WS-Security を適用した SOAP メッセージに対するアグリゲーションの評価

Evaluation of Aggregation of SOAP Message applied WS-Security

帯刀洋太 †, 森山真光 †
Yota Tatewaki†, and Masamitsu Moriyama†
† 近畿大学大学院　総合理工学研究科
†Graduate School of Science and Engineering, Kindai Univ.

要旨
SOAP は XML を用いて文書交換や遠隔手続呼出をする通信規約であり，冗長性に起因する通信量の増加が問題となっている．既存の手法として，複数の SOAP メッセージをアグリゲーションし通信量を軽減させる手法が提案されている．企業間電子商取引のシステムでは安全性の向上を目的として，SOAP の拡張仕様である WS-Security を適用することが一般的である．そこで，WS-Security を適用した SOAP メッセージに対して既存の手法を適用し評価する．

1. はじめに

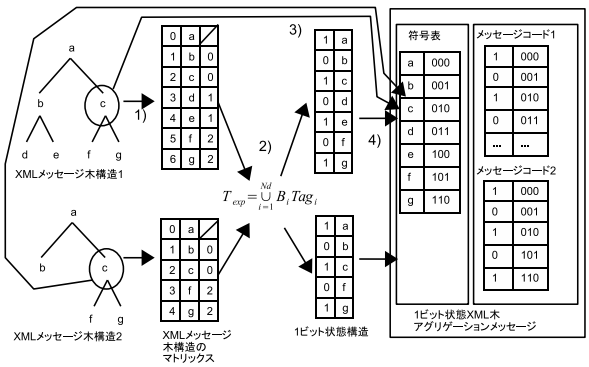
遠隔手続き呼び出し (以下 RPC) とは，コンピュータから別のコンピュータにあるサブルーチンや手続きを実行することを可能にする技術である．この RPC と言う技術は 1990 年に CORBA，1993 年に DCOM 等，様々な仕様を生みだし，それらは独自のプロトコルで用いることが原因でそれぞれ仕様同士の相互通信が複雑になることが問題となった．そこで 1998 年に HTTP と XML をベースとした SOAP と言う通信プロトコルが生まれ，サービス指向アーキテクチャ(以下 SOA) の基盤となる Web サービスと言う新しい技術が生まれた [1]．それは通信に一般的なプロトコルである HTTP を使用することから広く普及した．2012 年には，21,358 件の Web サービスが公開され，13,108 件の Web サービスが実際に使用できることが調査されている [1]．SOAP は Web サービス技術の中核となっており，従来研究ではパフォーマンスの向上に焦点が当てられている [2].

SOAP はメッセージの送受信の際に，メッセージの冗長性によるメッセージ量の増加により CORBA や Java RMI などの既存技術と比較して，通信量が大きいことが問題となっている．この問題を解決するため，類似度に基づく SOAP マルチキャストプロトコル (SMP)[3] や 1 ビット XML 状態木アグリゲーション [4] という手法が提案されている．これらの手法は複数の SOAP メッセージを一つのメッセージにアグリゲーションしメッセージ量を低減させ，そのアグリゲーションしたメッセージを中継サーバに送信し，その後，SOAP メッセージに分割しクライアントに送信する事で SOAP の通信量を低減させることが出来る手法である．SOAP が使用される企業間電子商取引のシステムでは安全性の向上を目的として，SOAP の拡張仕様である WS-Security を適用するのが一般的である．SMP 関連の研究は他にも文献があり，SMP における WS-Security による署名や暗号化に関する研究が行われている [5]．しかし，1 ビット XML 状態木アグリゲーションでは，そのような研究はされていない．そこで，本研究では 1 ビット XML 状態木アグリゲーションによる WS-Security を適用した SOAP メッセージのアグリゲーションを行い可逆性の検証及び，圧縮率による評価を行う．

2. 既存手法

1 ビット XML 状態木アグリゲーションは，複数の SOAP メッセージを 1 つにアグリゲーションする手法である [4]．図 1 に従来研究で提案された手法の 1 つである 1 ビット XML 状態木アグリゲーションの処理の流れを示す．まず幅優先探索を用いて SOAP メッセージ木構造からノードコンテンツのインデックスとノードコンテンツ，親のノードコンテンツのインデックスの 3 つから構成される SOAP メッセージ木構造のマトリックスを作成する (図 1-1)．次に SOAP メッセージ木構造のマトリックスから割り当てられるテキスト表現 T_{exp} を作成する (図 1-2)．Algorithm 1 に 1 ビット状態作成アルゴリズムを示す．現ノードの親ノードと次ノードの親ノードが同じ場合は 1 ビットのデータは 0 とし，異なる場合は 1 とする．次に全ての XML ノードの和集合に対して符号を割り当てた符号表を作成する．符号化にはハフ

[1]Web Services Architecture : http://www.w3.org/TR/ws-arch/#whatis



Algorithm 1 one-bit status creation

```
//Nd is the total number of nodes//Node is the content of node
//Parent is the index of parent node
for i = 0 to Nd − 1 do
  if Parent[i] = Parent[i + 1] then
    B[i] ⇐ 0; Tag[i] ⇐ Node[i]
  else
    B[i] ⇐ 1; Tag[i] ⇐ Node[i]
  end if
end for
```

図 1: 1 ビット XML 状態木アグリゲーションの処理の流れ [4]

マン符号と固定長符号の 2 つがある (図 1-3)．最後に 1 ビット状態構造から符号表に対応させたメッセージコードを作成し，テキスト形式で保存することでアグリゲーションメッセージを生成する (図 1-4)．

図 2，3 に架空の株価 Web サービスの getStockQuote(NAB，BHP) に対する SOAP レスポンスメッセージ 1 の Body 要素以下の木構造及び getStockQuote(NAB，WIL，BHP) に対する SOAP レスポンスメッセージ 2 の Body 要素以下の木構造を示す．

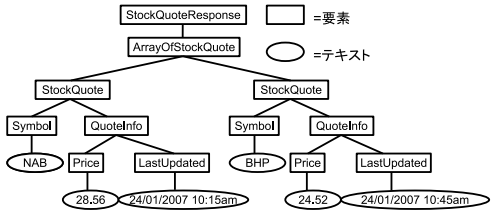


図 2: SOAP レスポンスメッセージ 1 の Body 要素以下の木構造

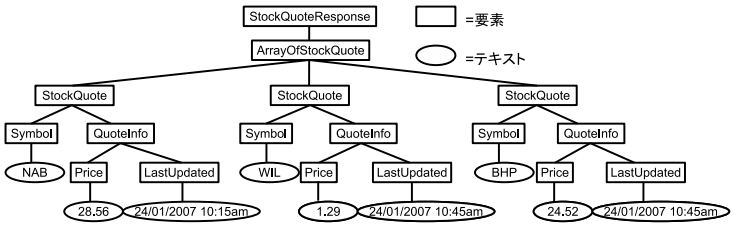


図 3: SOAP レスポンスメッセージ 2 の Body 要素以下の木構造

図 4 に SOAP レスポンスメッセージ 1 と SOAP レスポンスメッセージ 2 を 1 ビット XML 状態木アグリゲーションした例を示す．符号表は図 4(1) である．メッセージコードは図 4(2) である．XML ではエ

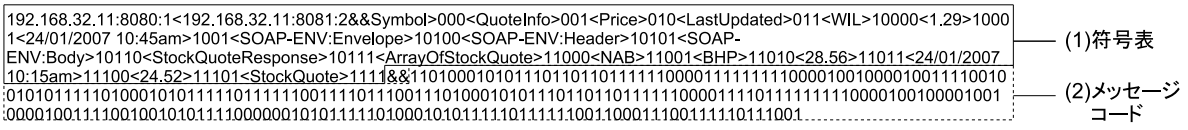


図 4: SOAP1 と SOAP2 の 1 ビット XML 状態木アグリゲーションメッセージ

スケープ文字に”>”と”<”，”&&”が指定されている．本研究ではノードの内容と符号を区切るために”>”と”<”を，符号表とメッセージコードを区切るために”&&”を使用している．

3.WS-Security を適用した SOAP メッセージ

図 5，6 にそれぞれ図 2，3 で使用した架空の株価 Web サービスに対するレスポンスメッセージを WS-Security で暗号化した木構造を示す．WS-Security を適用した SOAP メッセージは Header 部分の URI 属性と Body 部分の Id 属性とで関連付けられた CipharData 要素に暗号化された状態でメッセージが埋め込まれる．WS-Security では要素ごとに分けて，暗号化を掛けることが可能だが，今回は StockQuoteResponse 要素以下全てを暗号化している．

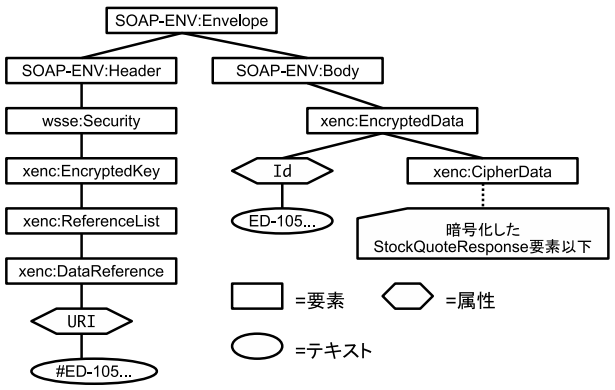


図 5: WS-Security を適用した SOAP レスポンスメッセージ 1 の木構造

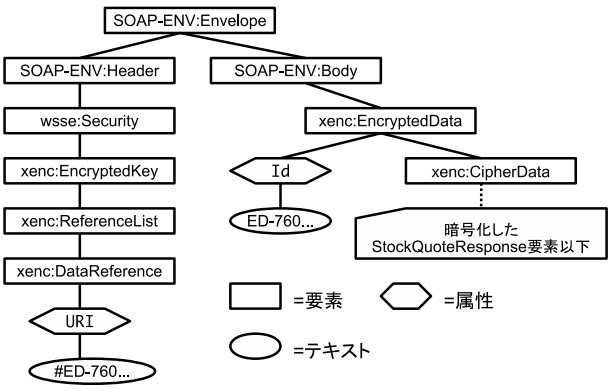


図 6: WS-Security を適用した SOAP レスポンスメッセージ 2 の木構造

4. 結果・考察

WS-Security を適用した SOAP メッセージに対して，1 ビット XML 状態木アグリゲーションによるアグリゲーションを行った．図 7 に WS-Security を適用した SOAP メッセージ 1，2 のアグリゲーションの結果を示す．結果は WS-Security を適用していない時のアグリゲーションメッセージと変わらず，

図 7: WS-Security を適用した SOAP メッセージ 1，2 の 1 ビット XML 状態木アグリゲーションメッセージ

符号表の部分である図 4(1) とメッセージコードの部分である図 4(2) の 2 つの要素からなるアグリゲーションメッセージが生成された．しかし，WS-Security を適用した SOAP メッセージの XML 属性である URI 属性や Id 属性といった情報の欠落が起きた．他にも，情報の欠落が見られ，以下の条件がある SOAP メッセージに対して情報の欠落が起きることが確認できた．

- XML 属性を持つ場合
- 空要素を持つ場合
- 単一要素に対して単一の子要素を持つ場合

このことからアグリゲーションの際に属性や空要素，単一要素に単一の子要素を持っていた場合といった特定の条件下ではアグリゲーション時に情報の欠落が起き，可逆性がないことを確認した．

図 8 に SOAP メッセージ及び WS-Security を適用した SOAP メッセージにおける 1 ビット XML 状態木アグリゲーション適用前と後のメッセージ量を示す．凡例は Aggregated_SOAP が WS-Securtiy の

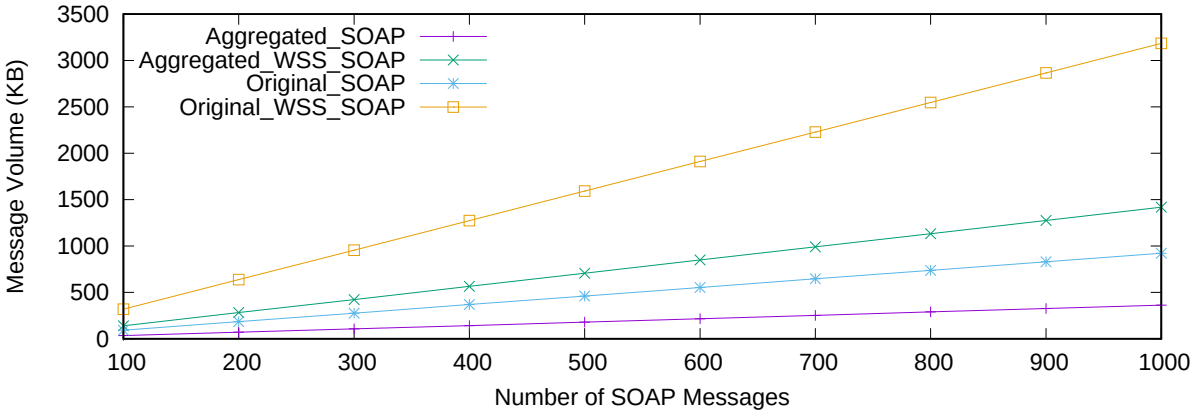


図 8: 1 ビット XML 状態木アグリゲーション適用前と後のメッセージ量

適用していない SOAP メッセージのアグリゲーション後，Aggregated_WSS_SOAP が WS-Securtiy の適用した SOAP メッセージのアグリゲーション後，Original_SOAP が WS-Securtiy の適用していない SOAP メッセージのアグリゲーション前，Original_WSS_SOAP が WS-Securtiy の適用した SOAP メッセージのアグリゲーション前とそれぞれなっている．メッセージ量は SOAP メッセージ 1000 個の時，WS-Security を適用していない SOAP メッセージで 60.7%の圧縮率，WS-Security を適用した SOAP メッセージで 55.5%の圧縮率となった．結果からメッセージの圧縮においては，WS-Security を適用した SOAP メッセージに対しても有効性があることを確認した．

5. おわりに

SOAP はメッセージの冗長性によるメッセージ量の増加により，通信量が大きいことが問題となっていた．その解決手法として，1 ビット XML 状態木アグリゲーションという手法が提案されているが，企業間電子商取引のシステムでは WS-Security の適用が一般的である．そこで，本稿では WS-Security を適用した SOAP メッセージに対して，1 ビット XML 状態木アグリゲーションを適用し評価した．結果，メッセージ量が SOAP メッセージ 1000 個の時，WS-Security を適用していない SOAP メッセージで 60.7%の圧縮率，WS-Security を適用した SOAP メッセージで最大 55.5%の圧縮率となった．メッセージの圧縮においては有効性を確認したが，属性や空要素，単一要素に単一の子要素を持っていた場合といった特定の条件下では，可逆性に問題があり，手法に対策が必要であることを確認した．今後，1 ビット XML 状態木アグリゲーションに情報量を付加し，それらの SOAP メッセージに対応した手法の考案を行う．

参考文献

[1] Zibin Zheng, Yilei Zhang and Micheal R.Luy, “*Investigating QoS of Real-World Web Services* , ” IEEE Trans. Services Computing, vol. 7, no. 1, 2014, pp. 32-39.

[2] Joe M. Tekli, Ernesto Damiani, Richard Chbeiret and Gabriele Gianini, “*SOAP Processing Performance and Enhancement* , ” IEEE Trans. Services Computing, vol. 5, no. 3, 2012, pp. 387-403.

[3] Khoi Anh Phan, Zahir Tari and Peter Bertok, “*Similarity-Based SOAP Multicast Protocol to Reduce Bandwidth and Latency in Web Services* , ” IEEE Trans. Services Computing, vol. 1, no. 2, 2008, pp. 88-103.

[4] Dhiah Al-Shammary and Ibrahim Khalil, “*Redundancy-aware SOAP messages compression and aggregation for enhanced performance* , ” JNCA, vol. 35, no. 1, 2011, pp. 365—381.

[5] Antonia Azzini, Stefania Marrara, Meiko Jensen and Jorg Schwenk, “*Extending the Similarity-Based XML Multicast Approach with Digital Signatures* , ” Proceedings of the 2009 ACM workshop on Secure web service, 2009, pp. 45-52.