

);

パラメータ

message

例外の原因を説明するエラーメッセージ。

③ X509CertificateNotFoundException (string, Exception)

X509CertificateNotFoundException クラスの新しいインスタンスを初期化。

宣言

```
public X509CertificateNotFoundException(  
    string message,  
    Exception innerException  
);
```

パラメータ

message

例外の原因を説明するエラーメッセージ。

innerException

現在の例外の原因である例外。innerException パラメータが null 参照でない場合は、内部例外を処理する catch ブロックで現在の例外が発生。

5. 列挙型

5. 1 CapicomSelectType

CAPICOM の証明書選択方法。

宣言

```
public enum CapicomSelectType
```

メンバ

Dialog

選択ダイアログを表示。

ShalHash

証明書の拇印で選択。

必要条件

名前空間: `Nori.Hpki.XmlSignature`

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

参照

`CapicomSelectType` クラス | `CapicomSelectType` メンバ | `Nori.Hpki.XmlSignature`

名前空間

5. 2 ChainCheckType

証明書信頼チェーン検証時の失効状態検証タイプ。

宣言

```
public enum ChainCheckType
```

メンバ

OnLine

証明書失効リストをオンラインで取得し失効確認を行う。

オンラインで取得できない場合は IE のキャッシュ内と証明書ストア内の証明書失効リストを使用。

Offline

IE のキャッシュ内と証明書ストア内の証明書失効リストを使用。

None

失効確認なし。

必要条件

名前空間: `Nori.Hpki.XmlSignature`

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

参照

`ChainCheckType` クラス | `ChainCheckType` メンバ | `Nori.Hpki.XmlSignature` 名前空間

5. 3 ChainTrustStatusType

証明書信頼チェーンの検証結果。

宣言

```
public enum ChainTrustStatusType
```

メンバ

TrustNoError

検証エラーなし。

TrustIsNotTimeValid

公開鍵証明書が有効期間外の場合。

TrustIsNotTimeNested

公開鍵証明書が有効期間が不適切な場合。

TrustIsRevoked

公開鍵証明書が失効されている場合。

TrustIsNotSignatureValid

公開鍵証明書が改ざんされている場合。

TrustIsNotValidForUsage

公開鍵証明書の使用方法に適合していない場合。

TrustIsUntrustedRoot

作成された証明書信頼チェーンのルート証明書は信頼されていないルート証明書である場合。

TrustRevocationStatusUnkonwn

公開鍵証明書に記述された失効リスト配布地点に失効リストが見つからない場合、
又は公開鍵証明書に失効リスト配布地点が記述されていない場合。

TrustIsCyclic

証明書信頼チェーンがサイクリックになっている場合。

TrustInvalidExtension

公開鍵証明書に無効な拡張を含んでいる場合。

TrustInvalidPolicyConstraints

公開鍵証明書もしくは信頼チェーンの証明書の一つに、拡張領域として PolicyConstraints が存在し、そこから発行された証明書の一つに許可されていない PolicyMapping もつか必要な Policies を持っていない場合。

TrustInvalidBasicConstraints

公開鍵証明書もしくは信頼チェーンの証明書の一つに、拡張領域として BasicConstraints が存在し、その証明書は、他の証明書を発行する設定になっていないのに信頼パスに存在したり、証明書チェーンのパスの長さを超えている場合。

TrustInvalidNameConstraints

公開鍵証明書もしくは信頼チェーンの証明書の一つに、不適切な NameConstraints が存在する場合。

TrustHasNotSupportedNameConstraint

公開鍵証明書もしくは信頼チェーンの証明書の一つに、サポートされていないフィールドを持つ NameConstraints が存在する場合
minimum、maximum フィールドがサポートされていない。そのため、minimum は常に”0”であり、maximum は常に空でなければならない。X400 Address や、EDI Party Name や Registered Id は、alternative name としてはサポートしていない。

TrustHasNotDefinedNameConstraint

公開鍵証明書もしくは信頼チェーンの証明書の一つに、NameConstraints が存在し、その次の証明書に NameConstraints 拡張領域が存在しない場合。

TrustHasNotPermittedNameConstraint

公開鍵証明書もしくは信頼チェーンの証明書の一つに、NameConstraints が存在し、その次の証明書に許可された名前が存在しない場合。

TrustHasExcludedNameConstraint

公開鍵証明書もしくは信頼チェーンの証明書の一つに、NameConstraints が存在し、その次の証明書に除外された名前が存在する場合。

TrustIsOfflineRevocation

公開鍵証明書もしくは信頼チェーンの一つの公開鍵証明書の失効状態が、オフラインになっているか古くなっている場合。

TrustNoIssuanceCahinPolicy

公開鍵証明書が、その上位パスにある公開鍵証明書の PolicyConstraints で要求されている発行ポリシーを持っていない場合。

TrustIsPartialchain

公開鍵証明書が不足しているため証明書信頼チェーンを作成できない場合。

TrustCtlIsNotTimeValid

証明書信頼リストが有効期間外である場合。

TrustCtlIsNotSignatureValid

証明書信頼リストが改ざんされている場合。

TrustCtlIsNotValidForUsage

証明書信頼リストの使用方法に適合してない場合。

必要条件

名前空間: `Nori.Hpki.XmlSignature`

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

参照

`ChainTrustStatusType` クラス | `ChainTrustStatusType` メンバ |
`Nori.Hpki.XmlSignature` 名前空間

5. 4 KeySpec

鍵のタイプ。

宣言

```
public enum KeySpec
```

メンバ

KeyExchange

鍵交換用暗号化鍵の場合。

Signature

署名鍵の場合。

必要条件

名前空間: `Nori.Hpki.XmlSignature`

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

参照

KeySpec クラス | KeySpec メンバ | `Nori.Hpki.XmlSignature` 名前空間

6. XmlSignatureService

XML フォーマットのデータに対する署名と検証の機能を提供する XML WEB サービス。

Classes

XmlSigner

XML 電子署名 Web サービス。

XmlVerifier

XML 電子署名 検証 Web サービス。

6. 1 XmlSigner

1) クラス説明

XML 電子署名 Web サービス。

System.Object

MarshalByValueComponent

WebService

BaseService

XmlSigner

宣言

```
public class XmlSigner : BaseService
```

必要条件

Namespace: XmlSignatureService

Assembly: XmlSignatureService (in XmlSignatureService.dll)

参照

XmlSigner Members | XmlSignatureService Namespace

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

```
public XmlSigner () ;
```


3) メソッド

① EnvelopingXmlSigner

Enveloping 型 XML 電子署名を付与。

宣言

```
public XmlNode EnvelopingXmlSigner(  
    XmlNode xmlNodeToSign,  
    string objectId  
);
```

パラメータ

xmlNodeToSign

XML 電子署名を付加する XML ドキュメント。

objectId

Enveloping 型 XML 電子署名の object タグの ID を指定。

戻り値

署名後の XML ドキュメント。

② EnvelopedXmlSigner

Envelope 型 XML 電子署名を付与。

宣言

```
public XmlNode EnvelopedXmlSigner(  
    XmlNode xmlNodeToSign  
);
```

パラメータ

xmlNodeToSign

XML 電子署名を付加する XML ドキュメント。

戻り値

署名後の XML ドキュメント。

6. 2 XmlVerifier

1) クラス説明

XML 電子署名 検証 Web サービス。

System.Object

```
· MarshalByValueComponent
  WebService
    BaseService
      XmlVerifier
```

宣言

```
public class XmlVerifier : BaseService
```

必要条件

Namespace: XmlSignatureService

Assembly: XmlSignatureService (in XmlSignatureService.dll)

参照

XmlVerifier Members | XmlSignatureService Namespace

2) コンストラクタ

XmlVerifier クラスの新しいインスタンスを初期化。

宣言

```
public XmlVerifier();
```

3) メソッド

① Verify

XML 電子署名を検証。

宣言

```
public XmlNode Verify(
    XmlNode xmlNodeToVerify
);
```

パラメータ

xmlNodeToVerify

検証する XML ドキュメント。

戻り値

検証結果。

研究成果の刊行に関する一覧表

書籍

なし

雑誌

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
西腋清行、 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

20031106

以降は雑誌/図書等に掲載された論文となりますので、
「研究成果の刊行に関する一覧表」をご参照ください。