Mission\_4.7\_App.01 IT-BCPの必要性と策定・運用のポイント【未定稿】

# 組織としての「事業継続計画」（BCP)の中で、セキュリティ侵害による被害を最小限にする対応も含めて明確にすることが重要です

## 事業継続計画（BCP）の一環としてのサイバーセキュリティ対策（明文化）

### ITサービスの継続

* + - * 緊急事態
      * ハードウェア障害、ソフトウェア障害
      * 情報セキュリティ「可用性」の確保
      * 情報セキュリティ「機密性」「完全性」の確保

## DXに対応しないためのリスク

## DXに対応したためのリスク

# 情報漏えい、長期のサービス停止は、信用失墜の可能性

## ITを活用してどんなに利便性の高いサービスを提供しても、どんなに業務を効率化しても、緊急事態（自然災害、大火災、感染症、テロ、サイバー攻撃など）、システムの不具合、セキュリティ侵害等で事業資産や社会的信用が失われ、早期復旧ができない場合は、事業の継続が困難になり、組織の存立さえも脅かされる可能性があります。

# 「想定外」にならないようにあらゆるケースを想定して（事前だけでなく事後の対策も合わせて網羅的な対処方法を策定）

## 事前だけでなく事後の「緊急時対応」も含めた一連の対応として、 フェーズごとの対策

### 特定

### 防御

### 検知

### 対応

### 復旧

## 緊急時対応手順の策定と体制整備

### インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、 復旧に向けた手順書策定や、復旧対応体制の整備をさせる。

## BCPとの整合

### BCPとの連携等、組織全体として整合のとれた復旧目標計画を定めさせる。

# 必ず演習を。（絵に書いた餅にしないように）

## また、業務停止等からの復旧対応について、適宜実践的な演習を実施させる。

## ・重要な業務が適切な時間内に復旧できず、 企業経営に致命的な影響を与える恐れがある。

## ・演習を実施していないと、不測の事態が起こった際に、 担当者が緊急時に適切に行動することが出来ない。

# IT-BCP策定モデル

## NISC

<https://www.nisc.go.jp/active/general/pdf/IT-BCP.pdf>;

## IT-BCPの課題

### (1) 非常時の意思決定に関 する在り方

* + - * 【部門間の連携】

### (2) 非常時の情報収集・伝 達・発信や業務系の情報 システムの在り方

* + - * 【危機的事象の特定】

### (3) データの消失を回避す るための対策の在り方

* + - * 【バックアップデータの保管】

### (4) 教育・訓練の在り方

* + - * 【平常時の運用】

## 「IT-BCP 策定モデルにおける策定ステップ」の概要

### STEP1 環境整備

* + - * 基本方針を決定し、実施・運用体制を構築する。

### STEP2 情報の収集・前提の整理

* + - * 危機的事象を特定し、特定した事象の顕在化がもたらす被害状況を想定する。

### STEP3 分析、課題の抽出

* + - * 情報システムの復旧優先度を設定し、運用継続に必要なリソースを整理する。

### STEP4 計画の策定

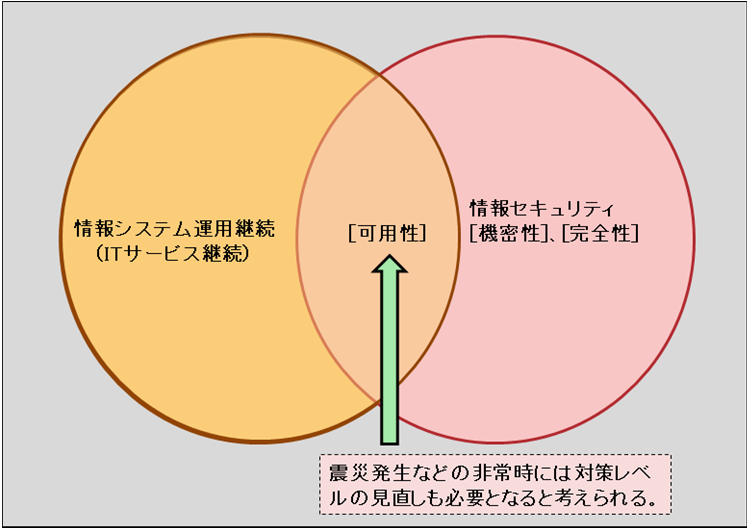
* + - * 事前対策計画、非常時の対応計画、教育訓練計画・維持改善計画を検討する。

### STEP5 実施（評価・改善）

* + - * 平常時にIT-BCPが発動されることはないため、定期的な訓練を通じて組織・個人における習熟度を維持し、計画に問題があれば見直しを図る。

### ※IT-BCPの策定には「情報システム部門」と「業務部門」等の関連部門間で適切な連携を図り、既存のBCPとの整合性を確保することが大切です

### 「IT サービス継続ガイドライン 改訂版」（経済産業省）の図を基に作成



## 「IT-BCP 策定モデルにおける策定ステップ」の詳細説明

### STEP1 環境整備

* + - * 情報システム部門で、IT-BCP 策定の方向性を検討する。
      * IT-BCP の策定に必要な体制を整備する。
      * IT-BCP の基本方針について関係者間で合意する。
      * IT-BCP の対象範囲について関係者間で合意する。

### STEP2 情報の収集・前提の整理

* + - * 危機的事象を特定する。
      * 危機的事象の顕在化がもたらす被災状況を想定する。

### STEP3 分析、課題の抽出

* + - * 業務部門と合意した対象範囲の組織や非常時優先業務、情報システム等のたな卸を行う。
      * 対象業務の目標復旧時間（以下、「業務RTO1」とする。）を明らかにする。
      * 情報システムを支える構成要素（リソース）を洗い出す。
      * 構成要素ごとに目標対策レベルを設定し、それに基づく情報システムの復旧優先度を設定する。

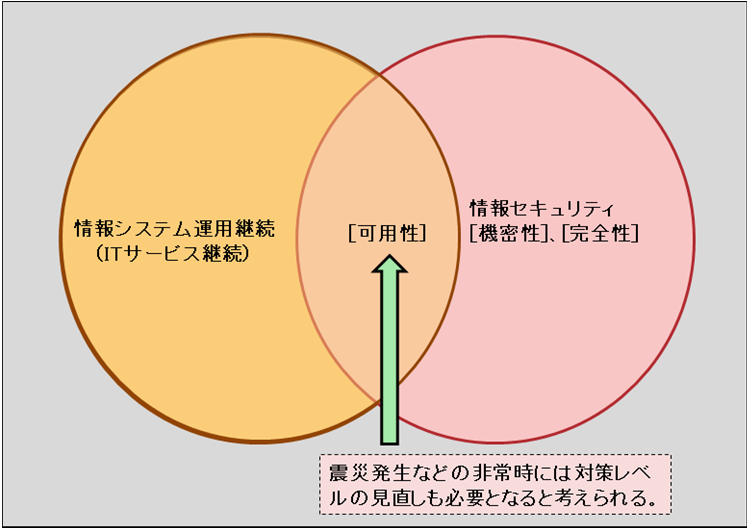
### STEP4 計画の策定

* + - * 【事前対策計画の策定】
      * 危機的事象の発生時に情報システムに生じる被害状況の想定に対する情報システムの抱える脆弱性（情報システムの運用継続を阻害する課題）を把握する。
      * 把握した現状の脆弱性を解消する対策（事前対策）を、システムごとに検討する。
      * 検討した事前対策により、目標対策レベルとシステム環境の現状のギャップを解消し、運用継続能力を継続的に強化していく実施計画を策定する。
      * 【非常時対応計画の策定】
      * 府省庁の防災対策等と非常時に連携する情報システムの復旧継続活動に必要な対応体制を構築する。
      * 非常時の初動から復旧までの大まかな流れを決めるために、全拠点における危機的事象の発生から復旧までの対応が示された「対応の全体フロー」を作成する。
      * 非常時の体制で定めた担当が、それぞれどのような対応するかをより明確にした、非常時における「対応手順書」を作成する。
      * 【教育・訓練計画の策定】
      * 教育・訓練計画は、担当者の理解度や対応力を向上させるとともに、事前対策の改善つなげることを意識して策定することが望ましい。計画は、年度単位で策定するとよい（雛形 「4.1.教育訓練計画」の例を参照のこと）。
      * 教育・訓練は、それぞれの対象者に適切な内容・時期で実施することで、その効果を高めることができると考えられる。以下に、体系的な訓練の実施パターンを例示する。
      * 非常時には様々な対応が求められるので、全ての必要事項を一度の訓練で扱うと十分な成果を得ることが難しくなると考えられる。継続的に、府省庁の実力（理解度、対策の進捗状況等）を勘案し危機的事象・情報システム・非常時の対応等のうち優先順位の高いものから段階的に取り組み、徐々に難易度を高めていく、計画時に配慮することが望ましい。
      * 【維持改善計画の策定】
      * 維持改善計画は、事前対策計画、非常時対応計画、教育訓練計画それぞれを定期的に見直し、情報システム運用継続計画の実行性を継続的に維持できるよう検討する。維持改善計画を着実に実施して、定期的に全体を確認できるようにすることが重要である。

### STEP5 実施（評価・改善）

* + - * 運用段階においては、策定された事前対策計画と教育訓練計画に則り、対策実施や教育訓練等の活動を行うことで、業務継続能力の強化を推進する。また、「維持改善計画」に基づいて、適宜各種計画の見直しを行い、計画の陳腐化を防ぎ、常に計画の最新化を維持するように努める。
      * 計画の見直し時には、関連部局や組織のレビュを必要に応じて受けるべきである。（防災、情報セキュリティ等の推進部門に、それぞれの分野の観点から指摘を受けることは有効である。）

### 「IT サービス継続ガイドライン 改訂版」（経済産業省）の図を基に作成



# 参考情報

## NIST SP 800-34

## NIST SP 800-53

## IT-BCP 策定モデル（NISC）

## サイバーセキュリティ経営ガイドライン

### 指示８ インシデントによる被害に備えた復旧体制の整備

## 5分でできる！情報セキュリティ自社診断

### №24 BCPを踏まえたセキュリティ事故対策

* + - * 24.秘密情報の漏えいや紛失、 盗難があった場合の対応手順書を作成するなどのように、 事故が発生した場合に備えた準備をしていますか？