資料６

SECURITIZE

パブリックブロックチェーンを活用した セキュリティトークン

2022年6月6日

Securitize Japan株式会社
森田 悟史

会社概要：Securitizeとは

- 2017年 - 創業、全ての資産をトークン化し、資本市場全体の効率化を実現を目指す
- 2019年 - デジタル証券に関わるTransfer Agentとして初めてSECに登録
- 2021年 - 6月、子会社のSecuritize Capitalを設立し、デジタル通貨ファンドの運用を開始予定
  - 9月、プライマリ、セカンダリ、BD機能を提供するSecuritize Marketsの稼働開始
  - 2021年末現在、米国を中心に200以上の顧客、約40万人の登録投資家をサポート
- 2022年 – Pacific Stock Transfer社を買収(登録企業3,000社、投資家口座数120万件)

社員

129	66	営業/マーケティング/管理者
	63	製品/エンジニアリング

拠点

本社:	サンフランシスコ
開発拠点:	テルアビブ｜ブエノスアイレス｜東京
その他拠点:	ニューヨーク｜マドリード ロンドン ｜東京

出資者

調達済み資金	$7,800万以上

AlgoCapital powering the borderless economy / BLOCKCHAIN CAPITAL / coinbase Ventures / GB Global Brain Corporation / Santander InnoVentures / Tomorrow, Together KDDI / MUFG / 三井不動産 Mitsui Fudosan / NOMURA / SBI Holdings / ripple / ソニーフィナンシャルベンチャーズ / TEZOS FOUNDATION / 三井住友信託銀行 SUMITOMO MITSUI TRUST BANK / NTT DATA

デジタル証券発行に必要な機能をトータルサポート

投資家
ダッシュボード

KYC/AML承認やウォレットの作成をはじめ、投資プロセス全体を通じて投資家が利用するツールを提供

デジタル証券

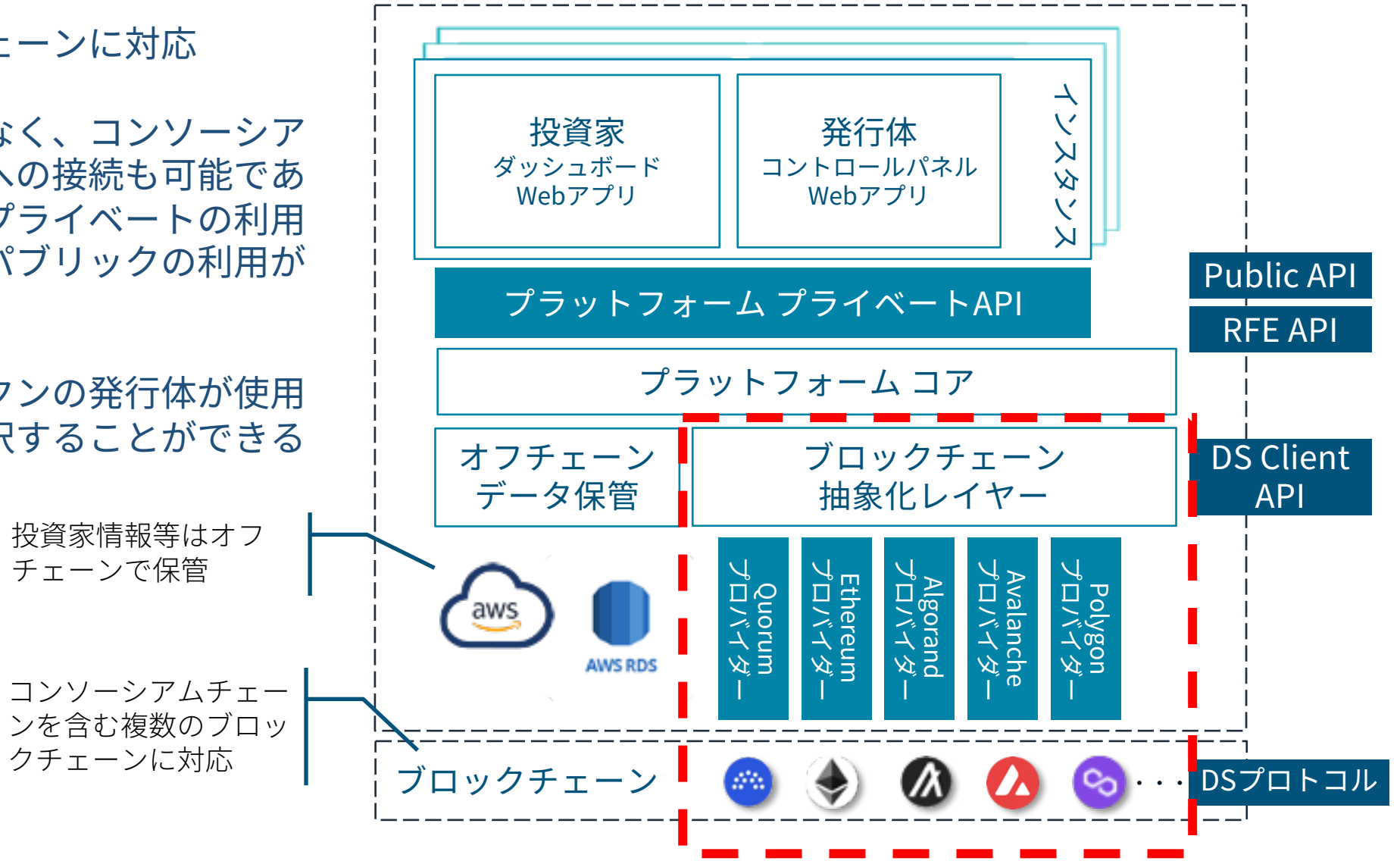
デジタル証券に対応する移転制限等が可能なスマートコントラクトの作成、発行

管理者
コントロールパネル

投資家およびデジタル証券のライフサイクル管理する発行体・証券会社・原簿管理者向けの機能を提供

Securitize PFの構造

- 複数のブロックチェーンに対応
- パブリックだけでなく、コンソーシアム、プライベートへの接続も可能であり、現状日本ではプライベートの利用が多く、米国ではパブリックの利用が多い
- セキュリティトークンの発行体が使用するチェーンを選択することができる



パブリックブロックチェーンを利用するための考慮

規制への対応はもちろん、投資家保護、攻撃への対策など考慮する必要があり、以下のような考慮ポイントがある。

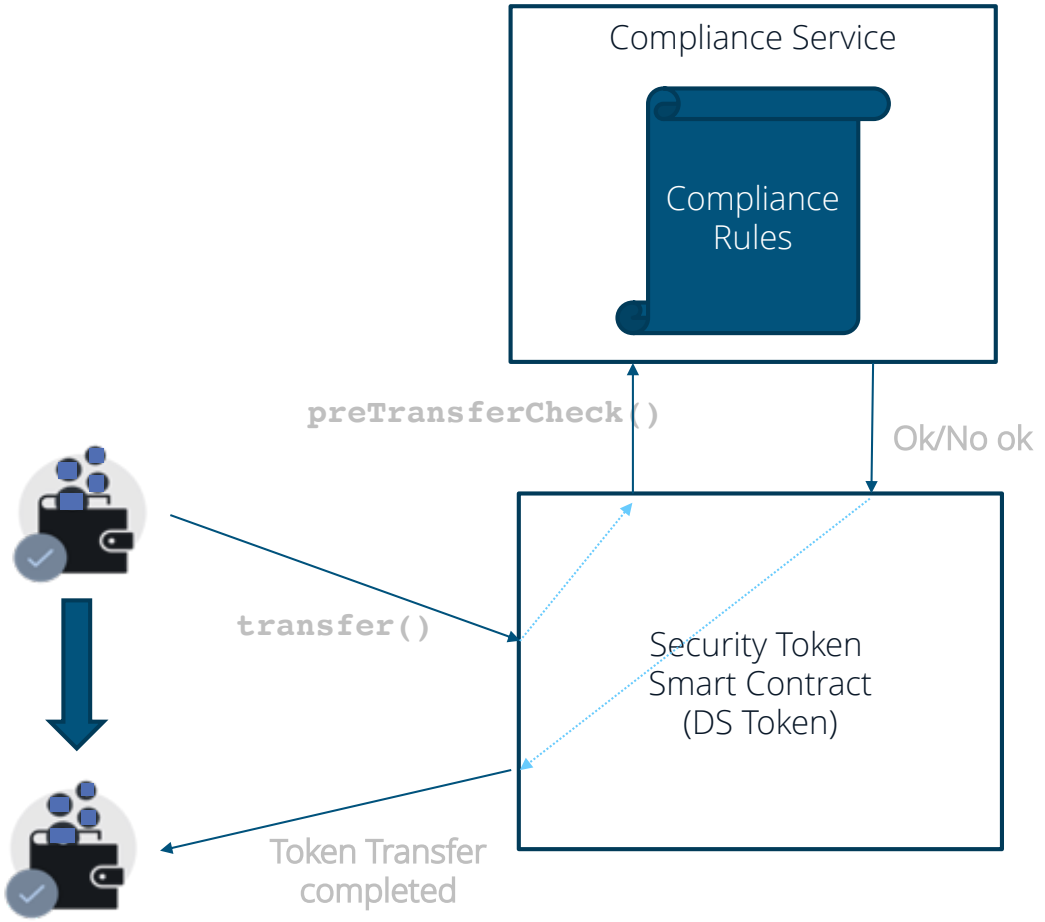
コントラクトへの攻撃の対応	スマートコントラクトを構成するプログラムにバグがあった場合に攻撃のリスクがあるため、スマートコントラクトの監査を受けている。（SecuritizeのDSトークンは2017年よりEthereum上での運用実績があり、安全性がある程度証明されている。） スマートコントラクトの実装方法として、ロジックとストレージを別のコントラクトに分けるアップグレード性を有した作りを採用しており、バグだけでなく、規制の変更等に伴うロジック変更に対応が可能。
意図しない流通への対応	様々なところで移転が発生する一方、コンプライアンスへの準拠が必須となるため、スマートコントラクトに移転制御の仕組みを組み込み、点々流通しないようになっている。ホワイトリストだけでなく、投資家の人数、居住国、適格性や、ロックアップ期間、保有量等による制限が可能。また、トークンの管理者権限により移転の停止や強制的な操作をすることが可能
プライバシー対応	世界中の不特定多数が接続しているため、個人情報などの秘匿性の高い情報はチェーン上には記録していない
特権機能の管理	セキュリティトークンには発行や償還、秘密鍵紛失者の救済措置などを行う特権機能が必要となるが、その特権機能を利用可能な特権的秘密鍵を適切に運用できるよう、複数登録・マルチシグ化・権限の階層化が可能となっている
ガスやフォーク対策	パブリックブロックチェーンの手数料はトークンの発行などの操作でも必要となるため、投資家による手数料負担のオプションなども選択できるようになっている。また、フォーク対策として、チェーン情報のDBへの同期まで待ち時間やデータの不整合が発生していないかのチェック、不整合発生時のアラームや緊急停止の仕組みなどを備える。

コンプライアンス制御の仕組み

意図しない流通への対応

- DSプロトコルのスマートコントラクトは、複数のコンプライアンス制限を保証します
  - ウォレットはKYCされたIDに割り当てる必要がある
  - ロックアップ期間中等、投資家による移転を制御する条件を設定
  - 投資家数はリアルタイムで更新され、移転時の人数制御等に利用される

```
 9    function transfer(address to, uint tokens) public returns (bool success);
10    function approve(address spender, uint tokens) public returns (bool success);
11    function transferFrom(address from, address to, uint tokens) public returns (bool success);
```

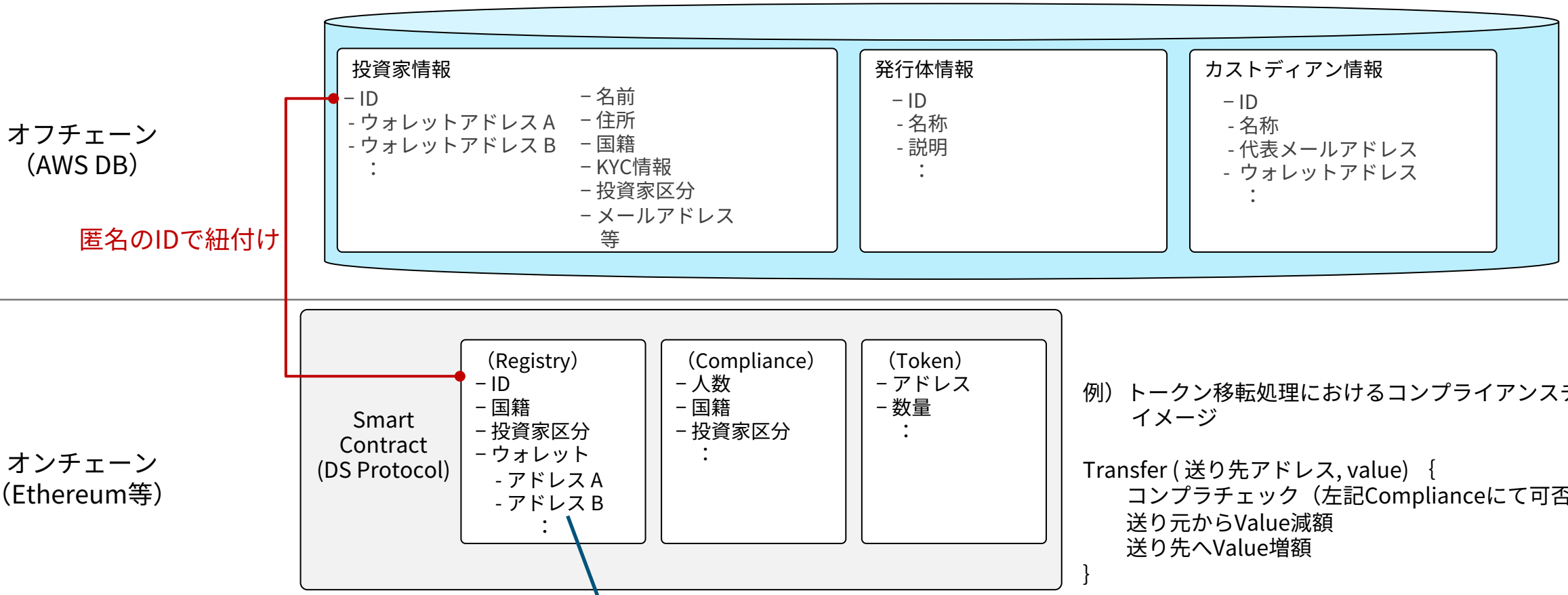


各アセットには、コンプライアンスを確保するためのスマートコントラクトが設定されています。

プライバシー対応

Securitize PF におけるデータ格納場所

Securitizeプラットフォームでは、ブロックチェーン上には原則個人情報等は格納せず、オフチェーンで管理している。
一部、セカンダリ市場など、複数のプラットフォームを横断してコンプライアンスを保つために必要な情報（国籍や投資家区分）はオンチェーン上で管理をしている。



例）トークン移転処理におけるコンプライアンスチェック
イメージ

```
Transfer ( 送り先アドレス, value)　{
　　コンプラチェック（左記Complianceにて可否確認）
　　送り元からValue減額
　　送り先へValue増額
}
```

秘密鍵の種類と権限

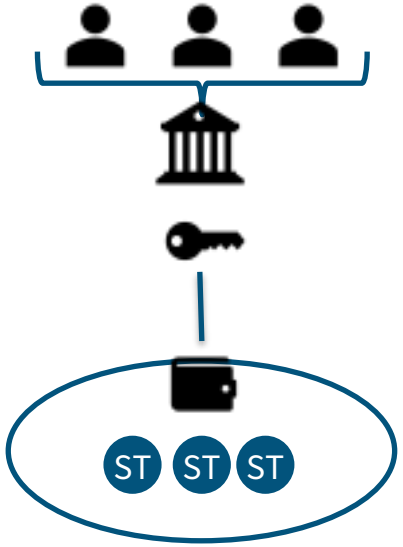
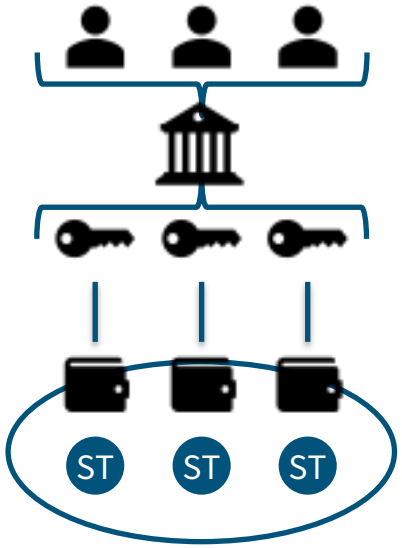
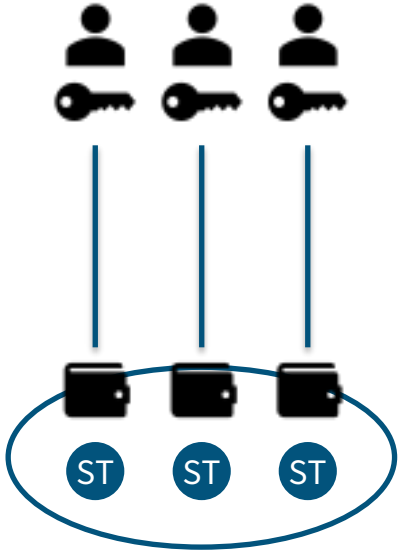
特権機能の管理

		マスター鍵	管理者鍵	ホワイトリスト登録鍵	投資家鍵
鍵の権限	スマートコントラクトのバージョンアップ	○			
	取引停止	○	○		
	管理者鍵の追加変更削除	○	○		
	トークンの発行・償還・その他特権的操作	○	○		
	ホワイトリスト鍵の追加変更削除	○	○	○	
	投資家アドレスのホワイトリスト登録	○	○	○	
	ST保有（保有制限の範囲内）				○
	ST移転（移転制限の範囲内）	○ （トレジャリー管理の場合）	○ （トレジャリー管理の場合）		○
管理方法		有事の際以外で取り出されることはない	管理者による管理：HWウォレット、ソフトウェアウォレット、ペーパーウォレット等 Securitizeによる管理：アカウントに紐付けるHSM管理	Securitizeプラットフォームに設定	次ページの通り

SECURITIZE

Securitizeが提供する投資家鍵の管理方法

ガス対策

	トレジャリー管理	中央管理	投資家自身による管理
トークン保管単位	単一の投資家群	投資家毎	投資家毎
秘密鍵管理者	なし	発行体、カストディアン等	投資家自身
投資家毎の残高	オフチェーン管理	オンチェーン管理	オンチェーン管理
移転時のコンプラチェック	オンチェーン （一部オフチェーン）	オンチェーン	オンチェーン
イメージ図			
管理コスト	低 ⟷ 高		

※それぞれの管理方法は発行後に移行可能

WWW.SECURITIZE.IO