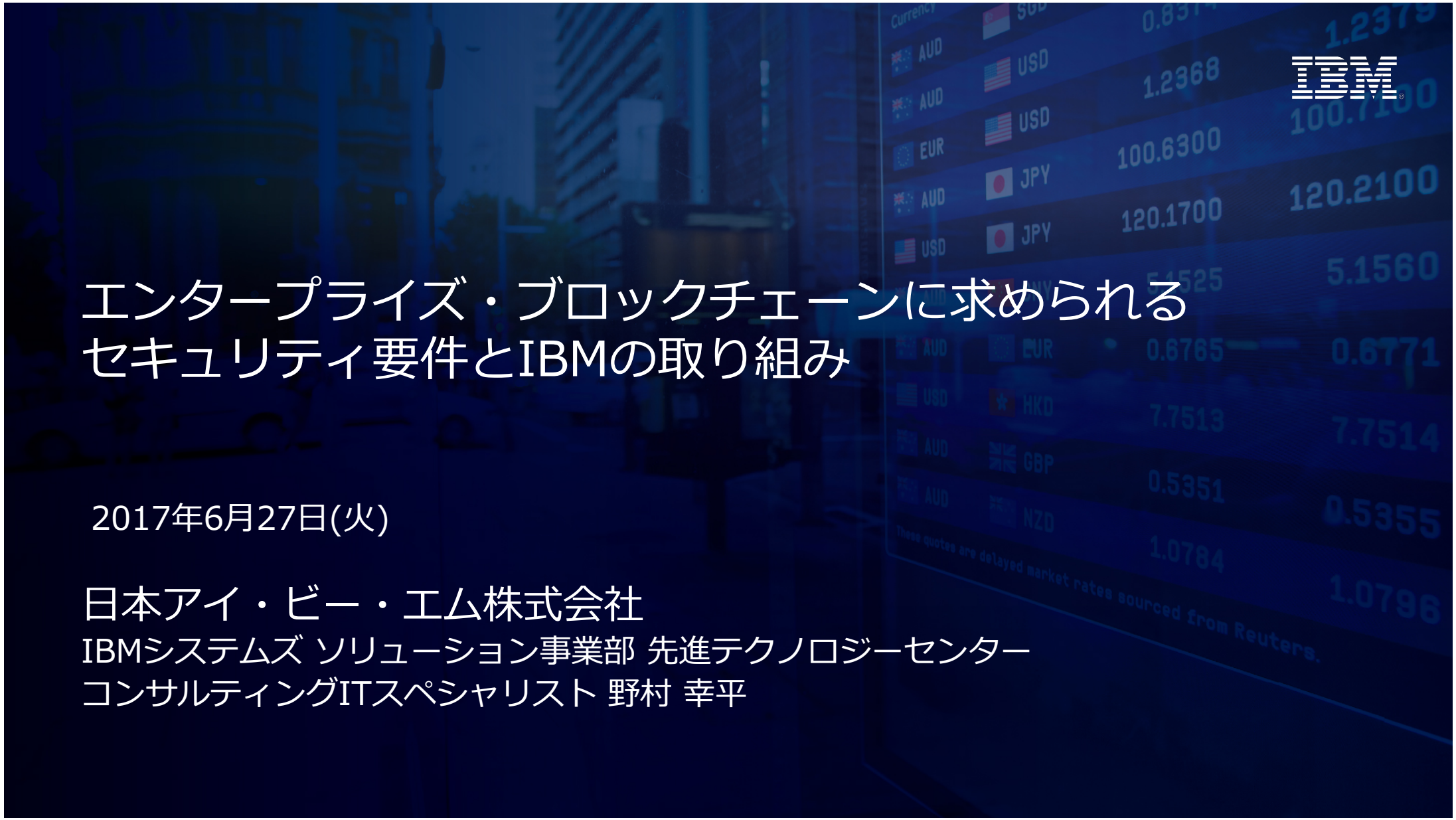


エンタープライズ・ブロックチェーンに求められるセキュリティ要件とIBMの取り組み

2017年6月27日(火)

日本アイ・ビー・エム株式会社
IBMシステムズ ソリューション事業部 先進テクノロジーセンター
コンサルティングITスペシャリスト 野村 幸平

エンタープライズ・ブロックチェーンの セキュリティ要件

IBMの目指すブロックチェーン

bitcoin

- 政府などにより規制されない、転々流通可能な仮想通貨
- 誰でもビットコインネットワークに参加可能 (Public Network)
- Proof of Work(マイニング)による合意形成

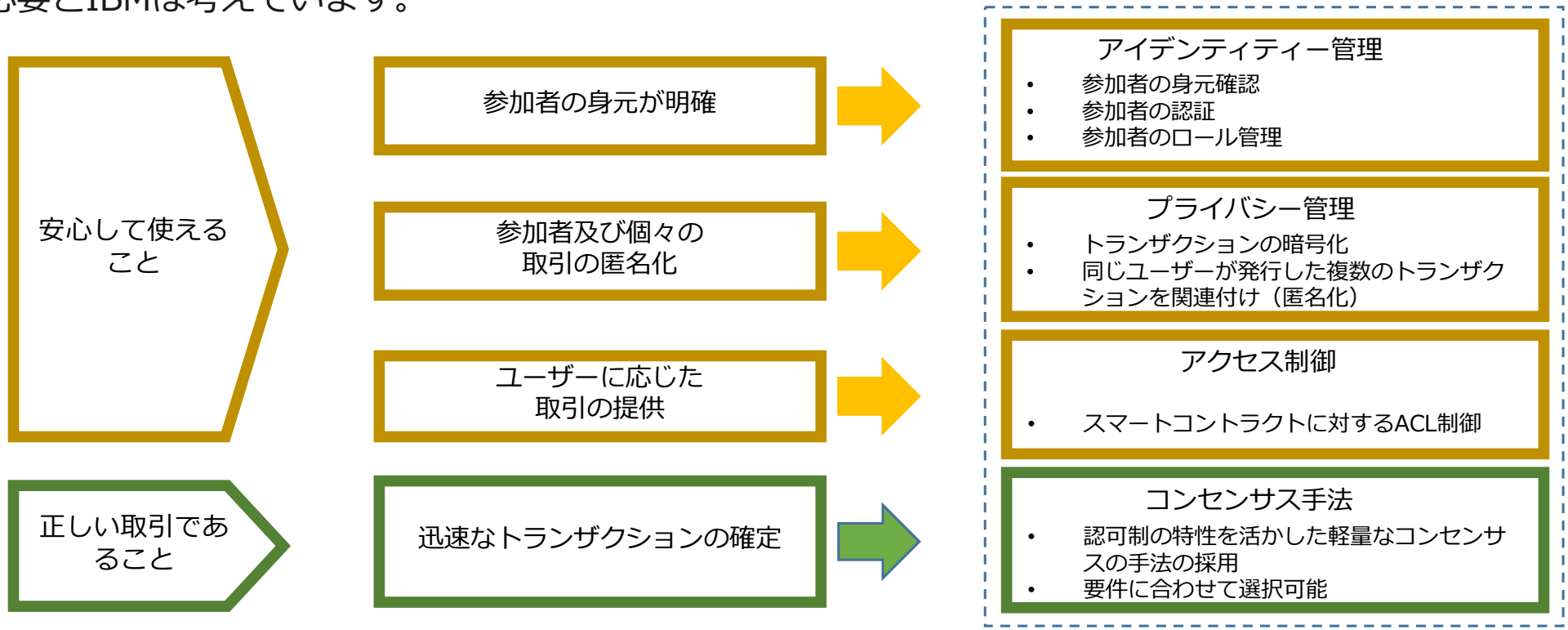
IBMの目指すブロックチェーン

- コンソーシアムなどのビジネスネットワークの中で、組織をまたがる業務に適用
- 許可制 ネットワーク
- 高い処理性能（スループットとレスポンス)

エンタープライズ向けブロックチェーンのセキュリティ要件

企業がビジネスでブロックチェーンを使用していくためには、
「安心して使えること」　参加者が特定できかつ取引の機密は守られる
「正しい取引であること」一度確定した取引が変更や取り消しされない
が必要とIBMは考えています。

要件 → **許可制ブロックチェーン**



エンタープライズ向けブロックチェーンにむけて

IBMの取り組み：Hyperledger Project

LINUX FOUNDATION
HYPERLEDGER PROJECT

- 2015年12月にアナウンスメント
  - 2017年6月現在 +130社
- 標準化の中で、先進的なブロックチェーン技術を推進
- IBM：発足メンバー
  - 45,000行に及ぶコードを寄贈
  - 技術ステアリング・コミッティーの初代議長（Chris Ferris）

プレミア会員

accenture, AIRBUS, AMERICAN EXPRESS, CHANGE HEALTHCARE, CME Group, DAIMLER, Digital Asset, DTCC, FUJITSU, HITACHI Inspire the Next, IBM, intel, J.P.Morgan, NEC, r3, SAP

一般会員

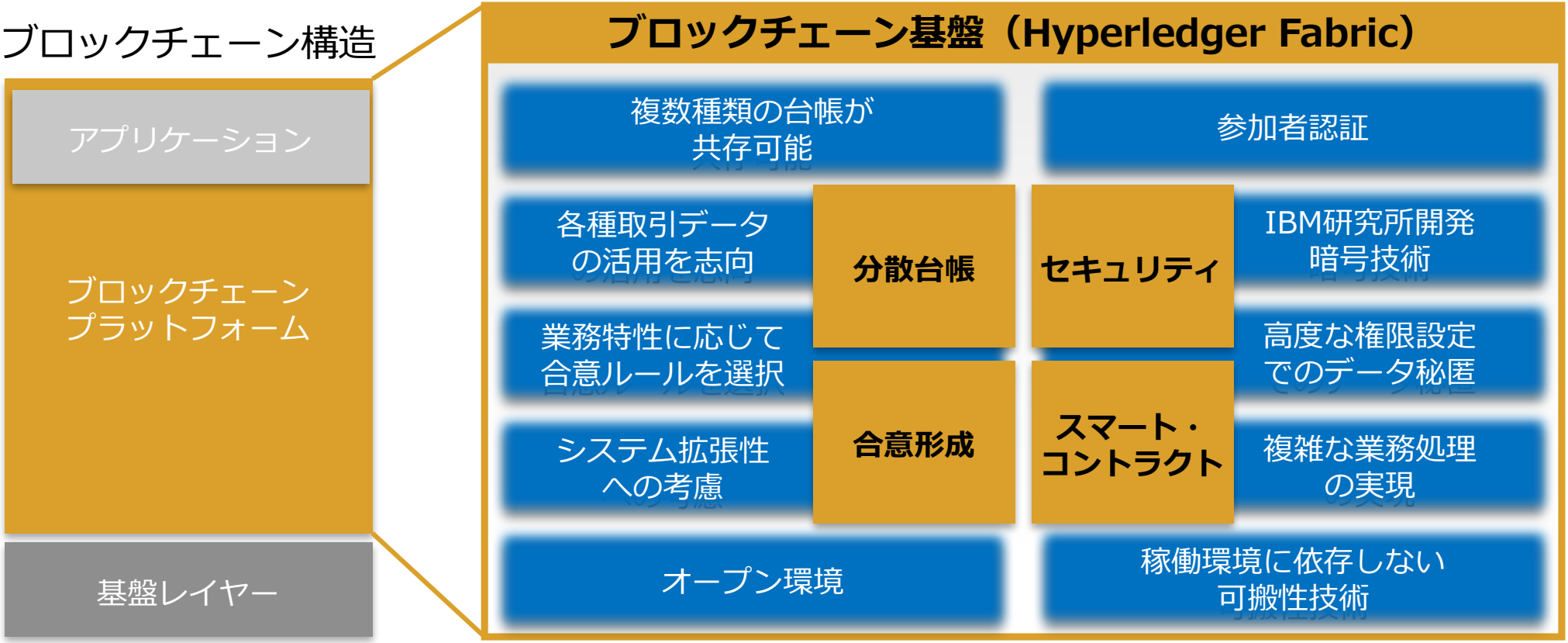
ブロックチェーンの構造と「追加で検討すべきセキュリティ要件」

Hyperledger Fabricによる
セキュリティ対策

Hyperledger Fabric の位置づけ

- ミドルウエア的位置づけ
- 利用される各分野で共通に必要とされるBlockchain技術を実装
- オープンなコミュニティでの開発体制

ブロックチェーン構造



Hyperledger Fabricの４つの技術要素

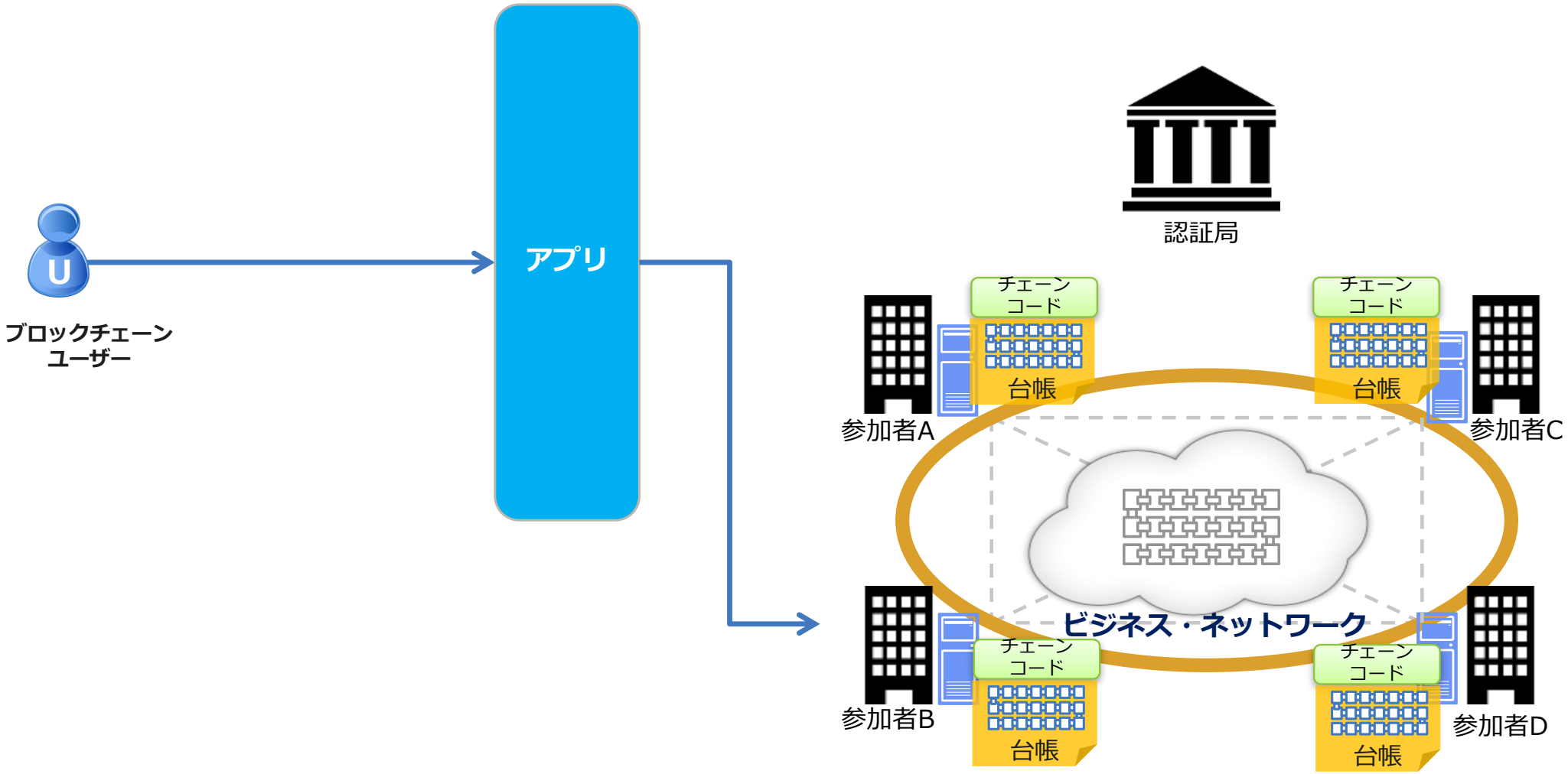
• Hyperledger Fabricは以下の４つの主な技術要素から成り立っています

ビジネス・ネットワーク上の参加者間で共有される取引データ台帳	分散台帳	セキュリティー	電子署名や認証機能により参加者間の匿名性を確保したり取引内容のプライバシーを保護する仕組み
分散ノード間で取引の完全性をシステム的に検証し保障する仕組み	合意形成	スマート・コントラクト	ビジネス・ロジックによる処理の自動化や、柔軟な台帳の活用を実現する為の仕組み

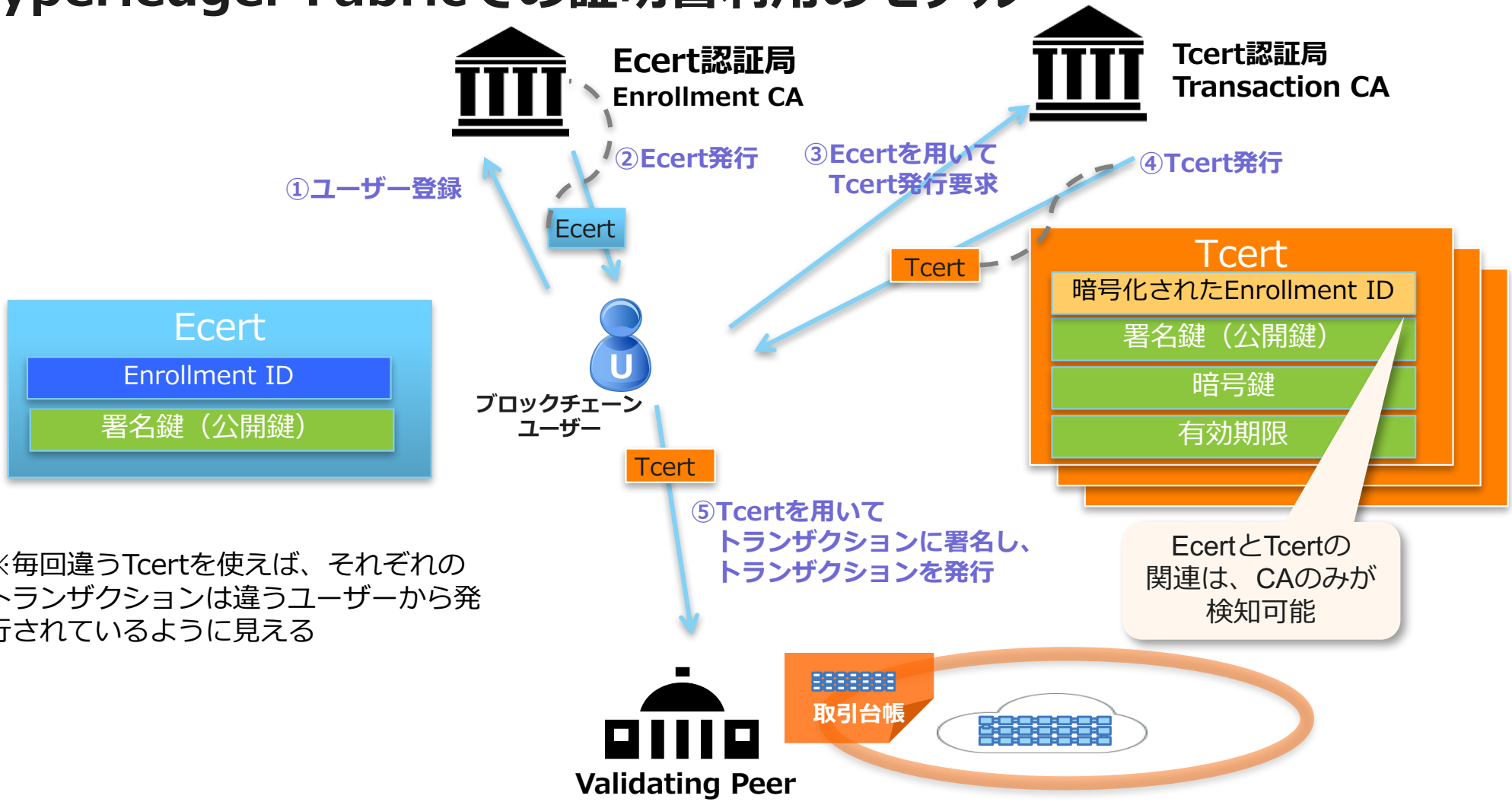
本日のトピック： セキュリティー

ビジネス・ネットワーク上の参加者間で共有される取引データ台帳	分散台帳	セキュリティー	電子署名や認証機能により参加者間の匿名性を確保したり取引内容のプライバシーを保護する仕組み
分散ノード間で取引の完全性をシステム的に検証し保障する仕組み	合意形成	スマート・コントラクト	ビジネス・ロジックによる処理の自動化や、柔軟な台帳の活用を実現する為の仕組み

Hyperledger Fabricにおける参加者とビジネス・ネットワーク構造

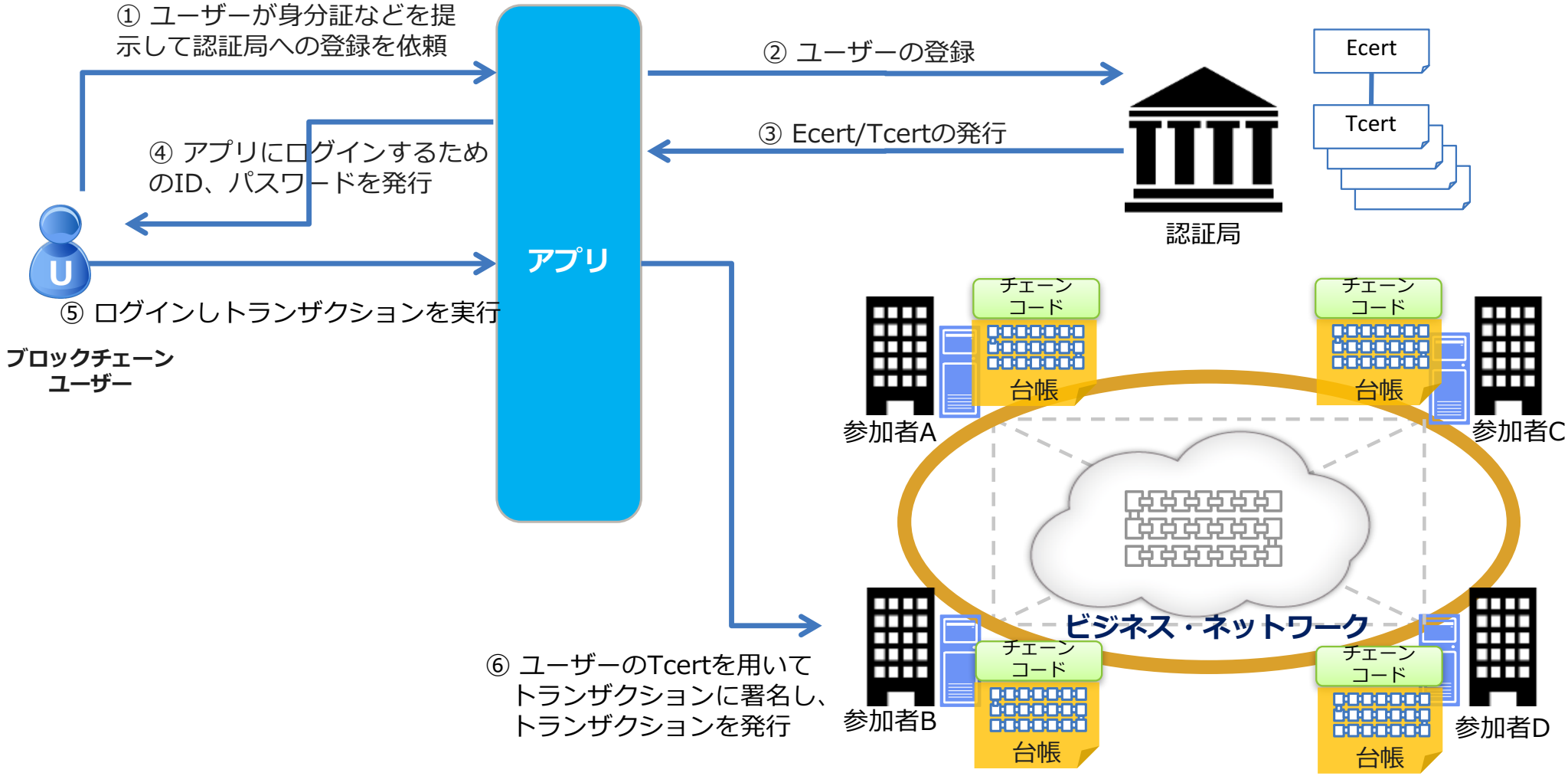


Hyperledger Fabricでの証明書利用のモデル



※毎回違うTcertを使えば、それぞれのトランザクションは違うユーザーから発行されているように見える

Hyperledger Fabricのセキュリティを考慮したトランザクション・フロー



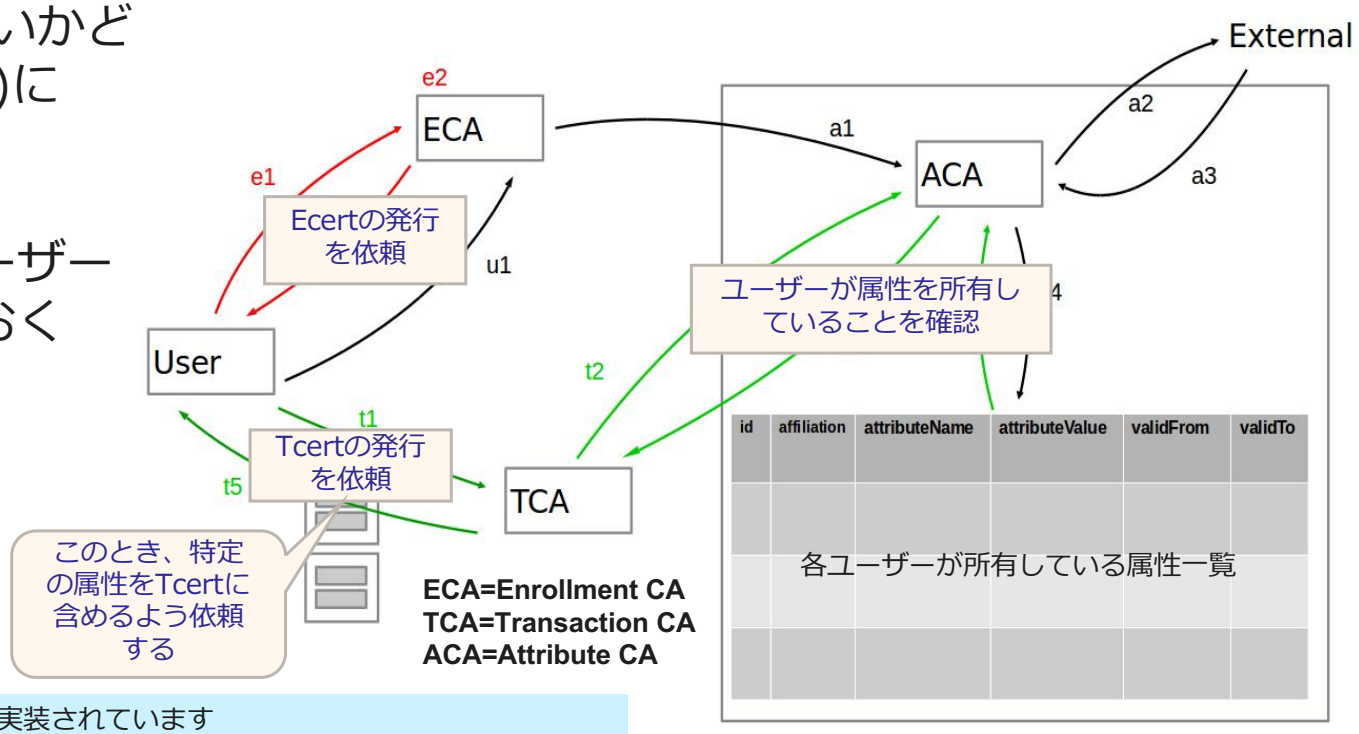
参考：Attribute Based Access Control (ABAC)によるアクセス制限

- **属性を用いることで、ロールベースのアクセス制御が可能になります**

✓特定の属性を含むTcertをもつユーザーだけに、アクセスを許可する

✓ある属性をTcertに入れてよいかどうかは、Attribute CA(ACA)によって判断される

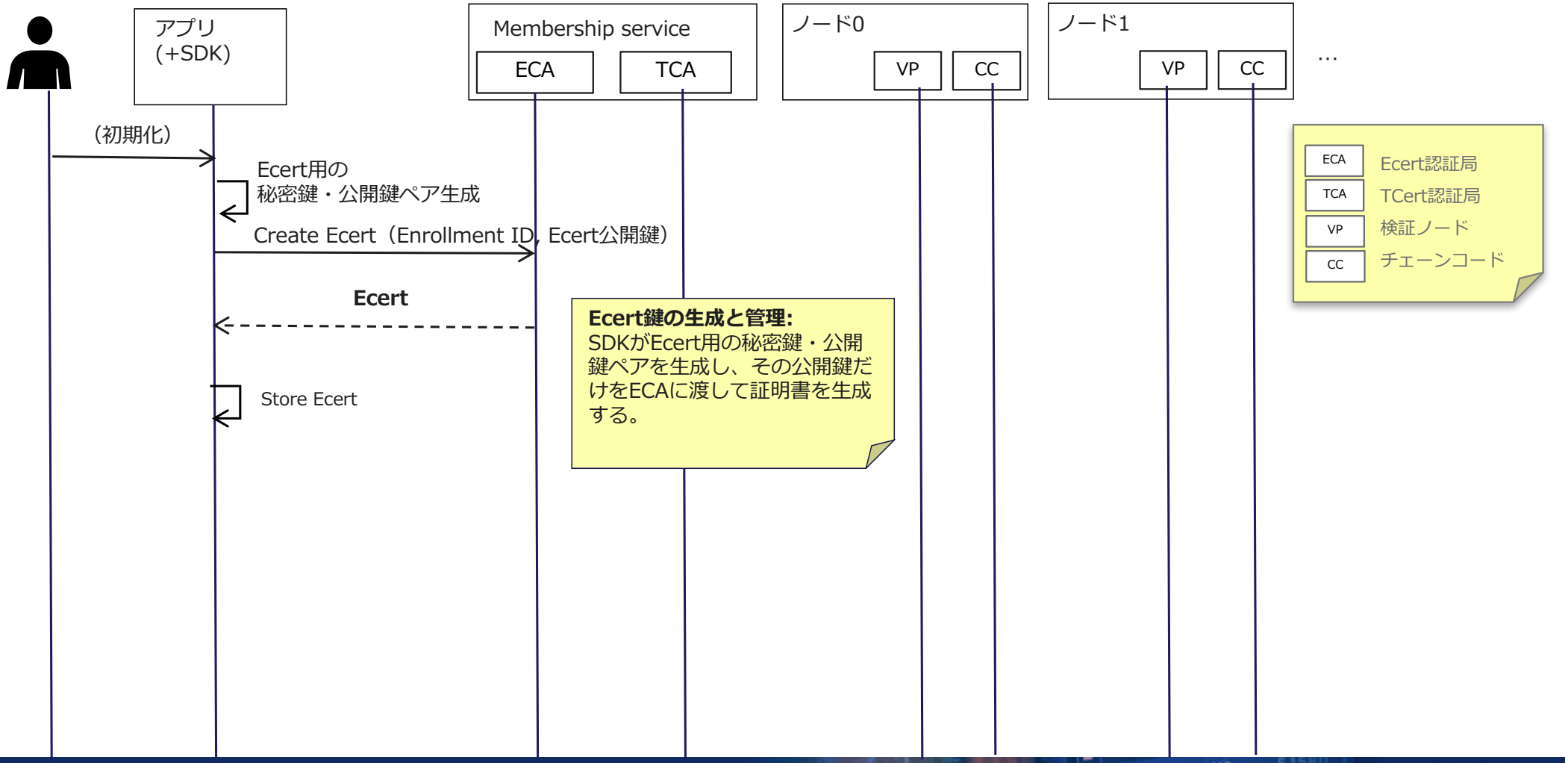
✓ACAには、あらかじめ各ユーザーに許可する属性を保存しておく



引用：Attribute Based Access Control
http://hyperledger-fabric.readthedocs.io/en/stable/tech/attributes/

この仕組みは、サンプルコード"asset_management02"に実装されています
https://github.com/hyperledger/fabric/tree/v0.6/examples/chaincode/go/asset_management02

参考：Hyperledger Fabricでの証明書利用（1）Ecert発行



参考：Hyperledger Fabricでの証明書利用 (2) トランザクション実行時