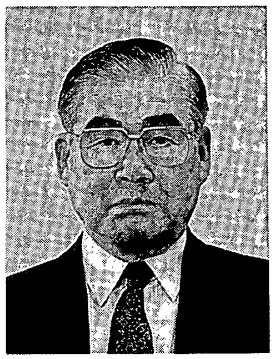
暗号政策の議論を深めよう



(株)情報通信総合研究所　社長　**本間　雅雄**

OECDの暗号政策ガイライン

OECD(経済協力開発機構)は去る3月末，暗号機能を実際に利用するにあたってのガイドライン「OECD暗号ガイドライン」を公表した．インターネット上での電子商取引や電子マネーの利用を進めるには，個人や企業の情報を安全な暗号に置き換え，第三者に不正に利用されないようにすることが不可欠である．

ガイドラインは，暗号技術の開発や普及は今後も市場に委ねるという基本的立場を示した上で，利用される技術がバラバラだと混乱が起きるため，各国が協調して国際的な技術標準作りを急ぐべきだ，と勧告している．

来春のOECD理事会で正式決定を行い，各国はそれを受けて暗号技術に関する国内の法整備に入る見通しで，電子商取引のグローバルなルール作りがいよいよ動きだすことになった．

ガイドラインは8項目から構成されている．

1．暗号機能は信頼性が高くなければならない．
2．暗号機能は利用者が自由に選択できなければならない．
3．暗号機能の開発は市場原理に委ねなければならない．
4．暗号機能の国際標準化を推進しなければならない．
5．プライバシーに対する個人の権利は十分尊重されなければならない．
6．適法な手続きによる情報へのアクセスは容認してもよい．
7．暗号サービスなどの提供者はその責任を明確にしなければならない．
8．各国は暗号政策を遂行するため協力しなければならない．

適法な手続きによる情報へのアクセス

この中で特に議論を呼びそうな項目は，「6．適法な手続きによる情報へのアクセス」である．その主文は「国の暗号政策は，暗号化されたデータの平文，または複号化のための暗号鍵に適法な手続きにもとづいてアクセスしてよい．これらの政策は本指針に含まれる他の原則を最大限尊重しなければならない．」ことを強調している．

また，「適法な手続きにもとづいて暗号化されたデータの平文もしくは暗号鍵にアクセスする場合，アクセスを要請する個人もしくは組織は平文を所有する法的権利を有するものに限り，かつ入手したデータは法で定める目的以外に使用してはならない．」ことを定めている．暗号鍵を紛失した場合のデータ復旧も考慮に入れて，当事者には個人も含めている．

電子商取引，電子マネー，電子データ交換などが，インターネットのようなオープンなネットワーク上で広く行われるようになれば，暗号の利用とその高度化は不可欠である．しかも，取引の範囲もボーダレスになっていく．

そういう状況のもとで，暗号の利用が無制限に行われれば，テロ集団や麻薬取引などの犯罪組織

が連絡に利用したり，脱税などの不正な方法で取得したお金を電子マネーに換えて外国に送金して，「資金洗浄」を行う危険性もある．

このため，OECDの暗号ガイドラインでは，安全保障や治安上の懸念がある場合に限り，適法な手続きに従って解読権（lawful access）を認めてもよいとして，その判断を各国に委ねることにした．

「キーリカバリー」方式

これまで米国政府は安全保障上の観点から，暗号を含む製品の輸出には慎重な態度をとってきた．しかし，議会の公聴会などで「米国政府は暗号に関するビジネス・チャンスを阻害している．このままでは日本や欧州に抜かれてしまう．」といった産業界からの証言が相次いだ．

昨年10月に米国政府は，暗号鍵を政府機関に寄託することを義務づける「キーエスクロー」方式の実施を断念して，適法な手続きによる情報へのアクセスを前提に，暗号鍵管理を民間に委ねる「キーリカバリー」方式が受け入れられれば，56キロビット長までの暗号ソフトの輸出を認める（従来は40ビットまで）意向を表明した．これまで強硬に反対してきたIBMやアップルコンピュータなどの大手11社は，新方式の共同開発に合意するなど同調する動きが相次いでいる．

フランスでは「ローフル・アクセス」を容認する法律が成立し，英国も法制化の準備に入っている．欧州では暗号鍵管理の方式として，トラステッド・サード・パーティと呼ぶ認証局と類似した方式が提案されている．

インターネットなどのオープンなネットワークの上で展開される電子商取引は，国境を超えて広がっていくだろう．そこでの暗号通信が国の安全保障に脅威を与えかねないことから，一定のセーフガードのもとでの「ローフル・アクセス」の容認が国際標準化する可能性が強い．

OECDの暗号政策ガイドラインは「ローフル・アクセス」の採否を各国の裁量に委ねているが，採用しない国に対しては暗号ソフトの輸出入を規制するか，輸出を認める場合でも政府が暗号鍵を留保するなどの条件を課すことになるだろう．そうなれば，暗号を使った海外との電子商取引ができなくなるだけでなく，暗号の解読権を外国に握られるという深刻な事態を招きかねない．

暗号政策の議論を急げ

法務省は通信傍受を法律上明文化することを法制審議会に諮問していたが，7月にようやく一定の条件のもとで認めるという答申を行った．現在でも，麻薬取引などで捜査に必要な場合は，裁判所の命令などによって傍受が行われているのだから，法律に根拠を求める方がケースバイケースの対応よりも，国の権力によるプライバシーの侵害に有効に対処できるのではないか．暗号鍵の問題は通信傍受を前提にしており，早期の解決を期待したい．電子商取引は暗号技術の進化を前提にしているが，暗号技術は国の安全保障政策と密接にかかわっている．一方，電子商取引は経済のグローバル化の流れにのって，国境を超えて広がっていくため，各国の暗号政策との調和が必要になってくる．

「ローフル・アクセス」を可能にする暗号鍵の管理方式も，国が直接関与しないトラステッド・サード・パーティーや民間の自主管理によるキーリカバリー方式が提起され，各国で議論されている．暗号技術は暗号鍵の管理システムと一体で，暗号政策の確立が遅れれば，わが国の暗号技術の開発もそれだけ遅れることになる．暗号政策について，本格的な議論が深まることを期待したい．