XML Consortium

[第五回 XMLコンソーシアムWeek]

暗号化XMLデータ利用技術についての課題と対策

【事例のご紹介】

TravelXMLを活用した
旅行商品取引Webサービス実証実験

2006年 5月24日

XMLコンソーシアム Webサービス実証部会
松山 憲和 (PFUアクティブラボ株式会社)
matsuyama.nori@pfu.fujitsu.com

XML Consortium

アジェンダ

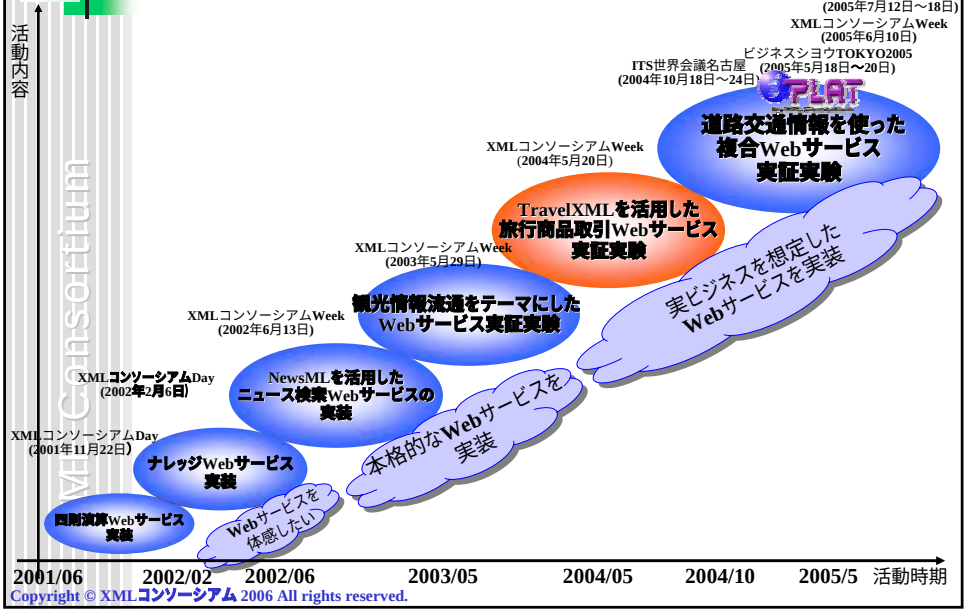
- 『TravelXMLを活用した
  旅行商品取引Webサービス』の概要
- セキュリティ 実証実験評価
- WS-Security利用上の課題解決に向けて

XML Consortium

[第五回 XMLコンソーシアムWeek]

TravelXMLを活用した 旅行商品取引Webサービス実証実験 概要のご紹介

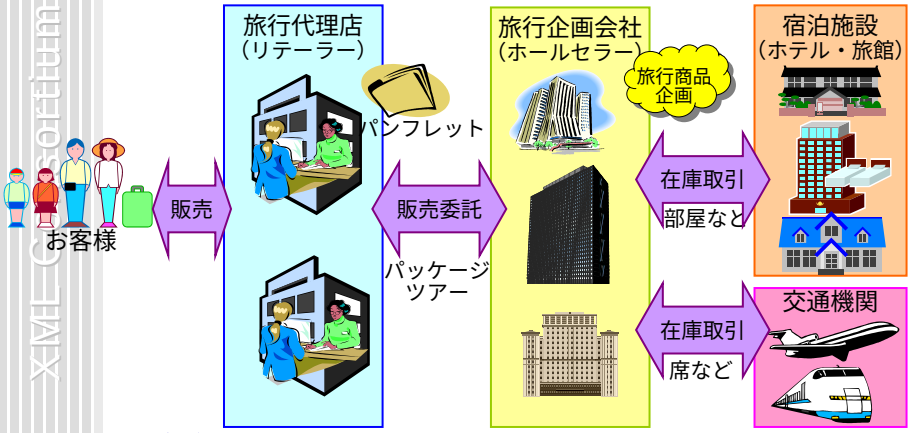
XMLコンソーシアム 実証実験実施状況



【TravelXMLを活用した旅行商品取引Webサービス】

旅行業界のビジネスモデル

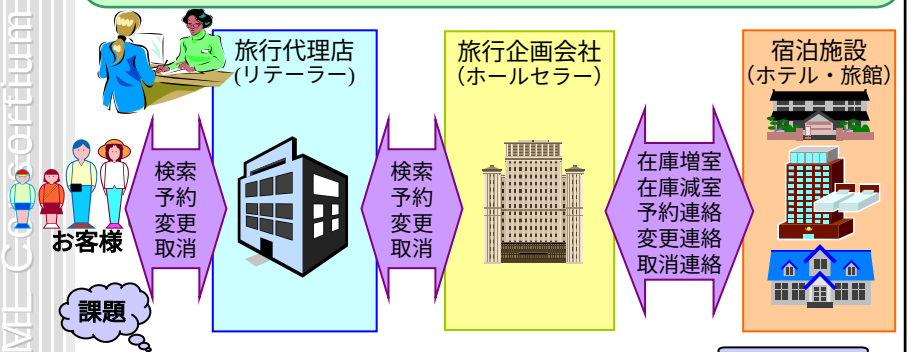
旅行企画会社は、
宿泊施設や交通機関から仕入れた在庫を企画商品化し、
パッケージツアーとして旅行代理店に販売を委託



【TravelXMLを活用した旅行商品取引Webサービス】

旅行の予約業務

- 旅行代理店 ⇔ 旅行企画会社
  - パッケージツアーの検索、予約、変更、取消
- 旅行企画会社 ⇔ 宿泊施設
  - 在庫増室、在庫減室、予約通知、変更通知、取消通知



- 旅行代理店、宿泊施設 ： 取引先毎に端末要
- バッチ処理による在庫のタイムラグ ： 機会損失

TravelXML
&
Webサービス

【TravelXMLを活用した旅行商品取引Webサービス】

実証実験の目的

TravelXMLを使った業務システムの構築

- 日本旅行業協会様とXMLコンソーシアムが共同開発し、標準化を推進しているTravelXML標準に基いて業務システムを構築（TravelXML1.1で実施）

B2BにおけるWebサービスの有効性検証

- 基幹業務（企業間電子商取引）システムにWebサービスの技術を適用
- TravelXMLの通信層にWebサービスを適用することの有効性（メリットの検証）
  - *セキュリティの適用：暗号化、ディジタル署名*

異種製品の相互接続性検証

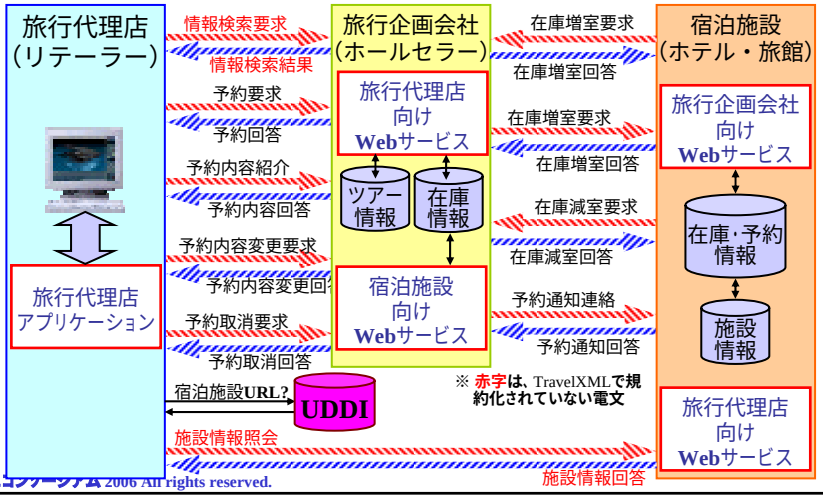
- 各社ミドルウェアの相互接続性の確認
  - ***WS-Security***

【TravelXMLを活用した旅行商品取引Webサービス】

実証実験システム概要

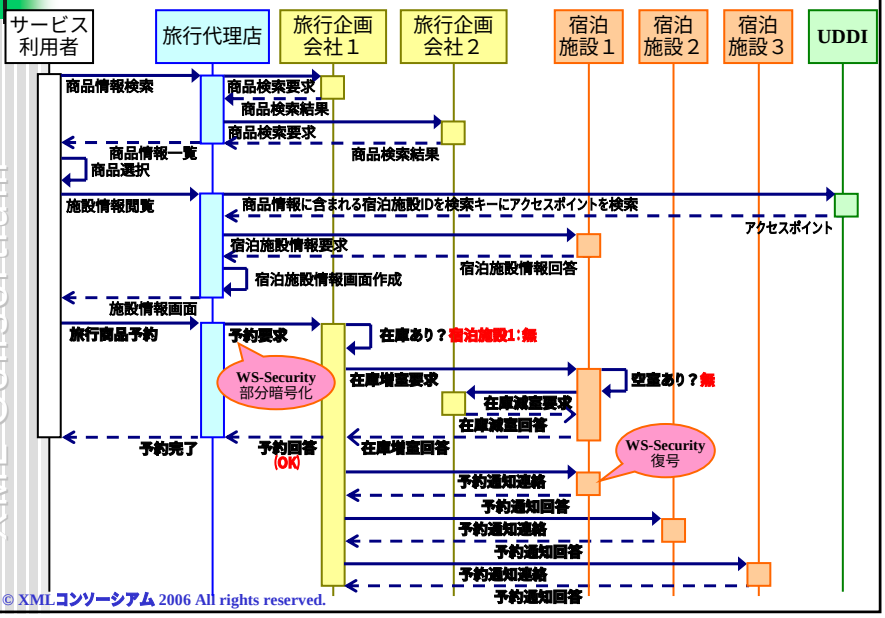
パッケージツアーの予約業務における、旅行代理店、旅行企画会社、宿泊施設間の電子商取引をTravelXML標準に従ってシステム構築

全てをWebサービスで連携



【TravelXMLを活用した旅行商品取引Webサービス】

処理シーケンス



【TravelXMLを活用した旅行商品取引Webサービス】

実証実験システム構成（1）

旅行代理店（リテーラー）	旅行企画会社（ホールセラー）	宿泊施設（ホテル・旅館）
ネットタイムトラベル（ネット・タイム）	アドソル日進旅行（アドソル日進）	東芝ホテル（東芝ソリューション）
ブレイニーワークストラベル（ブレイニーワークス）	HITACHI旅行（日立製作所）	ホテルNEC（NEC）
IBMトラベル（日本IBM）	UNISYS旅行（日本ユニシス）	ホテルUNISYS（日本ユニシス・ソフトウェア）
	IBM旅行（日本IBM）	ホテル日立システム（日立システムアンドサービス）
	インフォテリア旅行（インフォテリア）	ホテルIONA（日本アイオナ）

UDDI：宿泊施設UDDI（ブレイニーワークス）

セキュリティ：ハードウェア（東京エレクトロン）	セキュリティ：ソフトウェア（日立製作所）	セキュリティ：ソフトウェア（日本IBM）

SOAP Monitor（PFUアクティブラボ）

【TravelXMLを活用した旅行商品取引Webサービス】

実証実験システム構成（2）

XML Consortium

旅行代理店（リテーラー）	旅行企画会社（ホールセラー）	宿泊施設（ホテル・旅館）
Apache Tomcat 4.1.24 MySQL V4.0.18	Tomcat 4.1.24	Tomcat 4.1.30 MySQL V4.0.17
IBM WebSphere V5.1 IBM DB2 V8.1	HITACH Cosminexus V6 HiRDB V7	NEC ActiveGlobe WebOTX Ver5.3 Oracle Database 9i
	MS BizTalk Server 2004 SQL Server 2000	BEA WebLogic Platform 8.1J
	IBM WebSphere V5.1 DB2 UDB V8.1	PolarLake Database Integrator Oracle Application Server 10g Oracel Database 10g
	Infoteria ASTERIA 3	IONA Artix 2.0.3
セキュリティ：ハードウェア DataPower XS40	セキュリティ：ソフトウェア Apache XML Security	セキュリティ：ソフトウェア IBM XML Security Suite for Java

UDDI
IBM WebSphere UDDI Registry

SOAP Monitor

【TravelXMLを活用した旅行商品取引Webサービス】

開発/接続実験スケジュール

XML Consortium

2003年				2004年				
10月	11月	12月	1月	2月	3月	4月	5月	6月

▲部会 ▲部会 ▲部会 ▲特別集会 ▲Day ▲部会 ▲部会 ▲部会 ▲部会 ▲Week ▲総会

企画/調査 → 仕様検討 → 実装 → テスト

★プロジェクト開始(10/26)

▲第一回接続実験（3/26）
▲第二回接続実験(4/7)
▲第三回接続実験（4/16）
▲第四回接続実験（4/19）

★内覧会(4/20)

▲第五回接続実験（5/11）
▲第六回接続実験（5/14）
▲第七回接続実験（5/15）
▲第八回接続実験（5/18）
▲第九回接続実験（5/19）

★ニュースリリース(5/20)

内覧会(場所：東京エレクトロン)

第六回接続実験(場所：日立製作所)

【TravelXMLを活用した旅行商品取引Webサービス】

実証実験システム：開発規模

XML Consortium

開発期間	6ヶ月間（企画～設計～実装～テストまで）		
開発者数	総勢 37名		
参加企業	15社（ご協力頂いた社団法人日本旅行業協会様、旅行電子商取引促進機構様、**TravelXML**部会を除く）		
実装工数	合計：232 人日	旅行代理店（リテーラー）	41人日/3サーバ
		旅行企画会社（ホールセラー）	61人日/5サーバ
		宿泊施設（ホテル・旅館）	94人日/5サーバ
		UDDI,セキュリティ,**SOAPMonitor**	36人日
実装規模	合計：約90,000 **Step** （**Asteria**、**PolarLake** などステップ数換算できないものを除く）	旅行代理店（リテーラー）	20.7 **KStep**/3サーバ
		旅行企画会社（ホールセラー）	26.8 **KStep**/4サーバ
		宿泊施設（ホテル・旅館）	29.8 **KStep**/5サーバ
		UDDI,セキュリティ, **SOAPMonitor**	12.8 **KStep**
接続実験回数	約2ヶ月に9回		
使用した製品数	合計：20製品 （**バージョン・レベルが異なる製品は1つと数えた**）	**Web**サービス関係	10製品
		RDB	5製品
		業務パッケージ	1製品
		セキュリティ関係	4製品

XML Consortium

【第五回 XMLコンソーシアムWeek】

セキュリティ 実証実験評価と課題

セキュリティの確保

- 予約情報･個人情報の安全性の確保
  - 旅行の予約では個人の情報を扱う場合が多く、取引する情報の高い安全性の確保が必要になる。
  - 電子商取引に必要な否認防止、情報改竄防止、秘匿性の確保を署名認証技術や部分暗号化技術により実現。

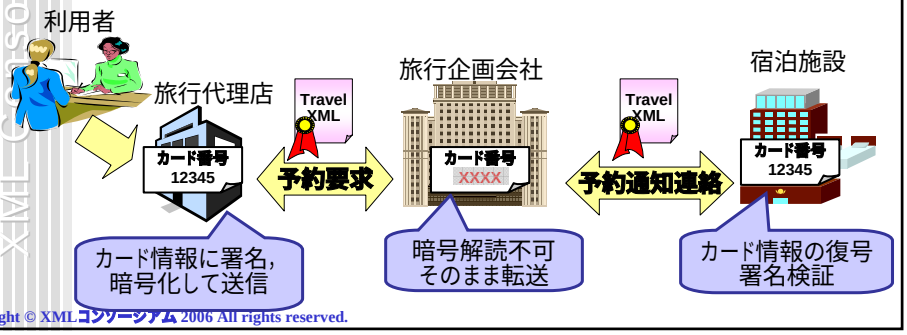
セキュリティ面から見た 実証実験の目的

- ビジネスシナリオベースで**Web**サービスのセキュリティを検証
- **Web**サービスにおける主なセキュリティ要件
  - 秘匿性確保，認証，改ざん検出，否認防止
- **SSL**などの既存技術を利用することで・・・
  - 通信路のセキュリティを確保することはできる
  - ただし**End to End**のセキュリティは確保できない
    - 中継者に全ての情報が開示されてしまう
    - 宿泊施設がリテーラーを認証することができない

本実証実験では，**WS-Security**を用いた
End to Endのセキュリティの検証を実施

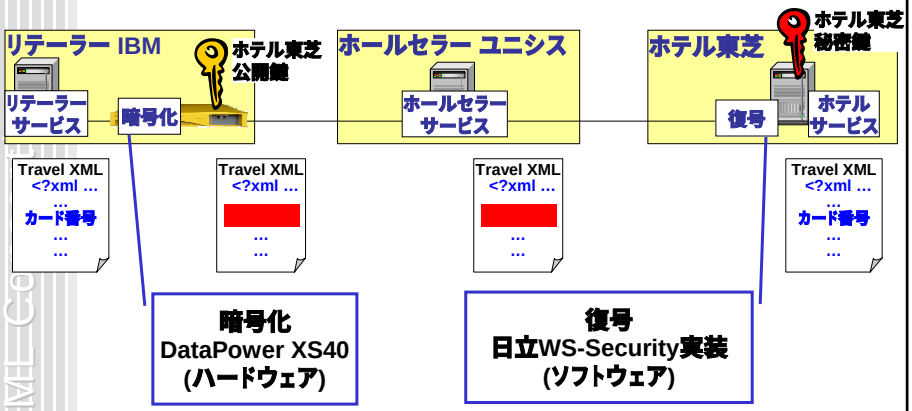
セキュリティ・シナリオの概要

- デモシナリオの想定
  - 身元保証としてクレジットカード情報を利用
    旅行代理店は，旅行企画会社を介して宿泊施設にカード情報を送信
    旅行企画会社はカード情報を知る必要はない
  - カード番号の部分暗号，部分署名を行なう
- メリット
  - 宿泊施設だけにカード情報を開示することが可能
    旅行企画会社は不要な機密情報の管理責任を負う必要がない
  - 宿泊施設が，旅行代理店の署名を検証をすることができる
    認証，改ざん検出，否認防止に利用可能



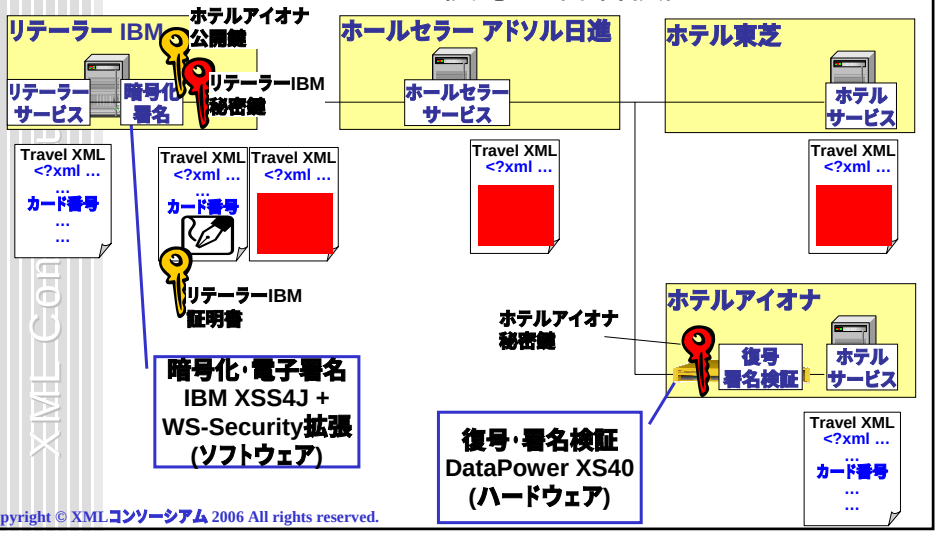
セキュリティ検証実験（1）

- ハードウェア装置で暗号化
- ソフトウェアで復号



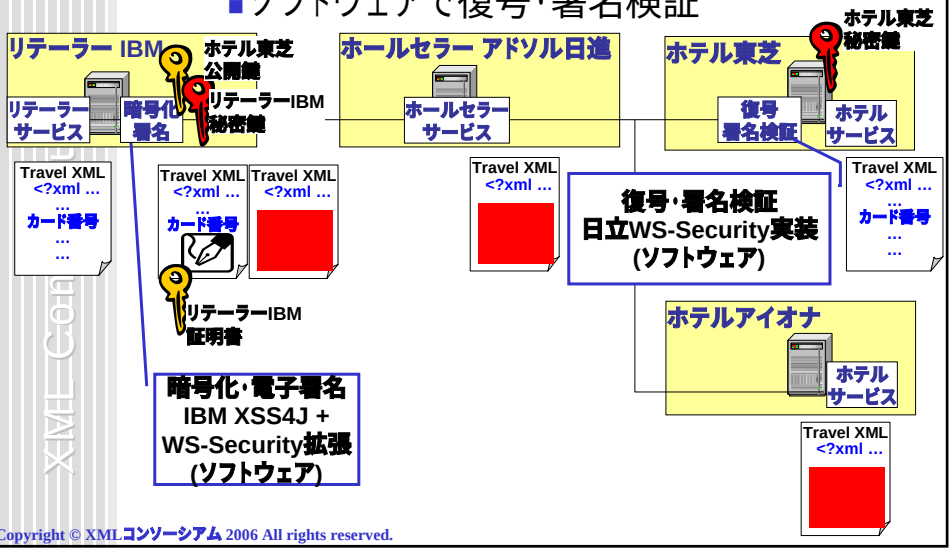
セキュリティ検証実験（2）

- ハードウェア装置で暗号化・署名
- ソフトウェアで復号・署名検証



セキュリティ検証実験（3）

- ソフトウェアで暗号化・署名
- ソフトウェアで復号・署名検証



【TravelXMLを活用した旅行商品取引Webサービス】

セキュリティ実装評価（1）

Webサービスで必要となる機能と実証実験におけるカバー範囲

セキュリティ上の課題	適用技術の例	検証
1）接続相手の識別と認証	SSL/TLS, WS-Security	ー
2）データ作成元の証明と認証	WS-Security, 暗号/署名	○
3）データの完全性		
3-1）通信中データの保護	SSL/TLS	-
3-2）SOAPメッセージの保護	XML電子署名（WS-Security）	○
4.データ機密性		
4-1）通信中データの機密性	SSL/TLS	-
4-2）SOAPメッセージの機密性	XML暗号（WS-Security）	○
5.メッセージの一意性保証	[タイムスタンプや乱数値] ＋XML電子署名	未

注：●課題項目はWS-I Security Scenarios (Working Group Draft 0.15)より
●今回検証=○、未検証＝未
●SSLは周知の技術として検証の必要無し(ー)と判断

【TravelXMLを活用した旅行商品取引Webサービス】

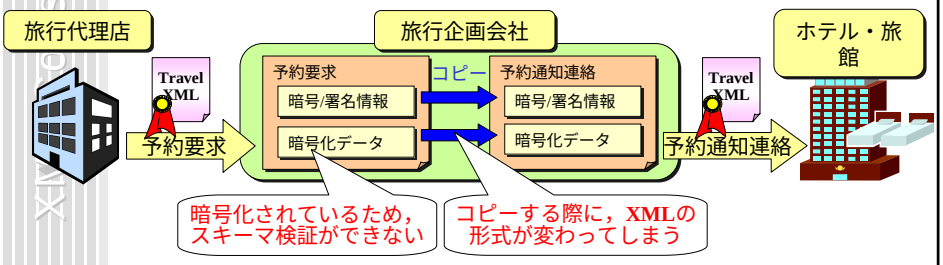
セキュリティ 実証実験評価（2）

WS-Security利用のメリット

- セキュリティ機能を部品として利用可
- 暗号/署名処理(XMLレベル)の相互接続性は問題なし

実装上の課題，問題点

- WS-Securityバージョンの相異 (SOAPレベル)
  - ➡ 今後，OASIS標準仕様に統一
- 処理負荷の増大について今後検証が必要
- ３者間通信の場合，中継者の実装に注意が必要



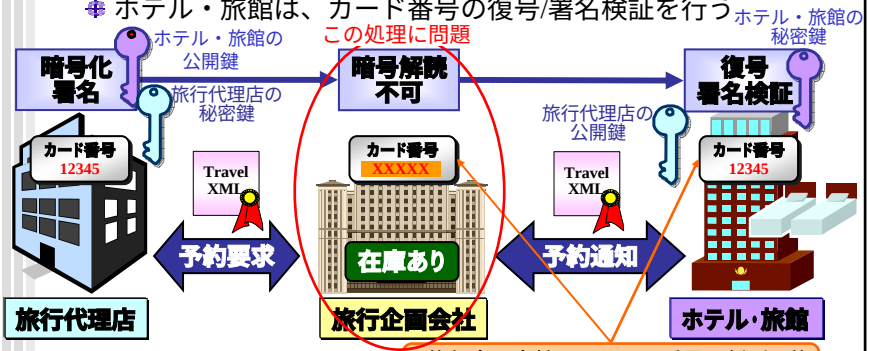
【TravelXMLを活用した旅行商品取引Webサービス】

セキュリティ 実証実験評価（3）

Webサービス(WS-Security)の場合の課題（1）

【TravelXMLを活用した旅行商品取引Webサービス実証実験】における利用例

- 旅行代理店は、カード番号の署名/暗号化を行う
- 旅行企画会社は、カード番号を解読できないまま、ホテル・旅館に予約内容を通知する
- ホテル・旅館は、カード番号の復号/署名検証を行う

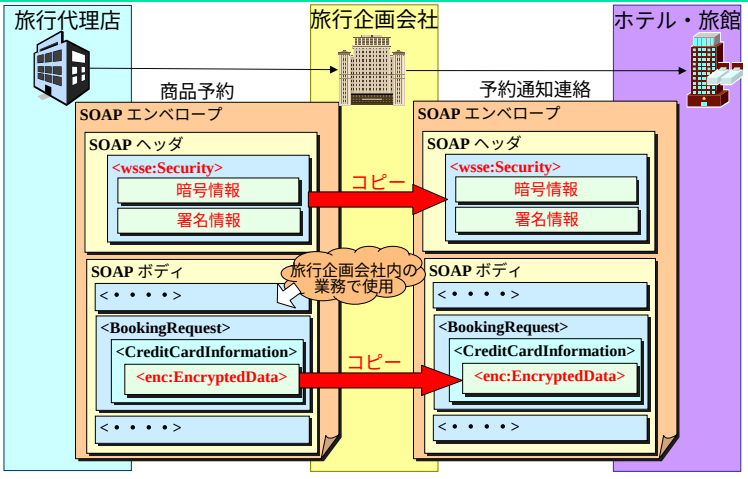


■旅行企画会社にはカード番号は判別不能
■ホテル・旅館はカード番号を復号できる

【TravelXMLを活用した旅行商品取引Webサービス】

セキュリティ 実証実験評価（4）

Webサービス(WS-Security)の場合の課題（2）



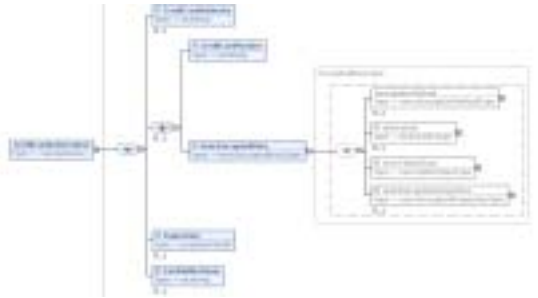
課題
- 旅行企画会社が受け取る商品予約のSOAPメッセージの妥当性検証ができない
  - ➢AXISのようなWebサービス開発ツールをそのまま利用することが困難

【TravelXMLを活用した旅行商品取引Webサービス】

セキュリティ 実証実験評価（5）

Webサービス(WS-Security)の場合の課題：まとめ

- 旅行代理店から送信された暗号化されたデータを含むSOAPメッセージを、受け取る旅行企画会社は妥当性検証を行なうことができない
  - 暗号化されたXMLインスタンスは、スキーマ構造が変わってしまうため妥当性検証ができない
- どの要素を暗号化するのかは、事前に関係者間で決めておく必要がある。
  - スキーマ策定時に暗号化すべき要素を事前に決めるのは困難。
  - 暗号化される要素を含んだ要素は別スキーマになる。



XML Consortium

【第五回 XMLコンソーシアムWeek】

WS-Security利用上の課題とその解決に向けて

WS-Security利用上の課題とその解決に向けて

XML Consortium

益々、重要になるセキュリティ

- **Web2.0、SOA**で再び見直されている**Web**サービス
  - 基盤技術として定着
- 増えるインターネット詐欺
  - スパイウェア
  - フィッシング
  - ファーミング(**pharming**)：**hosts**ファイル改竄、**DNS**ポイズニング
- 実業務への適用を通して見えてくる技術課題
  - できれば事前検証したいが…→実証実験が重要

課題の洗い出し/分析
課題対策/方式の模索

“ 実検証の場 ” が重要

XML Consortium

XML Consortium

[第五回 **XML**コンソーシアム**Week**]

ご清聴ありがとうございました。