「情報セキュリティ管理規程」作成の手引

情報社会の基盤整備の一つとして、情報セキュリティの充実が緊急の課題として浮上している。情報セキュリティには、技術的側面と管理的側面があるが、基本は「人」である。人の管理を充実させることなく情報セキュリティが万全になることは有り得ない。人の問題を放置したままでは、情報社会の安全・安定は得られない。

また、企業経営における情報セキュリティの目的は、経営活動における「情報活用」と、情報共有に必要な最低限の「情報保護」とのバランスをとることであり、安心して情報共有できる環境を創出し、保持することである。

情報セキュリティにおける人的側面の問題を解決するためには、一つの方策として、情報システムを運用する企業が、情報セキュリティ管理規程を定め、情報セキュリティに対する企業のポリシーを明確にして、情報システムの運用に当たることが必要である。

本情報セキュリティ管理規程（モデル）は、一つの完成した規程として作り上げている。その理由は、企業が本規程（モデル）を参考にして、自社用の情報セキュリティ管理規程を簡単に作れるようにするためである。そのためには、企業が本規程（モデル）の各条文の趣旨や狙い等を正しく理解し、自社用に不足している点があれば条文を追加し、不要な条文があれば削除し、自社に合致しない条文があれば修正して利用すべきものである。

本規程（モデル）は、以上のような考え方に基づき作成したものである。情報セキュリティ管理に関する規程がまだ作成されていない企業の参考に資することにより、情報セキュリティの強化に役立てることを目的としている。

上述のような点に留意し、この作成の手引きで「情報セキュリティ管理規程（モデル）」の各条文を設定した理由を理解していただき、自社用に手直しを加えていただきたい。

（前文）

前文は、各企業が自社の情報セキュリティポリシーに合わせて記述すべきものであり、他社のケースなどを気遣う必要はない。したがって、各企業の実情に合わせて記述するが、必要性がないと思われる場合や、特に書く内容はないと思われる場合は削除してもかまわない。記述する場合、一例をあげれば、次のような文面も考えられる。

情報は、人・物・金・技術・時間と同様、当社として最も重要な経営資源の一つであり、経営活動に有効活用しなければならない。情報の共有化を通じ、顧客や取引先も含めた効果を創出すべきであり、協業の成果を高める必要がある。情報共有化において信頼関係を確立するためのルールを定め、遵守するため本規程を制定する。

第１章　総則

第１条（目的）

目的には、規程の目的を簡単・明瞭に記述することが必要である。

顧客や取引先と当社の間および社内の部門間で、情報を共有して有効活用することがビジネスの基本である。本規程（モデル）では、情報共有の基本要件としての信頼関係を堅持するという意味で、情報セキュリティの確保を重要な経営の要素と位置づけている。

第 2 条（用語の定義）

規程の作成に際し、本規程（モデル）で取り上げた用語を必ずしも取り上げる必要はない。ただし、本規程（モデル）における用語の定義については、次のような諸点に留意したので参考にしていただきたい。

① 情報セキュリティ担当役員は、専任者を設置できない場合は兼務でよい。
② 情報セキュリティ担当は、専任者を設置できない場合は兼務でよい。
③ 本部情報セキュリティ担当は、情報セキュリティ担当と同様、兼務でもよい。本規程（モデル）では、本部が設置されている大きな組織を想定している（末尾の組織図を参照のこと）。
④ 情報資産を、情報のみとしたのでは活用できないケースが出てくる。そこで、情報の活用に関連する資産のすべてを含む必要がある。
⑤ 機密情報は、経営活動上の情報の重要度との相関性はないものとする。
⑥ 情報セキュリティ管理者は、通常、部長や課長が担当すればよい。
⑦ 情報管理者は、通常、部長や課長が担当すればよい。
⑧ 情報リスク管理者は、通常、部長や課長が担当すればよい。

第 3 条（対象情報）

対象情報とは、規程の対象となる情報である。この点を明確にしていないと、運用にあたり解釈上のトラブルが発生する可能性があるので注意しなければならない。

情報セキュリティの対象とする情報は、記録の媒体や形式を問わず、電子化された情報のみならず、書類等の非電子化情報も対象とし、かつ、人の記憶にある業務に関する情報も対象としなければならない。

自社の情報はもちろん、他社の情報であっても、社内に保管するものは対象としなければならない。

非電子化情報を対象とするのは、電子化情報も、その内容を紙に印字した途端、非電子化情報となるため、区分できないことにもよる。

特に、機密レベルの高い情報は、記録されずに人の記憶にのみある場合も多い。このような記憶情報の機密保持も、情報セキュリティにとって重要な位置づけとしなければならない。

第 4 条（保護対象）

保護対象では、情報セキュリティで保護するのは何か、その対象を明確に示さなければならない。

情報セキュリティとして、保護すべき対象は、情報だけでなく、情報の記録媒体、情報を保管する手段、情報システムのすべてとしなければならない。すなわち、情報を利用するために必要となる装置･設備等はすべて対象としなければ意味がない。

第 5 条（適用範囲）

適用範囲においては、この規程を誰に適用するのかを明確に定めることが必要である。本規程（モデル）で対象とする者は、当社の役員、監査役、従業員はもちろん、元従業員も含む。役員は、もっとも機密レベルの高い情報に接する機会が多いため、注意を喚起す

るためにも、明記しておくことが望ましい。従業員については、退職時、情報の持ち出しを禁止していると思われるが、元従業員の記憶の中に機密情報が存続するため、退職後の守秘義務も明確にしておく必要がある。

本規程（モデル）は、当社を対象としているが、当社グループ企業も、同等の情報セキュリティ管理を確立する必要があり、同様の規程を定めることにより、グループ企業の役員、監査役、従業員も対象とすべきである。取引先から見れば、当社と当社グループ企業は同一企業と見なされるので、同等の情報セキュリティ管理を確立することが望ましい。

当社の取引先で情報開示の対象となる企業は、取引基本契約に定める情報セキュリティ項目に従い、その従業員も、当該企業の情報セキュリティ規程の適用により対象となる。取引先の従業員と当社は、情報セキュリティに関して直接契約できないため、取引先と取引先従業員、取引先と当社、それぞれの情報セキュリティ契約を介して、情報セキュリティを保持させる必要がある。

第 6 条（情報セキュリティの評価）

企業を取り巻く経営環境は、常に変化しており、その変化内容は、タイムリーに情報セキュリティの規程や運用に反映されねばならない。そのため、定期的な情報セキュリティ評価が必要となる。情報セキュリティは、日常の情報管理活動の一環であり、その評価は重要な要素である。

第 7 条（規程の改廃）

規程の施行、変更、廃棄は、誰が、何時、どのように行うか、などを明確化しておく必要がある。本規程（モデル）の施行、変更、廃棄は、情報セキュリティ担当役員が提案し、社長が全社へ徹底すべきものであると考えている。

情報セキュリティは、すべての本部に関連するため、特定本部の担当役員ではなく、社長が制定しなければ、その効力は、限定的となる。

規程の改廃を社長が徹底するため、頻繁に変更することは困難な場合が多い。その場合、規程は変更の少ない内容に限定し、経営環境に合わせて、その都度変更しなければならない内容については、規程を補足する詳細基準や運用マニュアルに明記してもよい。

第 2 章　情報セキュリティの保持義務

第 8 条（情報セキュリティ保持の基本）

情報セキュリティを保持するための企業としてのポリシーを、明確に示すことが必要であると思われる。

[第 1 項]情報セキュリティ保持を特別視し、特定の本部を中心に保持することは困難であり、組織を通じた管理にしない限り、恒久的な対応とはならない。

[第 2 項]企業の長い歴史の中で、予算管理や人事管理などは、組織を通じた職場管理として根づいているが、情報セキュリティ管理も、これらと同様、職場での日常管理業務の一つに位置づけなければ、長続きしない。必然性が生じた時に限った一過性の取り組みでは、その経営効果は期待できず、実施のためのエネルギーだけが浪費される結果となる可能性がある。

第 9 条（目的外利用の禁止）

目的外利用の禁止は、原則を明確に定め、人によって解釈が異なることのないようにしなければならない。

[第 1 項]情報資産の利用を、本人の業務範囲に限定すれば、不正なアクセスはほぼ防ぐことができるため、目的外利用の禁止を徹底しなければならない。

[第 2 項]情報資産の利用が業務目的か私的目的かの判断は、第三者にとって難しい側面もあり、一概に断定できないが、ルールとして禁止するのは当然である。

[第 3 項]たとえば、インターネット利用で、外部に対し誹謗中傷など迷惑をかける場合も、大半は私的目的の場合が多いので、禁止事項とすべきである。そのために、インターネットの URL で、その接続を拒否するソフトウェアを導入する方法もある。

[第 4 項]今日の情報社会では、情報提供の要求は、金品の要求と同様に禁止すべきである。

第 10 条（情報の開示）

本規程（モデル）で定める情報開示は、情報管理者が許可することとしている。

[第 1 項]たとえば、機密情報の対象ではない社内情報について、取引の都合上、取引先へ開示する必要がある場合も生じる。そのような場合、本部情報セキュリティ担当などの許可を得なくても、情報管理者、即ち、部長や課長が判断し、その責任において、特例として情報開示を認めることができることにしている。

[第 2 項]業務上、本規程（モデル）に定める範囲以外の利用が必要な場合、たとえば、機密保持契約（NDA 契約：Non-Disclosure Agreement）が困難な場合、情報セキュリティ管理者の事前許可を得るとともに、情報管理者がその全責任を負うものとしている。企業同士の提携交渉など、役員に限定される場合、役員の責任において、情報が開示される場合もある。

[第 3 項]情報管理者に権限を与えているので、全責任は情報管理者が負わなければならない。

第 11 条（情報の返却･廃棄）

情報は、使用済みとなった時点での処理も重要な意味を持つことを理解しておかなければならない。

[第 1 項]社外に情報を開示する場合、開示する期限を定め、期限内に返却することを明確化しなければならない。

[第 2 項]運用上、返却に相当する措置として廃棄してもよいが、その場合は、確実に廃棄されたことを確認しなければならない。

[留意点]情報を開示する時には、NDA 契約など厳密な運用をしていても、その情報が不要（あるいは使用済み）となった場合の運用が疎かにされがちになるので、注意する必要がある。

第 12 条（取引先との契約）

取引先への情報開示は、契約締結を前提としなければならない。

[第 1 項]取引先に情報を開示する必要が出てきた場合には、情報開示に関する契約を締結しなければならないと定めている。これは原則である。

[第 2 項]保管方法については、自社と同レベルの基準での管理を要求する。複製は原則禁止とするが、業務上、複製物が必要となる場合、複製物の連番付与、開示先管理、期限満了後の廃棄について、明確化しなければならない。取引先の管理責任者を決め、違反時の罰則について定める必要がある。

第 13 条（誓約書の提出）

入社時、機密情報の取扱いに関する誓約書に署名させることは、今日では原則としなければならない。

[第 1 項]従業員として、入社時の動機づけは重要であり、違反時の処分にも従わせるため、機密情報の取扱いに関する誓約書に署名し、提出させることが必要である。

他社での勤務経験、大学や研究機関での研究経験などにより、守秘義務が課せられている者については、その旨、申告させるとともに、当社における情報開示を禁止しなければならない。

[第 2 項]当社の従業員が退職する場合、退職後も守秘義務が継続し、外部に開示しないことを誓約させ、誓約書に署名させることが必要である。特に、他社へ転職する場合もあるので、情報の持ち出しを禁止しなければならない。業務上収集した顧客名簿、メールアドレスなどの流用も禁止することが必要である。

[留意点]管理職に昇進する場合、情報セキュリティ管理者となり、情報セキュリティ管理上重要な立場となるため、改めて、誓約書を提出させることが望ましい。同時に、情報管理者、情報リスク管理者の役割も担うため、個別の誓約書ではなく統合した誓約書が望ましい。

第 3 章　情報セキュリティの管理体制

第 14 条（情報セキュリティ担当役員）

情報セキュリティの最高責任者には、役員を指名することが必要である。この役員が CSO（Chief Security Officer）である。

[第 1、2 項]社長が、情報セキュリティ担当役員を委嘱すべきである。情報セキュリティは、すべての本部に関係し、全社を統括した取り組みをする性格上、社長自ら委嘱することが重要である。

[第 3 項]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、情報セキュリティ担当役員を補佐するとともに、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、改善、担当役員への報告を行うことが必要である。

[留意点]情報セキュリティ担当は、専任者が望ましいが、困難な場合は、兼務でもよい。その場合、「全社情報セキュリティ委員会」などを組織して、補完する方法も有効であるので、自社に応じた運営を考慮することが望ましい。

第 15 条（本部管理体制）

各本部における管理体制を明確に位置づけることが、管理充実の第一歩である。

[第 1 項]社内の各本部ごとに、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ため、本部情報セキュリティ担当を本部長が指名する必要がある。

[第 2 項]本部においては、全社の場合と同様、本部情報セキュリティ担当が本部内の情

報セキュリティに関してすべての責任を持つ。
[第 3、4 項]部長や課長は、予算管理や人事管理と同様、情報セキュリティ管理者の役割を担うとともに、情報管理者、情報リスク管理者でもある。専任部署で情報セキュリティ管理をする方法もあるが、一部の特定の人だけによる情報セキュリティ管理は、組織に定着しない場合も多いため、本規程（モデル）では、組織の責任者を通じて管理することとしている。責任者と別の情報セキュリティ管理者を定める方法もあるが、上司の責任者に対して、職務を全うする難しさもあるため、責任者の兼務が、現実的であると思われる。

第 16 条（プロジェクトにおける管理体制）
プロジェクト方式による業務についても、情報セキュリティの管理体制をルール化しておく必要がある。組織をまたぐプロジェクト体制による業務が増加する中、プロジェクト推進における情報管理と情報セキュリティ管理の方法を明確にしなければならない。
プロジェクトにおいては、プロジェクトリーダが、責任者と同様、情報管理者、情報セキュリティ管理者を務める。プロジェクト終了後、業務がそれぞれの組織へ引き継がれる時は、情報セキュリティに関しても、責任を持って引き継がれなければならない。

第 17 条（共同プロジェクトにおける原則）
外部との共同プロジェクトが増加する中、共同プロジェクトにおける情報セキュリティ管理について、関連企業･団体と協議、調整し、その方法を明確化しなければならない。特に、同業他社との企業提携が一般的になる中、情報セキュリティに関する契約とプロジェクトにおける運用が大切である。
[第 1 項]共同プロジェクトにおいても、社内プロジェクトと同様、プロジェクトリーダが情報管理と情報セキュリティ管理の責任者となる。
[第 2 項]共同プロジェクトにおいては、当社の従業員がプロジェクトリーダを担当しない場合も、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と情報セキュリティ管理を担当する立場として、プロジェクトリーダと折衝する立場にあるとすべきである。
[第 3 項]プロジェクトリーダは、情報セキュリティ管理規程に精通し、情報セキュリティに関して参加企業との折衝にあたらなければならない。

第 4 章　機密情報の管理

第 18 条（機密情報）
機密情報の定義に従い、機密情報を指定する必要がある。
[第 1 項]機密情報は、業界によって大きく異なり、定義も違ってくる。一番の着眼点は、その情報の資産価値が喪失または減少することである。たとえば、その機密情報の漏洩が企業の信用へ大きな影響を及ぼすような情報は、機密情報としなければならない。
[第 2 項]機密情報管理という場合、自社の機密情報だけに目がいきがちであるが、取引先から預かった機密情報の管理も、自社情報以上に重視しなければならない。適切な管理ができていなければ、企業としての信用失墜にとどまらず、企業間の取引自体を失うことにも繋がる可能性があるので注意しなければならない。

第 19 条（機密区分の設定）

機密区分を設定する際には、企業のポリシーが明確になっている必要がある。

[第 1 項]本規程（モデル）における情報の機密区分は、「極秘」「厳秘」「部外秘」「社外秘」としているが、このうち「極秘」と「厳秘」は、特に機密レベルの高い情報である。したがって、「極秘」「厳秘」の情報は、ごく限られた範囲とし、機密レベルにふさわしい管理を行わなければならない。

[第 2 項]「極秘」は、経営上極めて重要で、ごく限られた関係者にのみ開示さる情報である。たとえば、目的外に使用された場合、企業の信用に重大な影響を及ぼすことが想定されるような情報である。

「厳秘」は、経営上重要で、限られた関係者にのみ開示される情報である。たとえば、目的外に使用された場合、企業の信用に影響を及ぼすことが想定されるような情報である。

「部外秘」は、部外へ開示した場合、混乱を招く恐れのある情報である。したがって、部内者には開示してもよいが、部外者には開示してはならない情報である。

「社外秘」は、社外には開示してはならないが、社内では積極的に共有、活用される情報で、社内情報の大半が該当する。

[第 3～5 項]機密区分の付与は、情報管理者が行い、環境の変化に対応して、適宜見直さなければならない。また、変更内容を、部門内および関連部門へ周知徹底することも必要である。

[留意点]機密区分の設定と徹底は、もっとも労力を要するため、検討段階で十分な議論を尽くすことが、社内でのコンセンサスづくりに有効である。

第 20 条（機密区分の表示）

機密区分は、その表示の形状、色および場所を定めることが望ましい。

[第 1 項]たとえば、各書類の右上に明示するとともに、書類の右下に、機密区分・有効期限・情報管理責任部門も表示することが必要である。機密情報については、朱書にすることが望ましい。

「社外秘」については、機密区分を表示しない場合も有り得ると思われる。その理由は、対象となる情報が多過ぎるためである。これらは、当該企業で合理的に決定すればよい。

[第 2 項]電子化情報も、書類に準じてモニター表示時および印刷時にも表示できるよう記録する必要がある。特に、モニター表示においては、改ざんされないファイル形式としなければならない。

第 21 条（機密情報の管理）

[第 1 項]機密情報は、書類または電子媒体を問わず、施錠可能な保管庫で保管しなければならない。したがって、サーバなどに常駐させた場合は、アクセスコントロールを施し、不正アクセスから守らなければならない。

[第 2 項]機密情報を収納する保管場所に、機密情報表示をしないのは、機密情報の所在を関係者以外に知らせることに直結するためである。

[第 3、4 項]機密区分が混在するファイルは、その中で一番機密レベルが高い機密区分に合わせざるを得ないため、機密レベルの低い情報にアクセス権限のある人が参照不可能となる。したがって、可能な限り、機密区分で分類しファイリングすべきであり、そのことを従業員へ徹底しなければならない。

第 22 条（機密情報の管理責任者）

機密区分設定やアクセス権限付与を含め、機密情報全般の管理は、情報管理者が担当しなければならない。

通常の組織においては、組織の責任者がすべての責任を負わなければならない。

第 23 条（機密情報へのアクセス管理）

[第 1、2 項]機密情報へのアクセスは、担当業務に照らし、個人ごとに権限を設定する。本部長の特命事項で専門的な内容など、部長や課長を経由せず、直接、担当者に指示される内容は、その担当者の上司である部長や課長であろうとも、アクセスする権限はない。

[第 3 項]機密情報は、利用目的を制限するとともに、アクセス権限者を制限しなければならない。

[第 4 項]機密情報に関し、アクセス状況を記録に残すとともに、アクセス実態掌握のため、定期的にアクセス記録を確認し、問題がある場合は、徹底的に調査、追及し、問題を解決しなければならない。

[第 5 項]他社の機密情報を保管する場合、NDA 契約の如何を問わず、アクセス状況を証明できるための体制をとらなければならない。

[留意点]「極秘」情報については、原則として電子化せず、ネットワークを経由した開示を廃止しなければ機密を守ることはできない。

第 24 条（電子化情報の取扱い）

[第 1 項]電子化情報は、原則、非電子化情報の取扱いと同じであるが、小型の記憶媒体に大量の情報を記憶できること、ネットワークを介して簡単に送付できること、複製物を簡単に作成できることなど、その特徴を考慮して、情報管理の詳細な手続を規定しなければならない。

[第 2 項]機密情報の保管を、サーバ以外のパソコンに認めた場合、持ち出しや情報参照が容易となり、情報セキュリティの確保が困難になるため、サーバに限定しなければならない。また、パソコンの廃棄時、ディスク保存内容の完全廃棄が、個別に必要となる。

[第 3～4 項]専門知識があり、かつ、悪意を持った人から、パソコンのローカル・ディスクの内容を守ることは難しい。したがって、フロッピーディスクなどの電子媒体での保存のみを認め、施錠可能な場所に保管しなければならない。

[第 5 項]電子化された機密情報については、保管方法、保管場所を制限するとともに、複製を禁止する必要がある。

第 25 条(ネットワークセキュリティの確保)

[第 1 項]社外ネットワークからのアクセスに対し、厳格な運用を規定しそのルールを徹底しない場合、社外への情報漏洩リスクが高まるため、アクセスを制限しなければならない。特に、業務効率化のため、在宅勤務や出張先からのアクセスが増える状況にあるため、ネットワークセキュリティの確保は重要である。

[第 2、3 項]社外への情報漏洩リスクで、もっとも注意すべきことは、内部からの情報漏洩である。したがって、データベースへのアクセスなど、ID やパスワードによるアクセス制限は必須である。

[第 4 項]外部のホームページなどへの書き込みなど、社内からの私的なアクセスを制限しなければならない。社内ネットワークには、従業員以外の勤務者のアクセスを認めている場合もあり、アクセスの可能性がある者全員への制限が必要である。ネットワークを介してのコンピュータウイルスの侵入を阻止するため、ファイアウォール上での防御および各パソコンへのワクチンソフト組み込みなどの対策を講じなければならない。コンピュータウイルスの侵入阻止とともに、社外へ、コンピュータウイルスを拡散させないための手段も導入すべきである。

[第 5 項]極秘情報をネットワーク経由で送付することは、理由の如何を問わず禁止すべきである。

第 26 条（個人情報の取扱い）

個人情報については、個人の権利を尊重し、保護を図るため、別途、個人情報取扱い規程を定め、個人情報保護に努めなければならない。

第 27 条（知的財産権の尊重）

[第 1、2 項]自社の知的財産を保護することはもとより、他社の知的財産を尊重しなければ、自社の知的財産も守れない。

第 5 章　機密情報の開示

第 28 条（情報開示の条件）

[第 1、2 項]企業間での提携関係が拡大する中、機密情報を開示する機会は多くなっている。ただし、機密情報を開示する前提条件として、NDA 契約を締結しなければならない。

第 29 条（機密保持契約）

[第 1 項]NDA 契約は、技術部門や営業部門での交渉が多いため、専門家のアドバイスと承認を得ることが望ましい。NDA 契約は、その性格により、当社全体に関係するもの、逆に特定の部門や従業員だけが対象となるものもあり、契約内容により適切な対応をしなければならない。NDA 契約は、開示範囲を限定するため、第三者へ再開示する場合は、再契約しなければならない。

[第 2 項]契約内容の妥当性、合理性、優位性を専門的な視点から確保するため、社内外の法律専門家に相談することが望ましい。

[第 3 項]契約の重要なポイントは、その内容と運用であり、契約内容を関連部門へ徹底しなければならない。特に、契約締結部門が、社内関連部門と情報を共有する場合は、契約内容に違反しないように注意しなければならない。

第 30 条（他社機密情報へのアクセス）

[第 1 項]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のみとしなければならない。また、機密情報を提供される前に NDA 契約を要求される場合、契約内容を十分に吟味し、不用意に同意のサインをしてはならない。同意できない場合、機密情報の開示を拒否するスタンスも重要である。

[第 2 項]購買部門が仕入先と交渉する場合などで、職務上の立場を利用し、他社に対し

て機密情報の提供を強要することは禁止しなければならない。

第 31 条（情報開示の方法）

機密情報の開示において、開示先、開示期限および回収方法について、常に意識するとともに、開示後の所在管理を重要視しなければならない。

[第 1 項]機密情報を開示する必要がある場合、複製物に、開示先、その情報管理責任者および連番を明記しなければならない。

[第 2 項]開示者は、開示から廃棄処分までを管理しなければならない。開示した機密情報は、保管期限とともに回収し、連番が揃っているか確認するとともに、欠番があれば、開示リストから、該当者に返却を請求する。

[第 3 項]回収が妥当でない場合は、廃棄しなければならない。その際、確実に廃棄されたことを確認しなければならない。

[第 4 項]営業部門などにおける取引先との交渉において、定められた範囲を超えて情報開示が必要な場合もあるが、そのような場合、情報管理者の責任において、開示を可能とする運用も必要である。他社の「社外秘」情報を入手する場合は、開示状況を確認し、不正な場合は、情報入手を拒否しなければならない。いずれの場合も情報管理者が全責任を負わなければならない。

第 6 章　緊急事態への対応

第 32 条（緊急事態の想定と対応計画）

[第 1 項]緊急事態が生じる前に、緊急事態を想定し、その対応計画を立案し訓練しておくことが、リスクを最小限にとどめる方法である。

[第 2 項]緊急事態の中には、想定困難なケースもあるので、対応計画にない場合も迅速に対処できるよう、携帯電話なども含め複数の手段による緊急連絡網を整備するとともに、うまく機能するよう定期的に訓練すべきである。

第 33 条（緊急事態発生時の対応）

[第 1～3 項]情報セキュリティに関する緊急事態が発生した場合、情報セキュリティ管理者の指揮に従い、緊急事態の影響度を把握し、対応計画に基づき対処するものとする。また、あらかじめ定めたルールに従って、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連絡するものとする。

第 7 章　情報セキュリティ教育

第 34 条（基本的教育）

[第 1 項]情報セキュリティ教育でもっとも重要なことは、情報セキュリティの第一線の責任者である情報セキュリティ管理者に対し、毎年定期的に、教育を実施することである。

[第 2 項]情報セキュリティの確保は、技術的側面から対応するだけでは限界がある。より効果的な情報セキュリティ管理の方法として、倫理教育を徹底する。

[第 3 項]情報セキュリティ管理の状況に関し、従業員へ周知徹底することにより、管理レベルを向上させる。

第 35 条（対象別教育）

[第 1 項]対象者別の情報セキュリティ教育では、入社時と管理職昇格時の教育が効果的である。入社直後の従業員に対しては、入社時の情報セキュリティに関する誓約内容を中心とした情報セキュリティ教育を実施する。

[第 2 項]管理職昇格時の教育は、情報セキュリティ管理者としての職務を全うできる情報セキュリティ教育を実施する。

[第 3 項]技術部門、営業部門、情報システム部門、法務部門など、担当する職種ごとに、情報セキュリティ管理項目が異なるため、専門分野に必要とされる情報セキュリティ教育を中心に実施する。

第 8 章　情報セキュリティ監査

第 36 条（本部管理）

情報セキュリティの確保は、それぞれの組織で、業務管理の一環として取り組まなければならない。したがって、各本部単位で情報セキュリティ管理状況を自己点検し、改善策を実行することを基本とする。

第 37 条（情報セキュリティ監査）

[第 1 項]社内での内部監査の一環として、情報セキュリティ監査を実施する。ただし、情報セキュリティの専門的な視点も必要であることから、内部監査部門が、情報セキュリティ担当に情報セキュリティ監査への協力を要請した場合、情報セキュリティ担当は応じるべきである。

[第 2 項]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する必要がある。

第 38 条（機密保持契約締結先の監査）

欧米企業では一般的になっているが、NDA 契約を締結した相手先企業での情報セキュリティ管理状況を確認するため、必要に応じて実査しなければならない。また、そのために契約書に監査条項を設けなければならない。

第 9 章　罰則

第 39 条（処罰）

各社の社内規程との関連もあるが、情報セキュリティ規程に違反した場合、社内罰則規程に基づき、厳罰に処分するものとする。

関連規程の参考例

本規程（モデル）の中に現れる規程と契約に関し、その中に含まれるべき主な項目は、以下のとおりである。

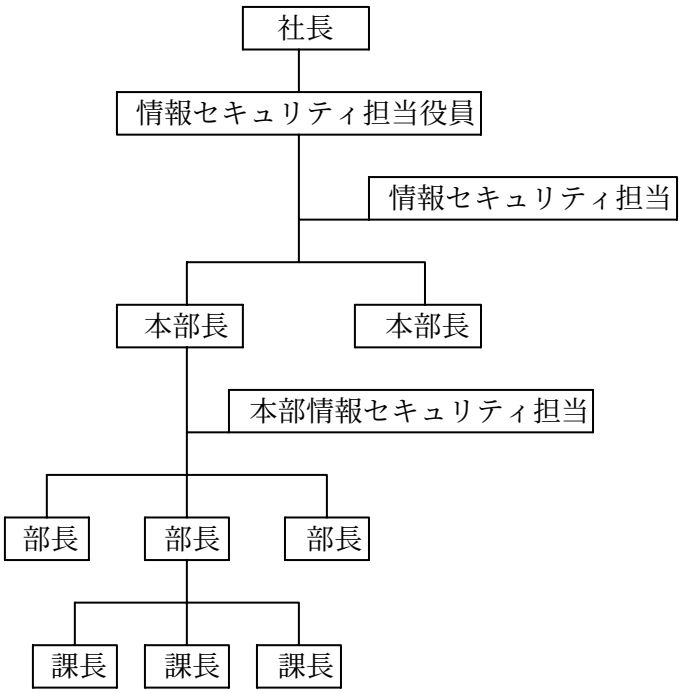
1．ネットワーク管理規程
基本方針、安全性・信頼性・整合性・発展性の確保、合理性と経済性の追求、ネットワーク管理者の役割、推進体制と役割、ネットワーク監査

2．個人情報取扱い規程
組織体制と管理責任、個人情報取扱いの基本原則、個人情報の取扱い方法、従業員教育と徹底、内部監査

3．機密保持契約
契約先におけるアクセス権限者の限定、機密情報の管理方法、複製の制限、守秘期間満了後の返却または廃棄方法、当社の立入り検査権、契約違反時の措置

4．罰則規程
具体的な内容は、次のように考えられる。
従業員が故意または重大な過失により本規程に違反し、「社員就業規則」に該当する場合は、同規則により措置される。役員は、商法等に照らして措置される。

情報セキュリティと組織との関連



管理者とは、部長および課長を指す。
管理者は､情報管理者､情報セキュリティ管理者および情報リスク管理者を兼務する。

（注）本規程（モデル）では、本部が存在する大きな組織を想定している。