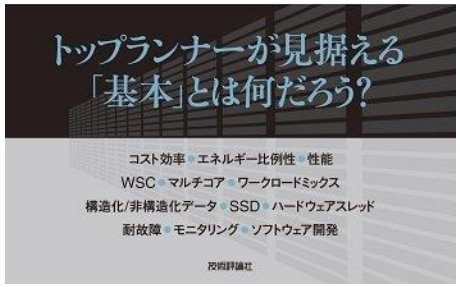
2017/1/30

マイナンバーカードを支える技術

株式会社カーリル
代表取締役・エンジニア 吉本龍司



WEB+DB PRESS plus
支えるシリーズ風に

マイナンバーカードとは何か

ISO/IEC 14443

非接触のICカード

13.56MHz

(図書館のICタグISO15693)

IC仕様書例

マイナンバーカードとは何か

ISO/IEC 7816-4

スマートカードの通信プロトコル

IPA資料

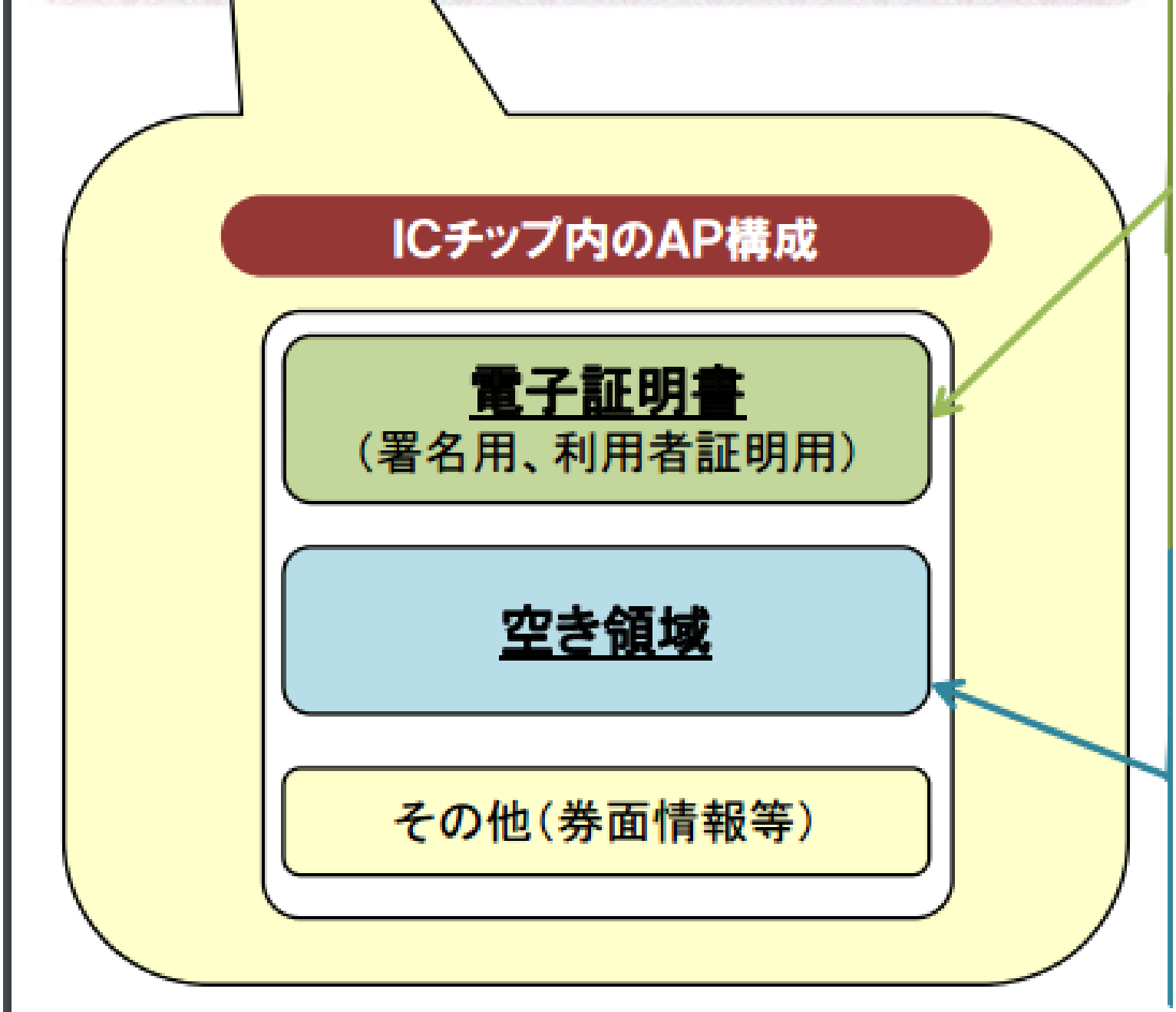
接触型と共通の部分(論理的な機能仕様)

非接触型独自規定部分(物理・電気的仕様、伝送プロトコル仕様)

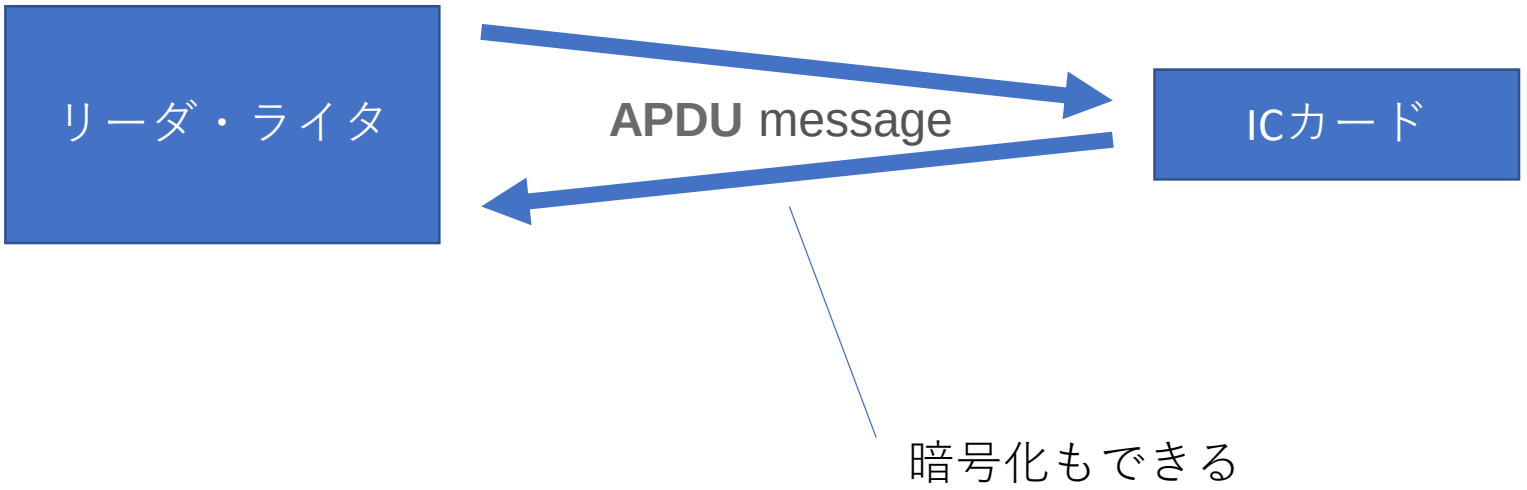
(検討委員会委員提供資料より

総務省資料に出てくるAP（アプリケーション）はここに由来

（検討委員会委員提供資料より作成）

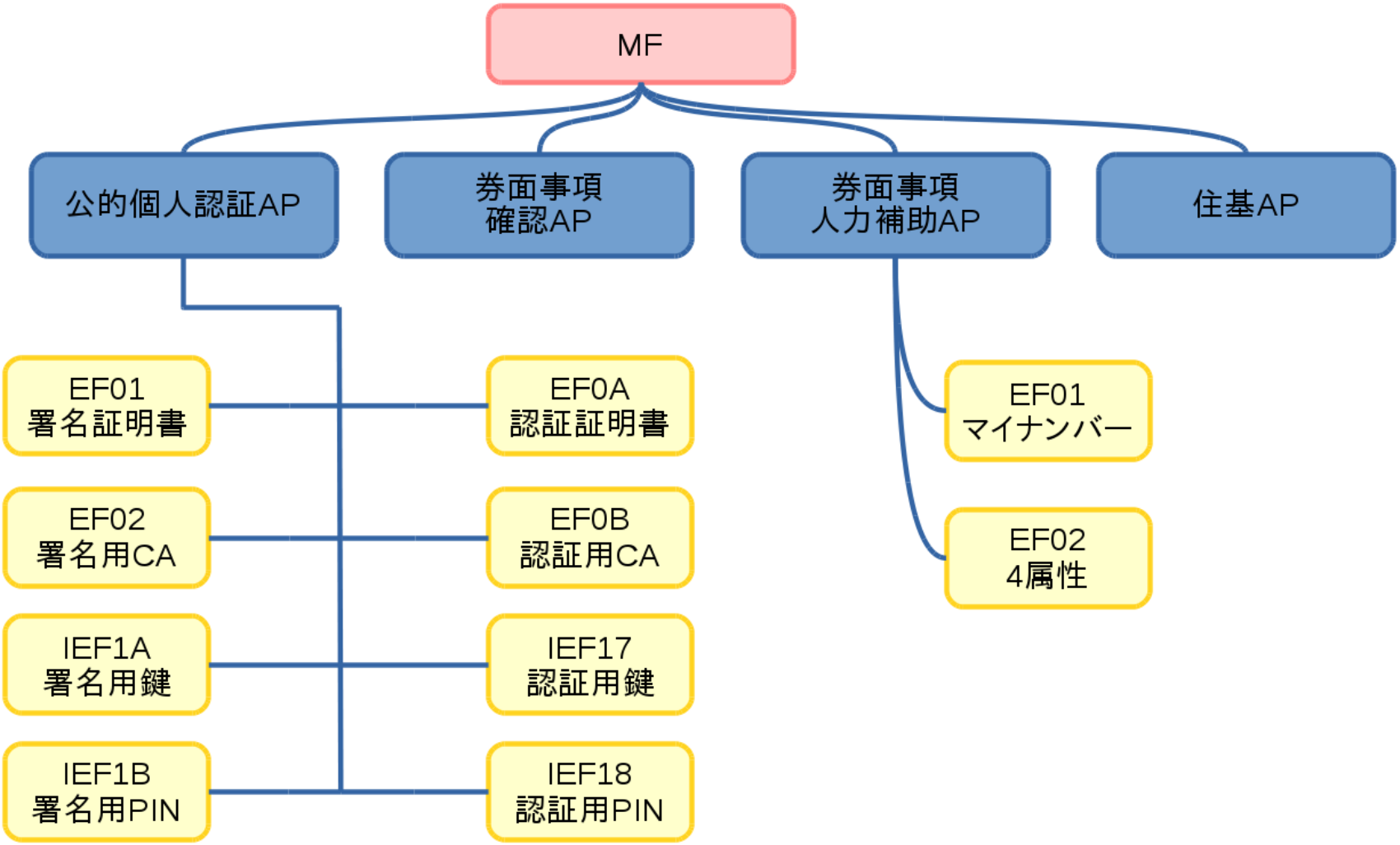

ICチップ内のAP構成
電子証明書
（署名用、利用者証明用）
空き領域
その他（券面情報等）

基本的な通信フォーマットは公開されていて、簡単に通信できる
（だから接続機器は安い）



http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-4_5_basic_organizations.aspx

暗号化機能付きUSBメモリのようなもの



AAAブログより引用・・・プロトコルを公開するべき
https://www.osstech.co.jp/~hamano/posts/jpki-ssh/

参考： B-CASカード/クローズなので品質が低い

マスターパスワードが判明
（toshibaをちょっと変えた・・）
内部ソフトウェアが外部から読み込めることがわかる
→同じカードをエミュレートするプログラムが開発される

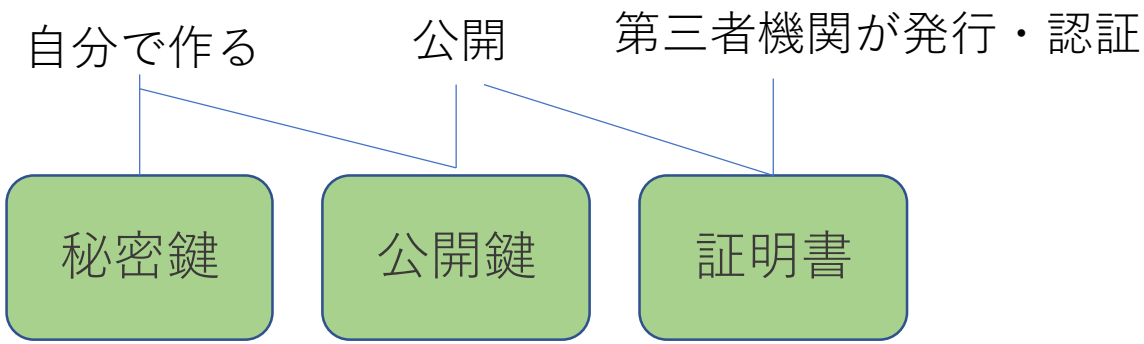
（図書館のICタグのようなもの）

公的個人認証(JPKI)とは

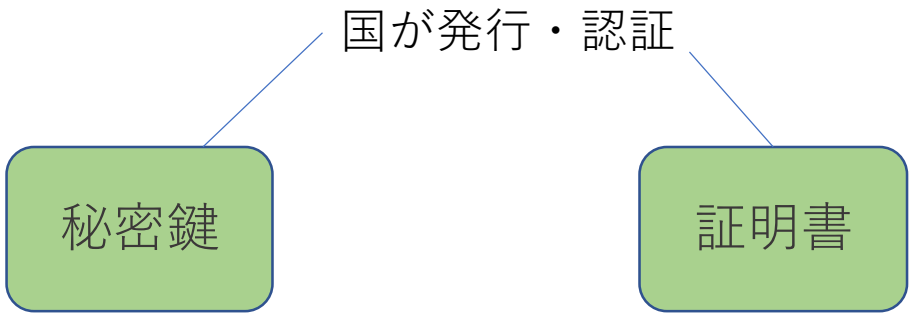
X.509
公開鍵証明書の規格

- ウェブのSSLと同じ（運用は異なる）

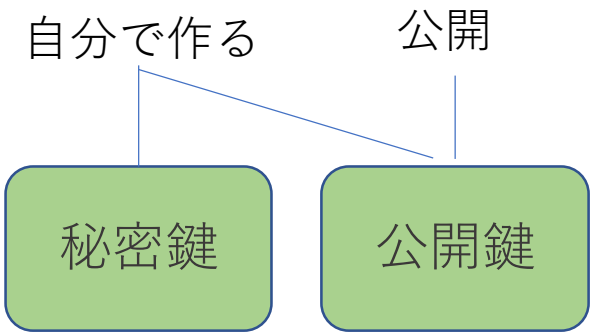
ウェブの暗号化（社会的信用）



公的個人認証（国家による信用）



SSH（ユーザー認証）



暗号化技術における有効期限の必要性

2048ビットの秘密鍵・・・現時点では十分？

MD5・・・数秒で解読できると言われる
将来的に簡単に解読できるようになる可能性が
高く、有効期限が必須

SHA-1・・・2011年に攻撃手法が公開

→ 公的個人認証の有効期限 5年
暗号化技術検討会

カーリルでは頻繁に鍵情報を変更
（たぶん他のIT系企業も同じ）

図書館では、システム更新期間(5年)が基本
※SSL問題

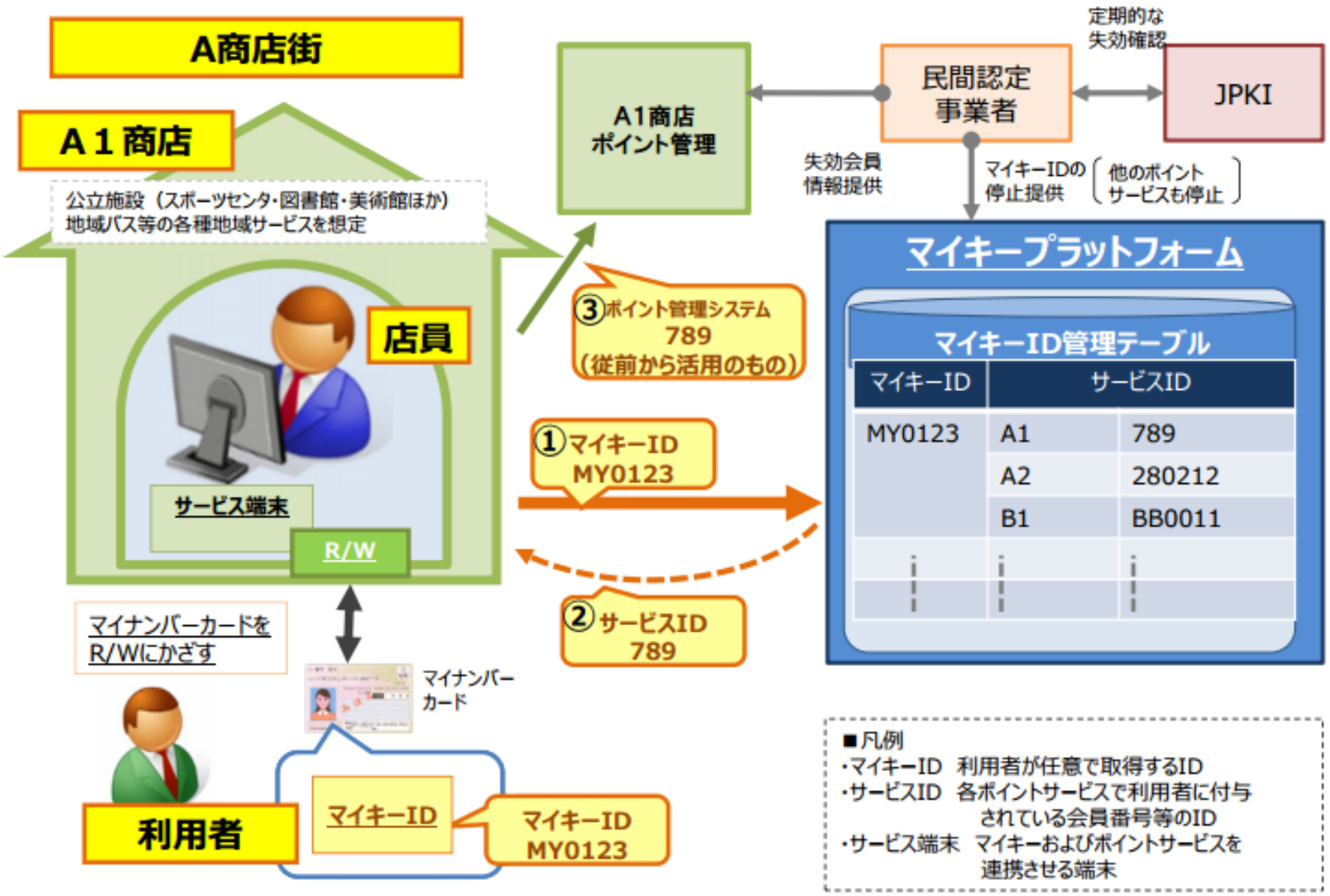
マイナンバーカードを
あくまで技術的視点でとらえる

けっこうしっかりしている

マイキープラットフォーム

（正確な実装に関する情報がない）

マイキープラットフォーム利用のイメージ（素案）



マイナンバーカードの比較して、

設計は稚拙であるが・・・

図書館はもっと脆弱

細かいところに突っ込むべきか
（質疑応答で一緒に考えたほうがいい気がする）

技術的論点1 セキュリティ

技術的論点2 ログデータの扱い

(技術的)論点3

図書館利用での金銭的インセンティブの付与

技術的論点4
技術的負債の返済計画

ここで図書館で自由宣言を見てみる

総務省じゃなくて、

日本図書館協会が、だめだと思う

(理想と現実)

履歴問題と読書通帳・実際の運用

iフィルターの受容

セキュリティクラウド

履歴問題と読書通帳・実際の運用

- 数年前の図書館大会・図書館の自由での発言

カーリルY氏

履歴情報については、特定の機器やサービスに限定せず、貸出記録のデータをダウンロード・外部連携するAPIを設計することで、

多くの問題を解消できる

エンドツーエンド暗号化の必要性

2015年頃から、
多くのウェブサービスがフルSSL化
（エドワード・スノーデンの影響が大きい）

カーリルは2016年3月より
すべての通信の暗号化を開始

ソフトバンクによる通信の不正改ざん問題
（ユーザー同意のない画像の不可逆圧縮）

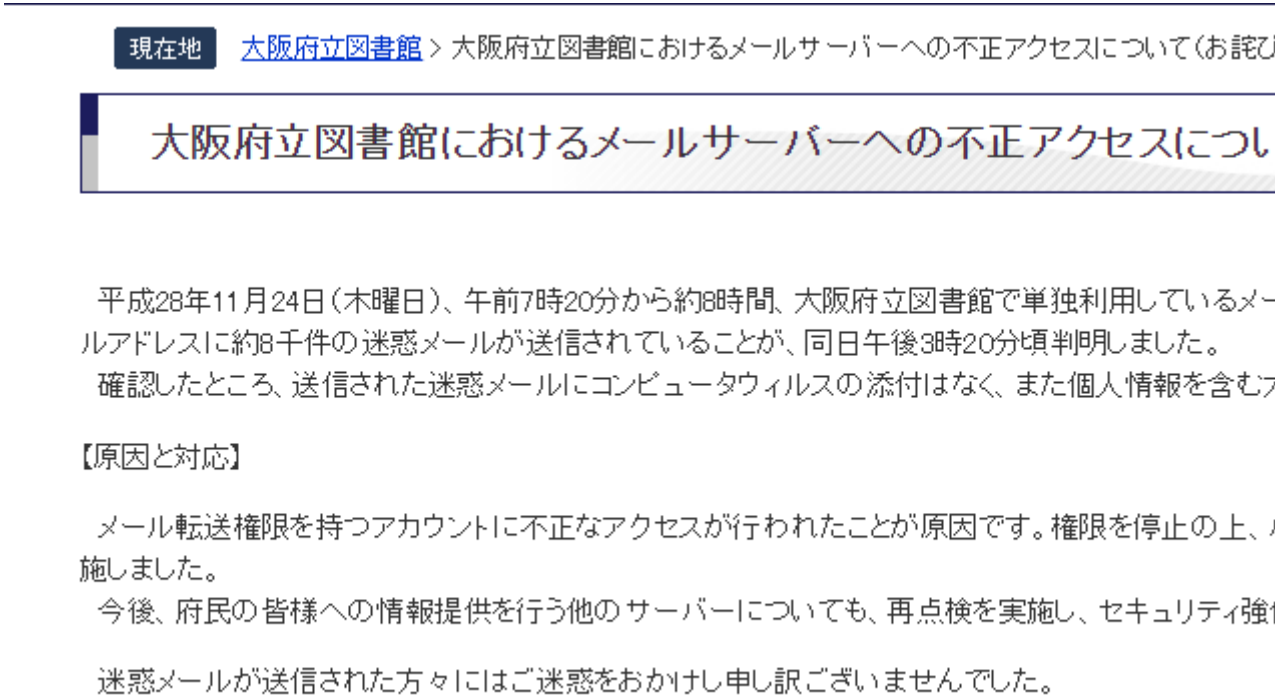
セキュリティクラウド問題

第三者による、ログ情報の取り扱い
（市町村・都道府県・国）

警察の捜査に対する対応

脆弱な図書館のセキュリティ

任せておけない・・というのもわかる
横断検索システムの30パーセントに脆弱性
特定大手ベンダーのセキュリティ品質不足



もはや、図書館は信頼されていない

図書館の自由の基盤となる

“技術”に関する議論が必須

マイナンバー図書館カードの話は、今始まったのか

Tポイントカードの議論も同じだったのでは？

カード共用化・共通化は潜在的なニーズとして存在している→プロトコルや基準は？

“認証”の共通化、相互運用は確実に求められる。

電子書籍・データベースの共同購入

（大学における学術認証フェデレーション「学認（**GakuNin**）」）

OpenID , OAuth2.0 （Google,Twitter,Facebook）

オープン化への希望

そもそも、たいした話ではない

（総務省がやりたいこと、図書館でちゃんと実装すれば）

自動貸出機のプロトコルオープン化
予約棚のプロトコルオープン化

ぜんぶ、積み残した課題では

図書館システムの共同調達

目録・書誌同定

自立定住圏での共同利用

国内ベンダーのレベルアップが急務
（少なくとも図書館についてはカーリルが責任をもつ）

内閣府「マイナポータル」の動作環境が絶望的と話題

2017年01月23日 11時00分　R25

内閣府が1月16日にオープンした、マイナンバー ポータルサイト「マイナポータル」の仕様が、ネット上で物議をかもしている。

※この画像はサイトのスクリーンショットです

「マイナポータル」は、別名「情報提供等記録開示システム」。マイナンバーを利用し、ユーザーがインターネット経由で自分の情報の確認や、自分に必要な行政手続ができることを目指すサイト。社会保険料や税金などの支払いをおこなえるサービスも検討されている。

本格的な運用は今年7月からとされているが、サイトの利用には、パソコンとICチップ搭載の個人番号カード、ICカードリーダーが必要。パソコンを持っていない人のためには公的機関に端末を設置することも検討され、将来的にはスマートフォン、タブレットの利用も想定されているというが、ICカードリーダーはユーザーが自分で購入しなくてはならない。

筋の良いものは広がる

筋の悪いものはなくなる

いろいろな取り組みを認めつつ、

何を守るべきなのか

- PDFダウンロード

https://goo.gl/954fgQ