平成 14 年度　セキュリティ研究部会　報告書

JUAS が作るセキュリティポリシー

―国際規格に準拠したセキュリティ管理汎用規定集―

平成 15 年 3 月

社団法人　日本情報システム・ユーザー協会

セキュリティ研究部会　報告書目次

はじめに

JUAS セキュリティ研究部会は今期で 4 年目を迎えました。
インターネットに代表される情報ネットワークが企業活動に欠かせないものとなるにつれ、この 4 年間で企業の情報セキュリティに対する関心は劇的に高まってきました。

世界一安全といわれる日本でも、ネットワークの世界は否応もないグローバルな世界で、ここでの情報セキュリティの確保は企業経営にとって、現時点での緊急・必須の課題であることは言うまでもありません。これに加え、「終身雇用」「系列」の崩壊など、企業構造の大きな変化によって企業内部のセキュリティリスクも確実に増大する一方です。 企業全体から眺めた、一貫した情報セキュリティ管理の必要性は、これまでになく高くなってきたと言えます。

しかし、いざ具体的に企業が本格的な情報セキュリティ管理を実施しようとすると現実の作業には多くのハードルが待ち構えていて、その実現は容易なことではありません。その大きなひとつが、「情報セキュリティの国際規格」といわれる ISO17799 などに準拠し、なおかつ自社の円滑な営業活動を妨げないセキュリティ管理基準（セキュリティポリシー）を策定することでしょう。

当研究部会には、この部会に継続して参加するうち、コンサルタントとして独立したり、専門家として講師を務めるレベルに達したメンバーが相当数を占めてきました。また、メンバーが所属する企業の業種も各種の製造業から、サービス、通信、金融・保険と多岐にわたり、弁護士も参加しています。

そこで今期はこれを奇貨とし、メンバーがこれまで蓄積してきた知識と経験を活用して智恵を出し合い、一定の国際規格に準拠した汎用的な標準規定集を作ろうということになりました。ここでは一般的なモデル企業を想定し、この企業のセキュリティ基本方針のような上位の規定から、各業務単位の下位の規定、および実際の一部の手順、ガイドラインまで、統一された規定集を作成の範囲としました。

この規定集の種本は、メンバーの中のコンサルタントが、これまで実際に講習のテキストとして使っていた規定例です。これを基本に、1年かけて 30 社近い部会メンバーが手分けし、不足している残りの部分を補い、国際規格（BS7799-I：1999,ISO/IEC17799,JISX5080）に準拠しつつ、かつ体系的に文書を統一して完成させたものです。

メンバーである現場のセキュリティ実務担当者が、月1回の定例会議だけでなく、多忙な業務の合間にグループ内の分科会まで開いて作成した規定は、実務に即した実際的な規定になっています。これから自社の規定集を作ろうという方々には必ず参考になるものと考えています。

情報セキュリティ管理の実施には、このほかにセキュリティリスク全体を集約しリスクに見合った具体的な個別のセキュリティ対策を設定するという、もうひとつの難関が待っていますが、少なくとも規定の策定に関しては、この報告書を一読し、本文の規定集を自社に合わせて加除訂正していけば、国際規格の難解な規範（コントロール）を元に、最初から作り上げるよりはるかに短時

間で規定集を完成させることができます。

最近は情報セキュリティに関する参考書もかなり出まわってきましたが、このようなユーザー企業の立場から作られた実践的でしかも汎用的な規定集はまだ極めて例が少なく、これから管理基準を作ろうというJUAS会員企業のセキュリティ担当者の方々に有益な資料になるものと確信しております。

また、我々、部会メンバーは、この汎用規定集が、JUAS会員企業にとどまらず、もっと広い範囲で活用されることを願っています。我々の活動の成果が多くの企業で役に立つということは、JUAS の名前が世に広がることであり、JUAS の認知度が高くなるということです。こうなれば、JUAS での活動にも気兼ねせず参加することができ、これまでの多年にわたる研究部会の苦労も十分に報われるということになります。

関係各位には、上記の趣旨をご理解の上、ご一読されて、この規定集の有用性に納得していただけるようなら、ぜひ、お知り合いの方々にもご紹介をしていただけるよう期待しております。

平成 15 年 3 月 31 日
JUAS セキュリティ研究部会　部会長　永田靖人

第１部　国際規格に準拠したセキュリティ管理汎用規定集

〔１〕 規定集の概要

〔２〕 基本規定

〔３〕 情報管理関連規定

〔４〕 システム開発・運用関連規定

〔５〕 一般運用管理規定

〔６〕 情報セキュリティガイドライン

規定集の概要

規定集の構成

情報セキュリティ関連規定は、企業の規定体系の一部を構成するもので、独立して存在するものではありません。企業の数ある規定類の中の一部を構成するもので、全体を階層構造にして整理する必要があります。企業の規定体系の中からセキュリティ管理に関連する規定を取り出したものが図表1．1です。

必ずこうしなければならないという基準はありませんが、国際規格などで言う「ポリシー」「ルール」「プロセデュア」という区別にならい３層になっています。

図表1．1のうち、○印のついている文書を作成対象としています。○印のついていない会社全体の経営ポリシー、従業員就業規則は余りにも範囲が広く、汎用的にできないので省略してあります。

セキュリティ関係の規定の中で一番上位にあるのは、「秘密保持規定」と「情報セキュリティ基本方針」（狭義のセキュリティポリシー）です。「情報セキュリティ基本方針」は、経営トップが全従業員に対して「会社として『情報』と『セキュリティ』をどのように考えるか」ということを宣言するものです。

この「情報セキュリティ基本方針」の中にパスワードの扱いなどの具体的かつ詳細な項目を入れている例もありますが、本規定集では情報セキュリティ基本方針(ポリシー)－規定(ルール)－ガイドライン(プロセデュア)という階層構造にしています。この区分の考え方は以下のとおりです。

情報セキュリティ基本方針

文字どおり「基本方針」です。会社として情報に対する基本的な考え方の宣言文です。この「基本方針」は、経営トップが情報セキュリティに対する考え方を意思表示するものです。できれば1頁にまとめ、会社全体としての基本方針（ビジネスポリシー）、他の基本方針（環境保全基本方針など）とともに一覧にして従業員手帳などに印刷して配布し、従業員がいつでも参照できるようにしておくと方針徹底の一助になると思います。

規定

情報セキュリティ基本方針を受けて策定される各種規定のことです。規定には、情報技術の進歩や法令の改廃によっても変更にならない不変的で基本的なルールを定めておきます。これは、規定はセキュリティマネジメントの枠組みを構成するもので、その更新は情報セキュリティ委員会などの承認手続きを必要とし、頻繁に改訂するものではないからです。

ガイドライン

ガイドラインで具体的かつ詳細なルールや手法を定めます。情報技術の進歩に伴い常時改訂されていかなければならない性質の内容も記載します。

「情報セキュリティ基本方針」などを社員だけにしか渡さないという企業もありますが、経営の透明性が重視されつつあり、社員だけでなく関連会社や外部の委託先の社員など関係者全員に渡すということを考えておいたほうがよいと思います。

モデル企業

規定を作成する場合、その構成や内容は，対象とする組織構成やセキュリティマネジメントの体制などにより変わってきます。そこで、本規定を作成するにあたり、前提としたモデル会社の組織構成を図表

1．2に示します。 モデル会社のイメージは、いくつかの事業部で構成され、全国に支社も持つ製造業で子会社もあり、規模は 2 部上場で、システム開発部門もあるという中規模の企業を想定しています。

また、セキュリティマネジメントの体制を図表1．3に示します。

組織構成では、組織外に情報処理システム等のアウトソーシング先や，社外の人で情報システムを利用する第三者がいます。

責任者の名称

前記のセキュリティマネジメント体制では、多種類の管理責任者が登場します。

また、各規定にもその対象範囲によって、責任者の名前が変ってきます。図表1．4は、本社部門および各事業部の各管理責任者の名称を表にしたものです。これら責任者は会社の規模によって同一人が複数兼ねる場合もあります。

表現・記述

規定を読みやすくするために、規定の作成にあたっては下記のような点に留意しました。

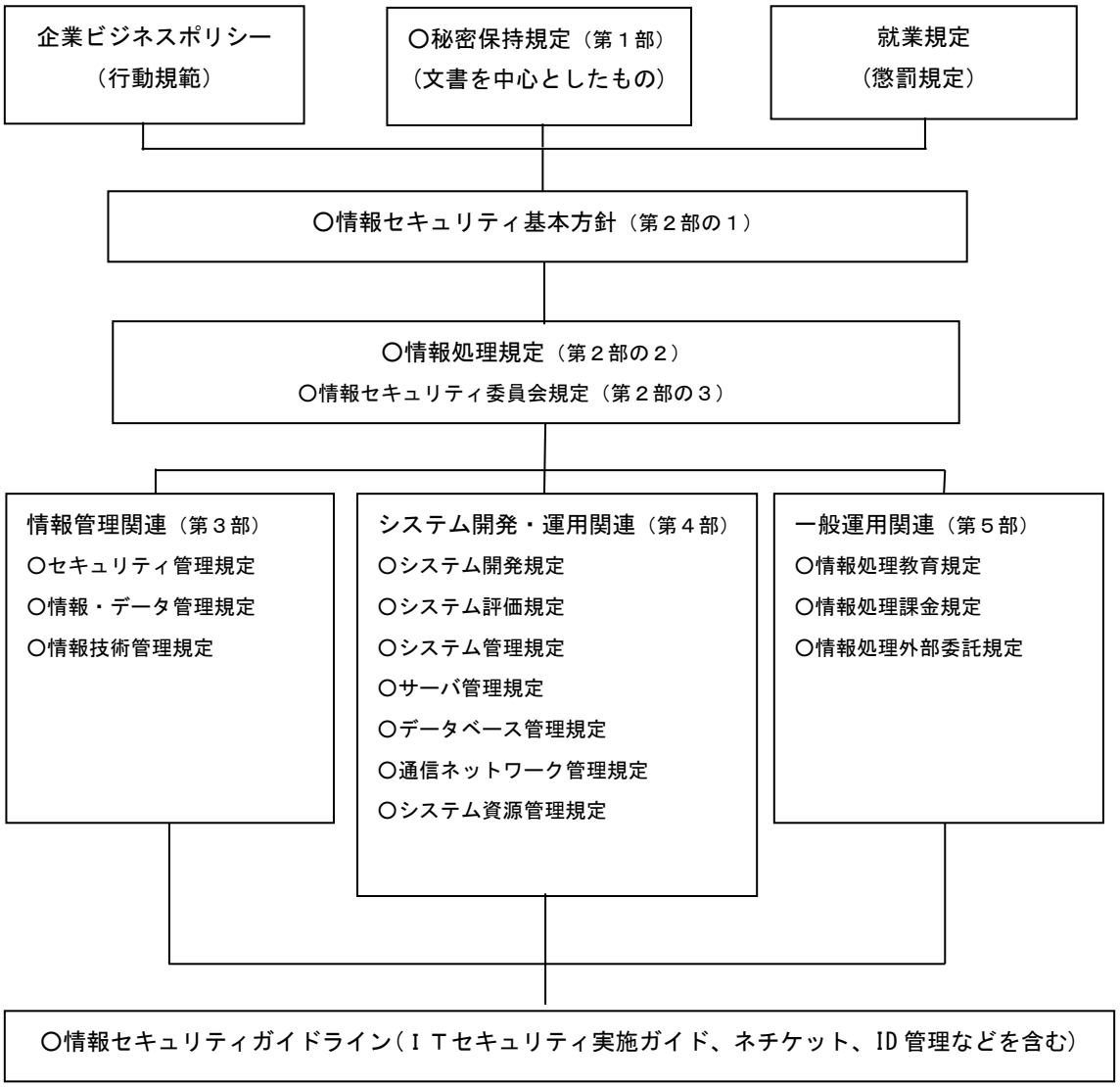
① あいまいな表現，概念的な表現は避ける。
たとえば『基本精神に則る』、『第1級の情報資産』、『業務の一環としてセキュリティを意識しなければならない』など。
② 主語を明確にする。
③ 義務であるのか，推奨であるのか、禁止であるのかを明確にする。
④ できるだけ例外は設けない。
⑤ 規定の記述は、できるだけ1つの規定の中で完結させる。複数の規定を参照する場合は、必ず参照する規定に対して、どこを参照すべきかのポインタを記述する。

以上が、この汎用的な規定集を策定するに当たっての前提条件です。読者の方々は、ご自分の会社の業務内容、組織、規模などに応じて、これからの規定集を加筆したり、削除したりしてその企業にふさわしい規定を完成させてください。

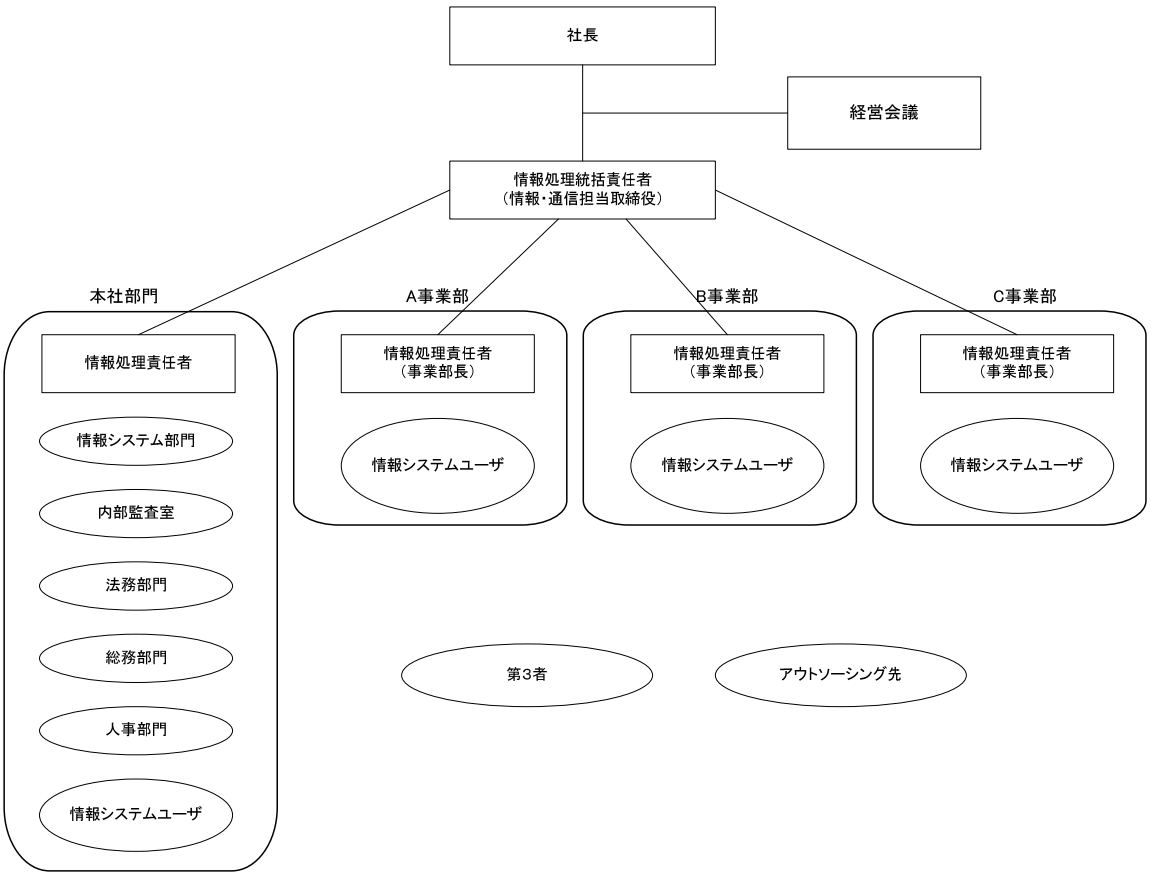
なお、この規定には、セキュリティマネジメント構築に欠かせない全社の情報資産の洗い出し、そのセキュリティリスクの見積もり、リスクアセスメントによる具体的な対策の決定というステップには言及していません。すなわち一定のリスクアセスメントが終わり、とるべき対策が大筋決定していることを前提としています。

この規定集の加筆訂正は、そうした段階を経て具体的に行うものですが、ISO/IEC17799 といった国際的な基準に準拠するためには、このレベルのルール、プロセデュアを社内で確立しておく必要があることを理解しておいてください。

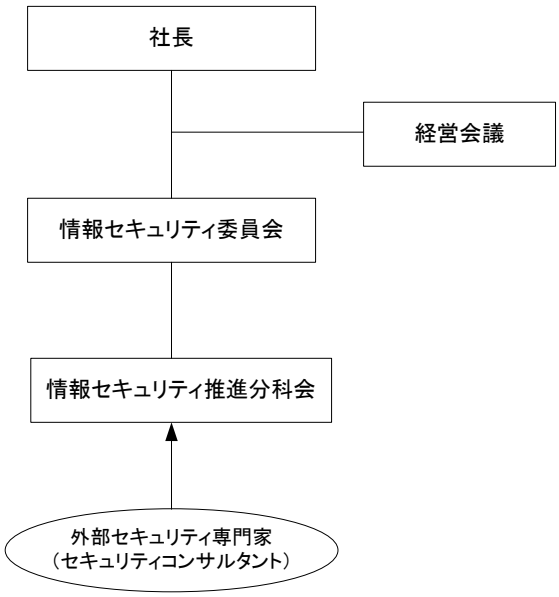
図表１．１　情報セキュリティ関連規定集の全体関係

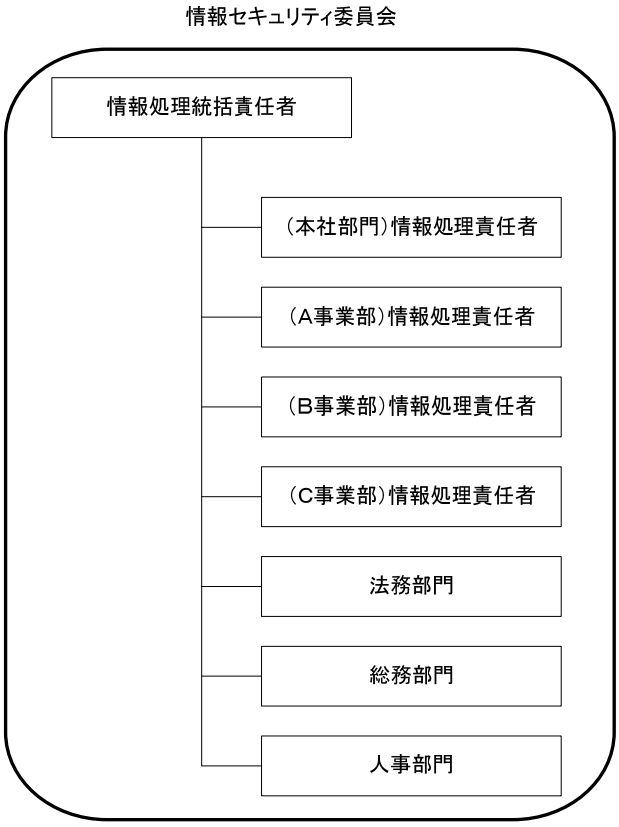


図表１．２　組織構成


社長
経営会議
情報処理統括責任者
（情報・通信担当取締役）
本社部門
情報処理責任者
情報システム部門
内部監査室
法務部門
総務部門
人事部門
情報システムユーザ
A事業部
情報処理責任者
（事業部長）
情報システムユーザ
B事業部
情報処理責任者
（事業部長）
情報システムユーザ
C事業部
情報処理責任者
（事業部長）
情報システムユーザ
第3者
アウトソーシング先

図表１．３　セキュリティマネジメント体制





■情報セキュリティ委員会

全社のセキュリティマネージメントの管理，推進を行い，委員長が全社のセキュリティマネージメントの責任者となります。委員長は，情報処理統括責任者が担当します。ISO/IEC 17799 で規定されている『情報セキュリティマネージメントフォーラム』に相当します。

■経営会議

情報セキュリティ委員会で実施する施策のうち経営にかかわる事項の承認を行います。たとえば，重要なセキュリティポリシーの改訂の承認などを想定しています。

■情報セキュリティ推進分科会

情報セキュリティ委員会が進める施策を具体化する実働部隊です。

■セキュリティ管理者

本社部門および各事業部の『情報処理責任者』,『情報通信ネットワーク管理責任者』,『情報・データ管理責任者』,『システム開発責任者』,『システム管理責任者』,『システム運用責任者』の総称です。

セキュリティ管理者についての詳細は、「セキュリティ管理規定」に記載されています。

図表１．４　管理責任者の名称

* セキュリティ管理規定で登場する総称

責任者名称	ライン組織		定義規定	ｾｷｭﾘﾃｨ管理者*	情報技術管理者*	備考
	本社	事業部				
情報処理統括責任者	○		情処			情報・通信担当取締役（CIO）
情報処理責任者	○	○	情処，セ管	○		事業部長
情報・データ管理責任者	○	○	情デ，セ管 情技	○	○	本社，事業部（情報処理責任者 or 指名者）
システム資源管理責任者	○	○	資源，情技		○	
情報通信ネットワーク管理責任者	○	○	NW，セ管，情技	○	○	
システム開発責任者	○	○	開発、セ管 情技	○	○	
システム管理責任者	○	○	シ管、セ管 情技	○	○	基幹システム，部署システム
サーバ管理責任者	○	○	サ管，セ管 情技	○	○	基幹サーバ，部署サーバ
データベース管理責任者	○	○	DB，セ管，情技	○	○	基幹DB，部署DB
情報処理教育責任者	○	○	情教			全社＆部署（事業部）
情報処理外部委託責任者	○	○	外委			
情報処理課金管理責任者	○	○	課金			
システム評価責任者	○		評価			

＜略号＞

情処:情報処理規定　／　セ管:セキュリティ管理規定　／　情デ:情報・データ管理規定　／　情技:情報技術管理規定　／　情教:情報処理教育規定　／　外委:情報処理外部委託規定　／　課金:情報処理課金規定　／　開発:システム開発規定　／　評価:システム評価規定　／　資源:システム資源管理規定　／　サ管:サーバ管理規定　／　DB:データベース管理規定　／　NW:通信ネットワーク管理規定　／　シ管:システム管理規定

〔1〕前提規定

秘密保持規定

秘密保持規定

秘密保持規定

第１章　総則

第1条（目的）

この規定は会社の秘密情報および会社が受領または保有する他者の秘密情報について、その秘密の維持、管理のための取り扱いを定め、重要財産として保全を図ることを目的とする。

第2条（定義）

1. この規定において「秘密情報」とは、会社の経営上・管理上（財務、人事関係など）、技術上・生産上・営業上の情報であって、秘密として取り扱われるべき情報をいう。
2. 秘密情報とは具体的に次の情報をいう。

(1) 業務の過程で生み出され、取得される全ての知識、経験または情報のうち、社外に漏洩すると会社が損害を受ける、または得られるべき利益を失うことになるもの、またはその恐れがあるもの。（不正競争防止法の適用を受ける営業秘密を含む）

(2) 会社が顧客、契約先、出資者その他の者から開示、提供された情報のうち、社外に漏洩すると情報の正当な保有者が損害を受ける、または得られるべき利益を失うことになるもの、またはその恐れがあるもの。

(3) 他社と書面または口頭による契約により、会社が秘密保持の義務を負うもの。

3. 情報とは、文書、記録媒体、試作品、生産設備およびその他の有体物並びに通信データ、言動等、その形態は問わない。

第3条（秘密の保持）

1. 会社の役員・社員（派遣社員・臨時社員を含む。以下同じ）は、関係法規、関係社内規定、就業規則に従い、直接であると間接であるとにかかわらず、在職中は当然に、退職後（別途定める期間）においても秘密情報を社外に漏洩しまたは不正に使用しない。
2. 会社の役員・社員は他社の秘密情報を不正に入手し、使用および漏洩することは他社の権益を侵害することであることを十分に認識し、秘密情報を管理・利用する。

第２章　秘密情報の管理

第4条（管理責任）

1. 秘密情報の管理責任は情報処理責任者が負う。
2. 情報処理責任者は、事業部および各部門の秘密情報をこの規定に基づいて管理・保全する。

第5条（秘密情報の分類）

財産的価値のレベルにより、秘密情報は以下の分類・対応をするものとする。

（1）極秘

社外に漏らされると会社が極めて重大な損失、不利益を受ける情報。この指定を受けた情報は、特に認めた者以外には開示しない。

（2）秘

極秘レベルではないが、社外に漏れることで当社が重大な損失、不利益を受ける可能性がある情報を指す。この指定を受けた情報は、業務上関わりのある部署の所属者以外には開示しない。

（3）社外秘

極秘・秘以外の秘密情報をいう。

第6条（秘密情報の指定と解除）

1. 情報処理責任者は秘密情報の区分指定を行う。
2. 情報処理責任者は秘密情報について、その秘密性に変化が生じた場合は、指定区分の変更・指定の解除を行う。

第7条（文書等への表示）

文書作成者は、所管する秘密情報を内在する電子ファイルを含む文書等については第5条に従い、スタンプまたは予め印刷した書式により、「極秘」「秘」「社外秘」の表示を行う。また、電子ファイルにはヘッダー部に同様な文字列を表示する。

第8条（口頭の開示）

1. 社員が社内において口頭で秘密情報を開示する場合は、情報処理責任者が指定した区分に従って、開示する相手を選び、秘密情報であることを宣言した後開示する。
2. 社員は社内の会議などで秘密情報を開示する場合は、情報処理責任者が指定した区分に従って予め出席者を限定するか、関係のない者の退出を求める。

第9条（事業所見学）

1. 社員は、社外の者に事業所の見学をさせる場合は、情報処理責任者の許可を受ける。
2. 情報処理責任者は、見学者に対し、業務上必要と認める場合を除き、撮影、模写、録音などを禁止する。
3. 情報処理責任者は、業務上必要と認めた秘密情報に関して見学、撮影、模写、録音など行わせる場合は、事前に秘密情報保護のための契約締結を行う。

第10条（廃棄）

情報処理責任者は、秘密情報の廃棄に当たっては、対象物に応じて文書は焼却、解体などにより、電子ファイルは記憶媒体を無意味な情報で上書き、破壊などにより秘密情報が漏洩することがない状態にして廃棄する。

第 11 条（秘密情報の社外開示）

社員は、業務を遂行する上で、取引先、顧客、提携先、コンサルタントなどに秘密情報を開示する場合は、情報処理責任者の承認を得て行う。また、必要に応じて秘密情報保護のための契約締結を行う。

第３章　その他

第 12 条（規定違反）

1. この規定に違反した者は、就業規則に基づいて懲戒に付する。
2. 会社はこの規定に違反する行為の差し止めを求め、また、会社が損害を被ったときは、この規定に違反した者に対し、その損害賠償を求めることができる。

第 13 条（規定の改廃および周知）

1. 本規定は情報処理統括責任者が任命した情報処理責任者が立案し、情報セキュリティ委員会のレビュー、情報処理統括責任者の決定を得て改廃を行う。
2. 第 1 項の決定事項は、これを社内に周知しなければならない。

〔２〕基本規定

１．情報セキュリティ基本方針

２．情報処理規定

３．情報セキュリティ委員会規定

１．情報セキュリティ基本方針

情報セキュリティ基本方針

第１章　はじめに

現在の世の中はかつてない情報化時代となっており、情報をいかに有効に利用することができるかどうかが会社の生命線になっている。この中で、当社は世の中に有益な製品を提供し、社会の進歩に貢献することを社是としてきている。

当社は投資家、顧客をはじめとするステークホルダーの信頼を得るため、情報セキュリティ管理に取り組む。会社の価値そのものである情報資産の重要性を認識し、有効利用していくために、役員を含め全社員は情報資産の機密性（Confidentiality）だけでなく、保全性（Integrity）、可用性（Availability）の確保に努めなければならない。

第２章　基本方針

1. 全社の情報セキュリティは情報処理統括責任者の主導のもとに、「情報セキュリティ委員会」で推進を図るものとする。
2. 経営戦略に関する情報、社員・顧客・取引先の個人情報、その他会社が定めた秘密情報は、企業における重要な財産であると認識し、法的な要請等の合理的な必要性がない限り、公開してはならない。情報全体の取り扱いに関しては、当社における文書管理規定、秘密保持規定を遵守する形で運用を行う義務を負う。上記秘密情報は法的にも保護されることを認識し、かつそのような情報を創出、活用する上で適法・適正な管理のもとに置かなくてはならない。
3. 当社のコンピュータネットワークは、業務を効率的に行うために整備・提供するものである。本ネットワークへのアクセスは業務の遂行を支援するために許可しているものであり、利用者は当社の制定する規定を守らなくてはならない。
4. 当方針に基づき、当社は情報処理全般に関する規定集を制定する。この規定集に含まれていない

個別内容については、各事業部において適正に標準、ガイドラインを制定し、維持管理していかなくてはならない。

5. 当方針および情報処理規定集において、情報処理および秘密情報の管理と運用に関して必要な事項を定める。役員を含める全社員はこれらに反する行為を行った場合は、就業規則に基づいて懲戒されるだけでなく、損害賠償の責に任ぜられる。

6. 個人情報の漏洩による社会的影響の大きさを鑑み、会社は個人情報を慎重に扱い管理する。また、不正競争防止法に関わる秘密情報も管理対象として慎重に扱い管理するものとする。

２．情報処理規定

情報処理規定

第１章　総則

第1条(目的)

この規定は、当社における情報管理全般を俯瞰する「情報セキュリティ基本方針」に基づき、情報処理全般が円滑に行われることを目的とする。情報処理の方針を明らかにすることで、情報の共有化・活用等が進み、経営活動の効率的運営を支える情報処理が的確に行われることを目指す。

第2条(適用範囲)

この規定は全部署の情報処理に関する業務に適用する。社内で働く各情報システム利用者は当然として、当社が主体となる関係会社、業務委託先会社との間の情報処理業務においても、本規定の適用を原則とする。

第3条(用語の定義)

本規定および本規定に基づき定められる各規定で用いられる主な用語の意味は次のとおりとする。

(1)「情報処理」

情報システムによって会社が必要な情報(電磁的記録)を収集、選別、加工、蓄積、検索、伝達すること。

(2)「情報処理統括責任者」

情報・通信担当取締役：全社の情報処理に統括責任を負うと共に、情報セキュリティ管理の統括責任を負う。

(3)「情報処理責任者」

事業部長および本社管理部門長：事業部の情報処理、情報セキュリティ管理に責任を負う者。 権限委譲する代理者を任命できる。

次の情報処理業務を行う。

①情報セキュリティの管理

②情報システムの開発、管理・運用

③情報資源の管理

④情報通信ネットワークの管理

⑤情報技術の管理

⑥情報処理の教育

⑦情報処理業務の外部委託管理

⑧情報処理費用の課金

(4)ユーザー

情報処理に携わる役員・社員（派遣社員、臨時社員を含む）

(5)第三者

関係会社の社員、外部委託先社員、電子商取引契約を結んだ取引先社員

第4条(規定の効力)

1. 会社の情報処理に関する事項はすべてこの規定を基本とする。
2. この規定に定めのない事項またはこの規定によることが適切でない事項は、本社情報システム部長の指示または承認を得て行う。

第5条(基本方針)

1. 会社が行う情報処理は定款、取締役会規則、行動規範などの「会社運営基本規定」に基づき、積極的に経営に役立つものである。
2. 情報処理はその遂行にあたり常にその実態を公正かつ的確に掌握し、最適なものである。
3. 情報処理は迅速かつ正確に行う。
4. 情報処理は各種法規を遵守し、あるべき姿を追求する。

第6条(情報処理の原則)

1. 会社の情報処理は会社方針・諸法令に準拠して行う。
2. 会社の情報処理は、適正を期し、不正・脱漏・誤謬等を防止し、継続的・自動的に確認・牽制できる手続きの確立を図る。

第7条(情報処理の統括)

会社の情報処理業務は情報処理統括責任者が統括する。

第8条(情報処理責任者)

1. 情報処理統括責任者は情報・通信担当取締役が担当し、情報処理責任者を統括する。
2. 情報処理業務を行う事業部には情報処理責任者をおく。
   情報処理責任者は事業部長あるいは事業部長が任命した代理者とする。

第9条(情報処理責任者の任務)

1. 情報処理統括責任者は全社の情報処理業務を主掌するとともに情報処理責任者を統括し、会社経営に必要な情報処理業務の遂行および経営体質の改善に努める。
2. 情報処理責任者は、担当事業部の経営に必要な情報処理業務の遂行および経営体質の改善に努める。代理者は事業部長を積極的に補佐する。
3. 社員は情報処理業務において問題あるときは、直ちに所属部門長および情報処理責任者に報告し、その指示を受けるものとする。

第10条(情報セキュリティ委員会)

1. 情報処理統括責任者を支援するため、「情報セキュリティ委員会」を主催する。委員長は情報処理統括責任者とし、委員は各事業部の情報処理責任者で構成する。

第11条(秘密情報管理)

情報処理により取り扱う情報は、「秘密保持規定」の定めによりこれを保持・運用し、漏洩など不測の損害の防止に努める。

第12条(業務効率の推進)

情報処理業務の推進にあたっては、この規定の定める原則を遵守するとともに、常にその経済性・効率性を追求し、業務の効率向上に努力するものとする。

第13条(付属規定)

1. 情報処理業務の共通的な実施基準、標準とすべき手続きについては、情報処理規定集に定める。
2. 個人情報保護、製品開発情報保護等に関し、部署独自のシステム運用を行う場合には、関連規定に準拠した運用基準、手続き等を定める。

第２章　方針・運営管理

第15条(情報システム戦略)

1. 情報処理統括責任者は、会社の全社戦略および事業戦略の実現を推進するために適切な全社情報システム戦略を立案し、その実現に努力するものとする。
2. 情報処理責任者は全社情報システム戦略に基づき、事業部の事業戦略の実現を推進するために適切な情報システム戦略を立案し、その実現に努力するものとする。
3. 情報システム戦略の立案およびその具体化にあたっては、情報処理統括責任者および情報処理責任者は、十分に協議し整合性の維持を図る。

第16条(情報処理の有効性の把握)

情報処理統括責任者および情報処理責任者は、情報処理業務がその業務目的に対して十分に効果的であるかどうかを把握するため、定期的に有効性の把握を行うものとする。

第３章　情報セキュリティの管理

第17条(目的)

情報処理に関わる情報資産を各種の脅威から保護し、安全な情報処理環境を実現する。

第18条(情報セキュリティ管理の原則)

1. 情報セキュリティの管理は経営管理上の重要事項として、その責任と役割を明確にし、具体的かつ適切に行う。
2. 自然発生的な災害・故障および人為的な過失・故意による情報資産への脅威に対して遺漏なく適切な対策を実施し、情報処理の安全性を確保する。
3. 情報セキュリティの管理は守るべき情報資産への脅威の大きさとその対策に要する費用のバランスを考慮し、現実的で適切なものである。
4. 不注意または故意による誤用のリスクに対し、情報システムの運用に際して関係者の職務を分離する。

第19条(情報セキュリティの管理)

情報システムのセキュリティ管理は、「セキュリティ管理規定」および本規定の原則に基づき行うものと

する。

第４章　情報システムの開発、管理・運用

第20条(目的)

1. 方針や戦略から展開された情報システム化計画を具体化し、目標を達成する情報システムを開発する。
2. 稼働中の情報システムを、規模に応じて管理・運用し、情報システムが目標とする機能、効果を継続的に実現する。

第21条(情報システム開発の原則)

1. 対象業務は全面的な見直しを行い、新しい業務プロセスに基づきシステム化する。
2. 開発規模、対象範囲、適用業務に応じた適正な手続きで行う。
3. 関連情報システムとの整合性の維持に配慮する。
4. 利用可能な最適技術を活用する。

第22条(情報システムの開発)

1. 情報システムは「システム開発規定」に定める基本方針に基づき開発するものとする。
2. 開発中の情報システムは、「システム評価規定」に定める基本方針に基づき評価し、必要に応じて対策を講じる。

第23条(情報システムの管理・運用の原則)

1. 情報システムの稼働状況を常に把握し、効果が最大限に発揮されるよう、不断に見直し・改訂を行い、常に最良のレベルに維持する。
2. 環境の変化に遅滞なく対応し、利用者の業務効率向上、会社の業績向上に貢献できるようにする。

第24条(情報システムの管理・運用)

1. 稼働中の情報システムは、「システム管理規定」の基本方針および本規定に定める原則に基づき管理・運用するものとする。
2. 稼働中の情報システムは、「システム評価規定」に定める基本方針に基づき利用者側からの評価を行い、必要に応じて対策を講じる。

第５章　情報資源の管理

第25条(目的)

1. 情報処理を通じて収集・蓄積される情報・データを適切に保管・管理し、会社の業務に有効に活用できるようにする。
2. 情報処理に必要なハードウエア・ソフトウエア等の情報システム資源を適切に管理し有効に活用する。

第26条(情報資源管理の原則)

1. 情報システムを通じて収集・蓄積される情報・データは会社の財産として、その取り扱いは公正かつ有効に行う。
2. 会社の情報・データは全社で共有することを原則とし、その有効活用を図る。

3. 会社の情報・データの内容については、その精度および鮮度の管理に責任を有する部門・部署が明確である。
4. 情報システム資源は情報処理に必要な共通基盤として利用目的に応じて共通化、共有化されるものとする。
5. 情報システム資源は安定的かつ適正なコストで構築・運用される。

第27条(情報資源の管理)
1. 情報・データの管理は「情報・データ管理規定」に定める基本方針に基づき行うものとする。
2. 情報システム資源は「システム資源管理規定」に定める基本方針に基づき行うものとする。

第６章　情報通信ネットワークの管理

第28条(目的)
情報処理業務のために必要な情報通信ネットワークを適切に構築し、常時安定的に利用できるようにする。

第29条(情報通信ネットワーク管理の原則)
1. 会社の情報通信ネットワークは情報流通の要として常時安定的に利用できるよう絶えず最新の動向に注目し、必要な措置を講じる。
2. 情報通信ネットワークの安全性、信頼性、効率性を維持・向上し、情報システムの安定的な稼働に寄与する。
3. 会社の情報通信ネットワークは全社で共有し、その有効活用を図る。

第30条(情報通信ネットワークの管理)
情報通信ネットワークの管理は「通信ネットワーク管理規定」に定める基本方針に基づき行うものとする。

第７章　情報技術の管理

第31条(目的)
情報処理業務に有効に活用できる情報技術を探索し、評価・選択し、導入・定着させる。

第32条(情報技術管理の原則)
1. 情報技術の進展度合い、社会情勢の変化、会社方針の変更など環境の変化に注目し、情報処理業務に適時適切に対応できるように、必要な措置を講じる。
2. 会社の情報技術は全社で共有し、その有効活用を図る。

第33条(情報技術の管理)
情報技術の管理は「情報技術管理規定」に定める基本方針に基づき行うものとする。

第８章　情報処理教育

第34条(目的)
1. 情報処理を方針どおりに遂行するため、情報システム利用者の情報リテラシー（情報セキュリティを含む）能力の向上をはかる。

2. 会社方針や環境変化に対応した情報処理の確立に遅滞なく対処できる情報処理要員の育成を行う。

第35条(情報処理教育の原則)
1. 情報の取り扱い能力は全ての社員が保有すべき基礎能力であり、担当業務に応じた適切な情報リテラシー教育を行う。
2. 情報処理業務を担当する社員は担当業務に応じた専門能力を保有すべきであり、適切な情報処理要員教育を行う。
3. 社員の教育は会社の定める教育関連諸規定を基本とする。情報リテラシー教育および情報処理要員教育については、必要に応じて速やかに関連諸規定、環境を整備し、社員に対する質の高い情報処理教育を行う。

第36条(情報処理教育)
1. 社員の情報リテラシー教育は、「情報処理教育規定」の定める基本方針に基づき行うものとする。
2. 情報処理業務を担当する社員に対する情報処理要員教育は、「情報処理教育規定」の定める基本方針に基づき行うものとする。

第９章　情報処理業務の外部委託管理

第37条(目的)
情報処理業務遂行の能力不足を補い、より効果的に業務を行うために、情報処理業務の一部または全部を外部委託する場合に遵守すべき原則を定める。

第38条(情報処理業務外部委託の原則)
1. 情報処理業務の外部委託は、下記の事項が、社内で実施するよりも同等以上に効率的に達成できる場合に行うものとする。
(1)情報システム資源の能力の不足を補う。
(2)情報処理要員の不足を補う。
(3)情報技術の不足を補う。
(4)情報処理コストの節減をはかる。
(5)所要期間の短縮をはかる。
2. 外部委託を行う際には、委託先が必要な内容について十分に専門性があるかどうかを評価してから委託を行うこと。なお、委託期間が終了した時(期間の定めが長期にわたる時には各期毎)には委託成果・プロセスの評価を「委託評価データベース」に基づいて行い、以降の対策として活用する。
3. 自社内の管理に基づき部分的に外部委託を行うのか、アウトソーシングして全面的に外部能力の活用をするのか、業務の内容と効果、外部能力を勘案し、決定すること。

第39条(情報処理業務の外部委託)
情報処理業務の外部委託は、「情報処理外部委託規定」に定める基本方針に基づき行うものとする。

第 10 章　情報処理費用の課金

第40条(目的)
情報処理に要した費用を受益者に課金し、事業部ごとの損益を明確にする。

第41条（情報処理課金の原則）

情報処理に要した費用は、その受益者が負担する。

第42条(情報処理課金)

課金額は、別に定める「情報処理課金規定」に基づいて算出する。

第 11 章　規定の改廃

第43条（規定の改廃および周知）

1. 本規定は情報処理統括責任者が任命した情報処理責任者が立案し、情報セキュリティ委員会のレビュー、情報処理統括責任者の決定を得て改廃を行う。
2. 第 1 項の決定事項は、これを社内に周知しなければならない。

３．情報セキュリティ委員会規定

情報セキュリティ委員会規定

第１章　 総則

第1条（目的）

この規定は、情報処理全般について、その円滑な運営を規定する「情報処理規定」に基づき、同規定が定める「情報セキュリティ委員会」の適切な運営をはかり、もって適切な情報セキュリティ水準の維持・向上に資することを目的とする。

第2条（基本方針）

1. 本委員会は、情報処理統括責任者を支援することを目的とする。
2. 本委員会の活動にあたり、関連する法令、規定類および各種規則を遵守しなければならない。

第3条（責任の所在）

1. 情報処理責任者は、自らが所管する事業部の情報セキュリティの状況を把握し、万一所管する事業部において、本委員会が定める情報セキュリティ関連事項に反する行為が行われたときは、当該行為に係る責任を負う。
2. 本委員会が定める情報セキュリティ関連事項に反する行為を行った者は、就業規則その他社内規定の定めに則り、その責任を明確にし、厳正な処分を行う。

第２章　実施体制

第4条（実施体制）

1. 本委員会は確実なセキュリティ管理を実現するため，役割・責任を明確化した組織・体制の整備を行うものとし、次のメンバーにより構成する。
   （1）委員長
   （2）委員
   事業部委員、法務担当委員、総務担当委員、人事担当委員
2. 委員長は、以下の役割を担う。
   （1）情報セキュリティの統括責任者として、情報セキュリティの対策状況を統括し必要に応じて経営会議への提言、報告を行う。
   （2）情報セキュリティ管理策の実行を支援するため，必要に応じて委員、セキュリティ管理者およびセキュリティ専門家で構成される情報セキュリティ推進分科会を設置する。
   （3）委員長は、情報処理統括責任者がこれを担う。
3. 事業部委員は、各事業部の情報セキュリティ対策を統括し、委員長と連携して以下の役割を担う。
   （1）各事業部における情報セキュリティに係る諸施策を立案し、本委員会に提言する。
   （2）本委員会の決議に基づき、自らが所管する事業部に対し、情報セキュリティに係る諸施策の実行

を指示する。
(3) 自らが所管する事業部の情報セキュリティ対応状況を把握し、適宜、委員長に報告する。
(4) 事業部委員は、各事業部の情報処理責任者がこれを担う。
4. 法務担当委員は、社内のセキュリティ侵害・事件に対する法的な対応を提言する。
5. 総務担当委員は、事業所への入門・入館・入室に関わる物理的セキュリティ対策を提言する。

6. 人事担当委員は、就業規則の懲戒に関わる提言をする。

第5条(委員会の役割)
情報セキュリティ委員会では次のことを行う。
(1) 会社の情報セキュリティ遵守の現況を審査し、是正措置を検討する。
(2) 社内のセキュリティ侵害・事件などセキュリティ問題の記録を分析し、必要に応じて規定の内容を変更、追加するなど情報セキュリティポリシーの見直しをする。
(3) 情報セキュリティ推進分科会が策定する組織・体制案およびセキュリティ施策を承認し、活動をレビューする。
(4) 事業継続計画を策定し、定期的な訓練、評価、見直しを行い常に実情に合ったものに保つ。
(5) 新しい情報セキュリティポリシーまたは修正されたポリシーを審査し、経営会議に上申する。
(6) その他必要な情報セキュリティ管理活動を各委員に指示する。

第３章　委員会の招集と開催

第6条(委員会の招集と開催)
1. 情報セキュリティ委員会は、委員長がこれを召集する。
2. 情報セキュリティ委員会は、原則として半期に 1 回これを開催する。但し、委員長が、その開催が必要と判断した場合、随時これを開催することができる。

第４章　規定の改廃

第7条(規定の改廃および周知)
1. 本規定は情報処理統括責任者が任命した情報処理責任者が立案し、情報セキュリティ委員会のレビュー、情報処理統括責任者の決定を得て改廃を行う。
2. 第 1 項の決定事項は、これを社内に周知しなければならない。

〔３〕情報管理関連規定

１．セキュリティ管理規定

２．情報・データ管理規定

３．情報技術管理規定

１．セキュリティ管理規定

セキュリティ管理規定

第１章　総則

第1条(目的)

本規定は「情報セキュリティ基本方針」「情報処理規定」に基づき、会社の保護すべき情報資産を特定して管理を着実に行うとともに、有効な活用促進を目的とするものである。

第2条(適用範囲)

本規定は会社の情報資産を管理、利用する全事業部および関連会社、アウトソーシング先に適用する。

第3条(用語の定義)

本規定で用いられる主な用語は、次のとおりとする。

(1)「情報資産」

情報処理により収集・蓄積される情報・データ、情報処理に必要な情報システム資源、情報通信ネットワークそして情報システムの総称

(2)「機密性」

アクセスを認可された者だけが、情報にアクセスできることを確実にすること。

(3)「完全性」

情報および処理方法が正確であることおよび完全であることを保護すること。

(4)「可用性」

認可された利用者が、必要なときに、情報および関連する資産にアクセスできることを確実にすること。

第4条(基本方針)

本規定の基本方針は次のとおりとする。

(1)「秘密保持規定」を初めとする各種規定に示される情報処理の基本精神、「個人情報保護基本法」「不正アクセス防止法」などの法規を遵守する。

(2)会社として保護すべき情報資産は秘密保持規定第2条2項に示す通りである。

(3)情報資産は活用して初めて価値を生むものであるので、むやみに秘密扱いをして可用性を損ねることなく、必要とする人間に早期に引き渡しができるようにする。

(4)セキュリティを考慮しなくてはいけない危険事象(脅威)として、次の各号に掲げる事項を考慮する。

①情報が不正に暴露される。

②情報が改ざん(不正に内容を変更)される。

③情報が妥当な時間内に利用できない。

④情報の処理を実施した利用者が追跡および特定できない。

⑤情報や処理の信頼性が保証できない。

(5)顧客の個人情報については、OECD「プライバシー保護と、個人データの国際流通についてのガイドライン」に従って管理する。また今後施行される法律についても準拠する。具体的な運用に関しては、情報セキュリティガイドラインに従う。

第5条(本規定の効力)

1. 本規定は情報セキュリティの管理に関して遵守すべき基本を定める。個別情報セキュリティの具体的管理規定については別途定める諸規定等に拠る。

2. 本規定に定めのない事項または本規定に拠ることが適切でない事項は、情報処理統括責任者の指示または承認を得て行う。

第6条(情報セキュリティ管理業務)

情報セキュリティの管理業務とは次の各号に掲げるものをいう。

①セキュリティ対策の計画

②セキュリティ対策の構築

③セキュリティ対策の運用

④セキュリティ対策の評価
⑤上記各号に関連する業務

第7条(情報セキュリティの管理責任)
1. 情報処理統括責任者は全社の情報セキュリティについて統括責任を負う。
2. 情報処理責任者は、事業部が管轄する情報セキュリティについての統括責任を負う。
3. 情報通信ネットワークのセキュリティ管理は「情報通信ネットワーク管理責任者」が行う。
4. 情報・データのセキュリティ管理は「情報・データ管理責任者」が行う。
5. 情報システムのセキュリティ管理は「システム開発責任者」、「システム管理責任者」、「サーバー管理責任者」、「データベース管理責任者」が行う。
6. 上記、第2項から第5項の管理者を「セキュリティ管理者」という。

第２章　情報処理統括責任者の責務

第8条(セキュリティ教育の実施)
1. 情報処理統括責任者の主管によりトップマネジメントから利用者に至るまでの全ての情報システム関連者にセキュリティ教育を行う。毎期毎に最低限、次の各号に関してセキュリティ教育を実施し、実施結果は個々の教育履歴として記録していく。
①組織や個人にとってのセキュリティの重要性
②秘匿、保全、可用、追跡、認証、信頼などの面から、情報システムにおけるセキュリティ対策の必要性
③利用者や組織にとってのセキュリティ問題のもつ意味
④情報セキュリティ管理計画
⑤情報の秘密分類
⑥データ所有者の責任
⑦業務実施者の責任
⑧セキュリティ問題発生時の報告
⑨無許可行為の禁止
⑩変更や構成管理
2. 当社の情報システムを利用している限り、第三者であっても同等の教育を実施する。

第9条(セキュリティ訓練の実施)
1.　情報処理統括責任者の主管により、当社ではセキュリティに責任をもつ人に対して、教育と共に訓練を行う。
セキュリティ訓練は以下の人に対して実施する。
・システム開発者
・システム運用者
・プロジェクトやシステムの「セキュリティ管理者」
・セキュリティ対策機能の管理者
2.　訓練の内容として、以下を含める。
・リスク分析
・セキュリティ対策の導入、管理、運用、利用
・セキュリティ問題の検出、報告、復旧

第 10 条(セキュリティ教育・訓練の効果評価)

1. 教育・訓練の主管者である情報処理統括責任者は、実施した教育・訓練の効果を確認し、評価する。効果は、実際のセキュリティ対策の実施状況を定期的に監視・監査することにより評価を行う。
2. 情報処理統括責任者は、効果を評価した教育・訓練の結果を把握し、必要に応じて教育プログラムを変更する。
3. 役員を含む当社社員は、教育を通じてそれぞれの立場で、業務の一環として、セキュリティを意識しなくてはならない。

第３章　セキュリティ管理者の責務

第 11 条(セキュリティ管理者の任務)

1.「セキュリティ管理者」は、守秘する情報資産の機密性・完全性を確保しなくてはならない。また、適切に可用性を維持することにより、必要な情報資産を必要な人に提供できるようにする責任を有する。
2.「セキュリティ管理者」は、会社内および会社の情報資産の利用を認めた関連会社および第三者に対して、セキュリティ管理上の必要な処置をとる。
3.「セキュリティ管理者」は、情報セキュリティ上の問題を認識したときは、直ちに情報処理統括責任者に報告し、その指示を受ける。
この連絡関係を例示すると次のようになる。ここでいう問題とは、狭義のセキュリティの欠陥にとどまらず、ソフトウエア誤動作等も含むものとする。

・社内一般の場合：
業務担当者 ⇔ 業務責任者⇔セキュリティ管理者 ⇔ 情報処理統括責任者

・外部協力企業の場合：
協力先会社責任者 ⇔ 窓口部署セキュリティ管理者 ⇔ 情報処理統括責任者

・顧客関係の場合：
一般の契約顧客 ⇔ サービス提供窓口 ⇔ 窓口部署セキュリティ管理者 ⇔ 情報処理統括責任者

第 12 条(セキュリティ管理者の権限)

「セキュリティ管理者」は、本規定および本規定に関連して制定される諸規定等に規定された権限に基づき、情報資産のセキュリティ管理業務を統括し必要な職能上の指示を与えることができる。

第 13 条(情報資産の価値と脅威の把握)

「セキュリティ管理者」は、各期毎に管理対象となる情報資産の棚卸しを行い、その情報資産の価値を把握し、またその情報資産に対して発生する可能性のある自然発生的な災害・故障および人為的な過失・故意によってもたらされる脅威の大きさと、その影響範囲を把握する。
脅威の把握・分析には本規定に添付する脅威分析シートを利用することを推奨する。

第 14 条(現状のセキュリティ対策の把握)

「セキュリティ管理者」は、各期毎に管理対象となる情報資産のセキュリティ対策の現状（規定・手続きの整備度、情報システムでの実現度、組織・体制の有効性）を分析し、実施できている点および不足している点を把握する。対策については前条でも使用を推奨している脅威分析シートを利用することを推奨する。

第 15 条 （セキュリティに関する技術動向の把握）

1. 「セキュリティ管理者」は情報処理統括責任者と連携して、定期的にセキュリティ管理に必要と予想される技術や製品の動向を把握する。情報技術の把握と展開については、「情報技術管理規定」で詳細を定める。

第 16 条(セキュリティ管理方針の策定)

「セキュリティ管理者」は管理対象となる情報資産の価値とその情報資産に対して発生する可能性のある脅威および現状のセキュリティ対策実施状況を鑑みて、機密性・完全性・可用性および経済性の観点から、実施するセキュリティ管理の基本方針を作成し、各期毎に見直す。

第 17 条(資源調達)

「セキュリティ管理者」は基本方針に基づき、セキュリティ管理を実現する上で必要な情報システム資源・設備の導入を主導する。

アウトソーシングサービスを活用する場合には、秘密保持規定で定められた手順を遵守する。

第 18 条(資源廃棄)

「セキュリティ管理者」は重要な情報を保管した記憶装置に対しては、物理的にデータ域を破壊するか、データ域を確実に上書きした後に処分する。

記憶媒体（ハードディスク等）を内蔵している装置に対して、処分する前にその全ての部品をチェックし、重要なデータやライセンス供与のソフトウエアが、完全に削除または上書き消去されていることを確認すること。

第 19 条(情報秘密分類と管理)

1. 「セキュリティ管理者」は秘密保持規定に基づき、情報資産の秘密分類を行い、資産目録に基づき適正な管理を実施する。
2. 「セキュリティ管理者」は定期的に情報資産の棚卸、秘密分類の見直しを実施する。
3. 情報資産は分類体系に従い、ラベル付けを行う。

第 20 条(建屋の管理)

「セキュリティ管理者」は、情報処理システムの運用に関連している機器・データ・記録媒体・印刷用紙などが保管・管理されている建物および部屋を物理的に管理し、必要に応じて入退室管理を行う。

①情報処理システムの運用上、保護しなくてはならない情報や機器類が存在する部屋、建物への入退出を事前に許可された者だけに制限する。また入退室を記録し保管する。

②管理対象の部屋および建物からの情報処理機器・データ・記憶媒体・印刷用紙などの持ち出し、持ち込みは事前に許可された者だけに制限すること。また持ち込み、持ち出しの記録をとり保管する。

③管理対象の部屋および建物への不正な侵入がないことを確認する手段を設ける。また、不正な侵

入が発生した場合にそれを追跡する手段を設ける。
④電磁波放射によるデータの盗聴を防止する。
⑤物品搬入時の受け渡し場所は情報処理施設／設備から隔離し、必要に応じ入退室を記録し、保管する。

第 21 条(周知・公報・教育)
「セキュリティ管理者」は、セキュリティ対策を実現する上で必要なルール・ガイドを情報システムの管理者・利用者に周知・公報し、必要に応じて教育する。

第 22 条(運用と変更管理)
1.「セキュリティ管理者」は、その管理範囲においてセキュリティ対策を円滑に運用する。
2.「セキュリティ管理者」は、システムの重要な変更について次の内容を遵守する。
①システム運用プログラムを変更した場合には、全ての関連情報を含む監査ログデータを採取し、保管する。
②運用とアプリケーションの変更手続きは一体とし、重要な変更の識別と記録を補完する。
③事前に変更が与える影響を評価し、認可の手続きに沿って認可を受けた上、変更の詳細を関係者に通知する。
④変更の中止、好ましい結果にならなかった変更の回復に対する責任を明らかにし、すみやかに対応と周知を行う。
3.「セキュリティ管理者」は、システムの保守において、次の内容を遵守する。
①システムの決められた整備間隔および仕様に従ってメンテナンスを実施する。
②メンテナンスは、事前に許可された者のみに制限する。
③メンテナンスの内容を記録し、保持する。
④メンテナンスのために、装置を敷地外に持ち出す場合は、適切な管理策を実施する。

第 23 条(セキュリティ問題の管理)
1. セキュリティ問題の発生の報告を受けた「セキュリティ管理者」は、対応が完了した後、事象の内容、対応などについて情報セキュリティ委員会へ報告を行う。
報告すべき内容は、少なくとも下記の内容を含む。
発生日時、検出者、担当「セキュリティ管理者」、対応実施者、発生システム、業務への影響、復旧作業の内容、復旧作業に要した工数
2. 報告を受けた「セキュリティ管理者」は、セキュリティ問題が発生したシステムへのアクセスログなど不正アクセスの証拠となる情報は、外部磁気記録媒体などに保管する。
3. セキュリティ問題の報告を受けた「セキュリティ管理者」は、情報処理統括責任者に報告を行った上、専門家組織への届け出を行い、必要に応じて対応の助言を得る。報告および助言を受ける専門家組織については、情報システムガイドラインに従う。
4.「セキュリティ管理者」はサービス利用者に報告されたセキュリティ問題につき、迅速かつ適時報告する。

第 24 条(秘密保持契約)
「セキュリティ管理者」はシステム利用者に不正アクセスの禁止条項を折り込んだ、秘密保持誓約書を提出させる。

第 25 条(関連会社・第三者への義務)

1.「セキュリティ管理者」は、セキュリティ管理のルール・ガイドに定められた必要事項を、システムの利用を希望する関連会社および第三者へ提示し、遵守させる。

2.「セキュリティ管理者」は、関連会社および第三者がセキュリティ管理の関連規定に対する違反を行った場合は、直ちに必要な処置をとる。

3.「セキュリティ管理者」は、関連会社および第三者との間で秘密保持規定に順ずる内容を秘密保持契約として取り交わす。

4.「セキュリティ管理者」は、システムの利用を希望する関連会社および第三者に対して、第 31 条、第 32 条に従い定期的にセキュリティ管理の監査を実施する。

第 26 条(アウトソーシング)

情報システム、情報資産の管理、運用をアウトソーシングする場合、当該事業部の情報処理責任者は、アウトソーシング先との間で、秘密保持規定に順ずる内容を秘密保持契約として取り交わす。詳細は情報処理外部委託規定第3章に従う。

第 27 条(評価の実施)

「セキュリティ管理者」は、セキュリティ対策が正しく運用されているか、環境変化による見直しが必要か否かを各期毎に評価し、情報処理統括責任者に報告する。

第４章　情報システム利用者の責務

第 28 条(情報システム利用者の義務)

1. 情報システムの利用者は、「セキュリティ管理者」が定めたセキュリティ管理のルール・ガイドを遵守する。

2. 情報システムの利用者にセキュリティ管理のルール・ガイドラインに違反した行為があった場合は、関連規定に定める罰則が適用される。

3. 情報システムの利用者は、本規定の上位標準である秘密保持規定などの規則、情報セキュリティガイドラインなどの全社共通規則、ガイドに従って個々の責務を果たす。

4. 情報システムの利用者は、「セキュリティ管理者」が実施する利用者教育を定期的に受講し、セキュリティ意識の向上に努める。

第 29 条(資源移動)

装置、情報、ソフトウエアは、「セキュリティ管理者」の許可なしに指定場所から持ち出さない。「セキュリティ管理者」は、許可を与えるときには、持ち出しと返却の記録をとり、保持する。また、定期的に記録に基づき、棚卸を実施する。

第 30 条(セキュリティ問題発生への対応)

セキュリティ欠陥、ソフトウェア誤動作、セキュリティ事故を検出したものは、直ちに業務を中止して「セキュリティ管理者」への報告を行い、指示に従って行動する。

第５章　内部監査室の責務

第 31 条(監査の実施)

1. 内部監査室は、定期的に各事業部、本社部門のセキュリティ管理の監査を行う。監査結果は、情報セキュリティ委員会に報告する。
2. 情報セキュリティ委員会は、報告を受けた監査結果のフォローアップを確実に行う。
3. 監査の具体的な運用については、情報セキュリティガイドラインに従う。

第 32 条(改善勧告の実施)
1. 内部監査室は、各事業部、本社部門のセキュリティ監査結果に基づいて、当該事業部、本社部門へ改善勧告を行う。
2. 各事業部、本社部門は、セキュリティ監査の改善勧告に基づきセキュリティ管理の改善計画を立案し、内部監査室および情報セキュリティ委員会に報告する。
3. 各事業部、本社部門は改善実施後、内部監査室により再監査を受ける。
4. 内部監査室は、各事業部、本社部門のセキュリティ監査結果に基づく、当該事業部、本社部門の改善勧告の実施についてフォローアップを確実に行う。

第６章　規定の改廃および周知

第 33 条(規定の改廃および周知)
1. 本規定は情報処理統括責任者が任命した情報処理責任者が立案し、情報セキュリティ委員会のレビュー、および経営会議の承認を得て、改廃を行う。
2. 第1項の決定事項は、これを社内に周知しなければならない。

２．情報・データ管理規定

情報・データ管理規定

第１章　総則

第1条(目的)

本規定は「情報処理規定」に基づき情報システムを通じて得られる情報・データ(以下「情報・データ」という)を、会社の経営目標を達成するために効果的に活用できるよう、その管理の基本を定める。

第2条(適用範囲)

本規定は会社における全ての「情報・データ」の管理に適用する。

第3条(用語の定義)

本規定で用いられる主な用語の意味は、次のとおりとする。

(1)情報・データ

「情報・データ」とは情報システムを通じて得られるコンピュータに認識できる形式で表現された全ての情報の総称をさす。

第4条(基本方針)

「情報・データ」の管理に関する基本方針は以下のとおりとする。

①「情報処理規定」に示された情報資源管理の原則を遵守する。

②会社の「情報・データ」は会社全体の重要な資源であり、常にその共有化・有効活用を推進する。

③「情報・データ」の効力を最大限に発揮できるように、その状態を最適に維持・管理する。

第5条(本規定の効力)

1. 本規定は会社の「情報・データ」に関して遵守すべき基本を定め、具体的な管理内容については別途定める諸規定等に拠る。
2. 本規定に定めのないものまたは本規定に拠ることが適切でないものについては、情報処理統括責任

者の指示または承認を得て行う。

第6条(情報・データの所有者)

1. 「情報・データ」の内容については、その維持・管理および精度に関する責任を有する部門・部署が明確でなければならない。
2. 「情報・データ」の内容の維持・管理責任を有する事業部長を情報・データの所有者（以下「情報所有者」という）という。

第7条 (情報・データ管理責任者)

1. 情報処理統括責任者は「本社情報・データ管理責任者」を任命する。
2. 事業部の情報・データ管理業務の責任は、当該事業部の「情報処理責任者」、または当該事業部長の任命する者が負う（以下「事業部情報・データ管理責任者」という）。
3. 情報処理責任者は情報処理統括責任者と連携し、次条に定める任務を遂行する。
4. 事業部あるいは本社をつけずに、単に「情報・データ管理責任者」という場合は、「事業部情報・データ管理責任者」と「本社情報・データ管理責任者」の両者をさす。

第8条(情報・データ管理責任者の任務)

1. 「本社情報・データ管理責任者」は全社レベルで「情報・データ」を安全かつ効率的に利用するための諸施策の立案・実施を、「事業部情報・データ管理責任者」とともに推進し、「情報・データ」の活用度向上を主導する。
2. 「事業部情報・データ管理責任者」は事業部レベルで「情報・データ」を安全かつ効率的に利用するための諸施策の立案・実施を、情報所有者とともに推進し、「情報・データ」の活用度向上を主導する。
3. 「情報・データ管理責任者」は、業務遂行上問題が発生した時は直ちに情報処理責任者に報告し、その指示を受けなければならない。

第9条(情報・データ管理責任者の権限)

「情報・データ管理責任者」は、本規定および本規定に基づき制定される諸規定等に規定された権限に基づき情報・データ管理業務を統括し必要な職務上の指示を与えることができる。

第 10 条(秘密保持)

情報・データ管理においては、「セキュリティ管理規定」を遵守し、不測の損害の防止に努めなければならない。

第２章　情報・データの収集･蓄積

第 11 条(情報・データ形態の最適化)

1. 情報システムを開発し、「情報・データ」をデータベース等に蓄積する場合は、共有化・有効活用が容易に行えるように可能な限りその形態を最適化する。
2. 「情報・データ管理責任者」は、情報所有者とともに、会社の「情報・データ」の共有化・有効活用のために適切なルールを定め「情報・データ」の形態の最適化を推進する。

第 12 条(情報・データの整備)

会社の「情報・データ」を有効に活用するためには、漏れや重複がなく、内容の正確性も確保されている必要がある。このために以下の事項を実施する。

①「情報・データ管理責任者」は情報所有者とともに、会社に有効な「情報・データ」について、漏れや重複をなくし、内容の正確性を保証し、共有化・有効活用が容易に行えるような施策の立案、推進を主導する。

②「情報・データ管理責任者」は「システム開発責任者」、「システム管理責任者」と連携して「情報・データ」の整備に努力する。

第 13 条(情報・データの保管)

情報所有者は、「情報・データ管理責任者」とともに、会社にとって有効な「情報・データ」ごとに適切な保管期間の基準を設け、「情報・データ」の保管を行う。

第 14 条(情報・データの廃棄)

1. 電子情報保存媒体を廃棄する際には、必ず記憶データの初期化処理を行ってから廃棄処分をする。電子情報保存媒体の取り扱いは本規定第 16 条、第 17 条の定めに従う。
2. 社内ネットワークシステムで使用する全ての媒体の処分に関しては、格納されている情報の秘密分類に応じて正確な処分を行う。重要なものの処分については、監査証跡を残すために記録をしておく。

第３章　情報・データの利用

第 15 条(情報・データの利用)

1. 「情報・データ管理責任者」は情報所有者とともに、社員が会社の「情報・データ」を利用し業務に活用できるよう、必要な施策を立案・実施する。
2. 社員が業務遂行上の必要性から会社の「情報・データ」を利用する場合は、「セキュリティ管理規定」および関連諸規定等に規定されたセキュリティに関する項目を遵守しなければならない。

第 16 条(情報・データの社外利用)

社員が会社の「情報・データ」を、所定の手続きで利用を許されて携帯または社外設置の情報処理機器や電子情報保存媒体にコピーし、会社指定の事務所以外（以下「社外利用」という）で利用する場合は次の各号に拠る。

①原則として必ず事前に所属長の承認を受ける。

②「情報・データ」の社外利用を行う者は定められた手順を厳守し、事故等が発生した場合は直ちに所属長に報告し、適切な処置をとらなければならない。

③「セキュリティ管理規定」および関連諸規定等に規定されたセキュリティに関する項目を遵守する。

④前項に違反した場合は、就業規則に基づき相応の罰則を課す。

第 17 条(システム文書の管理と利用)

システム文書(処理プロセス、データ構造、認可プロセスなど)については、特に厳正な保管を行わなくてはならない。システム文書へのアクセスできる者は、情報システム部の担当者と業務部門の責任者だけに限定する。公衆ネットワークで保持されるまたは供給されるシステム文書は、機密性と完全性を検討しこれを確保する。

第 18 条(情報・データの外部への提供)

会社の「情報・データ」を電子情報保存媒体等にコピーし社外の者に有償または無償で提供する場合は、定められた手続きに従い所属長の許可を受けなければならない。秘密を要する情報・データを提供する場合は、秘密保持規定に順ずる内容を秘密保持契約として取り交わす。

第４章　情報・データの保全

第 19 条(バックアップ取得の原則)

1. 「情報・データ」については災害、故障、過失、故意による破壊・削除・改ざん等に備え、その重要度等に応じ定期的にバックアップデータを取得しなければならない。
2. バックアップ手順、頻度、保管方法については、「情報・データ」の重要度に適合したものでなければならない。
3. 前項を実施するにあたっては「セキュリティ管理規定」および関連諸規定等に規定されたセキュリティに関する項目を遵守しなければならない。

第 20 条(バックアップ、復元手順の明確化)

「情報・データ」のバックアップおよびその復元手順は文書化し、必要な時にはいつでも参照できるようにし、作業担当者には十分な教育・訓練が実施されなければならない。

第 21 条(バックアップ媒体の保管・取り扱い)

1. バックアップ媒体はその他の電子媒体と同様に権限を与えられた者だけが取り扱いできるようにしておかなければならない。
3.　保管・取り扱いの手順は「セキュリティ管理規定」および関連諸規定等に規定されたセキュリティに関する項目に準拠しなければならない。

第 22 条(移送時の媒体の取り扱い)

バックアップデータの移送など秘密データを移動するときは、盗難や漏洩、改ざんを防止するため必要な措置を施さなければならない。具体的な措置については、情報セキュリティガイドラインに従う。

第 23 条（入力データの扱い)

業務システムに入力されるデータの正確性を保証するために、業務アプリケーションは適切な管理策を実装しなければならない。具体的な管理策についてはシステム開発規定に従う。

第５章　規定の改廃および周知

第 24 条(規定の改廃および周知)

1. 本規定は情報処理統括責任者が任命した情報処理責任者が立案し、情報セキュリティ委員会のレビュー、および経営会議の承認を得て、改廃を行う。
2. 第1項の決定事項は、これを社内に周知しなければならない。

［参考資料］

重要なバックアップデータの保護ルール（事例）

社内情報サーバーで管理されている運用ソフトウエア、事業部情報、顧客情報は、下記の規則に従ってバックアップする。

①バックアップコピーは毎日採取する。

②バックアップ媒体は、DAT を使用する。チャネル装置は二重化しておく。

③個々のシステムのバックアップ装置は1カ月に1回検査し、業務継続計画の要求事項に適合していることを確認する。

④運用ソフトウエア、事業部情報、顧客情報のバックアップ媒体は、バックアップコピーについての正確な記録と復旧手続書といっしょに、1カ月に1回、外部バックアップセンターに送付し、保管しておく。

⑤社内情報サーバーの業務アプリケーションについては、少なくとも、3世代のバックアップデータを保持する。

⑥バックアップデータは暗号化し、データの内容がわかるようなラベルは添付しない。媒体の物理管理は、説明書に記載の事項を遵守する。

⑦メインサイトで媒体に対して実施する管理対策と同等の管理対策を、外部バックアップセンターにも適用する。

⑧バックアップ媒体は、毎月、読めることを確認する。1年に1回、復旧手順のチェックとテストを実施し、手順の有効性と、復旧が規定の時間内に完了することを確認する。

３．情報技術管理規定

情報技術管理規定

第１章　総則

第1条(目的)

本規定は「情報処理規定」に基づき情報処理の基盤となる情報技術の管理に関する基本を定め、会社の情報処理の信頼性・安全性・効率性の向上に寄与する。

第2条(適用範囲)

本規定は会社の全部署の情報処理業務に関わる情報技術管理に適用する。

第3条(用語の定義)

本規定で用いられる主な用語は、次のとおりとする。

(1)「情報技術」

会社の情報処理を遂行する上で必要となるハードウエア・ソフトウエア・ネットワークの知識およびその利用技術をいう。

第4条(基本方針)

情報技術管理の基本方針は次のとおりとする。

①「情報処理規定」に示された情報処理の規定に則る。

②世の中の情報技術の動向・進展度合い、会社の情報システム要件の変化などを遅滞なく捉え、常に適切な情報技術の収集・蓄積・活用促進をはかる。

③収集・蓄積・活用促進した情報技術は、必要に応じて再利用できるように管理し、共有化を推進する。

④各種法規を遵守し、既定の規定との整合性を保ち、最適化を追求する。

第5条(本規定の効力)

1. 規定は情報技術の管理に関して遵守すべき基本を定め、具体的な管理内容については別途定める諸規定等による。

2. 本規定に定めのない事項または本規定に拠ることが適切でない事項は、情報処理統括責任者もしく

は情報処理責任者の指示または承認を得て行う。

第6条（情報技術管理業務）

情報技術管理の業務は次の各号に掲げる。

①情報技術の収集
②情報技術の評価・選定
③利用技術の標準作成・維持
④情報技術の利用支援
⑤情報技術・利用技術の共有化
⑥情報技術・利用技術の活用状況の評価
⑦上記各号に関連する業務

第7条（情報技術管理責任者）

1. 情報処理統括責任者は、情報技術を効率的に管理するために「情報技術管理責任者」を任命する。
2. 「情報技術管理責任者」は、下記、第3項から第6項までの統括管理責任を負う。
3. 「情報・データ」の情報技術管理は、「情報・データ管理規定」に定める「情報・データ管理責任者」が行う。
4. 情報システム資源の情報技術管理は「システム資源管理規定」に定める「情報システム資源管理責任者」が行う。
5. 情報通信ネットワークの情報技術管理は「通信ネットワーク管理規定」に定める「情報通信ネットワーク管理責任者」が行う。
6. 情報システムの情報技術管理は「システム開発規定」に定める「システム開発責任者」、「システム管理規定」に定める「システム管理責任者」、「サーバー管理規定」に定める「サーバー管理責任者」、「データベース管理規定」に定める「データベース管理責任者」が行う。

第8条（情報技術管理責任者の任務）

1. 「情報技術管理責任者」は、情報技術の収集・蓄積・共有化を推進し、会社の情報処理の信頼性・安全性・効率性に貢献する責任を有する。
2. 「情報技術管理責任者」は、管理業務において問題あるときは、直ちに情報処理責任者に報告し、その指示を受ける。

第9条（情報技術管理責任者の権限）

「情報技術管理責任者」は、本規定および本規定に基づき制定される諸規定等に規定された権限に基づき、情報技術の管理業務を統括し必要な職務上の指示を与えること。

第 10 条（秘密保持）

情報技術の管理においては、「セキュリティ管理規定」を遵守し、不測の損害の防止に努めなければならない。

第 11 条（業務効率の推進）

情報技術管理にあたっては、この規定の定める基本原則を遵守するとともに、常にその経済性を追

求し、管理業務の効率向上に努力する。

第２章　情報技術の管理

第 12 条(情報技術の収集)

1.「情報技術管理責任者」は、会社の情報処理に活用されている既存の情報技術を常に把握する。

2.「情報技術管理責任者」は、世の中の情報技術の動向・進展度合い、会社の情報システム要件の変化などの環境変化を常に把握する。

3.「情報技術管理責任者」は、上記第 1 項、第 2 項で把握した情報に基づき情報技術の「収集・蓄積・活用促進・共有化推進」の計画を立案する。

第 13 条(情報技術の評価・選定)

「情報技術管理責任者」は、情報処理の目的を達成するために必要な情報技術を以下の観点で評価し、選定する。

①既存の情報技術活用の可能性・妥当性。

②当該情報技術の世の中の技術動向・進展度合いから見た将来性・先進性

③当該情報技術の世の中の標準への適合性

④当該情報技術の情報処理目的への適合性

⑤当該情報技術の費用対効果の観点から見た経済性

⑥当該情報技術の導入に必要な納期・工数から見た適切性

⑦当該情報技術の他の情報処理へ再活用・展開の可能性

⑧当該情報技術の類似の他の情報技術との比較による第2項から第7項までの優位性

第 14 条(利用技術の標準作成・維持)

「情報技術管理責任者」は、情報技術の利用を効率的に行うために、当該情報技術の利用技術に関する情報セキュリティガイドラインの他に、マニュアル・ノウハウ集・Q＆A集等を作成・収集し、維持する。

第 15 条(情報技術の利用支援)

1.「情報技術管理責任者」は、前条で作成した利用技術情報を、情報技術の利用者へ周知しなければならない。

2.「情報技術管理責任者」は、必要に応じて利用者からの問い合せ対応等の体制を整備し、利用支援を行う。

3. オペレーティングシステムの変更に際しては、利用技術情報を駆使して最適なものの採用を推進・支援する。導入に際しては運用やセキュリティに悪影響がないことを確認するために、業務システムをレビューしてテストを行う。

4. ソフトウエアパッケージの変更に際しても、利用技術情報を駆使して最適なものの採用を推進・支援しなくてはならない。ソフトウエアパッケージは変更の必要が明確でない場合は変更せずに旧来のものを継続使用することを原則とする。変更の必要が明確な場合は、変更に伴うリスク分析を行ってその結果を関係者にレビューし、「システム管理責任者」の承認のもとで変更を行う。

5. 新規情報技術の導入時には、十分なレビュー、テストを済ませた後に変更通知を行い利用者に徹底をし、実施する。旧バージョンソフトウエアとオリジナルソフトは明確に識別して保管することにより、不測の事態に備えることとする。

第 16 条(情報技術・利用技術の共有化)

「情報技術管理責任者」は、情報技術およびその利用技術に関する情報を体系化し、必要に応じて再活用できるように整備し、共有化を推進しなければならない。

第 17 条(情報技術・利用技術の活用状況の評価)

1. 「情報技術管理責任者」は、情報技術およびその利用技術に関する情報の活用状況を評価し、必要に応じて活用促進のための方策を講じなければならない。
2. 情報処理技術の変化およびその影響については、毎年秋期を目処にレポートを作成し、翌年度の予算策定時のガイドとして情報提供を行う責務を負う。

第３章　情報セキュリティに関連する情報技術管理

第 18 条(システム文書の取り扱い)

1. 業務処理プロセス、データ構造、認可システムなどシステム文書に該当するものは、「システム管理者」の責任のもと、安全に管理すること。
2. システム文書へのアクセスは、承認された情報システム部の担当者と業務部門の「システム管理者」のみに限定する。
3. 「システム管理者」は、公衆ネットワークを経由して得られるシステム文書に関しても機密性と完全性を確保すること。

第 19 条(システムファイルのセキュリティ)

1. OS、ミドルウエア、業務アプリケーション、利用者プログラムなど、システムファイルへのアクセスは承認された情報システム部担当者など、限定された関係者が行う。
2. プログラムソースライブラリへのアクセスに関してはすべての監査ログを保持しておく。
3. 保持の期間については個々のシステムごとに設定が可能であるが、設定がない場合は保持期間を２カ月間とする。

第 20 条(暗号技術の使用)

1. 情報システム部は国際標準、業界標準に基づき暗号アルゴリズム、暗号鍵長などの暗号機能を導入し、社内に展開する。暗号機能については、情報システム部が定めたものを使用すること。個人の判断で暗号機能を導入・使用してはならない。
2. 秘密分類の極秘、秘情報について通信回線を用いて社外に転送することは原則として禁止する。転送しなくてはならない場合は情報システム部の許可を得なくてはならない。転送の場合および記憶媒体に保管する場合は暗号機能を用いて秘匿性と保全性を確保しなくてはならない。

第 21 条(デジタル署名と暗号鍵)

1. 情報システム部はデジタル署名の技術動向、運用動向を把握し、社内システムへの展開を推進する責務を負う。デジタル署名の法的な拘束力や国際的な動向について継続的に状況を把握し、秘密保持と効率運営に足る環境を検討する。
2. 暗号鍵については、必要に応じて公開鍵証明書を作成して使用すること。秘密鍵の安全性にも十分配慮し、鍵の有効期限設定やアーカイブ設定を行わなくてはならない。

第４章　規定の改廃および周知

第 22 条（規定の改廃および周知）

1. 本規定は情報処理統括責任者が任命した情報処理責任者が立案し、情報セキュリティ委員会のレビュー、および経営会議の承認を得て、改廃を行う。
2. 第1項の決定事項は、これを社内に周知しなければならない。

〔４〕システム開発・運用関連規定

１．システム開発規定

２．システム評価規定

３．システム管理規定

４．サーバー管理規定

５．データベース管理規定

６．通信ネットワーク管理規定

７．システム資源管理規定

１．システム開発規定

システム開発規定

第１章　総則

第1条(目的)

本規定は「情報処理規定」に基づきシステムの開発に関する基本を定め、システム開発時の信頼性・

安全性・効率性の向上に寄与する。

第2条（適用範囲）

本規定は当社がコンピュータシステムを利用して業務の改革・改善する場合に、システムの開発または導入を効果的に行うために適用する。

第3条（基本方針）

システム開発の基本方針は次のとおりとする。

(1) 「情報処理規定」の精神に則り、効果的で効率的かつ安全性の高い開発を行う。

(2) 開発の基準は、当該業務に法的な規制がある場合はそれに従い、ない場合は本規定を基本として自主的に定める。

(3) 開発の項目は、システム規模に応じて、大規模なシステムは詳細に、小規模なシステムには必要な項目を選択して適用するなど、適時適切（スケーラブル）な適用を心がける。

(4) 開発作業には、利用部門・システム部門双方が参加して、業務に適用して効果が上がるように心がける。

(5) ソフトウエアの開発を外部委託するか、もしくは市販のパッケージソフトウエアを導入する場合は、本規定の必要な部分を適用して判断する。

(6) 開発にあたっては手順書を作成しておく。手順書はできうる限り、ISO12207、IEEE730-2002、ISO9001-2000、ISO10006 などの標準的な開発方法論から取り入れること。

第4条（役割と責任）

会社はシステムの開発にあたっては、開発作業を効果的に行うために役割と責任を明確にする。

(1) 情報処理統括責任者はシステムの開発および開発規定の管理のために情報システム部門の長を開発責任者に任命する。開発責任者はシステムの開発を効果的・効率的かつ安全で信頼性を確保できるように行うために、開発のプロジェクトを組織する。開発責任者はシステム開発の全ての責任を負う。

(2) 開発責任者は開発作業を効率的に進めるために事務局を設置する。事務局は開発責任者の業務をサポートすると同時に、開発責任者からの委任があれば、責任者の行為を代行する。

(3) システム部門がシステム開発を行う場合は、プロジェクト責任者を設置する。プロジェクト責任者はシステム開発または導入過程のすべてに責任を負う。プロジェクト責任者はシステム開発を行うために要員を組織化する。

(4) 利用部門がシステム開発を行う場合は、プロジェクト責任者を設置する。プロジェクト責任者は利用部門の要求仕様の実現に責任を負う。プロジェクト責任者はシステム開発をシステム部門と共に行うために要員を組織化する。

(5) 監査部門は、必要に応じてシステム開発の過程を監査し、経営者に報告する。

(6) システムの開発を外部に委託する場合、もしくは市販のパッケージを購入する場合も、同様に責任者と担当者を設置する。外部業者の実体・実績の監査は責任者が指名したものが行い、導入時に業務に支障がないよう十分評価を行う。

第２章　企画・設計

第5条（企画の申請・承認）

システムを企画する際、企画提案部署は以下の事項を決定する必要がある。

(1) システムの企画が経営戦略に沿っていることを確認すること。
(2) システムの企画は経営者による承認を得ること。
(3) システムの使用目的を明記すること。
(4) システムの実現効果、概要、方針を明記すること。
(5) システムの要件を明記した要求仕様を提示すること。
(6) 企画をまとめるに当たって、必要に応じて予備調査・分析などを行っておくこと。
(7) 実現期限、投入可能なリソース、負担可能な予算の上限を明確にすること。

第6条(開発計画)

システム開発計画は、システム開発の計画段階で立案し、開発責任者の承認を得る。以下の事項を決定する必要がある。
(1) 要件定義、設計、開発、評価、稼動開始等各段階の実施時期を明確にすること。
(2) セキュリティ対策方針に基づき、要求仕様を満たすセキュリティ仕様を明確にすること。
(3) 組織内での開発実施体制を明記すること。少なくとも、開発責任部署と開発責任者、運用保守責任部署と運用保守責任者を明確にすること。
(4) システムを自社内で開発する場合は、開発のための手順書および要員管理の基準を定めること。
(5) システムの実現形態と実現方式を明確にすること。
(6) 開発環境、試験環境、運用環境を分離できるように検討すること。
(7) 外部委託者を受け入れて開発する場合は、情報処理外部委託規定に準拠すること。
(8) 暗号機能を組み込む場合は、暗号管理規定を参照すること。

第7条(要件定義)

新しいシステムに関する、または既存のシステムの改善に関する要件定義を行い、開発責任者の承認を得る。以下の事項を決定する必要がある。
(1) ユーザー部門の要求仕様を網羅していること。
(2) システム実現に必要な機能を抽出すること。
(3) セキュリティ対策の方針を満たした機能を抽出すること。
(4) 必要に応じてユーザーをユーザーID 単位で識別可能とすること。
(5) ユーザーの要求に対し、アクセスコントロールが可能なように検討すること。
(6) 必要に応じてハードウエア自体を認証し、識別可能とすること。
(7) 取扱いに注意すべき情報保護のため、暗号化を検討すること。
(8) システムの中で暗号化すべき部分を抽出し、部分ごとに暗号化の方針を決定すること。
(9) デジタル署名を使用する際は秘密鍵の機密性と公開鍵の完全性を保護すること。)
(10) 電子契約や電子支払い、デジタル署名の使用などで発生する紛争を解決することが必要な場合、否認拒否サービスを使用すること。
(11) ソフトウエアパッケージを使用する場合は、パッケージがユーザーの要求仕様をどの程度充足しているかを HIT/GAP 分析で確認しておくこと。
(12) ソフトウエアパッケージを使用する場合は、カスタマイズ(変更)をせずに継続使用できるという観点を考慮して選定すること。
(13) ソフトウエアパッケージを使用する場合は、パッケージを適用する分野での導入実績を評価しておくこと。

(14) ソフトウエアパッケージを使用する場合は、既存導入ユーザー企業がある場合、見学などして実績を確認しておくこと。
(15) ユーザーの要求仕様で見送った案件、変更した案件は記録として残しておくこと。

第8条(設計)

前条で抽出した要件に基づき、下記のように各部品について設計する必要がある。各仕様は各段階において開発責任者の承認を得る。

8.0(運用方案設計仕様)

システムの運用・保守に必要な機能を設計する際に満たすべき事項を定義する。なお、開発責任者の承認を得る前に運用保守責任者の承認を得るものとする。

(1) 業務運用に必要な要件を洗い出し、定義しておくこと。
(2) 年間運用の基本方針に必要な要件を洗い出し、方針を定義しておくこと。
(3) バックアップ(複製保管)／リストア(復旧)／アーカイブ(保存)に必要な要件を洗い出し、その基本方針を定義しておくこと。
(4) バックアップ(複製保管)保存方法、バックアップのリストア(復旧)手順、アーカイブ(保存)方法、災害時の復旧手順について検討しておくこと。
(5) 業務継続性を鑑み、災害時の業務の復旧手順、情報資産の盗聴・破壊・流出発生時の手順などについて、検討しておくこと。
(6) 業務要求の変化への対応、技術革新などによる恩恵を受けるために、システムの保守・改善の基本方針を定義しておくこと。
(7) 運用・保守の概要は利用部門にレビューし、確認を取っておくこと。

8.1(ハードウエア設計仕様)

システム開発に必要なハードウエアを設計する際に満たすべき事項を定義する。

(1) ハードウエアが継続的に使用し、保守を受けられる可能性を確認すること。
(2) システムの信頼性および性能について確認・評価しておくこと。
(3) 既存のインフラとの親和性を確認・評価しておくこと。
(4) 新規開発部分の設備と現状運用されている部分の設備を区分した上で設計を行うこと。)
(5) 端末の接続が発生する場合、端末の真正性を自動確認できるよう検討すること。
(6) ハードウエア仕様が業務要件やソフトウエア仕様を満たすように設計すること。
(7) ハードウエアの設計に当たっては、電源容量、発熱容量、あるいはセキュアな設置環境など設置環境面を考慮すること。
(8) CPU、メモリー、ディスク容量等、ハードウエアの部品について、監視の仕組みを組込み、資源管理可能な状態にすること。

8.2(ソフトウエア設計仕様)

システム開発に必要なソフトウエアを設計する際に満たすべき事項を定義する。

(1) ソフトウエアはユーザー要求を満たしていること。
(2) ネットワーク接続や経路を制御可能な機構を備えていること。
(3) ソフトウエアへのアクセス制御を適切に実現すること。
(4) ソフトウエアが管理する各情報へのアクセス制御を備えていること。

(5) 入力データの妥当性を確認する機構を備えていること。
(6) 入力データの処理エラーや故意の入力データによる改竄からデータやシステムを保護する機構を備えていること。
(7) ソフトウエアパッケージを利用の場合は、セキュリティ要件を満たしているかの評価を行うこと。
(8) ユーザー要求を実現できなかった案件、内容を変更した案件は記録として残しておくこと。
(9) 開発ソフトウエアがネットワークを通じて外部に接点を持っている場合（オープンシステム）、DoS攻撃、ウィルス、盗聴、ワーム攻撃、データ書き換えなどの外部セキュリティを十分考慮すること。

8.3（ソフトウエアモジュール設計仕様）

システム開発に必要なソフトウエアモジュールを設計する際に満たすべき事項を定義する。
(1)モジュールは原則として各モジュール自身の独立性を維持可能な単位まで分割すること。
(2) 認証情報とネットワーク情報を正しく取り扱えるようにすること。
(3) モジュール同士の結合度を考慮し合理的に配置すること。
(4) 取り扱うメッセージの真正性を確認するアルゴリズムを備えていること。

8.4（ネットワーク設計仕様）

システム開発に必要なネットワークを設計する際に満たすべき事項を定義する。
(1) ユーザーのアクセス制御を適切に行うこと。
(2) アクセス制限をかけるべきグループごとにアクセス制限を行っていること。
(3) 重要なアプリケーションへのネットワーク接続、セキュリティ管理範囲外部からのアクセスに対するアクセス制御をより厳格に行うこと。
(4) 遠隔ユーザーからのアクセスに対してはユーザー自体の真正性ないしはユーザーの接続元ノードの真正性を確認できる方式を検討すること。
(5) ユーザーが多様なアクセス経路からアクセスを行わないよう、不明なアクセス元からの経路を制限できるように検討すること。
(6) 発信源と宛先のアドレスチェック等に基づいたアクセス経路制御を行うよう検討すること。
(7) ネットワークサービスを利用する場合、サービス独自のセキュリティを提供していることがあるので、各サービスのセキュリティについて、サービス提供元からの説明を受けること。
(8) ケーブルを使用しての通信傍受を受けたり、ケーブル自体が損傷しないよう、適切に設置・保護してあること。
(9) ネットワークの拡大に伴い、該当のネットワークを分離する場合は、分割後のネットワークポリシーを定め、アクセス制御を十分検討すること。
(10) 保守作業をネットワーク回線を通じて行う場合は、経路の保護を図り、アクセス制御を十分検討すること。
(11) ネットワークへのトラヒックについて、利用状況の予測を立てること。
(12) ネットワークのトラヒック監視が可能な仕組みを組込み、ネットワーク容量の監視を可能とすること。
(13) ネットワーク容量やサービスは、常に最新のものを選択できるように定義しておくこと。
(14) ソフトウエアの開発時、または運用時にリモート開発やリモート診断を行う場合は、そのセキュリティを十分考慮に置くこと。

8.5（パッケージ構成仕様）

システム開発に必要なパッケージを決定する際に満たすべき事項を定義する。

(1) パッケージが継続的に使用し得る可能性を確認すること。

(2) パッケージのユーザー要求仕様・システム要求仕様のカバー率、既存のインフラとの親和性を確認・評価しておくこと。

(3) 開発方針との親和性を評価しておくこと。

(4) カスタマイズの有無、ある場合の想定量を検討しておくこと。

8.6(機械・電気仕様)

システムの機器類の設置・管理・運営に対してセキュリティを満たすような事項を定義する。

(1) 装置は作業エリアへの不必要な入室を抑えられるよう、設置場所、パーティション、施錠などのセキュリティの機能を持たせること。

(2) 窃盗、火災、爆発などのリスクを軽減する管理策を決定すること。

(3) 機器の設置場所については、侵入などの物理的・人的リスク対策、地震・火事などの災害リスク対策、温度湿度・電源などの設置環境リスク対策が考慮されていること。

(4) 電源の多重化、無停止電源装置、バックアップの設置等を念頭に置いて装置の仕様に適合した電力供給を続けられるよう方式を決定すること。

第３章　開発・導入

第 9 条(開発)

システムの開発では、開発担当者による不正行為を防止することが必要である。

開発作業にあたって、以下の事項を遵守しなければならない。

以下の事項は、開発において外部委託業者を使用する場合も含む。

(1) 開発のプロジェクト責任者、監督者は開発の要員管理を適切に行うこと。

(2) 監督者は開発担当者の作業範囲、責任範囲を明確にし、担当者に認識させること。

(3) 開発環境への入退室は、許可を与えられた者以外立ち入れないように厳格に管理すること。

(4) 開発環境への ID・パスワードは、必要に応じて発行し、不要となった時点で削除すること。

(5) 開発環境と本番環境は原則として別環境として構築し、環境間で十分なセキュリティ対策を行うこと。

(6) 開発担当者は前章で定めた設計仕様に基づき、別途プログラム基準に従い、プログラミングを行うこと。

(7) 隠れたルートやトロイの木馬のコードが問題になる場合は、作業は信頼できるスタッフに行わせること。

(8) 隠れたルートやトロイの木馬のコードが埋め込まれないよう、ソフトウエアのソースコードを検査すること。

(9) プログラムソースライブラリへのアクセスを厳格に管理すること。

(10) 開発中プログラムソースのバージョン管理・バックアップを適切に行うこと。

(11) 稼動中のシステムを更新または修正プログラムを導入する場合は、影響範囲の確認を行うこと。変更管理の手順を定め、変更を管理すること。

(12) 開発をリモート回線を通じて行うことを許可する場合は、情報保護のためのセキュリティ対策を十分に行うこと。

第 10 条(テスト)

開発対象のシステムが想定外の動作をすることによって発生する事故を防ぐためには正確なテストが必要である。また、テストに使用するデータの漏洩も防ぐ必要がある。
テストを行うにあたって、以下の事項を遵守しなければならない。

10.1（テスト環境）
(1) 開発環境とテスト環境は別環境で構築すること。
(2) 開発環境とテスト環境では異なるログオン手順を用いること。

10.2（データ・本番データの使用）
(1) 本番データをテストに使用しなければならない場合は、データの重要度にて、事前にデータを管理する者の承認を受けること。個人情報が特定できるデータを使用する場合は、マスキングを施すなど、個人が特定できぬよう適切な処置を図ること。
(2) 本番データの使用は、使用可能な範囲を明確にし、追跡可能な記録を取ること。
(3) テストに使用したデータ・本番データは、適切に管理、廃棄すること。
(4) 開発対象のシステムから出力されるデータが妥当なものであることを確認するための機能や手順を整備すること。

第 11 条（システム開発の委託）
外部委託業者を使用する場合、外部委託業者によって引き起こされるリスクを防止しなければならない。
外部委託業者を使用する場合は、以下の事項を遵守しなければならない。
(1) 外部委託業者の選定、機密保持契約は情報処理外部委託規定の規定に従い、行うこと。
(2) 外部委託開発要員の所属・身元を証明させること。
(3) 外部委託先業者に設計書およびソースコードの提出を可能な限り義務付けること。
(4) 開発環境、セキュリティなどに関しては、個別契約で明細を決めるようにすること。

第 12 条（製品の調達）
製品の調達とは、システム開発・導入作業全般に渡り、業務に必要な既成パッケージソフトウエア製品を購入することをいう。
製品の調達を行う場合、以下の事項を遵守しなければならない。
(1) 購入先または開発元の事業者が、品質上および財務経理上、信頼に足るものであることを確認すること。あるいは必要に応じて監査を行うこと。
(2)本規定の各基準に従い、当該製品がセキュリティ上問題にならないか、検証あるいは購入先に確認を行い、導入を行うこと。
(3) 当該製品に関する更新情報の提供が購入先より迅速に受けられる状態であることを確認しておくこと。
(4) 隠れたルートやトロイの木馬のコードが埋め込まれないよう、ソフトウエアは信頼できる製造元からソースコードを購入すること。

第 13 条（導入）
システムを導入するには、以下の事項を遵守しなければならない。
(1) 開発責任者はシステムの導入につき、導入計画を立案し、文書化すること。

(2) 開発責任者はシステムを導入する際、既に稼動しているシステムに接続する前に、計画段階の品質を満足させる十分な試験を行われていることを確認すること。
(3) 導入に関して事前のリハーサルが必要な場合は、事前に確認をしておくこと。
(4) 導入結果は報告書に文書化し、開発任者およびシステム利用部門責任者の承認を得ること。

第 14 条(稼働中システムの改善)
稼働中のシステムを改善する場合、以下の事項を遵守しなければならない。
(1) オペレーティングシステムを変更する場合、アプリケーションシステムの見直しおよびテストを実施すること。
(2) (1)以外の改善を行う場合は、第9条の規定に従うこと。

第４章　書類管理など

第 15 条(開発書類の管理)
開発過程の文書類は、別に文書管理規定を定めて管理する。

第 16 条(要員の教育)
各責任者は、システム開発・評価が適切に実施されるために、関係者に対する教育・訓練の機会を設ける。
教育は、システム毎に、プロジェクトフェーズおよび運用フェーズにおいて適宜実施する。各関係者の教育の実績は記録し、保管する。

第 17 条(変更管理)
プロジェクトチームは、開発文書やコンピュータの構成要素に重大な変更が生じた場合の変更管理、ユーザー要求仕様やシステム機能・テスト結果の対応表の作成を実施し、最新版を管理する。
また、その他の変更が生じた場合にも、常に各文書を最新にしておかなければならない。
変更した場合の履歴管理は、必要に応じて実施する。

第５章　改廃および周知

第 18 条(規定の改廃および周知)
本規定の制定、改訂、または失効の承認は、情報処理統括責任者が行う。
開発責任者は原本を正確に複製したものを関係者に公開し、周知徹底させる。
開発責任者は、セキュリティを保持した環境に原本を保管する。
開発責任者は、本規定の内容を変更した場合は、遅滞なく関係者に改訂を通知する。失効、廃棄した場合も同様とする。
開発責任者は規制当局または監査部門あるいは利害関係者が、システム開発の内容の開示を求めた場合は、これに応じる。

２．システム評価規定

システム評価規定

第１章　総則

第1条（目的）

本規定は「情報処理規定」に基づきシステムの評価に関する基本を定め、システム評価時の信頼性・安全性・効率性の向上に寄与する。

第2条（適用範囲）

本規定は会社が開発または導入したシステム評価に適用する。

第3条（基本方針）

システム評価の基本方針は次のとおりとする。

(1) 「情報処理規定」の精神に則り、効果的で効率的な評価を行う。

(2) 評価の基準は、当該業務に法的な規制がある場合はそれに従い、ない場合は本規定を基本として自主的に定める。

(3) 評価の項目は、システム規模に応じて、大規模なシステムは詳細に、小規模なシステムには必要な項目を選択して適用するなど、適時適切(スケーラブル)な適用を心がける。

(4) 評価作業には、利用部門(事業部門)・システム部門双方が参加して、業務に適用して効果が上がるように心がける。

第4条（役割と責任）

会社はシステムの評価にあたっては、評価作業を効果的に行うために役割と責任を明確にする。

(1) システムの評価には評価責任者を設置する。評価責任者はシステム規模に応じて適任者を選任する。評価責任者はシステムの評価を効果的・効率的に行うために、評価のプロジェクトを組織する。評価責任者はシステム評価の全ての責任を負う。

(2) 評価責任者は評価作業を効率的に進めるために事務局を設置する。事務局は責任者の業務をサポートすると同時に、総責任者からの委任があれば、責任者の行為を代行する。

(3) システム部門がシステム評価を行う場合は、評価責任者を設置する。システム評価責任者はシス

テム開発または導入過程の全てに責任を負う。システム評価責任者はシステム評価を行うために要員を組織化する。

(4) 利用部門がシステム評価を行う場合は、利用部門評価責任者を設置する。利用部門評価責任者は利用部門の要求仕様の実現に責任を負う。利用部門評価責任者はシステム評価を行うために要員を組織化する。

(5) 監査部門は、必要に応じてシステム評価の過程を監査し、経営者に報告する。

第２章　システムの評価

第5条（評価の位置付け）

システムを開発する上で、各工程においてシステムを評価することは目的にあったシステムを構築するためには必要なことである。システム評価は、システム開発の各工程毎に実施し、その結果を各開発にフィードバックし、必要に応じて開発内容の訂正を行う。システム評価結果が良と判定されて初めて開発は次工程に進む。

第6条（計画と承認）

システム評価計画は、システム開発の計画段階で立案し、総責任者の承認を得ること。

第7条（評価項目）

7.1（計画段階の評価）

システム開発計画時に実施すべき事項が網羅されていることを評価する。

(1) システム計画の立案体制は組織的に確立され、総責任者が承認していること。

(2) システム計画は、開発規定に基づいて策定され、総責任者が承認していること。

(3) システム計画は、経営方針に合致した内容であること。

(4) システム計画は、情報化の効果、推進体制、費用等を明確にしていること。

(5) システム計画は、情報システムの全体像を明確にしていること。

(6) システム計画は、システム開発の優先度を明確にしていること。

(7) システム計画は、システム開発によって生ずる組織および業務の変更の方針を明確にしていること。

(8) システム計画は、セキュリティ対策の方針を明確にしていること。

(9) システム計画は、定期的な見直しおよび経営環境等の変化に対応した見直しを行っていること。

7.2（要件定義の評価）

要件定義として実施すべき事項が網羅されていることを評価する。

(1) システム要求事項が漏れなく抽出できていること。

(2) システム要求事項が実現可能であることが示されること。

(3) システム要求事項をテストできるよう計画されていること。

(4) 運用および保守が実現可能であることが示されること。

(5) システム要求事項がシステム計画の内容に合致していること。

(6) 要求者との間でレビューが実施され、内容に齟齬がないこと。

(7) 要件定義の結果、開発費用、スケジュールに変更が出る場合、システム計画へのフィードバックがなされていること。

7.3（設計段階の評価）

システム設計時に実施すべき事項が網羅されていることを評価する。

(1) システム設計書は、プロジェクトの責任者が承認していること。

(2) 利用者が利用しやすく入出力帳票、入出力画面等を設計していること。

(3) データベースは、業務の内容に応じて設計していること。

(4) データの保全性を確保していること。

(5) ネットワークは、業務の内容に応じて設計していること。

(6) 情報システムの性能は、要求定義を満たしていること。

(7) システム構成は、ピーク時を想定して設計していること。

(8) 運用に必要な性能管理等の技術的な実現方法等を設計していること。

(9) 情報システムの障害対策を講じていること。

(10) 不正防止、機密保護等の機能をセキュリティ対策方針に基づいて設計していること。セキュリティ技術は、最新の技術を適用していること。

(11) 情報システムの利用に係る教育の方針、スケジュール等を明確にしていること。

7.4（製作段階の評価）

システム製作時に実施すべき事項が網羅されていることを評価する。

(1) プログラム仕様書に基づいてプログラミングしていることを検証していること。

(2) プログラムテストの結果を記録および保管していること。

(3) 重要プログラムは、プログラム作成者以外の者がテストしていること。

(4) プログラムテストの結果についてシステム計画時に想定した品質と比較して、その差異について分析し、必要に応じて有効な対策を講じていること。

7.5（パッケージ構成の評価）

パッケージを利用したシステム開発について実施すべき事項が網羅されていることを評価する。

(1) システム化の目標に合致したパッケージ等が選択されていること。

(2) システム化要件に沿って、比較検討が客観的に実施されていること。

(3) ソフトウエアライフサイクル全体についてのコスト、保守性に関する検討がされていること。

(4) 選択したパッケージについてシステム化要件とのフィットアンドギャップ分析がなされ、ギャップに対する対策が立案されていること。

7.6（テスト段階の評価）

システムテスト時に実施すべき事項が網羅されていることを評価する。

(1) テストはテスト計画を作成して行う。テスト計画は、目的、範囲、方法、スケジュール等を明確にしていること。テスト計画に盛り込む項目は、システムを評価できる項目を盛り込んでおくこと。

(2) テストデータの作成およびシステムテストは、テスト計画に基づいて行っていること。

(3) システムテストは、公正かつ客観的立場の者が実施していること。

(4) システムテストは、利用者が参画し、操作マニュアルに基づいて実施していること。

(5) システムテストの結果についてシステム計画時に想定した品質と比較して、その差異について分析し、必要に応じて有効な対策を講じていること。

(6) システムテスト結果として導入に際して問題となる事項が発生した場合、その対策を立案していること。

(7) システムテストの結果は、開発部門、運用保守部門および利用部門の責任者が承認しているこ

と。
(8) システムテストの結果を記録および保管していること。

7.7(導入承認の評価)
システム導入承認時に実施すべき事項が網羅されていることを評価する。
(1) 導入承認の条件が予め明確に定義されていること。
(2) 導入承認の条件に基づいて承認されていること。
(3) 導入承認に当たって、保留事項がある場合は、以後の対応スケジュールが明確化され、モニタリングする体制が整っていること。

7.8(稼働中システムの評価)
稼働中システムは以下の観点で評価する。
(1) 稼働中システムが、システム導入目的に合致した効果を発揮していること。
(2) 稼働中システムの稼動が設計値通りであること。(信頼性、可用性、保守性、保全性、機密性)
(3) 稼働中システムの操作性が使用者の満足度を満たしていること。

7.9(開発委託先の評価)
開発委託先の評価は外部委託規定に従う。

第8条(結果の報告と承認)
各評価結果は必ず文書化し、総責任者に報告し、承認を得るものとする。

第9条(評価結果の監査)
各評価結果は、システム監査の対象とする。監査部門は、必要に応じてシステム評価結果を監査し、経営者に報告する。

第３章 運用管理

第 10 条(評価書類の管理)
各評価結果の文書類は、別に文書管理規定を定めて管理する。

第 11 条(要員の教育)
各責任者は、システム開発・評価が適切に実施されるために、関係者に対する教育・訓練の機会を設ける。
教育は、システム毎に、プロジェクトフェーズおよび運用フェーズにおいて適宜実施する。各関係者の教育の実績は記録し、保管する。

第 12 条(変更管理)
プロジェクトチームは、開発文書やコンピュータの構成要素に重大な変更が生じた場合の変更管理、ユーザー要求仕様やシステム機能・テスト結果の対応表の作成を実施し、最新版を管理する。
また、その他の変更が生じた場合にも、常に各文書を最新にしておかなければならない。

第４章 改廃および周知

第 13 条（規定の改廃および周知）

本規定の制定、改訂、または失効の承認は、情報処理統括責任者が行う。

総責任者は原本を正確に複製したものを関係者に公開し、周知徹底させる。

総責任者は、セキュリティを保持した環境に原本を保管する。

総責任者は、本規定の内容を変更した場合は、遅滞なく関係者に改訂を通知する。失効、廃棄した場合も同様とする。

総責任者は規制当局または監査部門あるいは利害関係者が、システム評価の内容の開示を求めた場合は、これに応じる。

３．システム管理規定

システム管理規定

第１章　　総則

第1条（目的）

本規定は「情報処理規定」に基づきシステムの管理に関する基本を定め、会社のシステムの信頼性・安全性・効率性の向上に寄与する。なお、システム内のユーザーデータの管理は、「情報・データ管理規定」に従うものとし、本規定では規定しない。

第2条（適用範囲）

本規定は会社のシステムの管理に適用する。

第3条（基本方針）

システムの管理の基本方針は次のとおりとする。

①「情報処理規定」に示された「第５条　基本方針」を遵守する。

②世の中のシステムの動向・進展度合い、会社の情報システム要件の変化を遅滞なく捉え、常に適切にシステムの管理を行う。

③各種法規を遵守し、既定の規定との整合性を保ち、最適化を追求する。

第4条（本規定の効力）

1. 本規定はシステムの管理に関して遵守すべき基本を定め、具体的な管理内容については別途定める諸規定等によるものとする。
2. 本規定に定めのない事項または本規定に拠ることが適切でない事項は、基幹のシステムについては情報処理統括責任者の、事業所設置のシステムについては情報処理責任者の指示または承認を得て行う。

第5条（システム管理業務）

システム管理の業務は次の各号に掲げるものとする。

①システム構成管理

②システム維持・更新管理

③システム利用者管理

④システム操作管理

⑤システム処理管理

⑥システム問合わせ管理

⑦システムバックアップ管理

⑧システム障害管理

⑨システムセキュリティ管理

第6条（システム管理責任者）

1. 情報処理統括責任者は、基幹のシステムを効率的に管理するために「基幹システム管理責任者」を任命する。
2. 情報処理責任者は、事業部に設置のシステムを効率的に管理するために「事業部システム管理責任者」を任命する。
3. 「基幹システム管理責任者」および「事業部システム管理責任者」を総称して「システム管理責任者」という。

第7条（システム管理グループ）

1. 基幹システムの管理の実務を実施する「基幹システム管理グループ」を設置する。「基幹システム管理グループ」のリーダーは「基幹システム管理責任者」とし、メンバーは情報処理統括責任者が選任する。
2. 事業部システムの管理の実務を実施する「事業部システム管理グループ」を設置する。「事業部システム管理グループ」のリーダーは「事業部システム管理責任者」とし、メンバーは情報処理責任者が選任する。
3. 「基幹システム管理グループ」および「事業部システム管理グループ」を総称して「システム管理グループ」という。

第8条（システム管理責任者の任務）

1. 「システム管理責任者」は、会社のシステムの信頼性・安全性・効率性に貢献する責任を有する。
2. 「システム管理責任者」は、「システム管理グループ」が担当する業務の責任を有する。
3. 「基幹システム管理責任者」は、管理業務において問題あるときは、直ちに情報処理統括責任者に報告し、その指示を受けなければならない。
4. 「事業部システム管理責任者」は、管理業務において問題あるときは、直ちに情報処理責任者に報告し、その指示を受けなければならない。

第9条（システム管理責任者の権限）

「システム管理責任者」は、本規定および本規定に基づき制定される諸規定等に規定された権限に基づき、システムの管理業務を統括し必要な職務上の指示を与えること。

第 10 条（秘密保持）

システムの管理においては、「セキュリティ管理規定」および関連諸規定等を遵守し、不測の損害の防止に努めなければならない。

第 11 条（業務効率の推進）

システムの管理にあたっては、この規定の定める基本原則を遵守するとともに、常にその経済性を追求し、管理業務の効率向上に努力するものとする。

第２章　システムの管理

第 12 条（システム構成管理）

1. 「システム管理グループ」は、システム概要、システム構成モジュール、関連システムとの関係、システム主幹部門、開発言語、稼働機器環境等のシステム構成情報について記録し、変更があった場合は記録を更新し、常に記録を最新の状態に維持する。
2. 「システム管理グループ」は、障害発生時に備え、システムの開発者またはシステム提供ベンダー等にメンテナンスを委託し、その連絡先を常に把握しておくものとする。

第 13 条（システム維持・更新管理）

1. 「システム管理グループ」は、システムの名称、モジュール名、バージョン、稼働オプション、ソースコード、システム生成情報等のシステムの維持・更新に必要な情報について保管または記録し、変更があった場合は保管内容または記録を更新し、常にこれら情報を最新の状態に維持する。
2. 「システム管理グループ」は、機能改善、性能改善、障害事前防止などのためにシステムのバージョンアップ、稼動オプション変更等を実施する場合は、事前にテストを実施し、正常に稼動し、かつ他システムに悪影響を及ぼさないことを確認し、「システム管理責任者」の承認を得た後でなければ、実利用に供してはならない。

第 14 条（システム利用者管理）

1. システムの利用者登録は、システム主幹部門の依頼に基づいて、「システム管理責任者」の許可のもとに「システム管理グループ」が行う。
2. 「システム管理グループ」は、システムの利用者の氏名、所属部署、利用権限等について記録し、変更があった場合は記録を更新し、常に記録を最新の状態に維持する。

第 15 条（システム操作管理）

1. 「システム管理グループ」は、システム操作方法について記録し、変更があった場合は記録を更新し、常に記録を最新の状態に維持する。
2. 「システム管理グループ」は、システム操作履歴および操作者について記録し、「システム管理責任者」は日次で当該記録を検証する。

第 16 条（システム処理管理）

1. 「システム管理グループ」は、システムの日次処理、週次処理、月次処理、期初処理、期末処理、不定期処理等の処理方法と正常終了の検証方法について記録し、変更があった場合は記録を更新し、常に記録を最新の状態に維持する。

2.「システム管理グループ」は、システムの日次処理、週次処理、月次処理、期初処理、期末処理、不定期処理等の処理予定および処理結果と処理担当者について記録し、「システム管理責任者」は当該記録内容を記録がなされた時点で検証する。
3.「システム管理グループ」は、システムの例外処理の方法について記録し、変更があった場合は記録を更新し、常に記録を最新の状態に維持する。
4.「システム管理グループ」は、システムの例外処理を実施した場合は、処理日、処理内容、処理結果、処理担当者について記録し、「システム管理責任者」は当該記録内容を記録がなされた時点で検証する。
5.「システム管理グループ」は、「サーバー管理グループ」が実施するシステム処理プロセスの常時監視の結果、異常終了や異常な CPU 利用状態、異常な IO 実行状態、異常なメモリー利用状態等が判明した場合は、「サーバー管理グループ」と共同で異常状態からの回復を行う。

第 17 条(システム問合わせ管理)

「システム管理グループ」は、システムの利用方法、利用障害等についての利用者からの問合わせと、問合わせに対する回答の内容を記録し、これらを用いて利用者からの問合わせへの回答時間の短縮を図ると共に、記録結果を 6 ヶ月毎に分析し、システム機能改善の提案を行う。

第 18 条(システムバックアップ管理)

1.「システム管理グループ」は、毎月定期的に2組のシステムバックアップを作成し、1 組をシステム設置場所内の建物内に保管し、緊急に必要になった場合に備える。また、他の 1 組を遠隔地の安全な場所に保管し、地域災害などによりシステムが消失した場合の復旧に備える。但し、「サーバー管理グループ」が行うバックアップでこれらのバックアップ要件が充足される場合はこの限りではない。
2.「システム管理グループ」は、システムで稼働している業務システムのハードディスク内ユーザーデータ領域のバックアップを業務システムの特性に合わせて日次または周次に実施し、システム設置場所内の建物内に保管し、ユーザー誤操作等によるユーザーデータの消失の回復に備える。また、このバックアップは週に 1 度、2 組を作成し、1 組を遠隔地の安全な場所に保管し、地域災害などによりシステムが消失した場合の復旧に備える。但し、「サーバー管理グループ」が行うバックアップでこれらのバックアップ要件が充足される場合はこの限りではない。
3. システムバックアップは、「情報・データ管理規定」の「第 19 条 バックアップ取得の原則」、「第 20 条 バックアップ、復元手順の明確化」、「第 21 条 バックアップ媒体の保管・取り扱い」に従うこと。

第 19 条(システム障害管理)

1.「システム管理グループ」は、「サーバー管理グループ」が実施するシステムの稼動状態の定常的な監視に協力し、異常状態の早期発見に努める。
2.「システム管理グループ」は、システムに障害が発生した場合は、障害の原因となっているモジュールを特定または想定し、単独で、または該当のモジュールのメンテナンス委託先をコールし、メンテナンス委託先と共同して、早期の障害復旧を図る。

第３章　システムのセキュリティ管理

第 20 条(システムへのアクセスのキュリティ管理)

1.「システム管理責任者」の許可なく、システムを利用できないよう制御すること。
2.「システム管理責任者」の許可なく、システムのデータにアクセスできないよう制御すること。

3. システムを利用するためのパスワードは、利用者がいつでも変更できるようにすること。
4. パスワードは、第三者に推測、推定されにくいものを選定し、8文字以上で英字、数字、記号を必ず1文字以上使用したパスワードとするように利用者を指導すること。また、パスワードは 3 ヵ月ごとに変更するよう利用者を指導すること。この場合、変更後のパスワードは、3世代は異なるようにし、パスワードの変更方法に規則性を持たせないように指導すること。

第 21 条(システムの不正利用防止対策)
1. 「システム管理グループ」は、システムの利用者パスワード入力の成功、失敗のログを日時で検証し、不正利用の兆候の有無を判断し、不正な利用の兆候が見られる場合は、防御のための処置を講じること。
2. 「システム管理グループ」は、システムのデータベースのアクセスログを日時で検証し、不正アクセスの兆候の有無を判断し、不正なアクセスの兆候が見られる場合は、防御のための処置を講じること。

第 22 条(システム設置場所のセキュリティ管理)
1. 基幹システムの設置場所へは、「基幹システム管理責任者」が許可した者以外が物理的に近寄ることができないようにすること。
2. 事業部システムの設置場所は、部署に所属の要員以外の第三者が近寄った場合に部署に所属の要員が警告し、近寄ることを阻止できる場所に設置すること。
3. 事業部システムの設置場所に部署に所属の要員が誰もいない状態になる場合は、設置場所への出入り口の施錠などにより、物理的に第三者が近寄ることができないようにすること。

第 23 条(システム管理システム文書のセキュリティ管理)
1. 「システム管理責任者」は、システム管理のための各種システム文書を「秘密保持規定」の第5条(秘密情報の分類)に従って秘密情報分類を行うこと。
2. 極秘、秘、社外秘に分類されたシステム管理のための各種システム文書には、「システム管理責任者」の許可した者以外がアクセスできないようにすること。
3. 極秘、秘、社外秘に分類されたシステム管理のための各種システム文書書類を廃棄する時は、シュレッダーに掛けて廃棄すること。
4. 極秘、秘、社外秘に分類されたシステム管理のための各種システム文書電子データを廃棄する時は、完全削除すること。

第 24 条(システムバックアップ媒体のセキュリティ管理)
1. システムバックアップ媒体の保管場所へは、「システム管理責任者」が許可した者以外が物理的に近寄ることができないようにすること。
2. システムバックアップ媒体を廃棄する時は、バックアップ内容を完全削除または物理的にバックアップ内容を復元できないようにすること。

第 25 条(システムバックアップ媒体の転送セキュリティ)
「システム管理責任者」は、システムバックアップ媒体を転送する場合は、「セキュリティ管理者のための情報セキュリティガイドライン」に記載の「運送中の媒体のセキュリティについて」に従うこと。

第 26 条(システムのセキュリティ問題発生後の対応)

「システム管理責任者」は、システムのセキュリティ問題が発生した場合は、「セキュリティ管理者のための情報セキュリティガイドライン」に記載の「セキュリティ管理者のセキュリティ問題への対応」に従って対応すること。

第４章　規定の改廃および周知

第 27 条（規定の改廃および周知）

1. この規定の改廃は、情報システム部が立案し、情報システム部長の決定を得て行う。
2. 前項の決定事項は、これを社内に周知しなければならない。

４．サーバー管理規定

サーバー管理規定

第１章　総則

第1条（目的）

本規定は「情報処理規定」に基づきサーバーの管理に関する基本を定め、会社のサーバーの信頼性・安全性・効率性の向上に寄与する。

第2条（適用範囲）

本規定は会社のサーバーの管理に適用する。

第3条（基本方針）

サーバーの管理の基本方針は次のとおりとする。

①「情報処理規定」に示された「第５条　情報処理の基本方針」を遵守する。

②世の中のサーバーの動向・進展度合い、会社の情報システム要件の変化を遅滞なく捉え、常に適切にサーバーの管理を行う。

③各種法規を遵守し、既定の規定との整合性を保ち、最適化を追求する。

第4条（本規定の効力）

1．本規定はサーバーの管理に関して遵守すべき基本を定め、具体的な管理内容については別途定める諸規定等によるものとする。

2．本規定に定めのない事項または本規定に拠ることが適切でない事項は、基幹のサーバーについては情報処理統括責任者の、事業部設置のサーバーについては情報処理責任者の指示または承認

を得て行う。

第5条（サーバー管理業務）

サーバー管理の業務は次の各号に掲げるものとする。

①サーバー構成管理

②サーバーオペレーティングシステム管理

③サーバー稼働の業務システムのプロセス管理

④サーバーキャパシティ管理

⑤サーバーバックアップ管理

⑥サーバー障害管理

⑦サーバーセキュリティ管理

第6条（サーバー管理責任者）

1. 情報処理統括責任者は、基幹のサーバーを効率的に管理するために「基幹サーバー管理責任者」を任命する。
2. 情報処理責任者は、事業部に設置のサーバーを効率的に管理するために「事業部サーバー管理責任者」を任命する。
3. 「基幹サーバー管理責任者」および「事業部サーバー管理責任者」を総称して「サーバー管理責任者」という。

第7条（サーバー管理グループ）

1. 基幹サーバーの管理の実務を実施する「基幹サーバー管理グループ」を設置する。「基幹サーバー管理グループ」のリーダーは「基幹サーバー管理責任者」とし、メンバーは情報処理統括責任者が選任する。
2. 事業部サーバーの管理の実務を実施する「事業部サーバー管理グループ」を設置する。「事業部サーバー管理グループ」のリーダーは「事業部サーバー管理責任者」とし、メンバーは情報処理責任者が選任する。
3. 「基幹サーバー管理グループ」および「事業部サーバー管理グループ」を総称して「サーバー管理グループ」という。

第8条（サーバー管理責任者の任務）

1. 「サーバー管理責任者」は、会社のサーバーの信頼性・安全性・効率性に貢献する責任を有する。
2. 「サーバー管理責任者」は、「サーバー管理グループ」が担当する業務の責任を有する。
3. 「基幹サーバー管理責任者」は、管理業務において問題あるときは、直ちに情報処理統括責任者に報告し、その指示を受けなければならない。
4. 「事業部サーバー管理責任者」は、管理業務において問題あるときは、直ちに情報処理責任者に報告し、その指示を受けなければならない。

第9条（サーバー管理責任者の権限）

「サーバー管理責任者」は、本規定および本規定に基づき制定される諸規定等に規定された権限に基づき、サーバーの管理業務を統括し必要な職務上の指示を与えること。

第 10 条（秘密保持）

サーバーの管理においては、「セキュリティ管理規定」および関連諸規定等を遵守し、不測の損害の防止に努めなければならない。

第 11 条（業務効率の推進）

サーバーの管理にあたっては、この規定の定める基本原則を遵守するとともに、常にその経済性を追求し、管理業務の効率向上に努力するものとする。

第２章　サーバーの管理

第 12 条（サーバー構成管理）

1. 「サーバー管理グループ」は、サーバーを構成しているCPU、メモリー、ハードディスク、外部記憶装置、無停電電源装置などのハードウエア構成について記録し、変更があった場合は記録を更新し、常に記録を最新の状態に維持する。
2. 「サーバー管理グループ」は、サーバーを構成しているハードディスクの利用可能な総容量とアロケーションされているファイルの名称、利用目的、利用責任者、利用許可されているユーザー、利用許可の種別（読込み可、読込み書込み可等）、利用容量を記録し、記録を常に最新の状態に維持する。
3. 「サーバー管理グループ」は、サーバーを構成している各装置ごとに故障修理を依頼する業者とその連絡先を常に把握しておくものとする。

第 13 条（サーバーオペレーティングシステム管理）

1. 「サーバー管理グループ」は、サーバーを稼働させているオペレーティングシステムの名称、バージョン、適用オプション、適用済みパッチ等のオペレーティングシステムの維持・更新に必要な情報について記録し、変更があった場合は記録を更新し、常に記録を最新の状態に維持する。
2. 「サーバー管理グループ」は、機能改善、性能改善、障害事前防止などのために必要に応じて適宜、サーバーを稼働させているオペレーティングシステムのバージョンアップ、稼働オプション変更、パッチ適用等を実施すること。ただし、これらを実施する場合は、事前にテストを実施し、正常に稼働することを確認し、「サーバー管理責任者」の承認を得た後でなければ、実利用に供してはならない。
3. 「サーバー管理グループ」は、サーバーを稼働させているオペレーティングシステムに障害が発生した場合に障害回復を依頼する業者とその連絡先を常に把握しておくものとする。

第 14 条（サーバークセス管理）

1. サーバーのユーザー登録は、「サーバー管理責任者」の許可のもとに「サーバー管理グループ」が行う。
2. 「サーバー管理グループ」がユーザーファイルへのアクセス許可を登録ユーザーに与える場合は、該当するシステムの「システム管理責任者」の承認を必要とする。
3. 「サーバー管理グループ」は、サーバーに登録されているユーザーについて、ユーザー名、ユーザー種別、ディフォルトディレクトリ、アクセス権限等について記録し、変更があった場合は記録を更新し、常に記録を最新の状態に維持する。
4. 他システム経由でサーバーのプロセスまたはファイルにアクセスする利用形態では、サーバークセス管理は、「システム管理規定」に規程の「第 20 条　システムのシステムアクセスのセキュリティ管理」に基づいて、当該システムの「システム管理責任者」が責任をもって行う。

第 15 条(サーバー稼働の業務システムのプロセス管理)

1.「サーバー管理グループ」は、サーバーで稼働している業務システムの名称と業務システムのプロセス名、サービス特性(オンラインサービスプロセス、バッチサービスプロセス等)、稼働特性(定常利用時の CPU、IO、メモリーの利用状況等)、当該システムの「システム管理責任者」について記録し、変更があった場合は記録を更新し、常に記録を最新の状態に維持する。

2.「サーバー管理グループ」は、サーバーで稼働している業務システムのプロセスを常時監視し、異常終了や異常な CPU 利用状態、異常な IO 実行状態、異常なメモリー利用状態等になった場合は、当該システムの「システム管理責任者」と共同して異常状態からの回復を行う。

第 16 条(サーバーキャパシティ管理)

1.「サーバー管理グループ」は、サーバーの CPU、IO、メモリー、ディスクスペース等のキャパシティの利用状況を定常的に測定、記録し、キャパシティ利用状況の時系列変化を分析し、キャパシティ限界を超える時期について6ヶ月に1度の割合で予測すること。

2.「サーバー管理グループ」は、サーバーで実行されているプロセスを定常的に監視し、不必要にキャパシティを利用しているプロセスがないかどうかを確認し、該当するプロセスが存在する場合は是正のための処置を講じる。

第 17 条(サーバーバックアップ管理)

1.「サーバー管理グループ」は、毎月定期的に2組のサーバーバックアップを作成し、1 組をサーバー設置場所内の建物内に保管し、緊急に必要になった場合に備える。また、他の 1 組を遠隔地の安全な場所に保管し、地域災害などによりサーバーが消失した場合の復旧に備える。

2.「サーバー管理グループ」は、サーバーで稼働している業務システムのハードディスク内ユーザーデータ領域のバックアップを業務システムの特性に合わせて日次または周次に実施し、サーバー設置場所内の建物内に保管し、ユーザー誤操作等によるユーザーデータの消失の回復に備える。また、このバックアップは週に 1 度、2 組を作成し、1 組を遠隔地の安全な場所に保管し、地域災害などによりサーバーが消失した場合の復旧に備える。

3. サーバーバックアップは、「情報・データ管理規定」の第 19 条 (バックアップ取得の原則)、第 20 条 (バックアップ、復元手順の明確化) 、第 21 条 (バックアップ媒体の保管・取り扱い)に従うこと。

第 18 条(サーバー障害管理)

1.「サーバー管理グループ」は、サーバーの稼働状態を定常的に監視し、異常状態の早期発見に努める。

2.「サーバー管理グループ」は、サーバーに障害が発生した場合は、速やかに障害個所の切り分けを行い、障害の原因となっているプロセスまたは装置を特定または想定し、該当のプロセスまたは装置の修理業者をコールし、修理業者と共同して、早期の障害復旧を図る。

第３章　サーバーのセキュリティ管理

第 19 条(サーバーオペレーティングシステムのセキュリティ管理)

1.「サーバー管理責任者」の許可なく、サーバーのオペレーティングシステムに接続できないよう制御すること。

2.「サーバー管理責任者」の許可なく、サーバーのシステムコマンドを実行できないように制御するこ

と。
3. 「サーバー管理グループ」は、サーバーのオペレーティングシステムに接続するための ID、パスワードをディフォルトのままにしておいてはいけない。
4. サーバーのオペレーティングシステムに接続するためのパスワードは、第三者に推測、推定されにくいものを選定し、8文字以上で英字、数字、記号を必ず1文字以上使用したものとし、3 ヵ月ごとに変更すること。パスワードは、3世代は異なるようにし、パスワードの変更方法に規則性を持たせないこと。
5. サーバーのオペレーティングシステムに管理者権限で接続するための ID、パスワードは「サーバー管理グループ」のメンバーまたは「サーバー管理責任者」が特別に許可したもの以外に利用させてはならない。また、この ID、パスワードは、他の第三者に知られないよう厳重に管理すること。パスワードが漏洩した可能性がある場合は直ちにパスワードを変更すること。
6. サーバーのオペレーティングシステムに利用者権限で接続するための ID、パスワードは、そのサーバーで稼働する各業務システムの「システム管理責任者」が許可したもの以外に利用させてはならない。また、この ID、パスワードは、他の第三者に知られないよう厳重に管理すること。パスワードが漏洩した可能性がある場合は直ちにパスワードを変更すること。

第 20 条(サーバー稼働プロセスのセキュリティ管理)
1. サーバーのプロセスを利用するための ID、パスワードは、そのプロセスが属するシステムの「システム管理責任者」が許可したもの以外に利用させてはならない。また、この ID、パスワードは、他の第三者に知られないよう厳重に管理すること。パスワードが漏洩した可能性がある場合は直ちにパスワードを変更すること。
2. サーバーのプロセスを利用するためのパスワードは、第三者に推測、推定されにくいものを選定し、8文字以上で英字、数字、記号を必ず1文字以上使用したものとするよう指導すること。
3. サーバーのプロセスを利用するため、利用者が ID、パスワードを利用の都度入力するシステムでは、3 ヵ月ごとにパスワードを変更するよう指導すること。この場合、パスワードは、3世代は異なるようにし、パスワードの変更方法に規則性を持たせないよう指導すること。

第 21 条(サーバーファイルアクセスセキュリティ管理)
1. 「サーバー管理責任者」の許可なく、サーバーのシステムファイルにアクセスできないように制御すること。
2. 「サーバー管理グループ」は、各業務システムの「システム管理責任者」が許可したもの以外のものが各業務システムのファイルにアクセスできないよう制御すること。

第 22 条(サーバーのハッキング／クラッキング防止、ウイルス防止対策)
1. 「サーバー管理グループ」は、サーバーのハッキング／クラッキング防止情報等のセキュリティ情報を定常的に調査し、セキュリティ上の問題が発覚した場合は、セキュリティ問題修復のための、パッチまたはバージョンアップその他の処置を、テスト検証を行い、「サーバー管理責任者」の許可を得た後に実施すること。
2. 「サーバー管理グループ」は、サーバー起動時からメモリーに常駐するワクチンプログラムをサーバーで稼動させねばならない。また、ワクチンプログラムの最新パターンファイル、最新バージョンのプログラムファイルがネットワークにて自動的に配信され、自動更新がなされるようにすること。但し、このような自動配信の仕組みがない場合は、最新パターンファイル、最新バージョンのプログラムファイルが

作成される度に、手動にて更新を行うこと。
3.「サーバー管理グループ」は、サーバーのポートについて、必要なもののみを利用可能に設定し、その他のポートはすべて利用不能に設定しておくこと。
4.「サーバー管理グループ」は、サーバーのユーティリティについて、必要なもののみを利用可能に設定し、その他のものはすべて利用不能の状態にしておくこと。
5.「サーバー管理グループ」は、サーバーで実行されているプロセスを定常的に監視し、不審なプロセスがないかどうかを確認し、該当するプロセスが存在する場合は、防御のための処置を講じること。
6.「サーバー管理グループ」は、サーバーのログを定期的に解析し、不正なアクセスの有り無しを見極め、不正なアクセスがあった場合は、防御のための処置を講じること。

第 23 条(サーバー設置場所のセキュリティ管理)
1. 基幹サーバーの設置場所へは、「基幹サーバー管理責任者」が許可した者以外が物理的に近寄ることができないようにすること。
2. 事業部サーバーの設置場所は、部署に所属の要員以外の第三者が近寄った場合に部署に所属の要員が警告し、近寄ることを阻止できる場所に設置すること。
3. 事業部サーバーの設置場所に部署に所属の要員が誰もいない状態になる場合は、設置場所への出入り口の施錠などにより、物理的に第三者が近寄ることができないようにすること。

第 24 条(サーバー管理システム文書のセキュリティ管理)
1.「サーバー管理責任者」は、サーバー管理のための各種システム文書を「秘密保持規定」の第5条(秘密情報の分類)に従って秘密情報分類を行うこと。
2. 極秘、秘、社外秘に分類されたサーバー管理のための各種システム文書には、「サーバー管理責任者」の許可した者以外がアクセスできないようにすること。
3. 極秘、秘、社外秘に分類されたサーバー管理のための各種システム文書書類を廃棄する時は、シュレッダーに掛けて廃棄すること。
4. 極秘、秘、社外秘に分類されたサーバー管理のための各種システム文書電子データを廃棄する時は、完全削除すること。

第 25 条(サーバーバックアップ媒体のセキュリティ管理)
1. サーバーバックアップ媒体の保管場所へは、「サーバー管理責任者」が許可した者以外が物理的に近寄ることができないようにすること。
2. サーバーバックアップ媒体を廃棄する時は、バックアップ内容を完全削除または物理的にバックアップ内容を復元できないようにすること。

第 26 条(サーバーバックアップ媒体の転送セキュリティ)
「サーバー管理責任者」は、サーバーバックアップ媒体を転送する場合は、「セキュリティ管理者のための情報セキュリティガイドライン」に記載の「運送中の媒体のセキュリティについて」に従うこと。

第 27 条(サーバーのセキュリティ問題発生後の対応)
「サーバー管理責任者」は、サーバーのセキュリティ問題が発生した場合は、「セキュリティ管理者のための情報セキュリティガイドライン」に記載の「セキュリティ管理者のセキュリティ問題への対応」に従って対応すること。

第４章　規定の改廃および周知

第 28 条（規定の改廃および周知）

1. この規定の改廃は、情報システム部が立案し、情報システム部長の決定を得て行う。

2. 前項の決定事項は、これを社内に周知しなければならない。

５．データベース管理規定

データベース管理規定

第１章　総則

第1条（目的）

本規定は「情報処理規定」に基づきデータベースの管理に関する基本を定め、会社のデータベースの信頼性・安全性・効率性の向上に寄与する。なお、データベース内のユーザーデータの管理は、「情報・データ管理規定」に従うものとし、本規定では規定しない。

第2条（適用範囲）

本規定は会社のデータベースの管理に適用する。

第3条（基本方針）

データベースの管理の基本方針は次のとおりとする。

①「情報処理規定」に示された「第５条　基本方針」を遵守する。

②世の中のデータベースシステムの動向・進展度合い、会社の情報システム要件の変化を遅滞なく捉え、常に適切にデータベースの管理を行う。

③各種法規を遵守し、既定の規定との整合性を保ち、最適化を追求する。

第4条（本規定の効力）

1. 本規定はデータベースの管理に関して遵守すべき基本を定め、具体的な管理内容については別途定める諸規定等によるものとする。
2. 本規定に定めのない事項または本規定に拠ることが適切でない事項は、基幹のデータベースについては情報処理統括責任者の、事業部設置のデータベースについては情報処理責任者の指示または承認を得て行う。

第5条（データベース管理業務）

データベース管理の業務は次の各号に掲げるものとする。

①データベース構成管理

②データベースシステム管理

③データベースユーザー管理

④データベースリソース管理

⑤データベース稼働管理

⑥データベースキャパシティ管理

⑦データベースバックアップ管理

⑧データベース障害管理

⑨データベースセキュリティ管理

第6条（データベース管理責任者）

1. 情報処理統括責任者は、基幹のデータベースを効率的に管理するために「基幹データベース管理責任者」を任命する。
2. 情報処理責任者は、事業部に設置のデータベースを効率的に管理するために「事業部データベース管理責任者」を任命する。
3. 「基幹データベース管理責任者」および「事業部データベース管理責任者」を総称して「データベース管理責任者」という。

第7条（データベース管理グループ）

1. 基幹データベースの管理の実務を実施する「基幹データベース管理グループ」を設置する。「基幹データベース管理グループ」のリーダーは「基幹データベース管理責任者」とし、メンバーは情報処理統括責任者が選任する。
2. 事業部データベースの管理の実務を実施する「事業部データベース管理グループ」を設置する。「事業部データベース管理グループ」のリーダーは「事業部データベース管理責任者」とし、メンバーは情報処理責任者が選任する。
3. 「基幹データベース管理グループ」および「事業部データベース管理グループ」を総称して「データベース管理グループ」という。

第8条（データベース管理責任者の任務）

1. 「データベース管理責任者」は、会社のデータベースの信頼性・安全性・効率性に貢献する責任を有する。
2. 「データベース管理責任者」は、「データベース管理グループ」が担当する業務の責任を有する。
3. 「基幹データベース管理責任者」は、管理業務において問題あるときは、直ちに情報処理統括責任者に報告し、その指示を受けなければならない。
4. 「事業部データベース管理責任者」は、管理業務において問題あるときは、直ちに情報処理責任者に報告し、その指示を受けなければならない。

第9条（データベース管理責任者の権限）

「データベース管理責任者」は、本規定および本規定に基づき制定される諸規定等に規定された権

限に基づき、データベースの管理業務を統括し必要な職務上の指示を与えること。

第 10 条(秘密保持)

データベースの管理においては、「セキュリティ管理規定」および関連諸規定等を遵守し、不測の損害の防止に努めなければならない。

第 11 条(業務効率の推進)

データベースの管理にあたっては、この規定の定める基本原則を遵守するとともに、常にその経済性を追求し、管理業務の効率向上に努力するものとする。

第２章　データベースの管理

第 12 条(データベース構成管理)

1.「データベース管理グループ」は、データベースを構成している表領域、データベースファイル、パラメータファイル、ログファイルの名称およびアロケーション位置、アロケーションパラメータ、アロケーションスペース等の構成情報について記録し、変更があった場合は記録を更新し、常に記録を最新の状態に維持する。

◆ 表領域 ・ システム表領域 ・ ロールバックセグメント用表領域 ・ 一時表領域 ・ データ表領域 ・ 索引表領域 ◆ データベースファイル ・ 制御ファイル ・ REDO ログファイル ・ アーカイブログファイル ・ データファイル	◆ パラメータファイル ・ 初期化パラメータファイル ・ リスナパラメータファイル ◆ ログファイル ・ ALERT ログファイル ・ リスナログファイル ・ ユーザープロセスのログファイル ・ バックグラウンドプロセスのログファイル ・ トレースファイル ・ CORE ファイル

2.「データベース管理グループ」は、障害発生時に備え、データベースを構成しているユーザー表領域ごとに、「システム管理規定」の第6条で規定の「システム管理責任者」と、その連絡先を常に把握しておくものとする。

第 13 条(データベースシステム管理)

1.「データベース管理グループ」は、データベースシステムの名称、バージョン、稼働オプション、適用済みパッチ等のデータベースシステムの維持・更新に必要な情報について記録し、変更があった場合は記録を更新し、常に記録を最新の状態に維持する。

2.「データベース管理グループ」は、機能改善、性能改善、障害事前防止などのために必要に応じて適宜、データベースシステムのバージョンアップ、稼働オプション変更、パッチ適用等を実施すること。ただし、これらを実施する場合は、事前にテストを実施し、正常に稼働することを確認し、「データベース管理責任者」の承認を得た後でなければ、実利用に供してはならない。

3.「データベース管理グループ」は、データベースを稼働させているオペレーティングシステムに障害が発生した場合に障害回復を依頼する業者とその連絡先を常に把握しておくものとする。

第 14 条(データベースアクセス管理)

1. データベースのユーザー登録は、「データベース管理責任者」の許可のもとに「データベース管理グループ」が行う。
2.「データベース管理グループ」がユーザー表領域へのアクセス許可を登録ユーザーに与える場合は、該当するユーザー表領域を定義したシステムの「システム管理責任者」の承認を必要とする。
3.「データベース管理グループ」は、データベースに登録されてユーザーについて、ユーザー名、ユーザー種別、ディフォルト表領域、一時表領域、アクセス権、ロール、関係業務システム名について記録し、変更があった場合は記録を更新し、常に記録を最新の状態に維持する。
4. 他システム経由でデータベースにアクセスする利用形態では、データベースのアクセス管理は、「システム管理規定」で規定の「システムアクセス管理」に基づいて該当するシステムの「システム管理責任者」が責任をもって行う。

第 15 条(データベースプロセス稼働管理)

1.「データベース管理グループ」は、データベースプロセスの稼働特性(定常利用時の CPU、IO、メモリーの利用状況等)について月次に調査し、記録する。
2.「データベース管理グループ」は、データベースプロセスを常時監視し、異常終了や異常な CPU 利用状態、異常な IO 実行状態、異常なメモリー利用状態等になった場合は、関係するシステムを特定または想定し、該当システムの「システム管理グループ」と共同で異常状態からの回復を行う。

第 16 条(データベースキャパシティ管理)

「データベース管理グループ」は、データベースシステムの CPU、IO、メモリー、ディスクスペース等のキャパシティの利用状況を定常的に測定、記録し、キャパシティ利用状況の時系列変化を分析し、キャパシティ限界を超える時期について6ヶ月に1度の割合で予測すること。

第 17 条(データベースバックアップ管理)

1.「データベース管理グループ」は、毎月定期的に2組のデータベースバックアップを作成し、1 組をデータベース設置場所内の建物内に保管し、緊急に必要になった場合に備える。また、他の 1 組を遠隔地の安全な場所に保管し、地域災害などによりデータベースが消失した場合の復旧に備える。
2.「データベース管理グループ」は、データベースで稼働している業務システムのハードディスク内ユーザーデータ領域のバックアップを業務システムの特性に合わせて日次または周次に実施し、データベース設置場所内の建物内に保管し、ユーザー誤操作によるユーザーデータの消失の回復に備える。また、このバックアップは週に 1 度、2 組を作成し、1 組を遠隔地の安全な場所に保管し、地域災害などによりデータベースが消失した場合の復旧に備える。
3. データベースバックアップは、「情報・データ管理規定」の「第 19 条 バックアップ取得の原則」、「第 20 条 バックアップ、復元手順の明確化」、「第 21 条 バックアップ媒体の保管・取り扱い」に従うこと。

第 18 条(データベース障害管理)

1.「データベース管理グループ」は、データベースシステムの稼働状態を定常的に監視し、異常状態の早期発見に努める。

2.「データベース管理グループ」は、データベースシステムに障害が発生した場合は、速やかに障害個所の切り分けを行い、障害の原因となっているプロセスまたは装置を特定または想定し、該当のプロセスまたは装置の修理業者をコールし、修理業者と共同して、早期の障害復旧を図る。

第３章 データベースのセキュリティ管理

第 19 条(データベースへのアクセスのキュリティ管理)

1.「データベース管理責任者」の許可なく、データベースに接続できないよう制御すること。

2.「データベース管理責任者」の許可なく、データベースの特権コマンドを実行できないよう制御すること。

3.「データベース管理グループ」は、データベースに接続するための ID、パスワードをディフォルトのままにしておいてはいけない。

4. データベースに接続するためのパスワードは、第三者に推測、推定されにくいものを選定し、8文字以上で英字、数字、記号を必ず1文字以上使用したものとすること。また、利用のたびにパスワードをキー入力する場合は、そのパスワードは 3 ヵ月ごとに変更すること。この場合、変更後のパスワードは、3世代は異なるようにし、パスワードの変更方法に規則性を持たせないこと。

5. データベースに管理者権限で接続するための ID、パスワードは「データベース管理グループ」のメンバーまたは「データベース管理責任者」が特別に許可したもの以外に利用させてはならない。また、この ID、パスワードは、他の第三者に知られないよう厳重に管理すること。パスワードが漏洩した可能性がある場合は直ちにパスワードを変更すること。

6. データベースに利用者権限で接続するための ID、パスワードは、利用するユーザー表領域のシステムの「システム管理責任者」が許可したもの以外に利用させてはならない。また、この ID、パスワードは、他の第三者に知られないよう厳重に管理すること。パスワードが漏洩した可能性がある場合は直ちにパスワードを変更すること。

第 20 条(データベースのハッキング／クラッキング防止対策)

1.「データベース管理グループ」は、データベースのハッキング／クラッキング防止情報等のセキュリティ情報を定常的に調査し、セキュリティ上の問題が発覚した場合は、セキュリティ問題修復のための、パッチまたはバージョンアップその他の処置を、テスト検証を行い、「データベース管理責任者」の許可を得た後に実施すること。

2.「データベース管理グループ」は、データベースのユーティリティについて、必要なもののみを利用可能に設定し、その他のものはすべて利用不能の状態にしておくこと。

3.「データベース管理グループ」は、データベースのログを定期的に解析し、不正なアクセスの有り無しを見極め、不正なアクセスがあった場合は、防御のための処置を講じること。

第 21 条(データベース設置場所のセキュリティ管理)

1. 基幹データベースの設置場所へは、「基幹データベース管理責任者」が許可した者以外が物理的に近寄ることができないようにすること。

2. 事業部データベースの設置場所は、部署に所属の要員以外の第三者が近寄った場合に部署に所属の要員が警告し、近寄ることを阻止できる場所に設置すること。

3. 事業部データベースの設置場所に部署に所属の要員が誰もいない状態になる場合は、設置場所への出入り口の施錠などにより、物理的に第三者が近寄ることができないようにすること。

第 22 条（データベース管理システム文書のセキュリティ管理）

1. 「データベース管理責任者」は、データベース管理のための各種システム文書を「秘密保持規定」の「第 5 条　秘密情報の分類」に従って秘密情報分類を行うこと。
2. 極秘、秘、社外秘に分類されたデータベース管理のための各種システム文書には、「データベース管理責任者」の許可した者以外がアクセスできないようにすること。
3. 極秘、秘、社外秘に分類されたデータベース管理のための各種システム文書書類を廃棄する時は、シュレッダーに掛けて廃棄すること。
4. 極秘、秘、社外秘に分類されたデータベース管理のための各種システム文書電子データを廃棄する時は、完全削除すること。

第 23 条（データベースバックアップ媒体のセキュリティ管理）

1. データベースバックアップ媒体の保管場所へは、「データベース管理責任者」が許可した者以外が物理的に近寄ることができないようにすること。
2. データベースバックアップ媒体を廃棄する時は、バックアップ内容を完全削除または物理的にバックアップ内容を復元できないようにすること。

第 24 条（データベースバックアップ媒体の転送セキュリティ）

「データベース管理責任者」は、データベースバックアップ媒体を転送する場合は、「セキュリティ管理者のための情報セキュリティガイドライン」に記載の「運送中の媒体のセキュリティについて」に従うこと。

第 25 条（データベースのセキュリティ問題発生後の対応）

「データベース管理責任者」は、データベースのセキュリティ問題が発生した場合は、「セキュリティ管理者のための情報セキュリティガイドライン」に記載の「セキュリティ管理者のセキュリティ問題への対応」に従って対応すること。

第４章　規定の改廃および周知

第 26 条（規定の改廃および周知）

1. この規定の改廃は、情報システム部が立案し、情報システム部長の決定を得て行う。
2. 前項の決定事項は、これを社内に周知しなければならない。

６．通信ネットワーク管理規定

通信ネットワーク管理規定

第１章　　総則

第1条（目的）

本規定は「情報処理規定」に基づき情報通信ネットワークの管理に関する基本を定め、会社の情報通信ネットワークの信頼性・安全性・効率性の向上に寄与する。

第2条（適用範囲）

本規定は会社の情報通信ネットワークの管理に適用する。

第3条（基本方針）

情報通信ネットワークの管理の基本方針は次のとおりとする。

①「情報処理規定」に示された「第５条　基本方針」を遵守する。

②世の中の情報通信ネットワークの動向・進展度合い、会社の情報システム要件の変化を遅滞なく捉え、常に適切に情報通信ネットワークの管理を行う。

③各種法規を遵守し、既定の規定との整合性を保ち、最適化を追求する。

第4条（本規定の効力）

1．本規定は情報通信ネットワークの管理に関して遵守すべき基本を定め、具体的な管理内容については別途定める諸規定等によるものとする。

2．本規定に定めのない事項または本規定に拠ることが適切でない事項は、情報処理統括責任者の指示または承認を得て行う。

第5条（通信ネットワーク管理業務）

通信ネットワーク管理の業務は次の各号に掲げるものとする。

①ネットワーク構成管理

②ネットワークアドレス管理
③ネットワークキャパシティ管理
④ネットワークレスポンス管理
⑤ネットワーク障害管理
⑥ネットワークセキュリティ管理

第6条（情報通信ネットワーク管理責任者）
情報処理統括責任者は、情報通信ネットワークを効率的に管理するために「情報通信ネットワーク管理責任者」を任命する。

第7条（通信ネットワーク管理グループ）
情報通信ネットワークの管理の実務を実施する「通信ネットワーク管理グループ」を設置する。「通信ネットワーク管理グループ」のリーダーは「情報通信ネットワーク管理責任者」とし、メンバーは情報処理統括責任者が選任する。

第8条（情報通信ネットワーク管理責任者の任務）
1. 「情報通信ネットワーク管理責任者」は、会社の情報通信ネットワークの信頼性・安全性・効率性に貢献する責任を有する。
2. 「情報通信ネットワーク管理責任者」は、「通信ネットワーク管理グループ」が担当する業務の責任を有する。
3. 「情報通信ネットワーク管理責任者」は、管理業務において問題あるときは、直ちに情報処理統括責任者に報告し、その指示を受けなければならない。

第9条（情報通信ネットワーク管理責任者の権限）
「情報通信ネットワーク管理責任者」は、本規定および本規定に基づき制定される諸規定等に規定された権限に基づき、情報通信ネットワークの管理業務を統括し必要な職務上の指示を与えること。

第 10 条（秘密保持）
情報通信ネットワークの管理においては、「セキュリティ管理規定」および関連諸規定等を遵守し、不測の損害の防止に努めなければならない。

第 11 条（業務効率の推進）
情報通信ネットワークの管理にあたっては、この規定の定める基本原則を遵守するとともに、常にその経済性を追求し、管理業務の効率向上に努力するものとする。

第２章　情報通信ネットワークの管理

第 12 条（通信ネットワーク構成管理）
1. 「通信ネットワーク管理グループ」は、情報通信ネットワークを構成している通信回線、構内回線、接続機器の種類とキャパシティおよび相互の接続関係を常に把握しておくものとする。
2. 「通信ネットワーク管理グループ」は、情報通信ネットワークを構成している接続機器のファームウエアーのバージョンおよび設定を記録し、記録を常に最新の状態に維持する。
3. 「通信ネットワーク管理グループ」は、情報通信ネットワークを構成している通信回線、構内回線、接

続機器の各回線、各機器ごとに故障修理を依頼する業者とその連絡先を常に把握しておくものとする。

第 13 条（ネットワークアドレス管理）

「ネットワーク管理グループ」は、情報通信ネットワークに接続されている全ての機器のIPアドレス、MAC アドレスを記録し、記録を常に最新の状態に維持する。

第 14 条（ネットワークキャパシティ管理）

1.「通信ネットワーク管理グループ」は、情報通信ネットワークを構成している通信回線、構内回線、接続機器の各回線、各機器のキャパシティ利用状況を定常的に測定、記録し、キャパシティ利用状況の時系列変化を分析し、キャパシティ限界を超える時期について6カ月に1度の割合で予測すること。

2.「通信ネットワーク管理グループ」は、ネットワーク内のトラフィックを定常的にキャプチャーし、不正なパケットまたは不要なパケットが流れていないかどうかを確認し、不正または不要なパケットが流れている場合は是正のための処置を講じる。

第 15 条（ネットワークレスポンス管理）

1.「通信ネットワーク管理グループ」は、情報通信ネットワークに接続されている主要拠点間の通信回線を流れるトラフィックのレスポンスの許容範囲を設定する。

2.「通信ネットワーク管理グループ」は、情報通信ネットワークにより相互に接続されている主要拠点間のトラフィックレスポンスを定常的に測定、記録し、許容範囲を超える場合は是正のための処置を講じる。

第 16 条（ネットワーク障害管理）

1.「通信ネットワーク管理グループ」は、情報通信ネットワークを構成している通信回線、構内回線、接続機器の状態監視を定常的に行い、異常状態の早期発見に努める。

2.「通信ネットワーク管理グループ」は、情報通信ネットワークを利用した通信に、途絶または異常な遅延等の障害が発生した場合は、速やかに障害個所の切り分けを行い、障害の原因となっている回線または機器を特定または想定し、該当の機器または回線の修理業者をコールし、修理業者と共同して、早期の障害復旧を図る。

第３章　情報通信ネットワークのセキュリティ管理

第 17 条（社外ネットワークへの接続セキュリティ管理）

1.「情報通信ネットワーク管理責任者」の許可なく、社内ネットワークを社外ネットワークに接続させてはならない。

2.「情報通信ネットワーク管理責任者」の許可なく、社内ネットワークに接続している状態のままのパソコンを、通信モデムを用いて社外ネットワークに接続させてはならない。

3. 社内ネットワークと社外ネットワークとの間の通信では、HTTP プロトコル通信、HTTPS プロトコル通信、電子メールプロトコル通信（SMTP、POP 他）および使用が個別に許可される VPN 通信以外を使用させてはならない。

4. 社内ネットワークに社外ネットワークを接続する場合は、社外ネットワークから社内ネットワーク内を不正にアクセスされないよう、相互を接続する個所にファイヤウオールを設置し防御する。

5. 社内ネットワークに社外ネットワークを接続する場合は、相互を接続する個所にゲートウエイを設置し、社外から社内へのコンピュータウイルスの侵入と社内から社外へのコンピュータウイルスの流出を阻止する。
6. 社内ネットワークに社外ネットワークを接続する場合は、相互を接続する個所にゲートウエイを設置し、社内から閲覧する Web ページの URL フィルタリングを行い、業務に無関係の Web ページの閲覧を禁止する。
7. 社内ネットワークに社外ネットワークを接続する場合は、相互を接続する個所にゲートウエイを設置し、社内から社外へ通信されるデータの抜き取り検査を3カ月に1度の割合で行い、秘密情報の流出の有無をチェックする。秘密情報の流出または流出の疑いがある場合は、是正のための処置を担当する部署に通知する。

第 18 条（通信機器設置場所のセキュリティ管理）

WAN 回線と基幹 LAN を接続する通信機器、基幹 LAN を構成する LAN 間を接続する通信機器および基幹 LAN に接続した事務所フロアーに設置のスイッチ機器または集中ハブ機器の設置場所へは、「情報通信ネットワーク管理責任者」が許可した者以外が物理的に近寄ることができないようにすること。

第 19 条（通信配線のセキュリティ管理）

1. 社内への WAN 回線の引き込みは地下埋設によって行うこと。また、WAN 回線の社内への引き込み口の場所を第三者に確定または推測、推定されないようにすること。
2. WAN 回線の引き込み口から基幹 LAN までの配線、基幹 LAN の配線、基幹 LAN から事務所フロアに設置のスイッチまたは集中ハブまでの配線には、「情報通信ネットワーク管理責任者」が許可した者以外が物理的に近寄ることができないようにすること。

第 20 条（通信機器のセキュリティ管理）

1. 情報通信ネットワークに接続されている通信機器のファームウエアーのセキュリティ情報を定常的に調査し、セキュリティ上の問題が発覚した場合は、セキュリティ問題修復のための、パッチまたはバージョンアップその他の処置を、テスト検証を行い、「情報通信ネットワーク管理責任者」の承認を得た後に実施すること。
2. 情報通信ネットワークに接続されている通信機器のファームウエアーを操作するための ID、パスワードをディフォルトのままにしておいてはいけない。
3. 情報通信ネットワークに接続されている通信機器のファームウエアーを操作するためパスワードは、第三者に推測、推定されにくいものを選定し、8文字以上で英字、数字、記号を必ず1文字以上使用したものとし、3カ月ごとに変更すること。パスワードは、3世代は異なるようにし、パスワードの変更方法に規則性を持たせないこと。
4. 情報通信ネットワークに接続されている通信機器のファームウエアーを操作するための ID、パスワードは「通信ネットワーク管理グループ」のメンバーおよび「情報通信ネットワーク管理責任者」が特別に許可した者以外に知られないよう厳重に管理すること。パスワードが漏洩した可能性がある場合は直ちにパスワードを変更すること。

第 21 条（ネットワーク管理システム文書のセキュリティ管理）

1. 「情報通信ネットワーク管理責任者」は、ネットワーク管理のための各種システム文書を「秘密保持規

定」の「第 5 条　秘密情報の分類」に従って秘密情報分類を行うこと。
2. 極秘、秘、社外秘に分類されたネットワーク管理のための各種システム文書には、「情報通信ネットワーク管理責任者」の許可した者以外がアクセスできないようにすること。
3. 極秘、秘、社外秘に分類されたネットワーク管理のための各種システム文書書類を廃棄する時は、シュレッダーに掛けて廃棄すること。
4. 極秘、秘、社外秘に分類されたネットワーク管理のための各種システム文書電子データを廃棄する時は、完全削除すること。

第 22 条（ネットワークのセキュリティ問題発生後の対応）
「情報通信ネットワーク管理責任者」は、ネットワークのセキュリティ問題が発生した場合は、「セキュリティ管理者のための情報セキュリティガイドライン」に記載の「セキュリティ管理者のセキュリティ問題への対応」に従って対応すること。

第 4 章　規定の改廃および周知

第 23 条（規定の改廃および周知）
1. この規定の改廃は、情報システム部が立案し、情報システム部長の決定を得て行う。
2. 前項の決定事項は、これを社内に周知しなければならない。

７．システム資源管理規定

システム資源管理規定

第１章　総則

第1条(目的)

本規定は「情報処理規定」に基づきシステム資源の管理に関する基本を定め、会社のシステム資源管理の信頼性・安全性・効率性の向上に寄与する。

第2条(適用範囲)

本規定は会社のシステム資源管理に適用する。

第3条(基本方針)

システム資源の管理の基本方針は次のとおりとする。

①「情報処理規定」に示された「第 5 条　基本方針」を遵守する。

②世の中のシステム資源管理の動向・進展度合い、会社の情報システム要件の変化を遅滞なく捉え、常に適切にシステム資源の管理を行う。

③各種法規を遵守し、既定の規定との整合性を保ち、最適化を追求する。

第4条(本規定の効力)

1. 本規定はシステム資源の管理に関して遵守すべき基本を定め、具体的な管理内容については別途定める諸規定等によるものとする。
2. 本規定に定めのない事項または本規定に拠ることが適切でない事項は、情報処理統括責任者の指示または承認を得て行う。

第5条（システム資源管理業務）

システム資源管理の業務は次の各号に掲げるものとする。

①システム資源資産管理

②システム資源コスト管理

③システム資源調達管理

④システム資源契約管理

⑤システム資源管理データのバックアップ管理

⑥システム資源ライセンス使用状況管理

⑦システム資源セキュリティ管理

第6条（システム資源管理責任者）

情報処理統括責任者は、会社のシステム資源を効率的に管理するために「システム資源管理責任者」を任命する。

第7条（システム資源管理グループ）

会社のシステム資源管理の実務を実施する「システム資源管理グループ」を設置する。「システム資源管理グループ」のリーダーは「システム資源管理責任者」とし、メンバーは情報処理統括責任者が選任する。

第8条（システム資源管理責任者の任務）

1. 「システム資源管理責任者」は、会社のシステム資源の信頼性・安全性・効率性に貢献する責任を有する。
2. 「システム資源管理責任者」は、管理業務において問題あるときは、直ちに情報処理統括責任者に報告し、その指示を受けなければならない。

第9条（システム資源管理責任者の権限）

「システム資源管理責任者」は、本規定および本規定に基づき制定される諸規定等に規定された権限に基づき、システム資源の管理業務を統括し必要な職務上の指示を与えること。

第 10 条（秘密保持）

システム資源の管理においては、「セキュリティ管理規定」および関連諸規定等を遵守し、不測の損害の防止に努めなければならない。

第 11 条（業務効率の推進）

システム資源の管理にあたっては、この規定の定める基本原則を遵守するとともに、常にその経済性を追求し、管理業務の効率向上に努力するものとする。

第２章　システム資源の管理

第 12 条（システム資源資産管理）

「システム資源管理グループ」は、システム資源について資源名、資源属性（ハード属性、ソフト属性、設備属性他の属性）、財務、契約、設置場所、保有部門などの資産情報について記録し、変更があった場合は記録を更新し、常に記録を最新の状態に維持する。

第 13 条（システム資源コスト管理）

「システム資源管理グループ」は、システム資源の購入時コスト（支払総額、リース・レンタル対象額、減価償却対象額、経費対象額等）と運用時コスト（リース・レンタル料金、保守料金、保険料、修理費、減価償却費等）を記録し、資産毎、組織・管理者毎、予算種別毎、 コスト負担部門毎、あるいはコスト配賦別に管理する。また年間のシステム資源に要するコストの計画値、実績値を半期ごとに算定し、システム資源への情報化投資コスト管理を行う。これらの情報について変更があった場合は記録を更新し、常にこれら情報を最新の状態に維持する。

第 14 条（システム資源調達管理）

「システム資源管理グループ」は、システム資産、システム消耗品の調達およびシステムの開発、システム運用等のサービス役務等の調達について、業務プロセスの全般（申請、承認、見積、発注書の発行、 納品（完了）、請求書の照合）を管理する。

第 15 条（システム資源契約管理）

「システム資源管理グループ」は、システム資源のリース・レンタル契約、ソフトウエア利用許諾契約や保守契約、サービスプロバイダー契約などの契約を管理する。

第 16 条（システム資源ライセンス使用状況管理）

「システム資源管理グループ」は、システム資源のライセンス総数を管理する。また、ライセンスの配布先およびインストール先、現在稼働中のライセンス数、無効なライセンスの使用などのライセンス使用状況を管理する。これらの情報について変更があった場合は記録を更新し、常にこれらの情報を最新の状態に維持する。

第 17 条（システム資源管理データのバックアップ管理）

「システム資源管理グループ」は、毎月定期的に2組のシステム資源管理データのバックアップを作成し、1 組をシステム資源管理データ設置場所内の建物内に保管し、緊急に必要になった場合に備える。また、他の 1 組を遠隔地の安全な場所に保管し、地域災害などによりシステム資源管理データ設置場所が壊滅した場合の復旧に備える。

第３章　システム資源のセキュリティ管理

第 18 条（システム資源の不正利用防止対策）

「システム資源管理グループ」は、「システム管理規定」、「サーバー管理規定」「データベース管理規定」、「通信ネットワーク管理規定」で定めた各セキュリティ規定に従い、各管理グループに協力して、システム資源の不正利用防止に努めなければならない。

第 19 条（システム資源管理データへのアクセスのセキュリティ管理）

「システム資源管理責任者」の許可なく、システム資源管理データへのアクセスができないよう制御すること。

第 20 条（システム資源管理データの不正利用防止対策）

「システム資源管理グループ」は、システム資源管理データへのアクセス者、アクセスの成功、失敗の

ログを日時で検証し、不正利用の兆候の有無を判断し、不正な利用の兆候が見られる場合は、防御のための処置を講じること。

第 21 条（システム資源設置場所のセキュリティ管理）

「システム資源管理グループ」は、「システム管理規定」、「サーバー管理規定」「データベース管理規定」、「通信ネットワーク管理規定」の各規定で定めた規定に従い、各管理グループに協力して、システム資源設置場所のセキュリティ管理を実施すること。また、これらで規定していないシステム資源については、これらに準じて、システム資源設置場所のセキュリティ管理を実施すること。

第 22 条（システム資源管理システム文書のセキュリティ管理）

1. 「システム資源管理責任者」は、システム資源管理のための各種システム文書を「秘密保持規定」の第5条（秘密情報の分類）に従って秘密情報分類を行うこと。
2. 極秘、秘、社外秘に分類されたシステム資源管理のための各種システム文書には、「システム資源管理責任者」の許可した者以外がアクセスできないようにすること。
3. 極秘、秘、社外秘に分類されたシステム資源管理のための各種システム文書書類を廃棄する時は、シュレッダーに掛けて廃棄すること。
4. 極秘、秘、社外秘に分類されたシステム資源管理のための各種システム文書電子データを廃棄する時は、完全削除すること。

第 23 条（システム資源管理データバックアップ媒体のセキュリティ管理）

1. システム資源管理データバックアップ媒体の保管場所へは、「システム資源管理責任者」が許可した者以外が物理的に近寄ることができないようにすること。
2. システム資源管理データバックアップ媒体を廃棄する時は、バックアップ内容を完全削除または物理的にバックアップ内容を復元できないようにすること。

第 24 条（システム資源データバックアップ媒体の転送セキュリティ）

「システム資源管理責任者」は、システム資源管理データバックアップ媒体を転送する場合は、「セキュリティ管理者のための情報セキュリティガイドライン」に記載の「運送中の媒体のセキュリティについて」に従うこと。

第 25 条（システム資源のセキュリティ問題発生後の対応）

「システム資源管理責任者」は、システム資源のセキュリティ問題が発生した場合は、「セキュリティ管理者のための情報セキュリティガイドライン」に記載の「セキュリティ管理者のセキュリティ問題への対応」に従って対応すること。

第４章　規定の改廃および周知

第 26 条（規定の改廃および周知）

1. この規定の改廃は、情報システム部が立案し、情報システム部長の決定を得て行う。
2. 前項の決定事項は、これを社内に周知しなければならない。

〔５〕一般運用関連規定

１．情報処理教育規定

２．情報処理課金規定

３．情報処理外部委託規定

１．情報処理教育規定

情報処理教育規定

第１章　総則

第1条(目的)

本規定は「情報処理規定」に基づき情報処理教育に関する基本を定め、役員・社員(派遣社員・臨時社員を含む、以下同じ)の業務処理の信頼性・安全性・効率性の向上に寄与する。

第2条(適用範囲)

本規定は会社の情報処理教育に適用する。

第3条(基本方針)

情報処理教育の基本方針は次のとおりとする。

①「情報処理規定」に示された情報処理教育の原則を遵守する。

②情報技術の動向や情報処理教育のあり方、会社の情報処理教育要件の変化を遅滞なく捉え、常に適切な情報処理教育を行う。

③各種法規を遵守し、既定の規定との整合性を保ち、最適化を追求する。

第4条（本規定の効力）

1. 本規定は情報処理教育に関して遵守すべき基本を定め、具体的な内容については別途定める諸規定等によるものとする。
2. 本規定に定めのない事項または本規定に拠ることが適切でない事項は、情報処理統括責任者の指示または承認を得て行う。

第5条（情報処理教育業務）

情報処理教育の業務は次の各号に掲げるものとする。

①情報処理教育計画策定・実施
②情報処理教育カテゴリー策定
③情報処理教育カリキュラム策定
④情報処理教育実施管理（情報リテラシー教育および情報処理要員教育）
⑤情報処理教育成果の分析
⑥情報処理教育結果の評価

第6条（情報セキュリティ教育業務）

情報セキュリティ教育の業務は次の各号に掲げるものとする。

①情報セキュリティ教育計画策定・実施
②役員・社員への情報セキュリティ啓蒙
③役員・社員への情報セキュリティ教育（含むセキュリティ管理者教育）
④情報セキュリティ訓練
⑤情報セキュリティ教育・訓練の効果評価

第7条（情報処理教育責任者）

1. 情報処理統括責任者は、情報処理教育を効率的に管理するために「全社情報処理教育責任者」を任命する。
2. 情報処理責任者は、本社部門および事業部の情報処理教育を効率的に管理するために「事業部情　報処理教育責任者」を任命する。
3. 「全社情報処理教育責任者」および「事業部情報処理教育責任者」を総称して「情報処理教育責任者」という。

第8条（情報処理教育責任者の任務）

1. 「全社情報処理教育責任者」は、全社の情報処理教育および情報セキュリティ教育の有用性・適切性・効率性に貢献する責任を負う。
2. 「事業部情報処理教育責任者」は、本社部門および事業部の情報処理教育および情報セキュリティ教育の有用性・適切性・効率性に貢献する責任を負う。
3. 「全社情報処理教育責任者」は、情報処理教育業務において問題あるときは、直ちに情報処理統括責任者に報告し、その指示を受けなければならない。
4. 「全社情報処理教育責任者」は、情報処理教育に関する「計画」および「実施状況・結果」を定期的に「情報セキュリティ委員会」へ報告しなければならない。

5.「事業部情報処理教育責任者」は、情報処理教育業務において問題あるときは、直ちに情報処理責任者および全社情報処理教育責任者に報告し、その指示を受けなければならない。

第9条（情報処理教育責任者の権限）

「情報処理教育責任者」は、本規定および本規定に基づき制定される諸規定等に規定された権限に基づき、情報処理教育を統括し必要な職務上の指示を与える。

第 10 条（秘密保持）

情報処理教育においては、「セキュリティ管理規定」および関連諸規定等を遵守し、不測の損害の防止に努めなければならない。

第 11 条（業務効率の推進）

情報処理教育にあたっては、この規定の定める基本原則を遵守するとともに、常にその経済性を追求し、情報処理教育の効率向上に努力するものとする。

第２章　情報処理教育

第 12 条（情報処理教育計画策定・実施）

1.「全社情報処理教育責任者」は、年初に年度の全社の情報処理教育計画を策定し、情報処理統括責任者の承認を得て、計画を実施する。

2.「事業部情報処理教育責任者」は、所属する役員・社員について、次の各号を基本原則として、年初に年度の教育計画を作成し、事業部情報処理責任者の承認を得て、計画を実施する。

①業務に直結すること
②成果が測定できること
③目標が確実に達成されること
④費用対効果が向上すること
⑤個人の能力が最大限に引きだされること

第 13 条（情報処理教育カテゴリー策定）

「全社情報処理教育責任者」は、「事業部情報処理教育責任者」の協力を得て、情報処理教育を効果的に実施するために「業務遂行に必要なスキル」を抽出し、「業務遂行を達成目標」として、「情報処理教育カテゴリー」およびカテゴリーに属する「情報処理教育」項目を策定し、情報処理統括責任者の承認を得なければならない。策定した「情報処理教育カテゴリー」およびカテゴリーに属する「情報処理教育」項目は、毎年見直しを行い、情報処理統括責任者の承認を得て、改良・改善を行う。

第 14 条（情報処理教育カリキュラム策定）

「全社情報処理教育責任者」は、「事業部情報処理教育責任者」の協力を得て、「情報処理教育カテゴリー」内の「情報処理教育」項目を組み合わせて、本人の技能と能力レベルごとに「業務遂行の目標達成」のために必要な「情報処理教育」項目の実施順序と実施目標を決定し「情報処理教育カリキュラム」を策定し、情報処理統括責任者の承認を得なければならない。策定した「情報処理教育カリキュラム」は、毎年見直しを行い、情報処理統括責任者の承認を得て、改良・改善を行う。

第 15 条（情報処理教育実施管理）

1.「事業部情報処理教育責任者」は、所属する役員・社員について、年初に策定した「情報処理教育計画」に従って、本人の技能と能力レベルに合った「情報処理教育カリキュラム」を選定し、情報処理責任者の承認を得て本人に通知し、当該「情報処理教育カリキュラム」を受講させる。
2.「事業部情報処理教育責任者」は、所属する役員・社員について、受講した「情報処理教育」の受講報告書を提出させ、情報処理責任者の検証を経て保管する。

第 16 条(情報処理教育成果の分析)
1. 役員・社員は、受講した「情報処理教育カリキュラム」の学習成果を「事業部情報処理教育責任者」に報告し、「事業部情報処理教育責任者」は報告結果から学習達成度を分析し、本人のスキルセットを再確認し、その結果を情報処理責任者に報告する。
2. 役員・社員は、受講した「情報処理教育カリキュラム」が実務に直結した学習内容で、かつ最新情報であったことを確認する。もしそうでない場合は、「事業部情報処理教育責任者」に報告し、「事業部情報処理教育責任者」は、「情報処理教育カリキュラム」や教育内容の改良・改善の要望を「全社情報処理教育責任者」に報告する。

第 17 条(情報処理教育結果の評価)
情報処理責任者は、「情報処理教育カリキュラム」を受講した役員・社員について、受講後の 3 カ月目と 6 カ月目に業務実施内容の質の向上や効率向上の変化の観察を行い、情報処理教育結果の評価を行う。評価の結果、問題がある場合は、「事業部情報処理教育責任者」を経由して、「全社情報処理教育責任者」に報告し、「情報処理教育カリキュラム」や「情報処理教育」内容の改良・改善を要望する。

第３章 情報セキュリティ教育

第 18 条(情報セキュリティ教育計画策定・実施)
「全社情報処理教育責任者」は、年初に全社の「情報セキュリティ啓蒙」および「セキュリティ管理規定」の「第8条(セキュリティ教育の実施)」に基づいた「情報セキュリティ教育」の年度計画を策定し、情報処理統括責任者の承認を得て、計画を実施する。

第 19 条(役員・社員への情報セキュリティ啓蒙)
「全社情報処理教育責任者」は、「事業部情報処理教育責任者」の協力を得て、次の各号に関して情報セキュリティをわかりやすく解説したパンフレットや Web ページを作成し、これらを用いて全ての役員・社員に対し情報セキュリティの啓蒙活動を定常的に実施し、実施結果の効果をアンケートなどにより確認する。
①社員の役割
②社員の責任
③守秘義務
④情報保護の重要性
⑤異常発見時の対処
⑥規則や罰則
⑦情報セキュリティ問題発生事例

第 20 条(役員・社員への情報セキュリティ教育)

1.「事業部情報処理教育責任者」は、所属する役員・社員について、年初に策定した「情報セキュリティ教育」に従って情報セキュリティ教育を毎年定期的に実施する。
2.「事業部情報処理教育責任者」は、所属する役員・社員について、受講した「情報セキュリティ教育」の受講報告書を提出させ、情報処理責任者の検証を得て保管する。

第 21 条（情報セキュリティ訓練）

「全社情報処理教育責任者」は、「事業部情報処理教育責任者」の協力を得て、「セキュリティ管理規定」の「第9条（セキュリティ訓練の実施）」に基づき、情報セキュリティ訓練を毎年定期的に実施する。

第 22 条（情報セキュリティ教育・訓練の効果評価）

「全社情報処理教育責任者」は、「事業部情報処理教育責任者」の協力を得て、「セキュリティ管理規定」の「第 10 条（セキュリティ教育・訓練の効果評価）」に基づき、情報セキュリティ教育・訓練の効果評価を毎年定期的に実施する。

第４章　規定の改廃および周知

第 23 条（規定の改廃および周知）

1. この規定の改廃は、情報処理教育責任者が立案し、情報処理統括責任者の決定を得て行う。
2. 前項の決定事項は、これを社内に周知しなければならない。

２．情報処理課金規定

情報処理課金規定

第１章　総則

第1条（目的）

本規定は「情報処理規定」に基づき情報処理課金管理に関する基本を定め、会社の情報処理課金管理の信頼性・安全性・効率性の向上に寄与する。

第2条（適用範囲）

本規定は会社の情報処理課金に適用する。

第3条（基本方針）

情報処理課金管理の基本方針は次のとおりとする。

①「情報処理規定」に示された情報処理課金の原則を遵守する。

②世の中の情報処理課金管理の動向、会社の情報処理課金要件の変化を遅滞なく捉え、常に適切に情報処理課金管理を行う。

③各種法規を遵守し、既定の規定との整合性を保ち、最適化を追求する。

第4条（本規定の効力）

1．本規定は情報処理課金管理に関して遵守すべき基本を定め、具体的な管理内容については別途定める諸規定等によるものとする。

2．本規定に定めのない事項または本規定に拠ることが適切でない事項は、情報処理統括責任者の指示または承認を得て行う。

第5条（情報処理課金業務）

情報処理課金管理の業務は次の各号に掲げるものとする。

①情報処理課金計画策定

②情報処理課金単価管理

③情報処理課金の徴収・配賦管理
④情報処理課金実施管理
⑤情報処理課金結果の分析
⑥情報処理課金管理データのバックアップ管理
⑦情報処理課金管理のセキュリティ管理

第6条（情報処理課金管理責任者）
情報処理統括責任者は、会社のシステム資源を効率的に管理するために「情報処理課金管理責任者」を任命する。

第7条（情報処理課金管理責任者の任務）
1.「情報処理課金管理責任者」は、会社の情報処理課金管理の公平性・妥当性・効率性に貢献する責任を負う。
2.「情報処理課金管理責任者」は、情報処理課金業務において問題があるときは、直ちに情報処理統括責任者に報告し、その指示を受けなければならない。

第8条（情報処理課金管理責任者の権限）
「情報処理課金管理責任者」は、本規定および本規定に基づき制定される諸規定等に規定された権限に基づき、情報処理課金の管理業務を統括し必要な職務上の指示を与えること。

第9条（秘密保持）
情報処理課金管理においては、「セキュリティ管理規定」および関連諸規定等を遵守し、不測の損害の防止に努めなければならない。

第 10 条（業務効率の推進）
情報処理課金管理にあたっては、この規定の定める基本原則を遵守するとともに、常にその経済性を追求し、管理業務の効率向上に努力するものとする。

第２章　情報処理課金業務

第 11 条（情報処理課金計画策定）
「情報処理課金管理責任者」は、年初に年度の全社の情報処理課金計画を策定し、情報処理統括責任者の承認を得なければならない。

第 12 条（情報処理課金単価管理）
「情報処理課金管理責任者」は、システム資源規定に基づき、算出された運用時コスト（リース・レンタル料金、保守料金、保険料、修理費、減価償却費、運用費等）を記録し、資産毎、組織・管理者毎、課金種別毎（基本単価制、オプション単価制、従量制）、コスト配賦別に管理する。全社共通的に利用する資源については基本単価制を、特定の社員もしくは部署が利用する資源についてはオプション単価制に、運用時コストが利用頻度もしくは使用量と比例の関係がある資源については従量制にする。

第 13 条（情報処理課金の徴収・配賦管理）

「情報処理課金管理責任者」は、システム資源毎に課金の徴収方法（徴収頻度、費用計上科目、消費税有無等）と、配賦先システム資源もしくはそのシステム資源を管理する部署を記録し管理する。

第 14 条（情報処理課金実施管理）

「情報処理課金管理責任者」は、年初に策定した「情報処理課金計画」に従って、情報処理課金管理を実施する。

第 15 条（情報処理課金管理結果の分析）

「情報処理課金管理責任者」は、年間のシステム資源に要するコストの計画値、実績値を半期ごとに算定し、システム資源への情報化投資コストと課金単価のバランス管理を行う。これらの情報について変更があった場合は記録を更新し、常にこれら情報を最新の状態に維持する。

第 16 条（情報処理課金管理データのバックアップ管理）

「情報処理課金管理責任者」は、毎月定期的に2組の情報処理課金管理データのバックアップを作成し、1組を情報処理課金管理データ設置場所内の建物内に保管し、緊急に必要になった場合に備える。また、もう一方の1組は遠隔地の安全な場所に保管し、地域災害などにより情報処理課金管理データ設置場所が破壊した場合の復旧に備える。

第３章　情報処理課金のセキュリティ管理

第 17 条（情報処理課金管理データへのアクセスのセキュリティ管理）

「情報処理課金管理責任者」の許可なく、情報処理課金管理データへのアクセスができないよう制御する。

第 18 条（情報処理課金管理データの不正利用防止対策）

「情報処理課金管理責任者」は、情報処理課金管理データへのアクセス者、アクセスの成功、失敗のログを定期的に検証し、不正利用の兆候の有無を判断し、不正な利用の兆候が見られる場合は、防御のための処置を講じる。

第 19 条（情報処理課金管理の監査）

「情報処理課金管理責任者」は、年に少なくとも1回は、情報処理課金管理の単価設定、徴収、配賦管理について、監査部門からの監査を受けること。また、監査部門から指摘された事項については速やかに改善の措置を施す。

第 20 条（情報処理課金管理情報・データのセキュリティ管理）

1. 「情報処理課金管理責任者」は、情報処理課金管理のための情報・データを「秘密保持規定」に従って秘密情報分類を行う。
2. 極秘、秘、社外秘に分類された情報処理課金管理のためのシステム文書を廃棄する時は、シュレッダーに掛けて廃棄する。
3. 極秘、秘、社外秘に分類された情報処理課金管理のための電子情報、電子データを廃棄する時は、完全削除する。

第４章　規定の改廃および周知

第 21 条（規定の改廃および周知）

1. この規定の改廃は、情報処理課金管理責任者が立案し、情報処理統括責任者の決定を得て行う。

2. 前項の決定事項は、これを社内に周知しなければならない。

３．情報処理外部委託規定

情報処理外部委託規定

第１章　総則

第1条（目的）

本規定は「情報処理規定」に基づき情報処理外部委託に関する基本を定め、会社の情報処理外部委託の信頼性・安全性・効率性の向上に寄与する。

第2条（適用範囲）

本規定は会社の情報処理外部委託に適用する。

第3条（基本方針）

情報処理外部委託の基本方針は次のとおりとする。

①「情報処理規定」に示された情報処理外部委託の原則を遵守する。

②情報処理技術や外部委託先業界の動向、会社の外部委託要件の変化を遅滞なく捉え、常に適切な情報処理外部委託を行う。

③各種法規を遵守し、既定の規定との整合性を保ち、最適化を追求する。

第4条（本規定の効力）

1．本規定は情報処理外部委託に関して遵守すべき基本を定め、具体的な内容については別途定める諸規定等によるものとする。

2．本規定に定めのない事項または本規定に拠ることが適切でない事項は、情報処理統括責任者の指示または承認を得て行う。

第5条（情報処理外部委託業務）

情報処理外部委託の業務は次の各号に掲げるものとする。

①情報処理外部委託計画策定

②情報処理外部委託業者選定基準策定

③情報処理外部委託契約管理
④情報処理外部委託実施管理
⑤情報処理外部委託成果の分析
⑥情報処理外部委託結果の評価
⑦情報処理外部委託のセキュリティ管理

第6条（情報処理外部委託責任者）
情報処理統括責任者は、情報処理外部委託を効率的に管理するために「情報処理外部委託責任者」を任命する。

第7条（情報処理外部委託責任者の任務）
1.「情報処理外部委託責任者」は、会社の情報処理外部委託の信頼性・安全性・効率性に貢献する責任を負う。
2.「情報処理外部委託責任者」は、情報処理外部委託業務において問題あるときは、直ちに情報処理統括責任者に報告し、その指示を受けなければならない。

第8条（情報処理外部委託責任者の権限）
「情報処理外部委託責任者」は、本規定および本規定に基づき制定される諸規定等に規定された権限に基づき、情報処理外部委託を統括し必要な職務上の指示を与える。

第9条（機密保持）
情報処理外部委託においては、「セキュリティ管理規定」および関連諸規定等を遵守し、不測の損害の防止に努めなければならない。

第 10 条（業務効率の推進）
情報処理外部委託にあたっては、この規定の定める基本原則を遵守するとともに、常にその経済性を追求し情報処理外部委託の効率向上に努力するものとする。

第２章　情報処理外部委託

第 11 条（情報処理外部委託計画策定）
「情報処理外部委託責任者」は、年初に年度の全社の情報処理外部委託計画を策定し、情報処理統括責任者の承認を得なければならない。

第 12 条（情報処理外部委託業者の選定基準の策定）
1.「情報処理外部委託責任者」は、外部委託業者の選定基準を策定し、情報処理統括責任者の承認を得なければならない。
2.「情報処理外部委託責任者」は、第 17 条（情報処理外部委託結果の評価）に基づき、外部委託業者の選定基準の見直しを毎年行い、情報処理統括責任者の承認を得て、外部委託業者の選定基準の改良・改訂を行わなければならない。

第 13 条（情報処理外部委託業者の選定）
「情報処理外部委託責任者」は、外部委託業者選定基準に基づいて、当該委託業務の外部委託業

者を選定し、情報処理統括責任者の承認を得て、委託先を決定しなければならない。

第 14 条(情報処理外部委託契約管理)

1.「情報処理外部委託責任者」は、外部委託する情報処理業務について次の各号に掲げる事項を契約書に記載し、情報処理統括責任者の承認を得て、情報処理外部委託契約を行う。

①委託先名称
②委託業務名称
③委託業務内容
④委託業務実施場所
⑤委託業務実施結果の検証方法
⑥委託費用・支払方法
⑦委託先責任者
⑧委託業務実施要員名
⑨第三者委託
⑩委託先の検査権
⑪係争発生時の処置
⑫機密契約事項

2.「情報処理外部委託責任者」は、締結された情報処理外部委託契約書を保管・管理し、変更があった場合は更新し、常に契約書を最新の状態に維持する。

第 15 条(情報処理外部委託実施管理)

1.「情報処理外部委託責任者」は、年初に策定した「情報処理外部委託計画」に従って、情報処理外部委託を実施する。

2.「情報処理外部委託責任者」は、情報処理外部委託について実施された委託内容を「契約書」に記載の「委託業務実施結果の検証方法」に従って検証し、検証結果を情報処理責任者に報告する。検証結果に問題がある場合は、委託先責任者と協議し、是正のための処置を行う。

3.「情報処理外部委託責任者」は、情報処理外部委託について「契約書」に記載の「委託費用支払方法」に従って、情報処理責任者の承認を得て、費用を支払う。

第 16 条(情報処理外部委託成果の分析)

「情報処理外部委託責任者」は、実施した情報処理外部委託について、その成果を委託業務実施結果から実施達成度を分析し、委託先のスキルセットを再確認し、その結果を情報処理責任者および情報処理統括責任者に報告する。

第 17 条(情報処理外部委託結果の評価)

情報処理責任者は、実施された情報処理委託の実施結果について、実施後に部署業務の質の向上や効率向上の変化の観察を行い、情報処理外部委託結果の評価を行う。評価の結果、問題がある場合は、情報処理外部委託の改良・改善を検討し、情報処理統括責任者にその結果を報告し、承認を得なければならない。

第３章　情報処理外部委託のセキュリティ管理

第 18 条(情報処理外部委託機密契約の締結)

「情報処理外部委託責任者」は、情報処理外部委託を行う場合は、外部委託業者との間で、次の各号に示す機密契約に関する事項を含めた外部委託契約を取り交わさなければならない。

①法的な要求事項(例:データ保護法)

②外部委託に関わる全ての当事者のセキュリティ責任を明確にするための取り決め

③当社と同等のセキュリティ教育と訓練の実施

④組織の業務資産の保全性、機密性を維持し、テストする方法

⑤組織の重要な業務関連情報へのアクセスを、許可された利用者のみに制限するための物理的、論理的な管理対策

⑥災害発生時に、サービスの可用性を維持するための方法

⑦外部委託先の装置に対して実施する、物理的なセキュリティ対策

⑧監査の権利

第 19 条(情報処理外部委託機密契約事項遵守の監視)

1.「情報処理外部委託責任者」は、外部委託業者の業務管理者や業務担当者に対する機密事項教育やその遵守が徹底されているかを定常的に監視し、問題がある場合は、情報処理責任者に報告し、是正のための処置を講じなければならない。

2.「情報処理外部委託責任者」は、外部委託業者の業務管理者や業務担当者に対する機密事項教育やその遵守の検証を 6 カ月ごとに実施し、その検証結果を情報処理責任者に報告しなければならない。

3. 情報処理責任者は、前項の検証結果に問題がある場合は、情報処理統括責任者に報告し、是正のための処置を講じなければならない。

第 20 条(情報処理外部委託システム文書のセキュリティ管理)

1.「情報処理外部委託責任者」は、情報処理外部委託のための各種システム文書を「秘密保持規定」に従って秘密情報分類を行うこと。

2. 極秘、秘、社外秘に分類されたシステム管理のための各種システム文書には、「情報処理外部委託責任者」の許可した者以外がアクセスできないようにすること。

3. 極秘、秘、社外秘に分類されたシステム管理のための各種システム文書を廃棄する時は、シュレッダーに掛けて廃棄すること。

4. 極秘、秘、社外秘に分類されたシステム管理のための各種情報・データを廃棄する時は、完全削除すること。

第 21 条(情報処理外部委託のセキュリティ問題発生後の対応)

「情報処理外部委託責任者」は、情報処理外部委託においてセキュリティ問題が発生した場合は、「セキュリティ管理者のための情報セキュリティガイドライン」に記載の「セキュリティ管理者のセキュリティ問題への対応」に従って対応すること。

第 4 章　規定の改廃および周知

第 22 条(規定の改廃および周知)

1. この規定の改廃は、情報処理外部委託責任者が立案し、情報処理統括責任者の決定を得て行う。

2. 前項の決定事項は、これを社内に周知しなければならない。

〔６〕 情報セキュリティガイドライン
１． 情報セキュリティ管理者のための 情報セキュリティガイドライン
２． 情報システム利用者のための 情報セキュリティガイドライン

１． 情報セキュリティ管理者のための 情報セキュリティガイドライン

本ガイドラインは、情報処理規定集に準じるものとして制定します。

ただし、ここに掲載するものは、技術的な変化が激しくて標準化にそぐわないもの、運用面の事項であるために環境変化による変更が著しいものなどをまとめているため、外部環境の変化などに合わせ随時変更を行なってまいります。

当社の情報管理全般を主管する情報処理統括責任者を補佐して、全体効率最適化を目指すのがセキュリティ管理者の皆さんです。本ガイドラインは、皆さんが実際のシステム運用時に手順的に大きな間違いが起きないようにすることを主眼としていますので、随時このガイドラインを参照し、自らの管理態度・状況がこのガイドラインに沿っているのかどうかを確認してください。

なお、セキュリティ管理者とは、情報処理統括責任者、情報処理責任者、情報通信ネットワーク管理責任者、情報・データ管理責任者、システム管理責任者、サーバー管理責任者、データベース管理責任者、システム開発責任者を指します。（「セキュリティ管理規定」第７条）

１ 情報セキュリティ実施ガイドー組織・人的運用

（１） 情報セキュリティ推進分科会の設置

①情報セキュリティ委員会規定第４条第２項（２）に基づき、情報セキュリティ委員会の実務組織としてこの分科会を設置し、運営する。分科会のメンバーは、情報セキュリティ委員会がセキュリティ管理者等から選出した者とするが、代行・代理を認めるものとする。分科会メンバーの任期は１年とし、再任を妨げない。情報システム部を事務局とし、１回／３カ月を目処として開催する。

②本分科会は、情報セキュリティ確保のための具体的な方法と手段の策定を行なう。

③本分科会は、情報資産の秘密分類、情報資産の保護、監査、リスク分析、情報処理要員の教育と訓練、その他のセキュリティポリシーの普及徹底のための対策を検討・実施する。

（２） 情報セキュリティ専門家組織との連携、専門家からの支援

①当社は下記のセキュリティ関連組織と密接な連携をとり、セキュリティに関連する外部情報の早期入手・活用をはかる。(各組織と対応する情報の例を[　]内に示す)

・　財団法人日本規格協会[→セキュリティ標準技術、JIS 規格動向]

・　財団法人日本情報処理開発協会（ＪＩＰＤＥＣ）[→ＩＳＭＳ動向]

・情報処理振興事業協会（IPA）セキュリティセンター[→ウィルス関連情報、セキュリティ対策全般]

・コンピュータ緊急対応センター（JPCERT／CC）[→不正アクセスに関する動向、情報]

②外部のセキュリティコンサルタントや顧問弁護士との契約

・外部のセキュリティコンサルタントや顧問弁護士と契約し、セキュリティ問題発生時には、情報システム部及びセキュリティ管理者とホットラインを結び、いつでも助言を得られるようにする。

・必要に応じてセキュリティコンサルタントや顧問弁護士に、情報セキュリティ推進分科会に出席してもらう。

③外部の独立監査法人との契約

・情報セキュリティ問題が発生したときは、独立の監査法人と契約を結び、情報セキュリティに関する定期監査を受けることとする。

（3）　情報セキュリティ管理に関する訓練・教育・監査の取り組みについて

①情報処理統括責任者は、個別事業部と協力して情報セキュリティに関する訓練・教育を行なう。

②訓練は、全事業部でセキュリティに関連する者に対して実施する。訓練内容については外部コンサルタント、顧問弁護士、監査機関などと相談し、毎年見直しをしていくものとする。訓練の結果は教育実績として残し、全社情報処理教育責任者で管理する。

③教育に関しては、階層別教育、事業部での必須教育として行なうが、全社情報処理教育責任者がカリキュラムを毎年見直すものとする。この見直しに関しては外部コンサルタント、顧問弁護士や情報セキュリティ推進分科会と協議し、自社や外部での問題発生事例を随時組み込むものとする。

④内部監査室長は、各事業部、本社部門に対し、毎年計画的にセキュリティ監査を行なう。

⑤監査結果についての報告は、該当事業部長と情報セキュリティ委員会に対して行なう。本結果については、極秘のレベルとし、一般公開をしない。本監査で発見された問題に関しては、監査報告から２週間を目途として改善を行なう。

（4）　システム特権管理の考え方

①社内公開 Web サーバーの管理は、情報システム部に限定する。

②各事業部が運用・管理するサーバーの管理権限は、事業部の情報処理責任者に属する。

③管理権限の移管の決定及び権限付与は、情報処理責任者の責任で行なう。移管された管理権限を、さらに第三者に移管することを禁止する。権限の付与及び移管は、全て監査ログ情報を採取する。

④管理担当部員には、業務の遂行に必要な資源の利用に限定して、情報処理責任者よりアクセス権限が付与される。

⑤特権を付与されている人は、特権を使用して作業する時と、特権を必要としない通常の業務の時とでは、異なった利用者 ID を使用する。特権を使用した業務中に通常の業務は行なわない。

⑥全社に及ぶシステムの製品（例：OS、DBMS、アプリケーション）に関連する特権は、情報処理統括責任者が管理する。

（5） 情報システムの運用・管理担当者の審査

①情報システムの運用・管理担当者は、ネットワーク上において特別権限を保持することになるため、就任前において以下の項目の審査を実施する。専門職として採用する場合には、採用時に下記の調査をした上で採用の可否を決める。本審査の主管は人事部門とし、情報システム部の独自審査では済まないことを基本とする。

［正社員の身元審査］

・満足できる人物であることの証明（仕事と性格）
・応募者の履歴と専門資格の確認
・人間関係や金銭的な問題がないこと、行動に異常がないことの確認

②差別問題に踏み込まないことを前提として、本人が信用できることを確認する。

（6） 情報システムの運用・管理担当者の管理

①管理権限を付与している担当者については、運用開始後も信用チェックを定期的に実施する。同じ審査を委託業務実施要員に対しても実施する。これらのスタッフが委託先で採用されている場合は、委託先との外部委託契約書に委託先の審査責任を明記し、さらに審査が完了しないか審査結果に疑義や懸念がある場合は、委託先が負うべき通知手続きを明記する。

②情報システムに対する全ての作業は、上位のスタッフによる定期的なレビューと承認手続きを受ける。管理者はスタッフの個人的な事情が作業に影響することを認識し、人間関係や金銭的な問題、行動やライフスタイルの変化、欠勤、ストレスや失望感の兆候等に、常に注意をはらう。

（7） セキュリティ問題からの学習

①セキュリティ問題について、発見・検出したセキュリティ管理者および情報システム部は、それぞれ下記の内容を情報セキュリティ委員会に対してフィードバックする。情報セキュリティ委員会ではこれを蓄積し、防護策を徹底するとともに、教育・訓練などの材料として活用する。

・問題の内容
・影響（被害額、想定被害額）
・対処方法（暫定的対処方法、中長期的対処方法）

（8） セキュリティ管理者のセキュリティ問題への対応

①セキュリティ管理者は、セキュリティ問題に対応するために、次のような能力を持つ必要がある。また、問題発生時には次のような対応が不可欠である。

［能力要件］

・情報システムの故障やサービスの停止に、適切に対処することができる。

・サービス提供の拒否に対処して、善後処置を定めることができる。
・不完全または不正確な業務データを原因とするエラーに、対処することができる。
・秘密保持違反に対処するために、必要な対応策が実行できる。

[問題発生後の対応内容]

セキュリティ問題に対応する者は、次の項目に注意して問題の保存・解析・復旧を行なう。

・セキュリティ問題発生原因の分析と識別を行なう。
・問題回復により影響を受けたり、問題回復作業にかかわる人への連絡を行なう。
・関連官庁へ、問題及びそれに対して講じた処置を報告する（報告できる準備をする）。
・内部問題の分析、潜在的な契約違反や規則違反の証拠としての情報、あるいは民事及び刑事訴訟（例：コンピュータの誤用、データ保護法違反）の証拠としての情報、ソフトウエアやサービス提供者からの補償金獲得交渉のために、監査証跡や同等の証拠を採取し、安全に保管する。
・セキュリティ違反からの回復やシステム障害の修正措置は、慎重にかつ正式な手続きで管理する。
・動作中のシステムやデータに対するアクセス権限を明確に識別し、許可された担当者がアクセスする。
・実施した全ての非常措置は、詳細に文書に記録する。
・非常措置を情報処理責任者に報告し、十分なレビューを行なう。システムの安全性を確認する。ただし、復旧による遅延は最小限にする。
・再発防止対策の計画を立案し、実施する。

（9） システム利用者の登録手続き

①利用者の登録及び抹消の手続きは以下とする。

- システムの利用者は、認証ディレクトリに登録する。
- 認証ディレクトリを管理する情報処理責任者は、部員の業務遂行のために必要なソフトウエアとデータが利用できるように、利用者登録を行なう。
- 職務に変動があった場合には、情報処理責任者は、直ちに利用者の登録を更新（抹消または変更）する。
- 登録、更新（抹消または変更）に関するログデータを採取しておく。
- 利用者登録は、個人単位で行なう。個人ごとに一意に識別するための利用者 ID を付与する。
- 利用者は、サーバーの利用に際して、この利用者 ID を使用する。個人の利用者 ID を、他人と共用してはならない。
- グループとしての利用者 ID は付与しない。
- 利用者は、本人確認のために、パスワードを登録する。

②情報処理責任者は、３カ月に 1 回、利用者の登録内容が妥当であることを確認する（重複利用者 ID、利用権限など）。

③情報処理責任者が、明確に許可しない限り、サーバー上の情報は利用不可とする。

④社員（派遣社員・臨時社員を含む）は業務を行なうにあたって秘密保持契約を結ぶ。この秘密保

持契約の中には不正アクセスの禁止条項を記載する。

（１０）　利用者アクセス権限の見直し基準

①情報処理責任者は、１回／６カ月、部員のアクセス権限の妥当性を見直す。
②情報処理責任者は、１回／３カ月、特権の妥当性を見直す。
③情報処理責任者は、１回／３カ月、部員のアクセス権限や特権に不正がないことを確認する。

（１１）　業務システムの管理について

①社外公開セグメント内のサーバーでは、業務アプリケーションを動作させることはできない。
②業務アプリケーションは、各事業部管理サーバーなど社内セグメントでのみ実行する。
③ファイアウォールは、専用のシステムで動作させる。
④各業務アプリケーションが取り扱う情報の秘密分類の中で最も高い秘密分類を、その業務アプリケーションの秘密分類とする。
⑤情報処理責任者は、各業務アプリケーションの秘密分類を明確にする。
⑥情報処理責任者は、各業務アプリケーションごとに、実行を許可する部員と扱うデータベース（ファイル）に対するアクセス権限を設定することにより、アクセス制御を徹底する。

2　情報セキュリティ実施ガイドー技術的運用

（1）　コンピュータウィルス対策

①不正ソフトウエアから情報資産を保護するために、社内で利用する全ての PC について最新のワクチンプログラムを導入する。管理者は利用者に対し、PC 起動時からメモリーに常駐する形式でワクチンプログラムを稼動させるよう指導する。なお、会社は自動的に新規パターンファイルを提供するシステムを構築する。
②情報システム部は、パターンファイル配布用のサーバーには最新のパターンファイルを格納し、定期的にクライアントをチェックし、常に最新のパターンファイルを維持する。また、PC に最新のワクチンプログラムがインストールされているかを定期的にチェックする。
③各事業部は、業務上の必須教育の１つとして、事業部の責任でコンピュータウィルス対策に関する教育を実施する。この教育には問題を検出した際の報告と対処を含める。
④会社は、ソフトウエア使用許諾契約書の契約事項の遵守と非認可ソフトウエアの使用の禁止を宣言している。これが遵守されなかった場合に逸失する可能性がある利益の大きさに鑑み、本内容に反した利用者に対しては、厳罰で処することとする。
⑤セキュリティ管理者は、1 回／月、自事業部が管理している重要な業務を扱うシステムのソフトウエアやデータに承認されていないファイルや認可されていない変更がないことを検査する。この検査内容は記録として残しておく。
⑥セキュリティ管理者は、ウィルス感染からの回復のために適切な事業継続計画（必要な全てのデータやソフトウエアのバックアップと回復の準備を含む）を作成する。

⑦情報システム部は、不正ソフトウエアに関する情報を積極的に収集する。

（2） 電子メールのセキュリティ運用について

①情報処理統括責任者及びセキュリティ管理者は、電子メールの運用に関して以下の対策を実施する。

・すべての利用者に、電子メールソフトの機能を用いて、公開鍵方式による暗号の公開鍵と秘密鍵を生成させる仕組みを運用し、利用者自身のパソコンのハードディスク上にパスワード付で格納させる。さらに社内の認証局に、生成した公開鍵を含む証明書の登録を徹底する。

・電子メールを含む、社内と社外との間で送受信される全てのデータはメールサーバーでウィルスチェックを行なう。

・通信サービスが拒否される危険性を配慮して、緊急の通信手段を装備する。

・業務にかかわる情報を社外から受信する場合は、次の内容を徹底させる。

－データの秘匿と保全を確保するために、相手先には暗号化して電子署名を付けて送信してもらう。

－受信時は、添付された電子署名の正当性を確認し、自分の秘密鍵で暗号化された通信データを復号化する。

－復号化したデータは、利用する前に必ずウィルスチェックを行なう。

・業務にかかわる情報、法的問題に関わる事項（例：作成元、発送、配達、受領の証明）を社外に送信する場合は、通信データのウィルスチェックを行い、暗号化し、電子署名を付けて送信するよう指導を行なう。また、あて先が間違って誤配されることを防ぐために、重要な通信については、受信確認を義務づける。

・極秘レベル情報の社内通信は、データの秘匿と保全を確保するために暗号化して行なうよう、指導を行なう。

（3） サーバーへのログオンについて

①サーバーへのログオンについて、以下の仕組みで手続きを行なう。

・ログオン処理では、不正な利用者のアクセスを防ぐために、システムに関する情報の開示は最小限にする。

・システムやアプリケーションの識別子は、ログオンプロセスが成功するまで表示しない。

・コンピュータシステムへのアクセスは、許可されている利用者に限定される旨の一般警告を表示する（不正アクセス防止法への対応）。

・入力データ（パスワード）のどこが間違っているかなど、ログオン処理中に許可されていない利用者を助長するようなメッセージを表示しない。

・ログオン情報の妥当性確認結果の表示は、全てのデータの入力が完了した時点で行ない、エラーが検知されても、入力データのどの部分が間違っているかを表示しない。

・許容するログオン連続失敗回数を３回に制限し、下記を実施する。

－失敗した試みは記録する。

－ログオンの試行を許可する前に、一定のディレイタイムを設けるか、特別な許可を要求する。

－データリンクの接続を切る。

・ログオン処理のために許容される最長時間を１分間とし、この制限を超える場合には、ログオン処理を終了させる。
・ログオンが成功した時点で、下記の情報を表示すること。
－前回のログオンが成功した日時
－前回のログオン以降に、失敗したログオンがある場合は、その詳細

（４）　社外との情報、ソフトウエアの交換について

①社外と情報やソフトウエアを交換する場合は、ソフトウエア使用条件を明記した正式な契約書を取り交わすこと。
②契約のセキュリティ関連事項として、情報の秘密分類に応じた取り扱いを行なうこと。
③会社は、利用者がインターネットから許可なく表示やダウンロードした情報に責任を負わない。
④セキュリティ条件にかかわる契約事項として、下記を契約内容に含める。
・発信、発送、受領を管理し、通知する管理責任
・送り主、発信、発送、受領を通知する手続き
・梱包や発信の際に適用する必要最小限の技術規格
・宅配業者の身分確認方法
・データ紛失時の保証責任
・重要な情報に対する秘密分類とその管理方法
・情報やソフトウエアの所有権、データ保護の責任、ソフトウエアの著作権
・情報やソフトウエアの記録や読み出しに関する技術規格
・暗号秘密鍵の保護対策

（５）　運送中の媒体のセキュリティについて

①バックアップセンターへのバックアップデータの転送は、信頼できる運送業者による媒体の搬送または通信回線を介した暗号化したデータの転送とする。
②搬送を認可する宅配業者について、情報・データ管理責任者の合意を得ること。
③梱包は、運送途中で発生しがちな物理的な損傷から内容物を保護するために、十分な強度を確保し、製造業者の仕様に従うこと。
④重要な情報を無許可の開示や変更から保護するために、その情報に応じて施錠付のコンテナの使用、手作業による配達、不正なアクセスの跡が残るような包装、貨物を複数ルートで出荷するなどの対策を実施する。

（６）　電子取引のセキュリティについて

①詐欺、契約紛争、情報の暴露や改ざんなどの脅威から電子取引を保護するために、一般顧客には認証センターより証明書を取得させる。これをサービスの前提条件とする。
②一般顧客と WWW サーバー間は、SSL による通信を行ない、通信データの秘匿・保全を確保する。
③取引関連の注文書、受領書は一般顧客の電子署名を添付させる。受注サーバーは、一般顧客からの電子署名付のメッセージを証拠として保管しておく。

④顧客に義務付ける契約書によって、権限の詳細を含め合意された取引条件を裏付ける。
⑤サービスに関する条件を顧客に公表する。
⑥電子取引に用いられるホストコンピュータに対する攻撃からの保護や、システム構築時に必要になるネットワーク接続にかかわるセキュリティ問題に対して配慮する。

（7） 一般公開サーバーについて

①一般顧客などがアクセスする公開用サーバーに対しては、以下のようなルールで対応を行なう。
・一般顧客に公開している受注用の情報については、アクセス制御を適用し、営業部の管理者またはそれに代る者が所定のルールに従って行なう場合以外、変更や削除は不可とする。
・受注用の情報の公開に際して、営業部門の長の許可を必要とする。
・公開用サーバーでソフトウエア、データや他の高いレベルの保全が要求される情報を使用する場合、適切な機能（例：電子署名）によって保護する。
・顧客データとして入力されるデータは、顧客管理サーバーにアクセス制御を適用して管理する。顧客管理サーバーは公開サーバーと別のサーバーに構築し、この顧客データには、許可された業務担当者以外はアクセスできない。
・一般顧客は公開サーバーのみにアクセスできる。

（8） システム管理側のパスワード管理

①利用者の本人確認はパスワード（指紋照合、虹彩照合、その他のバイオメトリックスシステム、USB ロックキー、IC カード、等も可）を使用する。パスワードは、他人に推測されたり暴露されたりしないような管理を行なう。
②パスワードの管理に関して、下記を実施する。
・責任を明確にするために、各人がパスワードを使用し、他人と共用しない。
・利用者が自分でパスワードの決定と変更を行なうこととし、入力時のエラーを見込んだ確認手続きをシステム側で行なう。
・利用者に対し、信頼性の高いパスワードの選択を行なうことを義務化する。
・過去に使用したパスワードの記録を保持（３世代）し、３世代は同じパスワードの使用を禁止するようシステムの設定を行なう。
・パスワードは入力時にスクリーン上に表示しない。
・パスワードファイルはアプリケーションファイルと分離して保管する。
・パスワードは、一方向の暗号アルゴリズムを用いて暗号化して保管する。
・デフォルトのベンダーパスワードは、ソフトウエアをインストールしたら直ちに変更する。

（9） システム管理側のシステムユーティリティ

①システムユーティリティについては、許可された人だけが使用できるようにアクセス管理（実行権の付与）を行なう。
②システムユーティリティについて以下の施策を講じる。

・利用に際しては、パスワードまたはそれに代る手段による認証を行なう。
・アプリケーションソフトウエアから分離する。
・可能な限り少数の信頼できる許可者に使用を制限する。
・特別な使用については、情報処理責任者の許可を必要とする。
・情報処理責任者は使用条件を設定する。
・利用に関して監査ログを採取する。
・不要なシステムユーティリティはシステムから除去する。

（１０） 外部アウトソーシング先との接続について（メッセージ認証）

①インターネットや公衆電話網の利用は、通信データが改ざんされる危険性がある。外部のアウトソーシングサーバーとの通信データ、契約企業との通信データ、携帯 PC との通信データは、いずれも業務上重要である。このため、これらの通信時には通信データの暗号化と電子署名によるメッセージの認証を行なう。

（１１） プログラムソースライブラリの管理詳細について

①プログラムソースライブラリは、運用システムには保持しないで、開発用サーバー内の運用ソースコードライブラリで管理する。
②各アプリケーションごとに、プログラムライブラリ管理責任者を任命する。
③プログラムソースコードへのアクセスは許可性とする。
④開発や保守中のプログラムは、運用プログラムソースライブラリとは別の開発プログラムソースライブラリで管理する。
⑤プログラムソースライブラリの更新や開発者へのプログラムソースの配布は、アプリケーションのプログラムライブラリ管理責任者によってのみ実施する。
⑥プログラムリストは安全な環境に保持する。
⑦ソースプログラムの旧バージョンはアーカイブしておく。その際、それらが運用された正確な日時、全ての関連ソフトウエア、ジョブ制御、データ定義と手続きを明確にしておく。
⑧プログラムソースライブラリの保守やコピーは、全て開発サーバーのアクセス制御のもとで実施する。

（１２） 隠れ通信路と“トロイのコード”の防止

①プログラムに設定されるとセキュリティホールが作られてしまうソフトウエアコードを“トロイのコード”という。このコードが当社のイントラネットシステムに忍び込むことがないように、当社で使用するプログラムは下記の事項に配慮する。
・プログラムは信頼の高い製造元から購入する。
・コードの内容が確認できるように、ソースコードでプログラムを購入する。
・評価された製品を採用する。
・使用前に全てのソースコードを検査する。
・インストールされた以降のコードへのアクセスやコードの変更を制限する。

・重要なシステムに関わる作業は、信頼できるスタッフに行なわせる。

（１３） 事業継続計画と影響分析

トラブルが発生した際における影響分析とともに対応計画（コンティンジェンシープラン）を作成しておくことが重要である。このためには「リスク分析」を行ない、対応するシステムを早期に運用に供しなくてはならない。事業継続計画では、次の事項を考慮しなければならない。

・全ての責任と非常時の手続きを明確にし、合意すること。
・要求された時間内に回復または復旧するための非常時手続きを実行すること。
・合意された手続きや処理に関する文書を作成すること。
・危機管理を含め、合意された非常時手続き及び処理に関して関係者を教育すること。
・計画をテストし、更新すること。

［計画の作成］

①各事業継続計画では、実行開始条件と計画の各コンポーネントごとに実行する各個人の責任を明確に指定する。

②新たな要求事項が明確になったときには、確立されている非常手段（例：避難計画や最終対応手段）を適切かつ迅速に修正する。

③事業継続計画作成の枠組みでは、下記の事項を考慮する。

・各計画が実行開始される前に従うべきプロセス（例：状況の評価、かかわるべき人）を記載した、計画を実行するための条件。
・業務の運用や人命が危険にさらされる事故発生時の措置について記載する非常時の手続き。この手続きには、広報管理の取り決めや適切な機関（例：警察、消防署、地方行政機関）への効果的な連絡に関する取り決めを含める。
・主要な業務活動や支援サービスを代替の場所に移動するため、また、業務プロセスを要求時間内に回復するための最終対応手段の手続き。
・正常な業務に復帰するための措置、再開手続き。
・計画をいつ、どのようにテストし、どのようなプロセスで維持するか、を指定する保守スケジュール。
・事業継続プロセスを理解させ、そのプロセスが有効かつ確実に継続されることを可能にするための教育と意識向上活動。

④個人の責任を明らかにする。計画のどのコンポーネントにだれが責任を持つかを記載する。必要に応じて代理を任命する。

⑤個別の計画には特定の所有者を規定する。

⑥非常時手続き、マニュアルの最終対応手段計画、再開計画等の作成は、関係する適切な業務資源やプロセスの所有者の責任範囲内とする。

［事業継続計画の見直し］

①事業継続計画は、１回／６カ月、テストすること。

・事業継続計画のテストは、復旧チームの全てのメンバーと他の関連スタッフが、この計画の内容を確実に認識できるようなものにする。

②事業継続計画のテストスケジュールでは、計画の各要素がどのようにして、いつテストされるかを示す。

③事業継続計画のテストでは、下記の事項を考慮する。

・種々の状況に対するテーブルトップテスト（障害例を用いた業務回復配備の検討）

・シミュレーション（特に事故後の危機管理担当者の訓練）

・技術的回復テスト（情報システムを有効に復活させることができることを確実にテストする）

・完全なリハーサル（組織、スタッフ、装置、設備、プロセスが障害に対処できることをテストする）

④テストは、保守ツールなどを活用し、実務に影響を与えない範囲において、実際に障害を発生させて確認する。

⑤事業継続計画の継続的有効性を確保するために、１回／６カ月、レビューや更新を行なう。

⑥事業継続事項への適切な対処を確実にするための手続きは、組織の変更管理プログラムに含む。

⑦事業継続計画の定期レビューの責任は、事業部長が負う。

⑧事業継続計画に反映されていない業務管理の変更を明らかにし、その変更に従って計画を適切に更新する。

⑨正式な変更管理プロセス、更新された計画を配付し、完全な計画の定期的なレビューによって強化する。

3　情報セキュリティ実施ガイドー建物・設備環境運用

（1）　建屋管理の具体例

①情報処理機器が格納される建屋については、次のような点を注意して管理を行なわなくてはならない。

・情報処理設備を含む領域を「保護区域」に設定して、物理的な外壁で保護し、出入りの管理は係員がチェックする。

・建屋の外壁は一枚壁の構造にする。

・全ての外部ドアには、警報装置を設置し錠で保護する。

・建屋または建物へのアクセスは許可された者だけに制限する。

・セキュリティ外壁の全ての防火扉は、警報装置付で隙間なく閉まるものにする。

・保護区域への無許可の訪問者を退出させる。許可した訪問者については、その出入りの日時を記録する。

・保護区域への訪問者の訪問目的を制限する。

・保護区域のセキュリティ要求事項と非常時の手続きについて取り決める。

・重要な情報や情報処理設備へのアクセスは、管理され許可された人だけに制限する。

・全てのアクセスに関する監査証跡を正確に保管する。

・全てのスタッフはすぐに認識できる身分証明書を携帯する。
・保護区域へのアクセス権は、定期的にレビューし、更新する。
・保護区域の選択と設計においては、火災、洪水、爆発、社会不安、その他の自然及び人災の危険性を考慮したものにする。
・保護区域に隣接する建屋からの脅威（例：水漏れ）を考慮する。
・主要な設備は、一般の人の立ち入りを避ける場所に設置する。
・建物は目立たないものにし、その目的を示す表示は最小限とし、情報処理にかかわる存在を示す標識は、建物の内外を問わず、一切、非表示とする。
・情報を損なう危険性のある無用なアクセスを避けるために、処理支援機能（例：コピー機やファクシミリ）は、保護区域内に適切に設置する。
・スタッフが不在の場合は、ドアや窓は施錠する。
・１階の窓は外部からの侵入に対する保護を考慮する。
・全ての外部ドアや手が届く窓には、侵入検知システムを設置する。
・無人領域は常時、警報装置の電源を入れておく。
・組織によって運営される情報処理設備は、第三者によって運営される設備とは物理的に分離する。
・情報処理設備の場所を明示してある住所録や社内電話帳は、一般の人が容易に見ることができないように管理する。
・危険物や可燃物は保護区域から十分に離れた場所に安全に保管する。
・バックアップ媒体は、メインサイトで災害が発生しても、その災害によって損傷しないように、十分に離れた場所に設置・保管する。

（2） セキュリティチェックリスト

情報システムを管理、運用している事業部・部門のメンバーは下記内容を確認して、実施されているかどうかを報告することとする。

[保護区域内での業務について]

・保護区域での作業は、安全上の理由と不正行為を避けるために監督者不在で実施しない。
・社員が不在の保護区域は物理的に施錠し、定期的に確認する。
・第三者の保守要員に対しては、必要な時に限り保護区域や情報処理設備への限定アクセスを許可する。このアクセスは許可性であり、監視する。
・許可しない限り、写真撮影、ビデオ撮影、オーディオ他のレコーディングを行なってはならない。

[受け渡しエリアについて]

・無許可アクセスを避けるため、受け渡しエリアを管理し、情報処理設備からは隔離する。
・受け渡しエリアに対するリスク分析を実施する。
・建物外部からの受け渡しエリアへのアクセスは、身分証明書を所持している許可者に限定す

る。
・納品業者は建物の他の場所にアクセスしないで、品物を渡すことができるようにする。
・受け渡しエリアの内部ドアが開いている際は、外側のドアは閉める。
・搬入物は、受け渡しエリアから使用する場所に移動する前に点検し、登録する。

[装置の取り付け位置と保護について]
・装置は、環境上の脅威や非許可アクセスの機会を軽減できるような場所に設置し、それ自体の保護を行なう。
・装置は、作業エリアへの不必要なアクセスを最小限に抑えられる場所に設置する。
・重要なデータを処理する処理装置や保存設備は、使用中の状態を監視できるような位置に設置する。
・特別な保護が必要な装置は、他の装置から隔離して保護する。
・窃盗、火災、爆発、煙、水、埃、振動、化学物質の作用、電源供給妨害、電磁波放射を含む潜在リスクを最小限に抑えるための管理対策を実施する。
・情報処理設備の近傍での飲食や喫煙は禁止する。
・情報処理設備の運用に悪影響を及ぼす危険性に関して、その環境条件を監視する。
・近隣の建屋で発生する災害（例：火災、水漏れ、地下室浸水、爆発）からの影響を配慮する。

[装置の電源について]
・停電やその他の電源異常から装置を保護する。
・装置製造業者が指定した仕様に適合した電力を供給する。
・偶発事故対処計画では、無停電電源装置（UPS）が故障した場合の措置について考慮する。
・UPS 装置に対して、製造業者の勧告に従って容量の十分性の確認とテストを定期的に実施する。
・長時間の停電でも処理を継続しなければならない場合には、バックアップ発電機を装備する。
・発電機を取り付けた場合には、製造業者の指示に従って定期的にテストする。発電機を長時間運転できるように十分な燃料の供給を行なう。
・非常用電源スイッチは、非常時に直ちに電源を切断できるように装置ルームの非常口近くに設置する。主電源が停電した時のために非常用の照明を装備する。
・落雷防護は全ての建物に設置し、落雷防護フィルターを全ての外部通信回線に設置する。

[ケーブル配線について]
・データ転送や情報サービスのために使用する電源や通信ケーブルの配線は、傍受や損傷を受けないように保護する。
・情報処理設備に接続する電源や通信回線の外部からの取り込みは地下の埋設で行なう。
・ネットワークのケーブル配線に対する非許可の傍受や損傷から保護する。
・干渉を防止するために、電源ケーブルを通信ケーブルから分離する。
・重要なシステムについては、代替の経路や伝送媒体の使用、光ファイバケーブルの使用を配

慮する。

［装置の保守について］

・装置に対して、供給業者が推奨する整備間隔と仕様に従って保守を行なう。
・許可した保守担当者だけが装置の保守を行なう。
・発生した全ての障害や障害と判断される事象、全ての予防保守、全ての修正保守に関する記録を作成し、保管しておく。
・保守のために装置を建屋外に搬送する場合には、格納データを完全消去する。

以上

２．情報システム利用者のための情報セキュリティガイドライン

本ガイドラインは、情報処理規定集に準じるものとして制定します。ただし、ここに掲載するものは、技術的な変化が激しいもの、運用面等環境変化による内容変更が著しいもの、個人のシステム利用態度などによる部分が多いものなど、標準化するのにそぐわないものなどをまとめているため、外部環境等の変化などに合わせ随時変更を行なってまいります。

情報システム利用者（派遣社員・臨時社員を含む、以下同じ）の皆さんは、随時このガイドラインを参照し、自らの情報の利用態度、利用状況がこのガイドラインに沿っているのかどうかを確認して行動してください。

なお、皆さんは会社と「秘密保持誓約書」を交わしていることをくれぐれも忘れずにいてください。このガイドラインは、秘密保持などについての約束事を守るための手引きでもあります。

1　オフィスにおける情報セキュリティマナー

（1）　情報の取扱いと保管について

①書類や記憶媒体は、それを使用しない時、特に作業時間外には、放置したままにしてはいけません。施錠した机の引出しやキャビネット、またはセキュリティが確保された保管庫等に保管してください。特に、重要なビジネス情報は、それを使用しないときやオフィスを離れるときには、施錠して保管管理をしましょう。

②オフィス内の郵便物を他人が勝手に開封したり、持ち出したりできないよう管理してください。そのために、オフィス内における郵便物の受入・受渡場所を保護する必要があります。

③写真機や複写機の使用ルールを明確にして、無許可で使用されないようにしてください。

④電話、ファクシミリ、ビデオ通信・TV 会議システム等を使用して行なわれる情報の交換に対しても、「情報の秘密分類の取り扱い」に準拠してください。

⑤電話、ファクシミリ、ビデオ通信・TV 会議システム等を使用する時には、社員は、下記の事項に注意してください。

- 公衆電話、携帯電話を使用するときは、周りにいる人や盗聴機器による盗聴の危険性、電話の相手先にいる周りの人などを考慮して、発信する内容を考えてください。
- 公共の場所、オープンなオフィス、壁の薄い会議室などで秘密に関わる会話を行なわないでください。
- 無許可者による再生、ダイヤルミスによる誤保存などを避けるために、留守番電話のメッセージには重要な内容を残さないでください。

・ファクシミリを使用する場合には、特に下記の危険性に注意してください。
－ダイヤルミスまたは記憶間違いなどにより、間違った番号を呼び出して文書やメッセージを誤配信する
－「故意または誤りにより同報で特定の番号に送信される設定になっている状態」で文書やメッセージを誤配信する

（2） 事業所構内のセキュリティについて

①業務中は、身元を識別するために、見えやすいところに会社支給の名札をつけてください。
②入館時、入室時にカードを必要とする場所では、続けて後ろの人を招きいれてしまわないようにしてください。
③事務所内で迷っている人や名札をつけていない人がいたら、必ず声をかけてください。
④席を立つときは書類を裏返しにしておくようにしてください。
⑤不要となった情報はその時点で廃棄・消去をしてください。秘密情報（極秘、秘クラス）書類を廃棄する時は、必ずシュレッダーにかけてください。
⑥休憩時にオフィスに社員が誰もいなくなるような環境を作らないようにしてください。
⑦退社時や外出時に机の上に重要書類がない状態にしてください。
⑧個別オフィスへの最初の出社者、最後の退出者が分かり記録が残るようにしてください。

2 コンピュータシステムおよびパソコンの取扱いについて

（1） コンピュータシステムを利用できる範囲

①当社コンピュータシステムは、当社の重要な経営資産であり、正当な業務目的だけに利用できるものです。コンピュータシステムの利用権は、従業員に当然のものとして無条件に与えられるものではなく、業務上の特権として付与されるものです。利用者は業務を遂行するためにコンピュータシステムへのアクセスを許可されるものであり、個人的に利用してはいけません。
②コンピュータネットワーク上で作成、保管、送信、受信される情報・データは会社が設定する自動監視ソフトウエアで監視されています。会社のコンピュータは業務の遂行のためにあり、個人のプライバシーの保護は保証されていません。
③会社のコンピュータシステムは業務の遂行のために購入・整備されているものです。休憩時間といえども、私用の電子メールを打ったり、業務に関係のないホームページにアクセスしたり、ゲームをしたりすることは禁止します。

（2） パソコン利用の基本ルール

①パソコンに電源を入れたときに通常の表示画面と異なるなど、画面の様子に異常がないか、変わったところがないか、確認してください
②パソコンは利用者 ID とパスワードを入力しなければ利用できないようにしてください。

③パスワードはメモなどに書いておくことは避けてください。最低でも３カ月に１回はパスワードの変更を行なうようにしてください

④許可なくモデムなど通信機器をパソコンに接続してはいけません。

⑤モデムを用いた外部通信は、業務の必要性に基づいて必要最小限の範囲で行ってください。

⑥コンピュータのクロックの狂いを定期的(1 回／月)にチェックし､正しくない場合は修正してください。

⑦秘密情報などをパソコンで見る時やパスワードを打つときなどには、背後に他の人がいないかどうか確認するなど、他人に覗き見されないように注意してください。

⑧暗号化の鍵としてカードなどを用いる場合、この管理・保管に細心の注意をはかってください。複雑な暗号キーが組み込まれることになりますので、紛失すると業務に大幅な悪影響が出ます。

⑨情報漏えいを防止する意味合いもあり、業務上での無線 LAN の使用を禁止します。

（３） 暗号の利用管理

①暗号機能の使用に際しては、会社から支給されている機能だけを使用し、独自に入手したものを使用しないでください。

②暗号化データや暗号機能を他国に送付する場合は、国の輸出規制に抵触する場合があります。事業部長の許可を得たうえで送付してください。

（４） 離席時のセキュリティについて

①情報システム利用者は、パソコンが不正に利用されると、自分だけではなく、他人や会社が被害を受けることを認識し、パソコンのセキュリティに責任を持つことを約束しています。業務用のパソコンについて、下記の保護対策を実施しなくてはいけません。

・業務終了時にはセッションを切断しましょう。

・パソコン、端末を使用中に離席する場合、他人がパソコン内の情報やネットワーク内の情報に無断でアクセスするきっかけとなる恐れがあります。離席するときは、画面をクリアーし、キーロック、パスワードによる保護対策を実施してください。

・パソコン及び携帯パソコンは、未使用状態で一定時間を経過した場合にはパソコンの画面をクリアーし、キーロック、パスワードなどによる保護が自動的に行われるように条件設定してください。タイムアウトの時間は携帯パソコンで 5 分、社屋内のパソコンで 10 分とします。

（５） コンピュータウィルス防御に対する考え方と対応

①当社では、 コンピュータウィルスや不正ソフトウエアから情報資産を保護するために、業務で利用する全てのパソコンに最新のワクチンプログラムを導入することを義務付けています。パソコンを利用する社員及び関係者は、パソコン起動時からメモリーに常駐する形式でワクチンプログラムを稼動しなくてはなりません。なお、会社は自動的に最新パターンファイル、最新バージョンのプログラムファイルをネットワークにて配信するシステムを構築しています。

②パターンファイル配布用のサーバーには､定期的にLANに接続されているパソコンをチェックし、

常に最新のパターンファイルおよび最新バージョンのプログラムファイルが反映されるように自動更新を行っています。各利用者は、各自が使用するパソコンが、最新のパターンファイル、最新バージョンのプログラムファイルに更新されているかどうかのチェックを定期的(1回／月)に行ってください。

③携帯用パソコンに対しては、ウィルスチェックソフトおよびパターンファイルの最新版への自動更新を行っていません。VPNにより社内LANに接続する場合は、接続する前にウィルスチェックを行い、安全であることを確認してから接続してください。接続後は、ウィルスチェックソフトおよびパターンファイルの最新版への手動による更新操作を行ってください。

④コンピュータウィルスが発見された場合は、コンピュータウィルス対策チームに連絡し、対策チームメンバーの指示に従ってください。

⑤コンピュータウィルス対策に関する教育を、業務上の必須教育の一つとして実施しています。教育には、ウィルス発見など問題を検出した際の、報告と対処法を含めています。

⑥ソフトウエア使用許諾契約書の契約事項の遵守と非認可ソフトウエアの使用禁止を守ってください（業務で使用しているパソコンは会社のものですから、非許可のソフトウエアのインストールは業務を阻害していることになります)。

⑦外部ネットワーク経由で、あるいは、他の媒体よりファイルやソフトウエアを入手する場合には、作成元を確認してください。作成元が不明あるいは信頼できない場合には、入手してはいけません。入手した場合は、利用する前にコンピュータウィルスの検査を必ず行ってください。

⑧重要な業務を扱うシステムのソフトウエアやデータの内容に関して、1回／月、検査を行なってください。この自主検査内容と検査結果は記録として残しておかなければなりません。

処理内容や表示内容がおかしいと思った時は、すぐに処理をやめ、セキュリティ管理者に連絡してください。

（6） パスワード管理の手順

①利用者本人の確認はパスワードで行なっています。パスワードが他人に知られたり使用されたりしないように管理することは、雇用契約事項です。自主的な対応をお願いします。

②社内情報共有 Web システムおよびメールシステムの利用者には、職制経由で、直接、初期パスワードを通知します。その際、受領確認証が発行されます。システムへの最初のログオン時に、必ずパスワードを、本人指定のものに変更してください。

③利用者がパスワードを忘れた場合には登録パスワードを初期化し、本人であることを情報処理責任者が面談で確認した後、初期化パスワードを安全な方法で通知するようにしています。パスワードを忘れないようにしてください。

3　事業所外からのネットワークアクセスと携帯パソコンについて

（1） 外部接続時の利用者認証について

①業務上、外部から社内 Web サーバーにアクセスする必要のある社員は、事前の許可を得ることによって、インターネットを経由して暗号化通信（SSL）により社内 Web サーバーにアクセスできます。

②インターネット経由で社内 Web サーバーにアクセスを許可された社員は、SSL 通信許可データベースに登録されます。登録される内容は、利用者名と個人公開鍵です。個人秘密鍵および社内サーバー公開鍵は、IC カードを利用するためのパスワードとともに IC カードに格納され、登録利用者に配布されます。

③利用者は、社内 Web サーバーへのアクセスの際に、パスワードを入力して IC カードの正当な所持者であることを示します。

次に、社内 Web サーバーから送られてくるサーバー証明書を IC カード内になる社内サーバー公開鍵で復号化して、通信相手が社内 Web サーバーであることを確認します。（この操作は、Web ブラウザー上で行います。）

続けて、社内 Web サーバーに個人の秘密鍵で作成した個人証明書を送付します。（この操作も Web ブラウザー上で行います。）

④社内 Web サーバーでは、パソコンから送られてきた個人証明書を個人公開鍵で複合化して、通信相手が接続を許可された個人であることを確認します。相互に相手方の認証が完了すると、社内 Web サーバーとの間で SSL 暗号化通信が開始されます。

（2） 携帯用パソコンの運用について

①インターネットを経由して、社内 Web サーバーにアクセスできる社員と携帯パソコンを識別するために次の２点が仕組みとして整備されています。

・パソコンには個人秘密鍵および社内サーバー公開鍵を格納した IC カードを取り扱える仕組みを装備しています。

・社内 Web サーバーにアクセスできる社員には、個人秘密鍵および社内サーバー公開鍵を格納した IC カードを貸与します。IC カードの使用には付与されたパスワードが必要です。

②社外に持ち出すことができる携帯用パソコンに対して、下記の保護対策を実施してください。

・社員の使用する携帯用パソコンにはパソコン保護および SSL 暗号化通信を認証するための IC カードを装着します。

・IC カードの所有者確認はパスワードで行ないます。

・利用を許可する際、下記の事項に関する教育を実施します。この教育の受講者だけを使用許可対象者とします。

－社内サーバーから入手したすべてのデータは、ハードディスク上では暗号化して保存すること。

－意図した相手以外が周りにいる環境では使用しないこと。

－パソコンを手の届かないような場所に放置しないこと。

（3） ネットワークの分離と接続

①許可された社員のみ携帯パソコンから、インターネットを介して社内 Web サーバーにアクセスできます。

②通信モデムを社内 LAN に接続することは禁止します。

③社内 LAN と社外ネットワークの相互接続は、情報通信ネットワーク管理責任者の許可を必要とします。

④既設の社内 LAN への新規 LAN の接続は､情報通信ネットワーク管理責任者の許可を必要とします。

⑤社内 LAN への新規機器接続は、事業部長（情報処理責任者）および情報通信ネットワーク管理責任者の許可を必要とします。

4　電子情報の管理運用について

（1）　アクセス場所の特定

①許可された場所からだけ業務データを利用することができます。業務データは、事業部の情報保護方針に基づいてアクセス管理を行なうようにしなくてはいけません。

②公開サーバーシステムに、情報処理責任者の許可なく情報を掲載してはいけません。

（2）　情報、ソフトウエアの交換について

①社外組織との間で情報やソフトウエアを交換する場合、ソフトウエアの正しい使用条件（ライセンス数など）などを含めた正式な契約書を取り交わす必要があります。

②契約のセキュリティ関連事項として、情報の秘密分類に応じた取り扱いを行なわなくてはいけません。

（3）　電子情報化の中の個人情報保護

①個人(顧客を含む、以下同じ)情報の管理を厳格に行なうことが必要になっています。OECD「プライバシー保護と個人データの国際流通についてのガイドライン」に従って個人情報を保護します。

・個人情報は、個人の同意を得た上で個人が自ら提供した情報だけが保管できます。(収集制限の原則)

・個人情報は、サービスの提供に必要なものだけに限定し、「正確」「完全」「最新」を維持しなければなりません。(データ内容の原則)

・個人データ収集の目的を事前に個人に説明しなければなりません。(目的明確化の原則)

・利用目的は、該当するサービスに限定されます。(利用制限の原則)

・個人情報は、紛失、不正アクセス、破壊、開示などから保護しなければなりません。(安全保護の原則)

・個人データの管理については、該当する個人に通知しなければなりません。(公開の原則)

・個人からの要望があれば、登録内容を該当の個人に開示しなければなりません。(個人参加の原則)

・事業部長（情報処理責任者）は、上記の管理対策を実施する責任を負う。(責任の原則)

（４）　電子情報へのアクセス制御について

①情報処理規定集に基づくアクセス規則は、当社の情報システム全体に適用します。

②明らかに許可されない限り、アクセスはデータの所有者のみに限定されます。

③利用権限の制御は、データベース操作や OS の操作コマンドやツール（TELNET、FTP）などでも実施されます。

④一般顧客に関するすべての情報は、顧客管理サーバー上のデータベースだけに保管し、公開サーバーなどには置かないようにします。このデータベースの利用は、社内の情報システム施設内でだけ可能です。さらに、アクセス許可者及びその利用権限は「(管理部門）情報処理責任者」だけが指示できます。

⑤各サーバー上で動作する業務アプリケーションは、その業務アプリケーションからの利用が許可されたサーバー上のデータだけを利用できます。利用を許可されていない他のサーバーのデータを利用してはいけません。

⑥開発用サーバーで管理されているデータは、すべて部外秘の扱いとします。他のサーバーには、流通させないものとします。開発協力会社社員にも、開発用サーバーから入手した情報を契約に従って管理させなければなりません。

⑦業務受託範囲内の顧客の情報資産内にあるサーバーで管理されているデータは、全て「極秘」の扱いとします。

⑧情報の分類とその扱いは、当社イントラネットシステム全体に適用されます。当社イントラネット内で管理されているすべてのシステム操作やデータへのアクセスは、管理元の情報処理責任者が定めたアクセス権限に基づいて実施します。情報処理責任者が許可しない限り、該当のシステムへの操作や該当のデータへのアクセスは禁止します。

（５）　知的財産権保護について

①知的財産権の定義：「文芸、美術及び学術の著作物、実演家の実演、レコード及び放送、発明、科学的発見、意匠、商標、サービス・マーク及び商号その他の商業上の表示、不正競争に対する保護に関する権利ならびに産業、学術、文芸または美術の分野における知的活動から生ずる全ての権利」

②情報処理システムで扱うプログラムやデータは、この知的財産権の対象になりますので、以下のような保護措置をとります。

・著作権、意匠権、商標など、知的財産権があるものに関して、法的な規制事項を確実に遵守する必要があります。このために、情報の取り扱い規定（「セキュリティ管理規定」ほか）を作成し、定期的に教育を行なっていきます。

・ソフトウエアや情報処理製品の合法的な使用は、「セキュリティ管理規定」に準拠するものとします。

・ソフトウエア製品の取得手続きに関する規格（「セキュリティ管理者のための情報セキュリティガイドライン」）を発行します。

・ソフトウエア著作権やソフトウエア製品の取得手続きポリシーを維持し、それらのポリシーに違反したスタッフに対しては、罰則規定を適用する旨を通知します。（「情報セキュリティ基

本方針」）

・資産管理簿を作成し、管理します。（システム資源管理）

・ライセンス、マスターディスク、マニュアルなどの所有者に関する証拠を維持します。（総務部）

・情報システム部門は、ライセンス契約時の最大許容利用者数を超えないように管理します。

・情報システム部門は、許可されているソフトウエアや使用許諾を得ている製品を登録し、1回／６カ月、実態の確認を行ないます。（定期監査）

・事業部長は、ソフトウエアの使用許諾条件の遵守を部員に徹底させなければなりません。このため教育項目に含めなければなりません。

・管理規定に従ってソフトウエアの処分や他人への譲渡を行なわなければなりません。

・監査には、既定の監査ツールを使用しなければなりません。

・公衆ネットワークから得られるソフトウエアや情報に関しては、所有者の使用条件を遵守しなければなりません。

（６）　社外の電子掲示板、電子会議室等の利用に際しての留意事項と禁止事項

①社外の電子掲示板、電子会議室等で、許可無く会社としての意見を掲載する事は禁止します。社外の電子掲示板、電子会議室等に意見を掲載する場合は、それが会社の代表としての意見なのか、個人としての意見なのかを明確にする必要があります。

②社外の電子掲示板、電子会議室等で個人の資格で意見を掲載する場合でも、社内情報を掲載することは禁止します。

③掲載に際してはマナーを守り、相手を誹謗中傷することがないように注意してください。

５　電子メールの利用について

（１）　電子メールの特性について

①便利なツールとして使われている電子メールは、インターネット内の不特定多数のサーバーとサブネットワークを経由して相手に届きます。このため、途中で傍受されたり紛失したりする危険性が常に存在しますので、傍受されたくない内容を含むメールはその内容を暗号化して送信したり、必ず届く必要があるメールは、相手から受け取り確認のメールをもらうなどの考慮をする必要があります。このことを忘れずに利用することを心がけてください。

（２）　電子メール利用時のセキュリティの基本的な考え

①業務に関連するすべての情報の取り扱いは、秘密保持規定における「秘密情報の分類とに従いましょう。

②業務に関連する重要な情報の交換は、暗号機能付の電子メールで行ない、記録を残しましょう。

③受信した重要な情報を印刷した場合は、出力後すぐにプリンターから取り除きましょう。

④基本事項（例：作成元、発送、配達、受信の証明）については、認証機関による電子署名を利用

しましょう。

⑤電子メールアカウントのパスワードは、先に示した「パスワードについての約束事」を遵守してください。

（3）　電子メール利用時のネチケットについて

①電子メールの利用においては、ネットワーク上のマナーが重視されます。一般に「ネチケット」と言われますが、これを守らないと他人に不快な思いをさせたり、加害者になってしまうことがあります。当社のメールアドレス（@xxxxxx.co.jp）を用いたメールの発信でこのようなことがありますと、社会から大きな非難を受けることもあります。

特に守っていただきたい内容は次のようなものです。

- 本文中では「半角カナ」文字や特殊文字を使わないようにしましょう（文字化けが起き、場合によっては本文全体が読めなくなることもあります)。
- 大きすぎるファイルを送ることは避けましょう（メールツールによっては、１ＭＢクラスの文書でも受け付けることができないものがあります。また、相手方のメールボックスの許容サイズを超えてしまったりして迷惑をかけることがあります)。
- 大きなサイズのファイルや大量のデータを送る場合は、次のような方法を検討し、利用しましょう。

  －ファイルを圧縮して送付

  －ファイルを分割して送付

  －ファイル転送専用ＨＰにアップロードし、そこからダウンロードしてもらう
- 他の人の電子メールを転送などにより別の人に送付することを避けましょう（文書情報の中にはメール宛先の相手以外の人に知られたくないものや情報に該当するようなものが含まれている場合もありえます。また、メールの送付者が、自分が送付したメールを無断で他人に転送されることを不快に思うこともあります)。
- 電子メールは文章が未熟なまま発信されてしまうことがよくあります。配送する相手だけでなく、他の人が読んでも誤解されないよう、また不快に思われないようなきちんとした文章を作らなくてはいけません。発信する前に一度相手の立場になって読み返してください。

（4）　電子メール利用にかかわる具体的な内容

①業務にかかわる情報を電子メールで送受信する場合は、メッセージを暗号化することで、傍受や改ざんから保護しなければなりません。

②電子メール添付ファイルによって、コンピュータウィルスがシステムに侵入することを防御しなくてはなりません。このためには、信頼できないあるいは不明な発信元の添付ファイルは開かないでください。また、信頼される発信元からの添付ファイルであっても、表題などを読んでなりすましでないかを疑い、利用する前にワクチンで検査をしなくてはいけません。

③利用者は電子メールが機密性や安全性が高いものだと考えてはなりません。電子メールは受信者のコンピュータ以外から傍受され、暴露される可能性が常にあります。電子メールで、企業秘密はもとより、社員や顧客にかかわるプライバシー情報を送信してはなりません。

④利用者はチェーン電子メールを開始したり、転送してはなりません。チェーン電子メールとは、受信者に対して複数の人に類似・同一内容の転送を求めるメッセージが含まれるメール文書です。

⑤電子メールで、許可なく、企業秘密情報を送信してはなりません。また秘密情報が含まれる可能性を持つ電子メールの転送も行なってはなりません。

⑥電子メールの文面は、書面の手紙と同等の注意をはらって作成してください。イントラネットに接続するコンピュータで作成されたすべてのものは、意図しない他人が閲覧をする場合があることを自覚した上で作成・通信してください。

⑦メールサーバー内の電子メールは３０日間だけ保持された後、破棄されます。重要なメールは各自のパソコン内のフォルダーに保管・管理してください。

⑧電子メールを、製品・サービスに関わる無許可の購入や、他人を困らせたり中傷するために使用してはなりません。

⑨契約行為にかかわる電子メールの場合、認証機関の電子署名を付けて、メッセージの真正性を保証、及び確認してください。また、送受信した電子メールの内容を認証機関の電子署名付で保管するようにしてください。

⑩重要な通信の場合は、あて先の間違いなどによる誤配を防止することも考慮する必要があります。その場合は受信確認を必ず行なうようにしてください。

以上

第 2 部　規定集の解説

規定集の解説

規定集の解説

この解説は、研究部会が、各規定を策定する作業の中で多くの議論を呼んだ部分や、規定だけではわかりにくい部分を、今後この汎用規定を自社の規定に取りこむ際の参考になるよう、補足説明したものです。

各規定で説明の仕方が少しずつ違いますが、これは研究部会がサブグループに分かれて作業したためで、統一をするよりは、各サブグループの担当者の生の声をなるべく残したほうが、より実践的な参考になると考えたからです。

この研究部会に参加している弁護士を含む法務の専門家チームが、当規定を含むセキュリティ管理の実務面での法律・制度上の問題について解説する予定でしたが、作業期間の関係で、各規定そのものの吟味まで至らなかったため、これらの解説は、別に掲載しました。

各規定の解説は、規定集の掲載順に並べてあります。

秘密保持規定

本規定は情報セキュリティポリシーのいわば前提規定となる上位規定です。従来の規定は紙の情報を保護対象に限っていることが多いため、電子化された秘密情報に対しても適用できるよう見直しを行いました。

(1) 継承した点と見直した点の対比

対比項目	紙の秘密情報	電子化された秘密情報
1. 秘密情報の管理者	全ての管理職	全ての管理職も管理者ですが、情報処理責任者が各事業部の統括責任を負います。
2. 秘密情報の定義	会社の経営上・管理上(財務、人事関係など)、技術上・生産上・営業上の情報で、秘密として取扱う情報	継承
3. 秘密情報の区分	極秘、秘、社外秘	継承
4. 秘密区分の表示	極秘、秘、社外秘のスタンプ又は印刷で表示	電子ファイルのヘッダーに左記と同様な文字列を表示する。
5. 秘密区分の指定と解除	極秘は担当役員、秘・社外秘は所管の部長	事業部が行う
6. 廃棄	バインダーなどは解体し、文書は焼却	記憶媒体を無意味な情報で上書き、又は破壊

(2) ISO/IEC 17799に含まれない秘密保持対策

① 口頭での秘密情報開示

② 社内会議での秘密情報の開示

なお、紙の秘密情報は鍵のかかる金庫に保管し、鍵で開示の管理を行います。電子化された秘密情報

は保存される情報システムへのアカウント付与とアクセス管理で情報の開示の管理を行います。 詳細はガイドラインなどに記載されます。

情報セキュリティ基本方針

会社トップが情報セキュリティ管理に組織を上げて取組むという宣言文と、会社の目標管理の対象が基本方針に示されています。 情報セキュリティは計画的な投資とPDCAの管理サイクルを継続的に実施することで基本方針の目標に近づけることができます。

基本方針では、経営トップは誰に情報セキュリティ管理システムを主導させるかを明言しています。また、経営戦略に合わせて特に力を入れるセキュリティ対策を明記しています。例えば個人情報保護法案は法制化されていませんが、インターネットを使った電子商取引を活発化しようとする経営戦略にとって、個人情報の漏洩は会社のブランドイメージを下げる大きな脅威で、会社にとって優先的に取組む課題です。

情報処理規定

情報セキュリティ管理システムでは情報セキュリティ基本方針に従って、セキュリティ対策を具体化していきます。 本モデルでは情報セキュリティ関連規定は3層（ポリシー：基本方針、スタンダード：規定、プロシージャ：手順）で構成しています。

本規定は2層目の諸規定について、規定の名称とその規定が何の目的で策定されたかを規定しています。

(1) 情報セキュリティの管理 ⇒ 「セキュリティ管理規定」
(2) 情報システムの開発、管理・運用⇒ 「システム開発規定」、「システム評価規定」
(3) 情報処理資源の管理 ⇒ 「情報・データ管理規定」、「システム資源管理規定」
(4) 情報通信ネットワークの管理 ⇒ 「通信ネットワーク管理規定」
(5) 情報技術の管理 ⇒ 「情報技術管理規定」
(6) 情報処理教育 ⇒ 「情報処理教育規定」
(7) 情報処理業務の外部委託管理 ⇒ 「情報処理外部委託規定」
(8) 情報処理費用の課金 ⇒ 「情報処理課金規定」

情報セキュリティ委員会規定

・情報セキュリティ管理システムの PDCA を推進するために、会社の横断組織として情報セキュリティ委員会を設置し、委員長は情報処理統括責任者が務めます。
・本規定はISO/IEC 17799 4.1.1 ITセキュリティ委員会に準拠するよう、委員会の役割と構成員を規定しています。
・情報セキュリティ委員会は本モデルでは情報セキュリティ管理システムの運用に関る意志決定機関であり、経営会議への提言、報告を行いますが、この委員会を支援するために情報セキュリティ推進分科会（所謂ワーキンググループ）を設置しています。

セキュリティ管理規定

第 1 章　総則

第4条　基本方針

ISO/IEC 17799 では、関連法令等への準拠が上げられています。本規定では、個人情報についての記述の部分に、各国の法律やガイドラインで参照されているOECD『プライバシー保護と個人データの国際流通についてのガイドライン』に従うことを明記しています。今後、政府で議論されている『個人情報保護法』などが施行された場合は、同様に準拠性を追加する必要があります。

(5)情報処理統括責任者の責務

情報システムを利用した業務が一般の従業員に拡大したことにより、セキュリティを維持するためには、技術的な対策だけではなく、情報システム利用者への教育や情報システム部門メンバーの訓練を含めたセキュリティ対策を計画、構築、運用、評価する体制を整備することが非常に重要です。ISO/IEC 17799 では、セキュリティ組織として、『情報セキュリティマネジメントフォーラム』を組織することを規定しており、本規定の中では、『情報セキュリティ委員会』が相当します。

本規定の中では、情報処理統括責任者をこの委員会の委員長として、情報セキュリティマネジメントの総責任者に設定しています。大きな組織で、各部門やあるいは地域でバラバラな管理となり全社的に一貫したマネジメントが難しい場合は、各部門あるいは地域の代表者から構成する『クロスファンクショナルフォーラム』を組織して、組織、地域間の調整を行う場合も考えられます。なお、本規定においては、中規模の組織を想定しており、情報セキュリティマネジメントの推進は、『情報セキュリティ委員会』が統括し『クロスファンクショナルフォーラム』は設けていません。

第 2 章　セキュリティ管理者の責務

第 17 条　資源調達

昨今、情報システムの運用や保守などを外部業者にアウトソーシングする機会が増加しています。資源調達においても、この状況を考慮して秘密保持契約などにより秘密情報の漏洩などを防止する必要があります。

第19条　情報秘密分類と管理

ISO/IEC 17799 では、情報をその機密度毎に分類してラベル付けを行った上で管理することを推奨されています。を本規定では、ラベル付けを行うことを明記していますが、サーバー等に格納された電子データについても、リスク分析の結果に基づいた秘密分類を行い、それぞれの秘密レベルに応じた適正な管理(例えば、電子データへのアクセス制御、暗号化、電子署名)を実施する必要があります。

第20条　建屋の管理

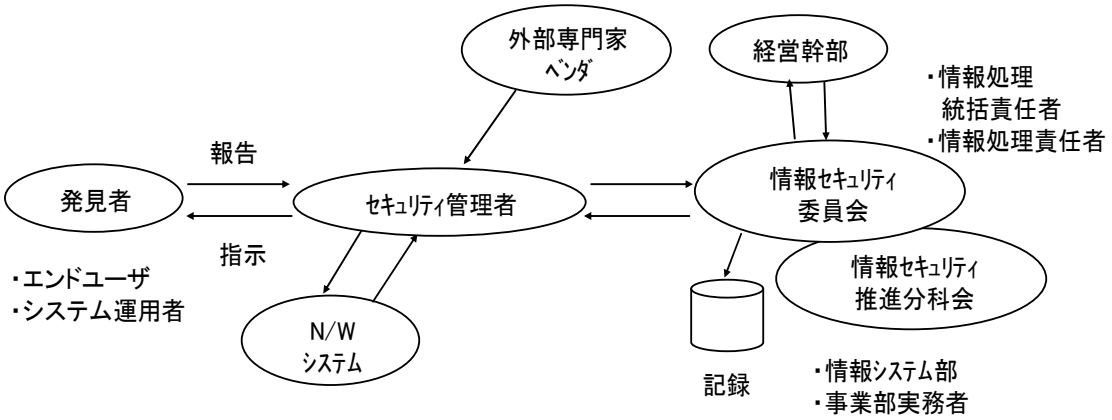
安全性を確保すべきエリア(セキュリティエリア)への入退室管理を確実に行い、その記録を一定期間保持することが必要です。また見落としがちですが、物品の持込、持ち出しもきちんと管理します。この仕組みは、万が一侵犯事象が発生したときの追跡や、システム監査などの証跡として利用されることを想定し記述しています。ISO/IEC 17799 では、荷物の受け渡し場所は情報処理設備、施設から隔離された場所に設けることを推奨しています。

第22条　運用と変更管理

システム保守についての記述は、いずれも ISO/IEC 17799 で推奨されている内容を記述しています。

第23条　セキュリティ問題の管理

本規定では、セキュリティ問題が発生したときの処理ルートを下記のように想定しています。



セキュリティ問題を発見した人がとるべき具体的な内容については、ガイドラインに記述します。

原則は、発見した人の裁量で処理することによる被害の拡大を抑止するとともに、適切な対応を迅速に遂行するための体制を整備することです。発見者には、必ずセキュリティ管理者に報告を行い、その指示の元適切な対応を遂行するよう、徹底する必要があります。

情報セキュリティ委員会に報告された内容は、記録されてセキュリティポリシーの評価、見直し、問題再発時の対応などに利用することを想定しています。

第24条　秘密保持契約

情報システム利用者にセキュリティポリシーの遵守を誓約させることが必要です。セキュリティポリシーに違反した場合は、罰則規定により処罰されることがあるので、その根拠としても必要です。 実際の運用では、雇用契約の中の1つの条項として盛り込むことを想定しています。

第25条　関連会社・第三者への義務

第26条　アウトソーシング

情報システムを利用している社外の人や組織、アウトソーシング先などに対しては、機密情報の漏洩を防止するために機密保持契約を結び、賠償責任や免責事項など具体的に取り決めておく必要があります。

このような第三者も、社内と同様にセキュリティマネジメントの対象と考えるべきですので、管理の妥当性を確認するためにも、定期的なセキュリティ監査が必要になってきます。

第 4 章　情報システム利用者の責務

第 28 条　情報システム利用者の義務

情報システム利用者が一般の従業員に拡大したことにより、情報システム利用者に起因するセキュリティ問題が発生する可能性が非常に高くなっており、情報システム利用者にセキュリティ教育の受講を義務付けることはセキュリティマネジメント上非常に重要なことです。利用者教育については、実施義務

はセキュリティ管理者に、受講義務は情報システム利用者にあると考えます。

第30条　セキュリティ問題発生への対応

ここでは、セキュリティ問題を『セキュリティ欠陥』、『ソフトウエア誤動作』、『セキュリティ事故』の3種類に分類しています。

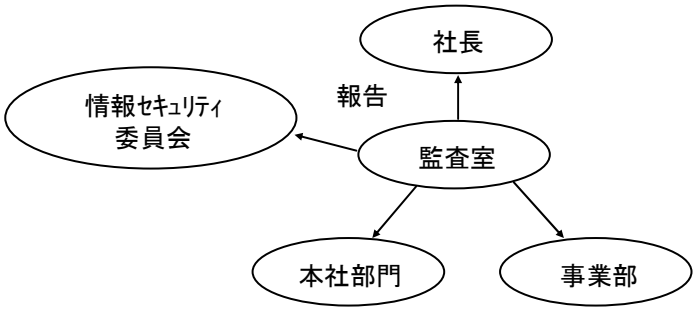
セキュリティ欠陥とは、ソフトウエアの構造やバグ、システム構成上から発生するセキュリティ上の脆弱性（セキュリティホール）を想定しています。具体的にはバッファオーバーフローを引き起こすようなソフトウエアのバグ、不適切なホストの設定に起因するサービス妨害に対する脆弱性などを想定しています。

ソフトウエア誤動作は、ソフトウエアのバグや設定ミスによるソフトウエアの想定外の動作を想定しています。

セキュリティ事故は、セキュリティ欠陥や、ソフトウエア誤動作により情報システムのセキュリティが崩壊し、具体的な被害が発生したことを想定しています。たとえば、ワームウィルスへの感染、公開ページの改ざんなどです。

第5章　内部監査室の責務

監査結果の報告のルートは下記のように想定しています。



本規定では、内部監査のうちセキュリティ監査を対象としています。セキュリティ監査では、システムの運用や利用がセキュリティポリシーに則って適正になされているかを定期的に監査します。この結果に基づいて、監査室は被監査部門に対して改善勧告を行い、勧告にもとづく改善経過をフォローアップします。またこの結果、セキュリティポリシー上の問題が発生した場合、情報セキュリティ委員会にて規定の改定を行うことを想定しています。社内の監査の実施責任部署は、本社部門の監査室を設定しています。

またシステムを利用している第三者がある場合、その責任部署のセキュリティ管理者が、セキュリティ監査を実施します。この結果も、内部監査と同様に情報セキュリティ委員会へ報告を行うことを想定しています。外部の組織は、委託元が直接管理できないことから、セキュリティ監査が特に重要になります。

第 6 章　規定の改廃および周知

第33条　規定の改廃および周知

本規定集では、上位3規定（基本方針、情報処理規定、セキュリティ管理規定）を社則と同様な位置付けと考えて、承認の権限を経営会議に設定しています。他の規定については、情報セキュリティ委員会に設定しています。

情報・データ管理規定

第 2 章　情報・データの利用

第 18 条（情報・データの外部への提供）

データを外部へ提供する場合は、秘密漏洩などを防止するために、秘密保持契約を結び提供先での情報の取り扱い方法や万が一の場合の損害賠償などの取り決めを行っておく必要があります。特に電子商取引などを実施している組織の場合、厳密なルールと仕組みを構築することが必要です。

第4章　情報・データの保全

第22条（移送時の媒体の取り扱い）

具体的な保護措置については、情報セキュリティガイドラインで記述しますが、一般的には下記のような内容を想定しています。

- 宅配業者の身分確認手段
- 信頼できる業者の選定
- データの紛失などに対する保証責任
- 確実な梱包
- 受け渡し手続き

第23条（入力データの扱い）

具体的な保護措置については、システム開発規定で記述しますが、一般的には下記のような内容を想定しています。

- データのレンジ確認
- 入力項目の抜けの確認
- データタイプ（文字、数値など）の確認

システム開発規定

・この開発規定は日本の平均的な会社がソフトウエア、ハードウエア、ネットワークなどを問わず、ITに関する技術開発・導入を行う場合に、そのリスク対策と品質の確保のために作成したものです。
・考え方、章立てなどは、SDLC(Software Development Life Cycle：IEEE Std 730-2002 など)の考え方に準拠しています。
・企業によっては、決裁方法や組織あるいは開発プロセスが異なる場合があります。その企業に合ったように適宜内容を読み替えていただくようお願いします。
・各章は詳細な表現までは及んでいません。その理由は、評価規定のときと同じです。
各自が、自分のところのシステムの規模に応じて、参考書や文献の情報を基に加筆訂正してください。
・この開発規定に関わらず、一連の規定集の中には、暗号に関する規定は設けていません。
・暗号は重要情報を守るための重要技術であり、ISO/IEC17799 の中でも数項目をさいて詳述しています。にもかかわらず触れていないのは、暗号の場合は暗号化する方法、暗号強度、適用すべき保護情報、暗号鍵の管理方法など、検討すべき項目が多層に渡り、一元的に表現することは不可能だからです。このため、重要であることを知りながら、触れていません。
・最初、読者の参考になるようなガイドライン程度の制定も検討し、議論も行いましたが、結局、作成を諦

めました。暗号は個別技術の検討が必要であるため、個々の規定についても特に考慮していませんし、規定も設けていません。各企業がリスクアセスメントを実施したうえ、要求レベルなどにあわせて個々に制定を検討するべきだと考えます。

・なお、汎用的に使用されている暗号技術の個別評価については、CREPTREC（http://www.ipa.go.jp/security/enc/CRYPTREC/index.html）に詳しく掲載されているので参考にしてください。

・この開発規定の中では、プロジェクトの推進体制のうち、プロジェクトマネジメント（PM）を行うのはプロジェクト責任者、PM の代行若しくは適切な推進を行う為に実際の推進・監督を行う役割を監督者と呼んでいます。監督者はプロジェクトコントロール（PC）やプロジェクトリーダーなどと呼ばれることもあります。

・セキュリティの設計に関しては、セキュリティ対策方針が制定してある前提で記述してありますが、企業によっては制定されていない場合があります。その場合は、プロジェクト責任者がセキュリティ基準を定め、開発責任者が承認するような実施が望ましいでしょう。

・この開発規定はセキュリティ確保のために作成したものですが、元々の考え方が SDLC などの標準開発手法を基本にしています。セキュリティ以外の目的にも利用されることを願っています。

システム評価規定

・この評価規定は日本の平均的な会社がソフトウエア、ハードウエア、ネットワークなどを問わずに、ITに関する技術開発・導入を行う場合に、その機能と品質を評価し、記録するために作成したものです。

・考え方、章立てなどは、システム監査基準に基づき規定しています。

・企業によっては、決裁方法や組織あるいは評価プロセスが異なる場合がありますが、そのときは、その企業に合ったように適宜内容を読み替えてください。

・各章は詳細な表現をあえて避けています。しかし、不足することのないよう、一テーマあたり 10 前後の項目に触れ、網羅的になるよう構成しました。 どの項目を採用し、どの項目を省略するかの選択は困難ですが、この規定を担当した著者らの経験を考慮しながら選択しました。

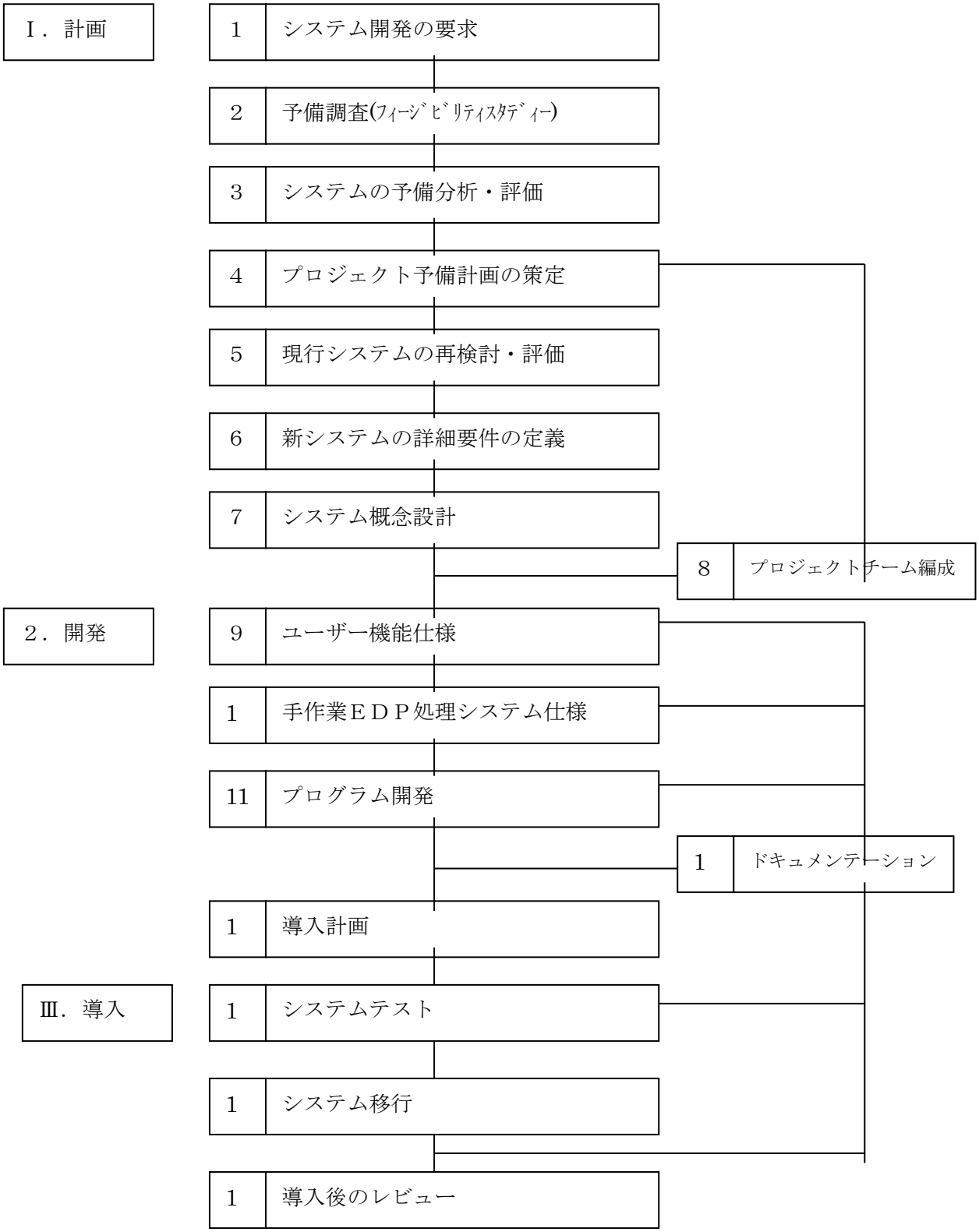
・この中の記載は、詳細までは及んでいないので、詳細が必要な場合は、それぞれの規定・参考書・文献などによって作成してください。

・最近の開発形態は、パッケージによる構成が浸透してきましたので、パッケージ構成についても評価項目としてあげています。パッケージの場合、メーカーが標準で提供している評価項目はそのまま利用し、カスタマイズした部分の様に標準が適用できない部分に関しては、独自に評価項目を設定するべきでしょう。

・システムの評価は、その規模、大きさや、ハードウエア中心なのか、ソフトウエア中心なのかで大きく異なります。大規模システムは詳細に、小規模システムはこの中の項目から抜粋するなど、システム規模によって適宜選択することが必要です。

・評価組織は、評価を行う品質管理(QC)組織がある場合、利用者が行う場合、アウトソーシングで評価する場合など企業によって大きく異なります。それぞれの事情に合わせて、読み替えてください。

システム開発ライフ・サイクル（ＳＤＬＣ）



〇以下の全 5 規程に関して、考慮した事項

・システム管理規定
・サーバー管理規定
・データベース管理規定
・通信ネットワーク管理規定
・システム資源管理規定

規程とは何か？を考え、規程は下記項目を必ず含むものとしました。

① 規定内で用いる言葉の定義
② 各規程が適応される業務範囲
③ 業務範囲に対する責任者と、責任者を任命するプロセス
④ 業務を管理する管理グループ
⑤ 責任者と管理グループの権限および任務
⑥ 管理グループの作業結果は、エビデンスとして保存とその方法
⑦ 管理対象は、文書（紙）および電子媒体（データ）であること
⑧ システムの現状把握
⑨ 事故発生後の対応
⑩ 定期的なシステム監査の必要性

①の例を挙げると、「システム資源」の意味するものは何か？を決定することに時間を要しました。具体的には、ハードウエア的な側面から見るとシステムリソース（CPU 使用率、メモリ使用率等）を意味するが、資産管理の側面から見るとライセンス等を含むためです。

また、各規程間との内容調整（名称、内容の重複等）に苦労しました。

システム管理規定

システム利用者がシステムを利用する際に、次の項目を含んだ

「作業計画書 兼 結果報告書」

を作成・運用することにより多くの規程をカバーできると考えています。

ただし、この場合のシステム利用とは Web ブラウジング、メール閲覧等の日常業務ではなく、ASP サービスとして稼働中のシステム等に対するアプリケーションリリース作業、ログ採取作業、DB データ書き換え等を指しています。

作業計画書 兼 結果報告書 項目一覧:

1） 作業計画書発行者氏名
2） 作業計画書発行日
3） 作業実施内容（作業内容、作業期間、作業対象マシン等）
4） 作業前確認印 押印欄（作業者とは異なる第三者印）
5） マシンルーム内作業者一覧
6） 作業結果報告書発行者氏名
7） 作業結果報告書発行日
8） 作業結果報告内容
9） 作業結果確認印 押印欄（作業者とは異なる第三者印）

上記 作業計画書 兼 作業報告書により、下記の条項を一部満たすと考えています。

第12条:システム維持・更新管理
第 13 項:システム利用者管理
第 14 条:システム操作管理
第20条:システムへのアクセスのセキュリティ管理
第21条:システムの不正利用セキュリティ管理
第22条:システム設置場所のセキュリティ管理

サーバー管理規定

第13条:オペレーティングシステム管理

オペレーティングシステム(以下、OS と記す)を管理すると、必然的にミドルウェア、業務アプリケーションの管理も行うべきですが、OS 以外の管理は「システム資源管理規定」内で規定しています。

第14条:サーバークセス管理

HTTP サーバー等のインターネット経由で接続されるサーバーについては、接続元 IP アドレス等の接続元を特定できる情報をロギングすることを推奨します。

第19条:OS のセキュリティ管理

現実問題として、OS にセキュリティホールが発見され、かつ、セキュリティパッチがリリースされたとしても、商用マシンへの適用は難しい場合があります。例えば、パッチ適応のためのサービスダウンタイムの発生、パッチ適応後のシステム異常等が考えられます。

第20条～第22条

サーバーのセキュリティ監視を実現するものとして、

1) ファイル改竄検知ソフト
Tripwire(http://www.tripwire.co.jp/)
2) アクセス監視システム
・IDS (Intrusion Detection System)
・IDP (Intrusion Detection and Prevention)
・IPS (Intrusion Prevention System)
3) 脆弱性調査ツール
・SAINT (http://www.saintcorporation.com/products/saint_engine.html)
・Nesus (http://www.nessus.org/)

などを、使用することを推奨します。

第25条:サーバーバックアップ媒体のセキュリティ管理

災害対策レベルとして、1992 年に米国の Share (http://www.share.org/) で制定された定義があります。この定義を元にセキュリティ要求度を決め、セキュリティ管理規定を作成することもひとつの方法です。

システム資源管理規定

第16条:システム資源ライセンス使用状況管理

第15条のシステム資源契約管理と内容的に一部重複しますが、昨今の著作権問題を意識し、条として独立させました。また、ライセンスのインストール先を管理することにより、同一ライセンスの二重使用抑制を意識しています。

第18条:システム資源の不正使用防止対策

管理対象PCのライセンス管理ソフトは存在するのですが、不完全な部分が多少存在するため、ライセンス管理ソフトを用いた管理は難しいのが実情です。

情報処理教育規定

第1条　目的

本規定の対象範囲は、役員・社員です。今日の企業は、業務の一部をアウトソーシングすることが日常化しています。そこで、アウトソーシング先(外部委託先)の教育については、外部委託規定で規定します。

第6条　情報セキュリティ教育業務

ISO/IEC 17799 の管理項目 20 は、IT セキュリティ教育と訓練を推奨しています。そこで、本条にもその内容を規定しています。

第 7 条　情報処理教育責任者

情報処理統括責任者は、全社で1人の「全社情報処理教育責任者」を任命します。「全社情報処理教育責任者」は、全社の情報処理教育及び情報セキュリティ教育の有用性・適切性・効率性への貢献の責任を負います。

一方各事業部の情報処理責任者は、「事業部情報処理教育責任者」を任命します。「事業部情報処理教育責任者」は、事業部に所属する社員の情報処理教育及び情報セキュリティ教育の実施管理を木目細かく管理します。

このように「全社情報処理教育責任者」と「事業部情報処理教育責任者」の責任範囲を明確に分けています。

第12条　情報処理教育計画策定・実施

「全社情報処理教育責任者」と「事業部情報処理教育責任者」の実施範囲を分けています。
全社情報処理教育責任者は、年初に年度の情報処理教育計画を策定します。
事業部情報処理教育責任者は、上記計画に則って、年初に年度の事業部に属する個々の社員について教育計画をブレークダウンしてゆきます。

第 19 条　役員・社員への情報セキュリティ啓蒙

実務レベルの教育は事業部毎に実施しますが、情報セキュリティの啓蒙は、事業部毎の実施ではなく全社で統一した啓蒙活動を実施します。

情報処理課金管理規定

第1条　目的

会社の情報システムに係る費用は、利用者の受益者が負担することを明確にするべきです。何故なら、利用者ニーズにのみ応えていたらコストは増加し、逆にコストを重視しセキュリティは穴だらけの安価なサービスを提供していても話にならないからです。利用者が納得するコスト、すなわち適正なコストで、安全で信頼性の高いシステムを提供する。その結果、効率的な情報システムの運営ができると考えられます。

第6条　情報処理課金管理責任者

情報処理統括責任者は、全社で1人の「情報処理課金管理責任者」を任命します。なぜ、各事業部に一人ではなく、全社で一人なのか。それは、あるシステムの利用範囲がその事業部に閉じていたとしても、全社で情報システムの運用に係る費用を把握する必要があり、その係った費用を利用量に応じて負担する仕組みを一元的に管理するためです。
情報処理課金管理責任者の具体的な任務は第7条に、権限は第8条に記します。

第12条　情報処理課金単価管理

単価は、次の3つを設定しました。

(1) 基本単価：全社で全従業員が共通的に利用する情報システムの利用単価のこと。これは、出退勤システムや出張旅費精算、全社掲示板、社外向け Web サーバー、FW などの全社共通的な情報システムの運用費用を、全社員で負担することを意味します。
(2) オプション単価：特定の部署や社員が利用する情報システムの利用単価のこと。これは、ML（メーリングリスト、特定フォーラム、モバイル端末から社内システムへのアクセスなどの特定用途で利用する情報システムの運用費用を、利用する社員が各々負担することを指します。
(3) 従量制：利用頻度もくしは、使用量と比例の関係がある情報システムの利用単価のこと。これは、メールボックスの容量やファイルサーバーの容量など、使用量とコストが比例関係のある情報システムの運用費用を、利用する社員が各々負担することを指します。

第15条　情報処理課金管理結果の分析

情報システムの発生費用と徴収金額の計画と実績の差異を分析することは重要です。課金単価は、1年に1回は必ず見直しを実施します。

第19条　情報処理課金管理の監査

ISO/IEC 17799の管理項目 126は、ビジネスプロセスの中断リスクを最小限に抑えるためのシステム監査を推奨しています。そこで、本条にもその内容を規定しました。

情報処理外部委託規定

第 9 条　秘密保持

ISO/IEC 17799 の管理項目 18 の機密保持契約では外部委託先との契約がまだ取り交わされていない場合には、情報処理施設／設備へのアクセス許可が与えられる前に機密保持合意書に署名する

ことを要求することが望ましいとされています。現実的に契約締結が遅れて、未締結のまま作業着手するケースは想定されるため、そのような場合合意書による秘密保持の確保も考慮することが望ましいでしょう。

第 6、7 条　情報処理外部委託責任者

情報処理外部委託責任者は 1 人と想定していますが、企業の外部委託のやり方によっては事業部ごとに任命して、個々に進めることもあります。本モデルでは全体最適、窓口一本化などの観点から 1 人にしています。

第 12 条　情報処理外部委託業者の選定基準の策定

外部委託業者の選定においてはその基準を明確（明文）化しておくことが取引の透明性を担保する上でも重要です。また、その基準に沿って選定すると共に委託業務の実績（結果）を評価し、場合によっては基準の見直しをし、より有用な委託先を選定するような PDCA サイクルの確立が重要です。

第 14 条　情報処理外部委託契約管理

外部委託契約の事項を列記していますが、開発委託の場合と運用委託の場合では重視する事項が一部異なると考えられるため、実際の契約では取捨選択もしくは追加（例えばエスクロー契約事項）も検討する必要があります。

第 18 条　情報処理の外務委託機密契約の締結

ISO/IEC 17799 の管理項目 20 は、IT セキュリティ教育と訓練の第三者にも推奨しています。そこで、本条に情報セキュリティ教育と訓練の実施を規定しています。

第 3 部　国際規格との準拠

〔1〕　各規格における ISO/IEC17799 管理項目の対応表（順引き）

〔2〕　ISO/IEC17799 の各項目から見た各規定の対応表

〔1〕 各規定における ISO/IEC17799 管理項目の対応表（順引き）

(1) 秘密保持規定と ISO/IEC17799 との対応

規定項目	ISO/IEC17799　対応項目
第1条　目的	
第2条　定義	
第3条　秘密の保持	
第4条　管理責任	5
第5条　秘密情報の分類	14
第6条　文書等への表示	15
第7条　秘密情報の指定と解除	15
第8条　口頭の開示	
第9条　事業所見学	18
第10条　廃棄	15
第11条　秘密情報の社外開示	18
第12条　規定違反	25
第13条　規定の改廃および周知	2

(2) 情報セキュリティ基本方針と ISO/IEC17799 との対応

規定項目	ISO/IEC17799　対応項目
第1章　はじめに	1
第2章　基本方針	1

(3) 情報セキュリティ委員会規定と ISO/IEC17799 との対応

規定項目	ISO/IEC17799　対応項目
第1条　目的	
第2条　基本方針	
第3条　責任の所在	5、25
第4条　実施体制	4、8
第5条　委員会の役割	3
第6条　委員会の招集と開催	4
第7条　規定の改廃および周知	2

(4) セキュリティ管理規定と ISO/IEC17799 との対応

規定項目	ISO/IEC17799 対応項目
第1章 総則	
1. 目的	
2. 適用範囲	
3. 用語の定義	
4. 基本方針	120
5. 責任	
6. 情報セキュリティ管理業務	
7. 情報セキュリティの管理責任	4、5、16
第2章 CIO の責務	
8. セキュリティ教育の実施	20
9.セキュリティ訓練の実施	20
10.セキュリティ教育・訓練の効果評価	20
第3章 セキュリティ管理者の責務	
11.セキュリティ管理者の任務	
12.セキュリティ管理者の権限	
13.情報資産の価値と脅威の把握	13
14.現状のセキュリティ対策の把握	24
15.セキュリティに関する技術動向の把握	
16.セキュリティ管理方針の策定	
17.資源調達	
18.資源廃棄	35、52、53
19.情報機密分類と管理	13～15
20.建屋の管理	26～28
21.周知・公報・教育	20
22.運用と変更管理	34, 107～109
23.セキュリティ問題の管理	16、21～23、41、50、123
24.秘密保持契約	18
25.関連会社・第三者への義務	10～12、16、124
26.アウトソーシング	10～12
27.評価の実施	9
第4章 情報システム利用者の責務	
28.情報システム利用者の義務	16, 55
29.資源移動	38
30.セキュリティ問題発生への対応	16、21～23、41
第5章 内部監査室の責務	
31.監査の実施	9、124、126
32.改善勧告の実施	9、124、126
第6章 規定の改廃及び周知	
33.規定の改廃及び周知	

(5)情報・データ管理規定とISO/IEC17799との対応

規定項目	ISO/IEC17799 対応項目
第1章 総則	
1. 目的	
2. 適用範囲	
3. 用語の定義	
4. 基本方針	
5. 本規定の効力	
6. 情報・データの所有者	
7. 情報・データ管理責任者	
8. 情報・データ管理責任者の任務	
9. 情報・データ管理責任者の権限	
10.機密保持	
第2章 情報・データの収集・蓄積	
11.情報・データ形態の最適化	
12.情報・データの整備	
13.情報・データの保管	
14.情報・データの廃棄	52、53
第3章 情報・データの利用	
15.情報・データの利用	
16.情報・データの社外利用	
17.システム文書の管理と利用	55
18.情報・データの外部への提供	11、12
第4章 情報・データの保全	
19.バックアップ取得の原則	48
20.バックアップ、復元手順の明確化	48
21.バックアップ媒体の保管・取り扱い	48
22.移送時の媒体の取り扱い	57
23.入力データの扱い	95
第5章 規定の改廃及び周知	
24.規定の改廃及び周知	

(6)情報技術管理規定とISO/IEC17799との対応

規定項目	ISO/IEC17799 対応項目
第1章 総則	
1. 目的	
2. 適用範囲	
3. 用語の定義	
4. 基本方針	
5. 本規定の効力	
6. 情報技術管理業務	
7. 情報技術管理責任者	
8. 情報技術管理責任者の任務	
9. 情報技術管理責任者の権限	
10.機密保持	
11.業務効率の推進	
第2章 情報技術の管理	
12.情報技術の収集	
13.情報技術の評価・選定	
14.利用技術の標準作成・維持	
15.情報技術の利用支援	
16.情報技術・利用技術の共有化	
17.情報技術・利用技術の活用状況の評価	
第3章 情報セキュリティに関連する情報技術管理	
18.システム文書の取り扱い	55
19.システムファイルのセキュリティ	55、106
20.暗号技術の使用	99、100
21.デジタル署名と暗号鍵	101～103
第4章 規定の改廃及び周知	
22.規定の改廃及び周知	

(7)システム開発規定とISO/IEC17799との対応

規定項目	ISO/IEC17799 対応項目
第 1 章 総 則	
第1条 目 的	
第2条 適用範囲	
第3条 基本方針	
第4条 責任	
第 2 章 企画・設計	
第5条 企画の申請・承認	
第6条 開発計画	
第7条 要件定義	63、94、99、100、101、102、109

第8条　設計	
8-0.運用方案設計仕様	39, 48
8-1.ハードウェア設計仕様	31、43、79
8-2.ソフトウェア設計仕様	47、76、77、87、95、96
8-3.ソフトウェアモジュール設計仕様	97
8-4.ネットワーク設計仕様	33、45、71、72、73、74、75、76、77、78
8-5.パッケージ構成仕様	109
8-6.機械・電気仕様	31、32
第 3 章　開発・導入	
第9条　開発	27、43、74、106、107、108、110
第 10 条　テスト	
10-1.テスト環境	43
10-2.データ・本番データの使用	98、105
第 11 条　システム開発の委託	
第 12 条　製品の調達	110
第 13 条　導入	
第 14 条　稼動中システムの改善	
第 4 章　書類管理など	
第 15 条　仕様書の管理	55
第 16 条　要員の教育	
第 17 条　変更管理	55、107
第 5 章　規定の改廃及び周知	
第 18 条　規定の改廃及び周知	

(8)システム評価規定とISO/IEC17799との対応

規定項目	**ISO/IEC17799　対応項目**
第 1 章　総　　則	
第1条　目　的	
第2条　適用範囲	
第3条　基本方針	
第4条　責任	
第 2 章　システムの評価	
7-1.計画段階の評価	94
7-2.要件定義の評価	
7-3.設計段階の評価	94
7-4.製作段階の評価	
7-5.パッケージ構成の評価	
7-6.テスト段階の評価	55
7-7.導入承認の評価	
7-8.稼動中システムの評価	

7-9.開発委託先の評価	12
第8条　結果報告と承認	
第9条　評価結果の監査	
第 3 章　書類管理など	
第 10 条　評価書類の管理	55
第 11 条　要員の教育	
第 12 条　変更管理	55、107
第 4 章　規定の改廃及び周知	
第 13 条　規定の改廃及び周知	

(9)システム管理規定とISO/IEC17799との対応

規定項目	ISO/IEC17799　対応項目
第 1 章　総則	
第1条　目的	
第2条　適用範囲	
第3条　基本方針	
第4条　本規定の効力	
第5条　システム管理業務	
第6条　システム管理責任者	
第7条　システム管理グループ	
第8条　システム管理責任者の任務	
第9条　システム管理責任者の権限	
第10条　機密保持	
第11条　業務効率の推進	
第2章　システムの管理	
第12条　システム構成管理	
第13条　システム維持・更新管理	
第14条　システム利用者管理	64
第15条　システム操作管理	
第16条　システム処理管理	89
第17条　システム問い合せ管理	
第18条　システムバックアップ管理	48
第19条　システム障害管理	
第3章　システムのセキュリティ管理	
第20条　システムへのアクセスのセキュリティ管理	63, 64, 68, 80, 87
第21条　システムの不正利用防止対策	63, 68, 82, 87, 90
第22条　システム設置場所のセキュリティ管理	28, 63, 88
第23条　システム管理ドキュメントのセキュリティ管理	55, 63, 87, 90
第24条　システムバックアップ媒体のセキュリティ管理	48, 63, 87, 90
第25条　システムバックアップ媒体の転送セキュリティ	48, 57, 63, 87

第26条　システムのセキュリティ問題発生後の対応	
第 4 章　規定の改廃および周知	
第27条　規定の改廃および周知	107

（10）サーバ管理規定と ISO/IEC17799 との対応

規定項目	ISO/IEC17799　対応項目
第 1 章　総則	
第1条　目的	
第2条　適用範囲	
第3条　基本方針	
第4条　本規定の効力	
第5条　サーバ管理業務	
第6条　サーバ管理責任者	
第7条　サーバ管理グループ	
第8条　サーバ管理責任者の任務	
第9条　サーバ管理責任者の権限	
第10条　機密保持	
第11条　業務効率の推進	
第 2 章　サーバの管理	
第12条　サーバ構成管理	
第13条　サーバオペレーティングシステム管理	108、 109
第14条　サーバアクセス管理	
第15条　サーバ稼働の業務システムプロセス管理	
第16条　サーバキャパシティ管理	45、 89
第17条　サーババックアップ管理	31、 48
第18条　サーバ障害管理	
第 3 章　サーバのセキュリティ管理	
第19条　サーバオペレーティングシステムのセキュリティ管理	63、 64、 65、 68、 80、 82、 87
第20条　サーバ稼働プロセスのセキュリティ管理	63、 64、 68、 87、 90、 96
第21条　サーバファイルアクセスセキュリティ管理	63、 87
第22条　サーバのハッキング／クラッキング防止対策、ウィルス防止対策	63、 87、 90
第23条　サーバ設置場所のセキュリティ管理	28、 63、 88
第24条　サーバ管理ドキュメントのセキュリティ管理	55、 63、 87
第25条　サーババックアップ媒体のセキュリティ管理	48、63、 87
第26条　サーババックアップ媒体の転送セキュリティ	48、 57、 63、 87
第27条　サーバのセキュリティ問題発生後の対応	
第 4 章　規定の改廃および周知	
第28条　規定の改廃および周知	107

（11）データベース管理規定とISO/IEC17799との対応

規定項目	ISO/IEC17799 対応項目
第1章 総則	
第1条 目的	
第2条 適用範囲	
第3条 基本方針	
第4条 本規定の効力	
第5条 データベース管理業務	
第6条 データベース管理責任者	
第7条 データベース管理グループ	
第8条 データベース管理責任者の任務	
第9条 データベース管理責任者の権限	
第10条 機密保持	
第11条 業務効率の推進	
第2章 データベース管理	
第12条 データベース構成管理	
第13条 データベースシステム管理	
第14条 データベースアクセス管理	
第15条 データベース稼働管理	
第16条 データベースキャパシティ管理	45
第17条 データベースバックアップ管理	48
第18条 データベース障害管理	
第3章 データベースのセキュリティ管理	
第19条 データベースへのアクセスのセキュリティ管理	63、64、 65、 68、 82、 87
第20条 データベースへのハッキング／クラッキング防止対策	63、 87、 90
第21条 データベース設置場所のセキュリティ管理	28、 63、 88
第22条 データベース管理ドキュメントのセキュリティ管理	55、 63、 87
第23条 データベースバックアップ媒体のセキュリティ管理	48、 63、 87
第24条 データベースバックアップ媒体の転送セキュリティ	48、 57、 63、 87
第25条 データベースのセキュリティ問題発生後の対応	
第4章 規定の改廃および周知	
第26条 規定の改廃および周知	107

（12）通信ネットワーク管理規定とISO/IEC17799との対応

規定項目	ISO/IEC17799 対応項目
第１章 総則	
第1条 目的	
第2条 適用範囲	
第3条 基本方針	
第4条 本規定の効力	
第5条 通信ネットワーク管理業務	
第6条 情報通信ネットワーク管理責任者	
第7条 通信ネットワーク管理グループ	
第8条 情報通信ネットワーク管理責任者の任務	
第9条 情報通信ネットワーク管理責任者の権限	
第10条 機密保持	
第11条 業務効率の推進	
第2章 情報通信ネットワークの管理	
第12条 通信ネットワーク構成管理	40、 70、 78
第13条 通信ネットワークアドレス管理	70、 78
第14条 通信ネットワークキャパシティ管理	45、 70、 78
第15条 通信ネットワークレスポンス管理	70、 78、 89
第16条 通信ネットワーク障害管理	70、 78
第3章 情報通信ネットワークのセキュリティ管理	
第17条 社外ネットワークへの接続セキュリティ管理	63、 64、 70、 76、 78、 87、 90、 110
第18条 通信機器設置場所のセキュリティ管理	28、 63、 70、 78、 88
第19条 通信配線のセキュリティ管理	31、 33、 63、 70、 75、 78、 82、 87
第20条 通信機器のセキュリティ管理	63、 68、 70、 75、 78、 82、 87
第21条 通信ネットワーク管理ドキュメントのセキュリティ管理	55、 63、 70、 78、 87
第22条 通信ネットワークのセキュリティ問題発生後の対応	70
第4章 規定の改廃および周知	
第23条 規定の改廃および周知	107

（13）システム資源管理規定とISO/IEC17799との対応

規定項目	ISO/IEC17799 対応項目
第1章 総則	
第1条 目的	
第2条 適用範囲	
第3条 基本方針	

第4条　本規定の効力	
第5条　システム資源管理業務	
第6条　システム資源管理責任者	
第7条　システム資源管理グループ	
第8条　システム資源管理責任者の任務	
第9条　システム資源管理責任者の権限	
第10条　機密保持	
第11条　業務効率の推進	
第2章　システム資源の管理	
第12条　システム資源資産管理	13、34、38、104、118
第13条　システム資源コスト管理	13
第14条　システム資源調達管理	13、104, 118
第15条　システム資源契約管理	13、 34、56、104
第16条　システム資源ライセンス使用状況管理	47、 64、 104
第17条　システム資源管理データのバックアップ管理	13、 48
第3章　システム資源のセキュリティ管理	
第18条　システム資源の不正利用防止対策	
第19条　システム資源管理データへのアクセスセキュリティ管理	63、87
第20条　システム資源管理データの不正利用防止対策	63、 87
第21条　システム資源設置場所のセキュリティ管理	28、 63
第22条　システム資源管理ドキュメントのセキュリティ管理	55、 63、 87
第23条　システム資源管理データバックアップ媒体のセキュリティ管理	63、 87
第24条　システム資源管理データバックアップ媒体の転送セキュリティ	57、 63、 87
第25条　システム資源のセキュリティ問題発生後の対応	
第4章　規定の改廃および周知	
第26条　規定の改廃および周知	107

（14）情報処理教育規定とISO/IEC17799との対応

規定項目	**ISO/IEC17799　対応項目**
第 1 章　総　　則	
第1条　目　的	
第2条　適用範囲	
第3条　基本方針	
第4条　本規定の効力	
第5条　情報処理教育業務	20
第6条　情報セキュリティ教育業務	20

第7条　情報処理教育責任者	
第8条　情報処理教育責任者の任務	
第9条　情報処理教育責任者の権限	
第 10 条　秘密保持	
第 11 条　業務効率の推進	
第 2 章　情報処理教育	
第 12 条　情報処理教育計画策定・実施	
第 13 条　情報処理教育カテゴリー策定	
第 14 条　情報処理教育カリキュラム策定	
第 15 条　情報処理教育実施管理	
第 16 条　情報処理教育成果の分析	
第 17 条　情報処理教育結果の評価	
第 3 章　情報セキュリティ教育	
第 18 条　情報セキュリティ教育計画策定・実施	20
第 19 条　役員・社員への情報セキュリティ啓蒙	20
第 20 条　役員・社員への情報セキュリティ教育	20
第 21 条　情報セキュリティ訓練	20
第 22 条　情報セキュリティ教育・訓練の効果評価	
第 4 章　規定の改廃及び周知	
第 23 条　規定の改廃及び周知	

（15）情報処理課金規定と ISO/IEC17799 との対応

規定項目	**ISO/IEC17799　対応項目**
第1章　総則	
第1条　目的	
第2条　適用範囲	
第3条　基本方針	
第4条　本規定の効力	
第5条　情報処理課金業務	
第6条　情報処理課金管理責任者	
第7条　情報処理課金管理責任者の任務	
第8条　情報処理課金管理責任者の権限	
第9条　秘密保持	
第10条　業務効率の推進	
第2章　情報処理課金業務	
第11条　情報処理課金計画策定	
第12条　情報処理課金単価管理	
第13条　情報処理課金の徴収、配賦管理	
第14条　情報処理課金実施管理	
第15条　情報処理課金結果の分析	
第16条　情報処理課金データのバックアップ	

第3章　情報処理課金のセキュリティ管理	
第17条　情報処理課金管理データへのアクセスセキュリティ管理	
第18条　情報処理課金管理データへの不正利用防止策	
第19条　情報処理課金管理の監査	126
第20条　情報処理課金管理情報・データのセキュリティ管理	55
第4章　規定の改廃及び周知	
第21条　規定の改廃及び周知	

（16）情報処理外部委託規定とISO/IEC17799との対応

規定項目	ISO/IEC17799　対応項目
第 1 章　総　　則	
第1条　目　的	
第2条　適用範囲	
第3条　基本方針	
第4条　本規定の効力	
第5条　情報処理外部委託業務	
第6条　情報処理外部委託責任者	
第7条　情報処理外部委託責任者の任務	
第8条　情報処理外部委託責任者の権限	
第9条　秘密保持	18
第 10 条　業務効率の推進	
第 2 章　情報処理外部委託	
第 11 条　情報処理外部委託計画策定	
第 12 条　情報処理外部委託業者選定基準策定	
第 13 条　情報処理外部委託業者の選定	
第 14 条　情報処理外部委託契約管理	11、12、18、44、111
第 15 条　情報処理外部委託実施管理	
第 16 条　情報処理外部委託成果の分析	
第 17 条　情報処理外部委託結果の評価	
第 3 章　情報処理外部委託のセキュリティ管理	
第 18 条　情報処理外部委託機密契約の締結	10、11、12、20, 44
第19条　情報処理外部委託機密契約事項遵守の監視	10、11
第 20 条　情報処理外部委託システム文書のセキュリティ管理	
第 21 条　情報処理外部委託のセキュリティ問題発生後の対応	
第 4 章　規定の改廃及び周知	
第 22 条　規定の改廃及び周知	

〔2〕ISO/IEC17799の各管理項目から見た各規定の対応表（逆引き）

NO	管理項目名	対応規定名と条項	備考
3 セキュリティポリシー			
3．1 情報セキュリティポリシー			
1	3．1．1 「IT セキュリティポリシー」に関する文書	情報セキュリティ基本方針 第1章 情報セキュリティ基本方針 第2章 情報処理規定	一部の組織でBS7799を取得する場合、その適用範囲のITセキュリティポリシーが全社的なポリシーとは別に必要。 審査機関からは、ありきたりでない、その適用範囲の
2	3．1．2 レビューと評価	情報セキュリティ委員会規定 第7条 秘密保持規定 第13条	
4 セキュリティ組織			
4．1 情報セキュリティ・インフラストラクチャ			
3	4．1．1 ITセキュリティ委員会	情報セキュリティ委員会規定 第3条 情報処理規定	
4	4．1．2 ITセキュリティの調整	情報セキュリティ委員会規定 第4条 情報セキュリティ委員会規定 第6条 セキュリティ管理規定 第7条	
5	4．1．3 ITセキュリティ責任の割り当て	情報セキュリティ委員会規定 第3条 秘密保持規定 第4条 セキュリティ管理規定 第7条	
6	4．1．4 情報処理設備の認可手続き		
7	4．1．5 専門家によるITセキュリティへの助		
8	4．1．6 組織間の協力	情報セキュリティ委員会規定 第4条	
9	4．1．7 ITセキュリティの第三者レビュー	セキュリティ管理規定 第27条 セキュリティ管理規定 第31条 セキュリティ管理規定 第32条	
4．2 第三者アクセスのセキュリティ			
10	4．2．1 第三者アクセスに伴うリスクの識別	情報処理外部委託規定 第3章 第18条 情報処理外部委託規定 第3章 第19条 セキュリティ管理規定 第25条 セキュリティ管理規定 第26条	
11	4．2．2 第三者アクセス時の契約書に記載するセキュリティ要求事項	情報処理外部委託規定 第2章 第14条 情報処理外部委託規定 第3章 第18条 情報処理外部委託規定 第3章 第19条 セキュリティ管理規定 第25条 セキュリティ管理規定 第26条 情報・データ管理規定 第18条	
4．3 アウトソーシング			
12	4．3．1 アウトソーシング契約におけるセキュリティ契約事項	システム評価規定 第2章 第7条 第7.9項 情報処理外部委託規定 第2章 第14条 情報処理外部委託規定 第3章 第18条 セキュリティ管理規定 第25条 セキュリティ管理規定 第26条 情報・データ管理規定 第18条 システム資源管理規定 第2章 第12条	
5 財産の分類及び管理			
5．1 財産に対する責任			
13	5．1．1 資産目録	セキュリティ管理規定 第13条 セキュリティ管理規定 第19条 システム資源管理規定 第2章 第12条	
5．2 情報の分類			
14	5．2．1 分類のためのガイドライン	秘密保持規定 第5条 セキュリティ管理規定 第19条 システム資源管理規定 第2章 第12条	
15	5．2．2 情報のラベル付けとその取り扱い	秘密保持規定 第6条 秘密保持規定 第7条 秘密保持規定 第10条 セキュリティ管理規定 第19条 システム資源管理規定 第2章 第12条	

〔2〕ISO/IEC17799の各管理項目から見た各規定の対応表（逆引き）

NO	管理項目名	対応規定名と条項	備考
6 スタッフのセキュリティ			
6．1 ジョブ定義及びリソーシングにおけるセキュリティ			
16	6．1．1 業務責任としてのセキュリティ	セキュリティ管理規定 第7条 セキュリティ管理規定 第23条 セキュリティ管理規定 第25条 セキュリティ管理規定 第28条 セキュリティ管理規定 第29条 セキュリティ管理規定 第30条	
17	6．1．2 人員の採用審査とポリシー	システム資源管理規定 第2章 第12条	
18	6．1．3 機密保持契約	情報処理外部委託規定 第1章 第9条 情情報処理外部委託規定 第2章 第14条 秘密保持規定 第9条 秘密保持規定 第11条 セキュリティ管理規定 第24条	
19	6．1．4 採用条件		各会社の「従業員規定・規則」、「就業規則」等で定める。
6．2 ユーザの訓練			
20	6．2．1 ITセキュリティ教育と訓練	情報処理教育規定 第1章 第5条 情報処理教育規定 第1章 第6条 情報処理教育規定 第1章 第18条 情報処理教育規定 第1章 第19条 情報処理教育規定 第1章 第20条 情報処理教育規定 第1章 第21条 情報処理外部委託規定 第3章 第18条 セキュリティ管理規定 第8条 セキュリティ管理規定 第9条 セキュリティ管理規定 第10条 セキュリティ管理規定 第21条	
6．3 セキュリティ事故及び誤動作への対処			
21	6．3．1 セキュリティ問題の報告	セキュリティ管理規定 第23条 セキュリティ管理規定 第30条	
22	6．3．2 セキュリティ欠陥に関する報告	セキュリティ管理規定 第23条 セキュリティ管理規定 第30条	
23	6．3．3 ソフトウェア誤動作に関する報告	セキュリティ管理規定 第23条 セキュリティ管理規定 第30条	
24	6．3．4 セキュリティ問題からの学習	セキュリティ管理規定 第14条 情報システム活用ガイドライン	
25	6．3．5 懲戒手続き	情報セキュリティ委員会規定 第3条 秘密保持規定 第12条 情報処理規定、就業規則	
7 物理的及び環境的セキュリティ			
7．1 安全領域			
26	7．1．1 物理的セキュリティ外壁	セキュリティ管理規定 第20条 情報システム活用ガイドライン	
27	7．1．2 物理的な出入り管理策(入退室管理)	システム開発規程 第3章 第9条 セキュリティ管理規定 第20条 情報システム活用ガイドライン	物理 設計段階でIT機器の設置場所等の環境に関する保護の検討を行う必要がある。
28	7．1．3 事務所・部屋・施設のセキュリティ	セキュリティ管理規定 第20条 システム運用規定 第22条 サーバ管理規定 第2章 第23条 データベース管理規定 第3章 第21条 通信ネットワーク管理規定 第3章 第18条 システム資源管理規定 第3章 第21条 情報システム活用ガイドライン	
29	7．1．4 保護区域での作業	情報システム活用ガイドライン	オフィス利用に関する規定を整備する。
30	7．1．5 受け渡しエリアの隔離	情報システム活用ガイドライン	
7．2 装置のセキュリティ			
31	7．2．1 装置の取り付け位置と保護	システム開発規定 第2章 第8条 第8.1項 システム開発規定 第2章 第8条 第8.6項 サーバ管理規定 第2章 第17条 通信ネットワーク管理規定 第3章 第19条	8.1 ハードウェア設計仕様では単にシステムの要求だけでなく、設置環境に対する要求の確認が必要。 8.6 設計段階でIT機器の設置場所等の環境に関する保護の検討を行う必要がある。

〔2〕ISO/IEC17799の各管理項目から見た各規定の対応表（逆引き）

NO	管理項目名	対応規定名と条項	備考
32	7．2．2 電源	システム開発規定 第2章 第8条 第8.6項	8.6 設計段階でIT機器の設置場所等の環境に関する保護の検討を行う必要がある。
33	7．2．3 ケーブル配線のセキュリティ	システム開発規定 第2章 第8条 第8.4項 通信ネットワーク管理規定 第3章 第19条	
34	7．2．4 装置の保守	セキュリティ管理規定 第22条 システム資源管理規定 第2章 第12条 システム資源管理規定 第2章 第15条	
35	7．2．5 建屋外の装置に対するセキュリティ		
36	7．2．6 装置の安全な処分と再使用	セキュリティ管理規定 第18条	
7．3 一般管理策			
37	7．3．1 クリアデスクとクリアスクリーンポリシー	情報システム活用ガイドライン	
38	7．3．2 資産の移動	セキュリティ管理規定 第29条 システム資源管理規定 第2章 第12条	
8 通信及び運用管理			
8．1 運用手順及び責任			
39	8．1．1 操作手順書	システム開発規定 第2章 第8条 第8.0項	各操作手順書は、網羅性と無矛盾性が審査機関から求められる。
40	8．1．2 運用変更管理	通信ネットワーク管理規定 第2章 第12条	
41	8．1．3 セキュリティ問題管理手続き	セキュリティ管理規定 第23条 セキュリティ管理規定 第30条	
42	8．1．4 職務の分離	情報処理規定	
43	8．1．5 開発と運用設備の分離	システム開発規定 第2章 第8条 第8.0項 システム開発規定 第3章 第9条 システム開発規定 第3章 第10条 第10.1項	
44	8．1．6 外部施設の管理	情報処理外部委託規定 第2章 第14条 情報処理外部委託規定 第3章 第18条	
8．2 システム計画の作成及び受入れ			
45	8．2．1 容量計画の作成	システム開発規定　第2章　第8条 第8.4項 サーバ管理規定 第2章 第16条 データベース管理規定 第2章 第16条 通信ネットワーク管理規定 第2章 第12条 システム資源管理規定　第13条～20条	システム開発規定 8.X　設計段階でネットワークへの負荷や、電源、記憶装置の容量など、システム資源の要求について、現状確認を確認し、システム稼動後の可用性が確保できるように設計しなければならない。
46	8．2．2 システムの受け入れ		
8．3 不正ソフトウェアからの保護			
47	8．3．1 不正ソフトウェアに対する管理対策	システム開発規定 第2章 第8条　第8.2項 システム資源管理規定 第2章 第16条 情報システム活用ガイドライン	
8．4 ハウスキーピング			
48	8．4．1 情報のバックアップ	システム開発規定 第2章 第8条 第8.0項 情報・データ管理規定 第19条 情報・データ管理規定 第20条 情報・データ管理規定 第21条 システム運用規定 第18条 システム運用規定 第24条 システム運用規定 第25条 サーバ管理規定 第2章 第17条 サーバ管理規定 第2章 第26条 データベース管理規定 第2章 第17条 データベース管理規定 第3章 第24条 システム資源管理規定 第2章 第17条	

〔2〕ISO/IEC17799の各管理項目から見た各規定の対応表（逆引き）

NO	管理項目名	対応規定名と条項	備考
49	8．4．2 オペレータ日誌	システム運用規定	
50	8．4．3 障害記録	セキュリティ管理規定 第23条	
8．5 ネットワークの管理			
51	8．5．1 ネットワーク管理対策	情報システム活用ガイドライン	
8．6 媒体の取り扱い及びセキュリティ			
52	8．6．1 取り外し可能なコンピュータ媒体の管理	セキュリティ管理規定 第18条 情報・データ管理規定 第14条	
53	8．6．2 媒体の処分	セキュリティ管理規定 第18条 情報・データ管理規定 第14条	
54	8．6．3 情報の取り扱い手続き	情報技術管理規定 第3章 第18条 情報技術管理規定 第3章 第19条	
55	8．6．4 システム文書のセキュリティ	システム開発規定 第4章 第15条 システム開発規定 第4章 第17条 システム評価規定 第2章 第7条 第7.6項 システム評価規定 第3章 第10条 システム評価規定 第3章 第12条 情報処理課金規定 第3章 第20条 セキュリティ管理規定 第28条 情報・データ管理規定 第17条 情報技術管理規定第 18条 情報技術管理規定第 19条 システム運用規定 第23条 サーバ管理規定 第2章 第24条 データベース管理規定 第3章 第22条 通信ネットワーク管理規定 第3章 第22条 システム資源管理規定 第3章 第32条	「文書管理規定」を別途作成する方法もある。
8．7 情報及びソフトウェアの交換			
56	8．7．1 情報およびソフトウェア交換に関す	システム資源管理規定 第2章 第15条 情報システム活用ガイドライン	
57	8．7．2 運送中の媒体のセキュリティ	情報・データ管理規定 第22条 システム運用規定 第25条 サーバ管理規定 第2章 第26条 データベース管理規定 第3章 第24条 システム資源管理規定 第3章 第24条	
58	8．7．3 電子取引のセキュリティ	情報システム活用ガイドライン	
59	8．7．4 電子メールのセキュリティ	情報システム活用ガイドライン	
60	8．7．5 電子オフィスシステムのセキュリティ	通信ネットワーク管理規定 情報システム活用ガイドライン	
61	8．7．6 一般に使用可能なシステム	情報システム活用ガイドライン	
62	8．7．7 情報交換の他の形態	情報システム活用ガイドライン	

〔2〕ISO/IEC17799の各管理項目から見た各規定の対応表（逆引き）

NO	管理項目名	対応規定名と条項	備考
9 アクセス制御			
9．1 アクセス制御に関するビジネス要求事項			
63	9．1．1 アクセス制御	システム開発規定 第2章 第7条 システム運用規定 第20条 システム運用規定 第21条 システム運用規定 第22条 システム運用規定 第23条 システム運用規定 第24条 システム運用規定 第25条 サーバ管理規定 第3章 第19条 サーバ管理規定 第3章 第20条 サーバ管理規定 第3章 第21条 サーバ管理規定 第3章 第22条 サーバ管理規定 第3章 第23条 サーバ管理規定 第3章 第24条 サーバ管理規定 第3章 第25条 サーバ管理規定 第3章 第26条 データベース管理規定 第2章 第19条 データベース管理規定 第2章 第20条 データベース管理規定 第2章 第21条 データベース管理規定 第2章 第22条 データベース管理規定 第2章 第23条 データベース管理規定 第2章 第24条 通信ネットワーク管理規定 第3章 第17条 通信ネットワーク管理規定 第3章 第18条 通信ネットワーク管理規定 第3章 第19条 通信ネットワーク管理規定 第3章 第20条 通信ネットワーク管理規定 第3章 第21条 システム資源管理規定 第3章 第19条 システム資源管理規定 第3章 第20条 システム資源管理規定 第3章 第21条 システム資源管理規定 第3章 第22条 システム資源管理規定 第3章 第23条 システム資源管理規定 第3章 第24条 情報システム活用ガイドライン	
9．2 ユーザアクセス管理			
64	9．2．1 利用者登録	システム管理規定 14条 システム運用規定 第20条 サーバ管理規定 第2章 第19条 サーバ管理規定 第2章 第20条 データベース管理規定 第3章 第19条 通信ネットワーク管理規定 第3章 第17条 システム資源管理規定 第2章 第16条	
65	9．2．2 特権の管理	サーバ管理規定 第2章 第19条 データベース管理規定 第3章 第19条 情報システム活用ガイドライン	
66	9．2．3 利用者パスワードの管理	情報システム活用ガイドライン	
67	9．2．4 利用者アクセス権限のレビュー	情報システム活用ガイドライン	
9．3 ユーザの責任			
68	9．3．1 パスワードの使用	システム運用規定 第20条 システム運用規定 第21条 サーバ管理規定 第2章 第19条 サーバ管理規定 第2章 第20条 データベース管理規定 第3章 第19条 情報システム活用ガイドライン	
69	9．3．2 無人装置	情報システム活用ガイドライン	
9．4 ネットワークのアクセス制御			
70	9．4．1 ネットワークサービスの使用についてのポリシー	通信ネットワーク管理規定 第2章 第12条 通信ネットワーク管理規定 第2章 第13条 通信ネットワーク管理規定 第2章 第14条 通信ネットワーク管理規定 第2章 第15条 通信ネットワーク管理規定 第2章 第16条 通信ネットワーク管理規定 第3章 第17条 通信ネットワーク管理規定 第3章 第18条 通信ネットワーク管理規定 第3章 第19条 通信ネットワーク管理規定 第3章 第20条 通信ネットワーク管理規定 第3章 第21条 通信ネットワーク管理規定 第3章 第22条	

〔2〕ISO/IEC17799の各管理項目から見た各規定の対応表（逆引き）

NO	管理項目名	対応規定名と条項	備考
71	9．4．2 強制経路	システム開発規定　第2章　第8条 第8.4項	
72	9．4．3 外部接続のための利用者認証	システシステム開発規定　第2章　第8条 第8.4項	
73	9．4．4 ノードの認証	システム開発規定 第2章 第8条 第8.4項	
74	9．4．5 リモート診断ポートの保護	システム開発規定 第2章 第8条 第8.4項 システム開発規定 第3章 第9条 通信ネットワーク管理規定	
75	9．4．6 ネットワークの分離	システム開発規定　第2章　第8条 第8.4項 通信ネットワーク管理規定 第3章 第20条 情報システム活用ガイドライン	
76	9．4．7 ネットワークの接続制御	システム開発規定 第2章 第8条 第8.2項 システム開発規定 第2章 第8条 第8.4項 通信ネットワーク管理規定 第3章 第17条	
77	9．4．8 ネットワーク経路指定制御	システム開発規定第2章 第8条 第8.2項 システム開発規定第2章 第8条 第8.4項	
78	9．4．9 ネットワークサービスのセキュリティ	システム開発規定 第2章 第8条 第8.4項 通信ネットワーク管理規定 第2章 第12条 通信ネットワーク管理規定 第2章 第13条 通信ネットワーク管理規定 第2章 第14条 通信ネットワーク管理規定 第2章 第15条 通信ネットワーク管理規定 第2章 第16条 通信ネットワーク管理規定 第3章 第17条 通信ネットワーク管理規定 第3章 第18条 通信ネットワーク管理規定 第3章 第19条 通信ネットワーク管理規定 第3章 第20条 通信ネットワーク管理規定 第3章 第21条	
9．5　オペレーティングシステムのアクセス制御			
79	9．5．1 自動端末識別	システム開発規定 第2章 第8条 第8.1項 情報システム活用ガイドライン	
80	9．5．2 端末のログオン手続き	システム運用規定 第20条 サーバ管理規定 第2章 第19条 情報システム活用ガイドライン	
81	9．5．3 利用者の識別と認証		
82	9．5．4 パスワード管理システム	システム運用規定 第21条 サーバ管理規定 第2章 第19条 データベース管理規定 第3章 第19条 通信ネットワーク管理規定 第3章 第19条 通信ネットワーク管理規定 第3章 第20条 情報システム活用ガイドライン	
83	9．5．5 システムユーティリティの使用	情報システム活用ガイドライン	
84	9．5．6 利用者を保護するための強制警報		
85	9．5．7 端末のタイムアウト	情報システム活用ガイドライン	
86	9．5．8 接続時間の制限	情報システム活用ガイドライン システム開発規定　第2章　第7条　第3項 システム開発規定　第2章　第8条　第XX項	

〔2〕ISO/IEC17799の各管理項目から見た各規定の対応表（逆引き）

NO	管理項目名	対応規定名と条項	備考
9．6 アプリケーションのアクセス制御			
87	9．6．1 情報アクセスの制限	システム開発規定 第2章 第8条 第8.2項 システム運用規定 第20条 システム運用規定 第21条 システム運用規定 第23条 システム運用規定 第24条 システム運用規定 第25条 サーバ管理規定 第3章 第19条 サーバ管理規定 第3章 第20条 サーバ管理規定 第3章 第21条 サーバ管理規定 第3章 第22条 サーバ管理規定 第3章 第24条 サーバ管理規定 第3章 第25条 サーバ管理規定 第3章 第26条 データベース管理規定 第3章 第19条 データベース管理規定 第3章 第22条 データベース管理規定 第3章 第23条 データベース管理規定 第3章 第24条 通信ネットワーク管理規定 第3章 第17条 通信ネットワーク管理規定 第3章 第19条 通信ネットワーク管理規定 第3章 第20条 通信ネットワーク管理規定 第3章 第21条 システム開発規定第2章第4条　第2項 システム資源管理規定 第3章 第19条 システム資源管理規定 第3章 第20条 システム資源管理規定 第3章 第22条 システム資源管理規定 第3章 第23条 システム資源管理規定 第3章 第24条 情報システム活用ガイドライン	
88	9．6．2 重要なシステムの隔離	システム運用規定 第22条 サーバ管理規定 第2章 第23条 データベース管理規定 第3章 第21条 通信ネットワーク管理規定 第3章 第18条 情報システム活用ガイドライン	
9．7 システムアクセス及びシステム使用の監視			
89	9．7．1 イベントの記録	システム運用規定 第16条 サーバ管理規定 第2章 第16条 通信ネットワーク管理規定 第2章 第15条	
90	9．7．2 システム使用の監視	システム運用規定 第21条 システム運用規定 第23条 システム運用規定 第24条 サーバ管理規定 第2章 第20条 サーバ管理規定 第2章 第22条 データベース管理規定 第3章 第20条 通信ネットワーク管理規定 第3章 第17条	
91	9．7．3 クロックの同期	情報システム活用ガイドライン	
9．8 モバイルコンピューティング及びテレワーキング			
92	9．8．1 モバイルコンピューティング	情報システム活用ガイドライン	
93	9．8．2 テレワーキング	情報システム活用ガイドライン	
10 システムの開発及びメンテナンス			
10．1 システムのセキュリティ要求事項			
94	10．1．1 セキュリティ要求事項の分析と明示	システム開発規定 第2章 第7条 システム評価規定 第2章 第7条 第7.1項 システム評価規定 第2章 第7条 第7.3項	
10．2 アプリケーションシステムのセキュリティ			
95	10．2．1 入力データの妥当性確認	システム開発規定 第2章 第8条 第8.2項 情報・データ管理規定 第23条 情報システム活用ガイドライン	
96	10．2．2 内部処理の管理	システム開発規定 第2章 第8条 第8.2項 サーバ管理規定 第2章 第20条	
97	10．2．3 メッセージ認証	システム開発規定　第2章　第8条　第8.3項 情報システム活用ガイドライン	
98	10．2．4 出力データの妥当性確認	システム開発規定 第3章 第10条 第10.2項	
10．3 暗号による管理策			
99	10．3．1 暗号管理の使用に関するポリシー	システム開発規定第2章第7条 情報技術管理規定第 20条	

〔2〕ISO/IEC17799の各管理項目から見た各規定の対応表（逆引き）

NO	管理項目名	対応規定名と条項	備考
100	10．3．2 暗号化	システム開発規定第2章第7条 情報技術管理規定第 20条	
101	10．3．3 デジタル署名	システム開発規定第2章第7条 情報技術管理規定 第21条	
102	10．3．4 否認防止サービス	システム開発規定 第2章 第7条 情報技術管理規定 第21条	
103	10．3．5 暗号鍵の管理	情報技術管理規定 第21条	
10．4 システムファイルのセキュリティ			
104	10．4．1 運用ソフトウェアの管理	システム資源管理規定 第2章 第12条 システム資源管理規定 第2章 第14条 システム資源管理規定 第2章 第15条 システム資源管理規定 第2章 第16条	
105	10．4．2 システムテストデータの保護	システム開発規定 第3章 第10条 第10.2項	
106	10．4．3 プログラムソースライブラリーへのアクセス管理	システム開発規定 第3章 第9条 情報技術管理規定 第19条	
10．5 開発及びサポートプロセスにおけるセキュリティ			
107	10．5．1 変更管理手続き	システム開発規定 第2章 第7条 システム開発規定 第3章 第9条 システム開発規定 第4章 第17条 システム評価規定 第3章 第12条 セキュリティ管理規定 第22条 システム運用規定 第27条 サーバ管理規定 第4章 第28条 データベース管理規定 第3章 第26条 通信ネットワーク管理規定 第4章 第23条 システム資源管理規定 第4章 第26条	
108	10．5．2 オペレーティングシステムの変更の技術レビュー	システム開発規定 第3章 第9条 セキュリティ管理規定 第22条 サーバ管理規定 第2章 第13条	
109	10．5．3 ソフトウェアパッケージの変更に対する制限に対する制限	セキュリティ管理規定 第22条 システム開発規定 第2章 第7条 システム開発規定 第2章 第8条 第8.5項 サーバ管理規定 第2章 第13条	
110	10．5．4 隠れ通信路とトロイのコード	システム開発規定 第3章 第9条 システム開発規定 第3章 第12条 通信ネットワーク管理規定 第3章 第17条 情報システム活用ガイドライン	
111	10．5．5 アウトソーシングによるソフトウェア開発	情報処理外部委託規定 第2章 第14条	
11 事業継続管理			
11．1 事業継続管理の種々の面			
112	11．1．1 業務継続管理手続き	情報システム活用ガイドライン	別途「コンティンジェンシープラン」を作成する。
113	11．1．2 業務継続と影響分析	情報システム活用ガイドライン	別途「コンティンジェンシープラン」を作成する。
114	11．1．3 継続計画の作成と実行	情報システム活用ガイドライン	別途「コンティンジェンシープラン」を作成する。
115	11．1．4 業務継続計画作成の枠組み	情報システム活用ガイドライン	別途「コンティンジェンシープラン」を作成する。
116	11．1．5 業務継続計画のテスト・維持・再評		別途「コンティンジェンシープラン」を作成する。
12 準拠			
12．1 法的要求事項への準拠			
117	12．1．1 適用法規の識別	情報処理規定	
118	12．1．2 知的財産権	システム資源管理規定 第3章 第12条 システム資源管理規定 第3章 第14条	
119	12．1．3 組織における記録の保護		

〔2〕ISO/IEC17799の各管理項目から見た各規定の対応表（逆引き）

NO	管理項目名	対応規定名と条項	備考
120	12．1．4 データの保護と個人情報のプライバシー	セキュリティ管理規定 第4条 情報システム活用ガイドライン	
121	12．1．5 情報処理施設の誤使用の防止	情報システム活用ガイドライン	
122	12．1．6 暗号による管理策の規制	情報システム活用ガイドライン	
123	12．1．7 情報の収集	セキュリティ管理規定 第23条	
12．2 セキュリティポリシー及び技術準拠のレビュー			
124	12．2．1 セキュリティポリシーへの準拠	セキュリティ管理規定 第25条 セキュリティ管理規定 第31条 セキュリティ管理規定 第32条	
125	12．2．2 技術準拠のチェック		
12．3 システム監査の考慮事項			
126	12．3．1 システム監査	情報処理課金規定 第3章 第19条 セキュリティ管理規定 第31条 セキュリティ管理規定 第32条	審査機関からは、監査結果について経営層がレビューを行う体制になっていることを求めれられる。
127	12．3．2 システム監査ツールの保護		システム監査用のツールを使用している場合は具体的にその保護手続きを規定する。

第 4 部　情報セキュリティに関する法令および法律について

〔1〕　情報セキュリティ関連法令・ガイドライン・基準

〔2〕　セキュリティ管理と法律

〔１〕情報セキュリティ関連法令・ガイドライン・基準

※ 法令は、電子政府の「法令データ提供システム」（平成 14 年 8 月 1 日現在） を参照。
（憲法・法律:1,793 件、政令・勅令:1,862 件、府令・省令:3,431 件、計:7,086 法令）

(1)情報保護の法的根拠

●近代国家の誕生において、とりわけ自由主義経済国家では、市民の財産権を保護する制度が確立しています。我が国でも、憲法第 29 条が財産権の保障を規定しています。財産権は、有体物だけでなく無体物の財産も含むので、この条項は広く財産権的情報（*Proprietary Information*）保護の根拠とされています。[1]

●情報の法的保護の側面からは、情報財のほか人格権的情報すなわち名誉や個人情報・プライバシーがあります。名誉については民法第 723 条や刑法第 230 条に規定されています。プライバシーの保護については、我が国では実定法上の規定がなく、[2]憲法第 13 条（個人の尊厳）等を根拠として判例法が確立しています。

●このほか最近では、「パブリシティ権」と呼ばれる財産権的価値（顧客吸引力）をもった著名な私的領域情報（氏名・肖像等）が類型化されています。

(2)情報セキュリティと法

●情報の安全管理面からは、次の3つの方法が考えられます。
①情報が固定された「モノ」自体を保護する
②情報が存在する建物や領域への侵入防止をはかる
③情報自体を保護する

●情報の安全性の担保からすれば、これらすべてに対策を施すべきです。しかし今日のような情報ネットワークが発達した社会では、「ネットワーク・セキュリティ」という視点からの法的対策を優先させることが望ましい。

●本書ではモノに固定された情報財の窃盗や私的領域への不法侵入については不法行為法や財産法の一般条項を例示するに止め、ネットワークへの不法アクセスや、磁気記憶装置等へ固定された情報の破壊や窃用（複製）等を目的とした犯罪に関する法令を中心に列挙します。[3]

(3)情報セキュリティ関係法令

●近年、グローバル化により商圏を一にする北米・欧州・日本等が、条約締結を含め、連携して電子化社会に対応した法制度整備を進めています。これらは、情報ネットワーク社会を俯瞰する意味からも

---

1 情報の自由な表現や流通という側面からは、憲法第 21 条（言論・表現の自由）が重要である。コミュニケーション活動においてもそれを完全ならしめるため、同条2項後段は「通信の秘密」を定め、郵便法や電気通信事業関連法においてプライベート・コミュニケーションの安全性を保障している。第 21 条は民主主義の実現・発展のために用意されたシステムであるが、インターネット社会では誰もが情報発信者になり得るので、マスメディア以外の企業活動においても無関係ではない。通信の秘密は、デジタル通信技術の発達により「放送と通信の融合化」が進み、微妙なものとなっている。（無線と有線電気通信では「通信の秘密」の概念が異なる。）

2 個人情報については、「個人情報の保護に関する法律（案）」及び「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（改正案）」の2法案及び関連法が国会で審議中である。（2003.4）

3 我が国の情報通信基本戦略（e-Japan 戦略）の「重点計画」においても「情報ネットワークシステムの安全性や信頼性の確保」が最重要かつ緊急な課題として採り上げられ対応が進められている。

重要であるため、併せて本書でも列挙します。(■で表示した法令)

●技術が急速に進歩するなかで、すべてを法律に頼ることは困難です。こうした場合、行政機関が実効的手法として業界団体に向けてガイドラインを策定公布し、企業団体を指導する場合があります。企業の情報保護担当者は、すべてを法令に拠ることなく、国際機関や行政機関のガイドライン、業界団体のガイドラインについても熟知し対処することが望ましいでしょう。

憲 法

●日本国憲法(昭和 21 年 11 月 3 日)
第 13 条(個人の尊厳)「すべて国民は、個人として尊重される。」
第 21 条 1項(言論・表現の自由)「言論、出版その他一切の表現の自由は、これを保障する。」
2項後段(通信の秘密)「通信の秘密は、これを侵してはならない。」
第 29 条(財産権の保障)「財産権は、これを侵してはならない。」

条 約

■サイバー犯罪条約(*The Convention of Cybercrime*) 2001 年 11 月 23 日署名
(経済産業省:サイバー刑事法研究会報告書から「サイバー犯罪条約逐条解説」)

情報基本法

●高度情報通信ネットワーク社会形成基本法(平成 12 年 12 月 6 日法律第 144 号)

情報通信事業法

●電気通信事業法(昭和 59 年 12 月 25 日法律第 86 号)
●有線テレビジョン放送法(昭和 47 年 7 月 1 日法律第 114 号) 最終改正:平成 13 年 6 月 29 日法律第 85 号
●有線電気通信法(昭和 28 年 7 月 31 日法律第 96 号) 最終改正:平成 11 年 12 月 22 日法律第 160 号
●電気通信事業法等の一部を改正する法律(平成 13 年法律第 62 号)
●電気通信基盤充実臨時措置法の一部を改正する法律(平成 13 年法律第 43 号)
●電波法の一部を改正する法律(平成 13 年法律第 48 号)
●通信・放送融合技術の開発の促進に関する法律(平成 13 年 6 月 8 日法律第 44 号)
●電気通信役務利用放送法(平成 13 年 6 月 29 日法律第 85 号)
■特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律
(平成 13 年 11 月 30 日法律第 137 号)第4条(発信者情報の開示請求等)

情報化促進支援法

●情報処理の促進に関する法律(昭和 45 年 5 月 22 日法律第 90 号)
●書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律(IT 書面一括法)(平成 12 年法律第 126 号)
■電子署名及び認証業務に関する法律(平成 12 年 5 月 31 日法律第 102 号)
■電子署名及び認証業務に関する法律第 17 条第 1 項に規定する指定調査機関を指定する省令(平成 13 年 3 月 30 日総務省・法務省・経済産業省令第 3 号)
●商業登記法の一部を改正する法律(平成 12 年法律第 40 号)

●電気通信回線による登記情報の提供に関する法律(平成 11 年 12 月 23 日法律第 226 号)

コンピュータ犯罪法　※ コンピュータ、情報ネットワーク犯罪に関する法律

■刑法 (1987、2002 年:コンピュータ犯罪の規定を追加)

○第7条の2(**電磁的記録の定義**)
○第 157 条(**公正証書原本不実記載等**)
○第 158 条(**偽造公文書行使等**)
○第 161 条の2(**電磁的記録不正作出及び供用**)
○第 234 条の2(**電子計算機損壊等業務妨害**)
○第 246 条の2(**電子計算機使用詐欺**)
○第 258 条(**公用文書等毀棄**) 電磁的記録の毀棄
○第 259 条(**私用文書等毀棄**) 電磁的記録の毀棄

■刑法の一部を改正する法律(平成 13 年法律第 97 号) 刑法に「第 163 条の 2、3、4、5」を追加。

○第 163 条の 2(**支払用カード電磁的記録不正作出等**)
○第 163 条の 3(**不正電磁的記録カード所持**)
○第 163 条の 4(**支払用カード電磁的記録不正作出準備**)
○第 163 条の 5(**未遂罪**)

不正アクセス等

■不正アクセス行為の禁止等に関する法律(平成 11 年 8 月 13 日法律第 128 号)
最終改正年月日:平成 11 年 12 月 22 日法律第 160 号

●不正アクセス行為の再発を防止するための都道府県公安委員会による援助に関する規則(平成 11 年 12 月 20 日国家公安委員会規則第 12 号)

■犯罪捜査のための通信傍受に関する法律(平成 11 年 8 月 18 日法律第 137 号)
最終改正年月日:平成 13 年 12 月 12 日法律第 153 号

情報財保護法 (知的財産権法)

●特許法(昭和 34 年 4 月 13 日法律第 121 号)
●実用新案法(昭和 34 年 4 月 13 日法律第 123 号)
●意匠法(昭和 34 年 4 月 13 日法律第 125 号)
●商標法(昭和 34 年 4 月 13 日法律第 127 号)
■著作権法(昭和 45 年 5 月 6 日法律第 48 号) (公衆送信) (自動公衆送信) (送信可能可)
●著作権等管理事業法(平成 12 年 11 月 29 日法律第 131 号)
■不正競争防止法(平成 5 年 5 月 19 日法律第 47 号)

情報取引法

●特定電子メールの送信の適正化等に関する法律(平成 14 年 4 月 17 日法律第 26 号)
■電子消費者契約及び電子承諾通知に関する民法の特例に関する法律(平成 13 年 6 月 29 日法律第 95 号)
●特定商取引に関する法律(昭和 51 年 6 月 4 日法律第 57 号)最終改正:平成 14 年 4 月 19 日法律第 28 号
●風俗営業等の規制及び業務の適正化等に関する法律(昭和 23 年 7 月 10 日法律第 122 号)最終改

正:平成 14 年 5 月 29 日法律第 45 号
第 31 条の 7～第 31 条の 11(映像送信型性風俗特殊営業の規制等)
●古物営業法(昭和 24 年 5 月 28 日法律第 108 号)最終改正:平成 11 年 12 月 8 日法律第 151 号

行政機関と情報

■行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律(昭和 63 年 12 月 16 日法律第 95 号) 現在、改正案が国会で審議中(2003.4)
●行政機関の保有する情報の公開に関する法律(平成 11 年 5 月 14 日法律第 42 号) 最終改正:平成 13 年 12 月 5 日法律第 140 号
●住民基本台帳法(昭和 42 年 7 月 25 日法律第 81 号) 最終改正:平成 13 年 7 月 4 日法律第 101 号
●住民基本台帳の一部の写しの閲覧及び住民票の写し等の交付に関する省令
(昭和 60 年 12 月 13 日自治省令第 28 号) 最終改正:平成 13 年 10 月 10 日総務省令第 135 号
●地方公共団体の議会の議員及び長の選挙に係る電磁的記録式投票機を用いて行う投票方法等の特例に関する法律(平成 13 年 12 月 7 日法律第 147 号)
●警察の保有する電子計算機処理に係る個人情報の取扱いに関する規則(平成 2 年 6 月 8 日国家公安委員会規則第 2 号)

地方自治体と情報

●個人情報保護条例を制定している地方自治体は、1982団体に及ぶ。(60.1%)(平成 13 年4月1日:総務省)

個人情報保護に関する規定がある主な法令

●高度情報通信ネットワーク社会形成基本法(平成 12 年 12 月 6 日法律第 144 号)
第 23 条(高度情報通信ネットワークの安全性の確保等)
●ヒトに関するクローン技術等の規制に関する法律(平成 12 年 12 月 6 日法律第 146 号)
第 13 条(個人情報の保護)
●感染症の予防及び感染症の患者に対する医療に関する法律(平成 10 年 10 月 2 日法律第 114 号)
第十六条(情報の公表)
●港湾労働法施行規則(昭和 63 年 12 月 13 日労働省令第 35 号)
第 11 条(許可の申請手続)
●労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律
(昭和 60 年 7 月 5 日法律第 88 号)
第 7 条(許可の基準等)
第 24 条の 3(個人情報の取扱い)
●職業安定法(昭和 22 年 11 月 30 日法律第 141 号)
第 5 条の 4(求職者等の個人情報の取扱い)
第 51 条(秘密を守る義務等)
■個人情報の保護に関する法律(案)(平成 13 年 3 月 27 日閣議決定) 現在、国会で審議中
●地方自治体の個人情報保護条例 (または個人情報保護が盛り込まれた各種規程)

刑法(一般)

●刑法(明治 40 年 4 月 24 日法律第 45 号)最終改正:平成 13 年 12 月 12 日法律第 153 号
第 130 条 (住居侵入等)
第 133 条(信書開封)
第 134 条(秘密漏示)
第 222 条(脅迫)
第 230 条(名誉毀損)
第 233 条(信用毀損及び業務妨害)
第 235 条(窃盗)
第 246 条(詐欺)
第 263 条(信書隠匿)

民法(不法行為)

●民法(民法第一編第二編第三編) (明治 29 年 4 月 27 日法律第 89 号) 最終改正:平成 13 年 6 月 8 日法律第 41 号
第 709 条(不法行為の一般的要件・効果)
第 710 条(非財産的損害の賠償)

手続法

●民事保全法(平成元年 12 月 22 日法律第 91 号) 最終改正年月日:平成 14 年 6 月 12 日法律第 65 号
●民事訴訟法(平成 8 年 6 月 26 日法律第 109 号) 最終改正年月日:平成 14 年 6 月 12 日法律第 65 号
●刑事訴訟法(昭和 23 年 7 月 10 日法律第 131 号) 最終改正:平成 13 年 12 月 12 日法律第 153 号

商事法

●商法(明治 32 年 3 月 9 日法律第 48 号)
第 33 条の 2(電子帳簿・電子貸借対照表) 第 130 条(電子財産目録)
●商法等の一部を改正する法律(平成 13 年法律第 128 号)
●商法等の一部を改正する法律の施行に伴う関係法律の整備に関する法律(平成 13 年法律第 129 号)
●商法等の一部を改正する法律(平成 14 年 5 月 29 日法律第 44 号)
●商法及び有限会社法の関係規定に基づく電磁的方法による情報の提供等に関する承諾の手続等を定める政令(平成 14 年 1 月 30 日政令第 20 号)
●証券取引法(昭和 23 年 4 月 13 日法律第 25 号)第 27 条の 30 の 2

税 法

●所得税法(昭和 40 年 3 月 31 日法律第 33 号)
●法人税法(昭和 40 年 3 月 31 日法律第 34 号)
●国税通則法(昭和 37 年 4 月 2 日法律第 66 号)
●国税徴収法(昭和 34 年 4 月 20 日法律第 147 号)
●地方税法(昭和 25 年 7 月 31 日法律第 226 号) 第 26 条
●電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律

（平成 10 年 3 月 31 日法律第 25 号） 最終改正年月日:平成 12 年 5 月 31 日法律第 97 号

その他

●廃棄物の処理及び清掃に関する法律(昭和 45 年 12 月 25 日法律第 137 号)最終改正:平成 14 年 5 月 29 日法律第 45 号　第 13 条の2～第 13 条の 11(情報処理センターに関する規定)

●製造物責任法(平成 6 年 7 月 1 日法律第 85 五号)

●環境基本法(平成 5 年 11 月 19 日法律第 91 号)最終改正年月日:平成 12 年 6 月 2 日法律第 110 号

OECD のガイドライン

●OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980.9.23

http://www.oecd.org/EN/document/0,,EN-document-0-nodirectorate-no-24-10255-0,00.html#title0

●OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security 2002.8.7

http://www.oecd.org/pdf/M00033000/M00033182.pdf

●OECD Guidelines for Cryptography Policy 1997.12.19

http://www.oecd.org/EN/document/0,,EN-document-29-nodirectorate-no-24-10242-29,00.html

行政機関のガイドライン

●電気通信事業における個人情報保護に関するガイドライン 平成 10 年 12 月 2 日(郵政省)

http://www.soumu.go.jp/joho_tsusin/pressrelease/japanese/denki/001215j603.html#b1

●発信者情報通知サービスの利用における発信者個人情報の保護に関するガイドライン

http://www.soumu.go.jp/joho_tsusin/pressrelease/japanese/denki/981026d601_4.html

●情報通信ネットワーク安全・信頼性対策実施登録規程(昭和 62 年郵政省告示第 74 号)

http://www.soumu.go.jp/joho_tsusin/whatsnew/kokuji/network_0203.html#r-2

●情報通信ネットワーク安全・信頼性基準(昭和 62 年郵政省告示第 73 号)

http://www.soumu.go.jp/joho_tsusin/whatsnew/kokuji/network_0203.html#r-1

●民間部門における電子計算機処理に係わる個人情報の保護に関するガイドライン 平成 9 年 3 月 4 日

(通商産業省告示第 98 号)

http://www.meti.go.jp/policy/netsecurity/downloadfiles/P-guideline.pdf

●情報システム安全対策基準 (1995.8.28　平成 9 年 9 月 24 日最終改正 通商産業省告示第 536 号)[4]

http://www.meti.go.jp/policy/netsecurity/downloadfiles/esecu03j.pdf

●コンピュータ不正アクセス対策基準 (平成 8 年 8 月 8 日 通商産業省告示第 362 号)

http://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm

---

4 情報処理サービス業情報システム安全対策実施事業所認定制度（安対制度：2000.7.31 廃止）とは異なる。

●コンピュータウイルス対策基準(平成 7 年　通商産業省告示第 429 号)
http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm
●システム監査基準 (平成 8 年 1 月 30 日　通商産業省機械情報産業局)
http://www.meti.go.jp/policy/netsecurity/systemauditG.htm
●ソフトウエア管理ガイドライン(平成 7 年 11 月 15 日　通商産業省公表)
http://www.meti.go.jp/policy/netsecurity/downloadfiles/softkanri-guide.htm
●情報システム安全対策指針(平成 9 年 9 月 18 日制定　国家公安委員会告示第9号)
http://www.npa.go.jp/hightech/antai_sisin/kokuji.htm

〔2〕セキュリティ管理と法律

第１　セキュリティマネジメントと責任

１　セキュリティマネジメントと民事責任

自社の情報システムのセキュリティマネジメントの不備によって事故が発生した場合、会社は、契約にもとづいて、契約上の義務の履行ができなくなったこと、又は遅れたことによる損害を賠償する義務を負う(債務不履行責任・担保責任)。

なお、この損害発生の原因となった会社従業員の行為、役員の行為が、違法な場合は、会社は、不法行為としても損害賠償責任をすべき義務を負う。その理由付けとしては、会社自体・役員の不法行為(民法 709 条、商法 266 条の 3)、従業員の不法行為(民法 709 条)についての使用者責任(民法 715 条)が考えられる。

債務不履行責任・担保責任と不法行為・使用者責にこれらの責任は、損害賠償の理由付けや立証の方法が異なるだけで、当然のことながら二重に賠償する義務があるわけではない。

なお、役員は、顧客に対して直接に加害行為をした場合に限らず、委任関係にある会社に対して、役員としてなすべきことをせず、又は会社の利益に反して自分の利益を図り、その結果、会社に損害を発生させ、その結果顧客に損害を発生させたときにも、役員は、忠実義務、善管注意義務違反を理由に、顧客から損倍賠償責任を問われることがある。

２　代表訴訟

更にこの場合、役員は、株主から、会社に与えた損害を会社に戻すよう求められることがある(株主代表訴訟)。大和銀行ニューヨーク支店従業員が米国債の不正簿外取引で約 11 億ﾄﾞﾙの損失を出し、これをFRBに報告しなかったことや虚偽報告を理由に 16 罪の有罪、3 億 4 千万ﾄﾞﾙの罰金の支払い、国外退去を命じられた大和銀行事件においては、個人株主などが当時の経営陣に日本円で、約 1830 億円の支払いを求めた代表訴訟を提起し、大阪地裁は、当時のニューヨーク支店長であった元副頭取に5億3000万ドル（約567億円）を、現ニューヨーク支店長を含む現・元役員ら11人に計約2億4500万ドル（約262億円）の支払いを命じたことは記憶に新しい。(その後大阪高裁で被告側旧経営陣 49 名が約 2 億 5 千万円を支払う条件で和解)。

３　大和銀行判決に学ぶ　国際標準によるリスクマネジメントの責任

この判決には、注目すべき点が二つある。その一つは、当時のニューヨーク支店長だった取締役にのみ「保管残高の確認を極めて不適切な方法で行い、適切な方法に改めなかった点で、任務を果たしていなかった責任がある」と、役員に、不正行為を発見・防止責任、すなわち役員にリスク管理の義務を負わせていることである。

二つ目は、コンプライアンスの維持にローカルルールは通用しないことを明らかにしたことである。

判決は、「大蔵省の要望、示唆に反してアメリカ当局に報告する期待可能性がなかった」と主張した 11 名の取締役に対し、「大蔵省が取締役らに対し、権限に基づき、アメリカ当局に対する報告をしないよう指示ないし命令したと認めるに足りる証拠はない」とする一方で、取締役らが「我が国内でのみ通用する非公式のローカルルールに固執し、大蔵省銀行局長の威信を頼りとして大和銀行の危機を克服しようとして、アメリカ当局の厳しい処分を受ける事態を招いた」と判断し、当時の取締役が「法令に違反してア

メリカでの報告を怠ったのは不適切な経営判断」だと断じ、それぞれの責任の度合いに応じて、計2億4500万ドルを連帯して支払うよう命じた。

このように、大和銀行事件大阪地裁判決は、役員が、会社に対し、国際標準にもとづくリスクマネジメントを行うべき責任があることを示している。

第２　BS7799、ISMS と免責

１　では国際規格といわれる BS7799、ISMS による情報セキュリティマネジメントは、民事責任を免責するか?

これらに従った認証を受けていることだけをもって民事責任を免れることはない。

なぜなら、

(1)まず、認証は、認証の時における枠組みの確立・維持の存在を根拠づけるだけで、具体的なセキュリティ対策の効果を保証するものではないからである。

(2)次に、これらの認証は、会社が決定した範囲のシステムのみに対するものにすぎないからである。セキュリティ事故の発生原因が、会社が決定した範囲外から生じたときは、取締役がなした範囲決定の合理性があったかどうかが問われることになる。従って、会社が認証取得範囲を決定する場合には、その合理性を立証できる根拠を準備しておかなければならない。

(3)第三に、認証が与えられる枠組は、会社の行ったリスクアセスメント・リスクマネジメントの結果、選択された程度以上のリスクがあると会社が決定したものに対する枠組みにすぎないからである。認証は、リスクアセスメントやマネジメント合理性までは保証しない。従って、ここでも会社は、リスクアセスメントやマネジメント手法の合理性を根拠づける証拠を残しておく必要がある。

(4)第四に認証が与えられるのは、サンプリング手法による調査の結果に対してだという限界を持つからである。従って、サンプリング手法それ自体の合理性や、それ自体が合理的であったとしても、たまたま調査から漏れた箇所の不備が理由となって事故が起こった場合には、不備の原因と防止策を講じられなかった理由が問題とされることになり、認証を受けているからといって、一律に免責が受けられるわけではない。従って、高度なリスク管理を必要とする場面では、調査手法についても全数検査などの合意を行う必要がある。役員は、その判断を行った合理性を問われても、これを立証できるように準備した上で、調査手法に関する契約を行う必要がある。

２　ではＢＳ7799 やＩＳＭＳによる情報セキュリティマネジメントは、民事責任を軽減するのに役立たないのか

極めて役立つ。

上記のように、BS7799、ISMSは、企業や役員に完全な免責を導くものではない。

しかし、経営陣は、BS7799、ISMSを実施した認証を得ている限り、情報セキュリティマネジメントに、国際標準の枠組みを採用していることを立証できる。

仮に、これを行っていなければ、役員は、自ら、行っているセキュリティ対策が、国際標準に合致していることを立証する必要がある。それができるのは、全ての業種について、世界規模の支配的な力を持つ企業に止まるであろう。

更に、上記 1 の問題は、いわゆる経営判断事項に当たる。従って、上記各項目の合理性の根拠は多くの場合、一応の合理性が認められれば足り、これが認められれば、多くの場合、責任を追及する側が、不合理であることを立証する必要があるということになろう。

しかも、BS7799、ISMSの認証取得の実務においては、範囲設定、リスクアセスメント、管理策の選定

にあたっては、役員、現場代表などが委員会に参加し、そこでの検討、手法の選択の理由と結果が必然的に残ることになる。それらは、検討プロセスの合理性を根拠づける優良な証拠になるであろう。

更に、枠組み確立後は、その維持のための文書、記録が作成されることになり、3 ケ月おきのサーベイ、少なくとも 1 年毎の見直しがなされ、その結果がいちいち経営陣にﾚﾋﾞｭｰされ、経営陣はこれに基づき新たに改善策を発令してその実施が監督されることになる。このようなPDCAサイクルの実現は、事故を未然に防止するのに極めて有用である。そして、事故が発生しても、その発見、対処が迅速化される。特に、コンティンジェンシープランの策定による危機管理は、発生したリスクの具体化を、予想された事態として予め準備した処理プロセスに取り込むもので、リスク管理の合理性を立証できる。

このように、BS7799、ISMSの認証取得は、民事責任それ自体を軽減するとともに、紛争となったときの準備に極めて有用である。

第３　セキュリティマネジメント標準の今後

セキュリティマネジメント標準は、今後、ISO9k、14k シリーズ、個人情報保護のマネジメントプログラム、リスク管理プログラムと統合される方向にある。経済産業省が、情報システム監査と ISMS を巻き込みつつ採用すべきレベルの多様化を図った情報セキュリティ監査制度も動きを始める。今後の動きを注視する必要がある。

おわりに

冒頭にも述べたように、JUAS セキュリティ研究部会も4年目を迎え、本年度は各社が現在取り組んでいる、ないしはこれから取り組もうとしているセキュリティ管理基準（セキュリティポリシー）の制定に直接役立てるための、ISO/IEC17799 に準拠した JUAS 版セキュリティポリシーの雛形をまとめることに特化した活動を行いました。

この企画に対しては、大勢の参加者（発足 30 名、最終執筆者 25 名）を得ることができ、平成 14 年 6 月 13 日を初回に、毎月第 2 木曜日を原則に部会を開催し、平成 15 年 3 月まで 12 回の部会および企業訪問を実施し、またこの間に 8 つのサブグループ毎の会合が持たれる等、1年にわたり活発な活動が続けられました。

活動は、第 1 回部会で策定すべきセキュリティポリシーの体系、全体の構成を討議、決定し、第 2 回以降、それぞれの規定等を、上記の 8 つのサブグループで分担策定し、毎月 1 回開催される部会で全体調整を行うという方法で進めました。また、8 グループの中に、策定される規定類を、①国際規格の準拠性の確認、②法的側面からのチェックという2つの視点から調整を担当するグループを設けたことは、この活動を効果的に進めるのに役立ち、実用的なセキュリティポリシーの雛型ができたものと考えます。
以下に活動の経過を示します。

第 1 回　平成 14 年 6 月 13 日（木）
- 趣旨および活動テーマ、活動計画の説明
- 作業内容に基づいたグループ編成

第 2 回　平成 14 年 7 月 11 日（木）
- 向山氏による情報処理規定集の全体および個々の内容についての説明

第 3 回　平成 14 年 8 月 8 日（木）
- サブグループ毎の目次案の報告

第 4 回　平成 14 年 9 月 12 日（木）
- サブグループ毎の進捗状況の報告

第 5 回　平成 14 年 10 月 10 日（木）
- サブグループ毎の進捗状況の報告

第 6 回　平成 14 年 11 月 14 日（木）
- サブグループ毎の作業進捗状況の報告および意見交換・調整

第 7 回　平成 14 年 12 月 12 日（木）
- サブグループ毎の作業進捗状況の報告および意見交換・調整

第 8 回　平成 15 年 1 月 9 日（木）
- サブグループ毎に作成した規定集たたき台原稿の読み合わせ

第 9 回　平成 15 年 2 月 5 日（水）
- ISMS 認定取得企業（株式会社アイネス）の訪問

第 10 回　平成 15 年 2 月 13 日（木）
- 全体の統一的表現すり合わせ

第 11 回　平成 15 年 3 月 13 日（木）

・ 提出原稿の最終調整

第 12 回 平成 15 年 3 月 31 日（月）

・ 完成原稿の最終確認

また、メンバーの中に、昨年から引き続き継続して参加される方も多かったこと、また、これから勉強して各社のセキュリティポリシー策定の参考にしようという若手から、すでに ISMS の審査員などされているベテランのコンサルタント、また法律の専門家など、多彩な人材がバランスよくおられたことにより、それぞれの参加目的に合致し、またお互いに刺激されながら充実した活動ができたものと考えます。

今回作成した実用的な JUAS 版セキュリティ管理基準（セキュリティポリシー）は、JUAS 会員企業はもとより、会員外企業でも十分活用可能な内容になっていると考えられ、広く活用されることを期待します。

最後に、この規定集の基本部分をオープンソースとして快く提供いただいたメンバーの向山聡氏（社会経済生産生本部）、また研究部会事務局としてお世話いただいた高橋節子氏、小川あつし氏、城戸裕美氏に感謝の意を表します。

	用語	意味（JIS定義）	対応英語
あ行			
	アクセスする。	資源を使用できるようにする。	to access
	アクセス制御	データ処理システムの資源に対して、認可されたエンティティが認可された方法だけでアクセス できることを確実にする手段。	access control
	アクセスレベル	保護された資源にアクセスするために、エンティティに必要な権限のレベ	access level
	アクセス権	あるサブジェクトが、特定の型の操作を行うために、特定のオブジェクトにアクセスする ための許可。	access right
	暗号	データを変換する原理、手段及び方法を具体化する技術分野であって、その意味内容を隠し、認可されていない利用を防ぎ、又は検出されない変更を防ぐことを目的とするもの。	cryptography
	暗号化	データの暗号変換。 備考1、暗号化により暗号文が得られる。 2、逆のプロセスを復号とよぶ。	encryption,encipherment
か行			
	可用性	認可されたエンティティから請求があり次第、アクセスし利用できるようにする、データ又は資源の特性。	availability
	監査証跡	セキュリティ監査で利用することを考えて収集するデータ	audit trail
	完全性	情報資産や情報システムが改ざんされないこと。→データの完全性参照。	integrity(JISハンドブックになし)
	機密性	データの特性であって、そのデータが、認可されていない個人、プロセス又は他のエンティティに利用可能とならない程度、又は暴露されない程度を示すもの。	confidentiality
	脅威	セキュリティの潜在的な違反	threat
	危機	特定の脅威が、データ処理システムの特定の脆弱性を利用する可能性。	risk
	計算機システム監	データ処理システム内で使う手続きの検査であって、その有効性と正しさとを評価し、 改善の推薦をおこなうもの。	computer-system audit
さ行			
	初期化	機械を始動可能状態にするための操作、又はデータ媒体を使用する前、若しくは処理を行う前に必要とされる操作。	initialization
	消去する。	データをデータ媒体から除去すること。 備考：消去は、通常、データを重ね書きするかポインタを削除することで行われる。	to erase
	障害対策計画、災害復旧計画	バックアップ手続き、緊急時の対応、及び災害後の復旧のための計画。	contigency plan, disaster recovery plan
	セキュリティ	通常、適切な行動を取ることにより、事故又は悪意に基づく行為からデータ及び資源を保護すること。そのような行為には、許可されていない変更、破壊、アクセス、暴露、取得などがある。	security
	セキュリティ監査	データ処理システムの記録及び行為に対する独立した検閲及び検査であって、システム制御が適切であるかどうかを試験し、設定したセキュリティ方針及び操作手続き適合しているかどうかを確認し、セキュリティへの侵入工作を検出し、さらに、制御、セキュリティ方針並びに手続きに対して、提示された変更を推薦することを目的とするもの。	security audit

	セキュリティレベル	階層的なセキュリティ区分とセキュリティ部類との組み合わせであって、あるオブジェクトの保護必要度、又はある個人のセキュリティ許容度を表すもの。	seculity level
	損失	セキュリティ破壊の招来から生じた損害の定量的な尺度。	loss
	情報	事実、事象、事物、過程、着想などの対象物に関して知り得たことであって、概念を含み、一定の分脈中で特定の意味を持つもの。	information
	情報管理	情報処理システムにおいて、情報の取得、分析、保存、検索及び配布を制御する機能。	information management
	情報処理	情報に対して行われる、データ処理を含む操作の体系的実施。データ通信、オフィスオートメーションなどの操作を含むことがある。	information processing
	脆弱性	データ処理システムの弱点又は欠陥。	vulnerability
た行			
	データ	情報の表現であって、伝達、解釈または処理に適するように形式化され、再度情報として解釈できるもの。 備考1、データに対する処理は、人間がおこなってもよいし、自動的手段で行ってもよい。	data
	データ管理	データ処理システムにおいて、データに対するアクセス、データの記憶の実行・監視及び入出力操作の制御をする機能。	data management
	データの復元	失われたデータ又は汚染されたデータを再生する行為。	data restoration
	データの完全性	データの特性であって、その正確さと一貫性が、データにどのような変更を行っても保存されるもの。	data integrity
な行			
は行			
	平文	暗号技術を使わずに、内容の意味を読み取ることのできるデータ。	plaintext,cleartext
	ファイル	一つの単位とそて記憶または処理される、レコードからなる名前のついた	file
	バックアップ	喪失もしくは破壊されたデータの復元を助けるために、またはシステムの作動を維持するために使用する手続き、技法またはハードウェアに関する用語。	backup
	プライバシ	個人に関するデータの、不当又は不法な収集及び利用によって、その個人の私生活又は私事への侵入をうける、ということのない権利。	privacy
	プライバシ保護、個人情報保護	プライバシを確保するためにとる手段。	privacy protection
ま行			
や行			
ら行			
	リスク分析	保護すべき情報資産（ハード、ソフト、データ、情報記録媒体、関連ドキュメント等）を明らかにし、それらに対するリスクを評価すること。情報資産に対して考えられる脅威を明らかにして、そのリスクの程度を評価する。	risk analysis（JISハンドブックになし）
わ行			

セキュリティ研究部会メンバー

部会長	永田　靖人	ぷらっとホーム㈱　取締役
副部会長	川井　雅之	㈱オーク情報システム　社長室担当部長　情報企画グループ長
副部会長	宮木　宏尚	東レ㈱）　システム企画開発部主幹（現　ミヤキ㈱　常務取締役）
	陸田　浩司	㈱アイネス　技術開発本部　生産管理部
	岸本　佳宏	ＩＴエンジニアリング㈱　アウトソーシング事業本部　インフラサービス事業部セキュリティサービス部
	上野　耕司	新日本石油㈱　情報システム部　情報インフラグループ主事
	柄澤　正明	川鉄情報システム㈱　第２総括部 主任部員（次長）
	荘司　芳久	㈱日立製作所　情報システム事業部 e-プラットホーム本部認証サービス部技師
	小川永志樹	横河電機㈱　海外システム事業部　制御システム事業本部 IA ソリューションセンター課長代理
	天沼　宏幸	旭化成情報システム㈱　技術企画部主査
	西川　征一	㈱シーエーシー　EST コンサルティング部シニア・コンサルタント
	坂本　隆明	アイエックス・ナレッジ㈱　ＰＳ事業部
	本間　広信	NTT コムウェア㈱　ＮＴＴ営業本部　第一営業部スペシャリスト
	三輪田泰典	㈱日立製作所　情報システム事業部 e-プラットホーム本部情報セキュリティソリューション部
	千枝　和行	山之内製薬㈱　情報システム部課長
	辻井　良彦	NTT インターネット㈱　第１システム事業部　ビジネスバリューネットワーク（決済）担当　ｉ-コレクトプロジェクトサブリーダ
	小熊　紀孝	㈱うえじま企画　管理部インフラ担当
	大平　稔則	キユーピー㈱　情報企画部
	吉田　　眞	㈱ハピネックス　経営コンサルタント
	長浜　正道	JUAS 公認情報システムコンサルタント（ISC065）
	羽田　卓郎	リコー・ヒューマン・クリエイツ㈱　リコー情報セキュリティ研究センター情報セキュリティマネジメント室副室長　ＩＳＭＳ主任審査員
	向山　　聡	社会経済生産性本部　経営コンサルタント
	綿貫　俊喜	ソニー生命保険㈱　事務管理部　ＩＳ管理課統括課長
	稲垣　隆一	稲垣隆一法律事務所弁護士
	藤田　素康	リコー・ヒューマン・クリエイツ㈱　リコー情報セキュリティ研究センター　所長
事務局	高橋　節子	（社）日本情報システム・ユーザー協会
	城戸　裕美	（社）日本情報システム・ユーザー協会

（順不同）

セキュリティ研究部会報告書　執筆分担表

第１部　国際規格に準拠したセキュリティ管理汎用規定集

規定集の概要　川井　雅之

〔１〕前提規定　岸本　佳宏＊　陸田　浩司　上野　耕司

〔２〕基本規定　岸本　佳宏＊　陸田　浩司　上野　耕司

〔３〕情報管理関連規定　柄澤　正明＊　荘司　芳久　小川永志樹

〔４〕システム開発・運用関連規定
システム開発規定／システム評価規定
千枝　和行＊　三輪田泰典　坂本　隆明　本間　広信
システム管理規定／サーバー管理規定／データベース管理規定
通信ネットワーク管理規定／システム資源管理規定
辻井　良彦　小熊　紀孝

〔５〕一般運用関連規定　西川　征一　天沼　宏幸

〔６〕情報セキュリティガイドライン　吉田　　眞　大平　稔則　長浜　正道　向山　　聡

第３部　国際規格との準拠　羽田　卓郎　綿貫　俊喜　向山　　聡

第４部　情報セキュリティに関する法令および法律について　稲垣　隆一　藤田　素康

おわりに　宮木　宏尚

（＊はサブリーダー）