1. システム構成

   - ユースケース１ ファンド・SSI・法人基礎情報の共有　の構成
   - ユースケース２ 公販ネットワークの非互換の課題解決　の構成
   - ユースケース３ 株券貸借取引における貸借料・担保金利および配当金相当額の情報共有　の構成

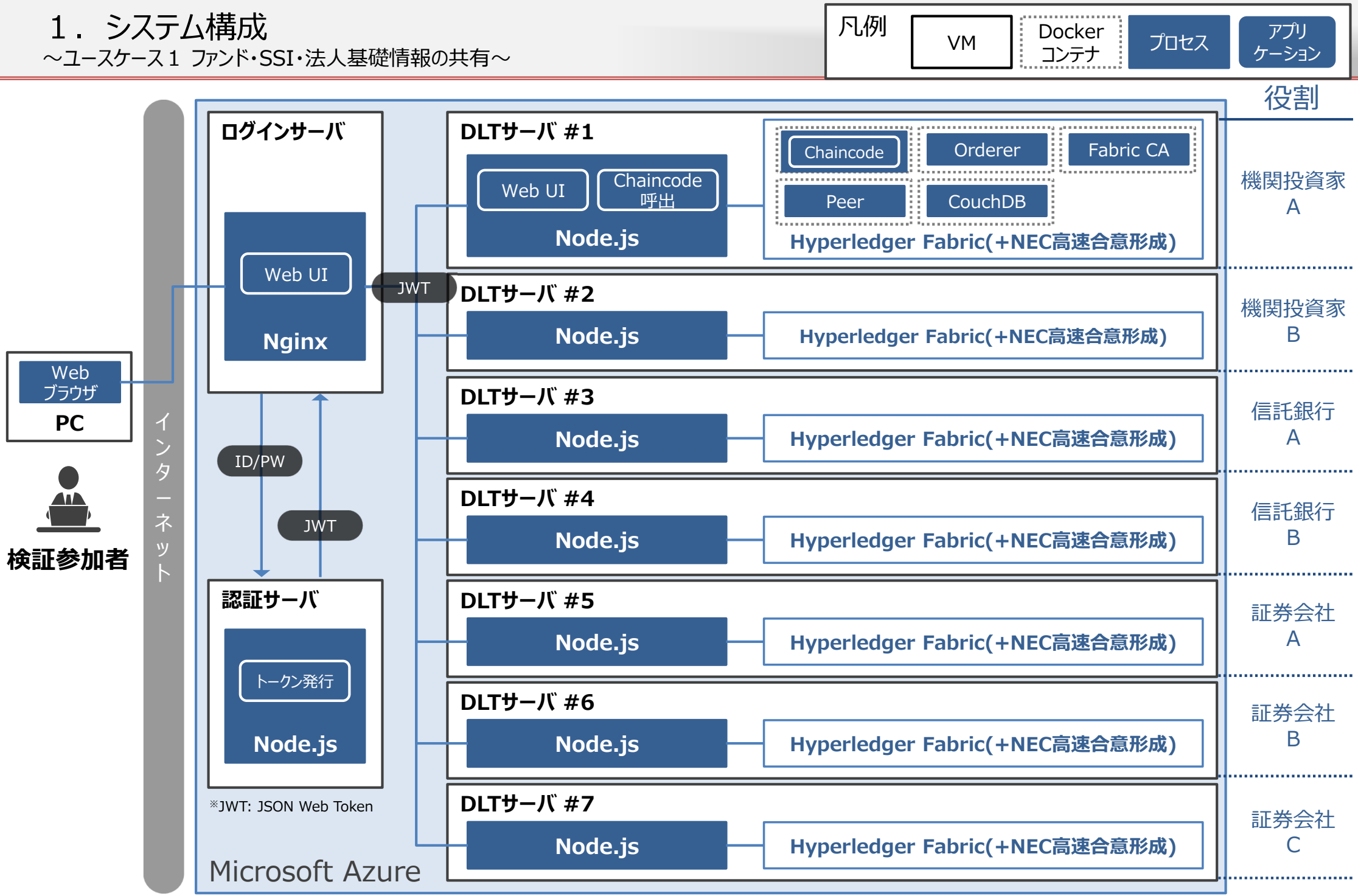
2. ソフトウェアスタック

3. データ共有範囲

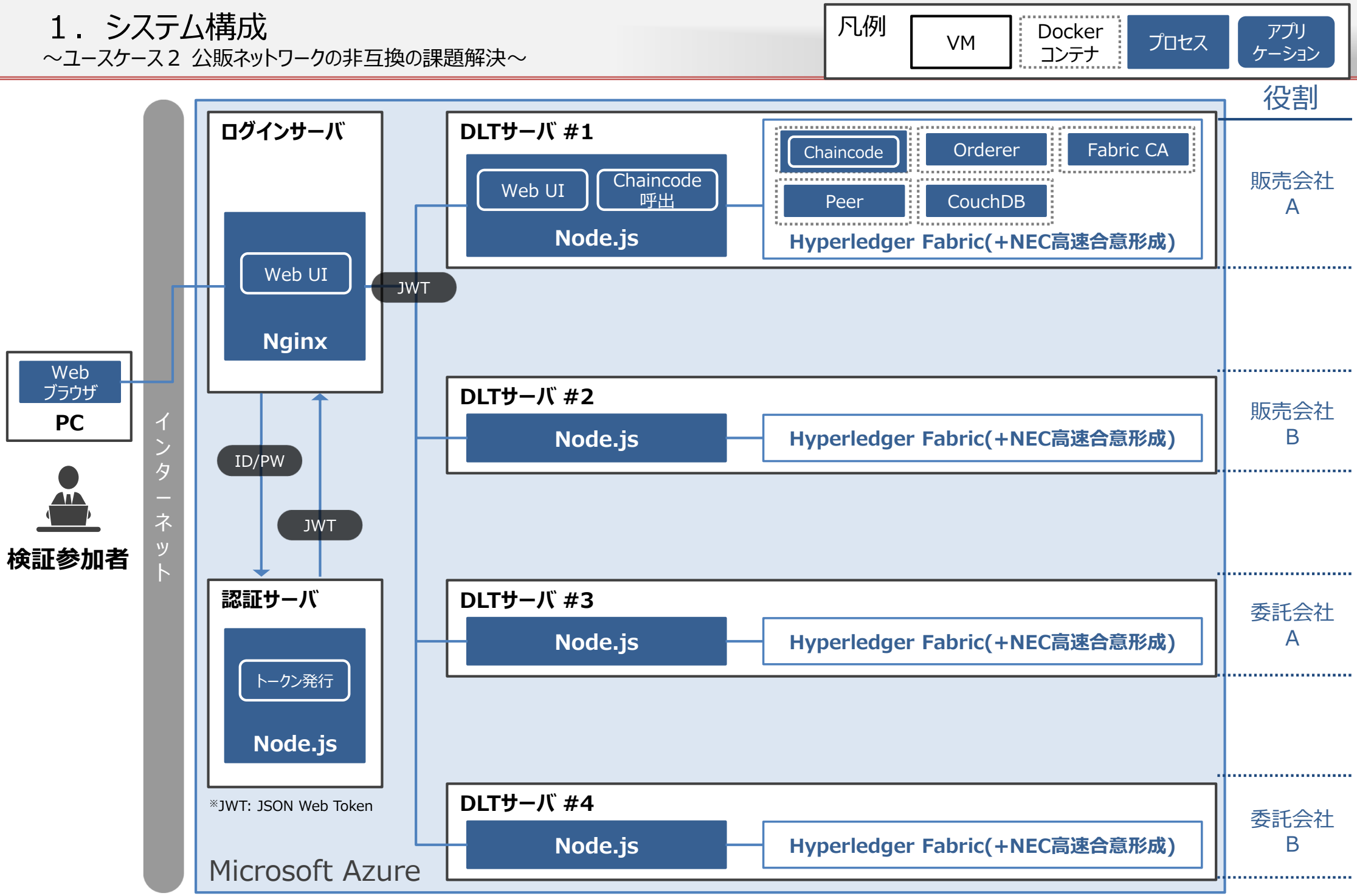
4. （補足）Private Data機能概要

1．システム構成

～ユースケース１ ファンド・SSI・法人基礎情報の共有～

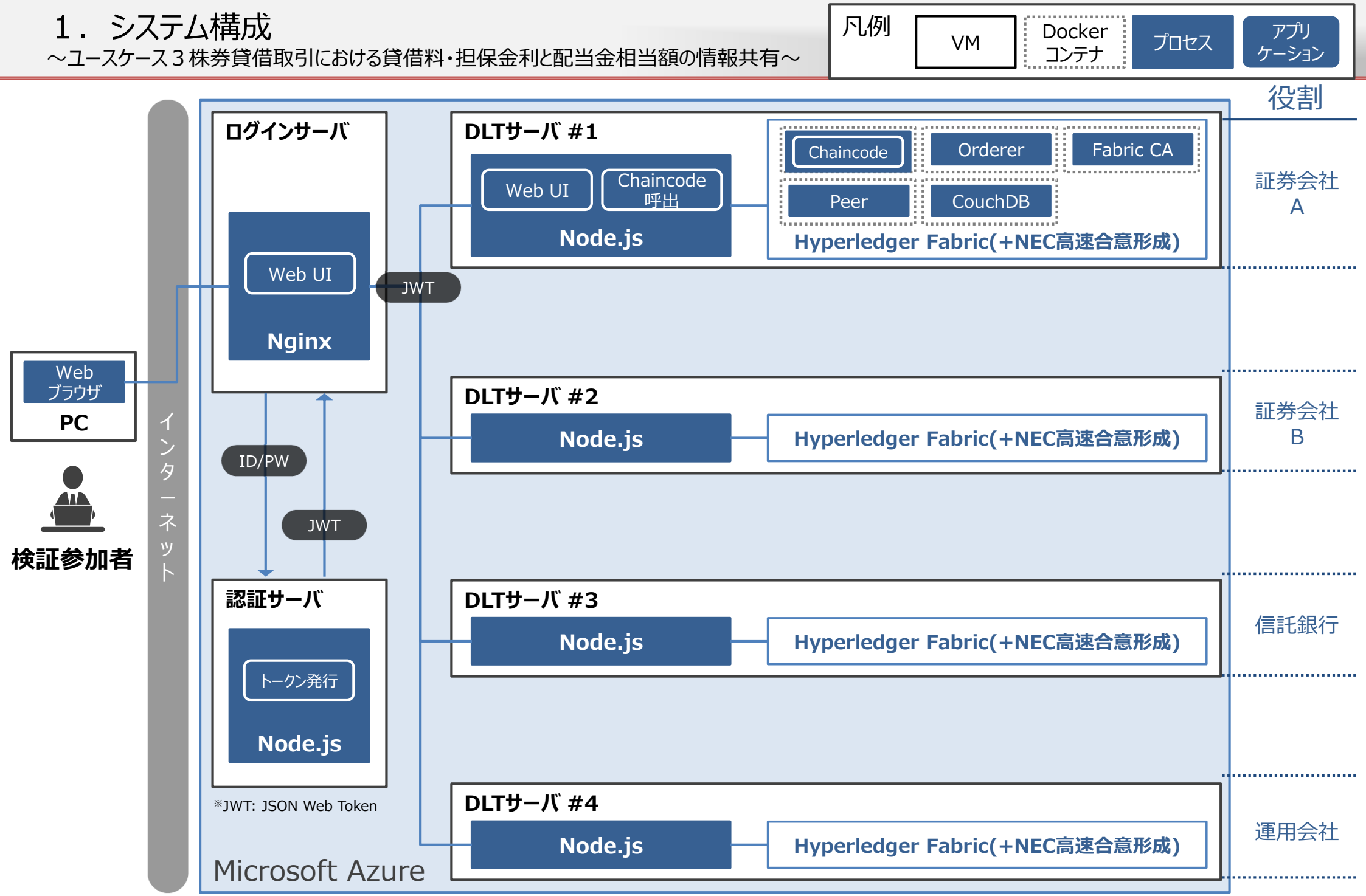


1．システム構成
～ユースケース２ 公販ネットワークの非互換の課題解決～

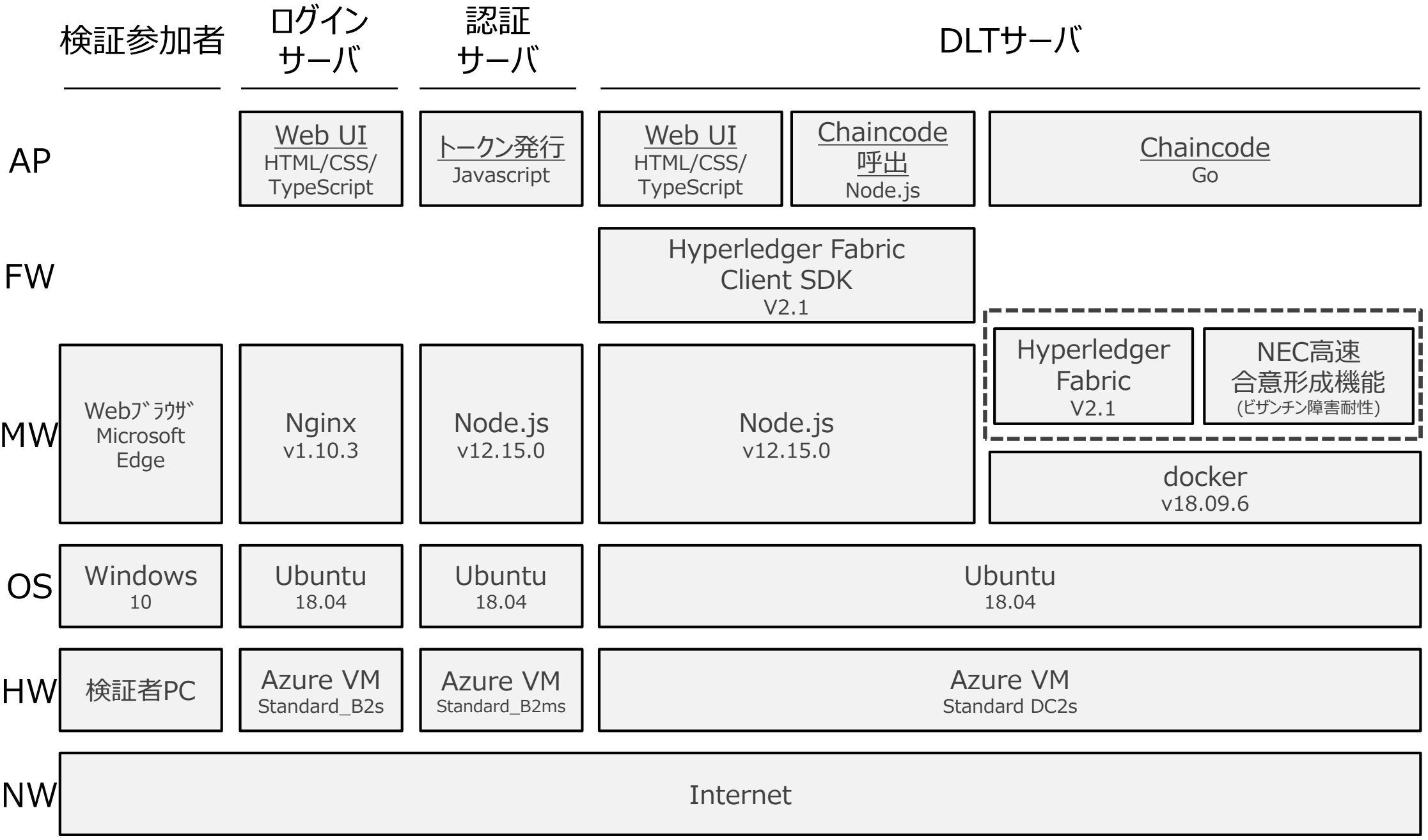


1．システム構成

～ユースケース３株券貸借取引における貸借料・担保金利と配当金相当額の情報共有～



2．ソフトウェアスタック



3．データ共有範囲

- Hyperledger FabricのPrivate Data機能にて各データ属性に応じたアクセスコントロールを設定
- Private Dataの組み合わせ(データ共有範囲の設定)は任意であり、サービス運用中の動的更新も可能

実施した3ユースケースにおけるPrivate Dataの組み合わせは以下の通り。

ユースケース１
ファンド・SSI・法人基礎情報の共有

データ	共有範囲
ファンド情報	全参加者間
SSI情報	※1 取引当事者間

※1
機関投資家**1**社：信託銀行**1**社：証券会社**N**社の組み合わせ

例）
機関投資家A：信託銀行B：証券会社C
機関投資家A：信託銀行A：証券会社A/B

ユースケース２
公販ネットワークの非互換の課題解決

データ	共有範囲
設定・解約	※2 取引当事者間
基準価額	※2 取引当事者間
申込不可日	※2 取引当事者間

※2
販売会社**1**社：委託会社**1**社の組み合わせ

例）
販売会社A：委託会社A
販売会社B：委託会社A

ユースケース３
株券貸借取引における貸借料・担保金利および配当金相当額の情報共有

データ	共有範囲
約定	※3 取引当事者間
貸借料計算結果	※3 取引当事者間

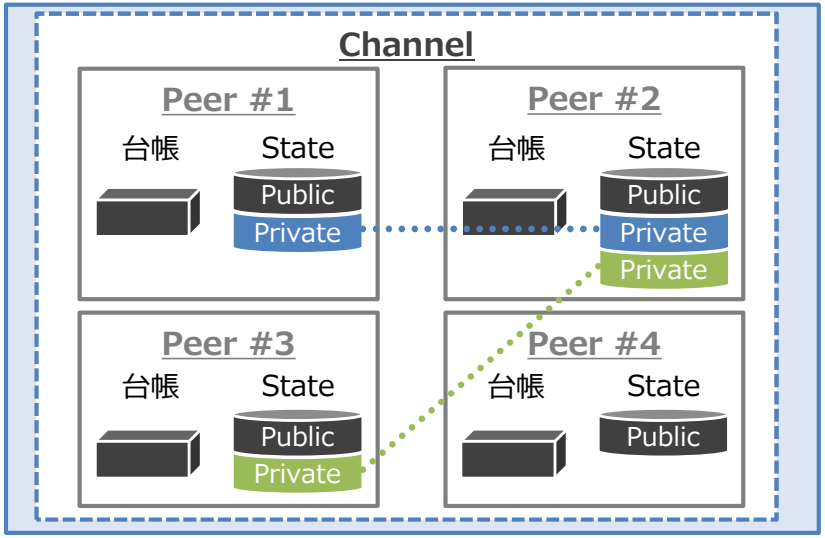
※3
証券会社**1**社：証券会社/信託銀行/運用会社**1**社の組み合わせ

例）
証券会社A：証券会社B
証券会社B：信託銀行

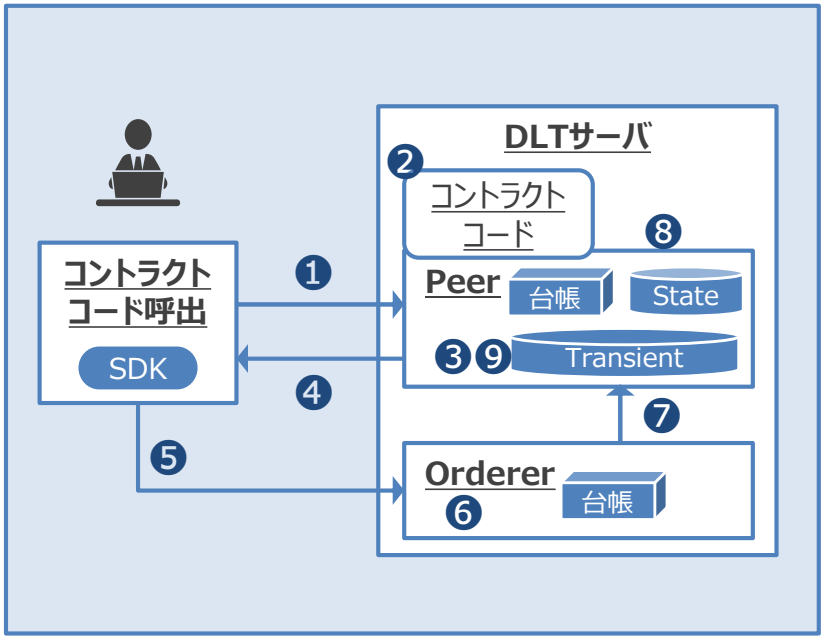
4．（補足）Private Data機能概要

- Private Dataとは、指定したDLTノード（Peer）間でのみ取引の内容（トランザクション）を共有する機能

- Hyperledger Fabricでは基本的にChannel(≒ユースケース)を分けることでデータ秘匿化する
- Channelに所属している組織全てではなく、一部の組織間でのみデータを共有したい場合には次の理由からChannel分割ではなく、Private Dataを活用することが望ましい
  - ✓ 別のChannelを作成する場合、管理コストが増える(Channel作成、ポリシー作成、コントラクトコードのデプロイ作業等)
  - ✓ Channelに所属するOrdererには取引の内容が見える可能性がある
- Private Dataは指定したPeer間でのみ取引の内容を共有し、取引のハッシュ値のみをブロックチェーンに記録(参加者全員に共有)する
  - ✓ Private DataはGossip Protocolを介して、許可されたPeer間でのみ通信する
  - ✓ 同一Channel上の他の許可されていないPeerを含め、Ordererも取引の内容を見ることができない
  - ✓ ハッシュ値はブロックにコミットされるため、Private Dataのやり取りをなかったことにすることはできない



- Private Dataを含んだ取引のフローは以下の順番で実行される
  - ❶ ユーザはコントラクトコード呼出アプリケーション経由で、トランザクションをPeerに送信し、コントラクトコードの仮実行を要求する。
  - ❷ Peerはトランザクション内のユーザの署名および自身がPrivate Dataの共有対象者か(Collection Policy)をチェックし、問題がなければコントラクトコードを仮実行する。
  - ❸ PeerはTransient Storeにデータを一時保存する。
  - ❹ Peerはコントラクトコードの実行結果をコントラクトコード呼出アプリケーションに返信する。(Private Dataはハッシュ値のみ返される)
  - ❺ ユーザはコントラクトコード呼出アプリケーション経由で、検証済みトランザクションをOrdererに送信し、トランザクションのコミットを要求する。
  - ❻ Ordererはブロックに入れるトランザクション群を合意形成し、ブロックを生成する。
  - ❼ Ordererはブロックを Peerに送信する。
  - ❽ Peerは受信したブロックおよびブロック内のトランザクションを検証し、問題がなければブロックをコミットする。この際、Transient Store内のPrivate Dataをハッシュ化し、ブロック内のトランザクションに含まれるPrivate Dataのハッシュ値と一致しているかを検証する。
  - ❾ Transient Store内のPrivate Dataは設定により一定時間で削除することが可能



https://hyperledger-fabric.readthedocs.io/en/release-2.1/private-data/private-data.html