GOVERNANCE INSTITUTE®

4.0

コントロール目標
マネジメントガイドライン
成熟度モデル

COBIT 4.0

IT ガバナンス協会®
IT ガバナンス協会(ITGI)(*www.itgi.org*)は、企業の情報技術の方向性とコントロールに関する国際レベルでの議論と標準化を推進するため 1998 年に設立された。効果的な IT ガバナンスは、IT によるビジネス達成目標のサポート、IT へのビジネス投資の最適化、および IT にかかわるリスクと機会の適切な管理を確実に保証する上で有用である。IT ガバナンス協会は、企業のリーダーや取締役会が IT ガバナンスにおける責務を果たす上で役立つ独自の調査内容、電子資料、および事例研究内容を提供している。

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E－mail: *info@itgi.org*
Web site: *www.itgi.org*

ISBN 1－933284－37－4
COBIT 4.0
Printed in the United States of America

COBIT 4.0 の日本語版について

１．Quality of the Translation

This Work is translated into Japanese from the English language version of COBIT 4.0 by the ITGI Japan with the permission of the IT Governance Institute. The ITGI Japan assumes sole responsibility for the accuracy and faithfulness of the translation.

１．本著作物の内容

この著作物は、IT Governance Instituteの許諾の下、日本ＩＴガバナンス協会（ITGI Japan)が、COBIT 4.0を英語から日本語に翻訳したものです。ITGI Japanは著作物の翻訳の正確さについてのみ、その責任を有します。

２．Copyright Notice

３．Disclaimer

ITGI created COBIT 4.0 (“Work”) primarily as an educational resource for controls professionals. ITGI makes no claim that use of any of the Work will assure a successful outcome.The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the controls professional should apply his or her own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

３．免責条項

ITGIは、主として専門家への教育目的で、本著作物を作成したものです。ITGIは、本著作物の使用に関し、如何なる責任も負いません。ITGIは、本著作物の正確性、完全性、最新性、商用性その他本著作物の使用者の特定の目的に合致することを、一切保証するものではありません。本著作物の使用は、本著作物の使用者の一切の責任に於いて使用して下さい。

COBIT 4.0

COBIT 4.0 の日本語版によせて

COBIT 4.0 の翻訳を公開することができ、大変うれしく思います。これも、NRI セキュアテクノロジーズ様、ISACA 東京支部、大阪支部、名古屋支部の有志の皆様の多大なる協力の賜物です。はじめにその功績に感謝の意を表したいと思います。とりわけ、翻訳を中心的に進めていただいた NRI セキュアテクノロジーズの広瀬真一様、翻訳のとりまとめを引き受けていただいた松原榮一様には、多忙な中ボランティアで今回の翻訳を完遂していただき感謝の念に耐えません。また、チームリーダの私に代わり、翻訳作業をしながら事務的な作業を積極的に引き受けていただいた妻川和佳様にも感謝いたします。

COBIT の初版が公表されたのが 1996 年です。その後現在までに 3 回の改訂が行われ、現在第 4 版となっています。その間、米国をはじめとする世界各国で情報システムに対する統制に関する事実上の標準として多くの人に利用されてきました。しかし残念ながら日本においては、翻訳が正式には行われなかったことから、その普及は一部の限られた人の間に限られてきたように思います。COBIT の翻訳がなかなか進まなかった背景には、その分量が多大であること、内容に専門性があることのみならず、COBIT は ISACA メンバーのいわばバイブルのようなものであり中途半端な翻訳はしたくないという思いもあったと思います。

今回の COBIT 4.0 の翻訳は、翻訳作業に携わった皆様、そして日本の ISACA メンバーの COBIT にかける熱い思いが詰まっています。ひょっとしたら完璧な翻訳ではないかもしれませんが、これからも随時改訂し、よりよいものにしていきたいと思っております。そして、多くの皆様に利用され、日本における IT ガバナンスの普及に貢献できれば幸いです。

今後とも、ISACA 及び ITGI の発展に皆様のご支援をいただければと思います。

ISACA 東京支部 2006-2007 副会長
COBIT 4.0 翻訳チームリーダー
丸山　満彦

COBIT 4.0 の日本語版によせて

ISACA 東京支部では、これまで、COBIT に関する様々な研究活動を続けてまいりました。過去にさかのぼると、COBIT の元となった“Control Objectives”の翻訳（「情報システム管理ガイド」として出版）に始まり、第 2 版、第 3 版（マネジメントガイドライン）の翻訳、公開を行ってまいりました。

この 1，2 年の間に、日本においては、日本語版 SOX 法に対する関心が高まってきており、“IT Control Objectives for Sarbanes-Oxley”の日本語訳を公表してから、COBIT ファミリーは日本でも事実上のスタンダードとして認知されるようになって来ました。そして、第 2 版は、新たに設立された日本 IT ガバナンス協会との共同作業により、COBIT 4.0 の日本語版に先立って公開することができました。

このような状況の中、COBIT 4.0 の日本語版をここに公開する運びとなりました。日本語化にあたっては、NRI セキュアテクノロジーズ株式会社様の多大なるご貢献と、東京･大阪･名古屋３支部から参加していただいた多くのボランティアの方々のご協力を頂きました。ISACA の日本 3 支部を代表して、そしてこの冊子を利用する専門家の皆様を代表して感謝の意を表します。

COBIT は、ISACA の活動の柱とする IT アシュアランス、情報セキュリティ、そして IT ガバナンスの分野での存在価値をますます高めています。これからも、多くの皆様に有用な情報を提供できるよう、活動を進めてまいりたいと思います。

ISACA 東京支部 2006-2007 会長
高須　昌也

ITGI　JAPAN　日本語化プロジェクト　第 2 弾

NRI セキュアテクノロジーズ株式会社様と ISACA 東京・大阪・名古屋支部のご協力により世界の IT ガバナンスと内部統制の準標準である COBIT 4.0 の日本語版を公開できることになりました。COBIT FOR SOX 2.0 と COBIT 4.0 を 2006 年中にとの目標に多くの方々のご協力により、ほぼ、目標を達成することができました。

COBIT の全体系を正式な形で翻訳して公開するのは今回がはじめてです。過去に ISACA 会員向けに 2.0 版、IT マネジメントガイド 3.0 版のみの公開が行われています。4.0 版では、経営戦略との整合性、価値創造、資源管理、リスク管理、成果管理など IT ガバナンスのフレームワークの追加が行われ、より経営の視点が強化されています。内部統制にとどまらず、IT 投資のガバナンスを幅広にとらえる考え方を参考にわが国独自の IT ガバナンス文化が創出されること願っております。

日本 IT ガバナンス協会代表
松尾　明

ACKNOWLEDGEMENTS

The IT Governance Institute wishes to recognise:

The Board of Trustees
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, International President
Abdul Hamid Bin Abdullah, CISA, CPA, Auditor General's Office, Singapore, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Jean−Louis Leignel, MAGE Conseil, France, Vice President
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Bent Poulsen, CISA, CISM, VP Securities Services, Denmark, Vice President
Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Emil D'Angelo, CISA, CISM, Bank of Tokyo−Mitsubishi, USA, Trustee
Ronald Saull, CSP, Great−West Life and IMG Financial, Canada, Trustee
Erik Guldentops, CISA, CISM, Belgium, Advisor, IT Governance Institute

The ITGI Committee
William C. Boni, CISM, Motorola, USA, Chair
Jean−Louis Leignel, MAGE Conseil, France, Vice Chair
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Tony Hayes, Queensland Health, Australia
Anil Jogani, CISA, FCA, Tally Solutions Limited, UK
John W. Lainhart IV, CISA, CISM, IBM, USA
Michael Schirmbrand, CISA, CISM, CPA, KPMG, Austria
Eddy Schuermans, CISA, PricewaterhouseCoopers, Belgium
Ronald Saull, CSP, Great−West Life and IMG Financial, Canada

The COBIT Steering Committee
Dan Casciano, CISA, Ernst & Young LLP, USA
Roger Debreceny, Ph.D., FCPA, University of Hawaii, USA
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgium
Steven De Haes, University of Antwerp Management School, Belgium
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISA, CISM, KPMG LLC, Austria
John W. Lainhart IV, CISA, CISM, IBM, USA
Ronald Saull, CSP, Great−West Life and IMG Financial, Canada
Michael Schirmbrand, CISA, CISM, CPA, KPMG, Austria
Eddy Schuermans, CISA, PricewaterhouseCoopers, Belgium
Roger Southgate, CISA, CISM, FCCA, UK
Mark Stanley, CISA, Toyota Financial Services, Canada
Dirk Steuperaert, CISA, PricewaterhouseCoopers LLC, Belgium

In addition to the individuals already recognised, ITGI is grateful to the following expert developers and reviewers:
Stephan Allemon, MCT Services, Belgium
Peter Andrews, CISA, CITP, MCMI, PJA Consulting, UK
Georges Ataya, CISA, CISM, CISSP, MSCS, PBA, Solvay Business School, Belgium
Gary Austin, KPMG, USA
Shafqat Azim, Gartner Consulting, USA
Neil Barton, Hewlett−Packard, UK
John W. Beveridge, CISA, CISM, CFE, CGFM, CQA, Massachusetts Office of the State Auditor, USA
Steve Bittinger, Gartner, Australia
Max Blecher, Virtual Alliance, South Africa
József Borda, Ph.D., CPA, CISA, CISM, Hunaudit Ltd., Hungary
Dirk Bruyndonckx, CISA, CISM, KPMG Advisory, Belgium
Ken W. Buechler, PMP, Great−West Life, Canada
Vincent A. Campitelli, Wachovia Corporation, USA
Don Caniglia, CISA, CISM, USA
Luis A. Capua, CISM, Sindicatura General de la Nación, Argentina
Sushil Chatterji, Edutech, Singapore
Jason Creasey, CISA, QiCA, Information Security Forum, UK
Jeffrey D. Custer, CISA, CPA, CIA, Ernst & Young, LLP, USA
Peter De Bruyn, Banksys, Belgium
Reynaldo J. de la Fuente, CISA, CISM, Datasec Ltd., Uruguay
Philip De Picker, MCA, CISA, National Bank of Belgium, Belgium
Jan Devos, Associatie Universiteit Gent, Belgium
Rupert Dodds, CISA, CISM, FCA, KPMG, New Zealand
Troy DuMoulin, Pink Elephant, Canada
Robert B. Emkow, CISA, Grant Thornton LLP, USA
Heidi L. Erchinger, CISA, CISSP, USA

ACKNOWLEDGEMENTS *CONT.*

Rafael Fabius, CISA, República AFAP SA, Uruguay
Christopher Fox, ACA, PricewaterhouseCoopers, USA
Bob Frelinger, CISA, Sun Microsystems, Inc., USA
Bob Gilbert, CISA, Tembec, Canada
Guy H. Groner, CISA, CIA, CISSP, USA
Peter Hill, CISA, CISM, IT Governance Network, UK and South Africa
Gary Hodgkiss, MBCS, CITP, Capgemini, UK
Benjamin K. Hsiao, CISA, Office of Inspector General, Federal Deposit Insurance Corporation (OIG/FDIC), USA
Wayne D. Jones, CISA, Australian National Audit Office, Australia
Niraj Kapasi, FCA, CISA, Kapasi Bangad & Co., India
Marco Kapp, Citicus Limited, UK
John A. Kay, CISA, USA
Kamal Khan, CISA, CISSP, MBCS, Rabobank, UK
Luc Kordel, CISA, RE, CISSP, CISM, CIA, RFA, RFCE, Dexia Bank, Belgium
Linda Kostic, CPA, CISA, USA
Sandeep Kothari, CA, CISA, CISM, CWA, ABN AMRO, Singapore
Elsa K. Lee, CISA, CISM, CSQA., Crowe Chizek LLP, USA
Debra Mallette, CSSBB, CISA, Kaiser Permanente, USA
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK
Akira Matsuo, CISA, CPA, ChoAoyama Audit Corp., Japan
Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia
Niels Thor Mikkelsen, CISA, CIA, Danske Bank A/S, Denmark
Simon Mingay, Gartner, UK
John A. Mitchell, CISA, QiCA, FIIA, MIIA, CITP, FBCS, CEng, LHS Business Control, UK
Jay S. Munnelly, CISA, CIA, CGFM, Federal Deposit Insurance Corporation, USA
Ed O'Donnell, Ph.D., CPA, Arizona State University, USA
Sue Owen, Department of Veterans Affairs, Australia
Rob Payne, Trencor Services (Pty) Ltd, South Africa
Andrea Pederiva, CISA, Deloitte, Italy
Vitor Prisca, CISM, Novabase, Portugal
Paul E. Proctor, CISSP, CISM, Gartner Inc., USA
David Pultorak, ITIL Masters, MCSE, CNE, CSP, CDP, CCP, CTT Fox IT, USA
Claus Rosenquist, CISA, TrygVesta, Denmark
Jeffrey L. Roth, CISA, CPEA, CHMM, USA
Patrick Ryan, CISA, KPMG, South Africa
John Sansbury, MBCS, CITP, Compass Management Consulting, UK
Max Shanahan, FCPA, CISA, Max Shanahan & Associates, Australia
Craig W. Silverthorne, CPA, CISA, CISM, IBM Business Consulting Services, USA
Chad Smith, Great－West Life, Canada
Gustavo A. Solis, CISA, CISM, Grupo Cynthus, Mexico
C. N. Srivatsan, CISA, FCA, Astral Management Consultants, India
Robert Stroud, Computer Associates, USA
Scott L. Summers, Ph.D., Brigham Young University, USA
Delton Sylvester, CISA, South Africa
Gilbert Van Fraeyenhoven, CISA, CISM, CISSP, MCA, Ernst & Young, Belgium
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium
Johan Van Grieken, CISA, Deloitte, Belgium
Peter Van Mol, Helios－IT, Belgium
Greet Volders, Voquals NV, Belgium
Thomas M. Wagner, Gartner Inc., USA
Robert M. Walters, CPA, CGA, CISA, Office of the Comptroller General, Canada
Phil Wilson, RuleSphere International Inc., USA
Freddy Withagels, Capgemini, Belgium
Tom Wong, CMA, CISA, CIA, Ernst & Young LLP, Canada

ITGI is pleased to recognise its sponsor and affiliates:
Bindview Corporation
ISACA chapters

COBIT 4.0 翻訳運営チーム

チームリーダー

東京支部	副会長	丸山　満彦

運営チームメンバー

東京支部	会長	高須　昌也
東京支部	副会長	太田　均
東京支部	常務理事(法務担当)	堀越　繁明
東京支部	常務理事(CISA 担当)	辻　哲宏
東京支部	常務理事(CISM 担当)	河端　宇一郎
東京支部	常務理事(調査研究担当)	木村　章展
東京支部	常務理事(教育担当)	岸　泰弘
東京支部	常務理事(基準担当)	中村　努
東京支部	理事	長尾　慎一郎

オブザーバ

大阪支部	元会長	小山　正弘
名古屋支部	会長	横山　宏

COBIT 4.0 翻訳チーム

関谷　浩之	(オリックス株式会社, CISA, CIA)
渡部　直人	(日本IBM株式会社, CISA, システム監査技術者)
松原　榮一	(ガートナー ジャパン, CISA)
五井　孝	(株式会社大和総研, CISA, システム監査技術者)
羽場　進	(CISA)
近野　章二	(株式会社日立製作所)
吉丸　成人	(監査法人トーマツ, CISA)
柳原　俊郎	(CISA, システム監査技術者)
福良　博史	(職業能力開発総合大学校東京校, CISA)
鈴木　マリ	(アフラック, CISA, CISM, CIA)
山瀬　恵	(CISA, システム監査技術者)
妻川　和佳	(監査法人トーマツ)
吉武　一	(日本ユニシス株式会社, CISA, CIA)
天野　八重子	(ピー・エー・ジー・インポート株式会社, CISA)
下道　高志	(サン・マイクロシステムズ株式会社, CISA, CISM)
清水　美欧	(日本電気株式会社, CISA, CIA, システム監査技術者)
上原　一浩	(カーディナルヘルス・ジャパン408株式会社, CISA, CIA)
藤井　正浩	(あずさ監査法人, CISA, システム監査技術者)
柘植　健藏	(株式会社プロティビティ ジャパン, CISA)
宗像　敏明	(チューリッヒインシュアランスカンパニー, CISA)
柳沼　克志	(株式会社ITプレナーズ　ジャパン・アジアパシフィック)
熊坂　祐二	(ベリングポイント株式会社, CISA)

COBIT 4.0翻訳協力

NRIセキュアテクノロジーズ株式会社　COBIT 4.0翻訳プロジェクトチーム

チームリーダー

広瀬　真一	(NRIセキュアテクノロジーズ株式会社, CISA, システム監査技術者)

メンバー

菅谷　光啓	(NRIセキュアテクノロジーズ株式会社, CISA, CISSP)
竹内　健治	(NRIセキュアテクノロジーズ株式会社, CISA, CISSP)
姫野　桂一	(NRIセキュアテクノロジーズ株式会社)
村主　俊彦	(NRIセキュアテクノロジーズ株式会社)
山倉　直	(NRIセキュアテクノロジーズ株式会社, CISA, システム監査技術者)
長谷川　剛	(NRIセキュアテクノロジーズ株式会社, CISA)
伊藤　清孝	(NRIセキュアテクノロジーズ株式会社, CISA)
薩摩　貴人	(NRIセキュアテクノロジーズ株式会社, CISA, CISSP)
上田　直哉	(NRIセキュアテクノロジーズ株式会社, CISA, システム監査技術者)
堤　順	(株式会社野村総合研究所)

COBIT 4.0

目　次

COBIT 4.0 へのフィードバックをお待ちしています。*www.isaca.org/cobitfeedback* からコメントをお送りください(訳者注:英語でのフィードバックとなります)。

COBIT エグゼクティブオーバービュー

COBIT エグゼクティブオーバービュー

多くの企業において、情報とその情報を支える技術は、最も価値ある資産であると同時に最も理解されにくい資産である。成功を収めている企業は、情報技術(IT)の便益を認識した上で、それらを利用して、利害関係者への価値の増大に貢献している。また、こうした企業は、たとえば、遵守しなければならない法令が増えてきていることや、多くのビジネスプロセスで IT が欠かせない役割を果たすようになっていることなどに関連するリスクを把握し、対処している。

今や、IT の価値を保証することの必要性、IT に関連するリスクと情報のコントロールに関連して増え続ける要求事項の管理が、企業のガバナンスにおいては重要な要素になっている。つまり、IT ガバナンスの主要な要素は、価値、リスク、コントロールである。

IT ガバナンスは、経営陣および取締役会が担うべき責務であり、IT が組織の戦略と組織の目標を支え、あるいは強化することを保証する、リーダシップの確立や、組織構造とプロセスの構築である。

また、IT ガバナンスとは、準拠すべき優れた実践方法(手法)を収集、整理し、これを仕組みとして定着させることによって、企業における IT が確実にビジネス目標をサポートできるようにするものである。IT ガバナンスを通じて、企業は情報を最大限に利活用することができ、便益の最大化、ビジネス機会に対する投資、競争優位性の確保を実現できるのである。こうした成果を上げるためには、IT のコントロールにかかわる何らかのフレームワークが必要である。すなわち、企業ガバナンスやリスク管理のフレームワークとして広く知られている Committee of Sponsoring Organisations of the Treadway Commission (COSO)発刊の『*Internal Control－Integrated Framework*』に適合し、かつ、これを補完できるフレームワーク、または、類似のフレームワークが必要である。

組織は、他のすべての資産と同様、情報資産に対しても、その品質、受託者としての責任、セキュリティにかかわる要求事項を満たす必要がある。また、マネジメント層は、アプリケーション、情報、インフラストラクチャ、要員といった、利用可能な IT 資源の利用を最適化する必要がある。これらの責務を果たし、組織の目標を達成するために、マネジメント層は、全社の IT アーキテクチャの現状を理解する必要がある。そして、その上で、どのようなガバナンスおよびコントロールを適用導入すべきかを決定する必要がある。

Control Objectives for Information and related Technology (COBIT®)は、ドメインとプロセスで構成されるフレームワークで、優れた実践方法(手法)を示し、管理しやすく、論理的な構成でアクティビティを提示するものである。さらに、アクティビティ(activity)を、管理しやすく論理的に理解しやすい構成で、提示するものである。COBIT による優れた実践方法(手法)は、多くの専門家の意見を代表するものである。提示される実践方法(手法)は、アクティビティをいかにして実行するかというよりは、その実行に対するコントロールに主眼を置いている。これらの実践基準は、IT 関連の投資の最適化、サービスの確実な提供、問題発生時の判断基準確立の拠り所となることを意図するものである。
ビジネス要件に対して IT を十分に機能させるには、マネジメント層は、内部統制システムまたはフレームワークを適切に導入する必要がある。COBIT のコントロールのフレームワークは、以下に示すニーズに応えるものである。

- ビジネス要件との関連付け
- 一般に認められたプロセスモデルによる IT アクティビティの体系的整理
- 活用すべき主要な IT 資源の識別
- 考慮すべき経営上のコントロール目標の設定

COBIT は、まず、ビジネスありきであり、ビジネス目標と IT 目標とを関連付け、各目標の達成度を測定するための測定基準と成熟度モデルを提供し、それらに関するビジネスプロセスオーナと IT プロセスオーナの責務を特定する。

COBIT はプロセスを重視し、そのプロセスモデルによって示される。プロセスモデルは、計画、構築、実行、およびモニタリングのすべての IT の責務領域に沿った形で 34 のプロセスから構成される。エンタープライズアーキテクチャの概念は、プロセスの成功に不可欠な資源、すなわちアプリケーション、情報、インフラストラクチャ、要員の特定に役立つ。

要するに、企業目標の達成に必要な情報を得るには、合理的にグルーピングされた一連のプロセスにより IT という資源を上手に管理する必要がある。

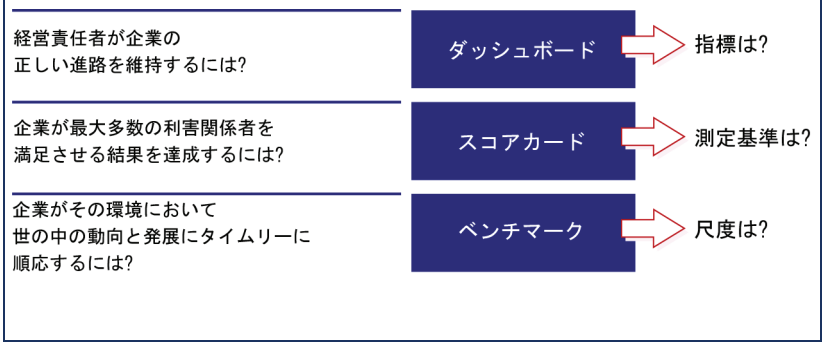
ところで、企業に必要な情報を提供する IT をどのようにコントロールすべきなのだろうか。どのようにしてリスクを管理し、企業が大きく依存している IT 資源を保全したら良いのだろうか。そして、企業は、IT による目標の達成とビジネスへの貢献をどうすれば確実に実現できるのだろうか。

まずマネジメント層は、ポリシー、手続、実践基準、および組織構造を実装することによって目指す、最終的な達成目標を定義したコントロール目標を設定する必要がある。コントロール目標を設定することで、以下の事項について、合理的な保証を与えることができる。

- ビジネス目標の達成
- 望ましくないイベントの防止または、発見および是正

次に、環境が多様化する今日、マネジメント層は、リスクやコントロールに関する難しい判断を迅速かつ適切に行うために、常に的確な情報を適時に得ることを必要としている。この要件について、何をどのように測定すべきだろうか。企業は、企業の現在の状況を見定め、どのような改善が必要であるか判断するための客観的測定指標を必要としており、この改善をモニタリングするための管理ツールキットを導入する必要がある。
従来から企業が直面している課題と、これに対処するために使用される管理情報ツールを図 1 に示す。ただし、ここに示すダッシュボードには指標が、スコアカードには測定基準が、ベンチマークには比較のための尺度が、それぞれ必要である。

図 1 管理情報



適切なITコントロールとパフォーマンスのレベルを決定すると同時に、モニタリングするという要件を満たすのが、COBIT 特有の仕様である。

- ソフトウェア工学研究所(CMU/SEI)の能力成熟度モデルから由来する、成熟度モデルと呼ばれる IT プロセス能力の**ベンチマーク**
- Robert Kaplan および David Norton のバランススコアカードの原則に基づいた、IT プロセスの結果と成果を定義および測定するための**目標と測定指標**
- COBIT の詳細なコントロール目標に基づいた、上記プロセスをコントロールするための**アクティビティの達成目標**

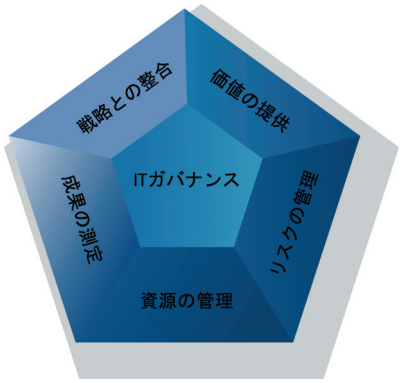
COBIT 成熟度モデルに基づくプロセス能力の評価が、IT ガバナンスを導入する上では重要なパートである。重要な IT プロセスおよびコントロールの特定後、成熟度モデルに基づく評価を行うことで、プロセス能力にどの程度ギャップがあるのかを明らかにし、それをマネジメント層に提示することができる。これにより、プロセス能力を到達すべきレベルにまで引き上げるための対応計画を作成できる。

つまり COBIT では、以下を確実に実現するためのフレームワークを提供することにより、IT ガバナンスをサポートする(**図 2**)。

- IT とビジネスとの整合がとられている
- IT によりビジネスが実現し、最大限の便益が得られている
- IT 資源が企業責任のもとに使用されている
- IT リスクが適切に管理されている

IT ガバナンスでは成果の測定が重要である。COBIT は、成果の測定をサポートしている。成果の測定とは、IT プロセスが何を提供する必要があるのか(プロセスの結果)、また、その IT プロセスがいかに結果を提供しているのか(プロセスの性能と)という観点から、測定可能な対象物を設定し、モニタリングすることである。多くの調査が示すところによれば、IT の費用、価値、およびリスクに関する透明性の欠如は、IT ガバナンスが求められる最も重要な要因のひとつである。IT ガバナンスの他の重点領域も影響するものの、透明性の確保は、主に成果の測定によって達成される。

図 2 IT ガバナンスの重点領域



- **戦略との整合**では、ビジネス計画と IT 計画とを確実に関連付けること、IT 価値の提供を定義、保守、検証すること、そして IT 運営を企業運営と整合させることに焦点を当てる。
- **価値の提供**では、提供サイクルを通じて、IT 価値を提供する。特に費用を最適化し、IT の本質的な価値を引き出すことで、戦略において IT に期待される便益の創出が確実に行われるようにする。
- **資源の管理**では、重要な IT 資源(アプリケーション、情報、インフラストラクチャ、要員)に対する投資の最適化と、適切な管理を対象とする。中でも主要な問題に関連しているのは、知識とインフラストラクチュアの最適化である。
- **リスクの管理**では、経営上層部がリスクを認識すること、企業のリスク傾向を明確に理解すること、(法・規制)遵守要件を理解すること、企業における重大なリスクに関する透明性、およびリスク管理における責務を組織に組み込むことが要求される。
- **成果の測定**では、戦略の実践状況、プロジェクトの完遂状況、資源の使用状況、プロセスの成果、およびサービスの提供状況を追跡およびモニタリングする。たとえば、戦略を従来の会計を超えて測定可能な目標に置き換えるバランススコアカードの使用など。

COBIT エグゼクティブオーバービュー

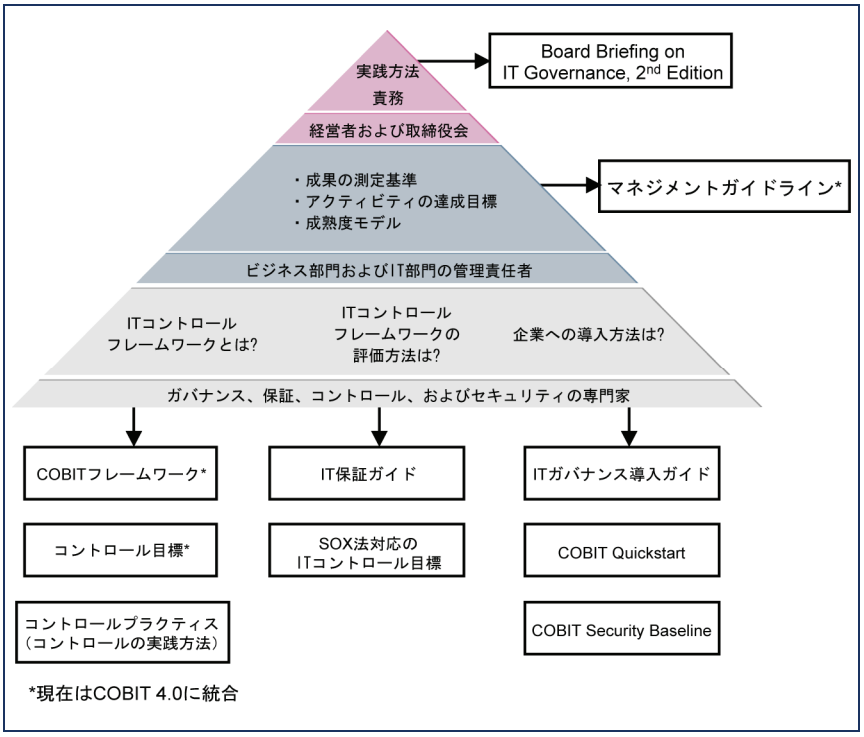
これらの IT ガバナンスが対象としている重点領域は、経営幹部層が企業内の IT を統制するために取り組むべき項目を表している。現場管理者は、進行中の IT アクティビティを整理し、管理するためにプロセスを使用する。COBIT では、通常 IT 部門で扱われるすべてのプロセスに対して一般的なプロセスモデルを規定しており、運用に携わる IT 管理者およびビジネス部門の管理者の双方が理解可能な共通の参照モデルを提供している。COBIT のプロセスモデルは、IT ガバナンスの重点領域と対応付けられており(付録Ⅱを参照)、現場管理者が実行すべき内容と経営陣が統制を望む対象とが橋渡しされている。

効果的なガバナンスを実現するため、経営幹部層は、現場管理者が、すべての IT プロセスを対象に定義されたコントロールフレームワークの範囲内で、コントロールを導入することを期待する。COBIT の IT コントロール目標は、IT プロセスごとに整理、分類されている。したがって、COBIT フレームワークにより、IT ガバナンスの要件、IT プロセス、および IT コントロールの関連性が明確に規定される。

COBIT は、IT の適正な管理およびコントロールに何が必要かに焦点を当てており、上位レベルに位置付けられるフレームワークである。COBIT では、他のより詳細な IT 標準やベストプラクティスとの整合および調整を行っている(付録Ⅳを参照)。COBIT は、これらの多様なガイドライン文書を統合する役割を果たしており、1 つの包括的なフレームワーク内で、主要な目標を要約すると同時に、これらの目標とガバナンスおよびビジネス要件との関連付けを行っている。

COSO(およびこれに準拠する同様のフレームワーク)は、一般的に、企業における内部統制フレームワークとして認知されている。COBIT は、IT 向けの内部統制フレームワークとして一般的に認知されている。

COBIT 製品は、3 つのレベルに整理されている(**図 3**)。おのおの、以下に示すグループをサポートする。
- 幹部経営層および取締役会
- ビジネス部門および IT 部門の管理責任者
- ガバナンス、保証、コントロール、およびセキュリティの専門家



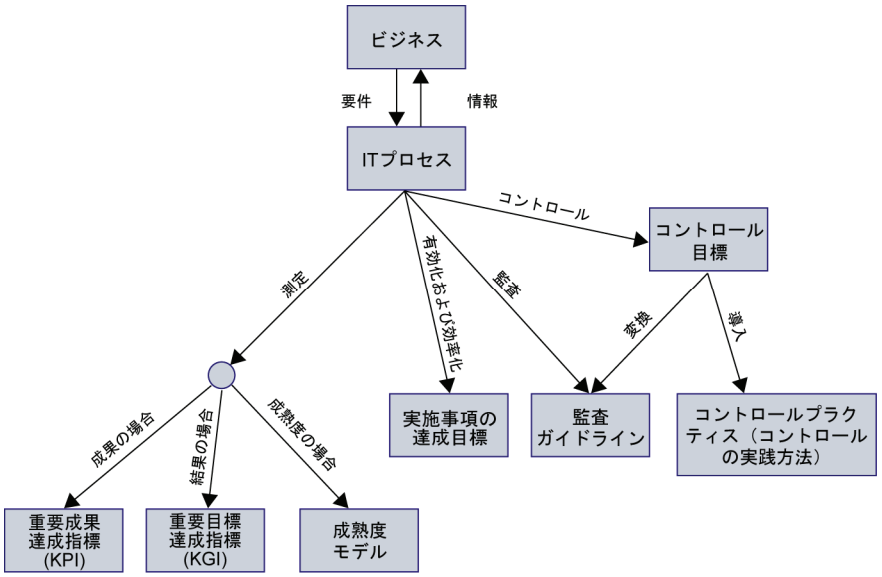
主に経営者を対象
- *Board Briefing on IT Governance, 2nd Edition*—IT ガバナンスの重要性、IT ガバナンスの問題、およびその管理における責務に対する経営者の理解を支援するように編纂されている。

主にビジネス部門および IT 部門の管理責任者を対象
- *マネジメントガイドライン*—責任の割り当て、成果の測定、およびベンチマーク評価と能力とのギャップの解消を支援するツールである。これらのガイドラインは、典型的なマネジメント層の疑問に対する回答を得る上で有用である。すなわち、IT のコントロールをどの程度にするか、そしてその費用の正当性をどう判断するのか。優れた成果であるか判断するための指標は何か。取り組むべき主要なマネジメントプラクティス(マネジメントの実践基準)は何か。他社はどうやっているのか。どのように測定し、比較すべきか。

主にガバナンス、保証、コントロール、およびセキュリティの専門家を対象
- *フレームワーク*—COBIT において、IT ガバナンス目標とベストプラクティスが、IT ドメインごとおよびプロセスごとにどのように編成され、ビジネス要件と対応付けられるか説明する。
- *コントロール目標*—すべての IT アクティビティについて、管理目標に関する一般的なベストプラクティスを規定する。
- *コントロールプラクティス(コントロールの実践基準)*—コントロールを導入する意義および導入方法のガイダンスを提供する。
- *IT 保証ガイド*—COBIT のすべての IT プロセスの監査について、一般的な監査アプローチおよび対応するガイドラインを提供する。
- *サーベインズ・オクスリー法(企業改革法)遵守のための IT 統制目標*—COBIT コントロール目標を基に IT 環境のコンプライアンスを確保するためのガイドラインを提供する。
- *IT ガバナンス導入ガイド*—COBIT が提供するものとそれを支援するツールキットを利用して、IT ガバナンスを導入するための一般的なロードマップを提供する。
- COBIT *クイックスタート*™—小規模組織向けおよび大企業の導入初期向けのコントロール基準を提供する。
- COBIT *セキュリティベースライン*™—企業内で情報セキュリティを導入するための必須手続に焦点を当てる。

これらすべての COBIT コンポーネントは相互に関連しており、多様なユーザによるガバナンス、管理、コントロール、および監査のニーズに対応している(**図 4**)。

図 4 COBIT コンポーネントの相互関係



COBIT は、マネジメント層を支援するフレームワークであり、ツールでもある。コントロール要件、技術上の課題、およびビジネスリスクについて現状とのギャップの橋渡しを可能とし、利害関係者に対して自身のコントロールレベルを説明可能とするよう留意したものである。COBIT を使うことで、企業全体の IT コントロールについて明確なポリシーと優れた実践基準を策定できる。COBIT は、継続的に更新され、他の標準とも調整が図られている。その結果、COBIT は、IT ベストプラクティスの集大成となっていると同時に、IT に関連するリスクと便益の理解と管理に役立つ、IT ガバナンスの包括的なフレームワークとなっている。COBIT のプロセス構造とその高いレベルからのビジネス志向のアプローチは、IT の全体像を浮き彫りにし、IT に関する決断を下すうえでとても役立つ。

IT ガバナンスのフレームワークとして COBIT を導入すると、次のような利点がある。
- ビジネス重視による、IT とビジネスとの整合性の向上
- マネジメント層の、IT の役割に関する理解の促進
- プロセス重視に基づく、オーナシップ(所有者)と責務の明確化
- サードパーティ(第三者組織)や監督機関による全般的な受容性の向上
- 共通の用語に基づく、すべての利害関係者による理解の共有
- IT 統制環境に関する COSO 要件の達成

以降、本書では COBIT フレームワーク、および COBIT の IT ドメインと 34 の IT プロセスごとに編成された COBIT のすべてのコアコンポーネントについて説明する。本書は、主要な COBIT ガイドライン用のリファレンスブックとして利用できる。巻末の付録もリファレンスとして有用である。

オンラインツール、導入ガイド、リファレンスガイド、教育用資料などの多数の ISACA および ITGI の製品により、COBIT 導入を容易にしている。これらの製品に関する最新情報は *www.isaca.org/cobit* から入手できる。

フレームワーク

COBIT フレームワーク

IT ガバナンスにおけるコントロールフレームワークの必要性

その理由

企業の幹部経営層は、情報が経営の明暗を左右するほどの甚大な影響力を持つものであるとの認識を次第に強めている。マネジメント層は、情報技術(IT)の取り扱い方についての理解を深め、IT を適切に活用することで競争優位性をさらに高められることを期待している。幹部経営層は特に、企業において、情報をうまく使うことによって、以下のような対処ができているかどうかを把握する必要がある。

- 企業目標を達成する見込みである
- 物事にたいしてそれを学び、適応できるだけの柔軟性を備えている
- 直面するリスクを慎重に管理している
- 機会を適切に認識し、対応している

好業績を上げている企業は、IT のリスクを認識し、IT の長所を利用して、以下の課題への対応方法を見出している。

- IT 戦略とビジネス戦略との整合性の確保
- IT 戦略および IT 達成目標の企業内への浸透
- 戦略と達成目標の実現を促進する組織構造の構築
- ビジネス部門と IT 部門間、および外部パートナーとの建設的な関係の構築と効果的なコミュニケーションの確立
- IT の成果の測定

企業は、以下のような目的をもった IT のガバナンスと、コントロールフレームワークを採用、導入することで初めて、ビジネス要件とガバナンス要件の両方を満足する効果的な対応策を講じることができる。

- ビジネス要件との IT との関連付け
- これらの要件に対する IT 成果の明確化(透明性の向上)
- IT に関連するアクティビティの一般的なプロセスモデルへの体系化
- 活用する主な IT 資源の特定
- 考慮すべき経営上のコントロール目標の定義

さらに、ガバナンスとコントロールフレームワークは、IT 管理のベストプラクティスの 1 つとなりつつあり、IT ガバナンスの確立および増加し続ける法的要件へのコンプライアンスを可能にする。

IT のベストプラクティスは、以下のような多くの要因によりその重要性が高まっている。

- 企業経営者や取締役会が求める IT 投資効果の向上(IT がビジネスニーズに応え、そのことで、利害関係者から見た価値を高める)
- 増大しがちな IT 費用への懸念
- 個人情報保護および会計報告(サーベンスオクスレー法、新 BIS 規制など)などの分野や、財務、医薬、医療など特定の領域における、IT コントロールの法的要件を満たす必要性
- サービスプロバイダの選定、およびサービスのアウトソーシングと調達の管理
- ネットワークセキュリティなどの IT にかかわるリスクの更なる多様化
- コントロールフレームワークとベストプラクティスの採用を含む IT ガバナンスのイニシアチブ、すなわち、IT に関連するアクティビティのうち、重要なものを対象として、モニタリングと改善を行い、ビジネス価値を高めると同時に、ビジネスリスクを低減を図る取組み
- 個別に構築された独自のアプローチではなく、標準のアプローチに従うことにより、可能な限り費用を最適化する必要性
- 成熟度の向上とそれに伴う COBIT、ITIL、ISO /IEC27002、17799、ISO 9001、CMM、PRINCE2 など広く認知されたフレームワークの適用の増加
- 企業において、一般に認知された標準に対する自社の達成状況と、競合他社と比較した場合の業績を評価(ベンチマーク評価)する必要性

関係者

ガバナンスおよびコントロールフレームワークは、個別のニーズを持つ社内外の多様な利害関係者に対応する必要がある。
- IT 投資による企業価値の創出を期待する組織内の利害関係者
  －IT 投資の意思決定者
  －IT 要件の決定者
  －IT サービスの利用者
- IT サービスを提供する社内外の利害関係者
  －IT 組織と IT プロセスの管理者
  －IT の開発者
  －IT サービスの運用者
- IT のコントロールやリスクに対する責任を負った社内外の利害関係者
  －セキュリティ、プライバシー、リスクなどに関する責任者
  －法令遵守に関する担当者
  －保険サービスを要求する者、提供する者

内容

前述の要件を満たすには、IT ガバナンスおよびコントロールのフレームワークが以下の一般的仕様を満たしている必要がある。
- ビジネス重視により、ビジネスで達成すべき目標と IT で達成すべき目標との整合をとれるようにする。
- 容易に内容把握できるように規定された体系により、プロセスのあり方を明確にし、何を対象とするか、どこまでをカバーするかを明らかにする。
- 一般に認知された IT のベストプラクティスおよび標準と整合すると同時に、特定の技術に依存していないことで、一般性を持ち、広く受け入れられる。
- すべての利害関係者が、通常、理解できる一連の用語と定義から成る、共通の言葉を使用する。
- 一般に認知された企業ガバナンス標準(COSO など)と、監督機関や外部監査者から要請される IT コントロールに準ずることにより、法規制へのコンプライアンスを支援する。

COBIT はどう対応しているか？

前出のセクションで述べた必要性に対応するため、COBIT フレームワークは、ビジネス重視、プロセス指向、コントロールベース、そして成果測定主導を主たる特徴として構築されている。

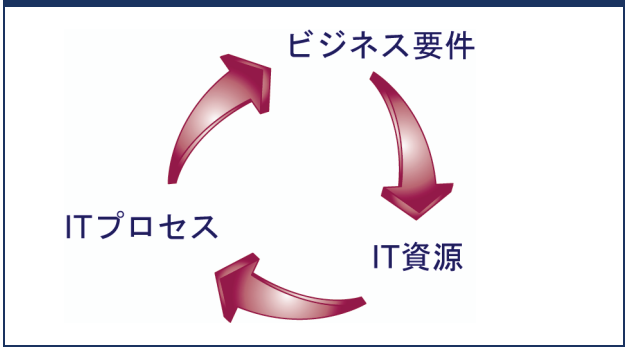
ビジネス重視

COBIT では、ビジネスを大前提としている。COBIT は、IT サービスプロバイダ、ユーザ、および監査人による使用のみを目的として設計されているのではなく、より重要な側面として、マネジメント層やビジネスプロセスオーナへの包括的な指針となるように設計されている。

COBIT フレームワークは、次の原則に基づいて作成されている(**図 5**)。すなわち、企業がその目標を達成するため、また必要な情報サービスを提供できるよう体系化された一連のプロセスを使用して IT 資源を管理およびコントロールするために、必要な情報を提供する、という原則である。

COBIT フレームワークでは、ビジネス要件との整合性を確保するための手段を提供している。

図 5 COBIT の基本原則



COBIT 情報要請規準

ビジネスの目標を達成するには、情報が一定のコントロール基準に従う必要がある。COBIT では、この基準を情報に対するビジネス要件と呼ぶ。品質、受託者としての責任、情報セキュリティにかかわる幅広い要求事項を基に、以下の 7 つの個別基準(部分的に重複)が定義されている。

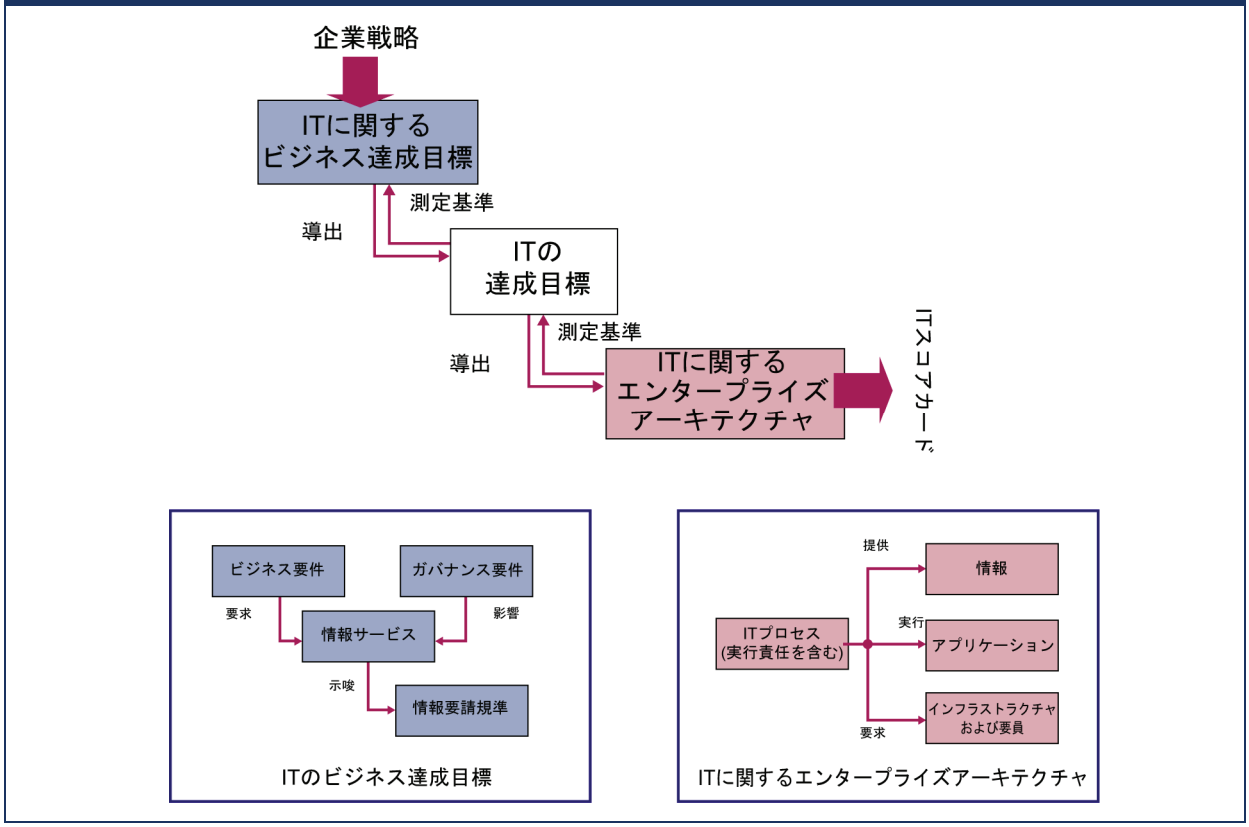
- 有効性。該当するビジネスプロセスに関連する適切な情報であること、またそれらの情報がタイムリーで正確かつ矛盾がなく、使用可能な状態で提供されることを指す。
- 効率性。情報の提供が資源の最適な(最も生産的かつ経済的な)利用により行われることを指す。
- 機密性。機密情報を不正な開示から保護することを指す。
- インテグリティ。情報の正確性と網羅性、およびビジネスの価値と期待に基づく情報の妥当性を指す。
- 可用性。現在および将来においてビジネスプロセスで必要な情報が利用可能であることを指す。また、そのために必要な資源および関連する能力の保全も考慮する。
- コンプライアンス。ビジネスプロセスが従うべき法律、規制、および契約条項の遵守、すなわち外部から課せられるビジネス基準と社内ポリシーの遵守を指す。
- 信頼性。マネジメント層が企業を運営し、受託者としての責任とガバナンス責任を果たせるように、適切な情報を提供することを指す。

ビジネス達成目標と IT の達成目標

情報要請規準は、ビジネス要件を定義するための一般的な方法であると同時に、一般的なビジネス達成目標と IT の達成目標の組合わせを規定し、ビジネス要件の設定と、各目標の達成状況の測定尺度を作成する際に、ビジネスとの関係付けをより適切に行うための基礎を与える。各企業は、ビジネスイニシアチブを実現するために IT を使用しており、これが IT に関するビジネス達成目標となり得る。付録 I に、一般的なビジネス達成目標と IT の達成目標とのマトリクスを示し、これらと情報管理の基準との関連を示す。これらの一般例は、企業の具体的なビジネス要件、達成目標、および測定指標を決定する際のガイドとして使用できる。

企業の戦略をサポートするサービスを、IT を利用して適切に提供するには、ビジネス部門(顧客)が要件確定を担当し、要件について方向性を示す必要があり、また、何を提供し、それをいかに提供するのかを IT 部門(供給者)が明確に理解している必要がある。**図 6** に、ビジネス部門が IT 対応によるイニシアチブ(IT のビジネス達成目標)を利用するには、企業の戦略をどのように目標に変換しなければならないのかを示す。これらの目標は、IT 部門自体の目標(IT の達成目標)の明確な定義に繋がる。さらにこれらの目標から派生して、企業の戦略における IT の適切な役割の実施に必要な、IT 資源および IT 能力(IT に関するエンタープライズアーキテクチャ)が定義される。こうした目標はすべて、顧客に分かりやすいビジネス用語で表現される必要がある。目標とその階層構造の効果的な関連付けにより、ビジネス部門は確実に企業の目標達成に対する IT の貢献を確認できる。

図 6 IT の達成目標および IT に関するエンタープライズアーキテクチャの定義



達成目標の体系を定義した後は、確実に想定どおり、運用が行われていることを確認するモニタリングが必要である。モニタリングを行うには、達成目標から導き出した測定指標を IT スコアカードに取り込む。これにより、顧客は、モニタリング結果を理解および追跡でき、供給者は供給者自身の社内目標に集中できるようになる。

付録 I では、一般的なビジネスの達成目標と、IT の達成目標、IT プロセス、および情報要請規準とのリレーションシップの全体像を掲げる。付録の各表では、COBIT の対象範囲と、COBIT とビジネス要因(driver)との間にあるビジネス上の関係の全体像を確認できる。

IT 資源

IT 部門は、明確に定義された一連のプロセスにより、これらの達成目標を実現する。一連のプロセスでは、ビジネス情報を活用しつつ、要員のスキルと技術インフラストラクチュアを使用して自動化されたビジネスアプリケーションを実行する。これらの資源は、プロセスとともに IT に関するエンタープライズアーキテクチャを構成する(**図 6**)。

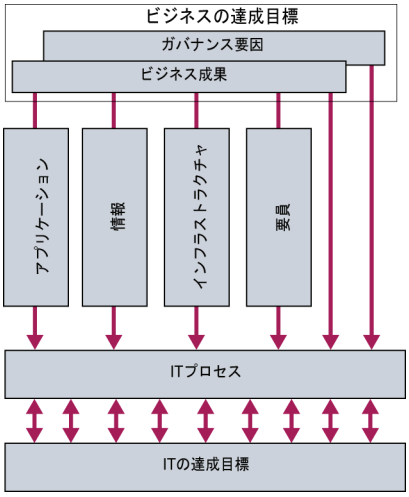
IT に関するビジネス要件に対応するため、企業は、期待する結果(売上や金銭的利益の向上など)を実現できるだけのビジネス上の能力(サプライチェーンの導入など)をサポートする十分な技術的能力(Enterprise Resource Planning(ERP)システムなど)を構築すべく、必要な資源に投資する必要がある。

COBIT で識別する IT 資源は、次のように定義される。

- アプリケーションとは、情報を処理する、自動化されたユーザシステムおよび手作業による手続を指す。
- 情報とは、ビジネスで使用される、任意の形式で情報システムに入力、処理、出力されるデータを指す。
- インフラストラクチュアとは、アプリケーションによる処理を可能にする技術および設備(ハードウェア、オペレーティングシステム、データベース管理システム、ネットワーク、マルチメディアなど、およびこれらを格納しサポートする環境)を指す。
- 要員とは、情報システムとサービスの計画、編成、調達、導入、提供、サポート、モニタリング、および評価に必要な要員を指す。社内の人材、アウトソーシング先の人材、および必要に応じて契約する人材が含まれる。

図 7 は、ビジネス達成目標と IT の達成目標にいかに関連しているか、IT プロセスを通じて IT 資源を管理することが IT の達成目標にいかに関連しているかをまとめたものである。

図 7 IT の達成目標の実現に向けた IT 資源の管理



プロセス指向

COBIT では、IT に関連するアクティビティを 4 つのドメインの一般的なプロセスモデルごとに定義する。4 つのドメインとは、計画と組織、調達と導入、サービス提供とサポート、およびモニタリングと評価である。各ドメインは、IT における従来の責任領域である計画、構築、実行、およびモニタリングに対応付けられる。

COBIT フレームワークは、企業内の誰もが IT に関連するアクティビティを参照および管理できるよう、参照用のプロセスモデルを共通の言葉で示している。IT に関連するすべての業務における運用モデルおよび共通の言葉の使用は、優れたガバナンスの実現に向けた最も重要な前提である。これにより、IT 成果の測定とモニタリング、サービスプロバイダとのコミュニケーション、および経営上のベストプラクティスの組み込みに関するフレームワークも提供される。プロセスモデルによりプロセスの担当責任が明確化され、実行責任および説明責任を定義できるようになる。

IT ガバナンスの有効性を高めるには、管理対象となる IT に関連するアクティビティおよび IT にかかわるリスクを理解することが重要である。これらは、以下のように要約できる。

計画と組織(PO)
このドメインでは、戦略と戦術を対象とし、ビジネス目標を達成するために IT を最大限に活用する方法を特定する。さらに、様々な立場から、戦略的構想の実現を計画、周知、および管理する必要がある。最終的には、適切な組織および技術インフラストラクチュアを整備する必要がある。このドメインは通常、マネジメント層による以下のような問いかけに対応している。
- IT 戦略とビジネス戦略は整合しているか。
- 企業はその資源の活用を最適化できているか。
- 組織の全員が IT 目標を理解しているか。
- IT リスクは理解および管理されているか。
- IT システムの質は、ビジネス上の必要性からみて妥当か。

調達と導入(AI)
IT 戦略を実現するには、IT ソリューションを特定、開発、または調達して、ビジネスプロセスに導入および統合する必要がある。IT ソリューションが継続してビジネス目標に沿うようにするため、既存システムの変更や保守についてもこのドメインで扱う。このドメインは通常、マネジメント層による以下のような問いかけに対応している。
- 新規プロジェクトは、ビジネス上の必要性を満たすソリューション策を提供できそうか。
- 新規プロジェクトは、予定どおりの期日に、予算の範囲内で実現できそうか。
- 新規システムは、導入後適切に機能するか。
- 変更は、現在のビジネス運営を混乱させることなく行われるか。

サービス提供とサポート(DS)
このドメインでは、求められるサービスの実際の提供について扱う。具体的には、サービスの提供、セキュリティの管理と継続性の管理、ユーザ向けサービスサポート、およびデータと運用設備の管理が含まれる。このドメインは通常、マネジメント層による以下のような問いかけに対応している。
- IT サービスは、ビジネス上の優先順位どおりに提供されているか。
- IT 運用にかかる費用(cost)は最適化されているか。
- 作業担当者は、IT システムを生産的かつ安全に使用可能か。
- 十分な機密性、インテグリティ、および可用性が確保されているか。

モニタリングと評価(ME)
すべての IT プロセスは、その質およびコントロール要件へのコンプライアンスを長期間定期的に評価する必要がある。このドメインでは、成果の管理、内部統制(internal control)のモニタリング、法令の遵守、およびガバナンスの提供について扱う。このドメインは通常、マネジメント層による以下のような問いかけに対応している。
- IT 成果の測定により、問題が手遅れになる前に発見されるか。
- マネジメント層は、内部統制が効果的かつ効率的であることを保証できるか。
- IT の成果をビジネス達成目標に結び付けることができるか。
- リスク、コントロール、コンプライアンス、および成果は測定および報告されているか。

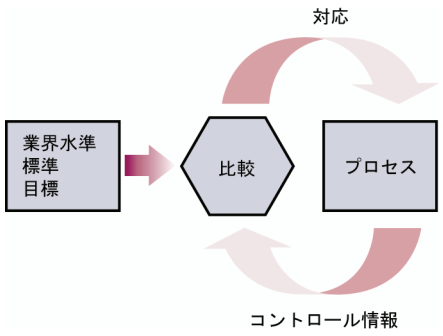
コントロールベース

プロセスにおけるコントロールの必要性
コントロールは、ビジネス目標の達成、および望ましくないイベントの阻止または発見と是正を合理的に保証するように設計されたポリシー、手続、実践基準、および組織構造であると定義される。

IT コントロールでなすべきことは、特定の IT に関する業務にコントロール手続を導入することにより、期待される結果や目的を記述することである。COBIT のコントロール目標は、各 IT プロセスを効果的にコントロールするための最小要件である。

図 8 に示す標準コントロールモデルをガイドとして使用できる。
コントロールの仕組みは、次のように例えると分かりやすい。暖房装置(プロセス)の温度(標準)を設定すると、当該装置は常に室温(コントロール情報)をチェック(比較)し、加温の強弱を促す信号を暖房装置に送る(対応)。

図 8 コントロールモデル



現場の実務に携わる管理者は、プロセスを利用することにより、進行中の IT の業務を整理し、管理できる。COBIT では、通常 IT 部門で扱われるすべてのプロセスに対して一般的なプロセスモデルを規定しており、IT 管理者および企業経営者の双方が理解可能な共通の参照モデルを提供している。効果的なガバナンスを実現するには、すべての IT プロセスを対象に定義されたコントロールフレームワークの範囲内で、現場の実務に携わる管理者がコントロールを導入する必要がある。COBIT の IT コントロール目標は、IT プロセス毎に編成されている。したがって、COBIT フレームワークにより、IT ガバナンスの要件、IT プロセス、および IT コントロールの関連性が明確に規定される。

COBIT の各 IT プロセスについては、コントロール目標の概要と、複数の詳細なコントロール目標が規定されている。一言で言えば、良く管理されたプロセスの特性を示したものである。

詳細なコントロール目標は、ドメインを示す 2 文字、プロセス番号、およびコントロール目標番号を並べた文字列により識別される。各 COBIT プロセスには、詳細なコントロール目標に加え、一般的なコントロール要件が規定されている(以下に、PCn(「プロセスコントロール」と番号)で識別して示す)。コントロール要件の全体像を把握するには、一般的なコントロール要件と詳細なプロセスコントロール目標を合わせて考慮する必要がある。

PC1 プロセスオーナ
各 COBIT プロセス毎に、オーナを割り当て、責任の所在を明確にできるようにする。

PC2 繰り返し使えること
COBIT プロセスは、繰り返し使えるように定義する。

PC3 目標および結果なしえるもの
各 COBIT プロセスについて明確な最終目標とその実現のための達成目標を設定し、効果的な実行を目指す。

PC4 役割と責任
各 COBIT プロセスについて明確な役割、アクティビティ、および責任を定義し、効率的な実行を目指す。

PC5 プロセスの成果
達成目標に対する各 COBIT プロセスの成果を測定する。

PC6 ポリシー、計画、および手続
COBIT プロセスの柱となる各ポリシー、計画、手続について、文書化、レビュー、更新、承認を行い、すべての関係者に周知する。

効果的なコントロールを行うことで、誤りが減り、目標と整合した首尾一貫した管理が行われるようになるため、リスクが低減し、プロセス間での価値のやりとりがより確実になると同時に、より効率が向上する。

COBIT では、各プロセスについて以下のような例も提示している。これらの例は、規範的または包括的なものではなく、実例的なものである。
- 一般的なインプットおよびアウトプット
- RACI チャートで示す、アクティビティと役割と責任の指針
- アクティビティの主要達成目標(最重要アクティビティ)
- 測定指標

プロセスオーナは、どのようなコントロールが必要かを理解することに加え、他のプロセスからのインプットとして何が必要なのかや、自身のプロセスのアウトプットとして、他のプロセスから何を必要とされているのかについても理解する必要がある。COBIT では、各プロセスについて、外部 IT 要件を含む鍵となるインプットおよびアウトプットの一般的な例が提示されている。アウトプットを示す表で「ALL」と示されているものは、他のすべてのプロセスへのインプットとなる。ただし、このようなアウトプットは、すべてのプロセスにおいてインプットとして明記されていない。このようなアウトプットには通常、品質標準や測定指標の要件、IT プロセスフレームワーク、文書化された役割と責任、企業の IT コントロールフレームワーク、IT ポリシー、人の役割と責任などが含まれる。

効果的なガバナンスでは、各プロセスにおける役割と責任の理解が鍵となる。COBIT では、各プロセスについて①実行責任者(R:Responsible) ②説明責任者(A:Accountable) ③協議先(C:Consulted)④報告先(I:Informed)を示す RACI チャートが提供されている。説明責任者は、最終的に全責任を負う人物であり、方針を示し、アクティビティについて許可を出す人物を指す。実行責任者は、作業を完遂させる人物を指す。他の 2 つの役割(協議先、報告先)が加わることにより、必要とされるすべての人が確実にプロセスに参加し、プロセスをサポートできるようになる。

ビジネスコントロールと IT コントロール
企業の内部統制の仕組みは、次の 3 つのレベルで IT に影響を与える。
- 幹部経営層レベルでは、ビジネス目標およびポリシーが設定され、企業戦略を実行するために企業の資源を配置および管理する方法が決定される。ガバナンスとコントロールの実行に対する総合的なアプローチは取締役会で決定され、企業全体に周知される。IT 統制環境は、この上位レベルの目標およびポリシーにより方向付けられる。
- ビジネスプロセスレベルでは、ビジネスに関連するアクティビティに個別にコントロールが適用される。多くのビジネスプロセスは自動化され、IT アプリケーションシステムに統合されているため、このレベルのコントロールの多くも自動化される。これらのコントロールを業務処理統制と呼ぶ。ただし、ビジネスプロセス内の一部のコントロール、たとえば、取引の認可、職務分離、手作業による調整などは、手作業による手続のままである。したがって、ビジネスプロセスレベルでのコントロールは、ビジネス部門により運用される手動コントロール、ビジネスコントロール、および自動化された業務処理統制を組み合わせたものである。業務処理統制の設計と開発には IT 部門によるサポートが必要であるが、定義と管理はいずれもビジネス部門の責務である。
- ビジネスプロセスをサポートするため、IT 部門は IT サービスを提供する。IT サービスは通常、多数のビジネスプロセスに対する共有サービスとして提供される。これは、開発または運用にかかわる IT プロセスの多くが企業全体に提供され、ネットワーク、データベース、オペレーティングシステム、ストレージなど、IT インフラストラクチュアの大部分が共通のサービスとして提供されるためである。すべての IT サービスに関連するアクティビティに適用されるコントロールを IT 全般統制と呼ぶ。業務処理統制の信頼性を高めるには、これらの全般統制を確実に運用する必要がある。たとえば、変更管理が十分に行われていない場合、自動インテグリティチェックの信頼性が予想外または意図的に脅かされる可能性がある。

IT 全般統制と業務処理統制
全般統制は、IT プロセスおよび IT サービスに組み込まれたコントロールである。以下に例を示す。
- システム開発
- 変更管理
- セキュリティ
- コンピュータオペレーション

ビジネスプロセスアプリケーションに組み込まれたコントロールは通常、業務処理統制と呼ばれる。以下に例を示す。
- 網羅性
- 正確性
- 妥当性
- 認可
- 職務分離

COBIT では、自動化された業務処理統制の設計と導入は IT 部門の責務であり、調達と導入ドメインの対象に含まれると同時に、COBIT の情報要請規準を使用して定義されたビジネス要件に基づいている、としている。ただし、業務処理統制の管理と責任は、IT 部門ではなくビジネスプロセスオーナにある。

IT 部門は、アプリケーションのサービスおよびそれをサポートするデータベースとインフラストラクチュアの提供とサポートを行う。

したがって、COBIT の IT プロセスにおいて IT 全般統制は扱われるが、業務処理統制は扱われない。業務処理統制はビジネスプロセスオーナの責務であり、先に述べたようにビジネスプロセスに統合されているためである。

以下に、推奨される一連の業務処理統制でなすべきことを、ACn(「業務処理統制」と番号)で識別して示す。

データの作成と認可のコントロール

AC1 データ準備手続

データを準備するための手続が整備されており、ユーザ部門に引き渡される。このコンテキストでは、インプットフォームを作成することで入力ミスや入力漏れを確実に最小限に抑えることができる。データ作成処理にエラー処理手続を組み込むことで、入力ミスや不正なデータがあった場合に、確実に発見、報告、および訂正できる。

AC2 原始帳票の認可手続

承認された要員が権限内で行動し、適切に原始帳票を準備しており、原始帳票の作成と承認において十分な職務分離が実施される。

AC3 原始帳票のデータ収集

手続の作成により、承認されたすべての原始帳票が確実に網羅的かつ正確で、責任の所在が適切に明確化されており、入力側への送信が遅延なく必要な場所に送られることが保証される。

AC4 原始帳票のエラー処理

データ作成処理にエラー処理手続を組み込むことで、入力ミスや不正なデータがあった場合に、適切に発見、報告、および訂正できる。

AC5 原始帳票の保持

データの修正や復元を容易にし、法的要件を満たすため、元の原始帳票を確実に保持するか、組織が適切な時間内に原始帳票を確実に再生できるよう、手続が整備される。

データ入力コントロール

AC6 データ入力の認可手続

承認された要員のみが確実にデータ入力を行うことを、手続により保証する。

AC7 正確性、網羅性、および認可のチェック

要員やシステムが生成またはインターフェースから入力した処理用トランザクションデータの正確性、網羅性、および妥当性が、さまざまなコントロールによりチェックされる。手続を定めることで、入力データの確認および編集が、可能な限り入力直後に行われることも保証される。

AC8 データ入力のエラー処理

誤入力されたデータの訂正と再送信に関する手続が整備、遵守される。

データ処理コントロール

AC9 データ処理のインテグリティ

データ処理に関する手続により、職務分離が確実に維持されていること、および実行された作業が定期的に確認されることが保証される。実行から次の実行までの総合コントロールや、マスターファイルの更新コントロールなど、適切な更新コントロールが確実に整備されていることも手続において保証される。

AC10 データ処理の妥当性チェックおよび編集
手続を定めることで、データ処理の妥当性チェック、認証、および編集が、可能な限り確実に処理直後に行われることが保証される。担当要員は、人工知能システムに基づいて重大な決定を承認する。

AC11 データ処理のエラー処理
データ処理のエラー処理手続により、誤りのあるトランザクションの特定が可能になる。また、誤りのあるトランザクションの処理や、他の有効なトランザクションの処理の不当な中断も回避できる。

データ出力コントロール
AC12 出力の処理と保持
IT アプリケーションからの出力の処理と保持は、定義済みの手続に従って行われ、プライバシー要件およびセキュリティ要件が考慮される。

AC13 出力の配布
IT アウトプットを配布する手続が定義、周知、および遵守される。

AC14 出力のバランス保持と調整
出力は、関連する総合コントロールに合わせて定期的にバランスが図られる。監査証跡により、トランザクションの処理の追跡および破損データの補正が容易になる。

AC15 出力のレビューとエラー処理
手続により、供給者および関連ユーザによる出力報告の正確性に関するレビューの実施が保証される。出力に含まれるエラーの特定と処理についても手続が整備される。

AC16 出力報告のセキュリティ確保
手続を定めることにより、ユーザへの配布前後の出力報告のセキュリティ保守が行われることが保証される。

境界におけるコントロール
AC17 真正性とインテグリティ
組織の外部で作成された情報について、重大な影響を及ぼす可能性がある処理を行う前に、情報を受け取った媒体(電話、ボイスメール、紙の文書、ファックス、または電子メール)を問わず、真正性とインテグリティが適切にチェックされる。

AC18 送信中や移送中の機密情報の保護
送信時および移送時における不正なアクセス、改変、および宛先間違いから、機密情報が十分に保護されている。

成果測定主導

すべての企業の基本的な要件として、自社の IT システムの現状を把握し、どのレベルの管理とコントロールが必要かを判断することがある。

企業の成果レベルを客観的に判断するのは容易ではない。ではこの要件について、何をどのように測定すべきだろうか。企業は、企業の現在の状況を見定め、どのような改善が必要であるか判定し、この改善をモニタリングするための管理ツールキットを導入する必要がある。

適正なレベルを決定するため、マネジメント層は、どこまで改善を行うべきであるか、そしてその費用を正当化するだけの価値はあるのかを検討しなければならない。

COBIT では、以下の概念の規定により、これらの問題に対応する。
- ベンチマーク評価を行い、必要な能力改善を特定可能にする成熟度モデル
- ビジネス達成目標と IT の達成目標をプロセスにおいてどのように達成するのかを示し、バランススコアカード方式に基づく内部プロセス成果の測定に使用される、IT プロセスの成果目標と測定指標
- プロセスを効果的に実行可能にするアクティビティの達成目標

成熟度モデル
民間企業や公営企業の経営幹部は、IT の管理状況について一層考慮することが求められている。この結果、各業務を改善し、情報インフラストラクチュアの管理とコントロールを適切なレベルにまで引き上げることが必要とされている。このような必要性が広く認識されつつある中、マネジメント層は、費用と利益のバランスと、関連する以下のような点について検討しなければならない。
- 業界内の競合他社の動向はどうか、また他社と比較した場合、自社はどのような位置付けにあるか。
- 適用可能な業界のベストプラクティスにはどのようなものがあるか、またそれらに対する自社の状況はどのようなものであるか。
- これらの比較結果から、自社は十分な対応を行っていると言えるか。
- IT プロセスの管理およびコントロールを適切なレベルにまで引き上げるために必要な対策を、どのように特定すべきか。

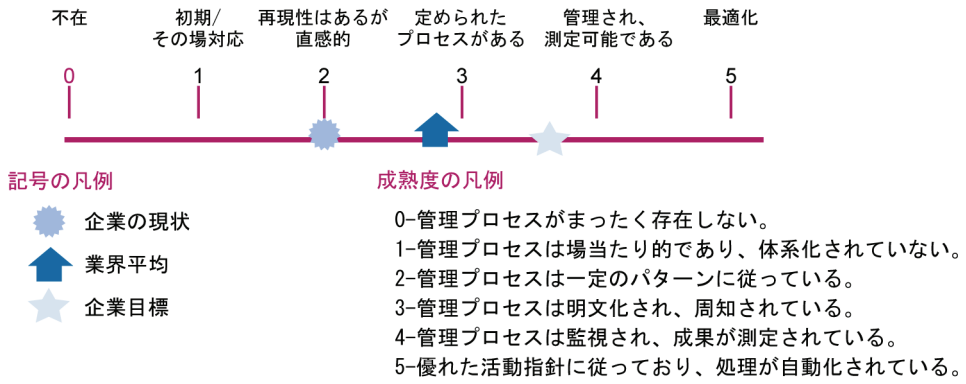
これらの疑問に対して、的確な答えを出すのは容易ではない。IT 部門のマネジメント層は、何をすべきかを明らかにするための効率的な方法がないものかと、ベンチマーク評価とセルフ評価のツールの類を常に関心をはらっている。COBIT のプロセス定義とコントロール目標の概要を押さえた段階で、プロセスオーナは、コントロール目標をベンチマークとして評価が実施できるようになる必要がある。これは次の 3 つのニーズに対応する。
1. 企業の現状を相対的に把握する測定指標
2. 企業の現状から、どのレベルに進むべきかを決定する効果的な方法
3. 進むべきレベルに対して、どの程度進捗したかを把握するツール

IT プロセスの管理とコントロールに関する成熟度モデルは、組織評価の手法に準じて構築されており、不在(0)から最適化(5)までのレベルで自己評価することができるようになっている。この方法は、ソフトウェア工学研究所(Software Engineering Institute)がソフトウェア開発能力の成熟度について定義した成熟度モデルが基になっている。どのようなモデルでも、尺度が微細すぎてはならない。モデル化の目的は一般的に、問題が存在する箇所と、改善策の優先順位を設定する方法を特定することであり、尺度が微細すぎるとそのシステムの使用は難しくなる上、理にかなった精度を提供できなくなる。コントロール目標をどの程度、厳格に遵守しているかを評価することが目的ではない。

成熟度レベルは、IT プロセスの現状と将来見込まれる状態を企業自身が認識できる説明資料(プロファイル)として設計されている。成熟度レベルは、下位レベルの全条件を満たさなければ次の上位レベルに移行できない、しきい値モデルとしての使用を前提としていない。COBIT の 34 の IT プロセスごとに作成された成熟度モデルを使用することで、マネジメント層は以下について認識できる。
- 企業の実際の能力－企業の現状
- 業界の現状－比較結果
- 企業の改善目標－企業のあるべき姿

マネジメント層への説明において、成熟度モデルを使用した評価結果を将来的な計画における投資対効果検討の論拠として容易に使用できるようにするには、結果を図式化する方法が必要である(**図 9**)。

図 9 成熟度モデルの図式化



34 の IT プロセスそれぞれについて成熟度モデルが定義されており、0(不在)から 5(最適化)までの漸進的な測定尺度が規定されている。この成熟度モデルは、**図 10** に示す一般成熟度モデルを基に作成されている。

COBIT は、IT プロセスを管理するために作成されたフレームワークであり、コントロールに主眼を置いている。これらの尺度は、適用にあたって実用的であり、平易で理解しやすいものである必要がある。IT プロセスの管理に関する事項は、本来、多様かつ主観的である。そのため意識を高め幅広い総意を獲得でき、改善に対する意欲を高める評価を通して、成熟度を評価することがもっとも望ましい方法である。これらの評価は、成熟度レベルの概要レベルで行うか、より厳密に、詳細な解説文と比較して行うことができる。いずれの方法でも、その企業において評価対象となるプロセスに関する専門的な知識が必要である。

図 10 一般成熟度モデル

0 不在　識別可能なプロセスが完全に欠落している。企業は、対応すべき問題が存在することすら認識していない。

1 初期/その場対応　企業は、対応が必要な問題の存在について認識している。ただし、標準化されたプロセスは存在せず、対応は、個人的に、または場合に応じて場当たり的に行われている。総合的な管理方法は体系化されていない。

2 再現性はあるが直感的　同じ仕事に携わる複数の要員において同等の手続が行われる段階にまで、プロセスが進歩している。標準的な手続に関する正式な研修や周知は行われておらず、実行責任は個人に委ねられている。個人の知識への依存度が高く、そのため、誤りが発生しやすい。

3 定められたプロセスがある　手続は標準化および文書化されており、研修により周知されている。ただし、このプロセスに従うかどうかの判断は個人に委ねられ、プロセスからの逸脱はほとんど発見されない。手続自体は、既存の実践基準を正式化しただけのものであり最適化されてはいない。

4 管理され、測定が可能である　手続の遵守状況をモニタリング、測定でき、プロセスが効果的に機能していないと判断された場合に対処が可能である。プロセスの改善が常時図られており、優れた実践基準を提供している。自動化やツールの活用は、限定的または断片的に行われている。

5 最適化　継続的改善、および他社との比較による成熟度モデル化の結果、プロセスがベストプラクティスのレベルにまで最適化されている。IT は統合され、ワークフローが自動化されている。これにより品質と有効性を改善するツールが提供され、企業の迅速な環境適応に貢献している。

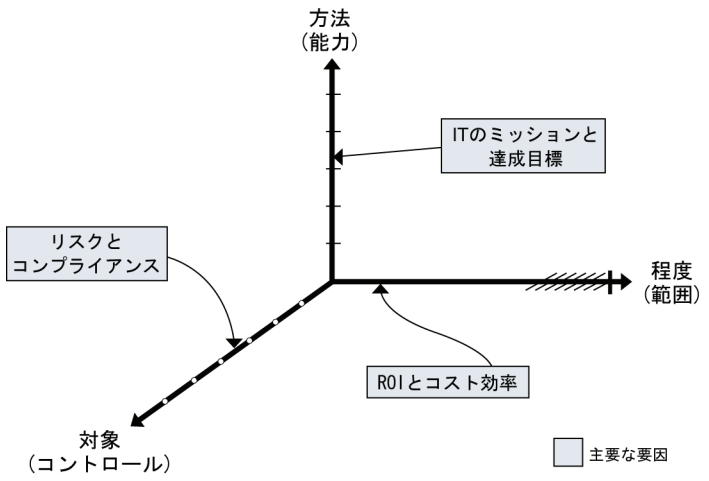
成熟度モデルによるアプローチの長所は、マネジメント層による自己評価が比較的簡単に実施できる点、および改善が必要な場合に想定される対策を比較的容易に把握できる点にある。プロセスがまったく存在しない場合も想定されるため、評価尺度には 0 というレベルも設けられている。0 から 5 までの評価レベルは、能力が「不在の状態」から「最適化された状態」まで、プロセスがどのように発展していくのかを表す単純な成熟尺度に基づいている。

ただし、プロセス管理能力は、プロセスの成果と同じではない。必要とされるプロセス管理能力は、ビジネス達成目標と IT の達成目標によって決まるが、これを IT 環境全体に対して同じレベルで適用する必要はない。たとえば、一貫して適用する必要がない場合や、一部のシステムまたは組織のみを対象とすればよい場合が想定される。IT プロセスにおける企業の実際の成果を判断するには、成果の測定(次のセクションを参照)が不可欠である。

適切なプロセス管理能力を適用することだけでリスクはある程度低減できる。とはいえ、企業は、リスクをどの程度許容するのか、しないのかについての考え方とビジネス目標を踏まえて、リスクの低減と価値の創出を保証することが必要であり、この観点から、コントロールを分析する必要がある。分析対象となるコントロールは、COBIT のコントロール目標によって導出される。付録Ⅲでは、内部統制の成熟度モデルを示す。これは、内部統制の確立と成果に関する企業の成熟度を表している。この分析は、外的な要因を受けて行われることが多いが、COBIT プロセスの「PO6 マネジメントの意図と方針の周知」および「ME2 内部統制のモニタリングと評価」に文書化されているように、仕組みとして定着させることが望ましい。

能力、成果、およびコントロールはすべて、プロセスの成熟度を表す軸となる(**図 11**)。

図 11 成熟度を表す 3 つの軸



成熟度モデルは、管理プロセスの発展度合い、つまり管理プロセスの実際の能力を測定する方法である。管理プロセスの発展度合いや能力の要件は、主に IT の達成目標およびその基となるビジネス上の必要性に左右される。実際に適用される能力の割合は、企業が投資から得ようとする効果に大きく左右される。たとえば、重要度の低いものに比べ、厳重なセキュリティ管理を必要とする重要なプロセスやシステムもある。一方、プロセスに適用する必要のあるコントロールがどの程度の強さが求められているのか、どの程度、高度なものが求められているのかは、企業がどの程度、リスクを許容するのか、しないのかといったリスク管理の選好度や、従わなければならないコンプライアンス上の要件によって決定されることが多い。

成熟度モデルの評価尺度は、責任者がマネジメント層に IT プロセス管理の不足点を示し、IT プロセス管理があるべきレベルに達するための目標を設定する上で役立つ。適正な成熟度レベルは、企業のビジネス目標、運営環境、および業界の実践基準に影響される。要するに、管理の成熟度レベルは、その企業における IT への依存度、技術がどの程度高度なのか、そして特に、企業の持つ情報の価値に依存する。

企業がその IT プロセスの管理とコントロールを改善するために、戦略的に設定する基準は、新しい国際標準および業界におけるベストプラクティスを検討することを通じて、設定することができる。今、まさに提示しようとしている実践基準は、将来的に、期待される成果レベルであると想定され、企業の長期的なビジョンを計画する上で参考になる。

成熟度モデルは、一般的な定性的なモデルを前提として構築されており(**図 10** を参照)、上位レベルになるに従い、以下の属性に基づく原則が追加されている。
- 認識および周知
- ポリシー、標準、および手続
- ツールと自動化
- スキルと専門知識
- 実行責任および説明責任
- 達成目標の設定および成果測定

図 12 の成熟度属性表は、IT プロセスの管理における特性を示し、プロセス不在の状態から最適化されたプロセスにいたる工程を示す。これらの属性は、より包括的な評価、ギャップ分析、および改善計画に利用できる。

つまり、成熟度モデルは、IT プロセスの管理とコントロールにおける企業の成長段階を示す一般的なプロファイルを提供するものであり、以下のように定義できる。
- 各々の成熟度レベルにおける一連の要件を示すと同時に、各々の成熟度がどのような状態であるかを示す
- 成熟度の差がどのように生じたのかの容易な測定を可能にする評価尺度である
- 実用的な比較に役立つ評価尺度である
- 現状と将来のあるべき姿を設定するための基礎である
- 選択したレベルの達成に必要な対応を判別するギャップ分析に活用できる
- 総合的に、企業における IT の管理状況を示す

COBIT の成熟度モデルでは、能力に焦点を当てているが、成果には必ずしも焦点を当てていない。成熟度モデルは、努力して達成すべき数値ではない。排他的な境界を定めてレベルを分離し、どのレベルにあるかを認定する正式な基準を設けようとするものでもない。成熟度モデルはむしろ、どのような状態であっても適用可能であるように設計されている。各レベルの説明を読むことで、企業が自社のプロセスがどのレベルに最も当てはまるのかを認識できるようになっている。適正な成熟度レベルは、企業のタイプ、環境、および戦略によって決定される。

成果、あるいは、いかに能力を活用し、展開するかは、費用対効果に基づく決定に左右される。たとえば、高レベルのセキュリティ管理では、企業が所有する最も重要なシステムにのみ焦点を当てなければならないこともある。

最後に、高レベルの成熟度になればなるほど、プロセスに対するコントロールは増加されるが、企業はリスクと価値の要因に基づいて、どのようなコントロールメカニズムを適用すべきかを分析する必要がある。COBIT のフレームワークで定義されている一般的なビジネス達成目標と IT の達成目標は、この分析を行う上で有用である。コントロールメカニズムは COBIT のコントロール目標により導出され、プロセスに対してどのようなコントロールを行うかが焦点となる。成熟度モデルでは、主にプロセスがどの程度、うまく管理されているのかが焦点となる。付録Ⅲには、企業における内部統制環境の状態と内部統制の確立状態を示す、一般成熟度モデルが記載されている。

統制環境を適切に導入するには、成熟度の 3 側面(能力、成果、およびコントロール)すべてについて、適切な対応を行う必要がある。成熟度が向上すると、リスクが低減し、効率性が向上する。その結果、誤りが減少し、プロセスの見通しが立てやすくなり、資源利用の費用効率が向上する。

図 12 成熟度属性表

認識および周知	ポリシー、標準、および手続	ツールと自動化	スキルと専門知識	実行責任および説明責任	達成目標の設定および成果測定
1 プロセスの必要性が認識されつつある。 問題について散発的な周知が行われている。	プロセスと実践基準は場当たり的である。 プロセスおよびポリシーが定義されていない。	いくつかのツールが存在するものの、標準のデスクトップツールに準ずる形で使用されている。 ツールの使用については特に定められていない。	プロセスに必要なスキルが特定されていない。 研修計画が存在せず、正式な研修は行われていない。	実行責任と説明責任について定義されていない。問題が発生した場合は、要員がそれぞれのイニシアチブに基づいて事後的に対応している。	達成目標が明確でなく、成果測定は行われていない。
2 対応の必要性が意識されている。 経営層は、全体的な課題について周知している。	類似した共通のプロセスが採用され始めているが、個人の専門知識に依存しており、大部分において直感的である。 個人の専門知識により、プロセスのいくつかの局面は再現可能である。ポリシーと手続の一部が文書化されているか、非公式ではあるが認識されている場合がある。	ツールの使用に関する共通のアプローチは存在するが、主担当者が作成した対応策を基にしている。ベンダーツールが入手されていたとしても、主担当者が作成した対応策を基に使用されている。 ベンダーツールが入手されていたとしても、正しく適用されていない場合や、使用されていない場合がある。	重要な領域に関するスキルの最小要件が特定されている。 研修は、合意済みの計画に沿った形ではなく、必要に応じて行われており、実地で非公式な研修が行われている。	責任に関する公式な合意は得られておらず、個人が各自の実行責任を想定し、説明責任も負っているものと認識されている。問題発生時には実行責任に関する混乱が生じ、責任転嫁が発生しがちである。	達成目標の設定が多少行われており、いくつかの財務対策が作成されているが、経営幹部にのみ周知されている。特定の領域のみにおいて、一貫性のないモニタリングが行われている。
3 対応の必要性が理解されている。 マネジメント層は、より正式化および構造化された方法で周知を行っている。	優れた実践基準が使用され始めている。 鍵となるすべてのアクティビティについて、プロセス、ポリシー、および手続が定義され、文書化されている。	プロセスを自動化するため、ツールの使用方法と標準化に関する計画が定義されている。 ツールはその基本目的に合わせて使用されているが、合意済みの計画に完全には従っていない場合や、他のツールと統合されていないことがある。	すべての領域についてスキル要件が定義され、文書化されている。 正式な研修計画が作成されているが、正式な研修は依然として個人的なイニシアチブに基づいて行われている。	プロセスの実行責任と説明責任が定義されており、プロセスオーナが特定されている。実行責任を果たすために必要な全権限を、プロセスオーナが保有していない可能性が高い。	有効性の達成目標および測定指標がいくつか設定されているが、周知されていない。ビジネス達成目標との明確な関連付けは存在する。成果測定プロセスが作成され始めているが、一貫して適用されていない。ITバランススコアの手法が採用されており、根本原因の分析が時折、直感的に適用されている。
4 要件全体が理解されている。 成熟した周知技法が適用され、標準的な周知ツールが使用されている。	プロセスが完全な形で確立されている。内部のベストプラクティスが適用されている。 プロセスの全側面が文書化されており、再現性がある。ポリシーがマネジメント層によって承認され、受け入れられている。プロセスと手続の作成と管理が標準化され、遵守されている。	ツールは、標準化された計画に従って導入されており、一部のツールは関連する他のツールと統合されている。 プロセスの管理を自動化し、重要なアクティビティとコントロールをモニタリングするため、ツールが主要な領域で使用されている。	すべての領域についてスキル要件が定期的に更新されている。すべての重要領域についてスキル向上が保証され、資格取得が奨励されている。 研修計画に従って成熟した研修技術が適用され、知識の共有が奨励されている。社内の各領域の専門家が研修に関与しており、研修計画の有効性が評価されている。	プロセスの実行責任と説明責任が定着して、広く理解されており、プロセスオーナが各自の責任を完全に果たせるようになっている。成果に報いる報酬の文化が定着しており、積極的な対応が意欲的に取り組まれている。	効率性と有効性が測定および周知され、ビジネス達成目標および IT 戦略計画と関連付けられている。IT バランススコアカードが一部の領域に導入されており、例外があればマネジメント層により発見される。また、根本原因の分析が標準化されている。継続的な改善が行われ始めている。
5 要件が先進的かつ先見的に認識されている。 動向を踏まえ、先を見越した周知が行われ、成熟した周知技法が適用されて、統合された周知ツールが使用されている。	外部のベストプラクティスと標準が適用されている。 文書化されたプロセスを基に、ワークフローが自動化されている。プロセス、ポリシー、手続が標準化および統合されており、全体的な管理および改善が可能になっている。	標準化されたツールセットが企業全体で使用されている。 プロセスを完全にサポートできるように、ツールは、関連する他のツールと完全に統合されている。 ツールを使用して、プロセスの改善とコントロール例外の自動検知がサポートされている。	組織は、明確に定義された個人および組織の達成目標を基に、スキルの継続的な向上を正式に推奨している。 研修と教育は、外部のベストプラクティスと、最先端のコンセプトと技術の使用に対応している。知識の共有は企業文化となっており、ナレッジベースシステムが提供されている。外部の専門家や業界リーダーの指導を受けている。	プロセスオーナは、決定および対処に必要な権限を与えられている。実行責任の理解は、組織全体に一貫して浸透している。	IT バランススコアカードを全領域において適用することにより、IT 成果をビジネス達成目標に関連付けた、統合された成果測定システムが存在する。例外があれば、いずれの領域であってもマネジメント層により一貫して発見される。また、根本原因の分析が適用されている。継続的な改善が日常化されている。

成果の測定

COBIT では、目標と測定指標が以下の 3 つのレベルで定義されている。

- IT の達成目標と測定指標。IT に対するビジネス部門の期待事項を定義する(IT の成果の測定にビジネス部門が使用する)。
- プロセスの達成目標と測定指標。IT の目標をサポートするために IT プロセスに要求される事項を定義する(IT プロセスオーナの成果を測定する方法)。
- プロセスの成果測定指標(達成目標が実現する見込みを示すために、プロセスの実行状況を測定)。

COBIT では、2 つの測定指標を使用する。目標達成指標と成果達成指標である。目標達成指標は下位レベル、成果達成指標は上位レベルとなる。

重要目標達成指標(KGI)は、IT プロセスのビジネス要件が達成されたかどうかを、マネジメント層が(事後的に)把握するための測定指標を定義したものである。ビジネス要件は、通常は以下のような情報管理の規準として表される。

- ビジネス上の必要性に対応するために必要な情報の可用性
- インテグリティと機密性の欠如のリスク
- プロセスと運用の費用効率
- 信頼性、有効性、およびコンプライアンスの確保

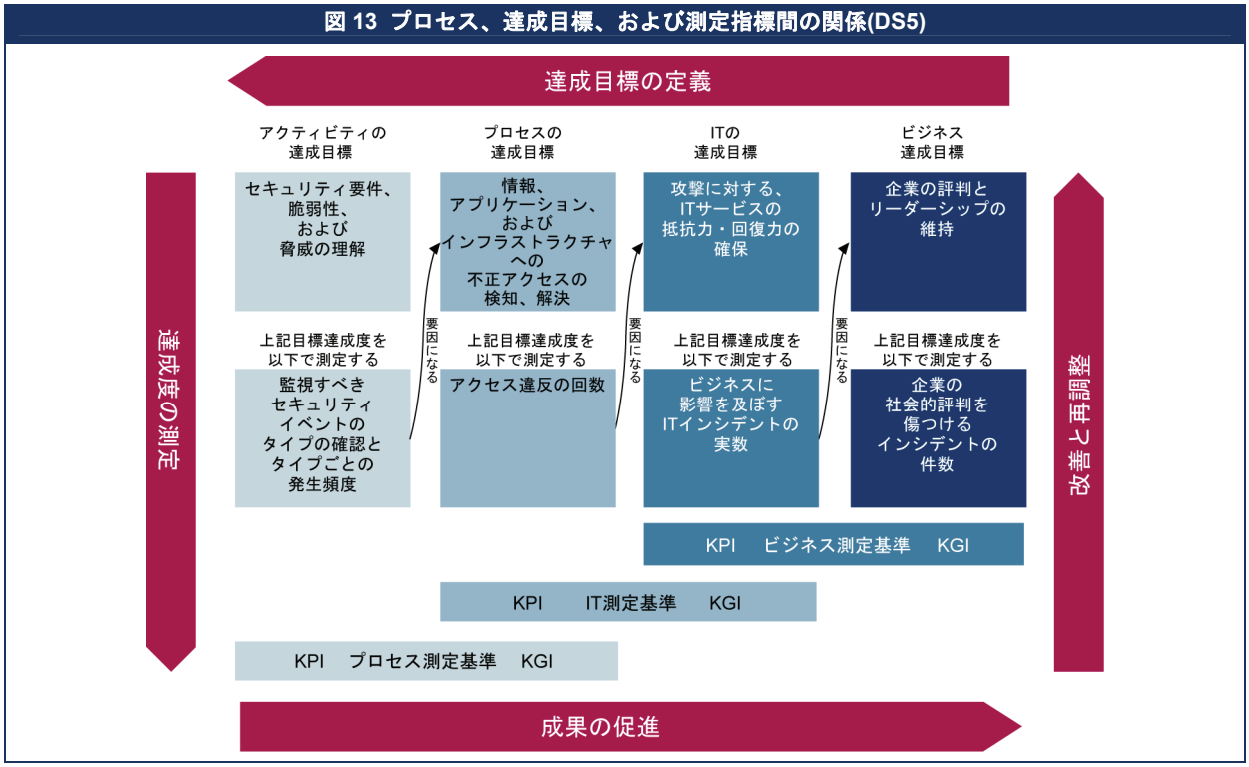
重要成果達成指標(KPI)は、達成目標の実現に向けた IT プロセスの実行状況を判断する測定指標を定義したものである。KPI は、目標が達成される見込みを判断するための最も重要な測定指標である。また、KPI は、能力、実践基準、およびスキルに関する優れた測定指標となる。KPI では、アクティビティの達成目標が測定される。アクティビティの達成目標は、プロセスの効果的な実行に向けプロセスオーナが実行すべき事項である。

有効な測定指標は、以下の特性を持つ必要がある。

- 努力の程度に対する幅広い見識を反映(成果および目標達成と、そのために費やされる努力との比較に関する見識)
- 内部比較が可能(たとえば、基準に対する割合や長期間にわたる数値)
- 企業の規模や業界を問わず外部比較が可能
- 精度の低い多数の測定指標よりも、精度の高い少数の測定指標が望ましい(さまざまな手段に対応できる非常に優れた測定指標であれば、測定指標は 1 つでもよい)
- 簡単に測定でき、目標と混同されにくいことが必要

図 13 は、「DS5 システムセキュリティの保証」を例に、プロセス、IT の達成目標、ビジネス達成目標、およびさまざまな測定指標間の関係を示している。

図 13 プロセス、達成目標、および測定指標間の関係(DS5)

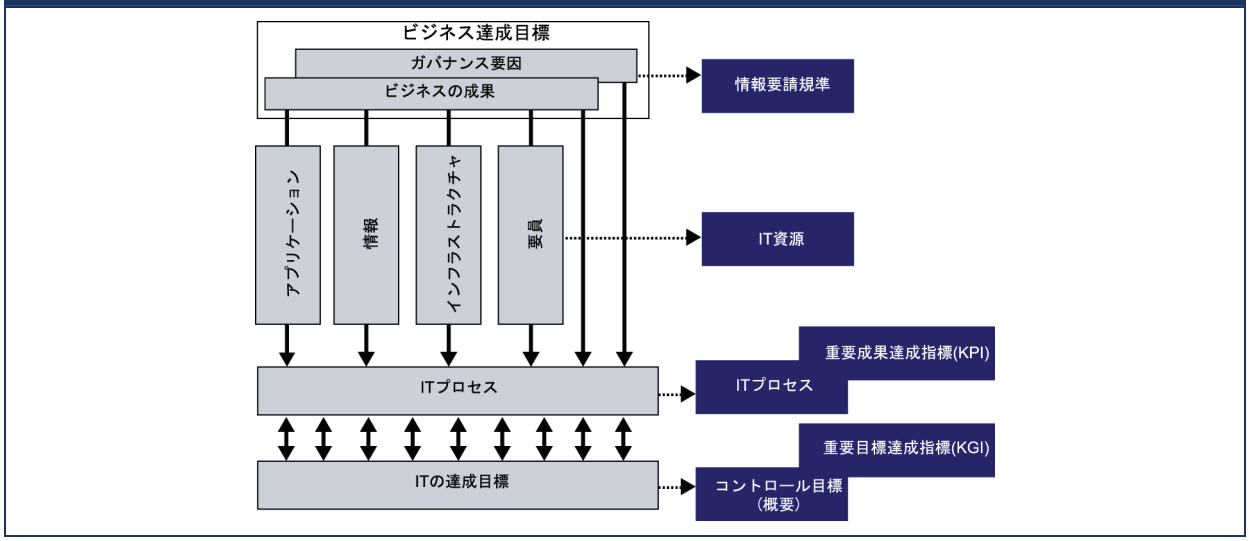


達成目標は、トップダウンで定義される。まず、ビジネス達成目標により複数の IT 達成目標が決定され、次に IT 達成目標によりさまざまなプロセス毎の達成目標が決定され、最後にそれぞれのプロセス達成目標毎により、アクティビティの達成目標が設定される。目標の達成は、成果の測定指標(重要目標達成指標(KGI))によって測定され、より上位の達成目標の達成度を左右する要因となる。たとえば、アクティビティの達成目標の達成度合いを測定する測定指標は、プロセスの達成目標の成果要因(重要成果達成指標(KPI))そのものである。測定指標の存在によって、マネジメント層による成果の補正と、達成目標に向けた再調整が可能になる。

COBIT フレームワークモデル

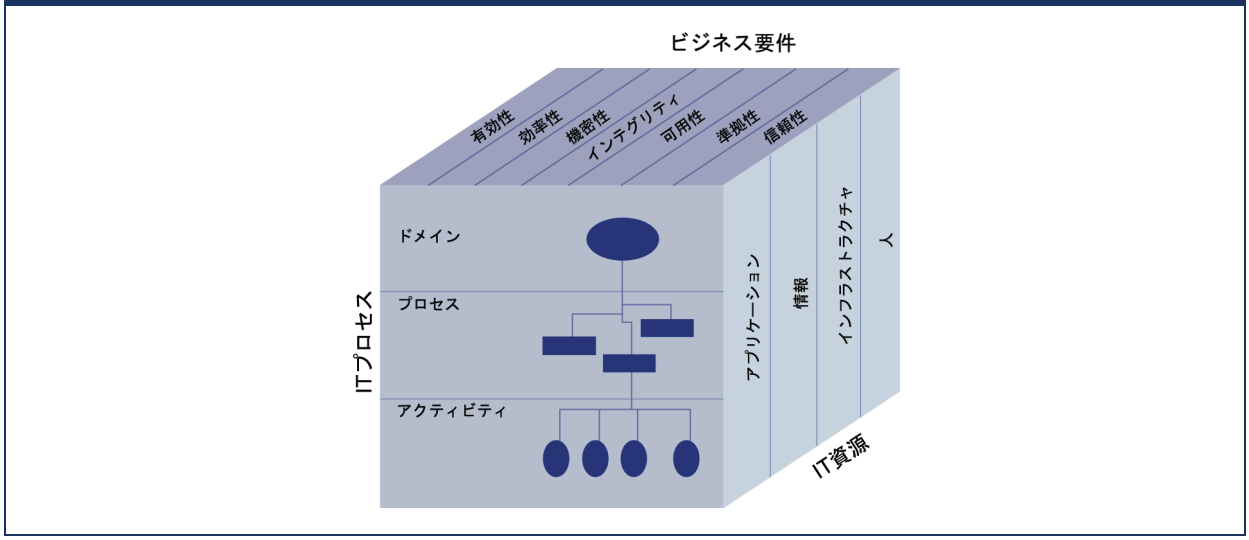
COBIT フレームワークは、このような背景に基づき、情報およびガバナンスのビジネス要件を、IT サービス機能の目標に関連付ける。COBIT プロセスモデルにより、IT に関連するアクティビティの実行とその実行を支える資源を、COBIT のコントロール目標を基に適切に管理およびコントロールできるようになる。同時に、COBIT の KGI 測定指標と KPI 測定指標を使用して IT に関連するアクティビティとコントロールとの間の整合をとることができると同時に、それぞれの目標達成状況をモニタリングできるようになる(図14)。

図 14 COBIT における管理、コントロール、整合、およびモニタリング



つまり、IT 資源を IT プロセスで管理することで、ビジネス要件に対応した IT の達成目標が達成される。**図 15** の COBIT キューブで示すように、これは、COBIT フレームワークの基本原則である。

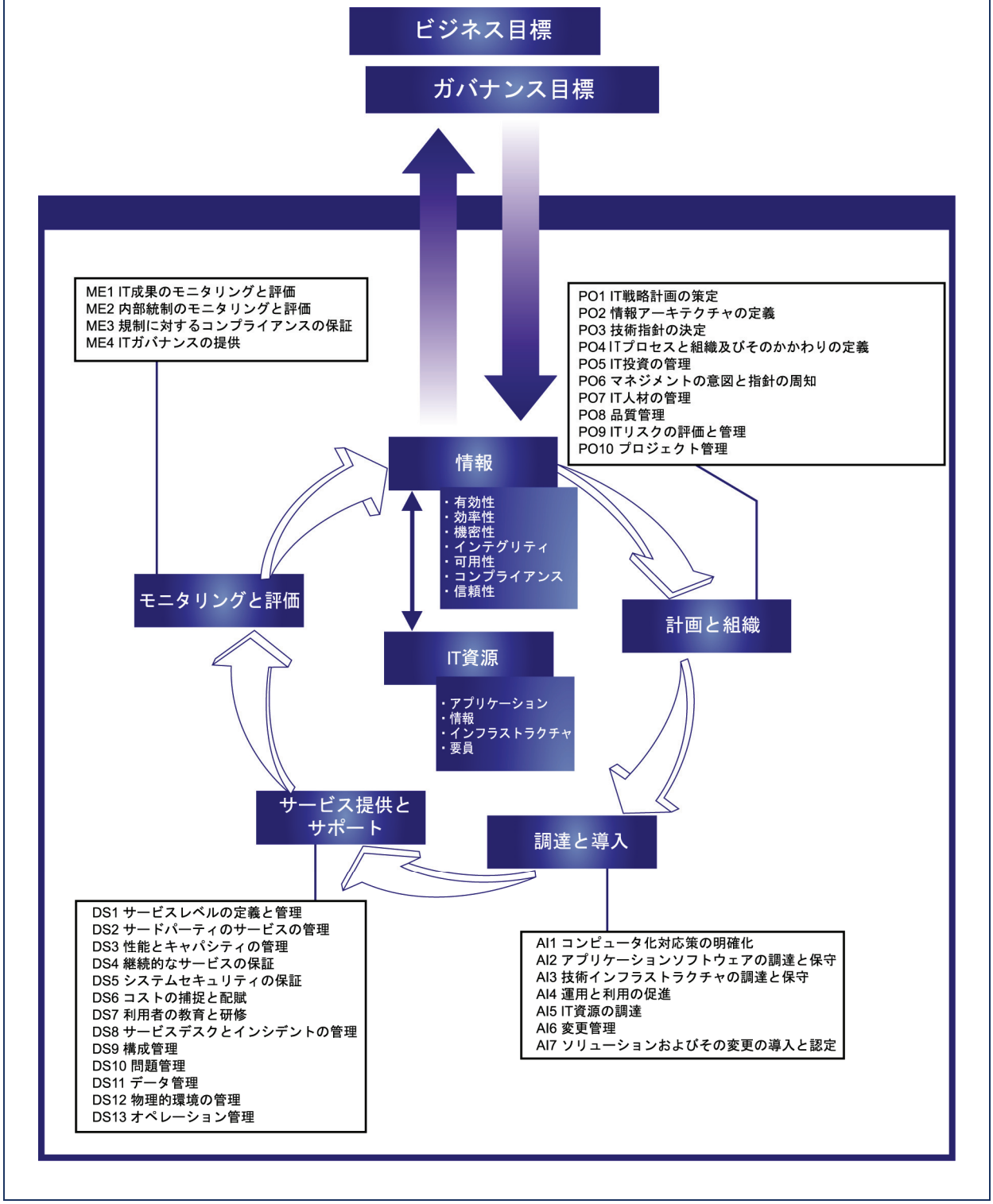
図 15 COBIT キューブ



COBIT 4.0

COBIT フレームワークのより詳細な全体像を**図 16** に示す。34 の汎用プロセスを含む 4 つのドメインの COBIT プロセスモデルで IT 資源を管理し、ビジネス要件およびガバナンス要件に従ってビジネス部門に情報を提供する。

図 16 COBIT フレームワークの全体像



COBIT の一般的適用性

COBIT は、既存の IT 標準およびベストプラクティスを分析した上で、これらと整合するように設計されている。また、広く認知されているガバナンス原則に準拠している。COBIT は、同様のガイドラインの中で上位に位置づけられており、ビジネス要件に対応する形で作成され、IT に関連するアクティビティの全範囲を対象としている。また、効果的なガバナンス、管理、およびコントロールを達成する方法ではなく、何を達成する必要があるかという点に焦点を当てている。したがって COBIT は、IT ガバナンスの実践基準の集大成と見なすことができ、経営幹部、ビジネス管理部門、IT 管理部門、ガバナンス・保証・セキュリティの専門家、および IT 監査と IT コントロールの専門家にとって有用である。COBIT は、他の標準やベストプラクティスを補足し、これらと併用できるように設計されている。

ベストプラクティスを導入する際は、企業のガバナンスおよびコントロールフレームワークと整合させる必要がある。さらに、組織にとって適切であることを確認し、現在使用している他の手法や実践基準と統合させる必要がある。標準やベストプラクティスは万能薬ではなく、その有効性は、実際の導入方法や最新の状態に保たれているかどうかに依存する。標準やベストプラクティスは、一連の方針として適用した場合、および具体的な手続を作成する土台として適用した場合が最も効果的である。ベストプラクティスを単に導入するだけでなく実用化するには、何を、どのように実行するのか、そしてそれがなぜ重要であるのかをマネジメント層およびスタッフが理解しなければならない。

ベストプラクティスをビジネス要件と整合させるには、COBIT を最上位のガイドラインとして導入することが推奨される。COBIT の導入により、基本的にどのような企業にも適用可能な、IT プロセスモデルに基づく総体的なコントロールフレームワークが確立できる。個別の領域を対象とした具体的な実践基準や標準を COBIT フレームワークに取り込むことで、これらの文書を階層的に整理できる。COBIT はさまざまなユーザにとって有用である。

- 経営幹部－しばしば予測が困難な IT 環境の中で、IT 投資による利益の獲得を図り、リスクとコントロールに対する投資のバランスを図る上で活用できる
- ビジネス管理部門－内部やサードパーティから提供された IT サービスを確実に管理およびコントロールする上で活用できる
- IT 管理部門－ビジネス戦略をサポートするためにビジネス部門が必要とする IT サービスを、コントロールおよび管理された方法で提供する上で活用できる
- 監査人－意見を実証し、また内部統制に関してマネジメント層に助言する上で活用できる

COBIT は、独立した非営利の研究機関により作成および保守されており、提携団体のメンバー、業界の専門家、およびコントロールとセキュリティの専門家の知識が取り込まれている。COBIT の内容は、IT のベストプラクティスを継続的に研究することで継続的に改訂されており、すべてのタイプのユーザにとって客観的で実用的な資料となっている。

COBIT は IT ガバナンスの目標と領域に焦点を当てており、COBIT のコントロールフレームワークを包括的に機能させ、企業のガバナンス方針と整合できるように設計されている。したがって、取締役会、経営幹部、監査人、および監督機関は COBIT を受け入れることができる。付録Ⅱでは、COBIT の詳細なコントロール目標を、IT ガバナンスの 5 つの関連領域および COSO のコントロール活動に対応付ける方法を示す。

図 17 は、COBIT フレームワークのさまざまな要素と IT ガバナンスの関連領域との関係を、要約して示したものである。

図 17 COBIT フレームワークおよび IT ガバナンスの関連領域

	達成目標	測定指標	実践基準	成熟度モデル
戦略との整合	P	P		
価値の提供		P	S	P
リスクの管理		S	P	S
資源管理		S	P	P
成果の測定	P	P		S

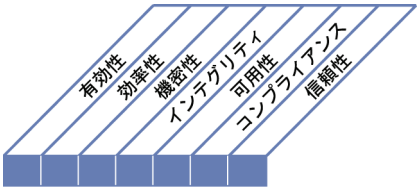
P=主要関連領域　S=副次的関連領域

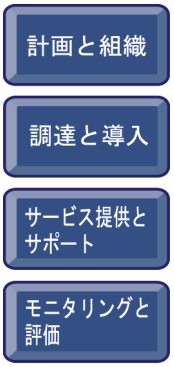
本書の使用方法

COBIT フレームワークの道案内

COBIT では、各 IT プロセスに対してコントロール目標の概要的な説明が記載されており、主要な目標と測定指標がウォーターフォール状に示されている(**図 18**)。

図 18 COBIT ナビゲーション





IT プロセス: <プロセス名>のコントロール目標は

<最も重要なビジネス達成目標の概要>を、**ビジネス要件**とし、

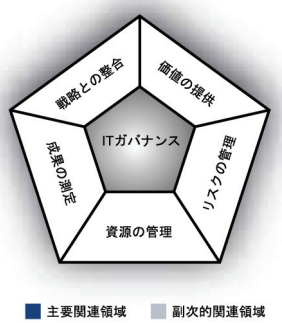
重点をおくべきコントロールは、<最も重要な IT の達成目標の概要>することである。

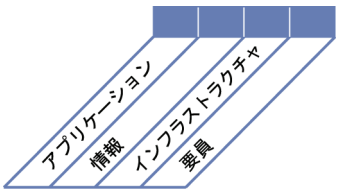
実現するための手段は、次の 3 項目である。

<主要なコントロール>

その成果の測定指標は、次の 3 項目である。

<主要な測定指標>





各 IT プロセスには、プロセスを確実にコントロールするために最低限必要な管理上のベストプラクティスとして、一般的な対応を記述した詳細なコントロール目標が示されている。

COBIT コアコンポーネントの概観

COBIT フレームワークには以下に示すコアコンポーネントがあり、本書の以降の章で示す 34 の IT プロセスごとに編成されている。これらのコンポーネントにより、各プロセスをコントロール、管理、および測定する方法の全体像を把握できる。各プロセスの説明は、以下の 4 つのセクションに分かれている。各セクションはほぼ 1 ページで記載されている。

- セクション 1 では、プロセスの目標を要約したプロセスの説明を示すとともに、概要レベルのコントロール目標をウォーターフォール状に示す。このページでは、このプロセスと情報要請規準である IT 資源および IT ガバナンスの関連領域との関連性も示されている。IT ガバナンスの関連領域については、主要な関連領域を P、副次的な関連領域を S で示してある。
- セクション 2 では、当該プロセスに関する詳細なコントロール目標を示す。
- セクション 3 では、プロセスのインプットとアウトプット、RACI チャート、目標、および測定指標を示す。
- セクション 4 では、プロセスの成熟度モデルを示す。

プロセスの成果内容は、以下のように捉えることもできる。

- プロセスのインプットは、プロセスオーナが他のプロセスから取得すべきものを示す。
- プロセス説明のコントロール目標は、プロセスオーナが実行すべき事項を示す。
- プロセスのアウトプットは、プロセスオーナが提供すべきものを示す。
- 目標と測定指標は、プロセスの測定方法を示す。
- RACI チャートは、どの権限を誰に委任すべきか定義する。
- 成熟度モデルは、改善に必要な対処を示す。

RACI チャートに示す役割は、すべてのプロセスについて、以下のように分類される。

- 最高経営責任者(CEO)
- 最高財務責任者(CFO)
- 企業幹部
- 最高情報責任者(CIO)
- ビジネスプロセスオーナ
- オペレーション責任者
- 設計責任者
- 開発責任者
- IT 管理責任者(大企業において、人材、予算、内部統制などを担当する部門の責任者)
- プロジェクトマネジメントオフィス(PMO)
- コンプライアンス、監査、リスク、およびセキュリティ(IT の運用責任ではなくコントロール責任を負うグループ)

一部のプロセスでは、このほかにプロセス固有の専門的な役割が存在する(DS8 のサービスデスク/インシデント管理担当者など)。

本書の構成要素は、数百名の専門家から収集され、厳密な調査とレビューを経たものではあるが、インプット、アウトプット、責任、測定指標、および目標は、実例的なものであり、規範的または包括的なものではないことに注意する必要がある。COBIT は専門知識を集約した原則を提供するものであり、各企業は、自社の戦略、達成目標、およびポリシーに基づいて、自社に効率的および効果的に適用可能な内容を選択する必要がある。

付録

本書の末尾には参考用に以下のセクションが収録されている。

Ⅰ. ビジネス達成目標と IT の達成目標の関連付け(3 つの表)
Ⅱ. IT プロセスと、IT ガバナンス関連領域、COSO、COBIT IT 資源、および COBIT 情報要請規準との対応関係
Ⅲ. 内部統制の成熟度モデル
Ⅳ. COBIT 4.0 の主要参考資料
Ⅴ. COBIT 第 3 版と COBIT 4.0 間の相互参照情報
Ⅵ. 研究開発へのアプローチ
Ⅶ. 用語集

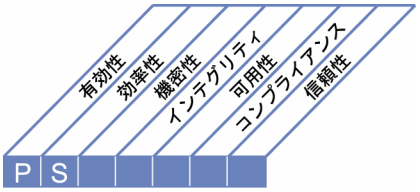
計画と組織

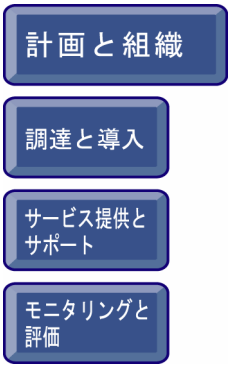
PO1 IT 戦略計画の策定
PO2 情報アーキテクチャの定義
PO3 技術指針の決定
PO4 IT プロセスと組織及びそのかかわりの定義
PO5 IT 投資の管理
PO6 マネジメントの意図と指針の周知
PO7 IT 人材の管理
PO8 品質管理
PO9 IT リスクの評価と管理
PO10 プロジェクト管理

コントロール目標 －概要－

PO1 IT 戦略計画の策定

ビジネス戦略およびビジネス上の優先順位に従って IT 資源の管理および割り当てを行うには、IT 戦略計画の策定が必要である。IT 部門およびビジネス部門の利害関係者は、プロジェクトおよびサービスのポートフォリオ(全体構成)から生み出される価値の最適化を実現する責任を有する。戦略計画を策定することにより、IT の利用機会および限界に対する主要な利害関係者の理解が深まり、現在の成果が評価され、必要な投資レベルが明確となる。ビジネス戦略やビジネス上の優先順位は IT 戦略計画のポートフォリオに反映され、IT 実行計画を通じて具現化されることになる。IT 実行計画は、ビジネス部門と IT 部門の双方から理解が得られ、承認を受けた簡潔な目標、計画、作業を定めたものである。





IT プロセス: IT 戦略計画の策定のコントロール目標は、

便益、費用、リスクに関わる**透明性を高める**とともに、ビジネス戦略やガバナンス上の要件を不断に維持し、もしくは発展させることを、**ビジネス要件**とし、

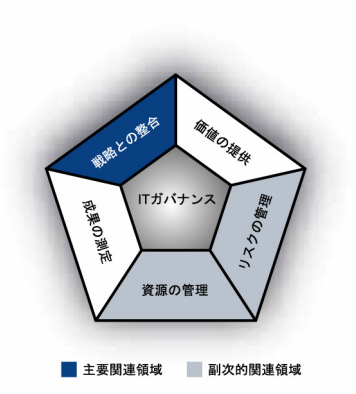
重点をおくべきコントロールは、ビジネス要件を満たすために、どのようなサービスを提供するかという検討に際して、IT とビジネスのマネジメント層が連携すると同時に、サービスを実現するために、透明性が高く、効果的な方法により戦略を策定することである。

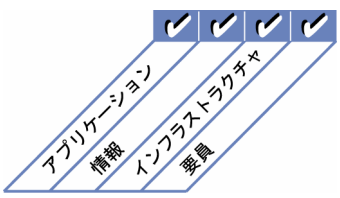
実現するための手段は、次の 3 項目である。

- ビジネス部門管理者およびマネジメント層と協議し、IT 戦略計画と、現在および将来のビジネス上の必要性との整合を確保
- 現在の IT に関する能力の把握
- ビジネス要件を定量化するためのビジネス目標の優先順位を決定するスキームの規定

その成果の測定指標は、次の 3 項目である。

- IT 戦略計画のうち、ビジネス戦略計画の達成を支援する IT 目標の割合
- IT プロジェクトのポートフォリオに挙げられたプロジェクトのうち、IT 戦術計画を直接の拠り所とするものの割合
- IT 戦略計画の更新が IT 実行計画に反映されるまでのタイムラグ





コントロール目標 －詳細－

PO1 IT 戦略計画の策定

PO1.1 IT 価値の管理
ビジネス部門と連携することで、企業全体の IT 関連投資のポートフォリオ(全体構成)に、ビジネス上の裏付けが確かな案件(プログラム)を確実に盛り込む。IT 投資には、必須な投資、継続的に必要な投資、および選択可能な投資があり、それぞれ資金配分の多様性および自由度に違いがあることを認識する。IT プロセスでは、プログラムの推進のために必要とされる IT 要素を効果的かつ効率的に提供する。また、プログラムの進行にあたって、費用、日程、機能などの逸脱が認められ、かつ、プログラムに期待される結果に影響を与えるかもしれない場合は、これを早期に警告する必要がある。IT サービスは、公平かつ法的強制力のあるサービス・レベル・アグリーメント(SLA)に基づき実行されなければならない。便益の達成および費用の管理に関する責任の所在を明確にし、モニタリングする。公正で透明性が高く、再現可能かつ比較可能な評価方法を確立し、財務的な価値を含めたビジネス上の価値や計画を遂行できない場合のリスク、期待された便益が得られないリスクなどを評価する。

PO1.2 ビジネスと IT の整合
現在の技術力と今後の方向性、IT がもたらすビジネス機会、それらの機会を逃さないためにビジネス部門が成すべきことについてマネジメント層を教育する。IT が整合性を保つためにビジネスの方向性を確実に理解させる。企業目標と IT の達成目標を明確に関連付け、ビジネス戦略と IT 戦略を統合し、ビジネス機会のみならず、現在の技術力の限界を認識し、幅広く周知徹底する。ビジネス(戦略)において、どの部分が IT に対する依存度が極めて高いのかを特定し、ビジネス部門と技術部門におけるそれぞれの責務の違いを調整し、双方の合意を得た適切な優先順位を設定する。

PO1.3 現在の成果の評価
既存計画および情報システムの成果を、ビジネス目標への貢献度、機能面、安定性、複雑性、費用、長所、および短所の観点から評価する。

PO1.4 IT 戦略計画
利害関係者との協力のもと、IT がどのように企業の戦略目的(目標)の達成に貢献できるのか、そして関連費用およびリスクにはどのようなものが考えられるのかを明確にした戦略計画を策定する。この計画では、IT が、IT 関連投資のプログラムや、IT の運用サービスの提供をどのように支援するのかを定める。また、計画の中で目標がどのように達成および測定されるのかを定義し、利害関係者からその目標について正式な承認を得る。IT 戦略計画は、投資および実行予算、資金源、調達戦略、取得戦略、および法律上・規制上の要件を網羅し、IT 実行計画を策定する上で活用できるよう十分に詳細である必要がある。

PO1.5 IT 実行計画
IT 戦略計画に基づき、IT 関連投資のポートフォリオの一部である IT 実行計画を作成する。戦術計画では、必要とされる IT イニシアチブ、資源上の要件、および資源の利用状況と便益達成のモニタリング方法と管理方法を記載する。戦術計画は、プロジェクト計画を策定する際に活用できるよう十分に詳細である必要がある。プロジェクトおよびサービスポートフォリオ(プロジェクトの結果として提供するサービスの全体構成)の分析を通じて、策定された IT 実行計画と IT イニシアチブを積極的に管理する。この管理では、定期的に要件と資源との間のバランスをとると同時に、戦略的および戦術的目標と期待される便益の達成度と比較し、計画からの逸脱が見られる場合は適切な対応措置を行う。

PO1.6 IT ポートフォリオの管理
プログラムの検討、策定、評価、優先順位付け、選定、開始、管理、およびコントロールを通じて、戦略的ビジネス目標を達成する。そのために、IT 関連投資のプログラム、すなわち、IT 関連投資プロジェクトのポートフォリオを、ビジネス部門とともに積極的に管理する。ポートフォリオの管理では、期待するビジネス成果を明確化し、その成果の達成に対して、プログラム目標の達成が貢献することを保証する。また、成果の達成に必要となる取組みの全容を理解した上で、指標を用いて責任範囲を明確化し、プログラム実施のためのプロジェクトを企画するとともに、資源および資金を割り当て、該当部署への権限委譲、プログラム開始時において必要なプロジェクトの実行指示を行う

マネジメントガイドライン

PO1 IT 戦略計画の策定

From	インプット
PO5	費用/便益報告書
PO9	リスク評価
PO10	最新のプロジェクトポートフォリオ
DS1	新規/更新されたサービス要件、最新のサービスポートフォリオ
*	ビジネス戦略およびビジネス上の優先順位
*	プログラムポートフォリオ
ME1	IT 計画にインプットされる成果
ME4	IT ガバナンスの状況報告書、IT に関する企業の戦略的方向性

* COBIT 外からのインプット

アウトプット	To						
IT 戦略計画	PO2…PO6		PO8	PO9	AI1	DS1	
IT 実行計画	PO2…PO6		PO9	AI1	DS1		
IT プロジェクトのポートフォリオ	PO5	PO6	PO10	AI6			
IT サービスポートフォリオ	PO5	PO6	PO9	DS1			
IT 調達戦略	DS2						
IT 取得戦略	AI5						

RACI チャート

役割

アクティビティ	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
ビジネス達成目標と IT の達成目標の関連付け	C	I	A/R	R	C						
重要な依存関係および最近の成果の特定	C	C	R	A/R	C	C	C	C	C		C
IT 戦略計画の策定	A	C	C	R	I	C	C	C	C	I	C
IT 実行計画の策定	C	I		A	C	C	C	C	C	R	I
プログラムポートフォリオの分析と、プロジェクトおよびサービスポートフォリオの管理	C	I	I	A	R	R	C	R	C	C	I

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- ビジネス部門管理者およびマネジメント層と協議し、IT 戦略計画を、現在および将来のビジネスニーズと整合を保ったものにすること
- 現在の IT 能力の把握
- IT 戦略計画の IT 実行計画への変換
- ビジネス要件を定量化するビジネス目標の優先順位を決定するスキームの規定

促進

プロセスの達成目標
- ビジネス要件を提供サービスに変換する方法の定義
- サービスの提供戦略の定義
- IT 関連のビジネス投資ポートフォリオの管理への管理支援
- リスクが IT 目標および資源に与える、ビジネス上の影響の明確化
- IT の費用、便益、戦略、ポリシー、およびサービスレベルに関する透明性とその理解の確保

促進

IT の達成目標
- ビジネス戦略と合致するビジネス要件への対応
- 取締役会の指示に従ったガバナンス要件への対応

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- ビジネス戦略/実行計画の更新が IT 戦略/実行計画に反映されるまでのタイムラグ
- ビジネス部門の代表者が積極的に参加した IT 戦略/実行計画会議の割合
- IT 戦略計画の更新が IT 実行計画に反映されるまでのタイムラグ
- 予め定められた計画の構成/内容に準拠して立案された IT 実行計画の割合
- ビジネスオーナが支持する IT イニシアチブ/プロジェクトの割合

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- IT 戦略計画のうち、ビジネス戦略計画の達成を支援する IT 目標の割合
- IT 実行計画のうち、ビジネス戦術計画の達成を支援する IT イニシアチブの割合
- IT プロジェクトのポートフォリオのうち、IT 実行計画から直接派生している IT プロジェクトの割合

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- IT 戦略/戦術計画に対するビジネスオーナの支持度
- ビジネス要件およびガバナンス要件に対するコンプライアンス
- プロジェクトおよびアプリケーションポートフォリオの現状(数量、範囲など)に対するビジネス部門の満足度

成熟度モデル

PO1 IT 戦略計画の策定

「どのような便益、費用、およびリスクがあるのかを誰にでも分かりやすく・見えるようにすると同時に、ビジネス戦略およびガバナンス上の要件を満たす、もしくはその発展を手助けする」という IT に対するビジネス要件を満たす上で、「IT 戦略計画の策定」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
IT 戦略計画の策定が行われていない。マネジメント層に、ビジネス目標の達成を支援するために IT 戦略計画の策定が必要であるという認識がない。

1 初期/その場対応
IT マネジメント層では、IT 戦略計画の必要性を認識している。IT 計画の策定は、特定のビジネス要件への対応として、必要に応じて行われている。IT 戦略計画の策定については、IT マネジメント層の会議で時折協議される。ビジネス要件、アプリケーション、および技術間の調整は、組織全体の戦略に基づく形ではなく、何らかの問題に対応する形で実施される。どのようなリスクをとらえ、どう対処するかというリスクへの戦略的な対応は、プロジェクトごとに非公式に行われる。

2 再現性はあるが直感的
IT 戦略計画は、必要に応じてビジネス管理部門と共有されている。IT 計画の更新は、マネジメント層の要請に応じて行われる。戦略的意思決定はプロジェクトごとに行われ、組織全体の戦略との整合はとれていない。主な戦略的意思決定におけるリスクおよびユーザの便益は、直感的に認識されている。

3 定められたプロセスがある
IT 戦略計画の策定時期および方法について定められたポリシーがある。IT 戦略計画は、体系的アプローチに従って策定される。このアプローチは、文書化され、全社員に周知されている。IT 計画の策定プロセスがある程度確立されており、そのプロセスに沿うことで適切な計画の策定が確保されている。しかし、当該プロセスの導入については個々の管理者に一任されており、このプロセスの検証手続も確立されていない。全社的な IT 戦略においては、先駆的であれ、追随的立場であれ、組織として進んでとるべきリスクが、戦略の実現と矛盾のないように定義されている。新しい製品および技術の調達に対しては、IT における財務、技術、および人材戦略が、徐々に考慮されるようになっている。IT 戦略計画の策定内容については、ビジネス管理部門の会議においても協議されている。

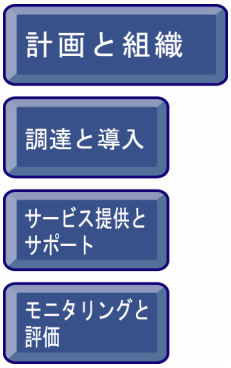
4 管理され、測定可能である
IT 戦略計画の策定は標準化された手続であり、その手続から逸脱するような事態が生じた場合はマネジメント層が発見できるようになっている。IT 戦略計画の策定は、マネジメント層レベルが、その責務を担う管理機能として定義されている。マネジメント層は、IT 戦略計画の策定プロセスをモニタリングし、それに基づき十分な情報を踏まえた上で意思決定を行い、その有効性を測定できる。短期的および長期的な IT 計画が策定され、必要に応じて更新され、その内容は組織のマネジメント層から末端まで浸透されている。IT 戦略と、組織全体の戦略は、徐々に、相互連携を強めている。その連携強化は、ビジネスプロセスおよび付加価値能力に焦点を当てると同時に、ビジネスプロセスのリエンジニアリング(再構築)を通じてアプリケーションおよび技術をより有効に活用することによってなされている。システム開発および運用に必要な社内外の人的資源活用に関する決定プロセスが、明確に定義されている。

5 最適化
IT 戦略計画の策定は、文書化され、日常的に運用されているプロセスであるだけでなく、ビジネス目標を設定する際に常に考慮されることで、IT への投資が明確なビジネス上の価値をもたらしている。IT 戦略計画の策定プロセスにおいては、リスクおよび付加価値に対する見方や、考え方が、常に見直されている。長期的であると同時に現実性のある IT 計画が策定され、技術面およびビジネス面における動向を反映するよう継続的に更新されている。認知度、信頼性をともに満足する業界基準に基づくベンチマーク評価が行われ、その評価プロセスは、戦略の策定プロセスに組み込まれている。IT 戦略計画では、新しい技術発展を通じて、いかに新たなビジネス能力を創出し、組織の競争優位性の向上を図るのかについても、明記している。

コントロール目標 －概要－

PO2 情報アーキテクチャの定義

情報システム部門は、ビジネス情報モデルを構築するのみならず、これを定期的に更新し、ビジネス情報を最大限に利用できるシステムを定義する必要がある。このビジネス情報モデルには、組織のデータ構文規則に従った企業データディクショナリ、データ分類体系、およびセキュリティレベルが含まれる。このプロセスは、安全で信頼性の高い情報を提供することを確実にすることにより、マネジメント層の意思決定の質を高める。また、情報システム資源をビジネス戦略に適切に合わせた合理的なものとする。この IT プロセスにおいては、データのインテグリティおよびセキュリティに関する説明責任能力の強化のほか、アプリケーションおよび組織全体にわたる情報共有の有効性とコントロールの強化が必要である。



IT プロセス: 情報アーキテクチャの定義のコントロール目標は、

要件に迅速に対応し、信頼性の高い一貫した情報を提供し、アプリケーションをビジネスプロセスにシームレスに統合することを、**ビジネス要件**とし、

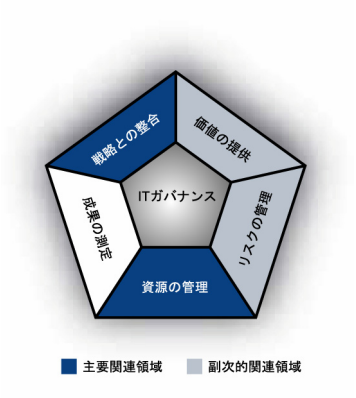
重点をおくべきコントロールは、データ分類体系を組み込んだ企業データモデルを構築し、すべてのデータのインテグリティおよび一貫性を確保することである。

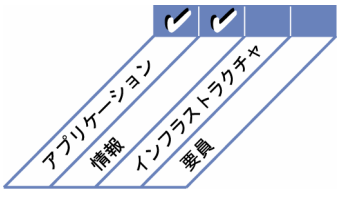
実現するための手段は、次の 3 項目である。

- 情報アーキテクチャおよびデータモデルの正確性の保証
- データのオーナシップの割り当て
- 合意された分類スキームを用いて情報を分類すること

その成果の測定指標は、次の 3 項目である。

- 冗長/重複データ要素の割合
- 情報アーキテクチャと合致しないアプリケーションの割合
- データ検証活動の頻度





コントロール目標 －詳細－

PO2 情報アーキテクチャの定義

PO2.1 企業の情報アーキテクチャモデル
企業情報モデルを構築し維持することにより、PO1 で述べた IT 計画に合致した、アプリケーションの開発や意思決定支援活動を可能とする。このモデルは、ビジネス部門による情報の作成、利用、共有の最適化を促進するとともに、情報のインテグリティの維持はもちろん、柔軟性、機能性、費用効率性、タイムリー性、安全性、障害回復性といった面でも有効に機能する。

PO2.2 企業データディクショナリおよびデータ構文規則
組織のデータ構文規則を組み込んだ企業データディクショナリを維持管理する。このディクショナリは、アプリケーションやシステムとの間でのデータ要素の共有を可能にする。また、IT 部門とビジネス部門との間で、データに関する共通認識を促進し、互換性のないデータ要素の作成を防止する。

PO2.3 データ分類体系
企業データの重要性および機密性(公開可能、機密、極秘など)に基づき、企業全体で適用可能な分類スキームを確立する。分類スキームでは、データのオーナシップの詳細な内容と、適切なセキュリティレベル、および保護コントロールを定義する。また、データの保持および破棄にかかわる必要事項のほか、データの重要性と機密性に関する概要を盛り込む。この分類スキームは、アクセスコントロール、アーカイブ、暗号化などのコントロールを適用する上で使用すべき基準とする。

PO2.4 インテグリティの管理
データベース、データウェアハウス、データアーカイブなど、電子的に保存されたすべてのデータのインテグリティと一貫性を確保する手続を策定し、導入する。

マネジメントガイドライン

PO2 情報アーキテクチャの定義

From	インプット
PO1	IT 戦略/実行計画
AI1	ビジネス要件の実現可能性調査
AI7	導入後レビュー
DS3	性能とキャパシティに関する情報
ME1	IT 計画にインプットされる成果

アウトプット	To						
データ分類体系	AI2						
最適化されたビジネスシステム計画	PO3	AI2					
データディクショナリ	AI2	DS11					
情報アーキテクチャ	PO3	DS5					
採用したデータの分類方法	DS1	DS4	DS5	DS11	DS12		
分類手続とツール	*						

* COBIT 外部へのアウトプット

RACI チャート

アクティビティ	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
企業情報モデルの構築と保守		C	I	A	C		R	C	C		C
企業データディクショナリの構築と保守				I	C		A/R	R			C
データ分類体系の確立と保守	I	C	A	C	C	I	C	C			R
データオーナに対する情報システム分類手続とツールの提供	I	C	A	C	C	I	C	C			R
情報モデル、データディクショナリ、および分類スキームを活用した、最適化されたビジネスシステムの計画策定	C	C	I	A	C		R	C			I

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- 情報アーキテクチャおよびデータモデルの正確性の保証
- データのオーナシップの割り当て
- 合意済みの分類スキームを用いた情報分類
- IT インフラストラクチャの構成要素間における一貫性の確保(情報アーキテクチャ、データディクショナリ、アプリケーション、データ構文、分類スキーム、およびセキュリティレベル)
- データのインテグリティの維持

促進

プロセスの達成目標
- 企業データモデルの構築
- データの冗長度の削減
- 効果的な情報管理の支援

促進

IT の達成目標
- 情報利用の最適化
- アプリケーションのビジネスプロセスへのシームレスな統合の実現
- ビジネス戦略と合致するビジネス要件への対応
- 機敏な IT 能力の創出

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 企業データモデルの更新頻度
- オーナが割り当てられていないデータ要素の割合
- データ検証活動の頻度
- ユーザコミュニティの関与度

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 企業データモデルに含まれないデータ要素の割合
- データ分類体系からの逸脱の割合
- 情報アーキテクチャに合致しないアプリケーションの割合

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 情報モデルに満足しているユーザの割合(データディクショナリはユーザフレンドリーか、など)
- 冗長/重複データ要素の割合

成熟度モデル

PO2 情報アーキテクチャの定義

「要件に迅速に対応し、信頼性の高い一貫した情報を提供し、アプリケーションをビジネスプロセスにシームレスに統合する。」という IT に対するビジネス要件を満たす上で、「情報アーキテクチャの定義」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
組織における情報アーキテクチャの重要性が認識されていない。組織内に、情報アーキテクチャの開発に必要な知識、ノウハウ、および実行責任の割り当てが存在しない。

1 初期/その場対応
マネジメント層は、情報アーキテクチャの必要性を認識している。情報アーキテクチャの一部のコンポーネントが、場当たり的に開発されている。定義は、情報ではなくデータに焦点を当てており、アプリケーションソフトウェアベンダーの提案に左右される。情報アーキテクチャの必要性を周知させる試みは散発的で、一貫性がない。

2 再現性はあるが直感的
情報アーキテクチャプロセスが構築されつつあり、組織内の複数の要員が、非公式かつ直感的ではあるが類似した手続に従っている。要員は、実務経験および各種技法の反復利用により、情報アーキテクチャの構築に必要なスキルを習得している。戦術的な必要に迫られ、情報アーキテクチャコンポーネントを個人レベルで開発している。

3 定められたプロセスがある
情報アーキテクチャの重要性が理解および認知されており、その構築と提供の実行責任が割り当てられ、明確に周知されている。関連手続、ツール、および技法は、十分に考え抜かれた高い精度を持つには至っていないものの標準化、文書化されており、非公式な研修活動の一環として活用されている。戦略的な要件を部分的に取り入れた情報アーキテクチャの基本ポリシーが作成されているが、ポリシー、標準、およびツールへのコンプライアンスは一貫して適用されていない。正式に定められたデータ管理組織が確立され、組織全体の標準を設定している。また、情報アーキテクチャの提供と使用に関する報告の実施に着手している。自動化ツールが採用され始めているが、使用されるプロセスや規則はデータベースソフトウェアベンダーの提案に基づいて定義されている。正式な研修活動が定義、文書化され、一貫して適用されている。

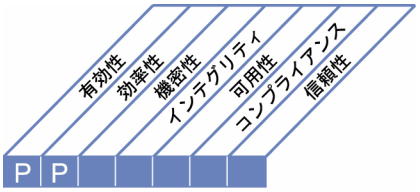
4 管理され、測定可能である
情報アーキテクチャの開発と運用はすべて、正式に定められた方法と技法に基づいている。アーキテクチャ開発プロセスの成果に関する説明責任が規定され、情報アーキテクチャの成果が測定されている。情報アーキテクチャの開発と運用においては、自動化された支援ツールが、広く導入されているが、統合はされていない。基本的な測定指標が明確にされ、測定システムが整備、または、実施されている。情報アーキテクチャの定義を行うプロセスでは、積極的に、将来のビジネスニーズに対処することに重点をおいている。データ管理組織は、すべてのアプリケーション開発作業に積極的に参加し、データの一貫性を確保している。自動化リポジトリ(訳注:データの意味などを一元管理するためのデータベースで、「メタデータリポジトリ」とも呼ばれる。)が全面的に導入されている。データベースに存在する情報コンテンツの最適な活用に向け、より複雑なデータモデルが導入されつつある。マネジメント層の情報システムおよび意思決定支援システムにおいて、利用可能な情報が活用されている。

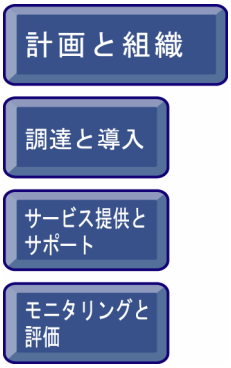
5 最適化
情報アーキテクチャは、あらゆるレベルで一貫して適用されている。ビジネスに対する情報アーキテクチャの価値が継続的に強調されている。IT 担当者は、すべてのビジネス要件を反映した堅固かつ即応性の高い情報アーキテクチャの開発と維持に必要な、専門知識とスキルを有している。情報アーキテクチャにより提供される情報は、一貫して幅広く利用されている。業界のベストプラクティスが、情報アーキテクチャの開発と維持、およびその継続的な改善プロセスに幅広く取り入れられている。データウェアハウス技術およびデータマイニング技術による情報活用戦略が策定されている。情報アーキテクチャは継続的に改善され、プロセス、組織、およびシステムに関する、従来の枠に収まらない情報についても検討されている。

コントロール目標 －概要－

PO3 技術指針の決定

情報サービス部門は、ビジネス部門を支援するために技術指針を定める必要がある。そのためには、技術インフラストラクチャ計画を策定する必要がある。また、製品、サービス、および提供手段に関して、技術が、どのような貢献ができるかについて、明確かつ現実的な見込みを立て、これを管理するアーキテクチャ委員会を設置しなければならない。技術インフラストラクチャ計画は定期的に更新されなければならず、システムアーキテクチャ、技術指針、調達計画、標準、移行戦略、および緊急時対応などの観点を含むことが必要である。これにより、プラットフォームとアプリケーションとの間の相互運用性の改善、競争的な環境における変化へのタイムリーな対応、および情報システム要員の確保と投資におけるスケールメリットを実現できる。





IT プロセス: 技術指針の決定のコントロール目標は、

現在および将来のビジネス要件を満たすために、安定性と費用効率に優れ、統合および標準化されたアプリケーションシステム、資源、および能力を保持することを、**ビジネス要件**とし、

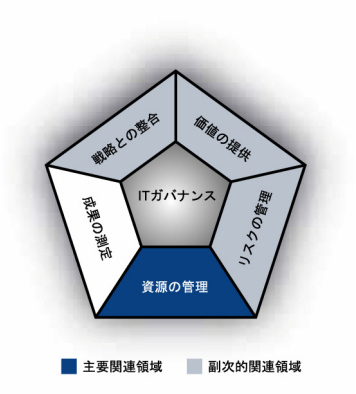
重点をおくべきコントロールは、技術進歩がもたらす事業機会を発見して活用するために、技術インフラストラクチヤ計画、アーキテクチャ、標準を定義し、導入することである。

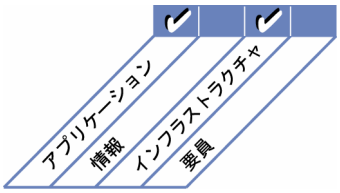
実現するための手段は、次の 3 項目である。

- アーキテクチャに関する指針を策定し、指針の遵守を確認するフォーラムの設置
- 費用、リスク、および要件との調整を図った技術インフラストラクチャ計画の作成
- 情報アーキテクチャ要件に基づく技術インフラストラクチャ標準の定義

その成果の測定指標は、次の 3 項目である。

- 技術インフラストラクチャ計画からの逸脱件数と内容
- 技術インフラストラクチャ計画の見直し/更新頻度
- 企業全体における部門ごとの技術プラットフォーム数





コントロール目標 －詳細－

PO3 技術指針の決定

PO3.1 技術指針計画の策定
既存技術および将来性のある新技術を分析し、IT 戦略とビジネスシステムアーキテクチャの実現に適した技術指針を計画する。また、ビジネスチャンスの創出が期待できる技術を、その計画の中で特定する。この計画では、インフラストラクチャの構成要素であるシステムアーキテクチャ、技術指針、移行戦略、および緊急時対応の側面を検討する必要がある。

PO3.2 技術インフラストラクチャ計画
IT 戦略/実行計画に沿った技術インフラストラクチャ計画を策定および維持する。この計画は技術指針に基づいて策定し、緊急時対応策および技術資源の調達に関する指針を含める。計画においては、競合環境の変化、情報システム要員の確保や投資におけるスケールメリットの実現、プラットフォームとアプリケーションとの間の相互運用性の改善を検討する。

PO3.3 将来の動向および規制のモニタリング
ビジネスの業種/業界動向、技術動向、インフラストラクチャの動向、および法規制関連の動向をモニタリングするプロセスを確立する。これらの動向の影響を考慮した IT 技術インフラストラクチャ計画を作成する。

PO3.4 技術標準
一貫性があり、効果的かつ安全な技術的対応策を企業全体に適用するため、技術フォーラムを設置して技術的なガイドライン、インフラストラクチャ関連製品に関する助言、および技術選択の指針を提示する。また、これらの標準やガイドライン等の文書にどの程度、準拠しているかどうかを測定する。このフォーラムでは、ビジネスとの関連性、リスク、および外部要件へのコンプライアンスを鑑みて、技術標準および実践基準についての指示を行う。

PO3.5 IT アーキテクチャ委員会
IT アーキテクチャ委員会を設置し、アーキテクチャに関するガイドラインとその適用に関する助言を提供するとともに、それらに対するコンプライアンスを確認する。ビジネス戦略の実現を可能にし、法規制の遵守と継続性の要件が考慮されたITアーキテクチャの設計を、委員会が指揮する。IT アーキテクチャは、情報アーキテクチャに関連付けられる。

マネジメントガイドライン

PO3 技術指針の決定

From	インプット
PO1	IT 戦略/戦術計画
PO2	最適化されたたビジネスシステム計画、情報アーキテクチャ
AI3	技術標準の更新
DS3	性能やキャパシティに関する情報

アウトプット	To						
技術機会	AI3						
技術標準	AI1	AI3	AI7	DS5			
「技術の状態」の定期的な更新	AI1	AI2	AI3				
技術インフラストラクチャ計画	AI3						
インフラストラクチャ要件	PO5						

RACI チャート

役割

アクティビティ

	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス、監査、リスク、セキュリティ
技術インフラストラクチャ計画の策定と維持		I	I	A		C	R	C	C		C
技術標準の策定と維持				A		C	R	C	I	I	I
技術標準の公開		I	I	A		I	R	I	I	I	I
技術進歩に関するモニタリング		I	I	A		C	R	C		C	C
新しい技術の(将来的)(戦略的)使用の定義		C	C	A		C	R	C		C	C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- 情報アーキテクチャ要件に基づく技術インフラストラクチャ標準の定義
- 費用、リスク、および要件との調整を図った技術インフラストラクチャ計画の確立
- アーキテクチャに関する指針を策定し、指針の遵守を確認するフォーラムの設置

促進

プロセスの達成目標
- 技術機会の発見および活用
- 技術インフラストラクチャ計画の作成および導入
- IT インフラストラクチャのアーキテクチャおよび技術標準の定義

促進

IT の達成目標
- IT インフラストラクチャ、資源、および能力の最適化
- 統合および/標準化されたアプリケーションシステムの調達と保守

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 技術フォーラムにより開催された会議の頻度
- IT アーキテクチャ委員会により開催された会議の頻度
- 技術インフラストラクチャ計画の見直し/更新頻度

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 技術標準からの逸脱の割合
- 企業全体における部門ごとの技術プラットフォーム数

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 技術インフラストラクチャ計画からの逸脱件数と内容

成熟度モデル

PO3 技術指針の決定

「現在および将来のビジネス要件を満たし、安定性と費用効率に優れ、統合および標準化されたアプリケーションシステム、資源、および能力を整備する。」という IT に対するビジネス要件を満たす上で、「技術指針の決定」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
組織における技術インフラストラクチャ計画の重要性が認識されていない。技術インフラストラクチャ計画の作成に必要な知識やノウハウが存在しない。技術的な変更の計画が資源の効果的な割り振りに重要であることが理解されていない。

1 初期/その場対応
マネジメント層は、技術インフラストラクチャ計画の必要性を認識している。技術コンポーネントの開発および将来性のある新技術の導入は場当たり的かつ単発的に行われている。インフラストラクチャ計画は事後的に策定され、運用面に焦点を当てたアプローチが採用されている。技術指針は、ハードウェア、システムソフトウェア、アプリケーションソフトウェアのベンダーから提示される、矛盾することも多い製品の展開計画に引きずられている。技術的な変化が及ぼし得る潜在的な影響力について首尾一貫した伝達がなされていない。

2 再現性はあるが直感的
技術計画の必要性および重要性が周知されている。計画策定は戦術的に行われ、ビジネスニーズに対応するための技術の利用方法ではなく、技術上の問題に対する技術的対応策の策定に焦点が当てられている。技術的な変更の評価は個々人の裁量に委ねられており、直感的ではあるが類似したプロセスが用いられている。要員は、実務に基づく学習および技法の反復利用により、技術計画の策定に必要なスキルを習得している。インフラストラクチャコンポーネントの開発に対する共通の技法および標準が確立されつつある。

3 定められたプロセスがある
マネジメント層は、技術インフラストラクチャ計画の重要性を認識している。技術インフラストラクチャ計画の策定プロセスがある程度確立されており、IT 戦略計画と整合されている。技術インフラストラクチャ計画が定義および文書化され、十分に周知されているが、一貫して適用されているわけではない。技術インフラストラクチャ指針では、リスクや組織の戦略との整合性に基づき、技術の使用を促進すべき分野と抑制すべき分野について、組織の認識が示されている。主要なベンダーの選択は、技術、製品に関するベンダーの長期開発計画を検討し、組織の指針との整合性を考慮した上で行われる。正式な研修が実施されており、役割と実行責任について周知されている。

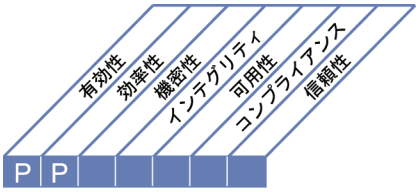
4 管理され、測定可能である
マネジメント層は、技術インフラストラクチャ計画の作成および維持を徹底させている。IT 担当スタッフは、技術インフラストラクチャ計画の策定に必要な専門知識とスキルを有している。技術の変動や将来性のある新技術による潜在的な影響が考慮されている。マネジメント層は、計画からの逸脱を発見し、問題の発生を予期できる。技術インフラストラクチャ計画の策定および維持に関する実行責任の所在が明確にされている。技術インフラストラクチャ計画の高度な策定プロセスが展開されており、変化に対する即応性がある。社内の優れた実践基準がプロセスに取り入れられている。IT 担当スタッフが技術の変動を確実に管理できるよう、人材戦略と技術指針との整合が図られている。新しい技術の導入のための移行計画が策定されている。必要な専門知識とスキルの獲得に向け、アウトソーシングの活用と他社との提携が図られている。マネジメント層は、新たなビジネス機会の開拓や運営効率の向上を進める上で、技術の利用を促進することと、抑制することのリスクを受容できるか否か分析している。

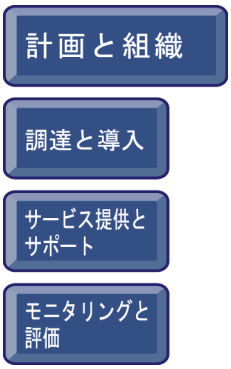
5 最適化
将来性のある新技術および発展を続ける技術を調査し、業界水準に照らして企業のベンチマーク評価を実施する調査研究部門がある。技術インフラストラクチャ計画の方向性は、技術ベンダーからの影響ではなく、業界および国際的な標準と発展状況を基に決定されている。技術的な変動によるビジネスへの潜在的な影響は、マネジメント層のレベルで検証されている。技術指針の新規作成および変更については、マネジメント層によって正式に承認されている。企業が有する堅固な技術インフラストラクチャ計画は、ビジネス要件が反映された即応性のあるもので、ビジネス環境の変化に合わせた修正が可能である。技術インフラストラクチャ計画の改善に向け、継続的かつ強制力のあるプロセスが整備されている。技術指針の決定においては、業界のベストプラクティスが広く取り入れられている。

コントロール目標 －概要－

PO4 IT プロセスと組織及びそのかかわりの定義

IT 組織の構築では、人材、スキル、機能、説明責任、権限、役割、実行責任、および監督に関する要件を考慮することが必要である。透明性とコントロールを確保し、マネジメント層とビジネス管理部門の関与を確実にするために、IT プロセスフレームワークに、IT 組織を組み込まなければならない。企業の戦略委員会は、取締役会を通して IT 部門の監督を徹底させなければならない。さらにビジネス部門と IT 部門が参加する 1 つ以上の運営委員会が、ビジネス上の必要性に応じて、IT 資源の優先順位を決定する必要がある。プロセス、管理ポリシー、および手続が、組織内のすべての機能のために、整備、運用される必要がある。その際には、コントロール、品質保証、リスク管理、情報セキュリティ、データとシステムのオーナシップ、および職務の分離に、特に留意することが必要である。ビジネス要件にタイムリーに対応するため、関連する意思決定プロセスには IT 部門も参加する。





IT プロセス: IT プロセスと組織およびそのリレーションシップの定義のコントロール目標は、

ガバナンス要件に準拠しつつビジネス戦略に迅速に対応すると同時に、明確かつ有能な連絡窓口を設けることを、**ビジネス要件**とし、

重点をおくべきコントロールは、

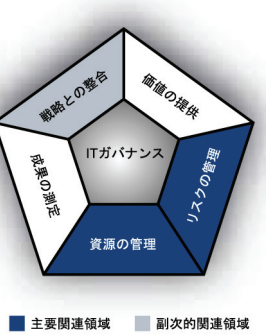
透明性、柔軟性、即応性を有する IT 組織構造を確立し、ビジネスプロセスと意思決定プロセスに統合されたオーナ、役割、および実行責任を含む IT プロセスを定義および導入することである。

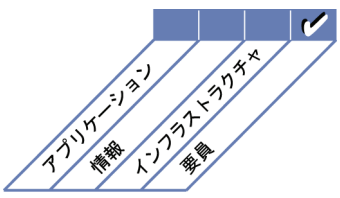
実現するための手段は、次の 3 項目である。

- IT プロセスフレームワークの定義
- 適切な組織および組織構造の確立
- 役割および実行責任の定義

その成果の測定指標は、次の 3 項目である。

- 職位および権限規定が文書化されている役割の割合
- ビジネス戦略上、IT 部門の支援を受けるべきでありながら受けていないビジネス部門/プロセスの数
- IT 部門外で行われ、承認されていない、または IT 部門の標準に従っていない主要な IT 活動の数





コントロール目標 －詳細－

PO4 IT プロセスと組織及びそのかかわりの定義

PO4.1 IT プロセスフレームワーク
IT 戦略計画を実行するための IT プロセスフレームワークを定義する。このフレームワークには、IT プロセスの構造と IT プロセス間のリレーションシップ(たとえば、プロセス間の差異や重複を管理する際に利用)、オーナシップ、成熟度、成果の測定、改善、コンプライアンス、品質目標、およびこれらの達成のための計画を含める。このフレームワークでは、IT 特有のプロセス、企業ポートフォリオの管理、ビジネスプロセスおよびビジネス変革プロセス、の各プロセスを統合する。IT プロセスフレームワークは、品質管理システムおよび内部統制のフレームワークに組み込む必要がある。

PO4.2 IT 戦略委員会
取締役会レベルで IT 戦略委員会を設置する。この委員会は、企業ガバナンスの一部として、IT ガバナンスへの対応を確実かつ適切に行い、取締役会の代理として戦略的方針に関する助言を行うほか、主要な投資のレビューを行う。

PO4.3 IT 運営委員会
マネジメント層、ビジネスおよび IT のマネジメント層で構成される、以下の役割を持つ IT 運営委員会(またはそれに準ずるもの)を設置する。
- 企業のビジネス戦略およびビジネス上の優先事項に沿った、IT 関連の投資プログラムの優先順位の決定
- プロジェクト状況の追跡と資源をめぐる悩みや争いの解決
- サービスレベルおよびサービスの改善のモニタリング

PO4.4 組織における IT 部門の配置
企業において IT が重要である場合は、ビジネスモデルに従って、全社的組織構造に IT 部門を組み込む。企業において IT が重要であるとは、特に、ビジネス戦略上、IT を重要視していること、現場の実務において IT への依存度が高いことである。CIO の報告先は、企業における IT の重要性によって決まる。

PO4.5 IT 組織の構造
ビジネス上の必要性を踏まえて、社内のみならず、社外も含めて適切な IT 組織構造を確立する。さらに、期待されるビジネス目標を達成し、かつ状況の変化に対応できるよう人員補充要件および調達戦略を調整するため、IT 組織構造の定期的な見直しのプロセスを整備する。

PO4.6 役割と責任
情報システムに関するすべての社員を対象として、役割と責任を定義、周知する。これにより、割り当てられた役割と責任を果たすのに十分な権限を組織のすべての要員に付与する。職務定義書を作成し、定期的に更新する。職務定義書には権限と責任の両方が明確に規定し、対応する職位に必要なスキルと経験の定義を盛り込み、成果の評価の際に活用できるようにする。職務定義書には、内部統制に関する責任を記載する必要がある。

PO4.7 IT の品質保証の責任
品質保証機能における成果達成の実行責任を割り当てる。同時に、適切な品質保証システム、コントロール、および周知に関わる専門家から構成される品質保証グループを編成する。品質保証部門の組織内での位置付けや、および責任と規模は、組織として求められる要件を満たしている。

PO4.8 リスク、セキュリティ、およびコンプライアンスに関する責任
ビジネスにおける IT 関連のリスクのオーナシップおよび実行責任を、適切なマネジメント層レベルに割り当てる。情報セキュリティ、物理的セキュリティ、およびコンプライアンスに関する具体的な責任を含め、IT リスクを管理する上で重要な役割を定義し、割り当てる。組織全体の課題に対応するため、全社レベルでのリスクおよびセキュリティ管理に関する責任を定める。システム固有のセキュリティ問題に対処するため、さらにシステム別のセキュリティ管理責任の割り当てが必要となる場合もある。マネジメント層から、IT のリスク傾向に関する指示、および未対応の IT リスクに関する承認を得る。

PO4.9 データおよびシステムのオーナシップ
ビジネス部門がデータおよび情報システムのオーナシップに関する責任を果たせるよう、手続およびツールを提供する。オーナは、情報およびシステムの分類について決定し、その分類に沿って当該情報およびシステムを保護する。

PO4.10 監督
適切な監督の実践基準を IT 部門に導入する。これにより、部門内における役割と責任が確実に果たされることを保証する。すべての要員がそれぞれの役割の実行と責任の行使に要する権限および資源を十分有しているかを見極める。また、KPI を全体的に見直す。

PO4.11 職務の分離
役割と責任の分離を行う。これにより、一個人に役割と責任が集中するがために、重要なプロセスが不適切に実施される可能性を減らす。また、マネジメント層は、要員が、割り当てられた職務および職位に関連して許可された業務のみを遂行していることを確認する。

PO4.12 IT スタッフの配置
IT スタッフの配置要件について、定期的に、またはビジネス環境、運用環境、もしくは IT 環境の大規模な変更に応じて評価する。これにより、IT 部門が有能な必要数のスタッフを確実に確保できるようにする。スタッフ配置では、ビジネス部門/IT 部門をまたぐスタッフ配置、部門間研修、業務のローテーションおよびアウトソーシングの可能性も検討する。

PO4.13 主要 IT 担当者
主要な IT 担当者を定義および特定し、当該要員に対する過度の依存を抑制する。緊急時における主要担当者との連絡方法を決めておく必要がある。

PO4.14 契約社員に関するポリシーおよび手続
IT 部門は、コンサルタントおよびその他の契約社員の活動をコントロールするポリシーと手続を策定し、実施する。組織の情報資産が確実に保護され、合意された契約事項が遵守されることが目的である。

PO4.15 リレーションシップ
IT 部門間、および、IT 部門内外のさまざまな関係者との間で最適な連携、情報共有、および協力体制を確立し、維持する。関係者とは、具体的には、取締役会、マネジメント層、ビジネス部門、個人ユーザ、サービスプロバイダ、セキュリティ担当者、リスク管理担当者、企業のコンプライアンス担当グループ、アウトソーシング発注者、および遠隔地管理担当者などである。

(空白ページ)

マネジメントガイドライン

PO4 IT プロセスと組織及びそのかかわりの定義

From	インプット
PO1	戦略/戦術計画
PO7	IT の人事ポリシーと手続、IT スキルマトリクス、職務記述書
PO8	品質改善策
PO9	IT にかかわるリスクの是正措置計画
ME1	是正措置計画
ME2	IT コントロールの有効性に関する報告書
ME3	IT サービスの提供に関する法令要件の一覧
ME4	プロセスフレームワークの改善

アウトプット	To						
IT プロセスフレームワーク	ME4						
文書化されたシステムオーナ	AI7	DS6					
IT 組織とそのリレーションシップ	PO7						
IT プロセスフレームワーク、文書化された役割および責任	ALL						
文書化された役割および責任	PO7						

RACI チャート

アクティビティ ＼ 役割	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス、監査、リスク、セキュリティ
委員会の設置、利害関係者およびベンダーとのリレーションシップの確立を含む、IT 組織構造の確立	C	C	C	A		C	C	C	R	C	I
IT プロセスフレームワークの策定	C	C	C	A		C	C	C	R	C	C
システムオーナの明確化		C	C	A	C	R	I	I	I	I	I
データオーナの明確化		I	A	C	C	I	R	I	I	I	C
監督業務および職務の分離を踏まえた、IT 担当者の役割および責任の確立と導入		I	I	A	I	C	C	C	R	C	C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- IT プロセスフレームワークの定義
- 適切な組織および組織構造の確立

促進

プロセスの達成目標
- 柔軟性および即応性を有する IT 組織構造とそのリレーションシップの確立
- すべての IT プロセスおよび利害関係者とのリレーションシップに関する、オーナ、役割、および責任の明確な定義

促進

IT の達成目標
- 取締役会の指示に従ったガバナンス要件への対応
- ビジネス戦略と合致するビジネス要件への対応
- 機敏な IT 能力の創出

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 職位規定および権限規定が文書化されている役割の割合
- ビジネス運用構造に関連付けられている IT 運用組織/プロセスの割合
- 戦略委員会および運営委員会による会議の頻度

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 職務の分離という観点から、責任の分担に問題が見られる事例数
- 責任の割り当てが欠如しているか不十分であるために発生した問題のうち、深刻化した問題、あるいは未解決の問題の数
- IT 部門の対応能力に満足している利害関係者の割合

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 利害関係者の満足度(調査)
- IT 組織の機能不全または必要な能力の欠如により対応が遅れているビジネスイニシアチブの数
- ビジネス戦略上、IT 部門の支援を受けるべきでありながら受けていないビジネスプロセスの数
- IT 部門外で行われ、承認されていない、または IT 部門の標準に従っていない主要な IT 活動の数

成熟度モデル

PO4 IT プロセスと組織及びそのかかわりの定義

「ガバナンス要件に準拠しつつビジネス戦略に迅速に対応すると同時に、明確かつ有能な連絡窓口を設ける。」という IT に対するビジネス要件を満たす上で、「IT プロセスと組織及びそのかかわりの定義」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
IT 組織は、ビジネス目標の達成に焦点を当てるよう、効果的に編成されていない。

1 初期/その場対応
IT 関連の活動および部門の対応は事後的であり、一貫して実行されていない。IT 部門がビジネスプロジェクトに関与するのは、プロジェクトの終盤に限られている。IT 部門は単なるサポート部門と捉えられており、総体的な組織構造の一部として認識されていない。IT 組織の必要性は暗黙的に理解されているが、役割と責任は正式化されておらず、徹底されていない。

2 再現性はあるが直感的
IT 部門は、顧客のニーズおよびベンダーとの関係において戦術的に対応できるように組織されているが、その対応は一貫していない。体系的な組織およびベンダー管理の必要性が周知されているが、意思決定は依然として主要担当者の知識とスキルに依存している。IT 組織の管理およびベンダーとの関係の管理に、共通の技法が使用され始めている。

3 定められたプロセスがある
IT 部門およびサードパーティの役割と責任が定義されている。IT 組織が確立され、それについて文書化および周知が行われており、IT 戦略との整合性が確保されている。内部統制環境も確立している。運営委員会、内部監査部門、およびベンダー管理部門を含む他部門との関係は、正規の手続に基づいている。IT 組織は必要とされる機能を完備している。IT 担当者が担う役割とユーザが担う役割とが定義されている。IT スタッフの配置に関する必須要件と必要な専門知識が定義され、満たされている。ユーザやサードパーティとの関係が正式に定義されている。役割と責任の分離が定義、実施されている。

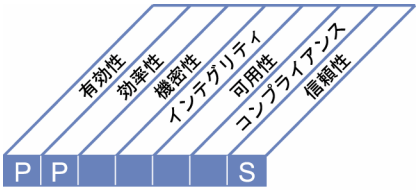
4 管理され、測定可能である
IT 組織は変化を先取りして、対応しており、ビジネス要件を満たすために必要な役割がすべて割り当てられている。IT 管理責任、プロセスのオーナシップ、説明責任、および実行責任が定義されており、相互の調整が図られている。IT 部門の編成において、社内の優れた実践基準が活かされている。IT マネジメント層は、どの組織とリレーションシップを選定したらよいか、どうモニタリングすればよいかを判断し、これを行う上で、必要となる専門知識とスキルを有している。ビジネス目標とユーザが定義した主要成功要因を測定可能な基準が標準化されている。プロジェクトにおける人員配置および専門家の育成に活用できるスキル一覧が利用可能な状態にある。スキルおよび資源の社内調達と社外調達のバランスは、明確に定められており、徹底されている。IT 組織の構造はビジネス上の必要性を適切に反映しており、技術そのものではなく戦略的ビジネスプロセスに適合したサービスの提供が可能になっている。

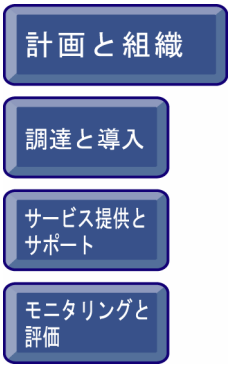
5 最適化
IT 組織の構造に、柔軟性および順応性がある。業界のベストプラクティスが取り入れられている。IT 組織およびプロセスの成果モニタリングを補助するため、関連技術が幅広く使用されている。組織の複雑さおよび地理的な分散に対応するために、関連技術が活用されている。継続的な改善プロセスが整備、運用されている。

コントロール目標 －概要－

PO5 IT 投資の管理

費用、便益、予算内での優先順位、正式な予算編成プロセス、および予算に照らした管理が組み込まれたフレームワークを構築および維持し、IT 関連の投資プログラムを管理する。利害関係者と協力し、IT 戦略計画および実行計画の枠内で総費用と便益を特定およびコントロールし、必要に応じて是正措置を講じる。このプロセスにより、IT とビジネスの利害関係者間の協力関係が促進され、IT 資源の効果的かつ効率的な使用が可能になる。さらに、オーナシップにおける総費用についての透明性と説明責任が確保され、ビジネス上の便益および IT 関連の投資からの収益の獲得が可能になる。





IT プロセス: IT 投資の管理のコントロール目標は、

エンドユーザの期待に応える統合/標準化されたサービスを提供し、IT の費用効率とビジネス収益性への貢献度を継続的かつ確実に向上させることを、**ビジネス要件**とし、

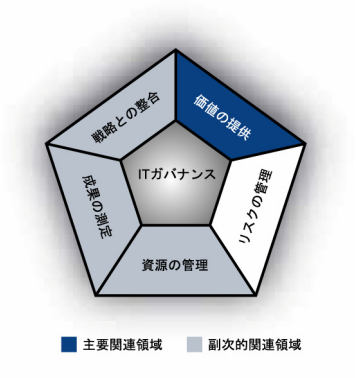
重点をおくべき IT 達成目標コントロールは、IT 戦略および投資上の決定に従って IT 予算を作成し、実績を把握し、IT 投資およびポートフォリオに関する効果的、かつ効率的な意思決定を行うことである。

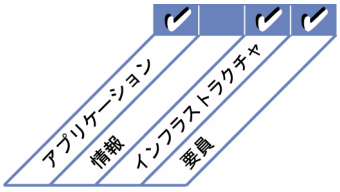
実現するための手段は、次の 3 項目である。

- 予算の予測と割り当て
- 正式な投資基準の定義(ROI、回収期間、NPV)
- 予測に照らしたビジネス価値の測定および評価

その成果の測定指標は、次の 3 項目である。

- 提供された IT サービスの単価削減率
- 予算総額に対する予算逸脱値の割合
- ビジネス価値として数値化された(接続性の向上による売上/サービスの増加など)IT 関連支出の割合





コントロール目標 －詳細－

PO5 IT 投資の管理

PO5.1 IT 財務管理フレームワーク
投資、サービス、資産のポートフォリオに基づいて、IT の予算編成や、費用/便益分析を行うための財務フレームワークを確立する。IT 関連の投資プログラム、IT サービス、および IT 資産のポートフォリオを維持管理する。これらのポートフォリオは、現行 IT 予算のよりどころとなる。新たな投資のための投資対効果検討のインプット情報を提供する際は、現在の IT 資産、サービスのポートフォリオを考慮する。新たな投資や、サービス、資産のポートフォリオの維持管理は、将来の IT 予算に影響する。これらのポートフォリオにおける費用、および便益に関連する情報を、予算の優先順位付けや、費用管理、便益管理に関連するプロセスに向けて、周知徹底する。

PO5.2 IT 予算内での優先順位の決定
運用、プロジェクト、維持管理のための IT 資源配分の優先順位付けのために、意思決定プロセスを導入する。IT 資源配分の優先順位付けを通じて、IT 関連投資のプログラム、その他の IT サービス、資産における企業ポートフォリオから生み出される収益の最適化を図ると同時に、収益の最適化に対する IT の貢献度を最大限に高める。

PO5.3 IT 予算編成プロセス
IT 関連投資プログラムの企業ポートフォリオにおいて確定した、優先順位を反映した予算の編成、管理のプロセスを確立する。予算の中には、現行のインフラストラクチャの運用、維持費用を含める。このプロセスは、総合的な IT 予算の編成に加え、各プログラムの、IT コンポーネントに重点を置いたプログラム別の予算編成に対応している必要がある。また、このプロセスには、全社の予算および各プログラムの個別予算の継続的な見直し、最適化、および承認を組み込む必要がある。

PO5.4 費用管理
実費用と予算を比較する費用管理プロセスを導入する。費用はモニタリングおよび報告される必要がある。予算からの逸脱がある場合は、それをタイムリーに特定し、プログラムへの影響を評価するとともに、当該プログラムのビジネス上のスポンサーと協力して適切な是正措置を講じ、必要に応じてプログラムの投資対効果検討内容を更新する必要がある。

PO5.5 便益管理
便益モニタリングプロセスを導入する。IT 関連の投資プログラムの一部として、または通常の業務支援の一環として、IT 部門に期待される業績への貢献内容を特定し、合意を得て、モニタリングおよび報告を行う。報告書を検討し、IT 部門による貢献に改善の余地がある場合は、適切な措置を策定、実施する必要がある。IT 部門の貢献における変化、または関連プロジェクトにおける変化がプログラムに何らかの影響を与える場合、当該プログラムの投資対効果検討内容を更新する必要がある。

マネジメントガイドライン

PO5 IT 投資の管理

From	インプット
PO1	戦略計画、IT 実行計画、プロジェクトおよびサービスポートフォリオ
PO3	インフラストラクチャ要件
PO10	最新の IT プロジェクトのポートフォリオ
AI1	ビジネス要件の実現可能性調査
AI7	導入後レビュー
DS3	成果および能力計画(要件)
DS6	IT の会計報告書
ME4	IT 関連のビジネス投資に期待されるビジネス成果

アウトプット	To						
費用/便益報告書	PO1	AI2	DS6	ME1	ME4		
IT 予算	DS6						
最新の IT サービスポートフォリオ	DS1						
最新の IT プロジェクトのポートフォリオ	PO10						

RACI チャート

アクティビティ ＼ 役割	CEO	CFO	企業幹部	CIO	ビジネス プロセス オーナー	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス、監査、リスク、セキュリティ
プログラムポートフォリオの維持	A	R	R	R	C					I	I
プロジェクトポートフォリオの維持	I	C	A/R	A/R	C		C	C		C	I
サービスポートフォリオの維持	I	C	A/R	A/R	C	C				C	I
IT 予算編成プロセスの確立と維持	I	C	C	A		C	C	C	R	C	
ビジネスにおける IT 投資、費用、および価値の特定、周知、およびモニタリング	I	C	C	A/R		C	C	C	R	C	C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- 正式な投資基準の定義(ROI、回収期間、NPV)
- 予算の予測と割り当て
- 予測に照らしたビジネス価値の測定および評価

促進

プロセスの達成目標
- IT 投資およびポートフォリオに関する意思決定を可能とすること
- IT 戦略および IT 投資に関する決定に沿った IT 予算の作成と追跡
- IT 費用の最適化および IT による便益の最大化

促進

IT の達成目標
- IT の費用効率およびビジネス収益性への IT の貢献度の向上
- IT 費用、便益、戦略、ポリシー、およびサービスレベルに関する透明性の確保と理解の実現
- IT 活用による費用効率の高いサービス品質、継続的な改善、および将来の変更に対する確実に対応すること

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 便益が事前に定義されているプロジェクトの割合
- 費用が計算されている IT サービスの割合
- プロジェクト後レビューが実施されているプロジェクトの割合
- 便益に関する報告書の作成頻度
- 成果に関する情報(費用効率、スケジュール効率、リスク分析結果)が入手可能なプロジェクトの割合

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 予算からの逸脱の件数
- 予算総額に対する予算逸脱値の割合
- 提供された IT サービスの単価削減率
- 事前に定義された便益を実現した IT 投資の割合

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 事前に定義されたビジネス上の便益を満たすか上回る成果が達成された IT 投資の割合
- ビジネス価値要因に関連付けられる IT の価値要因の割合
- ビジネス価値が明示された(接続性の向上による売上の増加など)IT 関連支出の割合

成熟度モデル

PO5 IT 投資の管理

「エンドユーザの期待に応える統合/標準化されたサービスを提供し、IT の費用効率とビジネス収益性への貢献度を継続的かつ確実に向上させる。」という IT に対するビジネス要件を満たす上で、「IT 投資の管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
IT 投資の選択および予算化の重要性が認識されていない。IT 投資および支出状況の追跡やモニタリングが行われていない。

1 初期/その場対応
組織は IT 投資管理の必要性を認識しているが、この必要性に関して一貫して周知されていない。IT 投資の選択および予算化の実行責任が、場当たり的に割り当てられている。IT 投資の選択および予算化は単発的に行われ、非公式な文書が作成されている。IT 投資の正当性は場当たり的に確認されている。事後的で、運用面重視の予算決定が行われている。

2 再現性はあるが直感的
IT 投資の選択および予算化が必要であることは、暗黙の了解となっている。選択および予算化のプロセスの必要性が周知されている。プロセスへのコンプライアンスは、組織内の各個人のイニシアチブに委ねられている。IT 予算のコンポーネント作成に、共通の技法が使われ始めている。事後的で戦術的な予算決定が行われている。

3 定められたプロセスがある
ビジネスおよび技術に関する主要な懸案事項を網羅した投資および予算化に関するポリシーとプロセスが定義および文書化され、周知されている。IT 予算は、IT 戦略計画およびビジネス戦略計画と整合されている。正式な予算化および IT 投資選択のプロセスが文書化され、周知されている。正式な研修が実施され始めているが、主に個人的なイニシアチブに依存している。IT 投資の選択および予算は正式に承認されている。IT 担当スタッフは、IT の予算編成および適切な IT 投資の提案に必要な専門知識とスキルを有している。

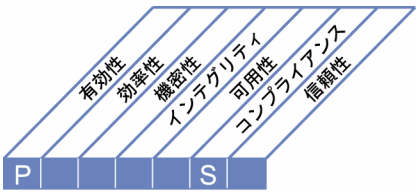
4 管理され、測定可能である
投資選択および予算化の実行責任および説明責任は特定の個人に割り当てられている。予算からの逸脱は特定され、解決されている。提案された投資内容のほか、既存業務に必要な直接および間接費用を対象として、ライフサイクル全体にわたる費用総額を考慮した、正式な費用分析方法が、取り決められており、その方法に基づく分析が実施されている。予め決められた、標準的な方法に基づき、予算化プロセスが使用されている。開発費用や運用費用にかかるハードウェアやソフトウェア経費が、システム統合や IIT 人材にシフトしていることの影響が、投資計画において認識されている。投資がもたらす便益および収益は、財務面および非財務面の双方から算出されている。

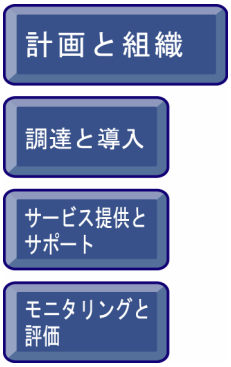
5 最適化
業界のベストプラクティスを活用することで、費用に対するベンチマーク評価が実施され、投資効果の向上に向けて、どのようなアプローチをとるべきかが特定されている。投資の選択および予算化のプロセスの際には、技術開発に関する分析が行われている。実際の投資成果の分析から得られた教訓に基づき、投資管理プロセスは、継続的に改善されている。投資内容は、価格/成果の改善傾向を鑑みて決定されている。資金調達における他の選択肢の正式な調査および評価は、組織の既存の資本構成を踏まえて、正式な評価方法を用いて実施されている。予算からの逸脱は、大きな問題となる前に早期発見されている。投資の決定には、ライフサイクル全体にわたる長期的な費用および便益の分析結果が反映されている。

コントロール目標 －概要－

PO6 マネジメントの意図と指針の周知

マネジメント層は、企業の IT コントロールフレームワークを策定し、ポリシーを定義、周知する必要がある。継続的な周知プログラムを導入し、マネジメント層が承認および推進する使命、サービス目標、ポリシー、手続などを明確に表明する必要がある。情報を周知することで、IT 目標の達成が促進され、さらにビジネスリスクおよび IT リスクのほか、目標や指針についての認識と理解を得ることができる。このプロセスにおいては、関連法規を確実に遵守する必要がある。





IT プロセス: マネジメントの意図と指針の周知のコントロール目標は、

現在および将来の IT サービス、関連リスク、および実行責任に関する正確かつタイムリーな情報の提供を、**ビジネス要件**とし、

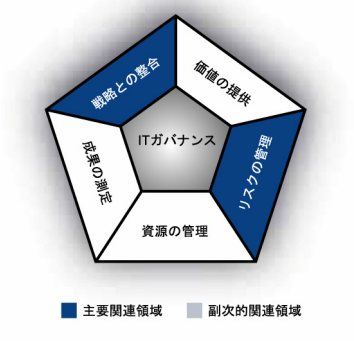
重点をおくべきコントロールは、承認済みの正確かつ理解しやすいポリシー、手続、ガイドライン、およびその他の文書を IT コントロールフレームワークに組み込み、利害関係者に提供することである。

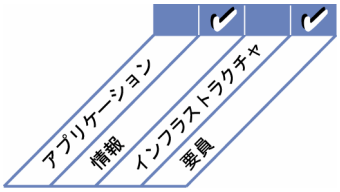
実現するための手段は、次の 3 項目である。

- IT コントロールフレームワークの定義
- IT ポリシーの作成および展開
- IT ポリシーの徹底

その成果の測定指標は、次の 3 項目である。

- IT サービスの中断に起因するビジネス活動の中断の件数
- 企業の IT コントロールフレームワークを理解している利害関係者の割合
- ポリシーに違反している利害関係者の割合





コントロール目標 －詳細－

PO6 マネジメントの意図と指針の周知

PO6.1 IT ポリシーおよび統制環境
企業の経営理念および運営方針に合致する IT の統制環境の要素を定義する。これらの要素には、IT 投資による価値の創出に対する期待/要件、リスクをどの程度許容するのか、しないのかについての考え方、インテグリティ、倫理的価値観、スタッフの能力、説明責任、および実行責任が含まれる。統制環境は、企業文化の上に構築する。企業文化は、重大なリスクへの対処の一方で、価値の提供を支援する。部門間の協力およびチームワークを促し、さらにコンプライアンスと継続的なプロセス改善を促進する。それればかりでなく、プロセスからの逸脱(失敗を含む)が適切に処理されることを支援する。

PO6.2 企業の IT リスクおよび内部統制のフレームワーク
企業全体を対象としたリスクと内部統制のアプローチを規定したフレームワークを作成および維持する。その目的は、IT 資源およびシステムの保護と同時に、価値の提供を実現することである。このフレームワークは、IT プロセスフレームワークおよび品質管理システムと統合され、ビジネス目標全般の達成に寄与するものでなければならない。このフレームワークは、情報資産に関するリスクを極小化すると同時に、提供する価値の最大化を実現することを目的としている。そのため、予防策の実施、不測事態のタイムリーな認識、損失の抑止およびビジネス資産のタイムリーな回復が必要となる。

PO6.3 IT ポリシーの管理
IT 戦略を支援する一連のポリシーを作成し、維持管理する。これら一連のポリシーには、ポリシーの目的、役割と責任、例外対応プロセス、規定遵守アプローチ、および手続、標準、ガイドラインの参照情報を含める必要がある。これらのポリシーでは、品質、セキュリティ、機密性、内部統制、知的財産権などの重要事項について規定し、その妥当性を定期的に検証および承認する必要がある。

PO6.4 ポリシーの展開
IT ポリシーをすべての関連スタッフに確実に展開して徹底させる。これにより、IT ポリシーを、企業の運営に不可欠な要素として組み込む。ポリシーの展開に際し、資源と意識に関するニーズ、および想定される結果について考慮する必要がある。

PO6.5 IT 目標と指針の周知
ビジネスおよび IT の目標と指針が企業全体で確実に意識および理解されるよう周知する。周知する情報は、使命、サービス目標、セキュリティ、内部統制、品質、倫理規定、行動規範、ポリシー、手続などであり、明確な方向付けを与えるものでなければならない。この周知活動は、継続的な周知プログラムに含まれる。周知は、マネジメント層の行動や言葉を後ろ盾として行う。マネジメント層は、IT セキュリティ意識を浸透させることに加えて、IT セキュリティが全社員の責任であることを周知することに、特に注力する必要がある。

マネジメントガイドライン

PO6 マネジメントの意図と指針の周知

From	インプット
PO1	IT 戦略/実行計画、IT プロジェクトおよびサービスポートフォリオ
PO9	IT にかかわるリスクに関するマネジメントガイドライン
ME2	IT コントロールの有効性に関する報告書

アウトプット	To							
企業の IT コントロールフレームワーク	ALL							
IT ポリシー	ALL							

RACI チャート

アクティビティ / 役割	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
IT 統制環境およびフレームワークの構築と維持	I	C	I	A/R	I	C		C	C		C
IT ポリシーの策定および保守	I	I	I	A/R		C	C	C	R		C
IT コントロールフレームワークおよび IT 目標と指針の周知	I	I	I	A/R					R		C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- IT コントロールフレームワークの定義
- IT ポリシーの策定および展開
- IT ポリシーの徹底

促進

プロセスの達成目標
- 共通かつ包括的な IT コントロールフレームワークの作成
- 共通かつ包括的な一連の IT ポリシーの策定
- IT 戦略、ポリシー、およびコントロールフレームワークの周知

促進

IT の達成目標
- IT 費用、便益、戦略、ポリシー、およびサービスレベルに関する透明性の確保と理解の実現
- 自動化された業務取引および情報交換の信頼性の確保
- 重要かつ機密の情報が、当該情報へのアクセスを許可されていないユーザに開示されないようにすること
- IT サービスの中断または変更が及ぼすビジネスへの影響の極小化
- アプリケーションおよび技術的対応策の適切な利用と成果達成の保証
- エラー、意図的な攻撃、または災害で生じた障害に対する、IT サービスおよび IT インフラストラクチャの耐性と回復力の確保

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- ポリシーの見直し/更新頻度
- ポリシーが承認されてからユーザに周知されるまでに要する時間
- 企業の IT コントロールフレームワークの見直し/更新頻度

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- IT ポリシーについて理解している利害関係者の割合
- 企業の IT コントロールフレームワークについて理解している利害関係者の割合
- ポリシーに違反している利害関係者の割合

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 機密情報の漏洩件数
- IT サービスの中断に起因するビジネス活動の中断の件数
- IT 費用、便益、戦略、ポリシー、およびサービスレベルに関する理解度

成熟度モデル

PO6 マネジメントの意図と指針の周知

「現在および将来の IT サービス、関連リスク、および実行責任に関する正確かつタイムリーな情報の提供。」という IT に対するビジネス要件を満たす上で、「マネジメントの意図と指針の周知」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
マネジメント層は、建設的な情報統制環境を確立していない。一連のポリシー、手続、標準、およびコンプライアンスプロセス確立の必要性が認識されていない。

1 初期/その場対応
情報統制環境に関する要件に対するマネジメント層の取り組みは、事後的である。問題が発生した場合に、ポリシー、手続、および標準が場当たり的に作成され、周知されている。作成、周知、およびコンプライアンスの各プロセスは非公式であり、一貫性がない。

2 再現性はあるが直感的
マネジメント層は、効果的な情報統制環境の必要性と要件を暗黙的に理解しているが、実践基準は概して非公式なものである。マネジメント層は、コントロールポリシー、手続、および標準の必要性を周知しているが、その作成は個々の管理者およびビジネス部門の裁量に委ねられている。品質の確保は追求すべき望ましい理念であると認識されているが、その実践は個々の管理者の裁量に委ねられている。研修は、必要に応じて個人単位で実施されている。

3 定められたプロセスがある
マネジメント層は、ポリシー、手続、および標準のフレームワークを含む完全な情報コントロールと品質管理の環境を作成し、文書化および周知している。ポリシーの作成プロセスは体系化され、維持されており、スタッフに周知されている。既存のポリシー、手続、および標準もある程度信頼できるものであり、重要事項も網羅されている。マネジメント層は IT セキュリティ意識の浸透の重要性を認識しており、セキュリティ意識向上プログラムを導入している。情報統制環境に対応した正式な研修が実施されているが、厳密に適用されてはいない。コントロールポリシーおよび標準の作成に関する総合的なフレームワークは存在するが、これらのポリシーや標準の遵守について、一貫したモニタリングは実施されていない。総合的な作成に関するフレームワークが規定されている。セキュリティ意識向上のための技法が、標準化および正式化されている。

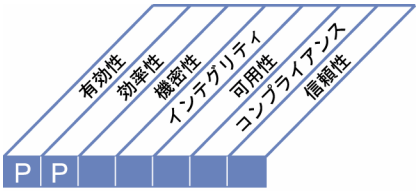
4 管理され、測定可能である
マネジメント層は、内部統制のポリシーの周知に関する実行責任を負っており、重大な変更に合わせた環境の整備に必要な資源の割り当て、および実行責任の委譲を行っている。品質および IT セキュリティに関する意識向上を確実にする、建設的かつ事前対応的な情報統制環境が確立されている。社内の優れた実践基準を組み合わせて完成された一連のポリシー、手続、および標準が作成、維持、周知されている。それらを展開し、その後のコンプライアンス状況を確認するフレームワークが確立されている。

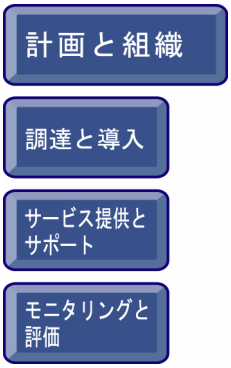
5 最適化
情報統制環境は、戦略管理フレームワークおよび構想との整合性が確保されており、頻繁に見直しおよび更新が行われ、継続的に改善されている。社内外の専門家が起用され、コントロール指針や周知技法に業界のベストプラクティスが確実に取り入れられている。モニタリング、セルフ評価、およびコンプライアンスチェックは、組織内に浸透している。ポリシーおよび知識ベースを保守し、情報周知を最大限に図るために、OA ツールと CBT ツール(コンピュータを利用した研修ツール)など、関連技術が駆使されている。

コントロール目標 －概要－

PO7 IT 人材の管理

ビジネス部門に対する IT サービスの創造と提供のために、有能な人材を獲得、維持し、意欲を引き出す。これは、採用、研修、業績評価、昇進、および解雇を支援するために、文書化され合意された行動基準を遵守することで達成される。要員は重要な資産であり、ガバナンスおよび内部統制環境は要員の意欲と能力に大きく依拠するため、このプロセスは非常に重要である。





IT プロセス: IT 人材の管理のコントロール目標は、

IT サービスの創造と提供を行う有能かつ意欲的な要員の確保を、**ビジネス要件**とし、

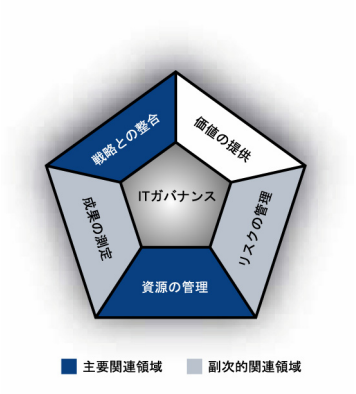
重点をおくべきコントロールは、要員の募集と教育、明確なキャリアパスに基づく意欲の引き出し、スキルに応じた役割の割り振り、定義されたレビュープロセスの確立、職位定義書の作成、個人への依存を確実に認識することである。

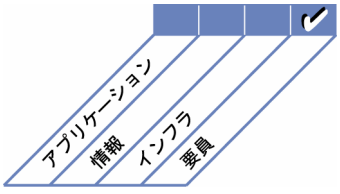
実現するための手段は、次の 3 項目である。

- スタッフの業績レビュー
- IT 実行計画を実現させるための IT 担当者の採用と教育
- 主要な人材への過剰依存によるリスクの軽減

その成果の測定指標は、次の 3 項目である。

- IT 担当者の専門知識とスキルに対する利害関係者の満足度
- IT 担当者の離職率
- 職務に必要な資格を有する IT 要員の割合





コントロール目標 －詳細－

PO7 IT 人材の管理

PO7.1 要員の募集および保持
IT 要員の募集プロセスと、組織全体の人事ポリシーおよび手続(採用、望ましい職場環境、新人研修などの)を確実に整合させる。マネジメント層は、組織の目標達成に必要なスキルを有する IT 人材が適材適所に確実に配置されるプロセスを導入する。

PO7.2 要員の能力
要員がそれぞれの役割を果たす上で必要な能力を有しているかどうか、学歴や研修内容、経験などを基に定期的に検証する。資格および認証プログラムを適宜取り入れて、中核となる IT 能力要件を定義し、継続的に維持されているか検証する。

PO7.3 役割に応じた人材配置
要員の役割、責任と報酬のフレームワークを定義し、モニタリングおよび監督する。同時に、管理ポリシーと管理手続、倫理規定と専門家としての行動基準を遵守することを要求する。
雇用契約条件においては、情報セキュリティ、内部統制、および法規制遵守に関する従業員の責任を強調する必要がある。監督の度合いは、 職位に求められる機密性および付与される責任の範囲に応じて定める必要がある。

PO7.4 要員の研修
IT 従業員の採用時に適切なオリエンテーションを行い、その後も継続的に研修を実施し、組織の目標達成に必要なレベルの知識、スキル、能力、内部統制とセキュリティへの意識を身に付けさせる。

PO7.5 個人に対する依存
知識の記録(文書化)、知識の共有、後任者育成、および予備要員の確保により、主要な要員に対する極度の依存を最小限に抑える。

PO7.6 要員の人事認可手続
IT 人材の募集プロセスには、経歴調査を含める。身元調査は、従業員、契約社員、およびベンダーに対して実施し、そのレビューの範囲および頻度は担当業務の機密性や重要性に応じて決定する。

PO7.7 従業員の業績評価
組織の達成目標に向けた各従業員の目標、確立された標準、各職務固有の責任、これらに関連する成果については、タイムリーな評価を定期的に実施する。また、従業員に対して、成果および勤務態度に関する指導を適宜行う。

PO7.8 職務の変更および解雇
職務の変更、特に解雇に際しては、臨機応変な対応を行う。知識の引継ぎ、責任の再割り当て、およびアクセス権の取り消しにより、リスクを最小限に抑え、当該職務が確実に継続されるようにする。

マネジメントガイドライン

PO7 IT 人材の管理

From	インプット
PO4	IT 組織およびそのリレーションシップ、文書化された役割および責任
AI1	ビジネス要件の実現可能性調査

アウトプット	To						
IT の人事ポリシーおよび手続	PO4						
IT スキルマトリクス	PO4	PO10					
職務定義書	PO4						
個別の研修を含むユーザのスキルと能力	DS7						
具体的な研修要件	DS7						
役割と責任	ALL						

RACI チャート

アクティビティ	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
IT スキル、職位定義書、給与支払い区分、個人的な業績ベンチマークの特定		C		A		C	C	C	R	C	
IT 人材に関する人事ポリシーおよび手続の実施(募集、採用、調査、報酬、研修、評価、昇進、および解雇)				A		R	R	R	R	R	C

役割

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- IT 実行計画を実現するための IT 担当者の採用と教育
- 主要な人材への過剰依存によるリスクの軽減
- スタッフの業績レビュー

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 専門的な能力開発プログラムを修了した IT 担当スタッフの割合
- 文書化された有効かつタイムリーな業績レビューを行っている IT 担当スタッフの割合
- 職務定義書および採用条件が規定されている IT 部門内の職位の割合
- 1 人あたりの研修および能力開発プログラム(指導を含む)への平均参加日数(年間)
- IT 担当スタッフのローテーション率
- 職務に必要な資格を有する IT 要員の割合
- IT 関連職務の欠員補充に要する平均日数

促進

プロセスの達成目標
- 実務的な IT 人事管理の実践基準の確立
- 全 IT 担当スタッフの有効活用および主担当者に対する依存度の極小化

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 担当役割に関し、戦略計画で定義された能力要件を満たす IT 担当スタッフの割合
- IT 関連職務の要員確保率
- 予定外の欠勤による損失日数
- 年間の IT 研修計画を修了した IT 担当スタッフの割合
- 人員に対する受託業者の実際の比率と予定比率との比較結果
- 身元調査を通過した IT 従業員の割合
- 適格な予備要員が割り当てられている IT 関連職務の割合

促進

IT の達成目標
- IT 戦略に対応する IT スキルの獲得と維持
- 機敏な IT 能力の創出

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- IT 担当者の専門知識とスキルに対する利害関係者の満足度
- 現状に満足している IT 担当者の割合(複合指標による)
- IT 担当者の離職率

成熟度モデル

PO7 IT 人材の管理

「IT サービスの創造と提供を行う有能かつ意欲的な要員の確保。」という IT に対するビジネス要件を満たす上で、「IT 人材の管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
IT 人材管理と組織の技術計画策定プロセスとを整合させることの重要性が認識されていない。IT 人材の管理について正式に責任が割り当てられた人物またはグループが存在しない。

1 初期/その場対応
マネジメント層は、IT 人材管理の必要性を認識している。IT 人材管理プロセスは、非公式で、事後的である。IT 人材プロセスの運用においては、IT 担当者の採用と管理に焦点が当てられている。ビジネスおよび技術の急速な変化と、ソリューションの一層の多様化により、新しいスキルや能力レベルの必要性が高まっていることが、認識されつつある。

2 再現性はあるが直感的
IT 担当者の採用および管理に戦術的なアプローチが用いられているが、これはプロジェクトごとの必要性に対応するものであり、優れたスキルを有するスタッフを社内外から適切なバランスで活用するという共通理解に基づいていない。新入社員に対して非公式な研修が実施されているが、その後は必要な場合のみ研修が実施されている。

3 定められたプロセスがある
IT 人材の管理に関するプロセスが定義および文書化されている。IT 人材管理計画が存在する。IT 担当者の採用および管理について、戦略的なアプローチが用いられている。IT 人材の必要性を満たす正式な研修計画が策定されている。技術スキルおよびビジネス管理スキルの発展を目指したローテーションプログラムが確立されている。

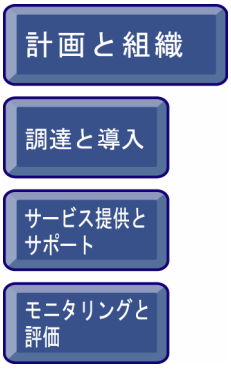
4 管理され、測定可能である
IT 人材管理計画の策定および維持に関する実行責任は、計画を策定し維持するのに必要な専門知識とスキルを有する特定の個人またはグループに割り当てられている。IT 人材管理計画の策定および管理プロセスには、変化に対する即応性がある。組織には、IT 人材管理計画からの逸脱を特定するための標準化された指標があり、特に IT 担当者の増員および離職管理に重点が置かれている。報酬および業績のレビューが制度化されつつあり、他の IT 組織および業界のベストプラクティスと比較検討されている。キャリアパスの整備を考慮した、積極的な IT 人材管理が行われている。

5 最適化
IT 人材管理計画は変化するビジネス要件に対応するために継続的に更新されている。IT 人材管理は技術計画に統合され、IT スキル開発の最適化および使用可能な IT スキルの活用が確実に行われている。IT 人材管理は企業の戦略方針に統合され、当該指針に対応している。報酬、業績レビュー、業界フォーラムへの参加、知識の継承、研修および指導など、IT 人材管理の各要素に業界のベストプラクティスが反映されている。新しい技術標準および製品を組織に導入する際は、必ず事前研修プログラムが用意されている。

コントロール目標 －概要－

PO8 品質管理

実績のある開発プロセス、調達プロセス、および標準が組み込まれた品質管理システムを作成し、維持する必要がある。これは、明確な品質要件、手続、およびポリシーを提示し、品質管理システムを計画、導入、維持することで実現できる。品質要件は、数値化された達成可能な指標として表し、周知する。モニタリング、分析、逸脱への対応、および利害関係者への結果報告を常時行うことにより、継続的な改善を実現する。品質管理は、IT によるビジネスへの価値提供と継続的な改善および利害関係者に対する透明性を確実に確保する上で不可欠である。



IT プロセス: 品質管理のコントロール目標は、

提供する IT サービスの品質を、継続的かつ測定可能な形で改善することを、**ビジネス要件**とし

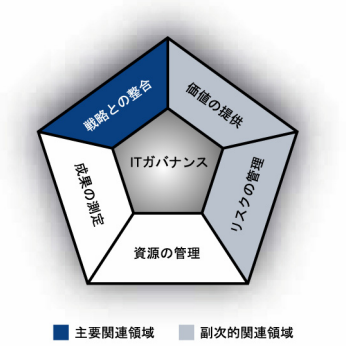
重点をおくべきコントロールは、品質管理システム(QMS)を定義し、事前に定義された目標に対して成果を継続的にモニタリングし、IT サービスの継続的な改善プログラムを導入することである。

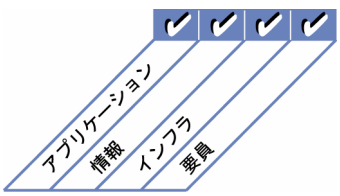
実現するための手段は、次の 3 項目である。

- 品質標準および品質の実践基準の定義
- 定義された品質標準および実践基準に対する、社内外の成果のモニタリングとレビュー
- 継続的な QMS の改善

その成果の測定指標は、次の 3 項目である。

- IT の品質に満足している利害関係者の割合(重要性により加重)
- 品質保証部門による正式な定期レビューの対象のうち、品質達成目標を満たしている IT プロセスの割合
- 品質保証(QA)レビューの対象となっているプロセスの割合





コントロール目標 －詳細－

PO8 品質管理

PO8.1 品質管理システム
ビジネス要件に沿った品質管理に関して、標準化された、正式で、かつ継続的なアプローチを提供する QMS を確立し、維持する。QMS は、品質要件と品質基準、主要 IT プロセスとその順序および相互関係を特定し、さらに不適合の定義、発見、是正、および防止に関するポリシー、基準、方法を特定する。QMS では、役割、任務、および実行責任を含む品質管理の組織構造を定義する必要がある。すべての主要分野において、基準およびポリシーに沿った品質計画を作成し、品質データを記録する。QMS の効果および適用レベルのモニタリングと測定を行い、必要に応じて改善を行う。

PO8.2 IT 標準および品質の実践基準
組織が QMS の目的を達成できるよう、主要な IT プロセスについて標準、手続、および実践基準を特定し、維持する。組織における品質の実践基準を改善、調整する際は、業界のベストプラクティスを参照する。

PO8.3 開発および調達標準
最終成果物のライフサイクルを通じてすべての開発および調達に関する標準を導入および維持し、主要な工程ごとに、合意された承認基準に基づいて承認を得る。検討すべき課題として、ソフトウェアコーディング標準、命名規則、ファイル形式、スキーマとデータディクショナリの設計標準、ユーザインターフェース標準、相互運用性、システムパフォーマンス効率、拡張性、開発標準およびテスト標準、要件に照らした評価、テスト計画、単体テスト、回帰テスト、および統合テストが挙げられる。

PO8.4 顧客中心
顧客の要求事項を特定し、それらと IT 標準および IT の実施内容との調整を図ることにより、品質管理を顧客に確実にフォーカスさせる。

PO8.5 継続的改善
継続的な改善を促進する総合的な品質計画が維持され、定期的に周知している。

PO8.6 品質の測定、モニタリング、およびレビュー
QMS への継続的なコンプライアンスおよび QMS が提供する価値をモニタリングするための測定項目を定義し、計画して導入する。プロセスオーナは、適切な是正措置および予防措置を講じるために、情報を測定、モニタリングおよび記録する必要がある。

マネジメントガイドライン

PO8 品質管理

From	インプット
PO1	IT 戦略計画
PO10	詳細なプロジェクト計画
ME1	是正措置計画

アウトプット	To						
調達標準	AI1	AI2	AI3	AI5	DS2		
開発標準	PO10	AI1	AI2	AI3	AI7		
品質標準および指標の要件	ALL						
品質改善策	PO4	AI6					

RACI チャート

アクティビティ ＼ 役割	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
品質管理システムの定義	C		C	A/R	I	I	I	I	I	I	C
品質管理システムの確立と維持	I	I	I	A/R	I	C	C	C	C	C	C
品質標準の策定と組織全体への周知		I		A/R	I	C	C	C	C	C	C
継続的改善に向けた品質計画の策定および管理				A/R	I	C	C	C	C	C	C
品質目標の達成状況の測定、モニタリング、およびレビュー				A/R	I	C	C	C	C	C	C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- 品質標準および品質の実践基準の定義
- 定義された品質標準および品質の実践基準に対する、社内外の成果のモニタリングとレビュー

促進

プロセスの達成目標
- IT プロセスの品質標準および品質重視の風土の確立
- 効率的かつ効果的な IT 品質保証部門の確立
- IT プロセスおよび IT プロジェクトの有効性のモニタリング

促進

IT の達成目標
- 提供サービスとサービスレベルに対するエンドユーザの満足の確保
- 対応策とサービスの提供における不備と補正作業の必要性の削減
- 期間内、予算内での品質標準を満たすプロジェクトの提供

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- QA レビューの対象となっているプロジェクトの割合
- 品質意識/品質管理研修を受けている IT 担当スタッフの割合
- 利害関係者が品質保証に積極的に協力している IT プロセスおよび IT プロジェクトの割合
- QA レビューの対象となっているプロセスの割合
- 品質調査に参加している利害関係者の割合

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 本番稼働前に解決されなかった不具合の割合
- ユーザあたりの重大インシデント件数の削減率(月間)
- 品質保証部門がレビューして承認した、品質達成目標を満たしている IT プロジェクトの割合
- 品質保証部門による正式な定期レビューの対象のうち、品質達成目標を満たしている IT プロセスの割合

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- IT の品質に満足している利害関係者の割合(重要性により加重)

成熟度モデル

PO8 品質管理

「提供するITサービスの品質を、継続的かつ測定可能な形で改善する。」というITに対するビジネス要件を満たす上で、「品質管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
組織には、QMS の計画策定プロセスおよびシステム開発ライフサイクルの方法論が欠如している。マネジメント層および IT 担当スタッフは、品質プログラムの必要性を認識していない。プロジェクトおよび運用における品質レビューはまったく行われていない。

1 初期/その場対応
マネジメント層は QMS の必要性を認識している。QMS は、品質管理を行う各担当者により運用されている。マネジメント層は非公式な品質判断を行っている。

2 再現性はあるが直感的
IT 部門内での QMS 活動を定義、モニタリングするプログラムが、策定され始めている。実施されている QMS 活動は、組織全体のプロセスではなく、IT プロジェクト指向および IT プロセス指向のイニシアチブに焦点が当てられている。

3 定められたプロセスがある
QMSプロセスが定義され、マネジメント層が周知しており、ITマネジメント層およびエンドユーザマネジメント層が関与している。すべての組織レベルを対象とした、品質に関する教育および研修プログラムが実施され始めている。品質に関する基本的な要求事項が定義され、各プロジェクト間および IT 組織内で共有されている。品質管理に関する共通のツールおよび実践基準が用いられ始めている。品質に対する満足度調査が計画され、不定期に実施されている。

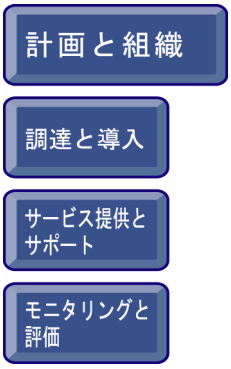
4 管理され、測定可能である
サードパーティに依存しているプロセスも含め、すべてのプロセスにおいて QMS が適用されている。品質指標に関する標準化された知識ベースが確立されつつある。QMS イニシアチブの妥当性を確認するために、費用/便益分析が使用されている。業界および競合他社に対するベンチマーク評価が実施され始めている。すべての組織レベルを対象とした、品質に関する教育および研修プログラムが制度化されている。ツールおよび実践基準が標準化されつつあり、定期的な根本原因の分析が行われている。品質に対する満足度調査が一貫して実施されている。標準化された品質測定プログラムが整備され、適切に体系化されている。IT マネジメント層は、品質指標に関する知識ベースを構築している。

5 最適化
QMSはすべてのIT活動に統合され、運用が徹底されている。QMSプロセスには、柔軟性とIT環境の変化に対する順応性がある。品質指標に関する知識ベースは、社外のベストプラクティスを取り入れて拡張されている。社外の標準に対するベンチマーク評価が日常的に実施されている。品質に対する満足度調査は継続的なプロセスであり、根本原因の分析や改善策の実施に繋がっている。品質管理プロセスのレベルは、正式に保証されている。

コントロール目標 －概要－

PO9 IT リスクの評価と管理

リスク管理フレームワークを構築し、維持する。フレームワークでは、合意された一般的な IT リスクレベル、リスク軽減戦略、および合意された残存リスクについて文書化する。すべての計画外のイベントが組織の達成目標に与える潜在的な影響を特定、分析、評価する必要がある。残存リスクを許容レベルまで軽減するために、リスク軽減戦略を導入する必要がある。利害関係者が理解可能なように評価結果をとりまとめると同時に、財務的な観点でもとりまとめる。これにより、利害関係者からみても、リスクが許容範囲におさまるようにする。



IT プロセス: IT リスクの評価と管理のコントロール目標は

IT リスク、および IT リスクがビジネスプロセスと達成目標に及ぼす潜在的な影響を分析し、周知することを、**ビジネス要件**とし、

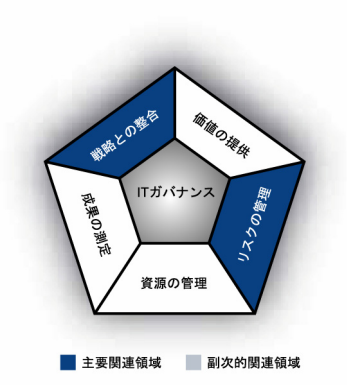
重点をおくべきコントロールは、ビジネス面および運用面の各種リスク管理フレームワークに統合されたリスク管理フレームワークの構築、リスク評価、リスクの軽減、および残存リスクの周知である。

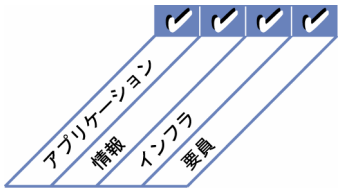
実現するための手段は、次の 3 項目である。

- 社内外の管理プロセスへのリスク管理の完全な組み込みと一貫した適用の保証
- リスク評価の実施
- リスク是正措置計画の提示と周知

その成果の測定指標は、次の 3 項目である。

- リスク評価の対象となる重要 IT 目標の割合
- 特定された重大 IT リスクのうち、実行計画が作成されているものの割合
- 導入が承認されたリスク管理実行計画の割合





コントロール目標 －詳細－

PO9 IT リスクの評価と管理

PO9.1 IT リスク管理とビジネスリスク管理の整合
IT ガバナンス、IT リスク管理、および IT コントロールフレームワークを、組織(企業)のリスク管理フレームワークと統合する。これには、組織として、リスクをどの程度許容するのか、しないのかについての考え方と、リスク許容レベルとの間の整合を確保することが含まれる。

PO9.2 リスクをめぐる状況の明確化
リスク評価フレームワークの適用背景を明確化し、確実に適正な結果が得られるようにする。これには、個々のリスク評価の社内外における背景、評価の達成目標、およびリスクが評価される基準の確定が含まれる。

PO9.3 イベントの特定
ビジネス、法規制、法律、技術、取引先、人材、および運用面において、企業目標または企業運営に影響を与える可能性のあるイベント(脅威および脆弱性)をすべて特定する。影響の性質(プラスの影響、マイナスの影響、またはその両方)を判断し、この情報を維持する。

PO9.4 リスク評価
特定されたすべてのリスクの発生可能性と影響を、定性的および定量的な方法を用いて繰り返し評価する。内在しているリスクおよび残存リスクの発生可能性と影響は、種類別、およびポートフォリオに基づいて、それぞれ判断する必要がある。

PO9.5 リスクへの対応
リスクのオーナと影響を受けるプロセスのオーナを特定し、費用効率に優れたコントロールとセキュリティ対策により継続的かつ確実にリスクを軽減するリスク対応策を作成して維持する。リスク対応策では、回避、軽減、共有、および許容などのリスク対応戦略を明確化する必要がある。対応策の作成にあたっては、費用および便益を考慮し、残存リスクを定義されたリスク許容レベルの範囲内に抑える対応策を選択する。

PO9.6 リスク対応実行計画の維持およびモニタリング
必要であると特定されたリスク対応策の導入に向け、コントロールについてアクティビティをすべてのレベルにわたり優先順位付けし、計画を策定する。アクティビティには、費用、便益、および実行責任の明確化が含まれる。推奨される実行策および残存リスクの許容に関する承認を求め、約束した実行策を、影響を受けるプロセスのオーナに、確実に自らのものとして認めさせる。

マネジメントガイドライン

PO9 IT リスクの評価と管理

From	インプット
PO1	IT 戦略/実行計画、IT サービスポートフォリオ
PO10	プロジェクトのリスク管理計画
DS2	サービスプロバイダに関するリスク
DS4	緊急時対応テストの結果
DS5	セキュリティ上の脅威と脆弱性
ME1	過去のリスク傾向およびイベント
ME4	企業の IT リスク傾向

アウトプット	To						
リスク評価	PO1	DS4	DS5	DS12	ME4		
リスクに関する報告書	ME4						
IT にかかわるリスクに関するマネジメントガイドライン	PO6						
IT にかかわるリスクの是正措置計画	PO4	AI6					

RACI チャート

アクティビティ ＼ 役割	CEO	CFO	企業幹部	C/O	ビジネス経営幹部	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
リスク管理の整合性に関する判断(リスクの評価など)	A	R/A	C	C	R/A	I					I
関連する戦略的ビジネス目標の理解		C	C	R/A	C	C					I
関連するビジネスプロセス目標の理解				C	C	R/A					I
社内の IT 目標の特定とリスク背景の明確化					R/A		C	C	C		I
目標に関連するイベントの特定[イベントの一部はビジネス指向(ビジネスは A)、一部は IT 指向(IT は A、ビジネスは C)	I			A/C	A	R	R	R	R		C
イベントに関連するリスクの評価				A/C	A	R	R	R	R		C
リスク対応策の評価	I	I	A	A/C	A	R	R	R	R		C
コントロールに関するアクティビティの優先順位付けおよび計画	C	C	A	A	R	R	C	C	C		C
リスク対応実行計画の承認および資金の確保		A	A		R	I	I	I	I		I
リスク対応実行計画の維持およびモニタリング	A	C	I	R	R	C	C	C	C	C	R

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- 管理プロセスへのリスク管理の完全な組み込み
- マネジメント層および主要担当者との定期的なリスク評価の実施
- リスク是正措置計画の提示と周知

プロセスの達成目標
- IT リスクの発生可能性と影響の明確化および低減
- 重大な IT リスクに対する、費用効率に優れた実行計画の策定

IT の達成目標
- IT 目標達成の保証
- リスクが IT 目標および資源に与える、ビジネス上の影響の明確化
- すべての IT 資産の責任の所在の明確化と適切な保護

促進

促進

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- リスク管理(評価および軽減)活動に費やされた IT 予算の割合
- IT リスク管理プロセスの見直し頻度
- 承認されたリスク評価の割合
- 合意された頻度の範囲内で何らかの措置が講じられたリスクモニタリング報告書の件数
- 特定された IT イベントがリスク評価に使用された割合
- 導入が承認されたリスク管理実行計画の割合

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 特定された重大 IT イベントのうち評価されたものの割合
- 新たに特定された IT リスク(前回の作業時との比較)の数
- リスク評価プロセスで特定されていないリスクに起因する重大インシデントの件数
- 特定された重大 IT リスクのうち、実行計画が作成されているものの割合

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- リスク評価の対象となっている重要 IT 目標の割合
- IT リスク評価のアプローチに統合された IT リスク評価の割合

成熟度モデル

PO9 IT リスクの評価と管理

「IT リスク、および IT リスクがビジネスプロセスと達成目標に及ぼす潜在的な影響を分析し、周知する。」という IT に対するビジネス要件を満たす上で、「IT リスクの評価と管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
プロセスおよびビジネスの意思決定におけるリスク評価は実施されていない。組織は、セキュリティ上の脆弱性および開発プロジェクトの不確実性に関連するビジネス上の影響を考慮していない。リスク管理と、IT 対応策の調達および IT サービスの提供との関連性が認識されていない。

1 初期/その場対応
IT リスクについては場当たり的に考慮されている。プロジェクトごとの判断により、プロジェクトリスクに対する非公式な評価が行われる場合がある。リスク評価は、プロジェクト計画に稀に組み込まれることがあるが、特定の管理者に実施が指示されることはほとんどない。セキュリティ、可用性、およびインテグリティなど、IT にかかわる具体的なリスクについて、プロジェクトごとに考慮されることもある。日常業務に影響を与える IT にかかわるリスクについて、経営会議で取り上げられることはほとんどない。リスクについて考慮されたとしても、リスクの軽減策に一貫性がない。IT リスクが検討を要する重要な課題であるという理解が広がりつつある。

2 再現性はあるが直感的
開発途中の未熟なリスク評価アプローチが存在する。アプローチの導入は個々のプロジェクト管理者の裁量に委ねられている。リスク管理は概して高いレベルにあるが、主要プロジェクトに対してのみ、または問題に対応するためにのみ、適用される傾向がある。リスクが特定された場合に、リスク軽減プロセスが導入され始めている。

3 定められたプロセスがある
組織全体のリスク管理ポリシーにより、リスク評価の実施時期および実施方法が定められている。リスク管理は、定義され文書化されたプロセスに従って行われる。全スタッフを対象としたリスク管理研修が実施されている。リスク管理プロセスの適用および研修への参加の決定は、個人の裁量に委ねられている。リスク評価の方法論は妥当かつ堅固なものであり、ビジネスに対する主要なリスクを確実に特定できる。リスクが特定された場合、通常は主要なリスクを軽減するプロセスが導入される。職務定義書では、リスク管理の実行責任についても言及されている。

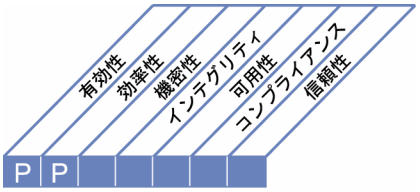
4 管理され、測定可能である
リスク評価およびリスク管理は標準手続に組み込まれている。リスク管理プロセスにおける例外事項は IT マネジメント層に報告される。IT リスクの管理は、マネジメント層レベルの責務である。リスクの評価および軽減は各プロジェクトレベルで行われており、さらに IT 運用全体のレベルでも定期的に実施されている。IT にかかわるリスクのシナリオに重大な影響を与える可能性があるビジネス環境および IT 環境の変化については、マネジメント層に報告されている。マネジメント層はリスクの状況をモニタリングし、詳細な情報に基づいてリスクの許容範囲を決定できる。特定されたすべてのリスクに対してオーナが指定されており、マネジメント層および IT マネジメント層が、組織として許容し得るリスクのレベルを決定している。IT マネジメント層は、リスクの評価およびリスク/リターン比率の定義に用いる標準指標を作成している。マネジメント層は、定期的にリスクの再評価を行う運用リスク管理プロジェクトのための予算を計上している。リスク管理用のデータベースが整備されており、リスク管理プロセスの一部が自動化され始めている。IT マネジメント層が、リスク軽減戦略について検討している。

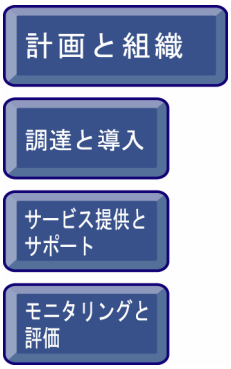
5 最適化
リスク管理が最適化されており、体系化されたプロセスが組織全体で徹底して運用され、適切に管理されている。優れた実践基準が組織全体に適用されている。リスク管理データの収集、分析、および報告の大部分が自動化されている。業界の専門家からの指導を受けており、IT 組織は経験に基づく情報の交換を目的として業界の有志のグループ(peer groups)に参加している。リスク管理は、ビジネス部門および IT 部門のすべての業務に実質的に統合され、十分に浸透しており、IT サービスのユーザがリスク管理に深く関与している。リスク管理計画が検討されずに IT の運用もしくは投資に関する重要な意思決定が行われた場合、マネジメント層はこれを発見し、対応策を講じることができる。マネジメント層は、継続的にリスク軽減戦略を評価している。

コントロール目標 －概要－

PO10 プロジェクト管理

すべてのITプロジェクトの管理を目的とするプログラムおよびプロジェクト管理フレームワークを確立する。このフレームワークでは、すべてのプロジェクトを適正に優先順位付けし、プロジェクト間の調整を行う。プロジェクトのリスク管理およびビジネスへの価値の提供を実現するため、フレームワークには、基本計画、資源の割り当て、成果物の定義、ユーザによる承認、サービスの提供に対する段階的なアプローチ、品質保証、正式なテスト計画、および導入後のテストと導入後レビューの実施を含める必要がある。このアプローチにより、予想外の費用やプロジェクトの中止によって生じるリスクが軽減され、ビジネス部門およびエンドユーザへの情報伝達および両者の関与が促進される。さらに、プロジェクト成果物の価値と品質が保証され、IT 関連の投資プログラムに対するそれらの貢献度を最大化できる。





IT プロセス: プロジェクト管理のコントロール目標は、

合意された期間、予算、および品質の範囲内でプロジェクトの成果を提供することを、**ビジネス要件**とし、

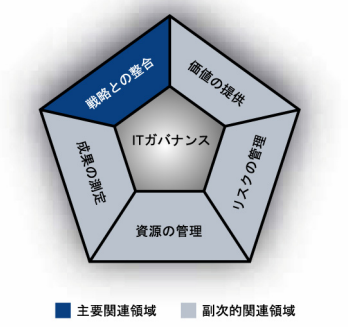
重点をおくべきコントロールは、IT プロジェクトに適用され、利害関係者の協力およびプロジェクトのリスクと進捗のモニタリングを可能にするプログラムおよびプロジェクト管理のアプローチを定義することである。

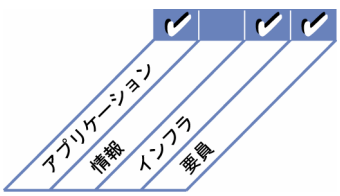
実現するための手段は、次の 3 項目である。

- プログラムとプロジェクトのフレームワークおよびアプローチの定義と実施
- プロジェクトマネジメントガイドラインの発行
- プロジェクトポートフォリオに詳述されている各プロジェクトの計画策定

その成果の測定指標は、次の 3 項目である。

- 利害関係者が期待する成果を達成したプロジェクトの割合(期間内、予算内で、要件を満たしている。重要性により加重)
- 導入後レビューが実施されたプロジェクトの割合
- プロジェクト管理標準および実践基準に準拠しているプロジェクトの割合





コントロール目標 －詳細－

PO10 プロジェクト管理

PO10.1 プログラム管理フレームワーク
プロジェクトの特定、定義、評価、優先順位付け、選択、開始、管理、およびコントロールにより、IT 関連の投資プログラムのポートフォリオに関連する、プロジェクトのプログラムを維持する。各プロジェクトが確実にプログラムの目標の達成を後押しするようにする。複数のプロジェクトのアクティビティおよび相互依存を調整し、プログラム内のすべてのプロジェクトが期待される成果の達成に貢献するよう管理し、資源要件や資源にかかわる問題に対処する。

PO10.2 プロジェクト管理フレームワーク
各実施プロジェクトに導入、適用する方法論に加え、プロジェクト管理の範囲と境界を定義するプロジェクト管理フレームワークを確立し、維持する。方法論には、少なくとも、プロジェクトの開始、計画、実行、コントロール、および終了の各段階のほか、チェックポイントおよび承認の工程を含める必要がある。フレームワークおよびフレームワークを支える方法論は、企業のポートフォリオ管理およびプログラム管理プロセスに統合されている必要がある。

PO10.3 プロジェクト管理のアプローチ
各プロジェクトの規模、複雑度、および法的要件に応じたプロジェクト管理のアプローチを確立する。プロジェクトガバナンスの体制には、プログラムのスポンサー、プロジェクトのスポンサー、運営委員会、プロジェクトオフィス(project office)、およびプロジェクト管理者の役割、実行責任、および説明責任のほか、それぞれが定められた責務(報告、段階ごとのレビューなど)を果たすための手段となる仕組みを組み込むことができる。すべての IT プロジェクトに対し、総合的な戦略プログラム内でのプロジェクトの実行に必要な権限を持つスポンサーを確実に割り当てる。

PO10.4 利害関係者の関与
IT 関連の投資プログラム全体の枠内におけるプロジェクトの定義と実行において、影響を受ける利害関係者の関与と協力を得る。

PO10.5 プロジェクト範囲の記述
プロジェクトの性質および範囲を定義および文書化し、プロジェクトの範囲および IT 関連の投資プログラム全体の枠内における他のプロジェクトとのリレーションシップについて、すべての利害関係者が共通の認識を持つようにし、その体制を促進する。この定義については、プロジェクトの開始前に、プログラムおよびプロジェクトのスポンサーから正式な承認を得なければならない。

PO10.6 プロジェクトの各フェーズの開始
プロジェクトの主要フェーズの開始が正式に承認され、すべての利害関係者に確実に周知させる。第 1 フェーズの承認は、プログラムのガバナンスに関する決定に基づいて行われる必要がある。以降の各フェーズの承認は、前フェーズの成果物のレビューと受入れ、また、プログラムの次回の主要なレビューにおける最新のビジネスケースの承認に基づいて行われなければならない。プロジェクトフェーズが重複している場合、プログラムおよびプロジェクトのスポンサーは、プロジェクトの進行を許可する承認手続の時期を定める必要がある。

PO10.7 統合プロジェクト計画
プロジェクトの開始から終了にいたるまで、その実行とコントロールの指針となる、承認済みの正式な統合プロジェクト計画(ビジネスおよび情報システムの資源についても扱う)を策定する。同一プログラム内の複数のプロジェクトにおけるアクティビティおよび相互依存について理解し、文書化する必要がある。プロジェクト計画は、プロジェクトの存続期間中保守されなければならない。プロジェクト計画および計画に対する変更は、プログラムおよびプロジェクトのガバナンスフレームワークに沿って承認される必要がある。

PO10.8 プロジェクトの資源
プロジェクトチームメンバーの実行責任、リレーションシップ、権限、および成果基準を定義し、有能なスタッフや受託業者の確保およびプロジェクトへのアサインの基本的な考え方を明確化する。プロジェクト目標の達成に向け、各プロジェクトに必要な製品およびサービスの調達について、組織における調達の実践基準に基づき計画および管理する必要がある。

PO10.9 プロジェクトのリスク管理
各プロジェクトに付随する固有のリスクを排除または極小化するため、不要な変更の原因となり得る領域とイベントに関する計画、特定、分析、対応、モニタリング、およびコントロールの体系化されたプロセスを適用する。プロジェクト管理プロセスおよびプロジェクトの成果物が抱えるリスクを把握し、一元的に記録する必要がある。

PO10.10 プロジェクトの品質計画
プロジェクトの品質システムおよびその導入方法が記載された、品質管理計画を作成する。この計画は正式にレビューし、関係者全員の合意を得た上で、統合プロジェクト計画に組み込む必要がある。

PO10.11 プロジェクト変更コントロール
各プロジェクトについて、変更コントロールの仕組みを確立する。これにより、プロジェクトのベースラインにかかわるすべての変更(費用、日程、範囲、品質など)を、プログラムおよびプロジェクトのガバナンスフレームワークに沿って適切にレビューおよび承認し、統合プロジェクト計画に組み込む。

PO10.12 保証方法に関するプロジェクト計画
プロジェクト計画の策定過程において、新規または修正されたシステムを認可する前提として必要とされる保証作業を明確にし、それらを統合プロジェクト計画に含める。この保証作業によって、内部統制およびセキュリティ機能が定められた要件を満たすことが保証されなくてはならない。

PO10.13 プロジェクトの成果の測定、報告、およびモニタリング
プロジェクトの主要基準(範囲、日程、品質、費用、リスクなど)に照らして、プロジェクトの成果を測定する。計画からの逸脱を特定し、逸脱によるプロジェクトおよびプログラム全体への影響を評価して、主要な利害関係者にその評価結果を報告する。また、必要に応じて、プログラムおよびプロジェクトのガバナンスフレームワークに沿った是正措置を提案、実施、およびモニタリングする。

PO10.14 プロジェクトの終了
各プロジェクトの終了時に、プロジェクトが計画どおりの成果および便益をもたらしたかどうか、プロジェクトの利害関係者が必ず確認するようにする。計画されたプロジェクトの成果およびプログラムの便益の達成に必要な事項のうち、未完了のものがあればそれを特定し、周知する。また、プロジェクトの実行により得られた教訓や知識を、将来のプロジェクトおよびプログラムにおいて活用できるよう、特定して文書化する。

(空白ページ)

マネジメントガイドライン

PO10 プロジェクト管理

From	インプット
PO1	プロジェクトポートフォリオ
PO5	最新の IT プロジェクトのポートフォリオ
PO7	IT スキルマトリクス
PO8	開発標準
AI7	導入後レビュー

アウトプット	To						
プロジェクトの成果報告書	ME1						
プロジェクトのリスク管理計画	PO9						
プロジェクトマネジメントガイドライン	AI1…AI7						
詳細なプロジェクト計画	PO8	AI1…AI7	DS6				
最新の IT プロジェクトのポートフォリオ	PO1	PO5					

RACI チャート

アクティビティ / 役割	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
IT 投資のためのプログラム/ポートフォリオ管理フレームワークの定義	C	C	A	R						C	C
IT プロジェクト管理フレームワークの確立と維持	I	I	I	R/A	I	C	C	C	C	R	C
IT プロジェクトのモニタリング、測定および管理システムの確立と維持	I	I	I	R		C	C	C	C	A/R	C
プロジェクト憲章、日程、品質計画、予算、コミュニケーション管理計画、およびリスク管理計画の作成			C	C	C	C	C	C	C	A/R	C
プロジェクトの利害関係者の協力および関与の確保	I		A	R	C						C
プロジェクトおよびプロジェクトに関する変更の効果的なコントロールの保証			C	C		C	C	C		A/R	C
プロジェクトの保証およびレビュー方法の定義と導入			I	C				I		A/R	C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- プログラムとプロジェクトのフレームワークおよびアプローチの定義と実施
- プロジェクトマネジメントガイドラインの発行
- プロジェクトポートフォリオに記述されている各プロジェクトの計画策定

促進

プロセスの達成目標
- プロジェクトの追跡調査および費用/時間コントロールの仕組みの確立
- プロジェクト状況の透明性の確保
- 重要な工程ごとのプロジェクト管理に関するタイムリーな意思決定

促進

IT の達成目標
- ビジネス戦略と合致するビジネス要件への対応
- 品質標準を満たすプロジェクトの、期間内、かつ予算内での遂行
- 取締役会の指示に従ったガバナンス要件への対応

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- プロジェクト管理標準および実践基準に準拠しているプロジェクトの割合
- 資格を有するか研修を受けたプロジェクト管理者の割合
- 導入後レビューが実施されたプロジェクトの割合
- プロジェクトに参加している利害関係者の割合(関与指数)

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 期間内、かつ予算内で実行されたプロジェクトの割合
- 利害関係者が期待する成果を達成したプロジェクトの割合

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 利害関係者が期待する成果を達成したプロジェクトの割合(期間内、予算内で、品質要件を満たしているかどうか―重要性により加重)

成熟度モデル

PO10 プロジェクト管理

「合意された期間、予算、および品質の範囲内でプロジェクトの成果を提供する。」というITに対するビジネス要件を満たす上で、「プロジェクト管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
プロジェクト管理の技法は用いられておらず、組織は、プロジェクトの不十分な管理および開発プロジェクトの失敗がビジネスに与える影響を考慮していない。

1 初期/その場対応
IT部門におけるプロジェクト管理技法およびアプローチの使用は、個々のIT管理者の判断に委ねられている。プロジェクトのオーナシップおよびプロジェクト管理に関して、マネジメント層の関与が欠如している。プロジェクト管理に関する重大な意思決定には、ユーザマネジメント層および顧客の意向が反映されていない。ITプロジェクトの定義において、顧客やユーザが、ほとんどあるいはまったく関与していない。IT 部門内に、プロジェクト管理を目的とした明確な組織が存在しない。プロジェクト管理に関する役割および責任が定義されていない。プロジェクト、日程、および工程が定義されていないか、定義されていたとしても不完全である。プロジェクトスタッフの作業時間および経費が追跡されておらず、予算との比較も行われていない。

2 再現性はあるが直感的
マネジメント層は、IT プロジェクト管理の必要性を理解し、周知している。組織は、さまざまなプロジェクトにおいて、何らかの技法や方法を確立し、利用しようとしている。各ITプロジェクトにおいて、ビジネス目標と技術目標が非公式に定義されている。ITプロジェクト管理への利害関係者の関与は限定的である。プロジェクト管理のさまざまな側面について、ガイドラインの初版が作成されている。プロジェクトマネジメントガイドラインの適用は、個々のプロジェクト管理者の裁量に委ねられている。

3 定められたプロセスがある
IT プロジェクト管理のプロセスおよび方法論が確立され、周知されている。IT プロジェクトは、適切なビジネス目標および技術目標とともに定義されている。IT部門およびビジネス部門におけるマネジメント層が、徐々にITプロジェクトの管理に責任を持って関与し始めている。IT 部門内にプロジェクトマネジメントオフィスが設置され、初期的な役割および責任が定義されている。IT プロジェクトはモニタリングされ、定義された最新の工程、日程、予算、および成果の測定項目が規定されている。プロジェクト管理研修が実施されている。プロジェクト管理研修は、主に各スタッフのイニシアチブに基づいて実施されている。品質保証手続およびシステム導入後のアクティビティは定義されているが、IT 管理者はこれらを広く適用していない。プロジェクトは、ポートフォリオとして管理され始めている。

4 管理され、測定可能である
マネジメント層は、正式かつ標準化されたプロジェクト指標と、プロジェクトの実行により得られた教訓のレビューを、プロジェクト完了後に実施することを義務付けている。プロジェクト管理は、IT 部門内に留まらず、組織全体で測定および評価されている。プロジェクト管理プロセスの改良は正式なものとされ、周知される。また、プロジェクトチームのメンバーに対して改良点に関する研修が実施されている。IT マネジメント層は、役割、責任、およびスタッフの成果基準が文書化されたプロジェクト組織構造を導入している。各工程における成果の評価基準が確立されている。価値およびリスクは、プロジェクトの開始前、進行中、および完了後の各段階で測定、管理されている。プロジェクトは、ITに特化した達成目標のみに限らず、組織の達成目標にも次第に対応するようになっている。プロジェクトに対し、利害関係者に加え、マネジメント層のスポンサーから強力かつ積極的な支援を得ている。プロジェクト管理に関する適切な研修が、プロジェクトマネジメントオフィスおよびIT部門全体のスタッフを対象として計画されている。

5 最適化
プロジェクトおよびプログラムのライフサイクル全体にわたる実績のある方法論が導入および徹底運用され、組織全体の文化に融合されている。プロジェクト管理のベストプラクティスを特定し、これを仕組みとして定着させる継続的なイニシアチブが導入されている。開発および運用プロジェクトの資源調達のための IT 戦略が定義および導入されている。統合されたプロジェクトマネジメントオフィスが、プロジェクトおよびプログラムの発足から完了後にいたるまで、すべての責任を担っている。組織レベルでプログラムおよびプロジェクトを計画することにより、戦略的イニシアチブを支えるため、ユーザおよびIT資源が最大限に活用されることを確実にしている。

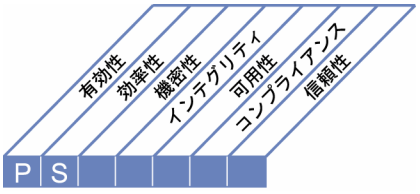
調達と導入

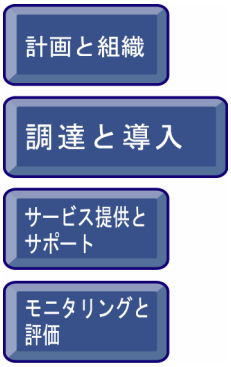
AI1 コンピュータ化対応策の明確化
AI2 アプリケーションソフトウェアの調達と保守
AI3 技術インフラストラクチャの調達と保守
AI4 運用と利用の促進
AI5 IT 資源の調達
AI6 変更管理
AI7 ソリューションおよびその変更の導入と認定

コントロール目標 －概要－

AI1 コンピュータ化対応策の明確化

新しいアプリケーションや機能を必要とする場合は、実際の調達または構築の前に、それらがビジネス要件を効果的かつ効率的なアプローチで確実に満たすものであるか分析する必要がある。この分析のプロセスには、ニーズの定義、代替となる調達元の検討、技術的および経済的実現性の見直し、リスク分析および費用対効果分析、アプリケーションを「開発」するか「購入」するかの最終決定が含まれる。これらすべての手続を踏むことにより、ソリューションの実施および導入費用が最小限に抑えられ、ビジネス目標の達成を確実に支援できるようになる。





IT プロセス: コンピュータ化対応策の明確化のコントロール目標は、

ビジネスの機能的要件およびコントロール要件を、効果的かつ効率的なシステムソリューションによって実現することを、**ビジネス要件**とし、

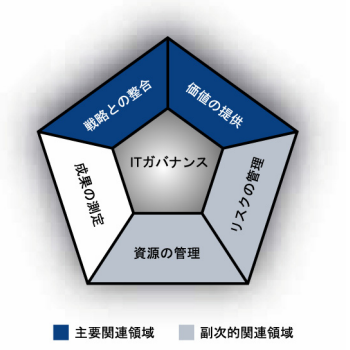
重点をおくべきコントロールは、技術的に実現可能で費用効率に優れたソリューションを明確にすることである。

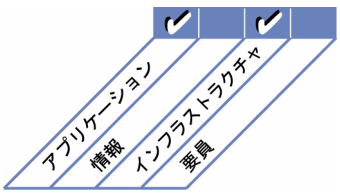
実現するための手段は、次の 3 項目である。

- ビジネス要件および技術的要件の定義
- 開発標準で定義されている実現可能性調査の実施
- 要件および実現可能性調査結果の承認(または否認)

その成果の測定指標は、次の 3 項目である。

- 誤った実現可能性見通しを立てた結果、見込まれた成果を達成できなかったプロジェクトの数
- ビジネスプロセスオーナが承認した実現可能性調査の割合
- 提供された機能に満足したユーザの割合





コントロール目標 －詳細－

AI1 コンピュータ化対応策の明確化

AI1.1 ビジネスの機能的および技術的要件の定義と保守

IT 関連の投資プログラムで期待される成果を得るために必要な、すべての案件についてビジネスの機能的および技術的な要件を特定し、優先順位を決定して、承認する。このとき、要件に対する承認基準が定義されている必要がある。これらの案件には、企業のビジネスの性質、ビジネスプロセス、要員のスキルと能力、組織構造、および実現技術に求められるあらゆる変更が含まれる。

要件では、ビジネスの機能的ニーズ、企業の技術的方向性、成果、費用、信頼性、互換性、可監査性、セキュリティ、可用性と継続性、人間工学、有用性、安全性、および関連法規を考慮しなければならない。進行中のシステム調達および開発のコントロールの基礎として、ビジネス要件のインテグリティ、正確性、および通用性(currency)を確実にし、管理するためのプロセスを確立する。ビジネススポンサーが、これらの要件に対する責任を持つ必要がある。

AI1.2 リスク分析報告

要件策定に向けた組織プロセスの一環として、ビジネスプロセスに関連するリスクを特定、文書化、分析する。リスクとしては、データのインテグリティ、セキュリティ、可用性、プライバシー、法令へのコンプライアンスなどを維持できないことが考えられる。必要な内部統制対策および監査証跡を、これらの要件の一環として明確化する必要がある。

AI1.3 実現可能性調査および代替対応策の策定

要件導入の実現性を検証する実現可能性調査を実施する。この調査では、確立されたビジネス上の機能的および技術的要件を満たすソフトウェア、ハードウェア、サービス、およびスキルに関する代替ソリューションを明確にし、各ソリューションの技術的および経済的な実現可能性(見込まれる費用と便益の分析)を、IT 関連の投資プログラムと照らし合わせて評価する必要がある。実現可能性調査の実施時には、ビジネスプロセス、技術、およびスキルに対する変更などの要因の影響を評価するため、作業を繰り返す必要がある場合がある。IT 部門によるサポートの下、ビジネス部門の管理者は実現可能性および代替ソリューションを評価し、ビジネススポンサーに提案する必要がある。

AI1.4 要件および実現可能性の決定および承認

ビジネススポンサーは、あらかじめ規定された主要な段階において、ビジネスの機能的および技術的要件と実現可能性調査の報告を承認する。各要件および報告の妥当性に問題のないことが確認された後、承認が下される。ソリューションおよび調達方法の選択に関しては、ビジネススポンサーに最終決定権がある。

マネジメントガイドライン

AI1 コンピュータ化対応策の明確化

From	インプット
PO1	IT 戦略/実行計画
PO3	「技術の状態」の定期的な更新、技術標準
PO8	調達および開発標準
PO10	プロジェクトマネジメントガイドラインおよび詳細なプロジェクト計画
AI6	変更プロセスの説明
DS1	サービス・レベル・アグリーメント(SLA)
DS3	成果および能力計画(要件)

アウトプット	To						
ビジネス要件の実現可能性調査	PO2	PO5	PO7	AI2	AI3	AI4	AI5

RACI チャート

アクティビティ / 役割	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
ビジネスの機能的および技術的要件の定義			C	C	R	C	R	R		A/R	I
要件のインテグリティ/通用性を目指したプロセスの確立				C		C		C		A/R	C
ビジネスプロセスリスクの特定、文書化、および分析			A/R	R	R	R	C	R		R	C
提案されたビジネス要件の導入に関する実現可能性調査/影響評価の実施			A/R	R	R	C	C	C		R	C
提案されたソリューションにおける IT 運用便益の評価		I	R	A/R	R	I	I	I		R	
提案されたソリューションにおけるビジネス便益の評価			A/R	R		C	C	C	I	R	
要件承認プロセスの作成			C	A		C	C	C		R	C
提案されたソリューションの承認		C	A/R	R	R	C	C	C	I	R	C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- ビジネス要件および技術的要件の定義
- 開発標準で定義された実現可能性調査の実施
- 初期段階でのセキュリティおよびコントロール要件の検討
- 要件および実現可能性調査結果の承認(または否認)

促進

プロセスの達成目標
- ユーザ要件を満たすソリューションの明確化
- 技術的に実現可能かつ費用効率に優れたソリューションの明確化
- 価値を最大限に拡張し、リスクを最小限に抑えることを考慮した「開発」または「購入」の決定

促進

IT の達成目標
- ビジネスの機能的要件およびコントロール要件を満足する、効果的かつ効率的なシステムソリューションを作成する方法の定義
- ビジネス戦略と整合性のとれたビジネス要件への対応

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- IT 年間計画において実現可能性調査の対象となるプロジェクトの割合
- ビジネスプロセスオーナが承認した実現可能性調査の割合

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 実現可能性調査の精度に満足した利害関係者の割合
- 実現可能性調査以降、実際の導入までの便益定義の変更度合い
- アーキテクチャと整合性のないアプリケーションポートフォリオの割合
- 期間内および予算内で実施された実現可能性調査の割合

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 不的確な実現可能性予測を行った結果、見込まれた成果を達成できなかったプロジェクトの数
- 提供された機能に満足したユーザの割合

成熟度モデル

AI1 コンピュータ化対応策の明確化

「ビジネスの機能的要件およびコントロール要件を満足する、効果的かつ効率的なシステムソリューションを作成する方法を定義する。」という IT に対するビジネス要件を満たす上で、「コンピュータ化対応策の明確化」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
システム、サービス、インフラストラクチャ、ソフトウェア、データ等にかかわるソリューションを、組織が開発、導入、改善するための機能面や運用面の要件を明確化する必要性を認識していない。また、当該ビジネスに潜在的に関連する技術的ソリューションの可用性についても十分に把握していない。

1 初期/その場対応
要件を定義し、技術的ソリューションを明確にする必要性があると認識している。個々のグループがニーズについて非公式に話し合い、要件について文書化されることもある。ただし、ソリューションは、各個人により、限定されたマーケット情報に基づいて、あるいはベンダーからの提案に応じて認識されるのみである。利用可能な技術についての体系的な調査や分析はほとんど行われていない。

2 再現性はあるが直感的
IT ソリューションを明確化するための何らかの直感的なアプローチはあるものの、その方法は部門間で異なる。ソリューションは IT 部門内のみの経験や知識に基づいて特定されており、正式なソリューションは無い。各プロジェクトの成功の可否は、少数の主担当者の力量に左右される。文書の質および意思決定の手法には、顕著なばらつきが見られる。要件の定義や技術的ソリューションの明確化には、体系化されていないアプローチが用いられる。

3 定められたプロセスがある
IT ソリューションの決定について、体系化された明確なアプローチが確立されている。IT ソリューション決定のアプローチでは、ビジネス要件またはユーザ要件、技術的機会、経済的な実現可能性、リスク評価、およびその他の要素について評価された、代替案の検討が求められる。IT ソリューション決定のプロセスは、関与するスタッフ個人の判断、投入した管理時間、当初のビジネス要件の優先順位や規模などの要素に基づいて、一部のプロジェクトに適用されている。体系化されたアプローチにより、要件の定義や IT ソリューションの明確化が行われている。

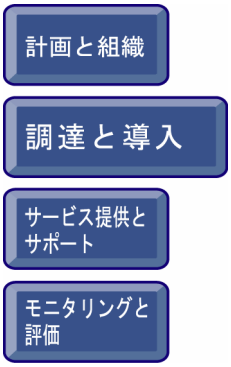
4 管理され、測定可能である
IT ソリューションの明確化と評価のための方法論が確立されており、大半のプロジェクトでその方法論が使用されている。プロジェクト関連文書の質は高く、各段階で適切な承認が行われている。要件が十分に明確化されており、事前に定義された体系に沿っている。代替ソリューションが費用と便益の分析も含めて検討されている。方法論は明確に定義されて周知されており、測定可能である。IT ソリューションの明確化および評価において、IT 管理部門とビジネス部門間の連携が明確に定義されている。

5 最適化
IT ソリューションの明確化および評価に関する方法論において、継続的な改善が実施されている。調達と導入に関する方法論には、大規模プロジェクト/小規模プロジェクトのいずれにも対応できる柔軟性がある。方法論は、技術的ソリューションに関する参考資料を含む、社内外の知識データベースによりサポートされている。方法論自体が、運用と保守の効率化を図るために事前に定義された体系に従って文書化されている。競争優位性の確保、ビジネスプロセスの再構成の促進、全体的な効率向上を図るため、技術利用の新たな機会の検討が頻繁になされる。仮に、技術またはビジネスの機能的要件の代替案を検討することなく IT ソリューションが承認された場合には、マネジメント層がこれを識別し、是正が可能である。

コントロール目標 －概要－

AI2 アプリケーションソフトウェアの調達と保守

アプリケーションは、ビジネス要件に沿った形で利用可能になっている必要がある。このプロセスには、アプリケーションの設計、業務処理統制とセキュリティ要件の適切な組み込み、および各種標準に準拠した実際の設計と構成が含まれる。このプロセスにより、組織は自動化された適切なアプリケーションを利用して、ビジネス運営を的確に支援できる。



IT プロセス: アプリケーションソフトウェアの調達と保守のコントロール目標は、

適切な時期に適正な費用で、ビジネス要件に沿った形でのアプリケーションの利用を可能にすることを、**ビジネス要件**とし、

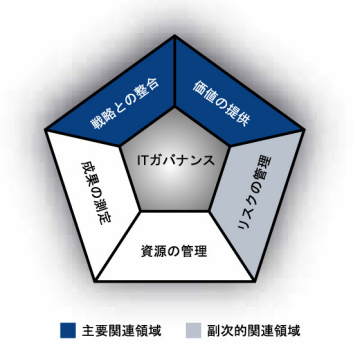
重点をおくべきコントロールは、タイムリーかつ費用効率に優れた開発プロセスの確立することである。

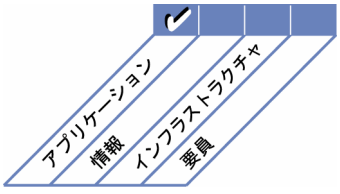
実現するための手段は、次の 3 項目である。

- ビジネス要件を設計仕様に反映すること
- 修正時の開発標準へのコンプライアンス
- 開発、テスト、および運用に関する活動の分離

その成果の測定指標は、次の 2 項目である。

- 大幅なダウンタイムの原因となった、アプリケーションごとの本番環境での重大問題発生件数
- 提供された機能に満足しているユーザの割合





コントロール目標 －詳細－

AI2 アプリケーションソフトウェアの調達と保守

AI2.1 概要設計
組織の技術的方向性や情報アーキテクチャを考慮の上、ビジネス要件をソフトウェア開発の概要設計仕様に反映させる。さらにこの概要設計がビジネス要件に確実に対応していることを踏まえ、設計仕様への承認を得る。

AI2.2 詳細設計
詳細設計およびソフトウェアアプリケーションの技術的要件を策定する。このとき、要件の受け入れ基準も定義する。この要件が、概要設計に確実に対応していることを踏まえ、要件への承認を得る。検討すべき項目として、インプット要件の定義と文書化、インターフェース定義、ユーザインターフェース、ソースデータの収集設計、プログラム仕様、ファイル要件の定義と文書化、処理要件、アウトプット要件の定義、コントロールと可監査性、セキュリティと可用性、およびテストなどの事項も適宜考慮する必要がある。開発または保守の際に重大な技術的矛盾または論理的矛盾が生じた場合は、評価を再度実施する。

AI2.3 業務処理統制および可監査性
ビジネスコントロールが業務処理統制に適切に反映され、それにより、処理が正確、完全かつタイムリーとなり、承認され監査可能になることが必要である。特に検討すべき項目として、認可方法、情報のインテグリティ、アクセスコントロール、バックアップ、および監査証跡の記録方法が挙げられる。

AI2.4 アプリケーションのセキュリティおよび可用性
サービスプロバイダが現行のビジネス要件を満たし、継続的に請負契約とサービス・レベル・アグリーメントを厳守しており、その成果に市場の状況および他のサービスプロバイダと比較した場合の優位性があることを確認するため、サービス提供状況のモニタリングプロセスを確立する。

AI2.5 調達したアプリケーションソフトウェアの構成および導入
調達したアプリケーションを、構成、受け入れ、およびテストの手続によりカスタマイズし、導入する。検討すべき項目として、契約条項に照らし合わせた検証、組織の情報アーキテクチャ、既存アプリケーション、既存アプリケーションとデータベースシステムとの相互運用性、システムパフォーマンスの効率性、文書およびユーザマニュアルの作成、統合計画およびシステムテスト計画などが挙げられる。

AI2.6 既存システムの大幅なアップグレード
現行の設計や機能に多大な影響を及ぼす大幅な変更を既存システムに加える場合、新規システムの開発の場合と同様の開発プロセスに従う。検討すべき項目として、影響分析、費用/便益の調整、要件の管理などが挙げられる。

AI2.7 アプリケーションソフトウェアの開発
アプリケーションが、確実に設計仕様、開発標準と文書化標準、および品質要件に従って開発されるようにする。アプリケーションソフトウェア開発プロセスの主要な各段階において、機能レビュー、パフォーマンスレビュー、品質レビューで問題がないことを確認し、承認する。検討すべき項目として、設計仕様がビジネス要件、機能的要件、および技術的要件を満たしていることの承認、変更要求の承認、アプリケーションソフトウェアが本番環境に適合し、また移行可能であることの確認などが挙げられる。さらに、サードパーティが開発したアプリケーションソフトウェアに関して、法律上および契約上のすべての側面が、確実に識別され、対応されるようにする。

AI2.8 ソフトウェアの品質保証に
要件定義および組織の品質に関するポリシーと手続で規定された品質を確保するために、ソフトウェア品質保証計画を策定、提供し、実施する。品質保証計画で検討すべき項目として、品質基準の規定、および検査、ウォークスルー、テストを含む検証と確認のプロセスなどが挙げられる。

AI2.9 アプリケーション要件の管理
設計、開発、導入の際に、個々の要件(否認されたすべての要件を含む)の状況が確実に追跡され、要件への変更が、確立された変更管理プロセスを経て確実に承認されるようにする。

AI2.10 アプリケーションソフトウェアの保守
ソフトウェアアプリケーションの保守およびリリースに関する戦略と計画を策定する。検討すべき項目として、リリースの計画とコントロール、資源調達計画、バグ修正と不具合修正、小規模な機能拡張、文書の改訂、緊急変更、他のアプリケーションやインフラストラクチャとの相互依存性、アップグレード戦略、サポートやアップグレードなどの契約条件、そしてビジネス上の必要性、リスク、およびセキュリティ要件に対する定期的なレビューなどが挙げられる。

マネジメントガイドライン

AI2 アプリケーションソフトウェアの調達と保守

From	インプット
PO2	データディクショナリ、データ分類スキーム、最適化されたビジネスシステム計画
PO3	「技術の状態」の定期的な更新
PO5	費用/便益報告書
PO8	調達標準と開発標準
PO10	プロジェクトマネジメントガイドライン、詳細なプロジェクト計画
AI1	ビジネス要件の実現可能性調査
AI6	変更プロセスの説明

アウトプット	To						
アプリケーションセキュリティのコントロールの詳細	DS5						
アプリケーションおよびパッケージソフトウェアの知識	AI4						
調達の決定	AI5						
当初計画されたサービス・レベル・アグリーメント(SLA)	DS1						
可用性、継続性、および回復仕様	DS3	DS4					

RACI チャート

アクティビティ ＼ 担当	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス、監査、リスク、セキュリティ
ビジネス要件の概要設計仕様への変換					C		C	A/R		R	C
詳細設計およびソフトウェアアプリケーションの技術的要件の策定				I	C	C	C	A/R		R	C
設計における業務処理統制の組み込み					R	C		A/R		R	R
調達した自動化機能のカスタマイズおよび導入					C	C		A/R		R	C
アプリケーション開発プロセスの管理に関する正式化された方法論およびプロセスの策定				C		C	C	A	C	R	C
プロジェクトのソフトウェア品質保証計画の策定					I		C	R		A/R	C
アプリケーション要件の追跡および管理								R		A/R	
ソフトウェアアプリケーションの保守計画の策定				C		C		A/R		C	

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- ビジネス要件の設計仕様への反映
- 修正時の開発標準へのコンプライアンス
- ビジネスとの関連性に基づいた要件の優先順位付け
- 開発、テスト、および運用に関する職務分離
- 既存技術への投資の促進

プロセスの達成目標
- 定義されたビジネス要件を適正な費用で満たすアプリケーションの調達と保守
- IT 戦略および IT アーキテクチャに沿ったアプリケーションの調達と保守
- 開発プロセスがタイムリーであり、費用効率が高いことの保証

IT の達成目標
- ビジネスの機能的要件およびコントロール要件を効果的かつ効率的なシステムソリューションによって実現する方法の定義
- 統合および標準化されたアプリケーションシステムの調達と保守

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- ソフトウェア品質保証計画が策定および実施されたアプリケーションソフトウェアプロジェクトの割合
- 開発標準へのコンプライアンスが適切にレビューおよび承認されたアプリケーションソフトウェアプロジェクトの割合
- ファンクションポイントやソースコード行数などの測定指標を基に計算された、機能提供までに要する平均時間
- ファンクションポイントやソースコード行数などの測定指標を基に計算された、機能提供までの平均プログラミング作業量

促進

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 予定された期間内および予算内で実施された開発プロジェクトの割合
- 既存アプリケーションの保守に費やされた開発作業量の割合
- 大幅なダウンタイムの原因となった、アプリケーションごとの本番環境での重大問題発生件数
- 月次報告された不具合の件数(ファンクションポイントあたり)

促進

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 所定の期間内にビジネス上の変化をもたらしたプロジェクトの割合
- 低品質のアプリケーション設計または開発により、規定の便益を達成できなかったプロジェクトの数
- 提供された機能に満足しているユーザの割合

成熟度モデル

AI2 アプリケーションソフトウェアの調達と保守

「適切な時期に適正な費用で、ビジネス要件に沿った形でアプリケーションを利用可能にする。」というITに対するビジネス要件を満たす上で、「アプリケーションソフトウェアの調達と保守」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
アプリケーションを設計し、仕様を定めるためのプロセスがない。アプリケーションは通常、ベンダーからの提案やブランドの認知度、あるいはIT部門の特定の製品に対する習熟度に基づいて調達されており、実際の要件はほとんどまたは一切考慮されていない。

1 初期/その場対応
アプリケーションの調達と保守に関するプロセスが必要であるという認識は存在する。アプリケーションソフトウェアの調達と保守のためのアプローチはプロジェクトごとに異なる。特定のビジネス要件に対してさまざまなソリューションが個別に適用される傾向があり、保守やサポートの非効率化が生じている。アプリケーションソフトウェアの設計または調達に際し、アプリケーションのセキュリティや可用性についてほとんど考慮されていない。

2 再現性はあるが直感的
アプリケーションの調達と保守に関して、IT 部門内のノウハウに基づいたさまざまな類似プロセスが存在する。 適正なアプリケーションの導入は、社内のスキルおよびIT部門の経験値に大きく依存している。保守に関する問題も多く、知識を持つ社内要員を失った場合の影響は大きい。アプリケーションソフトウェアの設計または調達に際し、アプリケーションのセキュリティや可用性についてほとんど考慮されていない。

3 定められたプロセスがある
アプリケーションソフトウェアの調達と保守に関して、明確に定義され、概ね周知されているプロセスが存在する。このプロセスは、IT戦略やビジネス戦略と整合されている。文書化されたプロセスを複数の異なるアプリケーションやプロジェクトに一貫して適用しようとする試みがある。規定された方法論は、概して柔軟性がなく、あらゆる場面での適用が難しいため、手続が省略される傾向がある。保守についてアクティビティが計画、予定、および調整されている。

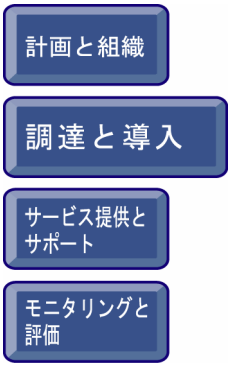
4 管理され、測定可能である
正式な、十分に周知された方法論があり、設計および仕様決定プロセス、調達基準、テストプロセス、および文書化する際の要件が組み込まれている。すべての手続が確実に遵守され、手続からの逸脱についてもすべて承認されるようにするための、文書化および合意された承認体系が存在する。実践基準および手続に十分な改良が加えられており、組織への十分な適合性が確保されている。これらは全社員によって使用され、ほとんどのアプリケーション要件に適用可能である。

5 最適化
アプリケーションソフトウェアの調達と保守の実践基準は、策定されたプロセスと整合が図られている。コンポーネントを基本としたアプローチが採用されており、事前定義および標準化されたアプリケーションがビジネス上の必要性に適合している。このアプローチは全社的に採用されている。調達と保守の方法論は十分に改良され、迅速な展開が可能である。これにより、変化するビジネス要件に敏感に反応し、柔軟な対応が可能である。アプリケーションソフトウェアの調達と導入の方法論に対して継続的な改善が図られており、その方法論は参考資料やベストプラクティスを含む、社内外の知識データベースにより支援されている。方法論が事前に定められた体系により文書化されており、運用と保守作業の効率化が図られている。

コントロール目標 －概要－

AI3 技術インフラストラクチャの調達と保守

組織は、技術インフラストラクチャの調達、導入、およびアップグレードに関するプロセスを策定する必要がある。これを実現するには、合意された技術戦略に基づいてインフラストラクチャを調達、保守、および保護するためのアプローチを計画し、開発環境とテスト環境を用意する必要がある。この結果、ビジネスアプリケーションに対する継続的な技術的サポートが確保される。



IT プロセス: 技術インフラストラクチャの調達と保守のコントロール目標は、

統合および標準化された IT インフラストラクチャの調達と保守を、**ビジネス要件**とし、

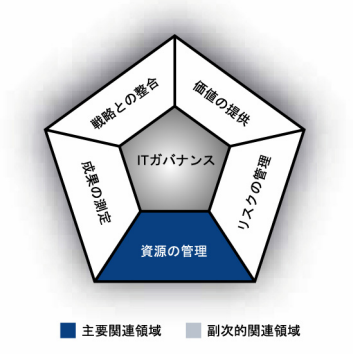
重点をおくべきコントロールは、定義された IT アーキテクチャおよび技術標準に合致する、ビジネスアプリケーションのための適切なプラットフォームを提供することである。

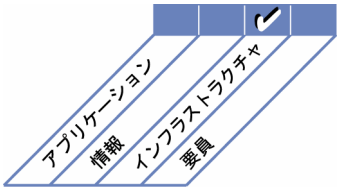
実現するための手段は、次の 3 項目である。

- 技術インフラストラクチャ計画と整合性のある技術調達計画の策定
- インフラストラクチャの保守の計画
- 内部統制、セキュリティ、および可監査性の測定指標の導入

その成果の測定指標は、次の 3 項目である。

- 定義された IT アーキテクチャおよび技術標準に合致しないプラットフォームの割合
- 陳腐化した(または、すぐに陳腐化する)インフラストラクチャによりサポートされている重要なビジネスプロセスの数
- サポート対象外(または近い将来サポート対象外になる)インフラストラクチャコンポーネントの数





コントロール目標 －詳細－

AI3 技術インフラストラクチャの調達と保守

AI3.1 技術インフラストラクチャの調達計画
確立された機能面および技術面でのビジネス要件を満たし、組織の技術的方向性と一致する技術インフラストラクチャの調達、導入、および保守の計画を策定する。この計画の策定においては、今後の技術的能力の追加導入に対する柔軟性、移行にかかる費用、技術上のリスク、および技術的なアップグレードに対する投資の使用期間を考慮する必要がある。新たな技術的能力の導入に際しては、複雑性に起因する費用、およびベンダーと製品の実用性について評価する。

AI3.2 インフラストラクチャ資源の保護と可用性
ハードウェアおよびインフラストラクチャソフトウェアの構成、統合、および保守の際に、内部統制、セキュリティ、および可監査性の測定指標を導入することで、資源を保護し、可用性およびインテグリティを確保する。機密性の高いインフラストラクチャコンポーネントの使用上の責任を明確に定義し、インフラストラクチャコンポーネントの開発および統合にあたる担当者に周知する必要がある。これらのコンポーネントの使用状況はすべてモニタリングおよび評価されなければならない。

AI3.3 インフラストラクチャの保守
インフラストラクチャ保守の戦略および計画を策定し、変更が組織の変更管理手続に従って確実にコントロールされるようにする。保守には、ビジネス上の必要性、パッチ管理およびアップグレード戦略、リスク、脆弱性の評価、およびセキュリティ要件に関する定期的なレビューを組み込む。

AI3.4 実現可能性テスト環境
調達と開発プロセスの初期段階において、アプリケーションやインフラストラクチャの効果的かつ効率的な実現可能性テストおよび統合テストをサポートする開発環境とテスト環境を構築する。機能性、ハードウェア構成とソフトウェア構成、統合テストとパフォーマンステスト、異なる環境間での移行、バージョンコントロール、テストデータとツール、およびセキュリティについて考慮する。

マネジメントガイドライン

AI3 技術インフラストラクチャの調達と保守

From	インプット
PO3	技術インフラストラクチャ計画、標準と機会、「技術の状態」の定期的な更新
PO8	調達標準と開発標準
PO10	プロジェクトマネジメントガイドラインおよび詳細なプロジェクト計画
AI1	ビジネス要件の実現可能性調査
AI6	変更プロセスの説明
DS3	成果および能力計画(要件)

アウトプット	To
調達の決定	AI5
テスト/インストール対象の構成済みシステム	AI7
物理的環境要件	DS12
技術標準の更新	PO3
システムモニタリング要件	DS3
インフラストラクチャに関する知識	AI4
当初計画されたオペレーショナル・レベル・アグリーメント(OLA)	DS1

RACI チャート

アクティビティ / 役割	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
調達手続/プロセスの定義		C		A		C	C	C	R		I
必要なインフラストラクチャの調達に関する(承認された)ベンダーとの交渉および調達		C/I		A	I	R	C	C	R		I
インフラストラクチャの保守に関する戦略および計画の策定				A		R	R	R	C		
インフラストラクチャコンポーネントを構成				A		R	C				I

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- 技術インフラストラクチャ計画と整合性がある技術調達計画の策定
- インフラストラクチャの保守の計画
- 開発環境およびテスト環境のインフラストラクチャの整備
- 内部統制、セキュリティ、および可監査性の測定指標の導入

プロセスの達成目標
- 定義された IT アーキテクチャおよび技術標準に合致する、ビジネスアプリケーションのための適切なプラットフォームの提供
- 信頼性の高い安全な IT インフラストラクチャの整備

IT の達成目標
- 統合および標準化された IT インフラストラクチャの調達と保守
- IT インフラストラクチャ、資源、および能力の最適化
- 変化に迅速に対応できる IT の構築

促進

促進

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- インフラストラクチャコンポーネントに加えられた緊急変更の回数およびタイプ
- 未解決の調達要求の数
- インフラストラクチャコンポーネントの構成に要した平均時間

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 定義された IT アーキテクチャおよび技術標準に合致しないプラットフォームの割合
- 社内における部門ごとに異なる技術プラットフォームの数
- 調達プロセス外で調達されたインフラストラクチャコンポーネントの割合
- サポート対象外(または近い将来サポート対象外になる)インフラストラクチャコンポーネントの数

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 陳腐化した(または、すぐに陳腐化する)インフラストラクチャによりサポートされている重要なビジネスプロセスの数

成熟度モデル

AI3 技術インフラストラクチャの調達と保守

「統合および標準化された IT インフラストラクチャの調達と保守。」という IT に対するビジネス要件を満たす上で、「技術インフラストラクチャの調達と保守」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
技術インフラストラクチャの管理が、対応すべき重要な問題であると認識されていない。

1 初期/その場対応
新たなアプリケーションが導入されるごとにインフラストラクチャに変更が加えられており、全体的な計画が存在しない。IT インフラストラクチャが重要であるという認識はあるが、一貫した総合的なアプローチは存在しない。保守活動は、短期的な必要性に応じて実施されている。本番環境とテスト環境が切り離されていない。

2 再現性はあるが直感的
IT インフラストラクチャを調達および保守する際の戦術的なアプローチに一貫性がある。ただし、IT インフラストラクチャの調達と保守は、策定された戦略に基づいておらず、サポートすべきビジネスアプリケーションの必要性も考慮されていない。いくつかの正式な実践基準により、IT インフラストラクチャの重要性は理解されている。予定されている保守もあるが、すべて完全に予定および調整されているわけではない。一部の環境では、独立したテスト環境が存在している。

3 定められたプロセスがある
IT インフラストラクチャの調達と保守について、明確に定義され、概ね周知されたプロセスが存在する。このプロセスは、重要なビジネスアプリケーションの必要性に対応しており、IT 戦略およびビジネス戦略と整合されているが、一貫して適用されているわけではない。保守は計画、予定化、および調整されている。テスト環境と本番環境が完全に切り離されている。

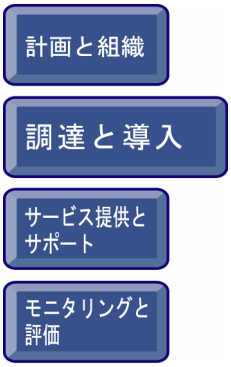
4 管理され、測定可能である
技術インフラストラクチャの調達と保守のプロセスは、ほとんどの状況下で適正に機能するレベルにまで整備されており、一貫して適用されている。また、プロセスでは、技術インフラストラクチャの再利用性に焦点が当てられている。IT インフラストラクチャは、ビジネスアプリケーションを十分にサポートしている。プロセスは適切に体系化されており、変化を先取りしている。拡張性、柔軟性、および統合性の目標レベルに到達するための費用と準備期間が、一部最適化されている。

5 最適化
技術インフラストラクチャの調達と保守のプロセスは事前対応的であり、重要なビジネスアプリケーションおよび技術アーキテクチャとの厳密な整合性が確保されている。組織は技術的ソリューションに関する優れた実践基準に倣い、最新のプラットフォーム開発および管理ツールについて把握している。インフラストラクチャコンポーネントの合理化と標準化、そして自動化ツールの利用により費用が削減されている。技術に対する高い見識があり、アウトソーシングも含め、事前対応的にパフォーマンスを改善する最適な方法を見出すことが可能である。IT インフラストラクチャの整備は、IT の活用を促進する主要動因として認識されている。

コントロール目標 －概要－

AI4 運用と利用の促進

新たなシステムに関する知識を利用可能にする必要がある。このプロセスでは、ユーザおよびIT部門のための文書や資料を作成し、アプリケーションとインフラストラクチャの適切な使用と運用を確保するための研修を実施する。



IT プロセス: 運用と利用の促進のコントロール目標は、

提供サービスとサービスレベルに対するエンドユーザの満足を確保し、アプリケーションおよび技術的ソリューションをビジネスプロセスにシームレスに統合することを、**ビジネス要件**とし、

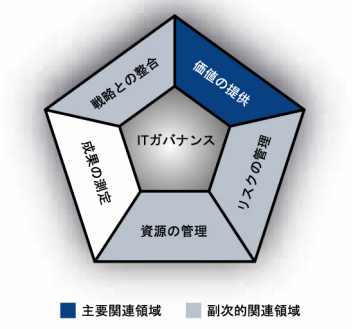
重点をおくべきコントロールは、効果的なユーザマニュアル、運用マニュアル、および研修資料を提供し、システムの正しい運用および使用に必要な知識を移転することである。

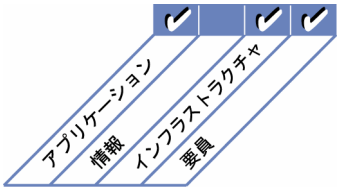
実現するための手段は、次の 3 項目である。

- 知識を移転するための文書の作成および提供
- ユーザ、ビジネス部門の管理者、サポートスタッフ、運用スタッフに対する周知および研修
- 研修資料の作成

その成果の測定指標は、次の 3 項目である。

- IT 関連の手続がビジネスプロセスにシームレスに統合されているアプリケーションの数
- アプリケーションの研修およびサポート資料に満足しているビジネスオーナの割合
- 適切なユーザ研修および運用サポート研修が整備されているアプリケーションの数





コントロール目標 －詳細－

AI4 運用と利用の促進

AI4.1 運用上のソリューションの計画
技術的側面、運用能力、必要なサービスレベルのすべてを特定および文書化する計画を策定する。これにより、自動化されたシステムやインフラストラクチャの導入またはアップグレードを実施して、すべての利害関係者が管理手続、ユーザ手続、および運用手続の作成に関してタイムリーに責任を果たすことができるようにする。

AI4.2 ビジネス部門の管理者への知識の移転
ビジネス部門の管理者に知識を移転する。これにより、ビジネス部門の管理者がシステムおよびデータのオーナシップを担い、サービスの提供と品質、内部統制、およびアプリケーション管理プロセスに関する責任を果たすことができるようにする。移転させる知識として、アクセスの承認、特権の管理、職務の分離、自動化されたビジネスコントロール、バックアップ/復元、物理的セキュリティ、およびソース文書のアーカイブなどに関する知識が含まれる必要がある。

AI4.3 エンドユーザへの知識の移転
エンドユーザに知識とスキルを移転させる。これにより、エンドユーザが効果的かつ効率的にアプリケーションシステムを使用し、ビジネスプロセスをサポートできるようにする。移転させる知識として、入門研修と継続研修およびスキル開発に対応する研修計画の策定、研修資料、ユーザマニュアル、手続マニュアル、オンラインヘルプ、サービスデスクサポート、主要ユーザの特定、評価などに関する知識が含まれる必要がある。

AI4.4 運用スタッフおよびサポートスタッフへの知識の移転
運用スタッフおよび技術サポートスタッフに知識とスキルを移転させる。これにより、彼らが必要なサービスレベルに従って効果的かつ効率的にアプリケーションシステムおよび関連インフラストラクチャを提供、サポート、および保守できるようにする。移転させる知識として、入門研修と継続研修およびスキル開発、研修資料、運用マニュアル、手続マニュアル、サービスデスクのシナリオなどに関する知識が含まれる必要がある。

マネジメントガイドライン

AI4 運用と利用の促進

From	インプット
PO10	プロジェクトマネジメントガイドラインおよび詳細なプロジェクト計画
AI1	ビジネス要件の実現可能性調査
AI2	アプリケーションおよびパッケージソフトウェアに関する知識
AI3	インフラストラクチャに関する知識
AI7	既知の確認済みエラー
DS7	必要な文書の更新

アウトプット	To						
ユーザマニュアル、運用マニュアル、サポートマニュアル、技術マニュアル、および管理マニュアル	AI7	DS4	DS8	DS9	DS11	DS13	
ソリューションの導入のための知識移転要件	DS7						
研修資料	DS7						

RACI チャート

アクティビティ ＼ 役割	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ	導入チーム	研修部門
ソリューションを運用可能にする戦略の策定				A	A	R		R			I	R	C
知識移転の方法論の策定				C	A							C	R
エンドユーザ向けの手続マニュアルの作成					A/R			R			C	C	
運用スタッフおよびサポートスタッフ向けの技術サポート文書の作成						A/R		C			C		
研修の整備と実施					A	A		R					R
研修結果の評価と必要に応じた文書の改訂					A	A						R	R

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- 知識を移転するための文書の作成および提供
- ユーザ、ビジネス部門の管理者、サポートスタッフ、運用スタッフに対する周知および研修
- 研修資料の作成

促進

プロセスの達成目標
- アプリケーションと技術的ソリューションに関する効果的なユーザマニュアル、運用マニュアル、および研修資料の提供
- 適切なシステム運用に必要な知識の移転

促進

IT の達成目標
- アプリケーションおよび技術的ソリューションの適切な利用と成果達成の確保
- 提供サービスとサービスレベルに対するエンドユーザの満足の確保
- アプリケーションおよび技術的ソリューションのビジネスプロセスへのシームレスな統合
- ソリューションとサービスの提供における不備と手戻りの必要性の削減

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 各アプリケーションの研修に対する、ユーザおよび運用スタッフの出席レベル
- 研修、手続、および各種資料の変更から、実際の更新までに要する時間
- ユーザマニュアルと運用マニュアルの利用可能性、インテグリティ、および正確性
- 適切なユーザおよび運用サポート研修が整備されているアプリケーションの数

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- ユーザマニュアル、運用マニュアル、および研修の不備に起因するインシデントの件数
- サービスデスクへの研修に関する問い合わせ件数
- ユーザ手続および運用手続に関連する研修と各種資料に対する満足度
- ユーザマニュアル、運用手続、および研修資料の作成/保守費用の削減額

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- IT 関連の手続がビジネスプロセスにシームレスに統合されているアプリケーションの数
- アプリケーションの研修およびサポート資料に満足しているビジネスオーナの割合

成熟度モデル

AI4 運用と利用の促進

「提供サービスとサービスレベルに対するエンドユーザの満足を確保し、アプリケーションおよび技術的ソリューションをビジネスプロセスにシームレスに統合する。」という IT に対するビジネス要件を満たす上で、「運用と利用の促進」のプロセスにおける管理の成熟度は、以下のとおりである。

0 不在
ユーザマニュアル、運用マニュアル、および研修資料の作成に関するプロセスがまったく存在しない。購入製品に同梱された資料のみ存在する。

1 初期/その場対応
プロセスの文書化の必要性が認識されている。文書は時折作成され、一貫性のない少数の限られたグループに配布されている。文書および手続の大部分が更新されていない。研修資料は 1 回限りの使用のために作成される傾向があり、品質にばらつきがある。異なるシステム間および部門間で手続がほとんど統合されていない。研修プログラムの策定において、各部門の意向が組み込まれていない。

2 再現性はあるが直感的
手続や文書の作成において類似したアプローチが使用されているが、体系化されたアプローチやフレームワークに基づいていない。ユーザ手続および運用手続の策定について、一貫したアプローチが存在しない。研修資料は個人またはプロジェクトチームごとに作成され、作成者によって品質にばらつきがある。ユーザサポートの手続や質の優劣の差が大きく、組織全体で一貫性や統合性がほとんど見られない。ビジネス部門やユーザ対象の研修プログラムが提供または促進されているが、研修の普及や提供に関する総合的な計画は存在しない。

3 定められたプロセスがある
ユーザマニュアル、運用マニュアル、および研修資料に関するフレームワークが、明確に定義および承認され、周知されている。手続は正式なライブラリで保管および保守されており、すべての利用者が必要に応じてアクセスできる。文書や手続への修正は、事後的に行われる。手続はオフラインで参照可能で、災害時でもアクセスおよび保守可能である。プロジェクト変更が、実際の手続の更新と研修資料に明確に反映されるようにするプロセスが存在する。定義されたアプローチがあるにもかかわらず、標準へのコンプライアンスを徹底するコントロールが存在しないため、実際の内容にはばらつきがある。ユーザは、非公式な形でこのプロセスに関与している。手続の策定と周知の過程で、自動化されたツールの使用が徐々に増加している。ビジネス部門とユーザ向けの研修が計画および予定化されている。

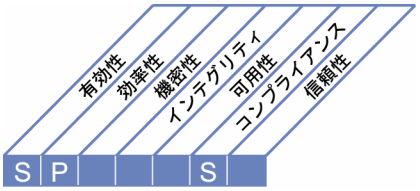
4 管理され、測定可能である
手続と研修資料の保守のためのフレームワークが定義されており、IT 管理部門がサポートしている。手続と研修マニュアルの保守に利用されるアプローチは、すべてのシステムおよび部門に適用可能であり、各プロセスをビジネスの観点から評価することが可能である。手続と研修資料が相互にリレーションシップや接点を持つように統合されている。すべてのプロセスについて標準が遵守され、手続が整備および保守されることを確実にするコントロールが存在する。継続的な改善プロセスの一環として、文書と研修に対するビジネス部門およびユーザからのフィードバックが収集され、評価されている。文書および研修資料の信頼性と可用性が、通常予測可能な高いレベルに保たれている。自動化された手続の文書化および管理に関する新たなプロセスが導入されている。自動化された手続の整備が、アプリケーションシステムの開発と徐々に統合され、一貫性とユーザアクセスが促進されている。ビジネス部門とユーザ向けに実施されている研修は、ビジネス上の必要性を臨機応変に組み込んだ内容である。IT 管理部門が、文書、研修資料、および研修プログラムの整備と実施のための指標を策定している。

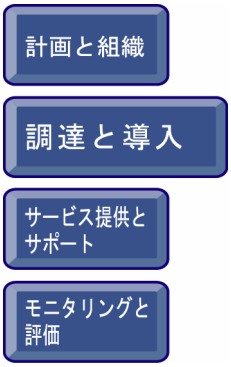
5 最適化
ユーザマニュアルと運用マニュアルの作成プロセスが、新たなツールや方法を採用することで継続的に改善されている。手続文書と研修文書は、常に進化するナレッジベースとして扱われており、最新の知識管理、ワークフロー、配布技術を用いて電子的に保守されている。これにより、資料の可用性と保守の容易性が確保されている。文書および研修資料は、組織、運用、およびソフトウェアの変更を反映し、常に最新の状態に保たれている。文書と研修資料の整備や研修プログラムの実施は、ビジネスやビジネスプロセスの定義と完全に統合されている。これにより、IT に焦点を当てた手続だけでなく、組織全体の要件に対応するものとなっている。

コントロール目標 －概要－

AI5 IT 資源の調達

要員、ハードウェア、ソフトウェア、サービスを含む IT 資源を調達する必要がある。そのためには、調達手続の策定と実施、ベンダーの選定、契約等の整備、および実際の調達が必要である。これらを行うことにより、組織はタイムリーかつ費用効率よく、必要な IT 資源をすべて確保可能になる。





IT プロセス: IT 資源の調達のコントロール目標は、

IT の費用効率およびビジネス収益性への IT の貢献度の向上を、**ビジネス要件**とし、

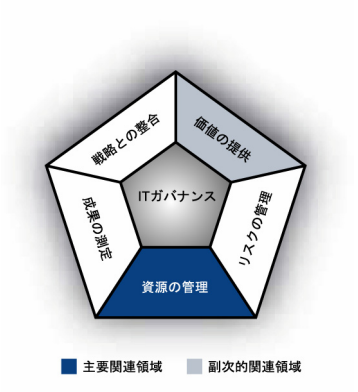
重点をおくべきコントロールは、サービス提供戦略に対応する IT スキルと、統合および標準化された IT インフラストラクチャを調達、維持し、IT 調達リスクを削減することである。

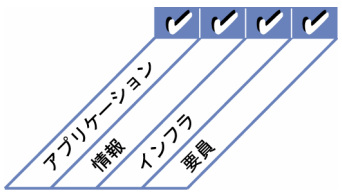
実現するための手段は、次の 3 項目である。

- 専門家による法的見地からの助言および契約に関する助言の取得
- 調達手続と標準の策定
- 策定された手続に沿った、要求されたハードウェア、ソフトウェア、およびサービスの調達

その成果の測定指標は、次の 3 項目である。

- 調達契約に関する係争の件数
- 購入費用の削減額
- サービスプロバイダに満足している主要な利害関係者の割合





コントロール目標 －詳細－

AI5 IT 資源の調達

AI5.1 調達のコントロール
IT 関連のインフラストラクチャ、設備、ハードウェア、ソフトウェア、およびサービスの調達が、ビジネス要件を確実に満たすよう、全組織の調達プロセスや調達戦略と整合性のとれた一連の手続および標準を整備し、それを遵守する。

AI5.2 サービスプロバイダとの契約の管理
すべてのサービスプロバイダに対する、契約の締結、変更、終了の手続を策定する。この手続では、少なくとも、法律、財務、組織、文書、成果、セキュリティ、知的財産、および契約の終了に関する責任と義務(罰則条項を含む)について扱う必要がある。すべての契約および契約変更について、法律の専門家のレビューを受ける必要がある。

AI5.3 サービスプロバイダの選定
持続性のある最適なサービスプロバイダを公正かつ正式な実施基準に従って選定する。要件は、サービスプロバイダ候補からの情報を基に策定し、顧客とサービスプロバイダとの間で合意されている。

AI5.4 ソフトウェアの調達
調達に関するすべての契約上の合意事項において、企業利益を確実に保護する。ソフトウェアの供給および継続的な使用にかかわるソフトウェア調達の契約条項に、すべての利害関係者の権利と義務を規定し、これを守らせる。これらの権利と義務には、知的財産の所有権とライセンス、保守、保証、調停手続、アップグレード関連条項、およびセキュリティとエスクローおよびアクセス権の目的への適合性などが含まれる。

AI5.5 開発資源の調達
調達に関するすべての契約上の合意事項において、企業利益を確実に保護する。開発資源調達の契約条項に、すべての利害関係者の権利と義務を規定し、これを守らせる。これらの権利と義務には、知的財産の所有権とライセンス、開発方法論と言語およびテストの目的への適合性、必要な成測定基準を含む品質管理プロセス、成果のレビュー、支払い基準、保証、調停手続、人材の管理、および組織のポリシーの遵守などが含まれる。

AI5.6 インフラストラクチャ、設備、および関連サービスの調達
インフラストラクチャ、設備、および関連サービスの調達の契約条項とその受入れ基準に、すべての利害関係者の権利と義務を規定し、これを守らせる。これらの権利と義務には、サービスレベル、保守手続、アクセスコントロール、セキュリティ、成果のレビュー、支払い基準、調停手続などが含まれる。

マネジメントガイドライン

AI5 IT 資源の調達

From	インプット
PO1	IT 調達戦略
PO8	調達標準
PO10	プロジェクトマネジメントガイドラインおよび詳細なプロジェクト計画
AI1	ビジネス要件の実現可能性調査
AI2-3	調達の決定
DS2	サービスプロバイダの一覧表

アウトプット	To						
サードパーティとのリレーションシップ管理要件	DS2						
調達されたアイテム	AI7						
契約等の整備	DS2						

RACI チャート

役割

アクティビティ	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
会社レベルの調達ポリシーと整合された IT 調達ポリシーおよび手続の策定	I	C		A		I	I	I	R		C
認可されたサービスプロバイダのリストの作成/保守									A/R		
提案依頼(RFP)プロセスを使用したサービスプロバイダの評価および選定	C	C		A		R		R	R	R	C
組織の利益を保護する契約の策定	R	C		A		R		R	R		C
確立された手続に従った調達				A		R		R	R		C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- 専門家による法的見地からの助言および契約に関する助言の取得
- 調達手続と標準の策定
- 策定された手続に沿った、要求されたハードウェア、ソフトウェア、およびサービスの調達

促進

プロセスの達成目標
- IT 調達リスクの削減
- IT の調達に見合う価値の取得

促進

IT の達成目標
- 統合および標準化されたアプリケーションおよび IT インフラストラクチャの調達と保守
- IT の提供戦略に対応する IT スキルの獲得と維持
- IT の費用効率およびビジネス収益性への IT の貢献度の向上

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 調達の要求から契約の締結または購入までに要する時間
- 推奨されるサービスプロバイダのリストで対応可能な調達要求の件数
- サービスプロバイダからの回答を基に改善の必要がある提案依頼(RFP)の件数
- 予定期間内に完了した調達要求の件数
- 同種類の調達商品またはサービスプロバイダの変更回数
- 提案依頼(RFP)に対する受信回答数

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 選択されたソリューションにより対処された初期要件の割合
- 現行の調達ポリシーおよび手続に従った調達の割合
- 調達商品またはサービスの単位原価の削減額

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 調達契約に関する係争の件数
- 購入費用の削減額
- サービスプロバイダに満足している主要な利害関係者の割合

成熟度モデル

AI5 IT 資源の調達

「IT の費用効率およびビジネス収益性への IT の貢献度の向上。」という IT に対するビジネス要件を満たす上で、「IT 資源の調達」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
IT 資源調達プロセスが定義されていない。組織は、タイムリーかつ費用効率に優れた方法ですべての IT 資源を確実に入手可能にするための、明確な調達ポリシーおよび手続の必要性を認識していない。

1 初期/その場対応
組織は、IT の調達を全社の調達プロセスに関連付ける、文書化されたポリシーと手続の必要性を認識している。IT 資源調達に関する契約は、正式な手続やポリシーに基づく形ではなく、プロジェクト管理者やその他の個人による専門的な判断によって策定、管理されている。企業の調達および契約の管理プロセスと IT 部門との間にはその場対応のリレーションシップしかない。調達に関する契約は、継続的にではなく、プロジェクトの終了時に管理される。

2 再現性はあるが直感的
組織として、IT 調達の基本的なポリシーと手続を保有する必要性を認識している。ポリシーと手続の一部は全社の調達プロセスに統合されている。調達プロセスは、概して大規模かつ注目度の高いプロジェクトで利用されている。IT 調達と契約管理に関する実行責任および説明責任は、個々の契約管理者の経験に基づいて規定されている。サービスプロバイダ管理とリレーションシップ管理の重要性は認識されているが、個人のイニシアチブに依存する形で実施されている。契約プロセスは、概して大規模かつ注目度の高いプロジェクトで利用されている。

3 定められたプロセスがある
マネジメント層が、IT 調達のポリシーと手続を制定している。ポリシーと手続は、全社の調達プロセスに基づいて策定されている。IT 調達の大部分が全社の調達システムに統合されている。IT 資源調達の指針となる IT 標準が存在する。IT 資源の供給者は、契約管理の観点から、組織のプロジェクト管理体系に組み込まれている。IT 部門管理者は、IT 部門全体に対して、適切な調達および契約管理の必要性を周知している。

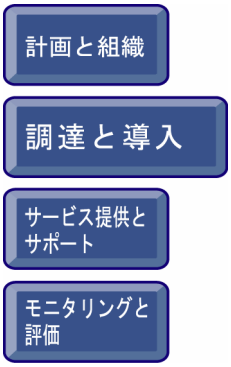
4 管理され、測定可能である
IT 調達が全社の調達システムに完全に統合されている。IT 資源調達の指針となる IT 標準が、すべての調達において適用されている。契約および調達管理に関する測定が、IT 調達の取引に関する契約および調達管理の測定が実施されている。そして、サポートするビジネス目標が報告されている。マネジメント層は通常、IT 調達ポリシーおよび手続に対する例外について認識できる。リレーションシップの戦略的な管理について整備されつつある。IT 管理部門は、成果の測定結果をレビューすることにより、すべての調達において調達プロセスおよび契約管理プロセスの遵守を徹底させている。

5 最適化
マネジメント層が、IT 調達に関する完全なプロセスを策定し、提示している。マネジメント層が、IT 調達に関するポリシーと手続の遵守を徹底させている。契約および調達管理の測定が、IT 調達の投資対効果検討書に関連する形で実施されている。長期にわたり、多くの供給者やパートナーとの間に良好なリレーションシップが構築されており、リレーションシップの質が測定およびモニタリングされている。リレーションシップは戦略的に管理されている。IT 資源調達のための IT 標準、ポリシー、および手続が戦略的に管理され、プロセスの測定結果に対応している。IT 部門管理者は、IT 部門全体に対して、適切な調達および契約管理の戦略的重要性を周知している。

コントロール目標 －概要－

AI6 変更管理

インフラストラクチャおよびアプリケーションに関連する緊急保守やパッチ適用を含む、本番環境におけるすべての変更は、コントロールされた方法で、正式に管理されなければならない。変更(手続、プロセス、システムパラメーター、およびサービスパラメーターを含む)は、変更の実施前に記録、評価、および承認されなければならず、変更の実施後には計画された成果に照らしてレビューしなければならない。これにより、本番環境の安定性やインテグリティに悪影響を及ぼすリスクを低減できる。



IT プロセス: 変更管理のコントロール目標は、

ビジネス戦略と整合性のとれたビジネス要件への対応と、ソリューションおよびサービスの提供における不備と手戻りの削減を、**ビジネス要件**とし、

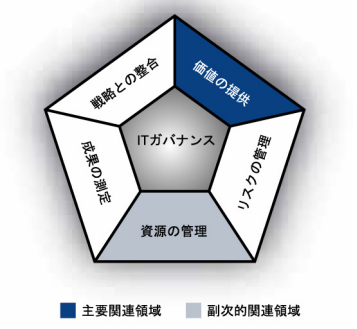
重点をおくべきコントロールは、IT インフラストラクチャ、アプリケーション、および技術的ソリューションに対するすべての変更に関する影響評価、認可、および実施をコントロールし、不完全な要求仕様に起因するエラーを最小限に抑え、未承認の変更の実施を防止することである。

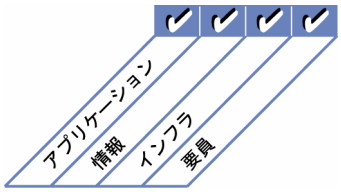
実現するための手段は、次の 3 項目である。

- 緊急変更を含む変更手続の策定および周知
- 変更の評価、優先順位付け、および承認
- 変更の状況追跡および報告

その成果の測定指標は、次の 3 項目である。

- 不正確な仕様や不完全な影響評価に起因するプロセスの中断またはデータエラーの数
- 不適切な変更仕様に起因する、アプリケーションやインフラストラクチャ関連の手戻りの量
- 正式な変更コントロールプロセスに従った変更の割合





コントロール目標 －詳細－

AI6 変更管理

AI6.1 変更の標準と手続
アプリケーション、手続、プロセス、システムパラメーターとサービスパラメーター、および基盤プラットフォームに対するすべての変更要求(保守やパッチ適用を含む)を、標準化された方法で処理できるよう、正式な変更管理手続を確立する。

AI6.2 影響評価、優先順位付け、および認可
すべての変更要求が、本番運用中のシステムや、その機能に与える影響について体系的かつ確実に評価されるようにする。この影響評価には、変更の分類および優先順位付けを含めるべきである。本番環境への移行に先立って、適切な利害関係者から変更内容について承認を得る。

AI6.3 緊急変更
規定された変更プロセスに従わない緊急変更の定義、提起、評価、および承認のプロセスを確立する。事後対応となったとしても、緊急変更の文書化およびテストを実施すべきである。

AI6.4 変更の状況追跡および報告
追跡および報告システムを構築し、アプリケーション、手続、プロセス、システムパラメーターとサービスパラメーター、および基盤プラットフォームに対する変更状況について、変更の要求元や関連する利害関係者に対し最新情報を継続的に提供する。

AI6.5 変更の終了および文書化
システムの変更を実施したときは常に、関連するシステムマニュアルやユーザマニュアル、手続などを必要に応じて更新する。変更の完全な実施を確実にするために、レビュープロセスを確立する。

マネジメントガイドライン

AI6 変更管理

From	インプット
PO1	IT プロジェクトのポートフォリオ
PO8	品質改善策
PO9	IT にかかわるリスク是正措置計画
PO10	プロジェクトマネジメントガイドラインおよび詳細なプロジェクト計画
DS3	必要な変更
DS5	必要なセキュリティ変更
DS8	サービス要求/変更要求
DS9-10	変更要求(変更の適用対象とその方法)
DS10	問題の記録

アウトプット	To						
変更プロセスの説明	AI1…AI3						
変更状況の報告	ME1						
変更の承認	AI7	DS8	DS10				

RACI チャート

役割

アクティビティ	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
変更要求の一貫した記録、評価、優先順位付けのための仕組みの策定および導入				A	I	R	C	R	C	C	C
ビジネス上の必要性に基づく変更の影響評価および優先順位付け				I	R	A/R	C	R	C	R	C
緊急変更や重要な変更の実施における、承認されたプロセスの遵守				I	I	A/R	I	R			C
変更の承認				I	C	A/R		R			
変更の関連情報の管理と周知				A	I	R	C	R	I	R	C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- 緊急変更やパッチ適用を含む変更手続の策定および周知
- 変更の評価、優先順位付け、および承認
- 計画的な変更
- 変更の状況追跡および報告

促進

プロセスの達成目標
- IT インフラストラクチャとアプリケーションへの承認された変更の実施
- IT インフラストラクチャ、アプリケーション、および技術的ソリューションへの変更による影響の評価
- 変更状況の追跡と主要な利害関係者への報告
- 不完全な要求仕様に起因するエラーを最小限に抑えること

促進

IT の達成目標
- ビジネス戦略と整合性のとれたビジネス要件への対応
- ソリューションとサービスの提供における不備と手戻りの削減
- IT サービスの中断または変更が及ぼすビジネスへの影響を最小限に抑えること
- ビジネスの機能要件やコントロール要件に対して、どのように効果的で効率的な自動化ソリューションを提供できるかを示す
- 情報および情報処理インフラストラクチャのインテグリティ維持

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 自動化ツールを使用して記録および追跡された変更の割合
- 正式な変更コントロールプロセスに従った変更の割合
- 承認された変更要求と否認された変更要求の比率
- 保守対象となっている各ビジネスアプリケーションまたはインフラストラクチャのバージョン数
- インフラストラクチャコンポーネントに対する緊急変更の回数およびタイプ
- インフラストラクチャコンポーネントに対するパッチの適用回数およびタイプ

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 不適切な変更仕様に起因するアプリケーション関連の手戻りの量
- 変更に要する時間と作業の削減額
- 全変更における緊急修正の割合
- 不適切な変更仕様に起因して、インフラストラクチャへの変更が成功しなかった割合
- 正式に追跡、報告、または承認されていない変更の数
- 未処理の変更要求の数

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 不正確な仕様や不完全な影響評価に起因するプロセスの中断またはデータエラーの数

成熟度モデル

AI6 変更管理

「ビジネス戦略と整合性のとれたビジネス要件への対応と、ソリューションおよびサービスの提供における不備と手戻りの削減。」というITに対するビジネス要件を満たす上で、「変更管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
変更管理プロセスが定義されておらず、実質的にはまったくコントロールされないまま変更を実施できる。そのような変更がIT部門とビジネス部門の運用において混乱を招く可能性があることが認識されておらず、優れた変更管理を実施することの利点についても認識されていない。

1 初期/その場対応
変更を管理し、コントロールする必要性は認識されている。実施されている活動にばらつきがあり、未承認の変更が行われる可能性が高い。変更に関する文書が存在しないか、存在しても内容が不十分である。また、システム構成に関する文書は不完全で信頼性が低い。貧弱な変更管理に起因する本番環境のサービス中断とともにエラーが発生する可能性が高い。

2 再現性はあるが直感的
非公式な変更管理プロセスが整備されており、大半の変更はこのアプローチに従って実施されている。しかし、このアプローチは体系化されておらず、未熟であり、エラーを誘発しやすい。システム構成に関する文書の正確性が一定しておらず、変更に先立って実施される計画策定と影響評価は限定的なものである。

3 定められたプロセスがある
分類、優先順位付け、緊急時の手続、変更の承認、およびリリース管理を含む正式な変更管理プロセスが整備されており、このプロセスが遵守されつつある。しかし、ワークアラウンド(回避策)が実施され、プロセスからの逸脱がしばしば発生する。エラーが依然として発生する可能性があり、未承認の変更がときどき発生する。ITにかかわる変更がビジネス運営に及ぼす影響の分析が正式に行われるようになりつつあり、新たなアプリケーションや技術の計画的な展開がサポートされている。

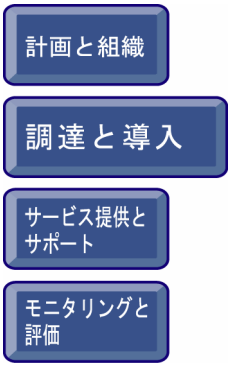
4 管理され、測定可能である
変更管理プロセスは十分整備されており、すべての変更に一貫して適用されている。マネジメント層は変更に関する例外対応は最小限に抑えられているという確信を持っている。プロセスは効率的かつ効果的であるが、確実に品質を保証するために、膨大な手作業と手動コントロールに依存している。変更適用後に発生する可能性がある問題を最小限に抑えるために、すべての変更に対する徹底した計画策定と影響評価の実施が義務付けられている。また、変更の承認プロセスも整備されている。変更は正式に追跡記録されており、変更管理マニュアルは最新かつ正確な状態に保たれている。システム構成に関する文書の内容は概ね正確である。ITの変更管理の計画策定および実施について、ビジネスプロセスの変更との統合が進められており、研修、組織改編、およびビジネスの継続性の問題にも確実に対処できるようになっている。ITの変更管理とビジネスプロセスの再設計の連携も進められている。変更管理プロセスの品質と成果について、一貫したモニタリングプロセスが存在している。

5 最適化
変更管理プロセスは定期的にレビューされ、常に優れた実践方法が取り入れられて、最新の状態に保たれている。レビュープロセスには、モニタリング結果が反映されている。構成情報はコンピュータで管理され、バージョンコントロールも実施されている。高度な変更履歴の追跡が行われており、未承認またはライセンスのないソフトウェアの検知ツールも採用されている。ITの変更管理はビジネスの変更管理と統合されており、ITが組織の生産性の拡大、および新たなビジネスチャンスの創出を確実に実現する鍵として機能している。

コントロール目標 －概要－

AI7 ソリューションおよびその変更の導入と認定

新規システムの開発完了後、そのシステムを実際に運用可能な状態にする必要がある。これには、適切なテストデータを使用した専用環境における公式的なテストの実施、展開と移行の指示書の策定、リリース計画策定と実際の本番環境への移行、および導入後のレビューが必要である。これにより、運用システムが合意された計画と成果に合致していることを保証する。



IT プロセス: ソリューションおよびその変更の導入と認定のコントロール目標は、

新規システムまたは変更されたシステムの導入後、重大な問題を発生させずに稼働することを、**ビジネス要件**とし、

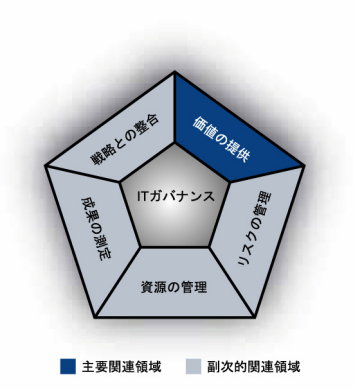
重点をおくべきコントロールは、アプリケーションとインフラストラクチャソリューションについて、本来の目的に適合していることとエラーがないことをテストし、本番環境に移行するためのリリース計画を策定することである。

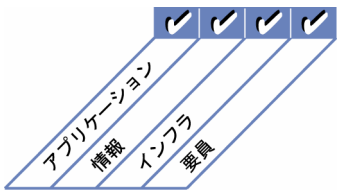
実現するための手段は、次の 4 項目である。

- テスト方法の確立
- リリース計画の策定
- ビジネス部門の管理者によるテスト結果の評価と承認
- 導入後レビューの実施

その成果の測定指標は、次の 3 項目である。

- 不適切なテストに起因するアプリケーションダウンタイムまたはデータ修正量
- 導入後プロセスによる測定において、期待される便益を実現したシステムの割合
- 文書化および承認されたテスト計画があるプロジェクトの割合





コントロール目標 －詳細－

AI7 ソリューションおよびその変更の導入と認定

AI7.1 研修
すべての情報システムの開発、導入、修正プロジェクトの一環として、策定された研修計画と導入計画、および関連資料に従って、影響を受ける部門のスタッフや IT 部門の運用グループのスタッフに研修を実施する。

AI7.2 テスト計画
テスト計画を策定し、関係者の承認を得る。テスト計画は、組織全体の標準に基づいており、役割、実行責任、および問題の有無の判定基準を定義する。計画においては、テストの準備(場所の準備を含む)、研修要件、定義されたテスト環境の導入または更新、テストケースの計画/実施/文書化/維持、エラーの処理と修正、および正式な承認について検討する必要がある。導入時のシステム障害や不具合に関するリスク評価に基づき、テスト計画は、パフォーマンス、負荷、可用性、およびパイロットテストとセキュリティテストの要件を含むべきである。

AI7.3 導入計画
導入計画を策定し、関係者の承認を得る。導入計画では、リリース設計、リリースパッケージの作成、展開手続/インストール方法、インシデントの処理、配布のコントロール(ツールを含む)、ソフトウェアの保管、リリースのレビュー、および変更の文書化を定義する。また、計画には、代替システムや変更取り消しなどに関する対策についても盛り込む必要がある。

AI7.4 テスト環境
テスト専用の独立したテスト環境を構築する。適切なテストを実施できるよう、今後の運用環境(同様のセキュリティ、内部統制、ワークロードなど)を反映したテスト環境を構築する必要がある。テスト環境において、最終的に本番環境で使用されるデータと同等のデータ(必要に応じて不必要な箇所が削除されている)を確実に使用するよう、手続を整備する必要がある。機密性を有するデータの開示を防ぐために、適切な対策を行う。テスト結果は文書化して保管しなければならない。

AI7.5 システムおよびデータの変換
組織における開発方法によって、すべての開発、導入、修正プロジェクトにおいて、ハードウェア、ソフトウェア、トランザクションデータ、マスターファイル、バックアップとアーカイブ、他のシステムとのインターフェース、手続、およびシステムのマニュアルなどの必須要素がすべて、事前に策定された計画に従って旧システムから新規システムに確実に変換されるようにする。変換前と変換後の結果の監査証跡を作成し、維持する必要がある。システムオーナは、移行が正常に行われたことを確認するため、新規システムの初回処理を詳細に検証する必要がある。

AI7.6 変更のテスト
変更に関するテストは、通常の運用環境での使用開始前に、策定された受け入れ計画に従って、独立したテスト環境で(開発グループから)独立したテスト担当グループが、性能の最適化を含む、影響評価、資源評価に基づいて確実に行うこと。計画の一部として並行テストまたはパイロットテストについて検討する必要がある。また、実際の展開前にセキュリティコントロールをテストおよび評価すべきであり、それによってセキュリティの有効性を保証することができる。代替システム/変更取り消しの計画についても、本番環境に変更を組み込む前に、策定およびテストする必要がある。

AI7.7 最終受け入れテスト
新規または変更された情報システムの最終受け入れまたは品質保証テストの一環として、影響を受ける部門の責任者と IT 部門が確実にテスト結果を正式に評価し、承認する手続を策定する必要がある。情報システムのすべてのコンポーネント(アプリケーションソフトウェア、設備、技術、ユーザ手続など)をテスト対象とし、すべてのコンポーネントが確実に情報セキュリティ要件を満たしていることを確認する。監査証跡、および将来のテストの実施に備えて、テストデータを保存すべきである。

AI7.8 本番環境への移行
導入計画に沿った、開発からテスト、そして運用へのシステムの移行をコントロールする正式な手続を導入する。マネジメント層は、新規システムの本番環境への引継ぎに際して、システムオーナの認可を義務付ける必要がある。さらに、旧システムを完全に廃止する前に、新システムが、日、月、四半期、年度のすべての本番運用サイクルにわたり正常に運用されることを確認する必要がある。

AI7.9 ソフトウェアのリリース
ソフトウェアのリリースは、承認、パッケージング、回帰テスト、配布、引継ぎ、状況追跡、変更取り消し手続、およびユーザ通知を確実に実施する正式な手続によって管理する必要がある。

AI7.10 システムの配布
承認を受けた構成アイテムのタイムリーかつ適切な配布と更新を実現するためのコントロール手続を確立する。これには、インテグリティのコントロールと、開発、テスト、運用の各担当者間における職務の分離、およびすべての活動に対する適正な監査証跡が含まれる。

AI7.11 変更の記録と追跡
アプリケーションシステムへの変更のモニタリングに使用するシステムを自動化する。これにより、アプリケーション、手続、プロセス、システムパラメーターとサービスパラメーター、および基盤プラットフォームに対する変更の記録と追跡をサポートする。

AI7.12 導入後レビュー
企業の開発標準と変更標準に沿って、運用中の情報システムの導入後レビューの実施を定めた手続を確立する。このレビューでは、変更が顧客の要件を満たし、最善の費用効率で計画時に見込んだ便益を提供できたか評価および報告する。

(空白ページ)

マネジメントガイドライン

AI7 ソリューションおよびその変更の導入と認定

From	インプット
PO3	技術標準
PO4	文書化されたシステムオーナ
PO8	開発標準
PO10	プロジェクトマネジメントガイドラインおよび詳細なプロジェクト計画
AI3	テスト/インストール対象の構成済みシステム
AI4	ユーザマニュアル、運用マニュアル、サポートマニュアル、技術マニュアル、および管理マニュアル
AI5	調達されたアイテム
AI6	変更の承認

アウトプット	To						
リリースされた構成アイテム	DS8	DS9					
既知の確認済みエラー	AI4						
本番環境への移行	DS13						
ソフトウェアのリリースおよび配布計画	DS13						
導入後レビュー	PO2	PO5	PO10				

RACI チャート

役割

アクティビティ	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス、監査、リスク、セキュリティ
導入計画の策定とレビュー			C	A	I	C	C	R		C	C
テスト戦略(開始基準と終了基準)および運用テストの計画策定方法の確立およびレビュー			C	A	C	C	C	R		C	C
ビジネス要件および技術的要件のリポジトリと認定されたシステムのテストケースの作成と保守				A				R			
テスト環境におけるシステムの変換テストと統合テストの実施			I	I	R	C	C	A/R		I	C
テスト環境の準備および最終受け入れテストの実施			I	I	R	A	C	A/R		I	C
合意された認定基準に基づいた本番環境への移行の推奨			I	R	A	R	C	R		I	C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- 稼働前に十分な受け入れテストを確実に実施するためのテスト方法の確立
- すべての構成アイテムに対する変更の追跡記録
- リリース計画の策定
- 導入後レビューの実施
- ビジネス部門の管理者によるテスト結果の評価と承認

促進

プロセスの達成目標
- アプリケーションおよび技術的ソリューションに関する、本来の目的への適合性の検証と確認
- 承認されたアプリケーションおよび技術的ソリューションのリリースおよび適切な配布
- アプリケーションおよび技術的ソリューションの使用に向けたビジネスユーザおよび運用担当者側の準備
- 新規ビジネスアプリケーション、および既存アプリケーションへの変更におけるエラーの確実な排除

促進

IT の達成目標
- 自動化された業務取引および情報交換の信頼性の保証
- ソリューションとサービスの提供における不備と手戻りの削減
- ビジネス戦略と整合性のとれたビジネス要件への対応
- アプリケーションおよび技術的ソリューションのビジネスプロセスへのシームレスな統合
- アプリケーションおよび技術的ソリューションの適切な利用と成果達成の確保
- エラー、意図的な攻撃、または災害で生じた障害に対する、IT サービスおよびインフラストラクチャの抵抗力・回復力の確保

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 導入プロセスおよび認定プロセスへの利害関係者の関与度
- 文書化および承認されたテスト計画があるプロジェクトの割合
- 導入後レビューから得られた教訓の数
- 導入および認可された機能の品質保証レビュー時に発見されたエラーの割合
- 導入前にマネジメント層から必要な承認を受けていない変更の数

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 社内または社外の監査時に発見された導入プロセスと認定プロセスに関するエラーの数
- 不適切な受け入れテストに起因する導入後の手戻りの作業量
- 不適切な研修に起因するユーザからサービスデスクへの問い合わせ件数
- 不適切なテストに起因するアプリケーションダウンタイムまたはデータ修正量

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 新規システムのデータインテグリティに満足している利害関係者の割合
- 導入後プロセスによる測定において、期待される便益を実現したシステムの割合

成熟度モデル

AI7 ソリューションおよびその変更の導入と認定

「新規システムまたは変更されたシステムを、導入後、重大な問題を発生させずに稼働する。」という IT に対するビジネス要件を満たす上で、「ソリューションおよびその変更の導入と認定」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
正式な導入プロセスや認定プロセスはまったく存在せず、マネジメント層や IT 担当スタッフも、各種のソリューションについて本来の目的との適合性を検証する必要性を認識していない。

1 初期/その場対応
導入されるソリューションが本来の目的に適合するものであるか検証および確認する必要性が認識されている。テストが実施されているプロジェクトもあるが、テストのイニシアチブは個々のプロジェクトチームに委ねられており、採用されるアプローチにもばらつきがある。正式な認定および承認は、ほとんど実施されていないか、まったく実施されていない。

2 再現性はあるが直感的
テストと認定のアプローチにある程度の一貫性はあるが、特定の方法論に基づいていないことが多い。通常個々の開発チームがテストのアプローチを決定しており、多くの場合統合テストは実施されていない。承認プロセスは非公式なものである。

3 定められたプロセスがある
導入、移行、変換、および受け入れに関する正式な方法論が整備されている。IT の導入プロセスと認定プロセスは、システムのライフサイクルに統合されており、ある程度自動化されている。研修、テスト、および本番環境への移行の状況とその認定については、個々人が判断しており、定義されたプロセスから逸脱する傾向がある。本番環境に導入するシステムの品質にばらつきがあり、新規システムの導入後に深刻な問題が発生する場合が多い。

4 管理され、測定可能である
正式化された手続が適切に体系化されており、確立されたテスト環境や認定手続において実用化できるレベルになっている。実際に、システムに対する主要な変更はすべてこの正式化されたアプローチに従って実施されている。ユーザ要件を満たすかどうかの評価が標準化され、測定可能になっており、マネジメント層が効果的にレビューおよび分析できる測定指標が規定されている。本番環境に導入されるシステムの品質は、マネジメント層が満足できる状態であり、導入後の問題も皆無と言えないまでも妥当な水準に抑えられている。プロセスの自動化は場当たり的に行われており、プロジェクトごとに状況が異なる。導入後の評価は実施されていないものの、マネジメント層は現行のシステムの有効性のレベルにおおよそ満足している。テストシステムは、実際の環境を的確に反映している。主要なプロジェクトにおいて、新規システムに対する負荷テストと既存システムに対する回帰テストが適用されている。

5 最適化
導入プロセスと認定プロセスは、継続的な改善と改良の結果、優れた実践基準のレベルにまで最適化されている。IT の導入プロセスと認定プロセスは、システムのライフサイクルに完全に統合され、自動化が妥当な場合は自動化されている。これにより、新規システムの研修、テスト、および本番環境への移行が最も効率的に実施されている。テスト環境、問題の記録プロセス、および障害解決のプロセスが十分に整備されており、本番環境への効率的かつ効果的な移行が実現している。通常認定後に再作業は発生せず、導入後の問題も軽微なものに限られている。導入後レビューが標準化され、レビューから得られた教訓がプロセスに反映されて、品質の継続的な改善が図られている。新規システムに対する負荷テストと変更されたシステムに対する回帰テストが一貫して適用されている。

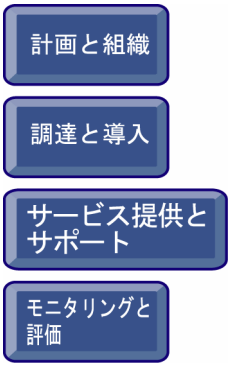
サービス提供とサポート

DS1 サービスレベルの定義と管理
DS2 サードパーティのサービスの管理
DS3 性能とキャパシティの管理
DS4 継続的なサービスの保証
DS5 システムセキュリティの保証
DS6 費用の捕捉と配賦
DS7 利用者の教育と研修
DS8 サービスデスクとインシデントの管理
DS9 構成管理
DS10 問題管理
DS11 データ管理
DS12 物理的環境の管理
DS13 オペレーション管理

コントロール目標 －概要－

DS1 サービスレベルの定義と管理

IT 管理部門とビジネス部門の顧客間で、求められるサービスについて効果的なコミュニケーションを行うためには、IT サービスおよびサービスレベルの定義と合意内容を文書化する必要がある。本プロセスには、サービスレベルの達成状況についてモニタリングし、利害関係者にタイムリーな報告をすることも含まれる。このプロセスにより、IT サービスと関連するビジネス要件との間の整合を図ることができる。



IT プロセス: サービスレベルの定義と管理のコントロール目標は、

主要な IT サービスとビジネス戦略との整合性が保証されることを、**ビジネス要件**とし、

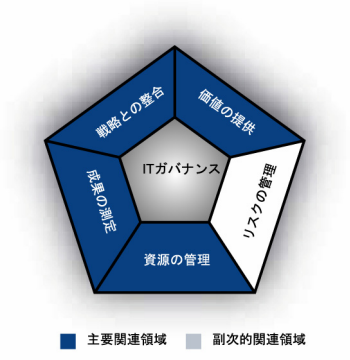
重点をおくべきコントロールは、サービス要件を特定し、サービスレベルについて合意し、サービスレベルの達成状況をモニタリングすることである。

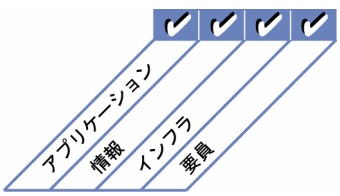
実現するための手段は、次の 3 項目である。

- 要件と提供能力を踏まえた上での社内外に対する正式な合意形成
- サービスレベル達成状況の報告(レポーティングとミーティング)
- 戦略策定に応じた新規または変更サービス要件の特定とコミュニケーション

その成果の測定指標は、次の 3 項目である。

- サービス提供が合意レベルへ到達していることに満足しているビジネス部門の利害関係者の割合
- カタログにない提供サービスの数
- ビジネス部門との正式な SLA レビュー会議の年間の開催回数





コントロール目標 －詳細－

DS1 サービスレベルの定義と管理

DS1.1 サービスレベル管理フレームワーク
顧客とサービスプロバイダ間で正式に合意されたサービスレベル管理プロセスを定めたフレームワークを定義する。このフレームワークを通じて、サービスレベルとビジネス要件およびビジネス上の優先事項との間の整合性を継続的に維持すると同時に、顧客とサービスプロバイダ双方における認識の共有を促進する。このフレームワークには、サービスに対する要件、サービス定義、サービス・レベル・アグリーメント(SLA)、オペレーショナル・レベル・アグリーメント(OLA)を策定し、および資金の調達元を明確にするためのプロセスを含める。これらのサービス属性は、サービスカタログ(service catalog)にまとめる。またこのフレームワークでは、サービスレベルの管理のための組織構造を定義する。その定義には、組織内外のサービスプロバイダと顧客の役割、タスク、および実行責任を含める。

DS1.2 サービスの定義
主にサービスカタログ/ポートフォリオ方式の導入を通じて収集され、蓄積されたサービス特性とビジネス要件に基づいて、IT サービスの基本的な定義を行う。

DS1.3 サービス・レベル・アグリーメント
顧客側の要件と IT の提供能力に基づいて、すべての重要な IT サービスについてサービス・レベル・アグリーメントを策定し、合意を得る。ここでは、顧客の確約事項、サービスサポート要件、利害関係者により承認されたサービスの量的/質的測定指標、資金の調達、および商業上の調整(該当する場合)、そしてサービス・レベル・アグリーメント(SLA)自体の監督業務を含む役割および実行責任が定められる。検討すべき事項は、可用性、信頼性、成果、容量計画、サポートレベル、継続計画、セキュリティ、および需要面での制約である。

DS1.4 オペレーショナル・レベル・アグリーメント
サービス・レベル・アグリーメント(SLA)を最適な形で満足するサービスの技術的提供方法を、オペレーショナル・レベル・アグリーメントにおいて明記する。オペレーショナル・レベル・アグリーメント(OLA)は、技術プロセスをサービスプロバイダに理解し易い形で規定し、必要に応じて、複数のサービス・レベル・アグリーメント(SLA)に対応する可能性がある。

DS1.5 サービスレベル達成状況のモニタリングと報告
規定されたサービスレベルの成果基準を継続的にモニタリングする。サービスレベルの達成状況に関する報告は、利害関係者が容易に理解できる形式で提出する。モニタリング結果の統計データを分析、処理し、サービス全般のほか、個々のサービスにおけるマイナス/プラス要因を特定する。

DS1.6 サービス・レベル・アグリーメントおよび請負契約の見直し
組織内外のサービスプロバイダと協力してサービス・レベル・アグリーメントとその請負契約を定期的に見直し、契約内容が有効かつ周辺動向に則した内容であり、要件の変化が反映されること確実にする。

マネジメントガイドライン

DS1 サービスレベルの定義と管理

From	インプット
PO1	IT 戦略/実行計画、IT サービスポートフォリオ
PO2	採用したデータの分類方法
PO5	最新の IT サービスポートフォリオ
AI2	当初計画されたサービス・レベル・アグリーメント(SLA)
AI3	当初計画されたオペレーショナル・レベル・アグリーメント(OLA)
DS4	災害時のサービス要件(役割および実行責任を含む)
ME1	IT 計画にインプットされる成果

アウトプット	To						
契約見直し結果の報告	DS2						
プロセスの成果報告	ME1						
新規または更新されたサービス要件	PO1						
サービス・レベル・アグリーメント(SLA)	AI1	DS2	DS3	DS4	DS6	DS8	DS13
オペレーショナル・レベル・アグリーメント(OLA)	DS4	DS5	DS6	DS7	DS8	DS11	DS13
最新の IT サービスポートフォリオ	PO1						

RACI チャート

担当

アクティビティ	CEO	CFO	企業幹部	CIO	ビジネス プロセス オーナー	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス、監査、リスク、セキュリティ	サービス管理担当者
IT サービス定義のためのフレームワークの策定			C	A	C	C	I	C	C	I	C	R
IT サービスカタログの作成			I	A	C	C	I	C	C	I	I	R
重要な IT サービスについてのサービス・レベル・アグリーメント(SLA)の定義		I	I	C	C	R	I	R	R	C	C	A/R
サービス・レベル・アグリーメント履行のためのオペレーショナル・レベル・アグリーメント(OLA)の定義				I	C	R	I	R	R	C	C	A/R
包括的なサービスレベル成果のモニタリングおよび報告				I	I	R		I	I		I	A/R
サービス・レベル・アグリーメント(SLA)とその請負契約の見直し		I		I	C	R		R	R		C	A/R
IT サービスカタログの見直しと更新			I	A	C	C	I	C	C	I	I	R
サービス改善計画の策定			I	A	I	R	I	R	C	C	I	R

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- サービスの定義
- 要件と提供能力を踏まえた上での社内外に対する正式な合意形成
- サービスレベル達成状況の報告(レポーティングとミーティング)
- 報告を受ける側に応じた報告の編成
- 戦略策定に対する新規または変更のサービス要件のフィードバック

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- ビジネス部門との正式な SLA レビュー会議の年間の開催回数
- 報告されたサービスレベルの割合
- 自動化された方法で報告されたサービスレベルの割合
- 顧客との合意後にサービスレベルの調整に要した作業日数

促進

プロセスの達成目標
- 求められるサービスレベルについての共通認識の確立
- サービス・レベル・アグリーメントおよび成果達成基準の正式化とモニタリング
- 提供サービスのレベルと、合意したサービスレベルとの合致
- ビジネス達成目標との整合が取れた最新のサービスカタログの作成

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- カタログにない提供サービスの数
- 合意したサービスレベルに到達しているサービスの割合
- 測定されているサービスレベルの割合

促進

IT の達成目標
- 提供サービスとサービスレベルに対するエンドユーザの満足の確保
- ビジネス戦略と合致するビジネス要件への対応
- IT 運用にかかる費用、便益、戦略、ポリシー、およびサービスレベルの透明性の確保と理解の実現

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- サービス提供が合意レベルへ到達していることに満足しているビジネス部門の利害関係者の割合
- サービス提供が合意レベルへ到達していることに満足しているユーザの割合

成熟度モデル

DS1 サービスレベルの定義と管理

「主要なITサービスとビジネス戦略との整合性が保証される。」というITに対するビジネス要件を満たす上で、「サービスレベルの定義と管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
マネジメント層がサービスレベルの定義プロセスの必要性を認識していない。それらをモニタリングする説明責任と実行責任が割り当てられていない。

1 初期/その場対応
サービスレベル管理の必要性は認識されているが、そのプロセスは非公式かつ事後的である。サービスの定義および管理の実行責任と説明責任について規定されていない。成果測定が行われているとしても、その測定はあいまいに定義された目標で定性的な測定に限られている。報告は非公式であり、報告頻度が低く継続性がない。

2 再現性はあるが直感的
合意されたサービスレベルが存在するが、これらのサービスレベルは非公式であり、見直しは行われていない。サービスレベルの報告が不完全であり、顧客にとって的外れまたは誤解を招く可能性がある。サービスレベルの報告は、個々の管理者のスキルおよびイニシアチブに依存する形で行われている。サービスレベル調整担当者が割り当てられ、実行責任が規定されているが、十分な権限は与えられていない。サービス・レベル・アグリーメント順守のためのプロセスが存在する場合でも、そのプロセスの実施は任意であり、強制されていない。

3 定められたプロセスがある
実行責任は明確に定義されているが、自由裁量に任されている。サービス・レベル・アグリーメントの策定プロセスが整備されており、サービスレベルと顧客満足度を再評価するためのチェックポイントが設けられている。標準プロセスを用いて、サービスとサービスレベルの定義、文書化、合意が実施されている。しかしサービスレベルの未達は識別されるが、それを解決する正式な手続がない。期待されるサービスレベルの達成と投下資金との間に明確な関連付けがある。合意されたサービスレベルはあるが、それがビジネスの必要性に対応していない可能性がある。

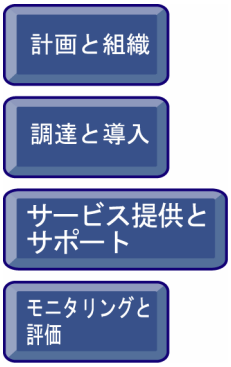
4 管理され、測定可能である
システム要件の定義段階において、サービスレベルが徐々に明確に定義され、アプリケーションおよび運用環境の設計の中に組み込まれている。顧客満足度が定期的に測定および評価されている。成果の測定指標に、IT の達成目標ではなく顧客のニーズが反映されている。サービスレベル評価の測定方法が標準化されつつあり、業界水準を反映している。サービスレベル定義の基準はビジネスの重点項目に基づいており、可用性、信頼性、成果、容量の余裕度、ユーザサポート、継続計画、およびセキュリティ上の検討事項が含まれる。サービスレベルに達していない場合には、その根本原因の分析が定期的に実施されている。サービスレベルモニタリングの報告プロセスが徐々に自動化されつつある。合意されたサービスレベルに達しない場合に発生し得る運用上および財務上のリスクが定義されており、明確に把握されている。KPI および KGI の正式な測定体系が構築、維持されている。

5 最適化
IT の目標とビジネス目標の整合性確保のため、サービスレベルの再評価が継続的に実施されている。同時に、費用対効果分析などの技術が活用されている。すべてのサービスレベルの管理プロセスにおいて、継続的な改善が課せられている。顧客満足度が継続的にモニタリング、管理されている。期待されるサービスレベルは各ビジネス部の戦略目標を反映していると同時に、業界水準に照らして評価されている。IT 管理部門には、サービスレベル目標の達成に必要な資源が割り当てられており、その説明責任が課されている。また、サービスレベル目標達成の動機付けとなる報酬体系が設定されている。マネジメント層は、継続的な改善プロセスの一環としてKPIおよびKGIのモニタリングを行っている。

コントロール目標 －概要－

DS2 サードパーティのサービスの管理

サードパーティが提供するサービスがビジネス要件を確実に満たすようにするには、効果的なサードパーティの管理プロセスが必要である。このプロセスでは、サードパーティとの合意のもと、役割、実行責任、および要求事項を明確に定義し、このような合意事項の有効性とコンプライアンスをレビューおよびモニタリングする。サードパーティが提供するサービスを効果的に管理することで、不適格なサービスプロバイダに起因するビジネスリスクを最小限に抑えることができる。



IT プロセス: サードパーティのサービスの管理のコントロール目標は、

便益、費用、およびリスクに関する透明性を維持し、サードパーティによる要件を満たすサービス提供を実現することを、**ビジネス要件**とし、

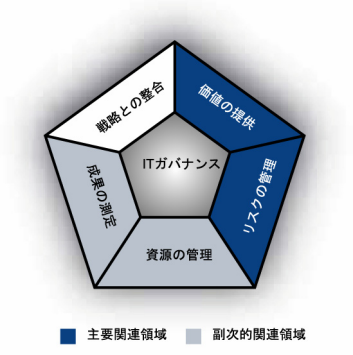
重点をおくべきコントロールは、適格なサービスプロバイダ(サードパーティ)とリレーションシップおよび相互責任を確立し、合意内容との適合性を検証し保証するためにサービス提供状況をモニタリングすることである。

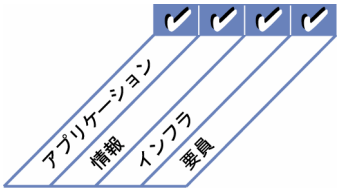
実現するための手段は、次の 3 項目である。

- サービスプロバイダからのサービスの特定と分類
- サービスプロバイダにかかわるリスクの特定と低減
- サービスプロバイダの成果のモニタリングと測定

その成果の測定指標は、次の 3 項目である。

- 契約されたサービスに関するユーザからの苦情件数
- 明確に定義された要件とサービスレベルを満たしている主要サービスプロバイダの割合
- モニタリング対象となっている主要サービスプロバイダの割合





コントロール目標 －詳細－

DS2 サードパーティのサービスの管理

DS2.1 すべてのサービスプロバイダとのリレーションシップの特定
すべてのサービスプロバイダのサービスを特定し、サービスプロバイダのタイプ、重要性、および依存度に従って分類する。技術的および組織的な関係を正式に文書化して管理する。この文書には、サービスプロバイダの役割および実行責任、目標、期待される成果物、および代表者の信用証明が含まれる。

DS2.2 サービスプロバイダとのリレーションシップ管理
サービスプロバイダごとにサービスプロバイダとのリレーションシップ管理プロセスを正式なものとする。リレーションシップオーナは連携して顧客およびサービスプロバイダにかかわる問題に取り組み、サービス・レベル・アグリーメントなどにより信頼と透明性に基づく良質なリレーションシップの維持に努めなければならない。

DS2.3 サービスプロバイダにかかわるリスクの管理
サービスプロバイダが安全かつ効率的な方法を使用し、継続的なサービスを提供する上で想定されるリスクを特定し、低減する。契約が、法令要件に従い一般的なビジネス標準に準拠していることを確認する。リスク管理ではさらに、秘密保持契約(NDA)、エスクロー契約(訳注:サードパーティ預託契約サービス提供者の破産等に備えて、ソースプログラム等をサードパーティに預託し、事由の発生時に、委託者に提供する契約)、サービスプロバイダの存続能力、セキュリティ要件へのコンプライアンス、代替サービスプロバイダ、SLA 未達と超過達成などについて検討すべきである。

DS2.4 サービスプロバイダの成果のモニタリング
サービス提供状況のモニタリングプロセスを確立する。これにより、サービスプロバイダが現行のビジネス要件を満たすと同時に、継続的に契約合意とサービス・レベル・アグリーメントを厳守し、その成果が、市場の状況および他のサービスプロバイダと比較した場合の優位性があることを確認する。

マネジメントガイドライン

DS2 サードパーティのサービスの管理

From	インプット
PO1	IT 調達戦略
PO8	調達基準
AI5	契約上の取り決め、サードパーティとのリレーションシップ管理における要件
DS1	サービス・レベル・アグリーメント(SLA)、契約レビュー結果の報告
DS4	災害時のサービス要件(役割および実行責任を含む)

アウトプット	To
プロセスの成果報告	ME1
サービスプロバイダー一覧表	AI5
サービスプロバイダにかかわるリスク	PO9

RACI チャート

アクティビティ	担当 CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO(プロジェクト・マネジメント・オフィス)	コンプライアンス・監査・リスク・セキュリティ
サードパーティとのサービス・リレーションシップの特定と分類				I	C	R	C	R	A/R	C	C
サービスプロバイダの管理プロセスの定義と文書化		C		A	I	R	I	R	R	C	C
サービスプロバイダの評価および選定に関するポリシーと手続の確立		C		A	C	C		C	R	C	C
サービスプロバイダにかかわるリスクの特定、評価および低減		I		A		R		R	R	C	C
サービスプロバイダからのサービス提供状況のモニタリング				R	A	R		R	R	C	C
すべての利害関係者に対するサービスのリレーションシップの長期的達成目標の評価	C	C	C	A/R	C	C	C	C	R	C	C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R:Responsible) ②説明責任者(A:Accountable) ③協議先(C:Consulted)④報告先(I:Informed)

達成目標とその評価指標

アクティビティの達成目標
- サービスプロバイダのサービスの特定と分類
- サービスプロバイダにかかわるリスクの特定と低減
- サービスプロバイダの成果のモニタリングと測定

促進

プロセスの達成目標
- 適格なサービスプロバイダ(サードパーティ)との相互責任を伴うリレーションシップの確立
- サービス提供のモニタリングと合意内容との適合性の確認
- サービスプロバイダが、関連する内外の標準に準拠していることの確認
- サービスプロバイダの関係継続要望の維持

促進

IT の達成目標
- サードパーティとのリレーションシップについての相互満足の達成
- 提供サービスとサービスレベルに対するエンドユーザの満足の確保
- IT 運用にかかる費用、便益、戦略、ポリシー、およびサービスレベルについての透明性の確保と理解の実現

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 明確に定義された要件とサービスレベルが義務付けられた主要サービスプロバイダの割合
- モニタリング対象となっている主要サービスプロバイダの割合
- サービスプロバイダからのコミュニケーションの有効性に対するビジネス部門の満足度
- ビジネス部門からのコミュニケーションの有効性に対するサービスプロバイダの満足度
- サービスプロバイダの契約不履行によって一定期間内に発生した重大インシデントの件数

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 明確に定義された要件とサービスレベルを満たす主要サービスプロバイダの割合
- サービスプロバイダとの正式な係争の件数
- サービスプロバイダからの請求書のうち係争の対象となったものの割合

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 契約されたサービスに関するユーザからの苦情件数
- 購入費用のうち、競争調達の対象となっている費用の割合

成熟度モデル

DS2 サードパーティのサービスの管理

「便益、費用、およびリスクに関する透明性を維持し、サードパーティによる要件を満たすサービス提供を実現する。」という IT に対するビジネス要件を満たす上で、「サードパーティのサービスの管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
実行責任および説明責任が定義されていない。サードパーティとの契約締結に関する正式なポリシーおよび手続が規定されていない。マネジメント層は、サードパーティからのサービスについて、承認もレビューも実施していない。成果測定が実施されておらず、サードパーティによる報告もない。契約上、報告義務が定められていないため、マネジメント層は、提供されるサービスの質を認識していない。

1 初期/その場対応
マネジメント層は、契約の締結を含め、サードパーティ管理に関するポリシーと手続を文書化する必要性を認識している。サービスプロバイダとの契約に盛り込むべき標準的な契約条項は定められていない。提供サービスの成果測定は非公式かつ事後的に実施されている。実施方法は、各担当者およびサービスプロバイダの経験に依存しており、たとえば要求された場合などに限り実施されている。

2 再現性はあるが直感的
サービスプロバイダ(サードパーティ)についての関連リスク、およびサービス提供状況の監督プロセスは非公式なものである。標準的なベンダーとの契約条項(提供されるべきサービスについての記述など)が規定された出来合いの契約書が締結され、使用されている。提供サービスに関する報告は実施されているが、ビジネス目標の達成に役立っていない。

3 定められたプロセスがある
ベンダーの審査およびベンダーとの交渉に関する明確なプロセスを含む、サードパーティのサービスを管理するための手続が適切に文書化され、整備されている。提供サービスに関する合意が存在する場合、サードパーティとの関係は純粋に契約に基づくものである。契約には提供されるサービスの性質が詳述されている。これには、法的要件、運用上の要件、およびコントロール要件が含まれている。サードパーティのサービスの監督実行責任が割り当てられている。契約条項は、契約の標準テンプレートに基づいている。サードパーティのサービスに関連するビジネスリスクについて評価および報告されている。

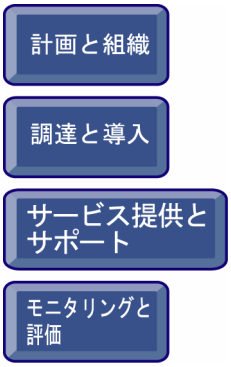
4 管理され、測定可能である
契約条項の定義に関する正式かつ標準化された基準が確立されている。この契約条項には、作業範囲、提供されるべきサービス/成果物、前提条件、スケジュール、費用、請求処理、および実行責任が含まれる。契約およびベンダーの管理の実行責任が割り当てられている。ベンダーの適格性、リスク、および能力が継続的に確認されている。サービス要件が定義され、ビジネス目標と関連付けられている。サービスの成果を契約条項に照らし合わせてレビューするプロセスが確立されている。これは、現行および将来のサードパーティのサービスの評価へのインプットとなる。調達プロセスにおいて、振替価格設定モデルが利用されている。関係者全員がサービス、費用、および各工程で期待される成果について認識している。サービスプロバイダの監督における KPI および KGI について合意が得られている。

5 最適化
サードパーティとの間で締結された契約が、事前に定義されている間隔で定期的にレビューされている。サービスプロバイダ管理と提供サービスの品質管理の実行責任が割り当てられている。運用、法律、コントロールに関する契約条項が遵守されているかどうかが、常にモニタリングされており、必要な場合に是正措置が講じられている。サードパーティに対する独立した定期レビューが実施されており、成果に関するフィードバックが提供され、サービス提供の改善に役立てられている。ビジネス状況の変化に対応する形で測定方法も変動する。成果測定により、サードパーティのサービスにおける潜在的問題を早期に発見できる。サービスレベル達成状況の包括的かつ明確な報告は、サードパーティに対する支払いに関連付けられている。マネジメント層は、KPI および KGI の結果に基づきサードパーティからのサービスの調達とモニタリングのプロセスを調整している。

コントロール目標 －概要－

DS3 性能とキャパシティの管理

IT 資源の性能とキャパシティを管理するには、IT 資源の性能とキャパシティを定期的にレビューするプロセスが必要である。このプロセスには、作業負荷、ストレージ、および緊急時の要件に基づいて今後のニーズを予測することが含まれる。このプロセスにより、ビジネス要件を支援する情報資源の継続的可用性が保証される。



IT プロセス: 性能とキャパシティの管理のコントロール目標は、

ビジネス上の必要性に応じて、IT のインフラストラクチャ、資源、および能力を最適化することを、**ビジネス要件**とし、

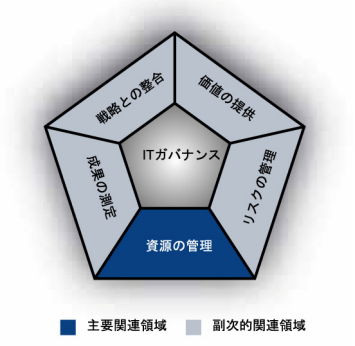
重点をおくべきコントロールは、モニタリングと測定により、サービス・レベル・アグリーメントにて合意した応答時間に関する要件を満たし、ダウンタイムを最小限に抑え、IT の性能とキャパシティの継続的改善を図ることである。

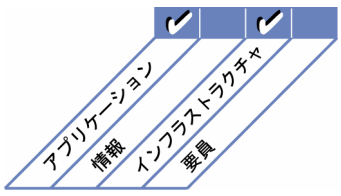
実現するための手段は、次の 3 項目である。

- システムキャパシティと可用性の計画策定と提供
- システム性能のモニタリングと報告
- システム性能のモデル化と予測

その成果の測定指標は、次の 3 項目である。

- 不十分なキャパシティ計画策定に起因する、1ユーザ、月あたりの損失時間数(1カ月あたり)
- 稼働率の上限を超過したピークの割合
- サービス・レベル・アグリーメント(SLA)に定められた要件を満たさなかった応答時間の割合





コントロール目標 －詳細－

DS3 性能とキャパシティの管理

DS3.1 性能とキャパシティの計画策定
IT 資源の性能とキャパシティのレビュー計画の策定プロセスを確立する。これにより、サービス・レベル・アグリーメントで規定されている合意された作業負荷を処理するための費用的に妥当な性能とキャパシティを保証する。性能とキャパシティの計画では、適切なモデル化技法を用いて、現状、および予測される IT 資源の性能、キャパシティ、およびスループットのモデルを作成することが必要である。

DS3.2 現状の性能とキャパシティ
現状の IT 資源の性能とキャパシティのレビューを実施する。これにより、サービス・レベル・アグリーメントに照らし合わせて十分な性能とキャパシティが提供されているかどうかを確認する。

DS3.3 将来の性能とキャパシティ
IT 資源の性能とキャパシティの予測を定期的に実施する。これにより、キャパシティ不足または性能の低下に起因するサービス中断のリスクを最小限に抑える。また、IT 資源の再配置を可能にするような余剰能力がないか検証する。作業負荷の傾向を識別し、かつ予測値を決定し、性能とキャパシティの計画に取り込む。

DS3.4 IT 資源の可用性
標準作業負荷、緊急事態、ストレージに関する要件、および IT 資源のライフサイクルなどの面を考慮して、必要となるキャパシティと性能を提供する。性能とキャパシティが必要とされるレベルに達していない場合の対策(作業の優先順位付け、フォールトトレランスメカニズム、資源の割り当て活動など)を定めるべきである。マネジメント層は、緊急時対応計画において確実に個々の IT 資源の可用性、キャパシティおよび性能について適切に対応可能であることを確認する必要がある。

DS3.5 モニタリングと報告
IT 資源の性能とキャパシティを継続的にモニタリングする。収集データは次の 2 つの目的で使用される。
- IT の現行の性能を維持および調整し、障害からの回復、緊急時対応、現状および予定されている作業負荷、ストレージに関する計画と資源調達などの課題に対応する。
- サービス・レベル・アグリーメント(SLA)での規定に従い、ビジネス部門に対し提供サービスの可用性の報告を行う。すべての例外報告に対して、是正措置に関する推奨案を追記する。

マネジメントガイドライン

DS3 性能とキャパシティの管理

From	インプット
AI2	可用性、継続性、および復旧の要件
AI3	システムモニタリング要件
DS1	サービス・レベル・アグリーメント(SLA)

アウトプット	To						
性能とキャパシティに関する情報	PO2	PO3					
性能とキャパシティに関する計画(要件)	PO5	AI1	AI3	ME1			
必要な変更	AI6						
プロセスの成果報告	ME1						

RACI チャート

担当

アクティビティ	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
IT 資源の性能とキャパシティのレビューに関する計画策定プロセスの確立				A		R	C	C	C	C	
IT 資源の現行の性能とキャパシティのレビュー				C	I	A/R		C	C	C	
IT 資源の性能とキャパシティの予測				C	C	A/R	C	C	C	C	
IT 資源に関する不適合を特定するギャップ分析の実施				C	I	A/R		R	C	C	I
IT 資源が利用不能になる潜在的リスクに備えた緊急時対応計画の策定				C	I	A/R		C	C	I	C
IT 資源の可用性、性能とキャパシティの継続的なモニタリングおよび報告				I	I	A/R		I	I	I	I

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- システムキャパシティと可用性の計画策定と提供
- システムキャパシティのモニタリングと報告
- システムキャパシティのモデル化と予測

促進

プロセスの達成目標
- ピーク時の負荷とトランザクションの応答時間のモニタリングと測定
- サービス・レベル・アグリーメント(SLA)における応答時間要件への適合
- 処理に失敗したトランザクションの最小化
- ダウンタイムの極小化
- IT 資源の利用の最適化

促進

IT の達成目標
- ビジネス戦略と合致するビジネス要件への対応
- 要求に応じて IT サービスを使用可能であることの保証
- IT インフラストラクチャ、資源、および能力の最適化

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 性能とキャパシティの予測の実施頻度
- キャパシティレビューの対象である資産の割合
- 集中管理ツールを使用してモニタリングされる資産の割合

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- ピーク時の負荷と全体的な稼働率
- 稼働率の上限を超過したピークの割合
- サービス・レベル・アグリーメント(SLA)に定められた要件を満たさなかった応答時間の割合
- 処理に失敗したトランザクションの障害発生率

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 不十分なキャパシティ計画策定に起因する、1 ユーザあたりの損失時間数(1 カ月あたり)
- 定められたサービス可用性計画が適用されていない重要なビジネスプロセスの数

成熟度モデル

DS3 性能とキャパシティの管理

「ビジネス上の必要性に応じて、IT のインフラストラクチャ、資源、および能力を最適化する。」という IT に対するビジネス要件を満たす上で、「性能とキャパシティの管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
マネジメント層が、主要なビジネスプロセスで高いレベルの成果を IT に求める場合があること、もしくは IT サービスに対する全体的なビジネス上のニーズがキャパシティを超える可能性があることを認識していない。キャパシティ計画策定プロセスが整備されていない。

1 初期/その場対応
性能とキャパシティに制約がある場合は、主にユーザがワークアラウンド(回避策)を検討しなければならない。キャパシティと性能の計画を策定する必要性について、ビジネスプロセスオーナがほとんど認識していない。性能とキャパシティの管理への対応は、概して事後的に行われている。キャパシティと性能の計画策定プロセスは非公式なものである。IT 資源の現行および将来のキャパシティと性能についての理解は限定的である。

2 再現性はあるが直感的
ビジネス部門と IT 部門の管理者は、性能とキャパシティを管理しない場合の影響について認識している。性能に関するニーズは概ね満たされているが、これは個別のシステム評価と、サポートチームおよびプロジェクトチームの知識に依存している。性能とキャパシティに関する問題の診断にさまざまなツールが用いられているものの、診断結果の首尾一貫性については、主要な担当者の力量に依存している。IT の性能とキャパシティに関する包括的な評価が行われておらず、また、ピーク時および最悪時の負荷状況について考慮されていない。可用性の問題が不意かつランダムに発生する可能性があり、問題の診断および是正に相当の時間がかかる。成果測定はすべて、顧客の必要性ではなく、主に IT 部門の必要性に基づいて行われている。

3 定められたプロセスがある
性能とキャパシティの要件は、システムのライフサイクル全体に対して定義されている。サービスレベル要件と指標が定義されており、この指標を用いて運用上の性能を測定できる。定義されたプロセスに従って将来の性能とキャパシティの要件がモデル化されている。性能に関する統計値を示す報告書が作成されている。性能とキャパシティに関連する問題が発生する可能性は依然として存在し、問題を是正するには時間がかかる。サービスレベルが公表されているが、ユーザと顧客がサービス提供能力について疑念を抱く余地がある。

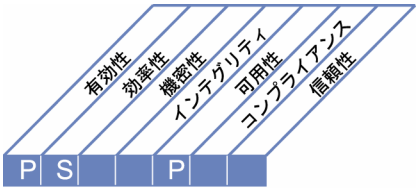
4 管理され、測定可能である
システムの使用状況、性能とキャパシティを測定するプロセスとツールが存在しており、測定結果は定義済みの達成目標と比較される。最新の情報が入手可能である。この情報には、標準化された性能に関する統計値と、性能とキャパシティの不足に起因するインシデントのアラート情報が含まれている。性能とキャパシティの不足に関する問題は、規定された標準手続に従って処理される。特定の資源(ディスクスペース、ネットワーク、サーバ、およびゲートウェイなど)のモニタリングに自動化ツールが用いられている。性能とキャパシティに関する統計値がビジネスプロセスの観点から報告され、その報告によりユーザと顧客が IT サービスレベルを理解できるようになっている。ユーザは現在のサービス提供能力に概ね満足しており、新たな、そしてさらに改善された可用性レベルを要求する可能性がある。IT の性能とキャパシティを測定するための KGI および KPI について合意が得られているが、これらの指標は、単に散発的かつ首尾一貫せずに適用されている可能性がある。

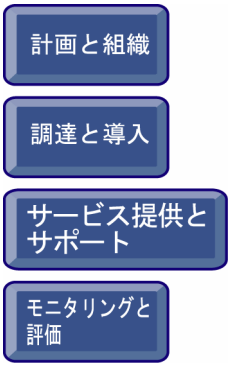
5 最適化
性能とキャパシティの計画は、ビジネス上の要件の予測と十分に同期されている。IT インフラストラクチャとビジネス上の要件の定期的なレビューが義務付けられており、これにより最小限の費用での最適なキャパシティの確実な実現が可能になっている。重要な IT 資源をモニタリングするためのツールが標準化されており、各プラットフォームで使用され、全社的なインシデント管理システムに関連付けられている。モニタリングツールは成果と能力に関連する問題を発見し、自動的に是正できる。傾向分析が実施され、業務量の増大に起因する差し迫った性能上の問題が発見される。この結果、対応計画の策定と、予期しない問題の回避が可能になる。IT の性能とキャパシティの測定指標が、すべての重要なビジネスプロセスについて KGI および KPI に最適に組み込まれており、首尾一貫して測定されている。マネジメント層は、KGI および KPI の分析を踏まえ、性能とキャパシティに関する計画の調整を行っている。

コントロール目標 －概要－

DS4 継続的なサービスの保証

継続的な IT サービスを提供するには、IT 継続計画の作成、保守、およびテスト、遠隔地のバックアップ保管施設の確保および定期的な継続計画に関するトレーニングの実施が必要である。効果的なサービス継続プロセスにより、主要な IT サービスの中断の可能性と、このような中断が主要なビジネスの機能とプロセスに及ぼす影響を最小限に抑えることができる。





IT プロセス: 継続的なサービスの保証のコントロール目標は、

IT サービスの中断発生時のビジネスに対する影響を最小限に抑えることを、**ビジネス要件**とし、

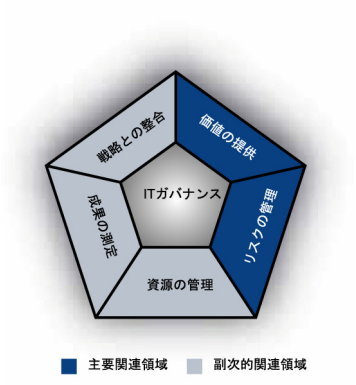
重点をおくべきコントロールは、障害からの回復力のあるシステム化を行い、IT 継続計画を作成、保守、およびテストすることである。

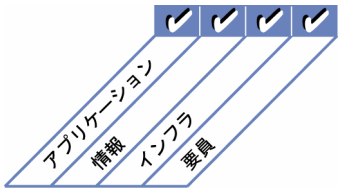
実現するための手段は、次の 3 項目である。

- IT 緊急時対応計画の作成と維持(改善)
- IT 緊急時対応計画に関する訓練とテスト
- 遠隔地における保管施設への緊急時対応計画のコピーとデータの保管

その成果の測定指標は、次の 2 項目である。

- 予定外の機能停止に起因する、1 ユーザ、月あたりの損失時間数
- IT 継続計画でカバーされていない、IT に依存している重要なビジネスプロセスの数





コントロール目標 －詳細－

DS4 継続的なサービスの保証

DS4.1 IT 継続フレームワーク
一貫したプロセスで全社的な事業継続管理を支援する、IT 継続フレームワークを作成する。このフレームワークの目的は、求められるインフラストラクチャの復旧能力の決定を支援し、災害復旧計画と IT 緊急時対応計画の策定を促進することである。このフレームワークには、内外のサービスプロバイダ、その管理者および取引顧客の役割、担当作業、および実行責任を含む、継続管理に必要な組織構造、そして災害復旧計画および IT 緊急時対応計画を文書化、テスト、および実施する際のルールと体制を規定する必要がある。また計画には、重要な資源の特定、その資源の可用性のモニタリングと報告、代替処理手続、およびバックアップと復旧に関する原則などの項目も規定する必要がある。

DS4.2 IT 継続計画
大規模な中断が主要なビジネスの機能とプロセスに及ぼす影響の軽減を目的とする、フレームワークに基づいた IT 継続計画を策定する。この計画では、すべての重要な IT サービスの障害からの回復、代替処理手続、および復旧能力に関する要件について規定する。また、計画では利用ガイドライン、役割と実行責任、手続、周知プロセス、およびテスト方法も規定しなければならない。

DS4.3 重要な IT 資源
IT 継続計画において、最重要と定められた要素に重点を置くことで、障害からの回復力を組み込み、災害復旧時の作業の優先順位を設定する。重要度が低い要素の回復を優先させることのないよう、優先的ビジネス要件に応じた対応と復旧を確実にする。また、費用を受容可能なレベルに抑え、法的要件および契約上の要件へのコンプライアンスも確保する。1～4 時間、4～24 時間、24 時間超、重要業務の運用期間など、さまざまなレベルにおける回復力、対応、および復旧要件を考慮する。

DS4.4 IT 継続計画の保守
IT 継続計画の内容が常に最新に保たれ、継続的に実際のビジネス要件が反映されることを確実にするために、IT 管理部門に対し、変更管理手続の策定および実施を促す。手続と実行責任における変更内容を明確かつタイムリーに周知することが不可欠である。

DS4.5 IT 継続計画のテスト
IT システムが効果的に回復可能であること、欠点が解消されること、および IT 継続計画の妥当性が維持されることを確実にするために、IT 継続計画の定期的なテストを実施する。このためには、綿密な準備、手続の文書化、テスト結果の報告、および結果に基づく対応計画の策定と実施が必要である。テストの範囲として、単一アプリケーションの復旧テストから、複数のテストシナリオを組み合わせたテスト、エンドツーエンドでのテスト、そしてベンダーを含む総合的なテストなどを想定する。

DS4.6 IT 継続計画に関する研修
すべての関係者が、インシデントまたは災害発生時の各自の役割および実行責任と実施手続に関する定期訓練セッションを確実に受講する。緊急時対応テストの結果に基づいて、訓練の内容を検証および補強する。

DS4.7 IT 継続計画の配付
計画が安全かつ適切な方法で確実に配付され、必要な時に必要な場所で許可を受けた当事者が利用できるように、定義および管理された配付方法が存在することを確認する。どのような災害発生状況においても、IT 継続計画が入手および参照可能な状態になっているよう配慮する必要がある。

DS4.8 IT サービスの復旧および再開
IT サービスの復旧および再開中に実施すべき措置を計画する。この計画には、バックアップサイトの起動、代替処理の開始、顧客および利害関係者への周知、再開手続などが規定される。IT の復旧にかかる時間とビジネスの復旧と再開のニーズを支援するために必要な技術投資について、ビジネス部門が確実に理解しているようにする。

DS4.9 遠隔地におけるバックアップ保管施設
すべての重要なバックアップメディア、文書、および IT 復旧計画と業務継続計画に必要なその他の IT 資源を、遠隔地の施設に保管する。保管するバックアップの内容については、ビジネスプロセスオーナと IT 担当者が協働して決定する必要がある。遠隔地の保管施設の管理者は、データ分類方法のポリシーと企業のメディア保管活動に対応しなければならない。IT 管理部門は、遠隔地保管施設について、保管内容、施設の物理的安全性、およびセキュリティを確実に定期的に(少なくとも 1 年に 1 回)評価する必要がある。アーカイブデータの復元のためのハードウェアとソフトウェアの互換性を確保し、アーカイブデータを定期的にテストおよび更新する。

DS4.10 再開後のレビュー
災害発生後に IT 機能が正常に再開した後、IT 管理部門が IT 復旧計画の妥当性を評価する手続を策定したか確認し、必要に応じて計画を更新する。

マネジメントガイドライン

DS4 継続的なサービスの保証

From	インプット
PO2	採用したデータの分類方法
PO9	リスク評価
AI2	可用性、継続性、および復旧の仕様
AI4	ユーザ、運用、サポート、技術、および管理の各マニュアル
DS1	サービス・レベル・アグリーメント(SLA)とオペレーショナル・レベル・アグリーメント(OLA)

アウトプット	To						
緊急時対応テストの結果	PO9						
IT 構成要素の重要度	DS9						
バックアップの保管と保護計画	DS11	DS13					
インシデント/災害のしきい値	DS8						
災害時サービス要件(役割および実行責任を含む)	DS1	DS2					
プロセスの成果報告	ME1						

RACI チャート

アクティビティ	担当 CEO	CFO	企業幹部	CIO	ビジネス プロセス オーナー	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO (プロジェクト・マネジメント・オフィス)	コンプライアンス・監査・リスク・セキュリティ
IT 継続フレームワークの作成		C	C	A	C	R	R	R	C	C	R
ビジネス影響分析とリスク評価の実施		C	C	C	C	A/R	C	C	C	C	C
IT 継続計画の策定と保守	I	C	C	C	I	A/R		C	C	C	C
復旧目標に基づく IT 資源の特定と分類				C		A/R		C	I	C	I
IT 継続計画を常に最新の状態で維持するための変更管理手続の策定と実施				I		A/R		R	R	R	I
IT 継続計画の定期的なテスト				I	I	A/R		C	C	I	I
テスト結果に基づく追加対応計画の作成				C	I	A/R	C	R	R	R	I
IT 継続計画に関する訓練の計画と実施				I	R	A/R		C	R	I	I
IT サービスの復旧および再開の計画策定		I	I	C	C	A/R	C	R	R	R	C
バックアップの保管と保護に関する計画の策定と実施				I		A/R		C	C	I	I
再開後のレビュー実施手続の確立				C		A/R		C	C		C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- IT 緊急時対応計画の作成と維持(改善)
- IT 緊急時対応計画に関する訓練とテスト
- 遠隔地の施設への緊急時対応計画のコピーとデータの保管

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- IT 継続計画の特定要素のテスト間隔
- IT 部門の当該従業員 1 人あたりの、IT 継続計画に関する年間の訓練時間
- 自動化された可用性モニタリングを行っている重要インフラストラクチャの割合
- IT 継続計画のレビュー実施頻度

促進

プロセスの達成目標
- 業務継続計画を支援する IT 継続計画の策定
- 実施、テスト、および維持可能な IT 継続計画の策定
- IT サービス中断発生の可能性の極小化

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- サービス・レベル・アグリーメント(SLA)に定められた要件を満たす可用性の割合
- IT 継続計画でカバーされていない IT に依存している重要なビジネスプロセスの数
- 復旧目標を達成したテストの割合
- 重要なシステムのサービス中断発生頻度

促進

IT の達成目標
- 要求に応じて IT サービスを使用可能であることの保証
- IT サービスの中断または変更が及ぼすビジネスへの影響の極小化
- エラー、意図的な攻撃、または災害で生じた障害に対する、IT サービスおよびインフラストラクチャの抵抗力・回復力の確実な保証

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 予定外の機能停止に起因する、1 ユーザあたりの損失時間数(1 カ月)

成熟度モデル

DS4 継続的なサービスの保証

「IT サービスの中断発生時のビジネスに対する影響を最小限に抑える。」という IT に対するビジネス要件を満たす上で、「継続的なサービスの保証」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
IT 運用におけるリスク、脆弱性、および脅威、または IT サービスを提供できなくなった場合のビジネスへの影響が認識されていない。マネジメント層がサービスの継続性について配慮する必要はないと考えている。

1 初期/その場対応
継続的なサービスの実行責任は正式に定められておらず、実行責任を果たす上での権限は限定的である。マネジメント層が、継続的なサービスの必要性とそれに関連するリスクを認識しつつある。マネジメント層の継続的なサービスに対する関心は、IT サービスではなく主にインフラストラクチャ資源に向けられている。サービス中断に際しては、ユーザがワークアラウンド(回避策)を講じている。大規模な中断に対し、IT 部門の対応が事後的であり準備がなされていない。計画的な機能停止は IT 部門のニーズに応じて予定され、ビジネス上の要件は考慮されない。

2 再現性はあるが直感的
継続的なサービスを保証するための実行責任が割り当てられている。継続的なサービスを保証する手法は断片的である。システムの可用性に関する報告は散発的に実施され、不完全である可能性がある。また、この報告ではビジネスに与える影響が考慮されていない。継続的なサービスの可用性を実現するための取り組みが行われ、その主要な方針が周知されているが、IT 継続計画が文書化されていない。重要なシステムとコンポーネントの一覧が作成されているが、信頼性が低い。継続的なサービスのための実践基準が徐々に見られるようになっているが、その成功は各担当者の裁量に依存している。

3 定められたプロセスがある
継続的なサービスの管理に関する説明責任の所在が明確化されている。継続的なサービスの計画策定とテストの実行責任が明確に定義され、割り当てられている。システムの重要度とビジネスに与える影響に基づくIT継続計画が文書化されている。継続的なサービスのテストに関する報告が定期的に行われている。各個人が率先して標準を遵守し、大規模なインシデントまたは災害発生時の対処に関する訓練を受けている。マネジメント層は、継続的なサービスを保証するための計画の必要性を一貫して周知させている。可用性の高いコンポーネントが使用され、システムの冗長化が図られている。重要なシステムとコンポーネントの一覧が維持されている。

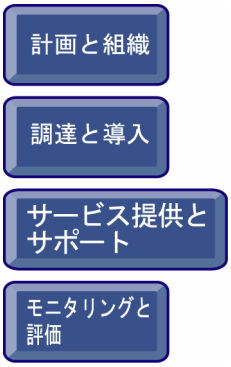
4 管理され、測定可能である
継続的なサービスの実行責任と標準が徹底運用されている。サービスの継続計画を維持する実行責任が割り当てられている。維持活動は、継続的サービスのテスト結果、内部の優れた実践基準、IT およびビジネスの変化に基づいて行われている。継続的なサービスに関する体系的なデータが収集、分析、報告され、これに基づいて対策がとられている。継続的なサービスプロセスに関する正式な訓練が実施されており、参加が義務付けられている。システム可用性に関する優れた実践基準が一貫して導入されている。可用性に関する実践基準と継続的なサービスの計画策定は相互に影響を及ぼしている。中断インシデントは分類され、それぞれの上位へのエスカレーションパスについて関係者全員が十分に認識している。継続的なサービスに関する KGI と KPI が策定および合意されているが、一貫した方法で測定されていない可能性がある。

5 最適化
継続的なサービスの統合プロセスでは、ベンチマーク評価と外部のベストプラクティスについても考慮されている。IT 継続計画が業務継続計画と統合されており、定期的に保守されている。継続的なサービスを保証するための要件を満たす上で、ハードウェアの早期出荷契約等が一般的である。IT 継続計画の包括的なテストが実施されており、その結果が計画の更新に利用されている。データが収集および分析され、プロセスが継続的に改善されている。可用性に関する実践基準と継続的なサービスの計画策定は完全に連携されている。マネジメント層は、SPOF(single point of failure)に起因する障害または大規模インシデントが発生しないことを保証できる。エスカレーションに関する実践基準は、理解されており、徹底して実施されている。継続的なサービスの達成に関する KGI と KPI が、体系的な方法で測定されている。マネジメント層は、測定された KGI と KPI に応じて継続的なサービスの計画を調整している。

コントロール目標 —概要—

DS5 システムセキュリティの保証

情報のインテグリティを維持し、IT 資産を保護するためには、セキュリティ管理のプロセスが必要である。このプロセスには、IT セキュリティに関する役割と責務、ポリシー、標準、および手続を定め、それらを運用、改善することが含まれる。また、セキュリティ管理には、セキュリティのモニタリングと定期的なテストの実施、および識別されたセキュリティの弱点やインシデントに対する是正措置の導入も含まれる。セキュリティ管理を効果的に実行することで、すべての IT 資産を保護し、セキュリティの脆弱性やインシデントがビジネスに与える影響を最小限に抑えることができる。



IT プロセス: システムセキュリティの保証のコントロール目標は、

情報および情報処理インフラストラクチャのインテグリティを維持し、セキュリティ上の脆弱性やインシデントによる影響を最小限に抑えることを、**ビジネス要件**とし、

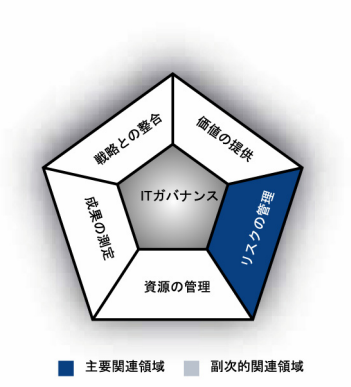
重点をおくべきコントロールは、IT セキュリティポリシー、手続および標準を明確に定め、セキュリティ上の脆弱性やインシデントをモニタリング、発見、報告、是正することである。

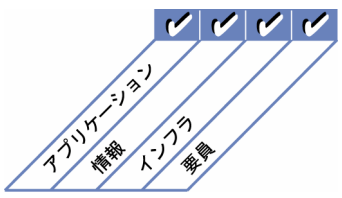
実現するための手段は、次の 3 項目である。

- セキュリティ要件と、脆弱性、脅威の認識
- 標準化された方法によるユーザの識別と認可の管理
- 定期的なセキュリティテストの実施

その成果の測定指標は、次の 3 項目である。

- 社会的信用に悪影響を及ぼしたインシデントの件数
- セキュリティ要件を満たしていないシステムの数
- 職務分離が適切に行われていない違反の数





コントロール目標 －詳細－

DS5 システムセキュリティの保証

DS5.1 IT セキュリティの管理
セキュリティに係る活動が、ビジネス上の要件に沿って実施されるよう、組織の適切な上位層において、最適な体制を組んで IT セキュリティを管理する。

DS5.2 IT セキュリティ計画
情報に関するビジネス要件、IT の構成、情報リスクへの対応計画、および情報セキュリティ文化を総合的な IT セキュリティ計画としてまとめる。この計画は、サービス、要員、ソフトウェア、およびハードウェアに対する適切な投資とともに、セキュリティポリシーや関連手続に盛り込まれる。セキュリティポリシーおよび手続は、利害関係者とユーザに周知する。

DS5.3 ID 管理
IT システムにおけるすべてのユーザ(内部、外部、臨時かどうかを問わず)と、ユーザのすべてのアクティビティ(ビジネスアプリケーションやシステムの操作、開発や保守)を、個々に識別しなくてはならない。システムやデータに対するユーザのアクセス権は、文書化された業務上の必要性や職務要件に即したものでなければならない。ユーザのアクセス権は、ユーザ管理職の申請に基づいてシステムオーナが承認し、セキュリティ責任者が実装する。ユーザ ID とアクセス権は、単一のリポジトリで集中管理する。ユーザの識別、認証の実施、およびアクセス権の徹底管理のために、費用効率に優れた技術面および手続面での対策を講じ、常に継続的な改善を行う。

DS5.4 ユーザアカウントの管理
ユーザアカウントおよびそれに付随するユーザ権限の申請、設定、発行、停止、変更、および抹消は、ユーザアカウント管理において確実に行う。ユーザアカウントの管理には、データオーナまたはシステムオーナがアクセス権限を付与する場合の承認手続も含まれる。これら一連の手続は、アドミニストレーター(特権ユーザ)、内部ユーザ、外部ユーザを含むすべてのユーザに、平常時・緊急時を問わず適用されるべきである。企業が所有するシステムと情報へのアクセスに関連した権利と義務は、あらゆるタイプのユーザごとに契約の形式で定める。すべてのアカウントとそれらに関連する権限の内容は、マネジメント層が定期的にレビューする。

DS5.5 セキュリティのテスト、監視、モニタリング
IT セキュリティの導入、運用に関して、テストおよびモニタリングを積極的に行うことが必要である。承認されたセキュリティレベルが確実に保たれていることを保証するために、IT セキュリティは定期的に見直しを行わなければならない。ログの取得、およびモニタリングの機能を活用することで、対応の必要な異例もしくは異常な行動を、早めに検知できる。ログ情報へのアクセスは、業務上の必要性に基づいて規定されるアクセス権およびログ保存基準に従って行う。

DS5.6 セキュリティインシデントの定義
起こり得るセキュリティインシデントの特性を明確に定義、周知し、インシデント管理または問題管理プロセスによって、セキュリティインシデントに確実に対応できるようにする。特性の定義には、セキュリティインシデントと見なされる判断基準および影響レベルが含まれる。影響レベルの定義は数を限定し、それぞれのレベルに対して要求される具体的な対処方法と、通知すべき要員を特定する。

DS5.7 セキュリティ技術の保護
重要なセキュリティ関連技術には、改ざんに対する確実な耐性を持たせる。また、セキュリティ関連文書が不必要に開示されないように、つまり、目立たないようにする。ただし、セキュリティ仕様の機密が漏れても、システムのセキュリティが保たれるようにしなくてはならない。

DS5.8 暗号鍵の管理
暗号鍵の生成・変更・取消・失効・交付・認証・保存・入力・使用・アーカイブ化を体系的に行うためのポリシーおよび手続を確実に整備し、暗号鍵の改変や、許可されていない暗号鍵の開示を防止する。

DS5.9 不正ソフトウェアの阻止、発見、および是正
予防・発見・対処のための対策(特に最新のセキュリティパッチとウイルス管理)を組織全体にわたって確実に実施し、IT システムおよび情報技術を悪意のあるソフトウェア(ウイルス、ワーム、スパイウェア、スパム、社内で開発された不正ソフトウェアなど)から確実に保護する。

DS5.10 ネットワークのセキュリティ
セキュリティ技術とそれに関連する管理手続(ファイアウォール、セキュリティアプライアンス、ネットワークのセグメント化、侵入検知など)をを使用し、ネットワークへのアクセスの許可とネットワークに出入りする情報フローを確実にコントロールする。

DS5.11 機密データの交換
機密性を有するトランザクションデータは、内容の真正性確保、送信証明、受信証明、および送信元による否認防止が可能なコントロールを備えた信頼できる経路あるいはメディアのみを介してやり取りを行う必要がある。

マネジメントガイドライン

DS5 システムセキュリティの保証

From	インプット
PO2	情報アーキテクチャ：採用したデータの分類方法
PO3	技術標準
PO9	リスク評価
AI2	アプリケーションセキュリティのコントロールの仕様
DS1	オペレーショナル・レベル・アグリーメント(OLA)

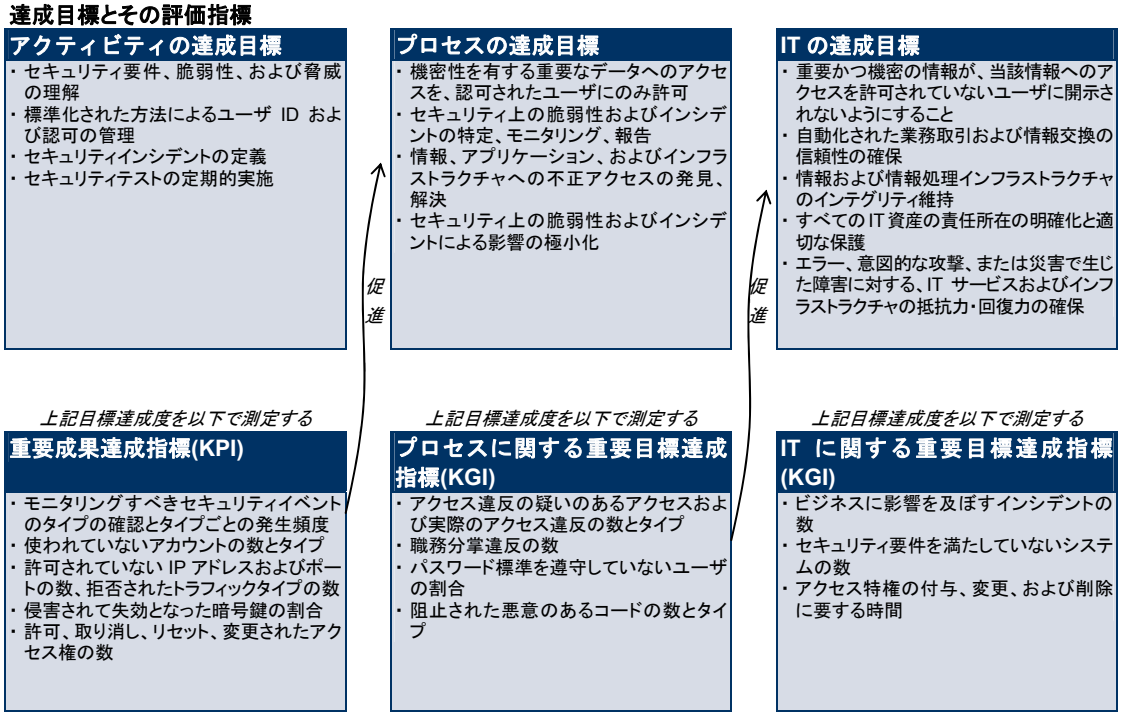
アウトプット	To
セキュリティインシデントの定義	DS8
セキュリティ意識の向上に関する具体的な研修要件	DS7
プロセスの成果報告	ME1
必要なセキュリティ変更	AI6
セキュリティ上の脅威と脆弱性	PO9

RACI チャート

アクティビティ / 担当	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
IT セキュリティ計画の定義と維持	I	C	C	A	C	C	C	C	I	I	R
ID(アカウント)管理プロセスの定義・作成・運用			I	A	C	R	R	I			C
潜在的および実際のセキュリティインシデントのモニタリング				A	I	R	C	C			R
ユーザのアクセス権・特権の定期的見直しと確認				I	A	C					R
暗号鍵の保持・保護のための手続作成と改訂				A		R			I		C
ネットワーク間の情報フローを保護する技術的・手続的なコントロールの導入・維持				A	C	C	R	R			C
定期的な脆弱性評価の実施		I		A	I	C	C	C			R

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標



成熟度モデル

DS5 システムセキュリティの保証

「情報および情報処理インフラストラクチャのインテグリティを維持し、セキュリティ上の脆弱性やインシデントによる影響を最小限に抑える。」という IT に対するビジネス要件を満たす上で、「システムセキュリティの保証」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
組織が IT セキュリティの必要性を認識していない。セキュリティを確保するための実行責任および説明責任が割り当てられていない。IT セキュリティ管理を支援する対策が実施されていない。IT セキュリティに関する報告および IT セキュリティ違反発生時にとるべき対応プロセスが存在しない。システムのセキュリティ管理プロセスと呼べるようなものがまったく存在しない。

1 初期/その場対応
組織が IT セキュリティの必要性を認識している。セキュリティの必要性に関する意識は、主として個人に依存している。IT セキュリティへの取り組みは事後対応という形である。IT セキュリティの成果測定は行われていない。責任の所在が明確ではなく、IT セキュリティ違反が発見された場合、責任のなすり合いが起こる。IT セキュリティ違反への対応は予測できない。

2 再現性はあるが直感的
IT セキュリティの実行責任および説明責任は IT セキュリティに関する調整を担う担当者に課せられているが、この担当者には限られた管理権限しか与えられていない。セキュリティの必要性に関する意識は断片的で限定的である。セキュリティ関係の情報はシステムによって生成されているが、分析は行われていない。サードパーティが提供するサービスが、セキュリティに関する組織特有のニーズに対応していない可能性がある。セキュリティポリシーを策定中であるが、スキルおよびツールが不十分である。IT セキュリティの報告体制は、不完全で、誤解を招きやすく、適切ではない。セキュリティ研修が提供されているが、受講するかどうかは主に個人の自発性に委ねられている。IT セキュリティは主に IT 部門の責任および分野であるとみなされており、ビジネス部門側に IT セキュリティが自己の責任分野であるとの意識がない。

3 定められたプロセスがある
セキュリティに対する意識があり、マネジメント層もその向上を推進している。IT セキュリティ手続が定義され、IT セキュリティポリシーとの整合が図られている。IT セキュリティに関する責任が割り当てられ、理解されているものの、一貫した実行はなされていない。リスク分析に基づいた IT セキュリティ計画とセキュリティソリューションがある。セキュリティに関する報告には、明確なビジネス的視点が含まれていない。セキュリティのテスト(侵入テストなど)は場当たり的に行われている。IT 部門とビジネス部門の両方を対象にしたセキュリティ研修が提供されているが、計画と運営は非公式に行われているにすぎない。

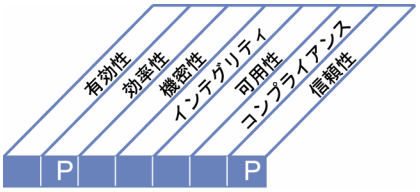
4 管理され、測定可能である
IT セキュリティの責任が明確に割り当てられ、管理、実行されている。IT セキュリティのリスクと影響に関する分析が、一貫して行われている。具体的なセキュリティ基準に基づき、セキュリティポリシーとセキュリティに関する活動が完了している。セキュリティ意識の向上に向けた取り組みには、全員の参加が義務付けられている。ユーザの識別や、認証、認可が標準化されている。セキュリティの監査および管理の責任を負うスタッフには、セキュリティ資格の取得が求められている。セキュリティテストは、正式な標準プロセスに従って実施され、それがセキュリティレベルの向上につながっている。IT セキュリティプロセスと組織全体のセキュリティ機能との調整が図られている。IT セキュリティに関する報告と、ビジネス目標との関連付けが行われている。IT セキュリティに関する研修が、ビジネス部門および IT 部門の双方において行われている。IT セキュリティに関する研修が業務上の要請や文書化されたセキュリティリスク分析結果に対応する形で計画、管理されている。セキュリティ管理に対する KGI と KPI が定義されているが、測定までは行われていない。

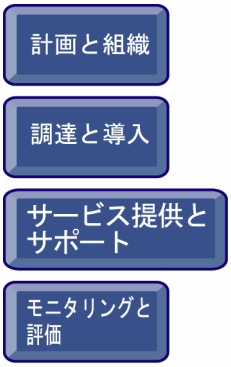
5 最適化
IT セキュリティはビジネス部門と IT 管理部門の共同責任であり、企業のセキュリティに関するビジネス目標に組み込まれている。IT セキュリティ要件が明確に定義および最適化されており、承認されたセキュリティ計画に盛り込まれている。ユーザおよび顧客は、セキュリティ要件の定義に対してますます大きな説明責任を負い、設計段階からセキュリティ機能がアプリケーションに組み込まれている。セキュリティインシデントへの対応は、自動化ツールを利用した正式なインシデント対応手続に基づいて、迅速に行われている。定期的なセキュリティ評価が行われ、導入したセキュリティ計画の有効性が評価されている。脅威および脆弱性に関する情報が体系的に収集・分析されている。リスクを軽減するための適切なコントロールが直ちに伝達され、実施されている。セキュリティテスト、インシデントの根本的原因の分析、およびリスクを積極的に発見することで、継続的にプロセスを改善している。組織全体でセキュリティプロセスと技術の統合が図られている。セキュリティ管理に関する重要目標達成指標(KGI)および重要成果達成指標(KPI)が収集され、周知されている。マネジメント層は KGI と KPI を用いて、セキュリティ計画を継続的に改善している。

コントロール目標 －概要－

DS6 費用の捕捉と配賦

IT 費用をビジネス部門に適正かつ公平に配賦するための体系を実現するには、IT 費用を正確に測定し、適正な配賦についてビジネス部門の同意を得る必要がある。このプロセスには、IT 費用を捕捉し、サービスを受けるユーザへ配賦および報告するためのシステムの構築と運用が含まれる。適正な配賦システムを導入することで、IT サービスの利用に関して、ビジネス部門が十分な情報を得た上での決定が可能になる。





IT プロセス: 費用の特定と配賦のコントロール目標は、

IT 費用の透明性と理解の確保、および十分な情報を得た上での IT サービスの利用による費用効率の向上を、**ビジネス要件**とし、

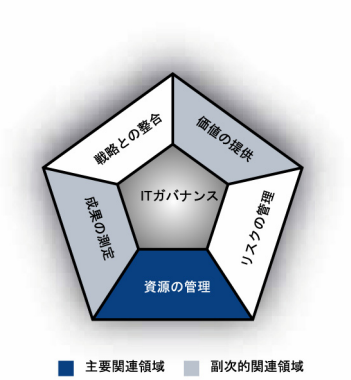
重点をおくべきコントロールは、IT 費用の完全かつ正確な捕捉、およびビジネス部門の同意を得た適正な配賦体系と、IT の利用および配賦費用に関するタイムリーな報告体系の確立することである。

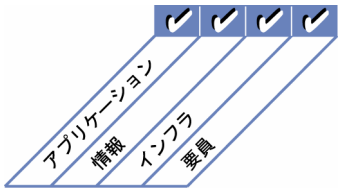
実現するための手段は、次の 3 項目である。

- 提供サービスの質/量に見合う課金
- 完備された費用モデルの構築とそれに対する同意
- 同意されたポリシーに基づく課金の実施

その成果の測定指標は、次の 3 項目である。

- ビジネス管理部門が承認した/支払った IT サービス費用請求の割合
- 予算、予測、および実費用間の不一致の割合
- 同意された費用モデルに基づいて配賦された IT 費用の総 IT 費用に対する割合





コントロール目標 －詳細－

DS6 費用の捕捉と配賦

DS6.1 サービスの定義
透明性のある費用モデルを実現するため、すべての IT 費用を特定し、これらの費用を IT サービスに対応付ける。IT サービスをビジネスプロセスに関連付け、ビジネス部門が関連サービスの費用請求レベルを特定できるようにする。

DS6.2 IT 財務管理
定義された費用モデルに従って実費用を捕捉および配賦する。企業の財務測定体系に従って、予測と実費用間の不一致を分析し、報告する。

DS6.3 費用モデルの策定と費用請求
サービス定義に基づいて、サービスの直接費、間接費、および諸経費を含み、サービスあたりのチャージバック率の計算を支援する費用モデルを策定する。この費用モデルは、企業の原価計算手続に沿ったものである必要がある。IT 費用モデルの策定により、サービスに対する費用請求をユーザが確実に特定、測定、および予測可能となり、資源の適切な利用が促進される。ユーザマネジメントが、サービスの実利用状況と課金状況を検証できる必要がある。

DS6.4 費用モデルの保守
費用/課金モデルの適合性を定期的にレビューおよびベンチマーク評価し、進化するビジネス活動と IT 活動に対する妥当性および適合性を維持する。

マネジメントガイドライン

DS6 費用の捕捉と配賦

From	インプット
PO4	文書化されたシステムオーナ
PO5	費用便益報告、IT 予算
PO10	詳細なプロジェクト計画
DS1	サービス・レベル・アグリーメント(SLA)とオペレーショナル・レベル・アグリーメント(OLA)

アウトプット	To
IT 会計報告	PO5
プロセスの成果報告	ME1

RACI チャート

担当

アクティビティ	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス、監査、リスク、セキュリティ
提供サービス/サポートされているビジネスプロセスへの IT インフラストラクチャの対応付け		C	C	A	C	C	C	C	R	C	
すべての IT 費用(要員的費用、技術的費用など)の特定と、これらの費用の IT サービスへの単位原価での対応付け		C		A		C	C	C	R	C	
IT 会計および原価管理のプロセスの確立と保守		C	C	A	C	C	C	C	R	C	
課金に関するポリシーと手続の確立と保守		C	C	A	C	C	C	C	R	C	

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- ビジネス管理部門による配賦費用のレビュー
- 提供サービスの質に見合う費用の調整
- 完備された費用モデルの構築とそれに対する同意
- 同意されたポリシーに基づく課金の実施
- 費用のベンチマーク評価の定期的な実施

促進

プロセスの達成目標
- IT 費用とサービスの適正かつ公平な定義付け
- IT サービスの費用の正確な捕捉
- IT サービス利用者への IT 費用の適正かつ公平な配賦

促進

IT の達成目標
- IT 運用にかかる費用、便益、戦略、ポリシー、およびサービスレベルについての透明性の確保と理解の実現
- IT の費用効率およびビジネス収益性への IT の貢献度の向上
- IT による費用効率の高いサービス品質、継続的な改善、および将来の変更に対する対応力の保証

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 費用モデルの定義に関与したビジネス部門の担当者の割合
- 費用配賦モデルのレビュー頻度
- 自動/手動で配賦された費用の割合

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 予算、予測、および実費用間の不一致の割合
- 同意された費用モデルに基づいて配賦された IT 費用の総 IT 費用に対する割合
- ビジネス部門の同意を得られなかった費用の割合

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- ビジネス管理部門が承認した/支払った IT サービスの費用請求の割合
- サービスあたりの長期的な単位原価
- IT サービスの費用モデルに対するビジネス部門の満足度(調査)

成熟度モデル

DS6 費用の捕捉と配賦

「IT 費用の透明性と理解の確保、および十分な情報を得た上での IT サービスの利用による費用効率の向上。」という IT に対するビジネス要件を満たす上で、「費用の捕捉と配賦」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
提供される情報サービスに関する費用を特定し配賦するために認知可能なプロセスがまったく存在しない。組織は、原価計算に関して対処すべき問題の存在さえ認識しておらず、したがってその問題に関する話し合いも行われていない。

1 初期/その場対応
情報サービスの全体的な費用について一般的な理解はあるが、ユーザ、顧客、部門、ユーザグループ、サービス組織単位、プロジェクト、および成果物ごとの費用について個別に認識されていない。マネジメントに費用総計が報告されるだけで、費用のモニタリングは事実上実施されていない。IT 費用は運用上の経費として配賦されている。ビジネス部門に対して、サービス提供の費用もしくは便益に関する情報が提供されていない。

2 再現性はあるが直感的
費用の集計と配賦の必要性が全体的に認識されている。費用配賦は非公式または費用に対する基本的な前提(ハードウェア費用など)に基づいて実施されており、価値要因への関連付けがほとんどなされていない。費用配賦プロセスは繰り返し実施されている。費用の捕捉および配賦に関する標準の手続について、正式な研修が行われておらず、また周知もされていない。費用の捕捉と配賦の実行責任が割り当てられていない。

3 定められたプロセスがある
情報サービスの費用モデルが定められ、文書化されている。ユーザに提供されるサービスと IT 費用の関連付けプロセスが策定されている。情報サービスにかかる費用について、適切に認識されている。ビジネス部門に対し、費用に関する基本的な情報が提供されている。

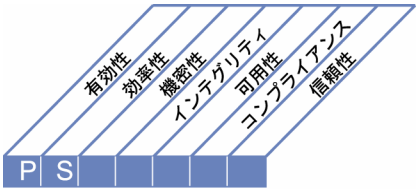
4 管理され、測定可能である
情報サービスの費用管理についての実行責任と説明責任の所在が明確化されており、すべてのレベルにおいて十分に理解されている。また、これらの費用管理に関する正式な研修が実施されている。タイムリーかつ自動化された方法を用いて直接費と間接費が捕捉され、マネジメント層、ビジネスプロセスオーナ、およびユーザに報告されている。費用のモニタリングと評価が概ね実施されており、費用の逸脱が発見されると対応措置がとられる。情報サービスの費用は、ビジネス目標とサービス・レベル・アグリーメント(SLA)に関連付けて報告されており、ビジネスプロセスオーナによりモニタリングされている。財務部門により、費用配賦プロセスの妥当性レビューが実施されている。自動化された原価計算システムが存在しているが、このシステムではビジネスプロセスではなく情報サービス機能に重点が置かれている。費用測定に関する KPI および KGI について合意が得られているが、その測定方法は一貫していない。

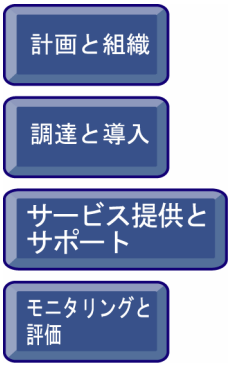
5 最適化
提供サービスの費用が捕捉、集計され、マネジメント層、ビジネスプロセスオーナ、およびユーザに報告されている。費用は請求可能項目として捕捉され、提供されたサービスに対して、利用率に基づいてユーザに適切に請求するチャージバックシステムで対応可能である。費用明細は、サービス・レベル・アグリーメント(SLA)に対応している。サービス費用のモニタリングおよび評価結果が、IT 資源の費用の最適化に活用されている。取得した費用の数値が、便益実現の検証、および組織の予算策定プロセスに利用されている。高度な報告システムを使用した情報サービスの費用報告により、ビジネス要件の変化について早期警告を得ることができる。提供されるサービスごとの処理量から導き出された、変動費用モデルが活用されている。費用管理は、継続的な改善および外部組織とのベンチマークの評価の結果、業界のベストプラクティスレベルにまで高められている。費用の最適化は継続的なプロセスとして実施されている。マネジメント層は、費用測定システムの再設計における継続的な改善プロセスの一環として、KPI および KGI のレビューを行っている。

コントロール目標 －概要－

DS7 利用者の教育と研修

IT 部門内を含む IT システムの全ユーザに対して効果的な教育を実施するには、ユーザグループごとの研修のニーズを特定する必要がある。このプロセスには、ニーズの特定の他に、効果的な研修のための戦略の策定と実施、および結果の測定が含まれる。効果的な研修プログラムにより、ユーザによるエラーの減少、生産性の向上、および主要コントロール(ユーザセキュリティ対策など)へのコンプライアンスの強化を実現でき、技術を一層効果的に利用できるようになる。





IT プロセス: 利用者の教育と研修のコントロール目標は、

アプリケーションおよび技術的ソリューションの効果的かつ効率的な利用と、ユーザによるポリシーおよび手続へのコンプライアンスを、**ビジネス要件**とし、

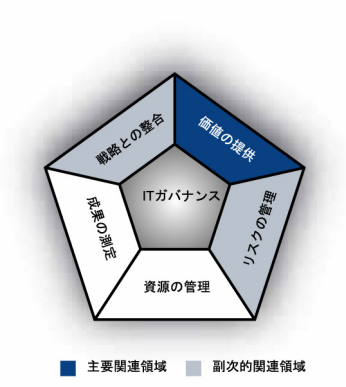
重点をおくべきコントロールは、IT ユーザの研修ニーズを明確に把握し、効果的な研修戦略と結果測定を実施することである。

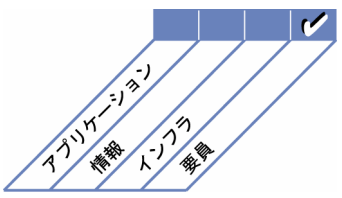
実現するための手段は、次の 4 項目である。

- 研修カリキュラムの作成
- 研修の準備
- 研修の実施
- 研修の有効性についてのモニタリングと報告

その成果の測定指標は、次の 3 項目である。

- ユーザ研修を実施しないことに起因するサービスデスクへの問い合わせの件数
- 実施された研修内容に満足している利害関係者の割合
- 研修ニーズの特定から研修実施までに要する時間





コントロール目標 －詳細－

DS7 利用者の教育と研修

DS7.1 教育と研修のニーズの特定

研修対象の各従業員グループに対し、以下を考慮して研修カリキュラムを策定し、定期的に更新する。

- 現在/将来のビジネス上の必要性と戦略
- 企業の価値基準(倫理基準、コントロールおよびセキュリティの企業風土など)
- 新規 IT インフラストラクチャやソフトウェア(パッケージおよびアプリケーション)の導入
- 現在のスキル、能力プロファイル、公的資格および資格取得の必要性
- 実施方法(セミナー型、e ラーニング型など)、対象グループの規模、参加のしやすさ、および実施時期

DS7.2 教育と研修の実施

特定された教育と研修のニーズに基づいて、研修対象グループとそのメンバー、効果的な実施方法、講師、トレーナー、およびメンターを定める。トレーナーを任命し、適時に研修セッションを計画する。登録者(受講の前提要件を含む)、出席状況、および成績評価を記録する必要がある。

DS7.3 受講研修内容の評価

教育と研修の終了後、その実施内容について、妥当性、内容の質、有効性、獲得および吸収できた知識、費用と価値の面から評価する。この評価の結果を、将来のカリキュラムの策定と研修セッションに役立てる。

マネジメントガイドライン

DS7 利用者の教育と研修

From	インプット
PO7	ユーザのスキルと能力(自己研修を含む)、特定の研修要件
AI4	研修資料、ソリューション導入にあたっての知識移転要件
DS1	オペレーショナル・レベル・アグリーメント(OLA)
DS5	セキュリティ意識の向上に関する具体的な研修要件
DS8	ユーザ満足度の調査報告

アウトプット	To
プロセスの成果報告	ME1
必要な文書の更新	AI4

RACI チャート

担当

アクティビティ	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO (プロジェクト・マネジメント・オフィス)	コンプライアンス・監査・リスク・セキュリティ	研修部門
ユーザの研修ニーズの特定とその分析			C	A	R	C	C	C	C	C	C	R
研修プログラムの作成			C	A	R	C	I	C	C	C	I	R
啓蒙活動および教育研修の実施			I	A	C	C	I	C	C	C	I	R
研修評価の実施			I	A	R	C	I	C	C	C	I	R
最良の研修実施方法およびツールの特定と評価			I	A/R	R	C	C	C	C	C	C	R

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R:Responsible) ②説明責任者(A:Accountable) ③協議先(C:Consulted)④報告先(I:Informed)

達成目標とその評価指標

アクティビティの達成目標
- 研修カリキュラムの作成
- 研修の準備
- 研修の実施
- 研修の有効性についてのモニタリングと報告

促進

プロセスの達成目標
- 最も費用効率に優れた方法を使用した、各レベルのユーザ向け研修プログラムの作成
- アプリケーションおよび技術ソリューションに関する知識のユーザへの移転
- アプリケーションと技術的対応策を利用する際のリスクと実行責任に関する意識の向上

促進

IT の達成目標
- 提供サービスとサービスレベルに対するエンドユーザの満足の確保
- アプリケーションおよび技術的対応策の適切な利用と成果達成の保証
- IT インフラストラクチャ、資源、および能力の最適化

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 研修カリキュラムの更新頻度
- 研修ニーズの特定から研修実施までに要する時間

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 研修に関するサービスデスクへの問い合わせ件数、または質問への回答件数
- 実施された研修内容に満足している利害関係者の割合
- 研修を受けた従業員の割合

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- システムに対する理解の向上による、従業員の測定された生産性の向上
- サービス、システム、または新たな技術の周知によるユーザ満足度の向上

成熟度モデル

DS7 利用者の教育と研修

「アプリケーションおよび技術的対応策の効果的かつ効率的な利用と、ユーザのポリシーおよび規定された手続への準拠。」というIT に対するビジネス要件を満たす上で、「利用者の教育と研修」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
教育研修プログラムがまったく存在ない。組織は、研修に関して対処すべき問題の存在さえ認識しておらず、したがってその問題に関する話し合いも行われていない。

1 初期/その場対応
教育研修プログラムの必要性を組織が認識している徴候はあるが、標準化されたプロセスが存在しない。体系的なプログラムが存在しないため、従業員が自ら研修コースを選択して参加している。こうした研修コースの中には、倫理規定、システムセキュリティの意識、およびセキュリティ活動に関する問題を扱っているものもある。マネジメントの取り組みに結束がなく、教育研修に関する課題や取り組みについての話し合いは散発的で一貫性がない。

2 再現性はあるが直感的
教育研修プログラムと関連プロセスの必要性が組織全体において認識されている。研修が、従業員の個別の業績計画に組み込まれるようになってきている。プロセスの成熟度は、複数のインストラクターが非公式な教育研修コースを実施する段階にまできているが、同一のテーマが異なるアプローチで扱われている。一部の研修コースでは、倫理規定、システムセキュリティの意識、およびセキュリティ活動に関する問題を扱っている。各研修担当者の知識に依存する部分が大きい。ただし、全体的な課題と、このような課題に対処する必要性に関しては、一貫して話し合われている。

3 定められたプロセスがある
教育研修プログラムが制度化され周知されており、従業員と管理者が研修の必要性を把握して文書化している。教育研修プロセスが標準化および文書化されている。教育研修プログラムを実施するための予算、資源、施設、講師が確保されつつある。倫理規定、システムセキュリティの意識およびセキュリティ活動に関する正式な研修コースが従業員を対象に実施されている。ほとんどの教育研修プロセスがモニタリングされているが、マネジメント層がすべての逸脱を発見できるとは考えにくい。教育研修における問題の分析は散発的にしか実施されていない。

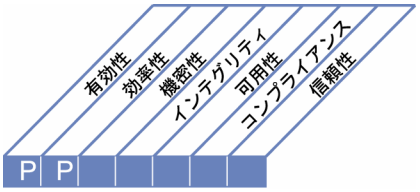
4 管理され、測定可能である
総合的な教育研修プログラムが設けられており、結果が測定可能である。実行責任が明確化されており、プロセスの担当責任が割り当てられている。教育研修が従業員のキャリアパスの一要素として組み込まれている。マネジメント層が教育研修コースの開催を支援し、コースに参加している。従業員全員が倫理規定およびシステムセキュリティの意識に関する研修を受講している。障害による、システムの可用性、機密性、およびインテグリティに影響を及ぼす被害を防ぐため、従業員全員が適切なレベルのシステムセキュリティ活動についての研修を受講している。マネジメント層が教育研修プログラムとプロセスを日常的にレビューおよび更新することにより、準拠状況をモニタリングしている。プロセスが継続的に改善されており、常に内部のベストプラクティスが採用されるようになっている。

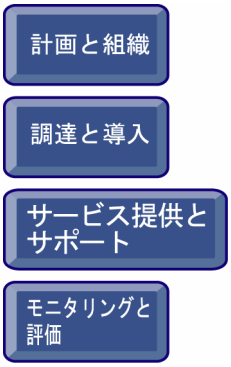
5 最適化
教育研修の結果として各個人の業績が向上している。教育研修が従業員のキャリアパスの重要な要素として組み込まれている。教育研修プログラムのために十分な予算、資源、施設、および講師が確保されている。外部のベストプラクティスや、成熟度モデルを利用し他社と比較することで、プロセスが洗練されてきており、継続的に改善されている。すべての問題や逸脱の根本原因が分析され、有効な対策が適宜特定および実施されている。倫理規定およびシステムセキュリティの原則に対する積極的な姿勢が見られる。教育研修プログラムに利用できるツールの提供および自動化のために、IT が広範囲で統合的かつ最適化された方法で IT が利用されている。研修に関する外部の専門家が活用され、ベンチマークを使用した指導が行われている。

コントロール目標 －概要－

DS8 サービスデスクとインシデントの管理

IT ユーザの問い合わせや発生した問題に対してタイムリーかつ効果的に対応するには、適切に構成、運用されているサービスデスクとインシデント管理プロセスが必要である。このプロセスには、インシデント登録、インシデントエスカレーション、傾向および根本原因の分析、および問題解決の機能を持つサービスデスクの設置が含まれる。ビジネス上の便益には、ユーザからの問い合わせに対する迅速な対応による、生産性の向上が含まれる。さらに、効果的な報告を通して、ビジネス部門はユーザ研修の不足といった根本原因の追究に取り組むことができる。





IT プロセス: サービスデスクとインシデントの管理のコントロール目標は、

エンドユーザからの問い合わせ、質問、およびインシデントを確実に解決および分析し、IT システムの効果的な利用を実現することを、**ビジネス要件**とし、

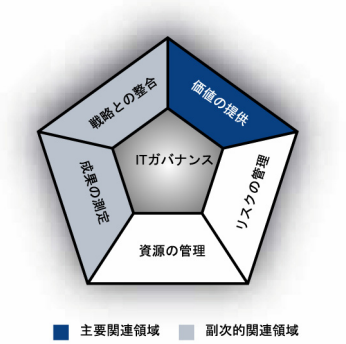
重点をおくべきコントロールは、速やかな対応、明確なエスカレーション手続、および解決策/傾向分析のプロフェッショナルな機能を持つサービスデスクの設置することである。

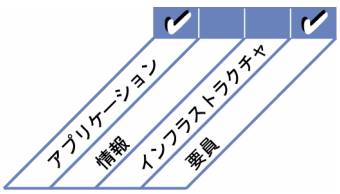
実現するための手段は、次の 3 項目である。

- サービスデスクの導入と運用
- 傾向のモニタリングと報告
- 明確なエスカレーション基準と手続の策定

その成果の測定指標は、次の 3 項目である。

- 一次サポートに対するユーザの満足度
- 合意/容認された期間内に解決したインシデントの割合
- 放棄呼率: サービスデスクが応答する前に、ユーザが問い合わせを放棄(切断)したコール(呼)の割合





コントロール目標 －詳細－

DS8 サービスデスクとインシデントの管理

DS8.1 サービスデスク
すべての問い合わせ、報告されたインシデント、およびサービスと情報に関する要求を登録、伝達、処理、分析し、ユーザと IT 部門とをつなぐ機能を果たすサービスデスクを設置する。該当サービス・レベル・アグリーメント(SLA)に関連する、合意されたサービスレベルに基づくモニタリングおよびエスカレーション手続が存在し、報告されたすべての課題を、インシデント、サービス要求、情報要求のいずれかに分類し、優先順位付けすることが可能になっている必要がある。サービスデスクとITサービスの質に対するエンドユーザの満足度を測定する。

DS8.2 顧客からの問い合わせの登録
問い合わせ、インシデント、サービス要求、情報要求を記録および追跡するための機能とシステムを確立する。このシステムは、インシデント管理、問題管理、変更管理、キャパシティ管理、および可用性管理といったプロセスと密接に連携する必要がある。インシデントはビジネスおよびサービスの優先度に基づいて分類し、該当する問題管理チームに転送する。顧客に対しては、それぞれの問い合わせへの対応状況を常に通知する。

DS8.3 インシデントエスカレーション
速やかに解決できないインシデントを、サービス・レベル・アグリーメント(SLA)で定められている制約の範囲内で適切にエスカレーションし、必要に応じてワークアラウンド(回避策)の提示を可能にする、サービスデスクの手続を確立する。インシデントの解決をどの IT グループが担当しているかにかかわらず、ユーザから報告されたインシデントの担当とライフサイクルのモニタリングは、確実にサービスデスクが担う。

DS8.4 インシデントのクローズ
顧客からの問い合わせへの対応終結ををタイムリーにモニタリングするための手続を確立する。インシデントの解決後、サービスデスクは根本原因が判明している場合はこの原因を記録し、実施された対応策に対して顧客の同意が得られていたことを確認する。

DS8.5 傾向分析
サービスデスクの活動に関する報告書を作成する。この報告書により、マネジメント層がサービスの成果と対応時間を測定して、傾向や再発性のある問題を特定できるようになり、サービスの継続的な改善が可能になる。

マネジメントガイドライン

DS8 サービスデスクとインシデントの管理

From	インプット
AI4	ユーザマニュアル、運用マニュアル、サポートマニュアル、技術マニュアル、および管理マニュアル
AI6	変更の承認
AI7	リリースされた構成管理アイテム
DS1	サービス・レベル・アグリーメント(SLA)とオペレーショナル・レベル・アグリーメント(OLA)
DS4	インシデント/災害のしきい値
DS5	セキュリティインシデントの定義
DS9	IT の構成/資産の詳細
DS10	既知の問題、既知のエラー、およびワークアラウンド(回避策)
DS13	インシデント情報

アウトプット	To						
サービス要求/変更要求	AI6						
インシデント報告	DS10						
プロセスの成果報告	ME1						
ユーザ満足度の調査報告	DS7	ME1					

RACI チャート

アクティビティ / 担当	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO (プロジェクト・マネジメント・オフィス)	コンプライアンス・監査・リスク・セキュリティ	サービスデスク/インシデント管理担当者
分類(重大度と影響力)およびエスカレーション(機能および階層)の手続の作成				C	C	C	C	C	C		C	A/R
インシデント/サービス要求/情報要求の発見と記録												A/R
問い合わせの分類、調査、および診断				I		C	C	C			I	A/R
インシデントの解決、回復、およびクローズ					I	R	R	R			C	A/R
ユーザへの通知(最新の進行状況など)				I	I							A/R
マネジメントレポートの作成	I			I	I	I			I		I	A/R

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R:Responsible) ②説明責任者(A:Accountable) ③協議先(C:Consulted)④報告先(I:Informed)

達成目標とその評価指標

アクティビティの達成目標
- サービスデスクの導入と運用
- 傾向のモニタリングと報告
- インシデント解決の優先順位とビジネス上の緊急課題との整合
- 明確なエスカレーション基準と手続の策定

プロセスの達成目標
- インシデントのタイムリーな分析、文書化、およびエスカレーション
- 問い合わせに対する正確かつタイムリーな対応
- インシデントと問い合わせの定期的な傾向分析の実施

IT の達成目標
- 提供サービスとサービスレベルに対するエンドユーザの満足の保証
- アプリケーションおよび技術的対応策の適切な利用と成果達成の保証
- 要求どおり IT サービスが使えることの保証

促進

促進

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 自動化ツールを使用して報告および記録されたインシデント/サービス要求の割合
- サービスデスクスタッフ1名あたりの年間の研修日数
- サービスデスクスタッフ1名あたりの問い合わせ処理件数(1 時間あたり)
- ローカルサポート(フィールドサポートや担当者の現地訪問)を必要とするインシデントの割合
- 未解決の問い合わせ数

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 総要求件数中、一次サポートでの解決割合
- 再調査を求められたインシデントの割合
- 放棄呼率
- 重大度別のインシデントの平均継続期間
- 電話および電子メール/Web での問い合わせに対する平均応答時間

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 一次サポート(サービスデスクまたは知識ベース)に対するユーザの満足度
- 合意/容認された期間内に解決したインシデントの割合

成熟度モデル

DS8 サービスデスクとインシデントの管理

「エンドユーザからの問い合わせ、質問、およびインシデントを確実に解決および分析し、IT システムの効果的な利用を実現する。」という IT に対するビジネス要件を満たす上で、「サービスデスクとインシデントの管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
ユーザからの問い合わせや課題報告を解決するためのサポートがまったく実施されていない。インシデント管理プロセスがまったく存在しない。組織が、対処すべき課題の存在さえ認識していない。

1 初期/その場対応
ユーザからの問い合わせに対応し、インシデントの解決を管理するための、ツールと要員が割り当てられたプロセスが必要であることをマネジメント層が認識している。ただし、標準化されたプロセスがなく、事後的なサポートのみ行われている。マネジメント層はユーザからの問い合わせ、インシデント、およびそれらの傾向をモニタリングしていない。確実に問題を解決するためのエスカレーションプロセスが規定されていない。

2 再現性はあるが直感的
サービスデスクの機能とインシデント管理プロセスの必要性が、組織全体で認識されている。問題解決の支援は、知識豊富な個人のネットワークにより、非公式な形で行われている。彼らは、何らかの共通ツールを利用してインシデントの解決を支援している。標準手続に関する正式な研修や話し合いが行われておらず、実行責任は各個人に委ねられている。

3 定められたプロセスがある
サービスデスクの機能とインシデント管理プロセスの必要性が認識され、対応が検討されている。手続が標準化および文書化されており、非公式な研修が実施され始めている。ただし、研修の受講と標準の遵守は各個人の判断に委ねられている。FAQ(よくある質問)とユーザガイドラインが策定されているが、周知されていないため各人はこれらの情報を自ら入手しなければならず、また、これらを完全に守っていない。問い合わせやインシデントは手作業で追跡され、個別にモニタリングされているが、正式な報告システムは存在しない。問い合わせやインシデントに対する対応の迅速さについて測定されていないため、インシデントが未解決のままになる可能性がある。ユーザに対し、問題とインシデントの報告先と報告方法が明確に周知されている。

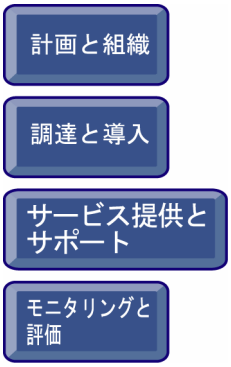
4 管理され、測定可能である
組織内のすべてのレベルでインシデント管理プロセスの効果が十分に理解されており、サービスデスクが適切な組織単位に設置されている。ツールと手法が、一元管理された知識ベースを活用して自動化されている。サービスデスクのスタッフと問題管理担当のスタッフが緊密に連携している。実行責任が明確化されており、有効性がモニタリングされている。インシデントの伝達、エスカレーション、および解決の手続が確立され、周知されている。サービスデスク要員は教育を受けており、業務に特化したソフトウェアを活用することでプロセスが改善されている。マネジメント層が、サービスデスクの成果測定のための KPI と KGI を策定している。

5 最適化
インシデント管理プロセスとサービスデスクが確立されており、適切に構成されている。十分な知識を備え、顧客を中心に考え、役立つサービスを提供することで、顧客サービス指向を実現している。KPI と KGI が体系的に測定および報告される。広範で包括的な FAQ が、知識ベースに欠くことのできない重要な要素となっている。ユーザがインシデントを自ら診断して解決するためのツールが用意されている。助言に一貫性があり、インシデントは体系的なエスカレーションプロセスにより迅速に解決される。マネジメント層が、インシデント管理プロセスとサービスデスクの成果統計を取得するための統合ツールを活用している。プロセスは、KPI と KGI の分析、継続的な改善、外部組織とのベンチマーク評価の結果を基に、業界のベストプラクティスのレベルにまで最適化されている。

コントロール目標 －概要－

DS9 構成管理

ハードウェアとソフトウェアの構成のインテグリティを確保するには、正確かつ網羅された構成管理用リポジトリの作成と保守が必要である。このプロセスには、初期構成情報の収集、ベースラインの設定、構成情報の検証と監査、および必要に応じた構成管理用リポジトリの更新が含まれる。効果的な構成管理により、システムの可用性が向上し、作業上の課題が最小限に抑えられ、課題を速やかに解決できるようになる。



IT プロセス: 構成管理のコントロール目標は、

IT インフラストラクチャ、資源、および能力を最適化し、IT 資産の詳細を把握することを、**ビジネス要件**とし、

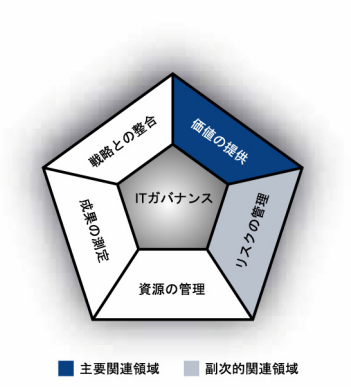
重点をおくべきコントロールは、資産構成の属性およびベースラインの正確かつ完全なリポジトリを作成および保守し、実際の資産構成と比較することである。

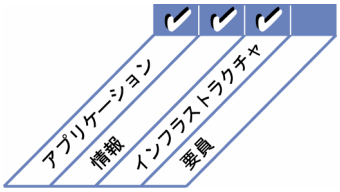
実現するための手段は、次の 3 項目である。

- すべての構成管理アイテムを含む集中管理リポジトリの作成
- 構成管理アイテムの識別と保守
- 構成データのインテグリティのレビュー

その成果の測定指標は、次の 3 項目である。

- 不適切な資産構成に起因するビジネス上のコンプライアンスに関する問題の数
- 構成管理用リポジトリと実際の資産構成の間で確認された相違の数
- リポジトリ内の、購入済みライセンスと所在不明ライセンスの割合





コントロール目標 －詳細－

DS9 構成管理

DS9.1 構成リポジトリとベースライン
構成管理アイテムの関連情報をすべて含む集中管理リポジトリを作成する。このリポジトリには、システムやサービスを運用、アクセス、および利用するためのハードウェア、アプリケーションソフトウェア、ミドルウェア、パラメータ、文書、手続、およびツールが含まれる。考慮すべき関連情報は命名規則、バージョン番号、およびライセンスの詳細である。すべてのシステムとサービスにおいて、構成管理アイテムのベースラインを、変更後、何らかの理由で元に戻す際のチェックポイントとして設定すべきである。

DS9.2 構成管理アイテムの識別と保守
次の手続を整備する。
- 構成管理アイテムとその属性の識別
- 新規/修正/削除済み構成管理アイテムの記録
- 構成管理用リポジトリにおける構成管理アイテム間のリレーションシップの識別と保守
- 現存する構成管理アイテムの構成管理用リポジトリへの追加更新
- 許可されていないソフトウェアの導入防止

これらの手続では、構成管理用リポジトリに対するすべての操作が適切に認可および記録されなければならない。また、これらの手続は変更管理および問題管理手続と適切に統合されていなければならない。

DS9.3 構成のインテグリティのレビュー
定期的に、必要に応じて適切なツールを用いて構成管理アイテムの状況をレビューおよび検証し、現在および過去の構成データが完全であることを確認して、実際の状況と比較する。個人所有やライセンスのないソフトウェア、あるいは契約済ライセンス数を超えたソフトウェアが存在していないかどうかを、ソフトウェア使用ポリシーに照らし合わせて定期的にレビューする。不備や逸脱がある場合は報告、対処および修正されなければならない。

マネジメントガイドライン

DS9 構成管理

From	インプット
AI4	ユーザマニュアル、運用マニュアル、サポートマニュアル、技術マニュアル、および管理マニュアル
AI7	リリースされた構成管理アイテム
DS4	IT 構成管理アイテムの重大度

アウトプット	To						
IT の構成/資産の詳細	DS8	DS10	DS13				
変更の適用対象とその方法	AI6						
プロセスの成果報告	ME1						

RACI チャート

アクティビティ / 担当	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ	構成管理担当者
構成管理の計画策定手続の作成					C	A	C	I	C		C	R
初期構成情報の収集とベースラインの確立						C	C	C			I	A/R
構成情報の検証と監査(未承認ソフトウェアの発見を含む)		I				A			I		I	A/R
構成管理用リポジトリの更新						R	R	R			I	A/R

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- すべての構成管理アイテムを含む集中管理リポジトリの作成
- 構成管理アイテムの識別と構成データの保守
- 構成データのインテグリティのレビュー

促進

プロセスの達成目標
- すべての資産、構成属性およびベースラインを含むリポジトリの作成
- 構成管理用リポジトリのインテグリティを保持
- 実際の資産構成がリポジトリのベースラインに準拠しているかどうかのレビュー

促進

IT の達成目標
- IT インフラストラクチャ、資源、および能力の最適化
- すべての IT 資産の所在明確化と保護

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 相違の特定から修正までに要する平均時間
- 不完全または失われた構成情報による相違の数
- 成果、セキュリティ、および可用性のサービスレベルに合致する構成管理アイテムの割合

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 構成管理用リポジトリと実際の資産構成の間で確認された相違の数
- リポジトリ内の、購入済みライセンスと所在不明ライセンスの割合

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 不適切な資産構成に起因するビジネス上のコンプライアンスに関する問題の数

成熟度モデル

DS9 構成管理

「IT インフラストラクチャ、資源、および能力を最適化し、IT 資産の詳細を把握する。」という IT に対するビジネス要件を満たす上で、「構成管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
マネジメント層は、IT インフラストラクチャ(ハードウェアやソフトウェアの構成)に関する報告および管理のプロセスを整備する利点について、正しく認識していない。

1 初期/その場対応
構成管理の必要性が認識されている。基本的な構成管理作業(ハードウェアとソフトウェアのインベントリーなど)が、各担当者の裁量に応じて実施されている。標準の実施基準が定められていない。

2 再現性はあるが直感的
マネジメント層が、IT 構成をコントロールする必要性を認識しており、構成情報を正確かつ網羅された状態で維持することの利点を理解しているが、技術要員の知識と力量に暗黙裡に依存している。構成管理ツールがある程度利用されているが、プラットフォーム間で異なる。また、標準の作業の実践基準が定められていない。構成データの内容が限定的であり、相互に関連するプロセス(変更管理と問題管理など)で使用されていない。

3 定められたプロセスがある
手続と作業の実践基準が文書化、標準化、および周知されている。ただし、研修への参加と標準の適用は個人の判断に委ねられている。プラットフォーム間を跨いで、同種の構成管理ツールが導入されつつある。手続からの逸脱が発見される可能性は低く、物理的な検証が一貫性のない方法で実施されている。装置とソフトウェアの変更に関する追跡の自動化がある程度は進められている。構成データは、相互に関連する複数のプロセスで使用されている。

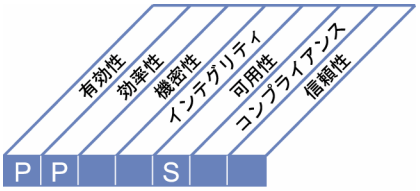
4 管理され、測定可能である
構成管理の必要性が組織内のすべてのレベルで認識されており、優れた実践基準の継続的な改善が図られている。手続と標準が周知され、研修に組み込まれている。逸脱についてモニタリング、追跡、および報告されている。自動化ツール(プッシュ技術など：ブロードキャストされる情報をクライアント側で解釈、表示する技術の総称)が標準の施行と安定性の向上に活用されている。構成管理システムはほとんどの IT 資産に対応しており、適切なリリース管理と配付コントロールを可能にしている。物理的検証に加え、例外分析が一貫して実施されており、例外の根本原因が調査されている。

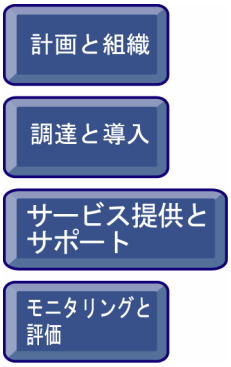
5 最適化
すべての IT 資産が、統合された構成管理システム内で管理されている。このシステムには、構成要素、構成要素間の相互関係、およびイベントに関するすべての必要情報が組み込まれている。構成データとベンダーカタログの整合性が取られている。相互に関連する複数のプロセスが完全に統合されている。これらのプロセスにおいては、構成データが自動化された手法で使用および更新される。ベースラインに関する監査レポートには、各装置の修理、保守、保証、アップグレード、および技術評価に必要不可欠な、ハードウェア/ソフトウェアに関するデータが記載されている。許可されていないソフトウェアのインストールを制限する規則が徹底して施行されている。マネジメント層は、アップグレード計画と技術更新能力に関する情報を含む分析報告から、修理とアップグレード実施の見通しを立てている。資産について追跡し、個々の IT 資産をモニタリングすることで、これらの資産を保護し、盗難、誤用、悪用を未然に防止している。

コントロール目標 －概要－

DS10 問題管理

効果的な問題管理を実施するには、問題を特定および分類し、根本原因を分析し、問題を解決する必要がある。問題管理プロセスには、改善のための提案事項の特定、問題の記録保持、および是正措置の状況のレビューも含まれる。効果的な問題管理プロセスにより、サービスレベルの向上、費用削減、および顧客(カスタマー)の利便性と満足度の向上を実現できる。





IT プロセス: 問題管理のコントロール目標は、

提供サービスとサービスレベルに対するエンドユーザの満足を確保し、対応策とサービスの提供における不備と手直し(リワーク)の必要性を削減することを、**ビジネス要件**とし、

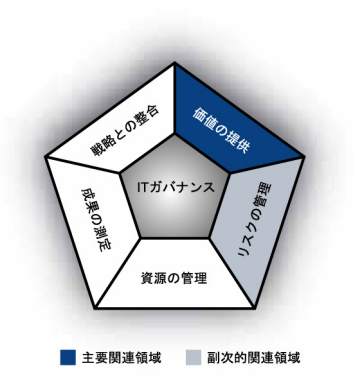
重点をおくべきコントロールは、運用上の問題の記録、追跡、および解決、すべての重大な問題の根本原因の調査、および特定された運用上の問題の解決策の策定することである。

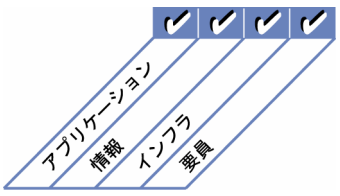
実現するための手段は、次の 3 項目である。

- 報告された問題に関する根本原因分析の実施
- 傾向の分析
- 問題の引受(オーナシップ)と解決の促進

その成果の測定指標は、次の 3 項目である。

- ビジネスに影響を及ぼす問題の再発数
- 要求された期間内に解決した問題の割合
- 継続中の問題に対して、重大度を基にした報告または更新の頻度





コントロール目標 －詳細－

DS10 問題管理

DS10.1 問題の特定と分類
インシデント管理の過程で特定された問題を報告、分類するためのプロセスを導入する。問題分類の手続はインシデント分類の手続に類似しており、カテゴリ、影響度、緊急度、優先度の決定が含まれる。問題は関連グループまたはドメイン(ハードウェア、ソフトウェア、サポートソフトウェアなど)に適切に分類しなければならない。これらのグループを、組織上の責任やユーザー/顧客ベースに合わせ、さらにサポートスタッフへの問題割り当ての基礎とする。

DS10.2 問題の追跡と解決
問題管理システムは、報告されたすべての問題を追跡、分析し、その根本原因を判別するための、適切な監査証跡機能を次の情報に対して提供する必要がある。
- 関連するすべての構成管理アイテム
- 未解決の問題とインシデント
- 既知のエラーとエラーの疑い

根本原因に対処する維持できる解決策を特定して実施し、確立されている変更管理プロセスに従い変更要求を提出する。解決プロセス全体にわたって、問題管理は、変更管理から問題やエラーの解決状況に関する報告を定期的に受ける必要がある。問題管理は、問題および既知のエラーのユーザサービスに対する継続的な影響をモニタリングする。この影響が深刻化した場合は、問題管理はその問題を適切な会議体にエスカレーションして、変更要求(RFC)の優先順位を上げてもらうか、または必要に応じて緊急の変更措置を実施する。問題解決の進捗状況は、サービス・レベル・アグリーメント(SLA)に照らし合わせてモニタリングする必要がある。

DS10.3 問題のクローズ
既知のエラーを成功裡に取除いたことを確認した後、または別の方法で問題を処理することをビジネス部門と合意した後、その問題の記録をクローズするための手続を整備、運用する。

DS10.4 変更管理、構成管理、および問題管理の統合
問題とインシデントの効果的な管理を保証するため、関連する変更管理、構成管理、および問題管理のプロセスを統合する。ビジネス上の改善よりも、問題の火消し作業に用いた作業量をモニタリングし、必要に応じて、問題を最小限に抑えるためにこれらのプロセスを改善する。

マネジメントガイドライン

DS10 問題管理

From	インプット
AI6	変更の承認
DS8	インシデント報告
DS9	IT の構成/資産の詳細
DS13	エラーログ

アウトプット	To
変更要求	AI6
問題の記録	AI6
プロセスの成果報告	ME1
既知の問題、既知のエラー、ワークアラウンド(回避策)	DS8

RACI チャート

アクティビティ / 担当	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO (プロジェクト・マネジメント・オフィス)	コンプライアンス・監査・リスク・セキュリティ	問題管理担当者
問題の特定と分類			I	I	C	A	C	C			I	R
根本原因の分析の実施						C		C				A/R
問題の解決					C	A	R	R		R	C	C
問題の状況の確認			I	I	C	A/R	C	C		C	C	R
改善のための提案事項の提示と関連する変更要求の作成					I	A	I	I		I		R
問題の記録保持					I	I		I			I	A/R

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- 問題管理担当者への十分な権限の付与
- 報告された問題に関する根本原因分析の実施
- 傾向の分析
- 問題とその解決工程の管理

促進

プロセスの達成目標
- 運用上の問題の解決までの記録と追跡
- すべての重大な問題の根本原因の調査
- 特定された運用上の問題の解決策の策定

促進

IT の達成目標
- 提供サービスとサービスレベルに対するエンドユーザの満足の確保
- 対応策とサービスの提供における不備と手直し(リワーク)の必要性の削減
- IT 目標の達成の保証

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 問題の記録から根本原因の特定までに要した平均時間
- 根本原因の分析が実施された問題の割合
- 問題の重大度に基づく、未解決の問題に関する報告または更新の頻度

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 記録および追跡された問題の割合
- 重大度別の(特定の期間内に)再発した問題の割合
- 要求された期間内に解決した問題の割合
- 重大度別の未解決/新規/解決済み問題の数
- 問題の特定から解決までに要した時間の平均と標準偏差
- 問題の解決からクローズまでに要した時間の平均と標準偏差

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- ビジネスに影響を及ぼす、繰り返し発生する問題の数
- 運用上の問題に起因する業務中断回数

成熟度モデル

DS10 問題管理

「提供サービスとサービスレベルに対するエンドユーザの満足を確保し、対応策とサービスの提供における不備と手直し(リワーク)の必要性を削減する。」というITに対するビジネス要件を満たす上で、「問題管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
問題とインシデントが区別されていないため、問題を管理する必要性が認識されていない。したがって、インシデントの根本原因の特定も行われていない。

1 初期/その場対応
問題を管理し、その根本にある原因を解決する必要性が、個人レベルで認識されている。知識豊富なキーとなるスタッフが、各々の専門分野に関連する問題について何らかの支援を行っているが、問題管理の実行責任は割り当てられていない。情報が共有されていないため、解決策を模索している間に新たな問題が発生し、生産性が失われる。

2 再現性はあるが直感的
IT 関連の問題をビジネス部門と情報サービス部門の両方で管理する必要性と効果について、広く認識されている。解決プロセスは、数名の主要なスタッフが問題の特定と解決の実行責任を担う、というレベルに達している。スタッフ間の情報共有は、非公式かつ事後的な方法で行われている。問題管理担当者が利用できる知識が十分に体系化されていないため、ユーザへのサービスレベルにばらつきや阻害が生じる。

3 定められたプロセスがある
効果的かつ統合された問題管理システムの必要性がマネジメント層の支援により受け入れられ、明らかにされている。人員補充および研修のための予算が確保されている。問題解決とエスカレーションのプロセスが標準化されている。問題とその解決策の記録と追跡は、一元管理されていない任意のツールを用いて、対応チーム内で断片的に行われている。問題管理の基準や標準は確立されているが、そこからの逸脱行為は、検知されない可能性がある。スタッフ間の情報共有は、正式かつ事前に行われている。マネジメント層によるインシデントのレビューや、問題特定および解決の分析は、限定的かつ非公式に行われている。

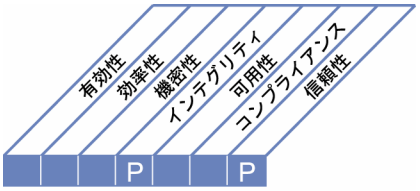
4 管理され、測定可能である
組織内のすべてのレベルで問題管理プロセスが理解されている。実行責任とオーナシップが明確に割り当てられている。手法や手続は文書化され、周知されており、その有効性が測定されている。問題の大半が特定、記録、報告されており、解決策が実施されている。この仕組みが価値ある資産として見なされ、IT 目標の達成と IT サービスの改善に大きく寄与するものとして捉えられているので、その知識とノウハウが培われ、維持され、より高められている。問題管理は、インシデント管理、変更管理、可用性管理、構成管理などの相互に関連するプロセスと適切に統合されており、データ管理、施設管理、および運用管理の面で顧客の支援につながっている。問題管理プロセスにおける KPI と KGI について合意が得られている。

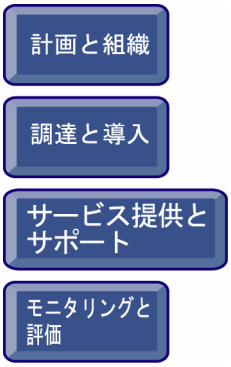
5 最適化
問題管理プロセスは、先見的で未然防止が可能なレベルにまで発展しており、IT 目標の達成に貢献している。問題が予期され、未然に防止されている。定期的にベンダーや専門家と連絡を取り合うことで、過去発生した問題や将来予想される問題のパターンに関する知識が維持されている。問題と解決策の記録、報告、および分析が自動化されており、構成データ管理と十分に統合されている。KPI と KGI が一貫して測定されている。大半のシステムは自動検知および警告メカニズムを備えており、継続的に追跡および評価されている。問題管理プロセスは、KPI と KGI の分析に基づいて、継続的な改善を目指して分析されており、利害関係者への報告が行われている。

コントロール目標 －概要－

DS11 データ管理

効果的なデータ管理を実施するには、データ要件を特定する必要がある。データ管理プロセスには、メディアライブラリ、データのバックアップと復元、およびメディアの適切な廃棄に関する管理手続の確立も含まれる。効果的なデータ管理は、ビジネスデータの質、適時性、および可用性の保証に有用である。





IT プロセス: データ管理のコントロール目標は、

情報の利用を最適化し、要求に応じた情報の可用性を保証することを、**ビジネス要件**とし、

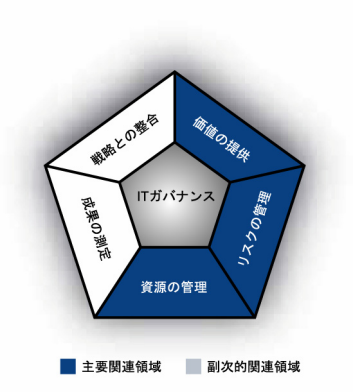
重点をおくべきコントロールは、データのインテグリティ、正確性、可用性、および保護を維持することである。

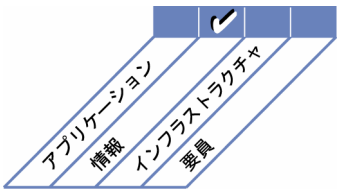
実現するための手段は、次の 3 項目である。

- データのバックアップと復元のテスト
- オンサイトおよび遠隔地におけるデータ保管の管理
- データおよび機器の安全な廃棄

その成果の測定指標は、次の 3 項目である。

- データの可用性に対するユーザの満足度
- 成功したデータ復元の割合
- メディア廃棄後に機密データが取得されたインシデントの件数





コントロール目標 －詳細－

DS11 データ管理

DS11.1 データ管理におけるビジネス要件
ビジネス部門から予定された原始帳票が受領され、ビジネス部門から受領したすべてのデータが処理され、ビジネス部門が必要とするアウトプットがすべて準備および提供され、必要とされる再開と再処理に対応される。これらのことを保証する手配をする。

DS11.2 データの保管および保持の調整
データの保管とアーカイブの手続を定義および導入し、データがアクセス可能および利用可能である状態を確保する。保管とアーカイブの手続では、データの取り出しに関する要件、費用効率、および継続的なインテグリティとセキュリティ上の要件を考慮する必要がある。暗号化と認証に使用されるデータ(暗号鍵、証明書)と同様に、文書、データ、アーカイブ、プログラム、報告書、およびメッセージ(受信/送信)に関する法令要件とビジネス要件を満たすため、保管および保持に関する手配を行う。

DS11.3 メディアライブラリ管理システム
オンサイトメディアの一覧を保守し、メディアの有用性とインテグリティを確保するための手続を定義および導入する。これらの手続には、指摘されたどんな相違に対しても、タイムリーなレビューとフォローアップのための手続を規定する必要がある。

DS11.4 廃棄
機器またはメディアを廃棄または別の用途とする場合に、このような機器やメディアに保存されている機密データやソフトウェアへのアクセスを防止するための手続を定義および導入する。このような手続により、削除または廃棄として識別されたデータへのアクセスが不可能であることを保証する必要がある。

DS11.5 バックアップと復元
ビジネス要件および継続計画に沿った、システム、データ、および文書のバックアップと復元の手続を策定および導入する。バックアップ手続に対するコンプライアンスについて検証し、完全な復元が可能かどうか、および復元に要する時間を検証する。バックアップメディアと復元プロセスをテストする。

DS11.6 データ管理におけるセキュリティ上の要件
データおよび機密メッセージの受信、処理、物理的保管、および出力に関連するセキュリティ要件を特定し、それを適用するための手配を行う。これには、物理的記録、データ伝送、および遠隔地で保管されているすべてのデータが含まれる。

マネジメントガイドライン

DS11 データ管理

From	インプット
PO2	データディクショナリ、採用したデータの分類方法
AI4	ユーザ、運用、サポート、技術、および管理の各マニュアル
DS1	オペレーショナル・レベル・アグリーメント(OLA)
DS4	バックアップの保管と保護に関する計画

アウトプット	To
プロセスの成果報告	ME1
データ管理に関するオペレータ向け指示書	DS13

RACI チャート

担当

アクティビティ	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
データの保管および保持に関する要件を取り入れた手続の定義				A	I	C	R				C
メディアライブラリの管理手続の定義、維持、および導入				A		R	C	C	I		C
メディアと機器の安全な廃棄手続の定義、保守、および導入				A	C	R			I		C
計画に基づくデータのバックアップ				A		R					
データ復元のための手続の定義、維持、および導入				A	C	R	C	C			I

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- データのバックアップと復元のテスト
- オンサイトおよび遠隔地におけるデータ保管の管理
- データおよび機器の安全な廃棄

促進

プロセスの達成目標
- 保管データのインテグリティ、正確性、有効性、および可用性の維持
- メディア廃棄時のデータのセキュリティ確保
- 保管メディアの効果的な管理

促進

IT の達成目標
- 情報利用の最適化
- 重要かつ機密の情報が、当該情報へのアクセスを許可されていないユーザに開示されないようにすること
- IT の法令へのコンプライアンスの確保

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- バックアップメディアのテスト実施頻度
- データ復元に要する平均時間

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 成功したデータ復元の割合
- メディア廃棄後に機密データが読み取られたインシデントの件数
- 記憶装置の容量不足に起因するダウンタイムの発生件数またはデータのインテグリティに関するインシデントの件数

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- ビジネスプロセスにとって重要なデータを復元できない状況の発生回数
- データ可用性に対するユーザの満足度
- 保管管理の問題に起因する法規制違反のインシデント件数

成熟度モデル

DS11 データ管理

「情報の利用を最適化し、要求に応じた情報の可用性を保証する。」という IT に対するビジネス要件を満たす上で、「データ管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
データが企業の資源および資産であるとは認識されていない。データのオーナシップが割り当てられていないか、データ管理の説明責任者が存在しない。データの品質およびセキュリティレベルが非常に低いか、またはまったく確保されていない。

1 初期/その場対応
組織が、適切なデータ管理の必要性を認識している。データ管理に関するセキュリティ要件は、その場に応じて具体的なアプローチがとられており、正式な周知手続が整備されていない。データ管理に関する具体的な研修が実施されていない。データ管理に関する責任の所在が明確でない。バックアップ/復元手続と廃棄方法については整備されている。

2 再現性はあるが直感的
適切なデータ管理の必要性が組織全体で認識されている。上位層におけるデータのオーナシップの割り当てが行われるようになってきている。主要な人員によってデータ管理におけるセキュリティ要件が文書化されている。IT 部門内で、データ管理の主要な活動(バックアップ、復元、廃棄)に対してある程度のモニタリングが実施されている。データ管理の実行責任が、主要な IT スタッフに非公式に割り当てられている。

3 定められたプロセスがある
IT 部門内および組織全体でのデータ管理の必要性が理解され、受け入れられている。データ管理の実行責任が規定されている。責任のあるグループに対してデータのオーナシップが割り当てられており、インテグリティとセキュリティはこの責任のあるグループによりコントロールされる。IT 部門内でデータ管理手続が正式に決められており、機器のバックアップ/復元および廃棄のための何らかのツールが利用されている。データ管理に対してある程度のモニタリング体制が整備されている。基本的な成果達成指標が策定されている。データ管理スタッフの研修が整備されつつある。

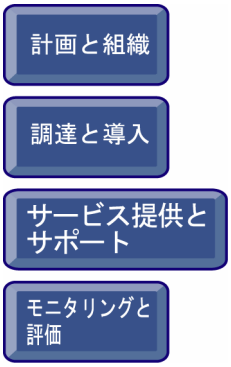
4 管理され、測定可能である
データ管理の必要性が組織内で理解され、必要な対応を取ることが受け入れられている。データのオーナシップと管理の責任が組織内で明確に定義され、割り当てられており、周知されている。手続が正式に決められて広く認識されており、知識が共有されている。現存するツールが利用されるようになってきている。達成目標および成果達成指標は、顧客との合意が得られており、適切に定義されたプロセスを通してモニタリングされている。データ管理スタッフのための正式な研修が実施されている。

5 最適化
データ管理と必要な対応すべてに関する理解の必要性について、組織内で理解され、受け入れられている。将来的なニーズと要件について事前に調査されている。データのオーナシップと管理の責任が明確に規定され、組織全体で周知され、タイムリーに更新されている。手続が正式に決められ、広く認識されており、知識の共有が標準の実践基準として実施されている。高度なツールが使用され、データ管理が最大限に自動化されている。達成目標および成果達成指標は、顧客との合意が得られており、ビジネス目標と関連付けられており、適切に定義されたプロセスを通して一貫してモニタリングされている。常に改善の検討が行われている。データ管理スタッフへの研修が仕組みとして定着している。

コントロール目標 －概要－

DS12 物理的環境の管理

コンピュータ機器と要員を保護するには、適切に設計および管理されている物理的施設が必要である。物理的環境を管理するプロセスには、物理的なサイト要件の定義、適切な施設の選定、および環境要因をモニタリングし物理的アクセスを管理するための効果的なプロセスの設計が含まれる。物理的環境を効果的に管理することで、コンピュータ機器と要員にかかわる障害に起因するビジネスの中断が減少する。



IT プロセス: 物理的環境の管理のコントロール目標は、

コンピュータ資産とビジネスデータを保護し、ビジネス中断のリスクを最小限に抑えることを、**ビジネス要件**とし、

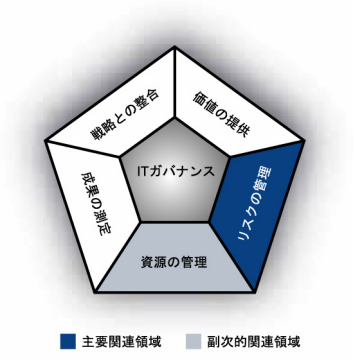
重点をおくべきコントロールは、IT 資産を、不正アクセス、損傷、盗難から保護する適切な物理的環境の導入および維持することである。

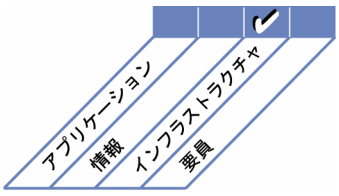
実現するための手段は、次の 2 項目である。

- 物理的なセキュリティ対策の実施
- 施設の選定と管理

その成果の測定指標は、次の 3 項目である。

- 物理的環境にかかわるインシデントに起因するダウンタイム
- 物理的なセキュリティ侵害または障害に起因するインシデントの件数
- 物理的リスクの評価とレビューの実施頻度





コントロール目標 －詳細－

DS12 物理的環境の管理

DS12.1 サイトの選定と配置
ビジネス戦略に関連付けられた技術戦略を支援する IT 機器のための物理的サイトを定義および選定する。サイトの選定と配置設計では、関連法令(労働安全衛生に関する規制など)を考慮する一方で、自然災害/人的災害に関連するリスクを考慮する必要がある。

DS12.2 物理的なセキュリティ対策
ビジネス要件に従って物理的セキュリティ対策を策定および導入する。物理的セキュリティ対策には、セキュリティ境界線、セキュリティゾーン、重要機器の配置、および受け渡しエリアの設定などが含まれるが、これだけに限定されるものではない。特に、重要な IT 業務が運用されていることを目立たないようにする必要がある。モニタリングの責任と、物理的セキュリティに関するインシデントの報告および解決のための手続を定める必要がある。

DS12.3 物理的アクセス
ビジネス上の必要性に基づき、緊急事態発生時を含めた施設、建物、敷地への立ち入りの許可、制限、取り消し手続を定義および導入する。施設、建物、敷地への立ち入りに際しては、正当性の評価、認可、記録、およびモニタリングを行う必要がある。これは、施設に立ち入るすべての人員(スタッフ、臨時スタッフ、取引先、ベンダー、訪問客、およびその他のサードパーティ全員)に適用される。

DS12.4 環境的要因からの保護
環境的要因から保護するための対策を確立および導入する。環境をモニタリングおよびコントロールするための特別な設備やデバイスを導入する必要がある。

DS12.5 物理的施設の管理
法律、規制、技術要件、ビジネス要件、ベンダーの仕様、および安全衛生ガイドラインに従って、電源装置や通信機器などの設備を管理する。

マネジメントガイドライン

DS12 物理的環境の管理

From	インプット
PO2	採用したデータの分類方法
PO9	リスク評価
AI3	物理的環境要件

アウトプット	To
プロセスの成果報告	ME1

RACI チャート

アクティビティ	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ
要求される物理的保護レベルの定義					C	A/R	C				C
サイト(データセンター、オフィスなど)の選定と委託	I	C	C	C	C	A/R	C		C	C	C
物理的環境に関する対策の実施					I	A/R	I	I			C
物理的環境の管理(保守、モニタリング、報告を含む)						A/R	C				
物理的アクセスを許可および維持する手続の定義および導入				C	I	A/R	I	I	I		C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- 物理的セキュリティ対策の導入
- 施設の厳密な選定と管理

促進

プロセスの達成目標
- IT インフラストラクチャおよび資源に適した物理的環境の整備と保守
- アクセス不要な人員の物理的環境へのアクセス制限

促進

IT の達成目標
- エラー、意図的な攻撃、または災害で生じた障害に対する、IT サービスおよびインフラストラクチャの抵抗力・回復力の保証
- 重要かつ機密度の高い情報が、当該情報へのアクセスを許可されていないユーザに開示されないことを保証
- IT サービスの中断または変更が及ぼすビジネスへの影響の極小化を保証
- すべての IT 資産の責任の所在の明確化と適切な保護

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 担当要員に対して安全性、セキュリティ、および施設に関する対策についての研修を実施する頻度
- 安全性、セキュリティ、および施設に関する対策についての研修を受けた担当要員の割合
- 前年のリスク低減テストの実施回数
- 物理的リスクの評価とレビューの実施頻度

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 物理的なセキュリティ侵害または障害に起因するインシデントの件数
- コンピュータ施設への不正アクセスインシデントの件数

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 物理的環境に関するインシデントに起因するダウンタイム
- 物理的環境に起因する損害発生件数
- 物理的環境に関するインシデントに起因するセキュリティ障害

成熟度モデル

DS12 物理的環境の管理

「コンピュータ資産とビジネスデータを保護し、ビジネス中断のリスクを最小限に抑える。」というITに対するビジネス要件を満たす上で、「物理的環境の管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
施設の保護またはコンピュータ資源への投資を保護する必要性が認識されていない。防火、粉じん、電力供給、高温多湿などの環境的要因について、モニタリングもコントロールも実施されていない。

1 初期/その場対応
組織が、人災や自然災害から資源や要員を保護する適切な物理的環境の整備に関するビジネス上の要件について認識している。施設と機器の管理について、主要な人員のスキルと能力に依存している。スタッフは制限なく施設内を移動できる。マネジメント層が、施設環境のコントロール状況とスタッフの移動についてモニタリングしていない。

2 再現性はあるが直感的
運用担当者により、環境のコントロールが導入およびモニタリングされている。物理的セキュリティの確保は非公式なプロセスであり、物理的施設のセキュリティについて高い意識を持つ少数の従業員により実施されている。施設保守手続が十分に文書化されておらず、数名の人員による優れた実践方法に依存している。物理的セキュリティの達成目標が正式な標準に基づいておらず、マネジメント層はセキュリティ目標の達成を保証できない。

3 定められたプロセスがある
コンピュータ環境のコントロールを維持する必要性が組織内で理解され、対応が検討されている。環境のコントロール、予防的保守、および物理的セキュリティは、予算項目としてマネジメント層により承認されており、マネジメント層により追跡される。アクセス制限が適用されており、許可された要員のみがコンピュータ関連施設にアクセスできる状態になっている。訪問者については、記録が残され、個別にスタッフが同行する。物理的施設は目立たず、容易に特定できないようになっている。安全衛生関連の規制の遵守状況が所轄機関によりモニタリングされている。安全衛生上のリスクに対して保険をかけているが、保険関連費用を低減させるための努力は最小限にとどまっている。

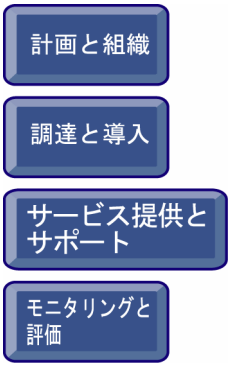
4 管理され、測定可能である
コンピュータ環境のコントロールを維持する必要性が十分に理解されており、組織構造や予算配分にも明確に反映されている。環境的セキュリティおよび物理的セキュリティの要件が文書化されており、施設へのアクセスが厳しくコントロールおよびモニタリングされている。責任とオーナシップが定められており、周知されている。施設担当スタッフが、緊急事態発生時の対応および安全衛生に関わる実践基準について十分な教育を受けている。施設へのアクセスを制限し、環境的要因および安全要因に対応するための標準化されたコントロール方法が整備されている。マネジメント層は、コントロールの有効性と確立された標準への準拠状況をモニタリングしている。マネジメント層は、コンピュータ環境の管理の成果を測定するための KPI と KGI を策定している。コンピュータ資源の復元可能性が組織のリスク管理プロセスに組み込まれている。統合された情報を利用して、保険の対象とする範囲および関連費用が最適化されている。

5 最適化
組織のコンピュータ環境の維持に必要な施設に関して合意された長期計画が存在する。すべての施設について標準が定められている。この標準では、サイトの選定、施設構造、防護、人的安全保護、機械系統、電気系統、環境要因(火災、落雷、洪水など)に対する保護が扱われている。すべての施設の一覧が作成され、組織の現行のリスク管理プロセスに従い分類されている。業務上の必要性に応じて施設へのアクセスが厳しくコントロールされ、継続的にモニタリングされている。また、訪問者が立ち入る際は、必ずスタッフが同行する。専用の装置によって環境がモニタリングおよびコントロールされており、この装置が設置されている部屋は「無人」になっている。KPI と KGI が一貫して測定されている。予防的保守プログラムによりスケジュールが遵守され、機密機器に対して定期的なテストが実施されている。施設に関する戦略と標準は、IT サービスの可用性の達成目標と整合されており、業務継続計画および危機管理と統合されている。マネジメント層は、KPI と KGI を用いて施設のレビューと最適化を継続的に実施しており、ビジネスへの貢献度の一層の向上を図っている。

コントロール目標 －概要－

DS13 オペレーション管理

データを完全かつ正確に処理するには、データ処理を効果的に管理し、ハードウェアを保守する必要がある。このプロセスには、計画された処理の効果的管理、機密性を有する出力の保護、インフラストラクチャのモニタリング、およびハードウェアの予防的保守のためのオペレーションポリシーおよび手続の策定が含まれる。効果的なオペレーション管理により、データのインテグリティが維持され、業務の遅延および IT 運用費用が削減される。



IT プロセス: オペレーション管理のコントロール目標は、

データのインテグリティを維持し、IT インフラストラクチャのエラーや障害に対する抵抗力・回復力を保証することを、**ビジネス要件**とし、

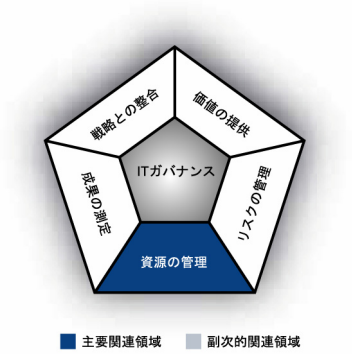
重点をおくべきコントロールは、計画されたデータ処理の運用サービスレベルを達成し、機密性を有する出力を保護し、インフラストラクチャをモニタリングおよび保守することである。

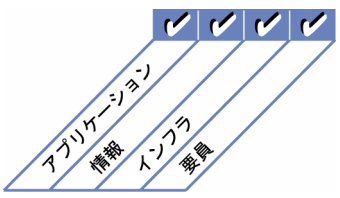
実現するための手段は、次の 2 項目である。

- 合意されたサービスレベルと定義された方針に従った IT 環境の運用
- IT インフラストラクチャの保守

その成果の測定指標は、次の 3 項目である。

- 運用上のインシデントの影響を受けるサービスレベルの数
- 運用上のインシデントに起因する予定外のダウンタイムの時間数
- 予防的保守スケジュールに組み込まれているハードウェア資産の割合





コントロール目標 －詳細－

DS13 オペレーション管理

DS13.1 オペレーション手続と指示
IT オペレーションの標準手続を策定、導入、保守し、オペレーション担当スタッフがすべての関連オペレーション任務を熟知しているようにする。継続的なオペレーションを保証するために、オペレーション手続はシフト交代時の引継ぎ項目(アクティビティ、状況に関する最新情報、オペレーションの問題、エスカレーション手続、および現行の責任に関する報告)が含まれている必要がある。

DS13.2 業務のスケジュール策定
業務、プロセス、任務のスケジュールを最も効率的な順序で構成し、ビジネス要件を満たすために処理能力と稼働率を最大にしながら、ジョブ、プロセス、タスクのスケジュールを最も効率的な順序で構成する。初期スケジュールとスケジュール変更は、ともに認可を得る必要がある。標準のジョブスケジュールからの逸脱を特定、調査、および承認するための手続を整備する必要がある。

DS13.3 IT インフラストラクチャのモニタリング
IT インフラストラクチャおよび関連イベントをモニタリングするための手続を定義し、導入する。運用および運用を取り巻き支援する他の活動を時系列に再構成、レビュー、および調査可能にするために、十分な時系列情報が運用ログに保管されることを保証する。

DS13.4 機密文書と出力デバイス
特殊書類、有価証券、特殊目的のプリンタやセキュリティトークンなどの機密性を有する IT 資産について、適切な物理的保護策、責任割り当て、および在庫管理手続を確立する。

DS13.5 ハードウェアの予防的保守
インフラストラクチャのタイムリーな保守を保証するための手続を定義し導入する。これにより、障害やパフォーマンス低下の発生頻度と影響を低減できる。

マネジメントガイドライン

DS13 オペレーション管理

From	インプット
AI4	ユーザ、運用、サポート、技術、および管理の各マニュアル
AI7	システムの本番環境への移行およびソフトウェアリリースおよび配付計画
DS1	サービス・レベル・アグリーメント(SLA)とオペレーショナル・レベル・アグリーメント(OLA)
DS4	バックアップの保管と保護に関する計画
DS9	IT の構成/資産の詳細
DS11	データ管理に関するオペレータ向け指示書

アウトプット	To
インシデント情報	DS8
エラーログ	DS10
プロセスの成果報告	ME1

RACI チャート

アクティビティ / 担当	CEO	CFO	企業幹部	CIO	ビジネス プロセス オーナー	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス、監査、リスク、セキュリティ
オペレーション手続(マニュアル、チェックリスト、シフト交代計画、引き継ぎ文書、エスカレーション手続など)の定義/変更						A/R					I
作業負荷とバッチジョブのスケジュール策定					C	A/R	C	C			
インフラストラクチャと処理のモニタリングおよび問題の解決						A/R					I
物理アウトプット(紙、メディアなど)の管理と保護						A/R					C
スケジュールとインフラストラクチャへの修正または変更の適用					C	A/R	C	C			C
認証デバイスを侵害、損失、盗難から保護するためのプロセスの導入/確立				A		R			I		C
予防的保守のスケジュール策定と実施						A/R					

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- 定義されている方針および厳密な監視を踏まえた、合意されたサービスレベルに従った IT 環境の運用
- IT インフラストラクチャの予防的保守とモニタリング

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- オペレーション要員 1 名あたりの年間研修日数
- 予防的保守スケジュールに組み込まれているハードウェア資産の割合
- 自動化された作業スケジュールの割合
- 運用手続の更新頻度

促進

プロセスの達成目標
- 運用手続の定義と、合意されたサービスレベルとの整合性の確保
- 計画された処理と特別な要求の処理を完全に行う
- 機密情報に対する物理的保護策の施行

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- オペレーション手続からの逸脱に起因するダウンタイムインシデントと遅延の件数
- 計画された作業と要求のうち、予定どおりに完了しなかったものの割合
- 不適切な手続に起因するダウンタイムインシデントと遅延の件数

促進

IT の達成目標
- エラー、意図的な攻撃、または災害で生じた障害に対する、IT サービスおよびインフラストラクチャの抵抗力・回復力の保証
- 提供されるサービスとサービスレベルに対するエンドユーザが満足することへの保証
- 要求に応じて IT サービスを使用可能であることの保証

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 運用上のインシデントの影響を受けるサービスレベルの数
- 運用上のインシデントに起因する予定外のダウンタイムの時間数

成熟度モデル

DS13 オペレーション管理

「データのインテグリティを維持し、IT インフラストラクチャのエラーや障害に対する抵抗力・回復力を確保する。」というITに対するビジネス要件を満たす上で、「オペレーション管理」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
組織は、基本的な IT サポートおよびオペレーション活動の確立のために時間も資源も投入していない。

1 初期/その場対応
IT サポート機能を構築する必要性を組織が認識している。標準手続はほとんど確立されておらず、オペレーション活動は事実上、事後的に行われている。オペレーションプロセスの大部分は非公式に計画され、処理要求は事前検証なしで受け入れられている。ビジネスプロセスを支援するコンピュータ、システム、およびアプリケーションの中断、遅延、および使用不能状態が頻繁に発生する。従業員が資源を利用できるまで待機している間に、時間が失われている。アウトプットメディアが予期しない場所で発見されたり、見つからなかったりする場合がある。

2 再現性はあるが直感的
IT サポート機能を提供する上で IT オペレーション活動が果たす主要な役割について、組織が認識している。ツール導入のための予算は、場合に応じて割り当てられている。IT サポートオペレーションは非公式かつ直感的に行われている。個人的なスキルや能力に大きく依存している。何をいつ、どのような順序で実行するべきかという指示が文書化されていない。何らかのオペレータ研修が実施されており、正式なオペレーション標準もいくつか存在する。

3 定められたプロセスがある
コンピュータオペレーション管理の必要性が組織内で理解され、受け入れられている。資源が配分されており、ある程度の実地研修(OJT)が実施されている。定型業務について正式に定義、標準化、文書化、および周知されている。イベントと完了タスクの結果が記録されているが、そのすべてがマネジメント層に報告されるわけではない。自動スケジュールツールなどのツールが導入され、オペレータの介入が削減されている。オペレーションに新規業務を組み込むためのコントロールが導入されている。予定外のイベントの発生を削減するための正式なポリシーが策定されている。ベンダーとの保守サービス契約は、事実上、依然として非公式なものである。

4 管理され、測定可能である
コンピュータオペレーションおよびサポートの実行責任が明確に定められており、オーナシップが割り当てられている。設備投資と人的資源への予算投入を通して、オペレーションが支援されている。研修が正式になっており、継続的に実施されている。スケジュールと業務が文書化され、IT 部門とビジネス顧客の両方に周知されている。標準化された成果目標に対する合意と定められたサービスレベルに基づいて、日常的な活動を測定およびモニタリングできる。確立されている水準からの逸脱が生じた場合は、速やかに対処および是正される。マネジメント層は、コンピュータ資源の使用状況と作業または割り当てられている業務の完了状況をモニタリングしている。継続的な改善の手段として、プロセスの自動化レベルの向上のための継続的な努力がなされている。ベンダーとの間で正式な保守サービス契約が締結されている。エラーや障害の原因分析により、問題管理、キャパシティ管理および可用性管理のプロセスとの完全な整合が図られている。

5 最適化
IT サポートオペレーションが効果的、効率的であり、生産性の低下を最小限に抑えてサービスレベルの要件を達成できるだけの十分な柔軟性を備えている。IT オペレーションの管理プロセスが標準化および文書化され、知識ベースに蓄積されており、継続的な改善が義務付けられている。システムを支援する自動化プロセスはシームレスに運用されており、環境の安定性の維持に貢献している。すべての問題と障害について、根本原因を特定するための分析が行われている。変更管理担当者との会合を定期的に行うことで、変更を作業スケジュールにタイムリーに組み込むことを保証する。装置の使用年数と機能不良の兆候の有無について、ベンダーと協力した分析が行われており、多くの場合予防的保守が可能になっている。

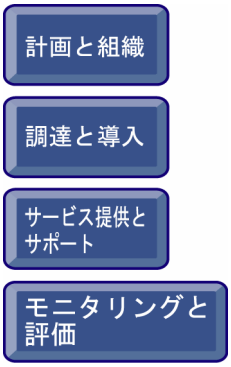
モニタリングと評価

ME1 IT 成果のモニタリングと評価
ME2 内部統制のモニタリングと評価
ME3 規制に対するコンプライアンスの保証
ME4 IT ガバナンスの提供

コントロール目標 －概要－

ME1 IT 成果のモニタリングと評価

IT 成果を効果的に管理するには、モニタリングプロセスが必要である。このプロセスには、妥当な成果達成指標の定義、体系的かつタイムリーな成果報告、および成果目標から逸脱した場合の迅速な対応が含まれる。指針やポリシーに沿って正しい運用が行われていることを確認するため、モニタリングが必要である。



IT プロセス: IT 成果のモニタリングと評価のコントロール目標は、

ガバナンス要件に従った、IT の費用、便益、戦略、ポリシー、およびサービスレベルの透明性の確保と理解を、**ビジネス要件**とし、

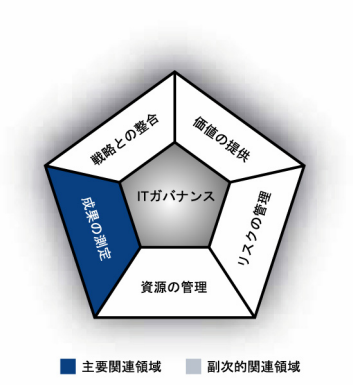
重点をおくべきコントロールは、プロセス指標のモニタリングと報告を行い、成果改善策を明確にし、実施することである。

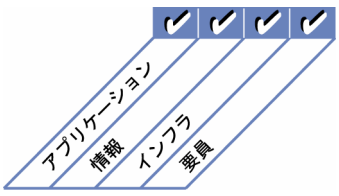
実現するための手段は、次の 2 項目である。

- プロセスの成果報告の照合と、マネジメント層への報告への組み込み
- 合意された目標達成レベルに照らした成果のレビューと、必要な是正措置の実施

その成果の測定指標は、次の 3 項目である。

- 成果報告に対するマネジメント層やガバナンス主体の満足度
- モニタリング活動の結果を受けて実施された改善策の件数
- モニタリング対象となっている重要プロセスの割合





コントロール目標 －詳細－

ME1 IT 成果のモニタリングと評価

ME1.1 モニタリングアプローチ
マネジメント層は、概括的なモニタリングフレームワークとモニタリングアプローチを確実に確立する必要がある。このフレームワークとアプローチは、企業のポートフォリオ管理とプログラム管理の各プロセス、および IT 能力と IT サービスの提供に固有の各プロセスの成果に対する IT の貢献度をモニタリングする対象範囲、従うべき方法論、およびプロセスを定義する。モニタリングフレームワークは、企業の成果管理システムに組み込む必要がある。

ME1.2 モニタリングデータの定義と収集
IT 部門のマネジメント層は、ビジネス部門と連携して、バランスの取れた成果目標、測定指標、達成目標、およびベンチマークを確実に定義し、ビジネス部門とその他の利害関係者の承認を得る。成果達成指標には、以下の内容が含まれなければならない。
- 財務をはじめとするビジネスへの貢献度
- ビジネス戦略計画と IT 戦略計画に照らした成果
- 法規制に関わるリスクとコンプライアンス
- 内部および外部ユーザの満足度
- 開発とサービス提供を含む重要 IT プロセス
- 新規技術や再利用可能インフラストラクチャの導入、ビジネス部門および IT 部門の人的スキルの向上など、将来指向の活動

達成目標に対する進捗を報告するため、タイムリーかつ正確なデータの収集が可能なプロセスを確立しなければならない。

ME1.3 モニタリング方法
モニタリングプロセスには、IT 成果の全体像を簡潔に示し、企業のモニタリングシステムに適合する方法(バランススコアカードなど)の導入が必要である。

ME1.4 成果評価
達成目標に照らして成果を定期的にレビューし、原因分析を行って、根本的な原因を解決する是正措置を講じる。

ME1.5 取締役会およびマネジメント層への報告
上級マネジメント層によるレビューのために、特定された目標に対して、組織としてどこまで到達しているのかについてのマネジメントレポートを作成する。報告は、特に、IT 関連の投資プログラムに関する企業のポートフォリオの成果、個々のプログラムのサービスレベル、およびその成果に対する IT の貢献度に的を絞る。計画された目標の達成度合い、成果物、達成された成果目標、および軽減されたリスクについて状況報告に含める必要がある。レビューでは、期待された成果からの逸脱が見られる場合はそのすべてを特定し、マネジメント層による実行策を実行し、報告する必要がある。

ME1.6 是正措置
成果のモニタリング、評価、および報告に基づいて必要な是正措置を特定し、実行する。これには、すべてのモニタリング、報告、および評価について、以下によるフォローアップが含まれる。
- マネジメント層の対応についての、レビュー、協議、および確定
- 是正措置に関する実行責任の割り当て
- 実施された是正措置の結果の追跡

マネジメントガイドライン

ME1 IT 成果のモニタリングと評価

From	インプット
PO5	費用便益報告
PO10	プロジェクトの成果報告
AI6	変更状況報告
DS1-13	プロセスの成果報告
DS8	IT ユーザ満足度報告
ME2	IT コントロールの有効性に関する報告
ME3	IT に関わるアクティビティにおける、外部法規制および規則へのコンプライアンスに関する報告
ME4	IT ガバナンス状況に関する報告

アウトプット	To						
IT 計画にインプットされる成果	PO1	PO2	DS1				
是正措置計画	PO4	PO8					
過去のリスクの傾向と発生したイベント	PO9						
プロセスの成果報告	ME2						

RACI チャート

役割

アクティビティ	取締役会	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス、監査、リスク、セキュリティ
モニタリングアプローチの確立		A	R	C	R	I	C	I	C	I		C
ビジネス目標をサポートする測定可能な目標の特定と収集		C	C	C	A	R	R		R			
スコアカードの作成					A		R	C	R	C		
成果の評価			I	I	A	R	R	C	R	C		
成果の報告	I	I	I	A	A	R	R	C	R	C		I
成果改善策の明確化とモニタリング					A	R	R	C	R	C		C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- プロセスの成果報告の把握と照合、およびマネジメント層への報告への組み込み
- 合意した達成目標に照らした成果のレビューと、必要な是正措置の実施

プロセスの達成目標
- IT プロセスおよび重要プロセスに対する測定可能な目標、KGI、KPI の設定
- プロセス指標の測定、モニタリング、および報告
- 成果改善策の明確化と実施

IT の達成目標
- 取締役会の指示に従ったガバナンス要件への対応
- ビジネス戦略と合致するビジネス要件への対応
- 費用効率の高い IT サービスの品質、継続的な改善、および将来の変更に対する対応力実現の保証
- IT の費用、便益、戦略、ポリシー、およびサービスレベルの透明性の確実な保証と理解の保証

促進

促進

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- プロセス上の何らかの不備が報告されてから対応策の実施までに要する時間
- 実際の成果目標、測定指標、達成目標、およびベンチマークを測定項目に反映するまでに要する時間
- プロセスあたりの指標の数
- 特定され、モニタリングに組み込まれた因果関係の数
- 測定データの収集に必要な労力
- 測定プロセスでは特定されない問題の数
- 業界水準と設定された達成目標に照らしてベンチマーク評価が可能な指標の割合

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 測定プロセスに対する利害関係者の満足度
- モニタリング対象となっている重要プロセスの割合
- モニタリング活動の結果を受けて実施された改善策の件数
- 達成された成果目標の数(コントロール目標における指標に基づく)

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- IT プロセスの有効性指標と効率性指標に関する達成目標に対する変更の数
- 成果報告に対するマネジメント層や管理部門の満足度
- 未解決のプロセス上の不備の削減数

成熟度モデル

ME1 IT 成果のモニタリングと評価

「ガバナンス要件に従った、IT の費用、便益、戦略、ポリシー、およびサービスレベルの透明性の確保と理解の実現」という IT に対するビジネス要件を満たす上で、「IT 成果のモニタリングと評価」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
組織にモニタリングプロセスが導入されていない。IT 部門は独自にプロジェクトやプロセスのモニタリングを行っていない。有用で、タイムリー、かつ正確な報告は作成されていない。明確に理解されたプロセス目標が必要であると認識されていない。

1 初期/その場対応
マネジメント層は、モニタリングプロセスに関する情報を収集し、評価する必要があることを認識している。しかし、情報収集と評価の標準的なプロセスは明確にされていない。モニタリングは実施されているが、指標は特定の IT プロジェクトやプロセスの必要性に応じて必要の都度、場当たり的に選択されている。通常、組織に何らかの損失や損害を与えるようなインシデントが発生してから、それに対応する形でモニタリングが実施される。経理部門により、IT にかかわる基本的な財務指標がモニタリングされている。

2 再現性はあるが直感的
モニタリング対象となる基本的な測定項目が特定されている。情報収集と評価の方法および技法は定められているが、モニタリングプロセスが組織全体で採用されているわけではない。モニタリング結果は、主担当者の専門知識に基づいて解釈される。情報収集用に一部のツールが選定され、導入されているが、計画的なアプローチに基づく情報収集は行われていない。

3 定められたプロセスがある
マネジメント層は、標準的なモニタリングプロセスを仕組みとして定着させ、周知している。モニタリングについての教育研修制度が導入されている。過去の成果情報が知識ベースとして正式に蓄積されている。評価は未だ個々の IT プロセスやプロジェクトのレベルで行われており、すべての IT プロセス間で一貫した評価が実施されているわけではない。IT プロセスとサービスレベルをモニタリングするツールが定義されている。組織の業績に対する情報サービス機能の貢献度の測定指標は定められているものの、財務面、業務面における従来の基準が活用されている。IT に特化した成果の測定項目、非財務的測定項目、戦略的測定項目、顧客満足度測定項目、およびサービスレベルが定義されている。成果測定のためのフレームワークが定義されている。

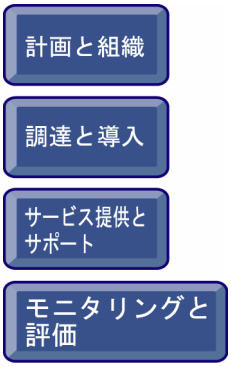
4 管理され、測定可能である
マネジメント層は、プロセス運用上許容できる逸脱レベルを定義している。モニタリング結果の報告は、標準化および定例化されつつある。すべての IT プロジェクトやプロセスにわたる指標が統一されている。IT 部門からマネジメント層への正式な報告システムが作られている。自動化されたツールが組織全体で導入されており、さまざまなアプリケーション、システム、プロセスに関する運用情報の収集とモニタリングに活用されている。マネジメント層は、利害関係者により承認された合意された基準に基づき、成果を評価できる。IT 部門の測定指標は、組織全体の達成目標と整合している。

5 最適化
継続的な品質改善プロセスが構築されており、組織全体のモニタリング標準やポリシーを最新の状態に維持するとともに、業界のベストプラクティスを取り入れている。モニタリングプロセスはすべて最適化され、組織全体の目標の達成を支援する手段として確立されている。ビジネス主導の指標が成果測定のために日常的に使用されており、IT バランススコアカードなどの戦略的評価フレームワークに統合されている。プロセスモニタリングと継続的な改善は、組織全体のビジネスプロセスの改善計画に沿って行われている。業界や主要な競合企業に対する汎用的な(比較の)基準を用いたベンチマーキングが行われている。

コントロール目標 －概要－

ME2 内部統制のモニタリングと評価

IT のための有効な内部統制プログラムを確立するには、明確なモニタリングプロセスが必要である。このモニタリングプロセスには、セルフアセスメントやサードパーティによるレビューの結果、発見されたコントロールの例外事項が含まれる。内部統制のモニタリングの主要な利点には、効果的かつ効率的な業務運営の実現と法規制へのコンプライアンスの確保がある。



IT プロセス: 内部統制のモニタリングと評価のコントロール目標は、

IT 目標の達成を保証し、IT 関連法規制へのコンプライアンスを確保することを、**ビジネス要件**とし、

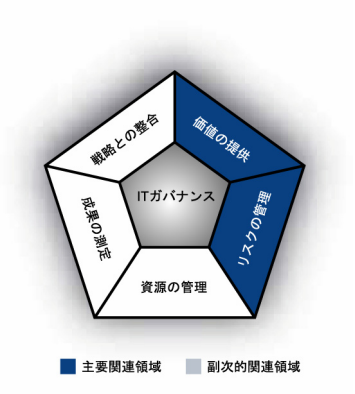
重点をおくべきコントロールは、IT 関連活動の内部統制プロセスをモニタリングし、是正措置を特定することである。

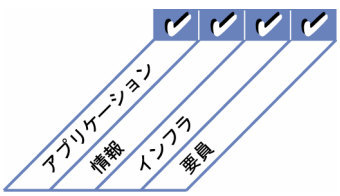
実現するための手段は、次の 3 項目である。

- IT プロセスフレームワークに組み込まれる内部統制の仕組みの構築
- IT に関する内部統制の有効性に関するモニタリングと報告
- 是正措置を講じるためのコントロールの例外事項に関するマネジメント層への報告

その成果の測定指標は、次の 3 項目である。

- 内部統制の主要な不備の件数
- コントロールの改善のための取り組みの件数
- コントロールセルフ評価の回数と範囲





コントロール目標 －詳細－

ME2 内部統制のモニタリングと評価

ME2.1 内部統制フレームワークのモニタリング
IT コントロール環境とコントロールフレームワークを継続的にモニタリングする。IT コントロール環境とコントロールフレームワークの改善のために、業界のベストプラクティスとベンチマークを用いた評価を実施しなければならない。

ME2.2 監督レビュー
たとえば、ポリシーや標準へのコンプライアンス、情報セキュリティ、変更管理、およびサービス・レベル・アグリーメント(SLA)で定められたコントロールなどの監督レビューにより、IT に関する内部統制の有効性をモニタリングし、報告する。

ME2.3 コントロールの例外事項
すべてのコントロールの例外事項に関する情報を記録し、根本原因の分析と是正措置に確実につなげる。マネジメント層は、該当部門の責任者に周知すべき不備、およびエスカレーションすべき不備を決定しなければならない。また、マネジメント層は影響を受ける関係者に通知する責任も負う。

ME2.4 コントロールセルフ評価
継続的なセルフ評価プログラムを導入し、マネジメント層による IT プロセス、ポリシー、および契約に関する内部統制のインテグリティと有効性の評価を実施する。

ME2.5 内部統制の保証
必要に応じて、サードパーティのレビューにより内部統制のインテグリティと有効性の保証を強化する。このようなレビューは、企業のコンプライアンスの担当部門のほか、マネジメント層の要請に応じて内部監査部門により実施されることがある。また、外部監査人およびコンサルタント、もしくは外部認証機関に委託されることもある。監査を実行する担当者は、たとえば Certified Information Systems Auditor™(公認情報システム監査人)(CISA®)などの資格保有者である必要がある。

ME2.6 サードパーティにおける内部統制
各外部サービスプロバイダの内部統制状況を評価する。外部サービスプロバイダが法規制要件および契約上の義務を遵守していることを確認する。これは、サードパーティによる監査、またはマネジメント層の内部監査部門によるレビューと監査結果から判別できる。

ME2.7 是正措置
コントロールの評価と報告に基づいて、必要な是正措置を特定し、実行する。これには、すべてのモニタリング、報告、および評価について、以下によるフォローアップが含まれる。
- マネジメント層の対応に関するレビュー、協議、および確立
- 是正措置に関する実行責任の割り当て(場合によりリスク受容も含まれる)
- 実行された是正措置の結果の追跡

マネジメントガイドライン

ME2 内部統制のモニタリングと評価

From	インプット
ME1	プロセスの成果報告

アウトプット	To						
IT コントロールの有効性に関する報告	PO4	PO6	ME1	ME4			

RACI チャート

アクティビティ	取締役会	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス、リスク、セキュリティ
IT 内部統制活動のモニタリングとコントロール					A		R		R	R		A/I
セルフ評価プロセスのモニタリング				I	A		R		R	R		C
独立したレビュー、監査、および検査の成果のモニタリング				I	A		R		R	R		C
サードパーティによるコントロールの確実性を保証するためのプロセスのモニタリング		I	I	I	A		R		R	R		C
コントロールの例外事項を特定し、評価するためのプロセスのモニタリング		I	I	I	A	I	R		R	R		C
コントロールの例外事項を特定し、是正するためのプロセスのモニタリング		I	I	I	A	I	R		R	R		C
主要な利害関係者への報告	I	I	I		A/R							I

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- IT プロセスフレームワークに組み込まれる内部統制の仕組みの構築
- IT に関する内部統制の有効性に関するモニタリングと報告
- 是正措置を講じるためのコントロールの例外事項に関するマネジメント層への報告

促進

プロセスの達成目標
- IT プロセスに対し設定された内部統制目標の達成度のモニタリング.
- 内部統制の是正措置の特定

促進

IT の達成目標
- エラー、故意による攻撃、または災害で生じた障害に対する、IT サービスおよびインフラストラクチャの抵抗力・回復力の保証
- IT 目標の達成の保証
- IT の法規制へのコンプライアンスの保証
- すべての IT 資産の責任の所在の明確化と適切な保護

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- コントロールセルフ評価の回数と範囲
- 監督レビューの対象となった内部統制の数と範囲
- 内部統制の不備の発生から報告までの所要時間
- 内部的なコンプライアンスに関する報告の件数、頻度、および範囲

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 内部統制インシデントの頻度
- 外部資格保有者および認証機関の報告で特定された不備の件数
- コントロールの改善のための取り組みの件数
- 法規制違反の件数
- 内部統制の問題に対するタイムリーな対応の件数

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 内部統制のモニタリング報告に対する、マネジメント層の満足度と安心度の指標
- 内部統制の主要な不備の件数

成熟度モデル

ME2 内部統制のモニタリングと評価

「IT 目標の達成を保証し、IT 関連法規制へのコンプライアンスを確保する。」というITに対するビジネス要件を満たす上で、「IT 内部統制のモニタリングと評価」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
組織には内部統制の有効性をモニタリングする手続がない。また、マネジメント層に対し内部統制に関する報告を行う制度もない。IT 運用上のセキュリティと内部統制の保証について認識されていない。マネジメント層および従業員に、総じて内部統制に関する認識がない。

1 初期/その場対応
マネジメント層は、一定の IT 管理と内部統制の保証の必要性を認識している。内部統制の妥当性の評価は、個人の力量に依存して場当たり的に行われている。IT マネジメント層は、内部統制の有効性のモニタリングに関する責任を正式に割り当てていない。ITに関する内部統制の評価は、従来の財務監査の一環として行われており、使用されている方法論やスキルは、情報サービス機能のニーズを満たしていない。

2 再現性はあるが直感的
組織は是正措置を実行するきっかけとして、コントロールに関する非公式な報告書を利用している。内部統制の評価は、主担当者のスキルに依存している。組織の内部統制のモニタリングに対する意識が高まってきている。情報サービスのマネジメント層は、重要と思われる内部統制の有効性を定期的にモニタリングしている。内部統制のモニタリングにおいて特定の方法論とツールが導入され始めているが、計画的な実施にはいたっていない。IT 環境に固有のリスク要因の特定は、個々の担当者のスキルに委ねられている。

3 定められたプロセスがある
マネジメント層は、内部統制のモニタリングを支援し、仕組みとして定着させている。内部統制のモニタリング活動について評価し、報告するためのポリシーと手続が確立されている。内部統制のモニタリングに関する教育研修制度が定義されている。セルフ評価や内部統制の保証のためのレビューのプロセスが定められており、ビジネス部門管理者と IT 部門管理者の役割も規定されている。ツールは活用されているが、必ずしもすべてのプロセスで統一して取り入れられてはいない。ITプロセスのリスク評価のポリシーが、IT 部門のために特別に作成されたコントロールフレームワーク内において使用されている。プロセス固有のリスクが定義され、リスク低減ポリシーが策定されている。

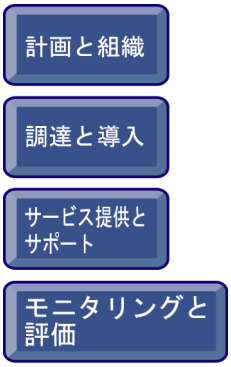
4 管理され、測定可能である
マネジメント層は、IT に関する内部統制のモニタリングのためのフレームワークを導入している。組織は、内部統制のモニタリングプロセスにおいて許容可能な逸脱レベルを設定している。評価を標準化し、コントロールの例外事項を自動的に発見するためのツールが導入されている。正式な IT 内部統制部門が設置されており、専門的技能と所定の資格を有する専門家が配置され、マネジメント層によって承認された正式なコントロールフレームワークが活用されている。高いスキルを持つ IT 担当スタッフが、内部統制の評価に日常的に参加している。過去の内部統制モニタリングの情報に基づいた指標となる知識ベースが確立されている。内部統制モニタリングに対するピアレビューが実施されている。

5 最適化
マネジメント層は、内部統制のモニタリングについて、経験則や業界のベストプラクティスを取り入れた継続的改善プログラムを組織全体に導入している。組織は必要に応じて最新の統合ツールを使用しており、重要なITコントロールの評価を効果的に行い、ITコントロールのモニタリング上のインシデントを迅速に発見できる。情報サービス機能において、知識の共有化が正式に行われている。業界水準や業界のベストプラクティスに対するベンチマーキングが正式に運用されている。

コントロール目標 －概要－

ME3 規制に対するコンプライアンスの保証

法規制面での監督を効果的に行うには、各種法規制に対するコンプライアンスを確保するための、独立したレビュープロセスを確立する必要がある。このプロセスには、監査の憲章、監査人の独立性、監査人の職業倫理と規範、計画策定、監査の実施、および監査活動に関する報告とフォローアップが含まれる。このプロセスの目的は、IT のコンプライアンスを積極的に保証することである。



IT プロセス: 規制に対するコンプライアンスの保証のコントロール目標は、

法規制に対するコンプライアンスを、**ビジネス要件**とし、

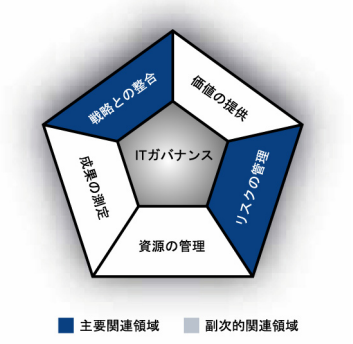
重点をおくべきコントロールは、すべての関連法規制および対応する IT のコンプライアンスレベルを特定し、IT プロセスを最適化して法規制違反のリスクを低減することである。

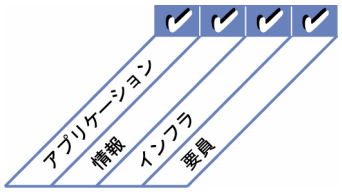
実現するための手段は、次の 3 項目である。

- IT 関連の法規制要件の特定
- 法的要件の影響評価
- 法的要件へのコンプライアンスに関するモニタリングと報告

その成果の測定指標は、次の 3 項目である。

- 和解金や罰金を含む、IT のコンプライアンス違反の費用
- 組織外におけるコンプライアンスに関する課題の特定から解決までに要する平均時間
- コンプライアンスに関するレビューの頻度





コントロール目標 －詳細－

ME3 規制に対するコンプライアンスの保証

ME3.1 IT に影響を及ぼす可能性がある法規制の特定
情報、情報サービス(外部サービスプロバイダのサービスを含む)の提供、および IT の組織、プロセス、インフラストラクチャに関係する、国内または国際的な法律、契約、政策、および規制上の要件のタイムリーな特定を保証するプロセスを策定し、導入する。電子商取引、データフロー、プライバシー、内部統制、財務報告、業界特有の規制、知的所有権と著作権、および安全衛生に関する法規制について考慮する。

ME3.2 法的要件への対応の最適化
IT のポリシー、標準、および手続をレビューおよび最適化し、法規制要件に対して効率的な対応を確実に行う。

ME3.3 法的要件へのコンプライアンスの評価
ビジネスと IT 部門のマネジメント層におけるガバナンスの監視と内部統制の運用により、法規制要件を含む IT のポリシー、標準、および手続に対するコンプライアンスを効率的に評価する。

ME3.4 コンプライアンスの積極的な保証
コンプライアンスを積極的に保証し、それについて報告を行う手続を策定し、導入する。また、この手続において、コンプライアンスが不十分である場合に、必要に応じて担当のプロセスオーナによるタイムリーな是正措置が講じられる。コンプライアンスの進捗と状況に関する IT 部門の報告を、その他のビジネス部門からの類似報告と統合する。

ME3.5 報告の統合
法規制要件に関する IT 部門の報告を、その他のビジネス部門からの類似報告と統合する。

マネジメントガイドライン

ME3 規制に対するコンプライアンスの保証

From	インプット
*	法規制のコンプライアンス要件

* COBIT 外からのインプット

アウトプット	To						
IT サービスの提供に関係する法規制要件の一覧表	PO4	ME4					
IT 活動の外部法規制要件へのコンプライアンスに関する報告	ME1						

RACI チャート

アクティビティ ＼ 役割	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス・監査・リスク・セキュリティ	取締役会
法律、契約、政策、および規制上の要件を特定するプロセスの策定と実行				A/R	C	I	I	I	C	I	R	
IT のポリシー、標準、および手続に対する IT 活動のコンプライアンスの評価	I	I	I	A/R	I	R	R	R	R	R	R	I
IT のポリシー、標準、および手続に対する IT 活動のコンプライアンスの積極的な保証に関する報告				A/R	C	C	C	C	C	C	R	
コンプライアンス要件に応じて、IT のポリシー、標準、および手続を整合するインプットの提供				A/R	C	C	C	C	C		R	
法的要件に関する IT 部門の報告と、その他のビジネス部門からの類似報告との統合				A/R		I	I	I	R	I	R	

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- IT 関連の法規制要件の特定
- IT 担当者への、コンプライアンスに関する責務の教育
- 法的要件の影響評価
- 法的要件へのコンプライアンスに関するモニタリングと報告

促進

プロセスの達成目標
- すべての関連法規制および IT のコンプライアンスレベルの特定
- IT のポリシー、標準、および手続の整合による、法規制違反のリスクの効率的管理
- IT 部門内で特定されたコンプライアンスに関する課題がビジネスに及ぼす影響の極小化

促進

IT の達成目標
- IT の法規制へのコンプライアンスの保証

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- 組織外におけるコンプライアンスに関する課題の特定から解決までに要する平均時間
- 新規法律または新しい規制が公布されてからコンプライアンスレビューの実施までに要する平均時間
- IT 部門の従業員 1 人あたりの、コンプライアンスに関する年間の研修日数

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- 年間に特定された、重要な法規制違反の課題の件数
- コンプライアンスレビューの頻度

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- 和解金や罰金を含む、IT のコンプライアンス違反の費用
- 取締役会への報告、または世論に対する悪影響や組織への損害につながった法規制違反の課題の件数

成熟度モデル

ME3 規制に対するコンプライアンスの保証

「法規制に対するコンプライアンス」という IT に対するビジネス要件を満たす上で、「規制に対するコンプライアンスの保証」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
IT に影響を及ぼす外部要件はほとんど認識されておらず、規制、法律、および契約上の要件に対するコンプライアンスに関するプロセスがない。

1 初期/その場対応
組織に影響を及ぼす、規制、契約、および法律上のコンプライアンス要件について認識されている。新規プロジェクト、または監査やレビューへの対応において必要性が生じた場合に限り、コンプライアンスを確保するための非公式なプロセスが利用されている。

2 再現性はあるが直感的
外部要件へのコンプライアンスの必要性が理解され、周知されている。金融規制や個人情報保護に関する法律などに対するコンプライアンスが継続的な要件となる場合において、個々のコンプライアンス手続が策定され、毎年、更新されている。しかし、標準的なアプローチは存在しない。個々の担当者の知識と責務に大きく依存しているため、過りが発生しやすい。外部要件とコンプライアンス上の課題に関する非公式の研修が実施されている。

3 定められたプロセスがある
規制、契約、および法律上の義務に対するコンプライアンスを確保するために、ポリシー、手続、およびプロセスが策定され、文書化および周知されているが、すべてが遂行され、最新になっており、導入する上で実用的な訳ではない。モニタリングはほとんど実施されておらず、対応できていないコンプライアンス要件がある。組織に影響を与える外部法規制要件と、定められたコンプライアンスプロセスについて研修が行われている。契約責任に関連するリスクを極小化するための、契約と法律に関する標準的プロセスが、形式上は存在する。

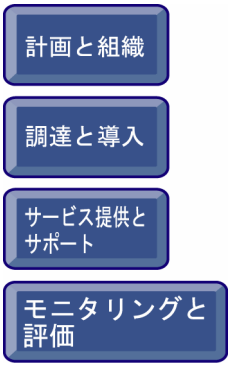
4 管理され、測定可能である
外部要件に起因する課題と損害にさらされること、およびすべてのレベルにおけるコンプライアンスの確保の必要性が、十分に理解されている。すべてのスタッフが自身のコンプライアンスに対する責務について確実に認識できるよう、正式な研修制度が整備されている。実行責任の所在が明確になっており、プロセスオーナという考え方が周知されている。プロセスには、外部要件と進行中の変更を特定するための環境のレビューが含まれる。外部要件に対する違反をモニタリングし、内部手続を実施して、是正措置を行うための仕組みが整備されている。法規制要件違反の課題が発生した場合は、持続的な解決策を特定するために、標準的な方法で根本原因が分析されている。現行規制や継続的なサービス契約への対応など特定のニーズに対して、組織内の優れた実践基準を標準化して活用している。

5 最適化
外部要件に準拠するために、適切に整備され、効率的かつ強制力のあるプロセスが存在し、組織全体に対する指導と調整を行う主管部門を中心に運用されている。該当する外部要件について、将来の動向や見込まれる変更、およびそれらを踏まえた新たな対応策の必要性などを含む豊富な知識を有している。組織は、自身が影響を受ける外部要件について理解し、それらの要件に対して主体的に影響を与えるために、各種規制団体および業界団体との公開討議に参加している。ベストプラクティスの策定により外部要件に対する効率的なコンプライアンスが確保されているため、コンプライアンス違反はほとんど発生していない。組織全体を対象とする一貫した追跡システムが存在するため、マネジメント層は業務の流れを文書化し、コンプライアンスモニタリングプロセスの品質と有効性を測定および改善できる。外部要件に対するセルフ評価のプロセスが導入され、優れた実践基準のレベルまで改善されている。コンプライアンスに関連する組織の管理体系と企業文化は十分に強固であり、関連プロセスが適切に整備され浸透しているため、プロセスに関する研修は新規要員補充の際、および重大な変更があった場合にのみ実施すればよい状態にある。

コントロール目標 －概要－

ME4 IT ガバナンスの提供

効果的なガバナンスフレームワークの確立には、組織構造、プロセス、リーダシップ、役割、および責務を定義し、企業の戦略と目標に沿った企業の IT 投資を確実に実現することが含まれる。



IT プロセス: IT ガバナンスの提供のコントロール目標は、

IT ガバナンスと企業のガバナンス目標との統合および法規制へのコンプライアンスを、**ビジネス要件**とし、

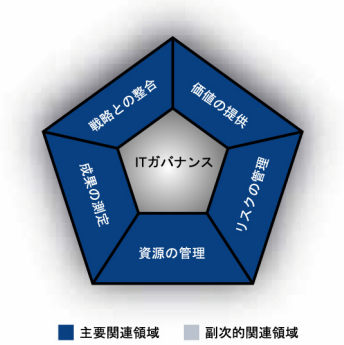
重点をおくべきコントロールは、IT の戦略、成果、およびリスクに関する取締役会への報告書を作成し、取締役会の指示に従ってガバナンス要件に対応することである。

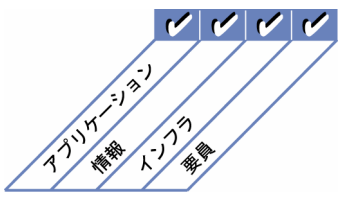
実現するための手段は、次の 2 項目である。

- コーポレートガバナンスに統合された IT ガバナンスフレームワークの確立
- IT ガバナンスの状況に関する独立した保証の獲得

その成果の測定指標は、次の 3 項目である。

- 利害関係者に対する、取締役会の IT に関する報告の頻度(成熟度に関する報告を含む)
- IT 部門から取締役会への報告の頻度(成熟度に関する報告を含む)
- IT のコンプライアンスレビューの頻度





コントロール目標 －詳細－

ME4 IT ガバナンスの提供

ME4.1 IT ガバナンスフレームワークの確立
取締役会と連携して、リーダシップ、プロセス、役割と責務、情報要件、および組織構造を含む IT ガバナンスフレームワークを定義および確立し、企業の IT 関連の投資プログラムを企業の戦略と目標に確実に整合させ、成果を達成する。フレームワークでは、企業の戦略、その戦略を実行するための IT 関連の投資プログラムのポートフォリオ、個々の投資プログラム、およびそれらのプログラムを構成するビジネスプロジェクト、IT プロジェクトなどの間の関連付けを明確に規定する必要がある。またフレームワークでは、内部統制や監督における機能停止を回避するため、明確な説明責任および実践基準を規定しなければならない。フレームワークは、企業全体の統制環境および一般に認められたコントロール原則と整合している必要があり、IT プロセスとコントロールフレームワークに基づいている必要がある。

ME4.2 戦略との整合
IT の役割や、技術の現状やケイパビリティおよび運用能力などの IT に関する戦略的な課題について、取締役会やマネジメント層の理解を得る。ビジネス戦略に対する IT の潜在的貢献に関する理解を、ビジネス部門と IT 部門の間で確実に共有する。IT 関連の投資がプログラムのポートフォリオとして管理されており、戦略の実現にあたって IT 能力がもたらす価値を最適化する目的でビジネス部門が行うすべての変更がそれらのプログラムに含まれている場合に限り、IT から本来の価値を得られることが明確に理解させる。取締役会と連携して、IT 戦略委員会などの管理組織を定義して導入し、マネジメント層に IT に関連する戦略的指針を示す。これにより、戦略と目標が各ビジネス部門およびIT部門の運用に確実に落とし込まれるようにし、ビジネス部門と IT 部門間の信頼関係が確立されるようにする。戦略上の決定や IT 関連の投資による便益享受において、ビジネス部門と IT 部門による共同責任を強調し、戦略とその実施において IT 部門とビジネス部門の連携を図る。

ME4.3 価値の提供
IT 関連の投資プログラムとその他の IT 資産やサービスを管理し、企業の戦略と目標の実現を支援するにあたって、それらが最大限の価値を確実に発揮できるようにする。IT 関連の投資に期待されるビジネス上の成果とそれらの成果の達成に必要なすべての取り組みが理解されていること、包括的かつ一貫したビジネスケースが作成され利害関係者によって承認されていること、資産と投資がその経済的ライフサイクルにわたり管理されていること、そして、新規サービスへの貢献、効率性の向上、顧客要望への対応力の強化など、便益の実現に向けた積極的な管理が行われていることを確認する。ポートフォリオ、プログラム、およびプロジェクトの管理に統制のとれたアプローチを用い、ビジネス部門がすべての IT 関連の投資を主導し、IT 部門が IT 能力とサービスの提供費用の最適化を保証するようにする。技術的なソリューションの細分化による費用および煩雑さの増大を避けるため、技術面での投資において、最大限の標準化を確実に行う。

ME4.4 資源の管理
定期的な評価により、IT 資産の投資、使用、および割り当てを最適化し、IT 部門が現在および将来の戦略的目標を達成し、ビジネス上の要件に対応できるだけの、要件に適合した有能かつ有効なリソースを十分に保有していることを確認する。マネジメント層は、リソース要件を効果的に満たし、アーキテクチャのポリシーと標準に準拠するために、明確で一貫した、強制力のある人材ポリシーと調達ポリシーを確実に用意する必要がある。IT インフラストラクチャを定期的に評価し、それが可能な限り標準化されており、必要に応じた相互運用性を有することが必要である。

ME4.5 リスクの管理
取締役会と連携して、企業の IT リスク傾向を定義する。IT リスクに対する選好(方針)を企業内に周知し、IT リスク管理計画について合意する。リスク管理の責務を組織に組み込み、ビジネス部門と IT 部門が IT にかかわるリスクとビジネスへの影響を定期的に評価および報告するようにする。IT 部門のマネジメント層は、特に IT コントロール上の不備、内部統制と監督における脆弱性、およびそれらがビジネスに与える実際的および潜在的な影響に注意を払いつつ、リスクの発生を確実にフォローアップする必要がある。企業における IT リスクの状況は、すべての利害関係者に対して明示されていなければならない。

ME4.6 成果の測定
関連ポートフォリオ、プログラム、および IT 成果を、タイムリーかつ正確な方法で取締役会とマネジメント層に報告する。特定された目標に企業としてどこまで到達しているのか、進捗状況に関するマネジメントレポートをマネジメント層に提出する必要がある。進捗状況として、計画された目標の達成度合い、得られた成果物、達成された成果目標および低減されたリスクを報告に含める必要がある。報告は、その他のビジネス部門からの類似報告と統合する。成果の測定指標は、主要な利害関係者によって承認される必要がある。取締役会とマネジメント層はこれらの成果報告について厳密に調査し、IT 部門のマネジメント層には計画からの逸脱および成果に関する問題について説明する機会が与えられなければならない。レビューの結果を受けて、適切な是正措置を実行し、コントロールする必要がある。

ME4.7 独立した保証
ITポリシー、標準、手続、および一般に認められた実践基準に対する IT のコンプライアンスに関して、独立した保証をタイムリーに取締役会に提示する(通常、監査委員会経由で提示される)ために、組織が確実にスキル的にも人数的にも十分なメンバーのいる担当部門を持っていること、または外部の保証サービスを活用していることを確認する。

マネジメントガイドライン

ME4 IT ガバナンスの提供

From	インプット
PO4	IT プロセスフレームワーク
PO5	費用便益報告
PO9	リスクの評価と報告
ME2	IT コントロールの有効性に関する報告
ME3	IT サービスの提供に関係する法規制要件の一覧表

アウトプット	To						
プロセスフレームワークの改善	PO4						
IT ガバナンス状況に関する報告	PO1	ME1					
IT 関連のビジネス投資に期待されるビジネス成果	PO5						
企業の IT に関する戦略的方針	PO1						
企業の IT リスクに対する選好(方針)	PO9						

RACI チャート

役割

アクティビティ	取締役会	CEO	CFO	企業幹部	CIO	ビジネスプロセスオーナ	オペレーション責任者	設計責任者	開発責任者	IT管理責任者	PMO（プロジェクト・マネジメント・オフィス）	コンプライアンス、監査、リスク、セキュリティ
マネジメント層と取締役会による IT 活動に対する監督と推進の確立	A	R	C	C	C							C
IT 成果、IT 戦略、資源とリスクの管理のビジネス戦略との整合、レビュー、承認、および周知	A	R	I	I	R							C
成果、およびポリシー、標準、手続へのコンプライアンスに関する独立した定期評価の実施	A	R	C	I	C		I	I	I	I	I	R
独立した評価による検出事項の解決、およびマネジメント層による合意された改善案の確実な実施	A	R	C	I	C		I	I	I	I	I	R
IT ガバナンス報告の作成	A	C	C	C	R	C	I	I	I	I	I	C

RACI チャートでは、IT プロセスのアクティビティ別の関与者と役割を以下の区分で明らかにしている。①実行責任者(R：Responsible) ②説明責任者(A：Accountable) ③協議先(C：Consulted)④報告先(I：Informed)

達成目標とその評価指標

アクティビティの達成目標
- コーポレートガバナンスに統合された IT ガバナンスフレームワークの確立
- IT ガバナンスの状況に関する独立した保証の獲得

促進

プロセスの達成目標
- IT ガバナンスとコーポレートガバナンスの目標の統合
- IT 戦略、成果、およびリスクに関する完全でタイムリーな取締役会への報告書の作成
- IT 戦略、成果、およびリスクに関する取締役会の懸案事項と質問に対する対応
- IT ポリシー、標準、および手続へのコンプライアンスに関する独立した保証の獲得

促進

IT の達成目標
- 取締役会の方針に従ったガバナンス要件への対応
- IT の費用、便益、戦略、ポリシー、およびサービスレベルの透明性と理解の保証
- IT の法規制へのコンプライアンスの保証
- IT 活用による費用効率の高いサービス品質、継続的な改善、および将来の変更に対する対応力の実現の保証

上記目標達成度を以下で測定する

重要成果達成指標(KPI)
- ガバナンスに関する行動規範などの研修を受けたスタッフの割合
- 部門あたりの倫理責任者の数
- IT運営/戦略会議でITガバナンスが議題項目として取り上げられる頻度
- IT ガバナンスについて研修済みまたはガバナンスの経験を有する取締役会メンバーの割合
- 改善案が合意されてから経過した期間
- 利害関係者の満足度調査に関する取締役会への報告の頻度

上記目標達成度を以下で測定する

プロセスに関する重要目標達成指標(KGI)
- IT 部門から取締役会への報告の頻度(成熟度に関する報告を含む)
- ガバナンスに対する違反の件数
- IT のコンプライアンスに関する独立したレビューの頻度

上記目標達成度を以下で測定する

IT に関する重要目標達成指標(KGI)
- IT が、積極的に取締役会で議題として取り上げられた回数
- 利害関係者に対する、取締役会の IT に関する報告の頻度(成熟度に関する報告を含む)
- 取締役会の議題として再度取り上げられた IT に関する課題の数

成熟度モデル

ME4 IT ガバナンスの提供

「IT ガバナンスと企業のガバナンス目標との統合および法規制へのコンプライアンス」という IT に対するビジネス要件を満たす上で、「IT ガバナンスの提供」プロセスにおける管理の成熟度は、以下のとおりである。

0 不在
IT ガバナンスプロセスとして識別できるものがまったく存在しない。組織は対処すべき課題の存在さえ認識しておらず、したがってその課題に関する話し合いも行われていない。

1 初期/その場対応
IT ガバナンスに関する課題が存在し、対処する必要があることが認識されている。個別的、または場合に応じた場当たり的なアプローチが適用されている。マネジメント層のアプローチは事後的であり、課題や課題に対処するためのアプローチに関して、散発的で一貫性のない議論しか行われていない。マネジメント層は、IT のビジネス成果に対する貢献について、大枠でしか把握していない。マネジメント層は、組織に損失や損害を与えるインシデントが発生してから、事後的に対応するのみである。

2 再現性はあるが直感的
IT ガバナンスの課題について認識されている。IT 計画策定、運用、およびモニタリングのプロセスを含む IT ガバナンスのアクティビティと成果達成指標が定義されつつある。改善が必要な IT プロセスの特定は、個人的な判断に基づいて行われている。マネジメント層は、IT ガバナンスの基本的な指標、および評価の方法と技法を明確化しているが、そのプロセスが組織全体で採用されているわけではない。ガバナンス標準と実行責任に関する周知は、各担当者に一任されている。各担当者が、さまざまな IT プロジェクトや IT プロセス内でガバナンスプロセスを実施している。IT ガバナンスについて測定するためのプロセス、ツール、および指標は限定的であり、その利用方法に関する専門知識が欠如しているために十分に活用されているとは言えない。

3 定められたプロセスがある
IT ガバナンスの重要性と必要性がマネジメント層によって理解され、組織内で周知されている。成果測定指標と成果達成のドライバーの関連付けが定義および明文化された、一連の IT ガバナンス指標基準が策定されている。手続は標準化および文書化されている。マネジメント層は標準化された手続を周知しており、研修制度が導入されている。IT ガバナンスの監督を支援するためのツールが特定されている。ダッシュボードが IT バランススコアカードの一部として定義されている。ただし、研修の受講や、標準の遵守および適用は、各担当者の判断に委ねられている。プロセスはモニタリング可能であるが、プロセスからの逸脱があった場合は各担当者のイニシアチブによって対処されることが多いため、マネジメント層によって発見される可能性は低い。

4 管理され、測定可能である
IT ガバナンスの課題については、すべてのレベルにおいて十分に理解されている。対象顧客が明確に把握されており、サービス・レベル・アグリーメント(SLA)により実行責任が定義およびモニタリングされている。実行責任の所在が明確になっており、プロセスオーナが規定されている。IT プロセスと IT ガバナンスは互いに整合し、ビジネス戦略および IT 戦略に統合されている。IT プロセスの改善は主として定量的な把握に基づいて行われ、手続やプロセス指標に対するコンプライアンスをモニタリングおよび測定できる。プロセスのすべての利害関係者が、リスク、IT の重要性、およびITが提供し得る便益について把握している。マネジメント層は、プロセス運用上の許容逸脱レベルを定めている。確立されている技術や業界に浸透している標準ツールを活用した技術が、限定的ではあるが戦術的に使用されている。IT ガバナンスは、戦略計画と運営計画の策定およびモニタリングプロセスに統合されている。すべての IT ガバナンスのアクティビティに関する成果達成指標が記録および追跡され、企業全体の改善につながっている。重要なプロセス成果の総合的な説明責任の所在が明確にされており、マネジメント層の報酬は重要な成果の測定結果に基づき算定されている。

5 最適化
IT ガバナンスの課題と対応策について、先進的かつ先見的な理解がある。研修と周知の徹底は、最先端の概念と技法によってサポートされている。プロセスは、継続的な改善および外部組織との協働による成熟度のモデル化の結果、業界のベストプラクティスのレベルにまで改善されている。IT ポリシーの導入により、組織、要員、およびプロセスにおいて、IT ガバナンス要件が迅速に適応され、最大限に支援されるようになっている。問題と逸脱については、すべて根本原因が分析され、目的に則した方法で効率的な措置が特定され、実施されている。IT が組織に組み込まれて最適化され、広範囲で使用されており、これによりワークフローが自動化され、品質と有効性を向上させるツールを活用できている。IT プロセスのリスクと利点が企業全体にわたり定義、調整、および周知されている。指針とするため、外部の専門家やベンチマークが活用されている。ガバナンスに期待される効果に関するモニタリング、セルフ評価、および周知が組織内で浸透しており、技術の最適な利用により、測定、分析、周知、および研修が支援されている。コーポレートガバナンスと IT ガバナンスは戦略的に関連付けられており、技術と人的資源および財源を活用することで、企業の競争優位性が強化されている。IT ガバナンス活動は、コーポレートのガバナンスプロセスと統合されている。

付録 I

ビジネス達成目標とIT 達成目標の関連付け

この付録では、汎用的なビジネス達成目標と、IT 達成目標、IT プロセス、および情報要請規準との関連について包括的に説明する。次の 3 つの表を用いる。

1. 1 番目の表には、バランススコアカードに従って分類されたビジネス達成目標と、IT 達成目標および情報要請規準との対応関係が示されている。この表では、特定の汎用的なビジネス達成目標について、その達成を支援する IT 達成目標、および関連する COBIT 情報要請規準が示されている。
2. 2 番目の表には、IT 達成目標と、COBIT の IT プロセスおよび IT 達成目標の基準となる情報要請規準との対応関係が示されている。
3. 3 番目の表は逆方向の対応関係を示し、支援対象となる IT 達成目標を IT プロセスごとに示している。

これらの表では、COBIT の対象範囲と、COBIT と各種ビジネス要因とのビジネス上の関係の全容が明示され、標準的なビジネス達成目標と、その実現に必要な IT 達成目標と IT プロセスとの対応関係を把握できる。これらの表は汎用的な達成目標に基づいて作成されている。従って、これらの表を基に各企業で調整を行い、独自の表を作成する必要がある。

これらの表では、COBIT 第 3 版のビジネス要件において用いられている情報要請規準についても確認できるよう、ビジネス達成目標と IT 達成目標が支援する最も重要な情報要請規準も示されている。

注:

1. ビジネス達成目標の表に示す情報要請規準は、関連する IT 達成目標に付随する情報要請規準を集約し、ビジネス達成目標に最も関連すると思われる情報要請規準について主観的評価を行った結果導出されたものである。主要重点領域と副次的重点領域の分類は、現時点では行われていない。これらはあくまでも 1 つの指標であり、読者が自らの企業のビジネス達成目標について評価する際、実施するプロセスの参考として活用できる。
2. IT 達成目標の表に示す情報要請規準の主要重点領域と副次的重点領域の区分は、IT プロセスごとの情報要請規準を集約し、IT 達成目標における主要重点領域と副次的重点領域に関する主観的評価を行った結果導出されたものである。またプロセスによってITの達成目標への影響度が違うことがある。これらはあくまでも 1 つの指標であり、読者が自らの企業における IT 達成目標について評価する際、実施するプロセスの参考として活用できる。

ビジネス達成目標とIT達成目標との対応関係

		ビジネス達成目標	IT達成目標								COBIT情報要請規準						
											有効性	効率性	機密性	インテグリティ	可用性	コンプライアンス	信頼性
財務上の視点	1	市場シェアの拡大	25	28							✓	✓					
	2	収益増	25	28							✓	✓					
	3	投資収益	24									✓					
	4	資産利用の最適化	14								✓	✓					
	5	ビジネスリスクの管理	2	14	17	18	19	20	21	22			✓	✓	✓		
顧客の視点	6	顧客指向/サービスの向上	3	23							✓						
	7	競争力のある製品とサービスの提供	5	24							✓	✓					
	8	サービスの可用性	10	16	22	23					✓				✓		
	9	ビジネス要件の変化に対する即応性(製品化に要する時間)	1	5	25						✓	✓					
	10	サービス提供に要する費用の最適化	7	8	10	24						✓					
内部的視点	11	企業の価値連鎖の自動化と統合	6	7	8	11					✓	✓					
	12	ビジネスプロセス機能の改善と保守	6	7	11						✓	✓					
	13	プロセス費用の削減	7	8	13	15	24					✓					
	14	外部法規制の遵守	2	19	20	21	22	26	27				✓			✓	
	15	透明性	2	18													✓
	16	内部ポリシーへのコンプライアンス	2	13									✓			✓	
	17	業務上の生産性およびスタッフの生産性の向上と維持	7	8	11	13					✓	✓					
学習と成長の視点	18	製品/ビジネスの革新性	5	25	28						✓	✓					
	19	戦略的な意思決定に利用可能な、信頼できる有用な情報の入手	2	4	12	20	26				✓			✓			✓
	20	優れたスキルと高い意欲を持つ人材の獲得と維持	9								✓	✓					

IT 達成目標と IT プロセスとの対応関係

	IT 達成目標	プロセス											COBIT情報要請規準						
													有効性	効率性	機密性	インテグリティ	可用性	コンプライアンス	信頼性
1	事業戦略と合致するビジネス要件への対応	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1		P	P		S	S		
2	取締役会の指示に従ったガバナンス要件への対応	PO1	PO4	PO10	ME1	ME3							P	P					
3	提供サービスとサービスレベルに対するエンドユーザの満足の確保	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13				P	P		S	S		
4	情報利用の最適化	PO2	DS11											S		P			S
5	機敏な IT 能力の創出	PO2	PO4	PO7	AI3								P	P		S			
6	ビジネスの機能的要件およびコントロール要件を効果的かつ効率的なコンピュータ化対応策に変換する方法の定義	AI1	AI2	AI6									P	P				S	
7	統合および標準化されたアプリケーションシステムの調達と保守	PO3	AI2	AI5									P	P				S	
8	統合および標準化された IT インフラストラクチャの調達と保守	AI3	AI5										S	P					
9	IT 戦略に対応する IT スキルの獲得と維持	PO7	AI5										P	P					
10	サードパーティとのリレーションシップについての相互満足の達成	DS2											P	P	S	S	S	S	S
11	アプリケーションおよび技術的対応策のビジネスプロセスへのスムーズな統合	PO2	AI4	AI7									P	P		S	S		
12	IT 費用、便益、戦略、ポリシー、およびサービスレベルに関する透明性の確保と理解の実現	PO5	PO6	DS1	DS2	DS6	ME1	ME3					P	P				S	S
13	アプリケーションおよび技術的対応策の適切な利用と成果達成の保証	PO6	AI4	AI7	DS7	DS8							P	S					
14	すべての IT 資産の責任の所在の明確化と適切な保護	PO9	DS5	DS9	DS12	ME2							S	S	P	P	P	S	S
15	IT インフラストラクチャ、資源、および能力の最適化	PO3	AI3	DS3	DS7	DS9							S	P					
16	対応策とサービスの提供における不備と補整作業の必要性の削減	PO8	AI4	AI6	AI7	DS10							P	P		S	S		
17	IT 目標の達成の保証	PO9	DS10	ME2									P	P	S	S	S	S	S
18	リスクが IT 目標および資源に与える、ビジネス上の影響の明確化	PO9											S	S	P	P	P	S	S
19	重要かつ機密の情報が、当該情報へのアクセスを許可されていないユーザに開示されないことの保証	PO6	DS5	DS11	DS12										P	P	S	S	S
20	自動化された業務取引および情報交換の信頼性の確保	PO6	AI7	DS5									P			P	S	S	
21	エラー、意図的な攻撃、または災害で生じた障害に対する、IT サービスおよびインフラストラクチャの抵抗力・回復力の確保	PO6	AI7	DS4	DS5	DS12	DS13	ME2					P	S		S	P		
22	IT サービスの中断または変更が及ぼすビジネスへの影響の極小化	PO6	AI6	DS4	DS12								P	S		S	P		
23	要求に応じて IT サービスが使用可能であることの保証	DS3	DS4	DS8	DS13								P	P			P		
24	IT の費用効率および事業収益性への IT の貢献度の向上	PO5	AI5	DS6									S	P					S
25	品質標準を満たすプロジェクトの、期間内、かつ予算内での遂行	PO8	PO10										P	P		S			S
26	情報および情報処理インフラストラクチャのインテグリティ維持	AI6	DS5										P	P		P	P		S
27	IT の法令へのコンプライアンスの確保	DS11	ME2	ME3	ME4										S	S		P	S
28	IT 活用による費用効率の高いサービス品質、継続的な改善、および将来の変更に対する対応力実現の実証	PO5	DS6	ME1	ME3								P	P					P

IT プロセスと IT 達成目標とのマトリクス

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
		事業戦略と合致するビジネス要件への対応	取締役会の指示に従ったガバナンス要件への対応	提供サービスとサービスレベルに対するエンドユーザの満足の確保	情報利用の最適化	機敏なIT能力の創出	ビジネスの機能的要件およびコントロール要件を効果的かつ効率的なコンピュータ化対応策に変換する方法の定義	統合および標準化されたアプリケーションシステムの調達と保守	統合および標準化されたITインフラの調達と維持	IT戦略に対応するITスキルの獲得と維持	サードパーティとの関係性についての相互満足の達成	アプリケーションおよび技術的対応策のビジネスプロセスへのシームレスな統合	ITコスト、便益、戦略、ポリシー、およびサービスレベルに関する透明性の確保と理解の実現	アプリケーションおよび技術的対応策の適切な利用と成果達成の保証	すべてのIT資産の責任の所在の明確化と適切な保護	ITインフラ、資源、および能力の最適化	対応策とサービスの提供におけるITの構築と補整作業の必要性の判断	IT目標の達成の保証	リスクがIT目標およびITサービスに与える、ビジネス上の影響の明確化	重要かつ機密の情報が、当該情報へのアクセスを許可されていないユーザに開示されないようにすること	自動化された業務取引および情報交換の信頼性の確保	エラー、意図的な攻撃、または災害で生じた障害に対する、ITサービスおよびインフラの抵抗力・回復力の確保	ITサービスの中断または変更が及ぼすビジネスへの影響の極小化	要求に応じてITサービスを使用可能であることの保証	ITのコスト効率および標準化されたITの構築を満たすプロジェクトの、期間内、かつ予算内での遂行	品質標準を満たすITの構築能力の向上	情報およびITインフラのインテグリティ（維持	ITの法令へのコンプライアンスの確保	ITの活用によるコスト効率の高いサービス品質、継続的な改善、および将来の変更に対する対応力実現の保証
PO1	IT 戦略計画の策定	✓	✓																										
PO2	情報アーキテクチャの定義	✓			✓	✓						✓																	
PO3	技術指針の決定							✓								✓													
PO4	ITプロセスと組織及びそのかかわりの定義	✓	✓			✓																							
PO5	IT 投資の管理												✓												✓				✓
PO6	マネジメントの意図と指針の周知												✓	✓						✓	✓	✓	✓						
PO7	IT 人材の管理					✓				✓																			
PO8	品質管理			✓													✓									✓			
PO9	IT リスクの評価と管理														✓			✓	✓										
PO10	プロジェクト管理	✓	✓																							✓			
AI1	コンピュータ化対応策の明確化	✓					✓																						
AI2	アプリケーションソフトウェアの調達と保守						✓	✓																					
AI3	技術インフラストラクチャの調達と保守					✓			✓							✓													
AI4	運用と利用の促進			✓								✓		✓			✓												
AI5	IT 資源の調達							✓	✓	✓															✓				
AI6	変更管理	✓					✓										✓						✓				✓		
AI7	ソリューションおよびその変更の導入と認定	✓										✓		✓			✓				✓	✓							
DS1	サービスレベルの定義と管理	✓		✓									✓																
DS2	サードパーティのサービスの管理			✓							✓		✓																
DS3	性能とキャパシティの管理	✓														✓								✓					
DS4	継続的なサービスの保証																					✓	✓	✓					
DS5	システムセキュリティの保証														✓					✓	✓	✓					✓		
DS6	費用の捕捉と配賦												✓												✓				✓
DS7	利用者の教育と研修			✓										✓		✓													
DS8	サービスデスクとインシデントの管理			✓										✓										✓					
DS9	構成管理														✓	✓													
DS10	問題管理			✓													✓	✓											
DS11	データ管理				✓															✓								✓	
DS12	物理的環境の管理														✓					✓		✓	✓						
DS13	オペレーション管理			✓																		✓		✓					
ME1	IT 成果のモニタリングと評価	✓	✓										✓																✓
ME2	内部統制のモニタリングと評価														✓			✓				✓						✓	
ME3	規制に対するコンプライアンスの保証																											✓	
ME4	IT ガバナンスの提供		✓										✓															✓	✓

付録 Ⅱ

IT プロセスと、IT ガバナンス重点領域、COSO、COBIT IT 資源、および COBIT 情報要請規準との対応関係

この付録では、COBIT の IT プロセスと、IT ガバナンスの 5 つの重点領域、COSO 構成要素、IT 資源、および情報要請規準との対応関係を示す。表には、COBIT Online でのベンチマーキングに基づく相対重要度指標(H(高)、M(中)、L(低))も示す。この表は 1 ページにまとめられており、COBIT フレームワークによる IT ガバナンスと COSO 要件への対応の概要、および IT プロセスと IT 資源/情報要請規準との対応関係の概要を示す。P は主要な関係、S は副次的な関係を示す。P も S も記載されていない場合は、無関係ではないものの、重要度が低いかリレーションシップが薄いことを示す。重要度指標は専門家の意見と調査結果に基づいており、あくまでも参考情報として示されている。読者は、各自の組織内でどのプロセスが重要であるか検討する必要がある。

ITプロセスと、ITガバナンスの重点領域、COSO、COBIT IT資源、およびCOBIT情報要請規準との対応関係

		重要度	ITガバナンスの重点領域					COSO					COBITのIT資源				COBIT情報要請規準						
			戦略との整合	価値の提供	資源の管理	リスクの管理	成果の測定	統制環境	リスク評価	統制活動	情報と伝達	モニタリング	要員	情報	アプリケーション	インフラストラクチャ	有効性	効率性	機密性	インテグリティ	可用性	コンプライアンス	信頼性
計画と組織																							
PO1	IT戦略計画の策定	H	P		S	S			P		S	S	✓	✓	✓	✓	P	S					
PO2	情報アーキテクチャの定義	L	P	S	P	S				P	P			✓	✓		S	P	S	P			
PO3	技術指針の決定	M	S	S	P	S			S	P	S				✓	✓	P	P					
PO4	ITプロセスと組織及びそのかかわりの定義	L	S		P	P		P			S	S	✓				P	P					
PO5	IT投資の管理	M	S	P	S		S		S	P			✓		✓	✓	P	P					S
PO6	マネジメントの意図と指針の周知	M	P			P		P			P		✓	✓			P					S	
PO7	IT人材の管理	L	P		P	S	S	P			S		✓				P	P					
PO8	品質管理	M	P	S		S		P		P	S	P	✓	✓	✓	✓	P	P		S			S
PO9	ITリスクの評価と管理	H	P			P			P				✓	✓	✓	✓	S	S	P	P	P	S	S
PO10	プロジェクト管理	H	P	S	S	S	S	S	S	P		S	✓		✓	✓	P	P					
調達と導入																							
AI1	コンピュータ化対応策の明確化	M	P	P	S	S				P					✓	✓	P	S					
AI2	アプリケーションソフトウェアの調達と保守	M	P	P		S				P					✓		P	P		S			S
AI3	技術インフラストラクチャの調達と保守	L			P					P						✓	S	P		S	S		
AI4	運用と利用の促進	L	S	P	S	S				P	S		✓		✓	✓	P	P		S	S	S	S
AI5	IT資源の調達	M		S	P					P			✓	✓	✓	✓	S	P				S	
AI6	変更管理	H		P	S				S	P		S	✓	✓	✓	✓	P	P		P	P		S
AI7	ソリューションおよびその変更の導入と認定	M	S	P	S	S	S			P	S	S	✓	✓	✓	✓	P	S		S	S		
サービス提供とサポート																							
DS1	サービスレベルの定義と管理	M	P	P	P		P	S		P	S	S	✓	✓	✓	✓	P	P	S	S	S	S	S
DS2	サードパーティのサービスの管理	L		P	S	P	S	P	S	P		S	✓	✓	✓	✓	P	P	S	S	S	S	S
DS3	性能とキャパシティの管理	L	S	S	P	S	S			P		S			✓	✓	P	P			S		
DS4	継続的なサービスの保証	M	S	P	S	P	S	S		P	S		✓	✓	✓	✓	P	S			P		
DS5	システムセキュリティの保証	H				P				P	S	S	✓	✓	✓	✓			P	P	S	S	S
DS6	費用の捕捉と配賦	L		S	P		S			P			✓	✓	✓	✓		P					P
DS7	利用者の教育と研修	L	S	P		S		P			S		✓				P	S					
DS8	サービスデスクとインシデントの管理	L	S	P			S	S			P	P	✓		✓		P	P					
DS9	構成管理	M		P		S				P				✓	✓	✓	P	S			S		S
DS10	問題管理	M		P		S				P	S	S	✓	✓	✓	✓	P	P			S		
DS11	データ管理	H		P	P	P				P				✓						P			P
DS12	物理的環境の管理	L			S	P			S	P						✓				P	P		
DS13	オペレーション管理	L			P					P	S		✓	✓	✓	✓	P	P		S	S		
モニタリングと評価																							
ME1	IT成果のモニタリングと評価	H					P				S	P	✓	✓	✓	✓	P	P	S	S	S	S	S
ME2	内部統制のモニタリングと評価	M		P		P						P	✓	✓	✓	✓	P	P	S	S	S	S	S
ME3	規制に対するコンプライアンスの保証	H	P			P				P	S	S	✓	✓	✓	✓						P	S
ME4	ITガバナンスの提供	H	P	P	P	P	P	P	S		S	P	✓	✓	✓	✓	P	P	S	S	S	S	S

注: このCOSO対応関係はオリジナルのCOSOフレームワークに基づいている。この対応関係は概ねその後の『COSO Enterprise Risk Management-Integrated Framework』にも適用される。このフレームワークは、内部統制について詳しく規定し、企業のリスク管理という広範な主題に重点を置いている。これはオリジナルのCOSO内部統制フレームワークに代わるものではなく、内部統制フレームワークを内部に組み込んだものであり、COBITのユーザはこの企業リスク管理フレームワークを参考にして内部統制に関するニーズに対応し、さらに充実したリスク管理プロセスを構築できる。

付録 II

(空白ページ)

付録 Ⅲ

内部統制の成熟度モデル

この付録では、企業内での内部統制環境の状況と、内部統制の確立状況を示す汎用的な成熟度モデルについて説明する。この成熟度モデルは、内部統制の管理と、より優れた内部統制を確立する必要性の認識を、その場対応レベルから最適化レベルへ発展させる過程を示す。この成熟度モデルは、COBIT のユーザが IT における効果的な内部統制の実現に必要な要件を正しく認識し、自社の成熟度を判断する上で役立つ概略的な指針となる。

内部統制の成熟度モデル

成熟度	内部統制環境の状況	内部統制の確立
0 不在	内部統制の必要性が認識されていない。企業文化または使命にコントロールが組み込まれていない。コントロールの不履行やインシデントが発生するリスクが高い。	内部統制の必要性を評価する意志がない。インシデントが発生した時点で、その都度対応している。
1 初期/その場対応	内部統制の必要性がある程度認識されている。リスク要件およびコントロール要件に対処するアプローチは場当たり的で一貫性がなく、周知やモニタリングが実施されていない。何らかの不履行があっても特定されない。従業員が各自の実行責任を認識していない。	IT コントロールに関する要件について、評価の必要性が認識されていない。評価が実施されたとしても、場当たり的かつ表面的なものであり、重大なインシデントに対応する形でのみ行われる。実際に発生したインシデントのみが評価の対象となる。
2 再現性はあるが直感的	コントロールが実施されているが、文書化されていない。運用は個々の担当者の知識と意欲に依存している。有効性が適切に評価されていない。コントロールに多くの不備があり、これらの不備への対応が適切に実施されておらず、重大な問題が生じる可能性がある。マネジメント層によるコントロールに関する問題の解決措置は後回しにされる傾向があり、継続的に実施されていない。従業員が各自の実行責任を認識していない可能性がある。	コントロールの必要性に関する評価は、選定された IT プロセスにおいて、現在のコントロールの成熟度、達成すべき成熟度レベル、およびその間の差異の判別が必要な場合のみ実施される。プロセスに関与しているチームや IT 管理者を対象にした非公式のワークショップが実施されている。このワークショップにおいて、プロセスのコントロールに対する適切なアプローチが定義され、合意された実行計画の実施に向けた動機付けが行われている。
3 定められたプロセスがある	コントロールが実施され、適切に文書化されている。運用の有効性が定期的に評価され、発見される問題は標準的な数である。ただし、評価プロセスは文書化されていない。マネジメント層は、ほとんどのコントロールに関する問題を事前に予測して対処できるが、コントロールにおける不備は残っており、依然として重大な問題が生じる可能性がある。従業員はコントロールに関する各自の実行責任を認識している。	価値要因とリスク要因に基づいて重要な IT プロセスが特定されている。詳細な分析が実施され、コントロール要件および逸脱の根本原因が特定され、改善の機会が設けられている。ワークショップの活用に加え、ツールの使用とインタビューの実施により分析が強化され、IT プロセスオーナが評価と改善のプロセスを確実に実施、促進している。
4 管理され、測定が可能である	効果的な内部統制およびリスク管理環境がある。文書化された正式なコントロール評価が頻繁に実施されている。多くのコントロールは自動化されており、定期的なレビューの対象になっている。マネジメント層は、コントロールに関する問題をほとんど発見できるが、すべての問題が常に特定されるわけではない。特定されたコントロール上の不備に対応するため、一貫したフォローアップが行われている。コントロールの自動化に、限定的ではあるが戦術的に技術が使用されている。	関連するビジネスプロセスオーナの全面的な協力と同意を得て、IT プロセスの重要性が定期的に定義されている。主要な利害関係者が関与する詳細かつ正確な分析の実施後に、これらのプロセスの実際の成熟度とポリシーに基づいて、コントロール要件の評価が実施されている。評価の説明責任が明確に定められ、割り当てられている。改善戦略が投資対効果検討書によって裏付けられている。期待される結果を達成する過程における成果が、一貫してモニタリングされている。コントロールの社外レビューが時折行われている。
5 最適化	全社的なリスク/コントロールプログラムが策定されており、コントロールとリスクの問題が継続的かつ効果的に解決されるようになっている。内部統制とリスク管理は企業の活動指針に組み込まれており、コントロールのモニタリング、リスク管理、および法令遵守の徹底に関して全面的な説明責任を負う、自動化された常時モニタリングシステムにより支援されている。セルフ評価、および差異分析と根本原因分析に基づいてコントロールが継続的に評価されている。従業員はコントロールの改善に積極的に関与している。	事業上の変更を行う際は、IT プロセスの重要性が考慮され、プロセスコントロール能力の再評価の必要性があれば、それが必ず実施される。IT プロセスオーナは、セルフ評価の定期的な実施により、コントロールの成熟度が適切なレベルにあり、事業上の必要性が満たされていることを確認している。また、IT プロセスオーナは、成熟度の特性を検討し、コントロールの効果と効率を向上させる努力をしている。組織は外部のベストプラクティスと比較したベンチマーキングを実施し、内部統制の有効性について外部からの助言を求めている。重要なプロセスについて独立したレビューが実施され、コントロールが望ましい成熟度レベルにあり、計画どおりに機能していることが確認されている。

付録Ⅲ

(空白ページ)

付録 Ⅳ

COBIT 4.0 の主要参考資料

COBIT 4.0 の主要参考資料

これまでの COBIT 作成/改訂作業では、IT ガバナンスおよびコントロールのあらゆる領域に対応できるよう COBIT のインテグリティを確保するため、各国の 40 を超える詳細な IT 標準、フレームワーク、ガイドライン、およびベストプラクティスのベースが用いられている。

COBIT は、IT の適切な管理およびコントロールの実現に向けて何が必要なのかという点に重点を置いているため、同等のガイドラインの中で上位レベルに位置付けられている。より詳細な IT 標準やベストプラクティスでは、IT の特定の側面をどのように管理、コントロールするかを記述しており、その点で下位レベルに位置付けられる。COBIT はこのような各種ガイダンス資料を総括するものであり、複数の重要目標を 1 つの包括的なフレームワークにまとめている。このフレームワークは、さらにガバナンス要件とビジネス要件にも紐付けされている。

この COBIT 改訂版(COBIT4.0)では、その対象範囲、一貫性、整合性を適切なものにするため、主な参照資料として 6 つの主要な国際的 IT 関連標準、フレームワーク、および活動指針を利用している。以下にそれらの参考資料を示す。

- トレッドウェイ委員会組織委員会(COSO):
  『*Internal Control–Integrated Framework*』(1994 年)
  『*Enterprise Risk Management–Integrated Framework*』(2004 年)
- 英国商務局 (OGC®):
  『IT Infrastructure Library® (ITIL®)』(1999-2004 年)
- 国際標準化機構:
  『ISO/IEC 17799:2005, Code of Practice for Information Security Management』
- ソフトウェアエンジニアリング研究所(SEI®):
  『SEI Capability Maturity Model (CMM®)』(1993)
  『SEI Capability Maturity Model Integration (CMMI®)』(2000 年)
- プロジェクトマネジメント協会(PMI®):
  『Project Management Body of Knowledge (PMBOK®)』(2000 年)
- Information Security Forum (ISF):
  『*The Standard of Good Practice for Information Security*』(2003 年)

付録Ⅳ

(空白ページ)

付録 V

COBIT 第 3 版と COBIT 4.0 間の相互参照情報

訳注: COBIT V3では、マネジメントガイドラインと、コントロール目標の説明が別冊になっており、日本語に翻訳されたのが、マネジメントガイドラインのみであったため、本章ではCOBIT V3のコントロール目標は、英文のままにしてあります。

COBIT 第 3 版と COBIT 4.0 間の相互参照情報

フレームワークレベルの変更

COBIT4.0 への改訂に伴う COBIT フレームワークの主な変更点を以下に示す。

- ドメイン M が ME(「Monitor and Evaluate(モニタリングと評価)」を指す)に変更された。
- M3 と M4 は IT プロセスではなく監査プロセスであった。この 2 つのプロセスは多数の IT 監査標準で十分に網羅されているため削除された。ただし、マネジメント層における保証機能の必要性と利用を強調する目的で、改訂後のフレームワークでもこれらのプロセスに言及している。
- ME3 は法規制面での監督に関するプロセスであり、以前は PO8 で取り扱われていた。
- ME4 は IT のガバナンス監督管理のプロセスである。これは、IT ガバナンスのためのフレームワークとしての COBIT の目的を反映している。ME4 プロセスをすべてのドメインの最後に位置付けることで、ME4 以前の各プロセスによる、企業における効果的な IT ガバナンスの実施という最終的な目的への寄与が強調される。
- PO8 が削除されたが、PO9「IT リスクの評価と管理」および PO10「プロジェクト管理」の番号付けを COBIT 第 3 版と一致させるため、第 3 版では PO11 プロセスであった「品質管理」が本版では PO8 となっている。ドメイン PO のプロセス数は、本版では 11 ではなく 10 となっている。
- ドメイン AI では、調達プロセスが追加され、さらに以前の AI5 にリリース管理の要素が組み込まれた。以前の AI5 にリリース管理の要素を組み込んだ結果、この AI5 をドメイン AI の最終プロセスとする必要性が生じ、本版では AI7 となっている。これにより空番となった AI5 には、新たな調達プロセスが追加された。ドメイン AI のプロセス数は、本版では 6 ではなく 7 となっている。

詳細なコントロール目標

前述のフレームワークレベルの変更における詳細なコントロール目標の内容の明確化と重点的な検討作業からも明らかなように、COBIT フレームワークの改訂に際して、フレームワーク内の詳細なコントロール目標の内容が大幅に変更された。汎用的な要素はすべてフレームワークレベルでのみ説明され、各プロセスでは繰り返し記述しないようにしたため、詳細なコントロール目標の要素のうち約 1/3 が削減され、318 から 214 になった。また、業務処理統制への言及はすべてフレームワークの説明セクションに移動され、具体的なコントロール目標が新たな記述としてまとめられた。コントロール目標に関連する移行作業の参考として、新旧の詳細なコントロール目標間の相互参照情報を以下の 2 つの表に示す。

マネジメントガイドライン

特定のプロセスで他のプロセスから必要とする情報と、そのプロセスの一般的な成果物を示すため、インプットとアウトプットの記載が追加されている。また、アクティビティと関連する実行責任に関する記述も追加されている。COBIT 第 3 版の「主要成功要因」は「インプット」と「アクティビティの達成目標」に置き換えられた。指標は、ビジネス達成目標、IT 達成目標、プロセス達成目標、アクティビティ達成目標という一貫性のある段階的な流れに基づいて記載されるようになった。COBIT 第 3 版の指標は再検討の結果拡張され、より標準的かつ測定可能な指標となっている。

相互参照: COBIT 第 3 版対 COBIT 4.0

COBIT 第 3 版	COBIT 4.0
PO1 Define a strategic IT plan.	
1.1 IT as part of the organisation's long-and short-range plan	1.4
1.2 IT long-range plan	1.4
1.3 IT long-range planning —approach and structure	1.4
1.4 IT long-range plan changes	1.4
1.5 Short-range planning for the IT function	1.5
1.6 Communication of IT plans	1.4
1.7 Monitoring and evaluating of IT plans	1.3
1.8 Assessment of existing systems	1.3
PO2 Define the information architecture.	
2.1 Information architecture model	2.1
2.2 Corporate data dictionary and data syntax rules	2.2

COBIT 第 3 版	COBIT 4.0
2.3 Data classification scheme	2.3
2.4 Security levels	2.3
PO3 Determine technological direction.	
3.1 Technological infrastructure planning	3.1
3.2 Monitor future trends and regulations.	3.3
3.3 Technological infrastructure contingency	3.1
3.4 Hardware and software acquisition plans	3.1, AI3.1
3.5 Technology standards	3.4, 3.5
PO4 Define the IT organisation and relationships.	
4.1 IT planning or steering comittee	4.3
4.2 Organisational placement of the IT function	4.4
4.3 Review of organisational achievements	4.5
4.4 Roles and responsibilities	4.6

COBIT 第 3 版	COBIT 4.0
4.5 Responsibility for quality assurance	4.7
4.6 Responsibility for logical and physical security	4.8
4.7 Ownership and custodianship	4.9
4.8 Data and system ownership	4.9
4.9 Supervision	4.10
4.10 Segregation of duties	4.11
4.11 IT staffing	4.12
4.12 Job or position descriptions for IT staff	4.6
4.13 Key IT personnel	4.13
4.14 Contracted staff policies and procedures	4.14
4.15 Relationships	4.15
PO5 Manage the IT investment.	
5.1 Annual IT operating budget	5.3
5.2 Cost and benefit monitoring	5.4

COBIT 第 3 版	COBIT 4.0
5.3 Cost and benefit justification	1.1, 5.4, 5.5
PO6 Communicate management aims and direction.	
6.1 Positive information control environment	6.1
6.2 Management's responsibility for policies	6.3, 6.4, 6.5
6.3 Communication of organisation policies	6.3, 6.4, 6.5
6.4 Policy implementation resources	6.4
6.5 Maintenance of policies	6.3, 6.4
6.6 Compliance with policies, procedures and standards	6.3, 6.4, 6.5
6.7 Quality commitment	6.3, 6.4, 6.5
6.8 Security and internal control framework policy	6.2
6.9 Intellectual property rights	6.3, 6.4, 6.5
6.10 Issue-specific policies	6.3, 6.4, 6.5
6.11 Communication of IT security awareness	6.3, 6.4, 6.5
PO7 Manage human resources.	
7.1 Personnel recruitment and promotion	7.1
7.2 Personnel qualifications	7.2
7.3 Roles and responsibilities	7.4
7.4 Personnel training	7.5
7.5 Cross-training or staff backup	7.6
7.6 Personnel clearance procedures	7.7
7.7 Employee job performance evaluation	7.8
7.8 Job change and termination	7.8
PO8 Ensure compliance with external requirements.	
8.1 External requirements review	ME3.1

COBIT 第 3 版	COBIT 4.0
8.2 Practices and procedures for complying with external requirements	ME3.2
8.3 Safety and ergonomic compliance	ME3.1
8.4 Privacy, intellectual property and data flow	ME3.1
8.5 Electronic commerce	ME3.1
8.6 Compliance with insurance contracts	ME3.1
PO9 Assess risks.	
9.1 Business risk assessment	9.1, 9.2, 9.4
9.2 Risk assessment approach	9.4
9.3 Risk identification	9.3
9.4 Risk measurement	9.1, 9.2, 9.3, 9.4
9.5 Risk action plan	9.5
9.6 Risk acceptance	9.5
9.7 Safeguard selection	9.5
9.8 Risk assessment committment	9.1
PO10 Manage projects.	
10.1 Project management framework	10.2
10.2 User department participation in project initiation	10.4
10.3 Project team membership and responsibilities	10.8
10.4 Project definition	10.5
10.5 Project approval	10.6
10.6 Project phase approval	10.6
10.7 Project master plan	10.7
10.8 System quality assurance plan	10.10
10.9 Planning of assurance methods	10.12
10.10 Formal project risk management	10.9
10.11 Test plan	AI7.2

COBIT 第 3 版	COBIT 4.0
10.12 Training plan	AI7.1
10.13 Post-implementation review plan	10.14 (一部)
PO11 Manage quality.	
11.1 General quality plan	8.5
11.2 Quality assurance (QA) approach	8.1
11.3 QA planning	8.1
11.4 QA review of adherence to IT standards and procedures	8.1, 8.2
11.5 System development life cycle (SDLC) methodology	8.2, 8.3
11.6 SDLC methodology for major changes to existing technology	8.2, 8.3
11.7 Updating of the SDLC methodology	8.2, 8.3
11.8 Co-ordination and communication	8.2
11.9 Acquisition and maintenance framework for the technology infrastructure	8.2
11.10 Third-party implementor relationships	DS2.3
11.11 Programme documentation standards	AI4.2, AI4.3, AI4.4
11.12 Programme testing standards	AI7.2, AI7.4
11.13 System testing standards	AI7.2, AI7.4
11.14 Parallel/pilot testing	AI7.2, AI7.4
11.15 System testing documentation	AI7.2, AI7.4
11.16 QA evaluation of adherence to development standards	8.2
11.17 QA review of the achievement of IT objectives	8.2
11.18 Quality metrics	8.6
11.19 Reports of QA reviews	8.2

COBIT 第 3 版	COBIT 4.0
AI1 Identify automated solutions.	
1.1 Definition of information requirements	1.1
1.2 Formulation of alternative courses of action	1.3, 5.1, PO1.4
1.3 Formulation of acquisition strategy	1.3, 5.1, PO1.4
1.4 Third-party service requirements	5.1, 5.3
1.5 Technological feasibility study	1.3
1.6 Economic feasibility study	1.3
1.7 Information architecture	1.3
1.8 Risk analysis report	1.2

COBIT 第 3 版	COBIT 4.0
1.9 Cost-effective security controls	1.1, 1.2
1.10 Audit trails design	1.1, 1.2
1.11 Ergonomics	1.1
1.12 Selection of system software	1.1, 1.3
1.13 Procurement control	5.1
1.14 Software product acquisition	5.1
1.15 Third-party software maintenance	5.4
1.16 Contract application programming	5.5
1.17 Acceptance of facilities	5.6
1.18 Acceptance of technology	3.1, 3.2, 3.3, 5.6

COBIT 第 3 版	COBIT 4.0
AI2 Acquire and maintain application software.	
2.1 Design methods	2.1
2.2 Major changes to existing systems	2.1, 2.2, 2.6
2.3 Design approval	2.1
2.4 File requirements definition and documentation	2.2
2.5 Programme specifications	2.2
2.6 Source data collection design	2.2
2.7 Input requirements definition and documentation	2.2
2.8 Definition of interfaces	2.2

COBIT 第 3 版	COBIT 4.0
2.9 User-machine interface	2.2
2.10 Processing requirements definition and documentation	2.2
2.11 Output requirements definition and documentation	2.2
2.12 Controllability	2.3, 2.4
2.13 Availability as a key design factor	2.2
2.14 IT integrity provisions in application programme software	2.3, DS11.5
2.15 Application software testing	2.8, 7.4
2.16 User reference and support materials	4.3, 4.4
2.17 Reassessment of system design	2.2
AI3 Acquire and maintain technology infrastructure.	
3.1 Assessment of new hardware and software	3.1, 3.2, 3.3
3.2 Preventive maintenance for hardware	DS13.5

COBIT 第 3 版	COBIT 4.0
3.3 System software security	3.1, 3.2, 3.3
3.4 System software installation	3.1, 3.2, 3.3
3.5 System software maintenance	3.3
3.6 System software change controls	AI6.1, AI7.3
3.7 Use and monitoring of system utilities	3.2
AI4 Develop and maintain procedures.	
4.1 Operational requirements and service levels	4.1
4.2 User procedures manual	4.2
4.3 Operations manual	4.4
4.4 Training materials	4.3, 4.4
AI5 Install and accredit systems.	
5.1 Training	7.1
5.2 Application software performance sizing	7.6, DS3.1
5.3 Implementation plan	7.2, 7.3
5.4 System conversion	7.5
5.5 Data conversion	7.5
5.6 Testing strategies and plans	7.2

COBIT 第 3 版	COBIT 4.0
5.7 Testing of changes	7.4, 7.6
5.8 Parallel/pilot testing criteria and performance	7.6
5.9 Final acceptance test	7.7
5.10 Security testing and accreditation	7.6
5.11 Operational test	7.6
5.12 Promotion to production	7.8
5.13 Evaluation of meeting user requirements	7.12
5.14 Management's post-implementation review	7.12
AI6 Manage changes.	
6.1 Change request initiation and control	6.1, 6.4
6.2 Impact assessment	6.2
6.3 Control of changes	7.11
6.4 Emergency changes	6.3
6.5 Documentation and procedures	6.5
6.6 Authorised maintenance	DS5.3
6.7 Software release policy	7.9
6.8 Distribution of software	7.10

COBIT 第 3 版	COBIT 4.0
DS1 Define and manage service levels.	
1.1 Service level agreement (SLA) framework	1.1
1.2 Aspects of SLAs	1.3
1.3 Performance procedures	1.1
1.4 Monitoring and reporting	1.5
1.5 Review of SLAs and contracts	1.6
1.6 Chargeable items	1.3
1.7 Service improvement programme	1.6
DS2 Manage third-party services.	
2.1 Supplier interfaces	2.1
2.2 Owner relationships	2.2
2.3 Third-party contracts	AI5.2
2.4 Third-party qualifications	AI5.3
2.5 Outsourcing contracts	AI5.2
2.6 Continuity of services	2.3
2.7 Security relationships	2.3
2.8 Monitoring	2.4
DS3 Manage performance and capacity.	
3.1 Availability and performance requirements	3.1
3.2 Availability plan	3.4
3.3 Monitoring and reporting	3.5
3.4 Modelling tools	3.1
3.5 Proactive performance management	3.3
3.6 Workload forecasting	3.3

COBIT 第 3 版	COBIT 4.0
3.7 Capacity management of resources	3.2
3.8 Resources availability	3.4
3.9 Resources schedule	3.4
DS4 Ensure continuous service.	
4.1 IT continuity framework	4.1
4.2 IT continuity plan strategy and philosophy	4.1
4.3 IT continuity plan contents	4.2
4.4 Minimising IT continuity requirements	4.3
4.5 Maintaining the IT continuity plan	4.4
4.6 Testing the IT continuity plan	4.5
4.7 IT continuity plan training	4.6
4.8 IT continuity plan distribution	4.7
4.9 User department alternative processing backup procedures	4.8
4.10 Critical IT resources	4.3
4.11 Backup site and hardware	4.8
4.12 Offsite backup storage	4.9
4.13 Wrap-up procedures	4.10
DS5 Ensure systems security.	
5.1 Manage security measures.	5.1

COBIT 第 3 版	COBIT 4.0
5.2 Identification, authentication and access	5.3
5.3 Security of online access to data	5.3
5.4 User account management	5.4
5.5 Management review of user accounts	5.4
5.6 User control of user accounts	5.4, 5.5
5.7 Security surveillance	5.5
5.8 Data classification	PO2.3
5.9 Central identification and access rights management	5.3
5.10 Violation and security activity reports	5.5
5.11 Incident handling	5.6
5.12 Reaccreditation	5.1
5.13 Counterparty trust	5.3, AC18
5.14 Transaction authorisation	5.3, AC17
5.15 Non-repudiation	5.11
5.16 Trusted path	5.11
5.17 Protection of security functions	5.7
5.18 Cryptographic key management	5.8
5.19 Malicious software prevention, detection and correction	5.9

付録 V

COBIT 第 3 版	COBIT 4.0
5.20 Firewall architectures and connections with public networks	5.10
5.21 Protection of electronic value	13.4
DS6 Identify and allocate costs.	
6.1 Chargeable items	6.1
6.2 Costing procedures	6.3
6.3 User billing and chargeback procedures	6.2, 6.4
DS7 Educate and train users.	
7.1 Identification of training needs	7.1
7.2 Training organisation	7.2
7.3 Security principles and awareness training	PO7.4
DS8 Assist and advise customers.	
8.1 Help desk	8.1, 8.5
8.2 Registration of customer queries	8.3, 8.4
8.3 Customer query escalation	8.3
8.4 Monitoring of clearance	10.3
8.5 Trend analysis and reporting	10.1
DS9 Manage the configuration.	
9.1 Configuration recording	9.1
9.2 Configuration baseline	9.1
9.3 Status accounting	9.3
9.4 Configuration control	9.3
9.5 Unauthorised software	9.3
9.6 Software storage	AI3.1
9.7 Configuration management procedures	9.2
9.8 Software accountability	9.1, 9.2
DS10 Manage problems and incidents.	
10.1 Problem management system	10.1, 10.2, 10.3, 10.4
10.2 Problem escalation	10.2
10.3 Problem tracking and audit trail	10.2

COBIT 第 3 版	COBIT 4.0
10.4 Emergency and temporary access authorisations	5.4, 12.3, AI6.3
10.5 Emergency processing priorities	10.1, 8.3
DS11 Manage data.	
11.1 Data preparation procedures	AC1
11.2 Source document authorisation procedures	AC2
11.3 Source document data collection	AC3
11.4 Source document error handling	AC4
11.5 Source document retention	AC5
11.6 Data input authorisation procedures	AC6
11.7 Accuracy, completeness and authorisation checks	AC7
11.8 Data input error handling	AC8
11.9 Data processing integrity	AC9
11.10 Data processing validation and editing	AC10
11.11 Data processing error handling	AC11
11.12 Output handling and retention	AC12
11.13 Output distribution	AC13
11.14 Output balancing and reconcilation	AC14
11.15 Output review and error handling	AC15
11.16 Security provision for output reports	AC16
11.17 Protection of sensitive information during transmission and transport	AC17
11.18 Protection of disposed sensitive information	11.4
11.19 Storage management	11.2
11.20 Retention periods and storage terms	11.2

COBIT 第 3 版	COBIT 4.0
11.21 Media library management system	11.3
11.22 Media library management responsibilities	11.3
11.23 Backup and restoration	11.5
11.24 Backup jobs	11.4
11.25 Backup storage	4.9, 11.3
11.26 Archiving	11.2
11.27 Protection of sensitive messages	11.6
11.28 Authentication and integrity	AC18
11.29 Electronic transaction integrity	5.11
11.30 Continued integrity of stored data	11.2
DS12 Manage facilities.	
12.1 Physical security	12.1, 12.2
12.2 Low profile of the IT site	12.1, 12.2
12.3 Visitor escort	12.3
12.4 Personnel health and safety	12.1, 12.5, ME3.1
12.5 Protection against environmental factors	12.4
12.6 Uninterruptible power supply	12.5
DS13 Manage operations.	
13.1 Processing operations procedures and instructions manual	13.1
13.2 Start-up process and other operations documentation	13.1
13.3 Job scheduling	13.2
13.4 Departures from standard job schedules	13.2
13.5 Processing continuity	13.1
13.6 Operation logs	13.1
13.7 Safeguard special forms and output devices	13.4
13.8 Remote operations	5.11

COBIT 第 3 版	COBIT 4.0
M1 Monitor the processes.	
1.1 Collecting monitoring data	1.2
1.2 Assessing performance	1.4
1.3 Assessing customer satisfaction	1.2
1.4 Management reporting	1.5
M2 Assess internal control adequacy.	
2.1 Internal control monitoring	2.2
2.2 Timely operation of internal controls	2.1
2.3 Internal control level reporting	2.2, 2.3
2.4 Operational security and internal control assurance	2.4
M3 Obtain independent assurance.	
3.1 Independent security and internal control certification/accreditation of IT services	2.5, 3.7
3.2 Independent security and internal control certification/accreditation of third-party service providers	2.5, 3.7
3.3 Independent effectiveness evaluation of IT services	2.5, 3.7
3.4 Independent effectiveness evaluation of third-party service providers	2.5, 3.7
3.5 Independent assurance of compliance with laws, regulatory requirements and contractual commitments	2.5, 3.7
3.6 Independent assurance of compliance with laws, regulatory requirements and contractual commitments by third-party service providers	2.5, 3.7
3.7 Competence of independent assurance function	2.5, 3.7
3.8 Proactive audit involvement	2.5, 3.7
M4 Provide for independent audit.	
4.1 Audit charter	2.5, 3.7
4.2 Independence	2.5, 3.7
4.3 Professional ethics and standards	2.5, 3.7
4.4 Competence	2.5, 3.7
4.5 Planning	2.5, 3.7
4.6 Performance of audit work	2.5, 3.7
4.7 Reporting	2.5, 3.7
4.8 Follow-up activities	2.5, 3.7

付録 V

相互参照: COBIT 4.0 対 COBIT 第 3 版

COBIT 4.0	COBIT第3版
PO1 IT 戦略計画の策定	
1.1 IT 価値の管理	5.3
1.2 ビジネスと IT の整合	新規
1.3 現在の成果の評価	1.7, 1.8
1.4 IT 戦略計画	1.1, 1.2, 1.3, 1.4, 1.6
1.5 IT 実行計画	1.5
1.6 IT ポートフォリオの管理	新規
PO2 情報アーキテクチャの定義	
2.1 企業の情報アーキテクチャモデル	2.1
2.2 企業データディクショナリおよびデータ構文規則	2.2
2.3 データ分類体系	2.3, 2.4
2.4 インテグリティの管理	新規
PO3 技術指針の決定	
3.1 技術指針計画の策定	3.1, 3.3, 3.4
3.2 技術インフラストラクチャ計画	新規
3.3 将来の動向および規制のモニタリング	3.2
3.4 技術標準	3.5
3.5 IT アーキテクチャ委員会	3.5
PO4 ITプロセスと組織及びそのかかわりの定義	
4.1 IT プロセスフレームワーク	新規
4.2 IT 戦略委員会	新規
4.3 IT 運営委員会	4.1
4.4 組織における IT 部門の配置	4.2
4.5 IT 組織の構造	4.3
4.6 役割と責任	4.4, 4.12
4.7 IT の品質保証の責任	4.5
4.8 リスク、セキュリティ、およびコンプライアンスに関する責任	4.6
4.9 データおよびシステムのオーナシップ	4.7, 4.8
4.10 監督	4.9
4.11 職務の分離	4.10

COBIT 4.0	COBIT第3版
4.12 IT スタッフの配置	4.11
4.13 主要 IT 担当者	4.13
4.14 契約社員に関するポリシーおよび手続	4.14
4.15 リレーションシップ	4.15
PO5 IT 投資の管理	
5.1 IT 財務管理フレームワーク	新規
5.2 IT 予算内での優先順位の決定	新規
5.3 IT 予算編成プロセス	5.1, 5.3
5.4 費用管理	5.2, 5.3
5.5 便益管理	5.3
PO6 マネジメントの意図と指針の周知	
6.1 IT ポリシーおよび統制環境	6.1
6.2 企業の IT リスクおよび内部統制のフレームワーク	6.8
6.3 IT ポリシーの管理	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
6.4 ポリシーの展開	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
6.5 IT 目標と指針の周知	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
PO7 IT 人材の管理	
7.1 要員の募集および保持	7.1
7.2 要員の能力	7.2
7.3 役割に応じた人材配置	新規
7.4 要員の研修	7.3, DS7.3
7.5 個人に対する依存	7.4
7.6 要員の人事認可手続	7.5
7.7 従業員の業績評価	7.6
7.8 職務の変更および解雇	7.7
PO8 品質管理	
8.1 品質管理システム	11.3

COBIT 4.0	COBIT第3版
8.2 IT IT 標準および品質の実践基準	11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.16, 11.17, 11.19
8.3 開発および調達標準	11.5, 11.6, 11.7
8.4 顧客中心	新規
8.5 継続的改善	新規
8.6 品質の測定、モニタリング、およびレビュー	11.18
PO9 IT リスクの評価と管理	
9.1 IT リスク管理とビジネスリスク管理の整合	9.1, 9.4
9.2 リスクをめぐる状況の明確化	9.1, 9.4
9.3 イベントの特定	9.3, 9.4
9.4 リスク評価	9.1, 9.2, 9.4
9.5 リスクへの対応	9.5, 9.6
9.6 リスク対応実行計画の維持およびモニタリング	新規
PO10 プロジェクト管理	
10.1 プログラム管理フレームワーク	新規
10.2 プロジェクト管理フレームワーク	10.1
10.3 プロジェクト管理のアプローチ	新規
10.4 利害関係者の関与	10.2
10.5 プロジェクト範囲の記述	10.4
10.6 プロジェクトの各フェーズの開始	10.5, 10.6
10.7 統合プロジェクト計画	10.7
10.8 プロジェクトの資源	10.3
10.9 プロジェクトのリスク管理	10.10
10.10 プロジェクトの品質計画	10.8
10.11 プロジェクト変更コントロール	新規
10.12 保証方法に関するプロジェクト計画	10.9
10.13 プロジェクトの成果の測定、報告、およびモニタリング	新規
10.14 プロジェクトの終了	10.13 (一部)

COBIT 4.0	COBIT第3版
AI1 コンピュータ化対応策の明確化	
1.1 ビジネスの機能的および技術的要件の定義と保守	1.1, 1.9, 1.10, 1.11, 1.12
1.2 リスク分析報告	1.9, 1.10
1.3 実現可能性調査および代替対応策の策定	1.3, 1.7, 1.12
1.4 要件および実現可能性の決定および承認	新規
AI2 アプリケーションソフトウェアの調達と保守	
2.1 概要設計	2.1, 2.2
2.2 詳細設計	2.2, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.13, 2.17
2.3 業務処理統制および可監査性	2.12, 2.14
2.4 アプリケーションのセキュリティおよび可用性	2.12
2.5 調達したアプリケーションソフトウェアの構成および導入	新規
2.6 既存システムの大幅なアップグレード	2.2
2.7 アプリケーションソフトウェアの開発	新規
2.8 ソフトウェアの品質保証	2.15
2.9 アプリケーション要件の管理	新規

COBIT 4.0	COBIT第3版
2.10 アプリケーションソフトウェアの保守	新規
AI3 技術インフラストラクチャの調達と保守	
3.1 技術インフラストラクチャの調達計画	PO3.4, 1.18, 3.1, 3.3, 3.4
3.2 インフラストラクチャ資源の保護と可用性	1.18, 3.1, 3.3, 3.4, 3.7
3.3 インフラストラクチャの保守	1.18, 3.1, 3.3, 3.4, 3.7
3.4 実現可能性テスト環境	新規
AI4 運用と利用の促進	
4.1 運用上のソリューションの計画	4.1
4.2 ビジネス部門の管理者への知識の移転	PO11.11, 4.2
4.3 エンドユーザへの知識の移転	PO11.11, 2.16, 4.4
4.4 運用スタッフおよびサポートスタッフへの知識の浸透	PO11.11, 2.16, 4.4
AI5 IT 資源の調達	
5.1 調達のコントロール	1.4, 1.13, 1.14
5.2 サービスプロバイダとの契約の管理	DS2.3, DS2.5
5.3 サービスプロバイダの選定	1.4, DS2.4
5.4 ソフトウェアの調達	1.15
5.5 開発資源の調達	1.16
5.6 インフラストラクチャ、設備、および関連サービスの調達	1.17, 1.18

COBIT 4.0	COBIT第3版
AI6 変更管理	
6.1 変更の標準と手続	6.1
6.2 影響評価、優先順位付け、および認可	6.2
6.3 緊急変更	6.4
6.4 変更の状況追跡および報告	6.1
6.5 変更の終了および文書化	6.5
AI7 ソリューションおよびその変更の導入と認定	
7.1 研修	5.1
7.2 テスト計画	PO11.12, PO11.13, PO11.14, PO11.15, 5.3
7.3 導入計画	5.3
7.4 テスト環境	PO11.12, PO11.13, PO11.14, PO11.15, 2.15, 5.7
7.5 システムおよびデータの変換	5.4, 5.5
7.6 変更のテスト	5.7
7.7 最終受け入れテスト	5.9
7.8 本番環境への移行	5.12
7.9 ソフトウェアのリリース	6.7
7.10 システムの配布	6.8
7.11 変更の記録と追跡	6.3
7.12 導入後レビュー	5.13, 5.14

COBIT 4.0	COBIT第3版
DS1 サービスレベルの定義と管理	
1.1 サービスレベル管理フレームワーク	1.1, 1.3
1.2 サービスの定義	新規
1.3 サービス・レベル・アグリーメント	1.2
1.4 オペレーショナル・レベル・アグリーメント	新規
1.5 サービスレベル達成状況のモニタリングと報告	1.4
1.6 サービス・レベル・アグリーメントおよび請負契約の見直し	1.5
DS2 サードパーティのサービスの管理	
2.1 すべてのサービスプロバイダとのリレーションシップの特定	2.1
2.2 サービスプロバイダとのリレーションシップの管理	2.2
2.3 サービスプロバイダにかかわるリスクの管理	2.6, 2.7
2.4 サービスプロバイダの成果のモニタリング	2.8

COBIT 4.0	COBIT第3版
DS3 性能とキャパシティの管理	
3.1 性能とキャパシティの計画策定	3.1, 3.4
3.2 現状の性能とキャパシティ	3.7
3.3 将来の性能とキャパシティ	3.5
3.4 IT 資源の可用性	3.2, 3.8, 3.9
3.5 モニタリングと報告	3.3
DS4 継続的なサービスの保証	
4.1 IT 継続フレームワーク	4.1, 4.2
4.2 IT 継続計画	4.3
4.3 重要な IT 資源	4.4, 4.10
4.4 IT 継続計画の保守	4.5
4.5 IT 継続計画のテスト	4.6
4.6 IT 継続計画に関する研修	4.7
4.7 IT 継続計画の配付	4.8

COBIT 4.0	COBIT第3版
4.8 IT サービスの復旧および再開	4.9, 4.11
4.9 遠隔地におけるバックアップ保管施設	4.12, 11.25
4.10 再開後のレビュー	4.13
DS5 システムセキュリティの保証	
5.1 IT 財務管理フレームワーク	5.1, 5.12
5.2 IT セキュリティ計画	新規
5.3 ID 管理	5.2, 5.3, 5.9, AI6.6
5.4 ユーザアカウントの管理	5.4, 5.5, 5.6, 10.4
5.5 セキュリティのテスト、監視、モニタリング	5.6, 5.7, 5.10
5.6 セキュリティインシデントの定義	5.11
5.7 セキュリティ技術の保護	5.17
5.8 暗号鍵の管理	5.18

付録 V

COBIT 4.0	COBIT第3版
5.9 不正ソフトウェアの阻止、発見、および是正	5.19
5.10 ネットワークのセキュリティ	5.20
5.11 機密データの交換	5.15, 5.16
DS6 費用の捕捉と配賦	
6.1 サービスの定義	6.1
6.2 IT 財務管理	6.3
6.3 費用モデルの策定と費用請求	6.2
6.4 費用モデルの保守	6.3
DS7 利用者の教育と研修	
7.1 教育と研修のニーズの特定	7.1
7.2 教育と研修の実施	7.2
7.3 受講研修内容の評価	新規
DS8 サービスデスクとインシデントの管理	
8.1 サービスデスク	8.1
8.2 顧客からの問い合わせの登録	10.3
8.3 インシデントエスカレーション	8.2
8.4 インシデントのクローズ	8.2

COBIT 4.0	COBIT第3版
8.5 傾向分析	8.1
DS9 構成管理	
9.1 構成リポジトリとベースライン	9.1, 9.2, 9.8
9.2 構成管理アイテムの特定と管理	9.7
9.3 構成のインテグリティのレビュー	9.3, 9.4, 9.5
DS10 問題管理	
10.1 問題の特定と分類	8.5
10.2 問題の追跡と解決	新規
10.3 問題のクローズ	8.4
10.4 変更管理、構成管理、および問題管理の統合	新規
DS11 データ管理	
11.1 データ管理におけるビジネス要件	新規
11.2 データの保管および保持の調整	11.19, 11.20, 11.26, 11.30
11.3 メディアライブラリ管理システム	11.21, 11.22, 11.25

COBIT 4.0	COBIT第3版
11.4 廃棄	11.18, 11.24
11.5 バックアップと復元	11.23
11.6 データ管理におけるセキュリティ上の要件	11.16, 11.17, 11.27
DS12 物理的環境の管理	
12.1 サイトの選定と配置	12.1, 12.2
12.2 物理的なセキュリティ対策	12.1, 12.2
12.3 物理的アクセス	10.4, 12.3
12.4 環境的要因からの保護	12.5
12.5 物理的施設の管理	12.6, 12.9
DS13 オペレーション管理	
13.1 オペレーション手続と指示	13.1, 13.2, 13.5, 13.6
13.2 業務のスケジュール策定	13.3, 13.4
13.3 IT インフラストラクチャのモニタリング	新規
13.4 機密文書と出力デバイス	5.21, 13.7
13.5 ハードウェアの予防的保守	AI3.2

COBIT 4.0	COBIT第3版
ME1 IT 成果のモニタリングと評価	
1.1 モニタリングアプローチ	1.0
1.2 モニタリングデータの定義と収集	1.1, 1.3
1.3 モニタリング方法	新規
1.4 成果評価	1.2
1.5 取締役会およびマネジメント層への報告	1.4
1.6 是正措置	新規
ME2 内部統制のモニタリングと評価	
2.1 内部統制フレームワークのモニタリング	2.0
2.2 監督レビュー	2.1
2.3 コントロール例外事項	新規

COBIT 4.0	COBIT第3版
2.4 コントロールセルフ評価	2.4
2.5 内部統制の保証	新規
2.6 サードパーティにおける内部統制	3.6
2.7 是正措置	新規
ME3 規制に対するコンプライアンスの保証	
3.1 IT に影響を及ぼす可能性がある法規制の特定	PO8.1, PO8.3, PO8.4, PO8.5, PO8.6
3.2 法的要件への対応の最適化	PO8.2
3.3 法的要件へのコンプライアンスの評価	新規

COBIT 4.0	COBIT第3版
3.4 コンプライアンスの積極的な保証	新規
3.5 報告の統合	新規
ME4 IT ガバナンスの提供	
4.1 IT ガバナンスフレームワークの確立	新規
4.2 戦略との整合	新規
4.3 価値の提供	新規
4.4 資源の管理	新規
4.5 リスクの管理	新規
4.6 成果の測定	新規
4.7 独立した保証	新規

付録 Ⅵ

研究開発へのアプローチ

研究開発へのアプローチ

COBIT フレームワークの内容の作成は、COBIT 運営委員会の監督下で行われている。COBIT 運営委員会は各国の産業界、学術界、および政府機関、そして IT ガバナンス、保証、コントロール、およびセキュリティ団体の代表者で構成されている。プロジェクトの研究開発における中間成果物の品質保証と専門的なレビューの実施を目的として、国際的なワークグループが設置されている。包括的なプロジェクト方針は、IT ガバナンス協会(ITGI)によって規定されている。

旧版の COBIT

COBIT フレームワークが第 1 版で定義された後、各種国際標準やガイドライン、ベストプラクティスの研究成果を基に、コントロール目標が作成された。次に、これらのコントロール目標が適切に導入されているかどうかを評価する監査ガイドラインが作成された。第 1 版および第 2 版のための研究では、各国で認知された情報源の収集と分析が行われた。この研究は、欧州(アムステルダム自由大学)、米国(カリフォルニア州立工科大学)、およびオーストラリア(ニューサウスウェールズ大学)の各チームにより進められた。研究者たちには、国際技術規格、行動規範、品質基準、監査における専門基準、および業界における実践基準方法と要件の収集、レビュー、評価、および適切な反映が課された。これらの基準、実践基準方法、要件などは、フレームワークと個々のコントロール目標の両方に関連している。収集および分析の完了後、研究者たちは各ドメインおよびプロセスを詳細に検討し、特定の IT プロセスに適用できる新たなコントロール目標またはコントロール目標の変更を提案するという課題に取り組んだ。研究成果の統合整理は COBIT 運営委員会により実施された。

COBIT 第 3 版プロジェクトではマネジメントガイドラインが作成され、新規/改訂された国際的なガイドラインや基準などに基づいて、COBIT 第 2 版の改訂作業が行われた。さらに、増大する経営上のコントロールへの対応、成果管理の導入、IT ガバナンスのさらなる進化に向け、COBIT フレームワークが改訂、拡張された。マネジメント層によるフレームワークの適用を可能にするとともに、マネジメント層がコントロールの導入とその情報技術/関連技術の改善を評価して意思決定できるようにし、成果を測定できるようにするため、マネジメントガイドラインには、コントロール目標に関連する成熟度モデル、主要成功要因、重要目標達成指標、および重要成果達成指標が組み込まれた。

マネジメントガイドラインの編集作業は、学術界、政府機関、および IT ガバナンス、保証、コントロール、セキュリティ分野の専門家 40 名で構成される国際的な委員会により実施された。これらの専門家は、専門の進行役が主導する滞在型ワークショップに参加した。このワークショップでは、COBIT 運営委員会が定めた作成ガイドラインが使用された。このワークショップは、Gartner Group および PricewaterhouseCoopers の多大な協力を得て実施された。これらの団体は、業界をリードする知識を提供するのみならず、コントロール、成果管理、および情報セキュリティの専門家を参加させることでワークショップに寄与した。このワークショップにより、COBIT の 34 の上位コントロール目標それぞれの成熟度モデル、主要成功要因、重要目標達成指標、および重要成果達成指標の草案が完成した。この最初の成果物の品質保証は COBIT 運営委員会が担当し、その結果は ISACA の Web サイトで公開された。マネジメントガイドライン文書には、COBIT フレームワークとの統合と整合を保ちつつ、主としてマネジメント層が活用できる手段が記載された。

COBIT 運営委員会の監督の下、ISACA 各支部の会員により、新規/改訂された国際的なガイドラインや基準などに基づいて COBIT 第 3 版のコントロール目標が改訂された。この改訂の目的は、すべての資料の総合的な分析やコントロール目標の再作成ではなく、補足的な改訂作業を行うことであった。マネジメントガイドラインの改訂結果を基に、COBIT フレームワーク、特に上位コントロール目標における検討事項、達成目標、成功要因に関する記述が改訂された。COBIT 第 3 版は 2000 年 7 月に発行された。

COBIT プロジェクトにおける活動の最新情報

COBIT の知識体系を継続的に発展させるため、COBIT 運営委員会は過去 2 年にわたり、COBIT のさまざまな側面について詳細な研究を実施している。これらの集中的な研究プロジェクトでは、コントロール目標とマネジメントガイドラインの各要素が対象とされた。研究対象となった特定領域の一部を以下に示す。

コントロール目標の研究

- COBIT－IT ガバナンスの調整(ボトムアップ)
- COBIT－IT ガバナンスの調整(トップダウン)
- COBIT およびその他の詳細な標準－COBIT と ITIL、CMM、COSO、PMBOK、ISF、および ISO 17799 との間の詳細な紐付け。この紐付けにより、用語、定義、概念の面で COBIT とこれらの標準とを整合。

付録VI

マネジメントガイドラインの研究

- KGI-KPI 因果関係分析
- KGI/KPI/CSF の品質レビューーKPI/KGI 因果関係分析に基づき、CSF を「外部に求めるもの」と「内部に求めるもの」に分類した。
- 指標概念の詳細分析−指標の専門家による綿密な検討作業により、指標概念の強化、「プロセス-IT-ビジネス」という段階的な指標の作成、指標の品質基準の定義が進められた。
- ビジネス達成目標、IT 達成目標、および IT プロセスの紐付けー8 つの異なる業界における詳細な調査から、COBIT プロセスが特定の IT 達成目標の達成、ひいてはビジネス達成目標の達成を支援する方法について、より詳しい洞察が得られた。この結果は法則化されて組み込まれている。
- 成熟度モデルの内容のレビューープロセス間およびプロセス内の成熟度レベルの一貫性と品質(成熟度モデルの特性の定義改善など)が確保された。

上記のプロジェクトはすべて COBIT 運営委員会により着手、監督され、日常の管理およびフォローアップはより少人数の COBIT コアチームにより実施された。前述した調査プロジェクトの大半は、ISACA 会員、COBIT ユーザ、専門アドバイザーおよび学術関係者で構成される専門家とボランティアのチームの多大なる協力の下で行われた。地域別開発グループがブリュッセル(ベルギー)、ロンドン(英国)、シカゴ(米国イリノイ州)、キャンベラ(オーストラリア首都特別地域)、ケープタウン(南アフリカ)、ワシントン(米国ワシントン DC)、およびコペンハーゲン(デンマーク)に設立された。各グループでは 5～10 名の COBIT ユーザが、1 年あたり平均して 2～3 回の会合を持ち、特定の調査を進め、COBIT コアチームから割り当てられたレビュー作業を実施した。さらに、一部の調査プロジェクトが University of Antwerp Management School (UAMS)やハワイ大学などのビジネススクールに委任された。

このような調査作業の結果は、長年にわたる COBIT ユーザからのフィードバックや、コントロールプラクティスなどの新たな成果物の開発時に指摘された問題とともに、核となる COBIT プロジェクトに反映され、COBIT のコントロール目標、マネジメントガイドライン、およびフレームワークの改訂と改善に活用された。コントロール目標とマネジメントガイドラインの内容のレビューおよび全体的な改訂作業にあたる主要な開発研究所が 2 箇所に設けられた。それぞれの研究所では、世界中から 40 名を超える IT ガバナンス、管理、およびコントロールの専門家(管理者、コンサルタント、学術関係者、および監査人)が作業を行った。さらに少人数のグループによって、上記のように大規模な作業で生成された重要なアウトプットの改善または最終決定が行われた。

最終草案に対し、約 100 名の参加者による完全公開レビュープロセスが実施された。寄せられた多数のコメントは、COBIT 運営委員会が実施する最終レビューワークショップで分析された。

ワークショップでの作業結果は、COBIT 運営委員会、COBIT コアチーム、および ITGI により処理され、新たな COBIT 資料として本版に盛り込まれている。COBIT Online®の導入により、COBIT の中核となる内容を、より容易に周辺動向に則した最新の内容に維持できるようになった。この情報源は COBIT の内容のマスタリポジトリとして使用される。COBIT Online は、ユーザからのフィードバックと、特定分野の内容の定期的なレビューにより改訂される。COBIT の内容をオフラインで参照する手段として、定期的に資料(紙媒体または電子媒体)が発行される。

付録 Ⅶ

用語集

用語集

アクセスコントロール－コンピュータシステムの資源へのアクセスを制限およびコントロールする仕組み。不正侵入や不正利用を防ぐ目的で導入する論理的または物理的コントロール手段。

アクティビティ－COBIT プロセスの運用に必要な主な活動。

業務処理統制－コンピュータ化対応策(アプリケーション)に組み込まれている一連のコントロール。

アプリケーションプログラム－データ入力、更新、または照会などの操作によりビジネスデータを処理するプログラム。システムプログラム(オペレーティングシステム、ネットワークコントロールプログラムなど)およびユーティリティプログラム(*copy*、*sort* など)と対照的。

監査規定－ISACA 理事会により承認されている、内部監査活動の目的、権限、および実行責任を定義した文書。

認証－ユーザの身元と電子情報に対するユーザのアクセス権限を確認する処理。認証の目的は、不正ログオン操作の防止である。

バランススコアカード－管理者がビジネス成果の達成状況を迅速かつ包括的に確認できるようにすることで、構想と戦略の面から企業の活動を評価する手法。財務、顧客、業務、学習という 4 つの視点からビジネスを評価するための管理ツールである。(Robert S. Kaplan および David Norton、1992)

ベンチマーキング－経営管理、特に戦略経営管理において用いられるプロセスであり、ベストプラクティス(一般にその企業が属する業界のベストプラクティス)に照らして、企業が自社のビジネスプロセスのさまざまな側面を評価する仕組み。

ビジネスプロセス－「プロセス」を参照。

能力－実施または達成に必要な特性を有していること。

CEO－最高経営責任者。

CFO－最高財務責任者。

CIO－最高情報責任者。最高技術責任者(CTO)とも呼ばれる。

能力成熟度モデル(CMM)－ソフトウェアエンジニアリング研究所(SEI)が開発したソフトウェア能力成熟度モデル(CMM)は、組織がソフトウェア開発プロセスの成熟度評価および成熟度レベルの向上に役立つベストプラクティスを特定するためのモデルであり、多数の組織に導入されている。

構成管理アイテム(CI)－構成管理のコントロール下にある(またはあるべき)、インフラストラクチャ、またはインフラストラクチャに関連する変更要求などのアイテムの構成要素。CI には、さまざまな複雑性、サイズ、タイプのものがあり、システム全体(すべてのハードウェア、ソフトウェア、文書を含む)から単一モジュール、小規模ハードウェアコンポーネントまで多岐にわたる。

構成管理－システムのライフサイクル全体において、一連の構成管理アイテムに対する変更をコントロールすること。

継続性－中断の発生を防止、削減し、中断から回復すること。これに関連して「事業回復計画」、「災害復旧計画」、「緊急時対応計画」という用語が用いられるが、これらはすべて継続性の回復面に焦点を当てている。

コントロール－事業目標の達成、および望ましくないイベントの阻止または発見を合理的に保証するように設計されたポリシー、手続、実践基準方法、および組織構造。

コントロールフレームワーク－支援コントロールモデルの適用により各ビジネスプロセスオーナの実行責任の履行を促進する、ビジネスプロセスオーナ向けの体系。

コントロール目標－コントロール手続を特定のプロセスに導入することで達成すべき、所期の結果または目的の記述。

コントロールプラクティス－資源の責任ある利用、適切なリスク管理、および IT と事業内容の整合性の確保によりコントロール目標の達成を支援する主要なコントロールメカニズム。

付録Ⅶ

COSO－トレッドウェイ委員会組織委員会。コーポレートガバナンスの国際公認基準となっている。*www.coso.org* を参照。

CSF－主要成功要因。

顧客－企業の IT サービスを利用する人または社内外の組織。

ダッシュボード－各レベルでの組織に対する期待事項を設定し、設定された目標に照らして成果達成状況を継続的にモニタリングするためのツール。

データ分類体系－データを重要性、機密性、オーナシップなどの因子によって分類する、企業全体で適用された体系。

データディクショナリ－データ要素の定義と表現を記述したメタデータの集合。

データオーナ－電子データのインテグリティ、正確な報告、および使用の責任を負う担当者(通常は管理者や取締役)。

DCO－詳細なコントロール目標。DCO は、特定のコントロール目標の構成要素である。

発見的コントロール－プロセスまたは最終成果物に対して重大な影響を及ぼすと企業が判断したイベント(望ましいものと望ましくないものの両方)、エラー、およびその他の事象を特定するために用いられるコントロール。

ドメイン－コントロール目標を IT 投資ライフサイクルの論理的段階別にグループ化したもの。

企業－共通の目的に向かってともに作業する個人の集合体。一般に会社、公的機関、慈善団体、トラストなどの組織形態の枠内で捉えられる。

エンタープライズアーキテクチャ－ビジネス達成目標とビジネス目標の実現に向けたビジネス指向の技術ロードマップ。

IT 指向のエンタープライズアーキテクチャ－資源(アプリケーション、情報、インフラストラクチャ、要員)を使用した、明確に定義されたプロセスにより実現する IT の提供対応。

企業のデータディクショナリ－企業内で使用される各データ要素の名前、タイプ、値の範囲、ソース、記録体系、およびアクセスの認可。各データを使用するアプリケーションプログラムを特定できるため、データ構造について検討する際に、影響を受けるプログラムのリストを作成できる。PO2.2 を参照。

フレームワーク－「コントロールフレームワーク」を参照。

全般統制－「IT 全般統制」とも言う。組織の IT システムのすべての機能と、広範なコンピュータ化対応策(アプリケーション)に適用されるコントロール。

ガバナンス－組織の方向付け、管理、コントロールを行う手段。

ガイドライン－物事の遂行方法を記述したもの。手続よりも規定性が低い。

インシデント－サービスの標準運用方法から逸脱し、サービス品質への悪影響または低下を招く(または招く可能性のある)イベント(「ITIL」でのインシデントと同等)。

情報アーキテクチャ－「IT アーキテクチャ」を参照。

インフラストラクチャ－アプリケーション処理を可能にする技術、要員、および設備。

内部統制－事業目標の達成、および望ましくないイベントの阻止または発見と是正を合理的に保証するように設計されたポリシー、手続、実践基準方法、および組織構造。

ISO 17799－国際標準化機構(ISO)が策定した情報セキュリティ管理実施基準。

ISO 9001:2000－国際標準化機構(ISO)が策定した品質管理実施基準。ISO 9001:2000 は、顧客の要求事項と当該法的要件を満たす製品を一貫して提供できる能力を証明し、顧客満足度を高めることを目標とする組織の品質管理システムに求められる要件を定めている。

IT－情報技術。

IT アーキテクチャ－既存の IT を拡張または維持し、新たな IT を獲得して企業の戦略目標およびビジネス達成目標を実現するための統合フレームワーク。

IT 投資ダッシュボード－IT 関連の投資プロジェクトの費用と収益を、企業の事業価値の観点でまとめた図表。

IT 戦略計画－ビジネス部門と IT 部門の連携による、企業の戦略目標達成に向けた IT 資源活用について定めた長期計画(3～5 カ年)。

IT 戦略委員会－主な IT 関連事項/決定に取締役会を確実に関与させるために設置する取締役会レベルの委員会。

IT 実行計画－IT 戦略計画に定められた方向性を基に、求められるイニシアチブ、資源の要件、および資源と便益をモニタリング/管理する方法を定めた中期計画(6～18 カ月)。

ITIL－英国商務局(OGC)の IT インフラストラクチャライブラリ。IT 運用サービスの管理と提供に関する一連の指針。

重要施策－プロセス達成目標の実現に向けプロセスオーナが実施する必要がある重要な管理の実践基準方法。

KGI－重要目標達成指標(Key goal indicator)。

KPI－重要成果達成指標(Key performance indicator)。

成熟度－期待される目標を達成する上で、ビジネス部門が各プロセスに対して保持できる信頼性と依存度の度合いを示す。

指標－目標に対する成果を測定するための基準。

OLA－オペレーショナル・レベル・アグリーメント。IT サービス提供をする各職域間の関係を定義した内部合意文書。

組織－企業の構成体系。

成果－プロセスの実際の導入または達成状況。

成果管理－従業員、チーム、プロセス、運用または財務上の成果測定など、あらゆるタイプの成果測定を管理する能力。この用語には、成果測定の完結したコントロールと定期的なモニタリングの意味も含まれる。

PMBOK－プロジェクトマネジメント知識体系(Project Management Body of Knowledge)。プロジェクトマネジメント協会(PMI)が策定したプロジェクトマネジメント基準。

PMO－PMO(プロジェクト・マネジメント・オフィス)。

ポリシー－一般に、概要的な行動原則および方針を記述した文書を指す。ポリシーの目的は、企業の経営チームが確立した理念、目標、および戦略計画と合致した意思決定を、現在および将来において実施できるよう導くことにある。ポリシーには、本来の内容に加え、ポリシーを遵守しなかった場合の処遇、例外への対処方法、およびポリシー遵守状況の確認と評価方法も記述する必要がある。

ポートフォリオ－事業収益の最大化に向けて選定、管理、モニタリングされるプログラム、プロジェクト、サービス、または資産の集合。

予防的コントロール－プロセスまたは最終製品に対して重大な悪影響を及ぼす可能性があると組織が判断した不測のイベント、エラー、およびその他の事象を未然に防止するための内部統制。

PRINCE2－Projects in a Controlled Environment。プロジェクトの組織化、マネジメント、およびコントロールを網羅するプロジェクト管理手法。

付録Ⅶ

問題－1 つ以上のインシデントの背後にある未知の根本原因。

手続－物事の特定の遂行方法、すでに確立されている物事の実行方法、または定義された一定の順序で行う一連の手続きを記述したもの。これにより、何らかの行動について、一貫性があり再現可能であることが保証される。

プロセス－一般に、組織のポリシーおよび標準に応じて決まる手続の集合を指す。複数のソース(他のプロセスを含む)からインプットを取り込み、インプットを処理し、プロセスのユーザに対してアウトプット(他のプロセスを含む)を生み出す。プロセスには、ビジネス上の明確な存在理由、説明責任を負うオーナ、プロセス実行に関連する明確な役割と実行責任、および成果測定手法がある。

プログラム－相互に依存するプロジェクトの体系的な集合。プログラムには、明確に定められたビジネス成果の達成に求められる(必要かつ十分な)事業全般、プロセス、要員、技術、組織の活動が含まれる。

プロジェクト－合意された日程と予算に基づく、定義された能力(求められるビジネス成果の達成に必要だが十分ではない)の企業への提供に関連する活動の体系的な集合。

QMS－品質マネジメントシステム。最終的にビジネス成果の向上につながる各種プロセスの改善とコントロールに必要なポリシーと手続を体系化したシステム。

RACI チャート－標準の組織フレームワークにおいて、実行責任者、説明責任者、協議先、報告先を示す。

回復力－システムまたはネットワークが、認識できる影響を最小限に抑えながら、中断から自動的に回復する能力。

リスク－特定の脅威によって資産または資産グループの脆弱性が悪用され、資産の損失または損害が生じる可能性。一般に、リスクは影響の度合いと発生の可能性の両方を考慮して測定される。

根本原因の分析－一般にエラーや問題などの結果から学習する仕組み。

職務分離－取引の開始と記録や資産管理について、実行責任者を切り離すことで、エラーや不正行為を防止または発見できるようにする基本的な内部統制。

単一窓口－IT サービスのユーザを対象とした、IT 組織内の単一連絡窓口。

サービスプロバイダ－顧客にサービスを供給する組織。

SLA－サービス・レベル・アグリーメント。サービスプロバイダと顧客/ユーザの間で締結され、サービスについて合意されたサービスレベルを記述した合意文書。

標準－企業または IT 管理部門により受け入れられ、承認された、ビジネス活動指針または技術製品。標準は、ポリシーまたはプロセスを支援するため、あるいは運用上の必要性に応じて導入できる。ポリシーと同様に、標準には、違反を検知する方法を記述する必要がある。

SDLC－システム開発ライフサイクル。ソフトウェアシステムの開発過程または調達過程におけるフェーズ。一般的なフェーズとして、実現可能性調査、要件調査、要件定義、詳細設計、プログラミング、テスト、導入、および導入後レビューを挙げることができる。

TCO－総所有費用。

技術インフラストラクチャ計画－技術インフラストラクチャの保守と開発に関する計画。

ユーザ－企業のシステムを利用する者。