受診履歴管理のマイナポータル連携とオンライン保険資格確認端末の機能の拡張

第7回　社会情報流通基盤研究センター・シンポジウム

東京工業大学　科学技術創成研究院

未来産業技術研究所 兼 社会情報流通基盤研究センター

小尾高史

ASIST
Assist in improving the information quality

オンライン保険資格確認から受診履歴管理・医療情報参照へ

- **オンライン保険資格確認によって生じる証跡データを受診履歴として管理し、その情報をもとに医療情報参照を実現**
  - 「だれ・どこ・いつ」の情報と、患者の明確な本人同意のもとで、当該患者の医療情報参照を実施
- **受診履歴管理サービスの実現に向けて**
  - 誰が受診履歴を管理するか
  - 患者はどのように受診履歴を参照するか
  - 資格確認端末と受診履歴管理サービスとの関係の整理

マイナポータルとの連携可能性

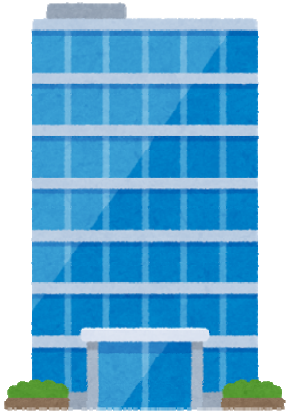
旅行先医療機関など

自宅

受診履歴参照

マイナポータル

受診履歴管理サービス



保険資格確認PF

オンライン保険資格確認

情報提供側医療機関

ASIST
Assist in improving the information quality

マイナポータルの有する機能

- **情報提供等記録表示**（番号法附則第6条第3項）
- **自己情報表示**（番号法附則第6条第４項第１号）
- **お知らせ**（番号法附則第6条第４項第２号）
- **外部連携機能**
  - ID（認証）連携・データ連携
  - 民間送達サービス
  - ワンストップサービス（番号法附則第6条第４項第３号）
  - 公金決済ワンストップサービス

自己情報表示機能の利用

情報提供側医療機関

保険資格確認PF

オンライン保険資格確認

資格確認時ログ（受診履歴）
（中間サーバ）

自宅

新規受診履歴登録の
“お知らせ”（登録必要）

マイナポータル

受診履歴参照
（自己情報表示）

旅行先医療機関など

受診履歴参照

受診履歴管理サービス

ID（認証）連携
受診履歴の提供（データ連携）
（オプトイン）

ASIST
Assist in improving the information quality

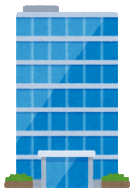
自己情報表示機能の利用 contd.

- **受診履歴の蓄積に特別な仕組みは不要**
  - 外部認証鍵の端末への搭載が進めば、保険資格確認の仕組みをほぼ流用可能
  - 受信履歴参照に時間がかかる可能性
- **マイナポータルからの受診履歴登録通知の取得や履歴参照が可能**
- **受診履歴の長期保存への対応が必要**
  - 受診履歴管理サービスの利用
  - マイナポータルとの連携により受診履歴の受診履歴管理サービスへの提供が可能
  - 必要になったときに登録することも可能
- **受診履歴開示に関する法整備が必要**
  - 番号法附則第6条第4項第1号は、法律の規定による個人情報の開示に関する手続きと規定

民間送達サービス機能の利用

情報提供側医療機関

オンライン保険資格確認



保険資格確認PF

受診履歴登録

受診履歴管理サービス

ID（認証）
連携

受診履歴参照

旅行先医療機関など

受診履歴参照

受診履歴参照
（件名のみ）

マイナポータル

自宅

新規受診履歴登録の
お知らせ（登録必要）
（民間送達サービス）

民間送達サービス機能の利用 contd.

- **受診履歴管理サービスへの登録が必要**
  - 初期登録はマイナポータルとの連携により実施
  - 受信履歴管理サービスへの受信履歴登録は端末で実施
  - 受診履歴管理に関する法整備は不要と想定
- **マイナポータルからの受診履歴登録通知の取得が可能**
- **マイナポータルからの受診履歴件名の取得が可能**
  - 情報実体は受診履歴管理サービスからの取得が必要

実現可能性を含め、どのような連携が望ましいかを検討

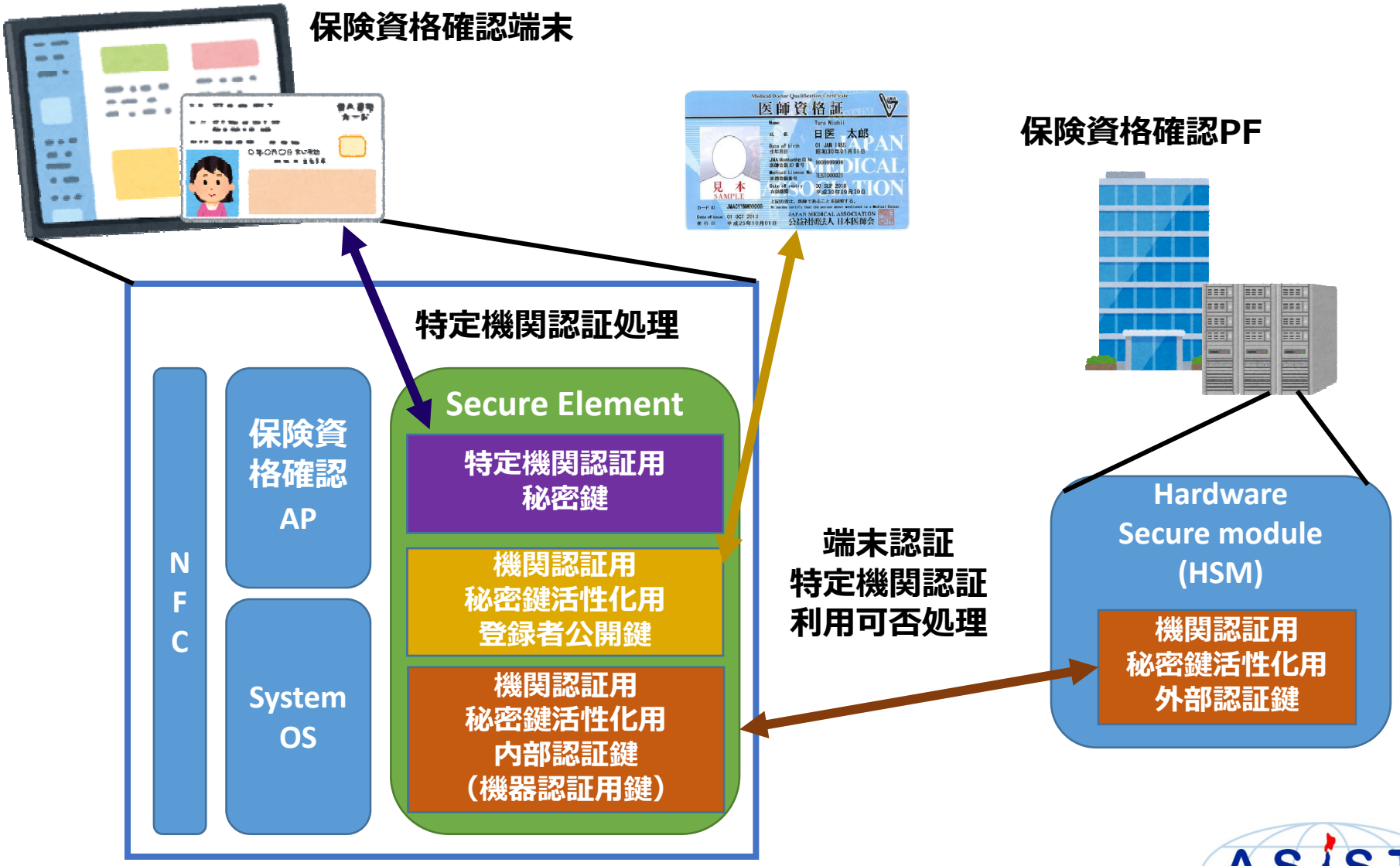
保険資格確認端末の検討

- **特定機関認証鍵格納方法**
  - 端末提供組織（保険資格確認PF）は、J-LISより発行された特定機関認証用公開鍵証明書及び秘密鍵をSecure Elementなどの格納媒体等に格納し端末に格納
  - 端末提供組織は端末と公開鍵証明書及び秘密鍵の紐づけ管理を実施
- **端末盗難時等の安全性確保**
  - 正規な利用以外では特定機関認証機能の利用禁止
  - 医療機関などの端末利用組織の管理者等と、端末及び特定機関認証用秘密鍵格納媒体との紐づけを実施
- **端末利用シーンの拡大**

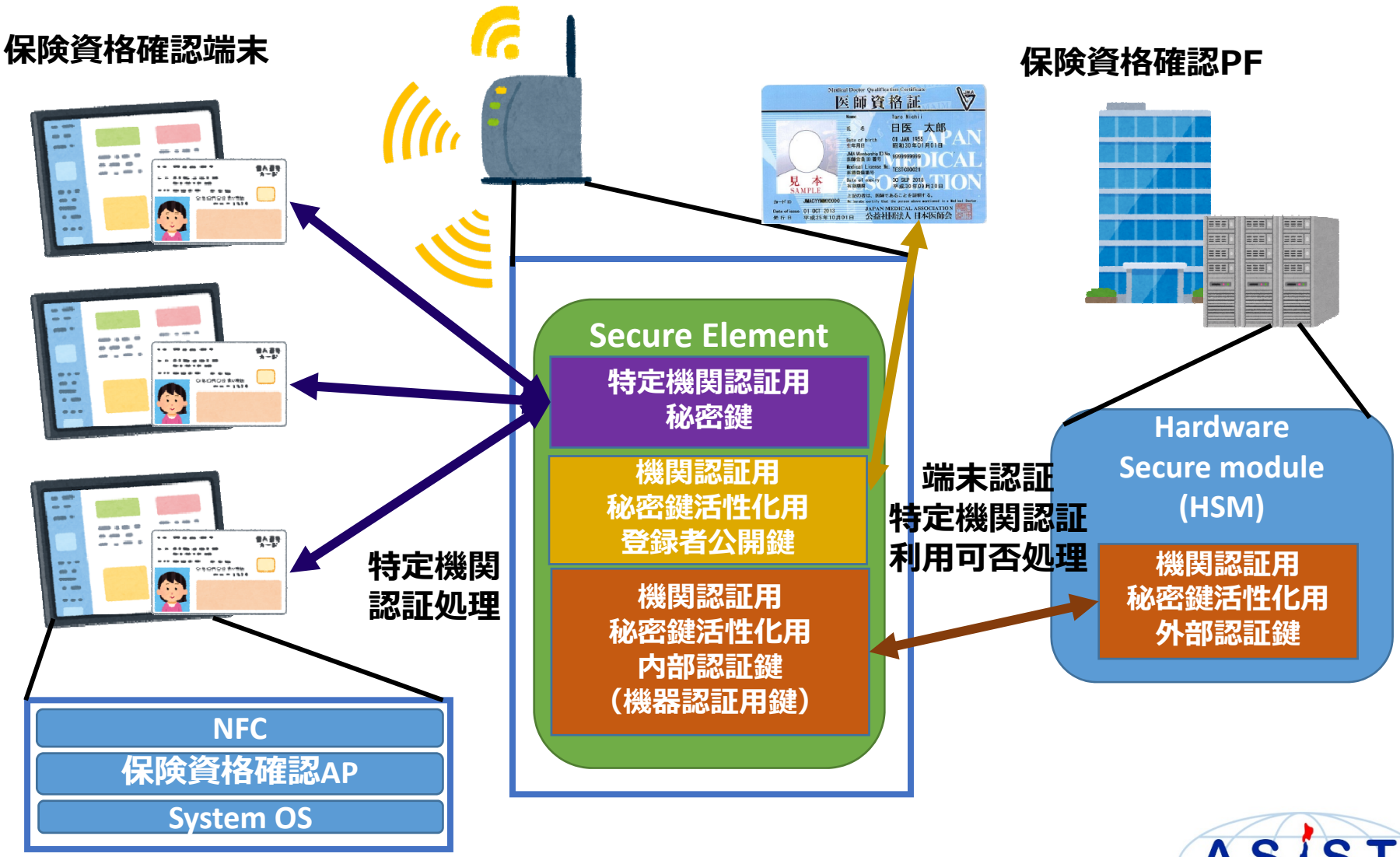
特定機関認証用秘密鍵の管理

- **機関認証用秘密鍵の安全な管理**
  - Secure Element（SAM, UIMなど）の利用
- **電源投入時（端末利用開始時）における端末等の正当性確認**
  - 特定機関認証用秘密鍵を利用する際には、あらかじめサービス提供機関との間で端末の認証等を行うことで、不正な鍵利用を防止
  - オフライン利用時には、端末登録組織（者）による認証（端末管理者のJPKI、HPKI等の利用を想定）

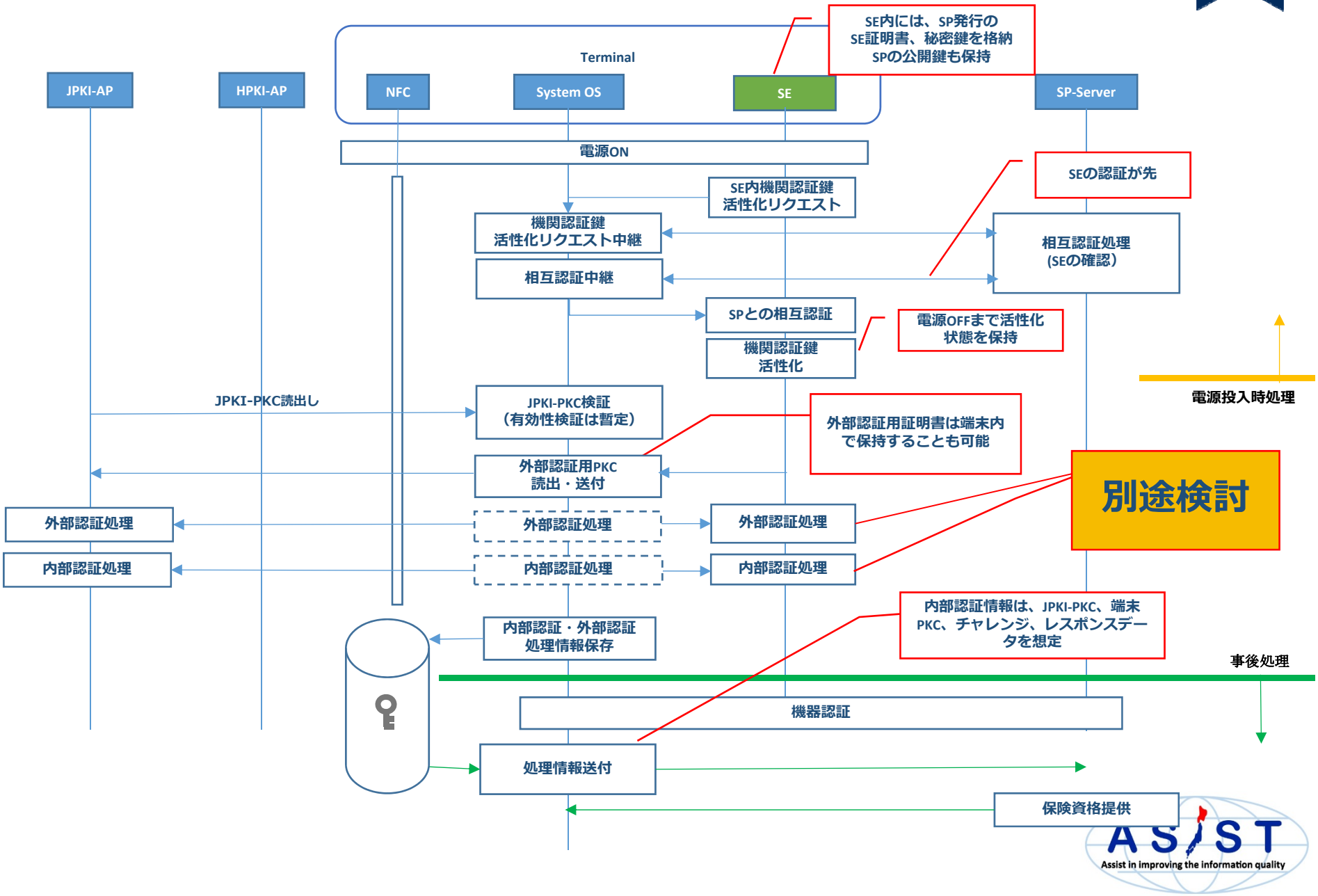
端末の構成(端末にSEを搭載)



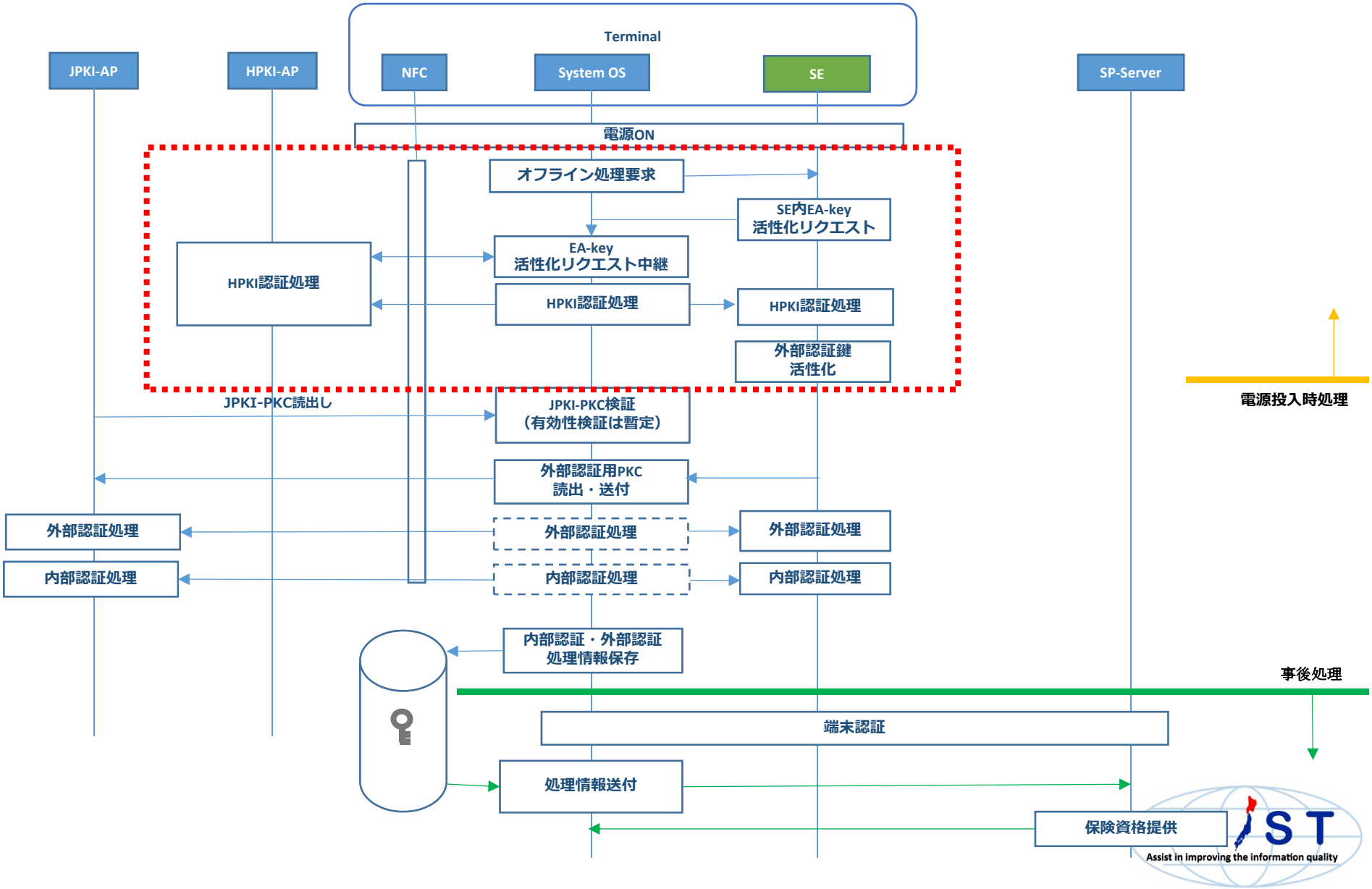
端末の構成(医療機関にSE格納端末を設置)



処理フロー（端末にSE搭載、一部オフライン時）



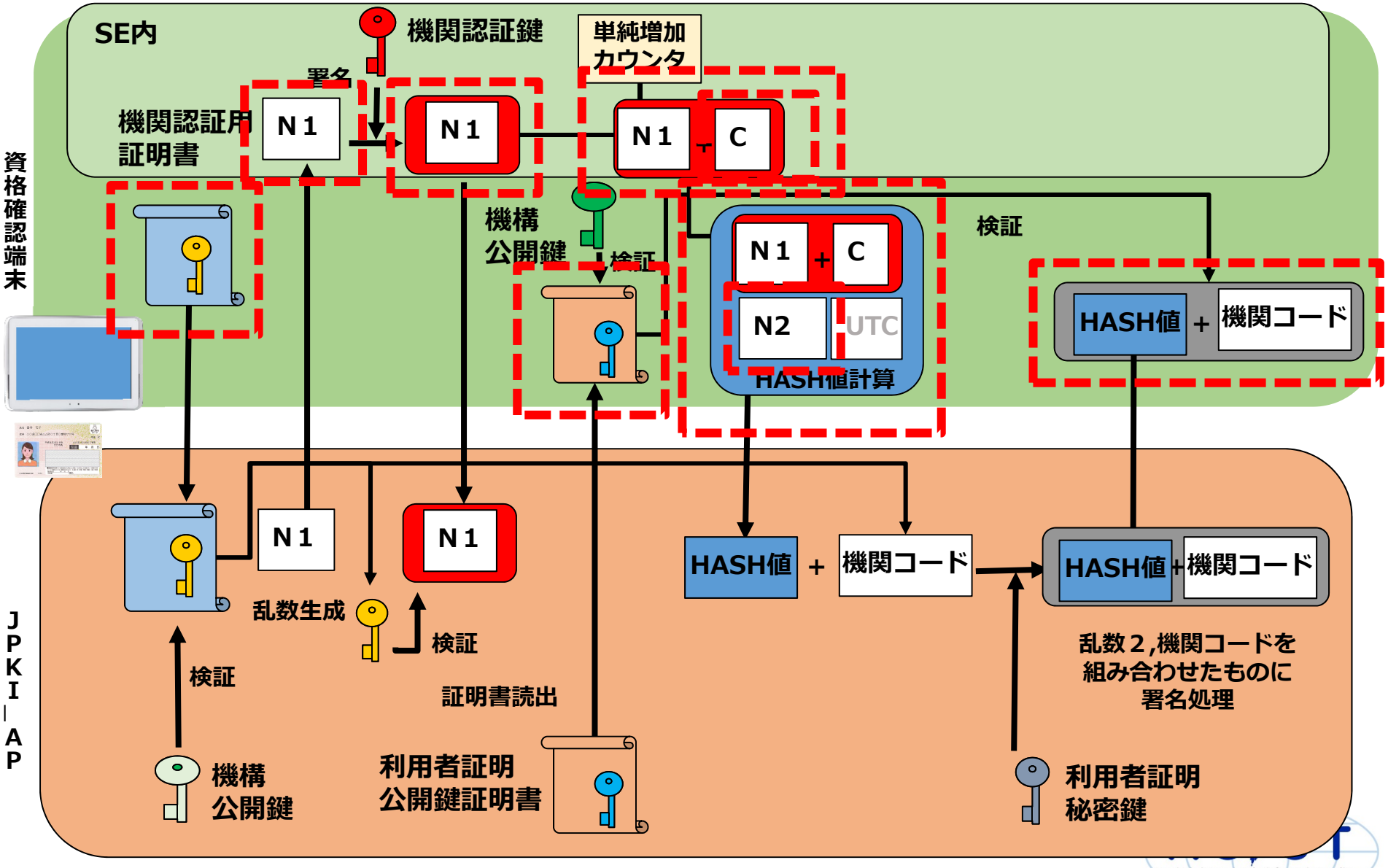
処理フロー（端末にSE搭載、完全オフライン時）



端末内処理の検討

- **内部認証と外部認証処理の紐づけ**
  - SE内の内部カウンターを利用
- **受診履歴生成時刻（日付）の証明**
  - Time Stamp with Tick Stampの応用
  - SPによる機関認証処理時刻の証明と内部認証処理時間の紐づけ

外部認証処理と内部認証処理の連携



Time Stamp with Tick Stamp

- TPMを用いて実現可能なタイムスタンプ相当の処理をベース
- SE内にTick Counterを設置
  - 電源投入時にTickCounterを初期化、TickNonceを生成
  - 一定時間毎（既知）にTickCounterをインクリメント
  - Ticks = TickCounter || TickNonce
- SE活性化後、端末は、乱数||$Ticks_1$（連結処理はSE内部)に対してS機器認証鍵で署名（Tick Stamp処理）し、SPへ送付（TickStamp1）
- SPは、Tickstamp1にタイムスタンプサーバ等でTimes Stampを押して端末に返送（TimeStamp(TickStamp1)）
- 端末は、Hash(Timestamp(TickStamp1))|| $Ticks_2$に対して、機器認証鍵で署名（TickStamp2)
- $Ticks_1$と$Ticks_2$の時間間隔は既知（T_{diff})なので、TickStamp1の生成時刻（T_1)は、TimeStamp(TickStamp1)生成時刻(Ts)から、
  $Ts- T_{diff} < T_1 < Ts+ T_{diff}$ と推定
- Time Stamp with Tick Stampは、 Message|| Ticksに対して、機器認証鍵で署名することで実施
- .NET card（or Javacard3 Connected Edition）以外は実施困難

Date Stamp with Tick Stamp

- **SE内にTick Counterを設置**
  - 電源投入時にTickCounterを初期化、TickNonceを生成
  - Tick Stamp処理を行うごとにTickCounterをインクリメント
  - Ticks = TickCounter || TickNonce
- **SPによるSE認証時に、SEはSPから送られた（Nonce||時刻）に対して、SE内で、（（Nonce||時刻）||Ticks||単純増加カウンタ）に機器認証鍵で署名し、SPへ送付（TickStamp1）**
- **SPは、Tickstamp1にタイムスタンプサーバ等でTimes Stampを押して端末に返送（TimeStamp(TickStamp1)）**
- **Date Stamp with Tick Stampは、 Message|| Ticksに対して、機器認証鍵で署名することで実施**
- **TickNonceにより、 TimeStamp(TickStamp1)と紐づけされるが、実際にTime Stamp with Tick Stampが押された時刻は分からない。**
- **日付が変わった場合には、機器内の処理でTimeStamp(TickStamp1)を再取得処理を行う必要がある**

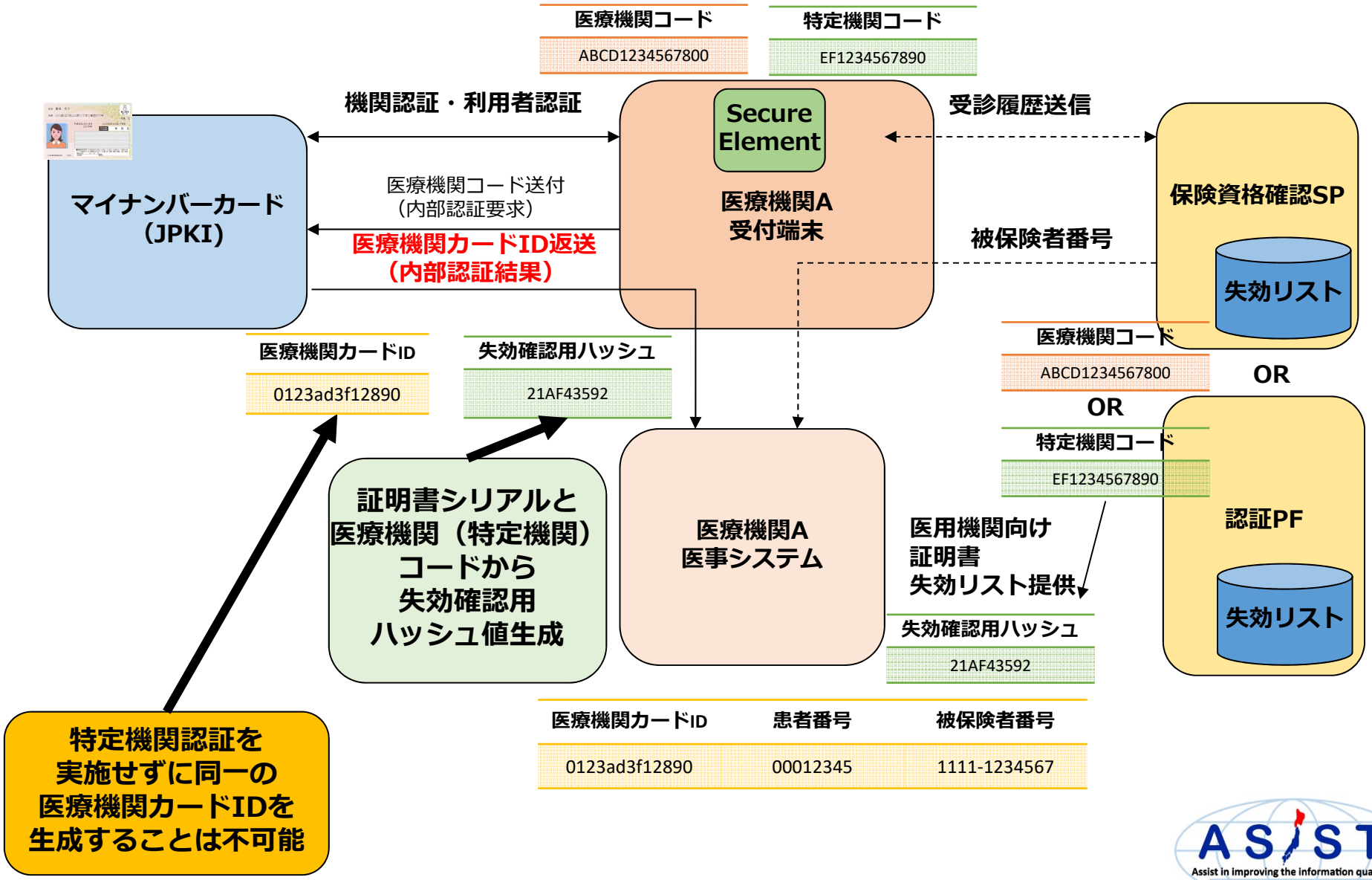
機関認証を利用した医療機関カードID

マイナンバーカード、保険資格確認端末のみで再診受付時などに患者を特定

- **シリアル番号の取得管理を医療機関は行えない**
  - 公的個人認証法第六十三条
    - …利用者証明検証者以外の者は、何人も、業として、…利用者証明用電子証明書の発行の番号の記録されたデータベースであって、当該データベースに記録された情報が他に提供されることが予定されているものを構成してはならない。
- **利用者証明書のCommonName(CN)の利用**
  - 利用方針が明確でない
  - 他分野と同じIDを利用することへの懸念

→ **機関認証による利用者証明機能を用いた医療機関カードIDの生成**

医療機関窓口での利用


医療機関コード
ABCD1234567800
特定機関コード
EF1234567890
機関認証・利用者認証
Secure Element
受診履歴送信
マイナンバーカード（JPKI）
医療機関コード送付
（内部認証要求）
医療機関カードID返送
（内部認証結果）
医療機関A
受付端末
保険資格確認SP
被保険者番号
失効リスト
医療機関カードID
0123ad3f12890
失効確認用ハッシュ
21AF43592
医療機関コード
ABCD1234567800
OR
OR
特定機関コード
EF1234567890
証明書シリアルと
医療機関（特定機関）
コードから
失効確認用
ハッシュ値生成
医療機関A
医事システム
医用機関向け
証明書
失効リスト提供
認証PF
失効リスト
失効確認用ハッシュ
21AF43592
医療機関カードID
患者番号
被保険者番号
0123ad3f12890
00012345
1111-1234567
特定機関認証を
実施せずに同一の
医療機関カードIDを
生成することは不可能

医療機関カードIDの特徴

- **カードID生成に利用者証明機能を利用**
- **医療機関毎（端末毎）に異なる医療機関カードIDを生成**
- **保険資格確認（機関認証処理）が行える組織以外は発行不可**
  - 生成には各医療機関ごとに異なる証明書記載の個別ID（機関コード）が必要
  - 端末ごとに格納された特定機関認証用公開鍵証明書との組み合わせでのみ実現
- **医療機関内では証明書シリアルと紐づけて管理しないため、外部から誰のIDかの推測は困難**
- **証明書シリアルと医療機関コード（特定機関コード）のハッシュ値を用いれば、認定認証機関（保険資格確認PF）から失効リストの提供も可能**

おわりに

- 特定機関認証を用いたJPKI利用者証明機能には、様々な応用例が存在
- 医療分野だけでなく様々な民間分野での利用を期待
- カードIDの生成は、PKCS#1 v1.5でのみ実現可能であり、今後JPKIが、PKCS-PSS (Probabilistic Signature Scheme)やECDSAに移行する際の方法は要検討

Tokyo Tech

Thank you

A part of this work was supported by Health Labour Sciences Research Grant, Research on Region Medical H28-Iryo-Shitei-034 and JSPS KAKENHI Grant Number 15K12458.