

(仮訳)

電子バンキンググループの活動の趣旨および白書

**Electronic Banking Group Initiatives
and White Papers**

バーゼル銀行監督委員会

**バーゼル
2000年10月**

バーゼル銀行監督委員会・電子バンキンググループ

議長：

Mr John D. Hawke, Jr. – Comptroller of the Currency, Washington, D.C.

Commission Bancaire et Financière, Brussels	Mr Koen Algoet Mr Jos Meuleman
Office of the Superintendent of Financial Institutions, Ottawa	Ms Judy Cameron Mr Brad Sullivan
Commission Bancaire, Paris	Mr Alain Duchâteau Mr Jérôme Deslandes
Deutsche Bundesbank, Frankfurt am Main	Ms Magdalene Heid Mr Andi Kloefer
Bundesaufsichtsamt für das Kreditwesen, Berlin	Mr Uwe Neumann
Banca d'Italia, Rome	Mr Filippo Siracusanò
日本銀行、東京	森 俊彦 桑原 啓彰 鈴木 知子
金融庁、東京	小島 一夫
Commission de Surveillance du Secteur Financier, Luxembourg	Mr David Hagen
De Nederlandsche Bank, Amsterdam	Mr Erik Smid
Eidgenössische Bankenkommision, Bern	Mr Michael Kunz
Financial Services Authority, London	Mr Jeremy Quick Ms Katy Martin
Federal Deposit Insurance Corporation, Washington, D.C.	Mr Michael Zamorski Mr John Carter
Federal Reserve Bank of New York	Mr George Juncker Mr Christopher Calabia Ms Barbara Yelcich
Federal Reserve Board, Washington, D.C.	Ms Heidi Richards Mr Jeff Marquardt
Office of the Comptroller of the Currency, Washington, D.C.	Mr Hugh Kelly Mr Clifford Wilke
Secretariat of the Basel Committee on Banking Supervision, Bank for International Settlements	Mr Jean-Philippe Svoronos
Observers:	
European Central Bank, Frankfurt am Main	Mr Michael Olsen
European Commission, Brussels	Mr Patrick Brady

活動の趣旨の概要

バーゼル銀行監督委員会・電子バンキンググループ

2000年10月

電子バンキンググループ（Electronic Banking Group、EBG）の作業計画には、電子バンキング業務に関する健全な監督ガイダンスを設定・共有するために銀行監督当局は積極的に協力し合うべきである、との共通認識が反映されている。こうした努力は、電子バンキングに対する世界各国の銀行監督当局の監督アプローチを調和させるための礎となろう。また、こうした努力は、銀行サービスを電子的に提供するための効率的な市場の発展を妨げる要因を減じることにもつながるであろう。

EBGは、電子バンキングが未だ初期の段階にあることを考慮し、技術革新を制限しかねない規制色の強い提言や規範的な基準を提示することは不適切であると考えます。従って、EBGの現段階における作業計画は、監督当局による問題の分析と対話を支援することを主眼とし、それによって電子バンキング業務に対する健全性監督の枠組みが発展してゆくことを期待するものとなっている。合理的な健全性基準は、銀行業界および同業界のサービスを楽しむ消費者を利するであろう革新や競争を阻害することなく、安全かつ健全に業務が遂行されるようなものでなければならない。

こうした観点から、EBGの活動は以下の項目に焦点を当てたものとなる。

1. EBGは、今日までに行われた作業や現在進行中の作業を踏まえ、電子バンキング業務における慎重なリスク管理のあり方を指し示す原則（guiding

principles) を策定する

本ガイダンスは、特に電子バンキングを対象として、バーゼル委員会の既存のリスク管理原則を延長したものに相当する。本ガイダンスは、電子バンキングに係るリスクを認知・査定・管理・統制する際に銀行がどのようなアプローチを採ることが望ましいかについて、監督当局が銀行に期待すべき事柄を概説したものである。

EBG は本作業の一環として以下のことを行う。

- ・ 銀行業界と協力し、テクノロジーのアウトソーシング、ネットワークとデータのセキュリティ、および急速に進展するその他の分野において、健全なリスク管理実務を把握し、その適用を促進する。
- ・ 新しいテクノロジーおよび生成する電子バンキングのビジネスモデルが銀行業界に及ぼす潜在的な影響を継続的に分析する。情報サービスやテクノロジー関連企業の金融部門への参入も含めた状況展開は、銀行の商品・サービスのグローバル化および均一化（commoditization）を加速する可能性があり、その結果、銀行業界のみならず商取引全般に多大な影響が及ぶことが予想される。

銀行および銀行監督当局の間には、電子バンキング業務に対しては伝統的な銀行業務と同様のアプローチで臨むべきであるという一般的な了解があるが、電子バンキングの特殊な性質を考えれば、なお分析と継続的な検討が必要である。テクノロジーの変化が急速であること、および、銀行がアウトソーシングや業務提携のかたちでサービス・プロバイダーに依存する傾向にあるため、一部の伝統的リスクは様相を変えたり拡大したりする可能性がある。

電子バンキングに対する監督プロセスは、状況変化に対応し得るよう十分に動的でなければならない。テクノロジーのアウトソーシングに係る管理やデュー・ディリジェンス、セキュリティ管理、金融サービスと非金融サービス

のウェブサイト上でのリンク、アグリゲーション (aggregation)¹など、電子バンキングを巡る重要な諸問題は、銀行監督当局と銀行業界代表との間で協力的な意見交換を行うことが有益であることを示している。

2. EBG は、クロスボーダー電子バンキング業務の適切な監督を支援するため、バーゼル委員会が公表した既存のガイダンスを修正する必要があるか、また、必要があるとすればどの点かを判断する

EBG は、標記の努力の一環として、如何なるクロスボーダー銀行業務に対して現地当局の承認を求め、また現地規制を適用するかについて、各国監督当局が採用し得る様々なアプローチについての実務的な意味合いを検討する。

ウェブ・サーバー、バックオフィス処理、その他の技術サポートを含め、電子バンキング事務が地元 (ないし母国) の法域外において行われる可能性を展望すると、母国当局と現地当局が協力し、電子的に行われるクロスボーダー業務を有効かつ先験的に監督し得る体制を確保することの重要性は増しつつある。

3. EBG は、電子バンキングのリスクおよび同リスクに対処するための健全な実務を把握するため、銀行業界内部および公的部門と民間部門の間の国際的な協調努力を促進する

- ・ EBG は、電子バンキングの進展についての情報伝達、および関連リスクに対する適切な監督対応やクロスボーダー調整の促進を図るため、地域銀

¹ アグリゲーター (aggregator) は、銀行、異業種の何れでもあり得る。アグリゲーターは顧客の代理人として行動し、顧客が複数金融機関に有する口座に係る総合情報を提供する。顧客から所要のセキュリティ・パスワードないし ID 番号を渡されたアグリゲーターは、主としてスクリーン・スクレーピング (screen scraping) という技術 (他の金融機関のウェブサイトからデータを抜き取る技術、ウェブサイトの所有者である金融機関はこれを把握していない場合が多い) により口座情報を統合する。

行監督者グループと協力する。

- ・ EBG は、電子バンキングの絶えず変化する現状と関連リスクを見極めるため、金融機関およびサービス・プロバイダーから継続的に情報を収集する。
- ・ EBG は、銀行・証券・保険業務およびそれらの市場に共通する電子商取引問題（リスク管理、法律問題、事務処理上の問題、セキュリティ問題等）について統合的な監督ガイダンスを策定するため、IOSCO、CPSS、IAIS 等の国際金融市場監督団体との協調を図る。

急速な発展を遂げつつある電子バンキングのデリバリー・チャンネルは、本来的にボーダーレスな性質を帯びている。従って、全世界の金融市場監督当局は、共通のリスクについて情報を交換したり、適切なリスク管理実務の開発を支援したりするため、積極的に協力する必要がある。また、EBG メンバーは、それぞれの属する法域内の銀行およびインターネット・サービス・プロバイダーとの協議を継続し、状況変化、リスク、およびリスク管理に係る進展を分析すべきである。

4. EBG は、銀行監督当局が開発しつつある電子バンキングに関連する監督研修プログラムおよび教材の交換を奨励・促進する

電子バンキングのデリバリー・チャンネルは、技術的に複雑であるとともに急速に進化する性質を帯びているため、銀行監督当局は状況変化に遅れをとらないよう相当な努力を払わなければならない。従って、EBG メンバーやその他の世界各国銀行監督当局が開発した検査員向け研修教材やガイダンスを積極的に交換することは、極めて有益であろうと思われる。

これにより、国際的な銀行監督界は、銀行システムの安全性と健全性を促進するとともに、電子バンキング業務の監督において競争条件の平等（level playing field）を実現・維持する能力を高めることにもなる。

電子バンキンググループ白書

2000年10月

クロスボーダー電子バンキングにおける監督上の課題

I. はじめに

本協議用ペーパーにおいては、電子バンキング業務におけるクロスボーダー監督上の問題点と課題を概観し、それらの問題点に対処するために監督当局の国際的協力が必要であるという点を指摘する。本ペーパーの末尾には4項目の行動計画が提示されている。電子バンキンググループ(EBG)は、こうした努力により、電子バンキングのリスクと監督上の諸問題において、監督当局間の国際協力と情報交換が促進されるであろうと考える。

II. 背景

バーゼル委員会は、実効的なクロスボーダーの情報伝達や調整に係るガイダンスを含め、母国および現地国の銀行監督当局による健全な監督のあり方を取り上げたペーパーを幾つか公表している²。これらのペーパーは、全ての国の銀

² バーゼル委員会の主要なガイダンスには以下のものが含まれる：「銀行の海外拠点監督上の原則」(「コンコルダット」、1983年5月)、「国際的業務を営む銀行グループおよびその海外拠点の監督のための最低基準」(1992年7月)、「クロスボーダー銀行業務の監督」(1996年10月)および「実効的な銀行監督のためのコアとなる諸原則」(1997年9月)。これらのガイダンスにより導入された母国当局と現地国当局の協力に関する考え方は、各国監督当局が二国間で結んだ覚書(Memorandum of Understanding、MOU)の多くに織り込まれている。

行監督当局やその他金融市場当局により、基本文献として参照されている。これらのペーパーは、(i)全世界的連結ベースの監督、(ii)現地国当局との接触と情報交換、および(iii)外銀の現地業務に対する監督について、幾つかの重要なクロスボーダー原則を設定している。

バーゼル委員会のガイダンスによって、現地国の監督当局は、現地国で免許を取得し、監督を受けている³クロスボーダー支店および子会社が親銀行の母国監督当局により有効に監督されている、という安心感を得てきた。しかし、電子バンキング業務の急速な拡大は、バーゼル委員会の既存のガイダンスが策定された時点では想定されていなかったクロスボーダー問題を数多く発生させている。

電子バンキングのベースとなるテクノロジーは、本質的に、銀行および顧客の“バーチャルな”地理的行動領域を拡大する一方、それに見合った“物理的な”拡大は必ずしも求めない。このような市場の拡大は国境を越えることもあり、銀行監督当局にとっては以下の要因によりクロスボーダー協力の必要性が増大する。

- (i) 世界の何処に所在する銀行であっても、相互に連結された電子的ネットワーク⁴を通じて、当該銀行が免許を取得しておらず監督も受けていない国の顧客を対象として、容易かつ高速に業務を行うことが潜在的に可能である。
- (ii) 銀行および異業種企業(non-bank)は、インターネットを用いることによって、国境を越え、かつ、これまで通常は監督対象となってきた銀行業務と⁵、

³ 欧州においては、第2次銀行指令(Second Banking Co-ordination Directive)に従って、欧州経済地域(European Economic Area < EEA >)内で免許を受けた銀行は母国当局の認可に基づいて他の EEA 国でサービスを提供することができる。

⁴ 典型例は、インターネットやワイヤレスなど、ウェブサイトを創設したり接続したりする技術(以後、本稿では“インターネット”と総称)。

⁵ 銀行監督当局のみならず、種々の金融市場当局が監視を行っている可能性がある。

如何なる金融市場当局からも監督を受けていない非銀行業務を、境界が不明なかたちでリンクさせることが潜在的に可能である。

- (iii) 各国当局は、他の法域から発する電子バンキング・サイトに自らの法域からアクセスすることをモニターないし統制しようとする際に、他の法域の母国当局の協力なしには実務的な困難に遭遇する。

従って、電子バンキング問題に対処するためバーゼル委員会のガイダンスに所要の修正を加えることは、EBGの主たる目標のひとつである。

III. 現 状

EBGが銀行監督当局に対して最近行ったサーベイによれば、監督当局は一般に、既存の法律・健全性規則・監督方針は電子バンキング業務にも適用されたと考えている。しかし、解答者の多くは、電子バンキングが特にもたらした問題やリスクに対処するためには、追加的かつ特別な監督ガイダンスが必要であると述べている。

EBGの判断によれば、殆ど全ての銀行は、新たなクロスボーダー市場に参入するに当って保守的なアプローチを採用している。すなわち、採られている手続きは、原則として、規制当局の公式の承認を要する外国市場に新たに参入する場合と同様である⁶。今日まで銀行は一般に、伝統的な店舗(brick and mortar)ベースのデリバリー・チャンネル(例えば、免許を受けた支店・代理店・子会社等)を通じて既に同様のサービスを提供している場合以外は、外国市場で電子

⁶ 一般に、伝統的な銀行環境においてクロスボーダー参入する場合は、免許の取得、当該金融機関と地域(現地国)当局の間で交わされた合意、および母国当局からの適宜の情報提供が必要となる。バーゼル委員会が1996年10月に公表したペーパー「クロスボーダー銀行業務の監督」には、こうした申請プロセスにおける現地国当局と母国当局の役割が述べられている。

バンキング・サービスを提供することを差し控えている。現時点でクロスボーダー電子バンキング業務を行っている銀行は、自国通貨建、ないし、現地通貨の決済システムに直接アクセスを有する国、もしくは免許を受けた物理的拠点を通じて間接的に同システムにアクセスを有する国の通貨建で電子バンキング業務を行うにとどまっている。

また、監督当局は、何れの法律や規則を適用すべきかという、クロスボーダー業務を巡って従来から存在する問題をより強く意識するようになってきている。EBG は、銀行業務に係る法律や規則の厳格度が国によって異なることを銘記している。これまで、規制上の相克が生じた場合は、銀行が他国の法域に進出する時点において、母国監督当局と現地国監督当局がケースバイケースで処理するのが一般的であった。EBG は、クロスボーダー電子バンキングから生じ得る法規上の問題も、同様に監督当局間でバイラテラルに処理されることになると考えている。

インターネットは、新たに出現した電子バンキング専門銀行（virtual only bank）にも、また既存の地理的に限定された銀行にも、国外に支店・代理店・子会社を設立する場合に通常必要となる出費や分析作業を必ずしも必要としないかたちで、活動範囲を外国市場に拡大する機会を与える。このため、銀行は現地の慣習、市場規約、規則、法規定を適切に理解しないままクロスボーダー電子バンキングを行う結果となりかねない。

更に、免許かつ（又は）監督を受けていない金融機関⁷は、クロスボーダー業務を行うに当たって、健全性監督を受けている銀行と同程度の規律を自らに課すとは限らない。この結果、免許を受けていない機関は、インターネットを通じて他の法域に進出し、当該法域で銀行に認められていない銀行類似サービスを提供する可能性がある。

銀行監督当局には以下の3つの課題がある。

⁷ もしくは、相対的に緩い監督監視体制下の銀行。

- (i) 監督当局は、インターネットの利用により国境を越えた電子バンキング・サービスの提供が可能になり、現在は法域毎に課されている認可手続きや規制プロセスが問い直される可能性があることを認識する必要がある。
- (ii) 監督当局は、現在規制対象となっている銀行に対して制限的なアプローチをとる一方、外国機関を同等の扱いとせず、外国機関がインターネットを通じて現地法域で同様の（もしくはほぼ同様の）業務を行う可能性を看過した場合の影響を、認識する必要がある。
- (iii) 監督当局は、クロスボーダー電子バンキングに係る法的枠組みが整備されるまでの間、銀行が法律を巡る不確実性に適切に対処できるようにしなければならない。

IV. クロスボーダー電子バンキングの監督に係る問題点と懸念

電子バンキングの進展に伴い、監督当局にとってクロスボーダー問題の一部は更に重みを増している。それらの問題は必ずしも新たに生じたものではないが、電子バンキング本来のボ - ダーレス性、および電子バンキングの前提となるテクノロジーの急速な発展が問題を一層複雑化している。

認可および規制問題

銀行は、物理的な世界において既に（郵便等を通じて）クロスボーダー・サービスを提供している。しかし、インターネット関連のテクノロジーは、各国当局の監督責任を巡って法域の潜在的な曖昧性を少なからず増幅させた。この結果、クロスボーダー電子バンキング業務に対しては十分な監督が行われない惧れがある。

また、銀行（ないし銀行業務）の定義上の曖昧さは、異業種企業が監督当局から認可や監督を一切受けずに銀行類似サービスを提供することをより容易に

する可能性もある。

更に、銀行は、現地の規制に関する知識を欠いたまま意図せずにクロスボーダー業務を行ってしまうことも有り得る。こうした場合、銀行にとっては、認可、消費者保護、記録保持・報告義務、マネー・ロンダリング防止規定など、当該国の様々な国内法規に抵触することに係るリーガル・リスクが高まる可能性がある。

健全性監督

既存の支払能力規制や健全性監督上のルールは電子バンキング業務、伝統的な銀行業務の双方に平等に適用されるが、電子的なデリバリー・チャンネルが新たに登場したことにより、監督当局にとっては新たな視点から再検討すべき健全性上の問題が浮上している。それらの問題には、アウトソーシングや業務提携取極めの監視、および、データの保護に関する統制とセキュリティ対策の監視（特に事務処理が異なる法域で行われている場合）が含まれる。

認可・規制問題におけると同様、電子バンキングの監督においても、母国当局と現地国当局の関係は複雑性と曖昧性を増す。バーゼル委員会の既存のガイダンスは銀行のクロスボーダー業務を監督する際の確固とした土台となっている。しかしながら、EBG は、本ガイダンスが電子バンキングの世界においても十分に堅牢なものであり続けるためには見直しが必要であると認識している。

V. クロスボーダー電子バンキングの課題に対処するための枠組み

具体的な監督のあり方は各国特有の様々な要因により異なる可能性があるとしても、クロスボーダー業務を有効に監督するためには、電子バンキング問題に対処するための枠組みが当局間に確立されていることが不可欠である。そう

した枠組みを設定する際の視点は、当該当局が母国当局であるか、現地国当局であるか、または、往々にしてそうであるように、その双方であるかによって異なろう。以下の2つのクロスボーダー・シナリオは、それぞれ異なる視点から検討を要する問題を浮き彫りにする。

1. 国内銀行が母国外の顧客に銀行サービスを提供(イン - アウト・シナリオ)
2. 母国(訳注:当該国監督当局にとっての母国)外に拠点を置く銀行が母国内で銀行サービスを提供(アウト - イン・シナリオ)。本シナリオは更に2つのケースに分かれる。すなわち、当該銀行が現地国(訳注:同)に物理的な拠点を有し、免許を受けて業務を行っている場合(物理的アウト - イン)、および当該銀行は現地国に物理的拠点と(又は)免許を有さず、銀行サービスはバーチャルな手法によってのみ提供している場合(バーチャル・アウト - イン)である⁸。

イン - アウト・シナリオ

銀行が外国で電子バンキング・サービスを提供する場合は、母国および現地国の当局が互いの監督プロセスを理解している必要がある。バーゼル委員会の既存のガイダンスは、銀行を連結ベースで監督する責任は母国監督当局に存し、現地国当局の監督対象は現地市場内で行われている業務に限定される、という原則を明確に打ち出している。

母国監督当局は、電子バンキング業務を連結ベースで把握し、連結ベースの監視アプローチでこれに臨まなければならない。母国監督当局は、通常、母国の法域外で行われる電子バンキング業務も母国内と同様の規則や統制の下に行われることを望むであろう。現地国において適用される規則や求められる統制

⁸ 監督当局は、明確なクロスボーダーのケースのみならず、国内市場のみを対象とする政策(イン - イン・シナリオ)も、インターネットのボーダーレスな性質の下では、国際的な調整を要するクロスボーダー問題を含み得ることを看過してはならない。例えば、“銀行サービス”の定義は、何れの機関が“銀行”であり、従って免許や監督を要するかを左右する。

が母国以上に厳格である限りにおいて、現地国当局は当該銀行が現地国のルールを遵守することを望むであろう⁹。

バーゼル委員会の既存のガイダンスによれば、母国監督当局は、銀行の電子バンキング業務を連結ベースで如何に監督しているかにつき現地国監督当局に明確な情報を提供しなければならない。一般に現地国監督当局は、母国監督当局の監督プログラムが有効に実施されることを期待する。母国監督当局の監督プログラムの有効性に懸念がある場合、現地国監督当局は母国監督当局とバイラテラルに接触する。必要な場合には、母国当局と現地国当局が協力して監督措置を採る。

アウト・イン・シナリオ

物理的アウト・イン・シナリオにおいては、外国銀行は多くの場合、現地国の法域内に免許を受けた何らかの物理的拠点¹⁰を有し、当該拠点は現地国監督当局の監督に服しているうえ、現地国の決済システムへのアクセスを有している。本シナリオにおいては、現地国当局は現地拠点に対して通常の監督プロセスを適用し、その際の主眼は現地市場内における活動に置くこととなろう。電子バンキングに関して規制上の問題が認められた場合は¹¹、免許を受けている現地拠点との間で現地において解決を図り、母国当局に適宜通知する。必要な場合には、現地国・母国双方の当局が協力して監督対応を採ることもあろう。

⁹ 母国監督当局に対し、あり得べき全ての法域の法規を知悉し、自らの法域外における法規の遵守をモニターすることを求めるのは恐らく非現実的であろう。しかし、母国監督当局は、自らの監督下で銀行サービスを提供している銀行が、外国法域で法律に違反したり不用意な行動を採ったりすることを回避するため、妥当な知識や方針・手順を有していることを確認しなければならない。

¹⁰ 物理的拠点は、現地で設立した銀行などの子会社、現地国監督当局から免許を受けた支店や代理店、あるいは銀行以外の業態の規制対象金融機関などのかたちをとる。

¹¹ 母国監督当局と現地国監督当局の意思疎通は、健全性関連事項のみならず、異なる法域の間で何れの法律を適用するかという問題においても必要となる。

バーチャル・アウト・イン・シナリオの場合、当該外銀は現地免許を取得した拠点を設けていない国、ないし現地の決済システムに直接のアクセスを有さない国の顧客に電子バンキング・サービスを提供している。本シナリオにおいては、“潜在的な”現地国当局は、当該バーチャル・バンクの業務の性質と範囲について幾つかの点を検討し、免許を取得して現地の規制監督に服することを求めるべきか否かを判断することになる¹²。

現地国当局、母国当局の双方が目標とすべきは、法域の曖昧性から生じるリーガル・リスクを回避ないし最小限にとどめ、電子バンキング業務が明確に定義された監督責任の下に適切な監督を受けるよう図ることである。バーチャル・バンクの業務が有能かつ協力的な銀行監督当局を欠く法域から行われる場合、現地国監督当局は、自国の居住者と銀行システムを守るためにどのような対応を採ることが適切であるかを検討する必要がある。

VI. クロスボーダー電子バンキングの課題に関する監督協力の可能性

母国市場の外における電子バンキングの進展は、遅速の別はあれ、母国市場における変化のペースと全く異なり得る。しかし、インターネットのボーダーレスな性質に鑑みれば、国外における進展は国内市場に影響を及ぼす可能性があり、多くの場合これは可能性にとどまらない。また、今日まで銀行顧客による電子バンキング取引の受入れはかなり控えめなものにとどまり、これに伴うリスクも限定的なものに過ぎないことは事実であるが、状況は変化する可能性が高い。

電子バンキングの急速な進展およびそれに付随するリスクが及ぼす影響を把握し、これに対処するためには、監督当局の機敏な対応、監督資源、またクロ

¹² 現状において、銀行監督当局の本件に対するアプローチは、伝統的な物理的アウト・イン業務に如何に対処するかに応じて区々である。

スポーダー問題における母国・現地国監督当局間の協力が必要となる。電子バンキング業務について監督上のガイダンス（supervisory expectations and guidance）を形成してゆくためには、国際レベルでの監督当局間の協力も重要である。こうした協力は、全ての法域において監督を強化するのみならず、世界的な競争条件の平等化を促進する¹³。クロスボーダーの協力によって既存の監督プログラムや健全性監視実務を拡大し、電子バンキングのリスク管理に関する監督ガイダンスを策定することができれば、電子バンキングに関する全く新しい法規の制定を避けることができるであろう¹⁴。

監督当局は、こうした監督手段やガイダンスを策定するに当たって、リスクを取る意欲の度合いは区々であり、リスクを相殺する手段も様々であることを認識しなければならない。多くの国の銀行監督制度において、自国の銀行に係るガイダンスは一律でない（one size doesn't fit all）。当局のガイダンスは、銀行の規模、複雑性、リスク・プロファイル、業務分野、内部的なリスク管理プロセスの有効性などによって異なる¹⁵。どのような監督ガイダンスにおいても、銀行経営者が様々なトレードオフに直面することは認知されていなければならない。ガイダンスが厳格かつ細部にわたり過ぎれば、銀行経営上必要な柔軟性が損なわれる。

また、銀行監督当局は、健全なリスク管理ガイダンスや業界基準を模索する

¹³ 市場は銀行と同様に区々であり、全ての市場において同一のガイダンスが適用されるとは考え難い。しかしながら、ガイダンスが類似していればいるほど、監督当局にとってクロスボーダー問題への対処は容易になるであろう。

¹⁴ EBG は、作業計画の Phase 以降、幾つかの分野において健全な市場実務に関するガイダンスを提示することを検討する。本件については、付随の白書「電子バンキングのリスク管理における監督上の課題」参照。

¹⁵ 2000 年問題（Y2K）における最近の経験は、金融機関に対する監督当局のガイダンスが一様でないことを示す好例であった。このことは補修措置やテストの分野において特に顕著であった。多くの国において、金融インフラストラクチャーの一部として他の金融機関にサービスを提供している大規模金融機関は、他の機関がそれらの大規模機関との間で十分な時間的余裕をもってテストを行うことができるよう、他の機関より早目に補修やテストの段階を終了するよう求められた。

に当っては、それらのガイダンスや基準が健全なリスク管理を伴いかつ電子バンキングの革新を不当に阻害することなく電子バンキングの発展を促進し得るように、民間銀行業界と協力して作業を進めるべきである。

VII. クロスボーダー電子バンキングの課題に対処するための次なるステップ

電子バンキングの急速な拡大は、銀行監督当局に対し、母国当局と現地当局の間における監督責任の分担や国際的な監督協調をはじめ、クロスボーダー監督上の新たな問題と課題を提示している。従って、EBGの作業計画のPhase（2000年6月～12月）（訳注：EBGでは、2000年上期をPhase Iとして本白書の作成作業を行い、同年下半期をPhase IIとして新たな作業に入る）においては、以下の項目に重点が置かれる。

1. クロスボーダー電子バンキング固有の問題に対処するため、バーゼル委員会の既存のガイダンスを修正する必要があるか否か、また修正する必要があるとすればどの部分かを検討する。
2. 地域的な銀行監督当局グループと協力し、国際的な電子バンキングの進展について情報交換を行うとともに、健全な監督実務の開発とクロスボーダーの調整を促進する。
3. 他の国際金融市場監督団体がクロスボーダー商取引全般に関するルールやガイダンスを設定しつつあり、これが電子バンキングに影響を与える可能性がある場合は、それらの国際金融市場監督団体と協力する。
4. 電子バンキングのリスクおよび同リスクに対処するための健全な実務を模索するため、銀行業界内部および公的部門と民間部門の間の国際協調努力を促進する。

電子バンキンググループ白書

2000年10月

電子バンキングのリスク管理における監督上の課題

I. はじめに

本協議用ペーパーにおいては、電子バンキングの進展状況を確認するとともに、電子バンキングが伝統的な銀行業務とどのような点で異なるかを分析する。本ペーパーは、バーゼル委員会が1998年3月に公表したペーパー「電子バンキングおよび電子マネー業務のリスク管理」に含まれている議論の延長である。本ペーパーにおいては、電子バンキングの急速な発展に伴ってどのような新しい傾向やリスク管理上の問題が生じ、銀行および銀行監督当局の対応を促しているかを明確にする。EBGは、これらのリスク問題に対処するためには既存のリスク管理フレームワークを拡大する必要があると考え、4つの作業項目を選定した。

II. 背景

銀行は、既に何年も前から消費者や法人に対して遠隔的にサービスを提供している。小口決済や法人のキャッシュ・マネジメント・システムを含む電子的資金移動、公にアクセス可能な現金引出機、個人口座管理などは、全世界的に定着した制度である。しかし、インターネットをはじめ公に解放されたネットワーク¹⁶を通じて金融サービスが提供されるようになったことから、金融サービ

¹⁶ インターネットという言葉は、ウェブサイトの創設や接続を可能にする全ての技術を包

ス業界には根本的な変化が生じつつある。こうした変化は、インターネット・テクノロジーの技術的特性の一部と相俟って、銀行・監督当局の双方に新たな懸念材料をもたらしている。EBG が G10 諸国の監督当局および銀行を対象として最近行ったサーベイによれば、銀行のリスク・プロファイルに影響を及ぼし得る傾向や問題が幾つか生じつつある。

- (i) 銀行、異業種企業の双方が新金融商品・サービスを急速に導入するに従い、電子金融サービス産業における競争は大幅に激化する。
- (ii) 遠隔通信、およびコンピューターのハードウェアとソフトウェアにおける急速な技術進歩に伴い、取引の処理速度が高まる。
- (iii) 銀行の経営陣およびスタッフは、往々にしてテクノロジーや電子バンキングのリスクに係る専門知識を欠いている。
- (iv) 外部サービス・プロバイダーへのアウトソーシングに依存する度合いが高まるにつれ、非金融企業との新たな業務提携や合併事業が盛んに行われるようになる。
- (v) 世界的に整合性のあるテクノロジー・インフラストラクチャーの必要性が高まる。本インフラストラクチャーは、取引量の変動に対応する能力、柔軟性、および個別企業内部および企業間における互換性を備え、かつ、情報とサービスの安全性・完全性・可用性 (security, integrity and availability) を保証し得るものでなければならない。
- (vi) インターネットをはじめとするオープン・ネットワークにおいては、顧客の真正性や有資格性を確認するための標準的な業界実務が確立されていないと、詐欺行為が行われる余地が大きくなる。
- (vii) 発展し続ける電子バンキング業務に現行法規を適用することが可能か、また何れの法域の法規を適用するかを巡って、法律や規制上の曖昧性や不確実性が存在する。

含する。現時点において、そうした技術に相当するのはインターネット、ワイヤレス、その他のネットワークである (以下、インターネットと総称)。

- (viii) 多量の顧客情報を収集・保存し、しばしば他者に提供したりすることは、顧客のプライバシー問題につながり、ひいては銀行の健全性にリスク（例えばリーガル・リスクやレピュテーション・リスク）を及ぼす恐れがある。
- (ix) オンライン・ディスクロージャーの有効性と効率性には疑問の余地がある。長々しく複雑なオンライン・ディスクロージャーを行うと、顧客は読み飛ばしてしまうか、甚だしい場合にはウェブサイトを見なくなることもあり得る。また、長大なディスクロージャーはウェブサイトやページのダウンロードに要する時間を長引かせる。

銀行および銀行監督当局は、伝統的な銀行業務に適用される監督原則は電子バンキングにも適用されるという点において概ね意見の一致をみている。しかし、テクノロジーの急速な変化は、銀行がテクノロジーのベンダーやサービス・プロバイダーに対する依存を強めていることと相俟って、伝統的なリスクを變形させ、時には拡大させている。EBG がアジア、欧州、および北米の監督当局と銀行を対象として最近行ったサーベイが示唆するところによれば、電子バンキング業務における総合的なリスク管理の枠組みを強化するためには、幾つかの分野において監督ガイダンスを追加する必要性がある。

電子バンキング業務は、国際協調努力を要し得るクロスボーダー問題を提起しているが、本ペーパーではこれらの問題には簡単に触れるにとどめる。クロスボーダー問題は、EBG が別途作成した白書において包括的に取り上げられている。

III. 現 状

銀行は電子バンキング業務に注力する度合いを強めており、インターネット・バンキング業務を世界規模で拡大し、ワイヤレス・ネットワークの利用を

検討し、電子商取引の一部新分野に進出しつつある。

銀行は、市場シェアを防衛ないし拡大するため、あるいは、ペーパーワークや人員を削減してコストを節約するための戦略として、電子バンキング・サービスを提供している。また、銀行はインターネットを利用することにより、既存の国境を越えて新規顧客を開拓する可能性を大幅に拡大した。しかし、オープン・ネットワークの特性と電子商取引の進展により、銀行は銀行・異業種企業の双方からかなり激しい競争に晒されている。更に、電子的なデリバリー・チャンネルは、法規環境が不明確かつ国毎に異なるという現状の中で運営されている。金融機関が十分な収益性を保ちつつ、提供サービスの安全性、完全性、および可用性を管理してゆくためには、こうした要因の全てが新たな課題を呈する。

業界サーベイの対象となった銀行の殆どは、第一の競争相手として他の銀行ないし金融サービス会社を挙げた。大手銀行の一部は、インターネットのポータルサイトやディスカウント・ブローカーをも主要競争相手と見なしている。これらの異業種企業は、小切手決済、電子請求呈示支払（electronic bill presentment and payment）等の金融サービスを自らのブランドにおいて自らのウェブサイト上で提供している¹⁷。

インターネット専門銀行も少数誕生しているが、既存の銀行（すなわち、これまで銀行業務に関わりのなかった新規参入者を除く）は、伝統的な店舗（“brick and mortar”）ベースの業務の延長として電子バンキングを提供している。インターネット専門銀行は、初期コストが低く、柔軟性が大きく、所要設備が少ないなどの利点を享受する可能性があるが、こうした戦略に対する当初の情熱は後退し、インターネットによるアクセスが可能な金融サービスと少数の物理的拠点を組み合わせる方式（“click and mortar” approach）へと修正されつつあ

¹⁷ 一部の大手銀行はこうした企業とも提携関係を結んでいるが、その場合は何れのブランドを前面に出すかについて両者間に対立が生じることがある。

る。銀行は一般に、インターネットのチャネルを総合的なデリバリー戦略の一部として組み入れている¹⁸。銀行は、自らのブランドの価値、および、商品・サービスのクロスセリングというかたちで既存の顧客関係を利用し得る可能性を再認識している。

当初、多くの銀行は、企業対消費者 (Business-to-Customer、B2C) のリテール電子バンキング・サービスに力点を置いた。しかし、最近に至って銀行は、企業対企業 (Business-to-Business、B2B) の電子商取引を支援する新しい商品・サービスを開発し始めている。例えば、一部の銀行は、企業間の安全な情報伝達を保証する認証機関制度を開発するためのジョイント・ベンチャーを設立した¹⁹。また、既存の電子的請求呈示システムに接続し得る、もしくは既存の同システムを改善のうえ接続し得る電子的請求支払システムの開発に向けて作業を行っている。何れの場合も、銀行は、既存の企業顧客との関係を基礎として業務を拡大し、それぞれの分野において基準を設定し、企業対企業電子商取引において重きを成し、商取引における“信頼のおける第三者”として既に獲得している評価を更に拡張すべく努力している。

また、大手銀行の一部は、フルサービスの企業対企業取引所や市場を創設するためにテクノロジー企業と戦略的提携を結んでいる。銀行は、外国為替、キャッシュ・マネジメント、決済等のサービスを提供することにより、これらのテクノロジー企業に大きく欠落している部分を埋めている²⁰。

¹⁸ 但し、少数の銀行は、インターネット専門銀行を設立し、銀行組織内の独立した部門として運営することに成功している。

¹⁹ 認証機関制度においては、電子署名を用いて既存ネットワーク参加者の本人確認を行う。認証機関は、システム参加者のアイデンティティーおよび同人の所有する一組の鍵（公開鍵と秘密鍵）を確認した後、電子認証と呼ばれる証明書を発行する。各参加者は、暗号技術を用いて全ての伝達情報（ネットワーク内で交わされる金融取引を含む）に電子署名を付す。

²⁰ 一方、テクノロジー企業の一部は、銀行が法人顧客ベースに資材調達サービスを提供するためのソフトウェアを開発する契約を結んでいる。

一部の銀行は、自らの内部調達事務にインターネット技術を導入した経験を生かし始め、現在、キャッシュ・マネジメント・サービスの自然な延長として顧客に資材調達サービスを提供している。一部の国の銀行は電子商取引分野への新規参入を目指しており、中小企業を対象として、ウェブサイトのデザインや運営といったサービスを提供したり、時にはインターネット・サービス・プロバイダーとして活動したりしている。

こうした活動は新たな収益源となり得る一方、監督当局として対処すべき新たなリスクを銀行にもたらす。

銀行業界は、電子商取引が信頼され、受容されるよう促すため、また、顧客から訴訟を起こされる結果となりかねない誤解を最小限にとどめるためには、適切な透明性を確保する必要があることを認識している。しかしながら、電子バンキングにおける対顧客オンライン・ディスクロージャーの最適の質と範囲については、業界代表者の間に多少の見解の相違がみられた。こうした見解の相違は、例えば、オンライン・ディスクロージャーの有効性と実行可能性、競争条件の平等についての懸念、あるいは技術的な問題などに起因するものである。

新しいテクノロジーは、多量の顧客情報を収集・保存・処理することを可能にした。既存の銀行も新規参入者も、こうした業務から高い収益を得ることを期待している。銀行も異業種からの参入者も、顧客情報は戦略的資産の中核であると考えている。新規市場参入者を含む一部の銀行は、銀行業務における顧客データの重要性を認識し、かなりの規模の資源を“データ・マイニング”²¹に投入することによって、複数のシステムから得られる情報や商品ラインを横断する情報を把握・統合する能力の向上を図っている。異業種企業の中には、顧客データベースへのアクセスのみを目的として既存銀行の買収を検討する先さ

²¹ データ・マイニングとは、アルゴリズムを用いて顧客の取引データから一定のパターンを抽出し、個々の顧客に適した商品・サービスを提供するための参考とする作業を指す。

え見られる。

顧客情報を収集し、“マイニング”する能力を強化することは、顧客のニーズをより正しく把握したうえ、そうしたニーズに合致し、かつ当該顧客に潜在するリスクを反映した新商品・サービスを創造・販売するための助けとなる場合があることは事実である。しかしながら、データの収集、第三者への供与、およびマイニングを拡大することは、銀行業界に潜在的なリーガル・リスクやレピュテーション・リスクをもたらす。

テクノロジーの進歩は“アグリゲーション (aggregation)”や“スクリーン・スクレーピング (screen-scraping)”の出現をも促した²²。アグリゲーションおよびスクリーン・スクレーピングは、現時点ではほぼ米国に集中しているが、銀行・異業種企業双方が新たな電子商取引のビジネス・モデルを導入しつつあるなかで、数年以内にごく当たり前の業務になるであろうと見る向きが業界には多い。こうした展開は、金融サービス業界に対して戦略上、競争上の大問題を提起するとともに、セキュリティ・リスク、リーガル・リスク、およびレピュテーション・リスクをももたらす。何故なら、銀行は現在、自分のデータベースから誰がスクリーン・スクレーピングを行っているかについて統制力を持たないにもかかわらず、情報が不適切に用いられた場合は責任を問われる惧れがあるからである。

電子バンキングを巡る上記のような展開は、以下のことを示唆する。

²² アグリゲーター (aggregator) は、銀行でも異業種企業でもあり得る。アグリゲーターは顧客の代理人として行動し、顧客が複数金融機関に有する口座について総合的な情報を提供する。顧客から所要のセキュリティ・パスワードないし ID 番号を伝えられたアグリゲーターは、主としてスクリーン・スクレーピングと呼ばれる技術 (他の金融機関のウェブサイトからデータを抜き取る技術、ウェブサイトの所有者である金融機関はこれを把握していないことが多い) により口座情報を統合する。業界人の多くは、アグリゲーション技術は金融サービスを拡大 (より広範な口座スウィープ、入札、インテリジェント・エージェント等) するためのベースとなるであろうと考えている。

- (i) 金融サービス部門においては、電子商取引の利益に与かろうとする意欲が拡大している。金融サービス産業は、顧客ベースを構築・維持する手段として、テクノロジーをベースとする金融サービスを顧客に直接提供することに力を入れる傾向が強まっている。
- (ii) 電子バンキングにおいては、マーケティングのスピードが成功の決定的要因のひとつとなっている。銀行は、マーケティングの所要時間を削減するため、異業種との提携により総合的な金融サービスを提供する傾向にある。
- (iii) 昨今の傾向である戦略的提携やテクノロジーのアウトソーシングは、今後とも拡大してゆくであろう。

こうした展開は、銀行と銀行監督当局の双方に課題を呈示している。銀行は、電子バンキング業務がもたらした新たなリスクに照らして、伝統的なリスク管理実務の頑健性を再吟味する必要がある。また、銀行監督当局は、電子バンキングに関する新たなレギュレーションや監督方針を導入するに当たり、銀行の安全かつ健全な業務運営を確保する一方で、革新を阻害したり異業種に対する銀行の競争力を削いだりすることのないよう、バランスの取れたアプローチを採る必要がある。

IV. 銀行のリスク・プロファイルおよびリスク管理実務に及ぶ影響

インターネットを用いた電子バンキングをデリバリー・チャネルのひとつとして提供する場合、銀行のリスク・プロファイルはある程度変化し、リスク管理上の新たな課題が生じる。従って銀行監督当局は、銀行が電子バンキングのデリバリー・チャネルを用いることによって、当該銀行の戦略リスク、オペレーショナル・リスク、レピュテーション・リスク、リーガル・リスク、信用リスク、流動性リスク、マーケット・リスク、および外為リスクにどのような影響が及ぶかを考慮しなければならない。

1. 戦略・業務リスク

戦略リスクは、電子バンキング業務が銀行に及ぼす最も大きなリスクのひとつである。戦略リスクは、より一般的かつ広範な性質を帯びているという点において、他のリスク・カテゴリーと異なる。銀行の取締役会や執行経営陣が採択する戦略上の決定は、他の全てのリスク・カテゴリーに影響を及ぼす。

顧客の間で電子バンキングの受入れないし電子バンキングに対する需要が拡大していること、また、電子バンキングによって業務が効率化され得ることに鑑みれば、大多数の銀行は、インターネットを用いたデリバリー・チャンネルを織り込んだ戦略を策定し、同チャンネルを通じて顧客に情報や取引サービスを提供する必要がある。当該戦略の内容や実施方法に欠陥があったり、何らかの点で十分な配慮に欠けていたりする場合は、テクノロジーの急速な変化や、銀行間ないし異業種との間の競争の激化、あるいは当該戦略そのものの性質に起因する甚大なリスクに晒される恐れがある。

電子バンキングにおける戦略リスクの一部は、タイミングの問題に直接関係している。テクノロジーのパイオニアとなることを経営方針として決定した場合、戦略リスクはかなり大きいと考え得る。甚だしい場合は、テクノロジーの急速な変化によって余剰システムを抱える結果となる。一方、テクノロジーをフォローする姿勢が過度に慎重であれば、既に飽和状態になった市場、ないし統合の進んでいる市場の中で適切な身の置き所を失う結果となりかねない。

インターネットの登場以前、銀行は系列組織内で固有のネットワークを運営し、これを限定的に他の銀行に接続していた。こうした固有のネットワークは、新規参入者に対する戦略上の防衛手段のひとつとなり、個々の銀行のフランチャイズを守ってきた。しかし、万人にアクセスを認めるオープン・ネットワークであるインターネットは、銀行・異業種の双方に対し、物理的なプレゼンス

の拡大なくして新たに業務を起こしたり既存の業務を拡大したりする自由を与えた。この結果、金融サービス業界内部の競争は著しく増大し、今後更に増大するものと予想される。

大多数の銀行は、電子バンキングのデリバリー・チャンネルによって長期的にオペレーショナル・コストを削減できると考えている。しかしながら、多くの銀行顧客は銀行との伝統的な関係を保ちたいと考えているため、銀行にとって既存の物理的インフラストラクチャーを放棄することは難しい。すなわち、銀行は、少なくとも当面は多様なデリバリー・チャンネルを運営し続ける必要があり、電子バンキングは追加的な出費となる。従って、オペレーショナル・コストの節約は長期的な展望に過ぎない。

市場シェアの維持を巡って銀行業界が抱える問題は、新規参入企業がインターネットを通じて既存の銀行顧客に個別金融サービスを提供しているという事実により複雑化している。アグリゲーションやスクリーン・スクレーピングといった技術の出現は、銀行に戦略上のチャンスと脅威の双方をもたらしている。アグリゲーター、その影響を受ける銀行、顧客の関係が今後どのように展開するかによって、銀行の仲介機能は更に低下する惧れがある。アグリゲーターは潜在的に、銀行と顧客の伝統的な関係を断ち切り、銀行がオンライン・ベースでリテール顧客に直接アクセスする能力を限定するからである。更に、銀行とノンバンクが積極的にアグリゲーションを行った場合、銀行の商品・サービスは一段と均一化し、銀行は収益マージンの縮小を被るとともに、新たなセキュリティ・リスクおよびリーガル・リスクに晒される惧れがある。

要すれば、銀行経営者はインターネット戦略の策定に当り、同戦略が競争力や収益力の維持に資する一方で²³、リスク・プロファイルを不当に拡大させることがないように、十分な注意を払う必要がある。監督当局は銀行に対し、自らの

²³ 競争力と収益力の維持に係る配慮には、金融仲介機能の低下を回避ないし緩和するための措置も含まれる。

戦略上の選択肢の利点と難点を注意深く検討することを求めなければならない。

2. オペレーショナル・リスク

電子バンキングは全ての側面においてテクノロジーに依存するため、オペレーショナル・リスクは重大なリスクのひとつである。銀行は、オペレーショナル・リスクを削減するため、全企業体を包摂する組織とテクノロジー・インフラストラクチャーを構築しようとするであろう。この組織とテクノロジー・インフラストラクチャーは、システムの互換性確保を容易化し、データの安全性・完全性・可用性を保証し、外部サービス・プロバイダーとの関係の適切な管理を下支えし得るものでなければならない。更に、テクノロジーはビジネス・モデルや事務処理プロセスをも劇的に変化させているため、銀行は必ず適切な業務管理手順（システム更新の手順を含む）および監査プロセスを設けておく必要がある。

(a) テクノロジーのインフラストラクチャー

電子バンキングは、様々なシステムやアプリケーションの技術的統合という問題を前面に押し出した。大手銀行の多くは、電子バンキング用のシステムと、旧来業務用の既存システム、および多数のサービス・プロバイダーや提携先のシステムの統合という課題に直面している。これらの銀行は、電子バンキング用のシステムを適切に統合し得なかった場合には取引処理上のミスから生じる甚大なオペレーショナル・リスクに晒されることになる。

従って大手銀行の多くは、テクノロジー・インフラストラクチャーに多大な投資を行うことにより、内部統制を改善し、リスク管理の監視プロセスを強化しようとしている。これらの銀行はまた、システムと運用を改善し、柔軟性、取引量の変化に対する対応能力、および企業内部ならびに外部サービス・プロバイダーとの間における互換性を高めたいと考えている。

大手銀行全般にみられるこうした傾向は評価すべきであるが、銀行業界全体を見渡すと、システムおよびリスク管理インフラストラクチャーの改善は未だ電子バンキングを有効に支え得るレベルに達していない。特に中小銀行は、ハードウェアやソフトウェアを購入したり、テクノロジー - 関連のスタッフを獲得したりするための予算に限界があるなど、厳しい状況に直面している。これら中小銀行の多くは、電子バンキング業務を支えるために必要なテクノロジー・インフラストラクチャーの管理を外部ベンダーに大きく依存している。こうした場合でも、関連事務が十分に統制・管理されていることを保証する最終的な責任は依然として銀行に存する。従って銀行監督当局としては、そうした統制・管理を適切に行う能力が銀行経営陣に恒常的に備わっているか否かを検証する必要性を感じるであろう。

(b) セキュリティ

EBGメンバーが実施したサーベイでは、大多数の銀行が電子バンキングにおける主たる懸念事項のひとつとしてセキュリティ・リスクを挙げた。“ハッキング(hacking)”²⁴、“スニффイング(sniffing)”²⁵、“スプーフィング(spoofing)”²⁶、“サービス妨害攻撃(denial of service attacks)”²⁷といった外部からの脅威は、銀行を新たなセキュリティ・リスクに晒している。オープン・ネットワークを用いた電子的デリバリー・チャネルは、情報の機密保持と保全、取引の否

²⁴ ハッキングとは、あるコンピューターに承認を得ずに侵入する行為を指す。こうした行為は、悪意ある動機から行われることもあれば、単にそうした行為が可能であることを証明するためあるいは、その他の個人的な理由に基づいて行われることもある。

²⁵ スニッフイングとは、あるネットワークの何処かにソフトウェアを不正に挿入し、これを用いて、システムを通過するユーザー・パスワードを捕捉(sniff)する行為を指す。

²⁶ スプーフィングとは、承認されたユーザーを装ってあるシステムにアクセスしようとする行為を指す。

²⁷ サービス妨害攻撃とは、あるサーバーに大量の通信を送付し、正当な通信に答えられないようにする行為を指す。

認が不可能となる条件の明確化（non-repudiation of transactions）、ユーザーの有資格性の確認とアクセス・コントロールについて、新たなセキュリティ上の課題を銀行に提起している。

EBG が最近行ったサーベイや業界実務家との協議によれば、大多数の銀行はセキュリティに対する外部からの脅威に対して敏感であるように窺われる。早急な対応を要する問題のひとつとして挙げられたのは、金額の大きい取引依頼について、本人確認および有資格性の確認を行うための手法を堅牢化することである²⁸。また銀行業界は、電子的な署名や記録の法的効力の問題を含め、暗号の要件について国際的なベスト・プラクティスを打ち立てるべく引続き努力する必要がある。更に、多くの銀行では、外部接続システムの管理に用いられているセキュリティ技術が内部ネットワークにも適用されているため、内部ネットワークから発生するセキュリティ・リスクの管理にも神経を使う必要がある。内部的なセキュリティ・エクスポージャーが適切に管理されていない場合、銀行の記録や顧客データの保全と機密保持に問題が生じ得る²⁹。

銀行がセキュリティ管理を疎かにすると、顧客の個人データを適切に保護していないと見なされて、レピュテーション・リスクないしリーガル・リスクに晒され、法律的な損害を被ったり、評判に傷がついたりする惧れがある。

銀行監督当局は、国際的なレベルにおいて、内部および外部セキュリティ・エクスポージャーに係るリスク管理の包括的アプローチの開発を促進すべきである。セキュリティ・リスクの管理に係る業界標準は常に変化しているため、

²⁸ 本人確認（identification）とは、取引を行う個人ないし組織のアイデンティティーを肯定的に認めることを意味する。本人確認の一般的な手段はパスワードであるが、身体的特徴に基づく本人確認（biometrics）など、現在開発途上にある他の手段が次第に主流を占める可能性もある。有資格性の確認（authorization）とは、ある個人が特定の取引を行う権限を有していることを認めることを意味する。

²⁹ 多くの銀行において、被用者の犯行を含む内部システムへの攻撃は、対外接続システムへの攻撃よりも頻度が高い。

銀行監督当局は業界との共同作業によりサウンド・プラクティスの開発を促進すべきかもしれない。

(c) データの保全

データの保全はシステムのセキュリティの重要な一要素である。銀行は、顧客、他の銀行、および外部サービス・プロバイダーとの関係を有効に管理するため、企業内部および企業間におけるシステムの互換性を改善しなければならない。電子的データの管理に関する業界標準が明確化されるまでの間、銀行は、送受信データの正確性を確保し、同データが毀損される危険性を排除し得る有効な統制プロセスを確立すべく、不断の努力を払う必要がある。本プロセスには、少なくとも、プロジェクト管理、システム開発のライフ・サイクル、システム更新の統制、および質の確保に関する健全な方針と実務が織り込まれていなければならない。銀行監督当局も銀行に対し、リスク管理に用いるデータが毀損されていないことを確認するよう促すべきである。

インターネットは低コストであるとともに広範に普及しているため、銀行はデータを保全するため、標準的な通信プロトコルとして TCP/IP³⁰を用いる傾向を強めている。TCP/IP を用いて通信を行うことには大きな利点があるが、旧来のシステムや他者のシステムとの間で遣り取りされるデータが正確に翻訳され、全体の中に織り込まれるよう図ることも必要となる。この目的においてミドルウェア³¹や XML³²等の言語を用いることも有効であるが、こうした新テクノロ

³⁰ TCP/IP とは、パケット化したデータをインターネット経由で送信する際の標準化された通信プロトコルである。TCP (Transfer Control Protocol) はデータ・パケットを組立てる際に用いられ、IP (Internet Protocol) はパケットのコンピュータ間における送信ルートを決定する際に用いられる。

³¹ ミドルウェアとは、ネットワーク上におけるクライアント/サーバー間の通信 (TCP/IP 等) を支援する通信処理ソフトウェアを指す。これによってクライアントのアプリケーションは、異なるプラットフォーム、データベース、あるいはメインフレームから情報を引き出したり更新したりすることができる。

ジーを支える業界標準は未だ発展の極く初期段階にある。

(d) システムの可用性 (System Availability)

電子バンキングの商品・サービスを常時確実に提供するためには、電子バンキングを支える安全な内部ネットワークを確保することに加え、許容能力について有効な計画を立てておくことが決定的に重要である。電子バンキングにおいては、顧客の価格感応度が高いことや取引が自動化されていることから、取引量のボラティリティが益々増大する可能性がある。また、競争圧力に加え、1週7日/1日24時間(24x7)体制のサービス提供が当然となりつつあることも影響して、顧客の要求水準はかなり高まり、ミスが容認される余地は小さくなっている。電子バンキング・サービスを提供している銀行は、競争に耐え、かつシステム・ダウンから生じ得る少なからぬ潜在的レピュテーション・リスクを回避するために、適切な構成の商品・サービスを安全、正確、かつ継続的に提供しなければならない。これらのことは、業務の継続性、回復、および事故発生時の対応について有効な計画を立てておくことが如何に重要であるかを示している。また、アウトソーシングが一般化している現状に鑑みれば、銀行は、外部サービス・プロバイダーも同様の計画を立て、その有効性を定期的にテストしていることを確認する必要がある。

サービス妨害攻撃を受けた場合も、銀行の同サービス提供能力はこの間において低下ないし完全に失われる恐れがある。こうした攻撃は、電子商取引の積極的な提供者に対して益々頻繁に行われるようになっている。銀行にとってのいまひとつの問題は、インターネットというネットワークそのものの可用性を統制する能力が銀行の側にないということである。従って銀行は、コンティンジェンシー・プランの一環として、インターネット・ネットワークに大規模な障害が発生した場合の代替的サービス送達手段を検討しておく必要がある。

³² XML (Extensive Mark-up Language) とは、ウェブ上における構造化データの交換を可能にする普遍的かつ柔軟なテキスト・ベースのデータ・フォーマットである。

(e) 内部統制・監査

如何なる銀行業務においても、ミスを検知・是正する能力は内部統制の決定的要素である。また銀行は、内部・外部双方に源を発する不正行為を防止し、銀行の情報と資産を守るために十分な統制を敷いていなければならない。

電子バンキングのもたらす効率性とコスト削減効果は、“STP (straight-through-processing)” が可能になるという点に負うところが大きい³³。STPには多くの利点がある。一方、現実には、広範なアクセス・チャネルの全てにわたって、内部統制、職責の適切な分割、監査による明快な検証を如何に行うべきか、という点が、電子バンキングにおいては従来と変わってくるという問題がある。銀行業界がこうした変化に対処することの難しさは、技能や専門知識が実務処理においても監査においても決定的に不足しているという事実によって増幅されている。銀行にとって、高度に自動化された環境下で有効なコントロール体制を確保し、同体制に対して独立した監査を行うことは、今後益々難しい課題となってゆくであろう。

(f) アウトソーシング

電子バンキングが銀行業界にもたらした変化の中でも、規模の大小を問わず全ての銀行のリスク・プロファイルに最も大きな影響を及ぼしているのは、アウトソーシングに対する依存度の高まりであろう。大手銀行は、自らはコア業務への集中を強める一方、それ以外の分野については他の機関と提携する、とかたちで様々な業務をアウトソースしている。小規模銀行の場合は、自力で電子バンキングのデリバリー・チャネルを構築するために必要なテクノロジーの専門知識や資金力に乏しい例が多いため、通常はアウトソーシングに依

³³ STPとは、取引プロセスの流れに人手が介入しない自動的取引処理を意味する。

存せざるを得ない。また、“ターンキー(turnkey)”(訳注：ある企業がユーザーに販売することを目的として構築・製造したシステム・パッケージ等) のコストが低下しつつあることも、小規模銀行がベンダーから電子バンキング・アプリケーションを購入し易くなっている理由の一つである。こうした展開は、銀行業界の効率性を高め、小規模銀行の競争力を補強し、銀行業界に最先端のアプリケーションを導入する原動力となる、という意味においてプラスの要素となる。しかしながら、アウトソーシングは、オペレーショナル・リスクの管理が一段と困難化するという問題をも銀行にもたらし得る³⁴。

サーベイから暫定的に判断すれば、銀行は比較的少数の第三者プロバイダーに依存する傾向にあるように窺われる。中小銀行の場合は特にその傾向が強い。中には、それらの第三者が実績のない新設企業である場合もみられる。このように少数の第三者に集中的に依存する傾向が窺われることについて、EBG は更に調査を行う所存である。こうした状況においては、それらのサービス・プロバイダーの何れかに大きな問題が生じた場合にシステミックな影響が懸念されるからである。

銀行は、アウトソーシングに係るリスクを適切に管理するため、第三者サービス・プロバイダーに対してデュー・ディリジェンスを行うとともに、同プロバイダーの企業としての存続能力を継続的にモニターしなければならない。契約条件やサービス水準に関する合意が適切であるか否かについても、リーガル・リスクの観点から注意深く検討しなければならない。事務処理や、セキュリティ・完全性・可用性に係るリスク管理なども、アウトソーシングによって複雑化する。更に、テクノロジー・プロバイダーや提携先の多くは新設の企業であり、銀行業務に必要な統制についての知識を欠いている惧れがある。銀行は、第三者サービス・プロバイダーに極く小さな問題が生じた場合でも、潜在的な財務損失や少なからぬリーガル・リスクおよびレピュテーション・リス

³⁴ 本ペーパーの随所で指摘されているとおり、アウトソーシングの管理は、その他の様々なリスクを成功裡に管理し得るか否かにも影響を及ぼすことを銘記しておく必要がある。

クに晒される可能性がある。電子バンキング業務は多数のベンダーやサービス・プロバイダーに支えられている場合が多いということも問題を複雑化させている。今日まで、実際に支障が発生するには至っていないように窺われるが、今後はこうした問題が潜在的に極めて重大な影響を及ぼし、監督当局と業界の大きな懸念材料となる惧れがある。

アウトソーシングは、プライバシーに関するリスク・エクスポージャーの拡大にもつながる。銀行は、ベンダー等の第三者が如何に顧客データを収集・利用しているかを必ずしも正確に把握しておらず、第三者のそうした活動を適切に管理していない場合もある。また、サービス・プロバイダーやベンダーの法律上の権利や責任は必ずしも明確になっていない。銀行に対しては、ベンダーとの契約締結およびその後の継続的な関係において、プライバシーの問題に対処するよう促すべきである。

世界各国の様々な銀行監督当局は、テーマをテクノロジーのアウトソーシングに絞ったガイダンスを作成している。EBG は、それらのガイダンスを吟味し、この分野において、銀行業界・監督当局双方のサウンド・プラクティスを開発すべく調整を行う方法を模索する所存である。

3. レピュテーション・リスク

電子バンキングのデリバリー・チャンネルが利用不可能になるような何らかの悪条件が発生した場合、銀行の評判は損なわれる惧れがある。銀行は長年にわたり信頼性に係る評判に基づいて業務を行ってきた。電子バンキングにおいても、信頼されるネットワークを提供する能力は決定的に重要であり、インターネット・バンキング・サービスの運営が拙劣であったり、その他の理由で顧客や世間一般から厭離されるような内容であれば、銀行の評判は損なわれかねない。

銀行は、安全、正確かつタイムリーな電子バンキング・サービスを継続的に送達することができなければ、評判を損なう恐れがある。また、電子メールによる照会に答えなかったり、適切なディスクロージャーを行わなかったり、顧客のプライバシーを侵害したりした場合も評判に悪影響が及び得る。

銀行のウェブサイトが第三者やアウトソース先プロバイダーのウェブサイトにはハイパーテキストによってリンクされている場合、特定の商品・サービスの提供者が誰であるか、あるいはそれらの商品・サービスが保険対象となっているか否かについて、顧客の間に混乱が生じる可能性がある。顧客はまた、そうしたリンクは銀行が第三者の商品・サービスを保証していることを意味するのか否かについても誤解し、問題が生じた場合には銀行に補償を求めてくる可能性がある。

更に、銀行ないし銀行の競争相手である異業種のウェブサイト上に甚大なセキュリティ侵害が生じた場合、銀行がインターネット・ベースの取引を適切に運営し得るのか否かについて、消費者ないし市場の全般的信認が揺らぐ恐れがある。

ある銀行にデータやプライバシーの保護に係る何らかの問題が生じた場合は、当該銀行の評判のみならず、類似業務を行っていると考えられているその他全ての銀行の評判が脅かされかねない。

評判が損なわれかねない事態の発生を防ぐため、銀行は自らの電子バンキング業務についてパフォーマンス基準を設定・モニターすべきである。銀行の評判を守るためには、業務の継続性、回復・事故対応に係る計画、および情報通信戦略を定期的に見直し、テストすることも極めて重要である。

4. リーガル・リスク

電子バンキング業務から生じるリーガル・リスクは、懸念が増大しているいまひとつの分野である。既存法規の枠組みは“物理的”な銀行業務の世界に生じる問題を前提として構築されている。従って、全ての国の監督当局は現在、発展途上にある電子バンキングのデリバリー・チャンネルと既存法規の枠組みが如何に影響し合うか、また曖昧な点がないかを検討している。

銀行は、インターネットを通じて他の法域の顧客と関係を結ぶ際に、それらの国に特有の銀行法規や顧客保護法規を熟知していない可能性があり、これがリーガル・リスクを高めている。銀行の側に外国の顧客を勧誘する意図がない場合でも、国によってはオンライン・サービスを提供しているという事実をもって勧誘と見なす可能性がある。例えば、銀行が母国語以外の言語でウェブサイトを開いている場合、その言語が用いられている国の規制当局は当該銀行が自国の居住者にサービスを提供していると判断し、当該銀行に現地の法規を適用しようとするケースが考えられる。

インターネット上で収集した情報の権限外ないし不正使用も、リーガル・リスクの潜在的な原因の一つである。銀行および第三者ベンダーが顧客情報を管理しているデータ・ウェアハウス³⁵は、権限を持たない人物によって攻撃されたり侵入を試みられたりする惧れがある。例えば、ハッカー等が銀行ないしベンダーのデータベースに侵入もしくは自らのデータベースを構築し、当該顧客情報を犯罪目的で使用するといったケースが考えられる。権限を与えられているスタッフが故意にデータを不正使用することもあり得る。銀行およびベンダーを対象として EBG が行ったサーベイによれば、こうした攻撃は、未だ影響は軽微ながら既に行われている。

³⁵ データ・ウェアハウスとは顧客取引に係る大規模なデータベースであり、定期的に更新されてデータ・マイニングの源泉となる。

一部の分野では新たな立法措置が採られつつあるが、それらの法律の有効性も不確実である。電子的契約や電子署名の有効性に係る法律は未だ整備の途上にあり、内容も国によってまちまちである。犯罪防止の観点からは、銀行が有効な“顧客を知る(know your customer < KYC >)”実務を励行することが益々重要になりつつある。

5. その他の伝統的銀行リスク

電子バンキングのデリバリー・チャンネルは、信用リスク、流動性リスク、金利リスク、マーケット・リスクといった伝統的な銀行リスクにも影響を及ぼす。電子バンキングの導入がもたらす影響は、必ずしも銀行のリスク・プロファイルを増減させるものではない。しかし、リスクの様相は変化する可能性があり、しかも変化の仕方は時として複雑である。

(a) 信用リスク

電子バンキング業務は、幾つかの経路により銀行の信用リスクに影響を及ぼし得る。インターネットのデリバリー・チャンネルを用いることにより、銀行は小規模行を始めとして業容を急速に拡大することが可能になり、その結果、資産の質や内部統制に係るリスクが高まることも考えられる。また、インターネットの利用は地理的業務範囲を伝統的な領域の外に拡大することも可能にするため、地域市場の特性やリスクを理解すること、および域外貸出の担保を確認したり質権を確保したりすることが大きな課題となる。予定顧客のアイデンティティーや信用度を確認することは健全な与信決定の必須要素であるが、インターネットはこの作業をも難しくする³⁶。更に、インターネット専門銀行の中には、ネット上で設定する預金に対して高金利を支払う傾向がみられる。こうした場合は、高預金金利を賄うため通常のレベルを超える非優良貸出が行われ

³⁶ 一方、インターネットのデリバリー・チャンネルを利用することにより、銀行は特定の市場産業・市場・地域への与信集中を緩和し得る可能性もある。

る惧れがある。これらのことは、デリバリー・チャネルの何れを問わず、与信引受けに係る方針や、与信のモニタリング・管理実務の健全性が如何に重要であるかを示唆している。

(b) 流動性リスク

インターネット上に情報や誤報が流れるスピードの速さは、銀行の流動性リスク・プロファイルに影響を及ぼす可能性がある。ある銀行についての芳しくない情報は、それが事実あるとないに関わらず、インターネット上で掲示板や通信社を通じて簡単に伝播する。この結果、何時であれ何曜日であれ、預金者は一斉に資金を引き上げることがあり得る。また、インターネットのチャネルを通じて新規に獲得した顧客が金利等の条件のみを理由に口座を維持している限りにおいて、インターネット・バンキングは預金のボラティリティを増大させるということができる。従って、電子バンキングの取引規模によっては、流動性および預貸の変化を従来以上に緊密にモニターする必要がある。

(c) マーケット・リスク

最近においてインターネット上での証券発行・取引が増大していることは、銀行のマーケット・リスク・プロファイルに複雑な影響を及ぼす。市場の観点から見ると、インターネット上における証券取引量の増大は、ボラティリティの増大につながる一方、流動性を高める効果をも持ち得る。個別銀行の観点から見ると、インターネット・バンキング業務を行うことによって当該銀行が預金のブローキングや貸出の売却、証券化プログラムなどに着手したり、そうした活動を拡大したりするならば、マーケット・リスクは増大する可能性がある。銀行・監督当局の双方は、流動性リスクの場合と同様に、電子バンキング業務の拡大が市場のボラティリティに及ぼす影響をモニターする必要がある。

(d) 外為リスク

銀行は、外国の顧客から預金を受け入れたり、自国通貨以外の通貨建の口座を設けたりする時に外為リスクに晒され得る。銀行はインターネットを通じて地理的活動範囲を拡大する機会を得ており、その範囲は国外にまで及ぶ。従って、一部の銀行は電子バンキング業務を通じて、伝統的なデリバリー・チャンネルを通じて被る以上の外為リスクを被る可能性がある。また、外為リスクは政治・社会・経済情勢の変化によっても増大し得るが、クロスボーダー業務の経験が浅い銀行はこうした点を十分理解していない場合がある。監督当局は、銀行がインターネットを通じてクロスボーダー電子バンキング業務を開始する際は、こうしたリスクを適切に管理し得るリスク管理システムと専門知識が当該銀行に備わっていることを確認しなければならない。

V. 銀行監督当局への影響

以上の議論が示すとおり、電子バンキングにおける基本タイプのリスクは新しいものではない。しかし、それらのリスクの独特の発生態様および銀行に及ぼす影響の規模とスピードは、銀行経営者にとっても監督当局にとっても未経験のものがある。リスクの評価は常に動的な作業であるが、電子バンキングを支えるテクノロジーの急速な革新、システムをアウトソースする傾向の強まり、インターネットをはじめとするオープン・ネットワークへの一部商品・サービスの依存といった展開は、厳密かつ継続的なリスク管理プロセスの必要性を高めている。

銀行監督当局は監督下の銀行に対し、リスク管理の3つの基本要素、すなわち、リスクの査定、リスク・エクスポージャーの統制、およびリスクのモニタリングを含んだ包括的なリスク管理プロセスを電子バンキングの分野において整備するよう求めるべきである。この包括的なリスク管理の枠組みは、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なければならない。

また、本リスク管理プロセスは、取締役会や上級経営陣の適切な監視によって支えられ、かつ、電子バンキングの高度に技術的な新展開に対処し得る知識と技能を備えたスタッフによって遂行されなければならない³⁷。

同様に銀行監督当局は、電子バンキングのデリバリー・チャンネルの発達に伴って発生するリスクや課題を確実に理解するため、テクノロジーに関する適切な知識と技能を有する監督スタッフを自ら確保することが決定的に必要であることを認識しなければならない。監督当局は、益々複雑化するテクノロジーと市場の展開に後れを取らないため、既存の監督スタッフに対するテクノロジー面のトレーニングを強化する一方、補強措置として外部の専門家を採用することを優先度の高い課題とすべきである。

VI. 電子バンキングのリスク管理における課題に対応するための次なるステップ

EBG は、健全なリスク管理実務や業界基準を模索するに当っては、それらのガイダンスや基準が健全なリスク管理を伴いかつ電子バンキングの有用な革新や試みを不当に阻害することなく電子バンキングの発展を促進し得るように、継続的な国際協力を行うことが有益であると考えます。従って、EBG の作業計画の Phase （2000 年 6 月～12 月）においては以下の項目に重点が置かれる。

1. EBG は、今日までに EBG メンバーが行ってきた作業を踏まえ、電子バンキング業務における慎重なリスク管理のあり方に係る監督ガイダンス（supervisory guidance）を策定する。本ガイダンスは、バーゼル委員会の

³⁷ バーゼル委員会が 1998 年 3 月に公表したペーパー「電子バンキングおよび電子マネー業務のリスク管理」には、電子バンキングに従事する銀行が考慮すべきリスク管理上の諸点が概説されている。

既存のリスク管理原則を延長したものに相当し、銀行が電子バンキングに関連するリスクを如何に評価・統制・モニターすべきかについて、監督当局が銀行に期待すべき事柄の概要を具体的に述べたものとなる。

- 2 . EBG は、銀行業界およびテクノロジー・プロバイダーと協力のうえ、テクノロジーのアウトソーシング、セキュリティ問題、アグリゲーション等の最重要分野ないし新興分野において、業界の健全なリスク管理実務を認定し、その適用を促進する。
- 3 . EBG は、新しいテクノロジーと生成期にある電子バンキング・ビジネスモデル（例えば、アグリゲーション、企業対企業 / 企業対消費者の電子商取引など）が銀行業界に及ぼす潜在的な影響を引続き分析する。こうした状況の進展は、情報サービスやテクノロジー関連企業の金融部門への参入と相俟って、銀行の商品・サービスのグローバル化および均一化を加速する方向に向かっている。それらが、銀行業界に対して多大な戦略上および競争上の影響を与えるであろう。
- 4 . EBG は、銀行監督当局が開発しつつある電子バンキング関連の監督研修プログラムおよび教材の交換を奨励・促進する。