情報システム運用継続計画の策定ならびに運用継続を実現する配電システムの再構築について

中部電力（株），（株）中電シーティーアイ

■ 執筆者Ｐｒｏｆｉｌｅ ■

井上　裕成

1994 年　中部電力（株）入社
　　配電設計業務担当
1995 年　情報システム部所属
　　業務システム開発・保守業務担当
2009 年　現在 共通系設備計画策定担当

村田　誠

2000 年　（株）中電シーティーアイ入社
　　インフラ開発・構築担当
2009 年　現在 基盤システム部所属
　　配電系インフラ開発・構築担当

■ 論文要旨 ■

近年大規模災害等により，企業の事業が中断に追い込まれるケースが見受けられる．中部電力グループでは，東海，東南海・南海地震等による大規模災害や有事の際にも，安定した電力供給を目指し，復旧体制の整備・電力設備の信頼性向上対策など，ライフライン企業として災害対策の更なる強化に努めている．

このような中で，昨今のお客さま向けサービス・業務支援等の情報システム導入の増加により，情報システム運用の中断が事業の中断に直結することが懸念される．

そこで中部電力（株）では，情報システム運用の継続を実現する「情報システム運用継続計画」（以下 IT-BCP という）を策定し，まずは電力設備の早期復旧に必要となる配電システムを対象に， IT-BCP に準拠したシステムに再構築することで，システムの早期復旧を可能とした．

今後は，事業継続に必要となる情報システムを選定し，IT-BCP を展開していく．

■ 論文目次 ■

■ 図表一覧 ■

■ 付録一覧 ■

１．はじめに

１．１　当社の概要

中部電力グループは，愛知・岐阜（一部を除く）・三重（一部を除く）・長野・静岡（富士川以西）中部 5 県に，ライフラインである電気を中心に，ガス・LNG やオンサイトエネルギーなど，お客さまの多様化するニーズに対応した「安定」にかつ「安価」なエネルギーサービスを供給している．

またエネルギーの安定供給と地球環境の保全という，未来の世代に対する責任を全うするために，原子力を中心とする水力，太陽光等の非化石エネルギー比率の向上を目指した取り組みも進めている．

１．２　背景

近年地震，台風，感染症（SARS,新型インフルエンザ）等の自然災害，大規模システム障害，テロ等の人的災害の結果，企業の基幹業務が中断に追い込まれるケースが見受けられる．

公益性の高いライフラインの供給を担う中部電力グループでは，今世紀前半に発生する可能性が高いといわれている東海，東南海・南海地震などの大規模災害に備え，復旧体制の整備や電力設備の信頼性向上対策など，更なる強化に努めている．

一方社内業務では，お客さまサービス・業務支援等に向けた情報システムの導入増加など，情報システムに対する依存度の高まりから，情報システム運用の中断が業務の中断に直結し，お客さまをはじめ取引先などのステークホルダーに影響を及ぼすことが懸念される．

そこで情報システム部門では，経営・情報システムを取り巻く環境の変化に対応した，業務の継続に必要となる情報システム運用の継続※を実現していく．

※）情報システム運用の中断後，早期復旧による継続を含む

（１）　大規模災害発生の可能性

内閣府中央防災会議「東南海，南海地震等に関する専門調査会」の報告によると，今世紀前半に東海，東南海・南海地震が高い確率で発生するといわれている．

表 1　海溝型地震の 30 年以内の発生確率

地震名	想定地震規模 （マグニチュード）	地震発生確率 （30 年以内）
東海地震	M8.0 程度	80%程度
東南海地震	M8.1 前後	60%程度
南海地震	M8.4 前後	50%程度

（出典：地震調査研究推進本部「全国を概観した地震動予測地図報告書（H18/9 改訂）」より抜粋）

（２）　情報システム環境の変化

中部電力（株）では，平成 11 年にメインフレームを中心としたコンピュータセンタ 2 拠点相互バックアップを整備した．その後，インターネットの普及や設備のサーバ化など，業務を支える情報システムの利用形態・環境も複雑になり，大きく変化してきた．

（3）　規格・標準化の動向

国内では，内閣府，経済産業省などが BCP に関するガイドラインを公表し，各企業の導入機運を高めている．また海外では，国際標準化機構（ISO）が「事業継続マネジメント」に関する国際標準化を進めている．（付録　表 1 参照）

2．IT-BCP の策定

2．1　概要

大規模災害時，従業員の安否確認，災害対応・復旧支援業務および事業を継続するために必要な一定の通常業務（以下「非常時優先業務」という．）の実施に全力をあげることが求められる．

ヒト，モノ，カネ，情報等の経営資源は，被災状況が沈静化するまでの期間，使用することが制約される．非常時優先業務以外の通常業務は，率先して休止，もしくは非常時優先業務に支障を与えない範囲で実施する必要がある．

情報システム部門では，大規模災害発生に備え，被害を最小限に食い止め，速やかに復旧作業を実施するための防災対策を実施してきたが，従来の防災対策に加え，非常時優先業務に必要な情報システム運用を継続するため，「情報システム運用継続計画（以下 IT-BCP という）」を策定し，情報システムの運用継続を実現していく．

2．2　目的

大規模災害時に備え，以下対策等を実施することにより，非常時優先業務に必要な情報システムのより一層の「復旧時間短縮」，「運用レベル向上」（図 1）を実現する．

- 緊急時の体制確立（組織の継続）
- 情報システムリソースバックアップ（設備・データ等の両拠点確保）（図 2）
- 代替環境事前準備（正拠点環境の代替となる副拠点環境の準備）（図 2）

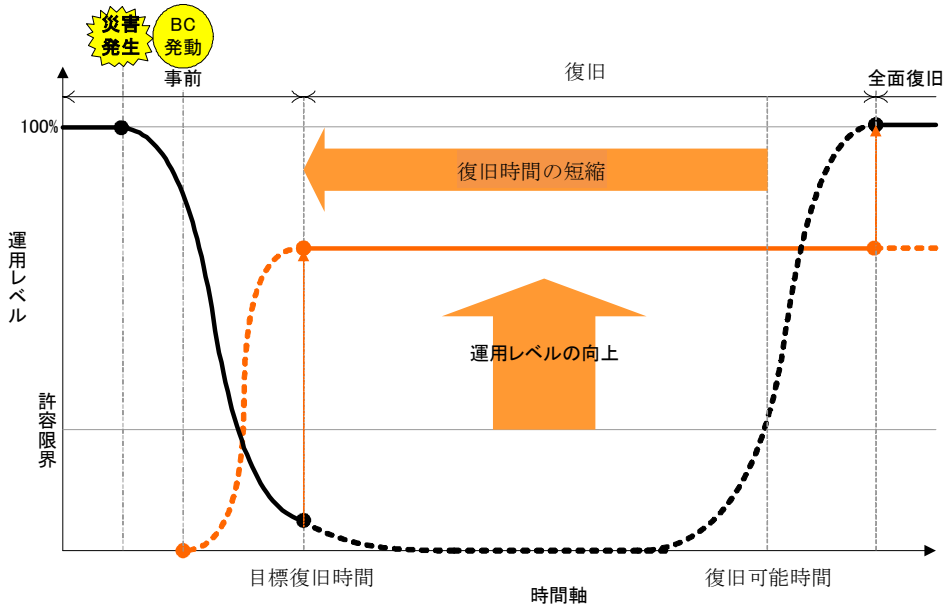

図 1　IT-BCP 実施による運用継続レベル

（出典：内閣府「事業継続ガイドライン　第一版」を基に追加）

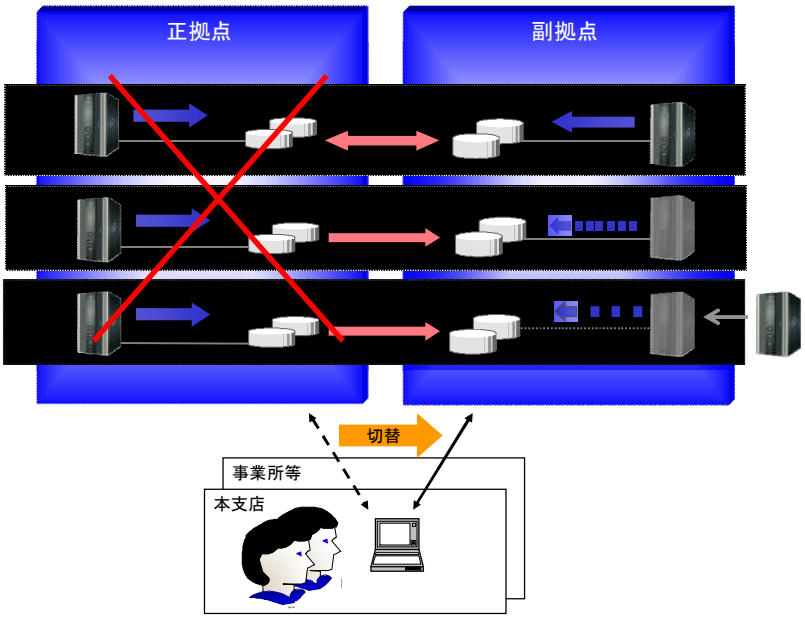

図 2　代替環境切替イメージ

また IT-BCP を実現し，維持・管理するために，PDCA サイクル（計画，実施，評価，見直し等）で管理する IT-BCM を確立する．（図 3）

本論文では，IT-BCP と IT-BCM を便宜的に「IT-BCP」と表現する．

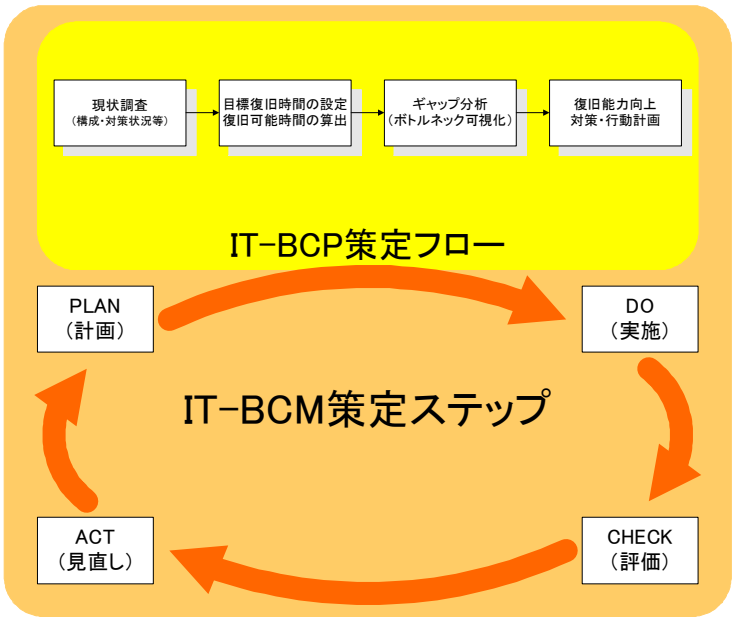

図 3　IT-BCM 策定ステップ

２．３　策定の流れ

IT-BCP 策定の主な流れとタスクを以下に説明する.

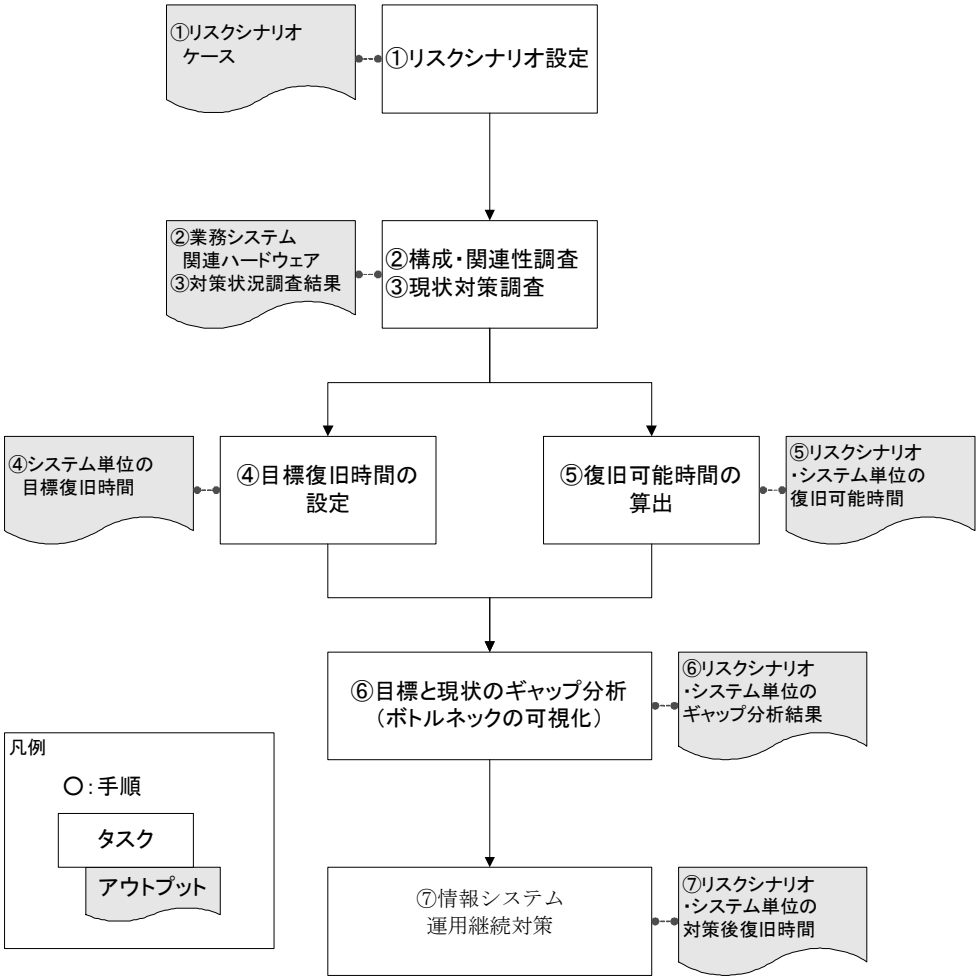

図 4　IT-BCP 概要フロー図

表 2　IT-BCP タスク概要

NO	タスク	内　　容
①	リスクシナリオ設定	地震，台風等の脅威が情報システムリソースに与えるリスクからシナリオを設定
②	構成・関連性調査	情報システム運用に必要な情報システムリソース（H/W，S/W，N/W，拠点建物，設備等）の把握
③	現状対策調査	情報システムリソース単位の対策状況の把握
④	目標復旧時間設定（RTO）	情報システム運用中断に伴う影響ならびに中断許容時間の設定
⑤	復旧可能時間算出（RTC）	運用中断から復旧までのプロセス整理ならびに復旧可能時間の算出
⑥	ボトルネックの可視化	リスクシナリオ毎に RTO と RTC のギャップから復旧長期化要因（以下ボトルネックという）の可視化
⑦	情報システム運用継続対策	ボトルネック解消ならびに復旧能力向上対策・行動計画の策定

（1）　リスクシナリオ設定

想定できるリスクシナリオ全てに対策を実施するには，多大な費用がかかり，また現実的ではないため，情報システム運用に関わるコンピュータセンタ拠点を対象とし，想定されるリスクから 9 つのシナリオに絞り込み設定した.

- リスクの考え方

情報システム運用の継続を妨げる自然災害，人的災害など脅威（原因）にはさまざまなものがあるため，脆弱性（可能性）から発生した際のリスク（結果）を絞り込む.（付録　図 1 参照）

- リスクシナリオの考え方

可視化したリスクが情報システム運用におよぼす影響範囲（広域・局所）から被害をイメージし，シナリオを絞り込む.

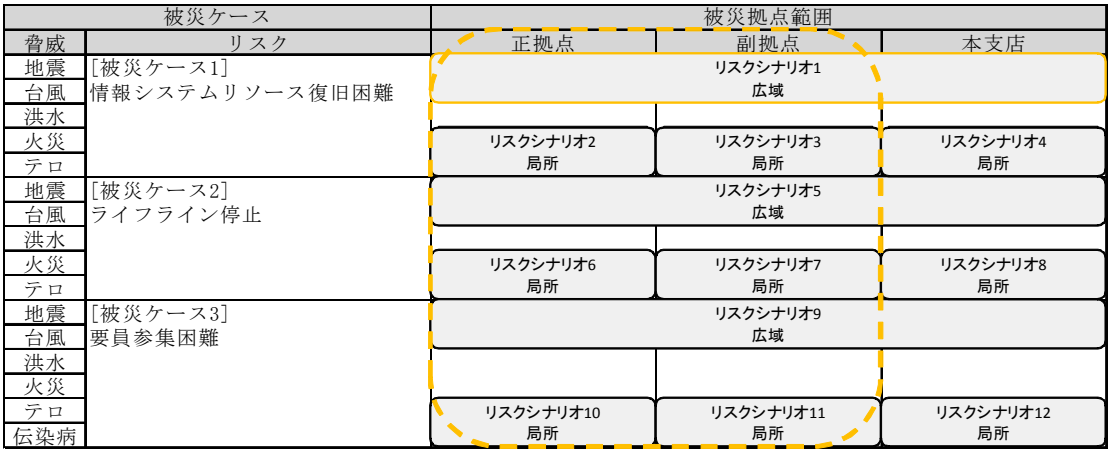

図 5　リスクシナリオ

（2）　目標復旧時間設定

非常時優先業務運用に影響を及ぼさない情報システム運用の中断から復旧までの許容時間を目標復旧時間（以下 RTO：Recovery Time Objective という）として設定する.

本来 RTO を設定するには，非常時優先業務が被災により中断した場合の影響を分析した上で優先度，目標復旧時間を設定する．しかし，現時点では非常時優先業務の分析を実施していないため，事業継続計画を策定している他社の事例等をもとに，中断に伴い影響を受ける範囲から RTO を仮設定した．（表 3）

表 3　情報システムの RTO

優先度	カテゴリ	RTO
S	従業員の安否確認，災害対応・復旧支援業務に必要	0.1 日
A	顧客にサービス提供する業務に必要	1 日
B	取引先，投資家等ステークホルダーに影響を及ぼす業務に必要	3 日
C	社内業務に必要	14 日

なお災害時には，機器，要員等リソースが限定されるため，平常時の運用レベルと比較した場合，運用レベルが低下することを想定しておく.

（3） 復旧可能時間算出

情報システム運用の中断から復旧までを復旧可能時間（以下 RTC：Recovery Time capability という）として算出する．

- 算出方法

リスクシナリオ単位に，建物や電力などのファシリティ，インフラ，業務 AP 等を段階的に復旧し，かかる時間を積算する．

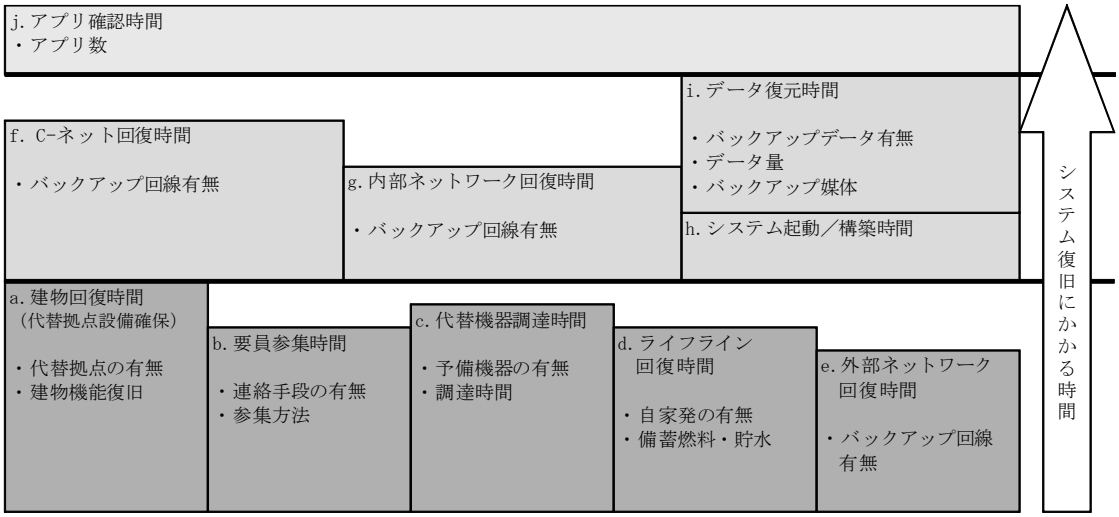

図 6 算出方法

- 算出条件
  - 限られたリソースの使用

    災害時には，公共交通機関等周辺環境の混乱により，外部からリソースを調達することが困難であるため，基本的には限られたリソースを使用し復旧する．
  - 算出根拠の設定

    リスクシナリオにもとづき，要員参集時間，ネットワーク回復時間等，各情報システムリソース復旧にかかる算出根拠を設定する．
  - 復旧シナリオの設定

    復旧には，「機器を移設する．」，「機器を修理する．」等様々な方法が考えられるため，復旧時のシナリオも設定する．

（4） ボトルネックの可視化

リスクシナリオ単位の RTC 算出結果と仮設定した RTO を比較し，IT-BCP 実現の妨げとなっているボトルネックを可視化する．

（5） ボトルネック解消対策の実施

情報システム運用を継続する上で必要となる，共通インフラ基盤のボトルネックを中心に，RTC を短縮する対策，行動計画を順次実施する．

具体的には，コンピュータセンタ正拠点が機能しない場合に，代替となる副拠点で情報システム運用を継続するために必要な対策，行動計画を順次実施する．

また業務システムの対策を実施するにあたっては，機器取替・再開発時に，効果等を勘案して，情報システムの RTO を満たす標準化したシステム構成（以下 DR：Disaster

Recovery モデルという）に近づけていくことにより，大規模災害発生時の混乱した状況下での，速やかな切り替えを実現する．

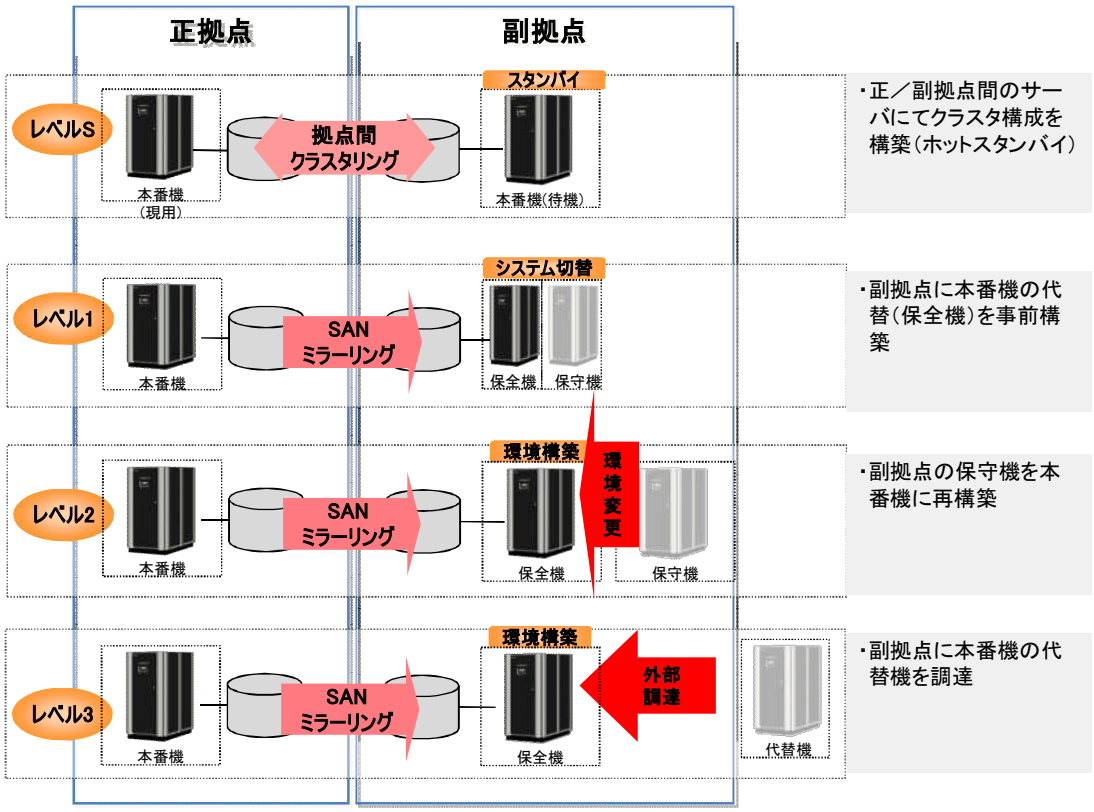

図 7 DR モデル

表 4　DR モデルの RTO・RPO

DR モデル		RTO		RPO※
レベル	名称	オンライン	バッチ	
S	遠隔クラスタ型	30 分程度	3 日程度	直近
1	保全機事前構築型	3 時間程度	3 日程度	直近
2	保全機事後構築型	7 日程度 （システム構築）		直近
3	保全機事後調達型	40 日程度 （調達＋システム構築）		直近

※）損壊したデータを復旧させる時点「目標復旧時点（Recovery Point Objective）」

2．4　IT-BCP 実施状況（配電システム抜粋）

全システムを対象に情報システムの運用継続を実現するため，IT-BCP を実施している．

電力設備の早期復旧を実現するために必要となる配電システム※の IT-BCP 実施状況（平成 19 年度末時点）では，RTO と RTC に約 32～42 時間のギャップがあり，30 分間隔で拠点間のファイル転送を実施していることがボトルネックとなっている．

※）お客さまに電気をお届けするために必要な電柱・変圧器等の配電設備，供給等を管理するシステム．

表 5　配電システムの IT-BCP 実施状況

NO	タスク	内　　容
①	構成・関連性調査	• 両拠点に合計 22 台のサーバを配置
②	現状対策調査	• 両拠点に本番の代替となる機器を設置（図 8） • データの外部保管は，両拠点のサーバで相互に 30 分間隔で転送する方式
③	目標復旧時間設定（RTO）	• RTO：0.1 日（約 3 時間）に設定（優先度：S） 災害時に電力供給業務を支援するシステム
④	復旧可能時間算出（RTC）	• RTC：約 35～45 時間 システム起動時間（3 時間）＋データ復元時間（30～40 時間）＋アプリ確認時間（2 時間） • 片拠点被災時は，健全拠点のサーバで運用継続
⑤	ボトルネックの可視化	• ギャップ：約 32～42 時間 • ボトルネック：30 分間隔のファイル転送によるデータ損失
⑥	情報システム運用継続対策	• 拠点間のデータ同期性を高める対策の実施．（DR モデルの SAN ミラーリングによる対策）

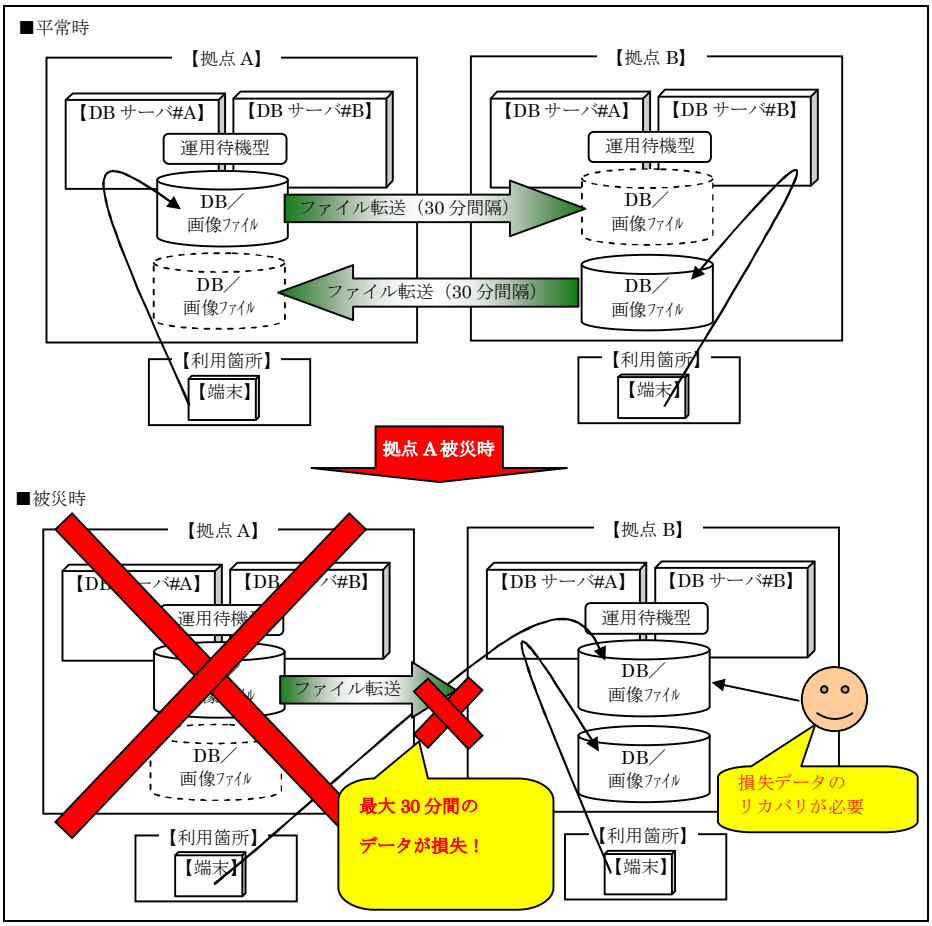

図 8　旧配電システム構成図

３．IT-BCP に準拠した配電システムの再構築

前述の IT-BCP 実施状況から，配電システムでは RTO と RTC に大きなギャップがあることが判明した．そこで，配電システム再構築のタイミングで IT-BCP の DR モデルに準拠したシステム構成に変更し，災害時の運用継続の実現を図った．

ここでは，再構築に伴うデータ保全機能の概要ならびに設計上の考慮点を中心に説明する．

３．１　新配電システムの要件定義

配電システムの再構築では，RTO 以外に，保全対象データのサイズ増加，および対象サーバの拡充という要求があった．具体的な要求内容は以下のとおり．

＜新配電システムへの要求内容＞

- RTO：約 3 時間
- データサイズ増加：DB データ（ギガバイトオーダ），画像ファイル（テラバイトオーダ）
- 復旧対象機器：DB サーバ以外に， WebAP サーバも対象

RTO が約 3 時間という要求を満たすため，新配電システムでは，DR モデルのレベル１でシステムを再構築する．構築にあたり，システム化要件定義を（表 6）にまとめる．

表 6　新データ保全機能のシステム化要件

要件区分	要件定義
システム構成	• 正拠点に本番機，副拠点に保全機を配置 • 正／副拠点間のデータ同期性を保つ SAN ミラーリングを使用 • 対象サーバは DB サーバと WebAP サーバ
データ保全	• DB データ，画像ファイル，プログラムなど，その特性に応じたデータ保全の仕組みを構築・開発 • データ復元の長時間化に対応するため RPO を直近
運用インフラ	• 保全機への切替時間を短縮するため，以下の切替機能を開発 － システム切替機能（保守機の環境から保全機の環境への切替） － ネットワーク切替機能（端末の接続先サーバ切替）
構築・テスト	• 事例のないシステム構成のため，技術検証レベルからテスト実施 • 保全データの同期性の検証を実施 • 開発する切替機能を使用し，サーバの切替を 3 時間で実施
運用	• 24 時間 365 日勤務の運用要員で切替操作を実施 • 切替操作に関するマニュアルを整備 • 運用開始前に運用要員による切替訓練の実施

３．２　システム構成

（１）　設計／構築内容

DR モデルレベル 1 は，保全環境と保守環境を 1 台のサーバで共用し，被災時に保守から保全に環境を切替えて，ミラーリングされた SAN に接続する構成である．

このようなレベル 1 の DR モデルは，SAN ベンダでの事例がなく，中部電力（株）が新配電システムにてはじめて実装するモデルである．

具体的には，図 9 に示すとおり，正拠点に本番サーバを構築し，副拠点に保全／保守機を構築する．（主要ハードウェアとソフトウェアの構成は付録の表２を参照のこと）

新データ保全機能におけるシステム構成のポイントを以下に記載する．

- SAN 上のデータをテープにバックアップするバックアップ管理機器を導入
- 大量データの保存および複数サーバ間でのファイル共有を目的に NAS を導入
- 副拠点のサーバは保全と保守の SAN／ネットワークに接続する構成

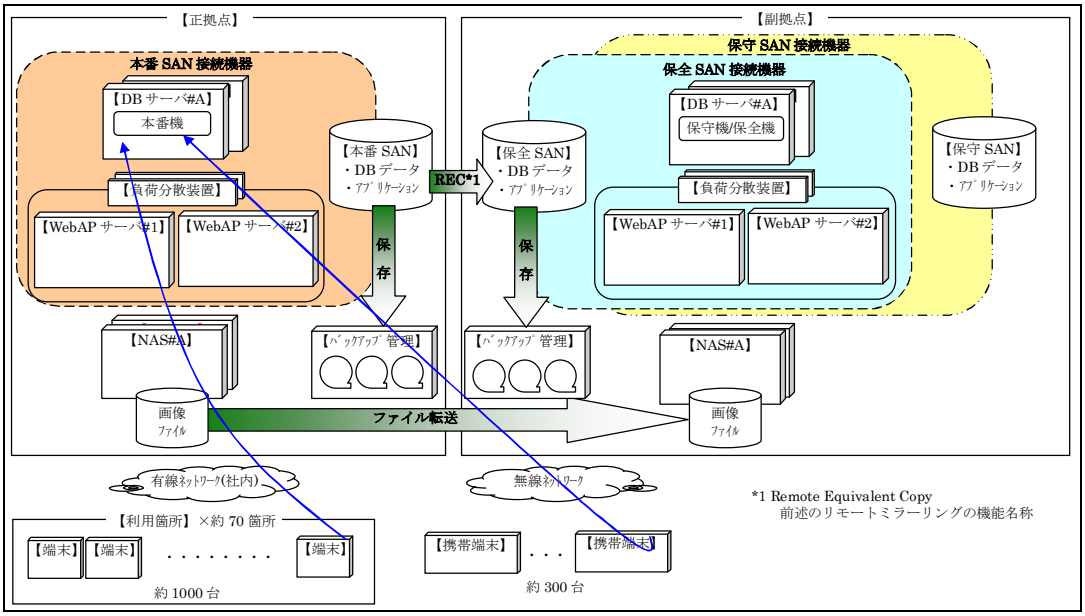

図 9 新配電システム構成図

３．３　データ保全

（１）　設計／構築内容

保全すべきデータの特性を考慮し，データの配置を設計した．

表 7　特性を考慮したデータの配置

データ区分	特性	データ配置
DB データ	• サイズはギガバイトオーダ • 一部を失った場合，業務システムがエラーとなり，処理再開時にデータの再投入が必要	SAN
画像ファイル	• サイズはテラバイトオーダ • 一部を失っても業務システムは停止しない • 原本となるデータが利用箇所に存在しリカバリが DB データに比べ容易	NAS
アプリケーション	• サイズはデータに比べ小さい • 保全側でも最新のアプリケーションが必要	SAN
設定ファイル	• サイズはデータに比べ小さい • 制約上 SAN に配置できないファイル有り • 更新頻度は少ない	サーバ内蔵ディスク

（2）　設計上の考慮点

データ保全設計において，以下の考慮を行なった．

- 画像ファイルは，テラバイトオーダであり単純に SAN に配置すると設備費用が高くなる．データ特性を考慮し NAS に配置してファイル転送でデータを保全（図 10）
- 大量の画像ファイルから更新されたファイルのみ副拠点に転送する仕組みを開発
- 設定ファイルは日次バックアップ処理で配置したサーバ内蔵ディスクから SAN ディスクにコピーし，SAN ミラーリングでデータ保全

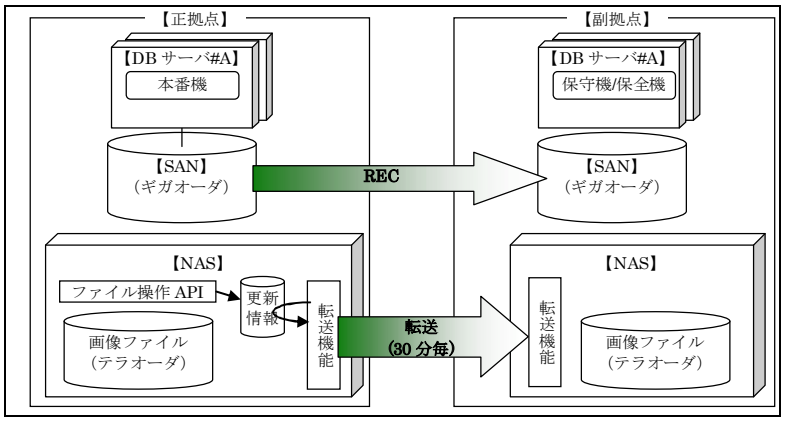

図 10　データ保全の仕組み

3．4　運用インフラ

（1）　設計／開発内容

保全環境への切替時間の短縮化を図る目的で開発した，運用インフラの機能を以下に述べる．

a.　システム切替機能

保守環境と保全環境の早期切替を実現するため，保守／保全機に保全環境用と保守環境用のネットワーク・SAN を接続する．OS 環境はブートメニューを使用して選択起動する方式とする．（図 11）

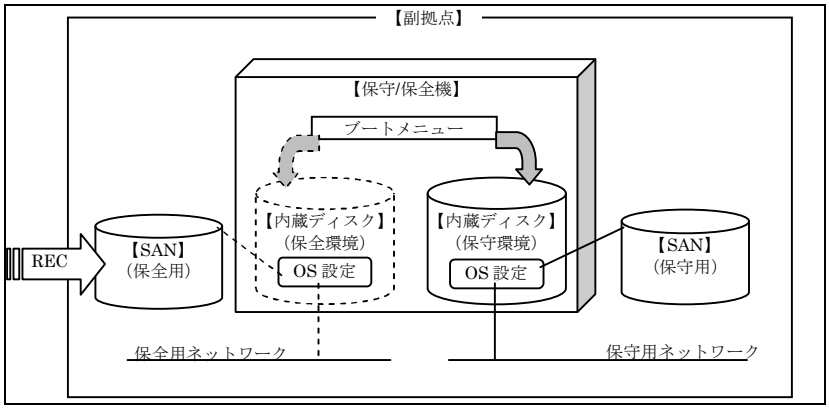

図 11　保全／保守機のシステム環境切替方式

b.　ネットワーク切替機能

保全機を起動しても，システム利用者の端末など連携機器からの接続先サーバを，

本番機から副拠点の保全機に切り替え（以下ネットワーク切替という）なければ使用できない．図 12に示すように，DNS サーバの IP アドレス切替の仕組みにより，システム利用者は接続先サーバの変更を意識する必要がない．

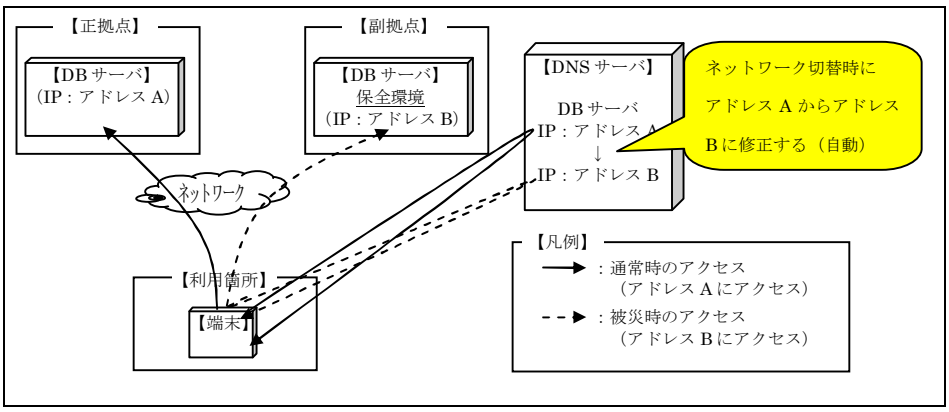

図 12　DNS の IP アドレス切替方式

（2）　設計上の考慮点

開発した２つの切替機能について，以下の設計上の考慮を行なった．

a.　システム切替機能

副拠点の保守／保全機は，通常保守環境として起動しているため，保守目的にリブートを行なう場合がある．誤ってブートメニューから保全環境を選択して起動した場合，以下の問題が発生する可能性がある．（図 13）

① 本番 SAN から REC※されている保全 SAN ディスクを強制的にサーバでマウントすることによりデータ破壊が発生する．

※リモートミラーリングの機能名称(Remote Equivalent Copy)

② 保全環境のシステムが本番環境のシステムとして起動するため，誤って他の本番サーバと連携し，誤処理が発生する．

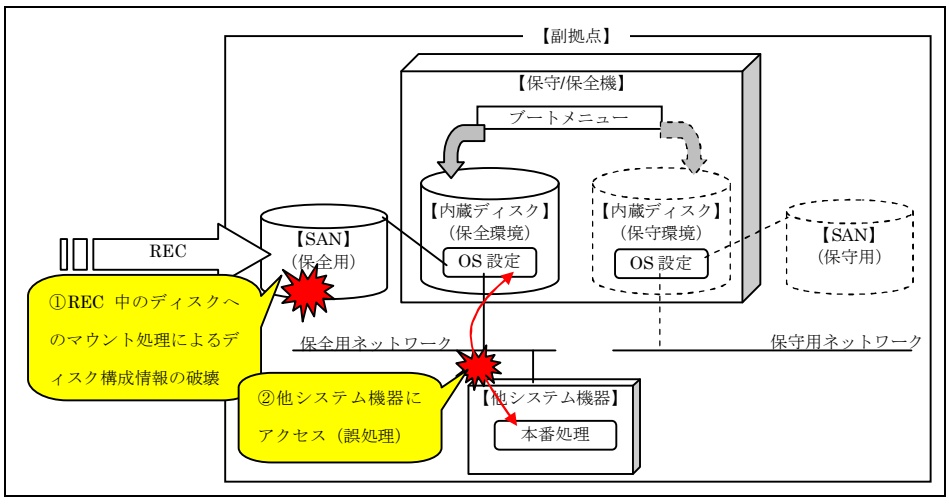

図 13 誤った保全環境起動による影響（データ破壊と誤処理）

これらの問題に対応するため，以下のサーバ起動制御を行なった．（図 14）

① ブートメニューのデフォルト起動環境を保守環境とすることにより，誤って起動した場合に保全 SAN ディスクのデータ破壊を回避する．

② ブートメニューから保全環境選択後，REC されている保全 SAN ディスクのマウント前でシステム起動を一時停止させる．その後人間系で判断し，コマンド投入により，起動処理を継続する．誤操作防止のため，2 重チェックを行なう．

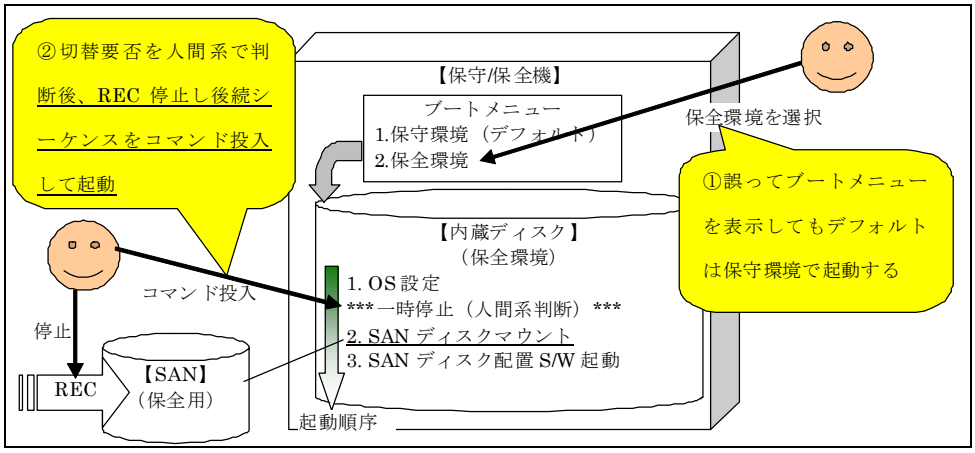

図 14 サーバ起動制御による障害未然防止

b. ネットワーク切替機能

DNS サーバ側では他システムの IP アドレスを切り替える機能が存在したが，他システムの切替手順に依存しない被災切替オペレーションを実現するため，配電システムの IP アドレスを切り替える専用の機能（コマンド）を開発した．

3．5 構築・テスト

DR モデルレベル 1 の適用が中部電力（株）で今回はじめてであり，また SAN ベンダでも事例がないことから，システム設計・構築に関する情報を得ることができなかった．このため，データ保全機能を構築するにあたり，テストを技術検証レベルから開始し，運用で使用できるレベルまで実施した．

（1） 構築・テストフェーズの考え方

まず，REC された副拠点の SAN ディスクを HP-UX の OS から接続できるかという OS レベルの検証（単体テストレベル）を行い，OS 上位のソフトウェアの環境切替と動作確認（結合テストレベル）を実施し，その後切替手順を見直して運用に耐えられる手順を作成（総合テストレベル）するという，3 フェーズで運用できるデータ保全機能の構築・テストを行なった．（図 15）

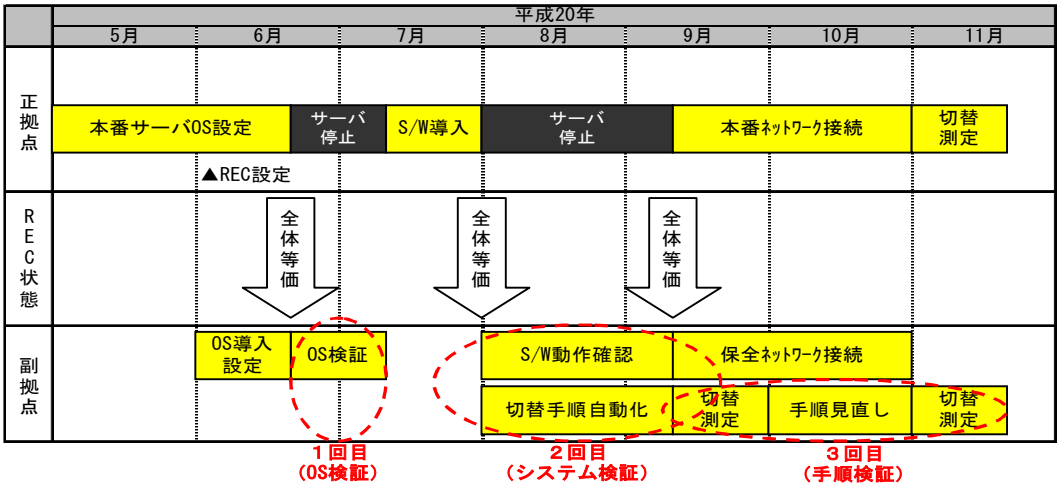

図 15　構築・テストフェーズの考え方

（2）　OS レベルの検証項目（単体テストレベルの検証）

- 正拠点のサーバと REC を正常に停止させた状態でテストする.
- REC されたディスクを使用し，保全機の OS および主要 S/W（Oracle や Websphere）の起動を確認する.
- 保全機の起動操作は，エラー箇所を特定するため 1 ステップずつ入力して検証する.

（3）　システムレベルの検証項目（結合テストレベルの検証）

- 保守環境で起動していたサーバをブートメニューで保全機へ切り替え起動する.
- 保全機で，システムが正常に切り替えられたか確認する.
- 被災時を想定したデータ更新中の REC 強制切断での切替テストを実施し，データの同期性を検証する.

（4）　切替手順の検証項目（総合テストレベルの検証）

- 切替訓練を兼ねて，マニュアル化した切替手順が運用要員にて操作可能か検証する.
- 切替手順に沿って， DB サーバを 3 時間以内に切り替えられることを確認する.

3．6　運用

（1）　被災切替時の運用

正拠点から副拠点への切替は，以下の順序で行なう設計とした．また，関連するシステムの切替箇所を図 16 に示す.

① 正拠点のサーバを停止（停止できる状況であれば）
② SAN の REC 機能の停止
③ 副拠点のデータバックアップ（被災時のデータを保障）
④ DNS による IP アドレスの切替
⑤ 副拠点のサーバの起動と保全 SAN 接続
⑥ 保全機でのシステム動作確認
⑦ 閉塞解除＆業務再開

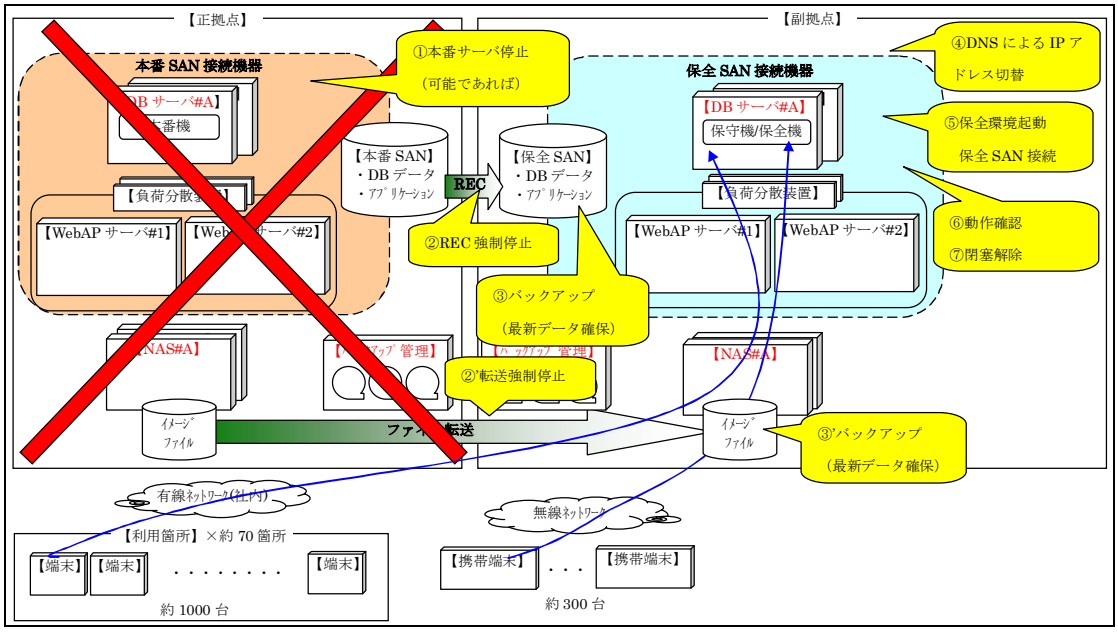

図 16　被災切替運用

（2）　設計上の考慮点

災害時には，24 時間 365 日勤務の運用要員にて正拠点から副拠点にシステム環境の切替を行なう必要がある．切替は，手順が多く複雑だと誤操作が発生する可能性があるため，マニュアル化して運用要員で実行できる簡略な手順が望ましい．切替手順について以下の考慮を行い，簡略化を図った．

a.　同時実行可能手順と先行/後続手順の関係整理

複数サーバの起動など前の処理の完了を待たず次の操作が行なえる手順と，SAN 接続後のシステム起動操作などの先行／後続関係のある手順を整理することで，運用要員の不要な待ち時間をなくし，簡略化した．

b.　切替手順の半自動化

切替操作は，コマンド投入後に応答キー（Y/N）を入力する形で実装した．この実装方法により，１つ１つコマンドを投入するよりも，キーの入力量を減らすことにより，操作を簡略化した．

c.　動作確認ツールによる複数機能の一括動作確認

機能毎に動作確認するツールに加え，複数の機能の動作確認を一括で行なえるツールを開発し，切替後の動作確認時間の短縮化を図った．

上記，切替手順の簡略化前（平成 20 年 9 月）と簡略化後（11 月）に運用者による切替訓練を実施し，切替時間を測定した．図 17に示すとおり，3 時間以内で切り替えられることが確認できた．

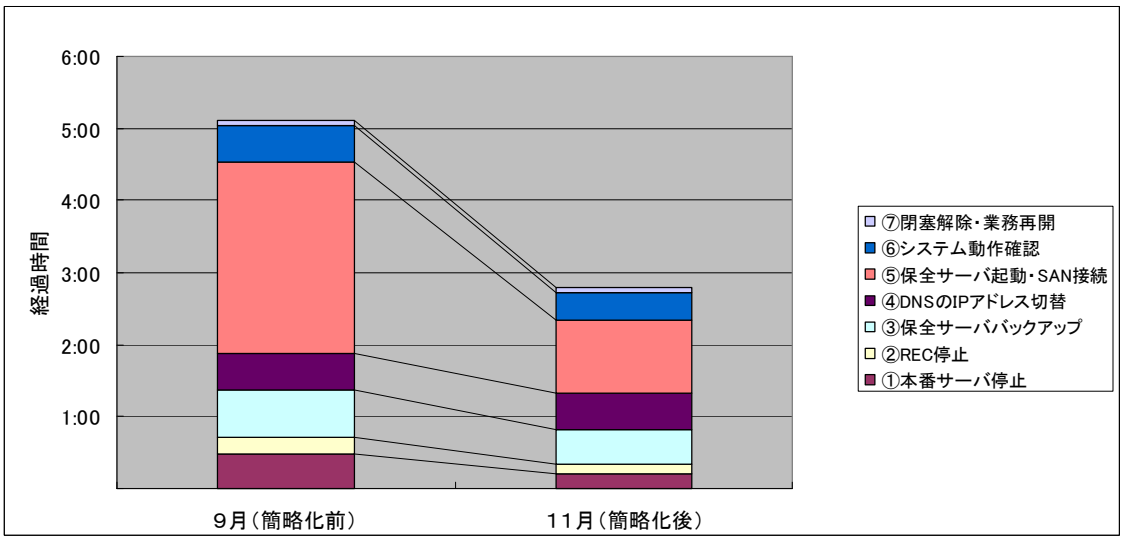

図 17　運用者による被災切替時間の測定結果

４．課題と今後の展望

４．１　被災訓練の実施

運用要員にて配電システムの切替ができることは，前述の通り確認できた．今後は以下の観点で，定期的な訓練を実施していく．

- 切替オペレーションの属人化の排除
- メインフレームも含めた被災切替確認
- 要員参集から業務処理再開までの，人間系の確認を含めた訓練.

※平成 22 年 1 月に一部の訓練を実施予定.

４．２　システム変更対応

DR モデルレベル 1 では，保全／保守機が通常保守環境として起動しているため，本番環境の設定反映が随時行なえない．そのため，本番環境への設定変更を厳密に管理し，適切なタイミングで保全環境へ反映していく．

また，将来計画されているメインフレーム上で稼動する業務システムのオープン化時に，今回の被災対応システムを拡充して対応していく．

４．３　IT-BCP に準拠したシステム構築ガイドの作成

配電システムの再構築では，DR モデルに準拠するため，先に述べた設計上の考慮を行った．今後，IT-BCP を円滑に展開していくため，設計上のポイントを整理し，DR モデルのガイドに追加していく．（平成 21 年度に作成予定）

表 8　DR モデル準拠システムの構築ガイド記載事項案

設計フェーズ	記載事項
システム構成	• RPO に応じた SAN 以外のストレージ装置の追加 • 保全／保守機の SAN・ネットワーク環境
データ保全	• データ特性を考慮した配置

設計フェーズ	記載事項
	• ソフトウェアの制約を考慮したアプリケーション，設定ファイルの配置
運用インフラ	• システム切替機能の設計 • ネットワーク切替機能の設計
構築・テスト	• REC 後の保全機の S/W 動作確認 • 運用要員による切替訓練と時間測定
運用	• 本番／保全環境の整合管理 • 切替手順の簡略化とドキュメント体系の標準化 • 切替・被災訓練を定常化する運用計画

５．おわりに

情報システム運用の継続を実現するにも，人（復旧・運転要員等），モノ（サーバ等機器類），カネ（代替環境構築費用等），情報（データバックアップ）等多大な経営資源を必要とする.

大規模災害時の混乱した状況のもと，限られたこれらのリソースですべての情報システム運用を継続・復旧することには，限界がある.

今回情報システム部門の取り組みとして IT-BCP を推進してきたが，今後は業務を中心として実施する事業継続計画（BCP）を推進する中で，情報システムがなければ継続できない非常時優先業務を対象に，情報システム運用の継続を実現していく.

また，災害訓練等を定期的に実施することにより，実施した対策，DR モデル等の見直しを実施し，より精度の高い情報システム運用の継続の実現を目指す.

最後に IT-BCP の策定・配電システムの再構築にあたり多大なご支援をいただきました富士通総研（株）殿，富士通（株）殿ならびに関係者各位に感謝の意を表します.

参考文献

［１］地震調査研究推進本部：全国を概観した地震動予測地図報告書（H18/9改訂）
［２］内閣府：事業継続ガイドライン　第一版
［３］経済産業省：事業継続計画（BCP）策定ガイドライン

付録

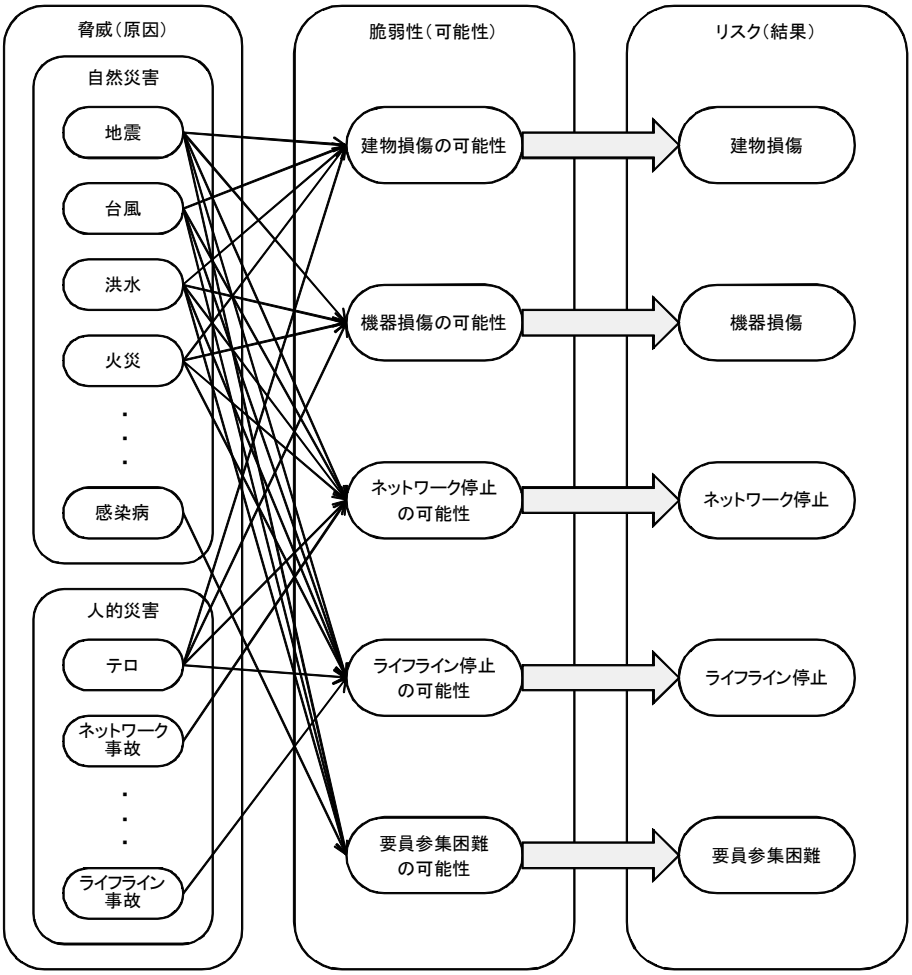

図 1　脅威－脆弱性－リスクの関係

表 1　規格化・標準化動向

発行元	名称	概要	公表時期
内閣府	事業継続ガイドライン	政府としてまとめた初の事業継続ガイド	平成 17 年 8 月
経済産業省	事業継続策定ガイドライン	情報システムを中心とした事業継続ガイド	平成 17 年 8 月
内閣府 中央防災会議	首都直下地震対策大綱	首都中枢機関の事業継続計画を策定を決定	平成 17 年 9 月
経済産業省 中小企業庁	中小企業 BCP 策定運用指針	中小企業を対象にした事業継続指針	平成 18 年 2 月
日本情報処理開発協会	事業継続管理（BCM）に関する利用ガイド	情報システムの活用・事業継続のガイド	平成 18 年 3 月
内閣府	中央省庁業務継続ガイドライン第１版	各省庁が作成する事業継続ガイド	平成 19 年 6 月
国土交通省	国土交通省業務継続計画	「首都直下地震対策大綱」を受け作成	平成 19 年 6 月
中央省庁等	各省庁業務継続計画	17 の中央省庁等で業継続計画を策定	平成 20 年 4 月 ～7 月
今後の動向			
国際標準化機構（ISO）	（仮）事業継続に関する国際規格	事業継続の国際規格	平成 22 年以降

表 2 H/W と S/W 構成

機器名	H/W 機種	OS	搭載主要 S/W
DB サーバ	HPIntegrity rx6600	HP-UX11i v2	MC/ServiceGuard
			Oracle Database
			SystemWalker/OperationMGR
			ETERNUS SF Storage Cruiser Agent
			ETERNUS SF Advanced Copy Manager Agent
			ETERNUS SF Recovery Manager for Oracle
WebAP サーバ	HPIntegrity rx3600	HP-UX11i v2	WebSphere
			IBM HTTP Server
			SystemWalker/OperationMGR
			ETERNUS SF Storage Cruiser Agent
			ETERNUS SF Advanced Copy Manager Agent
ﾌｧｲﾙ共有	HP DL380 G5 Storage Server	WindowsUnified Data Storage Server 2003	HP Backup Exec 11d for Windows Servers
負荷分散装置	BIG-IP6400	－	－