サイエンティフィック・システム研究会
情報化された組織のセキュリティマネジメント WG　中間まとめ

「BCP」

2011 年 5 月 18 日

サイエンティフィック・システム研究会
情報化された組織のセキュリティマネジメント WG
《A グループ》

目次

まえがき

事業継続計画(BCP: Business Continuity Plan) とは、災害や事故で被害を受けた際に、重要業務をなるべく中断させず、中断したとしてもできるだけ早急に復旧させ、業務継続を実現させるための計画である。大学をはじめとする教育研究機関においては、多くの学生を抱え、学生の状況を速やかに把握し、教育業務が停止する期間を短く抑えることを目指すだけでなく、研究を、大学病院を有する大学の場合には診療の業務停滞を抑え、速やかに通常状態に戻ることを目指さなければならない。

情報化が進んでいる現在において、組織全体の BCP のなかでも、ネットワークやサーバーを管理運営している情報(ICT: Information and Communication Technology) 部門の復旧活動がキーとなることが予想される。広範囲の地域に及ぶ大地震や津波などの大規模災害の場合には、電力や水道などのライフライン復旧が第一に必要であるが、その後の復旧をスムーズに行い、同時に被災者と外部との情報共有、各業務の普及を考えた場合、ICT 部門の BCP を事前に構築しておくことは、たいへん重要である。

本報告は、大学等の ICT 部門が BCP を策定するために必要な情報を提供することを目指すものである。

活動メンバー

■全体

			氏名	機関/所属(2011 年 5 月 13 日現在)
会員	担当幹事		長谷川　明生	中京大学
	推進委員	(まとめ役)	山守　一徳	三重大学
			吉田　和幸	大分大学
			笠原　義晃	九州大学
			武蔵　泰雄	熊本大学
			湯浅　富久子	高エネルギー加速器研究機構
			鈴木　聡	高エネルギー加速器研究機構
			只木　進一	佐賀大学
			西村　浩二	広島大学
賛助会員(富士通)	推進委員	(まとめ役)	吉田　真和	富士通(株)
			飯島　敏治	富士通(株)
			南場　進	富士通(株)
			山路　光昭	富士通(株)
			桜井　秀志	富士通(株)
			山下　眞一郎	(株)富士通九州システムズ
			田口　雅晴	(株)富士通九州システムズ
			須永　知之	(株)富士通ｿｰｼｱﾙｻｲｴﾝｽﾗﾎﾞﾗﾄﾘ
	オブザーバ		山口　正雄	富士通(株)

■グループ

◆A グループ

テーマ: BCP、情報漏えい(重要情報持ち出し)、クラウド、認証

只木 進一 [班長]、湯浅 富久子、西村 浩二、山守 一徳、
山路 光昭、櫻井 秀志、山下 眞一郎、須永 知之

◆B グループ

テーマ: DNS

鈴木 聡 [班長]、吉田 和幸、笠原 義晃、武蔵 泰雄、長谷川 明生、
吉田 真和、飯島 敏治、南場 進、田口 雅晴

1. 教育 ICT 部門にとっての BCP

大学全体の BCP の目的を明らかにしていくことで、様々な対処の優先順位を決める指針を定めておく必要がある。教職員、学生の安全確保が最優先であることは明らかである。また、復旧活動にネットワーク等の情報基盤が不可欠であり、その後の業務復旧時には、様々な情報が不可欠となる。たとえば、認証データに基づいた安否確認、メールや Web を通じた情報伝達が災害直後に必要なる。また、多くの業務がネットワークに依存し、様々なデータが電子媒体に保存されている。ICT 基盤の復旧は、大学全体の業務復旧の前提となる。つまり、大学全体の BCP の中で、ICT 部門の BCP は非常に重要となる。従って、大学全体の BCP に取り組む一方で、ICT 部門だけでできる BCP を検討しておくことは、スムーズな復旧に欠かせない要件である。

1.1. 事前準備

災害時等に迅速にサービスを復旧させるために以下の事前準備が必要である。

1.1.1. 体制の取り決め

- 必要な人員の確保の仕方、発動させる基準を決める。
- 外部（ICT 部門以外の学内、業者など）への依存状況を整理する。
- 外部に依存できない場合の対策を検討する。

1.1.2. 対象システムの把握

- システム復旧の優先順位を事前に決める。
- システムの稼働条件を整理し、システム間の依存性を把握する。
- システムの設置場所、ラックの状況についても把握する。

1.1.3. 準備可能な物

- 災害時に備えた機材等の準備状況の確認し、整備する。
-

1.2. 大規模災害以外への対応

大地震などの大災害の頻度は非常に少ない。しかし、そのための BCP を策定することで、日常的に発生する様々な災害・障害への準備が可能となる。

- 大規模災害以外にも、サーバー攻撃、予定外の停電、伝染病等による要員不足などにも対応できる準備が望ましい。
- サーバー攻撃では、攻撃を受けた場合だけなく、攻撃元になってしまった場合の対応も考えておかなければならない。
- 予定外の停電、電力会社の給電不足による計画停電の頻発、落雷や事故による電圧変動なども考えられる。
- 伝染病などによる、要員の不足の際の対応体制も整理が必要である。

2. 教育研究機関 ICT 部門の特殊性

教育研究機関の ICT 部門には、以下の特殊性があり、BCP を検討する時に考慮する必要がある

(1) . オープンソース化が進んでいる

- 民間企業と比べると、オープンソース化が進んでおり、自組織によってメンテナンスしている割合が多く、自立性が高い。
- そのため、復旧時にも業者に応援していただくのは難である可能性がある。

(2) . 多様・多数のサービス

- 要員に対して、様々な多くのサービスを ICT 部門で稼働させているが、その中でコアサービスの数は少ない可能性がある。
- コアサービスは何であるのか把握し、重要度・優先度を検討しておく必要がある。ネットワーク、DNS、認証、Mail が最優先となるであろう。

(3) . 少ない人員

- ICT 部門の人員は極めて少なく、必要最小限に抑えられている。
- そのため、意思決定する時は容易ではある。
- キーとなる人材に頼りすぎているため、その人材が動けない場合には、事業継続が困難となりやすい。
- システム毎に複数の人員が対応できる準備ができていない場合もある。

(4) . 事務系との連携が悪い場合が多い。

- 命令系統が教学と事務に分かれ、教員職員と事務職員の間での連携が悪いことが多く、意志疎通がうまくいかない危険性がある。
- そのため、ICT 部門のセンターでできることが限られる。
- しかし、診療や事務もネットワークに依存しており、教学以外の重要情報システムを把握しておく必要がある。
- 大学病院は地域の中核医療施設であり、早急な復旧が必要である。

(5) . わがままな利用者

- 学内の利用者の方々から様々な要求が挙がり、わずかな人数の要求のためだけに振り回される可能性がある。
- 障害発生時の復旧のさせ方においても、恩恵を蒙る人数に比例して復旧されるとは限らない。
- BCP を作っておかないと、理不尽な要求に振り回される恐れがある。
- BCP を作る場合にも、出来る範囲を限定させるのに困難が伴うかもしれない。

3. BCP の基盤

BCP の基盤として、以下の項目を検討する必要がある。

(1) . 検討組織の構築
(2) . 情報システム・サービスの現状把握
(3) . 情報システム以外の施設設備の状況把握と対策
(4) . 重要情報バックアップ
(5) . 初期行動計画立案
(6) . 訓練
(7) . 緊急情報網
(8) . 運用体制の構築と維持管理

3.1. 検討組織の構築

まず初めに BCP の検討組織を作ると良い。検討組織の構築に当たっては、以下のことに留意すべきである。

(1) . 全学的検討組織が必要
- ICT 部門の BCP ではあるが、ICT の恩恵を受けていない人は皆無であろう。
- 検討組織は一部の部門だけの寄せ集めではなく、全ての部門が関わることが望ましい。
- ICT 部門の運営委員会などを通じて、学内の同意と学内への周知が必要である。

(2) . 全体を掌握しているコアメンバーで WG を作る
- 検討事項が幅広いため、全体を掌握しているコアメンバーでワーキンググループを作る。
- 素案を揉んでから、検討委員会で全体会議するのが望ましい。

(3) . センター定期打ち合わせなどで地道に策定
- 素案作成は少しずつ行うことになる。

(4) . ICT 部門の定期打ち合わせで議題に挙げ、地道に進めることが良い。
- できれば大学や研究所の BCP のひな型が欲しい。

3.2. 情報システム・サービスの現状把握

次に、情報システム・サービスの現状把握を行う。以下の点に留意する。

(1) . システム概要
- システムを概要把握する。

(2) . 設置場所とその概要
- サーバの設置場所とおおよそどういう場所なのかを把握する。
- ネットワークの経路やノードの設置場所もどういう場所なのかも把握する。

- ネットワークの線の経路およびその状況も普段より把握しておけば、災害時の断線推測する場合に役に立つ。

(3) . ハードウェア構成、保守業者

- ハードウェア構成を把握し、保守業者に関する情報を収集する。
- 起動時に必要な電力や、稼働中のピーク電力を調べておく
- 回線業者、機材ベンダー、保守業者等との関係を整理し、災害時の対応を協議しておくことが望ましい。

(4) . OS とアプリケーションのバックアップ状況

- OS は何であるか、アプリケーションのバックアップはどのように行っているのかを調べる。
- 設定、データのバックアップ状態を調べる。
- バックアップの保管先・保管場所の調査も行う。
- 本当に必要なデータは何かを見極める。

(5) . 再構築のコスト

- 故障した場合、再構築するのにかかるコスト（費用、設備、時間）を把握する。
- 現実的時間でリストアできるかも考えておく。

(6) . 代替の可能性

- 代替えサーバで稼働させることが可能であるのかを調査する。

(7) . 当該システムが依存している他システム

- 分散システムとなっているので、システム間の依存関係が重要である。
- 本システムが依存している他システムがないかを調べる。
- 復旧の順序を確かめる。

(8) . 本システムに依存している他システム

- 本システムに依存している他システムがないかを調べる。復旧の重要度に影響する。

(9) . 作業できる職員

- 復旧のために作業できる職員が誰であるかを調べる。
- 複数人が作業できるようになっていることが望ましい。

(10) . 全システムをやらなくても良い

- 全システムを復旧させる必要がないかもしれない。災害時故障発生を機会に停止のままとなるシステムもあり得る。

3.3. 情報システム以外の施設設備の状況把握と対策

情報システムは、稼働させるために電力などが必要であるため、以下の観点での調査把握が必要である。

(1) . 設置場所の環境

- 設置場所の耐震性などを把握しておく。
- 災害時に状況推測しないといけない場合に役に立つ。

(2) . 主要設備

- 設置場所は、何が整っている場所にあるのか。
- 建物設備についても把握しておく。

(3) . ラックの状況

- ラックの耐震固定状況、ラックの中の空き状況などを把握しておく。
- 復旧時に必要な部品が推測しやすくなる。

(4) . 電力

- 外部電源を使えるか。外部電源で稼働可能な時間を調べておく。しかし、非常用電源を ICT 部門で保有することは困難な場合が多い。
- 個々のブレーカーに繋がっている装置はどれか、各コンセントはどのブレーカーに繋がっているのか、ブレーカーの最大アンペアなども調べておく。
- システム更新時には調査されているが、その後の変更が分からない可能性が高い。

(5) . 通信手段

- 現場間で連絡を取って復旧作業に当たる必要がある。
- 固定電話や携帯電話などの通信手段を調べておく必要がある。
- トランシーバなど、携帯電話が不通時の要員間の作業時の連絡手段を用意しておく必要がある。

(6) . 通信回線

- 外部接続の回線の状況、キャリア、迂回路を確認しておく必要がある。
- 可能ならば、複数回線を持つ。とくに、病院はバックアップ回線が欲しい。
- 学内の建物･キャンパスを結ぶことができる無線 LAN 装置等を持っておくと安心。

3.4. 重要情報バックアップ

バックアップが重要であることは明らかであるが、以下の点を再度確認する。

(1) . 現状把握と対策

- 普段の運用状況を確認する。
- バックアップの不備が見つかれば対策を取る。

(2) . バックアップ方式

- 媒体は何を用いているかを整理する。
- その媒体を読み取る装置自身の故障対策があるかを調べる。

(3) . バックアップの内容

- バックアップに漏れはないのか、復旧させるのに必要なバックアップが揃っているかを確認する。

(4) . バックアップ頻度

- バックアップの頻度は適切であるのかを確認する。

(5) . バックアップ保管場所

- 保管場所自身の耐震性や防火性、防水性、盗難防止度合いなどの確認を行う。
- サーバと同じ場所ではなく、遠隔地への保管、大学間での相互保管などを検討する。

3.5. 初期行動計画立案

災害時の初動活動を計画立案しておくことが重要である。

(1) . 緊急連絡体制

- 緊急連絡網を取り決め、連絡が付かない場合の対処策まで用意しておくこと。
- 連絡網は伝達が途絶えることがあり得る。その対策が必要である。

(2) . 連絡先一覧

- 持ち歩けるような、個人情報を無くしたものも用意する。
- 出勤経路(徒歩で来れるかなど)も把握しておく。
- 組織内だけでなく、業者への連絡先も複数人で一覧管理していることが望ましい。
- コアメンバーが徒歩で参集できるかを確認しておく。

(3) . 事象、時間帯による体制

- 発生事象によって、初期活動が異なる。
- 発生時刻の時間帯によっても、初期活動が異なる。
- 場合分けにより取り決め、周知しておく必要がある。

(4) . 被害・状況の把握内容と手順

- 遠方からの僅かで不確かな情報しか入手できない場合が多い。
- 情報を出す側の技能レベルが期待できないだけでなく、情報を受ける側も人材不足から技術レベルが十分でない場合も想定される。
- 状況把握を行う手順を用意しておくと良い。

(5) . 復旧、代替の手順

- 復旧の手順や代替品を用意する手順を取り決めておく必要がある。
- 命令を出す指揮系統も混乱していることが想定される。
- 手順が事前用意されていれば、初動活動がスムーズに適切に行うことができる。

3.6. 緊急連絡網

(1) . 安否確認システム

- 全構成員に一斉メールを送る。
- 携帯電話アドレスをどうやって更新しておくかが課題となる。
- 他の目的としても日常的に使用しておくことで、携帯電話アドレスの更新を図り、稼働テストを日常的に行うことができる。

(2) . 緊急情報サイトの準備

3.7. 訓練

日頃より訓練しておくことが必要である。訓練は、BCP の見直しの機会として有用である。

(1) . 机上訓練

- 小さなグループ単位で、対応手順の確認を机上で行う。半日程度でも十分である。

(2) . システム復旧作業訓練

- 再構築の実施をしてみると良い。

(3) . シナリオによる訓練

- 災害時のシナリオを作って、業者も含めた連絡伝達訓練、故障原因調査訓練などを行う。
- シナリオは、訓練当日まで明かさない方が良い。

3.8. 運用体制の構築と維持管理

BCP を策定しておくことは、日頃の運用体制の見直しや維持管理の仕方の決定に大変役立つ。

(1) . 役割確認

- ICT 部門内での役割分担を明確化しておく。

(2) . 定期見直し

- 組織変更時だけでなく、サポート業者内の人的異動時、ICT 部門内での人材異動時など、人的体制の確認を行う必要がある。
- システム更新時や、新規システム導入時、旧システム廃止時など、システム構成の見直しを BCP の観点からも詳細に行う必要がある。
- 設置場所の変更やサポート業者内の変更など、環境要素に変更があった時に、維持管理の仕方や運用体制の見直しを行う必要がある。

(3) . バージョン管理

- バージョンアップを行った時、確実にバージョン管理を行うこと。

４．参考情報

(1) 内閣府「中央省庁業務継続計画」
http://www.bousai.go.jp/jishin/gyomukeizoku/

(2) 総務省「地方公共団体におけるICT部門の業務継続計画(BCP)策定に関するガイドライン」
http://www.soumu.go.jp/menu_news/s-news/2008/080821_3.html

(3) 中小企業庁「中小企業 BCP 策定運用指針」
http://www.chusho.meti.go.jp/bcp/

(4) 経済産業省「事業継続計画(BCP)策定ガイドライン」
http://www.meti.go.jp/policy/netsecurity/downloadfiles/6_bcpguide.pdf

ICT 部門の業務継続のための基礎的対策計画
第2版
(サンプル)

○○大学情報基盤センター

2011 年 4 月 1 日

表 1: 計画の改定一覧

版	日付	内容	承認者
暫定	2010/4/1	暫定的計画	センター長 佐賀太郎
初版	2010/10/1	初版	CIO 大学一男
第 2 版	2011/4/1	クラウドへ対応	CIO 大学一男

(注意)

- 本計画を改定 (一部改定を含む) した場合には、旧計画を速やかに回収し、新計画を配布するものとする。旧計画は情報基盤センター事務部門 (事務局情報企画室) にて保管する。
- 計画の改定は、上記履歴にて管理する。
- 本計画 (原本) の原本は情報基盤センター事務部門にて保管する。
- 本計画 (写し) は、情報基盤センター、情報基盤センター医学部分館、事務局情報企画室、事務局総務部総務課にて保管する。
- 本計画の写しを、センター長、副センター長、事務局情報企画室長、事務局総務部総務課長が自宅に保管する。
- 自宅に本計画の写しを保管するものの異動があった場合には、速やかに後任者にひき継ぐ。

目 次

第1章　趣旨・基本方針

1.1　趣旨

「業務継続計画」とは、大規模な災害、事故、事件等（以下、「災害事故」と略称する。）で○○大学の庁舎、職員等に相当の被害があっても、情報基盤センターの担う重要業務をなるべく中断させず、中断してもできるだけ早急に（あるいは、許容される時間内に）復旧させるために策定するものである。

○○大学情報基盤センターが平常時に提供しているサービスが長期間停止した場合、○○大学の活動に大きな支障が生じる。また、災害・事故の発生時は、たとえ庁舎、職員等に相当な被害が発生しても、地域の公共施設として、災害応急対応、災害復旧の業務を実施しなければならない。このため、災害・事故時においても○○大学の業務を実施・継続できるような周到な備えが不可欠である。

そして、このような○○大学の業務の実施・継続には、今日において、その業務を支える情報システムやネットワーク等の稼働が必要不可欠である。また、情報システムやネットワーク等は、あらかじめ対策を講じておかないと、災害・事故の発生後から対策を始めるのでは稼動できないことはもとより、早期復旧も困難であるという特性を持つ。そこで、全庁的な業務継続計画が必要との認識を持ちつつも、まずは「ICT 部門の業務継続のための基礎的対策計画」を先行して策定し、災害事故時の重要業務の実施継続を行うための基盤を整えることとする。また、初版においては地震を対象リスクとしているが、今後、対象リスクを広げて、どのような事象に対しても継続対応ができるように努めていく。

1.2　基本方針

1.2.1　ICT 部門の責務遂行

災害・事故時の業務の継続早期復旧に当たっては、ICT 部門として基幹業務に必要なシステムを早期復旧する。

1.2.2　来訪者、職員、関係者の安全確保

災害・事故時の業務の継続・早期復旧に当たっては、執務室等への来訪者、職員、契約先職員その他の関係者の安全確保を第一とする。

1.2.3　計画の有効性の維持・改善

本計画は、毎年、適切に関係者に周知し、訓練を行い、また常に最新の状況を反映した計画となるよう点検を行う。そして、それらの結果を踏まえて是正措置を講ずるとともに、少なくとも年に 1 度定期的に (前提条件に大きな変更があればその都度) 、計画の全般にわたる見直しを行う。

第2章　緊急対応

2.1　緊急時対応体制

大規模な災害・事故が発生した場合に、事前に定められた指揮命令系統にしたがって、正確に情報が収集・伝達され、的確に対応の指示や復命がなされるように、以下の組織体制で活動する。

2.1.1　センター長

本計画に従った緊急時対応の責任者として、以下の役割を担当する。

- ICT 部門の業務継続に関わる調査や対応活動の開始と終了の判断及び指示
- 情報システムの業務継続に関する方針や方法の意思決定
- ○○大学の災害対策本部への状況報告と本部決定事項の部門内への伝達
- 他の業務部門との調整の総括、支援依頼

センター長が不在の場合は、副センター長が役割を担当する。センター長、副センター長がともに不在の場合は事務局情報企画室長が役割を担当する。

2.1.2　対応要員と参集ルール

全員参集

職員 (非常勤を除く) は、次の場合には、全員自動参集とし、全員が対応要員となる。

- ○○市内で震度５強以上の地震が発生した場合
- 復旧見込みの立っていない大規模ネットワーク障害、停電が大学周辺で発生したことが報道された場合

安否確認

- 安否確認担当者は、事務局情報企画室長、その代理は事務局情報企画室係長とする。
- 安否確認の作業は、就業時間内は執務室で行う。夜間休日の場合、執務室に出勤して行うことを原則とするが、庁舎に入れない場合、参集ができない場合等については、庁舎の近隣の市の関連施設又は自宅で行う。

- 職員は、自動参集に該当する災害事故の発生時には、安否確認担当者に安否の連絡を行う。
- 安否確認担当者は、連絡のない職員に対して継続的に連絡を試みる。
- 安否確認の詳細は、安否確認マニュアルによるものとする。

初期対応による自動参集

震度 4 以上 5 弱以下の地震が発生した場合は、以下の初期対応要員が自動参集し、情報通信機器等の被害状況をセンター長に報告する。その後の対応は、センター長の指示に従う。

初期対応要員

- ○○一郎
- △△三郎

その他

その他、時間外における、情報基盤センターの停電、外部からの不正侵入の検知などがあった場合には、それらを検知した者がセンター長に報告し、その後の対応は、センター長の指示に従う。

2.1.3 外部事業者

A社・B社・C社においては、○○市内で震度 6 強以上の地震が発災した場合は、自動的に自社に参集することとしている。外部事業者の連絡先の情報の確認及び支援の要請に関して事前に調整する。

年次の計画見直しにおいて、協力関係の維持に関して各社に確認すること。システム更新等により協力関係を結ぶ企業に変更があった場合は、同様の協力関係を構築するように努める。

2.1.4 緊急時における行動計画

参集要領

ICT 部門の職員は、2.1.2 により参集し、システムの被害状況確認、対応活動を開始する。

実施項目 (初動対応項目)

就業時間内の場合

#	内容	確認	備考
1	来訪者職員等の負傷者対応、誘導		
	ICT 部門内及び周辺の学生、来訪者、職員（契約先職員等を含む。以下同じ。）で負傷しているものへの応急措置を行う。また、重傷者以外の来訪者については、次項の避難の必要性がない場合には、適切な場所へ誘導して集め、そこに当分の間、とどまるよう要請する。		
2	庁舎からの避難		
	避難指示があった場合又は庁舎にとどまっていると危険と判断される場合には、来訪者、職員を庁舎の外の安全な場所に退避させる。来訪者については、適切に誘導する。		
3	初期消火、延焼防止措置等の二次被害防止策		
	ICT 部門及びその周辺で火災が発生し、初期消火が有効であると判断される場合には、火災の発生を庁舎管理部門に至急連絡するとともに、可能な範囲内で初期消火を行う。		
	庁舎内で小規模な火災が発生し、緊急避難が必要でない場合には以下の措置を講ずる。 • 防火扉を閉鎖し、煙の侵入や延焼を防止する。鎮火後に、復旧等の対応活動を開始する。 • 緊急用システムを除くサーバ類を一旦停止する。		
4	職員その他関係者の安否確認		
	避難の必要がなく、負傷者対応、二次災害の防止への対応以外に手が空く要員が確保でき次第、センター長又はその指名する者が、点呼により職員の安否状況を確認する。ICT 部門への来訪者についても、職員に誰が来訪していたか報告させ、漏れなく安否を確認すること。		緊急連絡網
	外出者や休暇中の職員がいる場合は、固定電話、携帯電話又は携帯メールで連絡がつく範囲で安否確認を行う。ただし、至急連絡を取る必要がなければ、ある程度落ち着いてからでもよい。		
	外出者や休暇中の職員の安否が確認できない場合は、災害時伝言ダイヤル（171）を活用し、部門番号（0xx-xxx-xxxx）で登録された情報が無いかを確認する（なお、平常時より、171 は災害時に活用するよう職員に周知しておくこと）。		

#	内容	確認	備考
	センター長は、災害対策本部へ ICT 部門の安否確認結果を報告する。報告時間に定めがない場合、途中経過でよいので、本部の立上げを見計らって第一報をする。		
5	重要書類・データ類の保護		
	ICT 部門のフロアから退去が必要な場合（ただし、危険が迫り至急避難する場合を除く）、庁舎の損傷で漏水等が懸念されるなど、重要書類、バックアップ媒体等が損傷するおそれのある場合は、それらを庁舎内の安全な場所に移動させるか、庁舎外へ持ち出す。 重要書類やデータが損傷した場合、あらかじめ保管してあるバックアップ媒体を活用して、業務継続に必要な情報の復元処置を行う。		
6	外部事業者（保守ベンダ等）との連絡確保		
	保守ベンダ等の至急対応を要請すべき外部事業者との連絡手段を確保する。固定電話、メール、災害対策本部の災害時優先電話、携帯電話、携帯メールなどによる。そのほか、職員・外部事業者の従業員による直接の往来（状況によっては自転車等を利用）などあらゆる手段を使用する。		連絡先一覧
	業務継続に必須の外部事業者の要員については、連絡先一覧を参照して、連絡手段を必ず確保する。		
7	被害状況の調査		
	被害チェックシートを使用して情報システム、インフラに関する被害を確認し、必要な報告を行う。		被害チェックシート
	倒壊の危険がある庁舎、二次災害が発生している庁舎の場合、ICT 部門としては、入館可能かどうか庁舎管理部門に確認する。		
	被害状況は時間の経過により変化するため、継続的に監視を行う。		
8	業務継続・代替復旧活動の開始判断		
	センター長は、被害情報の報告結果及び要員の参集状況を考慮して、どのような業務継続の対応活動を開始するかを判断する (一部の業務継続の活動の開始の判断は、例えば情報が十分にそろうまで、後刻に先送りすることも考えられる)。		
	全庁の災害応急、復旧活動と整合を取りつつ、開始を決定した対応活動に必要な要員を指名し、情報システムの業務継続の体制を確立する。		

就業時間内の場合

#	内容	確認	備考
1	自己及び家族の安全の確認		
	災害・事故発生時においては、自己及び家族の安全の確認後、自宅の火災発生などの二次災害の防止を講じた上、次項の自動参集対応に入る。		

#	内容	確認	備考
	速やかに安否確認担当者に安否の連絡を行い、可能であれば出勤できる時間のメドも伝える。すぐにつながらない場合には、一定時間ごとに連絡を試みる。		
	自己又は家族が負傷した場合、自宅が大きく損傷した場合などは、参集できない旨を連絡する。		
2	自動参集対応		
	震度×以上の地震の場合、全員が自動参集する。震度はラジオ等で確認するが、確認できない場合、まずは参集を開始する。		
	参集に当たっては、通勤途上の安全に配慮し、靴、服装などに留意する。また、水、食糧を持参するよう努める。		
	規定の集合場所に自動参集する。集合場所から距離があり、公共交通機関が途絶している場合、参集するかの判断は、別に定める基準に従う（別途、参集基準を定めておく）。		
	自宅周辺及び参集途上において、救助の必要がある被害者がいる場合、参集すべきか救助に当たるべきかの判断は、別に定める基準に従う（別途、参集基準を定めておく）		
3	職員、関係する要員の参集状況及び安否の確認		
	ICT 部門の職員の参集状況及び未参集者の安否確認を行う。 • 安否確認担当者も出勤してに安否連絡を行う。 • 連絡がない職員には安否確認担当者が連絡を行う。 • 緊急連絡網に記述されている保守ベンダの責任者へも同様に連絡を行う。		緊急連絡網
	安否が確認できない職員がいる場合、災害時伝言ダイヤル（171）を活用し、部門番号（0xx-xxx-xxxx）で登録された情報が無いかを確認する（なお、平時より 171 は災害時に活用するよう、あらかじめ職員に周知すること）。		
	センター長は、災害対策本部へ ICT 部門の安否確認結果を報告する。報告時間に定めがない場合、途中経過でよいので、本部の立上げを見計らって第一報をする。		
4	重要書類・データ類の保護		
	ICT 部門のフロアから退去が必要な場合（ただし、危険が迫り至急避難する場合を除く）、庁舎の損傷で漏水等が懸念されるなど、重要書類、バックアップ媒体等が損傷するおそれのある場合は、それらを庁舎内の安全な場所に移動させるか、庁舎外へ持ち出す。 重要書類やデータが損傷した場合、あらかじめ保管してあるバックアップ媒体を活用して、業務継続に必要な情報の復元処置を行う。		

#	内容	確認	備考
5	二次被害防止策の実施		
	火災など二次災害が発生している場合は、一時的に緊急用システムを除くサーバ類を一旦停止し、災害での混乱が落ち着いた後、復旧を開始する。		
6	外部事業者（保守ベンダ等）との連絡確保		連絡先一覧
	保守ベンダ等の至急対応を要請すべき外部事業者との連絡手段を確保する。固定電話、メール、災害対策本部の災害時優先電話、携帯電話、携帯メールなどによる。そのほか、職員・外部事業者の従業員による直接の往来（状況によっては自転車等を利用）などあらゆる手段を使用する。		
	業務継続に必須の外部事業者の要員については、連絡先一覧を参照して、連絡手段を必ず確保する。		
7	被害状況の調査		被害チェックシート
	被害チェックシートを使用して情報システム、インフラに関する被害を確認し、必要な報告を行う。		
	倒壊の危険がある庁舎、二次災害が発生している庁舎の場合、ICT部門としては、入館可能かどうか庁舎管理部門に確認する。		
	被害状況は時間の経過により変化するため、継続的に監視を行う。		
8	業務継続・代替復旧活動の開始判断		
	センター長は、被害情報の報告結果及び要員の参集状況を考慮して、どのような業務継続の対応活動を開始するかを判断する (一部の業務継続の活動の開始の判断は、例えば情報が十分にそろうまで、後刻に先送りすることも考えられる)。		
	全庁の災害応急、復旧活動と整合を取りつつ、開始を決定した対応活動に必要な要員を指名し、情報システムの業務継続の体制を確立する。		

2.1.5 緊急連絡リスト

「スタッフの状況と緊急連絡先」を別紙により作成する。また、個人情報を最小限とした「持ち出し用緊急連絡先」を別紙により作成し、携行する。

2.1.6 被害チェックリスト

分類	項目	被害
要員安否	死者	名
	行方不明者	名
	負傷者	名
	参集者	名
	参集予定者	名
ライフライン	電気	あり・なし
	ガス	あり・なし
	水道	あり・なし
	電話	あり・なし
情報基盤センター	建物被害	あり・なし
	サーバ室被害	あり・なし
	電源設備	あり・なし
	空調設備	あり・なし
	通信設備	あり・なし
医学分館	建物被害	あり・なし
	サーバ室被害	あり・なし
	電源設備	あり・なし
	空調設備	あり・なし
	通信設備	あり・なし
事務局	建物被害	あり・なし
	サーバ室被害	あり・なし
	電源設備	あり・なし
	空調設備	あり・なし
	通信設備	あり・なし

- 要員の個々の安否は「スタッフの状況と緊急連絡先」(別紙) で行う。
- 情報システム個々の被害状況は「システム状況一覧」(別紙) で行う。

第3章　被害を受ける可能性と事前対策計画

3.1　リソースの現状 (脆弱性) と代替の有無

別紙によりリソースの状況を整理し、更新する。

- システム状況一覧
- 建物
- ラックの設置状況
- スタッフの状況と緊急連絡先
- 業者一覧
- 現状の脆弱性と対策計画
- 問題点

第4章　業務継続計画の運用体制

4.1　体制

センター長は、ICT 部門の事業用継続計画の運用の責任者であり、事業継続計画の立案、対策の実施と状況を確認するとともに、事業継続計画に関する教育・訓練を統括する。

ICT 部門のメンバーは、平常時に事業継続計画の維持管理として、定期点検、見直しを行う。また、対策状況の把握、改善、及び確認を行う。教育・訓練に参加し、事業継続計画を実質化する。

4.2　見直し

事業継続計画は、学期ごとに最新性と正確性を確認する。また、システム更新時に、全面的な確認及び見直しを行う。ただし、以下のように見直しの必要が生じた場合には、確認及び見直しを行う。

- 組織体制の変更
- 制度等の改訂
- システム更新以外のシステム構成の大幅な変更

4.3　見直しルール

学期ごとの見直しを行った場合には、センター長の承認の後、改訂記録に記述する。システム更新時及び大規模な見直しを行った場合には、センター長の確認の後、CIO の承認を得て、改訂記録に記述する。

4.4　見直し項目

4.5　訓練計画

机上訓練：センター長、教員及び技術職員、常勤事務職員が参加し、事業継続計画書を読み合わせ、各要員が緊急時に行うべき行動を確認する。

システム復旧訓練:バックアップデータからリカバリできるかと要する時間を確認する。

表 4.1: 学期毎の見直し

チェック	項目	補足
	人事異動や組織変更による事業継続要員の変更はないか	
	要員やベンダ等の電話番号やメールアドレスの変更はないか	
	計画書がすべて最新か	
	復旧用媒体、復旧手順が準備されているか	
	非常用電源、UPS、非常用通信手段が使用できるか	
	外部事業者との関係を確認する	
	机上訓練が実施されたか	
	訓練によって判明した課題が解決されたか	

表 4.2: システム更新時見直し

チェック	項目	補足
	新システムに対応して変更は必要ないか	
	検討された課題への対策・改善が実施されているか	予算等の課題
	外部事業者との関係の進捗を確認する	

対象情報システム			設置場所	ハードウェア			代替機	再インストール可能性	バックアップ状況				管理者		復旧手段	備考	他システムへの依存	
名称	サービス内容	主管部門	建物	機種名	ラック等	保守業者			分類	バックアップ	媒体	場所	主	副				
ネットワーク基盤	コアスイッチ	情報基盤センター	情報基盤センター本館	Cisco Catalist 6509	ラック1	○○ネットワークシステムズ	なし	対象外	設定内容	あり	CD	情報基盤センター本館	鍋島次郎	三日月二郎				
ネットワーク基盤	DNSサーバ	情報基盤センター	情報基盤センター本館	Sun Fire X2100	ラック1	××システム	なし	可	OS及びアプリ	あり	CD	情報基盤センター本館	三日月二郎	鍋島次郎			コアスイッチ	
								可	設定内容・データ	あり	CD	情報基盤センター本館						
認証基盤	ユーザデータベース	情報基盤センター	情報基盤センター本館	Sun Fire X2100	ラック1	△△コンピューティング	なし	可	OS及びアプリ	あり	CD	情報基盤センター本館	三日月二郎	鍋島次郎			DNSサーバ	
								可	設定内容・データ	なし								
認証基盤	LDAP主サーバ	情報基盤センター	情報基盤センター本館	Sun Fire X2100	ラック1	△△コンピューティング	あり	可	OS及びアプリ	あり	CD	情報基盤センター本館	佐賀太郎	鍋島次郎	ユーザデータベース内に準備済み		ユーザデータベース	
								可	設定内容・データ	あり	CD	情報基盤センター本館						
電子メール	IMAPサーバ	情報基盤センター	情報基盤センター本館	Sun Fire X2100	ラック1	△△コンピューティング	あり	可	OS及びアプリ	あり	CD	情報基盤センター本館	鍋島次郎	嘉瀬一子		旧機材あり	LDAP主サーバ	
								可	設定内容	あり	CD	情報基盤センター本館						
								対象外	データ	なし								
利用者ファイル	メインファイルサーバ	情報基盤センター	情報基盤センター本館	NetApp	ラック1	△△コンピューティング	なし	可	OS及びアプリ	あり	CD	情報基盤センター本館	鹿島末男	嘉瀬一子			DNSサーバ	LDAP主サーバ
								対象外	データ	なし								

名称	建築時期	新耐震基準	耐震補強	耐震診断結果	耐震改善予定	洪水の可能性	防火設備	延焼の可能性	入退室管理	非常電源
情報基盤センター本館	1990	未対応	不明	問題なし	なし	あり	通常	低	ICカード	あり
情報基盤センター医学部分館	1990	未対応	済	問題なし	なし	なし	通常	低	ICカード	あり
事務局情報企画室	1980	未対応	不明	不明	なし	あり	通常	低	磁気カード	なし

名称	設置場所	場所詳細	耐震	UPS能力	電源取り出し
ラック1	情報基盤センター本館	西側右端	ボルト止め	6000W	LP1
ラックM1	情報基盤センター医学部分	北側	ボルト止め	6000W	LP1
ラックR	情報基盤センター本館	東側中央	なし	3000W	LP2

管理者氏名	職	メールアドレス	勤務場所	職場電話	居住地域	自宅電話	携帯電話	携帯メール	私用メール
佐賀太郎	センター長	taros@cc.****-u.ac.jp	情報基盤センター本館	28-****	市内	0952-**-****	090-****-****	taro@****.ne.jp	taro@****.co.jp
鍋島次郎	准教授	jiron@cc.****-u.ac.jp	情報基盤センター医学部分館	28-****	福岡市	092-***-****	090-****-****	jjjs@***.ne.jp	
嘉瀬一子	係長	ichikok@cc.****-u.ac.jp	事務局情報企画室	28-****	小城市	092-***-****	090-****-****	ichikase@***.ne.jp	
三日月二郎	技術職員	mikazuki@cc.****-u.ac.jp	情報基盤センター本館	28-****	市内	0952-**-****	090-****-****	mikamika@***.ne.jp	
鹿島末男	准教授	kasima@cc.****-u.ac.jp	情報基盤センター本館	28-****	市内	092-***-****	090-****-****	kasikasi@***.ne.jp	

業者名	担当者	電話番号	地域	メールアドレス	携帯電話	携帯メール	契約状況		
							災害時SLAの有無	対応責任	サービス継続への対応
○○ネットワークシステム	福岡太郎	090-***-****	福岡市				なし	免責	あり
××システム	佐賀一郎		市内				あり	責任あり	なし
△△コンピューティング	長崎太郎		長崎市				なし	免責	なし

対象	現状レベル	対策内容	対策後のレベル	必要予算（千円）	実施目標	担当者
情報基盤センター本館	耐震レベルが不明	施設課を通じて確認する	耐震レベルの判明	要調査	2011年度	佐賀太郎
ラックR	耐震ボルト無し	耐震ボルトによる固定	耐震ボルト留め	200	2011年度	三日月二郎
ユーザデータベースのバックアップ	ない	バックアップ態勢	定期バックアップが行われる	なし	2011年度	三日月二郎
手回し充電器	ない	購入と配布	3台	10	2012年度	嘉瀬一子
IMAPサーバの運用	主担当者が退職予定	運用方法引きつき	主担当者の変更	なし	2012年度	鍋島次郎

問題点の内容	現状	当面の対策と効果	検討スケジュール	担当者
電子メールシステムのハードウェア保守業者との関係	災害時のSLA契約がない	現状のSLの確認	平成23年度以降	鍋島次郎
データバックアップの場所	センター内にしかない	サブセンターへの移送	平成23年度以降	鹿島末男

氏名	自宅電話	携帯電話	携帯メール
佐賀	0952-**-****	090-****-****	taro@****.ne.jp
鍋島	092-***-****	090-****-****	jjis@***.ne.jp
嘉瀬	092-***-****	090-****-****	ichikase@***.ne.jp
三日月	0952-**-****	090-****-****	mikamika@***.ne.jp
鹿島	092-***-****	090-****-****	kasikasi@***.ne.jp