事務ガイドライン（第三分冊：金融会社関係　16　暗号資産交換業者関係）　新旧対照表（案）

改正案	現行
Ⅱ　暗号資産交換業者の監督上の着眼点	Ⅱ　暗号資産交換業者の監督上の着眼点
Ⅱ－２　業務の適切性等	Ⅱ－２　業務の適切性等
Ⅱ－２－２　利用者保護のための情報提供・相談機能等	Ⅱ－２－２　利用者保護のための情報提供・相談機能等
Ⅱ－２－２－４　暗号資産の流出リスクへの対応	Ⅱ－２－２－４　暗号資産の流出リスクへの対応
Ⅱ－２－２－４－２　主な着眼点	Ⅱ－２－２－４－２　主な着眼点
(1)　（略）	(1)　（略）
(2)　流出リスクの特定・評価	(2)　流出リスクの特定・評価
①　取り扱う暗号資産の種類ごとに、当該暗号資産の流出リスクを特定・評価しているか。	①　取り扱う暗号資産の種類ごとに、当該暗号資産の流出リスクを特定・評価しているか。
（注）流出リスクの特定・評価に際しては、「金融分野におけるサイバーセキュリティに関するガイドライン」や、協会及び専門的知見を有する関係団体等におけるセキュリティ対策に係る指針等も参考とする必要があることに留意する。	（注）流出リスクの特定・評価に際しては、協会や専門的知見を有する関係団体等におけるセキュリティ対策に係る指針等も参考とする必要があることに留意する
②～④　（略）	②～④　（略）
(3)　流出リスクの低減	(3)　流出リスクの低減
①　（略）	①　（略）
②　上記①のほか、流出リスクの低減に際しては、流出の態様の変化や技術の進歩等を踏まえつつ、「金融分野におけるサイバーセキュリティに関するガイドライン」や、協会及び専門的知見を有する関係団体等におけるセキュリティ対策に係る指針等も参考とする必要があるが、例えば、以下の点を含め、上記(2)で特定・評価された流出リスクに対して有効な低減措置を講じているか。	②　上記①のほか、流出リスクの低減に際しては、流出の態様の変化や技術の進歩等を踏まえつつ、協会や専門的知見を有する関係団体等におけるセキュリティ対策に係る指針等も参考とする必要があるが、例えば、以下の点を含め、上記(2)で特定・評価された流出リスクに対して有効な低減措置を講じているか。

改正案	現行
イ．対象暗号資産を移転する場合には、あらかじめ社内規則等で定められた手続に従い、複数の担当者が関与する体制となっているか。	イ．対象暗号資産を移転する場合には、あらかじめ社内規則等で定められた手続に従い、複数の担当者が関与する体制となっているか。
ロ．権限者以外の者が使用（署名）できない方法で秘密鍵等を管理しているか。特にハードウェアや紙等の物理媒体で秘密鍵等を管理する場合には、施錠されたセキュリティルーム、金庫など権限者以外の者がアクセスすることができない環境で保管しているか。	ロ．権限者以外の者が使用（署名）できない方法で秘密鍵等を管理しているか。特にハードウェアや紙等の物理媒体で秘密鍵等を管理する場合には、施錠されたセキュリティルーム、金庫など権限者以外の者がアクセスすることができない環境で保管しているか。
ハ．対象暗号資産の移転について、複数の秘密鍵等を用いた電子署名を必要とする等の適切な措置を講じているか。複数の秘密鍵等を用いる場合には、各秘密鍵等の保管場所を分けて管理しているか。	ハ．対象暗号資産の移転について、複数の秘密鍵等を用いた電子署名を必要とする等の適切な措置を講じているか。複数の秘密鍵等を用いる場合には、各秘密鍵等の保管場所を分けて管理しているか。
ニ．対象暗号資産の移転に際して、当該対象暗号資産の移転に係る取引内容が真正であることを確認しているか。	ニ．対象暗号資産の移転に際して、当該対象暗号資産の移転に係る取引内容が真正であることを確認しているか。
ホ．利用者からの依頼によって対象暗号資産が自動的に外部に移転する仕組みを用いる場合には、一回又は短時間に移転できる対象暗号資産の上限を設定しているか。	ホ．利用者からの依頼によって対象暗号資産が自動的に外部に移転する仕組みを用いる場合には、一回又は短時間に移転できる対象暗号資産の上限を設定しているか。
ヘ．秘密鍵等が紛失した場合に備え、バックアップを作成しているか。バックアップについても、Ⅱ－２－２－３－２⑶⑤及び⑥並びに上記ロに基づいて安全に管理しているか。	ヘ．秘密鍵等が紛失した場合に備え、バックアップを作成しているか。バックアップについても、Ⅱ－２－２－３－２⑶⑤及び⑥並びに上記ロに基づいて安全に管理しているか。
ト．対象暗号資産の移転の手続について内部監査の対象としているか。	ト．対象暗号資産の移転の手続について内部監査の対象としているか。
Ⅱ－２－３　事務運営	Ⅱ－２－３　事務運営
Ⅱ－２－３－１　システムリスク管理	Ⅱ－２－３－１　システムリスク管理

改正案	現行
Ⅱ－２－３－１－１　意義 システムリスクとは、コンピュータシステムのダウン又は誤作動等のシステムの不備等に伴い利用者や暗号資産交換業者が損失を被るリスクや、コンピュータが不正に使用されることにより利用者や暗号資産交換業者が損失を被るリスクをいう。暗号資産交換業者はその業務の性質上、インターネットを前提とする高度・複雑な情報システムを有していることが多く、また、暗号資産はブロックチェーン等に電子的に記録されネットワークで移転できる財産的価値であるため、日々手口が高度化するサイバー攻撃により重要情報に対する不正アクセス、漏えい等のリスクが顕在化している。このため、定期的なリスク評価に加え、外部環境の変化や事故・事件を把握し、自社システムへの影響有無等、適時のリスク評価が必要である。特に、外部サービス（クラウド等）の利用が多いことから、外部委託管理態勢の整備が重要となっている。システムが安全かつ安定的に稼動することは資金決済システム及び暗号資産交換業者に対する信頼性を確保するための大前提であり、システム開発・運用の基本事項を確行するとともに、システムリスク管理態勢全体の充実強化は極めて重要である。このためには、経営資源の確保が必要であり、IT 戦略の策定など経営陣が主体となった取り組みが求められる。 こうした観点から、経営者がリーダーシップを発揮し、IT と経営戦略を連携させ、企業価値の創出を実現するための仕組みである「IT ガバナンス」を適切に機能させることが極めて重要である。	Ⅱ－２－３－１－１　意義 システムリスクとは、コンピュータシステムのダウン又は誤作動等のシステムの不備等に伴い利用者や暗号資産交換業者が損失を被るリスクや、コンピュータが不正に使用されることにより利用者や暗号資産交換業者が損失を被るリスクをいう。暗号資産交換業者はその業務の性質上、インターネットを前提とする高度・複雑な情報システムを有していることが多く、また、暗号資産はブロックチェーン等に電子的に記録されネットワークで移転できる財産的価値であるため、日々手口が高度化するサイバー攻撃により重要情報に対する不正アクセス、漏えい等のリスクが顕在化している。このため、定期的なリスク評価に加え、外部環境の変化や事故・事件を把握し、自社システムへの影響有無等、適時のリスク評価が必要である。特に、外部サービス（クラウド等）の利用が多いことから、外部委託管理態勢の整備が重要となっている。システムが安全かつ安定的に稼動することは資金決済システム及び暗号資産交換業者に対する信頼性を確保するための大前提であり、システム開発・運用の基本事項を確行するとともに、システムリスク管理態勢全体の充実強化は極めて重要である。このためには、経営資源の確保が必要であり、IT 戦略の策定など経営陣が主体となった取り組みが求められる。 こうした観点から、経営者がリーダーシップを発揮し、IT と経営戦略を連携させ、企業価値の創出を実現するための仕組みである「IT ガバナンス」を適切に機能させることが極めて重要である。

改正案	現行
（参考）金融機関のITガバナンスに関する対話のための論点・プラクティスの整理第２版（令和５年６月） なお、以下の各着眼点に記述されている字義どおりの対応が暗号資産交換業者においてなされていない場合にあっても、当該暗号資産交換業者の規模、特性からみて、利用者保護の観点から、特段の問題がないと認められれば、不適切とするものではない。	（参考）金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理（令和元年６月） なお、以下の各着眼点に記述されている字義どおりの対応が暗号資産交換業者においてなされていない場合にあっても、当該暗号資産交換業者の規模、特性からみて、利用者保護の観点から、特段の問題がないと認められれば、不適切とするものではない。
Ⅱ－２－３－１－２　主な着眼点 (1)～　(4)（略） (5)　サイバーセキュリティ管理 ①　取締役会等は、サイバーセキュリティの重要性を認識し、「金融分野におけるサイバーセキュリティに関するガイドライン」を踏まえ、必要な態勢を整備しているか。	Ⅱ－２－３－１－２　主な着眼点 (1)～　(4)（略） (5)　サイバーセキュリティ管理 ①　サイバーセキュリティについて、取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。
（削除）	②　サイバーセキュリティについて、組織体制の整備、社内規程の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。 ・　サイバー攻撃に対するモニタリング体制 ・　サイバー攻撃を受けた際の報告及び広報体制 ・　組織内 CSIRT（Computer Security Incident Response Team）等の緊急時対応及び早期警戒のための体制 ・　情報共有機関等を通じた情報収集・共有体制　等
（削除）	③　サイバー攻撃に備え、リスクベースで入口対策、内部対策、出口対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じているか。

改正案	現行
	・　入口対策（例えば、ファイアウォールの設置、抗ウィルスソフトの導入、不正侵入検知システム・不正侵入防止システムの導入等）
	・　内部対策（例えば、特権 ID・パスワードの適切な管理、不要な ID の削除、特定コマンドの実行監視、本番システム（サーバー間）のセキュア化（パケットフィルタや通信の暗号化）、開発環境（テスト環境含む。）と本番システム環境のネットワーク分離、利用目的に応じたネットワークセグメント分離　等）
	・　出口対策（例えば、通信ログ・イベントログ等の取得と分析、不適切な通信の検知・遮断　等）
②　（略）	④　サイバー攻撃を受けた場合に被害の拡大を防止するために、以下のような措置を速やかに実施する態勢を整備しているか。 ・　攻撃元の IP アドレスの特定と遮断 ・　DDoS 攻撃に対して自動的にアクセスを分散させる ・　システムの全部又は一部の一時的停止　等 また、影響範囲の確認や原因究明のためにログ保全やイメージコピー取得など事後調査（フォレンジック調査）に備えた手順を整備しているか。
③　脆弱性及び脅威情報の定期的な情報収集・分析・対応手順を明確に定め、組織的に実施しているか。 （注）ブロックチェーン等の技術を利用する場合、関連する周辺技術を含めた幅広い情報収集の必要性があることに留意する。	⑤　脆弱性及び脅威情報の定期的な情報収集・分析・対応手順を明確に定め、組織的に実施しているか。
また、システムの脆弱性について、OS の最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。	また、システムの脆弱性について、OS の最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。

改正案	現行
（削除）	⑥　サイバーセキュリティについて、第三者（外部機関）のセキュリティ診断（脆弱性診断、ソースコード診断、ペネトレーションテスト等）を活用するなど、セキュリティ水準の定期的な評価を実施し、セキュリティ対策の向上を図っているか。 　また、国内外でサイバーセキュリティ侵害事案が発生した場合には、適宜リスク評価を行っているか。
④　（略）	⑦　インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような取引のリスクに見合った適切な認証方式を導入しているか。 ・　可変式パスワードや電子証明書などの、固定式の ID・パスワードのみに頼らない認証方式 ・　取引に利用しているパソコン・スマートフォンとは別の機器を用いるなど、複数経路による取引認証 ・　ログインパスワードとは別の取引用パスワードの採用　等
⑤　（略）	⑧　インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような業務に応じた不正防止策を講じているか。 ・　不正な IP アドレスからの通信の遮断 ・　利用者に対してウィルス等の検知・駆除が行えるセキュリティ対策ソフトの導入・最新化を促す措置 ・　不正なログイン・異常な取引等を検知し、速やかに利用者に連絡する体制の整備 ・　前回ログイン（ログオフ）日時の画面への表示　等

改正案	現行
（削除）	⑨　サイバー攻撃を想定したコンティンジェンシープランを策定し、訓練や見直しを実施しているか。また、必要に応じて、業界横断的な演習に参加しているか。
（削除）	⑩　サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。