第3章　セキュリティ

3.1　情報セキュリティ

情報セキュリティとは、企業・組織における情報資産を不正侵入、情報漏えいなどから保持することをいいます。

情報セキュリティの三大要素としては、「機密性」、「完全性」、「可用性」があります。

・機密性…権限の範囲で使用させること
・完全性…情報が正しく保全され完全であること
・可用性…いつでも適切に効率よく利用されること

3.1.1　情報セキュリティにおけるリスクマネジメント

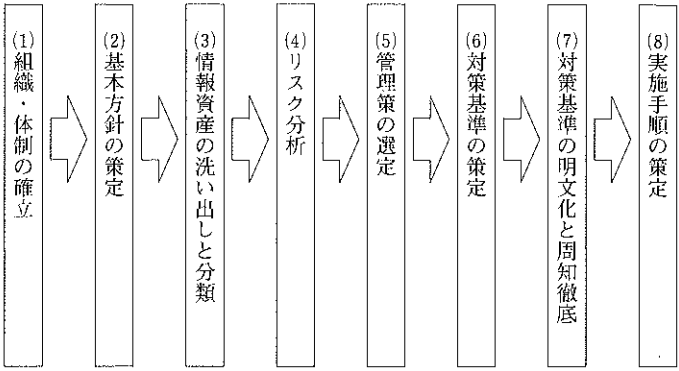
リスク項目	リスク内容
リスクの費用対効果	情報セキュリティ対策の費用＜守るべき情報資産の価値＞
リスクマネジメントサイクル	・リスクの分析 ・リスク処理策の選定 ・リスク処理の実施・運用 ・リスク処理結果の監視・評価
リスクのコントロール	・抑止のコントロール ・予防のコントロール ・発見のコントロール ・修復のコントロール
脅威から生じるリスク	・社会的信用の失墜リスク ・営業損失リスク ・機会損失リスク ・損害賠償の請求リスク

3.1.2　情報セキュリティポリシー

情報セキュリティポリシーとは、企業や組織において実施する情報セキュリティ対策の方針や行動指針を定めたものです。

情報セキュリティポリシーには、社内規程といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、ならびに情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するのが一般的です。

(1) 情報セキュリティポリシーの実施サイクル



(2) 情報セキュリティポリシーの内容

情報セキュリティポリシーでは、「基本方針」、「対策基準」、「実施内容」の三階層で構成されることが一般的です。

基本方針には、組織や企業の代表者による「なぜ情報セキュリティが必要であるのか」や「どのような方針で情報セキュリティを考えるか」、「顧客情報はどのような方針で取り扱うのか」といった宣言を記述します。

対策基準には、実際に情報セキュリティ対策の指針を記述します。多くの場合、対策基準にはどのような対策を行うのかという一般的な規定のみを記述します。

実施内容には、それぞれの対策基準ごとに、実施すべき情報セキュリティ対策の内容を具体的に記述します。

参考資料　独立行政法人情報処理推進機構 (IPA)

3.1.3　脅威

情報システム等に影響を与え、情報資産の損失を発生させる要因を「脅威」といいます。

脅威区分	脅　威　内　容
外部からの脅威	不正アクセス、なりすまし、盗聴、サーバ攻撃 不正配布、混入（コンピュータウイルス等）、Webの書換え 建物への侵入、立ち入り 浸水、冠水、爆発、火災、震災
内部からの脅威	情報の横流しや漏えい システムへの不正行為 コンピュータウイルス感染や不正配布・混入 情報システムの機器障害

3.1.4　脆弱性

脅威によるシステムや管理上の不備を「脆弱性」といいます。

脆弱性区分	脆　弱　な　内　容　と　対　策
IT機器・システム製品	除去する（取除き無用化する） 極小化する（減少化する） 監視する（つけ込まれないように監視する）
システム・ソフト製品	セキュリティ仕様の不備 セキュリティ構築の不備 セキュリティ運用の不備

3.1.5　必要な情報セキュリティ対策

トラブル	対　　策
ウイルス感染	ウイルス対策ソフトの導入 OSのアップデート Webブラウザのセキュリティ設定 メーラのセキュリティ設定
災害などによる機器障害	バックアップ 無停電電源装置の導入 設備の安全管理
不正侵入	パスワード管理 ファイアウォールの導入 不正侵入検知システムの導入 OSのアップデート ソフトウェアのアップデート
情報漏えい	ファイアウォールの導入 顧客データの管理 資料廃棄ルールの徹底 メディア、機器の廃棄ルールの徹底 無線LANのセキュリティ設定 ユーザ権限の管理 パスワード管理

3.2　個人情報保護

個人情報保護基本法の制定は、1980年OECD理事会勧告を経て2003年5月30日に公布されました。これにより個人情報取扱事業者は同法の業務規定を遵守する必要があります。本人の求めに応じて個人情報の開示、訂正、利用停止や苦情を適切に処理することが要求されるなどの取扱いが制定されています。

3.2.1　個人情報の定義

(1) 個人情報とは

生存する個人に関する情報であって、氏名、生年月日、個人別に付された番号、記号、符号、画像もしくは音声により本人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）を指します。また故人に関する情報であっても、当該情報が遺族等の生存する個人に関する情報でもある場合には、生存する個人を本人とする情報として、個人情報に当たることになります。

(2) 本人とは

この個人情報の持ち主をいいます。

(3) 業務上の個人情報とは

企業で取扱う個人情報は、外部から収集した情報、お客様からお預かりした情報や、社員の情報など全て含みます。

「例」・外部収集した情報：顧客管理台帳、受講者名簿、年賀状リスト等
・お客様からお預かりした情報：個人情報を含むデータやファイル等
・社員の情報：履歴書、各種届出、給与・賞与、税金等

3.2.2　個人情報保護の重要性

日常の業務では、様々な局面で個人情報を扱います。個人情報保護の重要性を十分認識し、お客様からお預かりした個人情報や社員情報を的確に管理するためのマネジメントシステムを構築し運用する必要があります。

業務に携わる全ての人が、個人情報の重要性をしっかり認識し、外部から収集した情報はもちろん、社内の個人情報も漏れることがないよう常に厳重な注意を払うことが大切です。

3.2.3　個人情報漏えいによる不利益

個人情報は一度社外に漏れてしまうと、その後の使われ方について追跡調査は不可能であり、回収することが非常に困難なため、どのような被害に遭遇するとも限りません。

「例」・ダイレクトメールや勧誘の電話に悩まされる
・クレジットカードなどの偽造により悪用され、覚えのない多額な請求書が送られてくる

不注意による個人情報漏えいが、本人に与える不利益だけでなく、企業の社会的信用の失墜、業務停止、賠償被害など、ひいては業界全体のイメージダウンに繋がり、産業の成長に大きな影響を与えることになります。

3.2.4　個人情報保護における規程

(1) プライバシーマーク制度

プライバシーマーク制度とは、一般財団法人日本情報経済社会推進協会（JIPDEC）により創設・制定され、JIS Q 15001に準拠した個人情報の適切な保護を講じている民間企業に対し、その旨を示すプライバシーマークを付与する制度です。

(2) 企業における規程の作成と運用

企業においては個人情報の収集・利用・提供等の取扱い方法別に、個人情報保護に関するコンプライアンスを策定します。このコンプライアンスは、社員が日常の業務において様々な個人情報を扱う上で基本的な考え方を示すと共に、情報の収集、利用、提供、管理についての基本的なルールやお客様からの開示、訂正、削除要求に対するルールを規定します。

3.2.5　個人情報の取扱に関する概要

(1) 個人情報の収集について

・個人情報の収集は、収集する企業の事業範囲内であらかじめ個人情報を取扱う目的を明確にして行います。
・次に示すような個人情報は、原則収集できません。
　（ア）思想、信条及び宗教
　（イ）人種及び民族
　（ウ）犯罪歴
　（エ）社会的差別の原因となる社会的身分
・個人情報の収集は、法律の範囲内で、公正な手段によって行います。
・個人情報を収集する時は、本人が取扱目的を確認できるようにします。
・本人以外からの個人情報の収集は、以上の制限のほか、本人の利益が侵害されるおそれのない場合に限り可能です。

(2) 個人情報の利用及び提供について

・個人情報の利用又は提供は、原則として収集したときの取扱目的の範囲内で行います。
・収集したときの取扱目的の範囲を超えて個人情報の利用や提供をするときは本人の同意を得ること、また本人にその目的を確認する機会を与えること等により、原則として本人の了解のもとに行います。
・収集したときの取扱目的の範囲を超える個人情報の利用や提供は、再度本人へ、利用の目的を変更した確認を取る必要があります。

(3) 個人情報の適正管理について

・個人情報を目的の範囲内で正確に取扱うと共に最新の状態に保つ必要があります。
・個人情報の漏えい、破壊及び滅失の防止その他個人情報の適切な管理のため必要な措置を講じなければなりません。
・個人情報を取扱う人は、業務に関して知り得た個人情報の内容をみだりに他人に知らせたり、又は不当な目的に使用することのないよう、十分な注意を払い業務を行わなければなりません。
・個人情報の処理を外部に委託するときは、原則として委託契約で個人情報の適切な取扱いについて受託者が取らなけ

ればならない措置を明らかにしておきます。
・保有する必要のなくなった個人情報は、確実に、かつ、速やかに廃棄します。

(4) 自己情報の開示等について
・本人から自己情報について開示を求められたときは、原則としてこれに応じなければなりません。
・本人から自己情報について訂正を求められたときは、必要な確認を行い、原則としてこれに応じなければなりません。
・本人から自己情報を利用し、又は提供することを拒まれたときは、原則としてこれに応じなければなりません。
・個人情報の取扱いに関する相談窓口を設置し、本人から自己情報の取扱いについて苦情等があったときは、適正に処理します。

(5) 責任体制について
・経営者は、コンプライアンスに定められた内容の実効性を確保するため、個人情報の管理者を指名します。
・個人情報の管理者は、コンプライアンスに定められた事項を遵守するとともに、個人情報の取扱いに係る規程の整備や継続的見直し、個人情報を取扱う者に対する研修の実施等、必要な措置をとる責任を負います。

(6) 監査
・個人情報保護システムについて、少なくとも年1回、コンプライアンスの規程に定める事項の遵守状況について監査を実施しなければなりません。
・監査の結果、コンプライアンスに不都合があった場合や、規程が遵守されていないものについて、改善をする必要があります。

(7) 個人情報保護罰則規定
個人情報取扱事業者は法の定める義務に違反し、この件に関する主務大臣の命令にも違反した場合、「6ヶ月以下の懲役または30万円以下の罰金」の刑事罰が課せられます。

3.2.6　個人情報流出事件について

近年、個人情報の漏えい事故が相変わらず出ております。注意喚起の目的で、最近の主な個人情報漏えい事件の流出件数が多いものに着眼し、抽出しました。ほとんどがヒューマンエラー（人的な原因）です。事故を起こさない為に、法律や基準を遵守し、情報の取扱いに注意しましょう。

事故事例一覧

会　社	内　　容
通信教育 出版会社	内容：顧客情報 件数：2,895万件 原因：DB管理者による不正行為
ソフトウェア 関連会社	内容：顧客情報 件数：290万件 原因：不正アクセス
都市銀行	内容：顧客情報 件数：148万件 原因：元部長代理による持出　約5万人分売却
音楽音響 機器販売 メーカー	内容：顧客情報 件数：10万件 原因：中国からの不正アクセス
情報処理 メーカー	内容：県職員の情報 件数：1万5千件 原因：私物PC Shareウイルスに感染
生命保険 会　　社	内容：顧客情報 件数：15万件 原因：PC置き引き
自動車 メーカー	内容：顧客情報 件数：538万件 原因：不明

3.2.7　個人情報漏えいのリスクへの対策

個人情報漏えいのリスクを削減する為に、以下の動作を確実に行いましょう。

・業務情報へのアクセス権限を明確にし、担当外業務の資料など、業務上で不必要な情報にアクセスさせない。
・個人所有のノートPCやストレージメディア（USBメモリなど）の持ち込み、使用を制限させる。
・業務外での電子メールやインターネットの使用を制限する。
・やむを得ず社外に持ち出す際にはパスワードの設定や暗号化を行い、第三者に渡っても参照できなくする。

3.3　ISMS（Information Security Management System）

情報セキュリティを維持するためには、企業や組織がセキュリティ方針を定め自らのリスクアセスメントにより必要なセキュリティレベルを構築、運用して継続的に資源配分しマネジメントすることが必要です。

2013年10月のISO/IEC27001の改定に伴い2014年3月にJIS（JISQ 27001）も改定されました。

情報セキュリティマネジメントシステムの国際規格で主として次の各セクションで構成されています。

要求事項No.	セクション名	PDCA
1	適用範囲	—
2	引用規格	—
3	用語及び定義	—
4	組織の状況	Plan（計画）
5	リーダーシップ	
6	計画	
7	支援	
8	運用	Do（実行）
9	パフォーマンス評価	Check（評価）
10	改善	Act（改善）

要求事項Noは、規格書の項番

毎年、「差分」のマネジメント実践によりスパイラルアップPDCAを目指す。

3.3.1　ISO／IEC 27001認証登録のメリット

(1) 競争優位性

ISMS認証取得は、顧客先発注条件の主要な要素となっています。

(2) 顧客からの信頼性

アウトソーサーが情報セキュリティマネジメントを実施し、ISMS認証を受けていれば、情報保護の予防策としては高い評価を得ることになります。

(3) コンプライアンス（法令遵守）

ISMSのマネジメントシステム構築と運用により、法令や各種規則などのルール、および社会的規範を守ることができます。

3.3.2　ISMSの構築

事業の活動全般と直面するリスクを考慮して、構築手順に従い策定し文書化されたISMSを確立、導入、運用、監視、見直しおよび維持を行い継続的に改善することが必要です。

箇　条	概　要
4 組織の状況	組織を取り巻く内外の状況や利害関係者のニーズ及び期待を理解、決定しそれらを考慮に入れたうえでISMSの適用範囲を定める事が求められている
4.1組織及びその状況の理解	
4.2利害関係者のニーズ及び期待の理解	
4.3情報セキュリティマネジメントシステムの適用範囲の決定	
4.4情報セキュリティマネジメントシステム	
5 リーダーシップ	ISMSを推進し、関係者の意識向上を図るためには、トップマネジメントの強力なリーダーシップが不可欠である。トップマネジメントの果たす役割について規定している
5.1リーダーシップ及びコミットメント	
5.2方針	
5.3組織の役割、責任及び権限	
6 計画	ISMSにおけるリスク及び機会を決定し、情報セキュリティアセスメント、情報セキュリティリスク対応のプロセスを適用する事が求められている 付随書Aの管理策と組織が適用した管理策を比較し除外した場合にはその理由を適用宣言書に記載することが求められている
6.1リスク及び機会に対処する活動	
6.1.1一般	
6.1.2情報セキュリティリスクアセスメント	
6.1.3情報セキュリティリスク対応	
6.2情報セキュリティ目的及びそれを達成するための計画策定	
7 支援	要求される文書類を文章化し、管理、維持しながら要員の力量、利害関係者との反復的かつ必要に応じたコミュニケーションを確立することを通じたISMS運用の支援について規定している
7.1資源	
7.2力量	
7.3認識	
7.4コミュニケーション	
7.5文書化した情報	
8 運用	情報セキュリティの要求事項を実現するために必要なプロセス群の策定、導入、実施及び管理について規定、また不可欠な情報セキュリティリスクアセスメント、情報セキュリティリスク対応を規定している
8.1運用の計画及び管理	
8.2情報セキュリティリスクアセスメント	
8.3情報セキュリティリスク対応	
9 パフォーマンス評価	情報セキュリティパフォーマンスの評価（監視、測定、分析、評価）、内部監査及びマネジメントレビューについて規定している
9.1監視、測定、分析及び評価	
9.2内部監査	
9.3マネジメントレビュー	
10 改善	不適合発生時の処置及びとった処置の文章化とISMSの適切性、妥当性、有効性の継続的改善について規定している
10.1不適合及び是正処置	
10.2継続的改善	

参考資料　一般財団法人日本情報経済社会推進協会（JIPDEC）

3.3.3　他のマネジメントシステム規格との共通化

HLS（ハイレベルストラクチャー）は、全てのISOのマネジメントシステムの要求事項を統一（共有化）し、複数のマネジメントシステムを導入する負荷を軽減する事を目的に開発されました。（2012年度より順次規格改定）

(1) 国際標準機構（ISO）マネジメントシステムの種類

ISO22301　事業継続マネジメントシステム
ISO27001　情報セキュリティマネジメントシステム
ISO14001　環境マネジメントシステム
ISO9001　品質マネジメントシステム
ISO20000　ITサービスマネジメントシステム
邦訳版は、日本工業規格「JISQ xxxxx」として発行されています

xxxxx：上記ISOに続く数値

High Level Structure:HLS マネジメントシステム規格共通の基本構造

ISO22301	ISO27001	ISO14001	ISO9001	ISO20000
BCMS	ISMS	EMS	QMS	ITSMS

略称

BCMS：Business Continuity Management System
　　事業継続マネジメントシステム
ISMS：Information Security Management System
　　情報セキュリティマネジメントシステム
EMS：Environmental Management System
　　環境マネジメントシステム
QMS：Quality Management System
　　品質マネジメントシステム
ITSMS：IT Servise Management System
　　ITサービスマネジメントシステム