

スタートアップ企業の資金調達手段として注目が高まる
暗号資産に関する欧州の規制・動向等についての調査報告書

令和 7 年 10 月

渥美坂井法律事務所・外国法共同事業

目次

第 1.	はじめに	1
I.	背景	1
II.	我が国における規制の状況	1
1.	資金決済法による規制	2
(1)	資金決済法による規制対象	2
(2)	資金決済法による規制内容	3
2.	金融商品取引法による規制	3
(1)	セキュリティトークンに関する規制	3
(2)	暗号資産に関する規制	4
3.	暗号資産に関する自主規制	5
III.	調査の目的	5
第 2.	欧州（EU）における暗号資産等に関する規制	6
I.	MiCA の概要等	6
II.	MiCA の施行について	7
1.	MiCA の施行	7
2.	MiCA の施行に関するモニタリング	7
3.	MiCA の施行に伴う議論	8
4.	マルタ当局において MiCA の施行に関し特筆すべき事項	8
III.	MiCA の章構成について	8
IV.	MiCA が適用される暗号資産の技術的要件	9
V.	MiCA の適用対象外とされる暗号資産及び暗号資産サービスについて	10
1.	発行者の特定できない（no identifiable issuer）暗号資産について	10
(1)	発行者の特定できない暗号資産	10
(2)	発行者の特定できない暗号資産に関する情報提供の実務について	11
(3)	発行者の特定できない暗号資産の規制の動向について	11
2.	完全に分散化された方法で提供される暗号資産サービスについて	11
(1)	完全に分散化された方法で提供される暗号資産サービス	11
(2)	完全に分散化された方法で提供される暗号資産サービスの特徵	12
(3)	完全に分散化された方法で提供される暗号資産サービスに関する各国当局にお ける議論	13
(4)	fully decentralized への該当性判断や新たな規制について	16
(5)	小括	16
VI.	ESMA-EBA が考慮する DeFi に関するリスクについて	16
1.	DeFi に関連する潜在的なリスク	16
2.	DeFi における MEV の抽出によるリスク	17
(1)	MEV とは	17
(2)	MEV の抽出の仕組み	17
(3)	MEV の抽出の弊害	18
3.	DeFi に対する新たな規制について	18
VII.	MiCA における暗号資産サービス業	19
1.	総説	19
(1)	暗号資産サービス業	19
(2)	CASP に共通して課される義務	19
2.	カストディアルウォレットに関する規制	21
3.	CASP に関するエンフォースメント	21
4.	CASP によるサイバーセキュリティ対策	22
5.	無許可の CASP の検知について	22
VIII.	暗号資産の貸付、借入、ステーキングについて	23

1. 総説.....	23
2. 暗号資産貸付及び借入について.....	23
(1) 暗号資産貸付.....	23
(2) 暗号資産貸付に関するサービスの提供方法.....	23
(3) 暗号資産借入.....	24
(4) 暗号資産借入に関するサービスの提供方法.....	24
(5) 暗号資産貸付及び借入に関するリスク.....	24
3. ステーキング.....	25
(1) ステーキング.....	25
(2) ステーキングのためのサービス.....	25
(3) ステーキングサービスの「顧客の代理での暗号資産の保管及び管理」への該当性.....	26
(4) ステーキングに関するリスク.....	26
IX. MiCA における暗号資産の発行・公衆への提供・上場に関する規制.....	26
1. 総説.....	26
2. 公衆への提供・上場について.....	27
(1) MiCA における暗号資産の発行に関する規定について.....	27
(2) 「公衆への提供」について.....	28
(3) 「上場」について.....	28
(4) その他の暗号資産の「公衆への提供」におけるホワイトペーパーの作成が免除される場合.....	28
(5) ホワイトペーパーの記載事項.....	29
(6) 承認・届出・公表.....	29
(7) 資産参照型トークンの発行事例がない背景.....	30
3. 発行・公衆への提供・上場に関する規制に関する罰則.....	31
X. MiCA における発行者の義務.....	31
1. 総説.....	31
2. 償還義務・準備資産に関する要件・自己資本要件・資産保全義務・流動性保持義務について.....	32
(1) 電子マネー・トークン及び資産参照型トークンの償還義務・準備資産に関する要件・自己資本要件・資産保全義務・流動性保持義務.....	32
(2) 準備資産の運用対象として認められている（預金以外の）投資資産.....	36
(3) 追加的な報告義務.....	36
3. 償還義務・準備資産に関する要件・自己資本要件・資産保全義務・流動性保持義務に違反した場合の罰則.....	36
XI. MiCA における暗号資産の不公正な取引に関する規制.....	37
1. 総説.....	37
(1) MAR（市場濫用規制）の参照について.....	37
(2) DeFi サービスにおける不公正取引規制の適用範囲について.....	37
(3) 地域的適用範囲.....	38
2. インサイダー取引規制.....	38
(1) インサイダー情報の定義.....	38
(2) インサイダー情報に関する禁止事項.....	39
(3) 正当化事由の不存在.....	40
3. 相場操縦規制.....	40
(1) 相場操縦に関する規定.....	40
(2) ベンチマークに関する相場操縦規制について.....	42
4. 罰則等.....	42
(1) 罰則.....	42
(2) 罰則に関する事例.....	43

5. フロントランニングの禁止	43
6. 市場濫用行為の検知について	43
(1) 市場濫用に関する規制技術基準	43
(2) その他の暗号資産	44
(3) 市場濫用行為に関する実務	44
第3. 暗号資産関係の詐欺・盗難・不公正取引等の摘発等をした事案の実態	45
I. 欧州（EU）における事案	45
1. 加盟国当局の要請に基づき、欧州連合司法協力庁が捜査を実施した事案	45
2. Operation Endgame	45
II. 香港における事案	45
1. JPEX 詐欺事件	46
2. Mixin ハッキング被害事件	47
3. 仮想通貨によるマネー・ローンダリングの摘発等の事例	47
III. シンガポールにおける事案	47
1. A&A Blockchain 事件	48
2. Amazing tech 事件	48
3. BingX 事件	48
4. その他	48
IV. アメリカにおける事案	49
1. 暗号資産に係る相場操縦に対する SEC による執行事例	49
2. 暗号資産に関する CFTC による執行事例	50
3. デジタル資産プラットフォームの元 CEO を詐欺で提訴した事案	50
4. 小括	50
第4. 暗号資産の不正流出を防ぐための規制や不正流出に対する利用者の救済（保険等）	51
I. 欧州（EU）における事案	51
1. 不正流出を防ぐための規制	51
2. 利用者救済制度	51
II. 香港における事案	51
1. 不正流出を防ぐための規制	51
2. 利用者救済制度	52
III. シンガポールにおける事案	53
1. 不正流出を防ぐための規制	53
2. 利用者救済制度	54
IV. アメリカにおける事案	54
1. 不正流出を防ぐための規制	54
2. 利用者救済制度	54
第5. IEO・ICO等の暗号資産を用いた資金調達の実施状況とそれを促す取組（私募等の柔構造化含む。）	55
I. 欧州（EU）における事案	55
1. 概要	55
2. 実際の取組	55
II. 香港における事案	55
1. 概要	55
2. 実際の取組	56
III. シンガポールにおける事案	58
1. 概要	58
2. 実際の取組	58
IV. アメリカにおける事案	59
1. 概要	59

2.	実際の取組.....	59
第 6.	まとめ	60
1.	暗号資産のホワイトペーパーの公表に関する規制	60
2.	暗号資産に関するインサイダー取引規制及び相場操縦規制	61
3.	暗号資産交換業等による規制の範囲の示唆	61
4.	我が国の暗号資産に関する規制への示唆	62
別表		63

第1. はじめに

I. 背景

日本政府において、「スタートアップ育成5か年計画」（2022年11月28日）を策定し、8000億円規模のスタートアップ企業への投資額を、2027年度に10倍を超える規模（10兆円規模）とすることを目標に掲げ、様々な施策を実行してきているところである。これを受けて、スタートアップ企業数の増加は見られる一方、スタートアップ企業等への資金提供が十分に実施されているとはいえない状況にある。こうした中、近年では Web3 ビジネスを行うスタートアップ企業等もいるところ、そうした企業を中心に、IEO（Initial Exchange Offering¹）等の暗号資産を用いた資金調達を行うことがある。

スタートアップ企業による資金調達環境の更なる整備を図っていく観点から、スタートアップ企業等における資金調達手段として注目が高まっている暗号資産について、無秩序な ICO（Initial Coin Offering²）のような詐欺的な資金調達を防ぎつつ、適切な資金調達手段がどのようなものかを検討する必要がある。

また、このような暗号資産に係る取引については、金融商品取引法におけるインサイダー取引や相場操縦等に相当する行為、又は暗号資産特有の手段を用いた手段により行為者が利益を得ることで、投資者の利益が害されるおそれがある。そのため、これらの行為を防止することが必要である。

以上の状況も踏まえ、包括的な規制が既に施行され、事例の蓄積が始まっていると考えられる欧州を中心に各種の規制の状況や動向調査を実施したものである。なお、本報告書の記載事項は特段の明記がない限り、2025年10月までに確認できている公表資料等に関して調査を行った結果に基づくものであり、各種規制改正や自主規制機関の規程変更等により、将来のある時点の取扱いと本報告書の記載時点におけるその内容が異なる場合がある。また、本報告書において引用している原文の訳は、いずれも渥美坂井法律事務所・外国法共同事業による仮訳である。

II. 我が国における規制の状況

まず、我が国における規制の状況を概観する。日本の法制度の下では、暗号資産は、主として、資金決済に関する法律（以下「資金決済法」という。）及び金融商品取引法の2つの法律によって規律されている。

¹ 企業や団体が発行するトークンを、暗号資産交換業者を介して投資者に販売し、その対価として暗号資産の払込を受ける行為。

² 企業や団体が発行するトークンを投資者に販売し、その対価として暗号資産の払込を受ける行為。

1. 資金決済法による規制

資金決済法において、暗号資産及び電子決済手段の定義（資金決済法第2条第14項³、同条第5項⁴）や、暗号資産取引の中心となる暗号資産交換業者の登録制（資金決済法第2条第16項⁵）、ステーブルコイン取引の中心となる電子決済手段取引業の登録制（資金決済法第2条第12項⁶）を中心に業務運営・利用者保護などを定めており、同法が我が国においては暗号資産及びステーブルコインに関する制度における中心的役割を果たしている。

(1) 資金決済法による規制対象

資金決済法においては、業として「暗号資産」の交換等や管理などを行うことを暗号資産交換業として規制している（資金決済法第2条第15項⁷）。また、「電子決済手段」として、いわゆるステーブルコインを定義し、業として電子決済手段の

³ 資金決済法

第2条

14 この法律において「暗号資産」とは、次に掲げるものをいう。ただし、金融商品取引法第29条の2第1項第8号に規定する権利を表示するものを除く。

- 一 物品等を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨、通貨建資産並びに電子決済手段（通貨建資産に該当するものを除く。）を除く。次号において同じ。）であって、電子情報処理組織を用いて移転することができるもの
- 二 不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの

⁴ 資金決済法

第2条

5 この法律において「電子決済手段」とは、次に掲げるものをいう。

- 一 物品等を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されている通貨建資産に限り、有価証券、電子記録債権法（平成19年法律第102号）第2条第1項に規定する電子記録債権、第3条第1項に規定する前払式支払手段その他これらに類するものとして内閣府令で定めるもの（流通性その他の事情を勘案して内閣府令で定めるものを除く。）を除く。次号において同じ。）であって、電子情報処理組織を用いて移転することができるもの（第3号に掲げるものに該当するものを除く。）
- 二 不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの（次号に掲げるものに該当するものを除く。）
- 三 特定信託受益権
- 四 前三号に掲げるものに準ずるものとして内閣府令で定めるもの

⁵ 資金決済法

第2条

16 この法律において「暗号資産交換業者」とは、第63条の2の登録を受けた者をいう。

⁶ 資金決済法

第2条

12 この法律において「電子決済手段等取引業者」とは、第62条の3の登録を受けた者をいう。

⁷ 資金決済法

第2条

15 この法律において「暗号資産交換業」とは、次に掲げる行為のいずれかを業として行うことをいい、「暗号資産の交換等」とは、第1号又は第2号に掲げる行為をいい、「暗号資産の管理」とは、第4号に掲げる行為をいう。

- 一 暗号資産の売買又は他の暗号資産との交換
- 二 前号に掲げる行為の媒介、取次ぎ又は代理
- 三 その行う前二号に掲げる行為に関して、利用者の金銭の管理をすること。
- 四 他人のために暗号資産の管理をすること（当該管理を業として行うことにつき他の法律に特別の規定のある場合を除く。）。

交換等や管理などを行うことを電子決済手段等取引業として規制し、登録制を定めている（資金決済法第2条第10項⁸）。なお、電子決済手段の定義には特定信託受益権（資金決済法第2条第5項第3号⁹）が含まれており、上記の電子決済手段に係る規制の対象となっている。

(2) 資金決済法による規制内容

規制内容の詳細は以下のとおり。

		暗号資産交換業	電子決済手段等取引業
参入形式		登録	
対象行為		① 暗号資産・電子決済手段の売買、他の暗号資産・電子決済手段との交換 ② ①の行為の媒介・取次ぎ・代理 ③ （暗号資産交換業者のみ）①②の行為に関して行う利用者の金銭の管理 ④ 他人のために行う暗号資産・電子決済手段の管理 ⑤ （電子決済手段等取引業者のみ）資金移動業者を代理して未達債務の増減を行う行為	
主体		株式会社	
財務要件		・資本金1,000万円以上 ・純資産が負の値でないこと	
受託資産の管理		・利用者の暗号資産の分別管理（原則コールドウォレット） ・利用者の暗号資産の管理状況の外部監査 ・利用者の金銭の信託	・利用者の電子決済手段の信託又は分別管理 ・利用者の電子決済手段の管理状況の外部監査 ・利用者の金銭の信託
利用者保護措置		・利用者への情報提供・説明義務 ・一定の表示の禁止（例：虚偽表示、誤認表示、投機を助長するような表示等） ・不適切な暗号資産を取り扱わないための措置等	・利用者への情報提供・説明義務 ・利用者の金銭その他の財産の受託の原則禁止 ・不適切な電子決済手段を取り扱わないための措置等
広告規制		・一定の事項の表示義務（例：暗号資産交換業者の商号、暗号資産の性質等）	・一定の事項の表示義務（例：特定電子決済手段等取引業者の商号） ・特定電子決済手段等取引契約の締結による利益の見込み等の事項について著しく事実に相違する表示及び著しく人を誤認させる表示の禁止
その他	情報の安全管理	情報の漏えい、滅失又は毀損の防止その他の情報の安全管理のために必要な措置	
	委託先管理	当該業務の適かつ確実な遂行を確保するために必要な措置	
AML/CFT		犯収法に基づく義務（取引時確認、疑わしい取引の届出、トラベルルール等）	

金融審議会 資金決済制度等に関するワーキング・グループ（第5回）

事務局説明資料より抜粋

2. 金融商品取引法による規制

(1) セキュリティトークンに関する規制

金融商品取引法においては、2020年5月改正において、いわゆる STO（Security Token Offering）に関する規律が整備された。「企業等が STO によって発行する株式、社債や、受益証券、集団投資スキーム持分等が規制対象となり、信託受益権、集団投資スキーム持分等の金融商品取引法第2条第2項各号に掲げる権利（第二項

⁸ 資金決済法

第2条

10 この法律において「電子決済手段等取引業」とは、次に掲げる行為のいずれかを業として行うことをいい、「電子決済手段の交換等」とは、第1号又は第2号に掲げる行為をいい、「電子決済手段の管理」とは、第3号に掲げる行為をいう。

一 電子決済手段の売買又は他の電子決済手段との交換

二 前号に掲げる行為の媒介、取次ぎ又は代理

三 他人のために電子決済手段の管理をすること（その内容等を勘案し、利用者の保護に欠けるおそれがないものとして内閣府令で定めるものを除く。）。

⁹ 脚注4参照。

有価証券)をトークン(電子情報処理組織を用いて移転することができる財産的価値(電子機器その他の物に電子的方法により記録されるものに限定))に表示したものは、流通性が高まると予想されることから、金融商品取引法上、新たに「電子記録移転権利」と定義され、従来の第二項有価証券ではなく「第一項有価証券」として取扱うこととされた¹⁰⁾ものである。金融商品取引法におけるセキュリティトークンは、電子記録移転有価証券表示権利等(金融商品取引業等に関する内閣府令(以下「業府令」という。))第1条第4項第17号、金融商品取引法第29条の2第1項第8号、業府令第6条の3)として、①金融商品取引法第2条第1項各号の有価証券がトークン化された、有価証券表示権利(金融商品取引法第2条第2項柱書)、②電子記録移転権利(金融商品取引法第2条第3項)、③適用除外電子記録移転権利(金融商品取引法第二条に規定する定義に関する内閣府令第9条の2により②から除外されるもの)に分類できる¹¹⁾。

以上のセキュリティトークンの規制の概要は、以下の通り。

		第一項有価証券		第二項有価証券	
		電子記録移転有価証券表示権利等(デジタル証券)			集団投資スキーム 持分、 信託受益権等
	株式 債券 投資信託等	トークン化 有価証券	電子記録 移転権利	適用除外 電子記録移転権利	
業としての売買	第1種金商業	第1種金商業 (変更登録が必要)		第2種金商業 (変更登録が必要)	第2種金商業
発行者の開示義務	発行・継続開示義務あり (公募であり、発行額1億円以上の場合。トークン 化有価証券、電子記録移転権利は追加項目あり)			原則としてなし (主として有価証券の投資する事業への 出資持分等について、500名以上の投資家 が所有することとなる勧誘を行うもの)	
自主規制機関	日本証券業協会	日本STO協会			第二種金融商品 取引業協会

一般社団法人日本STO協会「セキュリティトークンに関する現状等について」
「デジタル・分散型金融への対応のあり方等に関する研究会」(第11回)より抜粋

(2) 暗号資産に関する規制

以下に挙げるものに関しては、金融商品取引法第2条第24項第3号の2において、「暗号等資産」と定義され、金融商品取引法上の金融商品に含まれる。

- 資金決済法第2条第14項に規定する暗号資産
- 資金決済法第2条第5項に規定する電子決済手段のうち同項第4号で規定するもののうち投資者の保護を確保することが必要と認められるものとして内閣府令で定めるもの

¹⁰⁾ 第11回デジタル・分散型金融への対応のあり方等に関する研究会日本STO協会提出資料「セキュリティトークンに関する現状等について」

<https://www.fsa.go.jp/singi/digital/siryou/20230606/2jstoa.pdf>

¹¹⁾ なお、金融商品取引法に限らず不動産特定共同事業法に基づくセキュリティトークンの発行も認められているが、本報告書の目的を踏まえ、不動産特定共同事業法の詳細な整理は割愛する。

暗号等資産については、相場操縦に対する規制等、一部の不公正取引に対する規制が設けられている（金融商品取引法第 185 条の 22、第 185 条の 23、第 185 条の 24）。なお、暗号資産を含む暗号等資産に関する店頭デリバティブ取引又はその媒介、取次ぎ若しくは代理を業として行う場合には第一種金融商品取引業者の登録が必要である（金融商品取引法第 2 条第 8 項第 4 号、第 28 条第 1 項第 2 号、第 29 条）。

3. 暗号資産に関する自主規制

資金決済法に基づく暗号資産交換業に関しては、一般社団法人日本暗号資産等取引業協会（以下「JVCEA」という。）が認定資金決済事業者協会として認定されている。JVCEA の自主規制規則には、新規暗号資産の販売に関する規則、暗号資産交換業に係る暗号資産関係情報の管理体制の整備に関する規則等のように、インサイダー情報の管理に繋がりうる自主規制も存在するものの、現行の資金決済法及び JVCEA 自主規制規則を全体として見ても、金融商品取引法におけるインサイダー取引規制に相当する、暗号資産のインサイダー取引を禁止する規定は整備されていない。

III. 調査の目的

我が国の暗号資産に関しては、JVCEA が暗号資産交換業者に情報開示を求める自主規制が一部存在するものの、金融商品取引法に相当する発行者に対する開示規制が定められていない。このため、投資者に対して投資判断に必要な情報を提供することを発行者に義務付けることが現行制度上困難であり、結果として不適切又は違法な取引を招来する合理的な可能性がある。

また、暗号資産に関するインサイダー取引規制が定められていないことから、トークンでの資金調達に関する非公開情報を用いたインサイダー取引についても、金融商品取引法のように強制力をもって規制することも現行制度上困難である¹²。

このような状況に鑑みて、欧州において今般整備された、世界的にも先端的な内容を有する暗号資産に関する規制である MiCA (Markets in Crypto-Assets Regulation¹³) を調査し、我が国における暗号資産の規制の際に参照することとしたい。なお、暗号資産に関する犯罪の摘発状況、不正流出を防ぐための規制、トークンによる資金調達に関する取組状況については、欧州以外の法域も調査することとする。

¹² 2023 年 11 月に、証券監督者国際機構（IOSCO）による最終報告書（Policy Recommendations for Crypto and Digital Asset Markets Final Report）が公表され、同報告書では投資者保護／市場の公正・透明性／システミックリスク低減という証券市場規制の基本目的を、暗号資産・デジタル資産（Crypto and Digital Assets: CDA）市場においても適用すべきとの観点が示されている。インサイダー取引についても、同報告書の勧告第 10 において、「規制当局は、CASP に対し、重要な非公開情報の管理に関するシステム、方針及び手続を整備するよう求めるべきである。これには、該当する場合、暗号資産が自社プラットフォームで取引可能（上場・取扱承認）となるかどうかに関する情報や、顧客注文、取引執行、個人識別情報などに関する情報の管理も含まれる（Regulators should require a CASP to put in place systems, policies and procedures around the management of material non-public information, including, where relevant, information related to whether a crypto-asset will be admitted or listed for trading on its platform and information related to client orders, trade execution, and personally identifying information.）」として一定の規制に服すべきことが勧告されている。この最終報告書を踏まえた各国の対応状況を踏まえて、日本における規制の在り方を検討することは極めて有意義であるといえる。

¹³ European crypto-assets regulation (MiCA)
<https://eur-lex.europa.eu/EN/legal-content/summary/european-crypto-assets-regulation-mica.html>

また、当該調査に加え、我が国の金融商品取引法及び資金決済法と、MiCA における暗号資産及びステーブルコインに関する規制を比較する限度において、ステーブルコインの発行者に課された義務や CASP（Crypto-Asset Service Provider）に課された規制も調査することとしたい。

加えて、暗号資産に関する取引は時々刻々と変化をしているものであり、特に分散化などについては、従来の金融取引とは異なり、意思決定の主体や関連する主体間の関係性の多様性も踏まえ、そのような取引による将来的な金融取引の高度化の可能性もあるものの、一方で、将来的に適切な金融規制を整備するためには十分な調査・検討が現時点で必要である。このような視点を持って、現行の MiCA において規制の対象外とされている暗号資産や完全に分散化された（fully decentralized）暗号資産サービスに関する議論を調査することで、我が国における将来的な規制を検討する際の参考とされたい。

なお、本調査では、MiCA の制度設計・実施状況・監督運用の実態を多角的に把握するため、EU レベル及び加盟国レベルの主要関係機関である EC（European Commission）、マルタ当局等をヒアリング対象として選定した。

EC は MiCA の策定主体であり、マルタ当局は EU 域内で最も早期に CASP 登録制度を運用している主管当局の一つであることから（第 2.Ⅱ4 参照）、制度設計と現場運用の両面を把握する上で最適と判断した。

第2. 欧州（EU）における暗号資産等に関する規制

I. MiCA の概要等

MiCA は EU における暗号資産に関する新たな包括的な規制枠組みである。その概要は次のとおりである。

概要	① その他の暗号資産、電子マネートークン及び資産参照型トークンの発行・公衆への提供・上場、 ② CASP に対する行為規制、 ③ インサイダー取引や相場操縦などの不公正取引の禁止等について、EU 域内で統一的な規制枠組みを定めるもの。 EU 加盟国は MiCA の規制に応じた国内法を整備することが義務付けられている。
目的	暗号資産に関する包括的な規制によって法的な明確性を高め、顧客保護と市場の公正性を確保しながら、イノベーションと公正な競争を促進すること（MiCA 前文(6)）
暗号資産の分類	暗号資産を次の 3 つに分類 ● 電子マネートークン（electronic money token、単一の法定通貨の価値を参照するステーブルコイン等） ● 資産参照型トークン（asset-referenced token） ● その他の暗号資産（電子マネートークン及び資産参照型トークン以外の暗号資産）

行為規制	上記の暗号資産の分類に応じて、暗号資産の発行、公衆への提供、取引所への上場の各行為について規制 ¹⁴
	暗号資産に関するサービスを提供するためには、各国当局の認可取得を義務付け、預託を受けた暗号資産の分別管理義務やサービス内容の開示といった顧客保護のための義務を課す規制
開示規制	暗号資産発行の際に発行者が作成すべきホワイトペーパーの内容及び開示手続を規制
不公正取引規制	暗号資産に関するインサイダー取引と相場操縦を禁止

II. MiCA の施行について

1. MiCA の施行

MiCA は 2023 年 6 月に公布され、規定により一部（ステーブルコイン関連）は 2024 年 6 月から、大部分（その他 CASP 規制等）は 2024 年 12 月 30 日から適用開始となった。MiCA 第 143 条は、施行時点で各国法の下で営業していた CASP に対し、各加盟国が定める一定期間（最長 2026 年 6 月末まで）の猶予を認めている。加盟国各国の適用延期に関する定めは以下のとおり¹⁵。

- MiCA 第 143 条が許容する最大 18 か月の適用延期（2026 年 6 月末まで）を選択した国：イタリア、エストニア、キプロス、クロアチア、チェコ、デンマーク、フランス、ブルガリア、ベルギー、マルタ、ルクセンブルク、ルーマニア
- 12 か月の適用延期（2025 年 12 月末まで）を選択した国：アイルランド、オーストリア、ギリシャ、スペイン、スロバキア、ドイツ、ポルトガル、リトアニア
- 9 か月の適用延期（2025 年 6 月末まで）を選択した国：スウェーデン
- 6 か月の適用延期（2024 年 12 月末まで）を選択した国：オランダ、ハンガリー、フィンランド、ポーランド、ラトビア

2. MiCA の施行に関するモニタリング

EC へのヒアリングによれば、マルタ当局では、MiCA 施行から CASP に対するライセンス付与までの期間が非常に短かったことから、EC により、マルタ当局が MiCA を完全に施行しているかの調査を実施したとのことである。もっとも、当該調査の結果、マルタにおける MiCA の完全な施行が確認されたとのことである。このように、EC においては、加盟国による MiCA の施行状況をモニタリングし、MiCA の完

¹⁴ ただし、ビットコインやイーサリアムなどの識別可能な発行者が不在とされる暗号資産についてはこれらの行為規制は適用されない（MiCA 前文(22)）。なお、ビットコインやイーサリアムが発行者不在の暗号資産とされていることはマルタ当局へのヒアリングにおいて確認済み。

¹⁵ List of grandfathering periods decided by Member States under MiCA
https://www.esma.europa.eu/sites/default/files/2024-12/List_of_MiCA_grandfathering_periods_art._143_3.pdf

全な施行に疑義が存在する場合には、必要な調査を実施し、施行状況を確認している模様である。

3. MiCA の施行に伴う議論

EC へのヒアリングによれば、MiCA の施行に伴い、マルチイシュアンス（multi-issuance。EU 域内で発行された暗号資産について、互換性のある暗号資産を EU 域外でも発行すること。）について、一部の加盟国から違法であるとの指摘が寄せられたことが明らかとなった。もっとも、最終的には、マルチイシュアンスは MiCA において想定されているとして違法ではないとの結論に至ったとのことである。

4. マルタ当局において MiCA の施行に関し特筆すべき事項

マルタでは、MiCA で義務付けられていない独自の定期報告制度を導入したほか、MiCA 規則を補完するガイダンスとして MiCA Rulebook¹⁶を公開している。また、MiCA に特化したものではないものの、制裁金算定要素を明示したエンフォースメント・ポリシー¹⁷も公表された。

III. MiCA の章構成について

MiCA の章構成は次のとおりとなっている。条（Article）については、特に有意なものについて記載した。

前文（Whereas）

TITLE I 対象事項、範囲及び定義（SUBJECT MATTER, SCOPE AND DEFINITIONS）

TITLE II 資産参照型トークン又は電子マネートークン以外の暗号資産（CRYPTO-ASSETS OTHER THAN ASSET-REFERENCED TOKENS OR E-MONEY TOKENS）

第4条 公衆への提供

第5条 取引所への上場

第6条 暗号資産ホワイトペーパーの内容と形式

第7条 広告

第8条 ホワイトペーパー及び広告の届出

第9条 ホワイトペーパー及び広告の公表

第10条 公衆への提供結果及び資産保全

第11条 公衆への提供者及び取引所上場申請者の権利

第12条 ホワイトペーパー及び広告の修正

第13条 払戻しの権利

第14条 公衆への提供者及び取引所上場申請者の義務

第15条 ホワイトペーパーに記載された情報に関する責任

TITLE III 資産参照型トークン（ASSET-REFERENCED TOKENS）

¹⁶ MiCA Rulebook

<https://www.mfsa.mt/wp-content/uploads/2025/03/MiCA-Rulebook.pdf>

¹⁷ Guidance Note on the Methodology to Set Administrative Penalties Imposed on Entities and Individuals

<https://www.mfsa.mt/wp-content/uploads/2022/05/Guidance-Note-on-the-Methodology-to-Set-Administrative-Penalties-Imposed-on-Entities-and-Individuals.pdf>

CHAPTER 1	公衆への提供及び取引所への上場申請に関する認可
CHAPTER 2	発行者の義務
CHAPTER 3	準備資産
CHAPTER 4	発行者の買収
CHAPTER 5	重要な資産参照型トークン
CHAPTER 6	回復・償還計画
TITLE IV	電子マネートークン (E-MONEY TOKENS)
CHAPTER 1	電子マネートークンのすべての発行者が満たすべき要件
CHAPTER 2	重要な電子マネートークン
TITLE V	CASP の認可及び業務条件 (AUTHORISATION AND OPERATING CONDITIONS FOR CRYPTO-ASSET SERVICE PROVIDERS)
CHAPTER 1	CASP に関する認可
CHAPTER 2	すべての CASP の義務
CHAPTER 3	特定の CASP の義務
CHAPTER 4	CASP の買収
CHAPTER 5	重要な CASP
TITLE VI	暗号資産に関連する市場濫用の防止及び禁止 (PREVENTION AND PROHIBITION OF MARKET ABUSE INVOLVING CRYPTO-ASSETS)
第 86 条	市場濫用に関する規則の適用範囲
第 87 条	内部情報
第 88 条	内部情報の公開
第 89 条	インサイダー取引の禁止
第 90 条	内部情報の不法開示の禁止
第 91 条	相場操縦の禁止
第 92 条	市場濫用の防止及び検知
TITLE VII	主管当局、EBA、ESMA (COMPETENT AUTHORITIES, EBA AND ESMA)
CHAPTER 1	各主管当局の権限および主管当局・EBA・ESMA 間の協力
CHAPTER 2	ESMA 登録簿
CHAPTER 3	主管当局による行政制裁およびその他の行政措置
CHAPTER 4	重要な資産参照トークンおよび重要な電子マネートークンの発行者、ならびに監督カレッジに関する EBA の監督責任
CHAPTER 5	重要な資産参照トークンおよび重要な電子マネートークンの発行者に対する EBA の権限と職掌
TITLE VIII	委任法令 (DELEGATED ACTS)
TITLE IX	移行規定及び最終規定 (TRANSITIONAL AND FINAL PROVISIONS)
別紙 (ANNEX)	

IV. MiCA が適用される暗号資産の技術的要件

MiCA の適用対象となる暗号資産は、MiCA 第 3 条第 1 項において、以下のとおり規定されている。

- 暗号資産
分散型台帳技術又はこれに類似する技術を用いて電子的に移転及び保存可能な価値又は権利のデジタル表示 (a digital representation of a value or of a right)

that is able to be transferred and stored electronically using distributed ledger technology or similar technology) (同項(5))

なお、暗号資産の定義の中で使用されている「分散型台帳技術」についても同項において下記のとおり規定されている。

- 分散型台帳技術 (distributed ledger technology、以下「DLT」という。)
分散型台帳の運用及び使用を可能にする技術 (a technology that enables the operation and use of distributed ledger) (同項(1))
- 分散型台帳 (distributed ledger)
取引記録を保持する情報デポジトリであり、コンセンサスメカニズムを用いて、一連の DLT ネットワークノード間で共有され、同期されるもの (an information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism) (同項(2))

V. MiCA の適用対象外とされる暗号資産及び暗号資産サービスについて

MiCA の定める暗号資産の技術的要件に該当する場合であったとしても、当該暗号資産の発行者が特定できない場合には、暗号資産の発行に関する規制が適用されない。また、暗号資産サービスが完全に分散化された方法で提供される場合には、CASP に関する規制を適用しないとされている (MiCA 前文(22))。発行者の特定できない暗号資産及び完全に分散化された暗号資産サービスに関する規定の詳細は下記のとおりである。

1. 発行者の特定できない (no identifiable issuer) 暗号資産について

(1) 発行者の特定できない暗号資産

MiCA 前文(22)は、「暗号資産に特定可能な発行者が存在しない場合、当該暗号資産は本規則の第 II 編、第 III 編又は第 IV 編の適用範囲に含まれるべきではない。(Where crypto-assets have no identifiable issuer, they should not fall within the scope of Title II, III or IV of this Regulation.)」と記述している。暗号資産の発行者が特定できない (no identifiable issuer) 場合には、ホワイトペーパー作成・通知・公表といった義務を特定の者に課することが困難であるためである。なお、EC に対するヒアリングにおいては、ビットコイン、イーサリアム、ソラナには特定可能な発行者がおらず、発行者が特定できない暗号資産に該当するという旨の見解が示された。もっとも、その場合であっても、CASP は、取り扱う暗号資産について以下の点を含む一定の義務が課せられている。

- 顧客に対し、公正かつ明確で誤解を招かない情報を提供する義務 (MiCA 第 66 条第 2 項)
 - 顧客に対し、暗号資産取引に伴うリスクについて警告する義務 (MiCA 第 66 条第 3 項)
 - 顧客に対し、自らがサービスを提供する各暗号資産の発行に用いられるコンセンサスメカニズムが気候その他の環境に及ぼす影響に関する情報を自社のサイトの目立つ場所において一般向けに提供する義務 (MiCA 第 66 条第 5 項)
- そのため、CASP が、発行者の特定できない暗号資産を扱う場合であっても、上記情報提供義務を含めた一定の義務を顧客に対して果たさなければならない。

なお、この点について、ベルギー当局（Financial Services and Markets Authority）は、その公表資料において発行者が特定できないビットコインに関しても、CASP が取扱う場合には、MiCA に基づく情報提供義務を負う旨の見解を示している¹⁸。また、EC へのヒアリングにおいては、「暗号資産業界における義務を負う主体とは、MiCA に基づき認可された CASP である。」との見解が示されており、この見解は、ベルギー当局の見解と整合する。

(2) 発行者の特定できない暗号資産に関する情報提供の実務について

発行者を特定することが可能であり、MiCA に基づくホワイトペーパーの公表を通じて情報が提供される暗号資産に関しては、CASP が当該暗号資産を取り扱う際に、発行されたホワイトペーパーを参照することで、自己の情報提供義務を果たすことが可能である。一方、発行者の特定できない暗号資産に関しては、CASP が参照可能な資料が公表されていないため、CASP 自身で当該暗号資産に関するコンセンサスメカニズムの情報を調査し顧客に対する情報提供を行うことが想定される。既に CASP の認可を取得済みの事業者¹⁹においても、ビットコインについてコンセンサスメカニズムを公表している場合があることが確認できた²⁰。ESMA を含む欧州当局は、発行者の特定できない暗号資産に関する情報提供の方法について、現時点ではガイドラインを定めていないため、各 CASP において必要な情報を収集し適宜の方法で情報提供をしなければならない。

(3) 発行者の特定できない暗号資産の規制の動向について

公開資料において、発行者の特定できない暗号資産に関して新たな規制を課すことや CASP における情報提供義務を定めたガイドラインを発出する予定について確認することは出来なかった。

2. 完全に分散化された方法で提供される暗号資産サービスについて

(1) 完全に分散化された方法で提供される暗号資産サービス

MiCA 前文(22)において、「暗号資産サービスが仲介者なしで完全に分散化された方法で提供される場合、当該サービスは本規則の適用範囲に含まれるべきではない。（Where crypto-asset services are provided in a fully decentralized manner without any intermediary, they should not fall within the scope of this Regulation.）」とある。完全に分散化された方法で提供される暗号資産サービスの提供については MiCA の規制の適用除外とされることとなる。

なお、EC へのヒアリングによれば、同条の「仲介者なし」とはサービスの提供（自然人又は法人が職業的な立場で、対価を得るために行動すること）がない（特定できない）ことを意味するとのことであつた²¹。

¹⁸ <https://www.fsma.be/en/faq/20-what-impact-mica-regulation>

¹⁹ <https://www.esma.europa.eu/sites/default/files/2024-12/CASPS.csv>

²⁰ <https://www.bitpanda.com/en/prices/bitcoin-btc#esg-disclosure>

²¹ なお、EC へのヒアリングによれば、「十分に分散化されている」または「完全に分散化されている」という概念を定義するガイダンスを策定する予定はなく、必要とも考えていないとのこと。また、この議論は米国での「いつ十分に分散化されればルールの対象外となるか」という議論に端を発するものであるが、EU では同様の議論はなく、仲介者の有無に基づいて線引きを行っているとのことである。

(2) 完全に分散化された方法で提供される暗号資産サービスの特徴

現時点では、ESMA においては、fully decentralized の要件該当性について公式見解を示してはいないものの、ESMA-EBA (European Banking Authority) は、MiCA 第 142 条に基づき公表したレポート（以下「ESMA-EBA レポート」という。）²² において、DeFi サービスの提供方法について定めている。ESMA-EBA レポート 5 頁 10.において、DeFi サービスと完全に分散化された方法で提供される暗号資産サービスの関係性については明示的な記載はされていないものの、DeFi の意味として、「ブロックチェーンネットワーク上に構築された金融アプリケーションの体系であり、従来の金融システムの一部機能を、表面的にオープンかつ許可不要な形で再現し、従来型の金融仲介者や中央集権的機関を排除することを目的とするもの (a system of financial applications built on blockchain networks that aims to replicate some of the functions of the traditional financial system in a seemingly open and permissionless way, eliminating traditional financial intermediaries and centralized institutions.) 」としている。ESMA-EBA レポートの当該定義と MiCA 前文(22)の内容を踏まえると、DeFi サービスは、概ね完全に分散化された方法で提供されるものであり、MiCA の適用対象外とされると理解しても問題ない。ESMA-EBA レポートにおいては、DeFi サービスの特徴として、①DeFi アプリケーションインターフェースの利用、②アンホステッドウォレットを通じた利用、③中央集権型暗号資産取引プラットフォームを通じた提供を挙げているが、これらの特徴は完全に分散化された方法で提供される暗号資産サービスの特徴にも該当するものと考えられる。①～③の詳細は以下のとおりである。

- ① DeFi アプリケーションインターフェースは、プロトコルへのフロントエンドアクセスを提供し、顧客が高度な技術的知識やブロックチェーンの専門知識を必要とせずに、貸付、ステーキングなど多様な金融活動にウェブベースのインターフェースを通じて参加することを可能にする。これらのインターフェースは、第三者を介することなく、顧客による各種操作の自動化を支援する (ESMA-EBA レポート 12 頁 47.)。
- ② 顧客のアンホステッドウォレットは DeFi の不可欠な要素であり、十分な技術知識を持つ顧客が独自のインターフェースを通じて、あるいは外部 DeFi アプリケーションインターフェースにウォレットを接続することで、DeFi プロトコルとやりとりすることを可能にする (ESMA-EBA レポート 13 頁 49.)。そして、アンホステッドウォレットについて、顧客が秘密鍵を紛失すると資産へのアクセスが永久に失われる (ESMA-EBA レポート 13 頁 50.)。
- ③ 中央集権型のプラットフォームは、顧客のアンホステッドウォレットと連動し、法定通貨から暗号資産への交換や、暗号資産から法定通貨への交換を容易にし、顧客の DeFi へのアクセスを促進する上で重要な役割を果たしている (ESMA-EBA レポート 14 頁 53.)。

このように、ESMA は、DeFi サービスの特徴について述べているが、完全に分散化された暗号資産サービスとの関係で重要な要素としては、上記の①及び②の特徴であると考えられる。すなわち、顧客自身が、(i)アンホステッドウォレット

²² ESMA75-453128700-1391 Joint Report on the recent developments in crypto-assets (Article 142 of MiCAR)
<https://www.eba.europa.eu/sites/default/files/2025-01/5fe168a2-e5a6-41a1-a1b4-87a35e9ebb5c/Joint%20Report%20on%20recent%20developments%20in%20crypto-assets%20%28Art%20142%20MiCAR%29.pdf>

において秘密鍵を管理し（上記②参照）、(ii)DeFi アプリケーションインターフェースを利用して分散型台帳へアクセスし取引を実行すること（上記①参照）で、MiCA 前文(22)が記述する仲介者のいないサービスを実現することが可能であると考えられる。

(3) 完全に分散化された方法で提供される暗号資産サービスに関する各国当局における議論

完全に分散化された方法で提供される暗号資産サービスへの要件該当性について各国で活発な議論がなされている。参考として、フランス当局、デンマーク当局及びマルタ当局の公表資料又はヒアリングにおける見解を以下に紹介する。いずれの見解においても仲介者のいないサービス提供を実現するための方法について言及している。

① フランス当局の公表資料での見解

フランス当局の公開したディスカッションペーパー²³において、DeFi の特徴として、以下の3点が挙げられている。(2)において言及したとおり、DeFi の特徴は、完全に分散化された方法で提供される暗号資産サービスの特徴にも該当するところ、以下の特徴は、完全に分散化された方法で提供される暗号資産サービスの判断の参考となるものと考えられる。

A. 自動化され、分散化され、仲介者を排除したブロックチェーンプロトコル

取引処理やアクセス資格を単一の主体が決定しないことを指摘している。

B. スマートコントラクト機能

スマートコントラクト機能を DeFi のもっとも重要な特徴とした上で、スマートコントラクト機能を、取引実行のためにあらかじめ定められた条件が満たされているかを自動的に評価し、当事者の現実世界の契約機能を再現することを目的としたコードとしている。

C. 分散型アプリケーション

顧客がスマートコントラクトの機能を利用できるようにするためのソフトウェアアプリケーションを「分散型アプリケーション」として定義した上で、分散型アプリケーションの特徴としては、アプリケーションのコードが、利用者が再利用や修正が可能となるように公開されている必要があるとしている。

このように、フランス当局の見解も ESMA の見解同様、「仲介者なし」で提供される暗号資産サービスの特徴について言及されている。同見解においては、スマートコントラクト機能による取引の自動実行が重視されている。これは、サービス利用者の指示により取引が自動実行されることで、仲介者なしで

²³ AMF Discussion Paper on Decentralised Finance VEN
<https://www.amf-france.org/sites/institutionnel/files/private/2023-06/AMF%20Discussion%20Paper%20on%20Decentralised%20Finance%20VEN.pdf>

のサービス提供を実現するための要素であると考えられる。また、DeFi の使用例として次のようなものが挙げられている。

- A. 自動化マーケットメーカー（Automated Market Maker、以下「AMM」という。）・分散型取引所（Decentralized Exchange、以下「DEX」という。）

AMM 及び DEX は、暗号資産の交換を可能にするプロトコルの一種であり、取引当事者を結びつける役割を果たす。AMM 及び DEX では、オンチェーンで稼働し、スマートコントラクトによって人手を介さずに取引フローを自動的に管理する点に特徴がある。

- B. 貸付

貸付プロトコルは、暗号資産の貸し手と借り手を結びつけるものであり、預託者が自身の資産をステークすることで、通常はステーブルコイン形式の貸付を受けることが可能となる。預託された資産は、貸付に対する担保として機能する。

- C. ステーキング

顧客が資産を預け入れることで報酬（例：利息）を得られる仕組みを提供する。あるプロトコルでは、顧客がイーサ（Ethereum プロトコルのネイティブトークン）をステークすることで、ブロックチェーンの PoS（Proof of stake）メカニズムを通じて取引の検証に参加できる。この仕組みにより、新たなイーサがブロック生成に伴って発行され、検証者に対して、預け入れたステーク量に応じて報酬として分配される。

- D. アグリゲーター活動

複数のプロトコルにおける暗号資産の取引状況を把握してデータを集約することで、より良好な流動性や価格設定を提供することを可能とする。

- E. 予測市場（Prediction Markets）

将来の事象の結果に基づいて支払が行われる契約に顧客が参加できる仕組みである。予測市場においては、報酬は原資産やその価値ではなく、事象そのものに基づいて提供される。予測市場は経済活動の一形態として「ベッティング（賭け）」に最も近いものと位置づけられる。

- F. 資産管理

資産管理型の DeFi プロトコルは、顧客が自身の資産を購入・売却・移転するなどの形で管理できるように設計されている。DeFi においては資産保有者自身が戦略を策定・定義し、スマートコントラクトにより実行されることになる。

- G. マージン取引

マージン取引のプロトコルでは、第三者から借り入れた資金を用いて資産取引することが可能となる。外国為替（Forex）などの一部の従来型金融市場における証拠金取引やレバレッジ取引と類似している。

- H. デリバティブとシンセティック（合成）資産

他の「原資産」の価格に連動して価値が決定される金融商品を取引することが可能となる。これにより顧客は原資産又はその市場への間接的なエクスポージャーを得ることができる。

- I. 保険

顧客に対して損失補償を提供することを可能とするサービスもある。従来型の保険商品を模倣・代替しようとするものもあれば、DeFi プロトコ

ルに関連する事象（例：価格暴落、プロトコルのハッキング）に起因する損失に対して特定の補償を提供するものもある。

② デンマーク当局の公表資料での見解

デンマーク当局の公開したディスカッションペーパー²⁴においても、DeFiの特徴を整理しているが、同ディスカッションペーパーの目的においては、MiCA前文(22)の規定を参照した上で、「MiCAの規制の適用外とされる場合を評価すること」を目的としている。そのため、ESMA-EBA レポートにおいて言及されるDeFiの特徴については、MiCAにおける完全に分散化された方法で提供される暗号資産サービスを理解する上で有益なものになっていると考えられる。

DeFiの特徴として、特定の暗号資産サービスの提供が特定の法人の影響下にある場合には、**fully decentralized**に該当しないものと整理している。

特定の法人の影響下にあるか否かに関する考慮要素としては、暗号資産に関する技術自体の分散化とガバナンスの分散化を挙げている。まず、暗号資産に関するサービスが技術的に分散化されているかが考慮され、技術的に分散化されていないと判断された場合、ガバナンスの分散化の有無について検討することとされている。技術的分散化やガバナンスの分散化に関する詳細は以下のとおり記載されている。

A. 技術的分散化

技術的分散化の評価において、スマートコントラクト機能と分散型台帳の管理の方法について言及

B. ガバナンスの分散化

基本的には、特定の暗号資産サービスを運営するパートナーシップについて法的主体となり得る法人が形成されているかが最初に考慮され、仮に、そのような法人が形成されていないとしても、パートナーシップ構成員に付与されるガバナンストークンに関する権利内容や特定のパートナーシップ構成員に意思決定の権限が集中していないかといった事項を考慮する必要があるとされている。

③ マルタ当局へのヒアリングでの見解

マルタ当局へのヒアリングにおいて、DeFiに関して、次の判断基準が言及された。フランス当局の見解やデンマーク当局の見解同様、マルタ当局の見解に関しても、DeFiの判断基準が、完全に分散化された方法で提供される暗号資産サービスの判断基準の参考となるものと考えられる。

- A. オープン又はパーミッションレス型のブロックチェーン上で自律的に実行されること。
- B. 特定可能な中央運営者又は管理者がいないこと。
- C. オフチェーンの仲介者に依存しないこと。
- D. ルールを変更するために使用できる実質的な特権管理者キーや緊急バックドアが存在しないこと。

²⁴ Principles for the assessment of decentralisation in the markets for crypto-assets
https://blockchain.lawyer/assets/pdf/euci/2024_principles_decentralization.pdf

その上で、この基準との関係で、真に **fully decentralized** のプラットフォームに遭遇したことは一度もなく、常に何らかの管理主体が存在することについても言及している。

DeFi に関する具体的な事例に関し、アンホステッドウォレットの類型として、MetaMask などのソフトウェアウォレット、Ledger などのハードウェアウォレット、サービスプロバイダーを介さずブロックチェーン上で直接作成されたアドレスが関与する方法で使用するウォレットが挙げられた。

(4) **fully decentralized** への該当性判断や新たな規制について

EC へのヒアリングによれば、現時点で **fully decentralized** 該当性を判断するための新たなガイダンスや立法措置は検討されていないとのことであった。また、同ヒアリングでは、真に **fully decentralized** と言えるものはごく少数だと評価しているとの指摘もなされたが、その指摘は、一般に DeFi と称されるサービスの多くは、仲介者、サービスプロバイダーが存在しているとの認識に基づくものである。

ESMA-EBA レポートや EU 加盟国の規制当局によるディスカッションペーパーは、**fully decentralized** の該当性判断に際して一定の指針を示すものとはなっているが、現時点では必ずしも見解の統一には至っていないように見受けられる。

(5) 小括

EU 加盟国の規制当局の見解を踏まえても、**fully decentralized** の該当性判断について、容易に該当するものではないとの大枠という、一定の解釈の方向性を示すものとはなっているが、詳細な判断基準等については、現時点では必ずしも見解の統一には至っていないものと見受けられる。

VI. ESMA-EBA が考慮する DeFi に関するリスクについて

ESMA-EBA は、ESMA-EBA レポートにおいて、次のとおり、DeFi に関するリスクについても考慮対象としている。DeFi は、完全に分散化された方法で提供される暗号資産サービスの特徴も有するところ、ESMA-EBA レポートで指摘されているリスクは、MiCA の適用対象外とされる暗号資産サービスに関して、ESMA-EBA が考慮しているリスクと共通のものがあると考えられる。

1. DeFi に関連する潜在的なリスク

ESMA-EBA は、DeFi による暗号資産市場への影響や潜在的なリスクとして、以下の着眼点を指摘している。

- DeFi においては、サービス利用者の管理するアンホステッドウォレットにおいて秘密鍵を管理しているため、アンホステッドウォレットへのサイバー攻撃により暗号資産が盗難されるリスクが存在する。実際に、秘密鍵の侵害による DeFi からの暗号資産の盗難額は、DeFi における全暗号資産盗難額の 50% を占める。ハッキングの件数と盗難された暗号資産額は、最近では、オンチェーン（スマートコントラクト機能等）への攻撃よりもオフチェーン（アンホステッドウォレットへのアクセス権を与える秘密鍵の侵害等）への攻撃による成功率の方が高い（ESMA-EBA レポート 14 頁 55.）。

- スマートコントラクトの悪用による暗号資産の盗難のリスクにも言及されている。スマートコントラクトの悪用の方法としては、スマートコントラクトに利用されている数式やプログラミングの誤りを利用して悪用するケースがあり、スマートコントラクトによる取引実行は第三者の検証なく自動実行されるため、このような問題が生じる（ESMA-EBA レポート 18 頁 70.）。
 - DeFi については、AML/CFT 規制枠組みと管理が欠如している。特に、ノンカストディアルウォレットについて AML/CFT 規制枠組みが困難なことについて問題意識が持たれている（EC へのヒアリングにおいてもその旨言及された。）。
 - DeFi においては、DeFi プロトコルのガバナンスが分散化されているため、51% のガバナンス権限を取得することにより、自己にとって有利なガバナンスに関する決定が下されるリスクも存在する（ESMA-EBA レポート 19 頁 79.）。
 - DeFi は仲介者なしで利用することが可能であるため匿名での利用が可能であり、AML/CFT に関するリスクが存在する（ESMA-EBA レポート 2 頁 2.3.4.）。
- このように、2.V.で言及した DeFi の特徴に起因して、一定のリスクが生じている。

2. DeFi における MEV の抽出によるリスク

ESMA-EBA レポートにおいては、MEV (Maximal Extractable Value) の抽出が DeFi に与える影響についても記載されている。

(1) MEV とは

MEV とは、ESMA-EBA レポート 27 頁 100.において、「ブロックチェーンのマイナー、バリデーター²⁵、ブロック構築バリューチェーン内のその他の主体が、ブロック生成プロセス中に取引を含める、除外する、又は順序を変更することで得られる最大価値を指す(MEV refers to the maximum amount of value a blockchain miner, validator or another agent in the block-building value chain make by including, excluding, or changing the order of transactions during the block production process.) 」とされている。

(2) MEV の抽出の仕組み

ブロックチェーンに取り込まれていない取引は、マイナーによる PoW (Proof of work) やバリデーターによる PoS による検証によってブロックチェーンに取り込まれることとなる。PoW や PoS のためには、取引執行者からマイナーやバリデーターに対してガス代が支払われる。そのため、未検証の取引よりも高いガス代を設定して取引を執行することで、先行する取引よりも先に PoW や PoS によりブロックチェーンに取引を取り込むことが可能となる。MEV の抽出の主体となりうる者及びその実施方法は以下のとおりとされている (ESMA-EBA レポート 27 頁 100.)。

²⁵ ステーキングを通じて取引やブロックの正当性を検証・承認するブロックチェーンの参加者を指す一般的な名称

① MEV の抽出の主体

MEV の抽出により利益を得る者は、一般的に MEV サーチャーと呼ばれている。MEV サーチャーは単独又は複数において、未検証の取引から収益機会を特定し、最も収益性の高いガス代（未検証の取引のガス代よりも高いが、当該取引により早く検証を実施してもらうための最低額）を設定し取引を執行する。MEV サーチャーが得られた利益の一部はマイナーやバリデーターに提供される（ESMA-EBA レポート 29 頁 107.）。

② MEV の抽出の方法

- 裁定取引
異なる市場間において未検証の取引の価格差を利用して利益を得る方法
- フロントランニング取引
未検証の取引よりも高い手数料で同じ取引を執行する方法
- サンドイッチ攻撃
先行する取引により取引の価格を操作し、被操作対象の取引の後続取引によって利益を得る方法。

このように、執行された取引の検証順序を変更することで、利益を得ることが MEV の抽出の仕組みである。（ESMA-EBA レポート 29 頁 109.）

(3) MEV の抽出の弊害

ESMA-EBA は、利用されたブロックに関して権利を有する者から MEV の抽出者に富が移転することを MEV の抽出の負の外部性と指摘している（ESMA-EBA レポート 32 頁 119.）。また、検証を実施するマイナーやバリデーターに分散型台帳の管理が集中することで、外部からのサイバー攻撃に対して脆弱となるリスクについても言及している（ESMA-EBA レポート 33 頁 123.）。

なお、MEV の抽出は事実上あらゆる分散型ブロックチェーンにおいて発生する可能性があるものの、複雑な取引の場合に特に収益性が高いため、DeFi サービスを提供するプロトコルが MEV の抽出の標的とされやすい（ESMA-EBA レポート 28 頁 102.）。

3. DeFi に対する新たな規制について

ESMA-EBA 及び EC においては、上記第 2.VI.2.において記載したような DeFi サービスに関するリスクを認識しているものの、DeFi サービスについて新たな規制を設けることは現時点では検討していない様子である。ESMA-EBA レポートにおいても新たな規制措置については言及されておらず、EC に対するヒアリングにおいても、現時点では DeFi に対する立法措置は検討していないことが確認された。

VII. MiCA における暗号資産サービス業

1. 総説

(1) 暗号資産サービス業

CASP について、「職業又は事業として顧客に対し専門的基盤において一つ以上の暗号資産サービスを提供し、かつ第 59 条に従って暗号資産サービスの提供が認められている法人その他の事業体（a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services in accordance with Article 59）」と規定している（MiCA 第 3 条第 1 項(15)）。

暗号資産サービス業は、MiCA 第 3 条第 1 項(16)において次のとおり定義されている。なお、fully decentralized との関係に関しては、分散型台帳を利用したサービスが、fully decentralized に該当せず、MiCA 第 3 条第 1 項(16)のサービスのいずれかの提供を業として行う場合には、MiCA 第 59 条に基づき加盟国の規制当局から認可を受けなければならない²⁶。

- 顧客の代理での暗号資産の保管及び管理（providing custody and administration of crypto-assets on behalf of clients。いわゆる、カストディサービス²⁷）
- 暗号資産取引プラットフォームの運営（operation of a trading platform for crypto-assets）
- 法定通貨との暗号資産の交換（exchange of crypto-assets for funds）
- 他の暗号資産との暗号資産の交換（exchange of crypto-assets for other crypto-assets）
- 顧客の代理での暗号資産取引注文の執行（execution of orders for crypto-assets on behalf of clients）
- 暗号資産の取扱い（placing of crypto-assets）
- 顧客の代理での暗号資産取引注文の受信及び送信（reception and transmission of orders for crypto-assets on behalf of clients）
- 暗号資産に関する助言の提供（providing advice on crypto-assets）
- 暗号資産に関するポートフォリオ管理（providing portfolio management on crypto-assets）
- 顧客の代理での暗号資産の移転（providing transfer services for crypto-assets on behalf of clients）

(2) CASP に共通して課される義務

MiCA Title V には、顧客保護の観点から CASP が共通して遵守すべき義務が次のとおり定められている。

²⁶ EC へのヒアリングによれば、約 60 の CASP が加盟国により認可されており、ドイツとオランダが最も多くのライセンスを発行しているとのことである。

²⁷ EC へのヒアリングによれば、アンホステッドウォレットはハードウェア又はソフトウェアの製品であるためそれを販売すること自体は、「顧客の代理での暗号資産の保管及び管理」に該当するわけではないとのことである。

① 健全性要件（MiCA 第 67 条）

提供する暗号資産サービスの種類に応じた最低要件の額又は前年度の固定間接費の 4 分の 1 の額の資産を確保するための措置を講じなければならない。

② ガバナンス体制（MiCA 第 68 条）

CASP の経営機関の構成員は、十分に良好な信用を有し、個人としても集団としても、その職務を遂行するために適切な知識、技能及び経験を備えていなければならない。特に、当該構成員は、マネー・ローンダリング又はテロ資金供与に関連する犯罪、又はその信用に影響を及ぼすその他の犯罪により有罪判決を受けた者であってはならない。

③ 主管当局への報告義務（MiCA 第 69 条）

CASP は、新規に EU 加盟国での活動を行う前に管轄当局に報告しなければならない。当該報告においては、MiCA 第 68 条で定められたガバナンス体制を遵守していることが評価可能な情報も提供しなければならない。

④ 顧客の暗号資産及び資金の保管（MiCA 第 70 条）

CASP は自らが破綻した際には顧客から預託を受けた暗号資産を返還するための適切な措置を設けなければならない。具体的には、CASP は、顧客資金を受領した日の翌日の営業日終了時点までに当該資金を信用機関(credit institution)²⁸又は中央銀行に預託しなければならない。CASP の資産と明確に区別可能な口座に保管しなければならない（MiCA 第 70 条第 2 項及び第 3 項）。

⑤ 苦情処理手続（MiCA 第 71 条）

CASP は、顧客から受けた苦情を迅速に処理するための手続を定めた上で公開しなければならない。

⑥ 利益相反防止義務（MiCA 第 72 条）

CASP は、CASP 自身と以下の者の間で生じる利益相反への対応方針を定めた上でその内容を公表しなければならない。

- 株主又は組合員
- 直接的又は間接的に CASP、株主又は組合員に関連する者
- 経営陣の構成員
- 従業員
- 顧客

また、CASP の二人以上の顧客において生じた利益相反に対応するための措置も公表しなければならない。

²⁸ MiCA における信用機関 (credit institution) は、下記のとおり、Capital Requirements Regulation (CRR) 第 4 条第 1 項第 1 号に定義が規定されており、銀行を含む預金取扱機関を指す。“credit institution” means an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account

⑦ 外部委託に関する義務（MiCA 第 73 条）

CASP が第三者に業務を委託する場合には、暗号資産サービスの提供に支障が生じないような合理的措置を講じなければならない。

2. カストディアルウォレットに関する規制

顧客から秘密鍵の預託を受け暗号資産を管理する行為（カストディ）は、暗号資産サービスである「顧客の代理での暗号資産の保管及び管理」に該当する。カストディアルウォレットを提供する者は、CASP の上記第 2.VII.1.の義務に加え、次のとおり、MiCA 第 75 条に基づく以下の義務についても履行しなければならない。

① 契約内容の指定（同条第 1 項）

カストディ契約を締結する際には、セキュリティシステムや保管方針を明示しなければならない。

② 暗号資産の分別管理（同条第 2 項）及び明細の提供（同条第 5 項）

顧客のポジションを自己の保有分と分別管理の上、各顧客の残高を記録し、保管しなければならない。当該記録においては、顧客からの指示に基づく暗号資産の残高の変動が記録されなければならない。また、少なくとも 3 か月に一回は、暗号資産の残高の明細書を各顧客に提示しなければならない。当該明細書には、暗号資産の残高、価値、期中に実施された暗号資産の移転を明示しなければならない。

③ 暗号資産の権利の発生に伴う残高の変更（同条第 4 項）

顧客のために保管及び管理を行う暗号資産に付随する権利の行使を円滑に実施しなければならない。また、顧客の権利を創設又は変更する可能性のある事象が発生した場合には、直ちに顧客のポジション台帳に記録しなければならない。

④ 顧客財産との間の分別管理（同条第 7 項）

CASP 自身が保有する暗号資産と、顧客から預託を受けた暗号資産に関しては、分散型台帳においても分別されて保管されなければならない、CASP の債権者が顧客の暗号資産に対して強制執行できないようにしなければならない。

3. CASP に関するエンフォースメント

マルタ当局へのヒアリングによれば、CASP に対する監督の実行性を確保するための措置は以下の通り。

- 監督の実行性を確保するために、欧州各国の規制当局においては、MOU（Memorandum of Understanding）の締結により、監督の実行性確保が図られている。

- 具体的には、CASP を所管する部署が、国内の警察との間で MOU を締結している。EU 各加盟国の警察当局間では既に MOU が締結されているため、EU 各加盟国の警察当局を通じて、EU 各加盟国の CASP を所管する部署が CASP に対する監督の連携を行うことが可能となる。
- マルタ当局においては、英国やアメリカの司法省といった EU 域外の当局との間でデータ共有を行うためのタスクフォースが設立されている。
- CASP に関するエンフォースメントとして、マルタ当局は、OKCoin Europe Limited に罰金を科したとのことである。OKCoin Europe Limited は、顧客データの分析の不実施や、疑わしい取引の報告に対する十分な調査の懈怠といった AML に関する義務違反により 120 万ユーロの罰金が科された。

4. CASP によるサイバーセキュリティ対策

CASP にも DORA²⁹ (Digital Operational Resilience Act) が適用される。DORA 第 2 条 1 項において、CASP も DORA の適用対象である旨が明示されている (DORA 第 2 条第 1 項(f))。DORA においては次の事項が定められており、CASP も DORA の枠組みに従ったサイバーセキュリティ対策を講じることが求められる。

- ICT リスクマネジメント
 - ICT リスク管理の原則と要求事項を定めた枠組みの設定
- ICT 第三者リスク管理
 - ICT の第三者リスクの軽減措置の実施
- デジタル運用レジリエンステスト
 - 高度なテストなどさまざまなテストを含む運用レジリエンステストプログラムの策定
- ICT 関連インシデント
 - ICT 関連インシデントの管理、重大なインシデント及び重大なサイバー脅威の主管当局への通知
- 情報共有
 - サイバー脅威に関する情報と知識の交換
- 重要なサードパーティプロバイダーの監視
 - サイバー脅威に関する情報とインテリジェンスの交換

5. 無許可の CASP の検知について

マルタ当局へのヒアリングによれば、無許可の CASP を発見する方法について確認したところ、以下の回答が得られた。

- ウェブ検索を含むインターネット情報のスクリーニング
- 投資者からの通報
- 各国の主管当局間の情報共有

²⁹ Digital Operational Resilience Act
<https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>

VIII. 暗号資産の貸付、借入、ステーキングについて

1. 総説

暗号資産の貸付、借入、ステーキング行為について、それ自体は暗号資産サービス業の類型に定められておらず、MiCAによる直接の規制は定められていない。もっとも、ESMA-EBA レポートにおいては、暗号資産の貸付、借入及びステーキングに関するリスクについて、以下のような言及がみられる。

2. 暗号資産貸付及び借入について

(1) 暗号資産貸付

ESMA-EBA レポートにおいて、暗号資産貸付とは、「提供者（貸し手）は、顧客（借り手）が一定価値の暗号資産又は資金を担保として差し入れることと引き換えに、一定価値の暗号資産又は資金を顧客に譲渡する。借り手は、将来の期日に、譲渡された暗号資産又は資金の価値に相当する金額と、潜在的な追加利息を貸し手に返還することを約束する (Crypto-asset lending refers to the activity consisting of a provider transferring a certain value of crypto-assets or funds to a user in exchange for the user placing a certain value of crypto-assets or funds as collateral and a commitment that the borrower will return to the lender a value equivalent to the transferred value of crypto-assets or funds and potential additional interests on a future date to the lender.) 」こととされている (ESMA-EBA レポート 37 頁 142.)。

(2) 暗号資産貸付に関するサービスの提供方法

以下のように、暗号資産貸付は、中央集権型の暗号資産貸付サービスか DeFi による暗号資産貸付サービスにより実施される。

① 中央集権型の暗号資産貸付サービス (ESMA-EBA レポート 37 頁 143. 38 頁 145.149.)

中央集権型の暗号資産貸付サービスは、暗号資産サービス業の認可を得た者が提供するサービスである。顧客が CASP に預託している資金や暗号資産を担保として、暗号資産貸付が実施される。一般には、CASP は受け入れている担保の価格の 20%~80%の範囲で貸付を実施している。暗号資産の貸し手は、金利や手数料から収益を得る一方で、貸付対象の暗号資産や担保としている暗号資産に関する価格変動リスクを負うこととなる。

② DeFi の暗号資産貸付サービス (ESMA-EBA レポート 39 頁 154.155.)

DeFi による暗号資産貸付サービスは、暗号資産の借入者が、当該 DeFi のスマートコントラクトに担保となる暗号資産を差し入れることで、DeFi プロトコル自身又は他の顧客から暗号資産の貸付を受けるサービスである。他の顧客から暗号資産の貸付を受ける場合には、貸付者と借入者を相対で取引させる方法と、あらかじめプールされた暗号資産から貸付を実施する方法が存在する。

(3) 暗号資産借入

ESMA-EBA レポートにおいて、暗号資産借入とは、「顧客（貸し手）は、一定価値の暗号資産又は資金を別の顧客（借り手）に譲渡する。その見返りとして、借り手は将来の期日（又はその他のトリガー事象発生時）に、貸し手に対して同等の価値の暗号資産又は資金と、潜在的な追加利息を返還することを約束する（Crypto-asset borrowing refers to the activity consisting of a user transferring a certain value of crypto-assets or funds to a another user or the provider in exchange for a commitment that the borrower will return to the lender a value equivalent to the transferred crypto-assets or funds and potential additional interests on a future date.）」こととされている（ESMA-EBA レポート 40 頁 157.）。

(4) 暗号資産借入に関するサービスの提供方法

以下のように、暗号資産借入は、中央集権型の暗号資産貸付サービスか DeFi による暗号資産貸付サービスにより実施される。

① 中央集権型の暗号資産借入サービス（ESMA-EBA レポート 41 頁 158.160.）

中央集権型の暗号資産借入サービスは、暗号資産サービス業の認可を得た者が提供するサービスである。CASP 自身が顧客から暗号資産を借り入れる方法と、CASP が暗号資産の最終的な借入者とマッチさせる方法が存在する。CASP は概ね借入暗号資産の 30%以内の手数料を設定している。

② DeFi の暗号資産借入サービス（ESMA-EBA レポート 42 頁 161.~163.）

DeFi による暗号資産借入サービスに関しては、当該 DeFi サービスのスマートコントラクト機能によって、貸付者から受け入れた暗号資産をあらかじめプールして最終的な借入者に貸し付けるサービスが存在する。

(5) 暗号資産貸付及び借入に関するリスク

暗号資産貸付・借入に関するリスクについて、ESMA-EBA レポートにおいて下記のとおり言及されている。

① レバレッジに関するリスク（ESMA-EBA レポート 50 頁 196.~200.）

暗号資産貸付が繰り返される（特定の顧客が暗号資産を借入、それを貸し出し、その貸付でさらに借入を試みる。）ことで、最初に保有していた暗号資産に対する暗号資産の借入額の比率が大きくなり市場が脆弱となるリスクが生じる。

② 預託した担保に関するプロシクリシティに関するリスク（ESMA-EBA レポート 51 頁 202.）

貸し手は貸付不履行の影響を補うために担保資産を清算することができるため、信用リスクは通常、担保要件によって軽減され、過剰担保要件がある場合、

担保資産の清算によって貸し手が損失を被らない可能性もある。一方で、スマートコントラクトによる担保資産の清算は、借り手に対する救済手段が欠如した状態で、あらかじめ決められたルールに従い自動的に実行されるため、ストレス環境下ではプロシクリカル性（景気循環に順応する性質）が強まり、借り手の信用状況をさらに悪化させるリスクが存在する。

③ 流動性リスク（ESMA-EBA レポート 51 頁 203.）

貸し手及び借り手は、流動性リスクにも直面し得る。例えば、ある者が暗号資産を長期で貸し出し、短期で借り入れている場合、市場状況によっては短期債務の返済が困難となる可能性がある。

3. ステーキング

(1) ステーキング

ESMA-EBA レポートにおいては、ステーキングを、「PoW 及び PoS 類似のブロックチェーン合意形成メカニズムの運用を支援するため、暗号資産を固定化するプロセス」としている（ESMA-EBA レポート 42 頁 165.）。ステーキングとは、保有している暗号資産をブロックチェーン上に預け入れることで、取引やブロックの正当性を検証・承認し、そのブロックチェーンの安定稼働に貢献し、その対価として暗号資産等を獲得する仕組みを指す。

(2) ステーキングのためのサービス

ESMA-EBA レポートにおいては、ステーキングを提供するためのサービスとして、以下の 3 つのサービスを挙げている。

① バリデーター・アズ・ア・サービス（ESMA-EBA レポート 42 頁 168.）

独自にバリデーターとなる資本を有するが、ステーキングを実施するための技術的な手段を持たない個人に対し、ステーキングへのアクセスを容易にするためのサービスを提供する事業体を指す。具体的な事例を挙げると、イーサリアムに関しては、32ETH を保有する顧客は、バリデーター・アズ・ア・サービスに当該暗号資産を預託するのみでステーキングを実施することが可能となる。

② プール型ステーキング（ESMA-EBA レポート 42 頁 169.）

複数の顧客が自己の保有する暗号資産を持ち寄ってステーキングを実施するためのサービスを指す。

③ 中央集権型ステーキング（ESMA-EBA レポート 42 頁 169.）

CASP が提供するステーキングサービスであり、顧客が秘密鍵を CASP に預託せずともステーキングを実施することが可能なサービスが開発されている。

(3) ステーキングサービスの「顧客の代理での暗号資産の保管及び管理」への該当性

ステーキングサービスの提供が、MiCA 第 3 条 1 項(15)の「顧客の代理での暗号資産の保管及び管理」に該当するか否かは、秘密鍵をサービス提供者に対して預託するかどうかによって判断される（ESMA-EBA レポート 43 頁 170.）。

(4) ステーキングに関するリスク

ESMA-EBA レポートにおいては、ステーキングに関するリスクとして次のリスクを挙げている。

① 暗号資産の価格のボラティリティに関するリスク（ESMA-EBA レポート 53 頁 212.）

ステーキングでは、場合によっては、数十日にわたって暗号資産をブロックチェーンに預託することもあるため、当該預託期間中に暗号資産の価格が変動することでステーキングを実施した者が損害を被る可能性がある。

② バリデーターへのペナルティに関するリスク（ESMA-EBA レポート 53 頁 214.）

バリデーターが不正行為によるペナルティによりブロックチェーンに預託された暗号資産が没収されるリスクも存在する。特に、暗号資産の預託を受けてステーキングを実施しているバリデーターの暗号資産がペナルティにより没収された際、暗号資産の預託をした者とバリデーターの間でペナルティに関するリスクの分担が定められていない場合、特にこのリスクが顕著となる。なお、このリスクに関しては EC へのヒアリングにおいても言及がなされた。

③ カストディリスク（ESMA-EBA レポート 53 頁 216.）

ステーキングの実施のために暗号資産の預託を受ける者が破綻した場合に、資産の混同、記録管理の不備等によって、預託した暗号資産の返還を受けられないリスクが存在する。

IX. MiCA における暗号資産の発行・公衆への提供・上場に関する規制

1. 総説

MiCA においては暗号資産を以下の 3 種に分類した上で、公衆への提供、上場に関する規制を敷いている。公衆への提供、上場に関する規制は基本的に、欧州目論見書規制（Prospectus Regulation³⁰）に倣い規定されている。

電子マネートークン（electronic money token）	単一の法定通貨の価値を参照することで価値の安定化を図る暗号資産（a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency）
-----------------------------------	--

³⁰ Prospectus Regulation
<https://eur-lex.europa.eu/eli/reg/2017/1129/oj/eng>

	具体的な銘柄としては、EURC、EURO 等を指す ³¹ 。
資産参照型トークン(asset-referenced token)	一つ又は複数の法定通貨を含む、他の価値や権利、又はそれらの組み合わせを参照することで価値の安定化を図る暗号資産 (a type of crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies) 2025 年 10 月時点で資産参照型トークンとして承認された銘柄は存在しない。
その他暗号資産	電子マネートークン、資産参照型トークン以外の暗号資産 (a crypto-asset other than an asset-referenced token or e-money token) 具体的な銘柄としては、ビットコインやイーサリアム等を指す。

2. 公衆への提供・上場について

(1) MiCA における暗号資産の発行に関する規定について

MiCA において、公衆への提供、上場のみが暗号資産のプライマリー取引として規制されており（MiCA 第 4 条、第 5 条、第 16 条、第 48 条）、暗号資産の発行については規制されていない。電子マネートークン、資産参照型トークン、その他の暗号資産について発行が規制されていない理由は以下のとおりである。

① 電子マネートークン、資産参照型トークン

電子マネートークン、資産参照型トークンに関しては、発行者となり得る者が法定されている（電子マネートークンに関しては銀行等の信用機関、電子マネー事業者。資産参照型トークンに関しては、銀行等の信用機関、加盟国当局から認可を受けた法人。）。また、発行者及び発行者から承諾を得た者のみ「公衆への提供」や「上場」を行うことが可能であると定められている（MiCA 第 16 条、第 48 条）。このように、発行者の資格要件及び「公衆への提供」や「上場」のための手続により利用者保護が図られているため、利用者保護との関係で発行行為そのものを直接規制する必要はない。

② その他の暗号資産

その他の暗号資産は発行者が存在しない場合もあるため（MiCA 前文(22)）発行行為そのものを直接規制することは困難であり、その他の暗号資産の発行については、特段の規制は定められていない。利用者保護との関係では、暗号資産の「公衆への提供」や「上場」に先立ち、一定の例外的な場合を除き、ホワイトペーパーを公表するための手続を定めることで、利用者に対する情報提供を担保している。

³¹ <https://www.stablecoininsider.com/mica/>

(2) 「公衆への提供」について

「公衆への提供」には、欧州目論見書規制第 2 条(d)に倣って以下のような定義が置かれている。

- あらゆる形式及び手段により人に対して行われるコミュニケーションであって、提供の条件及び提供される暗号資産に関する十分な情報を提示することにより、潜在的保有者が当該暗号資産を購入するか否かを判断することを可能にするもの(a communication to persons in any form, and by any means, presenting sufficient information on the terms of the offer and the crypto-assets to be offered so as to enable prospective holders to decide whether to purchase those crypto-assets、MiCA 第 3 条第 1 項(12))

(3) 「上場」について

上場に関しては、「暗号資産取引プラットフォーム取引における上場 (admission of crypto-assets to trading on a trading platform for crypto-assets)」とのみ定義されており (MiCA 第 2 条)、暗号資産取引プラットフォーム (a trading platform for crypto-assets) の範囲は特段定義されていない。

(4) その他の暗号資産の「公衆への提供」におけるホワイトペーパーの作成が免除される場合

暗号資産について公衆への提供を行う場合には基本的にはホワイトペーパーの作成が必要である。もっとも、その他の暗号資産に関しては、欧州目論見書規制に倣い一定の場合 (提供の相手が適格機関投資者に限定される場合や少人数の場合など) にはホワイトペーパーの作成義務が免除されている。目論見書規制と MiCA の規定の対比は次のとおりである。

	目論見書規制 (第 1 条第 3 項及び第 4 項)	MiCA (第 4 条第 2 項)
適格機関投資者のみが相手の場合	免除	免除
加盟国毎に 150 人未満を相手とする場合	免除	免除
総額	12 か月の期間において 100 万ユーロ相当未満の場合免除	12 か月の期間において EU 域内での募集総額が 100 万ユーロ相当以下の場合免除
最低額面	10 万ユーロ以上の場合免除	規定無し

以上の免除規定のほか、その他の暗号資産に特有の、ホワイトペーパー発行の免除規定が次のとおり規定されている (MiCA 第 4 条第 3 項)。

- 暗号資産が無償で提供される場合
- 分散型台帳の維持又は取引の検証に対する報酬として生成される場合
- 既存の製品・サービスや稼働中の商品・サービスへのアクセス権として付与される場合
- 限定されたネットワークにおいてのみ、商品・サービスの対価として使用可能な場合

(5) ホワイトペーパーの記載事項

暗号資産発行の際にホワイトペーパーに記載が義務付けられている事項（主要なもの）は次のとおりとされている。

	その他の暗号資産 (MiCA 第 6 条)	資産参照型トークン (MiCA 第 19 条)	電子マネートークン (MiCA 第 51 条)
共通して 記載が必要 な事項	● 発行者に関する情報³² ● 公衆への提供又は取引所への上場に関する情報 ● 対象となる暗号資産の特徴 ● 基盤技術に関する情報 ● リスクに関する情報 ● 当該暗号資産の発行に使用されるコンセンサスメカニズムが気候に及ぼす主な悪影響及びその他の環境関連の悪影響に関する情報		
権利に関 する事項	暗号資産プロジェクトに関する情報	準備資産 (MiCA 第 19 条第 1 項(d)) や償還請求権 (MiCA 第 19 条第 6 項) に関する情報	額面価格でいつでも償還を受けることが可能である旨 (MiCA 第 49 条第 5 項)
その他	発行者以外の者による公衆への提供や上場承認申請が行われる場合には、その者に関する情報		

(6) 承認・届出・公表

目論見書規制においては、基本的に当局に目論見書を提出し公表前に承認を得なければ、公衆への提供や上場は認められない。一方、暗号資産に関しては、資産参照型トークンのみ、公衆への提供や上場の前にホワイトペーパーについて当局からの承認が必要である。その他の暗号資産及び電子マネートークンに関して

³² その他の暗号資産に関しては、公衆への提供をする者又は取引所上場申請者を記載し (information about the offeror or the person seeking admission to trading) (MiCA 第 6 条第 1 項(a))、公衆への提供をする者又は取引所上場申請者が発行者と異なる場合には、発行者に関する情報を記載しなければならない (information about the issuer, if different from the offeror or person seeking admission to trading) (MiCA 第 6 条第 1 項(b))。

は当局からの承認は不要で、加盟国における規制当局に対する事前通知を行うことで足りるとされている。

① その他の暗号資産に関する手続き

ホワイトペーパーの作成、規制当局への提出、公表等を行う必要があり、公表の 20 営業日前に、規制当局に対する通知が必要とされる（MiCA 第 8 条第 1 項及び第 5 項）（なお、規制当局は、当該ホワイトペーパーの公表前に事前承認を求めてはならないとされている（MiCA 第 8 条第 3 項））。また、公衆への提供又は上場を求める者は、ホワイトペーパー及び該当する場合にはマーケティングコミュニケーションを、自己のウェブサイト上に公表しなければならない。当該ウェブサイトは一般にアクセス可能であることとし、暗号資産の取引上場開始日の相当の期間前に、かついかなる場合も開始日前までに公表されなければならない（MiCA 第 9 条第 1 項）。

② 電子マネートークンに関する手続

ホワイトペーパーの公表の 20 営業日前には規制当局に提出が必要とされる（なお、規制当局は、当該ホワイトペーパーの公表前に事前承認を求めてはならないとされている。）（MiCA 第 51 条第 11 項）。上場申請や公衆への提供前の段階においては、発行者のウェブサイトにおいて暗号資産のホワイトペーパーを公表することが必要である（MiCA 第 51 条第 13 項）。

③ 資産参照型トークンに関する手続（信用機関が資産参照型トークンを発行する場合）

信用機関が発行する資産参照型トークンに関しては、暗号資産を発行する 90 営業日前までに規制当局に対して暗号資産の発行を通知し（MiCA 第 17 条第 1 項(b)）、ホワイトペーパーに関して公表前に当局からの承認を取得する必要がある（MiCA 第 17 条第 1 項(a)）。

④ 資産参照型トークンに関する手続（信用機関以外が資産参照型トークンを発行する場合）

信用機関以外の者が資産参照型トークンを発行しようとする場合、ホワイトペーパーを提出した上で MiCA 第 18 条に基づく認可申請を行い、MiCA 第 21 条に基づく認可を得なければならない。当該申請においては、経営陣による業務継続の可能性やマネロンリスク、テロ資金供与のリスクを評価した上で認可の可否が判断されることになる（MiCA 第 21 条第 2 項）。

(7) 資産参照型トークンの発行事例がない背景

資産参照型トークンに関しては、発行事例が確認できていない³³。これは、MiCA 第 18 条第 6 項に基づく「資産参照型トークンのホワイトペーパーに記載するべき

³³ 電子マネートークンに関しては、EURC や EURO、その他の暗号資産に関してはビットコインやイーサリアムといった発行事例が存在する。

事項の詳細を定めた技術的基準」、MiCA 第 36 条第 4 項に基づく「流動性要件の詳細」、MiCA 第 38 条第 5 項に基づく「準備資産の投資対象となる高流動性金融商品」については最終報告書公表済みであるものの、EC による採択及び欧州議会・理事会の審議待ちで未発効であることが原因の一つであると考えられる³⁴。

3. 発行・公衆への提供・上場に関する規制に関する罰則

EU加盟国においては、以下の基準を各加盟国国内法で定めるべき罰金の上限額の下限とし、発行・公衆への提供・上場に関する規制に違反した場合の罰則を加盟国内において規定しなければならない。

① その他の暗号資産 (MiCA 第 111 条第 1 項(a)、MiCA 第 111 条第 3 項(a)、(b))

最低額が、500 万ユーロ又は主管当局により承認された最新の財務諸表に基づく法人の年間総売上高の 3%

② 電子マネートークン (MiCA 第 111 条第 1 項(b)、MiCA 第 111 条第 3 項(a)、(d))

最低額が、500 万ユーロ又は主管当局により承認された最新の財務諸表に基づく法人の年間総売上高の 12.5%

③ 資産参照型トークン (MiCA 第 111 条第 1 項(c)、MiCA 第 111 条第 3 項(a)、(d))

最低額が、500 万ユーロ又は主管当局により承認された最新の財務諸表に基づく法人の年間総売上高の 12.5%

X. MiCA における発行者の義務

1. 総説

電子マネートークン及び資産参照型トークンについては、参照している通貨や資産の価値に応じた償還義務が定められている（電子マネートークンに関しては MiCA 第 49 条第 2 項、資産参照型トークンに関しては MiCA 第 39 条第 1 項）ため、MiCA において資産保全義務が課されている³⁵。また、その他の暗号資産については、電子マネートークン及び資産参照型トークンのような償還要件や準備資産に関する要件は適用されないものの、申込み期間中に調達した資金又は暗号資産を監視及び保全するための有効な体制を整備しなければならないとされ（MiCA 第 10 条第 3 項）、具体的には、資金が調達された場合には信用機関により保管し（同項(a)）、暗号資産が調達された場合には、顧客のために暗号資産のカストディ及び管理を提供する CASP により保管する必要がある（同項(b)）。

³⁴ ESMA Overview of Level 2 and Level 3 measures related to Regulation (EU) 2023/1114 Markets in Crypto-Assets (MiCA)
Last update: 16/07/2025

https://www.esma.europa.eu/sites/default/files/2025-07/ESMA75-113276571-1510_MiCA_Level_2_and_3_table.pdf

³⁵ 信用機関に関しては、バーゼルIIIに基づく自己資本維持義務や資産保全義務が資本要件指令（Capital Requirement Directive）により定められているため、MiCA における自己資本維持義務と資産保全義務が適用除外されている（EU 決済サービス指令等の概要
https://www.fsa.go.jp/singi/singi_kinyu/kessai_wg/siryou/20150915/02.pdf）。

2. 償還義務・準備資産に関する要件・自己資本要件・資産保全義務・流動性保持義務について

(1) 電子マネートークン及び資産参照型トークンの償還義務・準備資産に関する要件・自己資本要件・資産保全義務・流動性保持義務

電子マネートークン及び資産参照型トークンに関しては償還義務・準備資産に関する要件・自己資本要件・資産保全義務・流動性保持義務が定められている。重要な電子マネートークン及び資産参照型トークンに該当する場合には、追加的な義務が課される。

	電子マネートークン	資産参照型トークン
重要なものとして分類される指標	資産参照型トークンが重要とみなされる右記の基準について少なくとも3つの要件を満たすこと（MiCA 第56条）	以下の要件うち3以上の要件を満たす場合（MiCA 第43条） ・資産参照型トークンの保有者数が1000万人を超えること ・発行された資産参照型トークンの価値、その時価総額、又は当該トークン発行者の資産準備高のいずれかが50億ユーロを超えること ・当該関連期間における当該資産参照トークンの1日あたりの平均取引件数及び平均総取引額が、それぞれ250万件及び5億ユーロを超えること ・当該資産参照型トークンの発行者が、欧州議会及び理事会規則（EU）2022/1925(17)³⁶に基づきゲートキーパーとして指定された中核的プラットフォームサービス提供者であること ・資産参照型トークン発行者の活動が国際的に重要な規模であること（資産参照トークンの決済・送金利用を含む。）

³⁶ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)
<https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng>

	電子マネートークン	資産参照型トークン
		・資産参照型トークン又はその発行者が金融システムと相互に結びついていること ・同一発行者が少なくとも1つのほかの資産参照型トークン又は電子マネートークンを発行し、かつ少なくとも1つの暗号資産サービスを提供していること
準備資産	資産のうち、30%は信用機関において預金する必要がある（MiCA 第 54 条(a)）。残りの資産に関しては、安全・低リスクで、流動性が極めて高く、市場リスク・信用リスク・集中リスクが最小限である金融商品に投資され、かつその通貨（法定通貨）で表示されるものでなければならない（MiCA 第 54 条(b)）。具体的には、残りの資産については、即時の換金が可能な流動性の高い資産（EC 委任規則 2015/61³⁷で定めるレベル 1 資産）への投資による運用が認められている（MiCA	資産のうち、30%は資産参照型トークンが参照する法定通貨と同一の通貨建て信用機関において預金する必要がある（MiCA 第 36 条第 4 項(d)）。また、準備資産の一部を運用する場合、当該資産は、市場リスク・信用リスク・集中リスクが最小限であり、かつ高い流動性を有する金融商品にのみ投資されなければならない（MiCA 第 38 条第 1 項）。具体的には、残りの資産については、即時の換金が可能な流動性の高い資産（EC 委任規則 2015/61 で定めるレベル 1 資産³⁸）への投資による運用が認められている（MiCA 第 38 条第 1 項³⁹）。

³⁷ Commission Delegated Regulation (EU) 2015/61 of 10 October 2014 to supplement Regulation (EU) No 575/2013 of the European Parliament and the Council with regard to liquidity coverage requirement for Credit Institutions Text with EEA relevance

https://eur-lex.europa.eu/eli/reg_del/2015/61/oj/eng

³⁸ EC 委任規則 2015/61 で定めるレベル 1 資産の詳細は Delegated Regulation (EU) 2015/61 の第 10 条に定められている。具体的には、①硬貨および紙幣、②欧州中央銀行（ECB）または加盟国中央銀行に対する、もしくはこれらにより保証された資産、ならびに一定の信用格付（信用品質ステップ 1 以上）を有する第三国中央銀行に対する資産および引出し可能な中央銀行準備預金、③加盟国または一定の信用格付を有する第三国の中央政府、ならびにこれらと同等に扱われる地方政府・公共部門機関に対する、または保証された資産、④信用品質ステップ 1 に満たない第三国の中央政府または中央銀行に対する資産（ただし同一通貨のストレス下純流出額の範囲内に限る）、⑤加盟国政府等により設立・実質的に保証された信用機関または政策金融機関が発行する資産、⑥一定の要件（高格付、十分な担保カバレッジ、発行規模、透明性等）を満たす極めて高品質なカバードボンド、⑦CRR 第 117 条および第 118 条に規定される多国間開発銀行および国際機関に対する、または保証された資産をいう。

³⁹ 第 38 条第 1 項に規定する、市場リスク、信用リスクおよび集中リスクが最小限であり、かつ高い流動性を有するとみなされる金融商品に特定する規制上の技術基準（RTS）第 1 条第 1 項に詳細が定められている。
<https://www.eba.europa.eu/sites/default/files/2024-06/d92b94f8-8260-43b6-abae->

	電子マネートークン	資産参照型トークン
	第 54 条(b)、MiCA 第 38 条第 1 項)。	【重要な資産参照型トークン】 60%を資産参照型トークンが参照する法定通貨と同一の通貨建てで預金することが求められる。(MiCA 第 45 条第 7 項(b))
自己資本維持義務 (信用機関は適用除外)	35 万ユーロ又は直近 6 か月のトークンの準備資産の平均額の 2%、又は前年の固定間接費の 25%のいずれか高い額の自己資本の確保が必要 ⁴⁰ (MiCA 第 48 条第 3 項) 【重要な電子マネートークン】 重要な電子マネートークンに関しては上記基準のうち、直近 6 か月のトークンの準備資産の平均額については、3%と設定される (MiCA 第 58 条第 1 項(b))	35 万ユーロ (MiCA 第 35 条第 1 項(a)) 又は直近 6 か月のトークンの準備資産の平均額の 2% (同項(b))、又は前年の固定間接費の 25% (同項(c)) のいずれか高い額の自己資本の確保が必要 【重要な資産参照型トークン】 重要な資産参照型トークンに関しては上記基準のうち、直近 6 か月のトークンの準備資産の平均額については、3%と設定される (MiCA 第 45 条第 5 項)
資産保全義務 (信用機関は適用除外)	分別管理又は保険契約 ⁴¹ (重要な電子マネートークンのみ 6 か月毎の独立監査) (MiCA 第 58 条第 1 項(a))	分別管理 (MiCA 第 36 条第 2 項)、6 か月毎の独立監査 (MiCA 第 36 条第 9 項)
流動性維持義務	準備資産のうち少なくとも 20%を 1 営業日以内に、又は、少なくとも 30%を 5 営業日以内に売却可能な資産又は引き出し可能な金銭として保有する必要 (MiCA 第 58 条第 1 項(a))	準備資産のうち少なくとも 20%を 1 営業日以内に、又は、少なくとも 30%を 5 営業日以内に売却可能な資産又は引き出し可能な金銭として保有する必要 (MiCA 第 36 条第 4 項)

d21e022414ed/Final%20report_draft%20RTS%20to%20specify%20the%20HLFI%20in%20the%20reserve%20of%20assets%20Article%2038%205.pdf

⁴⁰ 自己資本要件の「35 万ユーロまたは直近 6 か月のトークンの日次発行残高総額の平均額の 2%」は、第二次電子マネー指令 (Payment Money Institution Directive 2) において、電子マネー事業者課されている自己資本要件と同様の水準 (EU 決済サービス指令等の概要 脚注 35 参照)。

⁴¹ MiCA で認められる保険契約の要件は、①当初の契約期間が 1 年以上であること、②その解約の通知期間は少なくとも 90 日間であること、③EU 法又は国内法に基づき認可された保険事業者から契約されること、④第三者機関によって提供されるものであることである (MiCA 第 67 条第 5 項)。

	電子マネートークン	資産参照型トークン
	【重要な電子マネートークン】 ● 準備資産のうち少なくとも40%を1営業日以内に、又は、少なくとも60%を5営業日以内に売却可能な資産又は引き出し可能な金銭として保有する必要（資産準備金の流動性要件をさらに明確化するため第36条(4)に基づく規制技術案第1条⁴²、MiCA第58条第1項(a)） ● 流動性ストレステストの実施（MiCA第45条第4項、MiCA第58条第1項(a)）	【重要な資産参照型トークン】 ● 準備資産のうち少なくとも40%を1営業日以内に、又は、少なくとも60%を5営業日以内に売却可能な資産又は引き出し可能な金銭として保有する必要（資産準備金の流動性要件をさらに明確化するため第36条第4項に基づく規制技術案第1条） ● 流動性ストレステストの実施（MiCA第45条第4項）
報告義務	EU圏内の法定通貨建ではない電子マネートークンについてのみ資産参照型トークンと同様の報告義務（MiCA第58条第3項）	発行額が1億ユーロを超える資産参照型トークンについて、以下の情報を当局に報告（MiCA第22条） ● 保有者数（MiCA第22条第1項(a)） ● 発行された資産参照型トークンの価値および資産準備金の規模（MiCA第22条第1項(b)） ● 四半期における1日当たりの平均取引件数及び平均総取引額（MiCA第22条第1項(c)） ● 単一通貨圏内における交換手段としての利用に関連する、当該四半期における1日あたりの平均取引件数及び平均総取引額の推定値（MiCA第22条第1項(d)）

⁴² Draft Regulatory Technical Standards to further specify the liquidity requirements of the reserve of assets under Article 36(4) of Regulation (EU) 2023/1114
https://www.eba.europa.eu/sites/default/files/2024-06/580db2f3-8370-4927-baa3-0f995722b417/Final%20report_draft%20RTS%20further%20specifying%20the%20liquidity%20requirements%20Article%2036%204.pdf

	電子マネートークン	資産参照型トークン
発行制限	EU 圏内の法定通貨建ではない電子マネートークンについてのみ資産参照型トークンと同様の発行制限 (MiCA 第 58 条第 3 項)	単一通貨圏において交換手段として用いられる日次取引件数及び日次取引額の四半期平均が、それぞれ 100 万件以上かつ 2 億ユーロ以上になった場合には発行停止 (MiCA 第 23 条)

(2) 準備資産の運用対象として認められている（預金以外の）投資資産

MiCA 第 38 条第 1 項において、投資が認められる資産の内容としては、①市場リスク、②信用リスク、③集中リスクが最小限の流動性の高い金融商品にのみ投資しなければならないとした上で、これらの基準の詳細を MiCA 第 38 条第 5 項に基づき、「市場リスク、信用リスク及び集中リスクが最小限の流動性の高い金融商品进行特定するための規制技術案⁴³」に委任している。基本的に EC 委任規則 2015/61 の第 10 条で定めるレベル 1 資産が対象とされている。

(3) 追加的な報告義務

EBA の発行したガイドライン「発行者による Title IIIの遵守に関する主管当局の監督業務を支援するためのテンプレートに関するガイドライン、発行者に対する監督業務の遂行を支援するためのテンプレートに関するガイドライン、Title IVに基づく発行者の遵守状況に関する監督業務の実施を支援するためのテンプレートに関するガイドライン⁴⁴」においては、MiCA Title IIIの暗号資産の発行・公衆への提供・上場に関する義務の履行状況確認のため、EU 通貨建の電子マネートークンの発行者も報告義務の名宛人としている。なお、当該ガイドラインにおいては、カストディアルウォレット間の取引については報告義務を課しているものの、カストディアルウォレットとノンカストディアルウォレット間の取引については報告義務を課していない。

3. 償還義務・準備資産に関する要件・自己資本要件・資産保全義務・流動性保持義務に違反した場合の罰則

EU加盟国においては、以下の基準を各加盟国国内法で定めるべき罰金の上限額の下限とし、償還義務・準備資産に関する要件・自己資本要件・資産保全義務・流動性保持義務に違反した場合の罰則を加盟国内において規定しなければならない。

⁴³ Draft Regulatory Technical Standards to specify the highly liquid financial instruments with minimal market risk, credit risk and concentration risk under Article 38(5) of Regulation (EU) 2023/1114
https://www.eba.europa.eu/sites/default/files/2024-06/d92b94f8-8260-43b6-abae-d21e022414ed/Final%20report_draft%20RTS%20to%20specify%20the%20HLFI%20in%20the%20reserve%20of%20assets%20Article%2038%205.pdf

⁴⁴ Guidelines on templates to assist competent authorities in performing their supervisory duties regarding issuers' compliance under MiCAR | European Banking Authority
<https://www.eba.europa.eu/sites/default/files/2024-12/907cde4b-7d25-4f41-b1ef-bb0a469f00ac/Final%20report%20on%20Guidelines%20on%20reporting%20on%20ARTs%20and%20EMTs.pdf>

① その他の暗号資産

最低額が、500 万ユーロ又は主管当局により承認された最新の財務諸表に基づく法人の年間総売上高の 3% (MiCA 第 111 条第 1 項(a)、MiCA 第 111 条第 3 項(a)、(b))

② 電子マネートークン

最低額が、500 万ユーロ又は主管当局により承認された最新の財務諸表に基づく法人の年間総売上高の 12.5% (MiCA 第 111 条第 1 項(b)、MiCA 第 111 条第 3 項(a)、(d))

③ 資産参照型トークン

最低額が、500 万ユーロ又は主管当局により承認された最新の財務諸表に基づく法人の年間総売上高の 12.5% (MiCA 第 111 条第 1 項(c)、MiCA 第 111 条第 3 項(a)、(d))

XI. MiCA における暗号資産の不公正な取引に関する規制

1. 総説

(1) MAR⁴⁵ (市場濫用規制) の参照について

MiCA の不公正取引規制は、市場濫用規制 (Market Abuse Regulation、以下「MAR」という。) の規定を参照しているものの、MAR の一部の規定については MiCA に規定されていない。その理由は、MiCA の前文(95)において、「暗号資産の発行者及び CASP は中小企業である場合が多いため、MAR の規定を適用することは不均衡であること (as issuers of crypto-assets and crypto-asset service providers are very often SMEs, it would be disproportionate to apply all the provisions of)」としている。

(2) DeFi サービスにおける不公正取引規制の適用範囲について

まず、MiCA の不公正取引に関する規制は、MiCA 第 2 条第 1 項に規定される者に限定されず、何人に対しても適用される (MiCA 第 86 条第 1 項、第 89 条)。また、不公正取引規制の適用範囲について、MiCA の対象の取引所や暗号資産サービス業者による活動に限定されていない。そのため、MiCA の適用対象外とされている完全に分散化された方法で提供される暗号資産サービスにおいて実行された、上場された暗号資産に関する取引においても不公正取引規制が適用される可能性がある⁴⁶。

⁴⁵ Market Abuse Regulation
<https://eur-lex.europa.eu/eli/reg/2014/596/oj/eng>

⁴⁶ Crypto-Asset Market Abuse Under EU MiCA | European Journal of Risk Regulation | Cambridge Core (II. The scope of application of MiCA's Title VI, 1. DeFi not excluded)
<https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/cryptoasset-market-abuse-under-eu-mica/FDC11EC096728B9EF1097A5346F0EF27>

(3) 地域的適用範囲

MiCA に定められた不公正取引に関する規制は、EU 域内以外の第三国にも適用される（MiCA 第 86 条第 3 項）⁴⁷。

2. インサイダー取引規制

(1) インサイダー情報の定義

MiCA 第 87 条のインサイダー情報の定義は以下のとおりであり、この規定は（MAR 第 7 条第 1 項(a)⁴⁸、(b)⁴⁹）において規定されているインサイダー情報の定義がベースとされている。

- 公開されていない正確な性質を有する情報であって、直接又は間接に、一又は複数の発行者、公衆への提供者若しくは取引所への上場を申請している者、又は一若しくは複数の暗号資産に関連するものをいい、かつ、当該情報が公表された場合には、当該暗号資産又は関連する暗号資産の価格に重大な影響を及ぼすおそれがあるものをいう（information of a precise nature, which has not been made public, relating, directly or indirectly, to one or more issuers, offerors or persons seeking admission to trading, or to one or more crypto-assets, and which, if it were made public, would likely have a significant effect on the prices of those crypto-assets or on the price of a related crypto-asset）。
- 顧客に代わって暗号資産の注文の執行を委託された者については、インサイダー情報には、顧客から伝達された情報であって、当該顧客の未約定の暗号資産の注文に関するものを含むものとする。当該情報は、正確な性質を有し、一又は複数の暗号資産の発行者、公衆への提供者若しくは取引所への上場を申請している者、又は一若しくは複数の暗号資産に直接又は間接に関連するものであって、当該情報が公表された場合には、当該暗号資産又は関連する暗号資産の価格に重大な影響を及ぼす可能性が高いものをいう（for persons charged with the execution of orders for crypto-assets on behalf of clients, it also means information of a precise nature conveyed by a client and relating to the client's pending orders in crypto-assets, relating, directly or indirectly, to one or more issuers, offerors or persons seeking admission to trading or to one or more crypto-assets, and which, if it were made public,

⁴⁷ This Title shall apply to actions and omissions, in the Union and in third countries, concerning crypto-assets as referred to in paragraph 1.

⁴⁸ 公開されていない正確な性質を有する情報であって、直接又は間接に、一又は複数の発行者又は一若しくは複数の金融商品に関連するものをいい、かつ、当該情報が公表された場合には、当該金融商品又は関連するデリバティブ金融商品の価格に重要な影響を及ぼすおそれがあるものをいう（information of a precise nature, which has not been made public, relating, directly or indirectly, to one or more issuers or to one or more financial instruments, and which, if it were made public, would be likely to have a significant effect on the prices of those financial instruments or on the price of related derivative financial instruments）。

⁴⁹ 金融商品の注文の執行を委託された者については、インサイダー情報には、顧客から伝達された情報であって、当該顧客の未執行の金融商品の注文に関するものを含むものとする。当該情報は、正確な性質を有し、一又は複数の発行者又は金融商品に直接又は間接に関連するものであって、当該情報が公表された場合には、当該金融商品、関連する現物商品契約又は関連するデリバティブ金融商品の価格に重要な影響を及ぼすおそれがあるものをいう（for persons charged with the execution of orders concerning financial instruments, it also means information conveyed by a client and relating to the client's pending orders in financial instruments, which is of a precise nature, relating, directly or indirectly, to one or more issuers or to one or more financial instruments, and which, if it were made public, would be likely to have a significant effect on the prices of those financial instruments, the price of related spot commodity contracts, or on the price of related derivative financial instruments）。

would likely have a significant effect on the prices of those crypto-assets or on the price of a related crypto-asset.) 。

(2) インサイダー情報に関する禁止事項

MiCA 第 89 条のインサイダー情報に関する禁止事項に関しても MAR 第 8 条第 1 項⁵⁰及び第 2 項⁵¹の規定を参照して規定されている。

- 本規則の目的上、インサイダー取引は、ある者がインサイダー情報を保有し、当該情報に関連する暗号資産を、自己の計算又は第三者の計算において、直接又は間接に取得し、又は処分することにより、当該情報を利用する場合に生じたものとみなされる。また、当該者がインサイダー情報を保有するに至る前に発注された、当該情報に関連する暗号資産に関する注文について、その情報を利用して取消し又は修正を行うことも、インサイダー取引とみなされる。さらに、インサイダー情報の利用には、自己の計算又は第三者の計算により、注文又は入札の提出、修正又は撤回を行うことも含まれる (For the purposes of this Regulation, insider dealing shall be deemed to arise where a person possesses inside information and uses that information by acquiring or disposing of, for its own account or for the account of a third party, directly or indirectly, crypto-assets to which that information relates. The use of inside information by cancelling or amending an order concerning a crypto-asset to which the information relates where the order was placed before the person concerned possessed the inside information, shall also be considered to be insider dealing. The use of inside information shall also comprise submitting, modifying or withdrawing a bid by a person for its own account or for the account of a third party.) 。
- いかなる者も、自己の計算又は第三者の計算にかかわらず、直接又は間接に、暗号資産に関するインサイダー取引を行い、若しくはこれを行おうとはならず、又は当該暗号資産に関するインサイダー情報を利用して当該暗号資産を取得し、若しくは処分してはならない。また、いかなる者も、他の者に対しインサイダー取引を行うよう勧告し、又はインサイダー取引を行うよう誘引して

⁵⁰ 本規則の目的上、インサイダー取引とは、ある者がインサイダー情報を保有し、その情報を利用して、自己の計算又は第三者の計算において、直接又は間接に、当該情報に関連する金融商品を取得し、又は処分する取引をいう。また、当該者がインサイダー情報を保有するに至る前に発注された、当該情報に関連する金融商品に関する注文について、その情報を利用して取消し又は修正を行うことも、インサイダー取引とみなされる (For the purposes of this Regulation, insider dealing arises where a person possesses inside information and uses that information by acquiring or disposing of, for its own account or for the account of a third party, directly or indirectly, financial instruments to which that information relates. The use of inside information by cancelling or amending an order concerning a financial instrument to which the information relates where the order was placed before the person concerned possessed the inside information, shall also be considered to be insider dealing. In relation to auctions of emission allowances or other auctioned products based thereon that are held pursuant to Regulation (EU) No 1031/2010, the use of inside information shall also comprise submitting, modifying or withdrawing a bid by a person for its own account or for the account of a third party.) 。

⁵¹ 本規則の目的上、他の者に対してインサイダー取引を行うよう勧告し、又は誘引する行為とは、ある者がインサイダー情報を保有し、かつ、次のいずれかに該当する場合をいう (For the purposes of this Regulation, recommending that another person engage in insider dealing, or inducing another person to engage in insider dealing, arises where the person possesses inside information and) 。

- (a) 当該情報に基づいて、他の者に対し、当該情報に関連する金融商品を取得し、又は処分することを勧告し、又はそのような取得若しくは処分を行うよう誘引する場合 (recommends, on the basis of that information, that another person acquire or dispose of financial instruments to which that information relates, or induces that person to make such an acquisition or disposal, or) 。
- (b) 当該情報に基づいて、他の者に対し、当該情報に関連する金融商品に関する注文を取消し、又は修正することを勧告し、又はそのような取消し若しくは修正を行うよう誘引する場合 (recommends, on the basis of that information, that another person cancel or amend an order concerning a financial instrument to which that information relates, or induces that person to make such a cancellation or amendment) 。

はならない (No person shall engage or attempt to engage in insider dealing or use inside information about crypto-assets to acquire, or dispose of, those crypto-assets, directly or indirectly, whether for that person's own account or for the account of a third party. No person shall recommend that another person engage in insider dealing or induce another person to engage in insider dealing.)。

(3) 正当化事由の不存在

MAR 第 9 条で自己内部者取引が規定されているが、MiCA においては、自己内部者取引が定められていない。具体的には、マーケットメーカーとして取引を行う場合や第三者のために執行を行う場合といった MAR の規制の下では許容される取引であっても、MiCA の規制の下ではインサイダー取引が成立する可能性がある。

また、MAR 第 9 条第 3 項⁵²において、内部者情報を知る前に実行された取引に関してインサイダー取引を適用しないとしているのとは異なり、MiCA においては内部者情報を知る前に実行された取引等に関してインサイダー取引を適用しないとする規定も存在しない。

また、MAR 第 5 条では一定の条件の下で容認されている自己株式売買 (Buy-back program) について、MiCA においては正当化事由が規定されていないため、基本的に Buy-back program は禁止されることになると考えられる。

3. 相場操縦規制

(1) 相場操縦に関する規定

MiCA 第 91 条の相場操縦に関しても、MAR 第 12 条第 1 項⁵³の規定をベースとして規定されている。

⁵² ある者がインサイダー情報を保有し、その情報を利用したことによりインサイダー取引を行ったものとみなされる場合であっても、当該者が金融商品を取得し、又は処分する取引を行い、その取引が善意に基づき履行期の到来した義務の履行として行われたものであり、かつ、インサイダー取引の禁止を回避する目的で行われたものではないときは、当該者はインサイダー取引を行ったものとはみなされない。ただし、次のいずれかに該当する場合に限る (inside information that that person has used that information and has thus engaged in insider dealing on the basis of an acquisition or disposal where that person conducts a transaction to acquire or dispose of financial instruments and that transaction is carried out in the discharge of an obligation that has become due in good faith and not to circumvent the prohibition against insider dealing and:)。

(a) 当該義務が、当該者がインサイダー情報を保有する以前に行われた注文又は締結された契約に基づいて生じたものである場合 (that obligation results from an order placed or an agreement concluded before the person concerned possessed inside information; or)。

(b) 当該取引が、当該者がインサイダー情報を保有する以前に生じた法令又は規制上の義務を履行するために行われたものである場合 (that transaction is carried out to satisfy a legal or regulatory obligation that arose, before the person concerned possessed inside information.)。

⁵³ 本規則の目的上、相場操縦とは、次の各号のいずれかに該当する活動をいう (For the purposes of this Regulation, market manipulation shall comprise the following activities:)。

(a) 取引を締結し、売買注文を提出し、又はその他の行為を行うことにより、次のいずれかに該当する結果を生じさせ、又は生じさせるおそれがある行為: (entering into a transaction, placing an order to trade or any other behaviour which:)

(i) 金融商品、関連する現物商品契約又は排出枠に基づくオークション対象商品の供給、需要又は価格について、虚偽又は誤解を招くシグナルを与え、又は与えるおそれがある行為 (gives, or is likely to give, false or misleading signals as to the supply of, demand for or price of a financial instrument, a related spot commodity contract or an auctioned product based on emission allowances; or)。

- いかなる者も、相場操縦を行い、又はこれを行おうとしてはならない。(No person shall engage in or attempt to engage in market manipulation.)
- 本規則の目的上、相場操縦とは、次の各号のいずれかに該当する活動をいう。
(For the purposes of this Regulation, market manipulation shall comprise any of the following activities)
 - (a) 正当な理由なく、取引を締結し、売買注文を提出し、又はその他の行為若しくは活動を行うことにより、次のいずれかに該当する結果を生じさせ、又は生じさせるおそれのある行為 (unless carried out for legitimate reasons, entering into a transaction, placing an order to trade or engaging in any other behaviour which)
 - (i) 暗号資産の供給、需要又は価格について虚偽又は誤解を招くシグナルを与え、又は与えるおそれがある行為 (gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of, a crypto-asset)
 - (ii) 一つ又は複数の暗号資産の価格を異常又は人為的な水準に維持する、又は維持するおそれがある行為 (secures, or is likely to secure, the price of one or several crypto-assets at an abnormal or artificial level)
 - (b) 虚偽の手段その他の欺瞞的な方法を用いて、取引を締結し、売買注文を提出し、又はその他の行為若しくは活動を行うことにより、一又は複数の暗号資産の価格に影響を与え、又は影響を与えるおそれがある行為 (entering into a transaction, placing an order to trade or any other activity or behaviour which affects or is likely to affect the price of one or several crypto-assets, while employing a fictitious device or any other form of deception or contrivance)
 - (c) メディア（インターネットを含む。）その他の手段を通じて情報を流布することにより、一又は複数の暗号資産の供給、需要又は価格について虚偽又は誤解を招くシグナルを与え、又は与えるおそれがある行為、又は一若しくは複数の暗号資産の価格を異常若しくは人為的な水準に維持し、又は維持す

-
- (ii) 一又は複数の金融商品、関連する現物商品契約又は排出枠に基づくオークション対象商品の価格を、異常又は人為的な水準に維持し、又は維持するおそれがある行為 (secures, or is likely to secure, the price of one or several financial instruments, a related spot commodity contract or an auctioned product based on emission allowances, at an abnormal or artificial level; unless the person who entered into the transaction, placed the order or engaged in the behaviour establishes that the reasons for doing so are legitimate and that that transaction, order or behaviour conforms to accepted market practices as established in accordance with Art 13;)
 - (b) 虚偽の手段その他の欺瞞的な方法を用いて、取引を締結し、売買注文を提出し、又はその他の活動若しくは行為を行うことにより、一又は複数の金融商品、関連する現物商品契約又は排出枠に基づくオークション対象商品の価格に影響を与え、又は影響を与えるおそれがある行為 (entering into a transaction, placing an order to trade or any other activity or behaviour which affects or is likely to affect the price of one or several financial instruments, a related spot commodity contract or an auctioned product based on emission allowances, which employs a fictitious device or any other form of deception or contrivance;)
 - (c) メディア（インターネットを含む。）その他の手段を通じて情報を流布することにより、金融商品、関連する現物商品契約又は排出枠に基づくオークション対象商品の供給、需要又は価格について虚偽又は誤解を招くシグナルを与え、又は与えるおそれがある行為、又は当該金融商品、契約若しくは商品の価格を異常若しくは人為的な水準に維持し、又は維持するおそれがある行為 (disseminating information through the media, including the internet, or by any other means, which gives, or is likely to give, false or misleading signals as to the supply of, demand for or price of a financial instrument, a related spot commodity contract or an auctioned product based on emission allowances, or secures, or is likely to secure, the price of one or several such instruments, contracts or products at an abnormal or artificial level, including the dissemination of rumours, where the person who made the dissemination knew, or ought to have known, that the information was false or misleading;)
 - (d) ベンチマークに関して虚偽又は誤解を招く情報を伝達し、又は虚偽若しくは誤解を招く入力値を提供する行為であって、その情報を伝達し、又は入力値を提供した者がそれが虚偽又は誤解を招くものであることを知っていた、又は知るべきであった場合のもの、又はその他ベンチマークの算定を操作する行為 (transmitting false or misleading information or providing false or misleading inputs in relation to a benchmark where the person who made the transmission or provided the input knew or ought to have known that it was false or misleading, or any other behaviour which manipulates the calculation of a benchmark.)

るおそれがある行為（disseminating information through the media, including the internet, or by any other means, which gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of one or several crypto-assets, or secures or is likely to secure, the price of one or several crypto-assets, at an abnormal or artificial level, including the dissemination of rumours, where the person who engaged in the dissemination knew, or ought to have known, that the information was false or misleading.）。

(2) ベンチマークに関する相場操縦規制について

ベンチマークに関する相場操縦について MiCA においては、MAR 第 12 条第 1 項(d)⁵⁴に相当する規定が存在しない。

4. 罰則等

(1) 罰則

インサイダー取引や相場操縦に関して、EU 加盟国当局は、以下の基準を各加盟国内法で定めるべき罰金の上限額の下限とした行政罰に関する国内法を整備しなければならない。（MiCA 第 111 条第 5 項）なお、インサイダー取引や相場操縦により得られた利益の 3 倍に相当する額を最高額とする行政罰を定めることも可能である（同項(h)⁵⁵）。

違反の種類	対象となる当事者	各加盟国内法で定めるべき罰金の上限額の下限 ⁵⁶
第 88 条違反 (インサイダー情報の公開義務)	自然人 (MiCA 第 111 条第 5 項(i))	1,000,000 ユーロ
	法人 (MiCA 第 111 条第 5 項(j))	2,500,000 ユーロ又は年間売上高の 2%
第 89 条～ 第 92 条違反	自然人 (MiCA 第 111 条第 5 項(i))	5,000,000 ユーロ

⁵⁴ 脚注 53 参照。

⁵⁵ 違反行為により得られた利益又は回避された損失の額を算定することができる場合には、当該額の少なくとも三倍に相当する額を上限とする行政上の制裁金を科すことができるものとし、この場合においては、(i)又は(j)に定める上限額を超えることとなるときであっても、これを妨げない（maximum administrative fines of at least three times the amount of the profits gained or losses avoided because of the infringement, where those can be determined, even if it exceeds the maximum amounts set out in point (i) or (j), as applicable;）。

⁵⁶ なお、ユーロを法定通貨としない国においては、2023 年 6 月 29 日時点の為替相場において同額の価値を基準とする。「in the Member States whose official currency is not the euro, the corresponding value in the official currency on 29 June 2023（MiCA 第 111 条第 5 項(i)及び(j)）」

(市場濫用)	法人 (MiCA 第 111 条第 5 項(j))	15,000,000 ユーロ又は年 間売上高の 15%
--------	------------------------------	--------------------------------

(2) 罰則に関する事例

なお、EC、マルタ当局等に対し、MiCA に基づき、相場操縦やインサイダー取引に罰則を課した事例を調査したものの、現時点で罰則を課した事例について確認することはできなかった。

5. フロントランニングの禁止

MiCA 第 78 条第 2 項において、インサイダー取引の規制とは関係なく、行為規制として従業員によるフロントランニングの禁止が定められている。同項の「情報」は内部者情報に限定されていないため、公開済みの注文情報に基づく注文行為が同項違反になる余地がある。なお同項に基づき MEV の抽出が禁止される可能性について、EC へのヒアリングにおいて確認したところ以下のような回答が得られた。

- ブロック生成過程でトランザクション順序を操作する MEV の抽出それ自体は直ちに違法と評価されるものではない。
- ただし、MEV の抽出の一形態であるトランザクションの並べ替えを利用したフロントランニングや相場操縦は、不公正取引に該当し得る。
- 非公開の内部者情報を利用して MEV を行えばインサイダー取引となり得る。
- その上で、MEV の抽出そのものを一律に禁止する計画はない。

6. 市場濫用行為の検知について

(1) 市場濫用に関する規制技術基準⁵⁷

MiCA 第 92 条第 3 項に基づき、市場濫用に関する規制技術基準が定められている。同基準においては、市場参加者に対して、市場濫用を能動的に防止・検知する義務が定められている。市場参加者は、市場濫用を監視・検知するための効果的なシステムを確立・維持しなければならない。これらのシステムは、事業の規模、性質、及び範囲に比例したものでなければならない。

⁵⁷ Guidelines on supervisory practices to prevent and detect market abuse under MiCA
https://www.esma.europa.eu/sites/default/files/2025-04/ESMA75-453128700-1408_Final_Report_MiCA_Guidelines_on_prevention_and_detection_of_market_abuse.pdf

(2) その他の暗号資産

疑わしい取引を検知した市場参加者は、市場濫用の合理的な疑いが生じた場合、遅滞なく主管当局に不審取引・注文報告書 (Suspicious Transaction or Order Report) を提出する義務がある⁵⁸。

また、MiCA で定められている報告事項としては、報告を行う事業体、不審な人物、不審な取引又は行動の詳細な説明、及び関連する DLT に関する技術的詳細が含まれる⁵⁹。

(3) 市場濫用行為に関する実務

マルタ当局へのヒアリングによれば、市場濫用行為を検知するための実務を確認したところ、以下の理由により、市場濫用行為を検知することは非常に困難であるとのことである。

- CASP が EU 域外の暗号資産取引所において取引を執行する場合には、当該取引のデータを取得することは非常に困難であり、仮にデータを取得できたとしても不完全なデータしか取得することができない。
- マーケットメーカーに対する規制が不十分である。
- CASP として監督を受ける取引所に上場される暗号資産に関しては、基本的に DeFi として MiCA の規制を受けない取引所において取引されている。そのため、上場に関する情報公開の前にノンカストディアルウォレットを通じた売買を行うことは可能であり、当該取引を完全に規制することは困難である。

⁵⁸ MiCA 第 92 条第 2 項に基づく「市場濫用の防止・検知・報告に関する体制等を定める規制技術基準」第 5 条及び第 6 条

https://eur-lex.europa.eu/eli/reg_del/2025/885/oj/eng

⁵⁹ MiCA 第 92 条第 2 項に基づく「市場濫用の防止・検知・報告に関する体制等を定める規制技術基準」ANNEX STOR template を参照。

第3.暗号資産関係の詐欺・盗難・不公正取引等の摘発等をした事案の実態

I. 欧州（EU）における事案

1. 加盟国当局の要請に基づき、欧州連合司法協力庁が捜査を実施した事案⁶⁰

2018 年頃からとあるオンライン投資プラットフォームで「高収益が得られる」とうたい、被害者から総額 1 億ユーロを集金した詐欺事件が起きた。この資金はリトアニアの銀行口座を経由してマネー・ローンダリングされていたため、スペイン及びポルトガル当局の依頼を受け、ユーロジャストが共同捜査チームを設置した。そしてスペイン・ポルトガルに加えイタリア、ルーマニア、ブルガリアの計 5 か国で家宅捜索を実施し、銀行口座や金融資産の凍結に至った。

2. Operation Endgame⁶¹

2024 年 5 月から実施されているエンドゲーム作戦（Operation Endgame）は、ドイツの犯罪対策中央局と連邦刑事警察局が実施した共同作戦であり、ある犯罪組織が資金洗浄やランサムウェア攻撃に使用していた 6 種類のマルウェア（IcedID、SystemBC、Bumblebee、Smokeloader、Pikabot、Trickbot）と、その関連インフラストラクチャを摘発・無力化することを目的としたものである。その結果、総取引量が 7000 万ユーロ以上にのぼる 99 個の暗号資産ウォレットが、関係各国の暗号資産取引所で凍結された。

II. 香港における事案

香港財經事務及庫務局（Financial Services and the Treasury Bureau、以下「FSTB」という。）の局長である許正宇氏が、2024 年 2 月に、香港立法会での書面答弁として公式に報告した内容によれば、香港では、近年、仮想資産⁶²に関連する犯罪件数が増加しており、2021 年が 1,397 件、2022 年が 2,336 件、2023 年が 3,415 件であり、被害金額はそれぞれ、2021 年が 8 億 2400 万香港ドル、2022 年が 17 億 400 万香港ドル、2023 年が 43 億 9800 万香港ドルに上った⁶³。

同報告によれば、このような増加傾向を背景に、香港証券先物委員会（The Securities and Futures Commission、以下「SFC」という。）及び香港警察は、暗号資産取引所及び関連する疑わしい活動に関する情報共有を強化し、2023 年 12 月以降は週 2 回の頻度で情報交換を行い、①疑わしい活動の情報共有、②リスク評価の仕組みの導入、及び③捜査の連携強化を目指した活動を行っている⁶⁴。以下、具体的な事案も紹介する。

⁶⁰ <https://www.eurojust.europa.eu/news/eurojust-coordinates-action-halt-cryptocurrency-fraud-over-100-million-euros-across-europe>

⁶¹ <https://www.amf-france.org/fr/actualites-publications/actualites/une-manipulation-de-marche-identifiee-et-signalee-par-lamf-sanctionnee-par-le-tribunal-correctionnel>

⁶² 香港当局においては、「Virtual Asset」の語が使用されているため、「仮想資産」と訳したもの。

⁶³ FSTB 局長である許正宇氏による書面答弁の（一）及び（二）を参照。

<https://www.info.gov.hk/gia/general/202402/21/P2024022100216.htm>

⁶⁴ 脚注 63。FSTB 局長である許正宇氏による書面答弁の（三）を参照。

1. JPEX 詐欺事件

香港における代表的な詐欺摘発事例としては、JPEX 事件がある。SFC による JPEX 事件に関する声明によれば、概要は次のとおりである。2022 年頃、「JPEX」という仮想通貨取引プラットフォームは、ソーシャルメディアのインフルエンサーや店頭型仮想通貨両替業者を通じて、香港の一般市民向けに積極的な宣伝を行っていた。しかし、当該プラットフォームは、仮想通貨取引に関するライセンスを一切申請、取得しておらず、無登録で営業していた⁶⁵。そのため、SFC は、2022 年 3 月以降、虚偽表示や無認可活動の疑いで JPEX に対する調査を開始した。JPEX は当該調査に対して非協力的であったことから、SFC は、同年 7 月 8 日、JPEX を SFC の「無認可・疑わしいウェブサイト」リスト⁶⁶に掲載した⁶⁷。

さらに、2023 年 9 月 13 日、SFC は、JPEX 及びその関連人物等の疑わしい点として、①ウェブサイト及び広告で「認可・ライセンスを持つデジタル資産・仮想通貨取引プラットフォーム」と虚偽表示し、いくつかの海外規制当局の許可を得たと虚偽の宣伝をしていること、②その一部の商品について、極めて高い利回りを提示していること、③仮想通貨の預金、貯蓄又は利息などの SFC の規制では認められていない商品を提供していること、④香港上場企業と業務提携・投資を受けたという虚偽の事実の宣伝をしていること、⑤投資者から出金ができない、又は口座残高の減少や改ざんがあったとの苦情が寄せられ、メディアでも報道されていること、を公表し、投資者に対する警告声明を発出した⁶⁸。その後、SFC は、詐欺の可能性が判明したことから、JPEX 事件を香港警察へ通報した。香港警察は JPEX 事件を捜査していたが、2025 年 11 月 5 日、香港警察は 16 名を正式に起訴したと発表し、被告らは翌 11 月 6 日に裁判所に出廷した⁶⁹。2025 年 11 月現在、捜査は継続中であり、逮捕者総数は 80 名に上っている⁷⁰。

また、JPEX 事件に関連する民事事件も報じられている。2024 年 7 月、JPEX の利用者である原告ら 2 名（個人）は、JPEX を運営する被告ら 7 名を香港区域裁判所に提訴し、自身が預けた約 24 万 USDT の返還を求めた⁷¹。香港区域裁判所は、2024 年 10 月末、原告らの請求を認容し、被告らが原告らの同意なしに資産を他のウォレットに移転した行為は信託義務に違反すると指摘し、被告らに対して原告が JPEX プラットフォームを通じて預け入れた約 24 万 USDT を返還するように命じた。

⁶⁵ <https://www.sfc.hk/en/News-and-announcements/Policy-statements-and-announcements/Statement-on-JPEX>

⁶⁶ <https://www.sfc.hk/en/alert-list>

⁶⁷ <https://www.sfc.hk/en/alert-list/2850>

<https://www.sfc.hk/en/News-and-announcements/Policy-statements-and-announcements/Statement-on-JPEX>

⁶⁸ <https://www.sfc.hk/en/News-and-announcements/Policy-statements-and-announcements/Warning-statement-on-unregulated-virtual-asset-trading-platform>

⁶⁹ 具体的に 16 人の被告のうち、6 人は犯罪組織の中核メンバーとされ、共謀詐欺、マネー・ローンダリング、司法妨害及び「虚偽又は事実を無視して他人に仮想通貨への投資を誘導した罪」で起訴された。また、店頭取引業者の責任者及びインフルエンサーである 7 人は詐欺、マネー・ローンダリング、「虚偽又は事実を無視して他人に仮想通貨への投資を誘導した罪」で起訴された。名義貸し口座の所有者 3 人はマネー・ローンダリングの罪で起訴された。

<https://news.mingpao.com/pns/%e6%b8%af%e8%81%9e/article/20260103/s00002/1767377277452/jpex%e6%a1%88%e6%b6%89%e6%b4%971880%e8%90%ac-%e6%9c%b1%e5%85%ac%e5%ad%90%e5%8a%a0%e6%8e%a73%e7%bd%aa>

⁷⁰ 脚注 69 参照。

⁷¹ 香港区域裁判所による *Chan Wing Yan and Another v. JP-EX Crypto Asset Platform Ltd and Others* [2024] HKDC 1628 第一審判決（2025 年 10 月 15 日時点、上訴又は再審の公表された情報は見当たらない。）。
https://legalref.judiciary.hk/lrs/common/ju/ju_frame.jsp?DIS=163837

2. Mixin ハッキング被害事件

2023 年、香港の仮想通貨関連企業「ミキシン (Mixin)」は、クラウドサービスプロバイダーのデータベースを通じたサイバー攻撃により、約 2 億アメリカドルに相当する仮想通貨を失った。同社は顧客の引き出しを一時停止し、影響を受けた脆弱性の修正を進めている⁷²。同社の、2024 年 4 月 9 日付けリリースによれば、当該事件の主な原因は、ハッカーが Mixin の出金処理において利用していた依存していた Google Cloud Services へ不正アクセスし、クラウド環境のソフトウェア脆弱性を悪用し、大量の不正な出金リクエストを生成したことにあるとされる⁷³。

3. 仮想通貨によるマネー・ローンダリングの摘発等の事例

2025 年 5 月 15 日、香港警察は、中国本土と香港で活動するマネー・ローンダリングの跨境犯罪集団を摘発した。当該犯罪集団は、中国本土の居住者を香港に呼び込み、500 以上の銀行口座を開かせ、詐欺事件の収益をその口座で受け取り、その後、仮想通貨両替所で仮想通貨に換金して犯罪収益の流れを隠蔽・転移させていた。2024 年 7 月から 2025 年 5 月までに総額 1 億 1800 万香港ドルを洗浄したとされ、そのうち約 1000 万香港ドルは 58 件の報告済み詐欺事件に由来する犯罪収益であることが確認された。同 58 件で被害者が被った損失の総額は約 4320 万香港ドルにのぼると報じられた⁷⁴。

また、香港警察は、2024 年 10 月、ディープフェイク技術で恋愛関係を偽装し、被害者を偽の仮想通貨投資に誘導した詐欺グループを摘発し、27 人を逮捕した⁷⁵。同事件では、約 3 億 6000 万香港ドルの被害が発生していた。

さらに、香港高等裁判所は、2024 年 12 月、Worldwide A-Plus Ltd に関する事件 (HCZZ 88/2024, HCA 2417/2024) で、香港初のトークンに対する法的な差止命令を行った⁷⁶。従来、匿名ウォレット所有者への通知は困難であったところ、当該トークンに対する差止命令の効果により、詐欺によって約 266 万米ドル相当の Tether (USDT) が不正送金された 2 つの匿名ウォレットに対し、ブロックチェーン上で直接記録される形で資産処分を世界的に禁止した。これにより、当該匿名ウォレットとの取引者もブロックチェーン上で法的制限を認識できるようになり、当該トークンに対する資産凍結が可能となった。

III. シンガポールにおける事案

シンガポールでは暗号資産に関連する詐欺事件が急増しており、警察当局も取締りを強化している。2024 年には詐欺被害総額が過去最高の 11 億シンガポールドルに達し、そのうち暗号資産関連の詐欺が全体の約 24.3%を占めたとのことである⁷⁷。具体的な事案としては以下がある。

このほか、シンガポール金融管理局 (Monetary Authority of Singapore、以下「MAS」という。) とシンガポール警察は、暗号資産関連の犯罪増加に対し取締りを強化

⁷² <https://jp.reuters.com/markets/cryptocurrency/ZJKNDQR33BLPXPTPIIIT2QJXSU-2023-09-26>

⁷³ <https://mixin.network/923/>

⁷⁴ https://www.hkcd.com.hk/hkcdweb/content/2025/05/17/content_8695268.html

⁷⁵ <https://therecord.media/hong-kong-police-bust-romance-scammers-face-swapping-deepfakes>

⁷⁶ <https://www.mittrade.com/insights/news/live-news/Art-3-601227-20250125>

<https://cointelegraph.com/news/hong-kong-tokenized-legal-notice-tron>

⁷⁷ <https://ca.marketscreener.com/news/latest/Singaporeans-lose-record-822-million-to-scams-in-2024-police-say-49150155/>

している。例えば、2025 年 6 月 20 日からは、無認可の外国為替・暗号資産取引プラットフォームである「Octa」と「XM」へのアクセスをジオブロッキングするという措置を発表している⁷⁸。

1. A&A Blockchain 事件

最近の代表的な詐欺事件の摘発事案としては、A&A Blockchain の元 CEO が、投資者向けのマーケティング資料の中で、「中国雲南省のマイニングマシン 30 万台の所有権の 70%を雲南順愛雲捷投資ホールディングスから取得することに合意した」旨の虚偽を述べ、700 人以上の投資者から合計約 670 万シンガポールドルを詐取した、というものがある⁷⁹。この事例に対しては、2024 年 8 月 26 日付で、首謀者に対し懲役 6 年及び罰金 1 万 6000 シンガポールドルの判決が言い渡されている⁸⁰。

2. Amazing tech 事件

近時の詐欺事件として、2025 年 7 月 31 日に、Tokenize Xchange の運営会社 Amazing tech の創設者兼 CEO である Hong Qi Yu 氏が、顧客資産の分別管理に関して虚偽の表示を行っていたとの嫌疑で詐欺で起訴された、というものがある。本事件に関しては、2025 年 7 月 4 日に MAS が Amazing tech の暗号資産業の許可申請を却下したのを受け、同月 20 日に同社はシンガポールでの事業ができなくなったため、顧客から受け取った資産を確実に返還する必要に迫られている。なお、Amazing tech によると、顧客はプラットフォーム上で暗号資産取引はできなくなったものの、資産を他のプラットフォームに移管することは可能とのことである（ただし同年 9 月 30 日までに移管や引出しを完了する必要がある。）⁸¹。

3. BingX 事件

最近の代表的な不正流出事案としては、2024 年 9 月にシンガポールを拠点とする暗号資産取引所 BingX がハッキング被害に遭った、というものがある。当初、被害額は 2600 万米ドルと報じられたが、その後の詳細な調査により、被害額は 5200 万米ドル以上だったことが判明している⁸²。なお、このハッキング事件に対し、BingX はすべての顧客損失を自己資本で全額補填すると声明を発表したが、これは事業者の自主的な判断によるものであり、規制上の義務ではない。

4. その他

そのほか、2025 年 1 月、警察が銀行に対し詐欺被害者の銀行口座の凍結命令を出せるよう、新法が可決された。この法律の下で警察は、被害者が詐欺師に送金したかどうか、詐欺師と現在も連絡を取り合っているかどうかなどを考慮して凍結命令を出すことになる。凍結命令は 30 日間有効で、更新は最大 5 回までであ

⁷⁸ <https://www.channelnewsasia.com/singapore/octa-xm-blocked-trading-platforms-online-brokers-forex-commodities-stocks-shares-indices-5168571>

⁷⁹ <https://www.police.gov.sg/-/media/SPF/Files/Publications/PDF/CAD-Report-2023.pdf>

⁸⁰ https://www.elitigation.sg/gd/s/2022_SGHC_264

⁸¹ <https://www.channelnewsasia.com/singapore/mas-tokenize-xchange-assets-money-license-5258531>

⁸² <https://www.vibrantiumaudits.com/post/massive-52-million-bingx-hack-how-it-happened-and-the-recovery-efforts>

る。現在は伝統的な銀行、銀行口座を対象としているが、内務省によると、今後状況次第では、仮想通貨取引所や送金会社、電子ウォレット提供会社にも凍結命令を出せるよう検討するとのことである⁸³。

また、2025 年 5 月には、MAS が「海外の顧客のみにサービスを提供する仮想通貨取引所は 6 月 30 日までに閉鎖しなければならない」と公表した。これは、海外の顧客のみにサービスを提供するという形態は、マネー・ローンダリングのリスクが高く、実質的な規制対象行為がシンガポール国外で行われる場合には MAS の規制が及ばない、というのが理由とされている。なお、シンガポールに拠点を置く世界最大級の仮想通貨取引所である Bitget と Bybit は香港やドバイへの移転を計画することになったとされている⁸⁴。

IV. アメリカにおける事案

2023 年 3 月時点までにおける、アメリカにおける主要な摘発事案については、EY ストラテジー・アンド・コンサルティング株式会社・ベーカー&マッケンジー法律事務所（外国法共同事業）「デジタル資産を用いた不公正取引等に関する国際的な規制動向、法規制当局による執行事例、及びマーケットにおける課題の分析調査に関する報告書⁸⁵」（令和 5 年（2023 年）3 月）において、すでに詳述されていることから、2023 年 4 月以降、2025 年 10 月時点において確認できたアメリカにおける主要な摘発事案の概要を記載する。

1. 暗号資産に係る相場操縦に対する SEC による執行事例⁸⁶

SEC は、2024 年 10 月 9 日、証券（securities）として提供・販売されている暗号資産の市場を操作するスキームに関与したとして、自称マーケットメーカー 3 社及び 9 名の個人を、詐欺行為などの禁止を定めた 1933 年証券法（Securities Act of 1933）⁸⁷第 17 条(a)(1)、(a)(3)、1934 年証券取引法（Securities Exchange Act of 1934）⁸⁸第 10 条（b）及び SEC 規則 10b-5(a)、(c)⁸⁹に違反したとして、民事制裁金の支払を求めるなどするとともに、連邦捜査局（FBI）と連携している。

具体的には、Howey 基準により、証券とされた暗号資産に関する事案であり、暗号資産の販売会社（crypto asset promotor）が、一般投資者に提供、販売した暗号資産について、人為的な取引高の作出や価格の操作（generating artificial trading volume or manipulating the price of crypto assets）を含む相場操縦を、マーケットメーカーに実施させ、当該暗号資産にアクティブな取引市場が存在するという虚偽の外観を作出し、当該販売会社が投資者に当該暗号資産を購入させた事案である。

⁸³ <https://www.reuters.com/world/asia-pacific/singapore-empowers-police-freeze-bank-accounts-scam-crackdown-2025-01-07/?/>

⁸⁴ <https://sg.news.yahoo.com/singapore-order-leads-unlicensed-crypto-exchanges-to-weigh-exit-014842926.html>

⁸⁵ https://www.fsa.go.jp/common/about/research/20230427/20230427_report_digitalassets.pdf

⁸⁶ <https://www.sec.gov/newsroom/press-releases/2024-166>

⁸⁷ SECURITIES ACT OF 1933

<https://www.govinfo.gov/content/pkg/COMPS-1884/pdf/COMPS-1884.pdf>

⁸⁸ SECURITIES EXCHANGE ACT OF 1934

<https://www.govinfo.gov/content/pkg/COMPS-1885/pdf/COMPS-1885.pdf>

⁸⁹ 17 C.F.R. 240.10b-5

<https://www.ecfr.gov/current/title-17/chapter-II/part-240/subpart-A/subject-group-ECFRbda83517ce4377f/section-240.10b-5>

2. 暗号資産に関する CFTC による執行事例

CFTC Releases FY 2024 Enforcement Results⁹⁰の Addendum において、Digital Asset の関連の執行事例として紹介されている事案は、10 件ほどあるところ、概要が掲載されている主な詐欺事案として、次の 3. を紹介する。

3. デジタル資産プラットフォームの元 CEO を詐欺で提訴した事案⁹¹

本事案は、Voyager Digital Ltd.、Voyager Digital Holdings, Inc.、Voyager Digital, LLC（総称して「Voyager」という。）の元 CEO である、スティーブン・アーリック（Stephen Ehrlich）氏を、デジタル資産プラットフォーム、Voyager の未登録のコモディティ・プール（commodity pool）の運用に関する不正及び登録義務違反を理由に、提訴した事案である。具体的には、以下のとおり。

Voyager は、SNS や自社のウェブサイトにおける投稿において、変動性の高い市場環境における顧客のデジタル資産のための安全な避難先資産（safe haven）であること、Voyager が従来の金融機関と同等の厳格さと信頼性（the same level of rigor and trust）をもって運営されることを宣伝し、加えて同社のプラットフォームにおいて管理されている特定のデジタル資産について最大 12%の利回りを保証していた。Voyager は、保証した利回りを支払うための収益のために、保管された顧客資産を 1つのプールにまとめ、高リスクの第三者へ貸付を実施していた。Voyager は、コモディティ・インタレスト（commodity interests）の運用・取引によって Voyager のために収益を生み出すという理解のもと、顧客のデジタル資産コモディティ 6 億 5000 万ドル超を、無担保の条件で「ファーム A（デジタル資産ヘッジファンド）」に移転し、ファーム A が Voyager の投資を他の投資とプールし、これにより、Voyager は Voyager プール（Voyager Pool）を運営していた。これは、アメリカ商品取引所法の規制対象であるコモディティ・プールに該当し、アメリカ商品先物取引委員会（Commodity Futures Trading Commission、以下「CFTC」という。）の登録を必要があるところ、CFTC 登録を受けることなく、コモディティ・プール・オペレーター（CPO）として活動していた。その後、ファーム A がデフォルトし、Voyager は、運転資金の流動性の問題に直面したにもかかわらず、引き続き、Voyager は安全であると主張し、17 億ドル超の負債を抱え、破産申請したものである。

4. 小括

従前、証券に該当する暗号資産であれば、1933 年証券法等の証券規制の対象となり、SEC による執行となる一方、該当しない暗号資産については「商品」（commodity）として商品先物取引規制の規制対象となり、CFTC による執行となっているため、上記のように暗号資産に関しては SEC、CFTC による執行事案が存在している。もっとも、個別の暗号資産に関して、例えば証券に該当するか商品に該当するかについて、SEC と CFTC による規制の重複の可能性が指摘されていた。具体的には、CFTC は従前からビットコイン、イーサリアム及びライトコイン

⁹⁰ https://www.cftc.gov/media/11596/DOE_ResultsFY24_AddendumA120424/download

⁹¹ <https://www.cftc.gov/PressRoom/PressReleases/8805-23>

ンについて商品であるという立場をとっていた⁹²一方で、SEC は一定のトークンが証券たりうるという立場をとっており⁹³、各暗号資産がいずれの規制に服するかについて専門家からの関心を集めていた⁹⁴。CLARITY 法案 (Digital Asset Market Clarity Act) ⁹⁵は、SEC と CFTC のデジタル商品に関する監督権限を明確化し、デジタル商品に対する包括的な規制の枠組みの構築を図るものであることから、同様の事案が将来的には別の機関により執行がなされる可能性もあり、法案の審議状況も含め、注視が必要と考える。

第4.暗号資産の不正流出を防ぐための規制や不正流出に対する利用者の救済(保険等)

I. 欧州 (EU) における事案

1. 不正流出を防ぐための規制

不正流出を防ぐための規制としては、第 2.V.6 において記載のとおり、DORA が CASP に適用され、サイバーセキュリティに関する措置を講ずることが義務付けられている。

2. 利用者救済制度

EC へのヒアリングにおいては、暗号資産の不正流出が生じた場合に損失を補填するための保険に関する制度を作る動きについて確認することはできなかった。

II. 香港における事案

1. 不正流出を防ぐための規制

SFC は、不正流出を防ぐための規制として、仮想通貨取引プラットフォームの監督強化を図っており、そのためにライセンス制度と警告制度⁹⁶を提供するプラッ

⁹² “Bitcoin and other virtual currencies are encompassed in the DeFinition and properly DeFined as commodities.”とされている。(2015 年 9 月 17 日付商品取引法 6 条(c)項及び(d)項に基づく手続開始命令 <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinflprord09172015.pdf>)

また、2023 年 3 月 23 日付商品取引所法及び委員会規則に基づく差止命令及びその他の衡平法上の救済並びに民事金銭的罰則を求める訴状においても“Binance,(中略), has solicited and accepted orders, accepted property to margin, and operated a facility for the trading of futures, options, swaps, and leveraged retail commodity transactions involving digital assets that are **commodities** including bitcoin (BTC), ether (ETH), and litecoin (LTC) for persons in the United States.”としている。(<https://www.cftc.gov/media/8351/%2520enfbinancecomplaint032723/download>)

⁹³ SEC のゲーリー・ゲンズラー委員長は繰り返し、暗号資産が証券取引法の適用対象たりうる旨言及していた。(<https://www.sec.gov/newsroom/speeches-statements/gensler-sec-speaks-090822> 及び <https://www.sec.gov/newsroom/speeches-statements/gensler-senate-testimony-091223>)

⁹⁴ CFTC に提出された 2019 年 3 月 27 日付 ABA Derivatives & Future Law Committee White Paper では”Digital assets can raise unprecedented, challenging jurisdictional issues.””The markets would benefit if the CFTC and SEC developed a shared understanding of their respective regulatory interests over digital assets where they may have overlapping regulatory interests.”と言及されている。(https://www.cftc.gov/sites/default/files/2019-03/tac032719_-%20ABAWhitePaper.pdf)

⁹⁵ <https://www.congress.gov/bill/119th-congress/house-bill/3633/text/ih?/> (2025 年 7 月 17 日、下院可決)
https://www.fsa.go.jp/singi/singi_kinyu/angoshisanseido_wg/gijishidai/20250902/03.pdf (金融審議会 第 2 回 暗号資産制度に関するワーキング・グループ事務局説明資料)

⁹⁶ 香港における名称は「Alert List」。

トフォームを「認可済み」又は「申請中」として公表する⁹⁷一方、無許可や詐欺的行為の疑いがある業者は「警示リスト」に掲載し⁹⁸、投資者に取引前の確認を促している。これにより、ライセンスを偽装する業者や出金拒否などの詐欺行為から投資者を保護することが企図されている。

さらに、SFCは「仮想資産取引プラットフォーム運営者ガイドライン」(Guidelines for Virtual Asset Trading Platform Operators、⁹⁹以下「香港 VATP ガイドライン」という。)を作成し、同ガイドラインの第 X 章「Custody of Client Assets」において、仮想資産取引プラットフォーム運営者に対し、顧客資産の安全管理を求めている。具体的には、2.で詳述するとおり、仮想資産取引プラットフォーム運営者は顧客資産を自己資産と厳格に分離し、98%以上をコールドウォレットで保管しなければならない、ホットウォレット資産は全額保険を付保し、コールドウォレットも大部分を補償対象とすることが求められている。また、香港 VATP ガイドラインにより、秘密鍵管理の内部統制、不正アクセス防止、定期的な資産照合と報告体制の整備が義務化されている。

2. 利用者救済制度

香港 VATP ガイドライン 10.22 条から 10.26 条は、仮想資産取引プラットフォーム運営者に対し、顧客資産に損失が生じた場合の補償体制の整備を義務づけている。まず、仮想資産取引プラットフォーム運営者は、SFC の承認を得た補償体制を整備し、コールドウォレット保管分の 50%及びホットウォレットその他の保管分の 100%の潜在的損失を補償対象とする必要がある(10.22 条)。補償手段としては、保険、信託口座での資金や仮想資産の保管、銀行保証などが想定されており、補償体制の変更には SFC の事前承認が必要となる。仮想資産取引プラットフォーム運営者は、日次で顧客資産総額を監視し、補償水準を維持するための内部統制を確立しなければならない(10.23 条)、補償対象資産がカバーされた金額を上回るおそれがある場合には、SFC に報告し、是正措置を取る必要がある(10.24 条)。そのほか、補償のための資金確保や仮想資産の分別管理(10.25 条)や保険会社の選定(10.26 条)に関して定めが設けられている。なお、香港 VATP ガイドラインの別紙 2(d)では、該当する場合、顧客に対してリスク開示を行わなければならない事項の一つとして、「投資者賠償基金(investor compensation fund)による保護が仮想資産を含む取引(トークンの性質を問わず)には適用されない。」旨が定められている。

その他、利用者救済に関する民間での取り組みについては、次のようなものがある。2025 年 8 月 27 日、香港認可仮想資産取引プラットフォームである HashKey Exchange は、Web3 保険プロバイダーである OneInfinity by OneDegree との長期的パートナーシップを一層強化し、HashKey Exchange のカスタディ保険プログラムをアップグレードしたことを発表した。強化されたカスタディ保険は、18 か月の保険期間を持ち、補償範囲を拡大するとともに、プラットフォームが保管する資産の少なくとも 50%をカバーし、AM Best による最低「A-」評価及び Standard &

⁹⁷ <https://www.sfc.hk/en/Welcome-to-the-Fintech-Contact-Point/Virtual-assets/Virtual-asset-trading-platforms-operators/Lists-of-virtual-asset-trading-platforms>

⁹⁸ https://www.sfc.hk/en/Alert_List

⁹⁹ 2023 年 6 月 1 日施行。

<https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/Guidelines-for-Virtual-Asset-Trading-Platform-Operators/Guidelines-for-Virtual-Asset-Trading-Platform-Operators.pdf>

Poor's による最低「AA-」評価を受けた場合であれば、再保険により保険をも支えることもできると宣伝されている¹⁰⁰。

さらに、2025 年 11 月 3 日、SFC は「仮想資産取引プラットフォームの共有流動性に関する通達」¹⁰¹を公表し、シェアード・オーダーブック¹⁰²に対する監督管理ガイドラインを出した。当該通達によれば、シェアード・オーダーブックを提供するプラットフォーム運営者が、シェアード・オーダーブックを通じて実行される取引について、自社のシェアード・オーダーブック上で実行された取引と同等の責任を負うものとされている（第 16 条）。また、プラットフォーム運営者は、決済失敗によって生じた顧客の損失を補填するために、香港にリザーブ・ファンドを設立し、これを信託形式で保有し、顧客補償のために指定しなければならない、また、リザーブ・ファンドの規模は、未決済取引の上限を下回ってはならず、また想定される未決済取引リスクに応じて調整されなければならない（第 17 条）。さらに、プラットフォーム運営者は、決済資産に関する潜在的な損失（たとえば盗難、詐欺、横領などによって生じる損失）を補償するために、保険を契約し、又は補償制度を設けなければならない。その補償額は香港 VATP ガイドライン 10.22 条で定められた金額を下回ってはならないとされている（第 18 条）。

III. シンガポールにおける事案

シンガポールの暗号資産規制には、「決済サービス法（Payment Services Act, PSA）」¹⁰³と「金融サービス・市場法（Financial Services and Markets Act, FSMA）」¹⁰⁴という主要な法律が存在する¹⁰⁵。

1. 不正流出を防ぐための規制

「決済サービス法」は、暗号資産を「デジタル決済トークン(Digital Payment Token、以下「DPT」という。）」と定義し、交換サービスや保管ウォレットサービスなどを規制対象としている。この法律は、事業規模とリスクプロファイルに応じて、標準決済機関（Standard Payment Institution）と主要決済機関（Major Payment Institution）の許認可を区分けするという、リスクベースのアプローチを採用している。

「決済サービス法」は、不正流出を防ぎ、顧客資産を保護するための具体的な措置として、顧客の暗号資産を事業者の自己資産から明確に分別管理し、法定信託（statutory trust）の下で管理することや、厳格なリスク管理と内部統制を義務付けるほか、顧客の DPT の少なくとも 90%をコールドウォレットで保管することを推奨している。

また、2025 年 6 月 30 日以降、シンガポールで登記されているが海外顧客のみを対象とするデジタル決済トークンサービスプロバイダー（DTSP）にも、「決済

¹⁰⁰ <https://group.hashkey.com/en/newsroom/hashkey-exchange-protected-by-the-worlds-largest-virtual-asset-insurance>

¹⁰¹ <https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=25EC56>

¹⁰² 異なるプラットフォームからの注文は、統合された共有流動性プール（aggregate shared liquidity pool）にまとめることが認められ、これにより複数のプラットフォーム間での注文のマッチング及び取引の実行が可能となる。

¹⁰³ <https://www.mas.gov.sg/regulation/acts/payment-services-act>

¹⁰⁴ <https://www.mas.gov.sg/regulation/acts/financial-services-and-markets-act-2022>

¹⁰⁵ <https://www.complycube.com/en/how-successful-is-singapore-crypto-regulation/>

サービス法」と「金融サービス・市場法」に基づく許認可取得が義務付けられることとなったため、MAS の無認可事業者への規制範囲は拡大している¹⁰⁶。

2. 利用者救済制度

暗号資産については、預金保険制度（Singapore Deposit Insurance Corporation Limited）の対象外である。ただし、2023 年から導入された法定信託制度により、暗号資産業者は顧客資産と自社資産を分離して保管することが義務付けられたため¹⁰⁷、暗号資産業者が破綻した際の資産保護が一定程度講じられている。

また、サイバー犯罪の増加に伴い、複数の保険会社が個人向けのサイバー保険の提供を開始している。例えば、Etiqua 社が提供するサイバー保険は詐欺、恐喝、個人情報盗難に対し年額最大 25000 シンガポールドルの保障を用意し、データ復旧にも対応している。しかし、こういったサイバー保険は、暗号資産取引との関係では適用されない¹⁰⁸。このため、個人が暗号資産の売買や送金に絡んで詐欺被害に遭ったり、暗号資産ウォレットがハッキングされて資産を盗まれたりしても、サイバー保険ではカバーされない可能性が高いとも考えられる。

暗号資産に特化したものとして、オンライン保険ブローカーである Insurance Market 社が提供する保険がある。同社は 2018 年、地元の貴金属保管企業 Silver Bullion 社の金庫施設「The Safe House」で顧客の暗号資産の秘密鍵をオフライン保管し、その盗難・紛失に備えて保険を付与する仕組みの提供を開始している¹⁰⁹。しかし、この保険は、暗号資産そのものの損失を補償するものではなく、限定的な状況下（例えば金庫での秘密鍵保管など）の損失を補償するものに留まる。

IV. アメリカにおける事案

1. 不正流出を防ぐための規制

アメリカ連邦法において、暗号資産であることをもって不正流出を防ぐことを求めるなどする規制は現状見当たらない。

もっとも、現在審議されている CLARITY 法案（Digital Asset Market Clarity Act）¹¹⁰では、顧客資産の分別管理規定や取引監視、記録の保持・報告に関する規定などが定められているところである。

2. 利用者救済制度

アメリカ連邦法において、暗号資産取引に関する保険など、利用者救済のための制度は現状見当たらない。また、現在審議されている CLARITY 法案においても、このような制度は定められていない。

¹⁰⁶ <https://www.tassure.com/mas-tightens-crypto-oversight-unlicensed-overseas-facing-entities-will-be-blocked/>

¹⁰⁷ <https://www.cnplaw.com/singapore-to-introduce-new-measures-to-ring-fence-customers-crypto-assets/>

¹⁰⁸ <https://www.straitstimes.com/singapore/personal-cyber-insurance-an-emerging-product-as-scams-climb>

¹⁰⁹ <https://www.insurancebusinessmag.com/asia/news/breaking-news/singaporean-broker-launches-insurance-for-cryptocurrency-storage-99163.aspx>

¹¹⁰ 金融審議会 第 2 回 暗号資産制度に関するワーキング・グループ事務局説明資料
https://www.fsa.go.jp/singi/singi_kinyu/angoshisanseido_wg/gijishidai/20250902/03.pdf

第5.IEO・ICO等の暗号資産を用いた資金調達の実施状況とそれを促す取組（私募等の柔構造化含む。）

I. 欧州（EU）における事案

1. 概要

本報告書の第2章VI.2.において記載したとおり、適格機関投資者へのその他の暗号資産の提供についてホワイトペーパー作成が免除されているため、この免除規定を通じて、スタートアップによるICO又はIEOが実施される可能性がある。

2. 実際の取組

公開資料において、2025年10月現在、規制レベルでIEO・ICO等の暗号資産を用いた資金調達を促す仕組みを確認することはできなかった。また、EUにおいて暗号資産を用いた資金調達を促すためにホワイトペーパー作成に関する負担を軽減するための議論は現時点ではないことが確認できた。マルタ当局に対するヒアリングでは、民間レベルにおいて、ホワイトペーパーの作成に不慣れなスタートアップ企業のために、ホワイトペーパー作成のサービスを提供する企業が設立された例が存在することが確認された。

II. 香港における事案

1. 概要

香港では、2017年以後、ブロックチェーン技術を活用したICOなど仮想通貨による資金調達が活発になっており、一部事例では投資リターンを約束するなど投資性を有するトークンが発行されている。SFCは、同年9月、トークンが株式・債券・集団投資スキーム（collective investment scheme、CIS）に該当する場合、香港の証券先物条例（the Securities and Futures Ordinance）の「証券（securities）」として規制対象となることを明確化した¹¹¹。SFCによれば、香港内外を問わず、香港の一般投資者を対象にICOや仮想通貨関連業務を行う場合、SFCのライセンス取得又は登録を義務付けることで、合法的な資金調達手段としてIEO・ICOの透明化と制度的整備を進めているとのことである^{112,113}。FSTB及び香港金融管理局（Hong Kong Monetary Authority、以下「HKMA」という。）は、デジタルトークンを、仮想通貨（virtual “currency”）ではなく、仮想商品（virtual “commodity”）とみなしている¹¹⁴。

¹¹¹ <https://www.sfc.hk/en/News-and-announcements/Policy-statements-and-announcements/Statement-on-initial-coin-offerings>

¹¹² 前掲注111。

¹¹³ 例えば、SFCは、2018年3月、ICO発行者であるBlack Cell Technology Ltd.による香港公衆向けICOの発行について、ICOの資金をモバイルアプリ開発に充て、トークン保有者に株式引換権を与える構成がCISに該当する可能性があるとして指摘した。そのため、SFCは、Black Cell Technology Ltd.に対して、無許可勧誘及び無登録の規制対象行為の懸念から規制措置を実施した。

<https://apps.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=18PR29>

¹¹⁴ <https://www.info.gov.hk/gia/general/201711/08/P2017110800405.htm>

<https://www.hkma.gov.hk/eng/news-and-media/press-releases/2015/02/20150211-3/>

香港政府は、仮想通貨やトークン化資産を活用した資金調達を戦略的に推進し、香港をデジタル資産の国際ハブ化とする方針を掲げている。2022 年 10 月の政策宣言¹¹⁵や 2025 年 6 月に公表された「デジタル資産発展政策宣言 2.0」¹¹⁶により、AML/CFT 対応の取引所ライセンス制度整備、トークン化資産の法的整備、政府発行グリーンボンドのトークン化試行など、多面的な制度基盤が整え、又は整えられつつある。

また、SFC は「仮想通貨取引プラットフォームの製品とサービスの拡張に関する通達」を公表している。同通達は、デジタル資産を、仮想通貨、トークン化証券（「デジタル証券」の一分類に属する。）、及びステーブルコイン等を指すと定義した上、①トークン発行要件の改定、②仮想通貨取引プラットフォームにおけるトークン化証券及びデジタル資産に関する投資商品の規制の整理、③同一プラットフォームで売買されていないデジタル資産に適用されるカスタディサービス制度の更新を通じて、認可を受けた仮想通貨取引プラットフォームが提供できる製品及びサービスの範囲を拡大することを目指すものとされている¹¹⁷。さらに、同日、SFC は「仮想通貨取引プラットフォームの共有流動性に関する通達」を公表し、SFC の認可を受けた仮想通貨取引プラットフォーム運営者が、自社のオーダーブックをグローバル関連会社の仮想通貨取引プラットフォーム運営者のオーダーブックと統合する際の監督方針及び期待基準を示した。これにより、異なるプラットフォームの間の流動性を期待しているものと考えられる。

2. 実際の取組

1.で述べたとおり、香港では、ICO や IEO を通じた仮想通貨による資金調達は、トークンが証券や集団投資スキームに該当する場合、SFC の規制対象となる。香港の一般投資者向けの ICO・IEO には SFC ライセンス取得や登録が義務付けられ、仮想通貨取引プラットフォーム（virtual asset trading platform、以下「VATP」という。）に適用されるガイドラインに基づき適格性・能力要件、顧客資産分別管理、取引誠実性、継続報告などの遵守が求められる。さらに、AML/CFT に関するガイドラインにより、リスクの高い顧客や無規制の仮想通貨サービスプロバイダー VASPs（virtual asset service providers、以下「VASPs」という。）を通じた取引への監視も強化されており、マネー・ローンダリング対策が徹底されている。

すなわち、SFC は、2023 年 6 月に発効した「反マネー・ローンダリング及びテロ資金防止条例（改正）」¹¹⁸に基づき、「香港 VATP ガイドライン」を制定し、VATP に対して、IEO やトークン販売を含む仮想通貨取引を行う際に、適格性・能力要件、取引の誠実性義務、顧客資産の分別管理、取引操作防止、継続的報告・通知などを遵守することを求めている。同時に実施された「マネー・ローンダリング及びテロ資金供与対策に関するガイドライン（SFC ライセンス取得法人及び SFC ライセンス取得仮想通貨サービス提供者向け）（Guideline on Anti-Money Laundering and Counter Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers、以下「AML/CFT ガイドライン」という。）」では、マネー・ローンダリングやテロ資金供与のリスクが高いと考えられる顧客の例として、マネー・ローンダリングやテロ資金供与や金融犯罪の前提犯罪と関

¹¹⁵ <https://www.info.gov.hk/gia/general/202210/31/P2022103000454.htm?fontSize=1>

¹¹⁶ <https://www.info.gov.hk/gia/general/202506/26/P2025062600269.htm?fontSize=1>

¹¹⁷ <https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=25EC57>

¹¹⁸ <https://www.legco.gov.hk/yr2022/english/ord/2022ord015-e.pdf>

連があると知られている ICO 及びマネー・ローンダリング・テロ資金対策管理が不十分な、又は無規制の VASPs を通じて行われる仮想資産関連活動などが挙げられた¹¹⁹。このように、ICO 及び IEO に対するマネー・ローンダリング対策が強化されている。SFC は、2024 年 6 月以降、迅速ライセンス審査手続を一部適用し、VATP 新規申請者の申請審査プロセスを効率化する動きを見せており¹²⁰、2025 年 1 月の通達により、2024 年 12 月 18 日以降に申請されるすべての新規 VATP 申請者に対して迅速ライセンス審査手続が適用されるようになった¹²¹。

また、2025 年 6 月には、SFC と FSTB は、仮想資産カストディ業務規制の立法提案に関する意見募集を行い、仮想資産の発行から流通・保管までの一連の流れについて整備を進め、仮想資産を通じた資金調達を促進することを目指す姿勢を明らかにした¹²²。2025 年 9 月 30 日、SFC 及び HKMA が「仲介業者の仮想資産関連活動に関する補足共同通達（Supplemental Joint Circular on Intermediaries' Virtual Asset-related Activities）」を公表し、従来の投資者保護要件（顧客の純資産評価や VA 先物のリスク開示）が機関投資者や法人プロ投資者には適用されないことを明確化した¹²³。さらに、同通達によれば、条件付きで顧客が仮想資産を用いて投資商品に申し込む行為や、仮想資産によって償還を受ける行為は償還する行為が、仮想資産取引サービスの提供とみなされない¹²⁴。また、SFC は 2025 年 4 月に、VATP や SFC 認可仮想資産ファンドによるステーキングサービスを一定条件下で解禁した¹²⁵。

また、トークン化分野では、SFC が仲介機関による証券トークン化を「伝統証券＋新技術」と位置付け、法的枠組み内での発行・販売・助言・運用・二次流通に関するルールを明確化した¹²⁶。2023 年から 2024 年には香港政府がグリーンボンドをトークン化し、2025 年度以降も恒常的発行を表明している¹²⁷。そのほか、2023 年 11 月に SFC は仲介業者向けのトークン化証券関連活動に関する通達（Circular on Intermediaries Engaging in Tokenised Securities-Related Activities）¹²⁸や投資商品のトークン化に関する通達（Circular on Tokenisation of SFC-Authorised Investment Products）¹²⁹を発表し、新たなリスクへの対応策を示して市場の健全かつ持続可能な発展を促した。それらの動きを踏まえ、2024 年には香港の一般投資者が売買可能な初のトークン化投資商品（投資者が実物の金の部分的な所有権を取得できるもの）を承認し、2025 年第 1 四半期にはアジア太平洋地域初となる 3 本のトークン化リテール向けマネー・マーケット・ファンド（主として香港ドル及び米ドル建てのマネー・マーケット商品に投資するもの）を認可した¹³⁰。2025

¹¹⁹ 第 12.15.2 条を参照。 https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/guideline-on-anti-money-laundering-and-counter-financing-of-terrorism-for-licensed-corporations/AML-Guideline-for-LCs-and-SFC-licensed-VASPs_Eng_1-Jun-2023.pdf

¹²⁰ <https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/licensing/doc?refNo=24EC65>,
<https://apps.sfc.hk/edistributionWeb/api/circular/openFile?lang=EN&refNo=24EC65>

¹²¹ <https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=25EC2>

¹²² <https://www.info.gov.hk/gia/general/202506/27/P2025062700385.htm?fontSize=1>

¹²³ 第 8、9 条を参照。 <https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=25EC50>

¹²⁴ 脚注 123 の第 7 条を参照。

¹²⁵ 脚注 123 の第 5 条を参照。

¹²⁶ <https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=23EC52>

¹²⁷ <https://www.info.gov.hk/gia/general/202507/30/P2025073000312.htm?fontSize=1>

¹²⁸ 脚注 126。

¹²⁹ <https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=23EC53>

¹³⁰ <https://www.info.gov.hk/gia/general/202507/30/P2025073000312.htm?fontSize=1>

年3月末時点で、これらファンドのトークン化クラスの純資産総額は9400万米ドルを超えている¹³¹。

なお、香港政府はステーブルコインに関するライセンス制度を整備し、2025年8月施行の「ステーブルコイン条例」により、発行者監督、AML、情報開示義務が課され、安全性の高い資金調達手段として活用可能となっている¹³²。

III. シンガポールにおける事案

1. 概要

歴史的に見ると、2017年から2018年にかけて投機的なICOやIEOが隆盛を極めた後、市場は規制準拠型のSTOへと構造的な転換を遂げた。この転換は、MASがトークンをその経済的機能に基づいて分類し、既存の証券先物法（Securities and Futures Act、SFA）を適用するという「技術中立性」の原則に基づいて早期に規制の枠組みを明確化したことにより、法的な実現可能性が担保されたことによる¹³³。

資金調達の促進策としては、主にSFAに基づく目論見書免除制度（私募制度）の柔軟な適用が挙げられる。特に注目すべき点は、認定投資者（Accredited Investor: AI）の純資産要件に暗号資産の価値を算入可能としたことである¹³⁴。

さらに、こうした規制環境を補完する仕組みとして、FinTech規制サンドボックス（Regulatory Sandbox）やFinancial Sector Technology & Innovation（FSTI）スキームなどの支援策が提供されている。この実際の取組については2.で紹介する。

2. 実際の取組

「金融サービス・市場法」が2016年に導入したものとして、「FinTech Regulatory Sandbox」がある¹³⁵。これは、フィンテック企業が限定的な環境と期間内で、既存の規制の一部を緩和した状態で革新的なサービスを試行できる制度である。

また、政策立案者と金融業界が共同で実施する「Project Guardian」という取組みもある¹³⁶。資産トークン化を通じて金融市場の流動性と効率性を高めるため、トークン化された債券、ファンド、ステーブルコイン、銀行負債など、多様な資産を対象とした実証実験を積極的に支援する取組みである。

この「Project Guardian」には、シンガポールの金融機関だけでなく、J.P. Morgan、Citi、UBSといった世界の主要金融機関や、日本金融庁（FSA）、英国金融行為規制機構（FCA）などの海外規制当局も参加しており、国際的な協力体制も構築されている¹³⁷。

¹³¹ https://www.sfc.hk/-/media/EN/files/COM/Annual-Report/2024-25/SFC-Annual-Report-2024-25_Eng_final.pdf 第75頁

¹³² <https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/stablecoin-issuers/>

¹³³ <https://www.pwc.ch/en/publications/2019/ch-PwC-Strategy&-ICO-Report-Summer-2019.pdf>

¹³⁴ <https://www.mas.gov.sg/regulation/capital-markets/offers-of-securities-and-securities-based-derivatives-contracts>

¹³⁵ <https://www.mas.gov.sg/development/fintech/regulatory-sandbox>

¹³⁶ <https://www.mas.gov.sg/schemes-and-initiatives/project-guardian>

¹³⁷ <https://www.fsa.go.jp/inter/etc/20230626/20230626.html>

IV. アメリカにおける事案

1. 概要

前提として、アメリカ連邦法における、暗号資産を用いた資金調達については、当該暗号資産が、証券（securities）に該当する場合には、1933年証券法等の適用があるとして、SECは、以下のIEOに対する公式警告（投資者アラート）を出しており、投資者に警戒を促している。

「The SEC's Office of Investor Education and Advocacyは、いわゆるIEOへの投資に先立ち注意喚起を行うため、本アラートを公表している。これらのオンライン取引プラットフォームは、通常、SECに登録されておらず、デューディリジェンスの実施を主張する場合もあるが、SECが承認したIEOというものは存在しない^{138,139}。IEOで発行されたトークンが有価証券である場合、当該オンライン取引プラットフォームは証券取引所としてSECに登録するか、ATS¹⁴⁰として運営する必要がある可能性がある。ATSは登録ブローカー・ディーラーでなければならず、適用要件に従う必要がある¹⁴¹。

その上で、実際に、証券に該当する暗号資産により、資金調達しようとした事案として、テレグラムによる事案がある。もっとも、以下のとおり、この事案については、必要な登録届出のない証券の販売であるとして、差止命令が発出されている。

「裁判所は、問題となる契約及び理解が、グラム（テレグラムのネイティブトークン）を二次市場に流通させるより大きなスキームの一部であることをSECが立証する高度の蓋然性を示したと認める。二次市場への転売は、必要な登録届出のない有価証券の販売の不可欠部分に当た」り¹⁴²、「テレグラムによる初期購入者へのグラムの販売は、当該購入者が法定の引受人として機能するものであり、継続する公開への分配行為の第一段階である...そして、テレグラムは証券法第4条(a)項又はRule 506(c)のいずれの登録免除の規定に該当しない」。¹⁴³

2. 実際の取組

他方で、証券に該当する暗号資産については、Regulation A+（Reg A+）による簡易な発行を行うことがありうるが、1933年証券法等に基づく証券発行規制によるものであり、株式発行の場合と異なる点は現状見受けられない。

¹³⁸ The SEC's Office of Investor Education and Advocacy is issuing this alert to urge investors to use caution before investing in so-called 'initial exchange offerings'... These online trading platforms, which are typically not registered with the SEC ... may also claim to perform due diligence... There is no such thing as an SEC-approved IEO."

<https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/initial>

¹³⁹ SECは、証券を承認又は不承認する立場の組織ではない。17 C.F.R. 230.481(b)(1)

¹⁴⁰ ATS（Alternative Trading System）とは、米国証券法に基づく「代替的取引システム」であり、証券取引所ではないものの、証券の売買を仲介する電子的な取引プラットフォームを指す。

¹⁴¹ If the IEO involves securities, the online trading platform may need to register with the SEC as a national securities exchange or operate as an ATS... An ATS must be a registered broker-dealer and comply with applicable requirements...

¹⁴² The Court finds that the SEC has shown a substantial likelihood of success in proving that the contracts and understandings at issue... are part of a larger scheme to distribute those Grams into a secondary public market... the resale of Grams into the secondary public market would be an integral part of the sale of securities without a required registration statement.

¹⁴³ Telegram's sale of Grams to the Initial Purchasers, who will function as statutory underwriters, is the first step in an ongoing public distribution of securities and... Telegram cannot receive the benefit of an exemption from the registration requirement under either section 4(a) or Rule 506(c).

このようなReg A+による簡易な発行事例としては、Blockstackによる発行事例¹⁴⁴、YouBow, Inc.による発行事例¹⁴⁵がある。

また、証券に該当する暗号資産のICOについては、株式発行と同様に、Regulation D (Reg D) 等の適用ある登録免除に厳格に適合することで私募スキームを用いた発行自体は法令上可能である¹⁴⁶。もっとも、CLARITY 法案において、デジタル商品に関する提供及び販売に関する規定等があるため、法案の審議状況も含め、注視が必要と考える。

第6.まとめ

本報告書では、欧州（EU）、アメリカ、アジアの暗号資産に関する制度を調査対象として、各国当局による公表資料を中心とした文献調査及び当局担当者へのヒアリングにより得られた情報を整理した。これらの情報を基に、日本における暗号資産規制に対しては、次の点が示唆的であるといえる。

我が国における暗号資産に関する規制を議論するにあたり、諸外国の現状の制度を参照することも想定されるところ、本報告書がその一助となれば、幸いである。

1. 暗号資産のホワイトペーパーの公表に関する規制

MiCA においては、「その他暗号資産」についても、一定の免除規定が適用される場合を除き、暗号資産の公衆への提供又は上場の実施に際して、ホワイトペーパーにおいて情報提供が義務付けられている。当該情報は、特にその他暗号資産については、調達した資金を用いて実施が企図されているプロジェクトに関する情報が含まれており、その他、公衆への提供者や発行者に関する情報、リスク要因、コンセンサスメカニズムが気候や環境等に及ぼす悪影響等に関する情報が含まれている。これらの情報の開示を義務付けることで、その他暗号資産の公衆への提供、上場等の段階におけるモラルハザードの発生を一定程度回避可能なものと思われる。

また、ホワイトペーパーの公表義務は、発行者規制に関する整理との観点でも重要である。MiCA においても目論見書規制の内容も念頭に整理をされており、従来の金融商品規制の内容を踏襲しようとする部分もありつつも、例えばビットコインなどの発行者に対する開示規制対応を求めることが難しい場合については、CASP を介した適切な情報開示を求めている。このように、どの組織に対する規制がないとも思われる完全に分散化された暗号資産サービスと異なり、ビットコインなどの最も分散化された場合であっても発行者の特定できない(no identifiable issuer) 暗号資産についての CASP 等を介した規制を実現し、もって取引の安全を図っていることは注目に値すると思われる。

¹⁴⁴ https://www.sec.gov/Archives/edgar/data/1693656/000110465919039908/a18-15736_1253g2.htm

¹⁴⁵ <https://www.sec.gov/Archives/edgar/data/1725129/000162827919000262/younow253g2.htm>

¹⁴⁶ SEC は「米国で提供・売付けられるすべての証券は、登録されるか、登録免除に適合しなければならない」と明記している。SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities (<https://www.sec.gov/newsroom/press-releases/2017-131>) において公表された Investigation Report (<https://www.sec.gov/files/litigation/investreport/34-81207.pdf>) において DAO Token を証券 (security) と認定したうえで、「All securities offered and sold in the United States must be registered with the Commission or must qualify for an exemption from the registration requirements.」と言及している。実際に Reg D により販売された例として ASPEN COIN が挙げられる。(<https://www.aspencoin.io/>)

2. 暗号資産に関するインサイダー取引規制及び相場操縦規制

MiCA においては、ステーブルコインを含む暗号資産について相場操縦規制及びインサイダー取引規制を定めている。これらの行為規制は、MiFID II における不公正行為規制のすべてを適用するのではなく、暗号資産取引の信頼性確保のために必要なものに限定して適用するという姿勢が反映されたものである（前文(95)¹⁴⁷）。規制の実効性を担保するためには、行為規制の対象となる者の事業規模等を勘案しつつ、投資者保護・市場の透明性・公平性確保と規制の実現可能性のバランスを考慮することが重要であるといえる。

MiCA における従業員等によるフロントランニングの禁止や、MEV において内部者情報利用や相場操縦に当たり得る整理が進められていることも、不公正取引規制の実質かとしては意義があると思われる。また、市場濫用行為を検知することは非常に困難であるとのマルタ当局等の経験は、制度を検討するにあたっては、実効性を保つための制度整備としてどのような執行措置も念頭においた整理が重要となることを示唆しているとも考えられる。

3. 暗号資産交換業等による規制の範囲の示唆

MiCA においては、暗号資産と法定通貨の交換や暗号資産間の交換や顧客の代理のみならず、取引プラットフォームの運営、保管及び管理（カストディ）、助言提供、ポートフォリオ管理なども規制の対象としていることがわかる。典型的な暗号資産の交換行為だけではなく、暗号資産交換業に関する様々な行為のリスクにも着目しており、カストディや取引に関与する行為も規制対象とすることで、不用意に規制の抜け道になってしまうような場合や、安易に DeFi が規制対象外とならないように工夫を行っていると考えられる。他方で、我が国においては、暗号資産交換業の媒介行為等に着目したライセンスの新設等も行っているところ、今後は規制の適用範囲だけでなく、各行為のリスクに応じた規制を行っていくことも重要と考える。

他方で、欧州においては、MiCA の規制対象外の分野（発行者の特定できない暗号資産、完全に分散化された方法で提供される暗号資産）や MiCA の規制範囲であるものの該当する行為が直接規制されていない分野（暗号資産の貸付、借入、ステーキング等）により生じるリスクについても引き続き活発な議論が行われている¹⁴⁸。このように、MiCA の適用範囲に関する継続的な議論についても引き続きフォローすることが必要と考えられる。

¹⁴⁷ It is important to ensure confidence in markets in crypto-assets and the integrity of those markets. It is therefore necessary to lay down rules to deter market abuse for crypto-assets that are admitted to trading. However, as issuers of crypto-assets and crypto-asset service providers are very often SMEs, it would be disproportionate to apply all of the provisions of Regulation (EU) No 596/2014 of the European Parliament and of the Council to them. It is therefore necessary to lay down specific rules prohibiting certain behaviours that are likely to undermine user confidence in markets in crypto-assets and the integrity of those markets, including insider dealing, unlawful disclosure of inside information and market manipulation related to crypto-assets.

¹⁴⁸ The EBA and ESMA will continue monitoring the relevance of DeFi in EU markets as part of wider innovation monitoring initiatives which help inform assessments of opportunities and risks, and any potential supervisory or regulatory actions. https://www.esma.europa.eu/sites/default/files/2025-01/EBA-ESMA_DeFi_factsheet.pdf

4. 我が国の暗号資産に関する規制への示唆

我が国においても今後、IEO による資金調達が発達する可能性がある。このような取引の実施に際しては、市場の透明性・公平性担保、投資者保護のための情報開示が必要である一方、あまりに厳しい規制を導入することによって IEO のような新規のマーケットの活性化が阻害されるというデメリットについても考慮する必要がある。この点についての MiCA のバランスの取り方については、示唆的であり、日本における制度導入においても参照されるべきものと考えられる。

以上

【別表】

	MiCA ¹	ドイツ	フランス	マルタ
当局の 権限 (抜粋)	主管当局は、国内法に従い、少なくとも以下の監督上および調査上の権限を有するものとする。(MiCA 第 94 条) ・情報及び書類の提出を求める ・違反が疑われる場合に暗号資産サービスの提供停止を命ずる ・違反が認められる場合に暗号資産サービスの提供を禁止する ・暗号資産サービスの提供に影響を及ぼし得るすべての重要な情報の開示を命ずる	MiCA の違反に関しては、BaFin ² が監督・調査権限を有する(KMAG ³ 第 3 条第 1 項)。 ・違反が疑われる場合等、暗号資産サービス提供を禁止することができる(KMAG 第 29 条) ・違反した場合等に、認可の取り消しをすることができる(KMAG 第 12 条) ・暗号資産サービスの提供に影響を及ぼし得るすべての重要な情報の開示を求めることができる(KMAG 第 30 条) ・広告に関して違反が疑われる場合には、その内容の変更を求めるほか、広告の停止又は禁止を命ずることができる(KMAG 第 17 条)	AMF ⁴ は、その他の暗号資産(資産参照型トークン及び電子マネートークン以外の暗号資産)に関して以下のような権限を有する(CMF ⁵ 第 621 の 7 の 3 条)。 ・MiCA 違反が疑われる場合には、連続 30 営業日を上限として、広告の中止又は停止を命ずることができる。 ・広告が MiCA 第 7 条の要件を満たさない場合には、その変更を求めることができる。 ・提供者又は上場申請者に対し、MiCA 遵守を確保するために必要なあらゆる措置を講ずることができ、MiCA に反すると AMF が考える実務又は行為の中止を求めることができる。	MiCA の違反に関しては、MFSA ⁶ が、例えば、以下のような監督・調査・行政制裁権限を有する。 ・MiCA に違反した疑いのある合理的な根拠がある場合、広告を停止又は禁止することができる(MiCA Act ⁷ 第 43 条第 1 項第 o 号)。 ・MiCA に違反した場合等に、違反行為の中止命令、公表声明、行政制裁金賦課、認可停止・取消し、経営機能禁止等を行うことができる(MiCA Act 第 46 条)。 ・問題のある暗号資産又は活動・実務について、禁止又は制限措置を講ずることができる(MiCA Act 第 45 条)。
公衆への 提供	・ホワイトペーパーを作成、公表の 20 営業日前までに所管官庁へ通知(MiCA 第 4 条、第 5 条、第 8 条) ※資産参照型トークンを除き事前承認不要。 ・相手が少数人や適格機関投資家の場合/既存の製品・サービスや稼働中の商品・サービスへのアクセス権として付与される場合は免除あり(MiCA 第 4 条) ・コンセンサスアルゴリズム等の技術的な要件等の記載が必要(MiCA 第 6 条)	公衆への提供に関して、BaFin は発行者に対して以下のような監督・調査権限を有する。 ・違反が疑われる場合に、公募や取引許可の停止を命ずることができる(KMAG 第 15 条第 1 項)。 ・資産参照型トークンが承認済みのホワイトペーパーなしに公衆へ提供される場合、公募の禁止(KMAG 第 15 条第 2 項)。 ・MiCA 又は KMAG 違反があった場合、又は違反の疑いがある場合に、公募又は取引許可を禁止することができる(KMAG 第 15 条第 3 項)。 ・ホワイトペーパー又は修正版ホワイトペーパーが法定記載事項を欠き、又は法定様式に適合しない場合、その変更を求めることができる(KMAG 第 16 条)。 ・投資者保護又は市場の円滑な機能確保のため、公衆へ提供される暗号資産の評価に影響し得る重要情報を公表することができる(KMAG 第 18 条)。	公衆への提供に関して、AMF は、その他暗号資産の発行者又は上場申請者に対して、以下のような監督・調査権限を有する。 ・CMF は、MiCA が適用されるその他暗号資産の公衆への提供及び取引プラットフォーム上場を国内法上明確に位置付け、これらの行為が MiCA の規律に服することを明示している(CMF 第 552 の 1 条)。 ・暗号資産の公衆への提供や上場に際し、MiCA 第 8 条に基づくホワイトペーパーの通知先は AMF であることを明示している(CMF 第 552 の 2 条)。 ・違反が疑われる場合には、公衆への提供又は上場申請に係るオペレーション全体の停止を命ずることができる(CMF 第 621 の 7 の 3 条)。 ・MiCA 違反があった場合、又は違反が生ずる合理的疑いがある場合には、公衆への提供又は上場申請を禁止することができる(CMF 第 621 の 7 の 3 条)。 ・ホワイトペーパー又は修正版ホワイトペーパーが MiCA 第 6 条所定の記載事項を欠く場合には、その変更を求めることができる(CMF 第 621 の 7 の 3 条)。 ・金融の安定又は暗号資産保有者、特に個人保有者の保護のために必要な場合には、ホワイトペーパーへの追加情報の記載を求めることができる(CMF 第 621 の 7 の 3 条)。 ・投資者保護のため、公衆へ提供され、又は取引に付される暗号資産の評価に影響し得る重要情報を公表し、又はその公表を求めることができる(CMF 第 621 の 7 の 3 条)。	公衆への提供に関して、MFSA が、発行者又は上場申請者に対して、例えば、以下のような監督・調査・行政制裁権限を有する。 ・暗号資産の公衆への提供や上場に際し、ホワイトペーパーの通知先が MFSA であることを明示している(MiCA Act 第 6 条)。 ・違反が疑われる場合、公衆への提供又は上場を最大 30 営業日停止することができる(MiCA Act 第 43 条第 1 項第 k 号)。 ・ホワイトペーパー通知なしの提供等が疑われる場合、事前警告なく即時停止を命ずることができる(MiCA Act 第 43 条第 1 項第 t 号)。 ・MiCA 等に違反した場合又は合理的疑いがある場合、公衆への提供又は上場を禁止することができる(MiCA Act 第 43 条第 1 項第 l 号)。 ・MFSA は、ホワイトペーパー又は修正版ホワイトペーパーが法定記載事項を欠く場合、その変更を求めることができる(MiCA Act 第 43 条第 1 項第 h 号)。 ・重要情報の開示を求めることができる(MiCA Act 第 43 条第 1 項第 r 号)。

¹ Markets in Crypto-Assets Regulation
² Bundesanstalt für Finanzdienstleistungsaufsicht ドイツ連邦金融監督庁
³ Kryptomärkteaufsichtsgesetz 暗号資産市場監督法 <https://www.gesetze-im-internet.de/kmag/>
⁴ Autorité des marchés financiers フランス金融市場庁
⁵ Code monétaire et financier 金融通貨法典 https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006072026/2025-02-23/
⁶ Malta Financial Services Authority マルタ金融サービス庁
⁷ Markets in Crypto-Assets Act 暗号資産市場法 <https://www.mfsa.mt/wp-content/uploads/2025/03/MiCA-Rulebook.pdf>

	MiCA ¹	ドイツ	フランス	マルタ
CASP ⁸ への規制	・暗号資産サービスを提供するためには CASP としての認可を当局から受ける必要がある。（MiCA 第 59 条） ・CASP は共通して以下が課される。 健全性要件、ガバナンス体制、主管当局への報告義務、顧客の暗号資産及び資金の保管、利益相反防止義務、外部委託に関する義務等（MiCA 第 59 条～第 74 条） ・CASP は提供する暗号資産サービスの種類ごとに追加で義務が課される。例えば、カストディサービスを提供する CASP は追加で暗号資産の分別管理義務等が課される。（MiCA 第 75 条～第 79 条）	・暗号資産サービスを提供するためには、BaFin による CASP としての認可を受ける必要がある（KMAG 第 2 条第 4 項第 3 号、第 9 条第 1 項第 3 号、第 11 条、第 14 条第 1 項、MiCA 第 59 条第 1 項 a））。CASP には、MiCA に基づき一定の義務が課されており、KMAG はこれらの義務の遵守について、BaFin による監督・調査・執行の仕組みを定めている。 ・BaFin は、CASP に対して業務事項に関する情報、書類およびデータの提出を求めることができる（KMAG 第 20 条第 1 項）。 ・特別の理由がなくても、CASP およびその外部委託先企業に対し立入検査を実施することができる（KMAG 第 20 条第 2 項）。 ・CASP に対して、健全性要件、所在地移転、クロスボーダー業務の開始・終了、重要な外部委託、支店設置等についての届出を求めることができる（KMAG 第 21 条第 1 項）。 ・CASP は、各四半期終了後に財務状況に関する情報をドイツ連邦銀行に提出しなければならない（KMAG 第 21 条第 4 項）。 ・BaFin およびドイツ連邦銀行は、経済状況、適正な業務運営、経営機関の能力等についてより深い把握が必要な場合には、追加的な届出義務・報告義務を課することができる（KMAG 第 21 条第 5 項）。 ・BaFin は、顧客又は暗号資産保有者の利益に重大な損害が生じることを防止するため、ウェブ上のコンテンツ削除、アクセス遮断、警告表示、ドメイン名削除等を命ずることができる（KMAG 第 4 条第 7 項）。	暗号資産サービスを提供するためには、AMF による CASP としての認可を受ける必要がある。CASP には、MiCA に基づき一定の義務が課されており、フランス法はこれらの義務の遵守について、AMF による監督・執行の仕組みを定めている。 ・AMF は、MiCA に基づく CASP の認可申請先であり、AMF 自身も、2024 年 12 月 30 日以降、暗号資産サービスは原則として事前に認可を受けた CASP のみが提供できると説明している。 ・CMF は、CASP を含む暗号資産サービス提供者に対して適用されるルールを AMF 一般規則で定める枠組みを置いている（CMF 第 621 の 7 条）。 ・フランス国内法上、一定の暗号資産サービス提供者には、顧客との契約締結、保管方針の策定、顧客資産の返還体制、顧客資産と自己資産の分別、顧客資産の無断利用禁止等の義務が課されている。少なくともカストディ型サービスについて、これらの義務が国内法上明記されている（CMF 第 54 の 10 の 5 条）。 ・AMF は、違反がある場合には、違反行為の中止命令、公表措置及び制裁手続の開始を行うことができる（CMF 第 621 の 15 条）。	暗号資産サービスを提供するためには、原則として、MFSA による CASP としての認可を受ける必要がある（MiCA Act 第 26 条第 1 項）。 CASP には、MiCA に基づき一定の義務が課されており、マルタでは、以下のような MFSA による監督・執行の仕組みを定めている。 ・CASP が MiCA、MiCA Act、その下位規則又はルールに違反した場合、又はこれらに関する義務・条件・命令に違反した場合には、MFSA は行政罰及びその他の行政措置を科すことができる（MiCA Act 第 46 条第 1 項）。また、調査・検査・要求への不協力も制裁対象となる（同条第 1 項第 b 号、第 2 項第 g 号）。 ・CASP に関する MiCA 違反について、MFSA は行政制裁を科すことができる（MiCA Act 第 46 条第 2 項第 d 号）。 ・違反がある場合、MFSA は、違反行為の中止及び再発防止命令を発することができる（MiCA Act 第 46 条第 3 項第 b 号）。 ・CASP 関係の違反については、MFSA は、CASP の経営機関の構成員その他責任ある自然人に対して、CASP における経営機能の行使を一時的に禁止することができる（MiCA Act 第 46 条第 3 項第 f 号）。 ・顧客又は暗号資産保有者に重大な損害が生ずる危険を回避するため、他に有効な手段がない場合には、MFSA はオンライン・インターフェース上のコンテンツ削除、アクセス制限、警告表示等を含む措置を命ずることができる（MiCA Act 第 43 条第 1 項第 y 号）
不公正取引規制	不公正取引については MiCA 第 86 条から第 92 条に定めがある。 ・インサイダー取引の禁止（MiCA 第 89 条） ・相場操縦の禁止（MiCA 第 91 条）	不公正取引規制に関して、BaFin は、暗号資産の発行者、申請者、提供者、CASP その他の関係者に対して、以下のような監督・調査・行政制裁を行う権限を有する。 ・BaFin は、MiCA Title VI 違反を追及するため、情報・書類・データ提出要求、召喚・聴取、搜索、証拠確保、通信データ取得等を行うことができる（KMAG 第 31 条）。 ・虚偽又は誤解を招く情報への訂正命令、インサイダー情報の公表代行等を行うことができる（KMAG 第 35 条、第 36 条）。 ・自然人については、相場操縦等は 500 万ユーロ以下、インサイダー情報公表義務違反等は 100 万ユーロ以下の制裁金を課することができる（KMAG 第 47 条第 5 項）。 ・法人については、相場操縦等は 1500 万ユーロ以下、又は場合によっては売上高割合基準、インサイダー情報公表義務違反等は 250 万ユーロ以下又は売上高割合基準として、制裁金を課することができる（KMAG 第 47 条第 6 項、第 7 項）。 ・重大違反については刑事罰の対象にもなり、インサイダー取引、違法推奨・誘引、違法開示、相場操縦の一定の場合が該当する（KMAG 第 46 条）	不公正取引規制に関して、AMF は以下のような監督・調査・制裁権限を有する。 ・AMF が調査・検査報告に基づき制裁手続を開始し、関係者に対して違反事実を通知し、制裁委員会に付託する枠組みを定めている。MiCA 違反についても、この国内制裁手続の枠組みに乗る（CMF 第 621 の 15 条）。 ・AMF は、MiCA 違反について、公表措置、違反行為の中止命令及び制裁を行う国内法上の基礎を有している（CMF 第 621 の 15 条、第 621 の 7 の 3）。 ・MiCA 違反に対する制裁として、法人に対して、最大 1 億ユーロ又は不法に得た利益が特定可能な場合はその 10 倍を上限とする制裁金を課することができる（CMF 第 621 の 15 条）。もっとも、不公正取引規制に違反した場合の制裁については、年間総売上高の 15%まで上限が引き上げることができる（同条）。 ・自然人については、MiCA 違反に対し、原則として 1500 万ユーロ以下又は違反により得た利益の 10 倍以下の制裁金を課することができる（CMF 第 L621-15 条 III）。 ・重大違反については刑事罰の対象にもなり、インサイダー取引については CMF 第 L465-1 条、相場操縦・虚偽又は誤解を招く情報の流布については CMF 第 L465-3-2 条が適用される。	不公正取引規制に関しては、MFSA が、以下のような監督・調査・制裁権限を有する。 ・MiCA Act 第 46 条は、MiCA 違反に対する行政罰及びその他行政措置の枠組みを定めており、不公正取引では MiCA 第 88 条違反及び MiCA Act 第 35 条違反、並びに MiCA 第 89 条から第 92 条まで違反及び MiCA Act 第 36 条違反が明示的に制裁対象となる。 ・自然人に対しては、インサイダー情報公表義務違反等について 100 万ユーロ以下、インサイダー取引・相場操縦等について 500 万ユーロ以下の行政制裁金を課することができる（MiCA Act 第 46 条第 3 項第 d 号(ii)、(iii)）。 ・法人に対しては、インサイダー情報公表義務違反等について 250 万ユーロ又は年次売上高の 2%、インサイダー取引・相場操縦等について 1500 万ユーロ又は年次売上高の 15%のいずれか高い額までの行政制裁金を課することができる（MiCA Act 第 46 条第 3 項第 e 号(v)、(vi)）。 ・利得吐出命令、CASP 認可の停止・取消し、経営機能禁止、自己勘定取引禁止等を課することができる（MiCA Act 第 46 条第 3 項第 g 号）。 ・なお、同一行為について MFSA が行政罰又はその他行政措置を課した場合、その刑事犯罪については手続を開始又は継続できないとされており、二重追及排除の仕組みが置かれている（MiCA Act 第 46 条第 8 項）。

※なお、本報告書における原文の訳は、いずれも渥美坂井法律事務所・外国法共同事業による仮訳である。

⁸ Crypto-Asset Service Provider