

SiteMinder

Federation Manager .NET SDK ガイド

12.52 SP1



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。本ドキュメントは、CA が知的財産権を有する機密情報であり、CA の事前の書面による承諾を受けずに本書の全部または一部を複製、譲渡、変更、開示、修正、複製することはできません。

本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし、CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負いません。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本書の制作者は CA および CA Inc. です。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2014 CA. All rights reserved. 本書に記載されたすべての商標、商号、サービス・マークおよびロゴは、それぞれの各社に帰属します。

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- SiteMinder
- CA SiteMinder® Federation (旧 CA Federation Manager)

CA への連絡先

テクニカルサポートの詳細については、弊社テクニカルサポートの Web サイト (<http://www.ca.com/jp/support/>) をご覧ください。

マニュアルの変更点

SiteMinder r12.51.または 12.52 では、このガイドに変更はありませんでした。

目次

第 1 章: CA SiteMinder® Federation .NET SDK の概要	7
.NET SDK のアーキテクチャ	7
プログラミングに関する要件	8
第 2 章: .NET SDK のインストール	9
Windows での .NET SDK のインストール	9
Windows での .NET SDK のアンインストール	10
第 3 章: .NET SDK コンポーネント	11
オープン形式 Cookie	11
IFederationOpenIdentity インターフェース	13
アイデンティティファクトリ	14
IFedIdentitySDKLogger インターフェース	14
第 4 章: .NET SDK の使用	15
アサーティングパーティでのプログラムフロー	15
依存パーティでのプログラムフロー	16
CA SiteMinder® Federation .NET SDK のログ記録.....	18
プログラミングの例.....	19
.NET SDK サンプルアプリケーション.....	21

第 1 章: CA SiteMinder® Federation .NET SDK の概要

このセクションには、以下のトピックが含まれています。

[.NET SDK のアーキテクチャ \(P. 7\)](#)

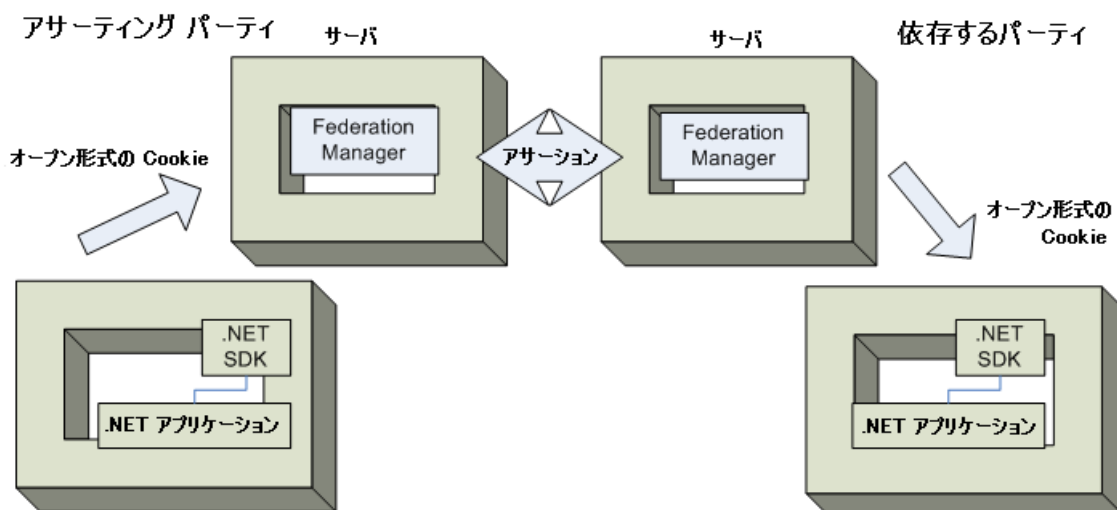
[プログラミングに関する要件 \(P. 8\)](#)

.NET SDK のアーキテクチャ

CA SiteMinder® Federation .NET SDK は、.NET アプリケーションの連携を支援します。.NET SDK を使用すると、.NET アプリケーションは CA SiteMinder® Federation にユーザ情報を提供し、CA SiteMinder® Federation によって提供されるユーザ情報を消費することができます。.NET SDK は、グローバルオープン形式 Cookie を使用して、ユーザの識別情報を表し、ユーザプリンシパルおよび属性をカプセル化します。.NET SDK は、共有秘密キーから派生するキーを使用して Cookie を暗号化します。共有秘密キーおよび暗号化変換に対応しているアプリケーションは、Cookie を使用してユーザ情報を取得できます。.NET SDK は、オープン形式 Cookie の暗号化および復号化に AES アルゴリズムを使用します。

アサーティングパーティ側の .NET アプリケーションは、.NET SDK を使用して認証されたユーザのログイン ID を CA SiteMinder® Federation へ渡します。CA SiteMinder® Federation は、Cookie からログイン ID を抽出し、依存パーティに送信されるフェデレーションアサーションに追加します。CA SiteMinder® Federation は、属性を Cookie に追加し、最長有効期間などの Cookie の設定の一部を変更することができます。依存パーティ側の .NET アプリケーションは、.NET SDK を使用して、CA SiteMinder® Federation によって送信されたユーザおよびセッション関連の情報を取得します。

以下の図は、アサーティングパーティおよび依存パーティ側での .NET SDK の役割を示しています。



プログラミングに関する要件

.NET SDK は、Microsoft 共通言語仕様 (CLS) の一部の機能のみを使用して、C# で実装されています。そのため、.NET SDK は、CLS をサポートする言語 (Visual Basic .NET、Visual C# .NET、Visual C++ .NET など) で作成されたアプリケーションからアクセスできます。

.NET SDK インターフェースは、CA.Federation.FedIdentitySdk.dll を介して使用できます。.NET アプリケーションはネームスペース CA.Federation.FedIdentitySdk を使用して、この DLL を参照できます。

.NET アプリケーションは、Cookie のゾーン、Cookie 名、および共有秘密キーを .NET SDK へ渡す必要があります。.NET アプリケーションは、便利な方法で設定ファイルなどへこのデータを格納できます。アプリケーションはパスワードを暗号化できますが、.NET SDK へ渡す前にそれを復号する必要があります。パスワードはプレーンテキスト文字配列として渡す必要があります。Cookie のゾーン、Cookie 名、および暗号化パスワードの設定値は、両方の側 (.NET Application および CA SiteMinder® Federation) で同じである必要があります。これらの値は帯域外で通信されます。

第 2 章: .NET SDK のインストール

Windows での .NET SDK のインストール

CA SiteMinder® Federation .NET SDK のインストールは、完全に自動化されています。インストールプログラムによって順を追って手順が示されます。

重要: .NET Framework のバージョン 3.5 が .NET SDK をインストールするシステムにインストールされている必要があります。そうでないと、インストールは失敗します。サポートされているオペレーティングシステムは、[エラー!ハイパーリンクの参照に誤りがあります](#)。サイト上の「Compatibility Matrix」に示されています。

.NET のインストール場所を指定できます。リンク ライブラリ、CA.Federation.FedIdentitySdk.dll はデフォルトで C:\Program Files\CA\Federation Manager\sdk\dotnet\bin にインストールされています。

`ca-fedmgr-dotnet-sdk-version-win32.exe` を使用して、.NET SDK インストーラを実行します。実行可能ファイルは[テクニカル サポート サイト](#)にあります。

サポート サイトでインストール キットを見つける方法

1. [Technical Support] をクリックします。
2. CA サポート オンラインにログインします。
3. [Download Center] をクリックします。

ダウンロードセンターで適切なインストールキットを検索します。

次の手順に従ってください:

1. 実行中のすべてのアプリケーションを終了します。
2. インストール実行ファイルが置かれている場所に移動します。
3. `ca-fedmgr-dotnet-sdk-version-win32.exe` をダブルクリックします。
インストール ウィザードが起動されます。
4. インストール ウィザードの指示に従ってインストールを完了します。
5. インストールが完了したら、システムを再起動します。

CA SiteMinder® Federation Windows エージェントのインストールが完了しました。

Windows での .NET SDK のアンインストール

.NET SDK を削除する前に、必ずシステムに JRE の有効なバージョンが展開されていることを確認してください。有効な JRE が存在しない場合、アンインストールは失敗します。

Windows から .NET SDK をアンインストールする方法

1. [コントロールパネル]で[プログラムの追加と削除]をダブルクリックします。
2. SiteMinder .NET SDK 12.52 SP1 を選択して [変更と削除] をクリックします。

画面のプロンプトに従い、完了したら [閉じる] をクリックします。

第 3 章: .NET SDK コンポーネント

このセクションには、以下のトピックが含まれています。

[オープン形式 Cookie](#) (P. 11)

[IFederationOpenIdentity インターフェース](#) (P. 13)

[アイデンティティ ファクトリ](#) (P. 14)

[IFedIdentitySDKLogger インターフェース](#) (P. 14)

オープン形式 Cookie

フェデレーション オープン形式 Cookie により、アプリケーションはユーザ属性を CA SiteMinder® Federation にアサートし、CA SiteMinder® Federation によりカプセル化されたユーザ属性を消費することができます。オープン形式 Cookie には以下の一般的特性があります。

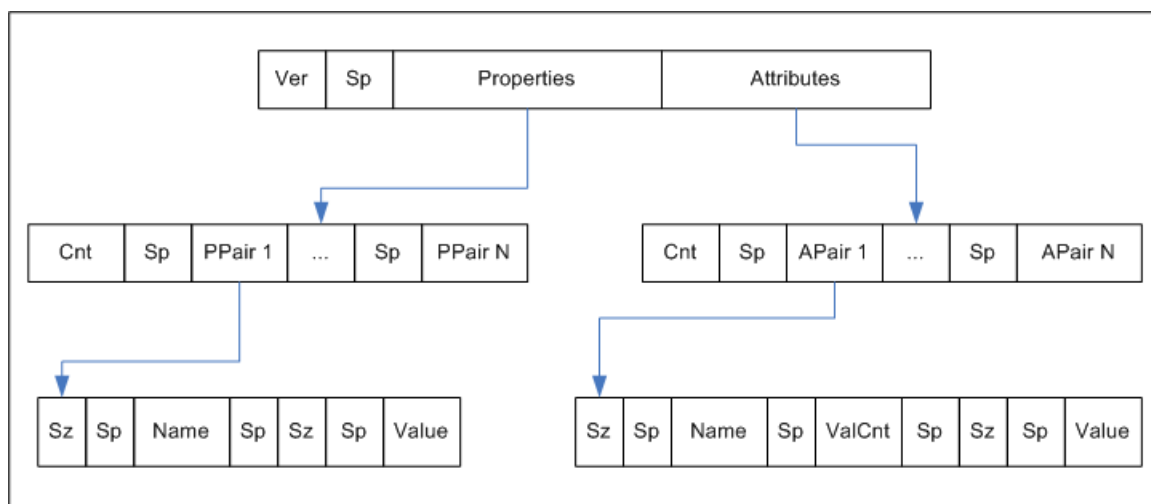
- Cookie は、任意のプログラミング言語で書かれたアプリケーションによってアクセス可能です。
- Cookie コンテンツは、UTF-8 バイトの文字列から構成され、それは国際文字セットをサポートします。
- UTF-8 バイトの各名前/値ペアの合わせたサイズは、名前/値ペアに先行します。
- スペース文字は読みやすいように追加されます。
- Cookie は簡単に解析でき、容易に拡張可能です。

重要: Cookie に「=」などのような安全でない文字が含まれる場合は、二重引用符でその値を囲んでください。ユーザ インターフェース、または SDK によってこのオプションを指定できます。

オープン形式 Cookie には以下のプロパティ情報が含まれます。

- Cookie バージョン
- 名前 ID
- 名前 ID 形式
- セッション ID
- AuthnContext
- UserDN (ユーザ ID と同じ)
- UserConsent
- ログイン ID
- ExpiresON (有効期限)

以下の図はオープン形式を表しています。



キー：

- Ver -- Cookie 形式バージョン。値は 1 です。
- Sp -- ASCII スペース文字。読みやすくするためにのみ使用されます。
- プロパティ -- プリンシパルに関する情報
- 属性 -- アサーションからの SAML 属性
- Cnt -- 次に続く名前値ペアの数。ASCII で表されます。
- Sz -- 次に続く名前または値の長さ
- ValCnt -- 属性値の数

このフォーマットのバックス・ナウア記法 (BNF) は以下の通りです (0* が 0 以上、1* が少なくとも 1 を意味します。)

- DIGIT = ASCII 数字 (0 ~ 9)
- CHAR = UTF-8 文字
- Sp = ASCII スペース (文字 32)
- トークン = 1*CHAR
- Cookie = バージョン Sp プロパティ属性
- バージョン = 1*DIGIT
- Cnt = 1*DIGIT
- プロパティ = Cnt 1*PPair
- 属性 = Cnt 0*APair
- ValCnt = 1*DIGIT
- PPair = Sz Sp 名前 Sp Sz Sp 値
- APair = Sz Sp 名前 Sp ValCnt Sp Sz Sp 値
- Sz = 1*DIGIT
- 名前 = トークン
- 値 = トークン

IFederationOpenIdentity インターフェース

IFederationOpenIdentity インターフェースにより、オープン形式 Cookie を操作するメソッドが定義されます。.NET SDK によって公開されたクラスは、ネームスペース `CA.Federation.FedIdentitySdk` 下で利用可能です。`IdentityFactory` クラスからメソッドを 1 つ呼び出すことにより、IFederationOpenIdentity インターフェースを実装します。

このインターフェースの詳細情報については、Doxygen で生成された参考資料を参照してください。

アイデンティティファクトリ

IdentityFactory クラスにより、IFederationOpenIdentity インターフェースの実装を取得するメソッドが提供されます。

注: 唯一サポートされた暗号変換は「AES128/CBC/PKCS5Padding」です。また、デフォルトを取得するために NULL を使用できます。

IdentityFactory クラスには、以下のメソッドが含まれています。

static IFederationOpenIdentity GetInstance (string cryptolInstance)

IFederationOpenIdentity インターフェースの実装オブジェクトを生成します。

静的な IFederationOpenIdentity GetInstance (文字列 cryptolInstance、bool bUseHmac)

IFederationOpenIdentity インターフェースの実装オブジェクトを生成します。

static IFederationOpenIdentity GetInstance (string zoneName, char[] password, string domain, string cryptolInstance)

IFederationOpenIdentity インターフェースの実装オブジェクトを生成します。

static IFederationOpenIdentity GetInstance (string zoneName, char[] password, string domain, string cryptolInstance, bool bUseHmac)

IFederationOpenIdentity インターフェースの実装オブジェクトを生成します。

IFedIdentitySDKLogger インターフェース

IFedIdentitySDKLogger インターフェースにより、カスタム ロギング メッセージを指定するための以下のメソッドが提供されます。

void LogTrace (string fileName, string methodName, string message)

トレース メッセージをログ記録します。

void LogError (string fileName, string methodName, string message)

エラー メッセージをログ記録します。

第 4 章: .NET SDK の使用

このセクションには、以下のトピックが含まれています。

[アサーティングパーティでのプログラムフロー](#) (P. 15)

[依存パーティでのプログラムフロー](#) (P. 16)

[CA SiteMinder® Federation .NET SDK のログ記録](#) (P. 18)

[プログラミングの例](#) (P. 19)

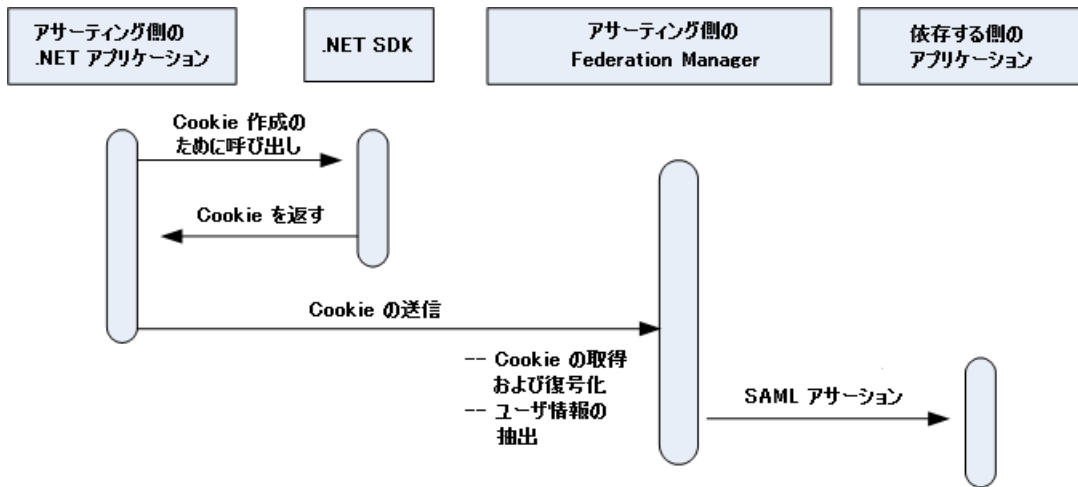
[.NET SDK サンプルアプリケーション](#) (P. 21)

アサーティングパーティでのプログラムフロー

アサーティングパーティでの CA SiteMinder® Federation で、.NET アプリケーションはユーザ ID 情報を CA SiteMinder® Federation に提供できます。アサーティングパーティでの CA SiteMinder® Federation によるプログラムフローは以下のように進行します。

1. .NET アプリケーションは、.NET SDK を呼び出し ID 情報を有するオープン形式 Cookie を生成します。
2. .NET SDK は暗号化された Cookie を返します。Cookie を暗号化するために使用されるキーは、CA SiteMinder® Federation と帯域外のアプリケーション間で通信される共有秘密キーから派生します。
3. .NET アプリケーションはアサーティングパーティの CA SiteMinder® Federation に Cookie を送信します。
4. CA SiteMinder® Federation は Cookie を受信し復号化します。
5. CA SiteMinder® Federation は Cookie からユーザ ID 情報を抽出します。
6. オプションで、CA SiteMinder® Federation は属性を更新または追加することにより Cookie を変更できます。
7. CA SiteMinder® Federation は [SAML アサーション] にユーザ ID 情報を挿入します。

以下の図は、アサーティングパーティでのプログラムフローを示しています。



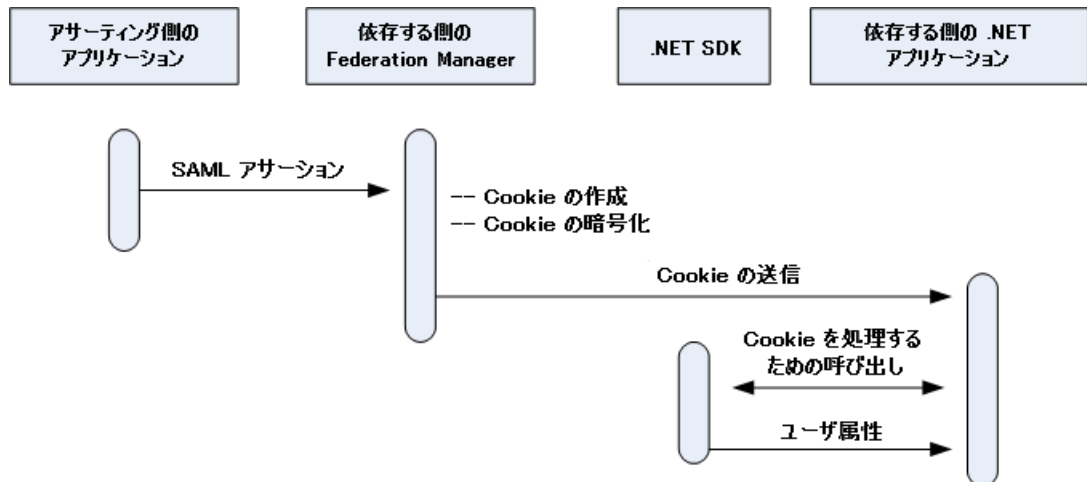
依存パーティでのプログラムフロー

依存パーティでの CA SiteMinder® Federation で、.NET アプリケーションは CA SiteMinder® Federation からユーザ情報を受信できます。依存パーティでの CA SiteMinder® Federation によるプログラムフローは以下のように進行します。

1. CA SiteMinder® Federation はリクエスト処理中に SAML アサーションを受信します。
2. CA SiteMinder® Federation は最新のユーザ情報で Cookie を作成します。
3. CA SiteMinder® Federation は FIPS に準拠しているアルゴリズムを使用して、Cookie を暗号化します。Cookie を暗号化するために使用されるキーは、CA SiteMinder® Federation と帯域外のアプリケーション間で通信される共有秘密キーから派生します。
4. CA SiteMinder® Federation は暗号化されたオープン形式 Cookie を .NET アプリケーションに送信します。

5. .NET アプリケーションは、.NET SDK を呼び出して Cookie の復号および処理を行います。
6. .NET アプリケーションは、アサーション属性および主要属性に対する値を取得します。
7. .NET アプリケーションは、スキュー時間を指定するしないにかかわらず、isExpired () メソッドを呼び出すことで Cookie が有効期限切れかどうかを判断できます。このメソッドは、オプションのスキュー時間に追加して、Cookie 上の有効期限スタンプを現在の GMT 時間と比較します。GMT 時間のほうが大きい場合、Cookie は期限切れです。Cookie の有効期限スタンプは、Cookie が作成されるときに setTimeToLive () メソッドを使用して指定されます。
8. .NET アプリケーションは、AuthnContext および UserConsent の URI を設定することもできます。

以下の図は、依存パーティでのプログラム フローを示しています。



CA SiteMinder® Federation .NET SDK のログ記録

.NET SDK ロガーが有効な場合、ロガーは標準出力ストリームにメッセージを書き込みます。ロギングは、デフォルトでは無効になっています。

CA SiteMinder® Federation.NET SDK ロギングを有効にする方法

1. `Logger.xml` ファイルを `.NET SDK` インストールディレクトリ¥`config` から `.NET SDK DLL the ¥bin` フォルダにコピーします。
2. `Logger.xml` で `EnableLogging` パラメータを `yes` に設定します。

ロギングが有効になります。

プログラミングの例

以下のコードフラグメントは、オープン形式 **Cookie** の作成方法を示しています。

```
// カスタムにバインドされる、インターフェース タイプ
IFederationOpenIdentity のオブジェクト参照を取得します
// IFederationOpenIdentity インターフェースの実装。
// AES128/CBC/PKCS5Padding は唯一サポートされた暗号変換文字列です。
```

```
IFederationOpenIdentity openID =
IdentityFactory.GetInstance("AES128/CBC/PKCS5Padding", UseHMACFlag);
```

```
// Cookie を作成するのに必要なパラメータを初期化します。
```

```
openID.InitCookieInfo (ドメイン、CookieZone、CookieName、パスワード)
```

```
// ユーザ属性を設定します。
```

```
openID.LoginID = txtLoginID.Text;
```

```
// オープン形式 Cookie を作成し、レスポンス オブジェクトへそれを設定
します。
```

```
openID.CreateCookie(HttpResponse);
```

以下のコードフラグメントは、オープン形式 **Cookie** を消費する方法を示しています。

```
// カスタムにバインドされる、インターフェース タイプ
IFederationOpenIdentity のオブジェクト参照を取得します
// IFederationOpenIdentity インターフェースの実装。
// AES128/CBC/PKCS5Padding は唯一サポートされた暗号変換文字列です。
```

```
IFederationOpenIdentity openID =
IdentityFactory.GetInstance("AES128/CBC/PKCS5Padding", UseHMACFlag);
```

```
// Cookie を抽出するために必要なパラメータを初期化します。
```

```
openID.InitCookieInfo (ドメイン、CookieZone、CookieName、パスワード)
```

```
// HttpRequest から Cookie を抽出して復号化し、Hashtable に属性を保存し
ます。
```

```
openID.ExtractCookie(HttpRequest);
```

```
//いくつかの属性を取得します。
```

```
文字列 id = openID.LoginID;
```

```
文字列 nid = openID.NameID;
```

.NET SDK サンプル アプリケーション

.NET テスト アプリケーションは、オープン形式 Cookie を生成し、.NET SDK を使用して、それを消費します。テスト アプリケーションは多くの方法で展開できます。推奨される 1 つの方法を以下に示します。

注: IIS Web Server が ASP.NET コンテンツを許可するように設定されていることを確認します。

.NET SDK テスト アプリケーションを展開する方法

1. フォルダ（この例では TestApplication）を作成します。
2. `dotNet_SDK_home¥testapp` から TestApplication フォルダに以下のファイルをコピーします。
 - OpenCookieConsumer.aspx.cs
 - OpenCookieConsumer.aspx
 - OpenCookieConsumetUseHMAC.aspx.cs
 - OpenCookieConsumetUseHMAC.aspx
 - OpenCookieGenerator.aspx.cs
 - OpenCookieGenerator.aspx
 - web.config
3. TestApplication ディレクトリで bin フォルダを作成します。
4. `dotNet_SDK_home¥bin` から TestApplication¥bin に CA.Federation.FedIdentitySdk.dll をコピーします。
5. 編集する web.config ファイルを開きます。 <appSettings> セクションで、パスワード、ゾーン、および名前のキーを変更します。
 - パスワードは暗号化キーを引き出すために使用される共有秘密キーです
 - ゾーンは Cookie ゾーンです。
 - 名前は Cookie 名です。生成された Cookie の最終名にはゾーンおよび名前が含まれます。
6. インターネット インフォメーション サービス マネージャに移動します。
7. Web サイトを右クリックします。
8. Web サイトの説明を入力します。

9. Web サイトに TCP ポート (たとえば 100) を割り当てます。
10. Web サイト ホーム ディレクトリ (すなわち、テストアプリケーション ディレクトリの場所) へのパスを入力するか参照します。
11. [Web サイトのアクセス許可] ダイアログ ボックスで、Read および Run スクリプト (ASP など) のオプションを選択します。
12. [完了] を選択します。
13. IIS を再起動します。
14. .NET SDK テスト アプリケーションのオープン形式 Cookie 作成ページにアクセスします。
15. ログイン ID を入力します。
16. [移動] をクリックします。

システムが、[.NET SDK テスト アプリケーション オープン形式 Cookie の消費] ページを表示します。OpenCookieConsumer.aspx ページに Cookie のコンテンツが表示されます。この場合、Cookie 内の属性はログイン ID のみです。

17. .NET SDK テスト アプリケーションのオープン形式 Cookie の使用ページにアクセスします。そこで、オープン形式 Cookie を復号し、Cookie に含まれる主要属性およびアサーション属性を表示します。