目　　次

第１章　情報セキュリティマネジメントシステム要求事項
対応文書一覧

規格項目	財団法人日本情報処理開発協会 ＩＳＭＳ規準要求事項 (Ver.2.0)	文書番号	文書名称
第4 情報セキュリティ マネジメントシステム			
1. 一般要求事項	組織は、自らの事業の活動全般及びリスク全般を考慮して、文書化されたＩＳＭＳを構築、導入、維持し、かつこれを継続的に改善すること。本基準で使われるプロセスは、図1に示すＰＤＣＡモデルに基づいている。	作成文書全般	
2. ＩＳＭＳの確立及び運営管理 (1) ＩＳＭＳの確立	組織は次の事項を実施すること。 ①事業の特徴、組織、その所在地、資産及び技術の観点から、ＩＳＭＳの適用範囲を定義する。 ②事業の特徴、組織、その所在地、資産及び技術の観点から、次の事項を満たすＩＳＭＳの基本方針を策定する。 (ア) ＩＳＭＳの目標を設定するための枠組みを含み、情報セキュリティに関する全般的な方向性及び行動指針を確立する。 (イ) 事業上の要求事項及び法的又は規制要求事項、並びに契約上のセキュリティ義務を考慮する。 (ウ) ＩＳＭＳを確立し、維持するために必要な戦略上の視点からみた組織環境、並びにリスクマネジメントのための環境を整備する。 (エ) リスクを評価するための基準を確立し、定義されたリスクアセスメントの構造を確立する（第4　2.(1)③参照）。 (オ) 経営陣による承認を得る。 ③リスクアセスメントについての体系的な取組方法を策定する。 当該ＩＳＭＳに適しており、また、明確にされた事業上の情報セキュリティ要求事項、並びに識別された法的及び規制要求事項に適したリスクアセスメントの方法を特定する。リスクを受容可能な水準にまで軽減するために、ＩＳＭＳの基本方針及び目標を設定する。また、リスクを受容するための基準を定め、受容可能なリスクの水準を特定する(第5　1.⑥参照)。 ④リスクを識別する。 (ア)当該ＩＳＭＳの範囲内の情報資産及び情報資産の責任者を特定する。 (イ)それらの情報資産に対する脅威を明確にする。 (ウ)脅威によって利用されるおそれのある脆弱性を明確にする。 (エ)機密性、完全性及び可用性の喪失が情報資産に及ぼすかもしれない影響を明確にする。 ⑤リスクアセスメントを実施する。 (ア) セキュリティ障害に起因して想定される事業上の損害を評価する。その際に、当該情報資産の機密性、完全性又は可用性の喪失による潜在的な影響を考慮する。 (イ) 一般に認識されている脅威及び脆弱性の観点から起こりうるセキュリティ障害などの現実的な発生可能性、情報資産に関連する影響、並びに現在実施されている管理策を考慮してアセスメントを実施する。 (ウ) リスクの度合いを算定する。	ＩＳＭ-Ａ-００１ ＩＳＭ-Ａ-００２ ＩＳＭ-Ａ-００３ ＩＳＭ-Ａ-００４ ＩＳＭ-Ａ-００５ ＩＳＭ-Ａ-００６ ＩＳＭ-Ａ-００７ ＩＳＭ-Ｂ-００１ ＩＳＭ-Ｃ-００１ ＩＳＭ-Ｄ-００１	情報セキュリティ基本方針 情報資産棚卸リスト 情報資産と企業経営に対する被害との関連表 リスクの識別表 リスクアセスメント結果報告書 リスク対応計画書 適用宣言書 情報セキュリティ規定 財産の分類および管理に関する手順書 情報セキュリティマネジメントマニュアル

規格項目	財団法人日本情報処理開発協会 ISMS規準要求事項(Ver.2.0)	文書番号	文書名称
	(エ)第4 2.(1)③で確立した評価基準を使用して、当該リスクについて、受容できるか、対応が必要かを決める。 ⑥リスク対応についての選択肢を明確にし、評価する。 考えられるリスク対応に関する選択肢として、次のような事項が含まれる。 (ア)適切な管理策を採用する。 (イ)リスクを保有する。リスクが組織の基本方針及びリスクの受容のための評価基準を明らかに満たす場合には、意識的かつ客観的に当該リスクを受容する(第4 2.(1)③参照)。 参考 リスクの保有(risk retention):あるリスクから損失の負担、又は利得の恩恵の受容。[TRQ0008:2003を参照] (ウ)リスクを回避する。 (エ)リスクを移転する。関連する事業上のリスクを、例えば、保険会社又は供給者という他者に移転する。 ⑦リスク対応に関する管理目的及び管理策を選択する。 本基準の附属書「詳細管理策」から、適切な管理目的及び管理策を選択する。また、この選択については、リスクアセスメント及びリスク対応プロセスの結果に基づいてその妥当性を示すこと。 参考 附属書「詳細管理策」のリストは組織が必要とする管理目的及び管理策の全てとは限らないので、組織は必要に応じて追加の管理目的及び管理策を選択してもよい。 ⑧適用宣言書を作成する。 第4 2.(1)⑦で選択した管理目的及び管理策、並びにこれらを選択した理由を文書化し、適用宣言書に含めること。また、附属書「詳細管理策」に記載する管理目的及び管理策の中から適用除外としたものは記録すること。 ⑨残留リスクに対する経営陣の承認及び当該ISMSを導入し、運用するための許可を得る。		
(2) ISMSの導入及び運用	組織は次の事項を実施すること。 ①情報セキュリティについてのリスクを管理するための、経営陣の適切な活動、責任及び優先順位が明確にされたリスク対応計画を策定する(第5参照)。 ②識別された管理目的を達成するためにリスク対応計画を実施する。これには、必要な資金の拠出を考慮し、役割及び責任を割り当てることを含む。 ③当該管理目的を達成するために第4 2.(1)⑦で選択した管理策を実施する。 ④教育・訓練及び認識させるためのプログラムを実施する(第5 2.(2)参照)。 ⑤運用を管理する。 ⑥経営資源を管理する(第5 2.参照)。 ⑦セキュリティ事件・事故を迅速に検出し、それらに対して迅速な対応を行うことのできる手順及びその他の管理策を実施する。	ISM-A-006 ISM-B-001 ISM-C ISM-D-001	リスク対応計画書 情報セキュリティ規定 各手順書 情報セキュリティマネジメントマニュアル

第２章　　モデル企業におけるシステム構築・認証取得概要（株式会社ウェブパークの場合）

この章では、事例として株式会社ウェブパーク（仮名）の情報セキュリティマネジメントシステムに対する取組みを紹介する。

(株)ウェブパークは 2004 年９月に BS7799-2 及び JIPDEC/ISMS（Ver.2.0）の認証を取得した。

2004 年２月に情報セキュリティマネジメントシステムの構築をスタートし、認証審査は 2004 年７月に行われた。

１．(株)ウェブパークの概要

（１）設立

1998 年７月

（２）事業内容

○　デジタルコンテンツ（Web コンテンツ、音声、動画、プログラム、グラフィック）の企画・制作
○　サーバー管理

（３）資本金

5000 万円

（４）従業員数

約 100 名

（５）組織

社長 ― 管理本部	経理・人事・法務
― MFS 本部	総務・マネジメントシステム・後方支援
― 営業部門	営業・企画・ディレクション
― 制作部門	Web コンテンツの制作
― 音声事業部	音声の営業から制作・検品まで
― IT 事業部	プログラミング、サーバー管理
― アウトソーシング事業部	某大規模 Web サイトの下請け制作
― 品質保証室	Web コンテンツの検品

２．取得の目的

(株)ウェブパークが ISMS の取得を目指すこととなった目的を紹介する。

（取得の目的）

○　属人的管理から、プロセスの管理に移行する。
○　情報セキュリティにおける社内の価値観を一つにする（共通言語化する）。
○　主体的継続的改善メカニズムを組織的に持ち、問題が生じた場合の是正処置、今後の予防処置を PDCA のサイクルで回す仕掛けを作る。

（期待する効果）

○　スタッフが安心して業務遂行できる土壌の提供。
○　顧客との信頼関係強化。
○　競争優位性。

（今後の方針、取組み）

１．情報セキュリティというテーマを PDCA のサイクルで回す。
２．現状のパフォーマンスを数値化する。
３．数値を見極めながら、目標管理制度（MBO）を入れる。
４．目標管理の結果を把握しながら、継続的改善を繰り返す。
５．考えられる予防処置をマネジメントシステムに追加しながら、マネジメントシステム全体を加速度的にレベルアップする。

3．　構築、認証審査までのスケジュール

(株)ウェブパークは 2004 年２月に活動を開始し、６ヵ月後に認証審査を受けた。諸事情により、短期間で審査を迎えることになったが、本来ならば仮運用をした後内部監査などにより問題点の是正を行い、さらに３ヵ月程度運用してから審査に臨んだほうがよいだろう。

参考までに、表１は認証取得までの(株)ウェブパークのスケジュールである。

表１　ISMS 認証取得スケジュール

2001 年 / 活動内容	2 月	3 月	4 月	5 月	6 月	7 月	8 月	9 月
セキュリティポリシー策定	◆							
情報資産の棚卸		◆						
適用範囲の確定		◆						
リスク評価		◆						
リスクマネジメント		◆						
適用宣言書作成		◆						
予備審査			◆					
規定・手順書作成				◆				
マネジメントマニュアル作成	→	→	→	→	→			
教育					◆			

以下、製品版をご覧ください

第３章　システム構築実例解説

１．セキュリティポリシー

●　作り方

管理枠組みの第一段階として、セキュリティポリシーを作成する。
セキュリティポリシーの位置づけは、経営陣によって情報セキュリティの管理に関する組織の取組方法を宣言することにある。取組方法と言っても大きな方針でよく、詳細な内容は、マネジメントシステム全体のことに関しては情報セキュリティマネジメントマニュアルに、詳細管理策については各手順書に譲り、セキュリティポリシーはポイントとなる項目についての要約的な内容でよい。

では、ポイントとなる項目とは何だろうか。
セキュリティポリシーの内容に関して BS7799 Part2 で要求しているのは、「情報セキュリティのための経営陣の指導及び支援を規定すること」ということだけであるが、Part1 で、内容に含めたほうがよい事項があげられているので、これを参考にするとよい。下記は Part1 からの引用である。

a) 情報セキュリティの定義、その目的及び適用範囲、並びに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。
b) 情報セキュリティの目標及び原則を支持する経営陣の意向声明書。
c) 組織にとって特に重要なセキュリティ基本方針、原則、標準類及び適合する要求事項の簡潔な説明。それらの例を、次に示す。
1)法律上及び契約上の要求事項への適合。
2)セキュリティ教育の要求事項。
3)ウイルス及び他の悪意あるソフトウェアの予防及び検出。
4)事業継続管理。
5)セキュリティ基本方針違反に対する措置。
d) セキュリティの事件・事故を報告することも含め、情報セキュリティマネジメントの一般的責任及び特定責任の定義。
e) 基本方針を支持する文書（例えば、特定の情報システムについてのより詳細なセキュリティ個別方針及び手順又は利用者が従うことが望ましいセキュリティ規則）の参照情報。

次に示す(株)ウェブパークのセキュリティポリシーは、これらをふまえて作成したものである。

● セキュリティポリシーの例

資料１.

IMS-A-001
株式会社　ウェブパーク

情報セキュリティ基本方針

制定：塚田　弘二 2004年2月15日

(株)ウェブパークは、お客様との信頼関係の上に成り立っています。当社がお客様の信頼を保持し、より良いサービスを提供していくためには、情報資産に対して適切な安全対策を実施し、紛失、盗難、不正使用から保護しなくてはなりません。

そのためには、物理的、技術的なセキュリティ強化はもちろんのこと、従業員がセキュリティに対して高い意識をもち、セキュリティを尊重した行動をとることが最も重要だと考えます。

ここに「情報セキュリティ基本方針」を定め、当社が保有する情報資産の適切な保護対策を実施するための指針とします。経営層を含む全従業員は、本趣旨を理解し、当社の情報セキュリティ手順書の内容を熟知・遵守します。

1.【情報セキュリティの定義】
情報セキュリティとは、情報の機密性・完全性・可用性を維持することと定義する。

2.【適用範囲】
当社の管理下にある、すべての業務活動に関わる情報を対象とする。

3.【管理者の任命と義務】
会社は情報セキュリティ委員会を設置するものとする。情報セキュリティ委員会は、各部門からタスクフォースを任命する。任命されたタスクフォースは、情報を不正な暴露、改ざんやサービスの妨害から保護すること。

4.【セキュリティ対策】
会社は、取り扱う情報に応じて、最適な情報セキュリティ対策を講ずるものとする。

5.【従業員の義務】
アルバイト社員を含む全従業員は、「情報セキュリティ基本方針」、「情報セキュリティ規定」および情報セキュリティの手順書に準じて行動すること。もし、違反した場合には、従業員罰則規定を適用するものとする。

6.【情報の特定と対策】
情報セキュリティ委員会は、企業秘密情報やプライバシー関連情報を特定する。特定した情報に対して、その保護のために最適な情報セキュリティ対策を講じるものとする。

以下、製品版をご覧ください

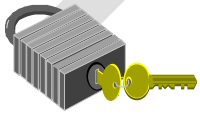
第４章　情報セキュリティ規定実例

情報セキュリティ規定は、リスクアセスメントおよびリスク対応プロセスの結果、規格の詳細管理策の中から選択することになった管理目的と管理策の内容を列挙したものである。各管理策を実行するために具体的な手順の必要なものは手順書が作成され、その手順書の名称が参照先として情報セキュリティ規定に記載されている。

(株)ウェブパークの情報セキュリティ規定を次に示す。

情報セキュリティ規定

Ver1.00



管理番号：ISM-B-001-1

発　行　：２００４年　４月　１日
改　訂　：　－
作成者　：情報セキュリティ委員　井上　義春／小森　裕子
承認者　：代表取締役　　塚田　弘二

制定／改訂履歴表

版数	制定／改訂内容	改訂頁	作成者	承認者	発行日／改訂日
1	制　定	－	井上　義春 小森　裕子	塚田　弘二	2004.04.01

目　　次

1．目的と位置づけ

BS7799-2:2002及びISMS認証基準Ver.2.0の規格に適合した当社の情報セキュリティマネジメントシステムを運営するために必要な規定をここで定める。

2．適用範囲

当社の管理下にある、すべての業務活動に関わる情報資産を対象とする。

3．情報セキュリティ基本方針

3.1　情報セキュリティ基本方針

【目的】

管理目的：情報セキュリティのための経営陣の指針および支持を規定するため。

【規定】

(1) 基本方針文書は、経営陣によって承認され、適当な手段で、全従業員に公表し、通知すること。

(2) 基本方針は、依然として適切であることを確実にするために、定期的に、また影響を及ぼす変化があった場合に、見直すこと。

【関連文書】

情報セキュリティマネジメントマニュアル

4．組織のセキュリティ

4.1　情報セキュリティ基盤

【目的】

組織内の情報セキュリティを管理するため。

【規定】

(1) セキュリティを主導するための明りょうな方向付け及び経営陣による目に見える形での支持を確実にするために、運営委員会を設置すること。運営委員会は、適切な責任分担及び十分な資源配分によって、セキュリティを促進すること。（関連文書：情報セキュリティマネジメントマニュアル）

(2) 大きな組織では、情報セキュリティの管理策の実施を調整するために、組織の関連部門からの管理者の代表を集めた委員会を利用すること。（関連文書：情報セキュリティマネジメントマニュアル）

(3) 個々の資産の保護に対する責任及び特定のセキュリティ手続の実施に対する責任を、明確に定めること。（関連文書：財産の分類および管理に関する手順書／スタッフのセキュリティに関する手順書）

(4) 新しい情報処理設備に対する経営陣による認可手続を確立すること。（関連文書：物理的セキュリティ施策／ハードウェア設置に関する手順書）

(5) 専門家による情報セキュリティの助言を内部又は外部の助言者から求め、組織全体を調整すること。（関連文書：情報セキュリティマネジメントマニュアル）

(6) 行政機関、規制機関、情報サービス提供者及び通信事業者との適切な関係を維持すること。（関連文書：情報セキュリティマネジメントマニュアル）

(7) 情報セキュリティ基本方針の実施を、他者がレビューすること。（関連文書：情報セキュリティマネジメントマニュアル）

4.2　第三者によるアクセスのセキュリティ

【目的】

第三者によってアクセスされる組織の情報処理設備および情報資産のセキュリティを維持するため。

【規定】

(1) 組織の情報処理施設への第三者のアクセスに関連づけてリスクアセスメントを実施し、適切なセキュリティ管理策を実施すること。

(2) 組織の情報処理施設への第三者アクセスにかかわる取決めは、必要なセキュリティ

財産の分類および管理に関する手順書
（ISM-C-001）作成のポイント

1. リスクアセスメントの前段階となる情報資産の棚卸し・分類に関する手順である。組織の情報資産を適切なレベルで保護するためには、この手順をしっかり作る必要がある。全従業員が参照する。

2．適用範囲内にあるすべての情報資産を不足なく洗い出すための手順を設ける。

3．すべての情報資産に関して責任者を明確にする手順を盛り込む。

4．リスクアセスメントの前段階として、情報資産に対する重要度、脅威、脆弱性を実際の所有者から洗い出すための手順を盛り込む。

5．情報資産の分類体系を定める。

【目的】

当文書は、(株)ウェブパーク（以下ウェブパーク）情報セキュリティ基本方針とそれに基づく情報セキュリティマネジメントシステムの要求事項に基づいて、社内の全情報資産の目録を作成し、総括的に分類を行う作業の手順を示し、作業の責任と成果物として発生する記録を明らかにするものである。

【主管部門】

情報セキュリティ委員会を主管組織とする。

【適用範囲】

ウェブパークの管理下にある､すべての業務活動に関わる情報資産を適用範囲とする。

【責任】

当文書に明記される情報資産の棚卸し作業は全従業員が参加して行い、情報資産の分類作業は、情報セキュリティ委員会が実施し、その責任を負うものとする。

【手順】

【1】情報資産の棚卸し

情報セキュリティ委員会は、毎年4月と10月に、下記の手順で全社の情報資産の情報を収集し、社で保有する財産目録を作成する。

1)情報セキュリティ委員会は、情報資産の棚卸しをする際に、全従業員に情報資産の入力フォームを提示する。

2)全従業員は、各個人に管理を任されている情報資産を入力フォームに列挙し、それぞれ情報セキュリティ委員会が提示した分類名のいずれかに落とし込む。また、情報資産の内容、情報資産の形態、保管場所、所有者、重要度、脅威・脆弱性を入力する。

3)各所属のセキュリティタスクフォースのメンバーは、所属の全従業員が情報資産を不足なく入力したのを確認し、また、自分の所属部署が組織として貸与され管理している情報資産を入力フォームに列挙し、それぞれ情報セキュリティ委員会が提示した分類名のいずれかに落とし込む。情報資産の内容、情報資産の形態、保管場所、所有者、重要度、脅威・脆弱性を入力する。

4)情報セキュリティ委員会は、全部門が情報資産を不足なく入力したのを確認し、また上記2)、3)で収集された情報に、ソフトウェア、物理財産、サービス等を含めた全社共有の情報資産を追加し、「情報資産棚卸リスト」を作成する。

- 情報資産分類名

分類名	解説
サーバー収集個人情報	ホスティング契約で預かった顧客のフォームなどから収集された個人情報のことで、CSV 形式のファイルなどに蓄積される
顧客預かりコンテンツ	ホスティング契約で預かった顧客のコンテンツ。HTML やイメージ、CGI プログラムなど、ウェブパークのサーバーで稼動している顧客コンテンツ
開発/制作済みコンテンツ	制作、開発の完了した HTML やイメージファイル、CGI プログラムなど
開発/制作中コンテンツ	現在制作、開発中の HTML やイメージファイル、CGI プログラムなど
デモ公開コンテンツ	公開前に、デモ用途で限定公開されているコンテンツ。主にデモサーバーに置かれているもの。同じコンテンツのバックアップが個人 PC にあっても、それは制作中もしくは制作済みコンテンツとなることに注意
開発コンテンツバックアップ	過去に開発を行ったもので、マスターとしてバックアップを行っている場合の分類。マスターでなければ開発済みコンテンツに分類する
社内開発/制作中コンテンツ	自社向けに制作、開発を行っているコンテンツ
社内開発/制作済みコンテンツ	自社向けに制作、開発を行ったコンテンツ

分類名	解説
顧客預かり機密情報 (過去)	過去に顧客より、社外秘や秘密などの指定を受けて預かった情報
顧客預かり機密情報 (現在)	現在仕掛り中の顧客より、社外秘や秘密などの指定を受けて預かっている情報
人事情報	従業員の人事情報
勤怠情報	従業員の出勤状況などの情報
従業員個人情報	各従業員の電話番号、住所などの個人情報
経営、営業情報	経営上の戦略、具体的な数値などの情報
経理情報	入金、出金などの出納情報
顧客情報	顧客についての具体的な情報
案件情報	顧客やディレクターからの指示など、案件の制作/開発に関わる情報。案件袋
特許情報	取得した、もしくは取得申請中の特許に関する情報
クレーム情報	顧客からのクレームに関する情報
公式 HP コンテンツ	ウェブパークのホームページ
公式 HP 収集個人情報	ウェブパークのホームページで収集された個人情報
資産情報	社で保有している資産の一覧などの情報
DNS エントリ	ウェブパークがホスティングサービスとして提供している DNS 情報
サーバー設定情報	サーバーの設定や作業履歴など、現在のサーバーの設定についての情報
顧客提供情報 (個別)	個々の案件別に顧客に提示した情報。議事録、見積書、提案書、要件定義書、試験結果報告書など
顧客提供情報 (一般)	一般に公表している情報。サービス内容のパンフレットや価格表など
社内教育案内	社内で受けられる教育に関する情報
従業員成績情報	従業員の成績や評価に関する情報
外注情報	外注先に関する情報。住所、連絡先や成績、評価などもこれに含まれる

分類名	解説
社内規則、マニュアルや 未記入の伝票、申請書など	社内のマニュアルや規則に関する情報
各種届出	記入済みの各種届出。物品購入申請書や給与振込口座届など
従業員スケジュール	各従業員の行動予定などの情報
募集資料	従業員の募集のためのリクルート資料
契約書、発注書、請求書	法的に拘束力のある顧客との取引文書
図書	社内資産としての図書、資料集など。ソフトウェアでない CD-ROM（素材集）などはここに分類する
銀行データ	銀行との取引に関する情報や出納情報

- **情報資産の内容**
  情報資産の詳細。

- **情報資産の形態**
  例）電子データ。紙。

- **保管場所**
  例）○○の PC。○F のキャビネット。

- **所有者**
  その情報資産を管理している者の氏名。

- **重要度**
  機密性・完全性・可用性それぞれについて下の基準でスコアをつける。

機密性のスコアリング基準

重要度	説明
1	開示しても問題ない
2	開示してもあまり問題ない
3	開示すると社内的に問題がある
4	開示すると社外的に問題がある
5	開示すると経営に関わる、法令・契約違反になる

完全性のスコアリング基準

重要度	説明
1	不完全・不正確でも問題ない
2	不完全・不正確でもあまり問題ない
3	完全・正確でないと社内的に問題がある
4	完全・正確でないと社外的に問題がある
5	完全・正確でないと経営に関わる、法令・契約違反になる

可用性のスコアリング基準

重要度	説明
1	利用できなくなっても問題ない
2	一ヵ月以上利用できなくても問題ない
3	一週間以上利用できなくても問題ない
4	一週間以内に利用できないと問題である
5	数時間利用できないと経営に関わる、法令・契約違反になる

- **脅威・脆弱性**

  想定される事故原因や現在の管理策では弱い点などを記入する。

  例）錠がついていないので、盗まれる可能性がある。
  ウイルス対策ソフトを入れていないので、コンピューターウイルスに攻撃され情報が破壊・流出するおそれがある。

【2】情報資産の分類

情報セキュリティ委員会は、上記「情報資産棚卸リスト」の作成後速やかに、「情報資産と企業経営に対する被害との関連表」や様々な外的要因を踏まえて再度、分類名、重要度を見直し、脅威・脆弱性をまとめ、新たに「リスクの識別表」を作成する（情報セキュリティマネジメントマニュアル「3.2 管理枠組みの確立」の項参照）。

【成果物・記録】

・ISM-A-002：情報資産棚卸リスト

資料2
管理番号：ISM-A-002
会社名：株式会社ウェブパーク

作成	承認

情報資産棚卸リスト

分類番号	情報資産分類名	情報資産の内容	情報資産の形態	保管場所	所有者			重要度			脅威・脆弱性
					部門	氏名	管轄	機密性	完全性	可用性	

以下、製品版をご覧ください

アクセス制御に関する手順書
（ISM-C-014）作成のポイント

1. 「業務アプリケーション」レベルのサービスに対するアクセス制御の規定を設けることで、業務システムの不正使用というリスクを避けるための規定である。Unix サーバーにログインできるアカウントやルーターなどのネットワーク機器におけるアカウント情報が「ネットワーク詳細規定」にて記述されるのに対し、ここでは、その上位に位置する業務アプリケーションにおけるアカウント情報が説明される。情報システムの管理部門向けに作成する。

2. 業務アプリケーション上のアクセス制御について規定を設ける。

【目的】

当文書は、(株)ウェブパーク（以下ウェブパーク）の情報セキュリティ基本方針とそれに基づく情報セキュリティマネジメントシステムの要求事項に基づいて、社内システムへアクセス可能なユーザーもしくはアカウントの管理についてその手順と責任を明らかにしたものである。

【適用範囲】

ウェブパーク社内のすべての情報資産を適用範囲とする。

【責任】

IT事業部

【手順】

【1】ユーザー登録

新規にユーザーを登録する作業は、対象システム別に下記の管理主体のみが行えるものとする。

1) 電子メール

社内の電子メールシステムのアカウントの新規登録、変更、削除は、IT事業部のみが行えるものとする。

アカウントの新規登録、変更、削除作業は、xxxxサーバー上のデータベース、「ユーザーアカウントリスト」に記録される。

2) 社内情報共有、情報交換システム

社内情報共有、情報交換システムのユーザーアカウント管理は、管理本部とMFS本部のみが行えるものとする。

アカウントの新規登録、変更、削除作業は、xxxxサーバー上のデータベース、「ユーザーアカウントリスト」に記録される。

【2】特権割り当て

特権（Unix上のrootアカウントの利用、Windows NT上のAdministratorアカウントの利用）は、「ネットワーク詳細規定」に準拠し、管理ユーザーもしくはITユーザーのみに限定する。

特権パスワードは、3カ月に一度もしくは管理ユーザー、ITユーザーの退職直後に変更するものとし、その変更作業は「サーバーオペレーター日誌」に記述するものとする。

【3】パスワード

特権アカウントのパスワードは、推測可能であったり辞書上の文字列であったりすることを避けるために、パスワード自動生成システムを利用して発行するものとする。

個人ユーザーのパスワードについては特に規定しないが、推測不可能なものを利用し、３カ月程度の周期で変更することが望ましい。

【記録】

・ISM-R-022：サーバーオペレーター日誌
・ISM-R-031：ユーザーアカウントリスト

【監査】

サーバーオペレーター日誌、ユーザーアカウントリストは、毎年３月、６月、９月、12月にセキュリティアドバイザーによって監査されるものとする。

管理番号:ISM-R-022
会社名:

サーバーオペレーター日誌

記　入	承　認
年　月　日	年　月　日

作業日時:	担当:
作業内容:	

管理番号：ISM-R-031
会社名：

作　成	承　認
年　月　日	年　月　日

ユーザーアカウントリスト

発行日	アカウント名	社員番号	部門	氏名	備考

第６章　情報セキュリティマネジメントマニュアル実例

情報セキュリティマネジメントマニュアルは、ISMS の管理および運用について定めた手順である。主に情報セキュリティマネジメントシステムを運営する事務局が使用する。
(株)ウェブパークの情報セキュリティマネジメントマニュアルは、下記のような章立てになっている。

1. 目的
   このマニュアルの目的を述べている。

2. 用語および定義
   このマニュアルで用いる用語とその定義を記述している。

3. 情報セキュリティマネジメントシステムの要求事項

3.1 一般
   規格の要求事項に従い、ISMS を確立・維持することを明示している。

3.2 管理枠組みの確立
   適用範囲の決定、基本方針の策定、リスクアセスメントの体系的な取組方法の策定、リスクの識別、リスクアセスメント、リスク対応、管理目的・管理策の選択、適用宣言書の作成、残留リスクおよび ISMS の導入・運用についての経営陣の承認に至る管理枠組みの手順を文書化し、明確にしている。

3.3 実行
   ISMS を構築、導入、維持し、かつこれを継続的に改善することを明示している。

3.4 文書
   ISMS 文書の体系について記述している。

3.5 文書管理
   ISMS 文書の見直し、保管、廃棄などの管理について規定している。

3.6 記録
   ISMS の運用結果としての記録をどのように管理するか規定している。

4. その他の要求事項

4.1 情報セキュリティ基本方針
   基本方針の作成・見直しについて規定している。

4.2 組織のセキュリティ

体制と責任に関する事項を規定している。

4.3 教育・訓練

情報セキュリティの教育・訓練について規定している。

4.4 事業継続管理

事業継続管理について規定している。

事業継続管理とは、組織の重要な事業プロセスになんらかの障害が発生した場合に、どう対処するかということを情報セキュリティの観点から管理することである。ISO14001 環境マネジメントシステムでいえば、緊急事態への対応がこれにあたる。例えば施設が火災に遭ってしまった場合を例にとると、環境マネジメントシステムでは近隣への環境被害（大気汚染や廃棄物発生など）を低減するためのアクションプランを策定するが、ISMS では情報資産をリカバーするためのアクションプランを策定する。

リスク評価に基づく事業継続計画を立て、定期的にテストとレビューを行わなくてはならない。

具体的な手順については(株)ウェブパークの情報セキュリティマネジメントマニュアルにある手順を参考にされたい。

4.5 法的要求事項への準拠

法的要求事項に準拠するための手順を記述してある。

4.6 内部監査

内部監査を行うための手順を記述している。

4.7 不適合ならびに是正および予防処置

内部監査やマネジメントレビューにおいて発見された不適合を、是正し予防するための手順を規定している。

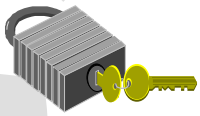
4.8 マネジメントレビュー

情報セキュリティ基本方針および ISMS 全体について経営層が見直しを行うための手順が規定されている。

(株)ウェブパークの情報セキュリティマネジメントマニュアルを以下に示す。

情報セキュリティ
マネジメントマニュアル

Ver1.00



管理番号：ISM-D-001-1

発　行　：２００４年０４月０１日
改　訂　：
作成者　：情報セキュリティ委員　井上　義春／小森　裕子
承認者　：代表取締役　　塚田　弘二

制定／改訂履歴表

版数	制定／改訂内容	改訂頁	作成者	承認者	発行日／ 改訂日
1.00	制　定	－	井上　義春 小森　裕子	塚田　弘二	2004.04.01

目　　次

1．目的

このマニュアルは、BS7799 および JIPDEC/ISMS 認証基準 Ver.2.0 に適合した(株)ウェブパークの情報セキュリティマネジメントシステムの基本的な事項を定め、情報セキュリティの推進を図ることを目的とする。

2．用語および定義

この情報セキュリティマネジメントマニュアルにおける用語の定義は原則としてBS7799で示された用語の定義に従う。ただし、当社で固有に使用している用語は、以下に定義する。

使 用 用 語	定　　義
BS7799	BS7799-2:2002
当社	(株)ウェブパーク
部門	管理本部、MFS本部、 営業部門、制作部門、 音声事業部、IT事業部、 アウトソーシング事業部、品質保証室
経営層	(株)ウェブパークの代表取締役
従業員	アルバイト社員を含む全従業員

3. 情報セキュリティマネジメントシステムの要求事項

3.1　一般

当社は、自らの事業の活動全般およびリスク全般を考慮して、文書化された ISMS を構築、導入、維持し、かつこれを継続的に改善する。

3.2　管理枠組みの確立

1.0　目的

ここでは、当社における情報セキュリティの管理目的および管理策を明確化、文書化するための責任および行動を定める。

2.0　適用範囲

当社の管理下にある、すべての業務活動に関わる情報。

3.0　責任

情報セキュリティ委員会。

4.0　実施時期

情報セキュリティ委員は、情報セキュリティマネジメントシステム導入時に管理枠組みを確立し、以下のとおり見直しを実施する。

4.1　定期的見直し

情報セキュリティ委員は、管理目的および管理策が当社の最新状況に対応していることを確かめるため、毎年４月と 10 月に見直しを実施する。

4.2　臨時の見直し

(1) 情報セキュリティ委員は、以下の事項が発生し、必要と認めた時、見直しを実施する。

① 当社の業務で扱う情報資産の大規模な変更

第７章　　帳票類一覧

No.	記録・帳票類の名称	文書・記録番号	手順書・規格番号
1	情報資産棚卸リスト	ISM-A-002	ISM-C-001 他
2	情報資産と企業経営に対する被害との関連表	ISM-A-003	ISM-D-001
3	リスクの識別表	ISM-A-004	ISM-C-001 他
4	リスクアセスメント結果報告書	ISM-A-005	ISM-D-001
5	リスク対応計画書	ISM-A-006	ISM-D-001
6	適用宣言書	ISM-A-007	ISM-D-001
7	文書・記録一覧	ISM-R-001	ISM-D-001
8	年間教育計画表	ISM-R-002	ISM-D-001
9	教育記録	ISM-R-003	ISM-D-001
10	事業継続リスクアセスメント	ISM-R-004	ISM-D-001
11	事業継続計画書	ISM-R-005	ISM-D-001
12	事業継続計画テスト結果記録	ISM-R-006	ISM-D-001
13	法的要求事項登録簿	ISM-R-007	ISM-D-001
14	年間監査計画表	ISM-R-008	ISM-D-001
15	監査チェックリスト	ISM-R-009	ISM-D-001
16	監査結果報告書	ISM-R-010	ISM-D-001
17	不適合報告書	ISM-R-011	ISM-C-005 他
18	見直し実施結果記録	ISM-R-012	ISM-D-001
19	鍵の申請書	ISM-R-013	ISM-C-003
20	鍵の所有者リスト	ISM-R-014	ISM-C-003
21	私物マシン使用許可願い	ISM-R-015	ISM-C-004
22	ハードウェア一覧	ISM-R-016	ISM-C-004
23	使用禁止ソフトウェアリスト	ISM-R-017	ISM-C-005 他
24	ソフトウェア監査記録	ISM-R-018	ISM-C-005 他
25	禁止ソフトウェア使用許可願い	ISM-R-019	ISM-C-005
26	新システム計画書	ISM-R-020	ISM-C-007
27	新システム試験結果報告書	ISM-R-021	ISM-C-007
28	サーバーオペレーター日誌	ISM-R-022	ISM-C-007 他
29	ネットワーク管理図	ISM-R-023	ISM-C-007 他
30	セキュリティアドバイザー監査記録	ISM-R-024	ISM-C-007
31	セキュリティ情報一覧	ISM-R-025	ISM-C-008
32	セキュリティ事故報告書	ISM-R-026	ISM-C-008
33	サービス一覧	ISM-R-027	ISM-C-009
34	アクセス制御リスト	ISM-R-028	ISM-C-009
35	バックアップリスト	ISM-R-029	ISM-C-0010
36	発行済証明書一覧	ISM-R-030	ISM-C-0012
37	ユーザーアカウントリスト	ISM-R-031	ISM-C-0014