ソリューション・レポート

NSM 監視サービス、および統合監視システムのご紹介

NSM 事業本部　NSM 技術研究室　三浦 邦威

１．はじめに

インターネットの普及にともない、EC(Electronic Commerce）サイトを代表として、24時間サービスを提供する必要のある公開システムが急増している。RAS（Remote Access Service)、VPN（Virtual Private Network）の普及により、イントラネット、エクストラネット環境のシステムにおいても同じことがいえる。しかしながら、現実にはサービスダウンが多大な経済と信用の損失につながる一部のシステムを除けば、24時間のサービス提供を保証するシステム、もしくは運用体制を整備することは、費用面の折り合いで困難であると推測する。ノンストップなサービス提供を保証することが難しいとしても、サービス提供が不可能となった際には、深夜であろうとも可及的速やかに対応できる体制を整備することが要求される。システムの24時間の稼動監視に頭を抱えているシステム運用関係者は、さぞかし多いことと思われる。

本レポートでは、NSM（Networked Systems Management）サービスの１つである、監視サービスを提供するために構築された「統合監視システム」を紹介する。特に24時間稼働が要求されているシステムの運用に問題を抱えている運用関係者の方には、問題解決に向けての参考としていただくと共に、監視サービスの利用を検討していただきたい。

２．監視システム

本章では、統合監視システムの構成要素となる「監視システム」について説明する。

監視システムとは、監視対象の状態をチェックし、監視対象上に発生した事象や記録すべき状態変化（イベント）を通知する機能をもつアプリケーション・ソフトウェア（監視アプリケーション）によって実装されたコンピュータシステムの総称とする。

監視システムは、監視対象の担当エンジニアによる対応のトリガーとなるシステムであり、システム運用管理において、監視システムの構築は必須である。監視システムにより、システム障害の予兆を検知して、エンドユーザーへの影響を未然に防ぐことができる。監視システムが構築されていない場合には、エンドユーザーからのクレームが対応のトリガーとなることが多く、正しいシステム運用管理を怠っているといっても過言ではない。

2.1　監視アプリケーションの監視形態

１つの監視アプリケーションでサポートできる監視対象項目は限定される。そのため、システム環境内には数種類の監視アプリケーションが複雑に共存して構築された監視システムが存在し、さまざまな体制によって運用されているのが現状である。監視項目と主な監視アプリケーションを表１に示す。

監視アプリケーションの監視形態はさまざまであるが、代表的な２つの形態を図１に示す。１つは、標準的な仕組みを用いて監視対象からイベントを検知する能動型の形態（図１左）である。もう１つは、イベント検知機能をもつ監視エージェントと、通知／管理機能をもつマネジャーで構成される受動型の形態（図１右）である。いずれにおいても、通知機能をもつものを監視マネジャーとし、監視マネジャーの動作するコンピュータを監視用コンピュータと定義する。

表1　監視項目と主な監視アプリケーション

監視項目	監視アプリケーション
システム	Windows NT パフォーマンス・モニター
ネットワーク	HP OpenView
ハードウェア	Compaq Insight Manager, IBM NetFinity Director/Manager,
ネットワークサービス	FreshWater SiteScope、Sirius Netkids iMark
アプリケーション	専用の管理ツール（Exchange リンクモニター等）

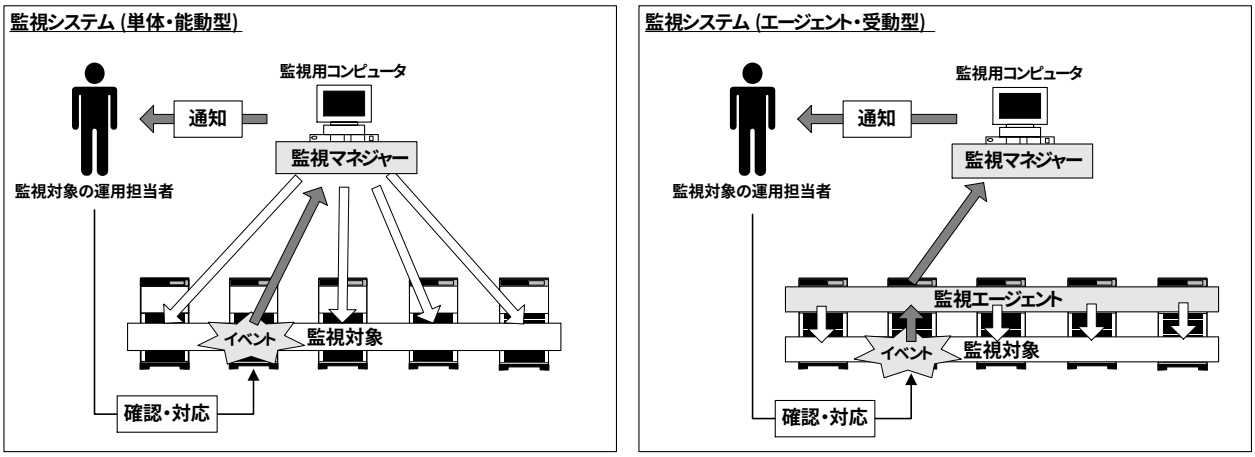

図1　監視システムの２つの形態

３．NSM サービスにおける監視サービス

当社では、システム運用管理のトータルサービスを「NSM サービス」として提供している。監視サービスは、NSM サービスの構成要素の１つである。

3.1　監視サービスの特徴

監視サービスでは、人間系によるシステム監視を行い、発生イベントをリアルタイム、かつ確実に伝達することを保証する。顧客のシステム環境に構築された監視システムでのイベント検知状況を、絶えず担当者(監視オペレータ)が監視し、イベント検知時にはイベント発生元の管理者や運用担当者などの、しかるべき連絡先へ確実に連絡を行う。

⑴　通知受信の確実性

検知したイベントの通知を自動的に発信することは、監視システムでも実装可能な機能である。しかし、あくまでも人間系でのサービスに頼る理由は、通知を受ける側に起因する。

監視システムでは、担当者への自動通知を実行する手段として電子メール、ポケットベル、SNMP(Simple Network Management Protocol) Trap などを備えている。しかし、これらは通知を受けるべき人物が、イベントを確実に認知したことを保証するものではない。電子メールサーバーの障害等による未通知やポケットベルの不携帯など、受信者側の諸事情により通知を受信、および認知できない状況であった場合には、無意味なものとなってしまう。通知先を複数名に設定することで、受信の可能性を高めることはできるが、やはり、受信認知を保証するものではない。かえって、複数名の受信者によって混乱を招く可能性も少なくない。

イベントが発生した際に、担当者による対応の第一歩が迅速に踏み出されることが監視サービスの使命である。電話という人間系手段によって通知を行い、担当者がイベントを認知したことを確認することが重要なのである。

⑵　費用対効果を発揮

監視専任のエンジニアを24時間体制で配備するには膨大な人件費がかかるため、一部のシステムを除いては費用対効果が見込めるはずもない。

それでも、システム導入初期のようにイベントが頻発する段階においては、24時間体制で監視を行うことの費用対効果は十分に見込める。しかし、イベントに確実に対応して消化し、構成変更などを順次行っていくことでシステムは次第に安定してイベント発生が減っていくものである。しかし、どんなに安定したシステムでも、イベントが発生する可能性が０％になることはなく、監視を継続する必要がある。さらに、監視をシステムの自動通知のみに頼ることは、リスクが高いことは前述のとおりである。たとえイ

ベント発生頻度が年に数回まで減少しても、担当者は監視システムが正常に動作していることを確認し、通知が確実に受信できる環境を維持しなければならない。いつ発生するか分からないイベントを拾うために、半永久的に単調な作業を続けていくのである。

本来、システム管理者は、想定したイベントへの最良の対処方法を策定したり、イベントが可能な限り発生しない安定したシステム運用を考えることに、その業務の重点を置くべきである。そのためには、監視コンソールの常時確認を行い、問題のあるときには連絡してくれる代理監視人が必要である。その役割を担うのが監視オペレータである。監視サービスでは、複数の顧客システムの監視を一元的に行うことで、人的リソースの効率化を実現し、高い費用対効果を発揮している。

⑶ イベントの一元管理

複数の監視システムが、１つの顧客システム環境に共存している場合、それらの間に混乱が発生してしまうことがある。例えば、ネットワークが切断された際には、ネットワーク監視システムがイベントを検知してネットワーク担当のシステム管理者へ通知を行う。さらに、派生したイベントが他の監視システムでも検出され、それぞれの管理者への通知が発生する。もし、各監視システムが独立して動作していれば、情報が錯綜して無駄な作業が発生してしまうことになりかねない。この問題を解決するには、複数の監視システムのイベントを一元的に管理する仕組みが必要である。

イベント管理アプリケーションは、複数の監視システム間のイベント関係を整然と定義し、統一の GUI（Graphical User Interface）から一元管理することができる。システム管理者は担当範囲のグレーゾーンを意識する必要がなくなり、監視オペレータは異なる監視コンソールのオペレーション方法を理解する必要がなくなる。

3.2 監視サービスと、他の NSM サービスとの関連性

NSM サービスのラインアップの中で、監視サービスと直接的に関連するサービスに、ハウジングサービスと SE（System Engineer）サービスがある。それぞれの概要は以下のとおりである。

・ハウジングサービス

システムに配慮した設置場所を提供するサービスで、高いセキュリティの確保された空間と冗長性のある電源を提供する。監視サービスと併せて提供する場合は、オペレータによる手順化された一次対応（リブート等）が可能になる。

・SE サービス

顧客の情報システム環境を運用代行するサービスであり、システムの障害対応、構成変更、メンテナンスなどの運用作業を提供する。監視サービスと併せて提供する場合は、イベントはシステムの担当 SE へ即座に通知され、迅速に適切な対応が行われる。

それぞれのサービスは、もちろん単体でも提供しているが、NSM サービスでは各サービスを連携させたシステム運用管理のトータルサービスを理想としている。

４．統合監視システム

統合監視システムは、顧客の情報システム環境にある複数の監視システムを集中管理し、24時間待機の監視オペレータを配備して、イベント発生時には監視対象の運用担当者に確実に通知することを目的に構築された、NSM サービスの中核システムである。

4.1 TME10 Enterprise Console の概要

統合監視システムでは、統合管理アプリケーションである TME10（Tivoli 社）のイベント管理アプリケーション「TME10 Enterprise Console（TEC）」を使用している。TEC は、さまざまな監視対象で発生するイベントのフォーマット統一と収集を行って一元化し、効果的な処理を実現している。

TEC では、まず監視対象に分散配置したイベントアダプターで情報を収集し、中央のイベントサーバーが情報を集約して処理し、分散イベントコンソールが監視オペレータ／管理者に情報を通知する。以下に、各コンポーネントについて説明する。

⑴ TEC イベントアダプター

イベントアダプターは、監視アプリケーション（情報ソース）からのイベント収集やローカル・フィルター処理、TEC で使用できる形式へのフォーマット変換、および中央のイベントサーバーへ送信を行うソフトウェア・プログラムである。

TEC のイベントアダプターは、OpenView 等の管理アプリケーション固有のアダプターや汎用のログファイル・アダプター、Windows NT イベントログ・アダプター、SNMP アダプターなどから構成される。また、TME10の基本セットである TME10 Framework がインストールされていないコンピュータにインストール可能な、非 TME イベントアダプターも用意されている。

⑵ TEC イベントサーバー

イベントアダプターから送信されたイベントを受信して、処理を行う中央サーバーである。イベントサーバーは、着信イベントごとにデータベース・エントリを作成し、ルールセットを参照してイベントの評価を行って対象のルール（事前に定義されたタスク）を実行する。また、現行のイベント情報によるイベントコンソールの更新を行う。

⑶ TEC イベントコンソール

監視オペレータが使用する GUI を提供する。利用者は、用途に合ったイベントビューを使用することができる。

4.2 統合監視システムでの TEC の実装

各監視システムの監視マネジャー上に TEC イベントアダプターをインストールすることにより、監視システムが検知したイベントを統合監視することが可能になる。統合監視システムにおける、TEC によるイベントの一元管理の仕組みを図２に示す。

4.3 統合監視システム環境構成

統合監視システムの環境構成を図３に示す。図中の各顧客環境については、現状を示すものではなく接続のイメージである。図３に記載されている用語を以下に解説する。

・統合ネットワーク

NSM サービス環境として新川事業所に構築された､ネットワーク・セグメントである。顧客システム環境とネットワークを介して接続され、遠隔で NSM サービスを提供する。NSM サービスの中枢を担っており、監視サービスのみを提供するための環境ではない。

・TMR サーバー

TMR（Tivoli Management Region : TME が稼働しているシステムセットの管理単位）を管理するコンピュータ。Windows NT 環境のドメイン・コントローラのようなものである。

・TEC サーバー

TEC イベントサーバーが動作するコンピュータ。

・監視オペレータ用 TEC コンソール

イベントの一次対応を行う監視オペレータが使用するイベントコンソール。全ての監視システムのイベントを表示する。

・SE 用 TEC コンソール

システム運用を担当する SE が使用するイベントコンソール。担当する顧客の監視システムのイベントを表示する。

・ファイアウォール

統合ネットワークと顧客ネットワーク間に設置しているセキュリティ装置｡「統合ネットワーク内の IP アドレス」と「顧客ネットワーク内の IP アドレス」間のサービス提供を行うのに必要な通信のみを許可するよう、セキュリティ・ポリシーを設定している。また、NAT（Network Address Translation）機能を使用して統合ネット

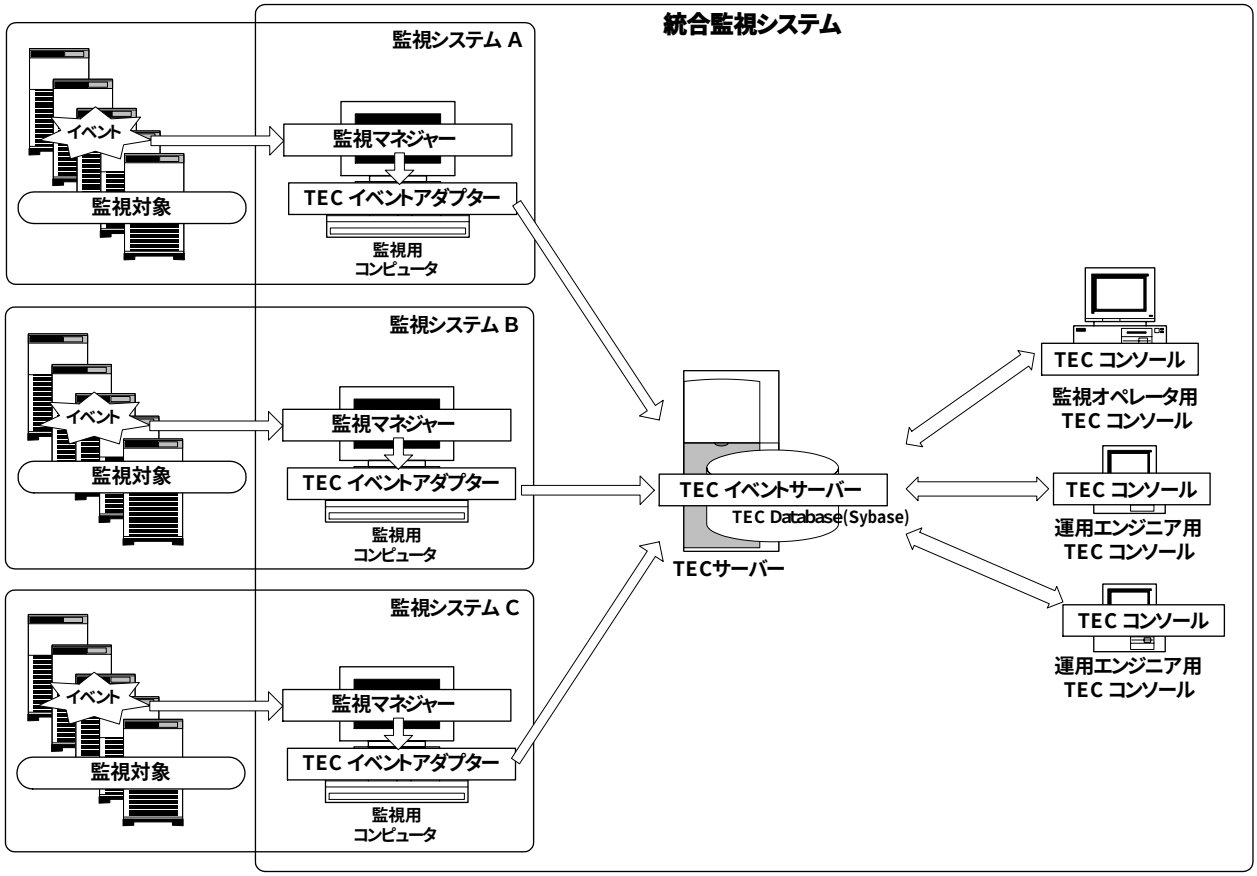

図２　TEC によるイベントの一元管理

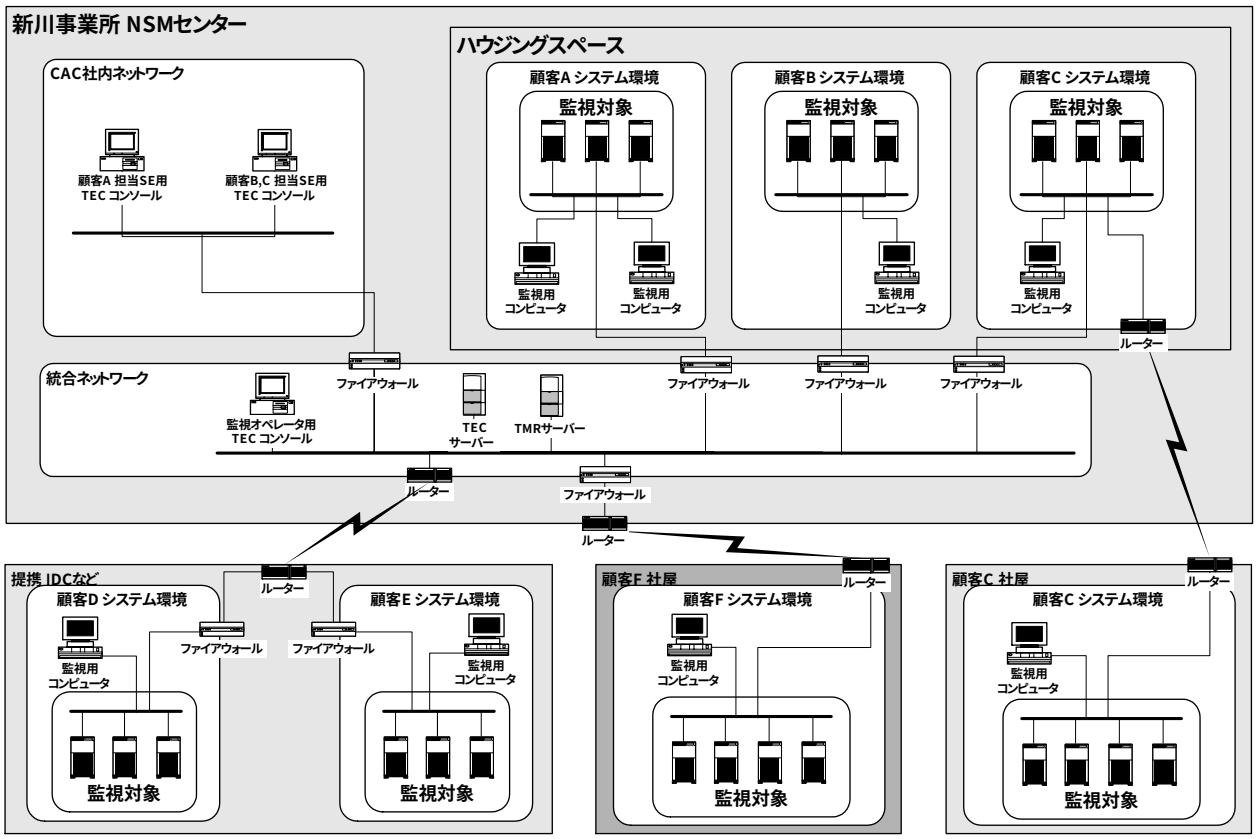

図3　統合監視システムの環境構成

ワーク・アドレスを顧客ネットワーク・アドレスに変換している。そのため、TEC イベントでは、TEC イベントサーバーとしてファイアウォールの顧客ネットワーク・アドレスを設定することになる。

・監視用コンピュータ
監視システムの監視マネジャー、および TEC イベントアダプターが動作するコンピュータ。

・監視対象
顧客情報システム環境内の監視対象項目。

4.4　イベント検知フロー

NT イベントログ・アダプターを例に、イベントの検知フローの流れを以下に説明する。図4のソフトウェア・コンポーネントと合わせて参照されたい。

①監視システムがイベントを検知したら、監視マネジャーは監視用コンピュータ内の NT イベントログ（アプリケーションログ）にイベント情報を書き込む。

②NT イベントログ・アダプターは、指定された設定内容にしたがって、対象イベントログの書込みを定期的にモニターしている。新しいイベントログ・エントリがあれば、フォーマットファイルに設定された内容にしたがって、TEC フォーマットに変換して TEC イベントを生成する。フォーマットファイルでは、通知するイベントと TEC イベント属性の値を指定する。NT イベントの各属性と TEC イベントとのマッピング、“顧客”属性に顧客名を指定している。

③イベントアダプターは、TCP／IP 標準プロセス通信を使用しており、指定されたイベントサーバー、ポート番号に生成された TEC イベントを送信する。

④TEC イベントサーバーは、受信したイベント内容とルールセットを参照して、実行すべきルールがある場合に実行する。ルールで指定できるアクションは次のとおりである。

・受信イベントの属性の変更
イベントの重大度、ステータスを変更することができる。

・他のイベントの属性変更
例えば、回復イベントの受信にともない、障害イベントをクローズする。

・重複イベントの表示の防止
同一イベントが定期的に発生して監視システムでコントロールできない場合などに使用する。

・アプリケーション、またはスクリプトの実行
通知、リカバリ・プログラムの実行、障害管理書の自動作成等を行う。

・イベントの廃棄

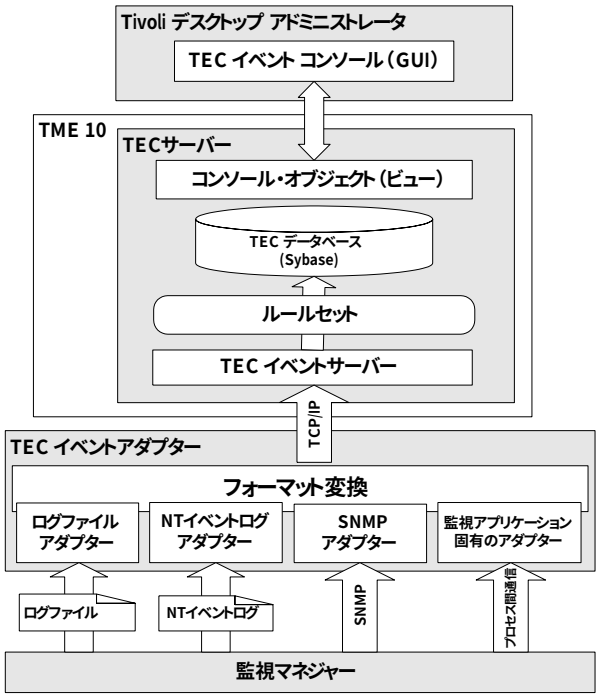

図４　ソフトウェア・コンポーネント

・イベントの相関比較
あるイベントが複数のイベントを引き起こすことが分かっている場合に、イベントの重大度の格付けやクローズを実行できる。
・新規イベントの作成

⑤TEC イベントサーバーは、TEC イベントをデータベース・エントリとして TEC データベースに格納する。

⑥TEC イベントサーバーは、イベントコンソール・オブジェクト（ビュー）を更新して、接続している TEC コンソールをリフレッシュする。ここで、監視オペレータは、イベントコンソールに新たに表示されたイベントを検知する。

4.5　監視オペレータによる一次対応

監視オペレータは、24時間365日待機してイベントに対応する。監視オペレータ用コンソールには、表２のように複数顧客、複数システムからのイベントが表示される。

原則として、監視オペレータからの一次対応は電話での担当者への連絡となる。顧客名、ソース(監視システム名)、ホスト名などから、あらかじめ取り決められた連絡先リスト（イベント発生システムの運用関係者）の優先順位にしたがって電話連絡を行う。図５にイベント発生／検知からオペレータによる通知、さらに運用担当者の対応にいたるまでの流れを示す。以下の説明と合わせて参照のされたい。

①監視用コンピュータがシステム環境に発生したイベントを検知する。

②監視用コンピュータは、連絡の必要のある（フィルターされなかった）イベントであれば、情報を TEC に送信する。

③パトライトを点灯して、監視オペレータへ新規イベントの着信を通知する。

④監視オペレータはイベント情報を確認し、イベントに対する一次対応アクション（この場合は電話連絡）を確定する。

⑤あらかじめ作成した連絡リストの運用担当者に電話連絡を行い、イベント情報を伝える。第一連絡先につながらない場合には、リストに基づいて順次連絡を試みる。

⑥連絡を受けた運用担当者がイベントの対応責任者となり、現状確認、内部連絡、エンドユーザーへの連絡／対処、障害対応／復旧等が行われ、運用体制で取り決められた責務を果たす。

連絡を無事に終え、イベントステータスを受付済（Ack）に変更することで、監視オペレータの任務は完了する。電話連絡を終えた後の対応については、監視サービスの範疇を越えるところであり、それぞれの運用体制／方針に依存するところである。しかし、万全を期すには、⑤を補填して、連絡リストに記載された全て運用担当者に連絡が付かなかった場合に、オペレータがどう対処すべきかを、あらかじめ取り決めておく必要があるだろう。例えば、「10分起きに再コール」や「留守番電話に伝言する」などが考えられる。

TEC ルールでは、電話不通時のバックアップ、および詳細なイベント情報を正確に伝えることを目的として、複数の運用担当者への電子メール通知を併用している。この場合には、受信者の内で、監視オペレータから最初に電話連絡を受けた者が、そのイベント（障害）についての対応担当者となる。言わば、オペレータが担当者をアサインする役割も担っているのである。

表２　監視オペレータ用コンソールのイメージ

重大度	顧客名	時刻	ソース	ホスト	説明	ステータス
Fatal	顧客 B	4/01 02:43	SiteScope	Host_a	Disk C>95%	Open
Critical	顧客 C	4/01 00:05	OpenView	Host_b	Node down	Ack
Critical	顧客 D	3/31 21:02	SiteScope	Host_c	FTP service not found	Ack
Warning	顧客 D	3/31 19:44	Insint Manager	Host_d	Disk(5)error	Close
Warning	顧客 A	3/31 18:53	PerfMon	Host_e	MTA Queue>30	Ack

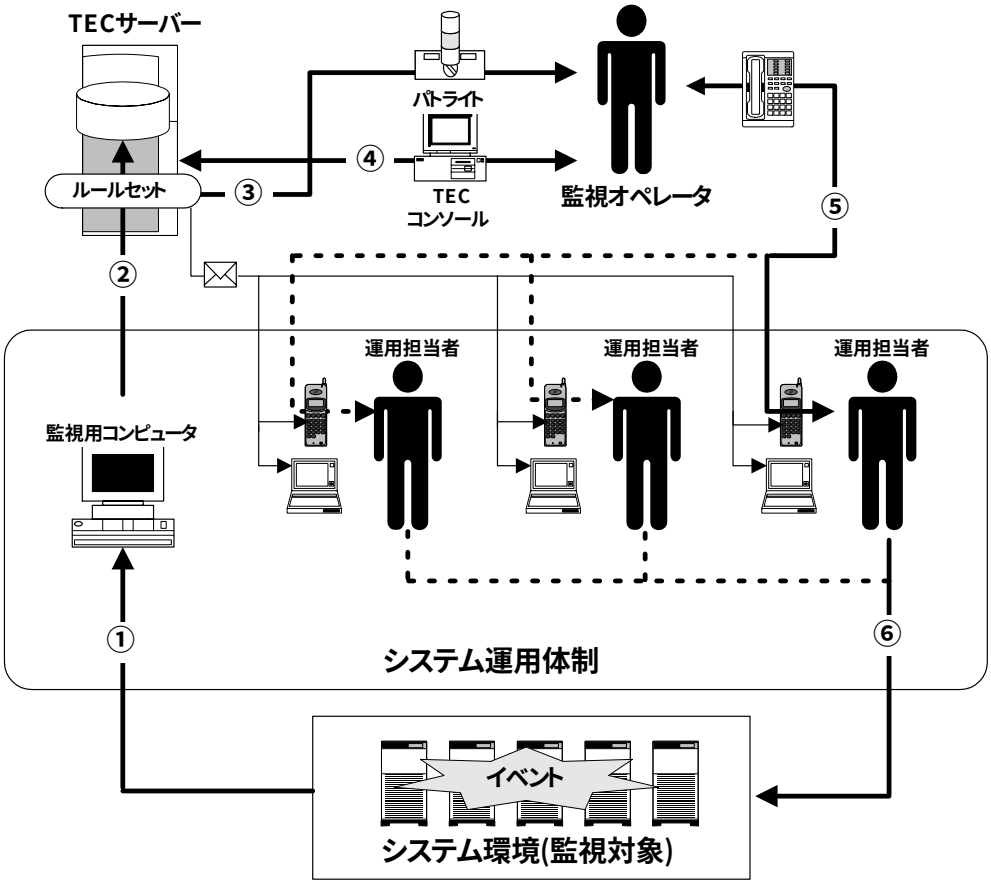

図５　イベント処理の流れ

５．統合監視システムへの統合プロセス

本章では、運用中の既存システムにNSMサービス（監視サービス）を適用する場合のポイントを、導入プロセスに基づいて説明する。

5.1　NSMサービス導入の検討から決定

NSMサービスの導入にあたって、顧客ネットワークとNSMセンターとのネットワーク接続が必要となる。回線の接続形態と速度は、導入するサービスの組合せによって異なる。監視サービスのみを導入した場合は、「図３の顧客F」のような接続形態となる。この形態では、ネットワーク・トラフィックはイベント通知のみとなるので、一般に提供されている最も低速な回線でも十分に要件を満たせる。

5.2　監視システムの構築

顧客環境内に監視システムを構築する必要がある。しかし、運用対象が新規システムでなければ、たいがいにおいて監視システムは既に構築されている。その場合には、TECイベントアダプターが動作する監視マネジャーのプラットフォームと、使用可能なアダプターを確認する必要がある。使用可能な非TMEイベントアダプターを表３に示す。

プラットフォームがWindows　NTの場合は、あらかじめフォーマットが定められているイベントログが、最も実装（フォーマットファイルの作成）が容易であり、可能な限りこれを採用している。また、監視用コンピュータの致命的な障害時（システム起動不可等）の対応体制（代替機の準備等）についても、この段階で考慮しておく必要がある。

表３　使用可能な非TMEイベントアダプター

プラットフォーム	アダプタータイプ
WindowsNT	イベントログ ログファイル SNMP
AIX, HPUX, Solaris, SunOS サポートするOSバージョンについては要確認	ログファイル SNMP HP OpenView SunNet Manager

5.3 通知イベントの決定

監視オペレータによる電話連絡や暫定対応が不要なイベントは、TEC に送信する必要がない。そこで、監視アプリケーションによって検知される全てのイベントの中から、TEC サーバーに送信すべきイベントのみをリストアップし、これに基づいて TEC イベントアダプターでフィルターをかけて発生イベントを選別する。

5.4 イベントに対応する連絡先リストの作成

通知が必要なそれぞれイベントについて、連絡先リストを作成する。さらに、全ての連絡先に連絡が失敗した場合や、リアルタイムでの対応を必要としないレベルのイベントへの対応方法を取り決めておく必要がある。例えば、バックアップ失敗やファイルシステムの使用率（80%超）など、性急な対応を必要としないイベントについては、「深夜の時間帯の連絡は避ける」指定をするなどの配慮を行う。

5.5 統合

・ネットワーク回線の接続
5.1項において決定したネットワーク回線の接続と、要件に応じてファイアウォールの設定を行う。
・監視アプリケーションの設定変更
使用するインタフェースにイベントが通知（NT イベントログへ書込みなど）されるように設定変更する。
・監視用コンピュータへ TEC イベントアダプターをインストール／設定決定事項から作成したフォーマットファイル、アダプター設定ファイルを使用する。

以上までの完了で、TEC サーバーでイベントが受信可能になる。

5.6 TEC コンソール・オブジェクト(ビュー)の設定変更

統合された監視システムのイベントが、監視オペレータ用 TEC コンソールに表示されるようにコンソール・オブジェクト設定する。

以上で監視システムの統合が完了し、監視システムがイベントを検知すると監視オペレータ用 TEC コンソールにイベントが表示されるようになる。

６．統合監視システムの監視

監視システムを統合することのデメリットとして、システムが複雑化することで障害が発生する可能性が高くなる（イベントの受信精度が低下する）ことが挙げられる。

また、統合監視システムは24時間サービスを提供する必要がある。そのため、統合監視システムの監視を行うための監視システムを別途構築している。この監視システムでは、各監視マネジャーの通知イベントが、監視オペレータ用コンソールに表示されるまでの各プロセスを常時監視している。統合監視システム環境でイベントが発生した場合は、警報装置で同フロアにいる監視オペレータに通知を行う。

７．おわりに

本稿では、NSM 監視サービスのバックボーンとなる統合監視システムについて紹介した。実際の付加機能については、漠然と「監視システム」として紹介した。今後、より多く監視システムが統合されるにつれ、このシステムは効果的に機能していくことになる。

2000年８月からサービス提供を開始したこのシステムに、現在までに８顧客11監視システムが統合されている。そして、既存の監視システム統合の他に、監視システムの構築を含めたネットワーク・サーバー稼働監視サービス、WWW サーバー・パフォーマンス監視サービス、不正アクセス監視サービスの統合を推進している。それらの詳細については、また機会があれば紹介したい。