

I S M S 管理マニュアル	
文書番号	
制定日	
改定日	
総ページ数	15 ページ (表紙含む)

【機密分類】社外秘

# I S M S 管理マニュアル

株式会社

文書番号		文書名	I S M S 管理マニュアル	ページ	2/10
章番号		内容	制定 / 改定履歴		

## 制定 / 改定履歴

版数	制定または改定主旨	承認	査問	作成	制定 / 改定日
1	制定				

## 配付

### 配付先の定義

配付用ではない。

この文書は社内公開文書として分類され、社員及び業務従事者だけが閲覧できる。

その他の者がこのマニュアルを閲覧するための要請は、経営者による認可を受けなければならない。

### 配付先リスト

配付用ではない。

文書番号		文書名	I S M S 管理マニュアル	ページ	3/10
章番号		内容	目的、責任、要求事項、承認		

## 目次

1	目的	4
2	責任	4
2.2	本マニュアルの実施に対する責任	4
3	要求事項	4
4	承認	4
5	情報セキュリティマネジメントシステム	5
5.1	一般要求事項	5
5.2	I S M S の確立及び運営管理	5
5.2.1	I S M S の確立	5
5.2.2	I S M S の導入及び運用	8
5.2.3	I S M S の監視及び見直し	9
5.2.4	I S M S の維持及び改善	エラー! ブックマークが定義されていません。
5.3	文書化	エラー! ブックマークが定義されていません。
5.3.1	一般	エラー! ブックマークが定義されていません。
5.3.2	文書管理	エラー! ブックマークが定義されていません。
5.3.3	記録の管理	エラー! ブックマークが定義されていません。
6	経営陣の責任	エラー! ブックマークが定義されていません。
6.1	経営陣のコミットメント	エラー! ブックマークが定義されていません。
6.2	経営資源の運用管理	エラー! ブックマークが定義されていません。
6.2.1	経営資源の提供	エラー! ブックマークが定義されていません。
6.2.2	教育・訓練、認識及び力量	エラー! ブックマークが定義されていません。
7	I S M S の内部監査	エラー! ブックマークが定義されていません。
8	マネジメントレビュー	エラー! ブックマークが定義されていません。
8.1	一般	エラー! ブックマークが定義されていません。
8.2	マネジメントレビューへのインプット	エラー! ブックマークが定義されていません。
8.3	マネジメントレビューからのアウトプット	エラー! ブックマークが定義されていません。
9	改善	エラー! ブックマークが定義されていません。
9.1	継続的改善	エラー! ブックマークが定義されていません。
9.2	是正処置	エラー! ブックマークが定義されていません。
9.3	予防処置	エラー! ブックマークが定義されていません。

文書番号		文書名	I S M S管理マニュアル	ページ	4/10
章番号		内容	目的、責任、要求事項、承認		

## 1 目的

---

本マニュアルは、当社が情報セキュリティマネジメントシステム(ISMS)を構築、実施、維持し、継続的に改善する為の管理枠組みを文書化する。ISO 27001:2005の第4、第5、第6、第7、第8に準拠する。

## 2 本文書の責任

---

本マニュアルの責任は、情報セキュリティ管理責任者にある。

## 3 要求事項

---

I S M S 認証基準(Veer.2.0)の第4、第5、第6、第7及び第8の要求事項を満たさなければならない。

1. 第4 情報セキュリティマネジメントシステム
2. 第5 経営陣の責任
3. 第6 I S M Sの内部監査
4. 第7 I S M Sのマネジメントレビュー
5. 第8 I S M Sの改善

## 4 承認

---

本マニュアルは、社長によって承認されなければならない。

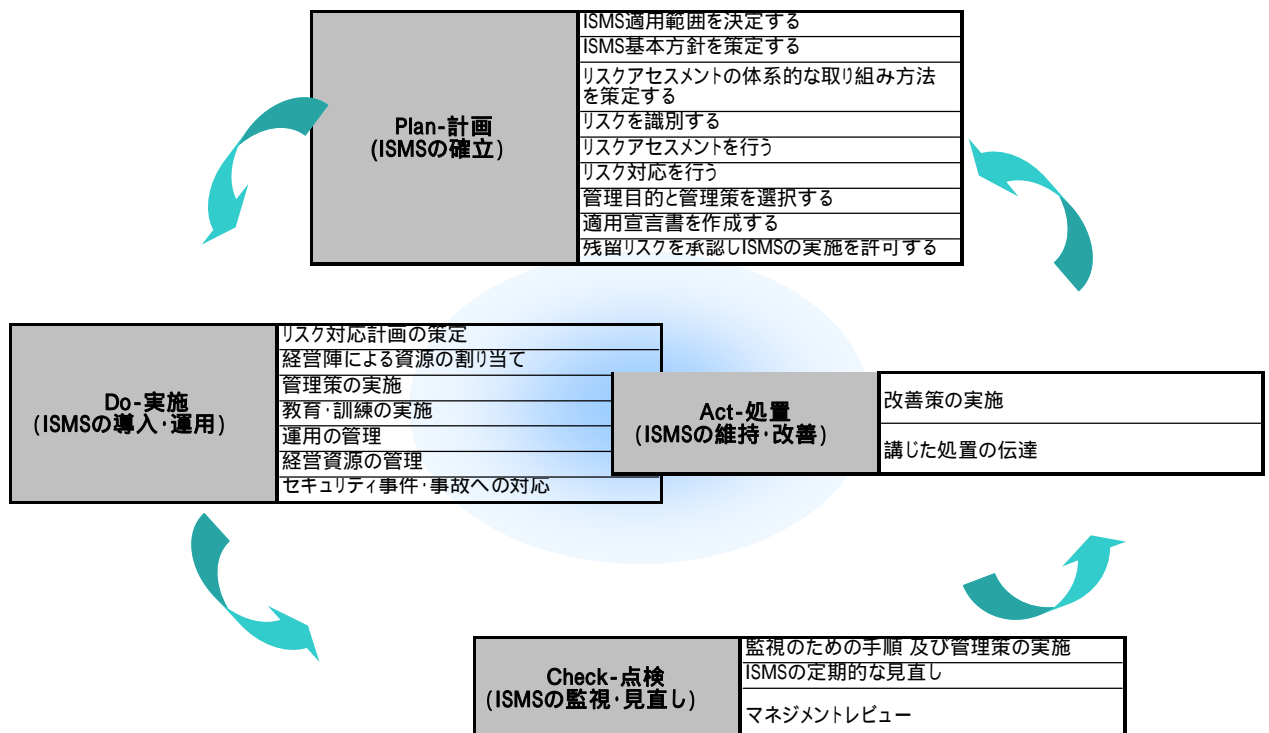
文書番号		文書名	I S M S 管理マニュアル	ページ	5/10
章番号		内容	目的、責任、要求事項、承認		

## 5 情報セキュリティマネジメントシステム

### 5.1 一般要求事項

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 I S M S を構築、導入、維持し、かつこれを継続的に改善する事。

次の P D C A モデルに基づく



### 5.2 I S M S の確立及び運営管理

#### 5.2.1 I S M S の確立

( 1 ) 適用範囲を定義する：次の事項を弐リヨして、適用範囲を適切に定義する。

1. 事業の特徴
2. 組織
3. 所在地
4. 資産

文書番号		文書名	I S M S 管理マニュアル	ページ	6/10
章番号		内容	目的、責任、要求事項、承認		

## 5. 技術

### 【関連文書】：適用範囲定義書

(2) 基本方針を策定する：次の事項を考慮して基本方針は次の事項を策定する。

1. その目標を確立する為の枠組みを含み、又情報セキュリティについての活動の方向性及び原則を全体的な意味において確立すること。
2. 事業上及び法令又は規制上の要求事項、並びに契約に基づくセキュリティ義務を考慮すること。
3. そのもとで I S M S を確立し維持する、戦略的に見た組織の状況、及びリスクマネジメントの状況を確認すること。
4. リスクを評価する基準、及び定義されるリスクアセスメントの構造を確認すること。
5. 経営者によって承認されていること。

### 【関連文書】：基本方針

(3) リスクアセスメントの体系的アプローチの策定

I S M S、識別された事業の情報セキュリティの要求事項、並びに法令及び規制上の要求事項に適した、リスクアセスメントの方法を特定しなければならない。リスクを受容できるレベルまで低減する、I S M S の為の方針及び目標を設定しなければならない。リスクを受容する為の基準を決定し、リスクの受容できるレベルを特定しなければならない。次の方法を採用する。

1. ベースラインアプローチ：同業種等で一般に広く使用される方法、技術を参考に自社のリスク、管理策を検討する。ギャップ分析の実施。
2. 詳細リスク分析及び管理：情報資産に対して詳細に脅威、脆弱性、資産価値及び業務影響評価を実施し、個別に管理策を検討する。
3. 組み合わせアプローチ：上記 1、2 を組み合わせて使用する。

### 【関連文書】：リスクアセスメント手順書

(4) リスクの識別

1. セキュリティに起因して想定される、組織に対する事業上の影響を評価する。その際、当該資産の機密性、完全性、可用性の喪失による影響を考慮する。
2. それら資産に対する脅威の識別、リスクアセスメントを実施する。現在実施されている管理策を考慮する。
3. リスクの水準を算定する。

文書番号		文書名	I S M S 管理マニュアル	ページ	7/10
章番号		内容	目的、責任、要求事項、承認		

4. 5.2.1(3)2 で確立したリスクを受容する為の基準を試用して、当該リスクについて、受容できるか、対応が必要かを定める。

【関連文書】：リスクアセスメント手順書

( 5 ) リスクアセスメントを実施する

1. セキュリティ障害に起因する事業損害についてのアセスメント。ここでは、資産の機密性、完全性又は、可用性の喪失による、予想される結果を考慮しなければならない。
2. 一般に認識されている脅威、資産と関係付けられた脆弱性及び影響、並びに現在実施されている管理策に照らしてみた、そのような障害が実際に起こる可能性についてのアセスメント。
3. リスクのレベルの算定。  
脅威のレベル：該当脅威の発生可能性  
脆弱性のレベル：当該脅威を発生させる弱点の度合  
資産価値：当該脅威の価値属性（機密性、完全性、可用性）  
業務影響レベル：当該脅威の発生による、業務の影響度合
4. リスクを受容できるか又は、対策を必要とするかを決定。  
保証の度合の決定：リスクレベルの算定結果、組織として受容できるリスクレベルを決定する。

( 6 ) リスク対応についての選択肢を明確にし、評価する

1. 低減：適切な管理策を採用する
2. 保有：リスクを保有する：リスクが基本方針及びリスク需要レベルを明らかに満たしている場合は、リスクを受容する  
残留リスク：保証の度合の範囲内で受容されたリスクを残留リスクと呼ぶ。  
残余リスク：保証の度合の範囲内に止まらないが、環境的、コスト的又は時間的な要員で対応できず、経営陣の承認を得たリスクを残余リスクと呼ぶ。
3. 回避：リスク要因そのものを排除するのとして、リスクを回避する
4. 移転：リスク要因を外部委託、契約等で移転する。保険やアウトソーシングサービスへの移転

( 7 ) リスク対応のための、管理目的及び管理策の選択

適切な管理目的及び、管理策を定め、リスクアセスメント及び、リスク対応のプロセスの結論に基づいて正当化しなければならない。

対策を施した結果、該当資産に対するリスク値は、6 以下となること、ないしは経営者による残留リスク及び残余リスクの承認を得ること。

文書番号		文書名	I S M S 管理マニュアル	ページ	8/10
章番号		内容	目的、責任、要求事項、承認		

- ( 8 ) 残留リスク、残余リスクの承認  
 残留リスクとなるものに対する経営者の承認、及びその残留リスクが伴う I S M S を導入及び運用する許可を得ること。マネジメントレビューの議案とする。

【関連文書】: リスクアセスメント報告書

- ( 9 ) 当該 I S M S の導入及び運用について経営陣の許可を得る。マネジメントレビューの議案とする。

- ( 1 0 ) <sup>L</sup> 適用宣言書の作成  
 前項に従って定めた管理目的及び、管理策、並びにそれらの理由を、適用宣言書に文書化しなければならない。

1. 5.2.1(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。
2. 現在実施されている管理目的及び管理策(5.2.1(5)2を参照)
3. ISO27001:2005の付属書Aの管理目的及び管理策の中から適用を除外したものをすべて、及びその除外の理由

【記録】: 適用宣言書

## 5.2.2 I S M S の導入及び運用

情報セキュリティ責任者は、I S M S の導入及び運用にあたっては、次の事項を実施しなければならない。

- ( 1 ) リスク対応計画を作成する。  
 【関連文書】リスク対応計画書
- ( 2 ) リスク対応計画を実施する。
- ( 3 ) 当該管理目的を達成するために選択した管理策を実施する。
- ( 4 ) 選択した管理策一式の有効性を測定する方法について規程する。また比較可能で再現可能な結果を出すために、管理策の有効性を評価するのにこの測定方法をどのように利用すべきか特定する。
  - 1 選択した管理策毎に、管理指標を設定する。この指標はできるだけ定量的であることが望ましい。
  - 2 指標項目例：コスト、事故発生件数、違反件数等
  - 3 この指標に基づく実績を、内部監査実施時期等にあわせ、定期的にレビューする。
- ( 5 ) 情報セキュリティ管理責任者は、訓練及び認識プログラムを実施する。

文書番号		文書名	I S M S 管理マニュアル	ページ	9/10
章番号		内容	目的、責任、要求事項、承認		

【関連文書】教育手順書、教育訓練年間計画書、教育訓練実施報告書

(6) 運用管理：情報セキュリティ管理責任者は、I S M S の運用及び実施管理策の運用を管理する。

- 1 情報セキュリティ管理責任者は、情報セキュリティフォーラムメンバーを参加者とSる、定例会議を主催する。
- 2 主な議題：セキュリティ事件事故状況、違反状況、脆弱性情報、技術動向、各種計画進捗等。

(7) 経営資源管理：次の経営資源の管理を実施する。

- 1 年度のセキュリティ対策予算を作成し実績管理する。
- 2 セキュリティ活動に必要な作業時間（従業員の教育時間、フォーラムメンバーの会議等の時間等）を計画し実績管理する。
- 3 情報システム機器を台帳管理する。
- 4 情報システムに利用するソフトウェアのライセンスを台帳管理する。
- 5 サーバやインターネット接続サービス等、情報セキュリティに関するアウトソーシングサービスの契約管理台帳を作成、維持する。

(8) セキュリティ事件・事故対応：情報セキュリティ管理責任者は、以下の事件、事故対応手順を策定する。

- 1 セキュリティ事故対応手順を、策定し手順書に文書化する。
- 2 事業継続の側面を、事業継続計画に含める。
- 3 システム運用に於ける事故対応手順を、策定する。
- 4 人的な策面に対応する手順を策定する。

### 5.2.3 I S M S の監視及び見直し

(1) 監視及び見直しの為の手順及び管理策を実施する。

1. 処理結果から誤りを速やかに検出する：セキュリティ誤動作の報告を実施する。（人的セキュリティ規程）
2. セキュリティ上の違反行為及びインシデントは未遂であっても、迅速に識別する。：セキュリティ弱点の報告を実施する。（人的セキュリティ規程）
3. 人又は情報技術によって導入されたセキュリティ活動が意図した通りに実施されているかどうかを経営者や管理者が判断できるようにする。：定期的に内部監査を実施し、監査報を実施する。（内部監査規程）
4. 指標を利用する事により、セキュリティ事象の検出を容易にし、その結果セキュリティインシデントを防止する。：リスクアセスメントの実施を現場レベルで行うように奨励し、結果を組織内で共有する。リスクアセスメントは定期的に見直す機会を設定し、かつ重大な変更や事

文書番号		文書名	I S M S 管理マニュアル	ページ	10/10
章番号		内容	目的、責任、要求事項、承認		

故の際は都度実施する。

(2) セキュリティ違反を解決する為にとった処置の有効性を判断する。

- 1 違反の対応手順に、管理策の有効性をレビューする手順を含める事。(人的セキュリティ管理規程)
- 2 レビューの結果を有効性評価表の指標に反映する。

(3) 有効性の測定

- 1 5.2.2(4)で規程した、各管理策の有効性指標項目について、測定を実施する。例、コスト、事故件数、違反件数等。

(4) 残留リスク及び受容可能リスクの見直し：経営陣が示した保証の度合に応じた、残留リスク及び受容可能リスクを下記を考慮して見直す。

1. 組織
2. 技術
3. 事業の目標及びプロセス
4. 識別された脅威
5. 実施された管理策の有効性
6. 法的又は規則的規制の変化、社会環境の変化等の外部要因。

(5) 内部監査

あらかじめ定められた間隔で I S M S の内部監査を実施する。

【関連文書】：内部監査に関する手順書

(6) マネジメントレビュー

年に1回以上、経営者フォーラムはマネジメントレビューを実施する。

(7) セキュリティ計画の更新：マネジメントレビューの結果、セキュリティ対応系か鶴を更新する。

【関連文書】セキュリティ対応計画書

(8) 記録

次の活動及び事象を記録する。

1. 運用の記録
2. 障害の記録
3. 事象の記録
4. その他