

ISMS ガイドライン(2001-1-26 版ドラフト)について

(財)日本情報処理開発協会

情報セキュリティ対策室

平成 13 年 1 月 26 日

本ドキュメントは、BS7799-2 を参考に作成したものである。

当初は情報システム安全対策実施事業所認定制度(安対制度)をある程度引き継いだ形で運用し、必要最小限のセキュリティマネジメント事項を附加したものとなる。本ガイドライン(案)はパイロット審査を通じてステップアップしていく予定である。

本ドキュメントでは、BS7799-2 の目次項目での日本に即した解釈としてのガイドライン(案)とともに、現時点での実現可能レベルを下記マークにより明示している。

	実現すべき事項
	JIS 規格の周知期間後に実現すべき事項
	全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
安	情報システム安全対策実施事業所認定基準に対する項目

また、本ガイドラインと関連する各ドキュメントとの関係は以下の通りである。

ISO 17799:2000	規格
BS7799-2:1999	要求事項(基準)
ISMS ガイドライン	実施ガイドライン

上記の ISO/IEC 17799:2000 は現時点では英語版を ISO 本部か(財)日本規格協会で購入できる(但し、対訳版は近々発売予定とのこと)。

参考 : BS7799-2:1999(仮訳) 目次

- | | |
|----------------------------|---------------------|
| 1. 適応範囲 | 4. 詳細管理策 |
| 2. 用語及び定義 | 4.1 セキュリティポリシー |
| 2.1 適応宣言書 | 4.2 セキュリティ組織 |
| 3. 情報セキュリティマネジメントシステムの要求事項 | 4.3 財産の分類及び管理 |
| 3.1 一般 | 4.4 スタッフのセキュリティ |
| 3.2 マネジメント枠組みの確立 | 4.5 物理的及び環境的セキュリティ |
| 3.3 実行 | 4.6 通信及び運用マネジメント |
| 3.4 ドキュメンテーション | 4.7 アクセス制御 |
| 3.5 文書管理 | 4.8 システムの開発及びメンテナンス |
| 3.6 記録 | 4.9 事業継続マネジメント |
| | 4.10 準拠 |

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目		ガイドライン(案)	安	備考
3 情報セキュリティマネジメントシステムの要求事項	3.1 一般	情報セキュリティマネジメントに関する組織を定め文書化すること。 保護すべき財産 組織の取組方法(リスクマネジメント) 管理目的及び管理策 要求される保証		
	3.2 マネジメント枠組みの確立	情報セキュリティマネジメントの目的及び管理方法を明確にし、文書化するために次の作業を行うこと。 セキュリティポリシー(狭義のポリシー)の策定 対象範囲(保護すべき情報資産・ルールの対象者等)の決定 リスクアセスメントの実施 リスク管理の検討 管理策(セキュリティスタンダード)の検討 管理策の適用宣言書の作成 以上の項目は、見直しの必要が発生する若しくは適切な間隔でレビューすること。		
	3.3 実行	実施手順の検討: セキュリティポリシー、規格への準拠 管理策実施手順の有効性(効果的実行)		
	3.4 ドキュメンテーション	情報セキュリティマネジメントシステム(ISMS)文書の構成:		
	3.5 文書管理	文書管理(作成・修正・廃止の手順及び責任の確立): 容易に識別可能な状態維持 定期的レビュー、必要に応じて更新 文書変更、改訂版の識別管理 廃止文書の撤去又は識別管理		

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- ： 実現すべき事項
- ： JIS規格の周知期間後に実現すべき事項
- ： 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安： 情報システム安全対策実施事業所認定基準に対する項目

項目		ガイドライン(案)	安	備考
	3.6 記録	情報セキュリティマネジメント文書に規定された管理に基づく記録の収集と管理： 記録の処理手順確立（識別、収集、見出し、ファイル、保管等） 実証記録例： 監査記録、ビジター記録、 ・セキュリティ事故・誤動作の障害記録 ・情報セキュリティ教育・訓練記録 ・オペレータ運転記録 ・セキュリティ関連イベント記録（監査ログ）・・・		
4 ・ 詳細 管理 策	4 ・ テ イ ・ ポ リ シ ー セ キ ユ リ	4.1.1 情報セキュリティポリシー		
		4.1.1.1 情報セキュリティポリシー文書	組織の情報セキュリティに関する方針が明確に示されること 経営者層等によって承認されていること 組織の全員に知らされていること	安
		4.1.1.2 レビューおよび評価	・定期的な見直しを実施すること ・情報セキュリティ環境が変化するとき必ず見直しのプロセスが組み込まれていること	
	4 ・ 2	4.2.1 情報セキュリティ・インフラストラクチャ		
		4.2.1.1 情報セキュリティフォーラム	情報セキュリティフォーラムを設置すること 経営陣の支持が得られる組織・体制 組織内のセキュリティ促進	
		4.2.1.2 情報セキュリティの調整	情報セキュリティに関する管理は、部門を代表する経営者間で役割を調整すること。 ・情報セキュリティの実施の漏れやむだな重複を避けるようにすること。	安
	4.2.1.3 情報セキュリティ責任の割当て	情報セキュリティの責任、セキュリティプロセス実施責任者を明確にすること 情報財産ごと所有者の責任者の任命 管理策実施者の責任の任命 役割、責任、免責事項、承認レベルの文書化		
	4.2.1.4 情報処理施設/設備の認可プロセス	新しい情報処理施設 / 設備の導入については、導入時の許可権限と手続きを明確にすること。		

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目		ガイドライン(案)	安	備考	
	4.2.1.5 専門家による情報セキュリティの助言	情報セキュリティ対策、緊急時対応へ助言を求めること ・社内アドバイザー ・外部専門家の助言のいずれかによる助言			
	4.2.1.6 組織間の協力	緊急時の対応に際し、他の機関と連絡および連携が取れるようにすること。 役所、情報サービス業者、通信事業者等 災害発生時に於いては設置されている対策機関	安		
	4.2.1.7 情報セキュリティの独立レビュー	情報セキュリティポリシーの実行状況をレビューすること(3.2の維持・改善) ・独立したレビュー組織によるレビュー ○内部監査(審査) ○外部監査			
	4.2.2 第三者のアクセス管理				
	4.2.2.1 第三者アクセスによるリスクの識別	第三者に許可する施設/設備へのアクセス管理すること アクセスのタイプ(物理的、論理的) 第三者の定義とアクセスリスク 各々の管理策	安		
	4.2.2.2 第三者との契約でのセキュリティ要求事項	第三者に許可する施設/設備へのアクセスについて契約等締結により管理すること。 ・セキュリティ要求事項	安		
	4.2.3 アウトソーシング				
	4.2.3.1 アウトソーシング契約におけるセキュリティ要求事項	外部委託をする場合は、委託先のセキュリティ管理策に関する項目を盛り込んだ契約を締結すること。			
4 . 3 財産 の	4.3.1 財産に対する責任				
	4.3.1.1 財産目録	重要な財産リストを作成すること 財産の区分 明確な識別 相対価値、重要度を把握できる内容			

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目		ガイドライン(案)	安	備考
分類 及び 管理	4.3.2 情報の分類			
	4.3.2.1 分類のガイドライン	情報の分類、保護管理策を設定すること 保護の必要性 重要度（保護の優先順位、保護の程度）		
	4.3.2.2 情報の分類および取扱い	情報の分類、取扱いについての手順を定めること		
4 . 4 ス タ ッ フ の セ キ ユ リ テ ィ	4.4.1 業務定義及びリソーシングにおけるセキュリティ			
	4.4.1.1 仕事の責任に情報セキュリティを含めること	セキュリティの役割及び責任は、業務に関する文書に記述すること		安
	4.4.1.2 人員採用審査及びポリシー	雇用者は採用条件に情報セキュリティに関する責任を明示すること。		
	4.4.1.3 機密保持合意書	採用時の署名（就業規則など会社の規定を遵守すること） ・定期的にセキュリティ教育を受講時し、最後に署名する		
	4.4.1.4 採用条件	採用時の条件を情報セキュリティ管理文書に明示する		
	4.4.2 ユーザの訓練			
	4.4.2.1 情報セキュリティ教育・訓練	継続性を重視した定期的な教育プログラム 情報セキュリティ上の役割変わる場合は重点的に教育を実施する（新入社員研修，新任部長研修等） 利用者への情報提供 障害復旧手順を確認するための訓練（バックアップテープのリストア等） 訓練の記録は，業務継続計画策定・見直しの作業に活用		安
4.4.3 セキュリティ事件及び誤動作への対応				

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目		ガイドライン(案)	安	備考
	4.4.3.1 セキュリティ事故の報告	セキュリティ事故は、直ちに責任者に報告すること 状況把握、応急処置、復旧手順の遂行 事故、欠陥に対する報告 類似事故防止のための情報の共有		
	4.4.3.2 セキュリティの欠陥報告	情報セキュリティの欠陥やその疑いを察知した場合の報告義務: 情報サービスのユーザへの報告義務の周知 原因の追究と情報収集 情報分析と速やかな対応		
	4.4.3.3 ソフトウェア誤動作の報告	ソフトウェアの誤動作の報告手順を定めること 報告手順に従う セキュリティ対策に関する情報は、直ちに管理者に報告		
	4.4.3.4 事故からの学習	事故から学習すること 事故、誤動作の識別への活用 ・事故・誤動作のタイプ、影響度合い、コストの定量化 類似事故防止のための情報の共有		
	4.4.3.5 懲戒プロセス	情報セキュリティの規定違反に対する処罰: ・正式な懲戒プロセスで処罰されること		
4	4.5.1 安全領域			
5	4.5.1.1 物理的セキュリティの境界線	敷地境界、事業所、重要室はセキュリティ区画とすること。 o セキュリティ区画とは、 ・容易に破壊されないこと。 ・容易に侵入されないこと。 ・他の区画からの延焼、浸水の影響を最小限にすること。 ・顧客情報の通過、滞留するエリア		
	4.5.1.2 物理的出入り管理策	セキュリティ区画は入退管理を行うこと。 ・セキュリティ区画には管理レベルを設定し、許可者以外が出入りできないようにすること。	安	

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目		ガイドライン(案)	安	備考
セ キ ユ リ テ ィ	4.5.1.3 オフィス、ルーム及び設備のセキュリティ	事業所内の各室にセキュリティ区画を定めること。 ・セキュリティ区画は明確な用途表示を避けること。	安	
	4.5.1.4 安全領域での作業	セキュリティ区画での作業は事前に届け出、責任者の許可を得ること 作業に必要なもの以外の持込を禁止する	安	
	4.5.1.5 受け渡しエリアの隔離	セキュリティ区画から隔離された物品の受け渡しエリアを設定し管理すること		
	4.5.2 装置のセキュリティ			
	4.5.2.1 装置の取付け位置及び保護	装置は環境上の脅威及び危険を軽減する場所に設けること 窃盗 / 火災 / 爆発 / 浸水 / 漏水 / 煙 / ほこり / 振動 / 小動物 / 化学物質 / 電源供給妨害 / 帯電 / 電磁放射線	安	
	4.5.2.2 電源	情報システムへの電力の要求条件を満たすこと 電源の安定化 電源の供給継続 避雷措置 関連法令の遵守	安	
	4.5.2.3 ケーブル配線のセキュリティ	通信ケーブルおよび電源ケーブルは電磁波が漏れない措置を講ずること。 通信ケーブルおよび電源ケーブルは保護措置を行うこと。	安	
	4.5.2.4 装置のメンテナンス	装置のメンテナンスは製造業者の説明書または手順書に従うこと 装置の説明書、手順書を管理する 点検結果、修理内容は記録する	安	
	4.5.2.5 敷地外における装置のセキュリティ	情報処理のため事業所外で使用する機器（データを含む）のセキュリティ対策を講ずること。セキュリティレベルは事業所内と同等とする		
	4.5.2.6 装置の安全な処分及び再利用	機器及びソフトウェアの廃棄、再利用、返却、譲渡を行う場合、情報の漏洩防止策をとること ・機器の廃棄、再利用時は、内部情報を抹消する		
4.5.3 一般管理策				

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目		ガイドライン(案)	安	備考
	4.5.3.1 クリアデスク及びクリアスクリーンポリシー	情報の放置を禁止すること ・離席時の注意 ・帰宅時の注意		
	4.5.3.2 財産の移動	装置、情報又はソフトウェアは、認可なしに移動しないこと ・資産管理簿の作成及び管理		
4 ・ 6 通 信 及 び 運 用 マ ネ ジ メ ン ト	4.6.1 運用手順及び責任			
	4.6.1.1 操作手順書	操作手順書を作成し、維持管理すること ・操作方法、障害発生時の対処等マニュアルの常備	安	
	4.6.1.2 運用変更管理	情報処理施設 / 設備及びシステムの変更は管理すること 重要な変更の識別及び記録 変更の潜在影響の評価 提案される変更の公式な承認手順 変更の詳細について、全関係者への通知 変更の中止及び変更からの回復に対する責任を明確にする手順。		
	4.6.1.3 事故管理手順	事故管理の責任を明確にし、事故時の管理手順を確立すること。		
	4.6.1.4 職務の分離	職務の許可権限を明確にすること	安	
	4.6.1.5 開発及び運用施設/設備の分離	情報処理サービスを提供する施設 / 設備と開発用施設 / 設備は分離すること		
	4.6.1.6 外部装置のマネジメント	事業所に立ち入る請負業者とはセキュリティ対策に関する契約を締結すること		
	4.6.2 システムの計画作成及び受け入れ			
	4.6.2.1 容量計画の作成	システムの処理能力、記憶容量について負荷を監視し、将来の需要容量を予測すること		

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目	ガイドライン(案)	安	備考
4.6.2.2 システムの受け入れ	新しいシステム、アップグレードおよび新バージョンの受け入れ基準を設け、導入前に試験を行うこと。		
4.6.3 悪質ソフトウェアからの保護			
4.6.3.1 悪質ソフトウェアに対する管理策	悪質ソフトウェア(コンピュータウイルス等)から保護すること 検出・防止管理策の決定 ユーザに対する周知徹底		
4.6.4 ハウスキーピング			
4.6.4.1 情報のバックアップ	重要データは分散保管等損壊防止措置を講ずること ・安全な方法で、安全な場所への保管		
4.6.4.2 オペレータ日誌	情報システムの運転記録を作成すること	安	
4.6.4.3 障害記録	障害は報告し、是正処置をとること 是正の結果は記録すること	安	
4.6.5 ネットワークマネジメント			
4.6.5.1 ネットワーク管理策	ネットワークによる利用者の不正アクセスを防止する措置を講ずること ・漏洩防止の仕組み ・機密保持機能		
4.6.6 媒体の取扱い及びセキュリティ			
4.6.6.1 取外し可能なコンピュータ媒体のマネジメント	移動可能な媒体の管理措置を講ずること ・受渡しは定めた方法で行う ・安全な定めた場所への保管管理(管理記録の整備)	安	
4.6.6.2 媒体の処分	媒体の処分については判読不可能、再現不可能とすること ・完全な消去 ・物理的な破壊		

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目		ガイドライン(案)	安	備考
	4.6.6.3 情報の取扱い手順	データの取り扱い、保管に関する手順を定めること	安	
	4.6.6.4 システムドキュメンテーションのセキュリティ	システムドキュメントへのアクセス者を定め、保護すること。		
	4.6.7 情報及びソフトウェアの交換			
	4.6.7.1 情報及びソフトウェアの交換合意事項	情報及び媒体等の交換にあたっては、必要な事項を定めた合意事項に基づき行うこと。		
	4.6.7.2 輸送中の媒体のセキュリティ	媒体の運送の際、運送業者の選定、梱包、取り扱いについて等媒体への改ざん等がないよう配慮すること。		
	4.6.7.3 電子取引のセキュリティ	電子取引は、詐欺活動、契約紛争、情報の開示・改ざんから保護すること		
	4.6.7.4 電子メールのセキュリティ	電子メールによるセキュリティ上のリスクを軽減する管理策を実行すること 重要な情報の送信する場合： ・相手先を限定し、宛先の十分な確認		
	4.6.7.5 電子オフィス・システムのセキュリティ	電子オフィスシステムに関する方針、規範を制定し、電子オフィスによるリスクを回避すること		
	4.6.7.6 公衆が利用できるシステム	一般公衆に提供するサービスは公衆が提供以外の行為ができないようにすること。		
	4.6.7.7 情報交換の他の形式	音声、ファクシミリ、ビデオ通信設備での情報を保護する管理策を実行すること 相手先を限定し、宛先の十分な確認		
4	4.7.1 アクセス制御に関するビジネス要求事項			
7	4.7.1.1 アクセス制御ポリシー	アクセス制御について方針、規範を設けること		
ア ク セ ス	4.7.2 ユーザアクセスのマネジメント			

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目		ガイドライン(案)	安	備考	
ス 制 御	4.7.2.1 ユーザ登録	情報システムの利用にかかる資格登録、変更、抹消手順を設けること ・必要最小限のアクセス権限を付与する ・不要になった或いは長期間未使用の登録削除の手続き	安		
	4.7.2.2 特権管理	特別な権限は少なくし、一般ユーザとは別に管理すること。 特権の利用は必要最小限とする 特権の利用は：コンピュータ、場所、期間を限定する	安		
	4.7.2.3 ユーザパスワードのマネジメント	パスワード履歴の管理（過去に使用したパスワードの禁止） パスワード再発行手続きの管理（通常の手続き，緊急時の手続き，本人確認）	安		
	4.7.2.4 ユーザのアクセス権のレビュー	ユーザのアクセス状況を定期的に確認すること ・特権の割当てを定期的にチェックする			
	4.7.3 ユーザの責任				
	4.7.3.1 パスワードの利用	ユーザはパスワードを適切に管理すること 定期的更新の義務付け 他人に見られない パスワードは個人管理 パスワードの構成			
	4.7.3.2 無人装置	無人運転をする場合は、自動制御装置および遠隔監視設備を設置すること。	安		
	4.7.4 ネットワークのアクセス制御				
	4.7.4.1 ネットワークサービスの使用についてのポリシー	ユーザへのアクセスの許可は提供するサービスのみに行うこと			
	4.7.4.2 強制経路	利用者のアクセス経路は与えられた権限の範囲内とすること			

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目	ガイドライン(案)	安	備考
4.7.4.3 外部接続のためのユーザ真正確認	外部から接続する使用者には真正性の確認を行うこと ・外部からシステム管理を行う場合: 認証機能 暗号機能 アクセス制御機能を設定する		
4.7.4.4 ノードの真正確認	遠隔コンピュータシステムへの接続は、真正確認を行うこと		
4.7.4.5 遠隔診断ポートの保護	診断ポートへのアクセスは、確実に制御されること		
4.7.4.6 ネットワークにおける分離	情報システムの利用形態に応じて、ネットワークを分離すること		
4.7.4.7 ネットワークの接続制御	共通ネットワークにおけるユーザの接続能力は、「アクセス制御ポリシー」に従って、制限されるものであること		
4.7.4.8 ネットワーク経路指定制御	共通ネットワークには、経路指定管理策を備えること		
4.7.4.9 ネットワークサービスのセキュリティ	組織によって使用されるネットワークサービスのセキュリティ属性について、明確な説明を確実に受けておくこと		
4.7.5 オペレーティングシステムのアクセス制御			
4.7.5.1 自動端末識別	情報システムへのアクセスの際、接続端末の真正性の確認をすること	安	
4.7.5.2 端末のログオン手順	情報サービスへのアクセスは、安全なログオンプロセスを用いること	安	
4.7.5.3 ユーザの身元確認及び真正確認	利用者IDによる管理を行うこと	安	
4.7.5.4 パスワードマネジメントシステム	パスワードの確認は対話式機能を有すること		
4.7.5.5 システムユーティリティの利用	システムユーティリティプログラムの使用は制限され、厳しく管理されること		

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目	ガイドライン(案)	安	備考
4.7.5.6 ユーザを安全防護するための脅迫警告	脅迫の標的となり得るユーザのために、脅迫警報を備えること		
4.7.5.7 端末のタイムアウト	一定時間作業が行われない場合は、接続を切断すること		
4.7.5.8 接続時間の制限	接続時間は制限すること		
4.7.6 アプリケーションのアクセス制限			
4.7.6.1 情報アクセスの制限	情報及びアプリケーションシステムの機能へのアクセスは、「アクセス制御ポリシー」に従って、制限されること	安	
4.7.6.2 慎重な取扱いを要するシステムの隔離	取扱いに慎重を要するシステムは、専用のコンピューティング環境とすること		
4.7.7 システムアクセス及びシステム使用の監視			
4.7.7.1 イベントの記録	セキュリティ関連イベントは記録し、管理すること イベントの動作履歴、使用記録 記録の随時分析 記録の処理手順に従った管理		
4.7.7.2 システム使用の監視	情報処理施設 / 設備の使用を監視する手順を確立し、監視すること 監視活動の結果はレビューする		
4.7.7.3 クロックの同期	コンピュータクロックは、記録を正確に行うために、同期化すること		
4.7.8 モバイルコンピューティング及びテレワーキング			
4.7.8.1 モバイルコンピューティング	モバイルコンピュータ利用は、方針、規範を制定し、管理すること		
4.7.8.2 テレワーキング	テレワーキングについて、方針、規範を制定管理すること		

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目		ガイドライン(案)	安	備考
4 . 8 シ ス テ ム の 開 発 及 び メン テナ ンス	4.8.1 システムのセキュリティ要求事項			
	4.8.1.1 セキュリティ要求事項の分析及び明示	新しいシステム、既存のシステムの改善に関するセキュリティ要求事項を分析し、これを満たすための管理策を明確にすること		
	4.8.2 アプリケーションシステムのセキュリティ			
	4.8.2.1 入力データの妥当性確認	入力されるデータは、入力チェックなどでその妥当性を確認すること		
	4.8.2.2 内部処理の管理	処理されたデータの改ざんを検出するために、システムに妥当性確認を組み込むこと		
	4.8.2.3 メッセージの真正確認	メッセージの真正確認のため、アプリケーションを用いること		
	4.8.2.4 出力データの妥当性確認	アプリケーションシステムから出力されるデータは、妥当性確認をすること		
	4.8.3 暗号による管理策			
	4.8.3.1 暗号による管理策の使用についてのポリシー	重要な情報は、パスワード、暗号化等対策を図ること		
	4.8.3.2 暗号化	重要な情報は、パスワード、暗号化等対策を図ること		
	4.8.3.3 デジタル署名	電子情報の真正性・完全性を保護する措置をとること。		
	4.8.3.4 非拒否サービス	電子情報の真正性・完全性を保護する措置をとること。		
	4.8.3.5 キー管理	暗号手法の使用を支持するために、一連の合意された規格、手順及び方法に基づくキー管理システムを用いること		
	4.8.4 システムファイルのセキュリティ			

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目		ガイドライン(案)	安	備考
	4.8.4.1 運用ソフトウェアの管理	運用システムでは使用するソフトウェアの管理策を定めること。		
	4.8.4.2 システム試験データの保護	試験データは保護され、管理されること		
	4.8.4.3 プログラムソースライブラリへのアクセス制御	プログラムソースライブラリへのアクセス管理策を定めること		
	4.8.5 開発及びサポートプロセスのセキュリティ			
	4.8.5.1 変更管理手順	情報システムの変更管理手順を定めること		
	4.8.5.2 オペレーティングシステムの変更の技術的レビュー	アプリケーションシステムを変更する場合の手順・試験等について定める。		
	4.8.5.3 ソフトウェアパッケージ変更に対する制限	ソフトウェアパッケージの変更は行わないこと。		
	4.8.5.4 コバート通信路及びトロイのコード	ソフトウェアの購入・使用・変更の管理策を定めること。		
	4.8.5.5 アウトソーシングによるソフトウェア開発	アウトソーシングによるソフト開発にあたっては管理策を定めること。		
	4.9.1 事業継続マネジメントの側面			
4 . 9 事業 継続 マ	4.9.1.1 事業継続マネジメントプロセス	組織全体に渡る事業継続を開発、維持するための、管理されたプロセスを整備すること		
	4.9.1.2 事業継続及び影響分析	事業継続への全般的取り組みのために、適切なリスクアセスメントに基づく戦略計画を立てること		
	4.9.1.3 継続計画を立て、実行する	重要な事業プロセスの障害又は故障の後、事業運営を維持し、若しくは、遅れることなく回復させるために、計画を立てること		

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目		ガイドライン(案)	安	備考
イ ジ メ ン ト	4.9.1.4 事業継続計画作成のための 枠組み	すべての計画が整合したものになることを確実にするため、また、試験及びメンテナ ンスの優先順位を明確にするために、事業継続計画の1つの枠組みを維持すること		
	4.9.1.5 事業継続計画の試験、維 持、再利用	事業継続計画は、最新で効果的なものであることを確実にするために、定期的に試験 し、定期的なレビューによって維持すること		
	4.10.1 法的要求事項への準拠			
4 . 1 0 準 拠	4.10.1.1 適用法規の識別	すべての関連法令、規制及び契約上の要求事項は、各情報システムについて、明確に定 め、文書化することとともにマネジメントシステムに反映させること		
	4.10.1.2 知的所有権	知的所有権に関わる物件の使用、並びに所有権のあるソフトウェア製品の使用につい て、法的制限事項に確実に準拠するように、適切な手順を実行すること		
	4.10.1.3 組織の記録の安全防護	組織の重要な記録は、紛失/消失、破壊及び改ざんから保護すること		
	4.10.1.4 データの保護及び個人情 報のプライバシーの保護	関連法規に従って個人情報を保護するために、管理策を適用すること		
	4.10.1.5 情報処理施設/設備の誤用 の防止	情報処理施設/設備の使用は経営陣が認可し、そのような施設/設備の誤用を防止す るために、管理策を適用すること		
	4.10.1.6 暗号による管理策の規制	暗号による管理策へのアクセス又はその使用を管理するために、国家が定める合意 書、法律、規制その他の法律文書への準拠を確実にする管理策が整っていること		
	4.10.1.7 証拠の収集	人又は組織を相手取っての訴訟が法律に関わるものである場合、提示される証拠は、 関連法規に定められる証拠に関する規則に準拠するものであること		
4.10.2 セキュリティポリシー及び 準拠のレビュー				

ISMSガイドライン(案)

(財)日本情報処理開発協会
 情報セキュリティ対策室
 2001年1月26日

- : 実現すべき事項
- : JIS規格の周知期間後に実現すべき事項
- : 全社的に実施することは難しいが、個別の業務対応などで実現すべき事項
- 安: 情報システム安全対策実施事業所認定基準に対する項目

項目		ガイドライン(案)	安	備考
	4.10.2.1 セキュリティポリシーへの準拠	管理責任者は担当部分のセキュリティ対策についてポリシーに準拠しているかどうか定期的に確認すること		
	4.10.2.2 技術的な準拠のチェック	情報システムは、セキュリティ実行規格に準拠していることを定期的に確認すること		
	4.10.3 システム監査の考慮事項			
	4.10.3.1 システム監査管理策	情報セキュリティマネジメントシステム監査は業務に支障がないよう計画し、被監査部門の合意の上実施すること	安	
	4.10.3.2 システム監査ツールの保護	情報セキュリティマネジメントシステム監査ツールは許可された者以外がアクセスできないよう管理すること		