COBIT™
フレームワーク

1998年4月
第2版

COBIT運営委員会および
情報システムコントロール財団

COBITの使命：
ビジネスマネジャーおよび監査人が日々利用するために
権威のある，最新の，国際的に一般に認められた
情報テクノロジーコントロール目標の体系を
調査し，開発し，公表し，推進すること

目　次

謝辞 4-5

経営者のための要約 7-8

背景 9-10

COBITフレームワーク

状況設定. 11-13
フレームワークの原則. 14-18
要約－高いレベルのコントロール目標 19
COBITフレームワーク利用の手引. 20-21
詳細－高いレベルのITコントロール目標. . . . 22-55

付録

Ⅰ. COBITプロジェクトの説明. 56-57
Ⅱ. 基本的資料一覧. 58-59
Ⅲ. 用語集 60

利用上の注意

情報システムコントロール財団と CobiT のスポンサーは，「情報システムおよび関連技術のための内部統制目標(Control Objectives for Information and Related Technology)」製品をを主に内部統制専門家のための教育用資料として作成した。情報システムコントロール財団とそのスポンサーはこの使用による結果がすべて成功を納めることを保証するわけでない。この製品はすべての適切な手続きとテストを包んでいるわけではない。また，同じ結論を得るための合理的に指示された他の代替手続きやテストを排除するものでもない。内部統制専門家は手続きやテストが適切であるかどうかを決定する際に，特定のコントロール環境に対する特定のシステムまたは情報技術に向けられた環境についての専門家としての判断を下すべきである。

情報システムコントロール財団
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
電話: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: research@isaca.org
Web site: www.isaca.org

ISBN 0-9629440-4-1 (フレームワーク)
ISBN 0-9629440-3-3 (CD-ROM 付き 5 分冊)

印刷：アメリカ合衆国

謝 辞

Principal Global
Corporate Sponsors

協賛企業

Fellesdata a/s, Norway
NoviT a/s, Norway

主要な協賛ISACA支部

Benelux
National Capital Area
New York Metropolitan
Norway
Toronto

協賛ISACA支部

Adelaide
Atlanta
Auckland
Austin
Bangkok
Brisbane
Canberra
Central Arkansas
Central Indiana
Central Maryland
Central New York
Denver
Detroit
Finland
Greater Hartford
Hawaii
Houston
Hudson Valley
Indonesia
London
Los Angeles
Middle Tennessee
Minnesota
New England
New Jersey
New Mexico
North Alabama
North Texas
Northeast Ohio
Northern United Kingdom
Philadelphia
Pittsburgh
Puget Sound
Research Triangle
Sacramento
San Diego
Santiago de Chile
Seoul
South Texas
St. Louis
Sweden
Tokyo
Tulsa
Victoria
Virginia
Wellington
Winnipeg

功労者

Bill Bartgis
John Beveridge
William Bialkowski
Allen Bragan
Maryanne S. Canant
Michael Donahue
John Lainhart
Akira Matsuo
Teresa McCauley
Robert G. Parker
Daniel Ramos
Deepak Sarup
Lily Shue
Patrick Stachtchenko
Kevin Weston

プロジェクトチーム

Erik Guldentops, S.W.I.F.T. S.C., Belgium
Eddy Schuermans, Coopers & Lybrand, Belgium
Thomas Lamm, ISACF, USA

プロジェクト運営委員会

Erik Guldentops, S.W.I.F.T. S.C., Belgium
John Beveridge, State Auditors' Office, Massachusetts, USA
Prof. Dr. Bart De Schutter, Vrije Universiteit Brussels, Chairman BRT Belgium
Gary Hardy,Arthur Andersen, United Kingdom
John Lainhart,Inspector General, U.S. House of Representatives, USA
Akira Matsuo,Chuo Audit Corporation, Japan
Eddy Schuermans,Coopers & Lybrand, Belgium
Paul Williams,Arthur Andersen, United Kingdom
Thomas Lamm, ISACF, USA

調査

Vrije Universiteit Amsterdam, The Netherlands
Prof. M.E. Van Biene-Hershey
Ren・Barlage, RB Consultants
California Polytechnic University, USA
Prof. Dan Manson, Lead Researcher

専門家によるレビューーヨーロッパ

Chris Bagot,NATO
Ren・Barlage,RB Consultants
Prof. Dr. Henri Beker,Zergo, Ltd
John Beveridge,ISACA Past International President
Erik Guldentops,S.W.I.F.T. S.C.
Gary Hardy,Arthur Andersen
Eddy Schuermans,Coopers & Lybrand
Alan Stanley,European Security Forum
Danny Van Riel,Johnson & Johnson
Bram Vandenberg,Ernst & Young

専門家によるレビューーUSA

謝 辞

Prof. Ulric J. Gelinas, Bentley College
John Hayes, Price Waterhouse LLP
Greg Hedges, Arthur Andersen & Co., S.C.
Dave Kent, Price Waterhouse LLP
Tom Kothe, Ernst & Young LLP
John Lainhart,Inspector General, U.S. House of Representatives
Robert Roussey, University of Southern California

品質保証

Gary Austin,GAO
Chris Bagot,NATO
Rick Beatty, California Federal Bank
Peter De Koninck, Coopers & Lybrand
Balencia Dozier, Manufacturers Bank
Doris Gin, Arthur Andersen & Company LLP
A.I. Heijkamp, Computercentrum VSB
Max Huijbers, Rijkscomputercentrum
Peter Maertens,NATO
Bill Pepper,Zergo, Ltd.
Mark Stanley,Santa Barbara Bank
Tjerk Terpstra,Inter Access
Mark Wheeler,Farmers Insurance
Carla Williams,Executive Consultants.

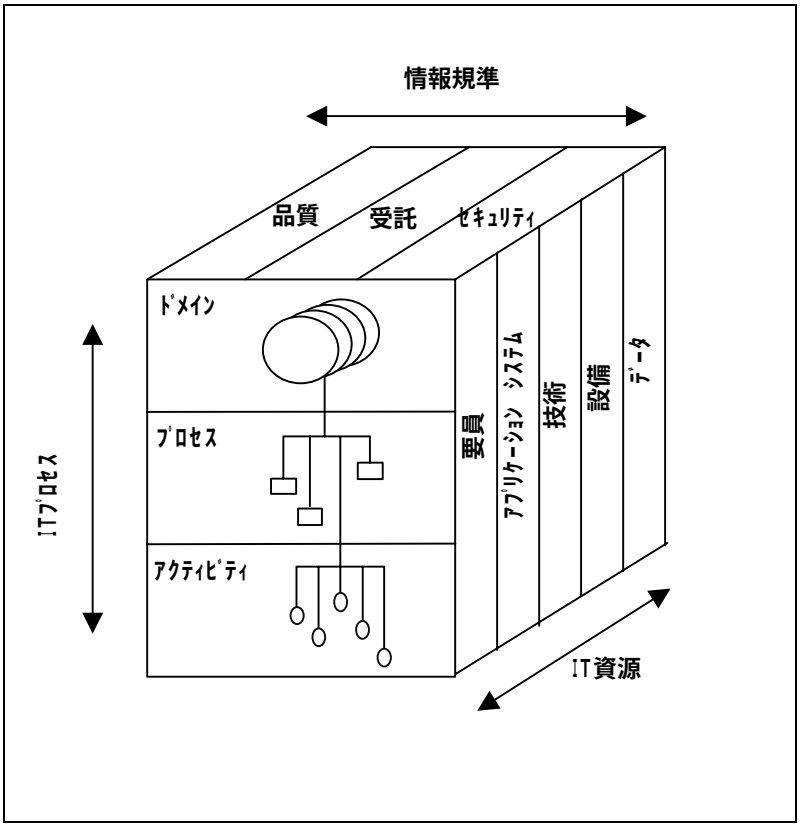
Special Thanks to the members of the Board of the Information Systems Audit and Control Association and Trustees of the Information Systems Audit and Control Foundation for their continuing and unwavering support of the COBIT Family of Products.

COBITフレームワークとコントロール目標の利用ガイド

異なった視点，異なった役割

概念的なフレームワークは，１）IT資源，2）情報のビジネス規準，3）ITプロセスという３つの視点からアプローチできる。これらの異なった視点により，フレームワークを効率的にアクセスできる。

例えば，企業の管理者は，品質，セキュリティあるいは受託について関心（７つの特定の情報規準にフレームワークによって説明される）をもって見たいかも知れない。IT管理者は，自ら責任があるIT資源を考慮したいかも知れない。プロセスのオーナ，IT専門家およびユーザは，特別のプロセスに特定の興味をもっているかも知れない。監査人は，コントロールの適用範囲の見地からフレームワークにアプローチしたいかも知れない。

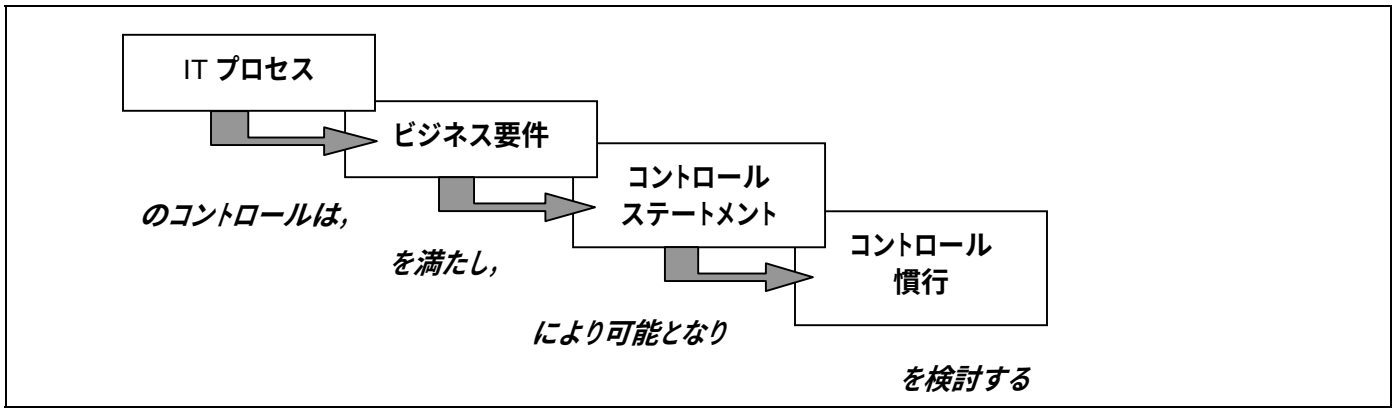


COBITフレームワーク

COBIT *フレームワーク*は，ある特定ITプロセスにおけるビジネスニーズという形態で，高いレベルにおけるコントロール目標だけが提示され，そのビジネス要件は，コントロールステイトメントによって可能となり，潜在的に適用可能なコントロールが検討される必要がある。

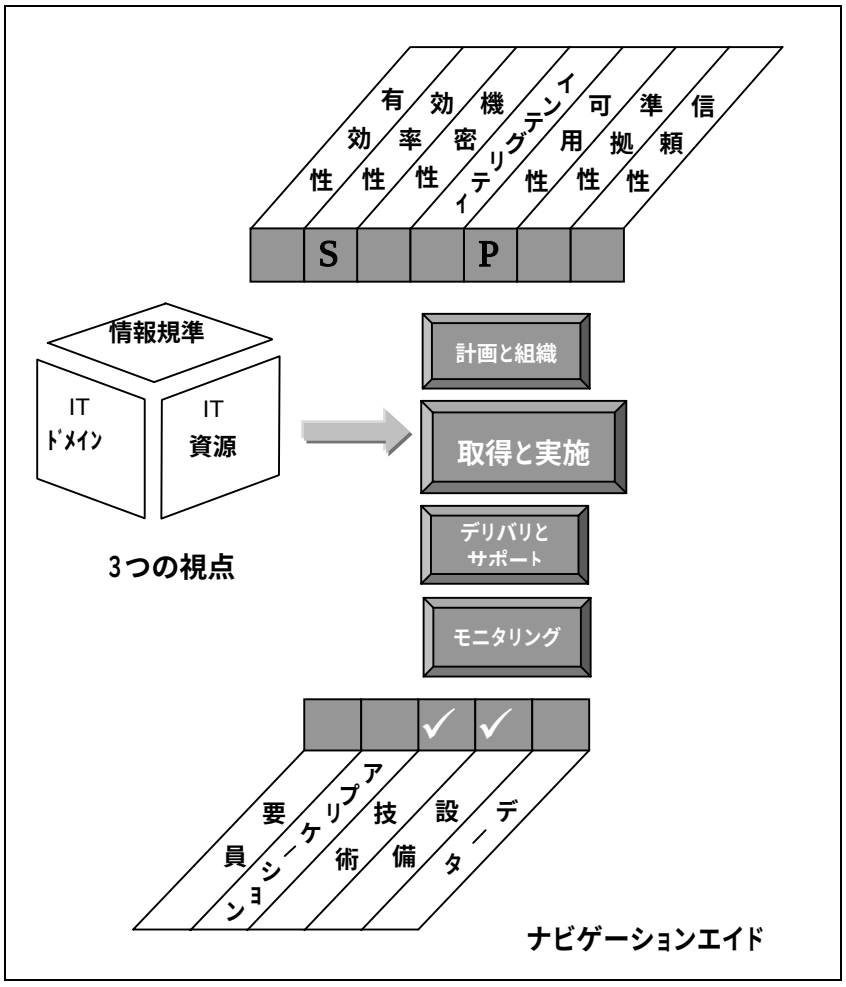
ITコントロール目標は，プロセス／アクティビティによって体系化されているが，ナビゲーションエイドは，上で説明されたような任意の視点から入れるように提供されるだけでなく，これらのエイドは，例えば，プロセスの導入／実施，プロセスの包括的な管理責任，プロセス毎のIT資源の利用というように結合され，または全体的なアプローチを可能にする。

ITコントロール目標は，つまり，技術プラットフォームに依存しないで一般論的に定義されているが，その一方でいくつかの特別な技術環境に対しては，コントロール目標が別途必要かも知れないことに留意しなければならない」。

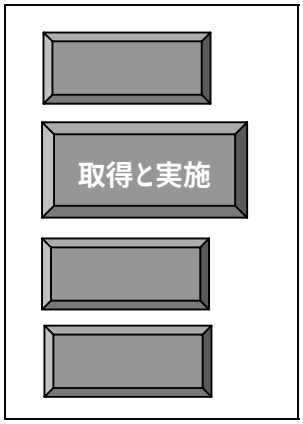


ナビゲーションエイド

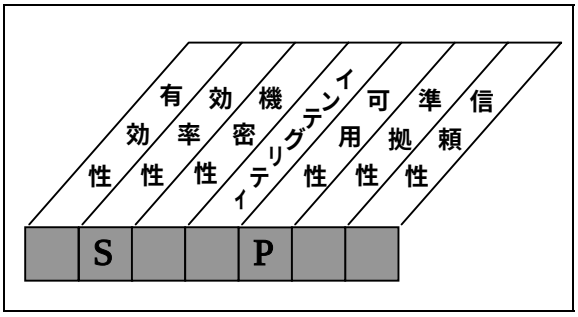
異なった視点をサポートするコントロール目標を効率的に使用するために，ナビゲーションエイドが高いレベルにおけるITコントロール目標の表現手法として提供される。COBIT *フレームワーク*に沿ったプロセス，資源，情報規準の３次元の各々は，ナビゲーションエイドによってアプローチできる。



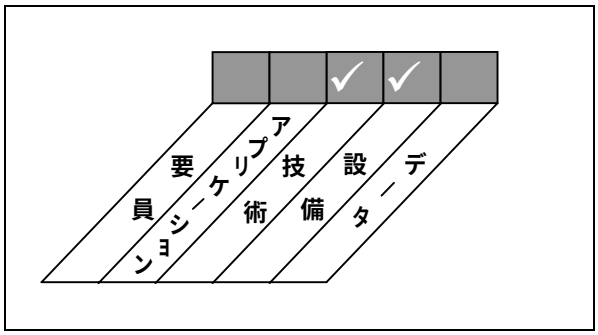
ITドメインは，コントロール目標の各頁の右上の角にこのアイコンで示され，レビュー対象のドメインが最もみ明るくされ，拡大して表示される。



情報規準への手掛かりは，どの規準が各々の高いレベルのITコントロール目標に適用可能であり，また，どの程度（第一次的か第二次的）までかを識別するこの小さなマトリックスによって，*コントロール目標*セクションの上部の左側角に表示される。

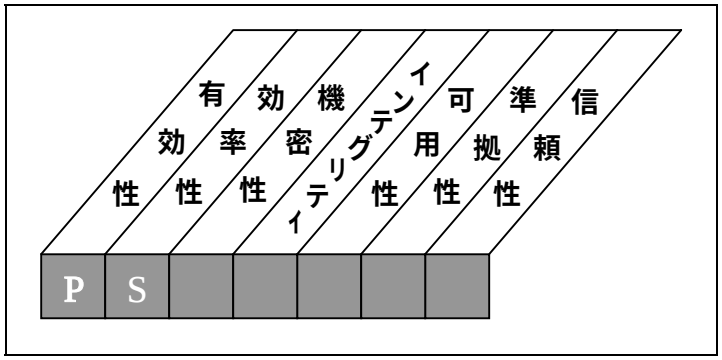


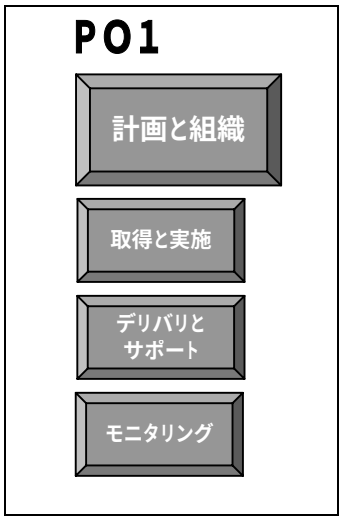
*コントロール目標*セクションの右下の角にある第二の小さなマトリックスは，検討中のプロセス（プロセスに単に参画しているものではない）によって特に管理されるIT資源を識別する。例えば，「データ管理」プロセスは，特にデータ資源のインテグリティと信頼性に集中しているが，一方，可用性と機密性はデータ（つまり，アプリケーションと技術）を使用する資源を管理するプロセスを通じて主に提供される。



高いレベルのコントロール目標

計画と組織





ITプロセスのコントロール

戦略的なIT計画の定義

満たされるビジネス要件

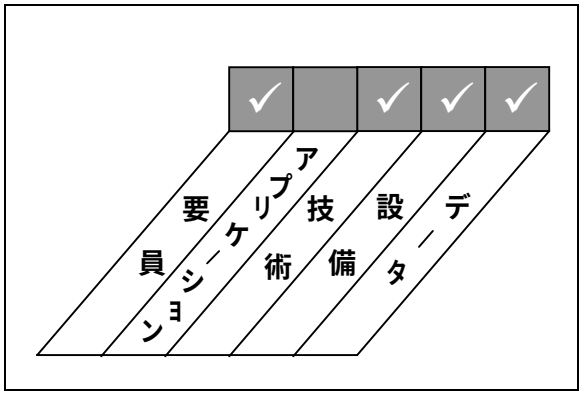
最適なバランスをさらに達成することを保証するのとともに，ITの機会とITビジネスの要件の最適なバランスを作り出すこと

実施方法

これは，長期計画を作成するもととなる定期的に行われる戦略的な計画プロセスによって可能となる。長期計画は，定期的に，短期の明確で具体的な目標を設ける業務計画に引き直されること

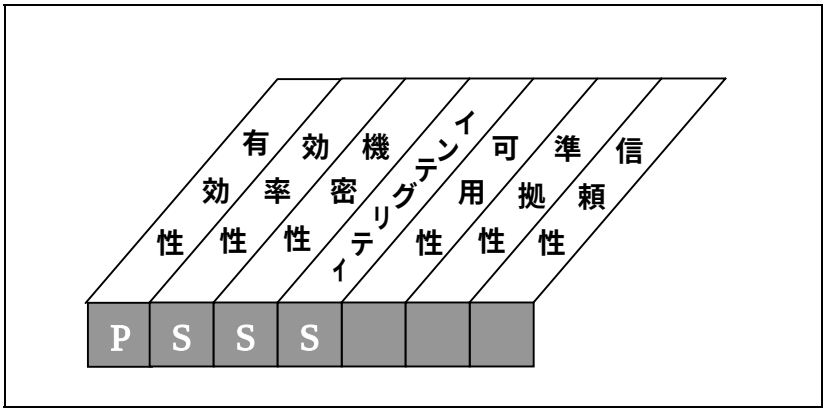
検討項目

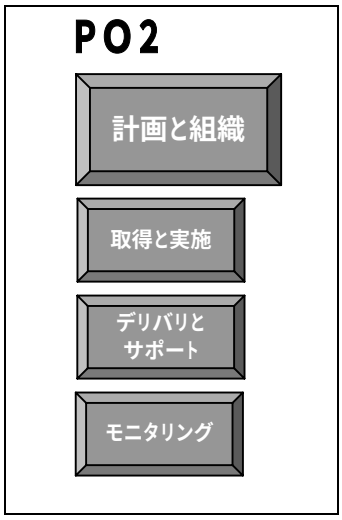
- **ビジネス目標の定義とITの必要性**
- **技術的解決策の一覧とインフラストラクチャの現状**
- **「技術監視」サービス**
- **組織の変更**
- **適時な実行可能性の研究**
- **既存システムの評価**



高いレベルのコントロール目標

計画と組織





ITプロセスのコントロール

情報基盤の定義

満たされるビジネス要件

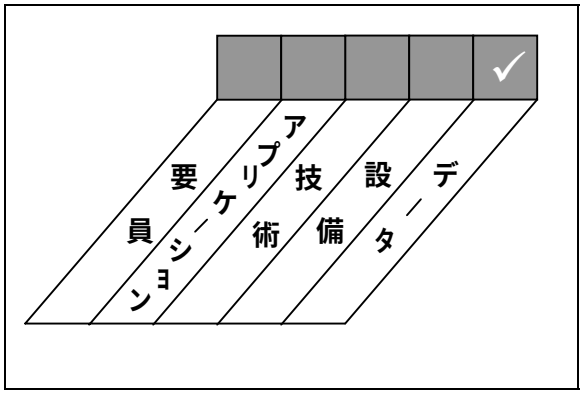
情報システムを最高に組織化すること

実施方法

ビジネス情報モデルの作成，保守およびこの情報の利用を最適化するために適切なシステムが定義されることを保証する

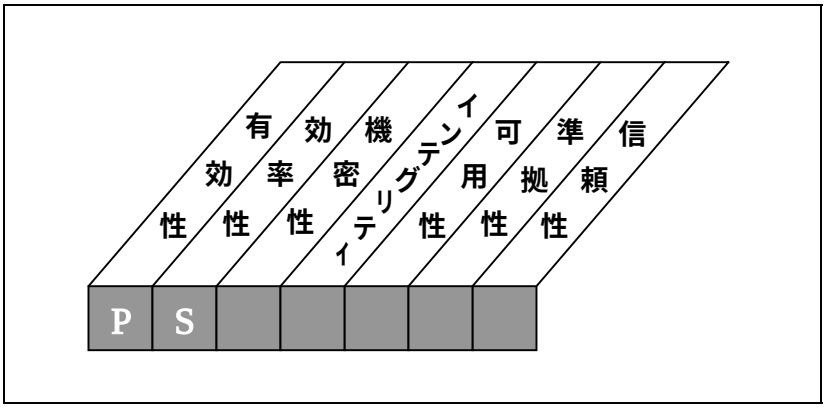
検討項目

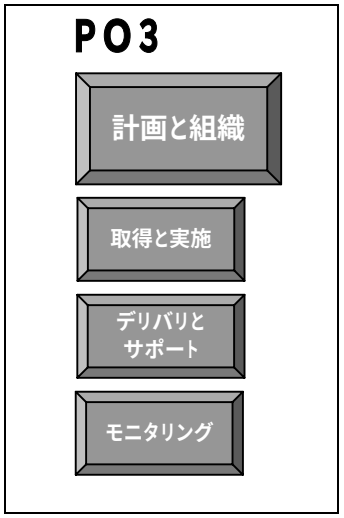
- 文書化
- データ・ディクショナリ
- データ構文規則
- データオーナーシップと重要度分類



高いレベルのコントロール目標

計画と組織





ITプロセスのコントロール

技術指針の決定

満たされるビジネス要件

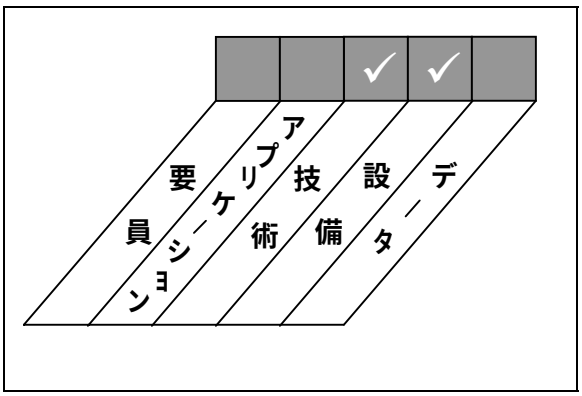
利用可能なそして先端技術を活用すること

実施方法

技術的なインフラストラクチャ計画の作成と保守

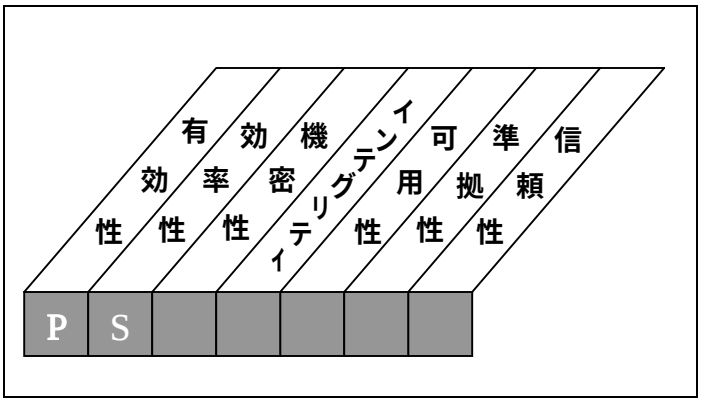
検討項目

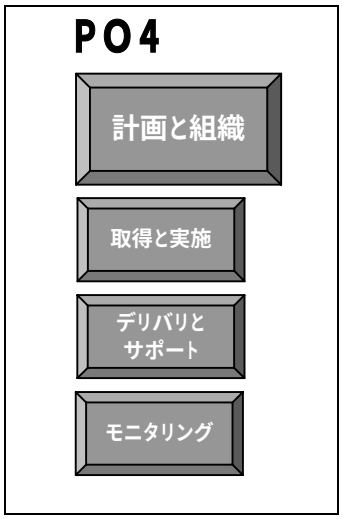
- **現行インフラストラクチャの適切性と発展の将来性**
- **技術開発のモニタリング**
- **コンテンジェンシー**
- **取得計画**



高いレベルのコントロール目標

計画と組織





ITプロセスのコントロール

IT組織と関連の定義

満たされるビジネス要件

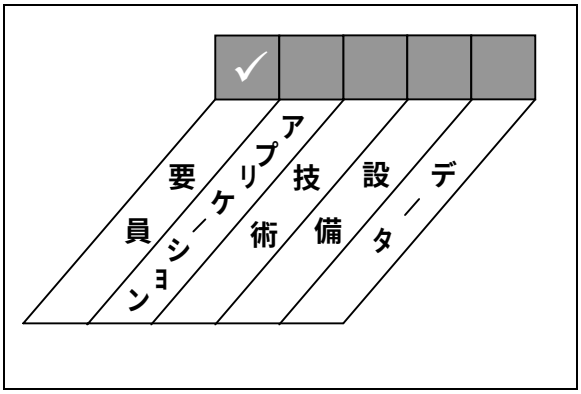
ITサービスの提供

実施方法

役割と責任が定義され，伝達されることを伴った人数と技能に適切な組織

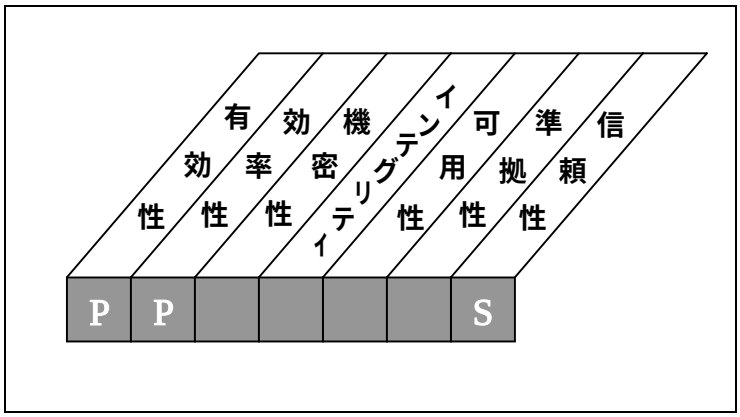
検討項目

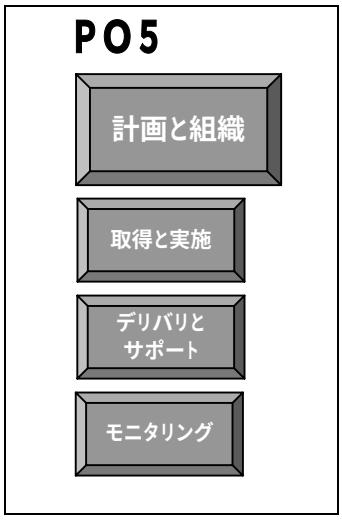
- 運営委員会
- ボードレベルの責任
- オーナーシップ，カスタディアンシップ
- 監督
- 職務の分離
- 役割と責任
- 職務記述
- スタッフの水準
- 重要な要員



高いレベルのコントロール目標

計画と組織





ITプロセスのコントロール

IT投資の管理

満たされるビジネス要件

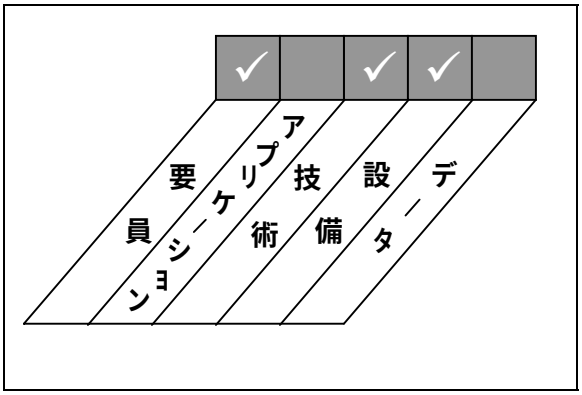
資金面を保証し，金融資源の支払いをコントロールすること

実施方法

定期的なIT投資と業務予算が本務によって作成され，承認される

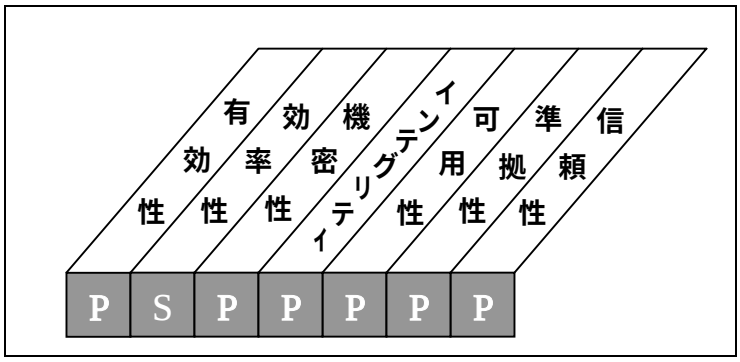
検討項目

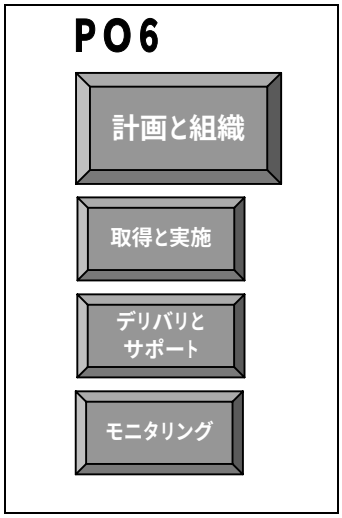
- **資金面の代替案**
- **実際の支払コントロール**
- **コストの正当化**
- **利益の正当化**



高いレベルのコントロール目標

計画と組織





ITプロセスのコントロール

マネジメント目標と指針の伝達

満たされるビジネス要件

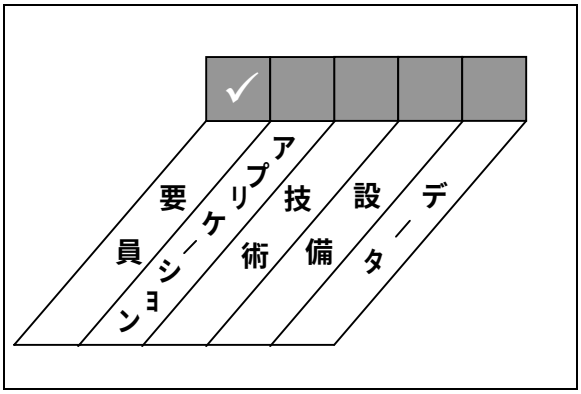
マネジメント目標のユーザの意識と理解を確保すること

実施方法

方針が作成され，ユーザコミュニティへ伝達される。さらに，戦略的な選択をユーザの実際的で利用可能なルールに置き換えるために作成される標準が必要である。

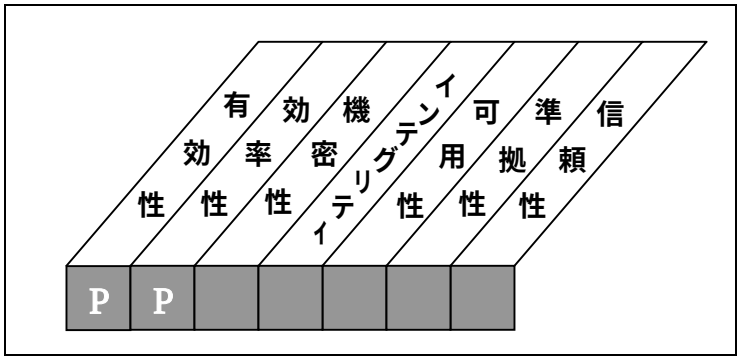
検討項目

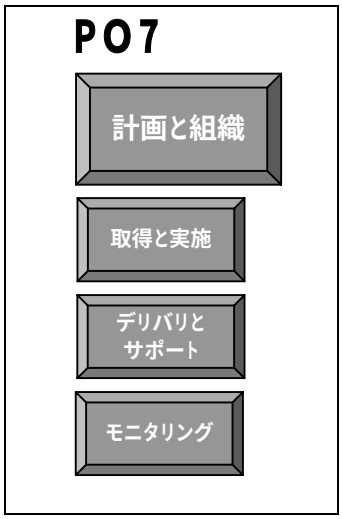
- **倫理／行動綱領**
- **技術指針**
- **準拠性**
- **品質のコミットメント**
- **セキュリティ方針**
- **内部統制の方針**



高いレベルのコントロール目標

計画と組織



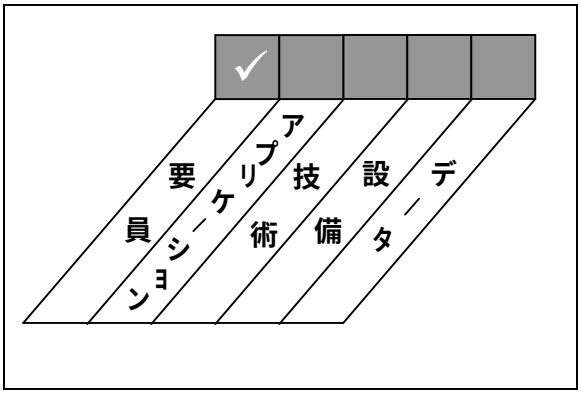


ITプロセスのコントロール
人的資源の管理

満たされるビジネス要件
ITプロセスへの要員の貢献を最大化すること

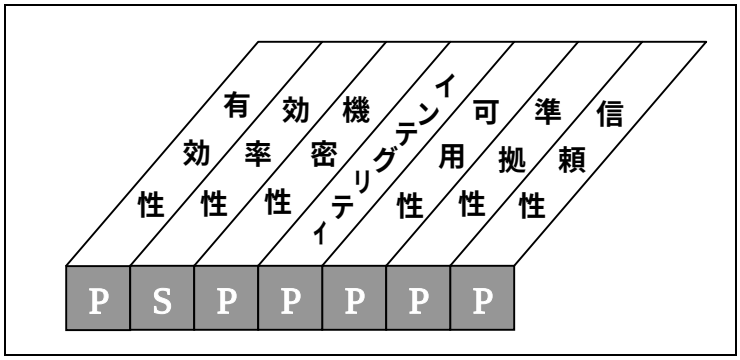
実施方法
健全な要員管理の技術

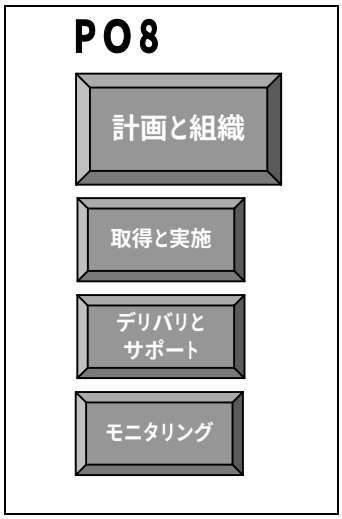
検討項目
- 新規採用と昇進
- 資格要件
- 教育
- 意識の植え付け
- 相互教育
- 解雇手続き
- 客観的かつ測定可能な業績評価



高いレベルのコントロール目標

計画と組織





ITプロセスのコントロール

外部要件への準拠性の保証

満たされるビジネス要件

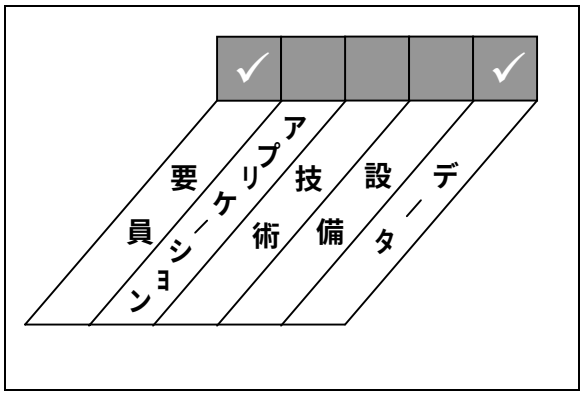
法的，規制，契約義務を満たすこと

実施方法

外部要件のITへの影響を識別し，分析し，それらの要件を遵守するために適切な対策をとる

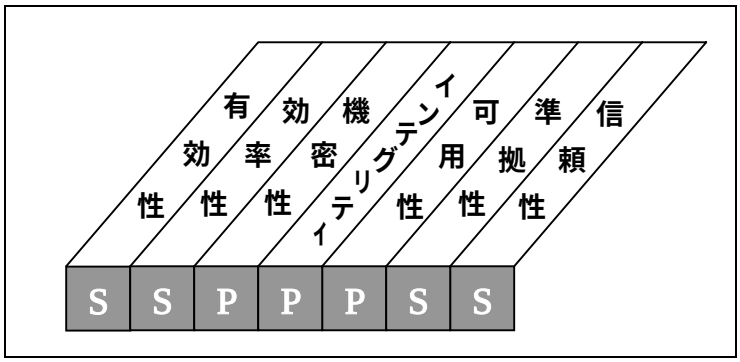
検討項目

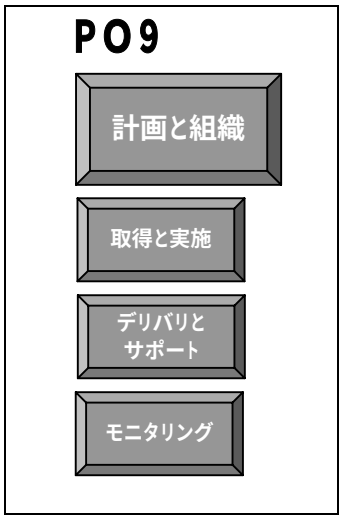
- **法律，規制，契約**
- **法的，規制の修正のモニタリング**
- **変更と修正の定期的レビュー**
- **法的な助言を求めること**
- **安全と人間工学**
- **プライバシー**
- **知的所有権**
- **データフロー**



高いレベルのコントロール目標

計画と組織





ITプロセスのコントロール

リスク評価

満たされるビジネス要件

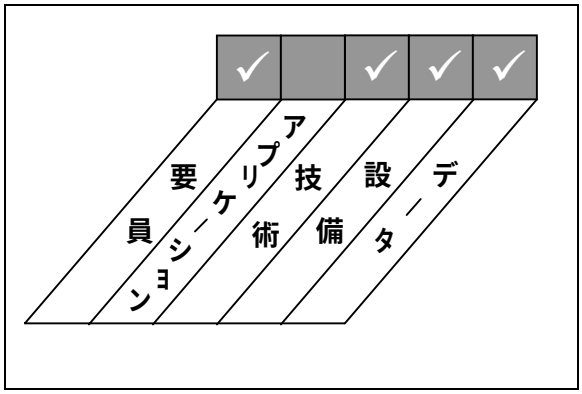
IT目標の達成を保証し，ITサービス提供に対する脅威へ対応すること

実施方法

リスクを低減するために，ITリスクの識別，影響分析，コスト－効果の良い対策をとることに自ら従事する組織

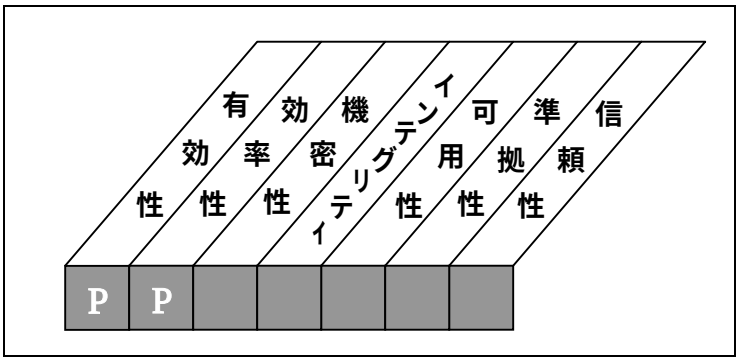
検討項目

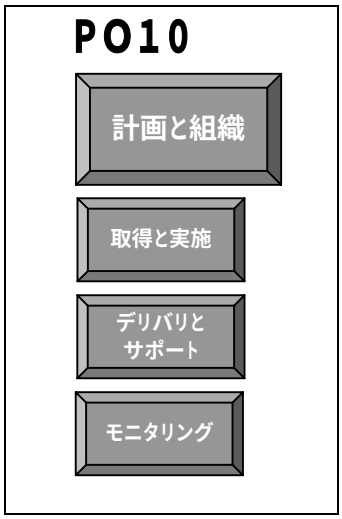
- **ITリスクの多様な種類（例：技術，セキュリティ，継続性，規則など）**
- **範囲：全体またはシステム固有**
- **リスク評価の更新**
- **リスク評価方法論**
- **定量的，そして／または定性的リスク測定**
- **リスク活動計画**



高いレベルのコントロール目標

計画と組織



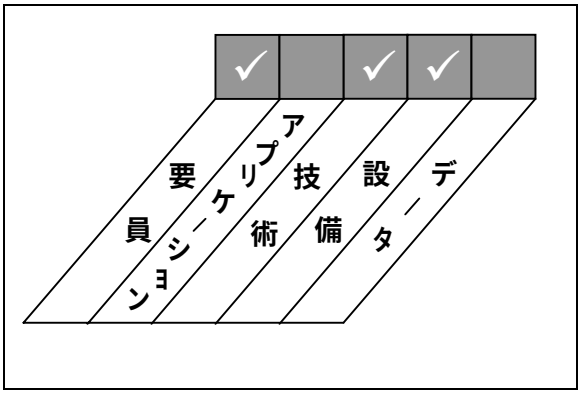


ITプロセスのコントロール
プロジェクト管理

満たされるビジネス要件
優先順位の設定と期限通りに予算内で提供すること

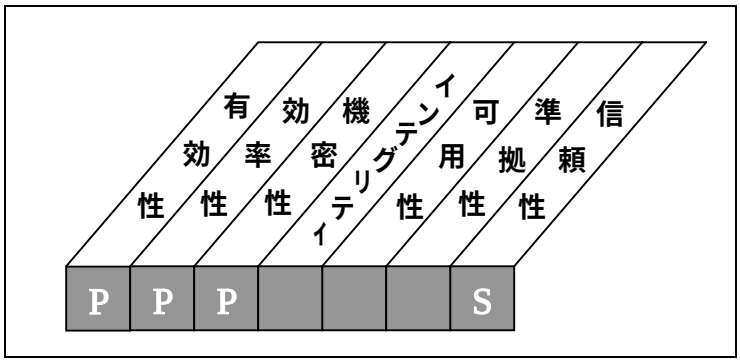
実施方法
業務計画に沿ったプロジェクトの識別と優先順位をつける組織。さらに，組織は，遂行中の各プロジェクトについて健全なプロジェクト管理技術を採用し，適用すること。

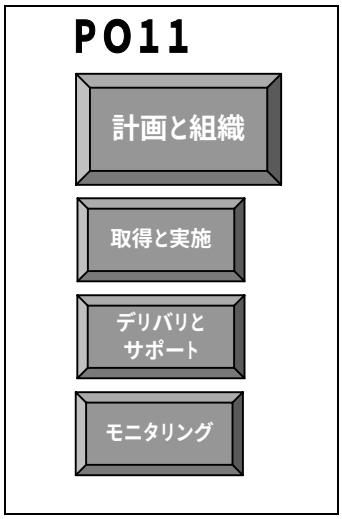
検討項目
- プロジェクトオーナーシップ
- ユーザの参画
- タスクの分解とマイルストーン
- 責任の割り当て
- プロジェクトとフェーズの承認
- コストと要員予算
- 品質保証計画と方法



高いレベルのコントロール目標

計画と組織



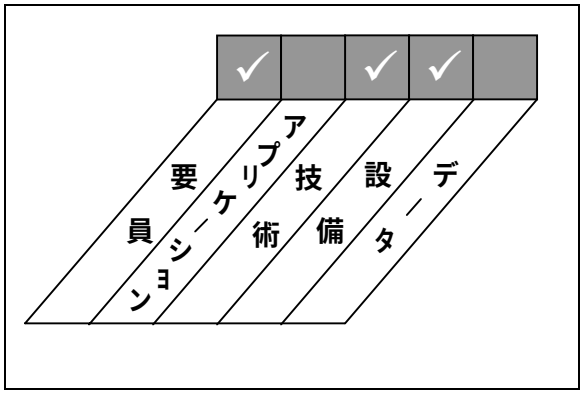


ITプロセスのコントロール
品質管理

満たされるビジネス要件
ITの顧客要件を満たすこと

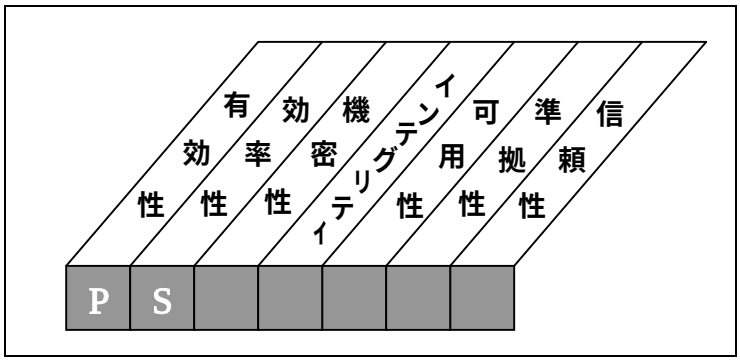
実施方法
組織による品質管理標準とシステムの計画，実施，保守。さらに，組織は，明確な開発フェーズを提供し，明確なフェーズと成果物を予測する方法論を採用し，適用する必要がある。

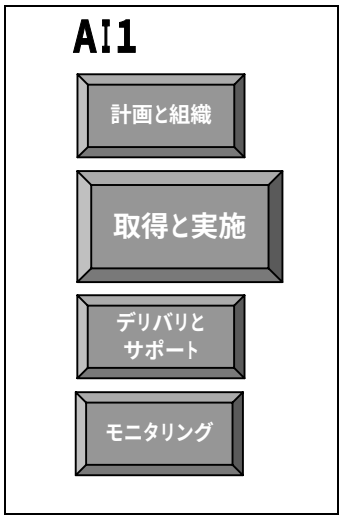
検討項目
- 品質計画の構造
- 品質保証の責任
- システム開発ライフサイクル方法論
- プログラムとシステムのテストと文書化
- 品質保証レビューと報告



高いレベルのコントロール目標

取得と実施





ITプロセスのコントロール

解決策の識別

満たされるビジネス要件

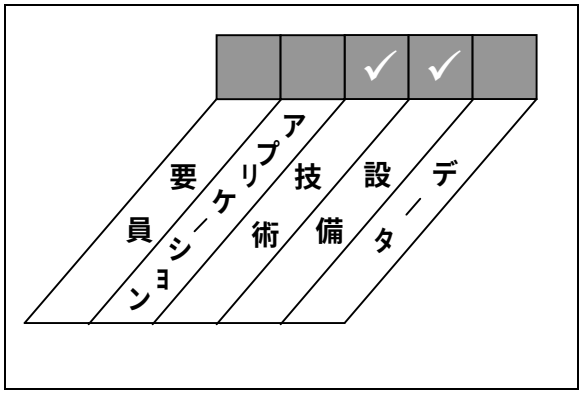
ユーザ要件を満たす最善のアプローチを保証すること

実施方法

ユーザ要件に対し，評価された代替機会の明確な分析

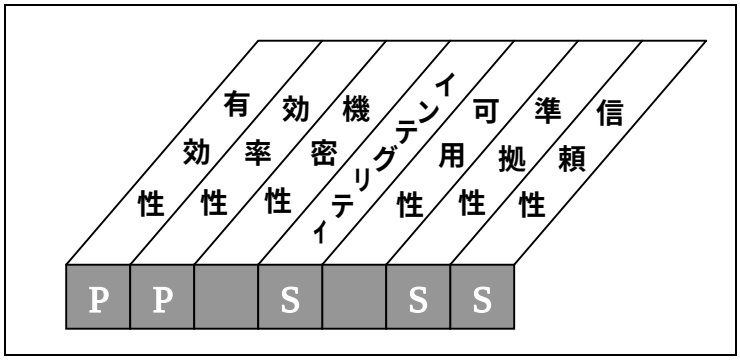
検討項目

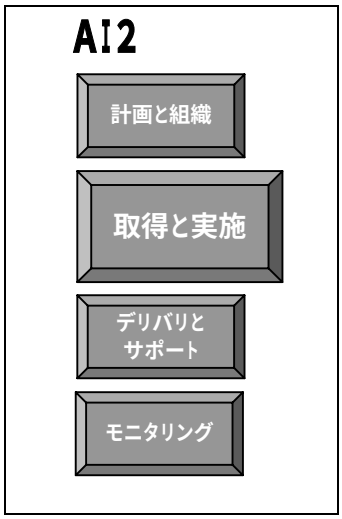
- 情報要件定義
- フィージビリティスタディ（コスト，便益，代替案等）
- ユーザ要件
- 情報基盤
- コスト－効果の良いセキュリティ
- 監査証跡
- 契約を出す
- ファシリティと技術の受け入れ



高いレベルのコントロール目標

取得と実施





ITプロセスのコントロール

アプリケーションソフトウェアの取得と保守

満たされるビジネス要件

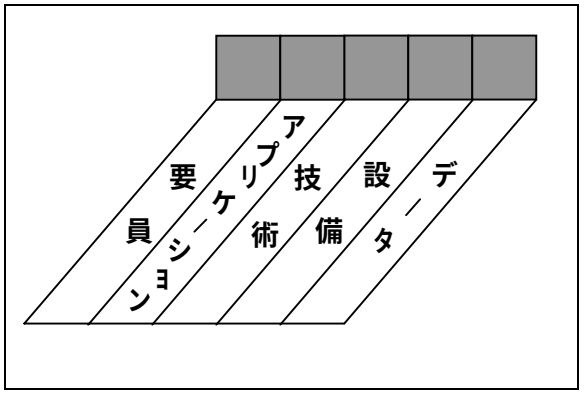
ビジネスプロセスを効果的に支援する自動機能を提供すること

実施方法

機能的な，そして業務的な要件の明確な記述の定義，そして明確な成果物のフェーズ化された導入。

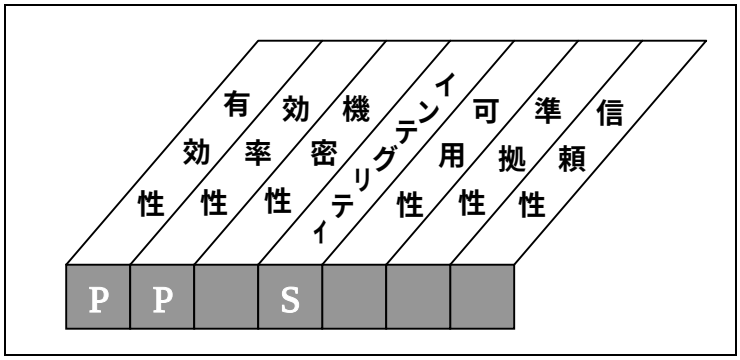
検討項目

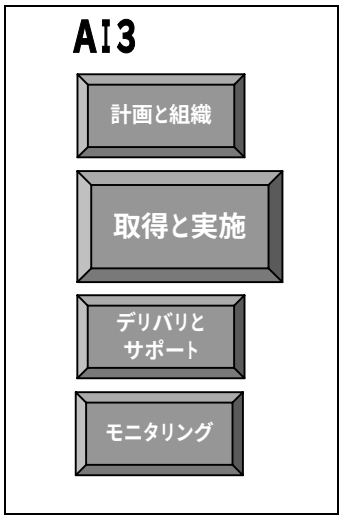
- **ユーザ要件**
- **ファイル，入力，処理，そして出力要件**
- **ユーザ－マシンインタフェース**
- **パッケージのカスタマイズ**
- **機能テスト**
- **アプリケーションコントロールとセキュリティ要件**
- **文書化**



高いレベルのコントロール目標

取得と実施





ITプロセスのコントロール

技術基盤の取得と保守

満たされるビジネス要件

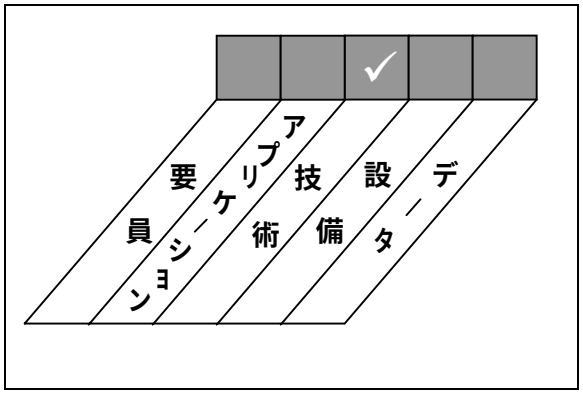
ビジネスアプリケーションを支援する適切なプラットフォームを提供すること

実施方法

ハードウェアとソフトウェアのパフォーマンス評価，ハードウェアの予防保守の準備，システムソフトウェアのインストール，セキュリティ，そしてコントロール

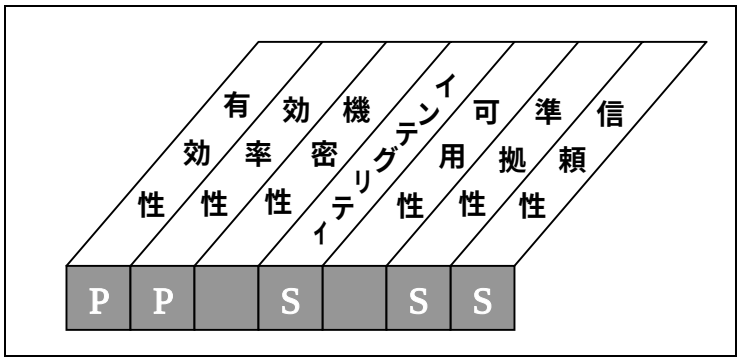
検討項目

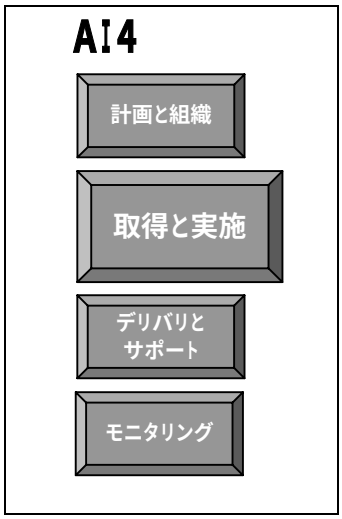
- **技術評価**
- **ハードウェア予防保守**
- **システムソフトウェアセキュリティ，インストール，保守，そして変更コントロール**



高いレベルのコントロール目標

取得と実施





ITプロセスのコントロール

ITシステム関連手続きの作成と保守

満たされるビジネス要件

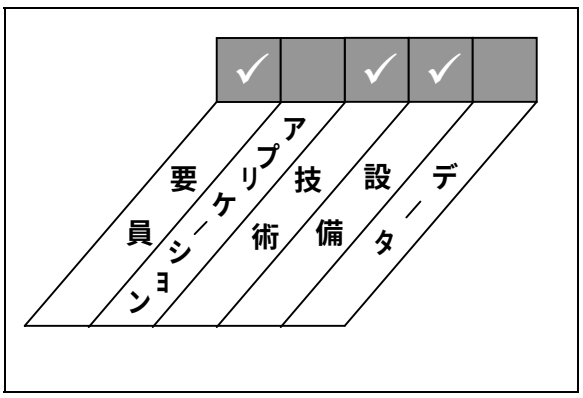
アプリケーションの適切な利用と技術的解決が適切に導入されることを保証すること

実施方法

ユーザと運用の手続きマニュアル,サービス要件および教育資料の作成に対する構造的アプローチ

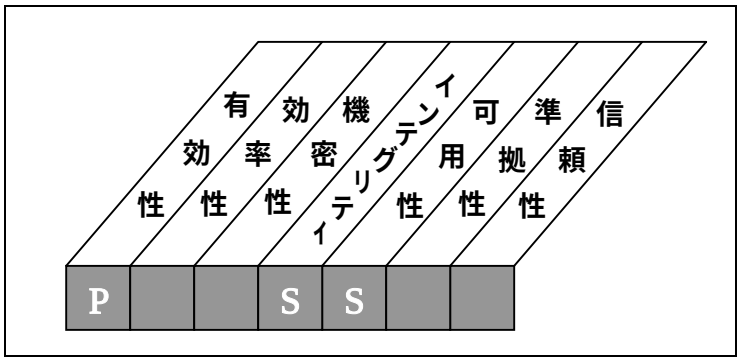
検討項目

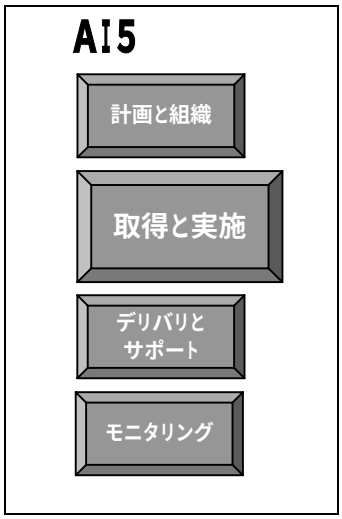
- **ユーザ手続きとコントロール**
- **運用手続きとコントロール**
- **教育資料**



高いレベルのコントロール目標

取得と実施



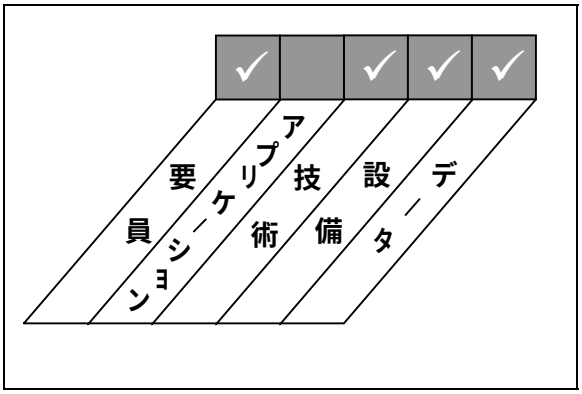


ITプロセスのコントロール
システムの認証と導入

満たされるビジネス要件
解決策が意図した目的に適合していることを検証し，確認すること

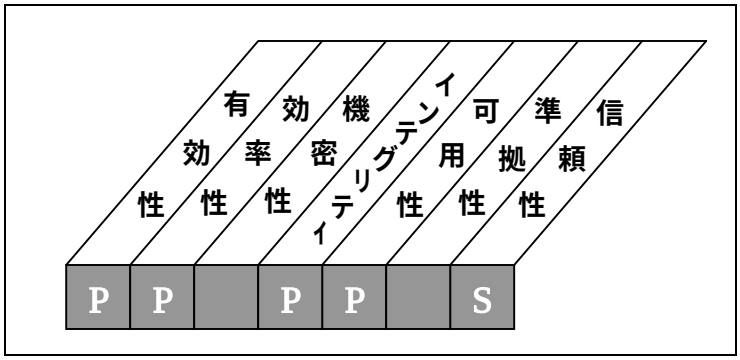
実施方法
設備の導入，移行，検収に関する十分に承認された計画の実現

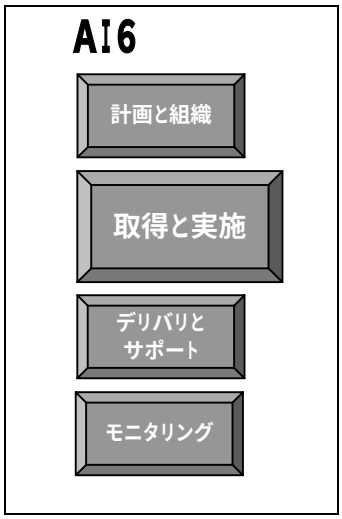
検討項目
- **教育**
- **データロード／移行**
- **特定テスト**
- **承認**
- **導入後レビュー**



高いレベルのコントロール目標

取得と実施





ITプロセスのコントロール

変更管理

満たされるビジネス要件

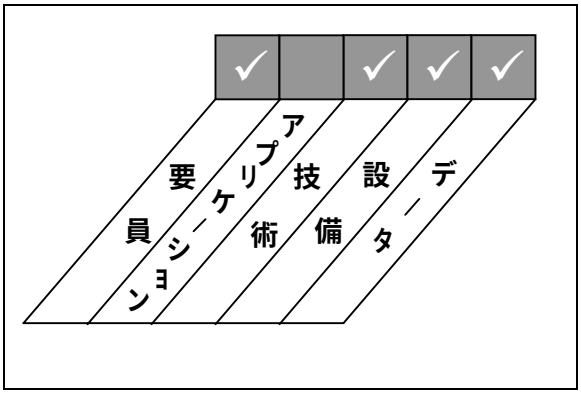
中断，未承認の変更，エラーの可能性を最小化すること

実施方法

要求され，既存のIT基盤に実施されたすべての変更の分析，実施およびフォローアップを提供する管理システム

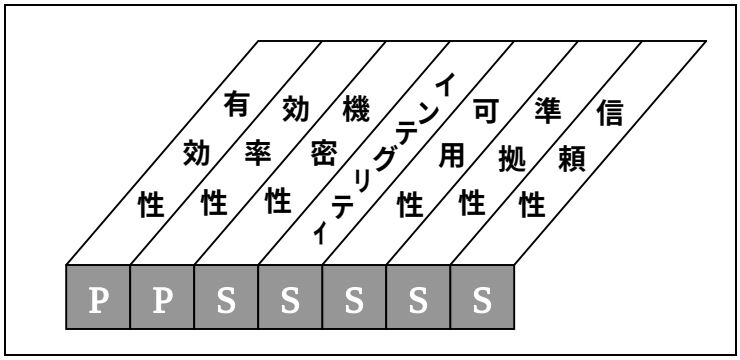
検討項目

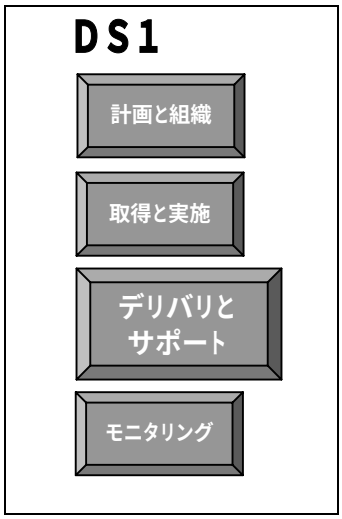
- **変更の識別**
- **分類，優先順位付け，緊急手続き**
- **影響の評価**
- **変更の承認**
- **リリース管理**
- **ソフトウェア配付**



高いレベルのコントロール目標

デリバリとサポート





ITプロセスのコントロール

サービスレベルの定義

満たされるビジネス要件

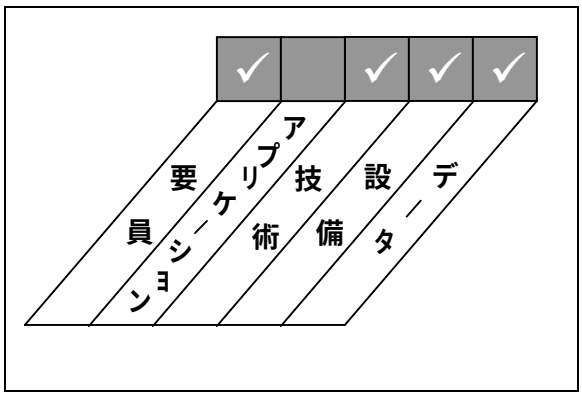
要請されたサービスレベルの共通的な理解を確立すること

実施方法

サービスの量と質を測定する業績規準を公式化するサービスレベル協定を作成する，監視する

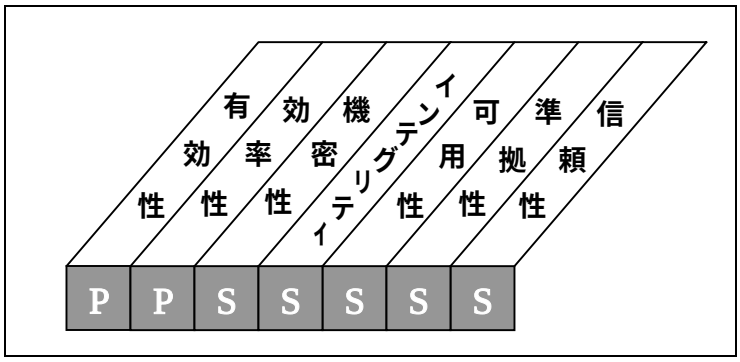
検討項目

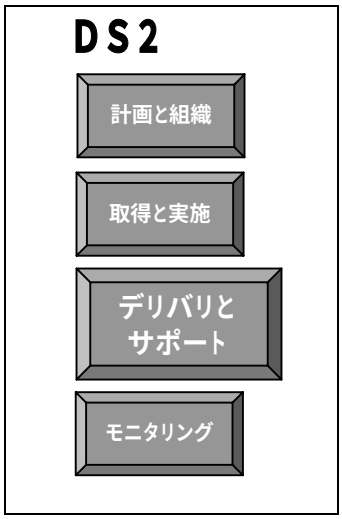
- **公式の合意**
- **責任の定義**
- **レスポンスタイムと量**
- **課金**
- **インテグリティの保証**
- **非開示の協定**



高いレベルのコントロール目標

デリバリとサポート





ITプロセスのコントロール

第三者機関のサービスの管理

満たされるビジネス要件

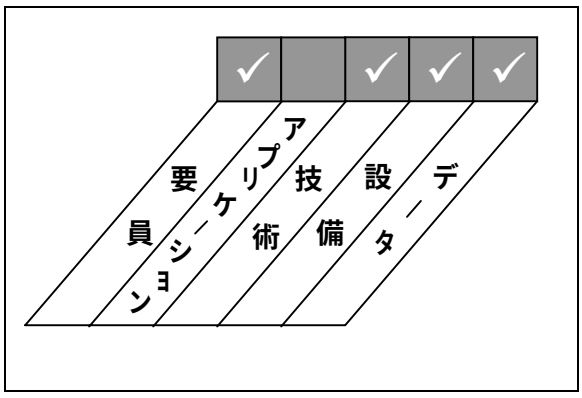
要件を満足し続けるために，第三者機関の役割と責任が明確に定義され，遵守されることを保証する

実施方法

既存の契約と手続きが効果的で組織の方針と合致していることをレビューし，モニタリングすることを目標に設けられたコントロール方法

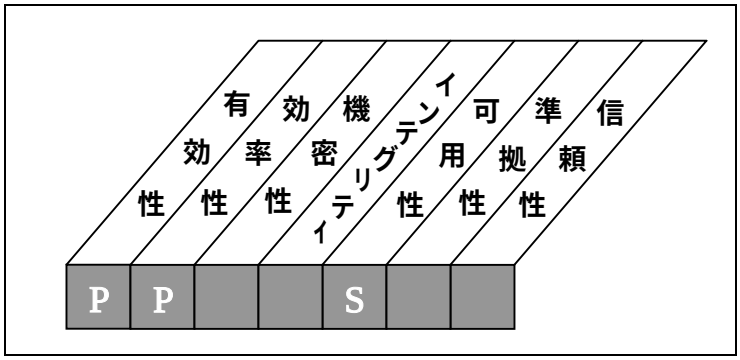
検討項目

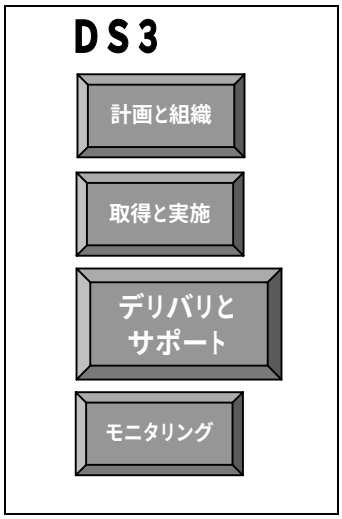
- **第三者機関のサービス合意書**
- **非開示の合意書**
- **法律と規制の要件**
- **サービスデリバリのモニタリング**



高いレベルのコントロール目標

デリバリとサポート





ITプロセスのコントロール

性能とキャパシティの管理

満たされるビジネス要件

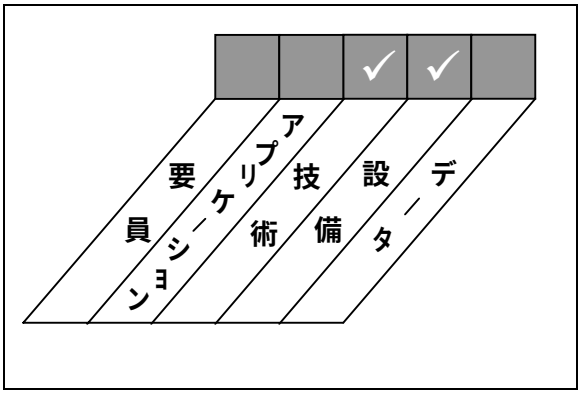
適切なキャパシティが利用可能で，所要の性能の要件を満足するために，最善で最適な利用がされていることを保証すること

実施方法

負荷管理，アプリケーションサイズ，資源と要求管理に関するデータを収集し，報告するキャパシティと性能管理のコントロール

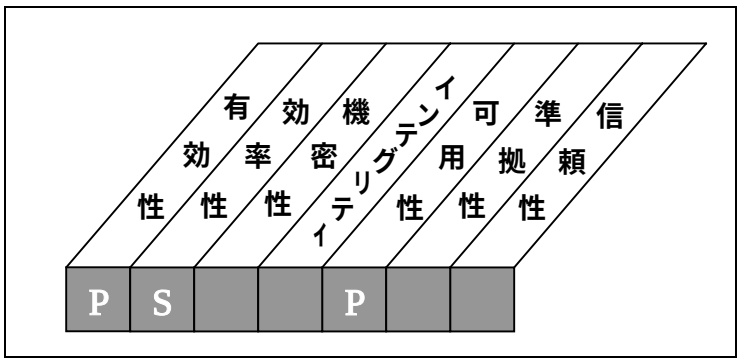
検討項目

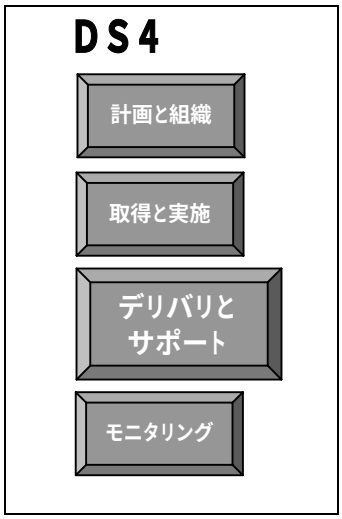
- **可用性と性能要件**
- **モニタリングとレポート**
- **モデリングツール**
- **キャパシティ管理**
- **資源の可用性**



高いレベルのコントロール目標

デリバリとサポート





ITプロセスのコントロール

継続的サービスの保証

満たされるビジネス要件

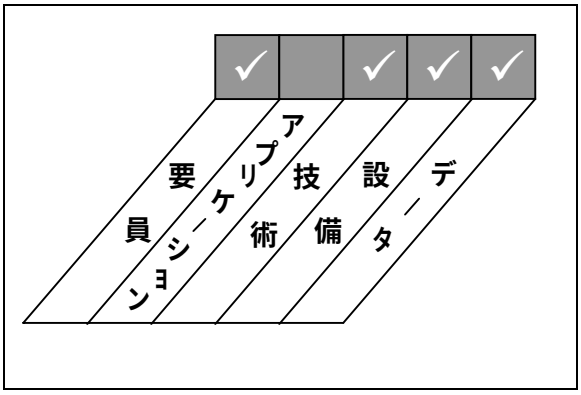
要求されたITサービスを利用可能とすること，および大きな中断の場合にビジネスへの影響を最小限に保証すること

実施方法

全体にわたるビジネス継続計画およびその関連するビジネス要件と調和している運用およびテストされたITの継続計画をもつ

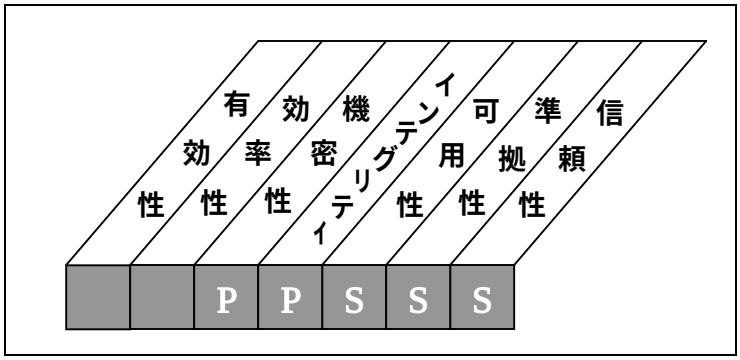
検討項目

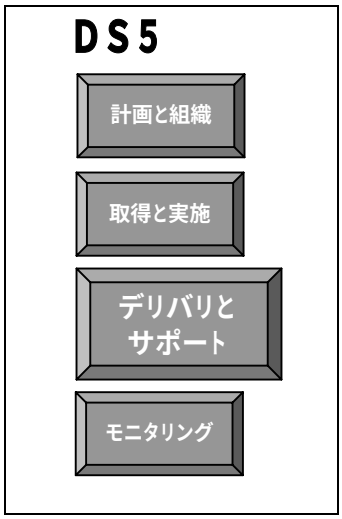
- **重要度の分類**
- **文書化された計画**
- **代替手続き**
- **バックアップとリカバリ**
- **体系的および定期的なテストと教育**



高いレベルのコントロール目標

デリバリとサポート





ITプロセスのコントロール

システムセキュリティの保証

満たされるビジネス要件

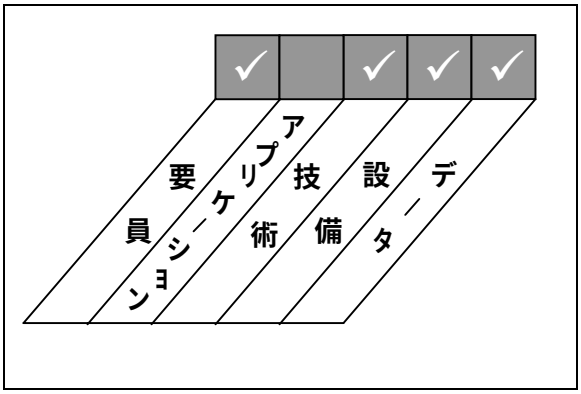
未許可の利用，開示，改ざん，損害，損失から情報を保護すること

実施方法

システム,データおよびプログラムへのアクセスが許可されたユーザだけに制限されていることを保証する論理的アクセスコントロール

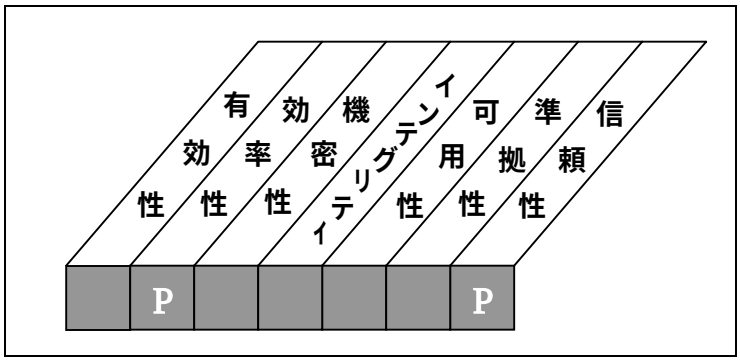
検討項目

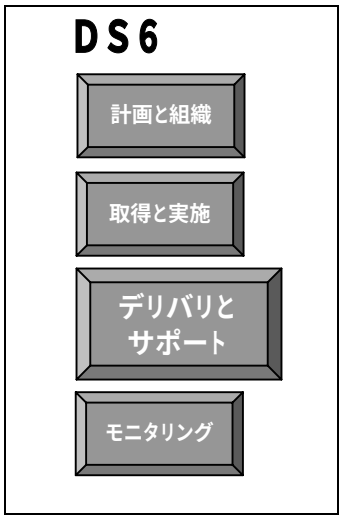
- **承認**
- **認証**
- **アクセス**
- **ユーザのプロフィールと識別**
- **暗号鍵管理**
- **事故の取扱い，報告とフォローアップ**
- **信頼できる経路**
- **ウィルス予防と検出**
- **ファイヤーウォール**



高いレベルのコントロール目標

デリバリとサポート



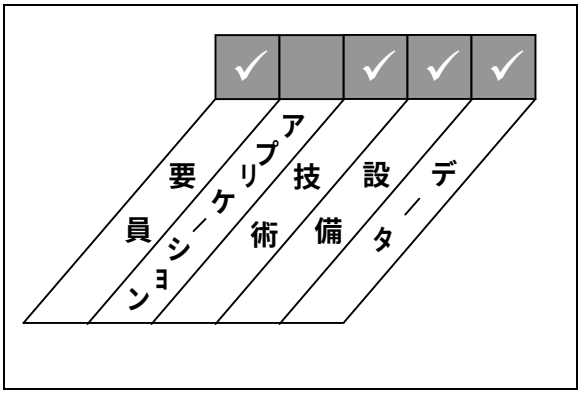


ITプロセスのコントロール
コストの識別と賦課

満たされるビジネス要件
ITサービスに賦課されるコストの正しい認識を保証すること

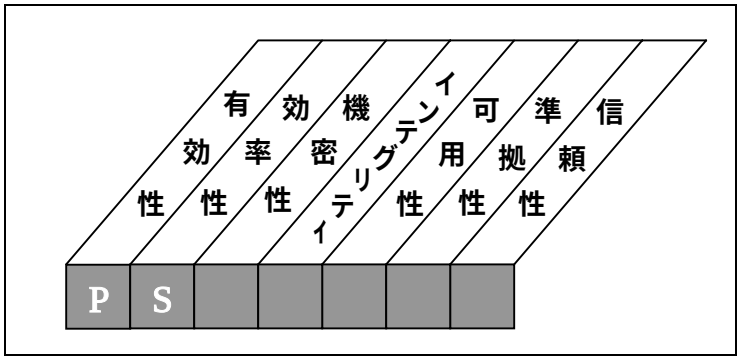
実施方法
コストが記録され，計算され，必要とされる詳細レベルで配分されていることを保証する原価会計システム

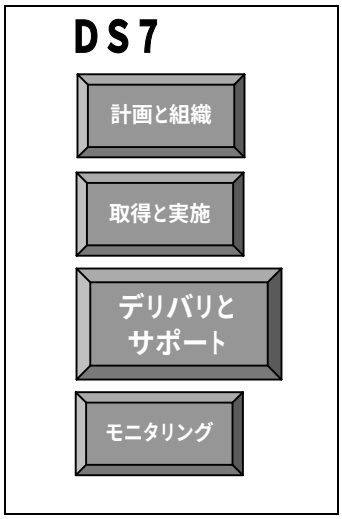
検討項目
- **資源の識別可能性と測定可能性**
- **賦課方針と手続き**
- **賦課率**



高いレベルのコントロール目標

デリバリとサポート



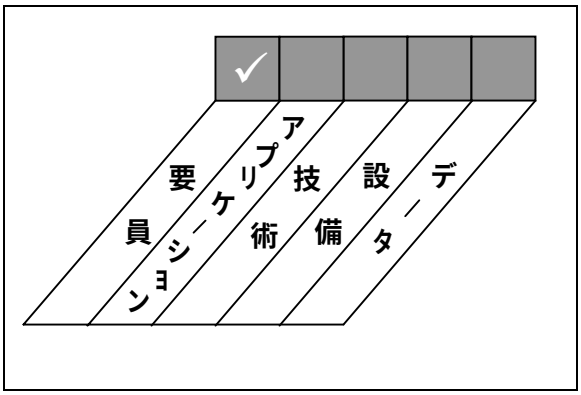


ITプロセスのコントロール
ユーザの教育と訓練

満たされるビジネス要件
ユーザが技術を効果的に利用し，関連するリスクと責任を認識していることを保証すること

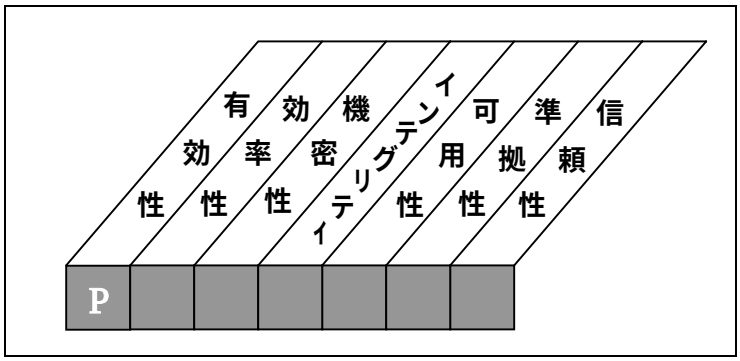
実施方法
包括的な教育と開発計画

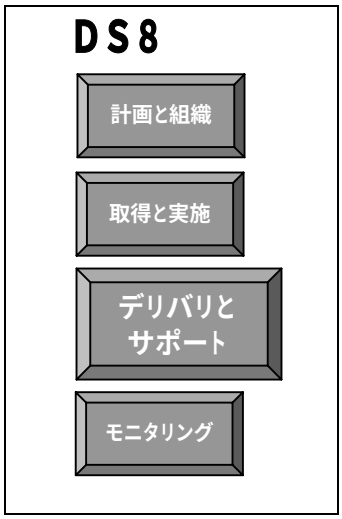
検討項目
- **教育カリキュラム**
- **意識キャンペーン**
- **意識付け技術**



高いレベルのコントロール目標

デリバリとサポート





ITプロセスのコントロール

ITのカスタマへの支援と助言

満たされるビジネス要件

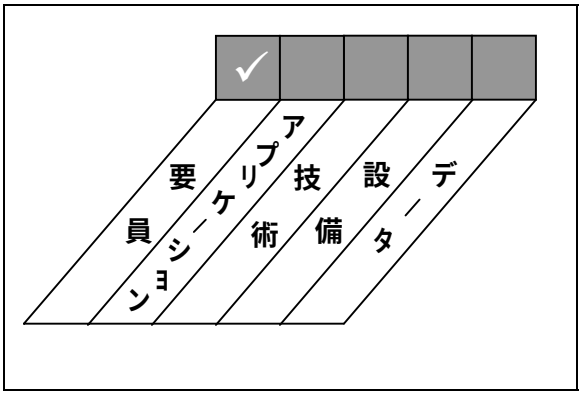
ユーザによって経験された問題が適切に解決されることを保証すること

実施方法

第一線のサポートと助言を提供するヘルプデスク機能

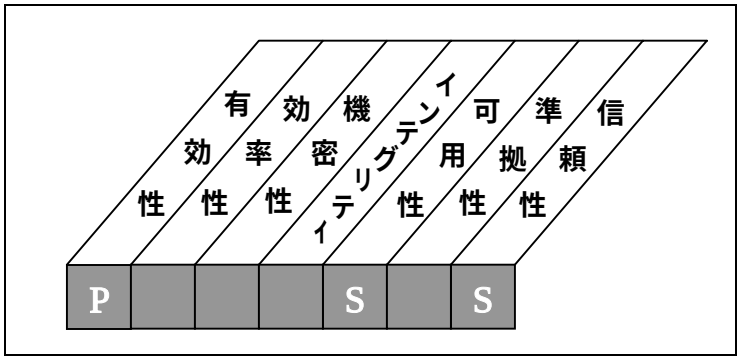
検討項目

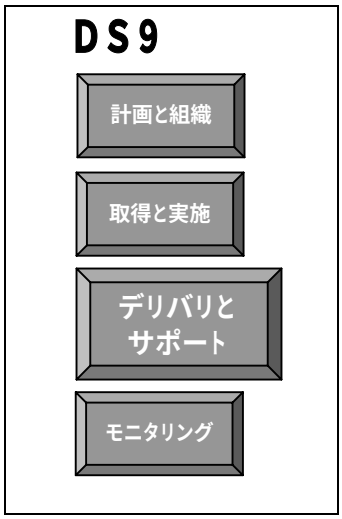
- カスタマの質問と問題へのレスポンス
- 質問のモニタリングと整理
- 傾向の分析と報告



高いレベルのコントロール目標

デリバリとサポート





ITプロセスのコントロール

構成管理

満たされるビジネス要件

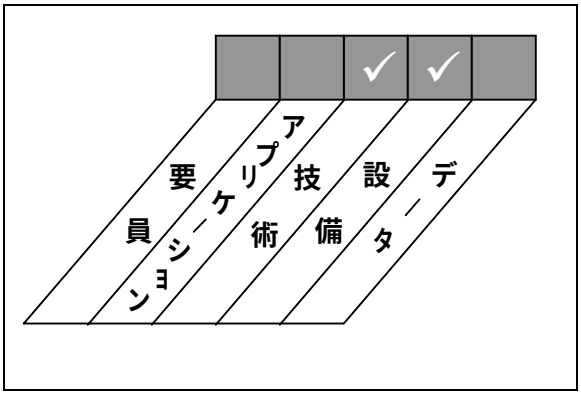
すべてのIT要素を説明し，未承認の変更を防止し，物理的存在を検証し，正しい変更管理の基礎を提供すること

実施方法

すべてのIT資産とそれらの物理的場所，そしてそれらの実在を確認する定期的な検証プログラムを識別し，記録するコントロール

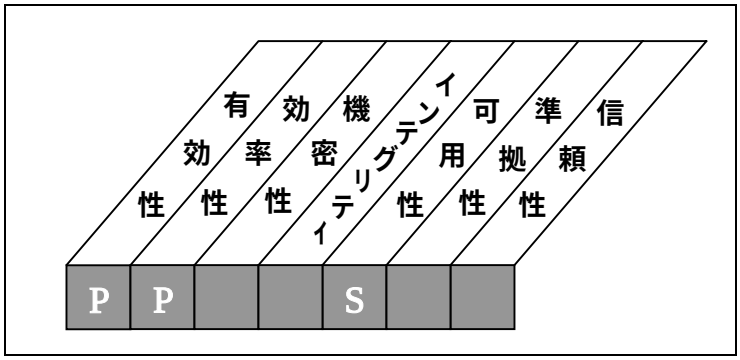
検討項目

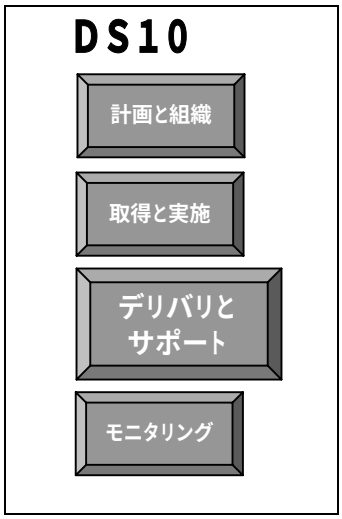
- **資産を記録すること**
- **構成変更管理**
- **未承認のソフトウェアチェック**
- **ソフトウェア保管コントロール**



高いレベルのコントロール目標

デリバリとサポート





ITプロセスのコントロール

問題と障害管理

満たされるビジネス要件

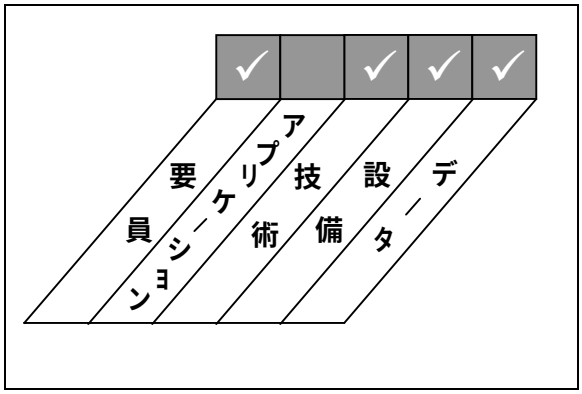
問題と障害が解決され，再発を防止するために原因が調査されていることを保証すること

実施方法

すべての障害を記録し，解決する問題管理システム

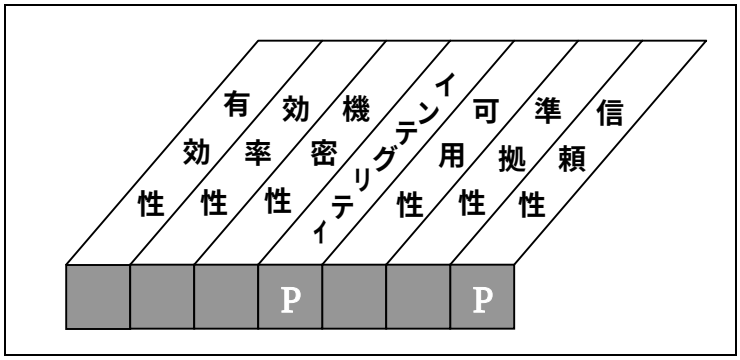
検討項目

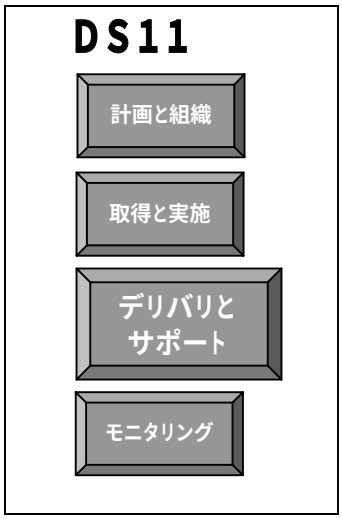
- **問題と解決の十分な監査証跡**
- **報告された問題の適時な解決**
- **上申手続き**
- **障害報告**



高いレベルのコントロール目標

デリバリとサポート





ITプロセスのコントロール

データ管理

満たされるビジネス要件

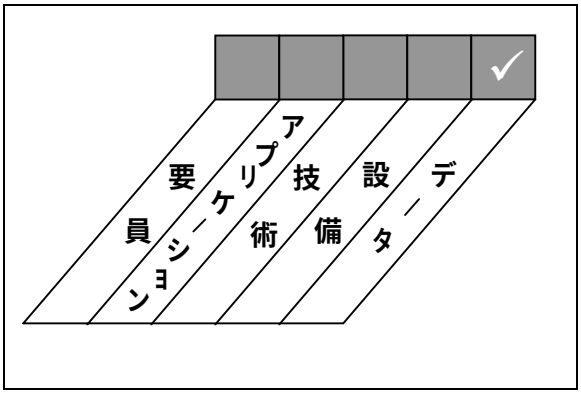
データの入力，更新，保管の間にデータが完全，正確，妥当であると保証すること

実施方法

IT運用上における業務処理統制および全般統制の効果的な組み合わせ

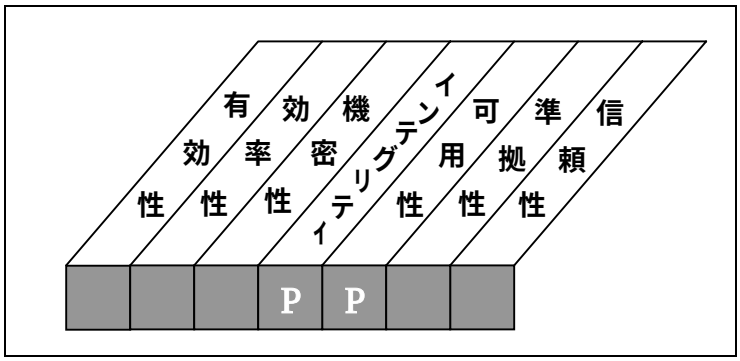
検討項目

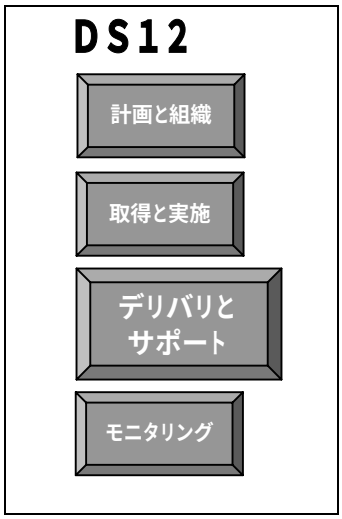
- **フォーム設計**
- **原始帳票のコントロール**
- **入力コントロール**
- **処理コントロール**
- **出力コントロール**
- **メディアの識別，移動，ライブラリ管理**
- **メディアの保管とバックアップ管理**
- **認証とインテグリティ**



高いレベルのコントロール目標

デリバリとサポート



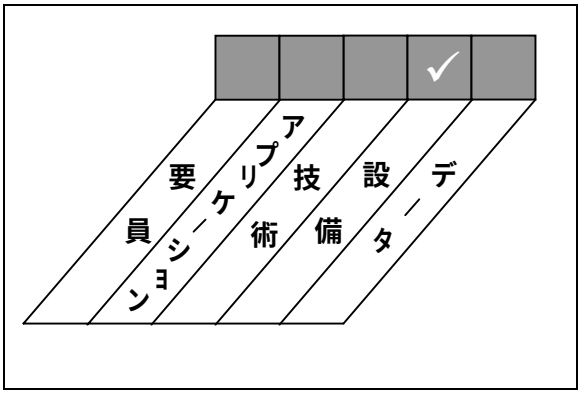


ITプロセスのコントロール
ファシリティ管理

満たされるビジネス要件
人災，天災からIT機器と要員を保護する適切な物理的環境を提供すること

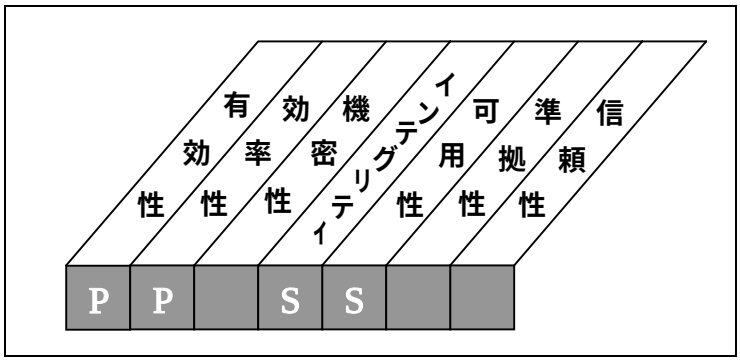
実施方法
適切に機能していることを定期的にレビューする適切な環境と物理的コントロールの導入

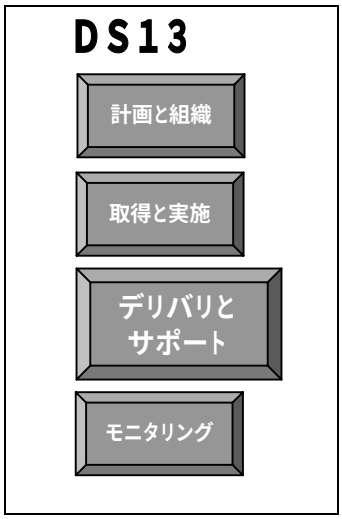
検討項目
- **設備へのアクセス**
- **サイトの識別**
- **物理的セキュリティ**
- **要員の健康と安全**
- **環境の脅威からの保護**



高いレベルのコントロール目標

デリバリとサポート





ITプロセスのコントロール

運用管理

満たされるビジネス要件

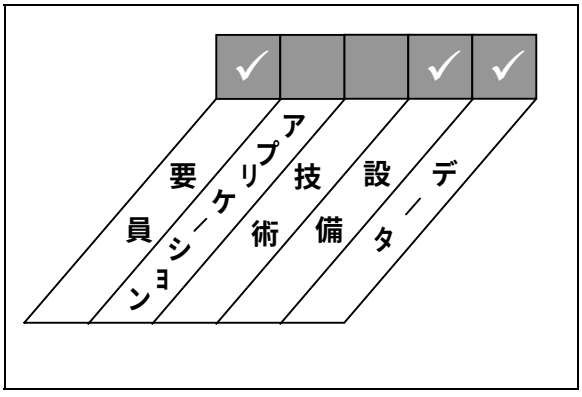
重要なITサポート機能が整然と規律正しく機能していることを保証すること

実施方法

すべての活動の達成に向けて，記録され，解決されるサポート活動計画

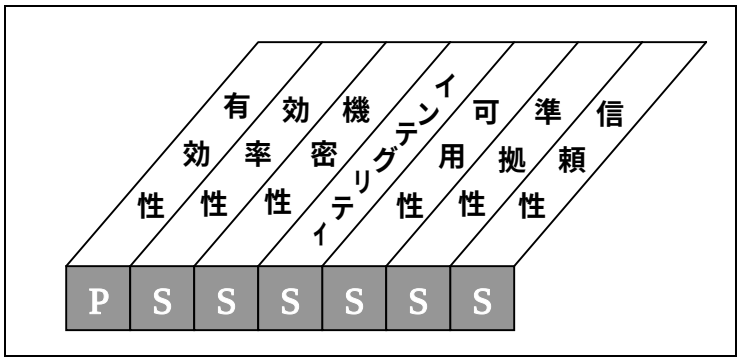
検討項目

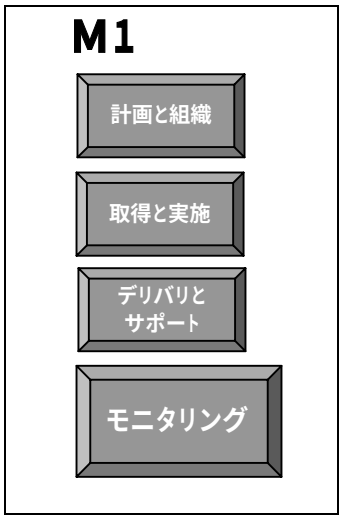
- **運用手続きマニュアル**
- **スタートアッププロセス文書**
- **ネットワークサービス管理**
- **作業量と要員のスケジューリング**
- **シフト引き継ぎプロセス**
- **システムイベント ロギング**



高いレベルのコントロール目標

モニタリング



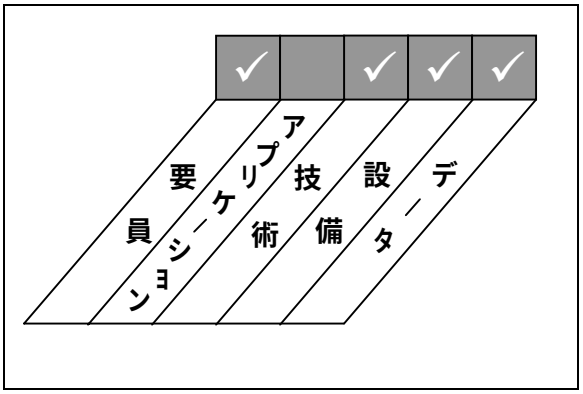


ITプロセスのコントロール
プロセスのモニタリング

満たされるビジネス要件
ITプロセスのために設定された業績目標の達成を保証すること

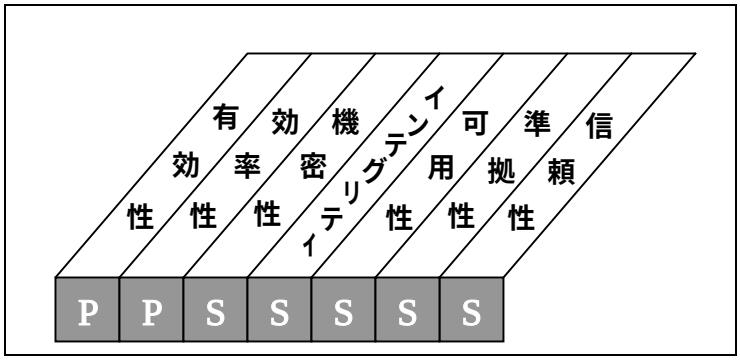
実施方法
関連する管理者の報告と業績指標の管理者の定義，定期的な報告の解決と同様にサポートシステムの導入

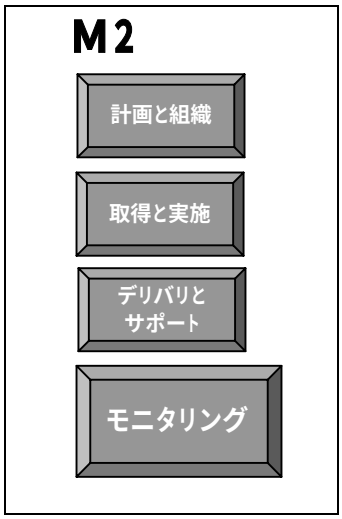
検討項目
- **重要な業績指標**
- **重要成功要因**
- **顧客満足度評価**
- **管理者の報告**



高いレベルのコントロール目標

モニタリング





ITプロセスのコントロール

内部統制の妥当性の評価

満たされるビジネス要件

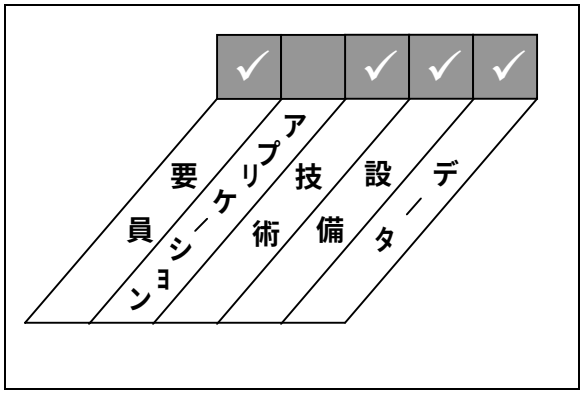
ITプロセスに対する一連の内部統制目標の達成を保証すること

実施方法

内部統制をモニタリングし，それらの有効性を評価し，定期的にそれらを報告することに対する管理者のコミット

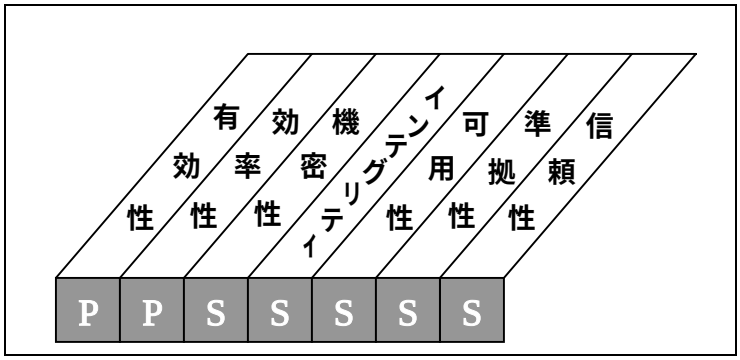
検討項目

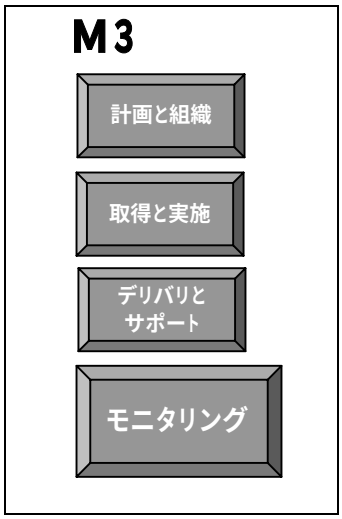
- 継続的な内部統制モニタリング
- ベンチマーク
- エラーと例外の報告
- 自己評価
- 管理者の報告



高いレベルのコントロール目標

モニタリング





ITプロセスのコントロール

独立した保証の確保

満たされるビジネス要件

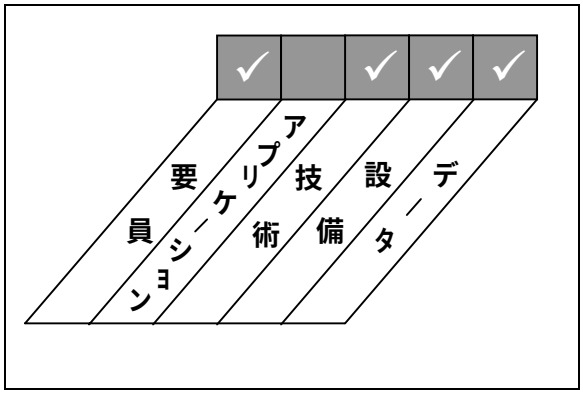
組織，顧客，第三者機関による提供者との間の信用と信頼を向上させること

実施方法

定期的な間隔で実行された独立的保証のレビュー

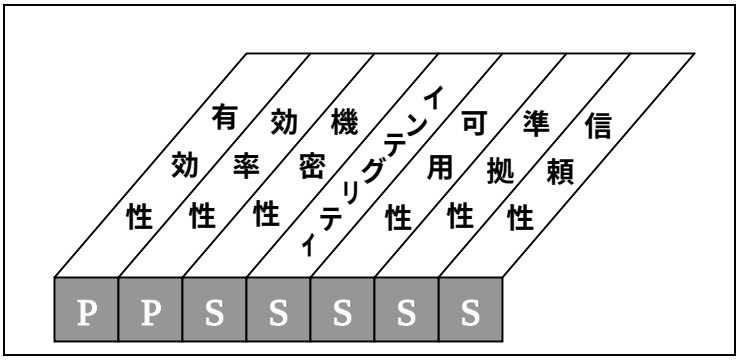
検討項目

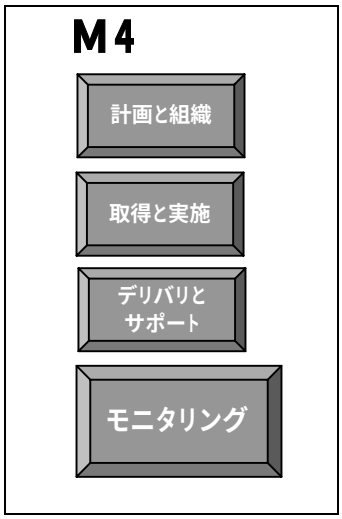
- **独立的保証と認可**
- **独立的な有効性評価**
- **法律や規制要件に対する準拠性の独立的保証**
- **契約上のコミットメントに対する準拠性の独立的保証**
- **第三者の提供者によるレビュー**
- **資格のある要員による保証レビューの実施**
- **積極的な監査の関与**



高いレベルのコントロール目標

モニタリング





ITプロセスのコントロール

独立的監査の提供

満たされるビジネス要件

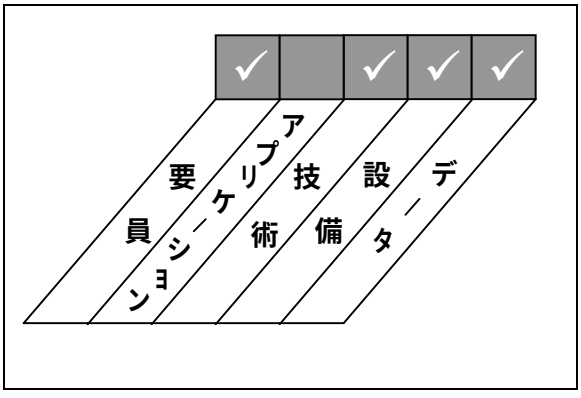
最善の慣行に基づく助言のより信頼レベルと便益を向上すること

実施方法

定期的に実行される独立的監査

検討項目

- **監査の独立性**
- **積極的な監査の関与**
- **権限のある要員による監査の実施**
- **発見事項と勧告の実施**
- **フォローアップ活動**

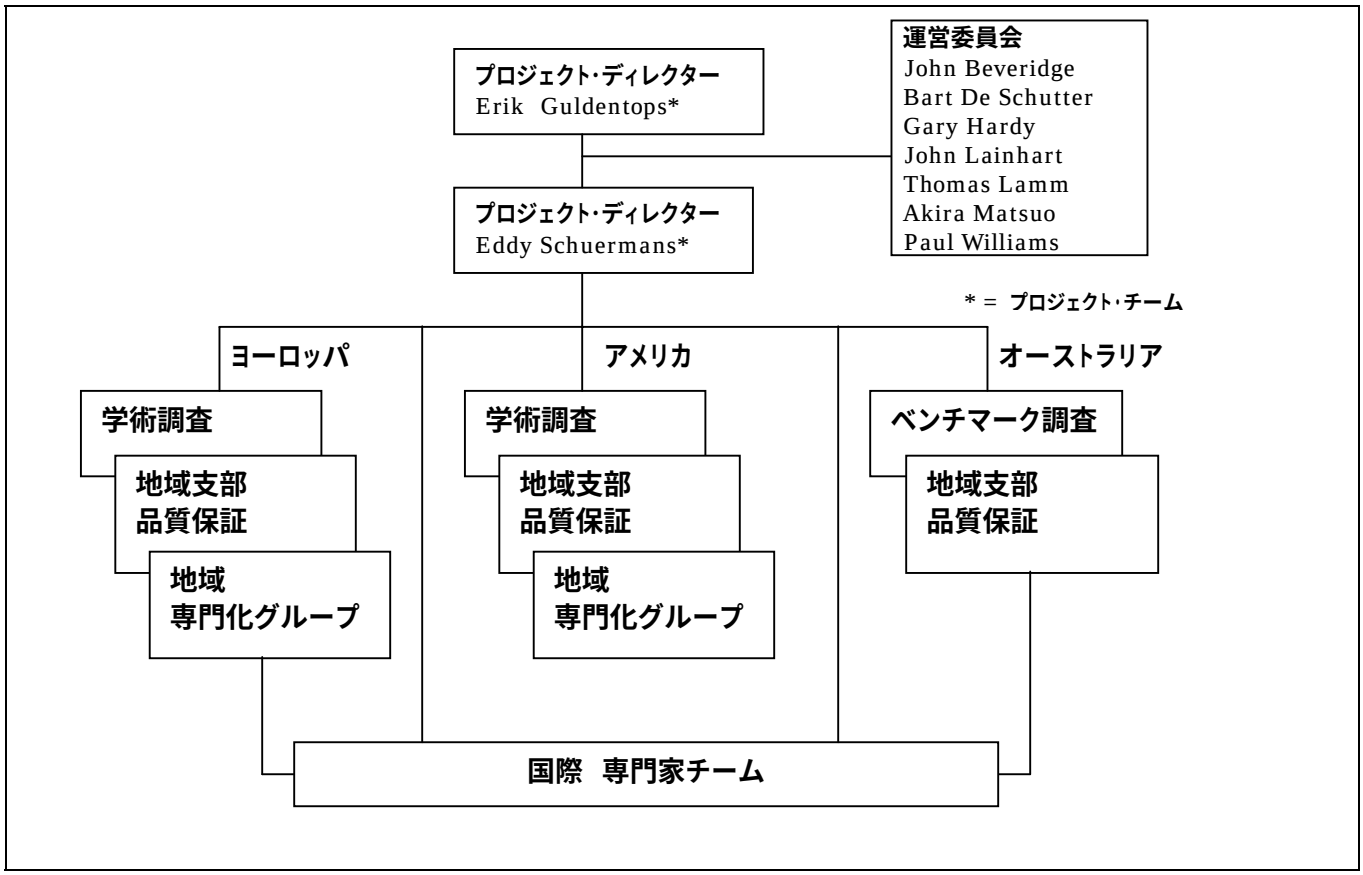


付録 I　COBITプロジェクトの説明

組織と責任

プロジェクトは，産業界，学会，政府および監査専門家からなる国際的な代表者によって形成されたプロジェクト運営委員会によって監督が続けられている。全般的なプロジェクトガイダンスは，ISACAの国際本部理事会によって提供されている。プロジェクト運営委員会は，COBIT *フレームワーク*の開発と調査結果の適用についての手段となってきている。

国際的ワーキンググループは，プロジェクトの中間調査と開発成果物の品質保証および専門家によるレビューの目的のために設置された。



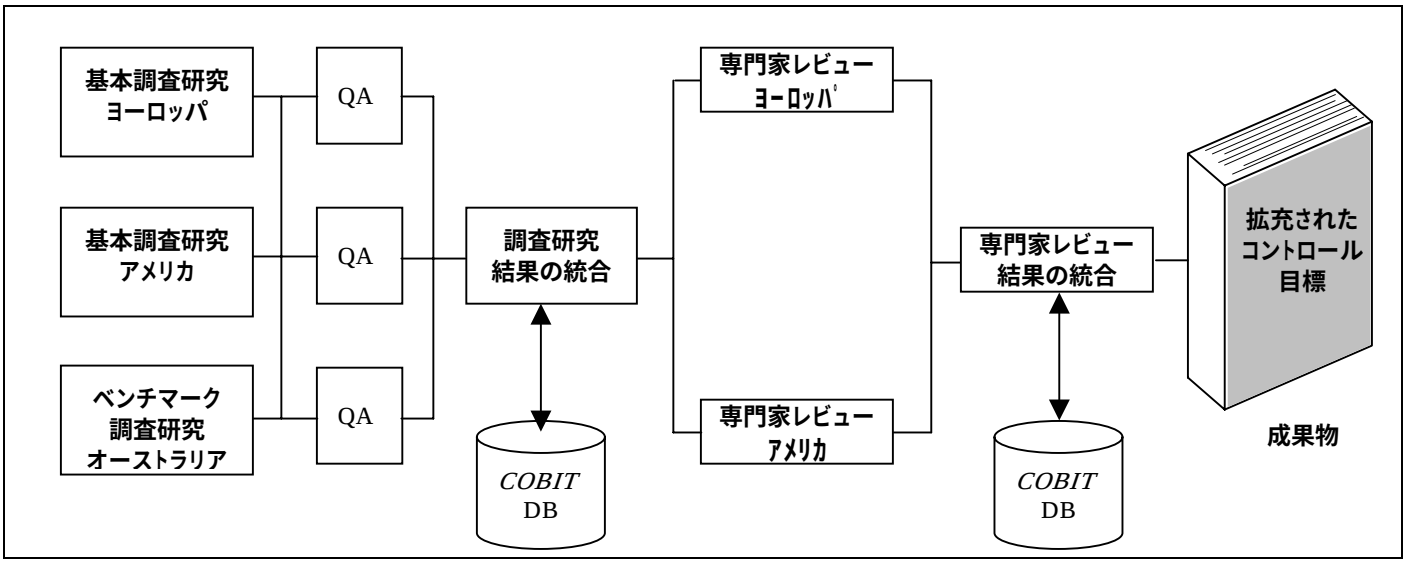
調査研究

調査研究は，識別された原典の収集と分析を含み，ヨーロッパ(アムステルダム自由大学)，アメリカ(カリフォルニアポリテック大学)，オーストラリア(ニューサウスウェールズ大学)の調査チームによって推進された。調査研究チームは，学界そして専門的代表者から構成されている。

収集と分析の後，調査研究員は，各ドメインとプロセスを深く検討することに挑戦し，また，その特定の情報技術プロセスに適用可能な新しいコントロール目標を提案している。調査研究員は，編集，レビュー，評価，およびそれらがフレームワークと個々のコントロール目標に関連するときには，国際的技術基準，行為綱領，品質標準，監査の専門基準，業界慣行と要件および業界特有の要件の適切な取込みを図った。彼らの努力は，品質レビュー者と専門家グループによる検討のための300以上にわたる新しい更新されたコ

ントロール目標を作り上げた。

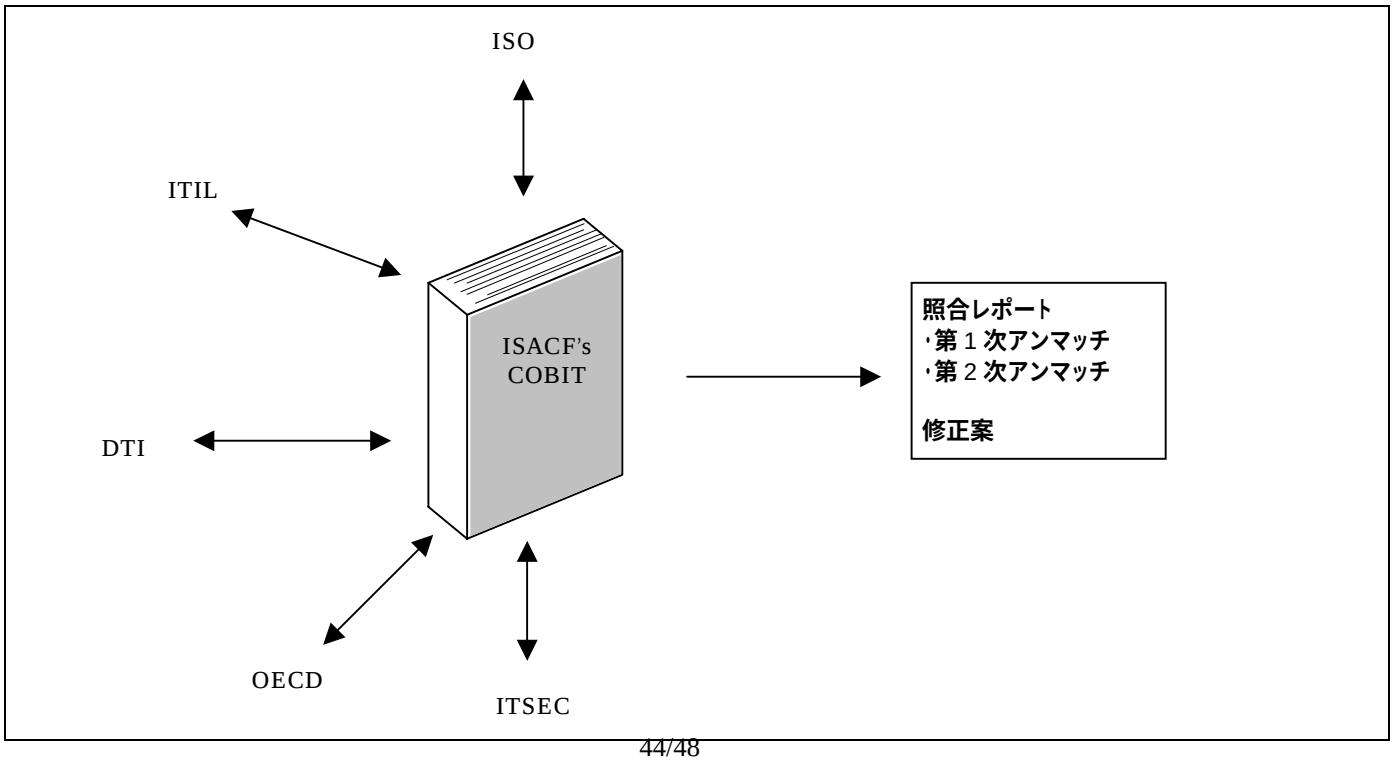
その結果の統合は，プロジェクトディレクタ，プロジェクトマネジャとISACF調査研究ディレクタから構成されるプロジェクトチームによって，主として実施された。



方法論と原典

運営委員会や，専門家グループによって挑戦され，更新されたフレームワークの開発に次いで，識別された文献と標準の各々と*コントロール目標*との個々の比較は，調査研究グループによって実施された。意図したことは，すべての資料の全般的な分析を実施することでもなく，最初から*コントロール目標*を再開発をすることでもなかった。それは比較と更新のプロセスであった。

この調査研究活動からの基本的な成果物は，第1次照合のリスト(*コントロール目標*で，比較資料でない)と，第二次照合(比較資料で，*コントロール目標*でない)である。



付録II　COBITの主な参考資料

COSO: Committee of Sponsoring Organisations of the Treadway Commission. Internal Control - Integrated Framework. 2 Vols. American Institute of Certified Accountants, New Jersey, 1994.

OECD Guidelines: Organisation for Economic Co-operation and Development. Guidelines for the Security of Information, Paris, 1992.

DTI Code of Practice for Information Security Management: Department of Trade and Industry and British Standard Institute. A Code of Practice for Information Security Management, London, 1993, 1995.

ISO 9000-3: International Organisation for Standardisation. Quality Management and Quality Assurance Standards - Part 3: Guidelines for the Application of ISO 9001 to the development, supply and maintenance of software, Switzerland, 1991.

NIST Security Handbook: National Institute of Standards and Technology, U.S. Department of Commerce. An Introduction to Computer Security: The NIST Handbook, Washington, DC, 1995.

ITIL IT Management Practices: Information Technology Infrastructure Library. Practices and guidelines developed by the Central Computer and Telecommunications Agency (CCTA), London, 1989.

IBAG Framework: Draft Framework from the Infosec Business Advisory Group to SOGIS (Senior Officials Group on Information Security, advising the European Commission) Brussels, Belgium, 1994.

NSW Premiers Office Statements of Best Practices and Planning Information Management and Techniques: Statements of Best Practice #1 through #6. Premier's Department New South Wales, Government of New South Wales, Australia, 1990 through 1994.

Memorandum Dutch Central Bank: Memorandum on the Reliability and Continuity of Electronic Data Processing in Banking. De Nederlandsche Bank, Reprint from Quarterly Bulletin #3, Netherlands, 1998.

EDPAF Monograph #7, EDI: An Audit Approach: Jamison, Rodger. EDI: An Audit Approach, Monograph Series #7, Information Systems Audit and Control Foundation, Inc., Rolling Meadows, IL, April 1994.

PCIE (President's Council on Integrity and Efficiency) Model Framework: A Model Framework for Management Over Automated Information Systems. Prepared jointly by the President's Council on Management Improvement and the President's Council on Integrity and Efficiency, Washington, DC, 1987.

Japan Information Systems Auditing Standards: Information System Auditing Standard of Japan. Provided by the Chuo Audit Corporation, Tokyo, August 1994.

Control Objectives Controls in an Information Systems Environment: Control Guidelines and Audit Procedures: EDP Auditors Foundation (now the Information Systems Audit and Control Foundation), Fourth Edition, Rolling Meadows, IL, 1992.

CISA Job Analysis: Information Systems Audit and Control Association Certification Board. 鼎ertified Information Systems Auditor Job Analysis Study， Rolling Meadow, IL, 1994.

CICA Computer Control Guidelines: Canadian Institute of Chartered Accountants, Toronto, 1986.

IFAC International Guidelines for Managing Security of Information and Communications: International Federation of Accountants, New York, NY, 1997.

IFAC International Guidelines on Information Technology Management - Managing Information Technology Planning for Business Impact (Draft): International Federation of Accountants, New York, NY, 1998.

Standards for Internal Control in the U.S. Federal Government: U.S. General Accounting Office, Washington, DC, 1983.

Guide for Auditing for Controls and Security, A System Development Life Cycle Approach: NBS Special Publication 500-153: National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC, 1988.

Government Auditing Standards: U. S. General Accounting Office, Washington, DC, 1994.
Denmark Generally Accepted IT Management Practices: The Institute of State Authorised Accountants, Denmark, 1994.

SPICE: Software Process Improvement and Capability Determination. A standard on software process improvement, British Standards Institution, London, 1995.

DRI International, Professional Practices for Business Continuity Planners: Disaster Recovery Institute International. Guideline for Business Continuity Planners, St. Louis, MO, 1997.

IIA, SAC Systems Audibility and Control: Institute of Internal Auditors Research Foundation, Systems Audibility and Control Report, Altamonte Springs, FL, 1991, 1994.

IIA, Professional Practices Pamphlet 97-1, Electronic Commerce: Institute of Internal Auditors Research Foundation, Altamonte Springs, FL, 1997.

E & Y Technical Reference Series: Ernst & Young, SAP R/3 Audit Guide, Cleveland, OH, 1996.

C & L Audit Guide SAP R/3: Coopers & Lybrand, SAP R/3: Its Use, Control and Audit, New York, NY, 1997.

ISO IEC JTC1/SC27 Information Technology - Security: International Organisation for Standardisation (ISO) Technical Committee on Information Technology Security, Switzerland, 1998.

ISO IEC JTC1/SC7 Software Engineering: International Organisation for Standardisation (ISO) Technical Committee on Software Process Assessment. An Assessment Model and Guidance Indicator, Switzerland, 1992.

ISO TC68/SC2/WG4, Information Security Guidelines for Banking and Related Financial Services: International Organisation for Standardisation (ISO) Technical Committee on Banking and Financial Services, Draft, Switzerland, 1997.

CCEB 96/011, Common Criteria for Information Technology Security Evaluation: Common Criteria Implementation Board, Alignment and comparison of existing European, US and Canadian IT Security Criteria, Draft, Washington, DC, 1997.

Recommended Practice for EDI: EDIFACT (EDI for Administration Commerce and Trade), Paris, 1987.

TickIT: Guide to Software Quality Management System Construction and Certification. British Department of Trade and Industry (DTI), London, 1994

ESF Baseline Control - Communications: European Security Forum, London. Communications Network Security, September 1991; Baseline Controls for Local Area Networks, September, 1994.

ESF Baseline Control - Microcomputers: European Security Forum, London. Baseline Controls Microcomputers Attached to Network, June 1990.

Computerised Information Systems (CIS) Audit Manual: EDP Auditors Foundation (now the Information Systems Audit and Control Foundation), Rolling Meadows, IL, 1992.

付録III　用語

AICPA	American Institute of Certified Public Accountants
CICA	Canadian Institute of Chartered Accountants
CISA	Certified Information Systems Auditor
CCEB	Common Criteria for Information Technology Security
Control	The policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected
COSO	Committee of Sponsoring Organisations of the Treadway Commission
DRI	Disaster Recovery Institute International
DTI	Department of Trade and Industry of the United Kingdom
EDIFACT	Electronic Data Interchange for Administration, Commerce and Trade
EDPAF	Electronic Data Processing Auditors Foundation (now ISACF)
ESF	European Security Forum, a cooperation of 70+ primarily European multi-nationals with the goal of researching common security and control issues in IT
GAO	U.S. General Accounting Office
I4	International Information Integrity Institute, similar association as the ESF, with similar goals but primarily U.S.-based and run by Stanford Research Institute
IBAG	Infosec Business Advisory Group, industry representatives who advise the Infosec Committee. This Committee is composed of government officials of the European Community and itself advises the European Commission on IT security matters
IFAC	International Federation of Accountants
IIA	Institute of Internal Auditors
INFOSEC	Advisory Committee for IT Security Matters to the European Commission
ISACA	Information Systems Audit and Control Association
ISACF	Information Systems Audit and Control Foundation
ISO	International Standards Organisation (with offices in Geneva, Switzerland)
ISO9000	Quality management and quality assurance standards as defined by ISO
IT Control Objective	A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity
ITIL	Information Technology Infrastructure Library
ITSEC	Information Technology Security Evaluation Criteria. The harmonised criteria of France, Germany, the Netherlands and the United Kingdom, since then also support by the European Commission (see also TCSEC, the U.S. equivalent)
NBS	National Bureau of Standards of the U.S.
NIST (formerly NBS)	National Institute of Standards and Technology, based in Washington, D.C.
NSW	New South Wales, Australia
OECD	Organisation for Economic Cooperation and Development
OSF	Open Software Foundation
PCIE	President's Council on Integrity and Efficiency
SPICE	Software Process Improvement and Capability Determination - a standard on software process improvement
TCSEC	Trusted Computer System Evaluation Criteria, also known as The Orange Book: security evaluation criteria for computer systems as originally defined by the U.S. Department of Defense. See also ITSEC, the European equivalent
TickIT	Guide to Software Quality Management System Construction and Certification