金融機関における情報セキュリティの重要性と対応策

―― インターネットを利用した金融サービスを中心に ――

平成12年４月18日

■要　　旨■

１．近年、情報通信技術（ＩＴ）の発展に伴い、金融サービスの分野でもインターネットに代表されるオープンシステムが急速に活用され始めている。これにつれて、システムへの不正侵入等を通じた業務妨害、データの盗取・改竄、成りすまし等のリスク（情報セキュリティリスク）を適切に管理していくことが喫緊の課題となりつつある。

２．こうしたリスクが顕現化し、不正送金や業務中断等が生じた場合には、個別金融機関の経営に直接影響を与えるだけでなく、決済システム全体に波及する懸念もある。進展著しいＩＴ革新のメリットを享受しつつ、金融界が健全な発展を遂げていくためには、各金融機関が情報セキュリティの重要性を十分に認識し、経営陣の積極的な関与の下で、状況に応じた的確なリスク管理を組織的・体系的に図っていくことが肝要である。

３．本稿は、こうした認識の下、各金融機関が的確な情報セキュリティ対策を実施するための一助として、情報セキュリティの重要性と対応上の留意点等について取り纏めたものである。

目　次

（情報セキュリティ問題については、日本銀行金融研究所のホームページ（http://www.imes.boj.or.jp/）に暗号化・認証等の技術的なテーマを中心とする各種の論文が掲載されているほか、日本銀行のホームページ（http://www.boj.or.jp/）でも関連の論文を提供しておりますので、ご参照下さい。）

本稿に関する照会先：日本銀行考査局　　電話：03-3277-2598、03-3277-1728

1．はじめに

近年、情報通信技術（ＩＴ(注1)）は急速な発達を遂げており、金融界においても、インターネットに代表されるオープンなネットワークを利用したシステム（以下「オープンシステム(注2)」という）を利用する動きが活発になってきている。

従来、金融機関が採用してきたシステムは、ネットワークに接続できる利用者を限定したもの（以下「クローズドシステム」という）が多く、それに対するセキュリティ対策としては、システムにかかわる内部者による不正行為の防止等に力点が置かれてきた。

こうした中にあって、オープンシステムの活用は、一方で利便性の高い金融サービスの提供を可能とすると同時に、リスクの多様化や複雑化をもたらしている。すなわち、クローズドシステムの下でも内在していたリスクの中で、システム障害や内部不正行為などはクローズド、オープンを問わず共通するほか、顧客への成りすましやネットワークを流れる情報の盗取・改竄等といったリスクはオープン化に伴い格段に高まってきている。加えて外部からの不正侵入、業務妨害といったオープンシステムに固有の新たなリスクも出現しつつある（本稿では、こうしたオープンシステムの活用に伴うリスクを一括し「情報セキュリティ(注3)リスク」と呼ぶ）。

このように多様化、複雑化しつつある情報セキュリティリスクを金融機関が適切に管理していくためには、他のリスク管理と同様に、まず、リスクを正確に把握したうえで必要な対策を確立し、それを着実に実践していくことが必須の課題となる(注4)。

本稿は、自らのシステム運行に関する経験に加え、情報セキュリティに関する調査・研究、内外関係機関との対話や考査等を通じて日本銀行が蓄積したノウハウに基づき、金融機関が情報セキュリティリスクを管理するうえでの要点を整理したものである(注5)。また、別添の「インターネット利用システムにおける情報セキュリティ対策のチェックポイント」は、インターネットを利用した個別システムにおける情報セキュリティ対策をチェックするうえでの主な項目を示したものである。本稿とあわせて、各金融機関が情報セキュリティ対策を策定、運用する際の一助となることを期待している。

（注１）ＩＴ（Information Technology）とは、コンピューターやネットワークに関する情報通信技術全般をいう。

（注２）オープンシステムは、本稿のようにネットワークの性格に着目して定義することが多いが、このほかに、ＵＮＩＸのようにプログラムの設計思想が広く公開されていたり、複数のコンピューターが処理を分散しながら相互に連携し全体として機能するようなシステムを指す場合もある。

（注３）情報セキュリティは、一般に「組織固有の情報やシステムを正当に保護し（機密性）、真正な状態を保ちつつ（完全性）、必要時に有効に利用できる（可用性）状態を確保すること」と定義されることが多い。

（注４）我が国全体としても、情報セキュリティ対策の重要性に関する認識がこのところ急速に高まりつつある。本年２月には「不正アクセス行為の禁止等に関する法律」が施行されたほか、「電子署名及び認証業務に関する法律案」が検討されているなど、電子政府実現に向けた情報セキュリティ面への取り組みが本格化し始めている。

（注５）クローズドシステムにおける情報セキュリティ対策については、既に各金融機関が比較的手厚い対応を取ってきていることもあり、本稿では省略する（詳しくは、（財）金融情報システムセンター＜ＦＩＳＣ＞作成の「金融機関等コンピュータシステムの安全対策基準」等を参照）。

2．情報セキュリティリスクの高まり

（1）オープンシステム化の進展と情報セキュリティリスク

我が国の金融機関では、経営環境が急速に変化する中で、顧客に利便性の高い金融サービスを迅速かつ安価に提供することが経営上の重要課題であるとの認識を強めており、こうした目標を実現する有力な手段として、近年発達の著しいＩＴの活用を進めてきている(注6)。

特に、インターネットに代表されるオープンシステム分野では、画期的な技術革新を背景に、従来のシステムに比べて格段に低コスト、短期間でシステムを構築し、広範囲の顧客にサービスを提供することが可能となってきている。金融界でも、顧客基盤の確立等の経営課題に迅速に対応していくことを強く意識し、その手段としてインターネットを利用する動きが広がっている(注7)。

一方、金融業務におけるＩＴの活用度合いの高まりやオープンシステムの利用拡大は、個別金融機関のリスク管理という観点からみると、新たな対策を要する情報セキュリティリスクを生み出している。

（新たなリスクの発生と従来からのリスクの増大）

これまで我が国の金融機関では、大型汎用コンピューターを中心としたクローズドシステムを前提に、①電算センターへの入退館の管理や専用回線によるネットワーク構築といった物理的な隔離、②独自のソフトや通信プロトコル（規約）の使用、③店舗内での防犯ビデオや目視による不正監視、等のセキュリティ対策を施してきた。こうした体制や施策の下では、外部からのセキュリティ侵害の可能性は比較的低かったと考えられる。

しかしながら、オープンシステム化の進展に伴って、外部からの侵入や情報の盗取等が従来に比べ遥かに容易となってきている。すなわち、金融機関内部の業務処理システムと外部ネットワークの接続に伴い、共通の通信プロトコルが利用されつつあり、また、顧客が取引に際して利用する端末も、ＣＤ・ＡＴＭと異なり金融機関の管理が十分には及ばない機器が増えてきている。

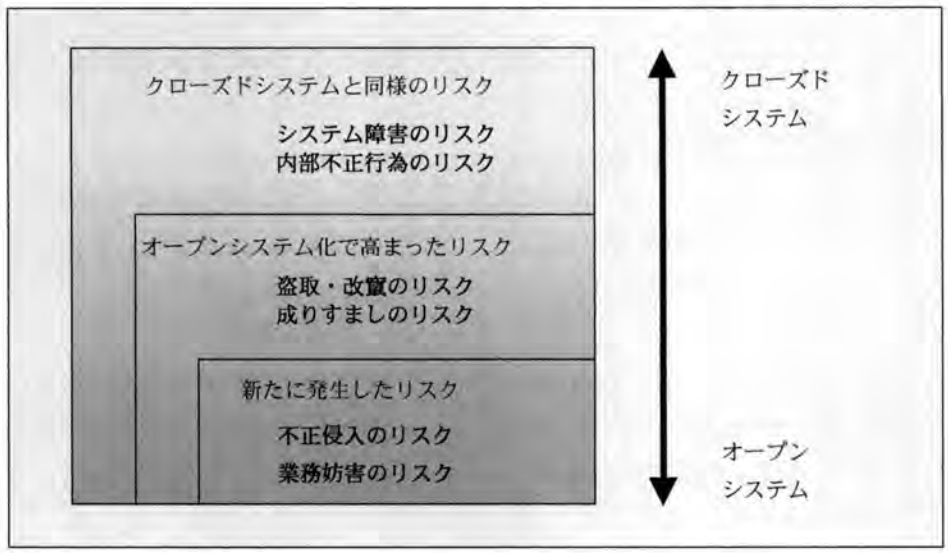
この結果、新たに、①外部から内部システムへの不正侵入（ハッキング）や業務妨害のリスクが生じているほか、従来からの②ネットワークを流れるデータの盗取による暗証番号等の不正入手、③通信データの改竄による不正送金、④取引相手等への成りすましによる資金不正取得、等といったリスクも格段に高まってきている（図表１参照）。

例えば、不正侵入や業務妨害については、高度な安全対策を施している米国の国家機関等でも度々ハッキングの被害を受けている。我が国でも本年１月以降、中央官庁等のホームページが改竄され、サービス提供が中断したほか、金

（注６）金融業は、もともと「商品に形がなくデータ処理が業務の核心である」という意味で典型的な情報産業であり、ＩＴをいかに活用していくかが金融機関経営上のキーポイントになってきている。実際、金融機関統合等を巡る最近の動きの中でも、巨額のＩＴ投資の効率化が統合等の一つの狙いに掲げられている。

（注７）インターネット・バンキング業務を開始する金融機関が目立つほか、異業種からの参入を含め、インターネット専業銀行やオンライン・トレーディングに特化した証券会社の設立を目指す動きがみられる。

（図表１）オープンシステムの利用拡大と新たなリスクの発生



融機関においても、セキュリティ侵害を被るケースがみられ始めている。また、サービスを提供しているシステムに許容量を超えるアクセスを集中させ、システムダウンを引き起こすことによって業務妨害が行われることもある（注８）。こうした事態が資金移動等を伴う金融サービスにおいて発生した場合には、単なる情報提供サービスの中断とは比べものにならない大きな影響（注９）が、当該金融機関のみならず決済システム全体にまで及びかねない。

（アウトソーシングの進展に伴う留意点）

最近は、金融機関でも、システムの開発から運用に至る業務を関連会社に委託したり専門の業者に任せる等、多様な形態でのアウトソーシング化が進展している。この結果、情報セキュリティの対象であるシステムそのものが金融機関の直接的な管理下から離れるケースが増えており、情報漏洩等のリスクの生じる余地が拡大している。その対応策としては、業務委託先との間のアウトソーシング契約において、遵守事項を明確化したりシステム監査実施の権利を留保する等、自らのセキュリティを主体的に確保するための方策を講じる必要がある。

（２）金融サービスへの影響

個別金融機関において業務妨害や不正侵入等の情報セキュリティリスクが顕現化すると、一時的にせよサービスの提供を中断せざるを得ない事態となる。こうした場合、単に業務運営上

（注８）本年２月、海外のオンライン・トレーディングに特化した証券会社等が提供するサービスにおいて、許容量を超えるアクセス集中により業務を中断させられた事例があった。

（注９）既に海外では、大手米銀が数十回にわたる不正侵入を受けた結果、計１千万ドルの大金が不正送金された事例が発生している。

の支障にとどまらず、金融機関としての信認を損なうレピュテーション（風評）リスクや、情報セキュリティ対策が不十分であったことを理由に訴訟を提起されるリーガルリスクも招くなど、当該金融機関は経営面でも少なからぬダメージを蒙る惧れがある。

さらに、近年、金融機関間の各種決済は高度にシステム化されており、ある金融機関のシステムの稼働がひとたび停止すると、当該金融機関の業務継続が困難となるだけでなく、決済システム全体に影響を与える可能性がある。各金融機関においては、システムの稼働停止が自らの問題だけにとどまらず、他の決済システム参加者にも多大な影響を与える可能性がある点を十分認識し、未然の防止対策を練るほか、素早い復旧のためのコンティンジェンシー・プランを整備しておく必要がある(注10)。

3．情報セキュリティポリシーの策定

金融機関の各種業務処理にオープンシステムが導入され始めたことを契機に、組織内の様々な部署が情報セキュリティ対策への取り組みを迫られるケースが増えている。こうした状況の下で、組織全体が足並みを揃え効果的に対策を進めていくためには、まず、その方針や具体的な内容を明文化し、組織全体に周知・徹底することが求められる。

従来、我が国の金融機関でも、情報セキュリティに関する対策がなかった訳ではないが、あくまで個別システム毎に講じられていた例が多く、全システムを対象とする横断的な対応は、欧米金融機関に比べて遅れていたように見受けられる。この点、オープンシステムの利用の拡大は、組織全体にかかる情報セキュリティリスクの的確な把握や、適切な対応策の策定・実施に向けての方針および基準の整備を迫っていると言っても過言ではない。

(1) 情報セキュリティポリシーとは何か

以上のような要請に対応するために、情報セキュリティ対策構築に当たり組織内で適用される考え方や方針を体系化したものを、「情報セキュリティポリシー(注11)」という。これは、組織が所有する情報およびシステムのセキュリティを適切に保護するための対応方針であり、通常、「情報セキュリティ対策に関する基本的な考え方（基本方針）」と「組織全体に共通する具体的な対策やクリアすべき基準（スタンダード）」から成ることが多い(注12)。因みに、情報セキュリティポリシーの基本方針に盛り込まれることが多い項目は、図表2のとおりである。

(注10) システム障害の発生を含めた個別金融機関の決済リスク管理の必要性については、「金融機関の決済リスク管理について」（『日本銀行調査月報』2000年2月号）を参照。

(注11) 情報セキュリティポリシーについては、金融監督庁が昨年公表した金融検査マニュアルにおいて、リスク管理の一環としてその重要性が指摘されている。また、ＦＩＳＣの「金融機関等におけるセキュリティポリシー策定のための手引書」[1999]で、策定手順等につき詳しく解説されている。

(注12) さらに、各個別分野における具体的な情報セキュリティ対策を記した文書（規程、マニュアル、手順書等）までを含める場合もある。なお、情報セキュリティポリシーの策定手順としては、保護すべき情報およびシステムを特定し、その重要性や脅威の大きさ等を考慮したうえで「基本方針」を策定することが大切である。次に、各々の脅威が発生する可能性や発生時のダメージを踏まえてリスクを評価し、セキュリティ対策が満たすべき基準（スタンダード）を設定することが望ましい。

（図表２）情報セキュリティポリシー（基本方針）の項目例

① 情報セキュリティ対策の目的と対象範囲
- 情報セキュリティ対策に関する基本的な考え方
- 保護されるべき情報およびシステムの対象範囲と保護理由
- 保護されるべき情報およびシステムの優先順位

② 情報セキュリティ対策の推進体制
- 経営陣の関与と責任、情報セキュリティ担当役員の任命とセキュリティ統括部署の設置
- 法律や規制等に関する法務部門のチェック、コンプライアンス
- 外部コンサルティングの利用等

③ 情報セキュリティ対策の運営
- 想定される情報セキュリティリスクとその管理
- 情報セキュリティ対策実施に関する決定プロセス
- 情報セキュリティ対策の見直し手続き
- 具体的な情報セキュリティ施策の概要

④ 利用者の管理と情報セキュリティ面での教育
- 各役職員の責任と違反時の取り決め（罰則等）
- 情報セキュリティ対策の遵守状況チェック（自己点検、内部検査）
- 情報セキュリティポリシーの啓蒙

⑤ 危機管理
- システムにおける障害発生時の対応

⑥ その他
- 定期的な情報セキュリティポリシーの見直し手続き

（2）情報セキュリティポリシーの効用

情報セキュリティポリシーの策定は、組織全体として総合的かつ効率的な情報セキュリティ対策の実施を通じて、図表3に示すようなセキュリティレベルの向上などの効用を金融機関にもたらすものと考えられる。

（図表3）情報セキュリティポリシーの効用

① 情報セキュリティの重要性に対する認識が組織内（特に経営陣）で高まり、必要な経営資源が情報セキュリティ対策に向けられる。

▼ 組織全体のセキュリティポリシーへの理解が進むことにより、必要な経営資源の投入が行われ易くなり、個別システムの開発過程においても必要なセキュリティ対策の実施に向けてのインセンティブが働く。

② 統一された基準に従ってセキュリティ対策が講じられることにより、組織全体として一定の情報セキュリティレベルが確保される。

③ 従来講じられてきた情報セキュリティ対策の不備が明確になり、リスクの把握が容易になる。

▼ 情報セキュリティポリシーに沿って考えれば、例えばオープンシステムで磁気キャッシュカードを使用する際にはセキュリティレベルの観点から相応の対策を講じることが求められ、現在金融機関が進めつつあるＩＣカード化の促進に繋がる（注13）など、旧来のセキュリティ対策を見直す（注14）契機ともなる。

④ 新たにシステムを開発する都度、当該システムの情報セキュリティ対策を効率的に検討することが可能となる。

⑤ 情報セキュリティ上の問題が発生した場合に、迅速な対応が期待できる。

（注13）本年3月から本格的に展開されたデビットカード（J-Debit）では磁気キャッシュカードを用いているが、参加者は限られているものの一部公衆回線を利用しているなど、オープンシステムの側面も有している。このため、ＩＣカード化の促進など、同じ磁気キャッシュカードを利用するＣＤ・ＡＴＭより一歩踏み込んだリスク管理を考慮する必要がある。

（注14）例えば、暗号化については、所謂「スクランブル」（四則演算等による簡易なデータ変換方式で処理方法を秘匿する方式）では不十分と考えられ、国際標準等を参照しながらより本格的な暗号技術の利用を検討することが望ましい。

（3）経営課題としての情報セキュリティポリシーの整備

（経営陣の強い関与による組織的対応の重要性）

これまで述べてきたように、金融機関においてＩＴの重要性やそれに伴うリスクが高まりつつある状況に照らすと、情報セキュリティリスクの管理は組織全体で取り組むべき重要な経営課題の一つとなってきている。

その際、所要のセキュリティレベルを確保するためには相応の経営資源の投入を要するほか、金融機関内の各部署より十分な理解と協力を得る必要がある。この点、通常、各役職員には情報セキュリティ対策の直接的なメリットが意識されにくいこともあって、ボトムアップの形態での対策進捗は容易でない。したがって、経営陣が、自社のＩＴ戦略等を踏まえつつ、情報セキュリティリスクの正確な把握、必要な対策の立案など、リスク管理に積極的に関与することが望まれる。

（情報セキュリティポリシーの周知と運用）

具体的には、経営陣がリーダーシップを発揮して情報セキュリティポリシーを定めるとともに、情報セキュリティに関する各部署の責任やポリシーが遵守されずに問題が生じた場合のルール等を明確化することにより、「組織全体にポリシーを遵守させる」との強い意思を明確に示すことが必要である（注15）。

特に、情報セキュリティリスクを定期的に把握する過程でポリシーに反する事項が判明した場合に、責任部署が所要の対策を立案するとともに、統括部署もしくは責任者が個別にこうした対応を承認する手続きも定めておくことが重要である。また、内部監査ないし検査が情報セキュリティポリシーの遵守状況をチェックすることも、ポリシーの実効性を高めていくのに有益であろう。

なお、情報セキュリティポリシーそのものも定期的な見直しが求められる。僅か１か所の情報セキュリティの弱点（セキュリティホール）からでも、不正侵入などが発生する惧れがあることから、最新のセキュリティ情報を定期的に確認し、必要に応じてセキュリティポリシーそのものも見直す体制を日頃から整えておくことは、重要なポイントである。

（国際的な標準との整合性）

グローバルな業務遂行やシステムの接続が進展する中で、我が国金融機関の情報セキュリティポリシーも国際水準と整合的であることが求められつつある。そのためには、最新の技術動向も踏まえつつ、国際標準化機構（ＩＳＯ）が策定している国際標準や各種ガイドライン（注16）を適宜参照しながら、自らの対応の妥当性を常時点検しておくことが望ましい。

（注15）情報セキュリティ統括責任者を任命するとともに、金融機関の規模や業務内容等によっては、システム開発、ユーザーのいずれの部門からも独立した情報セキュリティ統括部署を設けることが望ましい。

（注16）情報セキュリティの国際標準に関しては、前出ＦＩＳＣ作成の手引書のほか、以下の指針等が参考となる。詳しくは、岩下直行・矢田部充子「金融分野における情報セキュリティ技術の国際標準化動向」（『金融研究』18-2［1999］、日本銀行金融研究所）、宇根正志・中原慎一「最近の金融業務における情報セキュリティ評価・認定を巡る動向について」（同19-別冊1［2000］）を参照。

①ＢＳ７７９９：Code of practice for information security management（英国国内の情報セキュリティ対策に関する行動指針）

②ＩＳＯ／ＴＲ１３５６９：Banking and related financial services - information security guidelines（金融機関における情報セキュリティ対策に関する行動指針）

③ＩＳＯ１５４０８：通称 "Common Criteria"（情報セキュリティ製品・システムの評価基準を規定した国際標準）

4．情報セキュリティ対策の確立

（1）情報セキュリティ対策の適切な組み合わせ

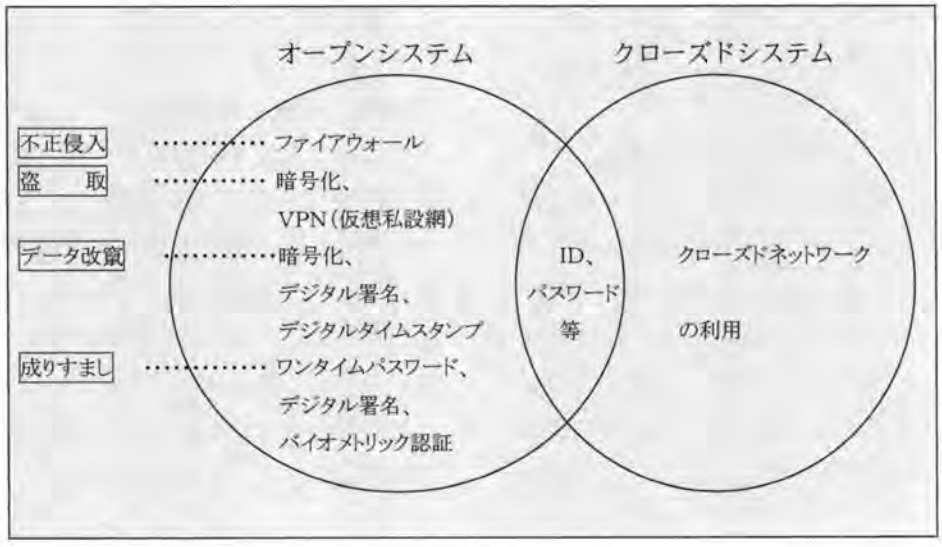
情報セキュリティポリシーが定まると、個別システムに求められるセキュリティ水準や具体的なセキュリティ対策の内容も自ずと決まってくる。クローズドシステムの場合には、主要な機器を電算センター内に囲い込むことによって、リスクをシステム部門、とりわけ運用部署に隔離することが可能であった。これに対し、インターネットに代表されるオープンシステムが主要な業務に活用される場合には、必要な情報セキュリティレベルを確保するため、図表4のような様々なセキュリティ技術が必要となってくる。

もっとも、こうしたセキュリティ技術は、今のところコスト面や普及度の制約から、利用者にとって必ずしも使い易いものばかりでない。したがって、各金融機関においては、情報およびシステムの重要性等に応じて許容できる情報セキュリティリスクの大きさを判断し、コスト面も睨みながら、各種の技術を適切に組み合わせることにより、総合的な対応を図っていく必要がある（注17）。

（2）新技術の適時適切な取り込み

公開鍵暗号を利用した電子認証（注18）は既に確立した技術であり、暗証番号による認証よりもセキュリティレベルが高いとされているが、

（図表4）オープンシステムにおける情報セキュリティ対策例



（注17）例えば、インターネット・バンキングにおいて顧客の真正性（間違いなく本人であること）を確認する手段としては、暗証番号（パスワード）が一般的であるが、情報セキュリティ対策上、万全とは言い切れない。したがって、業務面で取引限度額を設定したり、運用面で利用者に対し誕生日等の類推可能な暗証番号を使用しないよう注意を喚起するほか、システム面で暗証番号の桁数を増やすなど、いくつかの対策を組み合わせることが必要である。

（注18）電子認証とは、認証機関が発行する電子認証書を用いて、通信相手の真正性を確認したり、電子的な取引データが途中で改竄されていないことを証明すること。詳細は、谷口文一「金融業界におけるＰＫＩ・電子認証について」（『金融研究』19-別冊1［2000］、日本銀行金融研究所）を参照。

顧客にとって使い勝手の悪さ等もあって、現時点ではインターネット・バンキングなどにおける顧客認証手段として必ずしも普及していない(注19)。もっとも、秘密鍵や電子認証書を格納したＩＣカードの価格が下がり一般的な決済手段として利用可能となれば、金融機関が公開鍵暗号を利用し易くなると考えられる。

このほかにも「誰が、いつ、どんなデータを作成し送付したか」を第三者が証明する「電子公証」の技術である「デジタルタイムスタンプ」や、身体的な特徴（指紋、網膜、筆跡、声紋等）を利用した「バイオメトリック認証」など、新たな認証技術が進歩しつつある(注20)。将来、技術の進歩やその普及に伴い導入の条件が整った場合、あるいは取引限度額の引き上げなどによりリスクが増大した場合等には、必要に応じて、新技術を積極的に採用していくことが適当である。

オープンシステムを構築するハード・ソフトの技術進歩はテンポが速く、情報セキュリティ上の弱点（セキュリティホール）が数多く生じているうえ、それを放置しておくとシステム全体のセキュリティ水準が低下し、ハッキング等に悪用されかねない(注21)。セキュリティホール情報が得られた場合には、各システムで問題が実際に生じていないか早急に調査し、適切な対応策を講じなければならない。この際、その時点の環境でどの程度のリスクをもたらすかを適切に評価し、必要と判断される経営資源を遅滞なく投入し、早急に対策を講じていくことが求められる(注22)。また、日頃より技術面の動向を可能な限りフォローしていくことが望ましい。

（３）情報セキュリティ対策の適切な運用

情報セキュリティ対策は、個々の施策を構築するだけで有効な結果をもたらすものではない。例えば、不正侵入への対策では、ファイアウォール(注23)を設けるだけではなく、常に不正侵入の可能性を意識して、侵入行為の兆候を監視することが欠かせない。侵入の手口やファイアウォールの弱点に関する情報を集め対応を施すことによって、侵入の危険性を低下させることができる。また、万一侵入された場合に備え、被害を最小限に抑える応急措置や迅速な連絡体制等を予め用意しておくことも大切である(注24)。このほか、専門業者等に依頼して実施する侵入

(注19) 現在では、公開鍵による電子認証ではなく、アクセス時と資金移動時に異なる暗証番号を設定したり、送金先口座の限定、送金上限額の設定等の手法を組み合わせて、成りすましリスクの軽減を図っている金融機関が多い。

(注20) 新しい認証技術の詳細については、宇根正志・松浦幹太・田倉昭「デジタルタイムスタンプ技術の現状と課題」(『金融研究』19-別冊１［2000］、日本銀行金融研究所)、中山靖司・小松尚久「バイオメトリックスによる個人認証技術の現状と課題」(同［2000］)を参照。

(注21) セキュリティホールが発見されていたにも拘わらず、これを放置しシステムを使用し続けた結果、外部から情報セキュリティを侵害された事例が発生している。

(注22) セキュリティレベルを維持するために重要なこうした対応については、情報セキュリティ統括責任者が、暫定的および抜本的な対応の要否や内容の適否を判断していくことが望ましい。

(注23) ファイアウォールとは、外部のネットワークとの接点に設置され、予め定められた種類のデータ通信のみを可能とすることで、不正侵入や不用意な情報流出を阻止するための関所として機能する機器等をいう。

(注24) 情報セキュリティの侵害に起因してシステム全体が停止したり、業務に重大な影響が生じる場合も想定しておく必要があり、コンティンジェンシー・プランの中に、情報セキュリティ侵害が発生した場合の対応も盛り込んでおくことが有益である。

テストは、個々のセキュリティ対策の有効性を確認するうえで有益である。このように、適切な運用・管理が伴ってこそ情報セキュリティ対策はその真価を発揮することとなる。

情報セキュリティ対策のレベルを維持・向上させるためには、運用サイクルを確立することが極めて重要である。すなわち、①情報セキュリティ面でのリスク分析（どこに、どのようなリスクが、どの程度存在するかの調査）を行う、②把握したリスクについて技術・運用両面からの対応策を検討・実施する、③職員（派遣社員、パートやアウトソーシング先職員を含む）の教育・啓蒙を行う、④情報セキュリティにかかる監査により運用状況を確認する、⑤監査結果を次回のリスク分析に反映する、という組織的、継続的な運用面におけるサイクルを確立する必要がある。

また、分散処理技術を用いたシステムの利用が進んだ結果、セキュリティ対策の手薄な部分が無意識に放置されていたり、システムの構築後、時間の経過とともに技術環境の変化により従来のセキュリティ対策では不十分となってくるケースもある。特に、インターネットを利用したシステムでは情報セキュリティを損なうような要因が次々と発見され、対策との間でいたちごっこになるケースも少なからずみられる。こうしたケースでも、情報セキュリティ対策の運用サイクルが確立されていれば、定期的に点検が行われ、改めてリスクを把握し、組織全体による効果的な対応を図ることも可能となると考えられる。

5．おわりに

以上述べてきたとおり、これからの金融機関は、ＩＴ革新のメリットを十分に享受して経営発展の梃子としていくためにも、情報セキュリティの重要性を十分に認識し的確な対応策を取る必要がある。

もとより、求められるリスク管理の内容と水準は、各金融機関のシステム構成や業務内容により大きく異なるほか、技術革新等の変化が激しいため、「こうすれば大丈夫」といった一律の考え方は存在しない。各金融機関においては、国際機関や標準化団体等が公表している各種のガイドライン類なども参照しながら、常に自らの対応を見直し続けていく必要があろう。

日本銀行としては、各金融機関におけるそうした取り組みを積極的にサポートしていくとともに、個別金融機関のリスク管理の観点から、金融機関における情報セキュリティリスクの管理状況についてフォローしていく方針である。先に発表した「平成12年度の考査の実施方針等について」（本『日本銀行調査月報』「経済要録」に掲載）で触れたように、情報セキュリティ面に重点を置いたターゲット考査の実施も含めて、今後とも金融機関の実情把握と所要の施策の実行を促していきたい（注25）。

（注25）因みに、欧米の中央銀行等でも情報セキュリティに関するチェックポイントを公表するとともに、ＩＴに重点をおいた検査を行っている事例が見受けられる。

（別　添）

インターネット利用システムにおける情報セキュリティ対策のチェックポイント

（本チェックポイントの位置付け）

このチェックポイントは、金融機関が情報セキュリティリスク管理面での自らの対応状況を点検する際の参考に供する目的で、インターネットを利用した個別システムにおける情報セキュリティ対策をチェックするうえでの主な項目を整理したものである。

（利用に当たっての留意点）

チェックポイントの取り纏めに当たっては、オープンシステム化の進展に伴い一段とリスクが強まっている項目、および新たにリスクが生じている項目を中心としている。このため、電算センター等の建物、設備の安全対策等については触れておらず、また、組織内の全システムに適用することを想定したものでもない（ここに記載のない項目については、関連機関・団体等が公表している各種ガイドライン類を参照頂きたい）。

Ⅰ．情報セキュリティポリシー整備上のポイント

1．情報セキュリティポリシーの整備

（1）情報セキュリティ対策の目的、対象範囲を明確にしているか。
（2）情報セキュリティ対策を推進するための組織・運営体制を明確にしているか。
（3）情報セキュリティ対策に関する全役職員の責任や義務を明確にしているか。
（4）組織全体の情報セキュリティリスク（業務妨害、情報の盗取・改竄、成りすまし等）を把握するとともに、その対策を検討し、実施に移しているか。
（5）障害や不正行為等によりサービス提供が中断された場合における対応方針を明確にしているか。
（6）情報セキュリティポリシーを適用できない例外ケースの取り扱いを明確にしているか。
（7）アウトソーシング化やベンダーの活用に当たり、情報セキュリティポリシーの適用ルールを明確にしているか。

Ⅱ．情報セキュリティ対策策定上のポイント

1．情報セキュリティ対策の策定

（1）情報セキュリティポリシーを踏まえて情報セキュリティ対策を策定しているか。

① 情報の重要性やリスクの大きさ等を勘案して、業務面、システム運用面を含めた総合的な対策を講じているか。

② 情報セキュリティポリシーに沿わない対策を講ずる場合にも、同ポリシーに定められた手続きに従って承認しているか。

③ アウトソーシング化やベンダーの活用に当たり、委託先の運用状況を確認する体制を整備しているか。

（2）情報セキュリティ対策は、情報の重要性やリスクの大きさ等を踏まえ、最新のセキュリティ情報により定期的に見直しているか。

（3）インターネット接続により生じるシステム技術・運用面での弱点や情報セキュリティリスク顕現化の可能性を、最新の情報に基づき把握しているか。

（4）ベンダー等とネットワークを接続する場合には、相手方の情報セキュリティ対策をチェックしているか。

Ⅲ．情報セキュリティに関する体制面でのポイント

1．経営陣の関与

（1）経営陣は、情報セキュリティポリシーとその対策を承認しているか。

（2）経営陣は、情報セキュリティリスクの所在とその程度を認識しているか。

（3）システムの運営に支障をきたす不正行為等が発見された場合、経営陣は直ちに報告を受け、対策を指示する体制となっているか。

（4）経営陣は、情報セキュリティ侵害時の対応を含むコンティンジェンシー・プランを承認しているか。

2．情報セキュリティ統括部署の関与

（1）情報セキュリティ統括部署（もしくは統括責任者。以下同じ）は、情報セキュリティリスクの評価結果や同結果に基づき策定された情報セキュリティ対策の内容をチェックしているか。

（2）同部署は、各部署に対し定期的に情報セキュリティ対策を見直すように求めているか。

（3）同部署は、システム部門から独立していることが望ましい。

3．監査部門等の関与
（1）被監査部門から独立した監査部署が情報セキュリティにかかる監査を実施し、情報セキュリティポリシーの遵守状況や情報セキュリティ対策の妥当性等を検証しているか。 （2）システムの重要度に応じて、外部監査を受けることが望ましい。
4．法務部門の関与
（1）インターネットを用いて新規に業務を開始するに当たり、法務部門が取引規約等に記載される金融機関の責任範囲を確認しているか。 （2）法令改正等を受け、取引規約などでカバーしきれない法的なリスクの可能性について見直しているか。

Ⅳ．新たな情報セキュリティ対策のポイント

1．ファイアウォール
（1）ファイアウォールの導入および運用に当たり、適切な対策を講じているか。 ① 適切な通信制御ルールを整備し、適切に運用しているか。 ② ファイアウォール機器の物理的な管理を含め、適切なアクセス管理を行っているか。 ③ 通過する通信データを的確にモニタリングする体制を整備し、適切に運用しているか。 ④ ファイアウォールへの通信記録をログとして保存しているか。 ⑤ ファイアウォールの仕様に関するドキュメントを適切に管理しているか。 （2）ファイアウォールのセキュリティホール等に関する情報を収集し、所要の対策を講じているか。 （3）専門家等による侵入テストを実施するなど、ファイアウォールの信頼性を定期的に確認することが望ましい。
2．暗号
（1）機密性の高い情報を送受信する場合に、情報を暗号化しているか。 （2）暗号の利用および管理において、適切な運用ルールを整備し、適切に運用しているか（暗号鍵の管理ルールを明確にしているか）。 （3）暗号を利用するに当たっては、適切なセキュリティ評価を行うことが望ましい。 （4）公開鍵を使用する場合に、ペアとなる秘密鍵について適切に取り扱っているか。 ① 鍵の生成に使用した秘密鍵の推測などセキュリティ上の問題が発生していないことを、最新のセキュリティ情報に基づき定期的に確認しているか。 ② 鍵の配送・保管に当たっては、耐タンパー性（無理に鍵を盗取しようとすると当該鍵を消去してしまう等の特性）を有する装置等を利用することによって、秘密鍵の秘匿性および真正性が損なわれることがないよう配慮しているか。

3．電子署名
（1）高額な資金移動を伴うなどリスクが極めて大きな場合には、電子認証書等による利用者の認証を行っているか。 （2）重要な情報を送受信する場合には、漏洩や改竄等を防止するため、電子署名を利用することが望ましい。 （3）独自にＣＡ局（Certification Authority：認証局）を運営する場合には、運営方法に関するルールを整備し、ルールに沿って適切に運用しているか。 （4）ＣＡ局を第三者機関に委託する場合には、当該ＣＡ局の信用度、能力、責任範囲等を十分に考慮しているか。
4．業務妨害対策
（1）サーバーをダウンさせる目的で短期間にシステムの許容量を超えるアクセスを集中する攻撃（Denial of Service attack）を想定し、代替的な業務遂行策を立てているか。 （2）組織全体としてウィルス検知体制や同対策に関する運用ルールを整備し、適切に運用しているか。

Ⅴ．既存情報セキュリティ対策のポイント

1．ユーザーＩＤ、パスワード管理
（1）ユーザーＩＤの不正利用を抑止する対策を講じているか。 ① 一定回数以上ログインの失敗が繰り返された場合には、ログインが制限されるか。 ② システム用ＩＤ（特権ＩＤ等）については、必要に応じ、動的パスワード（専用装置によって生成される毎回異なるパスワード）を採用することが望ましい。 （2）適切なパスワード管理を行っているか。 ① パスワードは利用者が設定・変更する扱いとしているか。 ② パスワードを盗取することが困難になるよう配慮しているか。 ③ パスワードの変更をユーザーが定期的に行うようなシステムになっていることが望ましい。
2．障害対策、データの保全等
（1）データバックアップや通信記録の保全に当たり、取得タイミング、取得方法、保存形態、保存期間を定め、適切な運用を行っているか。 （2）監査記録として必要な情報（ユーザーＩＤ、使用した機能・データ、当該情報の変更の有無、利用日時、利用した機器・ネットワーク等）を取得しているか。

3．その他
（1）取引ピーク時も考慮したデータ量を用い、レスポンスなど所要の性能評価を適切に行っているか。 （2）資源管理面で、プログラム等が不正にインストールされたり、システムが不適切に利用されていないことを定期的に確認していることが望ましい。

Ⅵ．システム運用面でのポイント

1．システム運行のモニタリング
（1）ユーザーＩＤの不正な利用を監視するなど適切なモニタリング体制を整備しているか。 ① 不正アクセスの兆候があった場合の備えとして、応急措置を含め適切な対策を準備しているか。 ② システムの運行に当たり、ベンダーまたは特定の担当者に過度に依存することのないよう配慮していることが望ましい。 （2）情報セキュリティ面で問題が発生した場合の取り扱いを定め、周知しているか。
2．システムの変更管理
（1）システム変更に関するルールを整備しているか。 ① ハードウェア、ソフトウェアへの無権限者によるアクセスを制限しているか。 ② ハードウェア等の廃棄時に重要情報等を漏れなく削除しているか。 ③ ベンダーがハードウェアやソフトウェアをインストールする際に、不正行為がないことを確認しているか。
3．コンティンジェンシー・プランの整備
（1）実効性のある障害時対応策を策定しているか。 ① 緊急時の対応マニュアルが整備されているか。 ② システムを修正するに当たり、適切なシステム変更手続きを整備しているか。 ③ システム変更に伴うマニュアルの修正や緊急連絡網の差し替え等を確実に行っているか。 （2）コンティンジェンシー・プランについては、定期的に訓練を行い、その結果等を踏まえて適宜更新していくことが望ましい。
4．アウトソーシング、ベンダー管理
（1）システム運用等をアウトソーシングしている場合には、アウトソーシング先の情報セキュリティに関する管理体制等を確認し、その状況について適宜モニタリングしているか。 （2）ベンダー等に作業を依頼する場合には、情報セキュリティ面からの委託条件を明確にするとともに、その遵守状況を適切にモニタリングしているか。

5．システム要員等に対する啓蒙
（1）情報セキュリティ面で必要な知識や技術を備えた人材を育成しているか。 （2）職員等（派遣社員、パートを含む）に対し、情報セキュリティに関する研修の機会を十分に提供しているか。 （3）最新の情報セキュリティに関する注意事項等が、職員等に周知される体制になっていることが望ましい。