3）署名検証クラス

・ XmlVerifier

XML 電子署名を検証するクラス。

4）例外クラス

・ CertificateChainException

証明書信頼チェーン検証に失敗したときにスローされる例外。

・ SelectCertificateException

署名用証明書選択時に証明書が無かった時、または２つ以上あった時にスローする例外

・ SelectSigningKeyCancelException

署名用証明書選択時にキャンセルが押されたときにスローされる例外

・ ToSignElementXPathException

署名対象 XML エレメントを指定する Xpath 式が不正であるときスローされる例外

・ VerificationException

署名検証に失敗したときにスローされる例外

・ X509CertificateNotFoundException

Signature タグ内に公開鍵証明書が記述されていないときにスローされる例外

5）列挙型

・ CapicomSelectType

CAPICOM の証明書選択方法。

・ ChainCheckType

証明書信頼チェーン検証時の失効状態検証タイプ。

・ ChainTrustStatusType

証明書信頼チェーンの検証結果。

4. 署名・検証 XML WEB サービス

4.1 サービス概要

署名モジュールを基盤として、XML 電子署名機能、XML 電子署名検証機能を提供するサービスを開発した。

これは、今後の拡張性、他システムとの融合性を考慮し、SOAP、WSDL に基づいている XML WEB サービスとして実装した。

XmlSignatureService という WEB サービスに XmlSigner という XML 電子署名機能を提供するクラスと、XmlVerifier という XML 電子署名検証機能を提供するクラスを用意した。この WEB サービスを用いることにより、個々の医療情報システムにおいて柔軟且つ容易に署名・検証機能を組み込むことが可能となる。

4.2 サービス構成

XmlSignatureService のクラス構成は以下の通りである（詳細については添付資料１参照）。

⑤ 署名生成用クラス

・ XmlSigner

Enveloped 型、Enveloping 型署名を生成する WEB メソッドを提供するクラス。

⑥ 署名検証用クラス

・ XmlVerifier

Xml 電子署名を検証する WEB メソッドを提供するクラス。

5. 実証システム

開発したクラスライブラリ、XML WEB サービスの実運用性を評価するため、実証システムを構築した。この実証用システムは、現在、神戸大学医学部附属病院電子カルテシステムで開発が進められている HL7v3 対応対応ライブラリを用いて構築されたシステムである。

5.1 システム概要

このシステムの概要は以下の通りである。まず、クライアントアプリケーションにおいて、用意されたHL7v3メッセージに対し、署名クラスライブラリを用いて署名を施す。作成された署名付メッセージは実証サーバシステムに送信する。サーバシステムでは、受信した署名付HL7v3メッセージの署名を、署名・検証XML WEBサービスを用いて検証する。サーバシステムの受信結果は、HL7v3のAckメッセージとし、署名・検証XML WEBサービスを用いて署名された後、クライアントに送信される。クライアントでは、Ackメッセージ受信後、付与された署名を検証し結果を表示する。

5.2 システム構成

この実証用システムは、複数のXML WEBサービスを組み合わせて構築されている。そのシステム構成は、図5.2 実証システムシーケンスの通りである。以下に、システムの各構成要素について説明する。

1）MessageHandlingServiceClient
このシステムにおけるクライアントアプリケーション。XML 電子署名、検証機能を持っている。HL7v3 メッセージに署名を施し、サーバシステムに送信する。サーバシステムからは、署名付Ack メッセージを受信し、その署名を検証し結果を表示する。

2）MessageHandlingService
クライアントから署名付HL7v3 メッセージを受信し、各XML WEBサービスに処理を振り分ける、サーバシステムのハブとしての役割を持つサービス。次の４つの処理をそれぞれ適切なXML WEBサービスに振り分ける。
① 受信したメッセージの保存
② 受信したメッセージの署名検証
③ HL7メッセージの処理
④ Ackメッセージへの署名
最後に署名付Ackメッセージをクライアントアプリケーションに送信する。

3）TrackingService
XML メッセージを受け取り、サーバディレクトリにXML ファイルとして保存するサービス。

4）XmlSignatureService
XML 電子署名メッセージを受け取り、その署名を検証するサービス。また、XML メッセージを受信し、XML 電子署名を施す。

5）Hl7v3MessagingRouter
HL7v3 メッセージを受信し、メッセージのヘッダを解析し、適切なHL7v3 システムに処理を依頼するサービス。但し、この部分については現在開発中であるため、実装はまだない。実証システムでは、ダミーシステムとして、Pharmacyシステムを用意し、処理を依頼した。Pharmacyシステムは今回の実装では何も処理せず、保存するだけである。

6）PharmacySystem
ダミーシステム。
Hl7v3MessagingRouterからHL7v3メッセージを受信し、保存する。

7）IdentifierService
HL7v3メッセージのメッセージID発行要求を受付、ID を返信するサービス。ID 自体の発行は、

IdentifierIssuerService に依頼する。

8）IdentifierIssuerService
IdentifierService から ID 発行依頼を受付、ID を発行するサービス。

5.3 システムシーケンス概要

システムシーケンスの概要について、図 5.3 実証システムシーケンスの付番に沿って説明する。

① MessageServiceHandlingClient にて、HL7v3 対応メッセージに電子署名を付与し、MessageHandlingService に送信する。

② MessageHandlingService は受信したメッセージを、TrackingService の Tracker クラス、Save メソッドを用いて保存する。TrackingService は、保存ファイルの絶対パス、保存時間をログとして記録。
保存に失敗した場合、署名付 HL7v3Ack メッセージとして、保存に失敗した旨、MessageHandlingService から MessageServiceHandlingClient に通知される。

③ 受信したメッセージの署名を XmlSignatureService の XmlVerifier クラス、Verify メソッドを用いて検証する。検証に失敗した場合、署名付 HL7v3Ack メッセージとして、検証に失敗した旨、MessageHandlingService から MessageServiceHandlingClient に通知される。

④ 受信したメッセージを HL7V3MessageRouter へ送信。HL7V3MessageRouter の MessageRouter クラス、Send メソッドにより送信。HL7V3MessageRouter はこのメッセージを保存し、PharmacySystem に送信する。PharmacySystem の PharmacyOrderReceiver クラス、Send メソッドを用いて送信。また、HL7V3MessageRouter は、保存ファイルの絶対パス、保存時間をログとして記録。

⑤ PharmacySystem は受信したメッセージを保存。保存ファイルの絶対パス、保存時間はログとして記録される。

⑥ MessageHandlingService は MessageServiceHandlingClient に送信する Ack メッセージを作成する。その際、Ack メッセージに付与するメッセージ ID の発行を IdentifierService に依頼する。使用するメソッドは、IdentifierService の IssuerDelegate クラス、Issue メソッド。

⑦ IdentifierService はメッセージ ID 発行依頼を受付け、IdentifierIssuerService の Issue メソッドを用いて ID を発行。

⑧ IdentifierService は ID を MessageHandlingService に送信。

⑨ MessageHandlingService は作成した Ack メッセージに対し、XmlSignatureService の XmlSigner クラス、EnvelopingXmlSigner メソッドを用いて電子署名を付与。

⑩ MessageHandlingService は、署名付 HL7v3Ack メッセージを、MessageServiceHandlingClient に送信。MessageServiceHandlingClient はメッセージ受信後、付与された署名を検証し、検証結果を表示。

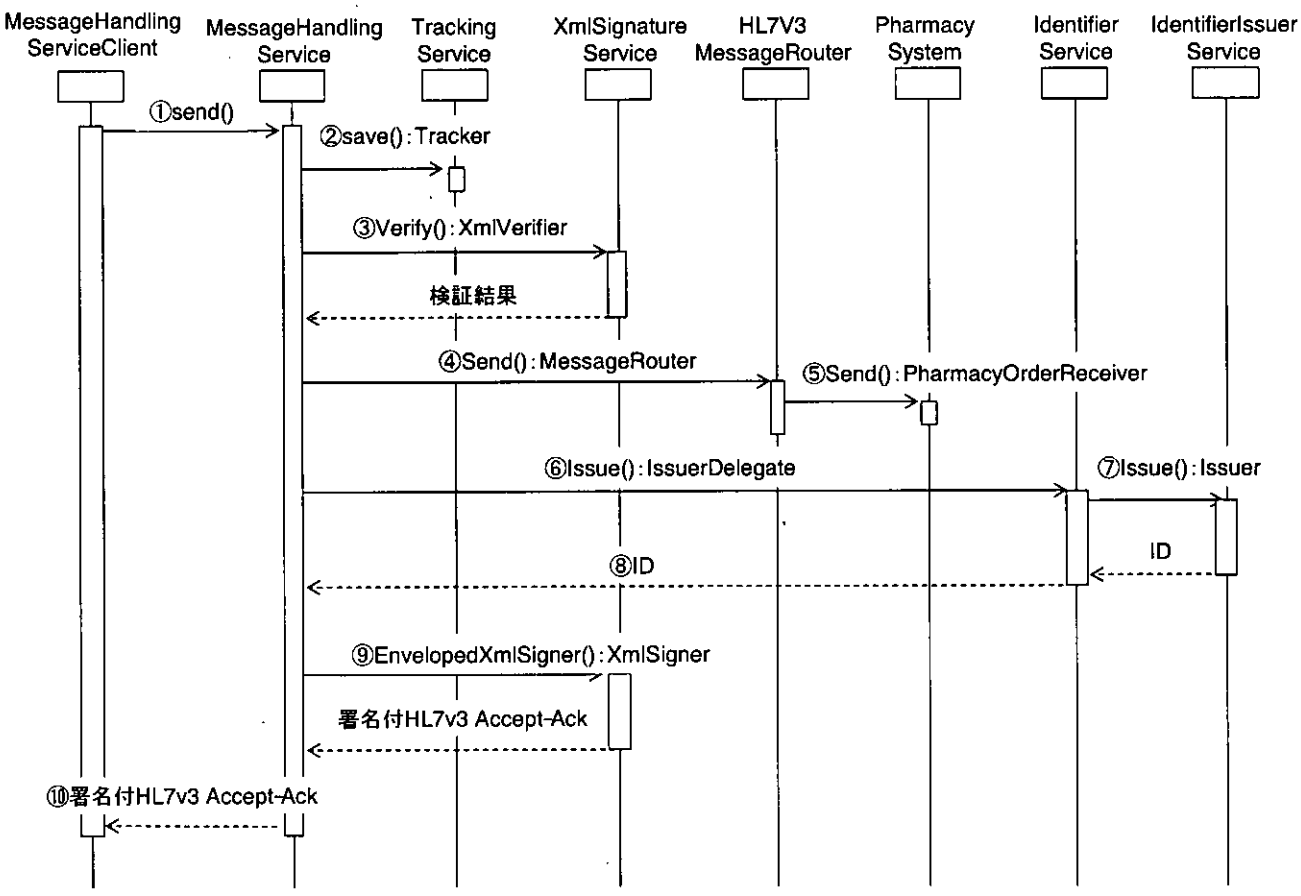

図 5.3 実証システムシーケンス

D．考察

平成 13 年度の研究成果では、保健医療分野において、処方箋等を電子的に交換する際のシナリオ、ユースケース、プロトコルが明確となり、電子署名の付加方法が同定された。本年度はその成果の実用性、安全性を検証するために、プロトタイプシステムを開発し、その実証実験を行うことを目的とした。しかしながら、実際に電子署名付き保健医療情報を作成し、それを交換しようとすると、それを利用する保健医療機関におけるセキュリティ環境整備が非常に大きな課題であることが判明した。これは、如何に厳密なセキュリティ技術を応用して、安全なシステムを開発したとしても、それを利用する、あるいは運用する環境のセキュリティがおざなりであれば、結局は交換される保健医療情報の信頼性が低下するからである。

今年度開発した XML 電子署名ライブラリは、W3C の仕様を実装したものとなっている。そのため、このライブラリは、認証のようなリアルタイムな場面で用いる署名、もしくは比較的短期間でその役割を終了するような署名に適してる。数年、数十年単位で用いられるような署名を行う場合には、別途、タイムスタンプや電子署名の長期保存といったことを考慮する必要がある。しかし、これらについては OASIS 等の標準化組織において仕様が策定中の部分もあり、実運用システムに組み込む上では十分に検討する必要がある。

今後の動向を見守りながら、ニーズに応じて対応を検討していきたい。

署名ライブラリは、enveloping 型と enveloped 型の XML 電子署名機能を実装した。これは医療における二つの署名タイプとうまく適合する。一つは処方箋タイプ、もう一つは診療録タイプである。

処方箋タイプとは、処方箋のように、処方全体に対して処方医師が署名するようなタイプであり、これは enveloping 型署名が適している。診療録タイプとは、診療録のようにある部分は主治医の署名、ある部分は放射線技師の署名のように一つの診療録に対して複数の署名が必要になるタイプである。これは enveloped 型署名が適している。

このように、XML 電子署名により、医療における多様な署名形態に対応することが可能であり、扱う医療情報の性質を考慮して最適な署名タイプを選択することが必要となる。

また、HL7v3 メッセージへの電子署名システムは、前述のように XML WEB サービスとして実装している。

このため、WSDL、SOAP を利用し、より柔軟且つ容易に、様々な形態のシステムに組み込むことが可能となっている。

但し、この電子署名システムの位置づけには若干注意が必要である。今回、電子署名システムを XML WEB サービスとすることにより、様々な医療情報システムに柔軟に署名、検証機能を組み込むことが可能となった。しかしこの署名・検証サービスは、あるシステムに対して署名、検証機能を組み入れるためのサービスとして捉える必要がある。即ち、DVCS (Data Validation and Certification Server Protocols) のような検証サービスとは明確に区別しなければならない。このサービスを署名、検証を代行する第三者として扱うわけではないということである。“C．研究結果 5.実証システム”

では、システムの内部サービス構成を紹介し、システムの柔軟性、拡張性を強調したが、それらのサービスはセキュリティの確保された領域の中で協調動作する1つのサービスとして構築されるべきものである。XML 電子署名に対応した DVCS に似た仕組みについては、現在、OASIS Digital Signature Services TC で仕様策定中である。このような動向の検討も今後の課題である。

E．結論

平成 14 年度の研究は、平成 13 年度に行った基礎的な事項の調査研究の成果の実用性、安全性を検証することが目的であった。

そのため、昨年度提案したユースケース、およびプロトコルに基づくプロトタイプシステムを開発し、その実証実験を行い、昨年度の提案が妥当であったことを証明した。

以上の研究結果を基に、来年度はより詳細な実用化研究とその検証を行うと共に、情報セキュリティポリシテンプレート、認証局実施規程テンプレートなど、これから各保健医療機関で必要となるリソースについて更に整備を行い、それらを公開できるようにする予定である。

平成 15 年度は、前年度開発したプロトタイプライブラリの実用化、及びそれを用いた署名・検証システムの構築を行った。“D．考察“に述べたような課題は残されているが、これらは時間をかけて取り組むべき性質の事項が多い。この研究の目途としては、ある程度限定したケースにおける、HL7v3 メッセージへの電子署名システムの実装及びその実運用性を確認することであった。

本研究により、医療情報という特殊な情報システムにおける XML 電子署名の有効性、また、今後主流となると予測される HL7v3 対応システムとの親和性とそのモデルについて明確に把握することができた。この成果を用いることで、神戸大学医学部附属病院電子カルテシステム、その他医療情報システム、様々なシステムに適した形で容易に電子署名機能を組み入れることが可能である。

F．健康危険情報

なし。

G．研究発表

1．石戸是亘、坂本憲広、ほか：HL7v3 に対応した XML 電子署名ライブラリの開発，第 23 回医療情報学連合大会論文集,23（Suppl.），516-519, 2003 年

2．西脇清行、石戸是亘、坂本憲広、ほか：XML 電子署名を用いたセキュアなインシデントレポートシステムの構築，第 23 回医療情報学連合大会論文集，23（Suppl.），607-9, 2003 年

H．知的財産権の出願・登録状況

1．特許取得

なし。

2．実用新案登録

なし。

3．その他

なし。

厚生労働科学研究費補助金（医療技術評価総合研究事業）
研究報告書

保健医療分野における電子署名の実用化に関する研究

添付資料1
開発ライブラリ、サービス仕様書

1．署名クラス

1．1 XmlSigner

1）クラス説明

XML 電子署名クラスの抽象クラス。

System.Object

XmlSigner

宣言

public abstract class XmlSigner

必要条件

名前空間: Nori.Hpki.XmlSignature

アセンブリ: XmlSignature (XmlSignature.dll 内)

参照

XmlSigner メンバ | Nori.Hpki.XmlSignature 名前空間

2）コンストラクタ

XmlSigner クラスの新しいインスタンスを初期化。

宣言

```
protected XmlSigner(
            SigningKeyStore signingKeyStore
);
```

パラメータ

signingKeyStore

署名用証明書を選択するための SigningKeyStore 抽象クラスのサブクラスインスタンス。

3）フィールド

①certificate

署名に使用する秘密鍵の公開鍵証明書。

宣言

protected X509Certificate certificate;

参照

XmlSigner クラス | Nori.Hpki.XmlSignature 名前空間

②containerName

署名に使用する秘密鍵を格納しているキーコンテナ名称。

宣言

protected string containerName;

③ cspName

署名に使用する秘密鍵を格納している CSP 名称。

宣言

protected string cspName;

4）メソッド

①GetElementToSign

Xml ドキュメントから XPath 式で指定された署名対象 XML エレメントを取得する。

宣言

```
protected XmlElement GetElementToSign(
    XmlDocument document,
    string xpath,
      XmlNamespaceManager namespaceManager
      );
```

パラメータ

document

署名対象 XML ドキュメント。

xpath

署名対象の Xml エレメントの XPath 式。

namespaceManager

XPath 式で使用する名前空間の解決のための XmlNamespaceManager クラスインスタンス。

戻り値

署名対象 XML エレメント。

例外

例外の種類 条件

ToSignElementXPathException 署名対象 XML エレメントを指定する Xpath 式が不正であるとき。

1．2　EnvelopedXmlSigner

1）クラス説明

Enveloped 型 XML 電子署名を行うクラス。

System.Object
　XmlSigner
　　EnvelopedXmlSigner

宣言

```
public class EnvelopedXmlSigner : XmlSigner
```

解説

SignedXml クラスを使用し、Enveloped 型 XML 電子署名を付与。

使用例

```
if( openFileDialog.ShowDialog() != DialogResult.OK )
{
    return;
}

//XML ドキュメントのインスタンス生成
XmlDocument xmlDocument = new XmlDocument();

//XML ロード
xmlDocument.Load( openFileDialog.FileName );

//キーストアクラスのインスタンス生成
SigningKeyStore keyStore = new SigningKeyStoreWithCapicom();

//XML 電子署名クラスのインスタンス生成
EnvelopedXmlSigner xmlSignature = new EnvelopedXmlSigner(keyStore);

try
{
    //署名の付与
    XmlDocument signedXmlDocument = xmlSignature.Sign(xmlDocument);
```

```
}
catch( SelectSigningKeyCancelException error )
{
    Console.WriteLine( error.Message );
}
```

必要条件

名前空間: Nori.Hpki.XmlSignature

アセンブリ: XmlSignature (XmlSignature.dll 内)

参照

EnvelopedXmlSigner メンバ | Nori.Hpki.XmlSignature 名前空間

2) コンストラクタ

EnvelopedXmlSigner クラスの新しいインスタンスを初期化。

宣言

```
public EnvelopedXmlSigner(
   SigningKeyStore signingKeyStore
);
```

パラメータ

signingKeyStore

署名用証明書を選択するための SigningKeyStore 抽象クラスのサブクラスインスタンス。

3) フィールド

① certificate

XmlSigner から継承。

② containerName

XmlSigner から継承。

③ cspName

XmlSigner から継承。

4）メソッド

① Sign(XmlDocument)

Enveloped 型 XML 電子署名を行う。

与えられた XML ドキュメントのルートエレメントに対して署名。

宣言

```
public XmlDocument Sign(
        XmlDocument documentToSign
        );
```

パラメータ

documentToSign

署名対象の Xml ドキュメント。

戻り値

署名された XML ドキュメント。

② Sign(XmlDocument, string, XmlNamespaceManager)

Enveloped 型 XML 電子署名を行う。

署名対象エレメントは XPath 式にて指定。

宣言

```
public XmlDocument Sign(
        XmlDocument documentToSign,
        string xpath,
        XmlNamespaceManager namespaceManager
);
```

パラメータ

documentToSign

署名対象の Xml ドキュメント。

xpath

署名対象の Xml エレメントの XPath 式

namespaceManager

XPath 式で使用する名前空間の解決のための XmlNamespaceManager クラスインスタンス。

戻り値

署名された XML ドキュメント。

例外

例外の種類 条件

ToSignElementXPathException 署名対象 XML エレメントを指定する Xpath 式が不正であるとき。

③ GetElementToSign

Xml ドキュメントから XPath 式で指定された署名対象 XML エレメントを取得。

宣言

```
protected XmlElement GetElementToSign(
        XmlDocument document,
        string xpath,
        XmlNamespaceManager namespaceManager
);
```

パラメータ

document

署名対象 XML ドキュメント。

xpath

署名対象の Xml エレメントの XPath 式。

namespaceManager

XPath 式で使用する名前空間の解決のための XmlNamespaceManager クラスインスタンス。

戻り値

署名対象 XML エレメント。

例外

例外の種類 条件

ToSignElementXPathException 署名対象 XML エレメントを指定する Xpath 式が不正であるとき。

1．3 EnvelopingXmlSignature

1）クラス説明

Enveloping 型 XML 電子署名を行うクラス。

System.Object
　XmlSigner
　　EnvelopingXmlSigner

宣言

```
public class EnvelopingXmlSigner : XmlSigner
```

解説

SignedXml クラスを使用し、Enveloping 型 XML 電子署名を付与。

使用例

```
if( openFileDialog.ShowDialog() != DialogResult.OK )
{
    return;
}

//XML ドキュメントのインスタンス生成
XmlDocument xmlDocument = new XmlDocument();

//XML ロード
xmlDocument.Load( openFileDialog.FileName );

//キーストアクラスのインスタンス生成
SigningKeyStore keyStore = new SigningKeyStoreWithCapicom();

//XML 電子署名クラスのインスタンス生成
EnvelopingXmlSigner xmlSignature = new EnvelopingXmlSigner(keyStore);

try
{
    //署名を付与
```

```
            XmlDocument signedXmlDocument =
xmlSignature.Sign(xmlDocument,"test");
        }
        catch( SelectSigningKeyCancelException error )
        {
            Console.WriteLine( error.Message );
        }
```

必要条件

名前空間: Nori.Hpki.XmlSignature

アセンブリ: XmlSignature (XmlSignature.dll 内)

参照

EnvelopingXmlSigner メンバ | Nori.Hpki.XmlSignature 名前空間

2) Sign(XmlDocument, string)

EnvelopingXmlSigner クラスの新しいインスタンスを初期化。

宣言

```
public EnvelopingXmlSigner(
        SigningKeyStore signingKeyStore
);
```

パラメータ

signingKeyStore

署名用証明書を選択するための SigningKeyStore 抽象クラスのサブクラスインスタンス。

3) フィールド

① certificate

XmlSigner から継承。

② containerName

XmlSigner から継承。

③ cspName

XmlSigner から継承。

4）メソッド

① Sign(XmlDocument, string)

Enveloping 型 XML 電子署名を行う

与えられた XML ドキュメントのルートエレメントに対して署名。

宣言

```
public XmlDocument Sign(
        XmlDocument documentToSign,
        string objectId
);
```

パラメータ

documentToSign

署名対象の Xml ドキュメント。

objectId

Object タグの ID 属性値。

戻り値

署名された XML ドキュメント。

② Sign(XmlDocument, string, XmlNamespaceManager, string)

Enveloping 型 XML 電子署名を付与。

署名対象エレメントは XPath 式にて指定。

宣言

```
public XmlDocument Sign(
        XmlDocument documentToSign,
        string xpath,
        XmlNamespaceManager namespaceManager,
        string objectId
);
```

パラメータ

documentToSign

署名対象の Xml ドキュメント。

xpath

署名対象の Xml エレメントの XPath 式。

namespaceManager

XPath 式で使用する名前空間の解決のための XmlNamespaceManager クラスインスタンス。

objectId

Object タグの ID 属性値。

戻り値

署名された XML ドキュメント。

例外

例外の種類 条件

ToSignElementXPathException 署名対象 XML エレメントを指定する Xpath 式が不正であるとき。

③ GetElementToSign

Xml ドキュメントから XPath 式で指定された署名対象 XML エレメントを取得。

宣言

```
protected XmlElement GetElementToSign(
        XmlDocument document,
        string xpath,
        XmlNamespaceManager namespaceManager
);
```

パラメータ

document

署名対象 XML ドキュメント。

xpath

署名対象の Xml エレメントの XPath 式。

namespaceManager

XPath 式で使用する名前空間の解決のための XmlNamespaceManager クラスインスタンス。

戻り値

署名対象 XML エレメント。

例外

例外の種類 条件

ToSignElementXPathException 署名対象 XML エレメントを指定する Xpath 式が不正であるとき。