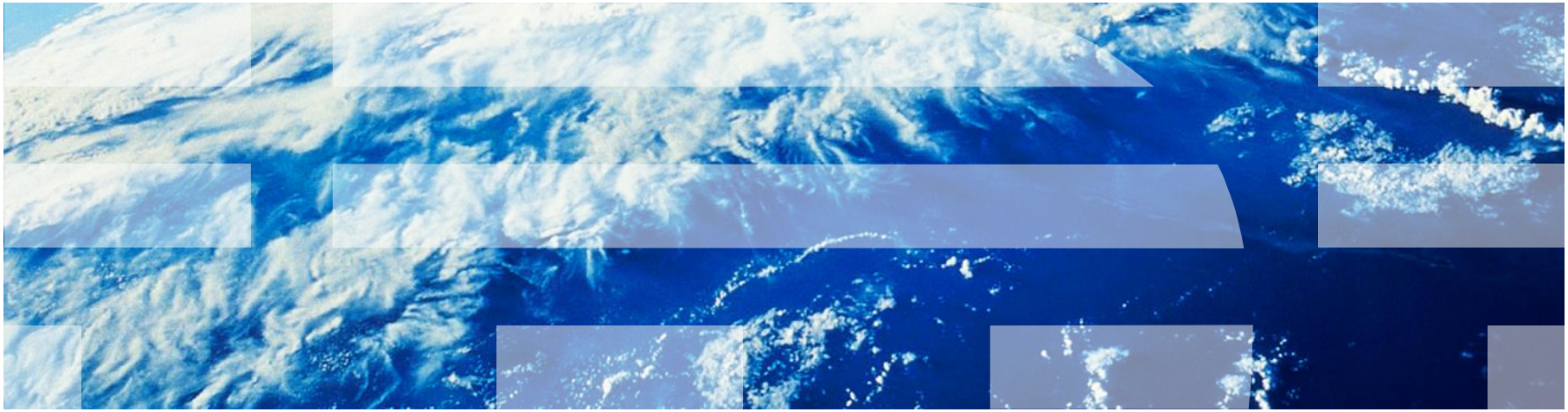
IBM Worklight Foundation V6.2.0 入門

デバイス・プロビジョニングの概念



2014 年 6 月 20 日

商標

- IBM、IBM ロゴ、ibm.com 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。

- 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
- デバイス ID
- デバイス・プロビジョニングについて
- プロビジョニングなし
- 自動プロビジョニング
- カスタム・プロビジョニング

概説 (1/2)

- デバイス・プロビジョニングは、IBM® Worklight® Foundation が提供する最も先進的で複雑なセキュリティー・フィーチャーの 1 つです。
- デバイス・プロビジョニングは、デバイス ID に証明書を添付するプロセスです。
- デバイス ID はユーザー ID に似ていますが、特定のデバイスを一意的に識別することを目的としています。
- デバイス ID は、さまざまな機能に不可欠です。以下に例を示します。
  - プッシュ通知 – 通知の送信先デバイスを確認したい場合
  - レポート – サーバーを利用しているデバイスの数を確認したい場合
- デバイス ID を知ることで、セキュリティー統合の可能性が大きく広がります。例えば、どのデバイスが Worklight Server との通信を許可されているかを判断できます。
- このトレーニング・モジュールでは、デバイス・プロビジョニングとは何か、どのようなタイプのデバイス・プロビジョニングが IBM Worklight Foundation でサポートされているか、デバイス・プロビジョニングのプロセスに含まれる成果物とは何かについて説明します。

概説 (2/2)

- IBM Worklight Foundation は、以下の 3 タイプのデバイス・プロビジョニングをサポートしています。
  - プロビジョニングなし
  - 自動プロビジョニング
  - カスタム・プロビジョニング
- このトレーニング・モジュールでは、最初の 2 つのタイプを重点的に扱います。
- カスタム・プロビジョニングについて詳しくは、チュートリアルおよびサンプルの表 9 にある**「カスタム・プロビジョニング」**トレーニング・モジュールおよびユーザー文書を参照してください。

アジェンダ

- 概要
- デバイス ID
- デバイス・プロビジョニングについて
- プロビジョニングなし
- 自動プロビジョニング
- カスタム・プロビジョニング

デバイス ID

- Worklight Server がデバイス ID を要求すると、クライアント・サイドのフレームワークによってデバイス ID が自動的に生成されます。
- デバイス IDは、Worklight Server で特定のデバイスを一意的に識別するために使用されます。
- ユーザー ID がユーザー認証に使用される方法と同様に、デバイス ID はデバイス認証に使用されます。
- デバイス・プロビジョニングは、デバイス ID に基づいて実行され、Android プラットフォームと iOS プラットフォームでサポートされます。

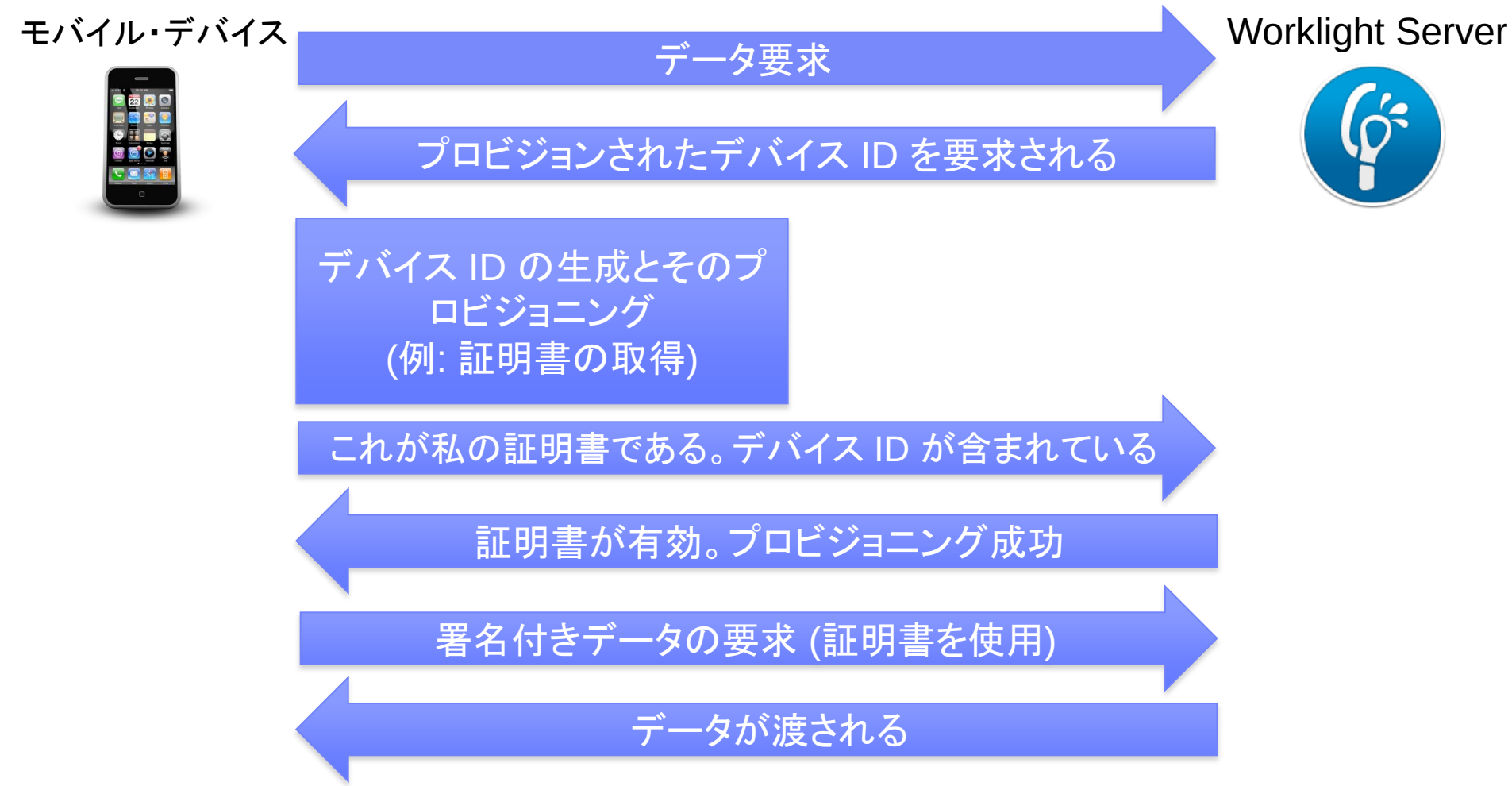
アジェンダ

- 概要
- デバイス ID
- デバイス・プロビジョニングについて
- プロビジョニングなし
- 自動プロビジョニング
- カスタム・プロビジョニング

デバイス・プロビジョニングについて (1/2)

- デバイス・プロビジョニングは、特定のデバイスを対象にして証明書が Worklight Server によって発行されるプロセスです。
- 発行された証明書には、プロビジョニング・プロセス時に取得されたデバイス情報が含まれています。
- 証明書が特定のデバイスに対して発行される前に、Worklight Server では、受け取ったデバイス資格情報に対して追加検証を実行できます。
- デバイス・プロビジョニングの証明書生成のために、独自の CA 鍵ストアを構成することも可能です。

デバイス・プロビジョニングについて(2/2)
概要



アジェンダ

- 概要
- デバイス ID
- デバイス・プロビジョニングについて
- プロビジョニングなし
- 自動プロビジョニング
- カスタム・プロビジョニング

プロビジョニングなし (1/2)

- **プロビジョニングなし**は、開発環境として適切です。
- **プロビジョニングなし**を使用することは、プロビジョニング・プロセスが Worklight Server によってトリガー (要求) されないことを意味します。
- アプリケーションはデバイス ID を取得し、現状のまま Worklight Server に送信します。
- Worklight Server は、このデバイスが Worklight Server との通信を許可されているかどうかを検証しません。
- 証明書は、どの段階でも発行されず、要求もされません。
- **プロビジョニングなし**は、モバイル・アプリケーションのデフォルト設定です。
- デフォルトのセキュリティー設定を使用する場合、**プロビジョニングなし**を手動で有効にする必要はありません。

プロビジョニングなし (2/2)

- カスタム・セキュリティー・テストを使用してデバイス ID を必要とするリソースを保護し、**プロビジョニングなし**を使用する場合、セキュリティー・テストにレルムを追加します。例:

```
<customSecurityTest name="customTests">
    …
    <test realm="wl_anonymousUserRealm" isInternalUserID="true" />
    <test realm="wl_deviceNoProvisioningRealm" isInternalDeviceID="true" />
</customSecurityTest>
```

アジェンダ

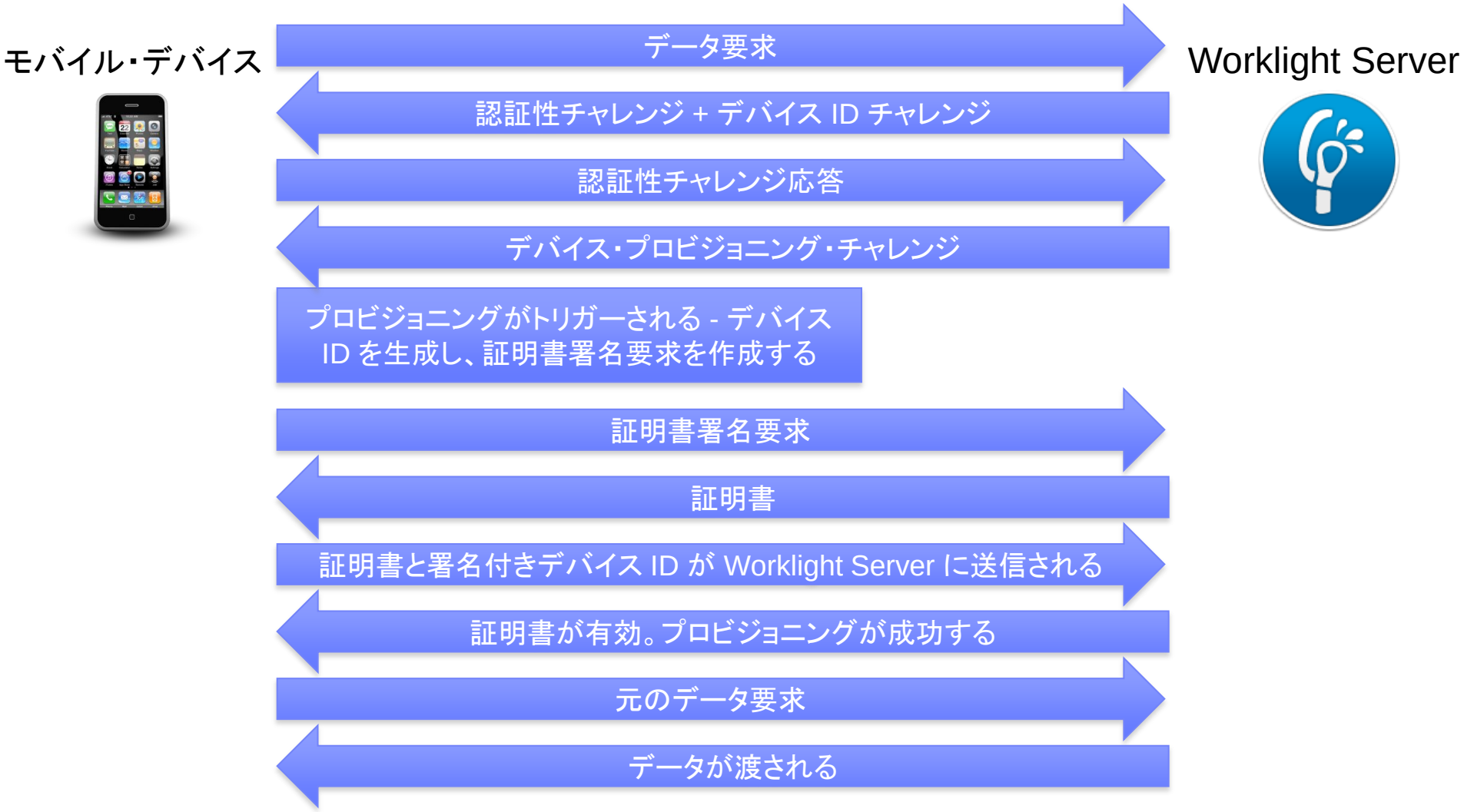
- 概要
- デバイス ID
- デバイス・プロビジョニングについて
- プロビジョニングなし
- 自動プロビジョニング
- カスタム・プロビジョニング

自動プロビジョニング (1/7)

- **自動プロビジョニング**は一回限りの自動プロセスであり、その間に Worklight Server によって証明書が発行され、クライアント・アプリケーションに送信されます。
- **自動プロビジョニング**は、プロビジョンされたデバイス ID を Worklight Server が要求したときにトリガーされます。
- アプリケーションはデバイス ID を取得し、自動プロビジョニング・プロセスを開始します。
- Worklight Server は提供されたデバイス情報を収集し、サーバー・サイドの CA 鍵ストアを使用して証明書を発行します。
- 証明書は、証明書を要求するすべてのデバイスに発行されます。したがって、**自動プロビジョニング**は、アプリケーションの認証性検査が成功した後に使用される場合にのみ意味があります。
- **自動プロビジョニング**のフローについては、これ以降のスライドを参照してください。

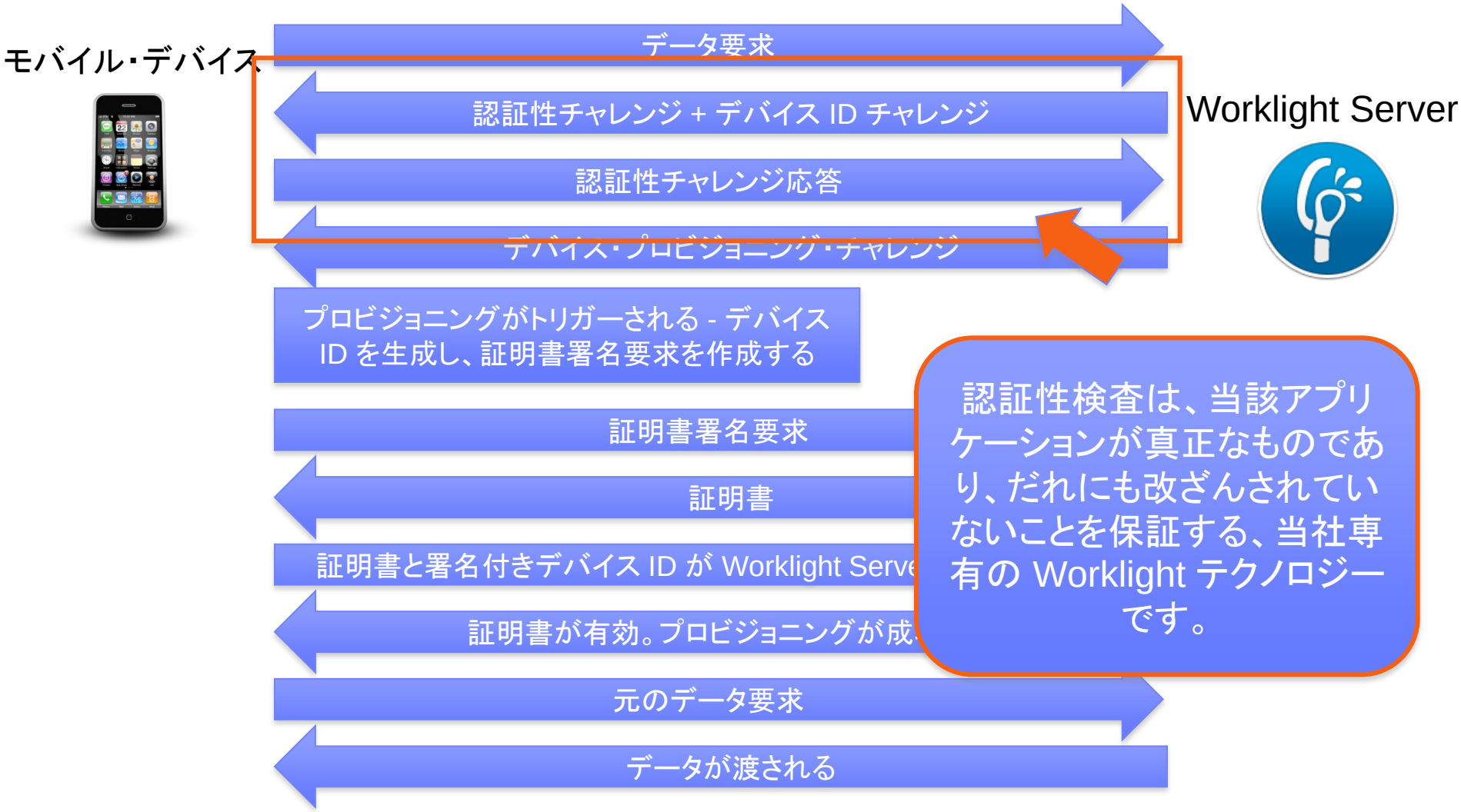
自動プロビジョニング (2/7)

- 初回のアプリケーション始動時の自動プロビジョニング



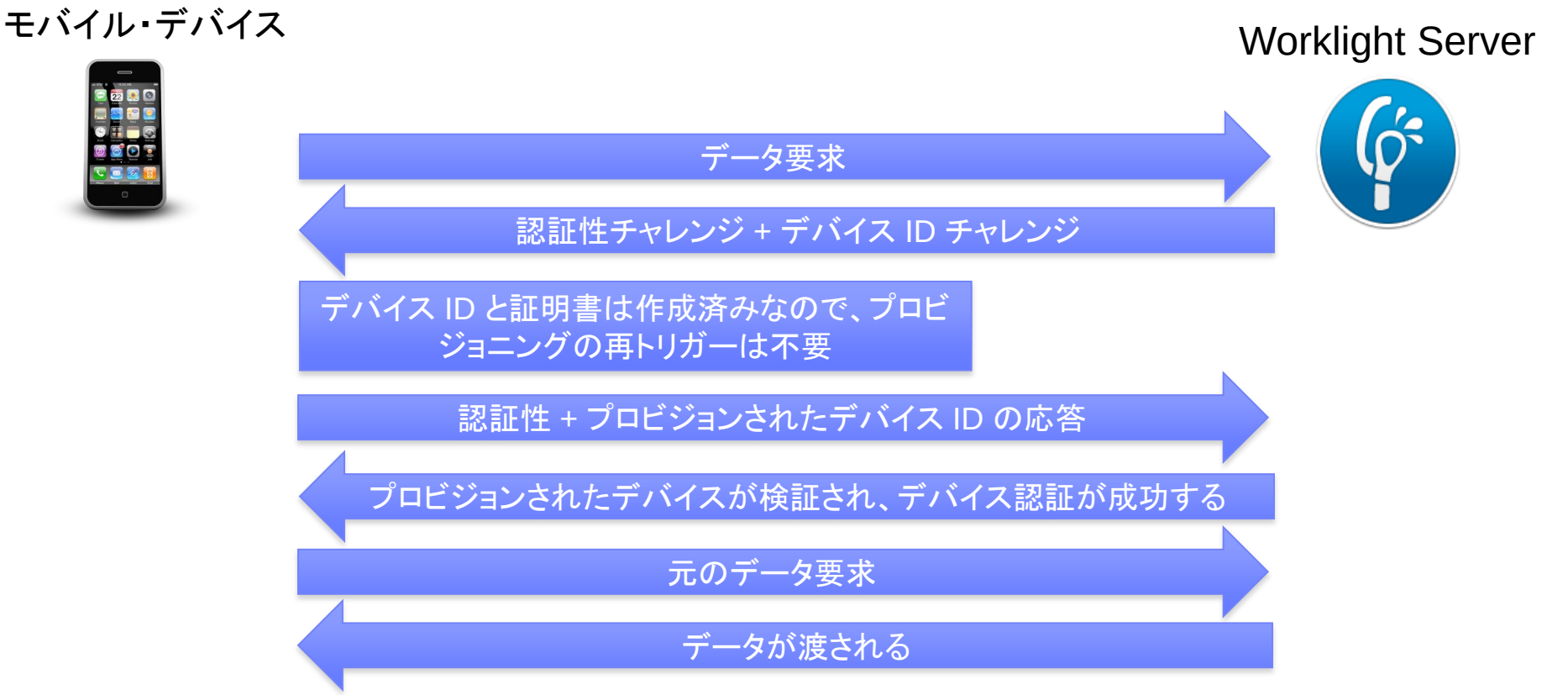
自動プロビジョニング (3/7)

- 初回のアプリケーション始動時の自動プロビジョニング



自動プロビジョニング (4/7)

- プロビジョン済みアプリケーションの 2 回目以降の始動



自動プロビジョニング (5/7)

- 自動プロビジョニングを使用可能にするにするために、以下のレルムを `authentication-config.xml` ファイルに追加します。
  - カスタム・セキュリティー・テストを使用する場合。

```
<customSecurityTest name="customTests">
    …
    <test realm="wl_authenticityRealm" />
    <test realm="wl_deviceAutoProvisioningRealm" isInternalDeviceID="true" />
</customSecurityTest>
```

  - モバイル・セキュリティー・テストを使用する場合。

```
<mobileSecurityTest name="mobileTests">
    …
    <testAppAuthenticity/>
    <testDeviceId provisioningType="auto" />
</mobileSecurityTest>
```

自動プロビジョニング (6/7)

- デフォルトでは、Worklight Server は、内部鍵ストアを使用して証明書を発行します。
- 独自の鍵ストアを使用するように Worklight Server に指示するには、`worklight.properties` ファイルを調整します。

```
##############################################################################################################################
#    Worklight Default Certificate (For device provisioning)
##############################################################################################################################
# You can change the default behavior with regard to CA certificates. You can also implement custom provisioning.
# If you want to change the auto-provisioning mechanism to use different granularity (application, device or group) or a
# different list of pre-required realms, you can create your own customized authenticator, login module and challenge handler.
# For more information, see the "Custom Authenticator and Login Module" Getting Started training module.

#The path to the keystore, relative to the server folder in the Worklight Project, for example: conf/my-cert.jks
#wl.ca.keystore.path=
#The type of the keystore file. Valid values are jks or pkcs12.
#wl.ca.keystore.type=
#The password to the keystore file.
#wl.ca.keystore.password=
#The alias of the entry where the private key and certificate are stored, in the keystore.
#wl.ca.key.alias=
#The password to the alias in the keystore.
#wl.ca.key.alias.password=

##############################################################################################################################
#    Worklight SSL keystore
##############################################################################################################################
#SSL certificate keystore location.
ssl.keystore.path=conf/default.keystore
#SSL certificate keystore type (jks or PKCS12)
ssl.keystore.type=jks
#SSL certificate keystore password.
ssl.keystore.password=worklight
```

- **注:** `wl.ca.keystore.path` プロパティーの値は、Worklight プロジェクトの `/server/` フォルダーに対する相対パスでも、あるいはファイル・システムに対する絶対パスでも構いません。

自動プロビジョニング (7/7)

- **自動プロビジョニング**は、アプリケーション認証性保護と併用する必要があります。
- 詳しくは、チュートリアルおよびサンプルの表 9 にある**「アプリケーション認証性保護」**トレーニング・モジュールおよび Worklight ユーザー文書を参照してください。

アジェンダ

- 概要
- デバイス ID
- デバイス・プロビジョニングについて
- プロビジョニングなし
- 自動プロビジョニング
- カスタム・プロビジョニング

カスタム・プロビジョニング

- **カスタム・プロビジョニング**は、**自動プロビジョニング**を拡張したものです。
- **カスタム・プロビジョニング**では、カスタム CSR と証明書検証機能を追加して、カスタム・デバイス・プロビジョニング・ルールを定義できます。
- 詳しくは、チュートリアルおよびサンプルの表 9 にある**「カスタム・プロビジョニング」**トレーニング・モジュールおよびユーザー文書を参照してください。

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