アクセス制御管理規程

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	第８条 改廃を９条へ移動し、８条として監視を挿入	2006.01.20
1.2	第９条　アクセス状況の報告　を追加 様式１「セキュリティ監視報告書」追加	2008.09.01
1.3	第４条～６条、８条、９条のネットワーク管理責任者を情報システム管理責任者に変更 様式１「セキュリティ監視報告書」のネットワーク管理者を情報システム管理責任者に変更	2009.07.21
1.4	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
1.5	規程作成細則実施に伴う書式変更	2010.04.01
1.6	第10条　条文の削除	2010.08.31
2.0	CSIRT 設置に伴う変更	2016.09.01
2.1	元号改正に伴う改正（様式１）	2019.05.01
2.2	システム更改に伴う改正（アクセス制御方針）	2020.03.01
2.3	パスワードの文字数、組み合わせ種類、変更タイミングの見直し	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
↓
本規程（アクセス制御管理規程）：運用部門の長
↓
ネットワーク管理規程：運用部門の長

目　　次

アクセス制御管理規程

規程番号　５００３－０００００－００－規
制 定 日　２００５年　4月　1日
改 正 日　２０２１年１２月　1日

（目　的）

第　１　条　　システムを安全に運用するために、ネットワーク、オペレーティングシステム、情報などへのアクセス制御を管理し、システム利用者の遵守事項を記すことを目的とする。

（適用対象）

第　２　条　　システムを運用する上でアクセス権限を必要とする、ネットワーク、オペレーティングシステム、ファイル等の情報などに適用する。

（方針及び業務上の要求事項）

第　３　条　　運用部門の長は、アクセス制御について次の業務上の要求事項を考慮し文書化しなければならない。

⑴ システムに関連するソフトウェアのセキュリティ要求事項
⑵ 情報の伝達経路及びアクセスの認可に対する方針
⑶ 異なるシステム及びネットワークにおけるアクセス制御と情報分類の方針との整合性
⑷ データ又はサービスへのアクセスの保護に関連する法令及び契約上の義務
⑸ システム利用者のアクセス権限

（システム利用者登録）

第　４　条　　運用部門の長は、システムへのアクセスを許可するための正規のシステム利用者の登録及び削除の手続きについて、次の事項を考慮して定めなければならない。

⑴ システム利用者との対応付けができ、また、システム利用者に自分の行動に責任を負わせることができるように、一意な利用者ＩＤを用いる。グループＩＤの使用は、実施される作業に適切な場合にだけ許可する。
⑵ システム利用者が情報システム又はサービスの使用に対して、所属部門の情報セキュリティ責任者から認可を得ているかを検査する。
⑶ 認可手続が完了するまでシステム利用者にアクセスさせないようにすることを確実にする。
⑷ サービスを使用するために登録されている全てのシステム利用者の正規の記録を維持管理する。
⑸ 職務を変更したシステム利用者、又は組織から離れたシステム利用者のアクセス権を直ちに取り消す。
⑹ 必要のないシステム利用者ＩＤがないか定期的に検査し、あれば削除する。
⑺ 同じシステム利用者ＩＤが別のシステム利用者に発行されないことを確実にする。

（特権管理）

第　５　条　　運用部門の長は、次により特権の割当てを制限し、管理する。

⑴ システム（ＯＳ、ＡＰ、ＤＢなど）に関連した特権と特権が割当てられる必要ある業務区分に関連した特権とを識別する。

⑵個人に対する特権は、使用の必要性に基づき、また、事象ごとに必要とされる場合に限って割当てる。
⑶割当てられた全ての特権の認可手続き及び記録を維持する。
⑷特権は、認可手続きが完了するまで許可しない。
⑸特権は、通常の業務用途に使用される利用者ＩＤとは別の利用者ＩＤに割当てる。

（システム利用者のパスワード管理）

第　６　条　　運用部門の長は、データ及び情報サービスへのアクセスに対する有効な管理を維持するため、システム利用者のアクセス権を見直す正規の手順を、次により定期的に実施する。

⑴システム利用者のアクセス権を定期的に、また、システムおよび運用の変更の都度見直す。
⑵特権の割当てを定期的に検査して、認可されていない特権が取得されていないことを確実にする。

（パスワードの使用）

第　７　条　　システム利用者は、パスワードの選択及び使用に際して、次の事項を遵守する。

⑴パスワードを秘密にしておく。
⑵パスワードを紙に記録して保管しない。ただし、記録がセキュリティを確保して保管される場合は、その限りではない。
⑶システムまたはパスワードに対する危険の兆候が見られる場合は、パスワードを変更する。
⑷最短１０文字（システムでの桁数が１０文字に満たない場合はその最大の桁数）の質の良いパスワードを選択する。質の良いパスワードとは、次の条件を満たす。
①覚えやすい。
②当人の関連情報から他の者が容易に推測できるまたは得られる事項に基づかない。
③連続した同一文字または数字だけ若しくはアルファベットだけの文字列ではない。
⑸パスワードは以下の項目をすべて組み合わせて作成すること。ただし、システムにより組み合わせに制限がある場合はそれに従う。
①アルファベット大文字（ＡからＺ）
②アルファベット小文字（ａからｚ）
③数字（０から９）
④アルファベット以外の文字（！、＄、＃、％等、スペースは除く）
⑹パスワードを他人に知られたときまたはその恐れがあると判断されたときは即座に変更する。
⑺初期パスワードは、最初のログオン時点で変更する。
⑻自動ログオン処理にパスワードを含めない。
⑼個人用のパスワードを共有しない。

（アクセス状況の監視）

第　８　条　　運用部門の長は、利用者が実行している手順が許可されたものだけであるかを確認するため、情報システムに対するアクセス状況を監視する体制を構築する。

⑴考慮すべき監視項目は次のとおり。
①承認されているアクセスの記録（成功したアクセスの記録）
②承認されていないアクセスの記録（失敗したアクセスの記録）

③特権ＩＤによる操作記録
④システム警告または障害の記録
・コンソールの警告または表示メッセージ
・システムログ（エラーメッセージまたは例外的な記録）
・ネットワーク管理システムの警告メッセージ
・ファイアウォールのポリシー違反ログ
・アクセス監視システムの警告ログ

(2)監視結果の検証頻度は関連する情報システムのリスクによって決定し、定期的に検証する。考慮するリスクの要因には次の項目が含まれる。
①本番業務システム（アプリケーション）の重要度
②情報の重要度
③システムに対する不正な侵入行為および誤用に関する過去の事例
④システム相互接続の範囲（特に外部ネットワークとの接続は重視する）

(3)イベントのロギングはセキュリティ関連のイベントを記録し保存する。
監査証跡には、以下の項目を含まなければならない。
①接続が行われたユーザ ID
②ログオンおよびログオフの日時
③端末の ID またはアドレス情報
④システムへのアクセスとして成功したものと、失敗（拒否）したものの記録
⑤データおよびその他の資源へのアクセスに成功したものと、失敗（拒否）したものの記録

(4)ログの採取にあたっては、採取の処理が停止せず、かつ内容に不正な操作が加えられないように適正な管理を行う。
イベントのロギングは、以下の項目を考慮しなければならない。
①ロギング機能が有効に作動しているか（停止していないか）を常時確認する。
②ログ採取の設定内容（記録するログの項目）についての変更の有無を確認する。
③ログファイルの内容に対する不正な編集または削除の有無を確認する。
④ログファイルの容量を超過し、イベントを記録することができない状況となっていないか、また、上書きが行われていないかを確認する。
⑤コンピュータのクロック（内部時計）の時間が正確であるかを確認する。
（ネットワーク環境内の全コンピュータクロックの可能な限り同期が取れていること）

（アクセス状況の報告）

第　９　条　　第８条の監視により、不適切な利用が発見された場合は、「セキュリティ監視報告書」（様式１）により、速やかに運用部門の長へ報告する。

また、運用部門の長は、定められた手順（社内セキュリティ監視手順）に従って、該当者所属部門の情報セキュリティ管理者および該当者に通知する。