『日経エレクトロニクス』2008年12月15日号　P119 ～ P126から転載

“ソース・コード強制開示”は本当か 中国，強制認証制度拡大の狙い

暗号方式の許可を得るなど先手も必要

尹 昌来
チャイナウェイ 代表取締役社長

中国政府が外国企業に対し，デジタル家電などの製品情報を開示する「新制度」を2009年5月に導入するとの新聞報道が日本国内に波紋を呼んでいる。中国へ輸入・販売する製品に認証を求め，その際に組み込みソフトや暗号ソフトのソース・コードの開示を要求するというのだ。これに対し，日本の企業や産業界からは，不安や心配，反発の声が上がった。（吉田 肇＝本誌）

（イラスト：つだ かつみ）

日本経済の中国市場への依存度が高まっている折，新たな規制によって中国への輸出が制限されては，深刻な影響があると日本企業が心配するのも無理のないことだ。新聞報道によると，2008年9月に訪中した日中経済協会は中国政府当局との会談で，新制度への懸念を表明したとされる[1]。

しかし，規制の詳細はいまだ明らかになっていない。実際はどうなのか，中国政府の狙いは何なのか，本当にソース・コードの強制開示が求められ，知的財産（知財）が流出するのだろうか――。

ファイアウオールやルータを認証

まず，中国政府の発表内容から事実を整理してみよう。公告が発表されたのは，新聞報道の約8カ月前の2008年1月28日である。国家質量監督検験検疫総局（AQSIQ）と国家認証認可監督管理委員会（CNCA）が，「強制認証制度（China Compulsory Certification：CCC）」の品目に情報セキュリティー製品を追加すると発表した。ファイアウオール，ルータ，OS，ネットワーク監視システムなど8大分類13種類を新たにCCC制度の対象に加え，その規制を2009年5月1日より施行するというのである（表1）。唐突であいまいな発表だったが，簡潔に言えば，既存のCCCにおける認証対象製品の品目追加だった。

日本の産業界や業界団体からは，この公告に対し，不安の声が上がった。経済産業省は，2008年6月に「対象製品リストは，認証の対象製品について明確なスペック等は明らかにされておりませんが，この措置により，認証取得にかかる膨大な業務が企業の負担となる可能性が高いことや，審査の

表1　情報セキュリティー製品のCCC対象リスト
経済産業省の資料を基に本誌が作成した。表記は原文に合わせた。

カテゴリ	製品名	対象範囲
1. ボーダー・セキュリティ	ファイアウオール	(1)ファイアウオールの機能を主機能とするソフトウエア，ハードユニット (2)その他のネットワーク製品のファイアウオール・モジュール
	LANカードおよびスイッチング・ハブ	(1)LANカード式パソコン (2)LANカード (3)LANカード式スイッチング・ハブ
	VPN	(1)VPN製品 (2)隔離およびデータの一方方向の転送製品
2. 通信セキュリティ	ルータ	IPSec/SSL，およびファイアウオール，ネット侵入探知，セキュリティチェックなどの単機能あるいはマルチ機能を持つセキュリティ・モジュール付きルータ
3. ID識別および訪問者管理システム	インテリジェントカードICチップ用OS（COS）	(1)接触式あるいは非接触式の層組放式のＣＯＳ (2)その他の一体型あるいは内装型のＣＯＳ
4. データのセキュリティ	データバックアップおよびリストア	独立のデータバックアップおよびデータの復元用ソフトウエア
5. ベース・プラットフォーム	OS	(1)独立のＯＳソフト (2)ＯＳ一体型の製品あるいはＯＳ内装型の製品
	データベースシステム	(1)独立のデータベース・システム・ソフトウエア (2)データベース・システムと一体型の製品あるいはデータベースを内装する製品
6. 内容のセキュリティ	迷惑メール防止製品	(1)フィルタータイプの迷惑メール防止ゲートウエイ (2)転送メールに対する迷惑メール防止システム (3)迷惑メール防止が一体となったメールサーバ (4)既存のメールサーバに導入する迷惑メール防止ソフトウエア
7. 分析・監査および監視・制御	不正アクセス侵入探知システム（IDS）	(1)ネットワーク型の侵入検知システム (2)パソコン本体侵入検知システム
	ネットワークの監視システム	ネットワークの監視システム
	操作履歴，ログを収集・分析する製品	パソコン本体，サーバ，ネットワーク，データベースおよびその他の応用システムなどのいずれか，あるいは複数の履歴・ログを収集・分析する製品
8. 応用のセキュリティ	ファイル改ざん検知システム	静止状態のホームページファイル，動態スクリプトファイルおよび目録に対し，自動的に復元するファイル改ざん検知システム

観点でソフトウエアの知財が侵される恐れがあるなど，事業活動に与える影響は軽微とは言えない範囲に及ぶことが予想されます」との見解を表明している[2]。

情報サービス産業協会(JISA)も，同年7月に発行したニュース速報の中で「制度が複雑で規格変更も頻繁に行われる等，特に海外企業の負担が大きくなっている。今回の措置拡大に伴い，セキュリティー関連ソフトも対象になると思われるが，その範囲は不明である」と，この問題に触れている[3]。

ソース・コードを開示？

ここまでは比較的冷静な反応だったが，2008年9月に新聞がこの問題を取り上げ，新制度によってソース・コードの開示が要求されるとの報道があり，波紋が大きくなった。新聞記事を引用してみよう[4]。

「中国政府が外国企業に対し，デジタル家電などの中核となる製品情報を中国当局に開示するよう命じる新制度を2009年5月から導入する方針であることが18日わかった。対象はICカードやデジタル複写機のほか，薄型テレビなども含まれる可能性がある。(中略)具体的には，対象となる製品について，デジタル家電などを制御するソフトウエアの設計図である『ソース・コード』の開示を外国企業に強制する」。

この報道後，情勢が微妙に変わり，危機感が強くなってきた。新聞報道によると，2008年10月には日本経団連 会長の御手洗冨士夫氏が定例会見でこの件について触れ，「ソース・コードの開示は，裸になるということ。日本企業も全部，断固として反対であり，反対し続ける」と述べたという[5]。

製品安全を求めるCCCとは

そもそもCCCとは，どんな制度だろうか。その概要を確認しておこう。同制度は，中国国内に流通する人の健康と安全，動植物の生命と健康，環境保護，公共安全に影響のある製品に対して，同国の技術標準に対する適合性の審査によって「強制」的に安全性を認証するもの。2002年8月に運用が始まった[注1]。背景には，中国のPL法ともいうべき「中国製品品質法」と，国内の強制規格に合致しない製品の生産・販売・輸入を禁じた「標準化法」という二つの法律の存在があり，両法律を具体的な制度として落とし込んだものといえる(図1)[注2]。

認証に当たっては，指定された試験機関へ技術資料や製品サンプルなどを提供しなくてはならない(p. ★の「CCCはCNCAが管理，公告を機に認証機関を追加」参照)。そこで，技術標準と適合するかを調べる「型式試験」によって，物理的・電気的な危険性や環境への影響などの問題がないかをチェックするのである。

型式試験に合格すると「国家強制製品認証証書」が発行され，製品へのCCCマークの添付が許される。このマークがないと，中国への輸出や同国内での販売ができな

注1) 以前は，中国商品検験局(CCIB：China Commodity Inspection Bureau)認証，および中国電気製品認証委員会(CCEE：China Commission for Certification of Electrica Equipment)認証という二つの製品安全の認証制度が存在していた。CCIB認証は輸入製品を，CCEE認証は国産，輸入を問わず中国国内で流通・販売する電気製品を対象としたものだったが，それぞれ独自に対象品目を決めていたため，適合基準の不整合や規制の重複などが問題となっていた。そこで，中国は2001年12月にWTOに加盟したのを契機に，両制度を統一した新たな認証制度としてCCCを発足させた。

注2) 中国の標準規格には国家規格，部門(業界)規格，企業規格の3種類がある。さらに，国家規格と部門規格には，強制規格と任意(推奨)規格の2種類がある。

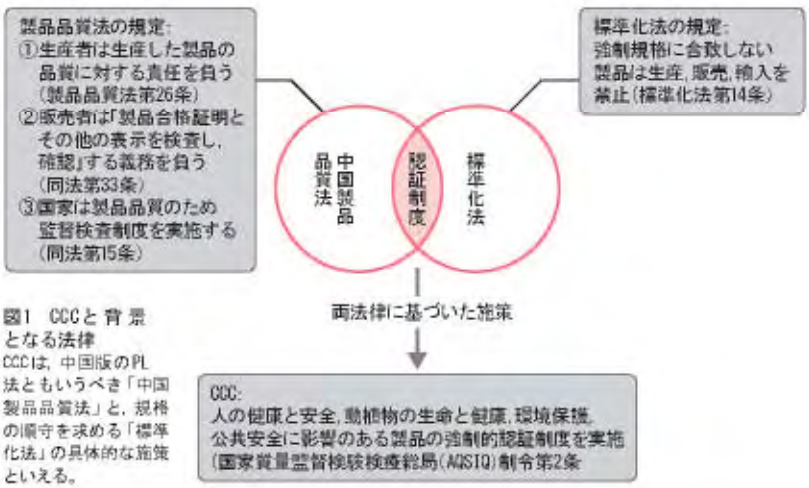


図1 CCCと背景となる法律
CCCは，中国版のPL法ともいうべき「中国製品品質法」と，規格の順守を求める「標準化法」の具体的な施策といえる。

い[注3]。施行当初の対象品目は19分野132品目だったが，その後追加されて現在は22分野159品目となっている。今後，CCCの対象製品は拡大すると想定される。今回のITセキュリティー製品の追加も，その一環の措置といえる。

相互認証を認めず

CCCには，かねて問題が指摘されている。手続きが煩雑で申請から許可が下りるまでに時間がかかる点だ(図2)。特に，現状のCCCは海外の適合性評価機関の参加を認めておらず，中国の試験機関に資料やサンプルを送付したり，生産工場の審査を受けたりしなくてはならない。外国企業にとって，取得手続きの時間と労力が大きな負担となっている。

通常，こうした認証制度では，異なる制度を国家間や地域間で相互認証できるよう，協定を結ぶことが多い。それによって，似たような認証手続きを何度も繰り返さずに済む。ところがCCCは，相互認証を一切認めていない(p. ★の「日本のセキュリティー製品認証は国際規格に準拠」参照)。

加えて，今回の情報セキュリティー製品の追加は，公告の発表から実施まで1年余りしかなく，対応の時間的余裕がないことも問題だ。2008年11月末時点で実施細目が明らかになっておらず，海外企業が認証を申請しても2009年5月までに許可を得るのは，実質的にはかなり難しいだろう[注4]。

通信機器はこれまでも

実は，既に中国には情報通信分野の製品を対象とした規制がある。例えば，通信分野では2001年から「通信装置入網管理規則(入網許可制度)」が施行され，ソフト・スイッチやGSM，CDMA基地局用機器，携帯端末などの製品に対して認証を要求している。また，無線LAN関連機器は2004年にCCCの対象品目に追加されており，強制認証が適用されている。このほか日本の電波法に相当する「中国電波法遠距離無線設備管理規定」などもある(図3)[注5]。これらの認証は，それぞれの認証実施細則に基づいて実施されている[注6]。

通信装置入網管理規則は，法制上はCCCとは別の規制だが，その実態はほぼ同等で，技術資料やサンプルを提供して試験や審査を通過しなくてはならない。ハードウエアばかりでなく，制御するためのソフトウエアも審査対象だ。つまり，これまでも国内外の通信各社は，試験機関であるChina Telecommunication Technology Labs(CTTL)で携帯電話機や基地局の認証を経験している。情報セキュリティーのCCC適用も認証の一環と考えられる。

強制開示は本当にあるか

2008年1月のあいまいな公告では，情報

注3) CCCマークを継続利用するには，初回の認証取得後も1回/年以上，定期的に審査を受けなければならない。

注4) 強制認証もさることながら，中国製品品質法の性能基準や環境基準も，解釈や対応が難しいとの指摘がある。

注5) このほか，医療分野でも2000年に発表された「中国医療器械管理条例」によって，医療機器の実証実験，登録制度，登録証書発行の制度を実施している。

注6) 例えば，通信端末設備の認証は，認証の適用範囲，認証の検査基準，実施の基本要求を規定した「電信設備強制認証実施規則：電信端末設備」(CNCA-07C-031：2007)に準拠している。無線LAN関連機器のCCCも同様の実施細則(CNCA-11C-048：2007)に基づいている。

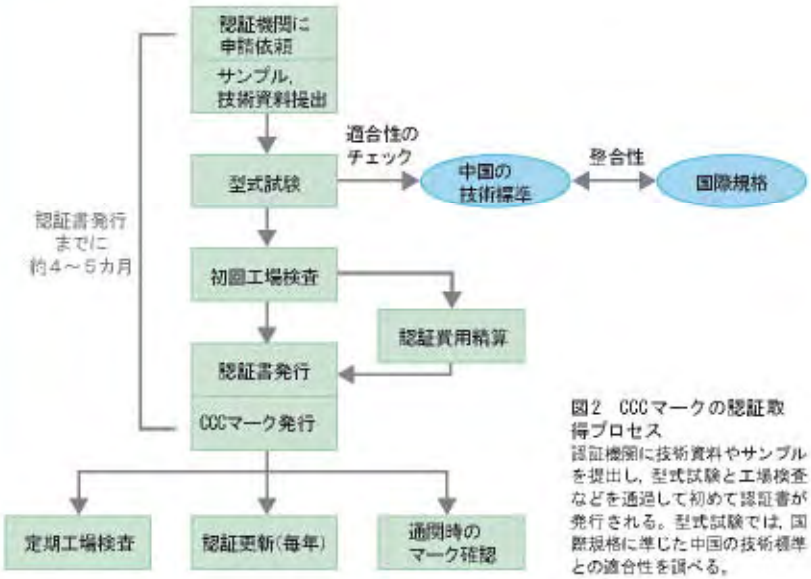


図2 CCCマークの認証取得プロセス
認証機関に技術資料やサンプルを提出し，型式試験と工場検査などを通過して初めて認証書が発行される。型式試験では，国際規格に準じた中国の技術標準との適合性を調べる。

セキュリティー製品に対する規制の詳細は分からないが，少なくとも公告の中にはソース・コードの開示を要求するとの文言はない。あらためて事実を整理すると，注目すべきは主に以下の3点といえる。

①対象企業は外国企業だけではない。中国市場で販売する中国国内企業，三資企業†などもすべて対象となる。
②今回の発表は，新制度ではない。既存のCCCへの情報セキュリティー製品(8大分類13種類)の追加であり，対象もデジタル家電などは含まれていない。
③実施細則がまだ公表されておらず，公告を見る限り，ソース・コードの開示は正式に要求されていない。

従って，細則が不明な段階では，"情報セキュリティー製品の強制認証"すなわち"ソース・コード強制開示"とは断言できない。今回のCCC拡大によって，情報セキュリティー製品を中国に輸出する際に技術資料やサンプルの提供を求められるのは間違いないが，求められる資料にソース・コードが含まれるかどうかは分からないのだ。私は日本の報道機関がやや過剰反応しているのではないかと考えている。冷静な視線で事実を追究すべきだろう。

むしろ「商用暗号管理条例」(国務院273号令，1999年公告)との関係に気を配るべきだ。この法律は暗号の安全性・確実性の担保を目的とした厳しいもので，中国国内で販売・流通する暗号化製品の暗号方式について，国家暗号管理機構の許可を義務付けている。許可のない暗号技術を含んだ製品は輸入・販売できない。

今回のCCC拡大で，ソース・コードの強制開示という話題ばかりが先行しているが，当局が把握したいのは，ソース・コードというよりは同条例で認定されたアルゴリズムを使った暗号処理方式を用いているのか，それが情報漏洩などに対して堅牢かという点だろう。CCC制度が情報セキュリティー製品に適用されれば，暗号技術を用いている製品には商用暗号管理条例に基づいた暗号利用の許可が求められ，その暗号が中国の規制・標準に適応するかどうかがチェックされる可能性が高い。許可されていない暗号技術を使った製品は，CCCマークが公布されない恐れがあるのだ。

現在，「各企業の知財を守るという前提で，CNCAが検査基準を検討している」(当局関係者)という。ソース・コードの開示要求の心配よりも，強制認証の申請前に商用暗号管理条例に合致した暗号方式を採用する，あるいは同条例の認定を取得するといった対策が先決と考えられる。

図3　中国製品品質法の範疇での管理規定
既に通信装置入網管理規則や中国電波法遠距離無線設備管理規定などが，中国製品品質法に基づき，情報通信機器に対してCCCに類した認証を求めている。情報セキュリティー製品のCCCへの追加は，従来の施策の延長と言える。

†三資企業＝外国企業が中国へ進出する際の企業形態の総称。中国企業と共同出資して合弁企業を作る「合弁」，中国企業とパートナー契約を結ぶ比較的小規模の「合作」，単独で現地企業を設立する「独資」の3種類の形態があるためこう呼ばれる。

国際的な信頼確保のために

実は，今回のCCCの対象拡大の背景には，中国の国家戦略とそれに基づく，二つの狙いがあるとみられる。一つは公共安全と強固な情報セキュリティー社会の実現，

もう一つは「IT強国」となるための標準化の策定とその実施である。

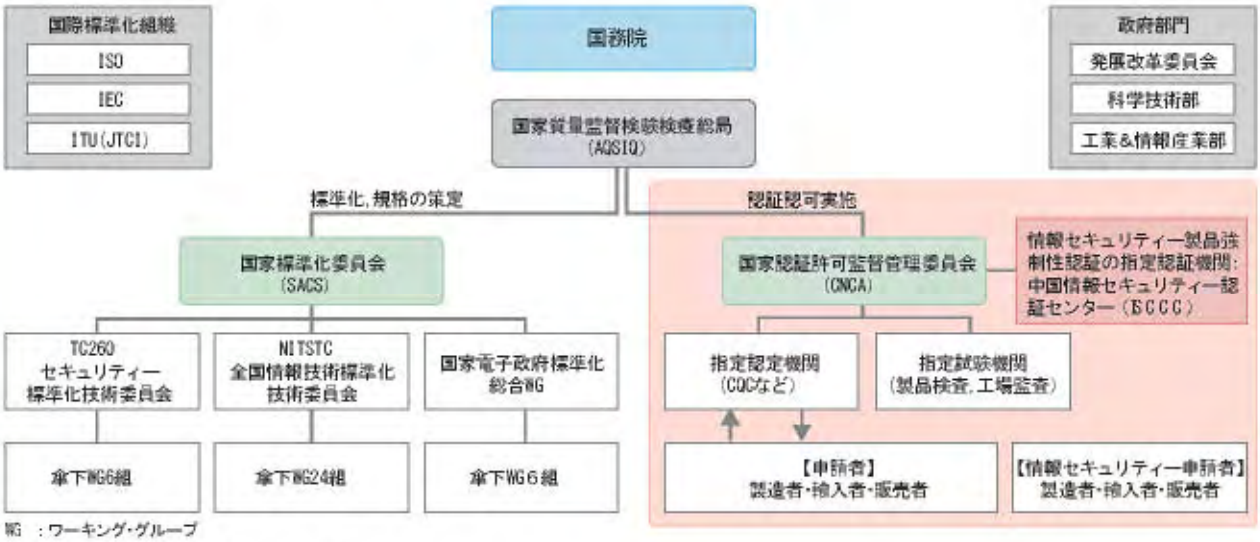
前者からひもといてみよう。中国政府は，人民大会などで今後の①環境汚染防止と処置，②生態環境保護，③資源エネルギー管理，④国家安全保障（セキュリティー），の4大分野に国家財政予算を先行投資することを表明している。今回のCCCの拡大は，④の具体策の一つと考えてよい。中国国内にとどまらず世界的にも注目される課題であり，国内市場の秩序を守るため認証制度を徹底して，規格を標準化しようとしているのだ。

中国は，インターネット人口が2007年に2億1000万人に達するIT大国である。だが，その90.56%にコンピュータ・ウイルス感染被害の経験があるといわれている。1998～2003年にかけては全国規模のウイルス感染が5回発生し，しばしば政府のネットワーク運営が困難になったし，2005年には，2027の公的機関のWebサイトを含む9100のWebサイトが改ざんされた。ハッカーの

CCCはCNCAが管理
公告を機に認証機関を追加

中国では，国務院の管轄下にある「国家質量監督検験検疫総局（AQSIQ）」が技術標準の作成や規制を監督している。CCC制度はAQSIQの下にある「国家認証許可監督管理委員会（CNCA）」が管理しており，実質的な認証業務はその傘下にある認証機関や試験機関が担っている（図A-1）。

2008年1月の公告で情報セキュリティー製品をCCCの対象にする際に，中国情報セキュリティー認証センター（ISCCC）が新たな認証機関として追加された。それと同時に，1次指定試験機関として，情報産業部コンピュータセキュリティー技術試験センターなど7カ所が追加されている。



図A-1　中国のIT標準化と認証実施の体系
CCCでは，CNCAの管理下にある複数の指定認証機関と，100カ所以上ある指定試験機関によって認証作業が実施される。情報セキュリティー製品を対象品目に加えるに当たっては，新たに認証機関としてISCCCと七つの試験機関が追加された。

被害件数も世界3位と，決して情報面で安全な国とはいえない。今回のCCCの拡張には，情報セキュリティー製品の品質を担保し，そうした汚名を払拭して国際的な信用を高めたいとの思惑がある。

大国から強国へ転換

もう一つの狙いは，IT強国への転換だ。ブランド力や技術力を強化して輸出を拡大し，国際的な技術規格策定への影響力を高めようとしている。今の中国は，「IT大国」だが「IT強国」とはいえないからだ。

中国の電子通信情報産業は巨大市場を形成しており，2007年度の売上高は前年度比18%増の5.6兆元（約80兆円）と2ケタ成長を続けている[注7]。電子情報産業の輸出入金額は，2007年度には前年度比23.5%増の8047億米ドルに達している。情報産業の一つの柱であるパソコンの生産台数は，2007年度は1億2000万台と全世界の40%を占める[注8]。

しかし，利益が少なく，技術面でもリーダーシップを発揮できていない。例えば，薄型テレビ事業の平均粗利益は，軒並み2%未満である。パソコンも，比較的利幅の大きなノート・パソコンは中国に進出している台湾系のODM（相手先ブランドによる設計・製造）メーカーが中心で，中国本土の大手パソコン・メーカーは生産量こそ多いものの小さい利幅に甘んじている[注9]。携帯電話機市場も，数ばかりで利益は小さい[注9]。

加えて，近代化の遅れから技術の標準化では海外勢の後塵を拝し，独自の技術規格をほとんど持たないのが実情だ。テレビやDVDプレーヤーなどのデジタル家電の主要技術は，海外メーカーが握っている。中国統計局は，IT輸出型企業の60%が海外特許の侵害といった問題に直面しており，その損失は年間450億ドルと試算している[注10]。IT分野での特許出願件数も，中国企業のそれは外資系企業の60%強にすぎない。

これまで中国は，低コストを武器に外資を呼び込んだ。それによって世界中の企業が工場を設置するようになったが，他の先進国と技術力で勝負できるようにはなっていないのだ。中国政府はこうした状況を憂慮し，今後の輸出製品構造の調整と技術立国路線を，中長期の国際戦略と位置付けている。特にIT分野では，中国主導での技術標準の策定とその認証実施が重要な課題だと認識して，戦略の転換を図ろうとしている（図4）。情報セキュリティー製品の規制強化は，その布石なのである。

早期対応と中国への働きかけを

だが，当局でも規制の細目はまだ決めかねているようで，規制強化の公表だけが先走った感は否めない。国内外の反応を見ながら決めようとの思惑もあるのだろう。

ただし，当局が公告を発表した以上，それが覆る可能性は極めて小さく，情報セキ

注7）2008年度の売上高は，前年度比23.6%増の4.75兆元（約63兆円）で，GDPに占める割合も2005年度の3.84%から2006年度には7.5%に増大している。

注8）台湾系の主なノート・パソコンベンダーとしては，大衆電脳，仁宝，神達，倫飛，緯創，藍天などがある。

注9）携帯電話機の生産台数は，2006年度に4億3000万台，2007年度には5億4000万台と世界の47%を占める規模となっているが，市場は過当競争に陥りつつある。一部企業は同市場のOEM事業から撤退し始めた。

注10）これは輸出額の25%に相当する。

図4　中国の経済発展の方向性
これまでは低コストを訴求して外資を呼び寄せ，国内産業を発展させてきた。これからは国内技術の振興による技術立国と，それによる内需の拡大を目指している。情報セキュリティー技術をCCCの対象に加えたのは，国内のIT技術を発展させる上で情報の安全性と秩序の維持を図るためと考えられる。

ュリティー製品が認証対象となることは避けられない。対象品目を中国で取り扱っている日本企業は，強制認証にいち早く対応できるよう情報収集するとともに，商用暗号管理条例に基づいて暗号利用の許可を得るなどの先手を打っておく方がよい。

同時に，今後の輸出手続きの簡素化を考えて，相互認証を強く働き掛けていくことも忘れてはならない。中国政府当局は依然として「相互認証を認めない」との立場を取っているが，今後の国際協調路線を考えるそうすれば，いずれ相互認証を認めざるを得ないと思われる。

と，このままで済む問題ではないだろう。CCCは施行から数年と歴史が浅いため，中国当局内部でも議論が不十分な面がある。政府や業界団体を通じて相互認証に向けた議論を活性化させることが肝要だ。

参考文献
1)『読売新聞』2008年9月24日付朝刊
http://www.osaj.jp/government/other/2008/080627_meti.html
3) http://www.jisa.or.jp/news/649/download/301.pdf
4)『読売新聞』2008年9月19日付朝刊
5)『読売新聞』2008年10月7日付朝刊
中国工業与信息化業部のWebサイト(http://www.miit.gov.cn/n11293472/)

日本のセキュリティー製品認証は国際規格に準拠

そもそも，製品の安全や規格を認証・評価する制度は各国が独自のものを運用しており，中国だけが特別ということはない。むしろ，現在，各国における認証基準は多様化しつつあり，今後もますます複雑化する傾向にある。

例えば，米国には北米輸入規格(UL)や米国規格協会(ANSI)，連邦通信委員会(FCC)などの多様な規格があるし，欧州にも携帯電話機を認証するGlobal Certification Forum(GCF)や欧州統一規格(EN規格)，EC指令など多くの規制がある。

日本にも電気用品安全法や消費生活用製品安全法などの法律をはじめ，電気通信端末機器審査協会(JATE)による情報通信機器に対する認証制度などがある。情報セキュリティーに対する評価・認証制度も既に存在している。製品評価技術基盤機構(NITE)は，2001年に「ITセキュリティー評価及び認証制度(JISEC)」や，情報処理推進機構(IPA)よる「暗号モジュール試験及び認証制度(JCMVP)」を発足させている。

JISECは，電子政府のセキュアな基盤構築に先駆けて，IT関連製品のセキュリティー機能・品質を国際規格(ISO/IEC 15408)に基づいて評価および認証するもので，OS，データベース管理システム，通信ソフトウエア，ファイアウオール，ICカード，リーダーなどのハードウエアが対象となっている。2003年10月31日には，日本は国際相互承認アレンジメントであるCCRA(Common Criteria Recognition Arrangement)に加盟した。これにより，JISECにおける認証製品は，CCRA加盟国においても認証製品として受け入れられる体制が確立された。現在，同制度の認証業務はNITEからIPAに移管されている。

また，2003年にJCMVPとして，暗号処理モジュールが，その内部に格納するセキュリティー機能並びに暗号鍵およびパスワードなどの重要情報を適切に保護していることを，第三者が試験・認証する仕組みが導入された。利用者が暗号モジュールのセキュリティー機能などに関して，正確で詳細な情報を把握できるようにする制度である。

ただし，今回の情報セキュリティー製品のCCCへの追加は，“強制”的であるという点で，これら日本のセキュリティー製品の認証制度と大きく異なる。