トピックス

情報セキュリティ評価基準について

情報通信システム研究室主任研究官　　進藤　文夫

1　はじめに

最近、我が国の官公庁、関連団体のコンピュータシステムが不法侵入を受ける被害が多発している。ホームページが何者かの手で書き換えられたり、データを消去されたりと情報セキュリティ管理体制の甘さを露呈するものであった。

コンピュータやインターネットの急速な普及に伴い、金融機関におけるコンピュータの不正操作等のコンピュータ犯罪も近年では、外部からの不正侵入やメール爆弾、コンピュータウイルスなどネットワークを利用したものが目立つようになってきた。また、その犯行も多様化すると共に、被害額も年々増加する傾向にある。このため、政府や地方自治体、金融機関、電力・ガス・通信・交通といった公共機関はもとより、プラントなどの大規模な工業設備を有する企業や、一般企業もプライバシー保護をはじめ、情報セキュリティに対する関心が急速に高まっている。

そこで、本稿では、最近とみに関心が高まっている「ISO（International Organization for Standardization：国際標準化機構）15408　情報セキュリティ評価基準」（以下、「ISO15408」という）について、簡単に紹介してみたい。

2においては、この基準の制定の沿革について述べ、**3**においては、この基準による評価・認証、**4**においては、セキュリティポリシーの概要について述べることとする。

2　セキュリティ評価基準制定の沿革

ISO15408は、情報セキュリティの観点から、情報通信システム及び関連製品が適切に設計され、セキュリティ機能が確実に実現されているかどうかを評価するためのものである。1999年６月にISO規格として承認された。この規格により、情報通信に関連したシステムや製品のセキュリティの度合いを様々な観点から系統的に評価できるようになる。ユーザは、導入を検討している情報通信システム・製品を共通の基準で比較することが可能となり、やみくもにシステムを導入するのではなく、必要なセキュリティレベルに応じた適正でしかも最低限のコストで、運用や管理まで考慮されたセキュリティ効果のあるシステム・製品を導入することが可能になる。

米国では1985年に、国防総省が軍事システム向けに調達する情報通信製品に対する情報セキュリティ評価基準書TCSEC（Trusted Computer System　Evaluation　Criteria：通称「オレンジブック」）を作成した。同時にこの基準を基に情報通信製品等を評価、認証する制度も発足させた。この基準ではレベルの低いものから、D，C1，C２，Ｂ１，Ｂ２，Ｂ３，Ａ１の7つのセキュリティレベルに分離し、各レベル毎にセキュリティの機能と品質が満たすべき要件を規定した。情報通信システム・製品の評価と認証は、国防総省のNCSC（National Computer Security Center）が

行ってきた。これは軍事関連のセキュリティ機能を対象としていたため、1992年末にNIST（National Institute of Standards and Technology）とNSA（National Security Agency）が中心となり、幅広いユーザが使えるセキュリティ機能を目指した新連邦基準としてFC（Federal Criteria）を公開した。

EC加盟国では、政府（軍事）用システムに係る評価基準を、商用システムまで含め、ECの統一的な評価基準としてITSEC（Information Technology Security Evaluation Criteria）を1991年に発表している。また、カナダでは、TCSECとITSEC両者の考えを取り入れて、独自の評価基準としてCTCPEC（Canadian Trusted Computer Product Evaluation Criteria）を1991年に作成している。

この結果、評価基準の国際協調の必要性が認識され、米国、カナダ、英国、ドイツ、フランス、オランダによって共通の基準であるCommon Criteria（CC）を作成するための共同作業の場としてセキュリティ共同検討会議Common Criteria Editorial Board（CCEB）が作られ、作業を開始した。CCの第１版は1996年１月、第２版は1998年５月に発刊された。

また、同時に各国での動向を踏まえて、評価基準の国際標準化がISOにおいても取り上げられ検討された結果、1999年６月にISO15408として国際規格化されたのである。これは1998年５月に発刊されたCC第２版が基になっている。

３　セキュリティ評価基準による評価・認証

情報通信システム・製品がISO15408に準拠して作成されていることを第三者が検査し、確認が終わると「認証書」を発行して公表するという制度を運用することが重要である。既に欧米では、ISO15408の基になっている情報セキュリティ評価基準のもとで、このような評価・認証制度が運用されている。米国では1985年から、英国では1991年から運用が開始された。英国の場合、この「認証書」を取得した情報通信関連製品のリストは、政府の刊行物として公開されている。情報通信関連製品の利用者は、当該製品を選ぶ場合の判断材料として、このリストを参照する。この「認証書」の発行には、「セキュリティ評価」と「セキュリティ認証」の二つの作業が必要になる。

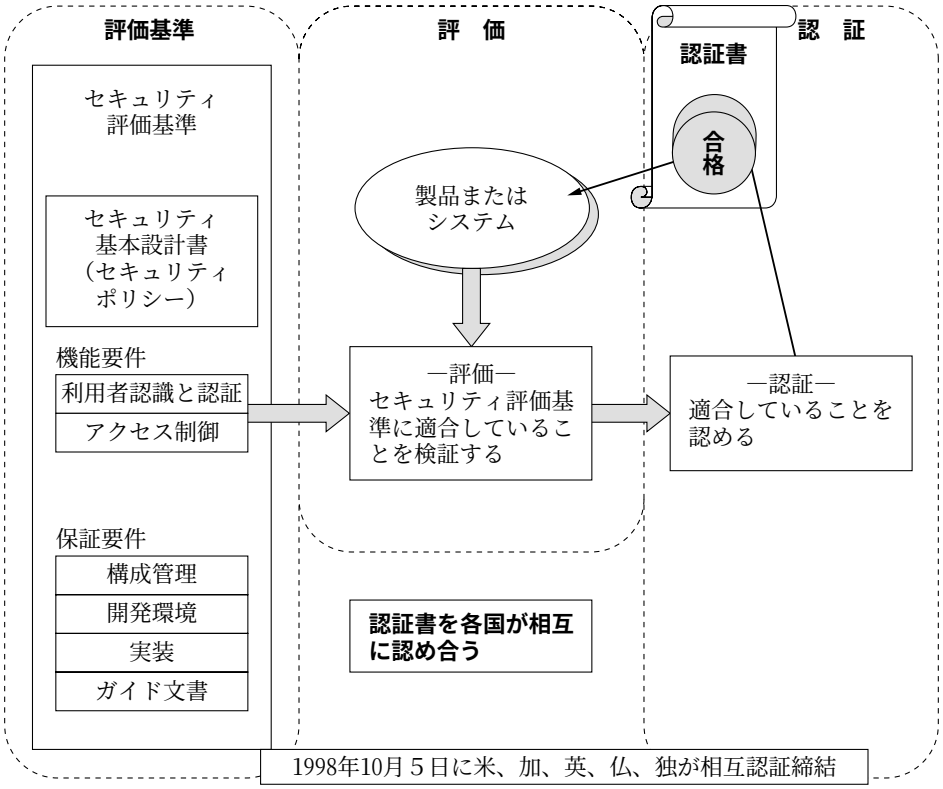
「セキュリティ評価」は、通常は民間の中立機関（評価機関）が情報通信関連製品の製造者や情報通信システムの管理者からの依頼を受け、ISO15408の要件に基づいて検査を行う。検査結果は、「評価報告書」に取りまとめられ認証機関に渡される。

「セキュリティ認証」は、欧米では政府関連の機関が実施している。評価作業が手続き的にも技術的にも問題なく実施されていることを確認後、「認証報告書」と「認証書」が認証機関によって作成され、「認証書」はセキュリティ評価の依頼者に渡される。依頼者は、この「認証書」の取得により、必要なセキュリティ対策が実施されていることを広く関係者に知ってもらうことができ、企業の信頼性の向上やイメージアップにつながる。

1998年10月、米国、カナダ、英国、フランス、ドイツの５か国は相互認証協定に合意した。これにより、それぞれの国内で認証を受けた情報通信システムや関連製品は、他の国でもその認証書が有効になる。情報セキュリティ評価・認証制度の概要を**図表１**に示す。我が国においても今後、情報セキュリティ評価・認証制度を早期に実施することが望まれる。

なお、ISO15408では、情報通信システム・関連製品がセキュリティ機能をどこまで保証しているかを表す尺度として、７段階の保証レベル（EAL：Evaluation Assurance Level）でレベル

図表１　情報セキュリティ評価・認証制度の概要



（出所）「国際セキュリティ標準ISO15408のすべて」田淵治樹、日経BP社、1999年

分けしている。上位（番号の大きい方）レベルは下位レベルの要件を含んでいる。対象とする情報通信システム・製品の性格、使用形態等によって、そのレベルを選択する。EAL１からEAL４までは商用システム・製品が備えるべきレベル、EAL５以上は現状では軍事用あるいはそれに準じる用途向きと言われているが、商用レベルでも金融など、高度なセキュリティを必要とする分野においてはEAL５あるいはそれ以上が適用される。情報セキュリティ保証レベルの概要は**図表２**のとおりである。

４　セキュリティポリシーの策定

インターネットとの接続等により、企業や組織の情報通信システムは高度にネットワーク化されてきた。これにより、ユーザも含めたセキュリティ対策とともに、セキュリティ対策に関して企業や組織全体としての意思統一を図るためのセキュリティポリシーの策定が必要となってきている。

セキュリティポリシーとは、このようなセキュリティ対策を進める上で、「企業や組織の情報セキュリティに対するルール・要件を文章化した規則集」であり、企業の就業規則等と同様、職員に対し強制力を持つとともに、具体的に実施される情報セキュリティ対策とその理由付けを提供するものである。記載項目例としては**図表３**のとおりである。

このようなセキュリティポリシー策定の効果としては、「企業や組織の情報セキュリティ対策の方針と要件の明確化」による安全対策の徹底、「企業や組織の情報セキュリティ対策の過不足点抽出」によるバランスのとれた安全対策の実施等が挙げられる。

図表２　情報セキュリティ保証レベルの概要

保証レベル	特　　徴	適　用　環　境　条　件
EAL１	一般向け機能のテスト	閉じられた環境での運用であり、安全な利用や運用が保証されている。
EAL２	プログラム構造の検証	利用者や開発者が限定されており、安全な運用を脅かす重大な脅威は存在しない。
EAL３	開発者実施テストの検証	不特定な利用者が利用できる環境であるため、不正対策が要求される。
EAL４	プログラムの処理内容の検証	コマーシャル向けの一般的なシステム・製品として、必要なセキュリティ確保が要求される。
EAL５	ソースコードの検証	コマーシャル向けのシステム・製品として、最大限のセキュリティ確保が要求される。
EAL６	ソフトウェアエンジニアリング工学による検証	多大なコストを負担しても保護しなければならない情報を処理するため、高いレベルのセキュリティを必要とする。
EAL７	公式言語使用による作成	最高レベルのセキュリティ確保を必要とする。

（出所）「国際セキュリティ標準ISO15408のすべて」田淵治樹、日経BP社、1999年

図表３　セキュリティポリシーの記載項目例

- **目的**
  セキュリティポリシーの必要性と役割について記載する。
- **適用範囲**
  セキュリティポリシーの適用対象となる人やシステムについて記載する。
- **保護対象資産**
  企業・組織にとって重要と判断される情報資産を明らかにする。情報資源には、情報と情報通信システム並びに、それらが正当に保護され機能するために必要な要件を含む。
- **資産の価値と機密レベル定義**
  資産の重要性基準を明記する。
- **準拠すべき法律、規則、標準**
  考慮すべき法律、規則、標準を明記する。
- **組織**
  組織全体、部門単位ごとのセキュリティ管理について、組織や人、それぞれの責任や規則を明記する。
- **脅威への対策**
  脅威への対策として、情報管理、物理管理、運用管理、開発管理、監査管理、人員管理等について定める。
- **処罰規定**
  セキュリティポリシーに違反した場合の罰則等を記載する。

（出所）「情報セキュリティ」山口英・鈴木裕信編、共立出版、2000年

情報セキュリティ対策の基本方針であるセキュリティポリシーの策定に当たっては、情報セキュリティの国際評価基準である「ISO15408」、FISC（金融情報システムセンター）が定めた「金融機関等コンピュータシステムの安全対策基準」、OECD（経済協力開発機構）が定めた「情報システムセキュリティガイドライン」等が参考になる。

５　おわりに

国民にあまねく公平なサービスを提供している郵政事業に不可欠な情報通信システムについても、そのシステムに障害等が発生した場合には、郵便

局の事務のみならず、国民生活等に多大な影響を与える恐れがある。そこで、郵便小包追跡システム、為替貯金・簡易保険の総合機械化システム等の郵政事業における情報通信システムについて適切な情報セキュリティ対策を実施することにより、その安全性・信頼性を確保することは重要な課題となっている。1999年７月には、行政情報システムの安全対策の充実・強化を図るため、行政情報システム各省庁連絡会議幹事会により「行政情報システムの安全対策指針」が策定されている。

2000年１月21日、情報セキュリティ関係省庁局長等会議が「ハッカー対策等の基盤整備に係る行動計画」を策定した。その具体的措置の中で情報通信システム・機器等の政府調達において、ISO15408を活用しつつセキュリティ水準の高い製品等を利用することとしている。

「Ⅳ取組強化のための具体的措置

１．政府部内における取組の強化

⑴　セキュリティに関する信頼性の高い政府システムの構築

【概要】略

【具体的措置】

①　セキュリティ水準の高い製品や技術等の利用

・各省庁は、新たなコンピュータシステムを構築する際、それぞれのシステムに応じた十分なセキュリティ水準の製品や技術等を利用するよう留意する。

・通商産業省は、情報機器等の政府調達におけるセキュリティ関連国際規格（ISO15408）の活用等の方針について、関係省庁と連携し、2001年５月までを目途に検討を行う。検討の結果については、行政情報システム各省庁連絡会議（総務庁を事務局とする各省庁会議）の場で提示し、同連絡会議において「各省庁の調達におけるセキュリティ水準の高い製品等の利用方針」の合意を目指す。

―略―

」

新聞報道によれば、通商産業省では2000年夏を目途にISO15408をJIS（Japanese Industrial Standards：日本工業規格）として採用するとしている。今後、郵政事業における情報通信システムにおいても、新しいシステム・製品を購入する場合は、ISO15408に規定された情報セキュリティ水準を満たすことを条件づけられるものと予想される。

また、上記行動計画においては、2000年12月までを目途に策定された各省庁向けの「情報セキュリティポリシーに関するガイドライン」を踏まえ、各省庁は2002年度中を目途に、情報セキュリティポリシーを策定し、これに基づく総合的・体系的な対策推進を図ることとされている。従って、郵政事業の情報通信システムにおける情報セキュリティポリシーを策定するに当たっても、上記ガイドラインのほかISO15408等の国際標準を参考にすることが求められるものと考える。

結局、今後は郵政事業の情報通信システムのセキュリティ対策を検討する場合には、ISO15408の概要を少しでも理解し活用することが必要になってくるものと思われる。

参考文献

・「国際セキュリティ標準ISO15408のすべて」 田淵治樹　日経BP社　1999年

・「情報セキュリティ」 山口英、鈴木裕信編　共立出版　2000年

・「情報システムの安全対策に関する中間報告書」 警察庁『情報システム安全対策研究会』 1996年

・「ISO/IEC15408『情報技術セキュリティ評価基準』のご紹介」 情報処理振興事業協会セキュリティセンター　1999年
・情報処理振興事業協会ホームページ　http：//www.ipa.go.jp/SECURITY