

付録 1

メディカル社の事例

ここでは、架空の医療機器メーカーを例に「臓器などを検査するための検体に関する個人情報」を対象としたリスクマネジメントの例を紹介します。

なお、本書の内容については、リスクアセスメント作業全般にわたる内容を紹介する上で多くの情報を記載していますが、ストーリーの中心となる内容を表中の太枠部分を追って理解することも可能です。

目次

1	設定	2
2	情報資産の洗い出し	4
3	脅威分析	8
4	ぜい弱性分析	12
5	リスク分析	13
6	リスク評価	14
7	リスク対応	15
8	リスクマネジメントの承認	18
9	まとめ	21
	最後に	21

1 設定

「株式会社 メディカル」は、全国の病院・医院を中心とする顧客に測定機器を提供している中堅医療機器メーカーである。分野によっては世界的なシェアを持つ技術重視の企業である。百件を超える国際特許を取得しているが、公開を嫌って特許申請を行っていない技術情報を多数保有しているため、従来から技術情報の管理を厳格に行ってきた。

社長は一代でこの会社を築きあげた創業者であり、常日頃から研究開発の実施と技術情報の保護の重要性を社内に啓発してきた。

ところが、ある出来事をきっかけに技術情報と同様に重要である個人情報管理を見直すこととなった。それは、研究所員の作業報告書に、リーダから電話による依頼で、検体情報にアクセス（リーダ保有の ID とパスワードを使用）した旨が記載されていた。この報告を見た研究所長がリーダに、研究所員に伝えた ID とパスワードを変更したのかと聞いたところ、回答が「あいまい」であったので調査したところ、変更されていることまでは確認された。

このような事実があったことを、たまたま社長と話す機会があった時に触れたところ、翌日に他社の個人情報漏洩事件が起こり、その原因が研究所長の話と類似していたことから事態を重くみた社長は「検体情報はその提供者にしてみれば大切な個人情報である。そのような管理は確実にしてほしい。」と研究所長に情報管理の調査を指示した。

研究所長は検体情報の管理を見直すことにし、情報セキュリティに詳しい技術部の A 主任を呼んで、検体情報の管理の状況を明らかにするため、まずは業務フロー図の作成を依頼した。

A 主任は上司である技術部長と相談し、業務を洗い出して整理した結果を図 1-1 と表 1-1 にまとめた。

なお、検体情報の内容は被験者の氏名、性別、生年月日、病歴、診療の記録、検体写真等であり、検体自身は、主に血液、尿、臓器片、細胞片等であり専門医が管理している。

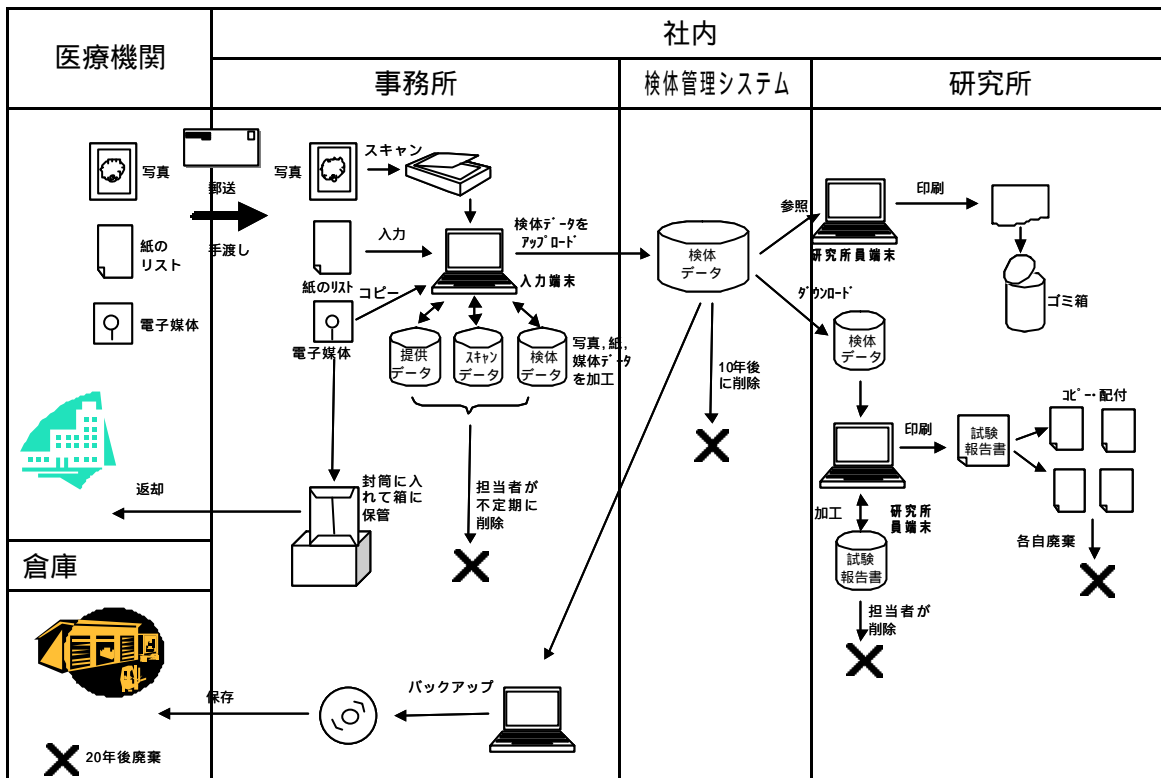


図 1-1 業務フロー

表 1-1 業務一覧

No	内容
	<p>メディカル社の事務所にて入力担当者が検体管理システム用の情報を医療機関より郵送もしくは手渡しで受け取る。</p> <p>情報：電子媒体、紙、写真</p>
	<p>事務所にて入力担当者が検体管理システムの入力端末へ で受け取った情報を取り込む。</p> <p>【登録方法】</p> <p>写真：スキャナーから読み込み</p> <p>紙：端末から手入力</p> <p>電子媒体：電子媒体から端末へコピー</p>
	<p>で端末に取り込まれた検体データを入力担当者がアップロード用に加工してから検体管理システムへアップロードする。</p> <p>アップロードが終了したデータは端末内HDへ保管される。保管されたデータは担当者が不定期に削除する。</p> <p>検体管理システム内のデータのうち、10年を経過したものは検体管理システム上からシステム管理者が削除する。</p>

No	内容
	登録済みの情報は入力担当者が封筒に入れて入力端末の横にある箱に入れ、事務所内ロッカーにて一旦保管し、その後入力担当者が医療機関へ郵送にて返却する。
	研究所の機器開発テストを行っている場所で研究所員端末から検体管理システムにアクセスし、データを参照する。参照後、端末に接続されているプリンタからデータを印刷する。印刷したデータは利用後に所員がゴミ箱に廃棄する。
	研究所内にて研究所員端末から検体管理システムへアクセスし、検体データをダウンロードする。ダウンロードしたデータは端末上で加工され、接続されているプリンタより試験報告書添付用に出力されることもある。
	研究所内にて研究所員が端末を使って試験報告書を作成する。報告書は作成後、プリンタより出力され、コピーを研究所員が研究所長、技術部長、営業部長、および役員全員に配布する。 配布時に検体データを参考情報として添付することがある。
	システム内の全検体情報は事務所にてシステム管理者が1ヶ月に1度バックアップを採取し、倉庫に保管する。保管されたデータは20年後に廃棄される。

図 1-1 と表 1-1 に従って分析してみると、メディカル社は、医療機関から機器開発の際のテスト用として多数の検体に関する情報の貸与を受けているが、その中に、検体提供者（患者）の氏名、住所および病歴等が記された記録も含まれている。

今回、新たに発見された問題としては、検体情報を印刷した紙がゴミ箱に捨てられていたことである（表 1-1 参照）。これは患者本人にとって重要な個人情報であり、今後もこのようなことが続けば、メディカル社から情報が漏洩する恐れがあり、懸念される点であった。

研究所長は、A 主任より検体情報の管理についての報告を受け、引き続き検体情報の個人情報管理に関して徹底的な調査を行うよう指示した。

A 主任の提案により、対象を「検体管理システムに関する個人情報」として、ISMS の考え方に基づくリスクアセスメントを行うこととなった。A 主任はリスクアセスメントを行うにあたり、JIPDEC（財団法人日本情報処理開発協会）から公表されている「ISMS ユーザーズガイド」および「ISMS ユーザーズガイド - リスクマネジメント編 -」を参考として作業を進めることにした。

2 情報資産の洗い出し

A 主任は作成した業務フロー（図 1-1, 表 1-1）から、検体管理システムに関係する情報資産の洗い出しを行った。業務フロー作成により情報の流れが分かっているため、作業を

効率的に行うことができた。

(1) 情報のライフサイクル表

A 主任は、情報が受領から返却まで様々な形態をとることを知っていたので、入手した検体情報についてライフサイクル表を作ることとし、情報がどのような取扱いを受けているのかを聞き出して表 1-2 を作成した。

表 1-2 情報のライフサイクル表

	情報	生成/受領	利用	保管	廃棄/返却
1	検体管理システム内個人情報	入力端末から情報をアップロードする。	必要な場合、研究所員が検体管理システムにアクセスして参照する。	システム内に保管し、情報は定期的にバックアップを採取する。	10 年を過ぎたデータはシステムから削除する。
2	入力端末内情報	(A)医療機関より電子媒体で提供を受け、入力端末でアップロード用に加工する。 (B)医療機関より紙および写真で提供を受け、入力端末で電子化する。	検体管理システムにアップロードする。	アップロード後のトラブルに備えて端末内 HD に加工データを保管する。	担当者が気づいたときに古いデータを削除する。
3	電子媒体	医療機関から郵送または手渡しで提供される。	入力用端末に 1 回のみ情報をコピーする。	封筒に入れて入力用端末の横にある箱に保管する。	医療機関に返却(郵送)する。
4	情報が記載された紙および写真	医療機関から郵送または手渡しで提供される。	紙は端末への入力時に参照する。 写真は入力端末のスクリーンで読み取る。	封筒に入れて入力用端末の横にある箱に保管する。	医療機関に返却(郵送)する。
5	研究所員端末内情報	システムから情報をダウンロードする。参照用に印刷することもある。 試験報告書に添付することもある。	研究所員端末内で加工される。	保管しない。	研究所員が気づいた時に削除している。
6	試験報告書	研究所員端末で作成する。その際、患者の個人情報を参考情報として添付することがある。 報告書は紙に印刷後配布される。	報告書は研究所長、技術部長、営業部長および役員全員に配布される。	保管は配布された各人に任されている。	廃棄は配布された各人に任されている。

7	バックアップ媒体	一ヶ月に一度、システム内の全検体情報を CD-R にバックアップする。バックアップは正副を取得する。	システムトラブル時に使用することがある。	施錠されている倉庫に保管する。	20 年後に廃棄することになっている（現在廃棄は発生していない）。
8	研究所内で参照用に印刷された紙	研究所員が端末から印刷する。	試験を行っている場所で参照する。	保管しない。	ゴミ箱に廃棄する。

ストーリー展開を追う方は表中の太枠部分 (No 1) に注目していただきたい。

(2) 資産洗い出しの結果

情報のライフサイクルを追う過程で有意義な情報を得て、結果として表 1-2 のとおり検体管理システムに係る個人情報を 8 種類に分けることができた。

また、各情報の管理状況についても把握することができた。

(3) 資産一覧作成

A 主任は資産価値を、情報の機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)に分けて評価し、これらの情報を表 1-3 のとおり資産一覧の形でまとめた。

評価は「ISMS ユーザーズガイド」にならって 4 段階とし、今後の作業を円滑に進めるために各資産に ID を付与した。

表 1-3 資産一覧

ID	資産	資産価値			資産価値の理由
		C	I	A	
A01	検体管理システム内 個人情報	4	3	2	C:患者のプライバシーに関わる個人情報 I:完全性が失われるとテスト評価に問題が生じる A:研究者が利用するのみであり厳しい可用性は要求されない
A02	入力端末内情報	4	3	2	C:患者のプライバシーに関わる個人情報 I:完全性が失われるとテスト評価に問題が生じる A:研究者が利用するのみであり厳しい可用性は要求されない
A03	電子媒体	4	3	2	C:患者のプライバシーに関わる個人情報 I:完全性が失われるとテスト評価に問題が生じる A:研究者が利用するのみであり厳しい可用性は要求されない
A04	情報が記載された紙 および写真	4	3	2	C:患者のプライバシーに関わる個人情報 I:完全性が失われるとテスト評価に問題が生じる A:研究者が利用するのみであり厳しい可用性は要求されない
A05	研究所員端末内情報	4	2	1	C:患者のプライバシーに関わる個人情報 I:完全性は必要だが、疑問があればシステムを参照可能 A:システムから再ダウンロード可能
A06	試験報告書の参考資料	4	1	1	C:患者のプライバシーに関わる個人情報 I:単なる参考資料 A:単なる参考資料
A07	バックアップ媒体	4	3	1	C:患者のプライバシーに関わる個人情報 I:完全性が失われるとテスト評価に問題が生じる A:トラブル発生時のみ必要となる
A08	研究所内で参照用に 印刷された紙	4	2	1	C:患者のプライバシーに関わる個人情報 I:完全性は必要だが、疑問があればシステムを参照可能 A:システムから再ダウンロード可能

ストーリー展開を追う方は表中の太枠部分 (A01) に注目していただきたい。(以下同様)

(4) 資産一覧の承認

A 主任は作成した資産一覧（表 1-3）を研究所員とともにレビューして誤りのないことを確認した。

資産価値の評価は経営判断が必要であり、経営陣の承認を受ける必要があるため、この段階で経営者のレビューを受けることにした。そこで A 主任は技術部長とともに、これまでの経緯を記した資料と資産一覧を直接社長に提出した。

社長は資産一覧を見て思い当たることがあった。実は試験報告書は、参考資料（表 1-3 の資産 ID：A06）と共に営業部長が新製品の売り込みのために顧客に見せて歩いているのだ。そこで、資産一覧自体については承認したが、試験報告書に参考情報として検体情報を添付する必要性、及び個人情報の漏洩防止策について再検討するように指示した。

3 脅威分析

A 主任は再度研究所に向かい、個人情報漏洩の対策を整理するため脅威一覧の作成作業への協力を研究所長に依頼した。社長から研究所に強い指示が出ているらしく、研究所長も事の重要さを認知しており、多忙ではあるが多くの実情を把握している研究所員のリーダーの B さんを担当に指名した。

(1) 脅威の洗い出し

脅威一覧の作成作業は、A 主任と研究所員リーダーの B さんがインタビュー形式で書き上げる方法を探ることにして、業務に詳しい研究所員に聞いて歩いた。幸い情報のライフサイクル表（表 1-2）や資産一覧（表 1-3）で、ある程度の脅威は分かっているので効率良く行えた。それらを基にして情報資産毎の脅威洗い出し作業を行い、表 1-4 のとおりまとめた。

表 1-4 情報資産毎の脅威の明確化

個人情報漏洩に関わる脅威					
ID	情報	生成/受領	利用	保管	廃棄/返却
A01	検体管理システム内個人情報	データアップロード中の外部からの盗聴	認可されていない者が研究所員端末から不正アクセス 研究所員端末画面のぞき見	認可されていない者によるシステム内データの漏洩・持ち出し 研究者、システム管理者によるデータ持ち出し	機器廃棄時の情報漏洩
A02	入力端末内情報	認可されていない者による入力端末内情報の持ち出しやコピー			機器廃棄時の情報漏洩
A03	電子媒体	医療機関から郵送中の盗難・紛失	医療機関から提供された電子媒体の盗難・紛失	医療機関から提供された紙・写真の盗難	医療機関への返送中の盗難・紛失
A04	情報が記載された紙および写真				
A05	研究所員端末内情報	認可されていない者による研究所員端末内情報の漏洩・持ち出し			機器廃棄時の情報漏洩
A06	試験報告書	報告書に添付された参考資料の不適切な配布による個人情報漏洩 報告書に添付された参考資料の盗難による個人情報漏洩			廃棄後の報告書から情報漏洩
A07	バックアップ媒体	システム管理者によるバックアップの不正コピー	バックアップ媒体の盗難		廃棄後の媒体から情報漏洩
A08	研究所内で参照用に印刷された紙	研究所内で印刷された紙の不正持ち出し、盗難			廃棄後の紙から情報漏洩

(2) 脅威一覧

A 主任は洗い出された表 1-4 の脅威を基に表 1-5 のとおり脅威一覧を作成し、脅威の評価を行った。なお、脅威の評価を行う際、ISMS ユーザーズガイド-リスクマネジメント編 -の P28 の表 2-11 や P29 の表 2-12 の「脅威の分類基準例」を参考にして値を入れた。

表 1-5 資産毎に識別された脅威と評価の一覧

資産				脅威			
ID	C	I	A	ID	内容	値	理由
A01	4	3	2	T01	データアップロード中の外部からの盗聴	1	データアップロードは社内 LAN で行うため発生頻度は低い
				T02	認可されていない者が研究所員端末から不正アクセス	2	研究所員は役割に応じた形での権限が付与されている。さらに研究所は厳密な入退管理がされている。但し、外部委託者などが端末にアクセスする可能性がある
				T03	研究所員端末画面ののぞき見	2	
				T04	認可されていない者によるシステム内情報の漏洩・持ち出し	2	
				T05	研究者、システム管理者によるデータ持ち出し	1	
				T06	機器廃棄時の情報漏洩	3	発生の可能性が高い
A02	4	3	2	T07	認可されていない者による入力端末内情報の持ち出しやコピー	3	入力端末は外部の者がアクセスしやすい場所に置かれている
				T08	機器廃棄時の情報漏洩	3	発生の可能性が高い
A03	4	3	2	T09	医療機関から郵送中の盗難・紛失	1	当社の責任範囲ではないが、受取っていないことを証明できず、紛失の責任を追究される可能性がないとは言えない
				T10	医療機関から提供された電子媒体の盗難・紛失	2	過去 2 回程度、紛失騒ぎがあった
A04	4	3	2	T11	医療機関から郵送中の盗難・紛失	1	当社の責任範囲ではないが、受取っていないことを証明できず、紛失の責任を追究される可能性がないとは言えない
				T12	医療機関から提供された紙・写真の盗難	2	盗難の事実はないが起こる可能性がある
A05	4	2	1	T13	認可されていない者による研究所員端末内情報の漏洩・持ち出し	2	盗難の事実はないが起こる可能性がある
				T14	機器廃棄時の情報漏洩	3	発生の可能性が高い

A06	4	1	1	T15	報告書に添付された参考資料の不適切な配布による個人情報漏洩	3	営業部長が新製品の売り込みのために顧客に見せて歩いている
				T16	報告書に添付された参考資料の盗難による個人情報漏洩	2	盗難の事実はないが起こる可能性がある
				T17	廃棄後の報告書から情報漏洩	3	発生の可能性が高い
A07	4	3	1	T18	システム管理者によるバックアップの不正コピー	1	厳密な秘密保持契約にサインしており、持ち出した場合の重い処罰が明確であるため、犯行の可能性は低い
				T19	バックアップ媒体の盗難	2	盗難の事実はないが起こる可能性がある
				T20	廃棄後の媒体から情報漏洩	3	発生の可能性が高い
A08	4	2	1	T21	研究所内で印刷された紙の不正持ち出し、盗難	2	盗難の事実はないが起こる可能性がある
				T22	廃棄後の紙から情報漏洩	3	発生の可能性が高い

4 ぜい弱性分析

A 主任はさらに、検体に関する個人情報のぜい弱性一覧を作成する作業を行った。

(1) ギャップ分析

A 主任はギャップ分析を用いてシステムのぜい弱性分析を行った。具体的には、ギャップ分析の対象に対し、JIS X 5080 等を参考に管理策を選択し、選択した管理策とシステムの管理状況との差異を明らかにする作業を実施した。

情報の取扱いについて、研究所員へのインタビューを繰り返した結果、検体管理システムの問題点が次第に明らかになっていった。得られた情報をまとめ、表 1-6 のぜい弱性と評価の一覧を作成した。

表 1-6 脅威に対するぜい弱性と評価の一覧

脅威 ID	ぜい弱性 ID	内容	値
T01	V01	HUB 及びそのポートが適切に管理されている	1
	V02	ネットワークが適切に管理され、外部から分離されている	1
T02	V03	パスワードの設定や変更について、定期的に変更する等の通常のルールは存在するが、例外時のルールが無く、各人が自分の判断で行っている。	3
	V04	社員不在時の監視体制が不十分	2
T03	V04	前述の V04 と同じ	2
T04	V03	前述の V03 と同じ	3
T05	V05	管理者によるシステム内情報の取扱いについて、チェック体制が不十分	2
	V06	バックアップデータは物理的に保護されているが、暗号化等による盗難時の配慮がなされていない	2
T06	V07	機器の廃棄時にハードディスク内情報の消去処理の確認が不十分	2
T07	V08	入力端末の起動パスワード、ハードディスク内暗号化、端末使用時のログイン等、システム的なアクセス制限がされていない	3
T08	V07	前述の V07 と同じ	2
...	(以下数十件のぜい弱性が発見された)		

(2) 研究主任からの呼び出し

ギャップ分析が終わった頃、A 主任は突然研究所員のリーダー B さんの上司である研究主任に呼び出された。研究主任は A 主任にリスクアセスメントについて一応のねぎらいの言葉をかけながら、次のように切り出した。

「君は、多忙を極める B さんの協力を得て研究所員の素行を調査して社長に報告しているそうじゃないか。まるで研究所員を犯罪者の様に扱っていると苦情が来ている。」

A 主任は、「そんなことはしていませんが…。研究所長から話は伝っていませんか。」と戸惑いながら回答した。A 主任は、今回のリスクアセスメントの趣旨について研究所内への説明を十分に行わず、協力のみを求めていたことに思い至った。精度の高い作業を行うためには現場の理解と協力が不可欠であり、リスクアセスメントを行う前に説明会を開催しておくべきだったと反省した。

早速 A 主任は技術部長に、今回の件について研究所員に理解と協力を促すための説明会実施を提案し、許可を得た。その結果、研究所員は A 主任の作業に対してこれまで以上に理解を示し協力的になった。

5 リスク分析

遅ればせながら現場説明会を実施した後、A 主任は、これまでに得られた脅威にぜい弱性に対応付けた表 1-6 を基にしてリスク値を算出した。その結果として、リスク値を表 1-7 のリスク値算出結果一覧にまとめた。

リスク値を算出する際、ISMS ユーザーズガイドの「4.2.5 STEP5 リスクアセスメントを行う」で紹介されている、次の式を用いて算出した。

$$\text{リスク値} = \text{「情報資産の価値」} \times \text{「脅威」} \times \text{「ぜい弱性」}$$

但し、ISMS ユーザーズガイド - リスクマネジメント編 - の P35【補足】「リスク値を算定することの意味」にて解説されているとおり、

- ・この計算式には厳密な理論性がないこと
- ・この式によって得られた数値だけに頼ってリスク値を決定せず人間の判断を優先して対策の必要性の有無を決定することも検討しなければいけないこと
- ・算定された数値の妥当性を検証していかなばならないこと

を常に頭において今後の作業を実施していくこととした。

A 主任はこれまでの結果をまとめ、算定された数値等の妥当性を検証するために、研究所長を含む数名の研究所員とレビューを行った。

レビューの結果を受けて、脅威の値とぜい弱性の値について若干の修正を行い、現場の意見を踏まえて分析結果を修正した。

また、その際に社長から指示のあった「試験報告書に検体情報を添付する必要があるのか」という質問について研究所員の意見を聞いた。研究所員は試験報告書への検体情報の添付は不必要と思える場合がほとんどだが、慣例を破ることを恐れてあえて添付しているとの意見であった。これに関するリスク分析結果は、高い値すなわちハイリスクであることを示している。

表 1-7 リスク値の算出結果

資産				脅威		ぜい弱性		リスク値						
ID	C	I	A	ID	値	ID	値	ID	C	I	A			
A01	4	3	2	T01	1	V01	1	R01	4	3	2			
						V02	1	R02	4	3	2			
				T02	2	V03	3	R03	2	4	1	8	1	2
						V04	2	R04	1	6	1	2	8	
				T03	2	V04	2	R05	1	6	1	2	8	
				T04	2	V03	3	R06	2	4	1	8	1	2
				T05	1	V05	2	R07	8	6	4			
						V06	2	R08	8	6	4			
T06	3	V07	2	R09	2	4	1	8	1	2				
A02	4	3	2	T07	3	V08	3	R10	3	6	2	7	1	8
				T08	3	V07	2	R11	2	4	1	8	1	2
..... (以下100件近くのリスクが発見された)														

表1-7の補足：

本事例ではA01（特に太枠部分）とA06（表1-7には出ていない）に焦点を当て展開していく。なお、A02（入力端末内情報）のリスク値は高く、検討すべき項目であるが、本事例では、その検討を省略する。

6 リスク評価

リスク分析の結果に対し、リスク対応を行うべきか否かの判断はA主任の責任範囲を超

えるため、それまでの全ての調査結果を技術部長に提出して判断を仰いだ。調査結果には試験報告書への検体情報の添付に関する研究所員の意見も含めた。

また、調査結果には、リスクの内容から見てリスク値が9以上に対してリスク対応を行うべきとのA主任自身の考えを参考意見として添えた。

技術部長は、受け取った資料に基づいてA主任と話し合い、結論としてリスク値9以上がリスク対応の対象と判断した。

7 リスク対応

ひとつのリスクに対するリスク対応の方法は「管理策の採用」「リスク保有」「リスク回避」「リスク移転」などの方法があり、「管理策の採用」を行うとしても物理的対策を取るか、システムの対策を取るか、または運用により対策するか等様々な方法があり得る。

A主任は、対応が必要なリスクに対して、考えられる複数のリスク対応策を検討し、その結果を表1-8にまとめて技術部長に提示した。

表 1-8 検討したリスク対応策

ぜい弱性	関連リスク	リスク内容	リスク値	リスク対応案	コスト
V03	R03 R06 ...	ユーザ ID およびパスワードはある程度管理されているが、例外時の管理手順などが言及されていないため、認可されていない者が研究所員端末や入力端末から不正アクセスし、検体システム内個人情報の漏洩、改ざん、破壊を行う。	12~24	【対策1】 システムのユーザ ID およびパスワードの例外時を含む詳細な管理ガイドラインを作り、利用者教育によりパスワード管理の重要性を啓発する。	小
				【対策2】 システムへのログインおよび重要な情報へのアクセスについて監査ログを採取し、定期的にチェックする。	中
V04	R04 R05 ...	研究所員が不在時の監視手段がないため、第三者による端末への不正アクセス、媒体の盗難、報告書等の不正コピーといったリスクがある。	8~16	【対策1】 研究所員の不在時、研究所は施錠し、清掃員の立ち入りも禁止する。	小
				【対策2】 研究所の出入り口に監視カメラを設置し、入退状況を監視する。	中

				<p>【対策 3】</p> <p>研究所に立ち入るすべての第三者について、守秘義務および事故発生時の損害賠償請求を契約にて明確に規定する。</p>	中
リスク値 8 については受容したため、表では割愛した。					
V07	R09 ...	研究所員端末、入力端末の廃棄時にハードディスク内情報が漏洩する。	12~24	<p>【対策 1】</p> <p>研究所員端末、入力端末の廃棄時はハードディスクの消去処理、破壊などにより情報の読み出しを不可能にする。</p>	中
				<p>【対策 2】</p> <p>ハードディスク暗号化ツール等により、ハードディスク内の情報を暗号化する。</p>	大
..... (以下 15 件のリスク対応策を作成した)					

技術部長は、研究所長、研究主任、A 主任とともに表 1-8 を基にリスク対応策を検討し、最終的な対策を表 1-9 のとおり決定した。また、具体的な対策コストを試算して添付した。

表 1-9 リスク対応策

ぜい弱性	関連リスク	リスク内容	リスク値	リスク対応
V03	R03 R06 ...	ユーザ ID およびパスワードはある程度管理されているが、例外時の管理手順などが言及されていないため、認可されていない者が研究所員端末や入力端末から不正アクセスし、検体システム内個人情報の漏洩、改ざん、破壊を行う。	12~24	<p>【表 1-8 V03 対策 1 と対策 2 を共に採用】</p> <p>リスクが高いため、万全の対策が必要である。</p> <p>システムのユーザ ID およびパスワードの例外時を含む詳細な管理ガイドラインを作り、利用者教育によりパスワード管理の重要性を啓発する。</p> <p>さらにシステムへのログインおよび重要な情報へのアクセスについて監査ログを採取し、定期的にチェックする。</p>
V04	R04 R05 ...	研究所内に研究所員がいなくなる場合の監視手段がないため、第三者による端末への不正ア	8~16	<p>【表 1-8 V04 対策 1 と対策 3 を採用】</p> <p>対策 2 については周囲の同意が得られず見合わせた。</p> <p>研究所員がいらない場合、研究所は施錠し、</p>

		クセス、媒体の盗難、報告書等の不正コピーといったリスクがある。		清掃員の立ち入りも禁止する。 ただし、中長期的な対策として研究所に立ち入るすべての第三者について守秘義務および事故発生時の損害賠償請求を契約にて明確に規定する必要がある。
V07	R09 ...	研究所員端末、入力端末の廃棄時にハードディスク内情報が漏洩する。	12~24	【表 1-8 V07 の対策 1 を採用】 対策 2 についてはコストが高いため見合わせた。 研究所員端末、入力端末の廃棄時はハードディスクの消去処理、破壊などにより情報の読み出しを不可能にする。
..... (以下 15 件のリスク対応を作成した)				

8 リスクマネジメントの承認

技術部長はリスク分析、リスク評価、リスク対応の過程を簡潔な報告書にまとめ、報告した。

2004年4月28日

社長殿

技術部長

検体管理システムの個人情報に関するリスクマネジメントについて

検体管理システムの個人情報に関するリスクマネジメントについて報告致します。以下をご一読いただき、ご承認をお願いします。

1. リスク分析

(1)実施概要

担当者：技術部 主任 A

手法：詳細リスク分析（日本情報処理開発協会(JIPDEC)発行の「ISMS ユーザーズガイド」を参照した）

期間：2004年2月20日～2004年4月10日

(2)結果

情報資産：8種類（社長承認済）

脅威：22種類（情報資産ごとに洗出し）

ぜい弱性：30件（脅威ごとに洗出し）

リスク：96件

リスク分布：

リスク値	1	2	3	4	6	8	9	12	16	18	24	27	36
リスク件数	0	4	4	5	8	13	3	15	4	16	20	2	2

実際の各リスク項目については別紙を参照

2. リスク対応

(1)実施概要

担当者：技術部長

手法：技術部 A主任のリスク分析結果に基づき、リスク対応を実施する

リスク受容レベル：9（リスク値9未満のリスクは一括して受容する）

リスク対応対象：62件（リスク値9以上）

(2)リスク対応表

リスク対応を要するリスクは6 2件であったが、対策を講じることにより複数のリスクに対応できるため、リスク対応は以下の7件に集約される。

	項目	内容	効果
1	パスワード管理ガイドライン	システムのユーザ ID およびパスワードの例外時を含む詳細な管理ガイドラインを作成し、パスワード管理を徹底させる	ぜい弱性：3 1 2 1
2	監査ログ	システムへのログインおよび検体データへのアクセスについて監査ログを採取し、定期的にチェックする	ぜい弱性：3 2 2 1
3	研究所の施錠	当社研究所員がいなくなる際には研究所を施錠し、清掃員の立ち入りも禁止する	ぜい弱性：3 1 2 1
4	検体情報の取扱いレベル	研究所における検体情報の取り扱いについては、重要機密情報として管理を行うよう規則を更改する。これにより、検体情報の印刷は原則禁止となる	ぜい弱性：3 1 2 1
5	試験報告書	試験報告書への検体情報の添付は原則行わないものとし、必要な場合には研究所長の許可を得る	ぜい弱性：3 1 2 1
6	返却前の帳票、媒体	医療機関から送付された検体情報を含む帳票、媒体は、入力処理完了後返却まで倉庫に保管し、施錠する。また返却が確実にされるよう、台帳管理を行う	ぜい弱性：3 2 2 1
7	情報セキュリティ教育	全社従業員に対して情報セキュリティ教育を行い、情報セキュリティの重要性を啓発する	ぜい弱性：3 2 2 1 脅威*1：3 2 2 1

*1 教育により従業員の注意が徹底されることで管理ミスの脅威も減少する

(3)リスク対応後の予想リスク分布

リスク分布：

リスク値	1	2	3	4	6	8	9	12	16	18	24	27	36
リスク数	0	8	8	16	28	36	0	0	0	0	0	0	0

実際の各リスク項目については別紙を参照

前表(2)リスク対応結果)の各値より算出されたリスク値を基に作り上げたが、本事例では省略している。

(4) リスク対応コスト

リスク対応には以下のコストが発生する。

	項目	一時コスト	ランニングコスト
1	パスワード管理ガイドライン(例外時を含む)	0.5 人月 (ガイドライン作成)	0.1 人月/月 (パスワード管理)
2	監査ログ	1,000,000 円 (システム設定を業者に依頼)	0.1 人月/月 (監査ログのバックアップ等)
3	研究所の施錠	50,000 円 (パスワード式の設置)	コストは無視できる (パスワード管理)
4	検体情報の取扱いレベル	50,000 円 (ステッカーの発注)	0.1 人月/月 (レベル管理)
5	試験報告書	コストは無視できる (注意勧告のみ)	コストは無視できる (教育に含まれる)
6	返却前の帳票、媒体	1.5 人月 (台帳作成, ルール作り)	0.1 人月/月 (台帳管理)
7	情報セキュリティ教育	2,000,000 円 (教材作成および教育を業者に依頼)	800,000 円/年 (教材改訂および教育を業者に依頼)

(5) その他

試験報告書に参考情報として検体情報を添付する必要性については、本報告書の資産 No5 に記述している通り、添付は原則行わないようにした。特に、営業部長に対しては、今回の対策を十分に説明し理解させた。

以上

報告書は、社長から承認を得られたが、更に技術部長、研究所長に対して、以下の指示が出された。

「今回の承認によって実際にリスク対応を実施していく訳だが、リスクは常に変化するものなので、リスク対応の妥当性について定期的に検証すること、問題がある、もしくはありそうだと判断される場合は、問題点を明らかにした上で、是正処置及び予防処置の徹底を図ること、あるいは、リスク算出の方法の見直しを含むリスクアセスメント手法そのものの見直しを検討すること。」

また、試験報告書への検体情報添付については、ルール作りを早急を実施するよう社長から新たに指示が出された。

9 まとめ

メディカル社のリスクマネジメントは、さまざまな問題を明確にしたが、従来より技術情報について厳格な管理をしていたこともあり、その大部分は個人情報の重要性認識の問題であった。

よって、今回は技術情報と同様に個人情報の管理を厳格に行うこと、社員の個人情報保護に関する意識を教育によって高めることが主な対策となった。

これらの対策は効果をあげ、ユーザ ID の貸し借りや個人情報がゴミ箱に捨てられるようなことは、それ以後見られなくなった。

最後に

この内容はあくまで例示であり、ISMS 構築における「リスクマネジメント」の一連の作業について分かりやすく説明することを目的としています。従って、リスクマネジメントの正式な手順よりも全体的な流れを重視し、詳細な個別資産の洗い出しや表などは、一部簡素化しています。このことは、完全性や可用性の観点からのリスク対応について十分に検討がなされていない点や、組織面においても、リスク分析の範囲やリスク判断の基準(クライテリア)を A 主任と B リーダのみに任せて進めている点なども含みます。

皆様方の取組みとしては、このようなことに留意され、本事例を参照に、ISMS 構築のための組織体制を充実され、リスクアセスメント実施の際は、対象となる情報資産などの網羅性を確保され、計画的な実施(確度の高いリスク評価を含みます)を実現されること、また、それらについて継続的に見直しをされることが望まれます。