

CSS2022

© Advanced IT Corporation 1

# 安心・安全な暗号資産取引基盤の提案

## SSVATF: Secure and Safe Virtual Asset Transfer Framework

2022年10月27日

**(株) IT企画 才所敏明**

(株)ZenmuTech  
 中央大学研究開発機構  
 toshiaki.saisho@advanced-it.co.jp  
 http://www.advanced-it.co.jp

**共 著 者**

**辻井重男**  
 中央大学研究開発機構

**櫻井幸一**  
 九州大学 大学院システム情報科学研究院  
 & サイバーセキュリティセンター  
 (株)国際電気通信基盤技術研究所

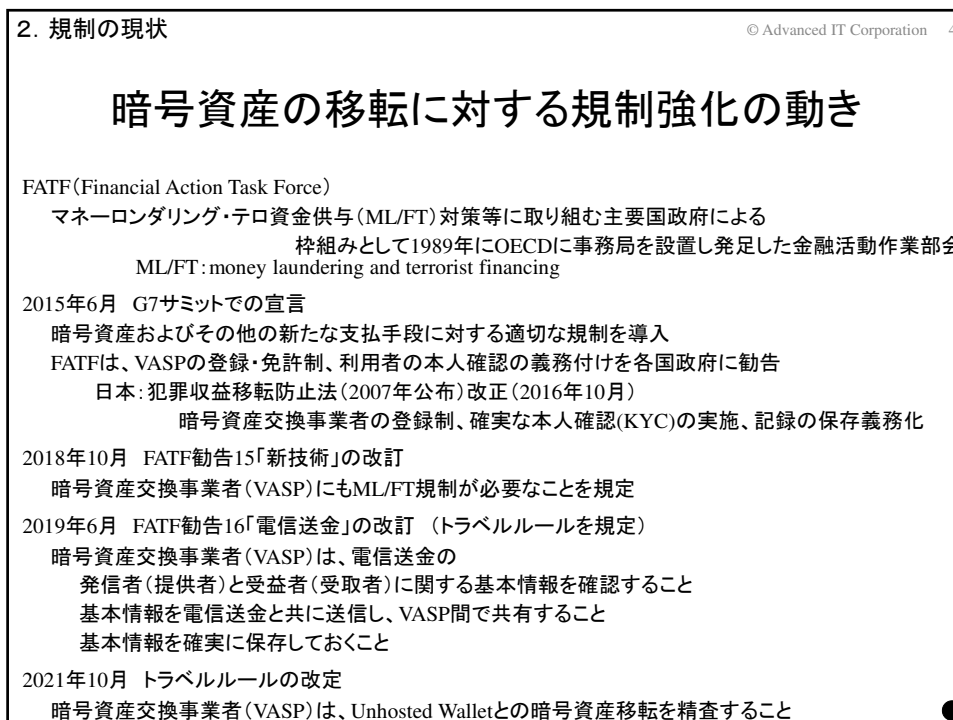
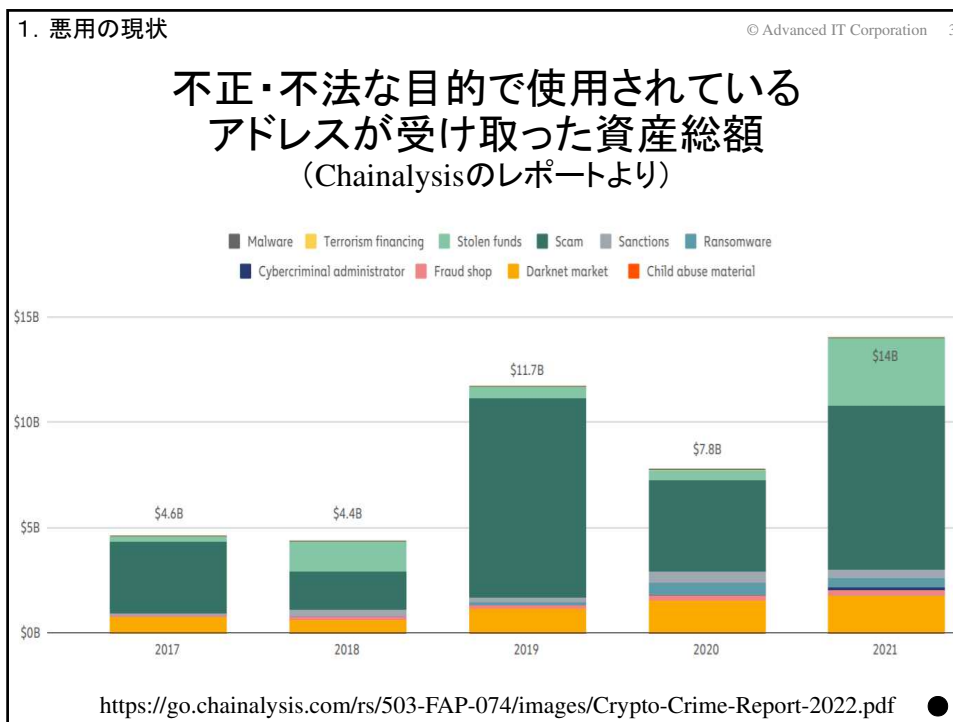
謝辞 本研究の一部は 一般財団法人テレコム先端技術研究支援センターの研究助成の支援を受けている。

CSS2022

© Advanced IT Corporation 2

**本日の発表内容**

1. 暗号資産の悪用の現状
2. 暗号資産の移転に対する規制強化の動き
3. 暗号資産業界の対応
4. 暗号資産に対する現状の規制の課題
5. 安心・安全で公正・公平な暗号資産移転を可能とする  
     暗号資産移転基盤SSVATF構想の紹介
6. SSVATF考察
7. 今後の検討課題



## 3. 業界の対応

© Advanced IT Corporation 5

## FATF16勧告(トラベルルール)への対応

## (1) VASP間通信の標準化

TRP: Travel Rule Protocol

メッセージフローの標準化 (OpenVASPが採用)

IVMS101: interVASP Messaging Standards

メッセージ形式の標準化 (OpenVASP、TRISA共に採用)

## (2) VASP間情報共有グループの形成

OpenVASP: OpenVASP Association

Blockchain-based Protocolによる信頼性確認

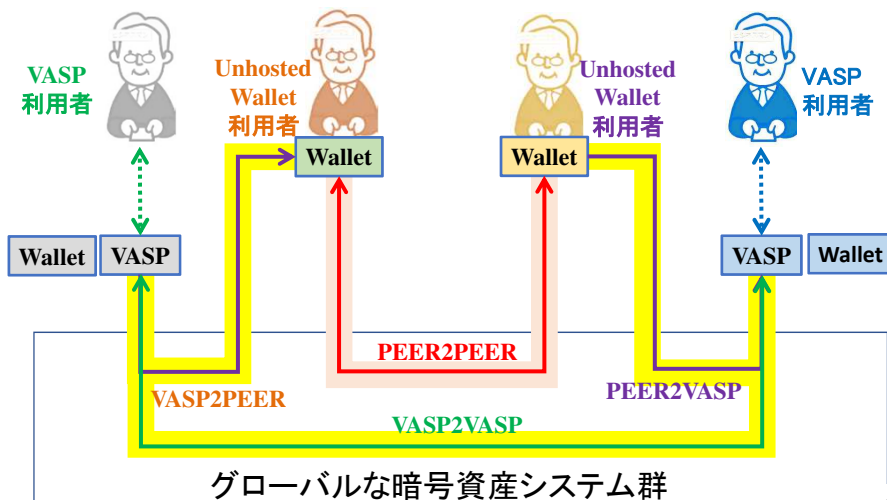
TRISA: Travel Rule Information Sharing Alliance

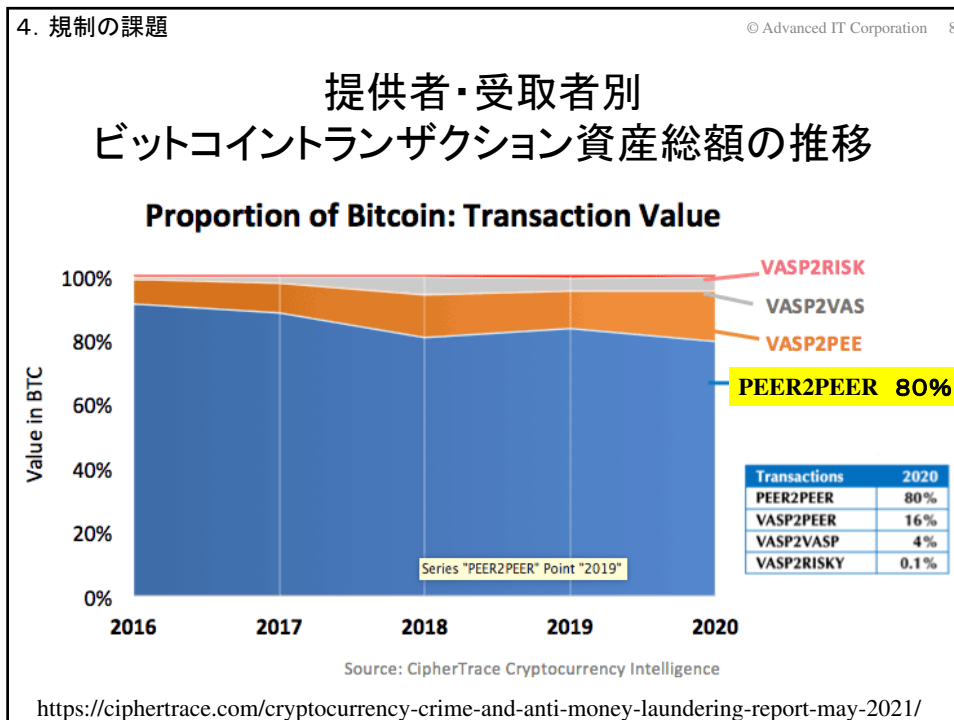
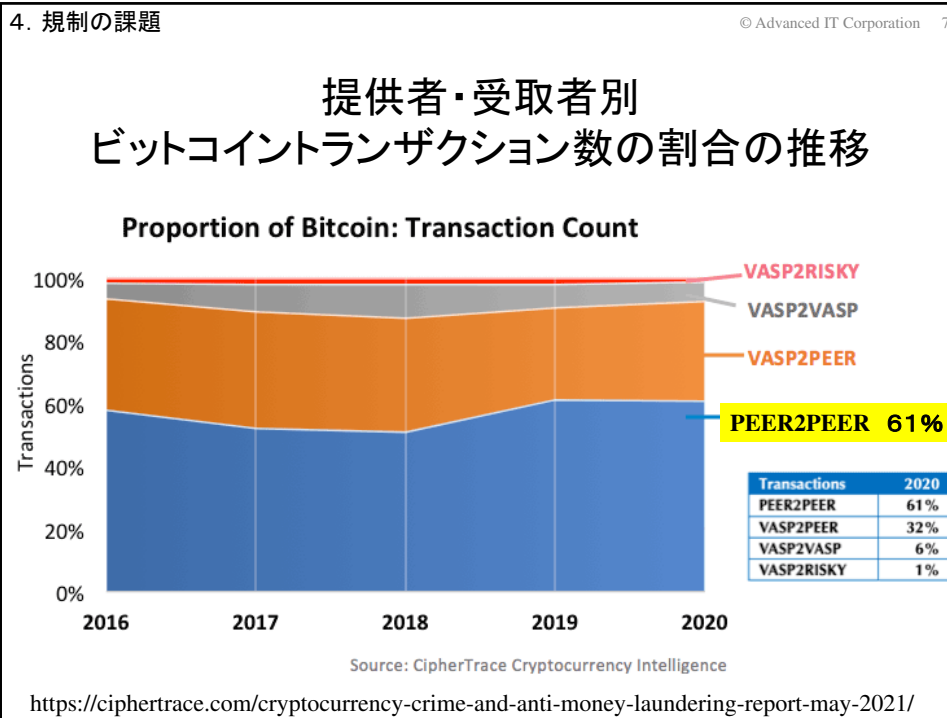
PKI-based Frameworkによる信頼性確認

● (3)

## 4. 規制の課題

© Advanced IT Corporation 6

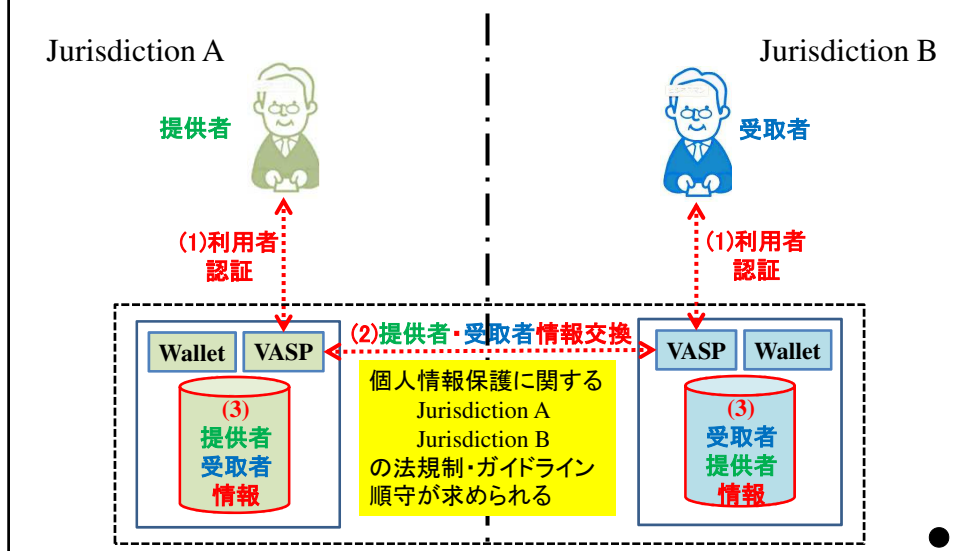
現在のトラベルルールの  
適用対象移転パターンの問題



## 4. 規制の課題

© Advanced IT Corporation 9

## 現在のトラベルルールの 個人情報のVASP間での共有の問題



## 5. SSVATF

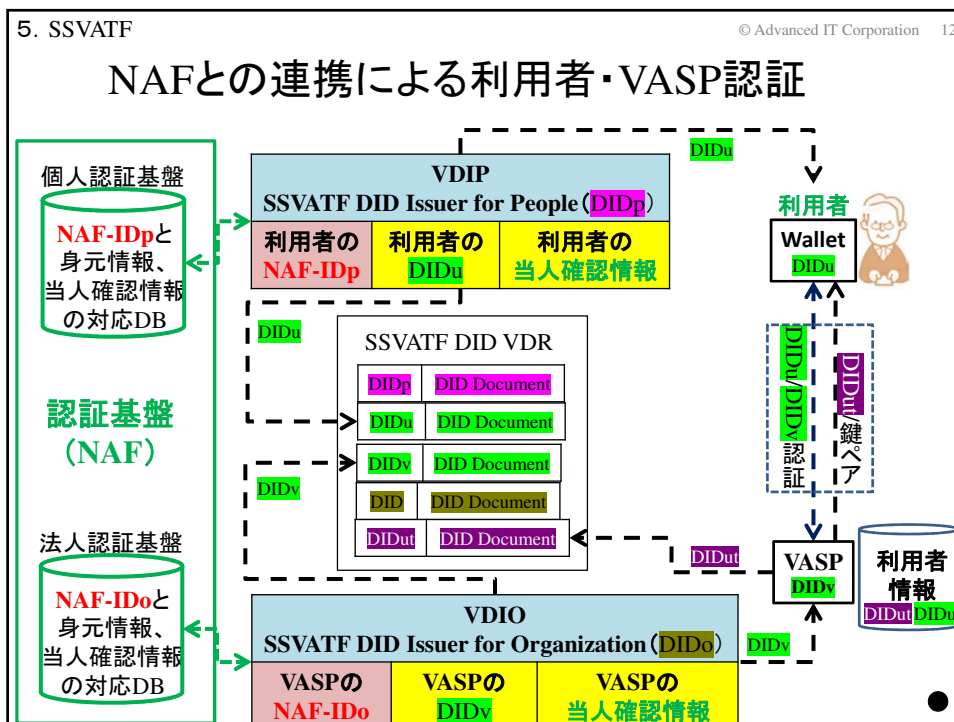
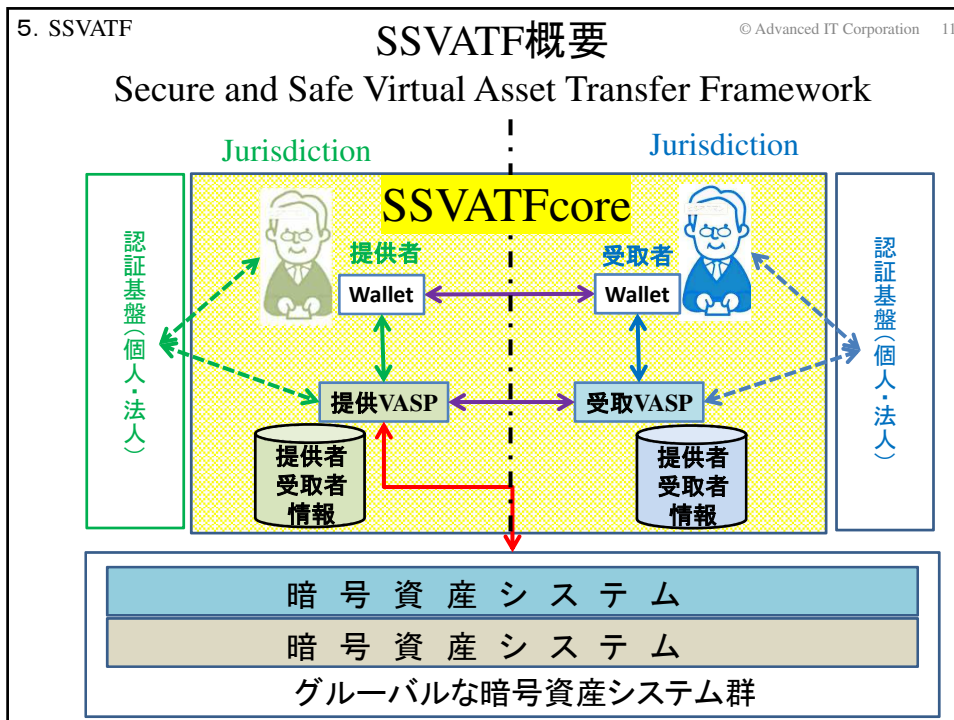
© Advanced IT Corporation 10

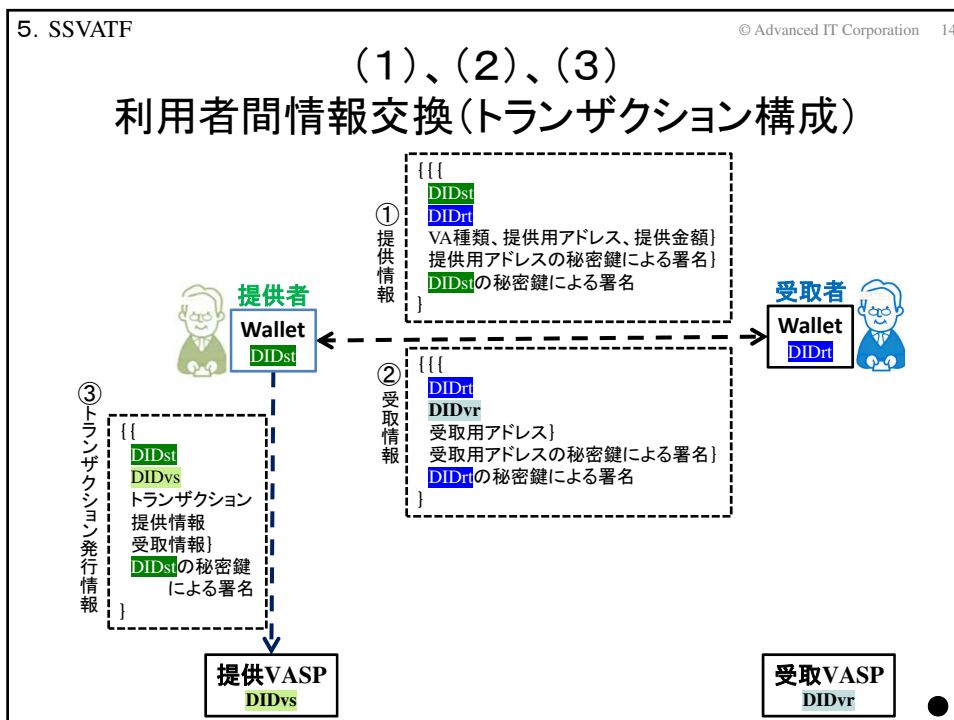
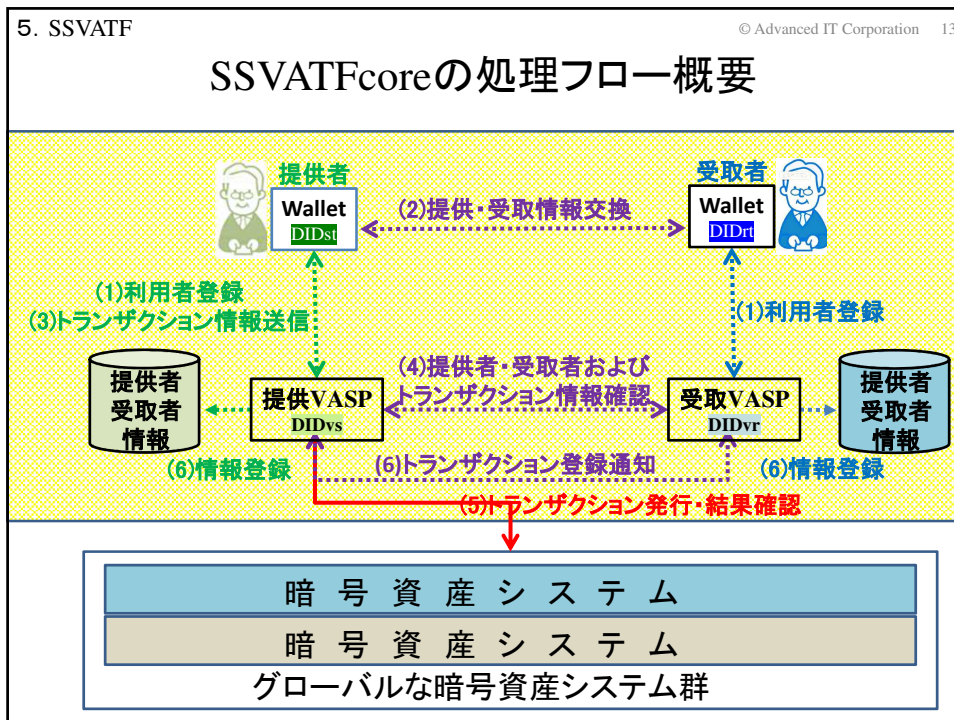
## 安心・安全な暗号資産取引基盤

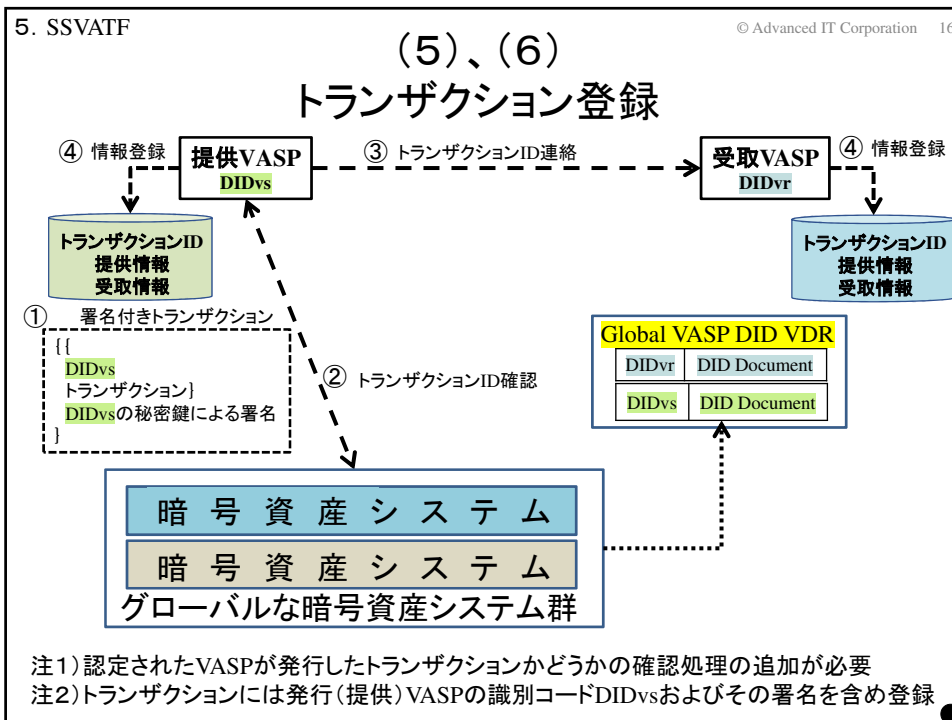
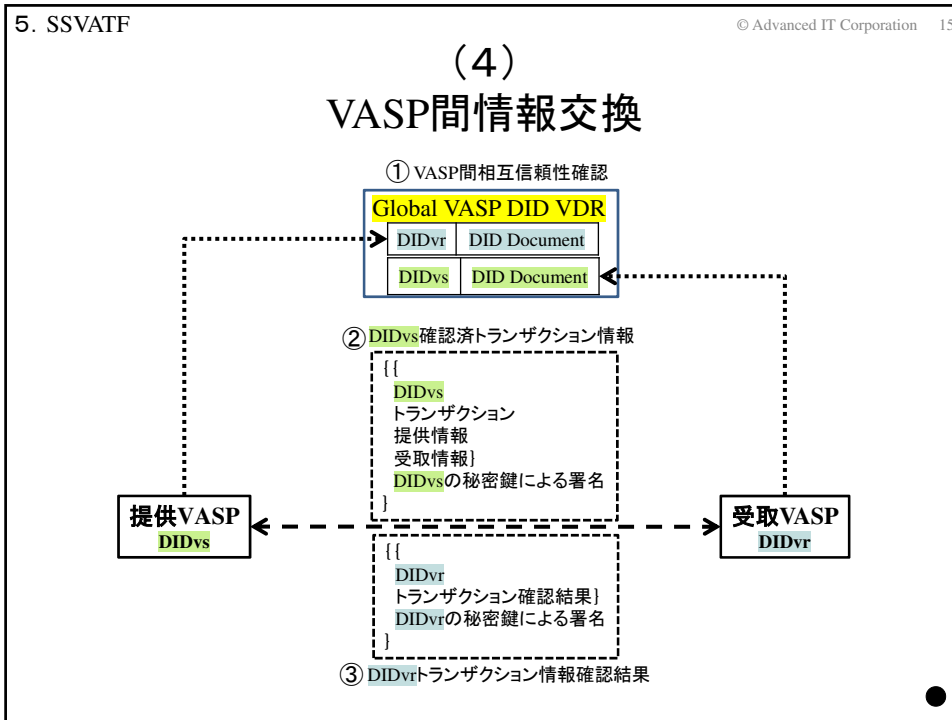
SSVATF: Secure and Safe Virtual Asset Transfer Framework

### 構想策定基本方針

- (1) VASPによる利用者の確実な本人確認
- (2) 資産移転における利用者の確実な匿名性の確保
- (3) 不正・不法な利用者の確実な特定・追跡性の確保
- (4) 個人情報・プライバシー情報の開示先・範囲の最少化
- (5) 暗号資産システム側の対応の最小化









## SSVATF考察(1/2)

### — 構想策定基本方針の観点から —

- (1)VASPによる利用者の確実な身元確認  
各国の制度に基づく確実な身元確認が期待されるNAFの利用  
身元確認の信頼性レベルに関する国際的な合意
- (2)資産移転における利用者の確実な匿名性の確保  
暗号資産移転時には暗号資産システムと同程度の匿名性確保
- (3)不正・不法な利用者の確実な特定・追跡性の確保  
利用者の特定・追跡に必要な情報の確実な記録・管理  
開示要請の合法性確認手続きの明確な定義と有効性の保証  
他国のVASPやNAFへの開示要請における各国間の協力 ●

## SSVATF考察(2/2)

### — 構想策定基本方針の観点から —

- (4)個人情報・プライバシー情報の開示先・範囲の最少化  
暗号資産移転時の個人情報の拡散の防止・抑止  
必要時の開示先・範囲の最少化の仕組みの検討(VC/VP/VR)
- (5)暗号資産システム側の対応の最少化  
トランザクションデータの正当性確認に  
認定されたVASPが発行した  
トランザクションかどうかの確認を追加  
ブロックチェーンにトランザクション登録時に、  
発行したVASPのDIDおよび署名を追加 ●

## 今後の検討課題

- (1) SSVATF基本方針に基づく改良・拡張案の検討
  - \* 利用者の特定・追跡性のための仕組み  
SSVATFcoreと暗号資産システムの役割分担の更なる検討
  - \* 暗号資産移転に伴う各国の様々な報告制度への対応  
各国の報告制度(スイス、米国(FINCIN)等)の動向把握
- (2) SSVATFのトラベルルール対応版の検討
  - \* トラベルルール改定動向の把握
  - \* トラベルルールへの各国の対応動向を把握
- (3) 異なるアプローチの検討(連携の可能性の検討)
  - \* 暗号資産用Walletの登録・認証による利用者の特定・追跡性  
Attestation Infrastructures for Private Wallets  
<https://arxiv.org/pdf/2102.12473.pdf>

# 終

(ご清聴、ありがとうございました。)