国際情報

ＩＩＡが提供するＩＴ監査のガイダンス「ＧＴＡＧ」の紹介

日本ユニシス株式会社　ビジネス・イノベーション・オフィス　シニア・マネジャー
法政大学　兼任講師
内部監査人協会（ＩＩＡ）　Advanced Technology Committee Member
公認内部監査人（ＣＩＡ）　公認金融監査人（ＣＦＳＡ）
内部統制評価指導士（ＣＣＳＡ）　公認情報システム監査人（ＣＩＳＡ）
Internal Quality Assessor/Validator

吉　武　　一

はじめに

今般、内部監査人協会（The Institute of Internal Auditors，Inc.：以下ＩＩＡと表記）のAdvanced Technology Committee（先進的技術委員会：以下ＡＴＣと表記）の委員に就任いたしました吉武と申します。今後、ＩＩＡのＩＴ監査関係の活動を適宜ご紹介させていただきたく、今回は、ＩＩＡが進めるＩＴ監査推進活動の１つとしてのGlobal Technology Audit Guide（ＩＴ監査の国際的ガイダンス：以下ＧＴＡＧと表記）についてご紹介させていただきます。

ＧＴＡＧは現ＩＩＡの事務総長であるDavid A. Richards氏が前職の別組織の内部監査部門長（ＣＡＥ：Chief Audit Executive）であったときに、特に経営者向けに書かれたＩＴマネジメントとコントロールについてのガイドの必要性を感じたところから始まっています。そこでRichards氏は、ＩＩＡの事務総長に就任して最初の仕事の１つとして、このＧＴＡＧ作成のためのプロジェクトを立ち上げ（注１）、現在も同プロジェクトは進行しています。

以下にこのＧＴＡＧについて説明をさせていただきます。

〔１〕ＧＴＡＧとは

ＧＴＡＧとは、前述のRichards氏の思いを踏まえ、主として内部監査部門長、監査委員会、経営者層向けに提供される、ＩＴマネジメントとＩＴ監査についての国際的なガイドである。ＩＩＡはＩＴマネジメントとＩＴ監査に関する諸テーマにつき、ＧＴＡＧ１「ＩＴコントロール」から順次ガイドを公表していっており、今年５月現在で、ＧＴＡＧ７「ＩＴのアウトソーシング」までを公表している。ＧＴＡＧ１からの各ＧＴＡＧのテーマについては、図表１をご参照願いたい。

ＩＴガバナンスやＩＴ監査については、ＩＴガバナンス協会のＣＯＢＩＴや経済産業省

＜図表１＞ＧＴＡＧ一覧

ＧＴＡＧ１	ＩＴコントロール
ＧＴＡＧ２	組織の成功に不可欠な変更・パッチ管理のコントロール
ＧＴＡＧ３	継続的監査
ＧＴＡＧ４	ＩＴ監査のマネジメント
ＧＴＡＧ５	プライバシー・リスクのマネジメントと監査
ＧＴＡＧ６	ＩＴ脆弱性のマネジメントと監査
ＧＴＡＧ７	ＩＴアウトソーシング
ＧＴＡＧ８	ＩＴアプリケーション統制
ＧＴＡＧ９	認証とアクセスのマネジメント（予定）

のシステム監査基準、システム管理基準等いろいろな基準やガイドが多様な団体から公表されているが、これらと比較してＧＴＡＧの特色は次の３点にあるといえる。

⑴　内部監査部門長や経営者向けを意識して書かれたＩＴマネジメントとＩＴ監査のガイドであること

⑵　ＩＴマネジメントやＩＴ監査を体系的に網羅するというより、⑴との関係で、今、内部監査部門長や経営者のニーズや関心が高いテーマについて取り組み、ガイドを公表していること

⑶　このガイドが全世界で利用されることを意識して書かれている

ということである。

⑴について補足説明すると、ＧＴＡＧは確かに内部監査部門長や経営者向けのガイドであるが、その目的のために、説明が簡潔かつ明瞭であり、これからＩＴ監査を始めようとする方々にとっても良き解説書となると思われる。

⑵について述べると、最初のＧＴＡＧ１で、「ＩＴコントロール」について概説した後は、現在のＩＴマネジメントやＩＴ監査において関心の高い、財務報告に関する内部統制、個人情報保護法、情報セキュリティ、監査の品質等に関係する事項をテーマとして扱っている。今年は、「ＩＴアウトソーシング」（３月公表済み）、「ＩＴアプリケーション統制」（７月公表予定）、「認証とアクセスのマネジメント」（11月公表予定）を公表する計画となっており、来年度のテーマ（３つ）は今年７月のＡＴＣで協議される予定となっている（この原稿が発行される頃は、決定済みとなっているかもしれない）。

⑶について、ＧＴＡＧはできるだけ全世界で活用されるガイドとなることを意識して書かれているので、例えば個人情報保護では、アメリカだけでなくヨーロッパや日本等の基準や制度についてもふれられている。またレビューもいろいろな地域の方々によってなされており、草案から公表までの間に各地域の意見を適宜反映する仕組みとなっている。私自身もＧＴＡＧ５からレビューアーとして参加させていただいている。

〔２〕各ＧＴＡＧの具体的内容

以下に各ＧＴＡＧについて簡単に紹介していく。

１．ＧＴＡＧ１

ＧＴＡＧシリーズの１番目としてＧＴＡＧ１は、「ＩＴコントロール」についての解説を行っている。アウトラインは図表２のとおりであり、ＩＴコントロールの構成要素、種類と役割、ＩＴコントロールに関する取締役会、経営陣、監査人の役割と責任等について解説している。リスクの評価と対応から統制活動へと続き、継続的に評価していく通常の内部統制や内部監査のフレームワークが、ＩＴ統制やＩＴ監査においても有効であることをＧＴＡＧ１は読者に対して示している。

また、ビジネスプロセスは絶え間なく変化し、ＩＴも進化し続ける。それとともに新たな脆弱性が出現したり脅威も拡大することから、監査方法も継続的に改善していかねばならず、「ＩＴコントロールの評価は継続的な

＜図表２＞ＧＴＡＧ１：ＩＴコントロール

ＩＴコントロールとは	ＩＴコントロールは、情報及び情報サービスへアシュアランスをもたらし、テクノロジーの利用に伴うリスクの低減に寄与するプロセス
ＩＴコントロールの構成要素（２種類）	①業務における（ＩＴにより）自動化されたコントロール ②ＩＴ自身のコントロール
コントロールの種類	⑴　①全般統制 　　②業務処理統制 ⑵　①防止的コントロール 　　②発見的コントロール 　　③是正的コントロール ⑶　①ガバナンス・コントロール 　　②マネジメント・コントロール 　　③テクニカル（技術的）コントロール （実施するコントロールは、「トップダウン・アプローチ」により、ガバナンス・コントロールからテクニカルコントロールまでを順に検討していく）
ＩＴコントロールの役割	①コストのコントロール ②競争力の維持 ③情報資産の保護 ④法律・規制等の遵守
組織的役割と責任	①取締役会、理事会：　・ガバナンス・コントロール 　・内部統制に対する主たる責任、監督機能発揮 ②経営陣：　・マネジメント・コントロール 　・ＩＴコントロールの定義、承認、実行、理解 ③監査人：内部監査人：・経営陣へのアシュアランス 　外部監査人：・定期的監査
リスク評価と対応	①リスクの識別 ②リスクへの対応戦略を決定 （受容 or 回避 or 共有 or 移転 or 低減） ③リスクへの対応戦略にそい、ＩＴコントロールのベースライン（最低線）を決定
コントロールに対するモニタリング	①コントロール評価のための適切な監査メソドロジーの利用 ②継続的なモニタリング、特別なレビュー、自動化された継続的監査
コントロールの評価	ＩＴコントロールの評価は継続的なプロセス なぜなら、・ビジネス・プロセスは絶えず変化する ・ＩＴは進化し続ける ・新たな脆弱性の出現に伴い、脅威も拡大する ・監査方法も改善し続ける

学習プロセス」（注２）という文言は、ＩＴ監査のベストプラクティスである。

２．ＧＴＡＧ２

ＧＴＡＧシリーズ２番目のＧＴＡＧ２は「組織の成功に不可欠な変更・パッチ管理のコントロール」について取り扱っている。ＩＩＡがＧＴＡＧ２として「変更・パッチ管理のコントロール」をテーマに選んだ理由は、ビジネスプロセスのアウトソーシングやＥＲＰ（Enterprise Resource Planning）における失敗、変更・パッチ管理に関するＳＯＸ法404条等の法的対応の必要性等を踏まえ、「変更・パッチ管理のコントロール」について早急にガイドを公表すべきと考えたからである。

ＧＴＡＧ２のアウトラインは図表３のとおりであるが、ＩＴ変更管理のあるべき姿、変更管理の成熟度、良好な変更・パッチコントロールの利点、監査実施のポイントについて解説している。変更・パッチ管理プロセスの

＜図表３＞ＧＴＡＧ２：変更・パッチのコントロール

ＩＴ変更管理の「あるべき姿」とは？	①安定し管理されたＩＴ本番環境であるためには、変更が予測可能で反復可能な方法で実施される必要がある ②変更を行うＩＴ担当者は、定義され、監視され、確実に実施される統制の行き届いたプロセスを遵守する必要がある ③防止的コントロール（職責分離）と発見的コントロール（監督）を組み合わせて用いる必要がある
変更管理の成熟度	①反応型：50%超の時間が計画されていない作業に費やされる。無秩序環境、その場しのぎ ②自己管理システム：35～50%以上の時間が計画されていない作業に費やされる。多少の技法はあるが、アカウンタビリティに欠ける （①、②は、「変更が組織をコントロール」） ③閉ループプロセス：15～35%以上の時間が計画されていない作業に費やされる。変更が文書化され承認されている ④継続的改善：５%未満の時間が計画されていない作業に費やされる。管理され状況が測定可能で、変更のレビュー及び学習プロセスが機能 （③、④は、「組織が変更をコントロール」）
変更管理に対する監査の必要性	①ＩＴコントロールに関する法的要求事項の増大 ②変更がコントロールされない場合、組織全体に影響が及ぶ可能性 （機能障害の80%は変更が原因）
良好な変更・パッチ管理プロセスの利点	①計画されていないＩＴ作業へ費やす時間の減少 ②ＩＴ停止時間の減少 ③重要なパッチを最小の中断でインストール ④火を消すその場しのぎの対応からの開放により、ＩＴスタッフ資源の再配分が可能 ⑤より多くの時間を新規開発に投入可能
変更・パッチ管理プロセスの評価	ＣＯＳＯ　ＥＲＭモデルの活用が有効 「内部環境」、「目的の設定」、「事象の確認」、「リスクへの対応」 「リスクの評価」、「統制活動」、「情報と伝達」、「モニタリング」
組織的役割と責任	①取締役会：ガバナンス機能 ②経営陣：変更管理プロセスの定義、承認、実施、実行 ③監査人：内部監査人――経営陣へのアシュアランス提供 外部監査人――独立的評価

評価において「ＣＯＳＯ　ＥＲＭモデルの活用が有効」（注３）と説明されており、ここでも、通常の内部統制や内部監査のフレームワークが有効であることを明示している。

３．ＧＴＡＧ３

ＧＴＡＧ３は「継続的監査」についてのガイドである。組織は、財務的損失やエラー、不正、非効率性といったリスクに継続的にさらされており、コントロールが効果的・効率的に機能し、リスクが軽減されることに対する、適時かつ継続的なアシュアランスを行うことへの要求が高まっていることから、ＧＴＡＧ３のテーマは「継続的監査」となった。アウトラインは図表４のとおりである。

ＧＴＡＧ３では、「継続的監査」、「継続的モニタリング」、「継続的アシュアランス」という３つの概念を定義し、経営陣の責任として被監査部門自身による継続的モニタリングと内部監査部門の継続的監査の効果的な組み合わせによる継続的アシュアランスの重要性を強調する。ＳＯＸ法対応等により内部監査部員が不足がちな昨今、効果的かつ効率的な監査のあり方についての貴重な示唆があると私は考えている。加えてＧＴＡＧ３は、継続的にモニタリングを実施していくためのツー

＜図表４＞ＧＴＡＧ３：継続的監査

継続的監査の役割	①リスク・マネジメントとコントロール・システムについて、適時かつ継続的アシュアランスの必要性 ②コントロールの不備とリスクをよりよく管理するための、より一層頻繁で適時な分析の提供	
概念の明確化	①継続的監査	・コントロールとリスク・アセスメントを含む継続的に監査関連活動を実施する方法 ・内部監査部門にて実施
	②継続的モニタリング	・方針・規程等やプロセスの効果的な運用を確実にするプロセス、及びコントロールの十分性と有効性を評価するプロセス ・前者は業務や財務の経営陣により実施される ・後者のプロセスでは、内部監査部門において、経営陣の管理活動の十分性を独立して評価
	③継続的アシュアランス	・継続的監査と継続的モニタリングの組み合わせ ・コントロール手段の有効性、意思決定のための情報の適切性、信頼性を確保する方法
三者の関係	・経営陣の役割が大きくなれば、内部監査の直接的役割は小さくできる（コントロールの継続的モニタリングにおける経営陣の役割に依拠する内部監査部門による継続的監査） ・継続的アシュアランスは、「経営陣による内部統制の効果的なモニタリング」と「内部監査部門の独立的評価」の組み合わせが理想的	
継続的監査実施の適用部分	①コントロールの継続的な評価 ・コントロールの不備の識別、・不正、無駄、乱用の識別 ②継続的リスク・アセスメント ・プロセスの一貫性の検証、・全社的監査計画の整備 ・個々の監査のサポート、・監査勧告のフォローアップ	
継続的監査実施の主要ステップ	①監査の目的と要件の設定 ②役員レベルの支援の確保 ③どの経営者がどこまでモニタリング役割を果たすのかの確認 ④適切な技術的解決方法の選択 ⑤情報源の識別とアクセスの獲得 ⑥業務プロセスの理解及び主要コントロールと主要リスクの識別 ⑦監査スキルセットの確立 ⑧結果の管理と報告	
継続的監査実施の利点	①監査活動の範囲拡大 ②リスク低減能力の増大 ③内部統制評価コストの低減 ④財務報告の信頼性向上 ⑤財務業務の改善 ⑥財務的エラーや不正の潜在性減少 ⑦売上計上漏れ減少による決算の改善 ⑧コンプライアンスを支援する継続的かつコスト効果の良い方法	

ルとしてのＩＴの活用についても述べている。

効果的・効率的な監査遂行の観点から、業務処理プロセスの中からサンプルを抽出して検証するサンプル監査から、ＩＴの活用による業務処理の継続的モニタリング監査へと監査方法を移行していくことの重要性について主張しているものである。

なお、本稿では“Continuous Auditing”の訳語を、通常使用されている「継続的監査」を当てたが、堀江正之教授は著書『ＩＴ保証の

概念フレームワーク』の中で、“Continuous Auditing”を「本書では『引き続き行われる』という意味合いの『継続的』ではなく、『切れ目がない』という意味で『連続的』と訳している」（注４）といわれており、ＩＴ活用等による切れ目のないモニタリングの観点から、参考になるコメントであると私は考えている。

４．ＧＴＡＧ４

ＧＴＡＧ４は「ＩＴ監査のマネジメント」である。図表５のアウトラインが示すとおり、まずＩＴの監査対象とそれに係るＩＴ関連リスクを述べた後、ＩＴ監査の実施方法とＩＴ監査の管理について述べている。ＩＴ監査の対象は狭義のシステムだけではなく、４つの

＜図表５＞ＧＴＡＧ４：ＩＴ監査のマネジメント

ＩＴの定義（監査対象としてのＩＴ環境の範囲）	①第１層 ＩＴ管理	ＩＴ環境を管理する人、方針、手続、プロセスの集合
	②第２層 技術的インフラ	重要な業務アプリケーションの基礎となりサポートするシステム：ＯＳ、データベース、ネットワーク
	③第３層 アプリケーション	業務運用に関連した特定のタスクを行うプログラム
	④第４層 外部との接続	インターネット、ＥＤＩ、その他の外部ネットワーク
ＩＴ関連リスク	①リスクとは	・基準：可用性、セキュリティ、インテグリティ、機密性、有効性、効率性 ・タイプ：・広範囲のリスク（組織体全体へ影響するリスク）、・特定のリスク ・留意点：・各組織が特定のリスク・プロファイルを持つ ・ＩＴ関連リスクは静的ではなく、動的に変化 ・ＩＴ関連リスクに付随する特性にも留意
	②リスク評価	・影響度と発生可能性から考察 ・推奨事項 ・前年のアップデートだけでなく、毎年詳細に実施 ・ＩＴ環境のすべての層を考慮 ・リスクの静的・動的両面を考慮 ・インタビューにのみ頼るのでなく、その他の技法も使用 ・適切なレベルでの分析 ・適切な要員によって実施
ＩＴ監査範囲の定義	①ＩＴ監査の範囲が十分に広くなるＩＴ監査範囲の定義を使用 ②ＩＴ環境のすべての層を取り扱う ③希少なＩＴ監査の経営資源とＩＴ監査のニーズを効果的にバランスさせる。ＩＴ監査計画をどのように構築するかを理解	
ＩＴ監査の実施	①通常の監査プロセス 「環境の理解」⇒「キーコントロールの識別」⇒「設計の評価」⇒「有効性のテスト」⇒「発見事項の報告」 ②フレームワークや基準の活用 ・ＣＯＳＯ、ＣＯＢＩＴ、ＩＳＯ27001／17799	
ＩＴ監査の管理	①新たな管理手法、手続が必要 ②ＩＴ監査の資源（人的資源等）の管理 ③ＩＴ監査推進のためのツールの活用 ・監査支援ツール：電子帳票、監査プロジェクト管理ソフト等 ・テスト支援ツール：データ分析ツール、セキュリティ分析ツール	
新たな課題	・ワイヤレスネットワーク、・モバイル装置、・データ管理、・プライバシー、・職責分離、・管理者権限アクセス、・著作権侵害、等	

層があることを示していることは重要である。

４つの層とは、ＩＴを管理する人や、方針、手続、プロセスの集合である第１層、技術的インフラの第２層、アプリケーションの第３層、インターネットに代表される外部との接続の第４層である。また、ＧＴＡＧ４でもＩＴ監査の管理のセクションで、ＩＴ監査推進のためのＩＴツール活用の重要性を述べている。

なお、ＩＴツールの活用については、ＩＩＡの「専門職的実施のフレームワーク」の実践要綱1220－２（注５）においてコンピュータ支援監査技法（ＣＡＡＴＳ：Computer-Assisted Audit Techniques）を取り扱っており、ＧＴＡＧ４を読まれる際のご参考になると思う。更に、ＧＴＡＧ４では「ワイヤレスネット・ワーク」や「モバイル装置」等の新たな課題に対しても、どのように監査を実施していくかの問題提起を行っている。

５．ＧＴＡＧ５

ＧＴＡＧ５は「プライバシー・リスクのマネジメントと監査」である。日本でも2005年から個人情報保護法が全面施行され、関心の高い分野である。プライバシー保護についてどこまで行えば良いのかというのは、返答の難しい質問であるが、ＧＴＡＧ５はＯＥＣＤ（経済協力開発機構）の原則やＩＳＯ（国際標準化機構）等の基準の紹介に終わらず、ＣＯＳＯ　ＥＲＭを利用したプライバシー統制の構築について述べ、最終的にプライバシー成熟度モデルの提示によって解を提示している。

この成熟モデルは、成熟の段階を初期（場当たりの対応）⇒再現性あり（方針はあり）⇒定義されている（文書化と組織化）⇒管理されている（測定可）⇒最適化（絶え間ない継続的改善）の５段階で説明している。

これは、アメリカ・カーネギーメロン大学ソフトウエア工学研究所が組織（企業・チーム）のソフトウエア・プロセスの成熟度評価の基準として開発した成熟度モデル、ＣＭＭ（Capability Maturity Model）が活用範囲の広いモデルであり、このように個人情報管理状況の評価にも活用できることを示している。また、内部監査の役割については前述のＩＩＡの実践要綱2100－８（注６）から説明を行っている。アウトラインは図表６のとおりである。

６．ＧＴＡＧ６

ＧＴＡＧ６は、「ＩＴ脆弱性のマネジメントと監査」について取り扱っている。脆弱性マネジメントを、図表７が示すとおり、「ライフサイクル」、「監査範囲」、「組織の成熟度」という各ポイントと、「識別と検証」、「リスク・アセスメントと優先順位付け」、「対応」、「継続的な改善」の視点との組み合わせから説明している。また脆弱性管理の状況を具体的に測定するための主要なメトリックス（評価指標）も紹介しており、これらは経営陣や内部監査人が各々の組織の状態を評価する際にも利用できるものである。

システム障害や情報漏洩等が業務の効果的・効率的遂行の阻害要因になるだけでなく、組織の信用を著しく傷つけることとなる昨今、ＩＴ脆弱性の管理状態についての内部監査を実施する際は、ぜひＧＴＡＧ６を活用していただきたく思う。

７．ＧＴＡＧ７

ＧＴＡＧ７は「ＩＴアウトソーシング」について取り扱っている。アウトソーシングの活用がますます広がる一方で、アウトソーシングは情報セキュリティやＳＯＸ法等でも重要な管理対象となっている昨今、正に時機を得たテーマであるといえる。

ＧＴＡＧ７では、図表８のとおり、アウトソーシングに係るリスクとコントロールについて、戦略・設計⇒フィージビリティ・スタ

＜図表６＞ＧＴＡＧ５：プライバシー・リスクのマネジメントと監査

プライバシーとは何か？	①様々な側面	・身体的なプライバシー、精神的なプライバシー ・顧客としてのプライバシー、従業員としてのプライバシー、国民としてのプライバシー等
	②個人情報	・紙ベースの情報、電子的な情報 ・機微情報、匿名扱いの情報
	③管理のプレイヤー	・データ本人、データ管理者、プライバシーオフィサー
プライバシーの原則とフレームワーク	①ベンチマークとなる基準 ・原則：ＯＥＣＤ1980、ＥＵ1995、ＣｏＥ、ＵＮ等 ・法律・規則・規約 ・基準：世界的基準・国家的基準・産業的基準・個人的基準 ・監査基準	
プライバシーの影響度とリスクモデル	①リスク：個人的、組織的、財務上、風評上 ②個人に対する脅威：顕在化するコスト、監視、ＩＤの盗難、スパム、人権の制限 ③組織に対する脅威：訴訟、ネガティブ広告、財務的な損失、余分な支出、業務運営の妨害、市場の失敗	
ＣＯＳＯ　ＥＲＭモデルを利用したプライバシー統制	内部環境の例 統制活動の例	・プライバシーに関する組織の文化や意向が、顧客や社会的責任に密接にリンクしており…… ・リスクへの対応を確実にするような、組織の方針、手続、システムが……
プライバシー成熟度モデル	・初期 ⇩ ・再現性 ⇩ ・定義 ⇩ ・管理 ⇩ ・最適化	・場当たりの対応 ・プライバシー・ポリシーは定められており、再現性はあり ・プライバシー・ポリシーと組織は整備されており、リスク評価はされている ・プライバシー・ポリシー・マネジメントは、組織内で熟慮した結果、効果的な水準に保たれている ・プライバシー・ポリシー、手続の実施、統制は、プライバシー目標の達成のために継続的に改善されている
内部監査の役割	①ＩＩＡ実践要綱21000－８：プライバシー・フレームワークにおける内部監査の役割 ②内部監査にできること ・フレームワークの評価、重要なリスクの識別、適切な勧告	
プライバシー監査	①プライバシーを含む監査活動計画 ②監査業務の準備 ・個人データの処理プロセスへの理解、脅威の識別、コントロールと対策の識別、優先順位付け ③評価の実施 ・プライバシー・マネジメントの評価、テスト実行のメソドロジー ④伝達とモニタリングの結果 ⑤プライバシー・マネジメントと監査マネジメント	
ＣＡＥからの質問	・内部監査部門長（ＣＡＥ）がたずねるべきプライバシーに関する10の質問（10個の質問リストアップ）	

＜図７＞ＧＴＡＧ６：ＩＴ脆弱性のマネジメントと監査

脆弱性マネジメントのライフサイクル	①識別と検証	・システムの範囲決定、発見、検証
	②リスク・アセスメントと優先順位付け	・リスク・アセスメント、脆弱性の優先順位付け
	③対応	・脆弱性の低減、脆弱性低減プロセスの確立
	④継続的な改善	・脆弱性拡散防止、業務運営レベル合意書の確立、自動化、過去――未来
監査範囲	①識別と検証	・資産の目録、・脆弱性の検知、・発見事項の検証
	②リスク・アセスメントと優先順位付け	・リスク・アセスメント、・脆弱性の優先順位
	③対応	・モニタリング、インシデント管理、変更管理、パッチテスト
	④保守と改善	・構成管理、・オペレーション・レベルの合意 ・方針と要求事項
組織の成熟度		成熟した組織
	①識別と検証	・有効な資産管理 ・調査され、管理された重要な資産の認識 ・調査の検証とエラー結果の識別
	②リスク・アセスメントと優先順位付け	・日常的なＩＴリスク・アセスメント ・対応費用が見積もられている ・前回のパッチと変更メトリックスを活用して高リスクなパッチを見つける
	③対応	・システム設計が標準化されている ・組織としての取決めがある ・パッチテストを含めパッチ適用が自動化されている ・対応が追跡され、検証されている
	④継続的な改善	・安全な構造のために構成管理に経営資源を投入している ・調査する頻度と範囲を増やしている ・生産に先立って装置が分析されている ・標準的なＩＴ設定がある ・パッチ適用によりリスクが識別されている
主要なメトリックス	・総システム数に対する、モニター又は調査されたシステムの割合 ・異常な脆弱性の数 ・管理されているシステムの割合 ・検証されている脆弱性の割合 ・対応完了までの平均時間 ・オペレーション・レベルの合意件数 ・計画されていない業務に要した時間 ・セキュリティ・インシデントの数 ・セキュリティ・インシデントの影響度	
脆弱性管理	・資産評価、・脅威分析、・脆弱性分析、・リスク測定、・リスク判定 （リスク・マネジメントと類似した目標）	

＜図表８＞ＧＴＡＧ７：ＩＴアウトソーシング

ＩＴアウトソーシングの主要なタイプ	・アプリケーションの管理、・インフラの管理、・ヘルプデスク・サービス ・独立したテストと有効性評価、・データセンターの管理 ・システム統合、・Ｒ＆Ｄサービス、・セキュリティサービス	
アウトソーシングのライフサイクル	・戦略、設計⇒フィージビリティ・スタディ⇒契約⇒移行⇒ ⇒最適化、改善⇒終結／更新交渉	
ＩＴアウトソーシングのリスクの例	戦略・設計	・アウトソーシング戦略が企業の事業目的に整合していない
	フィージビリティ・スタディ	・サプライヤーに対する不十分なデュー・デリジェンスや、組織による関連リスク評価の不十分さに起因して、元本回収期限、顧客やサプライチェーンへの影響度合い、コスト削減等の見込みを誤る
	契約	・調達方針が不整合である、・適切なSLAが締結されない ・業務面、人的資源面、法規則による影響が勘案されていない ・コンティンジェンシープランが計画されていない
	移行	・公式の移行計画の欠如、・適切なスキルの保持計画不備 ・ＩＴ運用上の問題点が効果的に伝達されず、効果的な解決がなされない
	最適化・改善	・アウトソーシング契約条件が有効に管理されておらず、その結果、アウトソーシングの利点と効率性が発揮されていない
	終了又は更新交渉	・アウトソーシング・プロセスの不適切な終結
ＩＴアウトソーシングのキー・コントロールについての勘案点（委託元側の運用）	ガバナンスのフレームワーク	・すべてのＩＴアウトソーシング契約と組織の重要な事業目的との整合確保 ・モニタリング・メカニズムの整備、・複雑な事業ポートフォリオを縦断するＩＴプロジェクトとサービスの変化管理、等……
	戦略・設計	・戦略の有効性評価、・選択肢の識別、・ビジネスモデルの準備 ・分担・協力関係等の決定とチーム編成
	フィージビリティ・スタディ	・ビジネスモデルとケースの策定、・最低基準線の設定 ・市場の理解、・選択肢の評価とベンチマーキング
	契約	・取引内容の策定、・アウトソーシング資産に対する合意 ・契約書交渉、・契約の締結と実行
	移行	・変更の実施、・迅速な投資回収、・文化の確立、人の管理（変更管理）
	最適化・改善	・契約事項のモニタリングと紛争の解決、・ビジネスの変化 ・ビジネス関係の再評価、利便性を発揮するビジネスケースの実現
	アウトソーシング契約における重要な構成要素	・サービスレベルとインセンティブ、・ベンダーの従業員 ・データ、プライバシー、知的資産の保護、・価格保護 ・サードパーティへの割当、・提携先が利用・作成する資産の所有権 ・異なる複数の法律制度におけるコンフリクト ・コンティンジェンシープラント変更管理、重要な悪影響の通知 ・監査権限、・終了
ＩＴアウトソーシングのキー・コントロールについての勘案点（委託先側の運用）	・統制環境 ・セキュリティに関する勘案事項： ・データ保護リスク、セキュリティ（ネットワーク） ・セキュリティ（ネットワーク・物理的・環境的・人的・論理的アクセス） ・事業継続 ・ＳＤＬＣ（システム開発ライフサイクル）におけるコントロール ・変更管理のコントロール ・人事に関する方針と規程	
ＣＡＥからの質問	・内部監査部門長（ＣＡＥ）がたずねるべきＩＴアウトソーシングに関する10の質問（10個の質問リストアップ）	

ディ⇒契約⇒移行⇒最適化・改善⇒契約終了又は更新交渉という、アウトソーシング・ライフサイクルを追って説明している。また、アウトソーシングの契約書締結時や契約書監査時の参照となるよう、契約における重要な構成要素（チェックポイント）についてもリストアップを行っている。

以上、今年５月現在で公表されている各ＧＴＡＧについて紹介をしてきた。この７月には、ＧＴＡＧ８として「ＩＴアプリケーション統制」が公表されるが、これはＳＯＸ法対応を意識したものである。それでは、ＧＴＡＧではＩＴ全般統制は取り扱わないのかという質問が出てくるが、ＩＩＡではこれを“Guide to the Assessment of IT General Controls Scope Based on Risk”（以下ＧＡＩＴ）という別のプロジェクトで取り扱っている。

幸い、日本では公認内部監査人（ＣＩＡ）等による研究会であるＣＩＡフォーラムの１つである「ＣＩＡフォーラム研究会No.12（ＧＡＩＴフレームワークの動向と研究）」の方々がこのＧＡＩＴについての研究を進めておられ、今秋ＧＡＩＴについての講演会が予定されている。

〔３〕ＧＴＡＧの翻訳

ＧＴＡＧの日本での浸透を願いＧＴＡＧの和訳は、上記ＣＩＡフォーラムの別の研究会、「ＣＩＡフォーラム研究会No.21（以下フォーラム21と表記）」のメンバーを中心に進められている。本稿もフォーラム21による翻訳も参考にして、謝意を込めて、本稿の最後にフォーラム21のメンバーを記載させていただく。

現在、公表された各ＧＴＡＧのHighlights（ＧＴＡＧのプレゼンテーション用説明資料）は翻訳され日本内部監査協会のホームページからダウンロードできる状態となっている。更に翻訳チームは各ＧＴＡＧのエグゼキュティブ・サマリー（内部監査部門長のための要約）の翻訳にとりかかっており、今秋までには公表できる見込みである。

とはいえ、ＧＴＡＧは前述のように毎年３つずつ公表されていく予定であり、翻訳チームの強化が望まれる。ＧＴＡＧ翻訳に興味のあるＣＩＡ等の方は、ぜひご一報願いたい。

おわりに

ＧＴＡＧはＩＴ監査についての網羅的・体系的説明書ではありませんが、正に今ここにあるＩＴ統制やＩＴ監査の課題について簡潔・明瞭に取扱っている、実用性を重んじたガイドであるといえます。

より多くの方々がＧＴＡＧを読んで、議論してくださり、ＧＴＡＧを出発点として、わが国のＩＴ統制、ＩＴ監査のあり方を探求され、効果的・効率的なＩＴ監査を遂行されていかれることを望むものであります。

以上、ＧＴＡＧのご紹介をさせていただきました。今後もＡＴＣ委員としてＩＩＡのＩＴ監査関係の活動を適宜ご紹介させていただきますので、よろしくお願いいたします。

【ご参考】

＊ＧＴＡＧに関係する資料は、次のホームページからダウンロードが可能です。
ＧＴＡＧ原本（英文）：http://www.theiia. org/guidance/technology/gtag/
ＧＴＡＧ Highlights等の和訳：http://www. iiajapan.com/data/ITAUDIT_TOP.htm

＊ＧＴＡＧの翻訳参加に関する照会
http://www.iiajapan.com/system/forum/No21.htmまで。

＊なお、本書におけるＧＴＡＧに関する解釈等は筆者自身の見解であり、日本内部監査協会としての見解ではありません。

（注１）GTAG1“Information Technology Controls”GTAG-Letter from the President-1
（注２）GTAG1“Information Technology Controls”GTAG-Conclusion-11
（注３）GTAG2“Change and Patch Management Controls Critical for Organizational Success”GTAG - Why Should I Care About the Way My Organization Is Managing Change? - 3
（注４）堀江正之著『ＩＴ保証の概念フレームワーク―ＩＴリスクからのアプローチ―』（有）森山書店、2006年、「４・３　情報の信頼性保証とシステムの信頼性保証」
（注５）内部監査人協会「専門職的実施のフレームワーク」実践要綱1220－２：コンピュータ支援監査技法（ＣＡＡＴｓ）、日本内部監査協会発行
（注６）同上実践要綱2100－８：プライバシー・フレームワークの評価における内部監査人の役割

ＣＩＡフォーラム研究会No.21のメンバー（敬称略・順不同）

＜座長＞
吉武　　一　（日本ユニシス株式会社）
＜ＧＴＡＧ翻訳チーム＞
有川　　寛　（日本放送協会）
関谷　浩之　（オリックス株式会社）
谷口　和久　（三井住友海上メットライフ生命保険株式会社）
森　　康裕　（野村不動産ホールディングス株式会社）
森田　弥生　（新日本監査法人）
＜ＩＴ監査研究チーム＞
内田　満之　（エキスパートアライアンス株式会社）
海老名　将　（東京ガス株式会社）
金田　雅子　（株式会社三菱ＵＦＪフィナンシャル・グループ）
清水　　修　（日興コーディアル証券株式会社）
高瀬　浩幸　（日本電気株式会社）
竹下　芳喜　（日本バルカー工業株式会社）
茅野　耕治　（ＮＴＴデータ・セキュリティ株式会社）
辻　　英夫　（有限会社システムデザイング）
中村　賀昭　（カルソニックカンセイ株式会社）
延地　俊英　（株式会社三井住友銀行）
村田　　一　（オリックス株式会社）
矢島　博之　（キリンビールホールディングス株式会社）