目　　次

７．リスクアセスメント

７．１　リスクの識別

リスク分析の方法は種々ありますが、ここでは詳細分析法の一つの方法を採用しています。手順は以下の通りです。

資産の特定→その資産のセキュリティを脅かすすべての脅威を列挙→この脅威が顕在化した時の損害の内容を機密性、完全性、可用性の面から推定→現時点で採られている対策の評価（不足点、充実点）

まず「情報資産台帳」に記載された情報資産について、機密性、完全性、可用性の面から発生しうるリスクを予測し、「リスクアセスメント結果表（IS-B-02)」に記載します。リスクアセスメントの実施に際しては、下記の点を留意します。

(1) 「情報資産台帳」に記載されている情報資産をさらにグループ化する。グループ化は下記の方法で行う。

① 「情報資産台帳」に記載されている情報資産のうち、保管責任者のみ異なる資産はグループ化する。

例

A 社関連営業資料（保管責任者M社員）

B 社関連営業資料（保管責任者Ｎ社員）→　顧客営業資料

② ①でグループ化した情報資産で、保管場所の属性が共通なものをさらにグループ化する。

例

A 社受注システム開発データ（保管場所開発部サーバ 1）

B 社受注システム開発データ（保管場所開発部サーバ 2）

→　受注システム開発データ

(2) (1)でグループ化した情報資産に対するすべての脅威を洗い出す。脅威は表 1 に示す脅威を考慮する。

(3) 脅威が発生したときの被害を機密性、完全性、可用性の面から推定する。

(4) 脅威の発生に備えて従来から実施している管理策を記述する。

表 1　脅威の事例

人的脅威（内部犯行）	委託先の脅威
データ持出し、漏洩、盗聴、無認可アクセス,	委託先社員の犯行（持出しなど）
データ改ざん、消去、機器破壊	データ紛失、不注意な取扱い
機器・媒体の無断使用	ネットワークからの脅威
人的脅威（外部犯行）	不正侵入によるデータ持出し、データ改ざん、消去
窃盗、機器破壊、データコピー、盗み見	ウィルスによるデータ破壊、漏洩、ネットワーク停止
人的脅威（ミス、能力不足、意識欠如）	踏み台にされて第三者攻撃
機器･ソフトの設定ミス、入力ミス、操作ミス	DOS/DDOS攻撃
紛失、漏洩、ソーシャルエンジニアリング	なりすまし
ウィルス付き媒体、PCの持ち込み	設備・ソフト・ネットワーク障害
ソフトウェアの違法な利用	機器の故障、異常動作、記録媒体異常、ソフトバグ
手順を無視した機器・ソフトの操作、誤用	ネットワーク障害、異常トラフィック
人的脅威（リソースの欠如）	電源変動、温度、湿度環境異常、水・ガス処理異常
キーパソンの退社、病欠	粉塵、ガス、液体などによる環境汚染
ストライキ	災害
	火災、地震、洪水,台風、雷、火山活動

(3) 社内システムの管理

社内システム／ネットワークの運用、アクセス制御、保守、日常監視について「社内システム構築・管理手順（IS-C-03)」に規定する。

(4) 社内システムの利用

個人貸与 PC 及び共通サーバへの利用方法､障害時の対処など利用者として順守するべき事項を「社内システム利用手順（IS-C-04)」に規定する。

(5) 事務室のセキュリティ

事務室への入退室手順、及び間仕切り、受渡し場所など物理的対策、ならびに第三者による当社情報資産へのアクセス対策について､「施設セキュリティ管理手順（IS-C-05)」に規定する。

本マニュアル、手順書類に定める事項に違反した社員に対して、当社の服務規程に定める懲戒規定に則り処罰する。また、IS 管理責任者は当該社員の情報資産に対するアクセス権限の見直しを実施する。

5.2　教育・訓練

5.2.1　要求される力量

ISMS の推進にかかわる社員が持つべき力量を下表に示す。

ISMS の業務	要求される力量	任命者
IS 委員会委員	・経営者とともに組織の ISMS の方向性を定め、行動指針を指示することができる。 ・経営規模とバランスのとれた ISMS を導入できる。	経営者
IS 管理責任者	・ISMS について精通している。 ・組織全体に ISMS を主導することができる。 ・組織に対する脅威と脆弱性を認識し、適切なリスク対応をとることができる。 ・経営陣に対してマネジメントレビューの判断材料を提供できる。	経営者
情報セキュリティ委員	・部門内で ISMS を指導できる。 ・部門内の ISMS の問題点を把握し、改善要求が出せる。 ・部門内の意見をまとめ、IS 推進委員会で提案できる。	IS 管理責任者
IS 事務局員	・ISMS の要求事項を理解し、ISMS 推進のための実務を遂行できる。 ・組織間の問題を調整できる。	IS 管理責任者
内部監査責任者	・監査プログラムを策定することができる。 ・監査チームを指導できる。	経営者
内部監査員（チームリーダー）	・ISMS の内部監査の方法に精通している。 ・マネジメントシステム（ISMS、QMS、EMS など）の内部監査の経験がある。 ・監査実施計画書を作成できる。また、内部監査員を指導して、監査結論を出し、監査報告書を作成できる。	経営者

第８章　ISMS システム文書様式集

ISMS の構築（P)、運用（D)、見直し（C)、改善（A）の各フェーズでは様々な文書や記録が作られます。この章ではその様式例を紹介します。

文書の中には、資産台帳や、リスク対応計画書のように文書番号を伴った ISMS 文書として管理されるものと、内部監査報告書やセキュリティインシデント報告書のように記録として保管されるものに分かれます。前者の文書の様式を IS-R-01～IS-R-29、後者の記録のための様式を IS-R-30 以降として採番してあります。

ISMS 文書名と、その様式番号の対応は以下の通りです。

文書分類	文書名	文書番号	様式番号
文書 B	情報資産台帳	IS-B-01	IS-R-01
	リスクアセスメント結果表	IS-B-02	IS-R-02
	適用宣言書	IS-B-03	IS-R-03
	リスク対応計画書	IS-B-04	IS-R-04
	法的要求事項登録簿	IS-B-05	IS-R-05
	事業継続リスクアセスメント	IS-B-06	IS-R-06
	事業継続計画書	IS-B-07	IS-R-07
	年間教育計画表	IS-B-08	IS-R-08
	社員資格登録簿	IS-B-09	IS-R-09
	ISMS 年間監査計画書	IS-B-10	IS-R-10
	文書・記録一覧表	IS-B-11	IS-R-11
	管理策有効性測定記録簿	IS-B-12	IS-R-12

記録様式については、すでに使用している様式があれば、それを継続して使用されることをお勧めします。また、組織によって必要となる記録は異なりますので、この様式集の中から取捨選択し、必要な様式は追加して下さい。