

---

# ICチップによる本人確認

---



OSSTech

Open Source Solution Technology Corporation

HAMANO Tsukasa <hamano@osstech.co.jp>

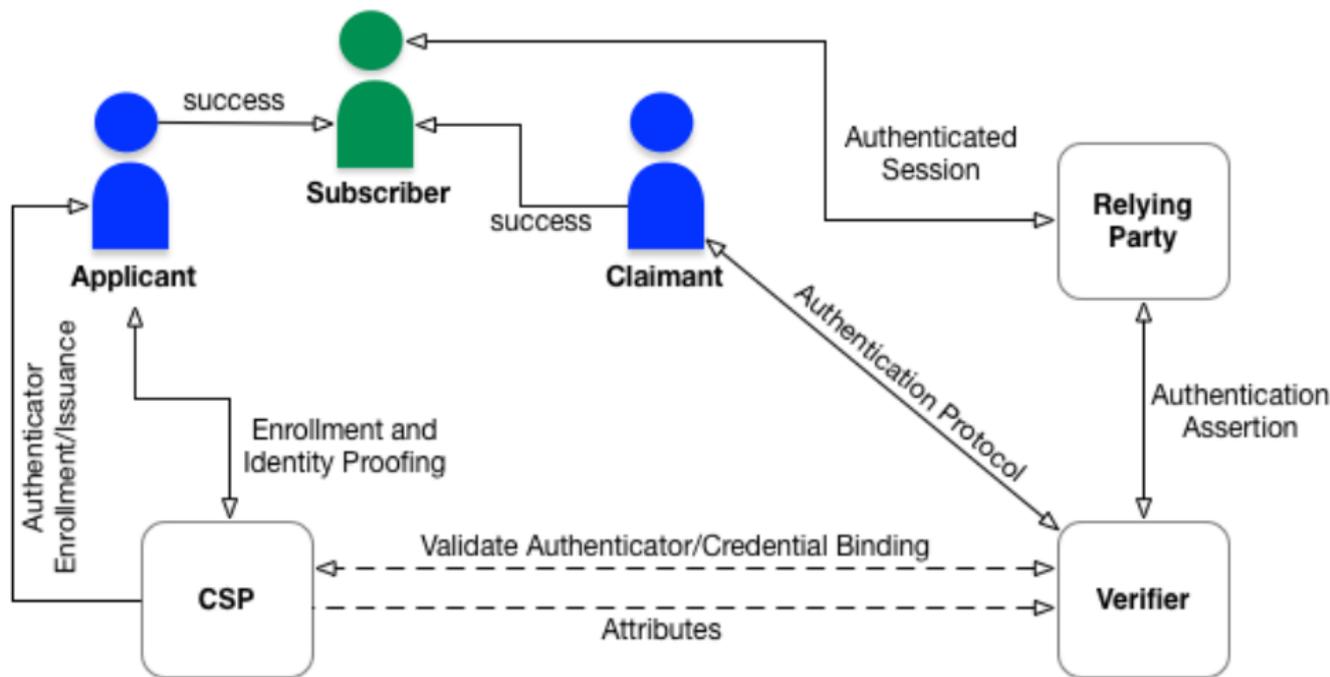
サルオフ#1

# 目次

- 運転免許証編
- パスポート編
- 在留カード編
- マイナンバーカード編
- NFC仕様

# NIST SP800-63

*Enrollment, Authenticator,  
and Lifecycle Maintenance*



# 本人確認書類

- 運転免許証
  - 発行者: 都道府県公安委員会
  - 発行数: 8200 万枚
- パスポート
  - 発行者: 外務省
  - 発行数: 3000 万枚
- マイナンバーカード
  - 発行者: 市区町村長
  - 発行数: 1600 万枚

※ 2019 年時点

# 55億円事件

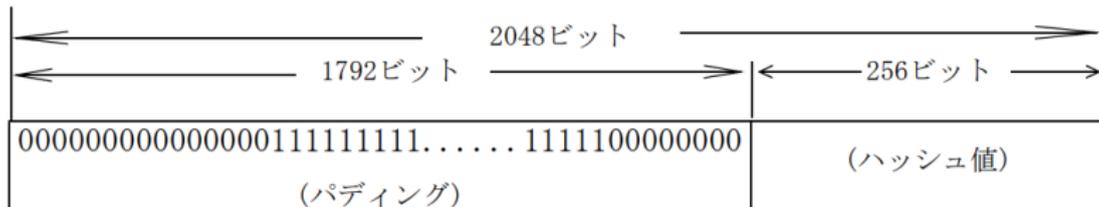


# 運転免許証仕様

## (2) 電子署名アルゴリズム

鍵長2048ビットのRSA公開鍵暗号方式を使用し、4 (1)ハッシュ値に対して電子署名の生成を行うこと。パディング規則は、PKCS #1 Version 1.5 に準拠すること。

(参考)



↓ 秘密鍵

電子署名(2048ビット)

パディング : 上位16ビット =b “0000 0000 0000 0001”

下位8ビット =b “0000 0000”

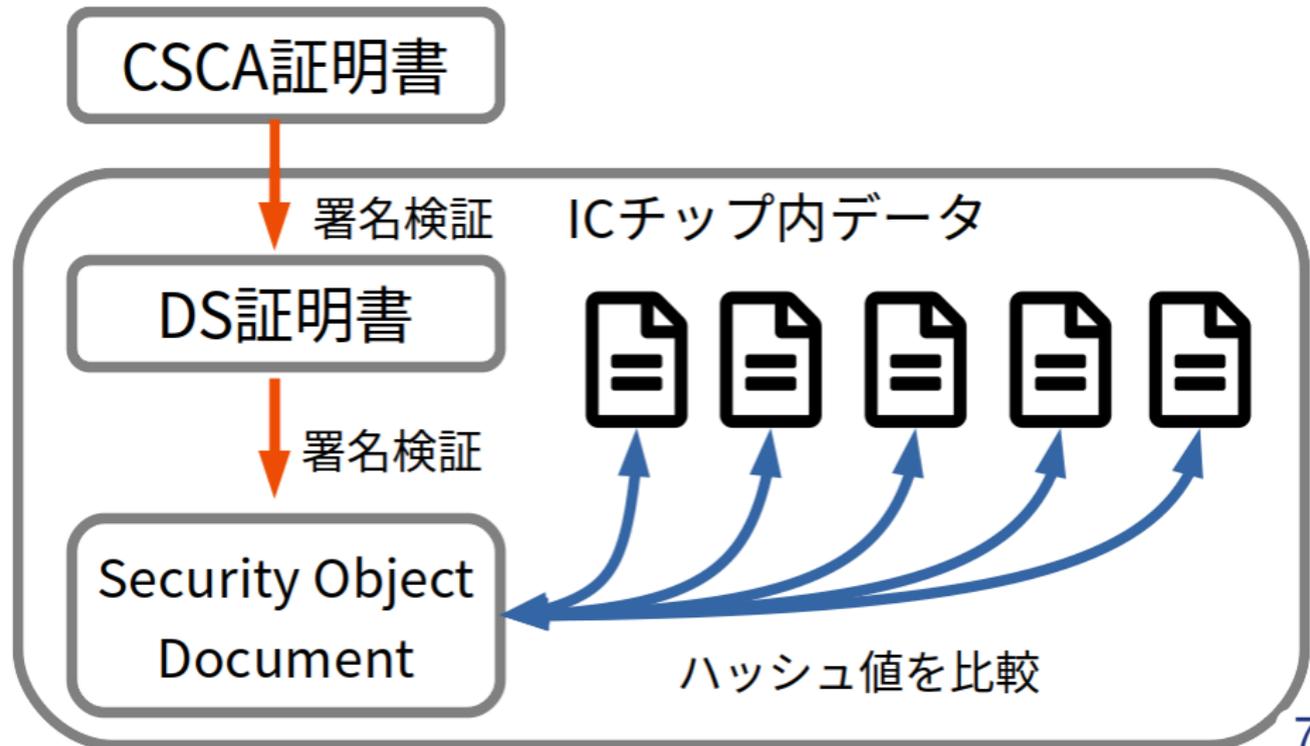
残りのビットはすべてb “1”

# パスポートのセキュリティ

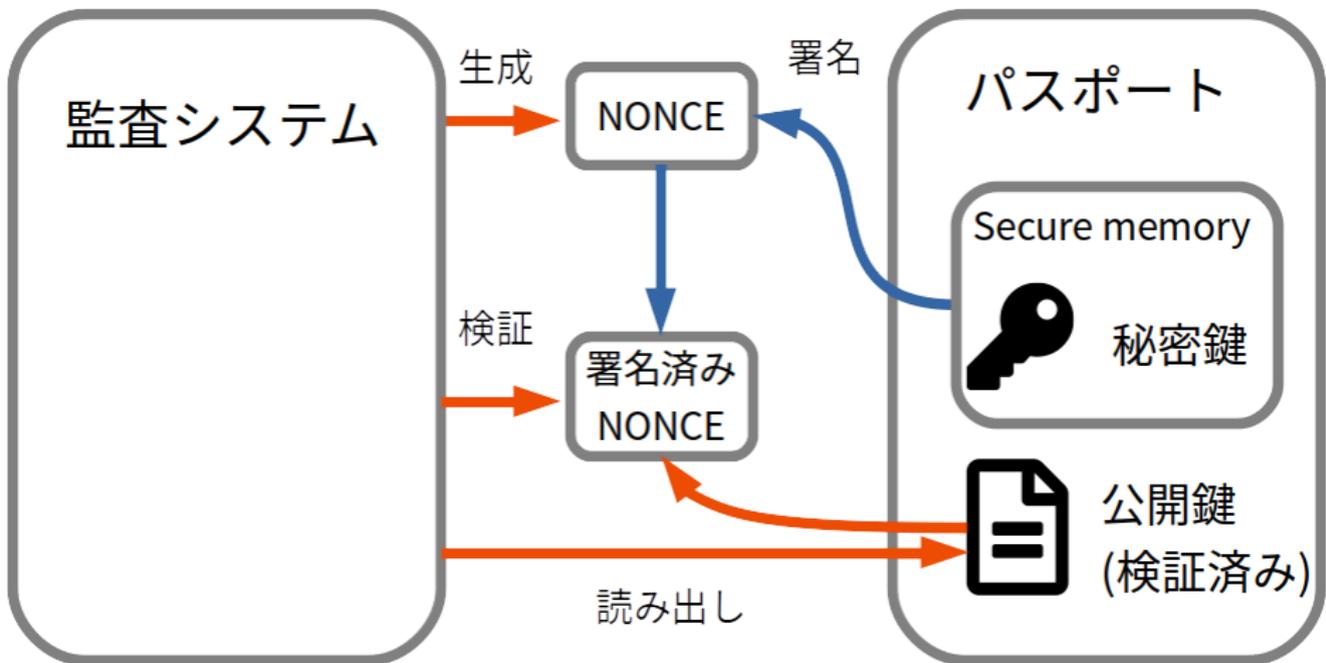
<https://www.osstech.co.jp/~hamano/posts/epassport-security/>



# Passive Authentication



# Active Authentication

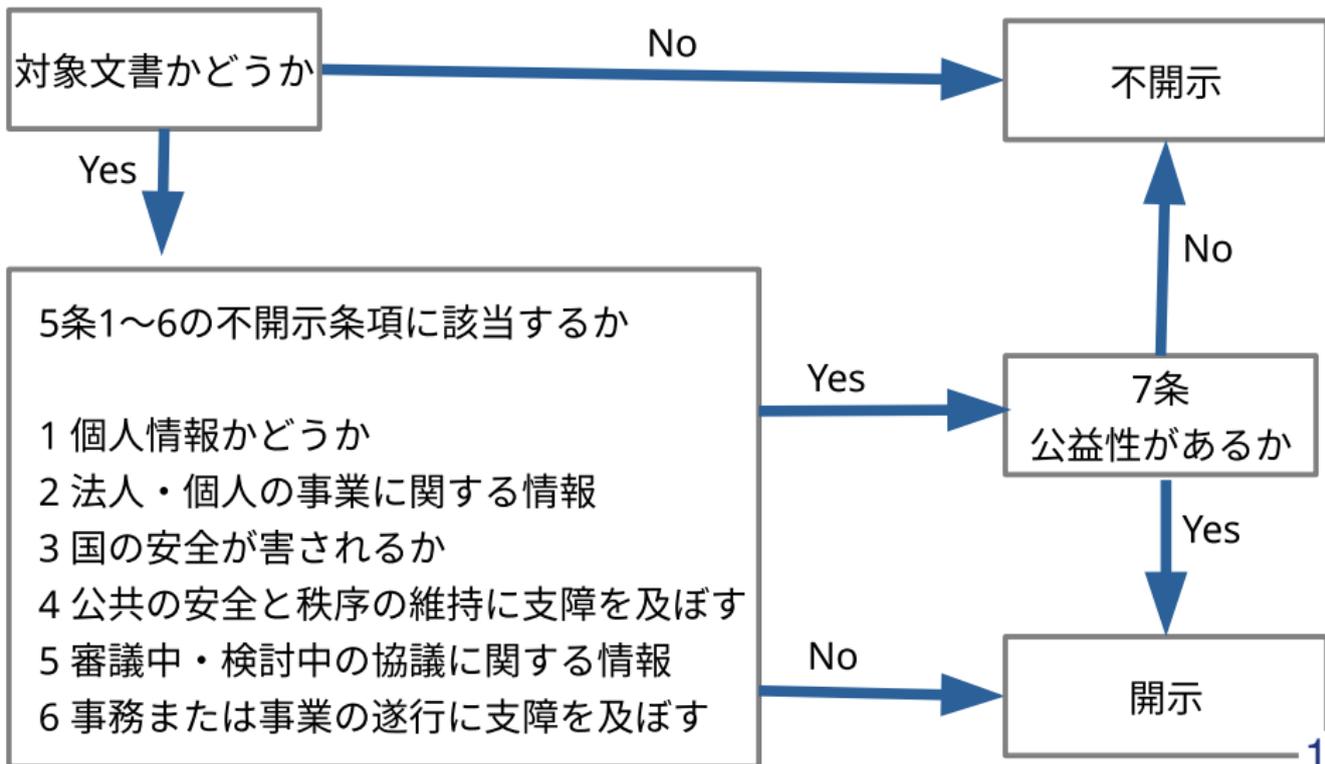


# 情報公開法

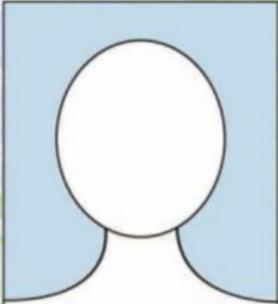
【第1条】この法律は、国民主権の理念にのっとり、行政文書の開示を請求する権利につき定めること等により、行政機関の保有する情報の一層の公開を図り、もって政府の有するその諸活動を国民に説明する責務が全うされるようにするとともに、国民の的確な理解と批判の下にある公正で民主的な行政の推進に資することを目的とする。

- 何人にも
- 目的理由は問わず
- 開示請求者に
- 公開しなければならない

# 情報公開法の論理構造



# 在留カード編

日本国政府 GOVERNMENT OF JAPAN	在留カード RESIDENCE CARD	番号 AB12345678CD No.
氏名 TURNER ELIZABETH NAME		
生年月日 1985年12月31日 性別 女 F. 国籍・地域 米国 DATE OF BIRTH Y M D SEX NATIONALITY/REGION		
住居地 東京都千代田区霞が関1丁目1番1号霞が関ハイツ202号 ADDRESS		
在留資格 留学 STATUS College Student	就労制限の有無 就労不可	
在留期間(満了日) 4年3月(2018年10月20日) PERIOD OF STAY (DATE OF EXPIRATION) Y M D		
許可の種類 在留期間更新許可(東京入国管理局長) 		
許可年月日 2014年06月10日 交付年月日 2014年06月10日		見本・SAMPLE
このカードは 2018年10月20日まで有効 です。 PERIOD OF VALIDITY OF THIS CARD		法務大臣 

# 犯罪収益防止法の改正

- 2018年11月30日施行の改正
  - 犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令
  - 改正規則6条1項1号へ
  - 同パブコメ43
    - ICチップ情報は真正なものが送信されなければならないことは勿論であり、特定事業者には真正なものであることの確認が求められます。
- 2020年4月1日施行の改正

# マイナンバーカード

公的個人認証AP

券面事項  
人力補助AP

券面事項  
確認AP

住基AP

空き領域

# LibJeID



IDリーダー(マイナンバーカード、  
運転免許証)

オープンソース・ソリューション・テクノロジー株式会社  
ツール

★★★★★ 18人



🚩 ほしいものリストに追加

インストール

- アプリソースコード

<https://github.com/osstech-jp/libjeid-android-app/>

- ライブラリ利用方法

<https://www.osstech.co.jp/download/libjeid/>

# NFC規格

## 通信規格(Technology)

NFCIP-1= ISO 18092

NFC F (Felica)  
JIS X 6319-4

NFC A  
ISO 14443-3A

NFC B  
ISO 14443-3B

NFC V  
ISO 15693

NFCIP-2 = ISO 21481

## Protocol

NFC-DEP

ISO-DEP  
ISO 14443-4

## Data Format

NDEF

非NDEF

## タグタイプ(Platform)

Type 1・・・Topaz

Type 2・・・Mifare Ultralight

Type 3・・・交通系、電子マネー

Type 4A・・・Mifare DESFire、Taspo

Type 4B・・・免許証、個人番号カード

Type 5・・・物品管理

# iOS11-13

## 通信規格(Technology)

NFCIP-1 = ISO 18092

NFC F (Felica)  
JIS X 6319-4

NFC A  
ISO 14443-3A

NFC B  
ISO 14443-3B

NFC V  
ISO 15693

NFCIP-2 = ISO 21481

## Protocol

NFC-DEP

ISO-DEP  
ISO 14443-4

## Data Format

NDEF

非NDEF

## タグタイプ(Platform)

Type 1・・・Topaz

Type 2・・・Mifare Ultralight

Type 3・・・交通系、電子マネー

Type 4A・・・Mifare DESFire、Taspo

Type 4B・・・免許証、個人番号カード

Type 5・・・物品管理

# マイナンバーカードと 電子署名の本

