2019 年 3 月 29 日

TaoTao 株式会社　事業継続計画

(Business Continuity Plan ： BCP)

2019 年 3 月 29 日

Ⅰ　基本方針

当社は、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、利用者の皆さまや当社の株主の皆さま等のステークホルダーへの影響を最小化することを目指します。また、事業継続による当社の企業価値の源泉たるブランド力の向上及び日本における暗号資産取引市場の信頼性の向上も目的としています。

Ⅱ　想定リスク

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で整理し、可能な限り幅広いケースへの対応を網羅することとします。

原因事象としては、大規模地震・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）、サイバーテロによる被災を想定します。

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、関係する外部機関（銀行等）の停止等を想定します。

Ⅲ　対応方針

結果事象を「局所被害」、「広域災害」及び「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継続のための態勢及び手順を定めます。

1. 局所被害

局所被害は、テロ（予告、破壊行為）あるいは局所的な停電等により、当社は被害を受けているものの、外部機関には特段の影響がない場合を指します。局所被害が発生した際には、

1　社員の安否確認（破壊行為発生の場合）

2　BCP 対策本部の設置

(1) 代表取締役を本部長として、セールス＆マーケティング・ユニット長、リスク・マネージメント・ユニット長、コーポレート・ユニット長及びシステム・ユニット長にて BCP 対策本部を設置し、対応を指揮します。

(2) BCP 対策本部は、各人が出勤可能で、かつ、本社オフィスが被害を受けていない場合は、本社オフィスにフィジカルに設置します。

(3) 本社オフィスが被災、あるいは、公共交通機関が麻痺状態にある、BCP 対策本部構成員が何らかの事情で出社できない場合は、Slack 等のバーチャルな手段で構成することにします。

3　被害状況の把握
(1) 本社オフィス、データセンターの被害状況を把握します。
(2) システムの稼働状況を把握します。
(3) 取引システムが停止した場合は、取引が停止したポイントを確定します。
(4) システム保守要員の対応可否に関する情報を把握します。
4　対応方法の検討・決定
5　利用者の皆さまへの連絡
(1) 対応方針、方法決定後、速やかにホームページに掲載します。
6　外部機関への連絡
(1) 金融庁（フィンテックモニタリング室）及び日本仮想通貨交換業協会業務部へ BCP 対応の実施を連絡します。
7　暫定復旧
(1) 被害の回復に時間がかかる場合は、暫定復旧（例えば、お客さまの暗号資産及び日本円の出庫・出金指図のみを受け付け、取引自体は停止。）を行う場合もあります。
8　本格復旧
(1) 全てのサービスを通常通り提供します。
(2) 本格復旧は、被害状況にもよりますが、可能な限り早期の復旧を図るべく最善の努力を行います。
9　RTO（目標復旧時間）
(1) 少なくとも暫定復旧は、24 時間以内を目指します。
(2) 本格復旧は、被害の程度によりますが、可能な限り早期の復旧を目指します。
等を行います。

2. 広域災害

広域災害は、大規模地震（震度 6 弱以上）、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します。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（取引銀行、電力、通信及び交通等のインフラ機関）の被害・復旧状況の把握を行います。

広域災害時の暫定復旧における RTO（目標復旧時間）は、災害の状況如何ではありますが、可能な限り、24 時間以内の復旧を目指すこととします。なお、本格復旧は電力、通信及び交通などのインフラ機関の復旧状況に依存する可能性がありますが、可能な限り早期の復旧を目指します。

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します。

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います。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こととします。

なお、システム障害の場合の RTO は、原則として 12 時間以内を目指します。

Ⅳ　体制・インフラの整備

1.　BCP 対策本部

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、上述の構成メンバーにより 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います。

2. バーチャル対応

必ずしもフィジカルに本社オフィス等に集合せずとも BCP 対応が進められるように、バーチャルなコミュニケーション手段を確保します。

3. データセンター

システムを設置しているデータセンターは、Uptime Institute（https://journal.uptimeinstitute.com/）の定める TierⅢ乃至 Tier III+ ガイドラインに従って運営されています。よって、災害による被災のリスクは相当程度低いものと考えられます。

4.　バックアップ体制

取引に関わるシステム機材については、冗長構成を取り、ハードウェア障害等による業務停止を回避する対策を取っていきます。

5. テスト・教育

定期的に 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少なくとも年 1 回以上実施します。

以上