

ICT部門における業務継続計画 訓練事例集(構成案)

2012年11月26日



目次

- 事例1 システム被害状況調査に関するシミュレーション訓練
- 事例2 …

BCPの検討実施段階に応じた訓練

- BCPの検討段階によって適切な訓練を実施し、実効性を高めていく必要がある。
- また、これらの訓練は一度実施すれば終わりというものでなく、内外の状況変化や時間の経過により陳腐化させないために、BCP策定後も、定期的に繰返し実施する必要がある。

実施段階	目的	概要	訓練の種類
BCP検討前	BCP関連メンバーの基礎教育	BCP策定前に検討メンバーに対し、BCPの基礎知識災害時に起こる事象、行動すべき内容などの理解を深め、BCPの取組み必要性に対する意識高揚を図る。	<ul style="list-style-type: none"> ・セミナー ・イメージアップ訓練
行動計画作成後	ドキュメントの内容理解、精度向上	作成した計画書に基づき、手順の確認、代替先への移動、確保している資源の確認などを行い、ドキュメントの内容理解を深めると共に抜け漏れや不整合のチェックを行なう。 <ul style="list-style-type: none"> －各種計画・マニュアル・チェックリストのチェック 	ウォークスルー (手順確認訓練)
事前対策実施後	事前対策の実効性確認と手順の体得	重要な要素となる項目について実効性を確認すると共に、何度も繰り返す、反復して身に付ける。 <ul style="list-style-type: none"> －連絡訓練、安否確認訓練、チーム・要員参集訓練、バックアップシステム稼動訓練、避難・消火・応急手当等の訓練、安否確認訓練、本部設置訓練、業務再開訓練、備品等の取扱訓練 など 	ドリル(反復訓練)
BCP策定後	BCPの実効性確認とBCP要員の理解向上	策定したBCPに基づき、一定の状況の中で、対応や意思決定する内容等を確認する。 <ul style="list-style-type: none"> －情報収集・管理、本部運営、チーム運営 	シミュレーション訓練 (状況設定訓練)
BCP策定後 (全体で確認)	各種BCP関連施策の整合確認とBCP要員の災害時対応力向上	シミュレーション訓練+ドリルを組み合わせ、模擬負傷者の救護、搬送や代替事務所への移動、目標復旧時間内の業務再開などに挑戦し、対応力を確認する。現実に見舞われるリアルな状況を可能な限り想定し、実際に活用する環境等で実施する。	フルスケール エクササイズ (総合演習)

※BCAOテキストを加工

事例1 システム被害状況調査に関するシミュレーション訓練

- 被災シナリオに基づいて被害状況を設定し、その被害を特定して適切に復旧方針を立てることができるか、シミュレーション訓練を実施した。

実施段階	目的	概要	訓練の種類
BCP検討前	BCP関連メンバーの基礎教育	BCP策定前に検討メンバーに対し、BCPの基礎知識災害時に起こる事象、行動すべき内容などの理解を深め、BCPの取組み必要性に対する意識高揚を図る。	<ul style="list-style-type: none"> ・セミナー ・イメージアップ訓練
行動計画作成後	ドキュメントの内容理解、精度向上	作成した計画書に基づき、手順の確認、代替先への移動、確保している資源の確認などを行い、ドキュメントの内容理解を深めると共に抜け漏れや不整合のチェックを行なう。 <ul style="list-style-type: none"> －各種計画・マニュアル・チェックリストのチェック 	ウォークスルー (手順確認訓練)
事前対策実施後	事前対策の実効性確認と手順の体得	重要な要素となる項目について実効性を確認すると共に、何度も繰り返し、反復して身に付ける。 <ul style="list-style-type: none"> －連絡訓練、安否確認訓練、チーム・要員参集訓練、バックアップシステム稼動訓練、避難・消火・応急手当等の訓練、安否確認訓練、本部設置訓練、業務再開訓練、備品等の取扱訓練 など 	ドリル(反復訓練)
BCP策定後	BCPの実効性確認とBCP要員の理解向上	策定したBCPに基づき、一定の状況の中で、対応や意思決定する内容等を確認する。 <ul style="list-style-type: none"> －情報収集・管理、本部運営、チーム運営 	シミュレーション訓練 (状況設定訓練)
BCP策定後 (全体で確認)	各種BCP関連施策の整合確認とBCP要員の災害時対応力向上	シミュレーション訓練+ドリルを組み合わせ、模擬負傷者の救護、搬送や代替事務所への移動、目標復旧時間内の業務再開などに挑戦し、対応力を確認する。現実に見舞われるリアルな状況を可能な限り想定し、実際に活用する環境等で実施する。	フルスケール エクササイズ (総合演習)

※BCAOテキストを加工

事例1 訓練概要

- 機器のランプやコンソール画面に状況設定を添付し、実際の被害調査箇所を確認した。

項目	内容説明
団体プロフィール	<ul style="list-style-type: none">● 関東地方沿岸部近辺に所在、人口約5万人● ほとんどのICT資産は庁内の電算室に設置、情報システム部門専任職員5名
背景と目的	<ul style="list-style-type: none">● ICT-BCPを策定したが、詳細な手順・チェックシートの検討や必要な機器の準備が十分できていなかった● 発災後72時間の初動フェーズに焦点をあて、ICT-BCPの内容理解を深めるとともに、手順とリソースの実効性を検証・強化することを目的とした
訓練範囲	<ul style="list-style-type: none">● 情報システム部門のみで初動フェーズのシステム被害状況調査を実施
訓練実施内容の解説	<ul style="list-style-type: none">● 就業時間中に震度6強の大きな地震が発生したことを想定● 情報システム関連機器について、参集時の初期評価と復旧に向けた初期損害評価を実施● 被災シナリオに基づいて、機器のステータスを表すランプやコンソール画面に状況設定を付箋やテキストなどで仕込み、被災時に調査すべき箇所を実際ひとつひとつ確認した
参加者と役割	<ul style="list-style-type: none">● 情報システム部門：情報システムの被害状況調査、復旧方針の検討● コンサルティング会社：災害対策本部役として全庁の情報提供・報告受け、訓練の進行・記録
評価項目(訓練KPI)	<ul style="list-style-type: none">● アンケートによる理解度(5段階)と妥当性(5段階)の主観的評価● 観察・記録による所要時間とつまずいた工程などの客観的評価
訓練の結果得られた教訓	<ul style="list-style-type: none">● 被災時の調査手順と実際の調査箇所を理解することができた● ICT-BCP/チェックシート、ネットワーク調査ツール、訓練の継続・運営などの改善案27件
事前準備事項と準備期間	<ul style="list-style-type: none">● 被災シナリオの検討、被災状況設定の仕込み、調査結果の模範解答策定などに約2週間

事例1 被災シナリオサンプル

- 訓練の目的に即して、被災シナリオを設計。
- 初回訓練としては、現状の対策である程度対応できる比較的軽微な被害を想定。

被災シナリオ(1/2)

- 平成24年11月7日(水)午前10時30分、***地震(マグニチュード7.9)が発生。
- ***周辺は震度6強。一部、液状化の被害も見られる。



被災シナリオ(2/2)

- 平日昼間に被災したことを想定。社会インフラは一時的に麻痺するものの半日~1日でほぼ復旧。
- 庁内では、建物は利用できるが、システムが停止し固定されていない備品が飛散する。

発災日時:平日昼間 ▼

		~24h	~36h	~72h
社会インフラ	電力	非常用電源	燃料補給により非常用電源を継続使用	
	ガス	利用不可	利用可能	
	水道	利用不可	利用可能	
	通信	防災用無線・インターネットは利用可能		
		携帯電話はメールのみ利用可能	携帯電話は通常通り利用可能	
	交通	鉄道運休	鉄道復旧	
庁内インフラ	建物	倒壊はなく利用可能、火災・水害なども発生しない		
		固定されていない機器が転倒・飛散		
	IT	本番システムは利用できないものがある(PC、サーバ、ストレージ)		
		庁内ネットワークは利用可能		
		待機系の資産は利用可能(予備PC、バックアップデータ)		
要員	要員は庁舎で活動可能			

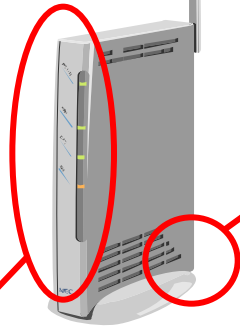
【ICTの被害状況設定】

- ルータの電源ケーブルが抜け落ち、インターネット不通
- ***サーバの運用系HDDに物理的障害が発生し、待機系に切り替わる
- ※***サーバはFTサーバで運用系/待機系の冗長構成。その内運用系のHDDに物理的障害が発生し待機系に切り替わり、システムとしては使用できている状況。

事例1 被害状況設定サンプル

- 災害時に実際に状況を調査するケーブルの位置やコンソール画面の中に、被災シナリオに従って被害状況を付箋などで添付する。

ルーター

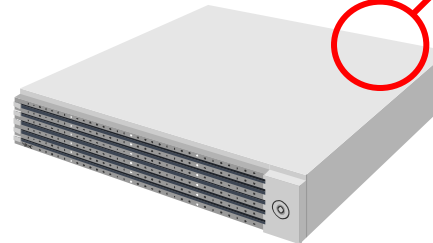


「アダプター抜け落ち」



「全消灯」

サーバ



「アンバー色点灯」

事例1 訓練記録サンプル

- 実態に即したチェックシートや手順の見直し、普段の資産管理の徹底などの課題が抽出された。

訓練記録：被害状況調査

- 参集後の初期調査は約20分で完了。設定した障害も実機を確認して円滑に発見できた。
- 標準のチェックシートが実態に合わない部分もあり、効率化の余地がある。

より実態に即したチェックシートが求められる

時刻	作業内容・状況	つまづいた工程 など
10:01	参集後の初期調査開始	<ul style="list-style-type: none"> ● 様式7で確認する指定避難場所に情報システム部門として支援すべき事項はないため、調査の必要はない ● 様式7で調査する「庁舎」は、情報システム部門では「分庁舎」になる ● 情報システム一覧に基づく状況確認は初期調査の段階ではできない
約20分でスムーズに初期調査完了		
10:22	情報システム部門責任者への初期調査結果報告	
10:25	初期損害調査開始	<ul style="list-style-type: none"> ● システムやネットワーク機器の目視確認より、Pingによる両者の一括確認を先にする方が効率的
10:44	機器の状況確認完了	
10:54	Pingによるネットワーク導通調査完了	<ul style="list-style-type: none"> ● Ping調査ツールがローカルディスクにインストールされておらず、ファイルサーバからダウンロードする必要があった ● Pingを返さない機器もあるため、機器の調査や人間系での判断が必要。すでに廃止したIPアドレスが残っているケースがあった。 ● 障害を検知した際には、実際には復旧作業を即時開始することが想定される。調査を継続する要員と役割分担をするなど要検討
10:55	情報システム部門責任者への初期損害調査結果報告	<ul style="list-style-type: none"> ● ネットワークの導通状況に関する報告が漏れていた
11:10	**サーバの復旧対策検討開始(様式13)	<ul style="list-style-type: none"> ● ベンダとの連絡状況を記述できるようにする必要がある(様式13)
11:19	情報システム部門責任者に**サーバ復旧対策報告	
11:21	情報システム部門責任者に**サーバ復旧対策報告完了	

効率的な手順を追求し、1分でも早く

システム単位の調査には約30分を要した
→今後のベンチマークに

事前準備と普段のIT資産管理の徹底が必要



事例1 模範解答サンプル

- 被災シナリオに基づいて、想定されるチェックシート記入例を作成。

様式7 被害チェックシート 被害版

2012年11月14日(水) 10:00 時点

被災状況 (企業概要 部情報シ ステム担当)	死者	0	就業時間内は点呼で、時間外は電話等 を使用して確認する。 就業時間内の場合は来客、外部要員及 び帰宅・休職要員の状況も合わせて確 認すること。 死者、行方不明者、負傷者に該当者が いる場合は、氏名も記録すること。
	行方不明者	0	
	負傷者	0	
	ICT部門の参加者(出勤者)	5	
	参加可能との連絡があったもの	1	
ライフライン (庁舎へ の供給)	電気	あり/なし	災害対策本部又は防災安全課が把握し ている情報を確認する(自ら確認して も良い)。
	ガス	あり/なし	
	水道	あり/なし	
庁舎	庁舎(入居可能か否か)	あり/なし	災害対策本部又は防災安全課が把握し ている情報を確認する。
	企画制作部情報システム担当機室	あり/なし	
	電算室	あり/なし	
	電源設備	あり/なし	
	空調設備	あり/なし	
	通信設備	あり/なし	
指定避難所	建物(入居可能か否か)	あり/なし	災害対策本部又は防災安全課が把握し ている情報を確認する。
	ホスト、サーバ設備等	あり/なし	
	ネットワーク	あり/なし	
	磁気媒体(電算室内)	あり/なし	
	磁気媒体(耐火金庫内)	あり/なし	
システム稼 働状況	情報システム 様式1:情報システム一覧で実施	あり/なし	システム又はサーバ単位に損害状況を 調査する。 ・電源がONになっているか ・異常ランプが点灯していないか ・コンソールに異常メッセージが 出力されていないか ・端末から接続可能か ・消火、臭気がないか ・外観からわかる破損がないか
	外部、避難所等の端末のネットワー ク	あり/なし	
特記事項	**サーバインバーランプ点灯。 インターネットサーバランプ消灯。		

様式13 復旧対策シート

報告

日時 2012年11月14日(水) 11:00 時点

記入者

システム名 **システム

優先度と
復旧見込

第一次復旧システム(～24時間)
 第二次復旧システム(～72時間)
 第三次復旧システム

復旧見込 1週間以内

復旧方針

場所: 庁舎内で復旧 庁舎外で復旧
 確認: 既存設備利用 設備手配により復旧
 情報: 災害による停止時点 バックアップからデータ復旧

復旧計画		～24時間	～72時間	～1週間
	ハード	待期系手配	待期系手配	運用系使用
	ソフト	/	/	/
	ネット ワーク	/	/	/

特記事項

運用系HDDに物理障害発生。
FTRのための待期系に切り替わり運用
通り運用。修理は1週間以内には対応可能。

報告に対する回答

日時 20 年 月 日 () :

記入者

指示事項

事例1 アンケートサンプル

- 理解度・妥当性を5段階で評価し、具体的に良かった点・改善すべき点を挙げていく形式。

***** ICT-BCP 訓練 2012.11.7

ICT-BCP 訓練 事後アンケート

この度は皆様ご多忙の中、ICT-BCP 訓練に長時間ご協力頂き、誠にありがとうございます。以下、事後アンケートとして、今回の訓練を通して、上手くいったこと、よく理解できなかったこと、その他気付かれたことなどについて具体的にご回答下さい。今回のICT-BCPの改善やその他の施策による業務継続性の向上への参考とさせていただきます。忌憚のないご意見をお寄せ下さい。

1. ご名前： _____

2. ご所属： _____

3. ご参加した訓練：①対応確認訓練 ②災害時に実施訓練 ③被害状況調査訓練
※該当するものにチェックを入れて下さい。

ご参加した訓練の理解度について、以下から該当するものを選択して下さい。また、よく理解できたが、分かりにくかった点を具体的に記述して下さい。

5: 十分理解できた
4: 概ね理解できた
3: どちらとも言えない
2: あまり理解できなかった
1: ほとんど理解できなかった

よく理解できた点： _____ 分かりにくかった点： _____

***** ICT-BCP 訓練 2012.11.7

ICT-BCP の活動中継の英語版について、以下から該当するものを選択して下さい。また、うまくいったが、気付いた改善点を具体的に記述して下さい。

5: 非常に適切な内容
4: 概ね適切な内容
3: どちらとも言えない
2: 改善すべき点が多い
1: 抜本的な見直しが必要

うまくいった点： _____ 改善すべき点： _____

事後準備や当日の運営などを含め、訓練の場の方についてお気づきの点がございましたら、具体的に記述して下さい。

訓練の場の方： **訓練運営方法についての提言**

その他に気付かれたこと、感想などご自由にご記入して下さい。

感想など： **その他**

ご協力ありがとうございました。

*** & NEC Corporation Confidential 2012.

- 【理解度】:**
- 5 十分理解できた
 - 4 概ね理解できた
 - 3 どちらとも言えない
 - 2 あまり理解できなかった
 - 1 ほとんど理解できなかった

- 【妥当性】:**
- 5 非常に適切な内容
 - 4 概ね適切な内容
 - 3 どちらとも言えない
 - 2 改善すべき点が多い
 - 1 抜本的な見直しが必要

Empowered by Innovation

NEC