

2.外部ネットワーク接続セキュリティ方針

0.9 版

----- 取扱注意事項 -----

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「外部接続に関する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. 既存のネットワークにおける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著作権は日本ネットワーク・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 作成サンプルポリシー」を明記して下さい。営利目的でも非営利目的の区別はありません。
- 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などマスコミ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ェ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

2	外部ネットワーク接続セキュリティ方針	3
2.1	趣旨	3
2.2	『外部ネットワーク接続 情報セキュリティポリシー』の適用範囲	4
2.3	『外部ネットワーク接続 情報セキュリティポリシー』の適用者	5
2.3.1	経営陣の責務	5
2.3.2	従業員の責務	5
2.3.3	外部委託業者に対する対応	5
2.4	『外部ネットワーク接続 情報セキュリティポリシー』の構成と位置付け	6
2.4.1	外部ネットワーク接続セキュリティ基本方針	6
2.4.2	外部ネットワーク接続セキュリティ方針	6
2.4.3	外部ネットワーク接続セキュリティ対策標準	6
2.4.4	外部ネットワーク接続セキュリティ実施手順書	6
2.4.5	既存の規定との関連	6
2.4.6	その他関連法規	6
2.5	『外部ネットワーク接続 情報セキュリティポリシー』の公開対象者	7
2.6	『外部ネットワーク接続 情報セキュリティポリシー』の公開	7
2.7	基本用語の定義	7
2.7.1	情報セキュリティ (BS7799 より抜粋)	8
2.7.2	リスクアセスメント (BS7799 より抜粋)	8
2.7.3	リスクマネジメント (BS7799 より抜粋)	8
2.7.4	脅威	8
2.7.5	脆弱性	8
2.8	体制	9
2.8.1	情報セキュリティ委員会	9
2.8.2	情報システム部	10
2.8.3	システムセキュリティ責任者	10
2.8.4	システム管理者	10
2.8.5	オペレーター	10
2.8.6	セキュリティ担当者	10
2.9	情報セキュリティ委員会の体制図及び構成メンバー	11
2.9.1	情報セキュリティ委員会の体制図	11
2.9.2	常勤委員	11
2.9.3	非常勤委員	11
2.9.4	委員長	11
2.9.5	副委員長	12
2.9.6	委員	12

2.9.7	事務局	12
2.9.8	タスクフォース	12
2.10	情報セキュリティ委員会の役割と責務	12
2.10.1	情報セキュリティマネジメントの企画及び計画	12
2.10.2	『外部ネットワーク接続 情報セキュリティポリシー』文書の配布責任	13
2.10.3	社内教育の実施	13
2.10.4	『外部ネットワーク接続 情報セキュリティポリシー』の遵守状況の評価及び改訂	13
2.10.5	監査結果の評価及び改訂	13
2.10.6	取締役会への報告	13
2.10.7	『外部ネットワーク接続 情報セキュリティポリシー』違反者への処罰	13
2.11	情報セキュリティマネジメント	14
2.11.1	リスク分析	14
2.11.2	ポリシー策定	14
2.11.3	対策の実施	15
2.11.4	教育・啓蒙	15
2.11.5	監査・評価	15
2.11.6	文書の改廃	15
2.12	違反時における罰則	15
2.13	情報セキュリティ侵害時の対応	15
2.14	執行期日	16

2 外部ネットワーク接続セキュリティ方針

2.1 趣旨

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が、現状を振り返ってみると、我々は、経営に大きな影響を与えるネットワークコンピュータ環境を、セキュリティ対策が十分に考慮されていない状態で利用し、重要な情報が無造作に取り扱われている状況を目にすることがある。

昨今、セキュリティに関する事件による被害は増大しており、我社でも、今後は、セキュリティを意識したネットワークコンピュータの利用を行っていかねばならないことは自明である。

我社は、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などの情報システム（以下、情報資産）を第4の資産として位置付け、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した。これは、我社の情報資産を、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り、情報資産へのセキュリティリスクを如何に軽減していくかについても規定するものである。

我社の情報セキュリティポリシーのうち、『外部ネットワーク接続 情報セキュリティポリシー』は、我社の外部接続ネットワークにおけるセキュリティの運用・管理を目的として策定された文書である。

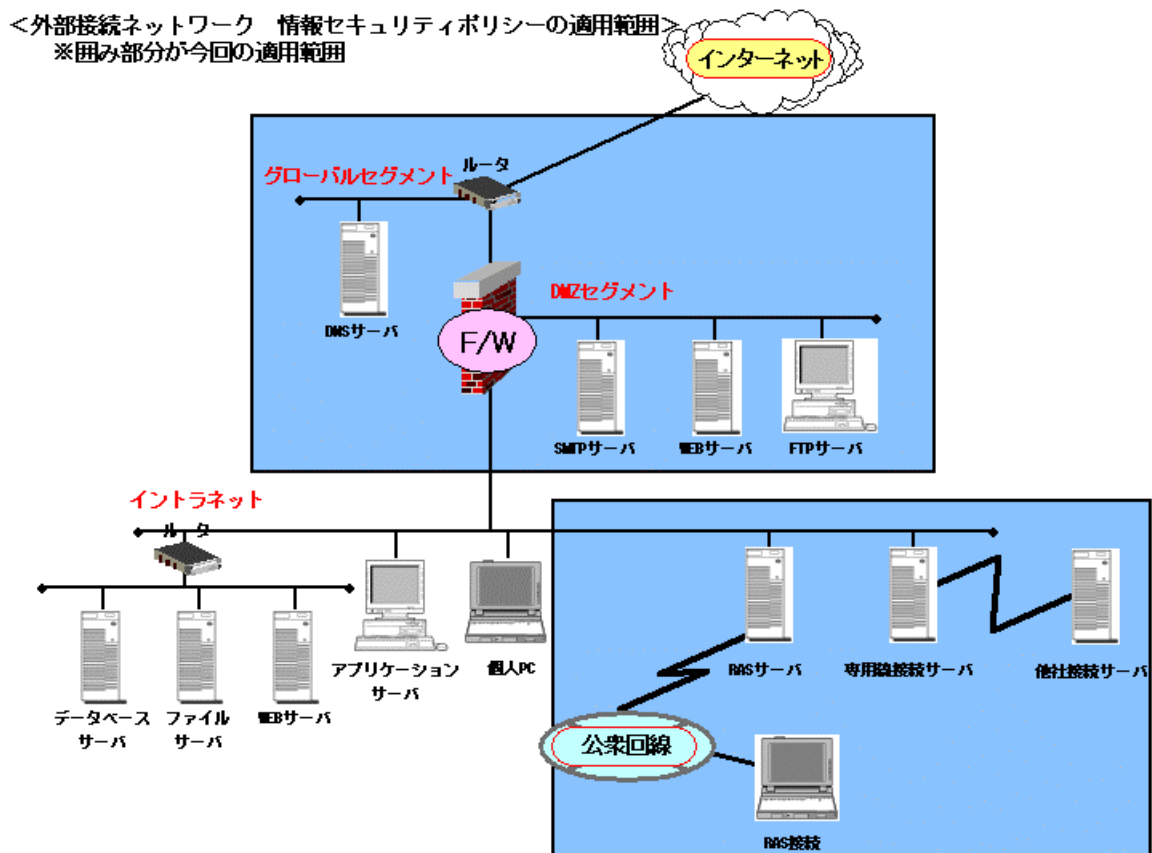
本外部ネットワーク接続セキュリティ方針では、外部接続ネットワークにおける情報セキュリティマネジメントの方針を記述する。

2.2 『外部ネットワーク接続 情報セキュリティポリシー』の適用範囲

本『外部ネットワーク接続 情報セキュリティポリシー』の適用範囲は、我社の「外部接続ネットワーク」に限定したものとす（定義事項）。

「外部接続ネットワーク」とは、外部からアクセスできる我社の情報資産に関するものから、弊社から外部ネットワークサービスの利用に関するものまでを含む（定義事項）。また、上記「外部接続ネットワーク」を考慮した場合に派生する物理的・人的セキュリティ管理策も一部では取り込まれている。

外部からアクセスできる我社の情報資産の具体例は、下図で示している範囲である。



2.3 『外部ネットワーク接続 情報セキュリティポリシー』の適用者

我社の経営陣・社員・契約社員（パートタイマーを含む）・第三者常駐者・外部委託者を従業員と定義する。

本『外部ネットワーク接続 情報セキュリティポリシー』の適用者は、従業員を含めた、我社の情報資産を利用するすべての者である。

2.3.1 経営陣の責務

経営陣は、『外部ネットワーク接続 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(必須行為)。

2.3.2 従業員の責務

従業員には、我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、私的利用までを許可するものではない(禁止)。

従業員は、情報資産を扱う上で、企業利益の維持・向上のために、『外部ネットワーク接続 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(必須行為)。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(必須行為)。

2.3.3 外部委託業者に対する対応

『外部ネットワーク接続 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(必須行為)。

2.4 『外部ネットワーク接続 情報セキュリティポリシー』の構成と位置付け

我社の『外部ネットワーク接続 情報セキュリティポリシー』は、以下の4つの階層に分けて策定・管理される文書とする（定義事項）。

2.4.1 外部ネットワーク接続セキュリティ基本方針

外部ネットワーク接続セキュリティ基本方針（以下、基本方針とする）は、我社の情報セキュリティマネジメントの取り組みを広く一般に知らしめるための文書である（定義事項）。

2.4.2 外部ネットワーク接続セキュリティ方針

外部ネットワーク接続セキュリティ方針（以下、セキュリティ方針とする）は、『外部ネットワーク接続 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（定義事項）。この文書は、我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（定義事項）。この文書に基づいて下層の文書（ルール規定）を策定する（支援義務）。

2.4.3 外部ネットワーク接続セキュリティ対策標準

外部ネットワーク接続セキュリティ対策標準（以下、対策標準とする）は、セキュリティ方針の下層に位置する文書である（定義事項）。この文書は、セキュリティ方針での宣言を受け、各項目毎に遵守すべき事項を網羅的に記述したものである（定義事項）。

2.4.4 外部ネットワーク接続セキュリティ実施手順書

外部ネットワーク接続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（定義事項）。この文書は、対策標準で記述された文書をより具体的に、配布すべき対象者毎に内容をカスタマイズしたものである（定義事項）。

2.4.5 既存の規定との関連

基本方針及びセキュリティ方針は、我社の他の規定（人事規定、就業規則等）と同等の位置付けの文書とする（定義事項）。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（定義事項）。

2.4.6 その他関連法規

本『外部ネットワーク接続 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(必須行為)。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。(必須行為)
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 (BS7799)
- ・ 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

2.5 『外部ネットワーク接続 情報セキュリティポリシー』の公開対象者

基本方針は、公開情報である。よって、社内及び社外の者すべてが公開対象である。
(定義事項)

セキュリティ方針は、従業員すべてを公開対象とする(定義事項)。一般には公表しない機密情報として取り扱う。以下、基本方針以外の文書は機密情報である。(定義事項)

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(定義事項)。

実施手順書は、該当する業務を行う者を公開対象とする(定義事項)。

2.6 『外部ネットワーク接続 情報セキュリティポリシー』の公開

基本方針を除く、『外部ネットワーク接続 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(必須行為)。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、公開を認めることがある。(権限留保)

2.7 基本用語の定義

本基本『外部ネットワーク接続 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される(定義事項)。

2.7.1 情報セキュリティ (BS7799 より抜粋)

情報の機密性、完全性及び利用の可用性の維持することとする (定義事項)。

注)

機密性とは、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、として定義する。

完全性とは、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、として定義する。

利用性とは、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、として定義する。

2.7.2 リスクアセスメント (BS7799 より抜粋)

情報及び情報処理施設/設備に対する脅威、影響及び脆弱性並びにそれらがおこる可能性の評価のこととする (定義事項)。

2.7.3 リスクマネジメント (BS7799 より抜粋)

許容範囲のコストにより、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、それを制御し、最小限に抑制するか、あるいは除去するプロセスのこととする (定義事項)。

2.7.4 脅威

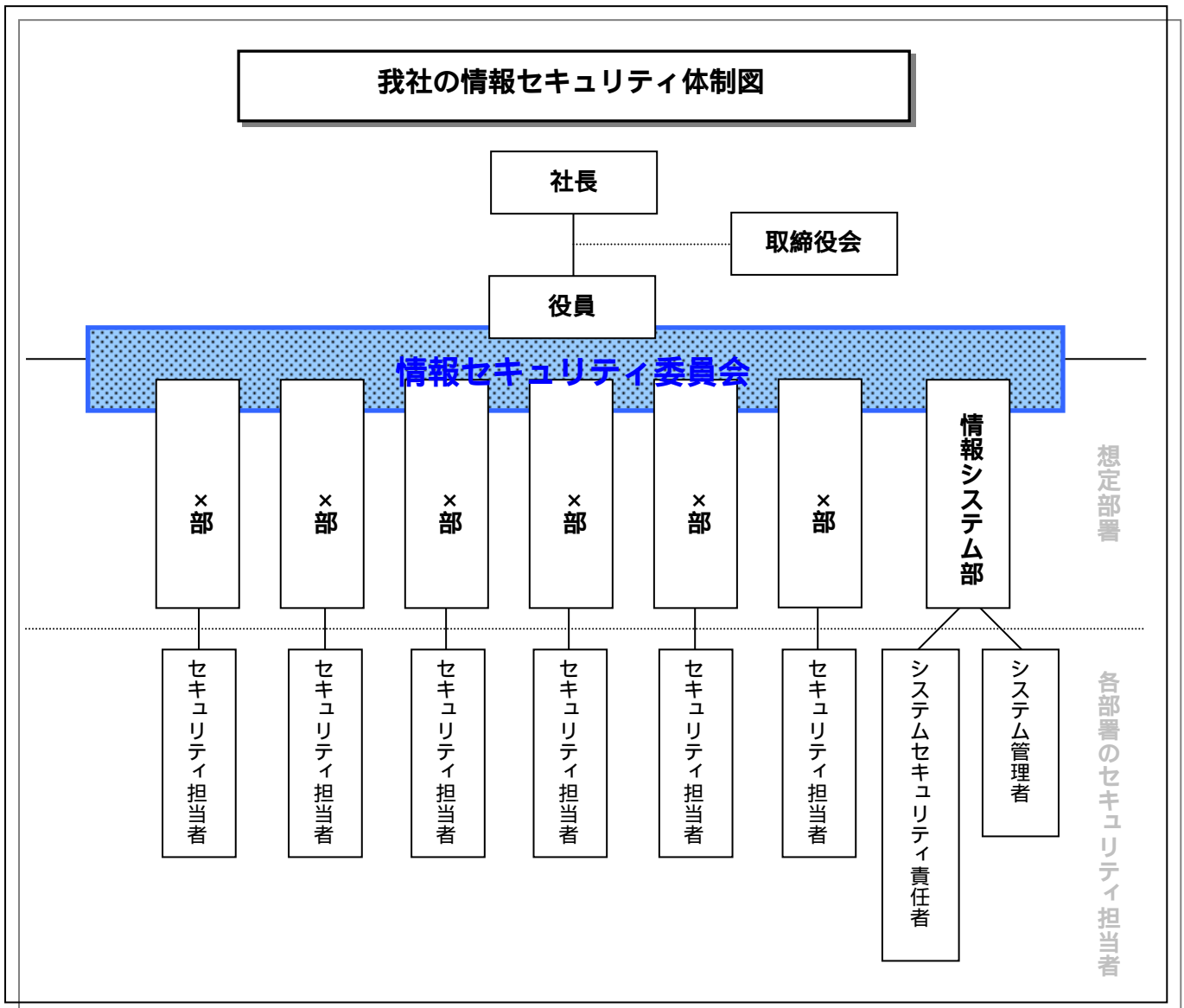
自然災害、機器障害、悪意のある行為など、損失を発生させる直接の要因である (定義事項)。

2.7.5 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・要員教育の不備など、脅威を発生し易くさせる要員、脅威を増加させる要因 (脆さ、弱点) のことである (定義事項)。

2.8 体制

我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（定義事項）。
体制図は下図を参照のこと。



2.8.1 情報セキュリティ委員会

我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（定義事項）。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。

2.8.2 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である。(定義事項)

情報システム部は、我社の情報機器の管理責任を有し、当社に係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。(必須行為)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。(必須行為)

2.8.3 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。(定義事項)

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。(必須行為)

2.8.4 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作業の管理責任を有する。(定義事項)

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。(定義事項)

2.8.5 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の実質的な作業を行う者である。(定義事項)

2.8.6 セキュリティ担当者

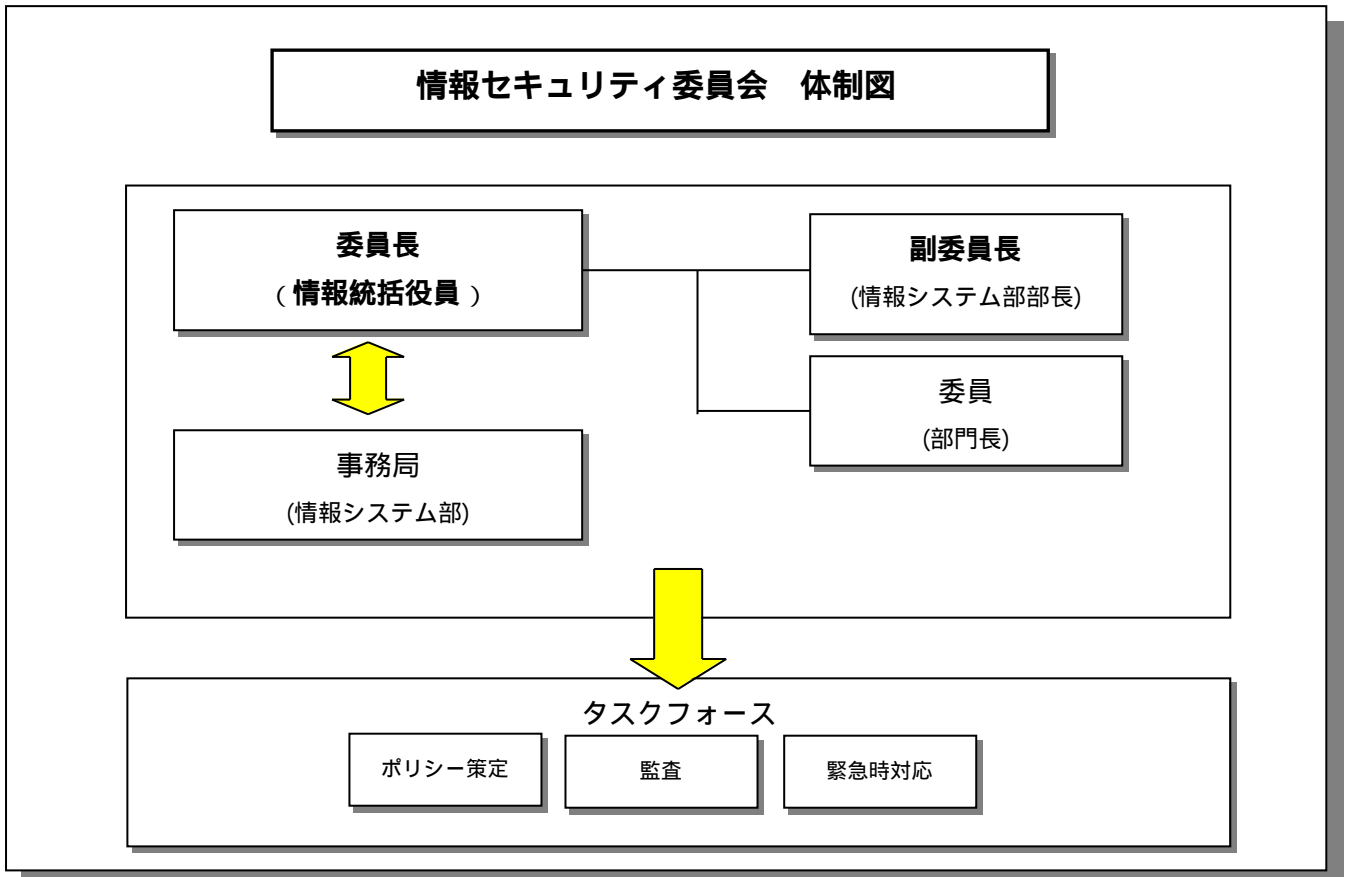
セキュリティ担当者は、情報システム部以外の各部署の部門長によって最低一人任命され、配置される者である。(定義事項)

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。(定義事項)

2.9 情報セキュリティ委員会の体制図及び構成メンバー

2.9.1 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。



2.9.2 常勤委員

常勤委員は、委員長、副委員長、委員とする(定義事項)。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(必須行為)。

2.9.3 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(定義事項)。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(定義事項)。

2.9.4 委員長

委員長は、我社の役員を情報統括役員として取締役会で指名する(定義事項)。委員長は、我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(定義事項)。

2.9.5 副委員長

副委員長は、情報システム部部长とする(定義事項)。副委員長は、委員長の補佐役である(定義事項)。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、委員長の代理となつて、職務を遂行する(定義事項)。

2.9.6 委員

委員は、各部門長とする(定義事項)。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。

2.9.7 事務局

事務局は、情報システム部とする(定義事項)。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(定義事項)。

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『外部ネットワーク接続 情報セキュリティポリシー』文書の管理を行う(定義事項)。

2.9.8 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つ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(定義事項)。タスクフォースには、『外部ネットワーク接続 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(定義事項)。

2.10 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(定義事項)。

2.10.1 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、我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(必須事項)。

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、『外部ネットワーク接続 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(必須事項)。

2.10.2 『外部ネットワーク接続 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、『外部ネットワーク接続 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(必須行為)。

2.10.3 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(定義事項)。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。(必須行為)

2.10.4 『外部ネットワーク接続 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『外部ネットワーク接続 情報セキュリティポリシー』遵守状況を定期的に調査し、『外部ネットワーク接続 情報セキュリティポリシー』のレビューを行う(定義事項)。また、従業員の『外部ネットワーク接続 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。(定義事項)

2.10.5 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、『外部ネットワーク接続 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(必須事項)。

2.10.6 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『外部ネットワーク接続 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(必須事項)。

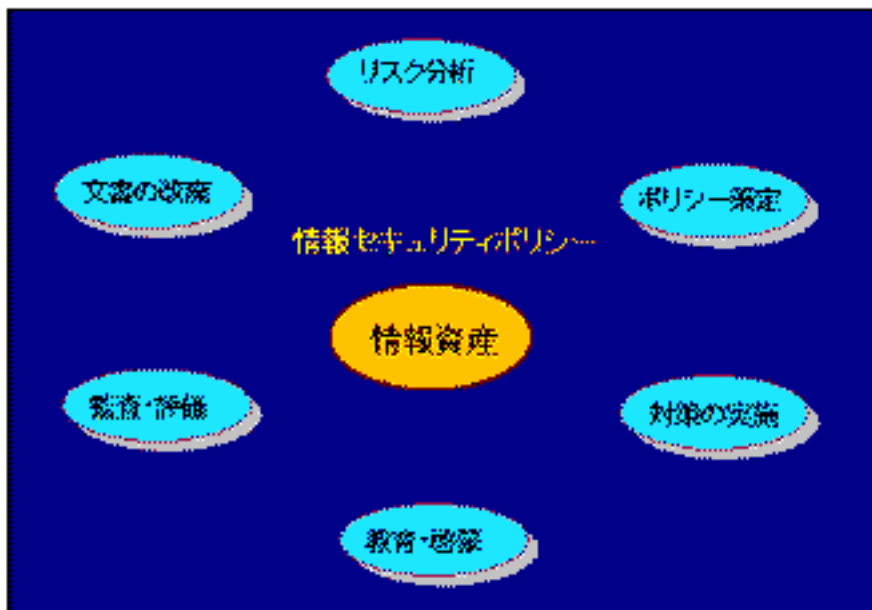
2.10.7 『外部ネットワーク接続 情報セキュリティポリシー』違反者への処罰

情報セキュリティ委員会は、従業員の『外部ネットワーク接続 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。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。

2.11 情報セキュリティマネジメント

我社は、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（定義事項）。

<情報セキュリティマネジメントサイクル>



2.11.1 リスク分析

我社の情報セキュリティ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によって行われる（定義事項）。

2.11.2 ポリシー策定

『外部ネットワーク接続 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によって行われる（定義事項）。

情報セキュリティ委員会では、『外部ネットワーク接続 セキュリティ基本方針』及び『外部ネットワーク接続 セキュリティ方針』並びに『外部ネットワーク接続 セキュリティ対策標準』を策定する。『外部ネットワーク接続 セキュリティ対策手順書』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。

2.11.3 対策の実施

我社で策定した『外部ネットワーク接続 情報セキュリティポリシー』は、従業員にとっては遵守することが前提であり、通常業務と兼務でセキュリティ対策を担当しなければならなくなった者には、兼務だからという「甘え」を許してはいけない。

2.11.4 教育・啓蒙

我社は、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（支援義務）。我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（必須義務）。同時に、我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（推奨行為）。

2.11.5 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、『外部ネットワーク接続 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。（必須行為）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。

2.11.6 文書の改廃

『外部ネットワーク接続 情報セキュリティポリシー』の改廃は、基本方針及びセキュリティ方針は、取締役会の承認を必要とする。（定義事項）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。（定義事項）

2.12 違反時における罰則

我社は、『外部ネットワーク接続 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。情報セキュリティ委員会は、『外部ネットワーク接続 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（定義事項）。

2.13 情報セキュリティ侵害時の対応

我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（必須行為）。

2.14 執行期日

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