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

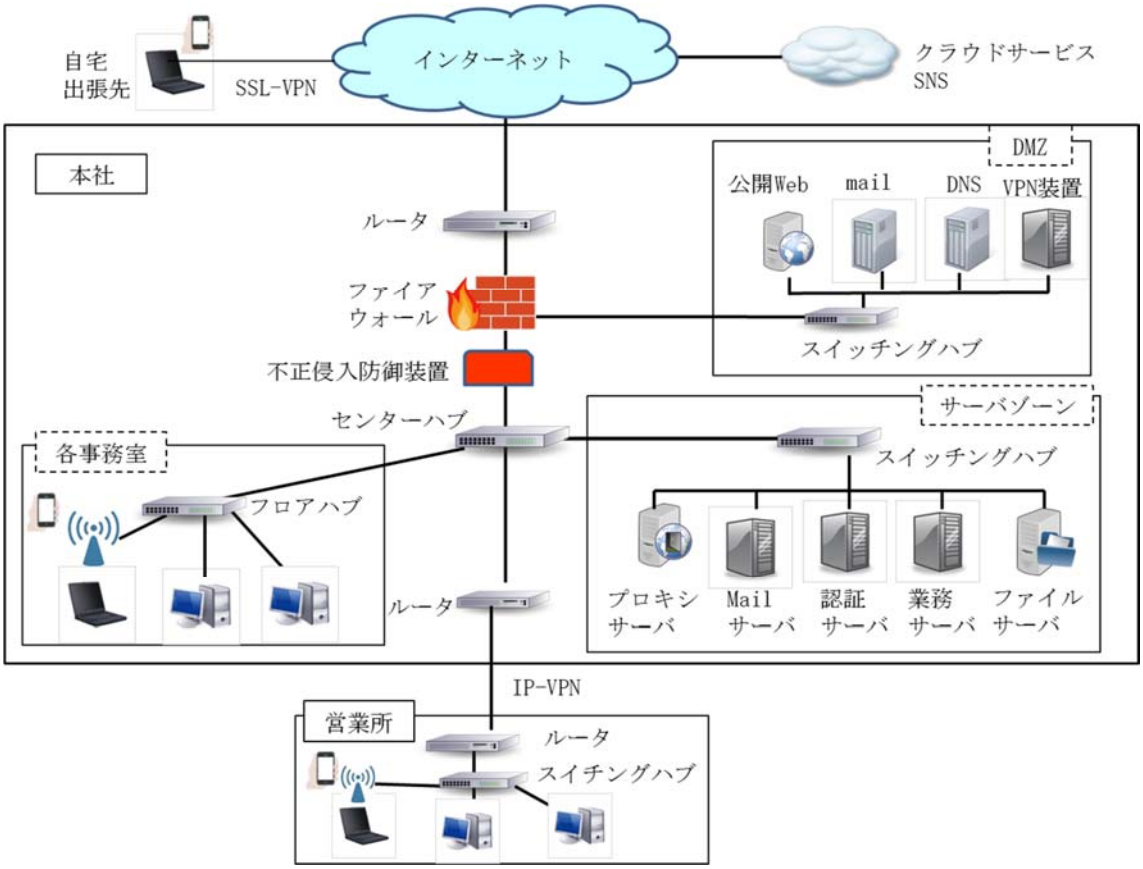
設置するネットワーク機器について以下の管理を行わなければならない。

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。