金融分野における情報セキュリティ管理の国際標準化動向

日本銀行金融研究所 岩下 直行

（本稿は、2001年2月14日に金融情報システム情報センターが開催した平成12年度セキュリティセミナーにおいて、岩下直行が行った講演内容に加筆・修正したものである）

1.情報セキュリティと金融業務

これまで、わが国では、金融機関向けの講演会などで情報セキュリティ技術や暗号技術等に触れると、「金融とどんな関係があるのか」といぶかしく思われることが多かった。一方、欧米諸国においては、従来から、金融業界は情報セキュリティ技術の最大のユーザーと位置付けられており、この点で、金融機関のセキュリティ対策における日本と欧米とのアプローチは随分異なるものであった。

(1) わが国の金融ネットワークを取り巻く環境の変化

とはいえ、わが国の金融機関がセキュリティ対策に不熱心であったという訳ではない。金融業はセキュリティに対する要請の強い産業であり、また、他の産業に先駆けてネットワーク・システムを構築してきた経緯もあるため、わが国においても、金融ネットワークの安全性を守りたいというニーズは非常に強かったと言える。わが国の金融機関がこれまで選択してきた戦略は、企業内、業界内に閉じた「クローズド・システム」を採用するというものであった。わが国の金融機関は、巨大なコンピュータ・センターにメインフレームを並べ、支店との間を専用回線でつなぐことにより、システムを外部から物理的に隔離することでセキュリティを確保しようとしてきた。ネットワーク提供者が利用者のアクセスを厳格に管理して外部からの侵入を排除し、システム全体のセキュリティを高めるという発想である。このため、「情報セキュリティ技術などという面倒臭い技術を使ってシステムを守る必要がない」と考えられていた面もあった。しかし、最近そうした環境が変わりつつある。
従来、金融ネットワークを外部からの隔離によって守ることができていたのは、金融業界が他の業界に先駆けて独自のネットワークを構築していたからに他ならない。しかし、インターネットの拡大は、そうした前提を崩しつつある。最近では、顧客がインターネット上から金融機関等のシステムに接続して金融取引を行うインターネット・バンキング、インターネット・トレーディングが急速に普及しており、ネットワークのオープン化が進んでいる。金融機関にとっても、インターネット技術を利用することにより、通信コストやシステム管理のコストを劇的に安くすることが可能なので、もし専用回線を利用せずにセキュリティが確保できるなら、より値段の安いオープンなネットワークを使用した方が効率的と考えられるようになった。こうした環境変化の結果、情報セキュリティ技術の重要性が強く認識されるようになってきたのである。

(2) 金融分野における情報セキュリティ対策

金融業務のセキュリティ対策を議論する国際会議などで、「日本ではクローズド・システムであれば暗号や認証を使わなくても良いと考えられている」とか「専用線であれば信頼できると考えられている」などと説明したところ、欧米の金融関係者から「そんな理屈はおかしい」と反論されてしまった経験がある。特に米国は、わが国とは通信産業を巡る事情が異なることもあり、「専用線といっても電話会社を通るのだから、セキュリティをよその会社に頼り切ってしまうことはできない」という考え方が根強いようである。米国の大手金融機関では、「自分の安全は自分で守ろう」という発想から、自ら暗号や認証といった技術を利用して主体的にセキュリティ対策を講じることが多いようである。どちらの考え方が正しいかは一概には言えないが、このような違いがあることはきちんと意識しておくべきだろう。
一方、日本においても、従来のクローズド・ネットワークからオープンなネットワークに移行してくると、従来のセキュリティ対策では十分でなく、ネットワーク上でデータを守り、顧客の情報を秘密にしたり、正規の顧客であるのかということを確認したりするために、暗号化、電子認証、ICカードといった技術を利用しようとする動きが出始めている。このようにパラダイムが変ってくると、わが国でも、それに合わせて、国際的な情報セキュリティ対策に関する基準を意識した、新しいルールを整備していく必要が出てくる。こうした背景から、情報セキュリティ技術に関する国際標準が注目されるようになってきているのだと思う。

(3) 欧州における情報セキュリティ・リスク顕在化の事例

情報セキュリティ技術は、ただ使ってさえいれば効果があるというものではない。最近では、様々な情報セキュリティ技術が選択可能になり、それを利用する側の自由度が高まっている。このため、金融機関がどのような情報セキュリティ技術を採用するかによって業務の安全性が左右され、情報セキュリティ・リスクの多寡が規定されることになる。万一、金融機関が選択した情報セキュリティ技術によって業務の安全性を十分に確保できなかった場合、セキュリティ侵害による業務の停滞や金銭的被害のリスクに晒されるだけでなく、金融機関としての信認を損なうレピュテーション・リスクや、訴訟を提起されるリーガル・リスクをも招来し、経営的なダメージに繋がることも考えられる。身近な例としては、金融機関のホームページが改ざんされ、「あの金融機関はセキュリティが弱い」という評判を立てられるというリスクも存在する。このように、わが国でも、情報セキュリティの問題は、切実度が増してきているように思われる。
欧州では、金融機関が情報セキュリティ侵害による大きなトラブルに遭遇したいくつかの事例がある。例え

ば、フランスでは、1999年から2000年にかけて、フランス銀行カード協会（Cartes Bancaires）の仕様に準拠した銀行取引カードの偽造事件が発生した。フランス銀行カード協会は、1989年にフランス全土で使用される金融取引用ICカードを導入し、それまでの磁気ストライプカードに対して多発していた偽造犯罪を激減させることに成功した。しかし、導入時期が早かったために利用していた技術が古く、新技術への移行を図っていたものの完全には移行できていない状況で、今回の偽造事件が発生してしまった。
フランス銀行カード協会のICカードには、RSA署名を生成する仕組みが組み込まれていて、その署名により正規のカードであることを確認していたが、RSA署名の鍵長、すなわち計算するときのブロックの長さが短いという問題があった。現在では、RSA署名の鍵長としては1,024ビット程度が普通と考えられているが、このカードでは200数十ビット程度であった。このICカードが導入された1980年代であれば、200ビット程度でも解読は難しかったが、コンピュータの能力の向上によって、現在では200ビットであればパソコンでも解読できてしまうようになった。
今回の事件の報道によれば、ある技術者が、このICカードを解析して、「偽造カードが作れてしまったので買い取って欲しい」とフランス銀行カード協会に持ちかけたとされている。協会がこの申し出を断り、事件が露見した結果、カードの安全性が揺らいでいることがテレビのトップニュースで報道され、信用が大きく傷ついてしまった。このトラブルに対して、フランス中央銀行は、「確かに脆弱性はあるが、今すぐシステムが崩壊してしまうわけではなく、また近いうちにより安全性の高いシステムに移行するように指導したので、動揺しないように」とのプレス・ステートメントを公表し、事態の沈静化を図ったという。
ドイツの銀行協会が発行したICカードについても、利用している電子署名アルゴリズムの脆弱性が指摘されるといった事件が発生している。これらの事例から分かるとおり、金融機関がセキュリティを守るためには、単にICカードや電子署名といった技術を使っているというだけでは十分ではなく、最新の基準によって評価された、信頼できる技術を使っているということが大事なのである。このために、信頼できる情報セキュリティ技術かどうかを見分ける方法が非常に重要になってきている。そのための手段としても、情報セキュリティ技術に関する国際標準が重要な意味を持つようになってきている。そこで、以下では、金融業務に適用される情報セキュリティ技術に関する国際標準の動向について、説明することとしたい。

2. 金融業務における国際標準化

標準化というと、主として工業分野で利用されるISOやJISといった公的な標準が連想され、「金融とはあまり関係のない分野」という印象を持つ方が多いと思う。しかし、わが国の金融業務の分野でも、ISOやJISといった形態こそとらないものの、様々な意味での「標準化」が行われてきた。例えば、伝統的な紙ベースの金融業務では、業界内の申し合わせという形で、手形、小切手や各種帳票類の様式の統一という標準化が行われていた。その後、金融業務がコンピューター・ネットワークを通じて行われるようになってからは、金融機関間のデータ通信フォーマット（全銀プロトコル）、金融機関コード、銀行取引カードのフォーマット等が標準化されている。こうした標準化は、金融取引における不要な多様性を排除し、業界全体における事務の合理化、顧客サービスの向上に貢献するものであった。

(1) 強制規格と任意規格

標準には様々な分類方法があるが、その1つは強制規格と任意規格という分類である。法令等により遵守することが求められ強制されているのが強制規格であり、特に求められていないものが任意規格である。ISOやJISは任意規格であるから、例えばISO9000を採用するかしないかは、各企業が判断することである。つまり、ISOというものは、守りたくなければ守らなくてよいものなのである。
しかし、こうした任意規格であっても、「それを守ることが世の中でどれくらい一般的か」によっては、事実上採用しなければならないというケースもあり得ることには注意が必要である。もしも、「英国ではすべての金融機関がISO17799を採用している」という状況になれば、日本から英国に進出したいと思う銀行にとっては、ISO17799を採用することが事実上必要とされるという状況も考えられるということだ。

(2) デジュール標準とデファクト標準

ISOやJISなど、公的な標準化機関により、透明性の高いプロセスで、関係国／関係企業のコンセンサスにより制定された標準を「デジュール標準（de jure standard、公的な標準）」という。一方、標準を巡る競争が市場で行われ、その結果、標準が事実上決定されたものを「デファクト標準（de facto standard、事実上の標準）」という【図１】。

【図１】デジュール標準とデファクト標準

	デジュール標準（公的な標準） de jure standard	デファクト標準（事実上の標準） de facto standard
定義	標準化機関により制定された標準	標準を巡る競争の結果，事実上決定された標準
特徴	（1）策定プロセスの透明性 （2）単一標準の提供 （3）オープンなメンバーシップ	（1）策定プロセスの速度が迅速 （2）標準普及と製品普及が同時 （3）市場競争で標準が一本化 （4）自規格を標準化できた者が市場を独占できる
欠点	（1）標準開発の速度が遅い （2）製品普及と標準普及のラグ （3）技術のフリーライド	（1）情報公開が不完全。開発企業による競争限定的行為の懸念 （2）閉鎖的なメンバーシップ （3）改正手続が不透明

従来、日本の銀行業界にとっては、このような標準化を巡る議論はあまり関係ない問題と思われてきた感があるが、これから日本の金融機関にも深く影響してくる話ではないかと考えている。

3. 情報セキュリティ技術の国際標準化

情報セキュリティ技術、暗号技術や認証技術においては、標準化されていることが大きな意味を持つ。金融業界で広く利用されてきたDESはData Encryption Standardの略称であり、現在米国で標準化が進められている次世代の米国連邦政府標準暗号AESはAdvanced Encryption Standardの略称であるが、いずれもStandard――「標準」という単語を含んでいることが象徴的である。

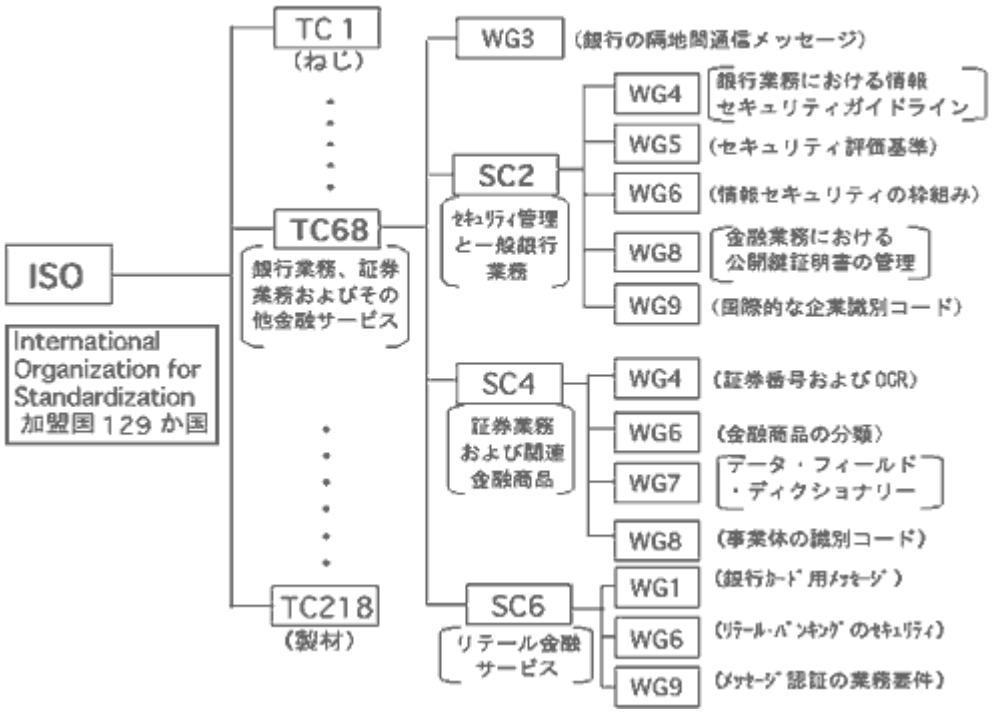
(1) 情報セキュリティ技術における標準化の重要性

なぜ情報セキュリティ技術では標準化が重要なのだろうか。ひとつには、情報セキュリティ技術は通信ネットワーク環境で利用されることが多く、互換性が大切であるため、標準化されていると便利であるということがあげられる。しかし、それだけではない。最大の理由は、標準化によって、安全性が評価されるということである。
セキュリティ技術、暗号技術や認証技術は、高度な数学を駆使し、難解な理論に基づいて設計されたものであることが多く、一人ひとりのユーザーが、良い技術か悪い技術かということを見極めていくのはたいへん難しい。このため、標準化を行い専門家が技術内容を吟味することによって、安全性に対するお墨付きが付与されることが期待されている。つまり、「この技術は非常に安全なものです」というお墨付きを得られることが、情報セキュリティ技術を標準化するインセンティブになっているのである。
現在、情報セキュリティ技術の学者、研究者が中心となって、新しい技術の安全性を評価し、最もすぐれているものを標準にしてみんなで使用するために、様々な安全性評価、標準化の活動が行われている。金融機関など、情報セキュリティ技術の利用者は、このような動きをウォッチし、その評価結果を採り入れていくことが、信頼できる情報セキュリティ技術を選択していくために非常に有効なことであると思う。
暗号アルゴリズムや電子署名といった比較的基礎的な技術については、公的な標準化機関が採択したデジュール標準が信頼できるものとして利用されている。例えば、金融業界では、従来はDESが広くに使われてきたが、近年、その強度が低下したため、それに代わるものとしてトリプルDESが使われるようになり、さらにアメリカの商務省がそのトリプルDESの次の暗号アルゴリズムとしてAdvanced Encryption Standard(AES)を選考するプロジェクトを立ち上げ、去年の10月にRijndaelという暗号アルゴリズムが選定された。これはベルギーの銀行間決済システムを維持管理する企業が開発した暗号アルゴリズムである。ここでもやはり、暗号の技術と金融業務というのが非常に密接に関連しているということがわかる。こうした新しい技術を、上手に自分たちのシステムの中に採り入れていくということが重要である。

(2) ISO／TC68

日本銀行は、ISOの中のTC68という委員会において、国内の事務局を務めている。この中でも、国際標準として様々な技術を比較検討し最も使えるものは何なのかと選定する作業を行っている。ここでは、国際的な銀行の情報セキュリティ技術のエキスパート等が集まり、様々な技術の評価を行っている。例えばICカードを使う際、「ある形で暗証番号の管理を行いたいが、これはどうだろうか」といったときに、「それだとこのようなリスクがあるからこうしよう」といった様々な議論を行っている。そのような議論を国内の金融業界に還元することにより、日本でこれまではあまり利用の経験が多くなかった情報セキュリティ技術に関して裾野のようなものを広げていくための活動を行っている【図2】【図3】【図4】。

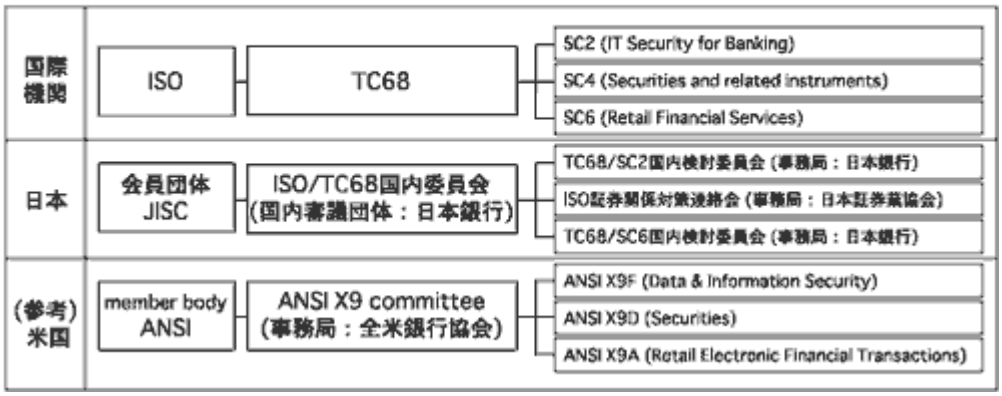
【図２】 ISO/TC68の組織



【図3】TC68の情報セキュリティ関連国際標準

ISO番号	国際標準の名称	概要説明
ISO 8730	メッセージ認証のための必要案件	大口金融取引用のMAC
ISO 8731	メッセージ認証用暗号アルゴリズム	DES暗号方式の仕様
ISO 8732	暗号鍵の管理	大口金融取引用の暗号鍵の管理方式
ISO 9564-1	暗証番号(PIN)管理とセキュリティ	暗証番号(PIN)の管理方式
ISO 9564-2	暗証番号管理用暗号アルゴリズム	DES暗号方式の仕様
ISO 9992	ICカードと端末間のメッセージ	リテール金融取引のICカードの処理手順
ISO 10126-1	メッセージ暗号化手順	大口金融取引の守秘目的の暗号化手法
ISO 10126-2	メッセージ暗号化用暗号アルゴリズム	DES暗号方式の仕様
ISO 10202	ICカードのセキュリティ対策	ICカードのコピー，改ざん，偽造等の防止
ISO 11131	サイン・オン認証	金融機関システム・アクセス時の相手認証手法
ISO 11166-1	公開鍵アルゴリズムを利用した鍵管理	SWIFT・USEのセキュリティ機構を標準化
ISO 11166-2	鍵管理用暗号アルゴリズム	RSA暗号方式の仕様
ISO 13491	安全な暗号装置	リテール金融取引用の暗号装置の要求機能

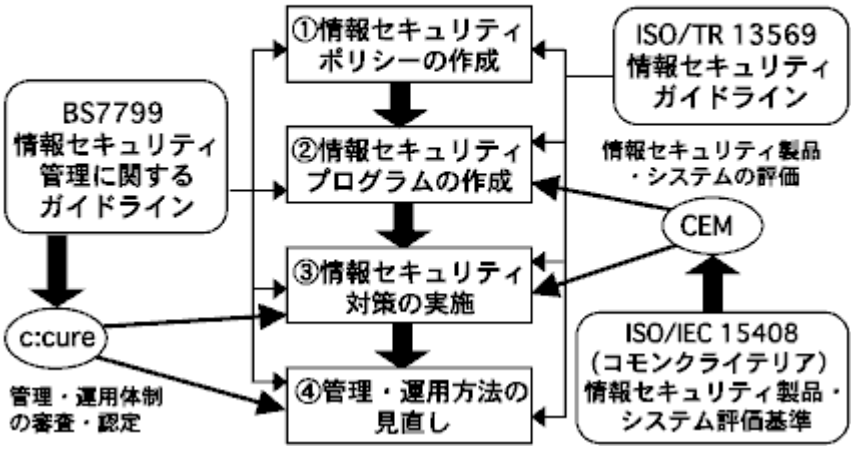
【図4】ISO／TC68に対応するわが国の国際標準化活動



(3) 情報セキュリティに関する評価・認証のための国際標準

情報セキュリティの評価・認証を行う国際標準としては、ISO15408とBS7799があげられる。ISO15408は、情報セキュリティ機器のための標準であり、ISO15408の適用対象として最も活発に検討されているのがICカードである。
先ほどご説明した事例のとおり、ICカードを使えば無条件で安全になるとは限らない。ICカードが本当に安全なのかを確認するためには、ICカードの分野のエキスパートが正確に評価する必要があるが、各金融機関がこれをチェックすることはかなり難しいのが実情であろう。そこで、セキュリティ評価の専門家が、ISO15408によって一定のルールに基づいた評価を行い、そのお墨付きを得ることができたものが安全であると信頼し使用するということが考えられているのである。
これに対してBS7799は、ユーザー自身のセキュリティの運用管理に対する安全性のお墨付きをつけてくれるための仕組みである。この2つの関係を図式的に示したものが【図5】である。

【図５】情報セキュリティ管理の国際標準の相関関係



いわゆる情報セキュリティを、ひとつの組織の中で守ろうとした場合には、まず、セキュリティポリシーを策定しなければならない。そして、それを用いて今度は実際に情報セキュリティを実施するための実施指針であるセキュリティプログラムをつくり、セキュリティ対策を実際に実施する。そのうえで、管理・運用体制を見直し、いわゆるプラン・ドゥー・シーでまた最初に戻るということを行う。このときに、どのようなセキュリティ対策を各ユーザーがとるかということをチェックしてくれるのがBS7799である。一方、各プロセスで具体的にセキュリティ対策を実施するためのセキュリティ機器やシステム等を評価してくれるのがISO15408である。

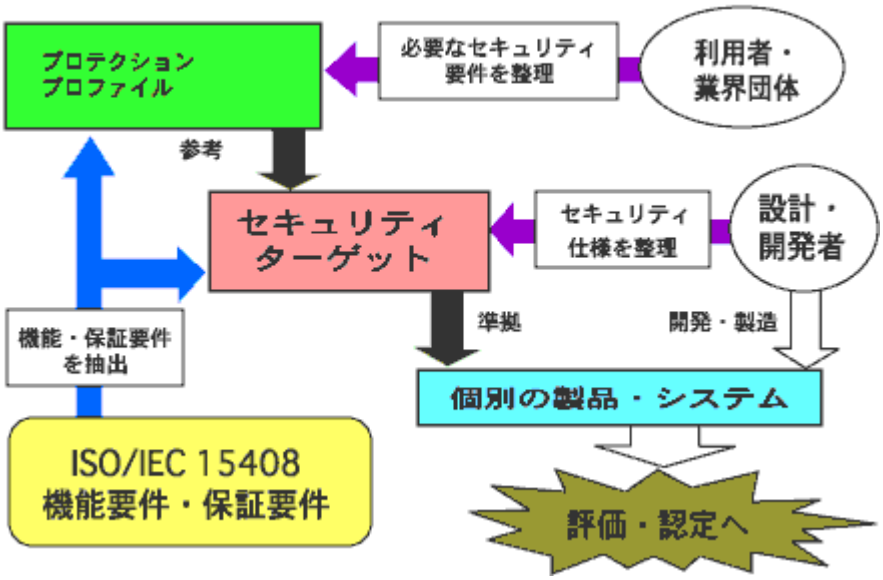
(4) ISO15408

ISO15408は個々の情報セキュリティ関連製品・システムが備えるセキュリティ機能および品質を、統一化された評価尺度に基いて第三者機関が客観的に評価・認定する際に用いられるセキュリティ評価基準の国際標準である。欧米の統一的なセキュリティ評価基準「コモンクライテリア」をベースに、1999年に策定された。2000年には、わが国でも、日本工業標準JIS X 5070として国内標準化されている。

i. ISO15408の構成
情報セキュリティの製品やシステムの評価を行うとき、セキュリティの要件をどのように決め、それをどのように評価するかといった際の枠組みを定義したものである。ISO15408には具体的なセキュリティ対策そのものについて記述されているのではなく、喩えて言えば、「テストの仕方」を書いてあるようなものである。

ii. ISO15408による評価・認証の手順
ISO15408を用いて評価・認証を行う場合の一般的な手順は、次のとおりである【図６】。

【図６】プロテクションプロファイルとセキュリティターゲットの利用方法



a) 利用者（または業界団体）は、ICカード等、評価対象のカテゴリーごとに必要とされるセキュリティ機能要件と保証要件をISO15408の評価モデルを参考にして選択し、プロテクションプロファイル（PP）を作成する。
b) 設計・開発者は、適用分野のPPを参考にして、個々の製品のセキュリティターゲット（ST）を作成し、そのSTに基づいて製品を製造する。
c) 評価機関は、STに基づいて開発・製造された製品のセキュリティ水準を、基となったPPおよびSTとともに、予め規定された手続きに沿って評価する。

d) 認証機関は、評価機関による評価が正当に行われたか否かを検証し、評価が正当なものであると判断した場合には認証書を発行する。評価結果と認証書は、認証機関が管理するカタログに登録される。
e) 個々の情報セキュリティ製品・システムの利用者は、適宜認証機関のカタログを参照することができる。
ここで重要な役割を果たすISO15408の評価・認証機関は、現時点ではまだ日本にはなく、このISO15408を日本国内で利用することはできない状態にある。現在、この評価・認証機関を立ち上げようという試みが進められており、つい最近、経済産業省が、評価・認証機関になることを希望する団体・企業に対して、マニュアルを示すといった説明会を行った。これから幾つかの評価・認証機関が立ち上がってくることが予想されている。とはいえ、ISO15408の評価・認証機関が設立され、各ベンダーが、「わが社のこの製品はISO15408の認証済みです」と宣言するようになり、認証済みの製品を購入するユーザーが出てくるまでには、なお時間が必要である。そもそも、ユーザーや業界団体がPPを策定している例がほとんどないため、制度的な枠組みがつくられても、実質的にはすぐに機能することは難しいであろう。
欧米の金融機関においては、自分たちがどのような要望を持っているのかということを整理してPPを策定ようという動きが出始めている。しかし、そうして策定されたPPが良いものなのか、現時点ではよくわからないという問題がある。この問題に答えるためには、そのPPに対応したSTに基づく製品が開発され、それを評価・認証して、金融機関が実際に使用してみて結果が良かったのかどうかを判断することが必要である。そうした経験を繰り返すことによって初めて議論が可能となり、「元のPPが悪かったので、もっといいものをつくらなくてはいけない」といった試行錯誤が何度か行われて、ISO15408によるセキュリティの評価・認証というものが機能するようになるのである。現時点では、それが今まさに走りはじめたばかりであり、今後どのように展開されるのかわからない状態である。
セキュリティの問題には、エンドユーザーがどのように関与するかということが重要である。ベンダーが何かシステムを提案し、「これだったら完璧です」と言い、「そうですか」とそれを使って本当に完璧だったらこれがいちばん楽である。しかしながら、セキュリティというのはそういうものではない。各金融機関の事情によりどのような部分に重点を置いたセキュリティ対策を採りたいか、例えば顧客がどういうタイプの人で、どれぐらいの金額の取引を行うのか、自分たちのシステムはどのようなものか、これらがすべて異なっているわけである。したがって、同じ製品ですべてOKということはあり得ないのである。
ただ、幸運なことに、日本の銀行の業務は各銀行によって大きく異なっているわけではない。業界団体や業界団体を含むコンソーシアムのメンバー等がPPを検討すれば、ある程度合意可能な標準的なセキュリティ要件を選び出すことができると思われる。日本の場合は主としてベンダー側がPPを策定する動きがみられているが、ユーザー側においてもそれなりのコミットメントを行っていかなくてはならない状況にあると思われる。

iii. 金融業界としてのISO15408への対応
金融業界のISO15408への対応として特筆すべきこととして、ISO/TC68の国際会議において、どの国がどのようなPPをつくっているか、それが本当に使えるものなのか等の検討を行うプロジェクトを英国、米国、フランスが中心となって発足させたことがあげられる。今後、こうした動きに日本も貢献していく必要がある。
これまでのところ、PPが策定されている金融関連機器としては、ICカード、CD/ATM、ファイア・ウォール等があげられる。PPに記載するセキュリティ要件は、単に厳格なものにすればよいということではない。コストとの対比で、本当にどのようなものが必要なのかということの見極めが必要である。例えばコンビニに置くようなCD/ATMはこのくらいでよいのではないか、などといった要件を議論することも可能と思われる。このような要件を適切に設定していくツールとして、今後、ISO15408が利用可能ではないかと考えられる。
先ほどご説明したISO15408の実施手順を聞かれた方は、「なんて面倒臭いことをするのだろう」と驚かれたかもしれない。最初にこの手の枠組みを整備していくのは大変な作業で、多くの英語の標準や論文を読まないといけないし、関係者と調整する手間も掛かる。しかし、この枠組みを整備していくプロセスで、ユーザーが何も言わずベンダー中心で進められてしまうと、後々ユーザーにとって不利になるかもしれない。ユーザーがどのように関与していくのか、これからが大事なところである。

(5) BS7799

BS7799は、各ユーザーサイドのセキュリティ管理を行うための英国の国内標準である。30ページぐらいのもので、BS7799-1とBS7799-2から構成されている。
このBS7799は、最初は英国国内で利用するために策定されたものであったため、英国の国内法等を意識した記述があったが、その後、これを国際標準化しようという動きがあり、英国にのみ適用される部分は削除され、国際的に利用可能なように書き直された。こうした経緯を経て、現在では、英国だけではなく、デンマークやオランダ等の国々において、特に金融機関がBS7799に準拠してセキュリティ対策を行っている。
日本では、去年の2月に各政府機関のホームページが次々に書き換えられるという事件が相次いで起きた。そこで、政府のセキュリティ対策として様々な取り組みが行われたが、政府機関のセキュリティポリシーを書く際、このBS7799に準拠した書き方をした。もちろんBS7799以外にも同じようなコンセプトのものがあるが、国際的に見て最も使用され、考え方自体も非常に説得的だということで使われたのだと思う。

i. BS7799-1の概要
1章から10章までの章があり、セキュリティポリシーの書き方等が出ている。ただ、書き方といっても、詳細なひな形があるわけではなく、どのようなことを盛り込んでいくかという項目が羅列してあるのみである。また、セキュリティ管理のための体制はどのようにしていかなくてはならないか、情報資産とはどういうもので、どのようにチェックしていかなくてはいけないか、人を雇うときにどのようなところに気をつけて雇わなくてはいけないか等をセキュリティの観点から記述している【図7】。

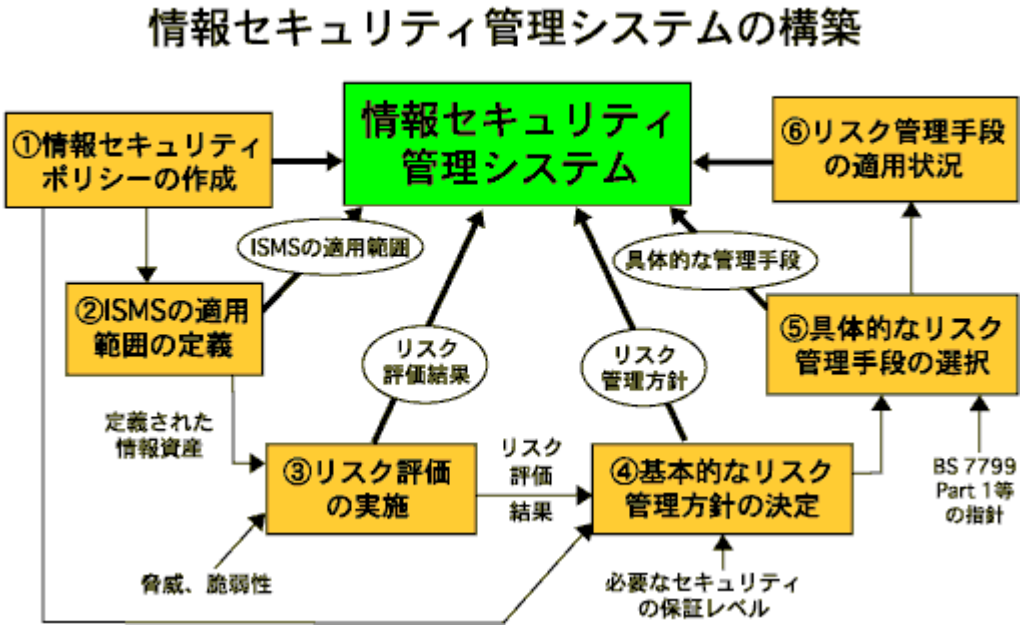
【図7】 BS 7799-1の概要

BS 7799：第1部の各章	主な章の概要

1. 情報セキュリティポリシー	情報セキュリティポリシーに盛り込むべき項目を説明。
2. セキュリテイ管理のための組織体制	情報セキュリティ管理を審議・承認する専門部署の役割等について説明。
3. 資産の分類と管理	セキュリティ対策の対象となる資産の分類方法等について説明。
4. ユーザー管理	役職員への研修プログラムや内部規則の策定等について説明。
5. 物理的なセキュリティ	安全領域の設置、入退室管理の実施、予備電源の確保等について説明。
6. コンピュータ・ネットワーク管理	ウイルス対策、ログ管理、ソフトウェアの更新管理等について説明。
7. システムへのアクセス管理	IDとパスワードによる管理、不正アクセスへの対策等について説明。
8. システム開発・維持管理	システム開発やメンテナンス時の留意点を説明。
9. 事業継続プラン	災害発生時への対応等について説明。
10.コンプライアンス	管理方法の関連法令等について説明 。

ii. BS7799-2の概要
BS7799-1はガイドラインであり、「～したほうが良い」と書いてあるに対して、BS7799-2は「～しなくてはいけない」と書いてある【図8】。BS7799-2の書き方は、標準に即した運用管理を行っているのであれば評価・認証制度に基づきお墨付きを付与する、というものであり、その制度をc:cureと呼ぶ。

【図８】 BS 7799-2の概要



このBS7799は、ISO9000という世界中で良く利用されている国際標準を、情報セキュリティ分野に拡張したものだ、と説明する人も多い。ISO9000は、英国流の品質管理システムに関する国際標準であり、まず欧州で広く利用されたが、世界に冠たるTQCの技術を持つ日本では、最初はあまり注目されていなかった。しかし、欧州や東南アジアの国々がISO9000の認証を取得することを、入札の条件等に利用する事例が増えたため、日本企業も慌ててISO9000の認証を取り始めたということがあった。BS7799による評価・認証制度は、ISO9000と同じような仕組みで、1998年４月に英国で導入された。この制度自体は現時点ではまだ走りはじめたばかりで、これがうまくいくかどうかはよくわからない。ただ、仮にISO9000のように急速に普及し、多くの会社がBS7799を取っているにもかかわらず取っていなかった時、欧州で取引をしようとする際にBS7799を取ることを要請され、これをやらなくてはならないという話になってしまったら、大変なことになる。今後、BS7799が、どのくらい国際的に普及し、マーケットで受け入れられるのかということを見極めていかなくてはいけないと思われる。
わが国でもかなり注目されたISO9000だが、その評価については色々な意見がある。品質管理の手法としては従来からのTQCを利用し、ヨーロッパをはじめ国際進出する際の方便として、ISO9000の認証を取得する、といった使い分けをしている企業もあると言われている。元々日本の製造業は、非常に優れた品質管理を実施してきたとされており、そのように割り切ることも可能であったということかもしれない。
しかし、BS7799が対象としている情報セキュリティ管理は、必ずしも日本の企業が得意とする分野ではない。最初に述べたように、日本企業の情報セキュリティ管理に対するカルチャーが海外とは相当異なり、クローズド・ネットワークを前提とした対策が中心であったためである。オープン・ネットワークの普及などを受けて、国内の状況も大きく変ってきており、セキュリティ対策について模索している企業も多いと思われるため、BS7799が示されると多くの企業が採用に傾く可能性がある。ただ、BS7799が本当に良いものか、役に立つかどうかは、まさに使い方次第で変ってくる。何もしないよりはBS7799に準拠した方が良いと思うが、まだ歴史の浅いものであるため、BS7799の認証が、優れたセキュリティ対策を実施し、被害を予防するために有効であったという実績が示されている訳ではない。果たして日本で適用するときに、この英国生まれの標準が

本当に役に立つのか、もっと日本流にモディファイした方がよいのか、評価・認証制度が本当に有効なのか、それともISO9000に関して一部で批判の声があるように、単なるペーパーワークを創り出すだけのものなのか、これらの疑問は現時点ではなかなかわからない。

iii. BS7799の国際標準化—ISO17799

BS7799-1は英国の国内標準であるが、2000年7月英国は、これを国際標準化することを提案した。ISO9000も英国の国内標準を国際標準化して普及させた経緯がある。英国による今回の国際標準化の提案を、2匹目のドジョウを狙ったものと警戒する声も強かった。BS7799-1が英国の標準である限りは、他の国はせいぜいそれを参照にする程度であるが、国際標準化され、国際的に普及してしまえば、日本としてもそれを意識せざるを得ないからである。

審議、投票の結果、2000年12月に、BS7799-1はISO17799として国際標準化された。ただし、国際標準となったのはパート1のいわゆるガイドライン部分のみで、認証制度に利用されるパート2は国際標準にはならなかった。この結果、国際標準としては、BS7799の認証制度を利用する枠組みは存在しないことになる。ただし、英国国内標準としてのBS7799-2は引き続き存在しているので、それに準拠して認証制度を利用することは可能であり、さらに、今後、ISO17799-2として認証制度が国際標準化される可能性も否定できない。

日本国内の対応としては、経済産業省が、ISO17799およびBS7799-2を参考にした国内での認証制度を立ち上げようとしている。現時点でこの制度の対象となるのは情報サービス事業者のみであるが、こうした国内の動きを含めて、BS7799／ISO17799を巡る動きには引き続き注目していく必要があろう。