

徳島大学における情報システムの BCP テスト結果と課題

BCP Test Results and Problems of Information Systems in Tokushima University

佐野 雅彦, 松浦 健二, 上田 哲史, 八木 香奈枝
Masahiko SANO, Kenji MATSUURA, Tetsushi UETA, Kanae YAGI

sano@tokushima-u.ac.jp, ma2@tokushima-u.ac.jp, ueta@tokushima-u.ac.jp, yagi.kanae@tokushima-u.ac.jp

徳島大学 情報センター

Center for Administration of Information Technology, Tokushima University

概要

徳島大学の所在地である徳島県は南海・東南海地震の発生確率が高いとされており、大規模災害を想定した事業継続計画 (BCP) の策定とその実施は重要である。本学では情報システムの BCP の一環として、DC を活用したネットワーク基盤及び広域無線の整備を平成 25 年度末に実施した。これは、被災確率の高いキャンパスに集中する基盤情報システムやネットワークを再設計し、被災時の可用性及び事業継続性の向上を目的としている。徳島大学情報センターでは、情報センターの ISMS 運用に従い、対策の有効性確認と試験のため、平成 26 年度、27 年度に情報システムの BCP テストを実施した。本論文では、これらテスト結果と改善課題および情報システムの BCP へのリスクの影響について考察する。

キーワード

情報系システム, BCP テスト, ISMS, リスク管理

1. はじめに

平成 23 年の東日本大震災以降、BCP と対策実施の重要度はより高まっている。徳島大学でも、南海・東南海地震による被災を想定した BCP の策定が実施[1]されているが、学内の情報系システムに関する対策の議論は少なかった。一方、総務省では災害に強い電子自治体に関する研究会報告[2]にて ICT-BCP の重要性が述べられている。情報センターでは徳島大学の基幹系情報システムの BCP の対策として、平成 25 年度末にキャンパス間ネットワークの再整備、キャンパス間ネットワークを補完

する広域無線アクセスライン、インターネット回線を代替する衛星インターネット、データセンタ (以下 DC) やコンテナ DC によるサーバ集約設備など、情報基盤アーキテクチャ・システム・サービスについて整備した [3]。これらの対策は、一般的なメールや Web ブラウザを利用する利用者から隠された部分であるが、徳島大学の情報システムの可用性向上のための重要な対策として、学内合意を形成して平成 25 年度末に整備した。

整備した設備が有効に作用することを確認するために、情報センターで運用する ISMS (ISO/IEC 27001) に従い、BCP の有効性測定のためのテストを平成 26 年度及び 27 年度に実施した。実際にテストを行うことにより机上想

定および机上テストで見落としした事項が発見でき、発見できた事項に対策を行える。結果としてBCP対策の有効性向上が期待できる。

本論文では、整備した設備等について、情報システムのBCP上の効果を検証するために実施した平成26、27年度のBCPテストとその結果、および結果から確認された課題とその改善について考察する。

2. 情報システムのBCPのための基盤整備

2.1 情報システムのBCP要件

情報センターでは、平成24年度から大規模災害（地震、津波）を想定した、情報システムのためのBCPを検討してきた。そのBCPの要件を以下に示す。

(1) 想定する災害

南海・東南海地震における、情報サービスの停止、情報基盤の損傷を主たる想定災害とする。

(2) BCPの目的

災害発生からの数日間（3-5日程度）における災害初期対応のための最低限のサービス提供と被災程度が甚大でない地区における基本的サービスを提供する。

(3) 災害時のサービス内容

甚大被害時の安否確認等に必要最低限の通信環境を提供する。これは電子メール、安否情報関連を中心とする学内外に公開するサービスを想定する。また、被災甚大地区の特定場所におけるインターネット接続環境、被災軽微地区でのインターネット接続環境及び電子メールの基本サービスを提供する。

2.2 平成25年度の整備

2.1節に示した要件に対して検討された主たる解決課題は表1-1に示すとおりであった。これは、災害発生後3日間は災害時における最低限のサービス提供を目的としており、徳島大学の地理的特性と当時のネットワーク基盤や電源事情、および、それらの上で構築されていた各種サービスを考慮したものである。本学主要3キャンパスのうち、新蔵地区および常三島地区は被災リスクが高く、これらの地区が機能停止しても他の地区への影響を最小限に抑える必要があった。これらの課題の解決方針として表1-2に示す5項目を検討した。項目1～2は項目3と関連して項目4の実現に必要であり、項目4は2.1節のBCPの目的の実現する事項である。項目5は災害時提供サービスの起動方法に関する項目である。表1-3では表1-2の5方針から、サービス機能の移転、ネットワーク構造変更、サービス機能移転に必要なサーバ移転、サービス継続のための電力供給の4対策を検討した。その結果、表1-4に示す3整備事業に纏められて平成25年度末に実施された。これらの検討詳細は文献[3]に詳述さ

れている。図1は、表1-1から表1-4までの各項目の関係性を示しており、実線矢印は項目間に主たる関係性の存在を示し、破線矢印は部分的な関係性の存在を示している。これは、表1-1に示されたBCPのための解決課題が表1-4に示した整備事業に至る過程の流れを示している。表1-4が示す整備事業はいずれも基盤整備であり、これに依存する上位サービスの整備については平成26年度以降に順次実施するものとした。これは、単年度事業として上位サービスを含めた整備は時間および予算の上の理由で困難であると判断したためである。

表1-1 想定解決課題

項	課題内容
1	地理的脆弱性
2	基幹網および電気系統の脆弱性
3	上位サービスの提供場所

表1-2 解決方針

項	方針内容
1	情報機器への電源継続供給
2	ネットワークの堅牢化
3	情報基盤運用の適正化
4	コミュニケーション手段の提供
5	手動・自動の戦略確定

表1-3 検討した対策

項	対策内容
1	ネットワークサービス機能移転
2	ネットワークトポロジ変更と広域無線網整備
3	分散物理サーバの集約
4	電力対策

表1-4 整備した設備

項	整備内容
1	コンテナDC設置、非常用自家発電機
2	ネットワーク基盤、仮想化基盤
3	広域無線LAN網、衛星インターネット

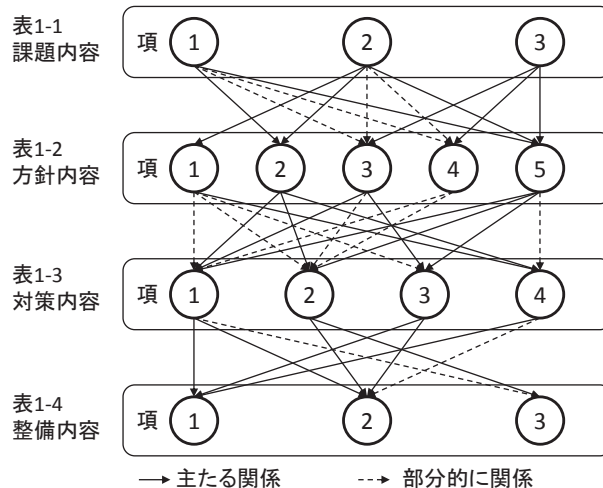


図1 検討事項間の関係性

図 2-1 は表 1-4 の整備事業実施前のネットワーク構成概略であり、図 2-2 は実施後の概略である。図 2-2 には未記載であるが常三島地区には自家発電装置（72 時間無給油稼働）、常三島地区・新蔵地区・蔵本地区を接続する広域無線 LAN が設置されている。図 2-1 に示す常三島地区を中心としたネットワーク接続構造から図 2-2 に示す外部 DC を中心としたネットワーク接続構造に変更しており、被災リスクが高い常三島地区、新蔵地区を経由しないネットワーク基盤を構築した。これにより、被災リスクの低い蔵本地区は、常三島地区の影響を受けないネットワーク回線を確保できた。被災リスクが高い地区では、基幹スイッチへの給電と経路損傷が無ければインターネットアクセスのための経路が確保できる。もし、確保できなかった場合は広域無線 LAN と衛星インターネットにより最低限のインターネット環境を提供する。

2.3 平成 26 年度以降の整備課題

平成 26 年度以降では平成 25 年度に整備した設備の活用と、その上で展開するサービスにおける BCP 対策の検討と実施を進めた。

(1) 整備設備のテスト

整備した設備は、表 2 に示すとおり、常時稼働設備と災害時稼働設備がある。常時稼働設備の正常性確認（故障や不具合等の有無の確認）は日常の動作監視、週次/月次点検業務で確認できるが、災害時における動作はそれを想定した試験により確認する必要がある。しかし、キャンパス間ネットワーク等の停止影響範囲の大きい設備を停止させてテストすることは難しく、電気設備点検のための停電等（計画停電）に便乗して実施するなどの工夫を要する。一方、災害時稼働に特化した設備は通常は業務運用していないため比較的任意に点検可能であるが、一部は常設していないため作業手順は多い。いずれの場合でも、BCP 上、期待どおりに稼働することが前提であるため、定期的なテストあるいは訓練によりその確実性を高める必要がある。また、テストあるいは訓練により問題・課題が生じた場合は期待どおりの稼働となるように改善する必要がある。

情報センターでは、情報センターの ISMS における事業継続の側面から、定期的なテストの実施を行うこととしており、平成 26 年度では主に単体の機能テスト、平成 27 年度は広域なテストを単独および計画停電時に実施することとした。

(2) 依存する上位サービスへの対策

表 1-4 で整備した設備に依存する上位サービスに関する対策の検討を行った。具体的には表 3 に示すとおりであるが、実際の対応は簡単ではないことが予想された。このため、(1) で述べた整備設備のテストの結果を踏まえて検討を進めることとした。以下では、対策が必要な

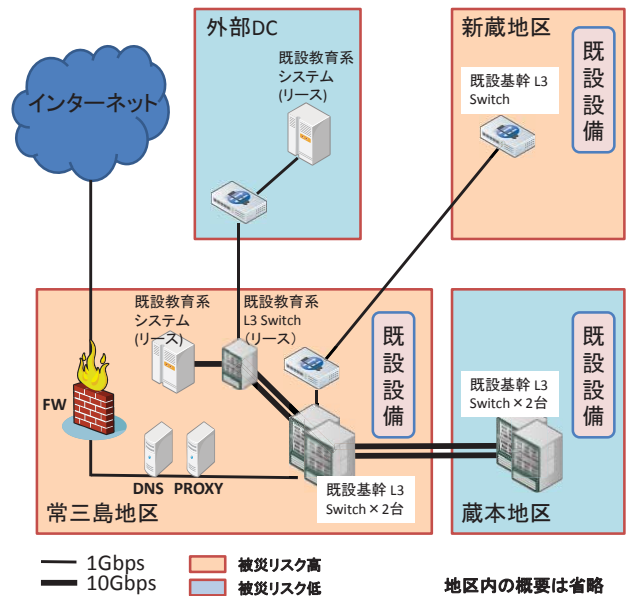


図 2-1 設備整備前のネットワーク概略図

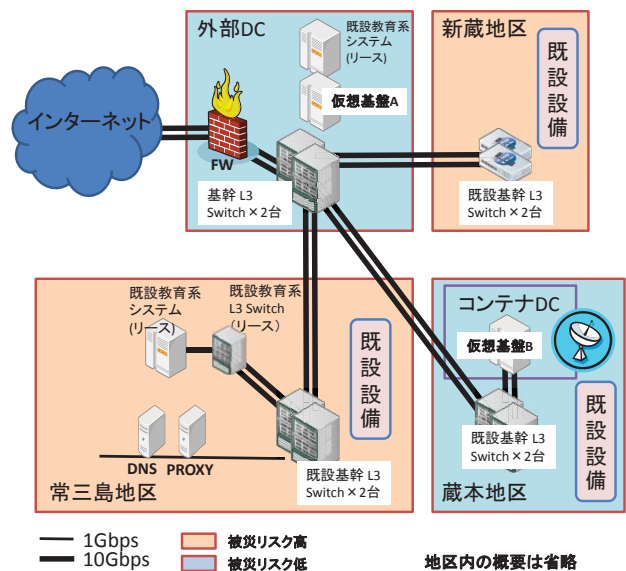


図 2-2 設備整備後のネットワーク概略図

表 2 常時稼働設備および災害時稼働設備

稼働分類	対象設備
常時稼働	ネットワーク基盤, 仮想化基盤, コンテナ DC
災害時稼働	広域衛星無線網, 衛星インターネット, 非常用自家発電機

表 3 対策を検討した上位サービス

サービス名	検討理由
DNS サービス	常三島設置で被災時停止
メールサービス	論理ネットワークの問題
プロキシサービス	常三島設置で被災時停止
認証系サービス	常三島設置で被災時停止
VPN サービス	常三島設置で被災時停止
NTP サービス	常三島設置で被災時停止

主要な課題事項について述べる。

a) DNS サービスの移行

平成 25 年度末の整備前では、図 2-1 に示すとおり DNS 機能の大半とメールや Web プロキシ等の主要なサービスおよびインターネットへのアクセス回線は常三島地区に集中し、常三島地区の被災により、実質学内の全サービスが停止するリスクを有していた。平成 25 年度末の整備後では、図 2-2 に示すとおり、常三島地区を経由しないインターネットへの接続経路が確保された。しかし本学の場合、利用者向け DNS サーバは常三島地区に集中しており、かつ、利用者の情報機器やサーバが参照する DNS サーバを変更するためには、多大な労力と期間を要することが想定されていた。

b) メールサービスの移行

学生用メールサービスについては、平成 24 年度の時点で、外部クラウドサービスに移行しており、教職員用および部局固有メールサービスが学内サービスとして残されていた。ただし、教職員用メールサービスも平成 24 年度時点で賃貸借により外部 DC 内に新メールサービスとして提供を開始していた。しかし、このサービスを構成する論理ネットワークは常三島地区経由で設計されており、整備した設備に合わせたネットワーク変更が必要であった。この変更は賃貸借システム全体に影響を与えるため、慎重な対応を必要とした。また、旧メールサーバの老朽化のため、旧メールサービス利用者を新メールサービスに移行させる必要もあった。

c) Web プロキシサービスの移行

本学で利用する Web プロキシサーバは、すべて常三島地区に設置していた。今後、外部 DC 上への移行が必要であるが、FQDN による設定であるため、比較的楽に移行可能と判断した。

d) 認証系サービスの移行

本学で運用する統合認証サービスは常三島地区に設置されている。全学に影響するサービスのため外部 DC への移設が必要であるが、慎重な移行が必要であった。なお、この統合認証サービスの背後に設置されている LDAP サーバは平成 25 年度時点で既に外部 DC 上に設置済みであったが、メールサービス同様、論理ネットワークの構成に課題があった。

3. BCP テスト計画

前節までに述べた設備整備状況と平成 26 年度以降に対策が必要な事項を踏まえて、平成 26 年度および 27 年度では BCP テストの方針を次のとおりとした。

平成 26 年度は表 1-4 で示した設備のうち非常時に運

用する設備を中心に機能テストと訓練を行い、その結果発見された課題への対応を実施する。平成 27 年度では前年度のテスト結果とその課題への対応結果を踏まえて、常用設備も考慮したより全体的なテストと訓練を実施するものとした。BCP テスト計画のスケジュール概要を表 4 に示す。表中、設備 1 から 3 は、表 1-4 に記載の設備を意味する。また、平成 28 年度の 3Q のテスト結果における 4Q の対策が未記載である理由は、主要問題は既に対策済みとしているためである。このため、テスト後に新たな課題が確認されれば改めて対応するものとした。なお、他の細かな課題は記載を省略している。

3.1 平成 26 年度計画

導入した設備のうち、(1) 広域無線 LAN 網および星インターネット設備、(2) 非常用自家発電装置について、機能テストおよび非常時の訓練を行う。設備納入時には納入業者によるテスト、手順書作成、教育が実施済みである。しかし、ISMS の管理策 A.17.1「情報セキュリティ継続」[4]より、事業継続のためのテストおよび訓練が重要である。そこで、情報センターでは下記の BCP テストの実施を計画した。

(1) 広域無線 LAN 網、衛星インターネットテスト

広域無線 LAN 網は各地区に設置されている広域無線 LAN 網と蔵本地区に設置されている衛星インターネット回線、可搬型衛星インターネット装置、および移動中継車(自転車)を含めたテストを実施する。これらは図 3 に示すフローで実施し、要した時間と課題点の洗い出しを行う。このテストは 3 地区で実施する必要がある。かつ、常三島地区はさらに 3 つの作業パートに分かれており、手順も複雑となるため、事前準備が不可欠である。なお、テスト実施時期は平成 26 年内の実施を予定した。

(2) 非常用自家発電機テスト

常三島地区に設置された非常用自家発電機は、商用電源停止後 72 時間の間、無給油で電力提供することを想定しており、事象発生時には最大 3 分以内に自動的に切り替わる。電源切断の事象は、津波による常三島地区の電源設備浸水(建物 1 階部浸水)による停電を想定している。このテストを実施するため、通常の業務状態において商用電源を切断することで、想定状況を設定した。このテストは、正常に切り替わることの確認と、給電対象装置が非常用自家発電機から給電されることの確認も含まれている。テスト実施時期は、平成 26 年度の計画停電(例年 10~12 月頃)までに実施し、計画停電時には非常用自家発電機により正常に情報システムの継続運用できることも確認する。

3.2 平成 27 年度計画

平成 27 年度は平成 26 年度の実施結果をふまえ、課題

事項への対応を検討したのち、上位サービスを含めたより全体的なテストを計画した。これは、被災により、地区間の通信線が切断された状況を想定しており、学外から大学 HP に安否確認のためのアクセスと、学内特定部署あるいは学外からの安否確認メール送信ができることを目的としていた。実施時期は常三島地区の計画停電日に実施し、利用者への影響の低減を考慮した。また、主要な対策をテスト実施日までに実施することとした。これには、4.1 節 (1) に後述する論理ネットワーク構成の変更が含まれている (平成27年4月にこの対策を実施)。

4. BCP テスト結果

3章のBCPテスト計画を実施した結果について年度別に述べる。なお、実施したテストの一覧を表5に示す。

4.1 平成26年度実施結果

以下では平成26年度分の主要事項について述べる。

(1) 広域無線 LAN 網、衛星インターネットテスト

平成26年6月24日に図3のフローに従い、情報センター内の人員9名で実施した。以下では項目毎のテスト結果と課題を示す。それぞれのテストに要した時間は約1~2時間であった。

・広域無線 LAN 網、衛星インターネット

装置に給電するための携帯型自家発電装置の接続手順の不備、広域衛星無線 AP への電源接続不備 (手が届かない) といった設備展開上の問題や、Web 閲覧は可能であるが、メールや大学 HP へのアクセスが不可であったなど、上位サービスを含めた問題が確認された。これは、本学内の無線 LAN の SSID を使用したものと、災害時専用の SSID を使用した異なる無線 LAN 環境を想定してテストを行ったが、それぞれに課題が発見される結果となった。これらの対策として、地区間を含めた論理ネットワーク構成の大幅な変更が必要であることが確認された (理由は5.1節に後述)。

・可搬型衛星インターネット、移動中継

操作マニュアルの不備があり、組み立てに時間を要したことや、装置間を接続するケーブルの不足、方位測定のためのコンパスの不足が確認された。また、衛星アンテナの設置には硬い足場の設置環境が必要であり敷板等の対策が必要であった。加えて悪天候時を想定した雨対策等の課題も確認された。なお、可搬型衛星インターネット装置は広域無線 LAN 設備と同様、携帯型自家発電装置を備える。

(2) 非常用自家発電機テスト

平成26年7月12日 (土) の午後に常三島地区計5名で実施した。事前の電気負荷状況を確認し、情報センター棟の電気室分電盤のブレーカを遮断することにより棟

表4 BCP テスト計画スケジュール概要

	平成26年度				平成27年度				平成28年度			
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q
基盤設備	設備1	テスト	対策		テスト	対策			テスト	対策		
	設備2				テスト	対策			テスト	対策		
	設備3	テスト	対策		テスト	対策			テスト	対策		
上位サービス	論理NW	テスト	対策		テスト	対策			テスト	対策		
	DNS					テスト			対策	テスト	対策	
	メール					テスト	対策			テスト		
	PROXY					テスト			対策	テスト		
	認証					テスト			対策	テスト		

(設備1,2,3は表14に示す内容)

表5 実施したBCPテストの一覧

実施日	テスト内容	目的
2014/6/24	広域無線 LAN 網接続、衛星インターネット接続ほか	設備テスト
2014/7/12	非常用自家発電機切り替え	設備テスト
2015/1/30	公式 HP 切り替え	部分テスト
2015/1/31	計画停電による非常用発電機稼働	実運用
2015/5/1	衛星インターネット接続	事前確認
2015/5/8	広域無線 LAN 網接続	部分テスト
2015/12/13	ネットワーク基盤、広域無線 LAN 網、衛星インターネット	上位サービスを含む複合テスト

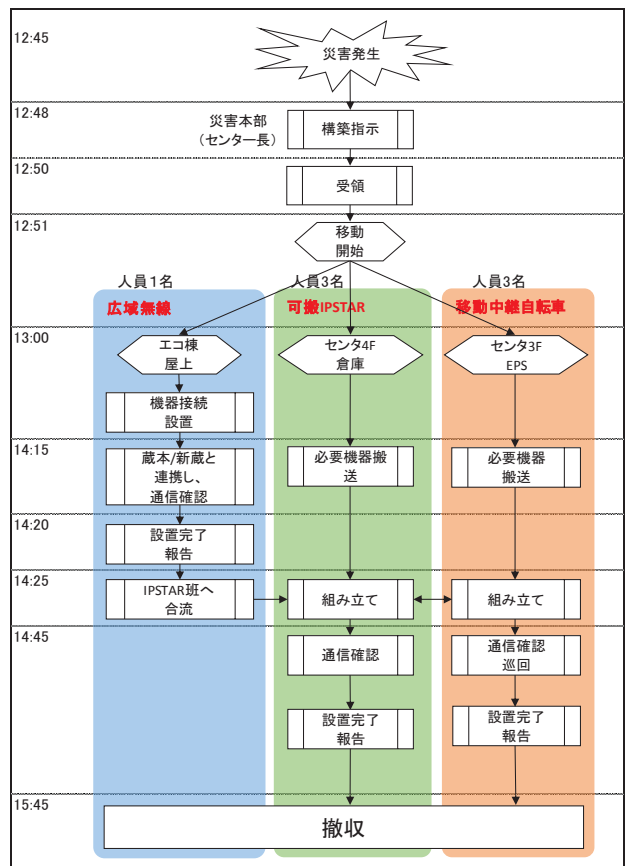


図3 BCP テストフロー (常三島地区)

内の電力供給を停止した。規定時間3分以内(実測8秒)に非常用自家発電機は稼働して給電対象のほとんどの機器は継続運用できたが、サーバ数台とスイッチ1台が停止した。これにより、埋もれていた問題点が発見され、その対策を実施した。その後、平成26年1月31日の計画停電字のテストでは、先のテストで原因不明であった事項、見逃していた事項を発見して対処した。前者は、非常用自家発電機に切り替わった際にサーバが再起動する事項であり、当該サーバがUPSを経由せずに接続されていたことが原因であった。後者は、サーバ室のエアコンが自動復旧しなかったこと、想定外の場所に設置されたサーバが発見されたこと、および防災監視盤の警報停止処置などの課題が発見された。

4.2 平成27年度実施結果

平成27年度は、平成26年度の課題への対応を踏まえ、上位サービスを含めたBCPテストを実施した。本節では、平成27年12月13日に実施したBCPテストについて述べ、個別の部分テストについては省略する。

上位サービスを含む複合テストは、常三島地区計画停電日に実施し、広域無線LAN網、衛星インターネット接続(可搬型衛星インターネットおよび移動中継車のテストは今回省略)、公式HPサービス、メールサービス、ネットワーク切断等のテストを、BCPに係る3部局、11名(情報センター8名、総務部2名、環境防災センター1名)が参加した。

(1) 広域無線LAN網、衛星インターネット接続

平成26年度の経験が生かされ、1時間で設備展開が可能となったことが確認された。しかし、前回は問題とされなかった点が今回は問題となり、新たにその原因が確認された。

(2) 公式HP切り替えテスト

公式HPの切り替えテストは平成27年1月に実施済みであったが、今回、常用サーバとバックアップ用サーバ間にソフトウェア上の不具合が生じて切り替えが遅れた。また、バックアップ機へのDNSの切り替えに様々な問題が発生して想定手順通りの実施ができず、現場判断で対応した。なお、公式HPサーバは常三島地区、バックアップサーバは外部DCに設置されている。

(3) ネットワーク切断テスト

(1)、(2)を実施後、常三島地区のネットワークが切断された状況を常三島基幹L3スイッチの光ファイバを抜くことにより模擬し、その状態で安否確認メールの送信と、同メールの受信者の返信および公式HPにアクセスして災害情報等を入手するテストを実施した。この際、学外からのアクセスには問題なかったが、常三島地区以外の地区からのアクセスには問題が生じた。これは前述したDNSの切り替えの問題とも関係しており、大

学全体のDNSの関係を見直す必要性が確認された。また、プロキシサーバに関する問題が生じ、プロキシサーバを設定している利用者が上記HPにアクセスできない現象も発生した。これは、プロキシサーバもDNSサーバと同様に常三島地区に集中しており、常三島地区と外部DCが切断されたことにより、プロキシサーバにアクセス不能になったためである。以上のとおり、ネットワーク切断テストをすることにより、対策できていない事項が明らかとなった。

(4) メールを用いた安否確認テスト

メール発信者は、広域無線LAN網を利用した衛星インターネット経由で外部DC内にあるメールサーバにアクセスし、安否確認メールの送信と返信の確認を行うことができた。これは、平成26年度のテストで確認された論理ネットワークの課題が解決済であったため、問題は生じなかった。

平成26、27年度のBCPテストの結果は前述のとおりである。ネットワーク基盤設備についての課題は減少し改善が確認された。しかし、上位サービスレベルでは様々な改善すべき課題が確認された。我々の当初の想定では、この種の問題が生じることは想定していたが、実際の影響度合いまたは対策に要するコスト(手間)はそれほど高くないと見込んでいた。これは、表1-4の整備により、物理的な構成は以前よりも整理されて簡素化されたため、対策もそれほどコストを要しないと判断していたためである。しかしながら、物理的に簡素化されても、論理的な複雑性が残されていたため、結果として対策実施に期間を要する事態となった。

5. 考察と課題

5.1 テスト結果の考察と課題

平成26年度の広域無線LAN網、衛星インターネットテストには9名の人員を投入した。本学の場合はキャンパスが3地区に分かれており、衛星インターネット装置は蔵本地区に設置されていることから、広域無線LAN網は、3か所全て起動する必要がある。この場合、実際の災害時に各地区に人員を派遣できるかどうかは検討が必要である。また、被災リスクの高い常三島地区や新蔵地区は、浸水により移動不可能となる場合も想定されるため、システムの自動起動の方法についても今後検討が必要である。なお今回のテストに要した時間は、最短地区で1時間、最長地区で1時間50分要した。手順書の不備や見落とし等による時間浪費があったが、改善により1時間程度で展開可能であると判断した。

情報センターでは、被災地区やその近隣における無線LAN環境を提供する手段として可搬型衛星インターネット装置を整備している。しかし本装置は分解して運搬

することは可能ではあるが、風等の影響を考慮すると、運搬には二人は必要とする。しかし、災害時に運搬者が確保できるかどうかは不明である。このため、現在では常三島地区の情報センター棟屋上に固定的に設置しており移動中継車と連携することにより、非常時の無線 LAN アクセスを提供可能としている。

4.1 節で述べたが、本学の論理ネットワークに大幅な変更の必要性が確認された。2.2 節に述べたとおり、当時のネットワークは、図 2-1 に示すとおり、常三島地区中心の物理ネットワーク構成である。図 2-1 中の常三島地区および外部 DC にある既設教育系のシステムはプライベートネットワーク内にあり、常三島地区の基幹 L3 スイッチにて NAPT していた。対策実施後は、図 2-2 に示すとおり、物理的には被災リスクの高い常三島地区を迂回可能となったが、論理ネットワークが変更されていなかったため、テストで問題が生じた。これを解決するためには、NAPT 箇所を外部 DC にて行う必要があり、大規模な変更を要することとなった。この変更は平成 27 年 4 月に実施された。

平成 27 年度では、上位サービスを含めたより複合的な BCP テストにより様々な課題を発見した。実際に光ファイバの取り外しによるネットワーク切断は、我々が想定していた以上の問題点を明らかにし、テストの効果があつたと言える。その多くは検討不足や見落としであり、サーバやネットワーク機器の平常時には影響しない設定の不具合等を発見した。とくに、DNS に関係する問題は、これまで運用してきた方法を大きく見直す契機となっている。これには、新たな利用者向け DNS サーバ群を構築して周知するか、既設 DNS サーバのネットワークごと移設するかの対策を検討している。また、Web のプロキシサーバの課題については、DNS に登録したサーバ名による運用であるため、プロキシサーバの外部 DC への移転は容易と考えている。なお、DNS サーバおよびプロキシサーバ対策は平成 28 年 9 月に完了予定である。

災害発生時の情報伝達手段としての大学公式 HP は、災害時に学内外から閲覧できることを想定しているが、平成 27 年 12 月のテストにより、災害時の運用が可能であることを確認した。DNS や HP コンテンツの切り替えなどの手作業部分が残されているが、本学の公式 HP のあり方の議論を踏まえた今後の検討課題としている。また、安否確認を本学のメールサーバを用いてテストし、対象者へのメール送信および対象者からの返信確認をすることができた。これは本学のメール基盤が想定どおり稼働したことを意味しており、BCP の安否確認の基盤として使用可能であると判断している。現在は、このメール基盤を活用した安否確認システムを構築中である。

今回、災害発生時の活動拠点として、蔵本地区の情報センター蔵本分室を選択した。この理由は、公式 HP 切

り替えのための DNS 設定変更作業や Firewall の設定変更などの作業は、情報セキュリティ上、学内の特定ネットワークから行う必要があることと、蔵本地区の被災リスクは常三島よりも低く、情報センター職員が蔵本分室に到達できる可能性が高いためである。しかし実際にテストを行ったところ、蔵本分室から特定のネットワーク機器にアクセスできず、アクセス経路確認を見落とししていたことが確認された。これは、当該機器に至るまでのフィルタリング設定の問題であった。

以上のことから、実際の事態を想定したテストを実施することにより様々な問題・課題を発見することができた。机上想定では問題ない事項も実テストすると様々な問題として表面化することも確認され、実テストの重要性を再確認した。結果として、より確実な BCP 対策として改善を行うことが実現できたと判断する。

本論文作成時点では、整備した仮想化基盤 A および B には、学内で共同利用されるサービスが移転しつつある。まず、2.1 節の BCP 対策として表 3 に示すサービスに関して、移設を要するサーバ数と移設済みサーバ数を可用性の重要度別に集計したものを表 6-1 に示す。可用性重要度 4 では約 90%、重要度 3 では 100% のサーバが移設済みであり、想定する最低限のサービスを提供するための環境整備が進んでいることが確認できる。

次に表 6-2 にこれら仮想化基盤の利用状況を示す。仮想化基盤 A では CPU コア資源の 50% 以上、同 B では 85% の資源が割当済みあるいは予約済みとなっている。これらを利用分類および地区別にみると、表 6-3 に示すとおり、被災リスクが高い常三島地区と新蔵地区の利用数（計 60 台）が全体（計 72 台）の 83% を占めており、情報センターだけでなく他の部局等においても BCP を想定した仮想化基盤の利用が進んでいることが確認できる（試験利用を除く）。これらのうち、情報センター設置サーバは 23 台（全体の 32%）であり、残り 37 台（51%）は部局等のサーバである。また、業務用サーバ 25 台は全体の 35% を占めている。仮想基盤の残りソースは、今後設置が想定されるサービスや業務系や研究・教育系のサービス等、BCP 上の初期対応以後に継続すべき情報サービスのために供される予定である。

表 6-4 には各仮想基盤の物理性能を示す。本装置導入時点において、既設物理サーバと同程度の性能を確保しており、既設物理サーバを集約する際の物理 CPU と仮想 CPU の性能は同等としている。なお、表 6-2 では表 6-4 から障害時の縮退分（ブレードサーバ 1 台相当のコア数とメモリ）を除いている。つまり各仮想基盤においてブレードサーバ 1 台の故障は想定済みである。

以上のことから、表 1-3 の 1 項の「ネットワークサービス機能の移転」対策は進捗していると判断できる。

5.2 BCP リスク変化の考察

これまでに述べたBCPテストとその対策により、情報システムのBCPにおけるリスクの変化について考察する。ここでは、表1-1に示す課題のリスクが平成25年度の設備整備を含めどのように変化したかについて、4章および5.1節に述べた結果から定性的評価を試みる。なお、リスク評価の対象は、2.1に述べたBCPの目的から可用性のリスクを重視し、機密性、完全性のリスクは今回評価しないものとする。

(1) 評価の手法

この評価では、ISMSのリスク評価手法[5]を参考に、定性評価のための補助情報を作成して評価する。ここで、 $リスク値 = 資産重要度 \times 脅威 \times 脆弱性$ で計算されるものとする。これはISMSにおけるリスクアセスメントの一手法であり、情報センターのISMSでもこの手法を用いている。

一連の対策およびテストは想定災害の発生を前提としていることから、災害の脅威（頻度）については無視あるいは定数とみなすことができる。また、ある資産におけるリスク値の変化を見る場合、資産重要度は評価の前後で不変であるとする、注目すべき変数は脆弱性だけとなる。よって、脆弱性の変化についてのみ評価した結果を定性評価のための情報とした。情報センターのISMSでは、脆弱性を1から4の4段階評価としている。脆弱性1は最も脆弱性が低いとし、4は最も高いとしている。無対策の場合は最高値4となり、一定の対策実施毎に数値を減じる手法を用いている。今回、表7に示す対策の評価基準により脆弱性を評価するものとした。表7中、脆弱性値が1と記載されているものは、その時点の脆弱性から1減じることを意味する。

(2) 脆弱性の評価

表7の基準をもとに、表1-1に示す課題に対する脆弱性値の変化を表8に示す。初期値は4である。評価対象とした時期は表5のテスト実施状況から、①平成25年度末の整備直後、②平成26年8月、③平成27年2月、④平成27年12月、⑤平成28年7月とした。また表1-1の2項目の脆弱性については2つに分割し、表8中では「課題2-1と課題2-2」として評価した。評価内容の概略を以下に示す。

・課題1：地理的脆弱性

①では、キャンパス間のネットワーク構成が変更されたことにより地理的脆弱性が改善したため初期値4から改善した。また④にて課題はあるものの、切断されていない地区からの通信や学外からの通信が可能であったことから、脆弱性が改善されたと判断した。

・課題2-1：基幹網の脆弱性

①では、課題1と同様にネットワーク構成が変更

されたことと、④にて、HPの閲覧や安否確認テストが可能となったことから、それぞれ脆弱性が改善されたと判断した。

・課題2-2：電気系統の脆弱性

①では、非常用自家発電機が設置され、③において②におけるテスト結果に対する改善が確認され、また④においても不具合なしにテスト完了できたことから、それぞれ脆弱性が改善されたと判断した。

・課題3：上位サービスの提供場所の脆弱性

①では、仮想化基盤が外部DCとコンテナDCに設置されており、その後、段階的にサーバ等の移行が進んでいる。⑤においては、相当数のサーバが仮想化基盤に移設あるいは新設されているため、それぞれ脆弱性が改善されたと判断した。

表6-1 BCP対策におけるサーバの移設状況

可用性重要度	移設等必要数	仮想化基盤A	仮想化基盤B	移設済小計	移設済割合
4	19	12	5	17	89%
3	4	3	1	4	100%

(可用性2以上でBCP目的に直接関係するサーバのみ記載)

表6-2 仮想化基盤の利用状況(平成28年7月時点)

種類	仮想化基盤A			仮想化基盤B		
	基幹サービス用			一般サービス用		
目的	資源数	割当数	使用率	資源数	割当数	使用率
CPU	80	46	58%	112	95	85%
メモリ	480	142	30%	672	338	50%
DISK	10,550	5,136	49%	12,900	9,900	77%

(メモリ、DISKの単位は何れもGB)

表6-3 地区毎のサーバ数利用内訳

種類	仮想化基盤A			仮想化基盤B		
	教研	業務	基幹	教研	業務	基幹
常三島	3	7	15	11	5	4
新蔵	0	2	1	0	11	1
蔵本	0	0	0	6	5	1

(教研:教育研究用,業務:業務用,基幹:基幹サービス用)

表6-4 各仮想基盤の物理性能

名称	CPU性能	各Blade		Blade総数	Core総数	MEM総数
		CPU数	MEM			
仮想基盤A	Intel Xeon E5-2670 (2.6GHz/8 CORE)	2	96GB	6	96	576
仮想基盤B	Intel Xeon E5-2670 (2.6GHz/8 CORE)	2	96GB	8	128	768

表7 脆弱性評価の基準

対策の判断基準	脆弱性値
無対策	4
物理的対策の実施あるいは設備整備の実施	-1
依存する上位サービスへの対策実施	-1
依存する上位サービスを用いたBCPの対策実施	-1

表8 脆弱性値の変化

脆弱性	評価時期					
	①	②	③	④	⑤	
課題1	3	3	3	2	2	①2014年3月末
課題2-1	3	3	3	2	2	②2014年8月
課題2-2	3	3	2	1	1	③2015年2月
課題3	3	3	3	3	2	④2015年12月
						⑤2016年7月

これまでの評価の結果、各脆弱性の値は段階的に減少していることが確認できる。ただし脆弱性値が1まで減少したものは、電源設備関係のみとなっており、他の脆弱性については改善の余地がある。いずれの場合でも、「(1)評価の前提」より、リスク値が減少したと言える。なお、残された改善余地が改善されたかどうか、依存する上位サービスを用いた BCP の対策実施できたかどうかは平成28年冬頃に予定する BCP テストの結果を待つ必要がある。

5.3 評価方法の考察と課題

本論文では、情報システムの BCP に対する対策方法について、これまで実施してきた対策やテスト結果から、表1に示す課題と対策事項の関係を結び付け、実施事項から対象とした課題のリスク変化を脆弱性値の変化として扱い、これを評価することにより、BCP 対策の改善を定性的に見てきた。これまで感覚的に改善されたと感じてきたことに対して、一定の評価を示すことができたことは有効であったと言える。しかし、表1、図2の関係性を用いた評価は主観的部分も含まれるため改善の余地があると言える。例えば、図2中のグラフで各有効枝に重み付けする等を行うことにより、後の検討事項における優先度等を数値化できる可能性があり、より客観的に検討できることが期待できる。

5.4 他組織への適用に関する考察

本論文で実施した手法がどの程度他組織に適用できるかを考察する。まず、前提とした BCP の目的から表1-1に示すような解決課題が明らかになっている場合、本手法と同様にして、表1-3に示すような対策ならびに表1-4に示すような実施計画に結びつけることが期待できる。その際、図2のように項目間の影響の可視化により、検討漏れや対策漏れを抑制することが期待できる。

次に、DNS サーバやプロキシサーバなどのネットワーク基盤サービスに対する本学で適用した対策については、各組織の地理的要素やネットワーク構造、サービス構成等に依存する部分が多いことから、事例依存と判断される。本学のように各キャンパスの間に DC を確保できるような類似した環境であれば適用できる点は多いと推測する。なお、本論文では述べなかったが、サービスの依存関係およびサービス設置場所等に関連付けておくことで課題点の発見と対策方針決定の支援も期待できる。

最後に、BCP 対策の有効性を評価するには、実際のテストや訓練の実施が重要である。それらの実施結果を踏まえて、対策の有効性を議論できる。例えば ISMS あるいは ISMS に準じた活動を実施する組織では、一連の対策の結果、リスク再評価によるサービスの可用性のリスク値の低減が期待できる。今回の手法はその可用性を算

出するための入力情報として活用できると考えている。

以上のとおり、適用できる場面は事例依存ではあるが、有用であり本手法あるいは類似手法による効果が期待できる。

6. おわりに

徳島大学における情報システムの BCP として、情報センターが平成24年度より取り組んできた事項について、BCP テスト結果の形で事例紹介するとともに、そのテスト結果から確認された課題についての考察を行った。また、テスト結果の考察から、BCP に影響するリスクの変化を定性的に評価した。その結果、その影響割合は低下しており、より確実な BCP としての改善が進んでいると言える。また、本手法が他の組織に適用できるかについて考察を行った結果、有用であると考察した。その一方で、本論文で述べたことは情報システム BCP 全体の一部であり、他の部分の BCP テストや見直しなど、継続的な改善の取り組みが必要である。

参考文献

- [1] 粕淵 義郎, 中野 晋, “国立大学法人における巨大災害時事業継続のあり方”, 土木学会論文誌 F6 (安全問題), Vol.68, No. 2, pp.58-65, 2012.
- [2] 総務省災害に強い自治体に関する研究会, “災害に強い電子自治体に関する研究会報告書”, http://www.soumu.go.jp/main_content/000222224.pdf, 2013 (2016.7.20 参照).
- [3] 松浦 健二, 上田 哲史, 佐野 雅彦, 関 陽介, 松村 健, 八木 香奈枝, “徳島大学における情報システム BCP 及び非常時のワイヤレスアクセスラインの整備”, 学術情報処理研究, Vol. 18, pp. 99-107, 2014.
- [4] JIS Q 27001:2014, 日本規格協会.
- [5] ISO/IEC 27005:2011, 日本規格協会.