緊急事態発生時における事業継続計画（ＢＣＰ）について

平成１７年８月１７日制定
平成２０年１０月１４日改正
株式会社 日本証券クリアリング機構

弊社は、我が国における市場横断的な清算機関として、その役割を確実に果たすという観点から、平成１６年２月には、システム障害等の緊急事態発生時における業務執行の基本方針を策定し、さらに、平成１７年３月には、当社を取り巻く様々なリスクに対してより適切に対応するため、システム障害、災害、テロ等、あらゆるリスクの発現を想定した事業継続に関する基本的対応、体制、手順等を定め、緊急時事業継続計画（ＢＣＰ）としてとりまとめました。

その後、弊社では、当該ＢＣＰを踏まえ、安定的な業務提供を行うための一層の基盤強化に向けた対応の一環として、清算参加者をはじめとする関係機関の方々にも当社のＢＣＰの内容を知っていただくために、セキュリティ等の面で問題とならない範囲で平成１７年８月にその概要を公表いたしておりましたが、業務運営基盤のより一層の強化の観点から、平成２０年１０月より弊社清算システムにおけるバックアップセンタ（セカンダリセンタ）を開設・稼動させましたことから、当該セカンダリセンタの存在を踏まえた所要の改正を行い、以下のとおり改正版の基本方針を公表いたします。（平成１７年８月版からの改正箇所は赤字にて記載しております。）

なお、現在、既に公表している緊急事態発生時の対応方針、マニュアルについては、引き続きＢＣＰの一部を構成する文書として位置付け、適用しますので、清算参加者及び関係機関の皆様への対応に特段の変更はないことを念のため申し添えます。

項目	内容
１．目的	・ リスクが顕在化した際に、可能な限り事業継続を図ることにより、清算参加者、指定市場開設者、資金決済銀行及びその他関係機関への影響を最小化し、我が国における市場横断的な清算機関としての責務を果たすことを目的とする。
２．対象範囲	

項目	内容
（１） 想定するリスク	・ 業務停止につながる恐れのある想定リスクを、原因事象及び結果事象の組み合わせとして整理することにより、可能な限り幅広いケースへの対応を網羅する。 ・ 原因事象としては、地震・風水害・疫病等の自然災害等、システム障害、電力・通信等の社会インフラの停止、テロ（予告・破壊行為）、サイバーテロでの被災を想定する。 ・ 原因事象が発生することによりもたらされる結果事象としては、建物の利用不能、システムの利用不能、人員の不足、外部機関の停止等を想定する。
（２） 継続対象業務	・ 清算約定に係る当社と清算参加者との決済業務並びに東京証券取引所（東証）及びジャスダック証券取引所への担保サービス提供業務を継続対象業務とし、可能な限り業務を継続しうる態勢を整備する。
３．対応方針の設定	・ 結果事象を「局所被害」「広域災害」「システム障害」に分類し、各々について、想定されるリスクが顕在化した際の対応方針並びに事業を可能な限り継続するための態勢及び手順を定める。
（１） 局所被害	・ 局所被害は、テロ（予告、破壊行為）等により、当社は被害を受けているものの、外部関係機関には特段の影響がない場合を指す。 ・ 局所被害が発生した際には、①ＢＣＰ対策本部の設置、②被害状況の把握、③対応方法の検討・決定、④外部機関への連絡、⑤代替運用の実施（システムセンタの切替、代替オフィスへの異動等）、⑥本格復旧への準備等を行う。
（２） 広域災害	・ 広域災害は、大規模地震、風水害等により、当社及び外部機関がともに被害を受けている場合を指す。 ・ 広域災害が発生した際には、局所被害が発生した場合の対応に加え、一定の間隔で外部機関の被害・復旧状況の把握を行う。

項目	内容
（３） システム障害	・システム障害は、システムのハード障害、アプリケーション障害、通信回線障害等により、当社又は当社が清算・決済業務を遂行していくうえで関係する外部機関が被害を受けている場合を指す。 ・システム障害が発生した際には、局所被害又は広域災害が発生した場合の対応に先立って、障害の影響調査を実施する等の初動対応を行う。システム障害が重度であった場合には、ＢＣＰ対策本部を設置し、局所被害又は広域災害が発生した場合に準じた対応を実施する。
４．体制・インフラの整備 （１）ＢＣＰ対策本部	・当社は上記３．の対応を行うために、以下の体制・インフラの整備を行っている。 ・リスクが顕在化した際に、所要の対応を迅速かつ的確に行うため、ＢＣＰ対策本部を設置し、被害状況及び事業継続状況の把握、外部機関との連絡等を行うとともに、必要な意思決定を行う。
（２）人員の確保	・夜間・休日にリスクが顕在化した場合などを想定しあらかじめ初動対応にあたる人員を定める。
（３）通信手段の確保	・リスクが顕在化した際に、当社内外への連絡手段を確保するために、一般電話、FAX、災害時優先電話、携帯電話、電子メール、Target-JSCC サイト等の様々な通信手段を用意し外部関係機関との間で相互に連絡先を交換している。
（４）代替オフィス	・通常使用している建物が利用不能となった場合に、他の場所で事業を継続することができるよう、最低限の代替オフィスを用意し、あわせてリスクが顕在化した際に代替オフィスに移動する人員を定める。
（５）システムセンタ	・メインセンタ（プライマリセンタ）を開設する建物については、ＦＩＳＣ（(財）金融情報システムセンター）の「金融機関等コンピュータシステムの安全対策基準」をすべて満たし、かつＩＳＭＳ（情報セキュリティマネジメントシステム）認証を取得している。また、セカンダリセンタについては、プライマリセンタと同等の設備の堅牢性と通信ネットワークが具備され、かつプライマリセンタとの同時被災リスクが極めて低いと考えられる地域に開設している。

項目	内容
（６）バックアップ体制	・ 大規模災害等が発生し、プライマリセンタが利用不能となり、速やかな復旧が困難であると判断した場合、セカンダリセンタを使用して清算業務の継続を図る。この場合、リスク事象の発現後概ね２時間以内を目標とし、復旧を実現できる体制を整備する。
（７）テスト・教育研修	・ ＢＣＰの内容の検証を行うとともに、ＢＣＰに定める対応手順を円滑に行うため、テスト及び教育研修を定期的に実施する。 以　　上