

効率的な障害処置順位や中央装置における障害予兆検知の 提案機能

阪神高速技術(株)技術部情報管理課 棚橋 卓也
阪神高速技術(株)技術部情報管理課 吉田 翔
阪神高速道路(株)神戸管理部施設工事課 原田 克彦

要 旨

阪神高速道路の安全・安心・快適な走行のために、道路上には情報提供や情報収集する設備や ETC 設備などの多種多様な電気通信機器と、それらのデータを処理し、管理する中央装置が 24 時間 365 日稼働している。

これら高速道路における基幹システムの障害は利用されるお客さまに対して、サービス提供の停止等の不便をおかけすることになるため、効率良く障害対応を行うためには、障害の兆候を早期に発見することが重要である。

本稿では、中央装置の稼働状況や各種統計情報を駆使し、平常時の計測データと比較することで異常値を見つける手法や、多種のアラームのなかから、処置の優先順位を示すことで効率的な補修運用を行った事例を紹介する。

キーワード： 障害監視, パレト分析, 障害処置順位, 水準値分析, システムリソース, 予兆検知

はじめに

阪神高速道路の安全・安心・快適な走行のために、道路上にある情報提供や情報収集する設備や ETC 設備などの電気通信機器（以降、端末装置）と、それら設備からのデータの処理および管理やお客さまからの問い合わせを処理する中央装置が 24 時間 365 日稼働している。

これら端末装置および中央装置で構成される基幹システムの障害は利用されるお客さまに対して、サービス停止等の不便をおかけすることになるため、効率良く障害対応したり、障害の兆候を早期に発見し処理することで、極力サービスの停止時間を少なくすることが重要である。

本稿では、第 1 章で端末装置の多種のアラームを統計し、その発生傾向を把握するための分析を

行い、処置の優先順位を示すことで効率的な補修運用を行った事例を、第 2 章で中央装置のリソース（CPU とメモリ）使用状況を用いて、平常時のリソース使用状況と比較することで異常値を発見する分析手法により、中央装置の異常状態を早期に検知し、対処した事例をそれぞれ報告する。

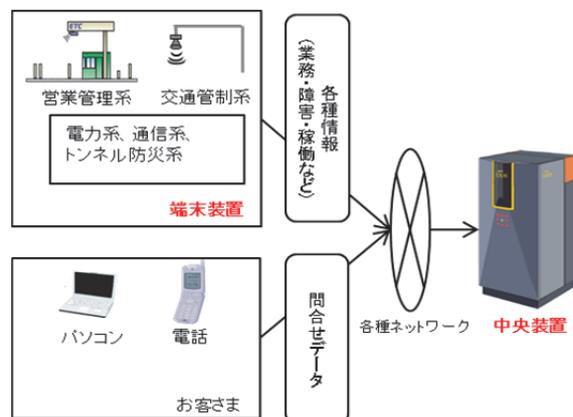


図-1 基幹システムの構成

1. 端末装置における障害処置順位の提案機能

1-1 障害監視運用と課題

阪神高速道路には情報提供や情報収集する設備や ETC 設備といった端末装置が約 35 万台設置されており、それらの障害発生時は昼夜問わず迅速な対応が求められる。

しかし、障害の発生を通知するアラームが月約 70 万件にもおよぶため、障害対応要員を効果的に配置し、障害処置を行うための優先順位の判断にノウハウを必要としていた。

1-2 分析手法の検討

(1) アラーム発生の傾向

アラーム発生件数の多い設備を特定するため、5 つの系統（電力系、通信系、トンネル防災系、営業管理系、交通管制系）別にアラーム発生件数を集計した後、アラーム発生件数の最も多い系統の設備別のアラーム発生割合を集計した。

集計結果からアラーム発生件数は、系統別では交通管制系が全体の約 80%であり、さらに詳細の設備別では、車両検知ヘッドが全体の約 50%であることが判明した。

これより、車両検知ヘッドのアラームを削減できれば、障害対応要員のアラーム確認時間を大幅に削減でき、効率的な障害処置が可能となる。

図-2 は系統別のアラーム発生件数、図-3 は全系統における設備別のアラーム発生割合のグラフである。

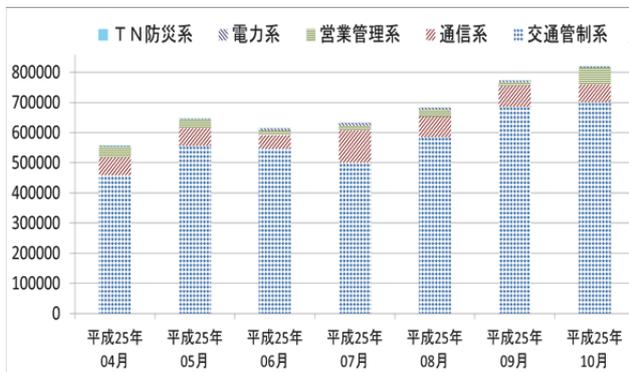


図-2 系統別のアラーム発生件数

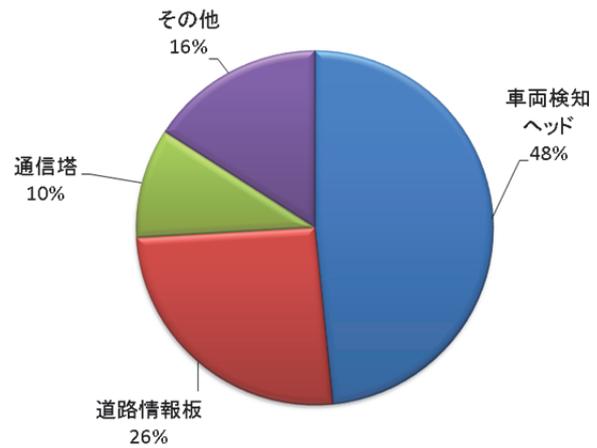


図-3 全系統における設備別のアラーム発生割合

(2) 分析手法

車両検知ヘッドについて、アラームが多く発生している装置を特定するために、パレート分析を行った。

パレート分析は、構成比率の大きな順に最上位の少数(A グループ)、中位の少数(B グループ)、下位の多数(C グループ)に分類し、それぞれを重要度に応じた異なる扱いにすることで、対処すべき対象グループに優先度をつけ管理効率を高める際に用いられる手法であり、今回の分析では以下の手順でパレート分析を行った。

- ①アラーム発生件数の順に端末装置を並べる。
 - ②アラーム発生件数の合計を 100 とし構成比率を算出。
 - ③アラーム発生件数の順に構成比率の累計を算出。
 - ④構成比率の累計によってグループ分けを実施。
- 今回は構成比率を以下のグループで実施した。

(単位：%)

A グループ： 0～70

B グループ： 71～90

C グループ： 91～100

図-4 は車両検知ヘッドのアラーム発生件数のパレート図である。

表-1 車両検知ヘッドアラーム発生状況

No	アラーム発生日時	アラーム復旧日時	アラーム継続時間	地区	路線名	設備名称
1	2013/7/1 0:01	2013/7/1 0:02	0:01:00	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
2	2013/7/1 0:02	2013/7/1 0:03	0:00:30	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
3	2013/7/1 0:04	2013/7/1 0:04	0:00:30	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
4	2013/7/1 0:05	2013/7/1 0:06	0:00:30	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
5	2013/7/1 0:07	2013/7/1 0:07	0:00:30	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
6	2013/7/1 0:08	2013/7/1 0:09	0:01:00	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
7	2013/7/1 0:09	2013/7/1 0:10	0:01:00	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
8	2013/7/1 0:11	2013/7/1 0:12	0:01:00	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
9	2013/7/1 0:12	2013/7/1 0:13	0:01:00	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
10	2013/7/1 0:14	2013/7/1 0:15	0:01:00	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
11	2013/7/1 0:15	2013/7/1 0:16	0:01:00	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
30015	2013/7/31 23:54	2013/7/31 23:55	0:01:00	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
30016	2013/7/31 23:55	2013/7/31 23:56	0:01:00	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
30017	2013/7/31 23:57	2013/7/31 23:58	0:01:00	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド
30018	2013/7/31 23:58	2013/7/31 23:59	0:01:00	大阪地区	1号環状線	環4.5 -03 車両検知ヘッド

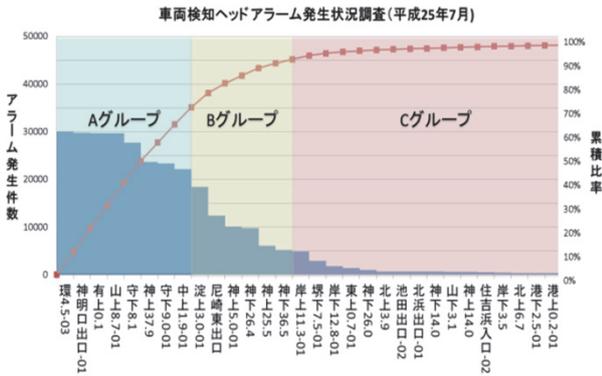


図-4 車両検知ヘッドのアラーム発生件数のパレート図

1-3 パレート分析による成果

(1) 分析結果

車両検知ヘッドのアラームについて、パレート分析を行った結果、全ヘッド 2,286 台の内、A グループに属する 8 台の設備について対策を行うだけで、車両検知ヘッドで発生しているアラームのうち約 70%が削減でき、B グループに属する 6 台の設備も加えた計 14 台を対策すれば、車両検知ヘッドのアラームの約 90%が削減できることから、ごく一部の車両検知ヘッドでアラームの大部分を占めていることが判明した。

また A, B グループの車両検知ヘッドのアラーム内容を詳細に分析した結果、発生しているアラームの継続時間（アラーム復旧時間-アラーム発生時間）が 30 秒~1 分程度で、復旧後に即、次のアラームが発生していることが判明した。本事象はこれまでの障害対応実績より、車両検知ヘッドの故障の予兆が多いことが確認できている。

これより、アラーム発生件数の多い車両検知ヘッドは完全に故障してはいないが、障害の予兆を示している状態である事が判明した。

表-1 は A グループに属するある 1 台の車両検知ヘッドのアラーム発生状況の例である。

(2) 効果

アラーム発生状況の分析結果より、障害の予兆が大量のアラームを発生させていることが分かった。

したがって、車両検知ヘッドに障害の予兆が発生した段階で予防処置を行えば、大量のアラームが削減できるため、車両検知ヘッドの障害発生件数を毎月集計し、毎月上位 5 台について予防処置を行う運用を試行した結果、5 ヶ月で 80 万件から 50 万件にアラーム件数が削減された。

図-5 は、試行運用後のアラーム件数削減推移のグラフである。

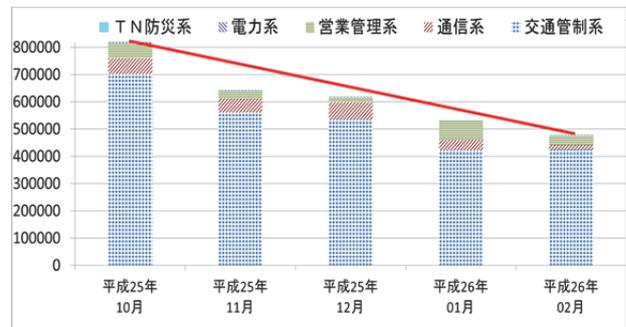


図-5 試行運用後のアラーム発生件数推移

このため、アラーム発生件数の集計割合を帳票化し、出力できるシステムを導入すれば、容易で均一的な処置が誰でも可能となり、効率的な運用が可能と考えた。

図-6 は設備種別指定画面, 図-7 は帳票出力画面である。

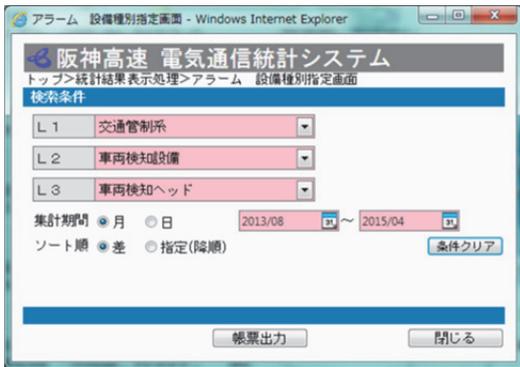


図-6 設備種別指定画面

日付	電力系	通信系	交通管制系			営業管理系	TN防災系	総計
			件数	差	割合			
平成26年06月	~	~	372,644	-23,582	86.3%	~	~	431,983
平成26年07月			387,838	15,194	82.1%			472,432
平成26年08月			494,591	106,753	83.4%			592,995
平成26年09月			468,633	-25,958	89.0%			526,266
平成26年10月			409,225	-59,408	88.0%			464,909
平成26年11月			336,394	-72,831	82.8%			406,097

図-7 帳票出力画面

システム化後,アラーム発生原因の特定が容易となり効率的な障害処置が可能となったことで,アラーム発生件数が,夏季に多数の車両検知ヘッドが故障したことによる一時的な増加はあったものの,徐々に減少し,最終的にはアラーム発生件数が30万件と当初の半分以下となった。

図-8 はシステム化後のアラーム発生件数推移である。



図-8 システム化後のアラーム発生件数推移

2. 中央装置の障害予兆検知

2-1 障害監視運用とその問題点

中央装置の障害監視の運用は,中央装置の稼働状況,とりわけ OS・ミドルウェア・アプリケーションプログラムといったソフトウェアの稼働状況を把握することは難しく,かつこれらは冗長構成等の対策もとれない。

したがって,障害が発生してから対処する「受動的な維持管理」により,障害が復旧するまではお客さまに対して影響があった。

2-2 分析手法の検討

(1) 中央装置のシステムリソース

中央装置は様々なシステムリソースから構成され,それらシステムリソースは使用状況を計測することができる。表-2 は,代表的なシステムリソースとその計測可能項目の一覧である。

表-2 代表的なシステムリソースとその計測可能項目

システムリソース	計測可能項目
CPU	・CPU使用率(単位時間当たりの使用時間)
メモリ	・メモリ使用率(物理メモリ量に対しての使用量)
ディスク	・ディスクI/O率(単位時間当たりの書き込み量・読み込み量) ・ディスク使用量(物理ディスク量に対しての使用量)
ネットワーク	・ネットワーク流量(単位時間当たりの送受信量)

これらシステムリソースは OS・ミドルウェア・アプリケーションプログラムの障害時に変化することが想定されるため,これらに起因したシステム障害を未然に防ぐことが期待できると考えた。

(2) 分析手法

中央装置の正常運用時のシステムリソースを計測し水準値を把握することで,通常運用時のシステムリソースの使用の変動と比較すれば,中央装置の異常を検知できると考えた。

中央装置の主要リソースである,CPU とメモリに焦点をあて,それらの水準値を策定するために

1 ヶ月間、正常稼働時の使用状況を取得した。また CPU およびメモリの特性を考慮し、以下の集計方法とした。

- CPUは同時間帯でどのような使用がされているか判断するため、横軸を時間とし、1ヵ月分のデータの同時間帯の値から最大値を算出し、グラフ化
- メモリは1ヵ月間を通して、メモリが解放されない事象（メモリリーク）を把握するために、横軸を日とし、グラフ化

上記の集計方法をもとに約200台の中央装置の水準値を策定した。図-9および図-10はETCの利用明細の入口・出口のマッチングを行う装置AのCPUおよびメモリの変動パターンである。

本装置を例にとると、CPU に関しては、0 時～2 時の時間帯はバックアップ処理により最大で100%に達し、それ以外の時間帯は 30%～60%が本装置の変動パターンの水準値である。一方でメモリに関しては約 75%で一定して使用するのが、本装置の変動パターンの水準値であることが分かる。

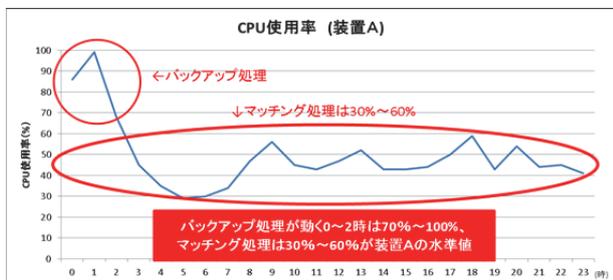


図-9 CPU変動パターンによる水準値例

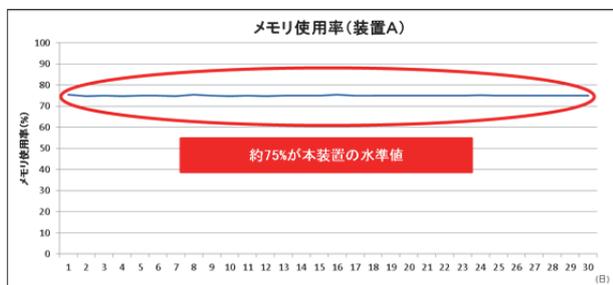


図-10 メモリ変動パターンによる水準値例

通常運用時に集計したリソース使用状況が、策定した変動パターンによる水準値のグラフから逸脱していないか比較することとした。

2-3 水準値分析による成果

(1) CPUの使用異常によるプログラムの不具合を早期に発見

1) 事象

2014年9月の集計結果において、WEB装置でCPUの使用状況が通常は最大でも約30%にも関わらず、9/10 21:20～21:40の間に最大で100%に達し、高負荷状態となったことを確認した。

WEB 装置の CPU が高負荷状態になると、阪神高速の各種 WEB サービス（企画割引申込 WEB・環境ロードプライシング申込 WEB・回数券付替サービス WEB・課金訂正受付 WEB・阪高割引施策受付 WEB）の処理が遅延したり、最悪の場合、システムダウンし各種 WEB サービスを提供できず、お客さまに影響を及ぼす。

図-11は水準値と2014年9月の計測値をグラフ化したもの、図-12は2014年9月の計測値をより詳細に把握するために、異常の時間帯を拡大したものである。

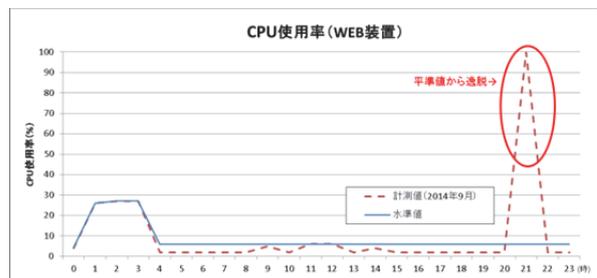


図-11 WEB装置における水準値と計測値

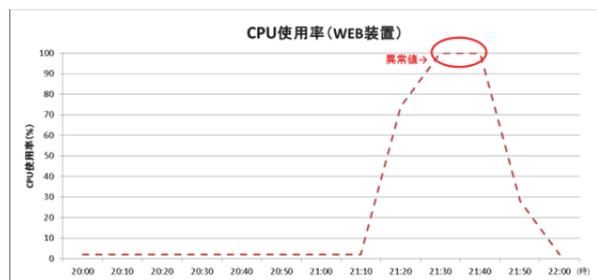


図-12 WEB装置における計測値（詳細）
(2014/9/10 20:00-22:00)

2) 原因調査

異常を検知できた時間帯の全5つのWEBサービスのアプリケーションログを調査したところ、環境

ロードプライジングのアプリケーションのログに、申込画面の「行追加ボタン」を押下したログが1秒間に10件のペースで断続的に30分間押下されたログが出力されていた。

また最大で100件までしか「行追加ボタン」で行を追加できないにも関わらず、100件以上行を追加しようとするログも出力されていた。図-13はアプリケーションログの抜粋である。

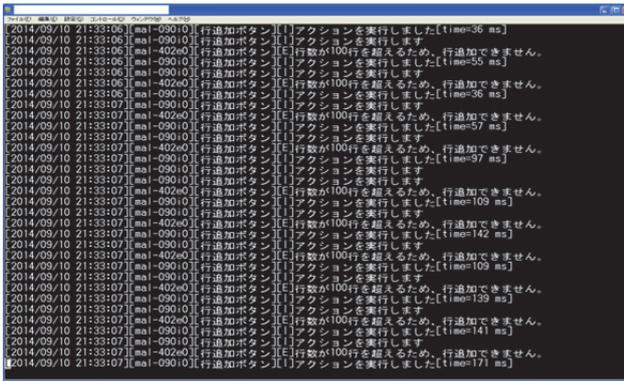


図-13 アプリケーションログ (抜粋)

「行追加ボタン」の連続押下により、システムの高負荷が続いたと考えた。断続的に高負荷状態となると、システム停止やレスポンス低下を引き起こす可能性がある。図-14は環境ロードプライジング申込画面と行追加ボタンである。(標準は5件まで登録できる入力フォームが用意されており、最大100件まで「行追加ボタン」で行を追加できる仕様)

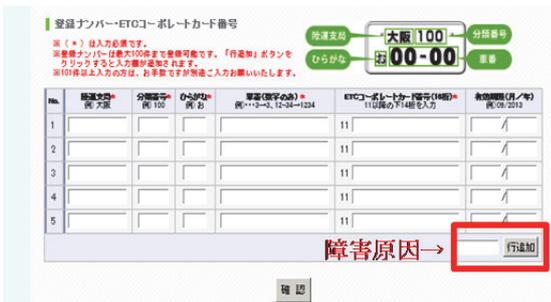


図-14 環境ロードプライジング申込画面と行追加ボタン

3) 対策

当初の設計における想定外の利用方法によることから、以下のシステム改修を行った。

- ・ 行追加ボタンの削除
 - ・ 標準で100件まで登録できる入力フォームを準備およびスクロールバーの追加
- システム改修以降は同事象が発生することはない、安定稼働している。

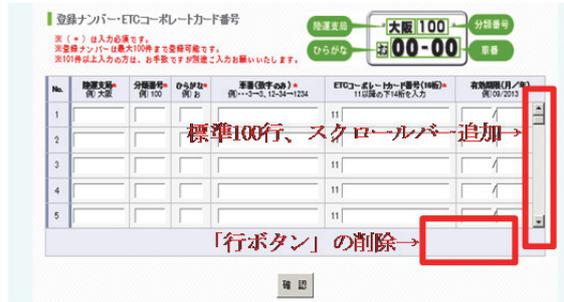


図-15 対策後の申込画面

(2) メモリの使用異常によるWindowsの既知不良を早期に発見

1) 事象

コンタクトセンターの装置において、水準値の変動パターンから逸脱し、かつ日々上昇し続け、メモリが解放されない事象(メモリリーク)を確認した。また水準値の策定のために、データを取得し始めた直後から、発生していることも合わせて確認した。

コンタクトセンター関連装置のメモリが不足すると、お客さまとの電話中に切断したり、オペレータがお客さまの情報を入力するシステムで異常が発生し入力できないといった影響がある。

またコンタクトセンター関連装置9台のうち6台で同事象が確認できた。図-16は6台のうち1台(コンタクトセンター装置A)のメモリ使用状況である。

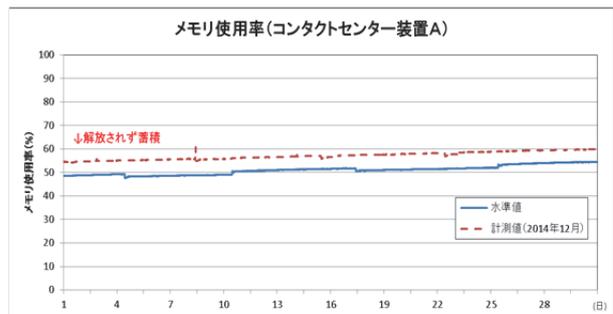


図-16 コンタクトセンター装置Aのメモリ使用率

2) 原因調査

水準値の変動パターンから逸脱し、かつ1か月に数%メモリ使用率が上昇している要因がどのプログラムかを特定するために、2015年1月の月初と月末でモニタリングしところ、svchost.exeというWindowsの各サービスを起動するための親プログラムがメモリ上昇の要因であることが分かった。

また本事象が確認できた6台の装置の共通点を調査すると、OSがWindowsであり、かつバージョンも2012を搭載している装置であることが確認できた。前述したとおり、本事象はデータを取得し始めた当初から発生していることも合わせて確認できている。

したがって、Windows2012に共通的な不具合があると推測し、Microsoft社が公開している技術サポート一覧を調査したところ、Windows2012にメモリが解放されない既知の不具合があることが判明した。図-17はMicrosoft社の技術サポートの公開情報である。

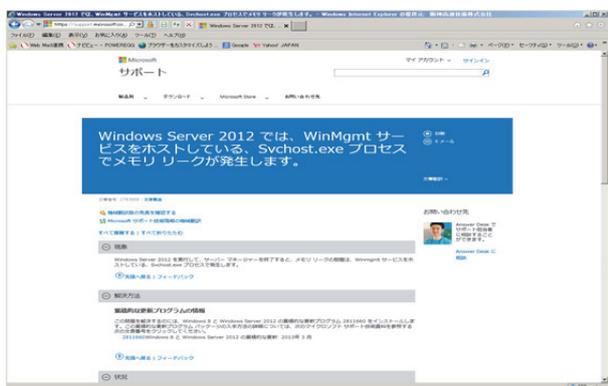


図-17 Microsoft社の技術サポート公開情報

3) 対策

Microsoft社はこの不具合に対する対策版（修正パッチ）を公開しているのので、検証環境での確認後、対策版（修正パッチ）を適用した。

図-18は修正パッチ適用後のメモリ使用状況であるが、約30%で安定して稼働していることが分かる。

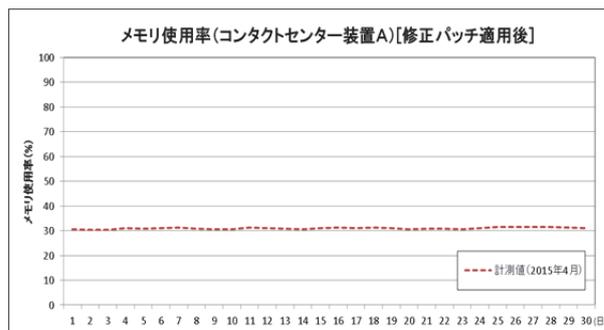


図-18 修正パッチ適用後のコンタクトセンター装置Aのメモリ使用率

3. まとめ

本稿では、今まで活用されていなかった端末装置のアラームおよび中央装置のリソースデータを活用・分析することで、効果が得られた事例を紹介した。

端末装置に関しては、大量のアラームを発生している装置が特定でき、効率的な補修運用を行うことで、大量のアラームが削減された。また結果的に特定した装置のアラームが障害の予兆であることも合わせて特定でき、予防保全を実施することで障害発生によるお客さまに対するサービス停止を未然に防ぐ効果もあった。

今後は大量のアラームに埋もれていた他アラームについても傾向分析を行うことでさらに有効な施策を探っていきたい。

一方、中央装置に関しても、障害発生前の予兆を示す装置が特定でき、2件の大規模なシステム障害の可能性を未然に防ぐことができた。

今後は、今回調査対象から除外したディスクおよびネットワーク関連のリソースを用いたシステム障害の予兆検知方法も検討していきたい。

謝辞：本論文を執筆するにあたり、ご協力いただいた大阪管理局保全部システム保全課、ならびに大阪管理局保全部施設工事課の方々に深く感謝の意を表します。

DETECTION OF SIGNS OF SERVER FAILURE AND PRIORITY SETTING FOR FIXING TERMINAL EQUIPMENT FAILURES

Takuya TANAHASHI, Sho YOSHIDA and Katsuhiko HARADA

For ensured safety, reliability and comfort of vehicles, there are a variety of electrical communication equipment on the Hanshin Expressway including traffic control equipment, electronic toll collection equipment and their servers which are operated 24 hours a day, 365 days a year. Since failures of the mission-critical system cause serious consequences to users, it is important to detect failure signs early and fix them efficiently. This report proposes a method to detect server failure signs by comparing current status data with normal-state measurements, and also presents a sample case of efficient implementation of repairs based on priorities set by using statistically processed alarm data.

棚橋 卓也



阪神高速技術株式会社
技術部 情報管理課
Takuya Tanahashi

吉田 翔



阪神高速技術株式会社
技術部 情報管理課
Sho Yoshida

原田 克彦



阪神高速道路株式会社
神戸管理部 施設工事課
Katsuhiko Harada