ISMS
リスクアセスメント講座

ISO27001
ISMSの基礎知識

合同会社Double Face

ISMSを理解する

- ## ISMSとは？

情報セキュリティ管理を行うための仕組みのこと（情報セキュリティマネジメントシステム）です。
ISO27001に準じて構築することで、外部審査を受審し、確実なセキュリティ管理が行われていることを外部から認証される制度となっています。

- ## ISMSの概要

ISMSは、基本となるPDCAサイクルを情報セキュリティに準拠させることで成り立ちます。
Plan　：　情報セキュリティ基本方針、情報資産洗い出し、リスクアセスメント
Do　　：　リスク対応実施
Check：　内部監査、マネジメントレビュー
Act　　：　改善実施
上記のサイクルを一年の活動を通して実施していくのがISMSの基本です。

- ## ISMSの構築

ISMSの構築作業とは、審査にいたるまでの期間にPDCAサイクルをすべて運営することで実現されます。
本手順書では、構築のステップを6段階に分けて解説します。

リスクアセスメントのステップ

Step1

1. 情報資産を取り扱うプロセスを洗い出す。
2. プロセスに起こりうる問題を洗い出す。
3. 問題に対応するために実現していることを洗い出す。
4. 問題が発生した場合の影響度合いを明確にする。
5. 問題の発生可能性を明確にする。
6. リスクの大きさを明確にする。

Step2

1. リスクの大きいものから、対応策を検討する。
2. 対応するための計画を立てる。
3. リスク対応計画の承認を受ける。
4. 適用宣言書を作る。
5. 対応計画の中で文書化が必要な項目を明確にする。
6. 対応計画の中で実作業が必要な項目を実施する。

Step1　リスクを特定し、大きさを評価する。

1. 資産を取り扱うプロセスを明確にする

◆ 資産を取り扱うプロセスとは？

資産には、業務として必要とされる以上何かしら取り扱うためのプロセスがあります。
プロセスには、次のような分類があり、それぞれのプロセスごとに脅威が起こりえます。

資産の種類	主要プロセス
情報（紙）	入手
	記入
	配布
	コピー
	保管
	ファイリング
	廃棄
	外部持ち出し
	FAX
	郵送
情報（データ）	入手
	修正
	作成
	メール
	保管
	共有
	削除
	コピー
	閲覧

2. 起こりうる脅威を明確にする

- 脅威とは

情報に、何かしら問題のある影響を与えうる事象を脅威といいます。
資産にプロセスが発生すると、何かしらの脅威がその裏にはあると考えられます。

例

保管	→	盗難・紛失
メール	→	誤送信・メールサーバー停止
HP公開	→	不正アクセス・HP停止
入力	→	入力ミス

- ポイント

情報に、起こりえる可能性のある脅威を当てはめることが重要です。
まず起こりえないリスクを当てはめても意味がないので、たとえば、盗難しても価値がないような情報には、盗難の可能性よりも紛失の可能性の方がありうる、といった具合に当てはめていきましょう。

3. 脅威による影響を明確にする

- ## 脅威と影響の関係

脅威とは、影響を起こしうる事象であると前項でご説明いたしましたが、影響は資産そのものに直接作用する影響のことをさします。

例

盗難	→	漏洩　（機密性）
誤送信	→	漏洩　（機密性）
メールサーバー停止	→	使用不可（可用性）
不正アクセス	→	漏洩（機密性）改ざん（完全性）
入力ミス	→	改ざん（可用性）

- ## ポイント

脅威による影響は、情報によって異なります。必ずしも盗難による漏洩が怖いとは限らず、場合によっては盗難することで使用できなくなることが問題になることもありますし、不正アクセスをされたからといって、必ずしも情報の漏洩が怖いわけでもなく、改ざんされるほうが怖い可能性もあります。

影響は、その情報に対して問題になる影響を当てはめることが重要です。

- ## 脅威に対して現状実施している対策を明確にする

脅威に対して、すでに実施済みの対策があればその対策内容を明確にします。もちろん、対策が十分に出来ていればそれ以上の対策は必要ないことになります。

4. リスクの発生可能性を明確にする

- ## リスクの発生可能性とは

脅威そのものが起こり、実際に企業に影響を与えてしまう可能性は、それぞれの事象によって異なってきます。
それらの可能性には、次のものの関連性により異なります。
・脅威そのものの発生可能性
・現状の対策度合い

- ## 脅威そのものの発生可能性とは

脅威そのものが発生する可能性には、その脅威の元となるプロセスが、頻繁に起こるものか、よく発生しうるものなのか、過去に発生したことがあるのか、などが発生可能性を評価する指標になります。

- ## 現状の対策度合いとは

現状の対策が出来ていると判断するのは企業判断です。現状に問題があると考えるのか、まったく問題がないと考えるのかを検討する必要があります。
特に、この対策度合いの確認はセキュリティの専門家や、コンサルタントにご確認いただくことが望ましいでしょう。

5. リスクの大きさを特定する

リスクの大きさとは

リスクの大きさは、影響の大きさと、発生可能性の高さで判定します。
影響が大きく、発生可能性の高いものは、リスクが大きく
影響が大きいが、発生可能性の低いものはリスクが中程度
影響が小さく、発生可能性が高いものは、リスクが中程度
影響も小さく、発生可能性も低いものは、リスクが小さい
これらが、簡易的なリスクの大きさの評価になります。
このリスクの判定を行ったら、リスク評価は終了です。

例

脅威	発生可能性	リスク値	リスク対応方針	リスク対応の指針
3	3	9	最優先	脅威が極めて高く、また、発生可能性もきわめて高いため、最優先での対応が必要
3	2	6	対策すべき	脅威は高いが、発生可能性は中程度のため、対策が必要である。
2	3	6	対策すべき	脅威は中程度であるが、発生可能性は高いため、対策が必要である。
2	2	4	要検討	脅威、発生可能性ともに中程度のため、コストに見合えば対策が必要である。
3	1	3	許容	
1	3	3	許容	
2	1	2	許容	脅威、または発生可能性がほとんどないため、特に対策を要しない。
1	2	2	許容	
1	1	1	許容	

Step2　リスクに対する対応策を検討する。

1. 対応策を検討する

◆ 対応策の考え方

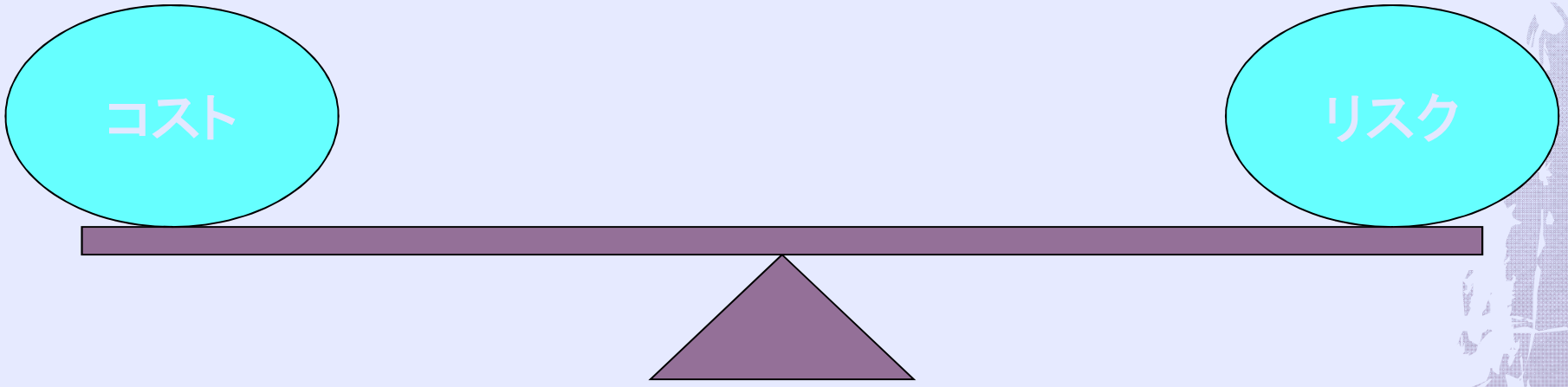
リスクに対する対応策の考え方で、まず必要となるのは対応するのか、しないのか、ということです。

その際に、情報セキュリティ基本方針が重要になってきます。

つまりは、**「情報セキュリティ基本方針で、リスク対応が必要だと定義しているリスクには積極的に対応が必要である」**ということです。

次に、対応が必要と判断された場合は、優先的に対応すべきなのかどうかが焦点となります。

もちろん、対応を優先すべきなのはリスクが高いものであるべきですが、リスク対応の優先順位を判断する際には、それだけではなく**「リスク対応にかかるコストが妥当なものであるか」**というものが判断に加わります。



2. 適用宣言書とは？

- 適用宣言書

ISMSにおいては、

要求事項という、実現必須の項目と

詳細管理策という、実施任意の項目

があります。

特に、詳細管理策は、リスクアセスメントの結果から必要なものを選択することになっており、
この結果がその組織におけるリスク対策の現状を示すものとなります。
そのため、適用宣言書はISMS取得企業に対して、実現状況を確認されることが多い文書です。
特に誤解の多い部分ですが、詳細管理策はすべての実現を求められているわけではありません。

3. 適用宣言書作成の流れ

◆ リスクアセスメントの結果

前回までで解説させていただいた、リスクアセスメントの結果から、対策が必要なものをまずは詳細管理策の中から選択します。

たとえば、従業員の不正持ち出しによる盗難リスクなどに対応する際には、

機密保持制約　＋　アクセス制御　＋　施設の出入り管理

などの対策を必要に応じて実現します。

◆ 過去に実施している対策

すでに実現しているリスク対策もあるはずですが、それらの内容は必ずしもリスクアセスメントの結果とは直接リンクしないこともあります。

それらのものについては、すでに実施している対策と、今回のリスク対策それぞれで登場したものは明確に区分けをしておきましょう。

また、その際に、その対策が本来何を防止するためだったのか明確にします。

何のために実施しているのかわからない対策は、過剰な対策である可能性があると判断されるわけです。

リスク対策との関連性


今回のリスク対策
既存のリスク対策
詳細管理策
133項目
リスク対策結果との
関連性
過去にリスク対策を
実施した目的

4. 適用・除外の理由

なぜ理由が必要なのか？

適用の理由及び適用除外の理由を適用宣言書には記載しなければなりません。
これは、のちに適用内容などを見直したり、セキュリティ管理策を変更する際に、
・そもそも何の目的で導入したのか？
・なぜこの管理策を外してもよいと判断したのか？
ということがわからなければ、妥当性のある見直しが出来ないためです。

理由の例

では、適用の理由とはどのような理由でしょうか。
これは、ストレートに言うならば、どのようなリスクに対応することを目的にしているのか、ということです。
例）入退室管理適用　→　部外者の侵入を防ぐため
適用除外の理由は、なぜ管理策を外してもよいと判断したか、ですが、理由は次のようなものが必要です。
例）該当する業務、プロセス、システムがないため
　導入することにより～のリスクが発生してしまうため
　導入するコスト等にメリットがないため
などです。重要なことは、導入することに本当に意味があるのか、ということです。

適用宣言書の作成例

大項目	中項目	小項目	適用	適用理由/適用除外理由	管理策の内容	対応文書
	管理目的及び管理策					
A.6	情報セキュリティのための組織					
	A.6.1	内部組織				
		A.6.1.1 情報セキュリティに対する経営陣の責任				
		A.6.1.2 情報セキュリティの調整				
		A.6.1.3 情報セキュリティ責任の割当て				
		A.6.1.4 情報処理設備の認可プロセス				
		A.6.1.5 秘密保持契約				
		A.6.1.6 関係当局との連絡				
		A.6.1.7 専門組織との連絡				
		A.6.1.8 情報セキュリティの独立したレビュー				
	A.6.2	外部組織				
		A.6.2.1 外部組織に関係したリスクの識別				
		A.6.2.2 顧客対応におけるセキュリティ				
		A.6.2.3 第三者との契約におけるセキュリティ				

適用宣言書の書式などに特に指定はありませんが、
適用の有無、適用理由及び適用除外の条件が必須項目です。
また、すでに実施している管理策と、リスクアセスメントで導入した管理策は両方とも記載が必要です。

5. お勧めの作成項目

◆ 適用宣言書の項目

適用宣言書の必須項目以外には、具体的な適用内容を記載しておくことをお勧めします。

適用内容が記載されていれば、現在の状況がわかりやすくなりますし、どうしても1年も経った後に見直しをしようとすると、忘れてしまうというリスクを回避できるためです。

また、関連する文書などが発生している場合は、その文書も適用宣言書内に書いておけば、見直しが必要となったときにその文書もあわせて見直しができるようになります。

◆ 書き方のススメ

適用宣言書の書き方にももちろん決まりはありませんが、適用項目については、既存管理策と新規導入の管理策を分けるなどしておくと、セキュリティの変遷が分かるため、明確化しておくことをお勧めいたします。

また、適用理由などはできる限り詳細に、たとえば、単に

外部からの侵入を防ぐため

等ではなく、

外部からの第三者の不正侵入による盗難を防ぐため

等と記載しておけば、侵入を防ぐ対策をすべきなのか、それとも盗難を防ぐ対策をすべきなのかでやることが変わってきます。

6. リスク対応計画の策定

◆ リスク対応計画とは

リスクについては何でもすべて今年度中に解決しなければならないわけではありません。
リスク対応は必要に応じて、
・長期的に対応を検討しなければならないもの
・短期間で解決しなければならないもの
に切り分けることが必要となります。
そのためにも、前回のリスクアセスメントの結果によるリスク評価が大きな分かれ目になります。
つまり、リスクレベルが高いもの＝優先度合いが高いもの
ということになります。