海外金融業界動向

“電子的なコミュニケーション内容のセキュリティ管理”

インターネットや携帯電話の普及に伴って、今や電子メールに代表される電子的なコミュニケーション手段は確実に日常的な手段として定着しつつあります。欧米の金融機関でもこうした電子的コミュニケーション手段を顧客とのリレーションやマーケティング活動に利用しようとしていることは言うまでもありません。しかし、その一方で電子メールなどに書かれている個人情報その他機密情報に係わるセキュリティ対策に対する関心も高まっています。そこで今回は、規制監督当局の動きも含めて欧米金融業界における電子的なコミュニケーション内容の保存や管理に関してどのような取り組みが行われているか、ＩＴの活用という観点からご紹介したいと思います。

増加する電子的コミュニケーションの利用と潜在的なリスクの高まり

近年の情報通信技術の革新によって、金融機関は顧客との間のみならず、提携先や取引先などとのコミュニケーションにおいて電子的な手段を活用する傾向が次第に顕著になっています。いわゆる電子メールはもとより、Instant Message（IM）、チャット、電子掲示板そして最近、関心を読んでいる Web-Site を応用したブログなど電子的なコミュニケーション手段は多岐にわたっています。ある調査によれば、2006 年までに米国の金融機関に送られてきた電子メールはおおよそ 10 億件に上るとも言われ、電子メールの潜在的な利用者は 500 百万人とも見込まれています。こうしたコミュニケーションの利便性が高まる一方で、そこで取り扱われている個人情報を始めとした機密情報の漏洩などのリスクの高まりに対してどのように対応すればよいかという困難な課題に直面しています。

当局から要請される新たな規制への対応

このような状況を踏まえて、金融機関を監督する当局もこれら電子的なコミュニケーションの情報に関する保存期間をきめ細かく規定するようになっており、金融機関としてもコンプライアンス対応の上からも重要な課題となっています。

BASELⅡに代表される金融業界に対する国際的なガイドラインとしてもオペレーショナル・リスク管理などの観点から然るべき規制を要請しています。

また、米国において 1990 年代以降、制定ないし改定された様々な法制度もそれぞれの立場や目的から電子的コミュニケーションに対する規制を定めています。米国の証券取引委員会(SEC)や全米証券業協会(NASD)などが定める施行規則においてもそれぞれのカテゴリーごとに保存期間を規定しています。また、現在わが国でも関心が高まっている財務情報に関する内部統制を強化することを目的として制定された「米国企業改革法(Sarbanes-Oxley Act：通称 SOX 法)」においても関連するルールを定めています。

包括的なセキュリティ対策の構築に向けて

以上のような状況を踏まえて、欧米の金融機関では規制・監督の当局から求められている様々なコンプライアンスに対して包括的な対応を行うために以下のようなアクションでこうした問題に取り組んでいます。

まず、第一に、当然のことですが、規制・監督の当局が求めているルールを理解する必要があります。金融機関として合理的な監視の仕組みを運用するために、その手続きを文書として記述、表現され、適切な方法で管理されていることを表明しなければなりません。

次に、第二には、それらの業務ルールに照らして電子的なコミュニケーションを監視ないし管理するシステムがどのような考え方で構築、運営されているのか、その的確性や妥当性について指針を策定する必要があります。

そして、第三にはコミュニケーション内容の電子的な記録がますます増加していくことを勘案して、保管コストと可用性とのバランスをとりながらストレージ技術を活用していくことが求められます。

最後に、第四として、こうした電子的コミュニケーションの記録も正式な法律文書として見なされるという観点から、いわゆるWORM（Write Only Read Many）標準の技術を前提にして、一旦書き込まれたら、消されたり、二度と書き換えられたり、修正されないように元の情報が保持されるような情報管理が必須となります。

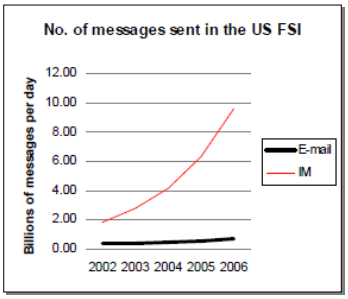
求められるわが国金融機関の対応

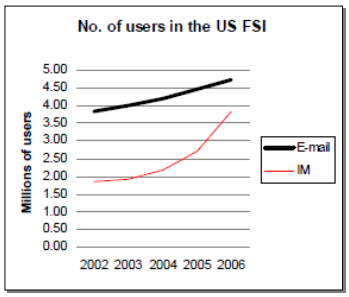
わが国でも、携帯メールのような電子的なコミュニケーション手段が確実にビジネス環境に浸透してきました。このようなコミュニケーション環境を前提にして、金融機関としてどのような情報セキュリティ対策をとるか、まさに現実的な課題となってきました。

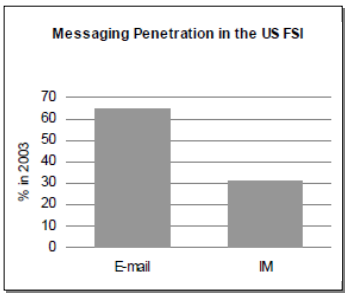
取り組むべき重要な課題について列挙すると、①BASELⅡで求められているオペレーショナル・リスク管理の観点から、個人情報を始めとする機密情報が電子的データとしてどのように伝達され、保管され、参照されているのか、一連の情報ライフサイクル・マネジメントとして把握できていること、②そうした情報のライフサイクルの中で、どのような業務プロセスが個々の情報に関連しているか、それぞれの組織、業務およびIT統制全般の観点から統制状況を可視化できていること、③そうした分析で浮き彫りにされたリスクがその発生頻度や影響度合いに応じて的確に把握され、然るべき対処が明確に定義されていること、などになろうかと思います。

わが国の金融機関においても近年、セールス・プロモーションやマーケティングなどの活動の一環として電子メールの活用が始まっています。それ以前からインターネット・バンキングなどによる残高照会や資金移動などの利用も進んでいます。そうした電子的なコミュニケーションにおいて重要な役割を果たしているメール・アドレスなどの個人情報について、より一層万全な備えが求められる時代になっています。

米国金融機関における電子メール取り扱い件数の伸び







Source: Celent Communications

求められる電子メールに対する包括的な管理システム

Legislative Acts
- Financial Modernization Act
- Sarbanes-Oxley Act
- Patriot Act

International Guidelines
- Basel II
- IAS
- IFRS

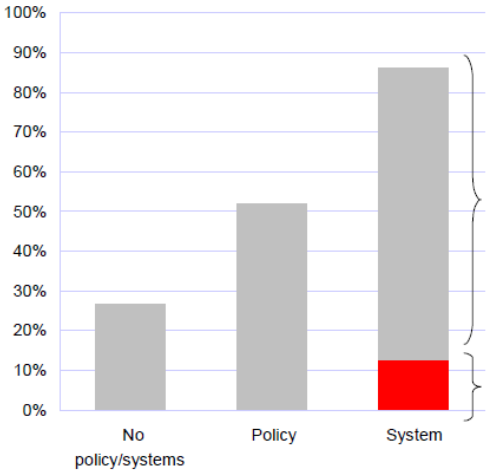
Supervisory Rules
- SEC Rules 10b, 17a-3, & 17a-4, S-P, S-K
- NASD Conduct Rules 2110, 2120, 2210, 2310, 3010, 3110
- NYSE Rules 342, 440, 472
- FRB P12-CFR-216
- OCC 2000-25
- FDIC 2000-332

Rules governing:
- Fraud, manipulation, deceit
- Record creation & preservation
- Consumer privacy
- Public communications
- Market disclosures
- Company supervision
- Internal control
- Operational risk mgmt

SEC 17a-4	SEC 17ad-7	SEC 204-2	SEC 31a-2	SOX	Patriot Act
3 Years	2 Years	5 Years	6 Years-Per-manently	7 Years	5 Years

Source: Celent Communications

電子メールに対するセキュリティ対策の未整備



Non-comprehensive System:
Fails to meet all business and compliance requirements

Comprehensive System:
Meets all business and compliance requirements

Source: Celent Communications

ストレージ技術の比較

Attribute	WORM Magnetic Disk	WORM Magnetic Tape	Optical	Magnetic Disk	Magnetic Tape	Film / Microfiche	Paper
Perfor-mance	High	Medium	Medium	High	Medium	Low	Low
Cost-effective-ness	High	High	Medium	High	High	Low	Low
Scalability	High	Medium	Low	High	Medium	Low	Low
WORM Compliance	Yes	Yes	Yes	No	No	Yes	Yes
Reusability	High	Medium	Low	High	Medium	Low	Low
Support of Full Docu-ment Life Cycle	High	Medium	Low	High	Medium	Low	Low

Source: Celent Communications