PRESS RELEASE

各　　位

カブドットコム証券株式会社
（コード番号：8703 東証1部）
代表執行役社長 齋藤 正勝

2006年4月17日

当社第2のビジネス拠点「福岡システムセンター」の開設について

～ 証券会社初自社で本格的な遠隔地・災害復旧(DR)サイトを構築し事業継続計画(BCP)を実現 ～

→ システム紹介

カブドットコム証券株式会社は、地震、火災などの自然災害、テロ、サイバーテロなどの人的災害、通信サービス提供や電力供給の中断など社会インフラの障害、大規模システム障害など大規模災害を想定した情報システム・リスクへの対策として、福岡県を拠点としたシステムセンターを開設しました。投資規模は既存システムの増強を含め、今後3年間で50億円程度、福岡において災害時には本社機能を完全に代替できる体制を構築する予定です。まず勘定系データベースシステムの災害復旧（DR：ディザスター・リカバリー）サイトについて、4月末までに災害復旧基盤として整備し、9月末までに全災害復旧対策を完了します。

当社は、お客様向けの発注系・勘定系の全システムを自社で開発し運営する唯一のネット証券です。当災害復旧（DR）サイトは、広域災害に備えた本格的な遠隔地・災害復旧サイトを証券会社で初めて自社で構築するものです。当センター開設にあたり、システム部門の組織改変を始めとしたシステム・サービス管理体制等の整備・拡充等の施策を進め、事業継続計画（BCP： ビジネス・コンティニュイティ・プラン）の実現を図ると共に、福岡を新規事業等の第2のビジネス拠点として展開して参ります。

■災害時システムセンターとしての福岡の優位性
当システムセンターは九州電力グループである株式会社キューデンインフォコム（QIC）が提供するIDCサービス（インターネット・データセンター・サービス）を選定しました。

【福岡システムセンターの主な特徴】

- ミッションクリティカルな電気事業を通じて培ったノウハウにより九州電力グループが提供する高品質・高付加価値サービス
- 金融情報システムセンター（FISC）の『金融機関等コンピュータシステムの安全対策基準』にも対応した堅牢で強固なファシリティとセキュリティ
- 平成17年3月の福岡西方沖地震（マグニチュード（M）7.0と推定）でも、ビル免震構造等の対策により被害ゼロで継続運転を実証（一輪差しの花瓶も倒れなかった）
- 高品質かつリーズナブルな東京～福岡間高速バックアップ回線
- 福岡県が運営する福岡ギガビットハイウェイ（FGH）や日韓光海底ケーブルネットワーク（KJCN）、および当社がインターネット接続に利用するインターネットサービスプロバイダである、株式会社インターネットイニシアティブ（IIJ）の福岡アクセスポイントとの容易な接続性

福岡は、現在運用中の当社のデータセンターから約1000kmの距離があり、広域災害に備えた遠隔地かつ本サイトと同時被災しない立地で、平常時の東京からの利便性も高く（空路で東京～福岡間1.5時間、福岡空港から市内中心地まで地下鉄利用で10分程度）災害時は陸路・空路・海路の活用が可能であることを主な理由にシステムセンターの立地として選択致しました。福岡の高い都市機能、豊富な人材、IT産業の集積、アジアへの展開可能性など潜在的なポテンシャルの高さも、今後当社の福岡を拠点とした事業展開に極めて有益に働くものと期待しています。

■当社の事業継続計画(BCP)の基本方針
不慮の災害や事故、あるいは障害等により重大な損害を被り業務の遂行が困難になった場合に、損害の範囲と業務への影響を極小化し、迅速かつ効率的に業務の復旧を行うために、事業継続計画（BCP）をあらかじめ定めています。

【対象範囲】
(1) 想定するリスク
災害には様々な原因が考えられますが、当社のコンピュータシステムに損害を与え得るリスクとして、地震・火災などの自然災害、テロ、サイバーテロなどの人的災害、通信サービス提供や電力供給の中断など社会インフラの障害、当社システムの大規模障害、コンピュータ犯罪、オペレーションミス・その他の過失などを想定しています。
(2) 適用範囲
当社コンピュータシステムで提供されている業務（発注系、勘定系、資金決済系、各種サービス業務、内部管理業務）及び、当社の役職員、当社業務に従事する派遣職員に適用します。当社に関係する関係諸機関および供給者には、平常時より当社のBCPの理解を求め、未然防止策及び連絡体制等を整備します。

【未然防止策】
上記対象範囲「(1) 想定するリスク」に定めるリスクを軽減するため、以下の施策を施しています。
【1】 当社システムの二重化、バックアップ等（WEBサーバ等の負荷分散機能、高速インターネット回線の地域分散接続、ファイアウォール等の設置、等）
【2】 防犯体制（虹彩認証、指紋認証、監視カメラ等）
【3】 ビル自然災害対策（免震構造、24時間自家発電に対応した電源供給、金融情報システムセンター（FISC）準拠）
【4】 コンピュータ犯罪・オペレーションミス・その他の過失等の対策（ISMSをベースとした各種規程・手順・遵守事項の整備）

これらの施策は、平常時のシステムに関する情報の開示として、毎月の業務開示、システムリポート（処理実績パフォーマンス、設備増強計画、システム詳細情報、システム不備状況等）と併せて、当社ホームページに掲載しています。

【基本対応方針】
大規模自然災害やコンピュータシステム障害により、業務への支障が発生した場合、また発生が予想される場合、指示命令系統や役割分担を明確にし、迅速な対策を講じ被害を最小限に留めるために緊急時対策本部を編成し、本部が策定する基本対応方針に基づき、復旧作業

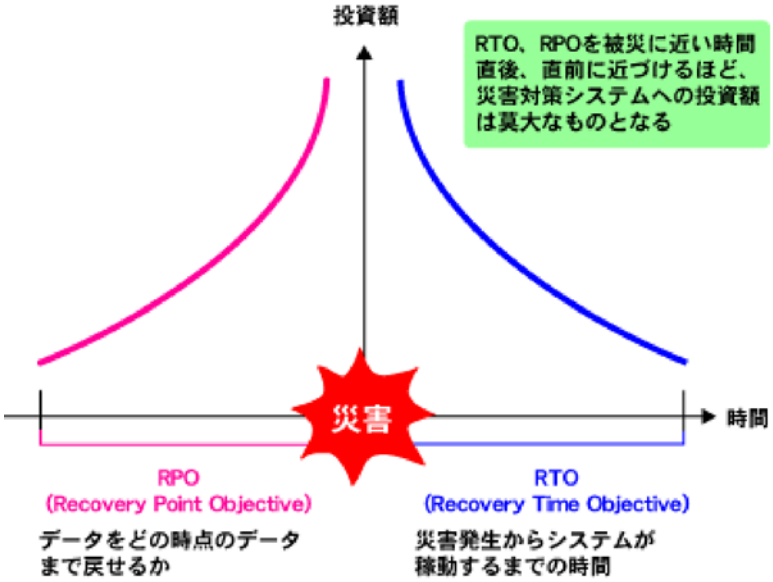
を進めます。
通常時より、ISMS・QMSに基づいた品質管理委員会にて、当社を取り巻く様々なリスクを認識しこれに適格に対応するための検討を行なっています。

【対応のための体制整備】
災害等発生時には、緊急時対策本部の組織・分担を設置し、初期対応・暫定対応・本格復旧の対応手順、従業員安全確保・安否確認と要員招集、外部組織連絡、広報対応を定め、最低半年に1回の「緊急時連絡網」訓練や教育、維持管理、再評価を行ない、PDCAサイクル(*)を継続的に繰り返し、情報セキュリティレベルの向上に努めております。

■災害等発生時の復旧時間目標
一般的に多く採用される大規模災害復旧対策としては、日次の周期で各種バックアップメディアを遠隔地にある拠点にて保護・管理し、災害時に初めてシステム機能を代替する方式です。当社でも、各種データ等のバックアップ保護・管理を、大阪にある拠点にて日次周期の更新にて行なって参りました。今回の東京～福岡の遠隔地・災害復旧（DR）サイトでは、当社の事業継続性及び復旧させるデータおよびシステムのリアルタイム性を意識し、遠距離間における災害対策システムの要件として、実際に災害が発生してからデータ復旧・システムが再稼動するために必要な所要時間を重要視しました。

そこで、「災害発生時点からどこまで遡ってデータを復旧できるか」の指標としてRPO（Recovery Point Objective）を、「災害発生からどれだけの時間でシステムを稼働できるか」の指標としてRTO（Recovery Time Objective）を用いることとし、それぞれRPOは5分以内、RTOは30分以内を目標としました。尚、当社は株式等の注文において、執行時間が5分を超えないことを保証するSLA（サービス品質保証制度）を証券会社で唯一実施しています。

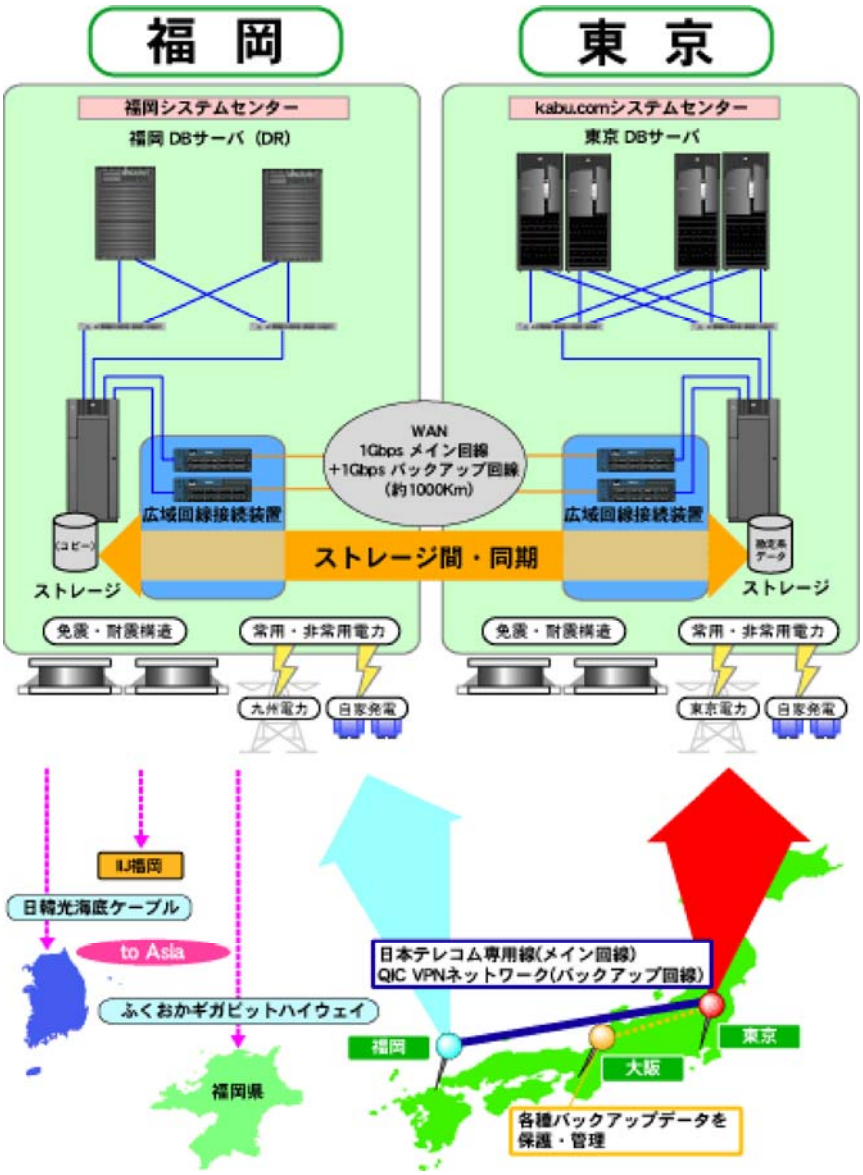
［RPO/RTOの考え方］



このような遠隔地間における極めて短い時間でのデータ復旧・システム再稼働は、従来はシステム構築・運用費用が非常に高額となり、また通信距離長に伴う技術的なハードルも高かったのですが、システムインテグレーターとして伊藤忠テクノサイエンス株式会社（CTC）が中心に提供する、日本ヒューレット・パッカード株式会社及びシスコシステムズ株式会社の最新オープン系テクノロジーを用いたDRソリューションを採用することにより、当社の経営指標であり競合他社比でトップクラスとなっているコストカバー率（委託手数料／シス

テム関連費（不動産関係費・減価償却費・事務費）率）を高水準に維持しつつ、DRサイトの復旧時間目標の実現が可能となりました。

［災害復旧(DR)基盤構成の概要］



■災害復旧(DR)サイト構成要素の選定事由について
当社は、お客様向けの発注系・勘定系の全システムを自社で開発・運営しているため、当DRサイトの構成要素を選定する際に、既存システムとの親和性は極めて重要な要素でした。

当社システムは、顧客管理系システム・注文管理系システムのOS・RDBMSにWindows ®とMicrosoft SQLServer ® を用い、勘定系システムのOS・RDBMSにHP-UX ® を主としたUnixとOracle ® を用いており、これらをHP Integrity SuperDome ® を中心としたマルチプラットフォーム環境で稼動させています。よって、DRサイトを構築する上でも、ホスト・OS等のインフラ環境に依存せず、かつオープンシステムとしてスタンダードな構成を必要としていました。ストレージシステムをベースとした遠隔地間ディスク複製テクノロジーは、ストレージに接続されるハードウェアやOS、RDBMSを始めとした各種アプリケーションに依存せず、かつそれぞれの組み合わせが可能である為、当社の要件を満たすと判断し、採用に至りました。

また、DRサイト拠点として福岡を選定することは、従来は距離（約1000km）から生ずる

拠点間の通信時の回線遅延、及び高額な接続回線コストにより非常に困難な状況でしたが、技術革新によりある程度の通信遅延を許容する遠隔地間ディスク複製テクノロジー、WAN環境におけるストレージ間通信とTCP/IP通信を混在させた上で最適化するネットワーク技術が登場したこと、日本国内での光ファイバー敷設を始めとする通信インフラの整備状況が進んだことによる接続回線コストのダウンにより、現実的な選択肢となり得ました。

東京～福岡間の通信方法については、将来的に福岡を拠点としたサービス展開を予定していることから、データバックアップ専用ではなく一般的なアプリケーション間の通信も発生しうる事を考慮する必要がありました。そこで、東京～福岡のストレージ間で発生する通信を、インターネットの世界において事実上の標準となっているTCP/IPプロトコルに変換することで、1本の物理回線に複数のアプリケーション間の通信やストレージ間通信による論理回線をシームレスに統合し、東京～福岡間のネットワークのコスト効率、利用効率の高い通信の実装が可能となりました。これらの構成要素により、業界に先駆けて当社の環境以外の要素に依存しない、導入が容易なオープンシステムとしての標準技術を用いたDR環境の構成が可能となりました。

■国際基準に準拠した情報セキュリティ管理（ISMS）の取り組み
当社は、2004年5月に国内証券会社では初めて、情報セキュリティ管理（ISMS）の標準規格である「ISMS適合性評価制度（Ver2.0）」と同、国際規格である「BS7799-2:2002」の認証を同時に取得いたしました。また、品質マネジメントシステム（QMS）の国際規格である「ISO9001:2000」認証も全業務について国内証券会社で初めて取得しております。今後も、情報セキュリティポリシーを元に、お客様向けシステムの安定稼働を目的として、技術的なセキュリティのほかに、組織が保護すべき情報資産や人間系の運用・管理面等に対してリスク分析・評価を行なうとともに、事業継続計画（BCP）を拡大・強化し、大規模災害時にも安定した取引環境を提供できるよう、PDCAサイクル(※)を継続的に繰り返し、情報セキュリティレベルの向上に努めて参ります。

尚、当社の情報セキュリティに関する取り組み状況は、「IR情報／業務情報」の「システムリポート」（毎月初旬更新）、「システム紹介」等で開示・説明して参ります。

(※) PDCA：Plan（情報セキュリティ対策の計画・目標）、Do（対策の実施・運用）、Check（実施結果の点検・監視）、Act（見直し・改善・処置）による継続的改善をISMS・QMSをベースに実施。