甲南経営研究　第40巻第3・4号（2000.3）

ECASとシステム保証サービス

池　田　公　司

I　はじめに

エリオット委員会報告書（Special Committee on Assurance Services [1997]）を契機として，情報システムの信頼性保証が重要なテーマとなっている。これは，外部監査としてシステム自体の監査を行うというアプローチであり，システム監査の新しい方向性を示唆している（池田 [1999]; Murthy et al.[1999]）。現在の動向として，このシステムの保証は，いわゆる電子商取引保証業務（Electronic Commerce Assurance Service; ECAS）の一環として議論されることが多い。そこで，本稿では Nagel et al.[1999] を手掛かりとして，ECASのコンテクストにおけるシステム保証サービスの特質を検討することにしたい。

II　ECASの背景

先ず最初に，Nagel et al.[1999] に依拠して，ECASの性格や監査プロフェッションとの関わりについて概観しておきたい（Nagel et al.[1999], pp. 3-69）。

(1)　市場としての成長性

WWW（World Wide Web）を通じて取り引きされる財やサービスは，2000年までに1兆ドルまで成長することが見込まれている。しかしながら，

他方では，ウェブ上で電子商取引を行う当事者や，潜在的にそれに関わる当事者は，取引を行う相手方に懸念を抱いている。例えば，売り手側は，ハッカーがシステムに不正にアクセスすることや，顧客が他の顧客の機密情報にアクセスすることを懸念している。また，買い手側は，インターネット上にクレジットカードの番号を流すこと等を懸念している。AICPA の統計調査によると，オンラインショッピング利用者の85％が，クレジットカードの利用に躊躇している。こうした懸念は様々な言葉で表現されているが，総て信頼性（trust）の問題に帰着する。

CPA は，資本市場の財務諸表に関して，信頼しうる第三者たる仲介者（trusted third-party intermediaries）として長い歴史を有している。CPA は電子商取引（Electronic Commerce; EC）の市場においても同様な役割を果たしうるであろう。

⑵ コンサルティングサービスの機会

CPA や監査法人のコンサルティング部門にとって，EC には大きな機会がある。コンピュータのハードウェアおよびソフトウェアの選定と導入，EC システムと既存システムとのインターフェース，内部統制の設計と導入，および EC 活動の監視や管理等につき，クライアントは支援を必要としている。

⑶ 電子商取引の保証業務

ECAS への関心の高まりは，保証業務特別委員会（エリオット委員会）が

図1　ウェブトラスシール

動機付けとなっている（Special Committee on Assurance Services [1997]; Elliott [1992], [1994a], [1994b], [1995] and [1997]）。エリオット委員会は，ECAS 市場が毎年10億ドル成長すると見込んでいる。AICPA は，1997年に Everett Johnson を主査として電子商取引のタスクフォース（Electronic Commerce Taskforce）を編成し，アテステーション基準の下でのウェブトラスト（WebTrust under the Attestation Standards）を開発した（「図1」を参照）。

(4) 競　争

しかしながら，ECAS 市場の成長性に着目しているのは CPA のみでない。以下に例示するような潜在的競争者が存在している。AICPA は ECAS 市場の需要に素早く対応することが必要である。AMEX 等のクレジットカード会社は，本質的に，EC の信頼性確保と密接な関係を有しているといえよう。

① 組織体

- AICPA
- 州の会計士協会
- 内部監査人協会（IIA）

② データベースプロバイダ

- Dun & Bradstreet
- Standard & Poor
- Chaners, Thomas Directories
- BBB On-Line

③ テクニカルリソース

- VeriSign
- Visa/MasterCard
- American Express
- Cybercash, Digicash

ECAS とシステム保証サービス（池田公司）

④ プロフェッショナルファーム

- 地方および地域ごとの会計事務所
- Big 5 会計事務所
- IT コンサルティング会社（EDS 等）
- American Express, Triple Check

⑸ 古いリスクと新しいリスク

CPA は ECAS 市場に関連するリスクのレベルとタイプを知らなければならない。高度に統合されたペーパーレスの EC システムは，監査証跡や職務の分掌といった伝統的な内部統制を著しく後退させる。

⑹ 開かれた機会

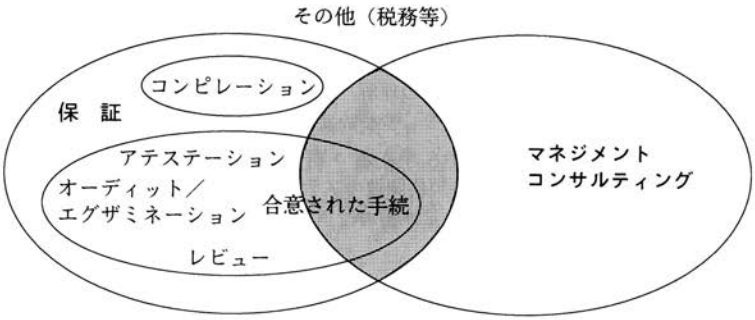
エリオット委員会の最終報告書には，会計士が提供しうる様々な ECAS 活動が含まれている。それを受けて AICPA は，企業対顧客（business-to-consumer）のウェブトラストをアテステーション基準に基づいて開発したが，企業対企業（business-to-business）ヴァージョンのウェブトラストも開発しつつある。前者は専らインターネットショッピングの信頼性保証に終始するが，後者はより拡張された意義を有することになるであろう。

しかしながら，CPA は AICPA が特定なプロダクトを開発するまで手を拱いて待つべきではない。CPA が行いうる ECAS には多くの形態が存在するからである。小規模および大規模の会計事務所にとって，豊富な機会が存在している。

III ECAS に適用される職業基準

「図２」は，エリオット委員会の最終報告書に基づいて，保証業務や種々の活動の関係を示したものである。「図２」に示された個々の活動には，下に掲げたように，それぞれ対応した職業基準があり，特定なクライアントに対して一つまたは複数を組み合わせて適用する。

図2　CPAサービスの領域



（出所）Nagel et al.[1999], p. 121.

① アテステーション契約基準書（Statement on Standards for Attestation Engagements; SSAE）

② コンサルティング業務基準書（Statement on Standards for Consulting Services; SSCS）

③ 会計およびレビュー業務基準書（Statement on Standards for Accounting and Review Services; SSARS）

④ 監査基準書（Statements on Auditing Standards; SAS）

「図2」に示されるように，CPAの提供するサービスはオーバーラップしている。従って，個々のECASサービスは異なったタスクを伴うことがあり，異なった基準を適用しなければならないこともある。個々のタスクにどの基準を適用すべきかは，監査人の責任において判断される問題である。例えば，アテステーション契約の総ての特徴を有する契約を，名称としてアテステーション契約と呼ばない場合であっても，アテステーション基準に準拠すべき要件が否定されることにはならない。

AICPAは，明示的に，ウェブトラスト契約はAT100（アテステーション基準）に準拠しなければならない（must comply with AT100）としている。加えて，「図2」では示されていないが，品質管理（quality control）等に関

表１　アテステーション契約基準書の構成

セクションおよびタイトル		ソース	発行年月
AT100	アテステーション基準	SSAE-1	1986年３月
	AT100.32 クライアントの理解	SSAE-7	1997年10月
	AT100.78 アテステーション契約基準 －第1号の改正－	SSAE-5	1995年11月
	AT100.83-.85 MAS契約関連のアテスト業務	SSAE-1	1987年12月
	アテステーション契約基準書の改正	SSAE-9	1999年１月
AT9100	アテステーション基準 －セクション100の解釈指針－		
AT200	予測財務情報およびプロジェクション	SSAE-1	1985年10月
AT300	見積財務情報に対する報告	SSAE-1	1988年９月
AT400	財務報告に関するエンティティの内部統制に対する報告	SSAE-2	1993年５月
	アテステーション契約基準書の改正	SSAE-9	1999年１月
AT500	準拠性のアテステーション	SSAE-3	1993年12月
	アテステーション契約基準書の改正	SSAE-9	1999年１月
AT600	合意された契約	SSAE-4	1995年９月
AT700	経営者の討議と分析	SSAE-8	1998年３月

（出所）Nagel et al.[1999], p. 127.

する他の職業基準も必然的に適用されることになるであろう。それ以外の基準は，個々の ECAS サービスの特徴に依存して適用されるであろう。また，SAS の基準の多くは有用な指針を与えるであろう。

「表１」はアテステーション基準の内容構成を示したものであるが，とりわけ AT100 に含まれる基準が重要である。AT100 は ECAS のコーナーストーンをなしている。

アテスト業務（attest service）は，伝統的に，一般に認められた監査基準（GAAS）に準拠した歴史的財務諸表の監査業務に限定されてきた。しかしながら，監査人がクライアントに提供するアテスト業務を拡張した結果，既存の GAAS を適用することはより困難となり，とりわけ財務諸表指向の業務から ECAS 等の新しい業務が引き離されている。こうしたことから，アテス

テーション基準のイントロダクションでは次のように述べられている。

「これらのアテステーション基準および関連する解釈指針を適用する主たる目的は，アテスト機能の一般的なフレームワークを提供し，かつ合理的な基礎を設定することにある。そうしたものとして，基準と解釈指針は，(a)新たに発展しつつあるアテスト業務を実施する公認会計士に有用かつ必要な指針を提供し，また(b)必要に応じて，AICPA の基準設定主体がそうした業務を扱う際の解釈基準を示すものである。」

アテステーション基準は，一般に認められた監査基準が自然に拡張したものである。監査基準と同様，アテステーション基準も技術的能力，精神的独立性，正当な注意義務，適切な計画および監督，十分な証拠，および適切な報告の必要性を取り扱っているが，その範囲はより広範である（11個のアテステーション基準は「表２」を参照)。アテステーション基準は，拡張しつつあるアテスト業務に適用されるものであり，例えば，内部会計統制システムに関する記述，コンピュータソフトウェアに関する記述，制定法・規制・契約条件への準拠性，投資効率の統計数値，財務諸表の補足情報等に対する報告を含む。このように，このアテステーション基準は，変化する環境や社会の要求に対処するために開発されてきた。

「表２」のアテステーション基準は，GAAS 基準と比較した場合に，次のような特質が認められる。

① アテステーション基準と GAAS の間には二つの概念的な差異がある。第一に，アテステーション基準は歴史的財務諸表を超えたアテスト機能の枠組みを与えている。従ってアテステーション基準では，「財務諸表」や「一般に認められた会計原則」へは言及しない。第二に，実施基準および報告基準において明らかなように，アテステーション基準は増加しつつあるアテスト業務を収容しており，そこでは伝統的監査で表明されるレベル（積極的意見）以下の保証水準が認められている。

表2　アテステーション基準

一般基準

一　契約は，適切なテクニカルトレーニングを受け，アテスト機能の能力を有する単一もしくは複数の監査人によって実施されなければならない。

二　契約は，アサーションの内容につき適切な知識を有する単一もしくは複数の監査人によって実施されなければならない。

三　監査人は，次の各号に示す条件が存在すると認められる場合に限り，契約を実施しなければならない。

・　アサーションは，認められた機関の設定した基準に照らして評価できるか，または当該アサーションの表示において，知識のある読者には明確かつ分かり易く記載された基準に照らして評価することができる。

・　アサーションは，そうした基準を用いた見積値または測定値と合理的に一致する。

四　契約に関連する総ての事項において，単一もしくは複数の監査人は，精神的独立性を維持しなければならない。

五　契約の実施に際しては，正当な注意を払わなければならない。

実施基準

一　業務は適切に計画し，かつ必要に応じて補助者を監督しなければならない。

二　十分な証拠を入手し，報告書で表明される結論の合理的基礎としなければならない。

報告基準

一　報告書では，報告が行われるアサーションを識別し，契約の性格について述べなければならない。

二　報告書では，当該アサーションが制度的に確立された基準，または表明された基準に準拠して表示されているかにつき，監査人の結論を述べなければならない。

三　報告書では，契約またはアサーションの表示につき，監査人による重要留意事項の総てを述べなければならない。

四　合意された規準に準拠して作成されたアサーションを評価する契約，または合意された手続きを適用する契約に関する報告書では，そうした規準や手続きを合意した当事者に対して，利用を制限する文言を含めなければならない。

（出所）Nagel et al.[1999], p. 129.

②　これらの二つの主要な差異に加えて，もう一つの概念的な差異がある。すなわち，アテステーション基準においては，ユーザニーズに基づいてカスタマイズされたアテスト業務に対してもフォーマルに適用される。

この場合，ユーザーはアテスト契約の性格と範囲，またはアサーションを評価するための特殊な規準の確定に関与し，報告書の利用が制限されることを認めることになる。これらは実質的な差異であるが，すでに市場や公共会計実務で起こっている変化を認識したに過ぎない。

③　これらの三つの概念的な差異によって，アテステーション基準の構成はGAASのそれと異なっている。構成上の違いは，(a)GAASには含まれない二つの一般基準がアテステーション基準に含まれること，および(b)GAAS実施基準の一つと報告基準の二つがアテステーション基準には明示的に含まれないことである。

④　二つの一般原則（第二原則および第三原則）が含まれるのは，アテスト契約を定義し，アテスト機能の境界を画定するためである。一度アテステーションの内容が歴史的財務諸表を超えると，その範囲の拡張をどこまで認めるかを決定する必要がある。アテステーション基準では，(a)監査人がアサーションの内容につき適切な知識を有すること―第二原則―，および(b)当該アサーションが，確立または表明された規準を用いた見積値・測定値と合理的に一致すること―第三原則―が要求される。

⑤　GAAS実施基準の第二は，いくつかの理由によりアテステーション基準には含まれない。その第二基準は「信頼性を置くための基礎として，また監査手続を制限するテスト範囲を決定するために既存の内部統制を調査し評価すること」を要求している。この基準を含まない最も重要な理由は，アテステーションの第二実施基準は，内部統制の調査と評価を包摂しているからである（内部統制の調査と評価は十分な証拠を収集する際の一要素である）。もう一つの理由は，内部統制の概念が，ある種のアサーション（例えば，コンピュータソフトウェアに関する情報等）にはレリバントではないからである。

⑥　アテステーションの報告基準は，GAASのそれとは異なった形で構成

されている。これは，単一なレベルおよび形態の保証を超えて，様々なアサーションの表示に関するアテスト機能を拡張した自然な結果である。また，アテステーション基準には，新しい報告テーマも含まれる。すなわち，利用者に対してある種の報告書の利用を制限するものであるが，これは，アテスト機能をユーザニーズに応じてカスタマイズしたことの自然な結果である。

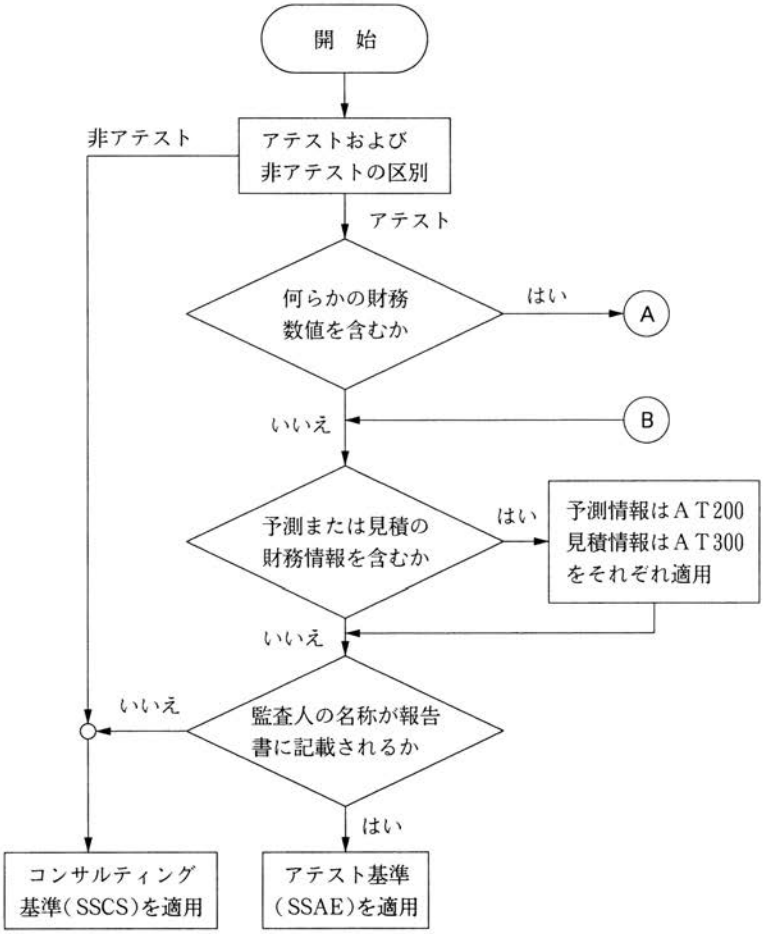
⑦ 加えて，GAAS における二つの報告基準が，アテステーション基準からは削除されている。一つは，監査報告書で「会計原則が前期に引き続き当期も継続して適用されているか」を述べなければならない基準である。今一つは，「財務諸表のインフォメーティヴな開示は，報告書で特に述べない限り，合理的に適切なものとみなされなければならない」という基準である。これら二つの基準がアテステーション基準に含まれないのは，アテステーションの第二報告基準にそれらが包摂されているからである。アテステーションの第二報告基準は，アサーションが確立または表明された規準に準拠して表示されているかにつき，結論を要求している。

IV　ECAS における職業基準の選択プロセス

「図 3」および「図 4」は，ECAS 契約における職業基準の選択プロセスをフローチャートの形式で示したものである。これらのフローチャートは単純化されているので，ここには含まれていない基準も ECAS に適用される場合がありうる。

「図 3」のフローチャートは，ある契約がアテストか非アテストかを識別することから出発している。ECAS 契約では，非アテストのタスクはコンサルティング基準（SSCS）の適用を受ける。これに対して，アテストのタスクは，アテステーション基準（SSAE），コンピレーションおよびレビュー基準

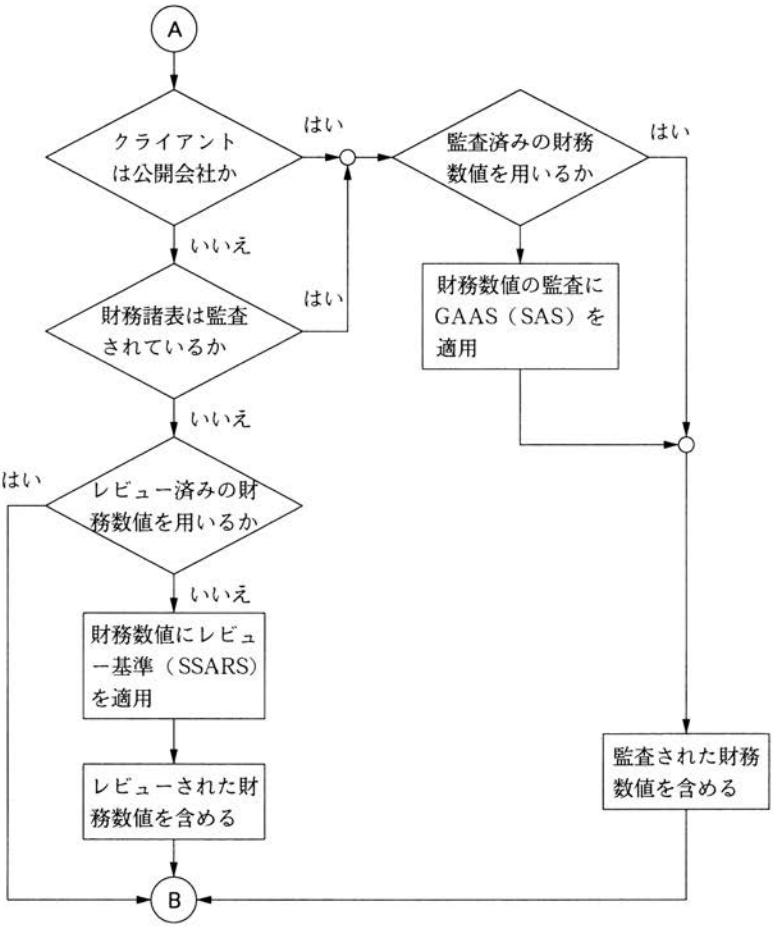
図3　ECAS契約における適切な職業基準の選択プロセス（その1）



（出所）Nagel et al.[1999], p. 187。

(SSARS)，および／または監査基準 (SAS) の適用を受ける。本質的には，「図4」に示されるように，クライアントが公開会社（または監査を受けている閉鎖会社）である場合には，GAAS（すなわち SAS）に準拠して監査を実施しなければならない。閉鎖会社の場合には，コンピレーションおよびレ

図4　ECAS契約における適切な職業基準の選択プロセス（その2）



（出所）Nagel et al.[1999], p. 188.

ビュー基準（SSARS）に準拠してレビューを実施しなければならない。

「図3」にみられるように，クライアントが予測財務諸表またはプロジェクション，もしくは見積財務情報を要求している場合には，AT200 または AT300 を適用するのが適切である。SSARS，SAS，AT200 および AT300

でカバーされないそれ以外のタスクは，アテステーション基準（AT100）の適用を受ける。また，「図3」および「図4」では示されていないが，クライアントが財務諸表に関連した内部統制のアテストを必要としている場合はAT400を，また何らかの要件や規制への準拠性につきアテストを必要としている場合はAT500を適用することができる。最後に，既知の利用者が手続きの設定に関与しており，かつ報告書の配布がそれらの利用者のみに限定されているような状況では，AT600を適用することができる。

以上に述べたアテステーション基準は，ECAS契約においては，最初にシステムの信頼性保証から適用される。

V　システムの信頼性保証

(1)　基準の適用可能性

上で検討したように，「アテステーション契約基準書」(SSAE) では11の基準が体系化されている（「表2」を参照)。これらの基準は，アテステーション契約の計画，実施および報告に関する権威ある基準を意味している。監査基準が「監査基準書」(SAS) において体系化されているのと同様に，アテステーション基準は，技術的能力，独立性，正当な注意義務，計画と監督，証拠資料および報告に関する問題を扱っている。しかしながら，その性格はより広範なものである。SSAEおよびSASは，何れもAICPAの監査基準審議会（Auditing Standards Board; ASB）で作成されたものである。

監査基準（SAS）の適用可能性はとりわけ財務諸表監査に関連しており，アテステーション基準を既存のSASで代用することはできないとしても，保証業務の監督と実施をより揺るぎないものとするために，確立されたSASの体系を指針として用いることが妨げられるわけではない。例えば，SSAEではある特定なタスクや手続きが要求されておらず，しかも，それらのタスクや手続きに関連したSASが当該ECASには適用されない場合であって

も，指針として適切である場合には言及することができる。一般的な観点から見て，SAS はアテステーション契約の概念的で健全な指針を提供している。

⑵ ECAS 契約の実施基準

GAAS には，次の三つの実施基準がある。

① 第一基準――業務は適切に計画し，何らかの補助者が存在する場合には，これを適切に監督しなければならない。

② 第二基準――監査を計画し，実施すべきテストの性格，時期および範囲を決定するために，内部統制を十分に理解しなければならない。

③ 第三基準――監査を実施している財務諸表につき監査意見を表明するための合理的基礎を与えるために，実査，立会，質問および確認を通して，十分にして適格な証拠資料を入手しなければならない。

これらの三つの実施基準は，電子商取引の保証業務（ECAS）に関して，計画，実施および報告の有用な枠組みを提供している。以下では，ECAS 契約のためのフォーマルな「トップダウン」アプローチを検討する。このアプローチは，適用可能な SSAE と既存の監査基準の両者に基づいている。

⑶ 第一実施基準

「表 3」は，第一基準に関連した ECAS 契約の内容と，参照すべき AICPA 職業基準を纏めたものである。また，Nagel et al.［1999］に収録されている実務支援ツールが対応表示されている。

⑷ 第二実施基準

「表 4」は，第二実施基準に関連した ECAS 契約の内容と，参照すべき AICPA 職業基準を纏めたものである。また，Nagel et al.［1999］に収録されている実務支援ツールが対応表示されている。

⑸ 第三実施基準

「表 5」は，第三実施基準に関連した ECAS 契約の内容と，参照すべき

表3　ECAS契約のための計画および監督

記　述	セクション	実務支援ツール
計画および監督		
・　契約の性格，監督および範囲の決定	AU310/311	アテステーションの計画書式
リスクおよび重要性		
・　エラーや脱落の程度の測定（過大／過小表示）	AU312	計画の重要性
・　アテステーションリスク（重要なエラーや脱落を見落とすこと）の要素に関する予備的な判断		
－　固有リスク（個々のアサーションに重要な脱落や虚偽表示が起こり易いこと）		
－　コントロールリスク（エンティティのコントロールが重要な脱落や虚偽表示に気付かないリスク）		
－　発見リスク（アシュアラーが重要な脱落や虚偽表示を発見できないリスク）		

（出所）Nagel et al.［1999］, p. 345.

表4　ECAS契約における内部統制の理解

記　述	セクション	実務支援ツール
システム		
・　フローチャートの作成によりシステムの重要なステップとコントロールポイントを識別すること	AU319	システム全体の質問書
内部統制		
・　ＥＣシステムおよび内部統制を詳細に理解すること		
－　アテステーションに関連したコントロールの設計を理解すること	AU319（SAS-78）（AT400）	リスク／統制マトリックス内部統制の自己評価質問書
－　それらのコントロールが運用されているかを決定すること		

（出所）Nagel et al.［1999］, p. 354.

表5　ECAS契約における証拠資料の収集と評価

記　述	セクション　実務支援ツール
コントロールのテスト	
・　特定なアサーションとコントロール	AU326　保証テスト手続プログラム
・　証拠資料	（SAS-80）
・　コントロールのテスト	
・　コントロールに関する結論を裏付ける運用上の有効性評価	
サンプリング	
・　属性テスト―発生率	AU350　属性サンプリングおよび
	（SAS-39）計画評価ワークシート

（出所）Nagel et al.［1999］, p. 366.

AICPA 職業基準を纏めたものである。また，Nagel et al.［1999］に収録されている実務支援ツールが対応表示されている。

VI　システム保証の方法論

(1)　ECAS を実施するためのプロセスおよび手続き

既に述べたように，財務諸表監査のための職業基準は ECAS 契約に特化して適用することはできないとしても，優れた基礎となりうるものである。とりわけ，GAAS に含まれる三つの実施基準は，保証の方法論として有用な枠組みを提供している。「表6」は，保証方法論のプロセスおよび手続きを五つの主要なステップ（①～⑤）に分けて纏めたものである。

(2)　支援ツール

Nagel et al.［1999］は，AICPA の職業基準に基づいて ECAS 契約を実施する際に用いる各種の支援ツールを開発している。システムの信頼性保証に関連したツールは，次の二つのカテゴリーに分けられる。

①　全般的な保証支援ツール

・　システム全体に関する質問書

・　属性サンプリング計画および評価書式

表6　ECASを実施するためのプロセスおよび手続き

計　画

① 計画および監督―契約の性格，時期および範囲を決定する。
- 経営者の関与およびリソースの考慮―組織的な環境，情報の報告手続およびモニタリングの方針を考慮する。

② ＥＣシステムとその内部統制を理解する。
- フローチャートを作成して，システムの重要な処理ステップとコントロールポイントを識別する。
- コントロール目的を決定する。
  - 承認，妥当性，正確性，および適時性を有する取引を保証する。
  - データのロス，ダメージまたは不正な開示を防止する。
- 重要かつ優先度の高い資産を決定する。
- リスクとその脅威を理解し評価する。
  - 内部的原因および外部的原因（ハッカー）。
  - 承認された行為と承認されていない行為。
  - 故意の行為（ウィルス）と故意でない行為（エラー，脱落および誤謬）。
- コントロール活動を識別する。
  - 企業全体のレベルとアプリケーションシステムのレベル。
  - 人員，システムおよび種々のツールに関するコントロール。
  - 予防的統制，発見統制および修正統制。

実　施

③ コントロールをテストし，マネジメントによるアサーションの準拠性を評価する。
- マネジメントによるアサーションを以下の目的にリンクさせる。
  - 財務諸表：実在または発生，完全性，権利および義務，評価または配分，作成および開示。
  - 保証報告書：承認，妥当性，正確性，適時性および機密性の保持された取引，データの完全性および可用性。
- 証拠を評価し，以下の方法を用いたテストを実施する。
  - 質問および立会。
  - 実査および再処理：サンプル，テストおよび監査証跡による記録の追跡。

④ 非準拠性を測定する。
- 潜在的なロスの程度，非準拠性の実質的なリスクを決定する。

報　告

⑤ 発見事項の報告
- エグザミネーションまたはレビュー報告書を作成する。
- 無限定意見または限定意見を発行する。
- 必要に応じて，外部のサービス組織に関する報告を含める。

（出所）Nagel et al.［1999］，pp. 395-396.

- 処理サービス組織に関する報告書

② 組織体レベルおよびアプリケーションレベルの支援ツール

- リスク／コントロールマトリックス
- 自己評価質問票
- 保証手続テスト実施計画

(3) リスク分析のためのシステムモデル

リスク評価とは，組織体の目的や目標を達成する際の内部的・外部的なリスクおよび脅威を識別し分析するプロセスである。リスク評価は，組織体全体のレベルまたは個々のアプリケーションシステムのレベルで行うことができる。この両者のリスク評価によって，コントロール活動を通じてのリスク管理の在り方が決定される。

ECAS 契約の場合，リスクの評価と分析は，全体的な情報システム環境のコンテクストと，個々の業務処理サイクルのコンテクストにおいて行われる。リンクされ階層化されたシステムモデル（linked and layered system model）を用いた体系的方法でリスク分析を行うことによって，組織体のコントロール目的を満たすために必要なコントロール活動につき，完全でバランスのとれた測定を行うことができる。

「表 7」は，一般的なシステム分析モデル（general systems analysis model）を示したものであり，EC 環境に適用されうるものである。このモデルは，階層化アプローチ（layered approach）を適用しており，組織体レベルおよびアプリケーションレベルの両者において，重要な処理ステップとセキュリティコントロールの要点をピンポイントで指摘し識別することができる。

いわゆる COSO と同様，「表 7」の階層化システムモデルは，コントロールの構成要素を二つの主要なカテゴリーに分けており，①組織体レベルのコントロールが全般管理，報告およびモニタリング活動を扱うのに対して，②アプリケーションコントロールは，特定システムの処理プロセスを扱ってい

表7　リスク分析のためのシステムモデル

組織体レベルの分析
① 戦略上の計画および目標
- 組織構造
- ビジネスプラン

② 電子商取引システム

アプリケーションレベルの分析
① 直接的なアプリケーションプロセス
- ユーザサービス（クライアント／サーバ）
  - ファイヤウォール
  - アクセス
  - 暗号化
  - ウィルスのプロテクション
- ビジネス／トランザクションサービス（ルールおよび論理）
  - ビジネス（組織体）・インバウンド・売上げ➡決済
  - ビジネス（組織体）・アウトバウンド・売上げ➡決済
  - 取引（システム）
- データサービス（通信）
  - 電子データ交換（ＥＤＩ）

② 間接的アプリケーション：支援サービス
- 設計および開発
  - 開発およびプロジェクト管理
  - 保守および修正
- ユーザ支援サービス
  - 操作
  - 訓練および文書化
- システム支援サービス
  - バックアップ
  - 被害からの回復

（出所）Nagel et al. [1999], p. 398.

る。更に，後者のアプリケーションコントロールは，直接および間接の二つが定義されており，直接コントロールは実際の取引処理に関連し，間接コントロールは開発・運用・バックアップ等の支援活動を表している。

VII　結びに代えて

以上の議論は，基本的に EC システムに特化した信頼性の保証問題であるが，対象を一般化して議論を展開することも可能である。すなわち，エリオット委員会報告書の流れを汲む Nagel et al.［1999］で検討されている枠組みは，情報システム一般の信頼性保証に対しても適用可能性を有していると考えられる。また，仮に EC システムの信頼性保証に限定して考えても，AICPA は企業対企業（business-to-business）ヴァージョンのウェブトラストを検討中であるから，その保障内容は単なるオンラインショッピングの範疇を超えて，より広範な意義と性格を有するようになるであろう。

【参考文献】

David, Julie Smith, Cheryl L.Dunn, William E.McCarthy, and Robin S.Poston［1999］, "The Research Pyramid: A Framework for Accounting Information Systems Research," *Journal of Information Systems* (Spring), pp.7-30.

Elliott, Robert K.［1992］, "The Third Wave Brakes on the Shore of Accounting," *Accounting Horizons* (June), pp.61-85.

――――［1994a］, "Confronting the Future: Choices for the Attest Function," *Accounting Horizons* (September), pp.106-124.

――――［1994b］, "The Future of Audits," *Journal of Accountancy* (September), pp.74-82.

――――［1995］, "The Future of Assurance Services: Implication for Academia," *Accounting Horizons* (December), pp.118-127.

――――［1997］, "Assurance Services Opportunities: Implication for Academia," *Accounting Horizons* (December), pp.61-74.

Murthy, Uday S.and Casper E.Wiggins, Jr.(Co-Editors of the Information Systems Section of American Accounting Association)［1999］, "A Perspective on Accounting Information Systems Research," *Journal of Information Systems* (Spring), pp.3-6.

Nagel, Karl D., Glen L.Gray［1999］, *Electronic Commerce Assurance Services 2000: Electronic Workpapers and Reference Guide*, Harcourt Brace Professional Publising.

Special Committee on Assurance Services［1997］, *Report of the Special Committee on Assurance Services*, American Institute of Certified Public Accountants

(http://www.aicpa.org/ assurance/indx.htm).
池田公司［1999］「IT 監査とリスク指向監査アプローチ」會計，第156巻第４号，99-113頁。