情報系センターにおける健康危機対応事業継続計画の作成: 山口大学メディア基盤センターにおける事例

On Formulation of Anti-Pandemic Bisiness Continuation Plans for Information Processing Centers: A Case Study at Media and Information Processing Center of Yamaguchi University

市川 哲彦 †, 永井 好和 †, 小河原 加久治 ‡

Ichikawa, Y.†, Nagai, Y.†, Ogawara, K.‡

ichikay@yamaguchi-u.ac.jp, ynagai@yamaguchi-u.ac.jp, ogawara@yamaguchi-u.ac.jp

山口大学大学情報機構メディア基盤センター †
山口大学大学大学院理工学研究科 ‡
Media and Information Technology Center, Yamaguchi University†
Graduate School of Science and Engineering, Yamaguchi University‡

概要

近年情報セキュリティの重要性が認識され，情報セキュリティを組織的にかつ継続的に維持するための情報セキュリティマネジメントシステム (information security management system, ISMS) の構築・運用が重要視されるようなった．ISMS を構築する上で，リスクアセスメントと共に重要な役割を果たすのが事業継続計画 (business continuity plan, BCP) の構築である．これまでは地震などの大規模災害対策に注目が集まりがちであったが，以前より懸念されていた新型インフルエンザによるパンデミックが 2009 年に実際に発生したことから，大学における健康危機対策のための BCP 作成が急務となっている．BCP 中の手順には，Web ページを用いた学生等への連絡や電子メイルを利用したスタッフ間の連絡・協議等が含まれるため，情報基盤の継続性が大前提となっている．このことは，大学全体の情報基盤を担っている情報系センターにおいても BCP の策定が必要とされていることを意味している．そこで本論文では，BCP の構成要素や論点を整理した上で，山口大学メディア基盤センターにおける健康危機 BCP を構築した事例を報告する．

キーワード

ISMS, 事業継続計画

1 はじめに

個人情報保護法などの法整備によって情報セキュリティの重要性が再認識され，また数々の情報漏洩事故などが報道されるにつれ，情報セキュリティを組織的にかつ継続的に維持するための情報セキュリティマネジメントシステム (information security management system, ISMS) の構築・運用が重要視されるようになった．この傾向は一般企業に見られるだけではなく，大学のような教育・研究機関においても個人情報保護やセキュリティ教育の観点から ISMS が重要視されるようになっている [1] [2]．ISMS ではリスクを把握し適切な対策を施すことが大切であり，そのためリスクアセスメントが重要な役割を果たすが，加えて事業継続計画 (business contnuity plan, BCP) の策定と管理もまた重要な位置を占める．

BCP は英国規格 BS25999-1:2006 [3] では次のように定義されている:

> 組織が，あらかじめ定めた受容可能なレベルでその重要な活動を実施し続けることを可能にするため，何らかのインシデント発生時に備えて，開発され，まとめられ，維持されている文書化された一連の手順及び情報の集合体。

また，リスクアセスメントの一種ととらえることもでき，発生確率は低いが業務に多大な影響を与えるテロや地震などの脅威に対するリスク対応計画であるとも言える．ただし，通常のリスク対応計画がリスクの低減，すなわちインシデントの顕在化を防ぐことが目的であるのに対し，BCP は，リスク緩和 (risk mitigation)，すなわちインシデント顕在化後の影響を小さくし，迅速に正常状態に戻すことを目的としている点が異なっている．

BCP は大規模災害を対象としているため，企業や大学等の全組織的な取り組みが何より重要である．とはいえ，近年の組織活動は情報システムへの依存度が極めて高く，そのため，業務に必要となる計算機システム，データ，通信ネットワーク等の維持・復旧や，遠隔業務のための VPN 系統の臨時作成など，情報システム部門の機能が全組織的 BCP の大前提となっていることも事実である．実際，健康危機に関しての対策基準を定めた文部科学省の「新型インフルエンザ対策に関する文部科学省行動計画」[4] では，関係各所との連絡や情報収集の手段として，電子メイルや Web ページの利用が度々言及されており，テレコミュニケーション能力の喪失やサーバ類のトラブルによって各種 IT サービスの可用性 (availability) [1] が損なわれた際のインパクトの大きさを見て取ることができる．

以上のことから，大学における情報処理センター系組織でも情報基盤を維持するための BCP 策定が急務であると言える．本センターでは 2008 年に ISO/IEC 27001 (JIS Q 27001) に基づく ISMS 認証を取得し，これにあわせて BCP の策定や訓練なども実施している．取得時にもパンデミックは念頭に置いてはいたものの，山口県の自然災害の状況に鑑み，雷や台風による停電や洪水に対する BCP 構築に高い優先度を与えていた．これは，鳥インフルエンザの人から人への感染例が報告されなかったことから，パンデミックをあまり重要視しなかったためである．しかしながら，その後 2009 年に豚由来の新型インフルエンザが人から人へと感染することが報告され，世界保健機構 (WHO) も 2009 年 4 月 29 日に phase 5[2]，つまりパンデミックであることを認定したため，健康危機対応の BCP が社会的に脚光を浴びることとなった．これを受け，本センターでも健康危機対策 BCP の準備を行い作成を行ったので，本論文にて事例として報告する．他大学における実践の参考に少しでもなればと考えている．

なお，学部レベルの BCP には情報セキュリティの側面だけではなく，情報収集，広報活動，マスク・消毒用アルコールなどの安全対策，学生の健康管理の視点，休校・閉鎖などの判断基準，保健所等の他組織との連携，など様々な側面が含まれているが，ここで報告するのはあくまで情報セキュリティの維持のみを念頭においた BCP となっている点に注意されたい．

以降はまず BCP 作成プロセスを含む事業継続管理 (business continutity management, BCM) について概略を述べた後，特に健康危機対策のための BCP を作成する上で留意した点について説明を行う．これらを踏まえ，本センターにおける健康危機 BCP について説明し，最後に，まとめと今後の課題について議論を行う．

2 BCM の概略

本節では先ず ISMS における BCM の位置づけを ISO 規格における記述を中心に概観し，更にそれらを少し整理して，BCP 作成手順をまとめる．

2.1 BCM と ISMS

一般に BCP は企業の全社的な活動を対象として計画されるため，例えば製造業であれば，代替生産拠点の確保や，代替部品供給業者の確保などによるサプライチェーンの維持が重要な課題となるのであるが，情報通信企業や金融業のように業務の維持が実質的にコンピュータシステムの維持に等しいような企業だけではなく，製造業・物流業であっても，情報基盤への依存度が極めて高いのが現実であるため，BCP や BCM に情報セキュリティの側面を含めることは必須であると言える．実際，情報セキュリティの国際規格である ISO/IEC 27001 (JIS Q 27001) の実践規範を定めた ISO/IEC 27002 [6][3] では，その「第 14 節 事業継続管理」において，情報システムについての BCM を確立し，サプライチェーン管理などの BCM と統合し，組織の BCM において情報セキュリティの側面を盛り込むことを要求している[4]．より具体的には表 1 に示す 5 項目を要求している[5]．

[1] 認可されたエンティティが要求したときに，アクセス及び利用が可能な特性．[5]

[2] その後 2009 年 6 月 11 日に最高レベルの phase 6 に変更．

[3] 文書名は ISO/IEC 17799:2005 であるが，2007 年 7 月 1 日発行の正誤票で 17799 は 27002 と修正されている．

[4] 注: ISO/IEC 27002 は実践規範であるため should (〜することが望ましい) を使って記述されているが，対する ISO/IEC 27001 は要求仕様であるため shall (〜しなくてはならない) を用いて同様の事項を要求しているため，実質的に要求事項であると言える．

[5] 14.1.3 項では BCP の機密性保持に注意を払うことが要求されているが，本稿では情報セキュリティの観点から問題の無い範囲のみ記述してある．

表- 1: ISO/IEC 27002 第 14 節 事業継続管理 要求事項

14.1.1 事業継続手続きへの情報セキュリティの組み込み 事業継続のために必要な情報セキュリティに言及した BCM の確立を要求している．BCM は，リスクアセスメント，関連資産の列挙とインパクト分析，BCP の策定，定期訓練，からなる．
14.1.2 事業継続とリスクアセスメント BCM の一環として，事業継続を脅かすリスクを特定し，定量評価してその影響度を分析し，優先順位付けを行うことが求められている．
14.1.3 情報セキュリティを組み込んだ継続計画の策定及び実施 BCM の一環として，要求されたレベルでの業務継続と，要求された時間内での要求されたレベルまでの業務復旧を行うために BCP を策定することが求められている．BCP を構成する項目はこの項でも，また，次項 14.1.4 ではより詳しく，説明されている．BCP の配備の方法についても要求事項があり，脆弱性に言及しているので取扱いに注意すること，安全性を考えて必要な物資と共に遠隔サイトにもコピーを置くこと，代替サイトを利用する際には代替サイトにもコピーを置くことなどが求められている．
14.1.4 BCP 策定の枠組み BCP に含めるべき項目を定めることを要求している．また，どのような項目を含めるべきかについても言及されており，BCP の発動条件，緊急時手順 (emergency procedure)，代替運用手順 (fallback procedure)，臨時運用手順 (temporary procedure)，再開手順 (resumption procedure)，見直しスケジュール，教育・訓練計画，責任者・代替責任者，各種手続きを実施するのに必要な重要な資産と資源，などが列挙されている．
14.1.5 BCP の試験，維持及び再評価 BCM の一環として，スタッフが BCP で定められた手順を実施できるようにテスト (訓練) を行うことが求められている．テストには，机上テスト，シミュレーション，復旧テスト，代替サイトでのテスト，サービスの供給者のテスト，完全なリハーサル，などが考えられる．結果に基づいて BCP は適宜修正される．事業を取り巻く環境・顧客・法律や諸手続の変化に合わせて適宜見直しが求められる．

2.2 BCP 策定手順

上述の通り BCP を作成する際には，まず事業継続を脅かすリスクを特定し，その影響度を分析し優先順位付けを行うことからスタートする．これはビジネスインパクト分析 (business impact analysis, BIA) と呼ばれる作業である．BIA では，あわせて各業務についての目標復旧時間 (recovery time objective, RTO)，バックアップデータからの復旧をする際には目標復旧ポイント (recovery point objectvie, RPO) などを定めていく．

このような目標が定められれば，後はそれを確実にするための手順を定めることとなる．文献 [7] 図表 6 のフェーズ分けを参考にした上で，上述の文献 [6]14.1.4 の項目 (表 1 14.1.4) を用いて作成すべき手順を整理すると表 2 のようになる．

フェーズ 0 として準備手順を含めたのは，BCP の実施ではかなりの準備が必要となる可能性があるためである．例えば，データの安全なバックアップをする際には，遠隔サイトの確保，バックアップ用サーバの設置，安全な通信経路の確保，日常的なバックアップ業務のための手順の作成と代替運用手順への組み込み，などが必要とされ，予算確保も含めて相当な作業量となる可能性がある．また，BCP で共通に使われる手順の確立や文献 [6]14.1.5 (表 1 14.1.5) で要求される教育・訓練も準備フェーズに重要な活動と位置づけられる．

3 情報セキュリティインシデントとしての健康危機の特性

健康危機 BCP についても上記の通り BIA を実施したのち，どのような事態が発生するかを念頭に置きつつ BCP を構築することなるが，文献 [8] 付録 D-1 でも真っ先に指摘している通り，通常の BCP に比して，被害発生の様相がパンデミック等の健康危機では異なる点に注意が必要である．自然災害やテロなどの被害では広域にかなり壊滅的な打撃が及び，サイト，設備，人，情報などのあらゆるものが危機にさらされる．また，コンピュータウィルスの蔓延や主要通信路やサーバ類の障害は，情報基盤に依存しているほぼ全ての業務の停止を意味するため，他企業などへの影響を考えると極めて短い RTO での対応が求められる．しかも，いずれのインシデントもあらかじめ予見することは非常に難しい．それに対して，健康危機では世界規模の影響がある一方で，最初の感染が報告されてからパンデミック状態になるまで数週間のタイムラグがあり，ある程度インシデントの発生を予測することができる．そこで，我々は顕著な違いとして次のような事項を考慮することとした:

表- 2: BCP 発動前後のフェーズと利用される手順

STEP	フェイズ名	含まれる手順
0	準備	・BCP 中の各種手順を実施するのに必要となる資源の確保と配置をする． ・緊急連絡網の整備や安否確認手順など，緊急時に共通に必要とされる手順の確立を行う． ・個別手順についての訓練を施し，周知徹底を行う．
1	BCP 発動	・インシデントを検知して BCP の発動条件と照らし合わせ BCP を発動する． ・緊急時手順に従って以降の手順の準備を行う．
2	業務再開	・代替運用手順に従って，代替機器への切り替え，遠隔サイトの準備などを行う． ・臨時運用手順に従って，完全に復旧できないが重要な業務については業務を継続する．
3	業務回復	・緊急度の高い業務が再開された後，復旧範囲を拡大していいく．
4	全面復旧	・再開手順に従って本来の業務態勢に移行する．

予測可能性 新型インフルエンザの発生などパンデミックの徴候が報告されてから，実際にパンデミックになるまでにはタイムラグがあるため，関連するサービスプロバイダや部品供給業者と事前に協議することができる．

可用性喪失確率の低さ 大規模災害や主要情報設備のトラブルはそのまま情報基盤の可用性の喪失に直結するのに対し，健康危機が発生して BCP 発動が必要な状態になったとしても，情報基盤はそのまま稼働を続けるため，情報基盤の可用性がすぐに損なわれるわけではない;

要員不足による可用性喪失 急激な可用性喪失にはつながらなくても，システムの運用に携わっている職員の多くが感染あるいは感染の疑いによる隔離され，システムトラブルへの対処ができない可能性がある．そのため，平常時では迅速に対処できるシステムトラブルであっても，要員不足によって対処が遅れ長期の可用性喪失につながる恐れがある．また，窓口業務などにあたる職員をシステム運用に回すような臨時運用を行った場合，利用者対応サービスなど優先順位の低いサービスのレベルが下がる可能性がある．一時的な要員不足であれば影響は小さいが，パンデミックの波は数ヶ月周期で発生し，しかも一回の影響が数週間の単位で継続するため，通常の要員不足に比べて影響が大きくなる;

サプライチェーンの問題による可用性喪失 平常状態であれば容易に調達可能な代替部品が，健康危機の広がりによってサプライチェーンが切れることで調達できなくなる可能性があり，そのために長期の可用性喪失が発生し得る．また，部品供給だけではなく保守契約を行ってているケースでは，本来のサービスレベルでの保守サービスを受けられなくなる可能性があることも考慮する必要がある;

臨時オペレータの誤操作による機密性や完全性の喪失 人員不足による可用性の喪失を防止あるいは緩和するために，臨時オペレータが運用に当たる場合があり得る．その際，普段行わない装置を操作するので，誤操作等により情報漏洩や情報破壊などが発生する可能性がある;

自宅・病院などから遠隔アクセスの必要性 平常時は機密性確保の観点から自宅等からの遠隔アクセスを許可していない場合でも，職員が隔離されたり，何らかの理由でキャンパスへの立ち入りが制限されるケースでは，一時的にでも自宅等からの遠隔アクセスを許可せざる得ない状況が発生し得る．その際には，あらかじめ安全な通信路の確保や専用端末の準備をすることが必要になる[6] ;

関係者への事前説明の必要性 大規模災害であれば情報系センターも多大な被害を被ることが容易に想像されるため，各種サービスレベルの一時的な低下について関係者へ説明することは比較的容易と考えられる．一方，健康危機の際に問題となる人員不足やサプライチェーンの問題による可用性喪失は関係者には想定しづらい可能性がある．事前に可用性喪失のケースを関係者に説明し，サービスレベルの低下について理解を求めることが必要と考えられる．

[6]なお，平常時から実施されている自宅や代替サイト等からのアクセスによる業務は，遠隔アクセスによる業務ではなく，テレワーキングに分類される．テレワーキングを行い場所や装置には，キャンパス内と同様のセキュリティレベルが平常時から要求されるためこのような問題は発生しない．

4 本センターにおける健康危機対応 BCP

本センターでは 2009 年 6 月に「健康危機に起因する科学技術上のリスクに対応するための事業継続計画」の初版を定めた．ここで，健康危機はインシデントの文類，科学技術上のリスクは大学におけるリスクの文類であり，学内のセキュリティマニュアルにて定義されている．健康危機はパンデミックだけでなく，大規模な食中毒，毒物・化学物質による被害なども含む概念であるが，発生の可能性を考慮して実質的にパンデミックのみを念頭に置いて作成した．また，大学のリスクには運営・法規制・財務・社会的評価など様々な側面があるが，ここでは科学技術上のリスクへの対応，すなわち情報基盤の維持のみが念頭に置いてある．そのため，マスク・消毒用アルコールなどの安全対策や学生・職員の健康管理の視点は含まれていない．以降本節では，まず BCP 作成手順について述べ，引き続き作成した BCP についてサービスレベルの決定，手順作成，訓練について説明を行う[7]．

4.1 健康危機対策 BCP 作成手順

本センターの BCP 作成手順を図 1 に示す．ここで最も注意を払ったのは，スタッフの人員不足による可用性の喪失である．本センターはセンター長 1 名 (兼任)，副センター長 3 名 (兼任)，教育職員 9 名 (専任)，技術職員 2 名，事務補佐員等 5 名から構成されており，これらのスタッフが 3 キャンパスに分散して配置されている (2009 年 7 月現在)．人数的には，他大学の同様のセンターに比べるとやや多めである．従って人員不足による可用性の喪失は発生しにくいと考えられるかもしれないが，適宜業務分担を行っているため，オペレーション手順に関する知識や管理者権限などはすべてのスタッフで同一ではなく，主要サービスを通常時に担当しているスタッフが全員隔離されてしまうようなケースでは，迅速な障害対応等を行うことが非常に難しくなる．

そこで，サービスレベルを低下させてでも，サービスの優先順位に応じ限られたスタッフによりサポートを続ける方針を採用している．また，人員が間に合わず臨時運用体制でもサポートできなくなった場合の対処方法と，時間外サポートの有無についても方針を決定するように手順が構成されている．これは，前節で説明した「関係者への事前説明の必要性」に関係する．BCP は CIO が決裁をして初めて有効となるのであるが，その際に，組織としてこれらの方針を認めてもらい，関係者に事前に説明を行い了解しておいてもらうことを想定している．これによって，関係者の要求するサービスレベルと我々の実際のサービスレベルの違いにより発生するトラブルを避けることができると考えている．

この作成手順を構築するにあたって敢えて取り入れなかった事項が幾つかあるので，ここで説明をしておく．前節で整理をした通り，パンデミックではある程度の予測可能性を持つことから，実際にパンデミックになるまでのタイムラグを利用して，関連するサービスプロバイダや部品供給業者と協議することができる．BCM の観点からは，可用性喪失リスクを低減・緩和するために，我々から契約業者に対して BCP の説明を求め，保守，部品供給，緊急時の体制などを確認し，要求レベルに合致するか否かの協議を行うことが望ましいのであるが，パンデミックでは若干のタイムラグがあること，また，事態も流動的であるということから，今後の BCM の課題として残し，今回の BCP 作成では考慮しないものとした．ただし，緊急時連絡網には関係業者の連絡先等を記載し，協議が円滑に行えるように配慮した．

また，インフルエンザ等の飛沫感染の可能性のある疾病が流行した際には，患者との濃厚接触者が隔離されてしまうため，窓口サポートに来た学生や職員に感染者が出た場合には，特定キャンパスに配置された全スタッフが隔離されるケースも考えられる．その際には可用性喪失の事態によっては，スタッフの臨時配置換えによる代替運用をするのか，あるいは一時的な移動や遠隔保守を基本とした臨時運用体制を取るのかについても検討する必要がある．なお，本学の場合は，構成する 3 キャンパス間の距離が 40Km 以内であり，自動車による 1 時間以内の移動が可能であるため，臨時配置換えの措置ははあえて計画には盛り込まず，臨機応変な臨時運用体制で事態にあたることを念頭において BCP 作成手順を構成している．

4.2 サービスサポートレベルの決定

現在 29 のセンターの主要サービスが識別されており，内訳は，物理ネットワークサービス，ファイアウォール，論理ネットワークサービス，認証サービス，NTP サービス，電子メイルサービス，ホスティングサービス, など多岐にわたる．優先順位については基本的には 2 段階で考えている．すなわち，欠員状態になった際に，臨時運用体制を取って継続するサービスと，欠員に伴う可用性の喪失を受容するサービスである．スタッフ間で意見交換を行った結果，大学の広報活動と情報交換の手段としてコンピュータネットワーク，Web ページ，電子メイルが頻繁に利用されていることから，これらについては高い優先順位を与え，教室システムの維持管理，計算サービスなどの教育・研究寄りのサービスや，NTP の

[7]第 2.1 節の脚注でも述べたが，BCP はセキュリティ上の理由から公開しないのが普通であるため，差し支えに無い範囲での説明である点はご了承願いたい．

Step 1. **サービス内容の確認**
提供しているサービスをリストアップし，主担当者および副担当を確認する．

Step 2. **サービスのサポートレベルの決定**
健康危機の状況としては次のものを想定する:

一部キャンパス閉鎖	一部のキャンパスへの立ち入りが禁止となっている
全学閉鎖	すべてのキャンパスへの立ち入りが禁止となっている
欠員	サービスの担当者が感染等の健康被害によりサービスの運営に係わることが困難になった

各サービスの各発生状況について，緩和策を次の中から選択する:

学内遠隔保守	他キャンパスからサービスの運営継続を行う
学外遠隔保守	学外からサービスの運営継続を行う
臨時運用	サービス担当者内外で状況を連絡しあい応援担当者を含む臨時運営体制へ移行
受容	インシデントによるセキュリティレベルの低下を一時的に受容し，インシデントには対処しない

臨時運用体制の維持が難しくなった時の対応を次の中から選択する:

移転	外部業者に運用継続を依頼する
受容	インシデントによるセキュリティレベルの低下を一時的に受容し，インシデントには対処しない

勤務時間外のサポートについてサービスレベルを決定する:

時間外勤務	休日出勤などを含めた緊急体制へ移行する
通常勤務	通常のサポート時間をそのまま適用する

※ 可用性の喪失への対応が平常時よりも遅れる可能性が想定されるのであれば RTO を設定する．

Step 3. **インフルエンザ等特定疾病に関する留意事項の確認**
関係各所と連絡を取り，健康危機の原因となる典型的な疾病について留意事項の有無を確認する．

Step 4. *BCP* **発動条件を定める**
※ 基本的には全学の方針に従うので，危機管理対策本部の設置などを BCP 発動条件とする．

Step 5. **各種手順を定める**

準備手順	インシデント発生に備えるための手順
緊急時手順	インシデント発生時に行う手順
代替運用手順	インシデント発生時に待機系に切り替えるための手順
臨時運用手順	サービスレベルが維持できない時の臨時運用手順
再開手順	インシデントの影響が小さくなり，代替運用や臨時運用の状態から正常運用状態に戻すための手順

図- 1: 健康危機 BCP 作成の手順

ように一時的に停止していてもシステム運用全体に大きなダメージを与えない基幹サービスについては，低い優先順位を与えることとした．

保守については学外遠隔保守までを視野に入れるかどうかが，機密性の観点から重要になるが，今回の BCP 作成では，学外遠隔保守はしない，という方針とした．これは (1) 現在の ISMS 手順で原則として学外保守は禁止していること，(2) 健康危機では地震などと異なり通勤困難となる可能性は少ないこと，(3) 職員が隔離された場合でも電話連絡などで指示を与えることは可能であること，という理由からである．なお，スタッフへの感染を避けるために予防的に遠隔保守に切り替えることも選択肢として考えられることや，強毒性のインフルエンザによってキャンパスが閉鎖される可能性もあり得るため，トンネリングや VPN などを用いたオペレーション継続や，大学間連携によるサービスレベルの維持などは引き続き議論を継続したいと考えている．

また，当面は時間外対応はせず，また，スタッフの臨時運用体制が取れなくなった際にはすべて受容する方針を採用している．今後，大学の危機管理マニュアルなどが整備されるにつれ，臨時勤務体制などが明確になる可能性もあるので，その際には対応を再検討する必要がある．

RTO の設定については，本来であれば全組織的な要求が先にあって，各種制約条件を加味した上で実現手順を考えるのであるが，今回は現員スタッフで対応可能な RTO を設定することとした．今後大学の方針が明らかになれば対応は再検討する必要がある．現在の BCP では，主要スタッフの業務ができなくなった状況を想定し，優先順位が高く臨時運用体制をとるサービスについては，

$$\text{治療期間} + \text{隔離期間} + \text{対処期間}$$

とし，それ以外については他のサービスに要員が回される可能性があるため

$$2 \quad (\text{治療期間} + \text{隔離期間}) + \text{対処期間}$$

と考えることとした．現在報道されている範囲[8] では隔離期間が 7 日，治療期間は数日ということであるので，平均的な対処期間が高々数日であることを考えると，優先順の高いサービスで RTO は 2 週間弱，優先順位の低いサービスでは約 3 週間となる．

4.3 手順の作成

サービスの担当者の明確化と優先順位付けが出来てしまえば，健康危機 BCP では後の手順の作成はそれほど困難ではない．地震や台風による停電などでは，電源系統の代替設備への切り替えや，故障した装置の修理，遠隔サイトからのバックアップデータのリストアなど，注意を要する技術的な手順が多々含まれるが，健康危機では人員の安否確認とサービスの優先順位に基づく迅速な臨時体制が作れれば良いからである．手順をまとめたものを表 3 に示す．以下では各手順について概略を述べる．

準備手順には，安否確認や相互連絡のための緊急時連絡網の確認のみを含めた．自然災害とは異なり公衆電話網や通信ネットワークインフラが急激な影響を受けるものではないため，携帯電話やメイルアドレスによる連絡で十分に対処できるものと考えているためである．遠隔アクセスが必要な場合には VPN 等の通信設備や専用端末の準備が含まれるが，今回学外遠隔保守は基本的にはしないこととしているため，そのための設備は不要である．他にも，応援要請への迅速な対応を可能とし，臨時要員によるオペレーションミスに起因する機密性・完全性の喪失を防止するためのクロストレイニング (普段担当しないサービスについての訓練) の検討も必要があるが，健康危機であれば電話連絡等により遠隔から指示を出すことも可能であることから，現在は手順に含めていない．

BCP 発動時 (大学の緊急対策本部が設置時) に実施されるのが緊急時手順であるが，今回は特別な手順は定めていない．安否確認手順を含めるべきはないかとの意見もあったが，健康危機によるインシデントでは電話連絡等は可能であること，また，センター内のような比較的少人数であれば，把握は容易であると考え，特別に安否確認のための手順は含めていない．また，代替運用手順も特に必要ではない．

臨時運用手順では，連絡を密に取り合い，保守体制の維持ができているかどうかを常に確認することと，必要に応じて応援を依頼することのみが手順に含まれている．統括責任者やサービス関連の権限の明確化，権限委譲のルール，応援要請の方法や応援先の優先順位，などを細かに定めることも考えられるものの，場合分けや手順の詳細度を上げ過ぎると，かえってインシデントが発生した際の対処が難しくなる点が懸念されるので，どこまで詳細に定めるかは引き続き訓練・評価の中で検討を進めたい．

[8] CDC, “Interim CDC Guidance for Institutions of Higher Education and Post-secondary Educational Institutions in Response to Human Infections with Novel Influenza A (H1N1) Virus”, Mary 11th, 2009, http://www.cdc.gov/h1n1flu/guidance/guidelines_colleges.htm.

表- 3: 事業継続のための各種手順

準備手順	安否確認及び相互連絡のための緊急時連絡網の確認を行う.
緊急時手順	特になし.
代替運用手順	特になし.
臨時運用手順	【連絡】 スタッフは健康状態や隔離等により勤務ができない際には，自分が関係するサービスの各担当者にその旨を伝える．勤務に戻る際も同様である. 【応援要請】 各サービスの担当者は保守体制の維持が困難になった場合，応援を要請する. ・応援要請先は他のスタッフの健康状態，技術レベル，勤務状況によって決定する. ・その際，優先順位の低いサービスについては応援を要請しないこともあり得る. ・優先順位の低いサービスの担当者が高いサービスの応援要請を受けた場合は，後者への担当変更を優先する. 【応援解除】 応援が必要で無くなった際には応援要請を解除する. 【権限】 応援要請・解除の判断は各サービスの担当者が行う.
再開手順	保守体制の維持が困難であったために停止していたサービスを再開し，縮退業務体制から平常状態に戻す.

4.4 健康危機 BCP の訓練計画

上記 BCP のついて机上訓練を実施している．本 BCP を作成する上でもっと重要な点が作成手順のステップ 1 とステップ 2，すなわち，各サービスの運用担当者が誰であるかを確認し，実際の担当者自身にその意識を持たせること，及び，サービス間の優先順位を明確にし，縮退運用の方針を全スタッフで共有することであると考えている．そこで，机上訓練では全スタッフに会議に参加しておらい，これらについて確認を行った．また，緊急連絡網についても内容の確認を行い，欠員等出た際には各自で相互に連絡を取り合い，臨時運用体制での運用に参加するように依頼を行った．実地訓練については今のところ特に必要ないのではないかと考えているが，今後の事態の推移を見ながら BCM の枠組みの中で検討を行いたいと考えている.

5 まとめと今後の課題

2009 年に入って新型インフルエンザによるパンデミックを原因とした事業崩壊 (business disruption) が本格的に懸念されるようになったことを受け，本学メディア基盤センターでは「健康危機に起因する科学技術上のリスクに対応するための事業継続計画」の作成を開始した．本論文では，その背景，BCP 作成の手順，健康危機における留意事項について議論した後，本センターで実際に使用した BCP 作成の手順と作成した BCP の一部について説明を行った.

新型インフルエンザがどのような形に変異するかは流動的であり，毒性や感染経路などは様々なものが今後考えられる．しかしながら，今回作成した BCP はリスクパターンを細分化せず，健康危機に起因する人員不足によってシステムの可用性が喪失する，という基本的なケースをカバーすることを念頭において作成されているため，基本的な BCP として利用することができるものと考えている．さらに，事業継続上重要なインシデントの一つであるキーパーソンの喪失に対応するための BCP の作成にも活用できるのではないかと考えている.

今回 BCP を策定し訓練を行う過程で，各サービスの担当者の再確認と，担当者間の相互コミュニケーションの中でセキュリティを維持していく方針を改めて確認した．これは BCP の一部が平常時の業務体制にも反映されたと言え，いわゆる対策の日常化[9]にもつながったものと考えており，これが BCP の有効性につながっていくことを期待している.

現在の BCP にまだ未確定な部分があり，例えば，大学の BCP ポリシーによっては維持すべきサービスレベルが引き上げられて RTO を短縮する必要が出てくる可能性もあるので，今後も関係各所と連絡を取りながら検討を続けたい.

そのほかにも引き続き検討すべき課題は多々ある．まず，現在は計算機の保守契約や通信回線契約を結んでいるいわゆる第二者の BCP を確認中であること，が挙げられる．本来であれば契約時に BCP まで確認を行うべきであるが，これまで BCP についてはあまり重視されていなかったため，機密保持などの要求事項は契約に含められているが，BCP の基本方針についての開示などは契約書類の雛形に含められてないのが実情のようである．今後は改善を促すような活動が必要と考えられる.

次に，BCP の有効性評価方法についても検討が必要である．BCP は，BCM の PDCA サイクルの中で評価に基づいて継続的な改善を行うことが求められる．こ

[9]注: BCP 中の手順を特殊なものとせず，日常的な手順の中に組み込むこと.

れは通常のリスクアセスメントに基づく管理策の適用についても同様であるのだが，通常リスクアセスメントで考察の対象となるインシデントに比べ，BCP が発動されるインシデントは，可能性は少ないものの事業崩壊の規模が極めて大きいという特性があり，有効性評価を誤った際の影響が極めて大きい．我々は，机上訓練の結果として問題が無さそうであることをある程度確認しているものの，有効性測定方法は確立していない．今後の重要な課題の一つである．

最後にアウトソーシングの検討が挙げられる．現在考えている範囲では，システム運用の一部アウトソーシングによる人員不足への柔軟な対処，Web サービス・電子メールサービスの一部アウトソーシングによる代替運用体制の導入，などが挙げられる．機密情報なども管理対象になっているために慎重に進めるべき事項であるが，地震・台風などの災害への対応時にも検討が必要となる事柄であるため，今後議論の対象としたいと考えている．

謝辞

本研究は山口大学大学情報機構メディア基盤センタースタッフならびに静岡大学情報基盤センター長谷川孝博准教授の多大なる協力のもとに行われました．ここに記して謝意を表します．

参考文献

[1] 八巻, 藤本, 長谷川, 館野, 小林, 野崎, 中山, 岡田, 井上：“大学の IT コンプライアンス”, 静岡学術出版 (2007).

[2] 電子情報通信学会編：“情報セキュリティハンドブック第 5 編第 4 章”, オーム社 (2004).

[3] BS 25999-1:2006: “事業継続マネジメント–第 1 部：実践規範”, 日本規格協会 (2006).

[4] 文部科学省新型インフルエンザ対策本部：“新型インフルエンザ対策に関する文部科学省行動計画”, http://www.mext.go.jp/a_menu/influtaisaku/ (2008).

[5] JIS Q 27001: 2006 (ISO/IEC 27001:2005): “情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステム要求事項”, 日本規格協会 (2006).

[6] ISO/IEC 17799:2005: “情報技術 – セキュリティ技術 – 情報セキュリティマネジメント実践のための規範”, 日本規格協会 (2005).

[7] 経済産業省企業における情報セキュリティガバナンスのあり方に関する研究会：“企業における情報セキュリティガバナンスのあり方に関する研究会報告書”, http://www.meti.go.jp/policy/netsecurity/downloadfiles/sec_gov-report.pdf (2005).

[8] Federal Finacial Institutions Examination Council (FFIEC): “Business Continuity Planning”, FFIEC IT Examination Handbook, http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#bcp (2008).