東京海上リスクコンサルティング（株）
第二事業部　主任研究員　八角 隆夫
E-mail: T.HAKKAKU@tokiomarine.co.jp

金融機関の情報セキュリティポリシー策定のための　アイディア・ヒント集（Ｖ１．０）

はじめに

情報セキュリティポリシーという概念は、もともと欧米における「COMMON CRITERIA」およびその前身である「ITSEC」や「TCSEC」から始まっていると考えられる。これらが誕生した１９８０年代後半当時はメインフレーム中心のいわば中央集権的情報システムの時代であったこともあり、情報セキュリティ　情報システムセキュリティという認識が主流であった。その後、クライアント・サーバー技術を利用した情報ネットワークシステムが普及し、エンドユーザーが直接情報を扱うようになってきたことはご承知の通りである。金融機関の情報の管理はさらに多様化しており、「情報」セキュリティをＩＴ部門だけで統括することは不可能になってきている。すなわち、情報セキュリティポリシー策定においては、紙メディアや口頭での情報も含めて金融機関が扱う全ての「情報」および「情報処理機能」を対象にしたリスク分析と対応策の検討を行い、これらを包括的に統制する経営方針を定める必要がある。これを推進するためにはトップを含めて全組織を挙げて取り組むことが求められる。情報セキュリティポリシー推進において重要なのは、合理的で身の丈にあった方針策定と実行可能な計画の立案である。経営課題全般を見渡せば、一方では４０１Ｋ年金・デビッドカード・インターネットバンキングおよび商品の多様化等の新しい業務展開に取り組む必要があり、他方ではリスク管理・内部統制などについて明確な経営方針の開示が求められている。さらに中期的には、流通業等他業界からの新規参入の激化が予想され、より一層の付加価値の創造とコストダウンを図ることも課題となっている。このため、総花的な「こうあるべき論」を廃し、各金融機関が主体的にリスクを判断した上での合理的に実行できる範囲の情報セキュリティを指向せざるを得ないことは自明である。また、方針を策定したら、経営レベルから実務担当者にいたるまで一致した考え方で取り組むことが求められる。

本資料はこうした推進上の論点、金融関係者の意見をまとめて、今後情報セキュリティを推進する方々への参考資料として作成した。

作成にあたっての方針は、次の通りである

１．金融機関が独自の情報セキュリティポリシーを策定するため、補助的にアイディアやヒントを提供することを目的とする。
２．原則として（財）金融情報システムセンターの手引書（本文中単に「手引書」と記している箇所は本手引書を指している）に準拠し、そこに示されている情報セキュリティポリシー策定の順序に従って、実務的な事項を中心にまとめていく。
３．内容としては、できる限り具体的な例を挙げるようにする。また、例外ケース、理想と現実的な技術との妥協、社内統制と対外公表や保証宣言との違い等、異なる考え方や対立する観点が存在しうる場合、なるべく両論を併記する。
４．今の時点で暫定的な結論さえ出せない問題については、その論点のみを提示する。

なお、本資料にまとめられているアイディアやヒントには、弊社がコンサルティングを通じて得たものに加え、（社）全国地方銀行協会や（社）全国信用金庫協会の方々をはじめ各金融機関関係者の方々とのディスカッションを通じて頂いたヒントやアドバイスが含まれている。また、これらの方々から本資料に対して色々な助言を頂いている。ここに改めてお礼を申しあげるとともに、今後ともさらなるご指導をお願い申しあげたい。

■　目次

Ⅰ．セキュリティポリシー策定の準備段階

＜概論＞

セキュリティポリシーの準備段階においては、自社（銀行・信金他）内の経営戦略の確認、コアとなるメンバーへの教育、おおよそのプロジェクトの進め方と着地点の検討など、プロジェクト全体のスケルトン作りが行われる。重要なのは、セキュリティポリシー策定プロジェクトのメンバー内で、自社の現時点および将来の「情報」・「情報システム」に関するリスクについてコンセンサスを持っておくことである。また、「自社の現状における情報セキュリティ水準」や「今後情報セキュリティに投下することが可能な経営資源（専担者のマン・アワー、予算、現場の事務手続き上の負荷等)」についても、ラフな認識あわせを行っておくことが望ましい。

情報セキュリティポリシーの策定とこれに基づいた具体的対策の推進は、短期的・刹那的なものでは無い。従って、弊社の考えであるが、専任担当者（役席・幹部でも可）無しに進めることはほぼ不可能と考えられる。

Ⅰ－１　情報セキュリティポリシー構築の事務局メンバー

今まで情報システム部門が担ってきたのに何を今更という反応も有るかも知れないが、元来金融機関は一種の情報処理を生業としてきたわけであり、その中で情報システム部門は効率的な情報処理を行うための仕組み作りを担当してきたわけである。この意味から言えば、セキュリティを確保するためには一般に情報処理の効率を下げる方向の検討が行われるので、情報システム部門には向かないのかも知れない。

現実論に戻って、情報セキュリティを検討するためには、顕在化しているリスク（事故事例等）や潜在的なリスクを洗い出す能力とともに、業務別の事務の流れと営業支店マネジメントの実情を熟知していることが要求される。また、自社や業界の経営上の課題や経営方針、さらに自社の強みと弱みについてもできる限り客観的に把握している人材が望まれる。また、監査役を最初から入れておいた方が良いとの意見もある。

これらから、一つのアイディアであるが、営業支店を数年以上経験した経営企画部門管理職をリーダーに、事務管理部門や情報システム部門から若手の補佐メンバーを１～２名つけて推進事務局を構成する、という方法が考えられる。また、組織的には経営企画（総合企画）部門に「リスク管理室」のような組織を創設し、リスク分野の一つとして情報セキュリティを担当するのがベストと考えられる。

Ⅰ－２　コアとなるメンバーが事前に勉強するテキスト等

日本の金融機関のサービス内容は世界的に見てもきわめて高いレベルにある。例えば米国の銀行の大部分は、支店網も少なく（州によっては支店の設置が許可されていない）メインの業務は小切手（パーソナル・チェック）の集計である。また、雇用、契約およびビジネススタイルが日本と欧米で異なることはあらためて触れるまでもない。従って、一般的には欧米の金融機関が作成した情報セキュリティポリシーが、日本の銀行に適合すると考えるのは無理がある。

こうした中で、海外の資料で参考になるものは、米国連邦準備銀行が１９９６年に作成した情報セキュリティ関連リスクに関する報告書、Common Criteria V2.1（ISO15408 と同じ内容＜すなわち製品等に対するセキュリティ与件を定めた技術的基準＞であり、次のサイトから無料でダウンロード可能である：http://csrc.ncsl.nist.gov/cc/)、ＢＳ７７９９および ISO/TR13569(Banking and related financial services Information security guideline)等と思われる。

日本のものでは、本資料でも参考にさせていただいた（財）金融情報システムセンターの「金融機関等におけるセキュリティポリシー策定のための手引書（平成１１年１月)」が筆頭に挙げられ、この１冊でほぼ要点が尽くされていると思われる。専門家によっては、システム監査に関する各種手引書やＪＩＳ Q 15001（個人情報の保護）を挙げる人もいることを付記しておきたい。

Ⅰ－3　セキュリティポリシーを策定する意味と目的

セキュリティポリシーの策定は対内部向けと対外部向けにそれぞれ次のような目的を持つ。

（1）対内部の目的

ＦＩＳＣ手引書に記されているように、情報セキュリティに関して内部的な意思統一を図ることが目的となる。すなわち、情報リスクの内容とその大きさを明らかにし、これに対してどのような組織でどのようにして安全を確保するかについての経営としての意思の表明であり、関連する規定を統制するいわゆる憲法にあたるものになる。これを定め、組織すべてに浸透し、マネジメントサイクルに組み込むことにより、より良い経営管理を実現することを狙いとするものである。

（2）対外部の目的

金融機関は、情報リスク対策が十分であること（もちろん他のリスクも同様であるが）を利害関係者に自ら証明する義務がある。これは従来からの「企業と株主の関係」では当然のことであるが、さらに預金者・取引先企業・他金融機関および金融監督庁に対しても同様の責務が存在すると考えられる。さらに金融機関の公共性を考慮すれば、社会全体に対しても責任が大きいと論ずる人も多い。経営者はこの義務、すなわち「アカウンタビリティ」を確保するために、情報リスク対策に関する基本理念としてセキュリティを明らかにし、企業活動を統制していくのである。

Ⅱ．基本方針の設定

＜概論＞

基本方針は、金融機関の自己責任での経営上の判断そのものである。従って、本来的に個々の金融機関の経営方針・経営上の判断に根拠を置くべき内容である。経営・幹部層および策定にあたる関係メンバーに、この点を再確認することが極めて重要である。

基本方針の策定においては、「（３．２．１）目的・目標の設定と明確化」→「（３．２．２）情報資産の洗い出し」→「（３．３．３）脅威の認識とリスクの評価」の順に検討するのは困難と見られ、むしろ 3.3.2→3.3.3→3.3.1 の順が適当であることは、手引書のＰ１２～Ｐ１４に書かれている通りである。

ただし、「自社における重要な情報資産は、リスクの大小にかかわらず保護する必要がある」という表現には、やや疑問がある。すなわち、情報セキュリティ対策の強化は、①その情報資産がさらされている脅威の大きさ（すなわち事故が発生した場合に銀行が失うものの大きさ）と②その情報資産に関する事故が発生する可能性（すなわち現状におけるセキュリティの強度の逆数に依存する関数）について、その積（①×②）が大きいものから優先して取り組んでいくのが合理的といえるのではないだろうか。

情報技術の進歩とそれに呼応したビジネス環境の変化が急激であることから、情報セキュリティポリシー策定作業にあたるメンバーは、２～３年後の自行のビジネス形態や情報ネットワーク技術の姿を思い描きながら検討を進める必要がある。また、基本方針の中には、ビジネスの変化や技術の進歩に応じて、自社の安全対策基準を見直すための組織と仕組みを盛り込んでおくことも重要である。

Ⅱ－1　情報セキュリティポリシーを検討する範囲

理想的には金融機関の保有する全情報および全情報ネットワークシステム機能について、一貫した理念の情報セキュリティポリシーを構築し、個々に必要なレベルに応じた対策が施されるべきであろう。しかしながら現実には、膨大な種類の業務・手続きおよび情報資産（帳票、電子的データ等）を相手にすることになり、いつまでたってもプロジェクトが収束しない懸念が大きい。さらに、

単年度で投下可能な経営資源（予算、マン・アワー）にも自ずと限界がある。このため、多くの金融機関においては、情報セキュリティポリシーの策定と体制立ち上げにあたって、当初検討する分野を限定して推進することとなろう。

選定にあたっては、取引量のボリューム、顧客との接点が多い業務、事務処理　パターンや例外処理規定が少ない業務、新規業務（サービス商品）等がポイントになると思われる。

いずれにしても、限られたゾーンの中で一連の分析～規定づくりや教育までを完結させれば、その後の横への展開もスムーズに流れると見られる。「手引書」の 2.3.2 項（Ｐ１３）をご参照願いたい。

金融機関によっては、一部の情報資産から始めることに抵抗感があるかも知れないが、情報セキュリティポリシー（すなわち情報資産のセキュリティに関する独自の経営方針）がそもそも任意のものであることを思い出していただきたい。また、例えば基本方針の附則として、当初の検討範囲とその後の展開計画を加える方法もあることを付言しておきたい。

Ⅱ－２　目標・目的と現実のギャップへの対処

ハイレベルな理念から現実的な施策にブレークダウンを行う際、必ず理想と現実のギャップに行き当たるはずである。例えば「お客様のプライバシーの保護については最重要課題として取り組み・・・・」という理念があったとする。渉外係の業務に着目すれば、彼らは①渉外手帳、②お客様に関する事務書類、③コンピュータアウトプット類、④携帯用コンピュータ内のデータ等色々な形態の顧客プライバシー情報を持ち歩いている。手帳や書類について毎日員数管理を行い、さらにコンピュータアウトプット類はピンク色の紙に出力して１枚１枚持ち出しと廃棄の管理を行ったとしても、携帯用コンピュータ内のデータ（例えば顧客のファイナンシャルプランニングのためのＥＸＣＥＬデータ）は保護が困難である。もしＰＣごと盗まれれば、たとえパスワードが掛かっていたとしてもハードディスクごとコピーされて、そのうちに解読されてしまう。これらに対してパーフェクトなセキュリティを実現するためには、多大な労力とコストがかかることになる。

目標・目的と現実とのギャップには次のような２つの類型がある。

＜業務手続き上のギャップ＞

業務上必須な手続きについて、その手続きが法令や取引慣行に縛られているためにセキュリティ対策上の抜本的改善ができない場合がある。例えば申込書類や総合通帳等は、渉外係が自筆署名や印鑑捺印を求めるために持ち歩く場合があるが、これを全廃することは困難である。しかし、人が書類を持ち歩く以上、紛失するリスクは皆無とは言えない。また、申込み書類を郵送する場合、書留郵便を利用すると追加料金が発生するが、この費用は直接または間接的にお客様が負担することになる。ケースバイケースではあるが、この費用の負担を納得していただけるお客様ばかりとは言い切れないのが現実である。

＜技術ギャップ＞

現在の技術では、セキュリティを確保するためには技術が未成熟であったり、その実現コストが極めて高価につく場合である。

前述の渉外係の例でいえば、携帯用コンピュータで扱うデータをすべて高いセキュリティを持つメディア（例えば、ＰＣカード（名刺大のカード）内にセキュリティ制御用プロセッサを持ち、不正なアクセスを許さない仕組み等）に持てばある程度解決するかも知れない。しかし、現状ではこのような仕組みはきわめて高価につく。

これらのようなケースでは、将来実現すべき情報セキュリティ水準と現在暫定的に運用する情報セキュリティ手続きとを分けて考えるのが実践的である。

Ⅱ－３　セキュリティポリシー規定と業務目的が競合した場合の救済

ＦＩＳＣ手引書の７７ページ（【例２】顧客対応の迅速性とデータ開示のセキュリティの競合の例）のように、業務の本来目的と情報セキュリティ規定が競合することがあり得る。こうしたケースに合理的に対応するためには、銀行のセキュリティポリシーおよび情報セキュリティ関連諸規定

に緊急時の例外的手続きが明示的に規定され、これを実現する仕組みが業務面においても情報システム面においても整備されていることが必要となる。

具体的にいえば、各部門の情報管理責任者（すなわち例外を許可する権限者）の不在代行者の規定や情報管理責任者同士の合議、さらに、ＣＩＯ等による緊急対応宣言の発動等、危機管理の観点を踏まえて事前に規定しておくことが必要である。また、技術的には、緊急対応用のマスターキーのような仕組みをしかるべき管理者が保管して必要な場面で発動する、前日のバックアップデータを限定的に利用可能とする、等の手法で解決しておくことが求められる。また、こうした緊急対応を行った事実を記録し、情報セキュリティの総括管理者に報告し、さらに必要に応じて規定の見直しを行うことも重要である。

Ⅱ－４　　リスクの分析・評価方法

基本方針の大前提となる、「万一情報セキュリティが破れた場合に銀行が被る損害リスク」の分析・評価に関する方法論は、ＢＳ７７９９規格やＦＩＳＣ手引書には載っていない。また、世の中に一般的に認知された方法も未だ無いようである。弊社では、ラフな分析と重要リスクの絞り込みにおいて、地銀協で１９９９年５月の「西暦２０００年問題に関する打ち合わせ会」にてご紹介した、縦軸にリスクが顕在化した場合の損害ランク取り、横軸に発生可能性を取って整理する（いずれもタスクフォースメンバーの意見を集約）方法＊を推奨している。

＊縦軸にリスク顕在化時の損害の大きさ、横軸に発生可能性をとる。＜参考２＞を参照願う。

ここで注意しなければならないのは、損害は直接的なもの（例えば利益、経費、賠償責任等）よりも間接的なもの（例えば銀行の信用低下、戦略推進上のスピード低下要因、銀行員の士気の低下等）の方が大きくなる場合が少なくないことである。これはどうやっても単純な説明はできない「経営レベル」の判断となりそうである。しかし、この点を無視して評価を進めるわけにいかないのも事実である。一つの解決策として、銀行の複数の経営層メンバーに参画してもらい、億円単位（千万円単位ほか）で荒く評価してもらうことも考えられる。

次に絞り込まれた重要なリスク項目に関する詳細分析を行う。銀行検査でのきちんとした説明の必要性を視野入れて考えれば、ここにはかなりの労力を注ぎ込むことが求められる。ここに至る過程で、「重要なリスクシナリオ」とされる項目が数種類から多くとも十数種類程度にまで絞り込まれているはずなので、それぞれについてシナリオを作成して時系列を追った損害の洗い出しと金額評価を行うことをお勧めしたい。もちろん、前述の「間接的な損害」を反映することも必要となる。

Ⅲ. 自社の安全対策基準の策定

＜概論＞

このフェーズでは、目標とする情報セキュリティ対策のレベルを明確化するのが最大のテーマである。

前節で述べたように、情報資産毎にリスクが顕在化した場合の脅威の大きさが違うし、事故の発生可能性も異なる。例えば「クラスA」、「クラスB」・・　・等のようにある程度色分けしてあれば、大括りで原則的対応条件を決めることが可能となる。さらに、個々の業務特有の事情での例外や、必要に応じて、情報システム上での技術的手法についても規定することになる。

Ⅲ－１　自社の安全対策基準は固定的なものなのか

自社の安全対策基準（すなわち情報の重要度に応じたセキュリティ対策内容に関する目安・ガイドライン）は、実務的には最も重要な規定となる。

例えば、渉外行員が持つ顧客リスト（住所・氏名・家族構成・資産・事業内容・当行との取引概

要等の情報が含まれる）があったとして、これにについて、①毎日棚卸し確認（または廃棄）するのか、②役席の承認手続きがあれば一定期間棚卸しせずに、個々の渉外係の責任で利用可能なのか、③個々の渉外係に取り扱いの注意を喚起し、万一外部に漏出した場合の罰則規定を定めるだけなのか、等、色々な対応方法の選択肢が考え得る。これらのうちどれを選択するかにより、日常業務の手続きに大きな影響を及ぼすことになる。

技術的な支援が得られず、紙ベースで管理している状況では①はほとんど現実にそぐわない。（軍などでの最高度の機密書類の管理においては実行しているかも知れない）②ないしは③を選択することであろう。しかし、渉外係に携帯型パソコンを持たすようになれば、状況は一変する。すなわち①のように毎日棚卸して不要データを持たせないようなルールであっても実行可能となる。

こうした事情から、自社の安全対策基準は、できる限り頻繁に見直していくことが求められる（現実的には年に１～２回か）。すなわち、"BEST EFFORT"を追求しながらも、現実的に実行できない安全対策基準とならないようにコントロールしていくことが重要なのである。→Ⅲ－２項参照

このような基準・規定の微妙なコントロールにおいては客観性の確保が困難となる可能性もあるので、できる限り外部の第三者によるアドバイス（コンサルティング）を得ることをお勧めする。

Ⅲ－２　技術の変化の継続的な評価とフィードバック

情報ネットワーク技術の急速な進歩は、これまでと同様、今後１０年以上続くと見られる。このため、ほんの半年～１年前には「技術的・コスト的に困難」であったことも簡単に解決可能となることが少なくない。企業の合理的な判断において、社員のロードを削減して情報ネットワーク技術で解決することは、予算が許す限り推進していくべきである。また、お客様に提供できるセキュリティ水準が向上することは、間接的ではあるが、金融機関の競争力強化に寄与すると考えられる。

重要なのは、見直し頻度である。少なくとも年に１回、できれば年に２回程度技術動向をチェックしていくことが望まれる。この結果は、少なくともＩＴ担当役員（ＣＩＯ）や情報セキュリティ委員会等に報告され、できれば役員会にも報告されることが望まれる。→Ⅳ．レビュー・承認参照

Ⅲ－３　自行のビジネスリスクの変化に対するフォローアップ

前項では、情報ネットワーク技術の変化の側面を論じたが、逆にリスクがどうなっているかをフォローしておくことが重要であることも論を待たない。

社会・経済的な環境変化、自行のビジネス領域の変化、コアとなるビジネス手法の変更等々がリスク構造そのものを変化させる可能性は高い。これらの変化を踏まえて既存の安全対策基準に手を入れていくことは、予想外のハードワークとなるかも知れない。しかしながら、いくつかの解決策はある。

一つは、外部の事故例や行内の「ヒヤリ・ハット」事例や懸念される事故等を調査・収集する方法である。ハインリッヒの法則によれば、一つの損害発生事故の背景には３０倍の以上の損害を伴わないレベルの事故が存在する、ということになる。弊社コンサルティングでの経験においても、複数の部門が重要性を指摘しているリスクシナリオの周辺には、重大な問題点が潜んでいる場合が多く、この方法は実践的かつ効率的と見られる。ただ、こうした「一種の警鐘」にあたる情報を「解決策がない、または、解決が困難（予算・人員 etc.）」という理由で（経営層に報告しないまま）握りつぶさないような配慮が望まれる。

今一つは、セキュリティーポリシー策定時のリスク評価プロセスを定期的に（例えば２～３年に一度）行う方法である。実施にロードがかかることを懸念する意見もあるかも知れないが、重要業務に関しては、本質的にこれが最良の方法と思われる。実施上の工夫としては、行内の教育カリキュラムにおける新任役席者や異動者に対する「情報セキュリティ」教育の一環として、業務上のリスク評価の演習を取り上げる方法もある。この場合は、受講者に対し「ここでの議論は自行の情報セキュリティポリシーにフィードバックされる」ことを宣言し、十分な討議材料を与えると共に自由な議論が可能な環境を整えれば、予想以上の成果が期待できる。

なお、新規ビジネスへの参入や基幹情報処理センターのアウトソーシング等、ビジネスプロセスの大幅な変化がある場合は、リスク評価プロセスを最初からやり直す必要があることは、いうまでもない。

Ⅲ－４　情報ネットワークシステムに要求するセキュリティ水準

自社の安全対策基準で情報ネットワークシステムに要求するセキュリティ水準をどのあたりに設定するかは、かなり難しい問題である。

参照するガイドラインとしては、建物や情報通信機器等のハードウェアや施設の運用はＦＩＳＣ「金融機関等コンピュータシステムの安全対策基準」、ソフトウェア等の製品の「評価保証レベル（ＥＡＬ：Evaluation Assurance Level）」という規定がＩＳＯ１５４０８にあり、既に一部のソフトウェア・ハードウェア製品における認証が始まっている。（「参考１」をご参照願いたい）

これらのガイドラインはいろいろな要素を個々に規定しているが、トータルなシステムとしての安全性・信頼性および可用性を十分に定義しているとはいえない点にも留意されたい。

Ⅲ－５　ソフトウェア・ハードウェア製品の選定

システム製品（ソフトウェア・ハードウェア）の採用について、ここで触れるのは不適切という意見があるかも知れない。しかし、情報セキュリティの推進において、コアとなるシステム製品の出来不出来が大きな要因をしめることも事実である。また、今後、金融機関の情報セキュリティ面での信頼性の尺度として、ある一定の認証（例えばＩＳＯやＪＩＳ）がキーポイントとなっていく可能性も否定しきれない。

これらのことから、以下にいくつかのソフトウェア・ハードウェア製品の選定のためのヒントをご紹介する。

・標準化、認証水準への配慮
・中長期的視点に立ったハード・ソフトおよびセキュリティ製品選定
・カスタマイズコスト、メンテナンスコストを重視
・教育の問題、現場での使い方のわかりやすさ
・エンドユーザーコンピューティングと基幹システムの接点・統一性

Ⅲ－６　アウトソーシング先に求める安全対策水準

安全には、可用性・信頼性・同一性・防犯・耐攻撃性および規定や法令等に対する準拠性等、色々な概念が含まれている。またさらに、日常業務規定外のオペレーションを求める場合の安全対策上のルールや安全性向上投資の際の意思決定と費用負担のルールまで拡がる。これらについての公的ガイドラインや社会通念は必ずしも形成されていないが、現時点で気づくいくつかの点について言及したい。

まず、可用性・信頼性さらにオンラインシステムの応答時間や異常から復旧時間などについて、一つの方法として「ＳＬＡ（Service Level Agreement）」導入が考えられる。例えば一定以上のＭＴＢＦ（故障と故障の間隔）、稼働率等にインセンティブを払うかわりにトラブルが一定以上になるとペナルティを取る仕組みを設ければ、相互の業務責任を明確にし、また安全な状態を達成する動機付けが生まれる。さらには、トラブルを「なあなあ」で済ませない土壌づくりにも役立つと考えられる。

次に同一性（データとオペレーションの正当性）については、監査システムの整備（すなわち監査用の独立した検証システムの構築）に期待せざるを得ない。こうしたシステム構築における業務的・技術的および運用的な困難さについては多くの読者が経験されていると思われるが、世の中全体の流れとしては被監査性や業務の正当性の確保の重要性が認識される方向にあり、アウトソーシングをトリガーとして整備を進める銀行が増えていくと見られる。

３番目にいわゆる犯罪が挙げられる。情報ネットワークシステムに対する攻撃およびその他の「情報ネットワークシステム攻撃以外の手段」による情報の盗取・不正流用および改竄等広範囲のリスクに対応し、かつ自らその安全性を証明していくことも求められる。最近の露見した、多数の官公庁や有名企業のシステムのプログラムが犯罪集団関係者によって開発されていたという事件の教訓から、開発を請け負う企業およびその納品物への正当性監査のニーズが高まっている。必ずしも我が国の企業風土に沿わない側面もあるが、関係者の定期的身元調査、開発室出入りにおける荷物検査、抜き取りサンプリングによるプログラムの徹底的検査等を行わなければ安全性が保証しき

れないという議論もある。

なお、上述したいくつかの論点を含め、通産省「情報処理サービス業電子計算機システム安全対策実施事業所認定制度」、ＩＳＯ９０００シリーズ、ＪＩＳＱ１５００１（プライバシーマーク制度）等の認証を得ているかどうかは、一定の目安となろう。しかしながら、金融ビジネス独特のセキュリティ要求も多いので、これらの認証取得が十分条件とはいえない。

Ⅳ．レビュー・承認

＜概論＞

レビュー・承認のフェーズにおいては、内容の妥当性を最終的に検討・議論するとともに、どうしてその結論に至ったかを経営層が理解し、納得することが重要である。経営層メンバーは、単に金融機関の情報セキュリティの責任者であるのみならず、対外的なスポークスマン役や内部での推進のリーダーシップを発揮することも求められる。このため、従来のように「細かいことは担当部が・・・」とはいっておられない立場にある。すなわち、情報セキュリティ上の脅威の分析に関する妥当性、情報セキュリティ施策の有効性、営業部店の負担、お客様や取引先企業の立場に立った評価等、多角的な視点で理解し納得しておくことが必要となる。

Ⅳ－１　　レビューに参画する経営層メンバーとその役割

概論で述べたように、経営者は情報セキュリティポリシーの策定に関連する諸事実および判断根拠等を十分に理解し、納得しておくことが求められる。最終レビューメンバーとしては、少なくともトップ（頭取・理事長）、ＣＩＯ、事務担当役員および監査役の出席を求めることをお勧めする。日程調整上これらすべてのメンバーが集まれないケースも考えられるが、その場合は役員から役員に伝える（もちろん事務局担当の同席は問題ないと思われる）方法がベストである。経営層メンバーは、日常の業務運営や企画・方針検討等あらゆる局面で情報セキュリティの視点からの発言・指示を行うことになる。従って、「当行の情報セキュリティ」について、その背景・現状・理念と方針・具体的な施策および諸規定について、クリアに説明できるようになっておくことが望まれる。

また、対外的には施策を話すだけではなく、「（世間や専門家が重要だという情報セキュリティ対策等について）どうして当行がその施策を採用していないか」についても明快に答えないとならない。例えば、リスク分析の結果どうであるか、お客様の利便性の観点からどうであるか、コスト問題はどうか、技術が成熟しているか等の論拠を挙げて説明することになろう。

以下にレビューを進める上でのポイントをご紹介する。

①総花的議論・完全主義的議論を排除し、比較優位の原則に基づく合理的論拠を確認する。
②営業上の施策（情報セキュリティの対象の業務）そのもののメリット・デメリットにも切り込む。
③営業上、実務遂行上のセキュリティ実施のための負担と潜在コストを熟慮する。
④事故が起きた場合を想定し、企業としてどのような責任が追及されるかも考えてみる。

Ⅳ－２　　承認手続き

「情報セキュリティポリシーの策定」は、金融機関にとって経営上の重要事項にあたるので、役員会への付議と承認が必要と思われる。また、承認手続きとはやや趣旨が違うが、効果的に推進するという観点からは、社内への周知（社内広報）やインターネットＷＥＢ掲載等による対外広報も重要である。

これらの諸施策の推進状況のフォローと経営環境の変化への対応のためには、「情報セキュリティ委員会」等の専門機関を設置して１回／２ヶ月程度のフォローアップを行うことが望まれる。

最終的には、営業報告書・有価証券報告書等において実施状況を報告し、株主総会等の最高議決機関における承認を求めることになる。

Ｖ．その他（セキュリティ水準の測定・監査およびその他の事項）

＜概論＞

以下は、Ｉ～IVの範疇に含まれない事項である。

Ｖ－１　　事前のセキュリティ水準の測定

情報セキュリティ・ポリシー策定に先立って自行のセキュリティ水準（特に弱点）を把握しておくことは、プロジェクト推進上の重要要素である。従来組織体制において、ＩＴ部門の役割が「何も問題が起こらないことを保証するもの（あるいは何も無くて当たり前）」と認識されている銀行においては、非常につらい経験となるであろう。

主にＩＴ分野をカバーする国際規格ＩＳＯ／ＴＲ１３５６９「金融関連サービスにおける情報セキュリティガイドライン（現時点ではテクニカルレポートのレベルであるため、国際規格として承認されたものではない）」では、いわゆる「レッド・チーム（疑似ハッキングによる弱点の解析が任務）」を外部委託する際の契約上の要点も記述されている。海外で実施していることをそのまま日本で受け入れるかどうかには議論の余地があるが、外部専門家による弱点解析の実施には次のようなメリットがあり、検討に値する。

（１） 少なくとも現時点での弱点をターゲットに対策を講じることができる。
（２） 経営層が自行のリスクを把握できる。→知らなかったではすまされない問題である。
（３）（ＩＴ部門や事務統括部門にとっては抵抗感があるかも知れないが）建前ではできている（規則にある）ことで、現実にはできていないことがあぶり出される。

これにより、より現実的なアプローチを選択することが可能となる。また、こうした弱点の検出を行った後に、個々の問題点を解決するために、
①そもそも技術的な対策（事故防止対策）の完成度どの程度か、
②予算がどのくらい必要か、
③ＩＴ部門や現場にとって対策のためにどの程度の人的・時間的な負荷がかかるか、

等を明らかにしておくことが望まれる。→これをやらないと、ＩＴ部門が一方的に苦しめられるだけで、問題解決につながらない恐れがある。

次に、ＩＴ周辺およびｎｏｎ－ＩＴ分野に焦点をあてた、現場や本店部門の調査であるが、次のような考え方でチェックを進めていくこととなろう。

（１）既存の規定や手順書を逸脱していることはないか。もしあるとすれば、どのような理由かを調べる。
①既存の規定が業務実態に合っていない。
②各現場責任者や担当者の情報セキュリティに対する認識・理解が不十分。このため必要な手順が省略された。
③情報セキュリティ以外の分野でも問題があり、当該職場全体の士気や業務統制に問題がある。
等々
（２）規定は無いが、日頃から情報セキュリティ上の問題点を感じている事実についてヒアリングする。
（３）日常業務において、情報セキュリティを確保するために、どのようなことを行い、それにどの程度のマン・アワーを割いているかについてヒアリングする。

これらから、情報セキュリティに関する実態・既存規定の問題点・行員の意識および実務上の負荷などを把握する。この調査は、日常の業務監査とは目的が違うので、各部門の長にはその旨を理解してもらう必要がある。

Ｖ－２　　部門・営業店のセキュリティ担当者の任命と組織化

すでにこのような役割のメンバーを任命している金融機関が多いものと考えられる。名称には、「情報化推進役」、「システム化推進委員」等バラエティーがあると思われる。

情報セキュリティポリシー推進においては、これらの方々に、

①情報資産と脅威の洗い出しにおける部門キーパーソン役

②部門の情報管理上の責任者（規定遵守のための教育と指示、例外の承認等を担当）としての役割

③部門としての要望や意見のとりまとめ役

等の役割を果たしてもらう必要がある。従って、適性としては、情報や情報ネットワークシステムをよく知っていることも重要ではあるが、部店内での指導力がさらに重要となる。このため、部内のトップ～№３の人材を充てることが望まれる。

ただし、対象とする範囲によっては、ＰＣやネットワークの知識の高いメンバーが必要になることもある。例えば、部門のエンドユーザーコンピューティングやファームバンキングを対象に選定した場合が挙げられる。

Ｖ－３　　セキュリティ・ポリシー策定後の業務監査

前項では、事前のセキュリティ水準測定のための調査の方法の例を述べたが、セキュリティ・ポリシー（基本方針と安全対策基準）策定後は、業務監査によってフォローしていくこととなる。

「調査」と「監査」の違いは改めて述べるまでもないが、監査では監査人の独立性（ビジネス部門との相互牽制的な権能）を確保する必要がある。従って、前項で述べたような改善のための実態把握を直接行うことはできない。すなわち、監査の一義的な目的は、規定通りに実務が遂行されているかを調べ、これを経営層や株主に報告することである。

しかしながら、慎重に監査人の独立性に配慮しつつ、監査人の眼を通じて情報セキュリティの実態を知り、フィードバックへの材料とすることは可能と思われる。この問題は、システム監査人の中でも色々と議論が行われているテーマである。各銀行の業務管理の実態や監査担当者の力量等を考慮しつつ、判断されたい。

Ｖ－４　　検査・監査におけるアウトソーシング先との関係

情報セキュリティ施策を推進する上で、アウトソーシング先が果たすべき主な役割は、次のようなものとなる。

（１）金融機関にとっての脅威（ＩＴリスク）を常にモニタリングし、弱点を明らかにするとともに適切な対応策をフィードバックする機能が必要となる。

（２）（金融監督庁の検査マニュアルの考え方においても明らかなように）金融機関は自らの安全性、すなわち情報セキュリティ施策の適切さを対外的に証明してみせる義務がある。
→Ｉ－３参照
特に情報技術の面で、アウトソーシング先の積極的な協力と関与が必要であり、これを要求することが必要となる。

（３）情報セキュリティが破れたとき、災害・障害等で金融機関の情報システムに問題が発生した場合等にリスクを最小限に抑制するためには、アウトソーシング先に適切な危機管理計画がありこれが当該金融機関の危機管理計画と整合していることが必要である。これを監査・検査で明らかにするためには、危機管理計画や規定の整備（特に変化があった場合のメンテナンスが重要）に加え、教育訓練の履歴を記録しておくことが必要である。

（４）アウトソーシング先自身が、公的な認証取得や外部監査を積極的に受け、自らのマネジメントの正当性と情報セキュリティの高さを立証していく方針であることが望まれる。このことは、金融機関の経営者に対して強いアカウンタビリティを提供する。

Ｖ－５　　行内でのＰＲと教育

情報セキュリティポリシーは、理念・宣言、規定、（予防対策・危機管理の）実施計画、監査とフォローアップの体制を定めただけでは不十分である。すなわち行内で継続的にＰＲや教育を実施し、常に行員や協力会社社員の意識を喚起しておくことにより、日頃の規定遵守を徹底するとともに、規定に書かれていない事項（事態）においても理念に照らして判断が出来る人材を育成しておくことが重要である。

具体的には次のような方法が考えられる。

＜媒体＞

- 行内教育
- 行内報、行内放送（ビデオニュース等）
- 外部マスコミ等への幹部層の発言
- 行内レターやマニュアル
- 既存マニュアルへの盛り込み
- 個人用手控えの配布（方針理念と基本事項）
- 情報システム利用時の警告やＨＥＬＰ文章

＜内容＞

- 基本理念、対外公表宣言、規定、事務ガイドライン等との対比
- 自行の情報セキュリティポリシーの概要・解説
- 「こんな時どうする」Ｑ＆Ａ集、お客様への応酬話法集
- 事故例、トラブル例の紹介
- 各種標準契約書文言とその解説
- 情報セキュリティ自習教材（世の中に銀行検定テキストのようなものがあれば良いが、現状では自家製となる）

Ｖ－６　対外的な広報・宣言における表現方法

考え方の整理としてまず重要なのは、

「自行で事故（事件）が起こることを前提とするか事故が起こらないことを前提とするかをはっきりさせること」

である。

事故が起きる可能性があることを前提にすれば、

①平時にできる限り金融機関が実践している情報セキュリティのための方針と取り組み概要を情報開示しておく（もちろん誇張や遠慮なく正確に）

②前項にもかかわらず、情報セキュリティが破れて事故に発展するリスクを１００％否定することはできない旨を伝える。

③従って、当行としては今後も情報セキュリティ水準を高める努力を続けていくことを宣言する。さらに顧客に対して、情報セキュリティ確保のための呼びかけ（身近な情報の管理：「暗証番号をお聞きすることは無い」等、ご不審に思われたことについてのご照会窓口）を行う。

等の内容となると考えられる。

一方、事故が起こらないことを前提とすれば、

①他の金融機関と横並び内容（すなわち目立たない）の情報セキュリティのための基本方針や担当組織を開示する

②顧客に対して、情報セキュリティ確保のための呼びかけ（身近な情報の管理：「暗証番号をお聞きすることは無い」等、ご不審に思われたことについてのご照会窓口）を行う。というような内容となる。

弊社としては、危機管理と経営の透明性の観点から前者の対応をお勧めする。

一般論として、「○○が無い」ことを証明することは「○○が有る」ことを証明するのに比べて著しく困難である。例えば、銀行の取引履歴らしき情報が世間に漏れた事件が発生した場合、事実は銀行にほとんど責任が無かったとしても、その潔白を証明することは著しく困難と思われる。さらに、銀行に責任があった場合には、事件が起こってから「当行では日頃からこれだけ情報セ

キュリティ対策に注力して・・・」と言っても、世間やマスコミはもはや聞いてくれない。すなわち、世間に公表していない内部資料を以て、賠償責任を巡る裁判で有利になったとしても、その金融機関は既に多くのものを失っているのである。

Ｖ－７　　ネットワークバンキングとコンビニＡＴＭ問題

これらの問題に関しては、関係者の間でリスクの内容や対応策の評価が未だ定まっていないと見られる。以下にいくつかの論点を紹介する。

（１）ネットワークバンキング

・通信キャリアやインターネットプロバイダ等の安全性に関する格付け問題。
・利用者と金融機関との責任分界点の問題。さらに、例えば「着信確認」、「内容証明」等広い意味での認証問題の解決手段をどうするか。
・ネットワークバンキング等で犯罪による被害を受けた利用者の救済方法。
・従来の暗証番号やパスワード等の弱いセキュリティレベルの補強。業界全体としてのＩＣカードやバイオメトリックスの導入問題。

（２）コンビニＡＴＭ

・設置ＡＴＭの物理的セキュリティ（防犯）の強化。
　→例えば取引ＬＯＧの入ったハードディスクごと盗まれたら・・・
・異常監視（コンビニ従業員や保守員の不正行為も含む）体制の強化。
・情報セキュリティに関する責任体制の見直し。

以上

＜参考１＞ＩＳＯ１５４０８におけるＥＡＬ問題

ＩＳＯ１５４０８に準拠し、既に一部のソフトウェア・ハードウェア製品における品質保証レベル認証が始まっている。しかしながら後述するように、現存する製品のほとんどは、一部の人々が金融業が選択することを推奨するような、ＥＡＬ５（７段階中）を満たせない（唯一モンデックス社のデジタル署名ソフトがＥＡＬ７相当といわれている）実状にある。少なくとも現時点（２０００年春）で、新規導入のシステム（例えばＯＳ、ミドルウェア、パッケージソフト等）にＥＡＬ５以上を要求することはほとんど不可能であり、可能であったとしても巨額の予算が必要となる。（注参照）従って、弊社では、今の時点でＥＡＬについて自社の安全対策基準には明記すべきではなく、ややあいまいとなるが、文章で自行が要求する技術的対策レベルを表現するのが適切と考えている。

注）現時点で保証レベル（ＥＡＬ）に応じた詳細な認証規定が公表されているのは、ＥＡＬ４以下に限られている。ＥＡＬ５～７は、現時点では「ＥＡＬ４に開発・テスト・メンテナンス時のセキュリティ与件を加えたもの」として規定されているが、弊社で知る限り、認証機関向けのドキュメントにおける定義の曖昧性が大きいように感じられる。今後も流動的要素が大きく、実際の認証作業がどうなるかも不透明と考えざるを得ない。このため、当局および各省庁の動き・発言（例えば「金融機関はＥＡＬ５以上」等の発言）を注視し、必要であれば堂々と反論（検査においては、今後試行される「意見申出制度等」）していくことをお勧めする。

＜参考２＞評価ミーティングにおけるリスクの整理の例