JAPAN SMARTPHONE SECURITY ASSOCIATION

セキュアコーディングガイド最新版のご紹介

JSSEC セキュアコーディングWG
福本 郁哉

Agenda

JAPAN SMARTPHONE SECURITY ASSOCIATION

- セキュアコーディングガイドの歩み
- 〃　第7版 (2016年9月1日版) の改訂内容
- 〃　第8版 (2017年2月1日版) の改定内容

セキュアコーディングガイドの歩み

2012年6月 初版公開

JAPAN SMARTPHONE SECURITY ASSOCIATION

Androidアプリセキュリティの教科書

Androidアプリセキュリティのノウハウ集
http://www.jssec.org/report/securecoding.html

- 通称 「**JSSECセキュアコーディンググガイド**」
- PDF文書とサンプルコード
- **無償**・商用利用可
- 利用ケースに応じた内容
  - 「Activityを作る・利用する」
  - 「HTTPS通信する」
  - etc.
- 通信キャリア、アプリベンダーで活用
- アプリ発注の際の受け入れ基準にするケースも

ガイドの歩み

JAPAN SMARTPHONE SECURITY ASSOCIATION

- 年1~2回のペースで改訂

2012年6月

2012年11月

2013年4月

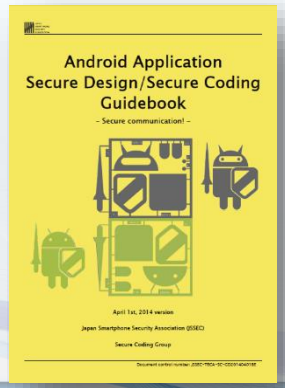
2014年7月

2015年6月

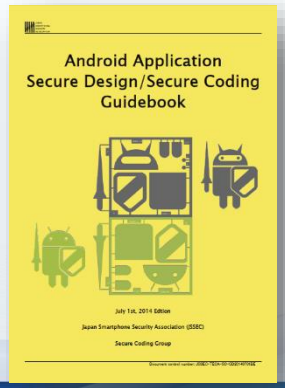
2016年2月

- 2014年 英語版リリース

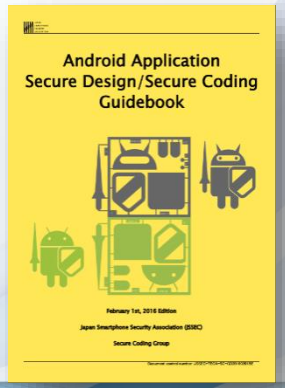
2014年4月



2014年7月



2016年2月



第7版 (2016年9月1日版)

第7版 (2016年9月1日版)

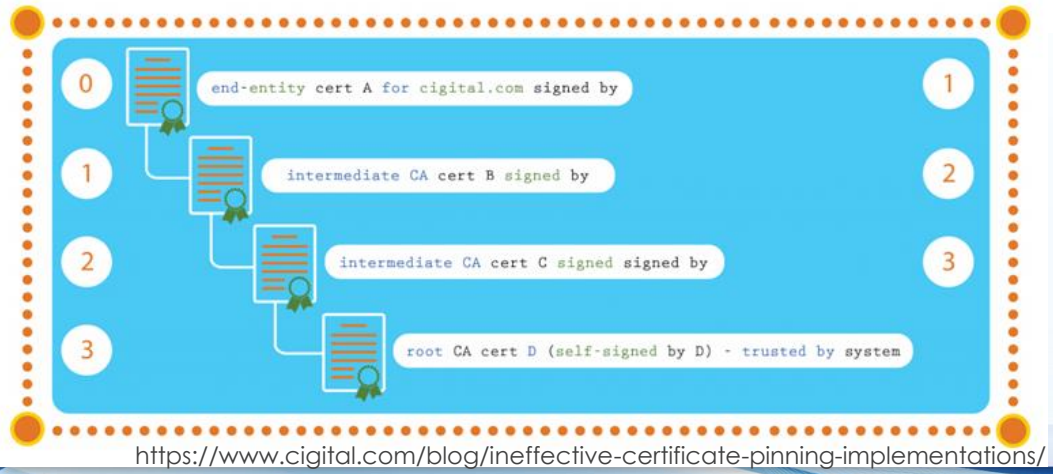
JAPAN SMARTPHONE SECURITY ASSOCIATION

前版（Android 6.x対応）で盛り込めなかった
脆弱性関係の記事、セキュリティアップデート情報
など

- **Pinning実装の注意点**
- **HTTPリクエストヘッダ設定時の注意点**
- etc.

Pinning実装時の注意点

証明書チェーンの検証



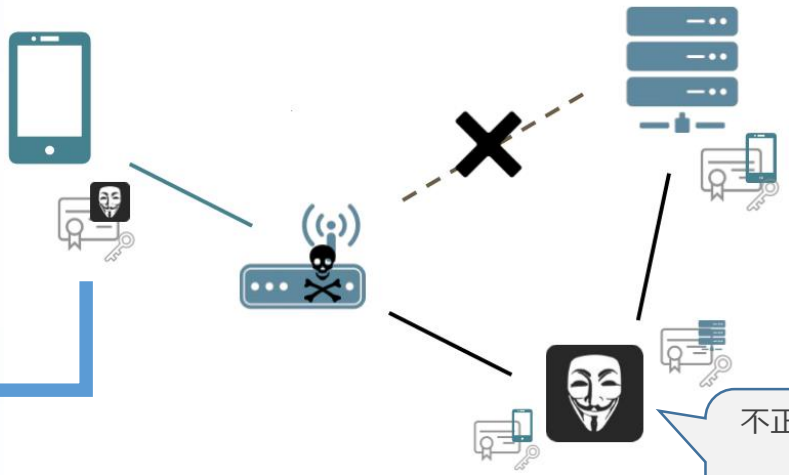
https://www.cigital.com/blog/ineffective-certificate-pinning-implementations/

不正なCA証明書を使った攻撃

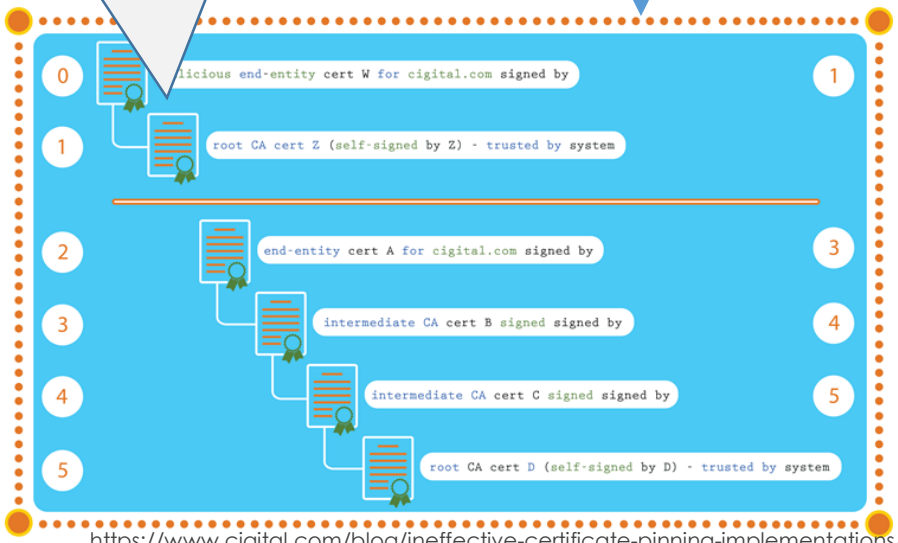
JAPAN SMARTPHONE SECURITY ASSOCIATION

クライアントでの検証は、
不正なCA証明書①で終了。

正しい証明書チェーンとみなされる



不正なCA証明書の作成
&
MITM
に成功した攻撃者



https://www.cigital.com/blog/ineffective-certificate-pinning-implementations/

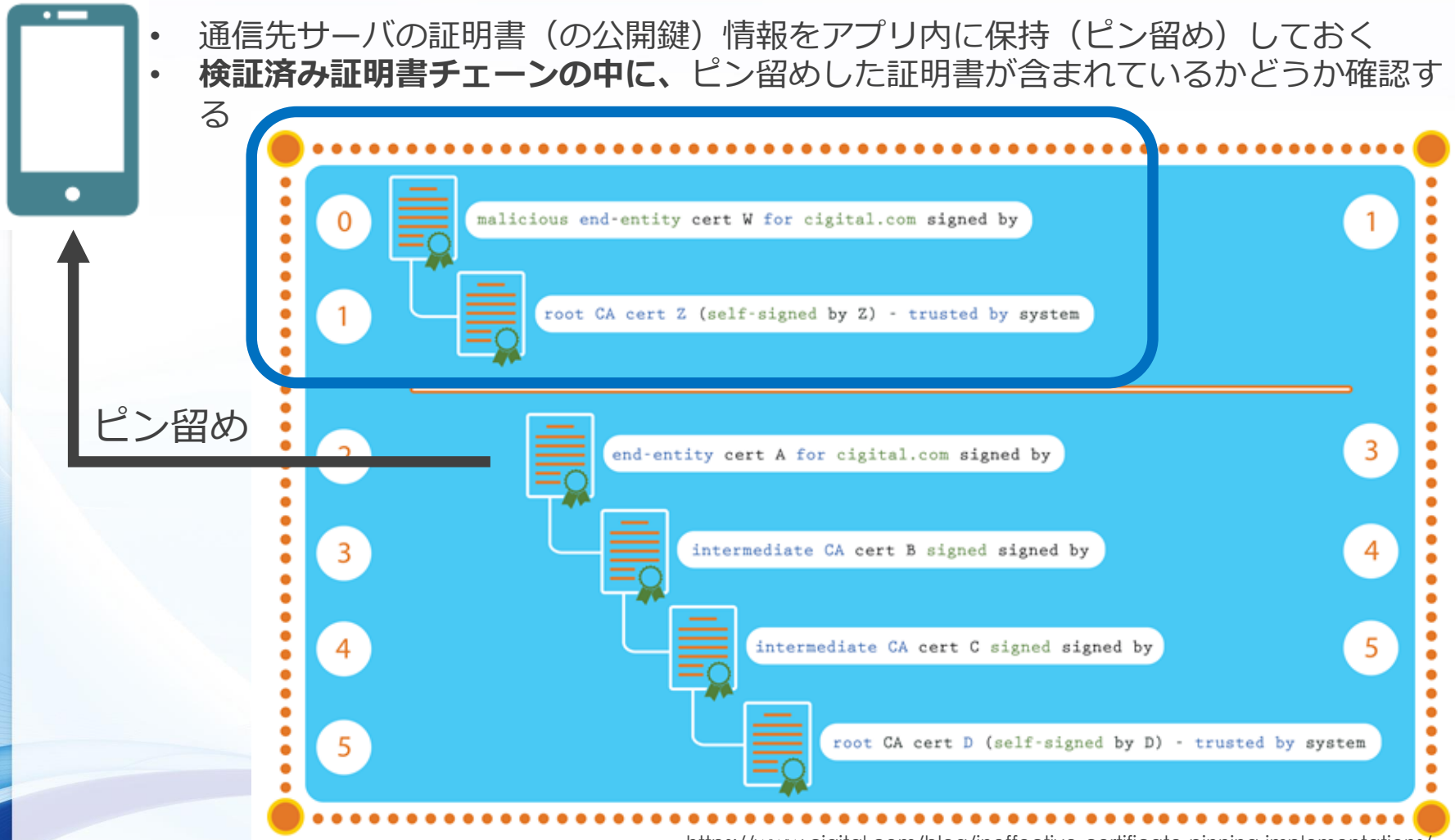
攻撃者が付け足した証明書チェーン
※ 不正なCA証明書を含む

本来の証明書チェーン
※ 正規のCA証明書を含む

Pinning検証

JAPAN SMARTPHONE SECURITY ASSOCIATION

- 通信先サーバの証明書（の公開鍵）情報をアプリ内に保持（ピン留め）しておく
- **検証済み証明書チェーンの中に、**ピン留めした証明書が含まれているかどうか確認する



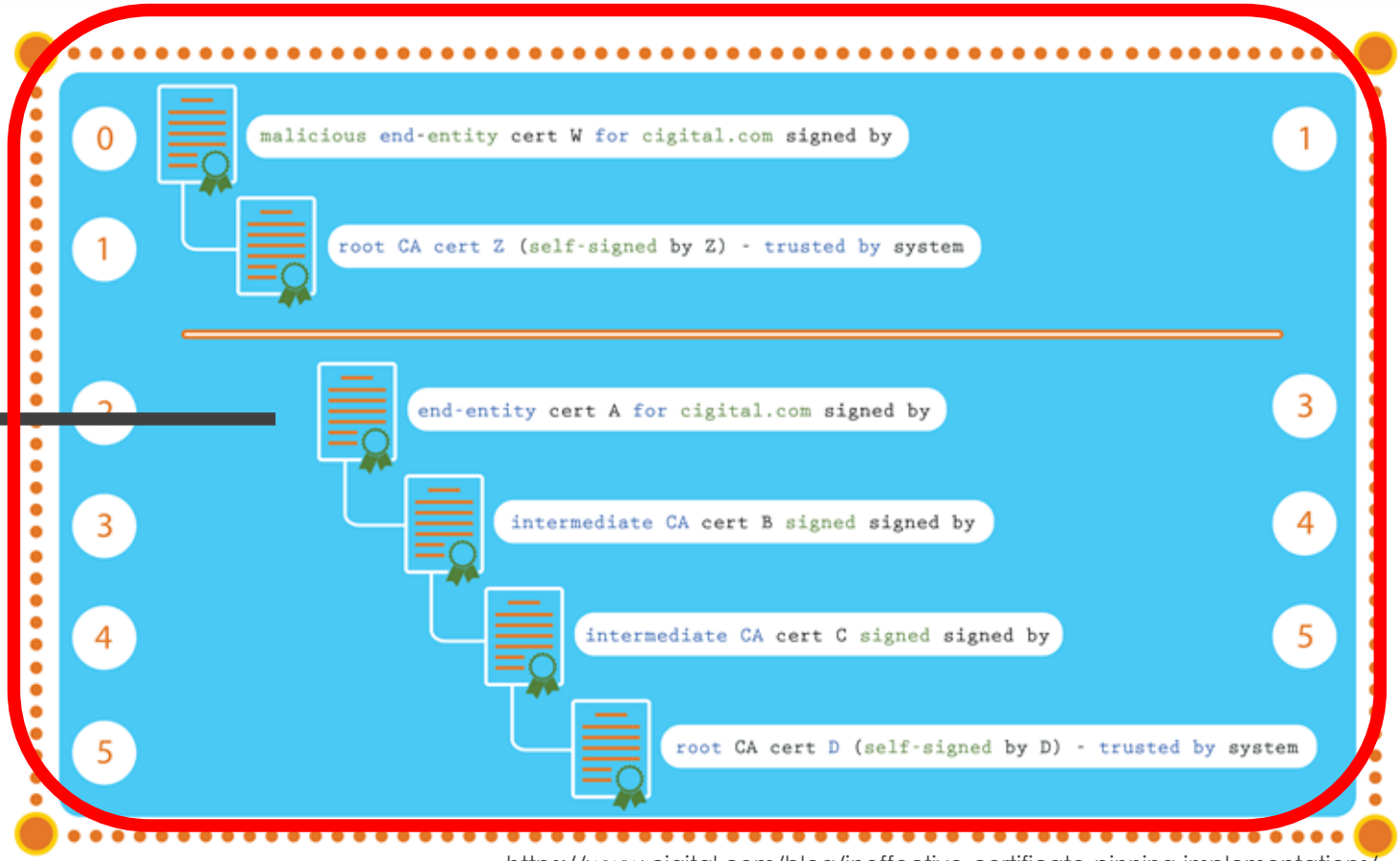
https://www.cigital.com/blog/ineffective-certificate-pinning-implementations/

Pinning検証の落とし穴

JAPAN SMARTPHONE SECURITY ASSOCIATION

- `javax.net.ssl.SSLSession.getPeerCertificates()`
- `javax.net.ssl.SSLSession.getPeerCertificateChain()`

ピン留め

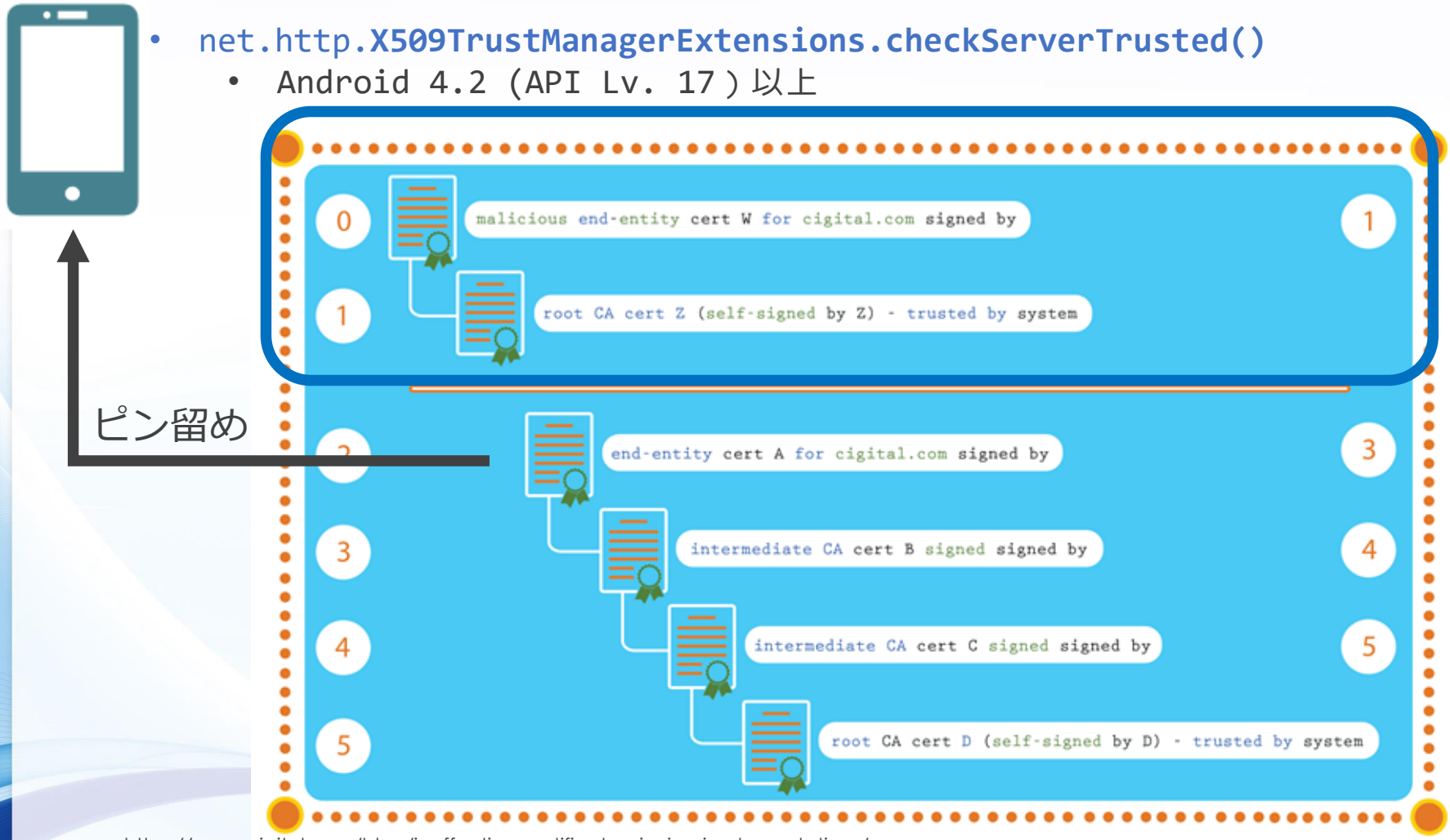


https://www.cigital.com/blog/ineffective-certificate-pinning-implementations/

Pinning検証の落とし穴を回避する

JAPAN SMARTPHONE SECURITY ASSOCIATION

- net.http.X509TrustManagerExtensions.checkServerTrusted()
  - Android 4.2 (API Lv. 17) 以上



https://www.cigital.com/blog/ineffective-certificate-pinning-implementations/

HTTPリクエストヘッダ設定時の注意点

HTTPリクエストヘッダ設定時の注意点

JAPAN SMARTPHONE SECURITY ASSOCIATION

- URLConnection クラスにHTTPヘッダインジェクションの脆弱性（Android 2.2 ～ 6.0）
  https://jvn.jp/vu/JVNVU99757346/index.html
  - OkHttp (< 2.5.0) に由来
- setRequestProperty()/addRequestProperty() を使用する際は、外部から受け取った値を使用する前に改行コードを排除する

```
// ★ポイント★ HTTP リクエストヘッダに入力値を使用する場合は、アプリケーション要件に従って
// 入力データをチェックする（「3.2 入力データの安全性を確認する」を参照）
if (strLanguage.matches("^[a-zA-Z ,-]+$")) {
    connection.addRequestProperty("Accept-Language", strLanguage);
} else {
    throw new IllegalArgumentException("Invalid Language : " + strLanguage);
}
```

その他の改訂ポイント

JAPAN SMARTPHONE SECURITY ASSOCIATION

- **Provider Installerの紹介**
  - Google Play開発者サービスの Security Provider が利用できる
  - Security Providerに脆弱性が見つかったとき、メーカー対応を待たずとも、Google Play Storeを通じて（比較的）迅速にアップデートされる
- **サンプルコードの修正＆削除**
  - 動かないサンプルアプリがありました
    - “WebView Assets”
    - 申し訳ありませんでした m(-_-)m
  - ガイドの内容と無関係なサンプルアプリがありました
    - “WebView Javascript Enable”
    - 実験のために作ったアプリでした
    - 実は第3版（日本語版）からあった
    - 誠に申し訳ありませんでした m(_ _)m

第8版 (2017年2月1日版)

明日公開

（冊子版は本日会場限定配布）

https://www.jssec.org/report/securecoding.html

第8版 (2017年2月1日版)

- **カバーデザイン刷新**
  - ４年ぶり２回目
- **Android 7.x 対応**
  - Network Security Configuration
  - 外部ストレージへのアクセスに関する仕様変更
    - Scoped Directory Access
    - MODE_WORLD_READABLE/WRITEABLE 使用不可
  - etc.

カバーデザイン刷新

カバーデザインが新しくなりました

初代

二代目

三代目

Android 7.x 対応
Network Security Configuration

Network Security Configuration

JAPAN SMARTPHONE SECURITY ASSOCIATION

- アプリのネットワーク通信に関するセキュリティ設定を **XML** で行うことができる
  - プライベート証明書の使用
  - Pinning検証
  - 非暗号化通信（HTTP）の抑制
  - デバッグ専用CA証明書の使用

- **追加コーディングの必要なし**
  - バグや脆弱性の作り込み防止に効果あり

Network Security Configuration
プライベート証明書の使用

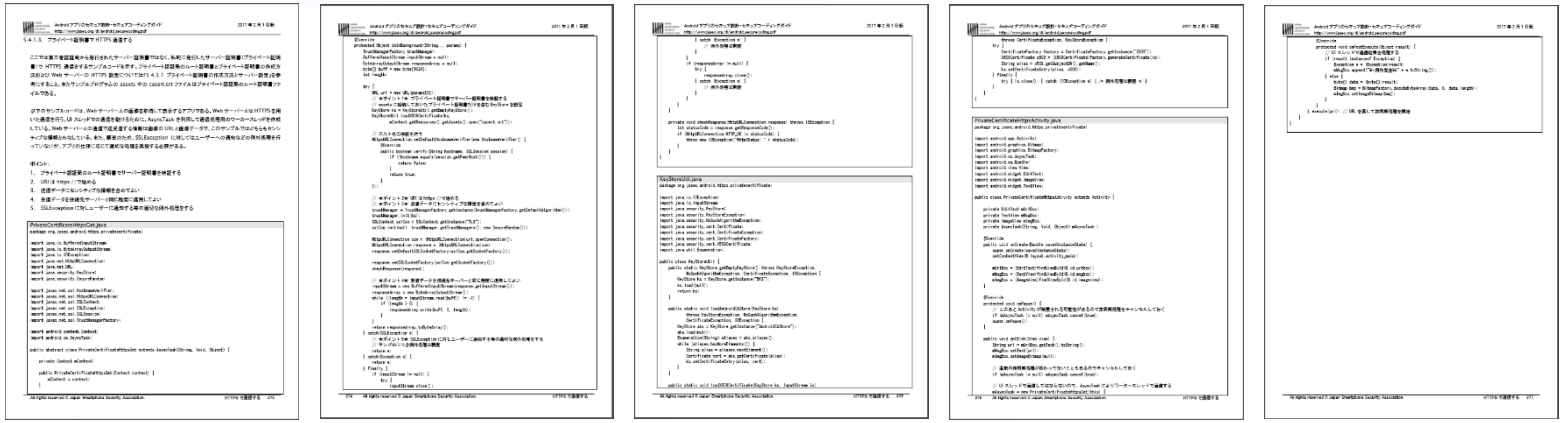
特定ドメインへの通信時にプライベート証明書を用いる

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config>
        <domain includeSubdomains="true">jssec.org</domain>
        <trust-anchors>
            <certificates src="@raw/private_ca" />
        </trust-anchors>
    </domain-config>
</network-security-config>
```

通信先ドメイン

プライベート証明書のパス

Network Security Configuration
プライベート証明書の使用



特定ドメインへの通信時にプライベート証明書を用いる

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config>
        <domain includeSubdomains="true">jssec.org</domain>
        <trust-anchors>
            <certificates src="@raw/private_ca" />
        </trust-anchors>
    </domain-config>
</network-security-config>
```

Network Security Configuration
プライベート証明書の使用

JAPAN SMARTPHONE SECURITY ASSOCIATION

アプリが行う全ての HTTPS 通信時にプライベート証明書を用いる

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config>
        <trust-anchors>
            <certificates src="@raw/private_ca" />
        </trust-anchors>
    base-config>
    rk-security-config>
```

<domain-config>：特定ドメインへのHTTPS通信

↓

<base-config>：全てのHTTPS通信

Network Security Configuration
Pinning検証

JAPAN SMARTPHONE SECURITY ASSOCIATION

通信先ドメイン

HTTPS 通信時にピンニングによる検証を行う

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config>
        <domain includeSubdomains="true">jssec.org</domain>
        <pin-set expiration="2018-12-31">
            <pin digest="SHA-256">e30Lky+iWK21yHSIs5DJoRzNikOdvQUOGXvurPidc2E=</pin>
            <!-- バックアップ用 -->
            <pin digest="SHA-256">fwza0LRMXouZHRC8Ei+4PyuldPDcf3UKgO/04cDM1oE=</pin>
        </pin-set>
    </domain-config>
</network-security-config>
```

通信先サーバの公開鍵ハッシュ

Network Security Configuration
非暗号化（HTTP)通信の抑制

非暗号化通信を許可しない

非暗号化通信を抑制する

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config cleartextTrafficPermitted="false">
        <domain includeSubdomains="true">jssec.org</domain>
    </domain-config>
</network-security-config>
```

- ✓ 抑制対象は HTTP, FTP, DownloadManager, MediaPlayer 等
  - ✓ 低レイヤーの、トラフィックの内容が暗号化されているかどうか判別が難しい通信では「best effort」で実施される
- ✓ **WebView には適用されない**

Network Security Configuration
デバッグ専用CA証明書

JAPAN SMARTPHONE SECURITY ASSOCIATION

デバッグ時にのみプライベート証明書を用いる

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <debug-overrides>
        <trust-anchors>
            <certificates src="@raw/private_cas" />
        </trust-anchors>
    </debug-overrides>
</network-security-config>
```

- ✓ android:debuggable が true のとき（デバッグビルドのとき）のみ、プライベートCA証明書を使用する
- ✓ 非リリースビルドは Play Store に載らない
- ✓ **デバッグ目的のためにサーバ証明書検証をバイパスさせてしまう、危険な実装をしなくても済む**

Android 7.x 対応
外部ストレージへのアクセスに関する仕様変更

MODE_WORLD_READABLE/WRITEABLE

- MODE_WORLD_READABLE / MODE_WORLD_WRITEABLE
- Android 4.2 (API Lv. 17) ～ 非推奨
- **Android 7.0 (API Lv. 24) ～ 使用不可**
  - セキュリティ例外がスローされる

SDNA「Androidアプリ脆弱性調査レポート 2015」

Scoped Directory Access

JAPAN SMARTPHONE SECURITY ASSOCIATION

- 外部ストレージの特定ディレクトリに対し、**Permissionなしに**アクセスできる

DIRECTORY_MUSIC	音楽ファイル
DIRECTORY_PODCASTS	ポッドキャスト
DIRECTORY_RINGTONES	着信音
DIRECTORY_ALARMS	アラーム音
DIRECTORY_NOTIFICATIONS	通知音
DIRECTORY_PICTURES	画像ファイル
DIRECTORY_MOVIES	動画ファイル
DIRECTORY_DOWNLOADS	ユーザーがダウンロードしたファイル
DIRECTORY_DCIM	カメラによる画像・動画ファイル
DIRECTORY_DOCUMENTS	ユーザーによって作られたドキュメント

外部ストレージへのアクセス問題

Android 7.0 未満では……

外部ストレージの特定ディレクトリ（e.g. “Pictures”）に写真アプリなどがアクセスする際、以下のような問題があった

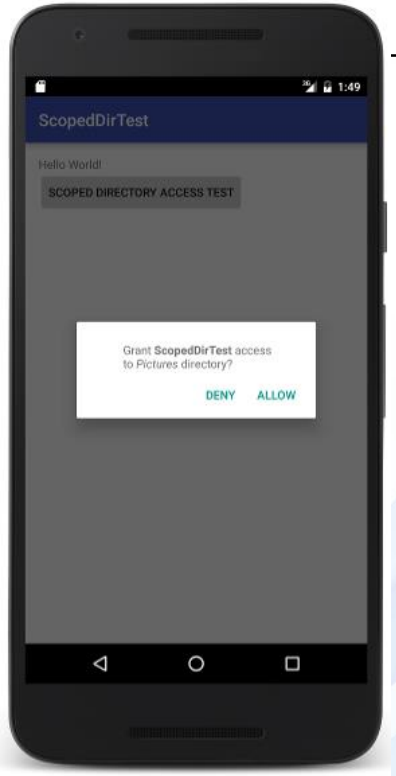
- READ/WRITE_EXTERNAL_STORAGE
  → 外部ストレージの全ての公開ディレクトリにアクセスできてしまう
- Storage Access Framework
  → 常に同じディレクトリにアクセスするアプリであっても、システムUIでユーザーにディレクトリを選択させる必要がある

Scoped Directory Access

JAPAN SMARTPHONE SECURITY ASSOCIATION

```
StorageManager sm =
        (StorageManager)getSystemService(Context.STORAGE_SERVICE);
StorageVolume volume = sm.getPrimaryStorageVolume();
Intent intent = volume.createAccessIntent(Environment.DIRECTORY_PICTURES);
startActivityForResult(intent, request_code);
```

DIRECTORY_MUSIC	音楽ファイル
DIRECTORY_PODCASTS	ポッドキャスト
DIRECTORY_RINGTONES	着信音
DIRECTORY_ALARMS	アラーム音
DIRECTORY_NOTIFICATIONS	通知音
DIRECTORY_PICTURES	画像ファイル
DIRECTORY_MOVIES	動画ファイル
DIRECTORY_DOWNLOADS	ユーザーがダウンロードしたファイル
DIRECTORY_DCIM	カメラによる画像・動画ファイル
DIRECTORY_DOCUMENTS	ユーザーによって作られたドキュメント



その他の改訂ポイント

- Android 2.x, 3.x についての記述を整理
- intent-filter定義の有無とコンポーネントの公開設定について解説
  - Activity, Receiver, Serviceについて、exported無指定の場合、デフォルトの挙動は…
    <intent-filter> あり → 公開扱い
    <intent-filter> なし → 非公開扱い
  - ガイドでは
    「intent-filterの有無によらず、exportedは明示的に指定すべし」としている
- Sticky Broadcastについて追記
  - 不特定多数のアプリからアクセスできてしまう
    - なので、センシティブな情報は送信しないように
  - Android 5.0 (API Lv. 15)で非推奨

おねがい

執筆へのご協力をお願いします

JAPAN SMARTPHONE SECURITY ASSOCIATION

ご協力いただける方は下記の要領でご連絡ください

1. **JSSEC会員でない方はAndroidセキュリティ部へご参加ください**
   - 会員かどうかは下記URLで確認
     - http://www.jssec.org/members/
   - Androidセキュリティ部への参加は下記URLからできます
     - https://groups.google.com/group/android-security-japan

2. **下記までご連絡下さい**
   - JSSEC技術部会副部会長 奥山謙
     Ken.Okuyama@sony.com

ご協力お願い致します