UPnP 機器の情報収集方法の検討・試作

佐藤 弓子†, 寺島 芳樹†, 土井 裕介†, 寺本 圭一†

† 株式会社東芝 研究開発センター 〒212-8582 川崎市幸区小向東芝町 1

E-mail: † {yumiko57.sato, yoshiki.terashima, yusuke.doi, keiichi.teramoto}@toshiba.co.jp

1. まえがき

近年，ネットワーク家電が増加してきている．一方，その品質保証，特に UPnP[1]をはじめとするネットワーク機能のテストが課題となっている．UPnP は通信プロトコルとして SSDP[2]や SOAP[3]を使用する．ネットワーク家電の通信機能の確認のために，これまでは，通信相手としてのコントロールポイントや UPnP 機器の実機等を使用して動作を確認していた．しかし，単体での動作確認には限界があり，実環境での組み合わせではじめて障害が確認される場合がある．このとき，対象機器を実際のネットワークに接続し，どのような通信がなされているのかをプロトコル解析ツールで確認する方法がある[4]．

UPnP 機器は新製品が続々とリリースされており，そのテストも多様となる．そこで，プロトコル解析ツールは機器毎の専用性が高いものよりも拡張性の高いものが求められる．よく知られているプロトコル解析ツールに Wireshark がある．Wireshark は 800 以上のプロトコルを解析できるうえ，プラグイン作成用の API が提供されているため，簡単に解析ツールを拡張することができる．

本稿では，UPnP 機器のテストに用いることを目的とし，汎用のプロトコル解析ツールの拡張による情報収集方法を提案する．また，機器間の通信の履歴から事後的な分析等に利用するために，解析した情報のサーバへの集約を実現する．

2. 解析ツール作成における課題と解決策

解析ツールの情報収集方法の構成例を図 1 に示す．コントロールポイントと UPnP 機器が同サブネットに設置されているとき，監視機器は UPnP 機器とコントロールポイント間の通信を監視する．また，その通信の中から必要な情報を取り出して遠隔の情報蓄積サーバへと送信する．

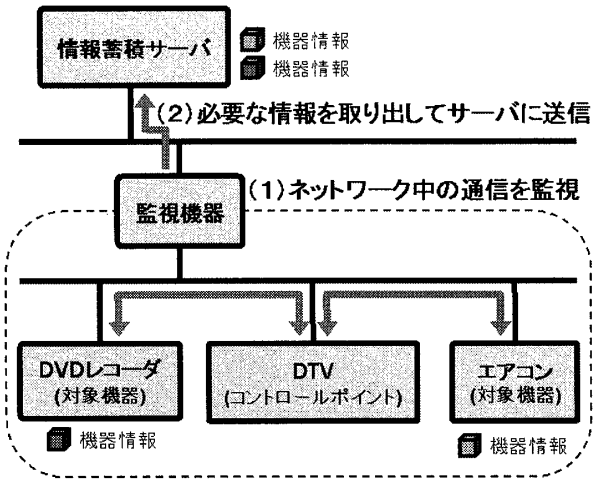

図 1. 情報収集方法

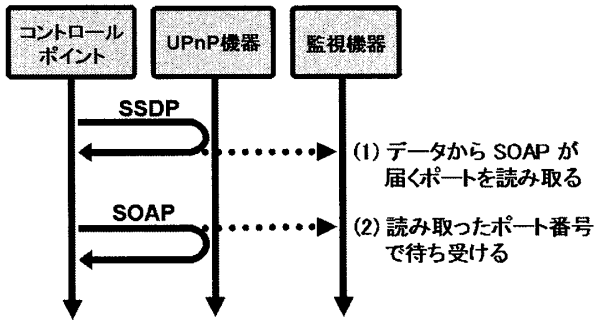

図 2. SOAP パケットのポート番号の読み取り

今回は監視機器のソフトウェアとして Wireshark を拡張し用いる．ただし，Wireshark ではポート番号が可変となる通信のペイロード自動判別ができない．UPnP の通信は図 2 に示すように SSDP と SOAP から成り，SOAP のポート番号が可変である．したがって Wireshark の拡張が必要である．

UPnP におけるコントロールポイントは，SSDP の LOCATION 情報により UPnP 機器の SOAP 通信のためのポート番号を取得する．図 2 に示すように，監視機器においてこの SSDP のパケットを分析することで，該当する通信を SOAP として解析する．

また，解析結果の送信機能は Wireshark にはないため，プラグイン用に組み込まれているスクリプト言語 Lua[5]に外部モジュールを追加して実現する．

Prototyping and Evaluation of an Information-gathering System for UPnP Device

† Yumiko SATO・Corporate Research & Development Center, TOSHIBA Corporation

3. 解析ツールの試作

図1の構成において，UPnP機器とコントロールポイント間のUPnP通信が正常に行われているかを確認するために監視機器に次の機能を実現した．

1) SSDPポートに届くパケットを監視
2) SSDPのパケットからSOAPで使用するポート番号(LOCATIONフィールド)を読み取る
3) 読み取ったポートに届くパケットを監視
4) SSDPパケットの送信元とSOAPパケットの受信先のIPアドレスが一致すればHTTPヘッダのCONTENT-TYPEを読み取る
5) SOAPが使用するCONTENT-TYPE（SOAP1.1の場合はtext/xml，SOAP1.2の場合はapplication/soap+xml)であればSOAPとして解析

これにより，SSDPに対応したSOAP通信を自動判別できる．

また，これらの通信内容を情報蓄積サーバに送信し，蓄積した情報から新たな結果を得ることが可能となる．例として対象機器の死活監視機能を監視機器と情報蓄積サーバを用いて実現する．監視機器の機能は以下のようになる．

1) SSDPポートに届くパケットを監視
2) SSDPパケットに含まれる参入・離脱情報(NTSフィールド)及びキャッシュ時間(CACHE-CONTROLフィールド)を読み取る
3) 監視対象機器ごとに，最新のパケット取得時刻，参入・離脱情報を定期的に情報蓄積サーバ送信
4) 監視対象機器ごとに，キャッシュ時間以内に次のSSDPパケットが届くかを監視．最後に受信したSSDPパケットに含まれる参入・離脱情報が参入を示していたにも関わらず，キャッシュ時間を越えても次のSSDPパケットが届かなかった場合は，監視対象機器が異常終了したとして情報蓄積サーバに通知

このように，機器間の通信の履歴を用いて監視対象機器の死活監視が可能となる．

4. 解析ツールの動作結果と評価

図1の構成において，今回開発した解析ツールをUPnP機器の通信の情報収集に適用した．

UPnP機器を起動し，コントロールポイントから制御した場合に，従来自動的にペイロード種別を判別できなかったUPnPパケットが自動的にSOAPと判断されることを確認した．

また，UPnP機器が起動した場合にUPnP機器の参入情報を情報蓄積サーバに送信すること，UPnP機器を通常通り終了させた場合に離脱情報を情報蓄積サーバに送信すること，UPnP機器を強制終了させた場合にキャッシュ時間以内に離脱情報を受信しなかった旨を情報蓄積サーバに送信することを確認した．さらに，この情報を用いて，UPnP機器の死活監視ができることを確認した．

本稿で提案した方式には次の利点が考えられる．

- データの内容を利用した解析ができるため，UPnPのSSAPとSOAPのように，異なるプロトコルが連携する場合に有効である．
- 通信を傍受して情報を集めるため，UPnP機器とコントロールポイントの通信に影響を与えない．
- 対象機器固有の処理のみをプラグインとして実装すればよいため，迅速な開発が可能である．

これらの利点により，提案方式は情報家電の動作検証に有効であると言える．

一方，次のような課題が残っている．

- 頻繁に情報を送信すると動作が重くなり，Wiresharkが停止してしまうため，送信する情報の選択・集約のしかたを工夫する必要がある．

5. むすび

本稿では，プロトコル解析ツールWiresharkを拡張し，UPnPにおけるSSDPとSOAPパケットを関連付けて解析可能にした．また，UPnP機器の通信から異常を検出するパターンを一つ実装し，Wiresharkを利用したUPnP機器の自動監視の可能性を示した．

参考文献

[1] UPnP Forum, http://www.upnp.org/
[2] INTERNET DRAFT <draft-cai-ssdp-v1-03.txt> Simple Service Discovery Protocol/1.0 Operating without an Arbiter
[3] Simple Object Access Protocol(SOAP)1.1, http://www.w3.org/TR/soap/
[4] 鈴木 他，“迅速な障害対応を支援するトラヒック可視化システムの構築と評価，”(B)信学論，vol.J92-B，no.7，pp.1072-1083，2009.
[5] Lua, http://www.lua.org/