BCAO関西支部　第71回勉強会　議事録

日時：10 月 17 日(水) 18:20～20:30　　場所：京セラ本社 （2F 会議室）

座長：野原　　書記：日下

出席者：川口、大舘、柳父、藤村、伊藤、久保田、田中、山口、梅田、佐竹、徳永、西野、増穂、寅屋敷、野原、日下
岡（講師、ITBO研究会　座長）、尾坂（京セラ）（順不同、敬称略） 計18名

内容：概要以下のとおり。

【第1部】京セラのBCP取り組み経緯の紹介（野原）　現況は同社HP掲載のCSR報告書参照。

【第2部】「某レンタルサーバ大規模障害の事例から、IT-BCP を考える」（岡） ※詳細は配付資料参照

●某レンタルサーバ大規模障害の事例（作業ミス→ データ消失［第1事故］＋情報漏洩［第2事故］）

（1）概要と原因（最終報告書 2012-7-31 による）

①第1事故：6/20、某レンタルサーバ会社で脆弱性対策（メールシステム障害解消のメンテナンス）を特定サーバに実施したところ、更新プログラムに不具合があったため、対象外のサーバを含む全サーバのデータを消失した。
バックアップディスクにも同時適用されたため、バックアップのデータも消失した。
［原因］1）担当者による本番環境下での独自のメンテナンス方法　2）担当者による作業許可の自己判断

②第2事故：第1事故で消失したデータの復元を実行した結果（リカバードファイル）を顧客に提供したところ、想定以上のデータを想定外の場所に復元してしまい、対象顧客以外から一時みられる状態となった。
［原因］1）データ消失を想定したマニュアルなし　2）検証不十分な復元プログラムの利用

（2）主な再発防止策

・第1事故　→　開発・運用プロセスの見直し、牽制を含めた体制確立、2次バックアップの取得など。

・第2事故　→　データ消失時の対応マニュアル整備、リスクマネジメント組織の設置と社員教育の実施など。

（3）某レンタルサーバ会社の顧客対応

・損害賠償：契約に基づき顧客が支払った総額を限度として損害賠償するのが一般的。但し甚大な被害は個別対応か。

・データ復旧：消失したデータ（メール、顧客情報等）は復旧できず。バックアップしていたデータも消失した。

・情報漏洩：復元データ提供期間中に漏洩被害にあった可能性のある顧客は最大 2,359 者。メールと電話で個別対応。

●IT-BCP について（意見交換） ※以下主な意見を記載しました。

・IT-BCP とは、期待されない事象（火災、ハッキング、オペレーションミスなど）により事業に不可欠な IT サービスが中断した際に、経営陣が望む時間内に IT サービスを再開・継続させるための行動計画。また自然災害やシステムダウンなどの緊急時における重要な情報システムの継続と早期復旧を実現するための業務継続計画（IT サービス継続の国際規格、ISO/IEC27031:IRBC による。講師説明）。

・IT-BCP の意味はまだ明確とはいえず、確立した概念かどうかについては、なお議論の余地がある。

・本日のレンタルサーバ大規模障害の事例は IT サービスの品質問題であり、BCP の事例とまではいえない。

・IT システムのトラブルで事業が停止した事例も実際にある。経営上、IT は極めて重要。

・財務データなど株主・投資家情報は IT で提供されるため、万一不具合があれば即経営に関わる。

（小職補足）

・多くの組織にとり IT は不可欠な事業資源だが、種々の問題を内包しており、過信は禁物。また、過度の IT 依存は事業継続リスクを増大させるので、常に適切な対策（バックアップなど）を取っておく必要がある。

・組織が IT をアウトソースする場合は事業の継続も一部依頼先に依存することになるため、相手の信頼性が重要であり、自己の責任で確認すべきである。また、依頼先のシステムダウンなど、万一の事態に備えておくことも大切。

（伊藤加筆）

・現在では IT という言葉と共に ICT (Information & Communication Technology)という言葉が頻繁に使われ始めている。その中でも iPhone 及びスマートフォンが Communication のツールとして世の中の話題の中心を占めている。これらの Device は PC が超小型化して電話という機能を持ったという代物であり、今後各自一台の PC が自分のポケットに入る感じになる。もしこれら多数の iPhone 及びスマートフォンがボットや他のサイバー攻撃の対象になる日が来れば、携帯電話（iPhone 及びスマートフォン）に入っている個人情報、会社の重要情報、連絡情報等もその対象となり、IT-BCP/ICT-BCP とは何も「会社の基幹システム保護やバックアップ」といったものだけではなく、既に身近な生活・仕事の一部として組み込まれてしまっている、という最低限の認識が必要。

注：ボットとは、コンピュータを悪用することを目的に作られたプログラムで、コンピュータに感染すると、インターネットを通じて悪意を持った第三者が、あなたのコンピュータを外部から遠隔操作することを目的として作成された悪性プログラム。感染すると、この悪意を持った攻撃者（以下、攻撃者）があなたのコンピュータを操り「迷惑メールの大量配信」、「特定サイトの攻撃」等の迷惑行為から、あなたのコンピュータ内の情報を盗み出す「スパイ活動」など深刻な被害をもたらす。この操られる動作が、ロボット（Robot）に似ているところから、ボット（BOT)と呼ばれ、ボットに感染したコンピュータは、攻撃者が用意した指令サーバなどに自動的に接続され数十～数百万台のボット感染コンピュータを従えた「ボットネットワーク」と言われる巨大ネットワークを形成する。感染したコンピュータは、攻撃者からの命令を待ち続け、攻撃者から命令が下されると、このボットネットワークに接続された感染コンピュータは、攻撃者の意のままに数十～数百万台の感染コンピュータを操ることができ、フィッシング目的などのスパムメールの大量送信や、特定サイトへの DDoS 攻撃などに利用され大きな脅威となるため、感染コンピュータを使用しているユーザーは、知らぬ間に犯罪の踏み台にされ、「被害者」であると同時に「加害者」にもなってしまう。

出典：サイバークリーンセンター　www.ccc.go.jp/bot/index.html）

前述の事例：

一連のパソコン遠隔操作事件では、全国で4人が逮捕されたが、すべて誤認逮捕であることが確定した。警察による誤認逮捕だったと公式謝罪をされたとしても、冤罪に遭った代償は計り知れず、このような事態に会社の人間が巻き込まれた場合、迅速かつ正確な対応（準備、広報、IT 部門とリスク管理/BC 関連部署等）が必要となる。サイバー攻撃に対する現在の日本の警察や検察、自衛隊、その他関連機関及び専門ベンダーの対処・捜査能力の向上や再編は必要であると思われるが、真犯人検挙までのハードルは極めて高く、犯人はサイバー空間に逃げ込み、現実空間の捜査が及ばない。「ホワイトハッカー」と呼ばれる善良なコンピュータ専門家や、専門家の力を得て犯人検挙に至ることを期待するとともに、政府・行政機関や民間企業のリスク管理/BC 関連部署においても「現状のサイバーワールドへの認識、しかも最低限の認識を以って当該担当部署やベンダー/専門家との密なコミュニケーションを継続的に取る事」が重要。

以　上