NIST Special ublication 800-34

IT システムにおける緊急時対応計画ガイド

米国国立標準技術研究所による推奨

Marianne Swanson, Amy Wohl, Lucinda Pope,
Tim Grance, Joan Hash, Ray Thomas,

National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

この文書は下記団体によって翻訳監修されています
独立行政法人 情報処理推進機構
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
NRI SECURE TECHNOLOGIES

NIST Special Publication 800-34

IT システムにおける緊急時対応計画ガイド

National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

米国国立標準技術研究所による推奨

Marianne Swanson, Amy Wohl, Lucinda Pope,
Tim Grance, Joan Hash, Ray Thomas,

2002年6月

米国商務省 長官
Donald L. Evans

技術管理局 技術担当商務次官
Phillip J. Bond

米国国立標準技術研究所 所長
Arden L. Bement, Jr.

コンピュータシステム技術に関する報告書

米国国立標準技術研究所（NIST: National Institute of Standards and Technology、以下、NISTと称する。）の情報技術ラボラトリ（ITL:Information Technology Laboratory）は、国家の測定及び標準基盤において技術的リーダーシップを提供することにより、米国の経済と公共福祉に貢献している。情報技術ラボラトリは、テスト、テスト技法、参照データの作成、コンセプト導入の検証、技術的分析を行い、情報技術の開発と生産的利用の拡大に努めている。情報技術ラボラトリの責務は、技術的、物理的、および管理的標準とガイドラインを策定することにあるが、連邦政府のコンピュータシステムにおいて、費用対効果の高いセキュリティと取り扱いに注意を要する非機密扱い情報のプライバシーを確保するためである。NIST Special Publication 800シリーズでは、コンピュータセキュリティにおける情報技術ラボラトリの調査、ガイダンス、成果を報告し、産業界、政府機関および教育機関との共同活動についても報告する。

米国政府印刷局
WASHINGTON: 2001

政府刊行物管理局、米国政府印刷局より販売
インターネット: bookstore.gpo.gov — 電話: (202) 512-1800 — Fax: (202) 512-2250
郵送: Stop SSOP, Washington, DC 20402-0001

謝辞

NIST技術担当編集者のElizabeth Lennon氏には、このドキュメントを編集していただき感謝している。また、このドキュメントの作成にご尽力いただいたNISTのMark Wilson氏およびRechard Korchak氏にも、感謝の意を表したい。

市販製品または民間組織については、参考までに書かれているに過ぎない。したがって、NISTによる推薦または公認を意味するものではなく、言及された製品がその目的に関して最も有効だと意味しているわけでもない。

エグゼクティブサマリ

NIST Special Publication 800-34『ITシステムのための緊急時対応計画ガイド（Contingency Planning Guide for Information Technology (IT) Systems）』では、政府機関におけるIT緊急時対応計画の手順、推奨事項、考慮事項について説明する。緊急時対応計画とは、緊急事態またはシステム中断があった場合にITサービスを復旧させるための暫定的な措置のことである。暫定的措置には、ITシステムおよび運用の別のサイトへの再配置、代替機器の利用によるIT機能の復旧、手動によるIT機能の実行などが含まれる。

ITシステムには、軽度（短時間の停電、ディスクドライブ障害など）から、重度（装置損壊、火災など）まで、自然災害からテロ行為に至る様々な脅威が存在する。そしてITシステムは、それらの脅威に対して脆弱である。多くの脆弱性は、技術的管理や、組織のリスクマネジメント業務の一環としての運用ソリューションによって最小化できるが、すべてのリスクをなくすことは事実上不可能である。多くの場合、重要なリソースが組織の統制がおよばないところに存在する場合（電力や通信など）、組織はその可用性を保証することはできない。したがって、システムおよびサービスの可用性低下リスクを低減するには、効果的な緊急時対応計画、実施、テストが不可欠である。また、緊急時対応計画を実効性のあるものにするために、連邦政府の管理部門は次の点を考慮する必要がある。

1. IT緊急時対応計画プロセスと、運用継続計画と事業継続計画プロセス全体におけるその位置づけを理解する。

2. 緊急時対応ポリシーと計画プロセスを策定または再検討して、準備計画、事業影響分析、代替サイト選択、復旧戦略など、計画サイクルの要素を実行する。

3. 保守、訓練、IT緊急時対応計画の演習に重点を置いて、緊急時対応計画ポリシーと計画を策定または再検討する。

このドキュメントでは、ITに関する以下の7種類のプラットフォーム[1]に対して推奨する緊急時対応計画について述べ、これらすべてのシステムに共通する戦略と手法を提供する。

---

[1] このドキュメントでは、IT プラットフォームまたは IT システムとは、主要なアプリケーションまたは汎用サポートシステムを指す用語として使用される。

・デスクトップとポータブルシステム

・サーバー

・ウェブサイト

・ローカルエリアネットワーク（LAN）

・ワイドエリアネットワーク（WAN）

・分散システム

・メインフレームシステム

さらにこのドキュメントでは、次の7つのステップからなる緊急時対応プロセスを定義している。この7段階のステップで、組織はITシステム向けに実行可能な緊急時対応計画の策定および保守に適用することができる。そして、システム開発ライフサイクルの各段階に統合できるよう設計されている。

1. **緊急時対応計画ポリシーステートメントの策定**
   正式な部門ポリシーまたは連邦政府ポリシーにより、効果的な緊急時対応計画の策定に必要な権限とガイダンスが得られる。

2. **事業影響分析（BIA：Business Impact Analysis）の実施**
   事業影響分析は、重要なITシステムおよびコンポーネントの特定と優先順位付けに役立つ。また、ユーザーが使いやすいように、事業影響分析を作成するためのテンプレートを提供している。

3. **予防対策の特定**
   システム中断の影響を極小化する対策によって、システムの可用性が高まり、緊急時対応ライフサイクルのコストが削減できる。

4. **復旧戦略の策定**
   周到な復旧戦略によって、システムの中断直後の効率的かつ迅速な復旧が保証される。

5. **IT緊急時対応計画の策定**
   緊急時対応計画には、詳細なガイダンスと、中断されたシステムを復旧する手順を含める必要がある。

6. **テスト、訓練、演習の計画**
   計画をテストすることで計画の漏れが特定でき、訓練することで計画を遂行する復旧要員を育成する。この両方によって、計画の効率が高まり連邦政府全体での対策が改善される。

7. **計画の保守**
   計画は、システムの拡張に伴って定期的に更新し最新の状態を保持したものでなければならない。

このドキュメントは、IT緊急時対応計画の策定のためのサンプルフォーマットとなる。フォーマットには、システム中断後に講じるアクションを規定した、3つのフェーズが定義されている。**通知/実行**フェーズでは、復旧担当者に通知して損害評価を実行するプロセスを規定する。**復旧**フェーズは、IT運用を代替サイトまたは緊急時対応機能を使用して復元するために、復旧チームと要員に提案される一連のアクションを示す。最終フェーズである**再構築**フェーズでは、システムを通常の運用状態に復元するために講じるアクションを示す。

目次

図

表

1. はじめに

情報技術（IT）および自動化された情報システムは、ビジネスプロセスにおいて不可欠な要素である。そのため、これらのシステムによって提供されるサービスが過度に中断されることがないように効果的に運用することが非常に重要である。緊急時対応計画ではこの要件を満たした完璧な計画と手順や技術的対策を確立し、サービスの中断または災害発生後、システムが迅速かつ効率的に復旧できるようにする。

IT緊急時対応計画とは、システムが中断された後、ITシステム、運用、データを復旧させるための、計画、手順、技術的対策を含めた組織的戦略のことである。緊急時対応計画には、一般的に、中断されたITサービスを復元するアプローチが1つ以上含まれている。例として、次のようなアプローチがある。

- 代替地点でのIT運用の復元
- 代替装置を使用するIT運用の復旧
- 影響を受けた一部またはすべての非IT（手動）手段によるビジネスプロセスの実行
  （通常は短期的な損害にのみ適用可能）

本ドキュメントは、IT緊急時対応計画の策定及びその維持更新に責任を持つ担当者へのガイダンスである。本ドキュメントでは、緊急時対応計画の本質的な要素およびプロセスについて説明する。そして、各種のITシステム向け緊急時対応計画についての具体的な検討事項および考慮すべき事項を明確にし、独自のIT緊急時計画を策定する読者に役立つ事例を提供する。本ドキュメントは、連邦情報処理規格刊行物（FIPS PUB）87、『Guidelines for ADP Contingency Planning』に代わるものである。

1.1 作成機関および適用範囲

このドキュメントは、NISTが、1987年のコンピュータセキュリティ法（Computer Security Act）および1996年の情報技術管理改革法（Information Technology Management Reform Act）、合衆国法律集第15編第278条g-3(a)(5)項に基づき、その法的責任を推進するために作成したものである。このドキュメントは、合衆国法律集第15編第278条g-3(a)(3)項における意味でのガイドラインではない。これらのガイドラインは、取り扱いに注意を要する情報を扱う連邦政府組織が使用するためのものである。これは行政管理予算局（OMB; Office of Management and Budget）Circular A-130付録IIIの要件と一致している。

このドキュメントは、非政府組織が自己責任において使用することもできる。著作権の制約はない(翻訳者注:著作権に関するこの記述は、SP800-34の英語の原文のことを言っており、日本語へ翻訳した本

書の著作権は、独立行政法人 情報処理推進機構 及び NRIセキュアテクノロジーズ株式会社に帰属する）。

このドキュメントにおける一切は、商務長官が法的権威に基づき連邦政府に対して義務および拘束力を与えた標準およびガイドラインを否定するものではない。また、これらのガイドラインは、商務長官、行政管理予算局長、または他のすべての連邦政府当局者の既存の権威に変更を加えたり、これらに取って代わるものと解釈してはならない。

1.2 目的

このIT緊急時対応計画ガイドでは、担当者が効果的なIT緊急時対応計画の策定および保守を行えるよう、計画時における基本的な原則および実施例を作成している。この原則はほとんどの組織のニーズを満たすが、各組織はそのほかにも独自のプロセスに固有の要件を持っていることがある。本ドキュメントには、担当者が情報システムおよび運用を評価し、緊急時対応の要件と優先度を決定する助けとなる指針が記載されている。本ガイダンスでは、計画者がIT要件を正確に反映し、緊急時対応計画原則をIT運用のすべての側面に統合するコスト効率の高いソリューションを作成するのに役立つ体系的な方法を提供する。

このガイダンスで提供されている内容は、緊急時対応計画の概念化から保守、廃棄に至る、緊急時対応計画のどの段階においても考慮する必要がある。本ドキュメントおよび付録を計画管理ツールとして使用すると、全体にわたって時間とコストをかけずに緊急時対応計画プロセスを策定することができる。

1.3 範囲

本ドキュメントは、NISTが連邦政府部局および機関に対する推奨ガイダンスとして発行している。ここでは、次の一般的なIT処理システムに対する緊急時対応計画原則を説明する。

- デスクトップコンピュータおよびポータブルシステム
  （ラップトップおよびハンドヘルドコンピュータ）

- サーバー

- ウェブサイト

- ローカルエリアネットワーク（LAN）

・ ワイドエリアネットワーク（WAN）

・ 分散システム

・ メインフレームシステム

本ドキュメントでは、スーパーコンピュータおよび無線ネットワーク向けの緊急時対応計画については触れていない。しかし、ここで述べる原則の多くはこれらのシステムに対しても適用される。

緊急時対応計画の策定担当者を支援するため、本ドキュメントでは、緊急時対応能力をサポートする汎用的な技術について述べる。しかし、IT設計と構成は多岐にわたり、開発スピードの高速化に伴う製品および機能の陳腐化により、ここで挙げる範囲が全体におよんでいるとは限らない。むしろ技術を適用し、組織のIT緊急時対応計画の機能を向上できる事例について説明する。

ここでは、ITシステムの運用に影響を及ぼす各種のインシデントに適用できる計画原則について概略を説明する。短期の中断をもたらす軽微なインシデントから、長期にわたって通常業務に影響する災害までを対象とする。ITシステムの設計とアプリケーションは多岐にわたるため、ここでは特定の種類のインシデントとそれに関連する緊急時対応の方法は取り上げていない。その代わり、このガイドラインでは、任意のITシステムに対して計画要件を特定し、災害に対する効果的な緊急時対応計画を策定できるプロセスを定義する。

本ガイドラインは、情報システムとその処理機能の復元に必要な場合を除いて、施設レベルまたは組織的なIT緊急時対応計画については説明しない。施設レベルおよび組織的な緊急時対応計画は通常、IT緊急時対応計画というよりは、むしろ運用継続計画（COOP; Continuity of Operation Plan）のが対象とするものである。また、ビジネスプロセスに対する緊急時対応計画については、通常、ビジネスの再開または事業継続計画で取り扱われる課題であるため、ここでは取り上げない。情報システムは通常、ビジネスプロセスをサポートする。しかし、ビジネスプロセスは情報システムに関係しない、他の多様なリソースおよび機能にも依存する。運用継続、ビジネスの再開、事業継続計画については、第2.2項で後述する、緊急事態管理計画の一部で触れている。

本ガイドでの情報は、NISTSpecial Publication800-12『An Introduction to Computer Security: The NIST Handbook』第11章「Preparing for Contingencies and Desasters」など、その他のNISTドキュメントによるガイダンスと一貫している。また、提案するガイダンスは、以下に挙げる緊急時対応、運用継続、災害復旧計画に関連する連邦政府の指示にも準拠している。

- コンピュータセキュリティ法（Computer Security Act of 1987）、1987年

- 行政管理予算局（OMB）Circular A-130、『Management of Federal Information Resources』付録III、2000年11月

- 連邦情報処理規格刊行物（FIPS PUB）87『Guidelines for ADP Contingency Planning』、1981年3月（本書により修正済み）

- 連邦準備令（FPC; Federal Preparedness Circular）65、『Federal Executive Branch Continuity of Operations』、1999年7月

- 大統領令（PDD; Presidential Decision Directive）67『Enduring Constitutional Government and Continuity of Government Operations』、1998年10月

- PDD 63『Critical Infrastructure Protection』、1998年5月

- 連邦緊急管理庁（FEMA; Federal Emergency Management Agency）『FRP; Federal Response Plan』、1999年4月

連邦政府部局および機関は、上記の連邦政策に加え、内部部門のポリシーに準拠する必要がある。本ガイダンスでは、連邦政府コンピュータシステムに対する緊急時対応計画を策定する方法とその理解について説明する。

ITシステム: *

ITシステムは、プロセス、通信、ストレージ、および関連リソース（アーキテクチャ）の境界を定義して特定される。

ITシステムのコンポーネントは、すべてが物理的に接続されている必要はない。たとえば、[1]オフィス内のスタンドアロンのパーソナルコンピュータ（PC）、[2]規定されたテレコミューティングプログラムルールの下で従業員の自宅に置かれたPC、[3]業務でモバイルコンピューティング機能を必要とする従業員に与えられたポータブルPC、[4]同じ環境と物理的条件で設置された、複数の同一構成を持つシステムがある。

* NIST Special Publication 800-18『Guide for Developing Security Plans for Information Technology Systems』の定義による。

1.4 対象とする読者

連邦政府組織内のマネージャ、およびシステムレベルまたは運用レベルのITセキュリティの担当者は、本ドキュメントに記述する原則を活用できる。以下のような人員が対象となる。

- マネージャ – IT運用を行うまたはITビジネスを手がける
- システム管理者 – 日々のIT運用の保守を担当する
- 情報システムセキュリティ担当者（ISSO; Information System Security Officer）およびスタッフ – 組織のITセキュリティ活動の開発、導入、保守を担当する
- システムエンジニアおよび設計者 - 情報システムの設計、導入、変更を担当する
- ユーザー – デスクトップまたはポータブルシステムを使用して、割り当てられた職務を遂行する
- その他の人員 – 情報システムの設計、管理、運用、保守、利用を担当する

さらに、緊急事態管理担当者は、施設レベルの緊急時対応を調整する必要が生じることがあるため、このドキュメントをIT緊急時対応計画活動に活用することができる。本ドキュメントに示す概念は、連邦政府システムだけのものではなく、民間または商業組織に利用されることもある。

1.5 ドキュメントの構成

本ドキュメントでは、多様な組織に適用できるIT緊急時対応計画プログラムの設計、復旧戦略オプションと技術的検討事項に対する組織のニーズの評価、復旧戦略のIT緊急時対応計画への文書化のプロセスを論理的に説明する。緊急時対応計画は、災害発生時に戦略を実行するための、「ユーザーマニュアル」として機能する。理解を深めるため可能な場所においては、例や仮のシチュエーションを紹介する。

本ドキュメントの後続の項では、緊急時対応計画について次の事項を説明している。

- 第2項、背景: 緊急時対応計画についての背景情報を述べる。緊急時対応計画の目的、各種の緊急時対応計画、組織のリスク管理およびシステム開発ライフサイクル管理プログラムへの計画の統合方法などを含む。

- 第3項、IT緊急時対応計画プロセス: 効果的な緊急時対応能力の開発に必要な基本的な計画原則を詳説する。この項で要約する原則は、すべてのITシステムに対し共通に適用される。この項では、準備計画、事業影響分析、代替サイト選択、復旧戦略など、計画サイクルのすべての要素に対する緊急時対応計画ガイダンスを説明する。また、緊急時対応チームの構築や、チームメンバーに一般的に割り当てられる役割と責任についても説明する。

- 第4項、IT緊急時対応計画策定: 緊急時対応戦略の文書化に必要な活動を、詳細化する。このようにして文書化したものが、IT緊急時対応計画となる。緊急時対応計画の整備、テスト、訓練、演習についても説明する。

- 第5項、緊急時対応計画の技術的な考慮事項: 第1.3項「範囲」に挙げた、ITシステムに固有の緊急時対応計画についての考慮事項を説明する。この項は緊急時対応計画の策定者が、対象システムに適切で技術的な緊急時対応策を特定、選択、導入する場合に役立つ。

本ドキュメントには、8つの付録が付属している。付録Aでは、IT緊急時対応計画のフォーマット例を提供する。付録Bでは、事業影響分析テンプレートの例を示す。付録Cは、IT緊急時対応計画に関する、よくある質問とその回答の一覧である。人員に関する考慮事項についての課題は、付録Dで説明する。付録Eは用語集である。付録FとGは、推奨するインターネット上の情報源と参考文献の一覧である。付録Hは、ドキュメントの索引である。

2. 背景

ITシステムは、軽度（短時間の停電、ディスクドライブ障害など）から、重度（装置破壊、火災など）まで、様々な脅威に対して脆弱である。多くの脆弱性は、組織のリスクマネジメント業務の一環として、行われる技術的対策、管理的対策、および運用的対策により最小化もしくは削除することができる。しかし、すべてのリスクをなくすことは事実上不可能である。[2] 緊急時対応計画は、効果的で効率的な復旧に重点を置き、システムとサービスが利用できなくなるリスクを低減させるために設計されている。

この項では、IT緊急時対応計画を組織のより広範囲なリスクマネジメント、セキュリティ、緊急時対応プログラムに組み込む方法について説明する。また、その他の緊急時対応関連の計画や、そのIT緊急時対応計画との関連性についても説明する。さらに、緊急時対応計画の原則をどのようにシステム開発ライフサイクルに組み込めば、システムの互換性を促進し、緊急事態に対して組織の迅速かつ効果的な対応能力を向上させる費用対効果の高い手段が得られるかについて説明する。

2.1 緊急時対応計画とリスクマネジメントプロセス

リスクマネジメントは、ITシステムに対するリスクを特定、コントロール、および低減するための幅広い活動を含んでいる。IT緊急時対応計画の視点から見たリスクマネジメントを行うことは、2つの主要な機能がある。まずリスクマネジメントでは、適切な措置を施し、インシデント発生の防止やインシデントによる影響を局限化するために、脅威と脆弱性を特定する必要がある。これらのセキュリティコントロールによって、ITシステムは以下の3種類の脅威から保護される。

- 自然 - 台風、竜巻、洪水、火災など
- 人的[3] – 操作ミス、妨害行為、悪意のあるコードの埋め込み、テロ攻撃など
- 環境 – 機器故障、ソフトウェアエラー、通信ネットワークの切断、停電など

---

[2] たとえば、重要なリソースが組織の統制が及ばないところに存在する場合（電力やテレコミュニケーションなど）、組織はその可用性を保証することができない。

[3] このドキュメントでは、サイバー攻撃（サービス拒否、ウイルスなど）への対応については取り上げない。これらの種類のインシデントへの対応には、IT 緊急時対応計画の対象範囲外の内容が含まれている。同様に、本ドキュメントでは、不法侵入、サービス拒否攻撃、悪意のあるロジックの注入などのサイバー犯罪に対するコンピュータフォレンジック分析による証拠保存に関連する、インシデント対応についても記述していない。

次に、リスクマネジメントは緊急時対応計画の適用が必要となるような残存リスクを特定する。したがって、緊急時対応計画は、リスクアセスメントとリスク低減プロセスによる結果と非常に密接な関係にある。図2-1には、セキュリティコントロールの特定と導入、緊急時対応計画の策定と保守、緊急事態発生時における対応計画との導入の関係を示す。

図2-1 リスクマネジメント導入の要素としての緊急時対応計画

サービス中断中のITシステムへのリスクを効果的に特定するには、ITシステム環境のリスクアセスメントが必要となる。完全なリスクアセスメントでは、システムの脆弱性、脅威、今行うべき対策を特定し、危険性および脅威の影響に基づいてリスクの判定を試みる。これらのリスクを評価することにより、リスクレベルが判定される（高度、中度、低度など）。NIST Special Publication 800-30『Guide to Information Technology Systems』では、リスクアセスメントの実施方法と、技術上、管理上、運用上の適切なセキュリティコントロールを判定する方法について、詳細なガイダンスを提供している。

リスクは時とともに変化し、システムの進展にしたがって以前とは異なる新しいリスクが発生することがある。そのため、リスクマネジメントプロセスは常に動的で変化していく必要がある。IT緊急時対応計画の担当者は、システムに存在するリスクを認識し、現在の緊急時対応計画が残存リスクに完全かつ効果的に対応できるかどうか確認する必要がある。第3.6項に述べるように、対象となるリスクに変更が生じると、緊急時対応計画の継続的な保守、テスト、さらに定期的なレビューが要求される。

2.2 計画の種類

IT緊急時対応計画は、緊急事態発生後の重要なITサービスの継続、復旧を目的として策定された幅広い対策範囲を規定する。IT緊急時対応計画は、組織またはビジネスプロセス継続および復旧計画を含む、より広範な緊急事態対策環境の対象に含まれる。最終的には、組織は一連の計画を使用して、組織のITシステム、ビジネスプロセス、施設に影響を及ぼす中断に対して対応、復旧、継続の準備をする。ITシステムとサポートするビジネスプロセスには内在的な関係がある。そのため、策定および更新において、各計画間の連携をとり、復旧戦略およびサポート用リソースが互いの足を引っ張ったり二重に処理を実施したりしないようにする必要がある。

一般には、IT緊急時対応計画とその関連計画領域の定義として、普遍的に受け入れられているものは存在しない。このような定義が存在しないことで、各種の計画の実際の範囲と目的を考える際に、混乱が生じることがある。本項では、IT緊急時計画に関する共通理解の基盤を提供するため、その他の種類の計画をいくつか特定し、IT緊急時対応計画と比較してその目的と範囲について説明する。これらの種類の計画には標準的な定義が存在しないため、組織が策定した実際の計画の範囲と、これから説明する内容とは異なる場合がある。本ドキュメントでこれらの計画について言及する場合、以下のような意味で使用する。

事業継続計画（BCP; Business Continuity Plan）

事業継続計画では、中断の発生中および発生後における、組織のビジネス機能を継続することに重点を置いている。ビジネス機能の例として、組織の給与支払いプロセスや、顧客情報プロセスが挙げられる。事業継続計画は、特定のビジネスプロセスを対象に策定されることも、すべての主要なビジネスプロセスを対象にすることもある。ITシステムは事業継続計画において、ビジネスプロセスをサポートするという観点で扱われる。場合によっては、事業継続計画は長期にわたる復旧プロセスと通常業務への復旧には対応せず、暫定的なビジネス継続要件のみを対象とすることがある。また、災害復旧計画、事業復旧計画、人員緊急時計画などを事業継続計画に追加することができる。事業継続計画で設定される責任と優先度は、運用継続計画での規定と調整され、矛盾を避ける必要がある。

事業復旧計画（BRP; Business Recovery Plan）、または事業再開計画

事業復旧計画では、緊急事態発生後のビジネスプロセスを復元するが、事業継続計画とは異なり、緊急時または中断時における重要プロセスの継続を確保する手順はない。事業復旧計画の策定にあたっては、災害復旧計画および事業継続計画と連携させる必要がある。事業復旧計画は事業継続計画に追加できる。

運用継続計画（COOP：Continuity of Operations Plan）

運用継続計画[4]では、組織（通常は本社）の本質的な機能を代替サイトで復元し、通常業務に戻るまで最大30日間該当機能を実行することに重点を置いている。運用継続計画は本社レベルの問題に対処するため、事業継続計画とは独立して策定され、実行される。実行可能な運用継続計画の導入については、PDD 67、『Enduring Constitutional Government and Continuity of Government Operations』で規定されている。運用継続計画の連邦政府執行機関であるFEMAは、FPC 65、『Federal Executive Branch Continuity of Operations』で運用継続計画ガイダンスを提供している。運用継続計画の標準要素には、権限委譲宣言、継承順序、重要な記録およびデータベースがある。運用継続計画では代替サイトでの組織の運用機能の復旧を重視しているため、この計画にはIT運用を含める必要はない。さらに、通常は代替サイトへの移転を必要としない軽微な中断については、対象としていない。しかし、運用継続計画に事業継続計画、事業復旧計画、災害復旧計画を付録として追加することができる。PDD-63、『Critical Infrastructure Protection』によると、国家のインフラストラクチャのサポートに欠かせないシステム向けの運用継続計画が、2003年5月に発効されている。

サポート継続計画/IT緊急時対応計画

OMB Circular A-130、付録IIIでは、汎用サポートシステム向けサポート継続計画および主要アプリケーション向け緊急時対応計画の策定と整備を要求している。本ガイドラインでは、サポート継続計画をIT緊急時対応計画と同義に扱っている。IT緊急時対応計画は各主要アプリケーションおよび汎用サポートシステム用に策定する必要があるため、組織の事業継続計画では複数の緊急時対応計画が整備されていることがある。

緊急時コミュニケーション計画

組織は、災害発生前に内部および外部との連絡手順を準備しておく必要がある。緊急時コミュニケーション計画は、一般人からの問い合わせに責任を持つ部署が策定することが多い。緊急時コミュニケーション計画の手順は、その他のすべての計画と調整を図り、承認された事柄のみが公表されるようにする。計画手順は、事業継続計画に付録として追加する必要がある。コミュニケーション計画では通常、災害対応に関して一般人からの質問に応答する権限を独占的に持つ、特定の要員を指定する。状況報告を要員および一般人に配布する手順を含むこともある。プレスリリース用のテンプレートも計画に含まれる。付録Dでは、緊急時コミュニケーション計画の対象となる課題に関して説明し、情報源を示す。

---

[4] 組織によっては、COOP を運用継続計画（Continuity of Operations Plan）ではなく、運用継続性（Continuity of Operations）の意味で使用する場合がある。

サイバーインシデント対応計画

サイバーインシデント対応計画は、組織のITシステムに対するサイバー攻撃への対処手順を確立する。これらの手順は、セキュリティ担当者がシステムまたはデータへの不正アクセス、サービス拒否、システムハードウェア、ソフトウェア、データへの不正な変更（ウイルス、ワーム、トロイの木馬に挙げられるような悪意のあるロジック）などの、不正なコンピュータインシデントを特定し、その影響を緩和し、復旧できるように設計されている。この計画は、事業継続計画の付録に追加することができる。

災害復旧計画（DRP; Disaster Recovery Plan）

その名前が示すように、災害復旧計画は、長期にわたって一般施設へのアクセスが阻害されるような重大な通常は壊滅的とされる事象に適用される。災害復旧計画は、緊急事態発生後に、対象のシステム、アプリケーション、またはコンピュータ施設を代替サイトで運用できるようにITに焦点をあてた設計がなされている。災害復旧計画の範囲はIT緊急時対応計画と重複する場合があるが、災害復旧計画は狭義であり、移転を必要としない軽微な中断には対応しない。組織のニーズによっては、複数の災害復旧計画を事業継続計画に追加することがある。

人員緊急時計画（OEP）

人員緊急時計画は、人員の健康や安全性、環境または、資産を脅かす恐れがあるような状況が発生した場合に、施設内の人員が行う対応手順を規定したものである。このような事象には、火災、台風、悪質な攻撃、医療上の緊急事態がある。人員緊急時計画は施設単位で策定され、建物の地理的な位置および構造的設計ごとに異なる。一般調達局（GSA; General Services Administration）所有の施設では、一般調達局人員緊急時計画テンプレートに基づく計画を保持している。施設の人員緊急時計画は事業継続計画に追加できるが、実行については独立して行われる。人員の安全と避難に関する計画については、付録Dで説明する。

表2-1は、上記で説明した計画の種類をまとめたものである。

計画名	目的	範囲
事業継続計画（BCP）	必要不可欠な業務を継続しながら、重大な中断状態から復旧する手順を提供する。	ビジネスプロセスを扱う。ITについては、ビジネスプロセスのサポートに影響するものに限って対処する。
事業復旧（再開）計画（BRP）	災害発生後、迅速にビジネス業務を復旧する手順を提供する。	ビジネスプロセスを扱う。IT特化ではないが、ビジネスプロセスのサポートに付いては、ITに基づいたものに限る。

運用継続計画（COOP）	組織において必要不可欠かつ戦略的な機能を代替サイトで最大30日間継続させるのに必要な手順や設備を提供する。	最も重要な組織のミッションのサブセットを扱う。通常は本社レベルに向けて策定される。ITには特化しない。
サポート継続計画/IT緊急時対応計画	主要なアプリケーションまたは汎用サポートシステムを復旧する手順や設備を提供する。	IT緊急時対応対応計画と同様、ITシステムの中断を扱い、ビジネスプロセスには特化しない。
緊急時コミュニケーション計画	要員および一般人に現状を報告する手順を提供する。	要員と一般人とのコミュニケーションを扱い、ITには特化しない。
サイバーインシデント対応計画	悪意のあるサイバーインシデントの検知、対応、その影響の低減のための戦略を提供する。	システムおよびネットワークに影響を及ぼすインシデントへの、情報セキュリティ対応策を重視する。
災害復旧計画（DRP）	代替サイトでのサービス提供能力の復旧を促進する詳細手順を提供する。	ほぼ、ITに特化している。影響が長期にわたる大規模災害に限定される。
人員緊急時計画（OEP）	物理的な脅威に対し、生命への危険および傷害の発生を最小化し、資産を損害から保護するため、調整された手順を提供する。	特定施設に関連する人員および資産を重視する。ビジネスプロセスまたは、ITシステムの機能性には特化しない。

表2-1 緊急時対応計画に関連する計画の種類

図2-2に、各種の計画の相互関連性と、その目的について示す。

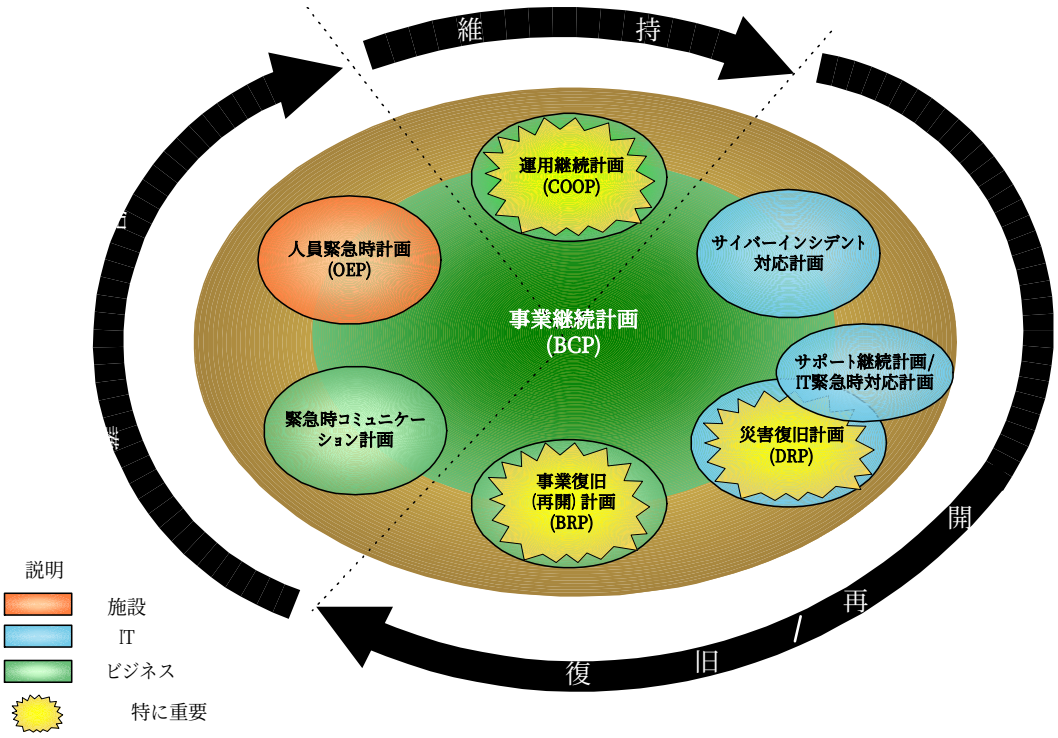


図2-2 緊急時対応計画の相互関係

2.3 緊急時対応計画とシステム開発ライフサイクル

システム開発ライフサイクル（SDLC; System Development Life Cycle）とは、システムの有効期間中にシステム所有者によって実行される、すべての行為をいう。ライフサイクルは、図2-3に示すように、プロジェクト開始に始まり、システム廃棄で終了する。[5] 緊急時対応計画は運用/保守フェーズで発生する行為に関連するが、有事対策は、コンピュータシステムのライフサイクルにおけるすべてのフェーズにおいて、認識され、統合されるべきものである。このアプローチにより、緊急時対応計画全般のコストを削減し、緊急時対応能力が向上し、緊急時対応計画を導入した場合のシステム運用への影響が軽減される。本項では、緊急時対応戦略をシステム開発ライフサイクルへ統合する一般的な方法を説明する。特定の緊急時対応および戦略については、第5項「緊急時対応計画の技術的な検討事項」を参照のこと。

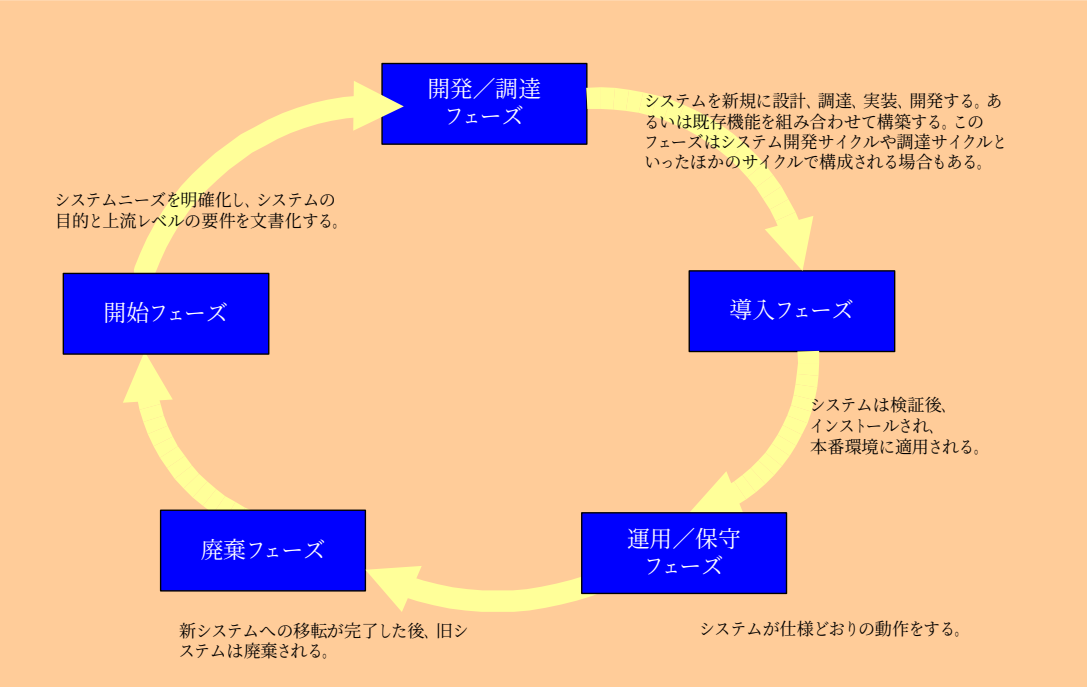


図2-3 システム開発ライフサイクル

開始フェーズ

新ITシステムを企画する場合、緊急時対応計画の要件を考慮する必要がある。開始フェーズでは、システム要件を特定し、その関連運用プロセスと一致させることによって、緊急時対応の初期要件が明らかになる。非常に高いシステム可用性が要求され、代替サイトにおける重複性、リアルタイムミ

---

[5] システム開発ライフサイクルには、いくつかのひな型がある。本ドキュメントで使用したモデルは、NIST Special Publication800-12、『An Introduction to Computer Security: The NIST Handbook』第 8 章に準じたものである。

ラーリング機能および、障害時におけるフェイルオーバー機能をシステム設計に取り入れる必要がでてくる。同様に、モバイルアプリケーションまたはアクセス不能な地点など、通常以外の条件でシステムを運用する場合、リモート診断機能や自己修復機能などの機能を設計に追加する必要がある。このフェーズでは、新ITシステムを既存または計画済みのすべてのITシステムに照らして評価し、適切な復旧優先度を決定する必要がある。この優先度は、複数のITシステムの復旧順序を作成する際に使用される。

開発/調達フェーズ

初期概念がシステム設計に反映され、特定の緊急時対応策が組み込まれる。開始フェーズと同様に、このフェーズに取り入れられる緊急時対応策は、システムおよび運用要件を反映したものでなければならない。設計には、システムアーキテクチャに対する冗長性と堅牢性を取り入れ、運用/保守フェーズにおける信頼性、保守可能性、可用性を最適化する。初期設計でこれらを導入することで、コストが削減され、運用/保守フェーズでのシステムの追加または更新などの問題が低減される。新しい汎用サポートシステムがホストするアプリケーションが複数ある場合、各アプリケーションの優先度を設定し、適切な緊急時対応策の選択と復旧手段の実行順序の決定を支援する。このフェーズで検討される緊急時対応策の例は、冗長性のある通信パス、システム全体の中断につながる単一障害点の除去、ネットワークコンポーネントおよびインターフェースのフォールトトレランス向上、適正サイズのバックアップ電源を持つ電源管理システム、負荷分散、システムの全般的な堅牢性を保つためのデータミラーリングおよび複製である。緊急時対応策として代替サイトを選択した場合、代替サイトの要件はこのフェーズで取り扱う。

導入フェーズ

システムが初期テスト中であっても緊急時対応戦略を検証し、技術的機能および復旧手順が正確で効果的であることを確認する必要がある。緊急時対応戦略の検証においては、テスト計画が求められる。これらの緊急時対策が検証されたら、それは緊急時対応計画の中に明確に文書化されることが望ましい。

運用/保守フェーズ

システムが運用段階になると、ユーザー、管理者、マネージャは、緊急時対応計画手順を包含する訓練と意識向上プログラムを整備しなければならない。演習とテストを実施し、手順が継続して有効になるようにする。定期的にバックアップを実施して、オフサイトに保存する。学習した事柄をもとに当該計画の手順に変更を加え、更新する必要がある。ITシステムが改善されたり、または外部インターフェースの変更などで修正された場合、このような変更を緊急時対応計画に反映させなければならない。変更内容はタイムリーに計画に盛り込んで文書化し、計画の有効性を維持する。

廃棄フェーズ

既存のコンピュータシステムを撤去し、別のシステムに交換する場合も、緊急事態について考慮しなければならない。新システムが稼働して完全にテストが完了するまでは（その緊急時対応能力も含めて）、レガシーシステムの緊急時対応計画を実施可能な状態にしておく必要がある。レガシーシステムが交換される際には、新システムに損失または障害が発生した場合の貴重なバックアップ能力を提供する場合がある。場合によっては、ハードウェアの装置部品（ハードドライブ、電源サプライ、メモリチップ、ネットワークカードなど）は、新システムで運用される新装置の予備部品として利用できる。さらに、レガシーシステムは新アプリケーションのテストシステムとして利用でき、システムを中断する恐れのある欠陥を特定し、運用環境にないシステム上で修正することができる。

3. IT緊急時対応計画のプロセス

本項では、効果的なIT緊急時対応計画の策定および保守に関するプロセスについて説明する。ここで示すプロセスは、すべてのITシステムに共通する。プロセスには、以下のような7つのステップがある。

1. 緊急時対応計画ポリシーステートメントの策定

2. 事業影響分析の実施

3. 予防対策の特定

4. 復旧戦略の策定

5. IT緊急時対応計画の策定

6. テスト、訓練、演習の計画

7. 計画の保守

これらのステップは、IT緊急時対応計画能力全体の主要な要素を表している。計画プロセスの7つのうち6ステップについて、本項で説明する。5番目の「緊急時対応計画」は、計画を構成する個々のを含み、IT緊急時対応計画の中核であるため、計画策定についてはそれ独自の項（第4項）で説明する。計画プロセスの責任は、一般に「緊急時対応計画コーディネーター」または「緊急時対応計画プランナー」にある。このスタッフは通常、連邦政府内の実質的なマネージャまたはリソースマネージャである。当該コーディネーターは、システムまたはシステムがサポートするビジネスプロセスに関連する他の実質的またはリソースマネージャと協力して戦略を策定する。緊急時対応計画コーディネーターは通常、緊急時対応計画の策定と実行についても管理する。すべての主要アプリケーションおよび汎用サポートシステムに対して、緊急時対応計画を策定する必要がある。図3-1は、緊急時対応計画プロセスを示す。

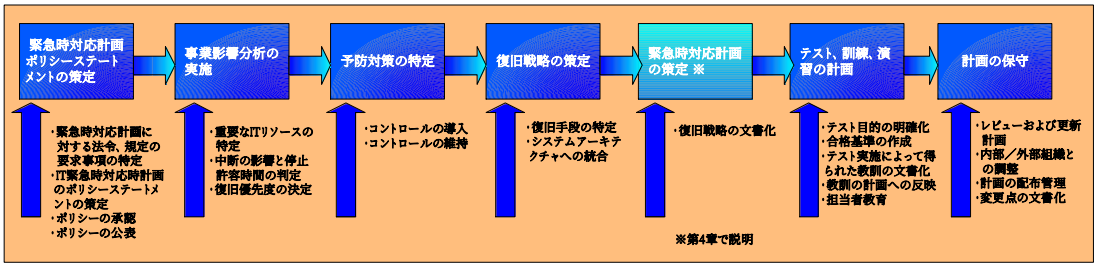


図3-1 緊急時対応計画プロセス

3.1 緊急時対応計画ポリシーステートメントの策定

連邦政府各省庁の緊急時対応計画要件を担当者が十分理解し計画を効果的に策定するために、緊急時対応計画は明確に定義された方針に基づくものでなければならない。緊急時対応計画ポリシーステートメントは、連邦政府の緊急時対応目標全般を定義し、IT緊急時対応計画に対する組織のフレームワークと責務を確立する。成功させるには、CIO（最高情報責任者）のような上級経営幹部が緊急時対応計画をサポートしなければならない。こういった上級経営幹部は、計画のポリシーや構造、目標や役割、権限、責任を決定するプロセスに関与する必要がある。最低でも緊急時対応ポリシーは、第1.1項で挙げた文書に記載された連邦政府ガイダンスに準拠しなければいけない。連邦政府はそれぞれのITシステム、運用、要件を評価して、緊急時対応計画要件を追加すべきかどうか決定する。鍵となるポリシー要素には、以下のようなものがある。

- 役割と責任
- 緊急時対応計画の対象となり、適用されるプラットフォームおよび組織機能の範囲
- リソース要件
- 訓練要件
- 演習とテストのスケジュール
- 計画の整備のスケジュール
- バックアップ頻度とバックアップメディアの保管

仮想連邦政府（HGA）におけるIT緊急時対応ポリシーの例*

すべての仮想連邦政府組織は、主要な各アプリケーションと設備全体をサポートするシステムに対する緊急時対応計画を定める。これは、72時間を越える障害が発生した場合における重要なIT運用の必要性を満たすものである。このようなIT運用の実施手順は、緊急時対応計画コーディネーターにより緊急時対応計画として公式に文書化される。そして、緊急時対応計画コーディネーターによって毎年再検討され、必要に応じて更新される。手順では夜間フルバックアップを実行し、指定のオフサイト施設へ送信されることを規定する。本計画では、指名スタッフおよび職位に特定の責務を割り当て、根本的なIT機能の復旧および継続性を支援する。そして、手順の実行に必要なリソースを確保し、維持する。また、対象システムの要員が緊急時対応手順を実行できるよう教育する。当該計画、復旧能力、担当者を毎年検証し、その弱点を特定する。

* 仮想連邦政府およびそのポリシーは、説明上のものである。NIST SP 800-12 第13章には、仮想連邦政府のコンピュータセキュリティに関する実例を示している。

IT緊急時対応計画ポリシーとプログラムが策定されると、ITセキュリティ、物理的セキュリティ、人的資源、IT運用、緊急時対応機能などの連邦政府に関連する活動との調整が行われる。IT緊急時対応活動は、これらの分野のプログラム要件と互換性を持ち、緊急時対応担当者は各分野の代表者と協議し、新たなまたは、展開されるポリシー、プログラム、能力を常に認識しておく必要がある。緊急時対応計画は、システムに関連するその他の既存の計画と調整して策定する。以下のような計画が対象となる。

・ システムセキュリティ計画など、セキュリティ関連計画

・ 人員緊急時計画、運用継続計画など、施設レベルの計画

・ 事業復旧計画または重要インフラ防護計画（CIP）など、連邦政府レベルの計画

3.2 事業影響分析の実施

事業影響分析は、緊急時対応計画プロセスにおける主要なステップである。事業影響分析は、緊急時対応計画コーディネーターが、システム要件、プロセス、および相互依存関係を十分に特定し、当該情報を使用して緊急時対応要件と優先度を決定することを可能にする。事業影響分析の目的は、事業影響分析が提供する個々のシステムコンポーネントとの重要なサービスと関連付け、その情報を基に中断によってシステムコンポーネントが受ける被害の原因を特徴付けることである。事業影響分析の結果は、組織の行う運用継続計画、事業継続計画、事業復旧計画の分析と戦略策定に取り入れられる。図3-2に挙げる事業影響分析プロセスの例では、緊急時対応計画コーディネーターが緊急時対応計画策定活動を合理化して強化し、より効果的な計画を作り出せるようにする[6]。事業影響分析プロセスの例と事業影響分析テンプレートの例を、付録Bに示す。

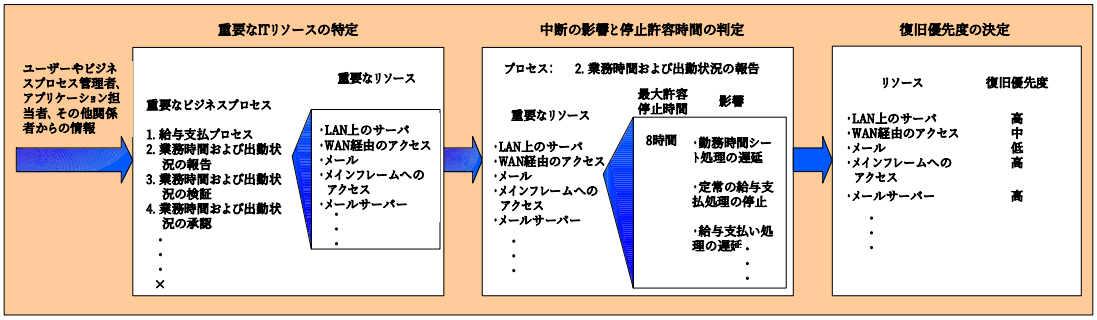


図3-2 仮想連邦政府における事業影響分析プロセス

3.2.1 重要なITリソースの特定

ITシステムは多数のコンポーネントやインターフェース、プロセスを持ち、非常に複雑になることがある。そのため、システムが複数のミッションを持ち、システムサービスもしくはシステム能力の重要性に対して異なる視点を持つようになる。最初の事業影響分析ステップでは、ITシステムを評価してシステムが実行する重要な機能を判定し、その実行に要求されるシステムリソースを特定する。このステップの実行には、通常2つの活動が要求される。

---

[6] ここで示す事業影響分析の例には、完全を期すための主要なアプリケーションまたは汎用サポートシステムに不慣れな緊急時対応計画コーディネーターを支援するために、基本ステップを含めている。多くの場合緊急時対応計画コーディネーターは、特定のシステムコンポーネントと、それがビジネスプロセスをサポートする方法について深く精通している。特に、小規模システムの場合はそうである。このような場合、すべての事業影響分析が必要ではなく緊急時対応計画コーディネーターはアプローチを変更して、システムと緊急時対応計画のニーズに適合させることができる。

・ 緊急時対応計画コーディネーターは、自組織が依存するまたは、ITシステムをサポートする方法を特定するシステムに関連する内外の連絡担当窓口（POC; Point of Contact）を特定し、調整を行う。連絡窓口を特定する際には、システムからのデータをやり取りする組織だけでなく、相互接続するあらゆるシステムをサポートする要員も含めることが重要である。[7]この協議によってシステムマネージャは、セキュリティ、管理、技術、運用の面からの要件を含む、システムが提供するサポートの全範囲を把握することができる。

・ 緊急時対応計画コーディネーターは、システムを評価して、重要なサービスをシステムリソースにリンクさせる。この分析では通常、電力、テレコミュニケーション接続、環境上の条件など、インフラストラクチャ要件を特定する。ルーター、アプリケーションサーバー、認証サーバーなどの特定のIT装置は、通常は重要であると認識される。しかし、分析によってプリンタやプリンタサーバーなどのITコンポーネントが、重要サービスのサポートには必要ではないと判断されることもある。

3.2.2 中断の影響と停止許容時間の判定

このステップでは、緊急時対応計画コーディネーターが前ステップで特定された重要リソースを分析し、該当リソースに障害が発生または中断された場合にITオペレーションへの影響を判定する。この分析は、中断による影響を2つの方法で評価する。

・ 中断による影響を、経過時間で追跡する。これによって、緊急時対応計画コーディネーターは、基本的な機能の実行が妨害または禁止される前に、リソースが拒絶される最大許容時間を判定できる。

・ 中断による影響を、関連リソースおよび依存するシステムを横断的に追跡し、障害が発生したシステムに依存する他のプロセスに影響が及ぶことによる、連鎖的な影響を特定する。

緊急時対応計画コーディネーターは、システム運用中断によるコストとシステム復旧に要求されるリソースのコストを対比して、IT システムを復旧する最良のポイントを判定する。[8] これは、図 3-3 に示すような簡単な表を利用して表現できる。2 本の線が交わる点が、組織がシステムの障害発生状態を許容できる期間を示す。

---

[7] 相互接続システムは、一つ以上の情報システムに直接接続し、データおよびその他の情報リソースを共有する。これらのシステムは、同じ組織内または関連機関が所有または運用する。

[8] 第 3.4 項「回復戦略の作成」では、各種の回復リソースおよび関連コストについて説明する。

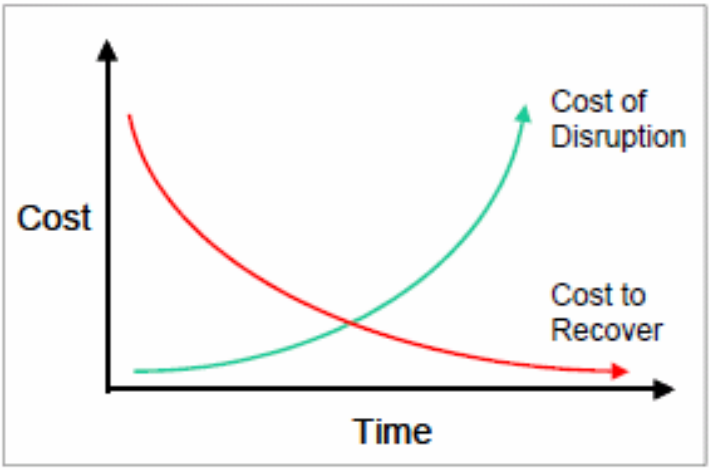


図3-3 復旧コストの調整

3.2.3 復旧優先度の決定

前ステップで規定した中断による影響と許容中断時間によって、緊急時対応計画コーディネーターは、担当者が緊急時対応計画活動中に導入する復旧戦略を策定して優先度付けできる。[9]たとえば、中断による影響を判定するステップでシステムが4時間以内に復旧すべきであることが判明すると、緊急時対応計画コーディネーターはその要求に応えるための対策を講じる必要がある。同様に、大部分のシステムコンポーネントが24時間の中断を許容しても、重要なコンポーネントの中断許容時間が8時間までの場合、緊急時対応計画コーディネーターは重要コンポーネントに必要なリソースを優先させる。これらの復旧戦略を優先度付けすることで、緊急時対応計画コーディネーターはより多くの情報を取得し、緊急時対応リソース割り当てと支出に関して適切な決定を下すことができ、時間と労力やコストを削減できる。

3.3 予防対策の特定

第3.2項で述べたように、事業影響分析は、緊急時対応計画コーディネーターに対し、システム可用性と復旧要件についての重要な情報を提供する。場合によっては、事業影響分析で特定された機能中断は、システムへの影響を抑制、検知または削減する予防対策によって低減または除去できることがある。実現可能で費用対効果が高い場合、それらの予防手段は災害発生からシステムを復旧するための活動として望ましい。システムの種類および構成によって利用できる予防対策は多様だが、以下に共通する対策を挙げる。

---

[9] 回復戦略には、第 3.3 項で述べた予防対策と、第 3.4 項で述べる回復手法および技術を組み合わせて盛り込むことができる。

・ すべてのシステムコンポーネント（システムおよび安全性制御を含む）に短期のバックアップ電力を供給する適正なサイズの無停電電源装置（UPS）の設置

・ ガソリンまたはディーゼル発電による長期バックアップ電力の提供

・ 特定コンポーネントの障害を許容するのに十分な余剰能力を備える空調システム（コンプレッサなど）

・ 防火システム

・ 火災および煙検知器

・ コンピュータルームの天井および床への水センサーの設置

・ 水害防止のためにIT装置に巻くビニールテープ

・ バックアップメディアおよび、重要な電子媒体以外の記録物を保管する耐火性および耐水性のコンテナ

・ 緊急時のマスターシステムシャットダウンスイッチ

・ バックアップメディア、電子媒体以外の記録物、システムマニュアルのオフサイト保管

・ 暗号鍵管理などの技術的なセキュリティコントロールや最小権限によるアクセスコントロール

・ 頻度の高い定期的なバックアップ

予防対策は緊急時対応計画の中で文書化し、システムの関連要員は予防策をいつどのように使用するか、訓練を受ける必要がある。これらの予防策を、緊急時において効果を発揮させるため、適切な状態に維持する必要がある。

3.4 復旧戦略の策定

復旧戦略では、ITオペレーションをサービス障害から迅速かつ効果的に復旧させる手段を規定する。戦略では、障害による影響と、事業影響分析で特定された許容中断時間を扱う。戦略を策定する際には、コスト、許容中断時間、セキュリティ、より大規模な組織レベルの緊急時対応計画を含む複数の代替案を検討する。

選択された復旧戦略は事業影響分析で特定された潜在的な影響を取り扱い、システムライフサイクルの設計および導入フェーズで、システムアーキテクチャに統合される。戦略にはインシデント全般を相互に復旧するために、いくつかの手法を組み合わせて取り入れる。多様な復旧アプローチが検討対象となり、インシデント、システムの種類、運用要件によって、選択される適切なアプローチは異なる。[10] 第3.4.2項で述べる具体的な復旧手法には、コールド/ウォーム/ホットサイト各ベンダーとの商用契約を含む、モバイルサイト、ミラーリングサイト、内部/外部組織との相互契約、装置ベンダーとのサービスレベル保証契約（SLAs）などが考えられる。さらに、システム復旧戦略を策定する際には、RAID（Redundant Arrays of Independent Disk）、自動フェイルオーバー、無停電電源装置（UPS）、ミラーリングシステムなどの技術を考慮する。

3.4.1 バックアップ手法

システムのデータは、定期的にバックアップしなければならない。ポリシーに、データの重要性と新しい情報が導入される頻度に基づくバックアップの頻度を指定する（毎日または毎週、差分のみ、または完全に）。データバックアップポリシーでは、保存したデータの場所、ファイルの命名規約、メディアローテーションの頻度、データをオフサイトに転送する手段を指定する。データは、磁気ディスク、テープ、光学的ディスク（コンパクトディスクなど）にバックアップされる。バックアップ実施に選択される手段は、システムおよびデータの可用性と完全性の要件に基づく。これらの手段には、電子書庫、ミラーリングディスク（DASDまたはRAIDを使用）[11]、フロッピーディスクがある。

バックアップデータをオフサイトに保存する方法も、実用的な手段である。商用データストレージ施設は、メディアを保管し、脅威となる要素からデータを保護するように特化して設計されている。オフサイトのストレージを使用する場合には、データは組織の施設でバックアップを行い、ラベリング、パッケージされ、ストレージ施設へ転送する。データが復旧またはテストのために必要な場合、組織はストレージ施設に連絡し、特定のデータを組織または代替施設に転送するよう要請する。[12] 商用ス

---

[10] 第 5 項「IT システムに固有の緊急時対応計画の検討事項」では、特定の IT システムに適用される回復手段について詳しく説明する。

[11] DASD および RAID については、第 5 項で説明する。

[12] バックアップテープは定期的にテストを行い、データが正しく保存されていて、データのエラーや消失がなくフ

トレージ施設では、メディア転送、対応/復旧サービスを提供することが多い。

オフサイトストレージ施設およびベンダーの選択にあたっては、次の条件を考慮する。

- **立地** - 組織からの距離、ストレージサイトが組織と同じ災害の被害を受ける確率。

- **アクセシビリティ** - ストレージからデータを取得するために必要な時間、ストレージ施設の運営時間帯。

- **セキュリティ** - ストレージ施設のセキュリティ機能と、データの機密性および、セキュリティ要件に見合った従業員の（機密保持にかかわる）信頼性。

- **環境** - ストレージ施設の構造上および環境上の条件。
（温度、湿度、防火体制、電源管理など）

- **コスト** - 発送、運用料金、災害対応/復旧サービスのコスト。

3.4.2 代替サイト

長期にわたって対策が必要な大規模災害は稀であるが、緊急時対応計画では考慮する必要がある。したがって、計画には、長期にわたる代替施設でのシステム運用の復旧と実行のための戦略を含める必要がある。一般には、代替サイトには3種類ある。

- 組織が所有または運営する、専用サイト

- 内部または外部の組織との相互契約または覚書

- 賃貸による商用施設

選択した代替サイトの種類に関わらず、施設は緊急時対応計画に定められたようにシステム運用をサポートできなければならない。3種類の代替サイトは、どの程度迅速に運用できるかによって分類できる。この要因に基づき、サイトはコールドサイト、ウォームサイト、ホットサイト、モバイルサイト、ミラーサイトに分類される。以下に、サイトを基本的なものから高度なものの順に説明する。

- **コールドサイト** 通常は、ITシステムをサポートするために十分なスペースとインフラストラクチャ

ァイルを取り出すことができることを確認する。また、緊急時対応計画コーディネーターは、あてはまる場合は、代替サイトが、組織の導入時と同様のバックアップ構成によってサポートすることを確認する。

(電力、テレコミュニケーション接続、環境制御) を備えた施設からなる。スペースには床上げなど、IT運用に適した特性がある。サイトにはIT機器がなく、通常は電話、ファックス、コピー機などのオフィスオートメーション機器が装備されていない。コールドサイトを使用する組織は、必要となる装置とテレコミュニケーション機能を備え、提供する責任を負う。

- **ウォームサイト** システムハードウェア、ソフトウェア、テレコミュニケーションや電源の全て、またはそのうちどれかを装備した、部分的に設備が整えられたオフィス空間である。ウォームサイトは、移設されたシステムを受け入れるため、運用状態で維持できるよう準備されている。このサイトは、システムおよび復旧要員を受け入れる前に準備されている必要がある。多くの場合、ウォームサイトは別のシステムまたは機能の通常の運用施設として使用され、緊急時対応計画が実行された場合には通常の業務は一時的に移転され、障害の起きたシステムを収容する。

- **ホットサイト** システム要件のサポートに適したサイズで、必要なシステムハードウェア、サポートするインフラストラクチャ、サポート要員を備えたオフィス空間である。ホットサイトは通常、年中無休でスタッフが常駐している。ホットサイト要員は、緊急時対応計画の実行が通知され次第、システムの使用準備を開始する。

- **モバイルサイト** 自給型の移動可能な設備で、システム要件に必要な特定のテレコミュニケーションおよびIT機器が特別にしつらえられたものである。、商用ベンダーからリースすることができる。施設はトラクタトレーラに搭載されていることが多く、運転して目的の代替地点に設置できる。大抵の場合、復旧ソリューションとして機能させるには、モバイルサイトはベンダーによって事前に設計しておく必要があり、SLAを両者間で締結しておく。これは、モバイルサイトの構築するには時間がかかるためで、事前に協議しておかなければ、モバイルサイトを導入するまでの時間が、システムの許容中断時間を超過してしまうためである。

- **ミラーサイト** リアルタイムで情報を完全にミラーリングする、完全冗長性を持つ施設である。ミラーサイトは、すべての技術的観点において、プライマリサイトと同一である。この類のサイトでは、データは、プライマリサイトと代替サイトで同時に処理され、保存される最高レベルの可用性を提供する。このサイトは通常、組織によって設計、構築、運用および、保守が行われる。

これら5つの選択肢には、コストと準備時間に明白な差がある。ミラーサイトは最もコストがかかる選択だが、実質的に100%の可用性が確保される。コールドサイトは保守に最もコストがかからないが、必要な装置の取得とインストールにそれなりの時間が必要になる。ウォームサイトのような、部分的に装備されたサイトは、この両端の間に位置する。多くの場合、モバイルサイトは目的の場所に24時間以内に導入される。しかし、インストールに必要な時間によって、対応時間が増加する。固定サイトを選択した場合、人員をそこまで移動させるのに必要な時間と移送手段について検討する必

要がある。[13] 固定された位置にあるサイトは、組織のプライマリサイトと同様に、災害により被害を受けないような地理的な位置にすべきである（天候による影響または電力網の障害など）。表3-1に、どの種類の代替サイトが組織の要件を満たすか、判定するための基準をまとめる。組織は、事業影響分析で定義した特定の要件に基づいて、サイトをさらに分析する。サイトを評価する際に、緊急時対応計画コーディネーターはシステムのセキュリティ、管理、運用、技術的管理が目的のサイトと両立するか確認する。このような管理には、ファイアウォール、物理的アクセス管理、データ関連の制御、サイトおよびサイトをサポートするスタッフのセキュリティ権限レベルがある。

表3-1 代替サイト選択基準[14]

サイト	コスト	ハードウェア装置	テレコミュニケーション	セットアップ時間	場所
コールドサイト	低	なし	なし	長時間	固定
ウォームサイト	中	部分的	部分的/完全	中	固定
ホットサイト	中/高	完全	完全	短時間	固定
モバイルサイト	高	不定	不定	不定	可動
ミラーサイト	高	完全	完全	なし	固定

これらの代替サイトは、組織が所有して運用することもあるが（内部復旧）、契約によって商用サイトを利用することもできる。商用ベンダーとサイトを契約する場合、適切なテスト期間、作業スペース、セキュリティ要件、ハードウェア要件、テレコミュニケーション要件、サポートサービス、復旧日数（組織が復旧期間に、どれだけスペースを使用できるか）について議論し、契約書に明記する必要がある。顧客は、複数の組織が同じ代替サイトをベンダーと契約しているかもしれないことを認識する：その結果、全顧客が同時に被害を受けた場合、全員をサイトに収容できない場合がある。このような状況にどのように対処し、優先度をどのように決定するかについて、ベンダーのポリシーについて協議する必要がある。

複数の組織が同一または類似のIT構成とバックアップ技術を持っている場合、公式な契約によって互いに代替サイトを提供したり、共同で代替サイトを契約したりすることがある。この種類のサイトは、相互契約または覚え書き（MOU：memorandum of understanding）によって設立される。相互契約は、災害発生時には各サイトが自らの作業のみならず、相互にサポートしなければならないため締結は慎重に行う。 この種類の契約では、双方の組織のアプリケーション復旧手順を両者が満足するように共同の視点で優先度をつけることが要求される。テストはパートナーのサイトで実施し、復旧

---

[13] 2001 年 9 月 11 日のような、広範囲にわたる災害発生時には、道路および橋の通行が封鎖され、航空路が制限されることがある。

[14] 表 3-1 の分析はそれぞれのサイトタイプの条件や、価値との関連を表したものである。

手順の機能性に加え、追加処理のしきい値互換性のあるシステムおよびバックアップ構成、十分なテレコミュニケーション接続、互換性のあるセキュリティ対策、他の権限のあるユーザーがアクセス可能なデータの機密性を評価する。

組織のニーズとパートナー組織の能力に適した代替サイトの覚え書き、契約（MOA：memorandum of agreement）、またはSLAを作成する。双方の法務部門が契約内容を確認して承認する。一般に、契約には最低でも次の要素を扱う。

- 契約／同意の期間
- 災害発生宣言および占有のコスト/料金構造（日割り）、管理、保守、テスト、年間コスト/料金増加、移送サポートコスト（オフサイトデータまたは供給品の受理と返却など、該当するもの）、コスト/経費割り当て（該当する場合）、請求および支払いスケジュール
- 災害の宣言（災害を規定する条件、通知手順など）
- サイト/施設のアクセスまたは利用の優先度
- サイトの可用性
- サイトの保証
- 同じリソースおよびサイトを契約しているする他のクライアント、およびサイトを利用するクライアントの総数（該当する場合）
- 契約／同意の変更または修正のプロセス
- 契約／同意の終了条件
- サービス拡張交渉のプロセス
- 互換性の保証
- ハードウェア、ソフトウェア、および任意の特殊なシステムのニーズ（ハードウェアおよびソフトウェア）のITシステム要件（データおよびテレコミュニケーション要件を含む）

- ハードウェア、ソフトウェア、インフラストラクチャを含む、変更管理および通知要件
- 特別なセキュリティニーズを含む、セキュリティ要件
- 提供される、または提供されないスタッフサポート
- 提供される、または提供されない施設サービス（オンサイトオフィス機器の利用、カフェテリアなど）
- スケジューリング、可用性、テスト経過時間、必要な場合は、追加テストを含むテスト
- 電子媒体およびハードコピーを含む、記録管理（オンサイトおよびオフサイト）
- サービスレベル管理（提供されるITサービスの性能測定、品質管理）
- 作業スペース要件（椅子、デスク、電話、PC）
- 提供される、または提供されない供給品（オフィスサプライ）
- その他、当該契約に含まれないコスト
- その他の契約条項（該当する場合）
- その他の技術的要件（該当する場合）

3.4.3 機器交換

ITシステムが破損または中断されたり、プライマリサイトが利用できなくなった場合、必要なハードウェアとソフトウェアを迅速に代替拠点に搬送し、復旧する必要がある。機器交換の準備には、次のような3つの基本的な対策がある。最適な戦略を選択する際には、壊滅的な災害時における移送が制限されたり一時的に不可能になる場合があることに留意する。

- **ベンダー契約**　緊急時対応計画を策定時には、緊急保守サービスに備え、ハードウェア、ソフトウェア、サポートベンダーとのSLAを締結する。SLAでは、通知後にベンダーがどの程度迅速に対応できるかを特記する。契約には、通常業務用に購入された機器に対する交換用機器の搬送の優先度状態も記載する。SLAには、壊滅的な災害によってベンダーの複数のクライアント

が被害を受けた場合の、組織における優先度についても記載する。このような場合、医療または安全性に関連するプロセスを持つ企業は、機器が配送される優先度が高くなることが多い。これらの折衝の詳細はSLAに記載し、緊急時対応計画とともに保持する。

- **機器インベントリ** 要求される機器は事前に購入して、復旧操作を実施する代替サイト（ウォームサイトまたはモバイルサイト）などの安全なオフサイト拠点に保管するか、一度別の拠点に保管してそこから代替サイトへ搬送する。しかし、このソリューションには欠点がある。組織はこの機器を事前に購入する財源を確保する必要があり[15]、システム技術と要件の変更に伴い、機器が旧式になったり利用に適さなくなったりすることがあるからだ。

- **既存の互換機器** 現在、契約したホットサイトまたは、政府機関の別の組織により使用されている機器が政府機関によって使用されることがある。ホットサイトおよび補完関係にある内部サイトとの契約では、同様の互換性のある機器は、組織によって緊急時対応として利用できることを明記する。

機器交換の選択肢を評価する際、緊急時対応計画コーディネーターは、機器が必要になった時点で購入することが費用対効果が高いが配送とセットアップで時間がかかるといったことを考慮すべきである。逆に、使用しない機器を保管するのはコストがかかるが、復旧操作を速やかに開始することができるということもありうる。また、事業影響分析で特定された影響に基づき、大量の機器交換が必要になるような広範囲の災害の可能性や、配送の遅れによって復旧期間が長引く恐れがあることにも留意する必要がある。どの対策を選択した場合でも機器の詳細リストは必要で、詳細は緊急時対応計画の中でも維持する。機器リストの文書化については、第4.1項「サポート情報」でさらに説明する。

3.4.4 役割と責任

システム復旧戦略を選択して導入した後、緊急時対応計画コーディネーターが、適切なチームを編成して戦略を導入する必要がある。各チームは、計画の実効性が求められる災害発生時に備えて、対応できるように訓練される必要がある。また、復旧担当者を、緊急事態に対応してサービス提供能力を復旧しシステムを通常運用状態に戻す特定のチームのうち1つに割り当てる。そのためには、復旧担当者が、復旧作業におけるチームの目標、実行する各ステップを把握し、いかに自らのチームと他のチームが関わっているかを明確に理解しておかなければならない。

必要なチームの種類は、影響を受けるシステムによって異なる。各チームの規模、チームの役職、

---

[15] 撤去された装置は、予備またはバックアップ用ハードウェアとして利用できる場合がある。この対策により、総設備交換コストを削減できる。

階層構造は、組織に依存する。優れた対策を立てるためには、全体的な意思決定責任にかかわる単独の権限的役割を定める以外にも、以下の機能を持つグループの一部、またはすべてを定める必要がある。

- 上級経営幹部
- 経営チーム
- 損害評価チーム
- オペレーティングシステム管理チーム
- システムソフトウェアチーム
- サーバー復旧チーム（クライアントサーバー、Webサーバーなど）
- LAN/WAN復旧チーム
- データベース復旧チーム
- ネットワーク運用復旧チーム
- アプリケーション復旧チーム
- テレコミュニケーションチーム
- ハードウェア復旧チーム
- 代替サイト復旧調整チーム
- 現サイト復旧/回収調整チーム
- テストチーム
- 運営サポートチーム

・ 移送および移転チーム

・ メディア対応チーム

・ 法務チーム

・ 物理的/人的安全確保チーム

・ 調達チーム（機器および供給品）

これらのチームには、スキルと知識をもとに人員を配置する。理想的には、チームには通常業務においても同一または同様の職務を行う人員を配置するのが望ましい。たとえば、サーバー復旧チームのメンバーには、サーバー管理者を含めることなどである。チームのメンバーは、緊急時対応計画の目的のみでなく、復旧戦略の実施に必要な手順も理解する必要がある。チームは、メンバーの誰かが対応できなかったり、代替チームメンバーが指名された場合でも対処可能であるような規模で編成する。 同様に、チームメンバーはチーム間の連携を促進するため、他のチームの目標と手順に精通していなければならない。緊急時対応計画コーディネーターは、要員の大多数または全員が対応できなくなるような災害が発生することも考慮しておく。このような状況では、組織の別地域の要員のみの活用または、請負業者またはベンダーの雇用によって、計画の実現が可能となることがある。このような人員は、代替チームとして調整し訓練される。

各チームはチームリーダーによって指揮される。リーダーはチームの作業全体を指揮し、経営陣に対するチームの代表者となり、他のチームリーダーの窓口となる。チームリーダーは、チームメンバーに情報を行き渡らせ、チーム内で必要な決定を承認する。チームリーダーは、第一リーダーが対応できない場合にリーダーとなる代替リーダーを指名しておく。

ほとんどのシステムでは、大規模なシステム障害または緊急事態に対するガイダンス全般を提供する経営チームが必要である。チームは、緊急時対応計画を実行する責任を持ち、緊急時対応策の運用を監視する。他のチームとのコミュニケーションを促進し、緊急時対応計画のテストと演習を監督する。また、経営チーム全体または一部が特殊なIT緊急時対応チームを指揮することがある。一般的には、経営チームを先導するCIOのような経営幹部は、計画を実行する最終権限を持ち、支出レベル、許容できるリスク、および連邦政府省庁間の調整に関する判断を行う。

後継者計画は通常運用継続計画の範囲であるが、IT緊急時対応計画に含めることもできる。後継者計画では、最高権威（通常はCIO以上）が対応できない場合、誰が緊急時対応計画の実行を担当するかを定義する。たとえば、CIOが負傷または死亡した場合、CIO代理が計画の責任を持ち、

CIOとCIO代理が負傷または死亡した場合、情報システムセキュリティマネージャが計画の責任を持つ。後継者は、組織のニーズに従って必要なレベルにまで下るが、運用継続計画と慎重に調整を行い、責任に矛盾が生じないようにする。

3.4.5 コストの考慮事項

緊急時対応コーディネーターは、選択した戦略が対処可能な要員と利用可能な予算枠で、効果的に導入されることを確認する必要がある。検討下におかれる代替サイトの種類、機器交換、ストレージオプションのコストを、予算上の制限と照らし合わせ比較する。[16] コーディネーターは、代替サイト契約料などの既知の緊急時対応計画の経費、政府機関全体への緊急時に対応する意識向上プログラム、および請負業者サポートの導入コストなど、あまり明確ではない経費も判断しなければならない。当該予算には、ソフトウェア、ハードウェア、移動と配送、テスト、計画訓練プログラム、意識向上プログラム、作業時間、その他の契約サービス、およびその他の該当するリソース（デスク、電話、ファックス、ペン、紙など）を含めた、十分な予算が必要である。連邦政府は、費用対効果分析を実行し、最適な復旧戦略を特定する。表3-2に、コストの考慮事項を評価するためのテンプレートを示す。

表3-2 復旧戦略の予算計画テンプレート

		ベンダーコスト	ハードウェアコスト	ソフトウェアコスト	移動/配送コスト	人件費/外注費	テストコスト	供給品コスト
代替サイト	コールドサイト							
	ウォームサイト							
	ホットサイト							
	モバイルサイト							
	ミラーサイト							
オフサイトストレージ	商用							
	内部							
機器交換	SLA							
	ストレージ							
	既存機器の利用							

[16] 可能な場合は、技術的回復手法のコストと利益を、システム作成中に評価する。

3.5 テスト、訓練、演習の計画

テストの計画は、緊急時対応能力を実行可能なものとするのに重要な要素である。テストを行うことによって、計画の欠点が明確になり、対処できるようになる。また、復旧担当者が計画を迅速かつ効果的に導入する能力を検証することもできる。さらに、IT緊急時対応計画の各要素をテストし、それぞれの復旧手順の正確さと計画全体の効果を確認する必要もある。緊急時対応テストで検証されるべき領域は、以下である。

- 代替プラットフォームでのバックアップメディアからのシステム復旧
- 復旧チーム間の共同作業
- 内部および外部との接続性
- 代替装置の使用によるシステム性能
- 通常業務の復旧
- 通知手順

テストで得られる効果を最大化するために、緊急時対応計画コーディネーターは明確なテスト目標と合格基準に対して選択した要素をテストするよう設計された計画を策定する必要がある。テスト目標と合格基準を使用することで、各計画要素と計画全体の効果が評価できる。テスト計画には、各テストとテスト参加者に対する詳細な時間枠を定めたスケジュールを含める。また、テスト計画では範囲、シナリオ、後方支援を明確に記述する。シナリオには最悪のインシデント、または最も発生する確率が高いインシデントを選択することができる。また、可能な限り現実に近い状態を想定する。演習には、2つの基本的なスタイルがある。

- **クラスルーム演習**　クラスルーム演習はテーブルトップとも呼ばれ、参加者は実際の復旧手順を実行せずに、手順を確認していく。クラスルーム演習は後述の機能演習よりも基本的かつ低コストであり、機能演習を実行する前に実施される。

- **機能演習**　機能演習は、テーブルトップよりも広範囲で、模擬的なイベントが必要になる。機能演習には、シミュレーションとウォーゲームが含まれる。また、組織の外部契約業者の役をする参加者向けにスクリプトを作成したり、実際の連邦政府内またはベンダーの参加者が加わることもあれば、代替サイトに実際に移動してシステムの切り替えを行うこともある。

事前にテストについて通知することには、チームメンバーが心理的に準備を整え、作業負荷の優先順位を決定できるという利点がある。チームメンバーが休暇中または作業が忙しくて参加できない場合も考えられる。要員の参加可能性は、実際の対応状況の把握に役立ち、計画の修正に重要な情報となる。重要なことは、演習が通常業務の妨げとなってはならないということである。代替施設でテストする場合、緊急時対応計画コーディネーターは、テスト実施日と演習について施設との調整を行う。[17] 得られたテスト結果と学習した事柄を文書化し、適宜、テスト参加者およびその他の担当者を含めてレビューする。また、テスト中に収集された情報、およびテスト後のレビューで得られた情報のうち計画の効率改善に役立つものは、緊急時対応計画に取り入れる必要がある。

緊急時対応計画を担当する人員を訓練して、テストを補完する。訓練は最低年1回実施し、計画の責務を負う新たな担当者は、任命後まもなく訓練を受ける。最終的には、緊急時対応計画担当者は訓練によって、各自の復旧手順を実際のマニュアルがなくても実行できるレベルに達するまでトレーニングが行われるようにする。これは、災害発生後の数時間、紙または電子媒体での計画が入手できない事態に備えるための、重要な目標である[18]。復旧担当者は、次の計画要素に対して訓練を受ける。

- 計画の目的
- チーム間の共同作業およびコミュニケーション
- 報告手順
- セキュリティ要件
- チーム固有のプロセス（通知/実行、復旧、再構築フェーズ）
- 各自の責任（通知/実行、復旧、再構築フェーズ）

---

[17] テスト時間と演習サポートを、契約内容に取り入れることができる。これについては、第3.4.2項「代替サイト」でも説明した。

[18] この状況は、ローカルコピーが破損したり、入手できない場合で、回復手順が開始された後にオフサイト計画を受け取った場合にも当てはまる。

3.6 計画の保守

計画を効果的なものとにするには、システム要件、手順、組織構造、ポリシーを正確に反映しすぐに使用できる状態で整備する必要がある。ビジネスニーズの変化、テクノロジーの進化、内部/外部の新しいポリシーによって、ITシステムには頻繁に変更が加えられる。このため、組織の変更管理プロセスの一部として、緊急時対応計画を定期的にレビューして更新し、新しい情報の文書化を行い、緊急時対応計画が必要に応じて改定されるようにすることが肝心である。一般的には、計画の正確性と完全性を確保するため、最低年1回または、計画の要素に重大な変化が発生したときに随時レビューを行う。連絡先リストなど、より頻繁にレビューが必要な要素もある。システムの種類と重要度を考慮すると、計画内容と手順を頻繁に評価することが望ましい場合もある。最低でも、計画のレビューでは、以下の要素に重点を置く必要がある。

- 運用要件
- セキュリティ要件
- 技術的手続き
- ハードウェア、ソフトウェア、その他の装置（種類、仕様、数量）
- チームメンバーの氏名および連絡先情報
- 代替サイトおよびオフサイトベンダーの連絡担当窓口を含めた、ベンダーの名称および連絡先情報
- 代替施設およびオフサイト施設の要件
- 重要な記録（電子媒体およびハードコピー）

IT緊急時対応計画には、基本的に機密な運用情報および人事情報が含まれることがあるため、計画の配布は記録して管理する必要がある。通常、計画のコピーが復旧担当者に提供され、自宅またはオフィスで保管される。コピーは代替サイトでバックアップ媒体に保管される。代替サイトでの計画コピーは、計画のローカルコピーが災害のためにアクセスできない場合にも、利用できる状態で保管する。緊急時対応計画コーディネーターは、計画コピーの記録と、その配布先を維持する。計画とともに保管すべきその他の情報として、ベンダーとの契約（SLAなどの契約）、ソフトウェアライセンス、システムユーザーマニュアル、セキュリティマニュアル、運用手順などがある。

計画、戦略、ポリシーへの変更内容は、緊急時対応計画コーディネーターを通じて調整され、コーディネーターは必要に応じ、変更に関係する計画またはプログラムの担当者に変更箇所を通知する。緊急時対応計画コーディネーターは、計画の変更をページ番号、変更コメント、変更日を記入する変更履歴に記録する。表3-3に示す変更履歴は、第4.1項で述べるように、計画に取り込む必要がある。

表3-3 変更履歴の例

変更履歴			
ページ番号	**変更コメント**	**変更日**	**署名**

緊急時対応計画コーディネーターは、関係する内部/外部の組織およびシステムの連絡担当窓口と頻繁に調整を行い、変更による効果がどの政府機関の緊急時対応計画においても反映されるようにする。厳密なバージョン管理を導入し、旧版の計画またはページを緊急時対応計画コーディネーターに差し戻し、新しい計画またはページに交換するよう依頼する。

緊急時対応計画コーディネーターは、サポート情報を評価して、情報が現状に即しており、システム要件に継続して適切に合致することを確認する。この情報には、次の事項が含まれる。

・ テスト時間を含む、代替サイト契約

・ オフサイトストレージ契約

・ ソフトウェアライセンス

・ 覚え書きまたはベンダーSLA

・ ハードウェアおよびソフトウェア要件

・ システム相互接続契約

・ セキュリティ要件

・ 復旧戦略

・ 緊急時対応ポリシー

・ 訓練および意識向上のための資料

・ テストの目的

変更には明確なものもあるが、追加分析が必要なものもある。事業影響分析を定期的にレビューして新しい情報で更新し、新しい緊急時対応要件および優先度を特定する。新しい技術が利用できるようになると、予防対策を増強したり、復旧戦略を修正したりすることもある。さらに、NIST SP 800-26『ITシステムのためのセキュリティ自己アセスメントガイド（Security Self-Assessment for Information Technology Systems）』[19]では、緊急時対応計画の要素の実行可能性を判定するためのチェックリストを提供している。

4. IT緊急時対応計画策定

本項では、緊急時対応計画を構成する主要な要素について説明する。第3項で述べたように、IT緊急時対応計画の策定は、包括的な緊急時対応計画プログラムを導入するプロセスにおいて、重要なステップである。緊急時対応計画には、災害発生後にITシステムを復旧するための詳細な役割、責任、チーム、手順が含まれる。緊急時対応計画では、緊急時の対策をサポートする技術的能力について文書化する。また、緊急時対応計画は、組織とその要件に適合するように策定される。さらに、計画の詳細度と柔軟性のバランスをとる必要がある。通常、計画が詳細になるとそのアプローチの拡張性と柔軟性は低くなる。ここで述べる情報はガイダンスの意味を持つが、本書での計画フォーマットを必要に応じて修正し、利用者固有のシステム、運用、および組織の要件に適合するよう改善することができる。付録Aでは、組織がそれぞれのシステムに対するIT緊急時対応計画策定に使用できるテンプレートを示す。付録Dは、IT緊急時対応計画策定において調整する必要がある要員計画に関する考慮事項を取り上げる。

---

[19] この表は、NIST SP 800-26、第 4.2.4 項「緊急時対応計画（Contingency Planning）」に掲載されているが、、http://csrc.nist.gov からでも入手可能である。

図4-1に示すように、このガイドでは緊急時対応計画の5つの主要コンポーネントを特定している。「サポート情報」と「計画の付録」コンポーネントは、計画を包括的なものとするために必要かつ基本的な情報を提供する。「通知/実行フェーズ」、「復旧フェーズ」、「再構築フェーズ」では、システム障害または緊急事態の発生後に組織がとるべき具体的な行動を扱う。各計画コンポーネントについては、この項で後述する。

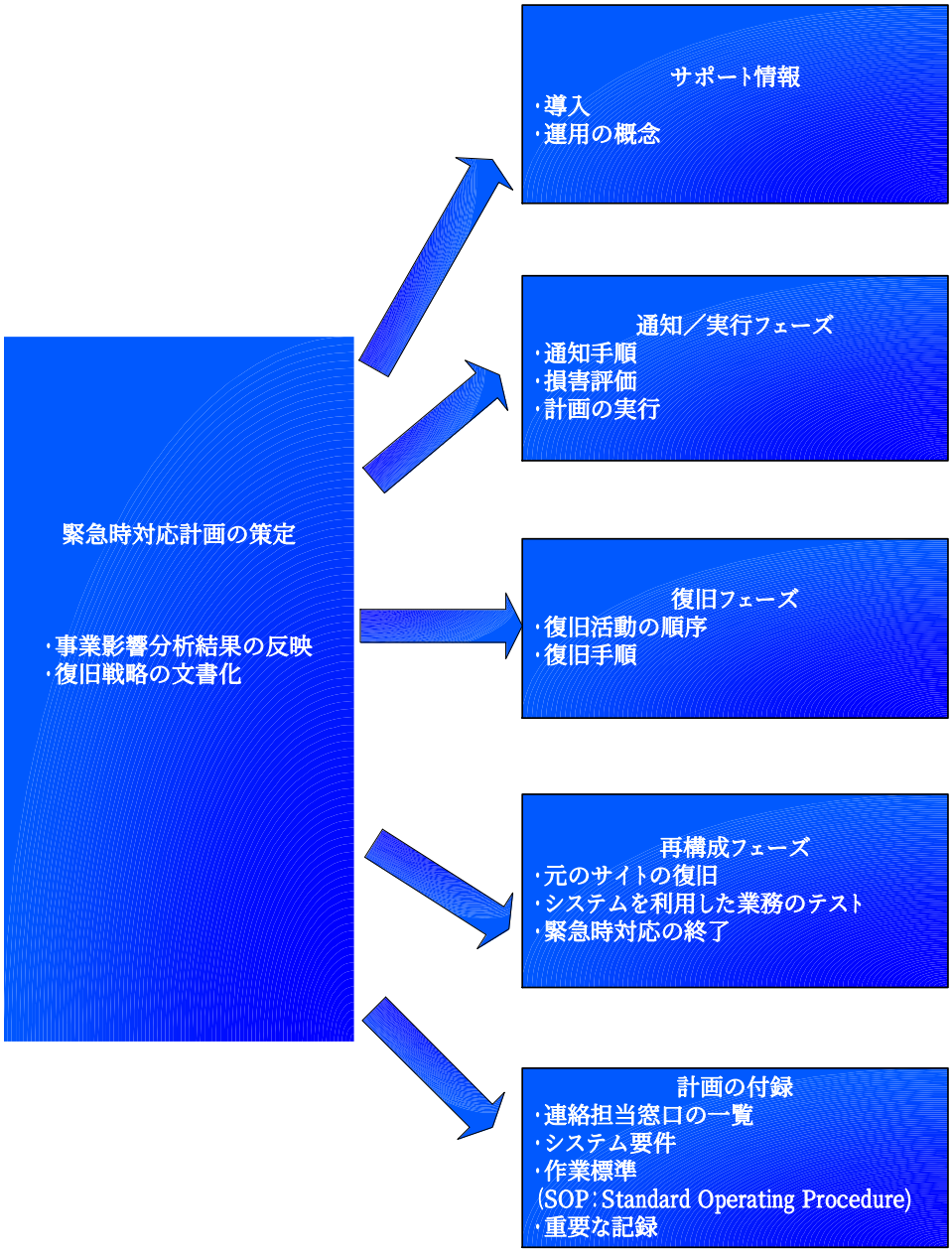


図4-1 緊急時対応計画の構造

緊急時対応計画では、計画やシステムに精通していない要員が復旧操作を実行する必要が出てきた場合においても、迅速に迷わず実施できるように記述する必要がある。このため、計画は、緊急時の実行に即し、明確で簡潔、容易でなければならない。可能な場合は、チェックリストおよびステップごとの手順を使用する。簡潔かつ整然とした様式を使用することで、計画が必要以上に複雑で混乱を招くものになる危険性を低減することができる。

4.1 サポート情報

サポート情報コンポーネントには、導入と運用の概念に関する項を含める。ここでは、緊急時対応計画の理解、導入、維持を容易にするための重要な背景情報および状況に関する情報を提供する。このような詳細情報によって、ガイドの適用可能性についての理解、計画をどのように使用するかの判断や関連する計画と計画範囲外の情報が入手できそうな情報提供箇所などのガイダンス適用可能性を理解する手助けとなる。

序章では、計画に含まれる情報の種類と場所を読者に示す。一般に、この項目には、目的、適用可能性、範囲、参考資料/要件、変更記録が含まれる。[20] これらの小項目について以下に述べる。

- **目的** この小項目は、IT緊急時対応計画を策定する理由を明記し、計画の目的を定義する。

- **適用可能性** ここでは、IT緊急時対応計画によって影響を受ける組織を文書化する。IT緊急時対応計画をサポートする関連計画、またはサポートされるすべての関連計画を特定し、その関連性を記述する。これらの関連計画は、緊急時対応計画の付録として包含する。

- **範囲** 範囲では、計画で対処する問題または対処しない問題、状況、条件について説明する。この項では、対象となるシステムおよび、システムが複数の拠点に分散している場合に、緊急時対応計画に含まれる地域を特定する。たとえば、4時間以内の短期障害については対処しない、またはIT施設が破壊されるような壊滅的な事態には対処しない、などがある。
  範囲では、すべての主要要員が緊急時に対応できるといった条件での、緊急時対応計画に関するあらゆる仮定を想定する。ただし、仮定を完全な計画と取り違えてはいけない。たとえば、緊急時対応計画では、災害が営業時間内にのみ発生すると仮定してはいけない。このような仮定に基づいて緊急時対応計画を策定すると、営業時間外に災害が発生した場合、緊急時対応計画コーディネーターは効果的にシステムを復旧できないことがある。

---

[20] 前述したように、この計画の構成は、緊急時対応計画の作成者へのガイダンスの意味を持つ。要員各位は、必要に応じて、システムおよび組織の緊急時対応計画要件に適するように、このフォーマットを追加、削除、修正することができる。

・ **参考資料/要件** この小項目では、緊急時対応計画に関する連邦政府の要件を特定する。適用する連邦政府のドキュメントには、本ガイドの第1.3項で挙げたドキュメントが含まれる。

・ **変更履歴** 緊急時対応計画は、実態に即したドキュメントでなければならず、システム、運用、組織の変更を反映するため、必要に応じて変更される。計画への修正は、計画の先頭部分にある変更履歴に記録する。[21]

運用概念の項では、ITシステムの詳細を記述し、緊急時対応計画フレームワークである、対応、復旧、再開活動を規定する。この項には、以下の要素を含めることができる。

・ **システム詳細** 緊急時対応計画に含まれるITシステムの一般的な情報を含めることが必要である。情報には、ITシステムアーキテクチャ、設置場所、そのほかの技術的に重要な考慮事項が含まれる。[22] セキュリティデバイス（ファイアウォール、内部/外部接続など）を含むシステムアーキテクチャ図も有効である。システム詳細の内容は、通常システムセキュリティ計画から取得できる。

・ **後継者の指定** 後継者とは、指定された要員が対応することができない場合または、実行することが不可能な場合に、緊急時対応計画を実行する責任者として指定された者のことである。[23]

・ **責任** 責任の項では、チーム間の階層構造と調整メカニズム、要件を含むIT緊急時対応チームの構造全体について示す。また、緊急事態発生時における、チームメンバーの役割および責任についての概要も示す。チームおよびチームメンバーは、緊急時対応計画の実行時に、特定の責任と復旧に関する役割を割り当てられる。この役割は、特定個人ではなくチームでの職位に対して割り当てる。チームメンバーを氏名ではなく役割別にリストすると、割り当てられたメンバーが対応できない場合の混乱を削減するばかりではなく、担当者が交代した場合にドキュメントに加える修正量を減らすことができる。

4.2 通知/実行フェーズ

通知/実行フェーズは、システム中断または緊急事態が検知された場合、または緊迫した状態にある場合に行う初期活動を定義する。このフェーズには、復旧担当者への通知、システム障害の評価、計画の実施などの活動が含まれる。通知/実行フェーズが完了すると復旧スタッフは、緊急事態

---

[21] 変更履歴については、第 3.6 項「計画の整備」で説明している。

[22] NISTSpecial Publication800-18『Guide for Developing Security Plans for Information Technology Systems』（1998 年 12 月）に、システム記述のフォーマットについて、ガイダンスが示されている。

[23] 後継の系列計画は、第 3.4.4 項「役割と責任」でも説明している。

対策の実行の準備をし、一時的にシステム機能を復旧する。

4.2.1 通知手順

イベントは、事前に察知できるものとできないものとがある。たとえば、ハリケーンが影響を及ぼす地域や、コンピュータウイルスなどが特定の日付を指定することは、あらかじめ通知される。しかし、機器の障害や犯罪行為は知ることができない。通知手続きは、両方の状況に関して文書化する必要がある。通知手順は、復旧担当者に、営業時間内または時間外で通知するための手段を記述する。迅速な通知は、ITシステムへの影響を低減するために重要である。場合によっては、システム担当者はハードウェアのクラッシュを回避してシステムを安全にシャットダウンできる余裕が得られる場合もある。このとき災害発生後の通知は、損害評価チームに伝達され、チームは状況を判断し、適切な次の手順を決定できるようにする。損害評価手順については、第4.2.2項で説明する。損害評価が完了すると、適切な復旧チームおよびサポートチームに通知される。

通知は電話、ポケットベル、電子メール（Eメール）、携帯電話を含むさまざまな手段で行うことができる。[24]　電子メール経由の通知は、積極的な応答を受ける保証がないため、注意が必要である。電子メールは職場または個人のアカウントに広く伝達、通知するための効果的な手段であるが、メッセージが必ず読まれるという保証はない。職場の電子メールアカウントには、非常に多くのメッセージが届くため、使用するアカウントを選択することも必要となる。個人の電子メールアカウントは、チェックの頻度が週1回にも満たないことがある。このため、電子メールによる通知手段を用いる場合、復旧担当者は、自分のアカウントを定期的かつ頻繁にチェックすることの必要性が通知されていなければならない。営業時間内に伝達された通知は、職場のアドレスに送信する。一方、個人の電子メールアドレスは、LANがダウンした場合に有効である。広範囲に及ぶ災害時に効果的な通知手段は、ラジオおよびテレビのアナウンス、ウェブサイトなどである。

通知手順には、災害発生後、特定の担当者に連絡が取れない場合の手順を定義する。通知手順は、緊急時対応計画で明確に文書化しておく必要がある。一般的な通知手段は、連絡網である。この方法では、通知義務を特定個人に割り当て、その担当者が責任を持って、他の復旧担当者に通知するものである。連絡網では、第一および代替連絡手段を定め、担当者に連絡できない場合にとる手段を記述する。図4-2に、連絡網の例を示す。

---

[24] 通知手段の組み合わせは、災害直後に殺到する携帯電話または電話サービスを緩和するために、採用されることがある。

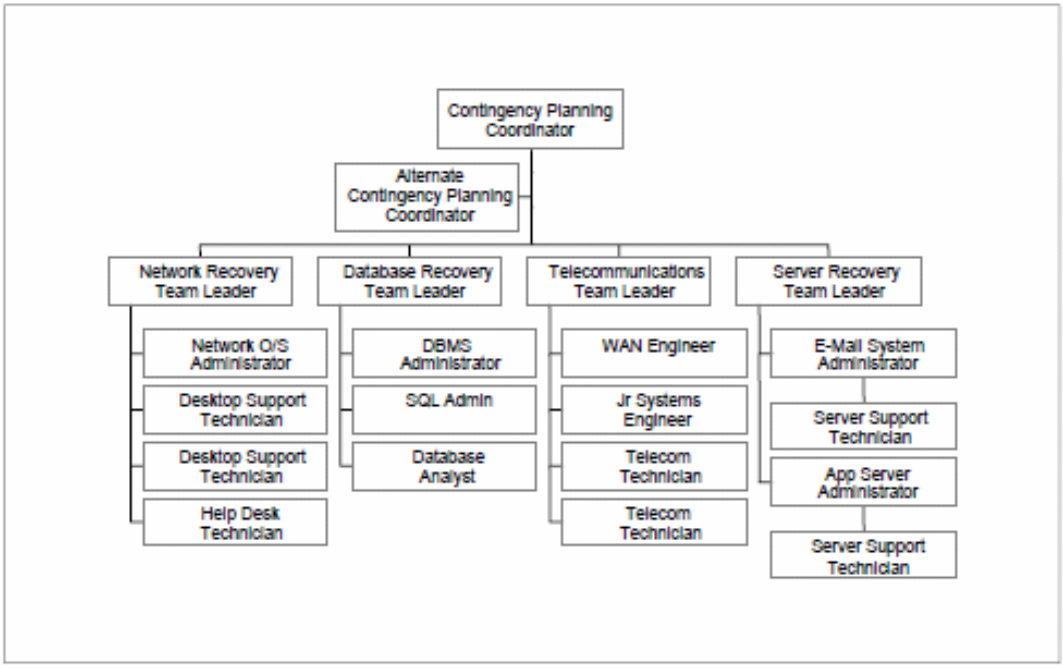


図4-2 連絡網の例

通知すべき担当者は、計画に付属されている連絡先リストに明記する。このリストには、担当者のチーム内での地位、氏名、連絡先情報（自宅、職場、ポケットベルの番号、電子メールアドレス、個人アドレスなど）を記載する。エントリの例は、以下のフォーマットになる。

システムソフトウェアチーム
チームリーダー – プライマリ
Jane Jones
1234 Any Street
Town, State, Zip Code
自宅: (123) 456-7890
職場: (123) 567-8901
携帯電話: (123) 678-9012
電子メール: jones@organization.ext; jones@home.ext

通知は、外部組織またはシステムへ内部接続するパートナーの連絡担当窓口にも送信する。状況を認識していないと、悪影響を受けることがあるためである。障害の種類によっては、連絡担当窓口に復旧の責任が発生する。そのため、外部組織と内部接続を行うシステムは、連絡担当窓口を特定し、規定されるシステム相互接続契約に従い、支援条件の元、組織が相互に支援するものである。

このような連絡担当窓口は、緊急時対応計画の付録にリストする。[25]

通知対象の担当者に伝達される情報の種類を、計画の中に文書化する。伝達される情報の量と詳細度は、通知されるチームによって異なる。通知情報には以下の項が含まれる。

・ 発生または発生の恐れのある緊急事態の種類

・ 生命の危険または傷害

・ 既知の損害の規模

・ 対応および復旧の詳細

・ 状況説明または今後の対応手順を話し合う場所と時期

・ 予想時間内に再配置を準備するための指示

・ 連絡網（ある場合）を使用し、通知を完了するための指示

4.2.2 損害評価

緊急時に緊急時対応計画がどのように導入されるかを判定するためには、システムに対する損害の種類と範囲を評価することが重要である。この損害評価は、人員の安全を最優先としながら、状況が許すかぎり迅速に完了すべきである。そのため、可能な場合は、損害評価チームが最初にインシデントを通知されるチームとなる。損害評価手順は、それぞれのシステムににについて固有のものであるが、次の項目を扱わなければならない。

・ 緊急事態または災害の原因

・ 二次災害または損害の可能性

・ 緊急事態により影響を受ける範囲

---

[25] 通常、連絡先リストには機密情報が含まれるため、注意して適切な方法で記録および、保管を行い、必要とする要員にのみ配布する。リストには日付を記載し、氏名、職位、連絡先情報が最新になるよう頻繁にレビューを行う。

・ 物理的インフラストラクチャの状態（コンピュータ室の構造上の完全性、電力、テレコミュニケーション、暖房、通気、空調の状態[HVAC]）

・ IT機器の品目および機能的な状態（完全機能、一部機能、機能停止など）

・ IT機器およびデータへの損害の種類（水害、火災および熱、物理的影響、電圧の急激な変化など）

・ 交換が必要なアイテム（ハードウェア、ソフトウェア、ファームウェア、サポート機材）

・ 通常業務に復旧するまでの予想時間

損害評価の担当者は、これらの手順を理解し紙媒体での緊急時対応計画が入手できない場合でも実行できるようにしておく必要がある。システムへの影響が判定されると、該当するチームに最新の情報が通知され、状況に対処するよう計画される。通知は、第4.2.1項で説明した手順を使用して実行される。

4.2.3 計画の実行

IT緊急時対応計画は、損害評価によって実行する基準が当該システムに対し1つ以上あてはまると判断された場合にのみ、実行される。実行基準にあてはまると、緊急時対応計画コーディネーターまたはCIO（存在する場合）が計画を実行する。[26]イベントに対する実行基準は各組織に固有で、緊急時対応計画ポリシーステートメントに記述される。基準は、以下の要素に基づく。

・ 人員の安全および、施設に対する損害の範囲

・ システムに対する損害の範囲（物理的、運用上、コスト面など）

・ 組織のミッションに対するシステムの重要性（重要なインフラストラクチャ保護資産など）

・ 障害の推定存続期間

---

[26] 本ドキュメントでは、緊急時対応計画コーディネーターまたはCIOがIT緊急時対応計画を導入する権限を持つことを想定している。この権限は、組織またはシステムによって異なる。ただし、この権限を持つ担当者は、計画内で明確に指定する必要がある。この権限を持つことのできる個人は１人だけで、必要な場合、後継者が想定する当該責任を明確に特定する。

システム損害が特定されると、緊急時対応計画コーディネーターは、適切な復旧戦略を選択し[27]、関連する復旧チームに通知することができる。通知は、第4.2.1項で要約した手順に従う。[28]

4.3 復旧フェーズ

復旧操作は、緊急時対応計画を実行して損害評価が完了し（可能な場合）、担当者に通知され適切なチームが起動した後に開始する。復旧フェーズでの活動は、一時的にIT処理機能を実行し、損害を修復して元のシステムに戻し、元の施設または新しい施設で運用機能を復旧するといった緊急時対応策に焦点を置いたものである。復旧フェーズが完了するとITシステムは、運用可能となり、計画で示すような機能を実行する。計画で定義される復旧戦略によっては、これらの機能に、一時的な手動処理、代替システムでの復旧および運用、代替サイトでの再配置および復旧を含むことができる。復旧の責任を担うチームは、これらの復旧戦略をよく理解して、イベントの初期段階で紙媒体での計画が入手できない場合でも必要な活動を実行できるようにしておく必要がある。

4.3.1 復旧活動の順序

独立した複数のコンポーネントを持つWANなど、複雑なシステムを復旧するには、事業影響分析で特定したシステム優先度を反映した復旧手順が必要となる。活動の順序にはシステムの許容中断時間を反映させ、関連システムとそのアプリケーションに重大な影響を回避しなければならない。復旧手順は段階別に順番に記述され、システムコンポーネントが論理的な方法で復元されるようにする。たとえば、LANを障害後に復旧する場合、最も重要なサーバーが、プリンタなどさほど重要でないデバイスよりも先に復旧されなければならない。同様に、アプリケーションサーバーを復旧する場合、アプリケーションやそのデータを復旧する前に、オペレーティングシステムの復旧と検証を行う。復旧手順には、以下のような状況が発生した場合の他のチームとの調整指示も含める。

- 活動が、目標時間枠内で完了しない場合
- 主要な段階が完了した場合
- 調達すべきアイテムがある場合

---

[27] たとえば、インシデントによって短期の障害のみが予測される、または物理的損害が特定のハードウェアデバイスに限定される場合、緊急時対応計画コーディネーターは、システムを他のデバイスを使用してオンサイトで回復することを選択できる。しかし、損害評価によって施設への広範な損害が判明した場合、緊急時対応計画コーディネーターは、システムと回復チームを代替サイトに長期にわたって再配置する必要がある。

[28] IT 運用を一時的に代替サイトに再配置する必要がある場合、回復チームメンバーの移動に関する調整が必要となる。特定の主要担当者に対しては、事前承認された出張権限を考慮してみるとよい。優先旅行代理店、ホテル、レンタカー会社などの旅行情報を緊急時対応計画の付録に追記できる。

・ その他、システム固有の考慮事項

代替サイトでシステムを復旧する必要がある場合、特定の機材を移送または調達しなければならない。これには、オフサイトストレージからのデータバックアップメディア、ハードウェア、復旧計画のコピー、ソフトウェアプログラムの配送などがある。復旧手順では、適切なチームまたはチームメンバーを指定し、機器、データ、重要なデータの配送を調整する。計画には、必要に応じて機器リストまたはベンダー連絡先情報などを記載した付録を含める。復旧手順には、システムの復旧に必要な資材のパッケージ、移送、購入に関する要件を明確に記述する。

4.3.2 復旧手順

復旧フェーズの運用を促進するため、緊急時対応計画に、ITシステムまたはシステムコンポーネントを復旧するための詳細な手順を規定する。システムの種類、構成、アプリケーションは多岐にわたるため、本ガイドラインでは特定の復旧手順については規定しない。ただし、各ITシステムの復旧に関する懸案項目は、第5項で詳述する。

手順は適切な復旧チームに割り当てられ、通常は以下の活動が記述される。

・ 損害を受けた施設または地域へアクセスする権限を取得する

・ システムに関係する内部および外部のビジネスパートナーに通知する

・ 必要なオフィス消耗品および作業空間を確保する

・ 必要なハードウェアコンポーネントを確保してインストールする

・ バックアップメディアを取得してロードする

・ 重要なオペレーティングシステムおよびアプリケーションソフトウェアを復旧する

・ システムデータを復旧する

・ セキュリティコントロールを含むシステムの機能をテストする

・ システムをネットワークまたは外部システムに接続する

・ 代替装置をうまく活用する

復旧手順は簡潔に、手続き順に記述する。緊急時の困難や混乱を防ぐため、手順にないステップを想定したり、また省略したりしない。チェックリスト形式にしておくことにより、順を追った復旧手順の文書化や、システムが正常に復旧しなかった場合のトラブルシューティングに役に立つ。次の例は、LAN復旧チームによる復旧手順チェックリストの一部である。

LAN復旧チーム用復旧プロセス

これらの手順は、バックアップテープからファイルを復元する場合に使用する。LAN復旧チームは、運用の継続に必要な、すべての重要なファイルをリロードする責務を負う。

・ ファイルと、ファイルの復元を開始する日付を特定する。	**時刻:__ :__**
・ テープのログ記録から、テープ番号を特定する。	**時刻:__ :__**
・ テープライブラリにテープがない場合、復旧施設にテープを要求する。	**時刻:__ :__**
その際、適切な権限を持つ担当者が署名する。	**時刻:__ :__**
・ テープを受理したら、日付と時刻を記録する。	**時刻:__ :__**
・ テープをドライブに挿入し、復旧プロセスを開始する。	**時刻:__ :__**
・ ファイルが復旧したら、LAN復旧チームリーダーに通知する。	**時刻:__ :__**

4.4 再構築フェーズ

再構築フェーズでは、復旧活動が終了し、通常業務は組織の施設に戻される。元の施設が復旧できない場合、このフェーズでの活動は、新しい施設がシステム処理の要件を満たすことを目的に行う。元のサイトまたは新しいサイトがITシステムおよび通常のプロセスをサポートできるレベルに復旧されると、元のサイトまたは新しいサイトにシステムを移転することができる。プライマリシステムが復旧されテストされるまで、IT緊急時対応システムは運用を継続する。再構築フェーズでは、サイトとITシステムの両方の復旧と移転を担当するチームを指定する。このフェーズでは、以下の主要な活動が発生する。

・ 電力、水、電話、セキュリティ、環境制御、オフィス機器、オフィス消耗品など、適切なインフラストラクチャのサポートの確保

・ システムハードウェア、ソフトウェア、ファームウェアのインストール。当該行為には、復旧フェーズで実行される手順と同様の、詳細な復旧手順が含まれる

・ ネットワークコンポーネントおよび外部システムとの接続とインターフェースの確立

・ 機能を保証するための、システム業務のテスト

・ 緊急時対応システムへの運用データのバックアップと、復旧したシステムへのアップロード

・ 緊急時対応システムのシャットダウン

・ 緊急時対応の終了

・ 緊急時サイトでのすべての機密資料のセキュリティ確保、廃棄、移動

・ 復旧担当者を元の施設へ復帰させる手配

このチームは、要求される機能を理解し、紙媒体での計画が入手できない場合でも機能を実行できるようにしておく必要がある。

4.5 計画の付録

緊急時対応計画の付録では、計画の本文で取り上げなかった重要な詳細事項を規定する。付録には、該当するシステムの特定の技術的、運用上、管理上の緊急事態要件を反映させる。ただし、緊急時対応計画によく使用される付録もある。一般的に、IT緊急時対応計画の付録には以下の項目が含まれる。

・ 緊急時対応計画チーム担当者の連絡先情報

・ オフサイトストレージおよび代替サイトの連絡担当窓口を含む、ベンダーの連絡先情報

・ システム復旧またはプロセスのための、標準的な運用手順およびチェックリスト

・機器および、システム運用のサポートに必要なハードウェア、ソフトウェア、ファームウェアおよび、その他のリソースに関するシステム要件リスト。モデルまたは、バージョン番号、スペックおよび、数量を含め、それぞれのアイテムに対し詳細を規定する

・ ベンダーサービス保証契約、他の組織との相互契約、その他の重要な記録

・ 代替サイトの詳細およびそのサイトに対する指示事項

・ 計画フェーズ中に実施される事業影響分析には、相互関係、リスク、優先度付け、システムの各要素への影響に関する有益な情報を含める。事業影響分析は、計画実行時に参照できるよう、付録に含める必要がある。

5. 技術的な緊急時対応計画の考慮事項

この項では、特定の種類のITシステムについて技術的な緊急時対応計画に関する考慮事項を説明することにより、これまでの項で示してきたプロセスおよびフレームワークのガイドラインを補完する。この項で示す情報は、ITシステムの種類に基づいて読者が特定の技術的な緊急時対応戦略を選択、策定、および導入する場合に役立つであろう。システムは千差万別であるため、ここでの情報は最も幅広く読者が使用できるレベルで提供する。ここで示す情報は、あるITシステムにはあてはまらない可能性もある。したがって、緊急時対応計画コーディネーターは必要に応じシステムに固有の緊急時対応要件に合致するように修正する必要がある。この項では、次のITプラットフォームを取り上げている。

- デスクトップコンピュータおよびポータブルシステム
- サーバー
- ウェブサイト
- ローカルエリアネットワーク
- ワイドエリアネットワーク
- 分散システム
- メインフレームシステム

それぞれのITプラットフォームの種類ごとに、2つの観点から技術的対策を検討する。まず、緊急時対応計画コーディネーターがシステム復旧戦略を計画する場合に考慮しなければならない技術的要件または要素について説明する。次に、それぞれのプラットフォームについて、技術に基づいた解決策を提示する。この項で取り上げる技術面での考慮事項と解決策には、第3.3項で説明した予防措置と、第3.4項で述べた復旧処置が含まれている。これらの緊急時対応処置のいくつかは、すべてのITシステムに共通である。共通した考慮事項は次のとおりである。

- データ、アプリケーション、およびオペレーティングシステムのバックアップ頻度とオフサイトでの保管
- 重要なシステムコンポーネントまたは機能の冗長性

・ システム構成および要件の文書化

・ システム復旧をスムーズに実施するために必要なシステムコンポーネント間および、プライマリサイトと代替サイト間における機器の相互運用性

・ 適切にサイジング、設定された電源管理システムおよび、環境の制御

これらの考慮事項のそれぞれについて、第5項全体にわたって説明する。

5.1 デスクトップコンピュータおよびポータブルシステム

デスクトップコンピュータまたはポータブルシステム（ラップトップまたはハンドヘルドデバイスなど）は、一般に、中央演算処理装置（CPU）、メモリ、ディスク記憶域、およびさまざまな入出力デバイスから構成されている。PCは1台につき1ユーザーが使用するように設計されている。

デスクトップコンピュータは、オフィスのデスクまたはテーブル上での使用に適した据え置き型のPCである。持ち運びや出張にはあまり適していない。デスクトップコンピュータの大多数は、他のネットワークデバイス、アプリケーション、およびインターネットと通信できるようにネットワーク接続されている。ラップトップコンピュータ（ノート型コンピュータとも呼ばれる）やハンドヘルドコンピュータなどのポータブルシステムは、利便性および出張目的などを考慮して持ち運びができるようにしたPCである。ポータブルシステムは、小型のデスクトップコンピュータであり、デスクトップコンピュータに匹敵する処理能力、メモリ、およびディスク記憶域を備えたものや、ハンドヘルドコンピュータのように処理能力、メモリ、およびディスク記憶域が制限されるものもある。ポータブルシステムは、ダイヤルアップ回線などのさまざまなメカニズムを通じて、他のネットワークデバイス、アプリケーション、およびインターネットに接続できる。

PCは、組織の所有するITインフラストラクチャにおいて、いたる所に存在する。デスクトップおよびポータブルコンピュータは、日常の自動処理の最も一般的なプラットフォームであり、緊急時対応計画で重要な要素である。PCは、組織のLANに直接接続することも、リモートロケーションから組織のネットワークにダイヤル回線で接続することも、またはスタンドアロンのシステムとして機能することもできる。

5.1.1 緊急時対応計画での考慮事項

デスクトップおよびポータブルシステムに関する緊急時対応計画では、データの可用性、機密性、および完全性に重点を置く必要がある。システム管理者は、これらの要件に対処するために、次の措置を考慮する必要がある。

- **オフサイトでのバックアップの保管** 第3.4.1項で述べたように、バックアップメディアは、オフサイトの安全かつ、環境が整えられた施設内で保管する必要がある。ユーザーが、ネットワーク経由でデータを保存するのではなく、スタンドアロンのシステム上でデータのバックアップを行えば、代替のバックアップ方法を提供することになる。緊急時対応計画のコピー、ソフトウェアライセンス、ベンダーのサービスレベル契約や他の契約、およびその他の重要なドキュメントは、バックアップメディアに格納する。緊急時対応計画コーディネーターが実施する事業影響分析は、どれだけの頻度でバックアップをオフサイトに送ればよいかを確定するのに役立つ。

- **各ユーザーに対するデータのバックアップの奨励** PCのバックアッププロセスがネットワークを通じて自動処理されるのでなければ、データのバックアップを定期的に行うことをユーザーに奨励する必要があり、従業員のセキュリティトレーニングおよび意識向上を利用して行うことができる。

- **パーソナルコンピュータ上のデータの保存に関するガイダンスの提供** ユーザーに対して特定のフォルダにデータを保存するように指導することで、IT部門のデスクトップサポート作業が軽減される。また、コンピュータの再構築が必要になった場合に、技術者は、システムの再ロード時にどのフォルダをコピーし保存すればよいかを把握できる。

- **ハードウェア、ソフトウェア、および周辺機器の標準化** ハードウェア、ソフトウェア、および周辺機器が組織内で標準化されていれば、より迅速にシステムの復旧を実施できる。組織内で設定を標準化できない場合でも、なるべく部門ごとまたはコンピュータの種類やモデルごと（可能な場合）に標準化する必要がある。さらに、災害時にいち早く復旧しなければならない重要なハードウェアコンポーネントは、既成品のコンピュータコンポーネントとの互換性を備えている必要がある。このように互換性があれば、ベンダーに特注機器を注文するといった、復旧の遅れを回避することができる。

- **システム設定およびベンダー情報の文書化** システム設定を十分に文書化しておけば、復旧が容易となる。同様に、交換用機器の購入を迅速に行えるように、緊急時対応計画へベンダーの名称と緊急時の連絡先情報を記載しておく必要がある。

- **セキュリティポリシーおよびシステムセキュリティコントロールとの調整** 以下で述べるデスクトップコンピュータおよびポータブルコンピュータの緊急時対応策は、セキュリティポリシーおよびシステムセキュリティコントロールと調整する必要がある。したがって、適切で技術的な緊急時対応策を選択する場合、システムの障害または緊急事態に実行される緊急時対応策によって、機密データの改ざんや漏洩が引き起こされないように、生産システムと同様のセキュリティコントロールおよびセキュリティ関連の活動（リスクアセスメントや脆弱性検査など）を緊急時対応策に導入する必要がある。

- **事業影響分析結果の使用** 関連する主要アプリケーションおよび一般サポートシステムの事業影響分析によって明らかになった影響および優先順位を検討して、関連要件を特定する必要がある。

5.1.2 緊急時対応策

技術的にさまざまな緊急時対応策をデスクトップコンピュータに使用できるが、ここではいくつかの効果的な実践例を取り上げる。このとき、主要アプリケーションと汎用サポートシステムの事業影響分析によるデータを使用して、復旧要件および導入の優先順位を特定する必要がある。

デスクトップコンピュータおよびポータブルシステムの緊急時対応策:

- システムおよびアプリケーション構成の文書化
- ハードウェア、ソフトウェア、および周辺機器の標準化
- データのバックアップに関するガイダンスの提供
- コンポーネント間の相互運用性の確保
- セキュリティポリシーおよびコントロールとの調整
- データのバックアップとオフサイトでの保管
- アプリケーションのバックアップとオフサイトでの保管
- 代替ハードディスクドライブの使用
- イメージディスク
- 重要なシステムコンポーネントにおける冗長性の実装
- 無停電電源装置の使用

バックアップは、PCのデータ可用性を確保する最も一般的な手段である。適切なバックアップソリューションを選択する場合、特定の要素を考慮しなければならない。

- **機器の相互運用性** 復旧をスムーズに行うため、バックアップデバイスは、プラットフォームのオペレーティングシステムおよびアプリケーションとの互換性を備えていなければならず、異なるモデルまたは種類のPCに簡単に装着できる必要がある。

- **記憶域ボリューム** 適切な記憶域を確保するために、バックアップを作成するデータの容量に基づいて適切なバックアップソリューションを決定する必要がある。

・ **メディアの寿命** メディアの使用および記憶メディアの寿命は、メディアの種類によって異なり、この寿命を過ぎると有効なデータ復旧に対するメディアの信頼性は失われる。

・ **バックアップソフトウェア** 適切なバックアップソリューションを選択する場合、データのバックアップに使用するソフトウェアまたは方法を考慮する必要がある。バックアップアプリケーションは、オペレーティングシステムのファイルマネージャを使用したファイルコピーと同じように簡単な場合もあるが、サイズの大きなデータの転送を伴う場合には、定期的に自動でファイルのバックアップを行うサードパーティのアプリケーションが必要になる。

PCデータのバックアップは、以下のようにさまざまな方法で実行できる。[29]

・ **フロッピーディスク** フロッピーディスクドライブは、大多数のデスクトップコンピュータに標準で装備されており、最も安価なバックアップソリューションである。ただし、このドライブは記憶容量が小さく、速度も遅い。

・ **テープドライブ** テープドライブは、デスクトップコンピュータにおいて一般的ではないが、大容量バックアップソリューションの一つの選択肢である。テープドライブは、自動的に作動するため、サードパーティのバックアップアプリケーションまたはオペレーティングシステムのバックアップ機能が必要になる。テープメディアは、比較的安価である。

・ **リムーバブルカートリッジ** リムーバブルカートリッジは、デスクトップコンピュータにおいて一般的でなく、多くの場合ポータブルまたは外部デバイスとしてのバックアップソリューションとして提供される。Iomega社のZip®およびJaz®記憶ドライブなどのリムーバブルカートリッジは、フロッピーディスクよりも高価である。また、メディアのモデルやブランドにもよるが、テープメディアと同程度のコストである。しかし、リムーバブルカートリッジは高速であり、携帯性に優れているため、柔軟に使用できる。また、ポータブルデバイスには、専用ドライバとアプリケーションが付属しており、データのバックアップが簡単にできる。

・ **コンパクトディスク** CD読み取り専用メモリ（CD-ROM）ドライブは、ほとんどのデスクトップコンピュータに標準で付属しているが、書き込み可能なCDドライブは、すべてのコンピュータに装備されているわけではない。CDは低コストの記憶メディアであり、フロッピーディスクよりも大容量の記憶容量を備えている。CDから読み取る場合は、オペレーティングシステムのファイルマネージャで十分だが、CDに書き込む場合は、書き込み可能なCD（CD-RW）ドライブと適切なソフトウェアが必要になる。

---

[29] 第 5.2.2 項では、完全、増分、および差分という、使用可能なバックアップ方法について説明している。

- **ネットワークストレージ** ネットワーク接続したPCに格納されたデータは、ネットワークディスクまたはネットワークストレージデバイスにバックアップを行うことができる。

  - **ネットワークディスク** ネットワークディスクは、データ記憶域を備えたサーバーを指す。PCからバックアップできるデータの容量は、ネットワークディスクの記憶容量または特定ユーザーへのディスク割り当てによって制限される。ただし、ユーザーがネットワークディスクにファイルを保存するように指示されている場合、ネットワークまたはサーバーのバックアッププログラムを使用して、ネットワークディスク自体のバックアップを作成する必要がある。

  - **ネットワークストレージデバイス** ネットワークバックアップシステムを構成することで、ネットワーク接続したPCのローカルドライブに対するバックアップを作成することができる。このバックアップの開始は、ネットワークバックアップシステムか実際のPCのどちらからでも行える。

- **複製または同期化** データの複製または同期化は、ポータブルコンピュータ用の一般的なバックアップ方法である。ハンドヘルドコンピュータまたはラップトップコンピュータは、PCに接続して、ポータブルシステムからデスクトップコンピュータへ必要なデータを複製できる。

- **インターネットバックアップ** インターネットバックアップ、つまりオンラインバックアップは有料の商用サービスであり、PCユーザーは、インターネットを介して遠隔地にデータのバックアップを行うことができる。このバックアッププログラムをPCにインストールすることにより、ユーザーはバックアップのスケジュールを設定し、バックアップを作成するファイルおよびフォルダの選択、ファイルの上書きを防止するための「アーカイブ」方式を設定できる。転送時には、データは暗号化されるが、モデム接続を介した際のデータ転送速度は低下する。インターネットバックアップのメリットは、ユーザーがデータバックアップ用のハードウェアやメディアを購入しなくてもよいという点にある。

データのバックアップに加えて組織では、システムドライバのバックアップも作成する必要がある。組織は、**ソフトウェアとソフトウェアライセンスをセカンダリロケーションに格納しなければならない。**ソフトウェアが既成品（COTS; Commercial Off-The-Shelf）であれば、中断前にインストールしたコピーまたはライセンスが利用できなくなった場合でも、ベンダーから購入できる。ただし、少なくとも特注のアプリケーションがデスクトップにインストールされている場合は、これを代替サイトに保存および格納するか、上記のいずれかの方法でバックアップを作成する必要がある。特にアプリケーションで（PCまたはネットワークサーバーの）ドライブマッピングをハードコード化している場合は、代替サイトで特注のアプリケーションを復旧する手順も文書化しておかなければならない。アプリケーションが別のシステム上で実行できないようなコードは、禁止する必要がある。ドライブマッピングがハードコード化されている場合、このアプリケーションを元のシステム以外における別のシステム上で復旧で

きるように修正する必要がある。

暗号化は、ポータブルコンピュータ用のセキュリティツールとしてますます普及しつつある。否認防止に電子署名が、機密性の保護に暗号化がますます使用されるようになってきているため、組織のバックアップ戦略に、暗号化鍵ペアを含めることを検討する必要がある。[30] 暗号化鍵ペアと検証鍵がPCに格納されている場合、そのPCが破損してしまうと、データを復旧できなくなったり検証できなくなる可能性がある。

ポータブルコンピュータは、盗難に対して脆弱であるため、盗まれたコンピュータからのデータ漏洩を防止するため、暗号化を使用することがある。また、ポータブルコンピュータのユーザーに、出張時に使用する**予備ハードディスクドライブ**を提供することも考えられる。このとき、予備ハードディスクドライブには、最低限必要なアプリケーションとデータしか格納しないようにする。予備ハードディスクドライブを使用することによって、コンピュータが盗まれた場合でもデータ損失の被害を最小限にとどめることができる。

イメージングは、もう1つの緊急時対応策である。標準デスクトップコンピュータのイメージを保存しておくことで、破損したコンピュータの復旧を行えるようになる。しかし、このイメージングでは、イメージに格納されたアプリケーションと設定をインストールできるが、現在ディスク上にあるすべてのデータは失われてしまう。したがって、PCユーザーに各データファイルのバックアップ作成を奨励する必要がある。なぜなら、ディスクイメージのサイズは大きくなる場合があるため、サーバーまたはサーバーパーティションなどをディスクイメージ専用の記憶域として割り当てる必要が生じるからである。複数のPCが破損した場合、復旧に必要となるイメージの数を減らすためには、PCのモデルと設定を組織内で標準化する必要がある。これによって、ディスク領域を節約でき、コンピュータの再構築プロセスが容易となる。サイトの移転が必要な場合は、PCの設定とミッションクリティカルな処理に必要な基本アプリケーションを、緊急時対応計画で文書化する必要がある。

システムとそのデータは、電源の不具合により破損する可能性がある。破損を防止するために、PCに**二重電源**を装備することができる。主電源がオーバーヒートしたり使用できなくなった場合に、補助電源が主電源となりシステムの中断をもたらすことがない。

補助電源は、ハードウェアの障害に対しては保護するが、停電の場合は保護できない。一方、**UPS**は、電力が供給されない場合にもシステムを保護できる。UPSは、通常30分から60分にわたりバックアップ用の臨時電力を供給する。これだけ時間があれば、正常にシャットダウンを行うのに十分である。二重電源とUPSの組み合わせを、他の緊急時対応策と比較するために、費用対効果分析

---

[30] 暗号化の詳細については、NIST SP 800-21『Guideline for Implementing Cryptography in the Federal Government』（1999 年 11 月）を参照のこと。

を行う必要がある。二重電源とUPSの組み合わせは、サーバーの場合はコスト効率が良いが、PCの場合はそうでないことがある。

5.2 サーバー

サーバーは、ファイル共有および記憶域、データ処理、集約的なアプリケーションのホスティングを扱い（電子メールや中央データベースなど）、印刷、アクセスコントロール、ユーザー認証、リモートアクセス接続、その他の共有ネットワークサービスをサポートする。ローカルユーザーは、ネットワーク接続したPCからサーバーにログインして、サーバーが提供するリソースにアクセスする。

サーバーとは、ディスクストレージ、プリンタ、ネットワークアプリケーションなどのリソースまたは一部のネットワークおよびネットワークリソースへのアクセスを提供するソフトウェアを実行するコンピュータである。ネットワークオペレーティングシステムが稼働していれば、どのタイプのコンピュータでもサーバーとして使用できる。サーバーは、標準的なPCである場合や、数百の要求を同時に処理するために複数のディスクドライブと大容量メモリを備えた大型コンピュータである場合もある。

5.2.1 緊急時対応計画での考慮事項

サーバーは、多くの重要なアプリケーションをサポートまたは提供しているため、サーバーの損害が、ビジネスプロセスにとって重大な問題を引き起こす可能性がある。サーバーの脆弱性に対処するには、次の措置を検討する必要がある。

- **バックアップメディアおよびソフトウェアのオフサイトでの保管** 前述のように、バックアップメディアおよびソフトウェアは、オフサイトの安全かつ、環境的に管理された施設内に保管する必要がある。ストレージ施設は、両方のサイトが同じ災害によって影響を受ける可能性を低減するため、元のサイトから十分に離れた場所に設けなければならない。

- **ハードウェア、ソフトウェア、および周辺機器の標準化** ハードウェア、ソフトウェア、および周辺機器が組織またはサイト全体で標準化されていれば、迅速にシステム復旧を行うことができる。標準的な構成は、緊急時対応計画で文書化を行う。

- **システム構成およびベンダーの文書化** システム構成を詳細に記録しておくことで、システム復旧能力が高まる。さらに、基本的なハードウェア、ソフトウェア、および他のコンポーネントを供給するベンダーを、緊急時対応計画に明記しておく必要がある。

- **セキュリティポリシーおよびシステムセキュリティコントロールとの調整**　サーバーの緊急時対応策は、セキュリティポリシーおよびシステムセキュリティコントロールと調整する必要がある。したがって、適切で技術的な緊急時対応策を選択するためには、システムの中断または緊急時に技術的な緊急時対応策を実行することで機密データの改ざんや漏洩が引き起こされないように、本番環境と同様のセキュリティコントロールおよびセキュリティ関連の活動（リスクアセスメントや脆弱性検査など）を、緊急時対応策に導入する必要がある。

- **事業影響分析結果の使用**　関連する主要アプリケーションおよび汎用サポートシステムの事業影響分析によって明らかになった影響および優先順位を検討して、関連要件を特定する必要がある。

5.2.2 緊急時対応策

サーバーの緊急時対応策
- システムおよびアプリケーション構成の文書化
- システムおよびアプリケーションのドキュメント化
- ハードウェア、ソフトウェア、および周辺機器の標準化
- セキュリティポリシーおよびコントロールの調整
- コンポーネント間の相互運用性の確保
- データのバックアップとオフサイトでの保管
- アプリケーションのバックアップとオフサイトでの保管
- 無停電電源装置の使用
- 重要なシステムコンポーネントにおける冗長性の実装
- 重要なシステムコンポーネントにおける耐障害性(フォールトトレランス)の実装
- データ複製
- ストレージソリューションの実装

サーバーの復旧能力を高めるためには、いくつかの技術的な手段をとることが可能である。主要アプリケーションおよび汎用サポートシステムの事業影響分析からは、復旧要件および優先順位の決定に役立つ情報が提供される。サーバーの緊急時対応計画では、サーバーによって提供されるネットワークサービスの信頼性と可用性に重点を置く必要がある。また、データの機密性と重要性の要件も考慮しなければならない。さらに、サーバーやそのアプリケーション、およびデータの可用性要件も評価する必要がある。予防的な緊急時対応手段としてできるだけ重要な機能は、重要でない機能と同じサーバーに置かない方がよい。たとえば、重要なアプリケーションを提供するサーバーは、そのアプリケーション専用に使用し、他のリソースは提供しないようにする。

PCと同様に、サーバーも定期的にバックアップを作成する必要がある。サーバーごとに独自のドライブを備えた分散型システム、または中央のバックアップデバイスが1台のサーバーに接続した集中型システムを通じて、サーバーのバックアップを行うことができる。サーバーデータを保存するためには、次に挙げる3つのタイプの**システムバックアップ**方法がある。

- **フル** フルバックアップでは、バックアップのために選択したディスク上またはフォルダ内の全ファイルを対象とする。バックアップが作成されたすべてのファイルは、単一のメディアまたは一連のメディアに記録されているので、特定のファイルまたはファイル群を簡単に検索できる。ただし、完全バックアップは、非常に長い時間を要する。さらに、あまり頻繁には変更されないファイル（システムファイルなど）の完全バックアップは、過度に不要なメディアストレージを増やすことになる。

- **増分** 増分バックアップは、バックアップのタイプに関係なく、直前のバックアップ以降に作成または変更されたファイルを対象とする。増分バックアップを使用すれば、記憶メディアをより効率的に使用することができ、バックアップ時間を短縮できる。ただし、増分バックアップからシステ

ムを復旧するには、別のバックアップ操作からメディアを取り出す必要がある。たとえば、ディレクトリを復旧する必要がある場合を考えてみる。最後のフルバックアップが3日前に実行され、毎日1つのファイルが変更された場合、フルバックアップで使用したメディアと、以降毎日の増分バックアップで使用したメディアがディレクトリ全体の復旧に必要となる。

- **差分** 差分バックアップは、直前の完全バックアップ以降に作成または修正されたファイルを格納する。したがって、前回のフルバックアップ後にファイルが変更された場合、次のフルバックアップが終了するまで差分バックアップは、変更のたびにファイルを保存することになる。差分バックアップは、フルバックアップに比べて実行時間が短縮される。差分バックアップからの復旧は、フルバックアップメディアと最後の差分バックアップメディアしか必要としないため、増分バックアップに比べて必要なメディア数も少なくなる。差分バックアップは、直前のフルバックアップ以降のデータ容量が、次のフルバックアップが行われるまで毎日増加しているため、増分バックアップに比べて実行時間が長くなるというデメリットがある。

システム構成および復旧要件に応じて、これらのバックアップ操作を組み合わせて使用することもできる。たとえば、完全バックアップを週末に行い、差分バックアップを毎晩行うことができる。サーバーのバックアップスケジュールを作成するときには、次の点を考慮する必要がある。

- メディアをどこに保管するのか
- どのデータのバックアップを作成する必要があるか
- どれだけの間隔でバックアップを実行するのか
- 緊急事態が起きた場合に、どれだけ迅速にバックアップを取り出せるのか
- メディアを取り出す権限は誰にあるのか
- メディアを取り出すのに、どれだけの時間がかかるのか
- メディアはどこに届けられるのか
- 誰がメディアからデータを復旧するのか
- どのようにメディアにラベルを付けるのか

・ どれだけの期間、バックアップメディアを保管しておくのか

・ いつメディアをオンサイトに格納し、メディアの保管に対してどのような環境管理が行われるのか

・ どのようなバックアップメディアが適切なのか

・ どのようなメディア読み取り機が、代替サイトで使用されるのか

バックアップメディアは、オフサイトで安全かつ環境管理された場所で保管する必要がある。オフサイトの場所を選択する場合、その場所の利用時間、バックアップメディアの利用しやすさ、物理的な記憶容量の制限、および契約条項を考慮に入れなければならない。このとき、**オフサイトの格納域から定期的にメディアを取り出して、バックアップが正しく行われていることを確認することが重要である。**緊急時対応計画コーディネーターは、バックアップメディアの検査間隔を決定する際に、事業影響分析を参照することとする。それぞれのバックアップテープ、カートリッジ、またはディスクには、緊急事態が発生したときに必要なデータを迅速に識別できるよう、一意のラベルを付ける必要がある。このため、効率的な記録および追跡戦略を作成する必要が求められる。これには、バックアップの作成年月日を使用したラベルをメディアに付けるという方法がある。他の戦略はより複雑になるが、たとえば複数組のメディアを交代で使用して、古いデータの終わりに付け加えるか、古いデータを上書きするという方法がある。マーキング戦略は、メディアを破棄するまで保管する期間を指示したメディア保管ガイドラインに適合する必要がある。

オフサイトでのバックアップメディアのストレージによって、システムを復旧することができるが、前回のバックアップ以降にサーバーに追加されたデータ、またはサーバー上で修正されたデータは、中断または災害で失われている可能性がある。このデータ損失の可能性を回避するために、バックアップ戦略は、ディスクミラーリング、RAID、負荷分散などの冗長性ソリューションで補完する必要がある。以下では、これらのソリューションについて説明する。事業影響分析によるデータは、緊急時対応計画コーディネーターがデータローテーションの適切な間隔を決める場合に役立つ。

RAIDは、データストレージにディスクの冗長性とフォールトトレランスを提供し、平均故障間隔（MTBF; Mean Time Between Failures）を短縮させる。RAIDはディスクドライブおよびディスクコントローラの障害を遮断するために使用される。さらに、RAIDは、単一のディスクではなく複数のディスクドライブにデータストレージを分散させるため、パフォーマンスと信頼性が向上する。RAIDは、ハードウェアでもソフトウェアでも実装できるが、どちらの場合でも、このソリューションは、オペレーティングシステムに対し、単一の論理的ハードディスクドライブとして考えられる。RAIDシステムには、ホットスワップが可能なドライブを使用することができる。つまり、ハードディスクドライブに障害が発生した

場合、システムをシャットダウンさせずに、そのハードディスクドライブを交換することができる。RAIDテクノロジーでは、ミラーリング、パリティ、およびストライピングの3つのデータ冗長性テクニックが使用される。

- **ミラーリング** この手法は、システムが別々のハードディスクドライブまたはドライブアレイに、データを同時に書き込む。ミラーリングには、ダウンタイムを最小限にとどめ、データの復旧を簡単にし、ディスクからの読み取り時のパフォーマンスを向上させるというメリットがある。1台のハードディスクドライブまたはディスクアレイに障害が発生した場合、稼働しているハードディスクまたはディスクアレイからシステムを操作できる。または、読み取り処理に対して一方のディスクを使用し、別の処理要求に対してもう一方のディスクを使用することもできる。ミラーリングには、両方のドライブまたはディスクアレイがディスク書き込み機能で動作しているため、システムのパフォーマンスの低下を招くというデメリットがある。ミラーリングは、フォールトトレランスが高く、ハードウェアRAIDコントローラまたはオペレーティングシステムを通じて実装できる。

- **パリティ** パリティは、データが失われたのか上書きされたのかを判断する手法である。パリティは、ミラーリングよりもフォールトトレランスが低い。しかし、ミラーリングではデータのコピーが必要になる一方で、パリティにはこのようなコピーを保存しなくてもデータを保護できるというメリットがある。

- **ストライピング** ストライピングは、データをすべてのドライブに分散させることによってハードウェアアレイコントローラのパフォーマンスを向上させる。ストライピングでは、データ要素は複数の断片に分割され、この断片が各ハードディスクドライブに分散される。ストライピングを使用すると、ドライブに格納されている各データの断片を同時にアクセスできるため、データの転送パフォーマンスが向上する。ストライピングはバイト単位でもブロック単位でも実装できる。バイトレベルのストライピングは、データをバイトレベルに分割して、ハードディスクドライブへデータを連続して格納する。ブロックレベルのストライピングでは、データを所定サイズのブロックに分割して、各ブロックがディスクに分散される。

RAIDソリューションはミラーリング、パリティ、およびストライピングの3つの手法に基づいて構成される。現在、6つのRAIDレベルを利用でき、それぞれのレベルが異なる構成を提供する。RAID-1とRAID-5が、データの冗長性に最も一般に使用されているレベルである。

- **RAID-0**では、最も単純なRAIDレベルでありストライピングだけを使用する。RAID-0は、他のレベルよりも読み取り/書き込み速度のパフォーマンスが高いが、データの冗長性は備えていない。したがって、RAID-0はデータ復旧ソリューションとしては推奨されていない。

- **RAID-1**では、ミラーリングを使用して同一のコピーを作成し、2台のドライブに格納する。RAID-1は、実装が単純で安価であるが、データを複製するために記憶容量の50パーセントが失われる。

- **RAID-2**では、ビットレベルのストライピングを使用するが、RAIDコントローラが高価で実装が困難なので、あまり採用されていない。

- **RAID-3**では、専用パリティを備えたバイトレベルのストライピングを使用する。RAID-3は大きなファイルを扱うアプリケーションには有効なソリューションであるが、パリティデータが1台のドライブに格納されるため、パリティ情報のフォールトトレランスは備えていない。

- **RAID-4**では、RAID-3に似ているが、バイトレベルのストライピングではなくブロックレベルのストライピングを使用する。この手法には、アプリケーションのニーズに合わせてブロックサイズを変更できるというメリットがある。RAID-4を使用した場合、1台のハードディスクドライブの記憶領域が失われる。

- **RAID-5**では、ブロックレベルのストライピングと分散パリティを使用する。このソリューションでは、RAID-3およびRAID-4で単一のディスクにパリティデータを保存していたために生じていた障害を解消する。RAID-5では、パリティが、データとともにすべてのドライブにわたって書き込まれる。パリティ情報のブロックを、実際のデータのブロックと別々のドライブに分けることにより、フォールトトレランスを実現している。1台のドライブに障害が発生しても、障害のあったドライブのデータは、アレイ内の他のドライブに格納されたデータから再構築することができる。さらに、アプリケーションのニーズに合わせてストライプセット（ストライプの集合）を変更できる。RAID-5を使用した場合、1台のハードディスクドライブの記憶領域が失われる。

個々のRAIDレベルでは、緊急時対応計画コーディネーターの緊急時対応要件を満たせない場合、複数のRAIDレベルを組み合わせて、両方のRAIDレベルのメリットを取り入れることができる。最も一般的な組み合わせは、RAID-0+1とRAID-1+0である。たとえばRAID-0+1では、8台のハードディスクドライブが、それぞれ4台のハードディスクドライブから成る2つの別々のアレイに分割される。続いて、RAID-1が適用されデータの冗長性を提供する2つのアレイがミラーリングされる。したがって、RAID-1の高いフォールトトレランスが、RAID-0の向上したパフォーマンス速度と組み合わされる。RAID-1+0の場合、8台のドライブがミラーリングされ、それぞれ2つのドライブを持った4つのセット、つまり4つのミラーリングセットが構成される。続いて、RAID-0が4つのセットすべてに適用され、ミラーリングセット全体にストライピングアレイを作成する。ただし、どちらの場合でもドライブの可記憶領域の50パーセントが失われる。

RAIDは、ディスクの冗長性にとって効果的な戦略である。ただし、電源など、他の重要サーバー部分の冗長性も提供されなければならない。サーバーは、2台の電源を備えることができ、このため主電源がオーバーヒートしたり使用不能になった場合に、補助電源がサーバーに給電し続けることができる。

補助電源はハードウェアの障害から保護できるが、電力の障害に対しては効果的な対策とはならない。短時間の電力を確保して電力の変動に対する保護には、**UPS**を導入する必要がある。UPSは、多くの場合、システムを正常にシャットダウンするのに十分なバックアップ電力を供給する。高可用性を必要とする場合は、ガソリンまたはディーゼル発電機が必要となる。発電機は、サイトの電力システムに直接接続でき、停電を検出すると自動的に始動するように設定できる。

電子書庫とリモートジャーナリングは、通信リンクを介してリモートテープドライブにバックアップを行う、付加的データバックアップ機能を提供する類似テクノロジーである。リモートジャーナリングと電子書庫は、サーバーがバックアップ時に破損した場合に、復旧時間の短縮とデータ損失の低減を実現する。電子書庫の場合、システムは、電子書庫プロバイダに接続され、オフサイトでバックアップが自動的に作成される。電子書庫では、光学式ディスク、磁気ディスク、大容量ストレージデバイス、または自動テープライブラリがストレージデバイスとして使用される。このテクノロジーを使用した場合、定期的なバックアップの合間にサーバーで変更が生じると、データが電子書庫へ転送される。このようなバックアップの合間での転送を、電子ジャーナリングと呼ぶ場合もある。

リモートジャーナリングでは、トランザクションログまたはジャーナルが、リモートロケーションへ転送される。サーバーを復旧する必要が生じた場合は、直前のサーバーのバックアップ以降に行われた、トランザクション、アプリケーション、またはデータベースの変更を復旧するために、このログまたはジャーナルが使用される。リモートジャーナリングは、バッチ処理によって行うことも、バッファリングソフトウェアを使用して継続的に交信することもできる。リモートジャーナリングと電子書庫では、転送データを受信する専用のオフサイトロケーションが必要になる。このサイトは、システムのホットサイト、オフサイトのストレージサイト、または別の適切な場所とすることが可能である。データ転送の容量と頻度に応じて、リモートジャーナリングまたは電子書庫が、帯域幅内に限られた接続を通じて行われる。

サーバーの負荷分散は、サーバーとアプリケーションの可用性を高める。負荷分散によって、1台のサーバーに作業負荷が集中しないように、共通のアプリケーションを実行している複数のサーバーのグループ間で、トラフィックが動的に配分される。この手法では、サーバーグループは、ネットワークに対し、単一のサーバーとして見なされる。負荷分散システムは、1台のサーバーにトラフィックが集中しないように、それぞれのサーバーを監視して、トラフィックを転送する最適な経路を決定し、パフォーマンスと可用性を高めている。負荷分散は、1つのサイト内のサーバー間、または異なるサ

イトのサーバー間で実装できる。異なるサイト間で負荷分散を使用することにより、1つまたは複数のサイトが運用できるかぎり、アプリケーションの運用を続けることができる。したがって、負荷分散は、システムの可用性要件によっては実行可能な緊急時対応手段となる。

ディスク複製では、データが2つの別々のディスクに書き込まれ、データの2つの有効なコピーが常に利用できるようになるため、復旧ウィンドウが最小となる。この2つのディスクは、保護（対象）サーバー（主要サーバー）と複製サーバー（バックアップサーバー）と呼ばれる。ディスク複製は、ローカルでも異なるロケーション間でも実装できる。2つの異なるデータ複製手法が可能であり、それぞれが異なる目標復旧時間（RTO; Recovery Time Objective）と目標復旧ポイント（RPO; Recovery Point Objective）を提供する。RTOは、システムが利用できなくなってから、重大な影響を組織に及ぼすまでに経過する時間の許容可能な最大値である。RPOは、処理を再開するために、復旧に必要であるデータが存在していた時点を指す。これらのディスク複製手法は次のとおりである。

- **同期またはミラーリング**　この方法では、ディスク間コピーを用い、変更が保護対象サーバーに適用されると同時に、複製サーバーに変更を適用することによって、データベースまたはファイルシステムの複製を保全する。同期モードは、保護対象サーバーでのパフォーマンスを低下させるため、帯域幅がサーバー間のデータ転送を制限しない物理的に短い距離間でのみ実装すべきである。同期ミラーリングでは、RTOは数分から数時間に及ぶため、RPOはコミットされていない作業が失われた時点まで引き下げられる。ミラーリングは、データの微塵ほどの消失も許容できないほど重要なアプリケーションに使用する必要がある。

- **非同期またはシャドウ処理**　この手法は、変更を継続的にログへ記録し、ログに記録された変更を複製サーバーに適用することにより、データベースまたはファイルシステムの複製を保持する。非同期シャドウ処理では、RTOは、未適用のログにおける変更を実装するために必要な時間に応じて、数時間から1日程度を要する。許容可能なRPOは、シャドウ処理サーバーが受信した最後のデータ転送時点である。非同期複製は、ネットワークの待ち時間が発生する比較的小規模な帯域幅で、長距離の接続を行う場合に有効である。その結果、シャドウ処理は保護対象サーバーのパフォーマンスの保持に役立つ。

また、複製ソリューションは、オペレーティングシステムに依存したいわゆるホストベース複製の場合もあり、同期と非同期の両方の複製を使用できる。適切なディスク複製手法および製品を選択するために緊急時対応計画コーディネーターは、プラットフォームのサポート、他の補完製品との統合、コスト、導入スピード、パフォーマンスの影響、および製品の完全性と管理容易性を評価する必要がある。

ディスク複製は、ロードバランサーとしても機能できる。この場合は、最もリソースを利用できるサ

ーバーへトラフィックが送られる。ディスク複製では、保護対象サーバーは、複製サーバーへ状況メッセージを送信する。保護対象サーバーが複製を停止するか、「危険状態」コールを送信した場合、複製コンピュータが保護対象サーバーの機能を自動的に引き継ぐ。複製が中止した場合、複製を開始する前に、保護対象サーバーとミラーリングサーバーとの間で再同期を行われなければならない。

緊急時対応計画コーディネーターは、2つのサイト間複製の実装を検討する場合、保護対象サーバーと複製サーバーのサポートインフラも検討しなければならない。適切なリソースを利用できる場合は、冗長な通信経路が提供される。緊急時対応計画コーディネーターは、複製されたコピーの破壊や、破壊されたディスクまたはデータからの複製などを含めた、ディスク複製の潜在的な短所を認識しなければならない。

記憶域の**仮想化**概念は、中央管理が可能なネットワークアプリケーション、オペレーションシステムおよび、ユーザーが単独のストレージプールとして扱われる、論理的かつ、仮想的ストレージデバイスにおける複数の物理的ストレージデバイスの組み合わせを行うプロセスである。記憶域の仮想化は、ネットワークのダウンタイムを必要とせずにストレージデバイスを追加できる。さらにダウンしたサーバーまたはストレージデバイスからの記憶域ボリュームを再割り当て、サーバーの割り当てた記憶域を、サーバーの要件に適合するよう、簡単に作成、削除、または拡張できるというメリットがある。仮想化テクノロジーは、**ネットワーク接続ストレージ**（NAS：Network-Attached Storage）環境を補完する。ネットワーク接続ストレージ環境はファイル指向であり、複数のサーバーに共通の記憶領域を提供する。ネットワーク接続ストレージ環境は、ファイル共有やWebおよびメールサービスなど、ファイルサーバーアプリケーションまたはストレージにとってメリットがある。また、ネットワーク接続ストレージデバイスまたはサーバーは、最小限のオペレーティングシステムで実行し、簡単にデータの移動ができるように設計されている。ファイル指向プロトコルを使用することにより、事実上どのオペレーティングシステムでも、あらゆるアプリケーションまたはあらゆるクライアントがデータをネットワーク接続ストレージデバイスへ送信したり、ネットワーク接続ストレージデバイスからデータを受信することができる。

仮想化テクノロジーは、**ストレージエリアネットワーク**（SAN：Storage Area Network）も補完することができる。これは、異なったオペレーティングシステムを搭載したコンピュータが、1台のストレージデバイスと通信できるようにする高速でパフォーマンスに優れたネットワークである。ネットワーク接続ストレージとは異なり、ストレージエリアネットワークは、ブロック単位でのデータアクセスを実現しており、ファイル指向トラフィックとは異なり、ストレージおよびバックアップトラフィックを処理するように構成されている。ストレージエリアネットワークは、ローカルでもリモート（限られた距離内）でも設置でき、通常、ファイバチャネルを介してサーバーと通信する。ストレージエリアネットワークソリューションは、データストレージをLANから切り離すため、バックアップデータを高速テープドライブへ送信できる。したがって、分散型または集中型のバックアップアーキテクチャとは異なり、ネットワークリソース

に影響を及ぼすことがない。仮想化、ネットワーク接続ストレージ、およびストレージエリアネットワークは、クライアント/サーバーアーキテクチャではなく、データ中心アーキテクチャに近づいている。システムマネージャが、データ中心アーキテクチャを導入することを検討している場合、このテクノロジーのメリットとデメリット、およびデータ中心ネットワークに対するシステムマネージャのニーズを考慮する必要がある。**iSCSI (Internet Small Computer System Interface)** は、ネットワーク接続ストレージおよびストレージエリアネットワークテクノロジーを補完するTCP/IPベースのストレージネットワーキング仕様である。iSCSIは、IPスタックのレイヤ上でネイティブなSCSIを転送するため、長距離ストレージの配備、管理、およびIPネットワーク上でのデータ転送が容易になっている。iSCSIは、IPネットワークに接続したすべての記憶域を、そのネットワークのどの地点からでもバックアップできるようになる。iSCSIでは、記憶域およびサーバーをあらゆる場所で追加でき、ストレージエリアネットワークとは異なり、距離による制限は受けない。

図5-1には、この項で説明したサーバーの緊急時対応策に関する可用性を位置づける相対的な尺度が示されている。高可用性とはデータの損失やサーバーのダウンタイムが分単位で見積もることができることを意味し、低可用性とはサーバーの復旧が完了するまでに数日を要する可能性があることを意味している。

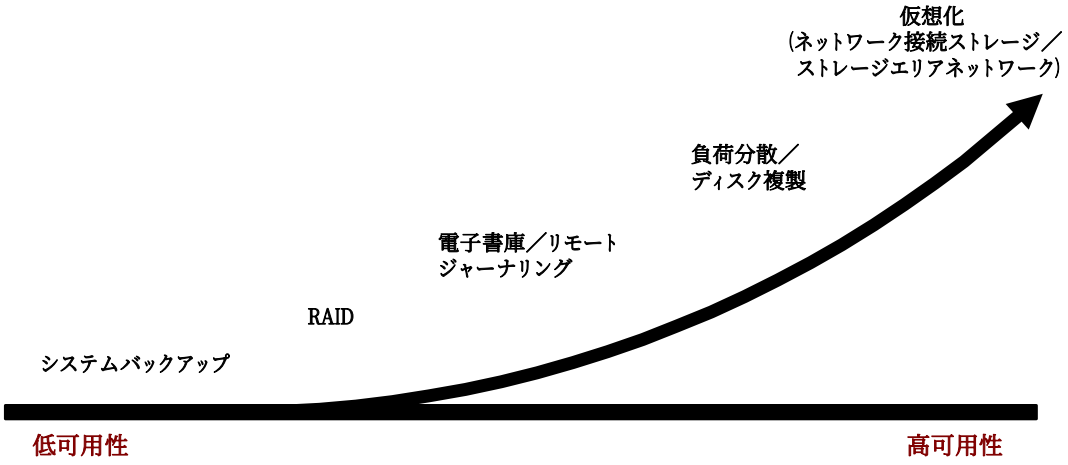


図5-1 サーバーの緊急時対応策と可用性

5.3 ウェブサイト

ウェブサイトは、World Wide Web（Web）または私設のイントラネットを介して、一般向けもしくは認証された個人に情報を与えるものである。外部のウェブサイトが電子商取引（eコマース）のポータルサイトになる場合もあり、組織は、ここを通じてインターネットでサービスを提供することができる。ウェブサイトは、企業ポリシー、人事フォーム、または従業員への電話帳などの情報を提供するために、組織内部で使用することができる。

ウェブサイトは、インターネットまたはイントラネット上での情報配信に使用される。ウェブサイトは、クライアントコンピュータのWebブラウザで読み取ることのできるハイパーテキストマークアップ言語（HTML）コードで作成される。ウェブサイトは、クライアントブラウザからの要求に対してWebページを提供するコンピュータ（Webサーバー）で管理される。Webサーバーは、ウェブサイトのコンポーネント（ページ、スクリプト、プログラム、マルチメディアファイルなど）を提供し、ハイパーテキストトランスファープロトコル（HTTP）を使用してそれらを送信する。ウェブサイトは静的なコンテンツでも動的なコンテンツでも提供できる。ウェブサイトは、組織の内部に置くことも（イントラネット）、インターネットを介して一般に公開することもできる。

5.3.1 緊急時対応計画での考慮事項

ウェブサイトの復旧戦略を決定する際には、第5.2項「サーバー」で示した情報に加え、いくつかの要素を考慮しなければならない。ウェブサイトの緊急時対応計画の実践には、次の手段が含まれる。

- **ウェブサイトの文書化** ウェブサイトの作成と運営で使用するハードウェア、ソフトウェア、およびそれらの設定を文書化しておく。

- **ウェブサイトのプログラミング** 他のアプリケーションと同様にウェブサイトは、公開前にテストサーバー上でテストされる必要がある。このとき、設定管理プログラムを点検し、変更箇所を適切に文書化しなければならない。承認済みのバージョンは、簡単な保存メディアであるCDに記録する必要がある。

- **ウェブサイトのコーディング** ウェブサイトは、IPアドレスを割り当てられたサーバー上で運営される。このIPアドレスは、ドメインネームサーバー（DNS）によって、ドメイン名つまり Uniform Resource Locator（URL）に対応付けられる。IPアドレスとドメイン名はランダムに割り当てることができるため、ウェブサイトは、コード（プログラム）内にIPアドレスまたはドメイン名を組み込まないほうがよい。ウェブサイトが別のサイトで復旧される場合、別のIPアドレスがサーバーに割り当てられることができるからである。ウェブサイトで、プログラムにハードコード化されたIPアドレ

ス、ドメイン名、またはドライブ文字が含まれている場合、システムの復旧が遅れる可能性がある。

・**緊急時対応策と適切なセキュリティポリシーおよびセキュリティコントロールとの整合性維持**
ウェブサイトは、ハッカーが組織のネットワークに侵入する入口となることが多い。したがって、Webサーバーとサポートインフラストラクチャは、強力なセキュリティコントロールで保護しなければならない。緊急時対応計画では、システムの復旧中にセキュリティが損なわれないように、これらのコントロールを調整しなければならない。したがって、攻撃を受けた後に再構築されたウェブサイトでは、適切なセキュリティコントロールとパッチが適用されなければならない。

・**緊急時対応策とインシデント対応手順との整合性維持** 外部に公開されるウェブサイトは、一般の人々に組織のイメージを植え付けるため、サイバー攻撃によってウェブサイトを書き換えられたり中傷されたりした場合、組織のイメージが悪くなってしまう。このような攻撃の影響を軽減するために、以下に挙げる緊急時対応策を、サイバーインシデントの影響を抑えるように設計されたインシデント対応手順と整合性をとる必要がある。

・ **事業影響分析の結果の使用** 関連する主要アプリケーションおよび一般サポートシステムの事業影響分析によって明らかになった影響および優先順位を検討して、関連要件を特定する必要がある。

5.3.2 緊急時対応策

ウェブサイトの緊急時対応策は、ウェブサイトとそのリソースの信頼性および可用性を確保するものでなければならない。コンテンツに変更のないWebページは、静的なページとみなされコンテンツが変更されるWebページは動的ページと呼ばれる。動的ページとは、クライアントとサーバーのどちらかまたは両方から開始された複数のトランザクションの結果である。動的ページで示されるコンテンツは、ファイアウォールで保護されたサーバーなど、ウェブサイト以外のサーバーに格納することができる。したがって、ウェブサイトでの緊急時対応策を選択する場合、ウェブサイトのサポ

ウェブサイトの緊急時対応策
- ウェブサイトの文書化
- ウェブサイトの適切なコード化、プログラミング、セキュリティポリシーおよびコントロールとの適合
- サポートインフラストラクチャの緊急時対応計画の考慮
- 負荷分散の導入
- インシデント対応手順との適合

ートインフラストラクチャを慎重に考慮する必要がある。サポートインフラストラクチャには、サーバー以外にもウェブサイトを提供するLANが含まれる。

ウェブサイトは受信処理するリクエスト数が多い。その一般的な緊急時対応策は**負荷分散**である。負荷分散では、Webトラフィックを少なくとも2台のサーバーに配分するクラスタアプローチを使用する。Webクラスタリングは、1台のサーバーがリクエストに応じているかのように見えるので、ユーザーが意識することはない。したがって、1台のサーバーに障害が発生した場合、トラフィックは別の稼働サーバーへ仕向けられる。負荷分散は、次の2つのアプローチで実施できる。

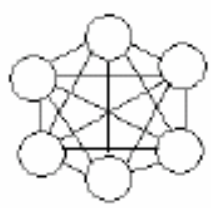
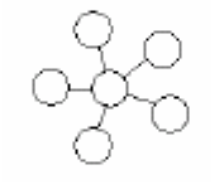
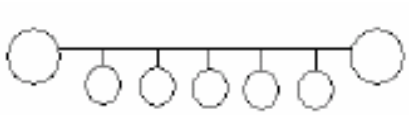
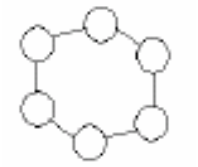
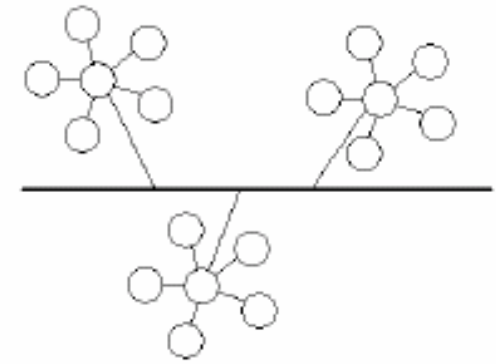
- **DNS** ユーザーがWebブラウザでURLを入力するとリクエストは、そのURLをIPアドレスに対応づけるDNSサーバーへ転送される。このIPアドレスはWebサーバーに割り当てられている。DNSサーバーは、続いてこのリクエストをいずれかのクラスタサーバーへ転送する。一般的なDNSアプローチの一例は、Berkeley Internet Name Daemon（BIND）によって用いられる「ラウンドロビン」方法である。

- **リバースプロキシ** リバースプロキシアプローチは、ブラウザのリクエストを一点に集約し、データのキャッシングを実行することにより帯域幅を軽減する。プロキシサーバーはクライアントとWebサーバー間に置かれ、クライアントのリクエストを受信しWebサーバーへ転送する。サーバーは、プロキシへレスポンスを返し、プロキシはこのレスポンスをリクエスト側のクライアントへ転送する。この方法では、1つのIPアドレスが必要になる。さらにトラフィックを分割する場合、1つのサブネットに負荷がかかり過ぎないようにするため、サーバーは別のサブネットに置かれることもある。さらに、ログは1か所に収集し監視することができる。これがリバースプロキシである。また、管理者は委任設定を定めることもできる。したがって、1台のコンピュータがクラッシュした場合、リバースプロキシの委任設定を再設定できる。この結果、クラッシュしたサーバーがリクエスト側のブラウザにエラーを返すことがなくなる。

5.4 ローカルエリアネットワーク（LAN）

LANは単一の組織が所有するものである。LANは、2台のPCを1台のハブに接続するような小さなものであったり、数百人のユーザーと複数のサーバーをサポートしている場合もある。表5-1に示すように、LANを設計する場合、複数のトポロジ（接続形態）が考えられる。

表5-1 LANトポロジ

トポロジ	図
メッシュ型 ネットワーク接続したコンポーネントは、ネットワークノード間で多数の冗長な相互接続で接続される。完全なメッシュトポロジでは、すべてのノードが、ネットワーク内における他のすべてのノードと接続されている。	
スター型 すべてのノードは中央のハブに接続する。	
バス型 すべてのノードは、バスまたはバックボーンと呼ばれる中央のケーブルに接続する。	
リング型 各ノードの両側にあるノード1個ずつに直接接続して、すべてのノードが閉じたループ状に互いに接続する。	
ツリー型 ツリーは、線形的なバスバックボーンで、複数のスター型ネットワークを接続した混成トポロジである。	

プロトコルは、ノード間通信を円滑に運ぶための、データ転送に関する取り決めの形式である。プロトコルは、送信側と受信側のノードのデータパケットの解釈の仕方を決定する。LANに実装されるネットワーク形態には、主要なネットワーク標準の1つであるイーサネット、トークンリングに加え、非

同期転送モード（ATM）、光ファイバー分散データインターフェイス（Fiber Distributed Data Interface（FDDI））がある。

また、LANは次の2つの主要なアーキテクチャで実装される。

- **ピアツーピア** - それぞれのノードは同等の機能と責任を持つ。たとえば、データを共有するためにハブを介し5台のPCをネットワーク接続する場合である。

- **クライアント/サーバー** - ネットワーク上の各ノードは、クライアントかサーバーのどちらかである。クライアントはPCの場合もプリンタの場合もあり、クライアントは、サーバーのリソースを信頼する。

LANのトポロジ、プロトコル、アーキテクチャ、およびノードは組織によって異なる。したがって、組織によって緊急時対応策は異なる。図5-2は、クライアント/サーバーのアーキテクチャとスター型トポロジで、イーサネットプロトコルを実行するLANを示している。このLANは、5台のデスクトップコンピュータ、1台のサーバー、1台のネットワークプリンタ、1台のローカルデスクトッププリンタ、および公衆交換電話網を使用したサーバーへのダイヤル回線アクセスから構成されている。

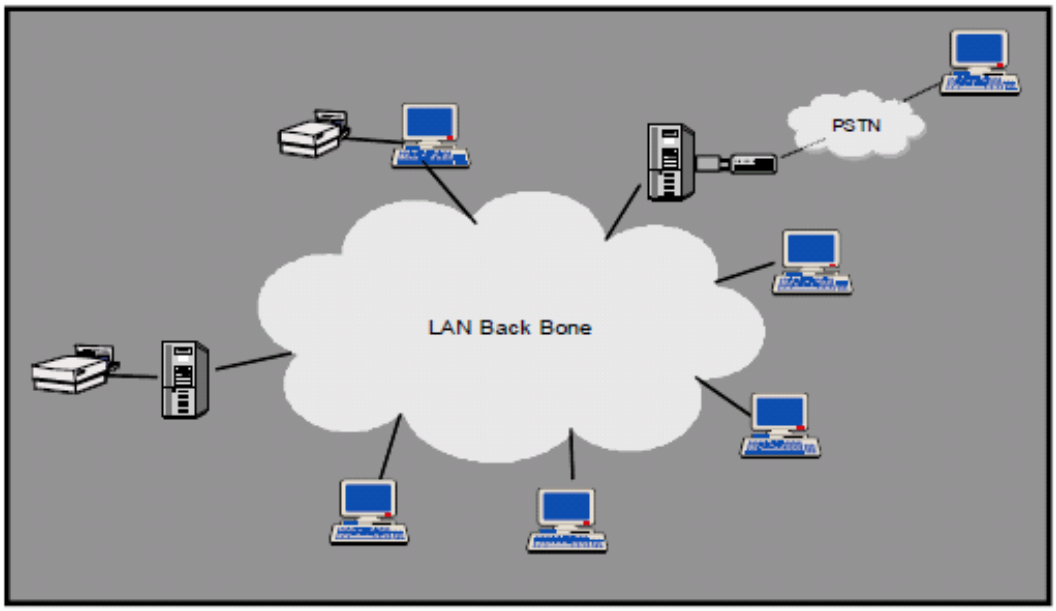


図5-2 ローカルエリアネットワーク

5.4.1 緊急時対応計画での考慮事項

LAN復旧戦略を策定する場合、緊急時対応計画コーディネーターは、第5項前半ですでに説明したデスクトップ、サーバー、およびウェブサイトに関する情報に従う必要がある。さらに、次の措置を考慮する必要がある。

- **LANの文書化** LANの物理的および論理的配置図は、最新のものにしておかなければならない。物理的な配置図では、LANを設置した施設の物理的なレイアウトを図示し、ケーブルジャック番号を物理的な配置図に記載する必要がある。論理的な配置図では、LANとそのノードを記載する必要がある。ネットワーク検出ソフトウェアを使用すれば、LANの正確な構成を取得できる。両方の配置図があれば、復旧要員がLANサービスの復旧を迅速に行う場合に役立つ。

- **システム構成とベンダー情報の文書化** 復旧を円滑に行うために、LAN通信で使用するネットワーク接続デバイス（スイッチ、ブリッジ、ハブなど）の構成を文書化しておく。また、ハードウェアおよびソフトウェアの再供給を迅速に手配できるように、ベンダーおよびその連絡先情報を、緊急時対応計画に文書化しておく必要がある。

- **セキュリティポリシーおよびセキュリティコントロールへの適合** LAN緊急時対応ソリューション緊急時対応策は、ネットワークの混乱を招く恐れのある脅威から保護するために、ネットワークセキュリティポリシーに適合させる必要がある。したがって、LANに関する適切な技術的な緊急時対応策を選択する場合には、ネットワークの中断時に、技術的な緊急時対応策を実施することで機密データの改ざんや漏洩が発生しないように、本番システムと同様のセキュリティコントロールおよびセキュリティ関連の活動（リスクアセスメントや脆弱性検査など）を、緊急時対応策に導入する必要がある。

- **事業影響分析結果の使用** 関連する主要アプリケーションおよび汎用サポートシステムの事業影響分析によって明らかになった影響および優先順位を検討して、LAN復旧の優先順位を特定する必要がある。

5.4.2 緊急時対応策

LAN緊急時対応計画を策定する場合、緊急時対応計画コーディネーターは、事業影響分析で説明する重要なシステムまたはプロセスに影響する**単一障害点**を特定する必要がある。この分析には、ケーブルの切断、電磁および無線周波数による妨害、火災や水害などの災害被害など、**ケーブルシステム**に対する脅威が含まれる。解決策として、適宜、冗長性のあるケーブルを設置することができる。たとえば、予備ケーブルをデスクトップに配備しただけではコスト効率が良くなるわけではないが、階と階の間に100Mbitケーブルを配備して、主ケーブルが切断した場合に両方の階のホストが再接続できるように備えれば、コスト効率は良くなると考えられる。

各コンピュータジャックに予備ケーブルを配線しても、多くの場合コスト効率は良くならない。ただし、それぞれのデスクトップジャックには通常、少なくとも1つの電話用ジャックとコンピュータ用ジャックが備えられている。組織でケーブルを配備する場合、データまたは電話用の予備ジャックを、数か所に1つずつ設けるという方法がある。このようにすると、ケーブル配線に問題が生じた場合、近くにある予備ジャックをバックアップとして使用できる。この場合、デスクトップから予備ジャックまで一時的にケーブルを接続すれば、新しいケーブルが、問題のあったジャックに再接続できるようになるまで、デスクトップの接続を確保できる。また、電話システムの接続ブロックが、バックボーンハブとして同じ場所にある場合、電話用ジャックが十分な帯域幅を確保できるならば、電話用ジャックをデータ用ジャックに簡単に変換できる。

緊急時対応計画では、ハブ、スイッチ、ルーター、ブリッジなどの**ネットワーク接続デバイス**も考慮する必要がある。事業影響分析では、ネットワーク内で果たす各デバイスの役割を記述する必要があり、事業影響分析の重要度に基づいて、緊急時対応策をデバイスごとに作成する必要がある。ネットワーク接続デバイスの緊急時対応戦略の例としては、冗長性のあるインテリジェントネットワークルータをネットワークに導入するという方法がある。これによって、ルーターに障害が発生した場合に、他のルーターがすべてのトラフィック負荷を引き継ぐことができるようになる。

LANの緊急時対応策
- LANの文書化
- ベンダーとの調整
- セキュリティポリシーおよびコントロールとの適合
- 単一障害点の特定
- 重要なコンポーネントにおける冗長性の実装
- LANの監視
- リモートアクセスおよび無線ローカルエリアネットワークテクノロジーの統合

リモートアクセスは、LAN上のサーバーとデバイスによってもたらされるサービスである。リモートアクセスは、オフサイトで作業するユーザーに利便性をもたらしたり、サーバーとデバイスがサイト間で通信する手段を提供する。リモートアクセスは、ダイヤルアップアクセスや仮想プライベートネットワーク（VPN）などのさまざまな方法で実施できる。緊急事態や重大なシステムの中断が生じた場合、リモートアクセスは、復旧チームまたはユーザーが別の場所から組織全体のデータにアクセスできるようにすることで、重要な緊急時対応機能として役立つ。リモートアクセスを緊急時対応戦略として確立する場合、データの帯域幅要件を特定し、リモートアクセスソリューションの評価に使用する必要がある。さらに、通信に機密情報が含まれる場合は、ワンタイムパスワードやデータの暗号化などのセキュリティコントロールを導入する必要がある。

無線ローカルエリアネットワークは、有線LANの障害発生後にネットワークサービスを復旧する、効果的な緊急時対応策として役立つ。無線ネットワークは、従来のLANのケーブルインフラストラクチャを必要としないため、一時的または永続的なソリューションとして手早く導入できる。ただし、無線ネットワークは、無線信号でデータを送信するため、データを傍受される可能性が生じる。無線ネットワークを導入する場合、通信トラフィックに機密情報が含まれるならば、データの暗号化などのセキュリティコントロールを導入する必要がある。

迅速な検知によりLAN破損の影響を軽減するためには、**監視ソフトウェア**の導入が有効である。監視ソフトウェアは、ノードに障害が発生し始めたり応答しなくなると警告を発する。監視ソフトウェアはトラブルの検知を促進し、多くの場合、ユーザーや他のノードが問題を認識する前に、管理者へ警告を与える。多くのタイプの監視ソフトウェアは、システムパラメータがその指定範囲から外れた場合、指定した個人に電子伝言を自動的に送信するように設定できる。

5.5 ワイドエリアネットワーク

ワイドエリアネットワーク（WAN）は、広範な地域に存在する2つ以上のLANから構成されるデータ通信網である。通常、公衆通信事業者（プロバイダ）が提供する通信リンクによって、1つのLANが他のLANとやり取りできるようになる。

LANを接続する以外にも、WANは別のWANに接続したり、LANをインターネットに接続することができる。WAN通信リンクのタイプには次の方法がある。

- **ダイヤルアップ** モデムを介したダイヤルアップ接続では、常設でない接続を介して最小のデータ転送を実現する。速度は、使用するモデムによって異なるが、最高56kbps（キロバイト毎秒）である。
- **統合サービスデジタル通信網（ISDN）** ISDNは、音声、映像、およびデータを、デジタルまたは標準の電話回線を通じて送信する国際的な通信規格である。ISDNは、64または128kbps程度の転送転送をサポートしている。

- **T-1** T-1は専用電話接続であり、1.544Mbpsのデータ速度をサポートする。T-1回線は、24本の64kbpsチャネルから構成され、チャネルごとに音声またはデータ信号を送信するように設定できる。T-1に満たないアクセスについても、64kbps回線の倍数であれば提供される。

- **T-3** T-3は専用電話接続であり、約43Mbpsのデータ速度をサポートする。T-3回線は、672本のチャネルから構成され、それぞれが64kbpsをサポートする。T-3は、DS3とも呼ばれている。

- **フレームリレー** フレームリレーは、WAN上のデバイスを接続するためのパケットスイッチングプロトコルである。フレームリレーでは、データは仮想回線上で転送される。フレームリレーネットワークは、T-1およびT-3のデータ転送速度をサポートする。

- **ATM** ATMは、固定サイズのパケットを使用して高速でデータを転送するネットワークテクノロジである。ATMのインプリメンテーションは、25から622Mbpsのデータ転送速度をサポートし、保証付きのスループットを提供する。

- **同期式光ネットワーク（SONET）** SONETは、光メディアでの同期データ転送規格である。SONETは、ギガビット転送速度をサポートしている。

- **無線** 無線LANブリッジは、複数のLANを接続することで、WANを構成する。無線は、直線距

離にして20から30マイルの距離をサポートする。

・ **仮想プライベートネットワーク（VPN）** VPNは、インターネット上のノード間での暗号化されたチャネルである。

図5-3には、本社のLANと、2つの支社のLANをリンクさせた企業でのWANを表している。このWANでは、インターネットへのリンクも確保している。

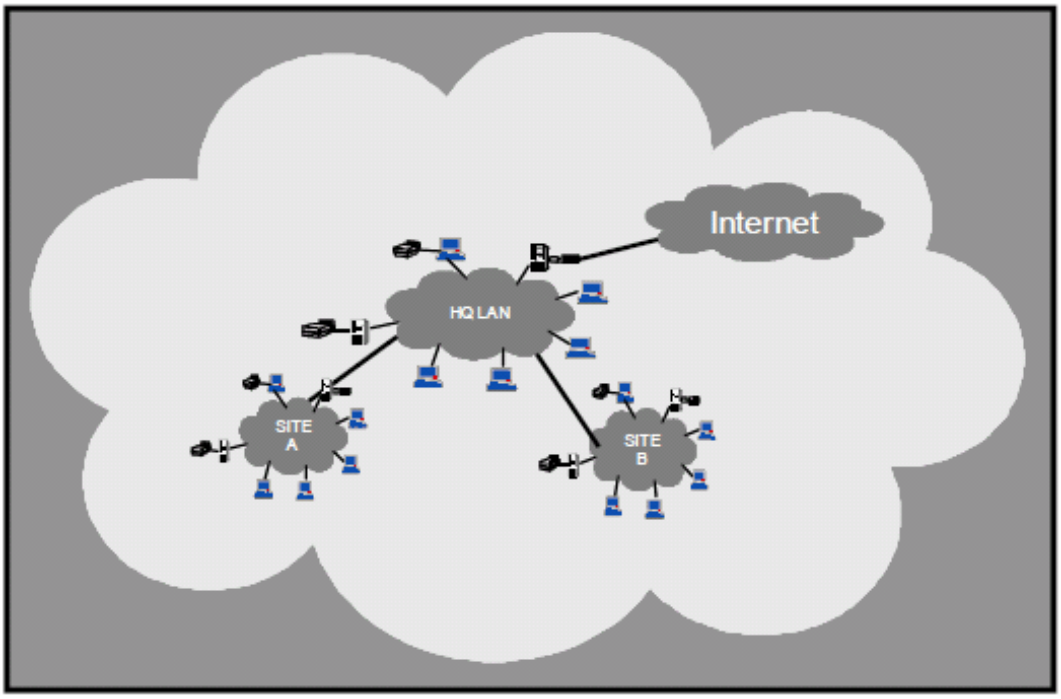


図5-3 ワイドエリアネットワーク

5.5.1 緊急時対応計画での考慮事項

WANの緊急時対応計画での考慮事項は、障害後にWANサービスを復旧する復旧要員の能力に重点を置く必要がある。以下に挙げた措置は、第5.5.2項でのWAN復旧戦略を補完し、全体的なWANの緊急時対応能力をもたらすものである。

- **WANの文書化** WANアーキテクチャ構成図は最新のものにしておく必要があり、ネットワーク接続デバイス、装置のアドレス（IPアドレス）、および通信リンクおよびベンダーのタイプを明記しておく必要がある。

WAN緊急時対応策
- WANの文書化
- ベンダーとの調整
- セキュリティポリシーおよびコントロールへの適合
- 単一障害点の特定
- 重要なコンポーネントにおける冗長性の導入
- SLAの設定

- **システム構成とベンダーの文書化** WAN通信を容易に復旧できるよう、メディアアクセス装置の設定を文書化しておく。緊急時対応計画には、障害発生後にハードウェアやソフトウェアなどのWANコンポーネントを迅速に交換できるように、ベンダーのリストを含める必要がある。また計画では、連絡担当窓口や連絡先情報など、通信プロバイダについても文書化しておく必要がある。

- **セキュリティポリシーおよびセキュリティコントロールへの適合** WAN緊急時対応ソリューション緊急時対応策は、ネットワークの可用性を損なう恐れのある脅威から保護するために、ネットワークセキュリティポリシーに適合させる必要がある。したがって、適切で技術的な緊急時対応策を選択する場合は、WANの接続障害時に、技術的な緊急時対応策を実行して機密データの改ざんや漏洩が発生しないように、本番環境と同様のセキュリティコントロールおよびセキュリティ関連の活動（リスクアセスメントや脆弱性検査など）を、緊急時対応策に導入する必要がある。

- **事業影響分析結果の使用** 関連する主要アプリケーションおよび汎用サポートシステムの事業影響分析によって明らかになった影響および優先順位を検討して、関連要件を特定する必要がある。

5.5.2 緊急時対応策

WANの緊急時対応策には、PC、サーバー、ウェブサイト、およびLANについて説明したすべての対策を含める必要がある。さらに、WAN緊急時対応計画では、異なる形態のLANを接続するための通信リンクを考慮しなければならない。WAN緊急時対応戦略は、ネットワークで転送するデータのタイプによって影響を受ける。ミッションクリティカルな分散システム（第5.6項参照）を提供するWANは、単にリソースを共有する目的で複数のLANを接続するWANよりも、堅固な復旧戦略を必要とする場合がある。組織は、WANの可用性を確保するために、次の緊急時対応策を考慮しなければならない。

- **冗長性のある通信リンク**　冗長性のある通信リンクは、通常、ネットワークが重要なデータを処理する場合に必要である。冗長リンクは、2つのT-1接続のように同じタイプで構成される場合もあるが、緊急事態時に重要な転送だけに対応できるように、限られた帯域幅を提供するバックアップリンクの場合もある。たとえば、ISDN回線は、プライマリ回線であるT-1接続の緊急事態用の通信リンクして使用することができる。緊急時対応計画コーディネーターは、冗長性のあるリンクを使用する場合、そのリンクが物理的に分離されており、同じ経路を通らないことを確認する必要がある。そうでなければ、ケーブルの切断などの単独インシデントによって、両方のリンクが影響を受けてしまう場合があるためである。

- **冗長性のあるネットワークサービスプロバイダ**　100パーセントのデータ可用性が必要な場合は、複数のネットワークサービスプロバイダ（NSP）を利用することにより、冗長性のある通信リンクを確保できる。このソリューションを選択する場合、管理者は、（複数の）ネットワークサービスプロバイダが、ビルの入口や境界を含むあらゆる地点で、共通の施設を共有していないことを確認する必要がある。

- **冗長性のあるネットワーク接続デバイス**　ルータ、スイッチ、ファイアウォールなどのネットワーク接続デバイスを二重化しておくことで、LANインターフェースでの可用性が高くなり、1つのデバイスに障害が発生した場合に対しても冗長性が得られる。また、二重化したデバイスにより、通過トラフィックの負荷分散も提供される。

- **ネットワークサービスプロバイダまたはインターネットサービスプロバイダによる冗長性**　緊急時対応計画コーディネーターは、その中核となるネットワークの堅牢性と信頼性を評価するために、選択したネットワークサービスプロバイダまたはインターネットサービスプロバイダを参考にする（冗長性のあるネットワーク接続デバイスや電源の保護など）。

独立したインターネット接続を2つの地理的に離れたLANから確立することで、より冗長性を高め

ることができる。一方の接続に障害が発生しても、もう一方の接続を通じて、インターネットトラフィックを転送できる。ただし、この戦略は、セキュリティと可用性との間で調和が取れていなければならない点が問題になる。インターネット接続が複数になれば、ハッカーに対するネットワークの脆弱性が増大する。したがって、前述したように、緊急時対応戦略は、どのような場合でも、セキュリティ上の考慮事項に照らして慎重に考慮しなければならない。

SLAは、ネットワークに関連したソフトウェアまたはハードウェアの問題が発生した後の迅速な復旧に役立つ。SLAは、ネットワークサービスプロバイダまたは、インターネットサービスプロバイダと共に作成されることもありベンダーのネットワークが利用不可能な場合に、目的とするネットワークの可用性を保証し、料金設定を行う。ネットワークサービスプロバイダまたはインターネットサービスプロバイダが、ルーターなどのネットワーク接続デバイスを提供する契約である場合、これらのデバイスの可用性はSLAに含まれる。

5.6 分散システム

分散システムは、クライアントおよびユーザーが広範囲に分散している環境で導入される。これらのシステムは、LANおよびWANリソースに基づいてユーザーのアクセスを可能にしているが、分散システムの構成要素には、中断および処理エラーを防止するための同期化および調整が必要である。複数の地域にまたがった連邦政府全体のビジネス機能をサポートしている大規模なデータベース管理システム（DBMS）は、一般的な分散システムの形態である。このタイプのアプリケーションでは、データはそれぞれのサーバー間で複製され、ユーザーは自身のローカルサーバーからシステムにアクセスする。

分散システムは、複数の独立した処理要素を相互接続した集合体であり、単独のビジネス機能を遂行するためにデータを交換し処理するように構成されている。ユーザーからすると、分散システムが単独のソースのように見える。分散システムでは、クライアント/サーバー関連モデルを使用して、異なる立地のユーザーに対し、アプリケーションのさらなるアクセス性をもたらす。

5.6.1 緊急時対応計画での考慮事項

分散システムにおける緊急時対応計画での考慮事項は、これまでのプラットフォームに関して論じてきた概念を描くものである。分散システムは広範囲にわたってローカルおよびワイドエリアネットワークの接続性に根ざしたものであり、分散システムの緊急時対応手段は、LANおよびWANについて説明してきた対策と類似している。

- **ハードウェア、ソフトウェア、および周辺機器の標準化** ハードウェア、ソフトウェア、および周辺機器が分散システム全体で標準化されていれば、迅速にシステム復旧を行うことができる。標準的な設定が指定され、リソースが共有されるため、復旧のコストは軽減される。また、コンポーネントの標準化により、組織全体でのシステムの保守も軽減される。

- **システム構成とベンダー情報の文書化** 分散システムのアーキテクチャとそのさまざまなコンポーネントの構成を文書化する。さらに、緊急時対応計画では、破損後の機器を効率よく迅速に交換できるように、ベンダー情報とモデル仕様を明記しておく必要がある。

- **セキュリティポリシーおよびセキュリティコントロールへの適合**　分散システムの緊急時対応策は、ネットワークセキュリティポリシーに適合させる必要がある。この場合、システムの中断に対して、技術的な緊急時対応策を実行することにより、機密データの改ざんや漏洩が引き起こされないように、本番環境と同様のセキュリティコントロールおよびセキュリティ関連活動（リスクアセスメントや脆弱性検査など）を、緊急時対応策に導入する必要がある。

- **事業影響分析結果の使用**　関連するLANまたはWANあるいはその両方の事業影響分析によって明らかになった影響および優先順位を検討して、復旧要件と優先順位を検討する必要がある。

5.6.2 緊急時対応策

分散システムは複数の地域に広がっているため、システムおよびそのサポートインフラストラクチャに対するリスクは、事業影響分析プロセスで徹底的に分析する必要がある。上述のように、分散システムの緊急時対応戦略は、一般的にシステムがLANおよびWANの可用性に依存していることを反映している。この事実に基づけば、分散システムの緊急時対応戦略を策定する場合、LANおよびWANで扱われていた次のテクノロジーを考慮しなければならない。

- システムバックアップ
- RAID
- 重要なシステムコンポーネントの冗長性
- 電子書庫およびリモートジャーナリング
- ディスク複製
- 仮想化、ネットワーク接続ストレージ、またはストレージエリアネットワーク
- リモートアクセス
- 無線ネットワーク

分散システムの緊急時対応策
- コンポーネントの標準化
- システムの文書化
- ベンダーとの調整
- セキュリティポリシーおよびコントロールへの適合
- サーバーの緊急時対応策の考慮
- LANの緊急時対応策の考慮
- WANの緊急時対応策の考慮

・ LANケーブルシステムの冗長性

・ WAN通信リンクの冗長性

緊急時対応策は、分散システムの設計および実装を行う際に、システムへ組み込むことができる。たとえば、すべてのデータを1つの場所（組織の本社など）に置き、ローカルサイトに複製するように、分散システムを構築することができる。ローカルサイトでの変更については、本社で複製が行われる。データが読み取り専用としてローカルサイトに複製される場合、分散システムでのデータは、各ローカルサイトでバックアップされる。これはつまり、本社のサーバーに障害が発生した場合でも、WANを介して、ローカルサイトのデータにアクセスできるということである。これとは反対に、データが、ローカルサイトから本社のサイトへ毎時間アップロードされている場合は、本社のサーバーは、ローカルサーバーのバックアップとして機能することになる。

上記の例で示すように、分散システムには緊急時対応戦略に組み込むことのできる特有の冗長性を提供する。たとえば、政府機関執行部とその小規模ローカルオフィス間において分散している重要なシステムがその例である。データを両方のサイトで複製していると仮定すると、費用対効果の高い復旧戦略は、2つのサイト間における相補合意を行うことである。この合意に基づくと、1つの事務所で障害が起きた場合、もう一方の事務所へ重要な要員を再配置して、システムを継続して機能することができる。この戦略は、代替サイトの調達、装備の必要がなくなるため、緊急時対応コストを大幅に節約できる。

5.7 メインフレームシステム

クライアント/サーバーアーキテクチャとは異なり、メインフレームアーキテクチャは集中化されている。メインフレームにアクセスするクライアントは、処理能力を持たない「ダム」ターミナルである。ダムターミナルは、メインフレームからの出力のみを受け取る。ただし、PCも、ターミナルエミュレーションソフトウェアを使用することによって、メインフレームにアクセスできる。

メインフレームは、大規模組織でのコンピューティングニーズを満たすように設計されたマルチユーザーコンピュータである。この用語は、1950年代後半および1960年代に開発された、大量のアカウンティングおよび情報管理機能を処理する大型の中央コンピュータを示すために生み出されたものである。メインフレームシステムは、分散システムとは異なり、複数のコンピュータにデータを分散させるのではなく、中央の場所にすべてのデータを格納する。

5.7.1 緊急時対応計画での考慮事項

メインフレームコンピュータは、これまで取り上げてきたプラットフォームよりも大型で高性能だが、緊急時対応要件に関して共有するところが多い。メインフレームは集中型のアーキテクチャを使用するため、分散システムまたはネットワークが本来備えている冗長性を持っていない。このため、メインフレームの可用性およびデータのバックアップが重要になる。メインフレームの緊急時対応要件の決定時には、次の対策を考慮する必要がある。

メインフレームの緊急時対応策
- データのバックアップとオフサイトでの保管
- システムの文書化
- ベンダーとの調整
- セキュリティポリシーおよびコントロールへの適合
- 重要なシステムコンポーネントにおける冗長性とフォールトトレランスの実装
- ホットサイトまたは相補合意の考慮
- ベンダーのSLAの設定
- データの複製
- ストレージソリューションのインプリメント
- 無停電電源装置の使用考慮

- **オフサイトでのバックアップメディアの保管** バックアップメディアは、環境管理された安全なオフサイト施設で、ラベル付け、記録、保管が行われる必要がある。ストレージ施設は、両方のサイトが同じ障害によって影響を受ける可能性を低減するため、元のサイトから十分に離れた場所に設けなければならない。

- **システム構成およびベンダーの文書化** システム構成を詳細に記録しておくことで、システム復旧能力を増強する。さらに、基本的なハードウェア、ソフトウェア、および他のコンポーネントを供給するベンダーを、緊急時対応計画に明記しておく必要がある。

- **ネットワークセキュリティポリシーおよびシステムセキュリティコントロールへの適合** メインフレームの緊急時対応策は、厳格なアクセスコントロールなどのネットワークセキュリティポリシーへ適合させる必要がある。ネットワークセキュリティコントロールは、メインフレームの可用性を損なう可能性のある攻撃から保護するために有効である。

- **事業影響分析結果の使用** 関連する主要アプリケーションおよび一般サポートシステムの事業影響分析によって明らかになった影響と優先順位を判断して、復旧要件と優先順位を検討する必要がある。

5.7.2 緊急時対応策

メインフレームでは、データが単一の場所に格納されるため、分散システムとは異なる緊急時対応策が必要になる。まず、メインフレームのデータストレージ機能と基本的なアーキテクチャに重点を置く必要がある。**冗長性のあるシステムコンポーネント**は、電源などのシステムコンポーネント障害によって、システムの障害が発生しないようにするために重要である。電力の変動によってメインフレームが影響を受けないようにするため、UPSと電源の監視および管理システムも用いる。メインフレームは通常、大規模で重要なアプリケーションを扱うため、**長時間のバックアップ電力**ソリューションが必要になる場合がある。ガソリンまたはディーゼル発電機を用いることにより、停電によるメインフレーム処理の中断を防止できる。

また、RAIDソリューションを導入することにより、DASDにディスクの冗長性がもたらされる。

それぞれのメインフレームのアーキテクチャは独特で、集中化されているため、緊急時対応戦略は、代替ウォームサイトまたはホットサイトで利用できる代替用システムを保有しなければならない。ただし、バックアップメインフレームのプラットフォームは、購入および保守に非常にコストがかかるため、多くの連邦政府が商用システムを共有している。[31]また、通常、損傷を受けた装置の修理に関して、ベンダーとサポート契約を結んでいる。ただし、ベンダーのサポートだけでは、許容可能な中断時間以内にシステム機能を復旧することはできない。どのような場合でも、システムの可用性要件を満たすために適切なサポートをベンダーが確実に提供できるように、**ベンダーのサービスレベル契約**を最新のものにし検討することが必要になる。

メインフレームは、定期的に**バックアップ**を行い、バックアップメディアは、オフサイトで保管する。バックアップおよび保有スケジュールは、処理されているデータの重要性と、そのデータを変更する頻度に基づいて決定する（バックアップソリューションについては、第5.2.2項の「緊急時対応策」を参照のこと）。サーバーの場合と同様に、別のサイトへのリモートジャーナリングまたは電子書庫は、効果的な技術的緊急時対応策である。さらに、さまざまなプラットフォームを1つの複製サーバーへ複製するディスクの複製、仮想化、ネットワーク接続ストレージ、またはストレージエリアネットワークテクノロジーが用いられる場合もある。

---

[31] 一般調達局の連邦テクノロジーサービスである連邦コンピュータ取得センターは、連邦政府を代表して、政府機関全体の取得契約を結んでいる。本プログラムは、1993 年に施行され、40 以上の連邦組織に災害回復サービスを提供している。

5.8 技術的な緊急時対応計画での考慮事項の要約

IT緊急時対応計画では、緊急時対応計画コーディネーターは、システム復旧戦略を計画するときに、次の2つの観点から、技術的な対策を考慮する必要がある。

- 緊急時対応での考慮事項では、緊急時対応策を補完する技術的要件または要素を取り上げる。

- 緊急時対応策は、技術的な基盤の上に作成され、緊急時対応戦略を導入するために使用される。

表5-2では、第5.1項から第5.7項および、関連するITプラットフォームで特定したすべての緊急時対応計画での考慮事項および解決策を要約する。緊急時対応計画での考慮事項およびソリューションは最高レベルのものを表示するが、すべてを含んだリストは表示しない。システムは組織によって異なるため、緊急時対応計画コーディネーターは、事業影響分析の結果を使用して、各ITシステムを評価しなければならない。その際、どの考慮事項と解決策が適切かというだけでなく、ここに示されていないか、あるいは他のITプラットフォームの考慮事項および解決策が適用できるかどうかについて判断する必要がある。

表5-2 緊急時対応戦略の要約

	デスクトップコンピュータとポータブルシステム	サーバー	ウェブサイト	ローカルエリアネットワーク	ワイドエリアネットワーク	分散システム	メインフレームシステム
緊急時**対応計画での考慮事項**[32]							
システム、設定、およびベンダー情報の文書化	×	×	×	×	×	×	×
各ユーザーに対するデータのバックアップの奨励	×						
適切なコード化、プログラミング、および文書化			×				
緊急時対応策とセキュリティポリシーとの整合性維持	×	×	×	×	×	×	×
緊急時対応策とシステムセキュリティコントロールとの整合性維持	×	×	×	×	×	×	×
サポートインフラストラクチャの緊急時対応の考慮			×			×	
ホットサイトと相補合意の考慮							×
インシデント対応手順への適合			×				
ベンダーとの調整				×	×	×	×
ベンダーとのSLAの設定					×		×
パーソナルコンピュータ上のデータの保存に関するガイダンスの提供	×						
ハードウェア、ソフトウェア、および周辺機器の標準化	×	×				×	
オフサイトでのバックアップメディアの保管	×	×					×
オフサイトでのバックアップの保管	×	×					
緊急時対応策[33]							
システム、アプリケーション、およびデータのバックアップ	×	×					
コンポーネント間の相互運用性の確保	×	×					
単一障害点の特定				×	×		
イメージディスク	×						
重要なコンポーネントにおけるフォールトトレランスの導入		×					×
負荷分散の導入		×	×				
重要なコンポーネントにおける冗長性の実装	×	×		×	×		×
ストレージソリューションの導入		×					×
リモートアクセスと無線テクノロジーの統合				×			
監視				×			
データの複製		×					×
代替ハードディスクドライブの使用	×						
無停電電源装置の使用	×	×					×

---

[32] 緊急時対応計画での考慮事項では、緊急時対応策を補完する技術的要件または要素を取り上げる。

[33] 緊急時対応策は技術的な基盤の上に作成され、緊急時対応戦略を導入するために使用される。

付録一覧

付録A
IT緊急時対応計画のフォーマット例

このフォーマット例は、情報技術（IT）緊急時対応計画を準備するためのテンプレートである。このテンプレートはガイドとして使用するように考えられており、緊急時対応計画コーディネーターは、システムの緊急時対応要件に適合し組織内のポリシーに準拠するよう、必要に応じてこのフォーマットを修正する必要がある。ガイドでは可能な箇所では、特定の項目を満たすのに必要な手順も示している。特定の項目には説明文が追加されているが、その情報は、その項に登場する情報を補足することを目的としている。このテキストはすべての組織に適合するものではないので、特定の連邦政府およびシステムの考慮事項を満たすように修正する必要がある。また、IT緊急時対応計画は、「公式使用限定」などのセキュリティラベルを付けなければならない。

1. はじめに

1.1 目的

この｛システム名｝の緊急時対応計画では、障害発生後に｛システム名｝を復旧する手順を定めている。この計画の目標は、次のように定められている。

・ 次のフェーズから構成され確立された計画を通じて、緊急時対応措置の有効性を最大化する。

  - **通知/実行フェーズ**（損害の検出と評価を行い、計画を実行性のあるものとする）

  - **復旧フェーズ**（一時的にITシステム運用を復旧し、元のシステムが受けた損害を復旧する）

  - **再構築フェーズ**（ITシステム処理機能を通常運用に戻す）

・ 通常業務が長期的に中断している間、｛システム名｝の処理要件の実行に必要な活動、リソース、および手順を特定する。

・ ｛組織名｝の指定された要員に責任を割り当て、通常業務の長期にわたる中断の間に｛システム名｝を復旧するガイダンスを提供する。

・ 緊急時対応計画戦略に関わる他の｛組織名｝スタッフとの協力を確保する。緊急時対応計画戦略に関わる外部の連絡先およびベンダーとの協力を確保する。

1.2 適用範囲

｛システム名｝の緊急時対応計画は、第一所在地（州、市）にある｛組織名｝の｛システム名｝の運用を復旧し再開するための必要な機能、運用、およびリソースに適用される。｛システム名｝の緊急時対応計画は、第2.3項「責任」で明記する｛組織名｝と｛システム名｝に関連したその他のすべての人員に適用される。

緊急時対応計画の｛システム名｝は、計画の目的を提供する｛計画名｝によって裏付けられるものである。また、この計画で要約される手順は、計画の目的を提供する｛計画名｝を調整し、｛計画名｝を裏付けるものである。

1.3 範囲

1.3.1 計画の原則

計画の基礎を作成するために様々なシナリオが考慮され、数々の想定条件が作成された。この計画の適用範囲は、2つの主要原則を前提としている。

・ 州、市における｛組織名｝の施設は利用できなくなっている。したがって｛組織名｝はその部署のため、｛システム名｝の処理を実行できない。

・ ｛組織名｝の代替運用施設として、州、市を指定する代替サイトとの有効な契約が取り交わされている。

- ｛組織名｝は、緊急事態のために元の施設が利用できない間、代替サイトの建物およびITリソースを使用して、｛システム名｝の機能を復旧する。

- 代替サイトにおける指定のコンピュータシステムは、｛システム名｝の情報処理を開始するように設定されている。

- 代替サイトは、通常業務に復帰するまでのシステムに障害が発生している間、｛システム名｝の復旧と処理を継続するために使用される。

1.3.2 想定条件

以上の原則に基づいて、IT緊急時対応計画を策定する際に、次の条件を前提とする。

・ {システム名}は、{組織名}のコンピュータセンターで動作不能になっており、48時間以内に復旧することができない。

・ {システム名}の主要な要員は決まっており、自組織の緊急事態での対応と復旧のための役割に関してトレーニングを受けている。彼らは、{システム名}の緊急時対応計画の対応が可能である。

・ 予防的コントロール（発電機、環境制御、防水シート、スプリンクラーシステム、消化器、消防署の支援など）は、災害時に十分に機能する。

・ {システム名}をサポートするコンポーネントなどのコンピュータセンター機器は、停電時に45分から1時間の電力を供給する無停電電源装置（UPS）に接続されている。

・ {組織名}のサイトに設置された{システム名}上のハードウェアおよびソフトウェアは、最低48時間利用できなくなる。

・ アプリケーションソフトウェアおよびデータの最新バックアップは破損しておらず、オフサイト施設で利用できる。

・ {システム名}の運用に必要な機器、接続、および機能は、州、市の代替サイトでも利用できる。

・ {システム名}のハードウェア、ソフトウェア、および通信プロバイダとの間で、緊急事態におけるシステム復旧をサポートするサービス契約が取り交わされている。

{システム名}の緊急時対応計画は、次の状況には適用されない。

・ **業務の全体的な復旧と継続性**　事業復旧計画と運用継続計画を、本計画に付け加える。

・ **緊急事態での人員の引き揚げ**　人員緊急時計画を、本計画に付け加える。

・ *他に制約があれば、本リストに追加する。*

1.4 参照/要件

この｛システム名｝の緊急時対応計画は、次のように｛組織名｝のIT緊急時対応計画ポリシーに準拠する。

組織は、中断が72時間以上に及ぶ場合の、重要なサポート業務のニーズを満たす緊急時対応計画機能を開発する。このような機能を実行するための手順は、公式的な緊急時対応計画で文書化し、最低1年に一度再検討して、必要に応じて更新する。また、対象システムの責任担当者が、緊急時対応手順を実行できるためのトレーニングを行う。計画、復旧機能、担当者のテストを1年に一度は実施し、弱点の特定を行う。

｛システム名｝の緊急時対応計画は、次の連邦および各省のポリシーにも準拠する。

- 1987年施行のコンピュータセキュリティ法、
- 行政管理予算局令A-130（OMB Circular A-130）『連邦情報リソースの管理（Management of Federal Information Resources）』、付録III（2000年11月）
- 連邦準備令（FPC; Federal Preparedness Circular）65、『連邦行政機関における業務の継続性（*Federal Executive Branch Continuity of Operations*）』、1999年7月
- 大統領令（PDD; Presidential Decision Directive）67『耐久的政府構造および、政府業務の継続性』Enduring Constitutional Government and Continuity of Government Operations』、1998年10月
- PDD 63『重要インフラ保護（Critical Infrastructure Protection）』、1998年5月
- 連邦危機管理庁（FEMA; Federal Emergency Management Agency）『連邦対応計画（FRP; Federal Response Plan）』、1999年4月
- 国防認可法令(Defense Authorization Act) (P.L. 106-398)中のタイトルX、サブタイトルGの『政府情報セキュリティ改正法(Government Information Security Reform)』、2000年10月30日
- *他に、適用可能な連邦政府のポリシーがあれば、追加する。*
- *他に、適用可能な各省のポリシーがあれば、追加する。*

1.5 変更の記録

最終版の印刷以降に本計画に加えられた変更点は次のとおりである。

変更の記録			
ページ	変更のコメント	変更日	署名

2. 運用のコンセプト

2.1 システムの説明およびアーキテクチャ

システムのアーキテクチャおよび機能の概要を記述する。運用環境、物理的立地、ユーザーの一般的な所在地、および外部組織/システムとのパートナーシップを表示する。また、バックアップ手順など、復旧するために重要なすべての技術的な考慮事項をも情報に含める。セキュリティコントロールや通信接続を含むアーキテクチャの図も記載する。

2.2 後継者の指定

{組織名} は、{システム名} の緊急時対応計画において、意志決定者がいないということがないように、部門が定めた順序に従って後継順位を定める。{組織名} の最高情報責任者 (CIO) は、{システム名} の緊急時対応計画において文書化した、人員の安全と手順の実行を確実とする責任を担う。CIOが全体の責任者としての役割を果たすことができない、またはこの責任を引継者に委任する選択を行った場合、代理CIOがこの責任者として機能する。*可能であれば、後継の説明を続ける。*

2.3 責任

ITシステムに影響を及ぼす緊急事態に対応する、次のようなチームを編成し、トレーニングを行う。

緊急時対応計画では、{システム名} の運用復旧に参加する複数のチームが構成される。{チーム名} は、{システム名} のコンピュータ環境およびすべてのアプリケーションの復旧に責任を負う。{チーム名} のメンバーには、{システム名} の日常業務および保守を担当する要員も含まれる。チームリーダーの肩書きを持つ要員が {チーム名} を指揮する。

チームとその責任、リーダーシップ、および復旧活動中の他のアプリケーションチームとの調整についての説明を継続する。

システム復旧にかかわるチームの関係、およびそのチームリーダーを次の図XXに示す。

(復旧チームの階層構造図を挿入する。チーム名とリーダーは記述するが、チームメンバーの実際の名前は含めない)。

全体的な復旧の目標および各チームの責任を記述する。これらの責任を遂行するために使用される手順の詳細は記述しない。詳細手順については、適切なフェーズの項目で詳述する。

3. 通知および実行フェーズ

このフェーズでは、{システム名}の中断によって発生した損害を見極め、評価するために行われる初期活動を説明する。この計画は、イベントの評価結果に基づき、緊急時対応計画コーディネーターによって実行される。

緊急時における、{組織名}の最優先事項は、人員の健康と安全性を保全することであり、その後、通知および実行手順を進める。

重要な要員の連絡先情報は、付録Aに記載する。通知順序は次のとおりである。

- 最初の対応者は、緊急時対応計画コーディネーターに通知し、知りえたすべての情報を緊急時対応計画コーディネーターに伝えなければならない。

- システム管理者は、損害評価チームリーダーに連絡し、イベントについて通知しなければならない。緊急時対応計画コーディネーターは、評価手順を開始するよう、チームリーダーに指示を出す。

- 損害評価チームリーダーは、チームのメンバーに通知し、損害の程度と予想復旧時間を判断するために、以下に要約した評価手順を遂行するようにメンバーを指揮しなければならない。損害評価をローカルで実施できないほどに状況が安全でない場合は、損害評価チームは以下の概要に従う必要がある。

  損害評価手順:

  (障害の原因、さらなる中断または損害の可能性、影響を受けた物理的領域および物理的インフラストラクチャの状態、交換する必要のあるIT機器の機能および在庫の状況、サービスを通常運用に戻すためにかかる予想時間を判断する行為を含む詳細な手順を要約する)。

  - 緊急時対応計画コーディネーターから通知を受けると、損害評価チームリーダーは...しなければならない。

  - 損害評価チームは...しなければならない。

代替評価手順:

- 緊急時対応計画コーディネーターから通知を受けると、損害評価チームリーダーは...しなければならない。

- 損害評価チームは...しなければならない。
  - 損害評価の終了時には、損害評価チームリーダーは、緊急時対応計画コーディネーターにその結果を通知しなければならない。
  - 緊急時対応計画コーディネーターは、その結果を評価し、緊急時対応計画を開始すべきかどうか、移転が必要かどうかを判断しなければならない。
  - 評価結果によっては、緊急時対応計画コーディネーターは評価結果を公安職員（警察や消防署など）に通知しなければならない。

下記事項の1つまたは複数にあてはまる場合に、緊急時対応計画を実行する必要がある。

1. 48時間以上{システム名}を利用できない場合。

2. *施設が損害を受けており、24時間以上利用できない場合。*

3. *他の基準に付いても適宜。*

- 計画を実施する必要がある場合、緊急時対応計画コーディネーターは、すべてのチームリーダーに通知し、イベントの詳細と移転が必要かどうかを通知しなければならない。

- 緊急時対応計画コーディネーターから通知を受けるとチームリーダーは、それぞれのチームに通知しなければならない。チームメンバーには、該当するすべての情報を知らせ、対応および必要に応じて、移転の用意を行うよう通知する。

- 緊急時対応計画コーディネーターは、緊急事態が宣言されたことをオフサイトの格納施設に通知し、代替サイトに必要な機材（損害評価で特定）を発送しなければならない。

- 緊急時対応計画コーディネーターは、緊急事態が宣言されたことを代替サイトに通知し、政府機関（機材、要員）の入設準備を整える。

- 緊急時対応計画コーディネーターは、インシデントの全般的な状況について残りの要員に（通知手順を通じて）通知しなければならない。

4. 復旧措置

他の作業は、元のシステムおよび機能に対する損害の修復に向けられているが、この項では代替サイトでのアプリケーションの復旧手順について説明する。

次の手順は、代替サイトにおける{システム名}の復旧である。手順は、必要なチームごとに概説する。各手順は、効率的な作業を維持するために、示された順序で実行する必要がある。

復旧の目標 *事業影響分析での決定に従って、最初の復旧目標を明記する。この目標を達成するための機能を実行する責任を担うチームごとに、チーム名とそれぞれの手順を記述する。*

- *{チーム名}*
  - *チームの復旧手順*
- *{チーム名}*
  - *チームの復旧手順*
- *{チーム名}*
  - *チームの復旧手順*

復旧の目標 *事業影響分析での決定に従って、2番目の復旧目標を明記する。この目標を達成するための機能を実行する責任を担うチームごとに、チーム名とそれぞれの手順を記述する。*

- *{チーム名}*
  - *チームの復旧手順*
- *{チーム名}*
  - *チームの復旧手順*
- *{チーム名}*
  - *チームの復旧手順*

復旧の目標 *(事業影響分析での決定に従って)残りの復旧目標を明記する。この目標を達成するための機能を実行する責任を担うチームごとに、チーム名とそれぞれの手順を記述する。*

5. 通常業務への復帰

この項では、{組織名} における元のサイトまたは新しいサイトでの {システム名} 運用復旧に必要な活動について説明する。元のサイトまたは新しいサイトでコンピュータセンターが復旧したら、代替サイトでの {システム名} 運用を元のオペレーションサイトに戻さなければならない。この目標は、代替サイトからコンピュータセンターへ運用をスムーズに移行させることである。

元のサイトまたは新しいサイトの復旧

通常業務を移転できるように、元のサイトを復旧または代替する手順を、必要なチームごとに要約する。IT機器および通信接続のテストを行う。

- *{チーム名}*
  - *チームの復旧手順*
- *{チーム名}*
  - *チームの復旧手順*

5.1 並行処理

元のサイトまたは新しいサイトのシステムと連携してシステムを運用する手順を、必要なチームごとに要約する。これらの手順には、元のシステムまたは新しいシステムが正常に機能するまでに行われるテスト手順や、緊急時対応システムを通常の手続きを経てシャットダウンする手順が含まれる。

- *{チーム名}*
  - *チームの復旧手順*
- *{チーム名}*
  - *チームの復旧手順*

5.2 計画の終了

組織が所有するすべての機器またはその他の機材を代替サイトから撤去する手順を、機密情報の処理に重点を置いて、必要なチームごとに要約する。機材、機器、およびバックアップメディアを適切に荷造りしラベルを付け所定の場所へ発送しなければならない。また、元のサイトまたは新しいサイトへ戻るよう、チームメンバーに指示を与える。

・ *{チーム名}*
  - *チームのテスト手順*
・ *{チーム名}*
  - *チームのテスト手順*

6. 計画の付録

付録は、システム要件および計画の要件に基づいていなければならない。

・ 要員の連絡先リスト

・ ベンダーの連絡先リスト

・ 機器および仕様

・ サービスレベル契約と同意覚書

・ IT作業標準

・ 事業影響分析

・ 関連する緊急時対応計画

・ 緊急時管理計画

・ 人員緊急時計画

・ 運用継続計画

付録B
事業影響分析の例と事業影響分析テンプレート

この例での組織は、約50人のユーザーに対応したローカルエリアネットワーク（LAN）を備えた小規模オフィスを備えている。事務所では、LANとそのコンポーネントを利用して、表計算、ワープロ、電子メール（eメール）の作成や使用などの標準的な自動処理を行っている。また、カスタマイズされたデータベースアプリケーションも使用して、在庫管理や主要なリソース管理を行っている。ネットワーク管理者は、LANの緊急時対応計画の策定を担当し、事業影響分析を開始した[34]。このLANには次のコンポーネントが含まれる。

- 認証サーバー/ネットワークオペレーションシステムサーバー
- データベースサーバー（カスタマイズされた在庫情報データベースアプリケーションをサポート）
- ファイルサーバー（在庫情報以外の一般的なファイルを格納）
- アプリケーションサーバー（事務所の自動ソフトウェアをサポート）
- ネットワークプリンタ
- 電子メールサーバーおよびアプリケーション
- 50台のデスクトップコンピュータ
- 5台のハブ

緊急時対応計画コーディネーターは、ネットワークの関係者の特定から、事業影響分析プロセスを開始する。この場合、コーディネーターは、次の人員に助言を求める。

- 現場事務所管理者
- 在庫プロセス管理者
- 無作為抽出したネットワークユーザー

---

[34] LAN は組織のワイドエリアネットワーク（WAN）に接続しているが、本計画の範囲はローカルネットワークに限定されているので、ここでは WAN コンポーネントを取り上げない。

・ 各ネットワークサーバーのシステム管理者

次のような記述をもとに、コーディネーターは以下のような情報を取得する。

・ 在庫システムは、上位組織のマスターリソース管理処理にとって重要である。このシステムは、各業務の終了時に、上位の大規模システムへ最新データを提供する。1営業日（8時間）以上にわたってシステムが使用できなくなった場合、上位組織にもたらされる影響は重大である。在庫管理には、システムデータベースへアクセスしてデータを処理する最低5人の要員および、デスクトップコンピュータが必要である。

・ 在庫以外のその他の処理は重要でないとみなすことができ、10日までの中断が許容される。

・ 現場事務所管理者と在庫管理者は、電子メールが不可欠なサービスであることを指摘するが、スタッフは3日間までは、電子メールを利用できなくても効率的に作業できる。

・ スタッフは、15営業日までは、表計算アプリケーションを利用できなくても、ビジネスプロセスに重大な影響を及ぼすことなく業務を遂行できる。

・ ワープロへのアクセスは、5営業日以内に復旧する必要がある。ただし、必要なフォームをハードコピーで利用できる場合、10日までは手動プロセスを利用できる。

・ 当日の在庫システム記録の出力は、通常、毎日印刷される。印刷するデータは、在庫システムスタッフが使用する任意のデスクトップコンピュータにも格納できる。緊急時には、業務に重大な影響が及ぶ前の3日間までは、電子メールによる在庫システム出力を電子的に転送できる。他の印刷機能は不可欠ではないとみなされ、10日までは利用できなくても、ビジネス機能には何ら影響しない。

関係者との対話によって得られた情報に基づいて、緊急時対応計画コーディネーターは、3段階の事業影響分析プロセスに従い、重要な情報技術（IT）リソースを特定し、中断時の影響と停止許容時間を判定し、復旧優先度を決定する。

重要なITリソースの特定

管理者は、重要である（以下のリソースが、重要なビジネスプロセスをサポートしていることを意とする）として、次のリソースを特定する。

・認証サーバー/ネットワークオペレーションシステムサーバー（ユーザーがLANにアクセスするために必要）

・ データベースサーバー（在庫システムの処理に必要）

・ 電子メールサーバーおよびアプリケーション

・ 5台のデスクトップコンピュータ（5人の在庫ユーザーをサポート）

・ 1台のハブ（5人の在庫ユーザーをサポート）

・ ネットワークケーブル

・ 電力

・ 暖房、換気、および空調装置（HVAC：Heating, ventilation and Air Conditioning）

・ 物理的セキュリティ

・ 施設

中断の影響と停止許容時間の判定

次に、管理者は重要なリソースについて、中断時の影響と許容可能な中断時間を判定する。

リソース	中断時の影響	許容可能な中断時間
認証サーバー	ユーザーが在庫システムにアクセスできなくなる。	8時間
データベースサーバー	ユーザーが在庫システムにアクセスできなくなる。	8時間
電子メールサーバー	ユーザーが電子メールを送信できなくなる。	2日
5台のデスクトップコンピュータ	ユーザーが在庫システムにアクセスできなくなる。	8時間
ハブ	ユーザーが在庫システムにアクセスできなくなる。	8時間
ネットワークケーブル	ユーザーが在庫システムにアクセスできなくなる。	8時間
電力	ユーザーが在庫システムにアクセスできなくなる。	8時間
プリンタ	ユーザーが在庫レポートを作成できなくなる。	4日

復旧優先度の決定

前の手順で完成した表を使用して、緊急時対応計画コーディネーターは、システムリソースの復旧の優先度を設定する。管理者は、高、中、低の簡単な等級を使用して、リソースの優先度を設定する。高の優先度は、許容可能な中断時間内に復旧する必要のある重要なリソースに基づくものである。中および低の優先度は、完全な運用機能の復旧により長い復旧期間を許容できることを意味している。

リソース	復旧優先度
認証サーバー	高
データベースサーバー	高
5台のデスクトップコンピュータ	高
1台のハブ	高
ネットワークケーブル	高
電力	高
電子メールサーバー	中
プリンタ	中
残りのデスクトップコンピュータ（45台）	低
残りのハブ（4台）	低

事業影響分析を完成させることにより、緊急時対応計画コーディネーターは、上記の復旧の優先度情報を使用して、すべてのシステムリソースをそれぞれの許容可能な中断時間内で優先度に従って復旧するための戦略を策定できる。

次のページには、事業影響分析を実施するためのテンプレートを記載している。

事業影響分析のテンプレート

このテンプレート例は、ユーザーがITシステムにおける事業影響分析の実施に役立つように設計されている。事業影響分析は、IT緊急時対応計画の策定における基本的なステップである。このテンプレートは、基本的なガイドとして考えられているだけであり、すべてのシステムに適用できるわけではない。ユーザーは、このテンプレートまたは一般的な事業影響分析アプローチを必要に応じて修正し、特定のシステムに適合させることもできる。

予備システム情報

組織:	事業影響分析実施日:
システム名:	事業影響分析 連絡担当窓口:
システムマネージャの連絡先（連絡担当窓口）:	
システムの詳細: 〔システムの目的および、システム図を含むアーキテクチャの説明〕	
A. システム連絡担当窓口の特定	**役割**
内部関係者 〔システムを使用またはサポートする組織内の人員、職位または事務所を特定する。またシステムとの関連性を明記する〕	
・ ・	・ ・
外部関係者 〔システムを使用またはサポートする組織外の人員、職位または事務所を特定する。またシステムとの関連性を明記する〕	
・ ・	・ ・
B. システムリソースの特定〔システムを構成する具体的なハードウェア、ソフトウェア、およびその他のリソースを特定する。数量とタイプも含める〕	
ハードウェア ・ ・	
ソフトウェア ・ ・	

その他のリソース ・ ・
C. 重要な役割の特定〔第A項で特定した重要とみなされる役割をリストする〕
・ ・ ・

D. 重要な役割と重要なリソースとの対応〔第C項でリストした役割の遂行に必要なITリソースを特定する〕	
重要な役割	重要なリソース
	・ ・
	・ ・
	・ ・

E. 中断時の影響と許容可能な中断時間の特定〔重要なリソースが利用できなくなった場合に、重要な役割に及ぶ影響を記述する。また、リソースを利用できずに許容できない影響が発生するまでの最大時間を明記する〕		
リソース	中断時の影響	許容可能な中断時間
	・ ・	・ ・
	・ ・	・ ・
	・ ・	・ ・

F. リソース復旧優先度の設定〔第E項で定めた中断時の影響と許容可能な中断時間に基づいて、特定リソースの復旧優先度をリストアップする。定量的または定性的尺度（高/中/低、1～5、A/B/Cなど）を使用する〕	
リソース	復旧優先度

付録C
よくある質問とその回答

1. 情報技術（IT）緊急時対応計画とはどのようなものか

IT緊急時対応計画とは、障害発生後にITシステム（主要アプリケーションまたは一般サポートシステム）、運用、およびデータを復旧するために調整された積極的な取り組みを意味する。この計画プロセスでは、緊急時対応計画のポリシーステートメントの策定、事業影響分析の実施、予防対策の特定、復旧戦略の策定、IT緊急時対応計画の策定、テスト、訓練、演習の計画、計画の保守という7つのステップが必要である。

2. 運用継続計画、事業継続計画、事業復旧計画、災害復旧計画、サポート継続計画、サイバーインシデント対応計画、および人員緊急時計画にはどのような違いがあるのか。

組織には、障害が発生した場合に、ビジネスプロセスおよびITシステムの対応、継続性、復旧、および再開に対して備えるための計画が必要である。それぞれの計画にはその目的と範囲があるが、これらの計画には標準的な定義が存在しないため、組織が策定した実際の計画の範囲と次の説明は異なる場合がある。

運用継続計画は大統領令（PDD ）67の要求事項である。組織（通常は本部）が基本的な機能を代替サイトで提供して、通常業務に復帰するまで最高30日間これらの機能を実行するための計画である。**事業継続計画**は、重大な障害の発生中およびその後において、ビジネス機能とそのビジネスプロセスをサポートするITシステムの維持を扱う。**事業復旧計画**は、組織のビジネスプロセスを代替サイトで再開する手順の文書化を行う。事業継続計画とは異なり事業復旧計画は、障害発生中のプロセス維持は取り扱っていない。**災害復旧計画**は、ITに重点を置いた計画であり、壊滅的な災害後に、対象のシステム、アプリケーション、またはコンピュータ施設の運用を代替サイトで復旧できるように策定されている。**IT緊急時対応計画**は、行政管理予算局（OMB：Office of Management and Budget）Circular A-130、付録IIIで要求されている**サポート継続計画**と同じものである。その計画では、ITシステムの復旧および再開手順を提供している。このタイプの計画は、代替サイトへの移転を必ずしも必要としない軽微な中断に対するシステムの復旧手順も含んでいるため、災害復旧計画よりも範囲が広い。**サイバーインシデント対応計画**は、セキュリティ担当者が組織のITシステムへのサイバー攻撃を特定および軽減し、そこから復旧する手順を確立する。**人員緊急時計画は**、人員の健康と安全、環境、または財産を脅かす緊急事態の場合に、施設の人員が従うべき指令を取り扱っている。それぞれの計画に関するポリシーと手順が互いに補完できるように、計画の策定者間で慎重な調整を図る必要がある。また、1つの計画、システム、またはプロセスにおける変更はすべて、関連するシステムおよびプロセスの計画策定者に伝えなければならない。

3. リスク管理と緊急時対応計画にはどのような関連性があるのか

リスク管理は、ITシステムに対するリスクを特定、コントロール、および低減するための幅広い行為を包含する。リスク管理は、天災や、人的および環境的脅威からシステムを保護するセキュリティコントロールを導入して、損害の発生を防止し、その可能性を低下させることである。リスク管理はまた、リスクによってシステムに障害が発生した場合の、リスクの発現範囲を極小化するための行為も包含する。これらの対策は、起こりうるイベントを予想して作成され、イベントの発生後に実行されるため、緊急時対応計画の基盤を形成する。

4. システム開発のライフサイクルのどのフェーズに、緊急時対応計画を組み込めばよいのか

緊急時対応計画は、運用/保守フェーズで行われる活動に関連しているが、緊急時対応策は、システム開発ライフサイクルのすべてのフェーズで特定し、導入しなければならない。緊急時対応計画をシステム開発ライフサイクルに導入することにより、緊急時対応計画全般のコストが削減され、計画の品質が向上し、計画導入後のシステム運用への影響が小さくなる。

5. IT緊急時対応計画を策定する前には、どのようなステップを踏む必要があるか

緊急時対応計画のプロセスにおいて最初のステップは、上級管理職（通常、最高情報責任者）の承認を受けた緊急時対応計画のポリシーステートメントを策定することである。このポリシーでは、組織の全体的な緊急時対応目標を定義し、IT緊急時対応計画に対する組織のフレームワークと責任を確定することである。ポリシーステートメントでは、役割と責任も取り上げる必要がある。ポリシーは、トレーニング要件、バックアップの頻度、オフサイトへのストレージの発送、計画の演習、テスト、および保守などの手順を検討したうえで策定される。

6. ITシステムの可用性を確保するために、どの緊急時対応策を導入すればよいかをどのようにして判断するか

事業影響分析は緊急時対応計画プロセスの2番目のステップであるが、可用性を確保するためにどの復旧戦略を導入すればよいかを判断する場合に中心となるものである。事業影響分析によって緊急時対応計画コーディネーターは、システム要件、プロセス、および相互依存関係を十分に特定し、緊急時対応要件と優先度を決定することができる。事業影響分析は、関連するすべてのシステムの所有者、エンドユーザー、内部／外部を問わず相互接続されたシステムパートナーからの情報を基に作成される。この情報をもとにして、ITシステムのミッションの遂行に重要なリソースを判定する必要がある。これによって、関連するシステムおよびプロセスでリソースが長期間利用できない結果発生する影響を判断でき、この影響に基づいて、リソースを復旧する順序を設定することができる。このように、リソース要件と復旧の優先順位を設定することで、適切な緊急時対応策を作成できる。

7. 復旧戦略では、どのタイプの代替サイトを選択すればよいのか

代替サイトのタイプは、事業影響分析の結果、決定する必要がある。選択する代替サイトは、コスト効率が良く組織のITシステムの可用性ニーズに適合していなければならない。システムで100パーセントの可用性が必要になる場合は、ミラーサイトが最適な選択である。ただし、数日間のダウンタイムを許容できるシステムの場合は、コールドサイトが好ましい選択肢となる。

8. 代替サイトまたはオフサイトの格納場所は、プライマリサイトからどの程度離れていなければならないのか

代替サイトまたはオフサイトの格納施設とプライマリサイトとの距離は、実際の距離よりはむしろ、考えられる潜在的脅威の範囲に基づいて判断する。緊急時対応計画コーディネーターは、安全で実用的なオフサイト施設を選択するために、リスクアセスメントを実施し、どのような地理的位置、アクセス要件、セキュリティ要件、環境、コスト要件が必要かを決定しなければならない。

9. イベントはいつ発生し、誰に通知する必要があるのか

通知手順は、緊急時対応計画で要約されていなければならない。緊急時対応計画コーディネーターは、ITシステムの中断が発生した場合に、誰に通知すべきか、どの順番で連絡するかを決定する必要がある。一般に通知対象者には、システム所有者、ユーザー、相互接続された主要アプリケーションおよび一般サポートシステムの連絡先が含まれる。ITシステムに相互接続している外部の事業体も通知手順に含める必要がある。連絡系統を定めておけば、通知先の順番と通知責任を明確化できる。

10. 再構築フェーズとはどのようなものなのか

再構築フェーズは、再開フェーズとも呼ばれ、復旧フェーズの実行後に導入される。再構築フェーズでは、元の施設およびITシステムを通常の運用状態に復旧する手順が実行される。甚大な損害を被った結果、元のサイトまたはシステムが使用できなくなった場合、再構築フェーズで、新しい施設またはITシステムを調達し用意するための措置が取られる。元のまたは新しいサイトおよびシステムの用意が整ったら、復旧活動が終了し、通常業務は組織の施設に戻される。

11. どの程度の頻度でIT緊急時対応計画を検証する必要があるのか

検証は、計画手順の実行可能性を評価し、計画を導入する復旧スタッフの能力を判断し、計画における欠陥を特定するのに役立つ。検証は、少なくとも年に一度か、あるいはITシステムやビジネスプロセス、IT緊急時対応計画に重大な変更が行われたときに実施する必要がある。緊急時対応計画の各要素は、最初は個別に検証し、続いて全体を検証することで、復旧手順の正確さと全体の有効性を確認する。検証および演習のスケジュールは、緊急時対応計画ポリシーに記載する。

12. どの程度の頻度で緊急時対応計画を更新する必要があるのか。

最新の計画は、それを適切に運用するのに不可欠である。原則として、計画は少なくとも年に一度、あるいは計画、システム、システムがサポートするビジネスプロセス、復旧手順で使用されるリソースに大きな変更があったときに、その正確度と完成度を見直す必要がある。検証〔質問9を参照〕で明らかになった欠陥は、計画の保守段階で対処する必要がある。契約リストなど、頻繁に変更される計画要素は、頻繁に再検討し更新しなければならない。保守スケジュールは、緊急時対応計画ポリシーに記載する必要がある。

13. 緊急時対応計画および復旧策の策定において、他のどのような活動と調整を行う必要があるのか

緊急時対応計画をシステム開発のライフサイクルに導入することに加え、ネットワークセキュリティポリシーと整合をとる必要がある。システムセキュリティ管理を検討する際は、インシデント対応手順と整合をとることで、システム可用性の脅威となる不正プログラムや攻撃から保護することができる。また、IT緊急時対応計画を策定するには、ITシステムや相互接続したシステム、ビジネスプロセスに関連する緊急時の準備計画と整合をとらなければならない。

付録D
緊急時対応計画における人的考慮事項

IT緊急時対応計画は、汎用サポートシステムおよび主要アプリケーションの復旧手段によって異なるが、それ単体が策定および実施されることは皆無である。ITの運用に影響するインシデントが発生すると、組織の人員にも影響が及ぶ。壊滅的なイベントを想定し計画を立てる場合には、人員の安全性、セキュリティ、および健康を十分に考慮する必要がある。避難手順を作成したり施設へアクセスする際には、その地域の災害時対応組織および連邦政府と協力する必要がある。また、メディアの問い合わせや対応メッセージを人員に通知するための方法と標準を作成しなければならない。これらの要素に対する計画は、一般に、人員緊急時計画、事業継続計画、または緊急時コミュニケーション計画に該当し、すべてIT緊急時対応計画と整合をとる必要がある。2001年のテロ攻撃に起因するこれらの問題に対する意識の高まりと、一般的なセキュリティの向上を考えてみると、このような「人的考慮事項」は、関連するあらゆる計画を検討する上での最重要課題となることは必至である。

人員の安全性と撤退

中断中および中断後の人員の安全と退避は、通常、人員緊急時計画で取り扱っている。要員は、自身の物理的なセキュリティおよび退去手順を認識し、定期的な避難訓練中に、これらの手順を実践する必要がある。人員緊急時計画とIT緊急時対応計画には、情報へのアクセスを防止し、中断や盗難の可能性を軽減するために、事務所、人員の作業場所、およびラップトップコンピュータの保護に関する指示事項を含めることができる。計画には、インシデントの性質やそれに対応する時間の範囲内で、身分証明書、車の鍵、およびその他の重要な所持品を収集することを促す項目を含めることができる。さらに、手順では、アクセスを復旧する方法を扱う必要がある。施設を撤退する場合の最適な方法の指示は、具体的なサイト要件と地域の消防規則に基づくものである。「フロア管理人」方式を計画に組み入れ、通常の措置として実施することもできる。この方式は、各フロアから1人または2人の特定の人員を指名し、トレーニングして、全人員の退避を担当させるというものである。同じ人員が通年にわたって退避の監督を担当しないようにするために、通常、この責任者は定期的に交替する。

人員緊急時計画には、災害後に人員の人数を数えるための手順と何通りかの連絡方法も含める必要がある。緊急事態前に誰が建物内におり、誰が人員の行動を把握しているか（オンサイト、オフサイトの双方）について上級管理職が把握することは、民間の公務機関（消防署、警察書、レスキュー隊）や家族に対し、適切な状況報告を行うという点から重要である。人員への指示事項には、建物から離れ、事前に計画された特定の場所で合流し消息を明らかにする手順を含める必要がある。また、事前に用意された場所が安全ではなかった場合、組織に連絡し所在情報を伝える手順を用意し

ておかなければならない。1人の人員または1つのチームへの集中報告方法を採用することで、情報の混乱や錯綜の可能性が低くなる。2001年9月11日のテロ攻撃時、多くの組織は、テレビとラジオでの通知またはインターネットのウェブサイトを上手く活用し、スタッフとの所在確認手順について連絡を行っていた。電話、伝言サービス、電子メール（eメール）、インスタントメッセンジャー（IM）、ウェブサイト、物理的な場所でのミーティング、またはこれらの組み合わせにより連絡方法を作成することができる。この情報は、同僚の連絡先情報と共に小さなカードに印刷し、配布した上で、IDバッジと共に保存することで慣習化できる。

人員の安全性と撤退計画のリソースは、gsa.gov、fema.gov、およびamericanredcross.orgにある。

人員の福利厚生

深刻な状況下では、多くの場合、人員と家族の問題に対処することが、ビジネスの再開よりも優先される。このような問題に対処する計画には、避難所、就業場所、および人材調達に関する項目を含めることがある。主要チームおよび代替チームの両方のメンバーが活動できなかったり責任を遂行できない場合、関連する組織からの要員、ベンダーまたはコンサルタントとの契約による要員を動員することができる。災害時にチームのメンバーと同様のアクセス権限を、ベンダーまたはコンサルタントが確実に得ることができるように、緊急時対応計画の中で、このような可能性に対する準備を行う。正規の要員が仕事に復帰できるようにはなったが、施設の安全が確認できない、使用できないといった場合、要員の代替サイトまたは自宅で作業を行うための調整を行う。これは、IT緊急時対応策で使用する代替サイトに付随する作業である。自宅にコンピュータまたはラップトップを持つ要員は、適宜、自宅から組織のネットワークへアクセスする方法について指示が与えられなければならない。また、要員が一時的な避難所を確保するための支援が必要になることもある。

災害時に命を落とす人がいたり、甚しい物理的破壊があった場合には、人員が多大な精神的ショックを受けることがあるため、災害後の悲嘆に対処するカウンセリングやその他の精神衛生サポートを用意しておく必要がある。すべての連邦政府が利用できる従業員援助プログラム（EAP; Employee Assistance Program）は、これらの問題にとって有用で重要なリソースである。アメリカ赤十字などの非営利組織も、食料、衣料、およびその他の支援プログラムのほか、カウンセリングサービスの人材を派遣している。人員は、健康に優れ、給与が続行されている状態に最も関心を抱く。組織がこの状態を伝達することは非常に重要である。*通常業務どおりに人員に給与を支払い続けられるように、あらゆる努力が行われなければならない。*悲嘆とストレスのために、調整期間中に生産性が低下する場合もある。

連邦従業員援助プログラムに関する情報は、www.opm.gov/ehs/Eappage.htmにある。非営利団体の災害時支援情報は、www.americanredcross.org/services/disasterから入手できる。

災害時対応組織との関係

組織が災害時に地域の消防署や警察署と初めてやりとりをするということがないように、地域の消防署と警察署との関係を構築して、信頼関係を築くのと同時に、徹底的な手順の理解を確立しておく必要がある。消防署員および警察官または連邦職員は、状況から判断して正当であれば、施設に対する主導権を取ることができる。組織は、これがなぜ起きたのかや、再び自身の施設へのアクセスを復旧するために、どの連絡先（連絡担当窓口）およびドキュメントが必要になるかについて認識しておく必要がある。消防署、警察署、およびレスキュー組織は、多くの場合、安全で組織的な手順の作成と、組織の予行演習への参加に進んで協力してくれる。組織の要件によっては、連邦または軍部の対応者との協力計画および演習も必要になる。

地域の災害時対応組織には、直接または州の緊急時管理部門を通じて連絡する。

コミュニケーション計画

コミュニケーション計画では、通常、要員および管理職への内部伝達と、一般人との外部コミュニケーションを扱う。有用な情報をもたらし、噂が広がらないようにするための最も効率的な方法は、明瞭かつ頻繁に伝達することである。この計画は、重大な災害時に組織が要員、市民および連邦職員、影響を受けた家族と友人との間での通信の発信地点になるという可能性も想定して策定されなければならない。

最も重要な活動の1つは、組織内での内部伝達である。スタッフと管理職は、何が発生したのか、その状況、取るべき行動、および状況を収拾する責任者について把握している必要がある。1人の要員またはチームが、内部伝達を担当しなければならない。この要員は、組織の上級管理職にアクセスできなければならない。さらに、組織は、音声メール、電子メール、ビラ、またはウェブサイトでの通知などの複数の伝達手段を使用できるように準備しておく必要がある。上級幹部からすべての人員、相互接続した連絡担当窓口、およびエンドユーザーへのはっきりとした頻繁な伝達が、中断後における内部の不安や心配を鎮め、一般的な疑問に回答するために必要になる。

組織は、内部伝達と同様に、外部関係者に伝達されるメッセージにも慎重に注意を払う必要がある。このために効果的な方法は、やはり組織から特定の連絡担当窓口またはチームをプレスリリースおよびメディアとの連絡窓口に指定することである。連絡担当窓口またはチームの手順には、公式声明を承認する際に顧問弁護士からの情報を参考にする手順を含める場合もある。これにより、置かれている状況の事実のみを述べた信頼のおけるメッセージが配信され、どのような行為が取られたかが明らかになる。要員は、組織に代わって自身のコメントをすることが一切ないように、あらゆるメディアの要求を、単一の連絡担当窓口または公開情報オフィスに照会するようにトレーニングを

行う。これらの手順は、人員緊急時計画または公開情報オフィスのガイダンスに記述することもできる。

国務省の国際情報プログラム（http://usinfo.state.gov/products/pubs/pressoffice/plan.htm）では、伝達計画の策定に役立つアドバイスとヒントを提供している。

災害時および災害後の人的考慮事項の計画に役立つその他のリソースには、次のものがある。

緊急時対応計画および管理、www.contingencyplanning.com
障害復旧研究所インターナショナル（Disaster Recovery Institute International）、www.dr.org
障害復旧ジャーナル（Disaster Recovery Journal）、www.drj.com

付録E
用語集

バックアップ:
必要時に、復旧を容易にするために作成されるファイルおよびプログラムのコピー

事業継続計画:
重大な障害の間およびその後に、どのようにして組織のビジネス機能を維持するかについて、あらかじめ規定された一連の指示または手順のドキュメント

事業影響分析:
重大な障害が起きた場合に、システムの緊急時対応要件および優先度を特定するために使用する、情報技術（IT）システムの要件、プロセス、および相互依存関係の分析

事業復旧/再開計画:
重大な障害が起きた後に、どのようにしてビジネスプロセスを復旧するかが事前に定められた一連の指示または手順のドキュメント

コールドサイト:
コンピュータ設備に必要な電気的および物理的なコンポーネントを備えているが、コンピュータ機器は配備していないバックアップ施設。このサイトは、ユーザーが主要なコンピューティングサイトから代替サイトに移動しなければならなくなった場合に、必要な交換用コンピュータ機器を受け入れる用意が整っている。

コンピュータ:
デジタルデータを受け入れ、データの処理方法に関するプログラムや一連の指示に基づいて情報を操作するデバイス

緊急時対応計画:
緊急事態、システムの障害、または災害が発生した場合に、代替場所で、コンピュータ運用などの業務を維持または復旧できるように設計された管理ポリシーおよび手順

緊急時対応計画立案:
（緊急時対応計画を参照。）

運用継続計画:

災害の結果、通常業務に復帰するまでの最大30日間、組織の基本的な機能をどのように維持するかを事前に定めた一連の指示または手順

サポート継続計画:

重大な中断が発生した場合に、主要アプリケーションおよび一般サポートシステムをどのように維持すればよいかを事前に定めた一連の指示または手順のドキュメント（行政管理予算局（OMB）A-130で要求されている）

災害復旧計画:

主要ハードウェアまたはソフトウェアの障害や施設の破壊が発生した合に、重要なアプリケーションを扱うための計画

中断:

汎用システムまたは主要アプリケーションを操作できない時間が、停止許容期間以上になる事態を引き起こす予期しないイベント（軽微または長期の停電、ネットワークの長期にわたる障害、機器や施設の損害や障害など）

汎用サポートシステム:

共通の機能を共有する同じマネジメントにおいて直接の管理下にある、相互接続された情報リソース。通常、ハードウェア、ソフトウェア、情報、データ、アプリケーション、通信、施設、および人員を含み、様々なユーザーまたはアプリケーションを支援する。個々のアプリケーションは、異なるミッションクリティカルな機能をサポートする。ユーザーは、同じ組織である場合もあれば、異なる組織の場合もある。

ホットサイト:

災害が起きた場合に使用するハードウェアおよびシステムソフトウェアが備わった、十分に運用可能なオフサイトのデータ処理施設

インシデント対応計画:

組織のITシステムに対する悪質なサイバー攻撃を検知、対応し、その影響範囲を制限するために事前に定められた一連の指示または手順のドキュメント

主要アプリケーション:

アプリケーション内の情報の漏洩、誤使用、不正なアクセス、または改ざんによるリスクや損害の規模が大きいため、セキュリティに対して特別な注意を必要とするアプリケーション。主要アプリケー

ションへの侵入口としては、多数の個別アプリケーションプログラムやハードウェア、ソフトウェア、通信コンポーネントなどが含まれる。主要アプリケーションとは、主要なソフトウェアアプリケーションであるか、特定のミッションクリティカルな機能をサポートする目的でハードウェアとソフトウェアを組み合わせたもののどちらかである。

モバイルサイト:

重大な障害の通知があったときに、十分な復旧機能を提供するために必要な特定のIT機器および通信装置を搭載した、内蔵型の移動式のシェル

相補同意:

2つの組織がお互いにバックアップしあうことの同意

リスク管理:

組織のミッションやビジネスへのリスクを継続的に評価するプロセス。リスクベースアプローチの一部であり、脅威と脆弱性を分析し、許容可能なレベルまたはリスクを達成し維持するために、費用対効果の高いコントロールを選択することによって、システムの適切なセキュリティを決定する。

システム:

主要アプリケーションか汎用サポートシステムのどちらかを簡潔に示す場合に使用される一般用語

システム開発ライフサイクル:

システムに関連した活動範囲。システムの開始、開発／調達、導入、運用および保守、システムの廃棄フェーズを網羅し、再び新たなシステムの構築を開始するサイクルを表す。

ウォームサイト:

重大な障害が起きた場合に、離れた場所からのIT運用をサポートする、ITおよび通信機器の一部が備えられた作業場所

付録F
リソース

情報技術（IT）緊急時対応計画の作業を支援する情報は、業界関連の団体や商用ベンダーのウェブサイトで入手できる。このリソースのリストは、調査の出発点を提供するものであり、すべての災害時計画組織およびサービスプロバイダの完全なリストではない。このリストに含まれるサービスプロバイダは、情報収集を目的としてのみの掲載であり、NISTによる推奨または公認を意味するものではない。

団体、刊行物、およびその他の情報ソース

緊急時対応計画者協会
www.acp-international.com

可用性ドットコム（便宜的訳出のみ）
Availability.com
www.availability.com

CBSニュースの災害リンク
http://www.cbsnews.com/digitaldan/disaster/disasters.htm

緊急時対応計画管理（CPM; Contingency Planning Management）
www.contingencyplanning.com

障害復旧機関インターナショナル（DRII）
www.drii.org

災害復旧ジャーナル（DRJ）
www.drj.com

INFOSYSSEC（インフォシスセック＝iNFORMATION SYSTEM SECURITY）
http://www.infosyssec.org/infosyssec/buscon1.htm

国家非常事態管理局
www.nemaweb.org

Survive（サバイブ）
www.survive.com

政府機関

連邦危機管理庁（FEMA; Federal Emergency Management Agency）
www.FEMA.gov

一般調達局（GSA; General Services Administration）、災害復旧サービス
http://www.gsa.gov/Portal/content/offerings_content.jsp?contentOID=117666&contentType=1004

商用ベンダー

Comdisco Recovery Services
www.comdisco.com

Gartner Incorporated
http://www3.gartner.com/Init

IBM Global Recovery Services
http://www-1.ibm.com/services/continuity/recover1.nsf/documents/home

Iron Mountain
www.ironmountain.com

Strohl Systems
www.strohl.com

SunGard
www.sungard.com

付録G
参考文献

Acharya, Soubir and Susan G. Friedman. “Backup Strategies for Networked Storage,”*InfoStor,* November 2001. http://is.pennnet.com/Articles/Article_Display.cfm?Section=Articles&Subsection=Display&ARTICLE_ID=126595

availability.com. “IT Availability Checklist.” http://www.availability.com/elements/information_technology/index.cfm?fuseaction=checklist

Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, “Government Information Security Reform,” October 30, 2000.

Disaster Recovery Journal. Volume 14, Issue 4, Fall 2001. http://www.drj.com/drj2/drj2.htm

DRI International. *http://www.drii.org/index.htm*

Computer Security Act of 1987, 40 U.S. Code 759 (Public Law 100-235), January 8, 1988.

Contingency Planning and Management Online. Volume VI, Number 5, September/October 2001. http://www.contingencyplanning.com

Contingency Planning and Management, *Master Source 2001, Buyer’s Guide Issue,* Volume 6, 2001.

Engelschall, Ralf. “Load Balancing Your Web Site,” *Web Techniques*, May 1998. http://www.webtechniques.com/archives/1998/05/engelschall/

Federal Emergency Management Agency. Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations (COOP),* July 1999.

Federal Emergency Management Agency. *The Federal Response Plan*, April 1999.

Flesher, Tom. “Remote Journaling: A New Trend in Data Recovery and Restoration,” *Contingency Planning & Management*, March 2000. http://www.contingencyplanning.com/article_index.cfm?article=243

Gartner Incorporated, “Fault-Tolerant Networks: Is There Such a Thing?” Research Note, June 14, 2001.

Gartner Incorporated, “Disaster Recovery: Weighing Data Replication Alternatives,” Research Note, June 15, 2001.

Gartner Incorporated, “High Availability: A Perspective,” Technology Overview, June 15, 2001.

Gartner Incorporated, “Disaster Management Plan for Remote Access,” September 20, 2001.

General Accounting Office, *Computer Security: Improvements needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-23IT, November 9, 2001.

General Accounting Office, *Federal Information System Control Audit Manual* (FISCAM), GAO/AIMD-12.19.6, January 1999.

General Accounting Office, *Year 2000 Computing Crisis: Business Continuity and Contingency Planning*, GAO/AIMD-10..1.19, August 1998.

General Accounting Office, *Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges*, GAO/AIMD-00-290, September 2000.

General Accounting Office, Executive Guide: *Information Security Management: Learning From Leading Organizations*, GAO/AIMD-98-68, May 1998.

Information Assurance Technical Framework (IATF), Release 3.0, October 2000. http://www.iatf.net/

INT Media Group, Incorporated. *Webopedia*. http://www.webopedia.com/

LoadBalancing.net. “Frequently Asked Questions.” http://www.loadbalancing.net/faq.html

Leary, Mark F., CPP. “A Rescue Plan for Your LAN,” *Security Management Online*. http://www.securitymanagement.com/library/000496.html

Maxwell, John. “Part II - Storage Virtualization: Beyond the Basics,” *InfoStor*, October 2001. http://is.pennnet.com/Articles/Article_Display.cfm?Section=Archives&Subsection=Display&ARTICLE_ID=123539

National Institute of Standards and Technology, Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

National Institute of Standards and Technology, Special Publication 800-18, *Guide for Developing Security Plans and Information Technology Systems,* December 1998.

National Institute of Standards and Technology, Special Publication 800-21, *Guideline for Implementing Cryptography in the Federal Government,* November 1999.

National Institute of Standards and Technology, DRAFT Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, December 2002.

National Institute of Standards and Technology, Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems,* August 2001.

National Institute of Standards and Technology, Special Publication 800-30, *Risk Management Guide,* June 2001.

Office of Management and Budget, Security of Federal Automated Information Resources, Appendix III to OMB Circular A-130, Management of Federal Information Resources, February 8, 1996.

PCWorld.com. “HassleFree Backups,” *PC World Magazine*, October 2001. http://www.pcworld.com/howto/article/0,aid,18040,00.asp

Presidential Decision Directive 62, Protection Against Unconventional Threats to the Homeland and Americans Overseas, May 1998.

Presidential Decision Directive 63, Protecting America's Critical Infrastructures, May 22, 1998.

Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government, October 21, 1998.

Seagate Technology. "Types of Backups," Technical Bulletin #4062. http://www.seagate.com/support/kb/tape/4062.html

Solinap, Tom. "RAID: An In-Depth Guide to RAID Technology," *SystemLogic.net*, January 24, 2001. http://www.systemlogic.net/articles/01/1/raid/

Sun Microsystems, Inc. "Remote Mirroring," Technical White Paper. http://www.sun.com/storage/white-papers/remote-mirroring.wp.html

Tanner, Dan. "Storage virtualization: What, how, and why," *InfoSto*, March 2001. http://is.pennnet.com/Articles/Article_Display.cfm?Section=Archives&Subsection=Display&ARTICLE_ID=94313

U.S. Department of Commerce, National Bureau of Standards, Federal Information Processing Standards Publication (FIPS PUB) 87, *Guidelines for ADP Contingency Planning*, March 1981.

Whatis.com. TechTarget.net. http://whatis.techtarget.com/

付録H

索引

(訳者注:このページについては翻訳を行っていない。英語原文を参照のこと)