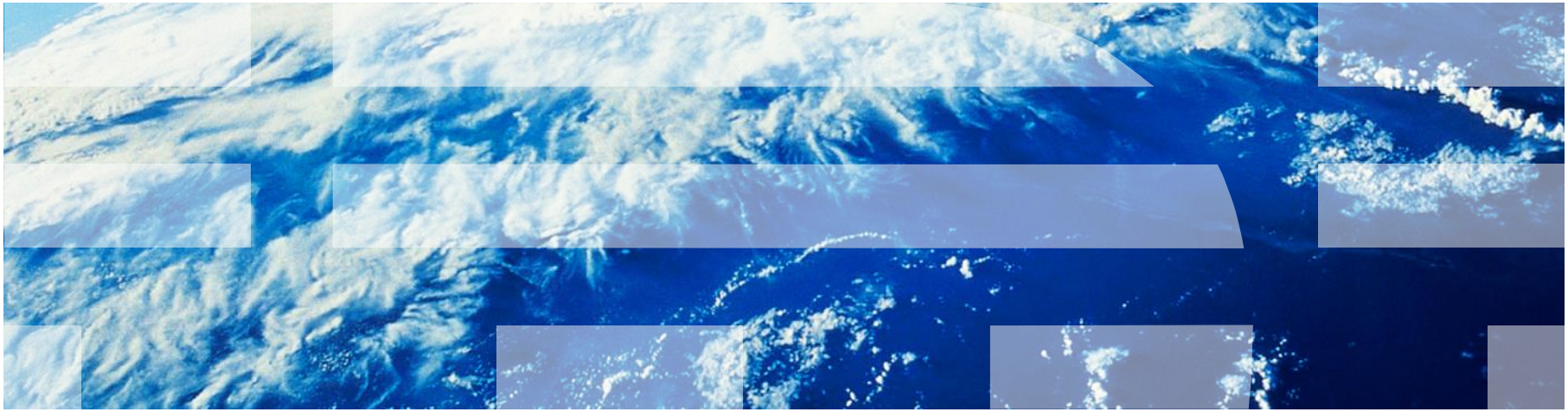
IBM Worklight Foundation V6.2.0 入門

WebSphere LTPA ベースの認証



2014 年 7 月 17 日

商標

- IBM、IBM ロゴ、ibm.com、WebSphere および Worklight は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。
- Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

- この資料は、事前に IBM の書面による許可を得ずにその一部または全部を複製することは禁じられています。

IBM® について

- http://www.ibm.com/ibm/us/en/ を参照してください。

このモジュールが対象とする環境

- このモジュールは、IBM® Worklight® Consumer Edition または IBM Worklight Enterprise Edition のいずれかで使用するように意図されています。
  - このモジュールで紹介する機能は、無料の IBM Worklight Developer Edition では使用できません。
  - このモジュールを使用するには、Worklight Server を WebSphere® Application Server フル・プロファイルまたは Liberty プロファイル上にデプロイする必要があります。

アジェンダ

- WebSphere LTPA ベースの認証の概要
- サーバー・サイドの認証オプションについて
- LTPA 認証用の Worklight Server の構成
  - WebSphere Application Server の構成
  - オプション 1 に必要な追加ステップ
  - Worklight Console を保護するためのオプション・ステップ
- クライアント・サイドの認証コンポーネントの作成
- 結果の確認
- 演習

WebSphere LTPA ベースの認証の概要

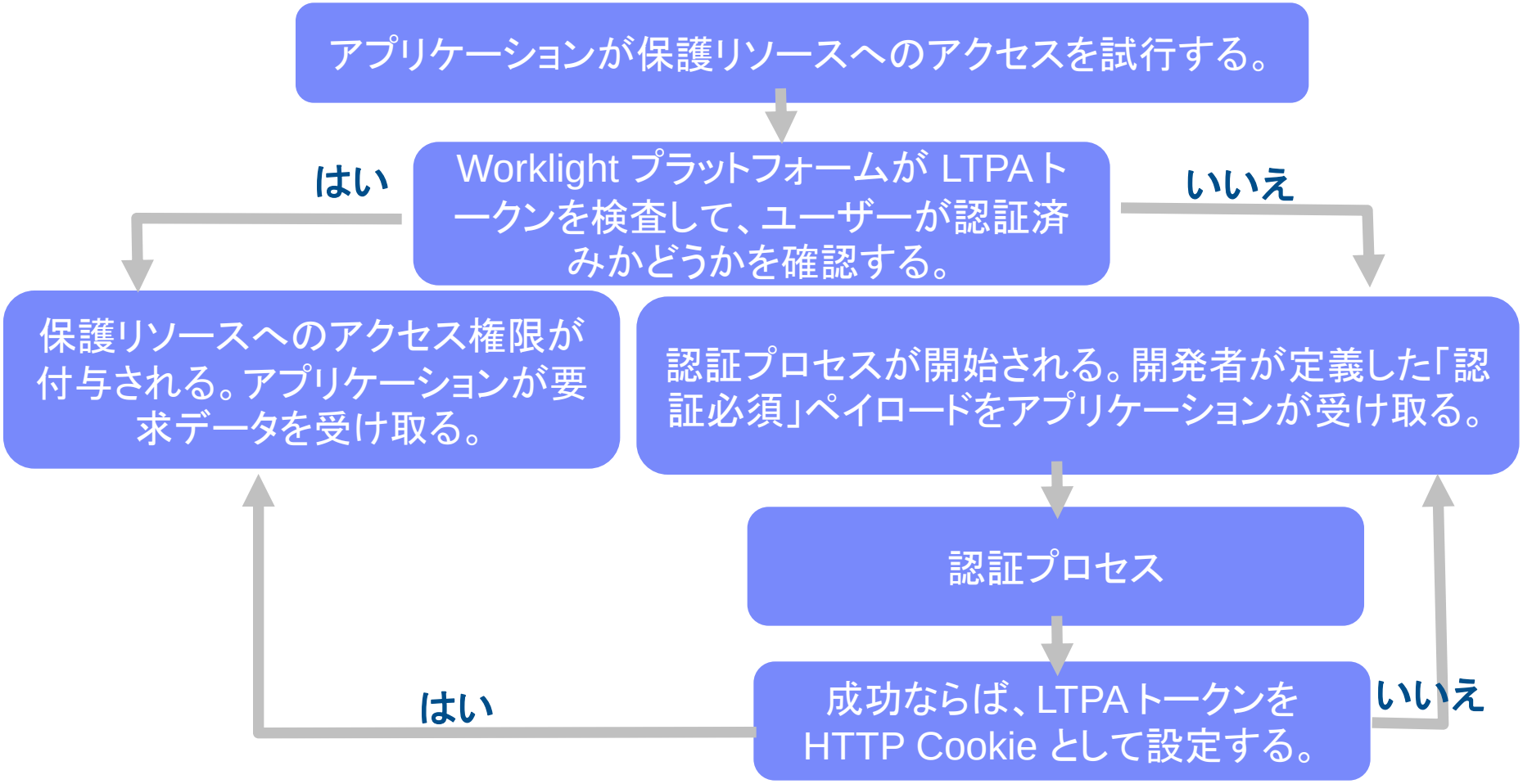
- WebSphere Application Server は、Lightweight Third-Party Authentication (LTPA) Cookie 内のセキュア・トークンを使用して、認証済みユーザーを検証します。また、WebSphere Application Server は、セキュアな WebSphere Application Server ドメイン全域でユーザーを信頼する目的でも、このメカニズムを使用します。
- Worklight を WebSphere Application Server 上で実行するときには、**WebSphereFormBasedAuthenticator** と **WebSphereLoginModule** を使用すると、LTPA トークンを使用して Worklight アプリケーションに対する認証を行うことが可能になります。
- Worklight アプリケーション用に WebSphere LTPA ベースの認証をサポートするには、2 つのオプションを使用できます。それらを **オプション 1** および **オプション 2** と呼びます。

アジェンダ

- WebSphere LTPA ベースの認証の概要
- サーバー・サイドの認証オプションについて
- LTPA 認証用の Worklight Server の構成
  - WebSphere Application Server の構成
  - オプション 1 に必要な追加ステップ
  - Worklight Console を保護するためのオプション・ステップ
- クライアント・サイドの認証コンポーネントの作成
- 結果の確認
- 演習

サーバー・サイドの認証オプションについて(1/7)

- 以下のダイアグラムは、WebSphere LTPA ベースの認証プロセスを示しています。



サーバー・サイドの認証オプションについて (2/7)

オプション 1

- 企業ポリシーにより、保護された WebSphere Application Server 上で WAR ファイルを保護する必要がある場合は、オプション 1 を使用してこの状況に対処できます。
- Worklight プロジェクト WAR ファイルで Web リソースを保護するには、リソースとユーザー・ロールを指定します。
  - この構成の一部として定義されている**オーセンティケーターとログイン・モジュール**は、(提供された資格情報に基づいて) ユーザーを認証し、その際に基礎となる WebSphere Application Server のセキュリティー API を使用します。つまりこのメカニズムでは、ユーザーが初回ログイン時にユーザー名とパスワードを指定した場合は、このデータを使用して、WebSphere Application Server が構成されている基本レジストリーに対してユーザーが認証されます。そうでない場合は、2 回目以降のアクセス時に有効な LTPA トークンが提供された場合に、この LTPA 資格情報が使用されます。

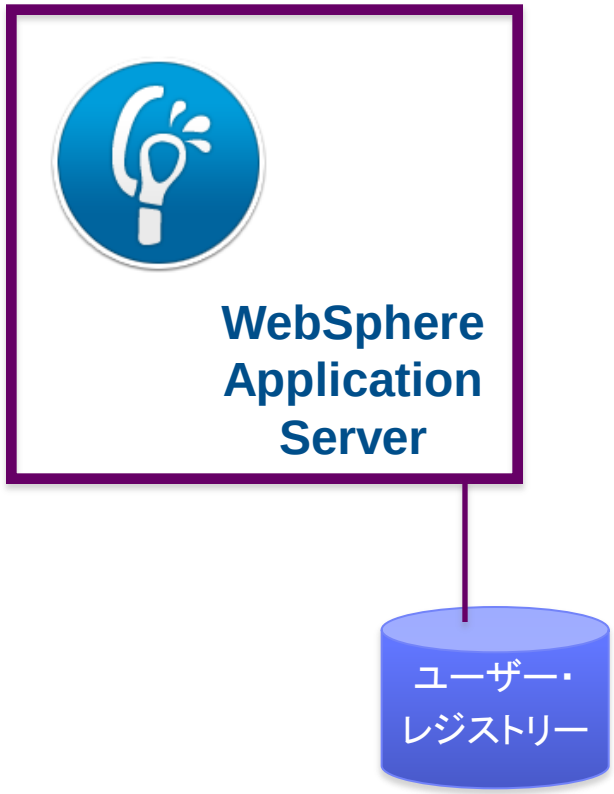
サーバー・サイドの認証オプションについて (3/7)

オプション 2

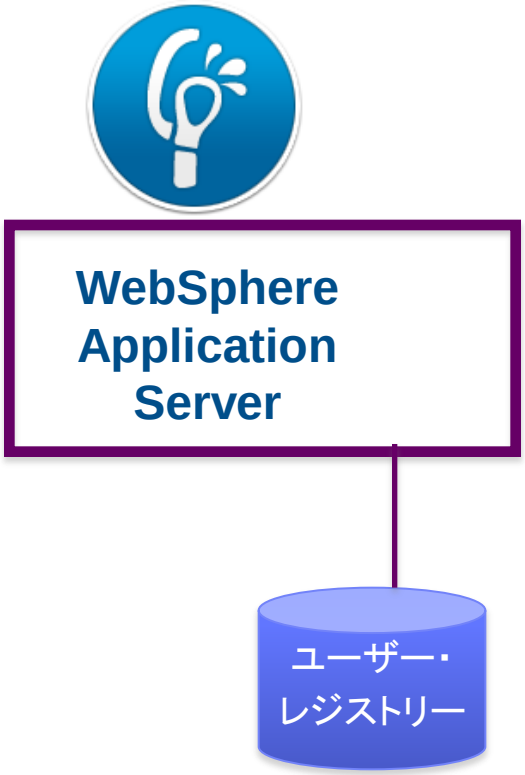
- オプション 2 は、基礎となる WebSphere Application Server インスタンスのセキュリティー構成を使用して、Worklight プラットフォーム・レベルでユーザー認証を処理する Worklight セキュリティー構成用です。
  - WebSphere Application Server 上に WAR ファイルとしてデプロイされる Worklight プロジェクトは保護されません。この WAR ファイルの `web.xml` ファイルは、Web リソースを保護するセキュリティー制約をまったく参照しません。
  - この構成の一部として定義されている**オーセンティケーターとログイン・モジュール**は、(提供された資格情報に基づいて) ユーザーを認証し、その際に基礎となる WebSphere Application Server のセキュリティー API を使用します。つまりこのメカニズムでは、ユーザーが初回ログイン時にユーザー名とパスワードを指定した場合は、このデータを使用して、WebSphere Application Server が構成されているレジストリーに対してユーザーが認証されます。そうでない場合は、2 回目以降のアクセス時に有効な LTPA トークンが提供された場合に、この LTPA 資格情報が使用されます。

サーバー・サイドの認証オプションについて(4/7)

- オプション 1: WebSphere Application Server によって認証が施行される



- オプション 2: WebSphere Application Server 構成に依存することで Worklight Server が認証を施行する



サーバー・サイドの認証オプションについて(5/7)

- オプション 1

アプリケーション

getSecretData

認証が要求される
(WebSphere Application Server によって)

submitAuthentication

ここで認証され、LTPA が設定される

getSecretData (LTPA で渡される)

秘密データが渡される

WebSphere Application Server

Worklight Server

WebSphere Application Server がユーザーの認証をユーザー・レジストリーと照合して行う。成功した認証に基づいて、Worklight ログイン・モジュールが Worklight ユーザーを設定する。

サーバー・サイドの認証オプションについて(6/7)

- オプション 2

アプリケーション

Worklight Server

getSecretData

(Worklight Server によって) 認証が要求される

submitAuthentication

ここで認証され、LTPA が設定される

getSecretData (LTPA で渡される)

秘密データが渡される

Worklight は、ログイン・モジュールを使用して WebSphere Application Server のセキュリティーを呼び出し、WebSphere Application Server のユーザー・レジストリーと照合してユーザーを認証する。

サーバー・サイドの認証オプションについて(7/7)

- オプション 1 とオプション 2 はどちらも利点があり、使用法が異なります。

	オプション 1	オプション 2
利点	このオプションでは、従来の WebSphere Application Server 認証と信頼モデルを使用します。 コンテナーはすべてのセキュリティーを施行します。したがって、Java™ Enterprise Edition (Java EE) コンテナーを保護することに費やした既存の投資を、他のソフトウェア・ベンダーの SSO 製品を使用することによって、再利用することができます。	このオプションでは、従来の WebSphere Application Server 認証と信頼モデルを使用し、なおかつ IBM Worklight プロジェクト WAR ファイルの変更による影響を受けません。 コンテナーはすべてのセキュリティーを施行します。したがって、Java™ Enterprise Edition (Java EE) コンテナーを保護することに費やした既存の投資を、他のソフトウェア・ベンダーの SSO 製品によって、再利用することができます。 デバイス、アプリケーション、アプリケーション・インスタンス、およびユーザーの階層化された認証は、意図したとおりに動作します。 Worklight ランタイムに固有のセキュリティー設定を構成することにより、基礎となるコンテナーのセキュリティーに妨害されることなく、柔軟性が達成されます。
使用法	このオプションは、デバイスが信頼でき、不正アプリケーションのアクセスが制限されるシナリオに適しています。	このオプションは、デバイスまたはデバイス上のアプリケーションが信頼できないシナリオに適しています。 IBM Worklight プラットフォームに組み込まれたマルチステップ認証性検査を使用すると、Jailbreak されたデバイス、不正アプリケーション、無許可のユーザーに対するサービス拒否が確実に行われます。

- **それらの利点を考慮すると、自分の業務でオプション 1 を必要としない場合は、オプション 2 が最適です。**

アジェンダ

- WebSphere LTPA ベースの認証の概要
- サーバー・サイドの認証オプションについて
- LTPA 認証用の Worklight Server の構成
  - WebSphere Application Server の構成
  - オプション 1 に必要な追加ステップ
  - Worklight Console を保護するためのオプション・ステップ
- クライアント・サイドの認証コンポーネントの作成
- 結果の確認
- 演習

WebSphere Application Server の構成 (1/4)

ステップ1: WebSphere Application Server のセキュリティーの有効化

- 2 つのオプションを比較するには、まず WebSphere Application Server 上で以下の設定を定義する必要があります。

  オプション 1 の場合:
  - 管理セキュリティーを使用可能にする
  - アプリケーション・セキュリティーを使用可能にする

  オプション 2 の場合:
  - 管理セキュリティーを使用可能にする

WebSphere Application Server の構成 (2/4)

ステップ2: authenticationConfig.xml のレルムとオーセンティケーターを構成する

- authenticationConfig.xml ファイルを {WAS_HOME}/profiles/{your profile}/installedApps/{your node}/{worklight EAR}/{worklight WAR}/WEB-INF/classes/conf の中から見つけ、“For websphere” というコメントの下のレルムをアンコメントして、以下のテキストのような状態にします。

```
<!-- For websphere -->
<realm name="WASLTPARealm" loginModule="WASLTPAModule">

  <className>com.worklight.core.auth.ext.WebSphereFormBasedAuthenticator</className>
  <parameter name="login-page" value="/login.html"/>
  <parameter name="error-page" value="/loginError.html"/>
</realm>
```

  - オプションとして、cookie-domain、cookie-name、および httponly-cookie というパラメーターを含めることができます。詳しくは、製品資料で LTPA オーセンティケーターに関するセクションを参照してください。

- 注: このレルムは既にアンコメントされている場合もあります。

WebSphere Application Server の構成 (3/4)

ステップ2: authenticationConfig.xml のレルムとオーセンティケーターを構成する

- “For websphere” というコメントの下のログイン・モジュールをアンコメントします。

```
<!-- For websphere -->
<loginModule name="WASLTPAModule">
  <className>com.worklight.core.auth.ext.WebSphereLoginModule</className>
</loginModule>
```

- 注: このログイン・モジュールは既にアンコメントされている場合もあります。

WebSphere Application Server の構成 (4/4)

ステップ3: authenticationConfig.xml のセキュリティー・テストを構成する

- セキュリティー・テストを必要に応じて authenticationConfig.xml に追加します。
  - Web 環境向けの開発を行う場合は、webSecurityTest を追加します。
  - モバイル環境向けの開発を行う場合は、mobileSecurityTest を追加します。

```
<securityTests>
        <webSecurityTest name="wasWebSecurity">
              <testUser realm="WASLTPARealm"/>
        </webSecurityTest>

        <mobileSecurityTest name="WAS-securityTest">
              <testAppAuthenticity/>
              <testDeviceId provisioningType="none" />
              <testUser realm="WASLTPARealm"
         </mobileSecurityTest>
 </securityTests>
```

アジェンダ

- WebSphere LTPA ベースの認証の概要
- サーバー・サイドの認証オプションについて
- LTPA 認証用の Worklight Server の構成
  - WebSphere Application Server の構成
  - オプション 1 に必要な追加ステップ
  - Worklight Console を保護するためのオプション・ステップ
- クライアント・サイドの認証コンポーネントの作成
- 結果の確認
- 演習

オプション 1 に必要な追加ステップ (1/3)
ステップ 1: login.html を作成する

- login.html という名前のファイルを作成し、WAR ファイルのルート ({WAS_HOME}/profiles/{your profile}/installedApps/{your node}/{worklight EAR}/{worklight WAR}) に保存します。
- この内容を以下のように設定します。

```
<html>
     <head></head>
     <body>
         <form action="j_security_check" method="post">
               Username: <input type="text" name="j_username" size="20"><br>
               Password: <input type="password" name="j_password" size="20"><br>
          <input type="submit" value="Login">
         </form>
     </body>
</html>
```

オプション 1 に必要な追加ステップ (2/3)
ステップ 2: loginError.html を作成する

- `loginError.html` エラー・ページを作成し、WAR ファイルのルート (`{WAS_HOME}/profiles/{your profile}/installedApps/{your node}/{worklight EAR}/{worklight WAR}`) に置きます。`loginError.html` ページは、ログインの失敗時に使用されます。
- この内容を以下のように設定します。

```
<html>
  <head></head>
   <body>
     Login invalid.
   </body>
</html>
```

オプション 1 に必要な追加ステップ (3/3)

ステップ 3: web.xml を構成する (このステップはオプション 2 では任意ですが、オプション 1 では必須です。)

- 次のパスの web.xml ファイルを見つけます。 {WAS_HOME}/profiles/{your profile}/installedApps/{your node}/{worklight EAR}/{worklight WAR}/WEB-INF/web.xml
- ルート・タグの中に、このコード・サンプルに示したタグを追加します。最も簡単な方法は、サンプルをコピー・アンド・ペーストすることです。
- これらのタグは、WAR ファイルで期待されている構成を WebSphere Application Server に渡します。

```
<security-constraint id="SecurityConstraint_1">
    <web-resource-collection id="WebResourceCollection_1">
      <web-resource-name>Snoop Servlet</web-resource-name>
      <description>Protection area for Snoop Servlet.</description>
      <url-pattern>/*</url-pattern>
      <http-method>GET</http-method>
      <http-method>POST</http-method>
    </web-resource-collection>
    <auth-constraint id="AuthConstraint_1">
      <description>Snoop Servlet Security:+:All Authenticated users
    for Snoop Servlet.</description>
      <role-name>Role 3</role-name>
    </auth-constraint>
    <user-data-constraint id="UserDataConstraint_1">
      <transport-guarantee>NONE</transport-guarantee>
    </user-data-constraint>
</security-constraint>
<security-role id="SecurityRole_1">
    <description>All Authenticated Users Role.</description>
    <role-name>Role 3</role-name>
</security-role>
<login-config>
    <auth-method>FORM</auth-method>
    <form-login-config>
      <form-login-page>/login.html</form-login-page>
      <form-error-page>/loginError.html</form-error-page>
    </form-login-config>
</login-config>
```

アジェンダ

- WebSphere LTPA ベースの認証の概要
- サーバー・サイドの認証オプションについて
- LTPA 認証用の Worklight Server の構成
  - WebSphere Application Server の構成
  - オプション 1 に必要な追加ステップ
  - Worklight Console を保護するためのオプション・ステップ
- クライアント・サイドの認証コンポーネントの作成
- 結果の確認
- 演習

オプション: Worklight Console の保護 (1/2)

- WebSphere Application Server の認証資格情報で Worklight Console を保護するには、authenticationConfig.xml ファイルを以下のように変更します。
  - <staticResources> エレメントをアンコメントし、静的リソースの保護を有効にします。

```
<!-- Uncomment the next element to protect the worklight console
 and the first section in securityTests below.  -->

<staticResources>

   <resource id="worklightConsole" securityTest="WorklightConsole">

        <urlPatterns>/console*</urlPatterns>

   </resource>

</staticResources>
```

オプション: Worklight Console の保護 (2/2)

- <customSecurityTest> エレメントを既存のセキュリティー・テストに追加します。

```
<securityTests>
    <customSecurityTest name="WorklightConsole">
        <test realm="WASLTPARealm" isInternalUserID="true"/>
    </customSecurityTest>
</securityTests>
```

アジェンダ

- WebSphere LTPA ベースの認証の概要
- サーバー・サイドの認証オプションについて
- LTPA 認証用の Worklight Server の構成
  - WebSphere Application Server の構成
  - オプション 1 に必要な追加ステップ
  - Worklight Console を保護するためのオプション・ステップ
- クライアント・サイドの認証コンポーネントの作成
- 結果の確認
- 演習

クライアント・サイドの認証コンポーネントの作成

- 認証モジュールの 1 つから既存の Worklight アプリケーションを使用します。
- アプリケーションに対してセキュリティーを実装するには、他の任意のタイプのレルムに対する実装と同じ方式に従ってから、該当レルムを使用するようにチャレンジ・ハンドラーを構成します。

```
var sampleAppRealmChallengeHandler = WL.Client.createChallengeHandler("WASLTPARealm");
```

- applicationDescriptor.xml ファイルで、アプリケーションが当該環境に対して使用する必要のあるセキュリティー・テストを指定します。

  以下に例を示します。

```
<common securityTest="WAS-securityTest"/>
<android version="1.0" securityTest="WAS-securityTest">
    <pushSender key= "keyTest" senderId="senderIdTest"/>
</android>
```

- オプション 2 を使用してアプリケーションをデプロイし、テストします。認証では、WebSphere Application Server が構成されている基礎となるユーザー・レジストリーから有効なユーザー名とパスワードを要求します。認証が成功すると、Worklight アプリケーションが認証されます。

アジェンダ

- WebSphere LTPA ベースの認証の概要
- サーバー・サイドの認証オプションについて
- LTPA 認証用の Worklight Server の構成
  - WebSphere Application Server の構成
  - オプション 1 に必要な追加ステップ
  - Worklight Console を保護するためのオプション・ステップ
- クライアント・サイドの認証コンポーネントの作成
- 結果の確認
- 演習

結果の確認

アジェンダ

- WebSphere LTPA ベースの認証の概要
- サーバー・サイドの認証オプションについて
- LTPA 認証用の Worklight Server の構成
  - WebSphere Application Server の構成
  - オプション 1 に必要な追加ステップ
  - Worklight Console を保護するためのオプション・ステップ
- クライアント・サイドの認証コンポーネントの作成
- 結果の確認
- 演習

演習

- オプション 2 に使用する認証サンプルを検討します。
- オプション 1 のステップで示したように、Worklight プロジェクト WAR を保護することによって、オプション 1 を実装します。
  - WAR ファイルの `web.xml` ファイルを更新します。
  - WAR ファイルを再パッケージし、WebSphere Application Server に再デプロイします。
- 予測される結果: ユーザー・エクスペリエンスは同じです。

特記事項

- これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。
- 本書は米国 IBM が提供する製品およびサービスについて作成したものです。
- 本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、または サービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の 製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作または サービスの 評価および検証は、お客様の責任で行っていただきます。
- IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。
  - 〒103-8510
    東京都中央区日本橋箱崎町19番21号
    日本アイ・ビー・エム株式会社
    法務・知的財産
    知的財産権ライセンス渉外
- **以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含む すべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が 禁じられる場合、強行規定の制限を受けるものとします。**
- この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。
- 本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部では ありません。それらの Web サイトは、お客様の責任でご使用ください。
- IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。
- 本プログラムのライセンス保持者で、(i) 独自に作成したプログラムと その他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。
  - IBM Corporation
    Dept F6, Bldg 1
    294 Route 100
    Somers NY 10589-3216
    USA
- 本プログラムに関する上記の情報は、適切な使用条件の下で使用すること ができますが、有償の場合もあります。
- 本書で説明されているライセンス・プログラムまたはその他のライセンス資 料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。
- IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、 他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

著作権使用許諾:

- 本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに 準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性が あることをほのめかしたり、保証することはできません。
- それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次の ように、著作権表示を入れていただく必要があります。
  - © (お客様の会社名) (西暦年).このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。© Copyright IBM Corp. _年を入れる_. All rights reserved.

プライバシー・ポリシーの考慮事項

- サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。
- このソフトウェア・オファリングは、展開される構成に応じて、(アプリケーション・サーバーが生成する) セッション情報を収集するセッションごとの Cookie を使用する場合があります。これらの Cookie は個人情報を含まず、セッション管理のために要求されるものです。加えて、匿名ユーザーの認識および管理のために持続的な Cookie が無作為に生成される場合があります。これらの Cookie も個人情報を含まず、要求されるものです。
- この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

サポートおよびコメント

- IBM Worklight の一連の文書、トレーニング資料、および質問をポストできるオンライン・フォーラムはすべて、次の IBM Web サイトからご覧になれます。
  - http://www.ibm.com/mobile-docs
- **サポート**
  - ソフトウェア・サブスクリプション & サポート (ソフトウェア・メンテナンスと呼ばれる場合もあります) は、パスポート・アドバンテージおよびパスポート・アドバンテージ・エクスプレスから購入されたライセンスに含まれています。International Passport Advantage Agreement および IBM International Passport Advantage Express Agreement の追加情報については、次のパスポート・アドバンテージ Web サイトを参照してください。
    - http://www.ibm.com/software/passportadvantage
  - ソフトウェア・サブスクリプション & サポートが有効になっている場合、IBM は、インストールおよび使用法 (ハウツー) に関する短期間の FAQ に対するサポートや、コード関連の質問に対するサポートを提供します。詳しくは、次の IBM ソフトウェア・サポート・ハンドブックを参照してください。
    - http://www.ibm.com/support/handbook
- **ご意見**
  - 本資料に関するご意見をお寄せください。本資料の具体的な誤りや欠落、正確性、編成、題材、または完成度に関するご意見をお寄せください。 お寄せいただくご意見は、本マニュアルまたは製品の情報、およびその情報の提示方法に関するもののみとしてください。
  - 製品の技術的な質問および情報、および価格については、担当の IBM 営業所、IBM ビジネス・パートナー、または認定リマーケターにお問い合わせください。
  - IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。IBM またはいかなる組織も、お客様から提示された問題についてご連絡を差し上げる場合にのみ、お客様が提供する個人情報を使用するものとします。
  - どうぞよろしくお願いいたします。
  - 次の IBM Worklight Developer Edition サポート・コミュニティーにご意見をお寄せください。
    - https://www.ibm.com/developerworks/mobile/worklight/connect.html
  - IBM からの回答を希望される場合は、以下の情報をご連絡ください。
    - 氏名
    - 住所
    - 企業または組織
    - 電話番号
    - E メール・アドレス

ありがとうございました