10 分で解かるＩＳＭＳの基本

鈴木　淑雄

ＩＳＭＳとは

例えば、製薬会社が新しい薬品を開発したとします。その薬品の構造や今までの試験データが盗難にあってしまったとしますとその製薬会社の損害は大きく今後の経営にも大きく影響を与えます。又、大手百貨店の外商部の顧客情報の流出なんかも経営にダメージを与えるでしょう。

この様に情報が盗難にあったり、紛失したり、流出したり、破損したりすると会社の経営にダメージを与えます。そんなダメージを軽減しようとするのがＩＳＭＳなんです。

すなわち、ＩＳＭＳとは情報セキュリティマネイジメントシステムと言い、「会社が持っている資産、特に情報に関連しているものの安全性を確保するためにその確保するシステムを作成・運用しなければなりませんよ。」と言うことなんです。（まあ、大なり小なりの差はあってもどの会社でもセキュリティは行っていると思いますが）

もうちょっと付け加えますと、情報セキュリティとは情報の機密性・完全性・可用性を維持することでこの 3 つは情報の 3 要素とか情報のＣ・Ｉ・Ａなんて呼んでます。

ＩＳＭＳの仲間

ＩＳＯ9000 シリーズの品質管理マネジメントシステム。ＩＳＯ14000 シリーズの環境マネジメントシステムが仲間です。因みにＩＳＭＳはＩＳＯの 27000 シリーズです。（ＪＩＳに対応してます。）

よって、今までに品質管理マネジメントや環境マネジメントに携わったことのある会社はＩＳＭＳも理解しやすいかと思います。

会社の情報資産とは

ＩＳＭＳは会社の情報資産を保護するために構築するものですから、資産をきちんと把握しておかなければなりません。

資産というとすぐにお金に関することを想像しますが、ここで扱う資産は各種情報に関するものであり、それは大きく分けますと　①情報　②ソフトウェア　③物理的資産　④サービスとなります。

どんなものが資産かといいますと

ざっと挙げますと

①　情報資産

データベース／データファイル（顧客情報・従業員情報・下請け等関連企業の情報）

システム設計書等のシステム開発用文書

契約書及び同意書

利用者マニュアル／操作マニュアル

訓練用資料

その他・各種文書／記録（会社の各種マニュアル・経営方針・就業規則関連・会社の組織図・会議議事録・各種決算書）

②　ソフトウェア資産

業務用ソフトウェア

システムソフトウェア
開発用ツール／ユーティリティー

③　物理的資産

コンピューター装置（プロセッサ、入力装置、表示装置、印刷装置、パソコン）
通信装置（モデム、ルータ、ＰＢＸ、電話（携帯も含む）、ファクス）
取り外し可能な媒体（テープ、ＦＤ、ハードディスク、ＣＤ、ＤＶＤ）
その他（無停電電源装置、空調設備、収納設備、）

④　サービス

通信サービス
輸送／配送サービス
一般ユーティリティ（照明、電源、冷暖房、空調）

などから、机とか筆記用具なども資産に入ります。
（全て書き出したら結構なページになります。しかし、ＩＳＭＳの認定を取得する場合はその作業を行わなければなりませんが）

資産を守る為のＩＳＭＳ

それじゃ、「資産を守る為にはどのようにＩＳＭＳを展開して行くか。」と言うことになります。
（手順はありますが、一番大切なのは会社のトップがやって行こうと言う意思があるかどうかだと思います。トップがやる気がないのにＩＳＭＳを構築しようとしても上手くは行かないでしょう。）
手順としましては、下記の 4 つの項目を回して（サイクル）行くことなんです。

Ⅰ　計画を立てる（Ｐｌａｎ）
Ⅱ　実行する（Ｄｏ）
Ⅲ　監視及びレビューを行う（Ｃｈｅｃｋ）
Ⅳ　維持及び改善をする（Ａｃｔ）

4 つの項目の頭文字を採って**ＰＤＣＡサイクル**なんて呼んでます。これは通常の仕事の中や他のマネジメントシステムでの良く出てくるもので仕事をしていく場合の基礎だと思います。
この 4 つの項目をもう少し詳しく説明しますと

Ⅰ　計画を立てる（Ｐｌａｎ）

1、ＩＳＭＳを理解する。
ＩＳＭＳがどのような仕組みになっているか。その重要性を良く知っておかなければＩＳＭＳを展開して行くことはできません。
2、ＩＳＭＳを行う目的を明確にする。
なんの為に行うか。そのメリットとデメリットをきちんと把握しておく。
3、リスクアセスメントを行う。
4、リスクを特定する。
5、リスクを分析・評価する方法を作成する。
6、リスクに対応する方法を作成する。
7、管理目的・管理策を選択する。
8、残留リスクの承認

9、ＩＳＭＳの実行許可
10、適応宣言書の作成

Ⅱ　実行する（Ｄｏ）

Ｉで立てた計画に沿って情報の保護を行う。

せっかく立派な計画書が作成されても、計画書どうりにシステムが動かなければ意味がありません。（実際に運用していくのは、社員なのですからここでは社員教育の重要性を再認識しておくべきです。）

Ⅲ　監視及びレビューを行う（Ｃｈｅｃｋ）

ＩＳＭＳが計画に沿ってきちんと実行されているか？成果は上がっているか？等評価を行う必要があります。もし、上手に運用されていないのであれば、その原因を調べる必要があります。

そして、この評価を経営トップに報告します。

Ⅳ　維持及び改善をする（Ａｃｔ）

ＩＳＭＳがきちんと機能しているのであれば、今後もその状態が続くように努力します。1 回レビューを行っただけで「ああ、成果が出ているから大丈夫。」だと判断して監視・レビューを行いませんとすぐにシステムは上手に回らなくなります。

世の中は常に変化しますので、その変化に対応した維持というのが必要なのです。

レビューを行いますと、やはり計画とのヅレがでてきますし、不都合も見つかります。

それをそのままにしておいてはなんの為のＩＳＭＳだか解からなくなりますので、ヅレや不都合に対して対策を立てる必要が出てきます。改善するんですね。

そして、その改善策を基に再計画を立て、実行し、レビューし、維持・改善し、とサイクルを回してよりよいＩＳＭＳを運用していくんです。

すべてのリスクに対応する必要はあるのか？

リスクと言うものを考えますと、大地震のような大きなリスクから迷惑メールみたいな小さなリスクまで多種多様です。（リスクの大小は個々によって異なりますが。）

そうなんです。考えられるリスクに対してすべて対応していたら莫大な経費が掛かってしまい、その経費のせいで会社が傾いてしまったとしたらこれはもう本末転倒です。

そうならないようにするためにリスク値を求めるんです。リスク値なんていうとなんかなんか難しそうですが、早い話、大きく会社の経営に響くと考えられるリスクを洗いだし、その対応策の費用を考慮した上でどの程度、ＩＳＭＳに反映させるかを判断します。（リスク値の分析の手法も出回っています。ちょっと難しいですが例を載せときます。）

例：

① 脅威を 3 段階で評価する。
② 脆弱性を 3 段階で評価する。
③ 情報資産価値を 8 段階で評価する。
　※　何段階に評価するかは会社の判断になります。
④ 脅威×脆弱性×情報資産価値＝リスク値を出す

⑤　何点以上の場合対策を行い、それ以下の場合はリスクを受容する。という決まりを決める。
（点数は何点でもよいがあまり小さいとすべてのリスクに対して対策を行わなければならなくなるし、又、大き過ぎますとリスクに対して対策しないなんてことも起こります。）

脅威		1			2			3		
脆弱性		1	2	3	1	2	3	1	2	3
資産価値	1	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27
	4	4	8	12	8	16	24	12	24	36
	5	5	10	15	10	20	30	15	30	45
	6	6	12	18	12	24	36	18	36	54
	7	7	14	21	14	28	42	21	42	63
	8	8	16	24	16	32	48	24	48	72

リスク受容表

リスク値 20 点以上（灰色の部分）の場合対応策を行うとした場合の表

脅威：情報システムや組織に損失や損害をもたらすセキュリティ事故の潜在的な原因。
脆弱性に誘引されて顕在化することにより組織及び組織の業務に影響を与える。
※　脅威の種類も沢山ありまして（自然災害・火事と大きな脅威から停電・ＦＤ等の書き込み不良などの小さな脅威まで考えますと多種多様）これを洗い出すのも一苦労です。
※※　「大地震は来たら被害は甚大だが、来る確立は小さいので脅威は 1 とする」ように脅威は被害の大きさとその頻度とのバランスになります。

脆弱性：脅威発生を誘引する情報資産固有の弱点やセキュリティホールのこと。
※　パソコンは電気がなければ動かない等やセキュリティを考えていない部分が脆弱性となります。
※※　一つの脅威に対しての対応方法から脆弱性を 3 段階に分けて考えます。

上記の例でリスク値を算出するのは結構大変です。
会社の規模にあった算出方法を決めておけばいいので柔軟に対応して下さい。

リスクの受容

リスク値を算出してこれはリスク値が高いから対応しなければならないと決めたとします。
しかし、その対応策を考えたらその費用が会社の経営に影響を与えるほどの金額だとしたらどうでしょう。
そうです、この場合も対応策を行う必要はありません。でもその理由はきちんと表記し、経営者の承認を得る必要があります。同じようにリスク値が低いものも、何故低いかと理由と共に表記して経

営者の承認を得たほうがいいでしょう。

リスクはあるが敢えてそのリスクを受け入れることをリスクの受容といいます。

セキュリティの種類

話が前後してしまうかもしれませんが、（セキュリティの要素からリスクを選択することもできますので）リスクが特定できましたらそのリスクに対して対応して行く訳ですがそれがセキュリティなんです。

では、セキュリティの区分けはどのように考えていくかといいますと、3 つの要素に分けて考えていきます。

1.物理的／環境的セキュリティ

2.人的セキュリティ

3.リーガル・セキュリティ

この 3 つは独立して存在場合や 2 つ、3 つが絡み合っている場合がありますので、事象を良く考えてセキュリティを構築する必要があります。

文章化する。

人間の記憶って結構曖昧なとこがありますので、これはこのようにしようと決めたらそれを文章化しときます。

もし、ＩＳＭＳの認定を受けようとしたらＩＳＯ27000 に書かれている要求事項を網羅しなければなりませんが、（結構な文章の量になります。）でも、そうでなければ最低限の事項を文章化しておけば充分ではないでしょうか。（ＩＳＭＳのそのものの目的がわかればおのずとどこまで当社では必要かと言うことが解かると思います。）

まとめ

情報セキュリティマネジメントシステムとは、情報資産を守り会社を安定して運営していく手段です。

会社の規模によりその実行範囲は異なるかと思いますが、できる範囲で徐々にシステムを構築して行くのが大切だと思います。

※ ここで紹介しましたＩＳＭＳは表題から推測できるかと思いますが、あくまでアウトライン（基本）を紹介したものであることをご了解ください。（本来のＩＳＭＳの規格にはもっと詳細な基準等が記載されています。）