

バーゼル銀行監督委員会「電子バンキング および電子マネー業務のリスク管理」 について

1998年 3 月

(掲載に当たって)

バーゼル銀行監督委員会では、3月20日、G-10中央銀行総裁会議での了承を経て、「電子バンキングおよび電子マネー業務のリスク管理」と題するペーパーを公表した。

バーゼル銀行監督委員会による本ペーパーに関するプレス・ステートメントおよび同ペーパーの仮訳は次のとおりである。

プレス・ステートメント

バーゼル銀行監督委員会（以下、バーゼル委）は、G-10諸国の中央銀行総裁の了承を得て、本日、「電子バンキングおよび電子マネー業務のリスク管理」に関するペーパーを発表する。本ペーパーの目的は、電子バンキングや電子マネーに伴うリスクを識別、評価、管理、コントロールする方法を策定するにあたり、監督当局や金融機関が考慮すべき諸要素を提示することである。

電子的な支払手段は、電子商取引が発展する中でその重要性を増しつつある。現時点において、電子バンキングと電子マネーは、未だ発展と利用の初期段階にある。電子バンキングや電子マネー業務は銀行に対して新たな機会を提供する一方、便益と共にリスクももたらすため、こうしたリスクを認識し、慎重に管理することが重要である。

バーゼル委は、電子的な小口商品・サービス

の技術進歩に関する監督上の問題や対応について検討と議論が進められている中で、本ペーパーがその第一歩になるものと考えている。今後の技術的發展や市場展開が不確実であることを前提とすれば、監督当局が有益なイノベーションや実験を阻害するような政策を回避することが重要である。本ペーパーは、電子バンキング・電子マネー業務のリスク管理に対する適切な監督アプローチの構築に資することを期待して、世界中の監督当局に配布される。

なお、本ペーパーの原文は、3月20日以降BISホームページ（<http://www.bis.org>）に掲載されるほか、各国監督当局、国際決済銀行にあるバーゼル委事務局から入手可能である。

1998年 3 月20日

電子バンキングおよび電子マネー業務のリスク管理

第1章 はじめに

電子的な支払手段は、電子商取引が発展する中でその重要性を増しつつあり、電子マネーを含む小口の電子バンキング・サービスや商品は、銀行にとって意味のある新たな機会の提供を可能としている。電子バンキングは、銀行が伝統的な預金・貸出業務の市場を拡大すること、新しい商品・サービスを提供すること、あるいは現行の支払サービス提供における競争上の地位を強化することを可能にするとみられる。さらに、電子バンキングは銀行の運営経費を削減する可能性をもっている。

より一般的には、電子バンキングと電子マネーの発展が続くことは、「銀行および決済システムの効率性向上」や、「国内外の小口取引における費用削減」につながるものと考えられる。この結果として、潜在的には生産性の向上と経済厚生が増大が実現する可能性もある。消費者や小売店は、資金受払いの効率性を高めることができ、より大きな利便性を享受できるようになるかもしれない。また、電子バンキングは、これまで金融システムへの参加が制限されていた消費者にとって、アクセス経路の拡大をもたらすと考えられよう。

本報告書の対象は、2つの点において限定されることとなる。第1に、本報告書は電子バンキングおよび電子マネー業務のリスク管理について銀行監督の視点からのみ扱うものであり、例えば、金融面への影響を考察するものではない。第2に、本報告書で記述されているリスクの多くは、銀行、ノンバンク双方の発行者および提供者に当てはまるものであるが、本報告書は銀行のみを対象とする。

1. 1. 目的および構成

電子マネーや幾つかの形態の電子バンキングは、未だ発展や利用の初期段階にある。電子バンキングと電子マネーの分野における今後の技術的発展や市場展開が不確実であることを前提とすれば、監督当局が有益なイノベーションや実験を阻害するような政策を回避することが重要である。また、バーゼル委員会としては、電子バンキングや電子マネー業務が金融機関に対して便益と共にリスクをももたらすこと、またこうしたリスクが便益に対して釣り合いがとれたものでなければならぬこと、を認識している。

本ペーパーの目的は、電子バンキングと電子マネーに伴うリスクを識別、評価、管理、コントロールする方法を策定するにあたり、監督当局および金融機関が考慮すべき諸要素を提示することである。バーゼル委員会としては、電子的な小口商品・サービスの技術進歩に関する監督上の問題と対応について検討と議論が進められている中で、本ペーパーがその第一歩になるものと考えている。

バーゼル委員会では、電子バンキング・電子マネー業務のリスク管理に対する適切な監督アプローチの構築に資することを期待して、本ペーパーを世界中の監督当局に配布する。監督当局の中には、その管轄下の金融機関に対し本ペーパーの配布を希望する先もあろう。

電子バンキングと電子マネーの技術は急速に変化しており、将来の商品やサービスが今日利用可能なものとはかなり異なると考えられるため、ここでの議論は一般的なものとならざるをえない。電子バンキング・電子マネー業務の中には、比較的発展の初期段階にあるものがみられるため、リスクの多くの側面は、必ずしも完全には認識されていないほか、その測定が容易

にできない状況にある。早計な規制的アプローチをとることは、こうした分野におけるイノベーションや創造性を阻害する危険を冒すこととなる。したがって、監督当局としては、既知の重大なリスクに対処するのに十分厳格かつ包括的であり、そして電子バンキング・電子マネー業務に伴う重大なリスクのタイプ・程度の変化にも十分柔軟に対応できるようなリスク管理プロセスを銀行が策定するよう奨励すべきである。また、リスク管理プロセスは、不断の改訂が行なわれている場合にのみ有効である。

本ペーパーの次節以下の構成は次のとおりである。まず、次節では、電子バンキングおよび電子マネーを定義し、電子マネー業務の担い手としての銀行の主な役割について述べる。続く第2章では、電子バンキングと電子マネーにおいて銀行が直面すると思われるリスクを明らかにする。ここでのリスクの識別・分析は、網羅的であることを目指してはならず、むしろ、銀行が直面すると考えられる問題のタイプを記述することを意図している。分析の結果、こうした問題の中では、オペレーショナル・リスク、評判（reputational）リスクおよび法的リスクの発生可能性が、相対的に高いことが示唆されている（注1）。

電子バンキングと電子マネーの発展が進むに

つれ、国境を越えた銀行と顧客との取引は増加すると考えられる。このような関係は銀行や監督当局に対し、別の論点とリスクを提起すると考えられる。こうした点に鑑み、第2章はクロスボーダー・リスクについても論述する。

リスクの識別・分析に基づき、第3章では電子バンキングや電子マネー業務を行う銀行のリスク管理プロセスにおける主な手順を概説する。こうしたプロセスには、リスクの評価、リスク・エクスポージャーをコントロールするための施策の実施、およびリスクのモニタリングという3つの主要な手順がある。

1. 2. 電子バンキングおよび電子マネーの定義

1. 2. 1 電子バンキングとは、電子的手段による小口・少額の銀行商品・サービスの提供を指す（注2）。このような商品・サービスには、預金受入れ、貸出、口座管理、財務相談、電子小切手による支払い、（後に定義する）電子マネー等その他の電子的な支払商品・サービスの提供が含まれる。

電子バンキングには、業務を行うデリバリー・チャンネルとしての性格と、こうした経路への顧客のアクセス手段という2つの基本的側面がある。一般的なデリバリー・チャンネルの類型としては、「クローズ型」および「オープン型」の

（注1）銀行は、株主の権利の価値に影響を及ぼしうるリスクにも直面すると考えられる。例えば、競合する新技術の選択に際し、銀行の経営陣は、普及せずに終わる技術を選択するリスクを負う。あるいは、他の商品・サービスにうまく適合しない技術を選択することもある。経営陣が行うあらゆる決定の場合と同様に、電子バンキング・電子マネーがもたらす財務的成功に関するリスクは、経営陣と株主にとって最大の関心事である。しかし、監督当局は銀行システムの安全性や健全性の確保には責任をもつが、銀行の収益力確保には責任をもたないため、こうした「株主の価値」という論点は、金融機関の存続性が脅かされない限り、監督当局にとって直接の関心事ではない。したがって、本ペーパーは、電子マネーや電子バンキングのリスクに関するこうした視点には基本的に立入らない。

（注2）本ペーパーは小口の電子バンキングと電子支払サービスに焦点を当てる。大口電子支払いおよび電子的に伝達される他の大口銀行サービスは、ここでの議論の対象外とする。

ネットワークがある。「クローズド・ネットワーク」では、参加条件に関する約定を結んだ参加者（金融機関、顧客、小売店、第三者たるサービス提供者）にアクセスが制限される。「オープン・ネットワーク」にはこのような参加条件がない。現在、顧客に電子バンキング商品・サービスを提供するために幅広く利用されているアクセス機器には、POS端末、ATM、電話、パーソナル・コンピュータ、スマート・カード等がある。

1. 2. 2 電子マネーは、POS端末経由で、または2つの機器間の直接転送で、もしくはインターネット等のオープン・コンピューター・ネットワーク上で、支払いを行う「ストアード・バリュー型」ないしプリペイドの支払メカニズムを指す（注3）。ストアード・バリュー型商品には、「ハードウェア型」ないし「カード

型」の仕組み（「電子財布」とも呼ばれる）と、「ソフトウェア型」ないし「ネットワーク型」の仕組み（「デジタル・キャッシュ」とも呼ばれる）が含まれる。ストアード・バリュー・カードは「単一目的」ないし「多目的」である（注4）。単一目的カード（テレホン・カード等）は、一種類の財またはサービス、あるいは一つのベンダーからの商品の購入に利用される。多目的カードは、幾つかのベンダーからのさまざまな購入に利用される（注5）。

銀行は発行者として電子マネー・スキームに参加すると考えられるが、それ以外の機能も果たすであろう。その中には、他の主体によって発行された電子マネーの流通、小売店の電子マネーによる売上げの換金、電子マネー取引の処理・清算・決済、および取引記録の維持が含まれる。

（注3）幾つかの公的機関がそれぞれに独自の電子マネーの定義を発表している。電子マネーに関する最近のG-10報告書に指摘されているように、技術革新によってプリペイド型電子メカニズムの型の区別が曖昧となっていくこと等もあって、電子マネーの正確な定義付けは困難である（これら一連の研究については、「電子マネーについて——消費者保護、法執行、監督、クロスボーダー問題——（Electronic Money: Consumer protection, law enforcement, supervisory and cross-border issues）」、<G-10電子マネーに関する作業部会、1997年4月>参照）。本ペーパーでは、電子マネーの定義に際し、G-10報告書と「電子マネーのセキュリティ（Security of Electronic Money）」（国際決済銀行、1996年8月）を引用している。後者の報告書は、ストアード・バリュー型商品の技術的な実現方法（technical representation）の区別について説明している。この中で、「残高型（balanced-based）」商品は、残高に対する入金、引落しの記帳により元帳を管理するものであり、「証書型（note-based）」商品は、一定の額面金額を表す「電子紙幣（電子コインやトークンとも呼ばれる）」の相当額を、機器から機器へ移転することにより取引を実行するものである。デビット・カードやクレジット・カードは、小口の電子支払メカニズムであるが、プリペイド型ではないため、電子マネーとはみなされない。

（注4）ストアード・バリュー・カードは、カードに搭載された磁気ストライプやコンピューター・チップの利用により特徴付けられるであろう。コンピューター・チップを搭載したプラスチック・カード（「スマート・カード」として知られる）は、デビットおよびクレジット・アプリケーションといった機能に加え、ストアード・バリュー・アプリケーションも実行するであろう。

（注5）多目的、多機能という言葉は、カードや機器が幾つかのタイプの支払手段（クレジット・カード、デビット・カード、ストアード・バリュー・カード等）として機能することや、こうしたカードが金融取引以外の目的（IDカード、個人の医療情報の保管等）に利用されること、を指しても用いられるようになってきている。用語法の統一が図られていないのは、おそらくは急速な技術革新のためであろう。

第2章 リスクの識別・分析

情報技術は急速に変化しているため、リスクを網羅したリストを作ることはできない。本ペーパーの狙いは、リスク管理の一般的指針を構築する基盤として、幾つかの代表的なリスクについて幅広く説明することである。電子バンキングや電子マネー業務を行う銀行が直面する個々のリスクは、バーゼル委員会によるリスク管理に関する他のペーパーで論述されたリスク・カテゴリーに従って分類可能であり、この意味で、これらのリスクは目新しいものではない(注6)。このような方法によるリスクの分類は、金融機関におけるリスクを系統的に識別する上で役立つであろう。別添は、電子バンキング・電子マネー業務において銀行が直面すると考えられる個々のリスクと問題の例を、リスク・カテゴリーに従って分類して示したものである。

電子バンキングや電子マネーがもたらすリスクの基本的なタイプは目新しいものではないが、幾つかのリスクが生じる特定のパターンや、そうしたリスクが銀行に及ぼす影響の大きさは、銀行および監督当局にとって新しいものであると考えられる。銀行が直面すると考えられるリスクや問題の中には、電子マネーと電子バンキングの両者に当てはまるものもある。しかし、それがどの程度当てはまるかは、それぞれの電子マネー・電子バンキング業務によって異なる。

現段階では、オペレーショナル・リスク、評判リスク、法的リスクが、ほとんどの電子バンキング・電子マネー業務において——特にさまざまな国際業務を行う銀行にとって——重要なリスク・カテゴリーであろうとみられる。この後の3つのセクションでは、これらのリスクの顕れ方について議論する。個々の問題の中には、複数のリスク・カテゴリーに跨るものもある。例えば、顧客情報への無権限アクセスを許すようなセキュリティ侵害は、オペレーショナル・リスクに分類されうるが、このような事態は、銀行を法的リスクや評判リスクにも晒すことになる。仮りにこれらの異なるタイプのリスクが一つの問題から生じる場合でも、適切なリスク管理のためには、それぞれのリスクに対処するための幾つかの方策が必要になると考えられる。その他のリスク(信用リスク、流動性リスク等)もまた、ある種の電子バンキングや電子マネー業務にとって重要であると考えられるが、これらについては後述する。さらに、潜在的なクロスボーダー・リスクについても言及する。

2. 1. オペレーショナル・リスク

オペレーショナル・リスクは、システムの信頼性・完全性が著しく損なわれることに伴う損失の可能性から生じる。銀行は外部または内部から自行のシステムや商品に対する攻撃を受け

(注6) 例えば、「金融派生商品のリスク管理に関するガイドライン (Risk Management Guidelines for Derivatives)」(バーゼル銀行監督委員会、1994年7月)、「実効的な銀行監督のためのコアとなる諸原則 (Core Principles for Effective Banking Supervision)」(バーゼル銀行監督委員会、1997年9月、『日本銀行月報』1997年10月号に掲載)参照。後者のペーパーは、8つのリスク・カテゴリー、すなわち、信用リスク、カントリー・リスクないし移転リスク、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、法的リスク、評判リスクについての基本的な議論を含んでいる。「G-10諸国の決済システム (Payment Systems in the Group of Ten Countries)」(国際決済銀行、1993年12月)では、銀行システムおよび決済システムにおけるリスクを定義している。

る可能性があるため、セキュリティに留意することが不可欠である。オペレーショナル・リスクは、顧客による誤用や、不適切に設計・構築された電子バンキングおよび電子マネー・システムからも生じうる。こうしたリスクが顕現化するパターンの多くは、電子バンキングと電子マネーの双方に当てはまる。

2. 1. 1 セキュリティ・リスク

オペレーショナル・リスクは、銀行の重要な勘定系システムやリスク管理システム、他の主体との通信情報へのアクセス管理に関して発生するほか、電子マネーの場合には、銀行が偽造の防止や検知のために用いる方策に関して発生する。銀行システムへのアクセス管理は、コンピュータの性能向上、アクセス・ポイントの地理的な広がり、インターネット等の公衆ネットワークを含むさまざまな通信経路の利用により、急速に複雑化してきている。電子マネーに関しては、セキュリティ侵害が銀行債務の不正な創出につながりうる点に留意することが重要である。その他の形態の電子バンキングに関しては、不正なアクセスが直接的な損失や顧客に対する債務の増加等の問題を生じさせることがある。

また、特定のアクセスや認証に関し、さまざまな問題が起こる可能性がある。例えば、不適切な管理の結果、インターネット上で活動するハッカーが攻撃に成功すれば、顧客の機密情報にアクセスし、これを引出して利用することにもなりかねない。適切な管理がなされなければ、外部の第三者が銀行のコンピューター・システムにアクセスし、ウィルスを感染させる可能性もある。

銀行は、電子マネーや電子バンキング・システムに対する外部からの攻撃に加え、従業員の不正によるオペレーショナル・リスクにも晒されている。従業員は、顧客口座にアクセスするため不正に認証データを入手したり、ストアード・バリュー・カードを盗取する可能性がある。従業員の意図せざるミスもまた、銀行システムを危険に晒すかもしれない。

監督当局にとっての直接の関心事項は、電子マネー偽造による犯罪のリスクである。このリスクは、銀行が適切な偽造の検知・防止対策を施さなければ一層高まる。銀行は、偽造された電子マネー残高の額に相当する責任を負う可能性があるため、偽造によるオペレーショナル・リスクに直面する。また、信頼性が損なわれたシステムの修復に係るコストも生じるとみられる。

2. 1. 2 システムの設計・実現・維持管理

銀行は、自らが選択したシステムが適切に設計・構築されないというリスクに直面する。例えば、銀行は、自らの選択した電子バンキングないし電子マネー・システムがユーザー側の要件と適合しない場合、既存のシステムが中断したり処理が遅延するリスクに晒される。

多くの銀行は、自らの電子マネー・電子バンキング業務の一部の具体化、運営、サポートを外部のサービス提供者や専門家に依存するとみられる。こうした依存関係は、銀行が自分自身では経済的に提供できない電子バンキング・電子マネー業務を部分的に外部委託することを可能にするものである点で、望ましい面をもっていられる。しかし、外部委託への依存は、銀行をオペレーショナル・リスクに晒すことに

なる。サービス提供者は、銀行から期待されているサービスを提供するために必須の専門能力を持合わせていないかもしれないし、タイムリーに技術を改良しないかもしれない。サービス提供者による運営は、システムの故障や財務上の問題によって中断される可能性もあり、その場合、銀行の商品・サービス提供力が脅かされかねない。

情報技術の特徴づける急速な変化は、銀行にとって、システムが陳腐化するリスクをもたらす。例えば、顧客による電子バンキングや電子マネー商品の利用を可能とするコンピューター・ソフトウェアには改良が必要となるが、ソフトウェアの改良版を配布する経路において、犯罪者や悪意をもつ人物が当該ソフトウェアを傍受し改竄してしまう可能性があり、銀行にリスクをもたらす。また、急速な技術変化により、スタッフが銀行の採用する新技術の特徴を完全に把握しきれないこともあろう。このことは、新システムや改良されたシステムに伴うオペレーショナルな問題につながりうる。

2. 1. 3 顧客による商品・サービスの誤用

従来の銀行サービスと同様、顧客による誤用も、それが故意のものであれ不注意によるものであれ、オペレーショナル・リスクの原因となる。銀行がセキュリティ面での予防措置について顧客を適切に教育していない場合、このリスクは高まるであろう。また、適切な取引確認手段がないと、顧客は以前に承認した取引を反復することが可能となり、銀行に金銭的損失を負わせる可能性がある。顧客が安全性の不十分な電子媒体を通じて個人情報（認証情報、クレジット・カード番号、銀行口座番号等）を用いることは、犯罪者に対し顧客口座へのアクセスを許

すこととなりかねない。この結果、銀行は顧客が承認していない取引により、金銭的損失を被ることがありうる。さらに、マネー・ロンダリングも G-10 報告書（「電子マネーについて——消費者保護、法執行、監督、クロスボーダー問題——」、1997 年 4 月）において指摘されているように、懸念の原因となりうる。

2. 2. 評判リスク

評判（reputational）リスクとは、資金調達源や顧客の致命的喪失につながるような、世間一般から重大な否定的評価を受けるリスクである。評判リスクには、銀行が顧客との関係を確立し維持する能力を著しく低下させているといった業務全般に関する否定的イメージを、世間に植えつける行為が含まれると考えられる。また、評判リスクは、銀行が、業務継続上、不可欠な能力を有することへの世間の信頼が、銀行の行為により、大いに損なわれる場合にも生じるであろう。評判リスクは、銀行自身の行為のほか、第三者の行為によっても起こりうる。評判リスクが高まると、他のリスク・カテゴリー、特にオペレーショナル・リスクについてのリスク・エクスポージャー増大や問題の顕現化に直結してしまう可能性がある。

評判リスクは、システムや商品が期待どおりに機能せず、世間に広く否定的反応を引き起こす場合に生じることがある。重大なセキュリティ侵害は、銀行のシステムに対する内部・外部どちらからの攻撃によるものであっても、銀行に対する世間の信頼を低下させる可能性がある。評判リスクは、サービスに関して顧客に問題が生じているケースで、顧客が商品の利用や問題解決手続について十分な情報を与えられていない場合にも生じるであろう。

第三者による誤用や違法行為、不正によっても、銀行は評判リスクに晒されよう。評判リスクは、重大な通信ネットワークの障害により顧客が自分の資金や口座情報にアクセスすることを妨げられたような場合、特に口座へのアクセス手段が他にない場合に顕現化すると考えられる。また、同一ないし類似の電子バンキングや電子マネー商品やサービスを提供する他の金融機関が失敗により多額の損失を生じさせた場合にも、たとえ当該銀行自体が同じ問題に直面していなくても、顧客はその銀行の商品やサービスに疑念を抱くようになるであろう。さらに、評判リスクは銀行を狙った攻撃から生じる可能性もある。例えば、銀行のウェブ・サイトに侵入したハッカーが、当該銀行やその商品についての不正確な情報を故意に広めるため、これを改竄するかもしれない。

評判リスクは個々の銀行にとって重大であるのみならず、銀行システム全体にとっても重大であると考えられる。例えば、世界的規模で活発に活動する銀行が電子バンキングや電子マネー・ビジネスについて大きく評判を損なった場合には、その他の銀行におけるシステムのセキュリティにも疑いが生じるかもしれない。極端な場合、このような状況が銀行システム全体のシステミックな機能停止につながる可能性もある。

2. 3. 法的リスク

法的リスクは、法律やルール、規則、予め定められた慣行に違反することやこれらを遵守しないことから生じるほか、取引当事者間の法的な権利義務関係が確立されていない場合に生じる。多くの小口電子バンキング・電子マネー業

務は比較的新しい性格をもつため、こうした取引における当事者間の権利義務関係は不明確な場合がある。例えば、国によっては、電子バンキングや電子マネー業務に対する幾つかの消費者保護ルールの適用関係が明確でない場合もある。加えて、法的リスクは、電子媒体を通じて形成された合意の有効性が不確実な場合にも生じるであろう。

電子マネー・スキームは、その残高限度額や取引限度額が緩やかで、かつ取引の追跡可能性に限界がある場合に、マネー・ロンダリングをはたらく者にとって魅力的なものとなろう。マネー・ロンダリング・ルールの適用は、幾つかの形態の電子的な支払いにおいては不適切かもしれない。電子バンキングでは遠隔からの操作が可能のため、銀行は従来型の犯罪行為防止・追跡方法を適用する際に一層の困難に直面すると考えられる。

電子バンキング・電子マネー業務を行う銀行は、顧客への情報開示やプライバシーの保護に関して法的リスクに直面する可能性がある。自らの権利義務に関して十分説明を受けていない顧客が、銀行を相手どって訴訟を起こすかもしれない。適切なプライバシー保護がなされない場合にも、国によっては銀行は監督当局による制裁を受けるであろう。

自己のインターネット上のサイトを他のサイトに接続することによって顧客サービスの向上を図ろうとする銀行も、法的リスクに直面する可能性がある。ハッカーが銀行の顧客をだますために、リンクされたサイトを利用するかもしれない。銀行は顧客から提訴される可能性がある。

電子商取引が拡大するにつれ、銀行は電子証明書を用いるシステム等の電子認証システムに

参加しようとするであろう（注7）。認証機関としての役割は、銀行を法的リスクに晒すと考えられる。例えば、認証機関たる銀行は、その証明書を依頼した者に生じた金銭的損失に対する責任を負うかもしれない。また、銀行が新たな認証システムに参加し、かつ契約において権利義務が明確に定められていない場合にも、法的リスクが生じうる。

2. 4. その他のリスク

信用リスクや流動性リスク、金利リスク、マーケット・リスク等、伝統的な銀行業務のリスクも電子バンキング・電子マネー業務から発生すると考えられるが、オペレーショナル・リスクや評判リスク、法的リスクに比べると、銀行や監督当局にとっての重要度は小さいとみられる。これは、電子バンキング・電子マネー業務に特化している銀行や銀行子会社に比べ、さまざまな銀行業務を行っている銀行に特に当てはまるであろう。

2. 4. 1 信用リスクとは、取引相手が履行期およびそれ以降も債務全額を履行しないリスクである。電子バンキング業務を行う銀行は、従来にない手段で与信を行い、従来の地理的境界を超えて市場を拡大するであろう。リモート・バンキングにより信用供与を申込んできた借手に対する信用力審査手続が不適切であれば、

銀行の信用リスクは高まる可能性がある。電子小切手による支払いの仕組みを取扱う銀行は、第三者たる仲介業者が支払いに関し債務不履行に陥った場合、信用リスクに直面するであろう。また、顧客に転売するために発行者から電子マネーを購入する銀行もまた、当該発行者が電子マネーの換金義務を果たせなくなった場合、信用リスクに晒される。

2. 4. 2 流動性リスクとは、銀行が、最終的には債務を履行できると考えられるものの、受容れ難いほどの損失を被ることなくしては履行期到来時に債務を履行できないことから生じるリスクである。流動性リスクは、電子マネー業務に特化する銀行にとって、換金・決済請求をカバーするために十分な資金を常に確保することができない場合、重大と考えられる。加えて、換金請求にタイムリーに対応できない場合には、当該金融機関に対し訴訟が提起され、評判の低下につながる可能性がある。

2. 4. 3 金利リスクとは、銀行の財務状況が不利な方向への金利変動に晒されることを指す。電子マネーの提供に特化する銀行は、不利な方向への金利変動が電子マネー負債残高に対応する資産の価値を減少させる分だけ、重大な金利リスクに直面すると考えられる。

（注7）認証機関によって発行される電子証明書は、ある電子署名がある特定の署名者によって実際に生成されたものであることを確認することを目的としている。認証機関の役割を果たす銀行は、口座へのアクセス機器を提供することや、公証人としての役割を果たすことに付随するサービスと同様のサービスを顧客に提供するものとみなされる。電子署名とは、受信者に対し発信者を特定することを目的とした、電子メッセージに付されたデータのことである。現在、多くの電子署名は暗号アルゴリズムを用いて生成されており、発信者がある関数を用いて署名を作成し、受信者がこれとは異なるが関連する関数を用いて当該署名を確認する。電子署名は通常、メッセージの完全性を証明するメカニズムも提供する。

2. 4. 4 マーケット・リスクは、為替レートを含む市場価格の変動によりオンバランス・シートおよびオフバランス・シートのポジションに生じる損失のリスクである。電子マネーの対価として外貨を受入れている銀行は、このタイプのリスクを被ることとなる。

2. 5. クロスボーダー問題

電子バンキングおよび電子マネー業務は、そもそもの特性として、銀行や顧客が地理的に到達可能な範囲を拡張するための技術に基づいている。このような市場の拡大は、ある種のリスクを際立たせながら、国境を越えて広がる可能性がある。銀行は、現在、国際業務において類似のタイプのリスクに直面しているが、こうしたリスクは、電子バンキングや電子マネーのクロスボーダーでの取扱いにも関係することに留意しておくことが重要である。銀行は、国境を越えて顧客と取引を行う場合、法律上および規制上の異なる要求に直面することとなる。国によっては、インターネット・バンキング等の新しい形態の小口電子バンキングや電子マネーに関する法的な要件が不明確と考えられる場合もある。加えて、それぞれの監督当局が責任をもつべき管轄権の範囲が曖昧である可能性もある。これらの問題点は、消費者保護法や記録保持・報告義務、プライバシーに関する規則、マネー・ロンダリング法を含む、国毎に異なる法律や規則の不遵守という法的リスクに銀行を晒すと考えられる。

オペレーショナル・リスクは、他国に所在するためにモニタリングが困難と考えられるサービス提供者を利用している銀行に生じうる。銀行は、国境を越えて電子バンキング・電子マネー業務を行う場合、他のリスクにも直面しよう。

海外に拠点を有するサービス提供者や電子バンキング・電子マネー業務への海外からの参加者と取引する銀行は、経済的、社会的ないし政治的要因からそれらの取引相手が債務不履行となるカントリー・リスクを被る。インターネットのようなオープン・ネットワークを通じてサービスを提供する銀行は、海外顧客からの信用供与申込を受けることがあるが、既存の顧客に対する方法でこれを評価することがより困難となる点で、信用リスクに晒されよう。電子マネーへの対価として外貨を受入れる銀行は、為替レートの変動によりマーケット・リスクを被ると考えられる。

第3章 リスク管理

多くの銀行にとって、電子バンキング・電子マネー業務を行うことには戦略的な理由があるように思われる。これに加え、電子バンキング・電子マネーの利用拡大は、消費者や小売店に便益をもたらし、銀行および決済システムの効率性を高める可能性がある。同時に、これまでの議論が示すように、電子バンキング・電子マネー業務を行う銀行にはリスクも存在する。リスクは便益に対して釣り合いがとれたものでなければならない。銀行はリスクを管理、コントロールできなければならないし、必要があれば関連するあらゆる損失を吸収できなければならない。また、電子バンキング・電子マネー業務から生じるリスクは、銀行が直面する他のリスクとの関連で評価されるべきである。現在のところ、電子バンキング・電子マネー業務は銀行業務全体の中では比較的小さいかもしれないが、監督当局はそれでもなお、経営陣上層部に対して「銀行の負うこれらのリスク・エクスポージャーにより、基幹システムが脅かされること

はない」ことを保証するよう求めることがある。

技術革新の急速な進展は、電子マネーや電子バンキングにおいて銀行が直面するリスクの性質や範囲に変化をもたらすであろう。監督当局は、銀行に対して、銀行経営陣が現在のリスクに対応し、かつ新たなリスクに適応することを可能にするプロセスをもつことを期待している。リスクの評価、リスク・エクスポージャーの管理、リスクのモニタリングの3つの基本的要素を含むリスク管理プロセスは、銀行や監督当局がこれらの目的を達成するのに役立つであろう。銀行は、電子バンキング・電子マネー業務に新たに取り組む場合や、これらに関する既往の取り組みを評価する際に、こうしたプロセスを活用することが考えられよう。

銀行にとっては、取締役会と経営陣上層部により適切に監視される包括的なリスク管理プロセスを備えておくことが必須である。電子バンキング・電子マネー業務における新しいリスクの識別および評価が行なわれる場合には、取締役会と経営陣上層部は、常にこれらの変化を報告されるようになっている必要がある。新しい業務が開始される場合には、常にこれに先立ってリスク管理プロセスを包括的に見直し、経営陣上層部がこのリスク管理プロセスによって当該業務から生じるいかなるリスクをも適切に評価、管理、モニタリングできることを確認すべきである。

3. 1. リスクの評価

リスクの評価は継続的なプロセスである。これは通常3つの手順を含んでいる。第1に、銀行は、リスクを識別するため、また可能であればこれを定量化するため、精緻な分析プロセス

を採用することがあろう。リスクを定量化できない場合でも、経営陣はなお、潜在的リスクがいかにして生じうるかを明らかにし、それらへの対応や制限のために採用してきた手順を確認することがあろう。銀行経営陣は、リスクが銀行に及ぼしうるインパクト（最大の潜在的インパクトを含む）およびそうした事態が生じる確率の双方の観点から、あらゆるリスクの重大さを合理的かつ防御的（defensible）に判定すべきである。

リスクの評価の第2の段階は、取締役会または経営陣上層部が、ある問題が顕現化した際に銀行がもちこたえうる損失の評価を基に、銀行のリスク許容度を決定することである。最後に、リスク・エクスポージャーが許容範囲内に収まるかを確認するために、経営陣はそのリスク許容度をリスクの重大さの評価と比較することができる。

3. 2. リスクの管理・コントロール

銀行経営陣は、リスクおよびリスク許容度を評価した後、リスクの管理・コントロールという手順を踏むべきである。当該リスク管理プロセスの手順には、セキュリティに係る方針や対策の実施、内部コミュニケーションの調整、商品やサービスの評価・改良、外部委託リスクのコントロール・管理を確実にするための施策の実施、情報開示や顧客教育の提供、コンティンジェンシー・プランの策定等の活動が含まれる。経営陣上層部は、リスク限度の遵守に責任をもつスタッフが、電子バンキング・電子マネー業務を行う部門から独立した権限をもつことを保証すべきである。あらゆる業務に内在するさまざまなリスクをコントロール・管理する銀行の能力は、方針や手続が文書により定められ、全

ての関係スタッフに閲覧可能とされている場合に高まることとなる。

3. 2. 1 セキュリティに係る方針および対策

セキュリティとは、データとオペレーティング・プロセスの完全性、真正性および機密性を守るために用いられる、システム、アプリケーションおよび内部コントロールの組合せのことである。適切なセキュリティは、銀行内部のプロセスや銀行と外部取引先間の通信に対する十分なセキュリティの方針と対策の策定、実施に依存する。セキュリティの方針と対策は、電子バンキングや電子マネー・システムに対する内外からの侵害のリスクのみならず、セキュリティ侵害から生じる評判リスクをも抑制することができる。

セキュリティの方針とは、情報セキュリティの確保を支持する経営陣の狙いを示すとともに、銀行のセキュリティ体系を説明するものである。また、セキュリティの方針は、銀行のセキュリティ・リスクの許容度を定義する指針を確立するものでもある。セキュリティの方針は、情報セキュリティ対策の構想、実施、強制の責任を規定するとともに、方針の遵守状況の評価、規律づけの手段の強制、セキュリティ違反の報告に関する諸手続を定めるものと考えられる。

セキュリティ対策とは、ハードウェアおよびソフトウェアと人事管理の組合せであって、安全なシステムとオペレーションの構築に貢献するためのものである。経営陣上層部は、セキュ

リティが包括的なプロセスであって、その強度はプロセスの中で最も脆弱な部分によって決定されることを認識すべきである。銀行は、内外からの侵害および電子バンキングや電子マネーの誤用を防止・削減するために、さまざまなセキュリティ対策を選択することができる。これらの対策には、例えば暗号化、パスワード、ファイアーウォール、ウイルス・コントロール、従業員審査が含まれる。暗号化とは、暗号アルゴリズムを利用して、無権限者が内容を見ることを防止するために、平文を暗号文に変換することである（注8）。パスワード、パスフレーズ、個人識別番号（PIN）、ハードウェア型トークン、バイオメトリクス（生物測定法）は、アクセスを制御し使用者を特定するための技術である。

ファイアーウォールは、インターネット等のオープン・ネットワークと接続された内部システムへの外部からのアクセスをふるい分け、制限するハードウェアとソフトウェアの組合せである。ファイアーウォールは、インターネット技術を用いた内部ネットワーク（イントラネット）をも分離することがある。ファイアーウォール技術は、適切に設計・運営されれば、アクセスを制御しデータの機密性・完全性を守るための効果的な対策となりうる。この技術は仕組みが複雑でコストがかかる可能性があるため、その強度と性能は保護される情報の機密性と釣合いのとれたものとすべきである。その設計にあたっては、組織全体としてのセキュリティ要件、明確なオペレーション手続、任務分掌、ファイアーウォールの構築・運営に責任をもつ信頼

（注8）暗号化に関する詳細な議論については、「電子マネーのセキュリティ」（国際決済銀行、1996年8月）、特に暗号に関する第4章1. 2を参照。

できるスタッフの選定等をよく考慮する必要がある。

ファイアーウォールは外部からのメッセージをふるい分けるものではあるが、インターネットからダウンロードされたウィルス感染プログラムに対する防御策になるとは限らない。このため、経営陣は、特にリモート・バンキングに関して、ウィルス侵入やデータ破壊の可能性を削減するための防御・検知策を講じるべきである。ウィルス感染リスクを低減させるためのプログラムには、ネットワーク管理、エンドユーザーに関する方針、ユーザー研修およびウィルス検知ソフトウェアが含まれるであろう。

セキュリティに対する脅威は全て外部からもたらされるわけではない。電子バンキングや電子マネー・システムは、現在および過去の従業員による無権限行為からも可能な限り防御されるべきである。既存の銀行業務の場合と同様、新規従業員、臨時従業員およびコンサルタントに対する素性調査は、内部管理および任務分掌とともに、システムのセキュリティを守るための重要な予防策である。

電子マネーにおいては、追加的なセキュリティ対策が、偽造やマネー・ロンダリングを含む侵害や誤用を抑止するのに役立つと考えられる(注9)。このような対策には、発行者ないし中央オペレーターとのオンライン交信、個々の取引のモニタリングと追跡、中央データベースにおける累積記録の維持、ストアード・バリュー・カードや小売店のハードウェアに装備された耐タンパー機器の使用、ストアード・バリュー・カードにお

ける価値限度額と有効期限の使用が含まれる。

3. 2. 2 内部コミュニケーション

もし経営陣上層部が、主要なスタッフに対して電子バンキングや電子マネーの提供が銀行の全般的な目的をいかにサポートするよう意図されているかを伝達するならば、オペレーショナル・リスク、評判リスク、法的リスクおよびその他のリスク(訳注:信用リスク、流動性リスク等)の多くを管理・コントロールすることが可能になる。同時に、技術スタッフは、経営陣上層部に対してシステムの強さや弱さのほか、システムがどのように稼働するよう設計されているかを明確に伝えるべきである。このような手続は、銀行組織内のさまざまなシステムの互換性のなさやデータ完全性の問題といったシステム設計の欠点に起因するオペレーショナル・リスク、システムが期待どおりに稼働しなかったという顧客の不満に伴う評判リスク、さらに信用リスクや流動性リスク等を削減することができる。

適切な内部コミュニケーションを確保するためには、全ての方針や手順は文書により提供されるべきである。これに加え、経営陣上層部は、スタッフや経営陣の専門能力の欠如から生じるオペレーショナル・リスクを抑制するため、技術革新のペースに合わせて技術・知識を継続的に教育し向上させることを企業の方針として採用すべきである。こうした研修には、技術課程のほか、スタッフが重要な市場の進展をフォローするための時間も含まれよう。

(注9) 電子マネーのセキュリティ対策に関する議論の詳細については、「電子マネーのセキュリティ」(国際決済銀行、1996年8月)参照。本報告書においては、ある単一の特定の対策に依存するよりも、複数のセキュリティ対策を組み合わせることが、電子マネーのセキュリティ問題を防止するにおそらく最も効果的であると結論づけられている。

3. 2. 3 評価および改良

商品やサービスが広範に導入される前にその評価を行うことも、オペレーショナル・リスクや評判リスクの削減に役立ちうる。テストは、装置やシステムが適切に機能し、要求したとおりの結果を生むことを証明するものである。パイロット計画やプロトタイプは新しいアプリケーションの開発に役立つ可能性がある。システムの処理遅延や障害のリスクも、現行のハードウェアやソフトウェアの性能を定期的に見直す方針によって削減されうる。

3. 2. 4 外部委託

銀行業界では、戦略的な観点から得意分野に業務を絞り、専門能力のない業務については外部の専門業者に依存する傾向が高まりつつある。こうした外部委託の取決めはコスト削減や規模の経済といった便益をもたらすかもしれないが、一方で、銀行は外部委託を行ったとしても、その業務に影響を及ぼすリスクの究極的な管理責任から免れるものではない。したがって、銀行は外部のサービス提供者への依存から生じるリスクを削減するような方針を採用すべきである。例えば、銀行経営陣はサービス提供者の業務遂行状況や財務状況をモニターすべきである。また、これとの契約関係や各当事者の期待や義務が明確に理解され、かつ法的に有効な書面の契約により定義されるようにすべきである。さらに必要であれば、速やかにサービス提供者を変更するための緊急時の取決めを維持すべきである。

銀行の機密情報に関するセキュリティは極めて重要である。外部委託の取決めによって、銀行は機密情報をサービス提供者と共有せざるをえない可能性がある。銀行経営陣は、機密デー

タを保護するためのサービス提供者の方針や手続を見直すことを通じ、サービス提供者が委託事務が行内で行われる場合と同程度のセキュリティ・レベルを維持する能力をもつか否かを評価すべきである。これに加え、監督当局は、必要に応じサービス提供者の能力や業務遂行状況、財務状況を独自に評価する権限を求めることがあろう。

3. 2. 5 情報開示および顧客教育

情報開示や顧客教育は、銀行が法的リスク、評判リスクを削減するのに役立つであろう。情報開示や新しい商品・サービスの利用法、利用料金、問題解決策・エラー修復手順を扱った顧客教育プログラムは、銀行が顧客保護やプライバシーに関する法規制を遵守するのに有用と思われる。また、情報の開示や銀行にリンクされたウェブ・サイトとの関係を説明することは、銀行にとって当該サイト上のサービス・商品に関する問題から生じる法的リスクを削減する上で有用と考えられる。

3. 2. 6 コンティンジェンシー・プランの策定

銀行は、電子バンキングや電子マネーのサービス提供にあたって、障害が発生した際の措置を定めたコンティンジェンシー・プランを策定することにより、内部プロセスやサービス・商品の提供における障害発生リスクを削減できる。こうしたプランには、データ復旧や代替的データ処理能力、緊急時の人員配備、顧客サービス・サポートを規定することとなろう。バックアップ・システムについては、それが引続き有効であることを確認するため、定期的にテストすべきである。また、銀行は、自らの緊急時の業務が通常業務と同様に安全であることを確

認すべきである。

電子バンキングや電子マネーにおいては、ハードウェアのベンダー、ソフトウェア・プロバイダー、インターネットのサービス・プロバイダー、通信会社等の外部業者への依存が重要な側面となっている。銀行経営陣は、こうしたサービス提供者がバックアップ能力を保持するように主張することがあろう。また、経営陣は、サービス提供者が機能不全に陥った場合に採りうる補償措置を検討することも考えられる。このようなプランには、他のプロバイダーとの短期契約、サービスの障害から生じる顧客の損失への対応を定めた方針が含まれるであろう。銀行は、必要があればサービス提供者を速やかに変更する権利を留保しておくことが望ましいか否かを検討すべきである。

また、コンティンジェンシー・プランの策定は、銀行自身の行動から発生する評判リスクや同一ないし類似の電子バンキングや電子マネー商品・サービスを提供する他の金融機関で起きた問題が惹起する評判リスクを削減するのに役立つと考えられる。例えば、銀行は、システム障害の間の顧客問題への対応手続を確立することを望むこともありうる。

3. 3. リスクのモニタリング

継続的なモニタリングは、いかなるリスク管理プロセスにおいても重要な側面である。電子バンキング・電子マネー業務については、その業務の性質が技術革新の出現につれ急速に変化すると考えられること、またインターネット等のオープン・ネットワークの利用に依存する商品もあることから、モニタリングがとりわけ重要である。モニタリングの2つの重要な要素は、システムのテストと監査である。

3. 3. 1 システムのテストと監視

システムの運行テストは、異常な取引パターンを検知し、主要システムの問題、障害、外部からの攻撃を防止するのに有用である。外部侵入（penetration）テストとは、通常の手続によらずシステムへの侵入を一定の条件下で試みることにより、セキュリティ・メカニズムの構築・運営上の欠陥を特定し、切り離し、確認することにより焦点を当てたものである。監視（surveillance）とは、取引を追跡するためにソフトウェアや監査用アプリケーションを用いて行うモニタリングの一形態である。監視は、外部侵入テストに比べ、通常の運行モニタリング、異常の調査、セキュリティ対策の遵守状況をテストすることによるセキュリティの有効性の継続的判断に力点が置かれている。

3. 3. 2 監査

（内部および外部）監査は、電子バンキングや電子マネー・サービスの提供において、欠陥の検知とリスクの削減のための重要で独立した統制の仕組みを提供する。監査役の役割は、適切な基準、方針、手続が策定され、銀行が常にこれに従うことを確保することである。監査スタッフは、正確な評価を行うため十分な専門知識をもたなければならない。内部の監査役は、リスク管理に関する決定を行う従業員とは別に、独立して設けられるべきである。内部監査を向上させるため、経営陣は、コンピューター・セキュリティのコンサルタントや関連の専門能力を有する専門家等、質の高い外部監査役に対して、電子バンキング・電子マネー業務に関する独立した評価を下すよう求めることがあろう。

3. 4. クロスボーダー・リスクの管理

クロスボーダー・リスクは、銀行が自国内で直面するリスクよりも複雑かもしれない。したがって、銀行および監督当局は、クロスボーダーの電子バンキング・電子マネー業務から生じるオペレーショナル・リスク、評判リスク、法的リスク、その他のリスク（訳注：信用リスク、流動性リスク等）の評価、管理、モニタリングに追加的注意を払う必要があると考えられる。

異なる国の市場の顧客にサービスを提供する銀行は、各国が要求する法的要件を理解し、商品やサービスに対する顧客の期待・知識が国によって異なるという認識を培う必要がある。また、経営陣上層部は、与信・流動性管理のための既存のシステムがクロスボーダー取引から生じうる問題点を考慮したものになっていることを確認すべきである。銀行はカントリー・リスクを評価し、海外の経済・政治状況に起因す

るサービスの支障を考慮したコンティンジェンシー・プランを策定する必要があると思われる。また、銀行は、海外のサービス提供者の債務の履行を強制する場合、困難に直面する可能性がある。海外に所在するサービス提供者に銀行が依存する場合、各国監督当局は、個々のケースに応じて、クロスボーダー・サービス提供者がもつ情報へのアクセスの容易さを評価することや、その活動を検討することを求めるかもしれない。

各国の監督当局は、管轄権に関する曖昧な点を発見し、議論することによって、重要な役割を果たすことができる。また、各国当局は、危険で違法な慣行を発見するための措置を講じる努力を続けることができる。最後に、各国当局は、商品・サービスの技術革新や業界慣行に関する情報を共有するための協調を継続し、かつ強化することができる。

別添 小口電子バンキングおよび電子マネーにおいて想定されるリスクとリスク管理策の例

以下の表は、電子バンキングおよび電子マネー業務を行うに際し、銀行が直面するリスクの例を示すとともに、こうしたリスクの管理に銀行が利用可能な対策を記したものである。なお、このリストは網羅的なものではなく例示的なものである。ここで挙げられているリスク管理策は、国内または国際的な監督政策を反映したものと解されるべきではない。

小口電子バンキングおよび電子マネーにおいて想定されるリスクとリスク管理策の例

想定されるリスク例	想定される顕現化パターン	金融機関への潜在的な影響	想定されるリスク管理策
オペレーショナル・リスク			
システムへの無権限アクセス	ハッカーが内部システムに侵入。無権限の第3者が、顧客の機密情報を傍受。銀行システムがウイルス感染。 銀行のシステムおよびデータの意図的な変造・破壊。	データの喪失。顧客情報の盗取・書替え。行内コンピューター・システム重要箇所の機能停止。システム修復に係るコスト。 銀行システムの安全性に対する疑念や世間からの否定的評価を引起す可能性。	脆弱な箇所への外部侵入テスト。使用時における異常検知のための監視。ファイアウォール、パスワード管理、暗号技術、エンドユーザーの適切な認証等通信上のセキュリティ対策の実施。 ウイルス・チェックの実施、内部システムにおけるセキュリティ対策の継続的モニタリングの実施。
従業員の不正	一般銀行口座からの資金引出しや、記録からの情報入手を目的とした従業員によるデータの変造。従業員によるスマート・カードの盗取。	顧客に生じた損失の補填および正確な顧客データの回復に係るコスト。見合いの前払資金を受領していない電子マネーの換金に伴う損失発生の可能性。顧客が銀行に対して不信感を抱く可能性。銀行が法律・規制上の制裁や世間から否定的評価を受ける可能性。	新規従業員を十分に審査するための方針確立。任務分掌等を明示した内部管理策の実施。従業員の事務処理に対する外部監査。スマート・カードの保管・製造等の適切な管理。
電子マネーの偽造	対価を支払わずに商品や資金を入手することを目的とした、犯罪者による電子マネー商品の変造・複製。	銀行が偽造された電子マネー相当額の責任を負う可能性。損なわれたシステムの修復に係るコストが発生する可能性。	発行者や中央オペレーターとのオンライン交信、個々の取引のモニタリング・追跡、中央データベースにおける累積記録の維持、ストアード・バリュー・カードや小売店のハードウェアへの耐タンパー機器の装備、監査証跡の確立。低い充填限度額が、犯罪者の偽造インセンティブを削ぐ可能性。

想定されるリスク例	想定される顕現化パターン	金融機関への潜在的な影響	想定されるリスク管理策
サービス提供者によるリスク	サービス提供者が銀行の期待するサービスを提供しない可能性。システムやデータの完全性・信頼性が損なわれる可能性。	サービス提供者が引き起こした問題について、銀行が顧客に対して説明責任をもつ可能性。	サービス提供者との契約に際して然るべき注意を払う。事務処理に関する基準を定め、緊急時対応や監査に関する条項を含むサービス提供者との契約を作成。サービス提供者に関するバックアップ体制の確立、代替的サービス提供者との契約締結等のコンティンジェンシー・プラン策定。
システムの陳腐化	取引処理の遅延や障害。システムやデータの完全性・信頼性の毀損。	世間からの否定的反応。誤取引から訴訟が提起される等の法的影響が発生する可能性。顧客に生じた問題の解決に係るコスト。	現行のハードウェア・ソフトウェアの性能の定期点検。システム・機器の改良に関する責任体制の確立。
スタッフおよび経営陣の専門能力の陳腐化	急速な技術変化により、銀行の経営陣やスタッフが、銀行の採用する新技術の特徴やサービス提供者の提供する技術改良について、完全に理解できない可能性。	新技術の不十分な実施。継続的サポートの提供停止。システムやデータの完全性・信頼性の毀損。	継続的な手順として、研修の位置付けを組織的に明確化。経営陣・スタッフに対する研修手順を計画段階から構築。
セキュリティに関する認識不足に伴う顧客の不適切な行動	顧客が、安全性の不十分な電子媒体を通じて、個人情報（クレジットカード番号、銀行口座番号等）を使用。犯罪者が、機密情報として取扱われるべきこれらの情報を盗取して顧客口座にアクセス。	無権限取引による金銭的損失。	安全性の不十分な取引における情報保護の重要性に関し、顧客に対して情報提供を行う。商品・サービスへのセキュリティ対策の導入。
顧客による取引否認	取引を完了した顧客が、その取引の存在を否認し、資金の払戻しを請求。	顧客による取引承認の立証に係る費用。立証されない場合、損失発生の可能性。	個人識別番号等、顧客認証能力を向上させるセキュリティ対策の導入。監査証跡の確立。
評判リスク			
重大かつ広範なシステム障害	顧客による資金・口座情報へのアクセスに障害が発生。	顧客が商品・サービスの利用を中止する可能性。直接影響を受けた顧客が銀行を離れ、問題が公となった場合、他の顧客もこれに追随。	導入前のシステム・テスト。システム停止中に顧客に生じた問題への対応を含むバックアップ体制やコンティンジェンシー・プランの策定。
重大なセキュリティ侵害	銀行システムがウィルスに感染、システムおよびデータの完全性に重大な問題が発生。ハッカーが内部システムに侵入。	顧客が商品・サービスの利用を中止する可能性。直接影響を受けた顧客が銀行を離れ、他の顧客もこれに追随。	外部侵入テストおよびその他の適切なセキュリティ対策の整備。コンティンジェンシー・プランの策定。 ウィルス・チェックの実施。
他の金融機関が提供する同一ないし類似のシステム・商品に生じた問題や誤用	他行での問題発生に伴い、自行為提供する電子マネーに対しても顧客の疑念が発生。	顧客が銀行を離れる可能性。	コンティンジェンシー・プランの策定。

想定されるリスク例	想定される顕現化パターン	金融機関への潜在的な影響	想定されるリスク管理策
法的リスク			
法律・ルール of 適用に関する不確実性・曖昧さ	銀行が意図せずして法律に抵触する可能性。既存の消費者保護、マネー・ロンダリング、署名に関するルールの適用について、不明確である可能性。	銀行が法律関係の支出を余儀なくされたり、規制上の制裁を受ける可能性。	電子マネーおよび電子バンキング業務を行う以前に、法的な不確実性のある分野を確認しておく。法的な不確実性に対するリスク許容度を慎重に判断。法律等の遵守状況の定期的点検。監督当局に対する説明の要求。法律等の遵守に関する研修の見直し。コンティンジェンシー・プランの策定。
マネー・ロンダリング	マネー・ロンダリング等の犯罪行為を行おうとする顧客により、銀行の電子バンキングまたは電子マネー・システムが、不正使用される可能性。	「顧客情報の把握（“know your customer”）」に関する法律違反に伴う制裁。	顧客の確認・審査技術を整備。監査証跡の確立。疑わしい行為の発見・報告に関する方針・手続の構築。電子マネーにおいては、低い充填限度額が、マネー・ロンダリングに対するインセンティブを削ぐ可能性。法律等の遵守状況の定期的点検。法律等の遵守に関する研修の見直し。コンティンジェンシー・プランの策定。
顧客への不十分な情報開示	顧客が、例えば紛争解決手続など、自らの権利義務関係について完全には理解していない可能性。このため、顧客が商品・サービスの利用に際し適切な注意を払わない可能性。	損失や、紛争の生じた取引の結果、顧客が銀行を提訴する可能性。銀行は規制・法律上の制裁を受ける可能性。	電子マネーおよび電子バンキング業務を行う以前に、適切な情報開示のあり方を確認。顧客に生じる可能性のある典型的な問題点を把握するための従業員研修。顧客にリスクが生じる可能性のある分野に関し、法律上要求されている最低水準を満たす情報開示を行うことの費用と便益を慎重に比較衡量。一般に開示する商品情報の考案および情宣。規制上の要件を定期的に見直す手続の構築。
顧客プライバシー保護の失敗	銀行が、顧客の承認なしに、顧客の金融取引パターンに関する情報を開示。	顧客から提訴された場合、銀行に訴訟関連費用が発生。銀行は、法律・規制上の制裁を受ける可能性。	プライバシー保護に関する方針の点検。プライバシー保護手続に関する従業員研修。セキュリティ対策の実施。法律等の遵守状況の定期的点検。法律等の遵守に関する研修の見直し。

想定されるリスク例	想定される顕現化パターン	金融機関への潜在的な影響	想定されるリスク管理策
リンクされたインターネット・サイトにおける問題	銀行が、自行のウェブ・サイトを、補完的な商品を提供する主体のウェブ・サイトとリンクさせる可能性。この場合、リンクされたサイトが銀行の顧客を失望させたり詐取する可能性。	銀行が顧客から提訴される可能性。	他のサイトとのリンクがもたらす法的影響やセキュリティ面のリスクを十分に理解する。銀行の役割や、リンクされたサイトで提供される商品に対する保証の扱いについての消費者の混乱を防止するため、消費者に適切な情報開示を行う。リンクされたサイトで利用可能な商品・サービスの品質について、銀行のサイトには表示しない。
認証機関のリスク	偽造された証明書が銀行の名で発行され、顧客を詐取。適切な本人確認なしに、銀行の顧客を装う者に証明書を発行。	信頼性の損なわれた証明書の取消・再発行に係るコスト。偽造証明書、または不正に入手された証明書を受領した者が、銀行を提訴する可能性。評判の低下。	適切なセキュリティ対策・管理の実施。
海外法管轄へのエクスポージャー	インターネット上でサービスを提供する銀行が、海外の顧客を獲得した結果、異なる法律・規制上の要件に服さざるをえなくなる可能性。各国当局の法管轄権の責任範囲が不明確。銀行が発行または取扱った電子マネーが、同行が免許を取得した国の外で使用される可能性。	銀行が他国における法規制に違反する可能性。銀行が予期せぬ法律関係の支出を余儀なくされる可能性。	電子マネーや電子バンキング業務が国境を越えて利用されると見込まれる程度を確認し、法律・法管轄権に関する不確実性に対する銀行の対応力を慎重に判断すること。各国の法規制状況に関する従業員研修。
信用リスク			
リモート・バンキングにより信用供与を申し込んできた借手の破綻	銀行が、通常のマーケットの外側で、データ入手が不可能またはコストがかかる顧客に対して信用供与を承認する可能性。	不良化した貸出に対する予期せぬ引当が必要となる可能性。	リモート・バンキングを通じた顧客に対する、従来の要件に則った信用力審査の確保。貸出の決定・手続の監査。
電子マネー発行者の破綻	銀行が顧客への転売または換金のために電子マネーを保有している間に、発行者が支払不能に陥る可能性。	発行者破綻時に、銀行が自行の顧客が保有する電子マネーの換金に、自己資金で応じなくてはなくなる可能性。	電子マネー・システムへ参加する前に、発行者に対し然るべき注意を払う。発行者の財務状況のモニタリング。破綻発生時のコンティンジェンシー・プランの策定。
流動性リスク			
電子マネー発行者の流動性不足	電子マネー換金請求の急増。電子マネーに特化した銀行において問題となる可能性。	銀行がよりコストのかかる資金源から資金を調達する結果、損失を被る可能性。流動性問題が一般的に認識されると、預金の引出しや電子マネーの換金がより広範化する可能性。換金請求にタイムリーに対応できない場合、評判の低下にもつながる可能性。	流動性の高い資産への投資。使用状況に関するモニタリング・システムの構築。定期的かつ包括的な監査の実施。

想定されるリスク例	想定される顕現化パターン	金融機関への潜在的な影響	想定されるリスク管理策
金利リスク			
電子マネー発行者の投資資産における予期せぬ金利変動	不利な方向への金利変動により、電子マネーの負債残高に対応する資産価値が減少する可能性。電子マネーに特化した銀行において問題となる可能性。	資産価値の予期せぬ減少により、銀行が規制上の要件を遵守できなくなる可能性。流動性問題が発生する可能性。	銀行のエクスポージャーに合った金利リスク管理策の設定。
マーケット・リスク			
電子マネーの対価として外貨を受入れるに伴う外為リスク	不利な方向への為替レート変動により、銀行が損失をカバーする必要がある可能性。	収益に対するマイナスの影響。	外為リスク管理やヘッジ・プログラムの確立。
カントリー・リスク			
海外を拠点とするサービス提供者や、電子マネー・電子バンキングへの海外参加者から発生する移転リスク	海外のサービス提供者や電子マネー・電子バンキングへの参加者が、経済的・社会的・政治的要因により債務を履行できなくなる可能性。	顧客に生じた問題の解決に係るコスト。銀行は顧客から提訴される可能性。	カントリー・リスク評価の実施。他の潜在的参加者と契約を締結するコンティンジェンシー・プランの策定。

バーゼル銀行監督委員会
(信用機構室)