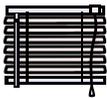


# WS-Policy 仕様

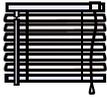
セキュリティ部会  
(株)JIEC 工藤 奈緒美



# 目次



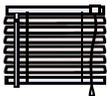
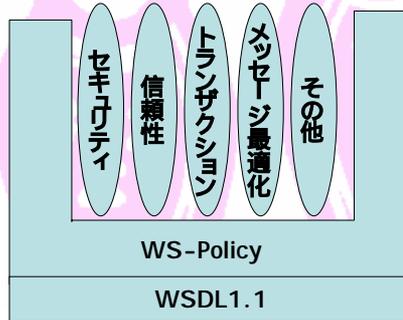
- WS-Policy
- WSDL との関係
- WS-Policy モデル
- WS-Policy フレームワーク
- ドメイン固有表明
  - WS-SecurityPolicy
- WSIT での実装
- まとめ



# WS-Policy



- WS-Policy 仕様とは、Web サービスの定義言語である WSDL で表現できない規則(ポリシー)を表現する XML を使用した記述ルール。
- Webサービスの能力、要件(制約)を表現するもの。



# wsdl1.1 で表現できること



- wsdl (<http://schemas.xmlsoap.org/wsdl/>) で表現できること

- 通信プロトコル
- 操作
- 電文形式

テレフォンバンキング・サービスの4つの操作

残高照会

支払先検索

支払先登録

支払

口座情報

検証コード

支払先リスト

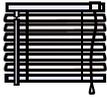
支払先

請求書情報

支払状況

テレフォンバンキング通信プロトコルはSOAP

PhoneBankingSOAP  
<http://www.complere.com/>

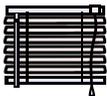


# WS-Policy 関連仕様



- ポリシー記述の枠組み
  - WS-Policy Framework [W3Cで標準化中]
  - WS-PolicyAttachment [W3Cで標準化中]
- ドメイン固有表明(Assertions)
  - WS-SecurityPolicy (セキュリティ) [OASIS で標準化中]
  - WS-RM Policy (高信頼メッセージング) [OASIS で標準化中]
  - WS-BA Policy (WS-BusinessActivity) (トランザクション) [OASIS で標準化中]
  - AT Policy (WS-AtomicTransaction) (トランザクション) [OASIS で標準化中]
  - WS-MTOMP Policy (メッセージ送信の最適化) [標準化団体未提出]
- ポリシー取得プロトコル
  - WS-MetadataExchange (メタデータ取得) [標準化団体未提出]

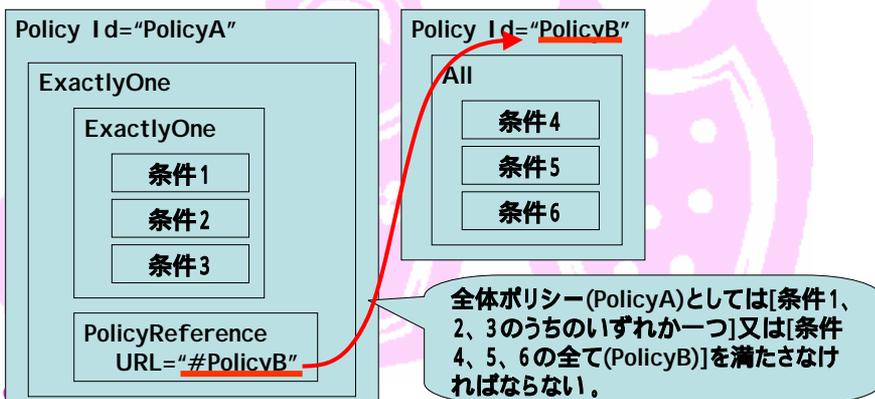
:

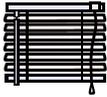


# WS-Policy モデル



- ポリシーは複数のポリシーを含むことができる。
- 複数ポリシーを AND または OR 条件で組み合わせることができる。

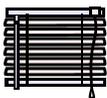
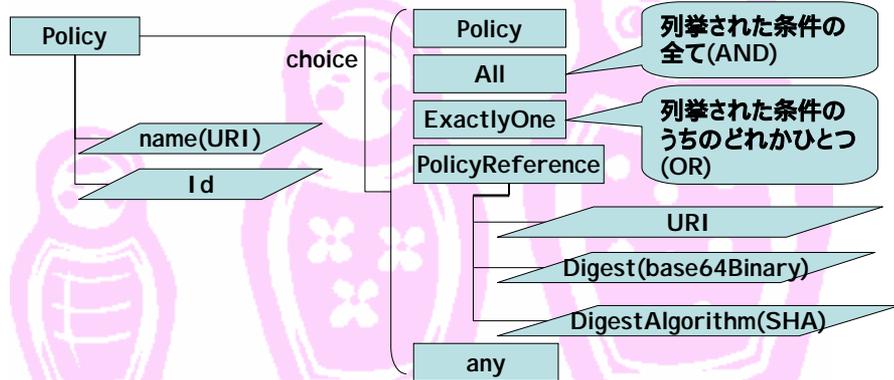




# WS-Policy Framework



<http://schemas.xmlsoap.org/ws/2004/09/policy/ws-policy.xsd>



## WS-Policy のスキーマ (抜粋)



```

<!-- //////////// WS-Policy //////////// -->
- <xs:element name="Policy">
- <xs:complexType>
- <xs:complexContent>
+ <xs:extension base="tns:OperatorContentType">
</xs:complexContent>
</xs:complexType>
</xs:element>
<xs:element name="All" type="tns:OperatorContentType" />
<xs:element name="ExactlyOne" type="tns:OperatorContentType" />
- <xs:complexType name="OperatorContentType">
- <xs:sequence>
- <xs:choice minOccurs="0" maxOccurs="unbounded">
  <xs:element ref="tns:Policy" />
  <xs:element ref="tns:All" />
  <xs:element ref="tns:ExactlyOne" />
  <xs:element ref="tns:PolicyReference" />
  <xs:any namespace="##other" processContents="lax" />
</xs:choice>
</xs:sequence>
</xs:complexType>

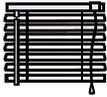
```

ポリシー要素の型

tns:OperatorContentType

繰り返し: 0 ~ ポリシー自体あってもなくても良い

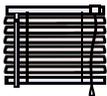
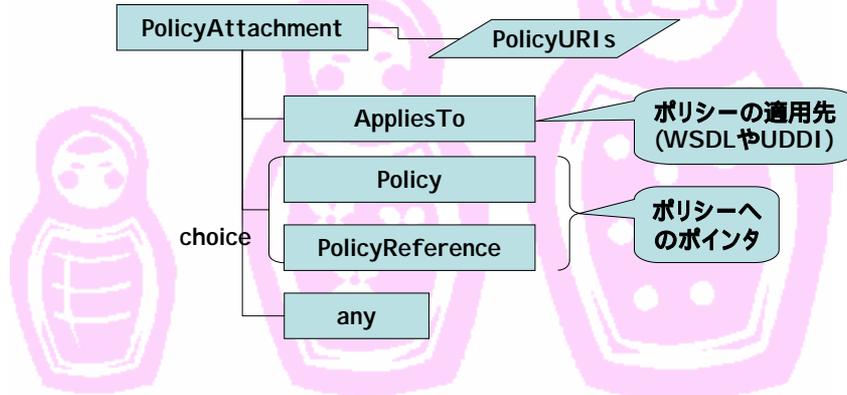
拡張可能



# WS-PolicyAttachment



<http://schemas.xmlsoap.org/ws/2004/09/policy/ws-policy.xsd>



# WS-PolicyAttachment のスキーマ (抜粋)



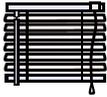
```

<!-- //////////// WS-PolicyAttachment //////////// -->
+ <xs:attribute name="PolicyURI s" />
- <xs:element name="PolicyAttachment" />
- <xs:complexType>
  - <xs:sequence>
    <xs:element ref="tns:AppliesTo" />
    <xs:choice maxOccurs="unbounded" />
      <xs:element ref="tns:Policy" />
      <xs:element ref="tns:PolicyReference" />
    </xs:choice>
  - <!--
    omitted only because it causes the content model to be non-deterministic
    <xs:element ref="wsse:Security" minOccurs="0" />
  -->
  <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
  <xs:anyAttribute namespace="##any" processContents="lax" />
</xs:complexType>
</xs:element>
+ <xs:element name="AppliesTo" />

```

Callouts from the diagram:

- `PolicyAttachment`: Webサービス本体 (wsdl)への紐付け
- `tns:AppliesTo`: ポリシーへの紐付け
- `tns:Policy` and `tns:PolicyReference`: ポリシーへの紐付け
- `xs:any`: 拡張可能



# WS-SecurityPolicy



<http://schemas.xmlsoap.org/ws/2005/07/securitypolicy>

**Webサービスのセキュリティに関する仕様**

**メッセージ保護方法(署名、暗号化)の表明方法**

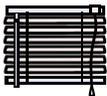
**セキュリティ・トークン(構成要素)の表明方法**

- ・ ユーザ名/パスワード
- ・ X.509証明書
- ・ Kerberosチケット
- ・ SAMLアサーション
- ・ RELライセンス
- ・ WS-SecureConversationのセキュリティ・コンテキスト・トークン

**署名、暗号化のアルゴリズムの表明方法**

- ・ AES、3DES、SHA、RSAなどを利用

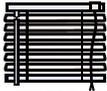
**鍵交換方式などの指定**



# WSIT とは



- ・ WSIT = Web Services Interoperability Technology
- ・ Java プラットフォームと .NET プラットフォームの相互運用性促進を目的に、SunMicrosystems が各種 Webサービス技術をまとめた実装
- ・ オープンソース
- ・ WSIT のチュートリアル  
(<http://java.sun.com/webservices/interop/reference/tutorial/doc/index.html>) で使用している設定ファイル  
WS-Policyを含んだWSDLのフォーマットを利用



# WSIT 設定ファイル



```

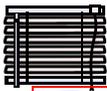
<?xml version="1.0" encoding="UTF-8"
definitions
  xmlns:xsi="http://www.w3.org/2001/XMLSchema"
  xmlns:wsd="http://schemas.xmlsoap.org/wsdl/"
  xmlns:wsdl:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:wsu="http://docs.oasis-open.org/ws-s2004-01/ws-s200401-wsu-wssecurity-utility-1.0.xsd"
  xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
  xmlns:wsrm="http://schemas.xmlsoap.org/ws/2005/02/rm/policy"
  xmlns:wsrel="http://schemas.xmlsoap.org/ws/2005/02/rm/policy"
  xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/policy/optimizedforserialization"
  xmlns:wsa10="http://schemas.xmlsoap.org/ws/2004/08/policy"
  xmlns:wsa11="http://www3.org/2005/08/addressing"
  xmlns:wsa12="http://schemas.sun.com/2006/03/ws/rt/rtserver"
  xmlns:wsa13="http://java.sun.com/xml/ws/wsrt/policy"
  message
  portType
  binding
  service
  wspPolicy
  wspPolicy
  wspPolicy
  
```

Eclipse SDK 3.2.1  
WTP(Web Tools Platform)プラグイン  
XML Editor

WSDL

WS-Policy

© )



# WSIT 設定ファイル



1. 計算機サービス全体のポリシー

このAll直下のポリシーを全て満たす必要がある

アドレッシングを使用

プライベートキーを保存したファイルにアクセスする仕組み

Java keystore を使用

信頼性のある証明書を保存したファイルにアクセスする仕組み

1.1. 共有鍵のポリシー

1.2. Trust10のポリシー

1.3. 署名に使用する要素のポリシー

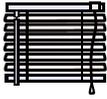
1.4. Wss11のポリシー

Sun/WSIT 独自のもの

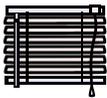
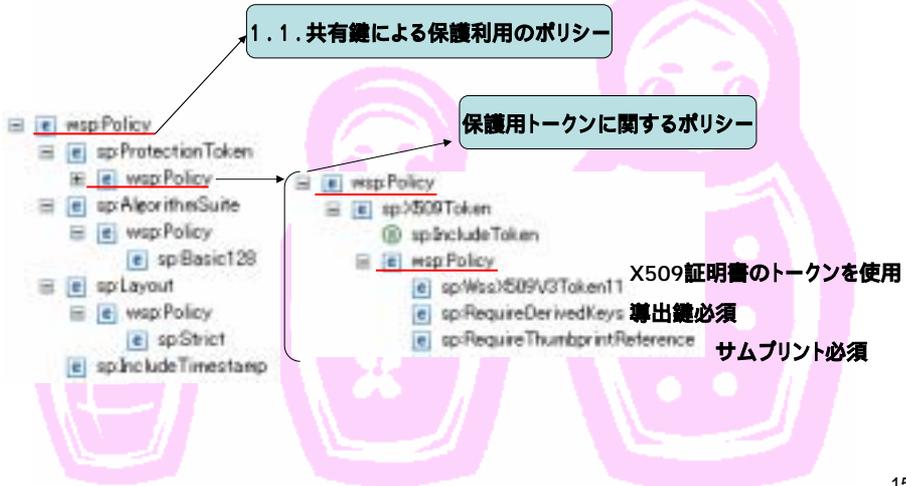
ポリシー 表明

```

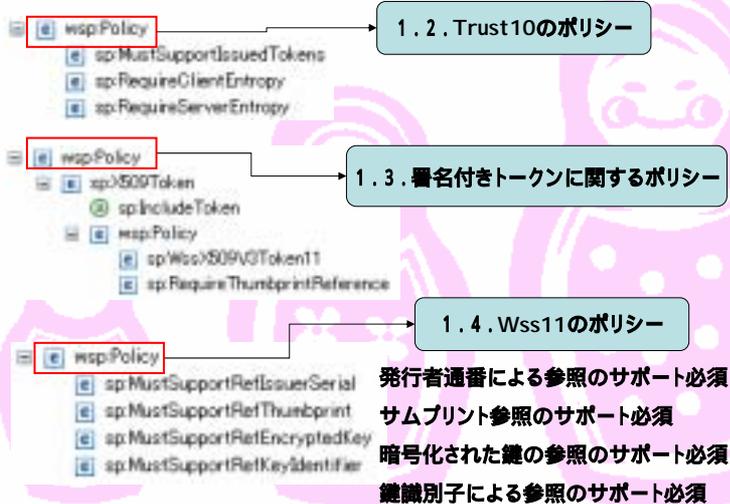
wspPolicy
  wspAll
    wsa:UsingAddressing
    sc:KeyStore
    sc:TrustStore
    sp:SymmetricBinding
    wspPolicy
    sp:Trust10
    sp:SignedSupportingTokens
    wspPolicy
    sp:Wss11
    wspPolicy
  
```

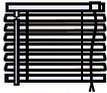


# WSIT 設定ファイル



# WSIT 設定ファイル





# WSIT 設定ファイル



2. 計算機入力のポリシー

このAll直下のポリシーを全て満たす必要がある

暗号化対象は SOAP の Body 部分

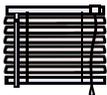
暗号化要素は特に指定なし

署名対象はSOAP の Body 部分と Header の一部

署名要素は特に指定なし

© XML Consortium 2005,2006

17

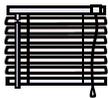


# まとめ

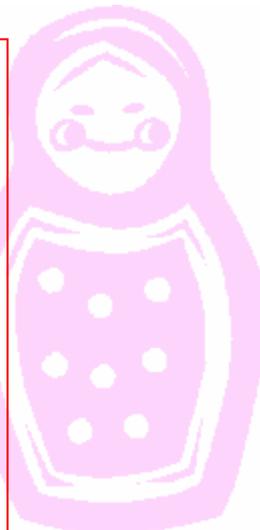
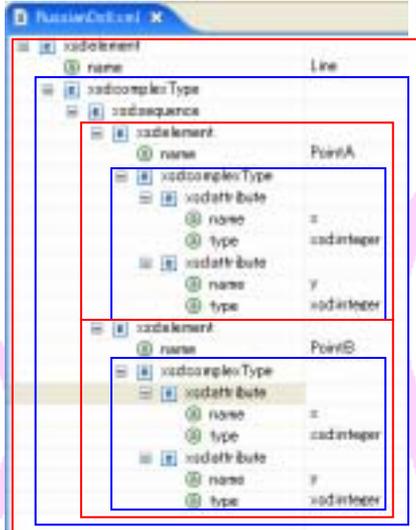


- WS-Policy は、Web サービスの WSDL で表現できない部分(ポリシーを表現するもの)。
- WS-Policy は、様々のドメイン固有ルールを組み合わせるルール。



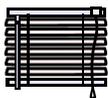


## (参考) XMLスキーマのデザインパターン ロシアン・ドール

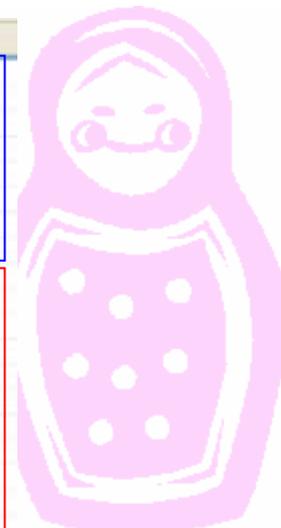
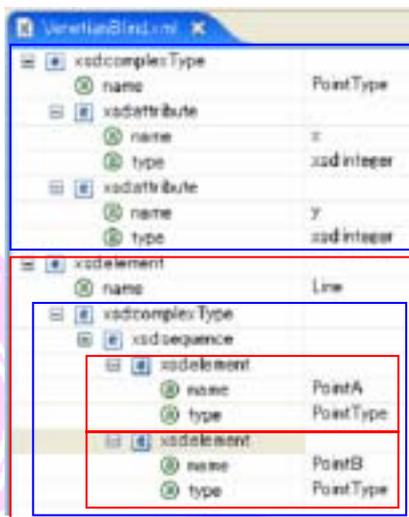


19

© XML Consortium 2005,2006

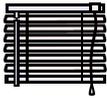


## (参考) XMLスキーマのデザインパターン ベネチアン・ブラインド

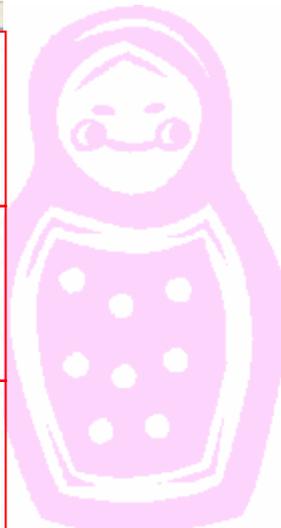
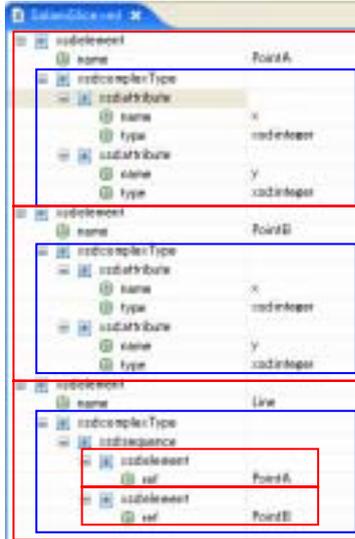


20

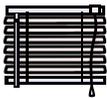
© XML Consortium 2005,2006



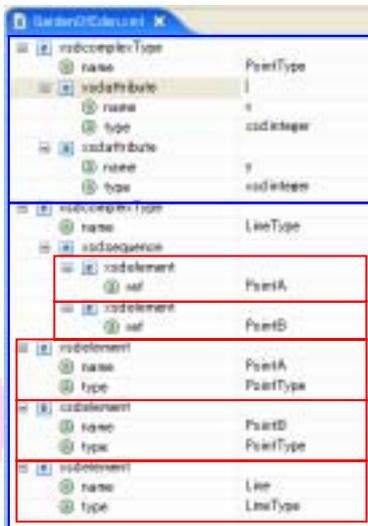
(参考) XMLスキーマのデザインパターン  
**サラミ・スライス**



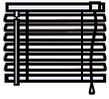
21



(参考) XMLスキーマのデザインパターン  
**ガーデン・オブ・エデン**



22



お疲れ様でした

