Orchestrating a brighter world NEC

日本銀行 決済の未来フォーラム デジタル通貨分科会

CBDCにおける Digital Identity の基礎知識

日本電気株式会社　宮川　晃一

自己紹介

宮川　晃一（みやかわ　こういち）

日本電気株式会社　金融システム本部　シニアエキスパート
（兼務）サイバーセキュリティ戦略本部
（兼務）レギュレーション調査室

OpenAPI/eKYC/Digital ID/My DATA/Identity Management/Cyber Securirty

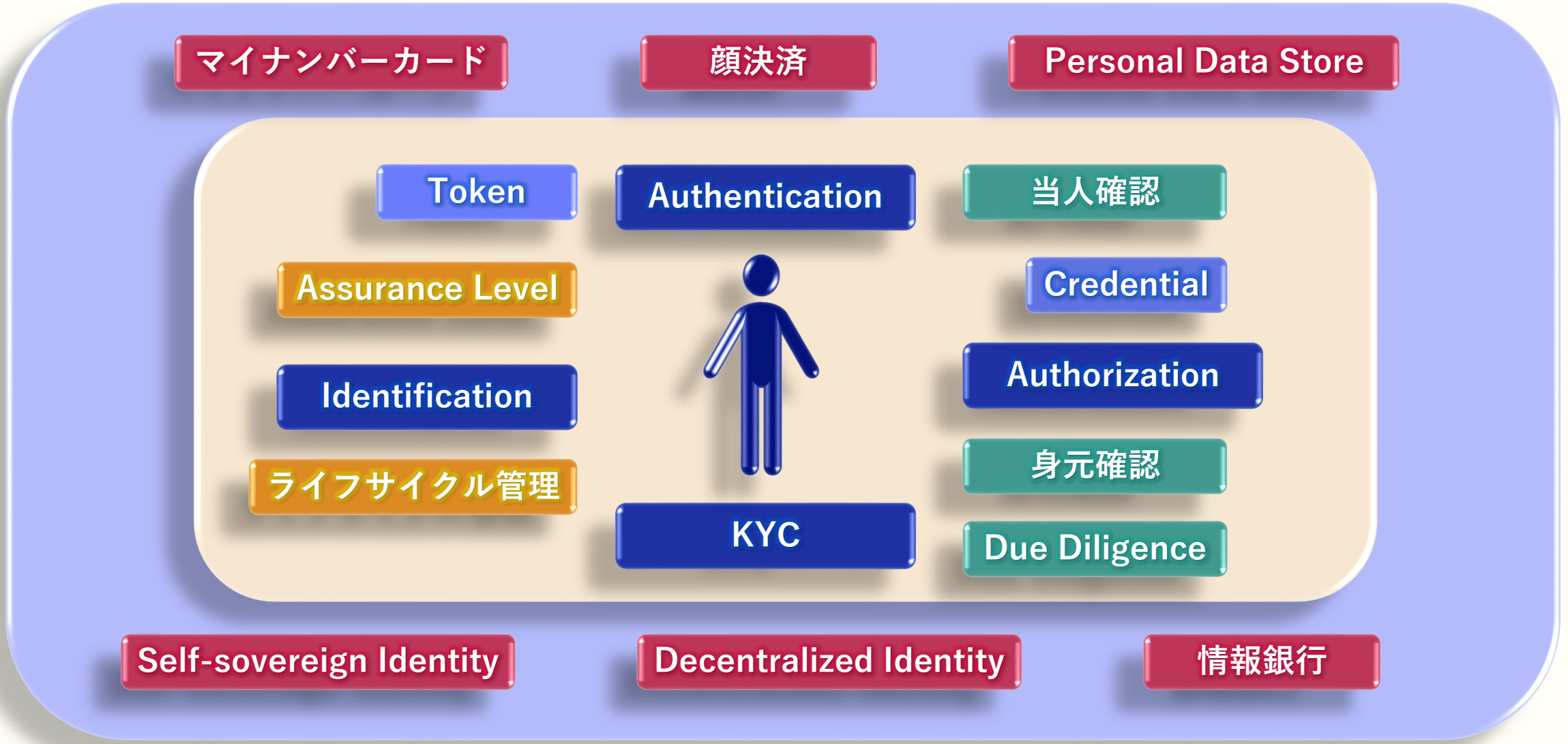
「サイバーセキュリティおよびデジタルアイデンティティの専門家」

【主な所属団体】
- クラウドセキュリティアライアンス（CSA-JC）理事
  https://www.cloudsecurityalliance.jp/site/?page_id=47
- 日本ネットワークセキュリティ協会（JNSA）
  標準化部会　デジタルアイデンティティWGリーダ
  https://www.jnsa.org/active/std_idm.html
- FISC オープンAPIに関する有識者検討会委員
  https://www.fisc.or.jp/document/public/003105.php

【主な著書】（共著）
「クラウド環境におけるアイデンティティ管理ガイドライン」－インプレスR&D
「セキュリティエンジニアの教科書」－C&R研究所
「Software Design 2020年11月号認証・認可特集」－技術評論社

目次

1．Digital Identity 周辺の言葉の定義



2．本人確認とは

身元確認と当人認証の違い

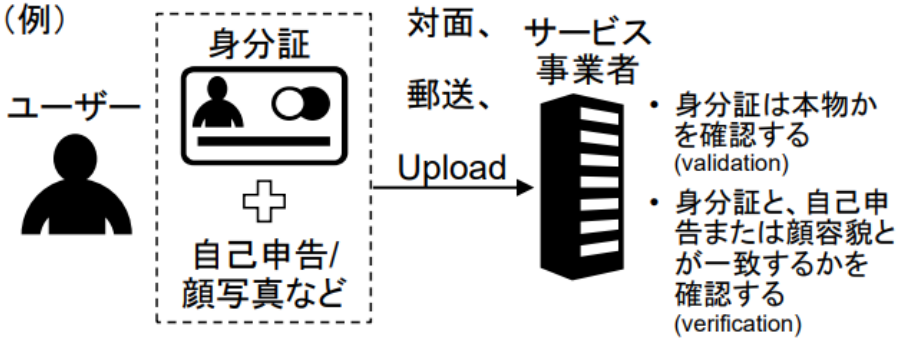
身元確認・当人認証とはなにか

両者をあわせて本人確認という

身元確認
（検討会スコープ）

- 登録する氏名・住所・生年月日等が正しいことを証明/確認すること

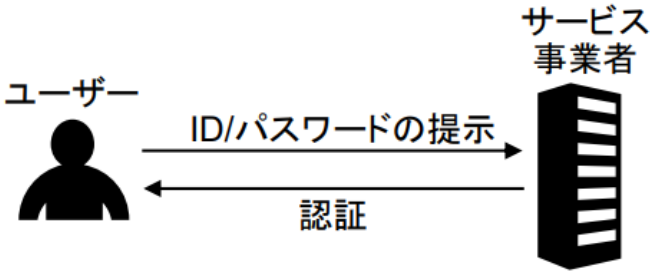
（例）



当人認証

- 認証の3要素[1)]のいずれかの照合で、その人が作業していることを示すこと

（例）



推奨されているレベル区分（2019年現在）

保証レベル 高

Lv3	「対面」で「公的身分証」を基にした身元の確認
Lv2	「郵送等の非対面」で「公的身分証」を活用した身元の確認
Lv1	「自己申告」を基にした身元の確認

保証レベル 高

Lv3	3要素のうち耐タンパ性を持つハードウェア[2)]を含めた複数を用いる認証
Lv2	3要素のうち複数用いる認証
Lv1	3要素のうち1つ用いる認証

出典：オンラインサービスにおける身元確認手法の整理に関する検討報告書

3．標準化ドキュメントとしてのNIST SP800-63

Digital Identity Guidelines

The four-volume SP 800-63 *Digital Identity Guidelines* document suite is available in both PDF format and online.

PDF versions of the documents are available from:

※NIST=米国国立標準技術研究所

Document	Title	URL
SP 800-63-3	Digital Identity Guidelines	https://doi.org/10.6028/NIST.SP.800-63-3
SP 800-63A	Enrollment and Identity Proofing	https://doi.org/10.6028/NIST.SP.800-63a
SP 800-63B	Authentication and Lifecycle Management	https://doi.org/10.6028/NIST.SP.800-63b
SP 800-63C	Federation and Assertions	https://doi.org/10.6028/NIST.SP.800-63c

デジタル認証のガイドライン　登録プロセスと身元確認　認証とライフサイクル管理　フェデレーンとアサーション

Identity Assurance Level（IAL）　Authenticator Assurance Level（AAL）　Federation Assurance Level（FAL）

SP 800-63-3
Digital Identity Guidelines

SP 800-63A
Enrollment & Identity Proofing

SP 800-63B
Authentication & Lifecycle Management

SP 800-63C
Federation & Assertions

Additional informative resources:

出典：NIST SP 800-63 Digital Identity Guidelines

4．Enrollment（登録）と Identity Proofing（身元保証）

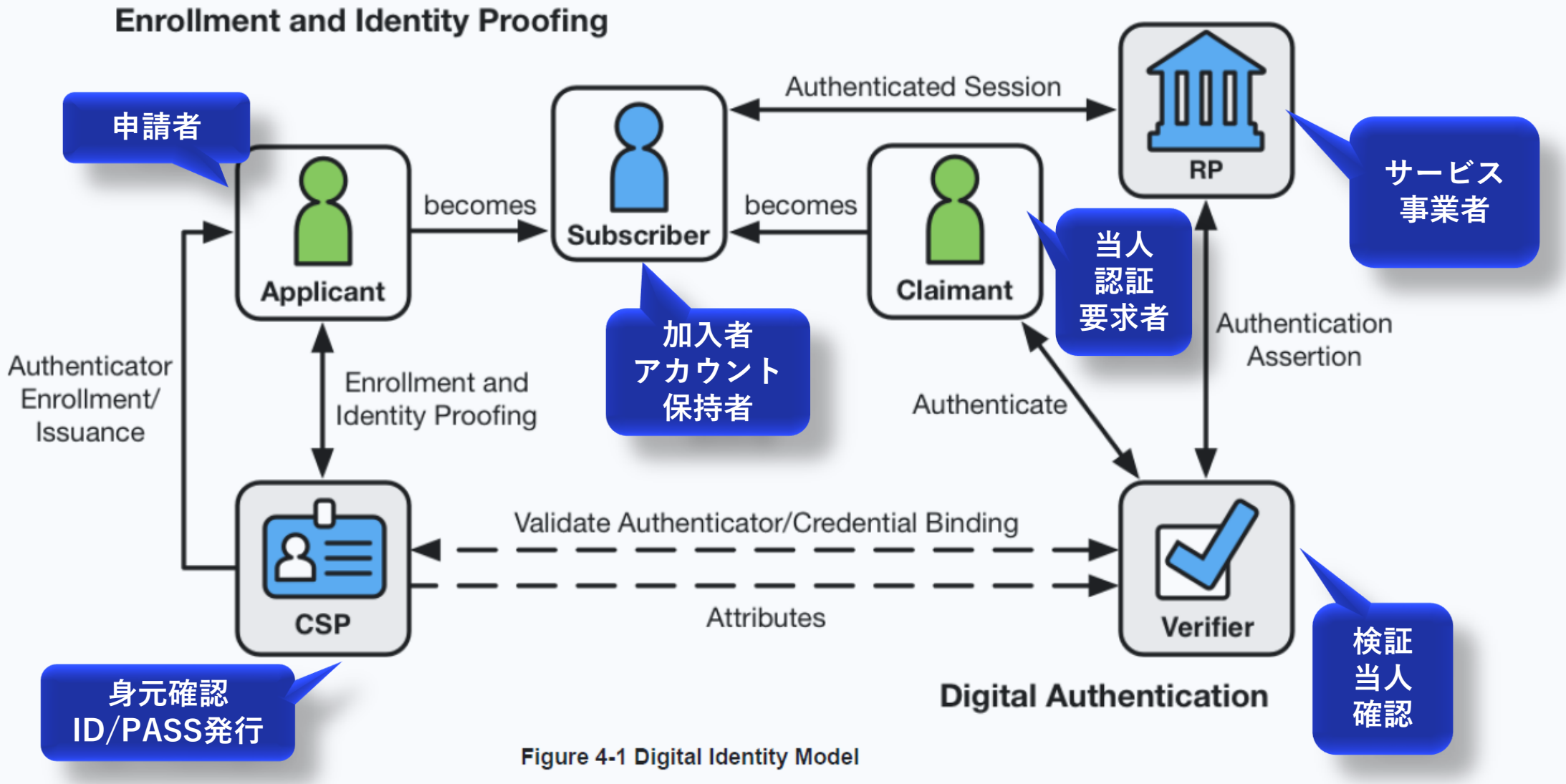


Figure 4-1 Digital Identity Model

出典：NIST SP 800-63 Digital Identity Guidelines

5．Assurance Level（評価保証レベル）

- **Identity Assurance Level（IAL）（SP 800-63A）**
  ユーザが申請者（Applicant）として新規登録（SignUp）する際に、CSP（Credential Service Provider）が行う

  身元確認（Identity Proofing）の厳密さや強度を示す
  Lv.1 本人確認不要、自己申告での登録でよい
  Lv.2 サービス内容により識別に用いられる属性をリモートまたは対面で確認する必要あり
  Lv.3 識別に用いられる属性を対面で確認する必要があり、確認書類の検証担当者は有資格者
- **Authenticator Assurance Level（AAL）（SP 800-63B）**
  登録済みユーザー（Claimant）がログインする際の**当人認証**プロセス（単要素認証or多要素認証、認証手段）の強度を示す
  Lv.1 単要素認証でOK
  Lv.2 2要素認証が必要、2要素目の認証手段はソフトウェアベースのものでOK
  Lv.3 2要素認証が必要、かつ2要素目の認証手段はハードウェアを用いたもの（ハードウェアトークン等）
- **Federation Assurance Level（FAL）（SP 800-63C）**
  IDトークンやSAML Assertion等、Assertionのフォーマットやデータやり取りの仕方の強度を示す
  Lv.1 Assertion（RPに送るIdPでの認証結果データ）への署名
  Lv.2 署名に加え、対象RPのみが復号可能な暗号化
  Lv.3 Lv.2に加え、Holder-of-Key Assertionの利用（ユーザごとの鍵とIdPが発行したAssertionを紐づけてRPに送り、RPはユーザがそのAssertionに紐づいた鍵を持っているか（ユーザの正当性）を確認）

出典：NIST SP 800-63 Digital Identity Guidelines

6．リスクと技術的な強度（リスクベースコントロール）

【リスク】
AML対策として物理社会での手続き以上のリスク対策が必要
なりすまし、偽造証明書、反社チェックへの対応

	口座開設 身元確認	残高照会 当人確認	送金 当人確認
物理社会	本人確認証明書 郵送確認	カード 暗証番号	カード 送金先 送金金額 暗証番号
デジタル社会	【技術強度】 eKYCアプリ 顔認証 本人確認証明書 PINコード	【技術強度】 ログインID パスワード ＋ IPアドレス 銀行アプリ 携帯固有番号	【技術強度】 送金先 送金金額 暗証番号 ＋ ログインID 多要素認証 IPアドレス 銀行アプリ 携帯固有番号 セッション時間

時間経過とともに本人確認の精度が落ちていく（継続的顧客管理の必要性）

"On the Internet, nobody knows you're a dog."

出典：Wikipedia: On the Internet, nobody knows you‘re a dog

7．匿名性の担保（Anonymization vs Pseudonymization）

※ISO/IEC27701(PIMS）関連文書参照

Anonymization　　一方向

名前：日電太郎
ID:12345
年齢：20
住所：東京都港区
職業：学生
趣味：音楽鑑賞

→

名前：****
ID:*****
年齢：20
住所：*****
職業：学生
趣味：音楽鑑賞

VS

Pseudonymization(※)　　双方向

名前：日電太郎
ID:12345
年齢：20
住所：東京都港区
職業：学生
趣味：音楽鑑賞

de-link →
← link

名前：日本二郎
ID: 85479
年齢：20
住所：大阪府大阪市
職業：学生
趣味：音楽鑑賞

Re-identification

一旦、Anonymizationされたデータは元に戻せない

Pseudonymizationは暗号技術によりデータは元に戻せる
また、匿名性の担保がしやすい。

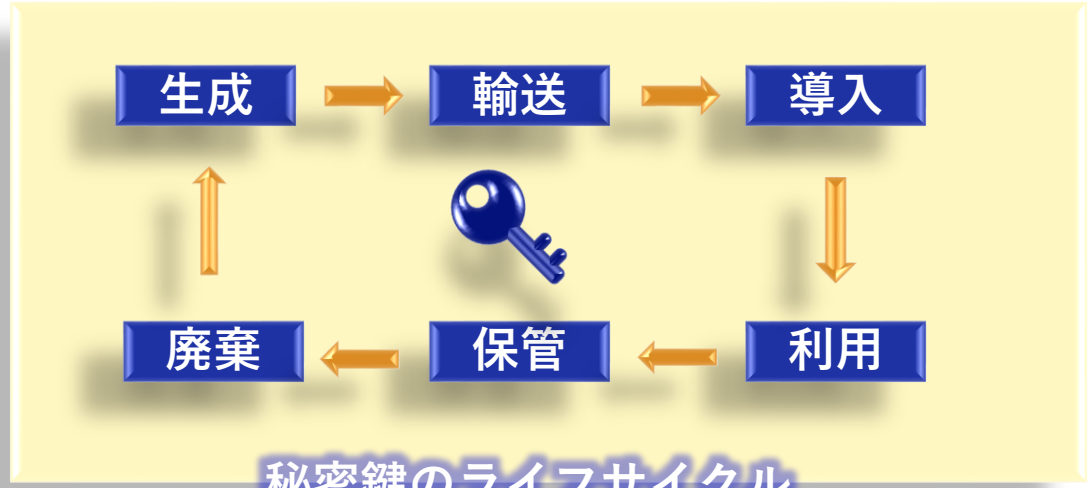
【ご参考：Tokenization 】

PCI-DSS(クレジットカード業界のセキュリティスタンダード)
で採用されている、カード情報をトークン化し無価値化する方式

【ポイント】
CBDCの匿名性を担保するには、de-link/link を国際的な枠組みの中で法的な手続きによって実行されることが重要である。その際、KYCで確実に本人確認することが必須要件となる。

8．PKI（公開鍵暗号基盤）活用時の秘密鍵管理

- PKIにおける秘密鍵の管理（ライフサイクル管理）、特に紛失時の復活を秘密鍵と公開鍵の組み合わせでどのように有効的に実施するか？　（HSMの有効性の検討）
- 秘密鍵が漏洩した場合は単純に「失効からの再発行」手続きで対応できるか？（運用課題）
- スマホを活用するにしても、紛失時の復活や機種変更手続きにおける不正排除などリスクがある。（スマホによるeKYCの有効活用は有用なソリューション）



秘密鍵のライフサイクル

秘密鍵の保管場所

9．まとめ

- NIST SP800-63はデジタルアイデンティティのスタンダード
- 本人確認は身元確認と当人確認で行う
- 保証レベルはリスクベースで考える
- 匿名化にも種類と特徴がある
- 秘密鍵の保管の課題は技術と運用面で検討が必要


Orchestrating a brighter world
NEC