

中国、IT セキュリティ製品の強制認証実施規則を発表

日本機械輸出組合
通商・投資グループ

1 . 13 品目の IT セキュリティ製品の強制認証制度の実施規則を発表

2009 年 4 月 27 日、中国の国家品質検査検疫総局、財政部、国家認証認可監督管理委員会の 3 機関が共同で「IT セキュリティ製品の強制認証実施要求の調整に関する公告（2009 年第 33 号公告）を公布した。同公告は、以下の 3 点について言及している。

- (1) 2008 年第 7 号公告に係る 13 品目の IT セキュリティ製品それぞれについて実施規則を付属資料として公布する。すなわち、セキュアオペレーティングシステム製品、セキュリティ隔離・情報交換製品、セキュアルータ製品、セキュリティ監督製品、セキュアデータベースシステム製品、アンチスパムメール製品、ファイアウォール製品、侵入検知システム、データバックアップ・リカバリー製品、ネットワークセキュリティ隔離カード・スイッチングハブ製品、ネットワーク脆弱性スキャン製品、ウェブサイトリカバリー製品、スマートカード COS 製品。
- (2) これら IT セキュリティ製品の強制認証を中国「政府調達法」に定める範囲内において実施する。
- (3) これら IT セキュリティ製品の強制認証の強制実施時期を 2010 年 5 月 1 日まで延期する。

この 2008 年第 7 号公告とは、2008 年 1 月 28 日、中国の国家品質検査検疫総局、国家認証認可監督管理委員会が制定した「一部の IT セキュリティ製品に対する強制認証の実施に関する公告」のことであり、中国で販売される製品の品質や安全性に関わる「強制認証制度 (CCC)」の対象製品として、8 類 13 品目の IT セキュリティ製品を追加して、2009 年 5 月 1 日から施行するというものである。すなわち、これら 13 品目の IT セキュリティ製品は、中国の強制製品認証証書を取得していない場合及び中国強制認証マークを付していない場合、すべての出荷、販売、輸入又はその他経営活動を行ってはならないとされた。なお、CCC は中国独自の制度で、運用が恣意的である。また、相互承認機関を認めていないので、外国企業にとって認証取得手続きが煩雑で時間と費用がかかるとの不満が強い。

2 . 日・米・EU による強い反発

中国は、2007 年 8 月にこの 13 品目の IT セキュリティ製品の強制認証に関する技術的規則案を WTO の TBT (貿易の技術的障害に関する協定) 委員会に通知していたが (G/TBT/N/CHN/278-290)、これに対して米国は、TBT 委員会において、本規則は商業的な情報技術製品における情報セキュリティの強制認証のグローバルな規範を超えるものであるとして最終規則の発行の延期要請を含む強い懸念を繰り返し表明した。米国の要請は米中間の通商貿易

合同委員会(JCCT)でも中国経過的審査メカニズム(TRM)でもなされた。とりわけ米国が懸念したのは、IT セキュリティ製品の強制認証に当り中国認証機関がソースコード提出を要請してくる可能性があり、中核技術情報が中国側に流出するおそれがあったからである。

この米国の強い懸念に日本とEU そして韓国も唱和し、2008 年 11 月に開かれた TBT 委員会では、商業製品の情報セキュリティ強制認証を行う如何なる措置の採用も取りやめるべきであると強く迫った。かかる日米欧の批判に対して、TBT 委員会では中国側の規則案は TBT 整合的であるとしつつも、最終規則の実施に一定の猶予期間(1年間)を設けることを示唆していた(WTO G/TBT/M/46(23 January 2009))。

この度公布された「2009 年第 33 号公告」で、対象製品は変わらないが、対象範囲が政府調達法に限定され、実施時期が 1 年延期されたことに対し、米国の USTR(アメリカ通商代表部)は、2009 年 4 月 29 日付“USTR NEWS”で、商業市場に用いられる IT 製品が強制認証の対象から除外されたことは評価するが、中国政府が調達する製品に情報セキュリティ強制認証規則がグローバル規範に整合しない方法で 2010 年 5 月から実施されることに対しては、引き続き大きな懸念を持ち続けると表明している。日本政府も政府調達法に対象範囲が限定されたからといって懸念は解消しておらず、2009 年第 33 号公告発布直後の 4 月 29 日に行われた日中首脳会談において日本側から中国に政府調達の範囲が広いことを挙げ制度自体の撤回を求め、また 6 月 7 日に開催された日中ハイレベル経済対話でも再考を求めたが、前進がなかったと報道されている。

3 . 今後の論点と対応

「2009 年第 33 号公告」の実施規則だけをみれば、ソースコードという文言自体はいずれにも記載されていないが、スマートカード COS 製品の実施細則では、“EAL4 +”での評価保証が要求されており、国家 IT セキュリティ評価センターの規則によると EAL4 以上の場合ソースコード開示が求められるという(遠藤 誠「中国知的財産権法 Q&A」No.59(日本機械輸出組合「知的財産権情報」ウェブページ <http://www.jmcti.org/>))。しかしながら、他の 12 品目の実施細則ではその点は不明であり、参照されている他の中国国家規格と併せ読み解くなどして実施細則各々にソースコード開示が実態上求められるかどうか専門的にチェックする必要がある。ただし、根拠規定がなくとも運用上ソースコード開示が求められないとは限らないことが依然として不透明なところである。

強制的なソースコード開示義務を課されるということは、サイバーアタックや技術流出が激しい現代の IT セキュリティ環境で、我が国の戦略技術に容易にアクセスできるツールを与えることにもなりかねない。かかる懸念を抱く企業は中国の政府調達法が対象とする調達案件から事実上排除されることになる。それは、IT セキュリティ製品のサプライヤーはもとより、IT セキュリティ製品のユーザーであるメーカーやエンジニアリング企業もサプライヤーから開示の許しが出るはずもないので、同様、事実上排除される。その点は外国製の IT セキュリティ製品のユーザーである中国国内企業も同じ立場に置かれることになる。

ちなみに中国は未だ WTO 政府調達協定に加入しておらず、政府調達の対象範囲は不透明である。また、将来にわたって 13 品目に限定されるという保証もない。WTO の TBT 委員会や中国

の WTO 政府調達協定加盟交渉で限定し明確化する努力は必要である。しかしそれには時間がかかり、一定の限界がある。IT セキュリティ製品のソフトウェアのソースコード開示が規定される規則の実施は、結果として中国自体に大きな不利益が及ぶことを中国当局に十分認識させた上で、撤廃又は無期延期を求めることが最上の対策であろう。従前に増して日米欧先進国のみならず中国国内産業も輪に巻き込んで、世界各国が一丸となって対応することが求められる。

他方、中国が情報セキュリティ機能の保証確保という目的を追求するのであれば、この強制認証制度の代替策として、先進国で採用されているセキュリティ評価基準である ISO/IEC15408 に基づく「IT セキュリティ評価及び認証制度」での相互承認協定(通称“Common Criteria”)を用いる方を中国に薦めることも有効であろう。