「システム監査用語の定義と解説」公開のこと

システム監査用語研究プロジェクト

「システム監査用語研究プロジェクト」では、３年間にわたって、システム監査に関連した用語の定義および解説の研究・とりまとめを行ってきました。

システム監査を取り巻く環境変化は目まぐるしく、活動途中で「システム監査基準」の改訂、「システム管理基準」の新設などもあり、用語の定義・解説について、途中で変更や追加を余儀なくされた状況も多々ありましたが、プロジェクトメンバーの皆さんの熱心な活動によって、ここに研究成果がまとまりましたので、皆さんにご参考にしていただきたく、公開させていただきます。

なお、この定義・解説は、皆さんが監査実務・執筆・講演などでお使いいただいて結構ですが、その際には出典を必ず明記していただきますよう、お願いします。

平成１７年６月１日

システム監査用語研究プロジェクト

小野　修一（主査）	岩崎　昭一	橘和　尚道
竹下　和孝	沼野　伸生	林　　兵江
本田　実		

システム監査用語の定義と解説

平成１７年６月

システム監査用語研究プロジェクト

１．システム監査

定義：システム監査は、組織体の情報システムにまつわるリスクに対するコントロールが、リスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行う活動である。

解説：この定義は、新しい『システム監査基準（2004.10 改訂）』にある「システム監査の目的」の記述から引用している。「情報セキュリティ監査基準(2003.4 策定)」の情報セキュリティ監査の考え方と整合性をとっているので、別項の『情報セキュリティ監査制度』の項も参照のこと。以下若干の補足をして解説とする。

システム監査の対象は、電子計算機とネットワークを中核とした情報システム及びそのライフサイクルプロセスであり、情報及びデータの収集・作成から活用・管理･廃棄までの全てのプロセスを含むものである。これを「情報システム」と総称している。

また、情報システムは組織体の目標達成に役立つ情報及び業務処理を提供することを使命とするが、システム監査はその使命の達成に貢献することを目的とする。

そしてその結果として組織体の『IT ガバナンス』の実現に、また情報システムにまつわる『リスク』に対する『コントロール』が適切に整備・運用されていることの説明責任を果たすことに寄与することとなる。

適切であるか否かを問われる情報システムにまつわるリスクに対するコントロールの目的は、新しいシステム監査基準の前文に次の四つにわけて示されている。

①情報システムが、組織体の経営方針及び戦略目標の実現に貢献するため

②情報システムが、組織体の目的を実現するように安全、有効かつ効率的に機能するため

③情報システムが、内部又は外部に報告する情報の信頼性を保つように機能するため

④情報システムが、関連法令、契約又は内部規程等に準拠するようにするため

なお『金融機関等のシステム監査指針（2000.7 改訂）』ではリスク管理の視点から、システム監査を「情報システムの有効性、効率性、信頼性、遵守性、および安全性の達成を妨げようとする情報システムリスクの管理体制が適切かつ効果的であるかを、監査対象から組織的に独立したシステム監査人が把握、評価し、その結果を経営者に報告するものである。」と定義している。

２．内部監査

定義：組織体の経営目標の効果的な達成に役立つことを目的として、経営諸活動の遂行状況を、合法性と合理性の観点から公正かつ客観的な立場で検討・評価し、これにもとづき特に改善を重視して助言・勧告を行う組織体内の独立的な機能である。

解説：この定義は日本内部監査協会が「内部監査基準(1996.5 改訂)」のなかで定めているものである。内部監査は組織体の独自の判断にもとづいて実施されるのであるが、定義された機能の効果を発揮させるためにも組織体の長に直属する組織上の位置づけも必要となっている。監査の観点は合法性(法に抵触してないか)と合理性(無駄なく能率的であるか)であるが、経営目標を効果的に達成するために、事業活動の効率的推進と規律保持・士気高揚をうながして、社会的信頼を確保する必要に応えるものである。

なお米国内部監査人協会（IIA）の新定義（1999.6）は、「内部監査は、組織体のオペレーションに価値を付加し、それを改善することを目的とする独立的かつ客観的アシュアランスおよびコンサルティング活動である。（山本明知氏訳）」となり、これまでの単なる「組織内の独立した評価機能」の定義から激変している。
また「品質及び/又は環境マネジメントシステム監査(JIS Q 19011)では、内部監査を「第一者監査」(独立性は監査の対象となる活動に関する責任を負っていないことで実証)と呼ぶこともある。

３．外部監査

定義：組織体の内部または外部の利害関係者のために、組織体から独立した外部の専門家によって実施される監査である。

解説：もともと組織体外部の会計監査人など第三者が行う『会計監査』のことである。法律に基づく監査制度として、商法・証券取引法による『会計監査人』(公認会計士・監査法人)の監査が代表的であるが、監督官庁の検査・監査など被監査組織体の意思に関係なく行われる監査もある。システム監査においては、システム監査企業台帳の登録企業による監査が代表的な事例である。『金融検査マニュアル』(システム統合リスクのチェックリスト)の「第三者機関による評価」の例示にある「システム監査人よるシステム監査」もこれにあたる。ただし登録企業やシステム監査人が内部監査の一部または全部を請け負う場合は、外部監査ではなく一部または全部の外部委託された内部監査ということになる。
なお、自治体の内部監査部門としての監査委員会に対し、外部監査の制度として「包括外部監査」と「個別外部監査」が制度化(地方自治法第 252 条の 27)されている。
また、「品質及び/又は環境マネジメントシステム監査(JIS Q 19011)では、外部監査には「第二者監査」(顧客など組織の利害関係者による監査)及び「第三者監査」(審査登録・認証機関などによる監査)と呼ばれるものが含まれる。

４．会計監査

定義：組織体の会計業務の監査をいい、主として財務諸表がその組織体の財産、損益の状況を適正に表示しているか否かを監査することをいう。

解説：法定監査としての会計監査の主体は、監査役と会計監査人(公認会計士・監査法人)に大別される。株式会社にあっては、いわゆる特例法の区分により次のように定められている。(三様監査については、『業務監査』の項目参照)

［株式会社の監査等に関する商法の特例に関する法律］（特例法）による区分

・大会社＝資本金５億円以上または負債合計 200 億円以上（同法 2 条）
　　会計監査人の監査を義務づける。監査役は業務監査にウエイトを置ける
・中会社＝資本金１億円超、５億円未満、負債合計 200 億円未満（同法非該当・商法適用）
　　監査役は業務監査と会計監査の両方を行う
・小会社＝資本金１億円以下、負債合計 200 億円未満（同法 22 条）
　　監査役は会計監査を行う

なお、2002 年の商法特例法の改正により、資本金１億円以上の株式会社は、定款に公認会計士または監査法人を会計監査人に選任する旨を定め、「みなし大会社」となり、大会社の規定の適用を受けることとなった。

５．業務監査

定義：組織体の会計以外の業務の監査をいい、組織体の人事、購買、製造、販売等の会計業務以外の業務活動全般にわたって、その遂行状況を監査することをいう。

解説 :組織体の経営目標の達成を目的とし、合法性、合理性の観点から経営諸活動を監査することで、内部監査部門の監査、監査役監査がそれぞれの立場でこれに関わっている。なお「会計以外の業務の監査」の用語は、商法の特例法第 14 条「監査役の監査報告書」にあるので、これを採用した。

また、この両監査と会計監査人監査をあわせて、「三様監査」と呼び次のように整理される。

［株式会社の監査制度］（いわゆる大会社の場合）

①商法監査（監査役、会計監査人＝公認会計士・監査法人）

②証券取引法監査（公認会計士・監査法人＝会計監査人）

③内部監査＝任意監査（内部監査人）

の三様監査から成立つ。なお、これを監査主体別に区分すれば、次のようになる。

・監査役監査(取締役の職務執行の適法性の監査)

・会計監査人監査(財務諸表の適正性の監査)

・内部監査(企業の内部統制の監査)

６．経営監査

定義：組織体の経営層を対象にした監査をいい、取締役の職務執行の監査を行う『監査役監査』や取締役会のリスク管理認識等を経営の視点から問う監査等をいう。

解説：商法 274 条に「監査役ハ取締役ノ職務ノ執行ヲ監査ス」るとあり、これこそ経営監査の代表例と言える。最近では『金融検査マニュアル』等で取締役、取締役会の経営戦略、リスク認識、リスク管理方針等を問う姿勢が強化され、『外部監査』・『内部監査』ともに経営監査の視点からの監査が一般化されてきている。新しいシステム監査の視点も同じ方向に向かっている。

７．任意監査

定義：組織体の自由意思によって行う内部監査をいい、『法定監査』・強制監査の監査役監査、会計監査人監査や監督官庁の検査・監査と区別される。

解説：システム監査は任意監査である。ただし監査の目的や監査主体によって法定監査・強制監査に該当することもある。『システム監査基準』に規定されるシステム監査は『内部監査』の位置づけであったが、現在は内部、『外部監査』に共通する基準になっている。『金融機関等のシステム監査指針』もシステム監査を「内部監査の一環として経営者からの委任を受けて実施するもの」としているが、外部機関の利用も有効としている。

８．法定監査

定義：商法で定める監査役監査、商法・証取法で定める会計監査人(公認会計士・監査法人)監査などのように、法令によって定められている監査をいう。

解説：『監査役監査』、『公認会計士監査』などの項目参照。

９．監査役監査

定義：商法ならびに「株式会社の監査等に関する商法の特例に関する法律（特例法）」で定める監査役監査をいう。商法では、「監査役ハ取締役ノ職務ノ執行ヲ監査ス」る権限を規定し、特例法では株式会社の規模により、監査役の業務監査と会計監査へのかかわりを規定している。

解説：『会計監査』、『業務監査』などの項目参照。

１０．公認会計士監査

定義：会計監査人すなわち公認会計士または監査法人が行う会計監査のことをいう。

解説：『会計監査』の項目参照。

１１．会計監査人

定義：会計監査人は公認会計士（外国公認会計士を含む。）または監査法人のことをいう。

解説：商法の特例法による区分で、資本金５億円以上または負債合計 200 億円以上（同法２条）の株式会社は、計算書類等について監査役の監査のほか、「会計監査人の監査」を義務づけられている。『会計監査』の項目参照。

１２．システム監査人の独立性

定義：監査結果の保証あるいは助言が公正・不偏であるために、システム監査人が被監査主体から組織的にも精神的にも独立していることをいう。

解説：システム監査が公正かつ妥当に実施されるためには、システム監査人の独立性、客観性が要求される。そのためには、システム監査人が被監査主体である情報システム部門はもちろんユーザ部門などから、外観上も精神上でも独立性を保持していることが必要である。『システム監査基準』ではその一般基準の中で、「外観上の独立性」と「精神上の独立性」を項を分けて定めている。

１３．システム監査技術者

定義：システム監査技術者試験の合格者をいう。「情報処理の促進に関する法律」に基づき定められた「情報処理技術者試験規則」による国家試験の合格者である。

解説：システム監査を普及するためには、システム監査人の養成が必要であり、そのための通産省・経済産業省の施策として能力認定試験（1986 年以降）が行われてきた。当初「情報処理システム監査技術者試験」の名称であったが、1994 年から現在の「システム監査技術者試験」となっている。その間、高度情報化人材育成標準カリキュラムに基づく育成カリキュラムに準拠した試験へ、更に現在の出題範囲、スキル標準の策定・公表による試験の実施に変るなど制度改善が行われてきた。

試験科目は、情報処理システムに関する知識、情報処理システムの監査に関する専門的知識、情報処理システムの監査に関する専門的能力を問うものである。試験(2005 年春より)は午前問題が多肢選択式(四肢択一)55 問(100 分)、午後Ⅰ問題が４問中３問選択記述式(90 分)、午後Ⅱ問題が３問中１問選択論述式(小論文、120 分)である。「合格率は 5.6～7.6 の間で平均 6.7%」となり、情報処理技術者試験の中で最も難しい試験の一つとされる。2004 年までの累計合格者は 5,440 人に達している。

なお、本試験制度の運営は独立行政法人情報処理推進機構:情報処理技術者試験センター（別掲参考 URL 参照）が行っている。(Information-technology Protection Agency, Japan=IPA)

１４．公認システム監査人

定義：システム監査技術者試験合格者について、実務経験を確認し継続教育を義務づけて「公認システム監査人」(CSA)として認定する制度である。システム監査の実務経験を積む間は、「システム監査人補」(ASA)として認定され、両者ともに一定の継続教育を受けることを義務づけられる。

解説：産業構造審議会の情報産業部会・情報人材対策小委員会は、その中間報告(1999.6.1)で次の２点の指摘を行った。一つは、「システム監査人がユーザの信頼を得るためには、単に知識等に習熟するのみならず、実践的監査経験を積むことが重要である。その観点から、従来より実施しているシステム監査技術者試験に合格した上で、一定の有効な実務経験を積んだことを確認することにより、システム監査人として認定する制度の創設を検討する。」またもう一つは「IT 技術が急速に変化する中で、システム監査人が最新の技術動向に対応できるよう情報処理技術者試験の見直しと併せて定期的セミナーの受講を義務づけるなどの方策を検討する。」である。

この提言を受けて、特定非営利活動法人の「日本システム監査人協会」(Systems Auditors Association of Japan=SAAJ)が 2002 年４月に、経済産業省の指導のもとにこの制度を創設した。公認システム監査人の英語名は、Certified Systems Auditor(CSA)である。またシステム監査人補は、Associate Systems Auditor (ASA)である。

なお、その他の高度情報処理技術者や公認会計士等関連資格の保持者に対して特別認定制度の講習・試験の合格を条件にシステム監査人補に認定する特認制度が設けられている。

本認定制度の運営は、特定非営利活動法人日本システム監査人協会(別掲参考 URL 参照)が行っている。

１５．専門監査人制度

定義：システム監査学会（JSSA；Japan Society for Systems Audits）が運営している制度であり、学会員の中で一定の要件を満たしたシステム監査人を専門監査人（CMA；Certified Master Auditor）として認定し、精度の高い監査の実施による情報化社会の安全化・安定化への貢献を目的としたものである。

解説：システム監査学会が 2004 年度から運営を開始した制度である。現在、専門監査人の区分として、情報セキュリティ専門監査人、個人情報保護専門監査人、会計システム

専門監査人の３つが設定されており、今後、新しい専門監査人区分の設定も検討されている。
それぞれの専門監査人の要件、認定を受けるための手順、認定を受けた後の更新手順などについては、システム監査学会のホームページに掲載されているので、参照のこと（別掲参考 URL 参照)。

１６．ＣＩＳＡ(公認情報システム監査人)

定義：米国の ISACA（Information Systems Audit and Control Association）の実施する CISA 試験（Certified Information Systems Auditor）の合格者に対し一定の実務経験を条件に認定される資格保持者をいう。資格の維持には継続教育を受ける必要がある。

解説：CISA 試験は、情報システム監査、コントロールおよびセキュリティの実務能力をテストするもので、200 問の多肢選択式問題(４時間)からなる。世界各国で受験可能で日本では、日本語で受験できる。CISA は日本語で「公認情報システム監査人」と訳されている。なお、ISACA(情報システムコントロール協会)は、情報システムの安全性・有効性向上、システム監査の普及等を目的とした非営利団体で、米国イリノイ州に本部があり、日本には東京、名古屋、大阪に支部がある。
試験の運営は、米国本部と各支部が担当している。(別掲参考 URL 参照)

１７．ＣＩＡ(公認内部監査人)

定義：米国の内部監査人協会(The Institute of Internal Auditors)の実施する CIA（Certified Internal Auditor=公認内部監査人）試験に合格し実務経験等の要件を満たしたものに授与される称号である。

解説：CIA 試験は、日本では日本内部監査協会(Institute of Internal Auditors Japan=IIA-J)が実施し、日本語で受験できる。試験科目は①監査理論および実務、②内部監査の技術および手続、③経営管理と情報技術、④監査環境の四つで、各３時間半で２日間の試験である。科目単位の合格が認められる。
なお、日本内部監査協会では、システム監査関連では「情報システム監査専門内部監査士」の認定制度を、1988 年から実施している。認定のための講習会が８日間(45 時間)あり、終了論文を提出後資格審査委員会において審査され「情報システム監査専門内部監査士」の称号を授与される。(別掲参考 URL 参照)

１８．情報セキュリティ監査制度

定義：情報セキュリティ監査は「情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うこと」と定義される。このような監査を行うために制度化された情報セキュリティ監査基準、同管理基準、同監査企業台帳など一連の経済産業省の施策をいう。

解説：情報セキュリティ監査の定義は新たに策定(2003.4)された情報セキュリティ監査基準に定められている。経済産業省は 2002 年９月より諮問研究会として「情報セキュリ

ティ監査研究会」を設置して検討を行い、その成果としてこの監査制度が出来あがった(2003.3.26)。
その主な点は、①情報セキュリティ監査のあり方、②情報セキュリティ監査の標準的な基準と監査主体のあり方、③電子政府に対する情報セキュリティ監査のあり方、それぞれへの提示であった。関係資料としては次のとおりである。

1.監査基準
　情報セキュリティ監査基準、同実施基準ガイドライン、同報告基準ガイドライン
2.管理基準
　情報セキュリティ管理基準、個別管理基準(監査項目)策定ガイドライン
3.モデル
　電子政府情報セキュリティ監査基準モデル、同管理基準モデル

なお、本制度の運用開始を受け、監査企業や監査人、一般企業や団体が一同に会して特定非営利活動法人日本セキュリティ監査協会(Japan information Security Audit association=JASA)を設立している(2002 年２月、別掲参考 URL 参照)。
また、同協会は「公認情報セキュリティ監査人」資格制度（英語名称：Certified Auditor for Information Security 略称：ケイズ CAIS）を創設した。同協会内に資格認定委員会を組織し、資格制度の運用ならびに資格認定を行うとともに、2004 年 12 月から資格認定の前提となる知識・経験を修得するための研修・トレーニングコースの開催、2005 年２月より認定を始めている。

１９．システム監査基準

定義：経済産業省により策定公表(1985 年策定、1996 年改訂、2004 年 10 月改訂)されているもので、システム監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的としたシステム監査人の「行為規範」である。

解説：1985 年通産省（当時）によって策定され公表されたもので、システム監査に必要な事項を網羅的に示すガイドラインとしての役割を果たしてきた。1996 年１月に第１回の改訂、そして今回 2004 年 10 月８日に第２回の改訂が公表された。改訂の内容は IT 投資の目的が現場の合理化から経営革新へと大きく変化するなか、国際的動向も踏まえたものとなり、旧システム監査基準の実施基準の主要部分を抜き出して、『システム管理基準』に独立させた。それは組織体のシステムリスク低減のための実践規範、システム監査人の「判断の尺度」に位置付けられている。
スリムになった新システム監査基準は、監査人の行為規範として位置付けられ、組織体の内部監査部門等が実施するシステム監査だけでなく、外部に監査を依頼するシステム監査においても利用できる。また保証型監査であっても、助言型監査でも利用できる内容である。
その構成は、次のようになっている。

①前文
　システム監査の位置づけ、性格、システム管理基準の関係等の記述
②システム監査の目的
　システム監査の目的の記述

③一般基準（８項目）
　システム監査人としての適格性及び監査業務上の遵守事項を規定
④実施基準（７項目）
　監査計画の立案及び監査手続の適用方法を中心に監査実施上の枠組みを規定
⑤報告基準（５項目）
　監査報告に係る留意事項と監査報告書の記載方式を規定

２０．システム管理基準

定義：経済産業省により新たに策定公表(2004.10.8)されたもので、組織体が主体的に経営戦略に沿って効果的な情報戦略を立案し、その戦略に基づき情報システムの企画・開発・運用・保守というライフサイクルの中で、効果的な情報システム投資のための、またリスクを低減するためのコントロールを適切に整備・運用するための実践規範であり、同時にシステム監査人の監査上の「判断の尺度」として位置付けられている。

解説：『システム監査基準』は 2004 年 10 月に２回目の改訂が公表された。改訂の内容はIT 投資の目的が現場の合理化から経営革新へと大きく変化するなか、国際的動向も踏まえ、システム監査基準の中の実施基準の主要部分を抜き出して、「システム管理基準」として独立させ、「システム監査基準」とともに姉妹編を構成することとなった。

この「システム管理基準」は、上述のように組織体の実践規範と位置づけられると同時に、システム監査基準に従ってシステム監査を実施する場合のシステム監査人の「判断の尺度」となる基準でもある。なお、情報セキュリティの確保の観点からの監査に際しては、情報セキュリティ管理基準の活用が望ましいとされている。

システム管理基準を分離した「システム監査基準」は、システム監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的としたシステム監査人の「行為規範」として位置付けられる。

システム管理基準の構成は、前文に続いて次のようになっている。

①情報戦略(47 項目)
②企画業務(23 項目)
③開発業務(49 項目)
④運用業務(73 項目)
⑤保守業務(19 項目)
⑥共通業務(76 項目)

２１．金融機関等のシステム監査指針

定義：金融機関等がシステム監査を実施する場合に参考となる手引き・参考書として活用されているものである。1987 年、（財）金融情報システムセンター（The Center for Financial Industry Information Systems=FISC、別掲参考 URL 参照）によって作成され、2000 年７月、大幅に改訂された。

解説：この新しい指針の構成は、以下のとおりである。なお、第１部は７ページ、第２部は 40 ページである。第３部のチェックポイント集も大部で、要点項目ごとに、①リスクは何か、②誰が、何をコントロールするのか、③どのようにコントロールするのか を

記述した上で、大項目、小項目に別れてチェックポイントと関係資料の例示がある。

第１部　エグゼクティブサマリー

第２部　フレームワーク

　第Ⅰ章　システム監査の基本概念

　第Ⅱ章　システム監査の実践

第３部　チェックポイント集

　１　情報システムの計画と管理

　２　情報システムリスクの管理

　３　情報セキュリティ

　４　システム開発

　５　システム運用

　６　システム利用

　７　入出力等の処理

　８　ＥＵＣ

　９　ネットワーク

１０　システム資産・資源管理

１１　外部委託

１２　コンティンジェンシープラン

１３　ドキュメンテーション

　用語の注釈　　付録

２２．システム監査企業台帳

定義：システム監査を組織体の外部に委託する場合に参考にできるよう「システム監査企業に関する規則」（1991.3 制定）により経済産業省に登録された「システム監査企業台帳」が毎年作成されている。

解説：台帳を閲覧できるところは、従来は同省情報処理振興課、各地通産局機械情報産業課、都道府県立図書館、全国の商工会議所等であったが、現在は Web で公開されている。現在 90 社前後の企業が登録されているが、それぞれ「企業概要」、「システム監査の実績」、「監査従事者の概要」、「システム監査の得意分野、特色」等が記載されている。

なお 2003 年より情報セキュリティ監査を実施する企業の任意登録制度として「情報セキュリティ監査企業台帳」が創設されている。

２３．金融検査マニュアル

定義：金融機関等の法令等遵守を含むリスク管理態勢を検査官が検証していく際に必要となる検査の基本的考え方と具体的着眼点を整理した「金融検査官の手引書」である。金融庁では、信用、市場性、流動性、事務、システムなどの各種のリスクに対応した検査マニュアルを用意しており、システムリスクについては「システムリスク管理態勢の確認検査用チェックリスト」がある。

解説：チェックリストは検査官用の手引書の位置付けであるが、金融機関等では自己責任原則の下、このチェックリストを踏まえて更に詳細なマニュアルを自主的に作成し、業

務の健全性、適切性の確保に努めることが期待されている。
「システムリスク管理態勢の確認検査用チェックリスト」の確認検査項目を列挙すると、Ⅰ.リスク管理に対する認識等、Ⅱ.適切なリスク管理態勢の確立、Ⅲ.監査及び問題点の是正、Ⅳ.企画・開発体制のあり方、Ⅴ.体制の整備、Ⅵ.外部委託管理、Ⅶ.防犯・防災・バックアップ・不正利用防止　となる。このうち上記Ⅲの冒頭の記述を参考に例示する。

Ⅲ．監査及び問題点の是正

１．内部監査

(1)内部監査部門の体制整備

①システム部門から独立した内部監査部門が定期的にシステム監査を行っているか。

②内部監査部門は、システム関係に精通した要員を確保しているか。
また必要に応じてシステム監査とシステム以外の監査を連携して行うことができる体制になっているか。

(注)「しているか」とあるのは、全ての金融機関に対しミニマム・スタンダードとして求められる項目である。

２４．監査目的

定義：監査を実施することによって達成しようとする事項または状態。

解説：監査目的とは、一つまたは複数の『監査テーマ』への取り組みを通し、その監査で達成しようとする事項または最終的な状態をいう。すなわち、監査目的は、監査実施を通し達成しようとする直接的事項の他、監査を実施し、指摘をして、その改善を通して最終的に到達しようとする状態を示す場合もある。

監査目的は、当該監査活動の意義を示し、全ての監査活動の拠り処となる。そして明確な監査目的は、監査活動を一貫したものとする。

例えば、企業経営において戦略的な情報システムの活用を志向する企業では、「当社情報システムは経営に役立っているかを確かめる」、又は「当社情報システムを経営に役立たせる」などが監査目的の一例である。

監査目的は、監査実施に先立ち、監査を行おう、または監査を受けようと決める人（監査実施の意思決定者）がその内容を決定する。

監査目的から必然的に『監査対象』が導かれ、また、監査目的を基に『監査テーマ』が決定される。

監査目的は、その内容をより明確にするため、その内容をブレイクダウンし具体化した「監査目標」により補足される場合もある。例えば、監査目的が「当社情報システムは経営に役立っているかを確かめる」の場合、「現状の管理会計システムは経営に役立っているかを確かめる」などが監査目的を補足する監査目標の一例である。

２５．監査テーマ

定義：『監査目的』実現のために、何処に焦点をおき監査するかを表した、具体的な監査の主題。

解説：監査テーマとは、『監査目的』に基づき定められた、その監査で具体的に評価しよ

うとする監査の主題である。そして、監査テーマが、監査人が監査報告書において意見表明する具体的ターゲットとなる。
例えば、『監査目的』が「当社情報システムは経営に役立っているかを確かめる」の場合、「管理会計システムの安全性／有効性を確かめる」「管理会計システムは、タイムリーかつ適切な情報を経営者に提供できているかを確かめる」などが監査テーマの一例である。
監査テーマは、監査実施に先立ち、監査実施意思決定者の意向、及び監査人が行う事前調査などに基づいて、監査人がその内容を検討し、監査実施意思決定者の了承を得て決定される。
監査テーマは、『監査範囲』、『監査項目』、『監査要点』設定の主要な要件となる。
『監査計画』の内、『中長期計画』、『基本計画』においては、その期間に実施する監査において重点を置く『監査テーマ』を「重点監査テーマ」として明確化する場合もある。

２６．監査対象

定義：『監査目的』達成のために、『監査手続』の適用範囲となり得る対象。

解説：監査対象は、『監査目的』から必然的に導かれる、『監査手続』の適用範囲となり得る全対象を意味し、その切り口は、業務、システム、組織、人、物、場所など、『監査目的』によって様々である。
例えば、『監査目的』が「当社情報システムは経営に役立っているかを確かめる」の場合、経営者、経営戦略・情報戦略、計画中・稼動中の情報システム、情報システム部門、情報システムの利用者などが監査対象の例である。
監査対象は、『監査手続』の適用範囲となり得る全対象を意味し、監査人は、監査対象の中から、『監査テーマ』、及びスケジュール、投下可能資源（人、もの、金など）等の制約条件も考慮して『監査範囲』を決定する。

２７．監査範囲

定義：『監査対象』のうち、『監査手続』を適用する範囲。

解説：監査範囲は、『監査対象』の一部または全部であり、『監査テーマ』への取組みのために、監査人が必要と判断した、『監査手続』の適用範囲である。
監査範囲は、監査人が、『監査テーマ』、及びスケジュール、投下可能資源（人、もの、金など）等の制約条件も考慮し、『監査対象』の中から抽出する。
例えば、『監査対象』が「経営者、経営戦略・情報戦略、全情報システム、情報システム部門、情報システムの利用者」で、『監査テーマ』が「管理会計システムは、タイムリーかつ適切な情報を経営者に提供できているかを確かめる」の場合、利用者としての経営者（経営企画部門）、情報システム部門が遂行する開発・運用業務、管理会計システムなどが監査範囲を構成する例である。

２８．監査項目

定義：『監査範囲』の中から抽出された、『監査手続』が適用される個々の対象。

解説：監査項目は、『監査テーマ』への取組みのために、『監査範囲』の中から監査人によ

って抽出された、『監査手続』を適用する個々の対象である。
例えば、『監査テーマ』が「管理会計システムは、タイムリーかつ適切な情報を経営者に提供できているかを確かめる」で、『監査範囲』が「利用者としての経営者（経営企画部門）、情報システム部門が遂行する開発・運用業務、管理会計システム」の場合、利用者である経営企画部門の管理会計システムに対する評価･意見、管理会計システムのシステム運用実態、管理会計システムのシステム設計書などが監査項目の例である。
システム管理基準に規定された各項目見出しは、一般的な監査項目を示したものといえる。

２９．監査要点

定義：『監査項目』について、評価する内容。

解説：監査要点は、『監査テーマ』への取組みのために、『監査項目』について、監査人が評価、確認する内容であり、その監査における、『監査項目』の判断の尺度である。
例えば、『監査テーマ』が「管理会計システムは、タイムリーかつ適切な情報を経営者に提供できているかを確かめる」で、『監査項目』が「管理会計システムのシステム設計」の場合、「システム設計書はユーザの承認を受けているか」などが監査要点の一例である。
システム管理基準に規定された小項目は、一般的な監査要点を示したものといえる。
システム監査の実務では、『監査項目』とその判断の尺度（『監査要点』）とを合わせて『監査項目』と表現する場合もある。しかし、『監査項目』と『監査要点』はその内容に本質的差異があるので、両者を『監査項目』と『監査要点』に区分し定義することが、監査の構造、監査の理論体系を明確に整理する上で有効といえる。

３０．監査手続

定義：監査人が、『監査要点』に対する合理的な評価、結論を得るために、『監査項目』に対して監査技術を選択し、適用する手順。

解説：監査手続とは、監査人が、『監査要点』に対する合理的な評価、結論を得るために、その十分な証拠の収集を目的として『監査項目』に対して行う、監査技術の選択、及び適用の具体的手順である。
監査手続では、『監査要点』に関する合理的な結論を得るために監査技術を選択し、その監査技術を『監査項目』に対しいつ、誰が、どのようにして、またどの程度適用するかなどの具体的適用手順が明らかにされる。
例えば、『監査項目』が「管理会計システムのシステム設計」で、監査要点が「システム設計書はユーザの承認を受けているか」の場合、管理会計システムのシステム設計書の査閲により、ユーザの承認の記録を確認する、あるいは、ヒアリングによりユーザ部門の責任者に管理会計システムのシステム設計書の承認を確認するなどが監査手続の例である。

３１．監査計画

定義：『監査目的』を有効かつ効率的に達成するために立てられた、監査実施の計画。

解説：監査計画は、『監査目的』を達成するために監査を有効かつ効率的に行うための計画である。

監査計画は、一般に期間計画と『個別計画』に分けられ、期間計画は、『中長期計画』および『基本計画』（年度計画）に分けられる。

監査計画は、監査人が立案し、監査計画書として文書化され、監査依頼者の了承を得て決定される。

３２．中長期計画

定義：中長期の経営計画および情報化計画と対応した、数年間を見通した監査の期間計画。

解説：中長期計画は、『監査計画』の内の期間計画の一つに位置付けられる。

中長期計画は、３～５年を展望した『システム監査』の実施方針、及び実施計画であり、監査対象組織体の中長期経営計画および中長期情報化計画と連動し、中長期的視点から情報システムのリスクに対するコントロールが、適切に整備・運用されているかを監査する計画である。

『中長期計画』への主な記載事項は、当該期間における『監査目的』、重点監査テーマ、『監査対象』（必要により『監査範囲』）、監査スケジュール（優先順位）、概算予算、育成計画を含めた監査要員計画、品質管理方針等が挙げられる。

３３．基本計画

定義：『中長期計画』を基にした、当該年度の監査の期間計画。

解説：基本計画は、『中長期計画』に基づき、具体化された当該年度の監査年間計画である。

主な記載項目は、当該年度における『監査目的』、重点監査テーマ、『監査対象』（必要により『監査範囲』、『監査項目』、『監査要点』）、監査スケジュール、予算、要員計画（実施体制）、品質管理計画等が挙げられる。

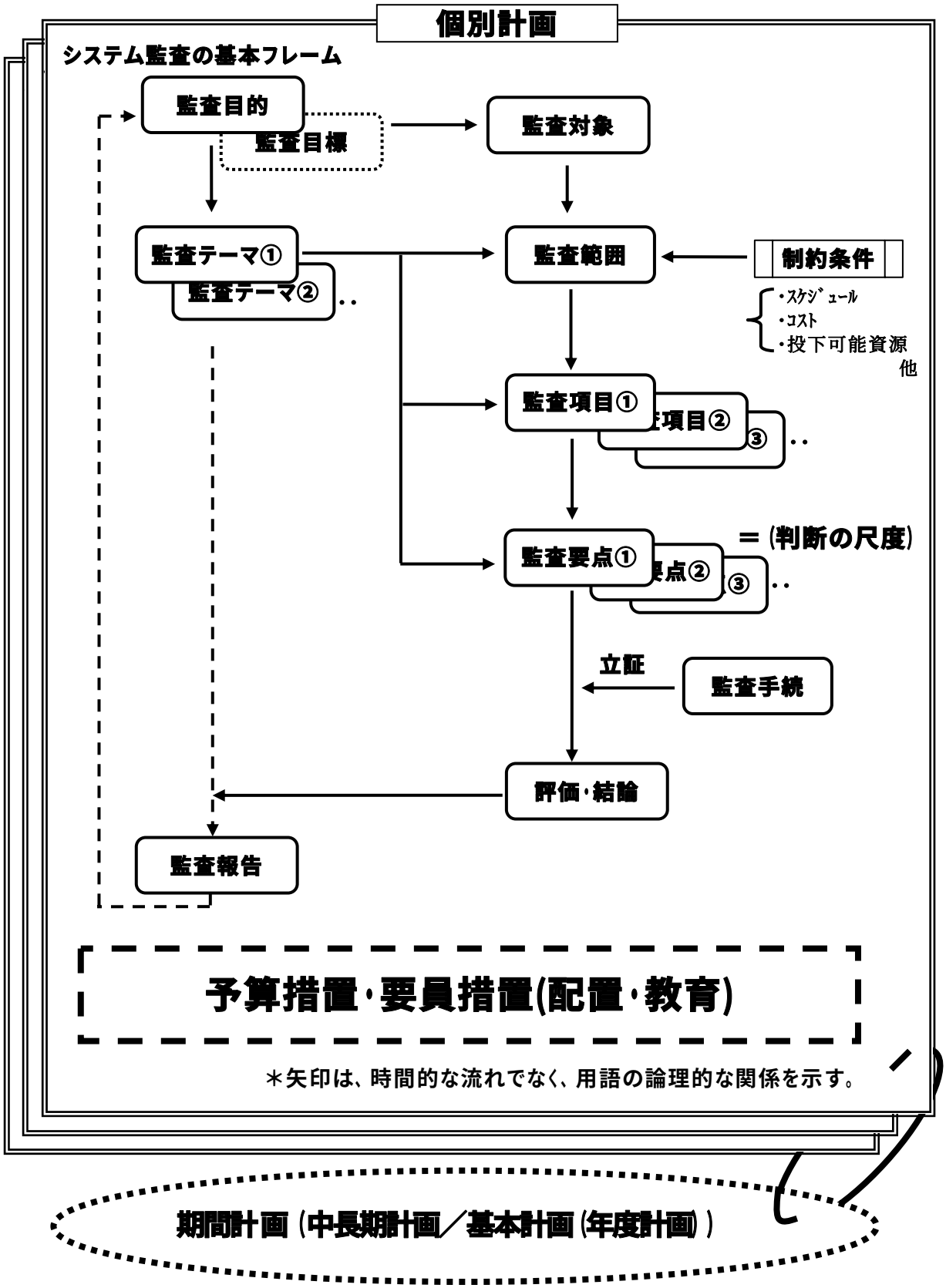
３４．個別計画

定義：『基本計画』を基に実施する、個々の監査の計画。

解説：個別計画は、期間計画（『中長期計画』、『基本計画』）に基づき実施する個々の監査の計画である。個別計画は、その監査の規模、複雑さにより更に具体化した実施計画に展開される場合もある。

個別計画は、個々の監査活動の拠り所となる計画であり、主な記載項目は、当該監査の『監査目的』、『監査テーマ』、『監査対象』、『監査範囲』、『監査項目』、『監査要点』、『監査手続』、監査スケジュール、予算、実施体制、品質管理手法等が挙げられる。

システム監査に関わる基本用語の関係概念図



３５．システム監査規程・マニュアル

定義：システム監査人がシステム監査を実施するに当たって、必要とするすべての規定や手順書類。

解説：システム監査マニュアルは、システム監査の品質向上や効率性向上、システム監査人の育成のために、有効である。

監査マニュアルとしては、以下のものが挙げられる。

・システム監査規程
・システム監査実施要領
・システム監査報告要領
・システム管理基準
・チェックリスト
・各種ドキュメントフォーム
・システム監査ツール使用マニュアル 等

監査マニュアルの記述内容としては、以下の項目が挙げられる。

・システム監査の目的
・システム監査の対象（組織、業務、情報資産等）
・システム監査人の役割、責任、権限
・システム監査人の資格要件、教育、訓練
・システム監査人の倫理規定
・システム監査計画書の作成基準
・システム監査実施基準
・システム監査調書の作成基準
・システム監査報告書の作成基準
・システム監査結果のフォローアップ
・システム監査人の判断の尺度としてのシステム管理基準
・他監査との調整指針
・関連法制度、基準　等

３６．監査証拠（audit evidence）

定義：システム監査報告書に記載する監査意見を立証するために必要な事実。

解説：監査証拠は、監査調書として実在するものであり、物理的証拠、文書的証拠、文書化された口頭的証拠、分析的証拠に大別される。

JIS Q 19011:2003 では「監査基準、に関連し、かつ、検証できる、記録、事実の記述又はその他の情報。監査証拠は定性的又は定量的なものがあり得る。」と定義している。

（補足）監査基準（audit criteria)：一連の方針、手順又は要求事項

システム監査人は、監査テーマを立証するために監査対象に監査技術を選択し適用し、監査証拠を入手する。監査証拠とは、システム監査人の観察結果、インタビュー結果の記録、収集した資料、監査テスト結果等のことである。監査テーマを立証するためには、十分な監査証拠が必要である。十分な監査証拠の要件としては、妥当性、正当性、適切性、有効性が要求される。

・妥当性とは、監査対象に精通した監査人であれば、同一の結論に到達するほどに、事実に基づき、妥当で説得力のあること
・正当性とは、依存できる情報で、しかも適切な監査技法の実施を通して、最も達成可能なこと
・適切性とは、監査による発見事項や勧告を裏付け、かつ監査テーマと合致していること
・有効性とは、組織体がその経営目標を達成することに貢献すること

監査証拠は、物理的証拠、文書的証拠、文書化された口頭的証拠、分析的証拠に大別されるが、それぞれは以下のとおりである。

ａ．物理的証拠とは、監査人が直接観察した事実。

ｂ．文書的証拠とは、議事録、レビューシート、設計書、テスト結果、ログリスト等、書面で残っている書類。監査人によって収集される最も一般的なタイプの証拠。書類での証拠には内部あるいは外部のものがある。また、文書的証拠の形態としては、紙や電子媒体などが挙げられる。

ｃ．文書化された口頭的証拠とは、システム監査人の質問等に対する、被監査部門の書面または口頭での回答を文書化し確認したもの。

ｄ．分析的証拠とは、物理的証拠や文書的証拠などの関連性を分析したもの。

３７．監査証跡（audit trail）

定義：各コントロール機能が情報システムの信頼性、安全性、効率性、有効性の確保に結びついていることを事後に実証するための手段。情報システムに関するさまざまな事象の発生から最終結果に至るまでの過程およびその逆方向の追跡ができる仕組み。

解説：監査証跡とは、情報システムおよび情報システムを運用する手続きが持っている各コントロール機能が、情報システムの健全性を確保することに有効であることを、事後に双方向で追跡し確認できる仕組みのことである。監査証跡から得られるものは時系列的な監査証拠になりうる。

具体的には、以下のものがある。

・トランザクション証跡
　監査対象の情報システムの取引を選び出し、データ処理内容と処理結果の相互関連を追跡できる一連の仕組み。
・アクセス証跡
　システム資源へのアクセスに関して因果関係を事後に追跡するための仕組み。

システム監査人は、監査証跡の十分性、正当性、適切性、有効性を確認した上で、監査証跡により各種コントロール機能の有効性を確認する。

３８．監査調書

定義：システム監査において、監査人が作成し、または収集した資料。

解説：監査調書は、監査報告書を作成する基礎資料、立証するための資料となる。

システム監査人は、システム監査の計画立案もしくは監査契約締結から、監査業務の遂行を経て、監査報告書の作成に至る全過程において、監査証拠となりうる資料を作成・

入手し、必要に応じて記録・編集して、監査調書を作成する。
システム監査人が、監査調書を作成する目的は、次のとおりである。
・監査業務の品質管理に役立てる。
・監査責任者による監査担当者の業務を指導監督するのに役立てる。
・次期以降の監査の合理的な実施を図るための資料として役立てる。
監査調書は原則として監査を実施した監査人が所有するが、被監査会社の許可なくして、その全部又は一部を他人に開示してはならない。

３９．準拠性調査

定義：経営管理者によって設定されたコントロール（規定およびマニアル類に規定されている事項）の整備および運用状況の検証。

解説：システム監査における準拠性調査では、情報システムの運用手続きやプログラムの処理の妥当性を内部統制の観点より調査する。
また、準拠性調査の技法としては、以下のものがある。
・コンピュータを利用しない場合
①証拠の調査
記録、書類、報告書等のように、特定のコントロールが正しく適用されたことを示す証拠を調査すること。
②再実行
ある種の判断が行為の基礎となっている場合に、結果が同じになるかどうかを確認すること。
③視察
実際の業務の実施されている現場に行き、内部統制が守られていることを確かめること。
・CAAT を適用する場合
①テストデータ法
②ITF 法
③並行シミュレーション法
④汎用監査ソフトウェア法
⑤コード比較法
⑥監査モジュール法
準拠性テストの実施に CAAT を適用する場合の留意点は、以下のとおりである。
－情報システムの処理フローを十分分析し、監査目的、コントロール、実証性テストによる監査手続との関連、監査リスク等を考慮して、対象とする運用手続き、プログラム処理手続きを決定する。
－対象とする運用手続き、プログラム処理手続きに対しては、さらに運用フロー、システムフロー等を参照のうえ分析し、対象とすべき運用手続き名、プログラム名、マスターファイル名、取引ファイル名、入出力帳票、画面等を明確にする。
－単純なプログラム処理の場合は、監査人自らプログラムを作成し、並行シミュレーションにより監査するのが効率的である。

－複雑なプログラムの場合は、種々の技法を複合的に利用する。

４０．実証性調査

定義：情報システムの生成するデータ、意思決定者の利用度、情報システムが使用している資源等の直接的な検証。

解説：システム監査における実証性調査では、監査の効率性、経済性、正確性の観点より調査する。

また、実証性調査の技法としては、以下のものがある。

・コンピュータを利用しない場合

①再実行

ある種の判断が行為の基礎となっている場合に、結果が同じになるかどうかを確認すること。

②実査

記録された最終結果と現状の物理的な比較をすること。

③証憑突合

記録された最終結果より、その起因となった取引、トランザクションを示す伝票類にさかのぼり突き合せること。

④構成分析

最終結果を分類、集計することによって、その内容の理解を深めること。

⑤照合調整

本来一致すべき２つの数字の間の違いを明確にし、説明すること。

⑥カットオフテスト

取引、トランザクションが適切な期間に記録されているか判断するために書類等を検査すること。

・CAAT を適用する場合

①汎用監査ソフトウェア法

②ユーティリティ・ソフトウェア法

③専用監査プログラム法

実証性テストの実施に CAAT を適用する場合の留意点は、以下のとおりである。

－監査目的にあった明細の記録されているファイルを確保する。

－ファイルとして入手したデータの合計値を確定する。

－原始データのサンプリング自体の正確性と妥当性を、その証拠能力に応じて適時にテストする。

－上記のステップで信頼性が確認されたファイルのデータを監査人の汎用監査プログラム等を用いて、並行シミュレーションなどにより実行する。

－例外データ、危険項目等の以上項目のみを論理的に抽出し、効果的な監査を実施することができる。

－計算、突合せ等の再実行は、全データに対して容易に実施することができる。

４１．精査

定義：監査目標ごとに監査対象項目の全件に対して監査手続を適用する監査方法。精細に監査すること。

解説：精査とは、特定の監査手続の実施に際して、監査対象の母集団からそのすべての項目を抽出して、それに対して監査手続を実施することである。

監査対象項目を全件監査することは、かなりの手間がかかるため、期間と労力を必要とする。個別計画を立案する際、精査で監査を実施するのか、試査で監査を実施するのか決めておく必要がある。

４２．試査

定義：監査目標ごとに監査対象項目の一部に対してのみ監査手続を適用し、その結果に基づいて監査対象項目全件の状況を推定する監査方法。

解説：試査とは、監査対象の一部を抽出して検討し、その適否をもって監査対象全体の適否を推定的に立証する方法である。試査の範囲を決定するためには、立証すべき監査テーマを設定し、入手すべき証拠資料の範囲を決定する必要がある。

試査の範囲を決定する方法としては、以下のものがある。

・サンプリングによる試査

母集団の特性を代表するサンプルに対する監査手続の結果から、母集団全体の一定の特性を推定して母集団に関する結論を得る方法である。

・特定項目抽出による試査

母集団に含まれる特定の性質を有する項目を識別して抽出し、これに対して監査手続を実施する方法である。

・経験的試査

監査人が、内部統制の状況や監査対象の重要性、監査上の危険性、過去の実績等を考慮した経験的判断により、試査の範囲を決定し、監査手続の適用の結果を評価する方法である。

・統計的試査

統計理論に基づいて決定されたサンプル数を無作為に抽出して検査し、サンプル結果を確率論に基づいて評価する方法である。

４３．実査

定義：監査対象である情報システムのドキュメント、プログラム、データ、要員などの実際の存在、数量、使用状況等を確認する手続き。

解説：実査は、会計分野の専門用語であり、その意味は、企業の現物のある資産について、実際の存在、数量、使用状況等を確認する手続きのことである。一般には、現金や受取手形等がその適用範囲であるが、棚卸資産や有形固定資産等にも必要に応じて適用される。

システム監査の観点で見ると、情報資産についての実際の存在、数量、使用状況等を確認する手続きということになる。

４４．予備調査

定義：監査対象の実態を明確に把握する調査のことで、本調査の円滑かつ効率的な実施を可能にするために行う事前調査。

解説：予備調査の実施手順は、以下のとおりである。

①監査対象の現状分析

監査対象業務やシステムの実態を次の点に留意し、現状分析する。

・監査対象組織、各種規定類等
・監査対象業務やシステムの範囲
・関連業務やシステムとのインタフェース
・処理の流れ、データの流れ
・運用手続きとコンピュータ処理のインタフェース

②問題点の洗い出し

監査テーマに対する被監査部門や組織体が目標とするレベルと現実のレベルとのギャップを識別して、想定される問題点を洗い出す。この際、考えられる原因や改善策の実現可能性、費用対効果は考慮しない。問題点の分類・整理にとどめる。

③本調査の見直し

個別計画書で計画した本調査の範囲及び手続きを見直す。

予備調査を実施する上での留意点は、以下のとおりである。

①目標レベルの明確化
②潜在的問題点に対する注意
③本調査での監査手続きの詳細化及び具体化

４５．本調査

定義：監査目的に則して対象業務の実態を調査・分析・検討すること。個別監査計画の監査項目を順次監査し、監査の項目、監査手続き、問題点、監査実施などを監査調書に記録する。

解説：本調査の実施手順は、以下のとおりである。

①現状の確認

予備調査で得た心証について現状はどうかをシステム監査人自ら現場に行き確認する。その際、新たな問題点の存在の可能性について配慮する必要がある。

②監査証拠の入手

個別計画書に従って、予備調査で得た心証を裏付ける資料を収集する。監査目標を達成するために必要な資料のみを入手し､不要な資料は入手しないようにする。また、資料の入手に際しては、可能な限り被監査部門の協力を得る。

③証拠能力の評価

入手した監査証拠は、当該監査目標を立証するために必要な証拠能力を備えているか否かを評価する。証拠能力が不十分な場合、代替的な監査証拠の転用あるいは追加的な監査証拠の入手を検討する必要がある。

本調査を実施する上での留意点は、以下のとおりである。

①積極的な現地調査
②被監査部門との十分な調整
③個別監査部門の適時見直し
④監査調書の作成

４６．評価・結論

定義：調査結果を踏まえて、監査対象の実態が監査目的に則して妥当であるか判断すること。

解説：本調査終了後、調査結果を踏まえて評価する。評価をより正確に行うため、システム監査人は、監査結果を被監査部門との意見交換を通じて確認した後、自らの判断基準に基づいて最終結論を下す。

４７．チェックリスト法

定義：システム監査人が作成したチェックリスト（質問書）に対して、特定者より回答を求めること。（システム監査技術者育成カリキュラム）

解説：チェックリストは、チェック項目に対する有無のみを確認する場合に使用し、質問書については、チェック項目の有無も含めて質問項目に対する回答を要求する場合に使用する。

個別の監査対象に対して、そのまま合致するチェックリストはないため、当該監査対象に精通したシステム監査人がカスタマイズする必要がある。

システム監査の各関係諸団体から公表されている基準・ガイドライン（システム監査基準、FISC のシステム監査指針等）を利用して、チェックリストを作成する場合が多い。

システム監査人には、適用対象組織体の業種、企業規模およびシステム規模等により、監査の目的を考慮する必要があり、監査対象の実態に適合するような質問内容・範囲に調整する能力が要求される。

４８．ドキュメントレビュー法

定義：特定の情報を収集するために、関連する資料および文書類をシステム監査人が自ら通査すること。（システム監査技術者育成カリキュラム）

解説：システム監査人は、事前準備の際、被監査部門におけるドキュメントの整備状況を確認して、どのドキュメントが利用可能かを明確に把握しておく必要がある。

ドキュメントレビューの目的は、監査テーマについての状況を調査する監査証拠を入手することである。

また、ドキュメント管理の監査として、ドキュメント（仕様書・変更依頼書等）の内容は、常に最新の状態を反映しているかを調査し、文書管理状況（原本の保管）を確認する。

４９．突合・照合法

定義：関連する記録間を突き合わせること、記録された最終結果をその起因となった事象を示す原始データまで遡り突き合わせること。（システム監査技術者育成カリキュラム）

解説：関連する複数の証拠資料を突合せる技法、記録された最終結果をその起因となる事象を示す原始データまで遡って突き合わせる技法等である。
なお、突合せ対象の関連する記録が、相互に同期していることを確認しなければならない。（プルーフリストによる照合、入力データと出力結果の照合等）

５０．現地調査法

定義：システム監査人が被監査部門へ赴き、そこでの作業状況を、自ら調査すること。（システム監査技術者育成カリキュラム）

解説：システム監査人が自ら監査対象の現状を確認し、理解することが重要である。
現地での調査は、システム環境（センター、事務所、工場等）における対象業務の始点および取引の発生源から開始し、業務処理フローをトレースすることが効果的である。現地の業務の妨げにならないような注意が必要であり、スケジュール調整をする。

５１．インタビュー法

定義：特定の事項を立証するために、システム監査人が直接、特定者に問い合わせ回答を入手すること。（システム監査技術者育成カリキュラム）

解説：システム監査人が監査対象の実態を調査するためには、インタビューにより必要な情報が入手可能である。効率よく必要十分な監査証拠を入手するため、あらかじめインタビュー対象部門・対象者を十分に検討し、質問内容を吟味しておく必要がある。
インタビューでのチェックリストの利用、インタビューに代わるアンケート調査、現地調査でのインタビュー等、各技法の適切な組み合わせを検討する。

５２．コンピュータ支援監査技法

定義：監査業務の過程において、コンピュータを使用する技法を「コンピュータ支援監査技法（Computer Assisted Audit Techniques：CAAT)」という。

解説：コンピュータを利用したシステム監査技法は、システム開発のテスト等に利用している技法であり、システム監査人側においても、コンピュータ内部処理の正確性をチェックするために利用する技法である。
なお、技法によっては、システム監査時に利用する技法と、システム開発の段階で、あらかじめツールをシステムに組み込むことが望ましい技法とがある。

５３．ユーティリティ・ソフトウェア法

定義：ユーティリティ・ソフトウェア法は、システム開発・運用・保守業務の支援のため、主としてメーカーから提供されるソフトウェア等を活用する技法である。

解説：監査目的によっては、ユーティリティ・ソフトウェア（テストデータ生成、テキストエディタ、ライブラリ・コピー、レポート生成プログラム等）およびアクセス管理ソフトウェア等を活用する技法がある。
しかし、ユーティリティ・ソフトウェアを使用するためには、システム監査人に技術的に高いスキルが要求される。

５４．テストデータ法

定義：準備されたテストデータを監査対象プログラムに投入し、期待した結果が出力されるか否かを確認する方法。（システム監査技術者育成カリキュラム）

解説：システム監査人が事前準備したテストデータを監査対象のプログラムに投入し、期待した結果が出力されるか否かを検証して、プログラム処理過程の正確性を確認する。

特定機能に限定したテストおよび総合的な計算機能・コントロール機能のテスト等、システム監査人の判断により範囲を限定することができる。

また、テストしたシステムが実際に稼動しているものと同一であることを確認する必要がある。

５５．汎用監査ソフトウェア法

定義：汎用監査ソフトウェアは、監査対象ファイルの検索、抽出、計算等、システム監査上使用頻度の高い機能に特化した、しかも非常に簡単な操作で利用できるソフトウェアのことであり、これは当ソフトウェアを利用する方法である。（システム監査技術者育成カリキュラム）

解説：汎用監査ソフトウェア（監査プログラム）は、システム監査人の指定した機能に従って、ファイルからデータを抽出して演算・比較を行い、レポート作成の機能を有し、汎用監査プログラム・パッケージとして開発されている。

提供される機能には、ファイルのアクセス・再編成、データの選択、統計的サンプリング、演算・比較（定量的分析）、層別分類と詳細分析、ファイル処理（整理）、レポート作成等がある。

５６．監査モジュール法

定義：監査対象ファイルよりシステム監査人が指定した抽出条件に合致したデータをシステム監査人用ファイルに記録し、レポートを出力するモジュールを、本番プログラムに組み込む方法。（システム監査技術者育成カリキュラム）

解説：監査モジュールは、監査用のモジュールを組み込み、監査人がパラメータで指定した抽出条件に合致したデータが通過する際に、このデータを抽出して、システム監査人用ファイルに記録するプログラムである。

５７．ＩＴＦ法

定義：監査対象ファイルの中にシステム監査人用の口座を作り、その口座に各種の操作をして処理の正確性を確認する方法。（システム監査技術者育成カリキュラム）

解説：ITF 法（Integrated Test Facility：統合テスト法）は、別称ミニカンパニー法とも呼ばれ、システムに架空の口座（ミニカンパニー）を設け、実稼動中にテストデータを流し、その結果をあらかじめ手作業にて得られた正しい結果と照合するという方法であり、オンラインシステムをテストする技法である。

実稼動中にテストデータを実データと共に入力して処理するため、いずれかの段階でテストデータを除去する必要がある。テストデータが業務処理および記録等に影響を与えないように留意する。

５８．並行シミュレーション法

定義：特定の監査目的を検証する機能を持ったプログラムを、システム監査人側で独自に準備し、それと監査対象プログラムに対して同一のデータを入力して、両者の実行結果を比較すること方法。（システム監査技術者育成カリキュラム）

解説：並行シミュレーション法（Parallel Simulation）は、アプリケーション・プログラムのすべての機能をテストするのではなく、システム監査人が監査目的のために、必要と認める機能のみを対象としている。

この技法はプログラム機能（入力確認手続、処理論理、コントロール等）をシミュレートするため、テスト用プログラムを用いて本番データを処理する。

本番の適用業務システムをシミュレートしたテスト用プログラムの作成が必要となる。

例として、在庫量が基準値以下になると、自動発注するような取引の自動生成ロジックのテストに効果的である。

５９．コード比較法

定義：あらかじめシステム監査人によって検証されたプログラムと監査対象プログラムとを、コーディングのレベルで１行づつ比較して、監査対象プログラム改竄の有無（ロジックの正確性）を確認する技法。（システム監査技術者育成カリキュラム）

解説：コード比較（Program Code Comparison）法は、本番用プログラムを、監査用プログラムと比較して、その正当性を検討する技法である。

ソース・コードあるいはオブジェクト・コードについて行なわれるが、使用中のプログラムとドキュメンテーションの間に差異がないかどうかの調査が可能である。

コード比較には、ソース・コードの２世代間比較、本番用オブジェクト・コードの２世代間比較、本番用オブジェクト・コードと監査用オブジェクト・コードの同一世代間比較、本番用オブジェクト・コードと監査用オブジェクト・コードの２世代間比較の４形態がある。

６０．ペネトレーションテスト（penetration test）

定義：無権限アクセス（不正アクセスを含む）からシステム資源が守られていることを確認するため、一般ユーザのアクセス権限あるいは無権限で、テスト対象システムへの侵入を試みる技法である。模擬（疑似）侵入テストともいう。

解説：システムの脆弱性を発見するには、非常に有効な技法である。専門会社に委託してペネトレーションアタックを行う際、外部システムへの不正アクセス、情報の漏洩等が発生しないよう事前に契約書を交わす必要がある。

６１．総合評価

定義：監査テーマに対する監査対象の状況についての、システム監査人の評価・結論の内容。

解説：『予備調査』、『本調査』で得た『監査証拠』を分析した結果として、『監査テーマ』に対する『監査対象』の状況についてシステム監査人が『評価・結論』としてまとめた内容であり、システム監査報告書の中に記載される。

評価には合理性、納得性、客観性、専門性が要求される。合理性は、適切な『監査手続』に基づいて十分な調査が行われていることによって得られる。納得性は、評価が明確な事実（監査証拠）に基づいて下されていることによって得られる。客観性は、明確な基準に照らして評価を行っていることによって得られる。さらに、専門性は、システム監査についての高い専門技術をもったシステム監査人が評価を行っていることによって得られる。

なお、評価・結論の内容を『監査依頼者』に報告するにあたっては、定性的な評価だけではなく、３段階あるいは５段階などの定量的評価も含めた方が、評価・結論の内容が明確に伝わり改善に結びつきやすい。

６２．指摘事項

定義：システム監査人が、『予備調査』および『本調査』の結果を踏まえ、自ら設定した合理的な判断基準に基づいて問題であると判断した事項。

解説：システム監査人は、『予備調査』および『本調査』を通じて入手した『監査証拠』を『監査目的』に照らして分析・評価し、その結果をシステム監査報告書にまとめて『監査依頼者』に報告する。システム監査人は、『監査証拠』を分析・評価した結果として、『監査対象』において問題であると判断した事項を、システム監査報告書に記載する。これが指摘事項である。

システム監査人は、『予備調査』および『本調査』の結果、『監査対象』において問題であると判断した事項は、小さな問題であっても指摘すべきである。小さな問題であっても、将来大きな問題に発展する可能性もあるからである。

ここでいう「問題」とは、監査計画で設定した監査基準と調査した結果とのギャップである。そして、定義にある「判断基準」には、次のようなものが含まれる。

・調査によって分かった事実がギャップに該当するかどかの判断基準
・ギャップを指摘事項にするかどうかの判断基準
・指摘事項を改善事項にするかどうかの判断基準
・改善事項を緊急改善と通常改善に切り分けるときの判断基準

定義で「自ら設定した判断基準」といっているが、監査実施組織が所属するシステム監査人の経験を集めて、監査実施組織としての判断基準を設けることは、判断の均質化が図れて有効である。

システム監査人は、システム監査報告書に指摘事項を記載するにあたって、以下の点に留意が必要である。

・問題であることの『監査証拠』による明確な裏付け
・被監査部門との意見交換による問題点についての事実誤認の排除と共通認識の確立

なお、監査テーマとは直接関係ない事項について、『予備調査』、『本調査』を通じてシステム監査人が知り得た事実のうち、システム監査人が『監査依頼者』に報告した方がよいと判断したことがあれば、補足意見という形でシステム監査報告書に記述して報告することがある。

６３．改善事項

定義：システム監査人が、『指摘事項』の中で改善が必要であると判断した事項。

解説：『指摘事項』をすべて改善しなければならないかというと、それは『監査目的』やその背景にある経営目的（経営戦略の実現、経営目標の達成、経営課題の解決）に基づいて判断する必要がある。システム監査人が、そうした判断によって改善が必要と判断した『指摘事項』が改善事項である。

システム監査人は、改善事項の指摘にあたって、被監査部門と改善の必要性についての共通認識をもつよう努めなければならない。また、改善事項に対して『改善案』を提示することも、システム監査人の重要な責務である。

６４．改善勧告

定義：システム監査人が、システム監査報告書に『改善事項』および『改善案』を記載し、『監査依頼者』に対して問題の改善を勧めること。

解説：システム監査人がシステム監査報告書に『改善事項』を記載するということは、その問題は現状のままで放置しておくことはできないと判断したということである。そして、改善勧告は、そのことを『監査依頼者』に伝え、『監査依頼者』から被監査部門に対する改善指示を勧めることである。

改善勧告によって、報告を受けた『監査依頼者』には改善実施の判断および改善指示の責任が、被監査部門には改善指示を受けて改善実施の責任が生じる。一方、システム監査報告を行ったシステム監査人は、被監査部門が行う改善活動に対する『フォローアップ』を行う必要がある。

システム監査人は、改善勧告および『改善案』の記載にあたっては、改善の実施を促進する明瞭、積極的かつ説得力のある記述に留意する必要がある。

６５．緊急改善

定義：『改善勧告』のうち、システム監査人が重大な問題であり、技術面・経済面から見た改善の実現可能性、改善にかかる投資対効果などを考慮した上で、速やかな改善実施が必要と判断した事項。

解説：『改善事項』を改善するためには、経営資源の投下が必要であり、すべての『改善事項』に対して同じ緊急度、優先度で改善を実施することは効率的ではない。システム監査人は、『監査目的』を踏まえ、『改善事項』の問題の大きさ（緊急性、重要性）を基本に、改善の実現可能性などを考慮した上で、緊急改善と『通常改善』に分けて、メリハリのある『改善勧告』を行う必要がある。

問題としてはそれほど大きくはないが、すぐに改善でき効果が期待されるものを緊急改善にして、改善実績を作るという方策もときには効果的である。

また、『改善事項』によっては、根本的な改善（恒久対応）には時間がかかるので通常改善とするが、問題としては放置できないので最低限の改善（暫定対応）を緊急改善とするということもあり得る。

６６．通常改善

定義：『改善勧告』のうち、システム監査人が『緊急改善』と判断した以外の事項。

解説：速やかに改善を実施する必要はないが、問題が存在していることは事実であり、計画を立てて改善を実施していく必要のある『改善事項』である。

重要性からいうと『緊急改善』に相当する問題であっても、改善に長期間あるいは多大な投資が伴うものは、通常改善として段階的改善を検討させることが現実的な場合もある。

６７．改善案

定義：『改善勧告』を行うに際して、システム監査人が考えた『改善事項』に対する改善方法の案。

解説：『改善事項』に対する改善方法を検討・策定し、『改善計画』にまとめることは、改善を実施する部門（通常は被監査部門）の責任である。システム監査人は、改善を実施する部門の改善活動に対する支援の一貫として、今までの経験に基づいて『改善事項』に対する改善方法の案を提示する。それが改善案である。改善案の立案にあたっては、システム監査人は、

・改善案の有効性（問題解決の効果の大きさ）
・改善案の実現可能性（技術的困難さ、改善を実施する部門の成熟度などを考慮）
・改善案の投資対効果

を考慮することも必要である。

６８．意見交換会

定義：システム監査報告書を監査依頼者に提出する前に、システム監査人と被監査部門との間で、システム監査報告書（案）の内容について意見を交換する場。

解説：意見交換会は以下の目的のために実施する。

・システム監査報告書（案）の内容について事実誤認がないことの確認
・システム監査報告書（案）の『指摘事項』、『改善勧告』、『改善案』に対する被監査部門の意見の聴取
・被監査部門としてシステム監査報告書（案）に記載して欲しい事項についての意見聴取

ただし、意見交換会はあくまでも被監査部門の意見を聞く場であり、システム監査報告書（案）のレビューを行う場ではないことに注意が必要である。被監査部門の意見を聞いた上で、システム監査人は自らの判断基準と責任において、システム監査報告書を完成させなければならない。

６９．監査報告（audit reporting）

定義：システム監査人がシステム監査の結果をシステム監査報告書にまとめ、『監査依頼者』に報告すること。

解説：監査報告の方法としては、『監査報告会』を開いて、システム監査人がシステム監査報告書に基づいて報告する方法が一般的である。場合によっては、『監査報告会』を開

かず、システム監査報告書を『監査依頼者』に提出することで監査報告とすることもある。また、『監査依頼者』に対する報告以外に、被監査部門の責任者に対する報告、被監査部門の関連部門の責任者に対する報告、監査役に対する監査報告など、組織体の状況や監査の目的に応じて、さまざまなケースがある。

７０．監査報告会

定義：システム監査人が、システム監査報告書に基づいて、システム監査の結果を『監査依頼者』に報告する場。

解説：監査報告会には、『監査依頼者』（民間企業であれば組織体の長、自治体であれば首長など）および CIO（情報統括役員）、被監査部門の責任者が出席するのが一般的である。監査報告会は短時間であること、出席し報告を受けるのが組織体の長や首長、上級管理者であることから、システム監査報告書を逐一報告するのではなく、重要なポイントに絞って報告することが有効である。そのために、システム監査報告書の重要な点をまとめた上級管理者向サマリ版を作成することは、よく採られる方法である。

７１．フォローアップ（follow-up）

定義：『改善勧告』に対する改善活動が『改善計画』の通りに行われるよう、システム監査人がシステム監査人の立場で支援・指導すること。システム監査基準では、「改善指導」という言い方をしている。

解説：システム監査は『監査報告』によって終了となるのではない。システム監査人が監査報告書に記載した『改善勧告』に対する改善が実施されてはじめて、システム監査を実施した意義が生まれる。

『改善勧告』に対する改善活動を計画・実施することは、改善実施部門の役割である。システム監査人は自らが行った『改善勧告』に対する改善活動が計画通りに実施されるよう、改善実施部門の改善活動の状況を定期的に確認し、改善実現のためにシステム監査人の立場で支援・指導する必要がある。システム監査人は、立場上、改善実施部門が行う改善活動に直接参加することはできないが、改善活動が計画通りに進んでいない場合、改善活動を円滑に進める方法を提案する、改善実施部門や関連部門の責任者に改善活動の円滑な実施について要請を行うといった行動はとることができる。これが、システム監査人の立場での支援・指導である。

ここでは、被監査部門と区別して改善実施部門という表現を採った。多くの場合、被監査部門が改善実施部門となるが、まれに、被監査部門以外が改善実施部門になることもある。

『内部監査』の場合には、監査部門がフォローアップ活動を行う。『外部監査』の場合には、一般的には『監査報告』までを外部監査企業と契約するが、フォローアップ活動を含めて契約し、外部監査企業が定期的なフォローアップ活動を行う方法もあり得る。しかし、多くは、組織体の中の然るべき部門（監査部門や経営管理部門など）が改善活動の状況を把握し、外部監査企業には次の監査の機会に前回の『改善勧告』に対する改善実施状況を含めて監査してもらうという方法が採られる。

７２．改善計画

定義：監査報告書に記載された改善勧告に対して、『監査報告』を受けた『監査依頼者』が改善指示を出し、その改善指示を受けた改善実施部門が改善の実施を計画すること。

解説：『改善勧告』に対する改善の実施には経営資源が必要であり、改善実施部門では、『改善勧告』の重要性・緊急性に加えて経営資源の状況も考慮した上で、『改善勧告』に対する改善実施の優先度を決定し、改善計画を策定する。

システム監査人は改善計画書を入手し、その妥当性を確認し、問題があれば改善実施部門に再検討を助言する。これも改善活動に対する支援・指導であり、『フォローアップ』の一環である。

最終的には、改善計画は改善実施部門の長、および組織体の長によって承認され、改善実施部門は改善計画に基づいて改善活動を実施する。

７３．改善措置

定義：『改善勧告』に対する改善策として、改善対象のシステムや業務プロセスなどに対して行われる変更。

解説：改善措置は、改善実施部門で検討・策定され、『改善計画』に盛り込まれる。改善実施部門は改善措置の検討・策定にあたって、システム監査人がシステム監査報告書に記載した『改善案』を参考にする。システムに対する技術的変更、システムを活用する業務プロセスや活用ルールなどの運用面の変更、組織体制や役割分担の変更などの改善措置が考えられる。

７４．改善報告

定義：改善実施部門が、『改善計画』に基づいて実施した改善活動の結果を報告書にまとめて報告すること。

解説：改善報告の方法としては、『内部監査』では、改善実施部門の責任者から直接、組織体の長に報告する方法と、一旦システム監査人が改善実施部門から報告を受ける方法がある。『外部監査』では、一般的には前者の方法だけである。

一旦システム監査人が改善報告を受ける場合には、システム監査人は改善報告の内容を確認し、改善報告書の内容に問題があれば、改善実施部門に再確認あるいは改善活動の追加実施を助言・指導する。さらに、システム監査人が改善結果について改善報告だけでなく、自ら確認する必要があると判断した場合には、『フォローアップ監査』を計画する。

７５．フォローアップ監査（follow-up audit）

定義：改善実施部門が行った改善活動の結果（改善状況）を、システム監査人が改めてシステム監査手続を用いて確認すること。

解説：フォローアッップ監査の手順は、システム監査の手順と同じである。ただし、『監査対象』および『監査項目』は『改善事項』に対する改善状況に限定する。それも、すべての改事項を対象にするのではなく、『監査手続』を用いて監査することが必要と判断したものだけを対象に実施する。

システム監査のプロセスとして、『監査報告』から６カ月後、あるいは１年後にフォローアップ監査を実施することを決めておくケースもある。この場合、改善実施部門はフォローアップ監査の実施時期を考慮して、『改善計画』を策定しなければならない。

７６．助言と保証

定義：「助言」は、システム監査の実施を通して、『監査対象』の改善のための指摘を行うことをいう。「保証」は、システム監査を実施した結果として、『監査対象』の状況について一定の保証を与えることをいう。

解説：システム監査の目的は、『監査対象』の『監査テーマ』についての状況を、『監査手続』を使用して調査し、改善すべき事項があれば指摘し改善につなげることである。これは「助言」に該当する。

最近の考え方として、システム監査人が監査結果として述べる意見・評価や『指摘事項』は、『監査対象』の状況について、第三者への開示を目的に一定の「保証」を与えるという考え方がいわれている。しかし、この場合の「保証」は、システム管理基準などに基づいて組織体として設定した監査基準、採用した『監査手続』、サンプリングで調査した中での「保証」であることに注意が必要である。

７７．監査依頼者

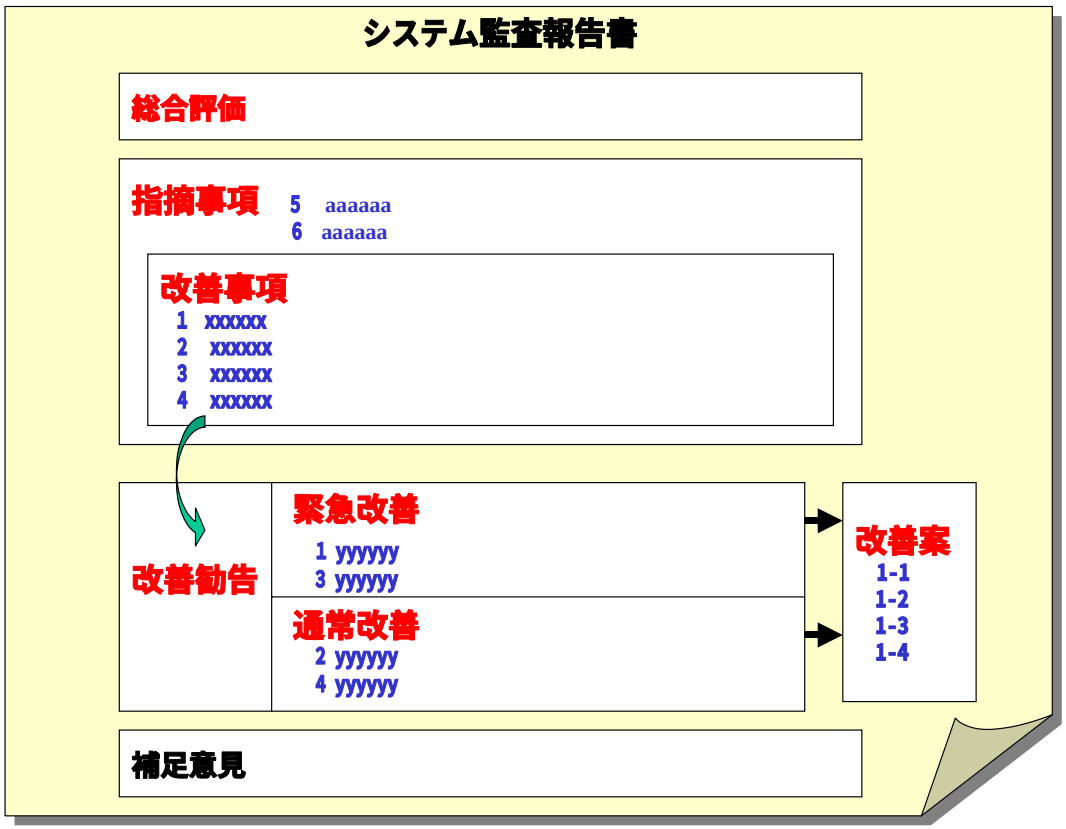
定義：システム監査の実施を依頼あるいは指示した者。

解説：『内部監査』の実施は組織体として決めるものであり、組織体の長（民間企業であれば社長、自治体であれば首長）の指示に基づいて実施される。その場合、組織体の長が監査依頼者となる。

『外部監査』は、組織体の長が監査法人やシステム監査専門企業に依頼して実施する。この場合、組織体の長が監査依頼者となる。

また、実態としては、組織体の長から監査実施の権限を委譲された CIO や事業部門責任者が監査依頼者となることもある。

＜＜監査報告についての用語体系図＞＞



７８．安全性（safety）

定義：情報システムが安定かつ正常に稼働すること。

解説：安全性とは、情報システムの稼動を阻害するリスクに対して、情報システムが保護され、安定かつ正常に稼働することをいう。

安全性を高めるためには、通信システムやコンピュータシステムの運用に際し、安全性を阻害するリスクへの対応計画や施策を行う。最近ではネットワークの普及により、ウイルスやハッキングによる被害や外部からの不正侵入に対する安全対策の重要性が増しているため、ネットワークセキュリティに対する安全性が話題となっている。ネットワークセキュリティ以外のリスクとしては、通信機器やコンピュータそのものによるハードウェアの不良、火災・水害、地震・停電、ハード・ソフトの設置環境、ソフトウェアのバグ、オペレーションミスなどの内部・外部の要因が掲げられる。

安全対策とリスクには相関関係が認められており、リスクを評価することで安全対策の実施状況評価が可能となる。したがって情報資源のリスクに関するチェックリストを作成して安全対策を計画するとよい。

７９．可用性（availability）

定義：許可された利用者が、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（JIS x 5080）。

解説：可用性とは、利用を許可されているユーザ（利用者）が、必要な時に、許可されている情報へのアクセス要求をする場合に、アクセス可能とすることをいう。すなわち、ユーザが情報システムの機能や資源を必要とするときに、直ちにそれを使用できることである。情報システムが使用可能である状態を確保するための可用性対策として、一部に障害が発生しても代替設備で運用を継続できるように装置を多重化したり、短時間（数分）で予備用装置に切り替えたり修復できるよう準備しておくことなどが行われる。このため、24 時間 365 日の連続利用のニーズに対応する耐故障性を備えたコンピュータ（フォールトトレラントコンピュータ)も開発されており、ネットワークを利用したビジネスなどに利用されている。

可用性は、『機密性』、『完全性』とともに情報セキュリティの重要要素である CIA（Confidentiality, Integrity, Availability）の一つである。

８０．機密性（confidentiality）

定義：アクセスを許可された者だけがアクセスできることを確実にすること（JIS x 5080)。

解説：機密性は、アクセスを許可された者だけがアクセスでき、アクセスを許可されていない者が利用できないようにすることである。情報の共有者（個人、組織体)以外の第三者(特に競合者)に、その情報が故意または偶然の手段で知られた場合には、損失が生じる。また、アクセス権を持たない者がアクセスすると、情報改ざん、不正情報の混入や漏洩などの被害が生じてしまう。このような被害が起きないように、機密性を高める施策がとられる。

機密性は保護の対象とする情報、情報を処理する機器や仕組みなどを議論する場面で考慮する。

情報に対する機密性では、企業や組織では機密情報の管理方針を策定し、すべての情報資源を機密区分することが重要である。機密区分とは、情報資源の機密度に応じて、極秘、秘、社外秘、部外秘などに区分される。情報システムでは、情報資源の機密度に応じてアクセス権限や利用者を区別する。この機密区分に基づいて、情報の利用（閲覧、変更、加工)、配布、持出し・持込み、保管、消去、廃棄に関する手順を定める。

通信処理における機密性は、ISO が定義する OSI ネットワーク管理の５つのカテゴリに分けて機密管理、課金管理、構成管理、障害管理、性能管理することが一般的である。

暗号化処理での機密性とは、目的とする受取人以外の人がメッセージを読みとれないようにすることである。

このように機密性は、システム監査の対象、機能や目的に応じて具体的な意味は異なってくる。

機密性は、『完全性』、『可用性』とともに CIA（Confidentiality, Integrity, Availability）の一つである。

８１．完全性（integrity）

定義：情報および処理方法の正確性および完全性を保持すること（JIS x 5080)。

解説：完全性とは情報および処理方法が正確であるようにすること、および、その正確である状況を保持すること。つまり許可されていない利用者、または内部利用者によって

情報が改ざん、または破壊されたりしないようにすることにより、情報の正確性と完全性を常に維持すること。

（参考）

OECD（経済協力開発機構）のセキュリティガイドラインでは、「情報の『機密性』、完全性、『可用性』を確保し、維持すること」と定義されており、情報セキュリティに関しては、この『機密性』、完全性、『可用性』の定義が CIA(confidentiality, integrity, availability）として広く利用されている。

『機密性』、完全性は「情報を守る」ことに力点を置いた考え方である。例えば、不正アクセスによるホームページの改ざんは、完全性が欠落していることになり、情報セキュリティ上の欠陥があることになる。

CIA のうち、一つの要件でも欠落すると、情報セキュリティとして機能しなくなる。例えば、DoS 攻撃によってサーバー利用が不能になると、『可用性』が喪失したことになり、情報セキュリティ上の欠陥があることになる。ネットワークから個人の信用情報が漏洩したならば、このネットワークは『機密性』を喪失し情報セキュリティ上の欠陥があることになる。

８２．戦略性（strategic）

定義：組織や企業の目標達成のため、長期的な価値や理念に基づき、情報技術(IT)の導入や情報システムの開発運用を行うこと。

解説：戦略性とは、組織や企業が存続・成長し、価値を増大させるための目標を達成するため、長期的な価値や理念に基づき、IT の導入や情報システム開発運用を行うこと。組織や企業では IT の導入や情報システム開発運用が、経営戦略の一環として計画され実行される。

事業環境や情報技術が急速に変化するなかで、戦略性の重要度が増している。インターネット技術に代表される IT を活用し、これまで以上の『ビジネスプロセス』効率化や活性化を図り、企業や業界を超えたコラボレーション、新しい『ビジネスモデル』の創造や事業価値を創出するには、組織や企業全体で選択と集中の判断を明確にして限られた資源を投入し、優先的に取り組む必要がある。

そのためには業務処理の効率化や省力化のようにコスト削減を構築目的とした従来の情報システムではなく、利益の創出、競争力強化を目的とする視点が必要である。 ダウンサイジング／ライトサイジング、分散処理から BPR（Business Process Re-engineering）や ERP（Enterprise Resource Planning）のように新しい概念を取り入れた全体システムを構築する。このため、業務プロセスや情報システムを戦略性の視点から評価し、今後の指針を得るため、システム監査は有効な手段となる。

システム監査は被監査部門から独立した立場で行なわれ、トップマネジメントの視点で、情報システムが経営に貢献しているかどうか判断するため、従来の『安全性』、『効率性』、『完全性』、『信頼性』、『可用性』、『機密性』、有用性と併せ、戦略性を考慮して調査し、あるべき姿を総合的に描くことが必要である。またシステム監査人には、自ら形成した判断基準に照らして評価し、戦略上の問題点についても説得力のある改善勧告を行うことが求められる。

８３．有効性（effectiveness）

定義：情報システムが、当初の目的通りに機能していること。

解説：有効性とは、情報システムが、機能面、経済面だけでなく、当初の目的通りに『安全性』、『効率性』、『信頼性』、『可用性』、『機密性』、『完全性』、有用性、『戦略性』の観点から経営に役立っていることである。情報システムの有効性を評価する指標として、投資効果が測定される。しかし、情報システムは多くの側面で利用され、その効果は複合的に表れるため、投資効果の測定方法を確立している企業は少ない。情報システムの有効性は、省力化という定量的な成果から時間短縮、機能向上、機密保全、経営戦略の部分などの定性的な貢献が求められるようになり、また投資の時期から遅れて効果が生じるため、効果測定の評価尺度が複雑であるからである。

有効性の判断基準は事業環境や適用する情報技術により変化するので、従来システムと同様な視点からのやり方を繰り返すことは、 企業の競争優位を損なう危険性を増す場合がある。

投資をしてコンピュータを導入しても、開発した情報システムが現場に適応しておらず使えなかったり、 全体の作業効率を低下させたり、という例は少なくない。システム部門の組織活動やシステム開発や運用のアウトソース状況を確認するには、システム開発投資に対して『効率性』・有効性の視点を重視して診断する。

８４．遵守性（observance）

定義：情報システムの開発や運用、情報システムの利用が、法規制や外部のルール、組織内部の方針やルールに沿って実施されていること。

解説：遵守性とは、情報システムの開発や運用、情報システムの利用が、法律・規則や外部のルール、組織内部の方針やルールに適合し、運用されていることである。

情報システムの開発や運用、情報システムの利用は、法規制や所属する業界や地域社会などの外部のルールに従うことで適法性を維持し違法性から逃れ、利用者の信頼を得る。また自ら定めた組織内部の方針やルールに沿って実行されることで、『内部統制』の側面で合理的経済的利益を享受することができる。

８５．経済性（economy）

定義：情報システムの開発や運用、利用が、適切な費用でまかなわれ、また利用部門に対して金銭で換算できる価値や効果を与えていること。

解説：経済性とは、情報システムの開発や運用、利用が、適切な費用でまかなわれ、また利用部門に対して、情報システム利用による価値や効果を金銭で換算し満足する状態にあることである。

情報システムを開発運用し、利用するためには、設備投資、設備やサービスの利用料、人件費などの費用が発生する。これらの費用が高いか安いかは、経済的な合理性により判断される。

情報システムが企業活動の中核とされる機能の多く(基幹システム)を担うようになり、また企業経営の中で情報通信システムの開発運用に要する費用が占める割合が大きくなってきた。従って過剰な情報投資はないか、予定された効果を提供しているか、不必

要な二重作業や重複機能はないか、セキュリティ被害発生時の回復処理で発生する費用は課題とならないかなど、情報システムの開発や運用面で経済効果を確認する場面が増加している。情報システムの利用形態は、生産、販売、在庫、調達、経理などの多様な場面でネットワークを経由して多岐にわたる。したがって、情報システムの開発や運用、利用が、適切な費用でまかなわれていること、また利用部門に対して金銭で換算できる価値や効果を与えており、利用者が経済効果を把握し、その投資効果に対して満足していることがポイントとなる。

８６．効率性（efficiency）

定義：情報システムおよびその設備、施設、要員の資源を最適に活用すること。

解説：効率性とは、情報システム、情報システムを開発・運用する設備、施設、要員などの資源を最適に活用することである。

投資をしてコンピュータを導入しても、開発した情報システムが現場に適応しておらず使えなかったり、 全体の作業効率を低下させたり、という例は少なくない。高度で複雑な情報システムや通信システムの運用では、サービスの継続性や事業の継続性に影響を与える事態も発生している。

このため情報システムの資源を有効活用し､投資対効果を高める工夫が求められている。システム監査は､システム開発投資や運用に対して効率性･『有効性』の視点から診断し、システム部門の組織活動やシステム開発や運用状況を確認するので、極めて有効である。

８７．信頼性（reliability）

定義：システムの不具合やハードの障害により情報システムが正常な機能を停止し、異常な出力結果になることを防ぐこと。また､障害発生時には損害に直結しないよう対応し、被害が拡大しないようにすること、速やかに復旧すること。

解説：信頼性とは、システムの不具合（例えば、プログラムミス、設計エラーなど）やハードウェアの障害により情報システムの正常なサービスが停止したり、異常な出力結果になることを防ぐことをいう。実際にトラブルが発生したときには、損害に直結しないよう、また被害が拡大しないようにすること、速やかに復旧することを含む。

IT 活用が進み、情報システムの重要性が増すほど、落雷･洪水･地震等の自然災害や回線の故障、人的な操作の誤り等によってシステムがダウンした場合の損失は重大となる。このような環境下では、情報システムの『安全性』や信頼性がどのレベルにあるのかを把握し、事前にこれらのリスクを推定し、事業への影響を最小限にとどめるため想定される事故や災害に備えておくことが重要となる。しかし、現在では情報システムが複雑化し、機能停止に陥った場合、手作業による回復処理は不可能な場合が多い。

そこで、障害発生防止や信頼性を高める対策として、厳重なシステムテスト、機器構成や通信回線の多重化、バックアップセンターの設置などを行う。また訓練や定期点検などの事前対策や障害発生後の回復手続き等の点検・評価を行う。

８８．業務処理統制（application control）

定義：個々の業務処理システムの入力、処理、出力について『安全性』､『信頼性』､『効率

性』を確保するためのコントロール。

解説：業務処理統制は、個々のアプリケーション・システム（業務処理システム）において、開始された取引が承認され、漏れなく重複なく正確に入力され、処理・出力されることを確保するために行う統制活動である。『全般統制』と対比される考え方であり、アプリケーション・コントロールとも呼ばれる。情報システムのコントロールは、情報システムの『安全性』･『信頼性』・『効率性』に影響を与えるリスクを適切に処理する仕組みのことであり、一般には設備面・技術面・運用管理の面から設計されている。このコントロールは、エディットテスト、合計、照合調整、識別、過誤・不明・例外データの報告等から構成される。

日常の業務活動は、業務処理から生じる情報、業務を行う人の活動、及び情報の入出力、処理等をコンピュータ上で行うアプリケーション・システムが組み合わさって機能している。

システム監査人は、各『ビジネスプロセス』の内容を理解し、IT のコントロール目標が設定されているか、目標と実態を比較するチェック体制が整備されているかなどにより、業務処理統制を確認する。また、アプリケーション・システムは、各業務システムの『ビジネスプロセス』ごとに作成されていても他の業務と連携している場合が多いので、例えば原価計算について会計処理だけでなく在庫システム、 販売管理システム、売掛金管理システムおよび関係するシステムとのインタフェース処理を確認し分析する必要がある。

８９．全般統制（general control）

定義：業務活動全体を対象とする情報システムのコントロール。

解説：全般統制とは業務活動全体を対象とするコントロールで、ジェネラルコントロールとも呼ばれ『業務処理統制』と対比する考え方である。従来、IT に関連する統制活動は、『業務処理統制』と全般統制に分けて考えられてきた。全般統制は、IT を利用した情報システムが適切に運用管理されることにより、複数の『業務処理統制』が有効に機能することを間接的に確保する統制活動である（COSO の定義）。

全般統制には、ネットワークの運用管理、アクセス・コントロールなどのセキュリティ管理、アプリケーションの取得・開発・運用、外部委託管理などが含まれる。

９０．予防牽制機能（Preventive control）

定義：業務の過程で誤謬や不正を生じさせる可能性のある行動や機会を牽制することで、事前に誤謬や不正の発生を防止する機能。

解説：予防牽制機能は、予め誤謬や不正の発生する機会を予防することで不正発生に至らないような組織上の仕組みを機能させて、業務処理の過程で誤謬や不正を生じさせる可能性のある行動や機会を牽制すること。例えば、特定者に権限が集中することをさけ、複数名により相互チェックすることで処理の誤りや不正がおきにくいようにする。誤謬摘示機能と『修正回復機能』と同様に、『内部統制』を構成する３つの主要機能の１つ。ログをとること、教育、規定の整備、なども予防牽制の役割を果たす。

９１．誤謬摘示機能（editing control）

定義：業務処理の過程で誤謬や不正が発生した場合にそのことを速やかに検知し、報告・警告する機能。

解説：誤謬摘示機能は業務処理の過程で誤謬や不正が発生した場合に、そのことを速やかに検知し、報告・警告など被害を最小限に抑えるために適切な対処がとれるようにすることである。『予防牽制機能』、『修正回復機能』とあわせ、『内部統制』を構成する３つの主要機能の１つ。

誤謬摘示機能は、プログラムによる誤謬摘示、記録や実在する資産との照合、発見された誤謬に関する適切な措置の機能に分類される。例えば、入力されたデータが事前に定められた範囲の数値や基準と異なる場合に、警告して入力訂正を促し、潜在エラーを解消する。

９２．修正回復機能（recovery control）

定義：業務処理の過程で誤謬や不正を発見した場合に、速やかな修正・回復を図り、組織体の業務活動に与える影響を最小限にとどめる機能。

解説：修正回復機能は業務処理の過程で誤謬や不正を発見した場合に、速やかな修正・回復を図り、組織体の業務活動に与える影響を最小限にとどめる機能である。

例えば、障害などの異常が発生した場合に、正常な元の状態に修復するための平均修復時間などの指標を使って、システムの保守の指針としても活用される。修正回復機能は、誤謬や不正が検出されることを前提として、検出機能と組み合わせて利用する。

また、修正回復機能は、日常的な回復機能と緊急回復機能に分けて考えるとよい。日常回復機能は、発生頻度の高いデータの不整合や誤謬を修正する機能で、緊急回復機能は災害発生時など、発生するとダメージが大きく、回復にも多くの時間や費用を要する場合の対応である。

いずれの場合も、事前に対応可能な回復手続を定めておくことが重要である。

９３．守秘義務（obligation to keep secrets）

定義：『機密性』のある情報を職務上知り得る立場にある者が、その情報を故意や過失により第三者に開示しないようつとめる義務

解説：守秘義務はシステム監査人のように『機密性』の高い情報を職務上知り得る立場にある者が、その情報を故意や過失により第三者に開示しないようつとめる義務である。システム監査上で知りえた秘密は漏らさない、監査の目的以外に利用しない、また第三者に利用されるような状況に置かないことが大切である。システム監査人は職業的専門家としての正当な注意を払い、入手する情報を扱い、保管することが期待されており義務がある。守秘義務を確認するため、一般には NDA（秘密保持契約書）を相互に交わして会話や情報交換を始める。

なお、守秘義務に関し、システム監査基準では、次のように定めている。

「システム監査人は、監査の業務上知り得た秘密を正当な理由なく他に開示し、又は、自らの利益のために利用してはならない。」

９４．職業倫理（professional ethics）

定義：監査人が専門家として備えるべき特定の使命、社会的責任あるいは行動規範。

解説：職業倫理はシステム監査人などの特定職業に携わる専門家が備える特定の使命、社会的責任あるいは行動規範、また倫理的な活動規範のことである。システム監査人には倫理基準の遵守、守秘、公正不偏の態度、独立性等が要求される。

倫理は組織の倫理と個人の倫理とに区分され、組織の倫理は会社の構成員がある特定の行為を行うような組織の定義や規則のこと。また、個人の倫理とは、個人がある特定の行為を行う上での氏名、責務、社会的責任や倫理観をいう。ここでは、職業倫理は、特定の職業に従事する者が備えるべき倫理事項であり、個人の倫理を問う。例えば、倫理は次のような場合に問題になる。

・倫理上の問題についての一般的なビジネス上の理解
・法規の遵守
・利害衝突
・接待費および贈与にかかる費用
・顧客とサプライヤーとの関係（贈与やキックバックを与えたり、受け入れたりすること）
・社会的責任

なお、職業倫理についてシステム監査基準では、次のように定めている。

「システム監査人は、職業倫理に従い、誠実に業務を実施しなければならない」

システム監査学会では倫理綱領を、日本システム監査人協会ではシステム監査人倫理規定を定めている。

９５．職務権限（job functions）

定義：組織および職位ごとに定めた、職務上の指示・実行の及ぶ範囲と責任のこと。

解説：職務権限は、組織および職位ごとに定めた、職務上の指揮命令・指示・実行の及ぶ範囲のことで、通常、職務規程で明文化されている。

権限には責任が付随し、その責任は、職務遂行責任（Obligation）・結果責任（Responsibility)・報告責任（Accountability）に分類される。このうち結果責任・報告責任の追及されない権限は、濫用に繋がる。職務権限を明確にしないことによって、指揮命令系統が混乱したり､権限が特定個人に偏重したりすることによる影響は大きい。業務が円滑に進まないだけでなく、不正や誤謬が発生するリスクが高まる。小規模組織では、これらを兼務することがあるが、組織の規模がある程度大きくなってきた段階で『職務分掌』・職務権限を明らかにすることが重要である。

９６．職務の分離（segregation of duties）

定義：『相互牽制』の観点から、職務をある組織または然るべき職位の要員に割当て、１つの職務を２つの組織が交互に行ったり、１人の担当者が２つ以上の職務を兼ねることのないようにすること。

解説：職務の分離は、『相互牽制』の観点から、職務をある組織または然るべき職位の要員に割当てコントロールすること。例えば、次のようなコントロールが該当する。

・１人の担当者が２つ以上の職務を兼ねることのないようにする（申請と承認、実行と監視）
・２人以上担当者が検査して処理する（入力と処理）
・１つの職務を２つの組織が交互に行なう（検査）
このように仕事上の責任を分散させることで、処理の誤りや違反行為を予防し、誤りや違反の事実を発見することができる。

９７．職務分掌（job duty）

定義：組織および組織を構成する役割や要員ごとの、業務処理過程における職務分担および責任・権限に関する定め。

解説：職務分掌は業務処理過程の職務分担と責任・権限について、組織および組織を構成する役割の単位や要員ごとに定めたもの。企業がある程度の規模になると、社長一人あるいは特定少数の者だけでは経営が立ち行かなくなる。そこで、分業（職務分掌）の必要が発生し、さらに分業が進んでくると、権限とその裏返しとしての責任の問題が生じる。会社が小規模のうちは、社長が自分の思っていた通りに物事を判断し、進めることが出来る。しかし規模が拡大していくと、個人の能力の限界を超えた部分について機能しない事態が発生する。個人の管理能力の限界は、仕事の量、人の数だけでなく、扱う金額等によっても、発生してくる。そこで自然と分業が進むか、分業を進めざるを得なくなり職務分掌と責任権限をどう定めるかの課題が起きる。
急成長会社の場合は、会社の成長のスピードに組織がついていけないことがあり、規模の拡大が、権限の明確化や体制整備より速い場合は、必要にせまられて権限が分散してしまうこともある。歴史のある企業の場合、公式的に権限を委譲するための組織改革が事業環境の変化に遅れている場合も多い。

９８．相互牽制（separate control）

定義：業務の遂行過程において、２名以上の従業員に分担させ、職務を分離することにより、不正や誤謬の発生を発見・予防し、あるいは自動的に検証できるようにした仕組みの総称。

解説：相互牽制とは業務の遂行過程において、２名以上の従業員に分担させ、職務を分離することにより、不正や誤謬の発生を発見・予防し、あるいは自動的に検証できるようにした仕組みの総称。内部牽制ともいう。
相互牽制は、取引を特定の人物のみで完結させずに、複数の者により分担して行わせることにより相互に牽制させ不正や誤謬を防ぐことをいい、一般に、①物の管理と②お金の管理と③帳簿の管理を分離して、三つのうち二つ以上の管理を兼任させないようにする。

９９．内部統制（internal control）

定義：業務の『有効性』と『効率性』、財務報告の『信頼性』、関連法規制への準拠という統制目的の達成に関して、合理的な保証を提供することを意図した、事業体の取締役会、経営者およびその他の構成員によって遂行されるプロセス。（COSO）

解説：内部統制の目的は、次の３つの統制目標の達成に対して合理的な保証を提供することにより、企業目的の実現を保証することにある。

・業務の『有効性』と『効率性』（業務能率の確保）

・財務報告の『信頼性』（適正情報の確保）

・関連法規の遵守（コンプライアンスの確保）

経営者が定めた制度や組織、必要な手続および諸規程等からなる経営の仕組みの総称でもあるが、COSO フレームワークでは、「統制環境」「リスク評価」「統制活動」「情報と伝達」「監視活動（モニタリング）」を内部統制の５構成要素としている。

さらに COSO-ERM では戦略を加味して戦略、業務、報告、遵守に拡張している。

経営資源の適切かつ効率的な保全、正確な業務記録の作成と信頼ある業務報告、法令・規則への遵守を合理的に保証するために行うことが、内部統制の役割である。

従って、望ましくない状況に陥ることを予防、早期発見、是正し、事業目的を達成するために組織、仕組みや手続として用意することを意図している。

会社の規模がある程度の段階に達する場合に、『職務分掌』と『職務権限』を明確にして組織機構を整備することである。内部統制では、分業体系化された組織単位がその組織目標達成のために正常に活動しているかどうかをチェックする。会計統制と業務統制は内部統制の機能である。

１００．外部統制（external control）

定義：法令・規則や業界団体など外部の利害関係者が定めた制度・組織・手続や規程等により、特定組織の経営管理の仕組みが影響を受けること。

解説：外部統制とは、法律や外部の利害関係者が定めた制度・組織、必要な手続および諸規程等からなる経営の仕組みの総称。経営資源の適切かつ効率的な保全、正確な業務記録の作成と信頼ある業務報告、法令・規則への遵守を合理的に保証するために行う。

１０１．ITガバナンス（IT governance）

定義：IT を活用して経営効率を増進させる手段。経営統制の一つの手法で、経営者の承認を必要とする意思決定過程に関係する組織計画・手続および方法。

・企業が競争優位性構築を目的に、IT（情報技術）戦略の策定・実行をコントロールし、あるべき方向へ導く組織能力（1998 年の BCG／通産省（現経済産業省）の「IT ガバナンススコアカード策定支援プロジェクト」）

・IT やそのプロセスにおけるリスクと利益をバランスさせながら価値を付加することによって、企業目標を達成するために、企業を方向付けし、コントロールする一連の関係構造とプロセス（COBIT3）

解説：IT ガバナンスとはコーポレートガバナンスの一環として経営効率を増進させるために行う、システム統制や会計統制、『業務処理統制』などを含む経営管理のための統制手段が確立されている統制である。利益や経営効率を最大化しリスクの最小化を目標とする。

システム統制では、インターネットの普及に伴い、本社・工場・倉庫間などの企業組織内部の連携だけでなく、企業相互間の業務連携が重要となり、相互の円滑な情報交換の

ため運用・技術、開発手法、セキュリティレベル、サービスレベルなどの標準化された手順が重要になっている。システム監査はこれらの情報システムに関連するリスクが適切にコントロールされているかを評価し、説明責任を果たすもの（システム監査基準、2004）であり、IT ガバナンスの実現に寄与する。例えば、システム統制では、企業が定める会計方針および会計処理方法に沿って構築された会計システムや業務処理システムなどの情報システムを通じて、処理や転記の誤りをなくし処理時間を大幅に短縮することや経営分析資料を提供することで業務効率を増進させ、迅速な経営意思決定を支援する。一方、会計統制では、『内部統制』の一つである資産の保全および会計記録の『信頼性』を確保するために組織計画や手続を定める。このため会計統制では、会計記録の正確性と『信頼性』をチェックし、定められた会計規則の遵守を促進して企業の財産を保全することに主眼が置かれる。

企業や組織全体の効率化や最適化を求めるためには、採用する IT や IT 活用方法にもルールや統制が必要であり、IT ガバナンスの重要性を裏付ける。

１０２．電子政府と電子自治体（e-Gov. and e-local Gov.）

定義：政府や中央官庁が実施する、IT 活用による行政効率化と利用者の利便性向上のこと（電子政府）。同様に、地方自治体が実施する場合を、電子自治体という。IT 活用とは、文書の電子化、ペーパレス化および情報ネットワークを通じた情報共有・活用に向けた業務改革を重点的に推進することにより、電子情報を紙情報と同等に扱う行政であり、IT をツールとし、庁内業務の効率化、高度化を推進していくこと（e-Japan 戦略）。

解説：電子政府では、政府が所有し管理運用する情報や手続が電子的にも対応可能となり、市民や企業が必要とする行政手続などの行政サービスが電子的に実施され、また情報の開示提供などのサービスを電子的に行われる。

2001 年に政府ＩＴ戦略本部で決定された e-Japan 戦略では「世界最先端の IT 国家に」という目標が掲げられ、霞ヶ関 WAN、総合行政ネットワーク（LGWAN）と、各都道府県、市町村までを接続したイメージが示された。

2004 年 6 月には、国の行政機関が扱う手続の 96%はオンライン化され、「電子政府構築計画」が改定された。改定「電子政府構築計画」では、整備されたオンラインの基盤を活用し、オンライン利用の利便性を高めるため次の計画が策定されている。

(1)年間申請件数が 10 万件以上の手続を重点に手続の簡素化・合理化の徹底、業務処理の短縮化を図る

(2)電子政府の総合窓口（e-Gov）を活用したワンストップサービスを推進する

(3)IT 導入による政府全体の業務・システムの最適化を戦略的・横断的に推進する

（電子政府サービスの例）

種類	電子サービスの名称と電子窓口
e-TAX	国税電子申告・納税システム　http://www.e-tax.nta.go.jp
電子申請 電子入札	政府の行政情報や行政手続を総合的に案内する電子政府総合窓口 各省庁のサイトへもリンクしている。　http://www.e-gov.go.jp
各省庁別	総務省、国交省、厚労省　など　http://www.e-gov.go.jp

電子自治体では、自宅や職場で利用されているパソコンや、駅、コンビニ、図書館、公民館などの設置された端末機を操作して、市民や企業が必要とする申請、届出、サービス予約や証明書発行などの行政手続ができるよう、電子化され効率的に整理されることが期待される。

地方公共団体は、政府が推進する e-Japan 構想で実現しようとしている電子行政サービスのなかでも、国民生活、企業活動それぞれの面で身近な部分を多く受け持っている。従って中央省庁自身の電子化と、省庁と地方公共団体とを電子的につなげるネットワーク基盤の整備（G to G）が進められた。電子自治体とは、国民に身近な行政の窓口の役割を担う電子サービスの提供手段であり、地方公共団体が責任推進主体となる。そこで窓口の電子サービスを実現するため、政府内部事務の電子化、政府と地方公共団体を結ぶネットワーク基盤が整備されてきた。

具体的に、身近な行政サービスが目的とする行政サービスの効率化、情報サービスと住民参加などの内容が課題となる。住民基本台帳法が改正され、2002 年には住民基本台帳ネットワークシステム(「住基ネット」(第１次))の運用が始まった。住基ネットにより、各種行政手続きで、住民票の写しの添付が不要となる。2003 年（第２次）からは、全国どこの市町村でも住民票の写しの交付が受けられる。住基ネットは、電子政府・電子自治体を支える基盤として、なりすましや文書の改ざんなどを防止する公的個人認証サービスの構築に大きな役割を占める。

（電子自治体：都道府県電子調達・入札システムの例）

種類	電子サービスの窓口
コアシステム	大阪府　http://www.pref.osaka.jp/kenso/e-nyusatsu/
電子調達	東京都　http://www.e-procurement.metro.Tokyo.jp/
電子申請	埼玉県　https://eshinsei.pref.saitama.lg.jp/request/
電子入札	千葉県　https://www.epr.pref.chiba.lg.jp/portal/

コアシステムとは、国土交通省（主として工事）や総務省（電子入札・開札）

１０３．ＣＯＢＩＴ (Control Objectives for Information and related Technology)

定義：優れた IT セキュリティおよびコントロール手続をおこなうために、適用可能で認知された標準として提供される、情報テクノロジを管理するための標準。(Cobit3)

解説：COBIT（コビットと呼ばれる）は、米国の「IT ガバナンス協会」が作成し提唱する、『IT ガバナンス』の成熟度を測るフレームワークである。組織が掲げる目標に対し、組織の総合的な実践能力を測る評価手法としても注目されている。

COBIT は、「プロセス」「IT 資源」「情報基準」の 3 つの視点により IT 戦略立案から導入・運用までの一連の流れを、4 つ管理プロセスと 34 の IT プロセスに分け、それぞれのプロセスについて、CSF（Critical Success Factor：重要成功要因）／KGI（key goal indicator：重要目標達成指標）／KPI（Key Performance Indicator：重要業績達成指標）を定義しており、その成熟度レベルを 6 段階で評価する。

COBIT が定義している 4 つの管理プロセスと 34 の IT プロセス

1. 企画・計画と組織 ・ 戦略的 IT 計画の定義 ・ 情報アーキテクチャの定義 ・ 技術指針の決定 ・ IT 組織の関係の定義 ・ IT 投資の管理 ・ 管理目標と指針の伝達 ・ 人的資源の管理 ・ 外部要求事項への準拠性の保証 ・ リスクの評価 ・ プロジェクト管理 ・ 品質管理 2. IT 調達と開発 ・ 自動化されたソリューションの検証 ・ アプリケーションソフトの調達・保守 ・ 技術基盤の調達・保守 ・ プロセスの開発・保守 ・ システムの導入と『信頼性』の付与 ・ 変更管理	3. デリバリと支援 ・ サービスレベルの定義と管理 ・ サードパーティのサービス管理 ・ 性能やキャパシティの管理 ・ 継続的サービスの保証 ・ システムセキュリティの保証 ・ コストの識別と配賦 ・ ユーザの教育・訓練 ・ 顧客の支援と助言 ・ 構成管理 ・ 問題と障害管理 ・ データ管理 ・ 設備管理 4. モニタリング ・ プロセスのモニタリング ・ 『内部統制』の妥当性の獲得 ・ 独立的保証の獲得 ・ 独立的監査の提供

成熟度レベル

レベル 5： 最適化されている(Optimized)	標準プロセスを改善・改良し、常に最適化された状態を維持している
レベル 4： 管理されている（Managed）	定義された標準プロセスに従って業務が進められているかモニタリングしている（また、その体制がある）
レベル 3： 定義されている（Defined）	標準プロセスがきちんと定義され、組織としてそれを認証している
レベル 2： 反復可能（Repeatable）	標準プロセスがあり、ほとんどがそのプロセスに従って業務をこなしているが、遵守は個人に依存している
レベル 1：初歩的（Initial）	場当たり的な対処
レベル 0： 存在しない（Non-Existent）	ルールや問題についての認識がない

１０４．ビジネスプロセス（business process）

定義：組織体が特定の目的を達成するために行う一連の活動、および組織の内外で連続する活動や手続の連鎖のこと。

解説：ビジネスプロセスは、組織が戦略を実行するための具体的な手法であり活動そのものである。ビジネスプロセスを業務プロセスとして細分化して捕らえると技術開発、調達、製造、販売、アフターサービス、請求回収、物流などの基幹業務プロセスと、財務経理、人材育成、IT 活用や総務人事などの支援業務プロセスに分けることができる。

組織が活動する環境や競争条件が変化すると、組織は存続するために新しい環境に適応する『ビジネスモデル』を作る。これがビジネスプロセスの再構築(BPR)であるが、従来手法の改善や不採算事業からの撤退、新規事業への参入といった程度ではなく、企業の存続をかけた大規模な改革を指している。特に、インターネットをはじめとする情報通信技術の急速な発展に伴い、時間や距離の概念が大きく変わった 1990 年代の後半以降、企業では製造拠点や販売物流の手法が大きく変わってきた。

これは、事業を継続する組織体が、ビジネスプロセスとして情報通信技術の導入と活用方法を工夫して大きく変化させながら、コストの発生と付加価値を創造するプロセスを冷静に見極めるようになってきたことを意味する。

１０５．プロジェクトマネジメント（project management）

定義：組織やチームに課せられた課題を目標期日までに達成するために全体と個々の目標成果を明らかにし、特定スキルをもつ人材、設備などを有効活用して日程、品質、予算やコストを最適化する手法。

解説：プロジェクトマネジメントとは、使命を達成するための有機的なチームを編成して、プロジェクトを公正な専門的手段で効率的、効果的に遂行して、確実な成果を獲得する実践的能力の総称。通常業務との違いは、目標とする成果は定型的でなく独創的なもので特定使命を受けて実施されること。また始まりと終わりのある特定期間に、資源、状況など、特定の制約条件のもとで達成を目指す、将来に向けた価値創造事業である。日本の PM 実践と研究では、大きく分けると次の５つの流れがある。

①情報処理技術者試験プロジェクトマネージャ（経産省、スキル標準に基づく）
②PMBOK（米国 PMI（Project Management Institute））
③P2M（NPO プロジェクトマネジメント資格認定センター）
④ISO10006（ISO）
⑤各組織が実施する固有のプロセス管理手法（独自ノウハウ）

どの手法に準拠すれば最も効率的に推進できるかは、プロジェクトの大きさや範囲（技術やスキル、開発など特定業務、社内、国内、国際など）に関わってくる。

スキル標準では、プロジェクトマネジメントの職種を「プロジェクトの立ち上げ、計画策定、遂行及び進捗管理を 実施し契約上の納入物にも責任を持つ」と定めている。IT 投資プロセスでは、戦略的情報化企画（課題整理/分析(ビジネス/IT)、ソリューション設計(構造/パターン)）、開発（コンポネント設計(システム/業務)、ソリューション構築(開発/実装)）及び運用・保守（ソリューション運用(システム/業務)、ソリューション保守(システム/業務)）を主な活動局面として以下を実施する。

－戦略的情報化企画　　・基本計画の策定
　　・管理／統制
－開発　　・管理／統制
－運用・保守　　・管理／統制

また、PMBOK（Project Management Body of Knowledge、通称ピンボクと呼ばれる）では、プロジェクトマネジメントに必要な知識エリアとして次の９領域を定めている。

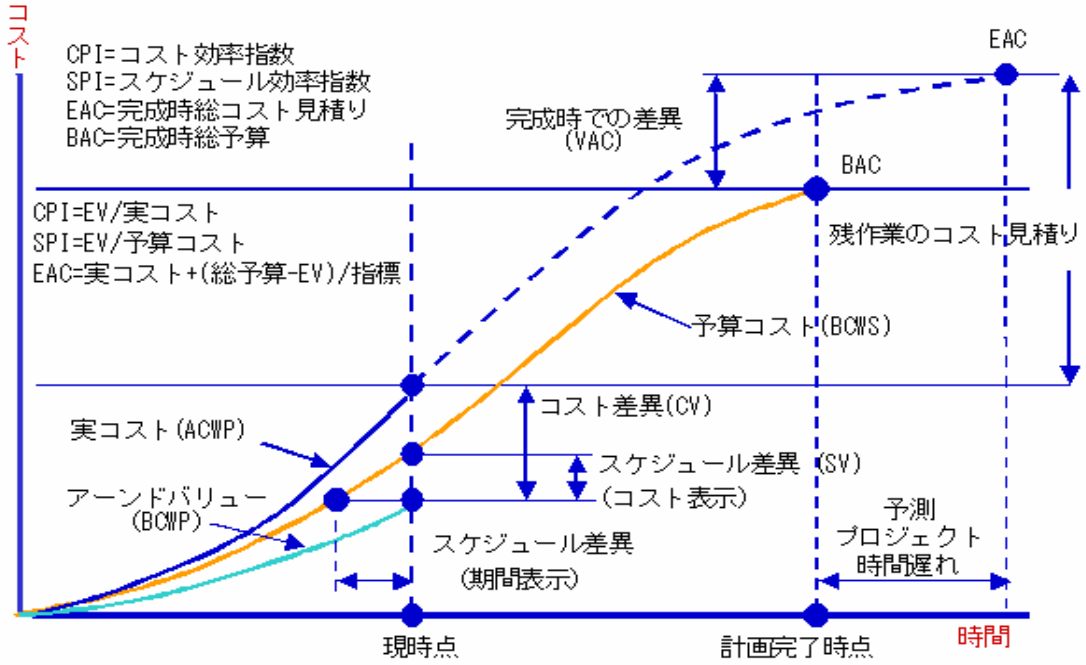
①統合マネジメント（計画策定、実行、全体の変更管理）
②スコープマネジメント（立上げ、計画、定義、検証・承認、変更管理、WBS、EVM）
③タイムマネジメント（アクティビティ定義、順序、期間見積もり、スケジュール作成、スケジュールコントロール）
④コストマネジメント（資源計画、コスト見積もり、予算化、コストコントロール）
⑤品質マネジメント（品質計画、品質保証、品質管理）
⑥人的資源マネジメント（組織計画、要員調達、チーム育成）
⑦コミュニケーションマネジメント（計画、情報配布、実績報告、完了）
⑧リスクマネジメント（計画、定性的リスク分析、定量的リスク分析、リスク対応計画、コントロール）
⑨調達マネジメント（計画、引合、発注先選定、契約管理、契約完了）

このようにプロジェクトマネジメントでは、活動を分割して異なる視点から評価しながら調整することが目標達成に有効である。最近は当初計画と実績の違いを EVM 手法により評価指標を用いて分析評価することが評価されているので次に紹介する。

EVM(Earned Value Method、アーンドバリュー技法)

PJ の実績を達成した価値により測定する手段で、コストや所要時間、品質の見積もりやパフォーマンス分析に活用する。EVM では、次の情報を元に、スケジュールとコストの実績状況を同一尺度で比較する。

EVM の指標と計算式の例



EVM 計算の例

PV	計画価値。計画された作業に対する予算化されたコスト。（Planned Value）
EV	アーンド・バリュー（Earned Value）。ある特定の時点で完了している作業に対する計画上の予算化されたコスト
AC	実コスト（Actual Cost）
BCWS	期間予算（Budgeted Cost of Work Scheduled）
BCWP	出来高（Budgeted Cost of Work Performed）
ACWP	実績コスト（Actual Cost of Work Performed）

評価の例：

コスト差異（CV:Cost Variance）　CV = EV－AC　マイナスの場合はコスト超過

BCWP>BCWS　進捗が早い、BCWP<BCWS　進捗遅れ

SPI=BCWP/BCWS　(スケジュール効率指数、Schedule Performance Index)

CPI=BCWP/ACWS　(コスト効率指数、Cost Performance Index)

出　典

WBS(Work Breakdown Structure)は、プロジェクトを作業項目や構成要素に分割して体系化することにより、資源計画だけでなくプロジェクトコストで大きな比重を占める人件費を見積もる手法である。

P2M（Project & Program Management for Enterprise Innovation）

国内で普及が図られている新しい『プロジェクトマネジメント』の知識体系。

１０６．ビジネスモデル（business method、model）

定義：企業が特定の目的を達成するため、何をどこでどのように実行して利益を得るかの仕組み、手法、形態のこと。

解説：ビジネスモデルは、特定の顧客や市場に対して、即時処理や従来の手続を簡略化するなどの時間的サービスや新たな付加価値を提供することにより顧客の支持を得て、圧倒的な集客やコスト削減に結びつけるような仕組みのことである。伝統的な企業では、長期間にわたり顧客や取引先からの信頼を得ている特徴や、事業として利益や技術力を維持確保している企業独自の工夫もビジネス上のノウハウや手法といえる。

デルモデル：ビジネスモデルの代表例である「デル・ダイレクト・モデル（デルモデル）」は、 顧客からの注文を受けてから生産を開始するため、必要なときに必要な量だけ部品を調達する徹底した SCM による完全注文生産であり、見込み生産はゼロである。コンピュータシステムを駆使することにより、独自の BTO（Build To Order=注文生産）とサプライチェーン・マネジメント（SCM）を実現しているところに特徴がある。このデルモデルは、基本を確立して以降、付加価値サービスを拡大した第 2 段階、インターネットによるビジネスとサービスの積極的な展開を開始した第 3 段階を経て、総合的なサービスやコンサルテーションを提供する第 4 段階にまで進展しているといわれる。

１０７．ビジネスモデル特許（business method patent）

定義：ビジネスの仕組みを特許化したもの。事業として何を行ない、どこで収益を上げる

のかという「儲けを生み出す具体的な仕組み」自体を内容として特許申請し、「発明」「新規性」「進歩性」が認められたもの。

解説：コンピュータ利用を組み合わせることで、従来の販売手法や工場の中の製造プロセスもビジネスモデル特許となりうるため、特許を取得することが着目される。

特許の対象となる『ビジネスモデル』は販売や電子商取引（EC）のプロセスに限定したものではない。 このためビジネスモデル特許に対する侵害事件の被告とされる事もありうるので、注意が必要である。ごく基本的なビジネスのアイデアやプロセスが特許化されており、先行者が利益を独り占め出来るわけで、Amazon.com の 1-Click（ワンクリック）特許を事例として特許紛争が始まった。

何が「特許として認められる新規性を備えた高度な技術」か、更に、特許や著作権の概念がない国との国際間の調整が WIPO(World Intellectual Property Organization)などで議論されている。

１０８．ベストプラクティス（best practice）

定義：最も優れた業績や評価を得ている企業や業務の実践方法。

解説：優れていると考えられる業務プロセス、業務推進の方法、ビジネスノウハウのことで、最も効果的､効率的な実践の方法。または最優良の事例。

「『ベンチマーキング』」手法では、自社を最高の状態に近づけるため、比較・分析の対象となる最高水準のモデルのことをベストプラクティスとする。

現実の業務改革プロジェクトでは、求められている改革の水準に到達できないケースが多い。これは、業務改革プロジェクトが、現在の組織、業務を前提とするか延長上で検討されているためであり、前提条件を変えない限り大改革は困難である。そこで、最高水準としてベストプラクティスの条件把握が求められる。

しかしながら、最適なベストプラクティスを調査し比較することは、現実的には困難である。『ビジネスモデル』、改革の理論、表面的な仕組みについて情報を得ても、その仕組みや成果を可能にしている条件や、関連する業務や取引先などの関係は社外や他業務との関係までは把握できないからである。

他社や他の業界の事例から、自社に必要な手法を学び取り応用する能力が問われる。

１０９．ベンチマーキング（bench-marking）

定義：組織が改善活動を行うときに、業界を超えて最も優れた方法あるいはプロセスを実行している組織から、その実践方法を学び、自社に適した形で導入して大きな改善に結びつけるための一連の活動(日本経営品質賞アセスメント基準書)。

解説：ベンチマーキングは、対象とする業務の『ベストプラクティス』（最も優れた実践方法）を探して、自社と比較分析して差異を把握し、そのギャップを埋めるように、自社の業務プロセスを改善する手法である。優れた業績や評価を得ている企業や業務の実践方法を学び、自社や自分のやりかたと比較して、その違いを解消していくことで、競合相手との優位性を確保していく手法である。

ベンチマーキングを進めるためには、自社の現状を正確に把握する必要がある。自社の強みと弱みを分析し、現状の競争能力と市場の評価を正確に評価します。そして、弱み

を改善するのか、強みをより強くするのかの方針に基づき、競争力を向上させるために最も効果的な業務プロセスを選定する。次に、対象とする業務プロセスの観点から業種や業界にこだわることなく『ベストプラクティス』をもつ企業を探す。対象企業が決まれば、その企業の業務プロセスの詳細な情報を収集し、分析し、指標とした『ベストプラクティス』と自社との差異を評価する。自社が目標とする改善テーマや水準をもとに実行計画書を作成して実践する。
ベンチマーキング手法では、優れた個々のプロセスを学び実践するとしても、全体のパフォーマンス向上が目的であり、細部にとらわれないことが重要である。
なお、システム開発や運用の現場で実践されているハードウェアの性能評価モデルを作ることをベンチマークテストというので、区別する。

１１０．ＣＭＭＩ（Capability Maturity Model Integration）

定義：ソフト開発組織の能力を、組織の能力成熟度または能力水準で評価するソフト開発のプロセス改善の指針。

解説：米カーネギー・メロン大学で開発されたソフトウェア開発の成熟度を評価する手法である CMM は、ソフトウェア開発を通じて経営管理全般への応用が展開されている。能力成熟度モデルである CMM が改定され、CMMI として統合された。

ＣＭＭｓの展開と分類	能力成熟度モデルの対象
SW-CMM（Software CMM）	ソフトウェアプロセス
SE-CMM（System Engineering CMM）	システム
SA-CMM（Software Acquisition CMM）	ソフトウェア取引
p-CMM（people-CMM）	人
IPD-CMM（Integrated Product Development CMM）	製品開発

CMMI では, SW-CMM 相当の組織の段階に対応して注目する領域を決めている。組織の能力成熟度を持った表現を Staged 表現、ISO/IEC TR 15504 の枠組みに沿って、プロセスごとに水準０から水準５までの６段階の能力水準を持つ表現を Continuous 表現と呼んでおり、２つの表現の間で変換ができるようになっている。
CMM がソフトウェアの開発、運用、保守の生産性を向上させるため、チームや組織の連携により、発展的に問題点を克服し改善していく能力（成熟度）の向上を図る仕組みであるのに対し、CMMI はプロセス及び製品改善を支援し、独立したそれぞれのモデルを用いる際に起きる不一致をなくし、重複を減らすことを意図している。
このため CMMI は、システムエンジニアリング、ソフトウェアエンジニアリング、ソフトウェア調達など、CMM より多くの分野をカバーしており、システム開発やソフトウェア開発及びそれらの調達におけるプロセス改善と供給者能力評価に使用できる。

SPA（Software Process Assessment）との関係

ソフトウェア開発の生産性と品質の向上を目指したプロセス改善活動がソフトウェア

プロセス改善(SPI: Software Process Improvement)であり、CMM または CMMI モデルに基づいたアセスメントを行う手法が SPA である。

１１１．ＥＡ（Enterprise Architecture；エンタープライズアーキテクチャ）

定義：組織の全体最適化の観点より、業務及びシステム双方の改革を実践するために、業務及びシステムを統一的な手法でモデル化し、改善することを目的とした、設計・管理手法。

解説：EA は、1987 年に John A.Zachman が提唱した「情報システムを設計するための枠組み」を基礎としており、1992 年に情報システムだけでなく組織全体を対象とする概念に拡張された。米国では、1996 年の IT 投資管理改革法に基づいて、EA 及び EA に基づく IT 投資管理が導入されている。

日本政府では、2003 年 7 月の「電子政府構築計画」の中で、EA の概念を取り込んだ「業務・システムの最適化計画策定指針」に基づいて、政府全体としての整合性を図りながら、2005 年度末までに業務・システムの最適化を推進していくことを発表している。

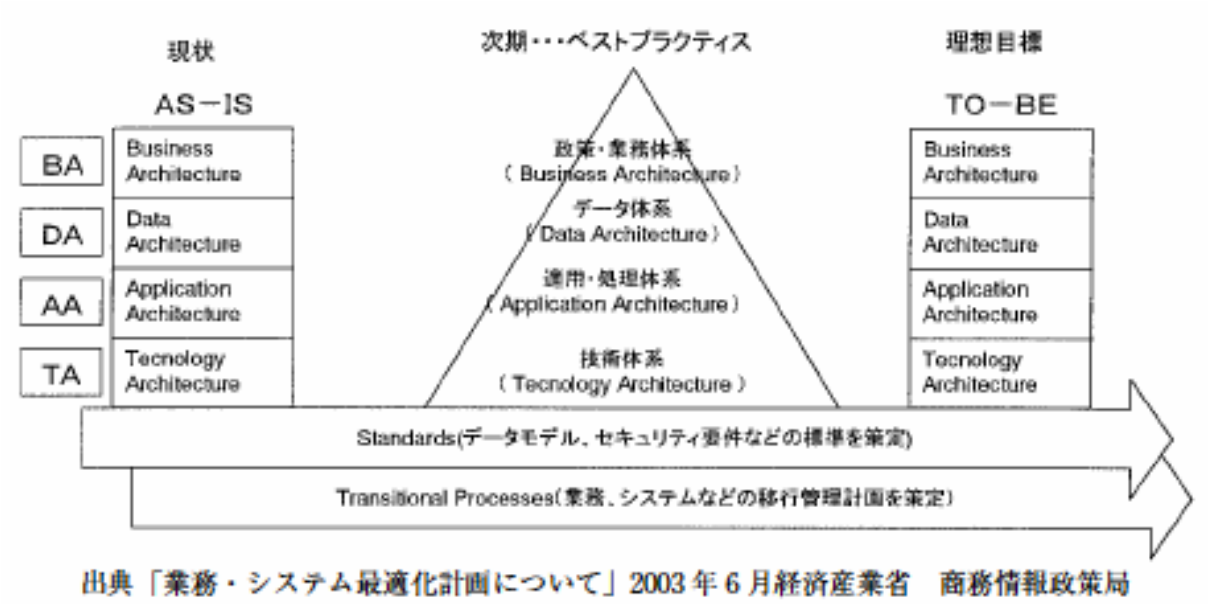
日本政府の EA（業務・システム最適化計画の策定手順）は以下の通りである。

第１ステップ：組織横断的に政策・業務分析を行い、非効率的な業務手順、システムの重複・無駄を洗い出す、業務改革の方向性を確定する。

第２ステップ：確定した改革の方向性と問題意識を踏まえ、組織全体の現状を掘り起す。

第３ステップ：作成された現状（ASIS）モデルを元に、改革の方向性に基づいた最適化設計をしなおし、将来（TOBE）モデルを作成する。将来モデルの作成に当たっては、今ある組織や業務処理の方法とは関係なく、本来組織がすべき機能とそこに必要となる情報の２つを抽出し、そこから理想像を逆算設計する方法をとる。

第４ステップ：現状モデルから将来モデルに向かっていくための現実的なステップとして次期モデルを作成する。



出典「業務・システム最適化計画について」2003 年 6 月経済産業省　商務情報政策局

1) 政策・業務体系（Business Architecture）
2) データ体系（Date Architecture）
3) 適用・処理体系（Application Architecture）
4) 技術体系（Technology Architecture）

１１２．ＣＯＳＯ（コーソー；トレッドウェイ委員会組織委員会：The Committee of Sponsoring Organizations of the Treadway Commission))

定義：トレッドウェイ委員会組織委員会：The Committee of Sponsoring Organizations of the Treadway Commission）の略称。

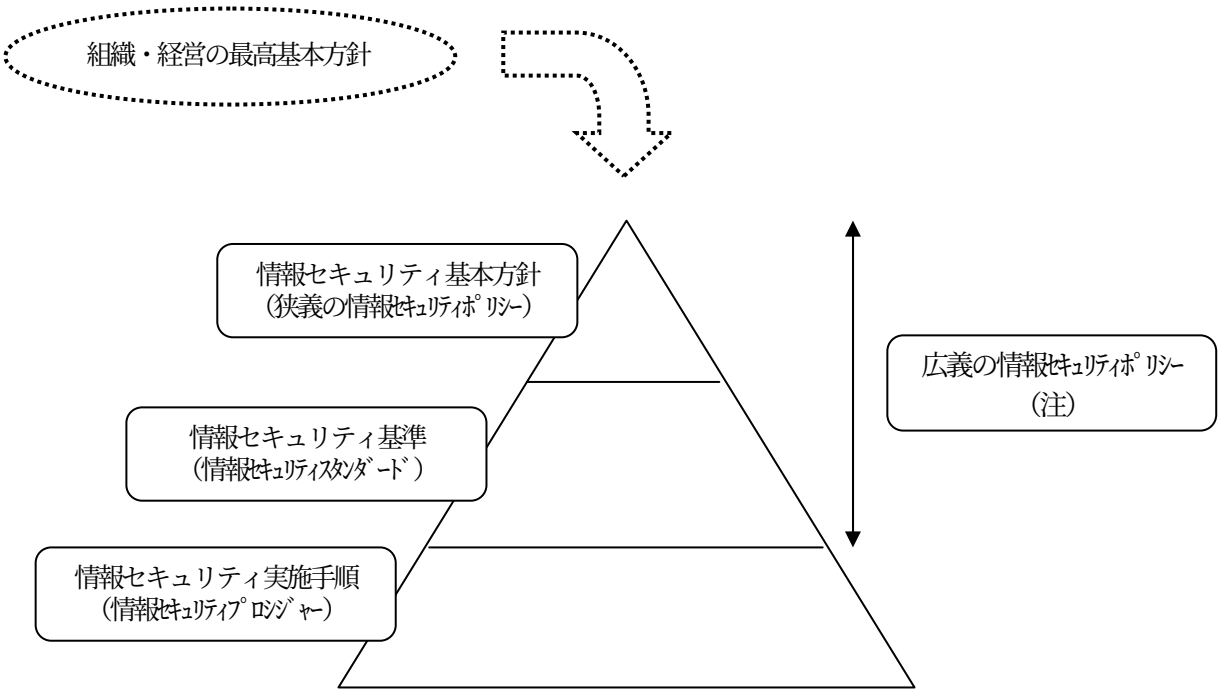
解説：1980 年代前半、アメリカにおける金融機関を含む多くの企業の経営破綻により、多くの企業不祥事が問題となった。1985 年にアメリカ公認会計士協会（AICPA）は、関連団体に働きかけ、「不正な財務報告全米委員会（The National Commission on Fraudulent Financial Reporting)」（委員長 J.C.Treadway, Jr.の名前を付けトレッドウェイ委員会と呼ぶ。）を共同で設立した。トレッドウェイ委員会は、1987 年に「不正な財務報告（通称「トレッドウェイ委員会報告書」)」と題する最終報告書を公表して、不正な財務報告を防止し発見するためのフレームワークとその方策を、上場企業（経営者)、外部監査人、米国証券取引委員会（SEC）およびそのほかの行政・立法機関、教育機関に向けて、さまざまな勧告を行った。

トレッドウェイ委員会の勧告を受けて、COSO（トレッドウェイ委員会組織委員会）は、内部統制に関する総合的な研究に着手し、1992 年「インターナル・コントロールの統合的枠組み（通称 COSO レポート)」を発表、1994 年には「『外部関係者への報告』の追補」を発表した。この内部統制の枠組みが、「COSO の内部統制フレームワーク」「COSO フレームワーク」と呼ばれるものである。

また、2004 年９月に COSO より、公表された「Enterprise Risk Management－Integrated Framework」は、COSO フレームワークを踏まえて、そのリスクマネジメントへの適用を提示したものとして注目されている。

１１３．情報セキュリティポリシー

定義：情報セキュリティポリシーとは、企業・組織が自己の保有する情報資産に対して、情報セキュリティを確保するための全般的な方向性および行動指針を規定したもの。情報セキュリティ基本方針ともいう。ここで定義する情報セキュリティポリシーの体系は、次図のとおりである。



（注）情報処理技術者試験においては、情報セキュリティ基本方針と情報セキュリティ基準の２階層を合わせて情報セキュリティポリシーと位置付けている。(広義のセキュリティポリシー)

情報セキュリティポリシー体系図

解説：以下、JIPDEC（日本情報処理開発協会）で運用する情報セキュリティマネジメントシステム（以下 ISMS という）適合性評価制度に基づき解説する。

（１）情報資産については、電子化されたデータのほか、紙ベースの情報、音声・画像等のデータも含まれる。対象とする情報資産は ISMS の適用範囲で定義する。

（２）情報セキュリティの確保とは、情報資産に対する機密性、完全性、可用性を確保することをいう。

（３）情報セキュリティポリシーは、次の項目を満たす必要がある。

①ISMS の目標を設定するための枠組みを含み、情報セキュリティに関する全般的な方向性および行動指針を確立すること。

②事業上の要求事項および法的または規制要求事項、並びに契約上のセキュリティ義務を考慮すること。

③ISMS を確立し、維持するために必要な戦略上の視点からみた組織環境、並びにリスクマネジメントのための環境を整備すること。
④リスクを評価するための基準を確立し、定義されたリスクアセスメントの構造を確立すること。
⑤経営陣（社長、情報セキュリティ担当役員などの上位経営管理者）による承認を得ること。

１１４．情報セキュリティスタンダード

定義：情報セキュリティスタンダードとは、情報セキュリティ基本方針に基づき、情報システムのセキュリティ対策水準を定義したもの。情報セキュリティ基準ともいう。

解説：情報資産（情報システムを含む）に対するリスク分析を行った後、対象とすべきセキュリティ管理項目（ISMS 適用範囲）毎に管理目的と管理策を選択して定義する。セキュリティ対策の評価・監査等を行う場合の物指しとしても利用することができる。ISMS 適合性評価制度における ISMS 認証基準(Ver.2.0)の附属書：「詳細管理策」で示す項目は次のとおりである。

（１）人的セキュリティ
（２）物理的及び環境的セキュリティ
（３）通信及び運用管理
（４）アクセス制御
（５）システムの開発及び保守
（６）事業継続管理
（７）適合性

１１５．情報セキュリティプロシジャー

定義：情報セキュリティプロシジャーとは、情報セキュリティ基準に基づき、情報システムのセキュリティ対策を実施するため管理方法、運用手順等を具体的に規定したもの。情報セキュリティ実施手順ともいう。

解説：ISMS 適合性評価制度において例示されている情報セキュリティ実施手順には、以下のものがある。(NPO 日本ネットワークセキュリティ協会・セキュリティポリシーWG 活動報告「ポリシー・サンプルの解釈と応用」(2003.6.4))

１１６．情報セキュリティ監査

定義：情報セキュリティ監査とは、情報セキュリティに係わるリスクのマネジメントが効果的に実施されていることを担保するために、独立かつ専門的な立場から、組織体の情報セキュリティの状況を検証又は評価して、情報セキュリティの適切性を保証し、情報セキュリティの改善に役立つ的確な助言を行うこと。

解説：情報セキュリティを脅かすリスクが多様化し複雑化している現状に鑑み、平成 13 年４月１日から経済産業省による「情報セキュリティ管理基準」と「情報セキュリティ監査基準」の２本の柱からなる情報セキュリティ監査制度が策定・運用開始され、更には情報セキュリティ監査を行う主体を登録する「情報セキュリティ監査企業台帳」制度が創設（同年６月１日開始）された。

情報セキュリティ監査については、これらの制度の中の「情報セキュリティ監査基準」に規定されている。以下本基準に基づき概説する。本基準は、情報セキュリティ監査の目的、一般基準、実施基準、報告基準から構成されている。

まず、情報セキュリティ監査の目的においては、その目的を「情報セキュリティに係わるリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価し、もって保証を与えあるいは助言を行うことにある。」と規定している。

一般基準では､情報セキュリティ監査人が独立かつ専門的立場から監査ができるように、システム監査人の権限と責任、独立性、専門能力、守秘義務等について規定している。

実施基準では、情報セキュリティ監査人が実施する監査手続きの内容、時期及び範囲等について適切な監査計画書を立案し、この監査計画にも続き監査を実施することを規定している。監査証拠の入手と評価、監査調書の作成と保存などの具体的な作業のほか、監査体制の確立や、他の専門職の利用についても規定している。
報告基準では、監査報告書の提出と開示、監査報告の根拠ほか、特に監査報告書の記載事項について明確にしている。情報セキュリティ監査人が監査の目的に応じて必要と判断した事項（保証意見または助言等）については、明瞭に記載しなければならないと規定している。また、検証または評価については、情報セキュリティ管理基準に基づき行うこととしている。

（１）組織が策定した情報セキュリティ管理基準の妥当性を評価、確認する。
- ●定めた情報セキュリティ管理基準が、脅威に対抗するに十分なものとなっているか。
- ●外部要因の変化に応じたリスク分析に基づいた情報セキュリティ管理基準が制定されているか。

（２）組織が策定した情報セキュリティ管理基準の遵守状況､および実施状況を評価、確認する。
- ●定めた情報セキュリティ管理基準が遵守されているか。
- ●内部要因の変化に応じて、情報セキュリティ対策が適切に実施されているか。

（３）監査結果の評価については助言型監査と保証型監査の２つがある。

１１７．情報セキュリティマネジメントシステム（ISMS）

定義：ISMS とは、企業・組織におけるマネジメントシステム全体のなかで、事業リスクのアプローチに基づいて、情報セキュリティの確立、導入、運用、監視、見直し、維持、改善を行うプロセスのこと。

解説：JIPDEC で運用している「ISMS 適合性評価制度（Version2.0 H15.4.1)」では、企業・組織が自らの事業の活動全般およびリスク全般を考慮して文書化した ISMS を構築､導入、維持し、かつこれを継続的に改善していくプロセスとしている。ISMS の基準で使われるプロセスは、次の図に示す PDCA モデルに基づいている。(以下 JIPDEC の ISMS パンフレットから抜粋)

１．ISMS とは

ISMS とは、個別の問題ごとの技術対策の他に、組織のマネジメントとして、自らのリスク評価により必要なセキュリティレベルを決め、プランを持ち、資源配分して､システムを運用することである｡組織が保護すべき情報資産について､機密性、完全性、可用性をバランスよく維持し改善することが情報セキュリティマネジメントシステム(ISMS)の要求する主要なコンセプトである。

- ●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。
- ●完全性：情報および処理方法が正確であること及び完全であることを保護すること。
- ●可用性：認可された利用者が、必要なときに、情報及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。

2．ISMS のポイント

制定した情報セキュリティポリシー(基本方針)に基づき、次表の計画―実施―点検―措置のサイクルを継続的に繰り返し、情報セキュリティレベルの向上を図る。このサイクルを図示すれば、下図のとおりである。

Plan―計画 （**ISMS** の確立）	組織の全般的な基本方針及び目標に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関する情報セキュリティ基本方針、目標、対象、プロセス及び手順を確立する。
Do―実施 （**ISMS** の導入及び運用）	その情報セキュリティ基本方針、管理策、プロセス及び手順を導入し、運用する。
Check―点検 （**ISMS** の監視及び見直し）	情報セキュリティ基本方針、目標及び実際の経験に照らしてプロセスの実施状況を法化し、可能な場合にこれを測定し、その結果をも治しのために経営陣に報告する。
Act―処置 （**ISMS** の維持及び改善）	ISMS の継続的な改善を達成するため、マネジメントレビューの結果に基づいて是正措置及び予防措置を講ずる。

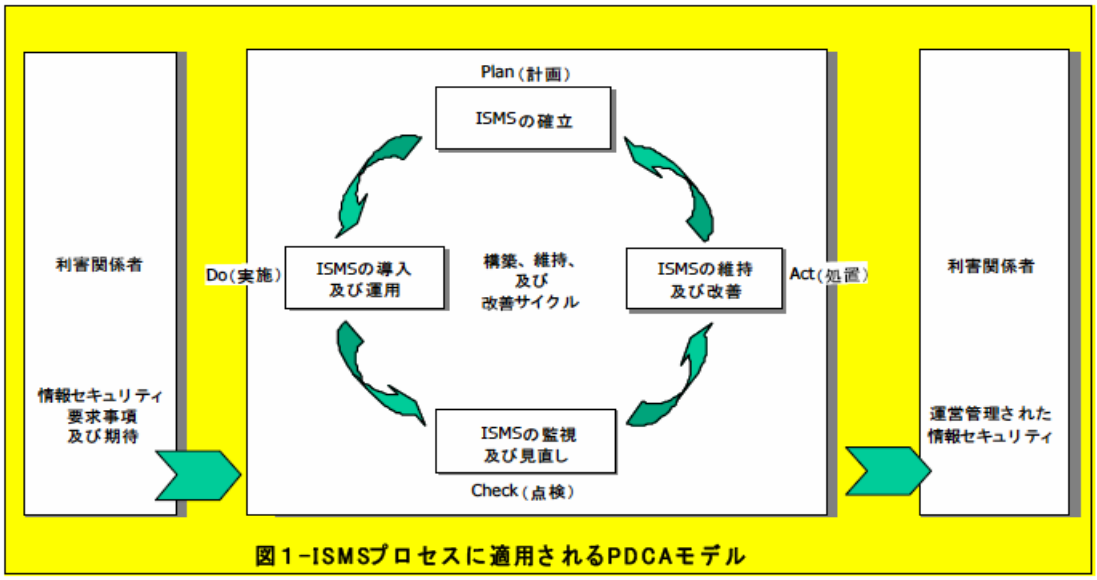


図１-ISMSプロセスに適用されるPDCAモデル

3．マネジメント枠組みの確立

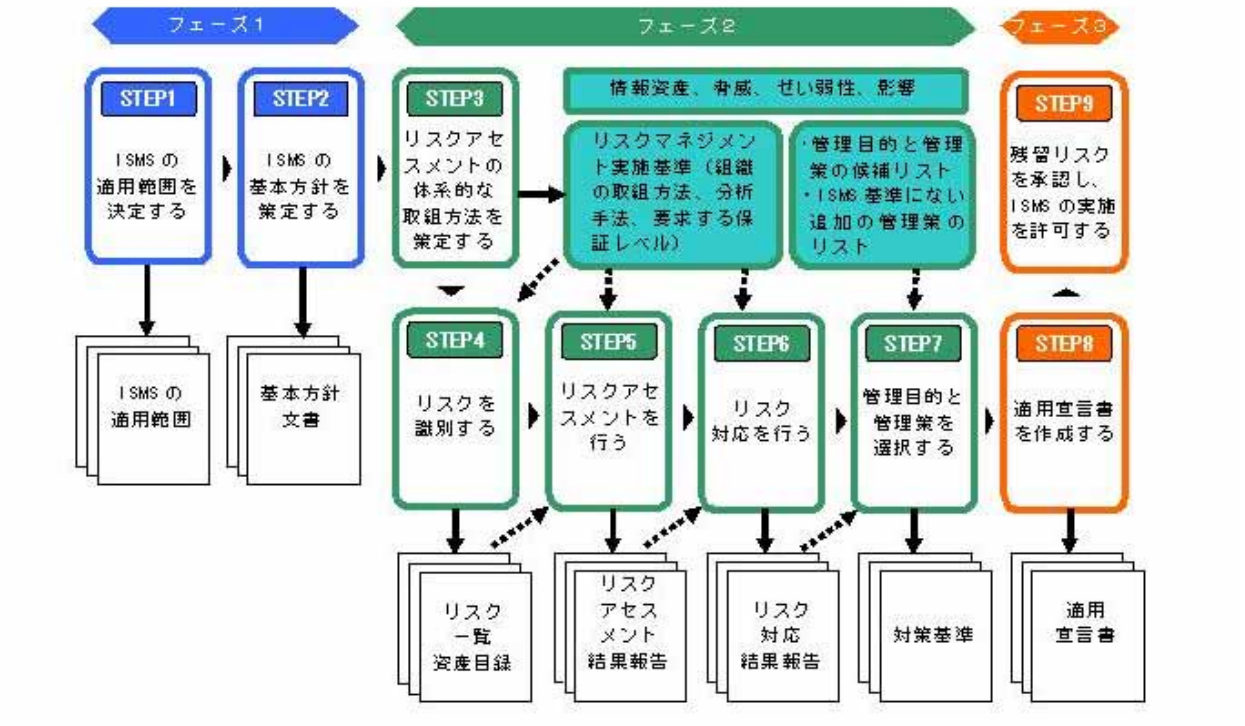
マネジメント枠組みに関する ISMS の要求事項は、情報セキュリティポリシー、管理目的、管理策、システム運用(実施)、さらには情報セキュリティ文書をはじめとするシステム文書、文書管理及び記録管理に関するものである。

この枠組みの確立にあたり ISMS の適用範囲を定義（STEP１）、情報セキュリティポリシーを策定(STEP２)する。策定した情報セキュリティポリシーに基づき、リスクアセスメントの体系的な取組方法を策定(STEP３)する。保護すべき情報資産対するリスクを識別（STEP４）し、リスクアセスメントを実施(STEP５)する。リスクア

セスメントの結果、リスクの受容ができない場合には、リスク対応の選択肢を評価（STEP６）する。リスク対応に基づき、実施すべき管理策を選択(STEP７)する。

詳細管理策
セキュリティポリシー セキュリティ組織 情報資産の分類及び管理 人的セキュリティ 物理的及び環境的セキュリティ 通信及び運用管理 アクセス制御 システムの開発及びメンテナンス 事業継続管理 準拠

「詳細管理策」にあるすべての管理策が実施されなければならないわけではなく、リスクアセスメントに基づき、管理策を選択して実施できる。特に重要なことは、この選択については適用宣言書で明確に公表(STEP８)することにある。また、上記の管理策だけでなく、組織がリスクアセスメントやリスクマネジメントの結果、何が残留リスクなのか、残留リスクはどの程度あるのかを明確にした上で経営陣が承認し、ISMS を運用することを許可（STEP９）する。各フェーズの関係を図示すれば次図のとおりである。



１１８．セキュリティホール

定義：セキュリティホールとは、情報資産保護のために講じているセキュリティ対策上の漏れ（弱点・欠陥）のこと。

解説：通常は、プログラムのバグに起因する不具合をさすが、関係者からパスワードを聞き出し、担当者に成りすましてシステム侵入することなど人的管理上の弱点などを含め広い意味で定義している。ハッカーやクラッカーは、このセキュリティホールを狙って攻撃をしてくるので、セキュリティホールを発見し、それを塞ぎ、また、セキュリティホールを攻撃された場合に迅速に対応する体制を整えておくことは、セキュリティ対策の最重要事項である。

セキュリティホールを攻撃された場合の具体的な被害例としては、①知らない間に WWW サーバ上の HTML ファイルが改ざんされてしまう、②ある WEB ページにアクセスした人のハードディスクの内容が消去されてしまう、③アクセスしてきた人の個人情報が盗まれる。等がある。

１１９．アクセスコントロール

定義：アクセスコントロールとは、情報システム資源への物理的／論理的なアクセス及び操作の制御のこと。

解説：物理的な制御としては、不正侵入を防止するための入退室管理、防犯設備、媒体機器への施錠等がある。論理的なアクセスコントロールとしては、ファイルやデータベース、ネットワークに対するユーザの不正なアクセスを防ぐための全ての対策が含まれる。通常、アクセスコントロールでは、最初にユーザのリソース使用権限の認証を行い、使用権限の有無を確認する。これにより不正使用の確認ができる。次に、アクセス要求種別がアクセス権の許容範囲かどうかを確認し、許容範囲内ならアクセスを許可する。また、アクセスの許可／不許可にかかわらず、アクセスログを記録し、随時または定期的にアクセス状況を分析できるようにしておくことも必要である。

１２０．暗号

定義：暗号とは、データの機密性を保持するために、平文（通常の文）を何らかの規則に従って変換し、そのままでは第三者にとって何を意味しているのかわからないデータに変換し、また、何らかの規則に従って元の平文に復元すること。この元の平文に復元することを「復号」という。

解説：現在広く使われている暗号の方法（暗号方式）を大別すると秘密鍵暗号方式と公開鍵暗号方式とがある。さらに秘密鍵暗号方式と公開鍵暗号方式を組み合わせたハイブリット暗号方式も利用されている。秘密鍵暗号方式（対象鍵方式ともいう）は、送信側、受信側で予め同一の暗号／復号のための鍵を用意して利用する方式である。

公開鍵暗号方式は、受信側で秘密鍵と公開鍵を用意し、公開鍵を送信側が入手できるように公開する。送信側は、予め受信側から公開された公開鍵を使用して暗号化し、データを送信する。受信側では、暗号化されたデータを自分の手元においた秘密鍵で復号する方式である。公開鍵方式は、第三者認証機関が発行する電子証明書や電子署名に広く用いられている。

暗号化技術の主なものとして、秘密鍵暗号方式に用いられる DES（Data Encryption Standard)と公開鍵暗号方式に用いられる RSA(Rivest-Shamir-Adleman の３人の頭文字)がある。

１２１．コンピュータウイルス

定義：第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムのこと。

解説：コンピュータウイルスとしての定義は、自己伝染機能、潜伏機能、発病機能のうち１つ以上を有しているものである。(「コンピュータウイルス対策基準」の用語の定義参照))

コンピュータウイルスは、ネットワークやフロッピーディスクなどを介して、コンピュータ内のファイルなどに密かに入り込み、そこからさらに別のコンピュータへと自分自身を複写して増殖していくことができ、特定の日時などの条件や、電子メールの開封といった特定の操作によって起動する様子が、人間や動物に感染して潜伏期間を経て発病する風邪（インフルエンザ）やエイズのウイルスに似ていることから、「コンピュータ･ウイルス」と呼ばれる。また、コンピュータウイルス対策プログラムをさして「ワクチン」ともいう。

コンピュータウイルス対策基準の３つの定義は、次のとおりである。

（１）自己伝染機能

自らの機能によって他のプログラムに自らをコピーしまたはシステムの機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

（２）潜伏機能

発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

（３）発病機能

プログラム、データ等のファイルを破壊したり、設計者の意図しない動作をする等の機能

また、最近、上記３つの機能をもち合わせていないウイルスプログラムが発見されており、それらも含めコンピュータウイルスと呼んでいる。

１２２．コンピュータウイルス対策

定義：コンピュータウイルス対策とは、コンピュータウイルスに対しての予防、発見、駆除、復旧などの対策を行うこと。

解説：1990 年２月、経済産業省（当時、通商産業省）は、コンピュータウイルスへの対策をとりまとめた「コンピュータウイルス対策基準」を制定し、その後 1995 年７月に改定された。新しい情報リスクとして出現したコンピュータウイルスに対し、それまでのセキュリティ対策基準を補完するため制定した。基準は、①システムユーザー、②システム管理者、③ソフトウェア供給者、④ネットワーク事業者、⑤システムサービス事業者の５つの対象ごとに、それぞれコンピュータウイルスに対する予防、発見、駆除、復旧

などの対策を具体的に示している。

１２３．コンピュータ犯罪

定義：コンピュータ犯罪とは、コンピュータが直接的あるいは間接的に介在した社会悪行為のこと。(通産省(現経済産業省)のコンピュータセキュリティ研究会による報告書「健全なる情報社会の構築に向けて（1982 年 10 月)」参照)

解説：ここでのコンピュータの「直接的」介在とは、電磁的記録の破壊あるいは偽造などのようにコンピュータシステムそのものに対して行われる機能阻害あるいは不正使用であり、「間接的」介在とは、コンピュータ･システム自体の使用は適性であるがこれを媒介にして不正な行為が行われることをいう。例えば、インターネットを利用した海賊版ソフトの販売や詐欺行為のことをさしている。

コンピュータ犯罪は、情報技術やネットワークの進展につれて犯罪手法も従来は考えられなかったものも出現してきているが、一般的に以下のように分類されている。

（１）金銭及び物品の不法領得
（２）情報関連資産の窃取
（３）情報関連資産の破壊
（４）情報サービスの盗用
（５）妨害行為

また、広義には、コンピュータを不正に使用したネットワーク犯罪、不正アクセス禁止法違反を含め、ハイテク犯罪と呼称している。(警視庁広報資料参照)

近年、国内では、コンピュータ犯罪対策として①不正アクセス禁止法(平成 12 年 2 月)、②個人情報保護法(平成 15 年 4 月)が法制化され、国際的には「サイバー犯罪防止条約」が検討されている。

１２４．コンピュータ不正アクセス

定義：コンピュータ不正アクセスとは、正規のアクセス権限のある者しか利用できないコンピュータに対して、他人（正規の利用権者以外の者）が、本人のパスワード等を利用して不正にアクセスすること。

解説：「不正アクセス行為の禁止等に関する法律（平成 12 年 2 月 13 日に施行)」(通称：不正アクセス禁止法）で禁止する行為は、①アクセス制御機能を有しているコンピュータ対して、②ネットワークを利用して、③本人のパスワード等（アクセス制限を免れることのできる情報、指令を含む）をコンピュータに入力する行為のことである。

以上の３つの要件が成立していれば、アクセスの結果として何もしていなくても法律違反となる。また、パスワード等のアクセス制御機能に係わる識別符号を正規の利用権者以外の者に対して提供した場合も不正アクセス行為を助長する行為として本法律違反となる。

《参考；コンピュータ不正アクセス対策基準》

コンピュータへの不正アクセスによる被害の予防、発見と復旧、拡大防止のために、企業や個人が取るべき対応策を定めたもの。経済産業省（旧通産省）が 1996 年８月に策定した。例えば、ID やパスワードを使ったユーザ認証を行ったり、データへのアクセ

スを制限したり、データ改ざんが起きた場合にはどのように対処するか、などのルールを決めておく。これらにより企業システムへの不正サクセスを防止するとともに、不正アクセスへの対処方法を明確にする。

１２５．情報セキュリティ（information security）

定義：情報の機密性、完全性および可用性の維持。（JIS X 5080:2002）

解説：組織経営に不可欠である情報は、適切に保護されなければならない。情報が適切に保護されていないと、漏洩したり、内容が不正確であったり、必要なときに使えない等、業務の遂行に支障をきたすリスクが発生する。情報セキュリティとは重要な情報をこのようなリスクから守ることをいう。また、機密性、完全性、可用性をさして情報セキュリティの３要素ともいう。関連用語：機密性、完全性、可用性の定義を参照。

１２６．脆弱性(vulnerabilities)

定義：脅威の発生を誘引する情報資産固有の弱点やセキュリティホールのこと。換言すれば、情報セキュリティに悪影響を与える可能性のある情報システムに内在する弱さの度合。（ISMS 認証基準ユーザーズガイド参照）

解説：脆弱性は、それだけでは何ら障害とはならないが、脅威を顕在化させ損害や障害を発生させる原因となる。逆をいえば脅威が存在しない脆弱性は、あまり気を配らなくてもよいことになる。

なお、脆弱性は、環境・施設、ハードウェア、ソフトウェア、組織などに大別し、さらに情報資産の特性や属性とそれらに対応する脅威との関連において個々に整理する。

１２７．個人情報

定義：個人情報とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより個人を識別することができるものを含む）をいう。（個人情報保護に関する法律（平成 15 年法律第五十七号　同年５月 30 日一部施行、平成 17 年４月１日全面施行）

解説：「個人情報」とは、生存する「個人に関する情報」であって、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む）をいう。「個人に関する情報、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、職種、肩書などの属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化されているかどうかを問わない。なお、死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となる。また、「生存する個人」には日本国民に限られず、外国人も含まれるが、法人その他の団体は「個人」に該当しないため、法人等の団体その他のものに関する情報は含まれない。（ただし、役員、従業員等に関する情報は個人情報）

（以上「個人情報保護に関する法律についての経済産業分野を対象とするガイドライン

（平成 16 年 10 月 22 日厚生労働省経済産業省告示第４号)」参照）

１２８．個人情報保護方針

定義：個人情報保護方針とは、事業者が個人情報を保護するための全般的な方針を定め文書化したもの。

解説：プライバシーポリシーともいう。以下、個人情報保護に関するコンプライアンス・プログラムの要求事項(JIS Q 15001)(平成 11 年４月２日)基づき解説する。事業者は、プライバシーポリシーを策定、文書化し、役員及び従業員に周知させるとともに、一般の人が入手可能な措置を講じなければならない。プライバシーポリシーに盛り込まなければならない項目は次のとおりである。

（１）事業の内容および規模を考慮した適切な個人情報の収集、利用及び提供に関すること。

（２）個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏洩などの予防及び是正に関すること。

（３）個人情報に関する法令及びその他の規範を遵守すること。

（４）コンプライアンス・プログラムの継続的改善に関すること。

なお、個人情報には、電子化されたデータのみならず、個人情報が記された書類等も全て含まれる。また、プライバシーポリシー（個人情報保護方針）を一般の人が入手可能な措置については、会社のホームページに掲載することなどが行われている。

１２９．プライバシーマーク制度

定義：個人情報の漏洩対策など適切なプライバシー保護措置を講ずる体制を整備し、個人情報の取扱いを適切に行っている事業者を日本情報処理開発協会（JIPDEC）が評価・認定し、その証として「プライバシーマーク」の使用を許諾する制度。

解説：本制度は、アメリカ、OECD 加盟国などの個人情報保護法制化の動きを受け、経済産業省の外郭団体である日本情報処理開発協会（JIPDEC）が、1998 年４月１日から制定・運用を開始している。認証取得のための個人情報保護に関するコンプライアンス・プログラムの要求事項は、1999 年３月 20 日に JIS 化（JIS Q 15001）された。事業者は、プライバシーマークを取得し、そのマークを事業活動の際に使用できるので、個人情報の保護に関する信頼獲得のインセンチブ（企業イメージアップ）が与えられ、一方消費者は、事業者の個人情報取扱いの適切性を容易に判断できる材料（プライバシーマーク）を得ることができる。

なお、プライバシーシール制度は、上記 JIPDEC のプライバシーマーク制度のほか、他にも幾つか著名な制度がある。

BBBOnline：米国 BBBOnLine は、米国やカナダの消費者を対象としてオンラインで業務を行う事業者が、ある一定の個人情報保護の規則を満たしているか審査認証して、プライバシーシールを付与する制度。JIPDEC のプライバシーマーク制度のモデルとなった制度で、プライバシーマークとの相互認証が可能である。

TRUSTe：インターネット上で公開、選択、アクセス、安全対策の４つのプライバシー原則への合意を示すサイトに、トラストマークと呼ぶシール表示が許可される制度。米国

基点で、シールを表示するサイトはTRUSTeによる監視および紛争調停にも合意する。

WebTrust制度：インターネット取引で、取引内容の開示、取引の正確な実施及び個人情報保護のための内部統制について、公認会計士がWebTrust原則及び規準に照らして監査し、「問題がない」場合にWebTrustシールを付与する制度。米国公認会計士協会及びカナダ勅許会計士協会が米国ベリサイン社の協力で共同開発し、1998年からサービスが開始された。

これらのプライバシーシール制度は、認可を受けた事業者のホームページや広告にシールが貼付されることにより、消費者が安心して取引できることの判断を容易にすることを目的としている。

１３０．監査リスク（audit risk）

定義：監査プロセスにおいて、十分な監査証拠を収集できなかったため、あるいは監査人が重要な問題を見逃したため、結果として誤った監査意見を表明してしまうこと。

解説：監査リスクを換言すれば、問題が無いのにあるといい、問題があるのにないという監査に内在するリスクを指している。一般に監査リスクは、固有リスク×統制リスク×発見リスクの積で表される。固有リスクは内部統制が存在しないと仮定した場合にその組織自体で監査証拠となるものに重要な虚位記載が発生する可能性をいう。統制リスクはその組織の内部統制によって重要な虚位記載を防止または発見されない可能性を指す。発見リスクは、監査人が内部統制において防止または発見されなかった重要な虚位記載を発見できない可能性を指す。

現在の監査において監査対象のリスクの大きさにより監査の程度や実施方法を定め、重大な問題が発生する可能性のあるところを重点に十分な監査証拠を入手しようとするリスクアプローチを用いることが主流となってきている。監査は日常業務への影響を最小限におさえることが求められており、時間や要員などの資源に限りがあるため、適切かつ重要な分野に絞って実施するが、監査リスクが内在することも考慮にいれておくことが必要である。

１３１．脅威 （threats）

定義：情報システムや組織に損失や損害をもたらすセキュリティ事故の潜在的な原因のこと。（ISMS認証基準ユーザーズガイド）

解説：脅威は、脆弱性により誘引され、顕在化することにより組織および組織の業務に影響を与える。脅威の大きさは、その要因や対象となる情報資産ごとにその発生の可能性を評価して決定される。

なお、脅威は、人為的脅威（意図的（計画的）脅威、偶発的脅威）と環境的な脅威に大別され、さらに、情報資産の特性や立地条件などの諸々の要因によって細分化する。

１３２．緊急時対応計画（contingency planning）

定義：緊急時対応計画とは、情報システムにおいて、大震災などの緊急事態が発生したときの行動や判断の基準、関連部門や組織トップの連絡体制、要員の安全確保策などを予め取り決めた計画のこと。

解説：通常発生するような故障は、緊急時対応計画に含めない。情報システムについては、地震や水害などの災害や、停電、通信回線の不通、あるいはサイバーテロなどへの対応などがある。具体的には、バックアップセンターの設置や、電源、通信回線の確保、復旧計画の立案、復旧後の切り替え手順などを定めておく。また緊急事態発生に備えた訓練計画と訓練の実施を含む。

１３３．リスク（risk）

定義：リスクとは、例えば、情報システムに対する脅威が現実化して損失が発生することがあるが、その「損失が発生する可能性」のこと。「リスクマネジメント－用語－規格において使用するための指針」（TR Q 0008:2003）では、リスクを「事象の発生確率とその結果の組み合わせ」と定義している。また、「リスクマネジメントシステム構築のための指針（JIS Q 2001:2001）」では、「事態の確からしさとその結果の組み合わせ、または事態の発生確率とその結果の組み合わせ」と定義している。

解説：本解説では、「TR Q 0008:2003」の定義をベースに解説する。リスクは、危害や危険あるいは損失そのものを指すものではなく、まだ発生していない危害や危険が発生する「可能性」を指している。このリスクは、まだ発生していない時点での不確実性（「可能性」）を表すものなので、そのままでは管理の対象とすることができない。管理するためには、具体的に把握できる実体としての対象が必要であり、リスクをもたらす「事象の発生確率（事態の確からしさ）」と「その結果」の２つの要素の組合せにより把握できるように定義されている。したがって、リスクを定義するには、「事象の発生確率」と「その結果」の２つの要素を定義することが必要である。この２つの要素を定義する方法として、幾つかの方法があり、代表的なものを以下に解説する。どの定義を採用するかは、業界や組織、リスクの対象とすべき資産の実態に即して適用できるものを選択することが重要である。

（１）事象の発生確率

一般的には、その事象がどの程度の確率あるいは頻度で発生するかを数学的な方法で説明することが可能である。確率で示せば「０≦発生確率≦１」である。このとき等号「＝」を含めることは、リスクが全く無いか、すべてがリスクであることを意味するのであり、リスクとして意味を成さないが、論理上あり得るものとして含めた。

また、発生確率の代わりに発生頻度や起こりやすさを階級や階層として選択されることがある。具体的な表現は、リスク算定参照。

（２）その結果

その結果とは、予定していた結果と実際の結果においてもたらされる損失との潜在的な差異のことである。予定していた結果がどのようなものであり、どのような損失をもたらすものかによりいろいろな定義がある。「影響」、「損失の大きさ」とも表現する。

一般的には、結果においてもたらされる損失を金額で示す。（損失の算出方法については、リスク算定を参照。）

以上の定義は、最初に示した「リスクマネジメント－用語－規格において使用するため

の指針(TR Q 0008:2003)」によるものであるが、情報セキュリティ分野（「IT セキュリティマネジメントのガイドライン（TR X 0036-1:2001)」）では「リスクとは、ある脅威が、資産または、資産グループのぜい（脆）弱性を利用して、資産への損失または損害をあたえる可能性」であると定義している。この定義のうち「可能性」を前記の「(１)事象の発生確率」に含めると「その結果」とは「脅威が資産の脆弱性を利用して資産に損失を与えること」といい換えることができる。
さらに、「その結果」に、好ましい状況を含める考え方と好ましい状況を含めない（好ましくない状況のみの）考え方がある。最近の考え方では、企業の経営者の判断の選択など戦略的な行為や企業の通常業務において為替や投資など成功すれば利益を生む行為もリスクに含めるのが一般的になってきている（TR Q 0008:2003)。
このように「その結果」(一般にリスクといわれる場合が多い。）には、利益と損失の両方を生み出す可能性のあるリスクと、安全に関する事項のように損失のみが生ずるリスクがあり、前者を「投機的リスク」、後者を「純粋リスク」として区別している。
なお、後者の安全の側面だけを扱う場合は、「安全性の側面－国際規格作成時での安全性の概念の取扱いに関するガイドライン(ISO/IEC Guide 51:1999)」の定義を利用することもできる。情報システムのリスクを取り扱う場合、情報システムの安全の側面のみを対象とするのであれば後者の定義を使用することも可能であるが、経営戦略を含めて広く情報システムに関わるリスクを対象とした場合は、前者の定義（TR Q 0008:2003）によることが至当であると考えられる。
以上のことからリスクは「事象の発生確率」と「その結果」の関数で示すことができる。（リスクの算定参照。）

リスク＝事象の発生確率（事態の確からしさ）×その結果（損失の大きさ）

参考に、情報システムに関わるリスクを例示しておく。

- システム投資に関するリスク（目標とするシステム効果が発揮できなかったリスクあるいは、予想以上のシステム効果が達成できたリスク）
- リスクマネジメントに関するリスク（リスクマネジメントが十分機能しないことなどによるリスク）
- システムの設計・開発段階でのリスク（機能の設計漏れ、開発の進捗遅れなどのリスク）
- テスト・移行段階でのリスク（テストの不十分さ、ずさんな移行計画などにより発生するリスク）
- 運用・維持段階でのリスク（震災、不正アクセス、情報漏えいなどのリスク）
- 組織的・人的リスク（担当者のモラールの低下、教育・研修不足などにより発生するリスク）

１３４．リスクアセスメント（risk assessment）

定義：リスクアセスメントとは、リスク分析からリスク評価までのすべてのプロセスのこと。

解説：リスクアセスメントは、リスクの対象とする資産（例えば、情報システム、データなど）に対するリスクを正確に捉え、分析し、評価するプロセスのことである。リスクアセスメントは、リスク分析とリスク評価の２つのプロセスに分かれ、更にリスク分析は、リスク因子の特定とリスク算定のプロセスに分かれる。（詳細は、リスク分析、リスク算定、リスク評価　参照）

リスクアセスメントの用語の使用例としては、「情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価する」（システム監査基準Ⅱ。システム監査の目的　抜粋）がある。ここでのリスクアセスメントは、「リスク分析を行いその評価に基づいてリスク対策が適切に行われて（コントロールされて）いるか」と、いい換えることができる。

情報システムの安全性や情報の信頼性を保つためには、資産に対するリスクが分析・評価され、それらのリスクに対する適切な対応が必要である。リスク分析により、すべてのリスク因子が抽出され、それらに対するリスクが算定され、評価するステップが重要となる。リスクに対する対策のみが先行すると、無駄な投資や対策漏れが生ずる。リスク分析はしたものの、それらのリスクに対する適切な対策が実施されないとリスクが発生する可能性が大となる。このような事態を避けるため、リスクとそのリスクに対する適切な対策を実施するため、リスクアセスメントのプロセスが必要である。

１３５．リスク分析（risk analysis）

定義：リスク分析とは、リスクに関する情報を調査・収集し、対象とするリスクを特定し、そのリスクの大きさを算定するプロセスのこと。（TR Q 0008）

解説：リスク分析は、リスクアセスメントにおける前段のプロセスであり、リスクの発見、リスクの特定、リスクの算定の各ステップにより、すべてのリスクを明かにし、そのリスクが発生する確からしさと影響度を明らかにする手順のことである。

リスク分析の最初の出発点はリスクの発見から始まる。組織（システム）に影響を与える可能性のあるものすべてのリスクを把握することが出発点である。実際には新たなリスクがつぎつぎと顕れるため日々注意が必要である。組織として一度発見したリスクは必ず記録し財産とする必要がある。発見したリスクの中から組織に重大な結果をもたらす可能性のあるものを特定し、その特定したすべてのリスクについて、リスクのもつ二つの要素であるリスクが顕在化する発生確率（確からしさ）とリスクが顕在化した場合の結果（影響の大きさ）を明らかにする。次にそれらのリスクの二つの要素を定量的または定性的に把握してリスクの算定を行う。

また、リスク分析については、リスクの発見、特定、算定のための様々な手法があり、これらを称して「リスク分析手法」という。分析には、定性的、定量的、また経営に資することを目的とした分析、設計などに反映させるための技術的分析など目的に応じて様々な手法がある。

リスク分析の最初のステップで行うリスクの発見は、具体的な計画策定の最初に行うリスクの発見はこの手法で行えば完璧というものはなく、組織の能力に依存するところが多い。関係者の経験、ブレーンストーミング、学会や同業他社の事故事例など出来る限

り多くの情報を集約することが一般的に行われる。
リスク発見の段階では個々のリスクの発生の蓋然性についての評価は行わず、特定のステップにおいて組織との関連性において検討すべきリスクを定める。
最後のステップは、リスク算定である。リスク算定により、個々のリスクに対する評価のための試料を提供することができる。
なお、ISMS 適合性評価制度において紹介されている「リスク分析手法」には、ベースラインアプローチ、非形式的アプローチ、詳細リスク分析、組合せアプローチ（複合アプローチ）がある。（ISMS 適合性評価制度ガイドライン参照：原出典は「IT セキュリティマネジメントガイドライン―第２部：IT セキュリティのマネジメント及び計画　TR X 0036-2:2001」）

１３６．リスク算定

定義：リスクの算定とは、それぞれのリスクの発生確率とその結果の値を設定するプロセスのこと。

解説：リスク算定は、リスクのもつ２つの要素であるリスクが顕在化する確からしさ（「発生確率」）とリスクが顕在化した場合の影響の大きさ（「その結果」）を定量的または定性的に把握して算定する。

リスク＝事象の発生確率（事態の確からしさ）×その結果（損失の大きさ）

定量的、定性的なリスク算定を例示すれば、以下のとおりである。本例は理解のための算定例であり、実務において想定損失値を算出するためには、更に詳細な算出根拠が必要となる。

（１）定量的方法

№	事　象	①発生確率 （発生頻度）	②その結果 （想定損失値）	③想定ﾘｽｸ値 ①×②	記　事
1	A事象	0.001	5,000	5	ﾘｽｸは小さい
2	B事象	0.010	1,500	15	
3	C事象	0.005	20,000	100	ﾘｽｸは大きい

（２）定性的方法

数値として把握できない場合は、点数を用いて表現することができる。（３段階、５段階評価など）

№	事　象	①発生頻度 （程度）	②想定損失値 （程度）	想定ﾘｽｸ値 ①×②	記　事
1	A事象	1	3	3	ﾘｽｸは小さい
2	B事象	5	1	5	
3	C事象	3	4	１２	ﾘｽｸは大きい

＜発生確率＞　考えられない（０）、まずない（１）、わずかである（２）、時々ある（３）、
多分ある（４）、しばしばある（５）
（日本語表現については、TR Q 0008:2003 用語の定義　参照）
＜想定損失値＞何もない（０）、少ない（１）、やや少ない（２、）中程度（３）
やや大きい（４）、大きい（５）、

（３）情報セキュリティに関する事例

情報セキュリティに分野については、想定損失値については、次の算出式を用いても同様に、定量的又は定性的に把握することができる。

想定損失値（リスク値）＝資産価値×脅威×脆弱性

№	事　象	①資産価値（程度）	②脅威（程度）	③脆弱性（程度）	リスク値 ①×②×③	記　事
1	A事象	1	2	1	2	ﾘｽｸは小さい
2	B事象	5	1	1	5	
3	C事象	3	3	2	１２	ﾘｽｸは大きい

(ISMS ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ（ISMS 認証基準（Ver.2.0）対応）　参照)

（４）定性的評価における留意事項

定量的評価については、「その結果」としての損失金額をどのように算出するかが重要なポイントとなる。例えば、人的被害（死亡・傷害）、財物損害（設備の損失）、信用失墜（個人情報漏洩）、利益損失（業務停止によるる機会損失）、賠償責任（民事訴訟）等すべてを金額として算出する必要がある。

定性的評価は、セキュリティ対策の選択に対しては容易である。（ベースラインアプローチ等）、しかし、金額算定が必要となる場合（リスク移転：保険）には、妥当となる金額を再算定する必要があり、改めて金額の算定が必要となる。したがって、リスク算定は、どのような利用目的で行うか予め利用目的を明確にして取り組むことが重要である。

算定のステップにおいては様々な手法が開発されている。情報セキュリティにおいてもTR X 0036-1：2001（ISO/IEC 13335-2:1997）では定性的な算定方法として、①ベースラインアプローチ、②非公式アプローチ、③詳細リスク分析、④組み合わせアプローチの４つの方法を示している。リスクマネジメントに関する規格ではオーストラリアニュージーランド規格（AS/NZS 4360）が参考になる。

このほか、フローチャート法、工程分析法、作業分析法、FMEA（Failure Mode and Effect Analysis）法、ETA（Event Tree Analysis)法、FTA（Fault Tree Analysis）法などがある。また定量的な算定方法においては統計分析のほかモンテカルロシミュレーションなどの手法も開発されている。

１３７．リスク評価（risk evaluation）

定義：リスクの大きさ（重大さ）を決定するために、リスク分析において算定されたリスクを、与えられた（あらかじめ用意された）リスク基準と比較・評価するリスクアセスメントにおける１つのプロセスのこと。(TR Q 0008)

解説：リスクのもつ２つの要素であるリスクが顕在化する「事象の発生確率（事態の確からしさ)」とリスクが顕在化した場合の「その結果（影響の大きさ)」を定量的または定性的に把握することがリスク算定であり、算定されたリスクの大きさ（リスク＝発生確率×影響の大きさ）を与えられたリスク基準と比較・評価して最終的な重要度を決定するプロセスがリスク評価である。

リスク評価において、それぞれ異質なリスクの重要性を比較する場合は、第１段階としてリスク算定における絶対的な数値を用い、第２段階としてそれぞれの算定値を評価基準と照らし合わせて相対的な評価値を出し、その結果を相互に比較することで評価をすることができる。

１３８．リスクコントロール（risk control）

定義：リスクマネジメントのプロセスにおいて、意思決定をする行動のこと。(TR Q 0008)

解説：リスクコントロールは、具体的には、リスクの顕在化の防止およびリスク顕在化の場合の影響度を局限化するための諸施策について意思決定をすることである。リスク対策ともいう。広義においては事業体の経営理念の実現を阻害するすべての要素を排除するためのすべての活動、内部統制などに近い概念で表現されることもある。

リスク対策は通常、リスク回避、リスク低減、リスク移転、リスク保有の４つを組み合わせて選択して行う。リスク対策の４つの概念は、次のとおり。

リスク回避：リスクのある状況に巻き込まれないようにすること、又はリスクのある状況から撤退する行為。

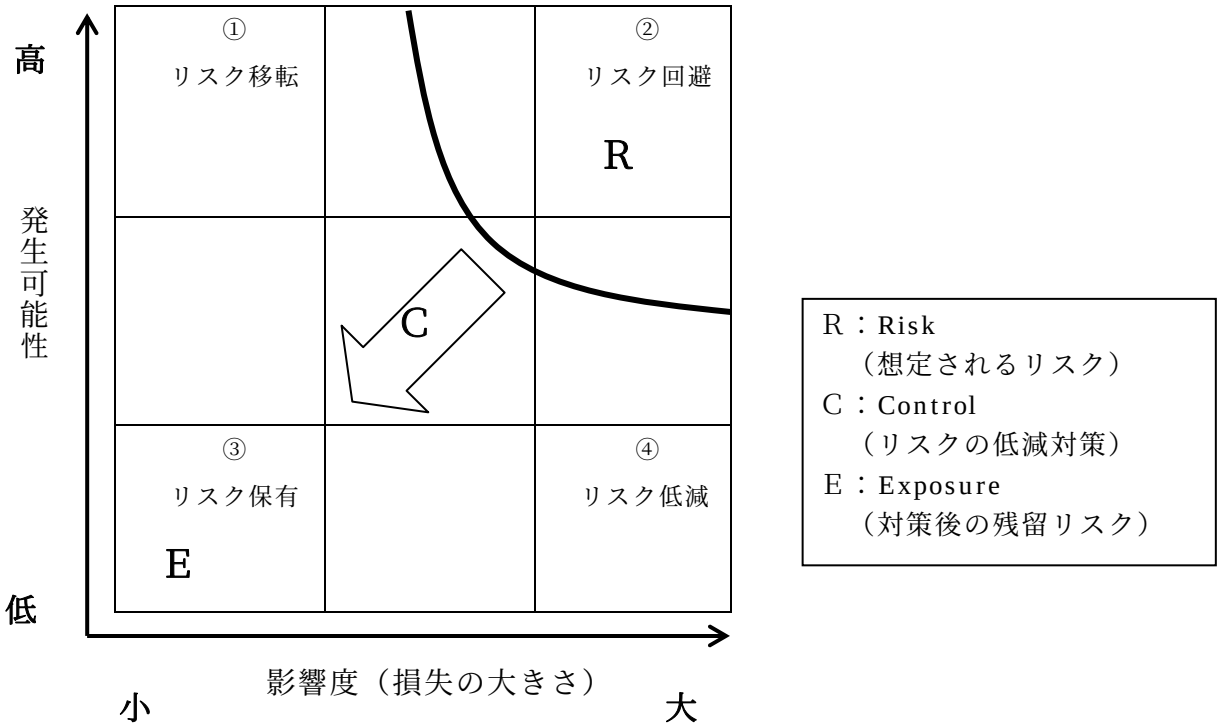
リスク低減：リスクに伴う発生確率若しくは好ましくない結果、又はそれらの両方を小さくするために取られる行為。一般のリスク対策を行うこと。

リスク移転：リスクに関して、損失の負担、又は利益の恩恵を他社と共有すること。保険に加入することなどが含まれる。

リスク保有：あるリスクからの損失の負担又は利益の恩恵を受容すること。何も対策を講じないで、損失が発生した場合は、自らその損失を負担すること。また、リスク低減対策を実施してもなおリスクが残ることが想定される。これを「残留リスク」といい、最終的には、「リスク保有」に含めて取り扱うこととなる。

なお、リスクそのものに利益を含むことが一般的になってきたため、TR Q 0008:2003(ISO/IEC Guide 73:2002)では「リスク低減」を「リスク最適化」と呼ぶこととなった。

リスク低減およびリスク対策について図示すれば次のとおりである。Ｒ，Ｃ，Ｅは、リスク低減を意味し、①、②、③、④は、リスク対策のとるべき考えかたを示している。



リスク低減の概念

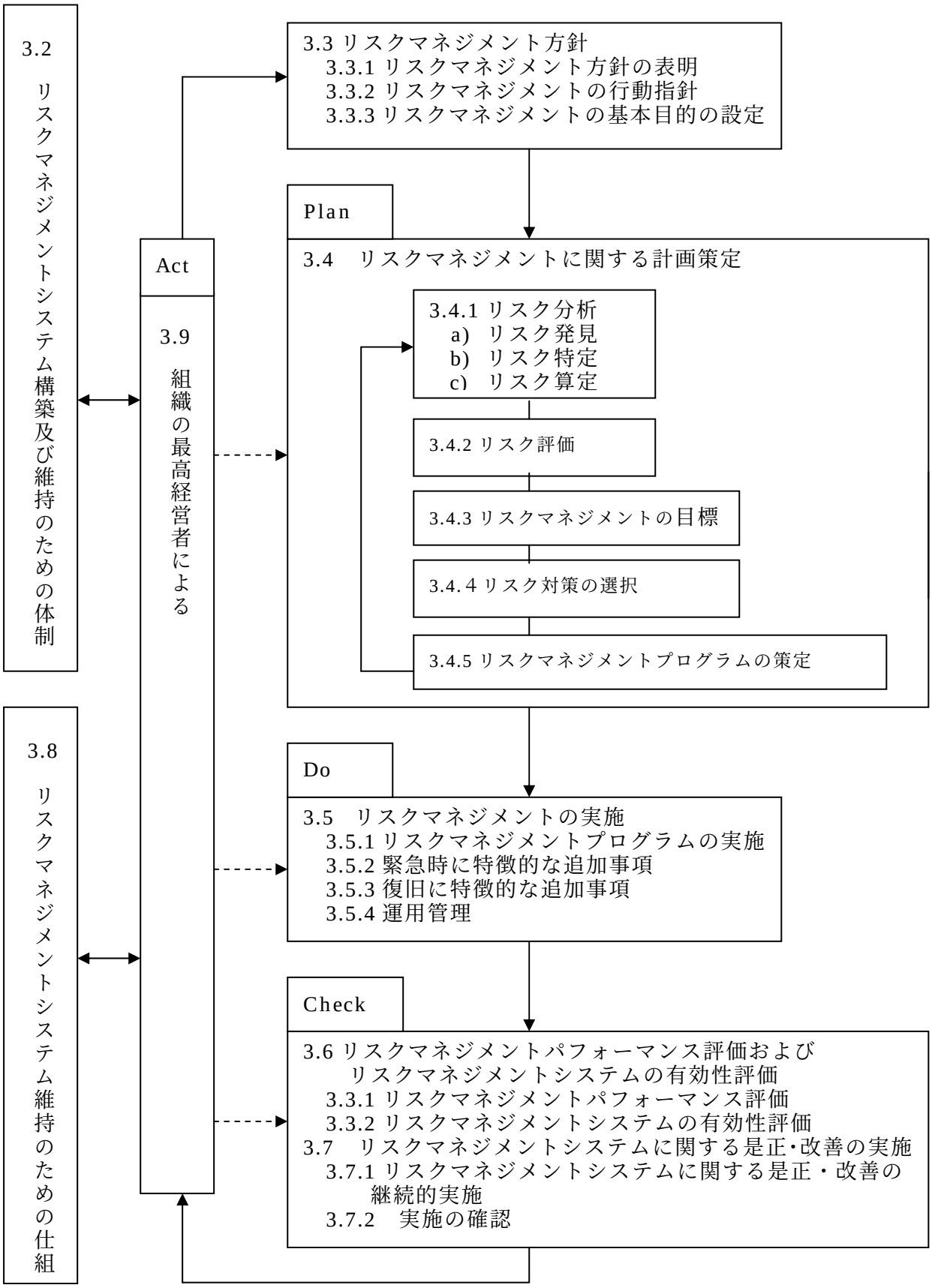
１３９．リスクマネジメント（risk management）

定義：リスクマネジメントとは、リスクに関して、組織を指導し管理する調整されたすべての活動のこと。(TR Q 0008)

解説：リスクマネジメントには、一般にリスク算定、リスク評価、リスク対応、リスク受容、およびリスクコミュニケーションを含む。古典的なリスクマネジメントでは、リスクの算定評価を行い、リスク対応（リスクコントロール）を通じて最小の費用で、リスクによる不利益の影響を最小化すること、などの定義がされ、最小のコストでリスクを最小化することを中心に定義されることが多い。

一方、この TR Q 0008:2003 による定義は、リスクそのものに利益を含むため、リスクマネジメントの定義も適切な利益のためにはコストが必ずしも最小でなく合理的であればよいため、このような幅広い定義となっている。

なお、リスクコミュニケーションは最近重要視されている概念で、株主、取引先、住民、自治体、従業員などなどステークホルダー（利害関係者）と事業者のリスクに関する情報を共有することである。リスクマネジメントの考え方を図示すれば次図のとおりである。



リスクマネジメントシステムのプロセスモデル

（図表引用　JIS Q 2001　リスクマネジメントシステム構築のための指針）

＜参考＞　　**リスク関する一般的な用語の定義／説明**

№	規格等 ／ 適用方法 ／ リスクに関する用語	JIS Q 2001 リスクマネジメント	TR Q 0008 正負のリスク	GUIDE 51 安全の分野	JIS X 5080 ISMSの実践規範	ISMS評価制度 リスクアセスメント	同左ユーザーズガイド リスクアセスメント	記事
1	リスク	○	●	●	○			
2	結果		○					
3	発生確率		○					
4	事象		○					
5	リスク因子(source)		○	(○)				＝hazard
6	リスク基準	○	○					
7	リスクマネジメント	○	○		○	○	○	management
8	リスクマネジメント基本目的	○						
9	リスクマネジメント行動指針	○						
10	リスクマネジメントシステム	○	○					
11	リスクマネジメントｼｽﾃﾑ担当	○						
12	リスクﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ担当責任者	○						
13	リスクマネジメントの目標	○						
14	リスクマネジメントﾊﾟﾌｫｰﾏﾝｽ	○						
15	リスクマネジメント文書	○						
16	リスクマネジメント方針	○						
17	ステークホルダー		○					
18	利害関係者		○					
19	リスクの認識		○					
20	リスクコミュニケーション		○					
21	リスクアセスメント		●	●	○	○	○	assessment
22	リスク分析		●	●		○	○	analysis
23	リスク特定		○					
24	リスク因子の特定		○				○	source
25	リスク算定		●					

26	リスク評価	○	○	○		○	○	evaluation
27	リスク対応		○			○	○	treatment
28	リスクコントロール		●					
28	リスクの最適化		○					＝ﾘｽｸ低減
30	リスクの低減	○	○					
31	軽減		○					
32	リスク回避	○	○					
33	リスク移転	○	○					
34	リスクファイナンシング		○					
35	リスクの保有	○	○					retention
36	リスクの受容		○			○	○	acceptance
37	リスク発見	○						
38	残留リスク		○	○		○	○	
39	緊急事態	○						
40	継続的改善	○						
41	組織の最高経営者	○						
42	リスク対策	○						
43	リスク発見	○						
44	安全（性）(safety)			○				
45	危害(harm)			○				
46	危険事象(harmful event)			○				
47	危険源(hazard)			○				=ﾘｽｸ因子
48	危険状態 (hazardous situation)			○				
49	許容可能なﾘｽｸ(tolerable risk)			○				
50	保護方策(protective measure)			○				
51	意図する使用			○				
52	合理的に予見可能な誤使用			○				

（注 1）JIS Q 2001 (2001.3.20)

（注 2）TR Q 0008 (2003.2.1)

（注 3）ISO/IEC GUIDE 51 (1999(E))

（注 4）JIS X 5080:2002

（注 5）ISMS 認証基準（Ver. 2.0）←JIS X 5080:2002 準拠 ＋ JIS X 5080:2002

（注 6）ISMS ユーザーガイド(ISMS 認証基準（Ver. 2.0）対応←JIS X 5080:2002 準拠

（注 7）●：用語集に採用の定義

（注 8）○：それぞれに定義あり

■参考 URL

独立行政法人情報処理推進機構:情報処理技術者試験センター
http://www.ipa.go.jp/
特定非営利活動法人日本システム監査人協会
http://www.saaj.or.jp/
システム監査学会
http://www.sysaudit.gr.jp/
ISACA（Information Systems Audit and Control Association）
米国本部　http://www.isaca.org/
日本支部　http://www.isaca.gr.jp/
日本内部監査協会
http://www.iiajapan.com/
特定非営利活動法人日本セキュリティ監査協会
http://www.jasa.jp/
（財）金融情報システムセンター
http://www.fisc.or.jp/