

# ISMS **ガイド**(Ver.0.8)

- パイロット審査に向けて -

ISMS : Information Security Management System

情報セキュリティマネジメントシステム

平成 13 年 9 月 14 日



財団法人 日本情報処理開発協会

## はじめに

(財)日本情報処理開発協会(以下、「JIPDEC」という)では、情報セキュリティマネジメントシステム(Information Security Management System:以下、「ISMS」という)適合性評価制度(以下、「本制度」という)の平成14年度4月からの本格運用を前に、本制度のパイロット事業(以下、「本事業」という)を行っています。

\*「ISMS 適合性評価制度パイロット事業実施要領」<http://www.isms.jipdec.or.jp/doc/ismspilot.pdf>を参照願います。

JIPDECでは、本事業を通じて、情報セキュリティに関する認証制度に伴う様々なノウハウ等を蓄積し、本制度を国際的に信頼を得ることができる制度として発展させるとともに、我が国の情報セキュリティレベルの向上に貢献していきます。

また、本事業の中で、情報処理サービス業情報システム安全対策実施事業所認定制度(以下、「安対制度」という)の認定取得事業者が、本制度へスムーズに移行し、安対制度の継続性が確保できることを実証していきます。

本書は、本事業にあたり、より円滑な実施を促すことを目的に作成しています。

本書は、「基本編」と「事例編」の2部構成となっています。「基本編」では、本事業の審査にあたって、基本的に留意すべきことをまとめており、「事例編」では、ある会社の審査までの一連の流れをストーリーとして解説し、審査のイメージを伝えるためにまとめています。

本書は、審査登録機関の審査員が本事業の審査業務を実施する上で、参考に供することを想定していますが、受審する事業者にとっても大いに参考になると思います。

なお、本書は審査の方法を規定するものではありません。また、記述内容は審査業務において必要なすべての事項を網羅しているものではないことをここに明記しておきます。

平成13年9月

財団法人日本情報処理開発協会

# 目 次

I 基本編	1
1. ISMS の要求事項	2
1.1 情報セキュリティポリシーの策定（「管理の目的及び管理策」）	4
1.1.1 ポリシー策定の組織体制	4
1.1.2 経営陣による承認	5
1.1.3 情報セキュリティ委員会の役割	5
1.1.4 情報セキュリティ策定チーム	5
1.1.5 専門家・外部コンサルタント	6
1.1.6 関係者への周知	6
1.1.7 定期的な見直し	6
1.2 情報資産の洗い出し（「保護すべき情報資産」）	7
1.2.1 洗い出しの対象	7
1.2.2 情報資産の価値	8
1.2.3 情報資産洗い出しの例	9
1.3 リスク評価（「要求される保証の度合い」）	10
1.3.1 ギャップ分析	10
1.3.2 詳細リスク評価	11
1.4 リスク管理の原則（「要求される保証の度合い」）	14
1.4.1 リスク許容	14
1.4.2 リスク低減	15
1.4.3 リスク移転	15
1.4.4 リスク回避	16
1.5 ISMS の構築	17
1.5.1 ここまでの説明と基準との整合	17
1.5.2 マネジメントシステムの構築	18
1.6 継続性の確保	21
1.6.1 運用の記録の例	21
1.6.2 適正な管理	21
1.6.3 継続性の確保	22

2. 審査のポイント .....	23
2.1 リスクマネジメントに関する審査上のポイント .....	24
2.1.1 リスクマネジメントの運用管理面 .....	25
2.1.2 リスクマネジメントの組織管理面 .....	33
2.2 選択された管理策に関する審査上のポイント .....	35
2.2.1 管理策例(1) セキュリティ組織 .....	37
2.2.2 管理策例(2) アクセス制御 .....	40
2.2.3 管理策例(3) 事業継続管理 .....	43
2.2.4 管理策例(4) 準拠 .....	47
3. 審査プロセスについて(参考) .....	50
3.1 ISMS適合性評価制度パイロット事業の枠組み .....	50
3.2 審査プロセスについて .....	52
3.2.1 審査の概要 .....	52
3.2.2 Stage1(文書審査)の内容 .....	58
3.2.3 Stage2(実地審査)の内容 .....	59
4. 参考文献 .....	60
4.1 参考文献 .....	60
4.2 法令等 .....	67
4.2.1 情報保護に関する法令 .....	67
4.2.2 コンピュータ犯罪に関する法令 .....	67
4.2.3 設備に関する法令 .....	68
4.2.4 社会的情報インフラに関する法令 .....	70
4.2.5 知的財産権に関する法令 .....	70
5. 用語の説明 .....	71

II 事例編	74
1. 事例会社の概要	75
2. ISMSの準備	76
2.1 企画	76
2.2 検討	78
2.2.1 課題(1) 情報セキュリティ管理の適用範囲	80
2.2.2 課題(2) 情報セキュリティリスク評価手順の策定	84
2.2.3 課題(3) 情報セキュリティ管理に関する規程類の整備	87
2.2.4 課題(4) 情報セキュリティに関する管理組織整備	91
2.2.5 課題(5) 情報セキュリティ教育・訓練	93
2.2.6 課題(6) 情報セキュリティの独立レビュー	95
2.2.7 課題(7) 情報セキュリティ事故管理	96
2.2.8 課題(8) コンプライアンス管理	100
2.2.9 課題(9) 事業継続計画作成	101
3. ISMSの運用	102
3.1 情報セキュリティリスク評価・リスク管理および適用宣言書作成	102
3.1.1 リスク評価	102
3.1.2 リスク管理	104
3.1.3 情報セキュリティ基本規程/情報セキュリティに関する全社規程/情報セキュリティガイドラインの見直し	105
3.1.4 適用宣言書の作成	107
3.2 情報セキュリティ教育	108
3.2.1 全社情報セキュリティ教育	108
3.2.2 部門情報セキュリティ教育・訓練	109
3.2.3 教育・訓練の改善	109
3.3 情報セキュリティ対策の運用および記録	110
3.3.1 情報セキュリティ対策の実施	110
3.3.2 情報セキュリティ対策に関する記録の収集とチェック	110
3.4 情報セキュリティ監査の実施および記録	111
3.4.1 情報セキュリティ監査の実施	111
3.4.2 情報セキュリティ監査記録	111

4. 審査事例	112
4.1 審査準備	112
4.2 審査実施	113
4.2.1 Stage 1 (文書審査)の審査業務計画	114
4.2.2 Stage 2 (実地審査)の審査業務計画	117
4.2.3 審査プログラム	118
4.3 審査結果	119
4.3.1 審査員メモ	119
4.3.2 審査結果	127
4.3.3 認証登録	127
4.3.4 維持審査/更新審査	128
5. 参照資料(会社の詳細情報)	129
5.1 基本情報	129
5.2 契約形態	131
5.2.1 ファシリティー提供	131
5.2.2 運用監視	131
5.2.3 運用委託	131
5.3 消費者金融業(以下A社)の与信枠設定サポートシステムの業務委託契約内容の要約	132
5.3.1 業務委託範囲	132
5.3.2 与信枠設定サポートシステム	132
5.3.3 機器の所有権	132
5.3.4 システム構成(概要)	133
5.3.5 情報セキュリティに関する覚書の内容の要約	134
5.4 情報セキュリティ基本規程	136
6. 付属資料(基準対応表)	139

# I 基本編

## 1. ISMS の要求事項

「情報セキュリティマネジメントシステム（ISMS）適合性評価制度」（以下、「本制度」とする）の基準「ISMS 認証基準(Ver.0.8)」(以下、「本基準」とする)の第3章には、「ISMSの要求事項」として情報セキュリティマネジメントシステム（以下、「ISMS」とする）の枠組み（フレームワーク）と、その実施における要求事項が記載されています。この要求事項は、ISMS構築を目指すすべての事業者が遵守しなければならないスタンダードであり、審査においても重要視すべき項目です。

### 【コラム】

#### <なぜ「情報セキュリティマネジメント」が必要なのか？>

そもそも、ISMS 導入の背景には「企業統治（コーポレートガバナンス）」という考え方の台頭があります。「企業の究極の目的、存在意義はどこにあるのか？」という問いかけに、ガバナンスは「投資家から預託された資産の効率的な活用とリターンの極大化」と答えます。今日、ガバナンスの実現は、「情報」を効率的にマネジメントし、利用、保存、保護することが絶対条件になっています。情報は、今日の企業活動の命脈（ライフライン）であり、IT 技術の活用は競争における優位性確保の重要な要素となっています。また、「情報」の価値の極大化と「情報化投資（IT 投資）」の額の極小化は、経営の指標として注目されています。「情報セキュリティマネジメント」は、適切なコントロール（統治）の導入により相反（あいはん）する指標をバランスし、情報を安全に活用可能な範囲を明らかにします。

事業者は、事業上有効かつ効率的な ISMS 構築のために、真に必要な業務を管理対象として選択し、過剰な管理やリソースの無駄使いを避けるため、適切な水準に情報セキュリティを維持する管理策を採用します。また、事業者には、第三者に対しセキュリティ水準について証明する責任があります。

### 第3 ISMSの要求事項

#### (1) 一般

組織固有の ISMS を確立し維持するため、以下の項目について文書化すること。

- (ア) 保護すべき情報資産
- (イ) リスクマネジメントに対する組織の取組方法
- (ウ) 管理目的及び管理策の内容
- (エ) 保護すべき情報資産に要求される保証の度合い

本基準の第1項( (1) )には、「ISMSとは何か?」という問いに対する答えがあります。この4つの事項を明らかにすることにより、事業者の「情報リスク管理」が有効で且つ効率的な状態に維持することを証明することが可能になります。

## 1.1 情報セキュリティポリシーの策定（「管理の目的及び管理策」）

情報セキュリティポリシー策定の目的は、ISMSを構築する事業者の情報セキュリティに対する考え方や取り組みを明確にすることにあります。事業者は、ISMSを確立する上で、このセキュリティポリシーを必ず策定するべきです。

情報セキュリティポリシーには、事業者が保有している情報資産とそれを保護する理由が明示され、その内容や記述のレベル（厳しさ等）には経営方針や社内風土も反映されていることがあるべき姿です。

### 【コラム】

#### <情報セキュリティポリシー（基本方針）の内容>

情報セキュリティポリシー文書には、例えば以下のような項目が含まれます。

情報セキュリティへの取り組みへの表明

目的

対象範囲

用語の定義

基本原則

コンプライアンス

罰則 等

### 1.1.1 ポリシー策定の組織体制

次に、ポリシー策定のための組織体制について紹介します。策定組織の人選には、事業者内の情報の取り扱いに関する様々な問題を討議するのに必要十分な範囲から召集すると同時に、実際のISMS運用の体制についても考慮し、関連部門から広く策定メンバーを募るべきです。以下に示したのは、情報セキュリティポリシー策定のための組織体制の一例です。

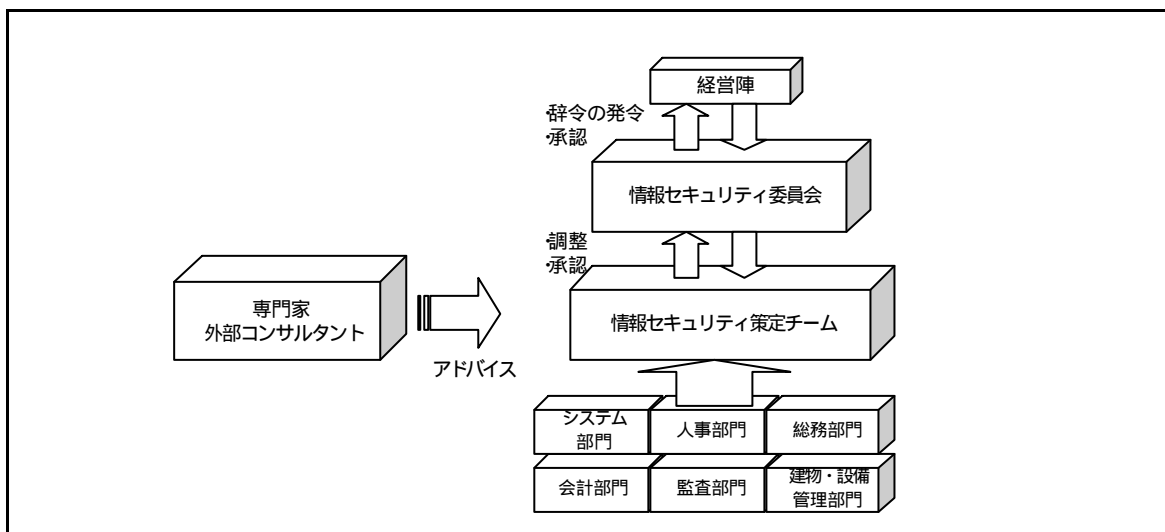


図 1-1 情報セキュリティポリシー策定のための組織体制の一例

### 1.1.2 経営陣による承認

情報セキュリティポリシーは、経営陣によって承認されなければなりません。

経営陣による承認は、会社がISMS構築に真剣であることとの意思表示といえます。また、違反者に対する罰則も明記する必要があるため、経営陣の承認は必須といえます。情報セキュリティポリシーは、それを形骸化させないためにも、組織における各自の情報セキュリティ上の権限と責任を、経営者の責任において規程文書の形で文章化することが重要です。

通常、策定する情報セキュリティポリシー及びスタンダードの文章が、事業者において既存の社内規程でどのような位置付けにするかを決定した段階で、「承認」等の権限から経営層の関与は、手続き等の面から決まるものです。

### 1.1.3 情報セキュリティ委員会の役割

情報セキュリティ委員会は、

- (1) 情報セキュリティポリシーの文書策定時には内容について実質的な決定機関となる
- (2) 導入段階の情報セキュリティポリシー導入を推進する各種施策や改訂を検討する
- (3) 運用段階でセキュリティ問題等が発生した場合の検討機関となる

という、事業者における情報セキュリティの中心的役割があります。

情報セキュリティ委員会を中心とした体制で策定されるポリシー文書は、委員会だけでなく事業者の経営陣により承認され、社内規程として関係者に周知され、さらに定期的に見直しを行わなければなりません。委員会は、事業者におけるすべての情報資産の取り扱いに責任を持ち、また情報セキュリティの方向性を社内に提言できるだけの情報セキュリティに関する理解と実行力をもった組織であるべきです。

### 1.1.4 情報セキュリティ策定チーム

情報セキュリティポリシー策定にあたり、社内の重要な情報資産について広く現状を把握し、その取り扱いを検討するのに十分な知見を持つメンバーで構成されるべきです。

また、情報資産の取り扱い方法の決定については、部署間での見解の相違や、利害関係の調整が必要になる場合が多くあります。策定チームは、そのような摩擦の調整役として、当事者に対してうまく働きかけることが求められます。この場合は、高いセキュリティ知識というよりは、社内的な「顔の広さ」というような資質が重要になります。

#### 1.1.5 専門家・外部コンサルタント

事業者は、社内において（できれば専任の）要員を確保し、ISMS 構築を進めるべきです。しかし、「情報セキュリティ」の対象とする範囲は、「IT 技術」から「経営的な判断」「ビジネスへの理解」と多岐にわたります。また、これら領域をバランスよく俯瞰的に見通すスキルが求められます。原則的に、会社の業務はその会社で業務についている人が一番知っているものですが、時として非常にミクロな視点での判断に終始してしまうことが多くあります。基準においても言及されている、外部の専門家・コンサルタントの登用は、この判断にマクロな（俯瞰的）視点を与え、また最新の情報を提供してくれる窓口の機能が期待されます。

#### 1.1.6 関係者への周知

情報セキュリティポリシーは、必要な関係者全員に周知される必要があります。情報セキュリティポリシーは、事業者において統一された内容で、関係者が等しく容易に理解できるよう、平易な文書で簡潔に記述される必要があります。

#### 1.1.7 定期的な見直し

事業者は、情報セキュリティポリシーを定期的に見直す必要があります。情報セキュリティポリシーの内容が、事業者が置かれている情報セキュリティ環境に適合しているか、また、ポリシーの対象者が遵守しているか等の視点から、定期的に見直す必要があります。

例えば、新たに業務を外部に委託する、情報システムが変更された等の時点で、当該業務のポリシーへの遵守状況を確認するとともに、ポリシー文書自体の形骸化、陳腐化に目を光らせる必要があります。

## 1.2 情報資産の洗い出し（「保護すべき情報資産」）

「情報資産の洗い出し」の目的は、事業者の情報資産及びその価値を明確にすることにあります。事業者がISMSを確立するには、まず、その対象となる情報資産を明確にする必要があります。情報資産一つひとつを明確にすることにより、ISMSの管理対象の詳細を把握し、適切な管理策を選択することが可能になります。また、情報資産を洗い出すことでその価値が明確化し、リスク評価の実施が可能となります。

事業者は、情報資産洗い出し作業の実施にあたり、洗い出しの対象、洗い出しの方法等を検討します。また、情報資産の重要度を決定するための基準についても検討し、決定する必要があります。これら、情報資産洗い出しの基準は、手順化し文書に残す必要があります。

### 1.2.1 洗い出しの対象

情報資産洗い出しは、原則的にISMSの適用範囲におけるすべての情報資産を対象に実施します。とはいえ、事業者にとって、網羅的な情報資産洗い出しは非常に負担が大きい作業になることは容易に想像できます。「情報のグループ化」は、作業負荷軽減と今後の分析作業を効率的に進めるために有効な考え方です。例えば、情報資産価値や属性（保管形態や保管期間、用途等）が一致するものを一つのグループとする等です。

### 1.2.2 情報資産の価値

グループ化された情報資産の価値を明確にするため、情報セキュリティの3要素「機密性」、「完全性」、「可用性」それぞれの観点から分析を行います。事業者は、「機密性」、「完全性」、「可用性」に関して、独自の判断基準を設ける必要があります。

以下に例を示します。

表 1-1 機密性の基準の例

資産価値	クラス	説明
1	公開	第三者に開示・提供可能
2	社外秘	組織内では開示・提供可能（第三者には不可）
3	秘密	特定の関係者または部署のみに開示・提供可能
4	極秘	所定の関係者のみに開示・提供可能

表 1-2 完全性の基準の例

資産価値	クラス	説明
1	低	情報の内容を変更された場合、ビジネスへの影響は少ない
2	中	情報の内容を変更された場合、ビジネスへの影響は大きい
3	高	情報の内容を変更された場合、ビジネスへの影響は深刻かつ重大

表 1-3 可用性の基準の例

資産価値	クラス	説明
1	低	1日の情報システム停止が許容される
2	中	業務時間内の利用は保証する 1時間の情報システム停止が許容される
3	高	1年365日、1日24時間のうち、99.9%以上利用できることを保証する 1分間以上の情報システム停止が許容されない

### 1.2.3 情報資産洗い出しの例

ISMSでは、情報資産の管理責任が明確にされている必要があります。グループ化された情報資産は、それぞれに管理責任者を決定する必要があります。

以下に例を示します。

表 1-4 情報資産洗い出し記入例

No	情報資産	管理責任者	情報資産の価値		
			機密性	完全性	可用性
1	顧客情報		4	2	1
2	契約書		3	3	1
3					

#### 【コラム】

##### < 明確にすべき情報資産の属性の例 >

(保管形態) 情報資産の保管されている状態

内容が同じ情報が複数種類の形態で保管されている場合、それら全てを明確にする

例:「紙の文書」,「メモ」,「ファイルサーバ」,「個人用 PC」,「FD」,「MO」,「録音テープ」,「ビデオテープ」等

(保管場所) 情報資産が通常保管されている場所

例:「キャビネット(鍵あり/なし)」,「書棚」,「個人の机の引出し」,「保管庫」,「外部委託倉庫」等

(保管期間) 情報資産を保管しておかなければならない期間

例:「～年 月 日」,「永久保管」等

(廃棄方法) 情報の廃棄方法

例:「シュレッダー」,「焼却」,「リサイクル」等

(用途) 情報資産の用途(用途が明確な場合は記入不要)

(利用者の範囲) 情報資産を配布する社員の範囲

あるいはその情報資産に対するアクセス権限を持つ利用者の範囲

例:「(役職名あるいは個人名)のみ」,「部署」,「社内限り」等

### 1.3 リスク評価（「要求される保証の度合い」）

事業者は、ISMS 構築のために、適用範囲内にある情報資産を洗い出し、その情報資産が持つ事業上の価値を明確にすることが必要です。さらに明確になった価値より、その情報資産が様々な脅威から保護されるべきであると判断した場合に、適切に保護できる環境を構築することが必要です。リスク評価（リスクアセスメント）は、このような必要性を満たす活動の第一歩です。

リスク評価の目的は、以下の事項を明確にすることです。

- (1)個々の情報資産の管理状況
- (2)及び存在する脅威
- (3)脅威に対して情報資産が持つ脆弱性
- (4)問題が発生した場合の事業上の影響度

ここでは、ISMS 構築のためのリスク評価の例として、「ギャップ分析」、「詳細リスク評価」の2段階で実施する場合の手順の概要を示します。

#### 1.3.1 ギャップ分析

ギャップ分析実施の目的は、本基準への準拠状況の把握にあります。ギャップ分析の実施は、一般的に推奨される管理のレベルと事業者の管理レベルの現状を比較し、「大きな差が認められる個所」、「明らかに管理策の適用を必要としている個所」、より詳細なリスクアセスメントが必要な個所等を明確にします。

ISMS の対象となるすべての情報資産は、ギャップ分析の対象です。分析は、情報資産一つひとつを個別にではなく、対象となる情報資産全体を一つの固まりと見て分析を実施します。ギャップの確認作業は、主に ISMS 構築の責任部署が主となり実施しますが、必要に応じて部門責任者や IT の管理者等に対してインタビューを実施します。

また、ギャップ分析では、網羅的に基準への準拠性を確認するために、基準の全項目に対して準拠状況を段階的に表現するチェックシート等を作成する必要があります。審査員は、このチェックシートをもとに、事業者における ISMS の管理状況の概況、問題の所在等を確認することが可能です。

### 1.3.2 詳細リスク評価

詳細リスク評価実施の目的は、前述のギャップ分析により発見された問題個所について、重大なリスクの存在を明らかにすることです。

詳細リスクアセスメントの対象は、ギャップ分析の結果、「基準に準拠していない」、「基準に一部準拠していない」と判断された個所のみとします。ギャップ分析では情報資産全体を一つの固まりとして評価しましたが、ここでは ISMS が対象とする情報資産のうち、準拠性が疑わしい基準項目に関連するものについて、情報資産ごとに評価を実施します。既に適切な管理策が適用されていると判断された基準項目については、詳細なリスクアセスメントは実施しません。また、基準項目の内容に該当するものがない場合には、管理策の項目自体をリスク評価の対象から除外します。

詳細リスク評価では、「情報の資産価値」、「脅威」、「脆弱性」、「リスク値」を数値で評価します。「リスク値」は「情報資産の価値の明確化」、「脅威分析」、「脆弱性分析」を行いこれらの結果から算出します。

#### (1) 情報資産の価値

情報資産の価値は、個々の情報資産が持つ「機密性」、「完全性」、「可用性」のそれぞれの視点から評価されます。これらの値は、情報資産洗い出し作業の際に明確にしているため、その結果を参照します。

#### (2) 脅威分析

脅威とは、情報セキュリティを要求される水準以下に引き下げる潜在的な要因をさします。

事業者は、情報資産に対する脅威を明確にするため、業務に関わる脅威に加えて一般的な脅威の例を合わせて検討する必要があります。一般的な脅威の例として『DISC PD3005 : 1999 (Guide on the selection of BS7799 controls)』の項目 2.2 「Security Concerns and BS7799 Controls」等があげられます。

事業者は、脅威の大きさを表すために独自の判断基準を設ける必要があります。

以下に、例を示します。

表 1-5 脅威の基準値例

脅威		
大きさ	クラス	説明
1	小	発生した場合でも、あまり大きな問題にはならない
2	中	発生した場合、問題になる
3	大	発生した場合、深刻かつ重大な問題に陥る

### (3) 脆弱性分析

脆弱性とは、情報資産や人員の管理方法に由来する弱点のことです。

事業者の実施する管理方法に問題があれば、弱点は大きく、脅威が表面化する可能性が高くなり、逆に、たとえ大きな脅威が存在したとしても適切な管理が実施されていれば、弱点が小さく、深刻な問題には陥らないことは容易に想定できます。脆弱性は、常に脅威と関連付けて検討する必要があります。脅威を完全に除去することは不可能ですが、脆弱性は適切な管理策を講じることにより大幅に低減させることが可能です。脆弱性の低減は、問題の発生を抑止し、結果的にリスクを減少させます。

事業者は、脆弱性の度合いを表すために独自の判断基準を設ける必要があります。

以下に、例を示します。

表 1-6 脆弱性の基準値例

脆弱性		
度合い	クラス	説明
1	低	適切な管理策が講じられていて安全である
2	中	管理策の追加等により改善の余地がある
3	高	全く管理策が講じられておらず脆弱である

(4) リスク値の算出

リスク値は、上記のプロセスにより明確になった「情報資産の価値」、「脅威の大きさ」、「脆弱性の度合い」を用いて、例えば、簡易的に以下の例のような式で算出します。

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

(例) 情報資産の種類：顧客情報（機密性：4、完全性：2、可用性：1）

脅威：3（情報が関係者外に漏洩した場合、信用の失墜に繋がる）

脆弱性：3（すべての作業担当者に特権が付与されていたので）

この場合のリスク値は、以下のようになります。

(a) 機密性に関わるリスク値： $4 \times 3 \times 3 = 36$

(b) 完全性に関わるリスク値： $2 \times 3 \times 3 = 18$

(c) 可用性に関わるリスク値： $1 \times 3 \times 3 = 9$

また、リスク値を算出し、以下の例のようなマトリクス、「リスク値早見表」を作成すると、以降の作業を効率的に進める助けになります。

表 1-7 リスク値早見表例

	脅威								
	1			2			3		
	脆弱性								
資産価値	1	2	3	1	2	3	1	2	3
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

## 1.4 リスク管理の原則（「要求される保証の度合い」）

リスク管理の目的は、リスク評価の作業で明確になったリスクを正確に把握し、そのリスクに対する適切な対処方法を決定することです。対処法は、存在するリスクについて、そのリスクが持つ大きさや特徴により判断します。ここでは、「リスク許容」、「リスク軽減」、「リスク移転」、「リスク回避」の4通りの方法を紹介します。

### 1.4.1 リスク許容

リスク許容とは、リスク評価の結果、存在するリスクのうち影響の少ないものを許容することです。リスクを許容した場合、そのリスクについてそれ以上の管理策を講じないことも考えられます。

例えば、リスク許容値は以下の例のような一覧表になることが考えられます。

表 1-8 リスク許容一覧の例(1)

	脅威								
	1			2			3		
	脆弱性								
資産価値	1	2	3	1	2	3	1	2	3
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

リスクを許容できる範囲       リスクに対して何らかの対策を講じる範囲

表 1-8 リスク許容一覧の例(1)では、たとえ資産価値が最低の「1」でも、脅威と脆弱性の視点からそれぞれが最大の値「3」をとる場合には無条件に対策をとらなければいけないと考えた場合、許容の水準はリスク値が「9」未満と決定できます。リスク評価作業の際に作成したリスク値のマトリクス（「リスク値早見表」）で、リスク値が「9」未満のものについては、現状の管理を許容し、許容したリスクについては「残余リスク」として管理することとしました。

表 1-9 リスク許容一覧の例(2)

	脅威								
	1			2			3		
	脆弱性								
資産価値	1	2	3	1	2	3	1	2	3
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

 リスクを許容できる範囲       リスクに対して何らかの対策を講じる範囲

また、表 1-9 リスク許容一覧の例(2)では、情報資産の価値が最大の「4」であれば無条件に対策をとるべきであるということで、リスク値の許容水準は「4」未満となります。

このリスク許容一覧は、あくまでリスク評価実施時のリスク環境をあらわすもので、情報資産の資産価値や脅威、脆弱性等の環境に変化が生じた場合は、適宜リスク値の見直しを実施しなければなりません。

#### 1.4.2 リスク低減

リスク低減とは、本基準の管理策を適用することにより、リスクを減少させることです。

リスク評価の結果、リスク値が許容水準以上のものについては、可能な限りリスクを低減するよう管理策の適用を検討します。(その場合でも、リスク低減を図る管理策の適用により業務に支障をきたすことがないよう、無理のない管理策の適用や、利用者への遵守を要求する必要があります。)

#### 1.4.3 リスク移転

リスク移転とは、保険等の利用によりリスクを他者(他社)に移すことです。

情報システムの運用を他者(他社)に外部委託する場合、契約等により自社のリスクを損害賠償等の形で移転してしまうことも、このリスク移転に相当します。

リスク管理上は、本基準の管理策を適用できない場合や、適用してもリスク値が許容水準以上の場合、リスク移転を検討します。例えば、地震等の不可避な脅威について、事業に与える影響は大きいですが、比較的発生する可能性が低いので保険の利用を検討する等ということが相当します。

#### 1.4.4 リスク回避

リスク回避とは、脅威発生の要因を停止あるいは全く別の方法に変更することにより、リスクが発生する可能性を取り去ることです。

例えば、業務プロセス A のリスク値が大きい場合、業務プロセス A を廃止してしまえば、業務プロセス A に関わるリスクは完全に除去したことになります。リスク管理上は、本基準の管理策を適用できない場合や、適用してもリスク値が許容水準以上の場合、リスク移転ができない場合等はリスク回避を検討する必要があります。

## 1.5 ISMS の構築

本基準には、この ISMS 構築の作業について「枠組みの確立」として 6 つの要求事項が定められています。

### 第3 ISMSの要求事項

#### (2) マネジメント枠組みの確立

管理目的及び管理策の内容を明確にすること。

の目的及び内容を文書化するために以下の作業を実施すること。

(ア) 情報セキュリティポリシーの策定

(イ) ISMSの対象範囲の決定

(ウ) リスク評価

(エ) リスクマネジメントの対象範囲の決定

(オ) 管理策の選択

(カ) 適用宣言書の作成

の各項目について、定期的もしくは必要に応じて見直しすること。

#### 1.5.1 ここまでの説明と基準との整合

基準((2))の(ア)~(ウ)で、ISMSの対象範囲を決定し、その内包するリスクを分析します。具体的には、情報セキュリティの基本的な方針を明文化したセキュリティポリシーを策定し((ア)、(イ))、管理対象の情報資産についてそのリスクを分析・評価((ウ))の作業を実施します。リスク評価の結果、管理するリスクが決定されます。

## 1.5.2 マネジメントシステムの構築

本制度では、マネジメントシステムの構築を「6ステップ」の作業で説明しています。

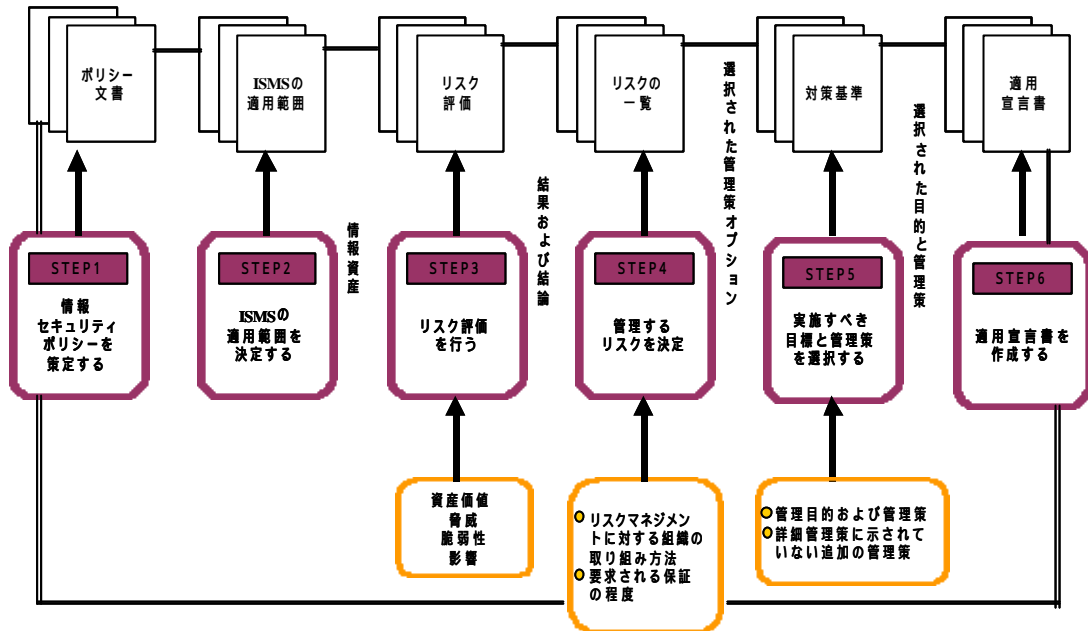


図 1-2 標準的な ISMS 構築のスキーム

各ステップは、第3 ISMSの要求事項(2) マネジメント枠組みの確立 の6つの項目(ア)~(カ)に対応しています。

### (1) 管理するリスクの決定

STEP1~4については、先に説明したとおりです。次のSTEP5については、管理対象となるリスクについて基準より管理策を選択し対策基準を策定します。

### (2) 対策基準について

対策基準は、ISMSを実行に移すための具体的管理策をまとめた文書です。STEP5の「実施すべき目標と管理策を選択する」とは、対策基準書を策定しISMS構築を実施段階に移すための重要な過程です。

## 【コラム】

### < 対策基準の項目例 >

対策基準には、以下のような項目が含まれます。

セキュリティ組織	: 情報セキュリティ委員会や情報資産に対する責任等
情報の取り扱い	: 情報の重要度区分と重要度に応じた管理方法等
人的セキュリティ	: 派遣社員やアルバイトの管理、ユーザへのセキュリティ訓練等
物理的セキュリティ	: 情報システムの設置条件や付帯設備等
運用管理	: 運用手順や責任、システム計画の作成、媒体の取り扱い等
アクセス制御	: ユーザの責任、ネットワーク、OS、アプリへのアクセス制御等
システム開発・保守	: システムのセキュリティ要求事項等
事業継続計画	: 障害や事故が発生した際の計画等
準拠（コンプライアンス）	: 法的要求事項への準拠や、システム監査等

### (3) 対策基準の項目選定

対策基準の内容は、本基準の項目を参照し、網羅性を意識したものでなければなりません。また、事業者固有のリスクを勘案し、業界標準となっているドキュメント等を参照し、独自のものを策定する必要があります。

### (4) 管理策選択にあたり考慮すべき事項

管理策の選択にあたっては、例えば、以下のような制限事項に留意する必要があります。

- (a) 時間的制限 : 選択した管理策が現実的な時間内に実行できるか
- (b) 財務上の制限 : 管理策のコストと保護すべき資産の価値がバランスしているか
- (c) 技術上の制限 : 選択した管理策が技術的に適用可能か
- (d) 社会的な制限 : 事業者の企業文化に馴染むか
- (e) 環境上の制限 : 地理・気候条件等が影響しないか
- (f) 法律上の制限 : IT関連の法律以外も考慮しているか

これらの制限事項を考慮することが、実効性のある管理策の選択につながります。

(5) 適用宣言書

STEP6では、適用宣言書を作成します。適用宣言書には、実行すべき管理目的及び管理策を記載します。

STEP3「リスク評価」及びSTEP4「管理するリスクを決定する」作業の結果を踏まえ、なぜそれらの管理目的及び管理策を選択したかの理由を明らかにします。さらに、適用宣言書には、どの基準項目が適用可能でないか、またなぜそれらが選択されなかったかの理由についても明記します。

## 1.6 継続性の確保

ISMSの適正さは、運用の記録によってのみ証明されるといっても過言ではありません。

事業者は、本基準の要求事項に準拠していることを実証するために、必要な記録を決定し、適切に管理しなければなりません。

### 第3 ISMSの要求事項

#### (6) 記録

第3(1)から(5)の内容に対する遵守状況を保証するために必要な記録を特定すること。

において特定された記録を管理する手続きを明確にし必要に応じて見直すこと。

において特定された記録に対し、損傷、劣化、紛失、消失を防止するための措置を講ずること。

#### 1.6.1 運用の記録の例

ISMS運用の記録には、以下のような例があげられます。

- (1) 情報セキュリティ委員会の議事録
- (2) 情報セキュリティポリシー等の規程類
- (3) 訪問者の記録
- (4) マシン室の入退室の記録
- (5) 情報システムやサーバへのアクセス許可・拒否の記録
- (6) システム変更記録
- (7) 事故の記録
- (8) 監査記録

#### 1.6.2 適正な管理

すべての記録は、読みやすく、関係している活動が特定できるものでなければなりません。

記録は、取り出しが容易で、損傷や劣化、紛失、消去しない適切な管理が実施されていることが必要です。ここでいう適切な管理とは、保存および利用の明確な手続きを定め、これを実行することです。この手続きも、他のポリシー文書同様に定期的に見直され、必要に応じて改訂する必要があります。

## 【コラム】

### <記録の適正さ>

記録の適正さを検討する視点の例を以下に示します。

ISMS の運用の適正さを証明しているか

管理手続きが適正に定められているか

記録の保管、利用にあたり管理手続きが適正に遵守されているか

### 1.6.3 継続性の確保

事業者は、これら運用の記録を取得しそれを評価し、許容しているリスクが適切か、導入している管理策が適切か等を判断します。運用の記録は、ISMS 運用の結果の証明のみならず、ISMS の見直し、特にリスク評価の見直しの非常に重要なきっかけを与えます。ISMS は一度構築してしまえば終わりというものではありません、継続的に見直しを通してブラッシュアップしていく必要があります。

## 2. 審査のポイント

審査員は、事業者が構築する ISMS の「適用範囲」や「要求される保証の度合い」を理解し、リスク評価の結果に応じた管理策が選択されているかという視点から、事業者の作業を確認・評価します。また、事業者が想定しているリスクに対して、リスクマネジメントが適切な水準に維持されるよう、運用されているか確認しなければなりません。

従って、審査で重要なポイントは、単に、本基準の「第4 詳細管理策」の管理策を実施しているか否かというよりも、事業者が採用したリスク評価方法やリスク評価から得られた結果の有効性、妥当性にあります。リスクマネジメントが不十分であるとき、「なぜそうなってしまったのか」そこに行き着く過程（プロセス）を突き止めることが大切です。

そのため審査員は、管理策の選択過程とその導入・運用が適切な管理の元を実施されていることを客観的に示す実体や証跡（証拠文書、運用の記録）を確認し、事業者のリスクマネジメントに対する姿勢や判断結果が十分に反映された適切な内容であることを判断しなければなりません。

ここでは、「2.1 リスクマネジメントに関する審査上のポイント」と「2.2 選択された管理策に関する審査上のポイント」を示します。

## 2.1 リスクマネジメントに関する審査上のポイント

リスクマネジメントの審査は、運用管理面と組織管理面の2つのポイントがあります。

リスクマネジメントの運用管理面は、リスク評価のプロセスとその証拠の確認が重要となります。下記(1)～(6)の観点で、「2.1.1 リスクマネジメントの運用管理面」において、解説していきます。

- (1)情報資産の洗い出しと分類
- (2)現状の把握、ギャップ分析
- (3)脅威、脆弱性、重要度分析
- (4)リスク評価方法
- (5)管理策の選択
- (6)セキュリティポリシー（対策基準）及びプロシージャ（手順等）の内容

また、リスクマネジメントの組織管理面は、「日常の判断」、「事故発生時の対応」、「管理の見直し」等の観点からの確認が重要となります。下記(1)(2)の観点で、「2.1.2 リスクマネジメントの組織管理面」において、解説していきます。

- (1)リスクマネジメント実施の体制
- (2)その体制に従い決定された事項の承認過程

### 2.1.1 リスクマネジメントの運用管理面

審査員は、事業者のリスクマネジメントが ISMS の適用範囲およびセキュリティポリシーと矛盾することなく、すべての領域を網羅的にカバーしていることを確認する必要があります。リスクマネジメントは、情報セキュリティの基本方針や ISMS の適用範囲（「事業者の場所・規模」、「業務内容」、「利用されている技術」、「保護すべき情報資産とその価値」）との整合性が維持されていなければならない。審査員は、これらを考慮しながら事業者のリスクマネジメントの正当性を判断する必要があります。

リスクマネジメントの運用管理面について、下記(1)～(6)の観点で、解説していきます。

- (1)情報資産の洗い出しと分類
- (2)現状の把握、ギャップ分析
- (3)脅威、脆弱性、重要度分析
- (4)リスク評価方法
- (5)管理策の選択
- (6)セキュリティポリシー（対策基準）及びプロシージャ（手順等）の内容

## (1) 情報資産の洗い出しと分類

審査員は、事業者の構築する ISMS の適用範囲を正しく理解し、その範囲の情報資産の洗い出し作業について、作業の概要を正しく把握し、その網羅性を確認する必要があります。

適用範囲に関してはまず、その範囲が明確に定められていること、実現可能な範囲であること、境界線および接点が明確にされていることを確認します。明らかに、重要な情報資産が日常的に範囲の境界線を越えてやり取りされている場合、やり取りの当事者や内容によっては適用範囲を不当に狭く設定していると判断することもあります。

次に、適用範囲に関連する情報資産とは下記のような例が考えられます。

- (a) 物理的資産（コンピュータ・ハードウェア）、通信機器、施設・設備（電源設備、建物等）
- (b) 情報・データ（文書、データベース等）
- (c) ソフトウェア（アプリケーションソフトウェア、OS、開発ツール等）
- (d) 製品やサービス
- (e) 企業イメージ（企業の評判、信頼度等）
- (f) 人員（社員[利用者、運用管理者等]、顧客等）

事業者にとって、たとえ被害にあったとしても事業上大きな影響を受けない情報資産まで精緻に洗い出す必要はありませんが、IT 関連の情報資産にだけ注目し、人員または、人員が取り扱う情報を見落とさないように、対象の網羅性に留意する必要があります。

### 【コラム】

ISMS 認証基準 (Ver.0.8) の 6.(7) には「電子取引を行う場合、詐欺行為、契約紛争、不正な情報開示及び情報の改竄を防止するための措置を講ずること。」と規定されています。この場合の対策は、「暗号化」や「強固なアクセス制御」といった技術的な対策を講じるだけでなく、契約書や契約書に基づき業務を遂行する人員に対する教育等の非技術的な管理策を投じる必要性を示唆しています。人員の規範や言動、取り扱う情報を視野に入れた検討がなされていないと、万全な管理策が選択されないことがあります。

審査員は、洗い出された各々の情報資産の重要度を情報セキュリティの「機密性」、「完全性」、「可用性」の視点から適切に評価され、分類・階層化されていることを確認する必要があります。それぞれの事業者ごとに、重要度の判断基準は異なるので、事業者の業務内容を良く理解し、どこに判断の重点を置くのかを確認することが重要です。評価に用いられる分類基準（例えば、機密性に関しては「極秘」、「部外秘」、「社外秘」、「一般」等のレベル分け）は、事業者の設定を尊重しますが、その基準が決定されたプロセスが明示されている手順書等を確認する必要があります。また、依存関係の高い情報資産についての複合的な判断等、例外的な判断については、個別の情報資産洗い出しの結果を検証し、適切な分類がなされているか確認することも重要です。

#### 【コラム】

例：(情報資産 A,B が強い依存関係があるにもかかわらず、レベル分けが異なって認識されている)

A: 葉書や FAX 等で受付けた受注伝票

B: A を電子処理したデータ

情報資産	機密性	完全性	可用性
A	1	2	2
B	3	2	2

この場合、A,Bの機密性のレベルを高いレベルである機密性 = 3として分類する必要があります。

(Aの機密性は、1から3に変更すべきです)

## (2) 現状の把握、ギャップ分析

審査員は、情報資産の分類基準について、事業者が現状に沿った分析を実施し決定したことを確認します。事業者は現状把握のために、情報資産の管理責任者へのインタビュー実施や、さらに広い対象への情報資産の取り扱いに関するアンケートを実施しているはずです。また、管理の実績を示す情報システムのログや運用の記録等を保管しています。現状把握プロセスの適正さは、これらの議事録やアンケート集計結果、ログ・作業記録、手順書等から確認できます。

次に、情報資産の重要度に応じた取り扱いのあるべき姿と現状の乖離を確認します。情報資産は、保管場所や管理状態によって「現状」が大きく異なる場合があります。審査員は、同じ情報資産であっても、その保管場所等刻々と変化する情報資産の状態に応じた現状分析を事業者が実施したことを確認することも重要です。

### 【コラム】

例えば、顧客情報がアクセス制御されたサーバで保管されていても、それがその状態のまま変化しないで保管されていることはありません。利用者のパソコンや携帯端末等に一部または全部がダウンロードされたり、電子メールに添付されて配布されたりすることがあります。もしプリンタで印刷出力され、そのまま放置されれば持ち出すことは容易です。このような状態は、ISMS 認証基準 (Ver.0.8) の「5.(3) 離席時や帰宅時における、机上やその他の場所への情報の放置を禁止すること。」の項目に違反していることになります。

### (3) 脅威、脆弱性、重要度分析

洗い出された情報資産は、個別に「脅威」、「脆弱性」を分析し「リスクの度合い」が決定されます。この分析結果は、後のリスクマネジメントに大きな影響を与えます。審査員はこのことに留意し、事業者の分析のプロセスを確認する必要があります。個別の情報資産を識別していても、脅威、脆弱性、重要度（リスクの度合い）が正しく認識されていなければ、適切な管理策を適応することはできません。誤った認識のまま放置されると、対策にかかる投資がかさむばかりか、セキュリティの水準やシステム全体のパフォーマンス低下にもつながります。審査員は、事業者がその業務内容に沿って適切な分類を適用しているか等の視点から確認します。

#### 【コラム】

脅威は、「災害」、「人災」、「故障」等に分類されることがあります。

例えば、GMITS では脅威を以下のように分類しています。

脅威分類の例（GMITS）

人為的脅威		環境的脅威
意図的脅威	偶発的脅威	
盗聴	作業ミスや怠慢	地震
情報改竄	データ、ファイル削除	落雷
不正侵入、不正アクセス	ルーティング等の設定ミス	洪水
悪意のあるコード（ウイルス等）	機器の故障等	火災等
盗難等		

\* GMITS: ISO/IEC TR 13335 Guidelines for the management of IT Security

#### (4) リスク評価方法

審査員は、事業者が利用したリスク評価方法の妥当性や、その評価方法から導かれた結果の妥当性を確認する必要があります。

GMITSでは、リスク評価方法として、下記の4つの手法を紹介しています。

- (a) Baseline Approach (ベースラインアプローチ)
- (b) Informal Approach (非公式的アプローチ)
- (c) Detailed Risk Approach (詳細リスク分析)
- (d) Combine Approach (組合せアプローチ)

各々、メリット、デメリットがあり、例えば「Baseline Approach (ベースラインアプローチ)」の場合、セキュリティを一定水準に維持するため、広く採用されている一般的な対応策を詳細なリスク評価をすることなく選択します。それ故、事業者の業務やセキュリティ環境に固有のリスクが検討されていないことが容易に想像されます。例えばこの場合は、新たな技術の出現等による対策の陳腐化を、事業者自身が把握しづらいという問題があります。

審査員は、様々なリスク評価の手法の限界を理解し、事業者の採用した評価手法が適切であるか確認する必要があります。

また、継続性の面からも事業者が採用したリスク評価方法を評価します。あまりにも複雑なリスク評価方法は、リスク環境の変化に応じ、それが適宜再検証できるか確認しなければなりません。

## (5) 管理策の選択

セキュリティ管理策は、事業者が独自に実施した「情報資産の洗い出し」、「個別情報資産の重要度分析」、「リスク評価」作業の結果より「要求される保証の度合い」を決定し、選択されます。審査員は、これらの分析作業の過程と結果を理解し、事業者により選択されたセキュリティ管理策の正当性を確認する必要があります。その際、事業者が属する業界や業種、業務内容等の外的環境や、事業者の顧客からの要求等も勘案しなければなりません。

それぞれの管理策が、なぜ選択されたかを理解し、その管理策と関連するほかの管理策を確認し、（選択されていない管理策があれば）なぜ選択されなかったかを確認しなければなりません。そのために、審査員は、管理策の記述された文書そのものと、管理策策定の過程を確認するために議事録等の客観的証拠を用います。

次に、審査員は事業者が選択し、実装した管理策が適切に運用されているかを判断するために、運用の記録を確認します。運用の記録を審査する際は、下記の項目等を確認する必要があります。

- (a) 必要事項が記録されているか
- (b) 記録が、当該管理策の運用状況を把握するのに適当か
- (c) 記録自体の完全性が維持されているか
- (d) 記録が閲覧可能な状態に維持されているか
- (e) 記録を元に定期的に管理策の妥当性が確認されているか

### 【コラム】

例：

ISMS 認証基準 (Ver.0.8) の 4 . 詳細管理策 7 . ( 2 ) の 「 特権の割り当て及び使用を制限し管理すること。 」 という管理策を事業者が選択したにも関わらず、ある共有サーバのアクセスログを確認したところ、ログに記載されているユーザ名の殆どが ' root ' であり、アクセスされた日時は、記録には残っていないというような場合、上記の詳細管理策が正しく運用されていないだけでなく、ISMS 認証基準 (Ver.0.8) の 3 . ISMS の要求事項 ( 6 ) 記録 第 3 ( 1 ) から ( 5 ) の内容に対する遵守状況を保証するために必要な記録を特定すること、にも違反することになります。

(6) セキュリティポリシー（対策基準）及びプロシージャ（手順等）の内容

セキュリティポリシーは、リスク評価の結果から選択された管理策やセキュリティ要件が規程文書の形で反映され、その内容は、適切な組織によって承認を受けていることが重要です。従って、セキュリティポリシーの内容把握以外にも審査員は、上記事項を客観的な証拠から確認するために、事業者が採用している「承認プロセス」や、「セキュリティ委員会」のような場で、その内容が定期的に見直され、改訂を行うプロセスを明文化された規程文書等から確認する必要があります。

【コラム】

ISMS 認証基準(Ver.0.8)の4.詳細管理策10.(2)、では、「すべての手続きが情報セキュリティポリシーに準拠して実行されていることを定期的に見直すこと。」、「情報システムが情報セキュリティポリシー及び関連する対策基準や手順書等に準拠していることを定期的を確認すること。」とあります。

セキュリティポリシーの遵守状況の確認に関しては、確認のための体制（モニタリングおよび内部監査等）があり、セキュリティに関する規程が、関係者にトレーニング等で周知、教育、同意され、確実に遵守されているのかを確認する必要があります。

## 2.1.2 リスクマネジメントの組織管理面

事業者は、ISMS構築および維持のために、方針決定や手順等を承認するための委員会と、実際の管理運営を推進する部門を設置するべきです。

審査員は、それらの組織の業務内容や職務権限、人的構成等の妥当性を検証し、それらが承認されたうえで確実に課された役割が実施されていることを確認する必要があります。

リスクマネジメントの組織管理面について、下記(1)(2)の観点で、解説していきます。

- (1) リスクマネジメント実施の体制
- (2) その体制に従い決定された事項の承認過程

### (1) リスクマネジメントを実施するための組織

リスクマネジメントは、判断基準の確立および実施、見直しをするための管理フレームワークを確立することが重要です。

審査員は、事業者が定めた体制および、それらの業務内容、責任範囲、報告先、構成員等の妥当性を確認する必要があります。事業者の規模によっては、上記のような体制を確立することが困難または、専任的な人材を割り振れない等十分なフレームワークを確立できない場合があります。このような場合でも、審査員は、これらの事態が経営層に理解されたうえで、現状のフレームワークで採用されている体制やプロセスが承認されていることを確認する必要があります。

事業者は、下記の組織体制を確立することになります。

- (a) リスク評価方法の検討、決定、見直しを実施する体制
- (b) リスク評価作業を計画し、定期的実施する体制
- (c) セキュリティポリシーの検討、作成、改訂を実施する体制
- (d) 策定したセキュリティポリシーを周知させる体制
- (e) セキュリティ管理策を実装する体制
- (f) 実装した対策を維持、改良する体制
- (g) 実装した対策を監査する体制

### 【コラム】

ISMS 認証基準 (Ver.0.8) の 4 . 詳細管理策 2 . ( 1 ) では、「 経営陣が情報セキュリティについて検討する委員会を設置すること。」「 組織内の情報セキュリティを管理するため、関連する部門と横断的に調整する部門等を設けること。」「 監督官庁、規制当局及びセキュリティ上重要な役割を担う外部組織への連絡体制を維持すること。」とあります。

(2) (1)で決定された事項の承認プロセス

(1)で示されたフレームワーク及びフレームワークが決定した事項、特に責任範囲、報告先、担当業務内容等が経営層に理解され、承認されていることを確認する必要があります。審査員は、これらのことを議事録やセキュリティポリシー等の客観的証拠から確認します。

**【コラム】**

ISMS 認証基準(Ver.0.8)の4．詳細管理策2.(1)では、「 情報処理施設及び設備の新規導入に対する経営陣による承認の手順を確立すること。」、「 情報セキュリティポリシーの導入や運用の状況を客観的に見直すこと。」とあります。

## 2.2 選択された管理策に関する審査上のポイント

ここでは、代表的な本基準の第4 詳細管理策を選択して、想定できるリスクとの関連性を示し、関連付けられたリスクから審査時のポイントを示すことを目的としています。従って、事業者がISMSを構築する際、リスク評価からリスクを明確にし、そのリスクに対して対応策を選択するというプロセスの逆方向で考えられていることとなります。審査員は、事業者が選択した管理策から、その妥当性や運用状況を示す記録や文章を審査するわけですから、ここで用いた考え方を審査時に利用することは有効であると考えられます。

以下にここで用いる表のフォーマットを説明します。

なお、表で例示した脅威、脆弱性以外にも想定できる事項は存在しますが、選択された管理策とリスクの関係性を考察するのが目的で作成されているため、脅威、脆弱性等の各項目を例示するにあたり、網羅性を重視してはしません。

ISMS 認証基準(Ver.0.8) の第4 詳細管理策の大項目の番号と名称		
大項目内の中項目の番号と名称		
目的：詳細管理策の大項目に記述されている目的		
説明：詳細管理策の大項目に対する説明		
中項目の番号と名称		
中項目内の小項目の番号と名称の一覧		
	ISMS 認証基準(Ver.0.8)	対応する安対基準
基準項目	ISMS 認証基準(Ver.0.8) の「4章 詳細管理策」で記述されている管理策を記述しています。	左記管理策と対応する情報処理サービス業情報システム安全対策実施事業所認定基準（安対基準）を記述しています。
情報資産	「基準項目」(選択された管理策)の対象となり、かつ重要と思われる「情報資産」を列挙しています。	
脅威	「基準項目」に関して対象となり、かつ重要と思われる「脅威」を列挙しています。	
脆弱性	「脅威」を誘引する可能性が高く、かつ重要と思われる「脆弱性」を列挙しています。	
リスク	「基準項目」の対応策が十分施されていない場合に想定されるリスクで、かつ重大だと思われる「リスク」を列挙しています。	
審査ポイント	関連付けられたリスクから、想定可能な審査のポイントを列挙しています。	
証拠 (証拠文書)	「基準項目」に示された管理策の実施を示す客観的な証拠やその運用のための手順書等で、かつ重要だと思われる「証拠(証拠文書)」を列挙しています。	
関連事項 (基準項目)	「基準項目」に示された管理策に関連のあると思われる他の「基準項目」を列挙しています。審査時に不適個所を指摘する際、不適個所に最も関連性の強い管理項目を指摘することになりますが、それを判断するには関連する他の管理策を考慮し、全体を把握する必要がありますので、関連すると想定される他の「基準項目」を列挙しています。	

## 2.2.1 管理策例(1) セキュリティ組織

### 2. セキュリティ組織

#### (2) 第三者アクセスのセキュリティ

目的：第三者によってアクセスされる組織の情報処理施設/設備及び情報財産のセキュリティを維持すること。

- ・第三者による組織の情報処理施設/設備へのアクセスを管理すること。
- ・第三者による組織の情報処理施設/設備へのアクセスが業務上必要となる場合は、リスク評価を行い、セキュリティ関連事項及び管理要求事項を決めること。決められた管理策は第三者の同意を得て契約書等に明記すること。

#### (2) 第三者アクセスのセキュリティ

第三者に対し、組織の情報処理施設及び設備へのアクセスを許可する場合、事前にリスク評価を行い必要な措置を講ずること。

第三者に対し、組織の情報処理施設及び設備へのアクセスを許可する場合、セキュリティ要求事項を明記した正式な契約を締結すること。

情報システムの管理や制御を外部委託する場合、セキュリティ要求事項を明記した正式な契約を締結すること。

	ISMS 認証基準 (Ver.0.8)	安対基準
基準項目	2. セキュリティ組織 (2) 第三者アクセスのセキュリティ 第三者に対し、組織の情報処理施設及び設備へのアクセスを許可する場合、セキュリティ要求事項を明記した正式な契約を締結すること。	第1-2-(6)外部委託 1 情報システムの安全対策に関する項目を盛り込んだ契約を締結すること。 2 委託先における安全対策の実施状況を把握すること。
情報資産	<ul style="list-style-type: none"> <li>・施設(建物等)</li> <li>・情報処理設備(CPU、ディスク、電源、通信機器等)</li> <li>・対象となる設備に格納された情報または、それを媒体に複製したもの</li> </ul>	
脅威	<ul style="list-style-type: none"> <li>・許可されていない第三者のアクセス(不正なアクセス)</li> <li>・第三者の施設/設備の誤用</li> <li>・アクセスが許可されている第三者のセキュリティ規定違反</li> </ul>	
脆弱性	<ul style="list-style-type: none"> <li>・施設への第三者による入退館が管理されていないこと</li> <li>・施設内における第三者の行動に制限が加えられていないこと</li> <li>・アクセスが制限されている情報や区画について明確な表示がされていないこと</li> <li>・アクセスする第三者にセキュリティに関する規程等が周知されていないこと</li> <li>・第三者による情報資産に対するアクセス現場に事業者の責任者が立ち会わないこと</li> <li>・委託契約やSLA(Service Level Agreement)の不備により事業者のリスクが第三者に移転されていないこと</li> </ul>	

リスク	<ul style="list-style-type: none"> <li>・施設／設備の損壊や人為的な破壊等によるサービス停止</li> <li>・当該施設／設備の情報の持ち出し、改ざん</li> <li>・訴訟、損害賠償</li> </ul>
審査ポイント	<ul style="list-style-type: none"> <li>・第三者の定義（例：顧客、取引先、開発・運用・清掃・配送等の業務委託先）がなされているか</li> <li>・重要な情報処理施設、設備の洗い出し及びそのプロセスが確立されているか</li> <li>・当該施設／設備のセキュリティ対策（特に第三者のアクセス制限）が施されているか</li> <li>・当該施設／設備における情報が管理（特に第三者による複写、持ち出しの制限）されているか</li> <li>・当該施設／設備における第三者の情報へのアクセスログが管理されているか</li> <li>・バックアップが作成され、適切に保管されているか</li> <li>・障害復旧手順が確認（バックアップ設備等を含む）されているか</li> <li>・インシデントリカバリーの手順が確立されているか</li> <li>・重大なリスクに関する組織の危機管理体制との連携がとられているか</li> <li>・対象とする施設／設備および情報資産に関して有効な範囲が定義されているか</li> <li>・当該情報資産が適切に管理されているか（権限が明確化されているか）</li> <li>・対象者が明確にされ、かつ採用されているコントロールに実効性があるか</li> </ul>
証跡 (証拠文書)	<ul style="list-style-type: none"> <li>・ISMSの範囲に関する文書</li> <li>・情報セキュリティポリシー文書</li> <li>・情報資産の一覧（情報、重要度、管理責任者）</li> <li>・当該施設のセキュリティ対策に関する文書</li> <li>・リスク評価シート</li> <li>・委託契約のフロー</li> <li>・委託契約書、または契約書の雛型等</li> <li>・施設の入退館管理に関する規程</li> <li>・施設の入退館の記録</li> <li>・施設内のアクセス制限に関する規程</li> <li>・施設内のセキュリティドア等の利用記録</li> <li>・IDカード等の配布、再発行に関する規程（特に、ビジターカードや短期間の発行に関するものについて）</li> <li>・IDカード等の配布管理の台帳</li> <li>・情報資産のアクセスに関する規程、手順</li> <li>・情報資産アクセスの記録（閲覧、複写、持ち出し）</li> </ul>

<p>関連事項 (基準項目)</p>	<p>4章 詳細管理策</p> <p>3. 情報資産の分類及び管理  情報資産に対する責任  情報の分類</p> <p>4. 人的セキュリティ  (2) ユーザの教育・訓練</p> <p>5. 物理セキュリティ  セキュリティ区画  装置のセキュリティ</p> <p>9. 事業継続管理</p>
------------------------	---

## 2.2.2 管理策例 ( 2 ) アクセス制御

7 . アクセス制御
( 4 ) ネットワークのアクセス制御

目的：ネットワーク上のサービスを保護すること。
内部及び外部ネットワーク上のサービスへのアクセス制御を実施し、セキュリティ上の影響がないように管理すること。

<p>( 4 ) ネットワークのアクセス制御</p> <p>明確に許可されたサービス以外のサービスへのアクセスを防止するための措置を講ずること。</p> <p>情報システムのユーザがコンピュータの各サービスにアクセスする場合のネットワークの経路を制御すること。</p> <p>情報システムに対する遠隔地からのアクセスを許可する場合、ユーザ認証を行うこと。</p> <p>遠隔地のコンピュータに対するアクセスを許可する場合、接続の認証を行うこと。</p> <p>診断用の通信ポートへの許可されないアクセスを防止するための措置を講ずること。</p> <p>情報システムに対する許可されないアクセスを防止するため、ネットワークを適切に分離すること。</p> <p>共有ネットワークへのアクセス権限は、第 4 7 ( 1 ) のアクセス制御ポリシーに従い付与されること。</p> <p>共有ネットワークへのアクセスを許可する場合、第 4 7 ( 1 ) のアクセス制御ポリシーに基づき、可能な限り経路を制御すること。</p> <p>ネットワークに関連する外部のサービスを受ける場合、そのサービスに施されたセキュリティに関する情報を入手し、これを文書化すること。</p>
--

	ISMS 認証基準 ( Ver . 0 . 8 )	安対基準
基準項目	7. アクセス制御 (4) ネットワークのアクセス制御 診断用の通信ポートへの許可されないアクセスを防止するための措置を講ずること。	特に該当する基準はない。
情報資産	<ul style="list-style-type: none"> <li>・ リモートで診断等の運用保守を行っている設備および設備上で稼動している業務サービス</li> <li>・ リモート運用保守の権限内でアクセスできる情報</li> </ul> <p>* リモートで行う運用保守業務を行っている場合もしくは緊急用として、リモートの運用保守ラインを持っている場合を想定。</p>	
脅威	<ul style="list-style-type: none"> <li>・ 無許可の通信ポート利用</li> <li>・ 誤用</li> <li>・ 成りすまし ( 盗聴 )</li> </ul>	

脆弱性	<ul style="list-style-type: none"> <li>・利用者認証の不備 リモート接続用IDの共用 アクセス可能な接続元(ソース)の制限の不備</li> <li>・利用可能サービス(例:モニタリング)の制限の不備</li> <li>・SLA(Service Level Agreement)の不備(運用保守をアウトソーシングしている場合)</li> </ul>
リスク	<ul style="list-style-type: none"> <li>・無許可アクセスによるデータの改ざん、破壊</li> <li>・無許可アクセスによるデータの参照、複写</li> <li>・無許可アクセスによるサービス停止による評判低下</li> <li>・サーバを支配される、または第三者に対して攻撃を向けるような踏み台にされる</li> <li>・訴訟</li> </ul>
審査ポイント	<p>関連する施設、設備の物理対策はとられているか</p> <ul style="list-style-type: none"> <li>・ベンダーも含めた運用管理体制(連絡体制)は、明確になっているか</li> <li>・診断ポートの使用の承認と記録を保持する仕組みがあるか</li> <li>・診断ポートの利用制限や権限が明確であるか</li> <li>・サーバ、ネットワーク機器のモニタ(生死、パフォーマンス、ディスク容量等)に限定しているか 管理者権限、設定の更新権限、データベースの操作を制限しているか 運用保守対象のサーバ、ネットワーク機器等のみアクセスを制限しているか (他のセグメントへのルート制限等も含む)</li> <li>・利用者認証機能はどのように強化しているか(ワンタイムパスワード、コールバック、発信者番号通知等)</li> <li>・保守作業者は明確になっているか(ベンダーから台帳を入手しているか)</li> <li>・台帳は、最新の状態にアップデートされているか</li> <li>・IDは一意に付与されているか</li> <li>・運用保守管理マニュアルはあるか</li> <li>・要員教育は実施されているか(ベンダー要員も含む)</li> <li>・作業記録をベンダーから入手しているか</li> <li>・ベンダーの作業場所におけるセキュリティ要件が契約書等に含まれているか</li> <li>・ベンダーの作業場所に対し監査権限があることが契約書等に明記されているか</li> <li>・損害賠償等の項目が、契約書等に明記されているか</li> <li>・運用保守に含まれる対象機器と運用保守の内容が明確であるか</li> <li>・運用保守に含まれるセキュリティ対策に実効性があるか</li> <li>・ベンダーとの契約内容が明確であり、実効性があるか</li> </ul>
証跡 (証拠文書)	<ul style="list-style-type: none"> <li>・運用保守方法およびセキュリティ対策の資料</li> <li>・運用保守マニュアル</li> <li>・ベンダー保守契約</li> <li>・保守作業者の台帳</li> <li>・作業記録</li> <li>・教育履歴</li> </ul>

関連事項 (基準項目)	4章 詳細管理策 7. アクセス制御 (4) ネットワークのアクセス制御
----------------	--

## 2.2.3 管理策例（3）事業継続管理

### 9．事業継続管理

#### （1）事業継続管理

目的：事業活動に対する障害に対処すること。また、重大な故障又は災害の影響から重要なビジネスプロセスを保護すること。

災害及びセキュリティ故障（自然災害、事故、装置の故障及び故意による行為等の結果）による事業の中断を、予防管理策と回復管理策の組合せによって許容されるレベルに抑えること。

#### （1）事業継続管理

組織全体に亘る事業継続を開発、維持するための管理手順を整備すること。

事業継続に取り組むため、リスク評価に基づいた戦略計画を策定すること。

重要な業務に障害または故障が発生した際に事業を維持し遅延なく復旧させるため、必要な計画を立案すること。

すべての計画の整合性を保ち、計画の試験と整備の優先順位を明確にするため、事業継続計画全体の枠組みを維持すること。

事業継続計画を定期的に試験し見直すこと。

	ISMS 認証基準 (Ver.0.8)	安対基準
基準項目	4章 9.事業継続管理 (1) 事業継続管理 重要な業務に障害または故障が発生した際に事業を維持し遅延なく復旧させるため、必要な計画を立案すること。	第2 - 2 - (2)情報システムの運用管理 1 情報システムの操作方法、障害発生時の対応方法について定めたマニュアルを常備すること。 第2 - 2 - (4)電源設備、空気調和設備、防災設備及び防犯設備の管理 1 関連設備の取扱い方法、障害発生時の対応方法について定めたマニュアルを常備すること。
情報資産	<ul style="list-style-type: none"> <li>・ 情報処理機器（CPU、ディスク、電源、通信機器等）</li> <li>・ 対象の設備に格納された情報または、それを媒体に複写したもの</li> <li>・ アプリケーション（基幹系アプリケーション、ECアプリケーション等）</li> <li>・ 災害時復旧計画書、緊急時対応計画書等</li> <li>・ 復旧に必要な施設（復旧のための通信機器や建物等）</li> </ul>	

脅威	<ul style="list-style-type: none"> <li>・DOS:Denial of Service（サービス拒否攻撃）、DDOS:Distributed Denial of Service（分散サービス拒否攻撃）等の攻撃</li> <li>・ウイルス感染</li> <li>・不正アクセス</li> <li>・運用の誤用</li> <li>・停電</li> <li>・機密情報の漏洩、改ざん、消去</li> <li>・サービスの停止</li> <li>・バックアップの不備（バックアップデータの内容、バックアップ用の設備、バックアップを利用するために必要なアプリケーション等）</li> <li>・スタッフの不備</li> <li>・災害、地震</li> </ul>
脆弱性	<ul style="list-style-type: none"> <li>・ウイルスチェック等の対応策がとられていないこと</li> <li>・施設への入退館が管理されていないこと</li> <li>・明確な運用手順書が準備されていないこと</li> <li>・復旧に関する規程等が周知されていないこと</li> <li>・復旧のためのテストを行っていないこと</li> <li>・復旧テストの項目の確認を行っていないこと</li> <li>・復旧テストを定期的に見なおしていないこと</li> <li>・遠隔地にバックアップ設備を設けていないこと</li> <li>・遠隔地に復旧に必要な書類のコピーが用意されていないこと</li> <li>・復旧に必要な人材が確保されていないこと</li> </ul>
リスク	<ul style="list-style-type: none"> <li>・施設／設備の損壊や人為的な破壊等によるサービス停止、評判低下</li> <li>・事業が復旧できない、倒産</li> <li>・訴訟、損害賠償</li> </ul>

<p>審査ポイント</p>	<ul style="list-style-type: none"> <li>・ 重要な業務の洗い出し及びそれらの業務に関連した情報資産の洗い出し及びそのプロセスが確立されているか</li> <li>・ 当該施設 / 設備のセキュリティ対策が施されているか</li> <li>・ 当該施設 / 設備における情報の管理は適切に行われているか</li> <li>・ 当該施設 / 設備における情報へのアクセスログは、適切に管理されているか</li> <li>・ バックアップが作成され、適切に保管されているか</li> <li>・ 復旧手順の確認（バックアップ設備等を含む）が行われているか</li> <li>・ 復旧テストの確認が行われているか</li> <li>・ 復旧計画が承認されているか</li> <li>・ インシデントリカバリーの手順が作成、見直されているか</li> <li>・ 社内及び社外の危機管理体制との連携がとられているか</li> <li>・ 当該システムの二重化を実施しているか</li> <li>・ 対象とする情報資産に関して有効な範囲が定義されているか</li> <li>・ 対象とする情報資産と他情報資産の依存性が十分検討されているか</li> </ul> <p>（ * 対象となる情報資産に着目する一方、それらが依存する他の情報資産が考慮されていない場合が多い⇒結論として復旧できない）</p> <ul style="list-style-type: none"> <li>・ 当該情報資産が適切な管理のもとにあるか（権限の明確化）</li> <li>・ バックアップされるデータの内容、保管期間等が十分議論され、経営陣に報告されているか</li> <li>・ 復旧のためのテストをしているか</li> <li>・ 対象者が明確にされ、かつ採用されているコントロールに実効性があるか</li> <li>・ 承認されたテスト結果に基づき、復旧の手順が見なおされているか</li> <li>・ 過去の事態に基づき、復旧の手順が見直されているか・サービス提供している場合、契約書等にサービス停止等に関する免責を明記しているか（SLA[Service Level Agreement]）</li> </ul>
<p>証跡 (証拠文書)</p>	<ul style="list-style-type: none"> <li>・ ISMSの範囲に関する文書</li> <li>・ 情報セキュリティポリシー文書</li> <li>・ 情報資産の一覧（情報、重要度、管理責任者）</li> <li>・ 当該施設のセキュリティ対策に関する文書</li> <li>・ リスクアセスメントシート</li> <li>・ 災害時復旧計画書、緊急時対応計画書等</li> <li>・ 災害時復旧計画、緊急時対応計画に対する承認書</li> <li>・ バックアップに関する規程、手順書等</li> <li>・ 復旧テストの記録</li> <li>・ 事故報告書（インシデントレポート）</li> <li>・ 当該システムのアクセス制限に関する規程</li> <li>・ 情報資産のアクセスに関する規程、手順書等</li> <li>・ 委託契約書やSLA(Service Level Agreement)</li> </ul>

<p>関連事項 (基準項目)</p>	<p>4章 詳細管理策</p> <p>1. 情報セキュリティポリシー (1) 情報セキュリティポリシー</p> <p>2. セキュリティ組織 (1) 情報セキュリティ・インフラストラクチャ</p> <p>3. 情報資産の分類及び管理 (1) 情報資産に対する責任 (2) 情報の分類</p> <p>4. 人的セキュリティ (2) ユーザの教育・訓練 (3) セキュリティ事故及び誤動作への対処</p> <p>5. 物理的セキュリティ (1) セキュリティ区画 (2) 装置のセキュリティ</p> <p>6. 通信及び運用管理 (1) 運用手順及び責任 (2) システム計画の作成及び受け入れ (4) 情報システムの管理 (5) ネットワークの管理</p> <p>7. アクセス制御 (1) アクセス制御に関する事業の要求事項 (2) ユーザアクセス管理 (3) ユーザの責任 (4) ネットワークのアクセス制御 (5) オペレーティングシステムのアクセス制御 (6) アプリケーションのアクセス制御 (7) システムアクセス及びシステム使用の監視</p> <p>8. システムの開発及びメンテナンス (1) システムのセキュリティ要求事項 (2) アプリケーションシステムのセキュリティ (3) 暗号による管理策 (4) システムファイルのセキュリティ (5) 開発及びサポートプロセスにおけるセキュリティ</p> <p>10. 準拠 (2) セキュリティポリシー遵守状況の確認</p>
------------------------	---

## 2.2.4 管理策例（４）準拠

10. 準拠
（２）セキュリティポリシー遵守状況の確認

目的：組織のセキュリティポリシー及び規格への準拠を確実にすること。
情報システムのセキュリティは、定期的にレビューを実施し、見直しを行うこと。

<p>（２）セキュリティポリシー遵守状況の確認</p> <p>すべての手続きが情報セキュリティポリシーに準拠して実行されていることを定期的に見直すこと。</p> <p>情報システムが情報セキュリティポリシー及び関連する対策基準や手順書等に準拠していることを定期的確認すること。</p>
--

	ISMS 認証基準 (Ver.0.8)	対応する安対基準
基準項目	<p>10. 準拠</p> <p>（２）セキュリティポリシー遵守状況の確認</p> <p>すべての手続きが情報セキュリティポリシーに準拠して実行されていることを定期的に見直すこと。</p>	<p>第 2 - 4 情報システムに係る監査</p> <p>(1) 情報システムの安全対策に係わる監査を実施すること。</p>
情報資産	適用範囲内のすべての情報資産	
脅威	すべての脅威	
脆弱性	すべての脆弱性	
リスク	<ul style="list-style-type: none"> <li>・ ビジネスの障害 <ul style="list-style-type: none"> <li>経営層が誤った認識をもつことによる訴訟、評価の低下</li> <li>従業員のセキュリティに対するモラルの低下</li> <li>効率性の低下</li> </ul> </li> <li>・ ポリシーの形骸化</li> <li>・ その他多くの項目が考慮される</li> </ul>	
審査ポイント	<ul style="list-style-type: none"> <li>・ ISMS 遵守確認のための内部監査（以下 ISMS 内部監査）組織、リソース、能力の確認 <ul style="list-style-type: none"> <li>ISMS 内部監査についての責任と権限は明確になっているか（４章 4.(1)）</li> <li>ISMS 内部監査は全社の内部監査の一環として行われ、整合性がとれているか</li> <li>組織及び構成員は被監査部門から独立（形式面のみならず、実態面としても）しているか</li> <li>ISMS 内部監査のための要員数は組織の規模、業務の複雑性と比較して適切な人員か</li> <li>ISMS 内部監査要員の能力は、業務の複雑性、専門性と比較して適切か</li> <li>ISMS 内部監査要員に対する教育は十分に行われているか</li> </ul> </li> </ul>	
（続く）		

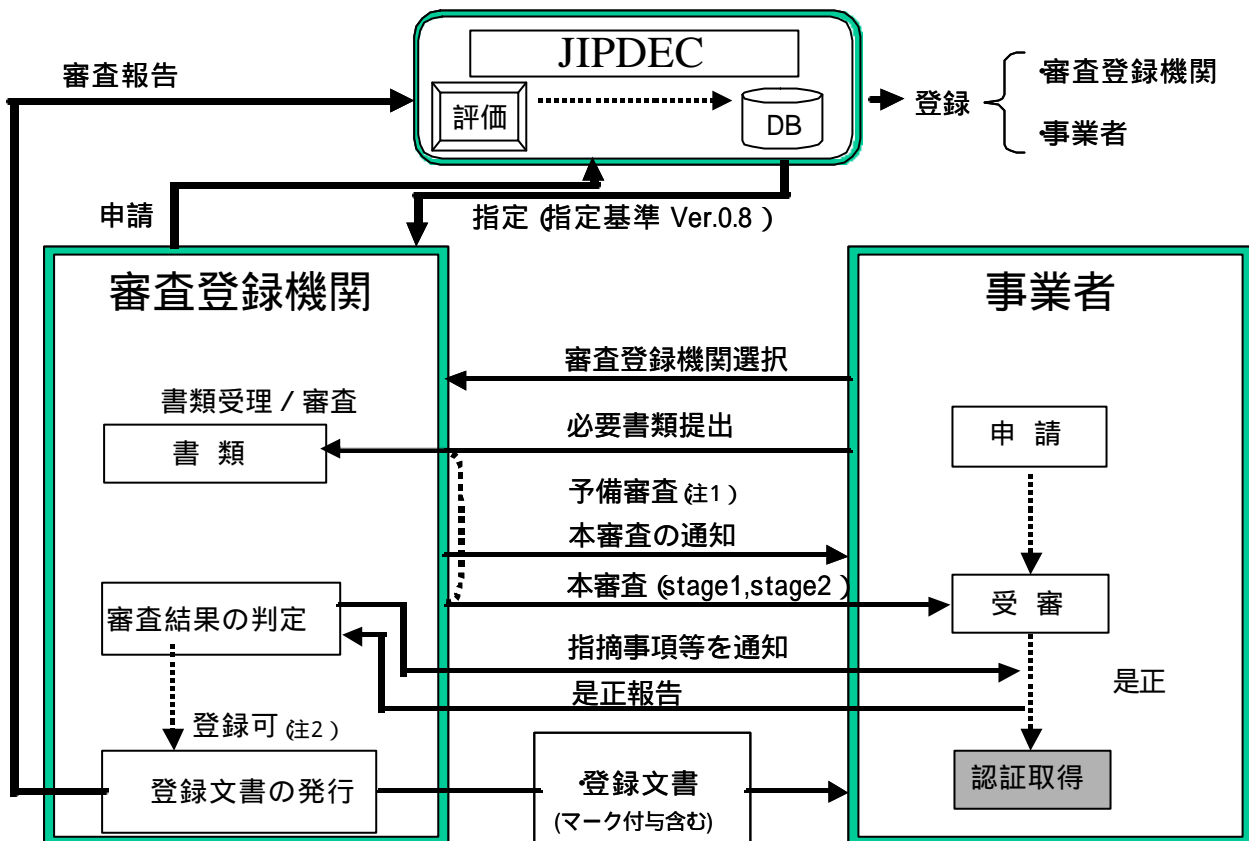
<p>( 続き )</p> <p>審査ポイント</p> <p>( 続く )</p>	<ul style="list-style-type: none"> <li>・ 外部専門家を ISMS 内部監査に利用する場合に特有の評価ポイント <ul style="list-style-type: none"> <li>外部の専門家を ISMS 遵守確認のための内部監査に利用している場合、選定にあたり専門能力について適切な評価を実施しているか</li> <li>外部の専門家を ISMS 遵守確認のための内部監査に利用している場合、秘密保持契約を締結しているか ( 4 章 2. (2) 参照 )</li> </ul> </li>   <li>・ ISMS 内部監査に関する規程の整備状況の確認 <ul style="list-style-type: none"> <li>ISMS 内部監査に関する規程は整備されているか、その内容の網羅性等は適切か</li> <li>ISMS 内部監査に関する手順書は整備されているか、その内容の網羅性等は適切か</li> <li>ISMS 内部監査のために必要なチェックリストは整備されているか</li> <li>ISMS 内部監査に必要な様式 ( 報告書、調書作成書等の様式は整備されているか</li> </ul> </li>   <li>・ ISMS 内部監査計画の内容の確認 <ul style="list-style-type: none"> <li>全社の内部監査の計画と ISMS 内部監査計画は整合しているか</li> <li>ISMS 内部監査の頻度は適切か</li> <li>ローテーションによる監査を実施している場合、ローテーション計画は適切か</li> <li>ISMS 内部監査計画は、リスク評価の結果及び組織体の長、情報セキュリティについての最高責任者、全社の内部監査の責任者等、情報セキュリティポリシーで決められたの意向等が反映されているか</li> <li>ISMS 内部監査の計画は情報セキュリティについての最高責任者等の適切な責任者によって承認されているか</li> </ul> </li>   <li>・ ISMS 内部監査実施内容の確認 <ul style="list-style-type: none"> <li>監査は監査計画に基づいて実施されているか</li> <li>ISMS 内部監査が定期的に実施されているか</li> <li>監査の実施のために必要なツール等は適切に利用されているか</li> <li>監査のサンプルの抽出方法、サンプル数、その評価は適切か</li> <li>分析的な手法を利用している場合、分析手法、その評価は適切か</li> <li>監査の実施結果は監査調書として文書化され、整理され、保存されているか</li> <li>3 章 ( (4)(5)(6) 参照 )</li> <li>監査調書は適切にレビューされているか</li> </ul> </li>   <li>・ ISMS 内部監査報告書の確認 <ul style="list-style-type: none"> <li>監査報告書は監査結果に基づいて作成されているか</li> <li>監査報告書は適切に承認されているか</li> <li>監査報告書は遅滞なく情報セキュリティについての最高責任者等の適切な責任者に報告されているか</li> </ul> </li> </ul>
---	--

<p>( 続き ) 審査ポイント</p>	<ul style="list-style-type: none"> <li>・ 監査結果の反映</li> <li>    監査結果に基づき、被監査部門は適切な改善案を立案しているか</li> <li>    被監査部門の改善案は承認され、実施されているか</li> <li>    ISMS 内部監査組織は改善案の進捗を把握しているか</li> </ul>
<p>証跡 ( 証拠文書 )</p>	<ul style="list-style-type: none"> <li>・ 情報セキュリティポリシー文書</li> <li>・ 監査報告書</li> <li>・ 監査調書</li> <li>・ ISMS 内部監査に関する規程 ( セキュリティが遵守されていることを確実にするための規程 )</li> <li>・ ISMS 内部監査の手順書</li> <li>・ ISMS 内部監査のためのチェックリスト</li> <li>・ ISMS に関する各種規程、手順書、チェックリスト等</li> </ul>
<p>関連事項 ( 基準項目 )</p>	<p>3 章 ISMS の要求事項</p> <p>    ( 2 ) マネジメント枠組みの確立</p> <p>4 章 詳細管理策</p> <p>    2 . セキュリティ組織</p> <p>        ( 1 ) 情報セキュリティ・インフラストラクチャ</p> <p>    4 . 人的セキュリティ</p> <p>        ( 1 ) 職務定義および採用におけるセキュリティ</p> <p>    9 . 事業継続管理</p> <p>        ( 1 ) 事業継続管理</p> <p>10 . 準拠</p> <p>    セキュリティポリシー準拠状況の確認</p> <p>    システム監査の考慮事項</p>

### 3. 審査プロセスについて（参考）

本章では、ISMS 適合性評価制度パイロット事業の枠組みと審査のプロセスについて記述しています。

#### 3.1 ISMS 適合性評価制度パイロット事業の枠組み



(注1) : 審査登録機関の事情により省くことができる（事業者のオプション）。また行われるタイミングは審査機関によって異なる。  
 (注2) : 審査登録後は、定期的なサーベイランス及び更新審査が実施される。

#### 審査登録機関の選択

パイロット事業者は、パイロット審査登録機関を選択し、審査登録業務契約(認証契約)を締結する。

#### 必要書類提出

パイロット事業者は、申請のための必要書類をパイロット審査登録機関に提出する。

#### 書類受理 / 審査

パイロット審査登録機関は、パイロット事業者からの提出書類を受理 / 審査する。

#### 予備審査

パイロット審査登録機関は、パイロット事業者に対し予備審査を実施する。ただし、予備審査は事業者のオプションであり、パイロット審査登録機関の事情により省くことができる。

#### 本審査の通知

パイロット審査登録機関は、本審査の実施予定等をパイロット事業者へ通知する。

#### 本審査

パイロット審査登録機関は、パイロット事業者に対し本審査を実施する。ただし、当協会の立会い審査を含む場合もある。

#### 指摘事項等の通知

パイロット審査結果により指摘事項等があれば、パイロット事業者へ通知する。

#### 是正措置

パイロット事業者は、指摘事項等を基に ISMS の是正措置をする。

#### 是正報告

パイロット事業者は、パイロット審査登録機関に対し是正報告をする。

#### 登録文書の発行

登録可の場合は、パイロット審査登録機関は、パイロット事業者に対して登録文書(マーク付与を含む)を発行する。

#### 審査報告

パイロット審査登録機関は、当協会に対しパイロット審査結果の報告をする。

尚、詳細については、以下の文書を参照してください。

- ISMS 適合性評価制度パイロット事業実施要領  
(<http://www.isms.jipdec.or.jp/doc/ismspilot.pdf>)
- ISMS 適合性評価制度運営要領(Ver.0.8)  
(<http://www.isms.jipdec.or.jp/doc/ismsabst08.pdf>)
- 審査登録機関に対する指定基準(Ver.0.8)  
(<http://www.isms.jipdec.or.jp/doc/ismsreg08.pdf>)

## 3.2 審査プロセスについて

### 3.2.1 審査の概要

「3.1 ISMS 適合性評価制度パイロット事業の枠組み」にあるとおり、認証審査は、契約、初回審査、認証、継続審査といった流れで行われます。以下に、主要なプロセスを示します。ただし、具体的な審査のプロセスは各審査登録機関(認証機関)によって異なる場合があります。

#### (1) 見積

見積依頼書を受理し、見積依頼データの内容を確認します。見積書の作成は、依頼内容に基づき行われます。

審査の工数の算定要素としては、ビジネスの内容、組織の規模、事業所の数、一般的なセキュリティリスクの程度、プロセスの複雑さ等があります。

そこで見積依頼データの基本的な事項について以下に示します。

- (a) 組織の責任者、所在地、組織の規模等の情報
- (b) 主要な製品、サービス、プロセスに関する情報、ISMSの概要
- (c) 情報セキュリティの主要な要素の概要（適用範囲、主要な情報セキュリティリスク、システムのユーザー数、ハードウェア、ソフトウェア、ネットワークの概要、等）
- (d) その他

これらの情報は、同時に審査に必要な能力を確保する情報としても用います。審査登録機関では、これらの見積依頼に関する情報を記入する書式等を準備しています。受審組織は、見積書等によって審査登録機関を選定し、認証契約を締結することになります。

なお、同じ規模で同じようなサービスを提供している組織が2つあっても、それぞれの組織の情報セキュリティポリシー、保証の程度、運用等によっては、見積工数が変わることがあります。

## (2) 認証契約の締結 / 審査準備

契約の締結にもとづき、審査計画を策定します。主要な計画内容は、審査チームの編成、審査日程の調整等です。

審査チームの編成では、チームのリーダーおよびメンバーが配員されます。編成に関しては、必要な工数を確保すること、審査チームがその審査を遂行することが出来る能力を確保することが主要なポイントとなります。

審査能力については、受審組織の業種、業務等の専門性、さらに組織が利用する IT 等についての専門性をチームで確保できるようにしなければなりません。もちろん、ISMS 認証基準(Ver.0.8)、審査技法、マネジメントシステム等に関する知識や経験も有していなければなりません。

次に、審査登録機関は、受審組織と協議して審査日程を調整します。調整された日程と必要な工数、および組織から提出された ISMS に関する資料をレビューすることによって、審査の詳細スケジュールを立案します。このスケジュールについても立案後、受審組織に確認を依頼し双方合意の上決定します。

審査の詳細なスケジュールは、審査登録機関と受審組織で合意された日程について、対象部門責任者等のスケジュール上のアポイントを確実にすること、および、それぞれの部門では、どの ISMS の要求事項が主要な事項として審査されるかといったことが分かる内容のものが示されます。

## (3) 初回審査

審査活動の目的は、ISMS 認証基準(Ver0.8)およびシステムの範囲に適用される要求事項を満たしていることを確認することにあります。このために審査では、計画され文書化されたシステムの内容や実施された活動及びその記録を評価し、適合していることを確認することにあります。もちろん、不適合であると評価されたときはそのことを報告することになります。不適合については、不適合の程度及びどのような是正が必要か受審組織にはっきりと理解され、最終的に審査側と受審側で合意する必要があります。このために審査登録機関では不適合の分類を定義しています。

(a) 不適合の分類

不適合の分類は、一般に重大な不適合と軽微な不適合に区分されます。例えば、以下のように定義されます。

**重大な不適合**

重大な不適合は、ISMS 認証基準(Ver0.8) に準拠しないシステムとなっている場合および準拠した計画であってもそのとおり実行されていない場合であり、組織の ISMS の適用範囲において重大なリスクが顕在化するか、する可能性が高いものです。

**軽微な不適合**

軽微な不適合は、ISMS 認証基準(Ver0.8) の要素について部分的に満たされていないが、重大なリスクが顕在化する可能性は低いと考えられるものです。

不適合が指摘されると、組織は是正を行い、再発防止の手段を講じることとなります。審査登録機関はこの是正等の活動を検証し、該当する不適合について対応が終わったことを確認します。この不適合が指摘された後の活動を、フォローアップ活動といいます。

(b) 審査の段階

初回審査を、文書審査 (Stage1) と実地審査 (Stage2) の 2 段階に分けて実施する例を示します。なお、審査員は、組織、業務等の概要について、見積から契約の段階で事前に理解しているものとします。

文書審査は、通常、受審する組織へ訪問して行われます。受審組織は、審査登録機関から ISMS 認証基準(Ver0.8)の要求事項に従っていることを示す客観的証拠を要求されます。

実地審査は、文書審査 (Stage1) により立案された審査計画にしたがって、審査を実施します。審査は全ての項目について実施するわけではなく、サンプルベースでチェックを行います。

文書審査 (Stage1) 及び実地審査 (Stage2) の内容は、「3.2.2 Stage 1 (文書審査) の内容」、「3.2.3 Stage 2 (実地審査) の内容」に示します。

(c) 審査活動

審査は、文書審査も実地審査も、通常、審査開始および終了の会議、審査の実施、審査報告、(不適合に対する)フォローアップ等で構成されます。

(d) 審査開始会議の議題

審査は、正式な審査開始会議ではじまります。主な出席者は、審査側は主任審査員、チームメンバー、技術専門家等です。受審側は、主に経営者、管理者、審査チームに同行するメンバー等です。

議題として取り上げられる内容には、以下のようなものがあります。

審査範囲の確認

審査、評価方法の説明

不適合の定義とそれに関する是正についての説明

監査計画の確認

システム文書のバージョンの確認

機密保持、等

(e) 審査終了会議の議題

終了会議も開始会議の出席者を集め、以下の内容についてカバーします。

審査範囲の再確認

指摘した不適合の内容

認証に関する決定

謝辞

機密保持の再確認

(f) 審査報告書の主要な項目

審査の正式な報告として、審査報告書が作成されます。審査報告書に含まれる内容には以下のようなものがあります。

審査の目的

対象と範囲

組織の ISMS の概要（ポリシー、手順書等を含む）

審査の実施概要（審査計画を含む）

審査の結論（認証の推薦に関するコメント）

不適合内容（分類を含む）

観察事項

審査責任者、等

(g) フォローアップ

不適合事項が指摘された場合等、フォローアップが必要な場合、その処置については、終了会議や報告書に示されます。

処置には、不適合事項への対応状況を確認するための追加の審査や是正計画の審査あるいは維持審査でのレビュー等があります。

(4) 認証

審査登録機関は、審査の結果をレビューし機関として認証を登録するとともに認証書（登録証）を発行します。

認証登録の決定は、審査チームからの審査報告にもとづいて行われるので、審査の終了会議で認証を推薦されれば、通常、結果が覆されることはありません。認証は、初回審査から3年間有効となります。

認証書に記載される事項として、適合性評価の基準となった ISMS 基準、認証範囲、対象となる事業所等があります。さらに、審査登録機関の認証マークや ISMS 評価登録マーク（認定機関の認定マーク）等が認証書に示されます。



図 3-1 ISMS 認定マーク

(5) 維持審査 / 更新審査

認証を維持するために、1年を超えないサイクルで維持審査が実施されます。維持審査では、前回指摘事項等の是正、改善状況の確認、基準への適合状況、維持状況の確認、ISMSの有効性の確認が行われます。

また、3年目には認証を継続する場合、更新審査を受審する必要があります。

(6) 予備審査

予備審査は、初回審査にさきがけ、審査に入る準備が出来ているかどうかの判定を目的に、審査登録機関によって実施されることがあります。通常、予備審査をうけるかどうかは任意となります。

主な活動内容は、ISMS認証基準(Ver0.8)の要求事項に基づくレビュー、初回審査までに準備すべき事項の明確化、ISMSの範囲等について審査側と受審側とで合意することになります。

なお、予備審査については、審査技法として、初回審査の文書審査、実地審査の技法が用いられること、および、審査登録機関によって取り扱いが違うと思われるため、特に具体的には示しません。

### 3.2.2 Stage 1（文書審査）の内容

#### (1) 概要

ISMSがその目的に沿って、計画され、文書化されていることを確認します。

この段階でもし不適合が示されたら、受審組織は第2段階(実地審査)の開始までに不適合の状態を解決する是正計画を提出する必要があります。もちろん、この段階でマネジメントシステムとして、計画に大きな欠陥がある等の場合は、第2段階に進むことは出来ません。

#### (2) 目的

情報セキュリティポリシーやISMSの目的に沿ってISMSが計画されていることを理解し、組織の第2段階受審について準備状況を確認します。同時に、審査側は第2段階で、焦点を当てる事項を明確にします。

#### (3) 対象

審査の対象を組織/体制で見ると、ISMSを適用する組織全体となります。しかし、この段階では、ISMSの計画に焦点をあて審査するため、特に経営層、ISMSの管理部門が中心となり、各所管部門は、特定したリスクが適切かどうかを確認するサイトツアーとして訪問する程度となります。

ISMSの認証基準で見ると、主に対象範囲の全ての情報資産を識別するためのリスクアセスメントの結果とその方法、リスクマネジメントへのアプローチ、要求される保証の度合い、情報セキュリティポリシーとISMSの構造及びの手順についての確認と文書化について検討します。

### 3.2.3 Stage 2（実地審査）の内容

#### (1) 概要

組織がその方針、目的、手順に従って実施しているかを確認します。

ISMS が規格、その他の標準に照らして合致し、方針、目的、目標を達成しているか確認します。（ISMSの有効性を確認する。）

#### (2) 目的

受審組織が、そのセキュリティポリシー、目的、手順を確実に遵守していること及び組織のISMSがISMS認証基準(Ver0.8)及び関連する文書に適合しており、組織のセキュリティポリシー目的を達成しようとしていることを確認します。

#### (3) 対象

審査の対象を組織/体制で表すとISMSを適用する組織全体となります。業務内容が同様の組織が複数ある場合には、サンプルを選んで対象とすることがあります。

ISMS認証基準(Ver0.8)で見ると全ての要求事項が対象となりますが、審査の焦点は以下の点にあてられています。

- (a) 情報セキュリティリスクのアセスメントとISMSの計画とフレームワーク
- (b) 適用宣言書
- (c) 情報セキュリティポリシー及びセキュリティ目的
- (d) 情報セキュリティ目的や目標に対するセキュリティパフォーマンスの監視、測定、報告やレビュー
- (e) 情報セキュリティレビューやマネジメントレビュー
- (f) 情報セキュリティポリシーに関するマネジメントの責任
- (g) 情報セキュリティポリシー、リスクアセスメントの結果、情報セキュリティの目的/目標、プログラム、手順、実施結果及びセキュリティレビューの結果の関連性

## 4. 参考文献

ISMS 適合性評価制度パイロット事業の実施に関する資料、および ISMS 構築において参考とすべき参考文献、法規制等の資料を示します。

### 4.1 参考文献

発行	文献名	備考
情報セキュリティ対策推進会議	重要インフラのサイバーテロ対策に係る特別行動計画（平成 12 年 12 月 15 日）	<a href="http://www.kantei.go.jp/jp/it/security/index.html">http://www.kantei.go.jp/jp/it/security/index.html</a>
内閣安全保障・危機管理室 情報セキュリティ対策推進室	情報セキュリティポリシーに関するガイドライン（平成 12 年 7 月）	<a href="http://www.kantei.go.jp/jp/it/security/index.html">http://www.kantei.go.jp/jp/it/security/index.html</a>
経済産業省 (旧通商産業省)	情報システム安全対策基準 (平成 7 年 8 月 29 日 通商産業省告示第 518 号)(制定) (平成 9 年 9 月 24 日 通商産業省告示第 536 号)(最終改正)	<a href="http://www.gip.jipdec.or.jp/policy/std-doc/security-std.html">http://www.gip.jipdec.or.jp/policy/std-doc/security-std.html</a>
	個人情報保護ハンドブック 「民間部門における電子計算機処理に係る個人情報保護ガイドライン」<解説書> (平成 10 年 6 月 通商産業省機械情報産業局)	<a href="http://www.meti.go.jp/policy/netsecurity/downloadfiles/P-guideline.pdf">http://www.meti.go.jp/policy/netsecurity/downloadfiles/P-guideline.pdf</a>
	コンピュータ不正アクセス対策基準 (平成 8 年通商産業省告示第 362 号)	<a href="http://www.meti.go.jp/kohosys/topics/10000098/eseu06j.pdf">http://www.meti.go.jp/kohosys/topics/10000098/eseu06j.pdf</a>
	コンピュータウイルス対策基準 (平成 7 年通商産業省告示第 429 号)	<a href="http://www.ipa.go.jp/security/antivirus/kijun952.html">http://www.ipa.go.jp/security/antivirus/kijun952.html</a>
	システム監査基準 (昭和 60 年 1 月通商産業省公表、 平成 8 年 1 月改訂)	<a href="http://www.meti.go.jp/kohosys/topics/10000098/eseu08j.pdf">http://www.meti.go.jp/kohosys/topics/10000098/eseu08j.pdf</a>
	ソフトウェア管理ガイドライン (平成 7 年 11 月 15 日通商産業省公表)	<a href="http://www.meti.go.jp/policy/netsecurity/downloadfiles/softkanri-guide.htm">http://www.meti.go.jp/policy/netsecurity/downloadfiles/softkanri-guide.htm</a>

発行	文献名	備考
警察庁	情報システム安全対策指針 (平成9年9月18日制定 国家公安委員会告示第9号) (平成11年11月22日一部改正 国家公安委員会告示第19号)	<a href="http://www.npa.go.jp/hightech/antai_sisin/kokuji.htm">http://www.npa.go.jp/hightech/antai_sisin/kokuji.htm</a>
行政情報システム各省庁連絡会議幹事会了承	行政情報システムの安全対策指針 (平成11年7月30日)	<a href="http://www.soumu.go.jp/gyoukan/kanri/990816c.htm">http://www.soumu.go.jp/gyoukan/kanri/990816c.htm</a>
総務省 (旧自治省)	地方公共団体コンピュータセキュリティ対策基準(昭和62年7月制定)	
総務省 (旧総務庁)	行政情報システムの安全対策に関するガイドライン(平成元年9月制定)	
総務省 (旧郵政省)	情報通信ネットワーク安全・信頼性基準 (昭和57年10月制定 平成13年3月29日最終改正)	<a href="http://www.yusei.go.jp/whatsnew/kokuji/network_2001feb.html">http://www.yusei.go.jp/whatsnew/kokuji/network_2001feb.html</a>
	電気通信事業における個人情報保護に関するガイドライン (平成3年9月制定 平成10年12月改定 郵政省告示第570号)	<a href="http://www.joho.soumu.go.jp/whatsnew/guideline_privacy_1.html">http://www.joho.soumu.go.jp/whatsnew/guideline_privacy_1.html</a>
	発信者情報通知サービスの利用における発信者個人情報の保護に関するガイドライン (平成8年11月制定)	<a href="http://www.joho.soumu.go.jp/policyreports/japanese/misc/bangou4.html">http://www.joho.soumu.go.jp/policyreports/japanese/misc/bangou4.html</a>
情報通信利用に係るセキュリティ保護に関する検討会	情報通信利用に係るセキュリティ保護に関する検討会報告書(平成12年11月)	<a href="http://www.yusei.go.jp/policyreports/japanese/group/tsusin/01205x01.html">http://www.yusei.go.jp/policyreports/japanese/group/tsusin/01205x01.html</a>
国土交通省 (旧建設省)	コンピュータシステム・情報通信システムを設置する建築物にかかわる安全対策基準 (昭和61年5月制定)	
金融庁 (旧金融監督庁)	検査マニュアル	<a href="http://www.fsa.go.jp/manual/manual.html">http://www.fsa.go.jp/manual/manual.html</a>
	事務ガイドライン	<a href="http://www.fsa.go.jp/guide/guide.html">http://www.fsa.go.jp/guide/guide.html</a>



発行	文献名	備考
(続き) 日本規格協会	JIS X 5070-1~3 情報技術セキュリティの評価基準 第一部: 総則及び一般モデル 第二部: セキュリティ機能要件 第三部: セキュリティ保証要件	
	JIS Z 9911-1~3:1996 品質システムの監査の指針 第一部: 監査 第二部: 品質システム監査員の資格基準 第三部: 監査プログラムの管理	
	JIS Q 14010:1996 環境監査の指針 一般原則	
	JIS Q 14011:1996 環境監査の指針 監査手順-環境マネジメントシステムの監査	
	JIS Q 14012:1996 環境監査の指針 環境監査員のための資格基準	
	JIS Q 15001 個人情報保護に関するコンプライアンス・プログラムの要求事項	<a href="http://www.jipdec.or.jp/security/privacy/JISQ15001.html">http://www.jipdec.or.jp/security/privacy/JISQ15001.html</a>
	JIS Q 2001:2001 リスクマネジメントシステム構築のための指針	
	JIS Z 9920:2000 苦情対応マネジメントシステムの指針	
	JIS Z 9361:1996 認証機関及び審査登録機関の認定審査並びに認定機関に対する一般要求事項 (Guide 61)	
	JIS Z 9362:1996 品質システム審査登録機関に対する一般要求事項 (Guide 62)	
	JIS Q 0066:2000 環境マネジメントシステムの審査登録機関に対する一般要求事項 (Guide 66)	
	JIS C 0364 建築電気設備シリーズ	建築電気設備の共用設置に関する基準
	BS15000:2000 Specification for IT Service management (英和対訳版)	
	社団法人電子情報技術産業協会 (JEITA)	JEITA IT-1001 情報システムの設備ガイド (案)

発行	文献名	備考
ISO	ISO/IEC TR 13335-1~4 Guidelines for the management of IT Security Part1: Concepts and models for IT Security Part2: Managing and planning IT Security Part3: Techniques for the management of IT Security Part4: Selection of safeguards	
	ISO TR 13569 Banking and related financial services - Information security guidelines	
OECD	Guidelines on the Protection of Privacy and Transborder Flows of Personal Data	<a href="http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM">http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM</a>
	Ministerial Declaration on the Protection of Privacy on Global Networks	<a href="http://www.oecd.org/dsti/sti/it/secur/act/privnote.htm">http://www.oecd.org/dsti/sti/it/secur/act/privnote.htm</a>
	Guidelines for the Security of Information Systems	<a href="http://www.oecd.org/dsti/sti/it/secur/prod/e_secur.htm">http://www.oecd.org/dsti/sti/it/secur/prod/e_secur.htm</a>
European Union (EU)	The European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data	<a href="http://www.privacy.org/pi/intl_orgs/ec/eudp.html">http://www.privacy.org/pi/intl_orgs/ec/eudp.html</a>
National Institute of Standards and Technology (NIST)	FIPS PUB 140-2 Security Requirements for Cryptographic Modules (01 May 25)	<a href="http://www.itl.nist.gov/fipspubs/">http://www.itl.nist.gov/fipspubs/</a>
Information Systems Audit and Control Association & Foundation (ISACA)	Control Objectives for Information and related Technology (COBIT)	<a href="http://www.isaca.org/cobit.htm">http://www.isaca.org/cobit.htm</a>
	Control Objectives for Net Centric Technology (CONCT) 邦訳: ネット中心テクノロジー管理ガイドライン	<a href="http://www.itec.co.jp/">http://www.itec.co.jp/</a>
ISACA 大阪支部・監査基準分科会	セキュリティポリシー -その作成のポイントと解説&サンプル- (平成 12年 2月)	<a href="http://www.isaca-osaka.org/secplcy1.pdf">http://www.isaca-osaka.org/secplcy1.pdf</a>
	ネットワーク管理のガイドライン (平成 9年 12月 31日)	<a href="http://www.isaca-osaka.org/guideline-index.htm">http://www.isaca-osaka.org/guideline-index.htm</a>

発行	文献名	備考
American Institute of Certified Public Accountants (AICPA)	WebTrust	<a href="http://www.aicpa.org/assurance/webtrust/princip.htm">http://www.aicpa.org/assurance/webtrust/princip.htm</a> <a href="http://webtrust.org/">http://webtrust.org/</a>
	SysTrust	<a href="http://www.aicpa.org/assurance/systrust/princip.htm">http://www.aicpa.org/assurance/systrust/princip.htm</a>
情報処理振興事業協会 (IPA)	情報システム部門責任者のための情報セキュリティブックレット (2001年3月)	<a href="http://www.ipa.go.jp/security/fy12/contents/booklet.pdf">http://www.ipa.go.jp/security/fy12/contents/booklet.pdf</a>
	暗号技術評価報告書 「CRYPTREC REPORT 2000」 (平成13年3月)	<a href="http://www.ipa.go.jp/security/enc/CRYPTREC/index.html">http://www.ipa.go.jp/security/enc/CRYPTREC/index.html</a>
社団法人情報サービス産業協会 (JISA)	情報システム安全対策基準解説書 (赤本) (平成8年10月1日改訂)	<a href="http://www.jisa.or.jp/">http://www.jisa.or.jp/</a>
	プライバシーマーク制度 (JIS Q 15001) における「システム監査ガイドライン第1版」 (1999年10月)	<a href="http://www.jisa.or.jp/privacy/index-j.html">http://www.jisa.or.jp/privacy/index-j.html</a>
	「情報サービス事業者のための個人情報保護のあり方 -情報サービス産業 個人情報保護ガイドライン- の解説 (平成12年8月)	<a href="http://www.jisa.or.jp/privacy/index-j.html">http://www.jisa.or.jp/privacy/index-j.html</a>
財団法人金融情報システムセンター (FISC)	金融機関等コンピュータシステムの安全性対策基準 (平成12年7月)	<a href="http://www.fisc.or.jp/ippan_3.htm">http://www.fisc.or.jp/ippan_3.htm</a>
	金融機関等コンピュータシステムの安全対策基準解説書 (平成12年7月)	
	金融機関等におけるコンティンジェンシープラン策定のための手引書 (平成6年1月)	
	金融機関等におけるコンティンジェンシープラン要綱 (平成8年1月)	
	金融機関等におけるセキュリティポリシー策定のための手引書 (平成11年1月)	
	金融機関等のセキュリティポリシーの策定・運用に関する研究会報告書 (平成13年6月)	
	金融機関等における個人データ保護のための取扱指針 (1987年3月策定、1999年4月改正)	
	金融機関等における個人データ保護ハンドブック (平成12年6月)	
(続く)		

発行	文献名	備考
( 続き )	金融機関等のシステム監査指針 (平成12年7月)	
社団法人日本マーケティング・リサーチ協会 (JMRA)	個人情報保護ガイドラインとプライバシーマーク制度の申請手続き概要(2000年9月)	<a href="http://www.jmra-net.or.jp/book/kaiyetu.html">http://www.jmra-net.or.jp/book/kaiyetu.html</a>
電子商取引推進協議会 (ECOM)	EC で取扱われる個人情報に関する調査報告書 (Ver.3.0)(平成13年3月)	<a href="http://www.ecom.or.jp/press/20010606_kojin.html">http://www.ecom.or.jp/press/20010606_kojin.html</a>
社団法人日本通信販売協会	通信販売業における電子商取引のガイドライン (平成11年1月19日制定 平成12年3月14日改訂)	<a href="http://www.jadma.org/guid_mai/guidelin.html">http://www.jadma.org/guid_mai/guidelin.html</a>
	通信販売における個人情報保護ガイドライン (平成7年9月12日制定)	<a href="http://www.jadma.org/guid_mai/guidelin.html">http://www.jadma.org/guid_mai/guidelin.html</a>
	テレビショッピングに関するガイドライン (平成9年3月11日制定)	<a href="http://www.jadma.org/guid_mai/guidelin.html">http://www.jadma.org/guid_mai/guidelin.html</a> #2
	通信教育に関するガイドライン (平成7年9月12日制定)	<a href="http://www.jadma.org/guid_mai/guidelin.html">http://www.jadma.org/guid_mai/guidelin.html</a> #4
日本証券業協会	インターネット取引において留意すべき事項について(ガイドライン) (平成13年4月)	<a href="http://www.jsda.or.jp/html/oshirase/internetwg/guidline.pdf">http://www.jsda.or.jp/html/oshirase/internetwg/guidline.pdf</a>

## 4.2 法令等

ここではパイロット事業において参考となる主要な法令を例示的に列挙します。

### 4.2.1 情報保護に関する法令

法令の名称	主な参考条項
日本国憲法	第21条
行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律	全般
行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律施行令	全般
貸金業の規制等に関する法律	第30条第2項 個人信用情報の目的外使用の禁止
割賦販売法	第39条 信用情報の適正な使用等
不正競争防止法	全般

### 4.2.2 コンピュータ犯罪に関する法令

法令の名称	主な参考条項
刑法	第7条の2 電磁的記録の定義 第157条第1項 電磁的公正証書原本不実記録罪 第158条第1項 不実記録電磁的公正証書原本供用罪 第161条の2 電磁的記録不正作出・不正作出電磁的記録供用罪 第234条の2 電子計算機損壊等業務妨害罪 第246条の2 電子計算機使用詐欺罪 第258条 公用電磁記録毀棄罪 第259条 私用電磁記録毀棄罪
不正アクセス行為の禁止等に関する法律	全般
労働基準法	第91条 制裁規定の制限
労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律	第24条の4 秘密を守る義務

#### 4.2.3 設備に関する法令

法令の名称	主な参考条項
建築基準法	第1条 目的 第2条 用語の定義 第6条 建築物の建築等に関する申請及び確認 第7条 建築物に関する完了検査 第20条 構造耐力
建築基準法施行令	第1条 用語の定義 第82条 応力度等 第82条の2 層間変形角 第82条の3 剛性率・偏心率等 第82条の4 保有水平耐力 第88条 地震力 第107条 耐火構造 第107条の2 準耐火構造 第108条 防火構造 第108条の2 準防火構造 第109条 防火戸その他の防火設備 第110条 防火戸の構造 第112条 防火区画 第117条 廊下、避難階段及び出入口の適用の範囲 第119条 廊下の幅 第120条 直通階段の設置 第121条 二以上の直通階段を設ける場合 第122条 避難階段の設置 第125条 屋外への出口 第126条の2 排煙設備の設置 第126条の3 排煙設備の構造 第129条 特殊建築物等の内装 第5章 避難施設等
消防法	第2条 用語例 第8条 防火管理 第9条 危険物等の貯蔵等の基準 第10条 危険物の貯蔵等の取扱い 第17条 消防用設備等の設置、維持義務等 第17条の3 消防用設備等の点検及び報告

法令の名称	主な参考条項
消防法施行令	第3条 防火管理者の資格 第4条 防火管理者の責務 第7条 消防用設備等の種類 第10条 消火器具に関する基準 第11条 屋内消火栓設備に関する基準 第12条 スプリンクラー設備に関する基準 第13条 水噴霧消火設備等を設置すべき防火対象物 第14条 水噴霧消火設備に関する基準 第15条 泡消火設備に関する基準 第16条 二酸化炭素消火設備に関する基準 第17条 ハロゲン化物消火設備に関する基準 第18条 粉末消火設備に関する基準 第21条 自動火災報知設備に関する基準 第23条 消防機関へ通報する火災報知設備に関する基準 第24条 非常警報器具又は非常警報設備に関する基準 第25条 避難器具に関する基準 第26条 誘導灯及び誘導標識に関する基準 第28条 排煙設備に関する基準
消防法施行規則	第3条 消防計画 第4条 防火管理者の選任又は解任の届出 第4条の4 防災表示等 第23条 自動火災報知設備の感知器等 第24条 自動火災報知設備に関する基準の細目 第30条 排煙設備に関する基準の細目 第31条の4 消防用設備等の点検及び報告
高圧ガス保安法	第35条 保安検査 第35条の2 定期自主検査
冷凍保安規則	第7条 定置式製造設備に係る技術上の基準 第8条 移動式製造設備に係る技術上の基準
大規模地震対策特別措置法	全般
建築物の耐震改修の促進に関する法律	全般
危険物の規制に関する政令	第8条の5 定期的に点検しなければならない製造所等の指定
電気通信事業法	第4節 電気通信設備
電気事業法	第42条 保安規程
電気設備技術基準	第15条 地絡に対する保護対策
エネルギーの使用の合理化に関する法律	全般

#### 4.2.4 社会的情報インフラに関する法令

法令の名称	主な参考条項
高度情報通信ネットワーク社会形成基本法	第22条 高度情報通信ネットワークの安全性の確保等
電子署名及び認証業務に関する法律	全般
電気通信事業法	第4条 秘密の保護 第35条 業務の停止等の報告 第41条 電気通信設備の維持
有線電気通信法	第9条 有線電気通信の秘密の保護
電波法	第59条 秘密の保護

#### 4.2.5 知的財産権に関する法令

法令の名称	主な参考条項
著作権法	第2条 定義 第10条 著作物の例示 第12条の2 データベースの著作物 第20条 同一性保持権 第47条の2 プログラムの著作物の複製物の所有者による複製等 第76条の2 創作年月日の登録 第113条 侵害とみなす行為
特許法	全般

## 5. 用語の説明

本書の中で用いられる主な用語の説明は、以下のとおりです。

### <情報セキュリティ>

- ・情報の機密性、完全性及び可用性を確保し、維持すること

\* 『ISMS認証基準(Ver.0.8)』発行:(財)日本情報処理開発協会(平成13年4月1日)

### <可用性>

- ・許可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること

\* 『ISMS技術委員会』

### <完全性>

- ・情報及び処理方法が正確であること及び完全であることを保護すること

\* 『ISMS技術委員会』

### <機密性>

- ・アクセスを認可された者だけが、情報にアクセスできることを確実にすること

\* 『ISMS技術委員会』

### <インシデント>

- ・情報セキュリティに関するトラブルや事故等の総称

\* 『ISMS技術委員会』

### <脅威>

- ・情報資産に影響を与え、損失を発生させる直接の要因  
(故意的(不正アクセス、改ざん等)や偶発的(自然災害、故障等)な事故の潜在的な原因等)

\* 『ISMS技術委員会』

### <脆弱性>

- ・脅威を受けた場合の情報資産の損失を起こしやすく、かつ、拡大させる要因

\* 『金融機関等におけるセキュリティ対策のための手引書』発行:(財)金融情報センター(平成11年1月)

### <リスク>

- ・ある脅威が、情報資産または情報資産グループの脆弱性を利用して、情報資産への損失、又は損害を与える可能性

(代表的なリスク：オペレーショナルリスク、評判リスク、法的リスク、信用リスク、移転リスク等)

\* 『JIS TR X 0036-1』発行:(財)日本規格協会(平成12年)

### <リスク分析>

- ・セキュリティリスクの識別、セキュリティリスクの程度の判定、及び統制が必要な領域の識別を実行するプロセス

\* 『JIS TR X 0036-1』発行:(財)日本規格協会(平成12年)

### <リスク評価>

- ・情報や情報処理設備等に対する脅威及びその脅威への脆弱性を分析し、その結果からリスクが顕在化する可能性及び顕在化した場合の事業への影響度を検証すること

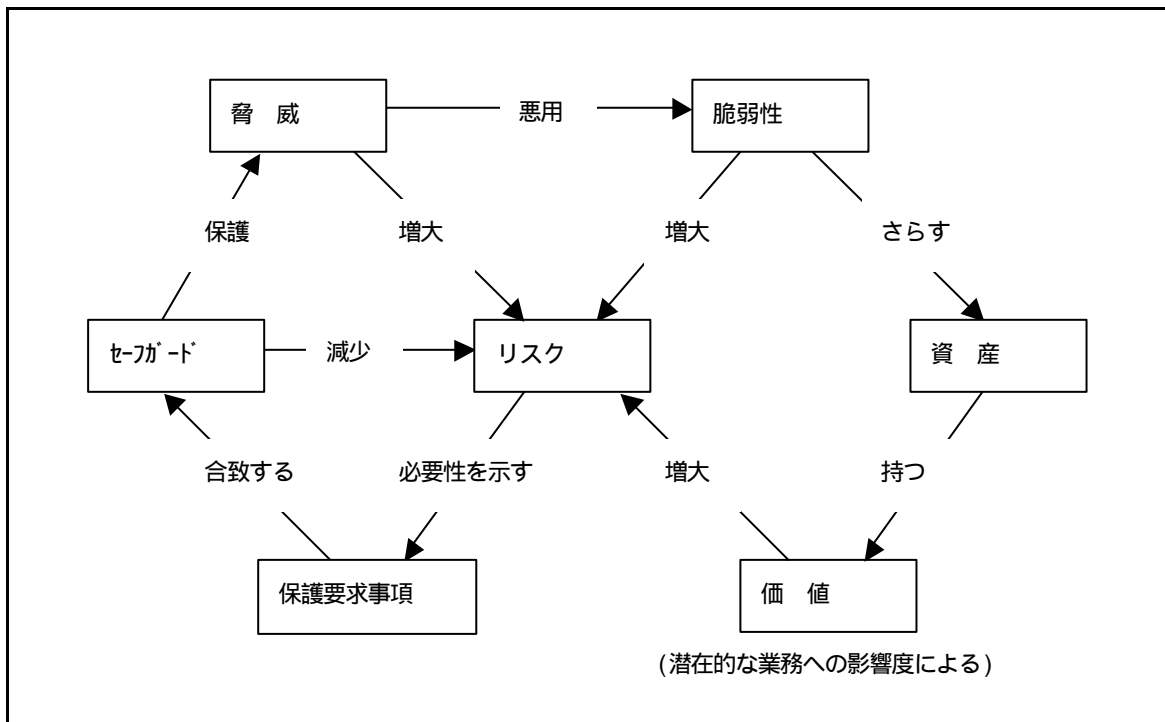
\* 『ISMS認証基準(Ver.0.8)』発行:(財)日本情報処理開発協会(平成13年4月1日)

### <リスクマネジメント>

- ・ITシステムの資源に影響を及ぼす不確かな事象を識別、制御、除去、または低減する総合的なプロセス。

\* 『JIS TR X 0036-1』発行:(財)日本規格協会(平成12年)

リスクマネジメントにおける関係



《出典：JIS TR X 0036-1》

#### < 情報 >

- ・コンピュータシステムや磁気媒体等に保存されているデータのみならず、入力前のメモや印刷されたもの、ならびに会話や記憶

\* 『金融機関等におけるセキュリティ策定のための手引書』発行：(財)金融情報リサーチセンター(平成 11年1月)

#### < 情報資産 >

- ・情報と情報システム、ならびにそれらが正当に保護され使用され機能するために必要な要件の総称

\* 『ISMS技術委員会』

#### < 情報システム >

- ・コンピュータ、サーバ、ワークステーション、パーソナルコンピュータ、通信関係機器(MDF、IDFを含む)、オフライン機器等の全部又は一部により構成される種々のデータを処理するためのシステム

\* 『(案)電子情報技術産業協会技術レポート/情報システムの設備ガイド』発行：(社)電子情報技術産業協会(2001年8月)

#### < 情報サービス >

- ・情報システムを利用して、情報の加工、検索等の処理並びに提供を行うサービス

\* 『ISMS技術委員会』

#### < 情報処理施設 >

- ・情報サービスを行うための情報システムを設置している建物及び室

\* 『ISMS技術委員会』

#### < 設備 >

- ・情報システムの運転を支援するために必要不可欠な電源設備、空気調和設備、防災設備、防犯設備及びそれらの付帯設備

\* 『ISMS技術委員会』

## II 事例編

# 1. 事例会社の概要

下記に、本事例の会社概要を示す。

表 1-1 会社概要

会社名	イーデータセンタ株式会社
事業内容	データセンタ事業、運用監視事業、運用委託事業を行っている。 主な顧客は、都市銀行、地方銀行、消費者金融業、製造業、ASP事業者（給与計算、電子メール配信サービス等）
従業員等数	242名

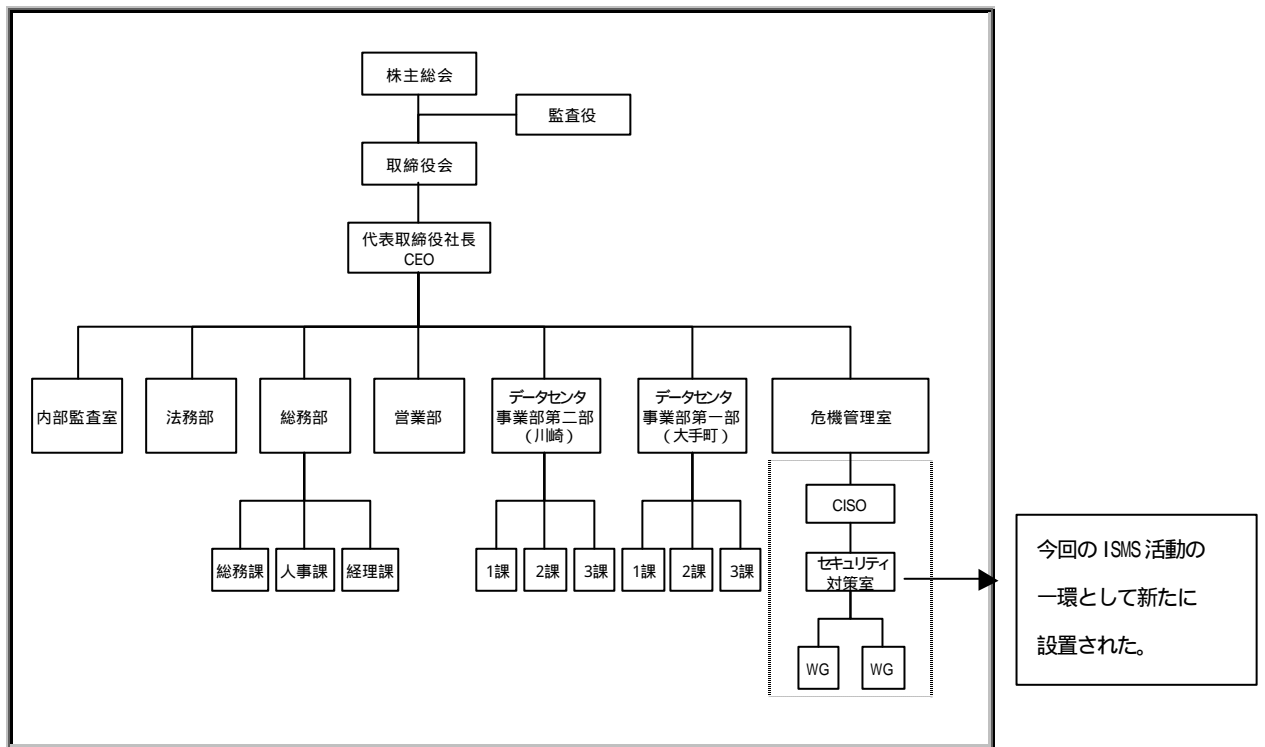


図 1-1 社内組織図

詳細は、「5. 参照資料（会社の詳細情報）」を参照のこと。

## 2. I S M S の準備

### 2.1 企画

他社 IDC のセキュリティ事故発生を契機に、社内の情報セキュリティ管理を見直すこととなった。

会社として、情報セキュリティ規程や関連する規程は存在するが、情報セキュリティに関する統一的な活動が不足しているとの認識から、データセンタ事業部第一部長を中心として、「情報セキュリティ対策推進会議」を設置し、検討することとした。下記の文献を参考に、プレスタディを実施した。

表 2-1 参考文献

	参考文献
1	FISC 情報セキュリティ策定の手引き
2	情報セキュリティポリシーに関するガイドライン
3	BS7799 Part1 , Part2

(基本編 4. 参考文献参照)

プレスタディの結果、データセンタ事業部第一部長は、情報セキュリティ管理の仕組みを確立することであることの重要性を認識した。

データセンタ事業部第一部長が、プレスタディの結果を社長に報告した結果、「会社として情報セキュリティ管理の仕組みを確立するように」との指示が下った。

プレスタディの結果報告の際に、データセンタ事業部第一部長は、社長に対して、情報セキュリティ管理の仕組みを確立するためには、各部との連携が不可欠である旨を説明し、各部門からの支援とコンセンサスを得る必要性から、「情報セキュリティ対策推進会議」を設置し、関係する各部門のメンバーを集めて検討することとし、取締役会の承認を得た。

下記が、情報セキュリティ対策推進会議のメンバー（部門）である。

表 2-2 情報セキュリティ対策推進会議メンバー（部門）一覧

部門名	役割	参加メンバー	選定理由
総務部	ルールを決める側として参加 * 執筆作業担当	総務課長 人事課長	<ul style="list-style-type: none"> <li>・ 全社規程類の発行の管理責任部門である。</li> <li>・ 人の採用の責任部門である（外注を含む）</li> <li>・ 社内のトラブル案件の相談窓口であり、情報セキュリティに関する対応も今後必要となる。</li> <li>・ ファシリティ面に責任を負う部門である。</li> <li>・ プライバシーを守るべき部門である。</li> <li>・ 懲罰等に関する部門である。</li> <li>・ 教育に関する部門である。</li> </ul>
内部監査室	ルールを決める側として参加	監査室長	<ul style="list-style-type: none"> <li>・ 内部監査を行う部門である。</li> <li>・ 情報セキュリティ監査の主管部門となる。</li> </ul>
法務部	ルールを決める側として参加 * 執筆作業担当	法務部長	<ul style="list-style-type: none"> <li>・ 契約関連および法務面に関連する事項を担当する部門である。</li> </ul>
データセンタ 事業部第一部 （大手町）	ルールを決める側として参加 * 執筆作業担当	事業部長 1 課長 2 課長 3 課長	<ul style="list-style-type: none"> <li>・ 大手町事業所の運用管理に責任をもつ部署である。</li> <li>・ システムの企画・開発・運用の管理責任部門であり、情報システムのセキュリティ対策を実施している。</li> <li>・ 大手町事業所内の LAN に責任を負っている。</li> </ul>

図 1-1 社内組織図を参照のこと

## 2.2 検討

情報セキュリティ対策推進会議は、下記を追加の参考文献として検討を行った。

表 2-3 参考文献

	参考文献
1	GMITS(ISO ISO/IEC TR 13335-1~4 Guidelines for the management of IT Security)
2	DISC PD3000~PD3005(日本規格協会 DISC PD 3000 シリーズ規格集(英和対訳版))

(基本編 4. 参考文献参照)

情報セキュリティ対策推進会議による検討の結果、以下の方針案が取締役会に報告され、承認された。

### 【情報セキュリティ管理方針案】

1. 「ISMS 認証基準(Ver.0.8)」に準拠し、情報セキュリティ管理を行う。第一ステップとして、データセンタ事業部第一部(大手町)内の業務を適用範囲とする。
2. 現在の情報セキュリティ基本規程および既存の情報セキュリティ関連文書を活用し、さらに必要となるドキュメントについては、適用範囲内向けのガイドラインの作成を行い、文書体系の整備を行う。
3. 適用範囲以外の組織についても、データセンタ事業部第一部(大手町)の情報セキュリティについて重要な関わりを持つ部署を、データセンタ事業部第一部(大手町)の業務に関連する部分に限り適用範囲とする。
4. 「ISMS 認証基準(Ver.0.8)」への準拠に対し、最初に検討すべき課題をリストアップする。

本年12月を目標に「ISMS 認証基準(Ver.0.8)」の認証を取得する。

検討の結果、最初に検討すべき課題として、下記の項目が識別された。

【「ISMS 認証基準(Ver.0.8)」への準拠に対し、最初に検討すべき課題】

- 課題(1) 情報セキュリティ管理適用範囲
- 課題(2) 情報セキュリティリスク評価手順の策定
- 課題(3) 情報セキュリティ管理に関する規程類の整備
- 課題(4) 情報セキュリティに関する管理組織整備
- 課題(5) 情報セキュリティ教育・訓練
- 課題(6) 情報セキュリティの独立レビュー
- 課題(7) 情報セキュリティ事故管理
- 課題(8) コンプライアンス管理
- 課題(9) 事業継続計画

(1)～(9)の課題に対して以下の通りの対策を実施していくことにした。

## 2.2.1 課題（１）情報セキュリティ管理の適用範囲

### (1) 方針

情報セキュリティ管理体制の構築を行うため、第一ステップとして特定の部門を対象として情報セキュリティ管理の実践を行い、その結果をもとに将来的には全社的な体制へと拡張する。

### (2) 部門の選択

組織が新しく、機動的に業務手順の変更等が行える部門を優先することとする。

### (3) 適用範囲の決定

適用範囲については情報セキュリティ対策推進会議が以下の２点を考慮して原案を作成し、取締役会にて承認された。

(a) 当社にとって情報セキュリティが特に重要な業務を含む。

(b) 物理的、論理的、組織的に境界があいまいでなく、範囲内の情報セキュリティ管理を構築することで一定の効果を上げられる。

(4) 適用範囲

適用範囲を下記の範囲とする。

表 2-4 適応範囲

	カテゴリ	対象	内容	関連する文書
1	ISMS	データセンタ事業部第一部(大手町)の行う事業全体に関する情報セキュリティマネジメント	<ul style="list-style-type: none"> <li>・データセンタ事業</li> <li>・運用監視事業</li> <li>・運用委託事業</li> </ul>	ISMS 文書
2	組織	データセンタ事業部第一部(大手町)	業務を行う部門	組織図 職務分掌
		情報セキュリティ対策室	情報セキュリティフォーラム及びクロスファンクショナルフォーラムの機能を持つ組織	
		総務部	以下の業務を範囲とする。 <ul style="list-style-type: none"> <li>・人事採用（外注含む）</li> <li>・施設管理</li> <li>・従業員教育</li> <li>・その他データセンタ事業部第一部（大手町）の情報セキュリティ管理に関わる業務</li> </ul>	
		法務部	以下の業務を範囲とする。 <ul style="list-style-type: none"> <li>・法律に関連する業務</li> <li>・データセンタ事業部第一部（大手町）の契約に関する業務</li> <li>・その他データセンタ事業部第一部（大手町）の情報セキュリティ管理に関わる業務</li> </ul>	
3	場所	大手町事業所	データセンタ事業部第一部(大手町)	フロアレイアウト

		本社（右部分）	情報セキュリティ対策室 総務部 法務部 内部監査室	（空調ダクト等の 設備の構成も含む） 電源・電話の配線図
--	--	---------	------------------------------------	------------------------------------

	カテゴリ	対象	内容	関連する文書
4	情報技術	ハードウェア・ソフトウェア	大手町事業所内で管理されるハード・ソフトウェアを適用範囲とする。	機器構成図 ネットワーク構成図
		ネットワーク	大手町事業所からの対顧客・対インターネット接続のルータを含む。	
5	情報資産	上記1~4に所属するすべての情報資産を適用範囲とする。 各部の作成する資産管理目録にて詳細が定義される。		資産管理台帳

## 2.2.2 課題（2）情報セキュリティリスク評価手順の策定

### (1) 方針

情報セキュリティリスク評価方針を決定するにあたり、GMITSを参照し、当社に適した方式を検討する。GMITSのBaseline Approachに基づき、情報資産とそれに関連する脅威をリストアップし、リスクの評価を行う方法を採用した。

### (2) 実施部門

リスク分析及びリスク評価は、下記の部門が実施する。

表 2-5 リスク分析及びリスク評価実施部門

	実施項目	実施組織	承認
1	リスク分析及びリスク管理手法の決定	情報セキュリティ対策室	危機管理室
2	リスク分析手順書作成	情報セキュリティ対策室	危機管理室
3	リスク評価実施	データセンタ事業部第一部(大手町)	情報セキュリティ対策室
4	リスク評価結果を情報セキュリティ対策室へ報告	データセンタ事業部第一部(大手町)	情報セキュリティ対策室
5	リスク管理（管理策の決定）	情報セキュリティ対策室	危機管理室
6	ガイドライン等の作成	情報セキュリティ対策室	危機管理室
7	ポリシー及び関連規程の見直し	情報セキュリティ対策室	危機管理室
8	リスク管理結果より対策の決定	データセンタ事業部第一部(大手町)	情報セキュリティ対策室
9	対策の実施・運用	データセンタ事業部第一部(大手町)	情報セキュリティ対策室

### (3) リスク評価についての方針

リスク評価についての方針は下記の通り決定された。

- (a) ISMS 認証基準 (Ver.0.8) を元にセキュリティ対策のチェックシートを作成し、チェックシートに現状を記述し、記入者がリスクを評価する。
- (b) リスク分析は、セキュリティ対策部門が実施できるよう、平易な表現で記述する。
- (c) 実現できない対策基準の要件は、情報セキュリティ対策室の検討メンバーが対策チームとなり、評価の上、リスクを許容する判断を下す。

(4) リスク評価手順

リスク評価の手順は下記の通り決定された。

- (a) 情報セキュリティ対策室がリスク評価シート(図2-1参照)の「当社状況」「関連する脅威」「関連する対策」を記述する。
- (b) リスク評価を行う部門は、「関連する情報資産」に、該当する資産を記述し、ビジネスへの影響を記入する。
- (c) リスク評価を行う部門は、「関連する対策」の「対策済」欄を記入する。
- (d) リスク評価を行う部門は、「リスク」を記入する。
- (e) リスク評価を行う部門は、すべてのリスク評価シートに対し2．～4．を行った後、結果を情報セキュリティ対策室に提出する。
- (f) 情報セキュリティ対策室は、提出されたリスク評価シートを元に、リスク管理を行う。

## リスク評価シート

No. \_\_\_\_\_

基準目的	【基準目的の番号】
基準項目	【基準項目の内容】
当社状況	【当社にとっての該当内容】

### 関連する情報資産

番号	内容	ビジネスへの影響
A1	【該当する情報資産 1】	【ABC で記入】

### 関連する脅威

番号	内容	備考
T1	【該当する脅威の内容】	

### 関連する対策

番号	内容	対策済	備考
P1	【当社における基準対策】	済の場合 ( )	対策状況、不備内容等

### リスク

A	T	P	内容	リスク	備考
資産	脅威	未実施 対策	【リスク内容】	ABC で記入	理由等

図 2-1 リスク評価シート

## 2.2.3 課題（3）情報セキュリティ管理に関する規程類の整備

### (1) 方針

現在、会社に存在する情報セキュリティに対する全社的なポリシーである「情報セキュリティ基本規程」と情報セキュリティに関連する各種の社内規程に準拠する形で各種ガイドライン等を作成し、それによってルール・手順書等を作成する。

### (2) ドキュメント体系

方針に基づくドキュメント体系は以下の通りである。

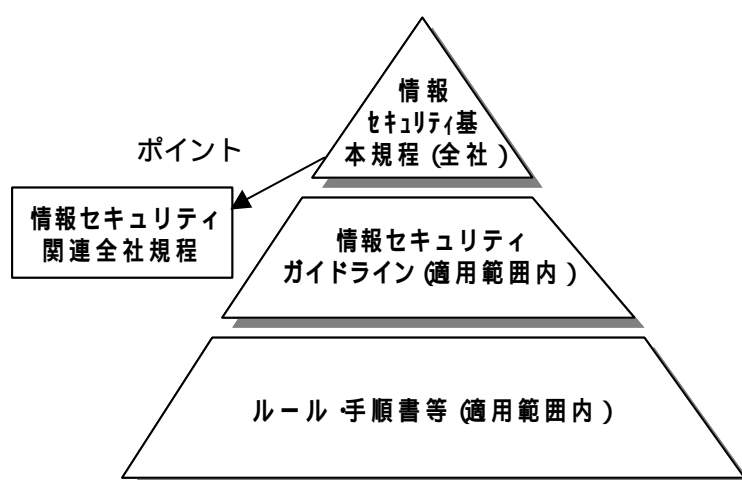


図 2-2 ドキュメント体系

#### (a) 情報セキュリティ基本規程

情報セキュリティポリシーにあたる文書である。当社の情報セキュリティに関する全社的な規程として存在する。

#### (b) 情報セキュリティ関連全社規程

情報セキュリティに関連する全社規程であり、全社員が対象となる。今回のリストアップでは、適用範囲内の情報資産について、情報セキュリティを守る対策として適用可能なものとして、情報セキュリティ対策室が選択した。

#### (c) 情報セキュリティガイドライン

情報セキュリティ管理を行うために必要であり、かつ上記(a)(b)に含まれないものについて、対策の指針を示すものとして新たに適用範囲内のみのガイドラインとして作成する。

#### (d) ルール・手順書等

(a)～(c)に基づいて作成される、部門内のルールおよび手順書。

### (3) ドキュメントのリストアップ

ドキュメント体系に対応するドキュメントのリストアップを行った。

表 2-6 情報セキュリティ基本規程（全社）

	ドキュメント名	内容	承認者	実施責任者
1	情報セキュリティ基本規程	全社の情報セキュリティ基本規程	取締役会	役員・従業員等

表 2-7 情報セキュリティ関連全社規程（全社）

	ドキュメント名	内容	承認者	実施責任者
1	文書管理規程	文書管理に関する規程	取締役会	従業員等
2	危機管理室規程	危機管理室の役割、メンバおよび責務に関する規程	取締役会	危機管理室
3	営業秘密管理規程	不正競争防止法に対応し、企業における営業秘密を管理するための規程	取締役会	役員・従業員等
4	内部監査規程	内部監査に関する規程	取締役会	内部監査室
5	就業規則	社員の就業に関する規則	取締役会	従業員等
6	システム開発規程	システム開発に関する規程	取締役会	関連部門
7	契約締結に関する規程	ユーザと契約を締結する際の規程	取締役会	
8	データセンタ内ネットワーク管理規程	データセンタの有線、無線LANの構成管理等	取締役会	
9	データセンタの環境整備に関する規程	耐震設備、耐火設備、電力供給、電話回線の維持等に関する規程	取締役会	
10	顧客情報保護規程	顧客情報保護に関する規程	取締役会	
11	携帯電話の使用に関する規程	携帯電話の使用に関する規程	取締役会	役員・従業員等

上記表2-6および表2-7は当社に既に存在する情報セキュリティ関連規程である。

表 2-8 情報セキュリティ関連規程（適用範囲）

	ドキュメント名	内容	承認者	実施責任者
1	情報セキュリティに関する 組織規程	情報セキュリティ管理体制 および責任に関するガイド ライン	取締役会	役員・従業員等

上記表 2-8 は、新たに作成する必要がある情報セキュリティ関連規程である。

表 2-9 情報セキュリティガイドライン（適用範囲内）(抜粋)

	ドキュメント名	内容	承認者	実施責任者
1	情報セキュリティ教育・訓練ガイドライン	情報セキュリティ教育に関するガイドライン	情報セキュリティ対策室長	総務部およびデータセンタ事業部第一部(大手町)の情報セキュリティ責任者
2	情報セキュリティ監査ガイドライン	情報セキュリティ監査の計画実施及び報告に関するガイドライン		内部監査室の情報セキュリティ責任者
3	情報セキュリティ事故管理ガイドライン	情報セキュリティ事故管理に関するガイドライン		各部の情報セキュリティ責任者
4	コンプライアンスガイドライン	法律等への準拠に関するガイドライン		各部の情報セキュリティ責任者
5	事業継続計画作成ガイドライン	事業継続計画作成に関するガイドライン		データセンタ事業部第一部(大手町)の情報セキュリティ責任者
6	物理的アクセス管理ガイドライン	入退室に関するガイドライン		総務部およびデータセンタ事業部第一部(大手町)の情報セキュリティ責任者
7	論理的アクセス管理ガイドライン	オペレーションシステム、アプリケーションシステム、データベース等の論理的アクセスを設定する際のガイドライン		

表 2-10 ルール・手順書等（適用範囲内）

	ドキュメント名	内容	承認者	実施責任者
1	ルール・手順書等 (ここでは詳細は記述しない)	上記1~3のドキュメントに従って各部門で作成する	情報セキュリティ対策室長	各部の情報セキュリティ責任者

上記表2-9および表 2-10は新たに作成する必要があるドキュメントである。

## 2.2.4 課題（４）情報セキュリティに関する管理組織整備

### (1) 方針

情報セキュリティに関する管理組織及び管理責任者として次の組織、責任者を設置あるいは任命することとした。

#### (a) 情報セキュリティ対策室

危機管理室の下部組織として、情報セキュリティ対策室を設置する。

情報セキュリティ対策室は、情報セキュリティに関する検討・承認および重要事項について危機管理室に事案を発議する組織としての機能および情報セキュリティに関する各部門の調整を行う機能を持つ。

#### (b) 情報セキュリティ責任者

適用範囲内の各部門に情報セキュリティ責任者を任命する。

### (2) 情報セキュリティ対策室

#### (a) 構成

情報セキュリティ担当役員（CISO：Chief Information Security Officer 相当）を情報セキュリティ対策室長とする。

情報セキュリティ対策室のメンバは、適用範囲内の各部門の部門長が兼任し、さらに事務・運営要員として専任スタッフを置く。

#### (b) 情報セキュリティ対策室の責務

情報セキュリティ基本規程のレビュー・改定案作成

情報セキュリティ関連各種ガイドラインの策定

情報セキュリティリスク評価の承認

情報セキュリティリスク管理の実施

情報セキュリティ事故の統括管理

情報セキュリティに関する各部の指導

情報セキュリティに関する社外組織との連携

その他、必要に応じ、情報セキュリティに関する重大な意思決定および危機管理室への起案を行う

(3) 情報セキュリティ責任者

各部門の部門長を情報セキュリティ責任者に任命する。

(4) 情報セキュリティ管理者

各部門からは、情報セキュリティ責任者を補佐する情報セキュリティ管理者（課長職相当）を2名任命させる。

(5) ドキュメント

「情報セキュリティに関する組織規程」に詳細を記述する。

「情報セキュリティ管理室会議議事録」を記録として保存する。

## 2.2.5 課題（5）情報セキュリティ教育・訓練

### (1) 方針

すべての役員・従業員等に対し、初期および定期的な情報セキュリティ教育を行う。

### (2) 全社的な情報セキュリティ教育

#### (a) 初期情報セキュリティ教育

総務部は、役員の新規任命時、従業員等の就業開始時に初期情報セキュリティ教育を実施する。また、ISMSの導入時に対象となる役員および従業員等に対し情報セキュリティ教育を行う。

#### (b) 定期情報セキュリティ教育

総務部は、役員・従業員等に対し、定期的な情報セキュリティ教育を実施する。

#### (c) 社内イントラによる随時の教育

情報セキュリティ教育のフォローアップとして、社内イントラにて教材を公開し、社員がいつでも参照可能な状態とする。

#### (d) 教育内容

上記(a)～(c)の教育内容を以下とする。

情報セキュリティに関する一般的な啓発

情報セキュリティ基本規程・全社的な情報セキュリティ関連規程および情報セキュリティに関するガイドラインの内容の説明等

#### (e) 情報セキュリティ教育の計画および記録

全役員・従業員等に対する情報セキュリティ教育計画を作成し、実施する。実施時には教育受講者の記録を作成し、全役員・従業員等が教育を受講したことを確認する。

(3) 部門による情報セキュリティ教育・訓練

(a) 情報セキュリティ教育・訓練

関連する各部門にて、業務を行うスタッフに対し、初期および定期的に情報セキュリティ教育・訓練を実施する。

(b) 教育・訓練内容

上記(2)-(e)の教育・訓練内容を以下とする。

業務および情報取り扱い時のルールに関する教育・訓練

事業継続計画実施に関する教育・訓練

情報セキュリティ事故対応に関する教育・訓練

教育マニュアルは各部門で作成する。

(c) 情報セキュリティ教育・訓練の計画および記録

部門内の全スタッフに対する情報セキュリティ教育計画を作成し、実施する。実施時には教育受講者の記録を作成し、全役員・従業員等が教育を受講したことを確認する。

(4) ドキュメント

「情報セキュリティ教育・訓練ガイドライン」に詳細を記述する。

「情報セキュリティ教育教材」を記録として保存する。

「情報セキュリティ教育出席簿」を記録として保存する。

## 2.2.6 課題（6）情報セキュリティの独立レビュー

### (1) 方針

内部監査室の監査の一環として、情報セキュリティ監査を実施する。

### (2) 情報セキュリティ監査

情報セキュリティ監査は、内部監査室が監査計画を立案し、各部門の監査を行う。

各部門が半年に1回以上の情報セキュリティ監査を受けるものとする。

情報セキュリティ監査の内容は下記の内容とする

(a) 情報セキュリティ基本規程・情報セキュリティに関する全社規程および情報セキュリティに関するガイドラインへの準拠に関する監査

(b) 関連する法律、条例、業界ガイドライン、契約等への準拠に関する監査

(c) 情報システムのセキュリティに関する技術的な監査（内部監査室の判断により、外部セキュリティ監査を実施している会社を利用することができる。）

### (3) 情報セキュリティ監査結果の報告

監査報告書は、内部監査室長が作成し、社長、情報セキュリティ対策室長及び監査対象部門を統括する部長に報告する。

### (4) 監査結果によるレビュー

情報セキュリティ対策室は、情報セキュリティ対策室長の指示により、監査結果を参考にして現在の情報セキュリティ対策等をレビューする。

### (5) 監査結果の反映

情報セキュリティ対策室は、監査結果によるレビューを受け、情報セキュリティ対策についての指示を出す。実行については、各部門の責任者が実施する。

### (6) ドキュメント

「情報セキュリティ監査ガイドライン」に詳細を記述する。

「情報セキュリティ監査報告書」を記録として保存する。

## 2.2.7 課題（7）情報セキュリティ事故管理

### (1) 方針

情報セキュリティ事故管理は、情報セキュリティ事故の発見・報告・対応および再発防止策の検討を管理する。

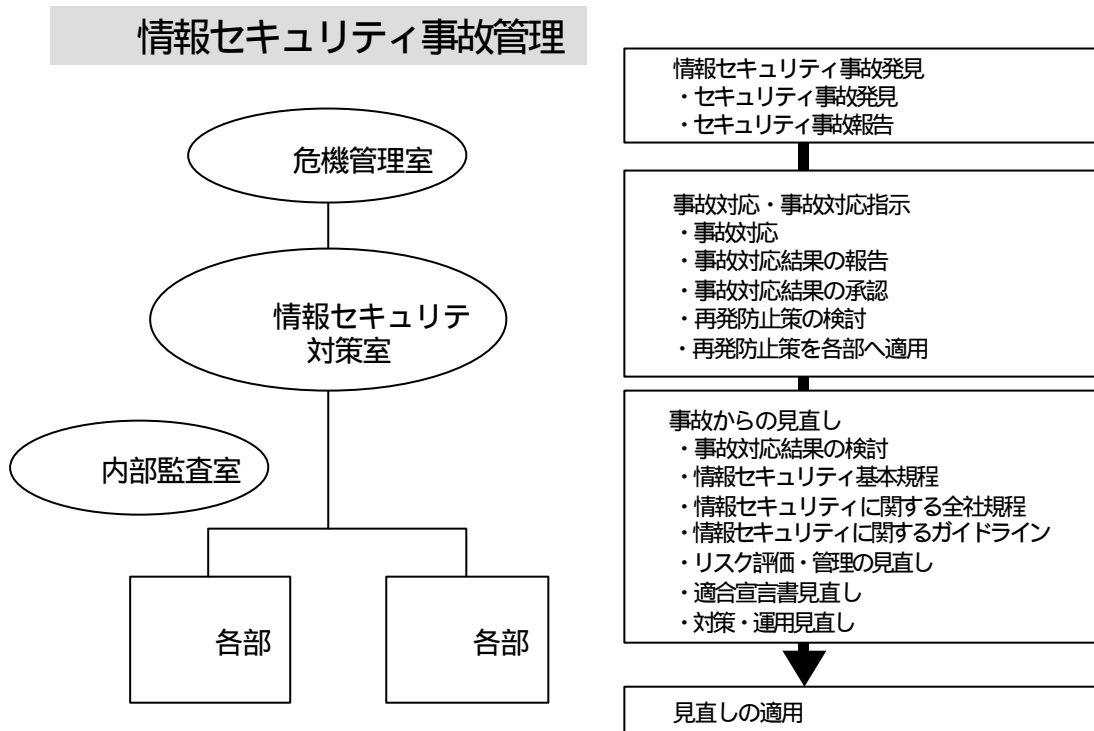


図 2-3 通常の情報セキュリティ事故管理系統

(2) 情報セキュリティ事故の定義

下記のいずれかを情報セキュリティ事故とする

表 2-11 情報セキュリティ事故の定義

	分類	内容	原因
1	業務障害	業務の継続が困難	天災、人災、公共インフラ停止、 機器破壊等
2	サービス障害	正常なサービスの継続が困難	ハード・ソフト障害、スタッフ の緊急入院等
3	情報障害	守るべき情報の不全	情報漏洩、情報改ざん、情報破 壊等
4	セキュリティ侵害	(実害とは関係なく)セキュリ ティ対策が破られる	不正アクセス、ウィルス発生、 パスワード漏洩等
5	セキュリティ障害	セキュリティ対策が実施されな いまたは効果がない	ファイアウォール設定不備、鍵 管理不備等
6	事故の疑い	上記1~5への重大な疑い	

(3) 情報セキュリティ事故の特例

特例として以下を定義する。

表 2-12 情報セキュリティ事故の特例

	分類	内容	原因
1	重大事故	経営に関わる事故	大災害、事件、多くのスタッフの緊急入院、大量の顧客情報流出等

重大事故については、別途「危機管理規程」にて定める。

(4) 事故発生時の連絡体制

情報セキュリティ事故またはセキュリティ事故に関する重大な疑いがある場合、発見者は情報セキュリティ事故の連絡を行う。

表 2-13 事故発生時の連絡体制

	連絡元	連絡先	内容
1	発見者	所属部門の情報セキュリティ責任者	情報セキュリティ事故の種類・状況 発見者氏名および発見者への連絡方法等
2	所属部門の情報セキュリティ責任者	情報セキュリティ対策室長	情報セキュリティ責任者の判断で、必要時に連絡
3	情報セキュリティ対策室長		情報セキュリティ対策室長が重大事故と判断した場合、「危機管理規程」に従い連絡

(5) 事故の調査および対応

情報セキュリティ事故の調査および対応は、情報セキュリティ責任者の指示により、各部門が行う。ただし、緊急性のある場合はこの限りではない。

(6) 事故の記録

情報セキュリティ事故対応後、情報セキュリティ責任者は、情報セキュリティ事故報告書を作成し、情報セキュリティ対策室に提出する。

(7) 事故からの学習

(a) 情報セキュリティ対策室は、情報セキュリティ事故報告書をもとに、情報セキュリティ管理および対策に関する全社的な見直しを行う。

(b) 情報セキュリティ対策室は、情報セキュリティ事故報告書をもとに、事故再発防止策の全社への適用を検討する。

(8) ドキュメント

「情報セキュリティ事故管理ガイドライン」に詳細を記述する。

「情報セキュリティ事故対策報告書」を記録として保存する。

## 2.2.8 課題（ 8 ）コンプライアンス管理

### (1) 方針

法務部が中心となり、コンプライアンス・プログラムを作成する。

### (2) 関連する法規のリストアップ

法務部は、当社業務に関連する法律、条例、業界ガイドライン等（以下、法令等）の一覧を作成する。

（本書 基本編 4 . 参考文献 (2) 法令等を参照のこと）

### (3) 責任部門および実施部門の明確化

情報セキュリティ対策室は、関連する法令等に対し、主体となって遵守すべき責任部門を割り当て、責任部門の情報セキュリティ責任者をその責任者とする。

### (4) コンプライアンス・プログラムの作成

各法律等の責任者がコンプライアンス・プログラムを作成する。この際、責任者は必要に応じ法務部の助言を受ける。

### (5) 社内規程および契約のチェック

法務部は社内規程および契約について、関連する法令等への準拠をチェックする。

### (6) ドキュメント

「コンプライアンスガイドライン」に詳細を記述する。

「コンプライアンス・プログラム」に詳細を記述する。

「コンプライアンス・プログラム」に従い、各種記録を保存する。

## 2.2.9 課題（9）事業継続計画作成

### (1) 方針

データセンタ事業部第一部(大手町)が中心となり、事業継続計画作成する。

### (2) 災害・事故の想定

考えうる災害および事故を想定し、業務への影響を分析する。

- |                |                         |
|----------------|-------------------------|
| (a) 天災         | : 地震、水害、火災、落雷等          |
| (b) 人災         | : テロ、犯罪、誤用等による事故等       |
| (c) 公共インフラの不全  | : 電力、水道、ガス、公衆回線等        |
| (d) 障害         | : ハード障害、ソフト障害、ネットワーク障害等 |
| (e) 情報セキュリティ侵害 | : 情報の改ざん、破壊、漏洩、サービス妨害等  |

### (3) リスク評価とクライシスマネジメントの実施

想定する災害・事故に対し、情報セキュリティリスク評価手順書に従ってリスクを評価し、クライシスマネジメントによるエスカレーションモデルを確立する。

### (4) 訓練および試験の実施

(3)で定義されたエスカレーションモデルに基づいて、訓練を実施する。

### (5) ドキュメント

「業務継続計画作成ガイドライン」に詳細を記述する。

「大手町事業所業務継続計画」に詳細を記述する。

「大手町事業所業務継続計画訓練・試験結果」を記録として保存する。

## 3. I S M S の運用

### 3.1 情報セキュリティリスク評価・リスク管理および適用宣言書作成

#### 3.1.1 リスク評価

「情報セキュリティリスク評価手順書」に従い、データセンタ事業部第一部(大手町)にてリスク評価を行った。

リスク評価結果の一部を図3-1に示す。

リスク評価シート

No. 17

基準目的	4章 2. セキュリティ組織 (2) 第三者アクセスのセキュリティ
基準項目	第三者に対し、組織の情報処理施設及び設備へのアクセスを許可する場合、事前にリスク評価を行い必要な措置を講ずること。
当社状況	第三者アクセス：メーカ CE の定期メンテナンス作業 (顧客によるネットワーク経由のアクセスは No.18 で記述する)

関連する情報資産

番号	内容	ビジネスへの影響
A1	大手町事業所内情報処理設備 (CPU、電源、通信機器等)	A
A2	大手町事業所内情報処理機器に格納された情報すべて	A

関連する脅威

番号	内容	備考
T1	許可されていない第三者のアクセス (不正なアクセス)	
T2	第三者の施設 / 設備の誤用	
T3	アクセスが許可されている第三者のセキュリティ 規程違反	

関連する対策

番号	内容	対策済	備考
P1	施設への第三者による入退館管理		外来者の予約・身元確認手続きなし
P2	施設内における第三者の行動への制限		事業所内の同行なし
P3	第三者へのネットワークアクセス制御	-	該当しない
P4	第三者への OS レベルアクセス制御		作業時に ID 貸与
P5	第三者へのアプリケーションアクセス制御		権限は与えない
P6	第三者のシステム使用の監視		作業時の立会い
P7	アクセス制限されている情報や区画への明確な表示		IC カード貸与で自由に行動可能
P8	アクセスする第三者へのセキュリティに関する規程等の周知	-	作業時に立ち会うため不要
P9	第三者による情報資産に対するアクセスの現場への組織の責任者の立ち会い		管理者が立ち会う

リスク

A	T	P	リスク内容	リスク	備考
A1	T1	P1	施設 / 設備の損壊や人為的な破壊等によるサービス停止	A	外来者が身分を偽って侵入し破壊
A2		P2			
A1	T2	P2	当該施設 / 設備の情報の持ち出し、改ざん	B	第三者の事業所内監視不備による持ち出し
A2		P7			
A1	T3	P2	当該施設 / 設備の情報の持ち出し、改ざん	C	第三者が不許可区域に立ち入り持ち出し
A2		P7			

図 3-1 リスク評価シート

### 3.1.2 リスク管理

リスク分析の結果、明らかとなったリスクについて、情報セキュリティ対策室がリスク管理を行った。(図 3-2 参照)

リスク管理結果は、情報セキュリティ対策室内の会議にて審査される。

リスク管理シート					No.	17
基準目的	4章 2. セキュリティ組織 (2) 第三者アクセスのセキュリティ					
基準項目	第三者に対し、組織の情報処理施設及び設備へのアクセスを許可する場合、事前にリスク評価を行い必要な措置を講ずること。					
当社状況	第三者アクセス：メーカ CE の定期メンテナンス作業					
リスク						
	内容	リスク	対策	反映先	結果	
1	施設 / 設備の損壊や人為的な破壊等によるサービス停止	A	<ul style="list-style-type: none"> <li>・ 外来者の予約 ( 外来者は 1 日以上前に管理者による予約要 ) ( 例外として情報セキュリティ責任者の承認があれば 2 時間前予約も可 )</li> <li>・ 外来者の身元確認手続き ( メーカ CE の場合、社員証確認・予約との照合 )</li> <li>・ 外来者には IC カードを渡さない ( 事業所内では管理者が同行 )</li> </ul> 管理策 ISMS 2.(2) ISMS 5.(1)	「物理的アクセス管理ガイドライン 第 4 章 3」 「大手町事業所入退管理手順第 8 章 9」 「障害管理手順 第 14 章」	C	
2	当該施設 / 設備の情報の持ち出し、改ざん	B	<ul style="list-style-type: none"> <li>・ 外来者の身元確認手続き ( メーカ CE の場合、社員証確認・予約との照合 )</li> <li>・ 外来者には IC カードを渡さない ( 事業所内では管理者が同行 )</li> <li>・ 出館時の持ち物検査</li> </ul> 管理策 ISMS 2.(2) ISMS 5.(1)	「物理的アクセス管理ガイドライン 第 4 章 3」 「大手町事業所入退管理手順 第 8 章 7」	C	
3	当該施設 / 設備の情報の持ち出し、改ざん	C	必要なし			

図 3-2 リスク管理シート (一部)

### 3.1.3 情報セキュリティ基本規程 / 情報セキュリティに関する全社規程 / 情報セキュリティガイドラインの見直し

リスク管理の結果必要となる規程・ガイドラインの見直しを行った。以下に議事録を記載する。

#### 情報セキュリティ対策会議議事録

日時：2001年8月5日

場所：大手町事業所 2階会議室

出席：山田取締役 (CISO)、鈴木部長 (データセンタ事業部第一部長)、伊藤部長 (法務部長)  
加藤部長 (総務部長)、中村部長 (内部監査室長)  
(事務) 佐藤課長、吉田

議題：リスク管理結果による規程・ガイドライン見直し

議事：

#### 1. 情報セキュリティ基本規程の見直しについて

事業継続計画に関するリスク分析の結果、不備が多かった。事業継続計画は当社にとって重要度が非常に高い。情報セキュリティ基本規程に明確に記述すべきではないか。

【結論】事業継続計画の不備は、情報セキュリティリスク評価で詳細に分析されている。情報セキュリティ規程への記述は継続案件とする。

#### 2. 情報セキュリティ関連全社規程の見直しについて

今回情報セキュリティ関連全社規程は見直しの必要はない。

情報セキュリティ関連ガイドラインの見直し

以下を見直す

物理的アクセス管理ガイドライン

情報セキュリティ管理シート 17のリスク 1、2に従って見直す。

### 3 . 監査の有効性について

内部監査という一般的なには被監査部門と独立した第三者による監査を意味する。したがって、内部監査室の要員がすべて他部門との兼務であれば有効な内部監査が実施できる可能性は低いと思われる。

現状では、内部監査室の要員のうち内部監査室長を含めすべてネットワーク運用管理部門、ファシリティ管理部門との兼務である。コスト削減のおり、内部監査室の専任者を要することは困難である。また、ネットワーク運用管理部門を監査するスキルを持っている要員が現在不足しており、やむを得ずネットワーク運用管理部門との兼務により実施している。要員不足は否めないが、監査の実施において有効性を確保するよう注意深く監視するとともに、独立した監査が可能な体制を早急に整えることとする。

### 4 . 監査員の教育訓練について

情報セキュリティ教育・訓練ガイドラインでは、各部門で部門内の全スタッフに対する情報セキュリティ教育計画を作成し、実施することになっている。しかしながら、情報セキュリティ監査が始まったばかりであり、内部監査室では具体的な教育計画の作成がされていない。また、実際の監査の教育も実施されていない。

計画を作成し、早急に教育を実施し、効果の確認をするものとする。

出席者署名 : \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

図 3-3 情報セキュリティ対策会議議事録

### 3.1.4 適用宣言書の作成

リスク管理の結果見直した部分を含め、適用宣言書を作成した。

適用宣言書は、ISMSの全管理策について作成し、各項目でYes/Noを明確に記述した。

2. セキュリティ組織			
管理目的			
(2) 第三者アクセスのセキュリティ			
目的：第三者によってアクセスされる組織の情報処理施設/設備及び情報財産のセキュリティを維持すること。			
管理策	当社の状況	適合	内容
第三者に対し、組織の情報処理施設及び設備へのアクセスを許可する場合、事前にリスク評価を行い必要な措置を講ずること。	第三者アクセス：メーカーCEの定期メンテナンス作業	Y	以下を遵守する 「物理的アクセス管理規程 第4章 3～5」 「大手町事業所入退管理手順 第8章 7～13」 「マシン室管理手順書 第2～4章」 「障害管理手順書 第14章」
第三者に対し、組織の情報処理施設及び設備へのアクセスを許可する場合、セキュリティ要求事項を明記した正式な契約を締結すること。	第三者アクセス：メーカーCEの定期メンテナンス作業	Y	以下を遵守する 「物理的アクセス管理規程 第19章 3」 「マシン保守契約書( B 社)」
情報システムの管理や制御を外部委託する場合、セキュリティ要求事項を明記した正式な契約を締結すること。	N/A	N/A	情報システム管理の外部委託は行っていない

図 3-4 適用宣言書 (部分)

## 3.2 情報セキュリティ教育

### 3.2.1 全社情報セキュリティ教育

#### (1) 教育計画の作成

総務部にて情報セキュリティ教育計画を作成し、適用範囲内の全役員・従業員等に対し教育を行うこととした。

情報セキュリティ教育は毎年4月に定期的に行うこととし、これ以外の時期に新たに任命される役員、新たに就業する従業員等については、個別に教育を行うものとした。

#### (2) 情報セキュリティ教育内容の作成

情報セキュリティ対策室が原案を作成し、総務部が教材として整理したものを使用し、情報セキュリティ教育を行った。

#### (3) 情報セキュリティ教育の実施

実施状況を以下に記述する。

表 3-1 情報セキュリティ教育実施状況

開催日	内容	対象	備考
第1回 4月30日	情報セキュリティに関する啓発 情報セキュリティ基本規程 情報セキュリティに関する全社規程 情報セキュリティに関するガイドライン 特別：「職場内の不審者への声かけについて」 特別：「パスワードの管理徹底について」	適用範囲内の 全役員・従業員 等、関連部門 (法務部等)の 従業員 = 47名	29名出席 「情報セキュリティの 心構えと注意」 「情報セキュリティ教 育出席簿」
第2回 5月7日	同上	第1回の不参 加者 = 18名	15名出席 記録は上記と同様 (3名への厳重注意)
第3回 5月9日	同上	3名	3名 記録は上記と同様

上記「特別」については、リスク管理の結果、教育項目に含めるものとした。

### 3.2.2 部門情報セキュリティ教育・訓練

#### (1) 情報セキュリティ教育・訓練計画

データセンタ事業部第一部(大手町)については、部門内情報セキュリティ教育・訓練を行う。教育・訓練計画を以下に記述する。

表 3-2 教育・訓練計画

	内容	ドキュメント	周期
1	情報システム運用技術教育・訓練	運用手順書	新規スタッフ 1回 / 1年
2	情報セキュリティ事故発見時の訓練	情報セキュリティ 事故管理ガイドラ イン	新規スタッフ 1回 / 1年
3	障害・セキュリティ欠陥発見時の教育・訓練	障害対応手順書	1回 / 1年
4	業務継続に関する教育・訓練 災害発生時の連絡 ハード・ソフト障害時の切り替え バックアップからのリストアップ	大手町事業所業務 継続計画	各項目に関する周 期は業務継続計画 に従う

#### (2) 情報セキュリティ教育・訓練の実施

データセンタ事業部第一部(大手町)の部門内情報セキュリティ教育・訓練は、計画に従って準じ実施した。

教育・訓練の結果は「教育・訓練出席者名簿」に記録した。

### 3.2.3 教育・訓練の改善

全社教育および部門情報セキュリティ教育の効果について、「教育アンケート」により出席者からアンケートを収集し、改善を行った。「教育アンケート」は記録として規定の期間保存する。

### 3.3 情報セキュリティ対策の運用および記録

#### 3.3.1 情報セキュリティ対策の実施

情報セキュリティ管理結果により見直された情報セキュリティ基本規程、情報セキュリティに関する全社規程 / 情報セキュリティに関するガイドラインを元に、データセンタ事業部第一部(大手町)にて情報セキュリティ対策を実施した。

- (1) 情報セキュリティに関する個々の対策についての管理者の明確化
- (2) 情報セキュリティに関するルール・手順書の整備
- (3) セキュリティに関する設備の導入（暗号化製品 / モバイルパソコン盗難防止用ワイヤー等）

#### 3.3.2 情報セキュリティ対策に関する記録の収集とチェック

下記の記録について、定期的チェックを行う（第三者アクセス部分の例）

表 3-3 記録の収集とチェック

	記録	周期	管理者	記録チェックの観点	対応するドキュメント
1	施設の予約および訪問者の記録	1回 / 月	施設管理者	予約者と訪問者の一致 不必要と考えられる訪問	物理的アクセス管理 ガイドライン 入退管理手順書
2	施設内のセキュリティドア等の利用記録	1回 / 月	施設管理者	入室と退室の整合性 過度に頻繁な入退室	物理的アクセス管理 ガイドライン
3	IDカード配布台帳 IDカード貸出し記録	1回 / 月	施設管理者	貸出し期限を越えた貸出し	物理的アクセス管理 ガイドライン
4	情報処理機器保守記録	1回 / 月	システム管理者	定期的な保守の実施 臨時保守の理由	運用手順書
5	保守時のID貸出し記録	1回 / 月	システム管理者	マシン保守記録との一致	運用手順書
6	情報処理関連設備 保守・試験記録	1回 / 月	施設管理者	定期保守および緊急保守	事業継続計画

### 3.4 情報セキュリティ監査の実施および記録

#### 3.4.1 情報セキュリティ監査の実施

情報セキュリティ監査計画に基づき、情報セキュリティ監査を行った。  
以下が実施内容である。

表 3-4 監査実施日

時期	2001年6月6日
実施者	内部監査室
監査対象	大手町
監査内容	入退館管理

#### 3.4.2 情報セキュリティ監査記録

「特に重要な問題とはない。」との監査報告書が作成された。

## 4. 審査事例

### 4.1 審査準備

審査登録機関は、イーデータセンター株式会社から、認証審査の相談を受けた。

審査登録機関は、認証審査の流れをイーデータセンター株式会社の担当者に説明し、見積依頼書の提出を、イーデータセンター株式会社の担当者に依頼した。

イーデータセンター株式会社では、会社概要、システム概要等で示されている内容に基づき、見積依頼書を作成した。

審査登録機関は、イーデータセンター株式会社からの見積依頼書を受理し、対象範囲のビジネスの内容、組織の規模等を考慮し、審査の工数の算定を行った。

この場合、見積工数は下記のとおり算定された。

表 4-1 見積もり工数

(人日)

見積詳細 審査段階	準 備	審 査	報告書作成	合 計
第1段階(文書審査)	0.5	1.5	1.0	3.0
第2段階(実地審査)	0.5	4.0	1.0	5.5
			合 計	8.5

審査登録機関では、上記の工数および工数に基づく費用を見積書として提示した。見積にあたっては、イーデータセンター株式会社の ISMS 適用範囲の業務ならびに情報セキュリティ上のリスクを理解できる等の専門性を有する審査員を適切に配員できるかどうかを確認し、適切な審査が実施できる能力を確保した。

審査登録機関は、イーデータセンター株式会社へ見積書を提出し、双方が同意のもと認証契約を行った。

## 4.2 審査実施

審査登録機関は、審査員を決定し、審査チームを編成し、審査日程の調整を行った。

イーデータセンター株式会社の審査実施にあたって、審査チームには審査をマネジメントするチームリーダーが配員された。さらに、十分な審査をするために審査チームが確保すべき専門性としては、IDC の経営・運営に関する事項、施設、設備に関する要求事項、利用しているサーバ、ネットワーク等の技術的事項、適用される法規制等があげられた。審査登録機関は、審査チームに IDC での業務経験がある審査員 A および関連する業務に携わった経験のある審査員 B の 2 名をアサインした。

審査登録機関は、審査日程の決定の手順を以下のように定めている。

- (1) 受審組織におおよその審査時期の希望をたずねる。
- (2) アサインされた審査員（全員）が対応可能な（あるいは調整できる）具体的な日程を受審組織に示す。
- (3) 最終的に受審組織と合意の上、決定する。決定したときには正式に文書で通知する。

審査チームは、以下の審査業務計画を作成し、審査を実施した。

#### 4.2.1 Stage 1（文書審査）の審査業務計画

審査チームは、参照する主要な文書類を以下とした。

表 4-2 文書審査対象文書

ISMS 要求事項	審査ポイント	事例のレビュー対象文書
セキュリティポリシー	セキュリティポリシーが発行され、経営陣によって承認され、全従業員に知らされ、組織に関連するものであり、適切にレビューし更新する仕組みがあることを確認する。	情報セキュリティ基本規程、およびその管理手順
適用範囲	範囲が明確に定められていること、適切/達成可能な範囲であること、境界線及び接点は明確にされている事を確認する。	ISMS 適用範囲に関する文書、組織図、設備/施設図面、ネットワーク図、ケーブル配線図
リスク評価	関連する全ての資産の脅威と脆弱性の包括的なリスク評価が行われていて、プロセスは文書化されており繰り返し実施可能であること、そして、現状のリスク評価の結果を維持していることを確認する。	リスク評価手順、 リスク評価の結果 (リスク評価シート)
リスクマネジメント/管理策の選択	リスク評価の検討結果を反映して管理策の選択が行われていることを確認する。 なぜ管理策が選択されたか理解し、なぜ確かな管理策が選択されなかったかを立証する為に客観的証拠を見る。	リスクマネジメント手順 (会議議事録、等) リスクマネジメント結果 (リスク管理シート) 選択された管理策一覧
適用宣言書	なぜ管理策が選択されたか理解できることを確認する。 なぜある管理策が選択されなかったかを立証する為に客観的証拠を見る。	適用宣言書
上記のレビュー	ポリシー、対象範囲、リスク評価の計画されたレビューであり、実施されたそのようなレビューを立証する為の証拠があること、およびその証拠にのっとったマネジメントチームの活動を確認する。	レビューの記録 マネジメントレビュー記録
文書管理	全ての文書を会社のポリシーに従って管理することを確認するために正式に文書化された手順を確立していることを確認する。	文書一覧 文書管理規程
記録	ISMS が機能していることを実証する為に利用可能でなければならない。	記録一覧

ISMS 要求事項	審査ポイント	事例のレビュー対象文書
その他の主要な手順	手順は適切であり、正式にレビューされていること、必要に応じ、技術的な準拠のチェックが実施されていることを確認する。	
教育訓練	どのようにトレーニングの必要点を明確にし、必要な手順を対象となる要員に理解させているかを確認する。	
セキュリティインシデント報告手順	プロセスが文書化され、使用され、事故が敏速に解決され、潜在的な問題や傾向を明確にするために調査する。	情報セキュリティ事故管理ガイドライン
事業継続計画	活動の証拠と文書化されたポリシー	事業継続計画作成ガイドライン 事業継続計画
法的要求事項	要求される法的要求事項を認識した証拠	コンプライアンスガイドライン コンプライアンスプログラム

審査チームは、文書審査に関して、下記のヒアリング対象を決定した。

表 4-3 文書審査ヒアリング対象

審査対象 ISMS 要求事項	経営層	情報セキュリティ対策室	内部監査室	法務部	総務部	データセンタ事業部第一部(大手町)
情報セキュリティポリシーおよびポリシーのレビュー						
適用範囲						
リスク評価						
リスクマネジメント						
管理策の選択						
文書管理						
記録						
情報セキュリティ組織						
教育訓練						
情報セキュリティ事故及び誤動作への対処						
事業継続管理						
法的及び準拠性						
情報セキュリティポリシー及び技術への準拠性レビュー						
情報セキュリティ手順						

\* : の箇所について、審査を行う。

#### 4.2.2 Stage 2（実地審査）の審査業務計画

審査チームは、実地審査に関して、下記のヒアリング対象を決定した。

表 4-4 実地審査ヒアリング対象

ISMS 要求事項 / 審査対象	経営層	情報セキュリティ対策室	内部監査室	法務部	総務部	データセンタ事業部第一部 (大手町)	備考
情報セキュリティポリシーおよびポリシーのレビュー							
適用範囲							
リスク評価							
リスクマネジメント							
管理策の選択							
文書管理							
記録							
情報セキュリティ組織							
教育訓練							
情報資産の分類と管理							
情報セキュリティ事故及び誤動作への対処							
物理的・環境的セキュリティ							ハイリスク領域に関する手順、運用面でのセキュリティ手順への準拠、内部監査の指摘事項については正が完了していない部門や手順
通信及び運用管理							
アクセスコントロール							
システムの開発及びメンテナンス							
事業継続管理							
法的及びその他の要求事項への準拠性							
情報セキュリティポリシー及び技術への準拠性レビュー							

\* : の箇所について、審査を行う。

#### 4.2.3 審査プログラム

審査プログラムは、第一段階、第二段階それぞれで策定される。第一段階は、審査概要で示されるように、主に経営層、マネジメントシステムの管理部門を中心に行われる。ここでは、第二段階の審査プログラムを例示する。

表 4-5 審査プログラム

段階	日付	時間	審査員	審査対象	チェック項目(＊)
第一段階	2001年 9月11日	9:00～	A、B	オープニングミーティング	
		9:20～	A、B	経営層	4.1、4.2
		10:15～	A、B	情報セキュリティ対策室	3.2、3.3、3.4、3.5、3.6 4.1～4.10
		12:00～	A、B	昼食	
		14:00	A、B	内部監査室	3.6、4.2、4.10
		16:00	A、B	審査チームミーティング	
		17:00	A、B	デイリーミーティング	
第二段階	2001年 9月12日	9:00～	A	総務部	3.5、4.1、4.2、4.10
		10:30～	A	総務部(人事)	3.5、3.6、4.2、4.4、4.10
		9:00～	B	データセンタ事業部 第一部(大手町)1課	4.1～4.10
		12:00～	A、B	昼食	
		13:00～	A	データセンタ事業部 第一部(大手町)2課	4.1～4.10
		13:00～	B	データセンタ事業部 第一部(大手町)3課	4.1～4.10
		16:00	A、B	審査チームミーティング	
		17:00	A、B	クロージングミーティング	

(＊)3.xは、ISMS認証基準(Ver0.8)の第3 ISMS要求事項、4.xは、第4 詳細管理策 参照のこと

## 4.3 審査結果

### 4.3.1 審査員メモ

(注意)

ここに示すメモは、あくまで想定された事例に基づくものである。

仮に実際の審査の過程において類似の状況があったとしても、必ずしも審査のすすめかたや証拠の収集をおこなう審査技法、および審査の結論が同じになるとは限りらない。

#### (1) 情報セキュリティ・インフラストラクチャに関する項目

##### (a) 規程関係についての状況

文書審査の結果、次のことが明らかになった。

#### 情報セキュリティ・インフラストラクチャについて

情報セキュリティフォーラム機能およびクロスファンクショナルフォーラム機能は「情報セキュリティ対策室」が担うものとして定義されている。

「情報セキュリティ対策室」は、情報セキュリティ担当役員が室長として運用している。

情報セキュリティ対策室のメンバは、ISMS 適用範囲内の各部門の部門長が兼任し、さらに事務・運営要員として専任スタッフを1名置いている。

「情報セキュリティ対策室」は1ヶ月に1回の頻度で定例会が開催され、情報セキュリティに関する報告・審議・承認が行われる。

情報処理施設および設備の新規導入について、一定金額以上のものは「取締役会」にて承認を行っている。

情報セキュリティ最新情報は、システム運用部門の不正アクセス監視チームが社内イントラで情報提供している。

監督官庁、規制当局との連絡は、必要時に総務部が行っている。

独立した監査部門が存在し、監査計画に従って定期的に情報セキュリティ監査を行っている。

(b) 実施状況のヒアリング

情報セキュリティ対策室長である情報セキュリティ担当役員にインタビューを実施した。その結果、下記の実施状況が把握できた。

前回の「情報セキュリティ対策室」定例会は8月に実施され、そこで情報セキュリティ基本規程の見直し、情報セキュリティ関連全社規程の見直し及び情報セキュリティ関連ガイドラインの見直しについて審議が行われていた。

「情報セキュリティ対策室」は、当初ISMS適用範囲内の各部門の部門長のみでスタートしたが、危機管理室の9月の決定により、適用範囲外である営業部と川崎事業部の部門長も参加し、全社をカバーする組織となっていた。

「情報セキュリティ対策室」定例会は基本的には全員参加であり、不参加のスタッフには議事録にて内容を通知している。

情報セキュリティ事故が発生した場合、次回の定例会に報告され、必要なら社内の情報セキュリティ対策および情報セキュリティポリシーの見直しが審議される。

前回議事録を閲覧した。情報セキュリティ基本規程の見直し、情報セキュリティ関連全社規程の見直し及び情報セキュリティ関連ガイドラインの見直しに関する審議が行われ、結果が残っている。

考察（審査員の心証）：

【情報セキュリティ対策室を中心とした、情報セキュリティに関する経営陣の意思決定、組織横断的な意思疎通がなされていること等、ISMS 認証基準(Ver.0.8)の4.2(1)をはじめとする情報セキュリティインフラストラクチャに関する条項に対し適合しているとの心証を得た。】

## (2) 内部監査についてのヒアリング

### (a) 規程関係・ガイドラインについての状況

デスクトップレビューの結果、次のことが明らかになった。

#### 内部監査について

データセンタでは内部監査制度があり、内部監査規程が定められている。

また、情報セキュリティについての情報セキュリティ監査ガイドラインが定められている。

内部監査規程の内容によると

- ・ 監査は半年に一度以上実施する。
- ・ 監査実施部門は内部監査室である。
- ・ 内部監査の実施結果は内部監査室長に報告される。
- ・ 内部監査室長は監査報告書を作成し、社長及び監査対象部門を統括する部長に速やかに報告することになっている。

情報セキュリティ監査ガイドラインの内容によると

- ・ 情報セキュリティ監査は内部監査の一環として実施する。
- ・ 内部監査規程は情報セキュリティ監査ガイドラインの上位規程となる。
- ・ 監査実施の前に監査計画を策定し、内部監査室及び情報セキュリティ対策室室長の承認を得ることになっている。
- ・ 情報セキュリティ監査結果については、社長、監査対象部門の責任者のほかに情報セキュリティ対策室長にも報告することになっている。

#### 教育について

情報セキュリティ教育・訓練ガイドラインでは次のことが規定されている。

- ・ 部門内の全スタッフに対する情報セキュリティ教育計画を作成し、実施する。
- ・ 各部門の管理職以上は担当者が教育を適切に受講していることを確認する。

(b) 実施状況のヒアリング

内部監査室長及び内部監査担当者にヒアリングを実施した。その結果、以下の実施状況が把握できた。

内部監査制度がはじまって1年未満であり、内部監査は一度しか行われていないが、内部監査報告書は作成されていた。監査報告書が作成されてから3ヶ月が経過しているが、「社長及び情報セキュリティ対策室長には報告していない」とのことである。

考察（審査員の心証）：

【監査報告書が3ヶ月を経てまだ社長、情報セキュリティ対策室長に報告されていないということは、内部監査規程違反、情報セキュリティ監査ガイドライン違反になると思われる。したがって、4章10(2) に対する不適合の可能性がある。】

担当者に監査調書の提出を求めたが、担当者4名中2名はノートに書いたメモ書きを提出した。残りの2名については、「ノートがいっぱいになったため、すでに廃棄した」とのことである。

考察（審査員の心証）：

【通常、監査の実施の証拠は、文書化され保管する必要がある。これを監査調書と呼び、監査調書は監査を実施した証拠の記録として重要である。したがって、3章(4) に対する不適合の可能性がある。】

内部監査担当者にノートの廃棄方法について確認したところ、「ノートは通常のごみとしてごみ箱に廃棄した」とのことである。各担当者が持っているノートについては、「リスク分析の時の対象となっておらず重要性の分類が行われていない。そのため通常のごみと同様にごみ箱にすてている」とのことである。

考察（審査員の心証）：

【各人が利用するノートについて、リスク評価が実施されておらず、重要性の分類がおこなわれていない。一般に、各人が利用するノートを会社の正式な文書として登録し、管理することは考えられない。しかしながら、各人のノートには、ミーティング時のメモ書き等、重要な機密情報が記載されていることが想定される。会社の正式な文書としないとしても、その取り扱いには十分に教育を実施して、情報保護に努める必要があります。この事実は情報保護に対する教育が十分にできていない状況証拠と考えられる。したがって、4章4(2) の不適合の可能性がある。】

### (3) アクセス権管理等についてのチェック

契約遵守（4章 10（1））についての検証を行うために、サンプルとして消費者金融会社（以下 A 社という）をサンプルに選び、審査手続きを実施した。

A 社との契約の内容等は詳細な説明は「5. 参照資料（会社の詳細情報）」を参照のこと。

#### (a) 実施状況（ヒアリング）

アクセス権登録の担当者に質問を実施し、ID 及びイニシャルパスワードの登録について質問をした結果、「ユーザの定めた手順通りに実施している」とのことである。ID 登録申請書について、2001 年 4 月から 8 月末までをレビューした結果、新規登録の申請のユーザ数は 15 名、アクセス権限の変更の申請は 30 名、廃棄についての申請は 10 名であった。このうち、A 社の責任者の承認印あるいはサインがないものが 15 名分あったが、データセンタ側では、そのまま新規登録、変更登録、廃棄登録を実施していた。

#### 考察（審査員の心証）：

【今回の契約では、ユーザの責任者の承認がないものを登録してよいかどうかについて、契約上明確になっていないように見られる。A 社とデータセンタ側の責任境界が不明確となるため、契約上明確にしておく必要がある。また、一般的な常識から考えて、データセンタが A 社の責任者の承認がないユーザの依頼というのは、ユーザとしての正式な依頼か否かが不明であり、契約に違反している可能性がある。】

また、A 社のアクセス権限の登録について、データセンタ側では特に上司による承認手続は実施していない。データセンタ側は「A 社の ID の新規登録、変更登録、廃棄登録の申請書にデータセンタ側の承認印を押印する部分がないため」と回答してきた。

#### 考察（審査員の心証）：

【データセンタ側のリスク評価の充分性に疑問が生じる。データセンタ側の担当者の判断のみでユーザ登録をすることは、ユーザとの間でトラブルが生じた場合、データセンタ側の責任の所在が不明確になる。データセンタとしてのリスクを考慮した場合、A 社のアクセス権の変更を実施したことについて、データセンタ側での承認手続を実施すべきと考えられる。この点について、ガイドライン等で決まっていなかったのか？決まっていなかったら、3 章(2) に対する不適合の可能性はある。決まっているのであれば、4 章 10（1）に対する不適合の可能性はある。】

データセンタ側では、A社からの指示がないため、特にチェックはしていないが、既に退職している人のユーザの ID(オペレーションシステム、アプリケーションシステム及びデータベース等)が多数存在すると考えている。

審査員はデフォルト ID のパスワードのチェックを実施した。オラクルのユーザ ID を調べた結果、次のデフォルト ID のパスワードがイニシャルパスワードであった。

system、scott、dbnmp、po8。

scott、dbnmp、po8 については業務引き受けの時に ID 削除の依頼があったと担当者は回答している。しかし、その証拠を示す書類がなかった。

考察 (審査員の心証):

【これは、契約違反と考えられる。したがって 4 章 10(1) に対する不適合の可能性はある。】

審査員はパスワードファイルにシャドウパスワードが利用されているかを検証した。運用責任者は「すべてのユーザについてシャドウパスワードを利用している」と回答した。その回答を裏付けるためにパスワードファイルをアウトプットしてもらった。パスワードファイルは以下の通りであった。(一部省略)

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:dXkLcCjNxJ:3:4:adm:/var/adm:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
mail:x:8:12:mail:/var/spool/mail:
uucp:x:9:14:uucp:/var/spool/uucppublic:
operator:RpNgXjgkRnCSi:10:4:operator:/root:/bin/bash
postmaster:x:14:12:postmaster:/var/spool/mail:/bin/false
test:x:0:0:test:/root:/bin/bash
9701238:x:501:100:smiyatake:/home/kanri:
9703482:x:502:100:eyabe:/home/kanri:
(一部省略)
0002948:PXMNxjPjeiFrq:501:100:tswatanabe:/home/kanri:
(一部省略)
8801859:x:0:0:yotomaru:/home/kanri:/bin/csh
```

考察（審査員の心証）：

【adm、operator、0002948 にシャドウパスワードが使われていない。これは契約違反であり、4 章 10(1) の不適合の可能性がある。また、test、8801859 の権限は root と同じ権限である。ユーザの8801859 がなぜ root 権限をもっているのか、追加で質問する必要があると思われる。ユーザからの依頼なのか、root、test のパスワードがないことに気がついて自分で root の権限を取ったのかが不明だからである。また 8801859 は c シェルが利用できる。管理の状況が不十分である可能性が高い。】

シャドウパスワードファイルについては以下の通りであった。（一部省略）

root:6ksTid0degINs:16243:0:30:3:3:30:0

bin:\*:15432:0:0:0:0:0

（一部省略）

test::16384: 0:0:0:0:0

（一部省略）

8801859:kld0krsYesKeW: : 0:0:0:0:0

考察（審査員の心証）：

【ユーザ test にはパスワードが設定されていない。test が誰に指示によって作成されているのか？ユーザが登録しているのか？データセンタ側が勝手に設定したユーザなのか？追加で質問する必要がある。ユーザが登録依頼しているものであり、ユーザがパスワードを null にしているのであれば、ユーザの責任である。データセンタ側が設定しているのであれば、契約違反である。】

負荷についての管理レポートをレビューした。管理レポートはデータセンタのユーザ担当の責任者名で契約に従い毎月提出されている。責任者にインタビューをした結果、「負荷管理システムの自動レポート作成機能によりレポートを作成しているため、毎月のレポートについての内容の正確性については特にチェックしていない」とのことである。「システムからのレポートは内容をチェックせずに自動的にユーザに郵送されるようになっている」とのことである。

考察（審査員の心証）：

【負荷管理システムの自動レポート機能が正しく設定されているかどうかについてデータセンタ側でチェックが必要ではないだろうか？】

バックアップテストについて前回 10月中旬に実施したため、4月下旬に3月末のシステム及びデータを用いて実施することになっていた。しかし、「システム開発のため現在まだ実施できていない」とのこと。契約では半年に一度することになっていたが、ユーザの担当者レベルと相談した結果、「今回のシステム開発が終了する12月末までは待ってもらうことになっている」とのことである。「ユーザの責任者が承認しているかどうかの確認はしていない」とのことである。

考察（審査員の心証）：

【担当者レベルで契約で定められているバックアップテストを延期することは契約違反にならないだろうか？なるとすると4章10(1) に対する不適合の可能性はある。】

今回のシステム開発プロジェクトのスケジュールをレビューした結果、ユーザアクセプタンステストを実施する前に、事業継続性の検証テストの予定がはいついていないことに気がついた。開発の契約では、新たなシステムのバックアップリカバリーテストをユーザアクセプタンステストの前に実施することになっていた。我々の指摘により、早速、プロジェクト担当者が日程の調整にはいったが、現在のところ「システム開発プロジェクトが遅れ気味で調整は困難」とのことである。ユーザの担当者に「リリース後にできないかについて確認をとる」とのことである。

考察（審査員の心証）：

【新たなシステムのバックアップリカバリーテストは重要なテストである。契約にも実施が盛り込まれており、通常は実施すべきである。ユーザからの正式な承認がない場合は4章10(1)に対する不適合の可能性はある。】

審査チームは、上記の審査活動の結果を総合的に判断し、数件の軽微な不適合を発行することとした。

#### 4.3.2 審査結果

審査の結果、軽微な不適合が指摘された。軽微な不適合については、イーデータセンター株式会社より、是正計画が示され、審査チームはその計画を適切であると判断し、是正計画を含め審査報告書を取りまとめ、審査登録機関に登録を推薦する旨報告した。

#### 4.3.3 認証登録

審査登録機関Aはその報告を受け、レビューした結果、イーデータセンター株式会社の認証を決定した。登録証には、下記の内容が記載されることになった。

表 4-6 登録証記載事項

・事業者	: イーデータセンター株式会社 大手町データセンター
・適用規格	: ISMS 認証基準 (Ver.0.8)
・適用範囲	: ISMS のスコープ
・適用サイト	: 住所

#### 4.3.4 維持審査 / 更新審査

事例会社の維持審査は半年に一回ごとで実施することが事例会社と審査登録機関の間で合意された。維持審査の工数は、1人日、3年後の更新審査は2人日と見積もられた。

維持審査では、ISMSのフレームワークに関する事項については毎回、審査対象とされ、選択された詳細管理策については、3年間（5回の維持審査）で一巡する割合で審査されることになった。

更新審査では、基本的にすべてのISMSの要素がチェックされることになっている。もちろん、この初回審査の不適合事項の是正結果については次回の維持審査で審査されることになっている。

## 5. 参照資料（会社の詳細情報）

ここでは、事例編のイーデータセンタ株式会社の詳細情報について記述しています。

### 5.1 基本情報

- (1) 認証取得申請事業者の名称  
イーデータセンタ株式会社（データセンタ事業部第一部（大手町データセンタ））
- (2) 認証取得申請事業者の業務  
データセンタ事業、運用監視事業、運用委託事業
- (3) 大手町事業所の設置状況  
通常オフィスビルの15Fから18Fまでの4フロアをデータセンタとして利用している。
- (4) 事業所の面積：  
10,000 m<sup>2</sup>のデータセンタエリアと1,000 m<sup>2</sup>の事務所エリア
- (5) 大手町データセンタの顧客  
都市銀行、地方銀行、消費者金融業、製造業、給与計算を実施しているASP、電子メール配信を実施しているASP他
- (6) 従業員等の数：

表 5-1 従業員数内訳

	従業員 (アルバイトを含む)	派遣社員
大手町事業所	35名	7名
全社	150名	50名

(7) 顧客及び顧客のシステム :

表 5-2 顧客システム内訳

	主要な顧客	主要な顧客のシステム
IBM AS400	都市銀行、地方銀行、	業務基幹システム
	地方銀行	与信管理システム
UNIX	消費者金融業	与信枠設定サポートシステム
	ASP 事業者	給与計算システム (SAP)
Windows NT, 2000, XP	ASP 事業者	電子メール配信システム

\*:UNIXはサンマイクロシステムズ、ヒューレットパッカード、IBM AIX、Linux等である。

## 5.2 契約形態

### 5.2.1 ファシリティ提供

#### (1) 電源

電源については、顧客のコンピュータに接続されている電源コネクタまでがデータセンター側の責任である。電源のバックアップは3日である。

#### (2) ネットワークコネクタ

構内ネットワークについては、顧客のコンピュータに接続されている LAN コネクタまでがデータセンター側の責任である。

#### (3) 物理的アクセス管理（防犯管理を含む）

データセンターの顧客に開放されている区画についての物理的アクセス管理についてはデータセンター側の責任である。顧客用のラックの鍵の管理もデータセンター側の責任である。

#### (4) 空調設備

空調設備については、全てデータセンターの責任である。温度湿度管理を実施している。

#### (5) 防災設備

防災設備については、全てデータセンターの責任である。

### 5.2.2 運用監視

顧客のサーバの死活監視、障害通知等のサービスの提供を契約に基づいて行う。

### 5.2.3 運用委託

顧客のシステム運用監視のみならず、運用まで請け負う。ホスト系の場合、バッチプログラムのキック、JCLの修正等、いわゆる運用業務一般に携わる。また、バックアップテープ等のサービス内容は顧客との個別の契約による。

### 5.3 消費者金融業（以下 A 社）の与信枠設定サポートシステムの業務委託契約内容の要約

#### 5.3.1 業務委託範囲

与信枠設定サポートシステムのサーバ等（スイッチングハブ、ルータ、トラフィックアナライザ、ロードバランサ等の機器も含む）の物理的アクセス管理、与信枠設定サポートシステムの運用全般

#### 5.3.2 与信枠設定サポートシステム

与信枠設定サポートシステムは A 社の顧客属性毎の与信枠を設定するプロセスをサポートする機能をもったシステムであり、A 社の特定のチームのみが利用するシステムである。

#### 5.3.3 機器の所有権

アプリケーションサーバ、データベースサーバ、付属機器（VPN ルータ等）OS 及びアプリケーションの所有権は A 社にある。

### 5.3.4 システム構成(概要)

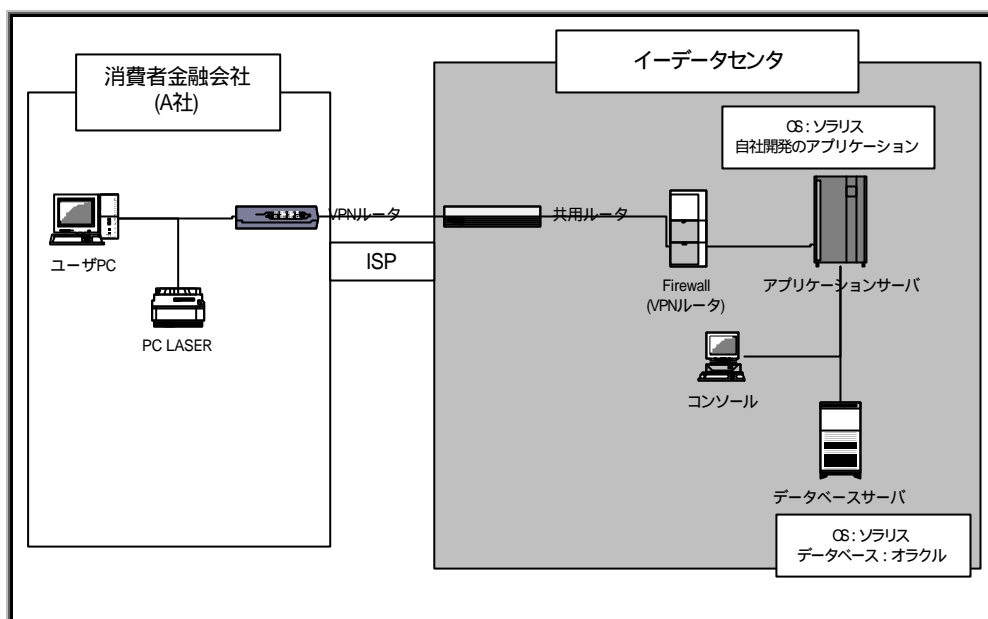


図 5-1 システム構成概要

A社とデータセンタ間はVPNを利用してつないでいる。  
システムはアプリケーションサーバ、データベースサーバからなる。  
アプリケーションサーバは、本番機2台、開発機1台である。  
データベースサーバは本番機1台、開発機1台である。  
アプリケーションサーバ、データベースサーバともOSはソラリス (Solaris 8) である。  
アプリケーションはA社開発のソフトウェアである。  
データベースはオラクルデータベース (oracle 8.1) を利用している。  
データセンタ内の共用ルータからデータベースサーバまでのネットワークはA社に責任がある。

### 5.3.5 情報セキュリティに関する覚書の内容の要約

#### (1) 論理的なアクセス管理

論理的なアクセス管理は A 社の依頼に基づきデータセンタのオペレータが実施する。

実施事項は以下の通りである。

ユーザ ID 新規登録、変更登録、登録抹消。

デフォルト ID の削除。(削除できないデフォルト ID は特殊文字を含む 10 文字以上のパスワードを設定し、そのパスワードをメモ書きし、封筒に入れ、割印をし、耐火金庫に保管する。)

ID 毎の資源へのアクセス権制御 (データベースも含む)。

パスワードファイルへのアクセス管理は特権ユーザのみにアクセス権を与える。

(OS のパスワードファイルはシャドウパスワードファイルを用いる)

データセンタは例外的な運用として、管理用に ID を登録することができる。この場合は、事前に A 社に ID 設定の目的、アクセス権等について、A 社の承認を得る必要がある。

四半期に一度全てのシステムの登録ユーザのアクセス権について A 社にレポートを提出する。

#### (2) パフォーマンス及び負荷管理

ネットワーク負荷状況は月次で A 社に報告する。

与信枠設定サポートシステムに関係するハードウェア (Firewall、アプリケーションサーバ、データサーバ、ロードバランサ、ルータ) についての障害監視を実施し、その結果を月次で A 社に報告する。

与信枠設定サポートシステムに関係するすべてのハードディスクの容量監視を実施し、その結果を月次で A 社に報告する。

与信枠設定サポートシステムで利用するオラクルデータベースのパフォーマンスチューニングはデータセンタが A 社に実施する。

与信枠設定サポートシステムに関係するすべての CPU の負荷監視を実施し、その結果を月次で A 社に報告する。

(3) 事業継続計画、バックアップ管理

A社の事業継続計画に従い、データセンタはシステム継続性の検証をする。  
データのバックアップ・リカバリーテストのテストはA社の指示書に従い、半年に1度以上データセンタ側で実施する。

実施内容及びその結果についてはA社に遅滞無く報告する。

アプリケーション、OS、DBMSのバージョンアップ等システムの大規模な変更がある場合は、A社の要請に従い別途システムの継続性の検証をする。

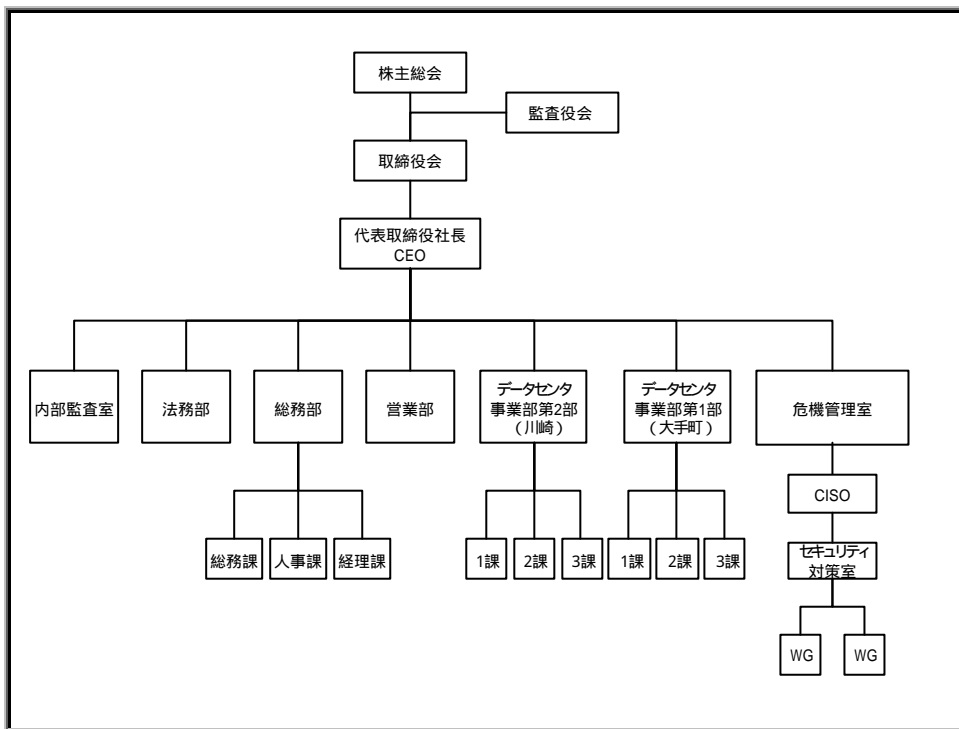


図 5-2社内組織図

## 5.4 情報セキュリティ基本規程

### 情報セキュリティ基本規程

#### 第1章 総則

##### (目的)

第1条 情報セキュリティ基本規程の設定目的は、社会的信用の失墜、事業の中断及び会社資産の喪失から当社を守り、当社のすべての従業員等に情報保護の必要性和責任について理解を深めることにある。

##### (用語の定義)

第2条 本規程において「情報資産」とは、情報、情報を取り扱うための機器（情報を処理するコンピュータ、及びそれを利用するために必要なデータ通信装置、記憶媒体、空調設備等を含む）サービス（電力、水道、通信サービス等を含む）ソフトウェア、及びそれらを取り扱う人材をいう。

- 2 本規程において「情報セキュリティ」とは、情報の機密性、完全性及び可用性を確保し維持することをいう。
- 3 本規程において「当社」とは、イーデータセンタ株式会社のことをいう。
- 4 本規程において「従業員等」とは当社の取締役、監査役及びこれに準ずる者（以下、役員等と呼ぶ）並びに従業員、臨時従業員のことをいう。
- 5 本規程において「顧客」とは当社と取引のある「個人」「法人」のことをいう。

##### (適用範囲)

第3条 本規程は、当社で取り扱うすべての有形・無形の情報に適用する。当社で取り扱う情報には、当社の情報のみならず、顧客から預かっている情報も含まれる。また、本規程は、当社のすべての従業員に適用される。また、本規程は、当社の役員等にも準用される。

- 2 当社で取り扱う情報を当社以外の第三者が取扱う場合においても、本規程に準拠した取扱を実施する旨の契約を締結するように努めるものとする。

##### (組織と責任)

第4条 危機管理室のもとに情報セキュリティ対策室を設置する。情報セキュリティ対策室の責任と権限は「情報セキュリティに関連する組織規程」で別途定めるものとする。

- 2 各部の長は情報セキュリティ管理者として、各部の情報セキュリティについての責任を有する。情報セキュリティ管理者は責任と権限は「情報セキュリティに関連する組織規程」で別途定めるものとする。

- 3 部長は情報セキュリティ担当者を1名以上任命するものとする。情報セキュリティ担当者についての職務は「情報セキュリティに関連する組織規程」で別途定めるものとする。

## 第2章 情報資産の管理と取扱い

### (情報資産に対する基本的な考え方)

第5条 情報資産に対する権限は、業務上必要な者のみに必要な権限のみを与えるものとする。また、必要な情報を適時に利用できるようにするための適切な体制を構築するものとする。

### (情報資産の管理)

第6条 当社で取り扱うすべての情報資産は、情報セキュリティ管理者によって適切に管理されなければならない。

### (情報資産の分類と対策の選択)

第7条 当社で取り扱うすべての情報資産は、その内容に応じて適切に分類され、情報資産の重要性に応じて適切に管理されなければならない。情報資産の分類及びその対策の選択については、「情報リスク管理規程」に別途定める。

### (情報資産の取扱い)

第8条 当社及び顧客が当社に預託した情報資産は、法令、契約及び当社の定める情報セキュリティに関連する規程に従い、適切に取り扱わなければならない。

第9条 情報セキュリティ管理者は、情報資産が適切に管理されていることを、継続的に監視しなければならない。

### (監査)

第10条 内部監査室は、情報資産の管理が適切に行われていることを定期的に監査しなければならない。内部監査の実施については、「内部監査規程」に別途定める。

### (セキュリティ事故の対応)

第11条 情報セキュリティに関連する事故が発生した場合は、発見者は速やかに情報セキュリティ管理者又は情報セキュリティ対策室にその内容を報告しなければならない。

- 2 情報セキュリティに関連する事故原因は分析され、必要に応じて再発防止策を講じなければならない。
- 3 その他、情報セキュリティ事故に関連する事項については、「情報セキュリティ事故管理規程」を別途定めるものとする。

(教育)

第12条 当社のすべての従業員等は、職務に応じて必要な情報セキュリティ教育を定期的に受けなければならない。

(例外管理)

第13条 技術的要件、費用上の問題等で本規程及び情報セキュリティ関連する規程に定められた事項の達成が困難と認められる場合は危機管理委員会の承認を受け、例外として別途運用することができる。

### 第3章 罰則

(従業員に対する罰則)

第14条 本規程及び情報セキュリティに関連する規程に違反する行為を行った従業員は、その程度に応じて就業規則に定めるところにより懲戒を受ける場合がある。

附則

(施行期日)

(ア)本規程は平成13年4月1日より施行する。ただし、第14条については平成13年10月1日より施行する。

(規程の改廃)

(イ)本規程の改廃は取締役会の承認に基づき行う。

## 6. 付属資料（基準対応表）

ISMS認証基準(Ver.0.8)及びBS7799監査ガイド(DISC PD3004:1999)と安全対策認定基準の対応表(参考)

\*本対応表はパイロット事業の参考としてISMSガイド(Ver. 0.8)のみに添付し、以降に発行するガイドには添付いたしません。

\*ISMS認証基準(Ver.0.8)に対応する旧安全対策認定基準は、関連した基準を掲載してあります。

I S M S 認証基準(Ver.0.8)		BS7799	旧)安全対策認定基準	
章	項目	管理目的	BS7799監査ガイド(PD3004)	
1	適用範囲			
2	用語及び定義 (1) 情報セキュリティ (2) リスクの評価 (3) 適用宣言書			
3 I S M S の 要 求 事 項	(1) 一般			
	(2) マネジメント枠組みの確立	3.1 管理の枠組み		
	(3) 管理策の実施	3.2 I S M S の実行		
	(4) 文書化	3.2.1 セキュリティポリシー・マニュアル及び手順		
	(5) 文書管理	3.2.2 文書管理		
	(6) 記録	3.2.3 記録		
4 詳 細 管 理 策	1. セキュリティポリシー	(1) 情報セキュリティポリシー	4.1.1 情報セキュリティポリシー	
	2. セキュリティ組織	(1) 情報セキュリティ・インフラストラクチャ	4.1.2.1 情報セキュリティ・インフラストラクチャ	第2-1-(1) 事業所の組織 第2-1-(2) 防災組織 第2-1-(3) 防犯組織 第2-1-(4) 監査組織
		(2) 第三者アクセスのセキュリティ	4.1.2.2 第三者アクセスのセキュリティ 4.1.2.3 アウトソーシング	第1-2-(1) 設備を設置する建築物 第1-2-(2) コンピュータ室、事務室 及びデータ保管室 第1-2-(3) 電源室及び空気調和室 第2-2-(1) 入退管理 第2-2-(2) 情報システムの運用管理 第2-2-(6) 外部委託
	3. 情報資産の分類及び管理	(1) 情報資産に対する責任	4.1.3.1 財産に対する責任	第2-2-(3) データ等保管管理
		(2) 情報の分類	4.1.3.2 情報の分類	第2-2-(3) データ等保管管理
	4. 人的セキュリティ	(1) 職務定義及び採用におけるセキュリティ	4.1.4.1 ジョブ定義及びリレーティングにおけるセキュリティ	第2-1-(1) 事業所の組織 第2-1-(2) 防災組織 第2-1-(3) 防犯組織 第2-1-(4) 監査組織
		(2) ユーザの教育・訓練	4.1.4.2 ユーザの訓練	第2-3-(1) 規程の教育の実施 第2-3-(2) 防災、防犯の訓練実施
		(3) セキュリティ事故及び誤動作への対処	4.1.4.3 セキュリティ事故及び誤動作への対応	第2-2-(2) 情報システムの運用管理 第2-2-(4) 電源設備、空調和設備 及び防災・防犯設備の管理 第2-2-(5) 監視

I S M S 認証基準(Ver.0.8)		BS7799	旧)安全対策認定基準	
章	項目	管理目的	BS7799監査ガイド(PD3004)	
4 詳細 管理 策	5. 物理的及び 環境的セキュリティ	(1) セキュリティ区画	4.1.5.1 安全領域	第1-2-(1) 設備を設置する建築物 第1-2-(2) コンピュータ室、事務室 及びデータ保管室 第1-2-(3) 電源室及び空気調和室 第2-2-(1) 入退管理 第2-2-(2) 情報システムの運用管理 第2-2-(3) データ等の保管管理 第2-2-(4) 電源設備、空気調和設備 及び防災・防犯設備の管理
		(2) 装置のセキュリティ	4.1.5.2 装置のセキュリティ	第1-1-(2) コンピュータ及び端末機 第1-1-(4) 電源設備 第1-1-(5) 空気調和設備 第1-2-(1) 設備を設置する建築物 第1-2-(2) コンピュータ室、事務室 及びデータ保管室 第1-2-(3) 電源室及び空気調和室 第2-2-(1) 入退管理 第2-2-(2) 情報システムの運用管理 第2-2-(4) 電源設備、空気調和設備 及び防災・防犯設備の管理
		(3) 一般管理策	4.1.5.3 一般管理策	第2-2-(3) データ等の保管管理
	6. 通信及び 運用管理	(1) 運用手順及び責任	4.1.6.1 運用手順及び責任	第2-1-(1) 事業所の組織体制 第2-2-(2) 情報システムの運用管理 第2-2-(3) データ等の保管管理 第2-2-(4) 電源設備、空気調和設備 及び防災・防犯設備の管理
		(2) システム計画の作成及び受け入れ	4.1.6.2 システム計画作成及び受け入れ	
		(3) 不正ソフトウェアからの保護	4.1.6.3 不正ソフトウェアからの保護	
		(4) 情報システムの管理	4.1.6.4 リスク・ヒューンク	第2-2-(2) 情報システムの運用管理 第2-2-(3) データ等の保管管理
(5) ネットワークの管理	4.1.6.5 ネットワークの管理			
(6) 媒体の取り扱い及びセキュリティ	4.1.6.6 媒体の取り扱い及びセキュリティ	第1-1-(3) データ等保管設備 第2-2-(2) 情報システムの運用管理 第2-2-(3) データ等の保管管理		
(7) 組織間における情報及びソフトウェアの交換	4.1.6.7 情報及びソフトウェアの交換	第2-2-(3) データ等の保管管理 第2-2-(6) 外部委託		

I S M S 認証基準(Ver.0.8)		BS7799	旧)安全対策認定基準	
章	項目	管理目的	BS7799監査ガイド(PD3004)	
4 情報管理	7. アクセス制御	(1) アクセス制御に関する事業の要求事項	4.1.7.1 システムアクセスに対するビジネス要求事項	第2-2-(2) 情報システムの運用管理 第2-2-(3) データ等の保管管理
		(2) ユーザアクセス管理	4.1.7.2 ユーザアクセス管理	第1-1-(1) 情報システムの機能 第2-2-(2) 情報システムの運用管理
		(3) ユーザの責任	4.1.7.3 ユーザ責任	第1-1-(1) 情報システムの機能 第2-2-(2) 情報システムの運用管理
		(4) ネットワークのアクセス制御	4.1.7.4 ネットワークのアクセス制御	
		(5) オペレーティングシステムのアクセス制御	4.1.7.5 オペレーティングシステムのアクセス制御	第1-1-(1) 情報システムの機能 第2-2-(2) 情報システムの運用管理
		(6) アプリケーションシステムのアクセス制御	4.1.7.6 アプリケーションのアクセス制御	第1-1-(1) 情報システムの機能 第2-2-(2) 情報システムの運用管理
		(7) システムアクセス及びシステム使用の監視	4.1.7.7 システムアクセス及びシステム使用の監視	第1-1-(2) コンピュータ及び端末機 第1-1-(4) 電源設備 第1-1-(5) 空気調和設備 第1-2-(1) 設備を設置する建築物 第1-2-(2) コンピュータ室、事務室及びデータ保管室 第2-2-(1) 入退管理 第2-2-(2) 情報システムの運用管理 第2-2-(3) データ等の保管管理 第2-2-(5) 監視
		(8) Eメールコンプライアンス及び遠隔地勤務	4.1.7.8 Eメールコンプライアンス及びテレワーク	
4 情報管理	8. システムの開発及びメンテナンス	(1) システムのセキュリティ要求事項	4.1.8.1 システムのセキュリティ要求事項	
		(2) アプリケーションシステムのセキュリティ	4.1.8.2 アプリケーションシステムのセキュリティ	
		(3) 暗号による管理策	4.1.8.3 暗号による管理策	
		(4) システムファイルのセキュリティ	4.1.8.4 システムファイルのセキュリティ	第2-2-(2) 情報システムの運用管理 第2-2-(3) データ等の保管管理
		(5) 開発及びホスティングにおけるセキュリティ	4.1.8.5 開発及びホスティングにおけるセキュリティ	第2-2-(2) 情報システムの運用管理 第2-2-(3) データ等の保管管理
9. 事業継続管理	(1) 事業継続管理	4.1.9.1 事業継続管理の種々の面	第2-3-(1) 安対の規程の教育実施 第2-3-(2) 防災、防犯の訓練の実施 第2-4-(1) 情報システム安全対策に係る監査	
10. 準拠	(1) 法的要求事項への準拠	4.1.10.1 法的要求事項への準拠	第2-4-(1) 情報システム安全対策に係る監査	
	(2) セキュリティポリシー遵守状況の確認	4.1.10.2 セキュリティポリシー及び技術準拠のレビュー	第2-4-(1) 情報システム安全対策に係る監査	
	(3) システム監査の考慮事項	4.1.10.3 システム監査の考慮事項		

**禁 無 断 転 載**

平成 13 年 9 月発行

発行者：財団法人 日本情報処理開発協会  
東京都港区芝公園 3-5-8 機械振興会館内 〒105-0011

TEL:03-3432-9386

FAX:03-3432-6200

E-mail:[info@isms.jpdec.or.jp](mailto:info@isms.jpdec.or.jp)