視システムと障害監視オペレーションは一体として設計・構築・運用をしなければ有効に機能することが困難であり，その設計は障害監視による受益者である下流側から設計・実装していかなければその目的を正しく達成することが困難である．そして，監視業務のシステムとオペレーションの双方について，適切なモデル化や構造化が必要であり，そのモデルや構造が一定の妥当性を持つ場合には，極めて大きな効果を得ることができる．

また, 障害監視はサービスの安定的な稼動が最終的な目的であることから，その目的に資するために後工程が何を求めているかが障害監視および障害対応における各プロセスの役割を決める上で最も重要である．

障害監視システムおよび障害対応オペレーションにおける個別プロセスのモデル化については，稿を改めて提案をする機会を得たいと考えている．

参考文献

[1] ITIL Service Operation, 2011(電子版) “4.2.5 Process activities, methods and techniques”