ネットワーク管理規程

株式会社三重県農協情報センター

改廃履歴

Rev	改 廃 内 容	実 施 日
1.0	初版	2005.04.01
1.1	機構改革に伴う部署変更 第４条	2006.04.01
1.2	利用者ＩＤ申請の様式を明示、添付 第７条	2006.08.01
1.3	第４条(2)　「ネットワーク管理担当者を置く」追記 第８条　一部削除 第21条　特権ＩＤについて、申請か ら保管までを明確化 第34条、第36条　ネットワーク管理 責任者→主管部署	2006.11.01
1.4	第37条　改廃の承認　社長→副社長	2008.10.30
1.5	第４条　業務個別ＬＡＮを削除	2009.07.21
1.6	関連規程に記述の情報セキュリティポリシー対策基準を情報セキュリティ対策規程に変更。	2010.01.08
1.7	規程作成細則実施に伴う書式変更	2010.04.01
1.8	第37条　条文の削除	2010.08.31
1.9	様式１の変更	2011.04.01
2.0	統合ネットワークの追加、LANアクセス権の見直し	2012.06.01
2.1	目次の見直し	2013.08.01
3.0	CSIRT設置に伴う変更	2016.09.01
3.1	様式１のCSIRT設置に伴う検印欄（部長検印）の追加	2016.11.21
3.2	元号改正に伴う改正（様式１）	2019.05.01
3.3	関連規程改正により変更	2020.03.01

Rev	改 廃 内 容	実 施 日
3.4	パスワード有効期限の見直し	2021.12.01

関連規程

情報セキュリティ対策規程：情報セキュリティ委員会
↓
システム運用管理規程：運用部門の長
↓
アクセス制御管理規程：運用部門の長
↓
本規程（ネットワーク管理規程）：運用部門の長

目　　次

ネットワーク管理規程

規程番号　５００４－０００－００－規
制 定 日　２００５年　４月　１日
改 正 日　２０２１年１２月　１日

第　１　章　総則

（目　的）
第　１条　本規程は、当社の円滑な業務推進に資するべく、当社が設置するネットワークおよびネットワークに接続されている機器およびこれらのセキュリティ対策のために必要な事項を定める。

（定　義）
第　２条　用語の定義は次のとおりとする。
（１）社内ネットワークとは、次のネットワークをいう。
① 統合ネットワークとは、ＪＡＳＴＥＭおよび県域システムのネットワークサービスを提供するネットワークをいう。
② 社内ＬＡＮとは、社内に設置された業務遂行のためのＬＡＮで、ＯＡ系セグメントと開発系セグメントおよび共通セグメントをいう。
③ 構内ＶＬＡＮとは、受託業務のサーバ等を接続する受託業務系セグメント（業務の必要性に応じてセグメン細分化）、ＪＡイントラネットの接続ポイントを持つＪＡ接続イントラセグメントをいう。なお、社内ＬＡＮも構内に接続される。
④ インターネットセグメントとは、DMZセグメントとプロバイダ接続ネットワークをいう。

（適用範囲）
第　３条　本規程の適用範囲は、社内ネットワークにて運用・管理される次の項目とする。
（１）情報資産
（２）情報資産の管理業務
（３）情報資産を取り扱う利用者
（４）情報資産を取り扱うためのハードウェア、ソフトウェア、記録媒体

（管理体制）
第　４条　管理体制は次のとおりとする。
（１）ネットワーク管理にかかる主管部署は運用部とし、ネットワーク管理担当者を置く。
① 統合ネットワーク
② 社内ＬＡＮ（ＯＡ系セグメント、開発系セグメント、共通セグメント）
③ 構内ＶＬＡＮ（受託業務系セグメント、ＪＡ接続イントラセグメント）
④ インターネットセグメント（DMZ，プロバイダ）

第　２　章　統合ネットワークの利用

（利用範囲）

第　５条　統合ネットワークの利用範囲は次のとおりとする。
（１）ＪＡＳＴＥＭネットワーク
（２）信用イントラネットシステムネットワーク
（３）管理・経済情報システムネットワーク
（４）ＪＡイントラシステムネットワーク

（ネットワーク認証）
第　６条　統合ネットワークに接続するネットワーク認証管理は次のとおりとする。
（１）専用線は、セキュリティが確保されたネットワークなので認証は行わない。
（２）フレッツ回線は、ＮＴＴの認証サーバーにて回線認証を行う。
（３）ＩＳＤＮ回線は、発番号とＣＨＡＰ認証を行う。

（領域分割）
第　７条　第５条で定めたネットワークで領域を分割する。

（共有ネットワーク）
第　８条　個別に分割されたネットワーク領域間での共有は認めない。
ただし、業務遂行上必要と運用部門の長が認めた場合は、必要な範囲のみ限定して共有を認める。

（利用申請）
第　９条　統合ネットワーク利用の登録・変更・削除申請は、「回線申請依頼書（三重県）」により利用者が申請手続きを行う。

（ネットワーク構成の登録・変更・削除）
第１０条　統合ネットワーク構成の登録・変更・削除作業は、主管部署が行う。

第　３　章　社内ＬＡＮ・構内ＶＬＡＮの利用

（利用者ＩＤ管理運用）
第１１条　社内ＬＡＮ・構内ＶＬＡＮの利用者ＩＤ管理は主管部署が行う。
２　主管部署は登録作業において同じ利用者ＩＤを別の利用者に付与してはならない。
３　主管部署は必要のない利用者ＩＤおよび特権ＩＤがないか毎年５月と１１月に検査し、あれば削除する。

（利用者ＩＤ対象者）
第１２条　雇員、パートタイム社員および派遣社員は、所属部門の情報セキュリティ責任者の判断により業務上必要と認める人に対し付与する。外部委託会社の要員は、外部委託契約上必要な範囲に限定して付与する。

（利用者ＩＤ申請）
第１３条　利用者ＩＤの登録・変更・削除申請は、「ユーザー／グループ登録依頼書（様式１）」により、所属部門の情報セキュリティ責任者の承認を得て、次の手続きにて申請する。
（１）登録は配属部署が申請手続を行う。
（２）異動に伴う変更は、転入部署が申請手続を行う。

（3）退職および派遣業務終了等で不要になった利用者ＩＤの削除は最終所属部署が申請手続を行う。

（利用者ＩＤ登録・変更・削除）
第１４条　利用者ＩＤの登録・変更・削除申請の受付および登録作業は、主管部署が行う。

（利用者ＩＤ使用範囲）
第１５条　利用者ＩＤの使用は、業務上の範囲に限るものとし、私的な利用をしてはならない。

（利用者ＩＤ監視）
第１６条　利用者ＩＤの利用状況については、主管部署にてログ（取引記録）分析により監視を行う。不審な利用が発見された場合は、速やかに運用部門の長へ報告する。

（個人パスワードの管理）
第１７条　使用者はパスワードの管理にあたって、自己のパスワードを他者に知られないよう管理する。

（パスワードの有効期限）
第１８条　パスワードの有効期限は設定しない。ただし、システムにより有効期限の設定に制限がある場合はそれに従う。

（パスワードの初期化）
第１９条　利用者は、パスワードの初期化が必要な事態が発生した場合は、所属部門の情報セキュリティ責任者の承認を得て、主管部署に申請を行う。
２　主管部署はパスワードの初期化を行い、申請者に結果を通知する。また、通知を受けた利用者は速やかに初期化されたパスワードを正式なパスワードに変更して使用する。

（初期パスワードの設定）
第２０条　初期パスワードの管理は主管部署とする。初期設定は主管部署が行う。

（資源へのアクセス権）
第２１条　資源へのアクセス権は次のとおりとする。
（1）社内ＬＡＮ
①　社員
社員には、ＯＡ系セグメントの資源へのアクセス権を付与する。また、開発系セグメントの資源については、開発担当者のみアクセス権を付与する。
②　雇員、パートタイム社員および派遣社員
雇員、パートタイム社員および派遣社員には、所属部門の情報セキュリティ責任者が必要と認めた者に、職務範囲に応じた資源へのアクセス権を付与する。
③　外部委託会社要員
外部委託会社要員には、開発系セグメントに限定してアクセス権を付与する。ただし、所属部門の情報セキュリティ責任者の判断により、職務範囲に応じてＯＡ系セグメントの資源へのアクセス権を付与する。
④　サーバ管理者
サーバ管理者には、管理対象サーバ内の全資源に対してアクセス権を付与する。
（2）構内ＶＬＡＮ
①　社員

社員には、所属部門の情報セキュリティ責任者が必要と認めた者に対し、職務範囲に応じた資源へのアクセス権を付与する。

② 雇員、パートタイム社員および派遣社員

雇員、パートタイム社員および派遣社員には、所属部門の情報セキュリティ責任者が必要と認めた者に対し、職務範囲に応じた資源へのアクセス権を付与する。

③ 外部委託会社要員

外部委託会社要員には、所属部門の情報セキュリティ責任者が必要と認めた者に対し、職務範囲に応じた資源へのアクセス権を付与する。

④ サーバ管理者

サーバ管理者には、管理対象サーバ内の全資源に対してアクセス権を付与する。

（アクセス権の単位）

第２２条　アクセス権は使用者個人、所属部署又はプロジェクト（グループ、チーム）単位で設定する。

（アクセス権の申請）

第２３条　アクセス権の申請は所属部門の情報セキュリティ責任者の許可を得て、主管部署に提出する。

（利用者の異動）

第２４条　部署間で異動が発生した場合は、旧部署での業務引継ぎが完了した時点で、速やかに主管部署にアクセス権の変更を依頼する。

（アクセス権を利用したデータの保護）

第２５条　利用者は利用している情報の公開範囲を認識しファイルサーバ等の適切な場所に保存する。

（特権ＩＤ）

第２６条　特権ＩＤの申請受付および登録作業は、主管部署が行う。業務上必要な最小限の権限を付与することとし、通常業務のＩＤとは別に設定する。

また、主管部署は、登録の記録を保管する。

（ウイルス対策）

第２７条　ウイルス対策にかかる管理は、別途定める「情報セキュリティインシデント対策管理規程」による。

第　４　章　インターネットの利用

（メールアドレスの交付）

第２８条　メールアドレスの交付は次のとおりとする。

（１）社員へのメールアドレスの交付

社員には原則個人ごとにメールアドレスを交付する。

（２）雇員、パートタイム社員および派遣社員へのメールアドレスの交付

原則禁止とする。ただし、所属部門の情報セキュリティ責任者の判断により、業務上必要な場合は交付可能とする。

（３）外部委託会社要員へのメールアドレスの交付

原則禁止とする。ただし、所属部門の情報セキュリティ責任者の判断により、業務上必要な場合は交付可能とする。

（4）その他個人以外に割り当てるメールアドレスの交付

所属部門の情報セキュリティ責任者の判断により、業務上必要な場合は交付する。

（メールアドレスの返還）

第２９条　メールアドレス取得者が異動、退職等になった場合には、該当部門の情報セキュリティ責任者は速やかに主管部署宛に変更（削除）通知をする。

（メールの利用）

第３０条　メール利用にかかる管理は別途定める「電子メール利用規程」による。

（ホームページへのアクセス）

第３１条　ホームページへのアクセスは、業務上の範囲に限るものとし、私的な利用をしてはならない。

（ホームページ閲覧の監視）

第３２条　ホームページアクセスの利用状況はネットワーク管理者および主管部署にて、ログ（閲覧履歴）により監視を行うことができる。

（利用方法）

第３３条　ホームページへのアクセスは、社内ＬＡＮのＯＡ系セグメントへのアクセス権限保有者とする。

（ファイルのダウンロードおよびアップロード）

第３４条　業務上の利用によりホームページ等からファイルの取込み（ダウンロード）等を行う場合には、必ずウイルスチェックを実施する。また、ファイルの登録（アップロード）は、原則禁止する。業務上の利用が必要な場合は、所属部門の情報セキュリティ責任者の承認を得て行う。

（会員登録が必要なページへのアクセス）

第３５条　会員登録が必要なＷｅｂへアクセスする必要が生じた場合は、その都度、所属部門の情報セキュリティ責任者の許可を得る。有料情報へのアクセスは、所属部門の情報セキュリティ責任者の承認を得て行う。

第　５　章　外部接続

（外部からの接続形態）

第３６条　外部接続とは、次の接続形態にて外部より社内ネットワークに接続するものをいう。

（1）リモートメンテナンス

保守契約ベンダーがリモートメンテナンスの為保守対象資源に接続

（2）直接接続

客先より直接社内ネットワークに接続

（3）ＳＯＨＯ接続

専用線、ＩＳＤＮ回線によるダイアルアップ接続

（4）外部常駐先接続
ＰＨＳ、携帯電話、ＩＳＤＮ回線、一般公衆回線によるダイアルアップ接続
（5）モバイル接続
ＰＨＳ、携帯電話、一般公衆回線によるダイアルアップ接続、設置場所不定

（利用範囲）
第３７条　外部接続の使用は、業務上の範囲に限るものとし、私的な利用をしてはならない。

（利用の監視）
第３８条　外部接続の利用状況については、ネットワーク管理者および主管部署にて、ログ（閲覧履歴）により監視を行うことができる。

（利用申請）
第３９条　外部からの接続（アクセス）は、システム環境設置時に利用者が所属部門の情報セキュリティ責任者の承認を得て、主管部署に申請する。

（アクセス方法）
第４０条　外部接続を使用する場合は、必要時間帯以外は接続を切る、ダイヤルアップ時はパスワード認証のほか相手電話番号認証またはコールバック方式とする等のセキュリティ保護手順を使用し接続する。

（利用停止）
第４１条　外部接続が不要または変更になった場合、また保守契約を停止した場合には、速やかに接続不能の措置をとり、主管部署に変更（削除）申請する。