特　集

大学における緊急事態対応計画と業務継続計画への提案

総合情報基盤センター　教授　高井正三

東日本大震災を体験し，情報システムのみならず，企業や行政機関における不測事態対応計画や業務継続計画の策定とその実施訓練が再認識され，我が国における BCP/DR（Business Continuity Planning/Disaster Recovery：業務継続計画／災害復旧）は「再拡大期」にある[1]という．1995 年 1 月 17 日の阪神・淡路大震災以降，先進企業等で BCP が整備され始め，2001 年 9 月 11 日のアメリカ合衆国で起こった同時多発テロを契機に，先進的企業から一般企業へ，国内対応からグルーバル対応へと BCP 拡大期に入った．しかしながら，2011 年 3 月 11 日の東日本大震災では，整備した BCP が機能せず，想定の範囲を遙かに超えて，福島の第一原発の放射能汚染が，国内のみならず国際問題までに発展した．東北地域の復旧・復興が遅々として進まない現実こそは，余りにも増えすぎた危機事象とそれに対応できない BCP/DR の考え方の変化，複合的に発生する危機事象への対応という大きな問題に直面している証である．本稿は大学の情報システムにおける緊急（不測）事態対応計画とその後の業務継続計画を提案しているが，大学全体，一般企業や行政機関にも参考になるよう，セキュリティ・ポリシーの核となる重要テーマとして提案するもので，今後の大学における BCP 策定と運用に活かして欲しい．

１．セキュリティ対策のこれまでの経緯

筆者は，平成 13（2001）年 10 月 4 日，富山大学黒田講堂会議室で開催された第 13 回学術及び総合情報処理センター研究交流・連絡会議で「４．セキュリティ・ポリシーの策定について」という討議議題を掲げ，本格的な大学におけるセキュリティ・ポリシー策定の必要性と実施体制，更にはサンプル・ポリシーを提案し，続く 2002 年 3 月発行の総合情報処理センター広報誌に「セキュリティ・ポリシー（案）の策定について」[2]を発表し，その第 3 章(2)基本ポリシーの記載事例「７．業務継続計画」の中で，「当該セキュリティ・ポリシーは，別途規定してある緊急対応計画との整合性を図り，障害やサイバー・テロリズムなどの脅威に対しても，業務継続性を維持できるセキュリティ管理策を講じるものとする.」と提案し，（4）情報セキュリティ・スタンダード（基準,規約）（案）で，5.1 教職員・学生の利用者向けスタンダード項目(16)緊急事態対応スタンダード，5.2 管理者向けスタンダード項目(19)緊急事態対応スタンダード，5.3 一般セキュリティ規定(8)業務継続で，「地震，風水害，火災，テロリズムなどの事態が発生したときは，業務継続計画に従って行動する．また，業務継続計画に従って行動できるように定期的に訓練を実施する.」と提案し，(6) プロシージャー（手順）に続く（7）の例：個別の運用規定／マニュアルで，復旧計画の立案と計画の実施，動作確認手順の確認など，具体的な緊急対応マニュアルを提案しているが，その内容は決して古びてはいない．

この記事は，当時発行された日経バイト誌「ゼロから始めるセキュリティ対策（著者：足利俊樹，株式会社ラック）」から，一部転載許可を得て記述したものであり，著者の足利氏から原稿の添削支援を受けた労作である．

2002 年 3 月 11 日～13 日には，富山大学先端技術研修プログラムで筆者が講師となり，情報処理コース（セキュリティ・ポリシーの策定と運用）を開講した．このコースでは，企業における具体的なセキュリティ管理を遂行するための手順，セキュリティ・ポリシーの策定方法とその効果的な運用方法を習得し，受講者の企業におけるリスク分析を経て，セキュリティ・ポリシー（案）を策定することを目標にしたところ，県内企業から若手技術者（28 歳から 42 歳）8 人が受講した．

歴史を遡ってみると，大学関連では文部科学省通達として，2001 年 6 月 15 日付けで，文部科学省大臣官房政策課長から，「情報セキュリティ対策について(依頼)」文書が出され，各大学で情報セキュリティ・ポリシーを策定

の上，情報セキュリティ実施手順を作成し，セキュリティ対策に遺漏のないよう通達があった．そして，2000 年 7 月 18 日付け内閣の情報セキュリティ対策推進会議で決定した「情報セキュリティ・ポリシーに関するガイドライン」と，2000 年 10 月付けの「A 省情報セキュリティポリシー（例）」［厳重取扱注意］（24 ページ＋参考 9 ページ）が添付されていた．

更に，2001 年 7 月 30 日には，文部科学省の情報セキュリティセミナーが開催され，セキュリティへの脅威，現状，技術，課題が示され，情報セキュリティ・ポリシーの考え方，必要性，策定の手順などが，具体的に提案された．

しかしながら，ガイドライン的な内容が大部分で，具体的なサンプルがなかったので，筆者のサンプル・ポリシーを参考にいくつかの大学で，情報セキュリティ・ポリシーが作成され，公開された．筆者も 2001 年 9 月 18 日付けで，「大学におけるセキュリティ・ポリシーの策定とその実施方法（A4 判 49 ページ）」を作成し，当時の経理部経理課情報企画係のスタッフと大学の情報資産の洗い出しと情報システムのリスク分析を行った．2001 年当時は皆さん結構燃えていたのだが，遂に，対外に公表されている富山大学版情報セキュリティ・ポリシーは未だに存在せず，従って緊急事態対応計画，業務継続計画も，日の目を見なかったようである．

平成 21 年 1 月 27 日（火）に開催された，平成 20 年度第 21 回役員会議事要旨よると，山西潤一理事・副学長から，「国立大学法人富山大学情報システム運用基本方針（富山大学情報セキュリティポリシー）」（案）及び「情報セキュリティ・インシデント対応基準」（案）について，制定理由及び制定案について説明があり，審議の結果，原案どおり了承され，実施日は平成 21 年 1 月 27 日とされた．とあるが，読んでもらえば，おおよそ，情報セキュリティ・ポリシーからは程遠いものであることは，素人でも分かる．

２．危機管理とリスク管理

危機管理とリスク管理は違うので，どこが違うのかを順を追って明らかにしたい．

2.1　用語の定義

（１）危機（Crisis）とは

危機とは，生命が脅かされ，そのものの存立・基盤などが危うくされる恐れの感じられる，絶体絶命の場合を指している[3]．

東日本大震災で海外の News Site では，Fukushima Nuclear Crisis（福島核危機）というように，「危機」という言葉が盛んに使用された．国立大学法人富山大学危機管理ガイドライン[4]によると，第 2 章に言葉の定義があり，危機＝「災害及び火災のほか，テロ，重篤な感染症などの重大な事件や事故で職員及び学生等の生命もしくは身体または大学法人の財産，名誉もしくは組織の存続に重大な被害が生じ，または生ずるおそれがある緊急の事象及び状態」と定義され，様々な「危機」が発生する可能性（＝リスク）と注意書きされている．

情報セキュリティ・ポリシーの制定に当たっては，用語の定義を明確にするため，規則の中で定義するのが一般的である．次に関連用語を定義するので，確認して欲しい．

（２）脅威（Threat）とは

組織や情報システムに恐怖や被害を与え，情報資産の損失を招く直接的な原因のこと．災害，障害，操作ミス，コンピューター犯罪，ネットワーク犯罪，テロリズムなどで，以下詳しくみてみよう．

(1)発生源からみた脅威

1）災害による脅威

地震，洪水，津波，落雷，火山の噴火，台風，高潮（富山湾では「寄り回り波」も），竜巻，地滑り，隕石落下など，自然災害による建物の倒壊・破壊・消失によって，情報通信システムが停止，復旧不能となる．

2）障害による脅威

・予期せぬハードウェア障害，ソフトウェア障害（ソフトウェア・バグによるエラー，モジュールのバ

ージョン不適合），ネットワーク障害，空調機などの設備故障，過負荷による動作異常，停電・瞬断等電源異常によって，情報通信システムが停止，復旧不能となる．
・入退館・入退室管理装置，監視カメラ，情報システム運用環境監視装置，情報システム運用監視装置，ネットワーク監視装置などの故障により，施設・設備の安全管理，情報通信システムの動作管理が停止・停滞し，運用や運用記録に支障・中断が生じる．
3）人為的行為による脅威
・操作ミスなど，過失によって，情報通信システムが停止，復旧不能となる．
・コンピュータ犯罪，ネットワーク犯罪など，不正攻撃によって，情報通信システムの運用が妨害され，異常停止し，復旧不能となる．
・火災や陸・海・空の交通事故など，人災による建物の破壊行為や直接的なシステム破壊行為などによって，情報通信システムの運用が妨害され，異常停止し，あるいはデータの破壊・消失によって，復旧不能となる．
・飛行物体の墜落，戦争やテロリストによるミサイルや爆弾（自爆を含む）による破壊行為によって，情報通信システムの運用が妨害され，異常停止し，復旧不能となる．
・凶悪犯による不法侵入・不法入室，不法占拠，破壊行為，暴力行為，殺人行為，放火行為，異常者の破廉恥行為など，人災による建物の破壊行為や直接的なシステム破壊行為などによって，情報通信システムの運用が妨害され，異常停止し，あるいはデータの破壊・消失によって，復旧不能となる．

(2)行為からみた脅威

1）ネットワーク攻撃
不正アクセス，盗聴，なりすまし，改ざん，否認，ウィルス／ワーム感染，スパイウェアなどの不正プログラムの組み込み，踏み台，サービス不能攻撃，間接的攻撃，SPAM メールなど．
2）不正使用
許可された使用目的以外の，情報システム資源の正しくない使用行為．
3）運用妨害
情報の窃盗，漏洩，改ざん，破壊，消失．
4）過失
操作ミスによるサービス停止，運用妨害，データや情報の消失，設備や書類等の情報資産の紛失
5）侵入
・建物やマシン室などへ物理的な侵入
・ネットワークを経由した不正侵入
6）盗聴
音声の盗聴，ネットワークからのパケット盗聴
7）破壊
物理的なデータや機器・設備の破壊，プログラムやデータの消去
8）改ざん
プログラムやデータの不正な書き換え
9）窃盗
・コンピュータやネットワーク機器などの物理的な窃盗
・プログラムやデータの窃盗（不正コピー，不正閲覧を含む）
10）なりすまし
正当な権限を持つ利用者，管理者になりすまして，建物や情報システムに侵入する行為．
11）否認
自ら行った注文，依頼，受領などの行為を，後から否定する行為
12）踏み台
・目標とするコンピュータや情報システムへ侵入・攻撃するために，セキュリティ対策の未熟な第3者のコンピュータや情報システムへ侵入し，そこを攻撃拠点として使用する行為
・サード・パーティ・リレー（Third Party Relay）は，SPAM メールなど不正なメールの発信源を第3者のメール・サーバを経由して発信したかのように見せること．
13）不正プログラムの組み込み
・キー・ストローク・ロガー（キー入力のログ記録ソフトウェア）など，本人の知らぬ間に趣味や嗜好・個人情報を収集し，ネットの特定の場所に送るプログラムをスパイウェアというが，このスパイウェ

アなどの不正プログラムを，他人のコンピュータに許可なく埋め込む行為．

14）サービス不能攻撃（DoS：Denial of Service）

・攻撃目標とするWebサイトに対して，大量のパケットを送りつけて，ネットワーク・トラッフィックを溢れさせ，当該 Web サイトのサービスを不能にする運用妨害攻撃

・複数台の攻撃用コンピュータを用意して，攻撃目標とする Web サイトに対して，一斉に大量のパケットを送りつけて，ネットワーク・トラッフィックを溢れさせ，当該 Web サイトのサービスを不能にする運用妨害攻撃は，分散型サービス不能攻撃(DDoS)という．

15）間接的攻撃

・Web サイトをアクセスするだけで，トロイの木馬型不正プログラムやウィルスを強制的にダウンロードさせられ，被害を受ける行為

・悪意をもったサイト管理者が Web ブラウザの Java 実行環境などのセキュリティ・ホールを突いて，ユーザーのハード・ディスクの中身を覗き見たり，削除したりする行為．

16）倫理観欠如による悪意の行為

・職員（社員）が個人の利益を尊重し，会社(企業)の不利益を省みない行為（サービス妨害，物理的破壊，窃盗，情報の窃盗，破壊，消失など）

・職員（社員）が小遣い欲しさに，会社(企業)の情報を漏洩する行為

(3)現象からみた脅威

1）事故

情報通信システムの故障，予期せぬシステムと環境の物理的な障害のこと

2）輻輳

ネットワーク用通信網のパケットが混み合う現象

3）過負荷

情報通信システムに処理能力以上の負荷が掛る現象

（３） 災害（Disaster）とは

・災害対策基本法（抜粋）の定義

災害とは暴風，豪雨，豪雪，洪水，高潮，地震，津波，噴火その他の異常な自然現象又は大規模な火事若しくは爆発その他その及ぼす被害の程度においてこれらに類する政令で定める原因により生ずる被害をいう．

・災害対策基本法施行令（抜粋）の定義

政令で定める原因は，放射性物質の大量の放出，多数の者の遭難を伴う船舶の沈没その他の大規模な事故とする．と定義しているが，最近では**突然発生する広範囲の竜巻**や**一時的な集中豪雨による大規模な地滑り**など，**複合的な被害**が多くなって来ている．

30 年ほど前に，変電所に落雷して大規模停電が発生して，復旧までにかなり時間がかかっていたが，昨今の極寒，寒冷地で長時間の停電が発生すれば，生命を脅かす大規模災害になりかねず，科学実験や情報通信サービスに大きな被害をもたらす．

また，最近多い，**伝染病（鳥インフルエンザや新型インフルエンザ等）や感染症（麻疹，風疹，サーズ SARS や学校でのノロウィルス感染）などの感染拡大と収束に時間を要する場合の被害**も無視できない．

更に，部品や燃料が入荷できないために工場の操業停止を余儀なくされ，計画停電で定常運転が不可能になり，事業縮小や時短勤務，生産縮小，取引量減少など，被災による二次的な被害が増大している．福島第一原発事故の放射能汚染の風評被害も同様である．

（４） リスク（Risk）とは

情報資産に被害または損害をもたらす可能性のこと．リスクとは本来，損失または利益をもたらす可能性または不確実性のことをいうが，利益と損失の両方をもたらすリスクのことを投機的リスクといい，損失のみをもたらすリスクのことを純粋リスクという．一般にリスクと言えば後者のリスクをいい，ここでは**情報資産を対象とし，必ず営業損失を伴うもの**と定義する．

大学の危機管理ガイドラインでは，様々な「危機」が発生する可能性，と定義して，以下のリスクを列挙し，損失の例を記述している．

（1）運営リスク・・・大学運営に関して生ずるリスク：建物の滅失，中核職員の離職（**他機関からの**

引き抜き), 教育・研究が不可能になる損失(インフルエンザなど伝染病の感染, 麻疹やノロウィルスによる感染拡大, ・・・)

(2)法規制上のリスク・・・法律や規制に関連して生起するリスク:法令や規則違反の罰課金や交付金・補助金の取り消し, 施設の閉鎖や研究業務の中止による損失.

(3)財務的リスク・・・資産に対するリスク:組織の施設の滅失, 財産の盗難, 著作権侵害による資産の第三者への移転, 金融資産の価値下落.

(4)名声に関わるリスク・・・立法関係者や国民の大学に対する評価の低下を指すリスク:受験者(倍率)の減少, 競争的資金の獲得状況の低下の公表に伴う評価の低下, 学生・職員の不祥事による大学評判の低下, 同窓会入会金納入率の減少・寄付金の減少.

(5)科学技術上のリスク・・・情報通信技術の発達に伴うリスク:各種サーバーへの攻撃の増大とクラッキングによる被害の増加など.

(6)その他のリスク

・病院における医療ミス/事故によるリスク

・構内外の交通事故によるリスク

・各種リスクに起因する訴訟等のリスク

・学生・職員が被害者となる事件・事故のリスク

・教育活動(アウトドア活動・野外実験・研修での事故, **単位誤認定や記入ミスによる卒業認定の取り消し, 体罰・注意や警告による学生の自殺, 教育施設・設備の破壊的行為, ・・・**)のリスク

以上のリスクに対して, 営業損失の概算がないため(恐らく算出できないのであろうが), どれくらいの損害・損失を受けるのか, 想像できない.

2.2 危機管理

以上の定義から, 危機管理は, 脅威(Threat)や災害(Disaster)が発生し際, または重大なリスクが発現した場合に, 学生・職員の生命を脅かす様な被害, 大学法人の資産や組織の存続に重大な被害が生じた際に, どのように対応し, 被害・損失を最小限に抑えるよう管理することである[5].

即ち, (1)平常時の準備, (2)危機発生時の対応, (3)危機発生後の対応, がポイントとなる.

(1)平常時の準備

危機管理マニュアルを作成し, 危機に備える. 大学版「危機管理ガイドライン」に示されている個別の「**緊急事態対応計画(対応マニュアル)**」を作成し, 具体的な行動をマニュアル化すべきである. 更に, マニュアルに従って想定訓練を, 体が自然に動くようなるまで, 重ねる必要がある. 最近の「防災訓練」のように.

(2)危機発生時の対応

対応組織を設置し, 迅速かつ的確に対応し, 情報管理を行って, 被害の拡大を防ぐ.

(3)危機発生後の対応

速やかに復旧し, **業務継続計画(BCP)**に基づいて, 事業活動を再開する.

本学の危機管理規則では,「本法人の職員及び学生等の安全確保を図るとともに, 教育研究活動の実施を確保する」としているが, 本文を読んでいくと,「危機が発生し又は発生するおそれがある場合」と表現が曖昧になり, 多分にリスク管理的要素が入り組んでいる.

2.3 リスク管理(Risk Management)

一方, リスク管理は, リスクが発現しないように, リスクを管理することである[5].

このリスク管理は, PDCA(Plan-Do-Check-Action) サイクルに基づき, 次の 5 段階の手順で実行するのが一般的である[3].

(1) 基本方針の策定

何のために何をして欲しいのか, 目的と行動指針を明示し, 職員・学生に伝える.

(2) 基本計画の策定

1)大学が直面しているリスクを把握・分析し, 優先順位を付ける. 縦軸に被害・損失の大きさ, 横軸に頻度を取ったリスクマップを作成し, 頻度が高く, 損害の大きいところを最優先として, 優先順位を付ける(試作図 1 参照).
2)戦略として, 回避, 低減, 移転, 受容の 4 つから選択して, 3)達成すべき目標と対策の方向性を決め, 4)対策が完了するまでの期限を決める.

(3) 対策の実施の策定

対策を講じるためにリスクを細分化し, そ

れぞれに Action Plan を立て，実行する．

（4）モニタリング

実施が形骸化しないために，2 通りでモニタリングをする．1 つは第三者が実施するリスク・マネジメント監査であり，他の 1 つは自己評価（Self Check）である．

（5）是正・改善

モニタリングで発見された問題を，経営のトップに報告し，レビューを実施して，是正・改善計画を立て，早い機会に計画を履行する．

3．大学における緊急事態対応計画の提案

3.1　大学の情報システムにおける緊急事態対応マニュアル（案）

資料番号４０１　緊急事態対応マニュアル（第 99 版）を参照

3.2　大学における緊急事態対応マニュアル

現在作成されている危機管理ガイドラインを整理して，危機管理とリスク管理を区分して，後述の BCP を含めて具体的なマニュアル（「危機管理マニュアル」，「リスク・マネジメント規定」，「リスク・マネジメント・マニュアル」）を作成し，重要な部分と連絡体制は「キャンパス・ガイド」と「在学生・教職員」向けのホームページに記載すべきと考える。

4．大学における業務継続計画への提案

4.1　企業における BCP のトレンド

東日本大震災以降増えたのが危機の複合的な事象に対応するよう，地震リスクを想定した BCP と，新型インフルエンザを想定した BCP で，この 2 つの BCP を策定している企業が多くなっているという．

最近では冷凍食品に農薬が混入されていて，この冷凍食品を食べたユーザー3,000 人近くが健康被害を受け，回収対象が 640 万パックにのぼり，関係会社の社長が辞任に追い込まれている．また，浜松の小学校で，1,000 人以上の児童がノロウィルス感染し，数日間休校という事態を引き起こしたパン製造会社と製造したパンの大量回収もまた，BCP の課題である．これらの商品の回収に多額の費用が発生し，多額の損害賠償を余儀なくされ，BCP が可能か，企業の存続が懸念される状況である．

昨年(2013 年)に数多く発生した通称「馬鹿アルバイト」による FaceBook への「悪ふざけ投稿」によって，多くの店が廃業に追い込まれたことは，リスク管理や BCP が機能しなかった証明でもある．

企業ではリスクを洗い出し，リスク・マップを作成し，優先順位を付けて，BCP の対象となるリスクを選定する．既に対策を講じている「頻度が多く，損害の大きい」リスクを除外して，「頻度」が少ない「非日常的なリスク」「多岐にわたる経営資源（Resource）に影響を与えるリスク」対象に BCP を策定すべきであろうと考える．企業のリスクは，以下の通りである．

（1）自然災害リスク
（2）その他の災害・事故リスク
（3）オペレーション・リスク
（4）情報セキュリティ・リスク
（5）法務リスク
（6）不正・内部統制リスク
（7）政治・経済リスク
（8）人事・労務リスク
（9）労働安全衛生リスク

一般に，「競合企業の台頭」「技術の陳腐化」「有能人材の流出」「人材の過不足」等は優先順位が高く，「知的財産権の被害」「インサイダー取引」「反社会的組織との関係」は優先順位が低いリスクとなっている．

4.2　大学における業務継続計画への提案

既に分析項目に上がっている，「危機管理マニュアル」にある大学におけるリスクを，リスク・マップに投影して（資料５０３試作を参照），対象となるリスクを選定して BCP を策定するのがベターである．

4.3　情報システムの業務継続計画の提案

資料番号３０２業務継続計画書（案）参照．

５．マニュアル作成と訓練実施の提案

5.1　マニュアル作成ガイドラインだけ？

本学の危機管理ガイドライン[4]には，第 7 章にマニュアルの作成方法が，実に細かく目次の構成例まで一覧表にして，詳細に記述されている．そして赤枠で注意があり，「緊急時には，マニュアルを参照して指示や進捗チェックを行うため，マニュアルは方針・組織・日常業務等の全てを理解でき，緊急時に実践的な活用ができるようにすべきである。」としているが，指示や進捗チェックのための「チェック・シート」の例もなければ，サンプルも記載がない．

本学で具体的に作成されているマニュアルには，「富山大学学生派遣留学・研修等の危機管理対応マニュアル」があり，内部は4つのマニュアルから構成され，マニュアル4が「派遣学生が行うべき危機管理対応」となっている．そして，留学先で実際に事件・事故が発生した場合は，「緊急連絡先へ連絡し，その指示に従って行動する．」となっていて，連絡体制図が記載されているが，当該学生の緊急対応行動指針（応急処置，連絡できない場合の対処方法，強盗に遭遇した場合の対処方法，・・・）や富山大学側の連絡先電話番号や電子メール・アドレスの記載がないのが，残念である．

いずれにしても，サンプル・マニュアルの記載が不可欠である．

5.2　先行事例に学ぶ

1）東京海上日動コンサルティング（株）開発グループ主任研究員の本田祐嗣氏の「大学の地震リスクマネジメント」[7]は，大地震発生時，その時に被害を最小限にとどめ事業を継続するための，事例として甲南大学と神戸大学の阪神淡路大震災の例を挙げて，予防と BCP の支店からリスク対策を提案している．

2)神戸大学情報基盤センターの尾川正美氏の「IT―BCP プロジェクトのご紹介」[8]では，地震などの自然災害と新型インフルエンザなどのパンデミックを招くものを対象に，情報インフラの緊急時対応計画と業務継続計画を策定するプロジェクトを記録している．最終報告書として，「リスクアセスメント実施報告書」，「事業継続計画書」，「インシデントマネジメント計画書」を出している．

3）その他政府からは，

・内閣府防災担当から「事業継続ガイドライン第一版」（2005.8.1）

・総務省自治行政局地域情報政策室から「地方公共団体における ICT 部門の BCP 策定に関するガイドライン（ICT-BCP ガイドライン）」の概要，（2012.1.31）

5.3　訓練実施の必要性

緊急時にマニュアルを読んでいる時間（暇）はない．従って，平常時には，想定危機に対応した訓練を実施しておく必要がある．**どんなに良い BCP でも実際の危機に遭遇した時に，日頃の訓練の成果が実証される．**

参考文献

[1] 日経コンピュータ連載記事「BCP/DR の現実解（第 1～4 回）」，森田太士，Nikkei Computer 2013.11.14-12.26,2013.

[2] セキュリティ・ポリシー（案）の策定について，高井正三，総合情報処理センター広報, Vol.6,No.1, 2002, 69-82, ISSN1342-9655, 2002.

[3] 新明解国語辞典，第 4 版，1993.9.30.

[4] 国立大学法人富山大学危機管理ガイドライン：学内のみ閲覧可能となっている site：http://int.u-toyama.ac.jp/for/pdf/risk_management.pdf

[5] 図解ひとめでわかるリスクマネジメント第 2 版，仁木一彦著，東洋経済新報社，2012.2.9，ISBN978-4-492-09300-9.

[6] BCP＜事業継続計画＞入門，緒方順一，石丸英治著，日経文庫, 2012.8.9, ¥830+TAX, ISBN978-4-532-11265-3.

[7]http://www.tokiorisk.co.jp/

[8]IT―BCP プロジェクトのご紹介，尾川正美，MAGE Vol.32, No.40, 6-15, 2012.3. http://www.istc.kobe-u.ac.jp/activity/mage/m40

資料４０１　緊急事態対応マニュアル（第 99 版）

２０〇〇年〇〇月〇〇日制定

国立大学法人富山大学
最高情報セキュリティ責任者（CISO）
常願寺　九郎

１．目標

本マニュアルの目標は，富山大学（以下「本学」という。）における情報活用システム，情報処理システムおよび情報通信システム（以下「情報システム」という。）の運用管理を担当している，総合情報基盤センターおよび各部局の運用管理担当者が，情報システムの運用に関しての緊急事態発生時における具体的な対応方法と手順を示すことである。

総合情報基盤センターおよび各部局の運用管理担当者の使命（Mission）は，情報システムを構成するコンピュータ・システムとネットワーク・システムを運用(Operation)し，情報システムを安定稼働し，システムの予防保守とシステム管理を実施して，研究開発，製造，営業，管理及び企画業務その他の諸活動における生産性向上に資することである。

この使命を遂行するために，情報システムが障害に耐えうるように予防保守をするとともに，万が一脅威となる攻撃や不測の災害や障害などにより緊急事態が発生した場合，可能な限り迅速に，正常状態に回復させるための方針，具体的な対応方法と手順を次章以降に示すので，日頃からこれらの緊急対応方法と手順を学習，訓練し，不測の事態に備えておくことが重要である。

２．緊急事態（不測事態）

情報システムを構成するコンピュータ・システムとネットワーク・システムを運用するに当たって，発生する緊急事態（不測事態：Contingency）とは，次の状態に遭遇することをいう。

（１）計算機室用空調機の異常停止，水漏れなどによる情報システム運転環境の異常事態
情報システム運転環境の異常により温湿度異常，電源の短絡、漏電等による停電等により，情報システムが故障し，運転が不能になる。

（２）ネットワーク・システムの異常停止
ハードウェア障害，ソフトウェア障害，過負荷による動作異常が発生する。

（３）情報システムの異常停止
ハードウェア障害，ソフトウェア障害，過負荷による動作異常が発生する。

（４）停電
落雷の発生などによる予期しない停電が発生する。

（５）盗難
コンピュータ・システム，ネットワーク・システムを構成する機器の盗難が発生する。

（６）不正アクセスによる情報の窃盗，漏洩，改ざん，破壊，消失等
情報システムへの不正侵入，不正アクセスによる情報の窃盗，漏洩，改ざん，破壊，消失，Web ページの書き換え，倫理観・道徳観の欠如による機密情報の漏洩等が発生する。

（７）不正攻撃によるネットワーク・システム，情報システムの運用妨害，異常停止等
ポート・スキャン，セキュリティ・ホール攻撃，バッファ・オーバーフロー攻撃等による不正侵入，不正攻撃が発生する。
コンピュータ・ウィルス／ワーム／ペストによる攻撃，混乱が発生する。
盗聴，なりすまし，サービス不能攻撃(Dos, DDos)，間接的攻撃（Web サイトにアクセス

するだけでウィルス／ワームに感染），P2P(Peer to Peer)による著作権違反のデータ転送によるネットワーク・トラフィックの異常過負荷等による運用妨害が発生する。

（８）自然災害による情報システムの異常停止

地震，洪水，津波，落雷，火山の噴火，台風，竜巻，地滑りなどによる建物の倒壊や一部破損が発生し、システム運用環境の異常事態が発生する。

（９）人災による情報システムの異常停止

近隣での火災発生や重度の振動によって，情報システムの異常停止が発生する。

オペレーターの健康障害やケアレス・ミス，訓練不足によってオペレーション・ミスが発生し，情報システムの異常停止が発生する。

凶悪犯による不法侵入，不法占拠，破壊行為，暴力行為，殺人行為，放火行為，異常者の破廉恥行為などのよる建物の破壊行為や直接的なシステム破壊行為などが発生する。

（10）その他の事故や緊急事態による情報システムの異常停止

飛行物体の墜落，隕石落下，戦争時のミサイルやテロリストによる爆弾などによる破壊行為が発生する。

３．緊急事態への対応方法と手順

情報システム運用管理部および各部局の運用管理担当者は，情報システムの運用に当たり，緊急事態が発生した場合，その正確な状況確認と具体的な対処方法と手順，事前に準備すべき内容を示す。

（１）計算機室用空調機の異常停止，水漏れなどによるシステム運転不能

情報システム部および各部の運用管理担当者の使命は，コンピュータとネットワーク・システムを常時運用することである。そのためにはコンピュータとネットワーク・システムの稼働環境である空調機を維持管理することが不可欠である。緊急事態の発生を予想して，以下の具体的な対応をとること。

１）水冷式・空冷式空調機

◇Ｖベルト切れ

・ベルト（通常２本）の交換，次回の予備Ｖベルトのストック

◇冷却水循環系のスケール（カリウム，カルシウム等）の凝固による水圧異常の発生

・定期循環系統洗浄（例年６月中１回）の実施

◇エアー・フィルターの目詰まり

・定期清掃，２回／年（６月，１２月）の実施

◇クーリング・タワーの汚染とフィルターの目詰まり

・定期清掃，２回／年（４月，１０月）の実施

◇フランジ，パッキンからの水漏れ

・定期目視点検（１回／月）の実施

◇排水管の目詰まりによる凝結水の溢れ

・溢れた排水の回収と排水管の清掃

・定期点検，排水管清掃２回／年（６月，１２月）の実施

◇運転異常

・運転インジケーター（メーター）の点検（起動時，停止時，随時）の実施

・異常時の施設課担当係に連絡して，点検，修理を実施

◇保守点検

・年間保守して，予防保守すること

◇第２空調機の設置と保守点検

・予備のため第２空調機を設置し，定期点検と予防保守することが不可決

２）ガス空調機

◇エアー・フィルターの目詰まり

・定期点検・清掃２回／年（６月，１２月）の実施

◇運転異常

・運転インジケーター（メーター）の点検（起動時，停止時，随時）の実施

・異常時の施設課担当係に連絡して，点検，修理を実施

◇保守点検

・ガス空調系は，エンジンを含めて年間保守契約して，予防保守の義務づけ

３）学部端末室の熱交換型空調機

◇エアー・フィルターの目詰まり

・定期点検・清掃２回／年（６月，１２月）の実施

◇運転異常

・運転インジケーター（メーター）の点検（起動時，停止時，随時）の実施

・異常時の施設課担当係に連絡して，点検，修理を実施

◇保守点検

・年間保守して，予防保守すること

（２）ネットワーク・システムの異常停止

ネットワーク・システムを常時運用するために，緊急事態の発生を予想して，以下の具体的な対応をとること。

◇停電（瞬断や予期しない停電）による停止

・瞬断に対しては無停電電源装置(UPS)の設置

・長時間停電にはネットワーク機器の電源スイッチの遮断と確認，監視サーバ類の自動シャットダウン手順の実行

・対策として大容量 UPS，CVCF，蓄電池，自家発電装置の設置，電源供給系統の２重化対策

◇機器の電源装置の故障

・電源モジュールの交換

・電源モジュールの二重化

・対策として，８時間以内に電源モジュール（部品）を調達して，復旧する契約締結

◇ネットワーク機器の障害

1)スーパーバイザー・モジュールの故障

2)ネットワーク・モジュールの故障

3)ファン（ブロア）モーターの故障

4)その他の部品の故障

・故障モジュールの同定と当該モジュールの交換，テスト，運用

・運用対策としてはモジュールの二重化による耐性を図る
・予備機器の準備
・交換予定モジュールの電源容量計算の実施

◇高熱による装置の動作不良
・設置環境悪化の原因除去と環境改善による適正温度・湿度の確保
・空調機やファンの設置，空調機の定期点検（最低２回／年の実施）

◇高負荷によるハング・アップ
・ハング・アップの原因除去，システムのリセット，正常動作の確認
・長期的対策としては，負荷原因を同定し，適正な負荷分散を図ること

◇ソフトウェアのバグによる停止
・原因の同定とバグの除去，パッチ(PTF)の適用
・ソフトウェアのバージョン・アップ，テスト，運用

◇物理的破壊による破損
・代替品の設置，テスト，運用
・設置場所の隔離，防壁の設置，設置部屋の施錠，ITV などによる監視と記録

◇装置の盗難によるネットワーク停止
・代替品の設置，テスト，運用
・設置場所の隔離，防壁の設置，設置部屋の施錠，ITV などによる監視と記録

（３）情報システムの異常停止

情報システムを常時運用するために，緊急事態の発生を予想して，以下の具体的な対応をとること。

◇停電（瞬断や予期しない停電）による停止
・瞬断に対しては無停電電源装置(UPS)の設置
・長時間停電には情報システム自動シャットダウン手順の実行
・対策として大容量 UPS，CVCF，蓄電池，自家発電装置の設置，電源供給系統の２重化

◇ハードウェア電源装置の故障
・電源モジュールの交換
・対策として，８時間以内に電源モジュール（部品）を調達して，復旧する契約締結

◇情報システムのハードウェア障害
・故障部品の同定，交換部品の調達，交換，テスト，運用
・対策として，８時間以内にモジュール（部品）を調達して，復旧する契約締結
・よく故障する部品については装置の抜本的な改善を要求する
・障害記録と保守，修理伝票の保存

◇高熱による装置の動作不良
・空調の調整，温湿度環境の適正化を図る
・通常は情報システムに設置の温度センサーが作動し，情報システムを強制停止する
・温度検出センサーが無いときは，環境センサーを設置するか，自動温湿度記録計を設置して，定期検査を行う
・大型 FAN を設置して，室内の空気の循環を良好にする

◇情報システムのソフトウェア障害

・障害ソフトウェアの現象確認，原因の同定，同一障害発生事例の調査，対処法の入手，パッチ・プログラム＝PTF(Program Temporary Fix)の入手，適用，テスト，運用
・対策として，ソフトウェア障害の随時連絡と PTF の随時供給，適用する保守契約締結
・よく発生するソフトウェア障害については抜本的な改善を要求する
・障害記録とパッチ適用，テストの実施伝票の保存

（4）停電

コンピュータとネットワーク･システムを常時運用するための電源の供給は不可欠であるが，作業停電や不測の瞬間停電など，緊急事態の発生を予想して，以下の具体的な対応をとること。

◇作業停電
・利用者への早めの通知（ニュース，速報，Web ページ，ML，Mail-Magazine 等）
・停電前の情報システム及びネットワーク・サーバの手動シャットダウン手順の実行
・ネットワーク機器，空調，照明の電源遮断
・作業後の速やかな情報システムのウォーム・スタート，ネットワーク・サーバの起動
・ネットワーク機器，空調，照明の電源投入
・情報システム，ネットワーク・サーバ，ネットワーク機器の動作確認
・サービス再開の通知（予め決められた連絡先）
・システム運用記録の記入

◇その他の停電（瞬断や予期しない停電）
・停電時刻の記録と停電原因の同定，今後の発生予想と復旧作業開始時刻の決定
・長時間（１分以上）停電には情報システムの自動シャットダウン手順の実行，ネットワーク・サーバの自動シャットダウン手順の実行
・停電による被害状況の把握（停止システムの調査，被害度の調査）
・復旧計画の立案と計画の実施，動作確認手順の確認
・復電後の情報システムのウォーム・スタート，ネットワーク・サーバの起動
・ネットワーク機器，空調，照明の電源投入
・情報システム，ネットワーク・サーバ，ネットワーク機器の動作確認
・サービス再開の通知（予め決められた連絡先）
・システム運用記録の記入

◇常時停電対策の実施
・瞬断に対しては無停電電源装置(UPS)の設置
・長時間停電には情報システム及びネットワーク・サーバの自動シャットダウン手順の設定，設定マニュアルの整備
・ネットワーク・サーバの起動手順，マニュアルの整備
・対策として大容量 UPS，CVCF，蓄電池，自家発電装置の設置，電源供給系統の２重化
・連絡先，連絡手順，連絡方法の取り決め
　運用管理者→施設課電気係
　緊急事態の連絡網に従って運用管理者に連絡し，対応措置を採る

（5）盗難

コンピュータとネットワーク・システムを構成する装置などが盗難などの被害あった場合を

予想して，以下の具体的な対応をとること。

◇盗難発生時の対応

・盗難機器・装置及びデータ，情報等の同定，盗難発生時刻の同定
・盗難被害調書の作成，警察への被害届，警察の現場検証立ち会い
・端末室入退出記録，防犯カメラ記録の分析による犯人の同定
・(警察外の場合）犯人への処分の基準の適用，処分の実施
・レンタル物品または購入物品の場合の事後手続き（弁償，購入）
・データや情報の復元処置，犯罪への対処方法
・今後の盗難への対策（２度と盗難に遭わないための対策)，装置の調達

◇盗難検知または防犯カメラ監視記録，入退出記録

・盗難検知センサーの設置と運用
・警報，連絡範囲の決定，警備会社の対応方法，窃盗犯の捕獲，捕獲後の処分
・端末室入退出管理システムの導入，運用と記録の採取
・端末室防犯カメラ(ITV 監視カメラ)の設置と記録の採取
・記録テープの交換方法と保存期間の決定
・ＬＡＮによる防犯カメラによる常時監視
・端末室入退出記録の採取と定期収集，解析

◇後処理

・予備装置の整備，交換，運用体制の確保

（６）不正アクセスによる情報の窃盗，漏洩，改ざん，破壊，消失等

コンピュータとネットワーク・システムに対して不正アクセスを受け，情報の窃盗，漏洩，改ざん，破壊，消失，Web ページの書き換え，倫理観・道徳観の欠如による機密情報の漏洩，その他の被害，損失のあった場合を予想して，以下の具体的な対応をとること。

◇不正アクセス発生時の対応

・不正アクセスの現象の同定，被害・原因の究明，原因の除去，回復措置，記録の保存
　・機密情報，重要情報の漏洩，閲覧，窃取・窃盗
　・情報システムおよび情報，データの破壊、消失
　・情報，データの改ざん

◇不正アクセス防衛対策

・リソース単位のアクセス制御の設定
・使用者権限の認証の実施
　・アクセス権の認証
　　・アクセス権の分類
　　・ディレクトリに対するアクセス権の設定
　　・データに対するアクセス権の設定
　　・ソフトウェアに対するアクセス権の設定
　　・アクセス権の管理権限の設定
　・アクセス・ログの保存と分析の定期的な実施，不審アクセスの対策措置
・利用者区分によるアクセス制御の設定
　・業務種別の利用区分とアクセス権の設定

・職務権限の利用区分とアクセス権の設定
・セキュリティ・ポリシーとアクセス権の設定
・OS のアクセス制御機能の適用
・DBMS のアクセス制御機能の適用
・ネットワークのアクセス制御機能
・ルーターの IP パケット・フィルタリング
・ダイナミック・パケット・フィルタリング
・ファイア・ウォール
・ファイア・ウォールによる内外からの不正アクセス制御
・ファイア・ウォール・ポリシーの設定
（インターネット・サービス利用基準，キャンパス情報ネットワーク・システム運用基準参照）
・プロトコル
・パケット・フィルタリング
・アプリケーション・ゲートウェイ
・ネットワークの閉域化
・暗号化と IP トンネル
・PVN の実現
◇不正アクセスの予防措置
・インターネット利用ガイドを配布して，不正アクセス検知時の対応手順を周知徹底
・新しい手口の情報収集と利用者への警告
・セキュリティ・ホールに対してパッチを当てる
・バージョン・アップする
・不正アクセスをしない，させない，受けないための最小限のルール，マナー，エチケット遵守の徹底と罰則の明記

（7）不正攻撃によるネットワーク・システム，情報システムの運用妨害，異常停止等

ポート・スキャン，セキュリティ・ホール攻撃，バッファ・オーバーフロー攻撃等による不正侵入，不正攻撃．コンピュータ・ウィルス／ワーム／ペストによる攻撃，混乱．盗聴，なりすまし，サービス不能攻撃(Dos，DDos)，間接的攻撃（Web サイトにアクセスするだけでウィルス感染），P2P(Peer to Peer)による著作権違反のデータ転送によるネットワーク・トラフィックの異常過負荷等による運用妨害，その他の被妨害，障害，異常停止などの被害，事故のあった場合を予想して，以下の具体的な対応をとること。

◇不正攻撃発生時の対応
・不正攻撃の同定，被害・原因の究明，原因の除去，回復措置，記録の保存
・ポート・スキャン攻撃
・セキュリティ・ホール攻撃
・バッファ・オーバーフロー攻撃
・なりすまし型（ID，パスワードの入手型，プロバイダ不正契約型）不正侵入
・Web ページの書き換え
・情報漏洩・改ざん・破壊

・サービス不能攻撃：DoS(Denial of Services)，DDoS
・コンピュータ・ウィルス型攻撃

◇不正攻撃防衛対策

・リソース単位のアクセス制御の設定
・使用者権限の認証の実施
・アクセス権の認証
・アクセス権の分類
・ディレクトリに対するアクセス権の設定
・データに対するアクセス権の設定
・ソフトウェアに対するアクセス権の設定
・アクセス権の管理権限の設定
・アクセス・ログの保存と分析の定期的な実施，不審アクセスの対策措置
・利用者区分によるアクセス制御の設定
・業務種別の利用区分とアクセス権の設定
・職務権限の利用区分とアクセス権の設定
・セキュリティ・ポリシーとアクセス権の設定
・OS のアクセス制御機能の適用
・DBMS のアクセス制御機能の適用
・ネットワークのアクセス制御機能
・ルーターの IP パケット・フィルタリング
・ダイナミック・パケット・フィルタリング
・ファイア・ウォール
・ファイア・ウォールによる内外からの不正アクセス制御
・ファイア・ウォール・ポリシーの設定（インターネット・サービス利用基準，キャンパス情報ネットワーク・システム運用基準があれば参照）
・プロトコル
・パケット・フィルタリング
・アプリケーション・ゲートウェイ
・ネットワークの閉域化
・暗号化と IP トンネル
・PVN の実現
・コンピュータ・ウィルス対策
・ウィルスの種類と発病の仕方，感染の方法を調査しておき，対策に備える
・自己伝染機能
・潜伏機能
・発病機能
・ウィルス侵入検知プログラム（ワクチン・ソフトウェア）の運用
・VirusWall
・Anti Virus
・パターン・ファイルの定期更新（１週間／管理者は毎日）
・感染範囲拡大防止策

・新種ウィルス情報の入手
・ウィルス発見報告ルートの確立と対応策の実施
・ネットワーク・システム感染時の感染範囲拡大防止策
・ネットワークの出入り口で検出
・VirusWall
・高度技術を駆使したウィルスへの対応策の策定
・ステルス・ウィルス
・突然変異型ウィルス
・ウィルス・リスク管理施策の必要性
・ウィルス感染防止施策の策定，実施
・ネットワークからのウィルス侵入防止施策の策定，実施
・システムの復旧と事後措置
・会社の総務部
・文部科学省
・IPA，JC/CERT などへの届出

◇不正アクセスの予防措置
・インターネット利用ガイドを配布して，不正アタック検知時の対応手順を周知徹底
・不正アタックからの防衛についての定期的な講習会の開催
・新しい手口の情報収集と利用者への警告
・セキュリティ・ホールに対してパッチを当てる
・バージョン・アップする
・不正アクセスをしない，させない，受けないための最小限のルール，マナー，エチケット遵守の徹底と罰則の明記

（8）自然災害による情報システムの異常停止

地震，洪水，津波，落雷，火山の噴火，台風などによる建物の倒壊によるシステムの停止を予想して，以下の具体的な対応をとること．

◇地震対策
・コンピュータ及びネットワーク機器収容ラックの転倒防止（免震対策ラック設置）
・コンピュータ及びネットワーク機器の移動防止，電源・信号ケーブル切断防止
・UPS の移動防止
・各種ケーブルの切断防止
・窓ガラスの破裂，飛散防止（無窓室），防雪防水確保

◇洪水・津波対策
・コンピュータ及びネットワーク機器収容ラックの水没防止
・配線，コネクタ類のショート防止
・建物への浸水防止

◇落雷対策
・避雷針の設置とアースの確認
・コンピュータ及びネットワーク機器への過電流防止
・停電防止

◇火山の噴火対策

・建物への火山弾，溶岩，粉塵等の侵入防止

・コンピュータ及びネットワーク機器への粉塵防止

・配線，コネクタ類の焼失，ショート防止

◇暴風雪対策

・台風など強風による屋外アンテナ，機器等の破壊防止

・配線，コネクタ類の切断，ショート防止

・建物への風雪の浸水防止，室外機周辺の除雪

（9）人災による情報システムの異常停止

凶悪犯による不法侵入，不法占拠，破壊行為，暴力行為，殺人行為，放火行為，異常者の破廉恥行為などのよる建物の破壊行為や直接的なシステム破壊行為などによるシステムの停止を予想して，以下の具体的な対応をとること．

◇建物への入退館対策

・不法侵入できないような入退館，入退室セキュリティ・システムの導入

・監視・防犯カメラの設置と記録の採取

◇暴力・殺人・放火・破壊行為など異常者対策

・防御方法の徹底と捕獲の対策の訓練

・迅速な通知・連絡対策の徹底と訓練

・最悪の場合は火災警報ボタンを押す訓練

・防犯カメラの設置と記録の採取，分析

（10）その他の事故や緊急事態による情報システムの異常停止

飛行物体の墜落，隕石落下，戦争時のミサイルやテロリストによる爆弾などによる破壊行為などによるシステムの停止を予想して，以下の具体的な対応をとること．

◇破壊行為などに対する対策

・可能な範囲で防御方法，防衛方法の研究と対策を練り上げておくこと．

・電話帳や用紙箱は防弾壁として使用可能などの知識を得ておくこと．

・バックアップ・システム／センターをバックアップ計画により確保しておくこと．

・利用者登録データのバックアップを用意しておくこと．

４．非常事態計画

非常事態（A state of emergency）とは，災害が発生している，正にその期間内の事態を指す．例えば，破壊活動の予告電話があり，実際に爆破が行われた場合や，大地震が発生してその揺れが収まり，二次災害に対する対策活動が必要な期間などを指す．

ここでは，危害にさらされている間の行動／対策及び判断の基準を示すので，非常事態に遭遇したときを予想して，以下の具体的な対応をとること．

（1）二次災害の防止を図る＝災害の拡大を防ぐこと

・コンピュータ・ワームによるネットワーク感染を防止する対策をとること

・ネットワーク（情報コンセント）からケーブルを外すこと

・同定したポートを中央のスイッチで停止すること

・予想される被害拡大のセグメントを同定し，ハブ機能を停止すること

・緊急通知の手段として，校内放送や宣伝カー，張り紙による警報を出すこと
・初期災害に続く二次災害の発生を抑圧すること
・このため，消火設備，防水設備，自家発電設備，無停電電源設備などを有効に作動させるようにしておくこと
・同時に要員が災害直後にすぐさま退避することなく，災害拡大防止措置を積極的におこなうこと
・水道やガス栓を閉めること
・電源をオフにすること
・防火シャッターの閉鎖と自動閉鎖の確認をすること

（2）社員の安全に主力を注ぐ＝要員の安全を図ること
・社員の保護を優先すること
・災害現場を退去するときの緊急対応＝災害拡大防止措置をとること

（3）非常事態の報告を適切に行わせること
・緊急時の連絡体制に従って，富山大学の上級管理者へ第一報すること
・警察署，消防署など，関連外部機関へ連絡すること
・非常事態の報告が適切であるかどうかで，その後のバックアップ及び復旧の速度その他事態の改善に非常に大きく影響する
・非常事態に備えて，報告が適時適切に行われるよう，緊急連絡手順，連絡体制を周知徹底しておくこと

（4）定期的なテストと訓練を行うこと
・頻繁なテストにより非常事態計画も事態に合わせて変更されていることを確認し，かつ訓練も兼ねるようにすること

5．バックアップ計画

バックアップ計画(Backup Planning)とは，非常事態発生により情報処理施設，ネットワーク施設が機能を果たさなくなった後，ある時間を経て元の状態に復旧するまでの間，富山大学が生き延びるのに必要な（最低限の）情報処理機能，ネットワーク機能を手当しておくことという．

（1）バックアップ施設の選定と確保

元の状態に復旧するのに要する期間は，想定する災害の規模によって，1か月から半年以上かかることがありうる．従って，バックアップ施設は現在の情報処理施設，ネットワーク施設の設置場所以外に立地を選定しておかなければならない．富山大学の場合は提携会社を決めて予めバックアップ施設を決めておく必要がある。

◇立地条件
・土地
　・地盤が強固，地震災害が歴史的にすくないこと
　・水害，雷害その他の自然災害に強いこと
　・交通の便がよいこと
・気候
　・温暖であること
・電力事情
　・良好であること

・空港／高速道路
・データ／処理結果の搬出入のために近いことが望ましい
・通信ネットワーク
・回線追加が容易に素早く行えること
・通信衛星利用のために電波障害が少ないこと
・住居環境
・要員の住居を手当てできること
・大規模施設では数十人体制で，数か月間移り住むことができること
・人
・安定した供給が得られること

（2）必要な設備
・バックアップ用コンピュータ，サーバ
・バックアップ用ネットワーク・サーバー，ネットワーク機器
・バックアップ用データ記憶装置
・自家発電装置

（3）バックアップ・センター／システムの確保
・民間の共同バックアップ・センターを確保しておく
・バックアップ・システムへの移行ができるようサーバを確保しておく

（4）バックアップ用データの採取
a．手作業バックアップ
・システムの初期設定，変更毎にシステムのフル・バックアップを採取すること
・データ記憶テープ類は一定の数を確保して，サイクリックに使用するようにすること
b．自動バックアップ
・ユーザ・ファイルなどは定期的に自動バックアップを採取すること

（5）自営バックアップ－コールド・サイト
・別のキャンパスに第１の自営バックアップ－コールド・サイトを確保すること
・提携会社関連施設の一部を借用し，自営バックアップ－コールド・サイトを確保すること

（6）バックアップすべき適用業務の選定
・各種事務管理情報システム
・学務情報システム
・入試情報システム
・ネットワーク・サーバ
・電子メール・サーバ
・ホームページ運用サーバ
・計算サーバ
・ファイル・サーバ
・薬品管理サーバ
・図書館情報システム
・総合情報基盤センター統合利用者管理システム

（7）監査の視点
(1) バックアップの方針／手順を明示した文書があるか

(2) バックアップ担当者，媒体の保存復旧チームの編成，リーダーの任命，要員の手配について示した文書があるか

(3) 諸施設，設備，機器の調達についての枠組みが示されているか

（8）バイタル情報（Vital Information：生命の維持に必要な情報＝組織運営に重要な情報）

以下の情報は組織運営に重要なので，バックアップ及び復元の手順を確認しておくこと

・各種事務管理情報
・施設管理情報，各種図面
・学務情報
・入試情報
・ネットワーク管理情報
・電子メール管理情報
・ホームページ管理情報
・利用者プログラム／データ
・危険物関係管理情報
・図書館管理情報，書誌情報 DB
・総合情報基盤センター登録利用者情報

6．復旧計画

復旧計画には単に球場に復旧する場合と，発展的に復旧する場合とを見極める必要がある。建物等の被害が甚大で，新規にサービス・センターを設置した方が経費的にも安価であると判断された場合は，次に挙げるように，発展的復旧を選択することも考える必要がある。

（1）復旧計画の方針

◇発展的復旧

1）この機会に新たなセンターを手配して移転する
2）１つの大型システムを複数のより小型のシステムに置き換える
　クライアント・サーバー型システムに置き換える
　より上位の大型機種への更新時期を早める
3）適用業務の再構築を行って，業務を効率化する
4）しかしながら，リスクが大きく，コストが高くなる
5）旧方式になっていたシステムの刷新を行う機会として活用の価値がある

◇旧状に復旧

1）ソフトウェアや情報システムの単純な復旧は比較的早くできる
2）ただし，機器の再調達には１ヶ月から半年，建物の再建には１年以上の時間を要する
3）業務再開が早いので，損失は小さくなる

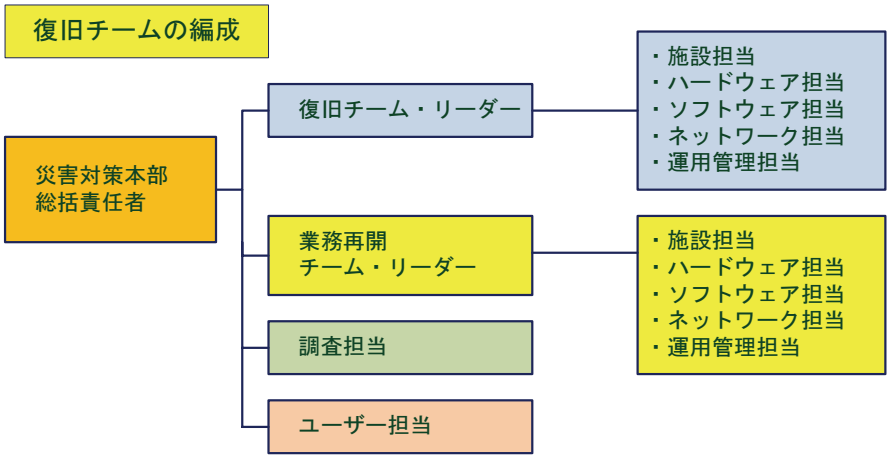
（2）監査の視点

1）復旧の方針／対策を明示したガイドがあるか
2）復旧チームの編成，リーダーの任命，要員の手配について示した文書があるか
3）諸施設，設備，機器の調達についての枠組みが示されているか

（3）業務復旧の基本方針

適用業務の構成要素毎に優先順位を設定し，優先順位の高いものから復旧計画を策定し，必要な設備，体制を整え，復旧計画を遂行していく。

（4）復旧チームの編成



７．業務継続計画（不測事態計画）の文書化

本業務継続計画の文書化の目標は，富山大学における情報システムが，自然災害，不慮の災害，サイバー・テロリズムなど不測の事態や脅威に遭遇し，システムが停止し，富山大学の情報基盤が使用不能となった場合，どのようにして情報基盤の正常化を復旧させ，会社としての業務を継続させていくかを示すことである。

即ち，遭遇している緊急時に，総合情報基盤センター，情報政策室および各部局のシステム運用管理担当者が，業務を継続させるための具体的な計画を示すことである。

（３０２　情報システム運用管理業務継続計画書　を参照）

なお，一般業務継続計画文書の満たすべき項目とその例は以下のとおりである。

１）満たすべき項目

非常事態計画，バックアップ計画，復旧計画には次の項目を網羅する

・目的及び要約
・目標
・想定事項
・対策
・付録

２）文書化の例

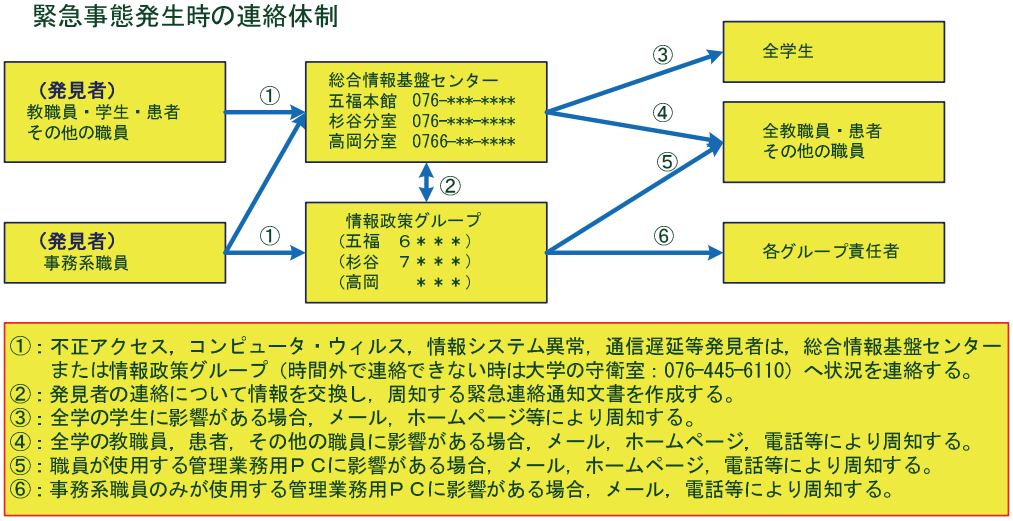
・災害復旧計画書目次例

１．業務復旧計画基本事項
１．１　役割と責任
１．２　適用範囲
１．３　災害想定
１．４　業務復旧の基本方針
１．５　災害状況調査
１．６　重要機器／資産リスト

２．業務復旧要員リスト
２．１　業務復旧要員
２．２　緊急連絡ネットワーク

８．不正アクセス，コンピュータ・ウィルス等による被害発生など緊急時の連絡体制

（１）緊急時の連絡体制



緊急時連絡体制　総合情報基盤センターと情報政策グループで作成

（２）緊急停止連絡通知文（「決済」済みで，事象発生時に直ちに通知できるものとする）

２０〇〇年〇〇月〇〇日

教職員・学生　各位

国立大学法人富山大学
最高情報セキュリティ責任者（CISO）
常願寺　九郎

コンピュータ不正アクセスに伴う業務サーバーの停止
及び不正アクセスの痕跡の確認について

現在，○○製薬株式会社の○○○○用ソフトウェア○○○（○○○○○○Server）及び○○○○（○○○○○○Server）がインストールされている学内のサーバー（パソコンを含む）に対し不正アクセスが行われています。

このため，○○○により運用している情報システム部の業務用サーバー（○○○○システム，○○○○向けホームページ・・・・・等）が被害を受ける可能性があるため，セキュリティの確認のため当該業務用サーバーを緊急停止させています。

この不正アクセスは，不正アクセスに成功したサーバーを踏み台にして他のサーバーに対しても不正アクセスを行うもので,不正アクセスに成功した場合,下記の痕跡を残す場合があります。

つきましては，○○○及び○○○が導入されているサーバーを運用している部局等は，不正アクセスの痕跡が無いか至急確認していただき，もし痕跡が確認されましたら，ネットワークケーブルを抜く等の方法でサーバーを切り離す等，他のサーバーへの加害者にならないよう至急対処していただきますようお願いします。

なお，詳細については，富山大学のホームページ「在学生・教職員」の「お知らせ」
【　URL=http://www.u-toyama.ac.jp/student-staff/index.html】をご覧下さい。

記

１．不正アクセスの痕跡ファイル

次の○○○○ファイルが有り，ファイル更新日時が２０○○年○○月○○日以降の場合，不正アクセスされた可能性がありますので，特に当該ファイルが有った場合は，ファイル内容を確認願います。

○○○○フォルダの中の,
○○○○フォルダの中に,
・ファイル名１
・ファイル名２　　（必ず，ファイル更新日時を確認して下さい）
・ファイル名３
・・・

２．その他

(1)○○○がインストールされているパソコンについても確認願います。
(2)業務用サーバの運用を再開した時は，事務局からメールにより通知をします。

連絡・照会先：○○○○（内線番号）

（３）運用再会通知文（決済済で，再開後直ちに通知できる）

２０○○年○○月○○日

教職員・学生　各位

国立大学法人富山大学
最高情報セキュリティ責任者（CISO）
常願寺　九郎

○○○○用サーバーの運用再開について（お知らせ）

セキュリティの確認のため２０〇〇年〇〇月〇〇日から停止していました情報システム部の〇〇〇〇用サーバー（〇〇〇〇システム，〇〇〇〇向けホームページ・・・・・・等）の運用を再開しましたのでお知らせします。

なお，詳細については，富山大学のホームページ「在学生・教職員」の「お知らせ」**【　URL=http://www.u-toyama.ac.jp/student-staff/index.html】**をご覧下さい。

連絡・照会先：〇〇〇〇（内線番号）

（４）管理業務一覧

（一覧表にして知らせる。省略）

９．事故報告書

コンピュータ・システムとネットワーク・システムを運用時に発生した事故報告について，次の項目について様式に従って記入し，提出すること．

（１）ネットワーク・システム事故経過記録報告書

作成日：平成〇〇（２０〇〇）年〇〇月〇〇日
記入者氏名：
１．事故の内容：
２．経過記録：
（１）内容：時系列記録
１）攻撃者の活動
２）発見経過・・・事故が発見された方法
３）決定経過・・・事故が存在することを判別するためにとられたアクション
４）調査経過・・・調査の段階毎の記述
５）復旧経過・・・事故から復旧するために使われた対策，手順，行動

（２）記録方法
１）記述的な経過記録
事故の起こった自称を時刻順に記述
（例）1999年12月31日23:59　ネットワーク・ログ管理サーバは，メール・サーバ，バイラス・ウォール，ファイア・ウォールが「ディスク・フル」状態で動作停止と報告してきた．
２）図式的な経過記録
事故説明に便利なように図式を用いた記述．発生場所など．
３）注釈
情報の発生源などの注釈，どのサーバのエラー・ログか等の注釈．
３．不正侵入情報
１）影響を受けたシステム／コンピュータのIPアドレス：

２）最初の探知の日時：
３）影響をうけたユーザ数：
４）損失の見積もり額：
５）休止期間：
６）進行状況：　進行中，　停止，
７）攻撃についての記述：
４．攻撃者情報
１）疑わしい攻撃元（ＩＰアドレス）：
２）内部の者／外部の者：
３）国内／国外
５．証拠の有用性
１）ログ情報の有用性
２）攻撃されたシステム／コンピュータの保護：された　　されていない
６．事故対策に使用したもの
１）印刷物：
２）電子メール：
３）ホームページ：
４）放送内容：
５）感染者リスト：
６）電話連絡先
７．事故後の状況説明会記録

（２）情報セキュリティ事故テクニカル報告書の記載事項
１）事故原因
どのセキュリティ・ホールは，何時，どこで，どのように使用されたか，攻撃者の技術的能力についての記述，使われたツールの記述を含むこと．

・誰が・・・攻撃パターンを記述，攻撃に使われたツールの数，形式，年代，
攻撃者のシステム攻略成功率
・何を・・・成功したもの，失敗したものの両方について，どのようなタイプのシステムが攻撃されたか，どのようなセキュリティ・ホールが使用されたか，あるいは狙われたか
攻撃されたシステムのハードウェア，ＯＳ，アプリケーション，格納されるデータのタイプで分類する
・どのように・・・どのように事故が起きたのかについての技術的な詳細説明
使用されたセキュリティ・ホールの記述，それがどのように使用されたか，この形態の使用を防ぐために設置された防衛策がどのように迂回されたか，アクセスと認可の取得過程，攻撃の記述
・何時・・・攻撃が起きた時刻，核攻撃の長さ（時間），攻撃の自動／手動の区別
・どこ・・・どこから攻撃が来たか，攻撃者がシステムにアクセスした経路

２）事故の影響
事故を抑制するために必要な人員，機材，ハードウェア，ソフトウェア，攻略された情報を含

むこと.

・システム・・・攻撃されたシステムの具体的記述＝ハードウェア・ベンダー，ＯＳのリビジョン，ソフトウェア・サービス，それぞれのパッチ・レベル，各タイプのシステム数，ネットワーク・トポロジーと情報，処理の形態など

・データ・・・どのようなタイプのデータが，どのように，どれだけの量悪影響を受けたか，悪影響を受けたデータのフォーマット，ファイル・システム，データベースなどの記憶装置環境，バックアップ・メディアの攻略状況

・停止時間・・・コンピュータ・システム，データ，ネットワーク，プロセス及び情報システム資源が被った停止時間，攻撃者が消費した資源，使用不可能になった資源，不安定だった資源の記述

・復旧・・・事故から復旧に関わる労力の要約（時間と人数），システムとデータを復元するために使われた時間,情報システム／ネットワーク･システムを使用できなかった時間，生産活動を処理するために必要とした時間，特定の技能を有する人材の人数と時間，資源不足と矛盾など

・人々・・・何人が事故の影響を受けたか，職種と人数，事故に費やされた労働力，失われた生産性とシステムの復旧に関わる人々の区別（エンド・ユーザ，運用管理者，オペレータ，コンサルタント），どの部分が攻撃者の発見と問題の解決になったか

３）解決

事故の診断と抑制，事故による損害の修理，再発防止策を含むこと.

・診断・・・攻撃を発見した個人の情報と，それが実際に攻撃であると判別した過程についての情報を含め，事故の特性を識別し，適切な対応を決定するために取られた過程を記述

・抑制・・・事故の間に使用されたセキュリティ・ホールを記述し，それを勧告または詳細情報の供給元への参照の記述，攻撃を停止するためにシステムに施された修正，成功に有無，有効性の記述，影響されたシステムを堅牢にするために取られた処置の詳細記述

・復元・・・システムとデータ利用を可能にすること，情報の正確さ，プライバシーの確保を含み，どのようにシステムと情報が修理されたか，情報復元のために何故それぞれの異なる過程が選択されたか，影響されたシステムと情報の識別，復元のために用いられた過程の説明

４）改良

セキュリティ・システムを改善するために，どんなことをすべきかを列挙し，方針，手続き及びプロセスにどのような部分修正が可能か，この事故の再発を防止するための技術的になにが必要かを含めること.

・セキュリティ・ホールの削除・・・セキュリティ・ホールの削除と新しいセキュリティ・ホールを監視し，その修理を促すためのに実施されるべきプロセスの記述

・防御策の追加・・・セキュリティ事故の可能性の減少させるための追加防御改善策

・探知の改善・・・セキュリティ事故への応答時間と影響の削減するための改善策

・自動化対応・・・セキュリティ事故への対応のスピード化，一貫性向上のための対応改善策

（３）情報セキュリティ事故エクゼクティブ報告書の記載事項

経営上の懸念に着目して，ビジネス用語で記述し，事故の責任と直接的，間接的コストなど，財務への影響を中心に記述する．２０分程度で説明できる内容の報告書とする.

１）事故原因

何が事故を起こしたのか，事故がどのようにして起きたか，誰に責任があったか，彼らの動機はなにか等，広報，訴訟に言及する際に必要な情報を含むこと．

・理由・・・何故事故が起きたか，攻撃の動機，攻撃者の識別，攻略された情報の重要性，攻撃者と組織の関係，攻撃の標的，攻撃のタイプ，攻撃の目的など
・誰が・・・攻撃者，組織との関係，年齢，非行歴，個人またはグループの判別，攻撃が手動か自動，攻撃の発生源など
・何時・・・セキュリティ事故の主要な時刻の列挙
・何処から・・・ネットワーク上の攻撃の発生源．内部からの攻撃では，開始した部門やシステム
・どのように・・・どのように犯人が問題を起こしたか．セキュリティ・ホールの欠陥，新たに見つかったミス，不正確な実装，実行の技術知識のレベル
・何を・・・組織への影響

２）事故の影響

事故の組織に対する金銭的な影響の最終結果，有形，無形のコスト，売上げ及び生産性の損失，当面の影響と長期的影響を含むこと．

・実際の損害・・・実際に攻撃者により盗まれた現実の資産，即ち，盗まれたコンピュータ機器，資金の振り込み，変換可能な資産
・直接的損害・・・直接的な損失で，システムの不正使用からの損失，知的所有権，停止時間やサービス不能からの損失も含む
・失われた売上げ・・・トランザクション処理に情報システムが使用できなかったことによる販売または注文の損失，延期された販売のコスト，許可されていない変更結果として後日判明する損失m，顧客信用の損失（失注）
・失われた生産性・・・情報が使用できないために浪費される時間のコスト，システムが攻撃されていなければそれを使用している人々と，他の実行すべき義務を持ちながら復元に関わっている人々の両方の生産性コスト，復元や調査に関わる停止時間と人員コスト
・復旧コスト・・・削除された情報を復元し，情報の正確さを確認するコスト，情報システムとデータの復旧に係る時間の労働力，時間外手当，復旧過程で消費された物資のコスト，復旧チームが長時間サポートするための経費を含む
・無形のコスト・・・セキュリティ事故による組織の信用損失，情報の暴露による組織への影響，及び他の形態の失われた将来の売上げを含む

３）解決

事故がどのように解決されたか，攻撃を判別し，評価するために必要な時間の量，攻撃を止めるために成功した戦略，その戦略がどのように再発を防止できるか，この事故の解決のために，要求された以上の行動を行った個人やグループを表彰し，事故の補助を頼まれた組織についての問題，犯人についての十分な情報，攻撃者が内部からなら，経営陣は起訴するか，降格や解雇などの処罰も決めて記述

４）改良

再発を防止するために何をなすべきかを経営陣に紹介する．改良は，方針，手続き，企業をより安全にできるシステムに関連する問題に集中し，将来のセキュリティ事故の影響をなくせるか，最小化できるような，システムや手続きへの改良コストを記述．事故が発見できるのを妨害したシステムや手続きの変更，これらの変更が減少させたであろう損失，変更の期待されるコストの

金銭的情報を詳述

（4）業務記録

事故の有無にかかわらす，業務記録日誌を付けることは不可欠である．

（5）チェック・リスト

1）事故の日誌を含み，すべての関係するもの（material）からの情報をまとめたか
また，ヘルプデスク，ネットワーク，システム，運用管理，アクセス，アカウンティング，監査及びセキュリティ・ログを集めたか

2）記録されなかった情報を集めるために，事故後の状況説明会を実施したか

3）他の報告書が基にすることができる事故の経過記録報告書を作成したか

4）他のシステムへの適用性を評価できるテクニカル報告書を作成したか

5）経営陣に事故の問題と影響を理解させるためのセクゼクティブ報告書を作成したか

6）特定の聴衆のために，事故報告書を作成してみたか
報道陣，利用者，システム運用管理者など

１０．更新履歴

第99版は２０〇〇年〇〇月〇〇日から実施する。

資料３０２　業務継続計画書（案）

２０〇〇年〇〇月〇〇日制定

国立大学法人富山大学
最高情報セキュリティ責任者（CISO）
常願寺　九郎

１．序文

１．１　適用範囲

本業務継続計画は，国立大学法人富山大学（以下「本学」という。）における情報活用システム，情報処理システム及び情報通信システム（以下「情報システム」という。）の運用管理業務を対象とする。

１．２　目的

本業務継続計画書の目的は，自然災害，不慮の災害，サイバー・テロリズムなどの不測の事態や脅威に遭遇することにより情報システムが停止し，富山大学の情報システムが使用不能となった場合，情報センター各部門の情報システム運用管理担当者等が，どのようにして情報システムを正常に復旧させ，情報システムサービスを継続させていくかを示すことである。

（1）業務内容と優先順位

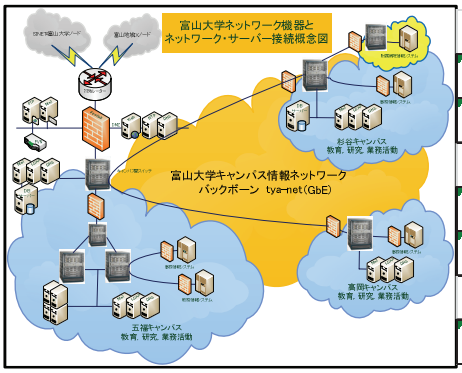
次に，業務継続計画の対象とする業務内容を，優先順位順に記述する。

1）通信ネットワーク経路の確保（ネットワーク概念図）

2）ネットワーク機器とネットワーク・サーバによる情報通信サービス業務（サンプル表例）

3）業務システム

(1)	附属病院情報システム	(2)	教務情報システム
(3)	入試情報システム	(4)	附属図書館情報システム
(5)	事務情報システム	(6)	その他の業務情報システム



2）ネットワーク機器とネットワーク・サーバによる情報通信サービス業務			
(1)	ルーター	(2)	DNSサーバー
(3)	Syslog収集解析サーバー	(4)	ファイア・ウォール
・・・			
(7)	認証サーバー	(8)	NTPサーバー
(9)	メール・サーバー	(10)	Webサーバー
・・・			
(21)	その他の適用業務サーバー	(22)	ユーザー運用サーバー

（２）業務停止許容時間

１）ネットワーク機器とネットワーク・サーバによる情報通信サービス業務

No.	情報システム名称	業務停止許容時間
(1)	ルーター	1時間
(2)	DNSサーバー	1時間
(3)	Syslog収集解析サーバー	1時間
(4)	ファイア・ウォール	1時間
・・・		
(7)	認証サーバー	1 時間
(8)	NTPサーバー	1 時間
(9)	メール・サーバー	3 時間
(10)	Webサーバー	1 日
・・・		
(21)	その他の適用業務サーバー	3時間～1日
(22)	ユーザー運用サーバー	3時間～1日

２）業務システム

No.	情報システム名称	最小業務停止許容時間	最大業務停止許容時間
(1)	附属病院情報システム	30分（原則無停止）	1日
(2)	教務情報システム	1時間	1日
(3)	入試情報システム	30分	1日
(4)	附属図書館情報システム	2時間	1日
(5)	事務情報システム	2時間	1日
(6)	その他の業務情報システム	1日	1週間

[注1]　ネットワーク機器およびサーバーの電源モジュールが故障した場合は，東京や大阪からモジュールを手配し，交換するまでの時間は１日程度を見積もるのが一般的で，無停止サービスを必要とする附属病院情報システム等はシステムの2重化をして，絶対停止しないようにする．

１．３　想定される災害と脅威

不測事態として想定される災害や脅威は，以下の通りである。

（１）自然災害による情報システムの異常停止

地震，洪水，津波，高波（寄り回り波），落雷，火山の噴火，台風，竜巻，地滑りなどによる

建物倒壊等によるシステムの停止

（2）サイバー・テロ，不正アクセスによる情報の漏洩，改ざん，破壊，情報システム異常停止

システムへの不正侵入（ポート・スキャン，セキュリティ・ホール攻撃，Webページの書き換え，情報の漏洩・改ざん・破壊，盗聴，なりすまし，サービス不能攻撃(Dos，DDos)，コンピュータ・ウィルス／ワーム感染，間接的攻撃（Webサイトにアクセスするだけで情報漏洩やシステム破壊），倫理観の欠如による不正行為（責任感や倫理観の欠如）によるシステムの停止

（3）人災による情報システムの異常停止

凶悪犯による不法侵入，不法占拠，破壊行為，暴力行為，殺人行為，放火行為，異常者の破廉恥行為などによる建物の破壊行為や直接的なシステム破壊行為などによるシステムの停止

（4）過失による情報システムの異常停止

火災の他，停電，断水，機器の操作ミス，設定誤り，ソフトウェア・バグ，既知の欠陥など，過失によるシステムの停止

（5）機器類の劣化，摩耗，過負荷による情報システムの異常停止

ハードウェア障害や過負荷による誤動作などによるシステムの停止

（6）その他の事故や緊急事態による情報システムの異常停止

飛行物体の墜落，隕石落下，戦争時のミサイルやテロリストによる爆弾などによる故意の破壊行為によるシステムの停止

1．4　復旧方法

不測事態により停止した情報システムの復旧計画は，以下のとおりである。

（1）情報システム停止の直接原因究明

1）不測事態発生の中から情報システム停止の直接原因を究明する。
2）直接原因を取り除くための計画を立案する。
3）計画は，システムが正常に動作するまでの詳細なプログラムを書く。
4）計画は，予め災害を想定し，各単体ごとの障害を前提で用意する。
5）直接の停止原因が究明できない場合は，（2）以降で原因を究明する計画を盛り込む。

（2）被害状況の調査と復旧計画の立案

1）被害状況を調査する。
2）情報システム停止の原因を調査または推定する。
3）被害を復旧するための計画を立案する。
　装置，モジュール，電源等の交換費用とそのスケジュールを立てる。
4）復旧のための要員手配と作業の分担を立案する。
5）復旧計画の概要を利用者に通知し，復旧期間を確認してもらう。
6）復旧に必要な予算と人員を手配する。
7）被害状況の大きさと復旧期間の長期化により，発展的復旧計画もあり得る。

（3）停止原因の除去対策の実施

1）停止原因となった装置，モジュール，電源等の交換を行う。
2）同装置，モジュール，電源等の動作を確認する。

（4）動作環境の復旧整備と確認検査

1）被害環境を復旧計画に基づいて復旧，整備する。

2）復旧計画によっては発展的復旧をするために，環境全体を変更する。

3）すべての動作環境の復旧を行った後，確認検査を実施する。

（5）情報システム復旧手順の確認

1）単体の再起動と動作テストを行う。

2）単体の正常動作確認を行う。

3）結合テストと正常稼働の確認を行う。

4）統合テストと正常稼働の確認を行う。

5）部局（部署）での接続テストを行う。

6）情報センターからの接続テストを行う。

（6）情報システム復旧手順の実施

確認された復旧手順を実施する。

1）単体の再起動と動作テスト

・コンピュータ及びネットワーク機器の単体での起動を実施する。

・単体での動作テストをマニュアルに従って実施する。

2）単体の正常動作確認

・動作不良の場合は，原因を究明し，修理する。

・正常動作を２人以上で確認する。

3）結合テストと正常稼働の確認

・システムの復旧手順に従い結合テストを実施する。

・結合テストで不具合が発見されたときは，原因を究明し除去する。

・再度結合テストを行い，正常動作を２人以上で確認する。

4）統合テストと正常稼働の確認

・統合テストを実施し，正常稼働を確認する。動作異常が発生した場合は修理する。

5）担当部局（部署）の職員で内部及び外部からの接続テストの実施

・担当部局（部署）の職員で内部からの接続テストを実施する。

・担当部局（部署）の職員で外部からの接続テストを実施する。

6）情報センターからの接続テストの実施

・情報センターからの接続テストを実施し，正常動作を確認する。

・動作テストが正常でないときは，原因を調査し，修理する。

（7）情報システム回復のユーザへの通知

1）情報システムの回復をユーザへ通知する。

2）通知は紙面，放送，Web等，様々な媒体による緊急連絡とする。

3）ユーザの接続開始に当たっては，注意事項を明確に通知する。

4）詳細な問い合わせの窓口を設置し，対応する。

5）ヘルプ・デスクを設置し，問題解決ケース・スタディを掲載する。

（8）未解決事項の確認と公表

1）災害復旧計画の実施にもかかわらず，期日までの未解決事項を確認する。

2）上層部への報告とユーザへの通知を徹底する。

3）最終的な未解決事項とその解決の見通しを公表する。

1．5　被害額の試算と報告書の作成

1）装置，モジュール，電源等の被害額を算出する。

2）環境被害の復旧経費を算出する。

3）情報資産リストを再構築する。

4）未解決事項の解決計画を作成する。

5）災害報告書を作成する。

6）新たな不測事態計画書を作成し直す。

7）バイタル・インフォメーションを再構築する。

1．6　重要適用業務

1）重要適用業務とその優先度を確認しておくこと。

2）重要適用業務が停止した場合の損害額を試算しておく。

3）重要適用業務に使用する情報システムのバックアップ計画と復旧計画を立案し，適時実施するものとする。

4）災害を予想し，予算と復旧要員，その他の物品調達に必要な外注先，保守契約先との間で不測事態計画を確認しておく。

1．7　重要適用業務以外の業務

1）一般サービス業務停止時の損害額を試算しておく。

2）リスク管理手順を確認しておく。

・バックアップ，リカバリー計画を立案し，実施する。

・業務担当者を確認しておく。

3）災害を予想し，予算と復旧要員，その他の物品調達に必要な外注先，保守契約先との間で不測事態計画を確認しておく。

2．緊急時対応計画

2．1　避難方法

（1）学生・患者，教職員，その他の職員の避難

・学生・患者，教職員及びその他の職員を安全に避難させる。

・学生・患者，教職員及びその他の職員の保護を優先する。

（2）サービス担当職員の避難

・サービス担当職員を安全に避難させる。

・サービス担当職員は災害現場を退去するとき，緊急対応措置として災害拡大防止措置をとる。

2．2　災害の拡大防止

（1）二次災害の防止（災害の拡大を防ぐ）

・初期災害に続く二次災害の発生を抑圧すること。
・このため，消火設備，防水設備，自家発電設備，無停電電源設備などを有効に作動させるようにしておくこと。
・同時に要員が災害直後にすぐさま退避することなく，災害拡大防止措置を積極的におこなうこと。
・水道やガス栓を閉めること。
・電源をオフにすること。
・防火シャッターの閉鎖と自動閉鎖の確認をすること。

２．３　連絡方法

（１）非常事態の報告

・非常事態の報告を適切に行わせること。
・緊急時の連絡体制に従って，富山大学の上級管理者へ第一報すること。

（２）外部への連絡

・警察署，消防署などの関係外部機関へ連絡すること。
（非常事態の報告が適切であるかどうかで，その後のバックアップ及び復旧の速度その他事態の改善に非常に大きく影響する。）

（３）手順と体制

・非常事態に備えて，報告が適時適切に行われるよう，緊急連絡手順，連絡体制を周知徹底しておくこと。
（緊急連絡網の図面：緊急連絡手順，緊急連絡体制）

２．４　訓練

（１）定期的なテストと訓練

・頻繁なテストにより非常事態計画も事態に合わせて変更されていることを確認し，かつ訓練も兼ねるようにすること。

（２）非常事態計画の周知

・テストと訓練を効果的に行うため，非常事態計画は常に最新のものを用意し，学生・患者，教職員及びその他の職員に周知徹底しておくこと。

３．業務継続計画

３．１　役割と職務

復旧過程での情報センター及び各部門（部署）での職員の役割と職務，職務ごとの責任者と代行者を，以下の通り指定するので，迅速に責務を果たすよう心がけること。

（１）情報センター

・情報センター災害対策本部
　・総括責任者（代行者）：
　・調査担当責任者（代行者）：
　・ユーザ担当責任者（代行者）：
　・復旧チーム責任者（代行者）：
　　・施設，設備，環境担当：
　　・ハードウェア担当：
　　・ソフトウェア担当：

・ネットワーク担当：
・運用管理担当：
・業務再開チーム責任者（代行者）：
・施設，設備，環境担当：
・情報システム担当：
・ネットワーク担当：
・運用管理担当：

（2）各部門（部署）

・各部門（部署）災害対策本部
・総括責任者（代行者）：
・調査兼ユーザ担当責任者（代行者）：
・システム復旧兼業務再開チーム責任者（代行者）：
・施設，設備，環境，端末PC，ネットワーク，運用管理担当者：

３．２　計画の実施

計画の実施に当たっては，１．４の復旧方法に従って計画を立案し，実施する。ただし，次の事項については総括責任者のもとに計画に組み入れるなど，状況を判断しながら担当者と検討して，計画を遂行する。

１）代替施設の活用
・現行施設での復旧が困難な場合
・発展的復旧を決断した場合

２）援助要員による業務支援
・援助要員の投入はコミュニケーションを増大させるので，予め援助要員の派遣元と業務支援内容を決めておくこと。
・物理的な環境整備に伴う労働力の増強などは受け入れることが望ましい。
ただし，業務支援執行責任者の指示に従うことを周知徹底する。

３）当該施設以外からの重要情報の収集
・重要な情報は，正確さを確認の上，復旧チームの全員へ正確に伝えること。
・時事刻々と入ってくる情報は整理して，優先度をつけて復旧チームへ連絡すること。

４）組織上層部からの催促と圧力への対応
・復旧の遅延などに対する上層部の催促と圧力には総括責任者が対応する。
・現場の担当者は直接上層部へ報告しないこと。

５）連絡
・発生した問題点と復旧の進捗状況を，随時総括責任者に連絡すること。
・二次的な災害が発生した場合，副次的な問題が発生した場合は直ちに連絡すること。

６）個人的な問い合わせに対する対応
・受付を一本化し，自動対応するように予め留守番電話の対応文を用意しておくこと。

３．３　業務継続における必要な人員と物資

（1）必要な人員

業務継続における必要な人員は，予め３．１において決めておくこと。

（2）必要な物資

業務継続における必要な物資，交換部品等は，予め復旧計画に基づいて調達しておくこと。

なお，消耗品類については，一定の在庫を確保するように，随時在庫管理しておくこと。

３．４　機能復旧の手順

機能復旧の手順は１．１に従って進めること。なお，通常業務が継続できない非常時においては，非常時の実施すべき業務を予め決定し，担当者及びユーザに通知しておく。

４．復旧計画

４．１　役割と職務

復旧計画の職員の責務については３．１と同様に実施する。

４．２　計画の実施

復旧計画の実施については，１．４の復旧計画に基づいて実施する。

４．３　復旧における必要な人員と物資

（１）必要な人員

復旧計画実施における必要な人員は，予め３．１と同様に決めておくこと。

（２）必要な物資

復旧計画における必要な物資，交換部品等は，予め復旧計画に基づいて調達しておくこと。

なお，消耗品類については，一定の在庫を確保するように，随時在庫管理しておくこと。

４．４　元の施設への帰還手順

代替施設において復旧作業を実施した場合は，元の施設への移動計画を立案し，スケジュールをユーザに通知して，計画を実施する。

移動が正常に終了した場合は，緊急時の施設を閉鎖する。ただし，以後の不測事態に備えて，これらの施設を別の用途で確保しておくことも考慮すべきである。

以上

５．更新履歴

この計画は平成○○（２０○○）年○○月○○日から実施する。

資料５０３　　大学におけるリスク・マップ例

損害の大きさ	4	・地震による建物倒壊と死者，負傷者の発生 ・火災や爆発による多数の死者，行方不明者発生			
	3	・火災や爆発による建物滅失 ・学生運動やテロによる建物占拠 ・不審者侵入による物的被害・破壊行為 ・入試合否プログラムのミスによる受験者への不利益発生	・停電による情報システムの停止	・感染症の発生による大規模集団健康被害	・有能研究者の転出
	2	・大規模停電による実験設備・装置の停止による物的被害，研究不能 ・台風・竜巻・積雪による建物損壊 ・著作権侵害の発生 ・教職員による採点ミスや成績の入力ミスによる学生への不利益発生	・薬品による健康被害 ・学生，患者，教職員の個人情報漏洩による営業損失の発生	・学生，患者，職員のモラル低下，不祥事による大学評価の下落 ・研究補助金の不正使用 ・データのねつ造や論文盗用による信用失墜	・有能研究者の採用不調 ・中核職員，専門技術者のスピンアウト
	1	・不審者侵入による窃盗 ・知的財産権の被侵害 ・学生，教職員の倫理違反行為による大学評価の下落，信用失墜	・学生，患者，教職員の人権侵害 ・教職員の贈収賄	・役職員の不正労働災害	・セクハラ，パワハラによる人権侵害発生 ・法律違反による情報資産被害
		1	2	3	4
		頻		度	