

# 暗号資産業界の健全な発展のために — 利用者の匿名性と特定・追跡性の両立 —

2023年6月1日

(株)IT企画 才所敏明

Mail : toshiaki.saisho@advanced-it.co.jp

URL : <http://www.advanced-it.co.jp>

(株)ZenmuTech

中央大学研究開発機構



# 自己紹介

1970年4月～1994年12月 東京芝浦電気(東芝)・情報システム部門  
東芝Gの技術部門・研究部門の

研究開発活動環境の整備・高度化を推進

1995年1月～2007年9月 東芝・セキュリティ技術研究開発部門  
東芝のセキュリティ技術センター発足と同時にセンター長就任  
東芝Gのセキュリティ技術開発・事業支援活動を推進

2007年10月 (株)IT企画を設立

情報技術および情報セキュリティ技術分野の研究開発や  
その応用事業に対するプロフェッショナルサービスを開始

[現職]

(株)IT企画 代表取締役社長

事業支援活動(顧問・相談役):2社(日、米)

研究開発活動(研究員):中央大学研究開発機構、九州大学大学院

主たる研究分野:

暗号・認証、秘密分散、バイオメトリクス、ブロックチェーン、  
暗号資産、メタバース、ブロックチェーンサービス基盤

# 講演内容

- (1)暗号資産の歴史
- (2)暗号資産の悪用(不正・不法な利用)の現状
- (3)暗号資産の悪用への対策の歴史
- (4)現時点の悪用対策の課題
- (5)暗号資産の悪用を防ぐための構想紹介  
安心・安全な暗号資産移転基盤  
SSVATF: Secure and Safe Virtual Asset Transfer Framework
- (6)関連情報紹介

## 暗号資産の歴史

2008年 Bitcoin(ブロックチェーン)(最初の暗号資産)

2010年 Bitcoinがピザ購入に使用(2枚で1万BTC:1BTC≒0.2円)

2010年 暗号資産交換事業者(VASP)が登場(Mt.Goxもその一つ)

2014年 Mt.Gox事件(約470億円分の暗号資産が流出)

2015年 Ethereum(スマートコントラクト)

2018年 コインチェック事件(約580億円分の暗号資産が流出)

2022年 TerraUSD(ステーブルコイン)の歴史的な大暴落(99%以上)

2022年 FTX経営破綻(広告塔の著名人も提訴(大谷・大阪も対象))

暗号資産:10083 時価総額:157.39兆円 (coinmarketcap 2023/05/27)

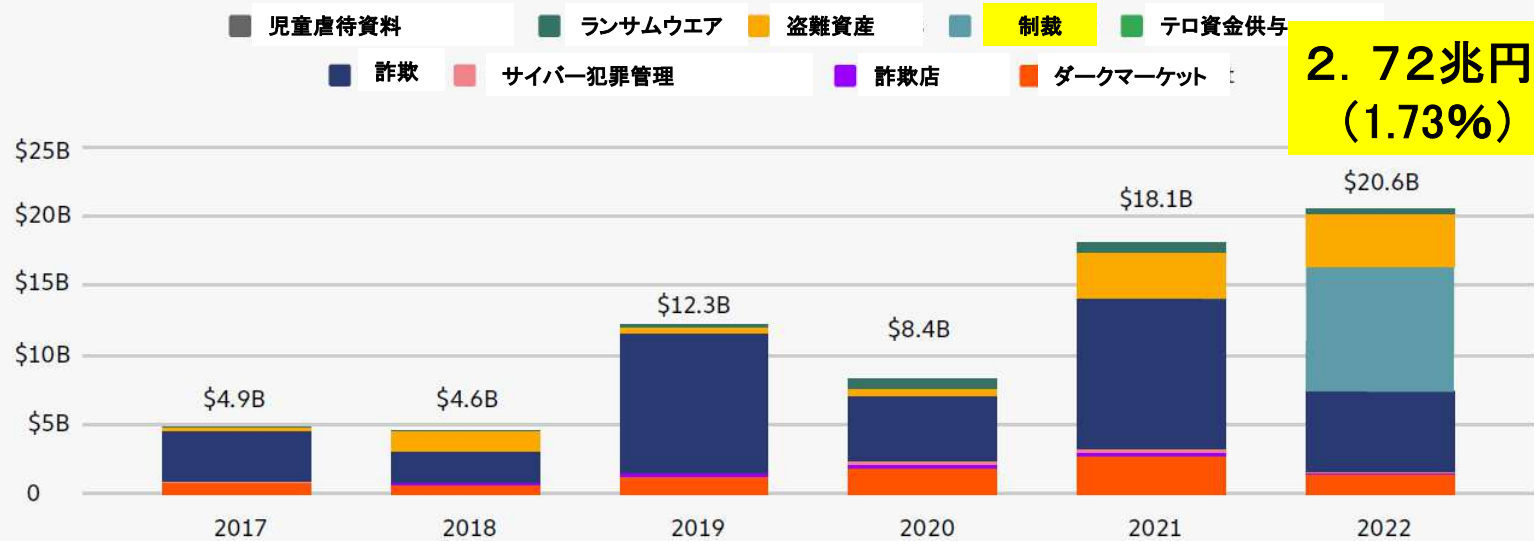
(所有者数:世界で1億人以上(2020年)、日本のアンケート結果:9~11%)

(2)悪用の現状

© Advanced IT Corporation 5

# 不正・不法な目的で使用されている アドレスが受け取った資産総額 (February 2023 Chainalysis)

Total cryptocurrency value received by illicit addresses, 2017 - 2022



<https://go.chainalysis.com/2023-crypto-crime-report.html>



## 暗号資産の悪用に対する対策の歴史

### FATF(Financial Action Task Force)

マネーロンダリング・テロ資金供与(ML/FT)対策等に取り組む主要国政府による  
枠組みとして1989年にOECDに事務局を設置し発足した金融活動作業部会  
(ML/FT: money laundering and terrorist financing)

2015年6月 G7サミットでの宣言

暗号資産およびその他の新たな支払手段に対する適切な規制を導入

→FATFは、VASP(暗号資産交換事業者)の登録・免許制、  
利用者の本人確認の義務付けを各国へ要請

### 2016年10月 (日本)犯罪収益移転防止法(2007年公布)を改正

VASPの登録制、確実な本人確認(KYC)の実施、記録の保存の義務化

2018年10月 FATF勧告15「新技術」の改訂

暗号資産交換事業者(VASP)にもML/FT規制が必要なことを規定

### 2019年6月 FATF勧告16「電信送金」の改訂 (トラベルルールを規定)

暗号資産交換事業者(VASP)は、電信送金の

発信者(提供者)と受益者(受取者)に関する基本情報を確認すること  
基本情報を電信送金と共に送信し、VASP間で共有すること  
基本情報を確実に保存しておくこと

### (3)悪用対策の歴史

© Advanced IT Corporation 7

#### 2021年3月 (日本)金融庁

2022年4月からのトラベルルールへの対応を日本暗号資産取引業協会へ要請

#### 2021年10月 トラベルルールの改定

暗号資産交換事業者(VASP)は、Unhosted Walletとの暗号資産移転を精査必須金融分野の新たな製品やサービスについては、

市場投入前にリスクを管理・軽減する適切な対策をとることも要請

#### 2023年2月:(日本)犯罪による収益の移転防止に関する法律施行令の

#### 一部を改正する政令案等の公表

改定されたトラベルルールで規定された

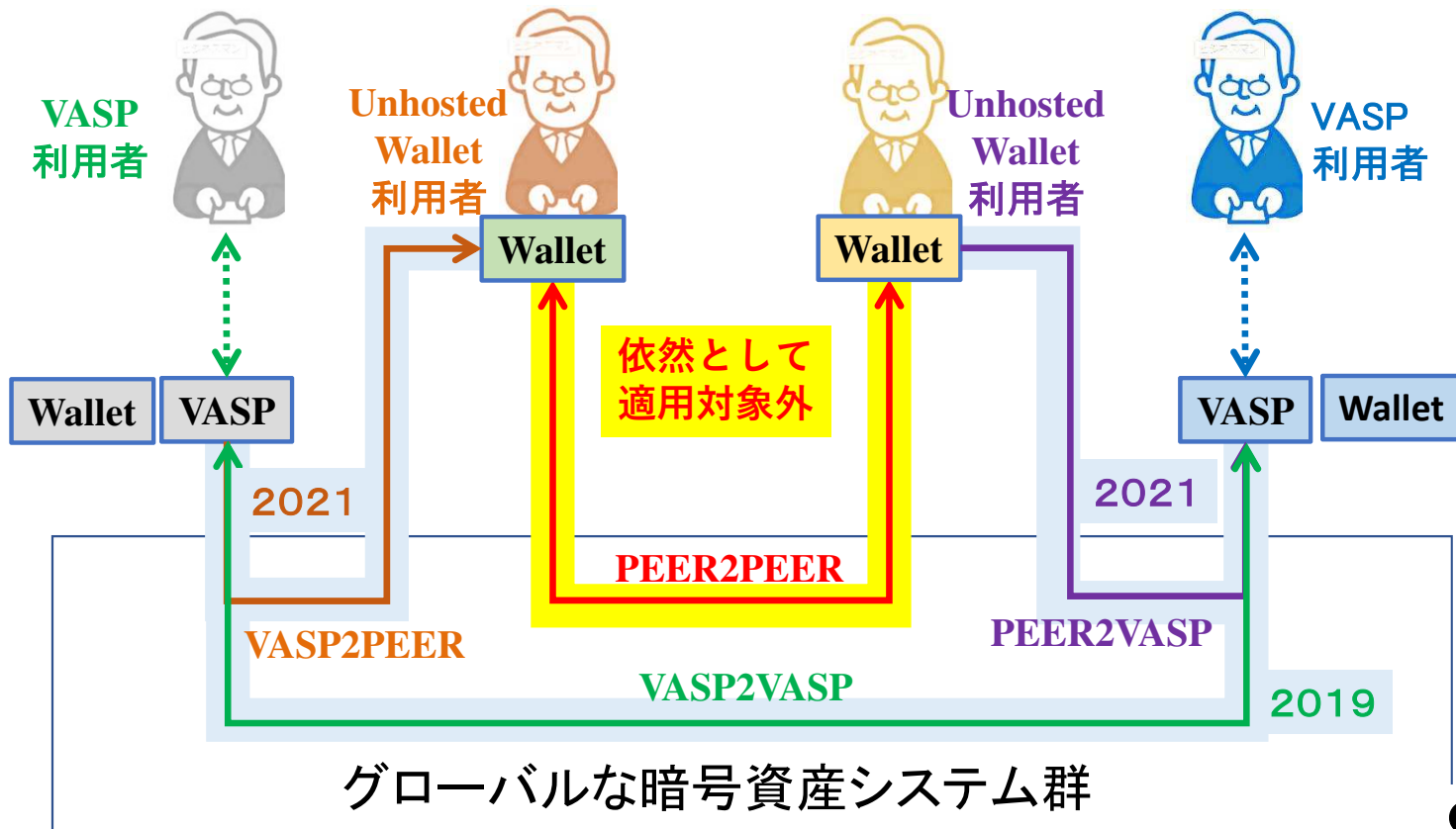
Unhosted Walletへの対応が盛り込まれる模様

●10分

(4)悪用対策の課題

© Advanced IT Corporation 8

# 現在のトラベルルールの課題[1] 適用対象移転パターンの問題

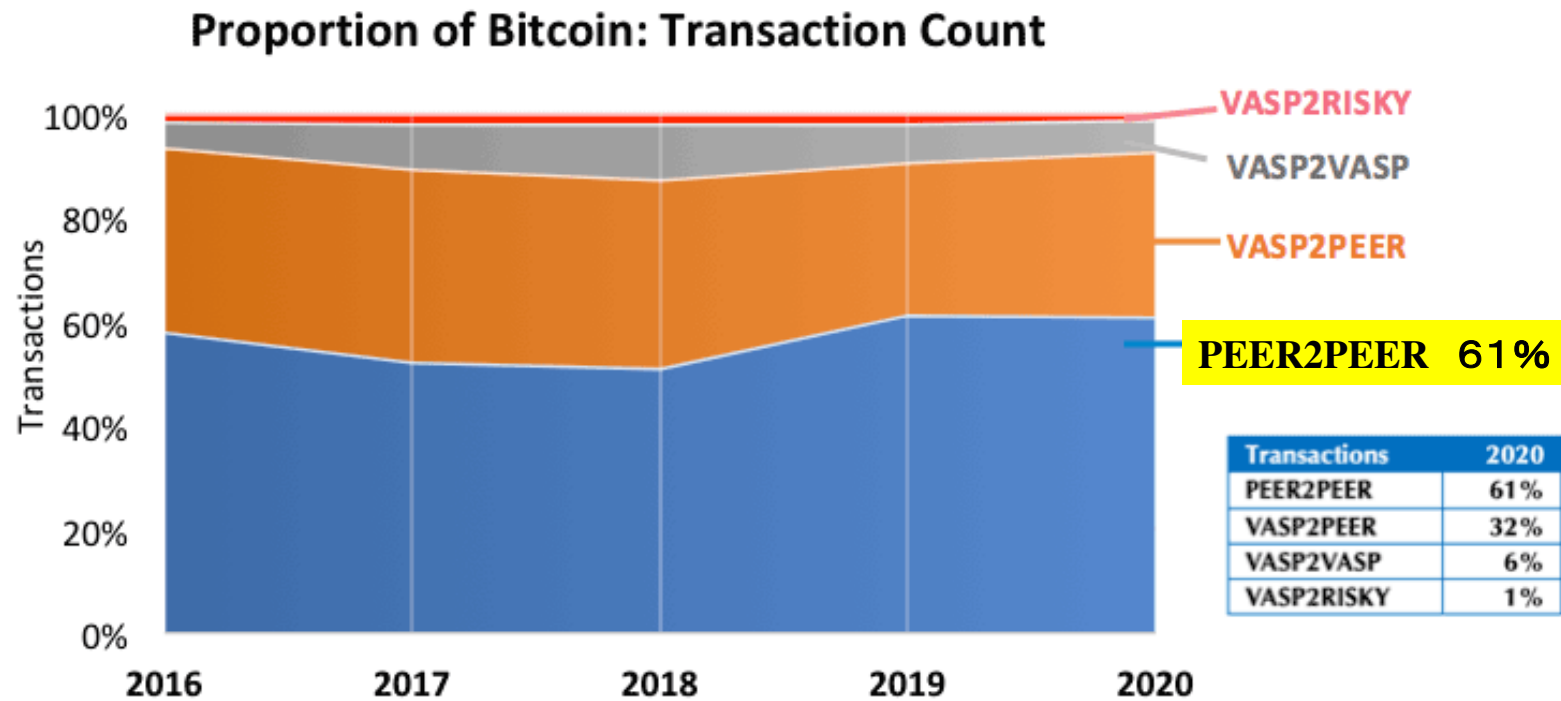




## (4)悪用対策の課題

© Advanced IT Corporation 9

## 提供者・受取者別 ビットコインランザクション数の割合の推移



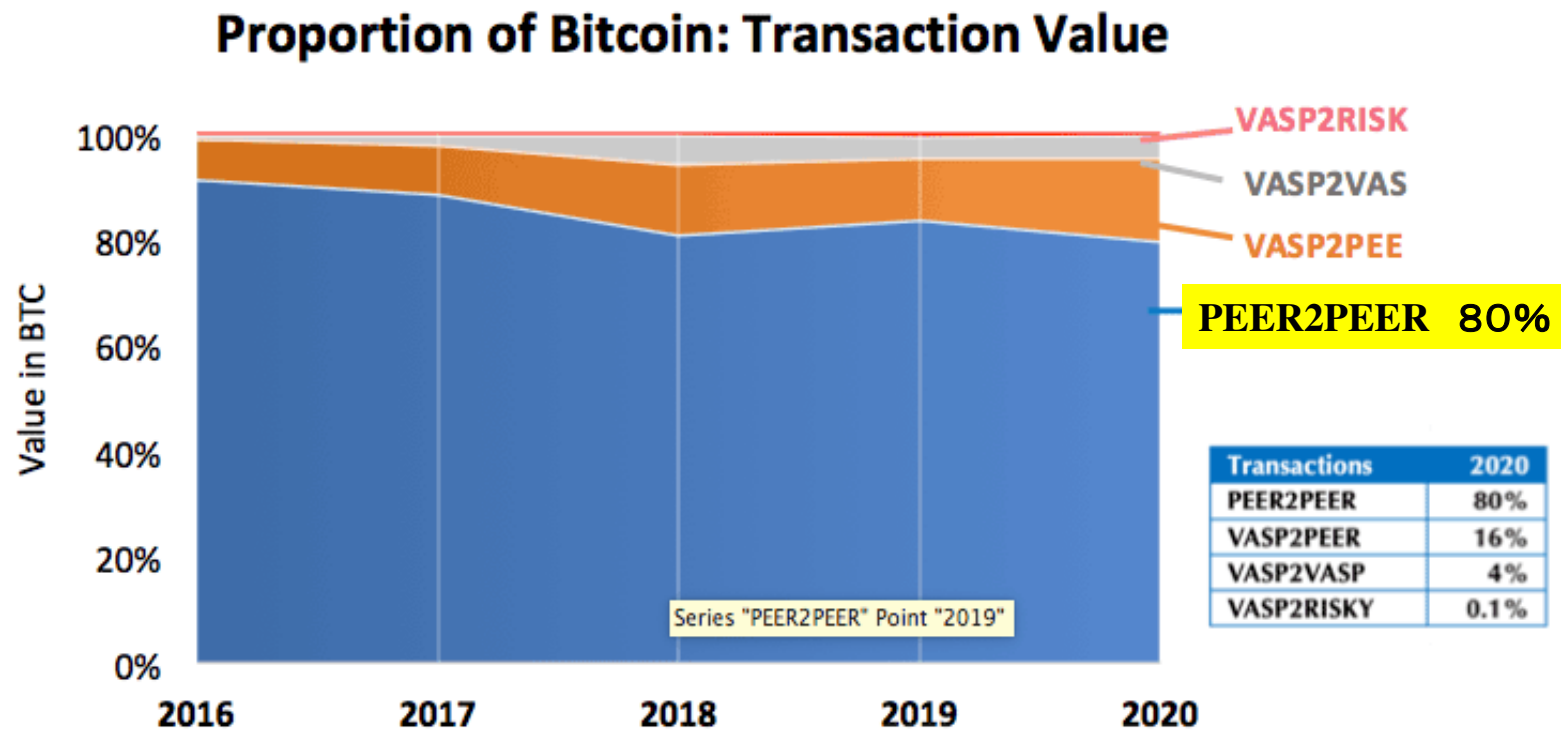
Source: CipherTrace Cryptocurrency Intelligence

<https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-may-2021/>

## (4)悪用対策の課題

© Advanced IT Corporation 10

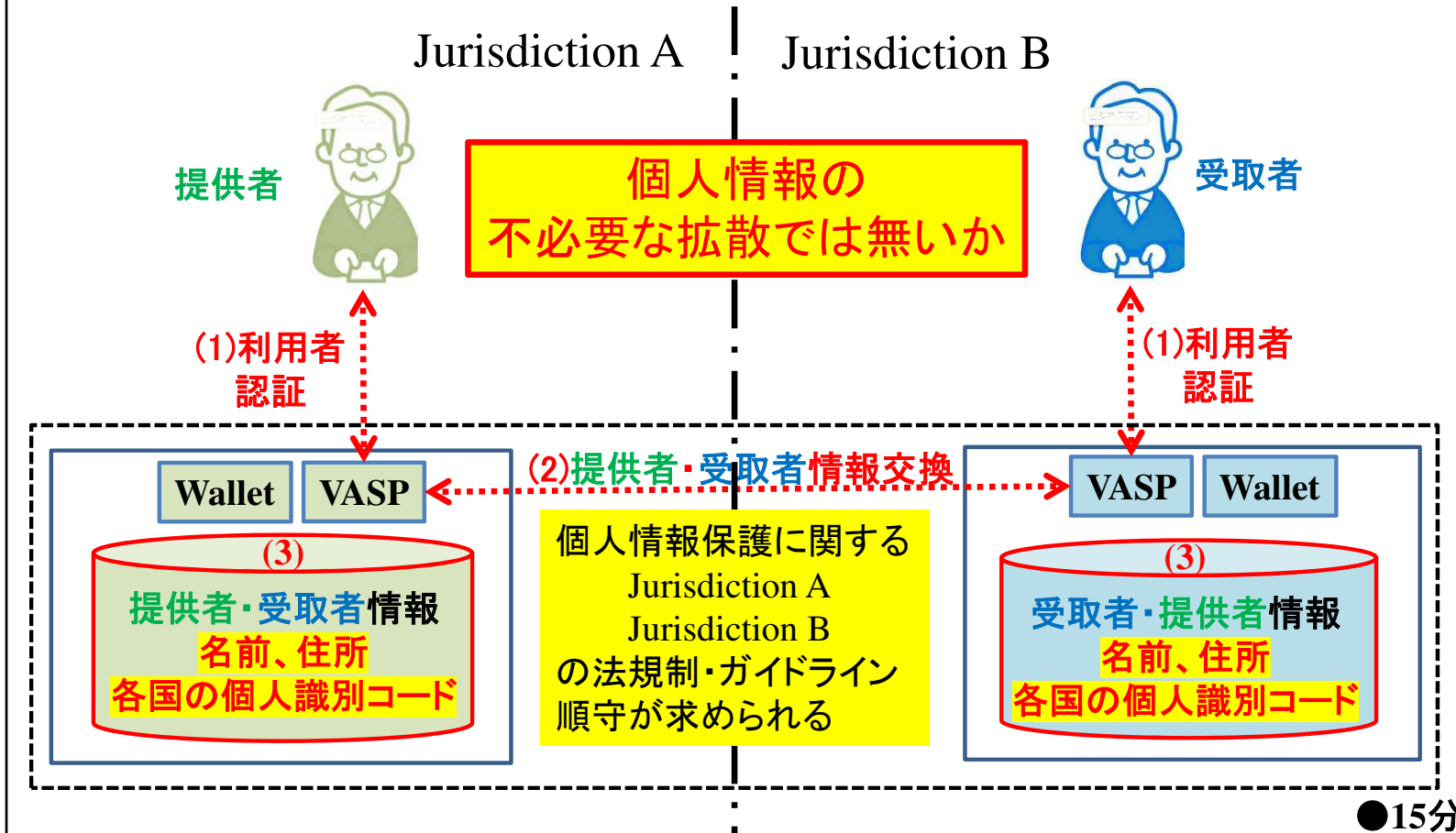
## 提供者・受取者別 ビットコインランザクション資産総額の推移



Source: CipherTrace Cryptocurrency Intelligence

<https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-may-2021/>

# 現在のトラベルルール課題[2] 個人情報のVASP間での共有の問題



(5)SSVATF

© Advanced IT Corporation 12

## 安心・安全な暗号資産移転基盤

SSVATF: Secure and Safe Virtual Asset Transfer Framework

### SSVATFに期待される機能

暗号資産移転のための基本機能は既存の暗号資産システムに期待

#### A: 暗号資産利用者にとって

- \* 資産移転における利用者の確実な匿名性  
(個人情報・プライバシー情報の保護)

#### B: 暗号資産交換事業者にとって

- \* 既存の暗号資産システムとの容易な連携

#### C: 暗号資産移転が展開される社会にとって

- \* 不正・不法な利用者の確実な特定・追跡性

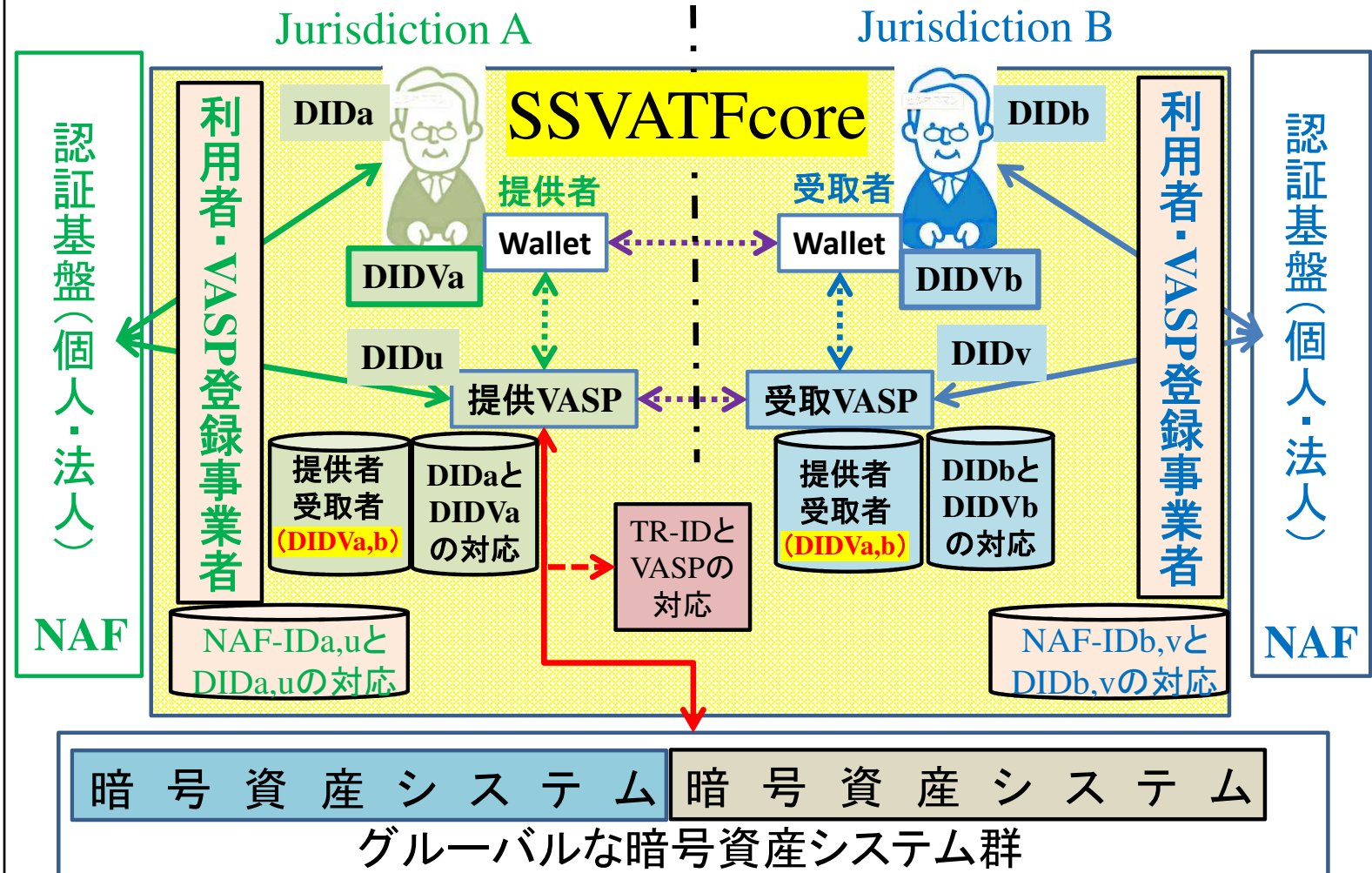


(5)SSVATF

# SSVATF概要

© Advanced IT Corporation 13

## Secure and Safe Virtual Asset Transfer Framework

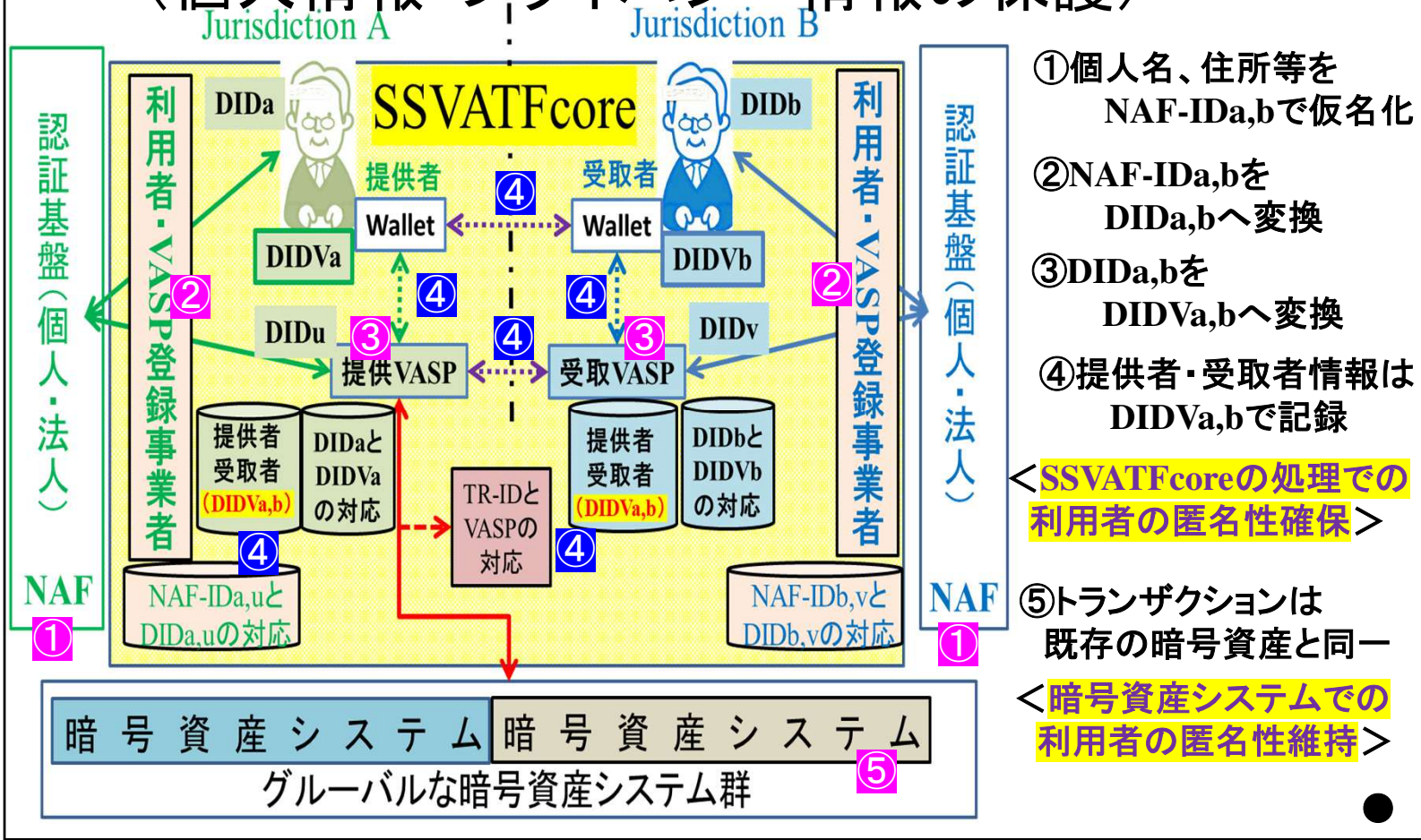


(5)SSVATF

© Advanced IT Corporation 14

# A:暗号資産利用者にとって

## \* 資産移転における利用者の確実な匿名性 (個人情報・プライバシー情報の保護)



- ①個人名、住所等を NAF-IDA,bで仮名化
  - ②NAF-IDA,bを DIDa,bへ変換
  - ③DIDa,bを DIDVa,bへ変換
  - ④提供者・受取者情報は DIDVa,bで記録
- <SSVATFcoreの処理での利用者の匿名性確保>
- ⑤トランザクションは 既存の暗号資産と同一
- <暗号資産システムでの利用者の匿名性維持>

(5)SSVATF

© Advanced IT Corporation 15

## B:暗号資産交換事業者にとって

### \* 既存の暗号資産システムとの容易な連携

既存の暗号資産システムは運用中であり、

多くの暗号資産システムとの連携を期待するには

→暗号資産システムへの変更は極力少なく(SSVATFの方針)

SSVATFで既存の暗号資産システムへ追加を期待する機能は次の一つ

トランザクションに関与する暗号資産の提供者・受取者が全員、  
特定・追跡性を確認されているかどうかにより、  
トランザクション承認処理の対象にするかどうかを判断

具体的には、

トランザクションの承認条件に、

トランザクションに付与された発行VASPの署名検証、を加える  
ことが必要

(登録済のVASPかどうかの確認が可能な情報は、SSVATF側が提供)





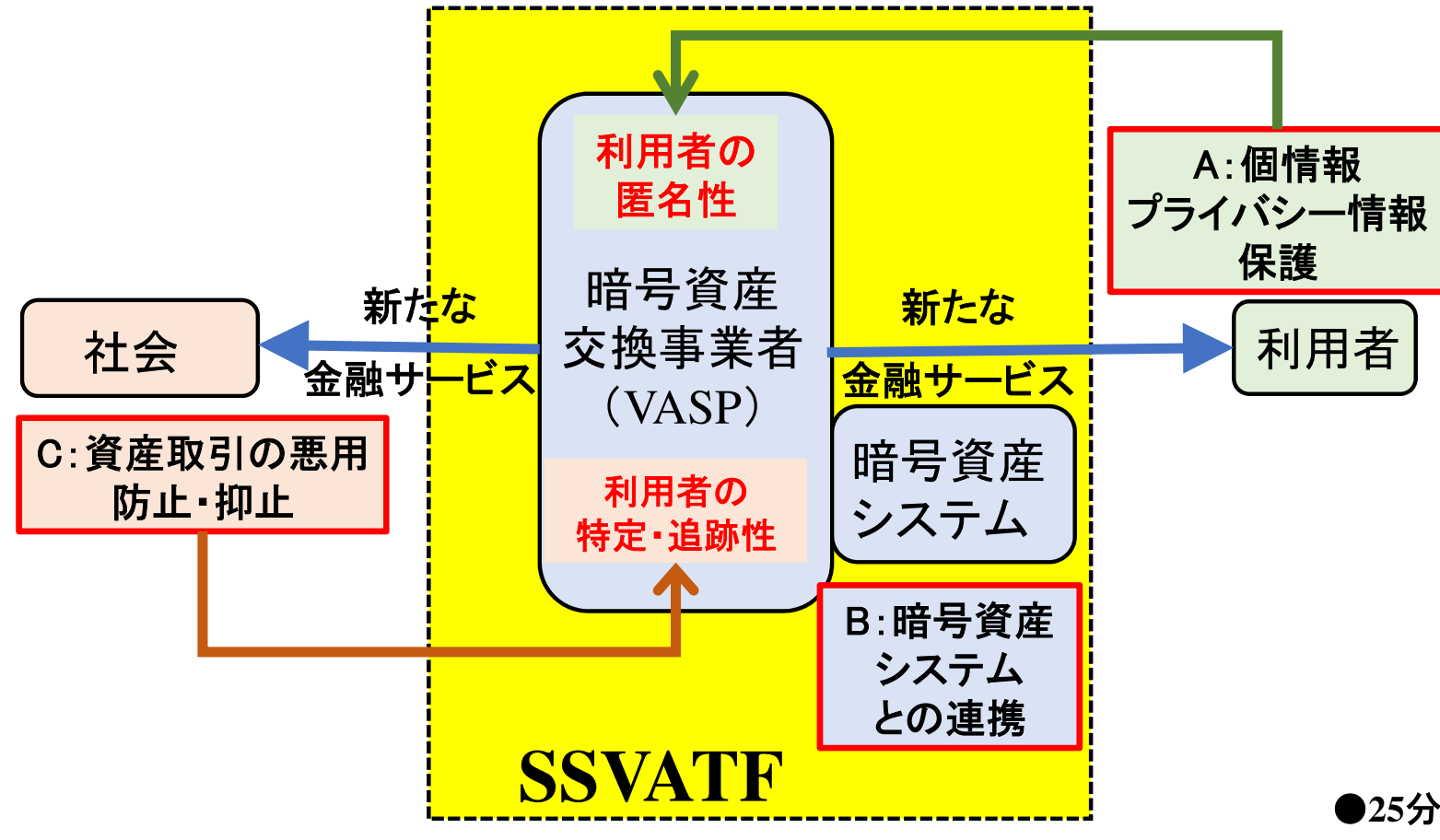


(5)SSVATF

© Advanced IT Corporation 17

# 安心・安全な暗号資産移転基盤

## SSVATF : Secure and Safe Virtual Asset Transfer Framework



## 関連情報

### (1)安心・安全な暗号資産取引を可能とする技術に関する研究

Attestation Infrastructures for Private Wallets (24 Feb 2021)

(<https://arxiv.org/pdf/2102.12473.pdf>)

SSVATFと同様、Unhosted Wallet間の暗号資産移転対応を含む研究  
TPM (Trusted Platform Module) チップによるセキュアなPrivate Wallet  
Private Walletのリモート認証(法令・ガイドライン順守Walletの認証)  
利用者の本人確認、匿名性と特定・追跡性の両立は、未検討  
PEER2PEER暗号資産移転における

トラベルルール要件の確認作業は、SSVATFと同様、VASPへ期待



## (6)関連情報

© Advanced IT Corporation 19

## (2)OECDが暗号資産による脱税対策案を発表(2022年10月)

暗号資産等報告枠組CARF(Crypto-Asset Reporting Framework)

暗号資産による脱税を防ぐための枠組みの提案で、

2022年10月G20財務大臣・中央銀行総裁会議へ提示

対象は、支払いや投資に使用できる暗号資産、NFT等

年に一度、暗号資産の取引に関する税務情報を自動的に

納税者が居住する管轄区域と交換することを規定

(国際的な脱税及び租税回避に対処するための

「暗号資産報告の枠組み」)

(国際的な税務報告の枠組みとしては共通報告基準(CRS)が導入されているが、仮想通貨や関連する取引はCRSの対象になっていない)

## (6)関連情報

© Advanced IT Corporation 20

(3)米国ホワイトハウスが「デジタル資産の責任ある開発に関する  
包括的フレームワーク」を発表(2022年9月)

バイデン大統領の「デジタル資産の責任ある開発の確保に関する  
大統領令」(2022年3月)に対する政府機関の政策提言(9月)

①Protecting Consumers, Investors, and Businesses

ステーブルコインTerraUSDの大暴落

②Promoting Access to Safe, Affordable Financial Services

③Fostering Financial Stability

④Advancing Responsible Innovation

⑤Reinforcing Our Global Financial Leadership and Competitiveness

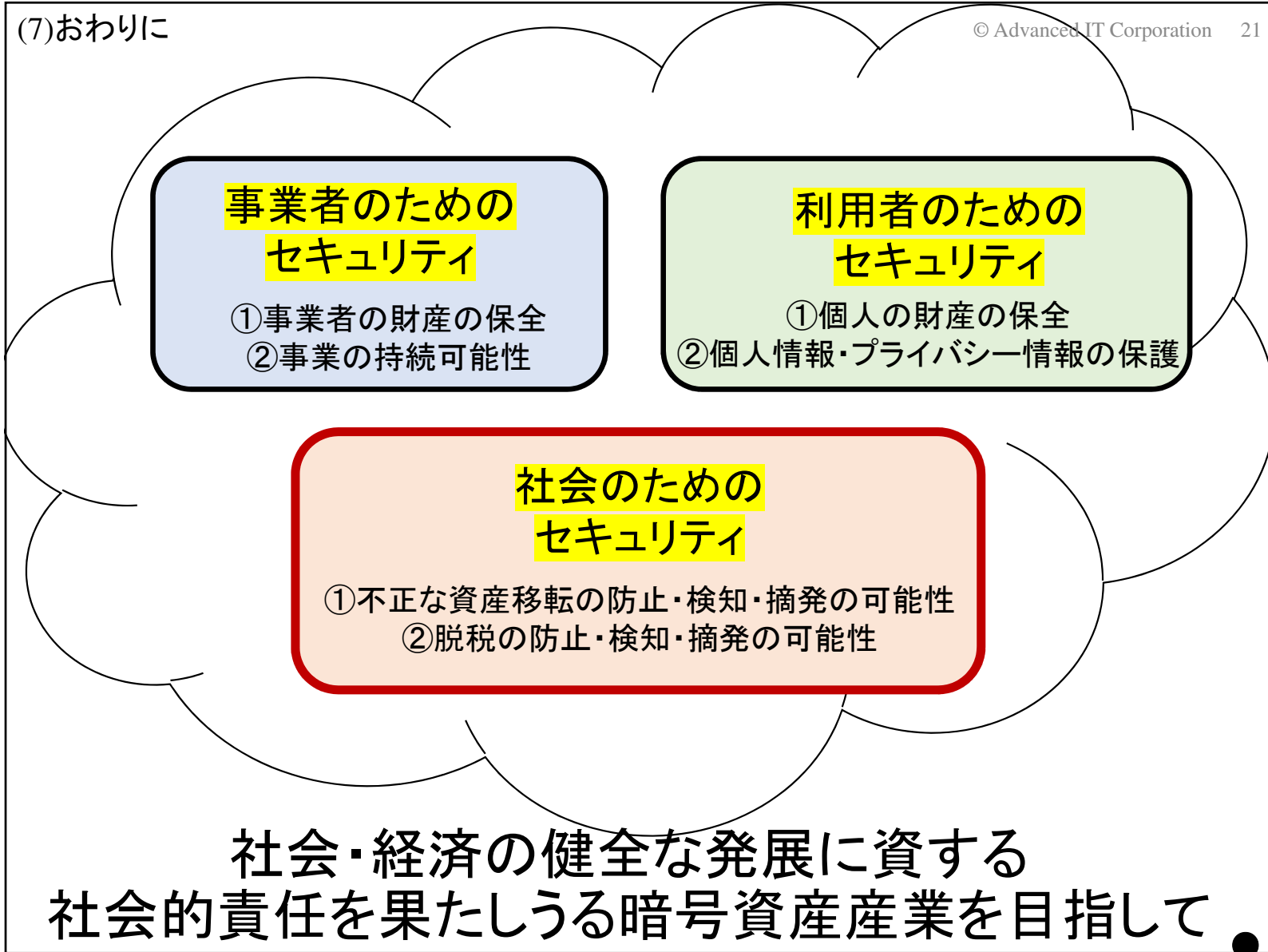
⑥Fighting Illicit Finance

VASPやNFTプラットフォーム事業者への

法規制の強化、罰則の強化の必要性

⑦Exploring a U.S. Central Bank Digital Currency (CBDC)

デジタル通貨の時代も、基軸通貨はデジタルドルへ



終

ご清聴、ありがとうございました。