暗号資産交換業に係る緊急時対応に関する規則（新旧対照）

改正案	現行	備考
暗号資産交換業に係る緊急時対応に関する規則 （2018年7月30日　制　　定） （2018年10月23日　一部改正） （2020年4月24日　一部改正） （2024年 2月 9日　一部改正） （202x年 x月 x日　一部改正）	暗号資産交換業に係る緊急時対応に関する規則 （2018年7月30日　制　　定） （2018年10月23日　一部改正） （2020年4月24日　一部改正） （2024年 2月 9日　一部改正）	
	第1章　総則	
	（目的） 第 1 条　本規則は、会員が行う暗号資産関連取引（暗号資産関連デリバティブ取引を除く。以下同じ。）に係る業務において生ずる緊急事態への対応方法（以下、「コンティンジェンシープラン」という。）並びにシステム障害発生時の対応に関する基本的な事項を定めることを目的とする。	
	（対応の原則） 第 2 条　会員は、緊急事態が発生した場合には、人命の救出と保護を最優先とし、対応しなければならない。	
	（事前準備） 第 3 条　会員は、緊急事態の発生に備え、緊急時における指示・命令系統、情報伝達経路、避難誘導路及び避難場所等の確保及び重要資産の保全方法を定め、実践を想定した訓練に努めなければならない。	
	（事後処理） 第4条　会員は、緊急事態対応が終結し次第、状況を調査・分析し、平常業務に戻れるよう適正な事後処理に努めなければならない。	
	第 2 章 コンティンジェンシープラン	
（コンティンジェンシープランの策定） 第5条　会員は、コンティンジェンシープランを策定し、緊急時体制を構築しなければならない。また、コンティンジェンシープランの策定及び更新を行うにあたっては、取締役会等による承認を受けなければならない。 2　会員は、以下の事項に留意して、コンティンジェンシープランの策定に努めなければならない。 (1) 客観的な水準が判断できるもの（例えば「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書」（公益財団法人金融情報システムセンター編））を根拠として、コンティンジェンシープランを策定すること。 具体的には、コン	（コンティンジェンシープランの策定） 第5条　会員は、コンティンジェンシープランを策定し、緊急時体制を構築しなければならない。また、コンティンジェンシープランの策定及び更新を行うにあたっては、取締役会等による承認を受けなければならない。 2　会員は、以下の事項に留意して、コンティンジェンシープランの策定に努めなければならない。 (1) 客観的な水準が判断できるもの（例えば「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書」（公益財団法人金融情報システムセンター編））を根拠として、コンティンジェンシープランを策定すること。	

ティンジェンシープランの策定に際しては、緊急事態のシナリオを設定し、緊急時体制の決定及び代替手段の詳細検討を行った上で、初期対応手順書、暫定対応手順書及び本格復旧手順書を作成し、かつ、コンティンジェンシープランの維持管理態勢を定めること。 (2) 想定する事態に関し、次に掲げる事項を含めて策定すること。 イ サイバー攻撃 ロ 災害・パンデミック ハ 会員の内部又は外部に起因するシステム障害 ニ 情報漏えい事案等 ホ 暗号資産の流出、消失又は不正利用等 (3) バッチ処理が大幅に遅延した場合など、十分なリスクシナリオを想定すること。 3　会員は、他の暗号資産交換業者その他金融機関等におけるシステム障害等の事例及び金融庁による業務改善命令等における事例、中央防災会議等の検討結果等を踏まえて、想定するシナリオを適宜見直し、コンティンジェンシープランを更新しなければならない。	(2) 想定する事態に関し、次に掲げる事項を含めて策定すること。 イ サイバー攻撃 ロ 災害・パンデミック ハ 会員の内部又は外部に起因するシステム障害 ニ 情報漏えい事案等 (3) バッチ処理が大幅に遅延した場合など、十分なリスクシナリオを想定すること。 3　会員は、他の暗号資産交換業者その他金融機関等におけるシステム障害等の事例及び金融庁による業務改善命令等における事例、中央防災会議等の検討結果等を踏まえて、想定するシナリオを適宜見直し、コンティンジェンシープランを更新しなければならない。	
	（指示・命令系統） 第 6 条　会員は、緊急事態に対処するための指示・命令系統及び情報伝達経路、対応手順その他緊急時対応として必要な事項を文書にまとめ、あらかじめ役職員に提示し、理解させなければならない。 2　前項の指示・命令系統及び情報伝達経路は、主たるルートが機能しない場合に備え、指示・命令を行うべき者が不在の場合の代行者の順位及び代替ルートなど、緊急時対応に必要な機能を維持するための備えを確保しなければならない。	
（関係機関との連絡） 第 7 条　会員は、緊急事態の発生時に連絡を取るべき関係機関（協会を含む。）を洗い出し、当該機関への連絡担当者及び連絡方法を記した書面を作成し、緊急時対応に関わる役職員に交付する。 2　会員は、関係機関に対し、緊急事態発生時の会員との交信手段及び連絡担当者を提示するなど、緊急時における関係機関との連絡体制の構築及びメンテナンスに努めなければならない。 3　前項にかかわらず、会員は、協会に対し、協会所定の書式により、連絡担当者等を届け出るものとする。 4　会員は、緊急事態が発生した場合には、直ちに協会にその事実を報告するとともに、協会が定めるガイドラインに基づいて、必要な事項を協会に報告しなければならない。 5　協会は、会員が関係機関に対して報告し又は資料の提出を行った場合には、当該会員に対して当該内容の報告又は当該資料の提出を求めることができ、会員は、やむを得ない事由がある場合を除き、これを報告又は提出しなければならない。	（関係機関との連絡） 第 7 条　会員は、緊急事態の発生時に連絡を取るべき関係機関を洗い出し、当該機関への連絡担当者及び連絡方法を記した書面を作成し、緊急時対応に関わる役職員に交付する。 2　会員は、関係機関に対し、緊急事態発生時の会員との交信手段及び連絡担当者を提示するなど、緊急時における関係機関との連絡体制の構築及びメンテナンスに努めなければならない。 3　協会との連絡については、協会が指定する届出書の提出をもって行うものとする。 （新設） （新設）	

6　協会は、業務上必要な範囲で、前二項に基づき会員から報告を受けた内容や提出された資料等を当該会員以外の第三者に提供することができるものとする。 7　協会は、緊急事態に対処するため、専門家を含む適切な外部機関に対し、必要に応じて支援及び助言を要請することができるものとする。	（新設） （新設）	
	（訓練） 第 8 条　会員は、コンティンジェンシープランに基づく訓練を定期的に実施しなければならない。 2　会員は、全社レベルにて、コンティンジェンシープランに基づく訓練を行わなければならない。 また、訓練の結果を検証し、コンティンジェンシープランの見直しを行わなければならない。 3　会員は、暗号資産関連取引に係る業務に関して外部委託先等を利用している場合には、前項の訓練については、外部委託先等と合同で実施することに努めなければならない。 4　会員は、必要に応じて、業界横断的な演習への参加に努めなければならない。	
	（バックアップ） 第 9 条　会員は、業務への影響が大きい重要なシステムについて、災害、システム障害等が発生した場合にも、速やかに業務を継続できる体制を整備しなければならない。 2　会員は、暗号資産の取引システムについては、メインシステムと並行運用するバックアップシステムを設置するなど、メインシステムの予期せぬ停止時においても速やかに売買取引が再開できるように努めなければならない。	
	第 3 章　システム障害等への対応	
	（システム障害の発生時の対応） 第 10 条　会員は、システム障害等が発生した場合には、利用者に対し、無用の混乱を生じさせないよう適切な措置を講じなければならない。	
	（障害発生への対応準備） 第 11 条　会員は、システム障害等の発生に備え、最悪のシナリオを想定した上で、必要な対応を行う体制を整備し、役職員への教育及び訓練を実施しなければならない。 2　会員は、システム障害等の発生に備え、外部委託先を含めた報告体制、指揮・命令系統を明確にしなければならない。 3　会員は、システム障害等の発生に備え、ノウハウ・経験を有する人材をシステム部門内、部門外及び外部委託先等から速やかに招集するために事前登録するなど、応援体制を明確にしなければならない。	
	（サイバー攻撃時の対応）	

	第 12 条 会員は、サイバー攻撃を受けた場合には、被害の拡大を防止するために、その必要に応じて、次の各号の措置を速やかに講じなければならない。 (1) 攻撃元の IP アドレスの特定と遮断 (2) DDoS 攻撃に対して自動的にアクセスを分散させる機能 (3) システムの全部又は一部の一時的停止	
	（発生報告） 第 13 条 会員は、業務に重大な影響を及ぼすシステム障害等が発生した場合に、速やかに代表取締役をはじめとする取締役に報告するとともに、報告に当たっては、最悪のシナリオの下で生じうる最大リスク等を報告する態勢としなければならない。 2 会員は、必要に応じて、対策本部を立ち上げ、代表取締役等自らが適切な指示・命令を行い、速やかに問題の解決を図る態勢としなければならない。	
	（利用者への対応） 第 14 条 会員は、システム障害等が発生した場合、障害の内容・発生原因、復旧見込等について速やかに公表するとともに、利用者からの問い合わせに的確に対応するため、必要に応じて、コールセンターや相談窓口の設置、協会に対応を依頼するなどの措置を迅速に行わなければならない。 2 会員は、システム障害等の発生に備え、関係業務部門への情報提供方法、内容を明確にしなければならない。	
	（再発防止） 第 15 条 会員は、システム障害等の発生原因の究明、復旧までの影響調査、改善措置、再発防止策等を的確に講じなければならない。 2 会員は、システム障害等の原因等の定期的な傾向分析を行い、それに応じた対応策をとらなければならない。 3 会員は、システム障害等の影響を極小化するために、例えば障害箇所を迂回するなどのシステム的な仕組みを整備しなければならない。	
	第 4 章 届出等 （システム障害等の当局への連絡等）	
	第 16 条 会員は、次の各号に係るコンピュータシステムの障害やサイバーセキュリティ事案が発生した場合には、その発生を認識次第、直ちに、その事実を当局及び協会に報告しなければならない。ただし、会員の一部のシステム・機器にこれらの影響が生じても他のシステム・機器へ速やかに交替することで実質的にはこれらの影響が生じない場合を除く。 (1) 暗号資産交換業に関する業務に遅延、停止等が生じているもの又はそのおそれがあるもの (2) その他業務上、(1)に類すると考えられるもの	

	2　会員は、前項の報告の後、速やかに所定の「障害発生等報告書」を作成し、当局に提出するほか、その写しを協会に提出しなければならない。 3　会員は、発生したシステム障害等の復旧時及び原因解明時には改めてその旨を当局及び協会に報告しなければならない。 4　会員は、システム障害の原因の解明がされていない場合でも、第1項の報告後、1 か月以内に、その現状について、当局及び協会に報告しなければならない。 5　会員は、システム障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、利用者や 業務に影響を及ぼす、又は及ぼす可能性が高いと認められるときは、当局及び協会に報告しなければならない。 6　会員は、重大なシステム障害等の発生理由が会員内部に起因する場合であって、自らが定める処分規定に基づき関係する役職員を処分した場合には、その結果を協会に報告しなければならない。	

「暗号資産交換業に係る緊急時対応に関する規則」に関するガイドライン（新旧対照）

改正案	現行	備考
「暗号資産交換業に係る緊急時対応に関する規則」に関するガイドライン （2018 年 7 月 30 日　制　　定） （2018 年 10 月 23 日　一部改正） （2020 年 4 月 24 日　一部改正） （2024 年 2 月 9 日　一部改正） （202x 年 x 月 x 日　一部改正）	「暗号資産交換業に係る緊急時対応に関する規則」に関するガイドライン （2018 年 7 月 30 日　制　　定） （2018 年 10 月 23 日　一部改正） （2020 年 4 月 24 日　一部改正） （2024 年 2 月 9 日　一部改正）	
	第 7 条第 1 項関係 緊急時における関係機関との連絡体制を取りまとめ、対象とする機関との連絡を取り合う役職員に連絡先、連絡方法などの必要事項を伝えて、臨機に行動できるようにする必要があります。役職員への連絡先等の情報伝達の方法は書面をもって行うことを基本としますが、併せて電磁的方法をもって伝達することも支障はありません。（停電時など電子ファイルが取り出せない事態及び電磁的方法が利用できない事態も想定することが肝要です。）なお、関係機関への連絡方法については、相手方の機関の指定する方法を優先することとなりますが、指定する方法によることが困難な場合や複数の方法を確保することが必要であると判断した場合には、当該機関と相談し、具体的な方法を取り決めます。協会への連絡については、原則として、別途、協会が指定する方法により行ってください。（システム障害報告については、第 16 条の規定に従い、当局への報告書の写しに協会が指定する表紙を付けて提出することとします。）	
第 7 条第 4 項関係 第 7 条第 4 項の規定による報告は、以下のとおりとします。なお、以下の提出資料は、あくまで一	（新設）	

例であり、これに限るものではありません。また第 7 条第 4 項に記載の通り、緊急事態が発生した事実については 24 時間以内ではなく、直ちにご報告をお願いいたします。

報告期限	原則：速やかに（原則 24 時間以内） 例外：人命の救助、災害の救援その他緊急事態への対応のため、緊急かつやむを得ないと認められるときは、当該事由が解消した後速やかに	24 時間以降、協会が求める期限まで
提出資料	【緊急事態全般】 (1) 以下の内容が分かる資料 ・事象の内容 ・利用者関係（対利用者影響、苦情状況、対応方針、対応状況等） ・発生からの経緯、対応状況等（時系列順に記載されたもの） ・当局との連携状況 ・コンティンジェンシープラン、行動フロー等 ・緊急時対応体制	【緊急事態全般】 １．原因にかかるもの (1) 調査体制が分かる資料 (2) 関係する会議体議事録 (3) 調査結果等の報告資料 (4) 関連社内規程 (5) 外部委託先等関係資料（関連社内規程、契約書、利用規約、SLA・SLO、委託先の管理状況が分かるもの、委託先選定・リスク評価にかかる資料等） ※外部委託先が原因に関与している場合 (6) 当局報告資料 ２．事業継続にかかるもの (1) 以下の内容が分かる資料 ・BCP ・財務計画、資金繰り関係 ・再発防止策 (2) 改定した規程、マニュアル、フロー等 (3) 関係する会議体議事録 (4) 当局報告資料 (5) 振り返り資料
	【暗号資産の流出、消失又は不正利用等】 (1) 以下の内容が分かる資料 ・流出先の暗号資産アドレスにかかる情報 ・被害拡大防止のための対応 ・ウォレット構成等 (2) ウォレット運用マニュアル・フロー図等	【暗号資産の流出、消失又は不正利用等】 (1) 業界への情報還元資料

第 8 条関係

会員において策定したコンティンジェンシープランについては、時間的制約や

	コンピュータ資源等の実効性を確認するため、あるいはほかの暗号資産交換業者等におけるシステム障害等の事例を踏まえ、想定シナリオを適宜見直し、訓練を実施する必要があります。また、暗号資産交換業者の間での取引量が増大するにつれて、決済に伴うリスクも増大するため、業界横断的な演習を実施することがより重要となります。	
	第９条関係 　　業務継続の体制整備の方法としては、例えばメインシステムとは異なる系統を利用したバックアップ用のシステムを遠隔地に設置するなどの方法が望ましいと考えられますが、これに限るものではありません。	