情報セキュリティ方針

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

情報セキュリティ方針

１　趣旨

ネットワークコンピュータを利用した経営環境が、当社に導入されて久しい。その間、当社の扱っている情報が、ネットワークコンピュータ上で扱われることが当然のこととなった。ネットワークコンピュータは、その導入による業務効率の影響は甚だしく、また、経営支援ツールとしても今後も大いに活用していくべきものである。インターネットを利用してビジネスチャンスを拡大している当社にとって、「セキュリティの確保」は必須事項である。昨今の度重なるセキュリティ事件は、当社にとっても「対岸の火事」ではなく、問題を発生させないために、早急に対応しなければならない経営課題である。

お客様との関係において、セキュリティ事件が発生した場合の営業機会の損失は甚だしいものになることは想像に難くない。当社は、顧客満足度を向上させるためにも、「セキュア」なブランドイメージを早急に構築しなければならない。

そのために、当社は、ネットワークコンピュータ上を流通する情報やコンピュータ及びネットワーク等の情報システム（以下、情報資産）を第４の資産と位置付ける。よって、当社は、情報資産を重要な資産とし、保護・管理しなければならない。

当社は、情報資産を保護する「情報セキュリティマネジメント」を実施するために、『情報セキュリティポリシー』を策定する。

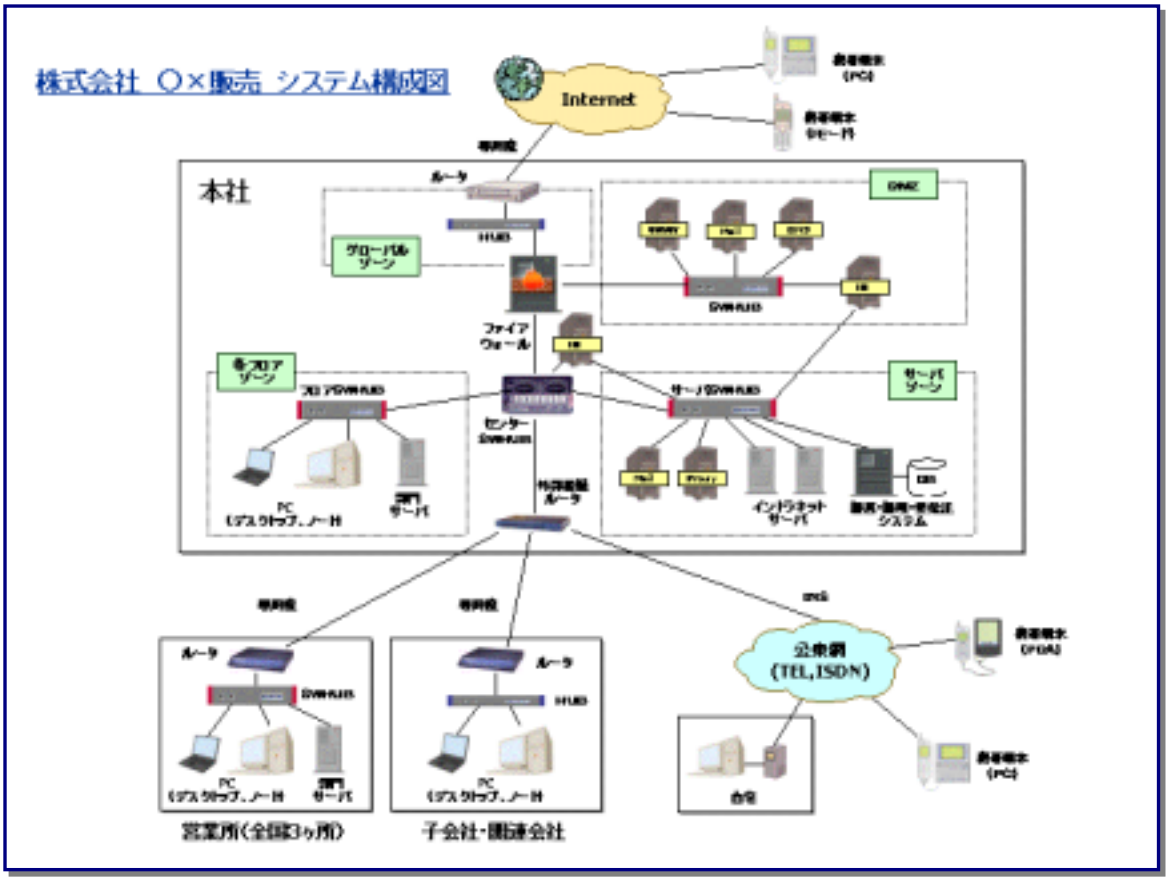
『情報セキュリティポリシー』は、当社の情報資産を、故意や偶然という区別に関係なく、改ざん、破壊、漏洩等から保護されるような管理策をまとめた文書である。

当社の情報資産を利用する者は、情報セキュリティの重要性を認知し、この『情報セキュリティポリシー』遵守しなければならない。

2　『情報セキュリティポリシー』の適用範囲

『情報セキュリティポリシー』の適用範囲は、当社の情報資産に関連する人的・物理的・環境的リソースも含むものとする。

当社の保有するシステムの具体例は、下図で示している範囲とする。



3　『情報セキュリティポリシー』の適用者

当社の社員・契約社員（一時雇用者を含む）を従業員と定義する。

『情報セキュリティポリシー』の適用者は、経営陣、従業員を含めた、当社の情報資産を利用するすべての者である。

3．1　経営陣の責務

経営陣は、『情報セキュリティポリシー』への支持・支援を表明し、率先して情報セキュリティマネジメントを推進しなければならない。

3．2　従業員の責務

従業員には、当社の情報資産の使用を認めるが、それは、円滑な業務遂行の手

段としての使用を認めることであり、私的利用を許可するものではない。

従業員は、情報資産を扱う上で、企業利益の維持・向上および顧客満足のために、『情報セキュリティポリシー』に同意し、遵守しなければならない。また、これに違反した者は、その結果について責任を負わなければならない。

３．３　外部委託業者に対する対応

『情報セキュリティポリシー』の適用範囲内で行う作業を、外部委託業者に依頼する場合には、契約上で遵守するべきセキュリティ管理策を明確にし、セキュリティ事故時の責任に関しても明確にしなければならない。

４　『情報セキュリティポリシー』の構成と位置付け

『情報セキュリティポリシー』は、以下の３つの階層に分けて策定・管理される文書とする。

４．１　情報セキュリティ方針

情報セキュリティ方針（以下、「方針」とする）は、『情報セキュリティポリシー』の最上位に位置する文書である。この文書は、当社の情報セキュリティマネジメントにおける方針を記述したものである。この文書に基づいて下層の文書を策定する。

４．２　情報セキュリティ対策標準

情報セキュリティ対策標準（以下、「対策標準」とする）は、方針の下層に位置する文書である。この文書は、方針での宣言を受け、項目毎に遵守すべき事項を網羅的に記述する。

４．３　情報セキュリティ実施手順書

情報セキュリティ実施手順書（以下、「実施手順書」とする）は、対策標準の下層に位置する文書である。この文書は、対策標準で記述された文書をより具体的に、配布するべき対象者毎に内容をカスタマイズして記述する。

４．４　既存の規定との関連

方針は、当社の他の規定（人事規定、就業規則等）と同等の位置付けの文書とする。よって、この文書の改廃は所定の規定に準じて行うものとする。

４．５　その他関連法規

『情報セキュリティポリシー』は、関連法規と照らして違反することの無いようにしなければならない。また、必要に応じて関連規格に遵守した管理策を導入しなければならない。

関連法規・関連規格としては、以下のものが挙げられる。

国際規格

・ISO/IEC 17799

・ISO/IEC TR 13335（GMITS）

国内規格

・ JIS Q 15001

国内法規

- 刑法
- 不正アクセス行為の禁止等に関する法律
- 建築基準法/同施行令
- 消防法/同施行令/同施行規則
- 不正競争防止法
- 著作権法

5　『情報セキュリティポリシー』の公開対象者

方針は、従業員すべてを公開対象とする。したがって、一般には公表しない機密情報として取り扱わなければならない。以下、方針以外の文書は機密情報である。

対策標準は、情報セキュリティ委員会メンバーと担当部署の者を公開対象とする。

実施手順書は、該当する業務を行う者を公開対象とする。

6　『情報セキュリティポリシー』の公開

『情報セキュリティポリシー』は機密文書として扱い、原則として、社外に公開してはならない。ただし、公開しなければ業務を遂行できない場合には、機密保持契約を締結した上で、公開を認める場合がある。

7　基本用語の定義

『情報セキュリティポリシー』における用語は以下の通り定義する。

7．1　情報セキュリティ（ISO/IEC17799 より抜粋）

情報の機密性、完全性及び利用の可能性の維持。

注）

機密性は、情報にアクセスすることが認可された者だけがアクセスできることを確実にすること、として定義される。

完全性は、情報及び処理方法の正確さ及び完全である状態を安全防護すること、として定義される。

利用の可能性は、認可されたユーザが、必要時に、情報及び関連財産にアクセスできることを確実にすること、として定義される。

7．2　リスクアセスメント（ISO/IEC17799 より抜粋）

情報及び情報処理施設/設備に対する脅威、それらへの影響及びバルネラビリティ並びにそれらがおこる可能性の評価。

７．３　リスクマネジメント（ISO/IEC17799 より抜粋）

許容コストにより、情報システムに影響を及ぼす可能性が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、又は除去するプロセス。

７．４　脅威

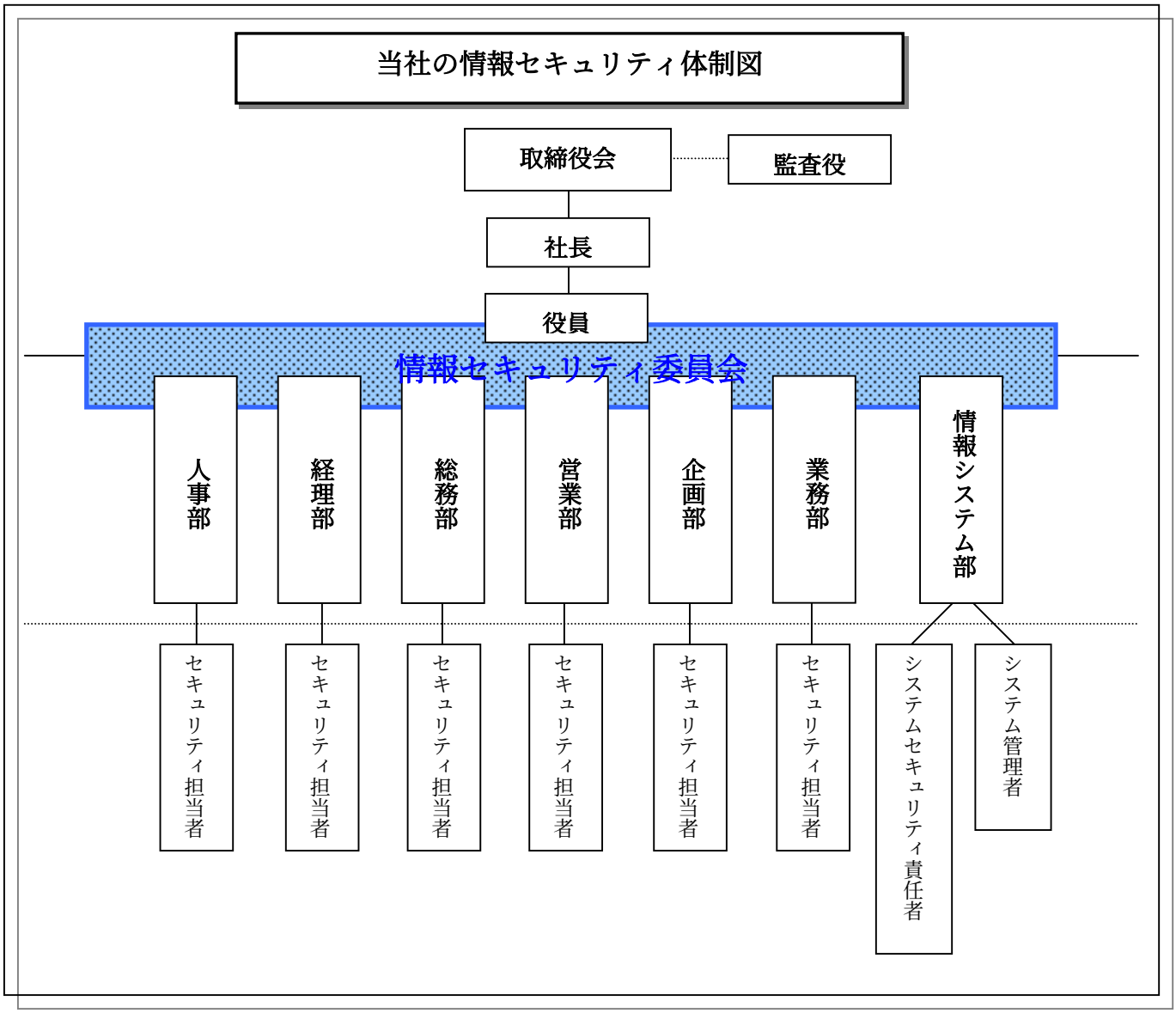
自然災害、機器障害、悪意のある行為等、損失を発生させる直接の要因のこととする。

７．５　脆弱性

建物の構造上の欠陥、定期点検の不備、情報セキュリティ規定・要員教育の不備等、脅威を発生し易くさせる要因、脅威を増加させる要因（脆さ、弱点）のこととする。

８　体制

当社の情報セキュリティマネジメントを遂行する体制を以下の通り定める。



８．１　情報セキュリティ委員会

当社の情報セキュリティを維持していくために、情報セキュリティ委員会を設け、全社的なマネジメント体制を整えるものとする。情報セキュリティ委員会の詳細情報に関しては、情報セキュリティ委員会構成メンバーを参照のこと。

８．２　情報システム部

情報システム部は、情報セキュリティ委員会で決定した対策事項を実施及び推進する担当部署とする。

情報システム部は、当社の情報機器の管理責任を有し、当社に関係するセキュリティ情報収集を行い、社内のセキュリティ対策に反映させなければならない。また、従業員から収集した情報を、必要に応じて情報セキュリティ委員会に報告しなければならない。

８．３　システムセキュリティ責任者

システムセキュリティ責任者は、情報システム部に属し、システム管理者の作業責任を有する。

システムセキュリティ責任者の役割は、システム管理者への作業指示・管理を行い、システム管理者同士での作業の「相互牽制」及び「職務の分離」が有効に働くように配慮しなければならない。

８．４　システム管理者

システム管理者は、情報システム部に属し、システムセキュリティ責任者より与えられた管理作業の責任を有する。

システム管理者の役割は、管理を依頼された情報機器に対して、セキュリティ対策を実施する現場レベルでの責任者である。

８．５　オペレーター

オペレーターは、情報システム部に属し、システム管理者の管理下のもとで実質的な作業を行う者である。

８．６　セキュリティ担当者

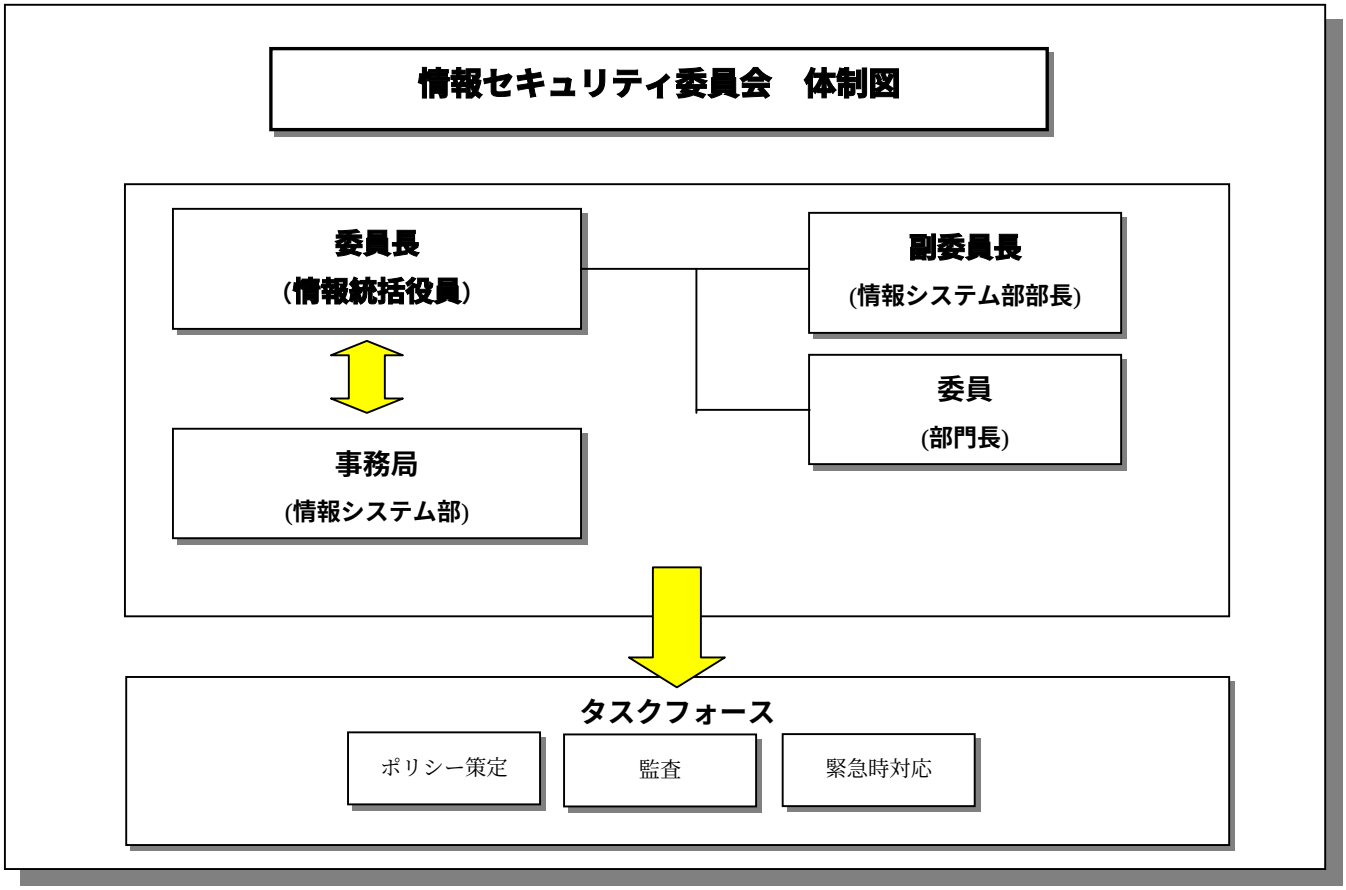
セキュリティ担当者は、情報システム部以外の各部署の部門長によって最低一人は任命され、配置される者である。

セキュリティ担当者の役割は、部門内におけるセキュリティ推進及び情報（社員のセキュリティ対策及び情報セキュリティマネジメントへの不平・不満及び問題点等）の収集担当であり、収集した情報は情報システム部へ報告する。

９　情報セキュリティ委員会の体制図及び構成メンバー

９．１　情報セキュリティ委員会の体制図

委員会の構成は下図の通り定める。



９．２　常勤委員

常勤委員は、委員長、副委員長、委員とする。常勤委員は、委員会が開催されたときは、必ず参加しなければならない。

９．３　非常勤委員

非常勤委員は、外部コンサルタント、法律専門家、システムセキュリティ責任者である。非常勤委員は、委員長によって召集されたときに参加する。

９．４　委員長

委員長は、当社の役員を情報統括役員として取締役会で指名する。委員長は、当社における情報セキュリティマネジメントに関しての最高責任者である。

９．５　副委員長

副委員長は、情報システム部部長とする。副委員長は、委員長の補佐役である。委員長が万一職務を遂行することが不可能になった場合には、委員長の代理となって、職務を遂行する。

９．６　委員

委員は、各部門長とする。委員は、情報セキュリティ委員会への議題（社内及び社外で起きているセキュリティ事象への対応等）を提示することができる。

９．７　事務局

事務局は、情報システム部とする。事務局は、情報セキュリティ委員会を運営する上での事務作業を行う。

また、情報セキュリティ委員会で作成・策定した情報セキュリティマネジメント計画書や『情報セキュリティポリシー』文書の管理を行う。

９．８　タスクフォース

情報セキュリティ委員会は、各作業を実施するにあたってタスクフォースを設けることができる。このタスクフォースの責任者は、いずれかの委員とする。タスクフォースには、『情報セキュリティポリシー』策定、監査、緊急時対応等の作業を実施する。

１０　情報セキュリティ委員会の役割と責務

情報セキュリティ委員会の主な役割を下記の通り定める。

１０．１　情報セキュリティマネジメントの企画及び計画

情報セキュリティ委員会は、当社における情報セキュリティマネジメントを実施していく企画及び計画を作成し、その計画通り情報セキュリティマネジメントを実施しなければならない。

この企画及び計画には、情報セキュリティマネジメントを遂行する為のリスクアセスメント、リスクマネジメントはもちろんのこと、『情報セキュリティポリシー』の見直しや従業員への普及・啓発も考慮に入れなければならない。

１０．２　『情報セキュリティポリシー』文書の配布責任

情報セキュリティ委員会は、『情報セキュリティポリシー』を策定又は改訂した場合には、迅速に対象従業員へその文書を配布しなければならない。

１０．３　社内教育の実施

情報セキュリティ委員会は、情報セキュリティに関する継続的な社内教育を行う。この社内教育は、意識向上と技術向上の両面から実施しなければならない。

１０．４　『情報セキュリティポリシー』の遵守状況の評価及び改訂

情報セキュリティ委員会は、従業員の『情報セキュリティポリシー』遵守状況を定期的に調査し、『情報セキュリティポリシー』のレビューを行うこととする。また、従業員の『情報セキュリティポリシー』に対する意見や要望を収集し、その妥当性を評価するとともに必要に応じて内容の改訂を行うこととする。

１０．５　監査結果の評価及び改訂

情報セキュリティ委員会は、監査の結果を受けて、『情報セキュリティポリシー』の妥当性を評価すると共に、必要に応じて、内容の改訂を行わなければならない。

１０．６　取締役会への報告

情報セキュリティ委員会は、情報セキュリティの維持・管理状況や『情報セキュリティポリシー』の改定状況、及び情報セキュリティに関する事故や問題の発生状況を取締役会へ報告しなければならない。

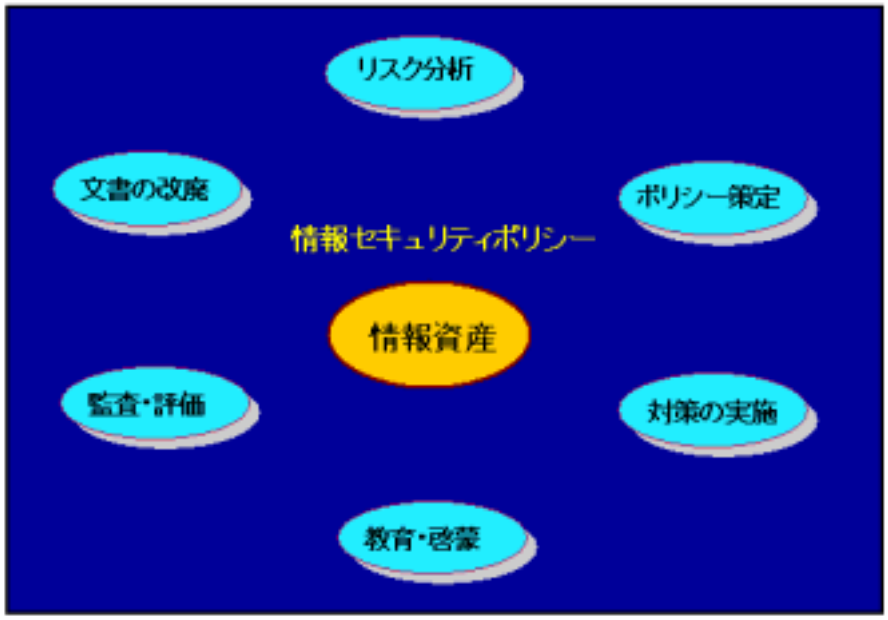
１０．７　『情報セキュリティポリシー』違反者への処罰

情報セキュリティ委員会は、従業員の『情報セキュリティポリシー』に違反した行為等が判明した場合、該当従業員に対して適切な処置を講じることとする。場合によっては、人事規定に基づいた処罰を人事部に申請することとする。

１１　情報セキュリティマネジメント

当社は、情報資産を保護するために、情報セキュリティマネジメントを以下の通り進めることとする。

＜情報セキュリティマネジメントサイクル＞



１１．１　リスク分析

当社の情報資産に関するリスクアセスメント、リスクマネジメント全般は、情報セキュリティ委員会が行うこととする。

１１．２　ポリシー策定

『情報セキュリティポリシー』の策定･評価･レビューは情報セキュリティ委員会が行うこととする。

情報セキュリティ委員会では、方針および対策標準を策定することとする。

対策手順書に関しては、情報セキュリティ委員会より指名された各情報システムの担当者が策定し、運用しなければならない。

１１．３　対策の実施

当社で策定した『情報セキュリティポリシー』に記述した対策は、計画的に実装しなければならない。情報システム部は、セキュリティ対策実装のための計画書を策定し、情報セキュリティ委員会の承認を得なければならない。

１１．４　教育・啓蒙

当社は、情報資産を扱うすべてのものに対し、意識向上と技術レベルの向上の両面から、積極的に情報セキュリティの教育を行うこととする。

当社の情報資産に関わるすべて者は、会社が提供する情報セキュリティの教育を受けなければならない。同時に、当社の情報資産に関わる者は、情報セキュリティに関する最新の情報について、自発的に情報セキュリティ委員に提言することが望ましい。

１１．５　監査・評価

情報セキュリティ委員会は、定期的あるいは発見の可能性のあるときに情報セキュリティに対する脅威、脆弱性を洗い出し、その対策を検討し、『情報セキュリティポリシー』に反映させなければならない。それらは、監査の結果、情報資産の利用者から届けられた情報、情報セキュリティの脆弱性に関する情報の収集等の活動から得られる情報をもとに行われる場合もある。

１１．６　文書の改廃

『情報セキュリティポリシー』の改廃は、方針は、取締役会の承認を必要とする。対策標準及び実施手順は、情報セキュリティ委員会が決議する。

１２　違反時における罰則

当社は、『情報セキュリティポリシー』の違反者に対し、厳格な措置をとることとする。情報セキュリティ委員会は、『情報セキュリティポリシー』に違反した事項の重要度を評価し、適切な処置を講じることとする。

１３　情報セキュリティ侵害時の対応

当社の情報セキュリティが侵害されたと思われる事象が判明した場合は、速やかに準備された対応方法に従って対応しなければならない。

１４　執行期日

本方針は、平成ｘｘ年ｘｘ月ｘｘ日に取締役会にて承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。