特集　情報セキュリティ政策

頻発するサイバーテロで急がれるITのセキュリティ品質向上

一般社団法人ITセキュリティセンター（ITSC）理事　宇賀村直紀

テロリストの攻撃対象となるITシステム

その昔、経理処理は全て人手に頼っていた。その後電卓というハードウェアで機械化が始まり、さらに経理処理はPC上の表計算ソフトウェアや経理ソフトウェアを使って紙の帳簿から経理データを扱う形態に変わった。しかし、分散した組織の経理処理を行うには個々の経理データを持ち寄ってさらに集計処理をしなければならなかった。今や遠隔地に分散した組織でもそれぞれが一つの経理システム（ITシステム）にデータを入力すると最初から一括した経理処理をすることができる。世界に分散した事業ですらインターネット上に有機的に構築されたITシステムにより統合される。その効果は絶大である。このようなITシステムは製造、商取引、行政等、我々が生活する社会のあらゆる部署に導入されている。

世界貿易センターに対するテロリズムでは航空機というハードウェアが武器として使われた。テロリストは攻撃対象にダメージを与えることを目的としているがセンセーショナルな効果があればさらに好都合なのだろう。その手段はハードウェアテロ

でもソフトウェアテロ（サイバーテロ）でも彼らの必要条件を満たせばよいのだとすると、冒頭で述べたインターネット上の巨大ＩＴシステムはテロリストにとって格好の攻撃対象である。

ＩＴのセキュリティ品質と製品仕様品質

ＩＴにはそのベンダーが定めた正当な利用者向けサービスの品質（ここでは「製品仕様品質」と呼ぶ）と不正な利用を阻止する品質（ここでは「セキュリティ品質」と呼ぶ）の二つが求められる。どちらもプログラム品質であるため、最終的な品質は設計からテストに至る地道な検証作業がいかに漏れなく行われるかにかかっている。これは、開発者がよく使う言葉でデバッグ（debug）、つまりバグとり作業である。その検証作業を軽減するツールはあるものの、設計者が定めた仕様どおりに動作することを丹念に検証していく以外によい方法はない。

製品仕様品質とセキュリティ品質の検証のために最後はデバッグを行うとしても、両者に対する最初の取組み方は大きく異なる。製品仕様品質は、設計者が定めた仕様が正しく動作することだけを確認すれば確保される。しかし、セキュリティ品質は、設計者が想定していない不正な利用方法に対しても適切な動作を求める。このため検証漏れが出やすい。これを脆弱性と呼ぶ。

例えばＬＡＮに接続されたクライアントＰＣからサーバＰＣにデータを送信する場合、製品仕様品質では、ＰＣからデータがサーバＰＣに届くことを確認できればよい。しかし、セキュリティ品質としては、そのデータがＬＡＮ上を電気信号として流れる時に漏洩したり改ざんされたりしないことまで検証することを求められる。ＩＴに対する不正な利用者インタフェースは至る所に存在し、完全には防御できないため厄介である。

ＩＴのセキュリティ品質対策

セキュリティ品質を向上させるための手法にはいろいろある。代表的な手法は下記の三つである。

うがむら　なおき

1973年から富士通株式会社でCOBOL、Java等の言語処理プログラム開発に従事、1998年、現情報処理推進機構（IPA）でITセキュリティ及び評価認証制度の設立作業を経て2001年電子情報技術産業協会（JEITA）に同制度のセキュリティ評価機関を設立し現在に至る。

● 方式A：セキュアな運用規則に従ってITを運用することによりセキュリティ品質を確保する（例：ISMS）。

● 方式B：ITの外部仕様とそのコンポーネントの特性に関する情報等から脆弱性を探索する（例：ブラックボックステスト）。

● 方式C：ISO/IEC15408（Common Criteria_：CC）に従って開発情報に基づく脆弱性を探索する。

近年話題になっているITシステムに対するサイバーテロ問題は、上記のどれか一つの手法を使えばすべて解決するわけではない。各手法にはそれぞれ長所短所があり、いずれも万能ではない。しかし、これらの手法を組み合わせてそれぞれの長所を活かす使い方をするとITシステムのセキュリティ品質は格段に向上する。

ITシステムはIT製品とアプリケーション（コンポーネント）により実装されることが一般的である。これらのコンポーネントごとのセキュリティ品質向上には方式Cが有効である。セキュリティ品質が確保されたコンポーネントを組み合わせてさらにITシステム全体のセキュリティ品質を向上させるには方式Bが有効である。そして更にITシステム全体の運用を方式Aで補完することによりITシステムのセキュリティはより強固になる（図1）。

ITのセキュリティ品質保証

日本では二〇〇〇年からセキュリティ国際標準ISO/IEC15408を基にした「ITセキュリティ評価及び認証制度」が運用されている。本制度は主にIT製品の開発設計から保守までのすべてのライフサイクルを公平中立な評価機関及び認証機関が検証することによりそのセキュリティ品質の正当性を保証する。検証対象（評価対象と呼ぶ）のセキュリティポリシー（方針）、開発ドキュメント等を使用して脆弱性を探索するため時間はかかるが多くのセキュリティ問題が検出される。この検証に合格した評価対象には国レベルが保証する認証書が交付される（図2）。

本制度を運用する国々は、主にIT製品に対して同一のセキュリティ国際標準を同一の手順により適用することを義務付けた協定CCRA（Common Criteria Recognition Arrangement）に加盟して、認証書の同質性を保証し、さらにその認証書の国家間での流通を図っている（図3）。CCRA加盟国は現在二六ヶ国に及び中国を除く世界の主要な経済圏をカバーしている。

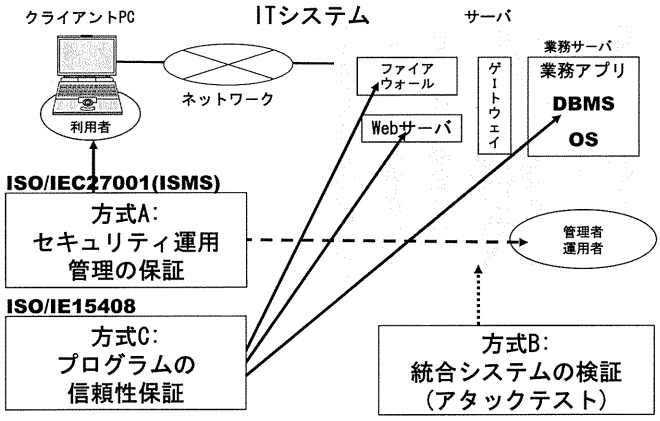


図1 ITシステムのセキュリティ保証

近年我が国で開発されるＩＴシステムには多くの海外ＩＴ製品が使われている。例えば、世界的に使用されているＯＳのWindows、データベース管理システムのＯＲＡＣＬＥ等は認証取得が常識となっている。いくら優秀な機能をもつＩＴ製品でもバックドアが仕込まれているかもしれない。保証のないＩＴ製品を組み込んだためにセキュリティトラブルが起きればＩＴシステム提供者の責任は重大である。

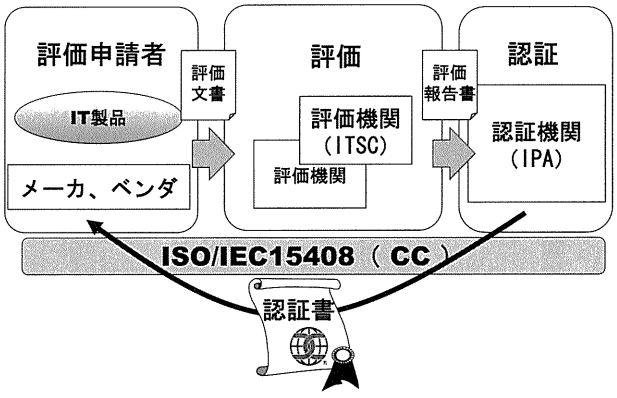


図２　セキュリティ評価認証制度の構成

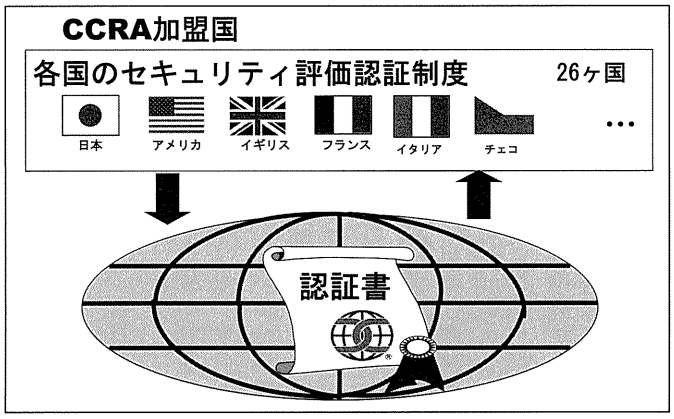
日本政府の対応とＩＴＳＣの役割

日本政府は、自らが調達するＩＴシステムの中で使用されるＩＴ製品に対してISO/IEC15408に基づく認証を必須とする旨の調達規定（統一基準）を定めている。当該統一基準ではそのＩＴ製品を特定するために次の製品分野を定めている。

①スマートカード（ＩＣカード）、②ファイアーウォール、③ＯＳ、④デジタル複合機、⑤不正侵入検知／防止システム（ＩＤＳ／ＩＰＳ）、⑥データベース管理システム（ＤＢＭＳ）

今後、少なくとも政府のＩＴシステムには、認証されたＩＴ製品が確実に導入されることを望みたい。

一般社団法人ＩＴセキュリテセンター（ＩＴＳＣ）はISO/IEC15408に基づく日本で最初のセキュリティ評価機関でありＩＴ製品に対する多くの評価実績を持つ。ＩＴＳＣはセキュリティ評価機関であるだけでなくＮＩＳＴ（米国国立標準技術研究所）及びＩＰＡ（情報処理推進機構）の暗号標準FIPS140、ISO/IEC19790に基づく暗号試験機関でもある。今や暗号機能の無いＩＴ製品は少なくなっているが、残念ながら暗号機能が正しく実装されていることが保証されたＩＴ製品は少ない。ＩＴＳＣは我が国ＩＴ製品のトータルなセキュリティ品質向上のため、その検証作業に引き続き努力してまいりたい。



CCRA：**IT**セキュリティの相互承認に関する国家間の協定

図３　認証書の流通