H13－セキュリティWG－2

情報セキュリティ対策マネジメント標準
(JIS X 5080:ISO/IEC 17799)の解説

平成１４年３月

電子商取引推進協議会
セキュリティWG

はじめに

EC サイトにおける脅威は、外部の第三者からの脅威だけでなく、EC サイト取引業者や EC サイト利用者による不正行為、EC サイト内部の第三者による犯行によっても引き起こされる。その他にも、サイト運営者による運用上のミスや故意の犯行、火災,水害等の災害といった脅威も存在する。

EC サイトが安全で信頼できるサービスを提供するためには、単にファイアウォールやウイルス対策ソフトウェアを導入するといったことだけではなく、このような諸々の脅威に備える必要がある。そのためには、EC サイトの構築と運営面において、セキュリティの確保に向けたマネジメントを組織的に体系立てて行うことが必要である。この取組みを情報セキュリティマネジメントシステム（ISMS）と呼ぶ。

ECOM では、この ISMS についての理解を深めることが大切であると考え、その手段として、JIS X 5080(ISO/IEC 17799)を題材としてその内容解釈の検討と再整理を行い、結果を報告書としてまとめた。

本報告書が、EC サイトの安全と信頼を守ることへの理解につながり、読者の皆様が携わる事業活動への一助となれば幸いである。

目次

第1部

JIS X 5080 (ISO/IEC 17799) の概要

1　JIS X 5080(ISO/IEC 17799)の概要

1.1　JIS X 5080(ISO/IEC 17799)の概要

JIS X 5080 は 2002 年 2 月に、国際標準となった ISO/IEC 17799 に準じて制定された情報セキュリティマネジメントについての国内規格である。

ISO/IEC 17799 は、英国規格協会が策定した情報セキュリティマネジメントに関する規格として BS7799 の一部が国際標準化されたものである。

BS7799 は、1995 年に IT セキュリティ管理対策として一般業界向けに策定され、欧州を中心に広く活用されているものである。最初に制定されたものは情報セキュリティマネジメントの実践規範と呼ばれ、パート1とも呼ばれているものである。1998 年には、情報セキュリティマネジメントシステムの仕様としてパート 2 が規定された。その後、1999 年 5 月にはパート 1 およびパート 2 について改訂が行われ、ネットワークや通信に関する対策について拡充された。

そして BS7799 パート 1 について 2000 年 9 月に ISO 標準化が行われ、ISO/IEC 17799 として制定された。

1.2　BS7799 の構成

ここで、JIS X 5080 の下となった BS7799 について概説する。この BS7799 は、2つのパートから構成されている。

パート 1：情報セキュリティマネジメントの実践規範

(Code of practice for information security management)

組織が情報セキュリティマネジメントを実施する際のガイドラインを提供するものであり、ベストプラクティスとしての管理項目が 127 項目にわたって記載されている。

パート 2：情報セキュティマネジメントシステムの仕様

(Specification for information security management systems)

パート 1 にもとづき、情報セキュリティマネジメントシステムを構築するための要求事項が記載されている。この要求事項は、パート 1 で示されている管理項目と一致しており、パート 1 が経験から得られたノウハウをベストプラクティスとして記述しているのに対して、パート 2 ではマネジメントの仕組みをシステム構築の面から体系的に整理したものとなっている。

1.3　情報セキュリティの定義と適用範囲

(1) 情報セキュリティの定義

本規格では、情報セキュリティとは情報システムの機密性、完全性、可用性を維持することと定義する。

(2) 適用範囲

本規格はあらゆる情報資産をその対象とし、電子化された情報だけでなく、紙媒体、音声、電話等の情報を扱うすべての媒体をその対象とする。

1.4　JIS X 5080 で示されるセキュリティ対策

JIS X 5080 で示されているセキュリティ対策は、経験上有効と考えられるセキュリティ対策項目の列挙であり、セキュリティ対策を行う上でのガイドラインとして活用できるものである。

1.5　本基準の狙い

情報セキュリティに責任を持つ者に求められる情報セキュリティの管理実施方法を確立するためのガイドを与え、情報システムのセキュリティの向上に寄与する。

1.6　用語および定義

本規格では、重要用語について以下のように定義している。

(1) セキュリティ要件に関する用語

- 機密性…情報にアクセスすることが認可されたものだけがアクセスできることの保障
- 完全性…情報および処理方法の正確さおよび完全である状態を安全に防護すること
- 可用性…認可されたユーザが、必要な時に情報および関連財産にアクセスできることを保証すること

(2) リスクアセスメント

情報および情報処理施設や設備に対する脅威、それらへの影響およびそれらの脆弱性ならびにそれらが起こる可能性の評価

(3) リスクマネジメント

許容コストにより、情報システムに影響を及ぼす可能性のあるセキュリティリスクを明確にし、制御し、最小限に抑制するか、または除去するプロセス

2　ISO/IEC 17799 および JIS X 5080 の概要

2.1　本規格におけるセキュリティ要求事項の体系

本規格におけるセキュリティ対策としての要求事項の体系を、図 2-1に示す。

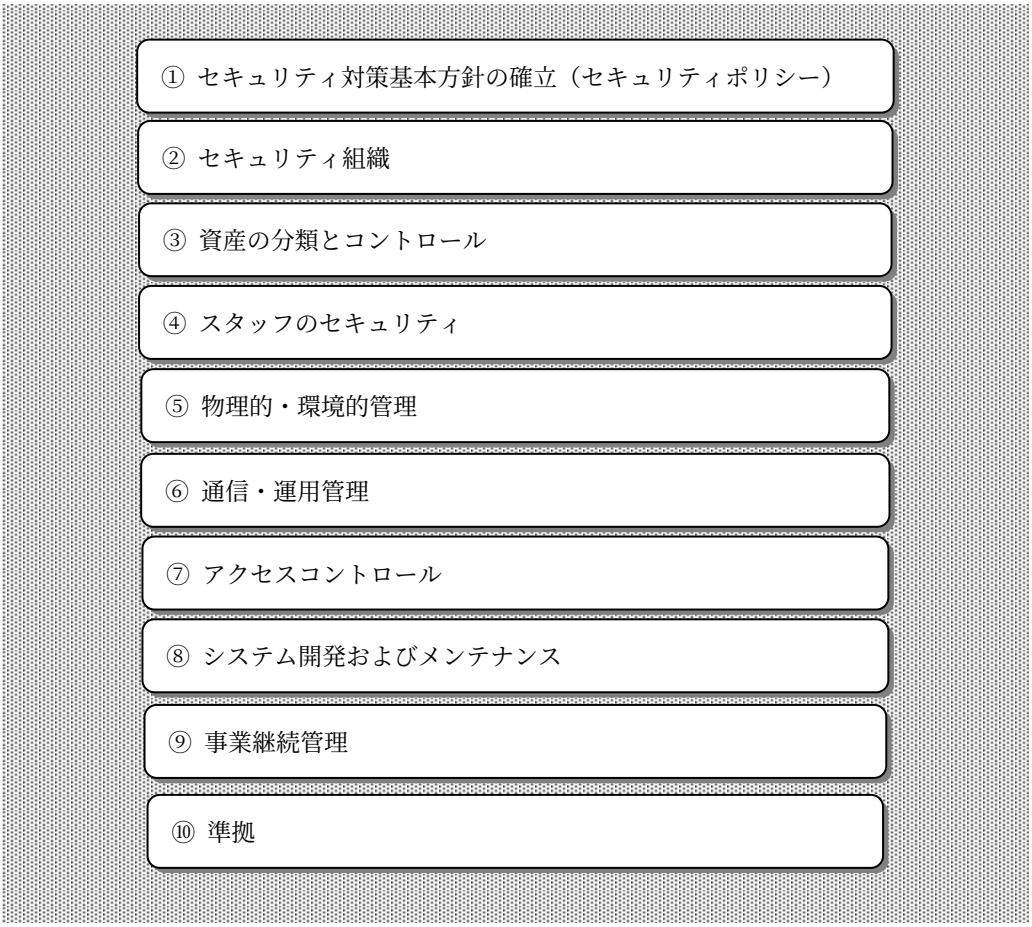

図 2-1　ISO/IEC 17799におけるセキュリティ要求事項の体系

2.2　セキュリティ要求事項の一覧

表 2-1に、本規格が情報セキュリティの確保のために要求している事項の一覧を示す。

表 2-1 JIS X 5080 (ISO/IEC 17799)における要求事項と本ガイドラインにおける要求事項の対応(1/6)

要求事項(コントロール)区分		要求事項	要求事項の概要	ISO/IEC 17799 における要求事項のタイトル
3. セキュリティ基本方針 Security Policy	3.1 情報セキュリティ基本方針 Information Security Policy	3.1.1 情報セキュリティ基本方針文書	組織のセキュリティポリシーの作成とその位置付けの確立	Information security policy document
		3.1.2 見直しおよび評価	組織のセキュリティポリシーの妥当性の継続的な維持のための定期的な見直しや必要に応じた改定の実施	Review and evaluation
4. 組織のセキュリティ Organizational Security	4.1 情報セキュリティ基盤 Information security Infrastructure	4.1.1 情報セキュリティ運営委員会	組織におけるセキュリティマネジメントの展開に関する経営陣の参加の確保	Management information security forum
		4.1.2 情報セキュリティの調整	セキュリティの確保にかかる諸施策の実施にかかわるチーム間での連携体制の確立	Information security co-ordination
		4.1.3 情報セキュリティ責任の割当て	セキュリティの確保にかかる関係者間での責任体制の確立	Allocation of information security responsibilities
		4.1.4 情報処理設備の認可手続	情報処理設備や関連施設の導入や新設についての適切な管理の実施	Authorization process for information processing facilities
		4.1.5 専門家による情報セキュリティの助言	セキュリティの専門家の活用による組織のセキュリティ強化の推進	Specialist information security advice
		4.1.6 組織間の協力	必要に応じた社内外の組織との連携	Co-operation between organizations
		4.1.7 情報セキュリティの他者によるレビュー	組織におけるセキュリティマネジメント全体についての監査の実施	Independent review of information security
	4.2 第三者によるアクセスのセキュリティ Security of Third Party Access	4.2.1 第三者のアクセスから生じるリスクの識別	外部の者をシステムの運用にかかわらせることについてのリスクの把握と適切な管理の実施	Identification of risks from third party access
		4.2.2 第三者との契約書に記載するセキュリティ要求事項	セキュリティポリシーの遵守が義務付けられる外部要員の把握と、契約書等によるこれらの外部要員に対するセキュリティ要求事項の明示	Security requirements in third party contracts
	4.3 外部委託 Outsourcing	4.3.1 外部委託契約におけるセキュリティ要求事項	情報処理にかかわる業務を外部に委託する場合における、委託契約等による委託先に対するセキュリティ要求事項の明示	Security requirements in outsourcing contracts
5. 資産の分類および管理 Asset Classification and Control	5.1 資産に対する責任 Accountability for Assets	5.1.1 資産目録	装置やソフトウェアや情報等、保護の対象となるシステム資産の把握	Inventory of assets
	5.2 情報の分類 Information Classification	5.2.1 分類の指針	保護対象資産に対する組織での整合性のある保護の実現のための、保護ガイドラインの確立	Classification guidelines
		5.2.2 情報のラベル付けおよび取扱い	個々の保護対象資産に対するガイドラインに沿った適切な保護要件の設定	Information labelling and handling
6. 人的セキュリティ Personal Security	6.1 職務定義および雇用におけるセキュリティ Security in Job Definition and Resourcing	6.1.1 セキュリティを職責に含めること	システム運用にかかわる従業員や外部要員に対する組織のセキュリティに関する役割および責任の明示	Including security in Job responsibilities
		6.1.2 要員審査およびその個別方針	組織のセキュリティを脅かすような不適正な人物の採用を防止するための施策の実施	Personnel screening and policy
		6.1.3 機密保持契約	就業規則または契約等での、従業員に対する機密の保持や非公開の義務付け	Confidentiality agreements
		6.1.4 雇用条件	従業員の採用にあたっての採用条件における組織のセキュリティポリシーの準拠義務の明示	Terms and conditions of employment
	6.2 利用者の訓練 User Training	6.2.1 情報セキュリティ教育および訓練	組織のすべての従業員や業務やシステムの運用にかかわる外部要員に対するセキュリティポリシーとセキュリティプロセスの教育の実施	Information security education and training
	6.3 セキュリティ事件・事故および誤動作への対処 Responding to Security Incidents and Malfunctions	6.3.1 セキュリティ事件・事故の報告	セキュリティ事故が発生した場合における、報告についてのルールの確立と、ルールに従った報告の実施	Reporting security incidents
		6.3.2 セキュリティの弱点の報告	セキュリティの欠陥またはセキュリティに対する脅威が検知された場合における、報告についてのルールの確立と、ルールに従った報告の実施	Reporting security weaknesses
		6.3.3 ソフトウェアの誤動作の報告	ソフトウェアの誤動作が発生した場合における、報告についてのルールの確立と、ルールに従った報告の実施	Reporting software malfunctions
		6.3.4 事件・事故からの学習	発生したセキュリティにかかる事故についての分析の実施による、教訓の抽出とセキュリティ対策へのフィードバックの実施	Learning from incidents
		6.3.5 懲戒手続	組織のセキュリティ要求事項違反に対する適切な懲戒の実施	Disciplinary process

(注)本表中の 要求事項区分ならびに要求事項の先頭にある n.、 n.m、 n.m.は、JIS X 5080(ISO/IEC 17799)における該当の章および節番号を示している。

表 4-1　JIS X 5080 (ISO/IEC 17799)における要求事項と本ガイドラインにおける要求事項の対応(2/6)

要求事項(コントロール)区分		要求事項	要求事項の概要	ISO/IEC 17799 における要求事項のタイトル
7. 物理的および環境的セキュリティ Physical and Environmental Security	7.1 セキュリティが保たれた領域 Secure Areas	7.1.1 物理的セキュリティ境界	情報処理設備や関連施設やオフィス等の保護領域に対する適切な物理的なバリアの設置	Physical security perimeter
		7.1.2 物理的入退管理策	保護領域に対する適切な立入りの制限と手続き等の管理ルールの確立	Physical entry controls
		7.1.3 オフィス、部屋および施設のセキュリティ	保護領域に対する適切な立入りについてのルールに基づく制限と管理の実施	Securing offices, rooms and facilities
		7.1.4 セキュリティが保たれた領域での作業	保護領域内での従業員や外部要員の活動についての適切な制限と管理の実施	Working in secure areas
		7.1.5 受渡し場所の隔離	必要な場合における受渡しエリアの設置による、外部と保護領域間での直接的な交流の抑止	Isolated delivery and loading areas
	7.2 装置のセキュリティ Equipment Security	7.2.1 装置の設置および保護	情報処理装置の設置にかかる安全の確保のための、設置場所の適切な選択と、適切な保護策の実施	Equipment siting and protection
		7.2.2 電源	電源装置に対する適切な保護策の実施 (停電およびその他の電気的な異常からの保護)	Power supplies
		7.2.3 ケーブル配線のセキュリティ	ケーブル配線に対する適切な保護策の実施 (損傷や傍受からの保護)	Cabling security
		7.2.4 装置の保守	装置のメンテナンスの適切な実施	Equipment maintenance
		7.2.5 事業敷地外における装置のセキュリティ	組織の敷地外に設置された装置に対する適切な保護策の実施	Security of equipment off-premises
		7.2.6 装置の安全な処分または再使用	装置の処分や再使用時の情報の消去についてのルールの確立とその実行についての管理の実施	Secure disposal or re-use of equipment
	7.3 その他の管理策 General Controls	7.3.1 クリアデスクおよびクリアスクリーンの個別方針	デスクおよびスクリーン上の情報等からセキュリティが脅かされないようにするためのオフィスにおける行動規範の確立とその実行	Clear desk and clear screen policy
		7.3.2 資産の移動	装置やソフトウェアや情報等の保護資産の外部への持出しに対する適切な制限と管理の実施	Removal of property
8. 通信および運用管理 Communications and Operations Managements	8.1 運用手順および責任 Operational Procedures and Responsibilities	8.1.1 操作手順書	ベンダーの指示に従った適切なシステム運用手順書の整備	Documented operating procedures
		8.1.2 運用変更管理	情報処理設備や関連施設やシステムの変更についての十分な管理の実施	Operational change control
		8.1.3 事件･事故管理手順	セキュリティ事故発生時の対処要領の確立	Incident management procedures
		8.1.4 職務の分離	スタッフの職務や権限の分離等のスタッフの不正に対する防止策の実施	Segregation of duties
		8.1.5 開発施設および運用施設の分離	開発およびテスト用の施設や設備と実運用に用いる施設や設備の分離	Separation of development and operational facilities
		8.1.6 外部委託による施設管理	システムの運用に他社の施設を使用する場合における、施設提供側に対するセキュリティ要求事項の明示	External facilities management
	8.2 システム計画の作成および受入れ System Planning and Acceptance	8.2.1 容量･能力の計画作成	適切なキャパシティマネジメントの実施による、システムのキャパシティにかかるトラブルの予防	Capacity planning
		8.2.2 システムの受入れ	新しい情報システムの導入やシステムのアップグレード等におけるソフトウェアの受入れについてのルールの確立とその実行	System acceptance
	8.3 悪意のあるソフトウェアからの保護　Protection against Malicious Software	8.3.1 悪意のあるソフトウェアに対する管理策	ソフトウェアの導入についての制限や使用中のソフトウェアに対する定期的なチェックの実施等、の有害プログラムに対する適切な対策の実施	Controls against malicious software
	8.4 システムの維持管理 Housekeeping	8.4.1 情報のバックアップ	システムに発生したトラブルからのシステムの復旧に必要な情報やソフトウェアのバックアップの確保	Information back-up
		8.4.2 運用の記録	日々のシステム運用におけるオペレーションの記録の作成とその保管の実施	Operator logs
		8.4.3 障害記録	システムに発生したトラブルと実施した処置についての報告の実施と、その記録の作成と保管の実施	Fault logging

(注) 本表中の　要求事項区分ならびに要求事項の先頭にある　n.、　n.m、　n.m. は、JIS　X　5080 (ISO/IEC 17799) における該当の章および節番号を示している。

表 4-1　JIS X 5080 (ISO/IEC 17799)における要求事項と本ガイドラインにおける要求事項の対応(3/6)

要求事項(コントロール)区分		要求事項	要求事項の概要	ISO/IEC 17799 における要求事項のタイトル
8. 通信および運用管理 Communications and Operations Management	8.5 ネットワークの管理 Network Management	8.5.1 ネットワーク管理策	ネットワークの使用に対する適切なセキュリティ対策の確立	Network controls
	8.6 媒体の取扱いおよびセキュリティ Media handling and Security	8.6.1 コンピュータの取外し可能な附属媒体の管理	取外し可能なコンピュータ媒体や印刷物の取扱いについてのルールの確立とその実行	Management of removable computer media
		8.6.2 媒体の処分	媒体の処分についてのルールの確立とその実行	Disposal of media
		8.6.3 情報の取扱い手順	保護対象のシステム資産の個々に対する保護要件と取扱いルールの確立	Information handling procedures
		8.6.4 システムに関する文書のセキュリティ	システムにかかわるドキュメンテーションに対する適切な保護管理の実施	Security of system documentation
	8.7 情報およびソフトウェアの交換 Exchanges of Information and Software	8.7.1 情報およびソフトウェア交換契約	情報およびソフトウェアの交換に際しての、他社との間での交換物件の保護についての合意の確立	Information and software exchange agreements
		8.7.2 配送中の媒体のセキュリティ	情報や媒体等の運送についての適切な保護策の実施	Security of media in transit
		8.7.3 電子商取引のセキュリティ	電子商取引サービスの提供または利用する場合にあたっての、対応システムに対する適切なセキュリティ対策の実施	Electronic commerce security
		8.7.4 電子メールのセキュリティ	電子メールサービスの提供または利用する場合にあたっての、適切なセキュリティ対策の実施	Security of electronic mail
		8.7.5 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サービスの提供または利用する場合にあたっての、対応システムに対する適切なセキュリティ対策の実施	Security of electronic office systems
		8.7.6 公開されているシステム	外部の公開するサービスの提供にあたっての、対応システムに対する適切なセキュリティ対策の実施	Publicly available systems
		8.7.7 情報交換のその他の形式	通信に音声、ファクシミリ、ビデオ通信を用いた場合における、適切なセキュリティ対策の実施	Other forms of information exchange

(注) 本表中の　要求事項区分ならびに要求事項の先頭にある　n.、 n. m、 n. m. は、JIS X 5080 (ISO/IEC 17799) における該当の章および節番号を示している。

表 4-1 JIS X 5080 (ISO/IEC 17799)における要求事項と本ガイドラインにおける要求事項の対応(4/6)

要求事項(コントロール)区分		要求事項	要求事項の概要	ISO/IEC 17799 における要求事項のタイトル
9. アクセス制御 Access Control	9.1 アクセス制御に関する業務上の要求事項 Business Requirement for Access Control	9.1.1 アクセス制御方針	システムへのアクセス制限・管理についての包括的なポリシーの確立	Access control policy
	9.2 利用者のアクセス管理 User Access Management	9.2.1 利用者登録	ユーザに対するするアクセス権の付与とその登録および抹消についての適切な管理の実施	User registration
		9.2.2 特権管理	システムアクセスにかかる特権の付与と管理についての厳格な管理の実施	Privilege management
		9.2.3 利用者のパスワードの管理	パスワードの付与とその管理の適切な実施	User password management
		9.2.4 利用者アクセス権の見直し	ユーザに対するアクセス権の付与や特権の付与についての定期的なチェックと必要な見直しの実施	Review of user access rights
	9.3 利用者の責任 User Responsibility	9.3.1 パスワードの使用	ユーザに対する付与しているパスワードの保護についての指導の実施	Password use
		9.3.2 利用者領域にある無人運転の装置	ユーザに対する使用可能状態での装置の放置の防止についての指導の実施	Unattended user equipment
	9.4 ネットワークのアクセス制御 Network Access Control	9.4.1 ネットワークサービスの使用についての個別方針	ネットワークの使用についての包括的なポリシーの確立	Policy on use of network services
		9.4.2 指定された接続経路	接続要求元から接続先までの接続経路の指定	Enforced path
		9.4.3 外部から接続する利用者の認証	外部からのアクセスに対する適切なユーザ認証の実施	User authentication for external connections
		9.4.4 ノードの認証	接続先が限定されているシステムにおける接続先ノードの認証の実施	Node authentication
		9.4.5 遠隔診断用ポートの保護	遠隔診断ポートがシステムへの侵入への入口に使われないようにする保護の実施	Remote diagnostic port protection
		9.4.6 ネットワークの領域分割	組織におけるネットワークの必要に応じたセグメント化の実施	Segregation in networks
		9.4.7 ネットワークの接続制御	ネットワークアクセスポリシーに沿った、システムへのアクセスやネットワークへの接続要求の個々に対する適切な制御の実施	Network connection control
		9.4.8 ネットワーク経路を指定した制御	外部ネットワークからのアクセス対するアクセス経路の指定	Network routing control
		9.4.9 ネットワークサービスのセキュリティ	ネットワークサービスの使用についての制限と、その使用にあたってのセキュリティ特性を反映したセキュリティ対策の実施	Security of network services
	9.5 オペレーティングシステムのアクセス制御 Operating system Access Control	9.5.1 自動の端末識別	必要な場合におけるアクセス端末に対する装置の自動的な認証の実施	Automatic terminal identification
		9.5.2 端末のログオン手順	攻撃を試みるものをガイドするようなログオンプロセスの設計の排除	Terminal log-on procedures
		9.5.3 利用者の識別および認証	システムへのアクセス要求者に対する適切な識別と認証の実施	User identification and authentication
		9.5.4 パスワード管理システム	システムへのアクセスに用いられるパスワードに対する厳格な管理の実施	Password management system
		9.5.5 システムユーティリティの使用	システムユーティリティの使用に対する制限と適切な管理の実施	Use of system utilities
		9.5.6 利用者を保護するための脅迫に対する警報	システムへのアクセスが脅迫によるものであることをシステム管理者等に知らせる機能の組込み	Duress alarm to safe quard users
		9.5.7 端末のタイムアウト機能	端末に対するタイムアウト機能(一定時間以上アクセスがない端末に対する接続の切断)の適用	Terminal time-out
		9.5.8 接続時間の制限	一つの端末からの接続に対する接続時間の制限の実施	Limitation of connection time

(注)本表中の 要求事項区分ならびに要求事項の先頭にある n.、 n.m、 n.m.は、JIS X 5080(ISO/IEC 17799)における該当の章および節番号を示している。

表 4-1　JIS X 5080 (ISO/IEC 17799)における要求事項と本ガイドラインにおける要求事項の対応(5/6)

要求事項(コントロール)区分		要求事項	要求事項の概要	ISO/IEC 17799 における要求事項のタイトル
9. アクセス制御 Access control	9.6 業務用ソフトウェアのアクセス制御 Application Access control	9.6.1 情報へのアクセス制限	情報やアプリケーションシステム機能に対応する適切なアクセス制限の実施	Information access restriction
		9.6.2 取扱いに慎重を要するシステムの隔離	慎重な取扱いを要するシステムの他のシステムからの隔離 (搭載サーバの分離やネットワーク的な干渉の排除)	Sensitive system isolation
	9.7 システムアクセスおよびシステム使用状況の監視 Monitoring system Access and Use	9.7.1 事象の記録	システムにおける例外事項やセキュリティ関連イベントについての記録の作成と保管の実施	Event logging
		9.7.2 システム使用状況の監視	情報処理設備や関連施設の使用についての適切な監視の実施と監視結果についての定期的なレビューの実施	Monitoring system use
		9.7.3 コンピュータ内の時計の同期	システム内で用いられるクロックの標準時への同期の確保	Clock synchronization
	9.8 移動型計算処理および遠隔作業 Mobile computing and Teleworking	9.8.1 移動型計算処理	モバイル端末の使用やモバイル環境での作業に対する適切なセキュリティ対策の実施	Mobile computing
		9.8.2 遠隔作業	テレワーキングにかかるリスクに対する適切なセキュリティ対策の実施	Teleworking
10. システムの開発および保守 Systems Development and Maintenance	10.1 システムのセキュリティ要求事項 Security requirements analysis and specification	10.1.1 セキュリティ要求事項の分析および明示	新規開発システムおよび既存システムの改修における、当該システムに対するセキュリティ要求事項の明確化	Security requirements analysis and specification
	10.2 業務用システムのセキュリティ Security in Application Systems	10.2.1 入力データの妥当性確認	入力データに対する受取り時又は処理に先立った妥当性チェックの実施	Input data validation
		10.2.2 内部処理の管理	日々の処理における内部処理の妥当性(正確性)についての確認の実施	Control of internal processing
		10.2.3 メッセージ認証	必要な場合におけるネットワーク経由で受取ったメッセージに対する真正性の確認の実施	Message authentication
		10.2.4 出力データの妥当性確認	日々の運用におけるシステム出力に対する妥当性のチェックの実施	Output data validation
	10.3 暗号による管理策 Cryptographic Controls	10.3.1 暗号による管理策の使用に関する個別方針	組織における暗号の適用についてのポリシーの確立	Policy on the use of cryptographic controls
		10.3.2 暗号化	メッセージやシステム上のデータに対する暗号適用ポリシーに沿った暗号化の実施	Encryption
		10.3.3 デジタル署名	必要な場合におけるデータに対するデジタル署名の適用	Digital signatures
		10.3.4 否認防止サービス	必要な場合における公証サービスの利用等、通信や処理に対する相手側の事後否認への備えの実施	Non-repudiation services
		10.3.5 かぎ管理	暗号鍵に対する厳格な管理の実施による暗号鍵の保護	Key management
	10.4 システムファイルのセキュリティ Security of System Files	10.4.1 運用ソフトウェアの管理	運用に用いているソフトウェアに対する適切な保護管理の実施	Control of operational software
		10.4.2 システム試験データの保護	システムの試験等で運用データを使用する場合における、運用データの確実な保護の実施	Protection of system test data
		10.4.3 プログラムソースライブラリへのアクセス制御	ソースライブラリに対する適切な保護管理の実施	Access control to program source library
	10.5 開発および支援過程におけるセキュリティ Security in Development and Support Processes	10.5.1 変更管理手順	アプリケーションの変更についての十分なレビューと適切な管理の実施	Change control procedures
		10.5.2 オペレーティングシステムの変更の技術的レビュー	オペレーティングシステムの変更にあたってのアプリケーションやセキュリティへの悪影響の予防策の実施	Technical review of operatig system changes
		10.5.3 パッケージソフトウェアの変更に対する制限	ソフトウェアパッケージの変更の制限と、変更にあたっての適切なレビューの実施	Restrictions on changes to software packages
		10.5.4 隠れチャネルおよびトロイの木馬	外部からソフトウェアを導入する場合におけるコバート通信路やトロイのコードに対する警戒の実施	Covert channels and Trojan code
		10.5.5 外部委託によるソフトウェア開発	ソフトウェアの開発を外部に委託する場合における、委託先に対する開発ソフトウェアのセキュリティ確保のために必要な諸施策の実施	Outsourced software development

(注) 本表中の 要求事項区分ならびに要求事項の先頭にある n.、 n.m、 n.m.は、JIS X 5080 (ISO/IEC 17799) における該当の章および節番号を示している。

表 4-1　JIS X 5080 (ISO/IEC 17799)における要求事項と本ガイドラインにおける要求事項の対応(6/6)

要求事項(コントロール)区分		要求事項	要求事項の概要	ISO/IEC 17799 における要求事項のタイトル
11. 事業継続管理 Business Continuity Management	11.1 事業継続管理の種々の面 Aspects of Business Continuity Management	11.1.1 事業継続管理手続	事業継続計画立案と維持のための仕組みの確立	Business continuity management process
		11.1.2 事業継続および影響分析	適切な事業継続計画立案のためのリスクアセスメントの適切な実施	Business continuity and impact analysis
		11.1.3 継続計画の作成および実施	リスクアセスメントに基づいた適切な事業継続計画の立案	Writing and implementing continuity plans
		11.1.4 事業継続経計画作成のための枠組み	業務単位に策定した事業継続計画のサイト全体としての事故処理要領への統合	Business continuity planning framework
		11.1.5 事業継続計画の試験、維持および再評価	立案した事故処理要領に対する試験の実施と、定期的なレビューの実施による必要な見直しの実施	Testing, maintaining and re-assessing business continuity plans
12. 適合性 Compliance	12.1 法的要求事項への適合 Compliance with Legal Requirements	12.1.1 適用法令の識別	準拠すべき法律、規制、契約等による要求事項の把握	Identification of applicable legislation
		12.1.2 知的所有権(IPR)	他社の著作権、意匠権、商標との知的所有権を侵害しないための適切な施策の実施	Intellectual property right (IPR)
		12.1.3 組織の記録の保護	保管が必要な組織の活動に関する記録の作成と紛失、破壊、改ざんからの防止	Safeguarding of organizational records
		12.1.4 データの保護および個人情報の保護	保護が必要なデータや個人情報の保護のための必要な施策の実施	Data protection and privacy of personal information
		12.1.5 情報処理施設の誤用の防止	情報処理設備や関連施設への不正なアクセスや不正な使用を防止するための施策の実施	Prevention of misuse of information processing facilities
		12.1.6 暗号による管理策の規制	暗号の利用における規制の遵守	Regulation of cryptographic controls
		12.1.7 証拠の収集	将来の紛争に備えた必要な証拠(情報)の確保	Collection of evidence
	12.2 セキュリティ基本方針および技術適合のレビュー Review of Security Policy and Technical Compliance	12.2.1 セキュリティ基本方針との適合	セキュリティ対策の実施状況についての定期的なチェックの実施	Compliance with security policy
		12.2.2 技術適合の検査	セキュリティ対策における技術面での対応が要求を満たしているかどうかについてのチェックの定期的な実施	Technical compliance checking
	12.3 システム監査の考慮事項 System Audit Considerations	12.3.1 システム監査管理策	システム監査の実施にあたっての、業務やシステムの運用への影響の排除	System audit controls
		12.3.2 システム監査ツールの保護	システムの監査に用いるツールや情報の整備や維持管理の実施	Protection of system audit tools

(注) 本表中の　要求事項区分ならびに要求事項の先頭にある　n.、 n.m、 n.m. は、JIS X 5080 (ISO/IEC 17799) における該当の章および節番号を示している。

第 2 部

JIS X 5080 (ISO/IEC 17799) における セキュリティ要求事項の解釈

(注)

この第 2 部は、JIS X 5080（ISO/IEC 17799）におけるセキュリティ要求事項を解釈したものである。JIS X 5080（ISO/IEC 17799）の記述をその求めていることが理解しやすいよう趣旨、要求事項、実施上のポイント、および参考に分解して、できるだけ端的な表現で示すように工夫してみた。このため、記述の組立てや表現はこれらの規格とは異なったものになっているが、これらの規格の言わんとしていることは忠実に受継いでいる。

ただし、規格そのものの参照を容易にするため、その章番、節番は、これらの規格における章番、節番に合わせ、章題や節題は JIS X 5080 の表現をそのまま当てはめた。

JIS X 5080（ISO/IEC 17799）は、そのタイトルにもあるように**“情報セキュリティマネジメントの実践のための規範”**を示したもので、情報セキュリティマネジメントのあるべき姿を描いたものである。

このため、これらの規格では、

- 必須事項と考えるものについては、「・・・・・ねばならない。」、
- 要望事項（実施が望まれるもの）と考えるものに対しては、「・・・・・が望ましい」

と言う表現を使い分けており、要望事項については組織のセキュリティポリシーに沿って採否を検討すればよいとしている。

本報告書では、必須事項と要望事項の使い分けは、その軽重とは関係がなく、この規格が本来期待している情報セキュリティマネジメントとしては、要望事項についても考慮すべき事項であると考え、すべてを「・・・・・ねばならない。」という表現を適用した。

それぞれの要求事項の適用にあたっては、それぞれの組織がサイトの運営実態に照らしてその採否と適用方法を考えなければならない。

3 セキュリティ基本方針

組織の情報セキュリティを確保するためには、組織における戦略的かつ組織的なセキュリティ活動が必要となる。組織のセキュリティ活動を戦略的かつ組織的なものにするためには、組織のすべての領域におけるセキュリティ活動についての要求の指針となる情報セキュリティ対策についての（トップレベルの）セキュリティポリシーが確立していなければならない。

3.1 情報セキュリティ基本方針

宣言された（トップレベルの）セキュリティポリシーは、組織におけるすべてのセキュリティ活動を統括するものである。（トップレベルの）セキュリティポリシーが機能するためには、その示すところが組織の運営実態に照らして適切なものであり、かつ、その位置付けが明確に示されていなければならない。

このため、（トップレベルの）セキュリティポリシーに関しては、

- 適切な情報セキュリティポリシー文書の発行とその位置付けの確立
- その妥当性を維持するためのレビューおよび評価の実施

が求められる。

3.1.1 情報セキュリティ基本方針文書

（トップレベルの）セキュリティポリシーは、経営レベルの課題としての組織の情報セキュリティ確保に向けた取組みを示すもので、外部の者も含むすべての関係者に徹底されなければならない。

(1) 要求事項

- 適切な（トップレベルの）セキュリティポリシーの確立

  （トップレベルの）セキュリティポリシーは、組織における情報セキュリティについての取組み方針を示すものとして、以下のような内容が含まれなければならない。また、その示すところは、組織の運用実態に照らして適切なものでなければならない。

  - 情報セキュリティの定義
  - セキュリティポリシーの全般的な目的
  - 適用範囲
  - 情報共有を可能にするための機構としてのセキュリティの重要性
  - 情報セキュリティの目標および原則についての経営陣の支持
  - 情報セキュリティについての取組み方針

－法的および契約上の要求事項への準拠
－セキュリティ教育にかかる要求事項
－ウイルス等の有害ソフトウェアの予防ならびに検出
－事業継続計画
－セキュリティポリシー違反への対応

・ 情報セキュリティ管理における責任の明確化と責任体制の確立
・ 関連文書

- 経営陣による承認と、経営陣による発行

  情報セキュリティへの取組みは経営レベルの課題であることを明確にするため、情報セキュリティ対策基本方針は、経営陣により承認され、経営陣によって発行されたものでなければならない。

- 従業員他関係者への周知

  組織におけるすべての活動にかかわる（トップレベルの）セキュリティポリシーは、従業員をはじめ外部からのサポート要員を含む組織の運営にかかわるすべてのスタッフに周知されていなければならない。

(2) **実施上のポイント**

- 情報セキュリティ対策への経営陣の参加の明示

  情報セキュリティは経営レベルの問題であることを明確にするため、情報セキュリティ対策基本方針には、経営者の参画とその責任が明記されていなければならない。

- （トップレベルの）セキュリティポリシーの記述について

  （トップレベルの）セキュリティポリシーは、関係者のすべてに徹底されなければならない。このため、（トップレベルの）セキュリティポリシーは理解し易く書かれ、かつ、常に身近に触れることができるようになっていることが要求される。

3.1.2 見直しおよび評価

組織の運営環境の変更等により、組織の運営実態に合わなくなった(トップレベルの)セキュリティポリシーは機能しないだけでなく有害にもなる。このため、(トップレベルの)セキュリティポリシーは、常にその妥当性が維持されていなければならない。

(1) **要求事項**

- (トップレベルの)セキュリティポリシーの維持およびレビュー責任者の確定
- (トップレベルの)セキュリティポリシー取扱い要領の確立
- 取扱い要領に従った(トップレベルの)セキュリティポリシーの見直しと必要な場合における適切な改定の実施

(2) 実施上のポイント

- (トップレベルの)セキュリティポリシーの取扱い要領について

  (トップレベルの)セキュリティポリシーの取扱い要領で明確にすべき事項としては、以下があげられる。

  ・ (トップレベルの)セキュリティポリシーの発行手続き

  ・ (トップレベルの)セキュリティポリシーの見直しおよび改訂手続き

  －定期的な見直しの実施

  －見直しが必要となる場合の明示

  －見直しおよび改訂の手続き

(3) 参考

- (トップレベルの)セキュリティポリシーの見直しが必要なケースと見直すべき事項

  表 3-1に、(トップレベルの)セキュリティポリシーの見直しのポイント、臨時の見直しが必要となる場合を示す。

表 3-1 (トップレベルの)セキュリティポリシーの見直しのポイント

項目	内容
① 定期的に見直しを行うべき事項	・セキュリティポリシーの有効性 ・情報セキュリティ対策コストとその妥当性 ・情報セキュリティ対策の事業効率に及ぼす影響 ・使用技術の有効性
② 臨時の見直しを行うべき要因	・重大なセキュリティ事故の発生 ・新しい脅威の発生 ・新しい脆弱点の発生 ・組織等運営体制の変更 ・技術インフラの変更

4 組織のセキュリティ

情報セキュリティは、セキュリティ技術の導入だけでは実現できず、組織の活動にかかわる従業員や外部からのサポート要員等の行動にかかわるところが多い。組織におけるスタッフの行動が、セキュリティポリシーに沿ったものになるようにするためには、組織およびスタッフに対する適切な管理も必要となる。

このためには、以下の施策の実施が必要となる。

(1) 情報セキュリティ対策推進組織の確立

(2) 外部要員に対するセキュリティ対策の確立

(3) アウトソーシングに対するセキュリティ対策の確立

4.1 情報セキュリティ基盤

組織におけるセキュリティ対策が機能するためには、それが経営陣を含む組織全体としての組織的な取組みになるようにする体制の確立が必要となる。

このためには、

- 情報セキュリティ委員会の組織
- 関連部門間の連携の確立
- 情報セキュリティ対策にかかる責任分担の明確化
- 情報処理施設や設備の導入要領の確立
- 情報セキュリティに関する専門家の活用
- セキュリティ事故発生時の組織間連携の確立
- 情報セキュリティ監査の実施

が必要となる。

4.1.1 情報セキュリティ運営委員会

組織の情報セキュリティの確保には、経営陣の参画が不可欠である。このため、情報セキュリティの確保にかかる活動に経営陣の実効的な参画が行われる仕組みの確立が必要となる。

(1) 要求事項

- 情報セキュリティおよび関連活動にかかる経営陣の責任の明確化
- 経営陣も参加した情報セキュリティ委員会（情報セキュリティフォーラム）の組織とその適切な運営

(2) **実施上のポイント**

- 情報セキュリティおよび関連活動における経営陣の責任
  - ・ セキュリティマネジメント活動の監督･指導
  - ・ 必要なリソースの確保
- 情報セキュリティ委員会で審議すべき事項
  - ・ 情報セキュリティ基本方針およびセキュリティの全般的責任についてのレビューと承認
  - ・ セキュリティ環境の変化が情報セキュリティに与える影響の分析
  - ・ 情報セキュリティ事故および事故処理についてのチェック
  - ・ 情報セキュリティ対策にかかる活動の推進策の審議と承認
  - ・ 総括責任者の任命とその責任の明確化

4.1.2 情報セキュリティの調整

大きな組織においては、組織の情報セキュリティの確保には組織運営にかかわる多くの業務が関係するため、さまざまな部門の連携が必要となる。このためには、関係する部門同士が情報セキュリティ対策の実施に関しお互いに連携ができる仕組みが構築されていなければならない。

(1) **要求事項**

- 情報セキュリティ対応部門間での責任分担の明確化
- 関係者における情報セキュリティにかかわる脅威と情報セキュリティ対策の取組みについての意識の醸成
- 情報セキュリティ対策へのシステム計画の反映
- 新規導入システムおよび新規提供サービスに対するセキュリティ対策の十分性の評価
- 情報セキュリティ事故の分析と問題点の抽出と対策の実施

(2) **実施上のポイント**

- 情報セキュリティ対策にかかる部門責任者間での情報セキュリティ対策の実施にあたっての認識と方法論の共有
- 日常業務における情報セキュリティの確保に向けた取組みの可視化

4.1.3 情報セキュリティ責任の割当て

組織のセキュリティの確保は多くの関係者がかかわる。定められたセキュリティの確保にかかるさまざまな施策が適切に機能するようにするためには、保護対象資産に対する保護責任や、セキュリティプロセスの実施責任等の組織内における情報セキュリティの確保についての責任分担が明確

にされ、それが当事者に周知されていなければならない。

(1) **要求事項**

- 総括責任者の任命とその責任の明確化
- 保護対象資産やセキュリティプロセスの実施等、セキュリティ対策にかかる活動の個々に対する責任者の明確化
- 保護対象情報の保有責任者の明確化

(2) **実施上のポイント**

- 責任体制の承認と文書化

4.1.4 情報処理設備の認可手続

不用意な情報処理関連施設や設備の導入は、サイトのセキュリティを脅威にさらす。このようなことを避けるためには、情報処理関連施設や設備の導入にあたっては、十分なチェックがなされるよう、導入についてのルール・手続きの確立とその適切な運用が行われなければならない。

(1) **要求事項**

- 機器の導入や持込みについてのルール・手続きの確立
- 定められたルール・手続きに従った機器等の情報処理関連施設や設備の導入あるいは持込みの実施

(2) **実施上のポイント**

- 機器等の情報処理関連施設や設備の導入や持込みについての認可制の導入
- 管理の対象とすべき機器等
  - ・ 新規に導入するハードウェアやソフトウェア
  - ・ 業務で使用する個人所有の機器
  - ・ セキュリティ対策の対象領域に持込む個人の作業に用いる個人所有機器
- 装置の導入や持込みの認可に当って審議すべき事項
  - ・ 目的および用途の妥当性
  - ・ セキュリティポリシー要求事項への準拠
  - ・ 他のシステム構成要素との親和性、整合性
- 新しい設備の導入に対する承認者のレベル
  - ・ 対象機器等の利用部門の責任者
  - ・ 対応システムのセキュリティ総括責任者

4.1.5　専門家による情報セキュリティの助言

情報セキュリティの確保には、高度の専門知識やスキルが必要となる。このため、必要に応じ情報セキュリティの専門家の支援が得られるような体制の整備も必要となる。

(1) **要求事項**

- 社内セキュリティ専門家の育成
- 社内セキュリティアドバイザ制の確立
- 社外セキュリティアドバイザの活用

(2) **実施上のポイント**

- 社内セキュリティアドバイザ制の導入で検討すべきこと
  - ・ 社内セキュリティアドバイザのタスクの明確化
  - ・ 社内セキュリティアドバイザの育成、確保
  - ・ 社内セキュリティアドバイザの活用環境の整備

4.1.6　組織間の協力

発生したセキュリティ事故に対し迅速かつ的確な対応が行われるようにするためには、事故発生時に社外からの応援も含み必要な体制が取れるような仕組みを確立しておくことも必要となる。

(1) **要求事項**

- セキュリティ事故対応体制の確立
- セキュリティ事故発生時における関連社外組織との円滑な連携の確保

(2) **実施上のポイント**

- セキュリティ事故の処理に必要な作業
  - ・ 発生した事故とその処理についての報告
  - ・ 事故処理についての社内外の関連部門や専門家への助言や支援の依頼
  - ・ 事故原因の究明、原因の除去、被害からの回復、再発防止策の展開

(3) **参考**

表 4-1に、セキュリティ事故の処理にかかわる社内部門や社外の機関を例示する。

表 4-1 セキュリティ事故の処理にかかわる社内外組織

連携すべき社内部門	連携すべき社外機関
・システム運用部門	・法執行機関（警察等） ・セキュリティ管理機関（IPA 等） ・ネットワークサービスプロバイダ ・システムサービスプロバイダ

4.1.7 情報セキュリティの他者によるレビュー

情報セキュリティ対策が適切に行われているかどうかについての監査が、定期的に行われることが望ましい。この監査においては、情報セキュリティ対策基本方針が適切かどうか、また、組織の運営において情報セキュリティ基本方針が適切に実行されているかどうかについてチェックされなければならない。

(1) **要求事項**

- 情報セキュリティ対策の実施状況についての監査の実施

(2) **実施上のポイント**

- 監査でチェックすべき事項

  情報セキュリティ対策の実施状況についての監査でチェックすべき事項としては、以下があげられる。

  ・ 情報セキュリティ対策基本方針の妥当性

  －有効性

  －実行可能性

  ・ 組織の活動のセキュリティ要求事項への準拠状況

- 監査の実行体制について

  この監査には、内部監査組織、外部機関等、セキュリティ対策実行体制とは独立した組織があたることが望ましい。

4.2 第三者によるアクセスのセキュリティ

組織の運営には、従業員だけでなく外部からの要員も多くかかわる。このため、外部から組織に派遣されている要員および外部への業務の委託についても、それらがセキュリティの脅威にならないようにするための施策を講じることが必要となる。

このためには、

- 外部要員の組織運営への参画にかかるﾘｽｸの明確化
- 外部要員の受入れにかかる契約におけるｾｷｭﾘﾃｨ要求事項の明確化

が゙必要となる。

4.2.1 第三者のアクセスから生じるリスクの識別

外部の者に組織の業務に従事させる場合、これらの者が組織の情報ｾｷｭﾘﾃｨの脅威にならないようにしなければならない。このためには、契約している請負業者に対し、情報ｾｷｭﾘﾃｨ面での管理の対象となる者を示し、これらの者への情報ｾｷｭﾘﾃｨにかかる責任を明確にし、情報ｾｷｭﾘﾃｨの確保についての協力が得られるようにしなければならない。

(1) 要求事項

- 外部の要員を組織の運営に参加させることにともなうﾘｽｸの明確化
- 外部のシステムとの接続にともなうﾘｽｸの明確化
- 管理対象者の明確化と、管理対象者への情報ｾｷｭﾘﾃｨ確保にかかる責任についての徹底

(2) 実施上のポイント

- 外部システムとの接続あるいは外部の者によるシステムへの接続にかかるﾘｽｸｱｾｽﾒﾝﾄについて

  外部システムとの接続あるいは外部の者によるシステムへの接続にかかるﾘｽｸの分析にあたって、評価すべき事項としては、以下があげられる。

  ・ 使用するアクセスのﾀｲﾌﾟ
  ・ アクセスする情報の重要性
  ・ アクセスする側において実施されているｾｷｭﾘﾃｨ対策の内容とﾚﾍﾞﾙ
  ・ アクセスによって組織に生じる可能性のあるﾘｽｸ
- ﾘｽｸの分析においては、外部の者による組織または組織の情報システムへのアクセスのすべてを対象にしなければならない。ﾘｽｸ評価の対象となる物理的アクセスおよび論理的アクセスの事例を“参考“に示す。
- 管理対象者の漏れのないﾘｽﾄｱｯﾌﾟ
- 管理対象者に明示すべき情報ｾｷｭﾘﾃｨ確保にかかる責任の明確化

  派遣契約等で明確にすべき管理対象者の情報ｾｷｭﾘﾃｨ確保にかかる責任等には、以下にあげるものがある。

  ・ 情報ｾｷｭﾘﾃｨの確保にかかる責任
  ・ ｾｷｭﾘﾃｨ要求事項

・ セキュリティ対策の内容

- セキュリティ要求事項および内部管理策の契約書への反映
- 契約締結前のシステムへのアクセス禁止
- セキュリティ要求事項等を明示した派遣契約前のシステムへのアクセスの禁止

(3) **参考**

- 管理対象となる情報システム資産へのアクセスと管理対象者
  管理対象となる情報システム資産へのアクセスと管理対象者を、表 4-2に例示する。

表 4-2 管理対象となる外部要員と外部からのアクセスの例

管理の対象となる 物理的アクセス	管理の対象となる 論理的アクセス	管理対象者
・オフィスへのアクセス ・コンピュータ室へのアクセス ・ファイリングキャビネットへのアクセス	・情報の交換、情報システムへのアクセス、保守等によるアクセス ・データベースへのアクセス ・情報システムへのアクセス	・ハードウェアおよびソフトウェアのメンテナンス等のシステムサポートスタッフ ・清掃人、賄い人、警備員等のオフィスサポートスタッフ ・研修生 ・短期の臨時職員 ・外部コンサルタント

4.2.2 第三者との契約書に記載するセキュリティ要求事項

外部の者に保護対象資産へのアクセスを許す場合は、セキュリティ要求事項を明示し、その遵守を要求しなければならない。このためには、システム等の保護対象資産にアクセスが許される者との間で、必要な契約の締結と、この契約に基づく管理が行われなければならない。

(1) **要求事項**

- 正式な契約に基づく受入れ外部要員に対するセキュリティ管理の実施
- 派遣要員に求めるセキュリティ要求事項の、派遣元との派遣契約書への完全な反映
- 契約上でのセキュリティ要求事項についての契約相手の完全な理解の確保
- 契約相手に保証責任を負わせることについての相手側の納得の確認

(2) **実施上のポイント**

- 外部要員の受入れにかかわる契約書には、情報セキュリティ対策基本方針と対策実施上の施策が反映されていなければならない。この契約書の中に記載されるべき情報セキュリティ関係事項としては、以下があげられる。
  ・ 情報セキュリティに関する一般的ポリシー
  ・ 資産の保護

・ 使用が許可される各サービスの記述
・ サービスの目標レベルとサービスの許可されないレベル
・ スタッフの転任に関する規定
・ 契約当事者のそれぞれの義務
・ 個人情報保護法、不正競争防止法等の関係する法律についての責任
・ 知的所有権および著作権譲渡および共同作業の保護
・ アクセス制御への合意事項
・ 検証可能な責任基準の明示とそれらの監視と報告
・ システムの利用者の活動を監視し、無効にする権利
・ 契約上の責任を監査する権利または監査を第三者に実施してもらう権利
・ 問題解決のための段階的処理プロセスの確立
・ 報告に含まれるべき内容と形式
・ 変更の手続き
・ 要求される物理的保護管理策およびその管理策が確実に実施されるためのメカニズム
・ 方法、手順、セキュリティについてのユーザと管理者への訓練
・ 不正ソフトウェアから確実に保護するための管理策
・ セキュリティ事故およびセキュリティ違反についての報告、通知、調査に関する取決め
・ 第三者と下請け業者のかかわりあい方

4.3 外部委託

組織の業務の一部を外部に委託することもある。このような場合、業務を外部に委託していることが、組織のセキュリティの脅威にならないようにしなければならない。

このためには、業務の外部委託にあたっては、その契約でセキュリティ要求事項を明確にし、委託先における適切なセキュリティ対策の実施を確実なものにしなければならない。

4.3.1 外部委託契約におけるセキュリティ要求事項

情報処理にかかる業務を外部に委託する場合、委託業務におけるセキュリティの確保についての要求事項を委託先に明確にし、委託作業に対してはその履行についての合意を得ていなければならない。このためには、委託業務にかかるセキュリティ要求事項を、委託契約の中に明示しておくことが必要である。

(1) 要求事項

- 情報システム、ネットワーク、デスクトップ環境等の外部業者へ委託にあたってのセキュリテ

ｨ要求事項の契約書への反映

(2) 実施上のポイント

- 業務委託契約書に記載すべきセキュﾘﾃｨ要求事項としては、以下があげられる。
  - 法的な規定に対する対応の明確化（個人情報保護法他）
  - 当事者に求められるセキュﾘﾃｨ責任の明確化
  - 財産の保全性、機密性の維持および試験の方法の明確化
  - アクセス制約、アクセス権限の物理的および論理的な管理策
  - 補助ｻｲﾄの準備等の災害時におけるサービスの維持確保
  - 装置の物理的セキュﾘﾃｨ対策
  - 監査の実施
- 保護対象情報資産ﾘｽﾄは、その変更が常に反映されなければならない。

5 資産の分類および管理

セキュリティの確保にかかる活動を確実なものにするためには、組織において保護の対象となる資産が把握され、それぞれの保護対象資産に求められる保護が明確にされていなければならない。

このことを実現するためには、

⑴ 保護対象資産の正確な把握

⑵ 保護対象資産の個々に対する保護要件の明確化

が必要となる。

5.1 資産に対する責任

セキュリティ対策の漏れを防ぐためには、組織における保護対象資産についての正確な管理台帳が作成されていなければならない。

5.1.1 資産目録

情報資産に対する適切な保護が行われるためには、保護すべき情報が正確に把握されていなければならない。このため、保護されるべき情報とそれぞれに求められる保護のレベルについての台帳を作成し、その内容の妥当性の維持管理に努めなければならない。

(1) 要求事項

- 保護対象資産台帳の作成と維持

(2) 参考

- 保護対象資産の洗出しに漏れがないようにしなければならない。情報システムにかかわる保護対象資産を、表 5-1に例示する。

表 5-1 情報システムにおける保護資産

情報資産	データベース、データファイル,システムドキュメンテーション、ユーザマニュアル、訓練資料、操作又はサポート手順、業務継続計画、フォールバック要領、アーカイブされた情報
ソフトウェア資産	アプリケーションソフトウェア、システムソフトウェア、開発用ツールおよびユーティリティ
物理的資産	コンピュータ装置(プロセッサ、モニタ、ラップトップ、モデム)、通信装置(ルータ、PBX、ファクシミリ、留守番電話)、磁気媒体(テープおよびディスク)その他の技術装置
サービス資産	コンピューティング、通信サービス、暖房や照明等の一般ユーティリティ、電源、空調

- それぞれの保護対象資産の属性として明確にすべき事項としては、以下があげられる。
  - 当該資産の形態
  - 当該資産の価値および重要度
  - 当該資産の所有者（管理責任者）
  - 当該資産の所在場所

5.2 情報の分類

保護の対象となる情報システム資産に対する保護が適切に行われるためには、保護の対象となる資産の個々に対し、保護要件が適切に指定されていなければならない。

このためには、

- 保護対象資産に対する保護基準（分類のガイドライン）の確立
- 個々の保護対象資産に対する適切な保護要件の指定

が必要となる。

5.2.1 分類の指針

情報資産に対する保護が適切に行われるためには、情報資産の保護管理の基準としての保護レベルのクラス分けと、それぞれの保護クラスに対する標準的な保護要件が確立されていなければならない。

(1) **要求事項**

- 情報資産の保護クラスの定義
- 保護対象資産個々に対する適用保護クラスの適切な指定

(2) **実施上のポイント**.

- 保護基準の策定にあたっては、必要以上に複雑にしない
- 保護資産の中には時間の経過にともない重要性が変化するものがある。このため、これらの情報資産に対する保護クラスの指定は、その変化に伴い変更されるような仕組みも必要となる
- 個々の保護資産に対する保護基準の適用（クラス分けあるいはラベル付け）にあたっての留意事項としては、以下があげられる。
  - 同じ情報資産でもその重要度は部門によって異なるため、適用する保護クラスの指定にあたっては、この点について十分留意すること
  - 保護資産個々に対する適用保護クラスの指定は、当該資産の管理責任者が当ることが

望ましい

5.2.2 情報のラベル付けおよび取扱い

保護対象の情報資産の保護が、それぞれの情報の特性に応じ適切に保護されるためには、保護対象情報の個々に対する保護レベルの指定が適切に行われ、指定された保護レベルに適用される保護が確実に実行されなければならない。このためには、保護対象情報に対する保護レベルの指定手順や、保護レベルごとの保護管理上の取扱い方法が明確にされていなければならない。

(1) **要求事項**

- 個々の情報に対する保護レベルの指定（ラベル付け）手順の確立
- 保護レベルごとの保護管理要領の確立

(2) **実施上のポイント**

- 取扱いに注意を要するまたは重要な情報と分類されている情報を含む印刷物やスクリーン表示等のシステム出力への該当ラベルの表示
- 物理的形式の情報に対する物理的なラベルの添付と、電子的形式の情報に対する電子的なラベル付け等ラベル付けについての工夫の実施
- 情報の保護管理要領は、情報の物理的形式および電子的形式を問わず適用できるものであること。このため、以下に示す情報処理活動も情報の保護管理要領で規定の対象に含まれていること
  - 複写、保存
  - 郵送および FAX または電子メールによる送信
  - 携帯電話、ボイスメール、留守番電話等を用いた話し言葉による送信、抹消

6 人的セキュリティ

組織の運営には、従業員だけでなく外部からの要員も多くかかわる。このため、外部から組織に派遣されている要員および外部への業務の委託についても、それらがセキュリティの脅威にならないようにするための施策を講じることが必要となる。

このためには、

(1) スタッフに対するセキュリティ管理の実施

(2) 情報システムユーザに対するセキュリティ教育の実施

(3) セキュリティ事故およびシステム異常発生時の報告の徹底

が必要となる。

6.1 職務定義および雇用におけるセキュリティ

スタッフの行動が組織のセキュリティの脅威にならないようにするためには、不適切な者が組織の活動にかかわらないようにするとともに、業務にあたる者に対しては、セキュリティポリシーに沿った業務を遂行することを義務付けるとともに、必要な指導を行わなければならない。

このことを実現するためには、

- ジョブ責任の定義におけるセキュリティにかかわる責任の明示
- 人員採用審査ポリシーの確立
- 機密保持合意書の作成
- 採用者に対するセキュリティ要求の実施

が必要となる。

6.1.1 セキュリティを職責に含めること

スタッフが業務をセキュリティポリシーに沿って遂行するようにするためには、ジョブ責任の定義の中でセキュリティに関する責任を明確にしておくことが必要となる。

(1) 要求事項

- 職責の定義におけるセキュリティに関する責任の明示
- セキュリティに関するすべての責任の分担の明確化

(2) 実施上のポイント

- セキュリティに関する責任について明確にすべき事項
  - ・ セキュリティポリシーの実行および維持に関する一般的責任

・ 保護対象財産の保護責任
・ セキュリティにかかわる諸施策の実行責任者

6.1.2 要員審査およびその個別方針

組織のセキュリティを脅かすような不適正な人物を、組織の運営に関与させないようにしなければならない。このためには、スタッフの採用にあたっての採用予定者に対する信用のチェックや、特定の業務の割当てにあたっての信用のチェックが必要とされる。

なお、個人の信用度に関する情報はプライバシーにかかわるため、その取扱いには十分な注意が必要である。

(1) 要求事項

- 従業員の採用時における信用度のチェックの実施
- 情報処理施設や設備にアクセスする業務への配置に当っての信用度の再確認の実施
- 特に重要なポストにいるスタッフに対する信用チェックの定期的な実施
- 請負業者との契約および臨時スタッフの受入れ時における信用チェックの実施
- 派遣要員の信用についての派遣元の責任の明確化
- 取扱いに慎重を要するシステムにアクセスするスタッフに対するセキュリティ管理能力の評価と向上の推進
- 業務に影響を与えることにつながるような部下の個人事情の把握

(2) 実施上のポイント

- スタッフの採用時における信用度のチェックのポイント
  - 仕事および人物を示す人物証明書の利用
  - 応募者の履歴書の確認
  - 学業･専門資格の確認
  - 身分証明のチェック（公的電子証明書、住民票、免許証他）

6.1.3 機密保持契約

スタッフが業務を通じて知り得た機密情報等を外部に漏らしたりすることを牽制するためには、スタッフを就業させるにあたって、機密保持契約または非開示を確約させておくことも必要である。

(1) 要求事項

- 対象となるすべてのスタッフとの機密保持または非開示合意書の締結

- 退職等採用または契約条件に変更が生じた場合における機密保持契約の見直しおよび適切な処置の実施

6.1.4 雇用条件

従業員の採用にあたっては、就業後の業務の遂行が情報セキュリティ対策基本方針の示すところに沿って行われるようにするため、採用条件に情報セキュリティに対する従業員の責任を明示しておくことも必要である。

(1) **要求事項**

- 採用条件の中での雇用後の情報セキュリティ関連要求事項の明示
- 違反者に対する処置の明確化
- 採用条件の中での従業員の法律上の責任および権利の明示

(2) **実施上のポイント**

- 採用条件の中で明示すべき情報セキュリティ関連要求事項について

  採用条件の中で明示すべき情報セキュリティ関連要求事項のなかで、特に重要なこととしては、以下があげられる。

  ・ セキュリティ要求事項の適用範囲

  一般に組織の敷地外および通常の就労時間外の作業にも適用される。

  ・ 雇用期間中における情報セキュリティに対する責任

  ・ 雇用終了後の定められた期間における責任の継続

  ・ 従業員の法律上の責任および権利

6.2 利用者の訓練

システムユーザのセキュリティへの無関心は、組織のセキュリティの脅威となる。システムのユーザが、情報セキュリティの脅威を認識し、日常の業務において組織のセキュリティポリシーを遵守できる態勢がとれるようにしなければならない。

このためには、ユーザに対する情報セキュリティに関する教育および訓練が必要となる。

6.2.1 情報セキュリティ教育および訓練

組織の運営にかかわるすべての従業員および外部要員に対する情報セキュリティ基本方針とセキュリティプロセスに対する教育と訓練は、適切に行われなければならない。

(1) **要求事項**

- 関係する業務に従事させる時における必要な教育と訓練の実施
- 定期的な更新指導の実施

(2) **実施上のポイント**

- 教育訓練の対象とすべき事項

  情報システムのユーザに対し実施すべき教育としては、以下があげられる。

  ・ 情報セキュリティ基本方針
  ・ 個別セキュリティ要求事項
  ・ 法律的な責任
  ・ 業務運営上の諸管理事項
  ・ ログオン手順やソフウエアパッケージの使用法等の情報処理施設や設備の正しい使用法等

6.3 セキュリティ事件・事故および誤動作への対処

セキュリティ事故に対しては適切な処置が取られなければならない。また、セキュリティ事故に発展しかねない兆候も見逃さないようにし、事故になる前に必要な対策を講じることが組織としてできるようになっていることも重要である。また、同じような事故が繰返されないよう、発生した事故については、その教訓が組織のセキュリティ対策にフィードバックされるようになっていなければならない。

このためには、

- 発生したセキュリティ事故に対する適切な報告の実施
- 発見したセキュリティにかかる欠陥に対する適切な報告の実施
- 発見したソフトウェア誤動作に対する適切な報告の実施
- 事故の教訓のフィードバック
- セキュリティ要求事項への違反に対する懲戒の実施

が必要となる。

6.3.1 セキュリティ事件・事故の報告

セキュリティ事故が発生した場合は、速やかに報告が行われ適切な処置が行われなければならない。

(1) **要求事項**

- 発生事故についての報告手順の確立
- 関係者への報告手順の徹底

(2) **実施上のポイント**

- 事故処理終了後の報告者へのフィードバックの実施
- 事故からの教訓の抽出と、業務プロセスおよび教育へのフィードバックの実施および活用

6.3.2 セキュリティの弱点の報告

情報システムやサービスにセキュリティの欠陥またはセキュリティに対する脅威を検知した場合、またはその疑いを認知した場合は、速やかに報告が行われ、必要な処置がとられるようになっていなければならない。

(1) **要求事項**

- 認知したセキュリティ欠陥についての報告要領の確立
- ユーザに対するセキュリティ欠陥の報告についての教育の実施

6.3.3 ソフトウェアの誤動作の報告

ソフトウェアにおける誤動作等の異常は大きな事故に結びつくことがある。このため、ソフトウェアの動作に異常が見られた場合は、その直接的な影響の大小にかかわらず、速やかな報告と適切な処置が行われるようになっていなければならない。

(1) **要求事項**

- ソフトウェアの誤動作他の異常発見時の報告手順の確立
- 報告に対する処理要領の確立

(2) **実施上のポイント**

- ソフトウェアの誤動作等の異常な動きに対する感度の向上
- 誤動作発生時における適切な暫定処置要領の確立

特に、許可なく疑いのあるソフトウェアの除去や回復処置の実行は、行われないようになっていなければならない。

(3) **参考**

- 常に、画面メッセージ等への注意を払い、問題の兆候を発見することができるようにする訓練も必要となる。
- ソフトウェアに誤動作等の異常が発生した場合の回復処置等は、専門スタッフによって行われなければならない。

6.3.4 事件・事故からの学習

セキュリティ事故をゼロにすることは困難であるが、セキュリティの確保に同じ失敗は繰返さないようにしなければならない。同一の原因によるセキュリティ事故の再発や、将来の事故における被害の極小化を図るためには、発生したセキュリティ事故についての体系的な分析を行い、教訓を抽出してセキュリティ対策への反映を図らなければならない。

(1) **要求事項**

- 定量的な分析の実施
- 定量的分析をもとにした監視メカニズムの確立
- これらの情報をもとにしたシステムの脆弱性の把握と事故の予測の実施
- これらの情報のセキュリティポリシーならびにセキュリティプロセスのレビューへの活用

(2) **実施上のポイント**

- 事故および誤動作のタイプ、大きさ、対策に要したコスト等に対する分析の実施

6.3.5 懲戒手続

情報セキュリティ基本方針は関係者が遵守しなければ機能しない。セキュリティ要求事項への違反に対する正式な懲戒制度の確立と、違反に対する懲戒制度に沿った厳格な実施も、関係者に情報セキュリティ基本方針を遵守させるための工夫の一つである。

(1) **要求事項**

- 従業員のセキュリティポリシーやセキュリティプロセス違反に対する懲戒プロセスの確立
- 違反発生時における定められた懲戒プロセスに従った公平な懲戒の実施

7　物理的および環境的セキュリティ

組織のセキュリティの確保のためには、許可されない者の情報処理設備や施設あるいは情報への物理的なアクセスが制限されていなければならない。

このためには、

⑴ 保護領域(安全領域)の確立

⑵ 装置のセキュリティの確保

⑶ 一般管理策の確立と実施

が必要となる。

7.1　セキュリティが保たれた領域

組織の敷地内に置かれた情報処理設備や施設および情報への認可されていない物理的なアクセスを防止するためには、保護対象領域を定め、その領域に対して適切な物理的なバリアを設けるとともに、この保護領域への出入りについて適切な管理を行うことが必要となる。

このことを実現するためには、

- 保護領域に対する物理的なセキュリティ外壁の設置
- 保護領域への物理的な出入りについての管理の実施
- オフィス、ルーム、および施設におけるセキュリティ対策の実施
- 保護領域における作業の管理の実施
- 受渡しエリアの設置と受渡しエリアにおける適切な管理の実施

が必要となる。

7.1.1　物理的セキュリティ境界

情報や情報処理施設および設備の物理的な保護の実現には、保護領域に対する物理的なバリアの設置も検討しなければならない。

(1) 要求事項

- 必要に応じた保護領域の設定
- 個々の保護領域の境界へのリスクアセスメントに基づく適切なバリアの設置

(2) 実施上のポイント

- 保護領域の境界の明示
- 敷地の外周、情報処理施設や設備を含む建物、および情報処理施設や設備の周辺のそ

れぞれにバリアを設けるといった階層的なバリアの構築
- 認可されない者のアクセスを排除するための設備の導入

7.1.2 物理的入退管理策

認可されていない者が保護領域に立入ることがないよう、保護領域への物理的な出入りは適切に管理されていなければならない。

(1) **要求事項**
- 保護領域への物理的な出入りについての適切なルールの確立
- 保護領域への物理的な出入りについてのルールに基づいた管理の実施

(2) **実施上のポイント**
- ビジターに対するルールの確立とその適用の遵守
- 取扱いに慎重を要する情報や情報処理施設および設備に対する物理的なアクセス管理の実施
- すべてのスタッフに対する明確な ID の付与
- スタッフ全員による不審な者の立入りについての監視
- 保護領域に対するアクセス権についての定期的な見直しの実施

(3) **参考**
- ビジターに対する管理領域内での行動の制約について

  ビジターは保護領域には入れないことを原則とし、立入ることを許可した場合は、以下に示すような管理を行う
  - 入退室の記録
  - 保護領域内での行動規範の明示
  - 保護領域内における行動の監視

7.1.3 オフィス、部屋および施設のセキュリティ

認可されていない者のオフィス、ルームおよび情報処理施設に対する立入りにより、システムのセキュリティが脅かされないようにするためには、オフィス、ルームおよび施設への部外者の立入りをしにくくする工夫が必要である。

(1) **要求事項**
- 主要な施設の設置場所の適切な選択

- 主要な設備や施設の目的,設置場所等の外部への隠蔽
- 情報を扱う機器等の保護領域内への設置
- 必要に応じた侵入検知システムの導入
- 情報処理設備や施設の第三者運営のものとの隔離
- 危険物および可燃物の保護領域からの隔離と安全な保管
- バックアップ装置や媒体のメインサイトからの隔離

7.1.4 セキュリティが保たれた領域での作業

保護領域におけるスタッフおよび第三者の活動が、セキュリティに脅威を及ぼさないようにするためには、保護領域におけるスタッフおよび第三者の活動について、適切な規制と管理が行われなければならない。

(1) **要求事項**

- 必要のない者に対する保護領域の存在および機能の隠匿
- 保護領域での作業の監督
- スタッフ不在時における施錠と、不在時に侵入がないことの確認
- 立入り制限の認可や作業の監視等による、サポートサービス員等の第三者の立入り制限
- 写真、ビデオ、オーディオ等の記録装置の持込みの禁止

7.1.5 受渡し場所の隔離

外部との情報や装置等の受渡しはセキュリティ上の穴になることもある。このようなことを防ぐためには、情報等の受渡し用の特別なエリアを設け、必要な管理を行い、物品等の搬入や搬出がセキュリティの脅威にならないようにしなければならない。このためには、保護対象領域と受渡しエリアの隔離等を含む受渡しエリアの適切な設置と、受渡しエリア内における安全措置を講じなければならない。

(1) **要求事項**

- 必要に応じた受渡しエリアの設置
- 受渡しエリアを介した外部との物品の授受についての安全策の確立とその実施

(2) **実施上のポイント**

- 外部との物品の授受についての安全策についての工夫
  - ・ 必要に応じた受渡しエリアの設置

・ 受渡しエリアへの外部からのアクセスの制限
・ 受渡しエリアの外部から内部への直接的な通抜けができる環境の排除
・ 搬入物の引渡しエリアから保護領域への引渡しにおける安全確認の実施
（潜在的危険物の発見･除去）
・ 敷地に入れる前の搬入物の登録

7.2 装置のセキュリティ

装置や装置内にある情報資産の喪失や損傷や情報の漏洩を防ぐためには、装置およびその設置に対する物理的な保護が必要となる。

このことを実現するためには、

- 装置の設置場所の適切な選定および適切な保護の実施
- 電源に対する適切なセキュリティ対策の実施
- ケーブル配線に対するセキュリティ対策の実施
- 装置のメンテナンスの適切な実施
- 敷地外に設置された装置に対する適切なセキュリティ対策の実施
- 装置の処分または再使用における安全対策の実施

が必要となる。

7.2.1 装置の設置および保護

装置の盗難や損傷または当該装置に要求されているセキュリティが危うくなることを防止するためには、装置を適切な場所に設置するとともに、適切な保護措置が講じられていなければならない。

(1) 要求事項

- 脅威や危険を軽減する場所への装置の設置
- 脅威や危険を軽減する管理策の設定とその実施

(2) 実施上のポイント

- 設置場所の選定ポイント
  - 機密データののぞき見のリスクを最小限にする場所への設置
  - 特別な保護を必要とするものと一般的な保護で十分なものとの隔離
  - 盗難や災害等の潜在的な危険性の少ない場所への設置
  - 隣接する敷地に生じた災害の影響の少ない場所への設置

・ 情報処理設備付近での飲食･喫煙のポリシーの策定
・ 情報処理設備の運用に悪影響を与える環境状態の監視
・ キーボードカバーの使用など適用工業環境（工場等）における特別な保護

(3) **参考**

- 潜在的な危険性の例
  窃盗、火災、爆発、煙、水漏れまたは水の供給不能、ほこり、振動、化学物質の影響、電源供給の妨害、電磁波

7.2.2 電源

各装置には、電源異常から装置を保護するための対策が講じられていなければならない。

(1) **要求事項**

- 適切な電力量の継続的な供給
- 非常時における電力の遮断

(2) **実施上のポイント**

- 連続的な電力の供給･重要な装置の正常終了または連続運転を支援するための UPS（無停電電源装置）の設置
- 長時間停電時のバックアップ発電機の設置
- 主電源停電時用の照明の配備等の UPS 異常時の対応計画の策定
- 適切な電力量の供給の確保のポイント
  ・ UPS 装置は適切な容量があることを定期的に確認すること
  ・ UPS 装置やバックアップ発電機は,製造業者の指示する方法に従ってテストすること
  ・ 外部通信回線への落雷防護フィルタの設置
- 非常時における電力の遮断についての工夫
  ・ 非常用電源スイッチを非常口付近に設置

7.2.3 ケーブル配線のセキュリティ

通信ケーブルへの細工が攻撃に用いられることを防ぐため、ケーブル配線に対しても適切な安全対策が講じられなければならない。

(1) **要求事項**

- ケーブル配線に対する適切な安全対策の実施

(2) **実施上のポイント**

- ケーブル配線に対する安全確保についての工夫
- アクセスが困難な場所への設置または十分な保護の実施
- 通信ケーブルと電源ケーブルの隔離
- 取扱いに慎重を要するまたは重要なシステムにおける以下の対策の実施
  - 代替経路または伝送路の確保
  - 光ファイバーの使用
  - 装置のケーブル接続部に対する認可されていない装置が接続されていないかどうか等についての定期的な点検の実施

7.2.4 装置の保守

情報処理に用いる装置の可用性と完全性を維持するためには、適切なメンテナンスが実施されなければならない。

(1) **要求事項**

- ベンダーの推奨に沿った適切な整備間隔でのメンテナンスの実施
- メンテナンス担当者以外の装置へのメンテナンスアクセスの禁止
- 発生した異常や障害、予防メンテナンス、修理メンテナンスについての記録の作成と保管
- 装置をメンテナンスのために保護領域外に持出す場合における情報の消去や保険の適用等の適切な安全策の実施

7.2.5 事業敷地外における装置のセキュリティ

組織の敷地外に設置された情報処理に用いる装置は、物理的ならびに論理的な脅威にさらされていると考えなければならない。このため、これらの装置に対しては、特別なセキュリティ対策による保護が講じられなければならない。

(1) **要求事項**

- 装置の敷地外への設置についての責任者の認可の実施
- 敷地内に置く装置と同様のセキュリティの確保
- 敷地外設置に対するリスクアセスメントに立脚した特別な保護措置の適用

(2) **実施上のポイント**

- オフサイト設置装置に求められる配慮

・ 公共の場所に放置しないこと
・ できるだけその存在の隠蔽を図ること

- 当該装置に求められている環境条件の確保
- 外部における作業についての安全ルールの確立とその遵守の指導
- 必要な場合における保険の適用

7.2.6 装置の安全な処分または再使用

不用意な装置の処分は、装置の不正な使用や装置に記憶されている情報へのアクセスによる情報漏れ等の事故につながる危険もある。このため、装置の処分や再使用に対するルールが適切に確立され、装置の処分や再使用はこのルールに沿って行われなければならない。

(1) **要求事項**

- 装置の処分についてのルールの確立とルールに従った処分の実施
- 装置の再使用についてのルールの確立とルールに従った再使用の実施

(2) **実施上のポイント**

- 記録媒体を内蔵している装置の処分についての留意事項
  ・ 確実な上書きの実施等、保護対象情報やライセンスソフトウエアの完全な消去の確認
  ・ 完全な上書きができない場合における完全な破壊の実施

7.3 その他の管理策

オフィス内に置かれた書類やＰＣのスクリーンも組織のセキュリティの脅威になりうる。また、組織の敷地外へのハードウェアや情報の持出しも、管理の対象にならなければならない。

このためには、

- デスクおよびスクリーン周辺におけるセキュリティ対策の実施
- 保護対象資産の移動に対するセキュリティ対策の実施

が必要となる。

7.3.1 クリアデスクおよびクリアスクリーンの個別方針

オフィスにおけるデスク上に置かれた書類やスクリーン上の情報からの、情報の漏洩や情報の改ざんが行われることもある。これらのことを防止するためには、オフィスにおけるデスクの整理やス

クリーンの表示についても、セキュリティの立場から適切なルールが決められ、このルールがオフィスで守られるようにしておかなければならない。

(1) **要求事項**

- 可読状態にある情報の取扱いについてのルールの確立とその適用
- 情報を記録した媒体の取扱いについてのルールの確立とその適用
- 情報処理設備の利用および運用ルールの確立とその適用

(2) **実施上のポイント**

- 規則の策定で考慮するポイント
  - 情報資産の分類
  - 情報資産のリスク
  - 組織の慣習および文化

(3) **参考**

- 取扱い規則での指定事項例
  - 使用しないときは、書類やコンピュータ媒体は施錠したキャビネット等の保管庫に保管すること
  - 必要のないときは,重要な情報は施錠して保管すること
  - 離席時は、パソコン、端末、プリンタに対してキーロックまたはパスワード等によるアクセス防止措置を施すこと
  - 郵便物の置き場所やファックスには盗難防止対策を施すこと
  - コピー機は、勤務時間外は使用不可にすること
  - 重要な情報や機密情報を印刷した時は、プリンタ上に放置しないこと

7.3.2 資産の移動

組織の敷地外でのハードウェアや情報やソフトウェア等の保護対象資産の外部への持出しは制限され、適切に管理されなければならない。

(1) **要求事項**

- 装置や情報資産の認可のない移動の禁止
- 装置や情報資産の持出しや持帰りについての記録の作成と保管
- 保護対象資産の保管状況についての抜打ち検査の実施

8 通信および運用管理

システム運用の不手際が組織の情報セキュリティを危うくすることがないよう、通信ならびにシステム運用については、セキュリティ面からも十分な管理が必要となる。

このために実施すべき施策としては、以下があげられる。

(1) システムの運用要領の確立と運用にかかる責任体制の確立
(2) 運用システムに対する適切なキャパシティマネジメントとシステムの受入れについての適切な管理の実施
(3) 有害プログラムからのシステムの保護
(4) システム運用を円滑にする環境の確保
(5) 適切なネットワーク管理の実施
(6) 取外し可能な媒体に対する適切な管理の実施
(7) 外部との情報やソフトウェアの交換に対する適切な管理の実施

8.1 運用手順および責任

システム運用上の不手際は、業務の混乱やセキュリティ事故につながる。システムの運用に不手際を生じさせないためには、不手際の発生を防止するための工夫が組込まれた運用方式が確立されていなければならない。

このためには、

- システム運用手順書の規定
- 運用環境の変更管理の実施
- 事故処理手順の規定
- 職務の分離
- 開発およびテスト環境と運用環境の分離
- 外部施設利用時のセキュリティに関する契約締結

等の実施が必要となる。

8.1.1 操作手順書

システムの運用に不手際を生じさせないための第一歩は、システムの起動および停止、バックアップの取得、メンテナンスの実施等、システムの運用についての適切なシステム運用手順書が整備されていることである。

(1) **要求事項**

- システム運用手順書の作成･変更要領の確立
- 作成･変更要領に沿ったシステム運用手順書の作成と維持

(2) **実施上のポイント**

- システム運用手順書の作成について
  - ・ システム運用手順書はジョブ毎に作成し、詳細な実施に関する指示を明記する
  - ・ 作成時や変更時における責任者の認可等の取扱い規定の策定

8.1.2 運用変更管理

情報処理施設あるいは設備、システム等の運用環境の変更の不用意な実施は、システムの運用やセキュリティに大きな影響を与える。このため、情報処理施設や設備、あるいはシステム等の変更は、十分な管理のもとで行われるようになっていなければならない。

(1) **要求事項**

- 運用環境変更要領の確立
- 運用環境の管理責任体制の明確化
- 規定された要領に従った運用環境の変更手続きの実施
- 変更履歴の記録と保存

(2) **実施上のポイント**

- 運用環境変更手続きで規定すべき事項
  - ・ 変更実施前の潜在影響の調査と評価
  - ・ 変更実施のための承認手続き
  - ・ 変更の具体的作業手順
  - ・ 変更の詳細内容の全関係者への通知
  - ・ 変更途中での終了或いは好ましくない結果に終わったときの回復手順と責任
- 運用環境の変更を行う場合の留意事項

  OS、ミドルウェアなどの変更とアプリケーションの変更は一体管理を行うこと

(3) **参考**

- 対象となる情報処理施設、設備、およびシステムの変更

  変更管理の対象となる情報処理施設および設備には空調や電力などの設備設置環境から各ハードウェア装置、ネットワーク関連機器まで情報処理に影響を及ぼす可能性のあるものがすべて含まれる。また、システムのオペレーティングシステム（OS）、ミドルウェアなどのオペレーションプログラムからネットワーク機器の OS、アプリケーションや各種パラメータなどの設定値の変更も、管理の対象となる。

8.1.3 事件・事故管理手順

セキュリティ事故発生時に必要な処置が適切に行われるようにするためには、さまざまなセキュリティ事故を想定した事故処理要領が確立されていなければならない。

(1) **要求事項**

- 事故処理についての責任体制の明確化
- 想定される潜在的セキュリティ事故の洗い出し
- 想定される事故に対する処理要領の確立

(2) **実施上のポイント**

- 事故処理要領で明確にすべき事項
  - ・ 事故発生時の原因分析と特定
  - ・ 再発防止策の策定と実施
  - ・ 事故発生時の証跡、証拠の収集
  - ・ 事故発生時の関連者への連絡
  - ・ 事故発生時の関連官庁への処置の報告
  - ・ システムの回復や修正作業のためにシステムやデータにアクセスする者の認証と許可されていない者のアクセスの禁止
  - ・ システムの回復や修正に関し実施した非常措置の記録
  - ・ システムの回復や修正作業の実施にあたっての責任者への報告と事前レビューの実施
  - ・ システムの回復や修正作業終了後の業務やシステムが正常状態に復旧したことの確認、およびセキュリティ対策の完了の確認の実施

8.1.4 職務の分離

システムの運用にかかわる者の過失や故意によるセキュリティ事故の発生をしにくくするためには、スタッフの職務や権限の分離等、職務の割当てにも工夫を行うことが必要である。

(1) **要求事項**

- 職務等の分離
- 分離が難しい場合、活動の監視や証跡の記録、責任者の監督など代替策の実施

(2) **実施上のポイント**

- 職務等の分離のポイント
  - ・ 指示と実行の分離
  - ・ 関連する担当プロセスの分離

・ 特に共謀の可能性がある業務は複数の人間がかかわるなどの特別な管理策の実施
・ セキュリティ監査体制の組織的独立

8.1.5 開発施設および運用施設の分離

開発環境と運用環境の同居は思わぬトラブルをもたらす可能性が高い。開発作業や運用が相互に悪い影響を与えることを避けるためには、開発環境と運用環境がお互いに干渉しないよう分離すべきである。

(1) **要求事項**

- 開発、テスト環境と運用環境の分離

(2) **実施上のポイント**

- 開発、テスト環境と運用環境の情報処理施設や設備の分離
- 開発ソフトウェアの運用への引渡し規則の確立
- 運用環境への開発者のアクセス原則禁止

8.1.6 外部委託による施設管理

外部の施設を利用する場合、施設提供側との間で、利用システムのセキュリティ保持に必要となる施策を確立しておくとともに、これらに関する義務、責任等を施設の使用契約の中で明記しておくことが求められる。

(1) **要求事項**

- 外部施設の使用についてのリスクアセスメントの実施
- 外部施設の使用についてのリスクアセスメントにもとづく適切なセキュリティ対策の確立
- 策定したセキュリティ対策に対する請負業者の同意取得と契約締結

8.2 システムの計画作成および受入れ

システムの運用が、そのキャパシティの問題やシステムの不完全さから混乱しないようにするためには、以下の施策の実施が求められる。

- キャパシティマネジメントの実施
- システムの運用受入れ条件の確立

8.2.1 容量・能力の計画作成

システムの容量不足から、システムの円滑な運用が損なわれないようにするためには、キャパシティマネジメントが適切に行われなければならない。

(1) **要求事項**

- 資源利用状況の監視と将来のキャパシティの予測
- システムに致命的な影響を及ぼす潜在的な隘路の洗出しと対応計画の作成

(2) **実施上のポイント**

- キャパシティマネジメントのポイント
  - 主要なシステム資源の使用状況の監視
  - 使用の傾向、特に業務アプリケーション等と連動したシステム資源使用傾向の把握による予測

8.2.2 システムの受入れ

不完全なシステムが不用意に実運用に供され、業務やシステム運用が混乱したりするのを避けるためには、システムの運用への受入れについての基準が確立され、システムの受入れはこの基準に沿って行われるようにしなければならない。

(1) **要求事項**

- 運用側からの開発システムの受入れに関する要求事項の明確化
- 開発システムの運用への受入れ要領の確立
- 受入れ要領に沿った開発システムの受入れの実施

(2) **実施上のポイント**

- 開発システムの運用への受入れ要領についてのポイント
  - システム運用委託部門、運用部門間での文書に基づく合意
  - 受入れにあたっての、事前テストによるシステムの基準を満たしていることの確認の徹底
- 開発システムの円滑な運用受入れ実現のポイント
  - 新たなシステム開発では開発プロセスの全段階での、操作関係者および当該システムのユーザの（意見の聴取等による）参画

8.3 悪意のあるソフトウェアからの保護

有害プログラムの侵入により、システムや情報が被害を受けないようにするためには、有害プログラムのシステムへの侵入の防止や、侵入の検知、侵入有害プログラムの速やかな除去等の、有害プログラム対策が適切に行われていなければならない。

8.3.1 悪意のあるソフトウェアに対する管理策

有害プログラムにより、システム上の情報やソフトウェアが破壊されたり改ざんされたりするのを防ぐためには、有害プログラムの防止および検出のための施策が確立し、それが適切に実施されていなければならない。

(1) **要求事項**

- ソフトウェア利用ルールの確立
- ウイルス対策用検出･修復ソフトウェアのインストールおよび定期的更新
- 重要なソフトウェアやデータに対する、不審なファイルの存在、改ざんの有無のチェックの定期的な実施
- ウイルス未確認のファイル、メール添付で入手したファイル等のウイルスの可能性のあるファイルの使用前チェック
- ウイルス感染時対策の事前準備
- 有害プログラムに対する最新情報の継続的入手と関係者への通知
- ユーザ意識高揚手順の作成と実施

(2) **実施上のポイント**

- ソフトウェアの利用ルールで規定すべき事項
  - ソフトウェア利用許諾契約に基づく正規の手段以外でのソフトウェアの入手の禁止
  - 外部ネットワーク等からファイルやソフトウェアを入手する場合のルール確立
- ウイルス感染に対して必要な備え
  - システムに対するウイルス対策手順策定と訓練、感染時の報告、回復手順作成と責任の明確化
  - ウイルス感染時に事業継続が行える為の手順の作成と実施

8.4 システムの維持管理

システムにﾄﾗﾌﾞﾙやｾｷｭﾘﾃｨ事故が発生しても、業務の継続に大きな影響が出ることは避けなければならない。このためには、このような場合におけるシステムの回復が迅速かつ的確に行えるようになっていなければならない。このことを実現するためには、日頃から、事故時の処置やシステムの回復に必要となるバックアップや情報が確保されていなければならない。

このためには、

- 情報のバックアップの取得
- オペレータ記録の作成と保管
- 発生事故および事故処理についての記録の作成と保管

が必要となる。

8.4.1 情報のバックアップ

システムにおけるﾄﾗﾌﾞﾙやｾｷｭﾘﾃｨ事故発生時における、情報の復旧や業務の継続のために必要となる重要なビジネス情報およびソフトウェアについては、バックアップ取得が確実に行われ、何時でも回復ができるようになっていなければならない。

(1) 要求事項

- 事業継続計画の要求事項に沿った情報およびソフトウェアのバックアップの取得要件と回復手順の確立
- 指定に従った情報およびソフトウェアのバックアップの定期的な取得と適切な保管
- バックアップから情報やソフトウェアが回復できるのに十分な設備の確保
- 回復機能の定期的な試験と回復処理訓練の実施

(2) 実施上のポイント

- 回復機能の定期的な試験と回復処理訓練の実施について
  - ・ バックアップ媒体に対する定期的な試験の実施
  - ・ バックアップに用いる機能の確認
  - ・ 回復手順の確認と試験
- 重要データの保存について
  - ・ 半永久的保管のアーカイブコピーの要求事項決定
  - ・ 回復手順の定期的なチェックの実施

8.4.2 運用の記録

問題が生じた場合における調査や、不適切なシステムのオペレーションを発見するためのシステム運用についての事後チェックのため、システムの運用における各種のオペレーションは、適切に記録され、その記録は適切に保管されていなければならない。

(1) **要求事項**

- 運用の記録についてのルールの確立と、ルールに沿った作成と保管
- 運用記録によるシステム運用についての第三者チェックの定期的な実施

(2) **実施上のポイント**

- 運用の記録についてのルールで規定すべき事項
  - 記載事項
  - 保管方法

8.4.3 障害記録

発生したセキュリティ事故に対する処理については、報告ならびに記録の作成とその保管が適切に行われなければならない。

(1) **要求事項**

- 事故処理報告ならびにその取扱い要領の確立
- ルールに沿った事故処理記録の作成と保管
- 報告された事故処理に対するレビューの実施

(2) **実施上のポイント**

- 事故処理に対するレビューのポイント
  - 処置が適切に完了したことの確認
  - 実施された処置が妥当なものであったことの確認、および正しい手順で行われたことの確認等の、実施した事故処理の妥当性の確認

8.5 ネットワークの管理

ネットワークに起因するセキュリティにかかわるトラブルを未然に防止するためには、ネットワークの使用について適切な管理がなされていなければならない。

8.5.1 ネットワーク管理策

ネットワークを介したシステムへのアクセスやデータの交換におけるセキュリティリスクを排除するためには、ネットワークの使用に対する適切なセキュリティ対策が確立され、これが適切に実施されていなければならない。

(1) **要求事項**

- ネットワークの運用責任とコンピュータ操作の分離
- オープンなネットワークを使用する通信のリスク対策
- データの機密性および完全性の確保
- 許可されていないアクセスからのシステムの保護
- リモート機器の管理責任の明確化、安全管理手順の確立

(2) **実施上のポイント**

- ネットワーク管理における保護の対象
  - ・ ネットワークを流れるデータ
  - ・ ネットワークに接続されている機器（リモートを含む）
  - ・ ネットワークに接続されているシステム

8.6 媒体の取扱いおよびセキュリティ

情報を記録したディスク、カセット等の媒体や、業務にかかわる文書やシステムドキュメンテーション等の印刷物のずさんな取扱いも、情報の漏洩や改ざんにつながる。このため、媒体や印刷物についても、その取扱いは適切に管理されなければならない。

このためには、

- 取外し可能なコンピュータ媒体に対する適切な保護管理の実施
- 媒体の処分の適切な実施
- 情報の取扱いに関するルールの確立と、ルールに沿った情報の取扱いの実施
- システムドキュメンテーションに対する適切な保護管理の実施

が必要となる。

8.6.1 コンピュータの取外し可能な付属媒体の管理

取外し可能なコンピュータ媒体や印刷物の不用意な取扱いがないようにするためには、取外し可能なコンピュータ媒体（印刷物も含む）についての管理ルールを確立し、これらに対するルール

に沿った取扱いが行われるようになっていなければならない。

(1) **要求事項**

- 取外し可能なコンピュータ媒体の管理ルールの作成と、ルールに沿った管理の実施

(2) **実施上のポイント**

- 取外し可能なコンピュータ媒体の取扱いルールで規定すべき事項
  - 廃棄時の内容消去
  - 外部持出し時の認可と記録の取得
  - 製造業者の仕様に従った安全な保管

8.6.2 媒体の処分

情報やソフトウェアが記録された媒体の不用意な処分は、媒体上の情報やソフトウェアの漏洩につながる。このため、媒体処分についてのルールの確立と、ルールに沿った媒体の処分がなされなければならない。

(1) **要求事項**

- 媒体の処分に関するルールの作成と実施
- ルールに従った媒体処分の実施
- 処分記録の作成と保管の実施

(2) **実施上のポイント**

- 重要情報が含まれている媒体に対する完全な処分の徹底
- 管理対象の漏れのない洗い出し
- 委託処分の場合、適切な業者の選択と適切な監督、指導の実施

8.6.3 情報の取扱い手順

情報の保護を実現するためには、保護対象の情報の個々に対して、取扱いルールを確立するとともに、それぞれに対し定められたルールに沿った取扱いが行われるようになっていなければならない。

(1) **要求事項**

- 保護管理対象の洗出しと、それぞれに対する取扱いルールの確立

(2) **実施上のポイント**

- 取扱いルールで規定すべき事項
  - 保護管理対象に対するアクセス制限の実施
  - データの引渡し記録の作成と保管の実施（データ保有者の把握）
  - 入力データの完全性のチェックと、処理および出力の妥当性の確認の実施
  - 出力待ちスプーリングデータに対する適切な保護の実施
  - 記録媒体の適切な保管環境での保管
  - 配布先の限定－必要最小限の配布
  - コピーしたデータに対するコピーであることの表示
  - 定期的な情報保有者の確認の実施

8.6.4 システムに関する文書のセキュリティ

システムドキュメンテーションは、攻撃者に対して攻撃の手掛かりを与えるものともなるので、適切な保護管理がなされなければならない。

(1) **要求事項**

- システムドキュメンテーションに対する厳格な保護管理の実施

(2) **実施上のポイント**

- アクセス権利者の制限の実施
- オープンなネットワークに対する十分な保護対策の実施
- オープンなネットワーク経由での授受に対する十分な保護管理対策の実施

8.7 情報およびソフトウェアの交換

組織間での情報やソフトウェアの交換にも、その喪失、漏洩、改ざん、破壊等の脅威がある。組織間での情報やソフトウェアの交換における安全を確保するためには、これらの交換についての適切な保護が行われなければならない。

このためには、

- 情報やソフトウェアの交換に対する責任や手順等の取決めの確立
- 物理的手段による引渡し、電子取引における情報の交換、電子メールによる情報の交換、電子オフィスシステムでの情報の交換、Webを用いた情報の交換、および音声、ファクシミリ、ビデオ通信等の交換手段ごとの保護対策の実施

が必要となる。

8.7.1 情報およびソフトウェア交換契約

外部の組織と情報やソフトウェアの交換を行う場合、交換される情報やソフトウェアの保護を確実にするため、交換相手との間で、これらの保護のための必要な手段や、情報等の授受の方法や保護の責任分担等について合意を確立しておかなければならない。

(1) **要求事項**

- 情報等の保護を目的とした情報等の交換に関する取決めの確立と合意

(2) **実施上のポイント**

- 情報やソフトウェアの交換についての取決めで明示すべき事項

  情報やソフトウェアの交換についての取決めで明示すべき事項としては、以下があげられる。

  ・ 情報等の発信および受領の責任者の管理責任
  ・ 情報等の引渡し手順
  ・ 情報等の梱包あるいは発信形状の最低限の技術規格
  ・ 宅配業者等を利用する場合の身分確認方法
  ・ 情報等の紛失時の責任
  ・ 機密度等により取扱いの異なる情報が判別できる仕組み
  ・ 情報およびソフトウェアの所有権、データの保護責任、ソフトウェアの著作権等の関連法規についての留意事項
  ・ 情報およびソフトウェアの利用環境および特別な留意事項

8.7.2 配送中の媒体のセキュリティ

情報等の授受に物理的手段を用いる場合においても、必要な保護が講じられなければならない。

(1) **要求事項**

- 信頼できるチャネル（宅配業者、運送業者等）の利用
- 使用する業者の指定に従った十分な梱包
- 必要な場合における特別な保護策の実施

(2) **実施上のポイント**

- 運搬物に対する特別な保護の事例
  ・ 施錠されたコンテナの使用
  ・ 手作業による運搬

・ 不正残跡包装の利用
・ 異なるルートを用いた分割配送の適用
・ コンテンツの暗号化の適用
・ デジタル署名の適用

8.7.3 電子商取引のセキュリティ

電子商取引を行う場合、対応システムには、システムのセキュリティ上の問題から商取引におけるトラブルが生じないようにするためのさまざまな対策が組込まれていなければならない。

(1) **要求事項**

- 電子商取引対応システムへの必要なセキュリティ対策の組込み

(2) **実施上のポイント**

- 電子商取引対応システムにおけるセキュリティ要求事項
  - ・ 取引の当事者間での取引相手の確認
  - ・ 取引相手の権限の確認
  - ・ 適切な取引手続きの設定、取引内容や契約の保証
  - ・ 購入者の信用審査
  - ・ 適切な決済手段の提供
  - ・ 注文情報の保護
  - ・ 詐欺等のトラブルについての責任の所在の明確化
  - ・ 取引当事者間での合意書の作成
  - ・ 法的要求事項への対応

8.7.4 電子メールのセキュリティ

電子メールで交換される情報の保護や、電子メールの使用がサイトのセキュリティの脅威にならないようにするためには、電子メールの使用についても適切なセキュリティ対策が講じられなければならない。このためには、ビジネスで使用する電子メールの利用ポリシーを定めるとともに、必要な管理が行われなければならない。

(1) **要求事項**

- 電子メールの使用についてのセキュリティポリシーの確立
- 電子メールの使用についてのセキュリティポリシーに沿った電子メールの使用

(2) **実施上のポイント**

- 電子メール利用にかかるセキュリティポリシーで規定すべき事項
  - 盗聴等の電子メールにかかる脅威への対策
  - 電子メールを使うべきでない時についてのガイドライン
  - 会社の信用を傷つけないための従業員の責任(中傷メールの送付、いやがらせメールの送付など)
  - 暗号手法の利用
  - 訴訟等で証拠として必要となるメッセージの保存
  - 発信者のわからないメッセージに対する対策

(3) **参考**

- 電子メール使用にかかる脅威
  - メッセージの第三者によるアクセスや改ざん
  - メールサービスの利用不能
  - 誤りの起き易さ(宛先不正や一般的な電子メールシステムの信頼性)
  - 電子メールをビジネスプロセスに利用する時のビジネス慣行の変更
  - 将来の紛争や訴訟等を考慮した出所、発信、配信、受信等の証拠の確保
  - スタッフのメールアドレスの外部への公開による危険性
  - メールサーバへの遠隔からのアクセスに起因する危険性

8.7.5 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では、組織の重要な情報が多く扱われている。これらの情報の保護や、電子オフィスシステムのセキュリティの破綻が、他のシステムに悪い影響を与えないようにするためには、電子オフィスシステムについても適切なセキュリティ対策が講じられなければならない。このためには、電子オフィスシステムの利用によるビジネスおよびセキュリティのリスクを抑制するためのポリシーやガイドラインが確立されていなければならない。

(1) **要求事項**

- 電子オフィスシステム利用についてのセキュリティポリシーの確立
- セキュリティ面からの電子オフィスシステム利用ガイドラインの作成

(2) **実施上のポイント**

- 対象となる電子オフィスシステムの範囲
  - 文書、コンピュータ、モバイルコンピューティング、移動通信、メール、音声メール、一般音声通信、マルチメディア、郵便サービス／施設、ファクシミリ等の利用
- 電子オフィスシステムの利用に関するセキュリティポリシーおよび利用ガイドラインで明確に

すべき事項

- 情報に対する脅威への対策
- 情報共有（電子掲示板等）の使用管理策
- システム上セキュリティが保たれない情報のシステムでの取り扱い禁止
- 機密保持が必要な個人のスケジュール情報等へのアクセス制限
- 通信順序や認可などビジネスアプリケーションに対するシステムの適合性等
- システム使用許可者およびアクセス可能な場所の明確化
- 特定設備を扱う利用者の制限
- 利用者の身分を明示
- システムに保持されている情報の保存およびバックアップ
- フォールバックの要求事項および取決め事項

8.7.6 公開されているシステム

Web 等外部に公開しているシステムへのアクセスに対しては、一般にユーザの認証が行われないため、さまざまな攻撃の対象となることが考えられる。このため、これらのシステムにおいては、攻撃を簡単に許さないためのセキュリティ対策が講じられていなければならない。

(1) **要求事項**

- Web 等外部に公開しているシステムの情報の保全、および改ざん防止策の実施
- 外部公開システムの情報に関する法規制対策の実施、公開前の内部認可プロセスの設定
- 高い保全性が要求される情報に対するデジタル署名の適用等の適切な保護対策の実施
- 外部公開システムにおける保護対策の実施

(2) **実施上のポイント**

- 個人情報保護法に従った情報の入手
- 外部公開システムに入力される情報の確実な処理
- 重要な情報の収集中や保管時における保護対策
- 外部公開システムのアクセスを利用した他システムへの意図的なアクセスの排除

8.7.7 交換情報のその他の形式

音声、ファクシミリ、ビデオ通信設備を用いた通信に対しても、必要な場合、適切なセキュリティ対策が講じられなければならない。これらの情報交換手段の使用についても、組織のセキュリティを守るための利用ポリシーを確立し、このポリシーの沿った使用が行われなければならない。

(1) **要求事項**

- 音声、ファクシミリ、ビデオ通信設備利用についての利用ポリシーの確立

(2) **実施上のポイント**

- ポリシー作成のポイント
  - 情報漏洩などへ注意
    - －電話などでの盗み聞きへの注意
    - －盗聴器等への対策
    - －情報が漏れやすい場所での会議など
- 留守番電話などメッセージ保存型システムでの第三者による故意、過失の情報漏洩対策
- ファクシミリ利用時の留意事項
  - ファクシミリ装置から許可されていないものの情報取り出し対策
  - 特定の番号にメッセージが故意・過失により送られるプログラミング
  - 番号誤りによる文書の誤配

9 アクセス制御

システムへの不正なアクセスを防止するためには、適切なアクセス制御ポリシーに基づく、ネットワークレベルでのアクセス制限、オペレーティングシステムレベルでのアクセス制限、アプリケーションレベルでのアクセス制限が適切に行われなければならない。また、これらのアクセス制限が指定通りに機能するためには、アクセス権やパスワードについても厳格な保護管理が必要となる。

これらを実現するためには、

(1) アクセス制御に関するビジネス要求事項の明確化

(2) ユーザアクセスに対する適切な管理の実施

(3) ユーザの責任についての適切な指導の実施

(4) 適切なネットワークアクセス制御の実施

(5) 適切なオペレーティングシステムへのアクセス制御の実施

(6) 適切なアプリケーションへのアクセス制御の実施

(7) システムへのアクセスおよびシステムの使用についての監視の実施

(8) モバイルコンピューティングおよびテレワーキングに対する適切なセキュリティ対策の実施

が必要となる。

9.1 アクセス制御に関する業務上の要求事項

システムへの不正なアクセスを防ぐための諸施策が適切に講じられるようにするためには、システムへのアクセスについてのビジネス面からの制御についての要求が明確にされてなければならない。

9.1.1 アクセス制御方針

アクセス制御ポリシーは、システムへのアクセスについてのビジネス面からの制約要件を定義するものであり、システムにおけるアクセス制御の基盤となるものである。

(1) 要求事項

- 業務単位での当該ビジネスに対するアクセス制御要件の確立
  - 業務単位に以下を実施

(2) 実施上のポイント

- 個別業務単位に定義するアクセス制御要件で定義すべき事項
  - 当該業務におけるセキュリティ要求事項

・ 使用されるすべての情報
・ 各情報に対する許される開示の範囲および指定する保護レベル
・ 当該業務の運営に関わるシステムおよびネットワーク相互間におけるアクセス制御ならびに情報保護の整合性についての要求
・ データまたはサービスへのアクセスの保護に関する関連法規ならびに契約上の義務
・ 当該業務をサポートするシステムに対するすべてのアクセスに対するアクセス権の管理

- アクセス制御規則の定義についての工夫
  ・ 無条件遵守事項と選択的あるいは条件付事項の区別の明示
  ・ 禁止事項の明確化（参考参照）
- 特に厳格なアクセス制限規則の検討が必要な事項
  ・ 期間の経過による変更等の予め決められたルールに沿ってプログラム的に行われる情報保護クラスの変更
  ・ ユーザの判断によって開始される情報保護クラスの変更
- 管理者またはその他の承認が必要になる規則と、そのような承認が必要でない規則の切分け

(3) 参考

禁止事項があいまいにならないようにするためには、禁止事項は明確に表現されなければならない。“明確に禁止されない限り、あらゆる事柄が一般的に許される”は、好ましくない表現方法であり、このような場合は、“明確に許されない限り、一般的に＊＊＊＊は禁止される”といった表現にすべきである。

9.2 利用者のアクセス管理

多くのユーザが使用するシステムについては、正当なユーザ以外のユーザのアクセスを防止するとともに、登録したユーザに対するアクセス権の適切な付与等、適切なユーザ管理が行われなければならない。

このためには、

- ユーザ登録の適切な実施
- 適切な特権管理の実施
- 適切なパスワード管理の実施
- ユーザに割当てたアクセス権についての見直しの実施

が必要となる。

9.2.1 利用者登録

ユーザのアクセス管理を適切に行うためには、ユーザの登録とその管理が適切に行われなければならない。

(1) **要求事項**

- 登録、取消し等のユーザ管理にかかる諸手続き等を定めたユーザ管理要領の確立
- ユーザ管理要領に基づくユーザ管理の実施
- ユーザ登録をベースとしたアクセス制御の実施
- スタッフまたはサービス業者による認可されていないアクセスの試みに対する牽制策の準備

(2) **実施上のポイント**

- ユーザ管理要領で規定すべき事項
  - 各ユーザまたはユーザグループへの ID の付与とその手順
  - 登録ユーザの対象システムへのアクセス権の保持の確認
  - 登録ユーザに認可されているアクセスのレベルに対する、業務目的ならびに組織のセキュリティポリシーとの整合性の確認
  - ユーザへの認可したアクセス権の通知
  - ユーザのアクセス条件の受入れについての確認書の入手
  - 業務からのアクセス認可手順完了前のサービスの提供の抑止等のサービス提供者における個別ユーザへのサービス提供開始手順
  - 登録ユーザに関する情報の台帳等への記録
  - ユーザ ID およびアカウントの重複発行のチェックの実施
  - ユーザグループへの ID の付与の制限の実施

9.2.2 特権管理

特権の不正な使用は、システムのセキュリティに重大な脅威となる。不用意な特権の付与や使用を防止するためには、システムへのアクセスにかかる特権の割当て、および使用に関しては、特に厳格な管理が行われなければならない。

(1) **要求事項**

- 認可基準や認可手続き等を定めた特権の割当てに関する認可要領の確立
- 特権の割当ての制限と手順に従った認可の実施
- 特権の使用についての制限の実施

- 特権の割当て状況についての管理の実施

(2) **実施上のポイント**

- 特権付与手順として明確にすべき事項
  - ・ 特権付与の対象
  - ・ 各特権が割当てられる必要のあるスタッフまたはスタッフグループの特定
- 特権の付与にあたっての留意事項
  - ・ 個人に対する特権付与の制限
    - －必要性の確認
    - －必要性に裏付けられた使用場面（イベント）の制限
    - －使用できる機能の制限（必要最小限の機能に限定）
  - ・ 同一人であっても、特権を付与するユーザ ID とビジネス用途に用いるユーザ ID の分離
- システムユーティリティやコマンド等の活用による特権付与の必要性の極小化
- 特権の割当て管理についての工夫
  - ・ 特権の付与状況についての台帳の作成と維持
  - ・ 特権の付与プロセスについての記録

9.2.3 利用者のパスワードの管理

システムへの不正なアクセスを防止するための要であるユーザパスワードが破られないようにするためには、ユーザが用いるパスワードについての適切な管理が行われるための仕組みの確立とルールに沿ったパスワード管理の実践が必要となる。

(1) **要求事項**

- パスワードの設定基準、パスワードの付与手順を定めたパスワード管理要領の確立
- 設定基準の沿ったパスワード割当ての実施
- パスワードに対する適切な保護の実行の推進

(2) **実施上のポイント**

- パスワードの管理についての工夫
  - ・ パスワードの付与にあたっての使用者からのパスワードの秘密保護について合意書の交換
  - ・ 暫定パスワードの安全な手段での交付（クリアテキストの電子メールは避ける）
  - ・ アクセス制限の組込みや暗号化等のパスワードのＰＣ上での格納にあたっての適切な保護策の実施
  - ・ ユーザの身分･真正性確認のために、指紋確認･署名確認･チップカード等も検討
- ユーザに対する暫定パスワードの本パスワードへの速やかな切替えの指導
- ユーザ身分確認前の暫定パスワード交付の禁止

9.2.4 利用者のアクセス権の見直し

業務の変更やシステムの利用者の変更等を考えると、ユーザに与えたアクセス権は永久的なものでなく、これらの変更に伴い必要な修正がなされなければならない。このような処置の漏れが、システムのセキュリティを危うくしないようにするためには、付与しているさまざまなアクセス権に対する定期的なチェックも必要である。

(1) **要求事項**

- ユーザのアクセス権の定期的な見直し
- ユーザのアクセス権変更後のレビューの実施

(2) **実施上のポイント**

- 付与した特権的アクセス権についての最低3ヶ月を目処とした高い頻度での見直しの実施
- 一般のアクセス権についても、最低6ヶ月ごとの見直しの実施

9.3 利用者の責任

ユーザにも、与えられたパスワードの保護等に努め自分に与えられたアクセス権がシステムへの不正なアクセスに用いられないようにする責任がある。

このためには、

- パスワードの使用についてのユーザの指導
- PC 等のシステムへのアクセス装置の放置の防止

が必要となる。

9.3.1 パスワードの使用

システムへのアクセスにおいてアクセス者の認証に用いられるパスワードが破られないようにするためには、ユーザ側においてもパスワードの設定やその使用について十分な注意が払われるよう、ユーザに対するパスワードの使用についての指導が必要となる。

(1) **要求事項**

- パスワードの設定基準の確立
- パスワード管理要領の確立
- 設定基準に沿った適切なパスワードの設定の実施
- パスワード管理要領に沿ったパスワードの保護管理の実施

- マクロ･キーまたはファンクション･キー等に記憶される自動ログオンプロセスへのパスワードの組込みの禁止

(2) **実施上のポイント**

- パスワードについてのメモ作成の禁止
- 適切なパスワードの原則
  - 6 文字長以上
  - 名前･電話番号･誕生日等、他人が容易に推測できるものに基づかないもの
- 暫定パスワードの使用制限―本パスワードへの早期切替え
  （暫定パスワードは最初のログオンで本パスワードに変えるようにすること）
- 複数の人に同一のパスワードを与えるパスワードの共有の制限
- 必要に応じたシングルサインオンの使用
- パスワードの変更サイクルの決め方
  - アクセス回数
  - 使用期間

9.3.2 利用者領域にある無人運転の装置

PC 等の端末装置の放置は、システムへの不正なアクセスの道具として、また情報の不正取得に用いられる危険性がある。このため、PC 等の端末装置が、第三者に操作されたり情報が見られたりする可能性がある環境で稼動状態のまま無人状態にならないようにするための施策も必要となる。

(1) **要求事項**

- システムと接続状態にある PC 等の装置に対するセキュリティ要求事項の明確化
- システムと接続状態にある PC 等の装置保護についてのサイト運営関係者への徹底

(2) **実施上のポイント**

- PC等の装置を無人状態におく場合における一般的な処置
  - パスワード保護のあるスクリーンセーバは除き、処理の終了にともなうセッション切断の励行
  - メインフレームの場合は、セッションが終了時のログオフの励行

9.4 ネットワークのアクセス制御

システムへの不正なアクセスの防止の第一歩は、外部と内部との間の通信を適切に制限することにある。

このことを実現するためには、

- ネットワークサービスの使用についてのポリシーの確立
- ユーザからネットワークサービスまでの接続経路の制限
- 外部からのアクセス者についての適切な認証の実施
- 外部ネットワーク経由でのコンピュータ間通信における相手システムに対する適切な認証の実施
- 遠隔診断ポートに対する適切な保護の実施
- ネットワークの分離によるセキュリティ対策の分割
- 個々のネットワークアクセスに対する接続制御の実施
- 個々のネットワークアクセスに対する接続経路の実施
- 使用するネットワークサービスのセキュリティ特性に応じたセキュリティ対策の実施

9.4.1 ネットワークサービスの使用についての個別方針

外部のネットワークとの不用意な接続は、システムのセキュリティを危険にさらす。このため、外部のネットワークとの接続については適切な制限と管理が必要となる。外部のネットワークとの接続を適切なものにするためには、ネットワーク接続制御前提となるシステムの外部ネットワークサービスへのアクセスや、他社または外部に置かれた自社システム等との接続等、ネットワークとの接続についてのポリシーが確立されていなければならない。

(1) **要求事項**

- ネットワーク接続ポリシーの確立

(2) **実施上のポイント**

- ネットワーク接続ポリシーで規定すべきこと
  - アクセスすることが許されるネットワークおよびネットワークサービス
  - ネットワークおよびネットワークサービスへのアクセスの認可手順
  - アクセスを保護するための管理策と管理手順
- 対象となる接続
  - 外部のネットワークサービス
  - 業務上の必要でネットワーク接続するユーザ
  - 外部に置かれる自社システム端末

9.4.2 指定された接続経路

外部システムと内部システム間の接続に対する経路についての制限を行い、不正な接続の試みが成功するチャンスを少なくするようにすることも、不正な接続を防止するための工夫の一つである。

(1) **要求事項**

- 接続要求元から接続先までの経路についての管理の実施

(2) **実施上のポイント**

- 検討の対象となる経路制限の方法
  - 専用のラインまたは電話番号の割当て
  - 指定されたアプリケーションまたはセキュリティゲートウェイへの自動接続
  - ユーザ毎に認可するメニューやサブメニューオプションなどのきめ細かい制限
  - 無制限のネットワークサーフィンの禁止
  - 指定されたアプリケーションまたは外部ネットワークユーザ用のセキュリティゲートウェイの使用を強制
  - セキュリティゲートウェイ（ファイアウォール等）を用いた外部からのアクセスに対する積極的な制御の実施
  - 内部ネットワークのセグメント化による内部システムへのネットワークアクセスの制限

9.4.3 外部から接続する利用者の認証

特別の場合を除き、外部との通信のすべてに対し接続対象サービスの保護レベルに応じた適切な相手認証を行わなければならない。

(1) **要求事項**

- 適切な認証方式の選択
- 適用する認証手順および認証についてのテスト等によるその有効性の確認の実施
- 認証が必要な場面に対する指定された認証の適用

(2) **実施上のポイント**

- 必要に応じたダイアルバックモデムを用いた認証の適用の検討
- 呼出しを含むネットワークサービスの使用の排除
- 必要な場合における接続の確実な切断

9.4.4 ノードの認証

ネットワークを介したシステム間接続に対しては、接続先のノードの真正性の確認等による適切な認証を行わなければならない。

(1) **要求事項**

- サービスの保護レベルに応じたノードに対する適切な認証の実施

(2) **実施上のポイント**

- ノードに対する適切な認証についての検討事項
  - 適切な認証方式の選択
  - 適用する認証手順およびアクセス制御についてのテスト等による有効性の確認の実施
  - 必要な場面における指定された認証の適用

9.4.5 遠隔診断用ポートの保護

診断ポートは、システムへの不正なアクセスを試みる者に侵入の手がかりに用いられることが多い。このため、診断ポートへのアクセスに対しては、適切な保護が必要であり、診断ポートに対する適切なアクセス制限の仕組みの確立は欠かせない。

(1) **要求事項**

- 遠隔診断ポートについてのアクセス制限ポリシーの確立
- 遠隔診断ポートに対する適切なセキュリティ機構の使用
- 遠隔診断ポートへのアクセスについての厳格な手順の確立とその運用

9.4.6 ネットワークの領域分割

きめの細かいネットワークアクセス制御と不正アクセスの影響の極小化ができるよう、内部ネットワークについても適切なセグメント化を検討することが必要である。

(1) **要求事項**

- 内部ネットワークの適切なセグメント化
- セグメントごとのセキュリティポリシーの確立

9.4.7 ネットワークの接続制御

個々のネットワークとの接続要求に対しては、接続対象ビジネスごとに指定されたネットワークアクセス制御ポリシーに沿った適切な接続制御が行われなければならない。

(1) **要求事項**

- 対象ビジネスに指定されたネットワークアクセス制御ポリシーに沿った適切な接続制御の実施
- 適用される接続制限の維持

(2) **実施上のポイント**

- 個々のビジネスアプリケーションのアクセスポリシーおよびセキュリティ要求事項の反映

(3) **参考**

- 接続制限の適用対象となるアプリケーションの例
  - 電子メール
  - 単方向ならびに双方向のファイル転送
  - 対話式アクセス
  - 時刻または期日にリンクしたネットワークアクセス

9.4.8 ネットワーク経路を指定した制御

外部ネットワークからのアクセスは、接続先までの経路の指定が行われていなければならない。

(1) **要求事項**

- ネットワークからの内部のサービスへの個々のアクセスに対する必要に応じた適切な経路制御の実施

(2) **実施上のポイント**

- 送信元と接続先のアドレスとその組合せについてのチェック
- 必要に応じたネットワークアドレス変換機構の使用
- 使用機能の強度の評価に基づく確実な実施

9.4.9 ネットワークサービスのセキュリティ

使用するネットワークサービスのセキュリティ特性は、セキュリティ対策へ反映されなければならない。

(1) **要求事項**

- 使用するネットワークサービスのセキュリティ特性の正確な把握
- そのセキュリティ特性のセキュリティ対策への適切な反映

9.5 オペレーティングシステムのアクセス制御

システムへの不正アクセスに対する論理的なバリアの一つであるオペレーティングシステムレベルでのアクセス制限も適切に機能するようになっていなければならない。

このためには、以下の施策の実施が必要となる。

- アクセス可能端末の制限
- セキュアなログオンプロセスの確立
- システムにアクセスする者に対する適切な識別と認証の実施
- システムにアクセスするために用いられるパスワードに対する適切な管理の実施
- システムユーティリティの使用に対する適切な管理の実施
- 必要に応じたユーザを安全防護するための脅迫警報の適用
- 端末に対するタイムアウト機能の組込み
- システムへの接続時間の制限の実施

9.5.1 自動の端末識別

システムへのアクセスの受付けにおいて、端末（アクセス機器）固有の ID を、アクセスする者の認証の一部に用いることも、場合によっては必要となる。

(1) **要求事項**

- 必要な場合における、システムにアクセスする端末等の機器に対する機器固有の ID 等を用いた認証の実施
- 機器固有の ID に対する改ざんの防止等の保護の実施

9.5.2 端末のログオン手順

ログオンプロセスの設計にあたっては、ログオンプロセスが、システムに対し不正なアクセスを試みる者に、結果として、不正なログオンを成功させることをガイドするようなことがないようにしなければならない。

(1) **要求事項**

- ログオンプロセスにおける不正なログオンを試みる者に対する便宜の提供になる機能の排除
- ログオンプロセスへの不正なログオンの試みに対する牽制の組込み

(2) **実施上のポイント**

- ログオンプロセスをセキュアなものにするための工夫

・ ログオンに用いる情報の隠蔽
・ ログオンの成功を誘導するようなプロセスの組込みの禁止
・ ログオン完了前におけるアクセス対象のシステムまたはアプリケーションの表示の禁止
・ 入力に対する段階的なチェック方式に代え、全項目入力終了後の一括チェック方式の選択等、ログオン情報の妥当性チェックのタイミングの適切な設定

- 不正ログオンを試みる者に対する牽制方法の例
  ・ ログオンプロセスの初期段階における、不正アクセスに対する一般的な警告の表示
- 不審なログオンの試みに対する警戒処置
  ・ ログオンの試みの失敗に対する適切な処置の組込み
  ・ ログオンに所定の時間以上を要した場合におけるログオンの拒否等による、ログオンプロセスの所要時間の制限
  ・ ログオン成功時に以下に示すような情報の表示を行い、正当なアクセス者に、当該アクセス者を名乗った不審なアクセスのチェックができるようにする機能の組込み
  －前回のログオンが正常に行われた日時
  －前回のログオン以降の失敗したログオンについての情報

(3) **参考**

- 制限回数以上の失敗をしたログオンの試みに対する実施すべき処置の例
  ・ 失敗した試みについての記録
  ・ 更なる試みに対する牽制
  ・ データリンク（セッション）の切断

9.5.3 利用者の識別および認証

システムへの不正なアクセスを防ぐためには、システムへアクセスする者に対する識別と認証が適切に行われなければならない。

(1) **要求事項**

- 共用ユーザ ID の使用が許される特別な場合を除いた、システムへアクセスする者に対する識別の実施
- システムへアクセスする者に対する適切な認証の実施

(2) **実施上のポイント**

- システムへのアクセス者に対する認証についてのポイント
  ・ 別途に許される場合を除き、同一ユーザ ID の複数人への付与の禁止
  ・ 共用ユーザ ID の付与の制限と適切な管理の実施
  －必要な場合に限定

－共用ユーザ ID 付与について責任者の認可制の採用
－割当て状況ならびに使用状況についての適切な管理の実施
・ 場面場面に応じた適切な認証方式（技術）の採用
・ ユーザ ID の中に付与された特権レベルを示すような文字の挿入の禁止

(3) **参考**

- 認証方式の選択肢
  - ・ パスワード
  - ・ メモリトークンやスマートカード等の物理的ツール
  - ・ 公開鍵証明書
  - ・ 生体認証技術

9.5.4 パスワード管理システム

システムセキュリティの要でもあるパスワードが破られないようにするためには、システムにアクセスするために用いられるパスワードに対し適切な管理が必要で、このためには、パスワードの管理に関する適切な仕組みの確立が必要となる。

(1) **要求事項**

- 有効なパスワードの設定の指導
- パスワード登録プロセスにおけるパスワードの保護
- パスワードの有効性の維持
- パスワードのセキュアな保管の実施
- 暫定パスワードの本パスワードへの早期切替え

(2) **実施上のポイント**

- 有効なパスワード設定の指導
  - ・ 共用パスワードの使用の制限
  （原則として一人一人に固有のパスワードを付与）
  - ・ 有効なパスワード選択の強要パスワード登録プロセスにおけるパスワードの保護
  - ・ 登録者自身による登録と、登録プロセス中における本人による設定の確認
  （パスワードの登録プロセスにおける他人の介在の排除）
- パスワードの有効性の維持
  - ・ 定期的な更新の実施
  - ・ 一定期間内におけるパスワードの再使用の禁止
- パスワードのセキュアな保管の実施
  - ・ 入力パスワードのスクリーン表示の禁止

・ パスワード管理ファイルのアプリケーションデータからの隔離
・ パスワード管理ファイルの（一方向アルゴリズム等を用いた）暗号化の検討

- 暫定パスワードの本パスワードへの早期切替え
  ・ インストール時におけるベンダー設定のデフォルトパスワードの変更
  ・ パスワード設定プロセスにアクセスするための暫定パスワードの用済み後の廃棄

9.5.5 システムユーティリティの使用

システムユーティリティはセキュリティの管理にかかわる機能を提供しているものが多い。このため、システムユーティリティの使用については適切な管理がなされなければならない。

(1) **要求事項**

- システムユーティリティの使用の制限
- システムユーティリティ使用時の適切なユーザ認証の実施
- システムユーティリティのアプリケーションからの分離
- 不要な（使用しない）ユーティリティのシステムからの除去
- システムユーティリティの使用についての記録の作成と保管

(2) **実施上のポイント**

- システムユーティリティ認可レベルの確立
- システムユーティリティの使用制限の方法
  ・ 使用目的の制限
  ・ 使用権限者の制限
  ・ 使用条件の制限

9.5.6 ユーザを保護するための脅迫に対する警報

正規のユーザが脅迫されてシステムにアクセスし自分の意図と異なる操作を強いられることも考えられる。このような危険を配慮しなければならないシステムにおいては、このようなケースにおいて、その操作が脅迫によるものであることをシステムの管理者に知らせる機能をシステムに組込むことも検討の対象となる。

(注) 脅迫警報とは、システムへのアクセスを何者かに脅迫されて行わされているような場合において、入力の中にそのことを伝えるメッセージを付加したものを指す。我国ではなじみはないが、本基準の発祥国である英国では、多くのシステムで検討の対象となる機能となっている。

(1) **要求事項**

- 脅迫警報組込みの要否の検討
- 脅迫警報を適用する場合における警報時の対処要領の明確化

(2) **実施上のポイント**

- 脅迫警報に対する対処要領で指定すべき事項
  - 応答の要否
  - 応答の手順

9.5.7 端末のタイムアウト機能

端末から長時間アクセスがない場合、稼動状態のまま放置されていることも考えられる。正当なアクセス者以外が、放置された端末を用いてシステムにアクセスすることを防ぐためには、端末にタイムアウト機能を組込むのも一つの工夫である。

(1) **要求事項**

- 端末に対する必要に応じたタイムアウト機能（一定時間活動がない場合における接続の遮断等）の組込みの実施

(2) **実施上のポイント**

- タイムアウト機能の組込みの検討対象となる機器等
  - リスクの高いロケーションに置かれた端末
  - リスクの高いシステムに接続されている端末

9.5.8 接続時間の制限

アプリケーションに対する異常に長い時間の接続は怪しいと考えなければならない。取扱いに慎重を要するアプリケーションに接続時間制限を設けるのも、不正なアクセスを排除するための一つの工夫である。

(1) **要求事項**

- 必要な場合におけるアプリケーションへの接続時間制限の適用

(2) **参考**

- 接続時間制限の実施例
  - バッチファイル転送などの場合における転送許可時間帯の設定
  - 短時間の対話型セッションの利用
  - 特別な要請がない場合における、通常の終業時間外での接続の禁止

9.6　業務用ソフトウェアのアクセス制御

システムへの不正アクセスに対する論理的なバリアの一つであるアプリケーションレベルでのアクセス制限も適切に機能するようになっていなければならない。

このためには、

- 情報へのアクセス制限の実施
- 慎重な取扱いを要するシステムの隔離

が必要である。

9.6.1　情報へのアクセスの制限

情報やアプリケーションシステムへの不正なアクセスを防ぐためには、情報やアプリケーションシステムの機能へのアクセスが制限され、適切に管理されなければならない。

9.6.2　取扱いに慎重を要するシステムの隔離

一つのシステムのセキュリティの破綻が他のシステムのセキュリティに悪い影響を及ぼすこともある。このため、慎重な取扱いを要するシステムは他のシステムから隔離し、業務の重要性が低いという理由からセキュリティが甘く設定されている他のシステムにおけるセキュリティ事故の影響を受けないようにしておくことも必要である。

(1) 要求事項

- 慎重な取扱いを要するシステムの他システムからの隔離

(2) 実施上のポイント

- システムの隔離の方法
  - ・ セグメントの分離
  - ・ 登載サーバの分離
  - ・ 搭載サーバに対するデータフローの制限
- 各システムに適用する保護のレベルについては、当該システムの所有者が判断しなければならない。

9.7 システムアクセスおよびシステム使用状況の監視

システムの不正な使用を防ぐためには、システムへの不正なアクセスを検出し、その証拠を押さえるための、システムへのアクセスや使用についての適切な監視も必要となる。

このためには、

- セキュリティに関係するイベントについての記録の作成と保管
- システムの使用についての監視の実施
- クロックの同期の確保

が必要となる。

9.7.1 事象の記録

システムの不正な使用や不適切な運用のチェックや、問題が生じたときの調査のため、例外事項およびその他のセキュリティ関連イベントについては、記録が作成され適切に保管されなければならない。

(1) 要求事項

- 将来の調査やアクセス制御の評価のための資料としての対象となるイベントについての記録（監査ログ:関係資料を含む）の作成
- 作成した記録の所定の期間の保管

(2) 参考

- 記録すべきイベントについて記録（監査ログ）に記載すべき事項
  - ユーザ ID
  - ログオンおよびログオフの日時
  - アクセス者の端末の ID またはロケーション
  - システムアクセスの試みに成功したもの拒否されたものの記録
  - データおよび他の資源へのアクセスの試みに成功したものおよび拒否されたものの記録

9.7.2 システム使用状況の監視

情報処理施設および設備は、故意や誤りにより不正に使用された場合は、それが発見され速やかに適切な処置がとられなければならない。このためには、情報処理施設および設備の使用について監視を行うことも必要である。

(1) **要求事項**

- 情報処理施設および設備の使用監視要領の確立
- 監視手順に基づいた情報処理施設および設備の使用についての監視の実施
- 監視結果のチェックの実施
- ロギング機能の保護

(2) **実施上のポイント**

- 監視要領の中での監視レベルの明確化
- 想定するリスクに対応した頻度での監視結果のチェックの実施
- システムログの取得に対する監視結果のチェックを効率的に行うための工夫の組込み
- ロギング機能に細工されないための、ロギング機能に対する適切なセキュリティ対策の実施

(3) **参考**

- 監視の対象とすべきイベントならびに記録すべき事項等
  - システムログのチェック頻度の検討要素
  - アプリケーションプロセスの重要性
  - 関係する情報の価値、重要性、および取扱いに求められる慎重度
  - システムへの侵入やシステムの誤使用等による事故事例
  - 当該システムにつながるタシステムとの関係からくるシステム相互接続の範囲
- システムログのチェック頻度の検討要素
  - アプリケーションプロセスの重要性
  - 関係する情報の価値、重要性、および取扱いに求められる慎重度
  - システムへの侵入やシステムの誤用等によるセキュリティ事故事例
- 当該システムにつながる他システムとの関係からくるシステム相互接続の範囲

表 9-1に、監視し記録すべきシステムのイベントを示す。

- システムログのチェック頻度の検討要素
  - アプリケーションプロセスの重要性
  - 関係する情報の価値、重要性、および取扱いに求められる慎重度
  - システムへの侵入やシステムの誤用等による事故事例
  - 当該システムにつながる他システムとの関係等からくるシステム相互接続の範囲

表 9-1 監視ならびに記録のの対象とすべきイベント

監視区分	監視ならびに記録の対象とすべきイベント
認可されているアクセス	ユーザ ID、キーイベントの日時、イベントのタイプ、アクセスされたファイル、使用されたプログラムおよびユーティリティ
すべての特権操作	スーパーバイザーアカウントの使用、システムの起動および停止入出力装置の取付けや取外し
認可されていないアクセスの試み	失敗した試み、ネットワーク・ゲートウェイおよびファイアウォールについてのアクセスポリシー違反および通知
次のようなシステム警告または故障	コンソール警告またはメッセージ、システムログ例外事項、ネットワーク管理アラーム

- システムログの取得およびチェックにおいて考慮すべき工夫
  - 監視情報の絞込み
  - 監視ログ分析ツールの活用
- ロギング機能に求められる保護
  - 意図的な停止やログファイルのオーバーフローによるロギング機能の動作停止の予防
  - 正式な手順を踏まない記録の対象とすべきイベントやメッセージタイプの変更
  - 正式な手順を踏まないログファイルの編集または削除

9.7.3 コンピュータ内の時計の同期

システムのクロックはシステムの処理やイベントの発生時刻を示すタイムスタンプとして用いられる。システムで用いられるクロックのすべては同期がとれていないとその機能は果たせない。このため、システムで用いるクロックは指定のものに同期されているようになっていなければならない。

(1) 要求事項

- システムで用いるクロックの同期の確保

(2) 実施上のポイント

- システムで用いるクロックの標準時間への同期
- 定期的な確認と必要な補正の実施

9.8 移動型計算処理遠隔作業

組織の管理領域外で作業が行われるモバイル環境でのシステムの使用やテレワーキングは、組織の管理領域内とは異なるセキュリティ上の脅威が多い。このため、このような環境における作業に対しては、特別なセキュリティ上の配慮が必要である。

このためには、

- モバイルコンピューティングに対するセキュリティ対策の実施
- テレワーキングに対するセキュリティ対策の実施

が必要となる。

9.8.1 移動型計算処理

モバイル端末からのシステムへのアクセスには特別なリスクが付随する。システムにモバイル端末からアクセスを許す場合、このシステムのモバイル環境での利用が、システムのセキュリティを脅かさないようにするためには、モバイル端末の使用やモバイル環境での作業に対して適切なセキュリティ対策が講じられなければならない。

(1) 要求事項

- モバイルコンピューティングに対するセキュリティポリシーの確立

(2) 実施上のポイント

- モバイルコンピューティングについてのセキュリティポリシーの中で明確にすべき事項
  - 保護されていない環境からのアクセスに対し必要となるシステム側における配慮
  - 保護されていない環境における作業に対するセキュリティ対策の明確化
- モバイル端末からのアクセスに対するセキュリティ対策のポイント
  - アクセス制御についての要求
  - 暗号化についての要求
  - バックアップについての要求
  - ウイルス対策についての要求
  - モバイル機能をネットワークに接続するにあたっての規則および注意
  - 公共の場所での作業についての注意事項
- 保護されていない環境での作業に対するセキュリティ対策のポイント
  - 使用する装置に対する物理的保護
  - 第三者（認可されていない者）による作業の盗聴、盗み見の防止
  - ウイルス等の有害なソフトウェアに対する適切な対策の適用
  - 情報のバックアップの確保

- モバイル環境で作業する者に対するセキュリティに関する教育

9.8.2 遠隔作業

企業等がその業務でテレワーキングを行う場合、組織の敷地外にあるテレワーキングサイトが無防備であれば、ここから組織のセキュリティが崩される恐れがある。このため、テレワーキングサイトに対しても組織のセキュリティポリシーに沿った適切なセキュリティ対策が講じられなければならない。

(1) **要求事項**

- テレワーキングに対するセキュリティポリシーの確立

(2) **実施上のポイント**

- テレワーキングに対するセキュリティポリシーで明確にすべき事項
  - テレワーキング活動に対する管理ポリシー
  - テレワーキングについての規則
  - テレワーキングにおける作業の手順
  - テレワーキングサイトにおけるセキュリティ対策
- テレワーキングの認可にあたって検討すべき事項
  - テレワーキングサイトの物理的セキュリティ（建物および位置環境）
  - 提案されたテレワーキング環境
  - 業務上の必要性
  - システムへのアクセスに適用されるセキュリティ対策
  - 第三者アクセスの脅威
- テレワーキングをセキュアなものにするためのポイント
  - 適切な装置および保管用備品の提供
  - 許される作業、作業時間、保有してよい情報、使用できるサービスの明確化
  - リモートアクセスの安全を図るために必要な装置の提供
  - 指定作業者以外の者（家族およびビジター等）の装置や情報へのアクセスに関する規則ならびに手引きの確立
  - 使用するハードウェアならびにソフトウェアに対する適切なサポートとメンテナンスの提供
  - バックアップ手順の明確化
  - 障害時における復旧ならびに再開手順の明確化
  - セキュリティ監視および監査の実施
  - テレワーキング活動の終了時におけるアクセス権の取消し、および装置の返却の適切な実施

10 システム開発および保守

業務運用に提供されるシステムにセキュリティ面での脆弱性が残されないようにしなければならない。このためには、使用するシステムについてのセキュリティ要求事項が明確にされ、それらがシステムに適切に反映されるようになっていなければならない。

このことを実現するためには、

(1) システムに対するセキュリティ要求事項の明確化

(2) アプリケーションシステムへのセキュリティ要求事項の組込み

(3) 暗号技術の適切な適用

(4) システムファイルの保護

(5) 開発およびサポートプロセスにおけるセキュリティ管理の実施

が必要となる。

10.1 システムのセキュリティ要求事項

運用で使用するシステムについては、その個々にセキュリティ要求事項が適切に定義されていなくてはならない。

10.1.1 セキュリティ要求事項の分析および明示

システムの新規開発あるいは既存システムの改修において、対象システムをセキュアなものにするためには、既存システムの改修も含めて開発するシステムにおけるセキュリティ要件を明確にしておかなければならない。システムのセキュリティ要件の定義は、当該システムを対象としたリスクアセスメントに基づいたものでなければならない。

(1) 要求事項

- 新システムの開発または既存システムの改修に対して定義するビジネス要求事項の中へのリスクアセスメントに基づいたセキュリティ要件の明示
- 使用するソフトウェアパッケージに対するセキュリティ要求事項についての満足度の確認
- システムに組込むべきセキュリティ機能、および運用で対応する事項の明示

(2) 実施上のポイント

- セキュリティ要求事項の検討における関係する情報資産のビジネス上の価値や、セキュリティ事故が発生した場合に生じうるビジネス上の損害の分析評価

(3) **参考**

- セキュリティ確保に要するコストは、開発途中や運用開始後のセキュリティ対策の組込みに比べ、設計段階から考慮すれば著しく安く済ますことができる。

10.2 業務用システムのセキュリティ

システムの誤った処理は業務の混乱を招く。アプリケーションシステムは、正しいデータを用い、正しく処理され、システムの出力は正しいことが保証されていなければならない。

このためには、

- 入力データの妥当性のチェック
- 内部処理の妥当性のチェック
- メッセージの真正性のチェック
- 出力データの妥当性のチェック

が必要となる。

10.2.1 入力データの妥当性確認

不正な入力データをもとにしたシステムの処理は、システムのエラーや業務の混乱を生じる。このため、システムに入力されたデータに対しては、処理に先立ちその妥当性のチェックを実施しなければならない。

(1) **要求事項**

- 入力データに対する妥当性のチェック確認要件の明示とエラー検出時の処理要領の確立
- 定められた要領に基づく入力データに対する妥当性チェックの実施
- エラーデータに対する適切な処理の実施
- データ入力プロセスにかかわるスタッフの責任の明確化

(2) **実施上のポイント**

- 入力データに対する妥当性チェックとしては以下がある。
  - ・ 形式チェック
  - ・ 入力データと原情報の一致性

(3) **参考**

- 入力データに対して実施すべき形式チェック
  - ・ 範囲外の値
  - ・ データフィールドの無効な文字

・ 入力落ちまたは不完全なデータ
・ 数値の上限および下限の超過
・ 認可されていない制御データ、または矛盾した制御データ

10.2.2 内部処理の管理

処理ロジックのエラーや処理ロジックに対する工作により、システムの意図していることと異なる処理により作られた不正なデータは、業務に大きな悪影響を及ぼす。このようなことを防止するためには、システムの内部処理の結果をチェックする仕組みをシステムあるいは業務の流れの中に組込んでおき、不正な処理の早期発見が行えるようにしておくとともに、不正な処理からの回復を行うために必要となる仕組を整備しておくことも必要となる。

(1) **要求事項**

- プログラムへの必要な場所に対する処理結果の検証機能の組込み
- データの更新、追加、削除機能のプログラム上での適切な配置
- 間違った順序でのプログラムの実行や、先行処理が正常に終了しなかった場合における後続処理の実行制御機能の組込み
- 不良処理からのデータの回復手段の準備

(2) **実施上のポイント**

- 処理結果の妥当性確認の手法
  - ・ セッションまたはバッチ単位でのデータファイルのバランスチェック
  - ・ データを共有する処理間でのデータ処理の妥当性のチェック
    複数の処理がデータを共有している場合、処理の順序やデータのアクセスに関する制御が適切に行われていないと、処理結果が不正になる。このため、これらの処理については、以下のようなチェックが必要となる。
    －ジョブ間の連携についてのチェック
    －更新前ファイル、更新後ファイルとトランザクションデータの整合性のチェック
    －プログラム間連携についてのチェック
  - ・ システム生成データに対する妥当性の確認
  - ・ ダウンロードまたはアップロードデータに対する完全性チェック
  - ・ レコードおよびファイルに対するハッシュ値の照合チェック
  - ・ アプリケーションプログラムの実行時刻のチェック

10.2.3 メッセージ認証

ネットワーク経由で受取ったデータは、改ざんされている可能性もある。このため、ネットワーク経由で受取ったデータに対しては、受取り時点またはその処理に先だって、その真正性の確認を行っておく必要がある場合がある。必要な場合における、受取りデータに対する真正性の確認は漏れないようにしなければならない。

(1) **要求事項**

- 必要な場合におけるデータの真正性の確認の実施

(2) **実施上のポイント**

- データの真正性確認の要否の検討
- 真正性確認が必要なデータに対する適切な真正性確認プロセスの組込み
- データの真正性の検証をサポートする適切なハードウェアまたはソフトウェアの適切な使用

(3) **参考**

- メッセージの真正性の確認技術としては、暗号化やデジタル署名がある

10.2.4 出力データの妥当性確認

システムの出力に問題があれば業務は混乱する。不適切な出力がそのまま業務で用いられないようにするためには、システムの出力について妥当性のチェックは欠かせない。

(1) **要求事項**

- 出力の妥当性の確認を適切に行うための仕組みの確立
- 出力の妥当性についての確認の実施

(2) **実施上のポイント**

- 出力の妥当性の確認を適切に行うための仕組みとして検討すべき事項
  - それぞれの出力に対する妥当性チェック要件の確立
  - 異常発見時の処置要領の確立
  - システムの出力処理ならびに業務での出力の処理にかかわる者の出力の妥当性の確保について責任の明示
- 出力に対する妥当性確認のポイント
  - 様式チェック等の外見性チェック
  - 出力数の確認（すべてのページやレコードが完全に出力していることの確認）

10.3 暗号による管理策

システムで取扱う情報のうち、特に取扱いに慎重を要するものについては、その秘匿と完全性が保証されていなければならない。このため、システムに格納されている情報や通信メッセージに対し暗号技術を適用することも必要となる。

暗号技術を適切に用いるためには、

- 暗号の適用についてのポリシーの確立
- 必要に応じた暗号化の実施
- 必要に応じたデジタル署名の利用
- 事後否認への備え
- 暗号鍵の適切な管理

が必要となる。

10.3.1 暗号による管理策の使用に関する個別方針

暗号の適用が適切に行われるためには、組織における暗号の使用についての適切なポリシー（暗号化ポリシー）が確立していなければならない。

(1) 要求事項

- 組織における暗号化ポリシーの確立

(2) 実施上のポイント

- 暗号化ポリシーで規定すべき事項
  - ・暗号の適用についての考え方
  - ・暗号鍵の管理についての取組み方針
  - ・暗号の適用に関する責任体制
    - －暗号適用ポリシーの実行についての責任
    - －暗号鍵の管理についての責任
  - ・必要な場面に対する適切な暗号レベルの決定要領
  - ・暗号技術の採用方針

10.3.2 暗号化

情報の保護のための暗号化は、組織の暗号化ポリシーにもとづいて行われなければならない。

(1) **要求事項**

- リスクアセスメントに基づく暗号化ポリシーに沿った暗号化要件の適切な指定
- 適切な暗号化技術（方式）の選択

(2) **実施上のポイント**

- 暗号化要件の指定で明確にすべきこと
  - 暗号化アルゴリズムのタイプおよび特性
  - 暗号鍵長
- 暗号技術（方式）の選択に当っての留意事項
  - 暗号化要件に対する満足度とその運用性
  - 関係する法律または規制の制約
  - 専門家の助言の活用

10.3.3 デジタル署名

ネットワーク経由での処理は、交換されるデータが改ざんされていないことを前提としている。改ざんされたデータによる処理が行われないようにするためには、交換したデータに対する真正性（改ざんされていないこと）の確認が必要となる。必要に応じ、データの真正性を確認または保証するための手段として、デジタル署名の適用も検討しなければならない。

(1) **要求事項**

- 必要な場面におけるデジタル署名の適用
- デジタル署名を利用する場合における適切な署名方式の採用
- 必要な場合における、デジタル署名されたデータの法的効力の確保

(2) **実施上のポイント**

- 署名方式検討のポイント
  - 署名アルゴリズムのタイプと特性
  - 暗号鍵長
- デジタル署名に用いる暗号鍵と、データの暗号化に用いる暗号鍵の分離
- デジタル署名の法的効力確保のための工夫
  - デジタル署名の法的効力についての相手側との合意の確保
  - 適用にあたっての専門家の助言の活用

- 暗号鍵の保護のポイント
  - 秘密鍵の機密性の確保
  - 公開鍵の完全性の確保

10.3.4 否認防止サービス

ネットワーク経由の処理においては、相手側からの処理の要求や処理結果の受取りの否認によりトラブルが生じることもある。このようなトラブルを避けるためには、相手の否認を拒否できる用意が必要である。このためには、必要な場面に対しては、イベントの発生または処理が実行されたことを第三者の立場からの証明する公証サービスの利用等も検討しておかなければならない。

(1) **要求事項**

- 必要な場合における公証サービスの利用の検討

(2) **実施上のポイント**

- 特に事後否認が大きな問題となるような処理に対する公証サービスの利用を検討
- 公証サービス利用上の留意点
  - 法的有効性の確認
  - 技術面での有効性の確認
  - 相手側の合意の要否の確認と、必要な場合における合意の確保

(3) **参考**

- 公証サービスに期待できることとしては、事象の発生、処理の完了、使用された情報の内容についての第三者の立場からの証明である。

10.3.5 かぎ管理

暗号鍵の漏洩、改ざん、破壊の発生は、暗号化が破綻するだけでなく、暗号化された情報の保護も危うくなる。このため、暗号鍵に対しては、漏洩や改ざんから守るための適切な保護がなされなければならない。

(1) **要求事項**

- 暗号鍵の管理の仕組みの確立
  - 暗号鍵生成システムの保護
  - 暗号鍵管理システムの保護
  - 暗号鍵アーカイブの保護

- システム運用上での暗号鍵管理要領の確立
- 外部の暗号サービスの提供者との間での、サービスの信頼性についての合意の確立

(2) **実施上のポイント**

- 暗号鍵管理要領で規定すべき事項
  - 暗号鍵の生成手順
  - 公開鍵証明書の必要性の考慮と取得手順
  - 暗号鍵の配布手順
  - 暗号鍵のインストール方法、利用方法、保管方法等を規定した配布先における暗号鍵の取扱い方法
  - 有効期限の管理等、暗号鍵の更新と更新手順
  - 暗号鍵へのアクセスについてのルール
  - セキュリティが損なわれた暗号鍵の取扱い
  - 消失したあるいは損傷した暗号鍵の回復手順
  - 暗号鍵のアーカイブ要領
  - 暗号鍵の破棄要領
  - 暗号鍵の管理にかかわる処理の記録と保管
  - 暗号鍵の管理についての監査の実施

10.4 システムファイルのセキュリティ

運用ソフトウェア、システム試験データ、プログラムソースライブラリ等のシステム運用の要となるシステムファイルは、外部への流出や改ざん破壊から十分に保護されていなければならない。

このためには、

- 運用ソフトウェアの管理
- システム試験データの保護
- プログラムソースライブラリへのアクセス管理

が必要となる。

10.4.1 運用ソフトウェアの管理

運用に用いられるソフトウェアが改ざんされたり、破壊されたりするようなことがあってはならない。このため、運用に用いられるソフトウェアに対しては適切な保護措置がとられなければならない。

(1) **要求事項**

- 予定されている更新についてのセキュリティ面からのレビューの実施と、必要な対策の実施
- 運用に用いられるソフトウェアのライブラリに対する適切な管理要領の確立と、この指定に基づくライブラリ管理の厳格な実施が必要
- ソフトウェアベンダの運用ライブラリへの物理的ならびに論理的アクセスの制限

(2) **実施上のポイント**

- ソフトウェアベンダの運用ライブラリへの物理的ならびに論理的アクセスの制限のためには、以下が必要となる
  - 管理者による承認
  - 活動に対する監視
- 運用プログラムのライブラリ管理要領で規定すべき事項
  - 適切な責任者の認可に基づくライブラリ管理責任者による運用プログラムの更新の実施
  - 実行コードのみの引渡し
  - すべてのテストの終了、業務サイドの受入れ承認、対応ソースライブラリの更新完了前の、運用システムにおける更新プログラムの実行の禁止
  - 運用プログラムライブラリの更新についての完全な監査ログの確保
  - 新バージョンのトラブルに備えた旧バージョンの保持
  - ベンダー提供のソフトウェアに対する独自のメンテナンスの自粛

10.4.2 システム試験データの保護

システムのテストに運用データを用いることがある。テスト目的で運用データを使用することにより実運用に用いられている情報の改ざんや破壊、あるいは漏洩が生じないようにするためには、テスト目的で使用される運用データに対する適切な保護がなされなければならない。

(1) **要求事項**

- テスト目的での運用データベースへのアクセスの制限
- 開発中のアプリケーションシステムのテストに用いるための運用データのコピーの制限
- テスト終了後におけるテストに用いられた運用データの消去

(2) **実施上のポイント**

- 運用データベースをテストで用いる場合の注意事項
- 運用で適用されているアクセス制御手順の適用
- 開発中のアプリケーションシステムでテストに運用情報を用いるための運用データのコピーの制限方法
  - コピーに対する認可制の採用

・ 運用情報のコピーについての履歴の作成と保管

10.4.3 プログラムソースライブラリへのアクセス管理

意図しない更新や改ざんからソースライブラリを保護するためには、その保管を適切に行うとともに、プログラムソースライブラリへのアクセスを制限するための仕組みを確立しておかなければならない。

(1) **要求事項**

- プログラムソースライブラリの管理要領の確立
- 管理要領に基づくプログラムソースライブラリ管理の実施

(2) **実施上のポイント**

- プログラムソースライブラリの管理要領で規定すべき事項
  - 旧バージョンの関連情報と一体となったアーカイブ
  - ソースライブラリのメンテナンスおよびコピーの実施手順の確立
  - ルールに沿ったメンテナンスとコピーの実施
  - ソースライブラリの運用環境からの隔離
  - ソ ースライブラリの保護についての責任体制の明確化
  - 運用に用いられているソースライブラリと開発中またはメンテナンス中のプログラムの隔離
  - ソースライブラリの更新やプログラマへのソースプログラムの引渡しについての責任体制の確立
  - プログラムソフトの安全な管理
  - ソースライブラリアクセスについてのログの保管
  - IT サポートスタッフのプログラムソースライブラリへのアクセスの制限

10.5 開発および支援過程におけるセキュリティ

不用意な新規システムの導入やシステムの変更は、システムのセキュリティを損なうことがにつながる。このため、システムの開発、導入、変更は厳しく管理されなければならない。

不用意な新規システムの導入やシステムの変更を防止するためには、以下の施策の実施が必要となる。

- 変更管理手順の確立
- オペレーティングシステムの変更の技術的レビューの実施
- ソフトウェアパッケージの変更に対する制限

- 導入ソフトウェアに対する隠れチャネルおよびトロイのコードのチェック
- ソフトウェアの委託開発についての適切な管理の実施

10.5.1 変更管理手順

不用意なアプリケーションソフトのメンテナンスは、業務やセキュリティに悪影響を与える。アプリケーションソフトのメンテナンスが業務に影響を与えたり、システムの機能や処理の完全性の損傷や、セキュリティの低下を招いたりしないようにするためには、アプリケーションソフトのメンテナンスについてのプロセスについて管理を確立しておかなければならない。

(1) **要求事項**

- アプリケーションソフトの変更ならびに切替え要領の確立
- 規定された変更･切替え要領に従ったアプリケーションソフトの変更、およびその管理の実施

(2) **実施上のポイント**

- アプリケーションソフトの変更、切替えの業務への影響の極小化実現の工夫
  - 切替え時の業務中断時間の極小化
  - 切替えのタイミングの適切な選択
- アプリケーションソフトの変更や切替え要領で規定すべきこと
  - 変更内容についての業務サイドからの承認の取得
  - 切替えに際しての新システムに対する業務サイドからの試験を通じた確認と承認
  - 当該変更のシステム運用手順や業務処理手順への反映
  - 関係ドキュメントの差換え、旧バージョン対応ドキュメントの廃棄またはアーカイブ
  - 変更内容と変更の承認についての記録の作成と保管
  - ソフトウェアのバージョン管理の完全な実施
  - 変更によりプログラムの制御の完全性が損なわれていないことを確認するレビューの実施
- アプリケーションの変更作業の実施にあたっての留意点
  - 他のアプリケーションを含むすべてのソフトウェア、情報、データベース、およびハードウェア等の変更対象のアプリケーションの機能や処理方式の十分な確認
  - 目標とする変更の影響範囲の洗出しと、それらに対する必要な変更の実施
  - 開発環境とは異なる環境での受入れテストの実施
  - サポートプログラマのシステムへのアクセスの制限

10.5.2 オペレーティングシステムの変更の技術的レビュー

バージョンアップやパッチ等のオペレーティングソフトの変更の不用意な実施は、システム運用やセキュリティに悪影響を与えることが多い。このため、オペレーティングシステムのメンテナンスの実施に対しては、十分な事前レビューの実施やアプリケーションレベルでの十分なテストが行わなければならない。

(1) **要求事項**

- オペレーティングシステムの変更にあたっての、アプリケーションへの影響についての徹底した事前レビューの実施
- 当該メンテナンスの事業継続計画への影響のチェックと反映

(2) **実施上のポイント**

- オペレーティングシステム担当チームとアプリケーション担当チームの適切な連携の確保
- アプリケーション担当チームにおける、オペレーティングシステムの変更に対応したアプリケーションソフトのレビューやテストに必要な人員、予算の確保

10.5.3 パッケージソフトウェアの変更に対する制限

ベンダー提供のソフトウェアパッケージの修正は、不用意な修正による機能や制御の破壊、あるいはセキュリティの低下といったリスクの他に、ベンダーによるバージョンアップ等への対応が困難になる等のリスクが伴う。このため、ベンダー提供のパッケージソフトの修正はできるだけ避けるようにするとともに、実施にあたっては十分な管理が行われなければならない。

(1) **要求事項**

- 修正の可否についての適切な判断の実施
- 修正したソフトウェアに対する完全なテストの実施
- オリジナルの保存と修正履歴の完全な保管

(2) **実施上のポイント**

- ソフトウェアパッケージの修正は原則として行わないこと
- ソフトウェアパッケージの修正にあたっての要確認事項
  - 修正を加えることについてのソフトウェアの機能、処理を損傷するリスク
  - ベンダーの同意の要否
  - 当該修正のベンダーによる対応の可能性の有無
  - ベンダーに対するメンテナンス責任の追及ができなくなる可能性

(3) **参考**

- ソフトウェアパッケージの修正にかかるリスク
  - 不用意な修正によるソフトウェアパッケージの機能や制御の完全性の破壊
  - ベンダーによるソフトウェアパッケージのバージョンアップへの対応の困難化
  - 将来のメンテナンスにおけるベンダーのサポートの困難化
  - プログラムの改変権への抵触

10.5.4 隠れチャネルおよびトロイの木馬

外部から導入するソフトウェアに対しては内部に仕組まれた隠れチャネルやトロイのコードによりシステムが被害を受けることがないように必要な注意を払らわなければならない。

(1) **要求事項**

- 導入ソフトウェアに対する隠れチャネルのチェックの実施
- 導入ソフトウェアに対するトロイのコードのチェックの実施

(2) **実施上のポイント**

- 隠れチャネルやトロイのコードに対する注意のポイント
  - 使用するソフトウェアは信頼できるベンダーのものに限定
  - ソースコードでの入手と使用前のトロイのコードの検査の実施
  - インストールされたソフトウェアへのアクセスおよび変更の制限
  - 重要システムの開発への信頼できるスタッフの投入

10.5.5 外部委託によるソフトウェアの開発

開発を外部に委託したソフトウェアが、信頼性の高いものであり、かつセキュリティ上の問題がないものとして納入されるようにするためには、委託先での開発に対しても開発管理についての適切な監督と指導が必要となる。また、納入されるソフトウェアの権利関係についてのトラブルを生じないようにするための必要な処置ならびに管理も必要である。

(1) **要求事項**

- 開発委託したソフトウェアの品質とセキュリティの確保
- 開発委託したソフトウェアについての権利関係に関するトラブルの予防
- 開発委託先等の倒産等の委託開発プロジェクトに対する影響への備えの実施

(2) **実施上のポイント**

- 開発委託したソフトウェアの品質とセキュリティの確保のために実施すべき事項
  - ・ 開発作業の質および正確さについての確認
  - ・ 開発委託契約における開発ソフトウェアの質についての要求の明示
  - ・ 開発作業の質や正確性についての監査権の確保
  - ・ 受入れにあたってのトロイのコードの検出試験の実施
- 開発委託したソフトウェアについての権利関係に関するトラブルの防止のためには、委託開発されたソフトウェアの所有権、知的財産権の所在の明確化や使用許諾等の権利関係の明確化が必要
- 開発委託先等の倒産が、委託開発プロジェクトへ影響を与えないようにするためには、開発あるいは開発成果物にかかわる開発委託先等の破産による開発プロジェクトや開発成果物に対する取扱いの明確化が必要

11 事業継続管理

セキュリティ事故が発生しても、業務の継続に支障がでるようなことは避けなければならない。このためには、事故が発生してもそれが業務の中断に直結しないようにする工夫をシステムに組込んでおくとともに、システムの速やかな回復等の事故処理が迅速にできようにするための備えが必要となる。

11.1 事業継続管理の種々の面

セキュリティ事故が業務の継続に支障をきたさないようにするため日頃からの備えとしては、以下の施策の実施が求められる。

- 事業継続管理プロセスの確立
- 事業継続計画の実行環境の整備
- ビジネス単位の事業継続計画の作成および維持
- 各事業継続計画の統合運用計画の作成

11.1.1 事業継続管理手続

事業継続計画が適切に策定されるためには、事業継続計画の立案と維持のための管理されたプロセスが確立していなければならない。

(1) 要求事項

- 事業継続計画作成要領の確立と維持

(2) 実施上のポイント

- 事業継続計画で定義すべきこと
  - ・リスク評価の実施
  - ・障害の事業に及ぼす影響を極小化するために必要な情報処理施設や設備についての要件の定義
  - ・必要に応じた保険加入の検討
  - ・ビジネス戦略に沿った事業継続戦略の確立
  - ・事業継続計画ならびにプロセスの定期的な見直しと更新
  - ・組織の各プロセスへの事業継続計画からの要求の確実な組込み
  - ・経営陣も参加している情報セキュリティマネジメント委員会による審議ならびに承認
- リスク分析のポイント

・ 重要なビジネスプロセスの洗出しと適切な優先順位の設定
・ リスクの洗出しとその発生頻度ならびに事業への影響の評価

11.1.2 事業継続および影響分析

事業継続計画が適切に策定されるためには、故障、災害、外部からの攻撃等の影響の分析等、事業継続計画作成のベースとなるリスクアセスメントを適切に実施しなければならない。

(1) **要求事項**

- 適切なリスクアセスメントの実施
- リスクアセスメントの結果の事業継続計画への反映

(2) **実施上のポイント**

- 障害の影響の分析においては、想定される損害の規模と回復に要する時間を考慮すること
- 評価の対象は、事業プロセスの全ての分野とし、情報処理施設や設備に限定しないこと
- リスク評価の対象は、情報処理関連施設や設備および装置の故障、災害、外部からの攻撃、運用の不手際も含めること

11.1.3 継続計画の作成および実施

事業継続計画は、セキュリティ事故の事業への影響や回復処理のやり方にもとづいて決められるもので、事業単位あるいはシステムの運用単位ごとに計画されるべきものである。このため、まず、事業継続計画の作成単位を設定し、それぞれに対する個別の事業継続計画を作成することが必要となる。

(1) **要求事項**

- 事業単位ごとの障害、故障、災害、外部からの攻撃を想定した事業継続計画の確立
- 業務運営ならびにシステム運営への策定した事業継続計画の組込み
- 作成した計画に対する定期的あるいは必要に応じた見直しの実施による作成した計画の有効性の維持
- 計画した事業計画の実行に必要なリソースの確保
- 関係者への計画の周知と、事業継続計画実施のための必要な教育の実施

(2) **実施上のポイント**

- 個別事業継続計画立案にあたって考慮すべき事項
  ・ 作成した計画についての責任者よる妥当性の確認

・非常時の対応についての責任体制
　－要求される時間内での復旧の確認等の作成した手順の妥当性の確認
　－システムの運用や業務の一部を外部に委託している場合における、業務委託先との連携が円滑に行えるかどうかについての確認

- 個別事業継続計画の取扱いについて
  ・計画の正式な文書化
  ・回復テスト等よる作成した計画の妥当性の確認

11.1.4 事業継続計画作成のための枠組み

事業継続計画は、事業単位あるいはシステム運用単位に作成されるものであるが、その実施にあたってはそれらの統合的な運用が必要となる。このため、個々に作成された各事業継続計画を統合した全体としての事業継続の統合運用計画を作成することが必要となる。事故発生時における、実際の事業継続にかかわる処理は、この統合運用計画に沿って行われる。

(1) 要求事項

- 事業単位やシステムの運用単位ごとに作成された事業継続計画を実行するための組織全体からみた統合運用計画の作成
- 事業継続統合運用計画の有効性の確認とその維持
- 関係者への周知

(2) 実施上のポイント

- 事業継続統括運用計画の作成において明確にすべき事項
  ・状況の評価、個別計画発動の検討等の計画実行開始前に実行すべき事項
  ・広報活動等の事業の運営に大きな影響がでたり、人命にかかわるよう問題が生じた場合における関係機関への連絡等の特別な処置
  ・主要な事業活動または事業支援サービスのバックアップへの切替え手順
  ・業務の再開始手順
  ・事業継続計画の見直し要領
  　－事業継続計画の見直しサイクル
  　－テストの内容や実施サイクル等の各計画についてのテスト計画の大枠
  　－訓練内容や実施サイクル等の各計画に対する訓練計画の大枠
  サイクルや内容等の各計画のテストおよび訓練計画の見直し計画の大枠
  ・事業継続計画にかかわる個々のプロセスに対する責任体制の明確化
  ・事業継続計画の関係者への周知活動
- 個別事業継続計画の責任者の割当ての例

表 11-1 個別事業継続計画に対する責任者の割り当て例

事業継続計画にかかる作業	責任者
・非常時手順 ・マニュアルフォールバック計画 ・再開計画	事業資源の所有者またはプロセスの責任者
・情報処理および通信施設等の代替技術サービスのフォールバック	サービス供給者

11.1.5 事業継続計画の試験、維持および再評価

業務処理方式の変更やシステムの変更等、組織の運営環境に変更が生じた場合は、既存の事業継続計画の見直しが必要であり、このような変更に際しては、事業継続計画の維持についての手順に沿った見直しが行われなければならない。組織の運営環境の変更に対する事業継続計画の見直しの漏れに備え、作成されている事業継続計画に対しては、レビューや回復テストや回復訓練を通じて、その有効性を定期的にチェックし、必要な手直しを行って、その有効性を維持するようにしなければならない。

(1) **要求事項**

- 事業継続計画の見直し要領の確立
- 見直し要領に基づいた定期的なレビューと必要な更新の実施
- テストや訓練等による作成された事業継続計画の有効性の確認の実施

(2) **実施上のポイント**

- 事業継続計画についてのテストおよび訓練要領の確立
- 全体的な試験および訓練とは別に、計画のコンポーネントについての頻繁な試験や訓練の実施
- 事業継続計画の試験や訓練に含まれるべきこと
  - ・ さまざまな状況に対する机上訓練
    - －事故発生時における対策チームの配置
    - －事故処理関係者の事故処理手順の確認
  - ・ 事故処理体制
  - ・ システムの回復手順
  - ・ バックアップシステムによる業務の継続
  - ・ 供給者施設およびサービスにおける障害発生時における契約に基づく処理
  - ・ 事業継続処理のプロセス全体のリハーサル

- 事業継続計画のレビューのポイント
  - 各事業継続計画のレビューについての責任者の明確化
  - 事業継続計画の見直しが必要となる場合
    - 情報処理施設や設備、装置、運用システムの変更
    - 運用関係者または事業継続計画関係者の変更
    - 関係サイトの所在地や電話番号の変更
    - 事業戦略の変更
    - 関係する法制の変更
    - 請負業者、供給業者、主要顧客の変更
    - 事業プロセスの追加、変更
    - 業務運営上および財務上のリスクの変化

12 適合性

組織のすべて領域における諸活動は、法律が定めるところや契約の要求事項に違反することなく、かつ、セキュリティポリシーの示すところに沿ったものでなければならない。

このためには、

⑴ 法的側面についての適切な対応の実施

⑵ セキュリティポリシーの遵守状況についての監査の実施

が必要となる。

また、監査の実施にあたっては、業務やシステムの運用に悪い影響を与えないように配慮しなければならない。

12.1 法的要求事項への適合

組織の全ての領域における諸活動において、法律や諸規制および契約上の制約等を守り、法的なトラブルの発生を防止するとともに、万一、紛争が生じても十分な対応ができるようにするためには、日頃からのそのための備えが必要となる。

このためには、

- 関係する法律や規制の明確化
- 知的所有権侵害の防止策の実施
- 組織の活動に関する記録の安全な保護の実施
- データおよび個人情報の保護についての規定違反の防止策の実施
- 情報処理施設や設備の不正使用の防止策の実施
- 暗号の使用に関する規制の遵守
- 訴訟等における証拠の提出に備えた記録の収集と保管

が必要となる。

12.1.1 適用法令の識別

組織の活動が法律、規則、および契約等の定めるところに違反しないようにするためには、遵守すべき法律、規則、契約上の要求事項を正確に把握するとともに、これらを遵守するための管理上の仕組みの確立が必要となる。

(1) 要求事項

- システム運営にかかる関連法制、規制、および契約上の要求事項の明確化

- 要求事項の遵守のための施策の確立
- 要求事項の個々に対する責任の所在の明確化

12.1.2 知的所有権（IPR）

システムの運営上、著作権、意匠権、または商標等の知的所有権のあるものに対する法的な制約に違反することがないよう、これらの取扱いについて十分な管理を行わなければならない。

(1) **要求事項**

- 他社の著作権、意匠権、商標等の知的財産権侵害防止策の確立
- 定められた他社知的財産権侵害防止策の実施

(2) **実施上のポイント**

- ソフトウェア著作権の保護のポイント
  - ソフトウェアおよび情報製品の合法使用を明確に定めたソフトウェア著作権準拠ポリシーの確立と公表
  - ソフトウェア製品の取得ルールの確立
  - スタッフその他の関係者に対するソフトウェア著作権保護についての教育の実施
  - スタッフその他の関係者に対するソフトウェア著作権保護違反に対する懲罰処置の明示
  - 所有するソフトウェア著作物管理台帳の作成と維持
  - ライセンス、マスターディスク、マニュアル等の正当な所有者であることを示すものの適切な管理
  - ライセンス条件違反（許容されたユーザ数以上での使用他）の防止
  - 使用許諾条件を守るためのポリシーの確立
  - ネットワークからダウンロードするソフトウェアおよび情報の使用にあたっての指定された使用条件の遵守
  - ソフトウェアの処分または他人への譲渡についてのポリシーの確立
  - 認可されていない製品がインストールされていないことについての検査の実施
  - 適切な資産管理ツールの使用

12.1.3 組織の活動の保護

組織における重要な活動についての記録は、将来、組織において必要不可欠となることがある。このため、該当する記録に対しては消失、破壊、改ざんからの保護が十分になされなければならない。

(1) **要求事項**

- 保護の対象となる記録の明確化
- 保護の対象となる記録の保管要領の確立
- 保護の対象となる記録の保管要領に従った保護管理の実施

(2) **実施上のポイント**

- 保管要件の指定で明確にすべきこと
  - 保管期間
  - 保管媒体のタイプ
  - 保管の方法
- 保管要件の指定にあたっての当該記録に対する法律等の要求への準拠
- 保管媒体の経時劣化についての配慮（媒体ベンダーの勧告に基づく対策の確立と実施）
- 保護の対象となる記録の保管要領の確立のポイント
  - 情報の保持、保管、および取扱いについてのルールの確立
  - 対象情報の保管管理スケジュールの確立
  - 法的要求事項に従った記録の保管要件の指定
- 電磁媒体による保管記録に対する長期間にわたる可読性の確保
  (将来の技術変化による保管情報の可読性の喪失の防止)
- 暗号化された情報に用いられた暗号鍵の保管とその取扱い方法の確立
- 必要に応じた迅速に求める形で取り出せる環境の整備と維持
- 重要な記録についての出所目録の整備

(3) **参考**

- 保護が求められる組織活動についての記録例
  - 法律または規制等の要求事項に関連する活動についての記録
  - 将来の訴訟等で提出が求められる可能性のある記録
  - 問題が生じた場合、事業の継続のために必要となる事業活動についての記録

12.1.4 データの保護および個人情報の保護

法律や契約等で保護が義務付けられているデータおよび個人情報に対しては、関係する法律や契約の要求に違反することがないよう、漏洩や改ざんが行われないようにする適切な保護を行わなければならない。

(1) **要求事項**

- 法律等により保護が求められている情報に対する保護管理策の確立
- 情報の保護についての責任体制の確立

- 保護対象情報に対する保護管理策に従った適切な保護の実施

(2) **実施上のポイント**

- 保護管理体制について
  - ・ 情報の保護に関する以下のようなタスクを持つ統括管理者を任命すること。この場合、できれば役員を任命することが望ましい。
    －マネージャ、情報利用者、関係サービス提供者に対する情報保護についての個々の責任および従うべき手順についての指導
    －個人情報のデータベース化の認可
  - ・ 情報の所有者の当該情報に対する保護責任の明確化

12.1.5 情報処理施設の誤用の防止

情報処理施設や設備の不正な使用を許してはならない。このため、情報処理施設や設備の使用については、十分な管理が必要となる。

(1) **要求事項**

- 情報処理施設や設備の不正使用防止策の確立
- 不正使用防止策に基づく情報処理施設や設備の使用に対する適切な管理の実施
- 情報処理施設や設備にアクセスする者に対するルールに基づいた使用についての指導の実施のポイント

(2) **実施上のポイント**

- 不正使用防止策に基づく情報処理施設や設備の使用に対する適切な管理の実施
  - ・ 情報処理施設や設備の使用に対するルールの明確化
  - ・ アクセス権の範囲の明確化
  - ・ 不正使用の牽制
- 情報処理施設や設備の使用に対する経営陣による認可制の導入
- 使用の監視にあたっての必要な手続きの実施

(3) **参考**

- 不正使用に対する牽制についての工夫
  - ・ 不正使用に対する懲罰制度の導入
  - ・ ログオン手順へのシステムの不正使用に対する警告の組込み

12.1.6 暗号による管理策の規制

暗号の使用に関しては、法的な規制が該当する場合がある。このため、暗号の使用にあたっては、使用する暗号に適用される法律等の規制に触れないように注意しなければならない。

(1) **要求事項**

- 暗号の使用における国内法の遵守
- 暗号技術、および暗号機能の追加が可能なハードウェアまたはソフトウェアの他国への移管あるいは他国からの導入についての関係国における輸出管理規制への準拠
- 暗号化された情報へのアクセスに関する法律に基づいた適切な対応

12.1.7 証拠の収集

業務の運営やシステムの運用にあたっては、将来の訴訟等に備え、業務処理やシステム処理に関し必要と思われる証拠（記録）の確保とその保管が適切に行われなければならない。

(1) **要求事項**

- 訴訟等における証拠の提出に関する法的な規制、および法廷で求められる手続きに準拠した証拠の提示を可能とする仕組みのシステムへの組込み
- 提示する証拠の質および完全性の確保のための施策の実施
- 訴訟問題になる可能性ある事故における適切な証拠の保全の実施

(2) **実施上のポイント**

- 証拠の質および完全性の確保のポイント
  - ・ 提示が求められる証拠に対する適切な管理プロセスに基づく証拠の準備
  - ・ 印刷物に対する原本性の保証とその作成、修正、保管等についての記録に対する適切な管理の実施
  - ・電磁媒体上の情報に対しては、コピーの保管と、コピープロセスについてのログと証人の確保
- 訴訟問題に発展することが想定される場合は、証拠の保全等に専門家の助言を求めること

12.2 セキュリティ基本方針および技術適合のレビュー

定められたセキュリティポリシーを有効なものにするためには、組織の全ての領域においてセキュリティポリシーに沿った業務やシステムの運用が行われていなければならない。

このことを確実にするためには、

- 組織の活動のセキュリティポリシーへの準拠についてのチェックの実施
- 適用技術の適正性のチェックの実施

が必要となる。

12.2.1 セキュリティ基本方針との適合

組織内のすべての領域における活動がセキュリティポリシーに沿って適切に行われているかどうかについて定期的なチェックを行い、その実施状況を把握し、問題点については、適宜、適切な改善がなされなければならない。

(1) **要求事項**

- 組織の諸活動がセキュリティポリシーに沿っているかどうかについての組織的チェックの定期的な実施

(2) **実施上のポイント**

- チェックの対象範囲
  - 情報システム
  - システムの供給者
  - 情報および情報財産の所有者
  - システムの利用者
  - 経営陣

12.2.2 技術適合の検査

情報システムのセキュリティの確保に用いている技術についても、それらが要求を満たしているかどうか、システムに脆弱なところはないか等についての定期的なチェックを行い、問題点に対しては適切な改善を行わなければならない。また、このチェックの一環としてシステムへの侵入試験を行う場合、試験がシステムの運用やセキュリティに悪影響を及ぼさないようにしなければならない。

(1) **要求事項**

- 運用システムのセキュリティ要求事項への対応についての定期的なチェックの実施
- 必要に応じた侵入テスト等のシステムに対する脆弱性検査の定期的な実施

(2) **実施上のポイント**

- 侵入テストがシステムの機能やセキュリティに悪影響を及ぼさないようにすること
- 使用技術の妥当性についてのチェックの資格を有する認可された者によってのみ、またはその監督下での実施

12.3 システム監査の考慮事項

- 組織におけるセキュリティ監査が円滑かつ効果的に行われるためには、以下の施策の実施が必要となる。
- 監査実施にあたっての十分な事前準備の実施
- 監査に用いるソフトウェアやデータベースに対する適切な保護の実施

12.3.1 システム監査管理策

システム監査の実施にあたっては、効果的な監査が円滑に行われるようにするとともに、日常の業務への影響を極力なくすようにするためには、監査の実施についての十分な準備が必要となる。

(1) **要求事項**

- 適切な実行計画の立案
- 計画に基づく事前準備の徹底

(2) **実施上のポイント**

- 監査要求事項に対する担当経営陣の承認の確保
- チェック範囲についての関係者の同意の確保
- チェックの対象となるソフトウェアやデータベースの保護（破壊の防止）
  - 読取専用のアクセス手段の適用
  - 読取専用のアクセス以外のアクセスが必要な場合におけるコピーの使用と、使用後のコピーの消去の実施
- チェックに使用される IT 資源の明確化と、使用の確保
- 特別な処理または当初の計画外の追加処理の実行に対する関係者の同意の確保
- システム資源へのすべてのアクセスに対するモニタリングと記録の実施
- チェックの実施に関するすべての手順、要求事項、実行責任の所在の明確化

12.3.2 セキュリティ監査ツールの保護

セキュリティ監査に用いられるソフトウェアやデータベースが改ざんされるようなことがあれば、適正な監査は期待できない。また、監査に用いられるツールには、通常のアクセス権を超えた機能が与えられていることが多く、不正に使用されるとその影響は大きい。このため、セキュリティ監査に用いられるソフトウェアやデータベースには、改ざんや不正使用が行われないよう十分な保護が求められる。

(1) **要求事項**

- セキュリティ監査に用いるソフトウェアやデータベースに対する適切な保護の実施

(2) **実施上のポイント**

- システム監査に用いるソフトウェアやデータベースの利用者環境や開発および運用環境からの隔離

第3部
ISMS 適合性認証制度の概要

13 セキュリティマネジメントにかかる認証制度

セキュリティマネジメントに関する評価･認証制度としては、英国で BS7799 に基づいた制度（以下、BS7799 認証制度）が制定されており、この制度は欧州を中心に認証取得が広がっている。日本においても最近になって認証取得を行う企業が出始めている。

一方、日本国内においても BS7799 に基づいた評価･認証制度（ISMS 適合性評価認証制度）の運用が開始されており、セキュリティマネジメントに対する意識は国際的に高まりつつある。

こういった制度の認証を取得することによるメリットとしては、まず自社のセキュリティ管理体制を見直すことができることに加え、客観的な評価･認証により、顧客に対して自社サービスや製品への安心感や信頼感を与えることができるという点があげられる。

以下では、BS7799 認証制度、および日本の ISMS 適合性評価認証制度について触れていく。

13.1 BS7799 認定制度

13.1.1 制度の概要

BS7799 に基づいて英国で運用されている情報セキュリティマネジメントシステムの評価･認証制度は、英国規格協会内の DISC（Delivering Information Solutions to Customers）という組織で制度管理が行われている。

BS7799 は、パート 1 についてはすでに ISO/IEC 17799 として国際規格化されているが、パート 2 はまだ国際規格化に向けた作業が進行中である。このパート 2 の規格化が完了すれば、BS7799 はさらに国際的に利用されることとなり、本制度もさらに多くの国で採用されるようになるであろう。

13.1.2 認証制度の発足経緯と普及状況

BS7799 認証制度は、英国において 1998 年に発足した。その後、スウェーデン、オランダ、デンマーク、オーストラリアなどでセキュリティマネジメントの標準として採用され、認証制度としてはイギリス、スウェーデン、オランダなどで本制度を導入している。なお、日本でも 2001 年 12 月現在で、NTT データ、日本ユニシスなどの 4 社が取得している。

13.1.3 認定プロセス

認定を受けるまでのプロセス概要は、下記のとおり。

(1) 評価・認証機関への評価の申請

英国では、評価･認証機関が複数存在し、評価･認定を受けたい組織は、まずどの機関へ依頼するのかを決定し申請を行う。日本ではBSIジャパンが唯一の評価･認証機関となっている。

(2) 評価・認証機関による書類審査の実施

下記の項目について記述されている資料を評価･認証機関へ提出し書類審査を受ける。

- セキュリティマネジメントシステムにかかる資料
- 評価･認定の適用範囲に関する資料
- セキュリティマネジメントにかかる管理者数、利用者数
- リスク分析手法にかかる資料

(3) 評価・認証機関による実地監査の実施

セキュリティマネジメントシステムが、実際に適用を行っている現場に正しく導入されているかどうかをチェックする。

(4) 認証書の発行

何らかの問題が見つかれば評価･認証機関より指摘を受け、その指摘に対する改善措置を実施し、それが評価･認証機関によって適合の評価を受けることができた後に評価･認証機関より認定書が発行される。

(5) 認定後のチェックと認定の更新

認定の有効期間は3年であり、更新するためには3年後に評価･認証機関による監査が必要となる。また、認定取得後、1 年ごとに査察訪問によるセキュリティマネジメントのチェックが行われることになる。

13.2 ISMS 適合性評価・認証制度

13.2.1 制度の概要

ISMS 適合性評価･認証制度は、財団法人日本情報処理開発協会（JIPDEC）によって運用が開始されたセキュリティマネジメントに関わる認定制度であり、民間ベースによる第三者認証制度である。

本制度は 2001 年 4 月よりパイロット事業として開始されており、2002 年 4 月から本格運用を実施する予定である。当面は、情報処理サービス業を対象に適合性評価を行うこととしている。

(1) 制度創設の背景

従来、情報システムに対するセキュリティに対して安全対策を実施している事業者を認定す

る制度としては、“情報サービス業情報システム安全対策実施事業所認定制度”（安対制度）があり、旧通商産業省（現在の経済産業省）によって制定され、2001 年 3 月まで運用されてきた。この制度はメインフレームコンピュータ時代に制定された制度であり、制度創設時は、情報処理サービス業の形態が計算センター中心であったことに対し、現在ではインターネット等のオープンネットワーク環境やクライアントサーバー型の環境が中心となりダウンサイジング化と低コスト化により業態が変化してきた。また、ビジネス形態から見ても、ASP や IDC といった新たなネットワークビジネスが登場しているなど、情報処理サービス業の形態が多様化してきている。

そこで、これまでの制度を現在の環境に適合させることが必要となったことから、国際的に整合性のとれた情報システムのセキュリティマネジメントに対する第三者認証制度を確立することとし、第三者認証とすることにより、客観性、信憑性を高めることとした。また、ISMS 適合性評価･認証制度の創設により、日本の情報セキュリティレベル全体の向上にも貢献し、諸外国からも信頼を得られる情報セキュリティレベルを達成するという効果も期待できる。

(2) 目的ならびに対象範囲

ISMS 適合性評価･認証制度は、組織全体の情報セキュリティマネジメントの有効性について、客観的な評価基準を提示するものであり、ネットワークを介してビジネスを行う際の取引相手の情報セキュリティレベルを評価する手段でもある。また、国際標準「ISO/OEC 17799（Code of practice for information security management）」をもとに策定されており、国際的な取引の安全性･信頼性を確保することも目的の1つである。

ISMS 適合性評価･認証制度の対象範囲は、情報処理サービス業（パイロット事業の対象業種）である。情報処理サービス業とは、電子計算機を用いて計算を行う事業および検索を行う事業等が該当する。なお、2002 年 4 月からの本格運用時には、情報サービス業以外へ業種分やへの適用が行われる予定である。

13.2.2 認定スキーム

ISMS 適合性評価･認証制度における認定スキームを、図 13-1に示す。

13.2.3 審査プロセス

ISMS 適合性評価･認証制度の審査プロセスは、

⑴ 見積

⑵ 認証契約の締結／審査準備

⑶ 初回審査

⑷ 認証

⑸ 継続審査／更新審査

からなる。また、予備審査については事業者のオプションであり、初回審査に先だって審査に入る準備ができているかを判定するものである。

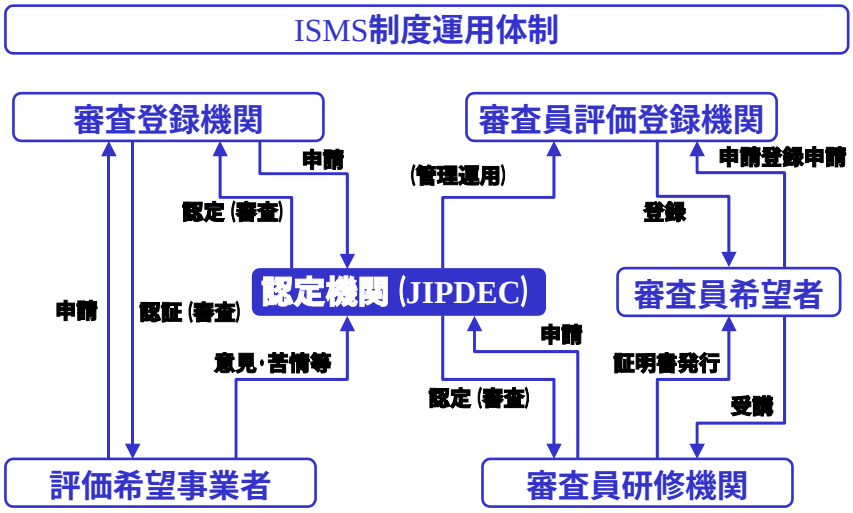

図 13-1　ISMS 適合性評価・認証制度の認定スキーム

(JIPDEC パンフレットより)

(1) 見積り

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、プロセスの複雑さなどがあり、見積を依頼する際には、下記の基本事項をデータを提示する。

- 組織の責任者、所在地、組織の規模等の情報
- 主要な製品、サービス、プロセスに関する情報、ISMS の概要
- 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
  - システムのユーザ数
  - ハードウェア
  - ソフトウェア
  - ネットワーク概要

(2) 認証契約の締結と審査準備

契約の締結にもとづいて審査計画を策定し、審査準備に入る。審査側では、認証基準、審査技法、マネジメントシステムに関する知識や経験を有する者で、受審組織の業種、業務などの専門性、組織が利用する IT などについての専門性を確保するよう審査チームを編成する。

審査機関は、受信組織と協議し、審査日程を決定する。

(3) 初回審査

審査は、ISMS 認証基準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を目的とし、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およびその記録を評価し、適合していることを確認する。

審査の結果、不適合であると評価されたときは、そのことを受審側へ報告するが、不適合である理由については受信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されることが必要となる。

なお、審査は、Stage1（文書審査）と Stage2（実地審査）からなる。

① Stage1（文書審査）

文書審査では、情報セキュリティポリシーや ISMS の目的に添って、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する。同時に、審査側は第 2 段階で焦点を当てる事項を明確にする。

審査の対象は、

- 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 の構造と手順

等である。

② Stage2（実地審査）

実地審査では、受信事業者がそのセキュリティポリシーや目的、手順を確実に遵守していること、および組織が ISMS 認証基準およ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と目的を達成していることを確認する。

審査の対象は、

- リスクアセスメントと ISMS の計画とフレームワーク
- 適用宣言書、情報セキュリティ、セキュリティ目的
- セキュリティパフォーマンスの監視、測定、報告、レビュー
- 情報セキュリティレビュー、マネジメントレビュー、マネジメントの責任
- 情報セキュリティポリシー、リスクアセスメントの結果

等である。

③ フォローアップ

審査において不適合事項が指摘された場合には、フォローアップが必要となる。その処置については、終了会議や報告書に提示されるが、処置の内容としては、

- 不適合事項への対応状況を確認するための追加の審査
- 是正計画の審査
- 維持審査でのレビュー

などがある。

(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を発行する。認証書に記載される事項は、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であり、認証書には、審査登録機関の認証マークと JIPDEC 認定マークが付与される。

なお、認証登録は、初回審査から3年間有効である。

(5) **維持審査と更新審査**

認証を維持するためには、1 年を超えないサイクルで維持審査を実施する必要がある。維持審査では、前回指摘された事項等に対する是正、改善状況の確認、基準への適合状況、維持状況の確認、ISMS の有効性の確認を行う。

また、認証を継続する場合には、更新審査を3年目に実施しなければならない。

(6) **予備審査**

予備審査はオプションであり、受けるかどうかは受審事業者の任意である。また、審査登録機関によって取扱いは異なる。

予備審査では、ISMS 認証基準の要求に基づくレビューを行い、初回審査までに受審側で準備すべき事項を明確化する。また、審査側と受審側との間で ISMS の範囲についての合意を行う。審査技法は、初回審査における文書審査、実地審査と同様の技法が用いられる。

13.2.4 公開情報

ISMS 適合性評価･認証制度に関連する文書については、JIPDEC のホームページにて以下の文書が公開されている（URL http://www.isms.jipdec.or.jp/std/）。

- ISMS 認証基準

  JIS X 5080(国際規格 ISO/IEC 17799:2000)及び英国規格 BS 7799-2:1999 (Specification for information security management system) を参照し、第三者である審査登録機関が本制度の認証を希望する事業者の適合性を評価するための基準。

- ISMS ガイド

  ISMS 認証基準に沿って、解説、例示等を含んで構成されており、審査業務を実施する上での参考ガイド。なお、本書内の例示はあくまでも審査のイメージを伝えることを目的としており審査方法を規定するものではない。

- ISMS 審査登録機関認定基準

  審査登録機関の認定審査及び登録を行う際の認定基準。

- ISMS 審査登録機関認定の手順

  審査登録機関が認定を受けるための手順と、認定を申請する機関及び認定された機関の権利と義務について規定したもの。

- ISMS 審査員研修機関認定基準

  審査員向けの研修を行う研修機関の認定審査及び登録を行う際の認定基準。

- ISMS 審査員研修コース基準

  審査員研修コースの内容について、その要求事項等を定めた研修コースの基準。

- ISMS 審査員研修機関認定の手順

  ISMS 審査員研修機関が認定を受けるための手順と、認定を申請する機関及び認定された機関の権利と義務について規定したもの。

- ISMS 審査員の資格基準

  各審査員（審査員補、審査員、主任審査員）についての資格要件を規定したもの。

- ISMS 審査員登録の手順

  各審査員の資格要件に基づいて評価登録する際の手順を規定したもの。

■ 本報告書の執筆に携わったメンバー（企業名 50 音順）

中部電力株式会社	情報システム部	杉原　武司
株式会社東芝	Net-Ready 推進本部	吉田　元永
日本ＩＢM株式会社	IBM グローバル・サービス	増田　佳正
日本電気株式会社	IT 基盤システム開発事業部	石田　文治
株式会社日立製作所	システム開発研究所	藤山　達也
富士電機情報ｻｰﾋﾞｽ株式会社	情報 SI 事業部	佐藤 美香子
松下電器産業株式会社	東京支社	網野　幾夫
株式会社メイテツコム	マルチメディア事業部	新保　尚二
電子商取引推進協議会		重松　孝明
電子商取引推進協議会		川村　尚哉

平成 14 年 3 月発行
発行：電子商取引推進協議会
東京都港区芝公園 3-5-8
機械振興会館 3F
Tel　03-3436-7500
e-mail　info@ecom.jp