CCSA, CFSA, CGAP 資格制度変更

# よくあるご質問

2018 年 8 月

The Institute of Internal Auditors | Global

# よくあるご質問（FAQ）

| | |
|---|---|
| 質問 1 | 公認公的部門監査人（CGAP）はどのように変更されるのでしょうか？ |
| 回答 | CGAP 資格は修了検定制度に再構成されます。但し、CGAP は今後も有効な資格であり、現在 CGAP 資格を保有されている方は、資格の継続的教育制度（CPE）に基づく諸要件を満たして、資格更新をされている限り、引き続き称号を使用することができます。さらに IIA では、2019 年中に「Active」の CGAP 資格保有者を対象に、CIA を取得していただくための「CIA チャレンジ試験」を提供する予定です。 |
| 質問 2 | 公認金融監査人（CFSA）はどのように変更されるのでしょうか？ |
| 回答 | CFSA 資格は修了検定制度に再構成されます。但し、CFSA は今後も有効な資格であり、現在 CGAP 資格を保有されている方は、資格の継続的教育制度（CPE）に基づく諸要件を満たして、資格更新をされている限り、引き続き称号を使用することができます。さらに IIA では、2019 年中に「Active」の CFSA 資格保有者を対象に、CIA を取得していただくための「CIA チャレンジ試験」を提供する予定です。 |
| 質問 3 | 内部統制評価指導士（CCSA）はどのように変更されるのでしょうか？ |
| 回答 | 現在の CCSA 資格試験は 2000 年はじめより開始されましたが、試験のトピックが 2013 年より開始された CRMA 試験の内容と一部重複しています。リスク・マネジメントの一環としてのインターナル・コントロールの観点から、CCSA 資格は公認リスク監査人（CRMA）の次回更新時より統合されることになります。但し、CCSA は今後も有効な資格であり、現在 CCSA 資格を保有されている方は、資格の継続的教育制度（CPE）に基づく諸要件を満たして、資格更新をされている限り、引き続き称号を使用することができます。さらに IIA では、2019 年中に「Active」の CCSA 資格保有者を対象に、CIA を取得していただくための「CIA チャレンジ試験」を提供する予定です。<br>※　CCSA 資格保有者が、CRMA の資格保有者となる趣旨ではございませんので、ご注意ください。<br>※　更新後の公認リスク監査人（CRMA）試験や認定要件の詳細につきましては、確定され次第、日本内部監査協会のウェブサイトにてお知らせ致します。 |
| 質問 4 | 引き続き CCSA、CFSA、または CGAP 試験に受験登録し、CCSA、CFSA、または CGAP 試験を受験することはできますか？ |
| 回答 | CCSA、CFSA、または CGAP 試験の日本での受験登録の最終期限は 2018 年 12 月 14 日（金）です。期日までに受験登録を完了された方には、2020 年 12 月 31 日まで各試験を受験することができます。 |
| 質問 5 | 現在保有している CCSA、CFSA、または CGAP 資格は今後も有効なのでしょうか？ |
| 回答 | はい、CCSA、CFSA、または CGAP は今後も有効な資格であり、現在 CCSA、CFSA、または CGAP 資格を保有されている方は、資格の継続的教育制度（CPE）に基づく諸要件を満たして、資格更新をされている限り、引き続き称号を使用することができます。もし、CPE の期限までに必要な要件が満たされなかった場合は、保有資格のステータスが自動的に「Inactive(grace period＝猶予期間)」となり、またこのステータスが 12 ヵ月以上継続した場合、ステータスは「Inactive（資格停止）」となります。「Inactive(grace period＝猶予期間)」または「Inactive（資格停止）」は復帰手続きを行わない限り、資格の称号を使用することはできません。 |

| | |
|---|---|
| 質問 6 | 現在保有している CCSA、CFSA、または CGAP 資格はどのようにすれば維持することができますか？ |
| 回答 | 資格の継続的教育制度（CPE）に基づく諸要件を満たして、資格更新をおこなってください。 |
| 質問 7 | もし資格のステータスが「Inactive(grace period＝猶予期間)」、「Inactive（資格停止）」または「Retired（定年等により退職し、現在仕事に従事していない状態）」の場合、「Active」に戻るための手続きはありますか？ |
| 回答 | はい、資格のステータスが「Inactive(grace period＝猶予期間)」の方は、前年と当年 2 年分の資格更新手続きを行ってください。「Inactive（資格停止）」の方は、復帰手数料の支払いを含む、復帰手続きを完了してください。詳細につきましては「継続的専門能力開発制度(CPE)ガイドライン」をご確認ください。 |
| 質問 8 | IIA は CCSA、CFSA、または CGAP 資格の CPE の要件を満たすための研修プログラムを引き続き提供されますか？ |
| 回答 | はい、IIA は今後も CPE の要件を支援するための各種のプログラムを提供してまいります。 |
| 質問 9 | 修了検定制度とは何ですか？ |
| 回答 | 修了検定制度は以下の要素により構成されます。<br>● カリキュラム<br>● IIA 国際本部または国別代表機関のカリキュラムに基づいて提供される研修コース<br>● 受講者の学習状況を確認するためのテスト<br>● テストに合格した方への修了証<br>IIA 国際本部では、現在、公的機関や金融機関の内部監査人を対象とした修了検定制度を開発中です。詳細につきましては 2019 年中にお知らせいたします。 |
| 質問 10 | 現在 CIA 資格に加えて、CCSA 資格（または、CFSA、CGAP）を保有しています。この場合はどうすればよいですか？ |
| 回答 | 保有資格のステータスを「Active」とするために、それぞれの資格更新手続きを継続してください。 |
| 質問 11 | 現在 CIA 資格は保有していませんが、CCSA 資格（または、CFSA、CGAP）を保有し、ステータスが「Active」です。この場合はどうすればよいですか？ |
| 回答 | 保有資格のステータスを「Active」とするために、それぞれの資格更新手続きを継続してください。また、あなたは「CIA チャレンジ試験」の受験要件を満たしています。受験要件をご確認ください。 |
| 質問 12 | 現在 CIA 資格は保有しておらず、CCSA 資格（または、CFSA、CGAP）を保有し、ステータスが「Inactive(grace period＝猶予期間)」です。この場合はどうすればよいですか？ |
| 回答 | CCSA、CFSA、または CGAP 資格のステータスが「Inactive(grace period＝猶予期間)」の方は、2018 年 12 月 10 日（月）までに、必要要件を満たして資格更新手続きを行い、資格のステータスを「Active」としてください。それにより「CIA チャレンジ試験」を受験いただくことができます。（2019 年 4 月 1 日受付開始） |

| | |
|---|---|
| 質問 13 | 現在 CIA は保有しておらず、CCSA 資格（または、CFSA、CGAP）を保有し、ステータスが「Inactive(資格停止)」（または「Retired（定年等により退職し、現在仕事に従事していない状態）」）です。この場合はどうすればよいですか？ |
| 回答 | CCSA、CFSA、または CGAP 資格のステータスが「Inactive(資格停止)」（または「Retired（定年等により退職し、現在仕事に従事していない状態）」）の方は、2018 年 12 月 10 日（月）までに、復帰手数料の支払いを含む、復帰手続きを完了してください。それにより「CIA チャレンジ試験」を受験いただくことができます。（2019 年 4 月 1 日受付開始） |
| 質問 14 | 現在 CIA 資格は保有しておらず、CCSA 資格（または、CFSA、CGAP）を受験中です。この場合はどうすればよいですか？ |
| 回答 | CCSA、CFSA、または CGAP 資格を受験中の方は、プログラムの有効期間中に受験を完了してください。また、2018 年 12 月 31 日までに試験に合格し、認定要件を満たされれば、「CIA チャレンジ試験」を受験いただくことができます。（2019 年 4 月 1 日受付開始） |
| 質問 15 | 現在 CIA 資格を保有しており、CCSA 資格（または、CFSA、CGAP）を受験中です。この場合はどうすればよいですか？ |
| 回答 | CCSA、CFSA、または CGAP 資格を受験中の方は、プログラムの有効期間中に受験を完了してください。その後、認定された場合は保有資格のステータスを「Active」とするために、それぞれの資格更新手続きを継続してください。 |
| 質問 16 | 2018 年 8 月 13 日に IIA より CCSA、CFSA、または CGAP 資格制度変更に関する正式な公表がなされた後も、引き続き CCSA、CFSA、または CGAP 試験に受験登録をすることはできますか？ |
| 回答 | CCSA、CFSA、または CGAP 試験の日本での受験登録の最終期限は 2018 年 12 月 14 日（金）です。期日までに受験登録を完了された方には、2020 年 12 月 31 日まで各試験を受験することができます。また、2018 年 12 月 31 日までに試験に合格し、認定要件を満たされれば、「CIA チャレンジ試験」を受験いただくことができます。（2019 年 4 月 1 日受付開始） |
| 質問 17 | 資格制度変更伴い、CCSA、CFSA、または CGAP 試験プログラムの延長手続きをおこなうことはできますか？ |
| 回答 | CCSA、CFSA、または CGAP 試験の験プログラムの延長手続きはお受付できません。 |
| 質問 18 | 「CIA チャレンジ試験」の受験要件とはどのようなものですか？いつまでに受験を完了しなければいけませんか？ |
| 回答 | 「CIA チャレンジ試験」は、CGAP、CFSA または CCSA 試験および CIA 試験のシラバスの相違点や、専門職的実施の国際フレームワーク（IPPF）に重点をおいて開発された特別な試験です。「CIA チャレンジ試験」に合格された方は、CIA 資格保有者となります。「CIA チャレンジ試験」は選択式の 150 問の試験で、受験時間は 3 時間です。試験シラバスについては別紙 A をご参照ください。 |
| 質問 19 | 「CIA チャレンジ試験」には何が含まれますか？費用は？ |
| 回答 | 日本内部監査協会では、2019 年 4 月 1 日の受付開始に向け、現在 IIA 国際本部と準備を進めております。詳細が決定し次第、日本内部監査協会ウェブサイトにてお知らせいたします。 |
| 質問 20 | 「CIA チャレンジ試験」の受験対象者は？ |
| 回答 | 「CIA チャレンジ試験」は、2018 年 12 月 31 日時点で CGAP、CFSA または CCSA 資格を保有（ステータスが「Active」な状態）している方が対象です。 |

| | |
|---|---|
| 質問 21 | 現在 CIA 試験を受験準備中ですが、CCSA 資格（または、CFSA、CGAP）は保有していません。「CIA チャレンジ試験」を受験できますか？ |
| 回答 | いいえ、できません。「CIA チャレンジ試験」は、CGAP、CFSA または CCSA 資格を保有（ステータスが「Active」な状態）している方が対象です。 |
| 質問 22 | もし現在 CIA 試験を受験中または、一部のパートに合格している場合、「CIA チャレンジ試験」を受験できますか？ |
| 回答 | 既に通常の CIA 試験に登録済みで、一部のパートに合格しておられる方でも「CIA チャレンジ試験」にお申込みは可能です。<br>● 一部のパートまたは全部のパートに合格していたとしても、これらに関する受験費用の返金は一切致しません。（本件への同意は必須要件です。）<br>● 「CIA チャレンジ試験」に合格されなかった場合、既に合格されているパートの結果はそのまま有効です。 |
| 質問 23 | いつから日本語による「CIA チャレンジ試験」を受験できますか？ |
| 回答 | 受験登録、受験申込、受験予約：　2019 年 4 月 1 日～2020 年 12 月 15 日<br>受験可能期間：　2020 年 1 月 1 日～2020 年 12 月 31 日 |
| 質問 24 | 「CIA チャレンジ試験」に合格しなかった場合、「CIA チャレンジ試験」の再受験はできますか？ |
| 回答 | 「CIA チャレンジ試験」に合格されなかった場合、90 日の経過期間を置いた後、再受験の申込が可能です。但し、受験可能な期間は 2020 年 12 月 31 日までです |

その他のご質問につきましては、日本内部監査協会　企画調査部　国際・資格課（cia-mailassisitance@iiajapan.com）までお問合せください。

## 別紙 A - CIA チャレンジ試験　シラバス

〔基本レベル〕の記述がない試験トピックについては〔熟達レベル〕で出題。

| I. 内部監査に不可欠な要素（30%） |
|---|
| **A. 内部監査の基礎** |
| 1. IIAの内部監査の使命,、内部監査の定義、内部監査の専門職的実施の基本原則監査および内部監査部門の目的、権限および責任を解釈する。 |
| 2. 内部監査基本規程」の要件（構成要素、取締役会による承認、規程の周知、等） について説明する。 〔基本レベル〕 |
| 3. 内部監査部門が提供するアシュアランス業務とコンサルティング業務の違いを理解する。 |
| 4. IIA の「倫理綱要」への適合を示す。 |
| **B. 独立性と客観性** |
| 1. 内部監査部門の組織上の独立性について理解する（独立性の重要性、職務上の報告等）。 〔基本レベル〕 |
| 2. 内部監査部門の独立性が損なわれていないかどうか識別する。 〔基本レベル〕 |
| 3. 個々の内部監査人の客観性が損なわれているかどうかを含めて、個々の内部監査人の客観性を評価し、維持する。 |
| 4. 客観性を促進する方針を分析する。 |
| **C. 熟達した専門的能力および専門職としての正当な注意** |
| 1. 内部監査部門の諸活動の責任を果たすために（開発するか、獲得するかして）必要な「知識、技能およびその他の能力」を理解する。 〔基本レベル〕 |
| 2. 技術的スキルやソフト・スキル（コミュニケーション・スキル、批判的思考、説得や交渉、コラボレーション・スキルなど）を含め、個人の職責を果たすために内部監査人が必要とする知識と能力を示す。 |
| 3. 専門職としての正当な注意を示す。 |
| **D. ガバナンス、リスク・マネジメントおよびコントロール** |
| 1. 組織体のガバナンスについての概念を説明する。 〔基本レベル〕 |
| 2. 組織体の文化がコントロール環境全体ならびに内部監査の個々の業務のリスクおよびコントロールに及ぼす影響を認識する。 〔基本レベル〕 |
| 3. 企業の社会的責任について説明する。 〔基本レベル〕 |
| 4. リスクとリスク・マネジメントの基本的な概念について理解する。 |
| 5. 様々なプロセスや部門・機能におけるリスク・マネジメントの有効性を検証する。 |
| 6. 組織体のリスク・マネジメント・プロセスにおける、内部監査部門の役割の適切性を認識する。 〔基本レベル〕 |
| 7. インターナル・コントロールの概念とコントロール手段の種類を理解する。 |
| 8. インターナル・コントロールの有効性と効率性を検証する。 |

| |
|---|
| **E. 不正リスク** |
| 1. 不正リスクおよび不正の種類を理解し、個々の内部監査業務を実施する際に不正リスクへの特別な配慮が必要かどうか判断する。 |
| 2. 不正発生の可能性を評価し（レッド・フラッグ等）、どのように組織体が不正リスクを発見し管理するかについて評価する。 |
| 3. 不正を防止し発見するためのコントロール手段や、組織体の不正に対する意識を向上させるための教育活動を推奨する。 |
| 4. フォレンジック監査（インタビュー、調査、テスト、その他）に関連する技法と内部監査の役割を理解する。 〔基本レベル〕 |
| **II. 内部監査の実務（40%）** |
| **A. 個々の業務に対する計画の策定** |
| 1. 個々の業務の目標、評価規準および個々の業務の範囲を決定する。 |
| 2. 主要なリスクおよびコントロールを確実に識別できるように個々の業務に対する計画を策定する。 |
| 3. 各監査領域について詳細なリスク評価を行う。その際に、リスクおよびコントロールの諸要素についての評価および優先順位付けを含める。 |
| 4. 個々の業務の手続を決定し、個々の業務の作業プログラムを作成する。 |
| 5. 個々の業務に必要な要員および監査資源のレベルを決定する。 |
| **B. 情報の収集** |
| 1. 個々の業務の領域に関する事前調査の一環として、関連する情報を収集し検討する。（前回監査の報告およびデータをレビューする、ウォークスルーおよびインタビューを実施する、観察を行う、その他） |
| 2. 個々の業務の領域に関する事前調査の一環として、チェックリストおよびリスクとコントロールの質問票を作成する。 |
| 3. 適切なサンプリング（非統計的サンプリング、判断サンプリング、発見サンプリング、その他）および統計的分析の技法を適用する。 |
| **C. 分析および評価** |
| 1. 電子化された監査ツールおよび技法（データマイニングおよびデータ抽出、継続的モニタリング、自動監査調書、埋込型監査モジュール、その他）を使用する。 |
| 2. 潜在的な監査証拠ソースの、関連性、十分性および信頼性を評価する。 |
| 3. 適切な分析的手法およびプロセス・マッピング技法（プロセス識別、ワークフロー分析、プロセスマップの作成および分析、スパゲティ・マップ、ＲＡＣＩ図、その他　を適用する。 |
| 4. 分析的レビュー技法（比率推定、差異分析、予算対実績、傾向分析、他の合理性テスト、ベンチマーキング、その他）を決定して適用する。 〔基本レベル〕 |
| 5. 結論および個々の業務の結果を裏付けるために、関連する情報の監査調書および文書を作成する。 |
| 6. 個々の業務の結論を要約してまとめる。そこには、リスクおよびコントロールの評価を含める。 |
| **D. 個々の業務の監督** |
| 1. 個々の業務の監督における主要な活動（業務分担を調整する、監査調書をレビューする、監査人の業績を評価する、その他）を識別する。 〔基本レベル〕 |

| |
|---|
| **E. 個々の業務の結果の伝達およびリスク受容** |
| 1. 個々の業務の対象部署（またはコンサルティング業務における依頼者）との事前の伝達を調整する。 |
| 2. 伝達の品質（正確な、客観的な、明確な、簡潔な、建設的な、完全な、および適時なならびに要素（目標、範囲、結論、改善のための提言、および改善措置の計画）を示す。 |
| 3. 個々の業務の進捗状況について中間報告を行う。 |
| 4. 組織体の価値を向上させ保全するために改善のための提言を作成する。 |
| 5. 監査終了会議の実施、監査報告書の作成（原稿作成、レビュー、承認、配付）および経営管理者からの回答の入手を含めた、個々の業務の伝達と報告のプロセスを説明する。 〔基本レベル〕 |
| 6. 残存リスクの評価に関する内部監査部門長の責任を説明する。 〔基本レベル〕 |
| 7. 組織体にとって受容できないのではないかとされる水準のリスクを経営管理者が受容している場合には）リスク受容を伝達するプロセスを説明する。） 〔基本レベル〕 |
| **F. 進捗状況のモニタリング** |
| 1. 経営管理者による改善措置計画を含めた、個々の業務の成果物を評価する。 |
| **III. 内部監査のためのビジネス知識（30%）** |
| **A. データ分析** |
| 1. データ分析、データの種類、データのガバナンス、および内部監査においてデータ分析を用いることの価値を説明する。 〔基本レベル〕 |
| 2. データ分析のプロセス（質問を明確にする、関連するデータを取得する、データのクリーニングや正規化をする、データを分析する、結果を伝達する）を説明する。 〔基本レベル〕 |
| 3. データ分析手法（異常値検知、診断解析、予測解析、ネットワーク解析、テキスト解析、その他）の内部監査への適用について理解する。 〔基本レベル〕 |
| **B. 情報セキュリティ** |
| 1. 一般的な物理的セキュリティ・コントロールの種類（カード、鍵、生体認証、その他の違いを理解する。〔基本レベル〕 |
| 2. 様々な形式のユーザ認証および承認コントロール手段（パスワード、２段階認証、生体認証、デジタル署名、その他）の違いを理解し、潜在的なリスクを識別する。 〔基本レベル〕 |
| 3. 様々な情報セキュリティ・コントロール手段（暗号化、ファイアウォール、アンチウイルス、その他）の目的および使用方法を説明する。 〔基本レベル〕 |
| 4. データ保護法令、ならびにデータ保護法令がデータ・セキュリティ方針および実務へ及ぼす潜在的な影響を理解する。 〔基本レベル〕 |
| 5. 最新のテクノロジーの実態およびセキュリティへの影響（ＢＹＯＤ（私的デバイスの活用）、スマート・デバイス、ＩＯＴ（モノのインターネット、その他））を理解する。 〔基本レベル〕 |
| 6. 既存および最新のサイバー・セキュリティのリスク（ハッキング、海賊行為、改竄身代金ウイルス攻撃、フィッシング攻撃、その他）を理解する。 〔基本レベル〕 |
| 7. サイバー・セキュリティおよび情報セキュリティ関連の方針を説明する。 〔基本レベル〕 |
| **C. アプリケーションおよびシステム・ソフトウェア** |
| 1. システム開発ライフサイクルと納入における中核的な活動（要件定義、設計、開発検証、デバッギング、配備、維持、その他）、ならびにプロセス全体を通じた変更管理の重要性を理解する。 〔基本レベル〕 |

2. 基本的なデータベース用語（データ、データベース、レコード、オブジェクト、フィールド、スキーマ、その他）およびインターネット用語（HTML、HTTP、URL、ドメイン名、ブラウザ、クリックスルー、電子データ交換（ＥＤＩ）、クッキー、その他）を説明する。〔基本レベル〕

**III. 内部監査のためのビジネス知識（30%）**

**A. データ分析**

1. データ分析、データの種類、データのガバナンス、および内部監査においてデータ分析を用いることの価値を説明する。〔基本レベル〕
2. データ分析のプロセス（質問を明確にする、関連するデータを取得する、データのクリーニングや正規化をする、データを分析する、結果を伝達する）を説明する。〔基本レベル〕
3. データ分析手法（異常値検知、診断解析、予測解析、ネットワーク解析、テキスト解析、その他）の内部監査への適用について理解する。〔基本レベル〕

**B. 情報セキュリティ**

1. 一般的な物理的セキュリティ・コントロールの種類（カード、鍵、生体認証、その他の違いを理解する。〔基本レベル〕
2. 様々な形式のユーザ認証および承認コントロール手段（パスワード、２段階認証、生体認証、デジタル署名、その他）の違いを理解し、潜在的なリスクを識別する。〔基本レベル〕
3. 様々な情報セキュリティ・コントロール手段（暗号化、ファイアウォール、アンチウイルス、その他）の目的および使用方法を説明する。〔基本レベル〕
4. データ保護法令、ならびにデータ保護法令がデータ・セキュリティ方針および実務へ及ぼす潜在的な影響を理解する。〔基本レベル〕
5. 最新のテクノロジーの実態およびセキュリティへの影響（ＢＹＯＤ（私的デバイスの活用）、スマート・デバイス、ＩＯＴ（モノのインターネット、その他））を理解する。〔基本レベル〕
6. 既存および最新のサイバー・セキュリティのリスク（ハッキング、海賊行為、改竄身代金ウイルス攻撃、フィッシング攻撃、その他）を理解する。〔基本レベル〕
7. サイバー・セキュリティおよび情報セキュリティ関連の方針を説明する。〔基本レベル〕

**C. アプリケーションおよびシステム・ソフトウェア**

1. システム開発ライフサイクルと納入における中核的な活動（要件定義、設計、開発検証、デバッギング、配備、維持、その他）、ならびにプロセス全体を通じた変更管理の重要性を理解する。〔基本レベル〕
2. 基本的なデータベース用語（データ、データベース、レコード、オブジェクト、フィールド、スキーマ、その他）およびインターネット用語（HTML、HTTP、URL、ドメイン名、ブラウザ、クリックスルー、電子データ交換（ＥＤＩ）、クッキー、その他）を説明する。〔基本レベル〕
3. ソフトウェア・システム（顧客関係管理（CRM）システム、エンタープライズ・　リソース・プランニング(ERP) システム、ガバナンス・リスク・コンプライアンスGRC）システム、その他）の主要な特徴を識別する。〔基本レベル〕

**D. IT インフラストラクチャーおよび IT コントロール・フレームワーク**

1. 基本的なＩＴインフラおよびネットワーク（サーバ、メインフレーム、クライア ント・サーバ・コンフィギュレーション、ゲートウェイ、ルータ、LAN、WAN、VPN、その他）の概念を説明し、潜在的なリスクを識別する。〔基本レベル〕
2. ネットワーク管理者、データベース管理者およびヘルプ・デスクの運営上の役割を理解する。〔基本レベ

| |
|---|
| ル〕 |
| 3. ＩＴコントロール・フレームワーク（COBIT、ISO27000、ITIL、その他）および基本的な IT コントロールの目的と利用方法を理解する。 〔基本レベル〕 |
| **E. 財務会計および財務** |
| 1. 財務会計の概念および基本原則（財務諸表の種類、および債券、リース、年金、無形資産、研究開発等の用語）を識別する。 〔基本レベル〕 |
| 2. 高度な最新の財務会計の概念（連結、投資、公正価値、パートナーシップ、外貨取引その他）を理解する。 〔基本レベル〕 |
| 3. 財務分析（水平分析および垂直分析、ならびに活動、収益性、流動性、レバレッジその他に関する諸比率）を理解する。 |
| 4. 収益サイクル、流動資産の管理活動と会計、サプライ・チェーン・マネジメント（在庫評価、買掛金勘定を含む）を説明する。 〔基本レベル〕 |