

富山大学における BCP の検討

Examination of BCP in University of Toyama

沖野 浩二 †, 金森 浩治 †, 黒田 卓 †, ‡

Koji Okino†, koji Kanamori†, Takashi kuroda†, ‡

okino@itc.u-toyama.ac.jp, kanamori@itc.u-toyama.ac.jp

富山大学 総合情報基盤センター †

富山大学 人間発達科学部 ‡

University of Toyama, Information Technology Center †

University of Toyama, Faculty of Human Development ‡

概要

3/11 以降, 多くの大学において事業継続計画 Business Continuity Plan(以下、BCP という。)の検討が行われており、いくつかの情報系センターでは、発電機の設置や学外への業務委託等が行われている。

しかし、これらを行う場合のコストや全体最適を検討している事例は、少ない。本論文では、リスクをモデル化し、いくつかのケースを想定し、それぞれに必要な対策コストを概算することにより、どのような対策を行うか検討した。その結果、システム集約化を行うことと学内と外部にあるデータセンター(以下、DC という。)を活用することにより、BCP を意識しながら、運用コストを低く抑えることができることが判明し、これらの対策を実施することになった。

キーワード

情報系センター運営, BCP

1 はじめに

BCP は、自然災害等の緊急時に業務を継続あるいは早期に復旧するための手順や対策を含めた計画であるが、大学において手順や対策までを議論している例は少ない。また、議論されているのは、情報系センターシステムの場合が多いが、これは、情報系センターの責任範囲が教育系システムの運用が中心であり、事務系システムを含めた、大学の情報システム全般を統括する組織ではない場合が多いからである。

加えて、日常の情報系センターが持つべき役割は、システムだけでなく、ネットワークやセキュリティなど他の要素も大きなものであり、これらは大学の教育・研究を支える基盤となっている。これらの他要素も、災害時に必要であり、BCP を検討するうえでは、これらの通常業務の全般の維持をどのように確保するかが重要で

ある。

大学における Business は、情報系センターが運用されることではなく、教育・研究が継続的に維持されることであるが、そのためにどのような要素があり、どの順位でリソースが割り当てられるかを議論されることは少ない。これは、大学に求める Business が管理職・職員・教員等の立場により大きく異なるからである。

さらに災害時には、教育・研究の維持より優先される事項として、学生・教職員の安全の確保や情報収集はもちろんであるが、大学によっては災害拠点病院であったり避難所に指定されているなど、いろいろな要素が考えられる。また、地方大学においては、その経済規模は、小さいものではなく、この経済活動の停止は、地域へ大きな影響を及ぼすこととなる。

このような中で、情報系センターの BCP は、大学の

情報システムの運用を維持することになり、災害時においてもシステムの運用が行われることが主眼になる。そのため、DC を利用したシステム運用や発電機の整備につながることが多い。しかし、これらを利用する確率やコスト評価、システムを運用するための資源評価を行っている事例は少ない。現在は、3/11 の印象が強いためこれらの予算を獲得することが可能であるが、今後、これらの予算を確保し続けることの保障はない。そこで、運用前にコスト評価を行うことにより、今後の負担を予測し、どのような対策を行うか検討した。

2 想定するリスク

本学は、3 キャンパス (五福・杉谷・高岡) に分離しており、その他に附属学校および寮を有している。3 キャンパス間の距離は、図 1 となっており、3 キャンパスに設置されている学部および機能は、表 1 の通りである。



図- 1: キャンパス配置図

キャンパス間の直線距離は、五福-杉谷 直線 5km, 五福-高岡 直線 18km, 杉谷-高岡 直線 16km となっている。

表- 1: キャンパス毎機能

キャンパス	学部等	緊急時施設
五福	経済・人文・人間発達 理・工・本部	避難所指定
杉谷	医・薬	附属病院
高岡	芸術文化	避難所指定

各キャンパスは、災害時にも運用を求められる、病院および避難所となっている。このため、どのキャンパスにおいても、災害に対応する必要がある。

一般に想定されるリスクは、下記のものがある。

天災 地震、津波・水害、落雷

人災 建物破壊、火災、停電、漏水、感染症

表- 2: 地理的環境

	五福	杉谷	高岡
地震	断層直下	断層近く	断層なし
海拔	10m	50m	7m
水害	1m	なし	0.5m

3 キャンパスの地理的な環境および水害発生時の影響は、表 2 が想定されている。地震発生時の最大震度や津波の到達予想については現在、想定中である。また、火災・停電のリスクに関しては、どの場所においても同等と考える。

3 通常時と非常時のシステム運用

通常時と非常時の運用に必要なリソースを検討した場合、まず、非常時よりも通常時の運用が停止せず、安定的に動作することが絶対な条件となる。加えて、想定されたリスクが発生した場合でも、通常システムが安定的に稼働すれば、バックアップリソースを準備する必要はなく、災害時にも稼働することができる設備を整備することが重要となる。このような点から耐震・発電等の機能を有した DC にてサーバを運用することは有意義だと考えられる。

ただし、想定されるすべてのリスクにおいて、次の 2 つの点を考慮する必要がある。1 点目、情報を一か所に集約することは、火災や水害等の発生時には、完全な情報の消失につながる可能性があるため、遠隔地バックアップの検討が必要である。2 点目として、強靱な DC を準備したとしても、DC が遠隔地にあった場合には、大学までの回線や電源の保障がない場合には、必ずしも学内から利用することができないという点である。これは、大学に電源が供給されない状態においては、近隣に住む教職員・学生も同様に、停電のため十分なシステムを利用できないという可能性があるということである。加えて、業務システムを在宅から利用するためには、学内規則の整備およびセキュリティをどのように維持するかを検討する必要がある。

現在の大学における教育・研究では、ネットワークがない状況で十分な活動ができることは少ないため、電源が回復した後は、早急なネットワークの再稼働が求められる。サーバを外部の DC に設置したとしても、学内のネットワーク機器は外部の DC に置くことはできないため、これを収容する建物やラックは耐震化すること

が必要となる。もちろん、電源がなければこれらの機器を運用することはできないため、発電機等の電源確保は重要であるといえる。ただし、学内に対して電源供給がされていない状態においては、各棟などに設置された HUB やユーザが利用する PC の電源もない可能性が高いため、すべてのネットワークを維持する必要性は必ずしも高くはない。災害時にこれらのシステムを利用したい場合には、システムだけでなく、ネットワークや情報機器の利用環境にまでの電源供給を考える必要がある。

これらを総括すると、BCP を検討した場合には、各キャンパスにおいて、ネットワークを収容する建物は、耐震性が求められる。サーバに関しては、建物はある程度距離が離れている二つの建物が必要となる。電源に関しては、利用環境を想定して考える必要がある。

ここでは、二つの建物を学内外または別キャンパスに配置することを検討する。学内に情報機器を設置する場合には、建物と機材が無事であれば、その建物に発電機を準備し、最低限の情報機器にだけ電源供給し、その建物で業務の継続ができる。しかし、システムを収容するために外部 DC を利用する場合には、通常業務および業務継続を検討する場合には、

- 大学から非常時に移動できる距離であること（保守の点から）
- 非常時の業務室が確保できるか

を検討する必要がある。

4 DC への回線速度

4.1 実験の目的

予備実験として、遠隔地にサーバを設置した場合に、どのくらいの帯域が必要かを評価するために、NAS へのデータ保存に際し利用できる各種転送プロトコルの転送時間、回線速度変更、NAS の同期に伴うデータ転送時間の影響を計測する。ここでは、遅延のない回線を標準値とし、回線の遅延による速度への影響は、UDP は影響しない、TCP の遅延と転送量は、式 (1) で与えられるので、

$$MaxThroughput(bit/s) = \frac{TCPWindowSize}{RTT(RoundTripTime)} \quad (1)$$

遅延が倍増するとともに、その性能は半分になるといいう理想状態を想定し、評価を行うこととする。

実験には、QNAP 社製 TS-469L(内蔵 HDD : Hitachi HDS721010CLA332(1Gx4)) を使用した。TS-469L は二台以上使用することでリアルタイムリモートレプリケーション (以下、RTRR) が使用できる。また RTRR 実行

時のデータ転送内容を暗号化したり、データ転送内容を圧縮することでトラフィックを軽減することも可能である。

回線速度の差を評価するために、AlliedTelesis 社製の以下の二種の L2 スイッチを使用した。

- CentreCOM FS708TPL(通信速度 : 100Mbps)
- CentreCOM GS908S-TP(通信速度 : 1000Mbps)

実際に転送するデータとして、以下のファイルを作成した。

- 100MByte(zip 圧縮時 0.1MByte)
- 1000MByte(zip 圧縮時 1MByte)
- 1000MByte(zip 圧縮時 1000MByte)

4.2 実験 1

実験 1 では、遠隔地の DC にサーバを設置した場合の帯域評価を行うために、PC から NAS へのアクセス速度を L2 スイッチを変化させることで評価を行った。速度は、100MByte ファイルの転送により評価を行った。

表- 3: プロトコル別 NAS へのアクセス速度

	1000Mbps	100Mbps
FTP(bin)	18.6s	91.3s
CIFS	19.2s	91.6s
FTPEs	53s	92s
SFTP	100s	113s

4.3 実験 2

実験 2 では、DC 間でのストレージデータの同期速度を評価するため、NAS-NAS 間を RTRR した場合の NAS1-NAS2 間のファイル転送時間を計測した。ストレージ間の速度を L2 スイッチを変更することで評価を行った。ファイルは、圧縮できる 1000MByte(表 4) のものと圧縮できない 1000MByte(表 5) のものの二つを利用し評価を行った。

4.4 実験考察

実験 1 の 100MByte の転送結果から、Word 等で画像入りのファイルを利用するような環境を想定した場合には、反応速度を確保する点から、ユーザがリアルタイムでファイルサーバにアクセスする場合 (CIFS) に

表- 4: RTRR による同期速度:zip 圧縮 1MByte

		1000Mbps	100Mbps
SSL あり	圧縮あり	39s	40s
SSL あり	圧縮なし	67s	96s
SSL なし	圧縮あり	40s	41s
SSL なし	圧縮なし	22s	101s

表- 5: RTRR による同期速度:zip 圧縮 1000MByte

		1000Mbps	100Mbps
SSL あり	圧縮あり	182s	182s
SSL あり	圧縮なし	69s	95s
SSL なし	圧縮あり	137s	141s
SSL なし	圧縮なし	23s	101s

は、回線速度を 1G 以上必要であることが判断できる。また、CIFS では tcp を利用するため、DC を設置する場所への遅延を考慮することが必要となる。

実験 2 の結果から同期を行う場合には、圧縮効率が悪い場合には、圧縮を選択しないほうが良いことがわかる。実際に SSL 暗号化を行い非圧縮で運用を行った場合を想定した場合には、現在のストレージの利用量 10TByte で一日の変更量がその 5% の 500GByte と想定した場合には、100Mbps の場合でも 500GByte/1000MByte x 100 s /60 /60 = 14h 程度で同期が終了するので、100Mbps で問題ないと判断できる。

これらの結果、DC にサーバを設置する場合には、1Gbps が望ましく、データのバックアップのみを行う場合には、近隣の DC ならば 100Mbps でも可能であると判断した。

この実験では、遅延は 1ms 以内である。実際には、近隣の DC に対しても数 ms の遅延があり、富山大学から金沢大学ノードまでの遅延平均が 10ms 程度であることから、遠隔地では 10ms 以上の遅延が予想される。遅延が 10ms とした場合には、実測した時間の 4 倍程度かかると想定される。サーバを遠隔地の DC に設置する場合には、クライアントサーバモデルから Web ベースシステムに変更するなど、遅延の影響を受けにくいものに変更する必要があることも確認できた。

5 DC のコスト評価

5.1 コストモデルの作成

2 か所のシステム設置場所について、次の 2 つの要素を変数として導入および運用コストの評価を行った。

DC の設置場所 学内, 学外

バックアップ内容 システム+データ, データのみ

ここでは、システム構築費用 (a)、ラック借り上げ費用 (b)、回線費用 (c) として、バックアップ構築にかかる費用をシステム構築費の 10%(データのみ) および 70%(データ+システム) と想定し、年間の保守費はメインおよびバックアップの構築費の 20% としてモデルを作成した。大学に設置した場合には、ラック借り上げ費用は 0 円とし、ラックの本数は、システムが n 本、データバックアップ専用の場合には 1 本とした。

現状と大学および DC に設置する場合、参考として DC にすべてのシステムを移設する場合についての費用をモデル化したものを表 6 に示す。

5.2 コスト評価

モデル化したものに以下の想定したラック費用および回線費用および条件を与えた場合についての概算を行った。

CaseA SINET を利用し、遠隔地にラックを借りた場合
回線費用 0 円、ラック一本 20 万円

CaseB DC を借りた場合 回線費用 10 万/月 ラック一本 20 万円

CaseC 格安ラックを借りた場合 回線費用 30 万/月
ラック一本 5 万

システムラックの本数を 4 本として、システム構築費が 500 万, 3000 万, 1 億の場合を想定し、それぞれの場合の計算結果を表 7 に示す。

これらの結果、システム費用が少ない場合には DC を利用するコストは増大するが、システムを集約した場合には、DC 単体でシステムを運用するコストと、大学でシステムを運用しつつバックアップを DC を持つコストが同等であることが判明した。また、システム全体を二重化することは、ランニングコストが増大しすぎることが分かった。

6 BCP に必要な要件

6.1 回復目標の時間的变化

一般に BCP では、

PhaseI 初動対応 (避難、消火、人命救助)

BCP 発動

PhaseII 初期対応 (情報収集、対応方針の決定)

表- 6: コスト評価

	Main	Sub	内容	(a)	(b)	(c)	構築	運用
現状	大学	なし		1			1a	0.2a
Case1	大学	大学	Data	1.1			1.1a	0.22a
Case2	大学	大学	Data+System	1.7			1.7a	0.34a
Case3	大学	DC	Data	1.1	1	1	1.1a	0.22a+12b+12c
Case4	大学	DC	Data+System	1.7	n	1	1.7a	0.34a+12nb+12c
参考	DC	なし		1	n	1	1a	0.2a+12nb+12c

表- 7: 概算値 (万円)

構築費, 条件	現状		Case1		Case2		Case3		Case4		参考 運用
	構築	運用	構築	運用	構築	運用	構築	運用	構築	運用	
500,A	500	100	550	110	850	170	550	350	550	1130	1060
500,B	500	100	550	110	850	170	550	470	500	1250	1180
500,C	500	100	550	110	850	170	550	530	500	770	700
3000,A	3000	600	3300	660	5100	1020	3300	900	5100	1980	1560
3000,B	3000	600	3300	660	5100	1020	3300	1020	5100	2100	1680
3000,C	3000	600	3300	660	5100	1020	3300	1080	5100	1620	1200
10000,A	10000	2000	11000	2200	17000	3400	11000	2440	17000	4360	2960
10000,B	10000	2000	11000	2200	17000	3400	11000	2560	17000	4480	3080
10000,C	10000	2000	11000	2200	17000	3400	11000	2620	17000	4000	2600

PhaseIII 仮復旧 (最低限必要なシステムの稼働)

PhaseIV 本格復旧 (全システムの復旧)

BCP 解除

という流れになる。それぞれの Phase に応じて、情報システムごとは、

ClassA 災害時に運用されるもの

ClassB 災害後においても継続して運用すべきもの

ClassC 災害後、数日以内(回復時)に運用が開始されるべきもの

ClassD 通常時において運用すべきもの

を判断する必要がある。ClassA については、災害発生時に運用される必要があるため、学外のある程度離れた距離に設置されることが必要と考えられる。ClassB については、大学の建物安全確認および電源の回復時には、早急に運用が再開される必要があるものである。ClassC については、その回復が落ち着き、大学の業務を標準状態に戻すために必要なものである。ClassD は、通常のシステムとなる。

本学における、それぞれの Class 分けの具体例を、下記に示す。

ClassA 安否確認システム・情報提供用 Web サーバ・DNS サーバ

ClassB ネットワーク・学務システム・施設系システム・電子メール

ClassC 人事システム・物品発注システム

ClassD その他

加えて、PhaseI 発生時に限定的であるが、組織として必要な最低限の情報系リソースとして、

- 情報収集のための Web アクセス
- 連絡手段としての電話、メールサービス

が必要となる。

システムを安定的に運用するために、図 2 のパスがすべて運用される必要がある。

6.2 リスクに対する対応方法

リスクに対応するには、大きく分けて次の二つの方法がある。

強靱化 災害発生時にも、運用できる能力を持つこと。

例えば、発電機の設置であったり、建物の耐震化、ラック等の免震化が上げられる。

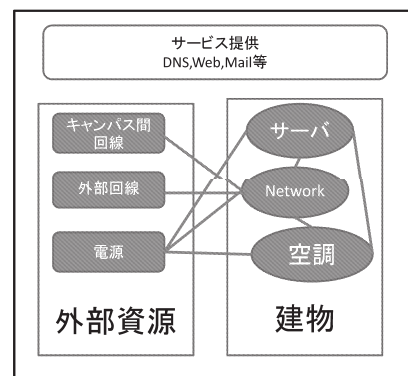


図- 2: 運用関連図

バックアップ 建物に対する影響が発生した場合に対して、バックアップを準備しておくこと。バックアップにはデータとシステムのバックアップの2種類があげられる。

また、通常リソースと非常時リソースについては、通常の運用に係るリソースは、{システムリソース プログラム 運用担当者 場所 電気 回線}があげられる。非常時にはこれに加えて回復担当者が必要になる。これらのうち、コストが掛かる順番で考えた場合には、運用担当者・回復担当者 プログラム システムリソース 電気 (回線・場所)となる。これらの資産を集約するか分散するかは大きくコストに影響する。適切に集約した場合には、コストの削減につながる。しかし、集約を行う場合には、一部でも別管理するものが残った場合には、思うようにコストの削減につながらないことに注意すべきである。また、1箇所だけで運用することは、障害のシングルポイントになることから、全体を考えた上で、冗長化やコスト評価を行ったうえで検討を行うことが必要である。

加えて、情報管理体制についての検討する必要がある。情報管理の点からは、情報の集約は漏えい時や障害時の影響が大きくなる可能性がある。ただ、情報の集約時には、情報を集積する場所の物理的なセキュリティの確保がしやすくなることや、組織外への業務委託となる可能性もあるため、これらを踏まえて判断する必要がある。

7 本学の対策

7.1 Class ごとの対策

Class ごとの対策として、非常時の最低限の情報収集方法および ClassA については早急に次の対策を行った。

最低限の情報収集方法については、情報センター独自の携帯電話を2台（別会社）準備し、これを利用することとした。今後、優先電話の配置や衛星電話・衛星回線の確保を検討することとした。ClassAについては、電力会社が異なること、本学のすべてのキャンパスと同時に停電しない距離にあることを前提に、非常時にはページの書き換えなどのオペレーションを依頼することができる環境が必要だと考えられた。そこで、学外に、DNS 設置と大学 Web サーバ（緊急時情報発信用）を構築し、震災の教訓から、距離的に約 100km 以上離れ、reboot 等の作業依頼が行えるところという条件を元に選定を行い、平成24年2月に岐阜大学総合情報メディアセンターと協定を締結、運用を開始した。

ClassB,Cについては、コスト評価からは、2つのキャンパスにおいて分散配置することが一番良いが、ほぼ同等な価格で行うことができる学内と外部の DC を借用しデータのみのバックアップを行うこととした。

ClassDについては、当面、対策を行わないこととした。

7.2 DC 設置場所

学内のシステム設置場所は、現在の総合情報基盤センターの本部がある五福キャンパスとするが、情報センターのシステムだけでなく、大学の情報システム全体に対して

- 学内の情報システムを集約し管理コストの削減
- 防犯カメラ・施錠管理などの物理的なセキュリティの確保
- 活断層があるため耐震性の確保

を行うために、データセンター棟を建築することとし、概算要求を行うこととした。

DC の設置場所として、五福キャンパスが選択された理由は、

- 五福キャンパスが SINET 接続点であること
- システムの多くが五福キャンパスに集約されていること
- 技術職員が五福キャンパスに配置されていることからである。

次に、DC を借りあげた場合の条件を検討した結果、次の仕様を満たす DC であることが必要だと判断した。DC の条件

- 入退館管理を完備していること
- 冗長化された空調、UPS が設置されていること

- 二系統の受電系統を有すること
- 非常用発電装置を有し、12 時間以上の発電が可能な燃料を確保していること
- 耐震構造の建物であり、免震機能を有すること
- 煙感知機能等を有し、ガス消火（ハロゲン・Co2・窒素等）機能を有すること
- 海岸線から 10km 以上離れ、海拔 5m 以上であること

さらに DC の仕様には、

- 本学のすべてのキャンパスから 5km 以上 50km 以内の距離であること
- IP アドレスを提供すること
- 無料で本学と BGP peer を行うこと

を追加した。

すべてのキャンパスから 5km 以上 50km 以内の距離であることについては、実際の運用を考えた場合には、本学の職員が頻繁に行くことができる距離、非常時にも徒歩や自転車等で行くことが必要であると考えた。5km 以上に関しては、五福キャンパスから 5km 範囲は下記の図 3 となる。

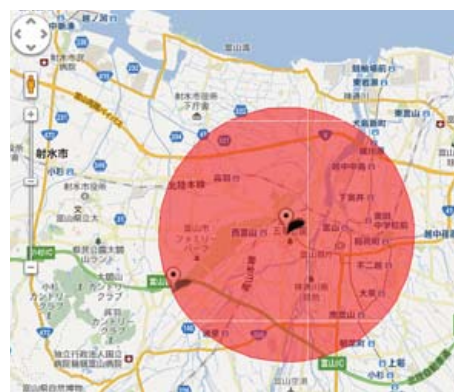


図- 3: 五福キャンパス 5km 圏内

このような広域の建物に影響が発生する災害を想定することは、地震、火災、水害、津波しか考えられない。DC に海岸線の距離および海拔を指定していることから水害および津波が除外され、火災についてもこれだけの距離が離れている鉄筋コンクリートの建物が同時に延焼することはない。地震に関しても一般に 5km 以上離れた耐震強度を有する建物が同時に破壊する状況は考えにくい。

また、本学 DC とバックアップ DC の間の回線を安価に冗長化することが望まれるため、IP アドレスは DC

事業者が提供することとし、その IP アドレスを提供する ISP との間に BGP peer を行うこととした。これにより、DC へのアクセスは、直接接続と SINET 接続の二重化となっている。また、ISP に直接接続することにより、高速で安定した接続を維持することができる。加えて、DC のアドレス空間を本学のアドレス空間とは別アドレスとしているため、非常時には商用回線からの接続も可能となっている。

実際に構築したネットワークは図 4 の通りとなる。

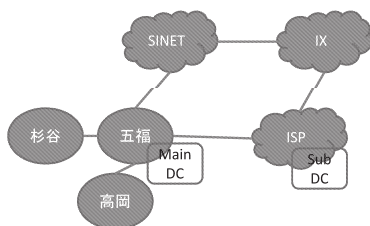


図- 4: ネットワーク図

データセンター棟については、平成 24 年度に学内希望順位 2 位で文部科学省に要望され、平成 24 年度補正により予算処置された。加えて、この建物においては、建物全体に対して 30 分程度電力を供給できる UPS(200kVA 程度) を設置することとなった。自家発電装置の導入は、維持管理の問題もあるため見送られ、発電装置を接続する電源回路を準備することとなった。これにより、今後、学内の情報システムのデータセンター棟への集約およびネットワーク機器の耐震性確保がなされた。

8 現状およびまとめ

本学の BCP の進捗状況は、ClassA に関しては、学外の大学と協定が締結され実施されている。ClassB,C は、学内 DC 棟に関しては現在設計中であるが、外部 DC の借上と ISP 接続回線の契約は完了しており、ストレージの設置および一部データのバックアップを行っている状態である。

データセンター棟に関しては、物理的なセキュリティを踏まえた耐震性を考慮したものとなっており、建築後は、事務系のシステムに関しては、今後のリプレース時期に学内 DC 棟に設置される予定である。

現状をまとめると図 5 のようになる。

今後、次期情報システムの更新に合わせ、ClassB,C の完全なデータバックアップ体制の整備を行う予定である。残る課題としては、学内の DC へ重大な損害が発

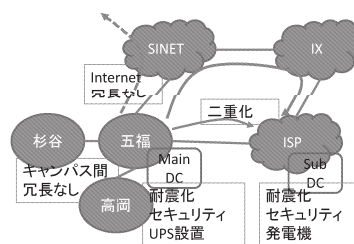


図- 5: 現状図

生した場合の ClassB,C のシステム稼働の確保、ClassD のシステムのデータバックアップ体制の整備、キャンパス間の回線の二重化、非常時の長時間の安定的な電源確保およびアップリンクの二重化についてである。このうち、アップリンクの二重化に関しては、DC のアドレスを提供している ISP と交渉しており、キャンパス間の回線については安価な地域 IP 網の利用を検討している。その他に関しては、今後の検討課題となっている。

参考文献

- [1] 東京海上日動リスクコンサルティング, "実践 事業継続マネジメント", 同文館出版, 2006.
- [2] 富士通オフィス機器, "よくわかる不測の事態に備える事業継続 BC 入門", FOM 出版, 2007.
- [3] 昆 正和, "どんな会社でも必ず役立つ あなたが作るやさしい BCP 第 2 版", 日刊工業新聞社, 2011.
- [4] 杉浦徳宏, 伊藤 篤, "サーバ室電力系統二重化による無停止運用と経過報告", p185-p190, 学術情報処理研究 No.15, 2011.
- [5] 鵜川義弘, 福井恵子, 平井清巳, 安藤明伸, 小野元久, 本田茂広, "大震災の経験から考察した BCP 非常用サーバ", p158-162, 学術情報処理研究 No.16, 2012.