

IBM Worklight V6.1.0 **入門**

アプリケーション認証性保護



商標

- IBM、IBM ロゴ および ibm.com 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、www.ibm.com/legal/copytrade.shtml をご覧ください。
- 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。

アジェンダ

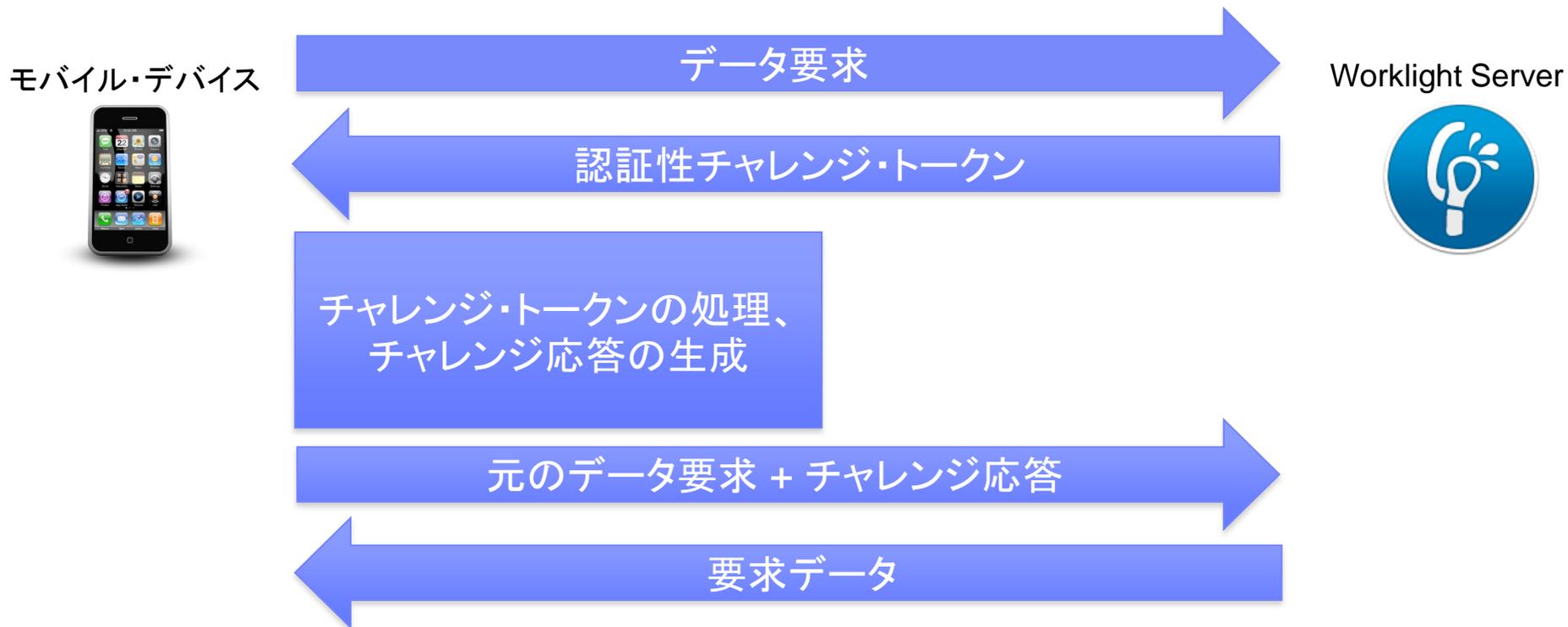
- 概要
- アプリケーション認証性検査の有効化 - ハイブリッド
- アプリケーション認証性検査の有効化 - ネイティブ
- Worklight Console からのアプリケーション認証性の制御

概要 (1/4)

- Worklight® Server が提供する HTTP サービス (API) へは、HTTP 要求を出すことで任意のエンティティからアクセスできます。
- 前のモジュールで説明したとおり、関連するサービスを各種のセキュリティ・テストで保護できます。
- アプリケーション認証性検査により、Worklight Server に接続しようとするアプリケーションが信頼できるものであり、第三者のアタッカーによって改ざんまたは変更されていないことを保証できます。
- アプリケーション認証性は、IBM Worklight Consumer Edition または IBM Worklight Enterprise Edition でのみ使用可能です。これは、無料の IBM Worklight Developer Edition では機能しません。
- アプリケーション認証性は、iOS および Android プラットフォームで使用可能です。

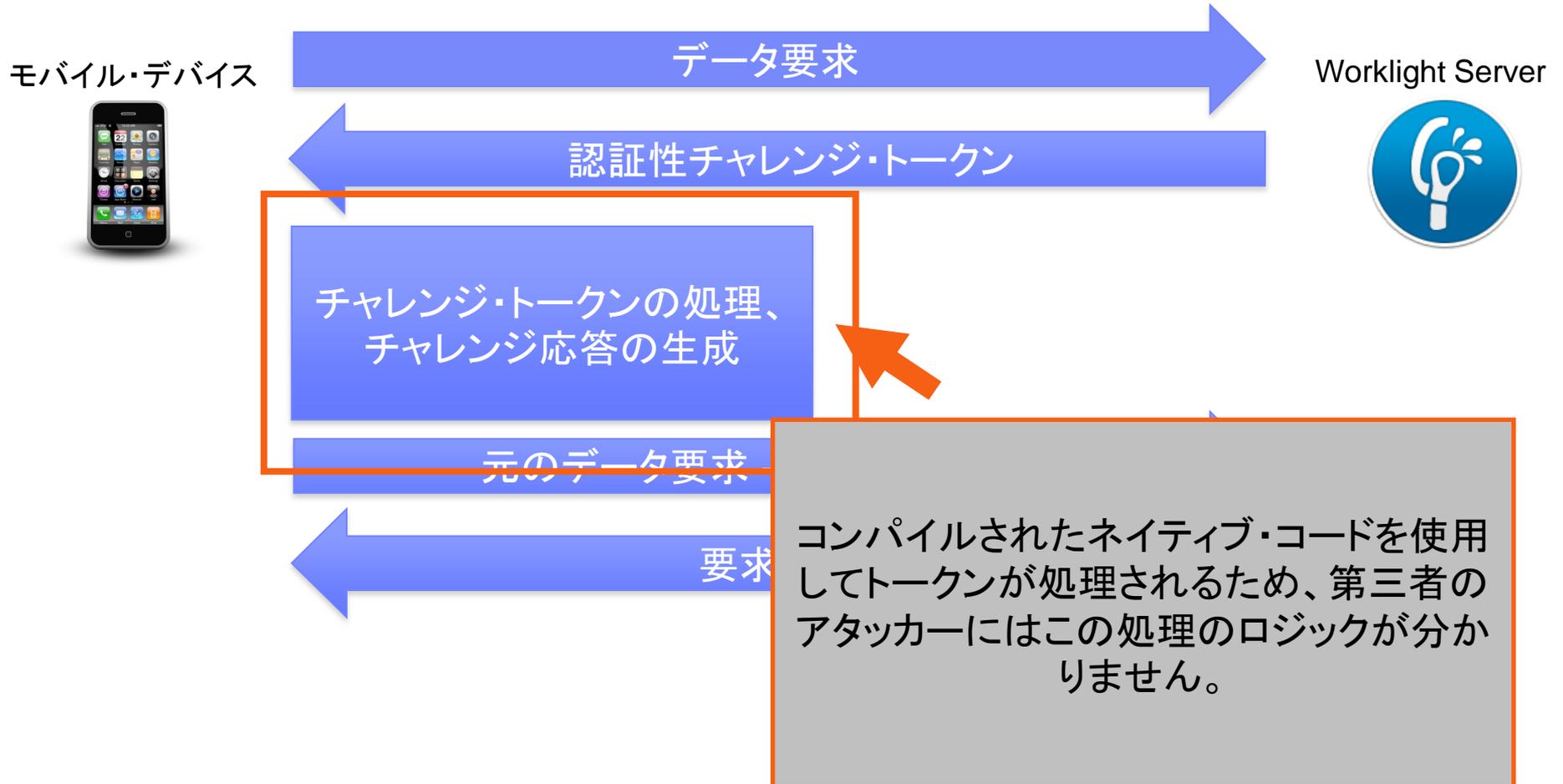
概要 (2/4)

- 認証性検査のフロー



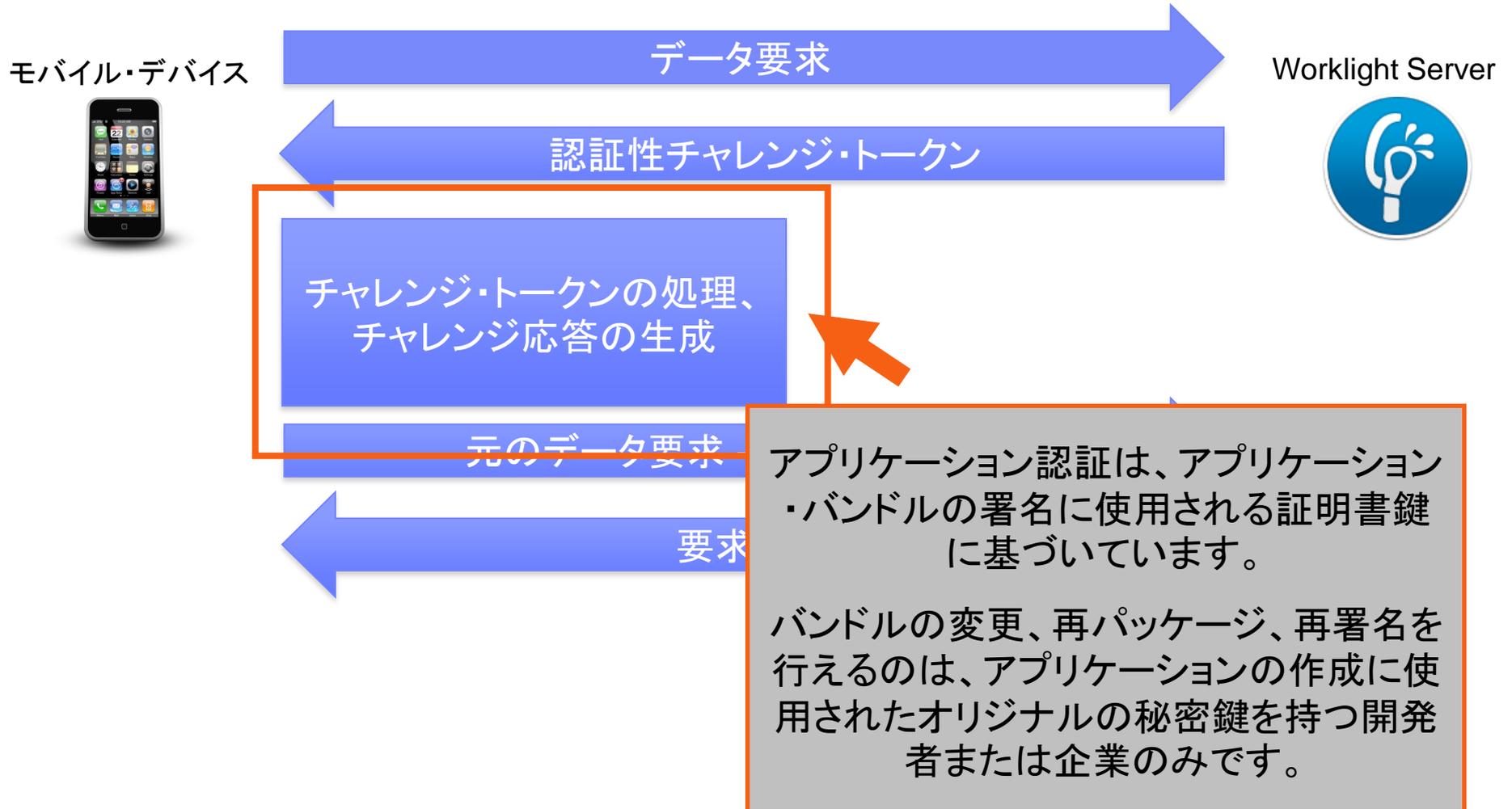
概要 (3/4)

- 認証性検査のフロー



概要 (4/4)

- 認証性検査のフロー



アジェンダ

- 概要
- アプリケーション認証性検査の有効化 - ハイブリッド
- アプリケーション認証性検査の有効化 - ネイティブ
- Worklight Console からのアプリケーション認証性の制御

アプリケーション認証性検査の有効化 - ハイブリッド (1/5)

- アプリケーション認証性を有効にする場合の最初のステップは、適切な認証レلمをセキュリティー・テストに追加することで、**authenticationConfig.xml** ファイルを変更することです。
- **<mobileSecurityTest>** を使用している場合、**<testAppAuthenticity/>** 子エレメントを追加する必要があります。
- **<customSecurityTest>** を使用している場合、**<test realm="wl_authenticityRealm"/>** 子エレメントを追加する必要があります。

```
<mobileSecurityTest name="mobileTest">  
  <testAppAuthenticity/>  
  <testUser realm="MyUserAuthRealm"/>  
  <testDeviceId provisioningType="auto" />  
</mobileSecurityTest>  
==  
<customSecurityTest name="mobileTest">  
  <test realm="wl_authenticityRealm" step="1"/>  
  <test realm="wl_antixsrfRealm" step="1"/>  
  <test realm="wl_remoteDisableRealm" step="1"/>  
  <test realm="MyUserAuthRealm" isInternalUserID="t  
  <test realm="wl_deviceAutoProvisioningRealm" isIn  
</customSecurityTest>
```

アプリケーション認証性検査の有効化 - ハイブリッド (2/5)

- 2 番目のステップは、アプリケーションの **application-descriptor.xml** ファイルの変更です。
- securityTest 属性を環境エレメントに追加します。以下に例を示します。

```
<android version="1.0" securityTest="customTests">
```

- **iOS 環境**のアプリケーション認証性検査を有効にするには、Apple Developer ポータルで定義したものと完全に同じようにアプリケーションの **bundleId** を指定する必要があります。以下に例を示します。



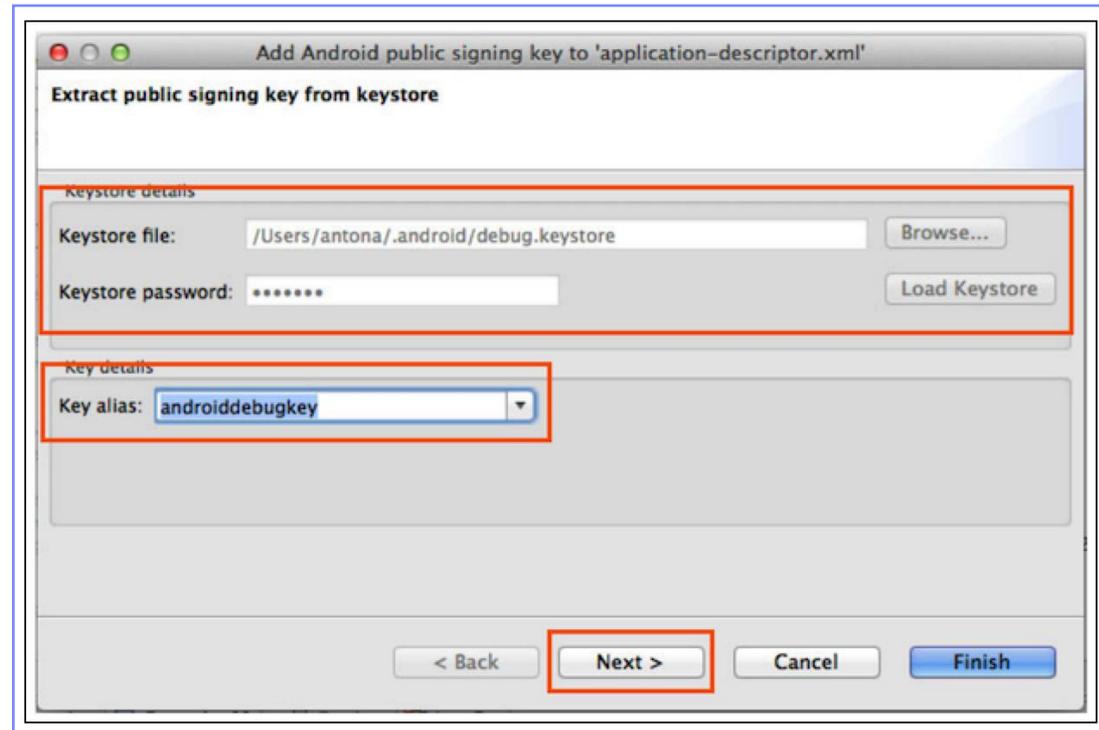
```
<mainFile>starbucks.html</mainFile>  
<thumbnailImage>common/images/thumbnail.png</thumbnailImage>  
<iphone bundleId="com.worklight.AntonDevApp" version="1.0">  
  <worklightSettings include="true"/>  
  <security>  
    <encryptWebResources enabled="false"/>  
    <testWebResourcesChecksum enabled="false" ignoreFileE  
  </security>  
</iphone>
```

アプリケーション認証性検査の有効化 - ハイブリッド (3/5)

- **Android 環境**のアプリケーション認証性検査を有効にするには、アプリケーション・バンドル (.apk ファイル) の署名に使用される証明書の公開署名鍵を抽出する必要があります。
- Worklight Studio では、このプロセスを単純化するツールが用意されています。
- 配布用のアプリケーション (実動) をビルドする場合、実動対応アプリケーションに署名するために使用する証明書から公開鍵を抽出する必要があります。
- 開発環境でアプリケーションをビルドする場合、Android SDK によって提供されているデフォルトの開発証明書の公開鍵を使用できます。
- 開発証明書は、**{user-home}/.android/debug.keystore** ファイル内の鍵ストアにあります。

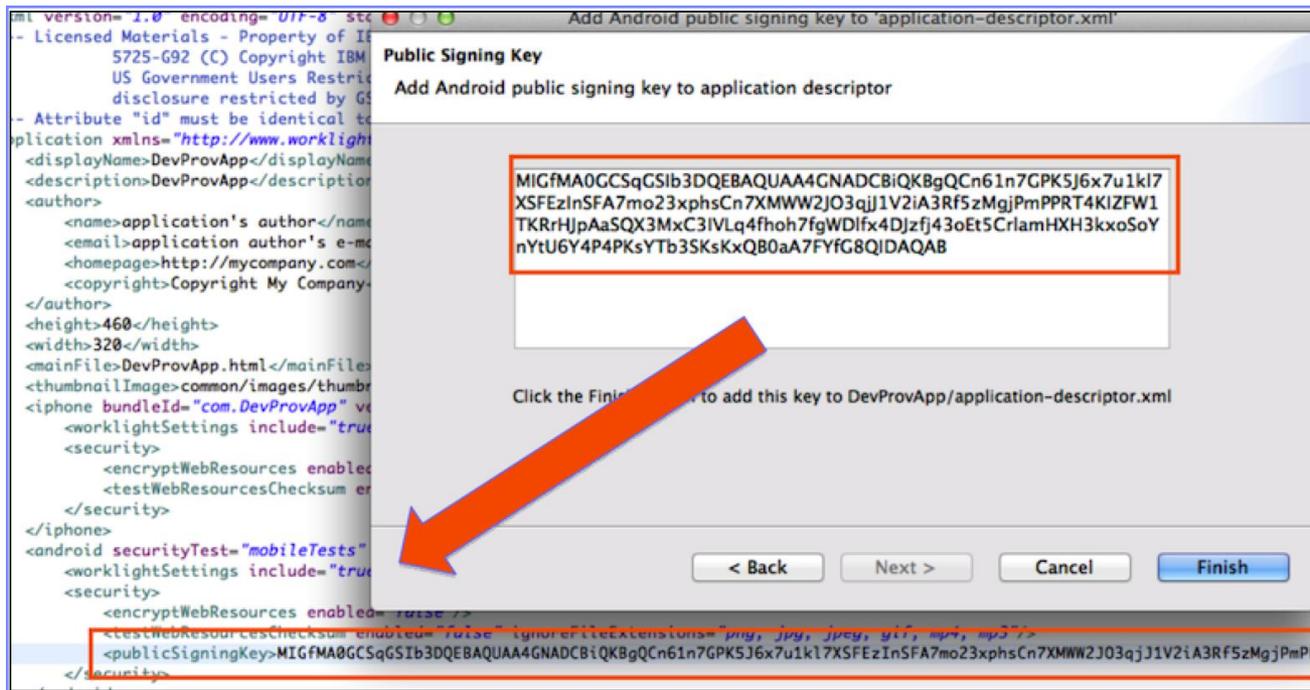
アプリケーション認証性検査の有効化 - ハイブリッド (4/5)

- 公開鍵の抽出は、手動で行うことも、Worklight Studio に用意されたウィザードを使用して行うこともできます。
- ウィザードを使用するには:
 1. ご使用の Android 環境を右クリックし、「公開署名鍵の抽出 (Extract public signing key)」を選択します。
 2. 鍵ストア・ファイルの場所とパスワードを指定し、「鍵ストアのロード (Load Keystore)」をクリックします。
 3. **debug.keystore** のデフォルトのパスワードは「android」です。
 4. 「鍵別名 (Key alias)」を設定し、「次へ (Next)」をクリックします。



アプリケーション認証性検査の有効化 - ハイブリッド (5/5)

- ダイアログが開き、公開鍵が表示されます。
- 「終了 (Finish)」をクリックすると、公開鍵が **application-descriptor.xml** ファイルの当該セクションに自動的に貼り付けられます。
- 必須エレメントの更新後に、アプリケーションを再ビルドして、Worklight Server に再デプロイします。



アジェンダ

- 概要
- アプリケーション認証性検査の有効化 - ハイブリッド
- アプリケーション認証性検査の有効化 - ネイティブ
- Worklight Console からのアプリケーション認証性の制御

アプリケーション認証性検査の有効化 - ネイティブ

- ネイティブ・アプリケーションでアプリケーション認証性を有効にする際は、以下のようにします。
 - **iOS 環境の場合**
 - Eclipse で実行するステップは前のスライドと同じですが、以下の追加のステップがあります。
 - Xcode でプロジェクトを開いてから、「その他のリンカー・フラグ (Other Linker Flags)」フィールドに、値 **-ObjC** を入力します。
 - **Android 環境の場合**
 - Eclipse で実行するステップは、前のスライドと同じです。その他のステップは不要です。

アジェンダ

- 概要
- アプリケーション認証性検査の有効化 - ハイブリッド
- アプリケーション認証性検査の有効化 - ネイティブ
- Worklight Console からのアプリケーション認証性の制御

Worklight Console からのアプリケーション認証性の制御 (1/2)

- Worklight Console には、アプリケーション認証性レールを有効/無効にする手段があります。
- この機能は、開発環境や QA 環境などで役に立つことがあります。
- 以下の 3 つのモードを設定できます。
 - **有効、ブロッキング (Enabled, blocking)** – このモードは、アプリケーション認証性検査が有効であることを意味します。アプリケーションが検査で不合格になると、Worklight Server はそのアプリケーションにサービスを提供しません。
 - **有効、サービス提供 (Enabled, serving)** – このモードは、アプリケーション認証性検査が有効であることを意味します。アプリケーションが検査で不合格になっても、Worklight Server はそのアプリケーションにサービスを提供します。
 - **無効 (Disabled)** – このモードは、アプリケーション認証性検査が無効であることを意味します。

Worklight Console からのアプリケーション認証性の制御 (2/2)

HelloWorklight HelloWorklight
✕ Delete

Last deployed at: 2013-11-04 16:28

	iPhone	Version 1.0 ● Active	Security Test: customTests App Authentication: ⚠ Enabled, servicing
	<input type="checkbox"/> Lock this version	Device Authentication: Default User Authentication: Default	
	iPad	Version 1.0 ● Active	Security Test: Default App Authentication: ⚠ Access Disabled
	<input type="checkbox"/> Lock this version	Device Authentication: Default User Authentication: Default	
	Android	Version 1.0 ● Active	Security Test: customTests App Authentication: ✔ Enabled, blocking
	<input type="checkbox"/> Lock this version	Device Authentication: Default User Authentication: Default	

[Preview as Common Resources](#)

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を提供し、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認できません。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問い合わせください。

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めめしたり、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、以下の具体的な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、または認定リマーカー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たします。
 - 次の IBM Worklight Developer Edition サポート・コミュニティ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

