災害に強い電子自治体に関する研究会「第２回合同WG」※ 議事概要

※第２回「ＩＣＴ利活用WG」及び第２回「ＩＣＴ部門の業務継続・セキュリティWG」を合同で開催

1. 開催日時：平成２４年２月２１日（火）　１３：３０～１６：１５
2. 開催場所：三田共用会議所　３階大会議室
3. 出 席 者：（主査を除き50音順）

＜ＩＣＴ利活用WG構成員＞

須藤修（主査）（東京大学大学院情報学環教授）
今井建彦（仙台市総務企画局情報政策部参事兼情報政策課長）
川島宏一（佐賀県特別顧問）
齋藤義男（東日本電信電話株式会社理事ビジネス＆オフィス事業推進本部公共営業部長）
前田みゆき（株式会社日立製作所自治体クラウド推進センタ長）
光延裕司（日本マイクロソフト株式会社公共営業本部長）

＜ＩＣＴ部門の業務継続・セキュリティWG構成員＞

伊藤毅（主査）（ＮＰＯ法人事業継続推進機構副理事長）
浅見良雄（埼玉県小鹿野町総合政策課主幹情報担当）
今井建彦（仙台市総務企画局情報政策部参事兼情報政策課長）
大高利夫（藤沢市総務部参事兼ＩＴ推進課長）
小屋晋吾（トレンドマイクロ株式会社戦略企画室統合政策担当部長）
佐々木忍（日本電気株式会社サービス事業本部グローバルサービス事業部シニアエキスパート）
林繁幸（防災・危機管理アドバイザー）

＜オブザーバ＞

伊駒政弘（財団法人地方自治情報センター研究開発部主席研究員）
鳥枝浩彰（総務省消防庁国民保護・防災部防災情報室課長補佐）
古屋修司（総務省情報流通行政局地方情報化推進室課長補佐）
百瀬昌幸（財団法人地方自治情報センター自治体セキュリティ支援室主任研究員）

4. 議題

- 第１回災害に強い電子自治体に関する研究会合同WGにおける主な意見・論点
- 藤沢市におけるＢＣＰの概要及び災害時のＩＣＴ利活用について
- 小鹿野町におけるＢＣＰの概要及び災害時のＩＣＴ利活用について
- 討議

【議事概要】

○　説明資料「藤沢市におけるＢＣＰの概要及び災害時のＩＣＴ利活用について」の３ページ目において、ＢＣＰというものを業務継続だけでなく災害対応業務にとっても役に立つような位置付けとしていた。また、説明資料「小鹿野町におけるＢＣＰの概要及び災害発生時のＩＣＴ利活用について」の７ページ目においても庁内合意における課題として挙げていた。職員の視点から見た場合、災害時にＢＣＰという通常業務の継続性の意味付け自体に苦労し、相手からの賛同を得られない経験をしたことがある。

実際は、災害時の対応業務を含め、ＢＣＰの中での連携面を含め、検討・対応している。ガイドラインの普及を進める中でＢＣＰというものの意義付けを格上げする必要があると感じている。ＢＣＰという言葉に拘束された場合、通常業務の継続計画と捉えられるが、実質は災害時の対応計画であり災害時の実質マネジメント計画である。このため、ＢＣＰという言葉に捉われず、ディザスターリスクマネジメントプランでもディザスターレスポンスプランでもよいが、ＢＣＰの位置付けを格上げして行政の内部でそのことの意義を直感的に反応できる位置付けが必要ではないかと感じた。

もう一点としては、東日本大震災を踏まえてどうするのか、東日本大震災の教訓をどう盛り込んでいくのかという点において、インターネットが発達した社会においての災害対応、例えばグーグルのパーソンファインダーあるいは他の自治体との連携が必要となる場合のように、情報というものが、庁内だけでなく庁外の助けてくださる方々と共有し業務継続面で他の自治体等の手助けが必要となる場合がある。実際上、人命救助の方に現地スタッフは全員行ってしまうので、業務継続面は他の人に実施していただかないといけない、避難所の援助についてはＮＰＯの支援を受けないといけないような状態になったりもする。

そのような災害時における自治体の役割自体が、今までのように情報を自らコントロールし自ら指揮命令をするような形態から、他の自治体等を利用した、協力者の力を活かすような意味付けに性格を変える必要があるのでは、またそういった事項をメッセージとして盛り込むと今回の東日本大震災を踏まえた内容となるのではと感じた。

○　ＢＣＰの名称というか位置付けの関係で、懸念している箇所がある。ＢＳ25777がＩＳＯ化したという話をしたが、ＩＳＯ化に伴って27031となっており、これはセキュリティの体系になっている。もう一つ、企業全体のＢＣＰ、ＢＳ25999はセキュリティではない別の体系で構成されている。そういう意味での位置付けは、ＩＣＴ－ＢＣＰはＢＣＰのため、自治体で言うと災害対応業務を含めて、そういう事業全体を絡めた時にＩＣＴというものはそれを下支えする準備だという位置付けにＩＳ

Ｏでは明確に位置付けられている。

その点、総務省はガイドラインをどのように位置付けられているか、それから言葉についてもＢＣＭではなくＩＲＢＣという言葉になっており、そこのところの考え方を整理する必要があると感じている。国際規格がそのように位置付けたという重みについては受け止めなければならないと思う。

ＢＣＰという言葉に捉われると、自治体は残った人員で何とか業務を継続しようという考え方があるため、その観点でＢＣＰはあまり作成されていない、当たり前のように実施するものであると考えている。

しかし、止めるべきものは止める。この時期は止めておいてもよい事項は明確にしておいた方が良いと思われる。そうして災害対応業務に駆けつけて力を注ぐ。

また、長期戦になった際の人員計画に弱い。一時的に配置する計画は非常に出来ているが、長期戦になった時は人を入れ替えなければならない。24時間勤務した場合、次の24時間勤務するまでは代わらなければならない等、そういうところを逆に業務継続のＢＣＰ等と含めて要員計画をもう少し見直す。更に、ＩＣＴ－ＢＣＰもＩＴ職員のみではもしかすると対応できないかもしれないため、そのような場合はＮＰＯ、ボランティア、他の自治体の協力を、どのように特に投入するかという観点がこれからの課題と認識している。

○　職員の頑張りに頼る部分が大きいという指摘があるが、その通りと認識している。大きな団体ではどのように職員の育成をするのか、小さい団体では専任で実施できる職員に対する業務時間をどのように確保するかが非常に大事と考えている。但し、その解決策は見当たっていない。

○　３月11日以降の東日本大震災で被災したある地方公共団体の動きを見ると情報政策課の大半の担当者は現場に出ており、情報システム機能の維持をする最低限の職員しか残っていなかった。実際問題として、ＢＣＰ発動時には現場優先となるため、情報政策課の必要な人員を確保できない事態が想定される。

○　第１回研究会の時にＢＣＰ策定の事例を話したが、今回のプレゼンは、それ以上に現場の臨場感あふれる形で策定されおり、訓練までされている点は良いな、と感じた。今回改めて強く感じたことは何より、作ることも大事だが教育訓練の実施が一番大事であると感じた。

ＢＣＰはプランであるため、作ることに力点が置かれるが、まずはとにかく小さく作ってどんどん訓練して大きく育てていくことができるような仕組みを構築することが大事であると強く感じた。

また、小さく作って大きく育てていくためには、ＩＣＴに強い人材がいるような自治体は別であるが、そうでない所、弊社においても小さな事業所は同じだと思うが、小さな自治体等では共通モデル、例えば重要業務は何か等をこの中である程度決めて作成していくことが重要だと感じた。

もう一つは、とにかく作ることが大切だ、実際に作った後色々考えた、と聞いた。勿論そうであるが、最初はなかなか考えること自体に時間が取れず、人もいないため出来ないと考えられる。まずは作る場において、一人でもあるいは一人ですら時間を割けない状況でも作成できるような様々なモデ

ルや、リファレンスモデルのようなものをこの中で作成していくことが重要だと強く感じた。

上記を作成していただいた後は、企業なら当たり前だが、社長の一声で作成しろと言って作らせる。作成した後については、飴と鞭ではないが、色々なプランはこちらで準備します、支援をします、ということを伝えることで作成させていく。そもそもこれは作成した方がよいものというよりは作成しなければならないものと思われるため、とにかく作成させ、その後は訓練して大きく育てていくところに力点を置いたプランを作成していきたいと思う。

○　全国の自治体の数を考えた時に1,700位の自治体があり、どういう風にＢＣＰに取り組んでいるか、という認識が非常に重要であると考えている。

第１回研究会で申し上げたように基礎的な連絡先の確認、基本的なデータをバックアップするという、お金をかけずにすぐにできるものについては、かなり取り組んでいるという実態がある。そこは一つのポイントと考えている。

これ程たくさんの自治体の中で、殆どの自治体は人口10万人以下の自治体であり、いかにそこできちんと立ち上げるか。先述したが、既にお金をかけないで出来るものはかなり取り組めている。次のステップとして、システムを使用した、ある程度お金が必要な世界をいかに実現していくのか、その仕組みを何らかの形でこの会合の中で何か案が出ないかと考えている。

例えば、被災者支援システムのようにここまで仕組や仕様がはっきりしているものがあれば、それを利用し、お金を極力かけないで共有できる仕組みは無いのか、また、災害時のコミュニケーションが非常にキーになるため、ソーシャルネットワーク等、色々な仕組みを提供、共有することによって、連絡手段が複数必要な場合に、その中の一つとして使用出来るような仕組みを作ることは出来ないか。

そういう具体的な、次の第一歩に踏み出せる仕組みというものを考えていくと、全国の自治体としても、もう一歩次の段階にステップアップ出来るのでは、と考えているところである。

○　それに関連して、総務省の他の部局で、現在ＩＣＴを活用した新しいまちづくりの検討をしており、その中で、今回の震災時に衛星をきちんと使用できなかったといった話が挙がった。衛星を自治体・病院・避難所になりうる教育施設で使用できるようにする、そのためには普段から使用できるようにしておかなければならないということでその検討が必要であると。

その他、通信網においてアンテナ基地局にほとんど電気が届かなくて携帯が使い物にならなくなったが、これについて、太陽光発電をアンテナ施設等に公的な資金で普及させる必要があるかもしれない。そうすると、携帯電話が使用できると同時に携帯の電源もそこで補充出来る、ということでそれは考えなければならないと思っている。そういうことについて自治部局とそういった動きも連動していただくと新たなシステム、これをどのように使用するのか、といったことについても描けると思う。

○　質問であるが、民間におけるＢＣＰについてはサードパーティーに対するコントロールがうまく

できないと結果としてビジネスがうまく続かない。自治体にそういった事象がどのくらいあるかはわからないが、例えば市区町村として県に依存するような事象、あるいは共同で何か生じた際に実施するような繋ぎ込みといったことを実施しているのか。

それからもう一つ。策定されたＢＣＰを自治体にコピーして使用していただいても構わないという話を出していただいたが、結果として、そもそもモチベーションがないとコピーしても使わない、維持をしない、システムが新規に一つ増えるとそれもケアできない。どこからモチベーションがやってきたのか、ということを教えていただきたい。

○　ＢＣＰにおいて、サードパーティー、県や他との関係、民間企業に協力いただかないと実現出来ない事項はたくさんある。例えば、数名派遣でＳＥを雇っているが、会社に戻るのか、こちらに戻ってくるのか、といった関係については事業主と調整を取っていただく対応を取ってもらっている。

各メーカー向けに本当は協定を結んだり、契約を結んだりといった形を取りたかったが、なかなか特定のユーザに対して契約を結べない。企業としてはなかなか言い出すことができないが、実態としては担当ＳＥ、担当営業は真っ先に駆けつけてくれる。

今回の被災時においては、どちらかというと人間関係や普段来ている人達との関係で、企業から行くようにといった指示以前に、どうだったかという声かけから始まり、来てくれた実績がある。こういった信頼関係、人間関係は大事と感じている。

県との間は縦の繋がりであるため、正式な防災計画のルートでの情報伝達という形に留めているが、自治体では中での組織にIT推進本部会議、セキュリティ委員会、地域IT推進委員会というものがあり、県の課長や地域の人達が含まれた会議があり、そういったところで連絡体制やＩＣＴについての取り組み、お願い、といった横への密度を高めている。

先ほど話に挙がっていた中で、ＢＣＰを作成するメリットの一つとして人員を組織の中で確保するという話があった。災害対応業務、地域防災計画に基づく配置計画が組織として決定されている。自治体においてＢＣＰを策定することのメリットとして、組織として初動においてＢＣＰが並列して発動し、そちらに専用の人員を割り当てるという計画が承認されており、ＩＴのＢＣＰのための要員は確保出来ている。これが計画を策定するメリットの一つと認識している。

○　首長がＩＣＴ－ＢＣＰを理解していないと、現場に全員行けといった状態になったりしてしまう。

○　民間との連携が話題に挙がっている。業務支援システムという観点から課題がいくつか出ていると認識している。

今、民間、ＮＰＯ等、また小さなＩＴベンダーである地場の企業が各被災自治体と話をする際、無償の話等、色々な協力を持ちかけている。

そこで１点ブレーキとなっているのは、被災者支援システムにより台帳を作成するが、そのデータを公開できない。このため、当該地場のＮＰＯに説明してもそこがブレーキとなってなかなか進まないということが、どちらかというと自治体の現場の人達から話があり、これは地域防災計画になるかもしれないが、ＩＣＰ－ＢＣＰの観点からそういったところに対する提言ができないかと思う。

もう一つ、これもＮＰＯの話となるが、仮設住宅に対して、例えば、暖房を提供したり、ご老人の方のところに回りたい等様々な申出を行ったところ、結局自治体から明確な指示ができないとのこと。どのようなことかというと、ある仮設住宅のご老人の所には１日３回、別々のＮＰＯが訪問してきた一方、ある地域には全く訪問が無い。そういった差が出ている実情もある。

ＩＣＴとは直接関係ないが、自治体がリスクマネジメントできるような支援をこの会合から発信できないかという思いがある。

○　被災者データの活用については恐らく、自治体等は法令遵守によって動くと思われる。総務省からガイドライン等を出していただき、それに基づいて条例化する等あればかなり展開が異なる。これは本研究会内での提言と関連して次の動きが取れるといった点で重要と思われる。

○　何点か現場経験に基づいて話をさせていただきたい。まずＢＣＰができた後、それを実効性あるものにするために訓練をするのであるが、私の経験からして、また国が今まで実施した訓練、我々が独自に計画して実施した訓練もだが、やはり訓練自体に実効性がないのが、殆どの自治体で実施されている訓練ではないのかと思っている。その点について、訓練を並行して行っていけるような組織体制を作成しておくことが必要ではないかと思われる。

やはりあくまで訓練は訓練ということであるため、最終的には出来あがり訓練となってしまう。従って、そういった点を重点的に行っていくと途中の過程が訓練のための訓練となってしまう。災害がその訓練通りに来てくれればよいが、決してそういう風にはならない。

それから、災害に対しての一番大きな点で自然災害は地震以外ある程度予測は出来るものであるため、やはり地震に特化した本当のＢＣＰ、ＩＣＴ－ＢＣＰというものを重点的に考え、それを応用した残りの自然災害というところにセットしたほうが良いと感じている。

それと地盤の話、比較的固い所であるといった話について、要は一律全国同じような方向性で対応を作成していって本当に良いのかどうかといった点も議論となると感じている。

昨年の台風12号の際に、深層崩壊というものがクローズアップされた。これについては昔からあったが、今後異常気象が続く中、災害によっては深層崩壊が増えていく。そうなると地盤が固い、弱いという問題ではなく、ご存知の通り深層崩壊の中で一番大きなものに台湾で80メートル崩れたというものがある。地盤面から80メートル下までが同時に崩れてしまうような事態、これには対応できないと思う。

まずそこまで対応できるようなものを計画することは無理ではないか、と言ってしまえば終わりであるが、やはり地盤が固いから少し程度は弱くしましょうといった点はいかがなものかと思っている。そういった点を含めて今後の計画に応用・運用していただければ良いと思っている。

それともう１点、これは聞いてみたいが、例えば本体サーバは他府県の方で有しており、そこは災害に遭わなかったためデータはそこに蓄積されている。では、それを取りに行くために、実は自分の自治体のＰＣ系が仮に全部駄目になった場合、どこかからＰＣを持って来なければならない。それを例えば、個人が有しているＰＣを持って来て、それにアクセスをさせ業務に反映するということは、そういう方法を取らざるを得なくなった場合、良いのだろうか。

何故このようなことを言うのかと言うと、殆どのＰＣはセキュリティが確保されている中で使用

されているが、どこかでセキュリティが守られない状況下で使用しなければならなくなった場合、例えば何かがそこに入りこんでしまってサイバーテロが発生する、というようなセキュリティの確保という点については如何なものか。

○　東日本大震災で被災したある地方公共団体において、ＢＣＰはなくとも結局の所、震災後の３月16日くらいには殆どの機能は復旧したため、反省点はあるがそれはそれで何とかなった。何故かというと、「官庁施設の総合耐震計画基準」などの基準が存在し、それに準じた建物及び設備を有している。また、メンテナンスを真面目に実施していた。窓口業務を支える基幹系システムなどにおいては、システム障害発生時の対応を含む日常の運用の手順についてガイドラインを策定し、マニュアル化しており、その内容も常に見直している。

運用には万全を期しているが年に数回は、障害が発生する。障害が発生した場合、夜中であろうが昼であろうが、職員は必要な場所に赴き、民間事業者も皆行く。来なければ呼び出す、ということを常に実施している。訓練のための訓練は実施していないが、実地において速やかな復旧を心がけており、それが訓練になっている。

今回の震災時も即全ての民間企業の皆さんに駆けつけていただき、問題無く復旧した。

必要に迫られ実施せざるを得なかったのだが、訓練のための訓練でなく、昼夜を問わずいつも集まっているということを実施していたため、比較的良かったと思っている。

東日本大震災で被災したある地方公共団体では、災害直後の状況を切り抜けると、次に復旧・復興のための業務が大量に発生した。現行のＩＣＴ－ＢＣＰガイドラインにはあまり記載がないが、このような業務にどのように対応するのかを明らかにするために、ＢＣＰが必要だと感じている。見直しにあたっては、このような点を重視した記載が必要だと思う。

その他必要と思われる反省点としては、通信網は２重化していたが、それでもつながらない時間、場所が発生した。またインターネットを重視する必要があると考えていたが、そこも一時的に使用できない時期もあった。これは、通信事業者、インターネットプロバイダー側の問題でもあるので、このような状況を踏まえた対応が必要だと思う。

先程話に挙がったが、前提条件として、自治体では対応できる限界がある。今回のように通信網が数ヶ月動かなかった、周りの環境が全く無くなった、物も買えない様な話になると、いくらＢＣＰを策定してもどうしようもない。

東日本大震災で発生した状況をどこまで、今回の見直しに反映させるのかは大きな課題だと思う。どの程度の状況までをＢＣＰの被害想定の範囲とするのか考える必要があると思う。現行のガイドラインを読んだが、２部と３部では被害想定に大きな違いがある。３部だと話が広がりすぎているような印象を持つ。

一番言いたいのは、日常業務をしっかりしていればある程度対応でき、そういったことを重視した簡単なＢＣＰ的なものがあり、更に今のガイドラインにあるような項目があるという形が必要ではないかということである。

○　計画をしっかり策定している箇所や日頃からしっかり手続を実施しているような箇所等、様々存

在するが、いずれにしても、何故こういうことを意識して実施する必要があるのかという意味、意義を理解していただくことが、もし作成されている所、あるいは作成されていないが行動されている所があれば大事であると考えている。

被災にあった箇所で被災者支援システムが必要であるということが分かったということであるし、それ以外で大都市にて質問を受けるものとして、小規模な自治体からしてみるとコスト的な負担が大きくて出来ない等、色々な事情があるとは考えられるが、意味・意義を示せるのかが大事である。

また計画を策定する中で、最低限何を実施することが必要か。我々も十分に利用者の期待に添えられない箇所もあったが、被災後沿岸部では、設備、電話局舎等流された箇所が沢山あった。色々な企業、自治体から修理依頼等いただいたが、全部に対応することが無理であったため、場面によっては不適切な発言で申し訳無いが、捨てる勇気が必要であった。

よって、最低限何をする必要があるのかということは今回計画を考える中で、捨てる勇気ではないが、本当に何が最低限必要なのか、被災発生０時間から３時間半以下の場合等、そこがきちんと整備出来ていれば、立派な100％の計画書ではないのかもしれないが、まだそこまでの気持ちになっていない自治体においてやってみればやれるかもしれないといった気持ちになっていただけるかと思う。

そういった場面を想定した場合、恐らく職員の方々は被災者の方の対応のため不在となっている、実際行かせていただいたが、色々な所でＩＴの担当者が不在となっていた。ということは、他の自治体か非被災地の方からの応援が入ることになる。

最低限何をすべきかを整理できれば、そこについてはマニュアル本というのか、業務の標準化なのか、そういったものが整理できれば応援部隊の人達も効率的に対応できるのではないのかと感じた。

○　訓練について申し上げると、これは日本を代表する通信事業者の幹部が話していた事例であるが、非常電源を立ち上げる際、通常電源を使用しないと立ち上がらない事象があった。要は電力が届かなかったため電話網が麻痺した。

今回の後すぐに改修をして非常電源を立ち上げることができるレベルにした。これは訓練をしていればわかったはず。実施していなかったためいざという際に回らなかった。今回の経験を活かして上手くなったと思うし、上手く回せるように訓練は必要であると思う。

マニュアル化しすぎて、形式化し、それしかないとしてしまうと却って動けなくなる恐れがある。現場の臨機応変さから指揮権の移譲もある程度認めるようにしなければならない。

ある地方公共団体では被災者支援システムを有していたが、その中心人物が津波でお亡くなりになったため、使用できなくなった。これに困り、緊密な関係があった地方公共団体にお願いし、その地方公共団体が動かしている、そういう意味では自治体連携でその後、上手く動けた、ということもある。

これから話す例は場違いかもしれないが、最近、第２次世界大戦の巡洋艦の乗組員の本を読んでいるが、砲撃発令指揮所というものがあり、そこが爆弾でやられてしまうと砲撃の発令が出ないということを実戦で経験したとのことだった。その後、誰が指揮系統を取るのかということを、やはりその後訓練を重ねて、ここがやられるとここが取る、ここがやられるとここが取る、ということ

を緊密に実施する。実際に訓練等していないとそういったことがわからず、それは重要と思われる。

（セキュリティ上、個人PCを庁内LANに接続してもよいかの問いに対しての発言）

○　決定的な答え等ではなく、いくつか事例もあったが、自宅待機で業務を継続することを前提で構築する必要がある。それが構築されていれば、自宅のＰＣが業務のネットワークに繋がるということを前提として置いておくべき。そのために、ある程度自宅のＰＣにはこの程度のセキュリティをしなければならないといった縛りをしている企業もある。もう一つは貸与しているケースもある。但し、貸与している予備機が常に動くか分からないというケースもあったりするようであるため、その辺の注意は必要である。

今回多かった事例は、停電のため、自宅で業務を行わせたが、データを消すという指示をどこで出すか、自宅で業務に繋いだＰＣも恐らくここには業務のデータがあるが、このデータはきちんと消しなさい、といった指示を出すことを大体の企業は失念していた傾向があり、しばらくその部分が脆弱であったという話があった。

この流出した分で漏えいしたかどうかは分からないが、今回散見したケースとして、この事象が起こったために再度連絡網を作成し直す企業があった。それが狙われた、あるいは社員が流した、といったことが結構あった。そこを注意しないと、連絡網を作成すると一気に会社個人情報が流出したケースもいくつかあったため、こういったケースは少しずつ活かしていかなければならない。

○　例えば、ある地方公共団体においては公務では絶対個人のＰＣは使用するな、という指示を流している。このため、個人のＰＣは絶対使用できない、持ち帰れない、データを持ち出すこともできない。

では、それがやられた際にどうするかというと、どこかを使用しなければならない。企業が自宅のＰＣをある程度業務用として認めています、というシステムを採用出来れば良いかもしれない。

○　あるいは近隣の自治体から拝借するような協力関係を構築しておく。伺った話では、自衛隊員等が皆ＰＣを持ってきて繋ごうとするため、セキュリティポリシーの不一致が生じて混乱したという話があった。持ち込みＰＣに対する最低限のセキュリティの準備を整えておく。今はＷｉｎｄｏｗｓ系のＰＣが非常に多いため、ある程度共通で動く基盤というものは比較的準備しやすいのではないか。

○　ある地方公共団体では、セキュリティに関して、災害時でもセキュリティの確保が大事と考えている。例えば、端末はシンクライアントのＰＣである。従って、極端に言うとＳｔａｎｄ　Ａｌｏｎｅでは動かない、ではどのように動かすか。

ＵＳＢにＬｉｎｕｘとＯｐｅｎＯｆｆｉｃｅを入れて、Ｓｔａｎｄ　ＡｌｏｎｅでＰＣとプリンタがワンセットで組合せて動くような環境を構築している。そういった方法でいざとなった場合、組合せによって動くよう、ある程度の環境があれば動くような形で、こちらがセキュリティを考えた対策まで用意することができるのではと考えている。

テレワークというのも必要な手段であると考えており、今後検討すべき課題もあろうと思う。

その他、ＰＣが不足するため、被災地では使用できるものはとにかく集めること、これは絶対であると思う。それに対し、どのような設定を施して、どのようなポリシーをかけて動かすか、この件につい

てもＰＣを構築する側の問題なので対応できると思っている。

また、個人のＰＣを持ち込んでは駄目である、データの持ち出しも駄目であるというのは、平常時ではその通りであるが、災害の時どのようにするか。セキュリティを担保した運用はできないか、というと、全くないわけではない。セキュリティを確保するための縛りであり、セキュリティさえ確保できれば自宅で作業をしても良い。

場合によっては通信が駄目であるという前提もあるが、ＵＳＢを、ＰＣに差し込むとそのデータの加工はできるがそのＵＳＢメモリーの中だけの加工しかできずコピーもプリントもできないといった仕掛けもあるため、そういった位置付けの検討や手段があるということをリストアップしておいて、いざという時に何を選択するのか、ということが大事であると思う。

セキュリティに関しては災害時という扱いであるため、災害時における個人情報保護法や個人情報保護条例に関しての除外の規定が存在する。その中で、どこまで運用するのかということに関して、垂れ流しにするのではなく、コントロールできる配下で実施する、災害協定を結んでいる自治体間で実施する、等様々な方法が考えられる。

その際、どのような答えを出すかという点について、我々はこういった災害時における個人情報保護という有識者のセミナーに管理職を全員集めて話を聞かせた。答えは出していないが、避難所の責任者になる、その他様々な責任者になる可能性があるため、このような個人情報について訊ねられるとこういった回答をしなさい、といったキーワード的な回答を身につけていくような活動を行っている。そのような啓発活動は大事であると思う。

セキュリティの意識やＢＣＰに対する意識をどのようにするかという時、人に対する研修や教育といった対応、人的対応が一番大事であると思う。そういった活動を定期的に実施していくことが大事であると思う。

○　ＢＣＰというのは特別仕様の、何年かに一度に来る時のために策定されるものではなく、日常業務の中でそのエッセンスが組込まれるようなＢＣＰであることが非常に重要である。

在宅で仕事をするといったことに関しても在宅勤務という、通常でもワークライフバランスの関係で在宅勤務ができる。ＣＯ２を減らしたいという事情もある。在宅勤務モードでＵＳＢを差せばセキュリティ上、完全に保護された状態で、自宅のＰＣにて本庁舎のＰＣ画面がミラーして映る。その台数と災害が起こった際、在宅勤務をするであろう台数を概ね揃えて日常勤務シフトと非常時モードをかなり類似させる。

そうしないと負担が大きく、非常時モードのためにシステムを準備した場合、そのための待機オペレーションコストを考えるとできないと思われる。これは非常に重要かと思われる。

またデータレベルの検証を、総務省でケーススタディーを実施するならば、個人情報保護法とも関連するが、何故このデータを出したのか、出していなかったのか、災害が発生すると、どこで災害が起こっているか、誰がどこに避難をしているか、どこで通行止めが発生しているか、災害対策本部は何をまとめて頼まなければならないのか、データパスとデータを連携、統括し、マスコミに公表し、災害対策本部として決定し、派遣する等で忙殺される、といった議論を生々しく議論していただくと、これをしなければならないとの実感を職員として有することができる。

是非シミュレーション的な議論の中でデータレベルの議論を突っ込んで実施していただきたい。そう

すると個人情報の問題も如実に出てくる。現実論としては、一回入力したデータを再入力するような事象も多々あり、七転八倒している。従って、その点を議論していただきたい。

○　当面議論を集約していく段階ではないし、意見を出すことが必要な状況である。

日本にＢＣＰが入ってきた時期には、ＢＣＰを作成するということに関しては様々な知識を有していたが、ＢＣＰを運用するということに関しては知識を有している人が殆どいなかった。そのため、日本に入ってきたガイドライン、最初に出来上がったガイドラインについてはどのように作成するか、ということについて徹底してフォーカスしていったというのがそもそもの歴史の経緯としてある。

それに基づいて2005年に内閣府が発表したが、その時点から一斉に様々な企業がＢＣＰの作成を開始、大変な厚さのＢＣＰを策定した。

その結果現在どうなったかというと全然改定できていないのが実情である。東日本大震災が起き、変えていかなければならない箇所が多大にあるが、それは全部見直さなければならず、情報を加える、また文章を加える、ということを実はずっと繰り返しているという歴史があることを認識いただきたい。

先程から意見にも出していただいていたが、そもそもＢＣＰとは何かという定義をきちんとできていない。

不測の自体が生じた際しなければならないことをもっと早くするためにはどうすればよいか、単純にそれを考えるためにＢＣＰを作成するのであるため、逆の言い方をすると、今、何かが起こった時には、自分達の対応が遅い、ということを分かっていない。想像力というかイマジネーションがきちんとあり、その上で実施すべきことが明確になっている。

従ってここで言いたいことは、こういうことをしなければならない、といった答えをいきなり出すのは危険だということである。どのような事態が考えられるのか、自分達がどのような事態に陥ってしまうのかということがしっかりと意識されれば、実はそれがそのままＢＣＰをしなければならないことにつながる、ということが必ずついてくる。

よって、そういった意識無しにこういった改装が必要だ、あれをすればよい、こういうフォーマットでこういうことを記載しなければならないということを実施した途端、ＢＣＰというものが非常に分かりづらいものとなってしまう。

従って、2005年から2007年くらいにかけて大変なＢＣＰを作成したことで一番苦労している。皆それらを捨てようとしている。はっきり申し上げてＩＳＯ、ＢＳ25999からは離脱しようとしているくらいである。非常に負荷がかかりすぎている。毎度のように更新の審査を受けなければならないし、勉強もしていかなければならないという負荷に対してどうなのかということに対して、嫌がっている企業が圧倒的に多いといった状況が現実としてある。

それからＩＴに関して、ＢＳ25777の話も上がっていたが、要はベースとしては、ＩＴＩＬ、ＩＴサービスマネジメントというＩＴの管理をどうするかという考え方の中のＩＴサービスのコンティニュティマネジメントという一つのライブラリである。

従って、本質的には災害対応というか、ＩＴサービスをどのように継続させていけばよいか、様々な事象においてもＩＴをどのように継続するかという考え方が記載されたものであるため、本質的にこれは幅広く見ると、通常の障害対応、運用性の向上等という色々な答えに繋がっていくはずものであるが、ＢＣＰという違う所からの切り口からスポットライトを当ててしまったため、非常にわかりづらくなっ

てしまっている。こういった点をばらしていければ非常に画期的な、画期的というか本来の方向に少しＢＣＰを戻していけるのではと考えている。

もうひとつ出ているようで出ていなかった重要な項目として、ベンダーの管理があげられる。自治体の方々の情報システムというのは非常にベンダーへの依存が多いということを考えた時に、ベンダーは継続性に対してどのような保証をしてくれるのか。まず保証はしない、絶対に。

そのような中でベンダーとの付き合い方、それは人間関係と一緒であるが、現実的なことを考え、公共災害時を考えた時に、駆けつけてくれる、これを保証される、色々な所に行かなければならないという中でどれだけの継続性が担保できるか、ということに関しても、やはりベンダー管理の仕方ということに関して、またそこにリスクがあるということに関してもしっかりとして認識を持っていただかなければならないと考えている。その点が気になっているところである。

少しまだ幅広く議論しながら、あまり型にはまらない、本質的にあるべき、要するに先述の通り災害時、被災時に自分達が早く対応していけるかどうか、ということを考える。

そのためにすべき事項は何か、その答えは与えるものではなく、発生しうる状況というものをどれだけ考えさせるか、というところのやり方、他の部署だけでやるというやり方もあれば、最初からこういうケースを想定していくというやり方もある。

○　日本人は型に嵌めたがる。このため、緊急事態に対しては結構災いをもたらす、要するに判断できない状態に陥る可能性があるため、その辺についてはここに集まっている方々の英知を集め、現場それから体験性、それらを両立させるような方向で考え、このＢＣＰをまとめていただきたい。

現場の首長を動かすということになると、実際の災害にあった時の利活用、この点をかなり言わないと、なかなか首長にも本気で取り組んでいただけないため、その観点も議論したいと考えている。

以上