コード署名用証明書　事始め

2016.5.26　NII　オープンフォーラム

国立情報学研究所　坂根栄作

お品書き

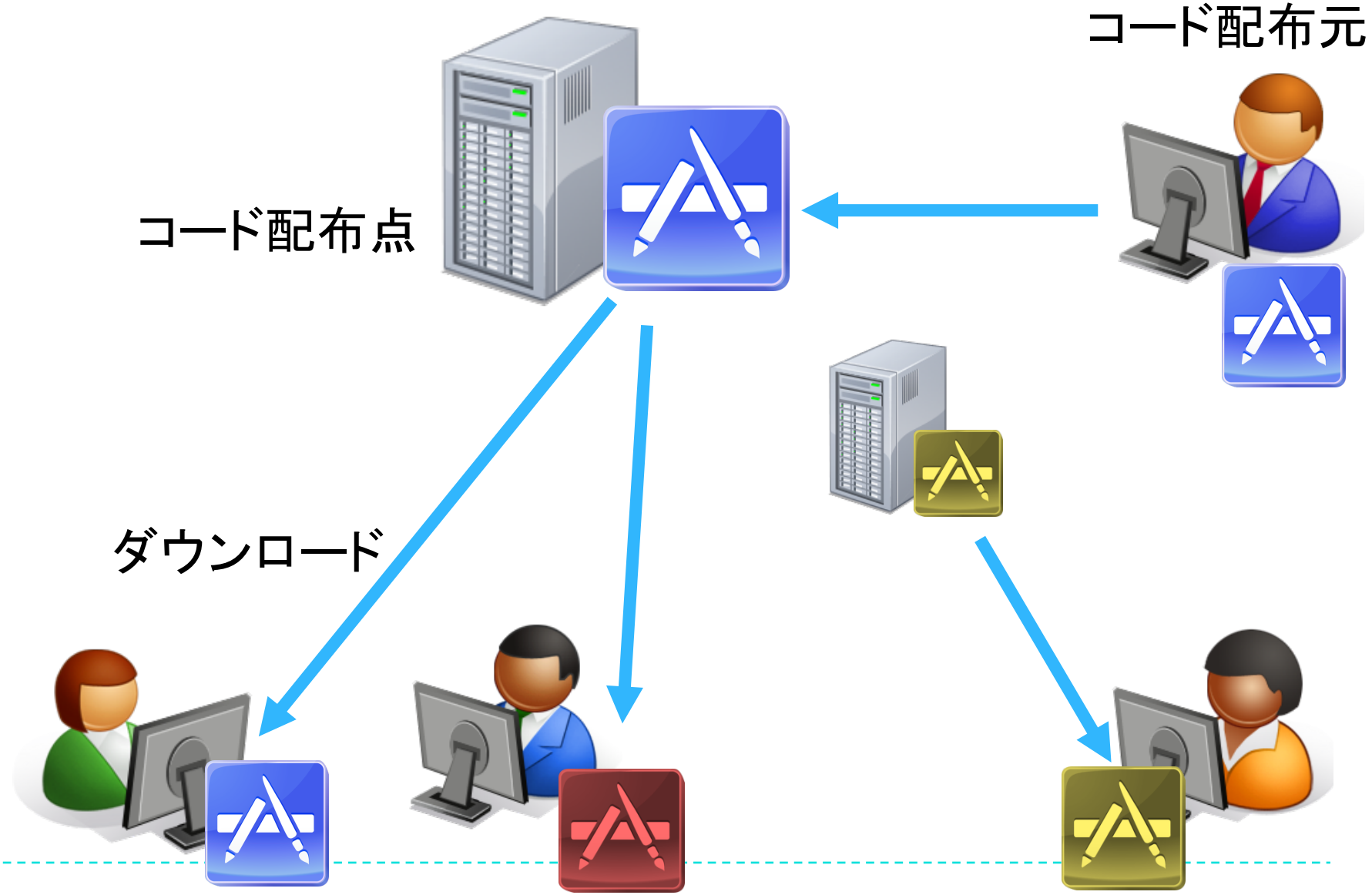
- コード署名とは？
- コード署名用証明書とは？
- コードとは？
- コード署名いろいろ
- コード署名のこれから

コード署名とは？

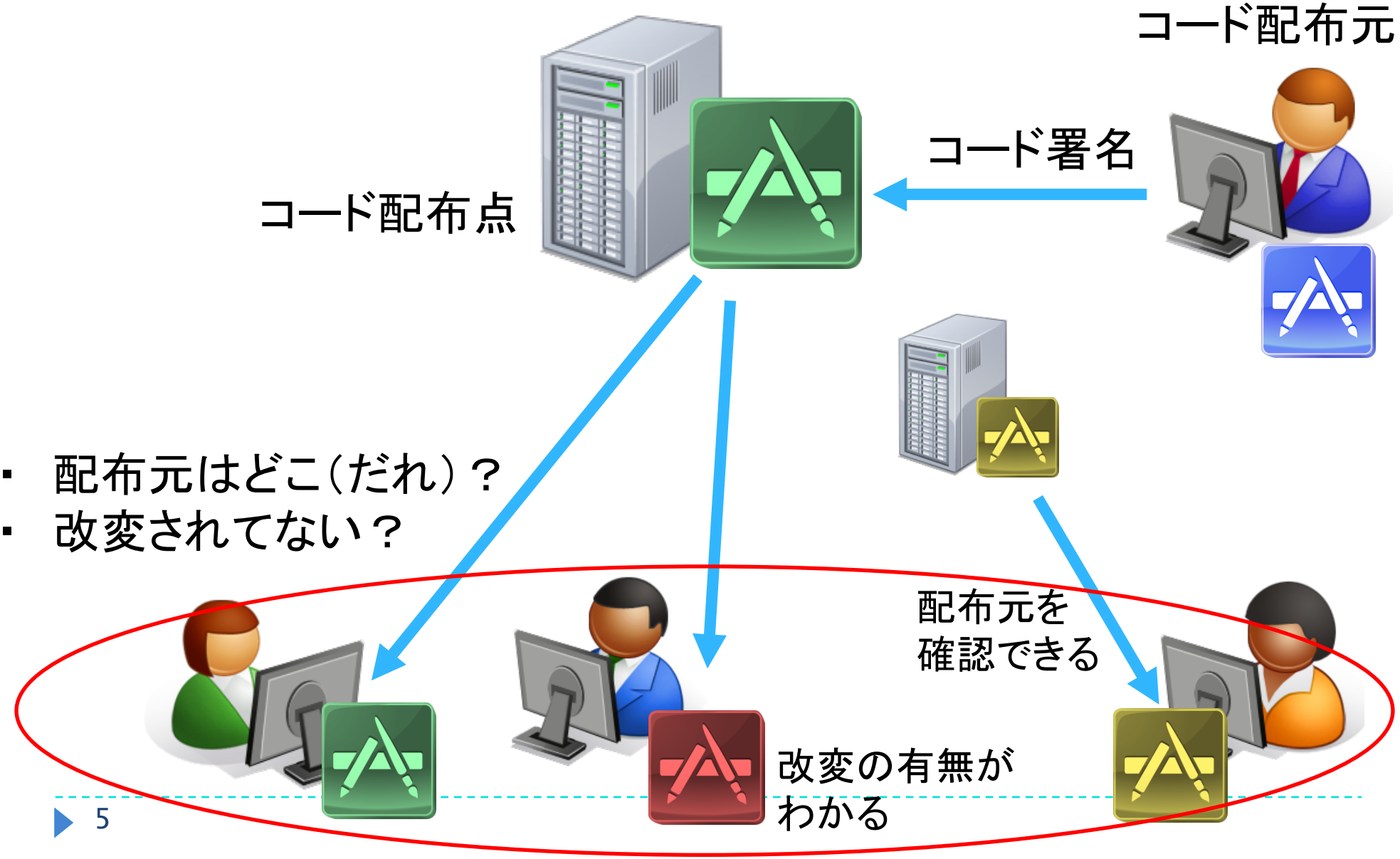
- RFC 5280 PKIX Certificate and CRL Profile
  - 4.2.1.12. Extended Key Usage
    id-kp-codeSigning
    -- Signing of downloadable executable code
- ダウンロード可能で実行可能なコードに電子署名すること

- コード署名の目的
  - 証明書保持者の同一性の確認
  - コードの完全性の確認
- だれが配布してるもので、それが改変されてないことを確認すること

コード署名が活きるのは？



コード署名が活きるのは？（続き）



- 配布元はどこ（だれ）？
- 改変されてない？

コード署名用証明書とは？ ～UPKI クライアント証明書との比較

コード署名用

- 用途
  - コードへの電子署名
- 識別名
  - O :機関名（英語表記）
  - CN = O
- 有効期間
  - 25ヶ月以内
- 拡張された鍵用途
  - codeSigning
- 公開鍵暗号
  - RSA 2048

クライアント

- 用途
  - クライアント認証
  - データへの電子署名
- 識別名
  - O :機関名（英語表記）
  - CN :利用者氏名／識別子
- 有効期間
  - 25ヶ月以内
- 拡張された鍵用途
  - clientAuth
- 公開鍵暗号
  - RSA 2048

UPKI コード署名用証明書の特徴 ～流通しているものとの比較

- 識別名の CN が機関名に一致
  - 法人向け。一般に流通しているものは個人向けもあり。
  - ある意味 EV コード署名用証明書プロファイルに類似。
- 有効期間は25ヶ月以内
  - ３年のものもあり。
- 現在の UPKI サービスではタイムスタンプを利用できない。。。
  - コード署名に用いた証明書の有効期限を過ぎると、結果的にコード署名の検証に失敗する。
  - コードの更新周期が長いものには向かない。
  - （コード更新周期）＜（コード署名用証明書有効期間）
    - 例えば、四半期ごとの定期的なコード更新・公開

署名対象のコードは？

- 基本的に何でもあり。

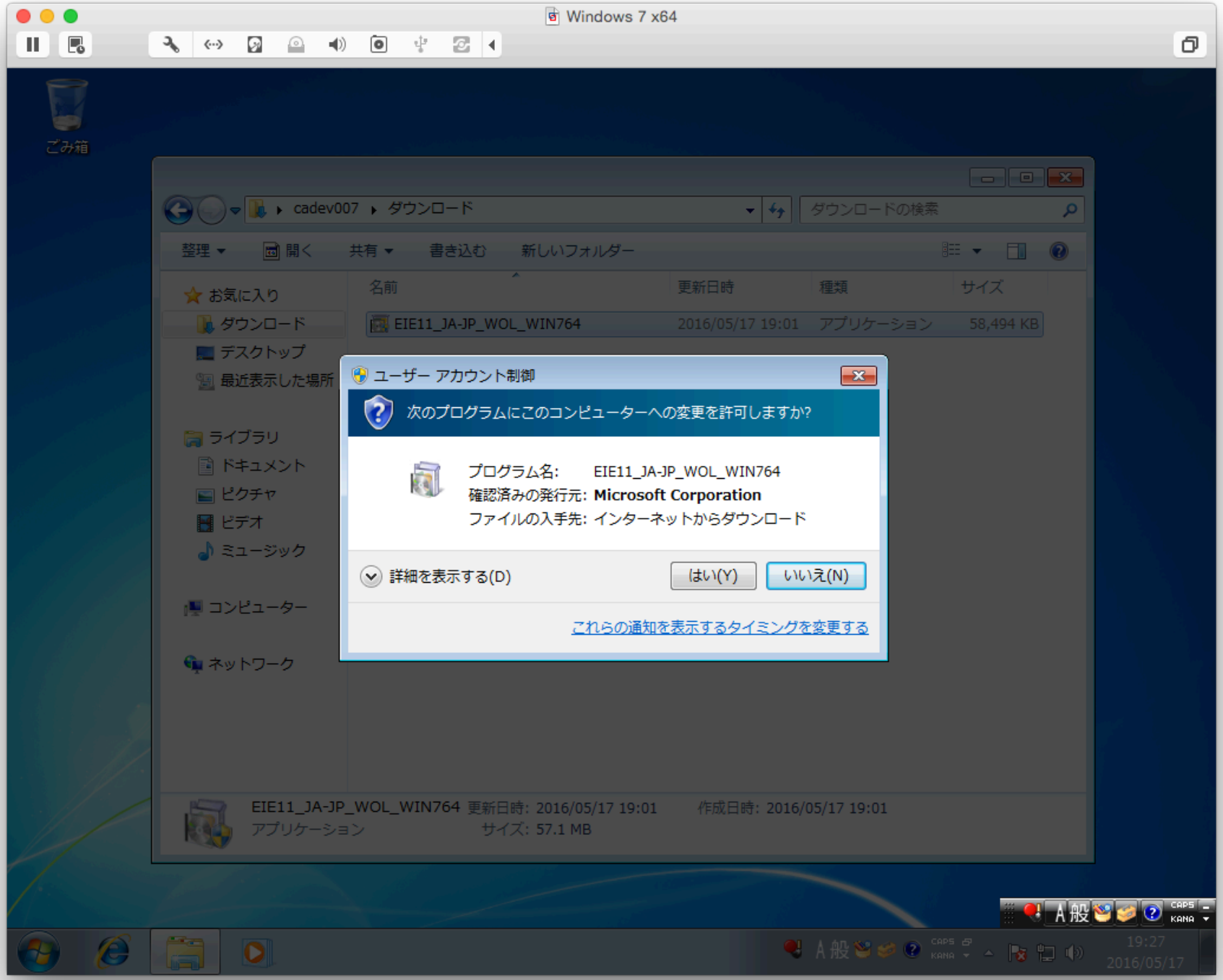
- コードへの署名
  - 対象コードのダイジェスト（ハッシュ値）を計算し、
  - 証明書と対をなす秘密鍵でダイジェストを暗号化する。
- コード署名の検証
  - コード署名用証明書を検証し、
  - 証明書（公開鍵）で、署名（暗号化されたダイジェスト）を復号化し、
  - 対象コードのダイジェストを計算し、
  - 復号化したダイジェストと直接計算したダイジェストの一致を確認する。
- ある意味、コード署名の検証の敷居が高い。。。
  - 配布先である利用者全員が容易に検証できること、が重要。

コード署名検証の簡便性

- コード署名用証明書の検証のし易さ
  - ルート証明書は既に実行環境にある…？
  - パブリックドメインの証明書を利用すれば OK, UPKI !!
    - 中間認証局証明書の取り扱い
- 復号化・ダイジェスト計算・比較のし易さ
  - 実行環境・プラットフォーム依存
  - パッケージ化（対象コード＋署名＋証明書）
  - ダウンロード時の検証・警告
  - 実行時の検証・警告

コード署名～導入の勘所

- 対象コードの用途
  - 何をするもの？　利用者はだれ？　実行環境は？
- 対象コードの配布形態
  - オンライン入手／ダウンロード可能
- コード署名の必要性
  - 配布元を担保する
  - 改変の有無を確認する
- 想定利用者および実行環境
  - コード署名検証の簡便性
  - 利用者への啓蒙のやり易さ
- コードの開発ライフサイクル
  - タイムスタンプ


Windows 7 x64
ごみ箱
cadev007 ▸ ダウンロード
ダウンロードの検索
整理
開く
共有
書き込む
新しいフォルダー
お気に入り
ダウンロード
デスクトップ
最近表示した場所
ライブラリ
ドキュメント
ピクチャ
ビデオ
ミュージック
コンピューター
ネットワーク
名前
更新日時
種類
サイズ
EIE11_JA-JP_WOL_WIN764
2016/05/17 19:01
アプリケーション
58,494 KB
ユーザー アカウント制御
次のプログラムにこのコンピューターへの変更を許可しますか?
プログラム名: EIE11_JA-JP_WOL_WIN764
確認済みの発行元: Microsoft Corporation
ファイルの入手先: インターネットからダウンロード
詳細を表示する(D)
はい(Y)
いいえ(N)
これらの通知を表示するタイミングを変更する
EIE11_JA-JP_WOL_WIN764 更新日時: 2016/05/17 19:01 作成日時: 2016/05/17 19:01
アプリケーション サイズ: 57.1 MB
19:27
2016/05/17

利用マニュアル（UPKI 提供）

- Adobe AIR (82)
- Android APK (157)
- Java JAR (97)
- OS X Application bundle (74)
- Microsoft Silverlight (91)
- Windows PowerShell (71)
- Windows デバイスドライバ (.exe, .cab, .dll) (154)

UPKI コード署名用証明書の入手手順

- 事前準備（開発環境、ツール）
- 鍵ペア生成、CSR生成
  - RSA 2048 bits
  - Subject DN に注意
- コード署名用証明書発行申請 TSV ファイル生成、登録担当者への申請・送付

- 証明書取得 URL の入手（メール）
- 取得 URL からダウンロード

Subject DN

識別名	要／不要	値および注意点
Country (C)	必須	JP
STate or province (ST)	使用しない	
Locality (L)	必須	Academe
Organization (O)	必須	機関名（英語表記）
Organization Unit (OU)	任意（省略可）	
Common Name (CN)	必須	機関名（英語表記）
Email	使用しない	

利用マニュアル（UPKI 提供）再掲

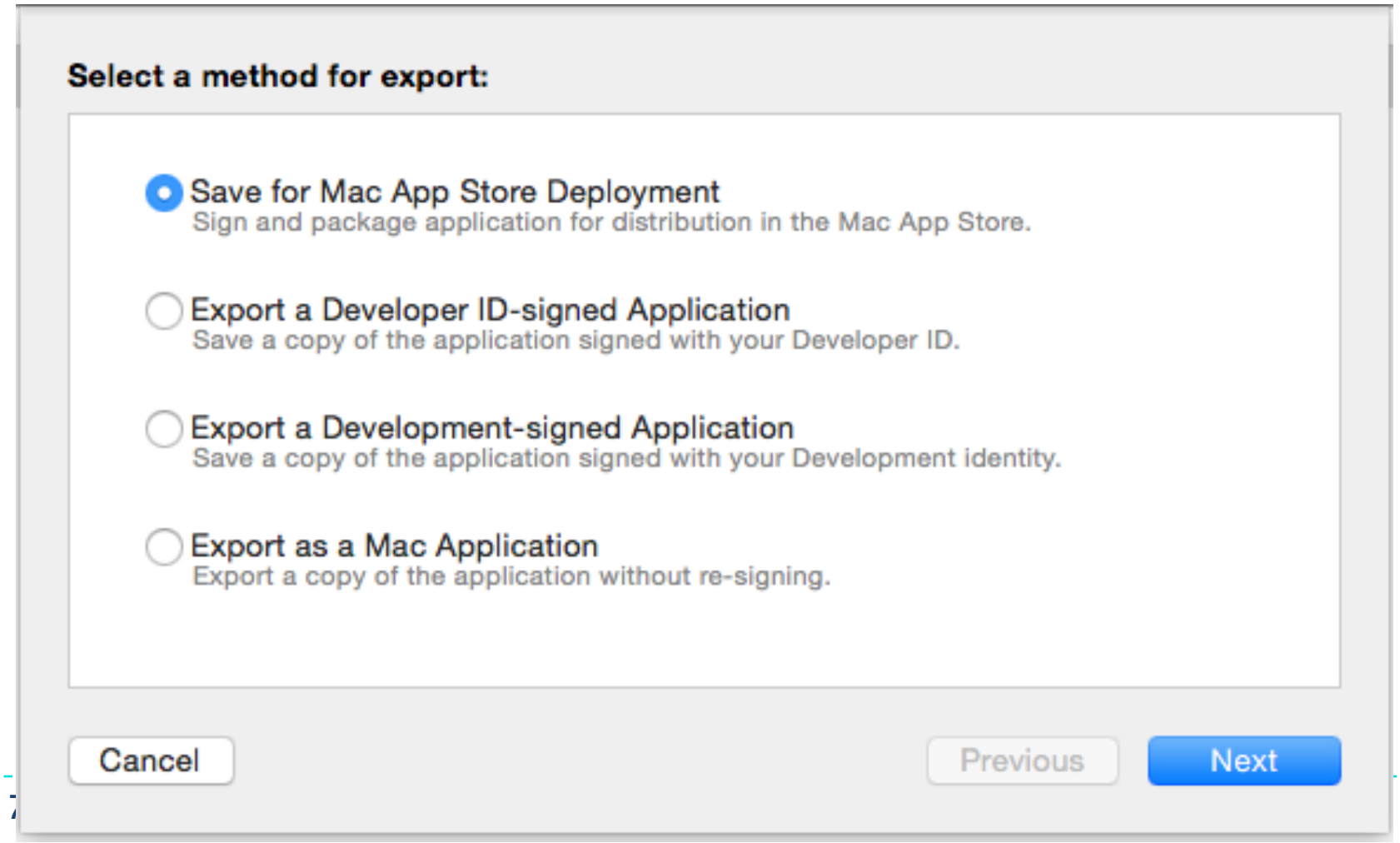
- Adobe AIR (82)
- Android APK (157)
- Java JAR (97)
- OS X App. bundle (74)
- Microsoft Silverlight (91)
- Windows PowerShell (71)
- Windows 実行ファイル汎用 (.exe, .cab, .dll) (154)

Windows

- Microsoft Authenticode
  - Windows 汎用実行ファイルに対するコード認証技術
- Microsoft Smartscreen
  - フィッシング詐欺対策
  - アプリケーション評価
  - マルウェア対策
  - 一定の評価を得ていないコードはブロックされる
- Smartscreen に対応するには
  - 一定の評価を得る
  - EV コード署名用証明書を利用する
  - Windows ストア経由で配布する
- カーネルモードドライバ (Windows 10)
  - ハードウェアデベロッパーセンターダッシュボードによる署名が必要
  - ダッシュボードには、EV 証明書が必要

OS X

- OS Application Bundle
  - Apple へのデベロッパ登録が必要



OS X（続き）

- 署名なしのアプリケーション


セキュリティとプライバシー
検索
一般
FileVault
ファイアウォール
プライバシー
このユーザのログインパスワードが設定されています
パスワードを変更...
スリープとスクリーンセーバの解除にパスワードを要求　開始後：
5 分後に
画面がロックされているときにメッセージを表示
ロックのメッセージを設定...
自動ログインを使用不可にする
ダウンロードしたアプリケーションの実行許可：
Mac App Store からのアプリケーションのみを許可
Mac App Store と確認済みの開発元からのアプリケーションを許可
すべてのアプリケーションを許可
“GIMP”は開発元を確認できないため、開けませんでした。
このまま開く
変更できないようにするにはカギをクリックします。
詳細...
?

コード署名のこれから…

- Extended Validation コード署名用証明書
  - SSL/TLS EV 証明書の EV
  - 法人向け、厳格な申請手続き、運用管理
    - CA/Browser Forum のガイドライン
    - Guidelines For The Issuance And Management Of Extended Validation Certificates (v1.5.9, March 18, 2016)
    - Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates (v1.3, Sept. 16, 2014)
  - UPKI でのサポートは未定
- タイムスタンプ
  - 中長期的に変化しないコード
  - 次期 UPKI システム仕様で検討

- 複数の実行環境での検証、マニュアルの充実

まとめ

- コード署名の目的は
  - 配布元の同一性の確認
  - コードの完全性の確認
- UPKI コード署名用証明書の特徴
- コード署名導入の勘所
  - コード署名検証のやり易さ
  - 利用者への啓蒙のやり易さ
- コード署名いろいろ
- 今後の課題

- 共に考え共に創る学術情報基盤を！
- UPKI はコード署名に注力していきます！

NAREGI-CA

An Open Source Software Package Enabling You To Build A PKI

https://ca-dev.naregi.org

NAREGI-CA は UPKI を応援しています！

勝手に