JISTAオープンフォーラム2014in関西

システム監査の勘所

～ITストラテジストとシステム監査～

2014年9月20日

特定非営利活動法人 日本システム監査人協会

林　裕正

本日の目次

■日本システム監査人協会のご紹介

■システム監査とは

■システム監査の勘所

★公開されている基準や、協会の情報以外の内容は講演者の個人見解です。

日本システム監査人協会のご紹介

Systems Auditors Association of Japan

■日本システム監査人協会の設立経緯

■日本システム監査人協会の事業

■公認システム監査人制度

■近畿支部のご紹介

日本システム監査人協会の設立経緯

■設立経緯
・システム監査技術者試験合格者とシステム監査登録企業を核に、任意団体として設立。発足は、1987年12月。
・2002年2月に特定非営利活動法人（NPO）として法人化。入会資格も一般にも解放。

■設立目的
・一般社会へのシステム監査の普及・啓発
・システム監査人の育成、認定
・システム監査技法の維持・向上
・健全な情報化社会の発展に寄与する

■会員構成
正会員（個人）：793名
正会員（団体）： 31社 （2013年12月末現在）

日本システム監査人協会の事業

■事業
- ・公認システム監査人認定
- ・教育研修（特別認定講習、継続教育講習）
- ・出版

「情報システム監査実践マニュアル」（赤本）
「個人情報保護マネジメントシステム実践マニュアル」（緑本）
「J-SOX対応IT統制監査実践マニュアル」（黄本）

■研究会活動

月例研究会（講演）、事例研究会、システム監査基準研究会、情報セキュリティ監査研究会、個人情報保護監査研究会

■支部活動

全国を8区域に分けて支部を結成し、セミナー等を実施

公認システム監査人制度

■制度概要

システム監査技術者試験合格者及びそれと同等の能力を有する者を審査し、監査人として登録を認める制度。

■名称と認定者数(2013年12月末現在)

・公認システム監査人(Certified Systems Auditor):353名

・システム監査人補(Associate Systems Auditor) :116名

■認定要件

CSAは協会認定委員による書類審査と面接にて認定。

ASAは書類審査による認定。

■有効期限

有効期限は2年。必要な継続教育を受けることで更新可能。

近畿支部のご紹介

■定例研究会（奇数月第3金曜日）

・近畿支部会員他を講師とする研究発表会

■システム監査勉強会（偶数月第3土曜日）

・本部月例研究会のDVD視聴による勉強会

■システム監査セミナー

・システム監査体験セミナー（入門編・実践編）、事例セミナー

■支部会員による研究活動

・システム監査法制化研究プロジェクト

・BCP研究プロジェクト

・ソフトウェア著作権研究プロジェクト

■支部会員向けサービス

・メルマガ／支部ホームページによる会員向け情報発信

最近の定例研究会のテーマ

■マネジメント規格の統合的な利用と効果的な認証審査（第139回）

■あなたのへそくり、奥様にばれていませんか？（第140回）

■サポート期限切れOSの守り方（第143回）

■中小企業におけるリスク認識の手法について（第145回）

■暗号通貨ビットコインの脆弱性と可能性（第147回）

⇒詳しくは近畿支部HPで！

http://www.saajk.org/

システム監査とは

■監査とは

■システム監査とは

■システム監査の目的

■システム監査に適用される基準

■システム監査基準と管理基準の構成

監査とは

対　象	企業や自治体など あらゆる組織体について、
内　容	経営や業務の活動が適切に行われていることを、法令や規定などに照らして点検・評価し、
目　的	その活動が適切でなければ指摘し、正しい方向へ誘導すること。 一部の監査では適切であることを外部へ保証すること。

システム監査とは

システム監査とは、業務処理で使用されている情報処理システムを対象に、経営に役立っているか、または組織体内外に対して信頼性が維持されているかなどを監査すること。

システム監査の目的

システム監査の目的は、組織体の情報システムにまつわるリスクに対するコントロールが、リスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証または評価することによって、保証を与えあるいは助言を行い、もってＩＴガバナンスの実現に寄与することにある。

（システム監査基準－2004年版－より）

システム監査に適用される基準

- システム監査基準（経済産業省）
- システム管理基準（経済産業省）
- 情報セキュリティ監査基準（経済産業省）
- 情報セキュリティ管理基準（経済産業省）
- 情報システム安全対策基準（経済産業省）
- コンピュータウイルス対策基準（経済産業省）
- コンピュータ不正アクセス対策基準（経済産業省）
- 地方公共団体における情報セキュリティ監査に関するガイドライン（総務省）
- 金融機関等のシステム監査指針（FISC）

など

システム監査基準と管理基準の構成

システム監査基準（20項目）

Ⅰ．前文
Ⅱ．システム監査の目的
Ⅲ．一般基準（8項目）
Ⅳ．実施基準（7項目）
Ⅴ．報告基準（5項目）

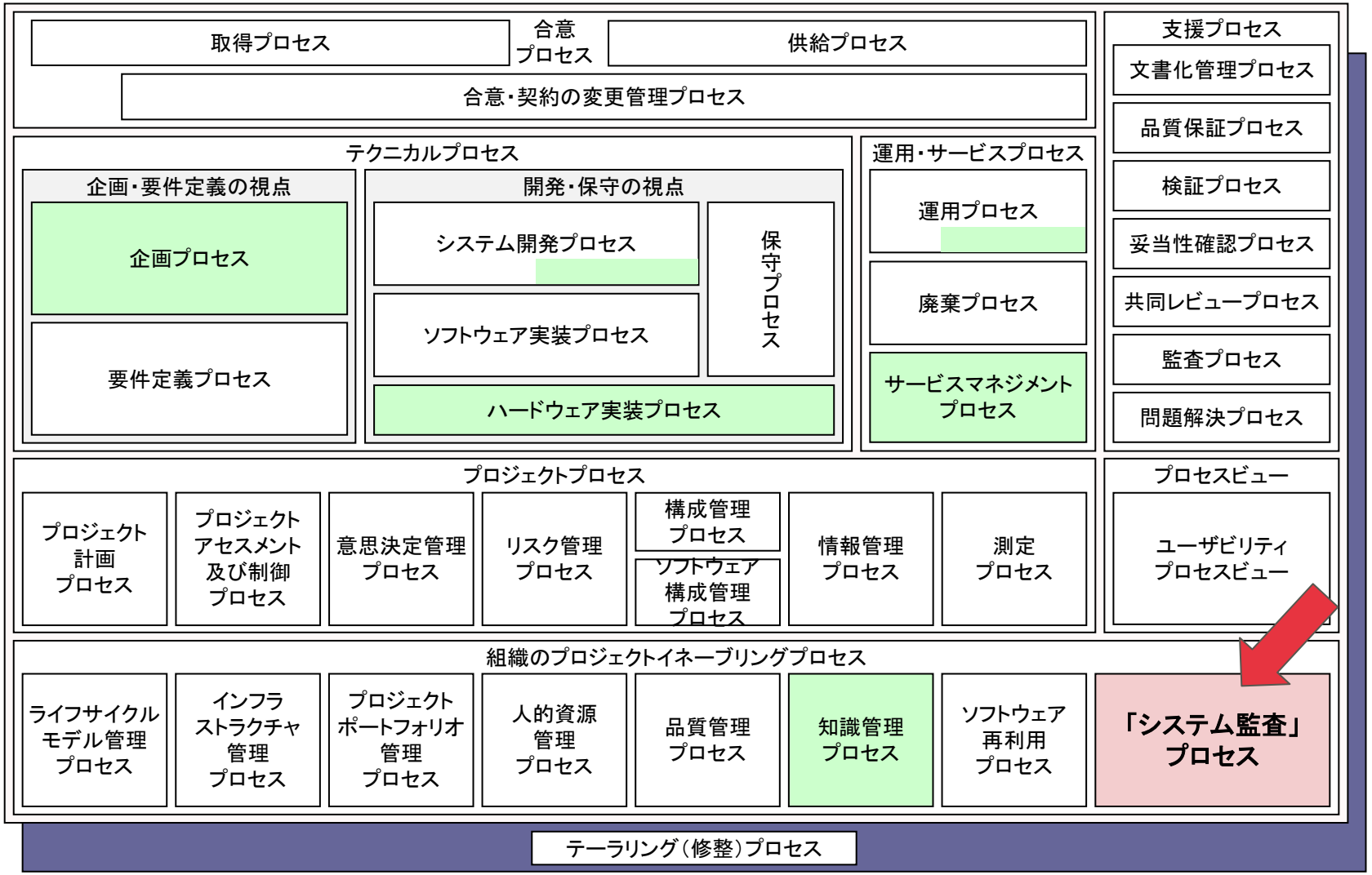
行動の規範

システム管理基準（287項目）

前文
Ⅰ．情報戦略（47項目）
Ⅱ．企画業務（23項目）
Ⅲ．開発業務（49項目）
Ⅳ．運用業務（73項目）
Ⅴ．保守業務（19項目）
Ⅵ．共通業務（76項目）

判断の尺度

（参考）共通フレーム2013のプロセス体系



（参考）政府情報システム標準ガイドライン

■政府情報システムの整備及び管理に関する標準ガイドライン（案）

・2014年8月21日　総務省がパブリックコメントを募集

・本ガイドライン（案）におけるシステム監査の記述

第2編　ITガバナンス

第8章　システム監査の計画

情報システムのリスクと対応状況を客観的に評価

第3編　ITマネジメント

第10章　システム監査の実施

監査体制の確立、監査実施計画書の作成、
監査の実施、指摘事項への対応、フォローアップ

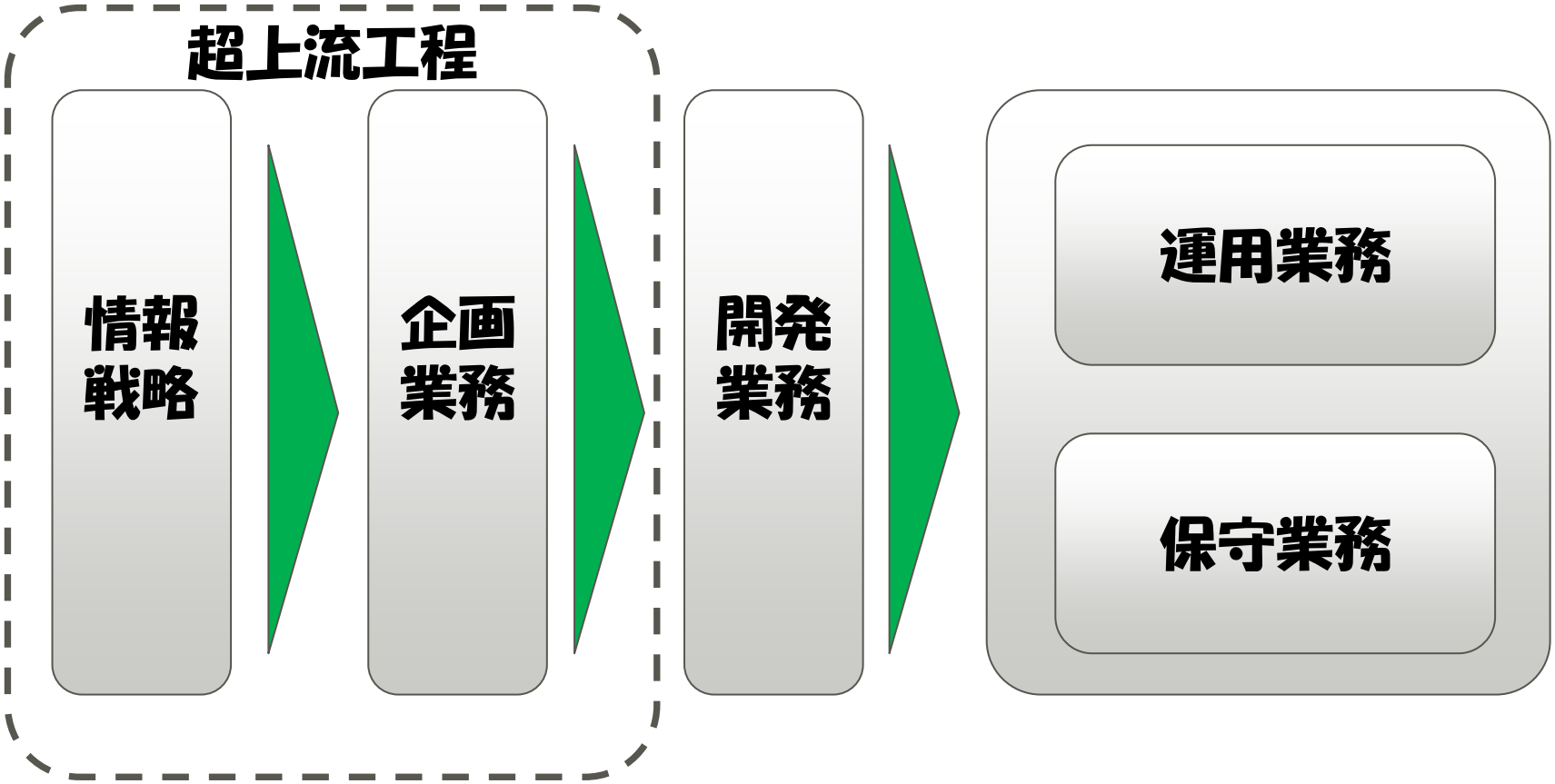
システム監査の勘所

■システム管理基準の構成

■ITストラテジストとシステム監査

■システム監査の勘所

システム管理基準の構成



共 通 業 務

ドキュメント管理　進捗管理　品質管理

人的資源管理　委託・受託管理　変更管理　災害対策

ITストラテジストとシステム監査

・システム監査への期待から考えると
「情報戦略」と「企画業務」の監査が重要。
・この分野を担う人材は「ITストラテジスト」である。

◆IPAが定義する対象者像
企業の経営戦略に基づいて、情報技術を活用して
基本戦略を策定・提案・推進する者

・ITストラテジストは、システム管理基準などを
自己の行動の「チェックリスト」として利用可能。

システム監査の勘所（情報戦略）

■情報戦略における監査のポイント

・組織体全体の情報システムのあるべき姿が明確になっているか？

・ITガバナンスの方針は明確か？

・全体最適化計画は利害関係者の合意を得ているか？

・情報セキュリティの基本方針は明確か？

・情報システム化委員会の権限と責任は明確か？

・情報システムに関連した事業継続計画の方針は明確になっているか？

システム監査の勘所(企画業務)

■企画業務における監査のポイント

- 開発計画は、ユーザ部門及び情報システム部門の役割分担を明確にしているか？
- 開発計画はシステムライフを設計する条件を明確にしているか？
- 情報システムの導入に伴って発生する可能性のあるリスク分析を実施しているか？
- パッケージソフトウェアの使用に当たっては、ユーザニーズとの整合性を検討しているか？
- システム開発に必要な要員のスキルは明確か？

最後に・・

ご清聴ありがとうございした。

これを機会に

「日本システム監査人協会」

入会をご検討ください。

よろしくお願いいたします。

⇒　http://www.saaj.or.jp/