（仮訳）

電子バンキングにおけるリスク管理の原則

バーゼル銀行監督委員会

バーゼル

2001 年 5 月

目　　次

バーゼル銀行監督委員会

電子バンキング･グループの構成

議長：Mr John Hawke, Jr、米国通貨監督庁長官、ワシントン DC

メンバー：

Commission Bancaire et Financière, Belgium	Mr Jos Meuleman Mr Koen Algoet
Office of the Superintendent of Financial Institutions, Canada	Ms Judy Cameron Mr Brad Sullivan
Commission Bancaire, France	Mr Alain Duchâteau Mr Jerôme Deslandes
Bundesaufsichtsamt für das Kreditwesen, Germany	Mr Stefan Czekay
Deutsche Bundesbank, Germany	Ms Magdalene Heid Mr Andi Kloefer
Banca d'Italia, Italy	Mr Filippo Siracusano
金融庁、日本	小島 一夫 中川 彩子
日本銀行、日本	森　 俊彦 桑原 啓彰 鈴木 知子
Commission de Surveillance du Secteur Financier, Luxemburg	Mr David Hagen Mr Claude Bernard
De Nederlandsche Bank N.V., The Netherlands	Mr Erik Smid

Banco de España, Spain	Ms Maria Jesús Neito
Financial Supervisory Authority, Sweden	Mr Jan Hedqvist
Federal Banking Commission, Switzerland	Mr Daniel Schmid
Financial Services Authority, United Kingdom	Mr Jeremy Quick Ms Katy Martin
Office of the Comptroller of the Currency (OCC), United States	Mr Hugh Kelly Mr Clifford Wilke
Board of Governors of the Federal Reserve System, United States	Ms Heidi Richards Mr Jeff Marquardt
Federal Deposit Insurance Corporation, United States	Ms Sandra Thomson Mr John Carter
Federal Reserve Bank of New York, United States	Mr George Juncker Ms Barbara Yelcich Mr Christopher Calabia Mr Thomas Whitford
Secretariat, Basel Committee on Banking Supervision, Bank for International Settlements	Mr J-P Svoronos

オブザーバー：

Australian Prudential Regulation Authority	Mr Graham Johnson
European Central Bank	Mr Michael Olsen
Hong Kong Monetary Authority	Mr Brian Lee
Monetary Authority of Singapore	Mr Enoch Ch’ng

電子バンキングにおけるリスク管理の原則

エグゼクティブ・サマリー

技術革新の継続、および既存の銀行や新規参入者の間の競争によって、リテールおよびホールセールの顧客が、電子的デリバリー・チャンネル、すなわちこれらを総称した電子バンキングを通じてアクセスしデリバリーを受けることのできる銀行商品・サービスの範囲は大きく広がった。しかし、電子バンキングの急速な発展はリスクと利益の双方を伴う。

バーゼル銀行監督委員会は、銀行が、電子バンキング・サービスの基本的な特性や課題に照らして、慎重にそれらのリスクを認識し、対処・管理することを期待する。電子バンキングの基本的な特性には、テクノロジーや顧客サービスの革新がもたらす変化の予期せぬスピード、電子的なオープン・ネットワークの遍在性およびグローバル性、電子バンキング・アプリケーションと既存のコンピューター・システムとの接続、および、所要の情報テクノロジーを提供する第三者に対する銀行の依存度の高まりが含まれる。バーゼル委員会は、これらの特性によって本質的に新しいリスクが生じることはないが、銀行業務に伴う伝統的なリスクの一部が拡大・変化し、銀行業務の総合的なリスク・プロファイルに影響が及ぶと考える。特に問題となるリスクは、ストラテジック・リスク、オペレーショナル・リスク、リーガル・リスクおよびレピュテーショナル・リスクである。

バーゼル委員会は、上記の結論に基づき、既存のリスク管理原則は電子バンキング業務にも適用され得るものの、電子バンキング業務の特性がもたらすリスク管理上の特殊な課題に対応するために改良・工夫され、場合によっては拡大されなければならないと考える。このためバーゼル委員会は、取締役会および上級管理職が銀行の既存のリスク管理方針・手順について、既に実施中ないし計画中の電子バンキング業務を対象とするように見直し、必要に応じて手直しすることが必要であると考える。バーゼル委員会はまた、電子バンキングのアプリケーションを既存のシステムに接続するということは、銀行が行う全ての銀行業務を対象とする包括的なリスク管理アプローチが必要となることを意味すると考える。

こうした電子バンキング業務に伴うリスクへの対応を促すため、バーゼル委員会は、銀行がリスクの監視に関する既存の方針とプロセスを拡大し、電子バンキング業務をも取り込むための助けとして、１４の「電子バンキングにおけるリスク管理の原則」を策定した。

これらの「リスク管理の原則」は、絶対的な規則として提示されるものでもなければ、「ベスト・プラクティス」ですらない。バーゼル委員会は、電子バンキングの分野においてリスク管理上の細部にわたる規則を定めることには弊害が伴い得ると考えている。このことは、テクノロジーや顧客サービスの革新がもたらす変化のスピードが速いため、そうした規則は短期間のうちに陳腐化する可能性が高いということに照らしても明らかである。従ってバーゼル委員会は、電子バンキング業務の安全性と健全性を促進すべく、監督上の観点から期待していること、およびガイダンスを「リスク管理の原則」として記述する一方、この分野における変化のスピード等を考慮に入れて、適用に際して所要の柔軟性を残しておくことを選択した。更にバーゼル委員会は、個々の銀行のリスク・プロファイルは異なっており、電子バンキング業務の規模、リスクの重大性、および、それらのリスクを管理する意欲と能力に相応したリスク削減手法が必要となること認識している。すなわち、電子バンキングのリスク管理においては、“画一的（one size fits all）”手法は必ずしも適切ではない。

同様の理由により、バーゼル委員会が公表する「リスク管理の原則」は、電子バンキングに関して特定の技術的選択肢や基準を設定することは企図していない。技術的選択肢については、テクノロジーが進歩する中で、銀行および基準設定機関が検討すべきである。但し、本レポートの付属文書においては、「リスク管理の原則」を補足するものとして、電子バンキングの分野で現在広く用いられているリスク削減手法の例が幾つか示されている。

従って、本レポートに述べられている「リスク管理の原則」およびサウンド・プラクティスは、各国当局が手段として用い、必要に応じて各国固有の規則や個別銀行のリスク・プロファイルに照らして修正しつつ適用することを前提としている。一部の分野の「原則」は、バーゼル委員会ないし各国当局が銀行監督ガイダンスの中で既に提示してきたものである。しかし、アウトソーシング関係の管理、セキュリティ管理、リーガル・リスクおよびレピュテーショナル・リスクの管理といった問題については、インターネットというデリバリー・チャンネルの特性と影響に照らして、これまでに提示されてきたものと比べより詳細な原則が必要となる。

「リスク管理の原則」は、明確となるように大きく３つのカテゴリーに分けられている。各々のカテゴリーに含まれる論点は互いに重複している場合が多い。３つのカテゴリーとは、「取締役会と経営陣による監視」、「セキュリティ管理」、「リーガル・リスクおよびレピュテーショナル・リスクの管理」である。

・取締役会と経営陣による監視

取締役会および上級管理職は、銀行の業務戦略を策定し、経営陣による有効なリスク管理体制を構築することに責任を有するため、電子バンキング・サービスを提供すべきか否か、また如何に提供すべきか、ということについて、十分な情報を得たうえで明示的かつ記録に残るかたちで戦略的決定を下すことが期待されている。当初の決定には、リスク管理上の具体的な責任、方針、および管理手順が含まれているべきであり、対象となるリスクにはクロスボーダー業務から発生するリスクも含まれる。経営陣による有効な監視には、電子バンキング・システムおよびデータを内外の脅威から適切に保護するためのセキュリティ対策の構築・維持など、セキュリティ管理プロセスの主要な側面を検証し、承認することが含まれるように期待されている。また経営陣は、電子バンキングの重要な機能を発揮するため、アウトソーシングや第三者委託に伴い複雑化し拡大してきているリスクを包括的に管理するプロセスにも注意を払うべきである。

・セキュリティ管理

電子バンキングに関して適切なセキュリティ管理プロセスが存在することを確認する責任は取締役会にあるが、電子バンキングがもたらすセキュリティ上の問題は従来以上に大きいため、経営陣はそれらのプロセスの内容についても特別な注意を払う必要がある。経営陣は、セキュリティ管理の具体的内容として、適切な権限の付与（authorisation）、正当性確認（authentication）のための措置、システム上および物理的なアクセス管理、内外ユーザーの活動に対して適切な境界と制限を維持し得る十分なシステム的セキュリティ対策、および取引・記録・情報に係るデータの完全性（integrity）について注意を払うべきである。また、全ての電子バンキング取引について明確な監査証跡（audit trails）を有するべきであり、主要な電子バンキング情報については機密度に応じた機密保持措置が採られるべきである。

顧客保護やプライバシーに関する法規は国によって異なるであろうが、全ての銀行は、顧客が伝統的なデリバリー・チャンネルを用いる場合に期待し得ると同レベルの情報開示・顧客データ保護・業務上の利用可能性（availability）を約束する明確な責任を有する。自国内と海外において行う電子バンキング業務に伴うリーガル・リスクおよびレピュテーショナル・リスクを最小化するため、銀行はウェブサイト上において十分な情報開示を行うとともに、電子バンキング・サービス提供先の国において適用されている顧客プライバシー関連の規則を確実に遵守し得るように適切な措置を採るべきである。

・リーガル・リスクおよびレピュテーショナル・リスクの管理

銀行は、業務リスク、リーガル・リスク、およびレピュテーショナル・リスクから身を守るため、常時かつ迅速なサービス提供に係る顧客の高い期待ならびに取引需要の拡大可能性に対処して、電子バンキング・サービスを安定的かつ適時に送達しなければならない。銀行は、電子バンキング・サービスを全てのエンドユーザーが利用できるようにするとともに、そうした能力を如何なる環境においても維持することができなければならない。内外からのセキュリティ侵害など、電子バンキング・システムおよびサービスの提供を阻害する惧れのある予期せぬ出来事から生じるオペレーショナル・リスク、リーガル・リスク、およびレピュテーショナル・リスクを最小化するためには、事件発生に備えた有効な対策も極めて重要である。従って銀行は、顧客の期待に応えるため、取引容量、業務の継続性、およびコンティンジェンシーについて有効なプランを策定すべきである。また、業務の継続性の確保、レピュテーショナル・リスクの管理、および電子バンキング・サービスの中断がもたらす責務の削減を図るべく、適切な障害対応計画をも策定すべきである。

「電子バンキングにおけるリスク管理の原則」に関する本レポートは一般に公開される。バーゼル銀行監督委員会は、銀行および銀行監督当局からのコメントを歓迎する。コメントは、ファックス（+41 61 280 9100）ないし電子メール（jean-philippe.svoronos@bis.org）により受け付ける。銀行からのコメントは、必要に応じ当該国の監督当局にもコピーを送付されたい。

電子バンキングにおけるリスク管理の原則

Ⅰ．はじめに

銀行は、何年も前から消費者および法人に対し遠隔地から電子的サービスを提供してきた。小口決済と対法人キャッシュ・マネジメントの双方を含む電子的資金移動、および、現金を引き出したりリテール口座を管理したりするために誰もがアクセスし得る自動機械は世界的に普及している。しかし、銀行の商品・サービスのデリバリー・チャンネルとしてインターネット[1]が世界的に受容されつつあることは、銀行に新たなビジネス・チャンスを、また消費者にはサービスの向上をもたらしている。

テクノロジーの革新が続いていること、および既存の銀行と新規市場参入者との間に競争が生じていることから、リテールおよびホールセールの銀行顧客に提供される電子バンキング[2]の商品・サービスの幅は広がっている。それらの商品・サービスには、情報アクセス、借入れ、預金口座の開設といった伝統的な業務のみならず、電子請求書に基づく支払サービス、顧客単位の金融「ポータル」、アカウント・アグリゲーション[3]、企業対企業の商取引市場・取引所といった比較的新しい商品・サービスも含まれる。

技術革新は大きな利益をもたらすが、電子バンキングの急速な進展はリスクと利益の双方を伴っており、銀行はそれらのリスクを認識し、慎重に管理することが肝要である[4]。こうしたことから、バーゼル銀行監督委員会は 1998 年に、電子バ

---

[1] 本レポートにおいて、インターネットとは、直接的なダイアルアップ接続、オープン・ネットワークであるワールド・ワイド・ウェブ、民間のバーチャル・ネットワークを含め、ウェブサイトの創設や接続を可能にする全ての関連技術および遠隔通信のオープン・ネットワークを意味する。

[2] 本レポートにおいて、電子バンキング（ないし **E バンキング**）とは、電子的チャンネルを通じたリテールおよび少額の銀行商品・サービスの提供、ならびに、大口の電子支払および電子的に行われるその他のホールセール銀行サービスを意味する。

[3] アカウント・アグリゲーション・サービスの顧客は、自らの金融および非金融勘定に関する情報を一個所に統合することができる。アグリゲーターの基本的な機能は、顧客が複数金融機関に有する勘定の統合情報を提供するため、顧客の代理人として行動することにある。顧客は、アグリゲーターが勘定情報にアクセスし、情報を統合することができるよう所要のセキュリティ・パスワードや個人 ID 番号（PIN）を教える。アグリゲーターは、主としてスクリーン・スクレイピングと呼ばれる技術を用いて情報を取得する。これは、他の機関のウェブサイトからデータを摂取するプロセスであり、情報を摂取される機関はこのことを知らない場合が多いが、金融機関同士の契約に基づいて直接的にデータが提供される場合もある。

[4] 情報テクノロジーの進歩は急速であるため、そうしたリスクを完全に網羅することは不可能

ンキングおよび電子マネーがリスク管理に及ぼす影響について暫定的な調査を行った[5]。この初期調査により、電子バンキングのリスク管理については更なる作業が必要であることが明らかになった。この使命は銀行監督当局と中央銀行からなるワーキンググループに託され、1999 年 11 月に電子バンキング・グループ（以下 EBG）が組成された。

バーゼル委員会は 2000 年 10 月に、電子バンキングの進展がもたらすリスク管理上および監督上の課題に関する EBG のレポートを公表した[6]。本レポートでは、電子バンキングに関わる主要なリスクが提示され、評価されている。それらのリスクとは、ストラテジック・リスク、レピュテーショナル・リスク、オペレーショナル・リスク（セキュリティ・リスクとリーガル・リスクを含む）[7]、および信用・マーケット・流動性の各リスクである。EBG は、電子バンキングはバーゼル委員会のこれまでの作業によって把握されていない新しいリスクをもたらすものではないと結論している。しかし、電子バンキングはそれらの伝統的なリスクの一部を増幅・変化させ、銀行業務の総合的なリスク・プロファイルに影響を与えると述べている。特に、電子バンキングの急速な導入と関連テクノロジーの複雑さがストラテジック・リスク、オペレーショナル・リスク、およびレピュテーショナル・リスクを高めることは確実である。

リスク管理上の課題

EBG は、電子バンキング（および電子商取引全般）の基本的な特性によって、リスク管理上の幾つかの課題が生じていることを指摘した。

- 電子バンキングにおけるテクノロジーおよび顧客サービスの革新のスピードは前例にないほど速い。これまで、新しい業務アプリケーションは十二分なテストを行ったうえで比較的長期間をかけて導入されるのが常であった。

である。しかし、電子バンキングに従事する銀行が直面するリスクは一般に新しいリスクではなく、バーゼル委員会の「実効的な銀行監督のためのコアとなる諸原則」（1997 年 9 月）に提示されているリスク・カテゴリーに含まれている。本ガイダンスは、信用リスク、カントリー・リスクおよびトランスファー・リスク、マーケット・リスク、金利リスク、流動性リスク、オペレーショナル・リスク、リーガル・リスク、レピュテーショナル・リスクの８つのカテゴリーを設けている。「コアとなる諸原則」は、BIS のウェブサイト（http://www.bis.org）において閲覧することができる。

[5] 「電子バンキングおよび電子マネー業務のリスク管理」（1998 年 3 月）、BIS のウェブサイト（http://www.bis.org）において閲覧可能。

[6] 「電子バンキング・グループの活動の趣旨および白書」（2000 年 10 月）、BIS のウェブサイト（http://www.bis.org）において閲覧可能。

[7] 本レポートでは、バーゼル委員会のリスク管理小委員会の定義に倣って、オペレーショナル・リスクにセキュリティ・リスクとリーガル・リスクを含める。

しかし今日では、銀行は競争圧力により、極めて短い時間的枠組みの中で新しい業務アプリケーションを適用することを余儀なくされており、構想から実施までの期間はしばしば数か月に過ぎない。こうした競争環境の中では、新しい電子バンキングを実施するに先立って、適切な経営戦略上の評価、リスク分析、およびセキュリティ上の検証を行うことがこれまで以上に重要な銀行経営上の課題となる。

・　取引の実行が可能な電子バンキングのウェブサイトおよび関連するリテールおよびホールセール業務アプリケーションは、電子的取引をよりストレートスルーに処理し得るよう、可能な限り旧来のコンピューター・システムに結合されている場合が多い。こうしたストレートスルーな自動処理は、手作業にありがちな人為的ミスや不正行為が行われる可能性を削減する一方、システムのデザイン、構造、互換性、およびオペレーション上の柔軟性に対する依存度を高める。

・　電子バンキングは情報テクノロジーに対する銀行の依存度を高め、これに伴って、オペレーション上およびセキュリティ上の課題の多くが技術的に更に複雑化するため、第三者との間でパートナーシップ・提携・アウトソーシングに関する取極めを結ぶ傾向が益々強まる。これらの第三者の多くは規制の対象となっていない。この結果、銀行と、インターネット・サービス・プロバイダーや通信会社などのテクノロジー企業をはじめとする非銀行企業が、共に関与する新しいビジネス・モデルが生まれている。

・　インターネットは遍在性およびグローバル性を有している。インターネットは、世界の何処からでも未知の人物がアクセスできるオープン・ネットワークであり、メッセージは未知の経路を経て送信され、ワイヤレスな通信手段も急速に進歩している。従って、インターネットは、セキュリティ管理、顧客の正当性確認技術、データの保護、監査証跡の保持、および顧客プライバシーに関る基準の重要性を著しく高める。

リスク管理の原則

バーゼル委員会は、EBG の初期の作業に基づき、伝統的な銀行リスク管理の原則は電子バンキングにも適用されるが、インターネットというデリバリー・チャンネルの複雑な特性に照らせば、これらの原則は、多くのオンライン銀行業務とそれに伴うリスク管理上の課題に合致するかたちに改められる必要があると結論付けた。このためバーゼル委員会は、取締役会および上級管理職が銀行の既存のリスク管理方針・手順について、既に実施中ないし計画中の電子バンキング業務

を対象とするように見直し、必要に応じて手直しすることが必要であると考える。バーゼル委員会はまた、銀行は全ての銀行業務を対象とする包括的なリスク管理手法を採用すべきであると考えており、電子バンキング業務に対するリスク管理上の監視は当該銀行の総合的なリスク管理の枠組みの一部となっていることが極めて重要であると考える。

こうした電子バンキング業務に伴うリスクへの対応を促すため、委員会は EBG に対し、銀行商品・サービスの安全かつ健全な電子的提供を促進するために、銀行がリスク監視のための既存の方針・手順を拡大して電子バンキング業務をも対象とするリスク管理原則を提示するように指示した。

本レポートに述べられている「電子バンキングにおけるリスク管理の原則」は、絶対的な規則ではなく、「ベスト・プラクティス」ですらない。これらは、安全かつ健全な電子バンキング業務を促進するためのガイダンスである。バーゼル委員会は、電子バンキングの分野においてリスク管理上の細部にわたる規則を定めることには弊害が伴い得ると考えている。このことは、テクノロジーや商品の革新がもたらす変化のスピードが速いため、そうした規則は短期間のうちに陳腐化する可能性が高いということに照らしても明らかである。従って、本レポートに述べられている原則は、厳格な規制ではなく、金融システムの安全性と健全性を確保するという銀行監督の全般的な目標に沿った監督当局の期待を表明したものである。

バーゼル委員会は、こうした監督上の期待は電子バンキングのデリバリー・チャンネルに特有の事情に照らして工夫・修正されるべきであるが、その他のデリバリー・チャンネルを用いた銀行業務に適用される原則と根本において異なるものであってはならないと考える。従って、以下に述べる原則は凡そ、バーゼル委員会ないし各国当局が既に数年にわたって表明してきた監督上の原則から導き出され、修正されたものである。しかし、アウトソーシング関係の管理、セキュリティ管理、リーガル・リスクおよびレピュテーショナル・リスクの管理など、一部の分野においては、インターネットというデリバリー・チャンネルの特性や影響に照らして、今日までに表明されてきた原則以上に詳しい原則を打ち出す必要が生じている。

バーゼル委員会は、各々の銀行が自らのリスク・プロファイル、事務構造、およびコーポレート・ガバナンスのあり方に照らし、かつ、自国の銀行監督当局が提示しているリスク管理上の特定の規則や方針に沿ってリスク管理プロセスを開発する必要があることを認識している。更に、本レポートに数多く述べられている電子バンキングのリスク管理実務は、現時点における業界のサウンド・プラク

ティスを示すものではあっても、全てを網羅したものであるとか、あるいは確定したものであると解釈されるべきではない。何故なら、セキュリティ管理やその他のリスク管理技術は、新しいテクノロジーや業務アプリケーションと足並みをそろえて引続き急速に発展しているからである。

本レポートは、個々のリスクに対処するために特定の技術的選択肢を提唱することを目的とするものではない。技術的な問題については、テクノロジーの進歩に合わせて、銀行および様々な基準設定機関が継続的に対処していく必要があろう。更に、銀行界がセキュリティ問題をはじめ電子バンキングを巡る技術的な課題に継続的に取り組む過程において、様々な革新的かつコスト効率のよいリスク管理手法が出現するものと予想される。また、それらの手法は、銀行毎に規模や業務の複雑性やリスク管理のあり方が異なること、あるいは法域毎に法規の枠組みが異なることから生じる問題にも対応し得るものとなることが予想される。

こうしたことから、委員会は電子バンキングのリスク管理において“画一的（one size fits all）”手法は不適切であると考えており、電子バンキングのデリバリー・チャンネルがもたらす追加的なリスクに対処するため、望ましい実務や基準について情報を交換し合うことを勧奨する。こうした監督上の考え方に従って、本レポートに述べられているリスク管理原則およびサウンド・プラクティスは、安全かつ健全な電子バンキング業務およびオペレーションを促進するための手段として各国当局が用い、必要に応じて各国固有の規則に照らして修正しつつ適用することを前提としている。

バーゼル委員会は、個々の銀行毎にリスク・プロファイルが異なるため、それぞれの電子バンキング業務の規模、負っているリスクの重大性、およびそれらのリスクを管理する意欲と能力に相応したリスク削減手法が必要となることを認識している。こうした相違を考慮し、本レポートに提示されているリスク管理原則は、全ての国の関係機関が実施し得る柔軟なものであると考えられている。各国当局は、個々の銀行の電子バンキング関連のリスクがどの程度重大なものであるかを見極めたうえ、当該銀行のリスク管理の枠組みにおいて、電子バンキングのリスク管理原則が十分に守られているか、またどの程度守られているかを判断することになろう。

Ⅱ．電子バンキングにおけるリスク管理の原則

本レポートに述べる電子バンキングのリスク管理原則は、おおまかに３つのカテゴリーに分類されており、それらのカテゴリーの間にはしばしば重複がみられ

る。しかし、これらの原則は優先度や重要度によってウェイト付けされていない。そうしたウェイトは時間の経過とともに変化する可能性があるため、優先順位をつけずに中立を保つことが望ましい。

A．取締役会および経営陣による監視[8]（原則１～３）

1．電子バンキング業務に対する経営陣の実効的な監視

2．包括的なセキュリティ管理プロセスの設定

3．アウトソーシング関係およびその他の第三者委託に対するデュー・ディリジェンスならびに経営陣による包括的監視プロセスの設定

B．セキュリティ管理（原則４～１０）

4．電子バンキングにおける顧客の正当性確認

5．電子バンキングの取引に関する取引否認の防止（non-repudiation）および責任の明確化

6．職責の分離を確保するための適切な措置

7．電子バンキングのシステム、データベース、アプリケーションにおける適切な権限管理

8．電子バンキングの取引・記録・情報に係るデータの完全性

9．電子バンキングの取引に関する明確な監査証跡の保持

10．重要な銀行情報に関する機密保持

C．リーガル・リスクおよびレピュテーショナル・リスクの管理（原則１１～１４）

11．電子バンキング・サービスに関する適切なディスクロージャー

12．顧客情報のプライバシー

13．電子バンキング・システムおよびサービスの利用可能性を確保するための、事務処理容量・業務の継続性・コンティンジェンシーに係るプラン

---

[8] 本レポートでは、取締役会と上級管理職によって構成される経営構造が言及されている。当委員会は、取締役会および上級管理職の機能に関して、国によって法律上および規制上の枠組みが大きく違うことを認識している。幾つかの国では、取締役会の、唯一ではないとしても主要な機能は、執行部（上級管理職、一般管理職）を監督し、両者が確実にその任務を遂行するようにすることである。このため、取締役会は時として監督役員会（supervisory board）とも呼ばれる。こうした場合、取締役会は執行機能を有していない。対照的に、他の国では取締役会はより広い権限を有し、銀行の経営の一般的な枠組みを策定する。こうした違いがあるため、本レポートでは、「取締役会」および「上級管理職」という概念は、銀行内の２つの意思決定機能を指すために用いられており、法的な構成概念は意味しない。

14．障害対応計画

上記の課題の各々については、銀行が電子バンキングとの関連においてこれらの課題に対処するためどのような基本的リスク管理原則を考えるべきかという観点から、以下の章でより詳しく論じる。必要に応じ、これらのリスクに対処するうえで有効と考えられるサウンド・プラクティスを付属文書として提示する。

Ａ．取締役会および経営陣による監視（原則１～３）

取締役会および上級管理職は、銀行の業務戦略策定に責任を負う。取引性のある電子バンキング・サービスの提供に先立って、当該行がそうしたサービスを提供することを望むか否かについて、明確な戦略的決定が下されるべきである。具体的に言えば、取締役会は、電子バンキングに係る企画が全社的戦略目標の中に明確に位置付けられているか、計画されている電子バンキング業務についてリスク分析が行われているか、認識されているリスクに対してリスク削減やモニタリングの適切なプロセスが設定されているか、また、電子バンキングの業績が業務計画・目的に照らして継続的に評価されているか、といったことを確認すべきである。

また、取締役会と上級管理職は、電子バンキング業務戦略に伴うオペレーショナル・リスクおよびセキュリティ・リスクの規模が適切に考慮され、対応が図られていることを確認すべきである。インターネットを介する金融サービスの提供は伝統的な銀行が持つリスク（例えば、戦略・レピュテーショナル・オペレーショナル・信用・流動性の各リスク）を大きく変化させ、ないし増加させる可能性すらある。従って、銀行の既存のリスク管理プロセス、セキュリティ管理プロセス、およびアウトソーシング先に対するデュー・ディリジェンスと監視プロセスが適切に評価され、電子バンキング・サービスに即して修正されるよう、所要の措置が採られるべきである。

原則１：取締役会および上級管理職は、電子バンキング業務に関連するリスクに対して経営陣による実効的な監視が行われるようにすべきである。実効的な監視には、電子バンキングに関連するリスクを管理するための明確な責任・方針・プロセスを設定することが含まれる。

電子バンキング業務に対して実効的な内部管理を行うためには、経営陣による

注意深い監視が不可欠である。インターネットというデリバリー・チャンネルは序文に述べたような特殊な性質を有しているうえ、電子バンキングの以下のような側面は伝統的なリスク管理プロセスに対して少なからぬ課題をもたらし得る。

- デリバリー・チャンネルの主要な要素（インターネットおよび関連テクノロジー）は、銀行の直接の統制が及ばないところにある。
- インターネットは、複数の国にまたがるサービスの提供を容易にする。それらの国には、当該銀行が物理的拠点を通じて既にサービスを行っている国以外の国も含まれる。
- 電子バンキングに関連する事柄は複雑であり、高度に技術的な用語や概念を伴うため、取締役会や上級管理職の伝統的な経験の範囲外である場合が多い。

電子バンキングの特性に照らせば、銀行のリスク・プロファイルや戦略に大きな影響を及ぼす可能性のある新たな電子バンキング・プロジェクトは、取締役会と上級管理職の検討に付し、適切な戦略分析およびコスト・ベネフィット分析の対象とすべきである。事前の戦略的検討や、計画との対比における継続的な実績評価が適切に行われていないと、銀行は電子バンキングのコストを過小評価したり、利益を過大評価したりする危険性がある。

また、取締役会と上級管理職は、銀行がリスク管理上の有効な監視を行う上で必要な専門知識を有さないまま、新たな電子バンキング業務に着手したり新たなテクノロジーを採用したりすることがないようにするべきである。経営陣およびスタッフの専門知識は、当該銀行の電子バンキング・アプリケーションおよび関連テクノロジーの技術レベルと複雑性に対応しているべきである。当該銀行の電子バンキング・システムおよびサービスが内部的に管理されていようと、第三者にアウトソースされていようと、適切な専門知識が必要である事に変わりはない。上級管理職による監視プロセスは日常的に運営され、電子バンキング・システムに大きな問題が生じたりセキュリティ侵害が起こったりした場合には、有効に対処することが可能でなければならない。電子バンキングはレピュテーショナル・リスクを増大させるため、システムの機能や顧客の満足度を注意深くモニターすること、および、障害発生時には取締役会や上級管理職に適切な報告が行われることが必要になる。

最後に、取締役会と上級管理職は、電子バンキング業務に対するリスク管理プロセスが当該銀行の総合的なリスク管理アプローチの一部となっていることを確保すべきである。リスク管理に関する既存の方針やプロセスは再評価され、実施中ないし計画中の電子バンキング業務をカバーし得るほど確固たるものであることが確認されるべきである。以下は、リスク管理上の監視について取締役会およ

び上級管理職が採り得るその他の措置の一部である。

- 電子バンキングにおいて当該銀行が容認し得るリスクの水準を明確に設定する。
- 主要な権限委任および報告ルールを設定する。これには、銀行の安全性・健全性やレピュテーションに影響を及ぼす事態（例えば、ネットワークへの不正侵入、従業員によるセキュリティ侵害、コンピューター設備の重大な不正使用）が生じた場合に、重大性に応じて上層部に報告を行う所要の手順（escalation procedures）が含まれる9。
- 商品・サービスの安全性、完全性、および利用可能性に係る電子バンキング特有のリスク要因に対処する。また、主要なシステムやアプリケーションのアウトソース先である第三者に対しても同様の措置を採るよう求める。
- クロスボーダー電子バンキング業務に着手するに先立ち、適切なデュー・ディリジェンスとリスク分析が行われることを確保する。

インターネットは、銀行の商品・サービスの提供能力を地理的にほぼ無限大に広げ、国境をまたいだ取引をも可能にした。こうしたクロスボーダー電子バンキング業務は、免許を取得した物理的拠点が現地に存在しない場合には、特に銀行のリーガル・リスク、規制リスク、カントリー・リスクを潜在的に増大させる。これは、銀行免許、監督、および消費者保護に関する規則が国毎に大きく異なることに起因する。クロスボーダー電子バンキングを計画している銀行は、不注意から外国の法規に違反してしまうことを防ぐため、またカントリー・リスク要因を管理するため、業務を開始する以前にそうしたリスクを十分に見極め、実効的なリスク管理を行う必要がある。

リスク管理プログラムの範囲や仕組みは、電子バンキング業務の範囲や複雑性に応じて銀行毎に異なるであろう。電子バンキング・サービスの監視に充当する資源は、システムの取引機能や重要性、ネットワークの脆弱性、および伝達される情報の機密度に相応しているべきである。

原則２：取締役会および上級管理職は、銀行のセキュリティ管理プロセスの主要な側面について検討し承認すべきである。

取締役会および上級管理職は、電子バンキングのシステムとデータを内外の脅威から適切に保護するセキュリティ対策の開発・維持を監視すべきである。こう

9 事態の重要度に応じて上層部に報告を上げる手順には、内部的な報告義務に加え、適切な監督当局に所要の報告を行うことも含まれているべきである。

した開発・維持には、適切な権限の承認、システム上および物理的なアクセス管理、および、内外ユーザーの活動に限界や制限を設ける適切なシステム的セキュリティ対策を確立することが含まれるべきである。

銀行の資産を守ることは取締役会の受託義務のひとつであり、上級管理職の基本的な責務の一つである。しかし、急速に進展する電子バンキングの環境においては、銀行資産の保護は困難な任務となる。これは、公開されたネットワークであるインターネットを通じて業務を行うこと、および革新的なテクノロジーを利用することに伴って複雑なセキュリティ・リスクが発生するためである。

取締役会および上級管理職は、電子バンキング業務において適切なセキュリティ管理を確保するため、行内に包括的なセキュリティ・プロセスが設定されていることを確認する必要がある。同プロセスは、方針と手順を含み、内外からセキュリティ侵害が行われる可能性に対し予防策と善後策の双方を備えたものでなければならない。電子バンキングにおける実効的なセキュリティ・プロセスの主要な要素には以下が含まれる。

- セキュリティに関する企業内の方針を設定・維持することについて、経営陣およびスタッフに明確な責任を付与する[10]。
- コンピューター施設に対する権限外の物理的アクセスを防止するため、万全な物理的管理を設定する。
- 電子バンキングのアプリケーションおよびデータベースに対する内外[11]からの権限外のアクセスを防止するため、万全なシステム上の管理およびモニタリング・プロセス[12]を設定する。
- セキュリティ対策および管理を定期的に見直す。こうした見直しには、セキュリティに関する業界の最新動向を常に把握すること、および、ソフトウェアの適宜更新やサービスパックのインストールなど所要の措置を採ることが含まれる[13]。

以上に加え、電子バンキングのセキュリティを確保するための助けとして、幾つかのサウンド・プラクティスを付属文書Ⅰに示す。

---

[10] 通常、本責任は監査機能の一部とすべきではない。監査機能は、セキュリティを監視する機能が有効に働いているか否かを検証することに責任を有する。

[11] 内部者には、従業員、契約先、およびアウトソース契約に基づいてアクセス権を有する者が含まれる。

[12] アクセス権限・特権を管理すること、およびネットワークに侵入しようとする試みを常時モニターすることを含む。

[13] ネットワークの動向、不正侵入の試み、および甚大なセキュリティ侵害の事例をモニターするための措置を含む。

原則３：取締役会および上級管理職は、電子バンキングにおける銀行のアウトソーシングやその他の第三者への事務委託を管理するため、包括的かつ継続的なデュー・ディリジェンスおよび監視のプロセスを設定すべきである。

電子バンキングの重要な機能に関しパートナーや第三者サービス・プロバイダーへの依存が高まれば、銀行経営陣の直接的な統制能力は低減する。従って、アウトソーシング等の第三者委託を管理するための包括的なプロセスが必要となる。こうしたプロセスには、パートナーやサービス・プロバイダーといった第三者が行う業務も含まれるべきである。また、アウトソースした業務が下請けに出されている場合も、銀行に重大な影響が及ぶ可能性があればこうしたプロセスの対象とすべきである。

従来は、アウトソーシングは特定の機能を単一のサービス・プロバイダーに委ねるにとどまる場合が多かった。しかし、近年は情報テクノロジーの進歩と電子バンキングの台頭に伴って、銀行のアウトソーシング関係は規模・複雑性ともに増大している。更に事態を複雑化させる要因として、アウトソースされた電子バンキング・サービスは他のサービス・プロバイダーないし他国に下請けされ得る。また、電子バンキングのアプリケーションが技術的に進歩し、戦略上の重要性を増すにつれて、電子バンキング機能の一部の分野は少数の専門化した第三者ベンダーおよびサービス・プロバイダーに依存するようになっている。こうした傾向はリスクの集中度を高める惧れがあるため、個々の銀行の立場からも銀行システム全体の立場からも注意を要する。

上記の要因は何れも、アウトソーシングおよびその他の外部委託、ならびに、これが銀行のリスク・プロファイルおよびリスク管理・監視能力に及ぼす影響を包括的かつ継続的に評価する必要性を示している[14]。取締役および上級管理職がアウトソーシング関係や第三者委託の監視に当って具体的に確認すべき事柄には以下が含まれる。

- 銀行は、電子バンキングのシステムやアプリケーションについて、アウトソーシングやその他のパートナーシップ取極めを行うことに伴うリスクを十分に理解している。

[14] そうした評価に際しては、当該第三者に対して統制力を行使し得る度合いを考慮に入れるべきである。ジョイント・ベンチャーに大口出資している場合は、サービス・プロバイダーとの契約関係における以上に統制力を行使し得る例が多い。しかし、そうした区別を前提として、ジョイント･ベンチャーやパートナーシップに対する株主の統制力が十分であると結論することはできない。特に、当該提携業務を実施するうえで必要なテクノロジーやサービスを小口出資者が提供している場合は注意を要する。上記のような区別は単に、評価はケース・バイ・ケ

・　電子バンキング・サービスに関する契約の締結に先立って、第三者サービス・プロバイダーやパートナーの能力や財務上の存続力につき適切なデュー・ディリジェンスが行われている。
・　アウトソーシング[15]ないしパートナーシップ関係における全当事者の契約上の責任が明確に定義されている。例えば、サービス・プロバイダーとの間の情報の授受に関する責任は明確にされているべきである。
・　アウトソースされた電子バンキングのシステムや業務には、リスク管理、セキュリティ、プライバシーについて、銀行自身の基準を満たす方針が適用されている。
・　アウトソースされた業務に対しては、独立した内部ないし外部監査が定期的に行われている。本監査は、当該業務が銀行内部でおこなわれている場合と少なくとも同等の内容とすべきである。
・　アウトソースした電子バンキング業務につき、適切なコンティンジェンシー・プランが立てられている。

以上に加え、電子バンキング・システムのアウトソーシングやその他の第三者委託を管理するための幾つかのサウンド・プラクティスを付属文書Ⅱに示す。

Ｂ．セキュリティ管理（原則４～５）

電子バンキングに関して適切なセキュリティ管理プロセスが存在することを確認する責任は取締役会にあるが、電子バンキングがもたらすセキュリティ上の問題は従来以上に大きいため、経営陣はそれらの管理プロセスの内容についても特別な注意を払う必要がある[16]。特に問題になるのは以下の諸点である。

・正当性の確認

・取引否認の防止

・データおよび取引の完全性

・職責の分離

・権限の管理

ースで行うべきであるとの結論を導くのみである場合が多い。

[15] 下請け業者をも含む。

[16] 例えば、取締役会が第三者ベンダーに電子バンキング・サービスを依存している場合、経営陣は当該ベンダーがこれらの事柄に適切に対処しており、少なくとも銀行自身の基準を満たしていることを確認する必要がある。

・監査証跡の維持

・重要な銀行情報の機密保持

原則４：銀行は、インターネットを介して業務を行う際に顧客の本人性および権限の正当性を確認する[17]（authenticate the identity and authorisation of customers）ため、適切な手段を講じるべきである。

銀行業務においては、個々の通信、取引、アクセス要請の正当性を確認することが不可欠である。従って、銀行は信頼性の高い手法を用いて、新規顧客の本人性や権限の正当性を確認し、また既存の顧客が電子取引を開始する際の本人性や権限の正当性を確認すべきである。

口座の新規開設に際する顧客確認は、なりすまし、詐欺的な口座開設申請、およびマネーロンダリングのリスクを削減するうえで重要である。銀行が顧客の正当性を適切に確認しなかった場合は、権限を持たない個人が電子バンキングの口座にアクセスすることを許し、究極的には、詐欺、機密情報の漏洩、犯罪行為への意図せざる関与といった事態に立ち至り、経済的な損失とレピュテーションの低下を招く惧れがある。

完全な電子的オープン・ネットワーク環境においては、個人のアイデンティティを特定し、その正当性を確認すること、および銀行システムへのアクセス権限を与えることは難しい。ユーザーに与えられた正当な権限は、「スプーフィング」と総称される様々な技術によって詐称され得る[18]。権限を有する正当な個人の交信は、「スニッファー」[19]という技術によってオンライン・ハッカーに奪い取られ、悪戯ないし犯罪行為に用いられ得る。また、正当性確認のための管理プロセスは、正当性確認データベース（authentication database）の改竄によっても欺かれ得る。

---

[17] 本報告書における「正当性の確認（authentication）」とは、顧客となる可能性のある人物もしくは既存の顧客の本人性ないし権限を確かめるために用いる技術、手順、およびプロセスを意味する。「本人性の確認（identification）」とは、口座開設時に顧客の本人確認を行うために用いる手順、技術、およびプロセスを意味する。「権限の確認（authorization）」は、顧客ないし従業員が銀行口座にアクセスする正当な権利を有していること、ないし、当該口座に関連する取引を行う権限を有していることを確かめるために用いる手順、技術、およびプロセスを意味する。

[18] スプーフィングとは、正当な顧客の口座番号、パスワード、個人 ID 番号、ないし E メール・アドレスを用いて、当該顧客になりすます行為。

[19] スニッファーとは、遠隔通信の交信内容を盗聴したり、パスワードや送信中のデータを詐取したりすることを可能にする手段。

従って銀行は、個人、代理人、ないしシステム[20]の本人性と権限の正当性を独自の手段で確認し、権限を持たない個人やシステムを可能な限り排除するため、適切な手法を選択する正式な方針と手順を設定しておくことが極めて重要である[21]。銀行は、個人 ID 番号、パスワード、スマート・カード、バイオメトリックス、電子認証など様々な方法を用いて正当性確認を行うことができる[22]。これらは、単独で用いることも組み合わせて用いる（例えば、パスワードとバイオメトリック・テクノロジー[23]を併用して正当性を確認）こともできる。一般論として、複数の方法を用いた正当性確認はより確実性が高い。

銀行は、電子バンキング・システムが全体として、あるいはシステムの様々な構成要素を通じて及ぼすリスクについての経営陣の評価に基づいて、何れの正当性確認手段を用いるかを決定しなければならない。リスク分析に際しては、当該電子バンキング・システムの取引内容（例えば、資金移動、請求書支払い、貸出の供与、アカウント・アグリゲーション等）[24]、保存されている電子バンキング・データの機密度と価値、および顧客にとっての当該正当性確認手段の使い勝手を評価すべきである。

顧客に対する本人確認や正当性確認のプロセスを堅固なものとすることは、クロスボーダー電子バンキングにおいて特に重要である。何故なら、国境をまたいで電子的に対顧客業務を行う場合は、なりすましが行われるリスクが増大したり、顧客となる人物に対して有効な信用審査を行うことがより難しくなるなど、問題が増幅するからである。

正当性確認の手段が進歩し続ける中にあって、銀行はこの分野における業界のサウンド・プラクティスをモニターし、採用することを勧奨される。例えば、サウンド・プラクティスには以下の事項の確認が含まれる。

---

[20] システムには、当該銀行自身のウェブサイトも含まれる。

[21] システムは、正当性を確認された個人、代理人、ないしシステムと取引を行っていること、および正当性確認のために用いたデータベースが有効であることを確保すべきである。

[22] 銀行は、公開鍵制度（PKI）を用いて顧客に電子認証を発行し、顧客と銀行との通信の安全性を確保することができる。電子認証と PKI については原則５においてより詳細に論じる。

[23] バイオメトリック・テクノロジーとは、個人の識別ないし正当性確認のため、身体上ないし行動上の特徴を自動的に看取するものである。本テクノロジーの代表的な例は、顔・虹彩・網膜・手・署名・声をスキャンしたり、打鍵の特徴を読んだりすることである。バイオメトリックスを用いた本人性の認定は極めて強力な正当性確認手段となるが、他の本人性・正当性確認手段に比べて適用が難しいと思われる。

[24] 有効な正当性確認手段は、取引否認のリスク、すなわち権限を有するユーザーが特定の取引を承認したことを事後的に否認するリスクをも減じる（原則５参照）。

・ 電子バンキングの顧客認証情報や機密度の高い情報へのアクセスを管理する認証システムは、改竄や変造の危険から守られていること。そうした改竄は察知され、その種の試みがあったことを記録した監査証跡が残されていること。

・ 正当性確認データベースへの個人・代理人・システムの追加・削除・変更は、正当な権限を有したもの[25]（authenticated source）により適切に承認されていること。

・ 未知の第三者が既知の顧客に取って替わることのないよう、電子バンキング・システムへの接続を管理する適切な措置が採られていること。

・ 正当性を確認された電子バンキングの通信は、通信の持続時間全体にわたって安全性を確保されており、セキュリティの確認が途切れた場合は正当性確認が再び行われること。

原則５：銀行は、取引の正当性を確認する際に、取引否認の防止（non-repudiation）を促進し、電子バンキング取引における責任を明確化する手段を用いるべきである。

取引否認の防止とは、電子的情報の受領者が当該情報を受領した事実を偽って否定する可能性から送信者を守るため、あるいは送信者が送信した事実を偽って否定する可能性から受信者を守るため、電子的情報の発信源および送達に関する証拠を設けることを意味する。取引否認のリスクは、クレジット・カードや証券取引などの伝統的な取引においても既に問題となっている。しかし、電子バンキングにおいては取引否認のリスクが一層高まる。これは、取引を申し入れてきた人物の本人性や権限の正当性確認が難しいこと、電子的取引が改竄されたりハイジャックされたりする惧れがあること、および、取引の詐欺的改竄があった旨、電子バンキングのユーザーが主張する惧れがあることによる。

こうした懸念の高まりに対処するため、銀行はそれぞれの電子バンキング取引の重要性やタイプに相応する妥当な努力を払って、以下のことを確保すべきである。

・ 電子バンキング・システムは、承認されたユーザーが意図せざる取引を開始してしまう可能性を減じ、かつ、顧客が自らの開始する取引に伴うリスクを十分に理解するよう考案されていること。

[25] 正当な権限を有したものは、場合によりシステムそのものであり得る。

・ 取引の全ての当事者について正当性確認が行われ、正当性が確認された通信経路に対する管理が維持されていること。

・ 全ての金融取引データは改竄から守られ、改竄が行われた場合は把握が可能であること。

銀行は、公開鍵制度[26]を用いた電子認証をはじめ、取引否認の防止、および電子バンキング取引の機密保持と完全性確保に資する様々な技術を用い始めている。銀行は、顧客ないし取引相手の本人性や正当性を確認する独自の手段として、顧客・取引相手に電子認証を発行し、取引否認のリスクを減じることができる。顧客の取引否認権が法律の特定の条項に規定されている国もあるが、電子署名の法的有効性を認める法律を承認している国もある。テクノロジーの進歩が続く中で、こうした技術は世界でより広く法的に受け入れられていくものと思われる。

原則６：銀行は、電子バンキングのシステム、データベース、アプリケーションについて、十分な職責分離が行われることを促す適切な措置を確保すべきである。

職責分離は、事務遂行の過程で不正行為が行われるリスクを削減し、取引および企業資産を適切に承認・記録・保護することを目的とする基本的な内部管理手段である。職責分離は、データの正確性や完全性を確保するうえで極めて重要であり、個人による不正行為を防止するために用いられる。職責が適切に分離されていれば、共犯によらない限り不正行為は起こり得ない。

電子バンキング・サービスにおいては、取引が電子的システムにより行われ、アイデンティティを隠したり偽ったりすることがより容易であるため、職責分離を設定・維持する方法に変更を加える必要が生じ得る。また、電子バンキングのアプリケーションにおいては、事務処理・取引機能がより圧縮され、統合されている場合が多い。従って、適切なレベルの管理を保つためには、職責分離を維持するために伝統的に用いられてきた管理方法を再検討・改訂する必要がある。デ

[26] 公開鍵制度（PKI）においては、各当事者が秘密鍵と公開鍵のペアを持っている。秘密鍵は１人のみが使えるよう隠されている。公開鍵は全ての当事者が用いる。秘密鍵からは書類に付する電子署名が作られる。ペアの鍵は、秘密鍵により暗号化されたメッセージを公開鍵によってのみ解読することができる仕組みとなっている。銀行は、自ら認証機関（CA）となることもできるし、信頼する第三者の発行する電子認証を用いて個人・企業を確認することもできる。しかし、第三者の発行する電子認証を用いて正当性確認を行う場合は、当該認証機関が認証を発行する際に、銀行自身がこれを行ったと仮定した場合と同レベルの正当性確認を行っていることを確かめるべきである。PKI による正当性確認システムの主たる難点は、適用が相対的に難しいことである。

ータベースのセキュリティ対策が不十分であれば、内外のネットワークからのアクセスを容易に許してしまう。従って、承認および本人性確認の厳格な手順、ストレートスルー・プロセッシングの安全かつ健全な構築、および十分な監査証跡の必要性が重視されるべきである。

電子バンキング環境において職責分離を設定・維持するため、一般的には以下のようなことが行われる。

- 取引プロセスおよびシステムは、単一の従業員ないしアウトソース先サービス・プロバイダーが取引を入力・承認・完了することのないように設計する。
- データ（ウェブサイトのコンテンツ等を含む）の登録者と同データの完全性を検証する者とを分離する。
- 電子バンキング・システムをテストし、職責分離を迂回する余地がないことを確認する。
- 電子バンキング・システムの開発者と管理者を分離する[27]。

原則７：銀行は、電子バンキングのシステム、データベース、およびアプリケーションについて、適切な権限付与の管理およびアクセス権限が設定されていることを確保すべきである。

職責分離を維持するため、銀行は権限とアクセス特権を厳格に管理する必要がある。適切な権限管理が行われていないと、個人が自らの権限を改竄して職責分離を迂回し、アクセス特権を与えられていない電子バンキング・システム、データベース、アプリケーションにアクセスすることを許してしまう惧れがある。

電子バンキング・システムにおいては、中央集中型ないし分散型の手法により銀行内に権限およびアクセス特権が設定され、一般に当該情報はデータベースに保存される。従って、これらのデータベースを改竄や変造から守ることは、権限管理を有効に行うための必須条件である。

電子バンキング・システム、データベース、およびアプリケーションに関する権限およびアクセス特権の適切な管理体制を設定するための助けとなるサウンド・プラクティスの一部を付属文書Ⅲに示す。

[27] あるいは、分離以外の手段を用いてリスク緩和を図る。

原則８：銀行は、電子バンキングの取引・記録・情報に関するデータの完全性（integrity）を守るため、適切な手段を講じるべきである。

データの完全性とは、送信中ないし保存中の情報に権限外の変更を加えることができないということを意味する。記録、情報、取引に関するデータの完全性が維持されていない場合、銀行は財務上の損失のみならずリーガル・リスクおよびレピュテーショナル・リスクに晒される。

電子バンキングにおいて行われるストレートスルー・プロセッシングの本来的な性質により、プログラミングの誤りや不正行為を早期に把握することはより難しくなる惧れがある。従って、銀行にとっては、安全性と健全性およびデータの完全性を確保し得る方法で、ストレートスルー・プロセッシングを実施することが重要である。

電子バンキング取引は公開されたネットワークを介して行われるため、データの変造、不正行為、および記録の改竄に係るリスクは高まる。従って銀行は、電子バンキングの取引・記録・情報の正確性・完全性・信頼性を確保するための適切な措置が採られていることを確認すべきである。それらの取引・記録・情報には、インターネット上で送信されているもの、銀行内部のデータベースに保存されているもの、ないし第三者サービス・プロバイダーが銀行に代わって送信ないし保存しているものが含まれる[28]。電子バンキング環境においてデータの完全性を維持するため、一般的には以下のようなことが行われる。

- 電子バンキングの取引は、取引プロセス全体を通して、改竄に対する抵抗力の極めて強い方法で行う。
- 電子バンキングに係る記録の保存・アクセス・修正は、改竄に対する抵抗力の極めて強い方法で行う。
- 電子バンキングにおける取引および記録保持のプロセスは、権限外の変更が行われたことを把握する仕組みを迂回することが事実上不可能であるようにする。
- 電子バンキング・システムを変更する際に、誤りないし過失により管理やデータの信頼性が損なわれることのないよう、モニタリングやテスティング手順を含む適切な変更管理方針を設定しておく。
- 電子バンキング取引の処理・モニタリング・記録保持を担当する部署は、

[28] 銀行は、改竄されたり質的に毀損されたりした記録を回復することが可能であるような記録保持システムを考案すべきである。

取引や記録の改竄を把握できる体制を整える。

原則９：銀行は、電子バンキングの全取引について明確な監査証跡（audit trails）が保持されていることを確保すべきである。

金融サービスをインターネット経由で送達する場合、電子バンキング環境に内部管理を実践していくことや明確な監査証跡を維持していくことを適合させなければ、それらはより難しくなる惧れがある。銀行は、高度に自動化された環境の中で有効な内部管理を行うとともに、同管理に対して独立した監査が行われることを確保するという課題を与えられている。特に、電子バンキングの重要なアプリケーション等については、例外なくこうしたことが求められる。

電子バンキング業務に関する明確な監査証跡が維持されていない場合、銀行の内部管理環境は弱まる惧れがある。これは、電子バンキング取引の記録や証拠の全てとは言わないまでも、多くが電子形態をとっているためである。何処に明確な監査証跡を維持しておくべきかを考える際は、以下のタイプの電子バンキング取引を検討対象とすべきである。

- 顧客勘定の開設・変更・閉鎖
- 財務上の結果を伴う取引
- 特定の顧客に対する限度超過の容認
- システムへのアクセスに関する権限や特権の付与・変更・撤回

電子バンキング取引に係る明確な監査証跡を確保するためのサウンド・プラクティスの幾つかを付属文書Ⅳに示す。

原則１０：銀行は、主要な電子バンキング情報の機密を保持するため、適切な手段を講じるべきである。機密保持の手段は、送信される情報やデータベースに保存される情報の機密度に相応したものとすべきである。

機密保持とは、主要な情報が銀行限りの扱いとされ、権限を与えられていない者により閲覧されたり用られたりすることがないということを意味する。銀行がデータを不適切に使用したり権限外に公開したりした場合は、レピュテーショナル・リスクおよびリーガル・リスクに晒される。電子バンキングの出現により、銀行はセキュリティ面で従来以上の課題を抱えることになった。電子バンキングにおいては、公開されたネットワークを介して送信される情報やデータベースに

保存されている情報に、権限を有さない者や不適切な者がアクセスしたり、情報提供時に顧客が意図しなかった方法でそれらの情報が用いられたりするリスクが高まるためである。また、サービス・プロバイダーを利用する度合いが高まっていることも、主要な銀行データが第三者に開示されるリスクをもたらしている。

主要電子バンキング情報の機密保持に関する上記の問題に対処するため、銀行は以下のことを確保すべきである。

- 機密性のある全ての銀行データおよび記録には、然るべく権限を付与され、正当性を確認された個人・代理人・システムのみがアクセスを有する。
- 機密性のある全ての銀行データは、安全な方法で維持され、公開されたネットワーク・私設ネットワーク・内部的なネットワークの何れを通じて送信される時も、権限を有さない者により閲覧されたり修正されたりすることのないよう保護される。
- アウトソーシング関係を通じて第三者がデータへのアクセスを有する場合も、データの使用や保護に関する銀行の基準や管理が遵守されている。
- 閲覧が限定されているデータへのアクセスは全て記録され、当該記録が改竄されることのないよう適切な努力が行われている。

C．リーガル・リスクおよびレピュテーショナル・リスクの管理（原則１１～１４）

顧客保護やプライバシーに関する具体的な法規は国によって異なるであろう。しかし、全ての銀行は、伝統的な銀行のデリバリー・チャンネルを用いて取引を行った場合と同レベルの情報開示・顧客データの保護・業務の利用可能性を顧客に約束する明確な責任を有する。

原則１１：銀行は、ウェブサイトにおいて十分な情報を提供し、顧客となる人が電子バンキング取引を開始するに先立って、当該銀行のアイデンティティや規制環境について十分な情報を得たうえで意思決定を行うことを可能にすべきである。

銀行は、国内・クロスボーダー双方の電子バンキング業務に伴うリーガル・リスクおよびレピュテーショナル・リスクを最小限にとどめるため、ウェブサイトにおいて十分な情報を提供し、顧客となる人が電子バンキング取引を開始するに先立って、当該銀行のアイデンティティや規制環境について十分な情報を得た

うえで意思決定を行うことを可能にすべきである。

銀行がウェブサイトにおいて提供する情報の例は以下のとおりである。

- 銀行の名称と本部（および該当する場合は現地営業所）の所在地
- 銀行の本部に対して第一義的監督責任を有する銀行監督当局
- サービス上の問題、苦情、口座の不正使用の可能性等について相談するため、銀行の顧客サービス・センターにコンタクトをとる方法
- 利用可能なオンブズマンや消費者保護制度へのアクセス・利用方法
- 適用される国家的な補償制度や預金保険の適用範囲および保護のレベル（ないし、そうした情報を提供しているウェブサイトへのリンク）
- 特定の国において適切な、ないし提供を義務付けられているその他の情報[29]

原則１２：銀行は、顧客のプライバシー保護に関し、当該銀行が電子バンキングの商品・サービスを提供している国において適用されている規則を遵守するため、適切な措置を講じるべきである。

顧客の情報プライバシーを維持することは、銀行の重要な責任の一つである。機密性のある顧客データを不適切に使用したり権限外に開示したりすれば、銀行はリーガル・リスクとレピュテーショナル・リスクの双方に晒される。顧客情報のプライバイシー保護に関するこうした問題に対処するため、銀行は以下のことを確保すべく妥当な努力を払うべきである。

- 顧客のプライバシーに関する銀行の方針と基準は、当該銀行が電子バンキングの商品・サービスを提供している全ての国の関連法規を考慮し、これを遵守したものとなっている。
- 顧客は、プライバシーに関する銀行の方針、および、電子バンキングの商品・サービスを利用することに伴うプライバシー問題について知識を与えられている。
- 顧客は、銀行がクロス・マーケティングの目的で顧客の個人的なニーズ、関心、資産状況、銀行取引について第三者に情報を提供することを拒否する（“opt out”する）ことができる。
- 顧客データは、明示的に認められた目的、ないし顧客が承認した目的以外

[29] 例えば、当該銀行が電子バンキング・サービスの提供対象としている国を明示したり、逆に、そうしたサービスの提供対象外としている国を明示したりすることが考えられる。

では用いられない。

・ アウトソーシング関係を通じて第三者が顧客データへのアクセスを与えられている場合も、顧客データの使用に関する銀行の基準は満たされている[30]。

電子バンキングにおいて顧客情報のプライバシー保護を促進するためのサウンド・プラクティスの幾つかを付属文書Ⅴに示す。

原則１３：銀行は、電子バンキングのシステムとサービスの利用可能性（availability）を確保するため、取引処理容量、業務の継続性、コンティンジェンシーについて、有効なプランニング・プロセスを設けるべきである。

銀行は、ビジネス・リスク、リーガル・リスク、およびレピュテーショナル・リスクから身を守るため、顧客の期待に応えて安定的かつ適時に電子バンキング・サービスを提供しなければならない。このため、銀行は電子バンキング・サービスを一次的（例えば内部的な銀行システムおよびアプリケーション）ないし二次的（例えばサービス・プロバイダーのシステムおよびアプリケーション）な供給源の何れかからエンドユーザーに提供する能力を備えていなければならない。十分な利用可能性を維持し得るか否かは、緊急時のバックアップ・システムによって、“サービス妨害攻撃（denial of service attacks）”をはじめ業務の中断につながる惧れのある障害をどの程度緩和することができるかにも依存する。

電子バンキング・システムおよびサービスの持続的利用可能性を確保することは、ピーク時間帯を中心に大量の取引需要が発生する可能性があるだけに難しい課題となり得る。また、顧客が短時間内の取引処理および恒常的利用可能性（24時間、7日）を強く期待していることに照らしても、取引処理容量・業務の継続性・コンティンジェンシーに関する健全なプランニングの重要性は高い。顧客の期待に応えて電子バンキング・サービスの継続性を保証するため、銀行は以下のことを確保する必要がある。

・ Eコマースの総合的な市場動向、および顧客の間での電子バンキング商品・サービスの予想普及率に照らし、電子バンキングの現在の容量と将来におけ

[30] 一部の国では、銀行が顧客情報を内部的な目的のために用いる際に、顧客の許可を得ることを法規により義務付けられていない場合がある。しかし、こうした国においても、同情報を第三者や系列会社に提供することについては、顧客に拒否する機会を与えるよう法規により義務付けられている場合がある。他の国では、内部的目的においても外部的目的においても、銀行が顧客データを用いることについては顧客に拒否権が与えられている。

る余力を分析する[31]。

- 電子バンキングの取引処理容量を推計し、ストレス・テストを行い、定期的に見直しを行う。
- 電子バンキングの処理やデリバリーの主要システムについて、業務の継続性確保およびコンティンジェンシーに係る適切な計画が立てられ、定期的にテストされている。

取引処理容量、業務の継続性、およびコンティンジェンシーのプランニングに関するサウンド・プラクティスを付属文書VIに示す。

原則１４：銀行は、内外からのセキュリティ侵害など、電子バンキング・システムおよびサービスの提供を阻害する惧れのある予期せぬ出来事から生じる問題を管理・抑制・最小化するため、適切な障害対応計画を策定すべきである。

障害対応の有効なメカニズムは、内外からのセキュリティ侵害など、電子バンキング・システムおよびサービスの提供を阻害する惧れのある予期せぬ出来事から生じるオペレーショナル・リスク、リーガル・リスク、およびレピュテーショナル・リスクを最小化するうえで極めて重要である。銀行は、業務の継続性を確保し、レピュテーショナル・リスクを管理し、アウトソースしたシステムや業務を含め電子バンキング・サービスが中断した場合に生じる責務を限定的なものにとどめるため、情報伝達戦略を含む適切な障害対応計画を策定すべきである。

予期せぬ障害に有効に対応し得るため、銀行は以下の体制を整備すべきである。

- 様々なシナリオ、業務、地理的区分に従って立案した、電子バンキング・システムおよびサービスを回復するための障害対応計画。シナリオ分析に際しては、リスクが発生する蓋然性と銀行への影響を考慮すべきである。第三者サービス・プロバイダーにアウトソースされた電子バンキング・システムも、これらの計画に含まれているべきである。
- 発生した事件や危機を直ちに把握し、被害の程度を評価し、サービスの中断に伴うレピュテーショナル・リスクを管理するメカニズム[32]

---

[31] 電子バンキングの重要なデリバリー・システムについては、現在および将来の容量を継続的に評価すべきである。

[32] ヘルプ・デスクや顧客サポート業務をモニターしたり、顧客からの苦情を定期的にチェックしたりすることにより、セキュリティ管理を通じて把握・報告された情報と実際のセキュリティ侵害とのギャップが判明する可能性がある。

・ セキュリティ侵害、オンライン・アタック、ないし電子バンキング・システムのダウンに際し、市場やメディア等の外部に生じる懸念に適切に対処するための情報伝達戦略

・ 重大なセキュリティ侵害や業務を阻害する出来事が発生した場合に、適切な監督当局に通知する明確なプロセス

・ 障害対応チーム。同チームは、緊急時に対処する権限を与えられているとともに、障害把握・対応システムを分析したり、障害に伴う事象の意味を解釈したりすることにおいて十分な訓練を受けているべきである。

・ 明確な命令系統。事件の重大性に相応した迅速な対応が可能となるよう、命令系統は内部業務とアウトソースされた業務の双方を包摂しているべきである。また、重大性に応じて上層部に報告を行う手順、および内部的な情報伝達手順が設けられ、必要な場合には取締役会にも通知が行われるべきである。

・ 電子バンキングに生じた重大な障害や業務回復状況につき、顧客、取引相手、メディアを含め、全ての外部関係者に適時かつ適切な方法で情報を提供するプロセス

・ 電子バンキング関連の障害に適切な事後検証を加えるとともに、侵害者の起訴に役立てるため、法廷で用い得る証拠を収集・保存するプロセス

電子バンキングにおけるセキュリティ管理のサウンド・プラクティス

1．セキュリティ体制が構築・維持され、顧客、銀行内部のユーザー、およびアウトソース先サービス・プロバイダーを含め、電子バンキング・システムおよびアプリケーションの全てのユーザーに明確な権限が付与されるべきである。システム上のアクセス管理も、適切な職責分離を支援し得るように構築されるべきである[33]。

2．電子バンキングのデータおよびシステムは、機密度と重要性に即して分類・保護されるべきである。全ての機密度とリスクの高い電子バンキング・システム、サーバー、データベース、およびアプリケーションは、暗号、アクセス管理、データ回復手順などの適切なメカニズムを用いて保護されるべきである。

3．機密度ないしリスクの高いデータを行内のデスクトップおよびラップトップ・コンピュータ内に保存することは最小限に止められ、かつ、暗号、アクセス管理、データ回復手順により適切に保護されるべきである。

4．権限外のアクセスを阻止するため、全ての重要な電子バンキング・システム、サーバー、データベースおよびアプリケーションに十分な物理的アクセス管理が設定されるべきである[34]。

5．以下を含め、電子バンキング・システムに対する外部からの脅威を緩和するための適切な技術が用いられるべきである。

- 全ての重要なエントリー・ポイント（例：リモート・アクセス・サーバー、電子メールの代理サーバー）および全てのデスクトップ・コンピュータにウィルス検知ソフトウェアを適用する。

---

[33] セキュリティの定義、質的基準、および認定制度の利用は、銀行毎に異なる場合もあれば標準化されている場合（すなわち、電子バンキング業務のセキュリティを保持育成するため銀行界が全国レベルで標準化）もある。銀行はまた、アクセス権限の設定に際して中央集中型ないし分散型の何れかを選択することができる。例えば、個々の人物、グループ、ないし職務上の役割に対し単一の権限付与機能を通じてアクセス権限を付与することもできる一方、業務ライン毎に異なる事情に対応するため、複数の権限付与機能を設定することもできる。

[34] 来訪者、出入り業者、技術者等の外部者も、営業所にアクセスを有する限り、必ずしも電子バンキング・サービスに直接関わっていなくとも権限外アクセス防止策の対象とすべきである。

・ 侵入検知ソフトウェア等のセキュリティ評価技術を用いて、ネットワーク、サーバーおよびファイヤーウォールを定期的に検証し、セキュリティ対策・管理上の問題点や違反を把握する。

・ 内外ネットワークに対し侵入テストを実施する。

6．機密事項を扱う全ての従業員およびサービス・プロバイダーに対しては、セキュリティ上の厳格な審査が行われるべきである。

アウトソースした電子バンキング・システムおよびサービスを管理するためのサウンド・プラクティス

1．銀行は、電子バンキング・システムないしサービスのアウトソーシングに関する決定を評価するための適切なプロセスを採用すべきである。

- 銀行経営陣は、電子バンキングに関して第三者との間でアウトソーシング取極めを結ぶに当って、戦略上の目的、利益、およびコストを明確に把握すべきである。
- 主要な電子バンキング機能ないしサービスのアウトソーシングに関する決定は、当該銀行の業務戦略との整合性、明確な業務上の必要性、およびアウトソーシングに伴う具体的なリスクの認識を前提とすべきである。
- 行内の全ての関連部署は、サービス・プロバイダーが如何に当該銀行の電子バンキング戦略をサポートし、当該銀行のオペレーション構造の中に織り込まれるかを理解する必要がある。

2．銀行は、電子バンキング・サービス・プロバイダーの選定に先立って、適切なリスク分析およびデュー・ディリジェンスを行い、以後も適切な間隔で同様のことを行うべきである。

- 銀行は、複数の電子バンキング・サービス・プロバイダーに見積もりを求めるプロセス、および、寄せられた様々な見積もりの中から選択を行う基準の設定を検討すべきである。
- サービス・プロバイダーの候補が挙がった時点で、銀行は当該サービス・プロバイダーの財務力、レピュテーション、リスク管理の方針と統制、義務の履行能力に関するリスク分析など、適切なデュー・ディリジェンスを行うべきである。
- その後で、銀行は契約の持続期間全体を通じて、サービス・プロバイダーがサービスおよび関連するリスク管理義務を履行する能力を備えているか否かを定期的にモニターし、必要に応じて[35]デュー・ディリジェンスの検証を行うべきである。
- 銀行は、電子バンキングをサポートするアウトソーシング取極めを監視

[35] 継続的なデュー・ディリジェンスをどの程度行うかは、アウトソースされた業務の重要性や、サービス・プロバイダーが事後的に下請け契約を結ぶなど、この間にシステムやリスク管

することに十分な資源を投入する必要がある。

- 電子バンキングのアウトソーシング取極めを監視する責任の所在は明確にされるべきである。
- アウトソーシング契約を終了する必要が生じた場合に備え、銀行はリスクを管理するための適切な退出戦略を立てておくべきである。

3．銀行は、電子バンキングに関する契約の妥当性を確保するための適切な手続きを採用すべきである。電子バンキング業務のアウトソーシングに関する契約は、例えば以下の点をカバーすべきである[36]。

- 双方の契約上の義務、および、重要サービスの下請けを含め、意思決定責任を明確に定義する。
- サービス・プロバイダーに情報を提供する責任、およびサービス・プロバイダーから情報を受領する責任を明確に定義する。銀行がサービス・レベルおよびリスクを適切に評価し得るよう、サービス・プロバイダーからは適時かつ包括的に情報を受領すべきである。サービスの中断、セキュリティ侵害、および銀行に甚大なリスクを及ぼし得るその他の出来事を銀行に通知する際の重要性基準と手順が明らかにされているべきである。
- 保険のカバレッジ、サービス・プロバイダーのサーバーやデータベースに保存されている情報の所有権、および、契約の満了ないし終了時に銀行が自らのデータを回収する権利を明確に定義すべきである。
- 平常時および緊急時におけるパフォーマンスの期待水準を定義する。
- サービス・プロバイダーが銀行の方針に従うことを確保するため、監査条項等の適切な手段と保証を定義する。
- サービス・プロバイダーのパフォーマンスが基準以下であった場合に、適時に整然と介入や是正措置を行うことを可能にする条項を設ける。
- クロスボーダーのアウトソーシング取極めの場合は、プライバシーや消費者保護に係る法規を含め、何れの国の法規を適用するかを明らかにする。
- セキュリティ、内部管理、および業務の継続性とコンティンジェンシーに関する計画について、銀行が独立した検証や外部監査を行う権利を明示的に定義する。

理のあり方に変化が生じた度合いに応じて決定すべきである。

[36] 銀行が他の法的契約を取り結ぶ場合と同様に、電子バンキングのアウトソーシング取極めに関する契約に盛り込まれた全ての条件は、銀行の法律顧問ないし法務部のチェックを受けるべきである。

4．銀行は、アウトソースされた業務に対し、独立した内部ないし外部監査が定期的に行われることを確保すべきである。監査は、当該業務が銀行内部で行われていたと仮定した場合と同様の規模で行われるべきである[37]。

・　重要な、もしくは技術的に高度な電子バンキング・サービスやアプリケーションをアウトソースしている場合、銀行は、十分な技術的専門知識を有する独立した第三者に依頼して、別途の定期的検証を行う必要があるかもしれない。

5．銀行は、アウトソースした電子バンキング業務について、適切なコンティンジェンシー・プランを策定すべきである。

・　銀行は、第三者にアウトソースした全ての重要な電子バンキング・システムおよびサービスについて、コンティンジェンシー・プランを策定し、定期的にテストする必要がある。

・　コンティンジェンシー・プランは、起こり得る最悪のシナリオを想定のうえ、アウトソースした業務が中断した場合でも電子バンキング・サービスの継続性を確保し得るものとすべきである。

・　銀行は、アウトソースした電子バンキング・サービスが中断した場合に、当該業務の回復を図り、財務面への影響を評価することに責任を有するチームを設けるべきである。

6．第三者に電子バンキング・サービスを提供する銀行は、サービス対象機関が独自のデュー・ディリジェンスおよびアウトソーシング関係の継続的な監視を有効に行うことができるよう、自らの業務、責任および義務を十分明確にすべきである。

・　銀行は、サービス対象機関に対し、当該電子バンキング・サービス取極めに係るリスクを把握・管理・モニターするために同機関が必要とする情報を提供する責任を負う。

[37] 行内に特別な監査機能が設けられていない場合は、少なくとも、アウトソーシング関係の管理に関わっていない職員がアウトソーシング取極めの管理状況を検証すべきである。

電子バンキング・アプリケーションの権限に係るサウンド・プラクティス

1．電子バンキング業務に関わる全ての個人、代理人、システムは、具体的に定義された権限とアクセス特権を付与されるべきである。

2．全ての電子バンキング・システムは、有効な権限データベースのみに連動するよう設計されるべきである。

3．個々の代理人ないしシステムは、電子バンキングの権限データベースに保存されている自らの権限やアクセス特権に変更を加える権限を与えられてはならない[38]。

4．電子バンキングの権限データベースに保存されているアクセス特権に個人・代理人・システムを追加したり変更を加えたりする際は、所要の承認を受けるべきである。本承認は、十分な権限を有し、適時適切な監視および監査を受け、かつ正当性を確認された主体により行われる。

5．電子バンキングの権限データベースが改竄に対して十分な抵抗力を持つよう、適切な措置が講じられるべきである。改竄の試みは、継続的なモニタリング・プロセスの過程において把握されるべきである。改竄の試みを記録しておくため、十分な監査証跡が残されるべきである。

6．電子バンキングの権限データベースが改竄された場合は、有効なデータベースと交換されるまで用いてはならない。

7．電子バンキング取引の遂行中に権限のレベルを変えようとする試みを阻止するための措置を講じ、そうし試みは記録し経営陣に報告すべきである。

[38] システム管理者を務めているユーザーについてはこれを実行することができない場合もあるため、これらのユーザー・アカウントの動向をモニターするためには、他の厳格な内部管理および職責分離措置を講じるべきである。

電子バンキング・システムの監査証跡に係るサウンド・プラクティス

1．明確な監査証跡を確立するとともに、紛争の解決に役立てるため、全ての電子バンキング取引について十分な記録が残されるべきである。

2．電子バンキング・システムは、法廷で用い得る証拠を捕捉・維持し得るよう設計されるべきである。設計に際しては、証拠を管理下に置くこと、および証拠の改竄や虚偽の証拠収集を阻止することに意を用いる。

3．処理システムおよび同システムに関連する監査証跡が第三者サービス・プロバイダーの責任に委ねられている場合：

- 銀行は、サービス・プロバイダーが維持している関連監査証跡に対するアクセスを確保すべきである。
- サービス・プロバイダーが維持している監査証跡は、銀行の内部基準を満たしているべきである。

付属文書　Ⅴ

顧客の電子バンキング情報に係るプライバシーを守るためのサウンド・プラクティス

1．銀行は、顧客の電子バンキング情報の機密を保持するため、適切な暗号技術、特定のプロトコル等のセキュリティ管理手段を用いるべきである。

2．銀行は、電子バンキングにおける顧客セキュリティのインフラストラクチャーとプロトコルを定期的に評価するため、適切な手順と管理を設けるべきである。

3．銀行は、第三者サービス・プロバイダーが採用している機密保持およびプライバシーに係る方針が銀行自身の同方針と整合的であることを確認すべきである。

4．銀行は、電子バンキングの顧客に対し、顧客情報の機密保持およびプライバシーについて情報を提供するため、以下を含む適切な措置を採るべきである。

- 顧客に対し、銀行のウェブサイト等において、プライバシーに係る自らの方針を伝える。顧客が同方針を完全に理解し得るよう、そうした文書には簡潔な言葉を用いることが肝要である。法律事項を長々と記述すれば正確であるかもしれないが、大多数の顧客には読まれない惧れが強い。
- 顧客に対し、パスワード、個人認識番号等の銀行・個人データを守る必要性を伝える。
- 顧客に対し、ウィルス防止ソフトウェア、物理的アクセス管理、インターネット接続に際する個人的ファイヤーウォールの設定など、パソコンのセキュリティ全般に関する情報を提供する。

電子バンキングの処理能力、業務の継続性、およびコンティンジェンシーに係るプランニングについてのサウンド・プラクティス

1．第三者サービス・プロバイダーにより提供されているものを含め、全ての電子バンキング・サービスおよびアプリケーションを認識し、その重要性を評価すべきである。

2．重要な電子バンキング・サービスおよびアプリケーションについては、それぞれについてサービスの中断が信用・マーケット・流動性・リーガル・オペレーショナルおよびレピュテーショナルの各リスクに及ぼし得る影響を評価すべきである。

3．重要な電子バンキング・サービスおよびアプリケーションについては、個別にパフォーマンス基準を設け、同基準に照らしてサービス・レベルをモニターすべきである。電子バンキング・システムが取引量の増減に耐え得ること、および、電子バンキングの将来的な拡大に係る銀行の予測に照らしてシステムの実績と処理能力に問題がないことを確保するため、適切な措置を採るべきである。

4．電子バンキング・システムの処理能力が一定のチェックポイントに達したと思われる場合に用いる選択肢として、取引をコントロールしつつ処理を進める手法を開発することを検討すべきである。

5．電子バンキング業務の継続性を確保するための計画として、業務回復のために第三者サービス・プロバイダー等の外部に依存しなければならない場合を検討しておくべきである。

6．電子バンキングに係るコンティンジェンシー・プランには、電子バンキングの処理能力を回復ないし更新したり、取引をサポートする情報を再構築したりするプロセスが示されているとともに、業務が中断した場合に重要な電子バンキング・システムおよびアプリケーションの利用可能性を回復するために採るべき措置が含まれているべきである。