組込みネットワークにおける障害管理手法の検討

岡田　英明†

三菱電機（株）情報技術総合研究所†

1. はじめに

機器の制御、管理を行う組込みネットワークシステムにおいては障害の検知とその対応を行う障害管理が特に重要である。例えば、組込みネットワークを使用するアプリケーションは慎重に設計、試験され、運用されるが、試験で発見されなかった欠陥が顕在化し、障害を発生させてしまう場合がある。このような障害を早期に検知し、他の機器への悪影響を防止し、障害状況を記録して後日の障害解析・対策に利用できるようにすることが必要である。

本稿では、イーサネットおよびTCP(UDP)/IPを使用する組込みネットワークシステムにおける障害管理の手法を検討する。

2. 障害管理機能

障害管理の機能を以下に示す6つの機能と定義する。

① 障害発生の検知と特定
② 障害発生位置の特定
③ 障害のシステムからの分離
④ 障害が発生したシステムの再構成
⑤ 障害の修復
⑥ 障害状況の記録

本稿では、システムに依存しない、①、②、③、⑥を検討対象とする。

①障害発生の検知と特定

組込みネットワークシステムに障害が発生したことを検知し、障害が発生した機器またはアプリケーションを特定する。

本稿においては、アプリケーションの障害を検討対象とする。すなわち、組込みネットワークシステムでは各アプリケーションの動作仕様が既知の情報として入手可能であると想定し、仕様と異なる動作を障害として検知する。また、アプリケーションの特定は、アプリケーションが使用する送信元IPアドレスを特定することと定義する。高い検知率、および短い検知時間を実現することが必要である。

②障害発生位置の特定

障害が発生したアプリケーションが動作する機器のネットワーク構成上の位置、すなわち接続されているイーサネットスイッチ（以下スイッチ）とそのポート番号を特定する。

①障害発生の検知と特定によって、障害発生アプリケーションのIPアドレスが特定される。③、⑥に示す障害への対応を行うためには、IPアドレスの特定だけではなく、ネットワークの構成を管理し、IPアドレスとネットワーク構成上の位置を関連付けることが必要である。

③障害のシステムからの分離

障害発生機器による通信をネットワークから遮断する。

障害発生機器の送信パケットによる悪影響を最小限にとどめるため、障害発生機器が接続されているスイッチにおいて通信を遮断することが必要である。

⑥障害状況の記録

後に障害解析に利用するために、障害が発生している、または発生が疑われる状況におけるトラフィックを記録する。

記録負荷と記録量の削減のため、関連するスイッチのみにおいて、特定のトラフィックのみを記録することが必要である。

以上の障害管理機能を図1に示す。

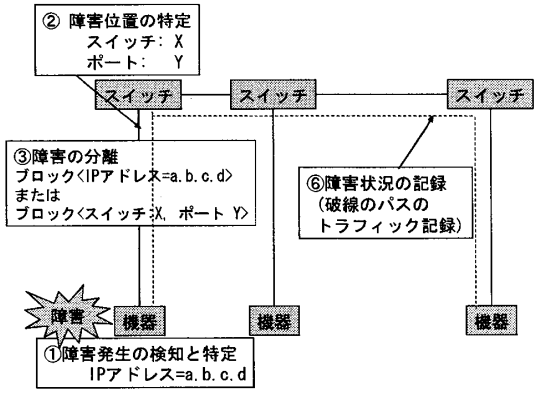

図1　障害管理機能

Study of fault management in embedded control networks
† Hideaki OKADA, Information Technology R&D Center, Mitsubishi Electric Corp.

3. 障害管理システム

障害管理システムの概略構成を図2に示す。

構成管理・障害管理サーバ

機器およびスイッチの接続構成情報を管理する。すなわち、各機器のIPアドレスと、各機器から構成管理サーバへの経路上のスイッチとその接続ポート番号を管理する。

また、障害管理クライアントを制御して、障害管理を行う。

構成情報付与機能

機器が送信する構成情報管理用パケットに対し、ネットワークの構成情報を付与する。

プローブ機能

入出力トラフィックを監視し、障害の検知を行う。また、障害管理クライアントの指示により、特定のトラフィックの監視、記録を行う。

フィルタ機能

障害管理クライアントの指示により、特定の物理ポート、IPアドレスを送信元とするパケットの破棄を行う。これは、高機能のスイッチには一般的な機能である。

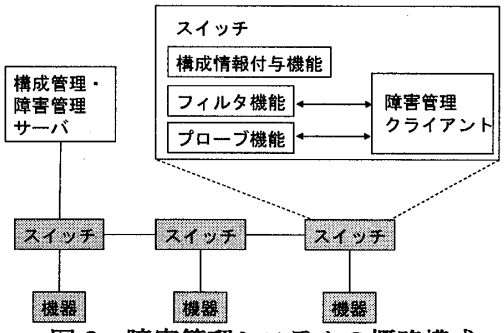

図2　障害管理システムの概略構成

これらの構成要素により、障害管理機能①、②、③、⑥を実現することができる。

プローブ機能により、ネットワーク上のトラフィックを観測し、①障害発生の検知と特定を行う。5章で障害検知手法を検討する。

構成管理・障害管理サーバが管理する構成情報によって、障害発生機器のIPアドレスから、②障害発生位置の特定を実現する。4章で構成管理手法を検討する。

フィルタ機能により、障害発生機器に対し、③障害のシステムからの分離を実現する。このとき、構成情報の利用により、機器接続スイッチポートのみにフィルタ機能を適用することにより、障害発生機器が接続されているスイッチにおける通信の遮断を実現する。

また、プローブ機能における記録により、特定のトラフィックの⑥障害状況の記録を実現する。このとき、構成情報の利用により、トラフィックに関連する特定のスイッチポートでのみ記録を行い、記録負荷および記録量の削減を実現する。

4. 構成管理手法の検討

構成管理手法として、DHCPリレー・エージェント・オプション、いわゆるDHCPスヌーピング、の考え方を応用したIPアドレス管理を行う。すなわち、機器ではDHCPクライアントが動作し、構成管理・障害管理サーバではDHCPサーバが動作する。機器からサーバへのDHCPメッセージに対し、各スイッチの構成情報付与機能がスイッチのIDと物理ポート番号をそれぞれ付与することにより、経路上のすべての構成情報が付与される。DHCPサーバである構成管理・障害管理サーバにおいて、この情報を収集、管理することにより、構成情報を管理する。

5. 障害検知手法の検討

障害検知手法として、FSM（有限状態機械）モデル化による障害検知[1]の適用を検討している。

FSMモデル化による障害検知は、組込みネットワークアプリケーションの動作仕様を利用する特長を持つ。また、障害検知のために特別なメッセージを送受信することなく、システム本来の入出力パケットの観測によって障害検知を行うため、障害検知によるアプリケーションへの影響がない、という特長を持つ。

FSMモデル化手法では、各アプリケーションをFSMとしてモデル化する。すなわち、各アプリケーションは、有限個の固有の状態を持ち、状態遷移を行うとともに、状態遷移に従ってパケットを送受信する。

各アプリケーションの動作仕様をFSMとしてモデル化するとともに、プローブ機能が入出力パケットを観測し、実際の状態遷移を推測する。その状態遷移が動作仕様の状態遷移と異なる場合、障害が発生している、と判断する。

6. おわりに

本稿では、障害管理の機能および障害管理システムの各機能の定義を行うとともに、構成管理および障害検知の手法について検討した。今後は、障害検知手法を具体的に適用するための検討、および障害検知率の算出方法の検討を行っていく。

参考文献

[1] David Lee, Passive testing and applications to network management, *Proceedings of IEEE International Conference on Network Protocols*, 1997