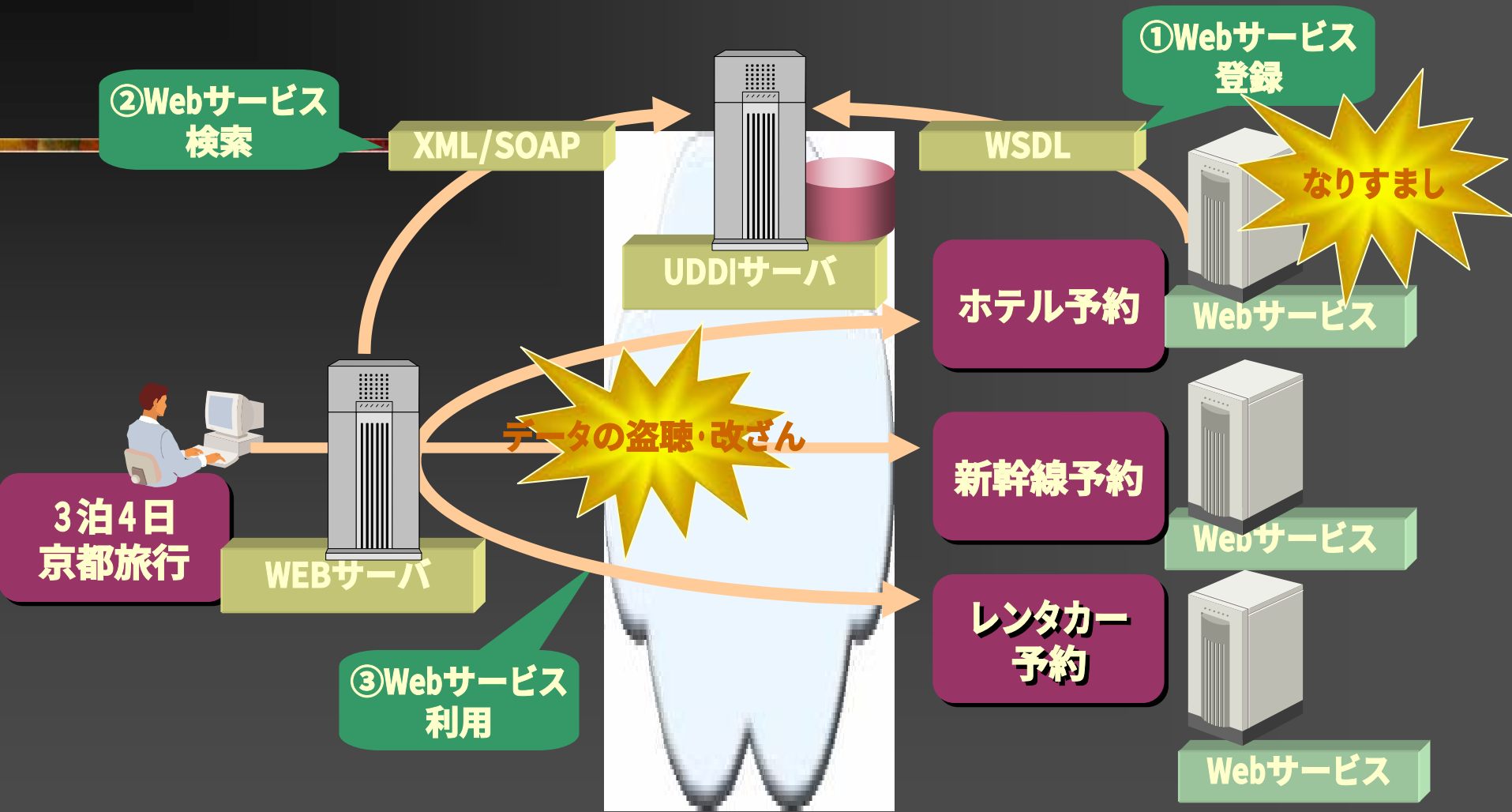
Webサービスにおける相互接続実証への取り組み
～セキュリティ分科会報告～

DOPG
セキュリティ分科会
松永和男

0．構成

- Webサービスの拡大とセキュリティの重要性
  - Webサービスの利用例
  - 情報セキュリティの脅威と動向
- セキュリティ分科会の活動の御紹介
  - セキュリティ分科会のこれまでの活動成果
- セキュリティ分科会の現在の活動と今後の取り組み
  - SOAP-SSL セキュリティ相互運用実験の成果
  - 今後の取り組み

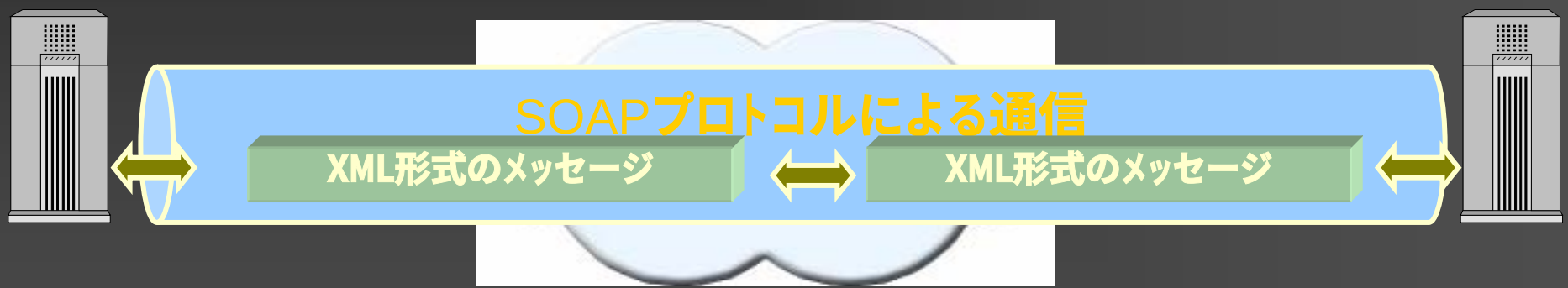
1．1Webサービスの利用例



SOAP:Simple Object Access Protocol
WSDL:Web Service Description Language
UDDI:Universal Description,Discovery,and Integration

1．2Webサービスを実現するセキュリティ技術

XML署名/暗号	XML文書に電子署名を付加、暗号化により盗聴・改ざんを防ぐ
SOAP on HTTPS	ネットワーク上の通信電文を暗号化する。更に、通信相手を認証することで、盗聴・改ざんを防ぐ



関連技術	XKMS:PKIの鍵管理運用を簡易化することを目指す技術 www.w3.org/TR/xkms/ SAML:Webサービス間のシングルサインオンを実現する技術 www.oasis-open.org./committees/security/

HTTPS:SSLプロトコルによるセキュリティを実現。
XKMS:XML key Management Specification
SAML:Security Assertion Markup Language

2．情報セキュリティの脅威と動向

回復･対策に要する
膨大な損害コスト

セキュリティ不備によるビジネスリスクの増大

信用の失墜･
経営者の責任問題

訴訟問題･損害賠
償への発展

企業活動の停止･
継続の危機

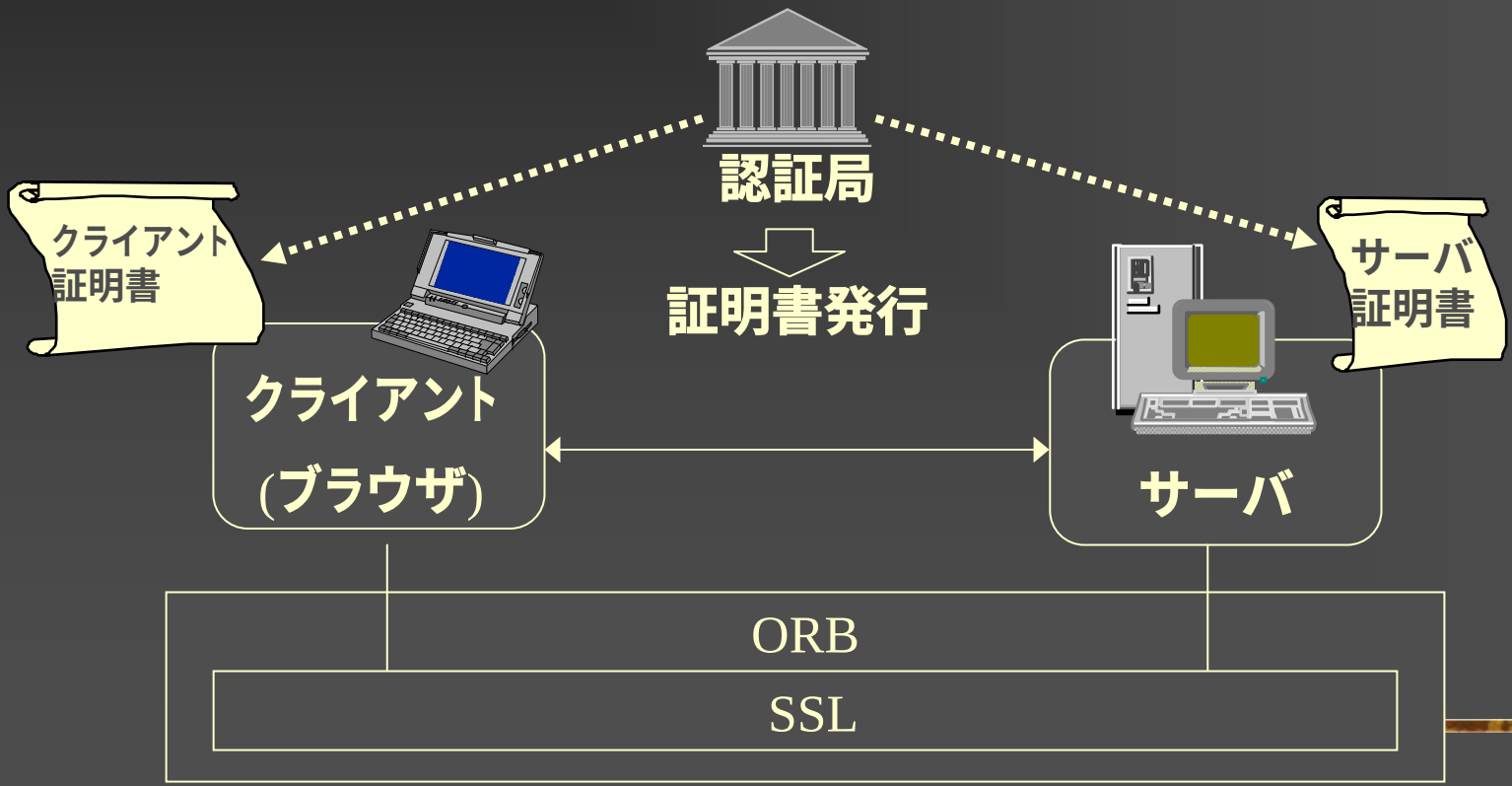
ブロードバンド時代は、
セキュリティをおろそかにしては、
企業活動が成り立たない時代

3．1　セキュリティ分科会の活動

- **目的：**
  CORBA/Webサービスに関する
  セキュリティ普及・推進
  (相互接続性の確認他)
- **活動履歴**
  * 2000年　3月セキュリティ分科会発足
  * **主な活動**：SSL-IIOP**実験実施**(2000)

3．2　SSL-IIOP接続実験の成果（1）

- システム構成
  - * 共通の認証局からサーバ，クライアントにSSL証明書を発行。



3．3　SSL-IIOP接続実験の成果（2）

- CORBA環境でSSLを用いたセキュリティのマルチベンダ接続の確認
  - 4ベンダ製品での相互運用性の確認に成功
  - 暗号レベルの相互接続性の確認
    - 3-DES, DES(40bit), RC4(40bit), RC2
  - ＳＳＬプロトコルの相互接続性の確認
    - SSL V3による接続に成功
- SSL接続のためのノウハウ蓄積
  - 証明書配布インタフェース
  - 証明書形式

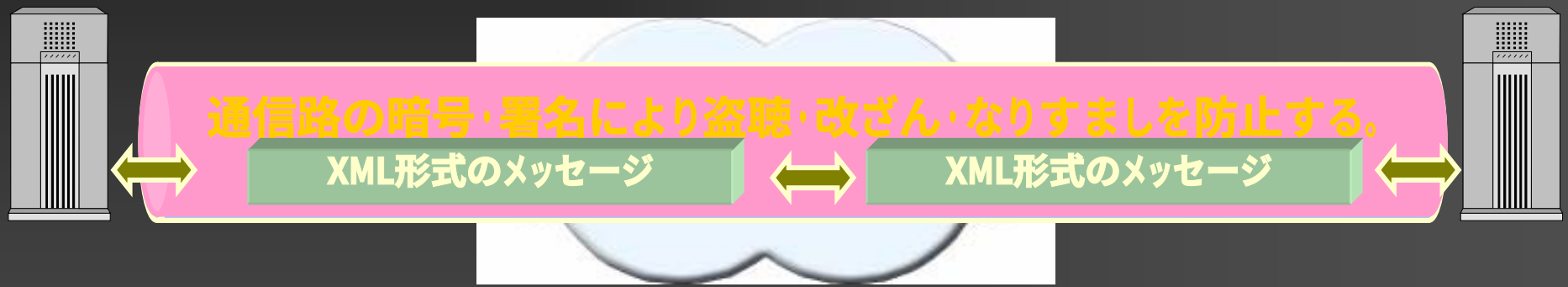
4．1　SOAP-SSL接続実験の目的

- 各ベンダ製品の相互運用性の確認
  - 顧客システムがマルチベンダ製品で構成される事を想定した事前の確認
  - マルチベンダシステム構築におけるノウハウの蓄積
    ⇒実際の御客様システム構築時に有効に活用
- Webサービス普及に向けて、顧客に安心して御利用頂くための実績作り
- 接続実験により得られる課題･改善項目の製品へのフィードバック

4．2　今回の接続実験の検討

XML署名/暗号

Webサービスに適用するための、標準仕様が検討の段階。製品実装に時間がかかる。



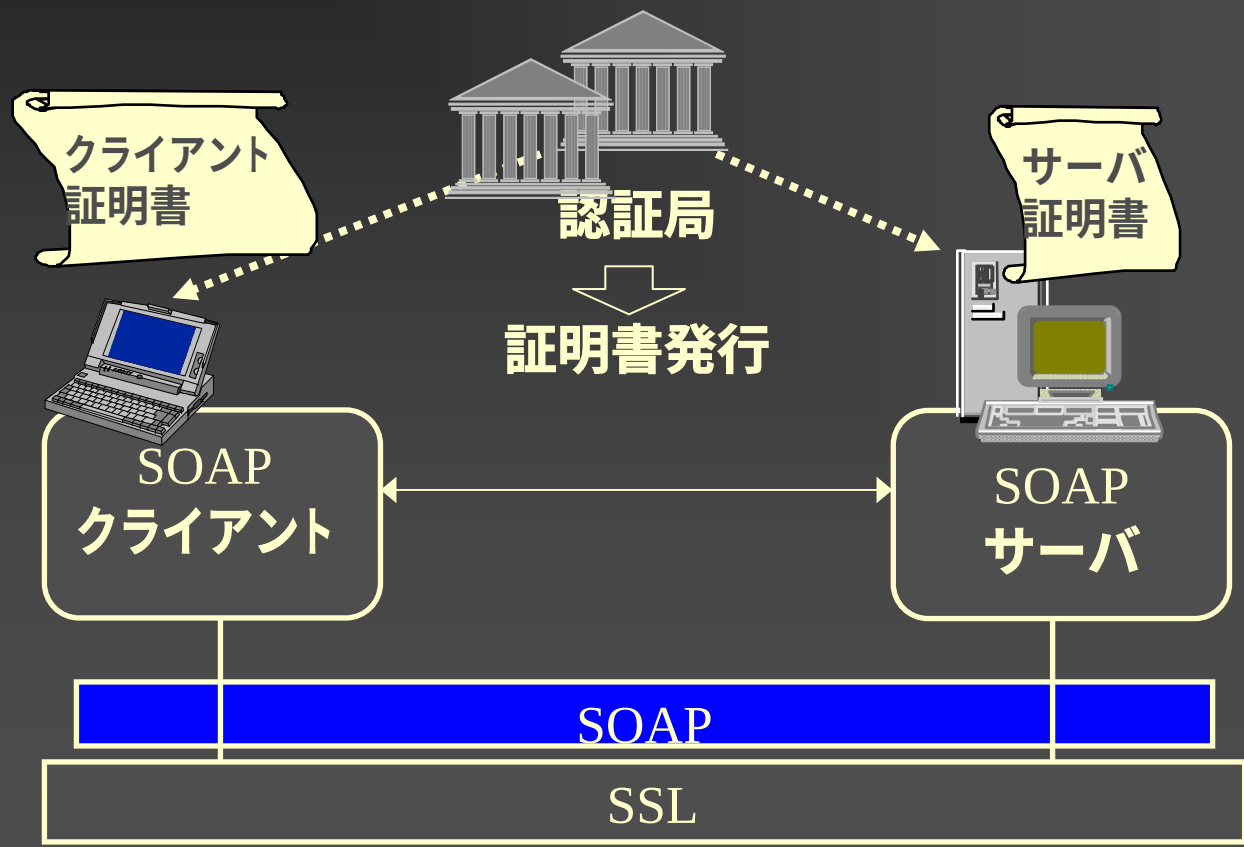
SOAP on HTTPS

接続仕様が確定している。
各社製品が実装段階にある。⇒実験で検証

4．3　SSL接続実験の構成

システム構成

認証局からサーバ，クライアントにSSL証明書を発行。



4．4　SSL(V3)による接続手順

4．5　SSL接続実験の条件

- テストツール
  - DOPG相互運用分科会で実証済みのテストケースをそのまま利用する。(「SOAP製品間でのデータ型網羅性に関する実証」から抜粋)
  - 上位アプリケーションに影響なくセキュリティ実現
- 実験参加ベンダ製品の総当たり組合せを実施。(4社)
- SSLプロトコルバージョン
  - V2,V3 (サーバ認証,サーバ＋クライアント相互認証)
- 暗号アルゴリズム、鍵長
  - サーバ･クライアント間のネゴシエーションで決定

5．1　実証実験結果（1）

製品名	クライアント	WebOTX	Oracle9*i*AS Release2	minexus	Interstage
サーバ	社名	NEC	日本オラクル	日立	富士通
WebOTX	NEC	◎	◎	◎	◎
Oracle9*i*AS Release2	日本オラクル	◎	◎	◎	◎
Cosminexus	日立	◎	◎	◎	◎
Interstage	富士通	◎	◎	◎	◎

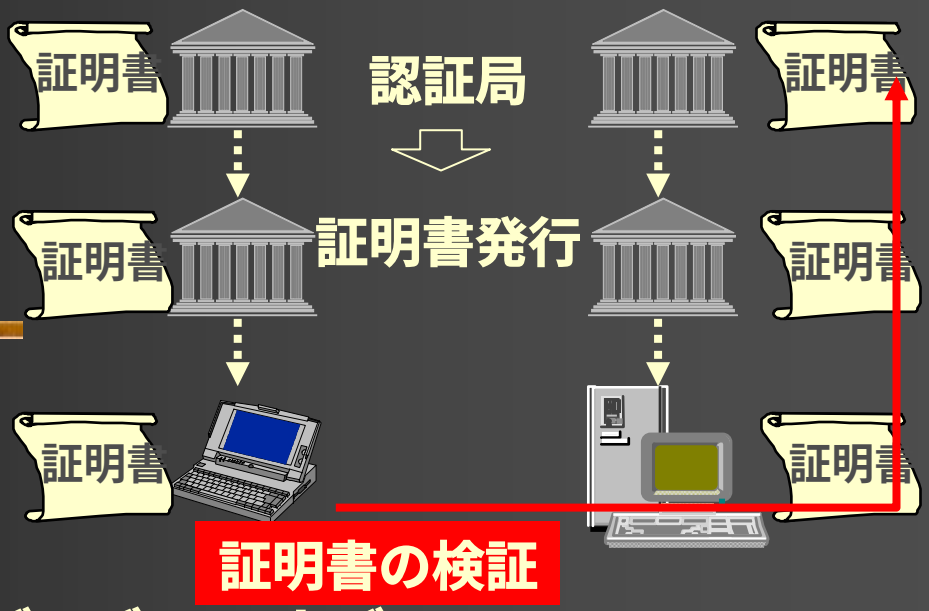
◎: 接続成功　(2003年5月30日現在)

- **日本電気** : ActiveGlobe WebOTX Ver5.1
- **日本オラクル** : Oracle9i Application Server Release 2 (9.0.3)
- **日立製作所** Cosminexus Version 5
- **富士通** : Interstage Application Server V5.0

5．2　実証実験結果（2）

- 実験に使用した証明書
  - Publicな認証サービス機関から発行される証明書と同等の証明書で接続テスト完了
- 暗号アルゴリズム
  - SSL_RSA_RC4_128_SHA
  - SSL_RSA_RC4_128_MD5
- SOAPメッセージとSSLプロトコルを組み合わせたセキュアな通信が可能であることを確認した。
  - *Webサービスの盗聴の防止が可能*
  - *Webサーバに対するなりすまし、改竄等の攻撃を防御可能*

5．3　成果･ノウハウ



- テスト準備段階
  - 認証局の選定
  - SSLで使用する暗号アルゴリズムのネゴシエーション
  - 証明書の有効期限管理･世代交代運用
- ノウハウ
  - 各社製品の環境構築時に、利用する暗号アルゴリズムを設計し、設定しておく必要がある。
  - 証明書検証用の上位証明書の入手･インストール
    - 通信相手の証明書を発行した認証局の証明書
    - 認証局が階層となっている場合の中間認証局証明書

6．　今後の取り組み

- Webサービス普及に向けた相互運用性の確認
  - OASIS,WSセキュリティ,業界標準に従い製品レベルでの相互運用性の確認を先行して実施していく。
  - 顧客システム構築のためのマルチベンダ接続テストを事前に実施することに意義。(日程・作業負担・コスト)
    - セキュリティに関する接続テストは容易ではない。
    - 事前準備からセキュリティ技術者が参加必要。
    - トラブル時の調査・対応が"むずかしい"ことがある。
- セキュリティはWebサービス分野において一層重要に
  - 特に認証やシングルサインオン実現の取り組みが活発。
  - SAML,Liberty Alliance,etc.

http://www.dopg.org/