情報セキュリティ基本方針

1.0 版

情報セキュリティ基本方針

ＩＴ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、コンピュータ上で扱われることが当然のこととなった。ＩＴ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、ＩＴ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十分に認知し、この『情報セキュリティポリシー』を遵守しなければならない。

情報セキュリティ方針

1.0版

情報セキュリティ方針

情報セキュリティ方針

１　趣旨

(A.5.1)

ＩＴ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、コンピュータ上で扱われることが当然のこととなった。ＩＴ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、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。

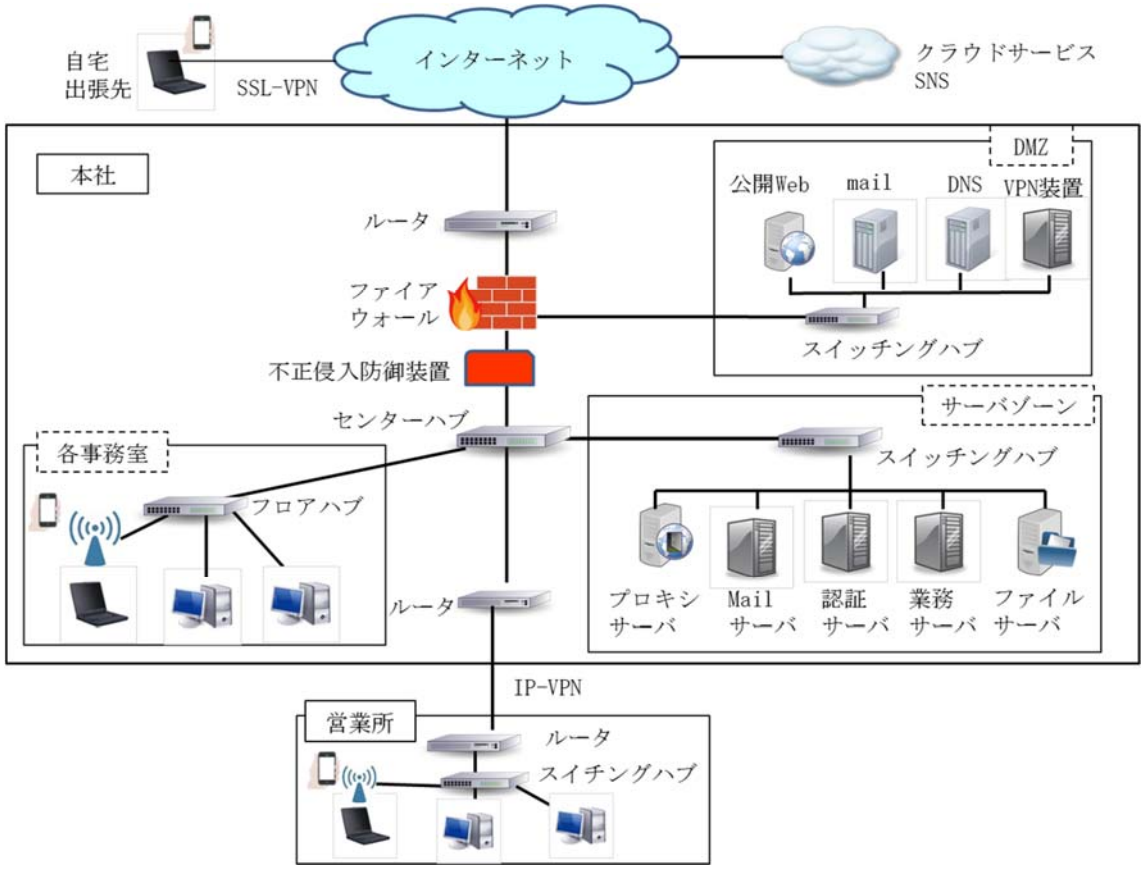
当社の情報資産を利用する者は、情報セキュリティの重要性を十分に認知し、この『情報セキュリティポリシー』遵守しなければならない。

２　『情報セキュリティポリシー』の適用範囲

(A.5.1.1)

『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・環境的リソースを含むものとする。

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

(A.5.1.1　A.6.1.1)

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

(A.7.2.1)

経営陣は、『情報セキュリティポリシー』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

（A.5.1.1　A.6.1）

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、私的利用を認めるものではない。

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

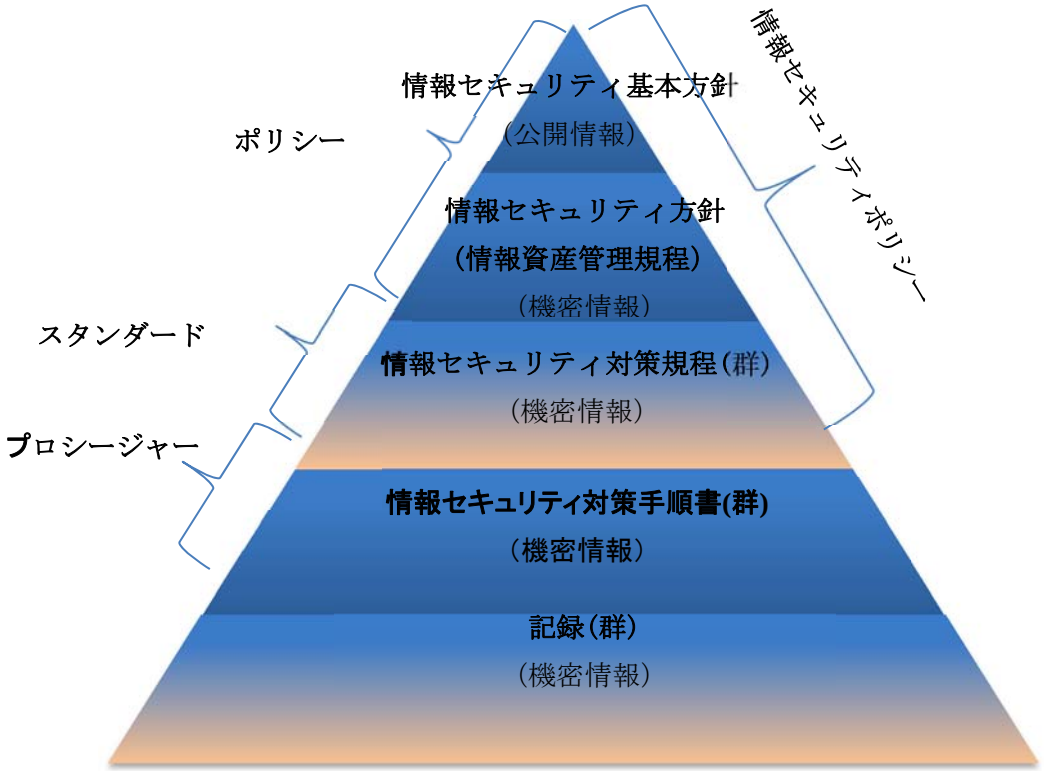
（A.5.1.1　A.14.2.7）

『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

（A.5.1.1）

『情報セキュリティポリシー』は、以下の「情報セキュリティ基本方針」を含む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

(A.5.1)

情報セキュリティ方針（以下、「方針」とする）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規程

(A.5.1.1)

情報セキュリティ対策規程（以下、「対策規程」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　情報セキュリティ対策手順書

(A.5.1.1)

情報セキュリティ対策手順書（以下、「対策手順書」とする）は、対策規程の下層に位置する文書である。この文書は、対策規程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　既存の規程との関連

(A.5.1.1)

方針は、当社の他の規程（人事規程、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程に準じて行うものとする。

４．５　その他関連法規

(A.5.1.1　A.18.1)

『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 27000 シリーズ

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（不正アクセス禁止法）
・ 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・個人情報の保護に関する法律（個人情報保護法）
・ 行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（番号法）
・外国為替及び外国貿易法（外為法）および輸出貿易管理令
・労働契約法
・労働基準法
・会社法
・金融商品取引法
・刑事訴訟法

５　『情報セキュリティポリシー』の公開対象者

(A.6.1.1)

（１）情報セキュリティ基本方針は、一般に公開する。

（２）情報セキュリティ方針は、従業員すべてに公開とする。外部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。情報セキュリティ方針以外の文書も機密情報である。

情報セキュリティ対策規程は、情報セキュリティ委員会メンバーと担当部署の者に公開とする。

（３）対策手順書は、該当する業務を行う者に公開とする。

（４）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。

６　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。

６．１　情報セキュリティ

情報の機密性、完全性及び可用性を維持すること。

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。

可用性は、許可されたユーザが、必要時に、必要な情報及び関連資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。

６．２　リスクアセスメント

情報及び情報処理施設/設備に対する脅威と重要度を特定し、事故発生につながる脆弱性及び事故のおこりやすさを評価すること。

６．３　リスクマネジメント

リスクアセスメントにより、情報及び情報処理施設/設備に影響を及ぼす可能性がある情報セキュリティリスクを明確にし、許容コストに応じて情報セキュリティリスクを制御し、最小限に抑制するか、又は除去するプロセスを指す。

６．４　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。

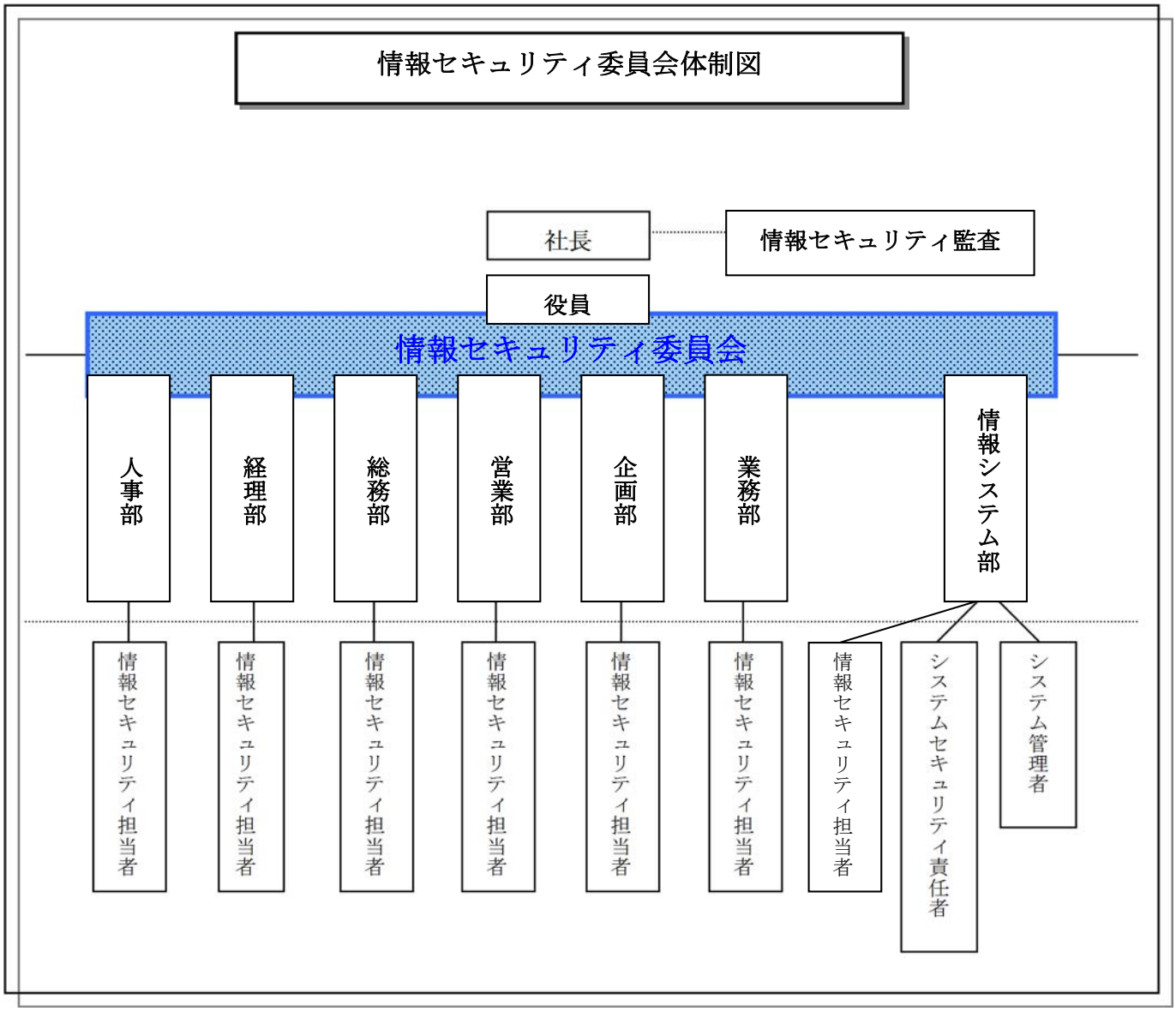
６．５　脆弱性

ハードウェア・ソフトウェアの欠陥、定期点検の不備、要員教育の不備等、脅威を増加させる要因（脆さ、弱点）のこと。

7　体制

(A.6.1)

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。



7．1　情報セキュリティ委員会

(A.6.1.1)

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。

７．２　情報システム部

(A.6.1.2)

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。

７．３　システムセキュリティ責任者

(A.6.1.2)

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。

７．４　システム管理者

(A.6.1.2)

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。

７．５　オペレーター

(A.6.1.2)

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。

７．６　情報セキュリティ担当者

(A.6.1.2)

情報セキュリティ担当者は、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。

情報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運用の点検結果の収集担当であり、収集した情報は各部の情報セキュリティ委員へ報告する。

７．７　情報セキュリティ監査

(A.6.1.2　A.12.7)

情報セキュリティ監査は、運用部門とは独立した組織を構成する事を目的とする。

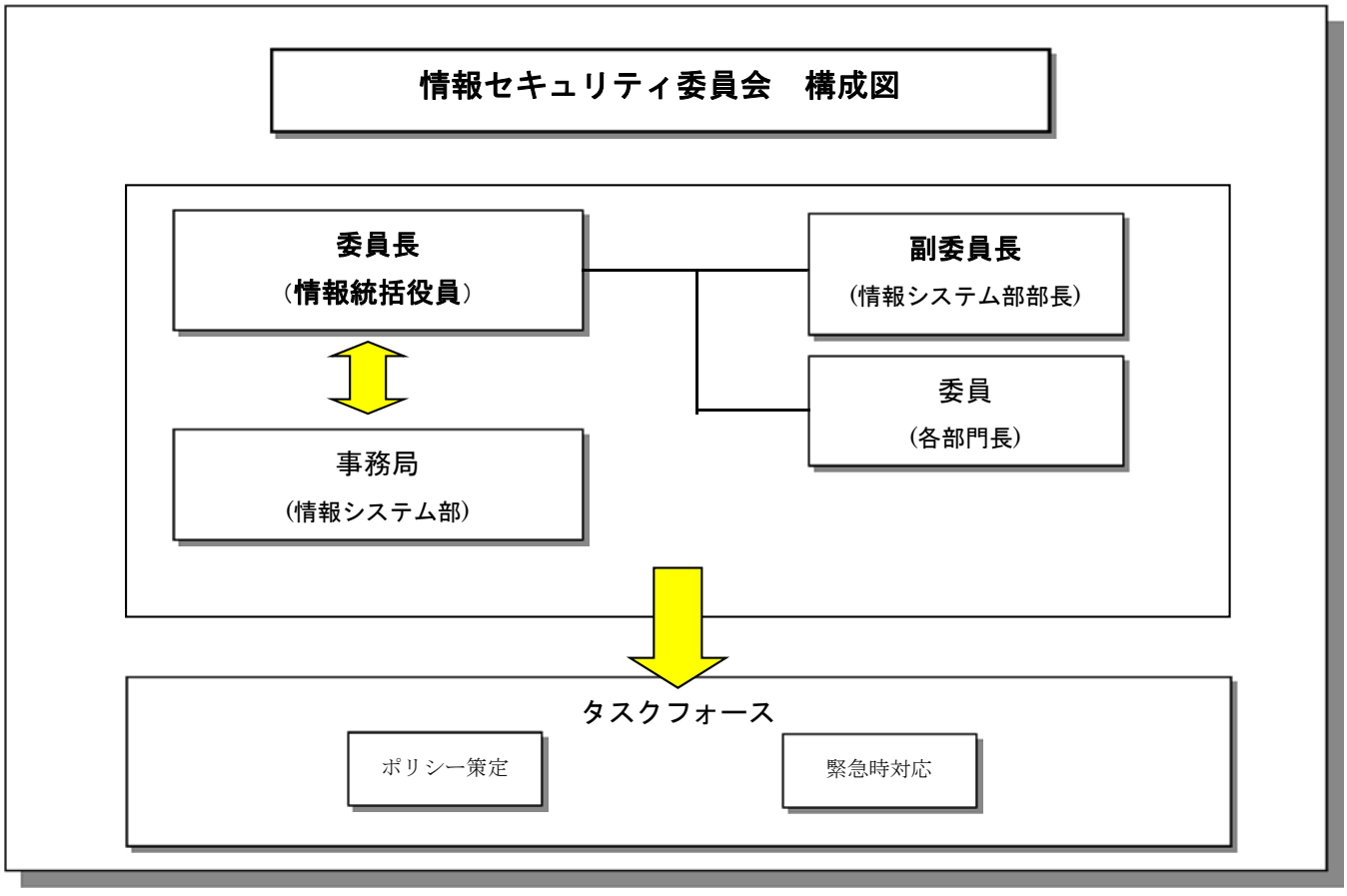
監査人は、自部門業務を監査しない体制を確保する事が望ましい。

８　情報セキュリティ委員会の構成図及び構成メンバー

８．１　情報セキュリティ委員会の構成図

(A.6.1.2)

委員会の構成は下図の通り定める。



８．２　常勤委員

常勤委員は、委員長、副委員長、委員とする。

８．３　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。

８．４　委員長

委員長は、当社の役員を情報統括役員として社長が任命する。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。

８．５　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。

８．６　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。

８．７　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。

８．８　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、緊急時対応等の作業を実施する。

９　情報セキュリティ委員会の役割と責務

(A.6.1.2)

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。

９．１　情報セキュリティマネジメントの企画及び計画

(A.6.1.1)

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。

９．２　『情報セキュリティポリシー』文書の配布責任

(A.7.2.2)

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、周知徹底させなければならない。

９．３　社内教育の実施

(A.7.2.2)

情報セキュリティ委員会は、経営陣、従業員に対し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。

９．４　『情報セキュリティポリシー』の遵守状況の評価及び改訂

(A.18.2.2)

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・準拠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。

９．５　監査結果の評価及び改訂

(A.18.2.2)

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。

９．６　社長への報告

(A.18.2.2)

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』の改訂状況、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社長へ報告しなければならない。

９．７　『情報セキュリティポリシー』違反者への処罰

(A.7.2.3)

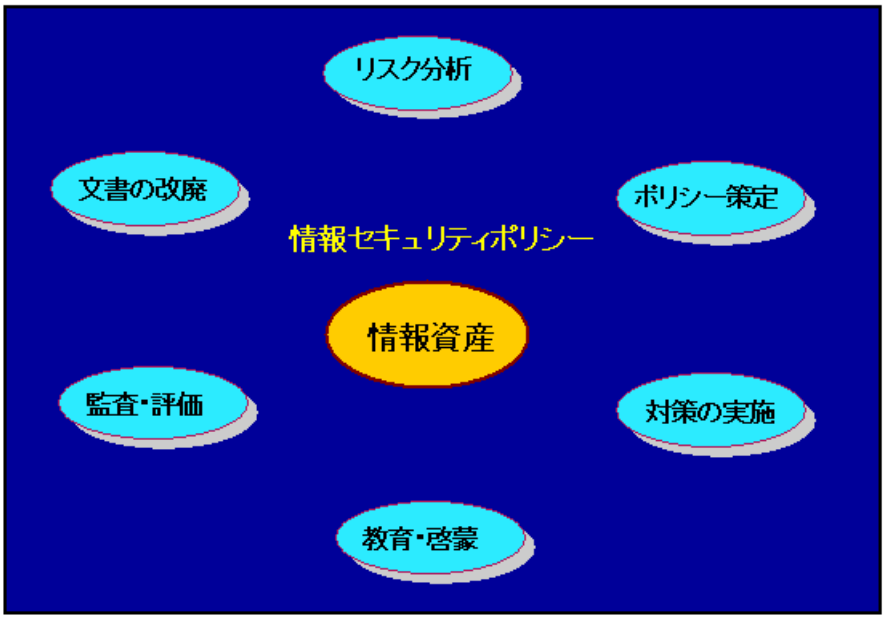
情報セキュリティ委員会は、従業員の『情報セキュリティポリシー』に違反した行為等が判明した場合、該当従業員に対して適切な処置を講じることとする。場合によっては、人事規程に基づいた処罰を人事部に申請することとする。

１０　情報セキュリティマネジメント

(A.5.1.1)

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＞



１０．１　リスク分析

(A.5.1.1)

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。

１０．２　情報セキュリティポリシー策定

(A.4.2　A.18.22)

『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、方針および対策規程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。

１０．３　対策の実施

(A.17.1.2)

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。

１０．４　教育・啓蒙

(A.7.2.2)

当社は、情報資産を扱うすべての者に対し、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教育を行うこととする。

当社の情報資産に関わるすべての者は、当社が実施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。

１０．５　評価

(A.18.2)

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。

１０．６　文書の改廃

(A.5.1.2)

『情報セキュリティ方針』及び『情報セキュリティ基本方針』の改廃は、社長の承認を必要とする。対策規程及び対策手順は、情報セキュリティ委員会が承認する。

１１　違反時における罰則

(A.7.2.3)

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。

１２　情報セキュリティ侵害時の対応

(A.16.1)

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。

１３　改訂

本方針は、平成ｘｘ年ｘｘ月ｘｘ日に社長によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

人的管理規程

1.0版

人的管理規程

人的管理規程

１　趣旨

本規程では、役員を含む従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にすることを目的とする。

２　対象者

当社の情報資産に携わっているすべての者（役員、従業員、契約相手、またはそれを運用、管理し、業務に携わっているすべての者）を対象とする。

３　対象システム

本規程は人的管理に関するものであり、情報システムや情報機器を対象としない。

４　遵守事項

４．１　雇用

４．１．１　雇用前

(A.7.1)

役員、従業員の雇用にあたっては、以下の事項を遵守しなければならない。

（１）経歴等の確認については、関連法令、規則及び倫理に従って行うこと。またこの確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行うこと。

（２）応募者の情報は、個人情報保護法に基づき、適切に処置すること。

（３）雇用する場合には、以下の事項について確認を行うこと。

・情報セキュリティに関するその役割を果たすために、必要な力量を備えていること

・組織にとって、その役割を任せられ、信頼できる人物であること

４．１．２　雇用条件

(A.7.1.2)

当社の情報資産に携わっているすべての者は、以下の条件を遵守しなければならない。

（１）従業員及び契約相手との雇用契約書には、情報セキュリティに関する責任及び組織の責任を記載しておくこと。

（２）従業員及び契約相手の契約上の義務ついて、以下の事項を明確にしておくこと。

・秘密保持契約書又は守秘義務契約書への署名、捺印をすること

・扱われる情報資産に対する保護、管理に関する責任を明確にしておくこと

・当社が定める情報セキュリティに関する要求事項に従わない場合にとる処置に

ついて、明確にしておくこと
・雇用期間の終了後についても、この雇用条件に定められた責任が継続することを明確にしておくこと

４．１．３　雇用期間中

(A.7.2)

当社の情報資産に携わっているすべての者は、以下を遵守しなければならない。

（１）組織の確立された方針及び手順に従った情報セキュリティの適用を、従業員及び契約相手に要求すること。

（２）職務に関連する組織の方針及び手順について、適切な意識向上のための教育及び訓練を定期的に受けること。

（３）教育、訓練の内容には、以下の項目を含めること。

・情報セキュリティに関する経営陣のコミットメント
・情報セキュリティに関する規則及び義務を熟知し、これを遵守すること
・情報セキュリティに関する基本的な手順及び規則
・これらに違反した場合の処置

４．１．４　雇用終了及び変更

(A.7.3)

当社の情報資産に携わっているすべての者は、以下を遵守しなければならない。

（１）雇用の終了又は変更後も、秘密保持契約又は守秘義務契約内容が継続することを、十分に認識させること。

４．２　プライバシー及び個人を特定できる情報の保護

(A.18.1.4)

顧客の個人情報（以下「顧客情報」とする）を適切に収集・保管・廃棄における取り扱い時に注意するべき事項をまとめ、発生しうる問題を未然に防ぐことを目的とする。

顧客情報を取り扱うすべてのコンピュータ及び媒体を対象とする。

４．２．１　顧客情報を取り扱う部門の特定

(A.8.1)

役員、従業員は、以下を遵守しなければならない。

（１）情報セキュリティ委員会は、当社内にて顧客情報を取り扱う部門を特定し、その部門長に対して、以下の遵守事項を徹底させなければならない。又、当該従業員に対する顧客情報の取り扱いについて、十分認識させなければならない。(「４．３情報セキュリティ教育」参照)

（２）特定されていない部門においては、顧客情報を取り扱ってはならない。

４．２．２　顧客情報管理責任者の設置

(A.8.1.2)

役員、従業員は、以下を遵守しなければならない。

（１）顧客情報の収集・保管・廃棄を行う部門の部門長は、顧客情報管理責任者を任命し、部門内に保有する顧客情報について、それぞれの責任者を明確にしなければならない。

４．２．３　顧客情報保護方針の公開

(A.18.1.4)

役員、従業員は、以下を遵守しなければならない。

（１）顧客情報管理責任者は、顧客情報を広く一般から収集する場合、当社の Web サイトや広告等に当社の顧客情報保護方針を公開しなければならない。

（２）顧客情報保護方針には、下記に記載される遵守事項の内容および当社への連絡先を明確にしなければならない。

４．２．４　顧客情報の収集

(A.8.1.1)

顧客情報の収集を行う者は、以下の事項を遵守しなければならない。

（１）顧客情報の収集時には、顧客に対して利用目的を明示し、顧客から同意を得なければならない。なお、収集以外の形で得た顧客情報を利用する場合は改めて顧客から同意を得なければならない。

（２）顧客に示した利用目的に必要な情報以外の情報を収集してはならない。

（３）収集した情報を顧客に明示した利用目的以外の利用をしてはならない。

４．２．５　顧客情報の保管

(A.8.1.2)

顧客情報管理責任者は、以下の事項を遵守しなければならない。

（１）顧客情報に対する登録・参照・変更・削除の実施可能な者を明確にし、顧客情報へのアクセス制限を実施しなければならない。

（２）顧客情報を利用する場合、正確な情報を利用しなければならず、そのための保護策を実施しなければならない。

（３）顧客情報のバックアップを実施しなければならない。バックアップした媒体は、顧客情報と同様の管理策を設けなければならない。

（４）顧客から当該顧客の顧客情報に関する開示・訂正・削除の要求があった場合、

これに対応しなければならない。

４．２．６　顧客情報の破棄

(A.8.1.4　A.8.3.2)

顧客情報管理責任者は、以下の事項を遵守しなければならない。

（１）顧客情報を廃棄する場合、第三者の目にさらされないように注意して廃棄しなければならない。

（２）電子媒体等の破棄においては、『システム利用規程』に基づいて実施しなければならない。

４．２．７　顧客からクレーム処理

(A.8.1.2)

顧客情報管理責任者は、以下の事項を遵守しなければならない。

（１）当社の業務において顧客からクレームを受けた場合には、速やかに対応しなければならない。

（２）顧客情報が漏えいしてしまったなど、必要がある場合、情報セキュリティ委員会を開催し、当社の見解を迅速に明確にし、関係者に周知しなければならない。

（３）いかなるクレームでも、第一報を 12 時間以内に情報セキュリティ委員会に報告し、その後の対応状況に関しても適宜連絡しなければならない。

４．３　情報セキュリティ教育

(A.7.2.2)

情報セキュリティ意識の向上のため、情報資産に携わっているすべての者、またはそれを運用、管理し、業務に携わっているすべての者を対象とし、情報セキュリティ教育、訓練に関わる事項を規定する。各自の責任及びその責任を果たす方法について、認識をさせることを目的とする。

４．３．１　教育の計画立案

(A.7.2.2)

教育部門ならびに、各部署の情報セキュリティ責任担当者は、対象者およびタイミング、もしくはその内容について、各教育を計画し、立案しなければならない。また、保護すべき情報及び情報を保護するために実施されている管理策を考慮に入れて、計画する。

（１）一般説明会

教育部門は、年に１回、情報資産に携わるすべての人に対して、情報セキュリティに関する説明会を実施しなければならない。

（2）再教育

教育部門は、情報セキュリティ違反者に対して、セキュリティの再教育を実施し、違反の再発防止に努めなければならない。

（3）新入社員、中間採用者への教育

教育部門は、新入社員、中間採用者に対して、入社時に情報セキュリティ教育を計画しなければならない。

（4）社内異動者への教育

各部署の情報セキュリティ責任担当者は、社内異動者に対して、異動時に、その部署の情報セキュリティに関して教育を計画しなければならない。

（5）契約社員および協力会社への教育

各部署の情報セキュリティ責任担当者は、契約社員および協力会社に対して、部署の情報セキュリティに関して、許可された権限と責務に応じた教育を計画しなければならない。

４．３．２　教育の実施

(A.7.2.2)

教育部門ならびに、各部署の情報セキュリティ責任担当者は、情報資産に携わるすべての人に対し、以下の教育内容について、教育資料を使用し、情報セキュリティ教育を実施しなければならない。

（1）教育内容

・当社の情報セキュリティ方針
・情報セキュリティの問題のもつ意味を理解
・組織や個人の情報セキュリティの重要性
・情報セキュリティ対策
・情報セキュリティ計画
・データ所有者の責任
・モラル教育
・法令、規則等の違反、罰則に関する事項
・禁止行為に関しての教育他
・最新の情報

（2）再教育

教育部門は、情報セキュリティ違反者に対して、情報セキュリティの再教育を実施し、違反の再発防止に努めなければならない。

（3）新入社員、中間採用者への教育

教育部門は、新入社員、中間採用者に対して、入社時に情報セキュリティ教育を実施しなければならない。

（４）社内異動者への教育

各部署の情報セキュリティ責任担当者は、社内異動者に対して、異動時に、その部署の情報セキュリティに関して教育を実施しなければならない。

（５）契約社員および協力会社への教育

各部署のセキュリティ責任担当者は、契約社員および協力会社に対して、部署の情報セキュリティに関して、許可された権限と責務に応じた教育を実施しなければならない。

４．３．３ 訓練の実施

(A.7.2.2)

教育部門ならびに、各部署の情報セキュリティ責任担当者は、情報セキュリティに責任をもつ対象者に対し、定期的に、以下の訓練内容について、訓練資料を使用し、情報セキュリティの訓練を実施しなければならない。

（１）訓練内容

・リスク分析
・情報セキュリティ対策についての導入、管理、運用、利用等
・情報セキュリティ問題の検出、検知、報告、復旧等

４．３．４ 教育、訓練資料

(A.7.2.2)

教育、訓練資料は、適切な教育、訓練を行うため、環境の変化及び、管理策の追加変更等を考慮に入れ、定期的な見直し行う。

教育、訓練資料には、以下のものがある。

・一般説明会教育資料
・再教育資料
・新入社員教育資料
・中間採用者教育資料
・社内異動者教育資料
・協力会社および契約社員教育資料
・情報セキュリティ対策訓練資料
・情報セキュリティ問題訓練資料

４．３．５ 教育実施記録

(A.7.2.2)

教育部門は、教育、訓練の実施状況に関して以下の記録を行わなければならない。

（１）記録項目

・教育の実施日、時間
・教育実施者（部署）
・教育の受講者
・教育の内容

４．３．６ 教育運用実施報告、確認

(A.7.2.2)

教育部門は、情報セキュリティ委員会に教育、訓練の実施状況を報告しなければならない。

情報セキュリティ委員会は、情報セキュリティの教育、訓練が適切に行われているかを把握するため、教育部門から提出される情報セキュリティ教育実施報告書を確認しなければならない。実施されていない場合、教育部門に対して、適切な指導を行わなければならない。

４．４ 懲戒手続

(A.7.2.3)

本規程は､当社の情報セキュリティ違反に対する罰則の適用手順及びそれに関わる遵守事項を規定する。

情報セキュリティ方針および規程類が適用されるすべての人を対象とする｡罰則事項の執行は、情報セキュリティ違反に対する罰則の適用に関わる情報セキュリティ委員会のメンバー、部門長及び人事部門の担当者を対象とする。

４．４．１ 罰則案件の届出

(A.7.2.3)

部門長は罰則に相当すると思われる従業員の情報セキュリティ違反を確認した場合、情報セキュリティ委員会に罰則の適用について審議を求める案件の届出を行わなければならない。なお、部門長の情報セキュリティ違反に関する罰則案件の届け出は情報セキュリティ委員会のメンバーが行うものとする。

４．４．２ 情報セキュリティ委員会での審議及び決定

(A.7.2.3)

情報セキュリティ委員会は届出が行われた罰則案件について審議を行い、罰則の適用と再教育についてその要否と程度または内容を決定しなければならない。また、審議するうえで、以下の事項を考慮する。

（１）違反の内容及び重大さ並びにその業務上の影響
（２）最初の違反か又は繰り返し起こされたものか
（３）違反者は、適切に教育、訓練されていたか

（４）関連する法令、規則又は取引契約内容についての確認
（５）その他、必要と判断される内容

４．４．３ 人事部門での罰則手続き

(A.7.2.3)

人事部門の担当者は情報セキュリティ委員会での決定に基づき、該当者に対する就業規則に従った罰則の決定及び適用に関する手続きの実施をしなければならない。

４．４．４ 再教育

(A.7.2.3)

情報セキュリティ委員会は罰則案件の審議結果で再教育が必要と決定した該当者に対して再教育を実施しなければならない。

５　運用確認事項

人的管理において、以下が行われていることを確認しなければならない。

（１）顧客情報の収集、保管、廃棄、クレーム等に関し、定期的に確認を行わなければならない。また、その状況を記録し保管しなければならない。
（２）教育実施後理解度を測り、理解度の低い者に対し、十分な理解が得られるように再教育等を実施しなければならない。
（３）関連法令、社内規程及び契約上の義務違反等を明確にし、それに対する被害状況等を確認する。その結果をもって、必要な対応策を検討し、実施可能な対応策を行わなければならない。実施が困難な場合は、残存リスクとして従業員が認識しなければならない。
（４）また、これらの事項については、必ず記録を残さなければならない。
（５）関連法規等ついては、定期的に見直し、最新の状態にし、従業員及び必要な契約相手等に知らしめなければならない。

６　除外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『４．４懲戒手続』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

外部委託先管理規程

1.0版

外部委託先管理規程

外部委託先管理規程

１　趣旨

本規程は、当社の業務を外部の業者に委託し、実施する場合の契約における問題および委託先を管理する上での問題を未然に防ぐことを目的とする。

２　対象者

委託を行うすべての従業員。

３　対象システム

委託業務で使用するすべてのもの。

４　遵守事項

４．１　委託先の選定に関する遵守事項

（１）　委託を行う者は、委託先として信頼できる業者を選ばなければならない。

・委託先の選定基準を作成し、その基準に従い委託先を選定すること、又委託先に周知すること。

・選定基準を定期的に見直すこと。

・選定先が基準に適合しているか定期的に見直しを行い不具合があれば是正処置を施すこと。

４．２　委託契約に関する遵守事項

(A.13.2.4、A.14.2.7、A.15.1.1)

（１）委託を行う者は、委託業務の仕様以外に、機密保持及び守秘義務、その他関連する以下の契約事項を盛り込まなければならない。

① 秘密保持契約又は守秘義務契約の内容

・保護される情報の定義（例えば、秘密情報）

・秘密を無期限に保持する場合も含めた、契約の有効期間

・契約終了時に要求する処置

・認可されていない情報開示を避けるための、署名者の責任及び行為

・情報、企業秘密及び知的財産の所有権、並びにこれらの秘密情報の保護との関連

・秘密情報の許可された利用範囲、及び情報を利用する署名者の権利

・秘密情報に関する行為の監査及び監視体制

・許可されていない開示又は秘密情報漏えいの、通知及び報告のプロセス

・契約終了時における情報の返却又は破棄に関する条件

・契約違反が発生した場合にとるべき処置

② 外部委託先による開発の内容

・外部委託した内容に関連する使用許諾に関する取り決め、コードの所有権及び知的財産権

・セキュリティに配慮した設計、コーディング及び試験の実施についての契約要求事項

・外部開発者への、承認済みの脅威モデルの提供

・成果物の質及び性格さに関する受け入れ試験

・セキュリティ及びプライバシーについて、容認可能な最低限のレベルを定めるためのセキュリティしきい（閾）値を用いていることを示す証拠の提出

・引渡しに当たって、悪意のある内容（意図的なもの及び意図しないもの）が含まれないよう十分な試験が実施されていることを示す証拠の提出

・既知の脆弱性がふくまれないよう、十分な試験が実施されていることを示す証拠の提出

・預託契約に関する取決め、例えば、ソースコードが利用できなくなった場合

・開発プロセス及び管理策を監査するための契約上の権利

・成果物の作成に用いたビルド環境の有効な文書化

・適用される法律の遵守及び管理の効率の検証については、組織が責任を負うこと

③ 供給者関係の内容

・組織が、自らの情報へのアクセスを許可する供給者の種類（例えば。ＩＴサービス、物流サービス、金融サービス、ＩＴ基盤の構成要素などの供給者）の特定及び文書化

・供給者関係を管理するための標準化されたプロセス及びライフサイクル

・様々な供給者に許可される情報へのアクセスの種類の定義、並びにそのアクセスの監視及び管理

・情報の種類及びアクセスの種類ごとの最低限の情報セキュリティ要求事項で、組織の事業上のニーズ及び要求事項並びに組織のリスクプロファイルに基づく供給者との個々の合意の基礎となるもの

・それぞれの供給者及びアクセスに関して確立した情報セキュリティ要求事項が順守されているか否かを監視するためのプロセスおよび手順、これには第三者のレビュー及び要求事項が順守されているか否かを監視うるためのプロセス及び手順、これには第三者おレビュー及び製品の妥当性確認も含まれる

・各当事者が提供うる情報又は情報処理の完全性お確実にするための、正確さ及び全さの管理

・組織の情報お保護するために供給者に適用する義務の種類
・供給者によるアクセスに伴うインシデント及び不測お事態への対処、これには、組織及び供給者の責任も含める
・各当事者が提供する情報又は情報処理お可用性を確実にするための、対応力に関する取決め、並びに必要な場合には、回復及び不測の事態に関する取決め
・調達に関する組織の要員を対象おした、適用あれる方針プロセス及び手順についての意識向上訓練
・供給者の要員とやり取りする組織お要員お対象とした、関与及び行動に関する適切な規則（これは、供給者の種類、並びに組織のシステム及び情報への供給者によるアクセスのレベルに基づく。）についての意識向上訓練
・情報セキュリティに関する要求事項及び管理策を、両当事者が署名する合意書の中に記載する条件
・情報、情報処理施設及び移動が必要なその他のものの移行の管理、並びにその移行期間全体にわたって情報セキュリティが維持されることの確実性

（２）委託を行う者は、委託業務の仕様以外に、品質管理に関する以下の契約事項を盛り込まなければならない。

① 委託業者は、スケジュールに従った作業を実施し、途中経過における進捗状況を明確にしなければならない。

委託業者は、品質管理のために実施する事項を明確にしなければならない。

（３）委託を行う者は、委託業務の仕様以外に、再委託に関する以下の契約事項を盛り込まなければならない。

① 委託業者が、再委託を行うためには、当社に事前の承認を得なければならない。

４．３　委託先の管理に関する遵守事項

（１）委託先の契約、基準、その他の契約事項等を定期的に見直しすること。
（２）契約事項が遵守されている事を定期的に監査すること。
（３）委託先が委託先の従業員に対し、必要な教育を行っているか定期的に監査すること。

４．４　委託先のクラウドサービスの利用に関する遵守事項

（１）クラウドサービスに要求するセキュリティレベル、サービスレベルを確認する。
（２）クラウドサービスのユーザインターフェイスの変更、機能変更・追加に注意し、認証などセキュリティ強化に繋がる変更は利用する。
（３）データセンターのロケーションにより適用される法律が違うことに注意する。

（4）公的な機関が提供するクラウド選定基準、ガイドライン等参照すること。

５　運用確認事項

５．１　委託先選定に関しての確認事項

（1）定期的に選定基準及び選定先の見直しが行われている事を確認する。

（2）定期的に監査が実施されているか確認すること。

（3）委託先管理に関する環境の変化が生じた時、関連業務が見直しされていることを確認すること。

５．２　委託先契約に関しての確認事項

（1）契約事項等か定期的に見直されているか確認すること。

５．３　委託先の管理に関しての確認事項

（1）基準及び契約事項等が定期的に見直されている事を確認する。

（2） 契約事項等が遵守されていることを定期的に確認する。

（3）従業員への教育が実施されているか確認する。

（4）情報セキュリティへの取組み及び委託先の情報セキュリティ対策状況を確認、すること。

（5）対外的な関連の為、書類は厳正に確認し適正に処理保管する事、又確認事項等での内容は書類で残し且つ相手先との確認のサインを残すこと。

５．４　委託先のクラウドサービスの利用に関しての確認事項

（1）定期的に監査を行い基準等が適切に運用されている事を確認する。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

文書管理規程

1.0版

文書管理規程

文書管理規程

１　趣旨

本規程は、情報セキュリティ文書である「情報セキュリティ基本方針」「情報セキュリティ方針」「情報セキュリティ対策規程」「情報セキュリティ対策手順書」及び「記録」に関する策定、改訂、評価、承認、保管、管理、配布、廃棄方法を定めたものであり、情報セキュリティ文書の適切な管理と運用を図ることを目的とする

２　対象者

情報セキュリティ委員会（以下、「委員会」とする）の構成メンバー及び情報システム担当者を対象とする。

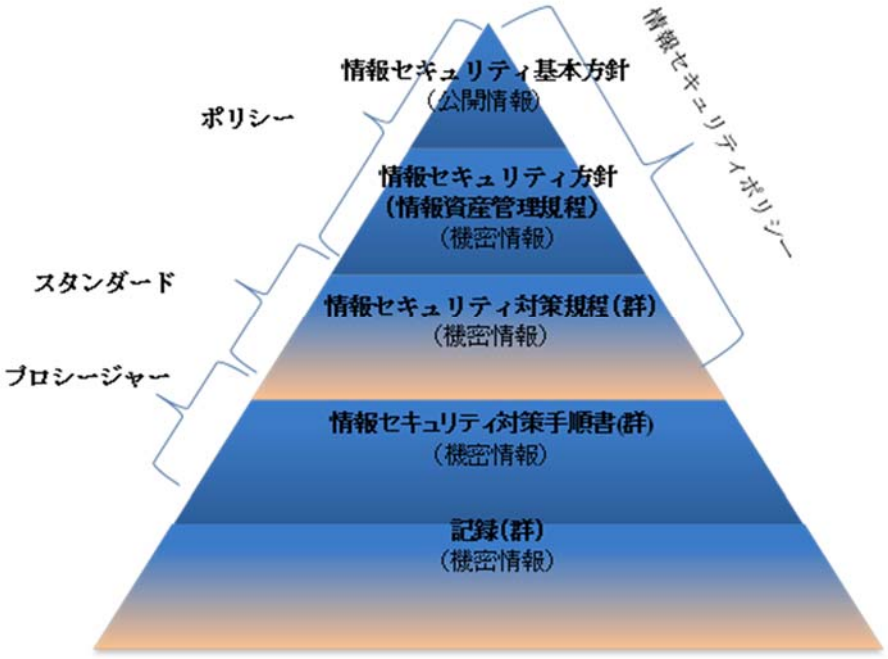
３　対象システム

本規程は情報セキュリティ文書に関するものであり、情報システムや情報機器を対象としない。

４　遵守事項

４．１ 情報セキュリティ文書の構成

情報セキュリティ文書（以下、「文書」とする）は、『情報セキュリティポリシー』と「情報セキュリティ対策手順書」及び「記録」から構成される。



４．１．１　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、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。

４．１．２　情報セキュリティ対策規程

情報セキュリティ対策規程（以下、「対策規程」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。

４．１．３　情報セキュリティ対策手順書

情報セキュリティ対策手順書（以下、「対策手順書」とする）は、「対策規程」の下層に位置する文書である。この文書は、「対策規程」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。

４．１．４　記録

記録は、情報セキュリティ対策の運用時の証拠を提供するために、作成する必要がある文書である。記録は、読みやすく、容易に識別可能で、検索可能にしておかなければならない。

４．２　文書の策定・改訂、評価、承認、保管・管理

「文書」の策定・改訂、評価、承認、保管・管理は下表のとおりとする。

	策定・改訂	評価	承認	保管・管理
方針	委員会	委員会	社長	事務局
対策規程	委員会	委員会	委員会	事務局
対策手順書	委員会が指定する情報システム担当者	委員会が指定する情報システム担当者	委員会	委員会が指定する情報システム担当者
監査記録、リスクアセスメント・対応・対策に関する記録	委員会が指定する情報システム担当者	委員会	社長	事務局
インシデント対応記録、是正措置記録	委員会が指定する情報システム担当者	委員会が指定する情報システム担当者	委員会	事務局
その他の記録	委員会が指定する情報システム担当者	―	―	委員会が指定する情報システム担当者

４．２．１　文書の策定・改訂の提案

委員会のメンバーは「文書」の策定・改訂の必要性を認識した場合、その「文書」の策定・改訂について提案することができる。

４．２．２　委員会での審議及び決定

委員会は提案された策定・改訂案件について審議を行い、策定・改訂を実施するかどうかを決定しなければならない。

４．２．３　策定・改訂結果の反映と記録

事務局及び情報システム担当者は実施することが決定した策定・改訂案件について「文書」の文言の変更を行うとともに、策定・改訂内容の記録を残さなければならない。

４．２．４　委員長に対する報告

委員会は実施することが決定した策定・改訂案件について委員長に報告しなければならない。

４．３　文書の配布

４．３．１　対象者への周知

委員会は、「文書」の策定・改訂を実施した場合、迅速に開示が許可された対象者へ周知しなければならない。

４．３．２　配布の手段

文書の配布については、以下を遵守しなければならない。

（１）委員会は、「文書」を社内 Web サーバ上で公開する。

（２）委員会は、Web サーバへのアクセスが、開示を許可された対象者のみが閲覧できるように正しく制御されるように、管理すること。

（３）委員会は、ネットワーク上の問題等によって「文書」の閲覧ができなくなることを避けるために、一定数の紙媒体による「文書」を保有していなければならない。

４．３．３　理解度の確認

配布文書を対象者が理解しているか確認するため、以下を遵守しなければならない。

（１）委員会は、Web ベースによる理解度チェック問題など、対象者の理解度を確認するための手段を用意しなければならない。

（２）対象者は、委員会からの周知を受けてから、速やかに「文書」の内容を確認し、理解しなければならない。

（３）対象者は、委員会が用意した理解度確認用の手段を、周知後１週間以内に実施しなければならない。

４．３．４　理解度実施の確認

配布文書を対象者が理解したか、以下により確認しなければならない。

（１）委員会は、対象者が理解度確認の手段をすべて実施し、必要な条件を満たすことにより、「文書」を受け取り正しく理解したとみなすことができる。

（２）部署のセキュリティ責任担当者は、各担当者の実施状況を Web の管理画面で確認することができる。セキュリティ責任担当者は、未実施者を識別し、未実施者に対して実施を促さなければならない。セキュリティ責任担当者は、やむを得ない理由で対象者の実施が困難な場合、速やかに委員会に報告しなければならない。

４．４　文書の廃棄

文書の廃棄にあたっては、以下を遵守しなければならない。

（１）「方針」の廃棄は、社長の承認を必要とする。「対策規程」及び「対策手順」の廃棄は、情報セキュリティ委員会の承認を必要とする。

（２）事務局及び情報システム担当者は、「文書」の廃棄の記録を残さなければならない。

５　運用確認事項

委員会は、本規程に基づき、運用の実施・記録の管理が確実に行われている事を定期的に確認しなければならない

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

監査規程

1.0版

監査規程

監査規程

１　趣旨

本規程は、マネジメントシステムの内部監査手続きが遵守事項に従って、有効且つ適正に行われることを目的とする。

２　対象者

当社の情報資産を扱うすべての人を対象とする。

なお、権限および責務は以下のグループによって区別される。

・情報セキュリティ委員会およびその構成メンバー

・情報セキュリティ委員会から任命された監査組織、およびその監査人

・被監査組織および被監査人

３　対象システム

本規程は監査に関するものであり、情報システムや情報機器を対象としない。

４　遵守事項

監査にあたっては、以下を遵守しなければならない。

４．１ 共通事項

（１）情報セキュリティ委員会は、監査組織を構成し、定期的に監査を実施しなければならない。監査の実施は定期的に年１回とする。監査の周期を変更する際には、情報セキュリティ委員会での承認を得なければならない。

（２）監査組織は、監査の対象、目的について、被監査組織（人）および被監査人と協議した上で合意しなければならない。監査組織は、合意した内容が監査の目的に合致しているかについて責任をもつ。

（３）監査組織は、合意された内容に基づいて監査を実施し、その結果を情報セキュリティ委員会へ報告しなければならない。情報セキュリティ委員会は、監査の結果を受けて、必要に応じて適切な是正措置を行わなければならない。

（４）監査組織は、被監査組織、および被監査人に対して独立していなければならない。もし独立した監査組織を構成できない場合には、相互監査体制をとりできる限り独立性を維持しなければならない。監査組織は、客観的に監査を行わなければならない。

（５）監査組織は、監査の実施にあたり専門の知識や技能を必要とする場合、専門家の協力を得ることができる。監査組織は、監査の目的について専門家に説明し、専門家による作業の結果について最終的な判断を下すことができなければならない。

（６）監査組織は、監査の過程において知りえた情報を、監査目的以外に公開してはならない。

（７）被監査組織および被監査人は、監査の円滑な実施のために、スケジュール調整、資料の提示、監査立会い等、監査組織の活動に協力しなければならない。

４．２　監査の計画

（１）監査組織は、合意された監査内容に基づいて、監査の計画を立てなければならない。監査組織は、監査の目的として以下を含めなければならない。

・内部統制が正しく規定されているか

・規定された内容にしたがって組織が効率的に実行しているか

（２）監査組織は、監査の計画にあたり以下の内容を検討または実施しなければならない。

・内部統制として実施されている活動内容

・資産およびそれらへのリスク分析

・情報セキュリティ方針や関連規程等の分析

・組織を取り巻く環境の変化

・内部統制を理解するためのヒアリングや観察

（３）監査組織は、監査項目に以下の内容を含めなければならない。

・セキュリティ方針および関連規程

・情報セキュリティ委員会の構成および実行

・情報資産を含む財産の管理

・社員、契約社員等の扱い

・物理的セキュリティ

・通信および運用

・アクセス制御

・システム開発

・事業継続計画

・法律、規制等への準拠

（４）監査組織は、計画した監査項目のそれぞれについて、問題点が内在する可能性について検討し、予測される内部統制リスクを判断した上で、実施手続きや監査のサンプリング密度を決定しなければならない。

（５）監査組織は、監査の実施手順および項目について、主要な内容を文書化しておかなければならない。

４．３　監査の実施

（１）監査組織は、各監査人に対して監査の実施を指示しなければならない。

（２）監査人は、あらかじめ決められた手続きに基づいて監査を実施しなければならない。監査手続きには必要に応じ、以下の内容を含めなければならない。

・インタビュー
・行動の観察
・証拠等の検閲
・監査人による作業手順の実施

（３）監査人は、組織内で提供されているサービスの可用性を考慮しなければならない。

（４）監査人は、システム監査ツールを使用するとき、システムへの影響に細心の注意を払わなければならない。監査時には、一般へのサービスは停止していることが望ましい。

（５）監査人は、情報セキュリティ方針と、実際のマネジメント活動を比較して、有効性についての判断をしなければならない。判断する観点としては以下を含めなければならない。

・組織の存在意義と情報セキュリティ方針との整合性
・情報セキュリティ方針と関連規程の整合性
・PDCA サイクルの適切な実施

（６）監査人は、監査結果を裏付けるために、監査によって得られた情報を記録しなければならない。

（７）監査人は、監査によって得られた情報を元に、内部統制リスクが予測範囲内であるかを評価し、実施手続きの妥当性を判断しなければならない。

（８）監査組織は、監査人からの報告を受けて、発見された問題の量や質が予測範囲を超えており、実施した手続きが妥当でないと判断した場合には、再度監査計画を立案して実行しなければならない。

４．４　監査結果の報告

（１）監査組織は、監査結果を元に監査報告書を作成し、情報セキュリティ委員会へ報告しなければならない。監査組織は、被監査人の不在、機密情報に関する閲覧

の拒絶など、さまざまな理由によって実施できなかった監査項目を監査報告書に含めなければならない。

（2）監査組織は、監査結果の裏付けとなる十分な根拠を提示できなければならない。

（3）監査組織は、問題点の指摘事項を報告する場合、問題点の重大性に応じて分類しなければならない。監査組織は、問題点を解決するための改善策について、可能な限り監査報告書に含めることが望ましい。

（4）監査報告書は、開示範囲を被監査組織、被監査人、情報セキュリティ委員会、および社長のみとしなければならない。

４．５　是正措置

（1）情報セキュリティ委員会は、監査組織からの報告を受けて、是正措置の計画立案をし、実行の判断をしなければならない。

（2）情報セキュリティ委員会は、実行可能となった是正措置について、緊急性、および重要性を考慮して、適切な時期に行なわなければならない。

（3）是正措置の指示を受けた被監査組織または被監査人は、速やかに是正措置を行い、実施した是正内容および時期を情報セキュリティ委員会に報告しなければならない。

５　運用確認事項

（1）監査組織は被監査組織、被監査人と監査の対象、目的について協議し、実施された監査結果を受けて、被監査組織、被監査人が必要に応じて適切な是正措置を行っているか確認すること。

（2）監査組織は被監査組織および被監査人に対して独立していること。

（3）監査組織は、合意された監査内容に基づき、予測される内部統制リスクを判断した上で実施手続きやサンプリング密度を決定し、監査人に定期的に年１回の監査の実施を指示していること。

（4）監査人は監査結果から内部統制リスクが予測範囲内であるかを評価し、実施手続きの妥当性を評価していること。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従わなければならない。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

物理的管理規程

1.0版

物理的管理規程

物理的管理規程

１　趣旨

本規程は、敷地・建物・室（サーバルーム等（以下、「サーバルーム」という））・機器・設備等を保護し、それらの損傷や利用の妨害、許可されていないアクセスを防止し、格納する情報の安全性を確保することを目的とする。

２　対象者

敷地・建物・室（サーバルーム等）の設置と利用、機器・設備等の利用に関わるすべての従業員。

３　対象システム

敷地内のすべての情報システム及びすべての機器。

４　遵守事項

４．１　物理的セキュリティ

４．１．１　セキュリティ区画の設定

（A.11.1、A.11.1.2、A.11.1.3、A.11.1.4）

対象物が必要なセキュリティ条件が異なる場合は、セキュリティ区画を明確化し、以下を遵守しなければならない。

（１）重要度の高い機器・設備を設置する場所にはその重要度に応じたセキュリティ区画が設定されなければならない。

（２）セキュリティ区画はその範囲を明確にしていなければならない。

（３）セキュリティ区画の管理については管理責任者を置かなければならない。

（４）セキュリティ区画には施錠設備を設けなければならない。

（５）セキュリティ区画は区画およびそこに設置する機器・設備等に関するセキュリティ上の各種のリスクを評価した上で必要な対策を実施しなければならない。リスクの要素には以下のものがある。

・盗難、破壊、地震、火災、水害等の水の事故、ほこり、振動、化学作用、電源事故、電磁波、静電気、小動物等の侵入等

４．１．２　セキュリティ区画の運用

（A.11.1.3）

セキュリティ区画の運用では、以下を遵守しなければならない。

（１）セキュリティ区画は従業員不在時には施錠しなければならない。

（２）セキュリティ区画への入場は、管理責任者の許可を受けて登録した特定のメン

バに制限しなければならない。

（３）セキュリティ区画への未登録者の入場については必ず入退場を記録し、登録メンバが同伴しなければならない。

（４）セキュリティ区画に入場する外部からの来訪者には区画内での注意事項を事前に説明しておかなければならない。

（５）セキュリティ区画に入場可能な登録メンバは定期的に見直さなければならない。

（６）セキュリティ区画に入場するものは身分証明となるカードあるいはバッジ等を常に明示しておかなければならない。また従業員は身分証明の明示がない入場者の相互確認を行わなければならない。

４．１．３　機器・設備の保護

(A.11.2.1)

機器、設備を保護するため、以下を遵守しなければならない。

（１）機器・設備の設置位置については、不正な操作が実施しにくく、不用意な操作ミス（間違いや見落とし）が起こりにくいように配慮しなければならない。

（２）重要度の高い機器・設備は他のものと分離して設置しなければならない。

（３）機器を設置する場合、落下や損傷の防止措置をとらなければならない。

（４）機器周辺では飲食・喫煙等を行ってはならない。

４．１．４　電源・空調の保護

(A.11.2.1、A.11.2.2、A.12.1.3)

電源、空調を保護するため、以下を遵守しなければならない。

（１）電源・空調室およびその設備には耐震、耐火、耐水などの防災対策を実施しなければならない。

（２）電源は、安定化装置の導入、負荷変動機器との配電隔離等によって電源容量と品質を確保しなければならない。

（３）電源は過電流・漏電等による機器への障害に対する保護措置をとらなければならない。

（４）電源には避雷設備を設置しなければならない。

（５）重要度の高い機器・設備に対する電源には、無停電装置、バックアップ電源等を設置しなければならない。

（６）空調設備は機器・設備を適切に運転するために十分な温度・湿度の調整能力を確保しなければならない。

（７）重要度の高い機器・設備に対する空調設備については予備装置を確保しなければならない。

４．１．５　ケーブルの保護

(A.11.2.3)

ケーブルを保護するため、以下を遵守しなければならない。

（１）ケーブルは、損傷（小動物対策を含む）や回線の盗聴を避けるため、保護用の電線管・カバーの使用や、敷設経路に対する配慮などの対策を行わなければならない。

（２）干渉防止のため、電源ケーブルと通信ケーブルは分離しなければならない。

（３）重要度の高いケーブルについては代替経路を準備しなければならない。

（４）ケーブルおよび端子については、未認可の機器・設備の接続や設置に対する監視または定期的チェックを行わなければならない。

４．２　サーバルームのセキュリティ

４．２．１　サーバルームの定義

サーバルームを以下と定義する。

（１）サーバルームは「重要度の高い情報資産が格納されているサーバがまとめて設置される部屋」とする。重要度の高い情報資産については別途定める。

（２）電子化されたデータとして保存する重要度の高い情報資産は、『システム利用規程』および『システム管理規程』に基づいて管理される場合を除き、サーバルームに設置するサーバでのみ保存されなければならない。

４．２．２　サーバルームの物理的セキュリティ

(A.11.1.3、A.11.1.4)

サーバルームを保護するため、以下を遵守しなければならない。

（１）サーバルームは独立した部屋として設置し、一般オフィスとの共用や他社オフィスとの隣接は避けなければならない。

（２）サーバルームは、危険物保管場所、火気施設、水道設備等、災害のリスクの大きい場所からは遠ざけて設置しなければならない。

（３）サーバルームの外観は目立ちにくいものとし、室名表示等も最小限にとどめなければならない。

（４）サーバルームの出入り口は原則 1 ヶ所に限定し、施錠設備を設けなければならない。

（５）サーバルームに窓を設けることは極力避け、設ける場合は網付きガラス・強化ガラス等を用いなければならない。

（６）サーバルームには設置する機器・設備の重要度に応じて、防犯カメラ、侵入報知機等の防犯設備の設置を検討しなければならない。

（７）サーバルームには必要に応じて、非常電話、非常ベル等の非常用連絡設備の設

置を検討しなければならない。

（８）サーバルームにはコピー・FAX 等、情報の複写や送信のための設備を設置してはならない。

４．２．３　サーバルームの運用

(A.11.1.2、A.11.1.5)

サーバルームの運用では、以下を遵守しなければならない。

（１）サーバルームは従業員不在時には施錠しなければならない。

（２）サーバルームおよびその鍵の管理については管理責任者を置かなければならない。

（３）サーバルームへの入室は、受付または認証装置（入館カード、パスワード入力、生体認証）等によって特定の登録メンバに制限されなければならない。

（４）サーバルームへの未登録者の入室および作業実施については管理責任者の許可と登録メンバの同伴がなければならない。

（５）サーバルームに入室可能な登録メンバは定期的に見直さなければならない。

（６）サーバルームに入室不要となった登録メンバは速やかに登録を解除し、入室のための認証を無効にしなければならない。

（７）サーバルームへの入退室は記録しなければならない。

（８）サーバルーム内で長時間作業を行う場合は一人では実施せず、必ず同伴者を伴わなければならない。

（９）サーバルーム内で管理責任者の許可なく撮影・録音を行ってはならない。

（１０）サーバルームには作業に必要のないもの（許可されていないパソコン、カメラ、携帯電話、スマートデバイス等）を持ち込みし置いてはならない。もし置いてあった場合は速やかに撤去しなければならない。

（１１）サーバルーム内の環境（機器・設備の有無、配置、利用状況等）は定期的に点検しなければならない。

４．３　職場環境におけるセキュリティ

４．３．１　書類・媒体等の取扱いと保管（クリアデスクポリシー）

(A.11.2.9)

書類、媒体等を取扱い、保管においては、以下を遵守しなければならない。

（１）従業員は使用していない書類や媒体をキャビネット等へ収納し、机上等に放置してはならない。

（２）従業員は重要度の高い書類や媒体を施錠保管し、特に必要な場合は耐火金庫・耐熱金庫に保管しなければならない。

４．３．２　画面に表示する情報の管理（クリアスクリーンポリシー）

(A.11.2.9)

離席時におけるパソコンについて、以下を遵守しなければならない。

（１）従業員は不正な操作や盗み見を防止するため、離席時にはログオフするか、画面・キーボードロック等の保護機能を使用しなければならない。

４．３．３　事務・通信機器の取扱い

(A.11.2.9、 A.12.1.1)

ホワイトボードやコピー機、FAX、プリンタなどの取扱いについて、以下を遵守しなければならない。

（１）従業員はホワイトボード等への書き込み内容を使用後に必ず消去し、放置してはならない。

（２）従業員はコピー機、FAX、プリンタ等の入出力書類を放置してはならない。特に重要度の高い書類は印刷および送受信の間、従業員が常に機器に（FAX の場合は送受信の両側とも）立ち会うようにしなくてはならない。

（３）従業員は FAX 送信時には必ず宛先を確認し、誤送信を防止しなければならない。

４．３．４　搬入物の受渡し

(A.11.1.6)

物の搬入にあたっては、以下を遵守しなければならない。

（１）搬入物の受渡しについては受渡し場所を設置し、サーバルームおよびセキュリティ区画とは分離しなければならない。

（２）受渡し場所への従業員以外のスタッフによるアクセスは、必ず従業員の監視付きで行い、アクセスを記録しなければならない。

（３）搬入物の受入れを行う従業員は受入れの際に危険物持込や情報漏洩等のリスクがないかどうか点検しなければならない。

（４）搬入物が登録の必要な情報資産である場合、搬入物の受入れを行う従業員は受入れ後速やかに登録作業を行わなければならない。

（５）郵便物の受入れ場所には盗み見や抜き取りを防止する対策を行わなければならない。

４．３．５　盗み聞きによる情報漏えい防止

(A.7.2.2)

盗み聞きに対応するため、以下を遵守しなければならない。

（１）従業員は電話や立ち話、オープンな会議スペースでの発言について、盗み聞きを防止するよう配慮しなければならない。

５　運用確認事項

物理的管理において、以下が行われていることを確認しなければならない。

（1）本規程に基づき、記録・運用が管理されている事を定期的に確認すること。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

リスク管理規程

1.0版

リスク管理規程

リスク管理規程

１　趣旨

本規程は、当社を取り巻く状況から派生する課題と、当社の経営課題並びに顧客等利害関係者からの要求事項を考慮し、情報セキュリティに関わる、リスクを防止又は低減する過程を定めることを目的とする。

２　対象者

当社の情報セキュリティ委員会。

３　対象システム

当社が保有するすべての情報資産を対象とする。

４　遵守事項

４．１ リスクアセスメント

当社を取り巻く状況から派生する課題と、経営課題並びに顧客等利害関係者からの要求事項が何なのか、またどこにどのような情報資産が存在し、どのような方法で管理されているかを洗い出す。洗い出された情報資産を機密性、完全性、可用性の観点から重要度の評価を行う。評価の結果、重要と判断された情報資産に対しての脅威や脆弱性は、どのようなものがあるかを洗い出して記述する。

情報資産の評価、洗い出された脅威、脆弱性により、情報資産に関わるリスクを算定する。

リスクアセスメントの過程は、検討された事項や除外の理由などを記録しておく。

４．１．１　組織の状況の確定

当社を取り巻く外部及び内部状況を洗い出す。外部状況としては、法律・規制・技術・自然環境、情報セキュリティ事件・事故の傾向、利害関係者の情報セキュリティに関する要求事項等があり、内部状況としては、経営方針・目標・課題・戦略、組織体制、社会的責任、企業文化、情報システムに関わるプロセス等がある。

洗い出した状況より、当社の情報セキュリティに影響を与える課題を確定する。

４．１．２　情報資産の洗い出しと重要度分析

当社の情報資産が業務の流れの中で、どこにどのような形でどのように利用、保管、管理されているかを洗い出す。情報資産は、関連会社や取引先などにも利用されている場合が多く、情報資産を取り扱う従業員に協力を得て存在を確認する。洗い出された情報資産は、情報資産管理者（情報やデータの持ち主で存在及び利用の責任者）とともに

機密性、完全性、可用性、また流出時の影響度などを考慮し重要度を付け、情報資産台帳に記録する

４．１．３　脅威の洗い出し

脅威の洗い出しにおいては、以下を遵守しなければならない。

（１）重要度付けの結果、重要と判断された情報資産に関する脅威を、従業員の協力・参画の元、情報資産の保存形態、利用形態を考慮して洗い出し、記録する。

（２）脅威の洗い出しにおいて、過去に発生したヒヤリ・ハット、事件・事故、業務遂行上の問題点を考慮して洗い出す。

４．１．４　脆弱性の洗い出し

対象となる情報資産を、保存形態、利用形態を考慮してその脆弱性を洗い出し記録する。

４．１．５　リスクの分析

（１）洗い出された脅威と脆弱性に対し、どのような時にどのような状況でどのような原因でどのようにリスクが発生するのか、発生した場合にどのような影響があるのかを分析する。

（２）分析の際に使用した状況・原因・影響について記録し、除外した部分や除外した理由について記録する。

４．１．６　リスクの特定

（１）分析されたリスクについて、当社に関係すると思われるリスクを特定する。

（２）特定したリスクについて、特定の理由と状況・原因・影響を記録する。

（３）特定に至らなかったリスクについては、至らなかった理由を記録する。

４．１．７　リスクの算定

（１）特定されたリスクに対し、起こり易さと、そのリスクが発生した場合に当社が被る損害（金額・範囲・関係する利害関係者等）について具体的な数値を示して算定を行う。

（２）算定の際に使用した条件・数値等を記録する。

４．２　リスクの対応

（１）アセスメントで洗い出し・分析・特定・算定されたリスクに対して、受容レベルを決定し記録する。

（２）受容レベルを超えるリスクに関してリスク対応の種類より対応を決定し記録す

る。

（3）決定の際に使用された判断材料について記録する。

４．２．１　リスク対応の種類

リスク対応は、以下からひとつ、または複数の組み合わせを選択する。

（1）リスクの回避

リスクを発生させる活動や行動を、開始しない、または継続しないと決定することにより、リスクを回避すること。

（2）リスクテイク

ある機会を追求するために，そのリスクを取る又は増加させること。

例えばビジネスの機会を追求または増加するためにリスクを取るまたはリスクを増加させること。利益を追求するために市場の拡大などを目ざす場合に、積極的にリスクを取ること。

（3）リスク源の除去

リスク源を取り除く。リスクの原因となっている脅威又は脆弱性を排除・除去すること。

（4）起こりやすさの変更

リスクの起こりやすさを変えること。リスクが発生する確率は同じではなく、少なくなる、または多くなる場所・要因・時間帯など様々な要素があり、これらを考慮してリスクの起こりやすさを変えること。

（5）結果の変更

事前の策により結果を変えること。万が一リスクが発生した場合に、損失をできるだけ小さくなるよう結果を変えること。

（6）リスクの共有

一つまたは複数の他者とリスクを共有すること。万が一リスクが発生した場合に保険などで被害に対する損害賠償などの減額を行うこと。

（7）リスクの保有

十分な情報に基づいた選択と経営者の判断によりリスクを保有する（受け入れる）こと。

４．３　管理策の決定

リスク対応の結果から受容レベル以下になるよう、具体的なセキュリティ管理策を決定し、経営者の承認を得て記録し、対策の流れを記載したリスク対応手順書を作成し関係者への周知・徹底を行う。

５　運用確認事項

リスク管理において、以下が行われていることを確認しなければならない。

（1）本規程に基づき、運用の実施・記録の管理が確実に行われ、管理されている事を定期的に確認する。

（2）情報セキュリティ委員会は、マネジメントサイクルが適切に運用されていることを最低年一回以上は確認し、問題があれば適切な助言や改善策を実施する。

（3）情報セキュリティ委員会は、最低年一回以上、従業員及び経営陣にリスクマネジメントに関する問題についてのアンケート調査を実施する。

（4）新しい脅威の情報を取得した場合は、リスクアセスメントとリスクマネジメントを実施し、新たなリスク対応や管理策がとられ、それらの管理策が周知徹底できているかを確認する。また、その管理策の効果を評価し、必要に応じ管理策の見直しを行う。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

セキュリティインシデント報告・対応規程

1.0版

セキュリティインシデント報告・対応規程

セキュリティインシデント報告・対応規程

１　趣旨

本規程は、セキュリティインシデントが発生した場合及びセキュリティインシデントの発生と疑われる場合、適切な連絡経路を通じて極力速やかに報告し、定められた手順に従って迅速に対応し、情報システム環境の復旧が速やかになされることと、発生した事態から問題点や改善点などに対する学習を行い、継続的な再発防止が行われることを目的とする。

当社におけるセキュリティインシデントとは次のような事態を指す。

（１）セキュリティに対する侵害

例　不正アクセスによる情報漏えい、従業員による情報漏えい、ウイルス・マルウエア感染、DoS 攻撃、記録媒体等の紛失　等

（２）システム・ネットワークの故障・損壊

例　電源異常、熱暴走、天災による機器損壊　等

（３）情報資産への脅威

例　建物への侵入　　等

２　対象者

当社のすべての従業員。

３　対象システム

当社の従業員が業務遂行のため利用するすべてのシステム。

４　遵守事項

経営者の同意・承認の元、未然に防げなかった事態が発生した際に、事態の可及的速やかな収拾と被害や影響範囲を最小にするために、平時からの取組と組織・役割の責任の明確化・伝達方法・事態の評価と対応及び再発防止を含む学習についての取り組みを明確にする。

４．１　平時の準備

(A.16.1.1)

セキュリティインシデントが発生した場合、あるいは発生が疑われる場合は情報セキュリティ委員会に遅滞なく報告がなされ、速やかにセキュリティインシデントの分析、封じ込め、原因の根絶、復旧が可能となるよう、４．２項以降に示す対応について以下の準備作業を行い、関係者に周知・徹底する。

（１）情報セキュリティ委員会は、想定するセキュリティインシデントの具体的な対

応手順を策定する。対応手順には，次の事項を含む。

- 緊急時対応の対応組織の始動、及び終了に関する契機
- 緊急時対応の対応組織の役割、責任の明確化

なお、緊急対応の実行責任者は，緊急時対策に関するすべての判断の権限及び責任をもつものとする。

- 組織の内部及び外部機関との協力関係の明記
- 組織の内外への必要な連絡先の明記

（2）情報セキュリティ委員会は、策定した対応手順でセキュリティインシデントに対応可能となるよう、定期的に訓練を行い、併せて対応手順に問題がないか確認を行い、対応手順に問題があれば是正する。

（3）情報セキュリティ委員会は、セキュリティインシデントの検知に必要な情報セキュリティ対策の導入に向け、情報セキュリティマネジメントを遂行しなければならない。

（4）情報セキュリティ委員会は、各システムの復旧優先度を決定しなければならない。復旧優先度の決定は、対象システムにおいて運用される業務の停止許容時間を観点において行う。(表１参照)

表１

復旧優先度	業務復旧までの許容時間
3	業務が停止することは許されない
2	24時間以内に復旧しなければならない
1	3日以内に復旧しなければならない
0	インシデント発生時は停止してもよい

４．２　事象の検知、報告と分析

(A.16.1.2)

セキュリティインシデント、あるいは発生が疑われる事象を検知したものは、情報セキュリティ委員会に遅滞なく報告しなければならない。

情報セキュリティ委員会は、報告されたセキュリティインシデントに応じ、策定した対応手順に従い、被害の特定、原因の分析を行う。

なお、策定した対応手順に該当しないセキュリティインシデントの場合、情報セキュリティ委員会は、そのための実行責任者を任命し、対応組織を始動し、被害の特定、原因の分析を行う。

検知したセキュリティインシデント情報、原因の分析状況について、実行責任者のもと、一元的に収集、管理する。

４．３　封じ込め、根絶、復旧

(A.16.1.5)

特定したセキュリティインシデントの原因に基づく対応手順に則り、被害の拡散を防止し、被害箇所の原因の根絶、修復を行い、復旧をする。

なお、セキュリティインシデントに関する情報は、実行責任者のもと、一元的に収集、管理する。以下の情報を管理、記録する。

・セキュリティインシデントの発生状況及び対応状況に関する情報
・自社のビジネス活動再開に関する情報
・顧客及び取引先等利害関係者の影響等に関する情報

４．４　インシデントからの学習

(A.16.1.6)

セキュリティインシデントの対応後、同様のセキュリティインシデントの再発防止、および対応手順の不備等について改善を行う。

（１）セキュリティインシデントへの対応が完了した後、情報セキュリティ委員会および情報システム部は、調査結果をもとに再発防止計画を作成しなければならない。再発防止計画作成時には、技術的側面と組織的側面の両方に留意する。

（２）情報セキュリティ委員会は発生したインシデントのうち、以下の要件を満たすものについては、再発防止計画と共に取締役会に報告しなければならない。

・社外の第三者からのセキュリティ侵害により当社が被害者となる場合
・顧客や取引先等の社外に対して当社が加害者となる場合

（３）再発防止計画は、すべての従業員に周知され、適切に実施されなければならない。

（４）情報セキュリティ委員会は、セキュリティインシデントの発生から再発防止計画作成までの一連の管理した記録から、対応手順の不備、または良かった点を整理し、対応手順を改善しなければならない。また、一連の記録を保管、管理しなければならない。

５　運用確認事項

インシデント発生時における対応方法について、あらかじめ報告及び復旧等に向けた手順を作成しているか確認する。また、インシデント対応実施後に再発防止策、対応手順の改善が行われているか、確認する。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

システム変更管理規程

1.0版

システム変更管理規程

システム変更管理規程

１　趣旨

本規程は、当社のシステム（アプリケーション、インフラ）の変更管理に関する事項を定めることにより、確実で適正なシステム変更が行われること及び変更に失敗した際のリカバリーを迅速に行うことを目的とする。

２　対象者

システムの変更（開発、保守運用）に従事するすべての従業員。

３　対象システム

当社業務で使用するすべてのシステム。

４　遵守事項

４．１　システム変更プロセスに関する遵守事項

(A.14.2.2)

（１）システム変更は予め定められたプロセスに従って行わなければならない。

・システム変更要求は、対象システムの認可された利用者によって行われなければならない。

・システム変更作業の開始前に、作業内容の提案について正式な承認を変更管理マネジャーから得なければならない。

・システム変更作業の実施前に、認可された利用者がその変更を受け入れることを担保しなければならない。

・システム変更作業の実施後、認可された利用者はその変更が要求に即したものであることを確認しなければならない。

・全ての変更要求および変更作業に関する要求から承認、確認の一連のプロセスについて、監査証跡を維持及び管理しなければならない。

４．２　システム変更作業に関する遵守事項

(A.14.2.2)

（１）システム変更作業は以下の項目を遵守して行われなければならない。

・変更によって変更管理体制及び完全性に関する手順が損なわれないことを担保するため、変更管理体制及び手順を変更作業の承認者に対してレビューしなければならない。

・作業者は、変更に際し修正が必要となる全てのソフトウェア、情報（データベースを含む)、権限、ハードウェア（サーバ及びネットワークや、それらの

設定を含む）を特定しなければならない。

・システムの脆弱性を最小限とするために、特にセキュリティを重視すべき箇所を特定し、変更後における脆弱性の有無及び影響度を評価しなければならない。

・システムの変更により、現在実現している信頼性、可用性が低下しないよう設計しなければならない。

・システム変更作業は関係する業務を妨げないことを原則とし、これを確保できる日時に実施する。ただし、緊急を要する変更及び業務の調整が可能である場合はこの通りではない。

・システム変更作業が失敗した際に、作業開始前の状態にロールバックする手順をレビューし、変更管理マネジャーに承認されなければならない。

（２）システム変更作業に際し、システムに関連する文書は以下の通り管理されなければならない。

・システムに関する一式の文書は、変更の完了時点で更新され、また古い文書は記録・保管しなければならない。

・アプリケーションの更新については、版数の管理を維持しなければならない。

・システム操作手順書等の運用文書類及び利用者の手順は、システム変更の際に必要に応じて変更されなければならない。また、変更後の手順は、文書化し保管しなければならない。

５　運用確認事項

アプリケーションの変更作業の際に、無関係なファイルが変更されたかどうかを確認するため、ファイル単位での更新履歴管理が必要である。

管理方法として、ファイルの更新日付やメッセージダイジェスト、差分出力等の結果を実施前後で比較する等の方法がある。

６　例外事項

業務都合等業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

システム開発規程

1.0版

システム開発規程

システム開発規程

１　趣旨

本規程は、情報システムの開発（企画、設計、開発、導入）及び更新に際し、情報セキュリティの維持・向上を図るため、必要な事項を定めるものとする。

２　対象者

当社の従業員及び協力会社社員で情報システムの企画、設計、開発及び導入に関わる全ての者。

３　対象システム

社内で利用される全ての情報システム。開発を伴わないパッケージシステムの導入も対象とする。

４　遵守事項

４．１ 企画・設計

４．１．１　企画の申請・承認

(A.14.2.1)

システム開発の企画にあたっては、以下を遵守しなければならない。

（１）新規システムの開発又は既存システムの変更を企画する者は、設計・開発に先立ち、情報セキュリティ委員会に申し出て、関連する各種規定について、提示・説明を受ける。

（２）情報システム主管部門は、提示された規定に従い、新規システム開発又は既存システム変更が可能であることを情報セキュリティ委員会に報告し、開発の承認を受ける。

（３）情報セキュリティ委員会は、システム開発及び運用開始後に必要となる各種規程類を提示し、この範囲の中で適切なシステムが開発されることを求める。また、開発プロジェクト遂行においても順守されるべき規定を提示する。

４．１．２　要件定義

(A.14.2.1)

システム開発の要件定義フェーズにおいては、以下を遵守しなければならない。

（１）システムの企画、設計を行う場合、セキュリティ設計を担当する者を、システム機能設計を担当する者とは別に置く。

（２）セキュリティ設計を担当する者は、セキュリティ要件を明確にする。

（３）セキュリティ設計担当者は、セキュリティ要件に従い、設計フェーズで実施す

る開発システムに関するリスクアセスメントの実施要項を明確にし、情報セキュリティ委員会に報告する。

（４）要件定義が完了した段階で、セキュリティ設計担当者は情報システム主管部門とともに、プロジェクト遂行の為のリスクアセスメントを実施し、抽出した対応すべきリスクへの対策の取組み状況について情報セキュリティ委員会に報告する。

４．１．３　設計

(A.14.2.1)

システム開発の設計フェーズにおいては、以下を遵守しなければならない。

（１）セキュリティ設計を担当する者は、企画書及び設計書等はドキュメントとして残す。

（２）セキュリティ設計担当者は、設計書を元に、情報システム主管部門とともにリスクアセスメントを実施し、抽出した対応すべきリスクへの対策の取組み状況について情報セキュリティ委員会に報告する。

４．２　開発・導入

４．２．１　開発環境

(A.14.2.6)

システム開発環境は、以下を遵守しなければならない。

（１）開発環境と本番環境は切り分ける。但し、開発作業による本番環境への影響が少ない場合は、この限りではない。

（２）本番環境を開発に用いる場合は、開発用に追加・変更した要件を明らかにし、本番開始後は適切な対処を行う。

（３）本番環境を開発に用いる場合、開発用に追加・変更される一般的な内容は、以下の通りである。

・開発用アカウントの追加
・管理者権限を持つアカウントのパスワードの変更
・テストデータの追加
・開発環境用のログデータ取得設定およびログデータ

４．２．２　本番データの使用

(A.14.3.1)

システム開発における本番データの取扱いは、以下を遵守しなければならない。

（１）システム開発又はテストにおいて本番データを使用する際は、事前に情報管理責任者の承認を受ける。

（2）システム開発又はテストにおいて使用する本番データは、厳密に保管・管理し、使用後の結果データ等は、直ちに復元不可能な措置を講じた上で破棄処分する。

４．２．３　システム開発の委託

システム開発を委託する場合は、以下を遵守しなければならない。

（1）システム開発を外部事業者に委託する場合、『外部委託先管理規程』に従う。

４．２．４　製品の調達

製品を調達する場合は、以下を遵守しなければならない。

（1）調達する製品は、次にあげる事項を満たすものとする。

・当該製品がセキュリティ要件を満たす機能を備えていること

・購入先又は開発元の事業者の連絡先が明らかなものであること

・該当製品に関する更新情報の提供が受けられること

４．２．５　導入

(A.14.2.8、A.14.2.9)

開発システムの導入にあたっては、以下を遵守しなければならない。

（1）システム開発の終了時又は外部委託先からの情報システム受け入れ時の情報セキュリティ上の検査項目を明確にする。

（2）本番環境へ移行する際は、リスクアセスメントにより抽出した対応すべきリスクへの対策の取組み状況について、不備・欠陥等の問題がないか確認する。

（3）導入する情報システムが、既に稼働中の情報システムと連携する場合は、不具合等が発生しないか十分に確認する。

４．３　仕様書等の取扱い

４．３．１　仕様書等の管理

開発仕様書等の取扱いは、以下を遵守しなければならない。

（1）システム管理者およびネットワーク管理者は、システム設計及び開発等に係る仕様書等を、情報システム毎に整理するとともに、システム管理者以外が取り扱えないように厳重に保管・管理する。

（2）システム管理者及びネットワーク管理者は、情報システムの変更の都度、仕様書に反映させ、常に最新の状態で管理する。

５　運用確認事項

システム開発において、以下が行われていることを確認しなければならない。

（1）セキュリティ設計担当者が、フェーズ毎に情報セキュリティ委員会に、リスクア

セスメントで抽出した対応すべきリスクへの対策の取組み状況について報告していることを確認する。

（2）システム管理者及びネットワーク管理者は、情報システムの変更の都度、情報セキュリティ委員会にリスクアセスメント結果を報告していることを確認する。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

システム管理規程

1.0版

システム管理規程

システム管理規程

１　趣旨

本規程は、サーバ、PC 及びスマートデバイス上の機密性・完全性・可用性を確保し、発生し得る各種問題を未然に防ぐことを目的とする。

２　対象者

（１）システム管理者

※システム管理者はサーバ管理者、ネットワーク管理者、クライアント端末管理者を指す。

（２）オペレータ

（３）システム設計者

（４）情報システム部

（５）情報セキュリティ委員会

３　対象システム

（１）本社、営業所、ホスティング、ハウジングを含む、全ての物理サーバシステム及び仮想サーバシステム。

（２）当社より支給・貸与した PC。

※本規程内では、「PC」はノートパソコンを含んだ PC 端末のことを指す。

（３）当社より支給・貸与したスマートデバイス。

※本規程内では、「スマートデバイス」はスマートフォン及びタブレット端末を指す。

４　遵守事項

４．１ アカウントの管理

４．１．１　アカウントの作成

(A.9.1.1、A.9.2.1、A.9.2.2、A.9.2.4、A.9.4.1)

（１）正式な社内プロセスにより、利用部門からシステム、アプリケーション、情報へアクセスするための新規アカウントの申請があった場合、システム管理者は、申請を受けたアカウントを利用者ごとに作成し、アカウントには業務に必要最小限のアクセス権限を設定すること。

（２）システム管理者は、作成したアカウントを『アカウント管理台帳』に記録すること。

（３）システム管理者は、アカウントに設定した初期パスワードは、推測しにくいものを設定し、セキュリティを確保し利用者へ確実に伝達すること。

４．１．２　アカウントの変更

(A.9.2.1、A.9.2.2、A.9.2.5)

（１）正式な社内プロセスにより、利用部門からアカウント変更の申請があった場合、システム管理者は、申請に従いアカウントの変更を行うこと。

（２）システム管理者は、定期的(例えば 1 年に１度)に利用部門の管理職にアカウント権限の見直しを依頼し、権限の変更が必要な場合、アカウント権限を変更すること。

（３）システム管理者は、『アカウント管理台帳』にアカウント変更内容を記録すること。

４．１．３　不要となったアカウントの削除

(A.9.2.1、A.9.2.2、A.9.2.6)

（１）正式な社内プロセスにより、利用部門からアカウント削除の申請があった場合、システム管理者は、申請に従いアカウントを停止・無効化すること。

（２）システム管理者は、定期的(例えば 1 年に 1 度)に利用部門の管理職にアカウントの棚卸しを依頼し、不要なアカウントは停止・無効化すること。

（３）システム管理者は、アカウント管理システムのアクセスログを確認し、一定期間(例えば３ヶ月間)使用されていないアカウントを停止・無効化すること。

（４）システム管理者は、『アカウント管理台帳』にアカウントの停止・無効化を記録すること。

４．１．４　特権アカウントの管理

(A.9.2.3、A.9.4.4)

（１）システム及びアプリケーションを制御するためのシステムユーティリティプログラムの使用はシステム管理者に制限する。

４．１．５　アカウント管理システム

(A.9.4.2、A.9.4.3)

（１）システム管理者は、パスワード管理システムのパスワードポリシーを次のように設定すること。

①パスワード長及び質(例：８文字以上、大文字、小文字、特殊文字の組み合わせ)を設定する。

②定期的(例：３カ月ごと)にパスワードを変更するように設定する。

③過去(例：過去１０回以内)に使用したパスワードの再使用を防止する。

④最初のログオン時に、利用者がパスワードを変更するように設定する。

⑤特に、重要なシステム、データへのアクセスが必要なアカウントには、パスワードに加え、二段階、二要素認証を実装する。

⑥認証に複数回(例：１０回)続けて失敗した場合、アカウントを使用停止にする。

４．１．６　パスワードを忘れた場合の処置

(A.9.2.2、A.9.2.4)

（１）パスワード再発行の申請を受けたシステム管理者は、速やかに新規のパスワードを発行して、利用者に通知すること。

（２）システム管理者は、申請してきた利用者が本人自身であることを何らかの方法（例えば電話返信）で確認すること。

４．２ サーバ管理

４．２．１　設計時の規定

(A.14.2.5、A.17.2.1)

（１）システム設計者は、サーバの設置の目的と当該サーバに保存する情報を明確にすること。また保存する情報に「顧客情報、プライバシー情報」などを含む場合は、『人的管理規程』を遵守すること。

（２）システム設計者は、サーバのセキュリティ設計を行う上で、必ずリスク分析を行うこと。リスク分析を行う上で、以下の項目を明確にすること。

①保護・脅威の対象（守るべき情報）

② 脅威

③ 脅威の原因、プロセス

④ 対策（予防、防御、検査、対応：回復）

（３）システム設計者は、OS のアクセス制御とアプリケーションとサービスのアクセス制御に関して、設計書を作成し、厳密にアクセス権を設定すること。この設計書は、変更履歴を含めて保管管理すること。

（４）システム設計者は、データのアクセス制御に関して、設計書を作成し、厳密にアクセス権を設定すること。これらのデータには、OS のシステムファイルやアプリケーション、アプリケーション設定ファイルなども含むこと。これらの設計書は、変更履歴を含めて保管管理すること。

（５）システム設計者は、CGI、API などのアプリケーション開発を行う際、リスク分析を実施し、仕様書の段階から、データの入力チェックなどの、セキュリティ対策の実施を行うこと。

（６）外部公開サーバに関して、情報セキュリティ委員会は、推奨プラットホームを規定すること。システム設計者は外部公開サーバのプラットホームについては、

情報セキュリティ委員会が規定する推奨プラットホームを採用すること。

（7）『リスクマネジメント規程』に従い、システム設計者がリスクアセスメントを実施した結果、サーバの高可用性が要求される場合、アセスメント結果に応じて、以下を考慮して冗長化を検討すること。

①仮想化技術を使用した冗長化

②アクティブ-アクティブ、アクティブ-スタンバイ構成による冗長化

③RAID(1、5、6)による冗長化

④データバックアップとコールドスタンバイによる冗長化

４．２．２　導入時の規定

(A.11.2.1、A.11.2.2、A.11.2.4、A.12.1.1)

（１）サーバ管理者は、サーバの設置場所をサーバルームまたは、それに準ずるセキュリティを確保でき、かつサポートユーティリティ(電気、通信サービス、空調、換気、給水等)を備えた場所にすること。

（２）サーバ管理者は、サーバを設置する場合、サーバ設置申請書を作成し、情報セキュリティ委員会で認可を受けること。

（３）サーバ管理者は、サーバの設置申請時にそのシステム構成を明確にすること。情報セキュリティ委員会により、システム構成の不備もしくは、改善要求を受けた場合、サーバ管理者は、直ちにシステム構成の再検討を行うこと。

（４）サーバ管理者は、情報及び情報システムの正しく安全な運用を確実にするため、管理体制及びサーバ管理者を明確にすること。人的不注意および故意の誤用のリスクを低減するため、サーバ管理者及びオペレータを２名以上任命すること。

（５）サーバ管理者は、サーバの設置申請時に運用手順書を作成し、情報セキュリティ委員会へ提出すること。また、運用手順書には侵害時対応手順を含むこと。

（６）システムセキュリティ責任者は、本規定が適用される以前の既存のサーバについては、３ヶ月以内に本規定に適合するようにすること。３ヶ月以内に、本規定に適合しない場合、情報セキュリティ委員会は、サーバの運用を強制的に停止させることができる。

４．２．３　環境設定の規定

(A.9.2.3、A.12.5.1、A.12.6.2、A.13.1.2)

（１）サーバ管理者は、サーバに使用するＯＳ及びソフトウェア（マルウェア対策ソフト、脆弱性検査ソフトを含む）には、情報セキュリティ委員会が規定したものを使用すること。

（２）サーバ管理者は、ＯＳのアクセス制御、ファイルのアクセス制御、アプリケーション及びサービスのアクセス制御は、厳密に行うこと。

（３）サーバ管理者、システム設計者は、ＷＥＢアクセスなどに使用する匿名ユーザアカウントを含む全てのアカウントのアクセス権限に対して、必要最低限のアクセス権限のみ許可すること。

（４）システム設計者は、リスク分析を実施し、仕様書の段階から、データの入力チェック、内部でのデータの処理プロセス、出力されるデータの妥当性などの、セキュリティ対策の実施を CGI、API などのアプリケーション開発を行う者に義務づけること。

（５）サーバ管理者は、サーバの趣旨、用途に応じた必要最低限のアプリケーション・サービス及びネットワーク・サービスのみインストールすること。

（６）サーバ管理者は、サーバには、システム管理者あるいはオペレータごとに個別のアカウントを割り当て、推測困難なパスワードを設定すること。特にシステム管理者もしくはシステム管理者に類する権限を持つアカウントのパスワードは、厳重に管理すること。

４．２．４　運用時の規定

(A.12.2.1、A.12.4.1、A.12.4.2、A.12.4.4、A.12.6.1)

（１）サーバ管理者は、サーバで使用するソフトウェアに最新のＯＳバージョン、最新のアプリケーションバージョンを使用し、最新のセキュリティパッチを適用すること。また不要サービスの削除を常に行うこと。

（２）サーバ管理者は、マルウェア対策として常にマルウェア対策ソフトウェアの定義ファイル、エンジンが最新のものとなるよう設定し、更新があった場合は直ちに最新のマルウェア対策ソフトウェアでサーバをチェックすること。

（３）サーバ管理者はサーバの認証ログ、アクセスログ、トランザクションログ、アプリケーションログ等サーバの趣旨、用途に応じたログの取得を行わなければならない。

（４）サーバ管理者は、ログを安全な場所に一定期間(例えば１年間)保存すること。

（５）サーバ管理者は、定期的(例えば毎月)にログの分析を行うこと。

（６）サーバ管理者は、サーバを信頼できる標準時刻と同期させたマスタクロックと同期させること。

（７）サーバ管理者は、定期的(例えば四半期に１度)に、第三者による以下の検査を受けること。

①脆弱性検査ソフトによる最新の脆弱性情報を含む検査

②「サーバ設置申請書」と実際の設置機器との整合性

③不要なアクセス権が存在しないこと

④不要なサービスが起動していないこと

⑤不要なアカウントが存在しないこと

⑥推測可能なパスワードが設定されていないこと

（７）サーバ管理者は、第三者による検査結果は必ず記録し、一定期間保管すること。

（８）第三者による検査によりセキュリティの不備が発見された場合、サーバ管理者は、直ちに不備を是正し、不備の内容と対策状況を情報セキュリティ委員会に報告すること。

（９）サーバ管理者は、セキュリティ侵害が発生した場合、セキュリティ侵害時の対応手順書に則って速やかに対応すること。またサーバ管理者は、セキュリティ侵害時の情報を、できるだけ速やかに、情報セキュリティ委員会に報告すること。情報セキュリティ委員会は、前述の報告を受けた後、各行政機関等への通報を含めて迅速に対応すること。

（１０）万が一、想定外のセキュリティ侵害が発生し、セキュリティ侵害時の対応手順書のみでは状況の改善が見込めない場合、サーバ管理者は即座に情報セキュリティ委員会に報告すること。サーバ管理者は、情報セキュリティ委員会の指示のもと、手順書外の行為を行うことができる。但し、作業実施記録は詳細に記録し保管すること。

（１１）サーバ管理者は、状況の改善後、作業実施記録を元にセキュリティ侵害時の対応手順書を更新すること。

４．３ クライアント端末の管理

４．３．１　クライアント端末の設定

(A.8.1.2、A.9.4.2、A.11.2.8、A.12.2.1、A.12.4.1、A.12.6.1、A.12.6.2)

（１）当社の業務において、従業員が使用できるPC、スマートデバイスは当社が支給・貸与したもののみとする。クライアント端末管理者は、PC、スマートデバイスを管理台帳で管理すること。

（２）クライアント端末管理者は、当社が支給・貸与するPC、スマートデバイスには、使用場所、使用する情報の重要度に応じて、ID、パスワードによる認証の他、二段階、二要素の認証機能を有効にすること。

（３）クライアント端末管理者は、当社が支給・貸与するPC、スマートデバイスには、規定されたソフトウェアを導入すること。したがって、それ以外のソフトウェアを導入できないように設定すること。

（４）クライアント端末管理者は、導入したソフトウェアを常に最新の状態とするため、修正プログラム等を自動適用する設定にすること。

（５）クライアント端末管理者は、当社が支給・貸与するPC、スマートデバイスには、規定されたマルウェア対策ソフトウェアを導入し、常に定義ファイル、エンジンが最新のものとなるように設定すること。

（６）クライアント端末管理者は、当社が支給・貸与するPC、スマートデバイスには、

規定された使用者ログ収集ソフトを導入すること。

（７）クライアント端末管理者は、当社が支給・貸与する PC、スマートデバイスのスクリーンロックを、PC に関しては１５分、スマートデバイスに関しては１分に設定すること。

（８）クライアント端末管理者は、当社が支給・貸与するスマートデバイスとクラウドサービスとのデータ連携機能を停止すること。

４．３．２　持ち出しクライアント端末の設定

(A.10.1.1、A.11.2.6)

（１）クライアント端末管理者は、持ち出し PC には、基本認証以外にも BIOS 上での認証を行うように設定すること。

（２）クライアント端末管理者は、持ち出し PC には、セキュリティチップ、暗号化機能を搭載した機種を選定すること。

（３）クライアント端末管理者は、持ち出しスマートデバイスには、認証機能、セキュリティチップ、暗号化機能を搭載した機種を選定すること。

４．３．３　クライアント端末の再利用

(A.11.2.7)

（１）PC、スマートデバイスの利用者が変わる場合、PC、スマートデバイスを初期化し、再設定すること。

４．４　ＬＡＮ接続

４．４．１　ＬＡＮ接続申請への対処

（１）情報システム部は、LAN に接続するクライアント端末は、当社が支給・貸与したもののみとし、利用者の個人所有の機器の LAN 接続を許可してはならない。

（２）情報システム部は、利用者からの申請に対し、利用目的、利用形態を審査し、審査結果を申請者に連絡すること。

（３）情報システム部は、利用申請に対し許可を与える場合、一定規則に則ってホスト名、IP アドレスを決定すること。また、必要に応じて DNS、およびディレクトリへの情報登録を行うこと。DHCP など、動的に IP アドレスが変化する利用が発生する場合は、その旨を認識すること。

（４）情報システム部は、利用申請に対し許可を与える場合に、接続する HUB・情報コンセント・利用ケーブル番号など、接続箇所を決定すること。

（５）情報システム部は、利用者に提供する以下の情報一覧（必要に応じて図を利用）を保存し、管理すること。

①IP アドレス利用一覧

②ホスト名称、DNS 登録一覧

③接続箇所利用一覧

（６）情報システム部は、利用申請に対し許可を与える場合、以下の情報を保存し、管理すること。

①利用者情報（氏名、所属、連絡先等）

②利用目的

③利用形態（設置箇所、利用時間帯、利用サービス、予定期間）

④利用機器情報（管理者、連絡先、MAC アドレス等ハードウェア情報、機器名称、IP アドレス、アドレス取得形態（固定 IP/DHCP）、接続箇所情報、DNS 登録の有無、ディレクトリ登録情報）

（７）情報システム部は、利用申請に対し許可を与える場合、申請者に対して以下の情報を連絡すること。

①許可された利用目的

②許可された利用形態（設置箇所、利用時間帯、利用サービス、予定期間）

③利用機器情報（ホスト名称、IP アドレス、アドレス取得形態（固定 IP/DHCP）、接続箇所情報、DNS 登録の有無、ディレクトリ登録情報）

４．４．２ ＬＡＮ接続時の留意点

（１）情報システム部は、緊急を要する場合など、必要に応じて利用者の LAN 接続を制限（アクセスの制御、切断など）することができる。また緊急時には、情報システム部は利用者に対して指示を与える前に LAN 接続を制限してもよい。

（２）情報システム部は、利用者の接続形態にあわせ、適切な認証機能・暗号化機能等を提供し、情報の保護に努めること。

①無線 LAN を利用する場合、認証および暗号化機能を利用すること。

②Switching HUB 等を利用して、利用者間でのパケットキャプチャができない仕組みを用いること。

③LAN に接続する機器の通信は、『システム利用規程』に照らして適切な通信のみに限定すること。

④リモートアクセスについては、『システム利用規程』に照らして適切な通信のみに限定すること。

⑤各サーバへのアクセス状況については、『本規程』に基づいて対処すること。

４．４．３ ＬＡＮ接続情報の更新、通知

（１）情報システム部は、利用者に許可した LAN 接続形態が守られているか、許可後 2 週間以内に、申請内容に照らして確認すること。また半年に一度、部門ごとの LAN 接続状態を確認すること。

（2）情報システム部は、利用者に許可した LAN 接続について、申請・変更時に予定していた期間が満了する2週間前に､利用者に期間の満了について通知すること。また、期間を満了する機器が周辺業務に影響を及ぼす事が無いか、あわせて調査すること。

４．４．４ 変更手続き

（1）情報システム部は、利用者からの変更申請に対し、利用目的・利用形態を審査し、申請結果を申請者に連絡しなければならない。変更申請は、変更時の申請に必要な情報（箇所、目的、事由）が明確になっていない場合、および変更前と比較して、同等以上のセキュリティが確保できない場合にはこれを許可しないこと。

（2）情報システム部は、変更申請に対し許可を与える場合、管理している情報（利用者情報、利用目的、利用形態、利用機器情報）を更新すること。

（3）情報システム部は、変更申請に対し許可を与える場合、申請者に対して以下の情報を連絡すること。

①許可された利用目的

②許可された利用形態（設置箇所、利用時間帯、利用サービス、予定期間）

③利用機器情報（ホスト名称、IP アドレス、アドレス取得形態（固定 IP/DHCP)、接続箇所情報、DNS 登録の有無、ディレクトリ登録情報）

４．４．５ 機器の撤去

（1）情報システム部は、以下に該当する場合、利用者の LAN 接続の終了を確認すること。

①申請・変更時に予定していた期間を満了した場合

②緊急時など、情報システム部が必要と判断した場合

③その他接続が不要、あるいは不適当と見なされる場合

（2）情報システム部は、利用者の LAN 接続終了にあわせ、利用者管理情報を更新（接続終了と判断できる状態に）すること。

（3）情報システム部は、以下の情報一覧を更新すること。

①IP アドレス利用一覧

②ホスト名称、DNS 登録一覧

③接続箇所利用一覧

４．５ マルウェア対策

４．５．１ マルウェア対策ソフトウェアの選定

（1）当社は、全てのサーバ、PC 及びスマートデバイスにマルウェア対策ソフトウェアを導入する。

（2）マルウェア対策ソフトウェアは、情報システム部が選定し、定期的に見直しを実施する。

（3）情報システム部が選定するマルウェア対策ソフトの要件には、以下の機能が含まれていなければならない。

①定義ファイルの自動更新機能

（ベンダー→社内サーバ→PC、ベンダー→スマートデバイス）

②常時スキャン機能

（サーバ、PC、スマートデバイス）

４．５．２　マルウェア対策ソフトの設定

（1）システム管理者は、マルウェア対策ソフトウェアは、常駐設定にし、ファイルへのアクセスおよび電子メールの受信時に、常時スキャンできるように設定すること。

（2）システム管理者は、常時スキャンだけではなく一週間に一度、ファイル全体に対するスキャンを実施するように設定すること。

（3）システム管理者は、定義ファイルを常時更新するように設定すること。

４．５．３　マルウェア対策窓口の設置

（1）情報システム部は、社内のマルウェア被害状況等を迅速に収集するために、マルウェア対策窓口を設置し周知徹底すること。

（2）マルウェア対策窓口は、社内のマルウェア被害状況を掌握し、問題発生時の一次対応を実施すること。

４．５．４　マルウェアに感染した場合

（1）利用者よりマルウェア感染の連絡を受けたシステム管理者は、ネットワーク機能を停止することを指示し、現場に急行すること。

（2）現場では、マルウェア対策ソフトの定義ファイルがいつ更新されているかを確認すること。最新であれば、PC、スマートデバイスに対してフルスキャンを実行し、マルウェアが検知されるかを確認すること。

（3）マルウェアが検知された場合、システム管理者は、そのマルウェアの特性上どのような挙動を示すか予測し、影響範囲の特定を実施すること。マルウェアが検知されなかった場合、ファイアウォールのログを確認し、怪しいログが残っていないかどうかを確認するなどして、原因を特定すること。

（4）情報システム部は、マルウェア被害の影響範囲が、社外にまで至っている場合、『セキュリティインシデント報告・対応規程』に従って、問題の沈静化を図ること。

４．６ 媒体の管理

４．６．１　サーバ、PC、スマートデバイス（IT 機器）の修理

（１）情報システム部は、故障の状況により、保管されている情報の確認や保護が実施できない場合、ハードディスク等の情報が保管されている装置を取り外して修理を依頼すること。

（２）情報システム部は、外部業者が社内に立ち入って修理を行う場合、『物理的管理規程』に基づいて対応すること。

４．６．２ 媒体の保管・再利用

(A.8.3.1、A.10.1.1、A.10.1.2)

（１）情報システム部は、機密性の高い情報を媒体に保存する場合、権限のない者が保管された情報にアクセスできないように、暗号化を行うか、媒体を鍵のかかる場所に保管し、鍵は容易に持ち出しが出来ない場所に保管すること。

（２）情報システム部は、暗号化鍵を、機密情報を保存した媒体とは別媒体に保管し、それぞれ別々の場所に保管すること。

（３）情報システム部は、機密性の高い情報が保存されている媒体を再利用する場合、保存されていた情報を、再生できない方法で消去すること。）

４．６．３　サーバ、PC、スマートデバイス（IT 機器）と媒体の廃棄

(A.8.3.2)

（１）情報システム部は、機密性の高い情報が保管されたハードディスク等媒体を廃棄する場合、理論的に情報を消去するか物理的に破壊して、情報が再生不能な状態にすること。

（２）情報システム部は、機密性の高い情報が保管されたバードディク等媒体の処分を外部業者に委託する場合、情報セキュリティ委員会の承認を得ること。外部業者に委託する場合、秘密保持及び、処分依頼品の再利用の禁止を契約書に含めること。

４．７ 脆弱性管理

４．７．１　脆弱性情報の収集

(A.12.6.1)

（１）情報システム部は、ソフトウェア及びハードウェアの各管理台帳をもとに、社内システムに導入されている全てのハードウェア及びソフトウェアの脆弱性情報を定期的に収集すること。

（２）脆弱性情報は、IPA、CERT、各ベンダーの Web サイトやサポートページなど、信用できる情報源から収集すること。

（3）収集した情報は、重要性、影響範囲などから以下の様に分類すること。

危険度　高：サーバの管理権限の剥奪などにより、業務が停止してしまう、または取引先などに影響を与える可能性があり、即座に対処が必要な情報

危険度　中：業務が停止あるいは取引先などには影響を与えないため、即座に対処する必要はないが、定期メンテナンス時などに対処する必要がある情報

危険度　低：特殊な環境/設定でのみ発生し、社内のシステムには関係がないため、特に対処しなくともよい情報

４．７．２　脆弱性情報の配布

(A.12.6.1)

（1）情報システム部は、収集した情報を危険度に応じて関係者に周知させること。

危険度　高：発見次第即座に関係者全員に連絡。連絡方法は基本的にはメールを使用。場合によっては社内放送なども利用。

危険度 中：週 1 回程度の定例報告を実施。メールにて関係者全員に連絡。

危険度 低:週 1 回程度の定例報告を実施。メールにてシステム管理者に連絡。

（2）情報システム部は、収集した情報を基に以下のものを作成、公開すること。

①サーバ設置時の OS の適用パッチ一覧

②サーバ設置時に必要となるサービスなどをまとめたセキュリティ設定チェックリスト

③アプリケーションの適用パッチ一覧

④アプリケーションの実装変更

４．７．３　脆弱性対応

(A.12.6.1)

（1）システム管理者は、セキュリティパッチの適用が可能な場合、危険度に応じて、パッチの適用を行うこと。

（2）システム管理者は、社内全てのサーバ、PC、スマートデバイス(IT 機器)に対して、（1）のパッチが適切に適用されているかを確認すること。

（3）セキュリティパッチの適用が、アプリケーションに大きな影響を与える可能性等が有る場合、システム管理者は、リスク分析を行い、情報セキュリティ委員会に報告し、以下の対応策の指示を受けること。

①障害のリスクを受容し、パッチを適用する。

②パッチを適用せず、リスクに運用で対処する。

③パッチを適用せず、リスクを受容する。

４．８　ログの取得及び監視

４．８．１　システムのログによる監視

(A.12.4)

（１）システム管理者は、対象システムの以下のログを取得すること。なお取得されたログはアクセス制御を施したログサーバに転送し、規定の期間(例えば１年間)安全に保管すること。

①取得対象

（ア）ログオン・ログオフの記録

（イ）サーバのアクセスログ

（ウ）システムログ

（エ）アプリケーションログ

（ウ）PC の使用ログ

②取得内容

（ア）アクセス時刻

（イ）アクセスの成功/失敗

（ウ）認証の成功/失敗

（エ）ファイルの作成/読み込み/書き込み/移動/コピー/消去

（オ）USB 等記録媒体の利用

（カ）メール、Web の利用履歴

（２）システム管理者は、許可された処理だけが実行されていることを確認するため、ログを定期的(例えば月１回)に分析すること。分析の結果、以下のような事象が確認された場合、情報セキュリティ委員会に報告すること。

①連続したアクセスの失敗

②連続した認証の失敗

③データベースからの大量データの送受信

④違反行為

⑤権限外の処理の試み

⑥ユーザアカウントに関する変更（追加、削除、グループ変更等）

⑦アクセス権の変更

（３）システム管理者は（２）の事象が、不正アクセスによってもたらされた疑いがある場合、『セキュリティインシデント報告・対応規程』に基づいて、原因究明、再発防止計画の作成等、適切な対応を実施すること。

（４）システム管理者は、（１）で取得するログの時間情報を適切に保ち、ログの証拠としての有効性を高めるため、NTP サーバを用いてシステム間の時刻同期をとる

こと。ただし、その場合、NTP サーバ自身のセキュリティ対策にも十分配慮すること。

４．９　サーバのバックアップ

(A.12.3)

（１）サーバ管理者は、業務上重要なサーバ（基幹システム、データベースサーバ、WWW サーバ、mail サーバ、ログサーバなど）については、そのデータ及び構成情報を定期的にバックアップすること。

（２）パッチの適用など、サーバのシステムに対して何らかの変更を行う場合、変更後、不具合が発生する可能性がある。その為、サーバ管理者は、サーバに対して変更を行う前にサーバのシステムバックアップを取ること。

（３）パッチの適用など、サーバのシステムに対して何らかの変更を行った場合、サーバ管理者は、安定動作確認後、サーバのシステムバックアップを取ること。

（４）サーバ管理者は、バックアップ頻度、バックアップ方法、バックアップメディア、バックアップメディアの保管場所を、以下を考慮して決定すること。

①事業継続性

②どの時点の情報にあるいはシステム構成に戻す必要があるのか

③何時までにシステムを復旧する必要があるのか

４．１０　システムの監視について

(A.12.1.3)

（１）システム管理者は、システム障害等の兆候をいち早く見つけるため、死活監視、リソース(CPU、メモリ、保存容量、IO、ネットワーク帯域等)監視、Error ログの監視を行うこと。

４．１１　運用業務

（１）システム管理者の運用業務はオペレータに委任することができるが、オペレータは運用手順書以外の操作を行ってはならない。

（２）システム管理者は、次の項目を含んだ運用日誌を作成し一定期間（例えば５年間)、保管管理すること。

①システムへのログイン時間とログオフ時間

②システムの設定変更内容

③ログの保存記録

④バックアップ実施記録

⑤システムエラーの記録とその是正処置

（３）情報セキュリティ委員会は、定期的に運用日誌を検査し不適切な記載が発見さ

れた場合、適切な是正処置をシステム管理者に指導すること。

５　運用確認事項

（１）『アカウント管理台帳』、『ハードウェア、ソフトウェア資産管理台帳』、『ログ』等運用において必要な記録が残っているかを定期的に確認すること。

（２）ハードウェア、ソフトウェアライセンスの棚卸しを定期的に実施すること。特に、持ち運びが可能な装置(ノート PC、スマートデバイス、USB 等)は高頻度で棚卸しを実施すること。

（３）本規程に基づき、システムが運用、管理されていることを定期的に確認すること。

（４）サーバ、クライアント端末ログの分析結果は、ネットワーク管理者と情報共有すること。

（５）『リスク管理規程』によるリスク評価結果、脆弱性管理の結果に基づき、定期的に運用方法を見直しすること。

（６）リスクを受容して運用している場合、新技術、運用方法により、リスクを低減する方法が無いかを定期的に評価すること。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならな

ﾚﾝ。

ネットワーク管理規程

1.0版

ネットワーク管理規程

ネットワーク管理規程

１　趣旨

本規程は、当社のネットワークの可用性の確保、および不正アクセスや通信の盗聴などの防止に必要なセキュリティに関して記載するもので、インターネット接続、社内ＬＡＮ、社内ＷＡＮにおいてネットワーク機器及び各種通信関連のサーバの構築の条件、及び運用・管理の実施方法の遵守事項を規定する。

２　対象者

ネットワークの構築、運用、管理する全ての従業員。

３　対象システム

インターネット接続、社内ＬＡＮ、社内ＷＡＮで構成する社内ネットワークのネットワーク機器及び各種通信関連サーバ。

４　遵守事項

４．１　設置基準

ネットワークを構成する機器の設置環境、機器に必要な機能などを以下に示す。

(A.9.1.2、A.13.1.3)

（１）対象のネットワーク環境

本規程が対象とするネットワーク環境は、以下に示す。

①インターネットと接続をするインターネット接続環境（グローバルアドレスを利用したネットワークとし、グローバルゾーンとＤＭＺの２つとする)。

②社内環境に設置するＬＡＮを利用した社内ＬＡＮ環境（プライベートアドレスを利用したネットワークとし、サーバゾーンと各フロアゾーンと営業所と子会社、関連会社の３つとする）

③専用線及び公衆回線、それに準ずる専用線を利用した社内ＷＡＮ環境（プライベートアドレスを利用したネットワークとする）

④社外から社内システムへのアクセスを提供するリモートアクセス接続環境

（２）対象のネットワーク構成機器

本規程が対象とするネットワークを構成する機器を、以下に示す

①ネットワーク機器（ルータ、ハブ、スイッチングハブ、無線ＬＡＮアクセスポイント、負荷分散装置、ＶＰＮ装置等）

②インターネット関連機器（ＤＮＳサーバ、WWWサーバ、メールサーバ、Ｐｒｏｘｙ、ファイアウォール、ＷＡＦ、不正侵入防御装置（ＩＤＳ、ＩＰＳ)、マルウエア対策サーバ、ＦＴＰサーバ等）

③リモートアクセスシステムにおいては、リモート接続用の専用機器（ルータ、サーバ等）と認証用サーバ

④イントラネット関連機器（WWWサーバ、ＬＤＡＰ／Ａｃｔｉｖｅ　Ｄｉｒｅｃｔｏｒｙサーバ、ＤＮＳサーバ、メールサーバ、ファイルサーバ、プリンタサーバ，マルウエア対策サーバ、業務システムサーバ、ＰＣなど）

⑤その他、Ｒａｄｉｕｓサーバ、不正アクセス監視サーバ、運用監視サーバ、時刻同期サーバ

（３）インターネット接続機器の設置環境

インターネットに接続する機器は、以下の環境に設置しなければならない。

①物理的な破壊、不正な操作などが行われないよう入退出管理が行われ、施錠した安全な場所、もしくは施錠されたボックスに設置する。

②突発的な停電への対策が行われていること。

③サーバは、サーバルームに構築するサーバ専用セグメントに接続すること。

（４）社内ＬＡＮ接続機器の設置環境

社内ＬＡＮに接続する機器は、以下の環境に設置しなければならない。

①イントラネットにおいて重要なサーバゾーンの機器は物理的な破壊、不正な操作などが行われないよう入退出管理が行われ、施錠した安全な場所、もしくは施錠されたボックスに設置する。

②イントラネットにおいて重要なサーバゾーンの機器には、突発的な停電への対策が行われていること。

③事務室に設置するハブ、無線ＬＡＮアクセスポイントは、社員が自由に操作できないよう空きポートの保護、設置場所の保護に努める。

（５）社内ＷＡＮ接続機器の設置環境

社内ＷＡＮに接続する機器は、以下の環境に設置しなければならない。

①物理的な破壊、不正な操作などが行われないよう入退出管理が行われ、施錠した安全な場所、もしくは施錠されたボックスに設置する。

②突発的な停電への対策が行われていること。

（６）リモートアクセス接続用機器の設置環境

リモートアクセス接続用の機器は、以下の環境に設置しなければならない。

①物理的な破壊、不正な操作などが行われないよう入退出管理が行われ、施錠した安全な場所、もしくは施錠されたボックスに設置する。

②突発的な停電への対策が行われていること。

③サーバは、サーバルームに構築するサーバ専用セグメントに接続すること。

（７）その他設置機器の管理事項

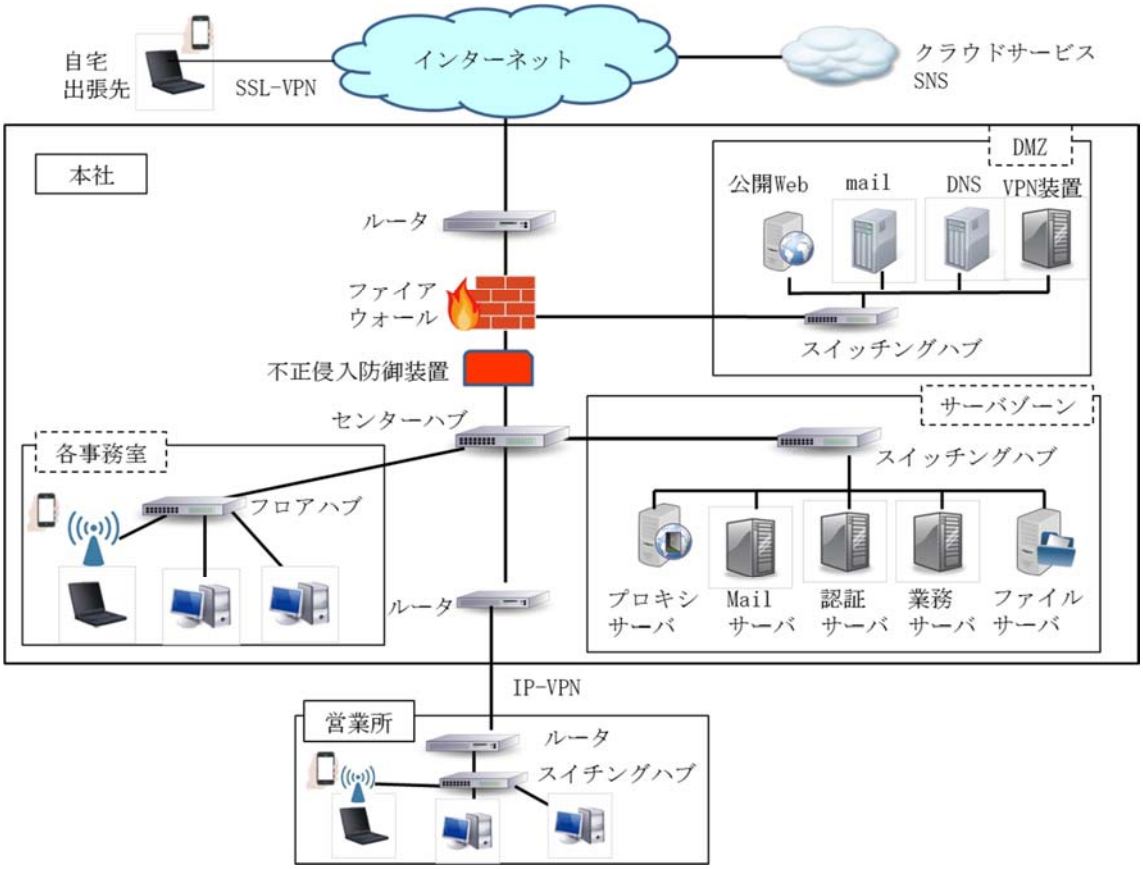
設置するネットワーク機器について以下の管理を行わなければならない。

①機器の設置、廃止、移動などを行う場合は、システムセキュリティ責任者に申

請の上、設置、変更、廃止の承認が必要である。

②各機器は、設置場所・接続機器状況・管理者を明確にすること。

下図にシステム構成図を示す。



４．２　導入時の遵守事項

インターネット接続環境、社内ＬＡＮ環境、社内ＷＡＮ環境、リモート接続環境にネットワーク機器の導入時における遵守事項を以下に示す。

４．２．１　共通の遵守事項

（A.9.1.1、A.9.1.2、A.9.2.3、A.9.2.4、A.9.2.5、A.13.1.1、A.13.1.2、A.13.1.3、A.13.2.1）

（１）インターネット、社内ＬＡＮ（有線ＬＡＮ、無線ＬＡＮ）、社内ＷＡＮ、リモートアクセスといったアクセス経路におけるリスクや、システムの重要度などを考慮し、ネットワークは適切にセグメント化した構成とし、セグメント間のアクセス制御をネットワーク機器は行うこと。

（２）ネットワーク機器の導入時には、以下のドキュメントを作成し、構成管理を行

うこと。

①ネットワーク構成図（物理構成及び論理構成）

②ネットワーク機器のＩＰアドレス

③ネットワーク機器の設定一覧

④ネットワーク機器のコンフィグまたはコンフィグファイル

⑤ネットワーク機器ソフトウェア版数

（３）ネットワーク機器の導入時には、運用手順書を作成すること。

（４）ネットワーク機器の停止が業務に重大な支障をきたすネットワーク機器については、冗長化を行うこと。

（５）主要な機器は、ネットワーク管理者、利用者、その他のアクセスログ、およびネットワーク機器の管理者IDの変更､操作などのイベントログを取得すること。

（６）主要な機器は稼働監視、不正アクセスの有無監視が可能なこと。

（７）パスワードの設定が可能な機器は､『システム管理規程』に準拠し、ネットワーク管理用のＩＤとそのＩＤを利用するネットワーク管理者、オペレータの関係をアクセス権も含め管理する。

（８）ネットワーク管理者ＩＤの初期パスワードは、導入時に変更すること。

（９）導入を委託したさいは、別途、定める受け入れ基準に従い、要求事項を満足しているか、検査を行うこと。検査結果が受け入れ基準を満たさない場合は、委託先に改修を行わせること。

（１０）インターネット接続環境、ＷＡＮなどにおいて外部サービスを利用する場合は、セキュリティについての提供内容、運用、障害時の対応などを確認したうえで導入すること。

４．２．２　インターネット接続環境における導入時遵守事項

（A.9.1.2、A.12.6.1、A.13.2.1、A.13.2.3）

（１）ネットワーク接続構成

インターネット接続環境に設置するネットワーク機器は、以下のセキュリティ対策を考慮した構成を行わなければならない。

①インターネットとの接続箇所は、原則、1か所に限定するが、別途、接続が必要な場合は、同等の構成を行うこと。

②ルータによるインターネットプロバイダ接続とし、プロバイダ側のネットワークはグローバルアドレスを利用しなければならない。

③プロバイダと当社の境界には、ファイアウォールを設置し、不正アクセスの対策を実施しなければならない。

④インターネット接続環境に接続できる機器は、インターネットサーバとする。

⑤インターネットサーバはファイアウォールを介して接続するＤＭＺに設置す

る。

⑥ファイアウォールでは、グローバルアドレスとプライベートアドレスの変換を行うこと。

⑦インターネット接続環境と社内ＬＡＮとの境界には、ファイアウォールを設置し、外部からの不正アクセスの対策を実施しなければならない。

⑧社内ＬＡＮから外部へのＷｅｂアクセスは、Ｐｒｏｘｙを経由すること。

（２）実装機能

インターネット接続環境に設置するネットワーク機器には、以下のセキュリティ機能を有する機器を設置すること。

①外部からの不正アクセスを防止、検知する機能を有する機能。

②Ｗｅｂ通信や送受信メールにおいてマルウエアを検知、防御する機能。

③重要な通信を暗号化する機能。

④送信メールの添付ファイルについてサイズ制限、拡張子による送信制限を行う機能。

⑤不正なサイトへのアクセスによるマルウエア、不正ソフトウェア感染防止のためのアクセス制限（以下、ＵＲＬフィルタ）。

⑥マルウエア、不正ソフトウェア感染を狙った虚偽のＷｅｂサイトへの誘導や宣伝を目的としたメール（以下、スパムメール）の利用者への到達制限機能。

⑦インターネットとの境界に設置するファイアウォール、ルータでは以下のログの取得機能。

（ア）アクセス日時

（イ）プロトコル番号

（ウ）ソースＩＰアドレス

（エ）ソースポート

（オ）ディスティネイションＩＰアドレス

（カ）ディスティネーションポート

（キ）許可しているアクセス及び、許可していないアクセス

（３）利用できるサービス

インターネット接続環境においては、以下のサービスを利用可能とする。

①社外ユーザ向けのWWWサービス（情報公開）

②社内ユーザ向けのWWWサービス（情報収集・公開）

③社内ユーザ向けのＳＮＳサービス

④メールの送受信サービス

⑤ドメインネームサービス

⑥ファイル転送サービス

⑦時刻同期サービス

４．２．３　社内ＬＡＮ環境における導入時遵守事項

（A.9.1.2、A.9.2.1、A.13.1.1、A.13.2.1）

（１）ネットワーク接続構成

社内ＬＡＮ環境に設置するネットワーク機器は、以下のセキュリティ対策を考慮した構成を行わなければならない。

①スイッチングハブ（レイヤ３、レイヤ２）とハブ、無線ＬＡＮ　ＡＰを使用し、ビル内のネットワークとする。

②接続できる機器は、各種サーバとＰＣとプリンタとする。

③使用するアドレスは、プライベートアドレスを利用すること。

④重要なシステムを構成するサーバ群と利用者が利用するＰＣとは別セグメントに分離した構成とし、サーバセグメントとそれ以外の利用者ＰＣ、インターネットなどの間でアクセス制御を行うこと。

⑤社内ＬＡＮに接続するＰＣは、『システム利用規程』に基づいて導入されたものに限る。個人所有のＰＣの社内ＬＡＮ接続は許可しない。

⑥社内ＬＡＮに接続するＰＣは、『物理的管理規程』または『システム利用規程』に基づいたセキュリティ対策が施されているものとする。

（２）実装機能

社内ＬＡＮ環境に設置するネットワーク機器には、以下のセキュリティ機能を有する機器を設置すること。

①ネットワークセグメント間において、通信サービス毎のアクセス制限が可能なこと。

②無線ＬＡＮアクセスポイントはＷＰＡまたはＷＰＡ２で通信の暗号化が可能なこと。

③無線ＬＡＮアクセスポイントには認可した機器、および一意のＩＤで認証・認可した人のみ接続が可能なこと。

（３）利用できるサービス

社内ＬＡＮ環境においては、以下のサービスを利用可能とする。(9.1.2)

①インターネット（WWWサービス）

②イントラネット（社内各業務システム）

③ファイル共有サービス

④プリンタ共有サービス

⑤ドメインネームサービス

⑥メールの送受信サービス

４．２．４　社内ＷＡＮ環境における導入時遵守事項

(A.9.1.2)

（１）ネットワーク接続構成

社内ＷＡＮ環境に設置するネットワーク機器は、以下のセキュリティ対策を考慮した構成を行わなければならない。

①ルータによる専用回線による専用接続とし、接続先は社内拠点（支店、営業所）及び子会社・関連会社とする。

②使用するアドレスは、プライベートアドレスを利用すること。

③専用線接続が困難な場合は、情報セキュリティ委員会が認めた場合のみインターネットを利用したＶＰＮ装置を利用した接続を認める。

④専用線、ＶＰＮ装置を利用した接続は、以下の構成情報を管理すること。

（ア）接続先住所、組織名称

（イ）接続目的

（ウ）接続種別（専用線、ＶＰＮ）

（エ）接続先双方のシステム構成

（オ）接続先双方のアクセス許可範囲

（カ）許可されるサービスとその方向性

（キ）接続先双方のシステム管理者名、システムセキュリティ責任者名

（ク）接続先双方の異常の定義と異常連絡体制

（２）実装機能

社内ＷＡＮ環境に設置するネットワーク機器には、以下のセキュリティ機能を有する機器を設置すること。

①ネットワークセグメント間において、通信サービス毎のアクセス制限が可能なこと。

②ＶＰＮでは、最低限、送信元及び送信先ＩＰアドレスによるアクセス制限を行うこと。

（３）利用できるサービス

社内ＷＡＮ環境においては、以下のサービスを利用可能とする。(9.1.2)

①インターネット

②イントラネット（社内各業務システム）

③ファイル共有サービス

④メールの送受信サービス

４．２．５　リモートアクセス接続環境における導入時遵守事項

（A.6.2.1、A.6.2.2、A.9.1.2、A.9.2.1、A.9.2.2、A.13.1.1、A.13.2.1、A.13.2.3）

（１）ネットワーク接続構成

リモートアクセス接続環境に設置するネットワーク機器は、以下のセキュリティ対策を考慮した構成にしなければならない。

①リモート接続用の専用機器（ルータ、サーバ等）と認証用サーバから構成する。

（２）実装機能

リモートアクセス接続環境に設置するネットワーク機器には、以下のセキュリティ機能を有する機器を設置しなければならない。

①社内にアクセスできるサーバおよびサービスは必要最低限に制限が可能なこと。

②利用者毎にアクセスできるサーバおよびサービスを制限可能とすること。

③社内に設置されたサーバのみにアクセスを制限すること。ただし、申請により許可された社員についてはインターネットへアクセスを可能とする。

④リモートアクセスシステムは、利用者情報を管理すること。

⑤リモートアクセスシステムでは、利用者認証（発信者識別、ワンタイムパスワード）を行うこと。

⑥リモートアクセスシステムは、通信手段としてＶＰＮ（暗号化）に対応していること。

⑦リモートアクセスシステムでは以下のログを取得、保存できること。

（ア）接続成功、失敗

（イ）接続の開始時間と終了時間

（ウ）接続時のアカウント名

（エ）発信者識別

（オ）障害情報（エラー情報）

⑧自宅からリモートアクセスする場合は、自宅のネットワークを安全に保つこと。無線ＬＡＮを自宅で利用する場合は、無線ＬＡＮに登録したＰＣのみにアクセス制限し、ＷＰＡまたはＷＰＡ２で通信を暗号化すること。

（３）利用できるサービス

リモートアクセス接続環境においては、以下のサービスを利用可能とする。

①ｈｔｔｐ、ｈｔｔｐｓを利用した社内システム

②電子メールサービス

③ファイル転送サービス

④ファイル共有サービス

⑤業務システムとして導入しているサービス

（4）クライアント端末の遵守機能

リモートアクセスに利用するクライアント端末は以下の機能を実装する。

①利用する社員の認証を行い権限のある者のみ利用可能とすること。

②クライアント端末は、ワンタイムパスワードに対応すること。

③クライアントは、通信手段として発信者識別・ＶＰＮ（暗号化）に対応すること。

④クライアント端末は、『システム利用規程』を満たし、かつ『システム利用規程』の対策を満たしていること。

４．３　運用時の遵守事項

インターネット接続環境、社内ＬＡＮ環境、社内ＷＡＮ環境、リモート接続環境にネットワーク機器の運用時におけるネットワーク管理者の遵守事項を以下に示す。

４．３．１　共通の遵守事項

（A.6.2.2、A.9.1.2、A.9.2.2、A.9.2.3、A.9.2.5、A.9.2.6、A.12.6.1、A.13.1.1）

（1）ネットワーク管理

ネットワーク機器の管理者の責任範囲､責任について明確化し､手順書に従い、運用すること。

また、ネットワーク管理者はサーバ管理者と職務を分離すること。

（2）構成管理

ネットワーク機器の以下の現状の構成管理の維持と最新情報の把握を行う。

①ネットワーク構成図（物理構成及び論理構成）

②ネットワーク機器のＩＰアドレスの管理

③ネットワーク機器の設定一覧

④ネットワーク機器のコンフィグファイルの管理

⑤ネットワーク機器のソフトウェア版数

⑥ネットワーク機器のソフトウェアの最新情報

⑦最新のパッチ情報

（3）変更管理

ネットワーク機器の追加、撤去や設定の変更、パッチ適用、ソフトウェアの版数アップ時においては、その変更における影響を事前に検証し問題が発生しないよう努め、変更内容および検証結果についても記録を残すこと。

（4）日常運用

ネットワーク機器の以下の監視と日常の運用を行う。

①日常の運用、監視で行ったことや、検討事項は記録として残すこと。

②フロアゾーンのスイッチ以外の主要ネットワーク機器が正常に動作している

か稼働を監視すること。

③インターネット、社内ＷＡＮ、および社内ＬＡＮのサーバゾーンの重要な機器においては、取得したアクセスログ、システムログなどを定期的に解析すること。

④ログの解析結果から異常やインシデントに結びつく危険な兆候を検出した場合は、『セキュリティインシデント報告・対応規程』に従った対応を行うこと。

⑤ネットワーク機器で行う各アクセス制御については、定期的に見直しすること。

⑥ネットワーク機器のソフトウェア、ファームウェアなどに対するパッチは、適用による影響、適用しないことによる影響を整理したうえで計画をたて適用すること。なお、適用が不可能な場合、代替策を講じること。

⑦ネットワーク管理者、オペレータの任命は、システムセキュリティ責任者の承認を得ること。

⑧『システム管理規程』に準拠し、ネットワーク管理者、オペレータのパスワードは定期的に変更を行い、担当者の異動があった場合は、そのＩＤの利用を停止すること。

⑨ネットワーク管理者ＩＤに共有ＩＤを利用する場合は、パスワードを定期的に変更し、ネットワーク管理者担当間のみで共有すること。また、ネットワーク管理者に異動、退職などの人事が発生した場合は、パスワードを早期に変更すること。

４．３．２　インターネット接続環境における遵守事項

（A.9.1.2、A.9.2.2、A.12.6.1、A.13.1.1）

（１）機器設定の最新化

インターネットの各機器の設定は、常に最新に保たねばならない。

①インターネットからのＷｅｂ通信やメールの添付ファイルを利用したマルウエア、不正ソフトウェアの攻撃に対するマルウエア対策として、パターン情報を常に最新に維持する。

②ＵＲＬフィルタのフィルタ情報を最新に維持する。

③スパムメールと判断する条件を最新化する。

（２）設定の見直し

インターネットの各機器の設定内容は、ログ解析やその他に基づき見直しを行わなければならない。

①ファイアウォールのアクセスルールを定期的に見直しする。

②インターネットからの不正アクセスに備えたアクセス制御の見直しをログ解析や世の中の動向を鑑みて行う。

③ＵＲＬフィルタを経由せず外部サービスやＦＴＰなどの利用が必要な場合は、部門責任者の承認を得たうえでＵＲＬフィルタ経由限定を解除する。

④ＵＲＬフィルタでアクセス制限したサイトへのアクセスや、スパムメール扱いされたメールの受信が必要な場合､部門責任者の承認を得たうえでＵＲＬフィルタ制限、スパム扱いを解除する。

⑤外部から不正中継される設定を検知した場合は、すみやかに設定の見直しを行う。

（３）脆弱性の検知、攻撃検知時の対応

インターネットの各機器の脆弱性や攻撃の検知時には以下の対応を行わなければならない。

①インターネットから直接アクセス可能なＩＰを持つ機器に対し、定期的に脆弱性検査を行い、検出した脆弱性に対し計画を立て、改善する。

②インターネット、または社内ネットワークからインターネットに対し不正アクセスやマルウエア、不正プログラムの攻撃を検知した時は、『リスク管理規程』にのっとり対応する。

４．３．３　社内ＬＡＮ環境における遵守事項

（A.9.1.2、A.9.2.2、A.12.6.1、A.13.1.1）

（１）機器設定の最新化

社内ＬＡＮに接続するＰＣの設定､その他の以下の情報を常に最新に保つこと。

①利用者情報（氏名、所属、連絡先等）

②利用目的

③利用形態（設置希望箇所、利用時間帯、利用サービス、予定期間）

④利用機器情報（管理者、連絡先、ＭＡＣアドレス等ハードウェア情報

⑤ＰＣ名称

⑥利用機器情報（ＭＡＣアドレス等ハードウェア情報、アドレス取得形態（固定ＩＰ/ＤＨＣＰ）、接続箇所情報、ＤＮＳ登録の有無、ディレクトリ登録情報）

⑦ＩＰアドレス

⑧ＯＳとそのバージョン

⑨ソフトウェアとそのバージョン

⑩無線ＬＡＮへの接続を認可するＰＣに関する上記の情報

⑪無線ＬＡＮへの接続を認可する利用者ＩＤ

⑫無線ＬＡＮからアクセスできるサーバおよびサービスへのアクセス制限を最新の情報に基づき維持する。

（２）設定の見直し

社内ＬＡＮの各機器の設定内容は、ログ解析やその他に基づき見直しを行うこと。

①社内ＬＡＮに接続するＰＣの利用者、利用目的、あるいは利用形態の変更や廃止の利用者からの申請に対し、情報システム部は、変更、撤去の手続きを行う。

②サーバセグメントと利用者のＰＣセグメント、インターネット接続セグメント間のアクセス制御の見直しをログ解析や世の中の動向を鑑みて行う。

③無線ＬＡＮ利用がない、または認可した人の異動、退職などにより不要となったＩＤがないか棚卸を行い、不要となったＩＤの削除を早期に行う。

（３）脆弱性の検知、攻撃検知時の対応

社内ＬＡＮの各機器の脆弱性や攻撃の検知時には以下の対応を行うこと。

①社内ＬＡＮの機器の脆弱性を認知した場合は、リスク評価を行い、計画を立て、改善する。

②社内ネットワーク内において不正アクセスやマルウエア、不正プログラムの攻撃を検知した時は、『リスク管理規程』にのっとり対応する。

４．３．４　社内ＷＡＮ環境における遵守事項

（A.9.1.2、A.9.2.2、A.12.6.1、A.13.1.1）

（１）機器設定の最新化

社内ＷＡＮ以下の構成情報を常に最新に保つこと。

①接続先住所、組織名称

②接続目的

③接続種別（専用線、ＶＰＮ）

④接続先双方のシステム構成

⑤接続先双方のアクセス許可範囲

⑥許可されるサービスとその方向性

⑦接続先双方のシステム管理者名、システムセキュリティ責任者名

⑧接続先双方の異常の定義と異常時連絡体制

（２）設定の見直し

社内ＷＡＮの各機器の設定内容は、ログ解析やその他に基づき見直しを行うこと。

①トラフィック変化に伴うネットワークの帯域の定期的な見直しを行う。

（３）脆弱性の検知、攻撃検知時の対応

社内ＷＡＮの各機器の脆弱性や攻撃の検知時には以下の対応を行うこと。

①社内ＷＡＮの機器の脆弱性を認知した場合は、リスク評価を行い、計画を立

て、改善する。

４．３．５　リモートアクセス接続環境における遵守事項

（A.6.2.2、A.9.1.2、A.9.2.1、A.9.2.2、A.9.2.6、A.12.6.1、A.13.1.1）

（１）機器設定の最新化

リモートアクセスの各機器の設定は、常に最新に保つこと。

①社内にアクセスできるサーバおよびサービスへのアクセス制限を最新の情報に基づき維持する。

②リモートアクセス接続を認可する人のＩＤを最新の状態で維持する。

③利用者毎にアクセスできるサーバおよびサービスを、最新の情報に基づき維持する。

（２）設定の見直し

リモートアクセスの各機器の設定内容は、ログ解析やその他に基づき見直しを行うこと。

①リモートアクセスの利用がない、または認可した人の異動、退職などにより不要となったＩＤがないか棚卸を行い､不要となったＩＤの削除を早期に行う。

②社内に設置されたサーバにのみアクセスを制限する。ただし、申請により許可された社員についてはインターネットへのアクセスを可能とする。

（３）脆弱性の検知、攻撃検知時の対応

リモートアクセスの各機器の脆弱性や攻撃を検知した時には、以下の対応を行うこと。

①インターネットから直接アクセス可能なＩＰアドレスを持つ機器に対し、定期的に脆弱性検査を行い、検出した脆弱性に対し計画を立て、改善する。

②インターネットからリモートアクセスに対し不正アクセスやマルウエア、不正プログラムの攻撃を検知した時は､『リスク管理規程』にのっとり対応する。

５　運用確認事項

インターネット接続環境、社内ＬＡＮ環境、社内ＷＡＮ環境、リモート接続環境において、本規程に基づき遵守事項が守られていることを、記録や再実施で定期的に確認すること。

５．１　共通の運用確認事項

（１）構成管理

ネットワーク機器の追加、撤去や設定の変更に伴う構成管理が、変更履歴やコンフィグファイルの日時から適切に行われていることを確認すること。

（2）変更管理

パッチ適用、ソフトウェアの版数アップは、実施しなかった時の影響や変更による影響の確認、または検証したうえで実施していることを、確認/検証日時、パッチ適用日時、実施者、承認者などの記録により確認すること。

（3）日常運用

ネットワーク機器は、以下の監視と日常の運用が維持できていることを確認すること。

①インターネット、社内ＷＡＮ、および社内ＬＡＮのサーバゾーンの重要な機器においては、アクセスログ、システムログが取得できていることを実際に確認する。

②記録からアクセスログ、システムログなどを定期的に解析し、異常やインシデントに結びつく危険な兆候を検出した場合は、『セキュリティインシデント報告・対応規程』に従い適切に対応しているか確認する。

③記録からアクセス制御について定期的に見直しを行い、必要であれば適切にアクセス制御を見直し、設定を変更しているか確認する。

④記録からネットワーク機器のソフトウェア、ファームウェアなどに対するパッチが提供されたとき、適用による影響、適用しないことによる影響を整理したうえで計画をたて、パッチ適用が行われているか、また、適用が不可能な場合、代替策を講じているか確認する。

⑤記録からネットワーク管理用のＩＤおよびアクセス権、およびネットワーク管理者、オペレータの棚卸を定期的に行っていることを確認する。

⑥記録からネットワーク管理者、オペレータの任命は、システムセキュリティ責任者の承認を得ていることを確認する。

⑦記録からネットワーク管理者、オペレータのパスワードが定期的に変更され、担当者の異動、退職があった場合は、そのＩＤの利用を速やかに停止していることを確認する。

⑧記録からネットワーク管理者ＩＤに共有ＩＤを利用する場合は、パスワードを定期的に変更し、ネットワーク管理者担当間のみで共有する。また、ネットワーク管理者に異動、退職などの人事が発生した場合は、パスワードを早期に変更していることを確認する。

５．２　インターネット接続環境における運用確認事項

（1）機器設定の最新化

インターネットの各機器の設定を、常に最新に保つ運用を行っていることを定期的に確認すること。

①インターネットからのＷｅｂ通信やメールの添付ファイルを利用したマルウ

エア､不正ソフトウェアの攻撃に対するマルウエア対策のパターン情報が最新になっていることを確認する。

②ＵＲＬフィルタのフィルタ情報が最新になっていることを確認する。

③スパムメールと判断する条件が最新になっていることを確認する。

（２）設定の見直し

インターネットの各機器の設定の見直しを行っていることを定期的に確認すること。

①記録からインターネットからの不正アクセスに備えたアクセス制御の見直しをしていることを確認する。

②記録からＵＲＬフィルタを経由せず外部サービスやＦＴＰなどの利用は、許可したもののみとなっているか確認する。

③記録からＵＲＬフィルタ制限、スパム扱いの解除は、許可したもののみとなっているか確認する。

（３）脆弱性の検知、攻撃検知時の対応

インターネットの各機器の脆弱性や攻撃を検知した時の対応が適正に行われていることを定期的に確認すること。

①脆弱性検査の報告と、検出した脆弱性に対する改善計画があることを確認する。

５．３　社内ＬＡＮ環境における運用確認事項

（１）機器設定の最新化

社内ＬＡＮの各機器の設定を、常に最新に保つ運用を行っていることを定期的に確認すること。

①台帳の変更履歴により社内ＬＡＮに接続するＰＣの設定、その他の管理情報を常に最新に保っていることを確認する。

（２）設定の見直し

記録から社内ＬＡＮの各機器の設定の見直しを行っていることを定期的に確認すること。

①記録から社内ＬＡＮの各機器の設定の見直しを、ＰＣの利用者、利用目的、あるいは利用形態の変更や廃止したさいに行っていることを確認する。

（３）脆弱性の検知、攻撃検知時の対応

社内ＬＡＮの各機器の脆弱性や攻撃の検知時の対応が適正に行われていることを定期的に確認すること。

①脆弱性検査の報告と、検出した脆弱性に対する改善計画があることを確認する。

５．４　社内ＷＡＮにおける運用確認事項

（１）機器設定の最新化

社内ＷＡＮの各機器の設定を、常に最新に保つ運用を行っていることを定期的に確認すること。

①台帳の変更履歴により構成情報を常に最新に保っていることをこと確認する。

（２）設定の見直し

記録から社内ＷＡＮの各機器の設定の見直しを行っていることを定期的に確認すること。

①記録から社内ＷＡＮの各機器の設定の見直しをトラフィック変化に伴い行っていることを確認する。

（３）脆弱性の検知、攻撃検知時の対応

社内ＷＡＮの各機器の脆弱性や攻撃の検知時の対応が適正に行われていることを定期的に確認すること。

①脆弱性検査の報告と、検出した脆弱性に対する改善計画があることを確認する。

５．５　リモートアクセス接続環境における運用確認事項

（１）機器設定の最新化

リモートアクセスの各機器の設定を、常に最新に保つ運用を行っていることを定期的に確認すること。

①記録から社内にアクセスできるサーバおよびサービスへのアクセス制限を最新に保っていることをこと確認する。

②記録からリモートアクセス接続を認可する人のＩＤの登録をしていることを確認する。

③記録から利用者毎にアクセスできるサーバおよびサービスを最新に保っていることを確認する。

（２）設定の見直し

記録からリモートアクセスの各機器の設定の見直しを行っていることを定期的に確認すること。

①記録からリモートアクセスの利用がない、または異動、退職などにより不要となったＩＤがないか棚卸を行い､不要となったＩＤの削除を速やかに行っていることを確認する。

②記録からリモートアクセス経由でインターネットへのアクセスは許可したもののみとしているか確認する。

③記録からリモートアクセス接続は許可したもののみとしているか確認する。

（３）脆弱性の検知、攻撃検知時の対応

リモートアクセスの各機器の脆弱性や攻撃の検知時の対応が適正に行われていることを定期的に確認すること。

①脆弱性検査の報告と、検出した脆弱性に対する改善計画があることを確認する。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

システム利用規程

1.0版

システム利用規程

システム利用規程

１　趣旨

本規程は、システムやネットワーク利用時における可用性・機密性・完全性を確保し、発生し得る各種問題を未然に防ぐことを目的とする。

２　対象者

ＰＣ、システム、ネットワークを利用するすべての従業員。

３　対象システム

当社より支給・貸与するＰＣ、および利用するシステムとネットワーク。

４　遵守事項

４．１　　ＰＣにおけるセキュリティ対策

４．１．１　ＰＣの利用

(A.9.3.1)

当社の業務に利用するＰＣは、以下のものでなければならない。

（１）当社が支給・貸与するＰＣのみとする。

４．１．２　ＰＣで使用できるソフトウェア

(A.12.6.1、A.12.6.2)

当社が支給・貸与するＰＣに導入するソフトウェアは、以下を遵守しなければならない。

（１）ＰＣの利用者は、システム管理者が初期導入したソフトウェアのみ使用すること。

（２）規定されたソフトウェア以外で、業務上やむを得ず使用する必要がある場合、ＰＣの利用者は、情報セキュリティ担当者に申請し、許可を得なければならない。

（３）ＰＣの利用者は、情報セキュリティ担当者が提供するソフトウェア情報をもとに最新の修正プログラム等を適用しなければならない。

４．１．３　ＰＣのパスワード管理

(A.9.4.2、A.9.4.3)

当社が支給・貸与するＰＣの盗難、紛失に備え、以下を遵守しなければならない。

（１）ＰＣの利用者は、支給・貸与を受けた場合、ＰＣログオンの初期パスワードを直ちに変更しなければならない。

（２）ＰＣの利用者は、システム管理者の設定したパスワードポリシーに従い、パスワードを設定し、定期的に変更しなければならない。
（３）ＰＣの利用者は、第三者が容易に推測できないパスワードを選択すること。

４．１．４　ＰＣでの情報の取り扱い

(A.8.2.3、A8.3.1、A.9.3.1、A.10.1.1)

当社が支給・貸与するＰＣでの情報の取扱いは、以下を遵守しなければならない。

（１）ＰＣの利用者は、ＰＣで機密情報を取り扱う場合には、機密情報を取り扱う許可を情報の管理責任者に申請し、許可を得なければならない。許可を得た機密情報は、万一の漏洩に備え、暗号化等の対策を実施しなければならない。
（３）ＰＣの利用者は、情報の管理責任者の許可無く、機密情報を外部媒体に保管してはならない。
（４）ＰＣの利用者は、機密情報取り扱い後には、不必要となった機密情報を直ちにＰＣと外部媒体から削除しなければならない。

４．１．５　ＰＣの使用場所

(A.6.2.2、A.11.1.5)

当社が支給・貸与するＰＣの利用は、利用を許可した以下の場所のみとする。

（１）当社の事務フロア、会議室。
（２）社外では不特定の他人の目にふれない場所。ただし、覗き見防止フィルターにより覗き見が困難な対策を施すＰＣは除く。

４．１．６　ＰＣの利用者の変更

(A.9.2.1)

当社が支給・貸与するＰＣの利用者を変更する場合は、以下を遵守しなければならない。

（１）ＰＣの利用者は、ＰＣの利用者を無断で変更してはならない。
（２）ＰＣの利用者を変更する場合には、情報セキュリティ担当者に返却しなければならない。

４．１．７　ＰＣの利用上の注意事項

(A.6.2.2、A.7.2.2、A.11.2.9、A.12.4.1、A.16.1.2)

当社が支給・貸与するＰＣの利用にあたり、以下を注意する。

（１）ＰＣの利用者は、社外にＰＣを持ち出す場合、盗難・窃盗に注意し取り扱わなければならない。
（２）ＰＣの利用者は、社外でＰＣを利用する場合、情報の盗み見に注意しなければ

ならない。

（３）ＰＣの利用者は、利用環境を整理整頓すると共に、デスクトップを整理し、クリアスクリーンを心がけなければならない。

（４）ＰＣの利用者は、定期的（１年に一回）に、ＰＣ利用に伴う教育を受講しなければならない。

（５）ＰＣの利用者は、ＰＣ利用に伴う、ＰＣ及びそれに付随する機器の紛失・盗難、また情報漏えい等セキュリティインシデントが発生した場合、『セキュリティインシデント報告・対応規程』に従い報告・対応しなければならない。

（６）ＰＣの利用状況は、情報セキュリティ担当者によってモニタリングされていることに留意していなければならない。

４．２　ＰＣや媒体の取り扱いに関するセキュリティ対策

４．２．１　使用機器に関する遵守事項

(A.8.3.1、A.9.3.1)

（１）利用者は、情報システム部が指定したＰＣや媒体を利用しなければならない。

（２）ＰＣや媒体は、盗難に遭わない様に、また紛失しない様に、利用者が管理を行わなければならない。

４．２．２　ＰＣの修理

(A.8.2.3、A.11.2.5)

（１）ＰＣの修理を依頼する場合は、申請書を提出し、情報セキュリティ担当者を通して修理を依頼しなければならない。

（２）ＰＣ等の修理を依頼する利用者は、機密性の高い情報が保管されていないことを確認した上で修理を依頼しなければならない。

故障の状況により、保管されている情報の確認や保護が実施できない場合には、利用者は、情報セキュリティ担当者から指定された方法にて修理を依頼しなければならない。

４．２．３　媒体の保管

(A.10.1.1、A.11.1.1)

（１）利用者が、機密性の高い情報を媒体に保存する時は、保管された情報に権限のない人がアクセスできないよう、データまたは媒体に対して暗号化を行い、媒体を鍵のかかる場所に保管し、鍵を管理しなければならない。

４．２．４　媒体の移動

(A.8.3.3、A.11.2.5)

（１）利用者は、機密性の高い情報を保管している媒体を、その情報の管理責任者の許可なく社外へ持ち出してはならない。

（２）利用者は、機密性の高い情報を保管している媒体を郵送や宅配便等で送付する場合、セキュリティが保たれた郵送や宅配便等を利用すること。

４．２．５　ＰＣと媒体の再利用および廃棄

(A.8.3.2)

（１）ＰＣまたは媒体の再利用および廃棄を行う場合は、情報セキュリティ担当者に廃棄申請を提出し、指定された方法にて再利用および廃棄処理を行う。

４．３　マルウェア対策

４．３．１　マルウェアやサイバー攻撃に関する教育の受講

(A.7.1.2、A.7.2.2)

当社より支給・貸与するＰＣ、およびシステム、ネットワークの利用にあたっては、以下の教育を受講しなければならない。

（１）ＰＣの利用者は、入社時には、マルウェアやサイバー攻撃に関する教育を受講しなければならない。

（２）ＰＣの利用者は、定期的（1 年に一回）に、マルウェアやサイバー攻撃に関する教育を受講しなければならない。

４．３．２　マルウェア対策ソフトの利用

(A.12.2.1)

当社より支給・貸与するＰＣは、マルウェア対策ソフトにより以下の対策をしなければならない。

（１）ＰＣの利用者は、システム管理者が設定したマルウェア対策ソフトの設定を変更してはならない。

（２）ＰＣの利用者は、ドライブ全体に対する定期スキャンを無効化してはならない。また、やむを得ずスキャンを停止した場合は、できるだけ早く定期スキャンを再開しなければならない。

４．３．３　電子メールやインターネット閲覧を介してのマルウェア被害の防止

(A.12.2.1)

電子メールや、インターネット閲覧による被害を招かないため、以下を遵守しなけれ

ばならない。

（１）ＰＣの利用者は、メールの受信にあたっては、メーラやＷｅｂメール上でスパムメールや迷惑メールを分別する機能を有効にしなければならない。

（２）ＰＣの利用者は、送信元不明（特にフリーメール）のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審だと疑われるメールの添付ファイルは安易に開いてはならない。また、安易にＵＲＬリンクをクリックしてはならない。不審だと疑われるメールを受信した場合は、即座に情報セキュリティ担当者に報告しなければならない。

（３）ＰＣの利用者は、ファイルを添付してメールを送信する場合、当該ファイルのマルウェア感染が無いことをマルウェア対策ソフトにて確認後、メールを送信しなければならない。

（４）インターネット閲覧によるマルウェア感染を防ぐ為に、ＰＣの利用者は、業務上関係のないサイトの閲覧をしてはならない。

４．３．４　マルウェアに感染した場合、または感染したと疑われる場合

(A.16.1.2、A.16.1.5、A.16.1.7)

マルウェアに感染、もしくは感染が疑われる場合は、利用者は以下を遵守しなければならない。

（１）ＰＣの利用者は、以下の症状などが見受けられた場合には、情報セキュリティ担当者に報告し、対応方法の指示を受け、対応しなければならない。

・マルウェア付のメールが送られたとの連絡が取引先などからあった。

・メールの添付ファイルを開いたが、何も表示されなかった。

・インターネットのサイトを閲覧中に表示される広告などの表示を消すことができなくなった。

（２）ＰＣの利用者は、有線ＬＡＮ接続のＰＣはネットワークケーブルを外し、無線ＬＡＮ接続のＰＣは無線ＬＡＮ機能をＯＦＦにしなければならない。

（３）ＰＣの利用者は、情報セキュリティ担当者の指示に従って、マルウェア駆除をしなければならない。

（４）ＰＣの利用者は、マルウェア被害の影響範囲が社外にまで至っている可能性が認められる場合、その影響について、情報セキュリティ担当者に報告しなければならない。

４．４　電子メール利用におけるセキュリティ対策

４．４．１　電子メールサービス利用端末機器のセキュリティ

(A.9.4.2、A.12.6.2)

（１）電子メールの利用にあたっては、情報システム部が指定した電子メールソフト

ウェアを用いなければならない。また、情報システム部の指示に従い、当該ソフトウェアを最新の状態に保たなければならない。

（２）電子メールの利用者は、電子メールソフトウェアにパスワードを保存してはならない。電子メールソフトウェア起動時にユーザ認証を必要とする設定にしなければならない。

４．４．２　電子メールで送受信される情報の保護

(A.10.1.1、A.13.2.3)

（１）電子メールの利用者は、当社の事業に関わる情報や、顧客・従業員の個人情報などの機密情報をメールにて送受信する場合は、機密情報の内容に応じて暗号化、電子署名などの処置を施さなければならない。

（２）電子メールの利用者は、電子メールの送信にあたっては、送信先のメールアドレスに間違いがないか、確認の上送信しなければならない。

（３）当社のセミナー案内や製品紹介メールなどのように電子メールで同報送信する場合は、送信先メールアドレスが受信者に閲覧できないよう、BCC を利用しなければならない。また、広告メール等の送信にあたっては、法律を遵守しなければならない。

（４）電子メールの利用者は、電子メールを社外の個人的なメールアドレスに転送する場合は、情報セキュリティ担当者に申請をし、許可を得なければならない。

４．４．３　電子メールサービスとネットワーク保護

(A.9.3.1、A.12.2.1、A.13.1.2、A.13.2.2、A.13.2.3)

（１）電子メールの利用者は、業務目的以外に電子メールサービスを利用してはならない。

（２）電子メールの利用者は、スパムメールを受信した場合は、これを転送してはならない。

（３）電子メールの利用者は、社外のメーリングリストに参加する場合は、当該メーリングリストの信頼性、および業務への必要性を充分考慮した上で参加しなければならない。また、参加意義の無くなった場合は、直ちに脱退しなくてはならない。また公序良俗に反する発言をしてはならない。

（４）電子メールの利用者は、電子メールの送信にあたっては、添付するファイルの容量を考慮しなければならない。規定容量以上のファイルを送信せざるを得ない場合は、情報セキュリティ担当者にて指定されたファイル共有サイト・ファイル転送サイトを利用しなければならない。

（５）電子メールの利用者は、その他、無用な電子メールを送受信することにより、ネットワークに負荷をかけてはならない。また、電子メールはテキスト形式で

送信するよう設定しなければならない。

４．５　Ｗｅｂサービス利用におけるセキュリティ対策

４．５．１　Ｗｅｂブラウザ利用端末機器のセキュリティ

(A.9.1.2、A.9.3.1、A.12.6.1)

（１）利用者は、Ｗｅｂブラウザの利用にあたって、情報システム部が指定したＷｅｂブラウザを用いなければならない。また、情報システム部の指示に従い、当該ソフトウェアを最新の状態に保たなければならない。

（２）利用者は、Ｗｅｂブラウザの利用にあたって、情報セキュリティ担当者が指定したＷｅｂブラウザの設定を施さなければならない。

（３）利用者は、社内からインターネットにアクセスするときは、必ず情報セキュリティ担当者が指定するＰｒｏｘｙサーバを使用しなければならない。

４．５．２　Ｗｅｂブラウザの利用

(A.9.1.2、A.9.3.1、A.12.2.1、A.12.6.2、A.18.1.1)

（１）利用者は、社内及びインターネット上のＷｅｂサーバへのアクセスは、業務上必要な場合のみ利用することができる。

（２）利用者は、ＵＲＬリンクをクリックするとき、リンク先のＵＲＬを確認してからクリックしなければならない。この場合、リンク先が、信頼できないＵＲＬである場合は、クリックしてはならない。また、バナー広告についても同様で、業務上必要のないバナー広告はクリックしてはならない。

（３）利用者は、業務上不必要なファイルやソフトウェア、不審なファイルなどをダウンロードしてはならない。

（４）利用者は、署名の無いあるいは信頼できないサイトの ActiveX、Java、JavaScript、VBScript などのコードは実行してはならない。

（５）業務と関連の無い Web メールを利用してメールの送受信を行ってはならない。

（６）利用者は、社内外のＷｅｂサーバに対して、攻撃等不正なアクセスを行ってはならない。また、攻撃や不正なアクセスを目的として社内外のシステムを利用してはならない。

４．５．３　Ｗｅｂサーバの利用

(A.9.3.1、A.13.2.2)

（１）利用者の情報の発信（掲示板、ＳＮＳなどへの書き込み）に関しては、部門長が業務上必要と認めた場合のみ許可される。このとき、情報の正確性を確保し、必要最小限の範囲で発信しなければならない。また、下記に該当する情報の発信は禁止する。また、情報の閲覧に関しても同様とする。

- 著作権、商標、肖像権を侵害するおそれのあるもの
- プライバシーを侵害するおそれのあるもの
- 他者の社会的評価にかかわる問題に関するもの
- 他者の名誉・信用を傷つけるおそれのあるもの
- 会社の信用・品位を傷つけるおそれのあるもの
- 性的な画像や文章に該当するおそれのあるもの
- 不正アクセスを助長するおそれのあるもの
- 差別的なもの
- 虚偽のもの
- 社内の機密情報
- その他公序良俗に反するおそれのあるもの

（２）利用者は、情報セキュリティ担当者の許可なく、インターネット上のサービス、たとえば、ファイル共有サイトやファイル交換サイトを通じて、他社とファイルを送受信するサービスなどを利用してはならない。

４．５．４　アクセス制御されたＷｅｂサイトの閲覧に関して

(A.9.4.2、A.11.1.5)

（１）利用者は、パスワードによってアクセス制御されたＷｅｂサイトの閲覧において、パスワードをＷｅｂブラウザに記憶させる設定を行ってはならない。

（２）利用者は、アクセス制御された社内Ｗｅｂサイトの閲覧時に離席、または閲覧しなくなった場合は必ず、Ｗｅｂブラウザを終了させるか、ＯＳのパスワード付スクリーンロックを実施しなければならない。

４．５．５　Ｗｅｂサイトの閲覧許可

(A.9.1.2)

（１）ＵＲＬフィルタリングにより業務上必要とされるサイトが閲覧できない場合、利用者は、情報セキュリティ担当者に申請し、許可を得た場合のみ、閲覧できるものとする。

４．６　ネットワークの利用

４．６．１　社内ネットワーク及びインターネットの業務目的以外の利用禁止

(A.9.1.2、A.9.3.1、A.9.4.1)

（１）社内ネットワークは、会社の情報資産であり、電子メールやＷｅｂサイトの利用などにおいて、業務目的以外の使用を禁止する。インターネットの利用についても同様である。

（２）情報セキュリティ委員会の許可無く、社内ネットワーク上に、電子メールサー

バや、Ｗｅｂサーバ、ＦＴＰサーバなどを構築してはならない。

（３）他人の利用者ＩＤを用いて、社内ネットワーク及び、社外のネットワーク、インターネット上のサイトへアクセスしてはならない。

（４）利用者は、故意もしくは不注意を問わず、社内ネットワーク及び社外ネットワーク、インターネット上のサーバに対して、許可されたアクセス権限以上のアクセスを行ってはならない。

４．６．２　社内ネットワークで利用可能なサービス

(A.9.3.1、A.9.4.1、A.9.4.2、A.9.4.3、A.10.1.1、A.13.1.2)

（１）業務システム（人事、経営、経理、交通費管理、受発注システム、イントラネットサーバなど）へのアクセスは、許可された利用者以外利用してはならない。

（２）機密情報をネットワークを介して扱う場合は、情報システム部の指示に従い、暗号化、電子署名などの処置を施さなければならない。

（３）利用者は、社内ネットワークにおいて、ネットワークモニターなどの、ネットワーク上を流れるパケットを盗聴できる機器及びソフトウェアを使用してはならない。

（４）利用者は、社内ネットワークサーバへのアクセス用のＩＤ及びパスワード、証明書は適切に管理しなければならない。

４．６．３　社内ネットワークへの接続時の注意事項

(A.6.2.1、A.9.1.2、A.9.3.1、A.12.2.1)

（１）自宅や、他組織のネットワークに接続していたＰＣは、マルウェア対策ソフトを用いて、最新の定義ファイルによりマルウェアチェックを実施し、異常が発見されなかったことを情報セキュリティ担当者が確認した後でなければ、社内ネットワークに接続してはならない。

（２）利用者は、ＩＰアドレスが固定の環境である社内ネットワークの場合、与えられたＩＰアドレス以外のＩＰアドレスを使用してはならない。

（３）利用者は、社内ネットワークに接続中のＰＣを、情報システム部の許可の無いADSL 回線、携帯電話、無線ＬＡＮ（公衆 Wi-Fi スポットなど）、専用線などを利用して、社外のネットワークに接続してはならない。

４．７　リモートアクセスサービス利用時のセキュリティ対策

４．７．１　利用申請

(A.6.2.1、A.6.2.2)

（１）業務上リモートアクセスサービスの利用が必要な者は、部門長の承認を得、情報システム部に申請しなければならない。

４．７．２　使用機器に関する遵守事項

(A.6.2.1、A.9.3.1)

（１）利用者は、社外から社内ネットワークへのアクセスにおいて、情報システム部が指定した機器を利用しなければならない。

（２）利用者は、インターネットから社内ネットワークへの接続手段を、情報セキュリティ委員会の許可を得ることなく設置してはならない。

（３）その他社内ＬＡＮ環境への接続にあたり、利用機器は、本規程に基づいて設定されなければならない。

（４）リモートアクセスで使用するＰＣは、盗難に遭わない様に、また紛失しない様に、利用者が管理を行わなければならない。

４．７．３　物理セキュリティ遵守事項

(A.6.2.1)

（１）リモートアクセスで使用するＰＣや Wi-Fi ルーターは、所有者の目に届く範囲内で管理できるようにし、使用しない時には、セキュリティが確保できる場所に保管しなければならない。

５　運用確認事項

（１）社内で実施される教育の内容を理解する。

（２）メール及びインターネット利用時のリスクを理解する。

（３）社外に情報を持ち出す場合は、その重要度を認識し、適切な管理策が取られていることを確認する。

（４）ＰＣの利用時、マルウェア対策、媒体管理等各種設定および設定が、正しく実施されていることを確認する。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ担当者に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

スマートデバイス利用規程

1.0版

スマートデバイス利用規程

スマートデバイス利用規程

１　趣旨

本規程は、スマートデバイスの利用に伴う、情報の漏えい、改ざん、破壊を防止することを目的とする。

２　対象者

当社の従業員等で業務にスマートデバイスを利用する全ての者。

３　対象システム

当社より支給・貸与されたスマートデバイス（スマートフォン、タブレット)。

４　遵守事項

４．１　スマートデバイスのセキュリティ対策

４．１．１　スマートデバイスの使用

(A.6.2.1)

当社の業務に利用するスマートデバイスは、以下のものでなければならない。

（１）当社が支給・貸与するスマートデバイス

４．１．２　スマートデバイスに導入するソフトウェア

(A.6.2.1　A.12.6.2)

（１）『システム管理規程』で規定されたソフトウェアを導入すること。支給・貸与するスマートデバイスには、それ以外のソフトウェアを導入してはならない。

（２）（１）にて指定したソフトウェア以外で、業務上やむを得ず導入しなければならないソフトウェアは、情報セキュリティ担当者に申請し、許可を得なければならない。

（３）導入したソフトウェアは、各機器のアップデート方法に従って常に最新の状態にしたうえで使用すること。

４．１．３　スマートデバイスの他者への利用の制限

(A8.3.1　A9.2.4　A.9.3.1　A9.4.2　A9.4.3)

（１）利用者は、スマートデバイスのロック機能（パスワード、生体認証など）を有効にし、第三者が無断でスマートデバイスを利用できないようにしなければならない。

（２）ロック機能はシステム管理者が定めた通りに使用し、ロック解除方法が第三者に漏れないようにしなければならない。

（３）社外持出用のスマートデバイスでは、盗難・紛失時の対策として、スマートデバイス本体のロック以外に、外部記憶媒体を利用するときは暗号化などの対策を行わなければならない。

４．１．４　スマートデバイスでの情報の取り扱い

(A.6.2.1)

（１）スマートデバイスで機密情報を取り扱う場合には、情報セキュリティ担当者に申請し、許可を得なければならない。許可を得た機密情報は、万一の漏洩に備え、暗号化等の対策を実施しなければならない。

（２）機密情報取り扱い後には、不必要となった情報を削除し、いつまでも保持してはならない。

４．１．５　社外持ち出し時の注意事項

(A.6.2.1　A.6.2.2　A8.3.1　A8.3.3　A.11.2.6)

（１）スマートデバイスを社外へ持ち出す際には、所定の手続きを行い、情報セキュリティ担当者の許可を得なければならない。

（２）移動時の交通機関や人混みでは、盗難に遭わないよう、適切にスマートデバイスを所持しなければならない。また、紛失対策（ストラップによる固定等）を施さなければならない。

（３）社外でスマートデバイスを使用する際には、盗み見に注意し安全な場所で利用しなければならない。やむを得ず周辺に他者がいる状態で利用する場合には、覗き見防止対策を施すこと（視野角コントロールフィルムや本体に搭載されている同等機能を有効にする）。

（４）紛失防止のため、スマートデバイスは常に手元に置き、放置しないようにすること。

（５）紛失に気付いた場合は、『セキュリティインシデント報告・対応規程』に基づき速やかに対応しなければならない。

４．１．６　スマートデバイスの利用者の変更

(A.9.2.6)

（１）スマートデバイスの利用者を無断で変更してはならない。

（２）利用者の変更が必要な場合には、情報セキュリティ担当者に返却しなければならない。

４．１．７　スマートデバイスの改造

(A.6.2.1)

（１）スマートデバイスのソフトウェア的な改造（ジェイルブレイク、ルート化）を行ってはならない。

４．２ マルウェア対策

４．２．１　マルウェア対策ソフトの利用

(A.6.2.1　A.12.2.1)

（１）利用者は、スマートデバイスに導入されたマルウェア対策ソフトの設定を変更せず、常駐設定にし、ファイルへのアクセスおよび電子メールの受信時には、常時スキャンできる状態で使用しなければならない。

４．２．２　電子メールやインターネット閲覧を介してのマルウェア被害の防止

(A.12.2.1)

（１）メールの受信にあたっては、スパムメールや迷惑メールを分別する機能を有効にしなければならない。

（２）送信元不明のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審だと思われるメールの添付ファイルは開かない、また安易にＵＲＬリンクをクリックしない。不審だと思われるメールを受信した場合は、即座に情報セキュリティ担当者に報告しなければならない。

（３）インターネット閲覧時には、業務上関係のないサイトを閲覧してはならない。

４．２．４　マルウェアに感染した場合、または感染したと疑われる場合

(A.16.1.2)

マルウェア対策ソフトがマルウェアを検知した場合、またマルウェアに感染、もしくは感染が疑われる場合は、利用者は『セキュリティインシデント報告・対応規程』に基づき対応し、以下を遵守すること。

（１）利用者は、感染が疑われる症状が発生した場合には、情報セキュリティ担当者に報告し、対応方法について指示を受けなければならない。

（２）無線通信機能（Wi-Fi、Bluetooth 等）や通信事業者が提供する通信をＯＦＦにしなければならない。

（３）情報セキュリティ担当者の指示に従って、マルウェアを駆除しなければならない。

（４）マルウェア被害の影響範囲が社外にまで至っているかを確認し、影響が確認された場合、情報セキュリティ担当者に報告しなければならない。

４．３　アプリケーション利用におけるセキュリティ対策

４．３．１　利用アプリケーションの制限

(A.6.2.1　A.12.6.2)

（１）情報セキュリティ担当者が許可したアプリケーションのみを使用する。

（２）アプリケーションに不要な権限を与えないように、あらかじめ設定されているアプリケーション毎の権限（電話帳や位置情報へのアクセス）を変更してはならない。

４．４　外部サービス利用におけるセキュリティ対策

４．４．１　クラウドサービスの利用

(A.13.1.2)

（１）クラウドサービスを利用する場合は、情報の重要度に応じて、情報セキュリティ担当者が許可したクラウドサービスを利用する。

４．４．２　SNS サービスの利用

(A.13.2.3)

（１）スマートデバイスで SNS サービスを利用する場合、『SNS 利用規程』を遵守する。

４．５　スマートデバイスの取り扱いに関するセキュリティ対策

４．５．１　スマートデバイスの修理

(A.11.2.7)

（１）当社にて支給・貸与されたスマートデバイスの修理を依頼する場合は、申請書を提出し、情報セキュリティ担当者を通して修理を依頼しなければならない。

（２）スマートデバイス等の修理を依頼する従業員は、機密性の高い情報が読み出し可能な状態で保管されていないことを確認した上で修理を依頼しなければならない。故障の状況により、保管されている情報の確認や保護が実施できない場合には、情報セキュリティ担当者から指定された方法にて修理を依頼しなければならない。

４．５．２　外付け媒体の制限

(A.8.3.1)

（１）スマートデバイスに外付け記憶媒体を装着する場合は、情報セキュリティ担当者に申請し許可を得なければならない。

４．５．３　スマートデバイスと媒体の廃棄

(A.8.3.2　A11.2.7)

（１）業務に使用したスマートデバイスや媒体の廃棄を行う場合は、情報セキュリティ担当者に廃棄申請を提出し、指定された方法にて廃棄処理を行わなければならない。

４．６　ネットワークの利用

４．６．１　社内ネットワークの利用

(A.9.1.2)

（１）スマートデバイスで社内ネットワークへアクセスする場合、情報セキュリティ担当者の許可を得て、定められた方法で接続しなければならない。

（２）社内と社外（通信業者の提供する通信手段）の通信切り替えに注意する。

４．６．２　社外ネットワークの利用

(A.6.2.2　A9.1.2　A13.2.1)

（１）スマートデバイスで社外ネットワークへアクセスする場合、通信業者の提供する通信手段および暗号化された通信手段を利用し、情報セキュリティ担当者が定めた方法でアクセスしなければならない。

（２）やむを得ず、無料 Wi-Fi などセキュリティが確保されているか不明なネットワークを利用する場合は、個人情報・機密情報等を扱わない通信に留めなければならない。

（３）新たな通信手段を用いる必要がある場合、情報セキュリティ担当者に申請し許可を得なければならない。

５　運用確認事項

（１）スマートデバイスを紛失していないか、手元にあることを常に確認する。

（２）ソフトウェアの最新の情報を常に把握し、脆弱性等が発見された場合、情報セキュリティ担当者の指示に従って、許可されたアプリケーションであっても一時利用停止などの措置を取る。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合

がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

SNS 利用規程

1.0 版

SNS 利用規程

SNS 利用規程

１　趣旨

本規程は、社員等が SNS を利用するに際し、企業情報の漏えいを防止すると共に、当社の信用失墜を防止することを目的とする。

２　対象者

当社の社員等で SNS を利用する全ての者。

３　対象システム

Facebook、Line 他、全ての SNS。

４　遵守事項

４．１　業務目的での利用

(A.9.2.1、A.14.1.2、A.18.1.1)

（１）業務を目的に SNS を利用する者は、事前に、利用目的、利用 SNS、作成予定利用アカウント名(作成したアカウント名が異なった場合は、作成後報告のこと)を情報セキュリティ担当者に申請し承認を得ること。

（２）SNS に記述する内容は、公開 Web サーバに記述する公開情報に準ずる。

（３）SNS 利用において、他利用者からのクレーム、中傷、炎上等がある場合は、情報セキュリティ担当者に報告すること。

４．２　業務目的外(私的利用)での利用

(A.9.3.1、A.14.1.2)

（１）社員等が SNS を利用する場合、当社の非公開情報、法律、公序良俗に違反する記載をしてはならない。

（２）社員等が取引先社員と SNS 上で私的に交流する場合、双方の立場をわきまえ、社会人として良識の範囲で交流すること。

（３)社員等は SNS のセキュリティ設定の問題により､SNS のアカウントが乗っ取られ、悪用される可能性のあることに注意すること。

（４）社員等は使用デバイス(PC、スマートフォン、タブレット)と SNS の設定により、使用デバイス上のデータ、写真、位置情報と SNS が自動連携され、自分のプライバシーデータ、写真、位置情報が予期せず公開される可能性のあることに注意すること。

（５）社員等は SNS の予期せぬ設定変更、機能追加によりセキュリティ制限レベルが変わり、情報がより一般に公開される可能性のあることに注意すること。

（６）社員等は SNS 利用において、当社の非公開情報の漏えいの可能性、他利用者からのクレーム、中傷、炎上等により当社の信用失墜がある可能性がある場合は、部門長及び情報セキュリティ委員会に報告すること。

５　運用確認事項

（１）総務部は、SNS 利用に伴う事故、問題等に関する情報を収集し、年に１度以上、事故、問題等発生のリスクを低減するため、SNS 利用に関する教育を実施すること。

（２）総務部は、年に１度以上、社員等の SNS に利用に伴う問題についてのアンケート調査を実施すること

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。