ICTシステムのサイレント故障・予兆監視

NEC・クラウドプラットフォーム事業部・主任　西川　昌利

ICTシステムが提供するサービスの範囲の拡大に比例して運用管理コストも増大している。企業としてはビジネス拡大のために更にサービスの拡大を行いたいが、運用コストが足かせとなっており、これまでのメッセージ発生を契機に対処を行うリアクティブな運用からサイレント故障や予兆を監視するプロアクティブな運用の実現が求められている。
本稿では、サイレント監視・予兆監視の手法とそれを実現するNECのインバリアント分析技術について紹介する。

1　ICTシステム監視の目的と課題

ICTシステム監視の目的は、ICTシステムが提供するサービスの継続性を向上し、サービスのダウンタイムを短縮、サービス低下を防止することにより、機会損失の抑止や社会的信用を維持することである。しかし、従来の運用監視の仕組み（事象を想定した単体での監視）では、サービス影響につながるすべての事象を検知できておらず、このようなサイレント故障により、サービスに影響を与えてしまっていることが多く見受けられる。

とくに昨今のICTシステムは、サービス範囲の拡大や仮想化・クラウドの普及により複雑化しており、監視項目が増大・多様化し、従来のICTシステム監視ではサービスダウンにつながる事象の網羅度は更に低くなっている。

2　サイレント故障の要因

従来の運用監視に内在するサイレント故障の要因について、以下に示す。

監視の仕組みは＜図１＞に示した通り、監視対象の情報収集、収集した情報の分析、分析結果の可視化の３つの機能に分けられるが、従来の運用監視には、それぞれの機能において、サイレント故障につながる要因が内在する。

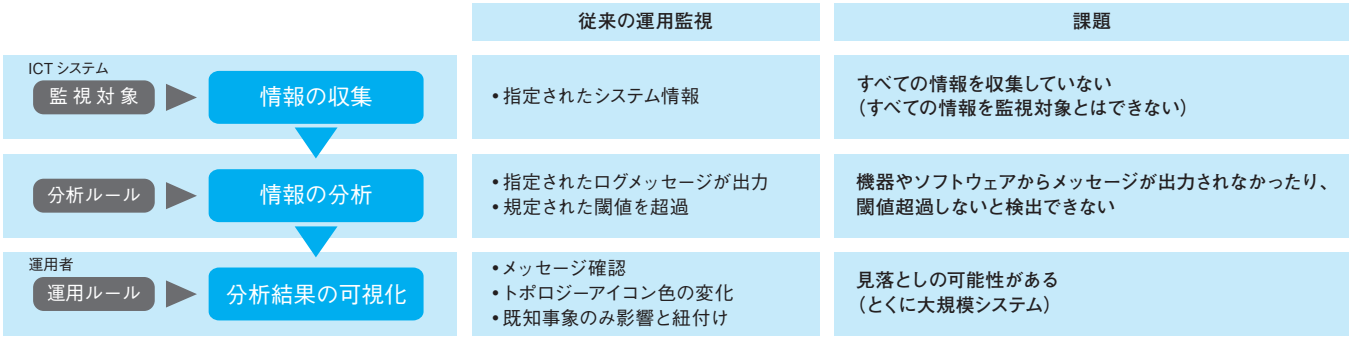

図１　内在するサイレント故障の要因

①情報の収集不足
ICTシステムのすべての部位を監視対象とはできない。

②情報の分析不足
閾値の超過や既定したメッセージが出力されなければ、故障検知できない。

③監視の表現力の不足
監視対象数が多い、メッセージラッシュなどにより、見落としが発生する。

サイレント故障を低減するためには、それぞれの機能の課題を解決することが必要となる。

3　サイレント故障監視へのアプローチ

3.1　予兆監視とサイレント故障監視の定義

ICTシステムが提供するサービスへの影響を低減するためには、サイレント故障と故障予兆について検討する必要がある。＜図２＞

●サイレント故障

サイレント故障とはICTシステムの自己診断機能（あらかじ

め準備された監視機能)で検知できない故障を指す。ICTシステムの様々な情報をもとに検知(故障前兆を含む)する手法を自己診断機能に追加することで、サイレント故障を低減することができる。

●故障予兆

予兆とは何かが起こりそうな状態を指す。ICTシステムの挙動を観察し、普段とは異なる挙動を検知する。挙動の差異の原因を確認することで、サービス影響や故障個所を特定する。

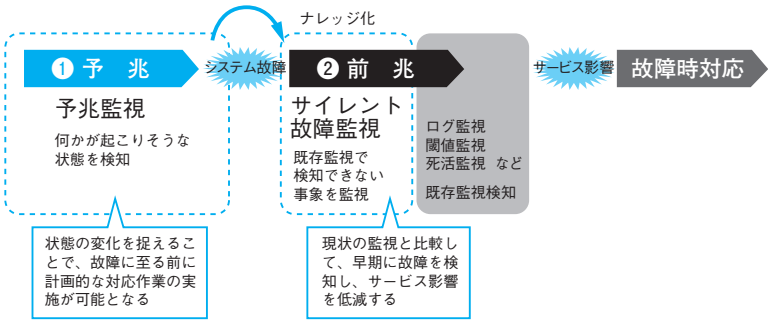

図2　サイレント故障と故障予兆

3.2　アプローチ方針

① 情報の収集不足への対応(サイレント故障の監視)

監視を行うには少なからず監視対象のリソースが利用されることから、必ずしもすべての部位が監視できるわけではない。このため、現在取得している性能値やメッセージなどから類推し、故障と紐付けて監視する必要がある。

例えば、A→B→Cと流れる処理があり、Bの監視を行っていないとする。この場合Bで故障が発生しても、サイレント故障となるが、Aの処理が行われた後にCの処理が行われないことをBの故障として定義することにより、Bの状態を監視することができる。

② 情報の分析不足への対応(予兆の確認)

①に示したような監視はシーケンスや構成を把握しているなど既知の事象に対しては、監視に組み込むことが有効であるが、逆に未知の事象に対しては定義できないという課題がある。また、ICTシステム構成やシーケンスに変更があった場合、事象の関係性を見直す必要がでてくる。

事象との紐付けやICTシステムの構成、サービスシーケンスを一旦無視して、すべての情報をもとにその関係性をモデル化し、挙動の変化を網羅的に監視する。挙動の変化を検知後にその原因を確認する運用を合わせて行うことを推奨する。

③ 監視の表現力不足への対応(可視化)

現状でも見落としはあるが、②を監視に組み込むと、監視対象が増加し、現状のメッセージとしての監視では見落としてしまうリスクが増加する。また、見せかけの関係性も取り込んでモデル化してしまい誤報となることで、運用者が注意して見なくなってしまう。このため、これまでのメッセージベースではなく、関係性の崩れ方の円グラフでの表現や、その集中度合をマップ表示させるなどの工夫が必要となる。

3.3　運用イメージ

現状のICTシステム監視は監視メッセージと事象が紐付いたものとなっている傾向にあるが、上記②の運用は紐付いたものにはならず、現状の監視運用には適合しない。このため、システムアセスメント運用を新設し、②の監視を実施。そこで故障と定義できた事象を①で監視することにより、現状の監視に適合させる。<図3>。

②での確認は、AI技術を適用し、確認手順をナレッジとして学習させることにより、故障判断もシステム化することができるようになるが、十分なナレッジが蓄積できるまでの間は、人間系で故障判断を行うことが必要となる。(故障判断のシステム化については、ICTシステム情報の内容やその標準化度合に依存するため、本稿では割愛する)

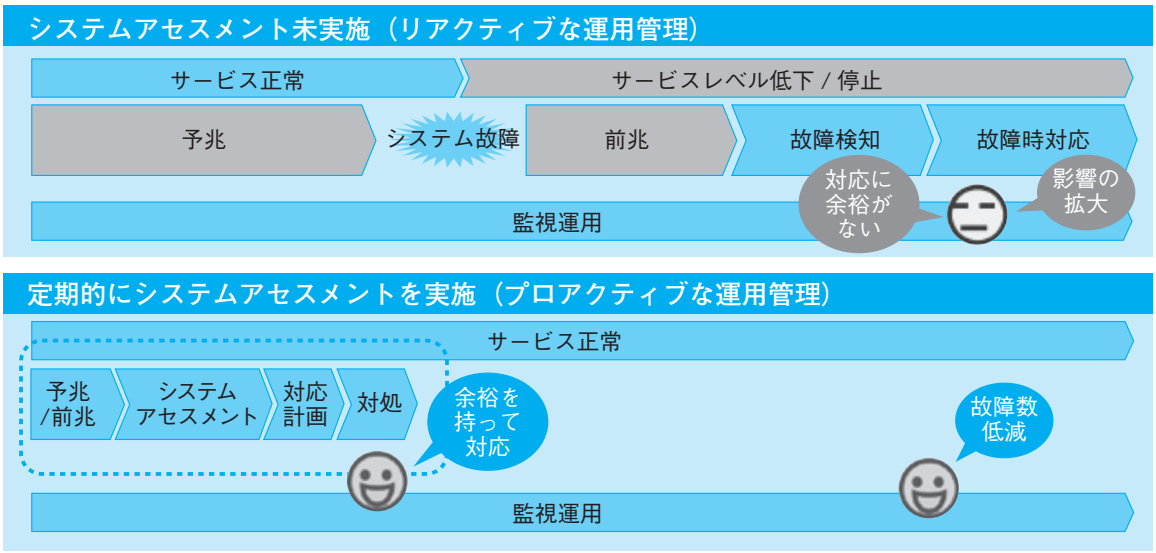

図3　サイレント故障を監視する運用

4　インバリアント分析技術

4.1　技術紹介

NECでは、ビッグデータ分析技術の1つとして、インバリアント分析技術（System Invariant Analysis Technology：以下SIAT）を開発し、ICTシステムのサイレント故障監視・予兆監視を実現するInvariant Analyzerとして製品化した。SIATの主な分析技術は以下の通りである。

●モデルの作成

性能情報などの時系列に並んだ数値データを入力することで、数値データ間にある不変的な相関関係（インバリアント）を自動的に抽出し、それぞれの関係性をy= f（x）の形式でモデル化する。＜図４＞

●挙動変化の検知

現在のデータや分析対象となる期間のデータを上記のモデルから予想される挙動と比較し、関係性の崩れを挙動変化として検知する。＜図５＞

SIATにICTシステムの性能データを入力することで、ロードバランスされた個々のサーバーのリソース使用状況の関係性（分散状態）やトランザクション量とCPU使用率などの間に成り立つ関係性の変化を監視することが可能となる。

また、Invariant Analyzerには、ICTシステムの利用特性（平日と休日など）に応じてモデル作成をアシストする機能＜図６＞や過去の挙動変化をナレッジとして登録する機能＜図７＞を具備することで、誤報の低減や原因の特定を強力に支援する。

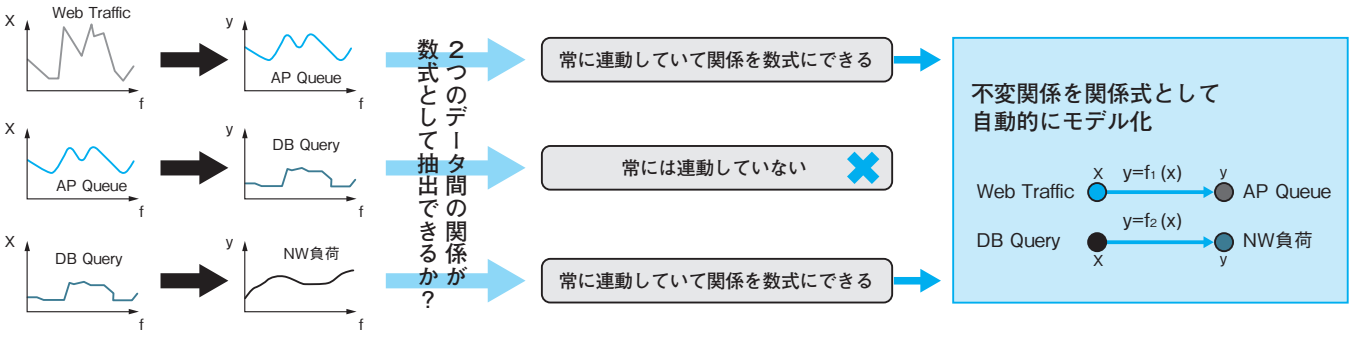

図４　相関モデルの作成

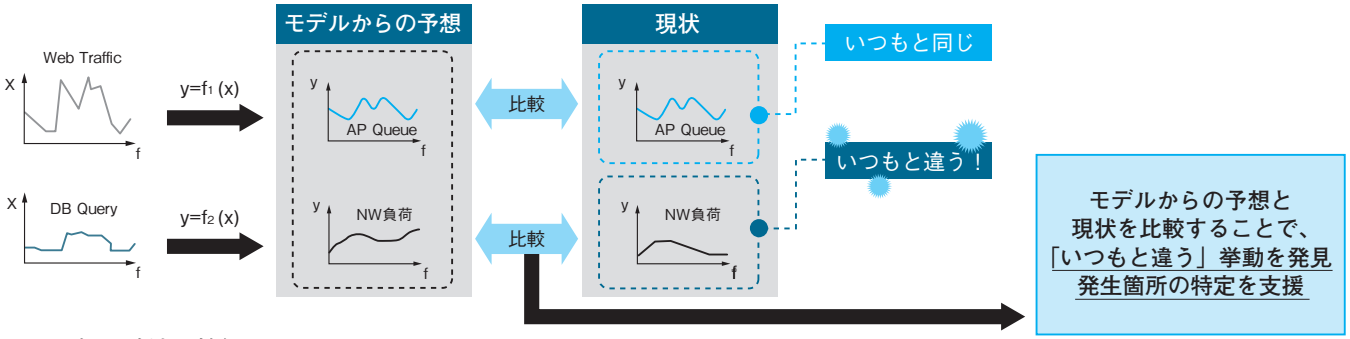

図５　相関破壊の検知

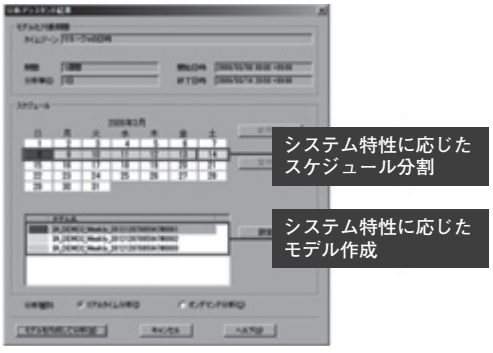

図６　モデル作成アシスト機能

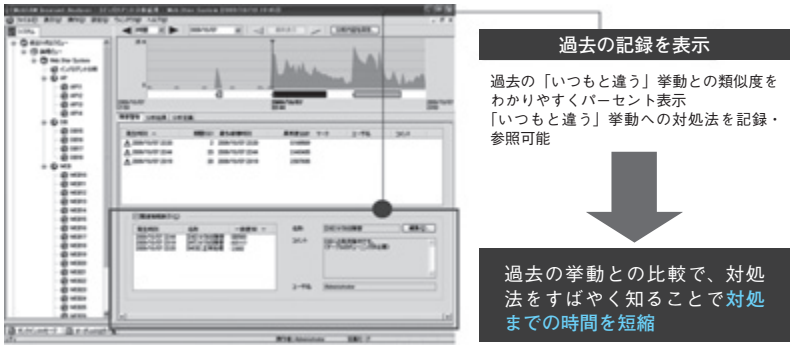

図７　ナレッジ機能

4.2 従来監視との比較

以下に従来の監視とSIATを利用した監視との比較を示す。ただし、SIATでの監視で従来の監視で検知できた事象を網羅できるわけではなく、従来の監視とSIATを利用した監視を併用することで、ICTシステムの監視品質を向上する。（性能情報をもとにした監視の比較。ログ監視や死活監視は割愛）

●ベースライン監視との比較

ベースラインは個々の測定時間ごとに取り得る値の範囲を学習するため、モデル作成までに長期間（最低でも数週間程度）を要する。対して、SIATを利用した監視は、性能情報間の関係性を見ることから、最低100ポイントのデータ（1分単位のデータであれば100分間）があれば十分に高い精度のモデルを作成することが可能であり、モデルの劣化時など、再作成の影響が少ない。

イベントなどで一時的にICTシステムの負荷が増大する場合、ベースライン監視では正常に稼働していても誤報となるが、SIATでは関係性を監視しているため、正常に稼働していれば負荷が増大しても誤報とはならない。

また、ベースライン監視は個々の監視項目の挙動を監視するものであり、監視項目以外の事象について検知できない場合がある。

●閾値監視との比較

閾値監視は上限、下限値を設定することで、危険な水準に達した場合に検知することが可能であるが、下限値に関しては、閑散時間帯を加味しなければ、誤報となる可能性がある。

また、監視項目ごとに閾値を設定する必要があり、項目に合わせて閾値を調整するような場合はメンテナンス性が低下する。

4.3 SIATを利用した監視例

例えば、個々の装置単位の受信パケット総計と送信パケット総計には強い相関関係があり、その相関関係を監視することにより、機器のリソース枯渇や間欠故障時などに発生する異常な破棄パケットの発生を検知することができる。（破棄パケットは通常時でも発生するため、そのカウンター情報を監視していても故障が検知できるとは限らない）

●従来の監視＜図8－①＞

ポート単位にパケット量の推移を監視しても閾値を超過していないため、故障を検知できない。

●ネットワーク監視ツールで、送受信パケットを集計して確認＜図8－②＞

装置単位の送受信パケットには強い相関関係があるため、グラフを重ね合わせて目視確認することで、相関関係の崩れを見つけることは可能。しかし、業務パケットと比較して、破棄パケットの量が少ないため、目視ではすぐに気づけない可能性がある。

●相関係数の変化を監視＜図8－③＞

相関度の強さを示す値として、相関係数がある。この相関係数の変化を確認することにより、グラフを重ね合わせただけでは見つけることができなかった微細な相関関係の崩れでも検知することができる。SIAT技術を導入したInvariant Analyzerにより、このような相関関係の崩れをリアルタイムで検知することが可能となる。

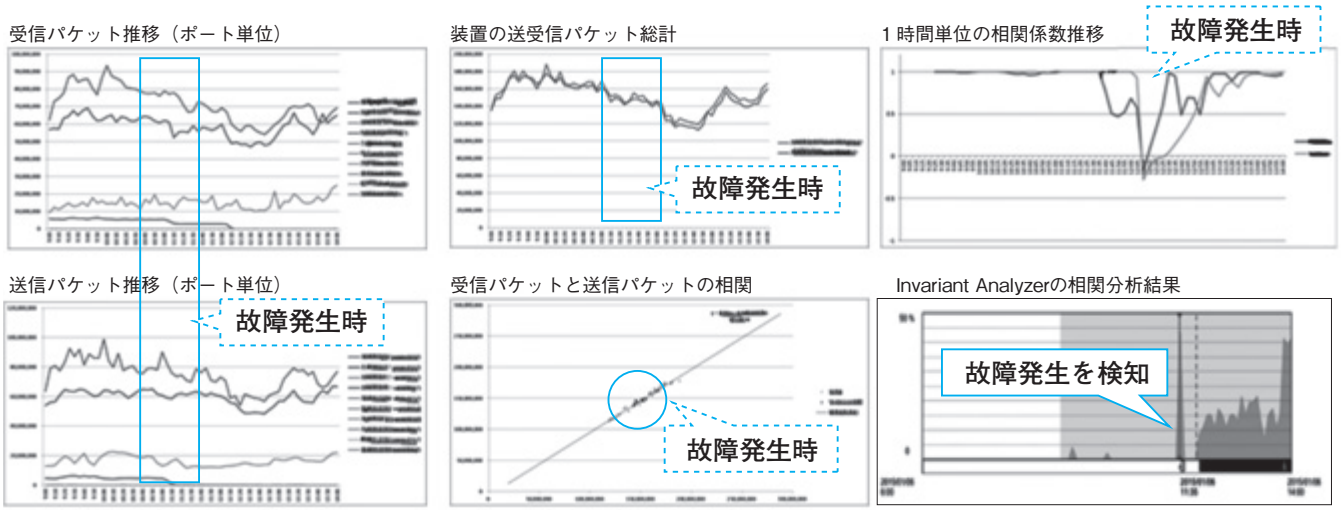

図8　相関監視の効果

5 分析事例

Invariant Analyzerでは＜表９＞にある通り、様々な業種のICTシステムにおいて既存で取得されているデータを用い、サイレント故障や障害予兆など従来の監視では見つからなかった故障を検知している。

No.1のWeb3Tier業務システムの分析事例について、詳細を以下に示す。

Web/AP/DBサーバーよりCPU、メモリ、ネットワーク、スワップ、ディスクなどの性能情報を取得。平常時をモデル化し、各性能データを分析。結果として、(ア) APサーバー処理遅延、(イ) DBサーバーへの負荷集中、(ウ)通常業務にないWebアクセスの発生を検知した。＜図10＞

6 今後の方針

6.1 分析対象拡大

ICTシステムの状態を示すデータとして、性能情報のほかにログメッセージやプロセス間通信やファイルのアクセスなどがある。NECはSIATでの性能情報の分析を始めとしてシステムから得られるあらゆる情報を活用し、ICTシステムの信頼性向上を支援する。＜図11＞

●ログメッセージの分析

とくに大規模システムにおいては、個々のICTシステム間に依存関係があるが、サイロ型に構築された結果、生成されるログメッセージは標準化されておらず、かつ大

表９　主なSIAT分析事例

No.	分析事例	分析データ	検知した異常	効果
1	Web3Tier業務システム	CPU、メモリ、ネットワーク、スワップ、ディスクの性能データ	• APサーバーの処理異常 • DBサーバーへの負荷集中 • 通常ではないアクセス発生	• 障害の検知 • 障害原因の絞り込み
2	Oracle DB分析 (1)	Oracle、OS、ネットワークの性能データ	• SQL実行回数の異常	• DB障害の検知 • 障害原因の絞り込み
3	Oracle DB分析 (2)	Oracle Statspackデータ	• Global Cacheの異常	• DB障害の検知 • 障害原因のSQL単位での絞り込み
4	NW分析	NWトラフィック	• トラフィック異常	• NW障害の早期発見 • 原因箇所のポート単位での絞り込み
5	NW・サービス性能分析	NWトラフィック、サービス要求／処理	• トラフィック異常 • 処理遅延	• サービス性能劣化の早期発見 • 原因箇所のサービス提供箇所単位での絞り込み
6	Netflow分析の検証	Netflowデータ	• スイッチ間ネットワーク負荷 • スイッチ間STP無効化 • ICMP大量投入	• NW障害の検知 • 障害原因のIPアドレス単位での絞り込み

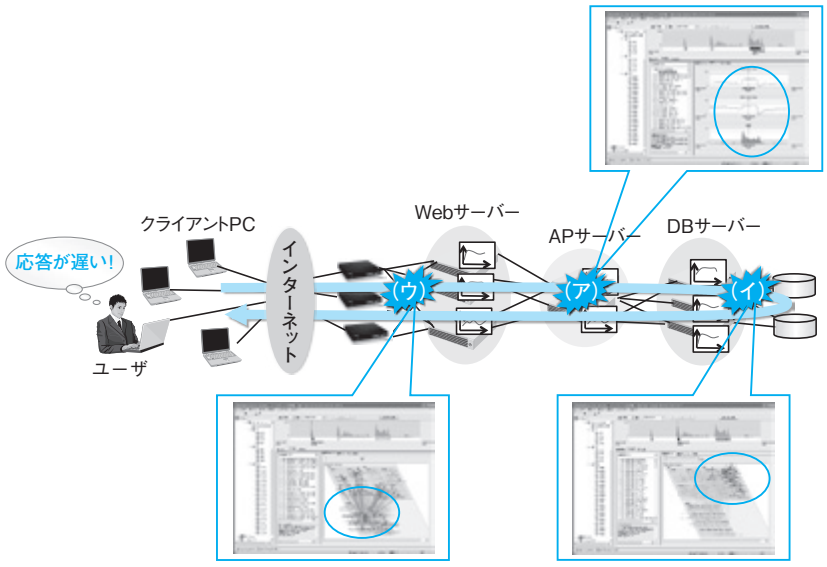

図10　Web3Tierシステムでのサイレント故障の検知事例

量であるため、予兆を含めた故障の見落としにつながるリスクがあった。

これらの大量かつ多種のログメッセージをオペレータが分かりやすい形に整理、可視化し、ログメッセージの各イベント間に成り立つ規則性を学習することで、既存の監視ルールでは見つけにくい故障の検知やその予兆を早期に検出する。

なおログメッセージの分析には以下が想定される。<表12>

●プロセス間通信、ファイルアクセスの分析

モデル対象となるログメッセージが出力されない場合や性能傾向に変化のない故障についてはSIATやログメッセージの分析を利用しても検知することが困難である。

プロセス間通信やファイルへのアクセスをモデル化し、挙動比較することで、SIATやログメッセージの分析で検知困難な故障や予兆を検知し、より高度な監視を実現する。

6.2 適用領域拡大

NECではますます複雑化・高度化する社会課題に対し、人とAIが協調しながら高度な叡智で解決する方針である。

SIATについては、インフラ／プラント・マネジメントとして発電所などの故障予兆監視を実現している。今後も様々な業種・業務へ適用領域を拡大していく。

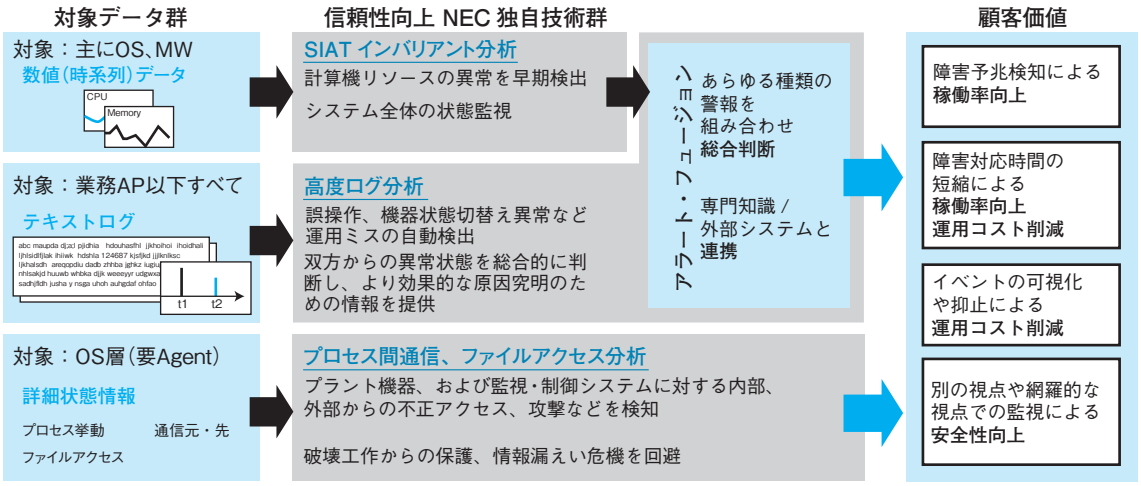

図11　あらゆる情報を活用したICTシステムの信頼性向上

表12　ログメッセージの分析例

	監視	予兆確認
エラーメッセージ抽出	エラーステータスのメッセージが出力されていないか確認する。	ワーニングを含めたメッセージの発生回数の推移を確認する。
処理抜け	通常発生するメッセージが出力されているか確認する。	同左。 メッセージが出力されていない原因を確認する。
通常異なるシーケンス	通常と異なるメッセージが出力されていないか確認する。	同左。 メッセージが出力されている原因を確認する。
戻り値	不正な戻り値がもどされていないか確認する。	同左。 戻り値の妥当性を確認する。
特定処理の追跡	シーケンスにそって処理を追跡し、異常や遅延がないことを確認する。	—
操作履歴	不正なオペレーションが実施されていないか確認する。	同左。 オペレーションによる異常がないか確認する。
トランザクション量確認（スループット）	処理の発生回数を確認する。	同左。 トランザクション量によるリソース利用状況を確認する。
処理時間の確認（TAT）	処理の開始から完了までを確認する。	同左。 処理遅延発生していないか確認する。

：一般的なログメッセージログ監視での分析　：特定部のみ監視されている分析