

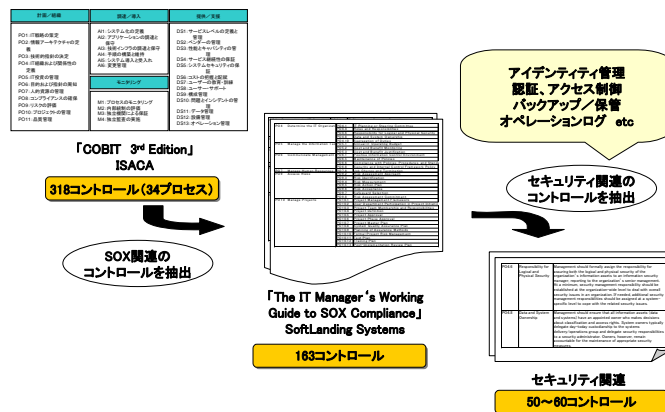
## “暗号化技術による情報セキュリティの確保”

近年、金融取引におけるさまざまな情報通信技術の活用が広がってきたことから、金融機関が保有する「顧客情報」や「取引情報」などは多様なリスクに晒されていると言えるでしょう。インターネットや携帯電話などによる金融取引が一般化するという経済社会の環境変化を受けて、金融機関を監督する当局もオペレーショナル・リスクを管理するための新たな制度を導入しつつあります。こうした新たな規制の動きを背景として、金融取引に関する情報を堅確なセキュリティ対策のもとで厳格に管理するために、後ほど紹介するさまざまな情報技術が適用されていますが、なかでも暗号化技術は非常に有効なものとして期待されています。そこで、欧米の金融機関における情報セキュリティへの取り組みについて、暗号化技術に関わる動向をご紹介します。

### 情報セキュリティに対する問題認識の高まり

わが国でも内部統制の強化に向けて多くの企業で組織的な取り組みが始まっていますが、こうした取り組みが先行した米国ではいわゆる SOX 法 (Sarbanes Oxley Act) 施行にあわせて情報セキュリティに対するコントロールがいかに行われているか、その実情を調査、評価されました。具体的には、情報セキュリティの確保に関する計画や組織的な導入状況、モニタリングおよびそれらの支援プロセスなどが対象となりました。

### SOX法のセキュリティ要件とは



その結果、IT 統制状況の評価として、アクセス制御やアイデンティティ管理などが不十分であるという指摘が数多く挙げられました。すなわち、本来の権限を有しない部外者が機密情報にアクセスすることが可能であったり、アイデンティティが厳格に管理されていないなどの不備が明らかにされました。

## SOX法に関わるITの欠陥 - TOP10 -

- IT対応が不十分な項目は、アクセス制御/アイデンティティ管理に集中(約7割)

1. 職務の分離(職務分掌)が認識、あるいは解決されていない
2. 財務アプリケーション(SAP、Oracleなど)やポータルを支えるOS(UNIXなど)が保護されていない
3. 財務アプリケーションを支えるDB(Oracleなど)が保護されていない
4. 実稼働後に、開発スタッフが業務処理を実行できるようになっている
5. 特権IDでアクセス可能なユーザーが多数いる
6. 離職者や職務を離れたコンサルタントのアクセス権が削除されていない
7. GL(総勘定元帳)アプリケーションへの記帳期間が厳しく管理されていない
8. カスタムのプログラム、テーブル、インタフェースのセキュリティが不十分である
9. マニュアルの手順書が存在しない、あるいは遂行されていない
10. システム関連のドキュメントが実際のプロセスに合致していない

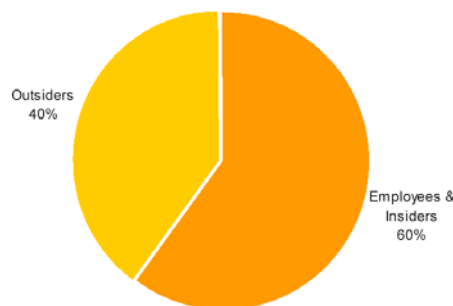
出典 Ernst&Young 404 Engagement Analysis

### 重要な役割を担うセキュリティ統括役員 (Chief Security Officer : CSO)

ある調査会社のリサーチ結果によれば、銀行における不正取引の半分以上は内部の行員や職員によるものであると言われています。そうした不正取引は上で述べたような情報セキュリティの「抜け穴」を利用して不正行為を行っていると思われます。従って、これらの情報セキュリティをいかに強化するか、金融機関のセキュリティ統括役員 (CSO) は待ったなしの対策を講じようとしています。

### 銀行における不正取引の過半は内部

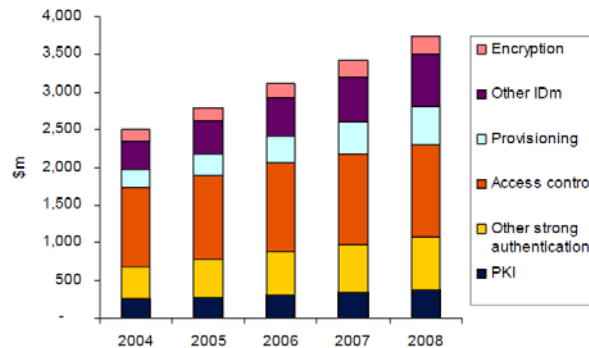
Sources Of Bank Fraud



Source: Celent Communications

2005年に行われたある調査によれば、北米の金融機関のIT費用の総額のうち約4%がこうした情報セキュリティ対策に充当されていると言われています。具体的には、いわゆるIDm (Identity and access management) やPKI (Public Key Infrastructure) などの認証基盤技術を始めとして、アクセス制御や暗号化などの技術がこれらの対策として活用されています。

## アクセス制御／アイデンティティ管理に係わる市場の伸長



Source: Datamonitor

### 統合情報セキュリティ基盤の構築アプローチ

金融機関を始めとして多くの組織や企業では、通常、統合的な情報セキュリティ基盤を次の6つのカテゴリーで構築しています。すなわち、「Firewall や VPN (Virtual Private Network) の構築」、「情報流出の検知と予防策」、「ウイルス対策やフィルタリングなどによるコンテンツ管理」、「アイデンティティやアクセス権の管理」、「セキュリティ・ポリシーの管理」および「その他セキュリティ・サービス」などです。

特に、暗号化技術は従来、特定のハードウェアの導入を必要とすることが一般的でしたが、近年ではソフトウェアに基づく暗号化が主流になっています。「コンテンツ管理」や「アイデンティティやアクセス権の管理」などの分野で共通して活用される中核的な技術となっています。機密情報に狙いを定めて攻撃してくる不正行為に対して、言わば「最後の砦」とも言える役割を担っています。

従って、暗号化技術のみならず、これらの多面的なセキュリティ対策を組み合わせるさまざまなリスクや脅威に対して予防や抑止などの対策を講じる訳ですが、最終的には「情報ライフ・サイクル・マネジメント」の仕組みの中でそれぞれの対策をポジショニングすることが肝要です。金融取引が始まる際の口座開設の際に入力される顧客情報から、その後の取引履歴や与信情報などを適格に管理することが必要です。

### わが国金融機関に対する示唆

わが国でも金融機関のみならずさまざまな企業において個人情報の漏洩や流出が相次ぎました。一旦、こうした不祥事が起こると、その影響は甚大なものがあり、金融機関の企業イメージやブランドなどを傷つけることとなります。従って、目下、鋭意、各金融機関で取り組まれている内部統制の強化に向けた取り組みの中で、まずは今日的なリスクや脅威に対してどの程度の対策が講じられているか、その実態をありのままに把握することが第一歩となるでしょう。その上で、金融機関として一定のセキュリティ強度を確保するた

めに補強すべき対策を優先順位付けすることになります。最終的には、上で述べたような「情報ライフ・サイクル・マネジメント」の構築に向けて統合的な情報セキュリティ基盤を構築すべきではないでしょうか。

今日では多くの取引情報がデジタル化されて生成、流通そして蓄積されています。従来であれば、これらの情報の流出や不正なコピーなどは必ずしも大規模に起こるとは限りませんが、今日的な金融取引の環境からすると、情報セキュリティの重要性ははるかに高まっていると言っても過言ではないでしょう。信頼性をモットーとする金融機関としては、情報セキュリティに対する備えを磐石に講じるべき時代と言えるでしょう。