# 3-2.互換性、課題と対策 ～XML署名ツール検証報告～

XMLコンソーシアムWeek　2010年3月16日

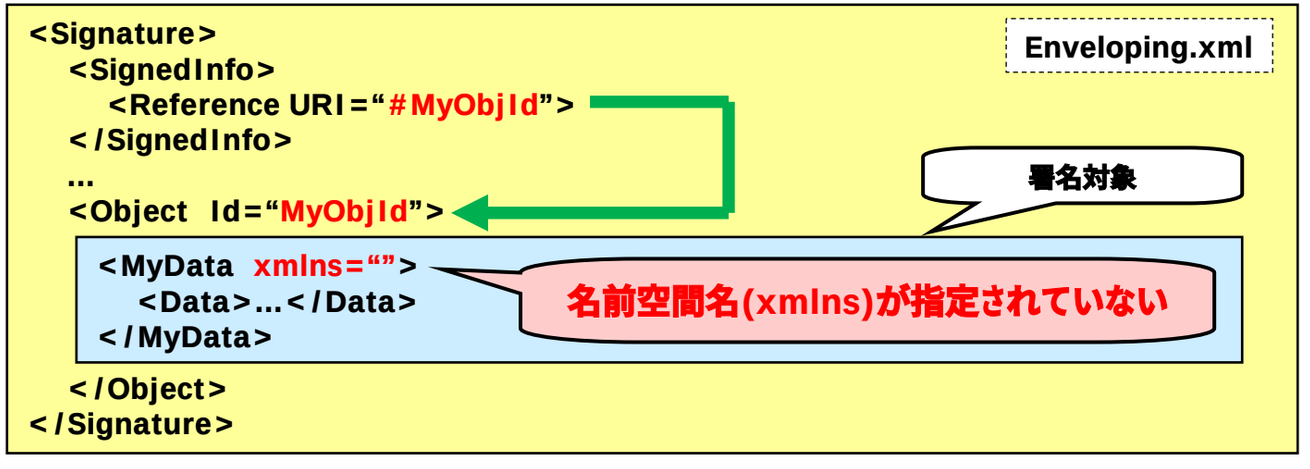
セキュリティ部会

宮地　直人 (ラング・エッジ)

miyachi@langedge.jp

# 昨年の課題

- **Enveloping**の名前空間無しの相互運用性問題
  - **Sun JAVA6** と **.NET** の**API**間で相互運用性が確認できない。
  - 名前空間名が指定されている場合には相互運用性を確認。
  - どちらかが間違っている？**XML**正規化 (**C14N**) の問題か？
  - 試験に使ったプログラムの間違いの可能性は？どこに問題が？



# 問題の明確化

- **Sun Java6 と .NET の SignedXml の違い**
  - **Enveloping署名対象のハッシュ値が異なっている。**
  - 署名値は正しいが署名対象のハッシュ値が不一致だった。

● **署名対象のオリジナルXML**

```
<Object Id="MyObjectId" xmlns="http://www.w3.org/2000/09/xmldsig#">
<MyData xmlns=""><Data Id="D1">book</Data><Data Id="D2">note</Data></MyData>
</Object>
```

● **.NETのハッシュ値と一致する正規化後のXML（注：改行が追加されています）**

```
<Object xmlns="http://www.w3.org/2000/09/xmldsig#" Id="MyObjectId">
<MyData xmlns=""><Data Id="D1">book</Data><Data Id="D2">note</Data></MyData>
</Object>
```

● **Sun Java6のハッシュ値と一致する正規化後のXML（注：改行が追加されています）**

```
<Object xmlns="http://www.w3.org/2000/09/xmldsig#" Id="MyObjectId">
<MyData><Data Id="D1">book</Data><Data Id="D2">note</Data></MyData>
</Object>
```

xmlns="" が省略されている

# プログラムミスが無いか確認

- **XMLSec**でも試してみた
  - http://www.aleksey.com/xmlsec/xmldsig-verifier.html
  - オンラインで検証した結果はやはり **.NET** と一致。
- **IBM Java6**でも試してみた
  - 同一の**class**ファイルを利用して環境のみ切り替えてみた。
  - 結果は **Sun Java6** とは一致せず **.NET** と一致。
- **IBM Java6**で相互運用性が確認されたと言うことは…
  - 同一プログラムなのでプログラムミスでは無いのではないか？
- 結論としてはプログラムミスの可能性は小さいと判断した

# まとめ

- やはり **Sun Java6**の問題のように思える
  - 今後**Sun**のコミュニティに報告して行きたいと考えている。
- 現時点での対応方法
  - 自分の**XML**（署名対象）には名前空間名をきちんとセットする。
  - **名前空間名付きEnvelopingはSun Java6も相互運用可能。**
- **IBM Java6とSun Java6のXML署名は別実装のようだ**
  - 同じプログラムが実行できるので相互運用性の確認に便利だ。
- 電子署名特に**PKI**の世界では相互運用性は重要
  - **XML署名のような基本APIのテスト項目等の整備が必要なのでは。**