暗号資産関連デリバティブ取引業に係る緊急時対応に関する規則（案）

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デリバティブ取引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。

(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、他の暗号資産関連デリバティブ取引業者その他の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。

（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。

３　会員は、暗号資産関連デリバティブ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、暗号資産関連デリバティブ取引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、顧客に対し、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。

（顧客への対応）

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、顧客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・機器が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) 暗号資産関連デリバティブ取引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、顧客や 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にあって、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。