ICS 35.030

CCS L 80

中華人民共和国標準

GB/T 20988-202X

GB/T 20988-2007/GB/T 30285-2013 の代替 GB/T

サイバーセキュリティ技術
情報システムの災害復旧仕様

(公開草案) （本書の完成：2024 年 2 月 23 日）

XXXX - XX - XX リリース　　XXXX - XX - XX インプリメンテーション

国家市场监督管理总局
国家标准化管理委员会 发 布

目次

序文 5

サイバーセキュリティ技術 情報システムの災害復旧仕様 7

1.適用範囲 7

2.参考文献 7

3.用語と定義 7

4 災害復旧の概要 10

4.1 災害復旧の目的 10
4.2 災害復旧ライフサイクルと作業範囲 10

5 災害復旧のための組織体制 11

5.1 組織構造の確立 11
5.2 組織団体の責任 12

6.災害復旧計画と設計 12

6.1 災害復旧要件の決定 12
6.2 災害復旧戦略の策定 13
6.3 災害復旧技術プログラムの設計 15
6.4 災害復旧センターの場所とレベル 19
6.5 災害復旧技術プログラムの検証と妥当性確認 19

7.災害復旧システムとセンタービルの導入 20

7.1 災害復旧システムの構築 20
7.2 災害復旧センターの建設 22

8.災害復旧システムのセキュリティ構築 23

8.1 セキュリティ保護 23
8.2 セキュリティ管理システム 23
8.3 セキュリティ管理アーキテクチャ 24
8.4 セキュリティ・マネージャー 24

8.5 安全な通信ネットワーク 24
8.6 安全なコンピューティング環境 25
8.7 セキュリティ施工管理 26
8.8 セキュリティの運用と保守管理 26
8.9 サプライチェーンの安全保障 26
8.10 データ・セキュリティ 28

9 災害復旧システムの運用管理 28

9.1 災害復旧計画の策定と管理 28
9.2 災害復旧システムの運用と保守 31
9.3 緊急対応と災害対策 33
9.4 リビルドとロールバック 34
9.5 災害復旧監査 34

10 試験評価方法 35

10.1 災害復旧総合試験評価要件 35
10.2 災害復旧のための組織的セットアップテスト評価手法 35
10.3 災害復旧計画と設計 試験と評価の方法論 37
10.4 災害復旧システムおよびセンター構築の試験・評価方法 49

附属書 A（規範） 災害復旧能力の分類 81

A.1 レベル 1 ベーシック・サポート 81
A.2 レベル 2 の代替地サポート 82
A.3 レベル 3 電子伝送と部分的な機器サポート 83
A.4 レベル 4 電子伝送と機器一式のサポート 84
A.5 レベル 5 リアルタイム・データ伝送と完全な機器サポート 85
A.6 レベル 6 ゼロ・データ・ロスおよびリモート・クラスタリング・サポート 86
A.7 災害復旧能力の格付けの原則 88
A.8 災害復旧センターの分類 88

附属書 B（参考） 業界における RTO/RPO と災害復旧能力レベルの関係例 89

附属書 C（参考） ある業界の情報システム要件分類の例 90

附属書 D (参考) クラウド・コンピューティング技術の災害復旧サービス例 91

附属書 E（参考） 災害復旧計画の枠組み 94

E.1 目的と範囲 94
E.2 組織と責任 94
E.3 リエゾンとコミュニケーション 94
E.4 重大インシデント対応プロセス 94
E.5 回復と再手術のプロセス 95
E.6 震災後の復旧とロールバック 95
E.7 プログラムのセーフガード条件 95
E.8 プログラムの附属書 96
参考文献 96

序文

この文書は、GB/T 1.1-2020 Guidelines for Standardisation Work Part 1: Structure and Drafting Rules for Standardisation Documents の規定に基づいて作成されている。

本書は、「情報セキュリティ技術情報システムの災害復旧に関する仕様」（GB/T 20988-2007）及び「情報セキュリティ技術災害復旧センターの建設管理及び運営維持に関する仕様」（GB/T 30285-2013）に代わるものであり、構造調整及び編集上の変更を除き、主な技術的変更点は以下の通りである：

a) 適用範囲を改訂した（第 1 章参照）；

b) 用語と定義の修正（第 3 章参照）；

c) 災害復旧ライフサイクルの概念とモデルの追加（第 4 章参照）；

d) 災害復旧のための組織設定の追加（第 5 章参照）；

e) 災害復旧計画と設計の、クラウド災害復旧などの側面を含むようにする修正（第 6 章参照）；

f) 災害復旧運用の実施段階の変更（第 7 章参照）；

g) 災害復旧システムのためのセキュリティ・ビルディングの追加（第 8 章参照）；

h) 災害復旧ライフサイクルにおける O&M 管理の変更（第 9 章参照）；

i) 災害復旧試験評価方法（第 10 章）が追加された。j) 災害復旧能力分類（附属書 A 参照）の改訂；

本書の内容の一部は特許で保護されている可能性があることに留意されたい。本書の発行団体は、そのような特許を特定する責任を負わない。

本文書は、ネットワークセキュリティ標準化国内技術委員会（SAC/TC 260）により提案され、その支援を受けている。

This document was drafted by: China Information Security Evaluation Centre, Beijing Anxin Tianxing Technology Co., Ltd, Beijing University of Posts and Telecommunications, Huawei Technologies Co., Ltd, China National Institute of Electronic Technology Standardization, China National Engineering Research Centre for Information Security Common Technology, Ltd, Beijing Financial Informatisation Research Institute, Ltd, Hangzhou Meitron Technology Co.Ltd.、北京金融情報化研究院有限公司、杭州美創科技有限公司、民航成都科技有限公司、中国国家電子技術標準化研究所、中国国家情報セキュリティ共通技術研究センター中国エネルギー建設集団山西電力調査設計研究院有限公司、成都民航電子科技有限公

司、安徽科学技術研究院、中国エネルギー建設集団山西電力調査設計研究院有限公司、成都民航電子科技有限公司、成都民航電子科技有限公司

Main drafters of this document: Sun Mingliang, Zhang Xiaofei, Chen Qingmin, Li Xiaoyong, Li Xiaocui, Wang Huizheng, Liu Xin, Yuan Jie, Deng Juan, Gu Yinhong, Hu Jianxun, Li Haipeng, Yang Xiaoping, Liao Yunhua, Feng Xiukang, Yang Xi, Chen Yonggang, Hu Chuntao, Cheng Yingbo, Li Qiuxiang, Lu Li, Zheng Fang, Zhao Zengzhen, Liu Feng, Peng Hailong, Li Jingyi, Ma Guoliang, Cao Jing, Chang Xinmiao, Cao Hao, Liu Bin, An Jincheng, Kang Nan,ワン・ユーイン

この文書とそれに代わる文書の連続バージョンは、次のように発行された：

2007 年に GB/T 20988-2007 として初めて公表され、2013 年に GB/T 30285-2013 として初めて公表された。

これが最初の修正である。

サイバーセキュリティ技術 情報システムの災害復旧仕様

1.適用範囲

本文書は、情報システム災害復旧の原則を確立し、情報システム災害復旧のライフサイクルを提案し、情報システム災害復旧において従うべき基本要件を規定し、災害復旧能力の分類と試験評価方法を記述する。

本文書は、情報システム災害復旧の計画、実施、セキュリティ構築、運用管理を実施するために、災害復旧需要者、サービス提供者、アセスメント評価者などの様々な種類の組織に適用される。

2.参考文献

以下の文書の内容は、本文中の規範的参照を通じて、本文書の必須規定を構成する。日付のある参考文献の場合、その日付に対応するバージョンのみが本書に適用され、日付のない参考文献の場合、最新バージョン（すべての変更指示を含む）が本書に適用される。

GB/T 20984-2022 情報セキュリティ技術 情報セキュリティリスク評価方法

GB/T 22239-2019 情報セキュリティ技術 ネットワークセキュリティレベル保護の基本要求事項

GB/T 25069-2022 情報セキュリティ技術用語集

GB/T 39204-2022 情報セキュリティ技術 重要情報インフラセキュリティ保護要求事項

GB 50174-2017 データセンター設計コード

3.用語と定義

GB/T 25069-2022 で定義されており、以下の用語および定義が本書に適用される。

3.1 オフサイト・ストレージ

メインセンターから安全な距離にある物理的な場所に記憶媒体を保管するプロセス（3.21）。

3.2 再開

災害復旧センター(3.19)は、プライマリーセンター(3.21)に代わり、重要な業務機能(3.3)を再開するプロセスを支援する。

3.3 重要なビジネス機能

CBF

一定期間の中断により、その運営に大きな影響を及ぼすサービスまたは機能。

3.4 リカバリーポイントの目標

RPO

アクティビティが業務を再開するために、アクティビティが使用する情報を復旧させる必要がある時点のこと。

[出典：GB/T 25069-2022, 3.253].

3.5 回復時間の目標

RTO

事故が発生してから、製品やサービス、活動、資源の復旧が完了するまでの期間。

注記：製品、サービス、活動については、回復時間の目標は、製品・サービスの供給停止や活動の実施不能など、組織にとって受け入れがたい負の影響に要する時間よりも短くする必要がある。

[出典：GB/T 25069-2022, 3.254].

3.6 回復

修復

災害復旧センター(3.19)からプライマリセンター(3.21)へ、事業運営を支える情報システムを復旧させるプロセス。

3.7 地域災害

地域または密接に関連する近隣地域の交通、通信、エネルギー、その他の重要なインフラに深刻な損害を与えたり、住民の大規模な避難を引き起こしたりする事象。

3.8 データバックアップ戦略

データ復旧と再構築の目標を達成するためのバックアップ手順と動作を定義する。復旧時間目標（3.5）および復旧ポイント目標（3.4）を満たすように、バックアップ時間、技術、メディア、オフサイト保管方法を決定する。

3.9 事業継続マネジメント

BCM

組織に対する潜在的な脅威と、それらが発生した場合に事業運営に与えうる影響を特定する一連の管理プロセスであり、主要な利害関係者の利益、評判、ブランド、価値創造活動を保護するために効果的に対応する能力を備えた組織のレジリエンスを構築するための枠組みを提供する。

[出典：GB/T 25069-2022, 3.714].

3.10 ビジネスインパクト分析

BIA

活動や事業の中断がもたらす潜在的な影響を分析するプロセス。

[出典：GB/T 25069-2022, 3.715].

3.11 避難訓練

緊急事態への備えと対応計画に基づき、要員の訓練と緊急事態への対応能力の向上を目的として実施される活動。

[出典：GB/T 25069-2022, 3.729].

3.12 災害

人為的または自然的な原因によって情報システムに深刻な障害や故障をもたらす突発的な事象で、情報システムによってサポートされる業務機能が停止するか、一定期間許容できないレベルのサービスに陥る。この結果、通常、情報システムを災害復旧センター(3.19)に切り替えて運用する必要が生じる。

3.13 災害復旧のためのバックアップ

災害復旧のために、システム、インフラ、専門技術サポート能力、運用管理能力をバックアップするプロセス(3.14)。

3.14 災害復旧

情報システムを災害による障害や麻痺の状態から正常に稼働できる状態に復旧させること、および情報システムがサポートするビジネス機能を災害による異常状態から許容可能な状態に復旧させることを目的とした活動およびプロセス。

[出典：GB/T 25069-2022, 3.766].

3.15 災害復旧計画

DRP

情報システムの災害復旧プロセスを計画するために必要なタスク、行動、データ、およびリソースを文書化したもので、事前に設定された災害復旧目標の範囲内で、情報システムによってサポートされる重要な業務機能を復旧させるために関係者を導くものである。

[出典：GB/T 25069-2022, 3.767].

3.16 災害復旧能力

災害復旧リソースと災害復旧計画を用いて、災害後にタイムリーに復旧し、業務を継続する能力。

3.17 災害復旧用バックアップシステム

災害復旧（3.14）目的の場合、データバックアップ災害復旧システム、代替データ処理システム、代替ネットワークシステムから構成される情報システム。

3.18 災害復旧計画

情報システムの災害復旧プロセスに必要なタスク、アクション、データ、リソースを定義した文書。事前に設定された災害復旧目標の範囲内で、情報システムによって支えられている重要な業務機能を復旧させるために、要員を導くために使用される。

3.19 災害復旧センター

省庁の重要な事業継続要件を満たし、災害復旧システム運用のためのサイトをホストする。

注 1：災害復旧センターは、災害復旧センター、バックアップセンターとも呼ばれる。

注 2：災害復旧センターが主催する業務および業務範囲には、災害復旧センター、災害復旧データセンター、その他の関連業務およびサイトが含まれる。

[出典：GB/T 30285-2013, 3.5, 修正].

3.20 プライマリーシステム

通常、組織の日常業務をサポートする情報システムである。

注 3：生産システム

[出典：GB/T 25069-2022, 3.522].

3.21 プライマリ・センター

プライマリ・システムが設置されているデータ・センター 注 4：プライマリ・サイト プライマリ・サイト

注 5：生産センター

4 災害復旧の概要

4.1 災害復旧の目的

災害復旧の目的は、組織が効果的な技術的・管理的手段によって、災害発生時に情報システム業務を迅速に復旧し、損失と影響を最小限に抑え、データの完全性と可用性を保護し、事業継続性を確保できるようにすることである。

4.2 災害復旧ライフサイクルと作業範囲

災害復旧のライフサイクルには、計画と設計、構築と実施、運用と管理が含まれ、継続的な改善を達成するために、ライフサイクルのプロセスを通じて、有効性分析とセキュリティ管理を継続的に実施する必要がある。図 1 を参照。

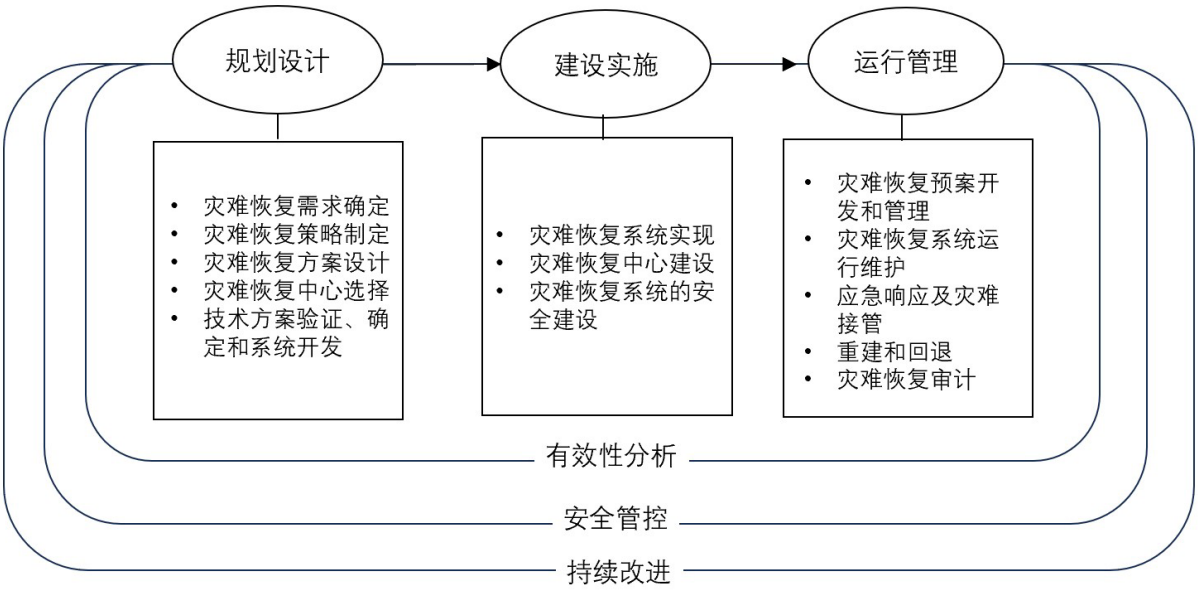

図 1 災害復旧ライフサイクルの概略図

情報システムの災害復旧業務には、災害復旧センターと災害復旧システムの計画、設計、構築、実施、日常業務における事前計画、運用・保守、監視・点検の管理が含まれ、緊急対応や災害時の引き継ぎ、再構築、ロールバック、監査関連業務も含まれる。組織の情報システム災害復旧組織は、ライフサイクル全体の災害復旧プロセスにおいて、資源配分、技術サービスプロセス、プロセス管理のコンプライアンスと有効性分析を実施し、事業の正常な遂行を確保しなければならない。災害復旧は、毎週継続的に行われる改善プロセスである。

現時点では、災害復旧センターも複数の機能の役割を提示し、災害復旧センターの一部は、データの統計、分析、複数の役割を果たす、災害復旧アプリケーションは、実際の状況に基づいて増加し、この文書で提示された技術仕様と要件をカットすることができる。

情報システムの災害復旧作業は、復旧能力目標に基づいて 6 つの段階に分けられる。各段階における具体的な作業は第 6 章から第 9 章の要求事項を満たし、レベルの分類は附属書 A の要求事項を満たし、試験・評価方法は第 10 章の要求事項を満たす必要がある。

5 災害復旧のための組織体制

5.1 組織構造の確立

情報システムを使用または管理する組織（以下「組織」という）は、日常の組織体制と連動して、災害復旧のための組織体制を確立し、その責任を明確にすべきである。これらの個人の中には、2 つ以上の機能を担当する者もいれば、複数の者が兼務する役職もあるだろう。

災害復旧のための組織構造は、一般的に以下のように設定することができる：

a) 災害復旧リーダーシップチーム；

b) 災害復旧管理チーム；

c) 災害復旧技術・実施チームと災害復旧保証チームである。

組織は、災害復旧の実施を支援するために外部の専門家を雇うこともできるし、適切な資格を有する外部組織に、日常業務チームだけでなく、実施チームの業務の一部または全部を委託することもできる。

5.2 組織団体の責任

各組織の構成と責任は以下の通りである：

-- 災害復旧リーダーシップチーム（Disaster Recovery Leadership Team: DRLT）は、情報システム災害復旧のための組織のリーダーシップ組織であり、チームリーダーは組織のトップマネジメントのメンバーであるべきである。災害復旧リーダーシップチームの責任は、災害復旧予算のレビューと承認、災害復旧戦略と計画のレビューと承認、災害復旧計画の実施の承認など、主要な情報システムの災害復旧に関する問題を主導し、決定を下すことである。

-- 災害復旧管理チームは、主に組織のビジネス、テクノロジー、ロジスティクス、その他関連部門の責任者で構成され、災害復旧リーダーシップチームのリーダーシップの下で活動する。災害復旧予算の編成・策定、災害復旧戦略・計画の編成・策定、災害復旧のための社内外のリソースの調整、災害復旧作業のチェックなど、主に情報システムの災害復旧作業の管理・調整に責任を負う。災害復旧予算の編成・策定、災害復旧戦略・計画の編成・策定、災害復旧のための内部・外部リソースの調整、災害復旧作業のチェックなど、情報システム災害復旧作業の管理・調整を主に担当する。

-- 災害復旧技術・実施チームは、災害復旧センターの専門スタッフ、技術スタッフ、運営・保守スタッフ、サービス・プロバイダーで構成され、災害復旧の計画・設計、建設・実施、運営・保守、緊急時対応計画の策定、テスト、リハーサル、実施など、災害復旧の具体的な実施に主に責任を負う。

-- 災害復旧支援チームは、組織の人的資源と後方支援スタッフで構成され、災害復旧に必要な資源の供給、災害復旧、災害現場の安全確保を担当する。

6.災害復旧計画と設計

6.1 災害復旧要件の決定

6.1.1 リスク分析

GB/T 20984-2022 を参照し、リスク分析活動を実施し、情報システムの資産とその価値、直面する脅威と脆弱性の存在を特定し、既存のリスクの予防と制御手段を識別するために、リスクアセスメントの方法論は、具体的に GB/T 20984-2022 を参照することができる。

6.1.2 ビジネスインパクト分析

組織のビジネス機能及び各ビジネス機能の関連性を特定し、各ビジネス機能をサポートする適切な情報システム及びその他のリソースを決定し、関連する機密性、完全性、可用性（時間機密性を含む）の要件を特定する。

様々なビジネス機能に対するディスラプションの影響は、定量的および／または定性的な方法を用いてアセスメントされるべきである：

a) 定量的分析：事業機能の中断の結果、組織が被る直接的・間接的な経済的損失の可能性を定量的にアセスメントする手法である；

b) 定性的分析：帰納と演繹、分析と統合、抽象化と一般化を用いて、組織の評判、顧客ロイヤルティ、従業員の信頼、社会的・政治的影響など、事業機能の中断が組織にもたらす潜在的な非経済的コストをアセスメントする。

6.1.3 災害復旧のニーズを特定する

リスク分析とビジネスインパクト分析の結果に基づき、以下のような災害復旧のニーズを特定する：

a) リスク分析とビジネスインパクト分析の結果を統合し、情報システムの復旧に優先順位をつける；

b) 災害復旧目標、すなわち RTO、RPO の指標を特定し、許容可能なサービスレベルまで復旧させることができる情報システムを決定する。附属書 B は、ある業界の RTO、RPO と災害復旧能力レベルの関係の例を示している。

6.2 災害復旧戦略の策定

6.2.1 災害復旧戦略の要件

災害復旧目標に基づき、災害復旧資源にかかるコストとリスクによって起こりうる損失とのバランスをとるという原則（以下、「コスト・リスクバランス原則」という）に従って、事業機能の災害復旧戦略を策定し、事業機能ごとに異なる災害復旧戦略を採用することができる。災害復旧戦略の要素には以下が含まれる：

a) 情報システムの分類を決定するリスク分析の結果によると、特定の方法の分類は、GB / T 20984 - 2022 の実装を参照することができます附属書 C は、業界の情報システムの要件の分類の例を示す；

b) 災害復旧能力のレベルを決定する。災害復旧能力のレベルが異なれば、必要なリソース要素も異なり、災害復旧リソース要素の要件も異なる；

c) 災害復旧リソース要素へのアクセスを決定する；

d) 災害復旧システムのセキュリティ要件を決定する；

e) 災害復旧における互換性要件を決定する。

6.2.2 災害復旧カテゴリーの計画

サービス提供の重要性、適時性の要件、構築計画に基づき、災害復旧のカテゴリーは、データ・レベル、アプリケーション・レベル、ビジネス・レベルに分けられる。

a) データレベルの災害復旧：災害発生時に、データが破損しないようにすることができる；

b) アプリケーション・レベルの災害復旧：データ・レベルの災害復旧を基本に、災害復旧センターに本番センターと同じ（または一部の）情報システムを構築し、本番センターの情報システムに障害が発生した場合、災害復旧センターがそれを引き継いで事業継続を確保する；

c) ビジネスレベルの災害復旧：アプリケーションレベルの災害復旧を基本とし、インフラや情報システム部分だけでなく、災害発生時にオンサイトサポートを提供するユーザーやビジネス担当者のためのオフィススペースも含まれる。

注：データ、アプリケーション、およびビジネスの各カテゴリーの回復力レベルは、それぞれのカテゴリーの RTO および RPO メトリクスによって決定される。

6.2.3 災害復旧レイアウト計画

組織は、コストとリスクのバランス、および経営要件という原則に基づいて、以下のレイアウトモデルを選択すべきである：

-- 1 つのプライマリ、1 つのバックアップ：1 つのプロダクション・センター、1 つの災害復旧・センター；

-- :: 複数のバックアップ：1 つの本番センターと複数の災害復旧センター；

-- バックアップ：2 つ以上のプロダクションセンターが互いにバックアップし合う；

-- 複数のマスターとバックアップ：複数のプロダクション・センターが 1 つの災害復旧センターを共有する；

-- ミックスモード：上記の混合。

注：相互バックアップには、すべてのセンターがリアルタイムのサービスを提供し、互いにバックアップし合うデュアル・ライブおよびマルチ・ライブ・アプローチが含まれる。

6.2.4 災害復旧リソース要素

災害復旧の各能力レベルをサポートするために必要なリソース要素には、以下のものが含まれる：

a) データバックアップおよび災害復旧システム：一般的に、災害復旧ハードウェア、ソフトウェア、データバックアップメディア（以下「メディア」という）で構成され、電子伝送に依存するバックアップおよび災害復旧システムの場合、災害復旧回線および対応する通信機器も含まれる；

b) バックアップ・データ処理システム：災害復旧システムの目的を果たすために必要なシステムで、バックアップ・コンピュータ、周辺機器、ソフトウェアを指す；

c) バックアップネットワークシステム：エンドユーザーがバックアップデータ処理システムにアクセスするために使用するネットワークで、バックアップネットワーク通信機器とバックアップデータ通信回線で構成される；

d) バックアップ・インフラ：災害復旧に必要な建物、設備、組織で、メディアのオフサイト保管、代替サーバー室、災害復旧用ジョブエイド、災害復旧要員が継続的に滞在できる居住施設など、災害復旧システムの運用をサポートする；

e) 専門技術サポート能力：災害復旧システムの期待目標を達成するために、災害復旧システムの運用をサポートし、総合的に保証する能力。これには、ハードウェア、システムソフトウェア、アプリケーションソフトウェアの問題を分析し対処する能力、ネットワークシステムの安全な運用を管理する能力、コミュニケーション能力、調整能力などが含まれる；

f) 運用・保守管理能力：運用環境管理、システム管理、セキュリティ管理、変更管理を含む；

g) 災害復旧計画：発動条件、実施目標、実施チーム、関連資産、切り替えプロセスを含む。

6.2.5 クラウドコンピューティング技術を利用した災害復旧のためのリソース要素

クラウドコンピューティング技術を利用した災害復旧業務では、6.2.4 の要件を満たすことを前提に、クラウドコンピューティング技術を利用する場合と利用しない場合において、本番センターと災害復旧センターの情報システムを組み合わせる複数の形態を考慮する。クラウドコンピューティング技術を使用する場合、オンクラウド、オフクラウド、クロスリージョン、クロスクラウドのシナリオの適用可能性と互換性の要件を考慮する必要がある。クラウドコンピューティング技術のシナリオを使用した災害復旧サービスの例を附属書 D に示す。

6.3 災害復旧技術プログラムの設計

6.3.1 災害復旧リソースへの要件とアクセス

6.3.1.1 データバックアップ災害復旧システム

組織は災害復旧目標に基づくべきであり、それはコストとリスクのバランス原則に従って決定されるべきである：

a) 災害復旧とデータバックアップの範囲；

b) データバックアップの時間間隔；

c) データバックアップと災害復旧のための技術とメディア；

d) データバックアップ災害復旧システムのセキュリティ要件。

データバックアップの災害復旧システムは、組織自身が構築することもできるし、他の組織のシステムやクラウドベンダーが提供する災害復旧サービスを借りて取得することもできる。

データバックアップと災害復旧システムは、災害復旧センターと本番センター間のデータの一貫性と完全性を保証するために、データの一貫性と完全性の検証を提供すべきである。

6.3.1.2 代替データ処理システム

組織は、コストとリスクのバランスの原則に従って、業務機能の災害復旧及び将来の開発の必要性に基づいて、待機データ処理システムの要件を決定し、待機データ処理システムを特定しなければならない：

a) データ処理能力；

b) ホストシステムとの互換性要件；

c) 通常レディ状態かランニング状態か；

d) レイアウト計画。

組織は、代替データ処理システムを取得するために、以下の 3 つのオプションから 1 つを選ぶことができる：

f) 事前にメーカーと緊急供給契約を結ぶ；

g) (f) 必要な機器を事前に購入し、災害復旧センターまたは安全な機器倉庫に保管する。 (g) 商用の災害復旧センターまたは協定を結んだ組織で、すでに利用可能な互換性のある機器をレンタルする。

バックアップのデータ処理システムは、システムの動作環境やソフトウェアのバージョンなどの点で、本番環境のデータ処理システムと完全に互換性がなければならない。

6.3.1.3 代替ネットワークシステム

組織は、バックアップデータ通信のための技術と回線帯域幅を選択し、コストとリスクのバランスの原則に従って、ネットワーク容量とスイッチング時間に対する業務機能の災害復旧の要件と将来の発展のニーズに基づいて、ネットワーク通信機器の機能と容量を決定し、災害復旧時にエンドユーザーが一定の割合でバックアップデータ処理システムに接続できるようにしなければならない。

組織は，6.3.1.2 に記載された手段によって，代替ネットワークシステムを入手することができる。代替データ通信回線は，自前のデータ通信回線を使用してもよいし，リースされた公衆データ通信回線を使用してもよい。

6.3.1.4 代替インフラ

組織は、以下のような災害復旧の目的に基づき、コストとリスクのバランス原則に従って、待機インフラの要件を決定すべきである：

a) メインセンターからの距離が必要である；

b) 敷地および環境（サイズ、温度、湿度、防火、電力、稼働時間など）要件；

c) O&M と管理要件。

組織が代替インフラを獲得するには、3 つの選択肢がある：

d) 組織が所有または運営する；

e) 複数当事者による共同建設または合意によるアクセス；

f) 商業用災害復旧センターのインフラをレンタルする。

6.3.1.5 専門的技術支援能力

組織は、災害復旧の目的およびコストとリスクのバランスの原則に従って、ソフトウェア、ハードウェア、ネットワークの観点から災害復旧センターの技術サポート要件を決定すべきである。これには、技術サポートの組織構造、さまざまな種類の技術サポート要員の数と質、その他の要件が含まれる。

組織が専門的なテクニカル・サポート能力を獲得するには、いくつかの選択肢がある：

a) 災害復旧・センターの専任テクニカル・サポート・スタッフ；

b) サードパーティのテクニカル・サポートおよびサービス・サポートへのアクセス；

c) RTO が短いビジネス機能については、災害発生時の交通や通信の不規則性により、テクニカルサポートスタッフが効果的なサポートを提供できない状況を考慮すべきである。

6.3.1.6 O&M 管理能力

組織は、災害復旧の目的およびコストとリスクのバランスの原則に従って、運用・保守管理の組織構造、要員の数および質、運用・保守管理システムの要件など、災害復旧センターの運用・保守管理に必要な要件を決定しなければならない。

組織は、災害復旧センターの運営と保守を管理するために、以下のモデルを選択することができる：

a) 自ら運営とメンテナンスを行う；

b) 運営と保守を他の組織に委ねる。

6.3.1.7 災害復旧計画

組織は、ニーズ分析の結果に基づき、コストとリスクのバランスの原則に従って、災害復旧計画を特定すべきである：

a) 総合的な条件；

b) 開発プロセスの要件；

c) 教育、訓練、演習の要件

d) マネジメントの要件

組織は、以下の方法で災害復旧計画の策定、実施、管理を完了することができる：

e) 組織によって独自に行われる；

f) その完成を導くために外部の専門家が起用された；

g) 外部組織に委託した。

6.3.1.8 クラウド災害復旧サービス

クラウド災害復旧サービスモデルを使用する場合、組織は災害復旧の目的に基づき、コストとリスクのバランス原則に従って、クラウド災害復旧サービスの要件を決定すべきである：

a) データレベルの災害復旧能力；

b) アプリケーションレベルの災害復旧のためのテイクオーバー機能；

c) システム・アーキテクチャと互換性能力要件；

d) 本番用クラウドプラットフォームから独立したオフサイトのクラウドプラットフォームシステム。

クラウド・災害復旧・サービスの採用は、以下のオプションからアクセスできる：

e) 組織独自のクラウドサービスのニーズを満たし、災害復旧を提供するために、組織が所有または運営する；

f) 外部組織が提供する災害復旧サービスのレンタル。

6.3.2 災害復旧システムのセキュリティ要件

災害復旧システムのネットワーク・セキュリティ要件は、それが伝送する情報システムの最高レベルより低くなく、具体的なセキュリティ要件は、関連する法律、規制、標準を参照することができる。

6.4 災害復旧センターの場所とレベル

6.4.1 災害復旧センター用地の選定

情報システム災害復旧レイアウト計画によると、災害復旧センターを選択または建設する場合、提案する災害復旧センターのセキュリティレベルと災害復旧センターと生産センターのレイアウトの関係は、リスク分析の結果に基づいて、災害復旧センターとメインセンターが同時に同じ種類のリスクにさらされることを避けるべきである。

災害復旧センターには、「併設型」と「オフサイト型」の 2 種類がある。GB 50174-2017 の 4.1 の要件に加え、災害復旧センターの場所には以下を含めるべきである：

a) コロケーション災害復旧センターの設置には、2 つのセンター間の安全距離に注意を払う必要があり、同じ変電所グリッド内や同じ通信ネットワークノード内に設置しないことが求められる。ネットワークの遅延が生産センターに与える影響も考慮する必要があり、コロケーション災害復旧センターと生産センター間の直線距離は 10～30km に設定する必要がある。

b) オフサイト災害復旧センターの立地は、同じ地域の地震帯、竜巻、台風ルート、その他の自然災害を避けるように考慮されるべきであり、オフサイト災害復旧センターの建設距離は 200km 以上であるべきである。

c) 重要な国の戦略的レベルでの災害復旧センターの設置には、探知防止や攻撃防止といった要素を考慮に入れるべきである。

6.4.2 災害復旧センターのインフラの分類

災害復旧センターのインフラは GB 50174-2017 の等級要求を参考に、災害復旧センターの機能の適時性の要求と災害復旧の目的に従って建設される。災害復旧センターのインフラのレベルは、本番センターと同じか、本番センターより一つ低いレベルでなければならない。

6.5 災害復旧技術プログラムの検証と妥当性確認

技術的ソリューションが災害復旧戦略の要件を満たしていることを確実にするために、組織の関連部門によって確認・検証され、確認・検証の結果は記録・保管されるべきである。技術的解決策の検証には、データの完全性と一貫性の検証、データのバックアップと復旧能力の検証、情報システムの切り替えとカットバック能力の検証、ネットワークシステムの切り替えとカットバック能力の検証、システムセキュリティの検証が含まれる。

7.災害復旧システムとセンタービルの導入

7.1 災害復旧システムの構築

7.1.1 全般

第 7 章の災害復旧の要件と計画・設計に基づき、災害復旧システムの導入計画を策定するとともに、導入計画に従って災害復旧システムの展開・設定を行い、展開したシステムのテストを行い、システムテスト合格後にシステムの検収・引渡しを行う。

7.1.2 実施プログラムの開発

災害復旧のニーズと計画設計に従って、災害復旧システムの実施計画を提出し、標準化し、文書に整理し、具体的な実施段階の基礎があるようにする。詳細な実施計画には、以下を含むが、これらに限定されない：

a) 建設目的と建設内容；

b) 技術実現プログラム；

c) システムおよびコンポーネントの安全機能と性能要件；

d) システムとコンポーネントの配備；

e) セキュリティ・コントロールのポリシーと設定；

f) 安全管理の構築要素をサポートする；

g) プロジェクト実施計画；

h) プロジェクトの投資見積もり。

7.1.3 システムの展開と構成

災害復旧システムの展開および構成には、主に以下を含むが、これらに限定されない：

a) 導入準備。災害復旧システムに関連するハードウェア機器の準備、ソフトウェアシステムの準備、環境の準備など、導入環境の準備を行う。導入の品質を確保するために、一連の実行可能なシステム品質管理プログラムを策定し、システム導入プロセスを効果的に指導することができる。災害復旧システムに関連するハードウェアおよびソフトウェア製品をテストし、テスト要件を満たした製品のみを具体的なシステム導入に使用することができる。

b) システムの展開。ポリシーを設定した災害復旧システムに関連する製品またはモジュールを実際のアプリケーション環境に展開し、関連するポリシーを調整する。システム導入のすべての側面は、品質管理プログラムの要件に従い、品質管理目標を達成するように展開する。

c) システム構成。災害復旧システムが適切に機能するように、災害復旧アプリケーションシステムをホストするハードウェアとソフトウェアを構成し、バックアップネットワークシステムが適切に機能するように、本番センターと災害復旧センターのネットワークを構成する。

7.1.4 システム・テスト

災害復旧要件と計画・設計に基づき、システムが設計された機能、性能、セキュリティを達成することをテストし、検証する。主に以下を含むが、これらに限定されるものではない：

a) 災害復旧アプリケーションシステムのソフトウェアとハードウェアをテストし、関連機能が正常であることを確認すると同時に、システム、アプリケーションソフトウェア、各種データが限られた期間内に正しく復旧できること、およびすべての主要な業務機能が正しく復旧できることを確認する；

b) 本番センターと災害復旧センター間のネットワークをテストし、クライアントがバックアップデータ処理システムと適切に通信できることを確認する。

c) ID 認証、アクセス制御、セキュリティ監査、データ保護、機能保護など、災害復旧システムのセキュリティをテストする。

同時に、試験結果を計画・設計と比較し、設計要求事項を満たしていない場合は、システムを修正するか、配置・設定をやり直し、要求事項を満たすまで 7.1.4 の試験プロセスを繰り返す。

7.1.5 検収および引渡し

災害復旧の計画、設計、実施計画に従って、システムが実施計画に厳格に従って構築され、設計された機能、性能、セキュリティなどを達成しているかどうかをテストする。主に以下の内容を含むが、これらに限定されるものではない：

a) 受入準備。設計ソリューションで達成すべき目標に基づいて、受入プログラムを作成する。受入プログラムは、契約条件、要求仕様書、設計ソリューションに基づき、ユーザーのニーズを十分に反映したものでなければならない。

b) 受入テストの組織化受入ワーキンググループは、受入計画の組織化と実施に責任を持ち、評価に合格したシステム受入計画に従って受入テストを実施するためにテスト実施者を組織する。受入テストの内容は、機能、性能、セキュリティをテストするための詳細設計プログラムと組み合わされる。

c) 受入報告。試験終了後、受入報告書を作成し、受入報告書には受入意見と受入結論を明確に記載する。

d) システム納入。システムの引渡しには、引渡し検収報告書、引渡しチェックリスト、管理者マニュアル、利用者マニュアル、セキュリティ概要およびシステム構成マニュアルが含まれ

るが、これらに限定されない。また、運用環境管理システム、システム管理システム、セキュリティ管理システム、変更管理システムなど、災害復旧の目的を達成するために確立されたさまざまな運用手順や管理システムも含まれる。

e) トレーニングの実施。災害復旧戦略の要件に従って、災害復旧システムの専門的な技術サポート能力を提供する。適切な技術サポート組織を設立し、技術サポートスタッフに定期的なスキルトレーニングを提供する。

7.2 災害復旧センターの建設

7.2.1 全般

災害復旧センターの建設プロセスは 7.1 章と整合させる必要があり、GB 50174-2017 の要求事項を参考に、特定の災害復旧建設標準を実施することができる。災害復旧の特殊性に応じて、以下の章内容にも注意する必要がある。

7.2.2 代替インフラ整備要件

災害復旧センターのインフラ建設は、組織の建設要件に従って組織し、実施することができる：

a) 作業設備には、情報システム作業設備と保障措置システム作業設備がある。例えば、電算室、主操作室、情報システム設備、試験・保守室などの情報システム作業設備、給配電設備、冷暖房換気設備、給排水設備、消火設備などの保障措置システム作業設備がある。

b) 補助施設には、日常業務補助施設、災害復旧補助施設、災害復旧訓練施設がある。例えば、災害復旧センター事務室、会議室、データ室などの日常業務補助施設、災害復旧指令センター、事務エリア、プレス発表センター（マルチメディアルーム）などの災害復旧支援施設、訓練教室、シミュレーション演習室などの災害復旧訓練施設である。

c) 生活支援施設には、日常警備要員のための生活施設や災害復旧要員のための生活施設が含まれる。例えば、寮、食堂、活動室などである。

d) その他に必要なエリアには、集合エリア、待合エリア、人の流れの物流経路などがある。

インフラ建設は、「統一された調整、分業、慎重な組織、厳格な監査」の原則に従い、インフラ計画と設計の要件に従って実施されるべきである。新たな災害復旧センターを建設または選定する際には、そのインフラも含めるべきである：

e) 関連する標準の要求事項と開発計画に準拠し、グリーン、低炭素、集約的、効率的という原則に従うべきである；

f) 災害復旧目的の要件を満たし、災害復旧作業に必要な通信、電力、地質、気象資源、さらに災害復旧要員や機材の到着を容易にする輸送条件を備えていなければならない。

g) 災害復旧センターのインフラ建設においては、建設管理チームを組織し、プロジェクトに対応するエンジニアリング資格とデータセンター建設の経験を有する建設請負ユニット、コストコンサルティングユニット、建設監督ユニットを選定し、関連する国家標準の要求事項に従って建設を完成させるべきである。

7.2.3 データバックアップおよび災害復旧システムの構築要件

データバックアップと災害復旧システムは、災害復旧センターと生産センターのデータの一貫性と完全性を保証するために、データの一貫性と事業継続性の原則に基づいて構築されるべきであり、データの一貫性と完全性の必要な検証は、システム実装の過程で実施されるべきである。複数の生産センターが共有する災害復旧センターについては、災害復旧センター内の異なる生産システムによってバックアップされたデータのセキュリティも、災害復旧システムの構築において考慮されるべきである。

7.2.4 代替データ処理システム構築の要件

組織の業務を継続的に運用するための構築要件を満たすために、災害復旧センターの待機用データ処理システムは、システムの動作環境、ソフトウェアのバージョン等において、本番用システムと完全な互換性を有することが必要である。

7.2.5 代替ネットワークシステム構築の要件

災害復旧センターのバックアップネットワークシステムには、災害復旧センターの内部ネットワーク、生産センターと災害復旧センターの間のバックアップネットワーク、災害復旧センターと上位機関の間のネットワークが含まれる。ネットワークは、通信回線とネットワーク機器で構成される。複数の生産センターが共有する災害復旧センターについては、災害復旧センター内の複数の生産システムのネットワークの相互運用性に起因するセキュリティリスクを回避するため、バックアップネットワークシステムの構築時に、異なる生産システムのセキュリティ分離に注意を払う必要がある。

8.災害復旧システムのセキュリティ構築

8.1 セキュリティ保護

災害復旧システムは、GB/T 22239-2019 を参考に、そのネットワークセキュリティレベルの保護レベルの要求に従って安全に構築することができ、重要な情報インフラの災害復旧システムも GB/T 39204-2022 の要求を満たす必要がある。

8.2 セキュリティ管理システム

災害復旧システムのセキュリティ管理システムの要件には、以下が含まれる：

a) 組織に適した災害復旧安全保護計画を策定し、災害復旧安全保護作業の目標を定め、管理システム、技術システム、運営・維持システム、保証システムの側面から計画を立て、組織、人員、資

金、設備などの資源の保証を強化し、災害復旧安全保護作業を支援する。災害復旧プロセスの安全保護計画を文書化し、承認後に関係者に送付する。災害復旧システムの安全保障戦略は、少なくとも 1 年に 1 回、あるいは重大な変更が生じたときに改訂する；

b) 災害復旧システムの管理システムとセキュリティ戦略を確立し、災害復旧システムが直面するセキュリティリスクと脅威の変化に応じて調整する必要がある。

8.3 セキュリティ管理アーキテクチャ

災害復旧セキュリティ管理団体は、第 6 章の災害復旧のための組織的設定に従うとともに、災害復旧システムセキュリティの観点から以下の要件を含む：

a) 災害復旧のための組織構造において、災害復旧システムのセキュリティと保護を管理する責任者を明確に指定し、評価と監督、説明責任のメカニズムを確立し、実施する必要がある；

b) 災害復旧安全管理機関の職員は、災害復旧に関する組織の意思決定システムに含まれるべきである。

8.4 セキュリティ・マネージャー

災害復旧システム・セキュリティ管理者の要件には以下が含まれる：

a) 災害復旧システムの要職に就く者は、そのセキュリティ・スキルを評価されるべきであり、要件を満たした者のみがそのポストに就くことを許されるべきである；

b) 災害復旧システムのための体系的な安全教育訓練システムを確立し、安全教育訓練と技能評価を定期的に実施すべきである；

c) 災害復旧システムのセキュリティ管理組織の責任者及び要職者の身元及びセキュリティ経歴が変更された場合又は必要な場合には、状況に応じて、関連する要求事項に従って、検証を再構築することができる；

d) セキュリティーと守秘義務に関する実務者の義務と義務を明確に定義し、セキュリティーと守秘義務に関する契約を結ぶべきである。

8.5 安全な通信ネットワーク

8.5.1 ネットワーク・アーキテクチャ

災害復旧システムの通信回線は、複数の通信キャリアによる多重ルーティング保護で「メイン 1 つ、バックアップ複数」として実現されるべきであり、ネットワークの重要ノードや重要施設には「デュアルノード」の冗長バックアップを導入することが望ましい。

8.5.2 相互接続セキュリティ

相互接続のセキュリティ要件には以下が含まれる：

a) 災害復旧システムと異なる業務システム間、異なる地域のシステム間、異なる事業者が運営するシステム間のセキュリティ相互接続戦略を確立または改善すべきである；

b) ローカルとオフサイトの両方の災害復旧システムにおいて、ユーザーID やアクセス権などの同一ユーザーの一貫性が維持されるべきである；

c) 異なる LAN から遠隔通信する災害復旧システム間で、セキュリティ対策を講じる。

8.5.3 境界防御

境界防御の要件には以下が含まれる：

a) 異なる業務システム間、異なる地域のシステム間、異なる事業者が運営するシステム間の災害復旧システムの相互運用性、データ交換、情報の流れは厳密に管理されなければならない；

b) 国境を越えた災害復旧システムへのアクセスとデータフローは、国境を越えた機器の管理されたインターフェイスを通じて通信されることが保証されるべきである。

8.5.4 セキュリティ監査

セキュリティ監査の機能要件には、これらに限定されないが、以下が含まれる：

a) 災害復旧システムは、データのバックアップ、復旧、削除、移行、システム構成の変更などの操作について監査されるべきである；

b) 監査データの管理機能が提供され、対応する権限を持つユーザーだけが対応する監査データを読むことができる。

c) 関連ログデータは 6 ヶ月以上保持する。

8.6 安全なコンピューティング環境

8.6.1 本人確認と承認

本人確認と認可の要件には以下が含まれる：

a) ユーザーの身元を特定し、認証し、適切なパスワード複雑性ポリシーを設定する；

b) 災害復旧システムの重要な業務操作、重要なユーザー操作、または異常なユーザー操作の動作を特定し、リストを作成する必要がある；

c) 災害復旧システムの機器、ユーザー、サービスまたはアプリケーション、およびデータは、セキュリ ティ管理の対象とし、重要な業務、重要なユーザー業務、または異常なユーザー操作行動については、動 的な本人確認方法を確立するか、多要素による本人確認およびその他の方法を使用する。

d) 災害復旧システムにおけるすべてのセキュリティ関連操作（ログアクセス、ポリシー管理、バックアップデータアクセスなどを含むが、これらに限定されない）について、アクセス制御ポリシーを設定する。 リソースへのアクセスは、操作権限が事前に定義された範囲を超えないようにし、最小特権の原則を満たすようにする。

8.6.2 侵入防止

侵入防止の要件には以下が含まれる：

a) 高度で持続可能な脅威などのサイバー攻撃に対する侵入防止能力を向上させるために、技術的手段を採用すべきである；

b) 災害復旧システムのバックグラウンド暗号化と動的パスワードの設定により、災害復旧システムのセキュリティを強化する技術的手段を採用すべきである。

8.6.3 自動化ツール

システムアカウント、設定、脆弱性、パッチ、ウイルスライブラリなどの管理をサポートするために、自動化ツールを使用すべきである。脆弱性とパッチは、検証後、適時に修正されるべきである。

8.7 セキュリティ施工管理

災害復旧システムの構築、転換、アップグレードにおいて、災害復旧システムの安全対策は、災害復旧システムの計画、構築、使用と同期させる必要があり、試験、評価、攻撃・防御訓練など様々な形で検証する必要がある。

8.8 セキュリティの運用と保守管理

セキュリティ O&M の要件には以下が含まれる：

a) また、災害復旧システムの運用・保守場所が中国国内にあることを保証し、中国国外での運用・保守が必要な場合は、中国の関連法規を遵守しなければならない。

b) 運用・保守に先立ち、保守要員との間でセキュリティおよび機密保持契約を締結すべきである；

c) 組織に登録された O&M ツールの使用を優先し、未登録の O&M ツールを使用する必要がある場合は、使用前に悪意のあるコードの検出などのテストを行うべきである。

8.9 サプライチェーンの安全保障

サプライチェーンのセキュリティ保護要件には以下が含まれる：

a) リスク管理戦略、供給業者の選定・管理戦略、製品開 発・調達戦略、セキュリティ維持戦略など、サプライチェー ンセキュリティ管理戦略を確立する。サプライチェーンセキュリティ

管理体制を確立し、サプライチェーンセキュリティ 管理のための資金、人員、権限などの利用可能な資源を提供する；

b) 関連する標準の要件を満たす災害復旧製品やサービスを調達し、使用すべきである。それらが国家安全保障に影響を及ぼす可能性がある場合は、国家サイバーセキュリティ審査に合格すべきである；

c) 資格を有する供給業者のカタログを作成し、維持すべきである。政治、外交、貿易などの非技術的要因による製品・サービスの供給中断リスクに備え、安全な供給者を選定すべきである；

d) 災害復旧製品やサービスの安定的あるいは多様な調達先を維持するため、調達チャネルの管理を強化すべきである；

e) 災害復旧製品・サービスを調達する際には、提供者のセキュリティ責任と義務を明確化し、災害復旧製品・サービスの設計、開発、生産、提供の主要な側面についてセキュリティ管理を強化することを提供者に求めるべきである。提供者は、利用者のデータを不正に取得したり、利用者のシステムや機器を管理・操作したり、利用者が製品に依存していることを利用して不当な利益を求めたり、利用者に新たな製品への交換を強要したりしないことを宣言するよう求められるべきである；

f) 災害復旧製品およびサービスの提供者とセキュリティおよび機密保持契約を締結し、契約の内容には、セキュリティ責任、機密保持の内容、報奨および処罰の仕組み、有効期間などを含めるべきである；

g) 災害復旧製品・サービスの提供者は、災害復旧製品・サービスの開発・製造に 10 年以上関与している事業体が所有または管理している、既知の技術に関する特許などの知的財産権について、認可を取得するか、災害復旧製品・サービスの耐用年数の間、継続的に認可を取得することを義務付けられるべきである；

h) 災害復旧製品やサービスの提供者は、中国語版の運用・保守、二次開発、その他の技術情報を提供すべきである；

i) サプライヤは、自社でカスタム開発ソフトウエアのソースコードセキュリティテ ストを実施するか、第三者サービス機関に委託すべきである；

j) 使用する災害復旧製品やサービスにセキュリティ上の欠陥、脆弱性、その他のリスクがある場合は、リスクや危険を排除するための対策を適時に講じる必要があり、重大なリスクを伴うものについては、規定に従って関連部門に報告する必要がある。

8.10 データ・セキュリティ

災害復旧システムのデータ・セキュリティ要件には以下が含まれる：

a) バックアップとリカバリー中の災害復旧システムのデータ完全性を検証すべきである；

b) ファイルがウイルスに感染するのを防ぐため、アンチウイルスソフトのスキャンをサポートすべきである；

c) データ漏洩防止機能をサポートし、暗号化されたストレージやアルゴリズムを使ってデータを保存し、不正アクセスやデータ漏洩を防ぐべきである；

d) 災害復旧システム設備が廃止され、放棄される場合、データ・セキュリティ保護戦略に従って、データの削除、破壊、記憶媒体の再利用に関する対応要件を設けるべきである。

9 災害復旧システムの運用管理

9.1 災害復旧計画の策定と管理

9.1.1 プログラム開発の原則

災害復旧計画（以下、計画）は、さまざまな災害シナリオを想定して策定されるものであり、災害復旧のレベルごとに対応する計画の策定とその実施・管理が必要となる。計画の策定は、以下の原則に従うべきである：

a) 関連性：データレベル、アプリケーションレベル、ビジネスレベルなど、さまざまな災害復旧カテゴリーに対応するプランを設計する；

b) 完全性：シナリオには想定される災害のシナリオが含まれている；

c) 利便性：計画は、緊急事態での使用に適した、わかりやすい言葉やフローチャートなどの形式をとっている；

d) 明確性：計画は明確な構造を採用し、リソースの明確な説明、具体的な作業要素やステップ、各タスクの明確な責任者を定めている；

e) 有効性：計画は、災害発生時の復旧のための実際的なニーズを可能な限り満たしており、実際のシステムおよび人員組織と常に最新の状態に保たれている；

f) 互換性：災害復旧計画は、ネットワーク・セキュリティ、データ・セキュリティ、その他の緊急時計画と有機的に統合されるべきである。

9.1.2 計画策定のプロセス

災害復旧計画策定の原則に基づき、その策定プロセスには次のようなものが含まれる：

a) 起草：リスク分析およびビジネス影響分析で特定された災害復旧の内容に従い、災害復旧能力レベルの要件に基づき、組織の他の関連する緊急対応計画と連携して、災害復旧計画の第一稿を作成する；

b) レビュー：組織は、完全性、使いやすさ、明確性、有効性、互換性について、災害復旧計画の最初の草案を批判的にレビューすべきである；

c) テスト：事前にテスト計画を作成し、そこにテストすべきケースを記述する。テストには、基本的な単体テスト、相関テスト、総合テストが含まれる。テストプロセスを詳細に文書化し、テスト報告書を作成する；

d) 修正：レビューとテストの結果に基づき、最初の草案レビュープロセスとテスト中に特定された問題や欠陥を修正し、承認された草案を作成する；

e) レビューと承認：承認案は災害復旧リーダーシップチームによってレビューされ、承認され、計画の執行草案と決定される；

f) 提出：事前提案に関する情報を規制当局または管轄当局に提出すること。

9.1.3 プログラムの内容

計画の内容には、以下を含むが、これに限定されるものではない：

a) 計画前の実施目標；

b) 計画実施に必要なリソース；

c) 計画実施チームの構成と責任分担；

d) 準備の重要度

e) 事前のプランニングが、発動条件の引き金となる；

f) 事前に提案された関連事業のリストと資産のリスト；

g) 資産の依存関係、関連付け、切り替えプロセスをあらかじめプログラムして切り替える；

h) 関連部署、通知プロセス、通知内容を事前に計画する；

i) 事前計画時のデータセキュリティ保護措置；

j) 事前に計画された演習後のデータ・セキュリティ保護措置；

k) 事前に計画された演習失敗のフォールバック・プロセス；

l) 事前に計画された技術プログラムと業務マニュアル。

9.1.4 計画前研修

関係者に情報システム災害復旧の目的とプロセスを理解させ、災害復旧の操作手順を熟知させるために、災害復旧計画訓練は以下の要求事項に従って組織されるべきである：

a) 災害復旧計画の初期段階から、災害復旧の概念に関する認識と教育への取り組みを開始する；

b) 研修の頻度や範囲など、研修のニーズを事前にアセスメントし、適切な研修・教育プログラムを策定・実施し、プログラムの内容が計画の要件と一致していることを確認し、研修後の記録を残す；

c) 計画実施チームが計画の内容を理解し、把握できるように、教育訓練後の災害復旧計画の監督と評価を行う。

9.1.5 プログラムの変更

災害復旧計画の実効性を確保するためには、災害復旧計画を厳格に維持し、以下の観点から変更管理を行う必要がある：

a) 事業の変更、情報システムの変更、人事異動などは、災害復旧計画の中で適時変更されるべきである；

b) 災害後の計画のテスト、リハーサル、実施の効果をアセスメントし、それに応じて計画を修正すべきである；

c) 災害復旧計画は定期的に見直され、改訂される。

9.1.6 プログラムの保存と配布

見直され、承認された災害復旧計画は、以下の原則に従って保管、配布されるべきである：

a) 事前計画は専任の担当者が行う；

b) プレ・プロポーザルは複数部あり、それぞれ別の場所に保管されている；

c) 災害対策計画は、災害復旧に携わるすべての職員に配布される；

d) この計画では、厳密なバージョン管理が実施され、各リビジョンの後、すべてのコピーが一律に更新される；

e) 古いバージョンの事前提案書は、関連規則に従って破棄される。

災害復旧シナリオのフレームワークの例を附属書 E に示す。

9.2 災害復旧システムの運用と保守

9.2.1 運転と保守の原則

災害復旧システムの運用と維持には、以下の原則が適切である：

a) セキュリティ原則：災害復旧システムのセキュリティ管理および要件のレベルは、本番システムのセキュリティ管理および要件のレベルと同じか、それよりも一段低い；

b) 関連性の原則：災害復旧システムの運用・保守システムは、生産システムの運用・保守システムと連動している；

c) 制度化の原則：災害復旧システムの運用・保守管理は制度化され、運用・保守管理の質と効率を向上させるために処理される；

d) 可用性の原則：災害復旧システムの運用と保守管理は、包括的なテストと定期的な検証メカニズムを通じて、災害復旧リソースの可用性と有効性を確保する。

9.2.2 オペレーション・モニタリング

運用監視は、原則として、災害復旧リソースとプロセスを対象とすることが求められ、監視には以下を含むが、これに限定されるものではない：

a) 災害復旧センターの電源環境の可用性；

b) 災害復旧リソースの利用可能性；

c) 災害復旧リソースの利用；

d) 災害復旧リソースのセキュリティ；

e) 災害復旧タスクの実行状況。

9.2.3 システム検査

9.2.3.1 検査内容

災害復旧システムの定期検査を実施し、検査結果の診断分析を行う必要がある。災害復旧システム検査のプロセスを詳細に記録し、検査報告書を作成し、過去の検査結果と比較分析する必要がある。災害復旧点検の内容には以下のものが含まれるが、これらに限定されるものではない：

a) 災害復旧センターの電源環境の可用性；

b) 災害復旧リソースの利用可能性；

c) 災害復旧リソースの利用率が変化する；

d) 災害復旧リソース変更ログ；

e) 災害復旧リソースのエラーログ；

f) 災害復旧リソースのセキュリティ；

g) 災害復旧タスクの実行状況。

9.2.3.2 検査の頻度

システムパトロールの頻度は、災害復旧のカテゴリーとレベルに連動して決めることができる。

9.2.3.3 検査報告書

検査報告書の要件には、以下を含むが、これに限定されるものではない：

a) 検査報告書には、検査時間、検査対象、検査ステップ、検査原稿、検査結果、検査幹部、検査レビュアー、検査結論および推奨事項が含まれるが、これらに限定されるものではない；

b) 検査報告書のテンプレートは定期的に見直し、改訂されるべきである；

c) 検査報告書は、紙ファイルまたは電子ファイルで保管することができる。

9.2.4 災害復旧訓練

9.2.4.1 演習の種類

災害復旧訓練の種類には、以下のようなものがある：

a) 机上演習：参加者は、会議の形で、演習のシナリオと控除に関する災害対策計画に基づいて、関連する担当者が計画に定められた義務と手順を習得することを確認するために、コマンドと意思決定と調整能力を向上させる；

b) シミュレーション演習：本番センターと同一または類似のテストシステムを構築し、テストデータを採用することで、参加者を組織し、災害復旧計画に沿った演習を実施し、災害復旧システムの可用性を検証する；

c) データ復旧の演習：バックアップデータの復旧テストを行い、バックアップデータの可用性と完全性を検証する；

d) 実戦演習：本番センターまたは災害復旧センターにおいて、参加者を組織し、災害復旧計画に従って実際の運用環境で演習を実施し、災害復旧計画とシステムの可用性を検証する。実地演習では、データが現実に有効であること、または演習前の状態に戻ることを確認する。

9.2.4.2 演習の頻度

災害復旧訓練の種類と頻度は、災害復旧のカテゴリーとレベルに基づいて決定される。

9.2.4.3 演習レポート

訓練報告書には、以下の項目を含めなければならないが、これに限定されるものではない：

a) 訓練報告書には、訓練目的、訓練計画、訓練指揮チーム、訓練実行チーム、訓練時間枠、訓練手順、訓練記録、訓練結果、訓練概要、および勧告が含まれるが、これらに限定されるものではない；

b) 訓練報告書のテンプレートは、定期的な見直しと改訂が必要である；

c) 演習報告は、紙ファイルまたは電子ファイルで保管することができる。

9.2.4.4 演習訓練

関係者に災害復旧演習の目的、演習計画を理解させ、災害復旧演習の手順を熟知させるため、災害復旧演習訓練は以下の要件に従って組織されるべきである：

a) 災害復旧の運用・保守の初期段階において、訓練の概念に関する啓蒙・教育を行う；

b) 災害復旧演習の前に、演習の目的、演習計画などについて的を絞った訓練を行う；

c) 災害復旧訓練の手順をマスターする；

d) 災害復旧訓練の教育訓練と訓練後の評価を実施し、訓練の実施に携わる者が訓練の目的、訓練計画、手順を理解し、習得していることを確認する。

9.3 緊急対応と災害対策

9.3.1 緊急対応

緊急時の対応には以下のものが含まれるが、これらに限定されるものではない：

a) 業務システムとデータ・セキュリティを最大限に保護し、劣化を抑制し、損失を削減するために必要な管理措置を講じる；

b) 災害シナリオに対応する災害復旧プランを選択し、災害復旧プランの起動を確認する；

c) 災害復旧計画に従って、緊急災害切り替えを行う；

d) 緊急災害切り替え後の業務とシステムの可用性を検証する；

e) 業務およびシステムの可用性の検証結果に基づき、緊急インシデント対応ステータスの終了または継続を決定する。

9.3.2 災害復旧インシデント報告

災害復旧事故の報告要件には、以下を含むが、これらに限定されるものではない：

a) 災害復旧イベントに応じて、災害復旧イベントレポートが作成される；

b) 災害復旧インシデント報告書には、災害の種類、災害の原因、事業への影響の範囲、事業への影響の長さ、データ損失の長さ、災害復旧計画および是正措置が含まれるが、これらに限定されるものではない；

c) 災害復旧インシデント報告テンプレートは、定期的な見直しと改訂が必要である；

d) 災害復旧インシデント・レポートは、紙ファイルまたは電子ファイルで保管することができる。

9.4 リビルドとロールバック

災害復旧が完了したら、まず第一に、災害後の復旧とロールバック・プログラムを策定する：

a) プロダクション・センターの障害は修理または再構築され、プロダクション・センターは通常操業に戻る；

b) 災害復旧センターから本番センターへのデータ同期を実施し、本番センターと災害復旧センター間のデータの一貫性を確保する；

c) 災害復旧センターから本番センターへの業務を削減するために、実際の演習でもよいので、削減計画を策定する；

d) 事業の可用性は、災害復旧センターから本番センターへ事業を切り戻した後に検証される；

e) 災害復旧センターからプロダクションセンターへの切り戻しの障害に対する対策を策定する。

9.5 災害復旧監査

定期的に組織される災害復旧監査は、内部監査部門または第三者監査人により組織されるべきであり、以下を含むべきであるが、これらに限定されるものではない：

a) 災害復旧準備計画の保管および配布記録；

b) 災害復旧準備訓練の記録；

c) 災害復旧準備報告の記録；

d) 災害復旧訓練の記録；

e) 災害復旧訓練報告書 アーカイブ記録；

f) 災害復旧システム検査報告書 アーカイブ記録；

g) 災害復旧インシデント・レポートのアーカイブ記録。

監査報告書で提案された改善点に対する回答は、監査報告書発行後に適時に提供されるべきである。

10 試験評価方法

10.1 災害復旧総合試験評価要件

情報システムの災害復旧作業は、災害復旧の目的が達成され、データの機密性、完全性、可用性が保護され、事業の継続性が保証されるように、様々な段階における災害復旧センターと災害復旧システムの計画・設計、建設・実施、運用・管理を試験・評価するために、附属書 A の要素とガイドラインを参照すべきである。

10.2 災害復旧のための組織的セットアップテスト評価手法

10.2.1 組織構造の確立

組織的セットアップテストの評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧リーダーシップ・チームのメンバーにインタビューを行い、災害復旧のための組織体制が日常的な組織体制と連動して確立されているかどうか、また、その組織体制に災害復旧リーダーシップ・チーム、災害復旧管理チーム、災害復旧技術・実施チーム、災害復旧保障チームなどが含まれているかどうかを確認する；

2）災害復旧の実施を支援するために外部の専門家を雇う場合は、その外部の専門家が関連する資格文書を持っているかどうかをチェックする。実施チームおよび日常業務チームの業務の一部または全部を請け負うために外部の組織を委託する場合は、その外部の組織が関連する資格文書を持っているかどうかをチェックする。

(b) 期待される結果

1）日常的な組織構造と連動した災害復旧組織構造を確立し、災害復旧リーダーシップチーム、災害復旧管理チーム、災害復旧技術・導入チーム、災害復旧保護チームを設置する；

2）災害復旧の実施を支援するために外部の専門家を雇う場合、あるいは、実施チームおよび日常業務チームの業務の一部または全部を外部組織に委託する場合、外部の専門家または外部組織は適切な資格を有している。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.2.2 組織団体の責任

組織の義務テストの評価には以下のものが含まれる。

a) 評価方法

1）災害復旧リーダーシップ・チームのメンバーにインタビューを行い、災害復旧のための様々な組織構造の構成と責任が明確に定義されていることを確認する；

2）災害復旧リーダーシップチーム（Disaster Recovery Leadership Team: DRLT）のメンバーにインタビューを行い、DRLT の議長が組織のトップマネジメントの一人であること、また、DRLT の役割が情報システムの災害復旧に関する主要事項を主導し、意思決定することであることを確認する；

3）災害復旧リーダーシップチームのメンバーにインタビューを行い、災害復旧管理チームが組織の業務、技術、ロジスティクス、その他の関連部門の責任者で構成されているかどうか、また、彼らの責務が情報システムの災害復旧の管理と調整であるかどうかを確認する；

4）災害復旧リーダーシップ・チームのメンバーにインタビューを行い、災害復旧技術・実施チームが災害復旧センターの専門家、技術者、運用・保守スタッフ、サービス・プロバイダーで構成されているかどうか、また、彼らの責務が実施に特化したものであるかどうかを確認する；

5）災害復旧リーダーシップ・チームのメンバーにインタビューを行い、災害復旧支援チームが組織の人事およびロジスティクス・スタッフで構成されているかどうか、また、災害復旧に必要な資源の供給、災害復旧、災害が発生した場所の安全確保を責務としているかどうかを確認する。

(b) 期待される結果

1）災害復旧のための組織構造は、構成と責任の観点から明確に定義されている；

2）災害復旧リーダーシップチーム（Disaster Recovery Leadership Team: DRLT）は、組織のトップマネジメントのメンバーが議長を務め、その役割は、情報システムの災害復旧に関する主要事項を主導し、意思決定することである；

3）災害復旧管理チームは、組織の業務部門、技術部門、物流部門、その他関連部門の責任者で構成され、その責務は、情報システムの災害復旧を管理・調整することである；

4）災害復旧技術・実施チームは、災害復旧センターの専門スタッフ、技術スタッフ、運営・保守スタッフ、サービス・プロバイダーで構成され、それぞれの担当は実施に特化している；

5）災害復旧支援チームは、組織の人的資源とロジスティクス・スタッフで構成され、災害復旧に必要な資源の供給、災害復旧、災害現場の安全確保を担当する。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3 災害復旧計画と設計 試験と評価の方法論

10.3.1 災害復旧ニーズの決定

10.3.1.1 リスク分析

リスク分析テスト評価には以下のものが含まれる。

a) 評価方法

災害復旧管理チームのメンバーにインタビューし、災害復旧設計計画書またはリスク分析報告書をレビューし、リスク分析が情報システムの資産とその価値、直面する脅威と存在する脆弱性の特定、既存のリスク予防と管理対策の特定などを含んでいるかどうかを確認し、リスク評価が GB/T 20984-2022 標準を参照して実施されているかどうかをチェックする。分析活動を行う。

b) 期待される結果

リスク分析活動は、GB/T 20984-2022 を参考に、組織の業務に即して実施され、リスク分析には、情報システム資産とその価値、脅威と脆弱性の特定、既存のリスク防止・管理措置の特定が含まれる。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.1.2 ビジネスインパクト分析

ビジネスインパクト分析テストの評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧管理チームのメンバーにインタビューし、災害復旧設計計画をレビューして、組織のビジネス機能とその相関関係が特定されていること、各ビジネス機能をサポートする適切な情報システムとその他のリソースが特定されていること、関連する機密性、完全性、可用性（時間機密性を含む）の要件が特定されていることを確認する；

2）災害復旧設計計画を見て、さまざまなビジネス機能への中断の影響をアセスメントするために、定量的および／または定性的な方法が使用されていることをチェックする。

(b) 期待される結果

1）組織の業務機能及び各業務機能の関連性が完全に特定され、各業務機能をサポートする対応する情報システム及びその他の資源が特定され、関連する機密性、完全性及び可用性（時間機密性を含む）の要求事項が明確化されている；

2）さまざまなビジネス機能に対するディスラプションの影響は、定量的および／または定性的手法を用いてアセスメントされた。

c) 結果の判定：上記の期待される結果をすべて満たしていれば適合と判定し、そうでなければ不適合または部分適合と判定する。

10.3.1.3 災害復旧ニーズの決定

災害復旧を判断するためのニーズテスト評価には、以下のようなものがある。

a) 評価方法

災害復旧管理チームのメンバーにインタビューを行い、災害復旧設計計画をレビューし、リスク分析とビジネスインパクト分析の結果を組み合わせて情報システムの復旧優先順位を決定しているか、災害復旧目標が定義されているかを確認する。

b) 期待される結果

リスク分析とビジネスインパクト分析の結果を統合し、情報システムの復旧優先順位と災害復旧目標（RTO と RPO 指標を含む）を決定する。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.2 災害復旧戦略の策定

10.3.2.1 災害復旧戦略の要件

災害復旧戦略では、テスト評価に以下を含めることを求めている。

a) 評価方法

災害復旧管理チームのメンバーと面談し、災害復旧設計計画を見直し、組織がコストとリスクのバランス原則に従って業務機能の災害復旧戦略を策定しているかどうか、業務機能ごとに異なる災害復旧戦略の採用を実現できるかどうかを確認する。災害復旧戦略の要素に、GB/T 20984-2022 方式と附属書 C を参照した情報システムの分類と等級付け、災害復旧能力のレベルの決定、災害復旧資源の要素の入手方法の決定、災害復旧システムのセキュリティ要件の決定、災害復旧における互換性要件の決定が含まれているかどうかをチェックする。

b) 期待される結果

組織の災害復旧目標と組み合わせて、業務機能の災害復旧戦略は、コストとリスクのバランス原則に従って策定され、業務機能ごとに異なる災害復旧戦略の採用を実現することができる。災害復旧戦略の要素には、GB/T 20984-2022 の方法論と附属書 C を参照した情報システムの分類と等級付け、災害復旧能力のレベルの決定、災害復旧リソース要素へのアクセスの決定、災害復旧システムのセキュリティ要件の決定、災害復旧における互換性要件の決定が含まれる。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.2.2 災害復旧カテゴリーの計画

災害復旧カテゴリーの計画テスト評価には、以下のものが含まれる。

a) 評価方法

災害復旧管理チームのメンバーにインタビューし、災害復旧設計計画を見直し、サービス提供の重要性、適時性の要件、構築計画に従って災害復旧のカテゴリーが定義されているか、サービスのカテゴリーがデータレベル、アプリケーションレベル、ビジネスレベルのいずれか 1 つ以上であるかを確認する。

b) 期待される結果

組織の災害復旧目標と連動して、サービス提供の重要性、適時性の要件、構築計画に基づいて災害復旧のカテゴリーが定義され、そのカテゴリーはデータレベル、アプリケーションレベル、ビジネスレベルの 1 つ以上となる。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.2.3 災害復旧レイアウト計画

災害復旧レイアウト計画テスト評価には以下のものが含まれる。

a) 評価方法

災害復旧管理チームのメンバーにインタビューし、災害復旧設計計画をレビューして、組織がコストとリスクのバランス原則、および管理要件に基づいて災害復旧レイアウトモデルを定義しているかどうか、また、そのモデルがプライマリ、プライマリ-マルチプル、相互バックアップ、マルチプライマリ、マルチプルバックアップ、およびハイブリッドアプローチのいずれか 1 つ以上であるかどうかを確認する。

b) 期待される結果

組織の災害復旧の目的に合わせて、災害復旧のレイアウトモードは、コスト・リスクバランスの原則と管理要件に従って定義され、レイアウトモードは、1 マスター、1 バックアップ、1 マスター、複数バックアップ、複数マスター、1 バックアップ、ハイブリッドモードのいずれか 1 つ以上となる。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.2.4 災害復旧リソース要素

災害復旧リソース要素試験評価には以下のものが含まれる。

a) 評価方法

災害復旧管理チームのメンバーにインタビューを行い、災害復旧設計計画または災害復旧計画を確認し、災害復旧関連のリソース要素を検証し、災害復旧の各能力レベルに必要なリソース要素が包括的であることを確認する。

b) 期待される結果

災害復旧の各能力レベルに必要なリソース要素は包括的であり、データバックアップと災害復旧システム、スタンバイデータプロセッシングシステム、スタンバイネットワークシステム、スタンバイインフラ、専門技術サポート能力、運用、保守、管理能力、災害復旧計画を含む。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.2.5 クラウド・コンピューティング技術を利用した災害復旧リソース要素

クラウドコンピューティング技術を使った災害復旧リソース要素のテストの評価には、以下のようなものがある。

a) 評価方法

1) 災害復旧管理チームのメンバーにインタビューを行い、クラウド・コンピューティング技術が採用されているかどうかを確認する；

2) 災害復旧管理チームのメンバーにインタビューを行い、災害復旧設計計画をレビューし、災害復旧関連のリソース要素を検証することで、クラウドコンピューティング技術の採用における災害復旧の各能力レベルに必要なリソース要素が包括的であるか、オンクラウ

ド、オフクラウド、クロスリージョン、クロスクラウドのシナリオの適用可能性と互換性要件が考慮されているかを確認する。

(b) 期待される結果

1）この組織は、クラウド災害復旧サービスモデルを使用している；

2）災害復旧リソースの要素を満たすことを前提に、オンクラウド、オフクラウド、クロスリージョン、クロスクラウドのシナリオの適用性と互換性の要件が十分に考慮されている。

(c) 結果の判定

上記の期待される結果がすべて満たされ適合と判定された場合、1）は満たされず不適合と判定され、それ以外は不適合または一部適合と判定される。

10.3.3 災害復旧技術プログラムの設計

10.3.3.1 災害復旧リソースへの要件とアクセス

10.3.3.1.1 データバックアップ災害復旧システム

データバックアップ災害復旧システム試験評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧技術と実施チームのメンバーにインタビューし、災害復旧技術プログラムを確認し、データバックアップと災害復旧システムが災害復旧とデータバックアップの範囲、データバックアップの時間間隔、データバックアップと災害復旧の技術とメディア、データバックアップと災害復旧システムのセキュリティ要件などを定義しているかどうかをチェックし、災害復旧技術プログラムにデータの整合性と完全性の検証に関連する指示が含まれているかどうかをチェックする；

2）データバックアップ災害復旧システムが、他機関のシステムまたはクラウドベンダーが提供するサービスをレンタルすることによって取得されている場合、災害復旧技術・実施チームのメンバーにインタビューを行い、他機関が提供する災害復旧技術ソリューションと契約を確認し、データバックアップ災害復旧システムが包括的な内容であるかどうかを判断することを確認する。

(b) 期待される結果

1）コストとリスクのバランスをとるという原則に従い、組織は、データバックアップと災害復旧システムの災害復旧とデータバックアップの範囲、データバックアップの時間間隔、データバックアップと災害復旧の技術とメディア、データバックアップと災害復旧システムのセキュリティ要件を定義した；

2）データバックアップおよび災害復旧システムが、他の組織のシステムまたはクラウドベンダーが提供するサービスをレンタルすることによって取得される場合、データバックアップおよび災害復旧システムは災害復旧の目的を満たしている。データバックアップ・災害復旧システムのリース契約またはサービス契約が有効であり、契約には災害復旧とデータバックアップの範囲、データバックアップの時間間隔、データバックアップ・災害復旧の技術とメディア、データバックアップ・災害復旧システムのセキュリティ要件が規定されている。

3）災害復旧技術プログラムのデータバックアップと災害復旧システムに関連する文書は完全であり、データ災害復旧システムの要件とアクセス方法を含み、データの一貫性と完全性の検証要件と方法を記述している。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.3.1.2 代替データ処理システム

代替データ処理システムのテスト評価には以下のものが含まれる。

a) 評価方法

1）災害復旧技術・実施チームのメンバーと面談し、災害復旧技術計画を確認し、代替データ処理システムが、データ処理能力、プライマリシステムとの互換性要件、通常準備状態か稼働中か、レイアウト計画などの観点から、コスト・リスクバランス原則に従って特定されているかどうかを確認する；

2）災害復旧技術および実施チームのメンバーへのインタビュー、災害復旧技術計画のレビュー、バックアップデータ処理システムへのアクセス方法のチェック、技術計画にシステムの動作環境およびソフトウェアのバージョン互換性に関する記述があるかどうかのチェック。

(b) 期待される結果

1）組織は、バックアップ・データ処理システムのデータ処理能力、プライマリ・システムとの互換性要件、通常の準備状態か運用状態か、レイアウト計画などを規定する；

2）すなわち、事前にベンダーと緊急供給契約を結ぶ方法、必要な機器を事前に購入し、災害復旧センターや安全な機器倉庫に保管する方法、商業災害復旧センターや契約を結んだ組織にすでにある互換性のある機器をレンタルする方法である；

3）災害復旧技術プログラムにおける待機データ処理システムに関連する文書の内容が、リソース要件やアクセス方法を含めて完全であり、その内容が関連する要件に沿ったものであり、システムの動作環境やソフトウェアのバージョン等に関して、待機データ処理システムと本番環境のデータ処理システムとの互換性に関連する要件や方法が記述されている。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.3.1.3 代替ネットワークシステム

代替ネットワークシステムのテスト評価には以下のものが含まれる。

a) 評価方法

1）災害復旧技術・実施チームのメンバーにインタビューを行い、災害復旧技術ソリューション文書を確認し、災害復旧リソース要件決定プロセスが災害復旧目標に基づいて代替ネットワークシステム要件を特定し、代替ネットワークシステム要件が代替ネットワークシステムの構築要件を満たしていることを確認する；

2）災害復旧の技術的解決策に関する文書を確認し、例えば、事前に緊急供給契約を締結したり、必要な機器を購入したりして、バックアップ・ネットワーク・システムにアクセスできるかどうかを確認する；

3）災害復旧のテクニカル・ソリューションのドキュメントを確認し、バックアップ・ネットワーク・システムが自前のデータ通信回線を使用しているのか、リースした公衆データ通信回線を使用しているのかをチェックする。

(b) 期待される結果

1）組織は、災害復旧リソースの必要性に基づいて、代替ネットワークシステムのリソース要件とアクセスを定義している；

2）災害復旧技術計画における待機ネットワークシステムに関連する文書の内容が完全であり、待機ネットワークシステムの資源の要件及びその入手方法を含み、その内容が関連する要件に適合している。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.3.1.4 代替インフラストラクチャー

代替インフラテストの評価には以下のものが含まれる。

a) 評価方法

1）災害復旧技術・実施チームのメンバーへのインタビュー、災害復旧技術ソリューション文書のレビュー、災害復旧リソース要件決定プロセスが災害復旧目的に基づいて代替インフラを特定していること、代替インフラ要件にプライマリセンターへの近接性、サイト、環境、運用・保守、管理要件などが含まれていることを確認する；

2）災害復旧技術・実施チームのメンバーにインタビューを行い、災害復旧技術プログラム文書を確認し、待機インフラが所有、共同建設、リースのいずれかの方法で取得されたかを確認する。

(b) 期待される結果

1）組織は、災害復旧リソース要件、およびプライマリセンターからの距離、サイト、環境、運用、保守、管理要件を含む代替インフラ要件に基づいて、代替インフラリソース要件とアクセスを指定する；

2）災害復旧技術計画のスタンバイネットワークシステムに関する文書が完全であり、スタンバイインフラ要件とアクセス方法を含み、内容が関連要件を満たしている。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.3.1.5 専門的技術支援能力

専門的技術支援能力テストの評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧技術・実施チームのメンバーにインタビューを行い、災害復旧技術ソリューション文書を確認し、災害復旧リソース要件決定プロセスが、災害復旧目標に従って、ソフトウェア、ハードウェア、ネットワークの分野における災害復旧センターの技術サポート能力の要件とアクセスを特定しているかどうかを確認する；

2）災害復旧技術・実施チームのメンバーにインタビューを行い、災害復旧技術プログラムの文書を確認し、専門技術支援の組織構造、様々なタイプの技術者の数と質、管理システムが確立されているかなどをチェックする。

(b) 期待される結果

1）組織は、災害復旧リソースの必要性に基づいて、専門的なテクニカルサポートの要件とアクセスを定義している；

2）災害復旧技術ソリューションにおける専門的技術サポートの要件には、組織構造、様々なタイプの技術者の数と質、管理体制が含まれる。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.3.1.6 O&M 管理能力

O&M 管理能力試験評価には以下のものが含まれる。

a) 評価方法

1）災害復旧技術・実施チームのメンバーと面談し、災害復旧技術プログラム文書を確認し、災害復旧資源要件決定プロセスが、災害復旧目標に従って O&M 管理能力要件とアクセスを特定していることを確認する；

2）災害復旧技術・実施チームのメンバーにインタビューを行い、災害復旧技術プログラムの文書を確認し、運営・維持管理の組織構造、各種技術者の数と質、管理体制が整備されているかどうかをチェックする。

(b) 期待される結果

1）組織は、災害復旧リソースの必要性に基づいて、O&M 管理能力の要件とアクセスを定義している；

2）災害復旧技術プログラムにおける運用・維持管理能力の要件には、組織構造、様々なタイプの技術者の数と質、管理システムが含まれる。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.3.1.7 災害復旧計画

災害復旧計画のテスト評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧技術・実施チームのメンバーにインタビューを行い、災害復旧計画が実施されているかどうかを確認する；

2）災害復旧技術計画書を見直し、災害復旧計画全体、策定プロセス、教育、訓練、演習、管理要件が明確に定義されているか、計画の作成が災害復旧の当初の策定要件を満たしているかを確認する。

b) 期待される結果

その組織は、災害復旧計画を策定している。この計画は完全なもので、全体、策定プロセス、教育、訓練、管理要件が含まれている。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.3.1.8 クラウド災害復旧サービス

クラウド災害復旧サービスのテスト評価には以下のものが含まれる。

a) 評価方法

1）DRT&IT（Disaster Recovery Technology and Implementation Team）のメンバーにインタビューを行い、クラウド災害復旧サービスモデルを使用しているかどうかを確認した；

2）災害復旧技術・実装チームのメンバーにインタビューを行い、災害復旧技術ソリューション文書を確認し、組織が災害復旧目的に基づいてサービス要件を特定していることを確認する。サービス要件に、データレベルの災害復旧機能、アプリケーションレベルの災害復旧のためのテイクオーバー機能、システムアーキテクチャと互換性機能の要件、本番用クラウドプラットフォームから独立したオフサイトのクラウドプラットフォームシステムが含まれているかどうかを確認する；

3）災害復旧技術・実施チームのメンバーにインタビューを行い、災害復旧技術ソリューション文書を確認し、組織が所有または運営する、あるいは外部機関が提供するリース災害復旧サービスを利用したサービスへのアクセス方法が明記されていることを確認する。

(b) 期待される結果

1）この組織は、クラウド災害復旧サービスモデルを使用している；

2）同組織は、クラウド災害復旧サービスの要件を策定した。これには、データレベルの災害復旧機能、アプリケーションレベルの災害復旧のためのテイクオーバー機能、システムアーキテクチャと互換性機能の要件、本番用クラウドプラットフォームから独立したオフサイトのクラウドプラットフォームシステムなどが含まれる；

3）組織が所有または運営する災害復旧サービス、あるいは外部組織からリースした災害復旧サービスを利用した、クラウド災害復旧サービスの取得を規定する。

c) 結果の判定 上記の期待される結果がすべて満たされている場合は適合、1)が満たされていない場合は非適合、それ以外は不適合または部分適合となる。

10.3.3.2 災害復旧システムのセキュリティ要件

災害復旧システムのセキュリティ要件テストの評価には、以下のものが含まれる。

a) 評価方法

災害復旧管理チームのメンバーと面談し、災害復旧技術ソリューション文書を確認し、災害復旧システムのサイバーセキュリティ要件が、それがホストする情報システムの最高レベルを下回っていないことを確認する。

b) 期待される結果

災害復旧システムのサイバーセキュリティ要件は、それがホストする情報システムの最高レベルに劣らない。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.4 災害復旧センターの所在地と格付け

10.3.4.1 災害復旧センター用地の選定

災害復旧センターのサイトテスト評価には、次のようなものが含まれた。

a) 評価方法

1）災害復旧管理チームのメンバーにインタビューし、災害復旧技術計画文書をチェックし、災害復旧センターの立地選定が GB 50174-2017 の関連要求に合致しているかどうか、同じ都市の災害復旧センターと異なる立地の災害復旧センターと生産センターの間のセキュリティ距離と住所条件の違いの要求を十分に考慮しているかどうか、重要な国家戦略レベルの災害復旧センターが反検知、攻撃などの要素の要求を考慮しているかどうかをチェックする。重要な国家戦略レベルの災害復旧センターの立地選定は、探知防止や攻撃防止などの要素を考慮しているかどうか；

2）災害復旧管理チームのメンバーと面談し、災害復旧技術計画文書をレビューし、GB 50174-2017 の階層要件を参照して組織が災害復旧センターのインフラを構築していることを確認する。

(b) 期待される結果

1）災害復旧センターの位置は、関連する国の基準および関連する技術的要件に準拠している；

2）災害復旧センターのインフラは、GB 50174-2017 の格付け要件に従って構築されている。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.4.2 災害復旧センターのインフラレベル

災害復旧センターのインフラの評価テストには、以下のものが含まれる。

a) 評価方法

1）災害復旧管理チームのメンバーにインタビューを行い、災害復旧技術計画文書を確認し、GB 50174-2017 の階層要件を参照して組織が災害復旧センターのインフラを構築していることを確認する；

2）災害復旧管理チームのメンバーにインタビューを行い、災害復旧技術ソリューションの文書を確認し、災害復旧センターのインフラが本番センターと同等か、それよりも 1 段階低いレベルに格付けされていることを確認する。

(b) 期待される結果

1）災害復旧センターのインフラは、GB 50174-2017 の格付け要件に従って構築されている；

2）災害復旧センターのインフラのレベルは、本番センターのレベルと同じか、1 つ下のレベルである。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.3.5 災害復旧技術プログラムの検証と妥当性確認

災害復旧技術プログラムの検証テスト評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧管理チームのメンバーと面談し、組織の関連部署が技術的ソリューションを検証・確認したことを確認する；

2）災害復旧技術プログラム文書のレビューと認証資料の検証を行い、認証資料にデータの完全性と整合性の検証、データのバックアップと復旧能力の検証、情報システムの切り替えとカットバック能力の検証、ネットワークシステムの切り替えとカットバック能力の検証、システムセキュリティの検証、その他の内容が含まれているかどうかを確認する。

(b) 期待される結果

1）災害復旧技術プログラムは、組織によって見直され、検証された；

2）災害復旧技術プログラムの検証には、データの完全性と整合性の検証、データのバックアップと復旧能力の検証、情報システムの切り替えとカットバック能力の検証、ネットワークシステムの切り替えとカットバック能力の検証、システムセキュリティの検証が含まれ、関連する記録と文書が完備されている。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.4 災害復旧システムおよびセンター構築の試験・評価方法

10.4.1 災害復旧システムの構築

10.4.1.1 実施プログラムの開発

災害復旧システム構築実施プログラム開発テスト評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧技術・実施チームにインタビューを行い、災害復旧のニーズと計画設計に基づき、災害復旧システム実施計画が標準的な方法で策定され、文書化されているかどうかを確認する；

2）災害復旧システムの実施計画を閲覧し、実施計画が、構築目的と構築内容、技術的な実施計画、システムおよびコンポーネントのセキュリティ機能と性能要件、システムおよびコンポーネントの配置、セキュリティ管理方針と構成、付随するセキュリティ管理構築内容、エンジニアリング実施計画、プロジェクト投資見積もりを網羅しているかどうかを確認する。

(b) 期待される結果

1）災害復旧のニーズと計画・設計に基づき、災害復旧システムの実施計画を策定し、標準化された文書を作成する；

2）災害復旧システム実施計画には、構築目的と構築内容、技術的実施計画、システムとコンポーネントのセキュリティ機能と性能要件、システムとコンポーネントの配備、セキュリティ管理戦略と構成、サポートするセキュリティ管理構築内容、エンジニアリング実施計画、プロジェクト投資見積もりが含まれる。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.4.1.2 システムの展開と構成

災害復旧システム構築システムの展開と構成テストの評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧技術および実施チームの担当者へのインタビュー、災害復旧システム実施計画のレビュー、災害復旧システム構築中の展開準備、システム展開、システム設定作業の視察；

2）品質管理プログラムが実施されているかどうかを確認し、それが有益かどうかを評価する；

3）災害復旧システムに関連するソフトウェアおよびハードウェア製品にテストレポートがあるかどうかを確認し、その信憑性と妥当性をアセスメントする；

4）災害復旧システムの現地調査を行い、災害復旧システム導入計画に従って、関連する製品またはモジュールが実際のアプリケーション環境に正しく導入されているかどうかを確認し、システム導入のすべての側面が品質管理プログラムの要件を遵守し、品質管理目標を達成しているかどうかを確認する；

5）災害復旧アプリケーションシステムのハードウェアとソフトウェアの構成、および本番センターと災害復旧センターのネットワーク構成を確認し、関連する構成が正しいかどうかをチェックするとともに、災害復旧システムと待機ネットワークシステムが正常に動作しているかどうかをチェックする。

(b) 期待される結果

1）災害復旧システム構築のプロセスは、展開準備、システム展開、システム構成という観点から実施された；

2）品質管理プログラムは実施されており、参考になる；

3）災害復旧システム関連のハードウェアおよびソフトウェア製品には、真正かつ有効なテストレポートがある；

4）災害復旧システムは、実装計画に従って、関連する製品またはモジュールを実際のアプリケーション環境に正しく配置し、システム実装のすべての側面が品質管理プログラムの要件に準拠し、品質管理目標を達成していることを確認する；

5）災害復旧アプリケーションシステムのハードウェアとソフトウェアの構成、本番センターと災害復旧センターのネットワーク構成が正しく、災害復旧システムとバックアップネットワークシステムが正常に動作している。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.4.1.3 システムテスト

災害復旧システム構築のためのシステムテスト評価には、以下のようなものがある。

a) 評価方法

1）災害復旧要件、計画・設計文書と合わせて、システムテスト文書をレビューし、計画・設計の機能、性能、セキュリティがテストされていることを確認する；

2）災害復旧アプリケーションをホストするハードウェアとソフトウェア、本番センターと災害復旧センター間のネットワーク、災害復旧システムのセキュリティのテストを確認するために、システムテスト文書を見直す。

(b) 期待される結果

1）災害復旧要件および計画・設計文書に従い、災害復旧システムの計画・設計の機能、性能、セキュリティをテストする；

2）テストには、災害復旧アプリケーションシステムをホストするハードウェアとソフトウェア、本番センターと災害復旧センター間のネットワーク、災害復旧システムのセキュリティなどが含まれる。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.4.1.4 検収および引渡し

災害復旧システム構築受入・引渡試験評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧技術・実施チームのメンバーにインタビューを行い、受入プログラム、受入報告書などの文書を確認し、受入準備、受入組織、システム提供、訓練などが実施されているかを確認する；

2）災害復旧技術・実施チームのメンバーにインタビューを行い、受入プログラムを設計したかどうか、設計プログラムの要件を満たしているかどうかを確認する；

3）災害復旧技術および導入チームのメンバーにインタビューを行い、受入テストが受入プログラムに従って実施されたかどうかを確認し、受入テスト文書をレビューして、詳細設計プログラムと連携して機能、パフォーマンス、セキュリティをテストしたかどうかを確認する；

4）災害復旧技術・実施チームのメンバーに、テスト終了後に受入報告書を作成したかどうかを聞き取り、受入報告書をレビューし、受入コメントと受入結論が明確に記載されているか、変更を示唆するものについては、修正と再受入を確認する；

5）災害復旧技術・実施チームのメンバーにシステムの納品が行われたかどうかを聞き取り、納品記録を確認し、検収報告書、納品チェックリスト、管理者マニュアル、ユーザーマニュアル、セキュリティ概要書、システム構成マニュアル、各種操作手順書、管理システムの納品を確認する；

6）災害復旧技術・実施チームのメンバーから、技術支援組織の設立の有無や訓練の実施状況について聞き取り、技術支援記録や訓練記録を確認し、技術支援組織の設立の有無やその能力、訓練の実施の有無や頻度などをチェックする。

(b) 期待される結果

1）検収・引渡しプロセスは、検収の準備、検収の組織化、システムの引渡し、トレーニングのために実施された；

2）受入プログラムを設計し、設計プログラムの要件を満たす；

3）受入テストは、受入プログラムに従って実施され、受入テスト文書には、詳細な設計計画、機能性、性能、セキュリティのテストが含まれる；

4）受入報告書を作成するためのテストが完了した後、報告書には、推奨事項の変更案、修正案、再受入について、意見の受入と結論の受入が明確に記載される；

5）システムは、検収報告書、納品チェックリスト、管理者マニュアル、ユーザーマニュアル、セキュリティ概要、さらにシステム構成マニュアル、各種操作手順書、管理システムとともに納品された；

6）技術支援組織の設立と定期的な研修。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.4.2 災害復旧センター建設

10.4.2.1 代替インフラ整備

災害復旧センター建設待機インフラ構築試験評価には、以下のものが含まれる。

a) 評価方法

1）建設実施文書をチェックし、現場での待機インフラの建設をチェックし、作業設備（情報システム作業設備、保障システム作業設備を含む）、補助設備、生活支援設備、その他必要なエリアが含まれているか、その建設が GB 50174-2017 標準の要求に沿っているかをチェックする；

2）新規建設や災害復旧センターのインフラ選定の場合、建設・実施書類のチェック、待機インフラ建設の現地視察が行われ、関連する標準や開発計画の要求事項に従って建設が行われているか、災害復旧作業の遂行に必要な通信、電力、地質、気象資源、災害復旧要員や機材の到着を容易にする輸送のための条件が整っているかなどが確認される；

3）災害復旧センターの新規建設やインフラの選定については、建設実施書類のチェック、現場での待機インフラの建設状況のチェック、建設管理チームの設置の有無、建設請負業者、コストコンサルタント、建設監督者の技術資格、関連プロジェクトの経験事例などをチェックし、彼らがプロジェクトに対応した技術資格とデータセンター建設の経験を有しているかどうかをチェックする。

(b) 期待される結果

1）バックアップインフラの建設には、作業施設（情報システム作業施設、保障システム作業施設を含む）、補助施設、生活支援施設、その他必要な区域が含まれ、関連施設の建設は GB 50174-2017 標準の要求を満たしている；

2）新たな災害復旧センターのインフラを建設または選定する場合は、関連する標準に準拠した要件および開発計画に従って建設し、災害復旧作業の実施に必要な通信、電力、地質、

気象資源などの条件、および災害復旧要員や機材の到着を容易にする輸送条件を備えなければならない；

3）新たな災害復旧センターのインフラを建設または選定する場合、建設管理チームが設置され、建設請負業者、コストコンサルタント、建設監督者は、エンジニアリングの資格、および関連プロジェクトの経験を有する。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.4.2.2 データバックアップ災害復旧システムの構築

災害復旧センター構築データバックアップ災害復旧システム構築試験評価には以下のものが含まれる。

a) 評価方法

1）災害復旧センターと本番センターのデータの整合性と完全性の検証文書を見直し、復旧センターと本番センターのデータを別々に見直し、整合性と完全性が有効であることを確認する；

2）複数の生産センターが共有する災害復旧センターについては、建設と実施に関する文書をチェックし、現場のデータバックアップと災害復旧システムの構築をチェックし、災害復旧センター内の異なる生産システムのバックアップデータが安全な方法で設計され、実施されているかどうかをチェックし、そのセキュリティが有効かどうかをテストし、検証する。

(b) 期待される結果

1）災害復旧センターと本番センターのデータには一貫性と完全性があり、データの一貫性と完全性の必要な検証は、システムの導入時に実施される；

2）複数のプロダクション・センターが共有する災害復旧センターでは、災害復旧センター内の異なるプロダクション・システムのバックアップ・データが十分に考慮され、セキュリティは効果的である。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.4.2.3 代替データ処理システム開発

災害復旧センター建設のための代替データ処理システム構築の試験評価には、以下の要素が含まれる。

a) 評価方法

1）バックアップ・データ処理システムを現地で視察し、システムの動作環境やソフトウェアのバージョンなど、本番システムと完全に互換性があることを確認する；

2）待機データ処理システムの運用能力に関するテストバリデーション文書をレビューし、テストバリデーションが実施されたかどうか、およびその有効性を確認する。

(b) 期待される結果

1）バックアップのデータ処理システムは、システムの動作環境やソフトウェアのバージョンにおいて、本番システムと完全な互換性がなければならない；

2）バックアップデータ処理システムを構築する際、運用能力のテスト検証を行い、テスト検証は有効であった。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部不適合」と判定される。

10.4.2.4 代替ネットワークシステム構築

災害復旧センター構築バックアップネットワークシステム構築テスト評価には、以下の内容が含まれる。

a) 評価方法

複数の本番センターが共有する災害復旧センターについては、スタンバイネットワークシステムとネットワークデバイスのセキュリティ隔離ポリシーと構成を見直し、本番システムごとにセキュリティ隔離が行われているか、セキュリティ隔離対策が有効であるかをテストして、その有効性を検証する。

b) 期待される結果

複数のプロダクション・センターが共有する災害復旧センターでは、バックアップ・ネットワーク・システムは、異なるプロダクション・システムのセキュリティ分離を提供し、災害復旧センター内の複数のプロダクション・システムのネットワーク相互運用性に起因するセキュリティ・リスクを回避することができる。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部不適合」と判定される。

10.5 災害復旧システムの安全性構築のための試験評価手法

10.5.1 ネットワーク・セキュリティ・レベルの保護

災害復旧システム・セキュリティ・ビルディング・ネットワーク・セキュリティ・レベルの保護テスト評価には、以下のものが含まれる。

a) 評価方法

災害復旧リーダーグループの責任者にインタビューを行い、評定、ファイリング、評価の証明書を確認し、GB/T 22239-2019 を参考に、災害復旧システムがネットワークセキュリティレベルの保護レベル要件に従って安全に構築されているかどうかを確認する。

b) 期待される結果

災害復旧システムは GB/T 22239-2019 に準拠し、ネットワークセキュリティレベルの保護レベルの要求に従って安全に構築されている。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.5.2 セキュリティ管理システム

災害復旧システムのセキュリティビルのセキュリティ管理システムの試験評価には、以下のものが含まれる。

a) 評価方法

1）計画策定、目標設定、実施戦略のプロセスを理解するために、準備の責任者である災害復旧管理チームおよび災害復旧技術・実施チームの専門スタッフおよび技術スタッフにインタビューを行う。災害復旧セキュリティ保護計画文書をレビューし、その計画に管理システム、技術システム、運用・保守システム、保護システムに関する詳細な計画が含まれているかどうかをチェックする。さらに、計画文書が承認され、関係者に送付されているかどうかを確認する；

2）災害復旧保護チームの人事・後方支援担当者にインタビューを行い、資源保護の戦略と実施状況を把握する。また、制度、人員、資金、設備などの資源の保護について確認するため、関連する予算配分記録、人員訓練記録、設備の調達・保守記録などを確認する；

3）災害復旧管理チームの責任者にインタビューし、改訂・更新プロセスにおいて考慮 された要因及び実施された改善策について質問する。災害復旧システムのセキュリティポリシー文書の改訂記録（改訂日、改訂内容、 承認プロセスなど）を確認することにより、セキュリティポリシーが少なくとも年 1 回改訂されているか、または重要な変更があった場合に更新されているかを確認する；

4）災害復旧技術・実施グループのチームメンバに面談し、新たなセキュリ ティリスクや脅威がどのように特定され、対応されているかを理解する。リスク評価報告書やポリシーの調整記録をレビューすることにより、セ キュリティリスクや脅威の変化に応じて管理システムやセキュリ ティポリシーが適宜調整されていることを検証する。

(b) 期待される結果

1）組織には、管理システム、技術システム、運用・保守システム、保証システムを詳述した包括的な災害復旧セキュリティ保護計画がある。この計画書は適切に承認され、関係者に配布され、すべての関係者が災害復旧の目的と戦略を認識していることを確認する；

2）組織は、災害復旧のための安全保障を支援するために、機関、人員、資金、設備などの資源を適切に確保することができる。予算配分、職員研修、機材調達、維持管理はきちんと文書化されており、組織が適切な資源確保策を講じていることを反映している；

3）災害復旧システムのセキュリティポリシー文書が、少なくとも年 1 回改訂されるか、システム又は環境に重大な変更があった場合は適時に更新される。改訂記録には、改訂日、改訂内容、承認プロセスが記載され、最新かつ効果的なセキュリ ティポリシーを維持するという組織のコミットメントを示す；

4）組織は、新たなセキュリティリスクや脅威を効果的に特定し、対応することができる。リスク評価報告書や方針調整記録から、セキュリティリスクや脅威の変化に応じて管理体制やセキュリティ方針が適宜調整され、災害復旧対策の有効性が常に最新の状態に保たれていることがわかる。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.5.3 セキュリティ管理アーキテクチャ

災害復旧システムのセキュリティ・ビルディング・セキュリティ管理試験評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧管理チームの責任者と面談し、組織図と関連する職務内容文書を確認し、災害復旧システムのセキュリティ保護を担当する専任の管理者が災害復旧組織構造の中で明確に指定されていることを確認する；

2）災害復旧セーフガード・チームの人事担当者にインタビューを行い、評価方針、監督プロセスの文書、説明責任システムの実施記録を確認し、災害復旧システムの安全と保護のための評価・監督・説明責任メカニズムが確立されているかどうかをチェックする；

3）災害復旧セキュリティ管理機関の職員にインタビューし、意思決定システムの文書を検討し、災害復旧セキュリティ管理機関の職員が災害復旧に関する組織の意思決定システムに含まれていることを確認する。

(b) 期待される結果

1）組織は、災害復旧システムのセキュリティ保護を管理する責任者を明確に指名し、組織構造の中で明確な責任と権限を与えている。災害復旧システムのセキュリティ保護に関する評価と監視の説明責任の仕組みが存在し、その仕組みが効果的に実施されたことを証明する記録がある；

2）災害復旧セキュリティ管理機関の職員は、組織の意思決定システムに効果的に組み込まれ、災害復旧計画のセキュリティが十分に考慮され実施されるよう、意思決定プロセスにおいて役割を果たすことができる。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.5.4 セキュリティ・マネージャー

災害復旧システムのセキュリティ構築セキュリティ管理者試験評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧保証チームの人事評価担当者にインタビューし、災害復旧システ ムの重要な役職に就いている人のセキュリティスキルが評価されているかど うかを確認する；

2）災害復旧保証チームの人材評価担当者及び訓練参加者にヒアリングを行い、災害復旧システムのセキュリティ教育訓練体制、訓練記録等の文書を確認し、災害復旧システムのセキュリティ教育訓練体制が整備され、定期的なセキュリティ教育訓練及び技能評価が実施されているかを確認する；

3）人事評価を担当する災害復旧セキュリティチームの関係者にインタビューを行い、人事異動の記録などの文書を確認し、災害復旧システムのセキュリティ管理機関の責任者及び重要な地位にある人員の身元及びセキュリティ経歴が変更された場合に、組織が関連する要求事項に従って再検証を実施しているかどうかを確認する；

4）災害復旧保証チームおよび関連する実務者にインタビューを行い、セキュリ ティおよび機密保持契約の写しを閲覧し、セキュリティおよび機密保持に関 する実務者の義務と義務が明確化されているか、また、関連する担当者がセキュリ ティおよび機密保持契約に署名しているかどうかを確認する。

(b) 期待される結果

1）災害復旧システムの要職にある要員は、セキュリティ技能試験に合格しており、試験記録は完全である；

2）組織は、災害復旧システムのセキュリティ教育・訓練システムを確立し、効果的に実施している。また、定期的な訓練と評価を実施し、職員のセキュリティ意識とスキルレベルを高めている；

3）セキュリティー管理組織の責任者や要職に就いている人員が変更されたことを受け、当組織は、すべての要員がセキュリティー要件を満たしていることを確認するため、適時に身元およびセキュリティー経歴の確認を行っている；

4）すべての実務家は、セキュリティーと機密保持の義務と義務を認識し、セキュリティーと機密保持に関する意識を強化するために、セキュリティーと機密保持に関する同意書に署名している。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.5.5 安全な通信ネットワーク

10.5.5.1 ネットワーク・アーキテクチャ

災害復旧システムのためのセキュア通信ネットワーク・アーキテクチャ・テストの評価には、以下のものが含まれる。

a) 評価方法 災害復旧技術・実施チームの技術スタッフにヒアリングし、ネットワークアーキテクチャー設計に関する資料を確認し、災害復旧システムの通信回線が「1 メイン・複数バックアップ」を実現しているか、複数のネットワーク事業者の複数ルートで保護されているかを確認する。重要なネットワークノードと重要な設備の構成とネットワークトポロジー図を

チェックし、重要なネットワークノードと重要な設備が「デュアルノード」の冗長バックアップを持っているかどうかをチェックする。

b) 期待される結果

災害復旧システムの通信回線は、「メイン１本、バックアップ複数本」の構成とし、複数のキャリアをカバーすることで、メイン回線に障害が発生した場合でもバックアップ回線にシームレスに切り替えられるようにし、途切れのない通信を確保する。ネットワークの主要ノードと重要施設は、「ダブルノード」冗長バックアップ戦略を採用し、システムの信頼性と耐障害性を向上させる。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.5.5.2 相互接続セキュリティ

災害復旧システム用セキュア通信ネットワークの相互接続セキュリティテストの評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧管理チームの責任者にインタビューし、相互接続セキュリティ関連文書を確認し、災害復旧システムと異なる業務システム間、異なる地域のシステム間、異なる事業者が運営するシステム間で、セキュリティ相互接続ポリシーが確立または改善されているかどうかを確認する；

2）災害復旧管理チームリーダーにインタビューし、ユーザー管理システムおよびアクセス制御ポリシーに関連する文書および構成を確認し、ローカルおよびオフサイトの災害復旧システムで同一ユーザーのユーザーID およびアクセス権が一貫しているかどうかをチェックする。これは、ユーザーアカウント情報、権限割り当て記録、および同期メカニズムを確認することによって行うことができる；

3）災害復旧管理チームの技術スタッフにインタビューを行い、遠隔通信のセキュリティ保護に関する文書や設定を確認し、異なる LAN から遠隔通信を行う災害復旧システム間でセキュリティ保護対策が実施されているかどうかを確認する。

(b) 期待される結果

1）組織は、災害復旧システムと、異なる業務システム、異なる地域システム、異なるオペレーターシステムとの間の安全な相互接続戦略を確立または改善し、すべての接続がセキュリティ要件を満たすようにしている；

2）同じユーザーが、ローカルおよびオフサイトの災害復旧システムで同じユーザー ID とアクセス権を持つ；

3）ファイアウォール、暗号化装置、VPN、ネットワーク侵入防御を含むがこれに限定されない効果的なセキュリティ対策が、異なる LAN をまたぐ遠隔通信のための災害復旧システム間で実施されている。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.5.5.3 境界防御

災害復旧システムの安全な通信境界保護テストの評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧技術・実施チームの技術スタッフにインタビューを行い、ネットワーク・アーキテクチャやセキュリティ・ボーダー保護に関する文書や設定を確認し、異なる業務システム、地域システム、オペレーター・システム間の災害復旧システムの相互運用性、データ交換、情報の流れが厳密に管理されているかどうかをチェックする；

2）災害復旧技術・実施チームの技術スタッフにインタビューを行い、国境デバイスのアクセス制御ポリシー構成を確認し、国境を越えた災害復旧システムへのアクセスとデータフローが国境デバイスの制御されたインターフェイスを介して通信されていることを確認する。

(b) 期待される結果

1）災害復旧システムは、異なる業務システム間、異なる地域のシステム間、異なる事業者が運営するシステム間の相互運用性、データ交換、情報の流れを厳密に管理する；

2）災害復旧システムへのアクセスと、境界を越えたデータフローは、境界・デバイス上の制御されたインターフェイスを通じて通信される。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.5.5.4 セキュリティ監査

災害復旧システム用セキュア通信ネットワークのセキュリティ監査テスト評価には、以下が含まれる。

a) 評価方法

1）災害復旧技術・実施チームの監査管理担当者にヒアリングを行い、監査戦略に関する文書や構成、監査ログ記録などを確認し、災害復旧システムにおけるデータのバックアップ、復旧、削除、移行、システム構成変更などの業務が監査されているかを確認する；

2）災害復旧技術および実施チームの担当者にインタビューを行い、監査管理システムの関連するアクセス制御ポリシーを確認し、適切な権限を持つユーザーのみが監査データを閲覧できるかどうかをチェックする；

3）災害復旧技術・実施チームの監査ログ管理を担当する技術スタッフにインタビューを行い、監査管理システムの構成と監査ログを確認し、関連するログデータの保存期間が 6 ヶ月以上であるかどうかを確認する。

(b) 期待される結果

1）データのバックアップ、リカバリ、削除、移行、システム構成の変更など、災害復旧システムの操作が監査される；

2）監査データは、効果的な管理機能によって保護されており、権限を与えられたユーザーのみが監査データにアクセスできるようにアクセス制御が行われている；

3）監査ログデータは、6 ヶ月以上の期間保持される。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.5.6 安全なコンピューティング環境

10.5.6.1 本人確認と承認

災害復旧システムのための安全なコンピューティング環境の識別と認可テストの評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧管理チームの責任者と面談し、認証および権限付与に関連する文書と ID 管理シス テムの構成を確認し、ユーザー ID が識別され認証されていること、適切なパスワード複雑 性ポリシーが設定されていることをチェックし、その有効性を検証するためにテストを行う；

2）災害復旧技術及び実施チームの技術スタッフにインタビューし、本人確認及び権限に関する文書、操作リスト文書などを確認し、災害復旧システムにおける重要な業務操作、重要

なユーザー操作、または異常なユーザー操作行動が明確化されているか、また、リストが形成されているかを確認する；

3）災害復旧技術および実施チームの技術担当者に聞き取り調査を行い、認証および権限 関連文書と ID 管理システムの構成を確認し、災害復旧システム設備、ユーザー、サービ スまたはアプリケーション、およびデータに対してセキュリティ管理が実施されて いるか、重要な業務操作、重要なユーザー操作、または異常なユーザー操作行動に対して動的 ID 認証が採用されているか、多要素 ID 認証が採用されているかなどを確認する；

4）災害復旧技術・実施チームの技術スタッフにインタビューし、認証・権限付与に関連する文書や設定を確認し、ログへのアクセス、ポリシー管理、バックアップデータなど、災害復旧システムにおけるすべてのセキュリティ関連操作についてアクセス制御ポリシーが設定されているかどうかをチェックし、操作権限が事前に定義された範囲を超えていないかどうか、最小権限の原則が満たされているかどうかをチェックする。

(b) 期待される結果

1）災害復旧システムは、効果的なユーザー識別および認証メカニズムを実装しており、パスワードの複雑性ポリシーは合理的に設定され、実施されている；

2）災害復旧システムの重要な業務操作、重要なユーザー操作、または異常なユーザー操作の動作を明確に定義し、リストを作成する；

3）災害復旧システム機器、ユーザー、サービス、アプリケーション、データには厳重なセキュリ ティ管理が実施され、重要な業務には動的 ID 認証または多要素認証が使用される；

4）アクセス制御ポリシーは、災害復旧システムにおけるすべてのセキュリティ関連操作に対して設定され、リソースにアクセスされるものは、操作権限が事前に定義された範囲を超えず、最小特権の原則が満たされる。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.5.6.2 侵入防止

災害復旧システムの安全なコンピューティング環境の侵入防止テストの評価には、以下のようなものがある。

a) 評価方法

1）災害復旧技術・実施チームの技術スタッフに、持続可能な高度な脅威やその他のサイバー攻撃をどのように監視、特定、対応しているか、また関連するツールや技術の選択と導入

についてインタビューする。高度で持続可能な脅威やその他のサイバー攻撃に対する侵入防止能力を向上させるために、侵入検知システム、侵入防止システム、脅威インテリジェンス防御システム、その他の技術的手段が使用されているかどうかを確認する；

2）災害復旧技術・実施チームの技術スタッフにインタビューし、災害復旧システ ムのセキュリティ強化策の選択、設定、管理のプロセスを理解する。災害復旧システムのセキュリティを強化するために、バックグラウンド暗号化や動的パスワードなどのセキュリティ対策が使用されているかどうかを確認する。

(b) 期待される結果

1）災害復旧システムは、高度で持続可能な脅威などのサイバー攻撃に対する侵入防止を向上させるために、効果的な技術的手段を採用している；

2）災害復旧システムのセキュリティは、バックグラウンドでの暗号化や動的パスワードなどのセキュリティ対策の導入により強化されている。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.5.6.3 自動化ツール

災害復旧システムの安全なコンピューティング環境のための自動化ツールテストの評価には、以下のようなものがある。

a) 評価方法

1）災害復旧技術・実施グループの技術スタッフに、自動化ツールの選択、配備、使用 について、また、自動化ツールを使用して管理効率とセキュリティをどのように向 上させることができるかについて、インタビューを実施する。アカウントの作成、変更、無効化、削除のプロセスが自動化されているかどうかなど、システムアカウントと構成を管理するために自動化ツールが導入されているかどうかを確認する；

2）災害復旧技術・実施チームの技術スタッフに、脆弱性管理およびパッチ適用に自動化ツールを使用しているかどうか（適用前にパッチが適切に検証されていることを確認する方法を含む）を聴取する。脆弱性の自動識別とアセスメント、パッチの自動展開など、脆弱性スキャンとパッチ管理に自動化ツールが使用されているかどうかを確認する；

3）災害復旧技術・実施チーム（DRT&IT）の技術スタッフにインタビューを行い、ウイルスデータベースの自動更新の実施について質問し、更新メカニズムの選択、監視、メンテナンス戦略を理解し、ウイルス保護ソフトウェアやその他のセキュリティツールが、最新の

脅威に対する効果的な保護を確保するために、ウイルスデータベースの自動更新メカニズムが設定されているかどうかを確認する。

(b) 期待される結果

1）システムアカウントと設定の効率的な管理は、自動化されたツールによって達成され、人的ミスを減らし、システムのセキュリティと安定性を向上させる；

2）自動化ツールは、脆弱性のタイムリーな特定とアセスメント、パッチの自動ダウンロードと適用をサポートし、システムが既知の脆弱性に対して最新の状態に保たれることを保証する；

3）ウイルス対策ソフトやセキュリティ・ツールは、ウイルス・データベースの自動更新メカニズムが設定されているため、新しいセキュリティの脅威にタイムリーに対応し、システムのセキュリティを守ることができる。

c) 結果の判定：上記の期待される結果をすべて満たしていれば適合と判定し、そうでなければ不適合または部分適合と判定する。

10.5.7 セキュリティ施工管理

災害復旧システムの安全ビル管理試験評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧管理チームおよび災害復旧技術・実施チームの管理者にインタビューを行い、セキュリティ構築に関する文書を確認し、災害復旧システムの構築、改修、アップグレードの際に、セキュリティ対策が計画、構築、使用において同期化されているかどうかを確認する；

2）災害復旧技術・実施チームにおいてテスト及びレビューを担当する技術要員に面談し、セキュリ ティテスト（侵入テスト、脆弱性スキャンなど）及びセキュリティレビュー（コードレビュー、アーキテク チャレビューなど）の実施状況及び結果を含むテスト及びレビュー記録をレビューし、テスト及びレ ビューを用いてセキュリティ構築プロセスが検証されているかどうかを確認する；

3）災害復旧管理チーム、災害復旧技術・実行チーム、災害復旧保証チームなどにおいて、攻撃・防御訓練に携わる担当者にヒアリングを行い、攻撃・防御訓練のシナリオ、参加者、発見されたセキュリティ上の問題点、その後の是正措置などの計画、実施記録、改善措置の記録を確認し、攻撃・防御訓練によってセキュリティの検証が行われているかを確認する。

(b) 期待される結果

1）災害復旧システムの構築、転換、アップグレードにおいて、災害復旧システムの安全対策の計画、構築、使用を同期させる必要がある；

2）災害復旧システムのセキュリティは、セキュリティテストとレビューの実施によって検証され、セキュリティ上の問題は効果的に特定され、解決された；

3）災害復旧システムの安全性は、攻撃と防御の演習を通じて検証された。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.5.8 セキュリティ運用・保守管理

災害復旧システムのセキュリティ運用・保守管理テストの評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧管理チームの運用・保守管理責任者からヒアリングを行い、運用・保守場所の選定根拠、海外運用・保守のコンプライアンス対策、関連法規の遵守状況を把握し、災害復旧システムの運用・保守場所の関連記録や契約書を確認し、運用・保守活動がすべてまたは主に中国国内で行われているかどうかをチェックする。海外での運用・保守が含まれる場合は、当該活動が中国の関連法規を遵守しているかを確認する必要がある；

2）災害復旧保証チームの人事部または災害復旧管理チームの運用・保守担当マネジャーにヒアリングを行い、セキュリティ・機密保持契約の締結プロセス、その内容、履行を監視する仕組みを把握する。保守要員と締結したセキュリティ秘密保持契約の文書を確認し、保守要員全員が運用保守前にセキュリティ秘密保持契約に署名しているかどうかを確認する；

3）災害復旧技術・実施グループの運用・保守チームにヒアリングを行い、運用・保守ツールの選定標準、申請プロセス、未申請ツールのテスト・承認プロセスを把握し、運用・保守ツールの登録・申請記録を確認し、申請された運用・保守ツールを優先的に使用しているかを確認する。未登録ツールの使用については、使用前に悪質コード検出などのテストに合格しているかを確認する。

(b) 期待される結果

1）災害復旧システムの運用・保守活動は、主に中国国内において、関連する国内法令を遵守して実施されるようにする。必要な海外での運用・保守活動については、明確なコンプライアンス文書と管理措置を設ける；

2）すべての保守要員は、運用と保守の前に、セキュリティと機密保持に関する同意書に署名する；

3）ツールの安全性と適用性を確保するため、組織に登録・申請された O&M ツールの使用が優先される。登録されていないツールについては、使用前に悪意のあるコードが含まれていないことを確認し、運転・保守プロセスのセキュリティを保護するために、厳格なテストプロセスが使用される。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部不適合」と判定される。

10.5.9 サプライチェーンの安全保障

災害復旧システムのサプライチェーン・セキュリティ・テスト評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧リーダーチームの責任者及び災害復旧支援チームのサプライチェーンマネジメントのロジスティクス支援担当者にインタビューを行い、サプライチェーンセキュリティマネジメント戦略、サプライチェーンセキュリティマネジメントシステム及びその他の文書を確認し、サプライチェーンセキュリティマネジメント戦略が策定されているかどうか、マネジメント戦略にリスクマネジメント、サプライヤーの選定・管理、製品開発・調達、セキュリティ・メンテナンスが含まれているかどうか、サプライチェーンセキュリティマネジメントシステムが策定されているかどうかを確認する。書類

2）災害復旧セキュリティチームのサプライチェーン管理を担当するロジスティクス担当者にインタビューを行い、災害復旧製品とサービスが関連する国家標準の要求事項に適合しているかどうかを裏付ける資料をチェックし、調達した災害復旧製品とサービスが関連する国家標準の要求事項を満たしているかどうかをチェックする。国家安全保障に影響を及ぼす可能性のある製品やサービスについては、審査記録を確認し、国家サイバーセキュリティ審査に合格しているかどうかをチェックする；

3）災害復旧保証チームのサプライチェーン管理責任者である調達・サプライチェーンマネージャーにインタビューを行い、適格サプライヤーのカタログとその設定・維持の記録を確認し、適格サプライヤーのカタログが設定・維持され、保証されたサプライヤーが選定されていることを確認する；

4）災害復旧保証チームまたは災害復旧管理チームのサプライチェーンマネージャーにインタビューを行い、調達チャネルの選択、管理、リスク管理方法を理解し、調達チャネル管理戦略を見

直し、調達チャネル管理が強化されているか、災害復旧製品・サービスの調達先が安定しているか、多様化されているかを確認する；

5）災害復旧保証チームまたは災害復旧管理チームの責任者である法務部 門と契約管理者に、セキュリティ及び機密保持に関する契約書の作成、交 渉及び実施の監督、ベンダーとの調達契約書のレビュー、プロバイダーのセキュリ ティ責任及び義務に関する明確性の確認等のプロセスについてインタビューを実施 する；

6）災害復旧セキュリティチームまたは災害復旧管理チームの担当者にインタビューを行い、災害復旧製品およびサービスの提供者とセキュリティおよび機密保持契約を締結しているかどうかを確認し、機密保持契約をチェックし、その内容にセキュリティ責任、機密保持の内容、報償および処罰の仕組み、有効期間が含まれているかどうかをチェックする；

7）災害復旧保証チームまたは災害復旧管理チームの担当調達部門と面談し、ベンダ ーから提供された知的財産権の使用許諾を裏付ける文書を確認し、関連す る知的財産権が 10 年以上使用許諾されているか、または災害復旧製品・サービ スの耐用期間中継続的に使用許諾されているかを確認する；

8）災害復旧技術・実施チームの関係者やサプライヤーにヒアリングを行い、調達契約書やサプライヤーから提供された技術情報などを確認し、サプライヤーが中国語版の運用・保守や二次開発に関する技術情報を提供しているかどうかを確認する；

9）災害復旧技術・実装チーム及びサプライヤの関連要員から事情を聴取し、調達契約書及び関連するテスト報告書を確認し、自社開発又はカスタマイズのために第三者サービス機関に委託したソフトウェアがソースコードセキュリティテストを受けているか、又はサプライヤが第三者機関発行のコードセキュリティテスト報告書を提供しているかを確認する；

10）　災害復旧技術及び実施チームの関係者にインタビューを行い、セキュリテ ィの欠陥及び脆弱性の特定、評価、対処のプロセスを理解し、セキュリテ ィの欠陥及び脆弱性が発見された場合の対応記録をチェックし、使用し ている災害復旧製品及びサービスにセキュリティの欠陥、脆弱性及びその他のリ スクがある場合、リスク及び危険を排除するために適時に対策が講じられて いるか、重大なリスクを含むものが規定に従って関連部門に報告されている か をチェックする。

b)　期待される結果

1）組織が、リスク管理、サプライヤ選定、製品開発・調達、セキュリテ ィ保守を包含する包括的なサプライチェーンセキュリティマネジメ ント戦略を確立している。具体的に期待されることとしては、リスク評価方法、サプライヤ評価標準、調達プロセスのセキュリティ要件、セキュリティ維持策を明記した戦略の策定と定期的な更新の

プロセスを文書化することである。サプライチェーンセキュリティ管理システムを開発し、サプライチェーンセ キュリティ管理のための資金、人員、許可などの利用可能な資源を提供する；

2）調達したすべての災害復旧製品およびサービスは、関連する国の標準およびセキュリティ要件に準拠しており、特に国の安全保障に関わるものは、国のサイバーセキュリティ審査に合格している；

3）厳格なアセスメントを受け、セキュリティ要件を満たした認定サプライヤーのカタログを確立し、維持することに成功した；

4）調達チャネルの安定性と多様性が確保され、供給元が単一になるリスクが効果的に軽減される；

5）災害復旧製品とサービスの調達は、プロバイダーのセキュリティ責任と義務を明確にする；

6）ベンダーのセキュリティ責任と義務は、すべてのベンダーとのセキュリティ機密保持契約において明確に定義されている。これには、災害復旧製品およびサービスのセキュリティ管理に関する要件、ユーザーデータへの不正アクセスやユーザーシステム機器の管理・操作の禁止などが含まれる；

7）サプライヤーは、提供する製品やサービスに関わるすべての知的財産権について、10年以上またはその使用期間中のライセンスを持つことが求められる。具体的に期待されることは、認可の文書化、認可の存続期間の記録、定期的な認可の検証報告などである；

8）災害復旧製品やサービスのプロバイダーは、運用と保守、二次開発やその他の技術情報の中国語版を提供する；

9）カスタム開発ソフトウェアのソースコードセキュリティテストを実施し、セキュリティテストレポートを作成する；

10）使用している製品やサービスにセキュリティ上の欠陥や脆弱性が発見された場合、組織は適時に修復策を講じることができ、重大なリスクを伴う場合には、規則に従って関係当局に報告することができる。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.5.10 データ・セキュリティ

災害復旧システムのデータ・セキュリティ・テスト評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧技術・実施チームの技術スタッフにインタビューし、バックアップ・復旧プロセスで実施されているデータ完全性の検証方法とその有効性を理解し、バックアップ・復旧業務の文書と関連業務の監査ログを確認し、バックアップ・復旧プロセスにおける災害復旧システムのデータ完全性が検証され、その有効性が検証されているかを確認する；

2）災害復旧技術・実施チームの技術スタッフにインタビューを行い、アンチウイルスソフトの導入戦略や設定を確認し、アンチウイルスソフトのスキャンがサポートされているか、ファイルがウイルスに感染するのを防ぐことができるかどうかを確認する；

3）災害復旧技術・実施チームの技術スタッフにヒアリングを行い、データ漏洩防止関連製品の構成を確認し、データ漏洩防止機能が採用されているか、データ保存に暗号化ストレージや暗号アルゴリズムが使用されているか、データへの不正アクセスやデータ漏洩を防止できるかを検証する；

4）災害復旧保証チームの人員にインタビューし、データ削除、破壊、記憶媒体の再利用の実施内容と監督措置を理解し、設備の廃止と放棄のプロセスをチェックし、災害復旧システム設備の廃止と放棄の際、データセキュリティ保護戦略に従って、データ削除、破壊、記憶媒体の再利用の対応要求が提示されているかどうかをチェックする。

(b) 期待される結果

1）すべてのバックアップとリカバリ作業はデータの完全性が検証され、監査ログはすべてのバックアップとリカバリ作業が確立されたデータ完全性検証プロセスに従っていることを示した；

2）アンチウィルス・ソフトウェアは、災害復旧システムのすべての重要なコンポーネントを包括的にカバーし、定期的なアップデートとスキャンを行い、ウィルス感染は報告されていない；

3）データ漏洩防止機能をサポートし、データへの不正アクセスや漏洩を防ぐことができる；

4）引退し、古くなったデータ記憶媒体は、データ・セキュリティ保護戦略に従って安全に削除・破棄され、未処理の機密データは残らない。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」、そうでない場合は「不適合」または「一部適合」と判断される。

10.6 災害復旧システム運用管理試験評価方法

10.6.1 災害復旧計画の策定と管理

10.6.1.1 計画策定の原則

災害復旧計画の策定と管理試験評価には、以下のものが含まれる。

a) 評価方法

災害復旧リーダーチームの人員にインタビューを行い、災害復旧要件および災害復旧技術計画との関連で災害復旧計画を見直し、適切な災害復旧およびその他の分類に従って設計されているか、想定される災害シナリオが含まれているか、緊急時に使用するのに適したわかりやすい内容になっているか、リソース、手順、責任者などが明記されているか、適時に更新されているか、他の計画との互換性はあるかなどを確認する。他の計画との互換性

b) 期待される成果

災害復旧計画は、対応する災害復旧カテゴリーに従って設計され、さまざまな災害シナリオに対応するように設計・策定され、理解しやすく、緊急事態での使用に適しており、資源、手順、責任者、適時更新、更新記録が明確であり、災害復旧に関連する他の計画との互換性が明確である。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は適合と判定され、そうでない場合は不適合または部分適合と判定される。

10.6.1.2 計画策定プロセス

災害復旧計画策定プロセステスト評価には、以下のものが含まれる。

a) 評価方法

災害復旧計画の策定過程の記録を確認し、起案、レビュー、テスト、完璧化、レビュー承認、ファイリングなどの過程を含むかどうかをチェックし、対応する過程の記録、署名、レビュー意見書などの文書が完備しているかどうかをチェックする。

b) 期待される結果

1) 計画策定のプロセスは完了し、起草、見直し、テスト、洗練、審査・承認、提出が含まれる；

2) 計画策定プロセスには、プロセス記録、署名、レビューコメント、報告書などの完全な文書化がある。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は適合と判定され、そうでない場合は不適合または部分適合と判定される。

10.6.1.3 計画の内容

災害復旧計画の内容テスト評価には、以下のものが含まれる。

a) 評価方法

災害復旧技術および実施チームの担当者へのインタビュー、災害復旧ニーズおよび災害復旧技術プログラムとの関連における災害復旧計画の見直し、計画の内容が包括的であり、災害復旧ニーズおよび災害復旧技術プログラムに沿ったものであることの確認。

b) 期待される結果

計画実施目的、計画実施に必要な資源、計画実施チームの構成と役割分担、計画の重要度、計画発動の発動条件、計画に関連する業務・資産の一覧、計画の切り替えに必要な資産の依存関係、関連付けと切り替えのプロセス、計画に関連する部署、通知のプロセス、通知の内容、訓練中のデータセキュリティ保護対策、計画、訓練終了後のデータセキュリティ保護対策、訓練失敗時のフォールバックプロセス、技術的解決策と運用マニュアルなど、災害復旧計画の内容が揃っている。リハーサル中のデータセキュリティ保護対策、リハーサル終了後のデータセキュリティ保護対策、リハーサル失敗時のフォールバック処理、計画書の技術的解決策と運用マニュアルなど、災害復旧の要件と災害復旧の技術計画に沿った内容になっている。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」と判定し、そうでない場合は「不適合」または「一部適合」と判定する。

10.6.1.4 計画前研修

災害復旧準備訓練試験評価には、以下の内容が含まれる。

a) 評価方法

1）災害復旧技術・実施チームのメンバーにインタビューを行い、事前計画訓練に関する資料やプロセス記録を確認し、訓練・教育の時期、頻度、範囲、カリキュラム、訓練記録が訓練ニーズに合致しているかをチェックする；

2）計画実施チームのメンバーの評価記録を確認し、関係者に質問して、計画の内容を把握しているか等を確認する。

(b) 期待される結果

1）災害復旧計画の早い段階で、災害復旧の概念に関する認識と教育の取り組みを始める；

2）研修の頻度や範囲、コース内容などが研修ニーズに合っており、研修記録がある；

3）プラン実施チームは、評価の記録を持ち、プランの内容とプロセスについて精通している。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」と判定し、そうでない場合は「不適合」または「一部適合」と判定する。

10.6.1.5 計画の変更

災害復旧計画変更テスト評価には以下のものが含まれる。

a) 評価方法

1）計画変更プロセスの記録を確認し、事業、情報システム、人員などに変更があった場合に、災害復旧計画が適時に変更されているかどうかをチェックする；

2）計画変更プロセスの記録を見直し、計画のテスト、リハーサル、災害後の実施の有効性がアセスメントされているか、適時に計画が変更されているかをチェックする；

3）計画の変更過程の記録を確認し、計画が定期的に見直し・改訂されているか、見直し・改訂の頻度等が要件を満たしているかをチェックする。

(b) 期待される結果

1）業務変更、情報システムの変更、人事異動などは、災害復旧計画の中で適時行われる；

2）計画のテスト、リハーサル、災害後の実施の有効性がアセスメントされ、計画が改訂された；

3）災害復旧計画は定期的に見直され、改訂される。

a) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」と判定し、そうでない場合は「不適合」または「一部適合」と判定する。

10.6.1.6 計画の保存と普及

災害復旧準備計画の保持と配布テスト評価には、以下のものが含まれる。

a) 評価方法

1）災害復旧技術・実施チーム（DRTIT）の要員と災害復旧保証チーム（DRAT）の要員にインタビューを行い、プレプランの保存と配布の責任者が指定されていることを確認する；

2）計画の保存と配布の記録を見て、複数のコピーが保存され、異なる場所に保管されていることをチェックし、関係者に配布されていることをチェックし、明確なバージョン管理がなされていることをチェックし、古いバージョンの計画は破棄されていることをチェックする。

(b) 期待される結果

1）あらかじめ用意されたプランを、分配記録とともに保管する者が任命されている；

2）プランの保存と配布に関する完全な記録。複数の保存用コピーがあり、異なる場所に保管され、関係者に配布され、明確なバージョン管理が行われ、プランの旧バージョンの破棄記録がある。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」と判定し、そうでない場合は「不適合」または「一部適合」と判定する。

10.6.2 災害復旧システムの運用と保守

10.6.2.1 運転と保守の原則

災害復旧システム運用保守原則試験評価には、以下の内容が含まれる。

a) 評価方法

災害復旧技術・実施チームと災害復旧セキュリティチームの人員にインタビューし、災害復旧システムの運用・保守システムをチェックし、災害復旧システムのセキュリティ管理レベルと要求が生産システムと一致しているか、あるいは一段階低いかをチェックし、災害復旧システムの運用・保守システムと生産システムの運用・保守システムがリンクしているかどうかをチェックし、災害復旧システムの運用・保守管理が制度化されているかどうかをチェックする、災害復旧システムの運用・保守管理が制度化され、プロセス指向であり、運用・保守管理の品質と効率を向上させることができるかどうかをチェックし、災害復旧システムの運用・保守管理が総合的なテストと定期的な検証メカニズムを通じて災害復旧資源の可用性と有効性を確保できるかどうかをチェックする。

b) 期待される結果

災害復旧システムのセキュリティ管理レベルと要求が本番システムのセキュリティ管理レベルと一致するか、本番システムより一段階低い。災害復旧システムの運用・保守システムが本番システムの運用・保守システムと連動している。災害復旧システムの運用・保守管理が体系化され、処理されており、運用・保守管理の質と効率が向上している。災害復旧システムの運用・保守管理が総合テストと定期的な検証メカニズムに合格しており、災害復旧資源

の可用性と有効性が確保されている。災害復旧システムの運用とメンテナンス管理は、総合テストと定期的な検証メカニズムに合格し、災害復旧資源の可用性と有効性を確保した。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は適合と判定され、そうでない場合は不適合または部分適合と判定される。

10.6.2.2 オペレーション・モニタリング

災害復旧システムの運用監視とテストの評価には、以下のものが含まれる。

a) 評価方法

監視プラットフォームと運用監視記録を確認し、災害復旧リソースとプロセスをカバーしているか、災害復旧センターの電源環境の可用性、災害復旧リソースの可用性、災害復旧リソースの使用率、災害復旧リソースのセキュリティ、災害復旧タスクの運用状況が含まれているかどうかをチェックする。

b) 期待される結果

運用監視は、災害復旧センターの電源環境の可用性、災害復旧リソースの可用性、災害復旧リソースの使用状況、災害復旧リソースのセキュリティ、災害復旧タスクの運用状況など、災害復旧リソースとプロセスを対象とする。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は適合と判定され、そうでない場合は不適合または部分適合と判定される。

10.6.2.3 システムパトロール

災害復旧システムのウォークスルーテスト評価には、以下のものが含まれる。

a) 評価方法

1) 監視・運用保守プラットフォームと検査プロセスの記録をチェックし、災害復旧システムの定期検査が実施されているかどうかを確認し、検査結果の診断分析を行い、検査が包括的であるかどうかをチェックする；

2) 検査プロセスログを確認し、検査の頻度が災害復旧カテゴリーおよびレベルの要件と一致していることを確認する；

3) 検査報告書を閲覧し、検査時間、検査対象、検査ステップ、検査スクリプト、検査結果、検査幹部、検査レビュアー、検査結論と勧告などが記載されているかどうかをチェックす

る。検査報告書のテンプレートを閲覧し、定期的に見直され改訂されているかどうかをチェックする。

(b) 期待される結果

1）検査は、災害復旧センターの電源環境の可用性、災害復旧リソースの可用性、災害復旧リソースの使用率の変化、災害復旧リソースの変更記録、災害復旧リソースのエラーログ、災害復旧リソースのセキュリティ、災害復旧タスクの運用状況など、包括的なものである。検査には詳細な記録と検査レポートがあり、過去の検査結果を比較・分析する；

2）検査の頻度は、災害復旧のカテゴリーとレベルに一致している；

3）検査報告書には、検査時間、検査対象、検査ステップ、検査原稿、検査結果、検査幹部、検査レビュアー、検査結論と勧告などが含まれる。検査報告書のテンプレートや、それに対応する定期的なレビューと修正の記録もある。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は適合と判定され、そうでない場合は不適合または部分適合と判定される。

10.6.2.4 災害復旧訓練

災害復旧システム演習テスト評価には、以下の内容が含まれる。

a) 評価方法

1）災害復旧技術・実施チームの人員および災害復旧保証チームの人員にインタビューを行い、適切な災害復旧演習が実施されているかどうか、また演習の種類がビジネスニーズに合致しているかどうかを確認する；

2）演習プロセスの記録を確認し、演習頻度ツアーが災害復旧カテゴリーおよびレベルの要件と一致していることをチェックする；

3）訓練報告書を見直し、訓練目的、訓練計画、訓練指揮チーム、訓練実行チーム、訓練時間枠、訓練手順、訓練記録、訓練結果、訓練概要、および推奨事項が記載されているかどうかを確認する；

4）演習報告書のテンプレートを見直し、定期的に見直し、改訂していることを確認する；

5）訓練資料や記録を確認し、災害復旧運用・維持管理の初期段階における訓練コンセプトの周知・教育の実施状況、災害復旧訓練前の訓練目的・訓練計画等の目標訓練の実施状況、災害復旧訓練のステップの習得状況の確認、災害復旧訓練教育・訓練後の事後評価の実施状況を確認し、訓練実施関係者が訓練目的・訓練計画・災害復旧訓練のステップを十分に

理解していることを確認する、訓練実施関係者が訓練目的、訓練計画、訓練ステップを理解しているか、訓練サインシート、試験記録等の文書があるか確認する。

(b) 期待される結果

1）対応する災害復旧演習が実施され、演習の種類はビジネスニーズに合致していた；

2）演習頻度ツアーは、災害復旧カテゴリーとレベルの要件に合致している；

3）訓練報告書には、訓練の目的、訓練計画、訓練指揮チーム、訓練実行チーム、訓練時間枠、訓練手順、訓練記録、訓練結果、訓練概要、および勧告が含まれる；

4）演習報告のテンプレートは定期的に見直され、改訂された；

5）災害復旧運用保守の初期段階において、演習の概念に関する広報・教育を企画・実施し、災害復旧演習の前に、演習の目的、演習計画等に関する目標訓練を実施し、災害復旧演習の手順を習得し、災害復旧演習教育・訓練後に、演習実施関係者が演習の目的、演習計画、演習の手順を理解・把握したことを確認するための事後評価を実施し、訓練署名用紙、試験記録等を作成した。文書化する。

c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」と判定し、そうでない場合は「不適合」または「一部適合」と判定する。

10.6.3 緊急対応と災害引き継ぎ

10.6.3.1 緊急時対応

緊急事態対応テストの評価には、以下のものが含まれる。

a) 評価方法

緊急事態対応に関する資料を確認し、緊急事態対応が、業務システムやデータセキュリティの保護、状況の悪化の抑制、損失の低減を最大化するために必要な管理措置を講じているかを確認し、災害シナリオに合わせて対応する災害復旧計画が選定されているかを確認し、災害復旧計画の発動状況を確認し、災害復旧計画に従って緊急事態切替が実施されているかを確認し、緊急事態切替後に業務やシステムの可用性を検証し、業務やシステムの可用性の検証結果に基づいて緊急事態対応状態の終了または継続を決定しているかを確認し、緊急事態対応に関する完全なプロセス記録文書があるかを確認する。緊急災害切替後にシステムの稼働状況を検証し、業務・システムの稼働状況の検証結果に基づいて緊急対応状態の終了・継続を決定しているか、緊急事態発生時のプロセス記録文書が完備しているかを確認する。

b) 期待される結果

緊急事態の対応では、業務システムとデータセキュリティを最大限に保護し、状況の悪化を抑制し、損失を削減するために必要な管理措置を講じ、災害シナリオと組み合わせて、対応する災害復旧計画を選択し、災害復旧計画の開始を確認し、災害復旧計画に従って、緊急災害の切り替えを実施し、緊急災害の切り替えは、業務とシステムの可用性を検証し、業務とシステムの可用性に応じて、検証結果を実施した。緊急対応状況の終了または継続を決定し、緊急イベントの完全なプロセス記録文書を持っている。

c) 結果判定：

上記の期待される結果をすべて満たしている場合は適合と判定され、そうでない場合は不適合または部分適合と判定される。

10.6.3.2 災害復旧インシデント報告

災害復旧インシデント報告テスト評価には以下が含まれる。

a) 評価方法

1）災害復旧インシデントレポートを確認し、災害の種類、災害の原因、ビジネスインパクトの範囲、ビジネスインパクトの期間、データ損失の期間、災害復旧計画、是正コメントが含まれているかどうかをチェックする；

2）災害復旧インシデント・レポートのテンプレートを見直し、定期的な見直し、改訂、対応する記録があるかどうかを確認する。

(b) 期待される結果

1）災害復旧インシデントレポートには、災害の種類、災害の原因、ビジネスへの影響の範囲、ビジネスへの影響の長さ、データ損失の長さ、災害復旧計画、是正措置が含まれる；

2）災害復旧インシデント・レポートのテンプレートは、定期的なレビュー、修正、対応とともに文書化される。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は適合と判定され、そうでない場合は不適合または部分適合と判定される。

10.6.4 リビルドとフォールバック

リビルドとロールバックのテスト評価には以下のものが含まれる。

a) 評価方法

1）災害復旧技術・実施チームの職員および災害復旧保証チームの職員にインタビューを行い、災害復旧が完了した後、最初に災害後の再建・ロールバックプログラムが実施されているかどうかを確認する；

2）再建と巻き返しのプログラムを見て、それらが包括的であることを確認する。

(b) 期待される結果

1）災害後の復旧とロールバック・プログラムは、災害復旧が完了した後、最初に策定された；

2）再構築とフォールバックの計画は完了しており、計画には、プロダクション・センターの障害の修復または再構築、災害復旧センターからプロダクション・センターへのデータ同期の実施、災害復旧センターからプロダクション・センターへのデータ同期の実施、災害復旧センターからプロダクション・センターへのカットバック後のビジネス可用性の検証、災害復旧センターからプロダクション・センターへのカットバックで障害が発生した場合の対策の策定などの要素が含まれている。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は「適合」と判定し、そうでない場合は「不適合」または「一部適合」と判定する。

10.6.5 災害復旧監査

災害復旧監査テストの評価には、以下のものが含まれる。

a) 評価方法

1）監査報告書およびその他の関連資料を検討し、内部監査人または第三者監査人による監査が定期的に実施され、発行されているかどうか、および監査が包括的であるかどうかをチェックする；

2）監査報告書で指摘された改善点および改善プログラムを確認し、改善点が適時に対応されたかどうか、またその対応状況を確認するため、災害復旧技術・実施チームの担当者にインタビューを行う。

(b) 期待される結果

1）内部監査員や第三者監査員による監査が定期的に実施され、災害復旧計画の保管・配布記録、災害復旧計画訓練記録、災害復旧計画報告記録、災害復旧訓練記録、災害復旧訓練報告書ファイリング記録、災害復旧システム点検報告書ファイリング記録などが含まれる；

2）監査報告書で提案された改善策へのタイムリーな対応。

(c) 結果の判定

上記の期待される結果をすべて満たしている場合は適合と判定され、そうでない場合は不適合または部分適合と判定される。

附属書 A（規範） 災害復旧能力の分類

A.1 レベル 1 ベーシック・サポート

レベル 1 の災害復旧能力は、表 A.1 に示すように、技術的および管理的な支援を受けるべきである。

表 A.1 レベル 1 - 基本的サポート

主体	基準
データバックアップ災害復旧システム	a) データの完全バックアップを少なくとも毎週行い、少なくとも 1 ヶ月分の冗長データを保持する； b) バックアップストレージはオフサイトまたはローカルに保存する。オフサイトまたはローカルのバックアップには、専用のバックアップストレージを使用する； c)プロダクション・センターと災害復旧・センターは、1 日レベルの RPO を達成するために、重要なシステムのデータを周期的に同期させる； d) 本番センターで災害が発生した場合、災害復旧センターは 72 時間以内にアプリケーションを引き上げ、業務を引き継ぐことができる。 注：データバックアップシステムを利用することで、ある程度の災害復旧対策は可能である。
代替データ処理システム	-
バックアップネットワークシステム	-
代替インフラ	メディア保管の条件を満たすサイトがある。
専門的な技術サポート能力	-
運転・保守管理能力	a) メディアへのアクセス、検証、ダンプ管理システムがある； b) メディア特性によるバックアップデータの定期的な有効性検証。
災害復旧計画	十分にテストされ、リハーサルされた適切な災害復旧計画を実施する。
注："-"は要求がないことを示す。	

A.2 レベル 2 の代替地サポート

レベル 2 の災害復旧能力は、表 A.2 に示すように、技術的および管理的な支援を受けるべきである。

表 A.2 レベル 2 - 代替地サポート

主体	基準
データバックアップ 災害復旧システム	a) データの完全バックアップを少なくとも毎週行い、少なくとも 1 ヶ月分の冗長データを保持する； b) バックアップストレージはオフサイトまたはローカルに保存され、オフサイトバックアップまたはローカルバックアップは専用のバックアップストレージを使用する； c)プロダクション・センターと災害復旧・センターは、1 日レベルの RPO を達成するために、重要なシステムのデータを周期的に同期させる； d) 本番センターで災害が発生した場合、災害復旧センターは 48 時間以内にアプリケーションを引き上げ、業務を引き継ぐことができる。 注：データバックアップシステムを利用することで、ある程度の災害復旧対策は可能である。
代替データ処理システム	a) 災害復旧に必要なデータ処理装置の一部を備えているか、または災害発生後、所定の期間内に必要なデータ処理装置を代替サイトに配備できること； b) バックアップデータ処理システムは、本番システムから独立して稼動する。
バックアップネットワークシステム	通信回線とそれに対応するネットワーク機器を部分的に備えているか、災害発生後、所定の期間内に必要な通信回線とネットワーク機器を代替サイトに再配置することができる。
代替インフラ	a) メディア保管の条件を満たすサイト b) 情報システムおよび重要な業務機能の運用再開の条件を満たすサイト。
専門的な技術サポート能力	災害復旧センターには、専任のコンピュータールーム運営マネージャーがいる。
運転・保守管理能力	a) メディアへのアクセス、検証、ダンプ管理システムがある； b) メディア特性によるバックアップデータの定期的な有効性検証； c) 代替サイト管理システムがある； d) 関連ベンダーと、災害復旧時間の要件を満たす緊急供給契約を結ぶ； e) 関連する通信事業者と、災害復旧時間要件を満たす代替通信回線契約を結ぶ。
災害復旧計画	完全にテストされ、リハーサルされた災害復旧計画がある。

主体	基準
注："-"は要求がないことを示す。	

A.3 レベル 3 電子伝送と部分的な機器サポート

レベル 3 の災害復旧能力は、表 A.3 に示すように、技術的および管理的な支援を受けるべきである。

表 A.3 レベル 3 - 電子伝送と部分的な機器サポート

主体	基準
データバックアップ災害復旧システム	a) 少なくとも 1 日 1 回、データの完全バックアップを行い、少なくとも 1 ヶ月分の冗長データを保持する； b) バックアップストレージはオフサイトまたはローカルに保存され、オフサイトバックアップまたはローカルバックアップは専用のバックアップストレージを使用する； c) 1 時間ごとから 1 日ごとの RPO を達成するために、重要なシステムのデータを周期的に同期させるプロダクションセンターと災害復旧センター； d) コピーデータは、データの整合性を保護するために、バックアップデータの暗号化を保護し、不正に改ざんされないように、変更および漏洩防止機構をすることはできない； f) 本番センターで災害が発生した場合、災害復旧センターは 24 時間以内にアプリケーションを引き上げ、業務を引き継ぐことができる。 注：データバックアップシステムを利用することで、ある程度の災害復旧対策は可能である。
代替データ処理システム	a) 災害復旧に必要なデータ処理装置の一部を備えている。 b) バックアップデータ処理システムは、本番システムから独立して稼動している。
バックアップネットワークシステム	いくつかの通信回線と対応するネットワーク機器を備えている。
代替インフラ	a) メディア保管の条件を満たすサイト b) 情報システムおよび重要な業務機能の運用再開の条件を満たすサイト。
専門的な技術サポート能力	災害復旧センターには、専任のコンピュータールーム運営マネージャーがいる。
災害復旧計画	完全にテストされ、リハーサルされた災害復旧計画がある。
注："-"は要求がないことを示す。	

A.4 レベル 4 電子伝送と機器一式のサポート

レベル 4 の災害復旧能力は、表 A.4 に示すように、技術的および管理的な支援を受けるべきである。

表 A.4 レベル 4 - 電子伝送と完全な機器サポート

主体	基準
データバックアップ災害復旧システム	a) 少なくとも 1 日 1 回、データのフルバックアップを行い、少なくとも 1 ヶ月分の冗長データを保持する； b) バックアップストレージはオフサイトまたはローカルに保存され、オフサイトバックアップまたはローカルバックアップは専用のバックアップストレージを使用する。 c) 生産センターと災害復旧センターでは、重要なシステムデータを 1 時間ごとの RPO で周期的に同期させる。 d) コピーデータは、データの整合性を保護するために、バックアップデータの暗号化を保護し、不正に改ざんされないように、変更および漏洩防止機構をすることはできない。 e) アンチランサム機能をサポートし、データ保存のための安全な隔離ゾーンを確立し、バックアップデータが不正にアクセスされるのを防ぐ； f) 本番センターで災害が発生した場合、災害復旧センターはアプリケーションを引き上げ、1 時間単位で業務を引き継ぐことができる。
代替データ処理システム	災害復旧に必要なすべてのデータ処理装置を、準備完了または稼働可能な状態にする。
バックアップネットワークシステム	a) 災害復旧に必要な通信回線を備えている。 b) 災害復旧に必要なネットワーク機器を備え、準備万端の状態にある。
代替インフラ	a) メディア保管の条件を満たすサイトを持つ； b) バックアップデータ処理システムおよびバックアップネットワーク機器の運用要件を満たすサイトを持つ； c) 重要なビジネス機能を再開するための運用要件を満たすサイトを持つ； d) 上記敷地は 7x24 時間維持されなければならない。
専門的な技術サポート能力	災害復旧センターで入手できる： a) 7x24 時間のコンピュータルーム専属マネージャー； (b) データ災害復旧システム、データバックアップシステム技術サポートスタッフ； c) 専属のハードウェアおよびネットワーク技術サポートスタッフ。

主体	基準
運転・保守管理能力	a) メディアへのアクセス、検証、ダンプ管理システムがある； b) メディア特性によるバックアップデータの定期的な有効性検証； c) 待機コンピュータ室の運営管理システムがある； d) ハードウェアとネットワークの運用管理システムがある； e) 電子伝送データのバックアップシステムの運用管理システムがある。
災害復旧計画	完全にテストされ、リハーサルされた災害復旧計画がある。
注："-"は要求がないことを示す。	

A.5 レベル 5 リアルタイム・データ伝送と完全な機器サポート

レベル 5 の災害復旧能力は、表 A.5 に示すように、技術的および管理的な支援を受けるべきである。

表 A.5 レベル 5 - リアルタイムデータ転送とフルデバイスサポート

主体	基準
データバックアップ災害復旧システム	a) 少なくとも 1 日 1 回、データのフルバックアップを行い、少なくとも 1 ヶ月分の冗長データを保持する； b) バックアップストレージはオフサイトまたはローカルに保存され、オフサイトバックアップまたはローカルバックアップは専用のバックアップストレージを使用する； c) プロダクション・センターと災害復旧・センターは、重要なシステム・データを周期的に同期させ、1 時間ごとの RPO とデータ損失ゼロを達成する； d) コピーデータは、データの整合性を保護するために、バックアップデータの暗号化を保護し、不正に改ざんされないように、変更および漏洩防止機構をすることはできない； e) アンチランサム機能をサポートし、データ保管のための安全な隔離領域を確立し、バックアップデータが不正にアクセスされるのを防ぐ； f) バックアップセンターは、本番センターと同じデータ形式でのバックアップと、バックアップセンターでの秒単位のリアルタイムデータマウントリカバリーをサポートする； g) データセンター間のネットワークジッターやフラッシュブレークなど、サブヘルシーシナリオ； h) プロダクション・センターで災害が発生した場合、災害復旧・センターはアプリケーションを素早く立ち上げ、分単位から時間単位で業務を引き継ぐことができる。

主体	基準
代替データ処理システム	災害復旧に必要なすべてのデータ処理装置を設置し、準備または稼働可能な状態にする。
バックアップネットワークシステム	a) 災害復旧のための通信回線を備える； b) 災害復旧に必要なネットワーク機器を備え、即応態勢を整えている； c) 通信網の自動切り替え機能または集中切り替え機能を持つ。
代替インフラ	a) メディア保管の条件を満たすサイトを持つ； b) バックアップデータ処理システムおよびバックアップネットワーク機器の運用要件を満たすサイトを持つ； c) 重要なビジネス機能を再開するための運用要件を満たすサイトを持つ； d) 上記敷地は 7x24 時間稼動するよう維持されなければならない。
専門的な技術サポート能力	災害復旧センターは 24 時間体制で専用となっている： a) コンピュータルームの管理者 (b) データ災害復旧システム、データバックアップシステム技術サポートスタッフ； c) ハードウェアとネットワークのテクニカルサポートスタッフ。
運転・保守管理能力	a) メディアへのアクセス、検証、ダンプ管理システムがある； b) メディア特性によるバックアップデータの定期的な有効性検証； c) 待機コンピュータ室の運営管理システムがある； d) ハードウェアとネットワークの運用管理システムがある； e) リアルタイムのデータ災害復旧およびデータバックアップシステムの運用管理システムがある。
災害復旧計画	完全にテストされ、リハーサルされた災害復旧計画がある。
注："-"は要求がないことを示す。	

A.6 レベル 6 ゼロ・データ・ロスおよびリモート・クラスタリング・サポート

レベル 6 の災害復旧能力は、表 A.6 に示すような技術的、管理的な支援を必要とする。

表 A.6 レベル 6 - データ損失ゼロとリモート・クラスタリング・サポート

主体	基準
データバックアップ災害復旧システム	a) 少なくとも 1 日 1 回、データのフルバックアップを行い、少なくとも 1 ヶ月分の冗長データを保持する； b) バックアップストレージはオフサイトまたはローカルに保存され、オフサイトバックアップまたはローカルバックアップは専用のバックアップストレージを使用する； c) プロダクション・センターと災害復旧・センターは、重要なシステム・データを周期的に同期させ、1 時間ごとの RPO とデータ損失ゼロを達成する； d) コピーデータは、データの整合性を保護するために、バックアップデータの暗号化を保護し、不正に改ざんされないように、変更および漏洩防止機構をすることはできない； e) アンチランサム機能をサポートし、データ保管のための安全な隔離領域を確立し、バックアップデータが不正にアクセスされるのを防ぐ； f) バックアップセンターは、本番センターと同じデータ形式でのバックアップと、バックアップセンターでの秒単位のリアルタイムデータマウントリカバリーをサポートする； g) データセンター間のネットワークジッターやフラッシュブレークなど、サブヘルシーシナリオ。 h) プロダクション・センターで災害が発生した場合、災害復旧・センターは迅速にアプリケーションを引き上げ、分単位で業務を引き継ぐことができる。
代替データ処理システム	a) バックアップデータ処理システムは、本番データ処理システムと同じ処理能力を持ち、完全な互換性がある； b) アプリケーションは「クラスタ化」され、リアルタイムでシームレスに切り替えることができる； c) 遠隔地のクラスタシステムのリアルタイム監視と自動切り替え機能。
バックアップネットワークシステム	a) メインシステムと同レベルの通信回線とネットワーク機器を備える； b) バックアップネットワークが稼動している； c) エンドユーザーは、ネットワーク経由でメインセンターとバックアップセンターの両方にアクセスできる。
代替インフラ	a) メディア保管の条件を満たすサイトを持つ； b) バックアップデータ処理システムおよびバックアップネットワーク機器の運用要件を満たすサイトを持つ； c) 重要なビジネス機能を再開するための運用要件を満たすサイトを持つ； d) 上記敷地は 7x24 時間維持されなければならない。

主体	基準
専門的な技術サポート能力	災害復旧センターは 24 時間体制で専用となっている： a) コンピュータルームの管理者 (b) データ災害復旧システムおよびデータ・バックアップ・システムのための専任の技術サポート・スタッフ； c) 専属のハードウェアおよびネットワーク技術サポートスタッフ； d) オペレーティング・システム、データベース、アプリケーション・ソフトウェアの専任テクニカル・サポート・スタッフ。
運転・保守管理能力	a) メディアへのアクセス、検証、ダンプ管理システムがある； b) メディア特性によるバックアップデータの定期的な有効性検証； c) 待機コンピュータ室の運営管理システムがある； d) ハードウェアとネットワークの運用管理システムがある； e) リアルタイムのデータバックアップシステム運用管理システムがある； f) オペレーティングシステム、データベース、アプリケーションソフトウェアの運用管理システムがある。
災害復旧計画	完全にテストされ、リハーサルされた災害復旧計画がある。
注："-"は要求がないことを示す。	

A.7 災害復旧能力の格付けの原則

特定のレベルの災害復旧能力を達成するためには、そのレベルの各要素に対応する要件を同時に満たす必要がある。

A.8 災害復旧センターの分類

災害復旧センターのレベルは、そのセンターがサポートできる災害復旧の最高レベルに等しい。

例：レベル 1 からレベル 5 までサポートできる災害復旧センターはレベル 5 である。

附属書 B（参考） 業界における RTO/RPO と災害復旧能力レベルの関係例

表 B.1 は、情報システム災害復旧の各レベルに対応する RTO/RPO 範囲を示している。

表 B.1 RTO/RPO と災害復旧能力レベルの関係

災害復旧能力レベル	RTO	RPO
1	2 日以上	1 日～7 日
2	24 時間以上	1 日～7 日
3	12 時間以上	時間から 1 日
4	時間から 1 日	時間から 1 日
5	分～時間	0
6	数分	0

附属書 C（参考） ある業界の情報システム要件分類の例

情報システム災害復旧要件の分類例を表 C.1 に示す。

表 C.1 情報システムの災害復旧要件の分類と災害復旧構築の例

ニーズの分類	ニーズ分類の根拠	復職命令	RTO	RPO	災害復旧工事レベル
最初のタイプ	短期的な混乱が国、外部機関、社会に重大な影響を及ぼすシステム；	そもそも	<6 時間	<15 分	≥5 段階以上
	短期的な混乱が、その部門の重要な事業機能に深刻な影響を及ぼし、大きな経済的損失をもたらすようなシステム；				
	ユニットとユーザーが、システムに対する短時間の中断に不寛容なシステム。				
カテゴリー2	短期的な中断が、その部門の重要なビジネス機能の一部に影響を及ぼし、大きな財務的損失をもたらすようなシステム；	次いで	<24 時間以内	<120 分	>3 レベル以上
	短時間のシステム中断に対して、ユニットとユーザーが一定の許容範囲を持っているシステム。				
カテゴリー3	短期的な混乱が、その部門の非重要なビジネス機能に影響を及ぼし、何らかの経済的損失をもたらすようなシステム；	究極	<7 日	<24 時間以内	レベル 2
	一定期間、業務機能の中断が許されるシステム。				

附属書 D (参考) クラウド・コンピューティング技術の災害復旧サービス例

クラウドコンピューティング技術に基づく情報システムの災害復旧サービスの例を表 D.1 に示す。

表 D.1 クラウド・コンピューティング技術の災害復旧サービスの例

サービスの種類	アプリケーションシナリオ	資源要素の要件	RPO	RTO
クラウドデータバックアップサービス	クラウド上にデータ・バックアップ・システムを導入し、本番環境のデータをクラウド上に定期的にバックアップする。	クラウドベースのデータバックアップシステム： -- :: 弾力性のあるデータバックアップサービスの提供 -- その他は 6.3.1.1 項と同様とする。	毎時	該当なし
		ネットワーク要件： -- :: 本番環境とクラウドで利用可能なデータ通信回線		
		セキュリティ要件： クラウドに保存されるデータは、データ漏洩を防ぐために分離される必要がある； -- セクション 6.3.1.1 にあるその他のセキュリティ要件		
コールド災害復旧サービス	クラウド上に展開されたバックアップ業務システムは、災害時にサービスを提供するために起動される。	クラウドベースのデータストレージシステム： -- :: 耐障害性と拡張性に優れたデータ・ストレージ・サービスの提供 -- 6.3.1.1 項のその他の要求事項	微細	毎時
		クラウドバックアップの業務システム要件： クラウド上でも本番環境と同じビジネスシステムの機能とパフォーマンスを提供する。 クラウドバックアップの業務システムは、システムの動作環境やソフトウェアのバージョンなどに完全に対応している必要がある。		
		ネットワーク要件： -- :: 本番環境とクラウド間の一方通行のリアルタイム・データ通信回線が利用できる。 -- 本番環境とクラウドで業務連絡ラインを分ける		

サービスの種類	アプリケーションシナリオ	資源要素の要件	RPO	RTO
		-- 本番環境とクラウド間のビジネスコミュニケーションライン		
		セキュリティ要件： クラウドに保存されるデータは、データ漏洩を防ぐために分離される必要がある； クラウド上の業務システムのバックアップには、業務システムに対する悪意のある改ざんを防ぐ隔離メカニズムが必要だ； -- 6.3.1.1 および各章に定めるその他のセキュリティ要件		
マルチ・アクティブ災害復旧サービス	2 つ以上の業務システムがクラウド上に展開され、同時にサービスを提供する；	クラウドベースのデータストレージシステム： -- :: 耐障害性と拡張性に優れたデータ・ストレージ・サービスの提供 -- 6.3.1.1 項のその他の要求事項	微細	0 分スケール
		クラウドベースのビジネスシステムの要件： クラウド上で複数の機能・性能の業務システムを展開し、同時にサービスを提供する。 -- クラウドにおける業務システムの弾力性 クラウドベースの業務システムは、システムの動作環境、ソフトウェアのバージョンなどの点で完全な互換性がなければならない。		
		ネットワーク要件： 複数のデータストレージシステム間の双方向リアルタイムデータ通信ラインが利用できる。 -- :: オペレーション・システムごとにオペレーショナル・コミュニケーション・ラインを分ける。 -- :: 業務システム間の運用通信経路の有無		

		セキュリティ要件： ラウドに保存されるデータは、データ漏洩を防ぐために分離される必要がある； ラウド上のビジネス・システムには、悪意ある改ざんを防ぐための隔離メカニズムが必要である。 -- セクション 6.3.1.1 にあるその他のセキュリティ要件		

附属書 E（参考） 災害復旧計画の枠組み

E.1 目的と範囲

このセクションは、災害復旧準備計画の目的、用語、方法論（復旧時間目標、復旧ポイント目標、最大許容ダウンタイムを含むが、これらに限定されない）を定義することから始めるべきである。以下を含む、プロフォーマの役割範囲を定義する：

a) 計画の適用範囲：計画が適用される組織、部門、事業単位を示す。

b) 問題解決の範囲：災害や不測の事態が発生した場合に、組織の情報システムの継続性とデータの完全性を確保することである。

c) 未対応の問題の範囲：プレプランでカバーされていない問題と、場合によっては他のプレプランや対応が必要になることを明確に示す。

E.2 組織と責任

このセクションでは、災害復旧組織の構成、各役職の任務、人員のリストについて詳細に記述する。災害復旧組織には、緊急対応チーム、災害復旧チームなどが含まれるが、これらに限定されるものではなく、その任務と責任は明確に定義されるべきである。

E.3 リエゾンとコミュニケーション

災害復旧に関わる人々や組織をリストアップした連絡先シート。災害復旧チーム、オペレーター、ベンダー、当局、メディア、従業員などを含む。連絡先には、固定電話、携帯電話、トランシーバー、電子メール、住居住所、緊急連絡先アプリケーションを含める。

災害復旧チーム、オペレーター、ベンダー、当局、メディア、従業員など、災害復旧に関連する人々や組織の連絡先を記入すること。電話番号、E メール、住所、緊急連絡先など、各人の連絡先を明記すること。

E.4 重大インシデント対応プロセス

E.4.1 イベント通知

情報システム関連の緊急事態が発生したこと、または発生しようとしていることを発見した者は、所定のプロセスに従って関係者に報告し、関係者が最初の判断、通知、処理を行う。

E.4.2 要員の避難

指定された集合場所と代替の集合場所を提供し、避難の周知方法、避難の組織と手順等も記載する。

E.4.3 ダメージアセスメント

緊急事態発生後、緊急対応チームの損害アセスメント担当者は、状況の深刻度を判断する。災害復旧の責任者は、適切な専門家を招集し、クリティカル・インシデントの慎重なアセスメントを実施し、情報システムおよび関連するビジネス・プロセスへの影響の程度を判断し、次に取るべき措置を決定すべきである。システムへの影響が確定したら、所定の通知プロセスに従って、適切なチームに最新情報を通知すべきである。

E.4.4 災害宣言

災害復旧計画の発動条件は、あらかじめ定めておくべきである。被害アセスメントの結果、1 つ以上の発動条件が満たされた場合、組織は災害復旧計画の発動を宣言する正式な災害宣言を行い、宣言のプロセスに従ってすべての関連部門に通知する。

E.5 回復と再手術のプロセス

E.5.1 回復

ビジネスインパクト分析とリスクアセスメントで特定された優先順位に従って、災害復旧センターで重要なビジネス機能を支えるデータ、データ処理システム、ネットワークシステムを復旧する。各ステップについて、時間、場所、人員、設備、詳細な作業手順を記述し、特定の状況が発生した場合のチーム間の調整の指示や例外処理プロセスも記載する。

E.5.2 作戦再開

この段階では、プライマリ・システムの運用管理に関わる主要なタスクが含まれ、運用再開のためのすべての運用プロセスや規定が含まれる。災害復旧センターのシステムは、プライマリシステムに代わり、重要なビジネス機能の提供をサポートする。このフェーズでは、詳細なビジネスインパクト分析の結果を提供し、災害復旧センター内のデータ、データ処理システム、ネットワークシステムの復旧プロセスを優先順位の高い順に記述する。チームの調整ガイドラインや特定の状況に対する例外処理手順を含めながら、運用ステップ、タイムライン、必要な機器や人員を定義する。

E.6 震災後の復旧とロールバック

最終段階は、メインセンターの再構築、災害復旧システムの停止、スムーズな移行、組織のメインシステムへのフォールバックである。この段階では、メイン・センターの再構築、組織のメイン・システムへの切り替え手順やステップを含む、災害復旧の詳細な計画を提供する必要がある。

E.7 プログラムのセーフガード条件

予備計画の保護条件は以下の通りである：

a) 専門的な技術サポート：技術専門家、セキュリティ専門家、およびリソースを十分に確保し、要請できるようにする。

b) 通信支援：代替通信手段を含め、通信システムの可用性を保証する。

c) 後方支援：緊急施設や設備の供給と維持を確保する。

E.8 プログラムの附属書

プロフォーマの附属書セクションに以下を含める（ただし、これらに限定されない）：

a) 人員避難計画；

b) 計画のための訓練、テスト、リハーサル・プログラム

c) 商品説明

d) 情報システムの標準操作手順；

e) サービス・レベル・アグリーメントと覚書；

f) リソースのリスト；

g) ビジネスインパクト分析レポート；

計画のバージョン管理、保管、配布の手順と方法、計画の定期的な見直しと更新サイクルの明確化。

参考文献

[1] GB/T 22240-2020 情報セキュリティ技術ネットワークセキュリティレベル保護分類ガイドライン

[2] GB/T 28453-2012 情報セキュリティ技術情報システムセキュリティマネジメントアセスメント要求事項

[3] GB/T 29246-2017 情報技術 セキュリティ技術 情報セキュリティマネジメントシステムの概要と語彙

[4] GB/T 30279-2020 情報セキュリティ技術 ネットワークセキュリティ脆弱性分類および評価ガイド

[5] GB/T 31509-2015 情報セキュリティ技術 情報セキュリティリスク評価実施ガイド

[6] GB/T 31722-2015 情報技術 セキュリティ技術 情報セキュリティリスク管理

[7] ISO 31000 リスクマネジメントガイドライン

[8] ISO/IEC 13335 情報技術-IT セキュリティ管理のためのガイドライン

[9] ISO/IEC 27005 情報技術-セキュリティ技術-情報セキュリティリスク管理

[10] NIST Special Publication 800-26 情報技術システムのためのセキュリティ自己評価ガイド

[11] NIST Special Publication 800-30 情報技術システムのためのリスク管理ガイド