

文書番号		文書名	基本方針	ページ	1/10
章番号		内容	ISMS 制定に伴う適用範囲定義書		

基本方針	
文書番号	
制定日	
改定日	
総ページ数	10 ページ (表紙含む)

【機密分類】社外秘

基本方針

株式会社

文書番号		文書名	基本方針	ページ	2/10
章番号		内容	目的		

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

全従業員

文書番号		文書名	基本方針	ページ	3/10
章番号		内容	目的		

目次

1	目的	4
2	責任	4
3	要求事項	4
4	承認	4
5	情報セキュリティ基本方針	5
5.1	情報セキュリティ基本方針文書	5
5.2	見直し及び評価	10

文書番号		文書名	基本方針	ページ	4/10
章番号		内容	「情報セキュリティポリシー」の適用者		

1 目的

本書は、当社の情報セキュリティマネジメントシステム(ISMS)の基本方針に関する、定義を行うものである。

2 責任

本書の責任は、社長にある。

3 要求事項

1. 情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項、関連する法令及び規則に従って規定するため。

4 承認

社長

文書番号		文書名	基本方針	ページ	5/10
章番号		内容	「情報セキュリティポリシー」の適用者		

5 情報セキュリティ基本方針

【管理目的】情報セキュリティのための経営陣の指針及び支持を規定するため。

5.1 情報セキュリティ基本方針文書

【要求事項】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事。

5.1.1 基本方針（トップポリシー）

以下を考慮し、経営の声明文を作成。

基本方針を作成する上での考慮事項

- 事業継続に関する方針：如何に事業継続を果すか。
- 損失の最小化に関する方針：事件、事故に対する対応で損失を最小化するために。
- 利益の最大化に関する方針：セキュリティ対策投資を以下に効率よく実施するか。

【方針宣言文】

情報セキュリティ基本方針

当社は国際規格である情報セキュリティマネジメントシステムを導入し、これによりシステムの継続的改善を実施する。

リスクアセスメントに基づく管理を実施し、管理が効果的かつ有効であることを確実にする。

従業員及び利害関係者に対する周知、教育を徹底し、遵守すべき各種の事項と行動規範を徹底する。

当社の顧客サービス事業の、あらゆる障害から事業継続を優先する。

事件、事故に対する情報資産の価値損失を最小にする体制を整える。

5.1.2 ISMSの概要

1. 定義

ISMSの目的のために次の用語及び定義を適用する。

- (ア) 可用性：当社の情報資産に認可された利用者が、必要な時に、アクセスできる事を確実にする。

文書番号		文書名	基本方針	ページ	6/10
章番号		内容	「情報セキュリティポリシー」の適用者		

- (イ) 完全性：情報及び処理方法が、正確であること及び完全である事を保護する事。
- (ウ) 機密性：アクセスを認可されたものだけが情報にアクセスできることを確実にする。
- (エ) 情報セキュリティ：情報の機密性、完全性及び可用性の維持。
- (オ) 情報セキュリティマネジメントシステム：マネジメントシステム全体の中で、事業リスクに対するアプローチに基づいて情報セキュリティの確立、導入、運用、監視、見直し、維持、改善をになう部分。
- (カ) 適用宣言書：組織のリスクアセスメント及びリスク対応プロセスの結果及び結論に基づいき、組織のISMSに適切で当てはまる管理目的及び管理策を記述した文書。
- (キ) リスクアセスメント：リスク分析からリスク評価までの全てのプロセス。
- (ク) リスクの受容：リスクを受容する意思決定。
- (ケ) リスク対応：リスクを変更させるための方策を、選択及び実施するプロセス。
- (コ) リスク評価：リスクの重大さを決定するために、算定されたリスクを与えられたリスク基準と比較するプロセス。
- (サ) リスクの分析：リスク因子を特定するための、及びリスクを算定するための情報の系統的使用。
- (シ) リスクマネジメント：リスクに関して組織を指揮し管理する調整された活動。

2. 目的

ISMSは、情報資産を保護するため、十分でバランスのとれた適切な情報セキュリティ管理策を確保し、顧客及び他の利害関係者に対して信頼を与える。

これは競争力、資金力、収益性、法令等の遵守及び企業イメージを維持し、改善する。

3. 適用範囲

ISMS認証基準(VER2.0)の第4、第5、第6及び第7に定める要求事項は全て満たす。また本基準書の附属書「詳細管理策」の要求事項の何れかが適用できない場合は、除外することができる。ただしリスクアセスメント及び該当する規制上の要求事項によって決定されるセキュリティ要求事項を満たす情報セキュリティを提供する組織の能力、責任等に影響を及ぼさないと判断されなければならない。

5. 1. 3 特に重要なセキュリティ方針

1. 【法律、契約等】個人情報保護法等、法律に遵守した事業活動を行う。
2. 【教育】従業員に対するセキュリティ教育を重視する。
3. 【ウィルス等の脅威】コンピュータに対するウィルス等の脅威に十分に備える。
4. 【事業継続】顧客の期待に応える事業継続計画を備え、実行する。
5. 【懲戒】規程に対する違反の対処は厳正、公平に実施する

文書番号		文書名	基本方針	ページ	7/10
章番号		内容	「情報セキュリティポリシー」の適用者		

5.1.4 ISMS 確立のための組織体制

1. 経営陣

- ISMS の確立に対する承認

2. 情報セキュリティ委員会：

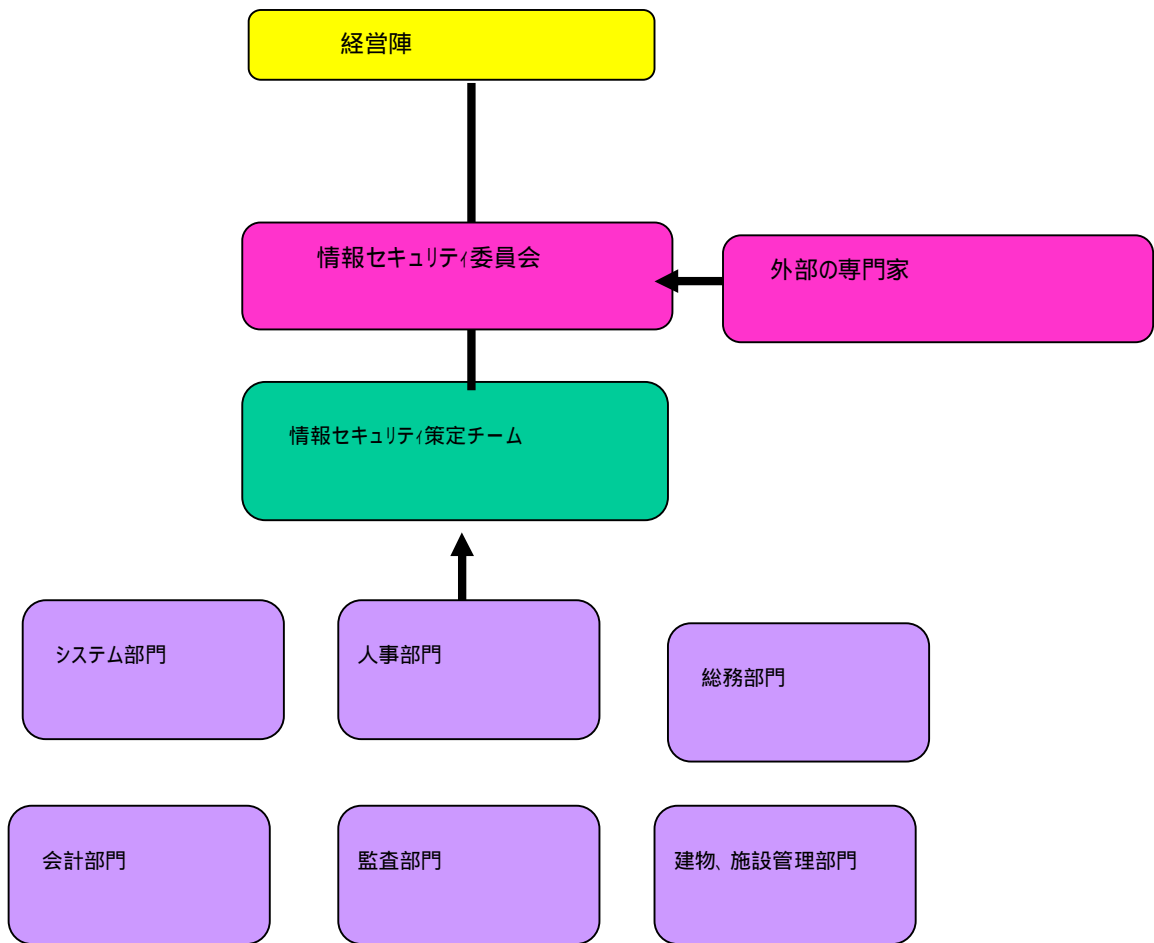
- リスクマネジメントの承認
- ISMS 関連文書の承認

3. 情報セキュリティ策定チーム

- ISMS 構築実務担当

4. 外部専門家

文書番号		文書名	基本方針	ページ	8/10
章番号		内容	「情報セキュリティポリシー」の適用者		



5.1.5 ISMS運用の為の組織体制

1. 経営者

- ISMS 確立に関する責任
- セキュリティ経営者フォーラムの組織
- セキュリティ責任者の任命
- 重大なセキュリティ事件、事故の対応責任
- 事業継続計画発動
- リスクの保証の程度の承認
- 許容するリスクの承認
- ポリシー違反の措置責任
- ISMS 運用に於けるマネジメントレビュー責任
- セキュリティのリソースの割り当て責任
- 情報セキュリティ事件、事故の警察等への通知判断
- マスコミ対応

文書番号		文書名	基本方針	ページ	9/10
章番号		内容	「情報セキュリティポリシー」の適用者		

- 外部に対する説明責任

2. 情報セキュリティ委員会

- 各部門のセキュリティ担当者の任命
- セキュリティ事件、事故の対応責任
- 重大なセキュリティ事件、事故の経営者への報告
- セキュリティ教育計画と実施
- セキュリティ対応計画の策定と実施
- セキュリティ事件、事故の問題分析

3. 情報セキュリティ監査責任者

- I S M S の確立及び運用に直接の利害を持たない。
- I S M S の基本的知識を有する。
- 監査の計画と実施

4. 適用範囲部門セキュリティ担当者

- セキュリティ事件、事故のセキュリティ委員会への報告
- 部門従業員の監視

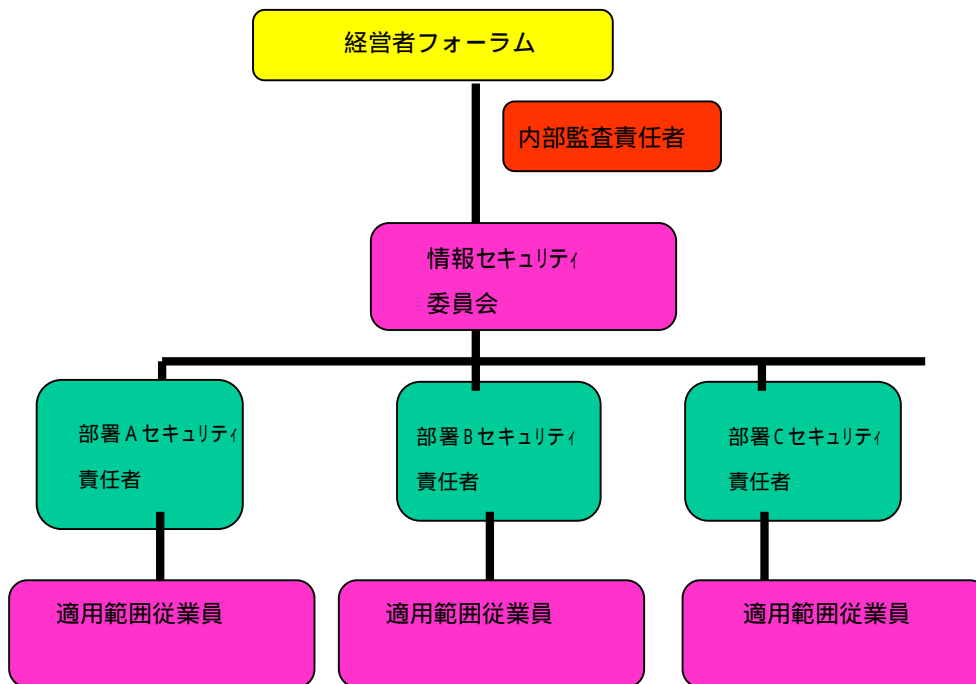
5. 適用範囲従業員

- セキュリティ教育の参加
- セキュリティポリシーの遵守
- セキュリティ事件、事故の発見と部門セキュリティ担当者又はセキュリティ委員会への報告
- 経営との情報セキュリティ誓約書の締結

6. 外部の専門家

- 必要に応じて、セキュリティの助言や監査に外部の専門家を用いる。

文書番号		文書名	基本方針	ページ	10/10
章番号		内容	「情報セキュリティポリシー」の適用者		



5.2 見直し及び評価

【要求事項】基本方針は、依然として適切である事を確実にするために、適期的に、また影響を及ぼす変化があった場合に、見直す事。

1. 定期的な見直し：マネジメントレビューを実施する際、情報セキュリティ責任者はH基本方針の見直しを提案すること。
2. 随時見直し：次の様な事象において見直しを実施する。
 - 情報システムの変更
 - 重大なセキュリティ事件、事故の対応
 - 組織変更
 - 事業変更