主要行等向けの総合的な監督指針　新旧対照表

現　行	改 正 案
【本編】	【本編】
Ⅴ　銀行グループに対する連結ベースの監督等	Ⅴ　銀行グループに対する連結ベースの監督等
Ⅴ－１　基本的な考え方	Ⅴ－１　基本的な考え方
Ⅴ－２　アームズ・レングス・ルール	Ⅴ－２　アームズ・レングス・ルール
Ⅴ－３　銀行及びグループ会社の業務範囲等	Ⅴ－３　銀行及びグループ会社の業務範囲等
Ⅴ－４　銀行主要株主	Ⅴ－４　銀行主要株主
Ⅴ－５　顧客の利益の保護のための体制整備	Ⅴ－５　顧客の利益の保護のための体制整備
（新設）	Ⅴ－６　暗号資産に関する留意事項
	Ⅴ－６－１　意義
	暗号資産の設計・仕様は様々であるところ、移転記録が公開されず、取引の追跡困難な暗号資産が存在する等、テロ資金供与やマネー・ローンダリングに利用されるリスクが高いものも存在する。また、一般的に、暗号資産は、その価値の裏付けとなる資産等がないため本源的な価値を観念し難く、価格の変動が大きいことを踏まえると、銀行グループが暗号資産を保有する際にはその価格変動リスクについての検討が必要となる。加えて、暗号資産の管理については、システムの誤作動やサイバー攻撃などのシステムリスクも存在する。 以上のほか、これらのリスクが顕在化した場合のレピュテーショナル・リスク等も考慮すれば、銀行グループによる暗号資産の取得は必要最小限度の範囲とする必要があり、かつ、銀行グループの業務において、暗号資産の取得、保有又は処分等（暗号資産を実質的な投資対象とするファンドに対する出資等の間接的な方法によるものを含む。以下「暗号資産の取得等」という。）が生じる場合には、銀行の固有業務の運営への支障や銀行グループとして重大な損害等が生じるおそれがないよう、十分な態勢整備が行われている必要がある。
	Ⅴ－６－２　主な着眼点

	銀行グループにおける暗号資産の取得等については、上述のとおり、銀行法施行規則第 13 条の6の9及び同条の6の 10 に基づく態勢整備がなされている必要がある。かかる態勢整備について、具体的には、以下の点に留意する必要がある。 ① 暗号資産の特性等を踏まえたリスクの特定・評価・低減 暗号資産の仕組み（発行者、管理者その他の関係者や当該暗号資産と密接に関連するプロジェクトの内容等を含む。）、想定される用途、流通状況及び当該暗号資産に使用される技術その他当該暗号資産の特性（以下「暗号資産の特性等」という。）等を踏まえ、暗号資産のリスクの特定・評価について十分な検討が行われ、以下の②から④の措置を含め、当該リスクを適切に低減するための内部管理態勢が整備されているか。また、これらについて定期的な検証及び見直しが実施されているか。 ② テロ資金供与及びマネー・ローンダリングへの対応 テロ資金供与及びマネー・ローンダリングに利用されるおそれが高い場合においては、暗号資産の取得等の適否を慎重に判断することとしているか。例えば、移転記録の追跡が著しく困難である暗号資産については、テロ資金供与及びマネー・ローンダリングに利用されるおそれが特に高いことから、暗号資産の取得等を行うことがないよう留意する。 また、暗号資産の取得等の相手方のテロ資金供与及びマネー・ローンダリング対策の状況等にも留意するなど、マネロン・テロ資金供与対策ガイドライン記載の措置に沿った対策が適切に講じられているか。特に、暗号資産の取得等に関して、海外に居住若しくは所在する者から又はこれらの者への暗号資産の移転を伴う可能性がある場合には、Ⅲ－３－１－３－１－２（４）に準じた対策が適切に講じられているか。 ③ 財務の健全性確保を図るための措置 銀行グループの業務において暗号資産の取得が必要となる場合であっても、健全性の確保の観点から、取得する暗号資産の量については当該業務のために必要最小限度の範囲とする等、適切な方針が定められているか。また、暗号資産の保有についても、当該暗号資産の市場リスク、流動性リスク等を考慮の上で、速やかに売却する等により適切な処分を図ることが可能な態勢となっているか。

	なお、銀行グループにおいては、投資の目的をもってする暗号資産の取得等を行わないこととしているか。 ④　暗号資産の取得等に係る安全管理措置 ・　暗号資産の管理を担当する部署及び責任者を明確にしているか（複数の部署で暗号資産の管理を担当する場合には、部署間の担当と責任が明確になっているか。）。また、取り扱う暗号資産の特性等に関して十分な知識・経験を有する者を配置しているか。 ・　暗号資産の管理、流出時の対応その他暗号資産に係る内部規程を適切に整備し、役職員に対する周知、徹底を図っているか。また、当該内部規程について、定期的な検証及び見直しが行われているか。 ・　不正アクセス等による暗号資産の流出の防止のための対策等、取り扱う暗号資産の管理に関するシステムリスク管理態勢が十分に構築されているか。また、当該システムリスク管理態勢について、専門家による定期的な検証及び見直しが行われているか。