

トラベルルール(FATF勧告16) の現状・課題・考察 (暗号資産業界の健全な発展のために)

2022年5月19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

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ーセンター
(株)国際電気通信基盤技術研究所

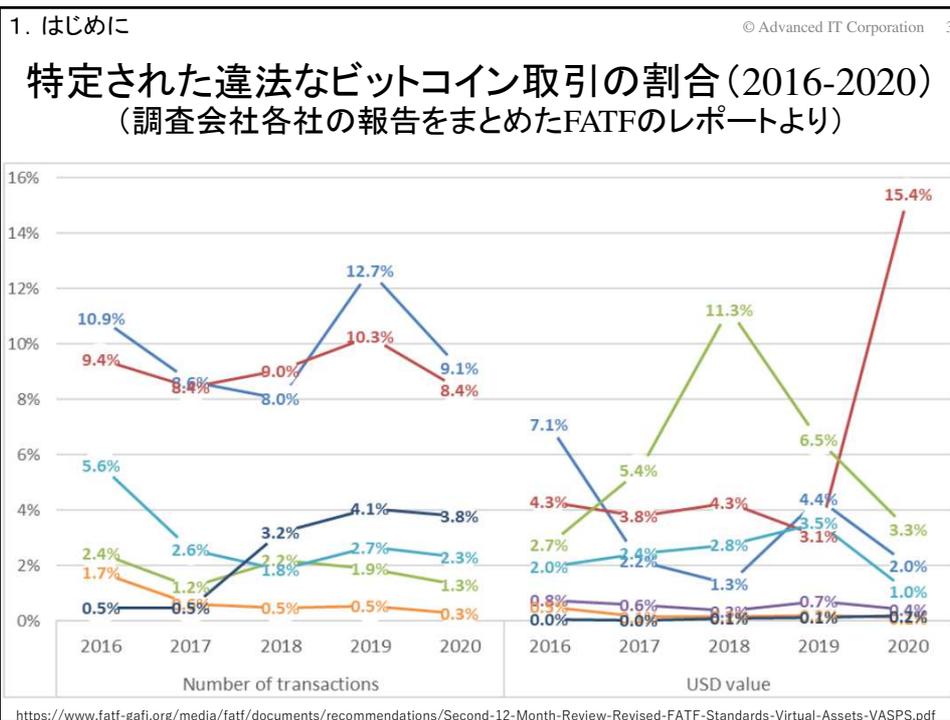
辻井重男

中央大学研究開発機構

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 (Chainalysisのレポートより)



<https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>



2. Travel Rule © Advanced IT Corporation 4

暗号資産への規制強化の動き

FATF (Financial Action Task Force)
1989年にマネーロンダリング・テロ資金 (ML/FT) 対策等に取り組む主要国政府による枠組みとしてOECDに事務局を設置し発足した金融活動作業部会

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の登録・免許制、利用者の本人確認の義務付けを各国政府に勧告

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

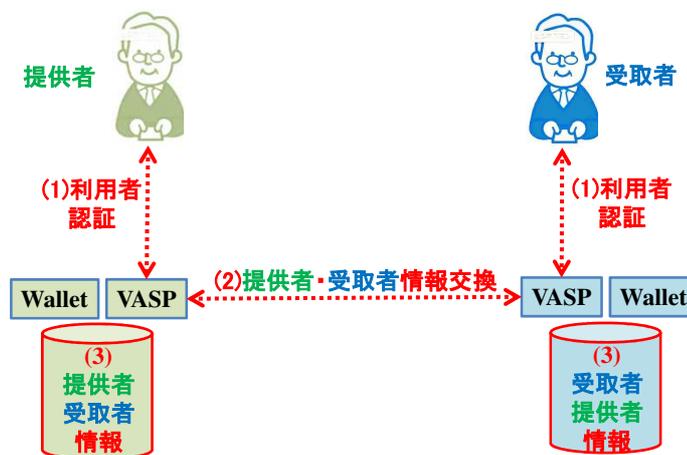
2019年6月 FATF勧告16「電信送金」の改訂 (トラベルルールを規定)
電信送金の発信者 (提供者) と受益者 (受取者) に関する
基本情報の確認・保存をVASPへ要求
具体的要件: 電信送金の発信者 (提供者) と受益者 (受取者) に関する
以下の基本情報を電信送金に含めておくこと

- 1) 資産提供者の名前
- 2) トランザクションの処理に利用される資産提供者のアカウント番号
- 3) 資産提供者の地理的な住所および国固有の個人識別番号等
- 4) 資産受取者の名前
- 5) トランザクションの処理に利用される資産受取者のアカウント番号

2. Travel Rule

© Advanced IT Corporation 5

トラベルルールによるVASPへの要請



3. TRへの対応

© Advanced IT Corporation 6

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)

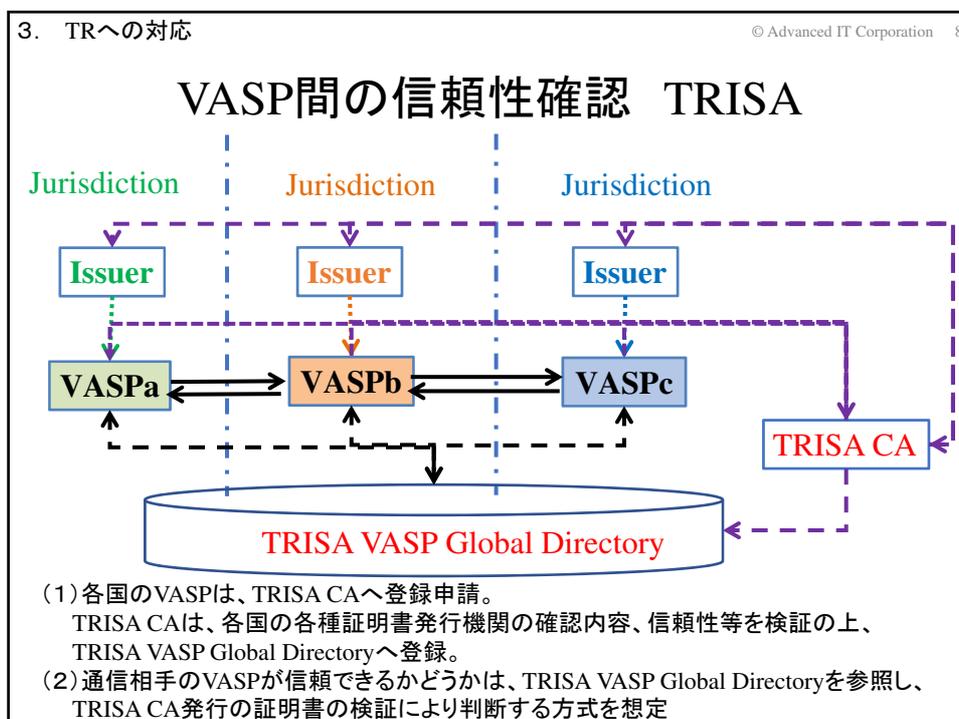
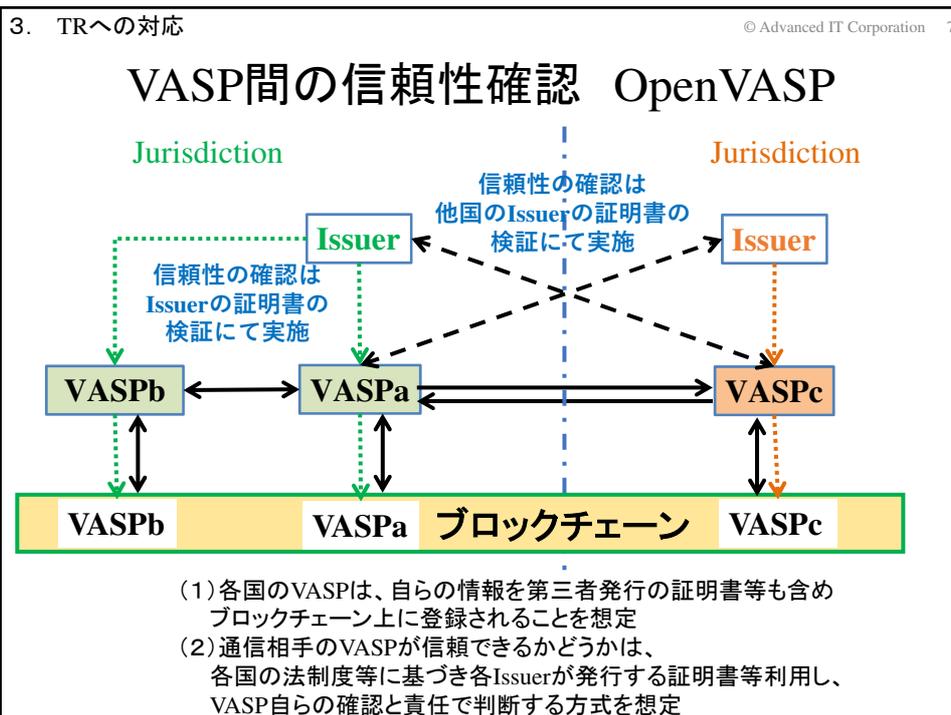
IVMS101: interVASP Messaging Standards

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

TRISA: Travel Rule Information Sharing Alliance



3. TRへの対応

© Advanced IT Corporation 9

VASP間の信頼性確認 OpenVASP/TRISA比較

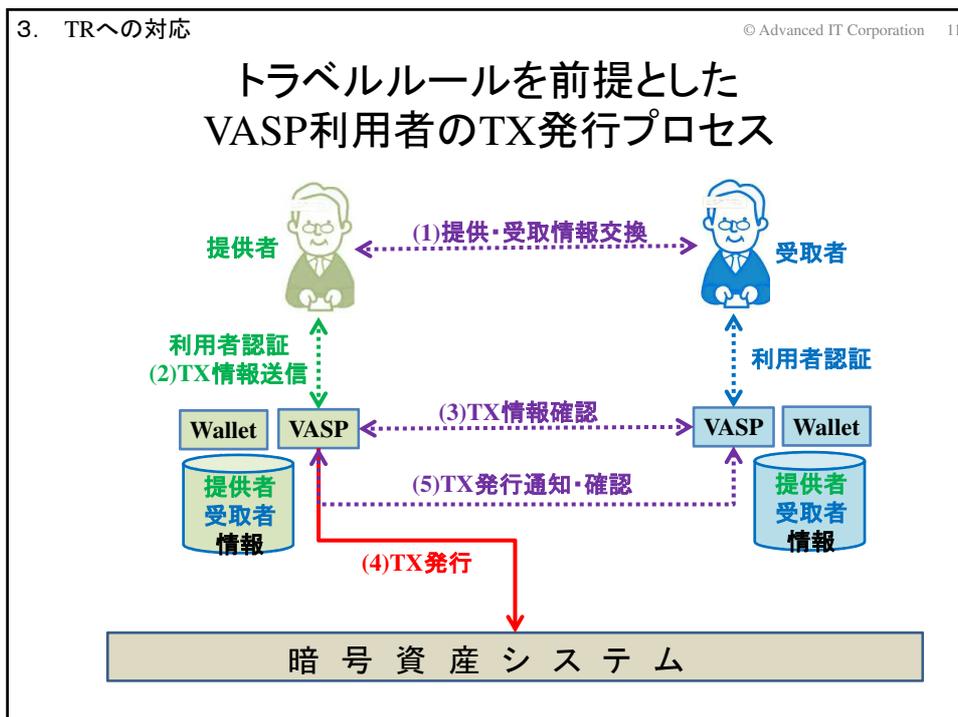
機能	OpenVASP	TRISA
VASP登録時の 信頼性確認	規定せず(各国政府の認定時の審査に期待)	TRISA CAによる登録時の審査
VASP間通信時の 信頼性確認	初回は各国の認定情報、業界の信頼度評価等で確認(信頼できるVASPはスマートコントラクトに登録)	TRISA CA発行の証明書(SSL/TLS)

3. TRへの対応

© Advanced IT Corporation 10

利用者の認証 OpenVASP/TRISA比較

機能	OpenVASP	TRISA
登録時の利用者認証 身元確認 身元情報の登録・管理 本人確認情報の登録・管理	規定せず ①VASPが個々の手順に従ってKYCを実施 ②VASPのKYCの適切さは、各国のVASP審査時の確認に期待	
利用時の利用者認証 本人確認		



3. TRへの対応 © Advanced IT Corporation 12

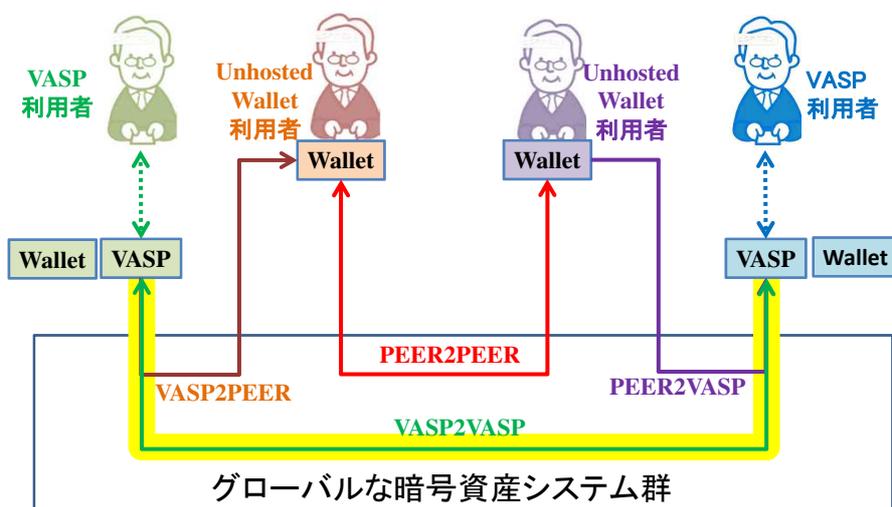
VASP利用者のTX発行プロセス OpenVASP/TRISA比較

機能	OpenVASP	TRISA
(1)提供・受取情報交換 (提供者 \leftrightarrow 受取者)	規定せず (受取者のVAAN)	規定せず (受取者のVASP)
(2)TX情報送信 (提供者 \rightarrow VASP)	金額、提供アドレス、 受取者のVAAN	金額、アドレス、 受取者のVASP
(3)TX情報確認 (VASP \leftrightarrow VASP)	\rightarrow 金額、提供者情報、 受取者情報(*) \leftarrow (*)に加え、 受取アドレス	\rightarrow 金額、アドレス、 提供者情報 \leftarrow 受取者情報
(4)TX発行 (VASP \leftrightarrow 暗号資産システム)	\rightarrow TX \leftarrow TXID	\rightarrow TX (VASP署名) \leftarrow TXID
(5)TX発行通知・確認 (VASP \leftrightarrow VASP)	\rightarrow (*)に加え、 提供アドレス、TXID \leftarrow 受信データをそのまま	\rightarrow TXID

3. TRの課題

© Advanced IT Corporation 13

暗号資産の移転パターン



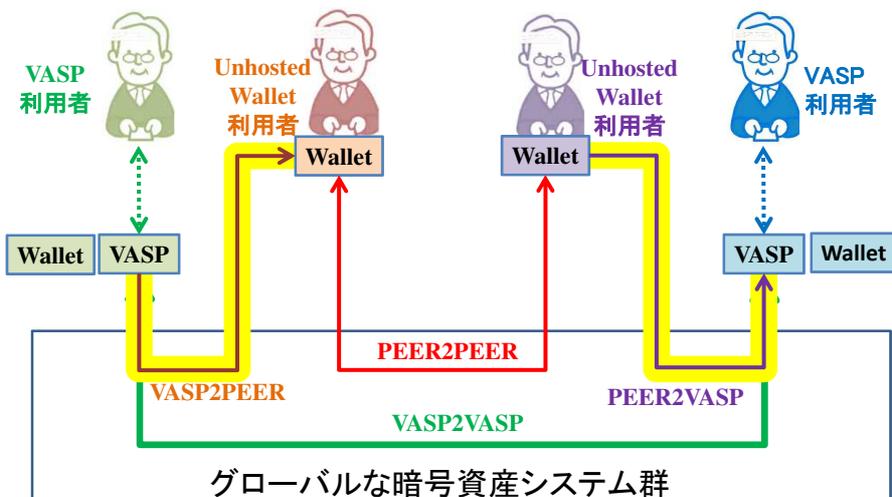
4. TRの改定

© Advanced IT Corporation 14

トラベルルール改定(2021年10月)

(1) Unhosted Walletへの対応

FATF: “VASPへUnhosted Walletとの暗号資産移転の精査を課す”



トラベルルール改定(2021年10月)

(2) 金融分野の新たな製品・サービスへの対応

FATF: 金融分野の新たな製品やサービスの、
 マネーロンダリングやテロ資金供与および
 不正・不法な取引の決済手段等、
 暗号資産が様々な犯罪に活用されるリスクを特定・評価し、
 市場投入前にリスクを管理・軽減する適切な対策を
 事業者にとらせることを要求

(現状の暗号資産システムが不正・不法な利用を防止・抑止する仕組み無しに社会に投入され、対策が後手に回っていることへの反省からの各国への要請と考えられる。)

Unhosted Wallet対応

AOPP: Address Ownership Proof Protocol

(1) 開発経緯

スイスの金融市場監督局(FINMA)が2019年8月よりVASPへ次の規制
 Unhosted Walletとの間の暗号資産の移転は、
 提供者および受取者の身元を確認
 Unhosted Wallet/暗号資産アドレスの所有権を確認
 できた場合にのみ可能
 本規制順守のためのツールとして、AOPPが開発された

(2) AOPPの仕組み

- ① VASPからUnhosted Walletへ何らかのメッセージを送信、
- ② Unhosted Walletはそのメッセージへ
 指定したアドレスに対応する秘密鍵で署名しVASPへ返送
- ③ VASPは指定されたアドレスに対応する公開鍵で署名検証し
 そのアドレスの所有(秘密鍵の所有)を確認

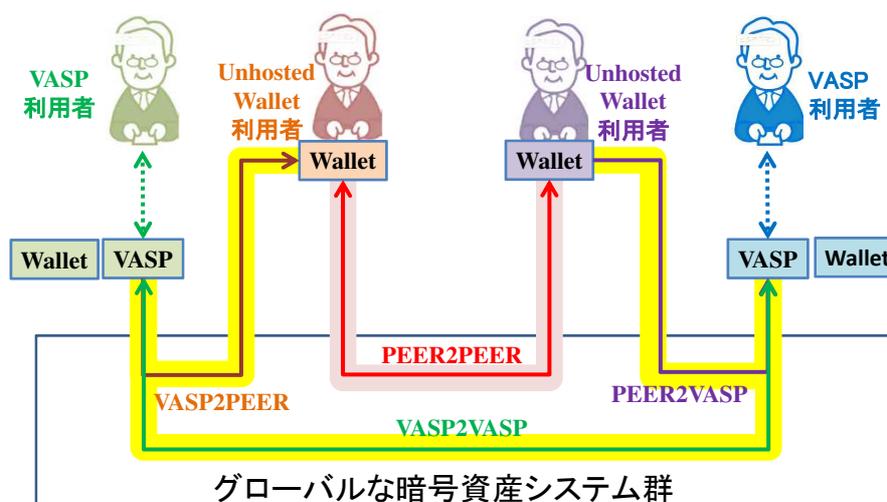
(3) 2021年版トラベルルールとの関係

VASPIにとっては、2019年版トラベルルール対応の仕組みへAOPPの追加により
 2021年のトラベルルールへの対応が可能
 Unhosted Wallet利用者は、AOPPに対応できるWalletが必要となる。

安心・安全で公平・公正な 暗号資産移転の仕組み実現上の課題・考察

- ①利用者の特定・追跡の仕組み上の課題 →①
- ②利用者の匿名性確保上の課題 →②
- ③個人情報の海外移転上の課題 →③
- ④暗号資産システム側の対応の課題 →④

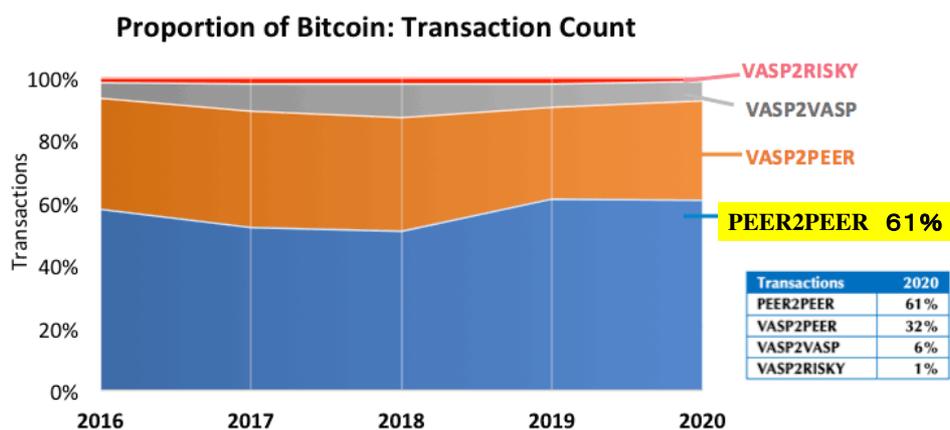
安心・安全で公平・公正な暗号資産移転のために ①利用者の特定・追跡の仕組み上の課題



6. 今後の課題

© Advanced IT Corporation 19

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



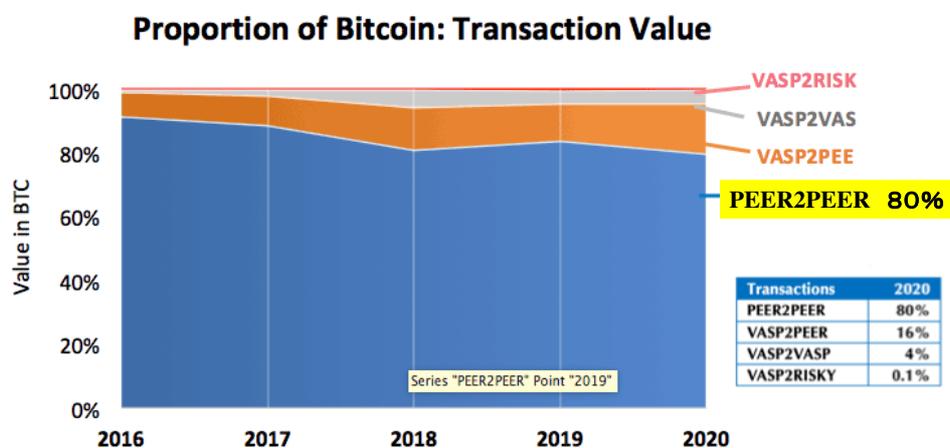
Source: CipherTrace Cryptocurrency Intelligence

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

6. 今後の課題

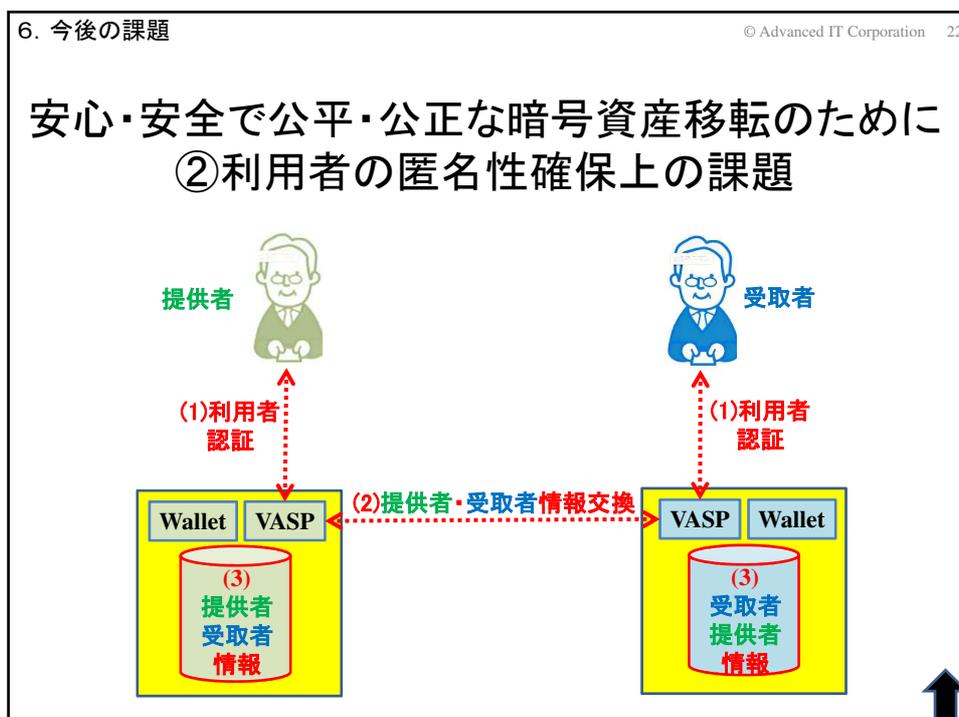
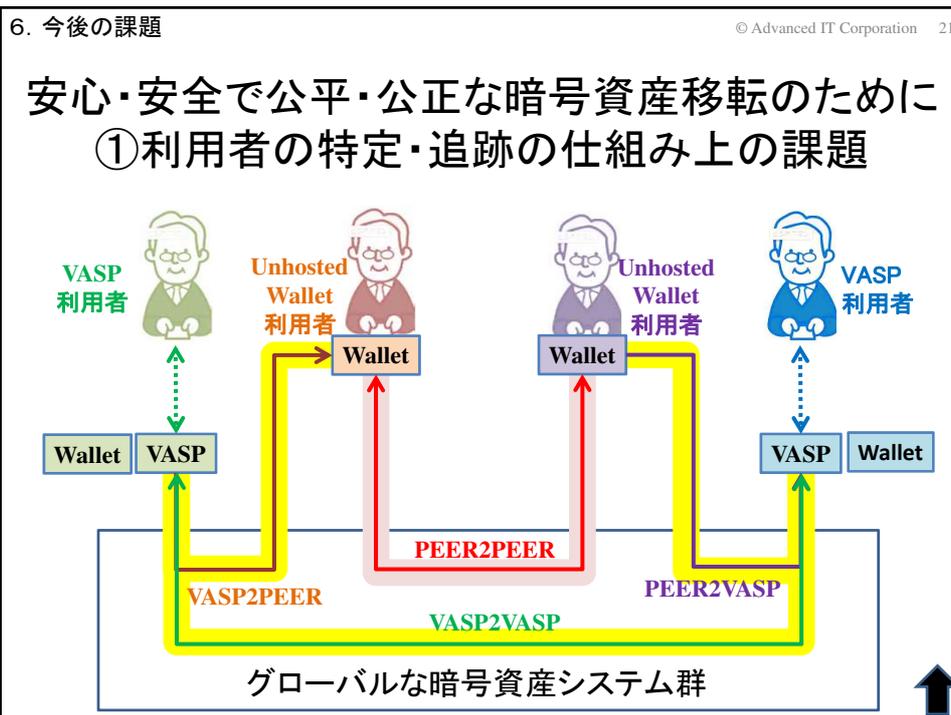
© Advanced IT Corporation 20

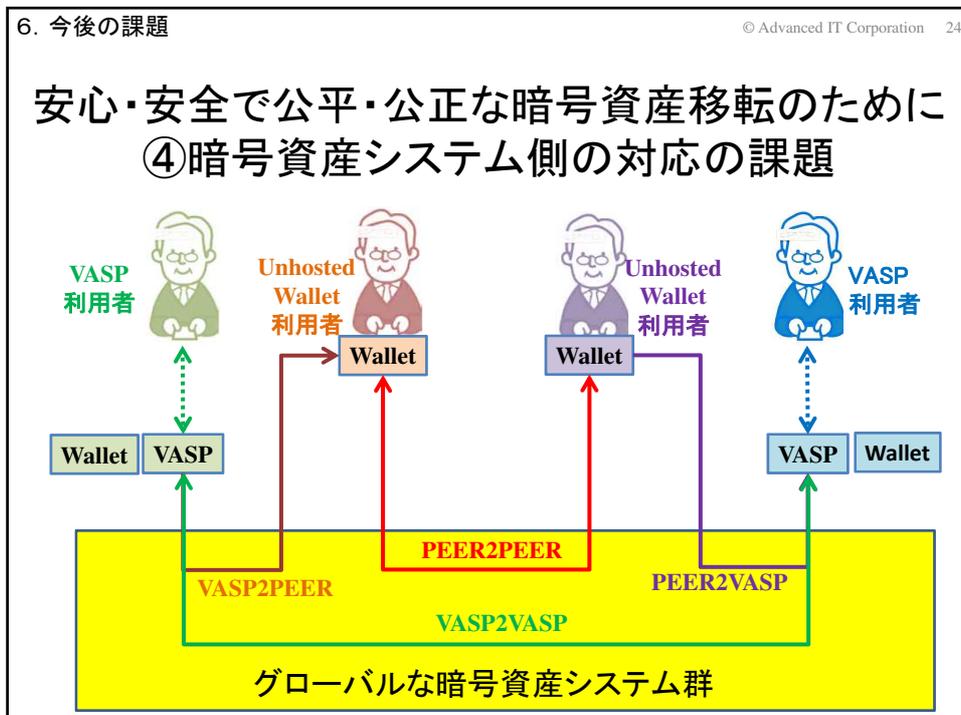
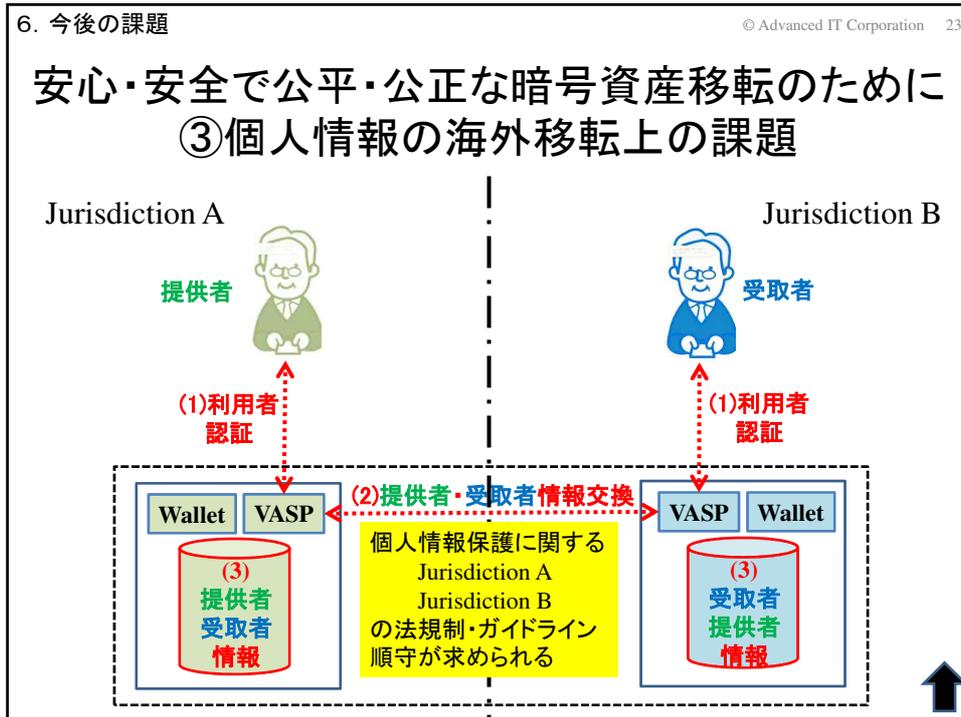
提供者・受取者別 ビットコインランザクション資産総額の推移



Source: CipherTrace Cryptocurrency Intelligence

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





まとめ

(1) 暗号資産の課題は社会の安心・安全上も大きな課題

強い匿名性が確保されているがゆえに、利用者の特定・追跡を困難とし、マネーロンダリングやテロ資金供与、不正・不法な取引の決済手段等、暗号資産が様々な犯罪に活用され、社会の犯罪・悪意を誘発する要因となっていることである。

(2) 暗号資産の課題克服は道半ば

FATFの勧告(トラベルルール)にも、PEER2PEERの暗号資産移転についての対策は含まれておらず、暗号資産業界はまだVASP2VASPの暗号資産移転に対する2019年版トラベルルールへの対応に苦心しているのが現状

(3) 安心・安全で公平・公正な

暗号資産移転の仕組み実現上の課題を整理・考察

- ①利用者の特定・追跡の仕組み上の課題
- ②利用者の匿名性確保上の課題
- ③個人情報の海外移転上の課題
- ④暗号資産システム側の対応の課題

(4) 暗号資産業界の健全な発展のために

安心・安全で公平・公正な暗号資産移転の仕組みに関する研究を推進する予定

終

(ご清聴、ありがとうございました)