# 情報セキュリティ対策規程

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 |
| 2.0 | 第３５条に予防処置、是正処置を追加 | 2005.08.01 |
| 3.0 | 第１条組織体制修正<br>第6条（2）（3）を情報資産取扱規程へ 移動のため削除<br>第6条（2）<br>第１４条（1）一部削除<br>第１５条（1）一部削除<br>第１６条（5）（6）を第１５条へ移動 | 2005.08.15 |
| 4.0 | 第１６条　責任を追加 | 2006.01.20 |
| 5.0 | 機構改革に伴う部署変更<br>第1条　情報セキュリティ管理組織体制図 | 2006.04.01 |
| 6.0 | 第１６条～第３２条<br>　情報システム管理責任者等<br>　→情報システム運用部門 | 2006.11.01 |
| 7.0 | 第３１条<br>　情報システムを運用管理する<br>　→情報システムを開発する | 2007.03.01 |
| 8.0 | 第2条<br>（3）情報セキュリティ委員会事務局を<br>　各部1名→総務部 | 2007.04.01 |
| 9.0 | 第2章1条　情報セキュリティ管理組織<br>　および体制図<br>代表取締役会長を削除<br>第１２章３８条<br>　改廃の決裁　社長→副社長 | 2008.10.30 |
| 10.0 | 第2章　第2条（7）、（8）<br>「ネットワーク管理責任者との兼務は認めない」、「情報システム管理責任者との兼務は認めない」を削除 | 2009.01.26 |
| 11.0 | 機構改革に伴う部署変更<br>第1条　情報セキュリティ管理組織体制図 | 2009.04.01 |
| 12.0 | 役割の見直し、全面見直し | 2009.10.01 |
| 13.0 | 目次第３４条(1)の字句誤り修正、第３条情報セキュリティ管理組織体制の役割(8) ～(10)の見直しおよび第３６条の字句誤り修正 | 2010.01.01 |

| Ｒｅｖ | 改 廃 内 容 | 実 施 日 |
|---|---|---|
| 13.1 | 規程作成細則実施に伴う書式変更 | 2010.04.01 |
| 14.0 | センター長の設置に伴う変更および書式の変更 | 2010.07.01 |
| 15.0 | 役員執行体制の変更に伴う改正および改廃の条文削除 | 2010.08.31 |
| 16.0 | 役員執行体制の変更に伴う改正 | 2011.07.08 |
| 16.1 | 監査部の名称変更 | 2012.04.01 |
| 17.0 | 体制図から企画部を削除 | 2012.04.09 |
| 18.0 | 第３４条（緊急事態への対応）の訓練について見直し | 2013.02.01 |
| 19.0 | 体制図の個人情報問合せ窓口（社外）を推進部から開発部に変更 | 2013.04.01 |
| 20.0 | 情報セキュリティ責任者・情報セキュリティ管理者の役割変更 | 2013.08.01 |
| 21.0 | 第１６条（1）入退出管理からサーバ室を削除 | 2014.03.20 |
| 22.0 | センター長の選任に伴う情報セキュリティ管理組織体制図兼個人情報保護管理組織体制図の改正 | 2014.04.01 |
| 23.0 | ISO/IEC27001:2013(JIS_Q_27001:2014)への移行に伴う見直し | 2014.09.10 |
| 24.0 | ＣＳＩＲＴ設置に伴う変更 | 2016.09.01 |
| 24.1 | 業務分掌の見直し<br>第２条（情報セキュリティ管理組織体制図兼個人情報保護管理組織体制図） | 2020.04.15 |
| 24.2 | 役員執行体制の変更に伴う改正 | 2021.06.30 |
| 24.3 | 第６条（情報の分類）(2) ラベリング<br>厳秘情報を特定できる場合は表記（ラベリング）を省略可とする。 | 2022.09.15 |
| 24.4 | 個人情報保護法改正（令和４年４月１日施行）による個人情報取扱規程の制定に伴う対応（第２条（情報セキュリティ管理組織体制図兼個人情報保護管理組織体制図）の変更） | 2022.04.01 |

| Ｒｅｖ | 改 廃 内 容 | 実　施　日 |
|---|---|---|
| 24.5 | 第２条（情報セキュリティ管理組織体制図兼個人情報保護管理組織体制図）の見直し | 2023.11.01 |
| 25.0 | ＩＳＭＳ規格改訂対応 | 2024.10.01 |

# 目　　次

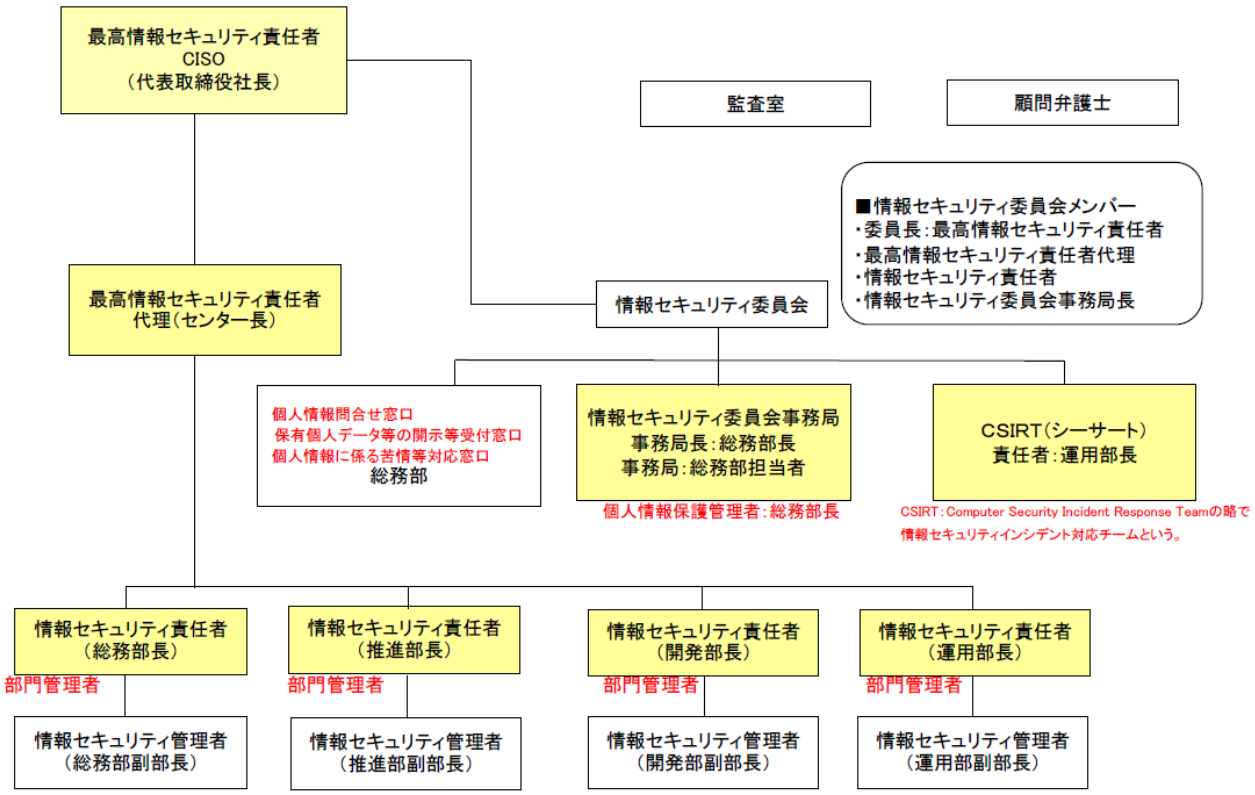
# 情報セキュリティ対策規程

規程番号　０３０１－０００－００－規
制 定 日　２００５年　４月　１日
改 正 日　２０２４年１０月　１日

（目的）
第　１条　本規程は情報セキュリティ基本方針に基づき、株式会社三重県農協情報センター（以下「当社」という。）の情報セキュリティを確保するために必要な組織・体制、情報の管理方法、その他について定めるものである。

（情報セキュリティ管理組織および体制）
第　２条　当社の情報セキュリティ管理組織および体制は、下記のとおりとする。

**情報セキュリティ管理組織体制図兼個人情報保護管理組織体制図**




（情報セキュリティ管理組織体制の役割）
第　３条　情報セキュリティ管理組織体制の役割を下記のとおりとする。

(1)　最高情報セキュリティ責任者（ＣＩＳＯ　：Chief Information Security Officer）
最高情報セキュリティ責任者は、社長がその任にあたり、当社全体の情報セキュリティを確保する責任を負う。また、全社的な視点から率先して情報セキュリティの確保を推進し、このために必要な権限を有する。

(2) 最高情報セキュリティ責任者代理

最高情報セキュリティ責任者代理は、最高情報セキュリティ責任者とともに当社全体の情報セキュリティを確保する責任を負う。また、最高情報セキュリティ責任者不在時等の場合は最高情報セキュリティ責任者に代わり役割を担う。

(3) 情報セキュリティ委員会

情報セキュリティ委員会は最高情報セキュリティ責任者を長とし、最高情報セキュリティ責任者代理、各部の部長、個人情報問合せ窓口責任者および情報セキュリティ委員会事務局長で構成する。情報セキュリティ委員会は、主に以下の役割を担う。

① 情報セキュリティ委員会の年４回以上の開催
② 情報セキュリティポリシーの策定および改訂
③ 情報資産のリスク分析
④ 情報セキュリティポリシーを遵守するために必要な体制の整備と維持
⑤ 情報セキュリティを強化するための推進策の承認
⑥ 情報セキュリティポリシーの遵守状況のレビューと承認
⑦ 情報セキュリティポリシーの啓蒙および教育活動方針の策定と実施
⑧ 内部監査結果の問題点に対する対策方針の策定
⑨ 情報セキュリティに関する事故およびその疑いがあった場合の調査および対策方針の策定
⑩ 関連部門および関連者への協力要請

(4) 情報セキュリティ委員会事務局長および事務局

情報セキュリティ委員会事務局長は、総務部長があたり、事務局は総務部に置く。事務局長および事務局は、主に以下の役割を担う。

① 情報セキュリティ委員会の開催準備と案内の実施
② ポリシー策定作業者の作業進捗管理と原案および改訂案のまとめ
③ 情報セキュリティ委員会への報告窓口および報告文書の取りまとめ
④ 当社のセキュリティ関連窓口
⑤ 情報セキュリティに関する最新情報の収集
⑥ 情報資産に対するセキュリティ対策および改善案の情報セキュリティ委員会への答申
⑦ 情報資産の利用状況の管理
⑧ 情報資産の保管方法および持ち出し手続きの策定
⑨ 情報資産管理手順の遵守状況の監視

(5) 監査室

監査室は、主に以下の役割を担う。

① 情報セキュリティポリシーの遵守状況の定期的な内部監査
② 上記以外に情報セキュリティ委員会から進言があった場合の内部監査の実施検討

(6) 情報セキュリティ責任者

情報セキュリティ責任者は、各部の部長とし、情報セキュリティ委員会の指示を受けて自部門における情報セキュリティポリシーの遵守および情報セキュリティを確保する責任を負い、主に以下の役割を担う。

① 自部門の情報セキュリティ遵守状況の把握と情報セキュリティ委員会への報告

| | |
|---|---|
| | ② 自部門の入退出管理など物理的なセキュリティ管理の実施<br>③ 自部門の従業員等に対するセキュリティ意識の啓蒙<br>④ 情報セキュリティ管理者の任命<br>⑤ 情報資産の利用権限の承認<br>⑥ 情報セキュリティ委員会からの要請への協力 |
| (7) | 情報セキュリティ管理者<br>情報セキュリティ管理者は、情報セキュリティ責任者が自部門の副部長から１名を任命する。情報セキュリティ管理者は、主に以下の役割を担う。<br>① 情報資産の取扱いに関する記録の適正な保管<br>② 情報セキュリティ委員会または情報セキュリティ責任者への情報セキュリティに関する事故およびその疑いの報告<br>③ 情報セキュリティ委員会からの要請への協力<br>④ 情報セキュリティに関する最新情報の収集 |
| （8） | ＣＳＩＲＴ責任者およびＣＳＩＲＴ<br>（ＣＳＩＲＴ：Computer Security Incident Response Team)<br>ＣＳＩＲＴは情報セキュリティ委員会の専門部会として設置する。ＣＳＩＲＴ責任者は、運用部門の長があたり、ＣＳＩＲＴは責任者のほか技術者および事務局員で構成する。ＣＳＩＲＴは主に以下の役割を担う。<br>① 情報システムに対する「故意」や「攻撃」によるインシデントについて一元的に対応する。<br>② インシデント発生を予防・抑制・検知するための事前対策を実施する。<br>③ インシデント発生時には、被害を極限化するための緊急対策を実施する。<br>④ インシデント収束後は、早期復旧をはかり、再発防止策を実施する。<br>⑤ 情報セキュリティに関する最新情報を収集する。<br>⑥ 情報セキュリティ対策および改善案を情報セキュリティ委員会へ答申する。<br>⑦ 標的型攻撃等サイバー攻撃に備えた情報セキュリティ教育を実施する。 |

(兼任に関する規定)

第　４条　役割の兼任は、特に定められている場合を除き認める。ただし、情報セキュリティ委員会に報告し、兼任に問題がないことを確認しなければならない。

(情報利用者)

第　５条　情報利用者とは、当社の情報資産を取り扱う役員や就業規則で規定されている従業員および外部委託契約を締結した企業の要員のことをいい、主に以下の役割を担う。

| | |
|---|---|
| (1) | 情報セキュリティポリシーおよびそれに付随する関連規程類に定められた規程の遵守 |
| (2) | 情報セキュリティ委員会からの要請への協力 |
| (3) | 情報セキュリティに関する事故およびその疑いがある場合の情報セキュリティ委員会、情報セキュリティ責任者または情報セキュリティ管理者への報告 |

(情報の分類)

第　６条　情報利用者は、定められた基準に従って情報を分類し、管理しなければならない。その場合、情報利用者にわかりやすいように分類区分を表記しなければならない。

2　当社で取り扱う情報は、原則として社外秘として扱わなければならない。また、下記に該当すると判断される場合、厳秘情報として分類しなければならない。

| |
|---|
| (1)　情報の重要度の定義<br>【厳秘情報】<br>社外に漏洩した場合に当社に極めて重大な影響または損害が生ずる恐れがあり、特定の関係者のみに開示される下記のような秘密情報を指す。<br>①　個人情報にあたる顧客情報<br>②　顧客団体の経営情報<br>③　自社の経営機密情報<br>④　社員情報<br>【社外秘情報】<br>厳秘情報以外の全ての情報を指す。 |
| (2)　ラベリング<br>厳秘情報については、表記（ラベリング）しなければならない。ただし、<br>情報資産の管理台帳や管理システムの棚卸機能等により、厳秘情報を特定できる場合は表記（ラベリング）を省略することができる。 |

(情報の管理方針)

第　7条　情報管理は、以下の方針に基づき行う。

| |
|---|
| (1)　情報の管理責任<br>情報の管理責任は、当該情報を主管する部門が有する。<br>なお、個人が作成中の文書および電子メール等の管理責任が定められていない情報（個人管理情報）は、個人の責任において適切に管理しなければならない。 |
| (2)　情報の取扱基準<br>情報セキュリティ委員会は、情報資産の保管・持出・複写・廃棄等、その取扱について、具体的な基準を定め、情報利用者に周知徹底しなければならない。 |
| (3)　情報の管理簿<br>情報セキュリティ管理者は、重要な情報については自部門の情報の管理簿（情報資産管理台帳）を作成し、管理しなければならない。情報セキュリティ管理者は、関連する部門の協力のもと、少なくとも年１回、管理している情報が管理簿と一致しているかどうかを確認し情報セキュリティ委員会へ報告しなければならない。 |
| (4)　プロジェクトにおける情報管理<br>各委員会など部門横断的なプロジェクトにおいては、各プロジェクトの特性に応じたリスクを考慮したうえで、適切に情報セキュリティを管理し、組み入れなければならない。 |

(個人情報の保護)

第　8条　個人情報とは、個人に関する情報であり、氏名および生年月日その他により個人を識別できるものをいい、情報利用者は、個人情報を取り扱う場合、個人情報保護マネジメントシステムに従い適切に保護しなければならない。

(雇用における機密保持契約)

第　9条　総務部は、従業員の採用にあたって、情報セキュリティに対する責任を説明し、雇用条件の一部として機密保持の誓約書に署名を求めなければならない。

(情報利用者の権利と義務)

第１０条　情報利用者は、職務内容に応じて必要な情報資産を利用する権利を有する。また、情報セキュリティポリシーおよび関連規程を遵守する義務を負う。

(利用権限の承認)

第１１条　情報セキュリティ管理者は、情報利用者に情報資産の利用が必要となった場合や利用権限の変更を行う場合など、速やかに当該システムの管理部署へ申請し承認を得なければならない。また、情報利用者の退職および異動による職務内容の変更があった場合には、速やかに利用権限の抹消あるいは変更をしなければならない。

(退職時の情報資産の返還)

第１２条　情報利用者は、退職する場合、業務で利用していた当社に関連するすべての情報資産を速やかに情報セキュリティ責任者に返還しなければならない。また、退職後の秘密保持に関する誓約書に署名しなければならない。

(情報利用者への教育)

第１３条　情報セキュリティ委員会は、情報利用者に対して情報セキュリティポリシーや情報セキュリティ等に関する教育を行わなければならない。

| |
|---|
| (1)　教育計画の立案<br>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関する教育体制とスケジュールを含めた教育計画を立案しなければならない。 |
| (2)　教育の実施<br>情報セキュリティ委員会は、教育計画に基づいて情報利用者に対する情報セキュリティポリシー教育を実施しなければならない。情報利用者は正当な理由なく定められた教育の受講を拒否してはならない。 |
| (3)　教育の記録<br>情報セキュリティ委員会は、情報利用者に対するセキュリティ教育の実施結果を記録し、保管しなければならない。 |
| (4)　教育の見直し<br>情報セキュリティ委員会は、セキュリティ教育の実施状況やセキュリティ事故状況および最新技術動向などを参考とし、定期的にセキュリティ教育の計画を見直さなければならない。 |

(セキュリティ事件・事故等の対応)

第１４条　セキュリティ事件・事故等の対応は、速やかに行わなければならない。

| |
|---|
| (1)　報告ルールの策定<br>情報セキュリティ委員会は、情報セキュリティに関連する事件・事故および不適切な行為、あるいは誤動作等による障害が発生した場合の報告ルールを定めなけ |

| | |
|---|---|
| | ればならない。 |
| (2) | 報告の義務<br>情報セキュリティに関連する事件・事故および不適切な行為あるいは誤動作による障害を発見した者は、定められた手順に従って速やかに報告しなければならない。 |
| (3) | 再発防止策<br>情報セキュリティ委員会は、損害や影響が大きいセキュリティ事件・事故あるいは誤動作による障害が発生した場合、速やかに原因分析および対策の策定を実施し、再発させないよう情報利用者に周知徹底させなければならない。 |

（外部委託 ）

第１５条　情報セキュリティ委員会は、当社以外の者に業務を委託する（以下「外部委託」という。）際には、情報セキュリティが損なわれないために、外部委託に関するルールを定めなければならない。

| | |
|---|---|
| (1) | 外部委託先の選定<br>業務委託部門は、外部委託先の選定においては、外部委託先として適切かどうかの判断をしなければならない。 |
| (2) | 外部委託契約の締結<br>業務委託部門は、守秘義務および損害賠償や監査権限などのセキュリティ関連事項が記載された契約を締結しなければならない。 |
| (3) | 外部委託先との情報共有<br>業務委託部門は、外部委託先に提供する情報資産を業務遂行にとって必要最小限の範囲に限定し、必要に応じて、提供した情報資産の一覧を外部委託先との双方で適切な対策を講じて管理しなければならない。また、双方が提供した情報資産は、外部委託業務完了時に委託時の契約に基づいて返却または破棄しなければならない。 |
| (4) | 外部委託先の管理<br>業務委託部門は、外部委託先のセキュリティ遵守状況を確認し、状況に応じて改善を求めなければならない。 |

（情報資産の保管や設置場所のセキュリティ）

第１６条　情報セキュリティ責任者は、当社で取り扱う情報資産の保管や設置場所については、火災・水害・地震等の災害による被害を受けにくい環境で、かつ一般の人が容易に立ち入りできない等の安全性を十分考慮しなければならない。

| | |
|---|---|
| (1) | 入退出管理<br>情報セキュリティ責任者は、当社の情報資産を保護するために建物、事務所およびマシン室などへの入退出者の確認を可能にしなければならない。<br>① 入退出者の管理と承認<br>全社のデータを保管する施設や設備および事務所等において、情報資産が適切に保管され、かつ安全が確保されている領域（以下「安全領域」という。）内に入室する者は、定められた情報セキュリティ責任者の承認を事前に得なければならない。 |

| |
|---|
| ② 入退出者の確認と記録<br>安全領域に入室する者は、入退カードや身分証明を着用して入室しなければならない。また、必要に応じて入退出を記録し、情報セキュリティ責任者はこれを一定期間保管しなければならない。<br>③ 共同利用している場合<br>情報セキュリティ責任者は、安全領域を他の組織（社外を含む）と共同利用する場合、その組織の入退出管理が本規程と同等以上になるようにその組織または安全領域を管理する組織に依頼しなければならない。 |
| (2) 安全領域のセキュリティ<br>情報セキュリティ責任者は、安全領域内で作業する場合のセキュリティを確保するために、以下の措置を講じなければならない。<br>① 災害によるコンピュータ機器等の情報資産の被害を最小限にするために、室内におかれる物品および機器等を整理しなければならない。<br>② 利用権限のない者が、安全領域の用途を容易に判断できないように、表示を必要最小限にしなければならない。<br>③ 安全領域には、必要のない危険物および可燃物を設置・保管してはならない。<br>④ 安全領域に設置されているコンピュータ機器や専用マシン等について権限のないものがアクセスまたは不正操作できないように安全管理を徹底しなければならない。 |
| (3) キャビネットの管理<br>情報セキュリティ責任者は、情報資産を管理するキャビネットに対して適切な管理策を講じなければならない。特に厳秘情報をキャビネットに保管する場合には施錠しなければならない。 |
| (4) 受渡し場所の設置<br>情報セキュリティ責任者は、セキュリティを確保するため、配送業者等によって配達される物品の受渡し場所を設置するなど、適切な管理策を講じなければならない。 |
| (5) クリアデスク、クリアスクリーン<br>① 情報利用者は、各自の机上に厳秘情報や社外秘情報等の重要書類を放置してはならない。<br>② 情報利用者は、帰宅時や外出時等、長時間机から離れる場合には、上記重要書類、個人使用ＰＣ等は机の中およびキャビネットに施錠して保管しなければならない。ただし、ＰＣ等は盗難防止用のワイヤーの使用を認める。<br>③ 情報利用者は、各自使用するコンソール端末やクライアントＰＣについては、パスワード付スクリーンセーバ等の設定をしなければならない。 |
| (6) 資産の移動<br>情報利用者は、組織に属する装置、情報もしくはソフトウェア等を情報セキュリティ管理者の承認を得ずに、移動してはならない。 |

（コンピュータ機器のセキュリティ）

第１７条　情報システムを運用管理する部門は、コンピュータ機器の設置場所におけるセキュリティ

を高めるための措置を講じなければならない。

| |
|---|
| (1)　装置の設置および保護<br>①　機器の設置<br>情報システムで使用される機器は、作業領域への不必要なアクセスが最小限に抑えられる場所に設置しなければならない。<br>②　予備機器・保守・保全<br>情報システムの重要性およびコスト等を考慮し、適切な設備（装置の二重化等）を検討しければならない。また、設備に対する保守要件を明確化しなければならない。 |
| (2)　電源の確保<br>停電等の災害時に当社のコンピュータ機器が安全停止できる時間の供給が可能な電源・空調設備等を持たせなければならない。 |
| (3)　ケーブルのセキュリティ<br>当社の業務で使用される電源ケーブルおよび通信ケーブルを損傷から保護するために適切な対策を講じなければならない。 |
| (4)　機器管理・廃棄<br>当社の情報システムで使用される機器等の保守、持ち出し、廃棄および再利用の手順を策定しなければならない。 |

(各種設備管理)

第１８条　情報セキュリティ責任者は、当社の情報資産に関わる電源・空調・給排水・防災・防犯および監視関連の設備は、円滑な運用を確保するため、適切に管理しなければならない。

(情報処理設備管理)

第１９条　情報システムを運用管理する部門は、セキュリティ維持と当社の情報処理設備を正しく安全に運用するために必要な方策を実施しなければならない。また、その管理状況を定期的に確認し、必要に応じて改善に努めなければならない。

| |
|---|
| (1)　操作手順整備<br>情報処理設備のセキュリティを保った運用のために必要な操作手順書を整備しなければならない。 |
| (2)　運用変更管理<br>情報処理施設およびシステムに対する変更について手順を定め、適切に管理しなければならない。 |
| (3)　セキュリティ事件・事故管理手順<br>セキュリティ事件・事故に対して効果的な対処を行うために、監査証跡やログ等のデータを収集するための手順を明確にしなければならない。 |
| (4)　職務の分離<br>不注意または故意によるシステムの誤用のリスクを低減するために職務および責任領域を分離しなければならない。 |
| (5)　情報システムの開発環境の整備<br>開発部門の協力の下、本番システムに影響を与えない開発環境やテスト環境を整備しなければならない。 |

| | |
|---|---|
| (6) | システムの受け入れ<br>開発部門の協力の下、システム障害のリスクを最小限にするために記憶容量や処理能力を予測しなければならない。また、新しい情報システム、バージョンアップ版等のシステムを受け入れる際の手順を確立しなければならない。 |
| (7) | コンピュータウイルス対策<br>コンピュータウイルスによる感染を防止するために、以下の対策を実施しなければならない。<br>① 当社の情報システムにおけるコンピュータウイルス対策手順書の策定<br>② 最新のウイルスへの迅速な対応<br>③ 対策実施状況のチェックおよび情報セキュリティ委員会への結果報告<br>④ ウイルス検出時の速やかな回復措置と再発防止策の策定と実施 |
| (8) | 購入ソフトウェアの保守<br>使用している購入ソフトウェアに対してセキュリティに関連する修正情報が製造販売元から報告された場合は、定められた手順に従って適用しなければならない。 |
| (9) | 情報のバックアップ<br>極めて重要と判断された情報やソフトウェア等のバックアップは、定期的に取得しなければならない。かつ、バックアップされた媒体は安全な場所や施設等に保管しなければならない。 |
| (10) | 運用の記録<br>適切な情報システムの運用がなされるよう運用担当者に作業記録を作成させなければならない。また、作業記録を確認し、問題やその兆候を発見した場合は適切な対処を施し、速やかに改善に努めなければならない。 |
| (11) | 障害対策<br>情報システムの障害が業務に与える影響を最小限にする為に必要な手順を明確化し、障害や災害からの早期回復および再発防止に努めなければならない。 |
| (12) | 新技術への対応<br>情報技術における最新の情報収集に努め、情報システムおよびネットワークに対する新技術の適用を検討および実施しなければならない。 |

(ネットワークの管理)

第２０条　ネットワークを運用管理する部門は、不注意または故意によるネットワークサービス停止やデータの機密性および完全性等を保護するためにネットワークを支える基盤の保護を確実にするための手順を定めなければならない。

(媒体の取扱に関する管理)

第２１条　情報セキュリティ委員会は、重要文書やシステムに関する文書および取り外し可能な機器の媒体（テープ・ディスク・カセット等）等を損傷、盗難および無許可のアクセスから保護する為、情報の取扱手順を確立しなければならない。

(情報およびソフトウェアの交換に関する管理)

第２２条　情報システムおよびネットワークを運用管理する部門は、組織間で情報を交換する場合、

情報の紛失・改ざんまたは誤用を防止するための手順を確立しなければならない。

| |
|---|
| (1)　情報およびソフトウェアの交換<br>組織間の情報およびソフトウェアの交換をする場合は、適切な管理のための合意を取り交わすこととし、必要に応じて正式な契約としなければならない。また、配送中の媒体等についてもその責任を明確にしなければならない。 |
| (2)　電子メールの管理<br>①　電子メール利用環境の整備<br>情報利用者が業務上必要な場合、適切かつ安全に電子メールを利用できる環境を構築しなければならない。<br>②　電子メール利用のルール<br>情報セキュリティ委員会の承認の下、電子メールを利用する際のルールを確立し、情報利用者に周知しなければならない。<br>③　メールボックスの閲覧<br>情報セキュリティ委員会の承認の下、必要に応じてメールボックスを閲覧し、情報利用者の不正行為の疑義が発生した場合、情報セキュリティ委員会へ報告しなければならない。 |
| (3)　社外向けWebサーバの管理<br>当社の社外向けWebサーバが常時正常かつ安全に稼働する環境を構築しなければならない。 |
| (4)　電話、ファクシミリ等の情報交換時の管理<br>音声/映像の通信設備およびファクシミリを使用して行われる情報交換を保護するために適切な手順を確立しなければならない。 |

(アクセス制御に関する業務上の要求事項)

第２３条　運用部門の長は、アクセス制御について明確に文書化しなければならない。また、情報利用者は、定義されたアクセス制御の内容に従わなければならない。

(情報利用者のアクセス管理)

第２４条　運用部門の長は、正当な権利を持たない者のアクセスを禁止するために、特権ＩＤや一般ユーザＩＤとパスワードが適切に管理されるよう定めなければならない。また、アクセス権を組織が定めた合理的な期間内で定期的な見直しを行わなければならない。

(パスワード使用における注意事項)

第２５条　情報システムを運用管理する部門は、安全なログオン手順を定め、パスワード使用において有効な対話的機能を情報利用者に対して提供しなければならない。

２　情報利用者は、パスワード管理について定められた手順に従って厳格に行わなければならない。

(無人運転装置に対するセキュリティ確保)

第２６条　情報システムを運用管理する部門は、利用者領域にある無人運転の装置に対して適切な保護対策を講じなければならない。

（ネットワークのアクセス制御）

第２７条　ネットワークを運用管理する部門は、内部および外部のネットワークを介したサービスへのアクセスを保護する為、適切な管理策を講じなければならない。

| |
|---|
| (1)　ネットワークサービスの使用時の個別方針<br>ネットワークおよびネットワークサービスの使用に関し、アクセスが許可されるサービスへのアクセスだけを提供する個別対策を講じなければならない。 |
| (2)　指定された接続経路<br>利用者端末とコンピュータサービスをつなぐネットワーク接続経路の管理を行わなければならない。 |
| (3)　外部から接続する利用者の認証<br>外部からの接続を行う際にはユーザ認証を実施しなければならない。 |
| (4)　ノード認証<br>外部への接続を行う際には、認証による管理を実施しなければならない。 |
| (5)　遠隔診断ポート保護<br>保守メンテナンス時における診断ポートへのアクセスに関しセキュリティ確保のため適切な保護を実施しなければならない。 |
| (6)　ネットワーク領域分割<br>認可されていないネットワーク利用者からのアクセスを制御するために、情報サービス、利用者および情報システムのグループ分割（物理的/論理的）等のネットワークの領域の管理を行わなければならない。 |
| (7)　共有ネットワークの制御<br>共有ネットワークにおいて、情報利用者が業務上必要とされるネットワークだけに接続できる環境を提供しなければならない。 |
| (8)　ネットワークサービス使用のセキュリティ<br>サービスを使用しようとする部門に対し、使用するネットワークサービスのセキュリティの特質について十分に説明を受けるよう指導しなければならない。 |

（システムへのアクセス制御）

第２８条　情報システムを運用管理する部門は、許可されない機器へのアクセスを防止するためにアクセス制御に対する手順を定め、情報利用者に周知徹底しなければならない。

| |
|---|
| (1)　コンピュータへのアクセス<br>情報サービスへのアクセスには、適切な認証機能を提供し、情報利用者に一意なＩＤを付与しなければならない。 |
| (2)　システムユーティリティプログラムの使用<br>システムユーティリティプログラムの使用については、システム保守担当者に限定し厳しく管理を行わなければならない。 |
| (3)　端末のタイムアウト機能<br>リスクの高いシステムを利用する端末が活動停止状態にある場合、許可されていないものによるアクセスを防ぐために一定の活動停止時間の経過後その端末に対して遮断させる等の対策を講じなければならない。 |
| (4)　接続時間の制限 |

| |
|---|
| リスクの高い業務システムについては、接続時間を制限させる対策を講じなければならない。 |
| (5) 重要なシステムの隔離<br>重要な情報等が格納されているシステムは専用の隔離された環境に設置しなければならない。 |

(システム使用状況の監視)

第２９条　情報システムを運用管理する部門は、システムや情報処理施設/設備等に対する許可されていない活動を検出するために、証拠となるようなイベントの記録を作成し組織で合意された期間保存しなければならない。また、監査記録の正確性を期すために機器等のクロックは同期を取るようにしなければならない。

(情報システムに対するセキュリティ要件の明確化)

第３０条　情報システムを運用管理する部門は、開発部門の協力の下、情報システムに対するセキュリティ要件を定めなければならない。

(暗号化の管理)

第３１条　情報システムを運用管理する部門は、開発部門の協力の下、必要に応じて情報の機密性を保証する暗号化方法を情報利用者に提供しなければならない。

(情報システムの開発管理)

第３２条　情報システムを開発する部門は、定められた手順に従って情報システムを開発・修正し、情報システムがセキュリティ要件を満たすことを確認しなければならない。また、外部委託先による開発および修正においても、同様のセキュリティ要件や標準開発手順の遵守を可能な限り求めなければならない。

| |
|---|
| (1) 業務用システムのセキュリティ<br>情報システムを開発する部門は、業務用システムにおける、利用者データの消失・変更および誤用を防止するため、入出力データの妥当性確認ほか必要なセキュリティ対策を組み込まなければならない。 |
| (2) 運用ソフトウェアの管理<br>情報システムを運用管理する部門は、運用ソフトウェアおよびプログラムライブラリ等の管理や取扱についてのルールや手順を定めなければならない。 |
| (3) システム試験データの保護<br>情報システムを開発する部門は、テストデータ使用に関する管理や取扱についてのルールや手順を定めなければならない。 |
| (4) ソースライブラリへのアクセス制御<br>情報システムを開発する部門は、ソースライブラリの管理や取扱についてのルールや手順を定めなければならない。 |

(開発および支援プロセスにおけるセキュリティ)

第３３条　情報システムを運用管理する部門は、開発部門の協力の下、オペレーティングシステムやパッケージソフトウェアおよび業務アプリケーションソフトウェアのセキュリティを維持す

るために、変更管理手順を定め、情報システムの変更の実施を厳しく管理しなければならない。

(緊急事態への対応)

第３４条　情報セキュリティ委員会は、情報セキュリティに関連する事故や災害によって情報システムおよびネットワーク、または設備が正常に運用できなくなった状況を想定した対応計画を策定しなければならない。

| | |
|---|---|
| (1) | 脅威インテリジェンスの構築<br>情報セキュリティ委員会は、当社全体の情報セキュリティにおける脅威に関する情報収集およびリスク分析を行い、その結果を基に当社の事業を継続するための脅威インテリジェンスとして緊急時対応計画書を策定しなければならない。 |
| (2) | 緊急時対応計画の訓練<br>緊急時対応計画書に基づき訓練を行わなければならない。また、必要に応じて対応計画を見直さなければならない。 |

(関連する法令の遵守)

第３５条　情報セキュリティ委員会は、関連する法令を情報利用者に遵守させなければならない。

| | |
|---|---|
| (1) | 関連する法令の明確化<br>情報セキュリティ委員会は、関連部門の協力の下、情報システムに関連する法令、規制および契約上の要求事項について明確にしなければならない。 |
| (2) | 遵守策の策定と適用<br>情報セキュリティ委員会は、関連部門の協力の下、情報セキュリティに関連する法令および情報セキュリティに係る知的財産権、または契約上の要求事項を情報利用者に遵守させるための管理策を講じなければならない。購入ソフトウェアについては、ライセンス管理、不正コピー防止など必要な管理を実施しなければならない。 |
| (3) | 証拠の収集<br>情報セキュリティ委員会は、関連部門の協力の下、法的な措置に対処するために十分な証拠を保全しなければならない。 |

(情報セキュリティポリシーの評価および見直し)

第３６条　情報セキュリティ委員会は、情報セキュリティポリシーの有効性および実効性を維持するために、ＰＤＣＡ（Ｐｌａｎ－Ｄｏ－Ｃｈｅｃｋ－Ａｃｔ）サイクルに基づいて情報セキュリティポリシーを定期的に評価し、必要に応じて見直さなければならない。

| | |
|---|---|
| (1) | 情報セキュリティポリシーおよび付随する関連規程類の評価<br>情報セキュリティ委員会は、関連部門の協力のもと、当社における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適切性および有効性を評価しなければならない。また、以下の場合に情報セキュリティに与える影響を調査し、情報セキュリティポリシーおよび付随する関連規程類を再評価しなければならない。<br>① 情報セキュリティに関する外部要件の変化があった場合<br>② 関連する法令の制定および改正があった場合<br>③ 運営組織や業務組織、就業場所に変化があった場合 |

| | |
|---|---|
| | ④ 情報セキュリティ責任者が、取り扱う情報資産の運用に関する不具合を認めた場合<br>⑤ 情報システム運用部門の長が、情報システムおよびネットワークに大規模な変更を認めた場合<br>⑥ 情報セキュリティに関連する事故や犯罪があった場合<br>⑦ 監査の結果、見直しの必要性が指摘された場合<br>なお、評価の記録は文書で保存しなければならない。 |
| (2) | 情報セキュリティポリシーおよび付随する関連規程類の見直し<br>情報セキュリティ委員会は、評価等の結果、情報セキュリティポリシーおよび付随する関連規程類の改訂が必要と判断された場合、当該規程の管理責任者とともに改訂案を策定しなければならない。また、改訂された場合は、その内容を情報利用者に速やかに伝達し、適切な教育を実施しなければならない。 |
| (3) | 予防処置、改善処置<br>情報セキュリティ委員会および情報セキュリティ責任者は、内部監査報告、障害報告、事件・事故報告、その他情報セキュリティポリシー遵守状況など評価分析し、未然防止のため予防処置を、また再発防止のため是正処置を講じなければならない。 |

(適用の例外に対する対応)

第３７条　情報セキュリティポリシーの適用において、例外は原則として認めない。ただし、例外が必要になった場合には、情報セキュリティ委員会がその是非を決定する。

　情報セキュリティ委員会は、その場合においてもリスクを十分に評価し、セキュリティ対策のレベルが下がる場合は必要な対策を講じなければならない。

(違反に対する措置)

第３８条　情報セキュリティ委員会は、情報セキュリティポリシー違反に対し、是正のために必要な措置について定めることができる。

| | |
|---|---|
| (1) | 違反を発見した場合の対応<br>情報セキュリティ責任者は、情報利用者が情報セキュリティポリシーに違反する行為を発見した場合、または行為の報告を受けた場合、当該情報利用者による情報資産の利用を停止させることができる。また、情報セキュリティ責任者は違反内容を速やかに情報セキュリティ委員会に報告しなければならない。 |
| (2) | 違反に対する罰則<br>当社の定める情報セキュリティポリシーおよびそれに付随する関連規程類に違反する行為があった場合は、就業規則等により処罰することがある。また、情報利用者による当該違反について、情報利用者の監督責任者等による監督義務違反が認められる場合には、同様の処分および措置の対象とする。 |