2002 年 11 月 8 日

情報セキュリティ管理規程（モデル）

前文
（前文は、各企業の情報セキュリティポリシーに合わせて記述すること）

第 1 章　総則

（目的）
第 1 条　本規程は、情報資産を経営活動に有効活用するため、全ての役員および従業員に対し、情報セキュリティに関する行動規範を示し、高い情報セキュリティレベルを確保することにより、経営に寄与することを目的とする。

（用語の定義）
第 2 条　本規程で用いる用語の定義は、次のとおりとする。
① 情報セキュリティ担当役員とは、全社情報セキュリティの総括責任者をいう。
② 情報セキュリティ担当とは、情報セキュリティ担当役員のスタッフであり、各本部の情報セキュリティ体制を統括する者をいう。
③ 本部情報セキュリティ担当とは、各本部にあって、情報セキュリティに関し本部長を補佐し、本部内を統括する者をいう。
④ 情報資産とは、情報およびその関連の資産をいい、情報記録媒体、情報利用手段、情報保管手段、情報システム、ネットワークなどを含む。
⑤ 機密情報とは、情報資産の中で、許可した者以外に開示したり、目的外に利用された場合、経営資源としての価値を損なう恐れのある情報をいう。
⑥ 情報セキュリティ管理者とは、部や課の組織にあって、情報セキュリティの確保に責任がある者をいう。
⑦ 情報管理者とは、部や課の組織にあって、情報管理に責任がある者をいう。
⑧ 情報リスク管理者とは、部や課の組織にあって、情報リスクに責任がある者をいう。

（対象情報）
第 3 条　本規程の対象情報は、記録媒体を問わず、社内に保管する全ての電子化情報、非電子化情報とし、業務に関する記憶情報を含む。

（保護対象）
第 4 条　本規程の保護対象は、情報のみに限らず、記録媒体、保管手段および情報システム等の全てとする。

（適用範囲）
第 5 条　本規程は、役員、監査役、従業員および元従業員に適用する。

（情報セキュリティの評価）
第 6 条　情報セキュリティを定期的に評価し、適正化を図るものとする。

（規程の改廃）
第 7 条　本規程の施行，変更および廃棄は、情報セキュリティ担当役員が提案し、役員会で承認した後、社長が通達するものとする。

第 2 章　情報セキュリティの保持義務

（情報セキュリティ保持の基本）
第 8 条　情報セキュリティの保持は、日常の経営活動、業務推進、組織運営の一環として取り組む。
2. 情報セキュリティの保持は、全従業員の責務であり、経営資源と同様に組織を通じて管理する。

（目的外利用の禁止）
第 9 条　情報は、定められた目的以外に利用してはならない。
2. 情報資産および情報システムは、私的な目的に利用してはならない。
3. 情報は、非合法な手段による利用、社内規則に違反した利用および社会通念に反する利用をしてはならない。
4. 情報は、提供を強要してはならない。

（情報の開示）
第 10 条　社外へ情報を開示する場合は、情報管理者の許可を受けなければならない。
2. 本規程に定める範囲以外での利用が業務上生じる場合は、事前に情報セキュリティ管理者の許可を得なければならない。
3. 前項の場合の責任は、情報管理者が負うものとする。

（情報の返却･廃棄）
第 11 条　情報は、開示期限を定め、期限内に返却または廃棄しなければならない。
2. 社外に保管する場合は、返却または廃棄の確認を必要とする。

（取引先との契約）
第 12 条　取引先に情報を開示する必要がある場合には､情報開示に関する契約を締結しなければならない。
2. 契約書には、次の各号を明記しなければならない。
① 保管方法
② 複製物の制限
③ 廃棄方法
④ 管理責任者
⑤ 違反時の罰則

（誓約書の提出）
第 13 条　従業員は、入社時に、機密情報の取扱いに関する誓約書に署名しなければならない。
2. 退職する場合は、理由の如何を問わず、退職後も機密情報を開示しないことを誓約し、誓約書に署名しなければならない。

第 3 章　情報セキュリティの管理体制

（情報セキュリティ担当役員）
第 14 条　社長は、情報セキュリティの総括責任者として、情報セキュリティ担当役員を指名する。
2. 情報セキュリティ担当役員は、全社の情報セキュリティを統括管理しその責任を負う。
3. 情報セキュリティ担当役員のもとに情報セキュリティ担当を置き、全社情報セキュリティ管理の運営、各本部での情報セキュリティ管理状態の把握、維持および情報セキュリティ担当役員への報告を行う。

（本部管理体制）
第 15 条　社内の各本部に、本部長が指名した本部情報セキュリティ担当を置く。
2. 本部情報セキュリティ担当は、情報セキュリティ確保のため、本部の管理者を統括しなければならない。
3. 管理者は、情報資産および情報セキュリティの管理を行う。
4. 管理者は、情報リスク管理者と連携をとり、情報セキュリティ管理の充実に努めなければならない。

（プロジェクトにおける管理体制）
第 16 条　プロジェクトにおける情報管理および情報セキュリティ管理は、プロジェクトリーダの責務とする。

（共同プロジェクトにおける原則）
第 17 条　外部との共同プロジェクトにおいては、社内プロジェクトと同様に、プロジェクトリーダが情報管理および情報セキュリティ管理の責任を負う。
2. 当社従業員がプロジェクトリーダを担当しない場合は、当該プロジェクト内で当社の最高責任者が、当社関連の情報管理および情報セキュリティ管理を担当する。
3. プロジェクトリーダは、当該プロジェクト推進に必要な情報セキュリティ管理規程を基に、参加企業の了解を得るものとする。また、当該企業は、プロジェクトリーダに情報セキュリティ管理の権限を委譲する。

第 4 章　機密情報の管理

（機密情報）
第 18 条　当社の情報資産の中で、許可した者以外に開示したり、目的外に利用された場合、経営資源としての価値を損なう恐れのある情報を機密情報とする。

2. 取引先情報を預かっている場合、取引先が機密情報と指定し、かつ、当社が同意した情報は機密情報として取り扱う。

（機密区分の設定）
第 19 条　当社の情報には、機密区分を設定する。
2. 機密区分は、次の各号とする。
　① 極秘
　② 厳秘
　③ 部外秘
　④ 社外秘
3. 機密区分の付与は、情報管理者が行い、適宜、見直さなければならない。
4. 機密区分の付与および変更にあたっては、関連情報との整合性確保の観点から、別途定める機密区分表に基づき合理的に行う。
5. 情報管理者は、機密区分の変更内容について、部門内と関連部門に周知徹底しなければならない。

（機密区分の表示）
第 20 条　機密区分は、各情報に明示するとともに、有効期限および情報管理責任部門を表示しなければならない。ただし、社外秘はこの限りでない。
2. 電子化情報は、モニター表示時および印刷時に機密区分を表示できるようにしなければならない。

（機密情報の管理）
第 21 条　機密情報は、施錠できる保管庫に保管しなければならない。
2. 機密情報の保管場所は、所在を表示してはならない。
3. 同一ファイル中に異なる機密区分の情報を混在させず、アクセス権限者ごとにファイルを分割しなければならない。
4. やむを得ず混在させる場合は、最も機密レベルの高い区分の管理方法を適用しなければならない。

（機密情報の管理責任者）
第 22 条　機密情報の管理は、情報管理者が兼務するものとする。

（機密情報へのアクセス管理）
第 23 条　機密情報へのアクセス権限は、情報管理者が機密区分に照らして付与するものとする。
2. 機密情報へのアクセス許可は、担当業務に必要な範囲とする。
3. 機密情報については、利用目的を制限するとともに、アクセス権限者を制限する。
4. 機密情報へのアクセス状況については、常にモニターして記録するとともに、定期的に実態を点検しなければならない。
5. 他社から預かる機密情報へのアクセス管理は、自社情報と同等以上のアクセス管理を行い、求めに応じてアクセス状況を証明できる体制をとらなければならない。

（電子化情報の取扱い）
第 24 条　電子化情報は、その特性を考慮し、情報セキュリティの確保に努めるものとする。
2. 電子化された機密情報の保管は、指定したサーバに限定して認めることとする。
3. 機密情報は、パソコンのローカルディスクなどでの保存を禁止する。
4. 機密度の高い情報は、記録媒体に保存して物理的に施錠できる場所に保存しなければならない
5. 電子化された機密情報の複製を認めない。

（ネットワークセキュリティの確保）
第 25 条　別途定めたネットワーク管理規程による接続方法のみにてネットワーク接続を許可する。
2. ネットワークを介した情報資源へのアクセスは、ユーザ ID とパスワードにより厳密に管理されなければならない。
3. パスワードは、適切に管理されるとともに、定期的に変更し、不正なアクセスを予防しなければならない。
4. インターネット利用にあたっては、マナーを守り、外部に迷惑をかけてはならない。
5. 極秘情報については、ネットワーク経由での送付を禁じる。

（個人情報の取扱い）
第 26 条　個人情報の取扱いは、個人情報保護法および個人情報取扱い規程に準拠して行うものとする。

（知的財産権の尊重）
第 27 条　知的財産権は、これを尊重しなければならない。
2. 特に他社の知的財産権を侵害しないように最大限の努力を払わなければならない。

第 5 章　機密情報の開示

（情報開示の条件）
第 28 条　機密情報の開示は、情報管理者が機密区分を確認したうえで許可するものとする。
2. 機密情報を開示する場合は、機密保持契約を締結しなければならない。

（機密保持契約）
第 29 条　機密情報の開示は、機密保持契約の対象者のみとし、開示を受けた者が第三者へ再開示することを禁止する。
2. 機密保持契約の承認は、専門家が行うものとする。
3. 機密保持契約の遵守は、常に組織内に徹底しなければならない。

（他社機密情報へのアクセス）
第 30 条　他社の機密情報へのアクセスは、当該企業が許可した場合に限る。
2. 職務上の立場を利用して、他社に機密情報の提供を強要することを禁止する。

（情報開示の方法）
第 31 条　機密情報を開示する必要がある場合は、開示先、その情報管理者および連番を明記しなければならない。
2. 開示者は、開示期限満了とともに、開示情報を回収しなければならない。
3. 回収が合理的でない場合あるいは不可能な場合は、廃棄を依頼するとともにその実施を確認しなければならない。
4. 定められた開示の範囲を越えて、機密情報を開示する必要が生じた場合、情報管理者の判断に委ねる。ただし、不都合が生じた場合は情報管理者が全責任を負うものとする。

第 6 章　緊急事態への対応

（緊急事態の想定と対応計画）
第 32 条　情報セキュリティに関しては、緊急事態を想定した対応策を定めなければならない。
2. 情報セキュリティに関する緊急事態の発生に備え、複数の連絡手段による連絡網を整備するとともに、定期的に訓練を実施しなければならない。

（緊急事態発生時の対応）
第 33 条　情報セキュリティに関する緊急事態が発生した場合は、情報セキュリティ管理者の指揮のもとに対応する。
2. 緊急事態の影響度に応じて、本部情報セキュリティ担当、情報セキュリティ担当あるいは情報セキュリティ担当役員へ報告するものとする。
3. 緊急事態の発生時には、あらかじめ定めた連絡網により関連部門へ緊急連絡するとともに、協力して解決に当たるものとする。

第 7 章　情報セキュリティ教育

（基本的教育）
第 34 条　管理者に対しては、情報セキュリティ教育を定期的に実施する。
2. 情報セキュリティ管理の充実のため、倫理教育を実施する。
3. 情報セキュリティ管理の状況を、定期的に従業員へ知らせることにより、管理レベルの向上に資するものとする。

（対象別教育）
第 35 条　従業員に対しては、入社時に、情報セキュリティに関する誓約内容を中心とした教育を実施する。
2. 管理職への昇格時には、情報セキュリティ管理者レベルの情報セキュリティ教育を実施する。
3. 担当する職種ごとに、専門分野に必要とされる情報セキュリティ教育を実施する。

第 8 章　情報セキュリティ監査

（本部管理）
第 36 条　各本部は、情報セキュリティ管理状況を自己点検し、管理レベルの向上に努めなければならない。

（情報セキュリティ監査）
第 37 条　内部監査の一環として、情報セキュリティ監査を実施しなければならない。
2. 情報セキュリティ管理に要する費用と、情報セキュリティ管理実施による経営効果を把握し、バランスのとれた情報セキュリティが構築されているかを監査しなければならない。

（機密保持契約締結先の監査）
第 38 条　機密保持契約を締結している企業の情報セキュリティ管理状況を確認するため、必要に応じて監査しなければならない。

第 9 章　罰則

（処罰）
第39条　　情報セキュリティ管理規程に違反した者は、罰則規程に基づき厳罰に処す。