東日本大震災におけるBCPの問題点

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2011.05.18更新

情報セキュリティ大学院大学　原田研究室

東日本大震災におけるBCPの問題点

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2011.05.18更新

情報セキュリティ大学院大学　原田研究室

No	検討項目	問題点	対応策
1	BCPの発動	①BCP、IT-BCPを発動する指揮命令系統が震災で機能しなかった（発動者や担当者が死亡したため、BCPを実施できなかった） ②BCPの発動を連絡するための通信インフラが不十分で、安否確認や被害状況の把握に手間取り、これに基づいたBCPの発動を速やかに行えなかった ③BCP、IT-BCPの文書が(停電や津波で）行方不明となり、BCPを発動できなかった ④一般社員がBCPとくに、IT-BCPを十分に内容を理解していないため、必要な措置がとれなかった ⑤津波や原子力発電所からの避難のため、必要なBCPを実施できなかった ⑥震災の全体像を把握するのに時間を要して、BCPの発動が遅れた	①BCPが機械的に発動できるように、マニュアル、取り決めなどを実施する ②本社のBCPの発動を待たなくてもよいように、現地に権限移譲しておく ③本社レベルのBCPと支社、現場レベルのBCPを階層化する。各レベルで個別にBCPが発動できるようにする ④BCPに関する文書類はオフィスが消滅してもアクセスできるようにする（クラウドに保管する、音声メッセージでアクセスできるように準備しておくなど）
2	BCPの不備	①BCP、IT-BCPの検討が十分でなく、使えなかった ②BCPの発動を連絡するための通信インフラが不十分で、取引先（サプライチェーン）と連携がとれず、適切なBCPを実施できなかった ③BCPで想定しなかった規模の災害のため、BCPで想定していない対応をとれなかった ④BCP、IT-BCPが(停電や津波で）広域被害を想定していなかった ⑤風評被害や二次被害などを考慮していなかった ⑥BCPでは、バックアップ電源装置は、数時間の利用しか考えていないため、連続運転が可能か分からなかった	①BCPを策定するとき、「初期対応」「暫定対応」「本格対応」にフェーズ分けするのがよいのではないか ②BCPでは、通常、事業ができなくなるようなシナリオを想定しない。しかし、想定するシナリオとは別に最悪のケースを分けて考えておく必要がある ③BCPを策定しても、現実に確かめるのは難しいので、BCPを点検するために、第三者による評価などがあるとよい ④BCPの機器は、連続運転が可能か、また制限事項を事前に確かめる

東日本大震災におけるBCPの問題点

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2011.05.18更新

情報セキュリティ大学院大学　原田研究室

No	検討項目	問題点	対応策
3	DRP(復旧計画)の問題	①BCPとDRを別のものととらえている ②DRについては、自社の被災を中心に考えているが、担当する従業員、機器の提供元、電源、通信インフラなどが得られない場合についての想定が甘かった ③すべてを喪失した際のDRを考えていない ④DRのための復旧用の資材や設備が地震で壊れたり津波で流失したが、調達が困難であった	①DRはBCPの一部として、復旧の部分だけを具体化したものと考えるとよい ②DRに必須の機器については、複数のチャンネルから調達できるようにしておく
4	インフラの問題	①早期にインフラが復旧すると想定（1週間程度）していたが、その通りにならない ②広域にインフラが損壊して、代替手段をとることができない ③電気が連続して利用できない（計画停電や総量規制）ことを考えていなかった ④不意の停電で、IT機器が故障しないような対策が必要となった	①BCPに必要な機器を搬入するルートを複数確保しておく（道路が使えないとき、空輸する手段を検討する） ②インフラがネックの場合には、立地を変更することも考える（最低限必要なBCPについては、インフラまで検討事項に含めておく）
5	通信インフラの問題	①通信インフラが、事業者の装置の故障、広域の震災のため広域に輻輳が広がり、ネットワークにアクセスできない状況が続いた ②企業のネットワークがIP-VPNを利用しているところは、IPネットワークの輻輳のため、帯域が制限された（BCPのTV会議ができなかった） ③携帯電話のネットワークは、基地局が故障してアクセス回線が少なくなった。スマートフォンなどの利用も進み、パケットネットワークも輻輳して、制限された	①被災地側での状況と、被災地以外での状況を把握できるように、MCAやPHS、アマチュア無線など、多重の通信手段を用意しておく ②非常時には音声ではなく、Webによる連絡など、多重の連絡手段を用意しておく ③セキュリティから無線LANを禁止している企業が多いが、非常時には、無線ルータ＋ノートPCの構成でインターネットへのアクセスを確保するなどの対策を用意しておく（情報セキュリティを解除することもBCPに記載しておく）

東日本大震災におけるBCPの問題点

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2011.05.18更新

情報セキュリティ大学院大学　原田研究室

No	検討項目	問題点	対応策
6	サプライチェーン	①取引先の絞り込みのため部品などが代替ができないため、被害にあったITが復旧できなかった ②復旧用のIT資材や設備が津波で流失し、その調達も困難であったこと ③ITに関する契約やITサービスのSLAが実施されない ④燃料などのサプライを十分に考えていないため、発電機を連続運転できなかった	①自分の事業に合わせて、どのようなサプライチェーンとなっているのかを分析して、それに対応した対策を考えておく ②バックアップの電源用に必要な燃料のサプライについても、複数のルートを用意しておく。自社の他地域から転送することができるように面的な備蓄も考慮する必要がある）
7	自社のセキュリティ環境の問題	①個人情報を管理していたサーバ室が崩壊したり、津波で流されて流出した。（これは、セキュリティインシデントとして扱うべきか？） ②シンクライアントの活用等によって、セキュリティレベルは高かったものの、これによって、自宅等で業務を継続することが出来なかった ③セキュリティはICカードの入室管理システムは電気を前提としているため、停電時のセキュリティを保持できない ④監視カメラなどが地震で壊れたり、電源が提供されないため、監視できていない（監視カメラに対する災害要件が必要）	①非常時には、情報セキュリティを解除できるような仕組みを考えておく ②人命（人間）に関するセキュリティは、フェイルセーフで対応する ③情報資産については、非常時でも機密保持が必要な場合には、災害で喪失する場合を想定した管理（常時暗号化）などが必要（津波でサーバが流出してもデータが解読されないようにする）
8	要員の問題	①スキルのある要員を多数失った（津波で行方不明となった） ②道路の損壊で、バックアップ要員が駆け付けることができない ③放射能汚染で、要員が駆け付けることができない ④要員の家族が不明で、要員の稼働を保証できない ⑤取引先などに要員派遣を要請しても、要員を手当できない ⑥計画停電のためにITの停止と動作のために要員を手当てが必要となるが、災害復旧で要員が不足しており、十分にITを動作させられない	①要員について、「初期対応」、「暫定対応」、「本格対応」のフェーズに分けて、適切に配置できるように計画する ②計画では、要員ごとに、スキル（非常時のリーダシップ、非常時の柔軟性）、住所、駆けつけ（家族のけがや住宅の損壊で駆けつけられない）のリスク評価 ③計画停電や急な停電の際の要員計画をする（サーバの停止、再稼働には待機要員が必要）

東日本大震災におけるBCPの問題点

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2011.05.18更新

情報セキュリティ大学院大学　原田研究室

No	検討項目	問題点	対応策
9	計画停電の影響	①ITは、電気の連続供給を前提としていることを自明としていた（サーバの空調、ネットワークを含めた全体に電気が必要であるが、発電機の容量が不足しているため、重要なサーバしか動作させられない） ②サーバのある箇所と、PCのある事業所が計画停電で異なる場合、サーバを前提として運用ができない ③多くの企業の処理がサーバ運用を前提としているため、企業活動がサーバとPCの動作時間に限定される ④企業のビジネスの処理の多くがワークフローとなっているため、サーバやPCが計画停電のため、承認などが遅れる（例外処理とすると、J-SOXでの内部統制を見直さなければならない） ⑤サーバの頻繁な動作、停止の手順ができていない（無停電での運用を前提としている） ⑥取引先と受発注がITで連携されているが、計画停電で連携がスムーズにできないケースがある	①停電による自社の影響を分析しておく ②非常時電源で動作させられる機器を選び、配線を変更しておき、それだけを動作させられるようにする（全てを動作させると、大規模な発電機器が必要となる） ③企業の場合、小規模な停電の場合には、車の電源を利用して、PC+携帯による最低限の通信環境が確保できるようにする
10	外部電源	①企業内部のネットワークインフラ全体をカバーする外部電源の用意ができていない　（特定のサーバを動作されることはできるが、端末まで含めたIT全体を動作させるまでの外部電源の用意がない） ②バッテリの定期的な充放電は想定されていないため、いつまで持つかわからない ③UPSは、計画停電のような長時間（3時間）の停電のための設計がされていないため、いつまで持つか分からない ④ディーゼルエンジンがあっても、燃料が必要となるが、この燃料を十分に手当てできない	①複数の企業で、外部電源を利用できるような体制を考える ②EV車の蓄電池を利用できるような仕組みを考えておく ③クラウド＋携帯＋ipadのような最小限のシステムで必要となる電気容量を事前に把握しておき、停電の際に使えるようにする

東日本大震災におけるBCPの問題点

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2011.05.18更新

情報セキュリティ大学院大学　原田研究室

No	検討項目	問題点	対応策
11	個人情報の取り扱い	①個人情報の開示がないため、不明者の特定に時間がかかった ②避難した場合の個人情報の開示の基準がないため、HPなどで流すまでに時間を要したため、連絡をとる手段を提供できなかった	①非常時の個人情報の取り扱いについての法制度を詰めておく
12	情報漏えい	①ハードディスクは津波程度では、復元が可能、第三者にNC機器、PCやサーバが拾得された場合を想定していない ②津波なのでIT機器が流出して、情報が漏えいすることを考えていなかった	①リスク分析を行って、緊急時でも機密性の保持が必要であれば、常時データベースは暗号化する。 ②サーバ機器は、停電するとハード的な扱いがないとデータを取り出せないようにする
13	バックアップ	①バックアップを遠隔地に設置するのは、同じ災害の影響を同時に受けないための対策であるが、今回の震災の範囲が広く、バックアップを含めて喪失したケースがある。 ②バックアップサイトが停電のため、バックアップとして機能しなかった ③バックアップが週1回のため、3.4-3.11の更新データが消失した（リアルタイムバックアップが必要→クラウドへの条件） ④バックアップはDailyやWeeklyのため、喪失したデータがある	①センターとバックアップセンター間の距離を見直す（同一の地震で被害を受けない→同一の災害で被害を受けない広域の分散を検討する） ②重要なデータベースの場合には、リアルタイムバックアップを検討する ③クラウドのインタフェースを標準化して、どのクラウドでもバックアップを受けてもらえるようにして、複数への分散バックアップが容易にできるようにする