ISMS
事業継続計画講座

ISO27001
ISMSの基礎知識

事業継続計画とは？

事業継続計画とは、ISMS及びITSMSにおいて実現が要求されている管理策であり、
「事業の継続におけるリスクが発生した際に、それでも事業を継続できるような体制を整えること」
を求めた管理策です。
大きなポイントとしては、リスクアセスメントと同様に、まずはリスクありきで、そのリスクに対して発生してしまった場合の対応を検討するという流れがリスクアセスメントとは少々異なっています。

A14

- 事業継続計画

リスクアセスメント

◆ 事業継続リスクのアセスメント

前述の通り、対象となるリスクは、事業継続上問題のあるリスクが対象となります。
しかし、リスクアセスメントと異なり、明確にプロセスアプローチが求められているわけではなく、事業の継続に問題のありうるリスクをある程度総当たりで検討していく必要があります。

事業継続に影響あるリスクの例）

- 災害
- システム障害
- 情報漏えい等のセキュリティ事故
- 疫病などの人員リスク
- 風評被害
- 契約上の紛争

・・・ など

リスク評価と対応の検討

- 優先順位の付け方

優先順位は通常のリスク評価と変わらず、

脅威の大きさ×発生可能性＝リスク値

となります。

ただし、発生可能性については、通常のリスクと同様に評価したのでは、ほとんど発生しないと想定されるものばかりになってしまうため、起こり得ないもの以外をなるべく残すようにすることが必要です。

さらに、脅威の大きさは、発生した場合の経営上の影響を考慮したうえで評価することが望ましいと考えられます。

事業継続計画策定　その1

◆ 事業継続計画とは

事業継続計画は、大きく分けて次の計画で成立するようになっています。

- 事業継続計画（リスクアセスメントを含む、対応の優先順位を特定した計画）
- 復旧計画（リスク発生時の対応について規程した計画）

復旧計画は後述しますので、事業継続計画について本章では解説します。

事業継続計画には次の内容を含める必要があります。

- リスク評価結果
- リスク評価結果に対応の優先順位
- 対応の要否及び今後の対応

事業継続計画策定　その2

◆ 事業継続計画の作成例

事業継続対象リスク	評価結果	今後の対応
メールサーバの停止	メールサーバそのものの停止の可能性はあるが、復旧は半日程度で可能であり、また、今後メールサーバの移行を検討中であり、移行後安定性を高めるため、リスクの発生可能性は低くなると想定される。	今年度は特に対応なし。 来年度以降、移行後に再度リスクについては検討するものとする。
サイボウズ停止	サイボウズは安定性が低いものの、業務に大きな影響を及ぼすような情報を現状使用しておらず、万一停止した場合のリスクも少ないと想定される。 また、サイボウズ自体のシステムを見直し中であり、今後移行を検討しているため、移行後は安定性が高まり、リスクの発生可能性は低くなると想定される。	今年度は特に対応なし。 来年度以降、移行後に再度リスクについては検討するものとする。
電話回線の停止	データセンタにおいては回線が多重化されている上、赤坂では緊急性の要する要件を電話にて扱っていない。 また、非常時には携帯電話の使用で対応できるため、電話回線が停止した場合も特に復旧などへの問題は発生しないものと想定される。	今年度は特になし。 赤坂内に緊急性のある電話を使用する業務が追加された場合には再度検討する。
インターネットの停止	データセンタにおいては回線が多重化されている上、赤坂では緊急性の要する要件をインターネット、メールにて扱っていない。	今年度は特になし。 赤坂内に緊急性のあるインターネット、メールを使用する業務が追加された場合には再度検討する。

復旧計画策定

復旧計画とは

復旧計画とは、事業継続に影響のあるリスクが発生した場合に、復旧するための計画を指します。
復旧計画には、次の内容を含めることが求められます。

- 復旧目標時間（停止等許容時間）
- 復旧手順
- 対応のために必要な資源
- 役割責任の分担

特に、復旧手順については次項のような手順が求められます。

復旧手順

一時対応

- 発生時の対応をまとめる
- 発生時に被害を少なくするための手順を策定
- また、連絡先などの対応も含める

代替手順

- 問題が発生している中、事業を継続するための代替手順
- 問題の対応及び、問題が発生している中の対応手順を含める

復旧手順

- 代替手順から、元にもどすための対応手順
- 元に戻す場合に別の資源などを使用することもある

事業継続計画の試験

◆ 事業継続計画の試験項目

事業継続計画の試験については、次のことを確認することが必要です。

- 実現可能性
- 対応手順における、手順の整合性確認

その際に試験する方法としては、次の方法があります。

- 机上試験
- 実地試験

可能な限り実地試験が望まれますが、対応することによりサービスの停止などのリスクが発生するものについては、机上試験を行うことでも要求は満たされます。

また、試験結果は記録が求められるので、試験結果として、

- 試験内容
- 試験結果
- 問題ごとがあった場合の今後の対応計画

を残す必要があります。

試験のポイント

チェックポイント	OK	NG	NGの場合対応処置
対応計画は、コスト的に妥当か		○	マスコミ、新聞などへの対応は本件では不要と考えられるため手順から削除。
対応計画は、必要な手順を含んでいるか		○	損害保険会社への連絡手順が不足しているため手順に追加
対応計画は、確実に復旧などの対応が出来る手順となっているか	○		
対応計画の手順に問題はないか		○	対応フェーズが発生時となっているが、発見時としないと対応時間が不明確になるため、手順を修正
対応計画は実現可能か	○		
対応計画の実施に必要な追加資源はないか		○	対応の経過と結果については最終的に決済をすることで記録を残すことが必要なため、手順に追加。
対応計画に含まれる連絡体制は整っているか		○	連絡先は、部門長、品質委員会、社長、お客様の担当者という表現に変更。
対応計画の実施に必要な役割責任は割り当てられているか	○		
対応計画の実施において、今後発生しうる問題はあるか	○		

事業継続計画の更新

再試験の実施

過去に対応した事業継続計画については、再試験を実施することで手順の整合性を確認する必要があります。

再試験の方法については、通常の試験と同様に、

- 机上試験
- 実地試験

のいずれかを選択することが許されます。

また、再試験については、毎年実施しなければならないわけではなく、事業継続計画の中において、対応を決定することが必要となります。