図解XML規格（セキュリティ編）
～セキュリティ関連XML規格の最新動向～
第2版

2002年6月10日

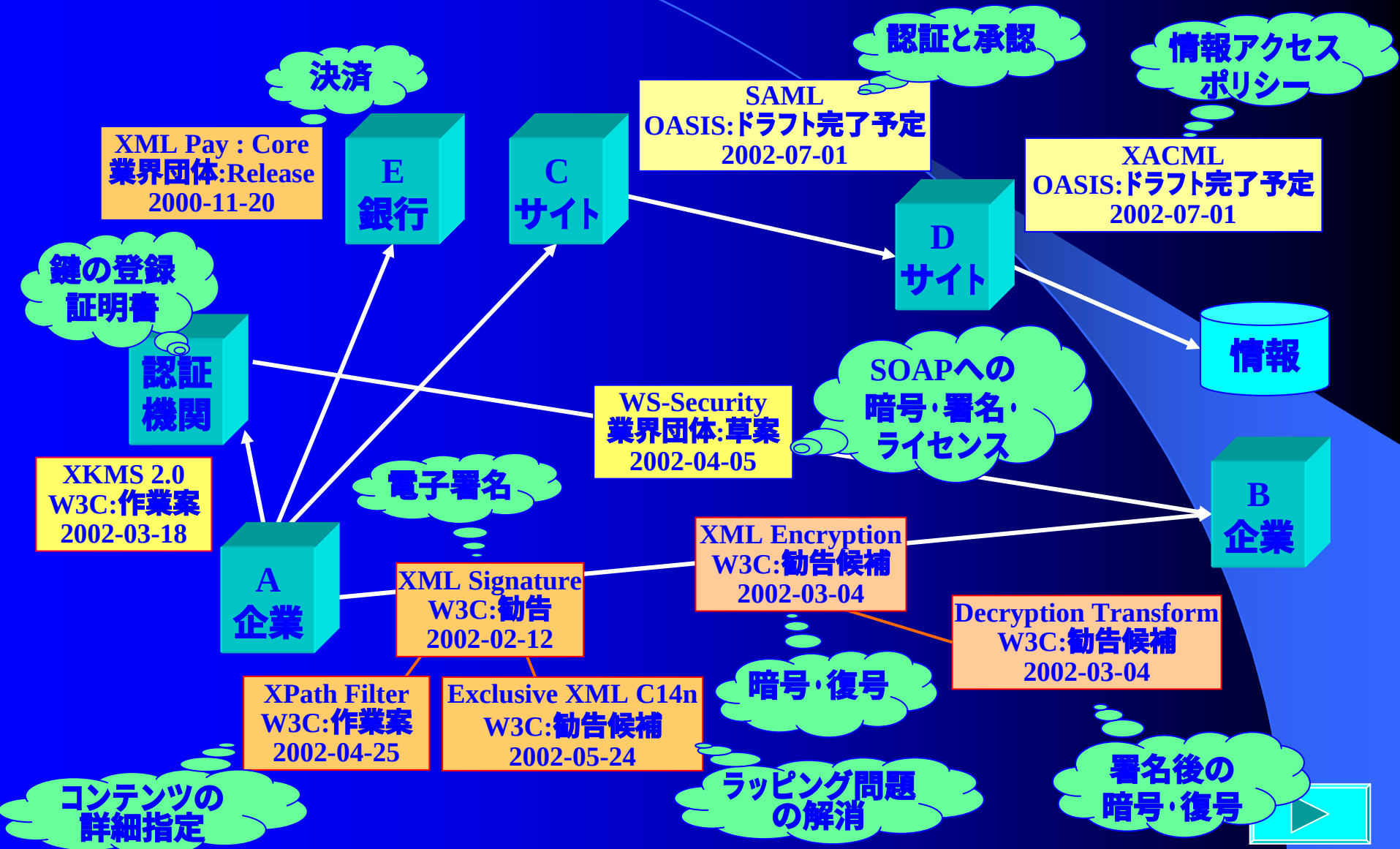
XMLコンソーシアム 基盤技術部会
共通基盤WG セキュリティSWG

メンバ紹介

- 富士ゼロックス (株)　　道村 唯夫
- ミノルタ (株)　　上田 隆司
- 沖電気工業 (株)　　池上 勝美

セキュリティ関連XML規格

Update

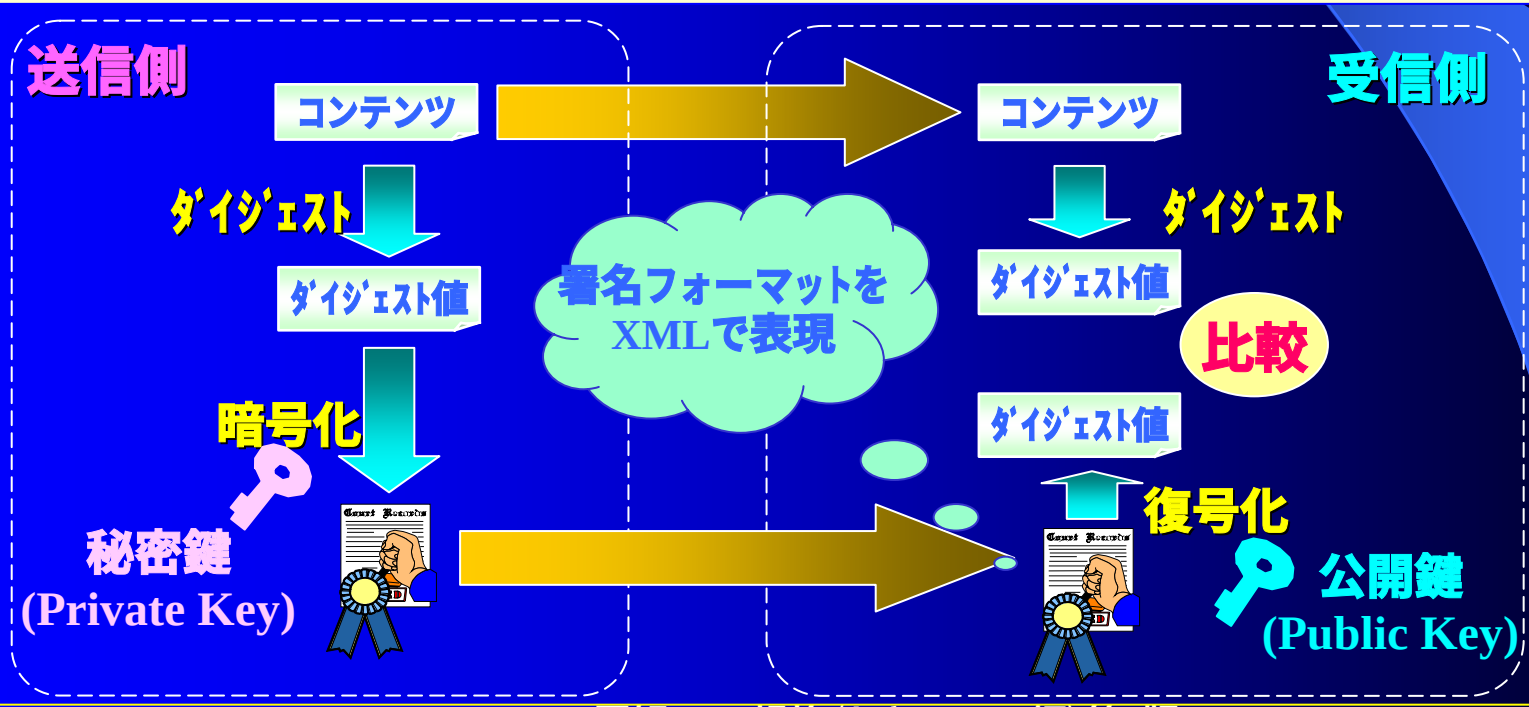


XML-Signature

電子署名の情報をXMLで表現する
W3Cで制定。2002-02-12 勧告

/2000/09/xmldsig#

- コンテンツの改ざんを検出する
- PKIと連動して送信側の否認を防止する
- 部分、複数コンテンツに対しての署名をサポートする



XML-Signature構文例

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod
   Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    </CanonicalizationMethod>
    <SignatureMethod  Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
     <Reference URI="#MyFirstSignature">
       <Transforms>
         <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
       </Transforms>
       <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
       <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
     </Reference>
  </SignedInfo>
  <SignatureValue>MC0CFFrVLtRlk.....=</SignatureValue>
  <KeyInfo>
    <KeyName>xmlTarou@xmlcon.com#DSAKey</KeyName>
  </KeyInfo>
  <Object Id="MyFirstSignature">
    <TestData>ようこそXMLコンソーシアム</TestData>
  </Object>
</Signature >
```

署名対象

アルゴリズム

SignedInfo：
署名の情報

SignatureValue：
署名値

KeyInfo：
公開鍵関連情報

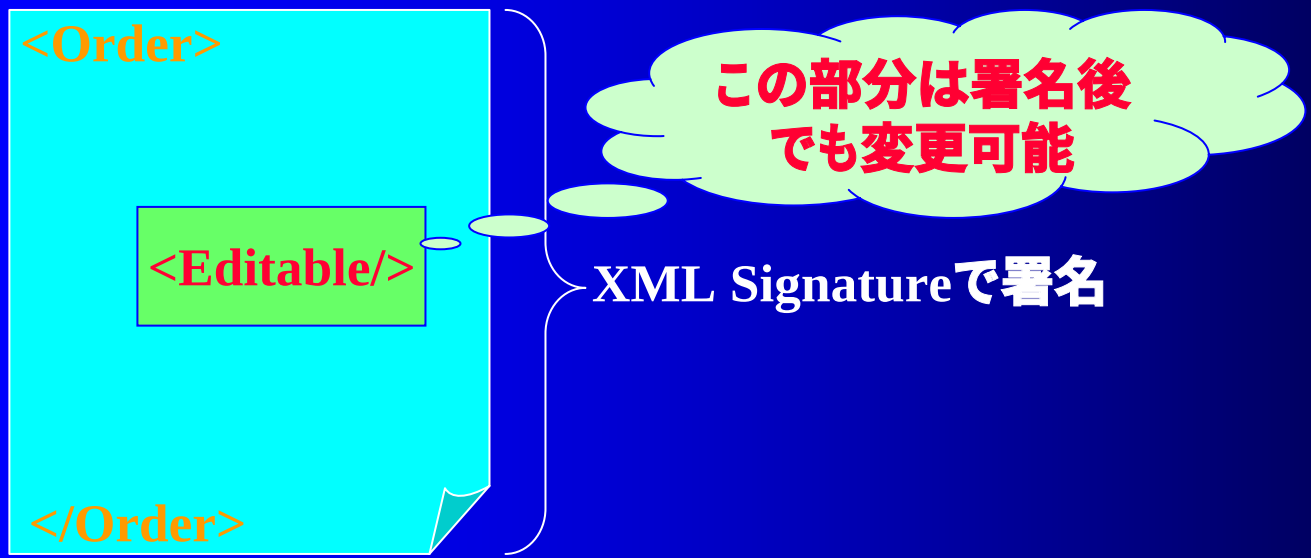
Object：
署名対象

XML-Signature XPath Filter 2.0

XPathの仕様を拡張する
W3Cで検討。2002-04-25 作業案。

/2002/04/xmldsig-filter2

・コンテンツ（署名対象）の詳細な指定が可能になる。
  ・Enveloped Signature（とりわけマルチサイン）の指定を明確にする
  ・署名後に変更可能な部分の指定が可能になる

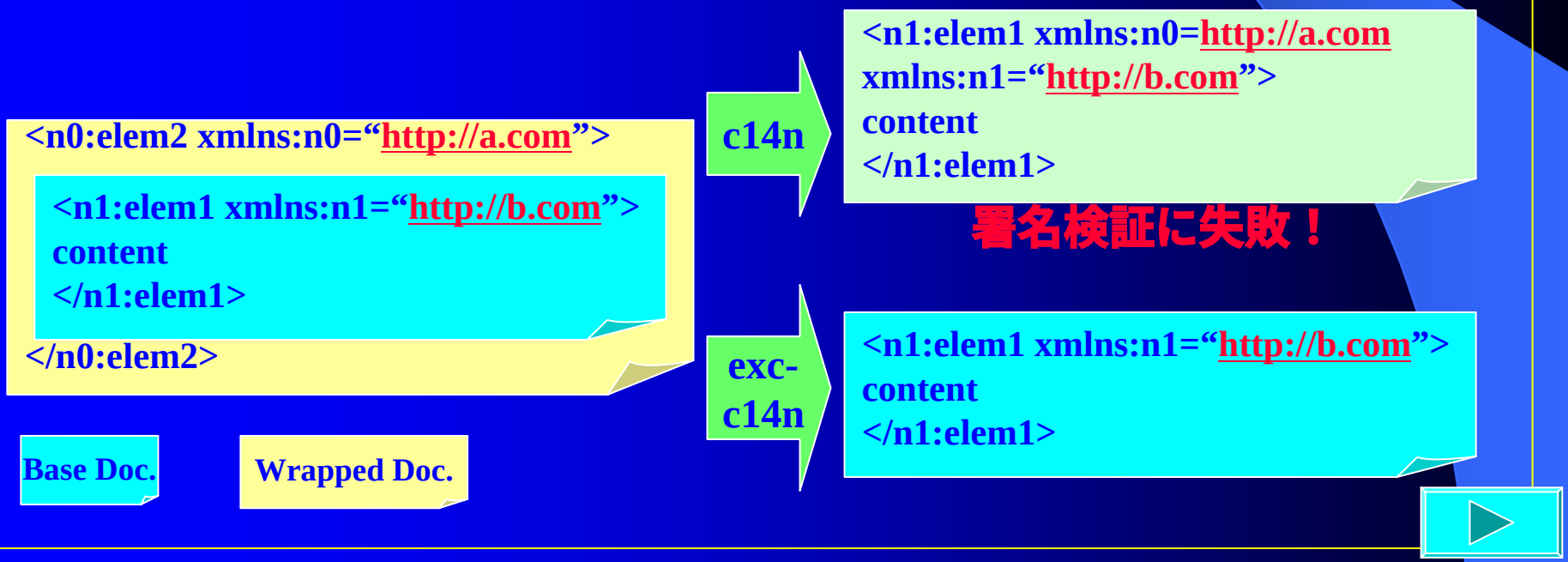


Exclusive XML Canonicalization

再ラッピング時の正規化問題を解決する
W3Cで検討。2002-05-24 勧告候補。

/2001/10/xml-exc-c14n#

・署名つきのXML 文書を別なName Space付き文書でラッピングするときに発生する問題を解決するアルゴリズム（処理手順）を規定する

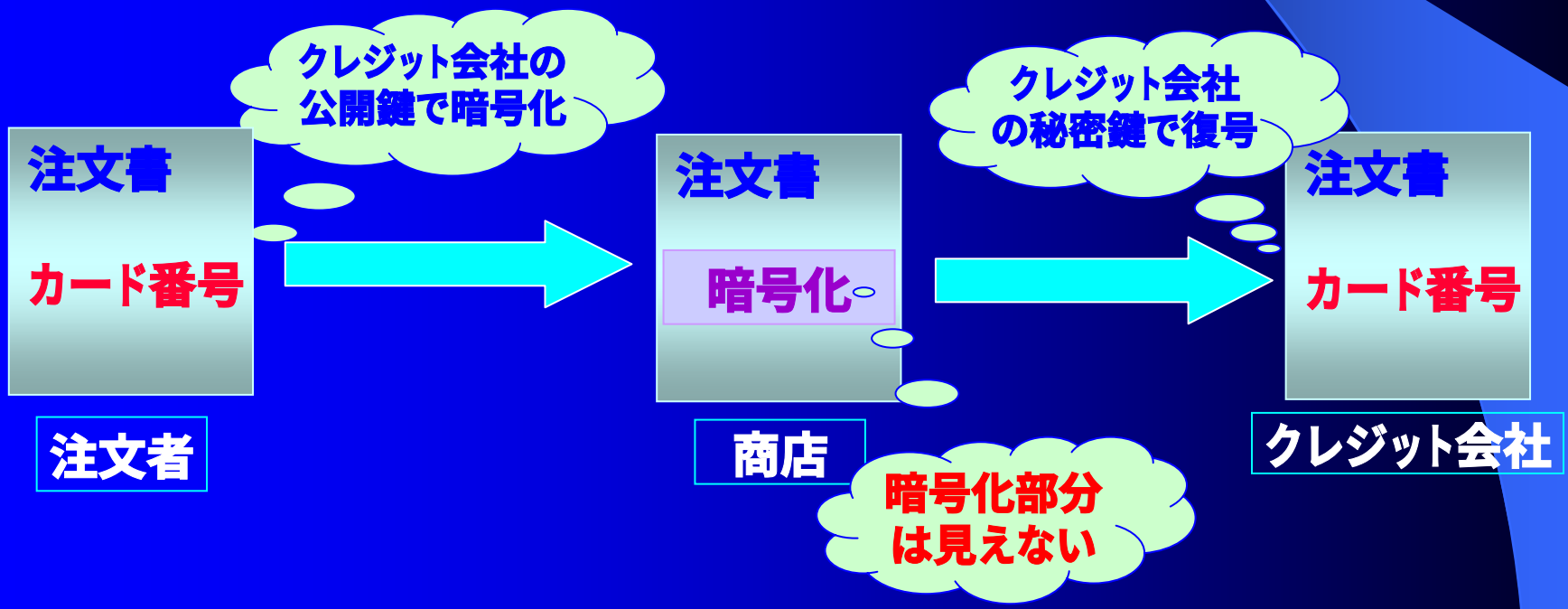


XML Encryption

暗号･復号化の情報をXMLで表現する
W3Cで検討。2002-03-04 勧告候補。

/2001/04/xmlenc#

･コンテンツの一部、または全部を暗号化する
･中継者に対する一部データの秘匿に有効である



XML Encryption構文例

```
<Order>


  <Creditcard>
    <EncryptedData Id="ED" xmlns="http://www.w3.org/2001/04/xmlenc#">
      <EncryptionMethod Algorithm="#tripledes-cbc">
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <EncryptedKey>
          <EncryptionMethod Algorithm="#rsa1_5">
          <ds:KeyInfo>
            <KeyName>my-rsa-key</KeyName>
          </ds:KeyInfo>
          <ChipherData>5+GpVuQNTAT3uY8pPed</ChipherData>
          <ReferenceList>
            <DataReference URI="#ED"/>
          </ReferenceList>
        </EncryptedKey>
      </KeyInfo>
      <ChipherData>
        <ChipherValue>41a2BdeaXEdda468Xaegde</ChipherValue>
      </ChipherData>
    </EncryptedData>
  <Creditcard>

<Order>
```

EncryptionMethod：
暗号ｱﾙｺﾞﾘｽﾞﾑ

EncryptedKey:
・コンテンツの暗号に使用した鍵（共通鍵）
・前記鍵を更に暗号化（公開鍵）

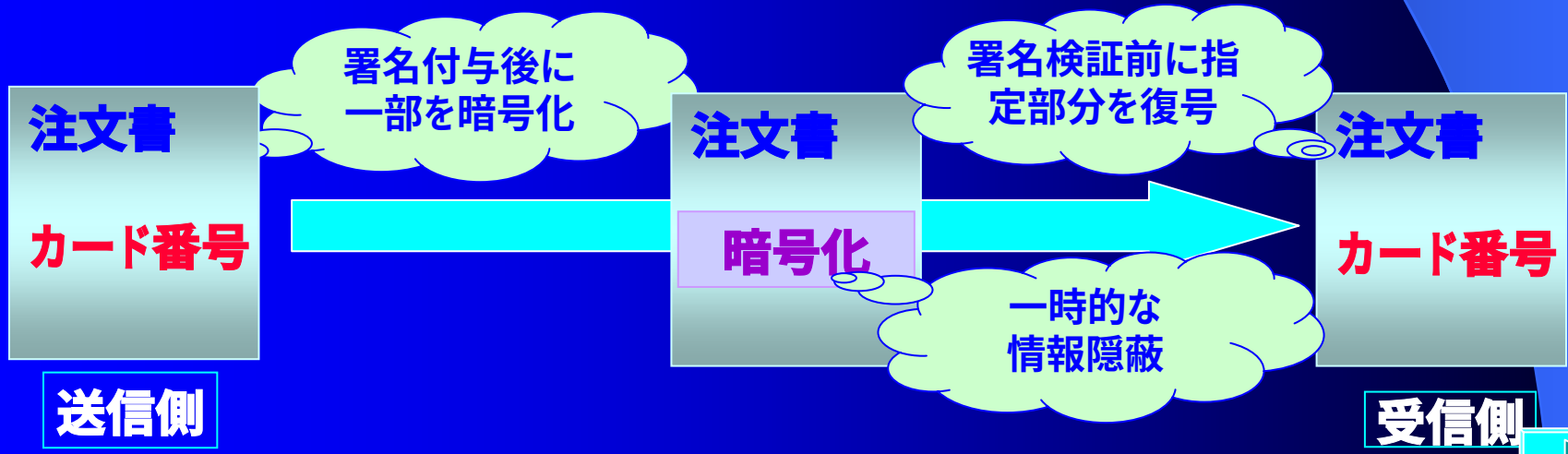
CipherValue：
暗号化されたコンテンツ

Decryption Transform for XML Signature

署名後に暗号化する部分の指定と処理手順を規定する
W3Cで検討。2002-03-04 勧告候補。

/2001/04/decrypt#

- **XML Signature内に復号対象を明示する**
- **受信側は平文で署名検証が可能**
- **通信経路での一時的な情報隠蔽に有効**
- **XML Signature/XML Encryptionの構文を使用**



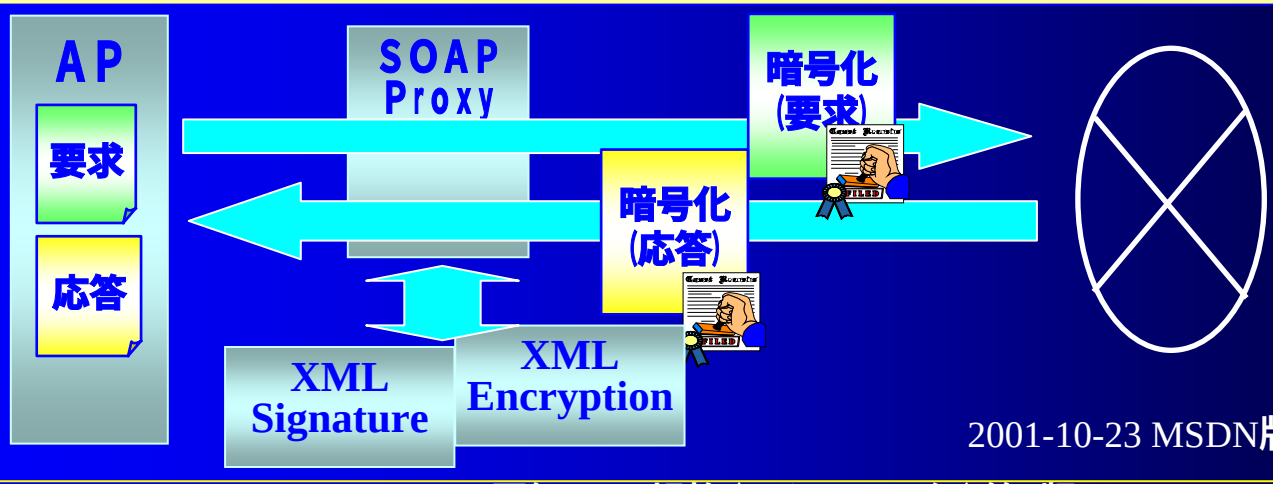
Web Services Security Language (WS-Security)

Update

SOAPに対するメッセージ認証・電子署名・暗号を規定
業界団体（W3Cに提出予定）。2002-04-05 草案

/2002/04/secext/

- Webサービスを安全に運用するためのセキュリティ技術の総称
- SOAPメッセージに対する機能拡張のタグセット
  - メッセージ認証：ログイン・パスワード情報、証明書
  - 完全性：電子署名（XML Signature）を使用する
  - 秘匿性：暗号化（XML Encryption）を使用する
- SOAP Security Extension：Digital Signatureから拡張



2001-10-23 MSDN版仕様書にて調査

WS-Security構文例

Update

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
            xmlns:wssec="http://schemas.xmlsoap.org/ws/2001/10/security">
  <S:Header>
    <wssec:Security>

      <wssec:BincarySecurityToken Id="myToken"
       ValutType="wssec:X590v3" EncodingType="wssec:Base64Binary">
         (X.509v3証明書)
       </ wssec:BincarySecurityToken>

      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:Reference>
          <ds:Transforms>
            <ds:Transform
       Algorithm="http://schemas.xmlsoap.org/2001/10/security#RouingSignatureTransform"/>
          </ds:Transforms>
        </ds:Reference>
      </ds:Signature>
    </wssec:Security>
  </S:Header>

  <S:Body>
    <enc:EncryptedData xmlns:enc=http://www.w3.org/2001/04/xmlenc#>
       (暗号化されたデータ)
    </enc: EncryptedData>
  </S:Body>
</S:Envelope>
```

SecurityToken：
メッセージ認証情報

電子署名
(XML Signature)

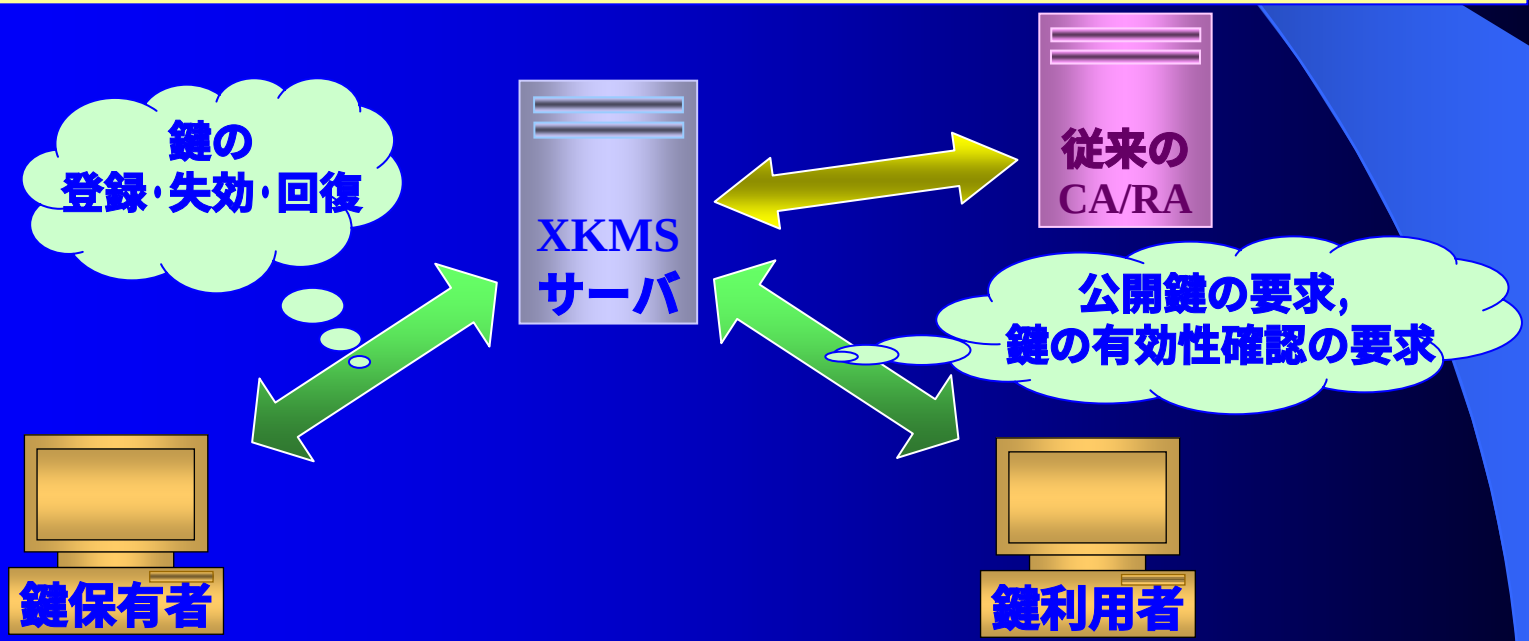
EnctyptedData：
暗号化データ
(XML Encryption)

XKMS 2.0 (XML Key Management Specification)

公開鍵を登録、配布するためのメッセージとプロトコル
W3Cで検討。2002-03-18 作業案。

/2002/03/xkms

- 公開鍵の登録 (X-KRSS) と公開鍵の問合せ (X-KISS) から構成される
- 鍵利用者の処理を軽減する (CRLの検証等)
- サーバの構成は適用範囲外となる



XKMSのメッセージ (X-KISS)

＜Locate＞

- **サービスから公開鍵関連情報 (鍵値、証明書) を取得する**
- **例えば、暗号化の際に受信者の名前から受信者の公開鍵を取得する**
- **公開鍵関連情報はXML Signatureの<KeyInfo>を使用する**

```
<Locate xmlns="http://www.xkms.org/schema/xkms-2001-01-20">
  <Query>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <KeyName>shimoda@o-camera.com</KeyName>
    </KeyInfo>
  </Query>

  <Respond>
    <string>KeyName</string>
    <string>KeyValue</string>
  </Respond>
</Locate>
```

Query：
公開鍵関連情報

Respond：
問合せ項目

XKMSのメッセージ (X-KISS)

＜Validate＞

・サービスに対して、公開鍵関連情報の有効性を問合せる

・例えば、署名検証の際に送信者が添付した公開鍵の有効性を検証する

```
<Validate xmlns="http://www.xkms.org/schema/xkms-2001-01-20">
  <Query>
    <Status>Indeterminate</Status>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <KeyValue>
        <RSAKeyValue>
          <Modulus>y0eZi+pL544O0anaCbHOF==</Modulus>
          <Exponent>AQAB</Exponent>
        </RSAKeyValue>
      </KeyValue>
    </KeyInfo>
  </Query>

  <Respond>
    <string>KeyName</string>
    <string>KeyValue</string>
  </Respond>
</Validate>
```

Query：
公開鍵関連情報

Respond：
問合せ項目

XKMSのメッセージ (X-KRSS)

＜Register＞

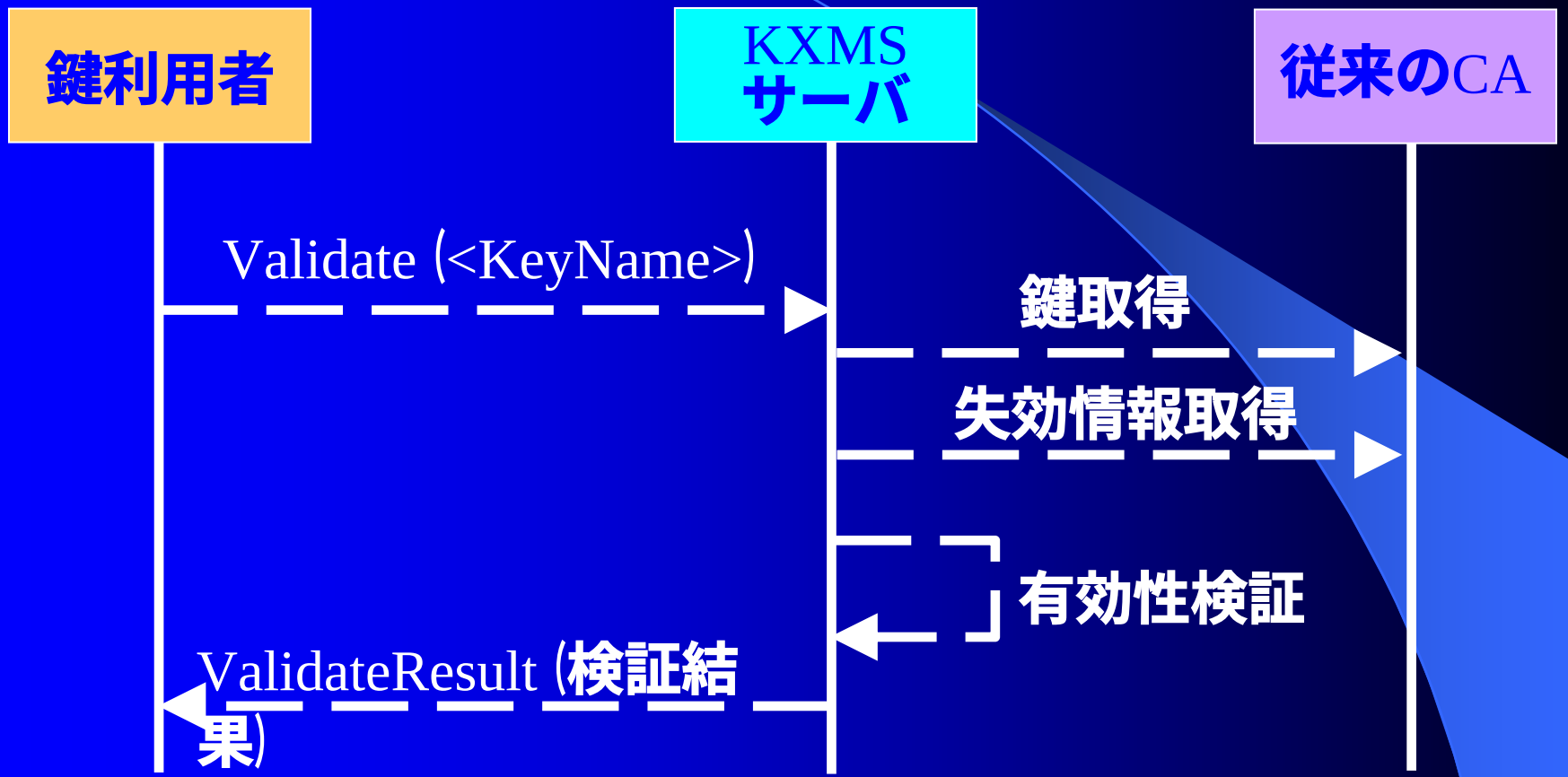
・サービスに対して、公開鍵関連情報の登録・失効・回復を行う
・クライアントサイド生成鍵の登録とサーバサイド生成鍵の取得が定義される

```
<Register xmlns="http://www.xkms.org/schema/xkms-2001-01-20">
  <Prototype Id="Ref1">
    <Status>Valid</Status>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <KeyValue>
        <RSAKeyValue>              </RSAKeyValue>
      </KeyValue>
    </KeyInfo>
    <PassPhrase>8czbkqkp9RSe1AxdDz8vu+eAlSE=</PassPhrase>
  </Prototype>
  <AuthInfo>
    <AuthUserInfo>
      <ProofOfPossession>      </ProofOfPossession>
      <KeyBindingAuth>       </KeyBindingAuth>
    </AuthUserInfo>
  </AuthInfo>
  <Respond>
    <string>KeyName</string>
    <string>X509Data</string>
  </Respond>
</Register>
```

Prototype：
登録する公開鍵関連情報

AuthInfo：
鍵所有者情報

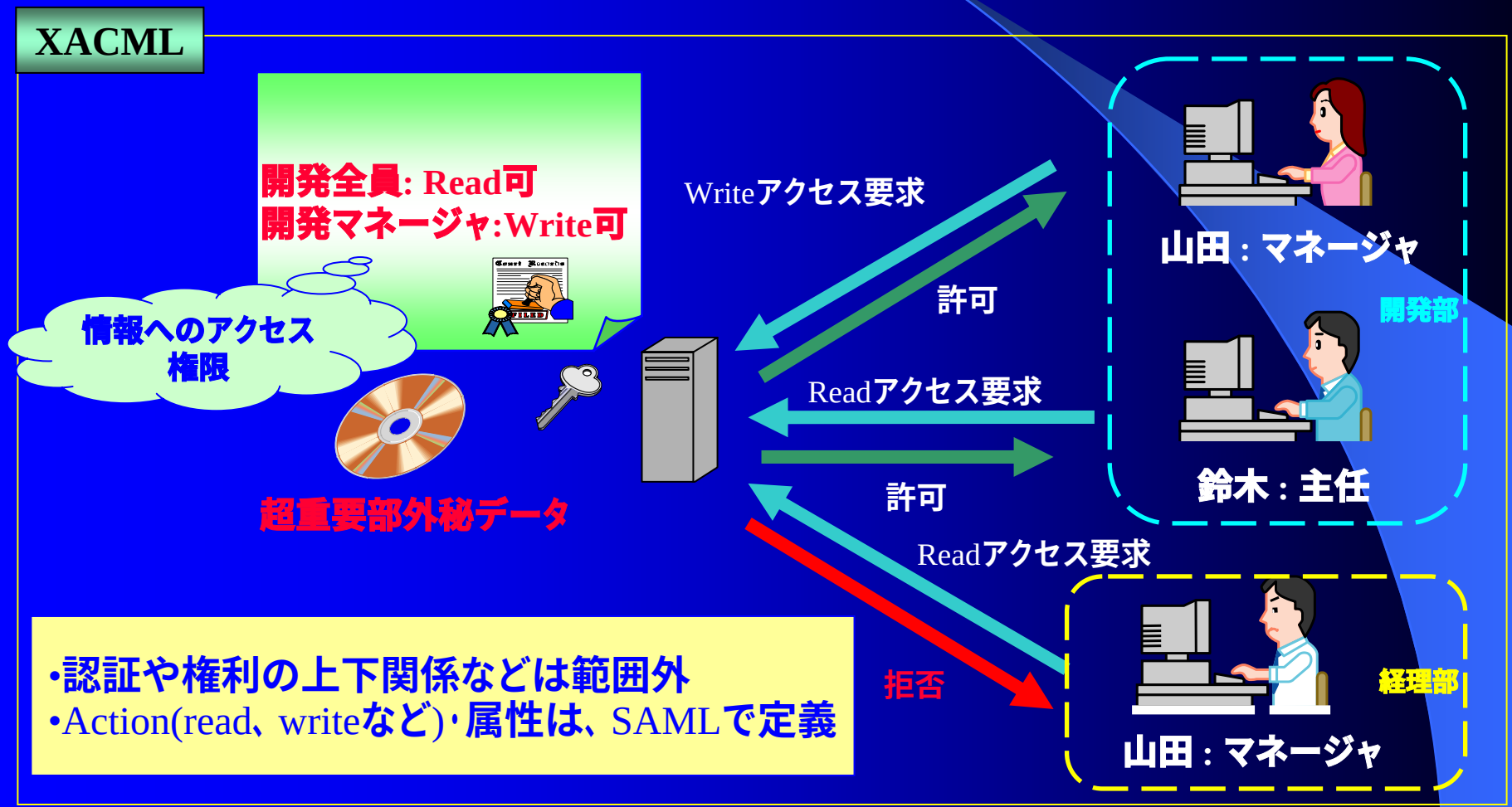
XKMSのプロトコル



Validate時のプロトコル概要
(XKMSサーバ＋従来CAの構成)

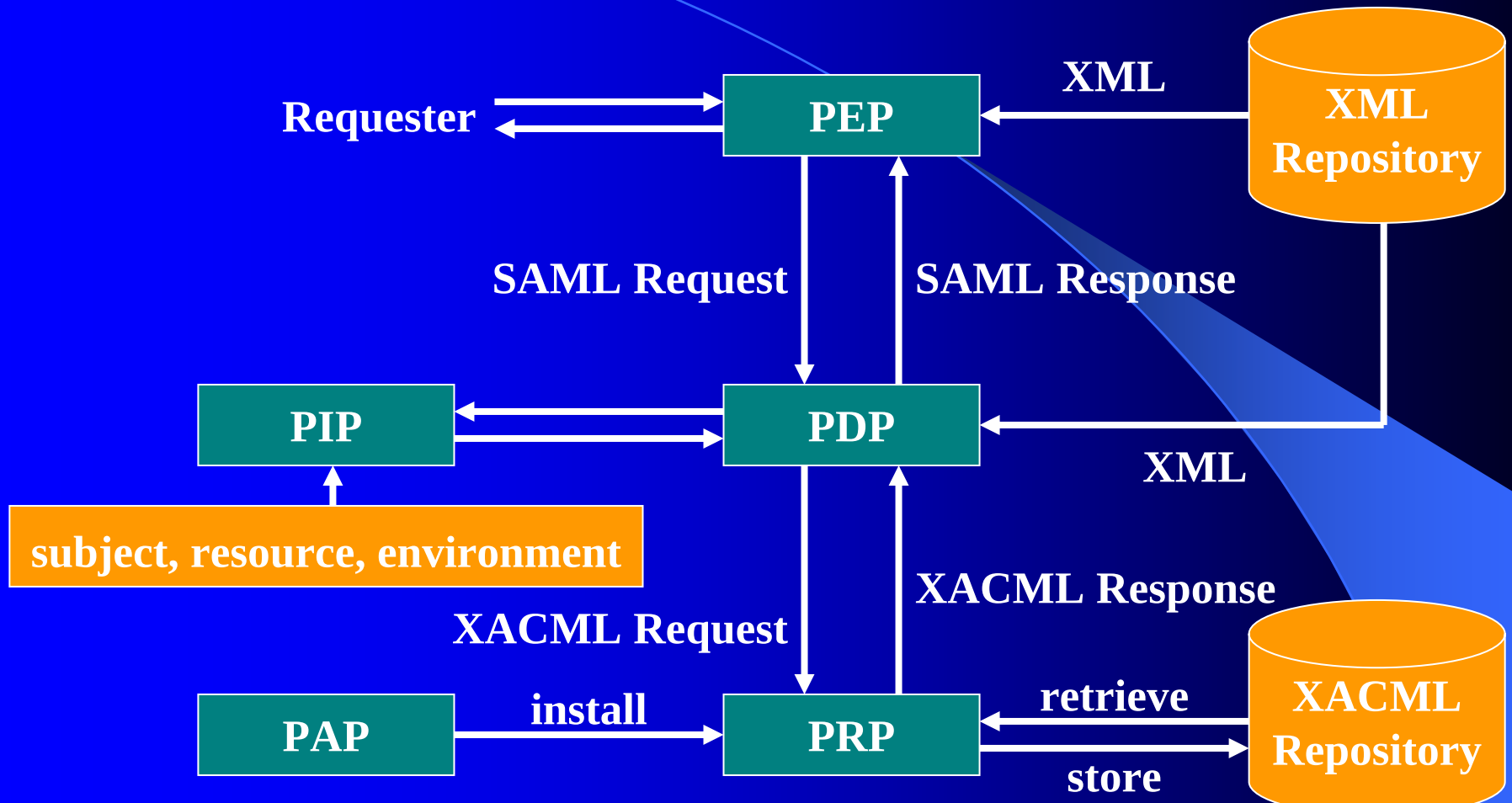
XACML
(eXtensible Access Control Markup Language)

情報へのアクセス･ポリシーを表現するための言語
OASISで検討中。2002-07-01 ドラフト完了予定



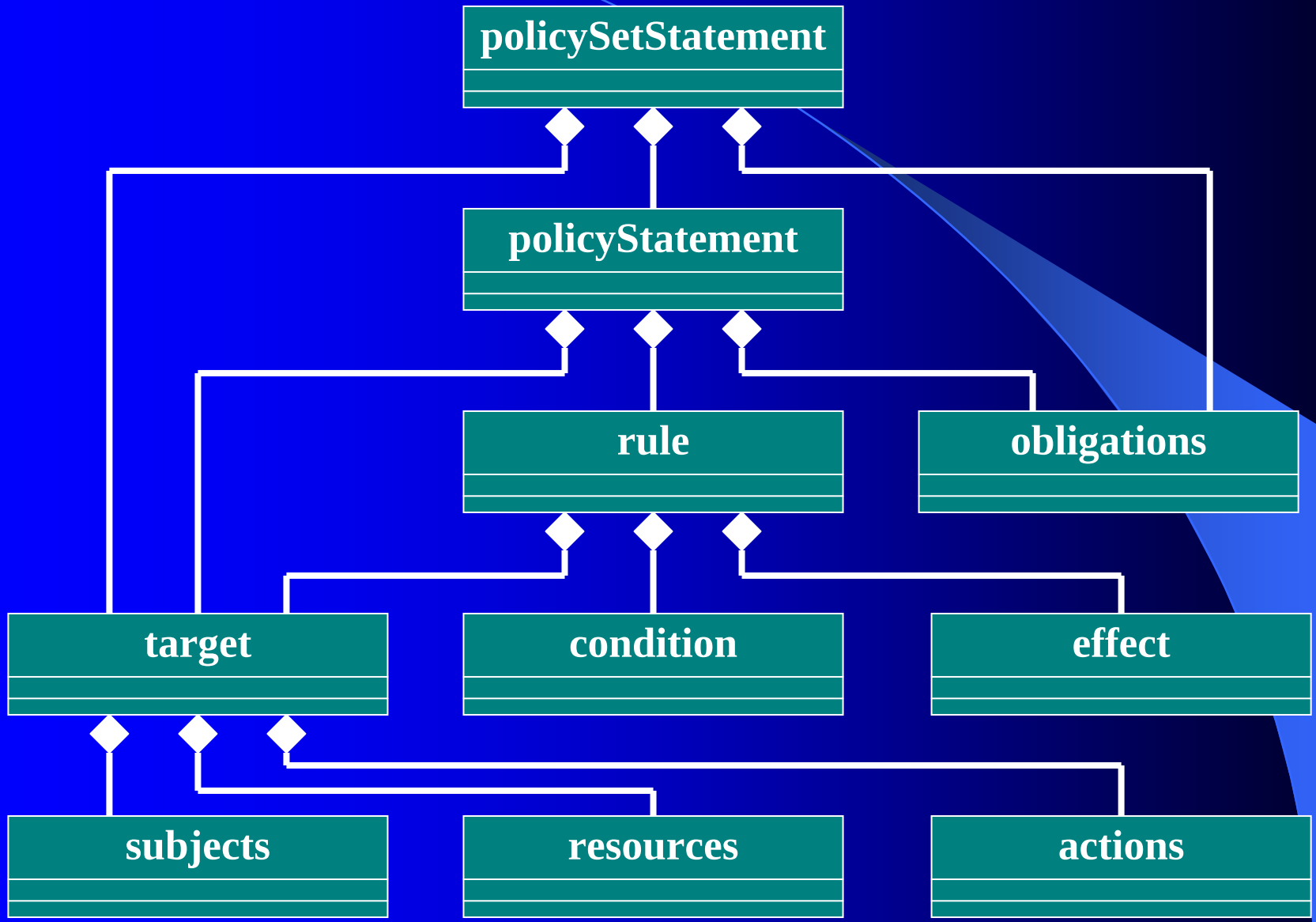
- 認証や権利の上下関係などは範囲外
- Action(read、writeなど)･属性は、SAMLで定義

XACMLのデータフローモデル



PEP: Policy enforcement point
PDP: Policy decision point
PRP: Policy retrieval point
PAP: Policy administration point
PIP: Policy information point

XACMLの構造


policySetStatement
policyStatement
rule
obligations
target
condition
effect
subjects
resources
actions

XACML構文例

```
<rule ruleId="//cons.com/rule/id/1" effect="Allow">
    <description>Sample policy</description>
    <target>
      <subjects>
        <saml:Attribute AttributeName="RFC822Name">
          <saml:AttributeValue>* </saml:AttributeValue>
        </saml:Attribute>
      </subjects>
      <resources>
        <saml:Attribute AttributeName="documentURI">
          <saml:AttributeValue>//cons.com/record.*</saml:AttributeValue>
        </saml:Attribute>
      </resouces>
      <actions>
        <saml:Action>read</saml:Action>
      </actions>
    </target>
    <condition>
      <not>
        <graterOrEqual>
          <minus>
            <saml:AttributeDesignator AttributeName="today'sDate" />
            <saml:AttributeDesignator AttributeName="employDoB" />
          </minus>
          <saml:Attribute AttributeName="ageOfConsent">
            <saml:AttributeValue>20-0-0</saml:AttributeValue>
          </saml:Attribute>
        </gratorOrEqual>
      </not>
    </condition>
</rule>
```

subjects
対象となる要求主体

resources
対象となるオブジェクト

actions
許可される動作

condition
許可される条件

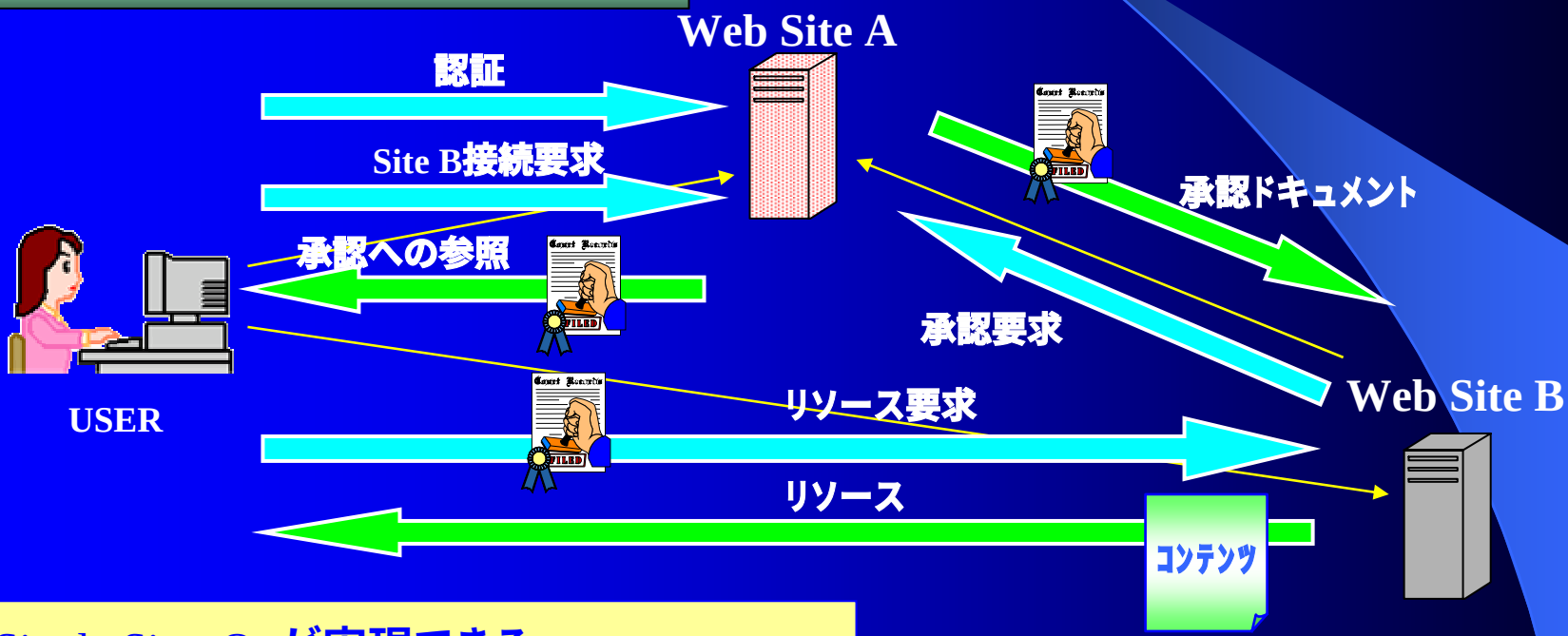
この例の場合、
「要求者(社員)の、
現在の年齢が
20歳未満」

SAML

Security Assertion Markup Language

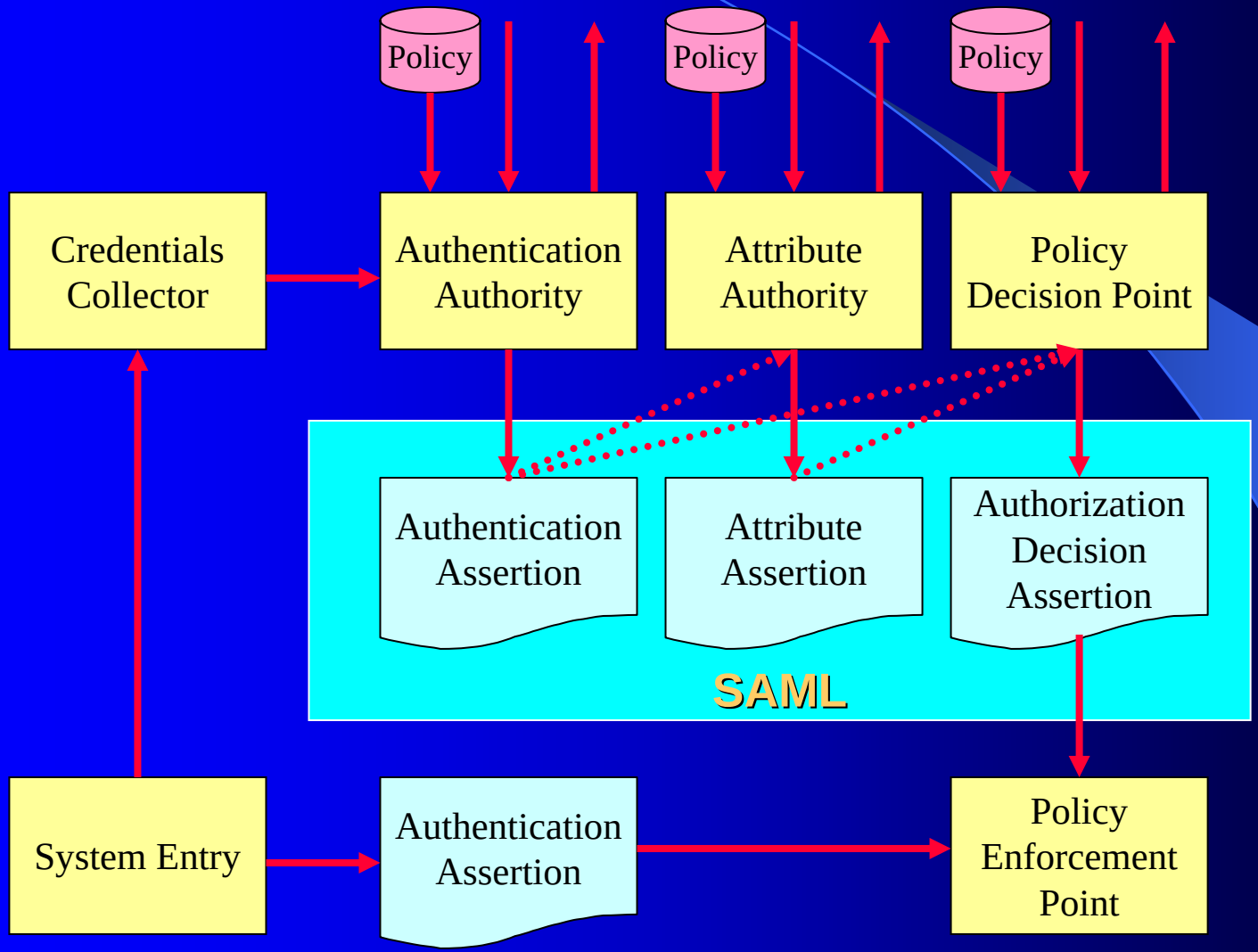
認証/承認/属性情報を交換するための言語。
OASISで検討中。2002-07-01 ドラフト完了予定

SAML：Single Sign-On Pull Model



- Single Sign-Onが実現できる
- アサーションの表現方法とプロトコルの定義
- 広範な既存認証機構との連携
- 三つのモデル(Pull / Push / 3rd Party Security)

SAMLのモデル


Policy
Policy
Policy
Credentials Collector
Authentication Authority
Attribute Authority
Policy Decision Point
Authentication Assertion
Attribute Assertion
Authorization Decision Assertion
SAML
System Entry
Authentication Assertion
Policy Enforcement Point

SAML構文例

- 認証の要求メッセージ

```
<samlp:Request MajorVersion="1" MinorVersion="0“
      RequestID=“8xtyzzKqPMLcFswefRIJAL">
      <samlp:RespondWith>AuthenticationStatement</samlp:RespondWith>
      <samlp:AuthenticationQuery>
        <saml:Subject>
          <saml:NameIdentifier Name=“JFB"/>
          <saml:SubjectConfirmation>
            <saml:ConfirmationMethod>
              http://www.oasis-open.org/…./draft-sstc-core-25/password
            </saml:ConfirmationMethod>
            <saml:SubjectConfirmationData>
              uTKaRyQmytsz=
            </saml:SubjectConfirmationData>
          </saml:SubjectConfirmation>
        </saml:Subject>
      </samlp:AuthenticationQuery>
</samlp:Request>
```

NameIdentifier
名前による識別子

ConfirmationMethod
パスワードによる確認

SAML構文例

- 認証の応答メッセージ（認証アサーション付き）

```
<samlp:Response InResponseTo="8xtyzzKqPMLcFswefRIJAL"
    MajorVersion="1" MinorVersion="0"
    ResponseID="xmlconsortium2002061002090011">
    <samlp:Status>
      <samlp:StatusCode Value="samlp:Success"/>
    </samlp:Status>
    <saml:Assertion AssertionID="qJcZsDTnJBPPe/4tIJKuZ/OLMtE= "
      IssueInstant="2002-06-10T11:22:33.456" Issuer="JUSTAir"
      MajorVersion="1" MinorVersion="0">
     <saml:Conditions
        NotBefore=" 2002-06-10T11:22:33.466"
        NotOnOrAfter=" 2002-06-10T15:22:33.466 "/>
     <saml:AuthenticationStatement
        AuthenticationInstant=" 2002-06-10T11:22:33.106"
        AuthenticationMethod="http://www.oasis-open.org/…/password">
       <saml:Subject>
        <saml:NameIdentifier Name="JFB"
    SecurityDomain="just:Reservation"/>
        <saml:SubjectConfirmation>
          <saml:ConfirmationMethod>
            http://www.oasis-open.org/…/password
          </saml:ConfirmationMethod>
        </saml:SubjectConfirmation>
       </saml:Subject>
     </saml:AuthenticationStatement>
    </saml:Assertion>
</samlp:Response>
```

Assertion
認証の証明

NameIdentifier
ユーザ識別子

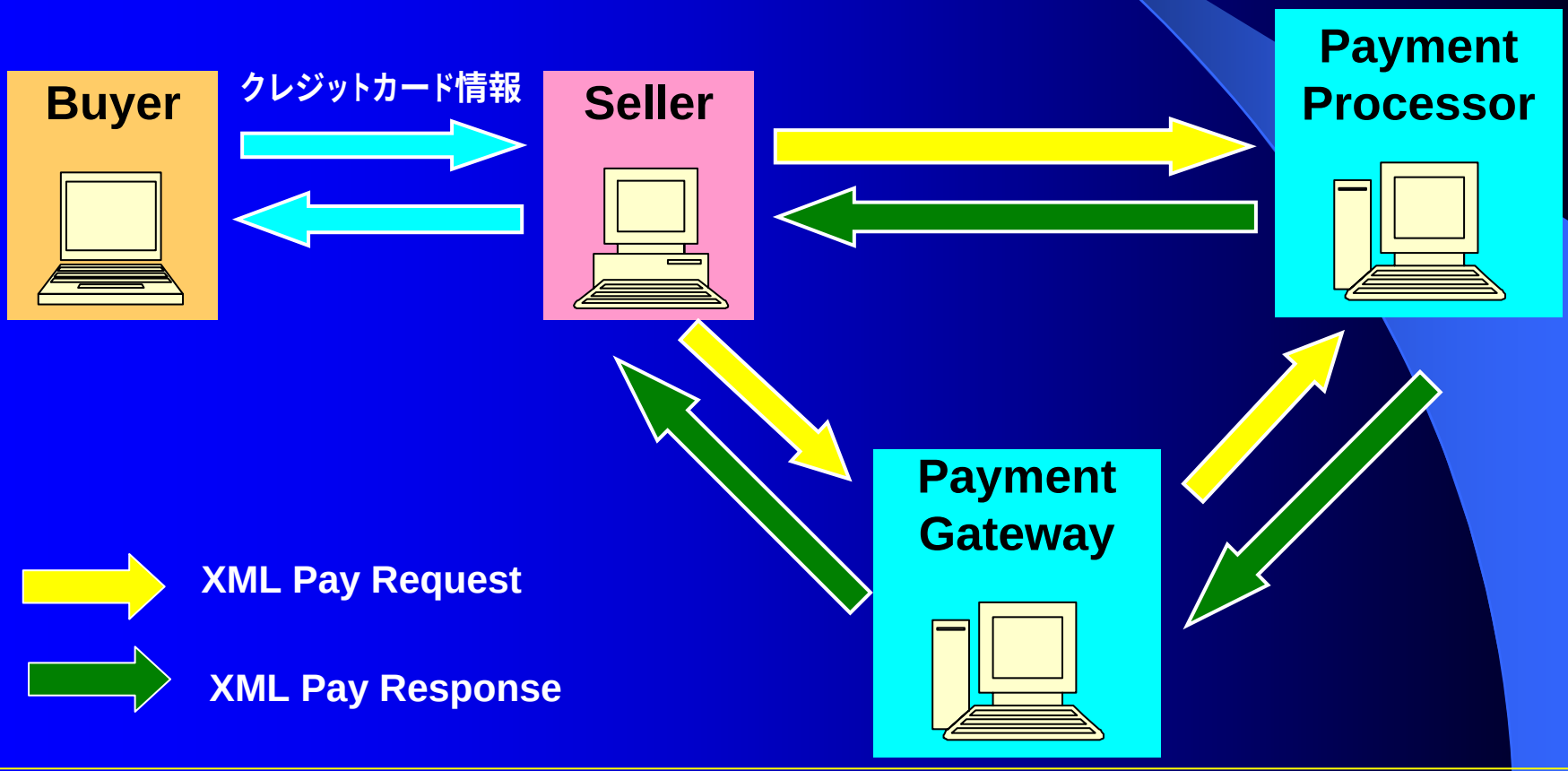
XML Pay

ネット取引の決済に関する言語

XMLPay：core	2000-11-20 Release
XMLPay：Registaration	検討中
XMLPay：Report	検討中

XML Pay

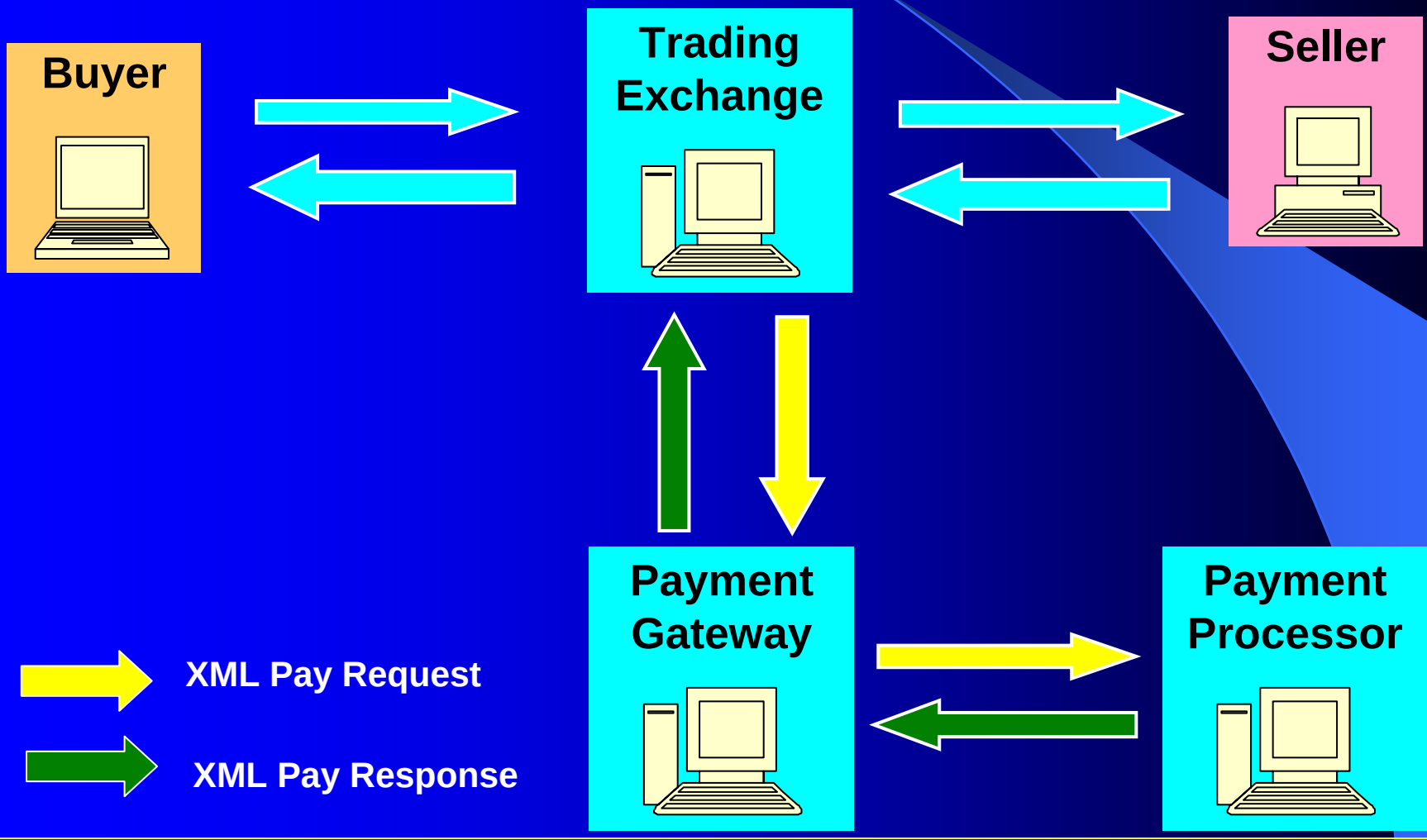
Business-to-Consumer Model



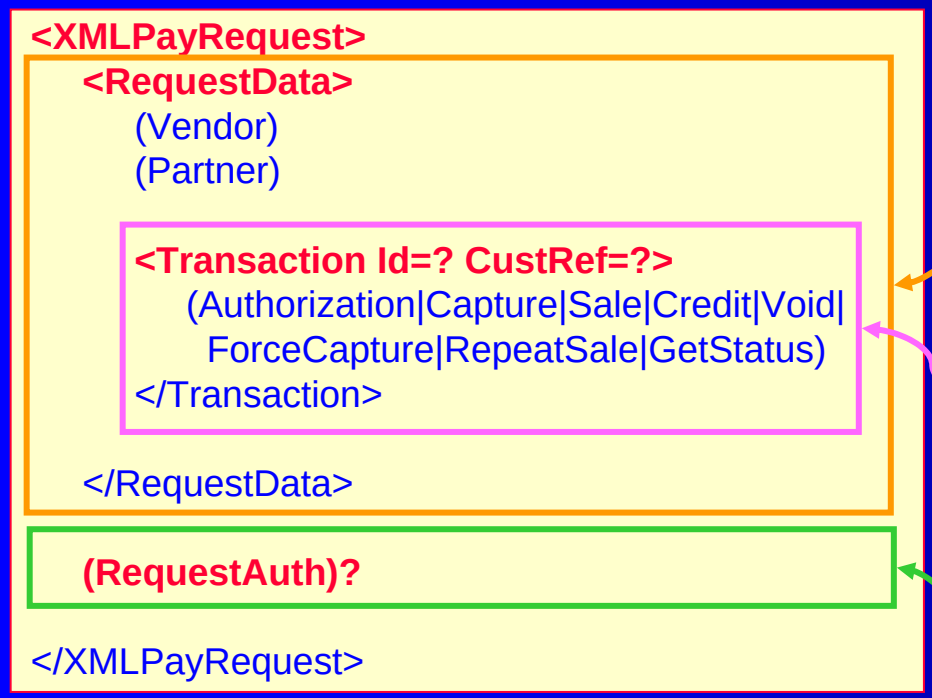
XML Pay

XML Pay

Business-to-Business Model



XML PayRequest(要求)構文例



取引者の内容

取引者の情報

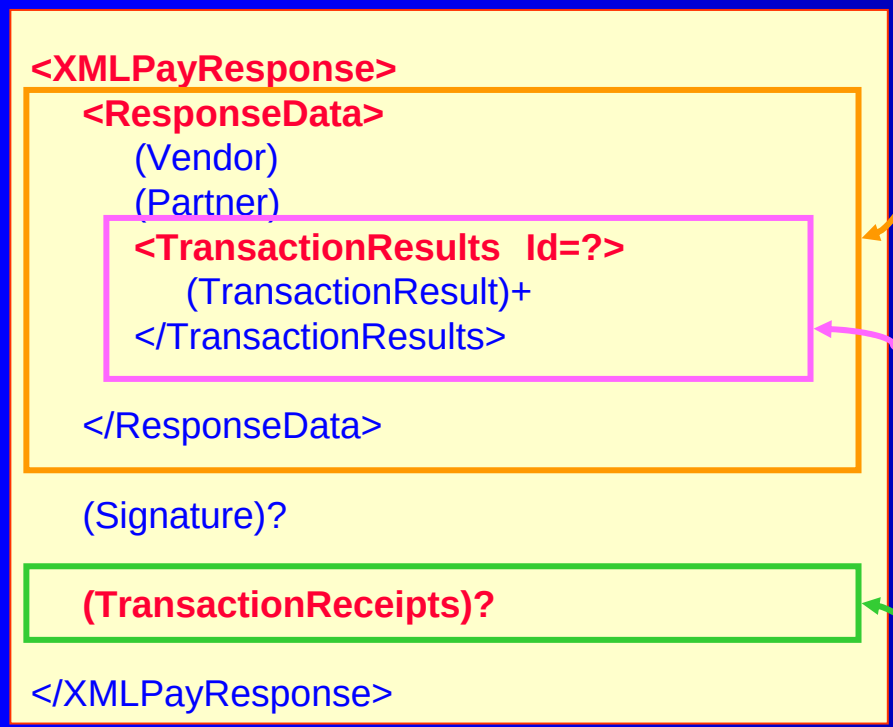
RequestData
取引の情報

Transaction
支払い取引リスト

Authorization：資金の有効性確認
Capture：　認可取引によって保証された資金を商店のアカウントへ転送
Sale：　販売の有効性確認
Credit：　SaleかCaptureを取り消す
Void：　未決のsale、capture、creditを取り消す
ForceCapture：バンド外認可(例えば音声認可)を通して留保された資金をcaptureする
RepeatSale：　販売取引を繰り返す
GetStatus：　取引のステータスを尋ねる

RequestAuth
提示ﾊﾟｰﾃｨの認証

XML PayResponse(返答)構文例



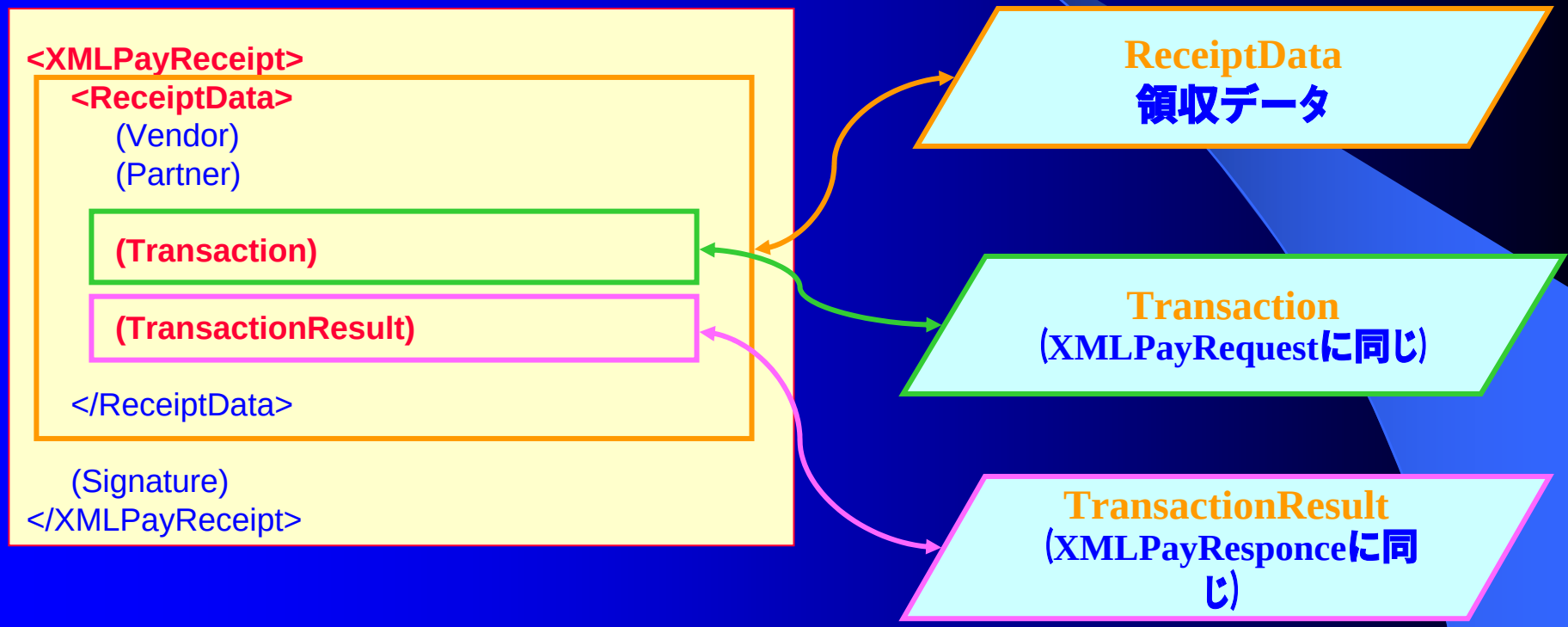
RequestData
結果の情報

TransactionResult
取引の結果

Result：　取引の結果を示す値
AVSResult：AVS（アドレス立証サービス）チェックの結果
CVResult：　CV（Credit Void）チェックの結果
Message：　結果説明
PNRef：　取引に割り当てられた確認者
AuthCode：取引用の認可コード
HostCode：支払いプロセッサによって返される結果コード
HostURL：　取引に言及する際に使用するURL
OrigResult：GetStatus要求に対する結果
Status：　現在のステータス
ReceiptURL：領収書に言及する際に使用するURL
ExtData：　拡張データ

TransactionReceipts
領収書のｵﾌﾟｼｮﾝ

XML PayReceipt(領収)構文例



付録

- Acronyms

ASN.1
Abstract Syntax Notation 1

CA
Certification Authority

CEP
Certificate Enrollment Protocol

CMC
Certificate Management protocol using CMS

CMP
Certificate Management Protocol

CMS
Cryptographic Message Syntax

CRL
Certificate Revocation List

CRMF
Certificate Request Message Format

CRS
Certificate Request Syntax

DOM
Document Object Model

DSA
Digital Signature Algorithm

HTTP
Hyper Text Transfer Protocol

LDAP
Lightweight Directory Access Protocol

MAC
Message Authentication Code

OSCP
Online Certificate Status Protocol

PGP
Pretty Good Privacy

PKCS
Public Key Cryptography System

PKI
Public Key Infrastructure

付録（続き）

- Acronyms (cont.)

RSA
: Rivest, Shamir, Adleman

SDK
: Software Development Kit

SHA
: Secure Hash Algorithm

SOAP
: Simple Object Access Protocol

SPKI
: Standard Public Key Infrastructure

SSL
: Secure Socket Layer

TLS
: Transport Level Security

WSDL
: Web Service Description Language

WWW
: World Wide Web

URI
: Uniform Resource Identifier

URL
: Uniform Resource Locator

URN
: Uniform Resource Name

X-KISS
: XML Key Information Service Specification

X-KRSS
: XML Key Registration Management Specification

X509
: ISO X.509 recommendation

XKMS
: XML Key Management Specification

XML
: Extensible Markup Language

URI

- XML Signature:
  - http://www.w3.org/TR/xmldsig-core/
- XPath Filter 2.0：
  - http://www.w3.org/TR/xmldsig-filter2/
- Exclusive XML Canonicalization
  - http://www.w3.org/TR/xml-exc-c14n/
- XML Encryption:
  - http://www.w3.org/TR/xmlenc-core/
- Decryption Transform:
  - http://www.w3.org/TR/xmlenc-decrypt/
- WS-Security
  - http://www.microsoft.com/japan/msdn/webservices/dnsrvspec/wssecurspecindex.asp

URI (続き)

- XKMS 2.0
  - http://www.w3.org/TR/xkms/
- XACML
  - http://www.xacml.org
- SAML
  - http://www.oasis-open.org/committees/security/
- XML Pay
  - http://www.verisign.com/developer/xml/xmlpay.html