論　文

成熟度モデルに基づく情報セキュリティ監査の新たな試み

堀 江 正 之*
（日本大学商学部教授）

1．序－リスク指向の情報セキュリティ管理と監査－

（1）リスク評価に基づく情報セキュリティ管理の勘所

いま仮に，試験問題で「情報セキュリティ対策としてのコントロールはどのように決定すべきですか。その要点を一言で答えなさい。」と問われたとする。どう答えればよいか。おそらく「情報セキュリティのリスク評価に基づいて決定する」というのが模範的な解答とされるだろう。ここでのキーワードはもちろん“リスク評価”である。

リスク評価に基づく情報セキュリティ対策の基本的な考え方は，リスクが高い対象には相対的に強固な対策を講じ，リスクが低い対象には相応の対策を講ずることによって，全体として効果的かつ効率的なコントロールが構築されるという点にある。“全体として”というくだりがミソである。情報セキュリティ対策は，複数のコントロールが結びつけられた“コントロールの鎖”として機能している。だから，鎖に一箇所でも弱いところがあると，鎖全体としての強度はもっとも弱い箇所の強度になってしまうのである。

譬えていえば，家の防犯対策として，守るべき資産の多寡を考慮しないで玄関の鍵をこれでもかといわんばかりに厳重にして，小路に面した裏手の窓を施錠しないという事態を避けることにある。

保護すべき情報資産の重要性に応じて，セキュリティ上の弱点を焙り出し，そこに重点的に必要な手当てを講ずる。しかもリスクは常に変動するからダイナミックに対応する。それによって全体として情報セキュリティ対策の適正水準を保つ。これが“リスク評価に基づく”情報セキュリティ対策の勘所である。

*1958年新潟県生まれ。1986年日本大学大学院商学研究科博士課程修了。1996年より日本大学商学部教授。『システム監査の理論』（『青木賞』受賞）などの著書がある。Information Systems Audit and Control Association 調査担当常務理事，経済産業省「情報セキュリティ監査研究会」委員などを歴任。現在，日本監査研究学会「監査教育の現状と課題研究部会」委員，日本内部監査協会「内部監査実務委員会第二部会」部会長。

（2）リスク評価に基づく情報セキュリティ管理の判断尺度

今般，経済産業省から情報セキュリティの管理と監査についての包括的な基準群が提示された[1)]。政府機関を含むあらゆる組織体に適用できる「情報セキュリティ管理基準」は，情報セキュリティ管理に関する国際標準ISO17799：2000（JIS X 5080：2002）を基に作られている。情報資産の機密性，完全性，及び可用性を確保するためのコントロール1,000項目弱が示されているが，すべてのコントロールを選択し実施することが推奨されているわけではない。リスク評価を行って，適宜追加又は削除することによって，組織体の実情に合わせたコントロールを設計すべきものとされている。

この「情報セキュリティ管理基準」と対をなすのが「情報セキュリティ監査基準」である。当該監査基準に基づいて行われる監査は，「情報セキュリティ管理基準」を監査上の判断の尺度（監査対象の良し悪しを判断するための“ものさし”）として用いることを原則とする。換言すれば，情報セキュリティ監査とは，組織体が採用する情報セキュリティ対策が「情報セキュリティ管理基準」に従って適切に運用されているかどうか，改善すべき事項がないかどうかの監査である。

しかし，「情報セキュリティ管理基準」は，組織体ごとにリスク評価を行って，適切なコントロールを取捨選択するというように，リスク評価を，基準適用に当たっての大原則としている。このことは，情報セキュリティ監査では，「情報セキュリティ管理基準」を基礎としつつ，リスク評価に基づいて組織体に見合った情報セキュリティ対策の適正水準を実質的な判断尺度とすることを意味する。ここに厄介な問題が生ずる。“判断尺度のゆらぎ”である。情報セキュリティ監査人の監査報告書に記載される「われわれは，“情報セキュリティ管理基準”に照らして，xxx（途中略）xxx監査を実施した」ということは，一体何を意味するのか。

また，情報セキュリティ対策にかけることができるコストや人員にはおのずと制約があるから，最初から完璧に近い水準を目指すことは現実的でない。中小零細企業や地方の市町村では，Webシステムの開発から運用までのすべてをごく少人数の職員又は派遣社員―極端な場合１人―に任せていることも決して珍しくない。そのような状況にあって，いきなり高度な情報セキュリティ対策を求めても，実行はおぼつかない。

このような問題を解決するための糸口となり得るのが，本稿で取り上げる情報セキュリティ対策の成熟度モデル（maturity model）である。現在の情報セキュリティ対策の水準を確認しながら，高次な水準へと段階的に上げてゆく。監査人は，情報セキュリティ対策の段階ごとに保証を与え，次の段階へと進むための改善提案を行うという考え方である。

１）経済産業省商務情報政策局長の諮問研究会として設置された「情報セキュリティ監査研究会」の成果として2003年３月に公表されたもので，“情報セキュリティ管理に関する基準群”及び“情報セキュリティ監査に関する基準群”に大別される。前者のカテゴリーには「情報セキュリティ管理基準」「個別管理基準策定ガイドライン」「電子政府情報セキュリティ管理基準モデル」がある。また，後者のカテゴリーには「情報セキュリティ監査基準」「情報セキュリティ監査基準―実施基準ガイドライン―」「情報セキュリティ監査基準―報告基準ガイドライン―」「電子政府情報セキュリティ監査基準モデル」がある。それぞれのカテゴリーごとに，いかなる組織体にも適用できる「情報セキュリティ管理基準」と「情報セキュリティ監査基準」の２つを最上位の“基準”として位置づけ，それらをより実践に即して解説したものを“ガイドライン”とし，さらに電子政府に固有の特質を加味した電子政府向けの管理と監査の実践手引書を“モデル”として示している。このように一連の基準群は，順次より具体的なものへと落とし込んでゆくという全体構想のもとで体系づけられている。これら情報セキュリティ管理と監査に関する基準群は，経済産業省のホームページ（http://www.meti.go.jp）から入手できる。

２．情報セキュリティ対策の成熟度モデル

（１）情報セキュリティ対策の“改善”をめぐる２つの意味

情報セキュリティ対策は，定期的に，できれば継続的に見直しが行われ，改善が図られなければならない。P（Plan）-D（Do）-C（Check）-A（Act）という管理サイクルに基づいたスパイラルアップである。

ここで“情報セキュリティ対策の効果を高める”という場合，２つの意味が区別される。

第１の意味は，事業戦略の変更，組織構造の再構築，新たな攻撃手段の出現，ITの進展などによる経営環境の変化，あるいはそれらに伴うリスクの変動を反映した情報セキュリティ対策の“改善”である。これがうまく行けば，結果として情報セキュリティ対策の効果が高められる。けれども，与件変化に伴う改善であるから，どちらかといえば情報セキュリティ対策の特定の水準―この水準が適正水準であるとは限らない―を想定し，その水準を“維持”するというニュアンスが強くなる。

情報セキュリティ監査人が行う情報セキュリティ対策についての改善提案も，このような与件変化に伴う改善を内容とする方が説得力ある監査報告となるだろう。監査人の改善提案と，その根拠となった事実との間の距離を縮めることができるからである。実務の現場でよく見受けられる「監査人からなぜこのような改善提案が出てきたのかその根拠がよく分からない」という被監査側からの疑問は確実に少なくなる。

第２の意味は，現在の情報セキュリティ対策の水準を，あるべき水準又は理想的な水準に向けて，段階的に高めてゆくという意味での“改善”である。必ずしも経営環境等の与件変化を前提としないこと，そして目標としての情報セキュリティ対策の水準が明示的に想定されている―数量水準として把握されるわけではないが―という点で，第1の意味と区別される。

この第２の意味が，情報セキュリティ対策の成熟度に応じた改善である。情報セキュリティ対策が段階的に徐々に完成してゆくプロセスを想定した上で，満たすべき一定の情報セキュリティ対策の要求水準によって段階を区分けする。情報セキュリティ監査では，成熟度に基づく段階を特定して，情報セキュリティ対策の有効性を評価する。例えば「現在採用されている情報セキュリティ対策は，第５段階―管理プロセスが最適化されている段階―の水準を前提とする限り，適切であると認める」あるいは「情報セキュリティ対策は現在第３段階―管理手続が標準化されている段階―にあるが，以下に提案するxxx（略）xxxという改善策が盛り込まれれば，第４段階―定量的な管理が行われている段階―へと進むことができる」といった意見表明を行う，これまでにはなかった新しい形の監査である。

（２）成熟度モデルの考え方

それでは，情報セキュリティ対策の成熟度は，どのように区分けされるのであろうか。情報セキュリティ対策の成熟度モデルとしてもっとも代表的なものは，ソフトウェア開発プロセスの能力評価のための成熟度モデルを，システムのセキュリティエンジニアリングに援用した技術仕様SSE-CMM（The System Security Engineering Capability Maturity Model）である[2)]。

2）Information Systems Security Engineering Association , *The System Security Engineering Capability Maturity Model―Model & Appraisal Method Summary*, Apr.1999. これは，NISTのホームページ（http://www.sse-cmm.org）から入手できる。

図１は，その基本的な考え方を表したものである[3)]。図の上段は，情報セキュリティ対策が段階を追って成熟してゆくイメージを表している。また，図の後段は，段階ごとに要求される特質を示したものである。段階ごとに要求特質を定義し，それが達成されていることをもって，情報セキュリティ対策がどの段階にあるかを判別する。成熟度の段階が上がってゆくに従って，要求特質も高度になる。いうまでもなく，上位の段階は，それよりも下位の要求特質を満たしていなければならない。各段階の要求特質の１つでも満たされなければ，それより１つ下の段階として判別される。

図１　成熟度モデルのイメージと要求特質

非公式な段階	計画と追跡がある段階	プロセスを標準化している段階	定量的なコントロールがある段階	継続的に改善している段階
・最低限の主要手続は実施している	・手続の実施を計画している ・手続の実施を訓練している ・実施結果を追跡している ・実施結果を点検している	・手続の標準を定義している ・標準となるプロセスがある ・定義されたプロセスを実施している	・測定可能な品質目標を設定している ・客観的な業績管理を行っている	・組織能力を改善している ・プロセスの効果を改善している

情報セキュリティ対策が成熟してゆくイメージを客観的なモデルとするためには，成熟度の段階ごとの要求特質をどれだけ厳密に規定できるかにかかっている。その一方で，成熟度の段階をあまり細かく分断しすぎると，実際の判別で使いにくくなる。成熟度モデルの段階の区切りと，それぞれの段階での要求特質の厳密さの程度は，成熟度モデルをどのような目的に使うかにかかっている。

SSE-CMMのようにシステムのセキュリティエンジニアリングへの適用に拘らなければ，例えば「必要かつ十分な情報セキュリティ対策がなく，最低限の手続が場当たり的に適用されている段階」「必要かつ十分な情報セキュリティ対策が，規定として整備されている段階」「必要かつ十分な情報セキュリティ対

3）情報システムコントロール協会ISACAが公表しているITコントロールのガイドブック*COBIT*（*Governance, Control and Audit for Information and Related Technology*）では，その第３版から，SSE-CMMの考え方を援用した「ITガバナンスの成熟度モデル」という概念を取り入れた。*COBIT*で示されているITガバナンスの成熟度モデルは，次の５段階である。第１段階：標準化された手続がそもそも存在しない場当たり的な段階。第２段階：手続に反復性はあるが個人の直感に頼る段階。第３段階：測定可能な洗練されたところまでゆかないがプロセスが明確に定義されている段階。第4段階：プロセスに対する監視と測定が可能で，プロセスが継続的に改善されている段階。第5段階：プロセスが継続的に改善され，外部の規範的実践に照らしても最適化されている段階。SSE-CMMで示された１から５までの各段階にそれぞれ対応していることが分かるだろう。

策が，規定に従って実際に運用されている段階」といった３段階モデルでも構わないだろう。

SSE-CMMのモデルは，個々のコントロール項目ごとに成熟度を評価するものではなく，また情報セキュリティ監査への適用を狙ったものでもない。そこで次に，この概念モデルが情報セキュリティ自己評価にどのように援用できるか，そしてさらに進んで情報セキュリティ対策の第三者認定・認証への応用について検討してみたい。

３．成熟度モデルを使った情報セキュリティ自己評価

（１）NISTが提案する自己評価

情報セキュリティ対策がどの程度有効か。それを情報セキュリティに直接的な責任を有するシステム部門又はユーザ部門が，自らの判断と責任において評価することを，情報セキュリティ自己評価という。

自己評価は，次のようなさまざまな目的に使うことができる。

・情報セキュリティ対策の現況についての全般的な理解を得ること。
・改善が必要な領域やコントロール項目を特定すること。
・情報セキュリティ対策の欠陥や弱点についての責任の所在を明らかにすること。
・情報システムに責任を負う管理者が，経営層又はユーザ部門に対してアカウンタビリティを果すための手段とすること。
・情報セキュリティ監査に利用すること。

米国商務省のNIST特別報告書800-26「ITシステムのためのセキュリティ自己評価ガイド」は，情報セキュリティ自己評価に成熟度モデルを組み込んだ使い方を提案している[4)]。NISTが提案している自己評価は，管理上のコントロール，業務上のコントロール，及び技術上のコントロールを網羅する225項目からなるコントロールごとに，次の５段階のうちいずれの段階にあるかを，それぞれの段階に割り振られた要求特質によって判別し，チェックマークを付けてゆく形で進められる[5)]。

４）National Institute of Standards and Technology, Technology Administration U.S. Department of Commerce, Computer Security－Security Self-Assessment Guide for Information Technology Systems, （NIST Special Publications 800-26）, Nov.2001. なお，本報告書は，米国商務省NISTのホームページ（http://csrc.nist.gov）から入手できる。

５）各段階で求められる要求特質は，次の通りである。第１レベル：①目的と範囲が明確であること。②責任の所在が明確であること。③準拠違反のペナルティが明確であること。第２レベル：①コントロールの適用領域が明示されていること。②適用されるコントロール手続が文書化されていること。③セキュリティの責任と役割が明確にされていること。第３レベル：①オーナとユーザがセキュリティ方針と手続を十分に認識していること。②方針と手続が正式に採用され，技術的コントロールが導入されていること。③セキュリティがシステムのライフサイクルを通じて管理されていること。④認証や認定のための手続が確立されていること。⑤セキュリティ状況記述書が作成されていること。⑥全従業員に対するセキュリティ手続についての適切な訓練が行われていること。第４レベル：①セキュリティ方針，手続，コントロールの適切性と有効性を評価するための効果的なプログラムがあること。②セキュリティ事故に基づく脆弱性の識別又はセキュリティ警告のメカニズムがあること。③重要なセキュリティ上の弱点を報告するプロセスが明確であり，弱点を補正するための効果的な行動計画が用意されていること。第５レベル：①費用対効果に優れたセキュリティを達成するための組織体全体をカバーする実行プログラムがあること。②ITセキュリティが組織体にとっての価値ある実践となっていること。③セキュリティ上の脆弱性が理解され管理されていること。④脅威は継続的に再評価され，コントロールがセキュリティ環境の変化に対応していること。⑤追加的又はより費用対効果に優れたセキュリティ対策の代替案が必要に応じて利用できること。⑥セキュリティ対策のコストと効果が可能な限り厳密に測定されていること。⑦セキュリティプログラムのステータスメトリクスが確立され合意されていること。ここでは，本稿での趣旨から逸れるため敢えて詳述しないが，NISTが提唱する成熟度モデルと前述したSSE-CMMの成熟度モデルには，要求特質からみたとき，同じ成熟度モデルといってもその考え方に違いがあることに気づくであろう。

第１レベル：コントロール目標が文書化されている段階
第２レベル：セキュリティコントロールが手続として文書化されている段階
第３レベル：手続が導入されている段階
第４レベル：手続とセキュリティコントロールがテストされレビューされている段階
第５レベル：手続とセキュリティコントロールが包括的なプログラムとして完全に統合されている段階

以下は，自己評価シートへの記入例である[6)]。レベルごとの要求水準の達成を確認しながら，チェックマークを付けてゆく。

コントロール（質問項目）	レベル１	レベル２	レベル３	レベル４	レベル５	リスクに基づく決定	コメント欄
＜リスク管理項目＞ 現在のシステム構成が、他のシステムとの接続を含め、文書化されているか	☑	☑	☑				
＜災害復旧対策＞ 処理の優先順位が確立され、経営層によって承認されているか	☑	☑	☑	☑		X	
＜アクセス承認＞ パスワードは少なくとも90日ごとに、あるいは必要に応じてより短い期間ごとに変更されているか	☑	☑				X	

NISTが提案する自己評価では，一つ一つのコントロール項目の判定に当たって，リスクを考慮すべきこととしている。リスク評価に基づいて成熟度を判定した場合には，評価シートの該当欄“リスクに基づく決定”にチェックマークを付し，また判定の根拠として特筆すべきものがあれば“コメント欄”に記入しておく。

このようにして作成された自己評価シートは，自己評価の目的に沿って，さまざまに加工できる。例え

6）NIST特別報告書800-26では，まず“管理上のコントロール”，“業務上のコントロール”，“技術上のコントロール”という３つの大項目を区分し，さらに“リスク管理体制”，“災害対策”，“論理的アクセス管理”など合計17の中項目を立て，大項目ごとに割り振っている。また，中項目ごとに示される個々の質問項目は，米国会計検査院の「連邦情報システムのコントロール・監査マニュアル」（Federal Information System Control Audit Manual：FISCAM）などから多くを援用している。

ば，質問項目を，管理対象，管理項目，又は管理部署といった適当なセグメントで括って，成熟度レベルごとにチェックマークの数を合計して，それをクロス集計したりレーダーチャートで表せば，コントロールの強みや弱みを分かり易く表現できる。

評価シートに付されたチェックマークの数を合計するという作業は，一見すると乱暴な感がある。しかし，情報セキュリティ対策の重点的投資領域の絞込みや，情報セキュリティ監査対象の優先順位付けなどには手軽で有効な手法である。

ただし，このときに注意しなければならないことがある。それは，質問項目を記述する際の抽象さ又は具体さにデコボコが生じないようにすることはいうまでもなく，客観的な事実を問う項目と評価者の主観的判断が多分に入り込む項目の混同集計も好ましくない。NISTの評価シートで旨く工夫されている点は，主観性が入り込む余地をできるだけ小さくするような質問項目を意識して使っていることである。

分かり易い例で説明してみよう。「パスワードは英数字の組み合わせで８桁以上としているか？」というのは客観的な事実を確認する質問項目である。これに対して「パスワードは推論し易いものとなっていないか？」という質問項目にすると，主観によるブレが入り込む余地が大きくなる。この点を強調して，評価シートの質問項目は事実確認ができるところまで具体的に落とし込むべきであるとする主張を散見するが，必ずしもそうとは思わない。

確かに，評価シートの質問項目は，客観的な事実確認に近いところに揃えておくことが望ましい。しかし，ここで紹介しているNISTの自己評価シートは，“ リスク評価シート ”としての性質も兼ね備えている。このような使い方をするときには，端末ごと，担当者ごと，あるいは対象システムやファイルごとに，リスクに応じてパスワードの桁数が個別的に決定されることを前提とした質問でなければならない。質問を極端に具体的かつ固定的にしてしまうと，リスク評価シートとしての意味をなさなくなる。

このように，一口に自己評価シートといっても，それをどのような目的でどのように使うかによって，同じ内容の質問であっても，質問項目の立て方にはおのずと違いが出てくるのである。

（2）自己評価と監査との関係

自己評価は情報セキュリティ監査とどのように関係しているか。自己評価の目的の一つに，情報セキュリティ監査のための利用があることはすでにふれた通りである。それでは，行為の当事者による自己評価の結果を，第三者評価としての監査ではどのように取り扱うことができるだろうか。

まず，自己評価の結果を監査人の監査証拠として利用するというあり方があり得る。本来監査人が行うべき業務を被監査部門に代行してもらうという意味において，監査事務の負担軽減となる。情報セキュリティ監査の目的が，情報セキュリティの欠陥又は弱点を見つけ出し，改善事項を提示することにあれば，このような進め方はかなり効果的である。なぜならば，被監査部門の方が，どこにどのようなリスクがあり，現在運用している情報セキュリティにいかなる欠陥があるかを，監査人よりも現場感覚として熟知している場合が多いからである。

ところが，情報セキュリティ監査の目的を，情報セキュリティ対策が適切に運用されているかどうかの“ お墨付き ”，すなわち情報セキュリティ対策の保証に置くと，被監査部門による自己評価の結果を監査人の監査証拠として無条件で採用することができなくなる。自己評価はあくまでも情報セキュリティ監査における予備的調査として位置づけられ，自己評価が適正かつ公正に行われたかどうかを監査人が確かめる手続を踏まなければならないからである。

ちなみに，わが国で100の地方自治体を対象に住民基本台帳ネットワークの監査法人による外部監査が

暫定的に行われたが，当該監査は自己評価の結果を監査人が確かめるという方法で進められた。被監査対象とされる自治体に自己評価シートをあらかじめ配布し，それに対する回答を得，一つ一つの回答が実態に即して正しく記入されているかどうかを監査人が改めて確証してゆくという手続がとられたのである。それならば，いっそのこと自己評価など行わないで，直接，監査人が質問項目に従って監査手続を実施すればよいではないか，という疑問も出てくるだろう。

しかし，住基ネットの監査では，外部監査特有のロジックが取り込まれた。各自治体の責任のもとで行われた自己評価の結果を，監査対象としての“言明（assertion）”―会計監査でいう財務諸表に該当するものと考えると分かり易い―としてとらえ，それに対して監査意見を表明するという論理である[7)]。あくまでも自己評価の結果についての監査意見であって，住基ネットが適切に運用されているという監査意見ではない。監査意見の対象を限定し，もって監査責任を明確にするという考え方が基底にある。

（3）CSAによる自己評価

上で述べた監査における自己評価の利用は，被監査側に監査人が作成した評価シートを渡し，回答を得るというものである。しかし，最近，北米で注目されているコントロール・セルフアセスメント（以下では，CSAという）と呼ばれる手法は，このような質問書法に限定されない。むしろCSAの本来のあり方は，自己評価シートを使った質問書法とはまったく異なった方法論にある。

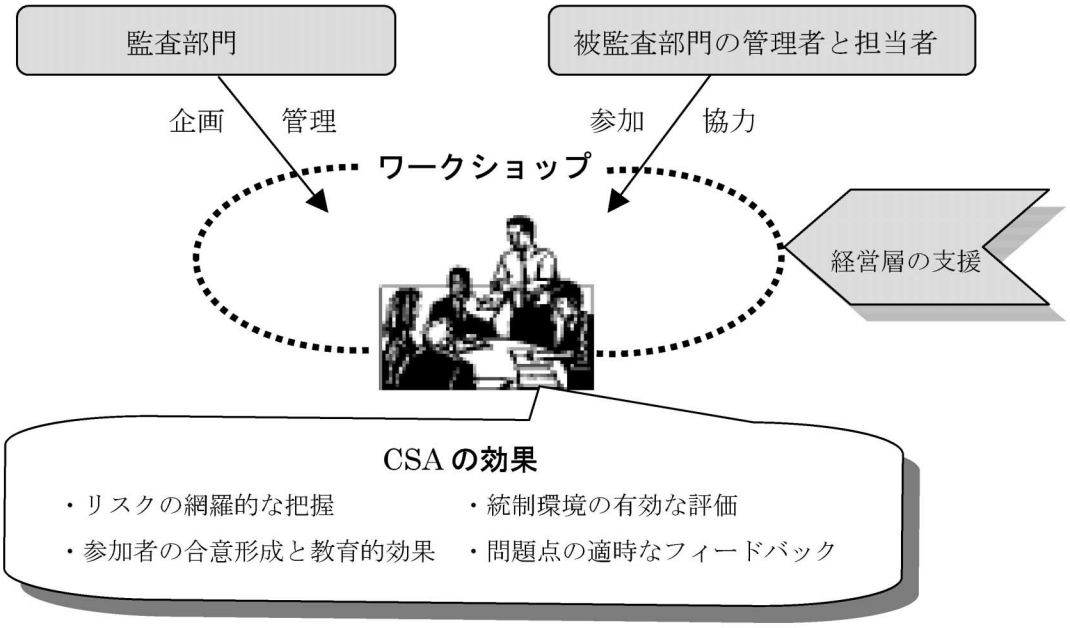
その方法論とは，特定の課題や業務プロセスについて，それに関連する管理者及び現場担当者を一室に集めてテーブルを囲み，ワークショップ方式で業務横断的なリスクを明らかにし，コントロールの問題点を明らかにしてゆくというものである。CSAは，質問書を使った自己評価，あるいは一対一のヒアリングを中心とした伝統的な監査手法の殻を打ち破るものとして，その目新しさも手伝い，北米では急速に普及している。

図２は，CSAのあり方と効果を表したものである[8)]。

7）各自治体に対して自己評価シート（“調査表”という）への回答を求め，かつその範囲を特定する自治体の長による証明（“市町村長記述書”という）を入手して，当該調査表が，「電子通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準」（総務省告示第334号），及び「住民基本台帳ネットワークシステムのセキュリティ対策に関する指針」（住基ネット推進協議会決定）に準拠しているかどうかを確かめる検証手続が行われた。したがって，検証結果としての監査人の意見は，まくまでも“調査表”が上記の基準に準拠しているかどうかについての意見である。このように，監査法人による住基ネットの監査の基本的な枠組みは，会計士監査のロジックをそのまま使った国際監査基準第100号「保証業務」に従って行われたものである。

8）CSAという手法は1987年に，カルガリーにあるGulf Canada Resources社において，事業プロセスと内部統制の有効性を評価するために開発された独特の自己評価手法を嚆矢とする。その後，周知の通り，1990年代に入って事業プロセス再構築のためのさまざまな経営管理手法が提唱され，その中で“グループプロセス・ワーク”，“セルフ・アカウンタビリティ”，“ソフトなデータ収集”への注目がCSAへの関心をより高めることとなった。今日，CSAは，その定義が困難なほど，さまざまな形で行われている。CSAが，Management Self-Assessment，Control and Risk Self-Assessment，Business Self-Assessment®などと呼ばれることがあるのも，そのような手法上の多様性にある。評価シートを使った質問書法も広い意味ではCSAに含まれる。Research Conducted and Reported for The IIA OTTAWA Chapter by Arthur Andersen，*Control Self-Assessment：Experience, Current Thinking, and Best Practices*, IIA, 1996, p.1.

図２　CSAのあり方と効果



このようなCSAの本来的な進め方を前提に考えると，すでに述べた自己評価と監査との関係は一変する。独立の立場からする客観的な検証という監査の本来的役割を後退させることになるからである。しかし，内部監査の領域でCSAが広く普及しているのは，内部監査がコンサルティングモードに入ってきたという理由だけではない[9)]。CSAには，質問書法にはない優れた効果が期待できるからである。

第１に，CSAを使えば，リスクを業務横断的に把握することができる。これに対して，質問書としての自己評価シートを該当部門に配布して記入を求める方法では，業務プロセスを跨ぐリスク評価，又は他の業務部門や他の業務プロセスへのリスクの派生を見極めることに限界がある。

第２に，CSAを使えば，統制環境の評価を有効に行うことができる。ワークショップを通じて，組織構成員の倫理観，組織風土，経営層の方針や経営戦略を踏まえたリスク評価を行うことができる。これに対して，自己評価シートでは，倫理観や組織風土といった要素を反映させることは難しい。

第３に，CSAを使えば，ワークショップを通じて参加者は共通認識を持つことができ，コントロールの必要性や重要性についての教育的な効果も生まれる。直接の当事者がワークショップに参加することから，その場で明らかになった問題点のフィードバックが適時に行われるという効果も期待でき

9）内部監査人協会の国際組織IIA（The Institute of Internal Auditors）は，1999年６月，組織内における内部統制の独立的評定（independent appraisal）として特徴づけられてきた伝統的な内部監査の定義を大きく改めた。新しい内部監査の定義はつぎの通りである。「内部監査は，付加価値をもたらし，組織の業務を向上するために設計された，独立性と客観性をもって行う保証とコンサルティングの活動である。それは，リスク管理，統制，及び統治のプロセスの有効性を評価し向上させるための体系的でよく洗練されたアプローチを提供することにより，組織がその目的を達成することを支援する。」（IIA Guidance Task Force, *A Vision for the Future : Professional Practices Framework for Internal Auditing*, IIA, 1999, p.5.）この定義からも明らかなように，内部監査は，付加価値の向上を意図したコンサルティングという色合いが一気に強まった。

る。これに対して，自己評価シートは，それ自体，教育手段としての機能やフィードバック機能を持っていない。

このように，CSAに期待される効果は，自己評価シートの限界を補うものでもある。したがって，成熟度モデルを前提とした自己評価においても，自己評価シートを補完するものとしてCSAの活用が考慮されてよい。否，むしろ自己評価のプロセスにリスク評価を組み込む場合には，CSAはきわめて有効なものとなるだろう。

監査人にとっても，CSAは，事業プロセスやコントロールの改善，あるいはリスクの低減という，経営に対する付加価値の提供を強く意識させる手法なのである。

４．成熟度モデルを使った情報セキュリティ対策の第三者保証

（１）成熟度モデルによる第三者保証の考え方

監査人が情報セキュリティ対策に保証を付与する場合，これまでの伝統的な考え方によれば，被監査側の情報セキュリティ対策の成熟度を考慮することなく，ある特定の判断尺度に照らして，当該基準を満たしているかどうかという観点から意見を表明するというものである。情報セキュリティ対策がどこまで進んでいるかを考慮しない保証である。喩えていえば，大学生の能力水準という“ものさし”で中学生の能力水準を測るということが起こりえる，あるいはそれを許容する。

このような前提で監査人が保証を付与しようとすれば，“判断尺度”と“情報セキュリティ対策の現実”とのギャップが大きすぎて，保証の付与そのものが困難であったり，ギャップを埋めるための折角の改善提案も現実味がないものとなる可能性が高い。たとえば，コントロールが未整備な組織を対象とした監査で，監査人が「情報セキュリティ管理基準」を厳格に適用すればするほど，被監査対象と判断尺度とのギャップは大きくなる。監査報告書に記載される改善提案は山のようになる。監査人の改善提案の実行が現実に不可能では，折角の監査も意味がない。そこで，監査人は管理基準を緩めて適用しようとする。そうすると，今度は，判断尺度からの大きな離脱を伴った保証や助言になってしまう。また，リスク評価を踏まえた情報セキュリティ対策の設定という視点を強調すればするほど，判断規準の固定性が損なわれる。これが，本稿の冒頭で述べた“判断尺度のゆらぎ”の問題である。

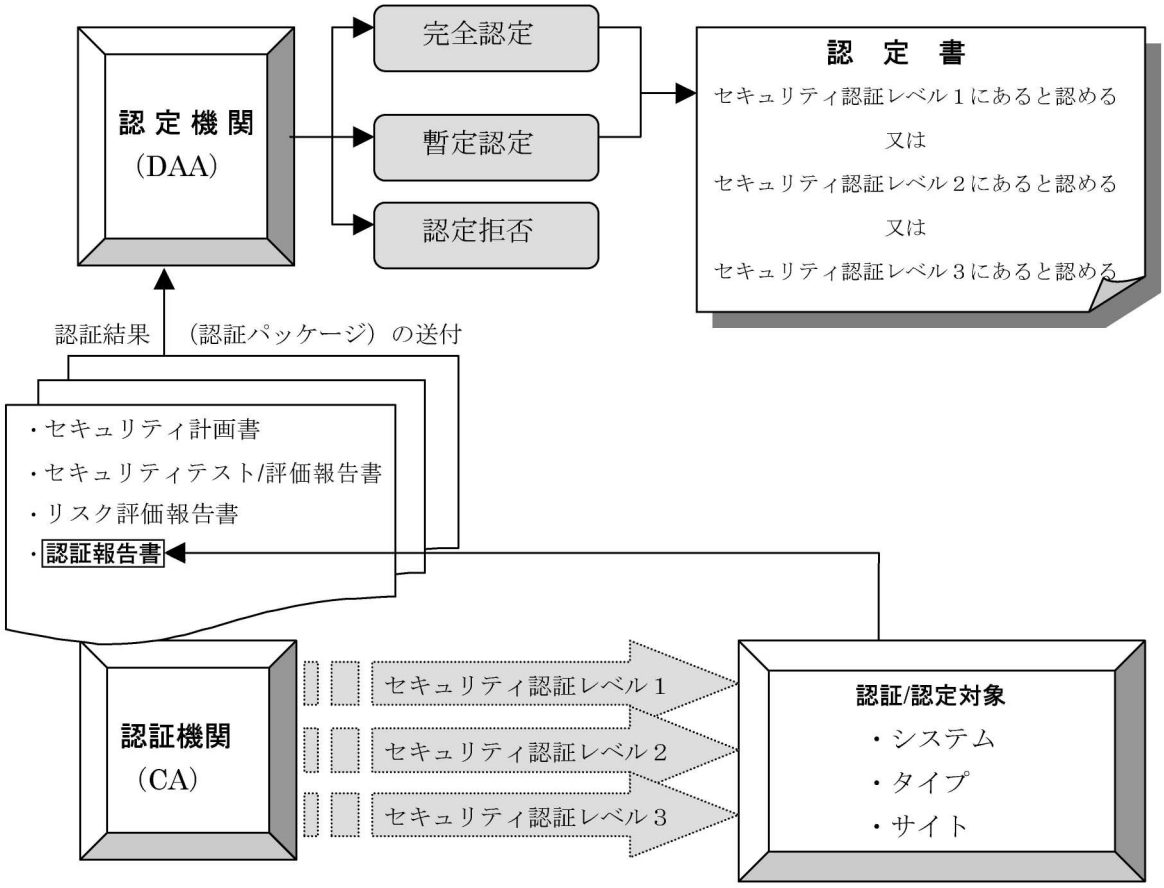
そこで，情報セキュリティ対策の水準を数段階の成熟度によって切り分け，「ある成熟度段階にあること」又は「ある成熟度段階を前提としたときに情報セキュリティ対策が適切であること」を保証してはどうか，という発想が出てくる。

米国商務省のNISTの特別報告書800-37が提案している「連邦情報システムのセキュリティ認証と認定のためのガイドライン」が，それである[10)]。このガイドラインは，情報セキュリティ対策の成熟度とそれに基づく保証を組み合わせた“成熟度－保証モデル”である。

図３は，同ガイドラインの基本的な仕組みを表したものである。

10）National Institute of Standards and Technology, Technology Administration U.S. Department of Commerce, Computer Security － Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, （NIST Special Publications 800-37）, Oct. 2002. なお，本報告書は，米国商務省NISTのホームページ（http://csrc.nist.gov）から入手できる。

図３　連邦情報システムのセキュリティ認証と認定の仕組み



（2）認定プロセスと認証プロセス

同ガイドラインの仕組みを理解するためには，認証（certification）と認定（accreditation）という２種類の保証が区別されていることにまずもって着目する必要があろう[11]。認証機関（Certification Agent：CA）による保証の結果に基づいて，認定機関（Designated Approving Authority：DAA）による保証が行われるという二段構えの構造がとられている。“ 認証 ” が第一次保証，“ 認定 ” が第二次保証といってよいだろう。

ITシステムの実際の評価は，認証機関（CA）が担う。これに対して認定機関（DAA）は，当該ITシステムのリスクが受容可能な水準まで引き下げられているかどうかによって，ITシステムの運用を正式に許可したり，拒絶したりする役割を担った上級職員である。

11）これは，用語の問題であるが，ここでは，日本規格協会の邦訳に依拠して，certificationを「認証」，accreditationを「認定」と訳出している。このような認証と認定の区別は，なにもNISTに固有のものではない。例えば，英国規格に基づく情報セキュリティ管理の保証にもこの区別がある。BS7799, DISC PD 3000, *Information Security Management : An Introduction*（日本規格協会訳，BS7799の公認認証計画の概要「情報セキュリティ管理：序文」）では，認証と認定を次のように定義して区別する。「認証とは，製品，プロセス又はサービスが規定要求事項に適合し準拠している旨を，第三者が文書で保証することである。」「認定とは，ある機関又は個人が能力を有している旨を，権限ある機関が正式に認めることである。」（日本規格協会訳，16－17ページ。）

＜認証のプロセス：第一次保証＞

認証機関（CA）は，セキュリティ計画書に記述されたセキュリティ要求事項とコントロールが遵守されているかどうかを，システム開発や日常の運用から独立した立場から評価を行う。その評価は，ITシステムの技術的な評価に留まらず，管理的側面を含めた全般的なものである。また，認証に当たっては，リスク評価を行って，ITシステムの脆弱性を評価することとされている。

そして，セキュリティ計画書，セキュリティテスト/評価報告書，リスク評価報告書，及び認証報告書（certifier's statement）を作成し，これらを“認証パッケージ”として認定機関（DAA）に送付する。

認証には，次の３つのレベルがある[12)]。

・セキュリティ認証レベル１（entry-level）：低い水準のセキュリティ対策を対象とした低水準の保証

・セキュリティ認証レベル２（mid-level）：中程度の水準のセキュリティ対策を対象とした中水準の保証

・セキュリティ認証レベル３（top-level）：高い水準のセキュリティ対策を対象とした高水準の保証

３つの認証レベルは，下に示すように，情報セキュリティ対策の成熟度を基にして，それに情報セキュリティ対策を評価するときの検証手続の厳格度を対応づけることによって決定されるようになっている。情報セキュリティ対策の成熟度が高ければ，そこで採用される検証手続は厳格なものとなり，逆に，情報セキュリティ対策の成熟度が低ければ，そこで採用される検証手続は緩くても構わない[13)]。

	情報セキュリティ対策の成熟度	検証手続の厳格度
認証レベル１	低 ……	低
認証レベル２	中 ……	中
認証レベル３	高 ……	高

次頁の表は，３つの認証レベルごとに，情報セキュリティ対策の成熟度と，検証手続の厳格を対比形式で整理したものである。

＜認定のプロセス：第二次保証＞

次に，認定機関（DAA）は，認証機関（CA）から送付されてきた認証パッケージ（セキュリティ計画書，セキュリティテスト/評価報告書，リスク評価報告書，及び認証報告書）に基づいて，システム運用のリスクという観点から，次の３つのいずれかの判定を行う。

①完全認定（full accreditation）

②暫定認定（interim accreditation）

③認定拒否（accreditation disapproval）

12）認証レベルは，これまで述べてきたような５段階ではなく３段階とされている。その理由は，おそらく第三者保証にとって５段階では細かすぎるということであると思われる。なお，参考までに，主要国の公認会計士協会が参加している国際会計士連盟が提起している保証業務では，“低レベル保証”では保証を付与する意義がなく，また保証主体（この場合は公認会計士又は監査法人）に対する責任追及を避けるために，“高レベル保証”（監査相当の保証）と“中レベル保証”（レビュー相当の保証）という２区分の保証業務しか提供できない。

13）情報セキュリティ対策の成熟度と実施すべき検証手続は，理論的にはまったく別のものである。低レベルのセキュリティ対策しか採用されていないITシステムであっても，厳格な検証手続を行うことは可能である。この場合には，低レベルのセキュリティ対策について高レベルの保証を付与することになる。高レベルの保証を付与するということは，検証手続を厳格にすることによって，その結果としての保証意見の失敗リスク（保証リスク）を低くすることを意味するのである。

表　情報セキュリティ対策の成熟度と検証手続の厳格度の対応

	情報セキュリティ対策の成熟度	検証手続の厳格度
認　証 レベル１	機密性：情報の未承認開示等の影響が小 完全性：情報の未承認修正等の影響が小 可用性：情報へのアクセス不能等の影響が小	厳格度の低い検証手続 ・関係者への質問 ・セキュリティポリシー、手続書、文書類のレビュー ・システム運用とセキュリティコントロールの観察
認　証 レベル２	機密性：情報の未承認開示等の影響が中 完全性：情報の未承認修正等の影響が中 可用性：情報へのアクセス不能等の影響が中	厳格度が中位の検証手続 ・レベル１の手続 ・機能テスト ・逆進分析及び逆進テスト ・侵入テスト（任意） ・セキュリティコントロールが正確かつ効果的であることの検証デモ
認　証 レベル３	機密性：情報の未承認開示等の影響が大 完全性：情報の未承認修正等の影響が大 可用性：情報へのアクセス不能等の影響が大	厳格度が高い検証手続 ・レベル１及び２の手続 ・システム設計分析 ・カバレッジ分析を伴った機能テスト ・侵入テスト ・セキュリティコントロールが正確かつ効果的であることの実証テスト

①の完全認定は，ITシステムがその情報セキュリティの要求事項をすべて満たし，コントロールが正しく導入されかつ効果的に運用されていることの保証である。認定機関（DAA）は，次のような認定書（accreditation decision letter）を発行する。ここで注目してもらいたい点は，「ある認証レベルにあることを認定」していることである（認定書の**ゴシック書体**の箇所）。

②の暫定認定は，ITシステムが，認定時点においてセキュリティ計画書に記述されたセキュリティ要求事項を満たしておらず，必要なコントロールのすべてが導入されているわけではなく，かつ効果的に運用されているわけでもないが，しかしITシステムをどうしても運用せざるを得ないという場合に使われる仮認定である。例えば，今日の環境のもとでのセキュリティ要求事項を満たすことが難しいレガシーシステム（廃棄できず残された古いシステム）を対象として，新システムへの移行までの期間に限定して，暫定的に保証を付与するという使い方がある。このように，暫定認定は，認定機関（DAA）が定めるある特定期間を限定して付与される認定である。

認　定　書

上級職員　殿

[設置場所 xxx]にある[IT システム名 xxx]及びそのシステム構成要素（このシステム構成要素の記載は任意）を対象とした認定のためのレビューは、行政管理予算庁回覧書 A-130 の附則３「自動化された連邦情報資源のセキュリティ」及び[組織名 xxx]の認証・認定プログラムに基づいて行われた。私は、セキュリティ認証の結果と、その結果を裏付ける認証パッケージ（例えば、IT システムのセキュリティ計画書、セキュリティテスト/評価活動の結果、及び最終的なリスク評価報告書）を注意深くレビューした。

[組織名 xxx]の認証・認定プログラムで定める規定に従って、採用されかつ計画されているセキュリティコントロールをレビューし、さらに業務上の要求事項に照らした場合の残存リスクの重み付けを行った結果、当該システム[IT システム名 xxx]は、さし当たっての運用又は継続的な運用にとって、**セキュリティ認証レベル[１、２又は３]にあることを認める。**

この認定は、上述の前提のもとでの私の正式な宣言であって、必要な情報セキュリティコントロールが適切に導入され、セキュリティの水準が満足すべき状態にある。

―以下、認定業務の限界についての記述は省略―

指定認定機関（DAA）　署名

③の認定拒否は，ITシステムがセキュリティ計画書に記述されたセキュリティ要求事項及びコントロールに合致しておらず，残余リスクがあまりに大きく，いかに当該ITシステムの運用が必要であろうとも，開発システムであればそれを運用に移行することはできず，またすでに運用中であればすぐにその運用を停止すべきことを指示するものである。この場合，認定機関（DAA）は，認定を行わないという旨の書面を，その判定を裏付ける書類とともに発行する。

（3）認証と認定を区別することの意味

公共性が高いシステムやミッションクリティカルなシステムに対して第三者保証を付与するということであればともかくも，そうでない場合には，何も認証と認定を区別することに積極的な意味はない。成熟度の判定は，第一次保証としての認証によって行われるものであって，第二次保証としての認定に進むことなく完結して構わないはずである。したがって，NISTが想定する認証と認定の区別の意味は，別のところにある。すなわち，情報セキュリティ対策の評価という任務―認証―と，情報セキュリティ対策を行

ってもなお残る脆弱性（残存リスクという）についての判定という任務―認定―を区別することにあるように思われる。

リスク評価に基づいて情報セキュリティ対策を設定するというスキームの中でおそらくもっとも厄介な作業は，残存リスクをどの水準にまで引き下げるかの意思決定であろう。概念的には「１－情報セキュリティ対策の有効性＝残存リスク」である。机上では，情報セキュリティ対策の有効性を高めるために，コントロールのタイトネスを全体として強くすれば，それだけ残存リスクは低く抑えることができる。

しかし，現実には，情報セキュリティを確保するためのコントロールにかけられる投資コストには制約があり，また組織構成員の倫理観といった要素を絡めるとコントロールの有効性と投資コストは必ずしも正比例しない。さらに，コントロールのタイトネスを高めれば，それだけ業務効率にブレーキがかかる。その反動がコントロールの無視につながるという悪循環に陥ることもある。したがって，残存リスクの許容水準の判定は，リスク評価に基づくといいながらも，実際にはきわめて複合的な判断が求められるのである。

このように，リスク評価と残存リスクの許容水準の決定は基本的には別の次元のものである。そこで，NISTのように，残存リスクについての許容判断を，リスク評価と切り離して，上級管理職（経営層）に委ねるという役割分担が合理性を帯びてくる。

くわえて，NISTの認証・認定スキームでは，認定機関（DAA）には特別な権限が与えられている。認証機関（CA）は，リスク評価を行って，その結果を認定機関に送付するだけである。けれども認定機関（DAA）には，システム開発やシステム運用を許可したり，禁止する権限がある。すなわち，①完全認定の場合は，ITシステムの開発及び運用にゴーサインを出すことになる。しかし，②暫定認定は，ITシステムの開発及び運用に仮のゴーサインを出すに過ぎない。③認定拒否は，ITシステム開発及び運用を差し止めることになる。

５．結び―判断尺度のゆらぎの克服―

情報セキュリティ対策の適正水準の決定という枠組みにリスク評価という視点を組み込むと，既製の“ある基準”がそのまま組織体に見合った情報セキュリティ対策の水準となるわけではない。突き詰めれば，リスク評価という視点を強調すればするほど，監査上の判断尺度がぐらつく。

リスク評価を前提とする限り，そもそも「情報セキュリティ管理基準」などの既製の基準は，組織体における情報セキュリティ対策が全体として適切であるかどうかを判断するための絶対的な“ものさし”ではありえない。組織体によっては，当該基準が想定している情報セキュリティ対策よりもさらに上の水準が適正水準となることもあれば，下の水準の場合もある。もし上の水準ということになれば，当初メルクマールとした既製の基準は，目標水準ではなくなる。

理屈の上では，リスクの受容可能水準が組織体におけるその時の情報セキュリティ対策の適正水準であろう。ところが，すでに明らかにしたように，リスクの受容可能水準というのは，情報セキュリティ対策に対する経営層の認識の程度，業務目的の効率的な達成とのトレードオフ関係，投資コストの制約などによっても影響を受けるという厄介なしろものである。さらには，リスク要因の変動によって，今日は有効とされたコントロールでも，翌日には無用の長物とならないとも限らない。リスクがもつこのような変動性という特質は，“判断尺度のゆらぎ”の問題を考えるときに，決定的に重要な意味をもつ。

さらに，“情報セキュリティ対策は成長させてゆくものである”という思考は，これまで必ずしも明示

的に提起されることはなかった。情報セキュリティ監査では，情報セキュリティ対策の適正水準ということを当初から想定しないか，あるいはある既製の基準をもって適正水準と見做すということが暗黙裡の前提とされていたことになる。既製の判断尺度を固定的に当てはめて，白か黒かしかない判断を求めることは，リスクに応じた情報セキュリティ対策の運用ということの本旨から考えて決して望ましいことではない。

このような意味において，本稿で取り上げた成熟度モデルは，リスク評価を前提としたときに生ずる監査上の“判断尺度のゆらぎ”という課題を克服するための一つの手掛りとなることは間違いない。