複数の言語に対応するプログラム自動採点サービスにおけるセキュリティ実装

平岡　利規†　　森山　真光†
† 近畿大学大学院総合理工学研究科エレクトロニクス系工学専攻

1. はじめに

プログラミングの学習効率を上げるためにプログラムの自動採点システムがある[1]. 既存のシステムは単一のアプリケーションであるため, 機能ごとの凝集度が低い, 拡張性が低い問題がある. そのため, 我々は既存システムの機能をサービスとして分割し, 連携を行った[2]. 連携されたサービス(自動採点サービス)は成績や提出物の盗聴, 改ざんを防止するため, セキュリティの実装した通信が必要である. そこで本研究では, 自動採点サービスに我々が提案するテンプレートに基づいた XML 暗号化と XML 署名[3]を実装し, 評価する.

2. セキュリティを実装した自動採点サービス

本研究ではテンプレートに基づいた XML 暗号化と XML 署名を本サービスに実装する. 図 1 に成績情報の XML, 暗号化した XML, 署名を施した XML を示す. 成績情報は提出物を特定することができる<score>以下すべての子要素に対して暗号化を行う. また, 改ざんを防止するためにすべての要素に対して署名を施す.

```
<score>
 <id>提出物ID</id>
 <uid>ユーザ名</uid>
 <qid>問題名</qid>
 <status>成否判定</status>
 <message>エラー文
 </message>
</score>
```

```
<score>
  <EncryptedData>
    <EncryptionMethod/>
    <KeyInfo>
    <EncryptedKey>
      <EncryptionMethod/>
      <CipherData>
        <CipherValue>
        </CipherValue>
      </CipherData>
    </EncryptedKey>
  </KeyInfo>
  <CipherData>
     <CipherValue>
     </CipherValue>
  </CipherData>
  </EncryptedData>
</score>
```

```
<score>
 <id></id>
 <uid></uid>
 <qid></qid>
 <status></status>
 <message/>
 <Signature>
  <SignedInfo>
   <CanonicalizationMethod/>
   <SignatureMethod/>
   <Reference>
    <Transforms>
     <Transform/>
    </Transforms>
    <DigestMethod/>
    <DigestValue>
    </DigestValue>
   </Reference>
  </SignedInfo>
  <SignatureValue>
  </SignatureValue>
  <KeyInfo>
   <KeyValue>
   </KeyValue>
  </KeyInfo>
 </Signature>
</score>
```

図1. 成績情報の XML(左上)と暗号化した XML(左下), 署名を施した XML(右)

3. 結果・考察

824 件の成績情報の XML に対して暗号化(Enc), 復号化(Dec), 署名(Sign), 署名の検証(Val)処理をそれぞれDOMを用いた手法(DOM)とテンプレートを用いた手法(Temp)で施した. 図 2 に XML 暗号化と XML 署名の処理時間の比較を示す. 図 2 より, テンプレートを用いた手法はEnc, Dec, Sign, Val でそれぞれ 32.5%, 23.3%, 8.0%, 48.9%の処理速度の減少が見られた. Temp を用いることですべての平均処理時間は 1ms 以下となった. また, 自動採点サービスにおいて提出物が同時に 50 件ある場合の平均レスポンスタイムは 4042ms である[2]. 平均レスポンスタイムと比較し, XML 暗号化と XML 署名の処理時間は 0.02%であった. そのため, 提案する Temp は自動採点サービスにおいて有効である.

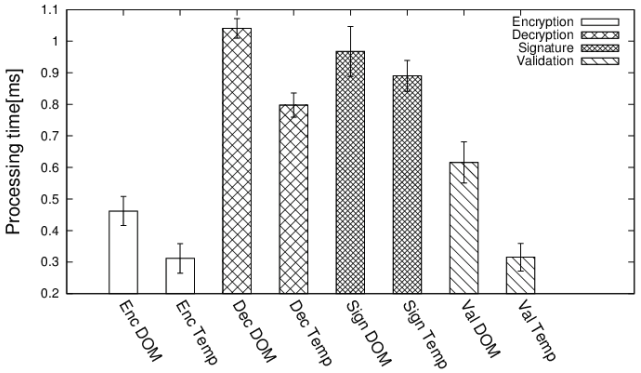

図 2. XML 暗号化と XML 署名の処理時間

4. むすび

自動採点サービスの成績や提出物の盗聴, 改ざんを防止するためテンプレートを用いた XML 暗号化と XML 署名の実装を行った. 自動採点サービスにおいてすべての処理で 1ms 以内に適用できた.

謝辞

本研究は JSPS 科研費 25330426 の助成を受けたものである.

参考文献

[1] Charlie D, et al. : "An Automated Learning System for Java Programming", *IEEE Transactions on Education*, pp.10–17, 2004.
[2] Masamitsu M, Riki H. : “Componentization via Services on Web Applications –in case of automatic programming marking using unit-”, 日本生産管理学会第43回全国大会講演論文集, 2016.
[3] 平岡利規, 森山真光 :「テンプレートに基づいたXML暗号化とXML署名の実装」, 経営情報学会関西支部学生大会, 2016.