論　　説

グローバル経営における技術情報管理

知的財産管理第２委員会
第　３　小　委　員　会*

抄　録　企業経営の目的は，開発・製造・販売により利益を得ることであり，利益を生み出す源泉の一つとして技術情報を如何に管理するかが，グローバル経営において健全な企業活動を行う上で重要な要素であることは言うまでもない。本稿では，利益を阻害しそうなリスク要因について総括的に取り上げ，リスク防止に向けた「グローバル経営における社内管理体制」を考察する。特に，米国・中国で考慮すべき「法律」と「IT化」におけるリスク対策に焦点を絞る。「国内の技術情報管理と，海外の技術情報の管理上での課題と対応策」について，会員企業の一助になれば幸いである。

目　次

1．　技術情報管理におけるリスク概観

企業活動により生じる技術情報は，財産的価値を有していることから，その管理を誤ると，経営上の損失が生じてしまう恐れがあることは言うまでもない。近年の大幅な社会変化（グローバル化，IT化）により，旧来の管理体制のままでは対処できない新たなリスクが生じつつあることを，我々は再認識する必要がある。これらリスクとその対処法を個々に論ずる前に，まず「リスク全体を概観」することにより論点を提示しておきたい。

1．1　流出リスクと流入リスク

生産拠点の海外シフトや現地企業との合弁事業を行う際に発生する「意図せざる技術流出」は，主に以下３点の要因によって発生する。

① 契約交渉時の不適切な対応，契約内容不備，契約後の社内管理体制の不備に起因する技術ライセンス／技術援助に伴う流出リスク。

② 技術指導や海外生産に伴う流出リスク。

③ 現地スタッフの転職や自社従業員のモラル（認識）低下に伴う流出リスク。

一方，このように日頃意識する機会の多い流出リスクに対し，事業をグローバル展開するにあたって我々がつい見落としがちであるのが流入リスクである。IT化により情報が国境さえも容易に超えて共有し得るものとなったが，例えば，海外拠点で得られた情報を「日本の親会社が共有・管理」できるようにすること自体が，情報の種類によっては他国の「輸出規制」に抵

* 2004年度　The Third Subcommittee, The Second Intellectual Property Management Committee

触する恐れがあることに注意が必要である。

つまり，技術を国外に持ち出す場合に一定の手続きや規制があるにも関わらず，電子データの共有化や電子メールの活用などにより，無意識のうちに法を侵す可能性があり得るということを認識しておく必要がある。自国内で創作された発明の自国への第１国出願の義務を課している国があることから考えても，このリスクを軽んじるわけにはいかない。

流入リスクについて，流出リスクと同等以上に注意を払うべき環境となりつつあることを，我々は意識しておかなければならない。

1. 2　法的リスク

各国の法体系を眺めてみると，ほとんどの国が，名称の違いこそあれ，「特許法」と，「不正競争防止法（トレードシークレット法)」の２つを設けており，一見，技術情報はどの国でもそれらの法により同等に保護されているように見える。しかしながら，詳しく見ていくと，法律は各国ごとに違いがある場合があり，注意が必要である。表１に法律の違いにより生じるリスクを示す。

表１　法的リスク

法律の違い	リスク類型	流出	流入
日本にある法律が,当該国に無い	機密保護できないリスク	①	－
	刑事規制に違反するリスク	②	③
日本にない法律が,当該国に有る	機密保護できないリスク	④	－
	刑事規制に違反するリスク	⑤	⑥

表１において，①は，法による機密保護が日本と同じようには当該国で期待できないリスクで，例として不正競争防止法が挙げられる。

②③は，情報流出について日本の刑事規制に違反するリスクで，例として，②では輸出管理令（政令で定められた特定の地域の現地法人への特定な技術情報提供など)，③では不正競争防止法の刑事規制が挙げられる。

④は，技術情報の流出が法により強制されるリスクで，例として，中国の技術輸出管理条例が挙げられる。

⑤⑥は，情報流出に対する当該国に独特の刑事規制に違反するリスクで，例として，米国の経済スパイ防止法が挙げられる。

これらのリスクを回避するためには，まず，法を熟知すること，次に，法を遵守してもなお

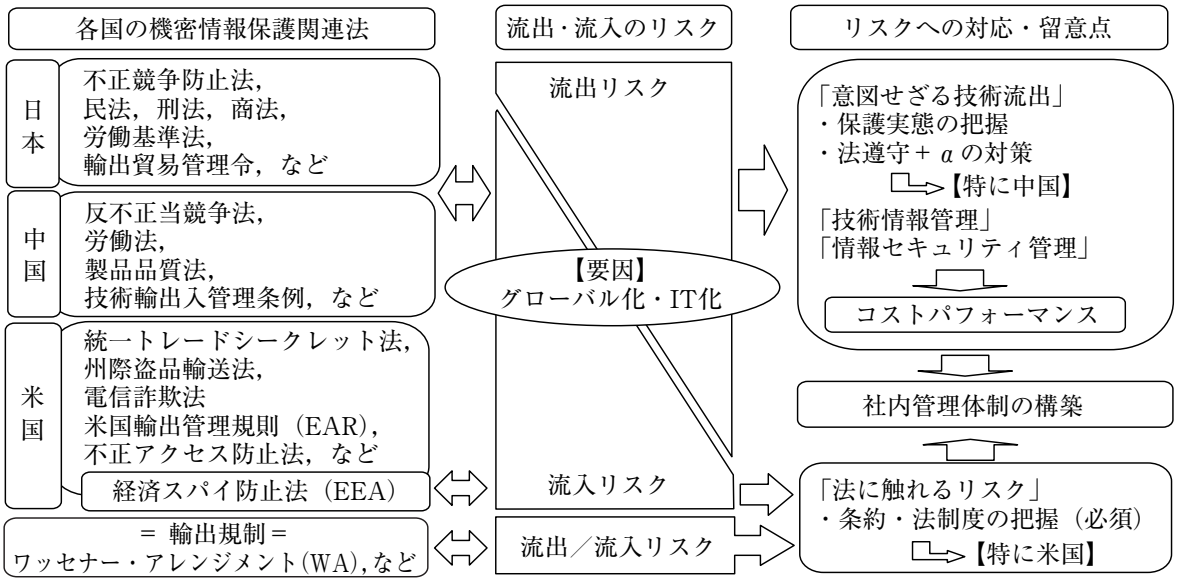


図１　技術情報管理におけるリスク概要図

生じる流出のリスクに対する手立てを講じること，の２段階のアクションが必要となる。

1．3　IT化に伴うリスク

インターネットに代表されるIT技術の飛躍的な発達により,ほとんどの情報は電子化され,国境さえも容易に超えて共有・流通し得るものとなり，しかも大量に集積することも二次加工することも非常に容易なものとなった。この「情報の共有性・流通性・集積性・加工性の高さ」は，特にグローバルに展開している企業にとっては，業務効率を飛躍的に高めるという多大な恩恵をもたらす一方で,情報の漏洩や消失,改竄などのリスクも飛躍的に高めるという深刻な副作用ももたらした。

以上の観点から模式的にまとめると図１のようになる。

2．法的リスク

2．1　日・米・中における法律の比較

(1) 日本における法律

日本では，従来は営業秘密そのものを直接保護する法律が無く，営業秘密侵害行為に対し，刑事的には営業秘密を化体する物品の窃盗罪などで取り締まり，民事的には不法行為として保護されてきた。

その後，営業秘密保護への国際的要請が高まり，特にTRIPS協定（1995年１月発効）締結の交渉項目に挙げられていたので，それを先取りする形で1990年に「不正競争防止法」が改正され，営業秘密の侵害行為に対し，差止請求,損害賠償請求などが認められ，民事的保護が図られるようになった。その際に，刑事罰の導入も検討されたが，当時は企業秘密，国家機密の漏洩を罰することに対する国民のアレルギーが強く，その導入が見送られた経緯がある。

ところが，2004年に「不正競争防止法の一部を改正する法律（法律第46号)」が施行され,営業秘密の侵害行為に対し，刑事罰が導入されることになり,営業秘密の取り扱いに関しては,特に注意が必要となった。

他に注目すべき法律として，外国為替及び外国貿易法（所謂「外為法」）があり，政令（外国為替及び輸出管理令）で定める特定技術の特定地域への提供は，政府の許可が必要である[1)]。また,2002年にキャッチオール規制が導入され,ほとんどの技術が特定の条件下で規制対象となった。表２に，日本の主な関連法規を示す。

(2) 米国における法律

米国では，日本と異なり，不正競争防止法が無く，従来は，技術情報は主に各州ごとの統一トレードシークレット法などで比較的緩やかに保護されてきた。他にも州際盗品輸送法，電信詐欺法等があるが，いずれも技術情報の侵害行為を直接規制するものではない。

ところが，1996年に連邦法である「経済スパイ防止法＜EEA（Economic Espionage Act)＞」が発効してからは，技術情報を含む営業秘密は厳しい刑事罰で手厚く保護されるようになった。また，法律の成り立ちから，同法は外国政府又は外国企業を対象としており，日系企業においては極めて危険な法律であるが，一般的に認識が乏しいように思われる。日系企業による営業秘密の窃盗は論外であるが，従業員を採用する時には注意が必要である。つまり，旧雇用者の営業秘密を聞き出すことなどは，明白な侵害行為となり，重い刑事罰の対象となる。

また，他にも日本には相当する法律が無く,気をつけるべき法律は「米国輸出管理規則＜EAR（Export Administration Regulations)＞」があり，米国からの技術流出に厳しい制限を加えている。公開前の特許情報も対象の例外ではなく，例えば，米国子会社でなされた発明を日本本社の知的財産部に相談することは違反とな

る。米国特許商標庁においては，特許技術情報の外国への移転が一定条件を満たせば，EARの適応を除外される規則を設けている。表3に米国の主な関連法規を示す。

表2　日本：機密情報関連の法律一覧

法律名称	条項，内容
不正競争防止法	第2条　第1項4～9号：営業秘密侵害行為類型，侵害者について規定。 ［民事的保護］3条　差止，4条　損害賠償，7条　信用回復措置。 ［刑事的保護］3年以下の懲役又は3百万円以下の罰金。
民法	709条　不法行為に対する損害賠償権。
労働基準法	89条　不法行為に対する損害賠償権。
商法	41条　支配人の義務，264条　取締役の競業避止。
刑法	134条　秘密漏示，235条　窃盗罪，247条　背任，253条　業務上横領，256条　盗品譲受。
外為法，外国為替及び輸出管理令	特定の国への特定技術の提供に関するもの。 刑事：5年以下の懲役又は役務価格の5倍以下の罰金。

表3　米国：機密情報関連の法律一覧

法律名称	条項，内容
経済スパイ防止法(EEA)＜連邦法＞	18 USC§1831～§1839，骨子は§1831及び§1832。1996年発効。非常に刑事的色彩の強い法律で，主に外国政府・企業を規制対象とした重い罰則あり。従業員から前雇用先の企業情報を入手した場合は，刑事罰が適用。
統一トレードシークレット法（UTSA）＜州法＞	40州程度が採用。刑事的制裁条項は含まない。
トレードシークレット窃盗に関し，刑事罰を含む州法＜州法＞	トレードシークレットを化体した有体財産の窃盗を規制。NJ州法モデルとNY州法モデルがある。
不正アクセス防止法＜連邦法＞	18 USC§1030(a)(4)。保護されているコンピュータへの不正アクセスを規制。
輸出管理規則（EAR）＜連邦法＞	15 CFR chapterⅦ, subchapter C。商品及び技術データの米国からの輸出及び再輸出を規制。米国でなされた発明を，米国以外の外国で出願する場合も規制対象。

表4　中国：機密情報関連の法律一覧

法律名称	条項，内容
反不正当競争法	10条：営業秘密の定義，侵害行為の定義。
	20条：侵害に対する損害賠償責任。
	25条：侵害に対する行政罰。
労働法	22条：労働契約において使用者の営業秘密保護に関する事項を約定できる。
	102条：労働者が違反した場合，損害賠償責任がある。
技術輸出入管理条例	11条：輸入制限技術を輸入する場合，関係機関に許可申請書類の提出が必要。
	25条：ライセンサーは提供した技術が完全で，誤りが無く，かつ有効であり，契約に定めた目標を達成できることを保証しなければならない。
	29条：契約には次に掲げる不当な制限を定めた条項を入れてはならない。 ①原材料・部品・製品又は設備の購入ルート。 ②ライセンシーによる改良技術の実施。

(3) 中国における法律

中国では，1993年から「反不正当競争法（不正競争防止法)」が存在し，「公知ではなく，権利者に経済的な利益をもたらすことができ，実用性を有し，かつ権利者が秘密保持措置を講じている技術情報及び営業情報」については，日本と同様に法律的な保護が与えられている。ところが,一般に営業秘密保持意識が希薄であり，自社の従業員及び退職者を介した営業秘密の流出が多く見られる[2),3),4)]。

「個人情報保護法」についても近々公布される予定である[5)]。草案によれば侵害者に対しては刑事罰が課せられるようになるため，今後の動向に注意を要する。

また,中国では「技術輸出入管理条例」により，技術を中国へ導入する際（特許ライセンスを含む）には種々の条件・制限が課されている[6)]。特に25条ライセンス技術の完全性の保証については，市場品質を維持するための技術情報をライセンシーへ教えざるを得ない内容となっている。表4に，中国の主な関連法規を示す。

2. 2 法的リスクに対する対策と留意点

(1) 米国における留意点

1）経済スパイ防止法（EEA）対策

まず法律を良く知ることが重要であり，その上で，一般的には以下の対策が考えられる。

① 会社の方針を従業員に明示し，その中にEEAに違反しないことを明記する。

② 従業員教育の中に,EEA防止対策を行う。

③ EEA違反防止対策として実行したことは，可能な限り書類に残す。刑事罰で有罪を避けるためには，犯罪の意図を否定する記録を残すことが肝要である。

特に注意すべきケースとして，従業員の採用があり，以下の対策が考えられる。

① 面接時，採用後に，旧雇用者の営業秘密を開示，入手，使用をしない。

② 新規採用者に旧雇用者の営業秘密について，守秘義務があることを明言して，違反しない旨契約を交わすか，誓約書を提出させる。

③ 旧雇用者との間で営業秘密を特定し，契約を結ぶ。

2）輸出管理規則（EAR）対策

特許公開前の技術情報の米国以外での開示に関しては，米国特許商標庁の独自の輸出規制規定（37 CFR Part 5）に従う必要がある。

(2) 中国における留意点

1）営業秘密の意識教育，規定設定

営業秘密が実際に流出した場合は，企業に甚大な被害を及ぼす恐れがあるので，自社の従業員へ営業秘密に関する常日頃からの教育を行い，営業秘密保持意識を高める努力を行う。また，労働契約や就業規則等で営業秘密に関する規定を盛り込んで，従業員等への心理的な拘束を与え，営業秘密漏洩に対する企業の強い姿勢を意識づける。なお，労働契約や就業規則等における営業秘密漏洩に関する規定は，実際に営業秘密漏洩が発生した場合にも，裁判等で有利な証拠として活用できる。

2）退職時への対応

特に注意すべき点として，従業員の退職時への対応において，以下が挙げられる。

① 労働契約等で秘密保持義務の期間を定めておく。期間は，可能な限り長期にするのが有利である。この場合，経済的補償を与えるのが一般的ではあるが，強制的な規定ではない。

② 労働法では労働者が労働契約を解除（退職）する場合，30日前までに使用者に通知しなければならないが，地域（例えば上海）によっては労働契約等により6ケ月前までに通知するように契約できる。このようにしておけば，その間，営業秘密を扱わない部署に配置転換する等により，最新の営業秘密の流出防止が可能である。

③ 労働法には競業規制に関する規定は無いが，地域（例えば上海）によっては労働契約等で競業規制を契約することができる。ただし，それに見合う経済補償が必要であり，競業規制の範囲を広く（曖昧に）したり，３年を超えるようにしてはならない。

３）合弁の相手先

合弁による中国への工場進出等にあたっては，その可否及び合弁相手先を事前に十分検討すべきである。「技術輸出入管理条例」第25条により，製造品質を維持するための「製造ノウハウ等は合弁相手先へ教えざるを得ない」と考える。対策として，肝となる部品は日本で製造して現地で組み込む方法も考えられるが，その行為自体が中国の関連法規に抵触する恐れもあるので，現地弁護士等に十分確認をする必要がある。

また,合弁による工場進出等を決定した後も，「必要以上の技術情報を開示しない」ように現場での管理を徹底することが肝要である。とかく，現場の日本人は良い製品を製造しようと必要以上の技術情報を合弁相手先に教えてしまうものである。そのようなことが無いよう，技術情報開示基準の策定・監視を日本において行う必要がある。

3． IT化に伴うリスク

3. 1　IT化とリスク要因

IT化に関連した技術情報の漏洩が表面化した事例は非常に少ない[7]。しかし，2005年４月１日の個人情報保護法の本格施行を前にして，個人情報の漏洩に関しては，その社会的影響の大きさを反映して多数の事例（表５）が報道されている[8]。個人情報，技術情報の差異はあるものの，情報の漏洩という観点では，情報漏洩のルートなどは両者に共通と考えられ，特徴やリスク要因も同様に分析できるであろう。

表５　情報漏洩の事例

漏洩ルートなど（報道年月）
(1) ネットワークを通じた漏洩 ① メール誤送信：県立科学館イベント登録者の氏名・メールアドレス約300人（2004－12） ② 不正アクセス：学習塾の全国模試を受験した小学生ら個人情報　約18万人（2004－８）
(2) 記録媒体の盗難・紛失 ① 小型記録媒体（USBフラッシュメモリ）紛失：人材派遣会社の高速データ通信サービス申込客の個人情報　約２千人（2004－７） ② CD－R流出：放送局の懸賞クイズ応募者の氏名・住所など個人情報　約１万人（2004－６）
(3) データの不正持出 ① ファイルを自宅のパソコンにメール送信：自動車会社の中古車保証サービス加入者の氏名・住所・登録番号　約４万人（2004－８） ② サーバからダウンロード：石油会社カード会員の個人情報　92万人（2004－６）
(4) 端末機器の盗難・紛失 ① ガスメータ検針用の携帯情報端末機の盗難：ガス会社の顧客情報500人（2005－２） ② ノートパソコンの盗難：住宅販売会社の顧客情報　約36万件（2004－６）

IT化を技術情報のデジタル化，電子化という観点でとらえた特徴と，更にその電子化された情報がネットワークを通じて伝送され得ることに伴う特徴，そして，これらの特徴から結果として発生するリスク要因を以下に示す。IT化の時代には，技術情報が紙に固定された時代に比較して，様々な新たな情報漏洩リスクが生まれていることが理解されよう。特に，ネットワーク化は，意図する／意図しないにかかわらず，情報がグローバルに流通し得ることを意味し，今までの発想では対応できないことを認識することが重要である。また，これらのリスク要因を考慮した情報管理の必要性が高まっていると言えよう。

(1) 電子情報の特徴

従来の暗黙知としてのノウハウが，技術情報

として資料化され，更には当該資料が電子化されることに伴い，以下のような特徴が生まれてきている。

① 複製による品質劣化がない。紙の資料などのアナログ情報に対して，電子化されたデジタル情報は，複製による品質劣化が無いため，何回複製しても，原本と同じ情報が保存される。

② 簡単に複製ができる。膨大な紙の資料を複写機で複写する場合に比較して，電子情報の複写（ファイル・コピー）は，簡単にかつ短時間で実行可能である。

③ 記録媒体が多様で集積度が高い。FD，CD－ROM，HD，フラッシュメモリなど，多種多様な小型・軽量・大容量の記録媒体が普及しており，膨大な情報であっても，小型・大容量の媒体に記録して容易に持ち歩くことが可能になった。

④ 管理を徹底することが難しい。機器，媒体，アクセス管理などの各要素を漏れなく管理する必要があり，紙の資料に比較して一般的に管理を徹底することが煩わしく，難しい。

⑤ 修正・加工・削除が容易である。電子化された情報は，部分的な修正をきれいにかつ容易に行うことが可能であり，また，データ分析などの加工，削除・抹消も容易である。

⑥ 意図しない重要な情報が蓄積されることがある。装置のセキュリティやメンテナンスなどの管理情報が，情報収集者の意図とは別の視点で加工することにより，重大な機密情報に変化することがある。

(2) ネットワーク化の特徴

電子化された資料が，ネットワークに接続されたサーバ，パソコンなどに保管されると，記録媒体の移動を伴わず，情報だけが伝達されるため，更に以下のような特徴が生まれる。

① 高速・大容量の伝送が可能になる。接続するネットワークに高速回線を利用することで，膨大な情報を瞬時に伝達することが可能になる。

② 保管場所以外からの遠隔アクセスが可能になる。情報が保管されている場所から離れた場所から，情報の閲覧，複写，取り出しなどを容易に行うことができる。

③ 簡単に送達・転送が可能になる。複写等を行った情報を，ネットワークを通じて，簡単に送達・転送することが可能である。

④ システム上のセキュリティの欠陥を完全に除去し難い。電子化された情報の流出防止のために，セキュリティ・システムを構築したとしても，欠陥による意図せざる情報流出，欠陥をついての不正アクセスなどの危険性があり，その欠陥を完全に除去することは困難である。

(3) リスク要因の考察

電子情報及びネットワーク化の特徴の結果として，技術情報管理上は，以下のようなリスクが生まれている。

① 膨大な情報の複製が瞬時に可能である。技術情報をLAN/WANを介してネットワークに接続されたサーバに保存し，多数のパソコンで当該技術情報を共同利用するような場合，サーバからパソコンに重要な技術情報を瞬時に複写することが可能であり，技術情報の保管場所に立ち入ることなく技術情報の流出の恐れがある。

② 二次流出が起こり易い。一旦，技術情報が流出すると，それがネットワークを通じて制約無しにダウンロード・転送が際限なく繰り返され，回収は困難になる。また，意図した転送の場合であっても，メール送信の誤操作による事件が多発している中で，宛先を誤った場合には，意図せざる流出になる危険性もある。

③ 記録媒体の紛失・盗難により膨大な情報の流出が起こり易い。膨大な情報であっても，小型・大容量の媒体に記録して容易に持ち歩く

ことが可能であり，また，情報を記憶したノートパソコンの携帯も日常化している。これらが，盗難にあったり，置き忘れなどにより紛失した場合は，情報流出につながることになる。

④ 情報流出が目立たない。紙の資料の場合，複写のための持ち出し等では痕跡が残り得るが，痕跡を残さずに複製することや，複製の痕跡の抹消が可能であり，複製・流出に気付き難い。

⑤ 情報の加工・流用が容易である。電子化された情報は，内容の検索・分類・分析などの加工は容易であり，また，複写による品質劣化が無く，部分の取り出しや修正も容易であるため，単なる複写だけではなく，二次利用としての流用を効率的かつ価値ある形態で可能である。

⑥ 情報の改竄・削除が容易に行える。電子化された情報を保存しているサーバ，パソコンなどに，ネットワークを通じて不正にアクセスすることにより，情報内容を改竄したり，情報そのものを完全に削除・抹消することは，専門家であれば容易であり，また，災害などによりサーバ，パソコンが損傷を受けることによっても，情報が消失する危険性がある。

⑦ 国境を越えて情報が流通する。物を通じた国際流通の場合には税関などの規制があるが，ネットワークを通じた情報の流通の場合には，容易に国境を越えてしまい，情報の移動を規制する法律に抵触する可能性がある。

3. 2 情報共有化と選別管理

(1) 情報の共有化による一括管理

ネットワークがグローバル展開されることで，情報流出リスクは国境を越えた地球規模リスクまで拡大する危険性を有している，との認識が必要である。このような状況下，社内の担当部署が個別に又は個人で情報管理していては，管理手法・体制や管理レベルに格差が生じ，リスク要因に対応した安全かつ確実な情報管理を行うことは極めて困難だと言わざるを得ない。

そこで，情報をデータベース化（共有化）して一括した管理下に置くことにより，統一されたレベルで情報管理を行うことが可能となる。これによってリスク要因に対応した共通的管理が可能となる。しかし，情報を共有化することは，一旦情報が流出すると，流用量が一度に大

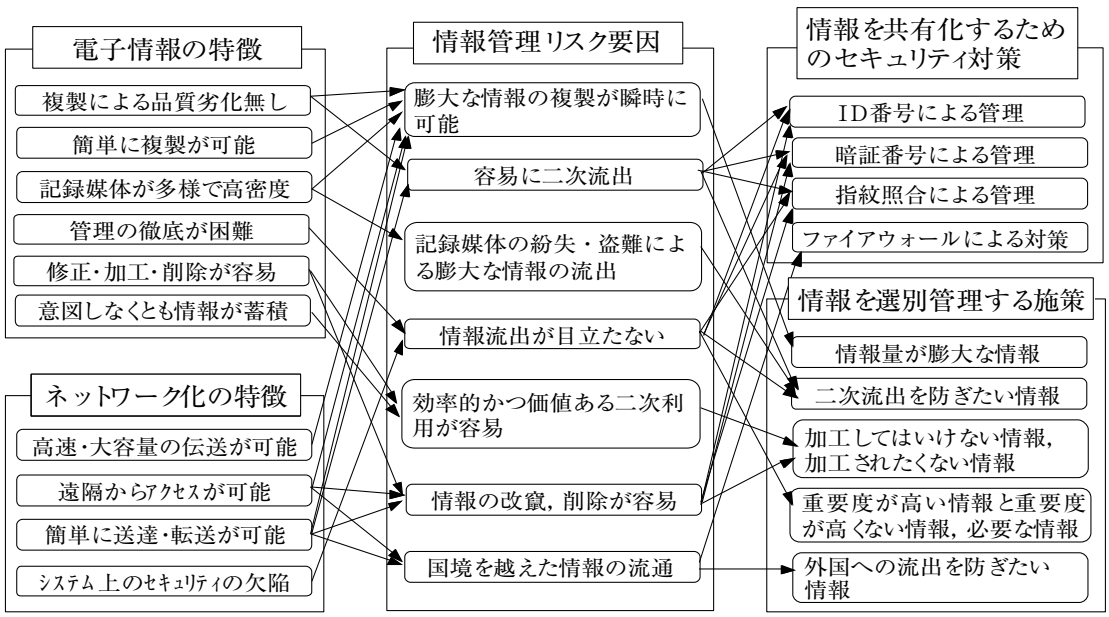


図2 IT化によるリスクと対策

量になされる危険性を持ち合わせているため，情報アクセスする段階で高度なセキュリティ対策が必要となる[9),10)]。一方，共有化された情報を情報の種類や重要度に応じた一定の条件下で，選別して情報を管理することにより，情報の性質に応じて安全に情報管理することが可能となる。

(2) 情報共有化するためのセキュリティ対策

① ID番号による管理：データベースに入る時に，該当データベースのID番号や入力者のID番号を入力させて照合することで，使用者をアクセス権がある限定された者に制限できるとともに，そのID番号を記憶して履歴管理することで使用者を管理できる。

② 暗証番号による管理：使用する際に暗証番号の入力を課すことで，暗証番号を知る特定の者のみが,データベースの使用が可能となる。

③ 指紋等照合による管理：データベースを使用する際に指紋等の個人を識別可能な情報の照合を行うことで，指紋等の登録者のみが使用できるようにするとともに，指紋の照合履歴を記憶することで使用者を管理できる。

④ ファイアウォールによる対策：社内と社外との境界（例えばWebサーバ）にファイアウォールを介在させることで，外部からの不正なアクセスに対して対応（不正侵入の防止）できる。

(3) 情報を選別管理する施策

① 情報量が膨大な情報：一度のアクセスでダウンロードできる情報量を制限することで，容易にダウンロードできないようにする。

② 二次流出を防ぎたい情報：ダウンロードした情報の再複製ができないような対応をしておき，万一流出した情報の拡散を防止する。又は，ダウンロードそのものを禁止しておく。

③ 加工してはいけない情報，加工されたくない情報：ダウンロードした情報が容易に加工できないよう，例えばPDF化しておく。

④ 重要度が高い情報と重要度が高くない情報，必要な情報：情報の重要度に応じたアクセス権を設定する。あるいは必要な情報のみに対してアクセス権を与えるようにし，不必要な情報へのアクセスを拒否する。

⑤ 外国への流出を防ぎたい情報：外国からのアクセスを許可しない。あるいは，週末や深夜に外国からの不正アクセスが多い実態への対応として,時間帯や曜日で制限する方法もある。

「情報を共有化するためのセキュリティ対策」と「情報を選別管理する施策」について，リスク要因に関連させた形で図２に示す。

3. 3 コストパフォーマンスを考慮した技術情報管理

(1) IT化のメリットとリスク

一般的に，IT化（電子化・ネットワーク化）に伴うリスクへの対策のためには，多大な投資が必要となる。また，IT化によるリスクとは，実はメリットと表裏一体のものであって不可分のものであるため（図３），セキュリティを高めれば高めるほどIT化によるメリットが薄れていく。例えば，アクセス管理が厳密になされ，例外が認められずに必要な情報が利用できなくなる，パスワードが厳密に管理されるようになったため，毎回の操作が面倒になる，などの状況を考えるとわかり易い。

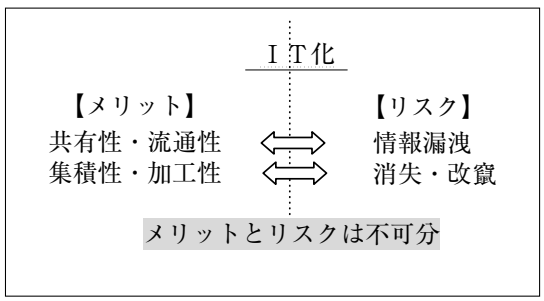


図３　IT化のメリットとリスク

従って，IT化に伴うリスク対策にあたって，注意すべき点は，次の２点である。

① 技術情報の価値を良く把握し，漏洩による損失の大きさと対策のための投資のバランスに注意すること。

② IT化により得られるメリットをなるべく阻害しないように情報の活用と漏洩のリスクとのバランスを考慮すること。

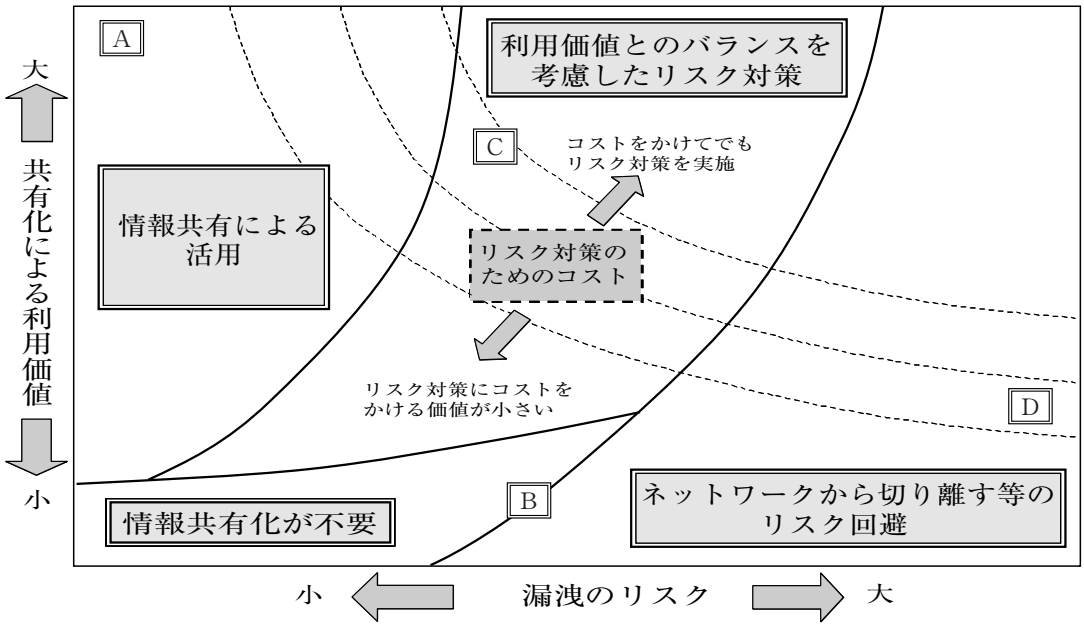
(2) 情報価値の把握

情報の価値の把握にあたっては，各種の知財価値評価の考え方が参考となるかもしれない。例えば，定性的なランク付けを行うやり方としての特許庁の特許評価指標（試案）や特許評価指標（技術移転版）や，定量的な評価としての，コスト・アプローチ法，DCF法，リアル・オプション法などである。どの評価手法を用いるかについては，一面的な評価ではなく，最も有効に利用するための選択肢を幾つか検討し，評価目的ごとに使い分けるべきである。

また，情報の価値は永続的価値というものではなく，時間とともに変化するものであり，寿命を考慮に入れて，定期的に見直されるべきである。更に，個別の技術情報ごとに評価するのではなく，基本技術の重要性と周辺技術の整備度といった事業化の容易性も考慮して，プロジェクト単位で群としても評価する必要がある。

(3) 潜在的に負の価値を有する情報

ところで，情報の中には，自社にとって利益の源泉となるような価値を有するものではないが,漏洩すると多大な損失を蒙る性質の情報や，情報自体が自社では思いもよらぬ使われ方をされた結果，意図しない技術流出につながる性質



事例Ａ：社内電話番号表：データの価値自体は低いが，共有化による利用価値は高い。漏洩時の損害は小さいが，データ量の増加によって大きくなる。
事例Ｂ：社内の１部門のみに必要な技術情報：データの価値自体は中位，共有化による利用価値は低い。漏洩時の損害は中位。
事例Ｃ：社内の横断的プロジェクトに必要な情報：データの価値自体は中位，共有化による利用価値も中位。漏洩時の損害は中位。
事例Ｄ：社内のコアコンピタンスに関する技術情報：データの価値自体は大きいし，共有化による利用価値は小さい。漏洩時の損害は大きい。

図４　情報の利用価値とリスク対策

の情報（潜在的に負の価値を有する情報）も存在する点に注意が必要である。

例えば，技術情報とは異なるが，漏洩により社会的信用を大きく失墜させる顧客リストなどの情報や，自社の設備に対し，メンテナンス業者が収集する設備の運転情報（この場合，自社設備の稼動状況が他社に漏洩するというリスクが存在する）などである。従って，価値評価にあたっては，単に「自社にとって価値をもつ情報」以外に，このような「潜在的に負の価値を有する情報」にも目を向けるべきである。

(4) IT化リスクと投資バランス

一方，情報を守るための投資について考えてみると，管理システム構築にかかるリソースは様々である。コストとして考えておかなければならないのは，システムにかかる初期投資以外に，メンテナンス要員の増員により増加する人件費や，今後のシステム維持管理のための運用にかかる継続的な管理コスト，将来システム更新時に必要となるコストなどがある。このように，IT化によるリスクへの対策のためには，多大な投資が必要であるので，漏洩時の損失の大きさと対策のための投資のバランスに注意して，投資にメリハリをつけることが重要である。

(5) 情報活用と漏洩リスクのバランス

コストパフォーマンスを考慮して技術情報管理を進めるためには，情報の活用と漏洩のリスクとのバランスを取ることが重要である。

全ての情報を共有化して一元的に管理することができれば利便性は高まるが，その分漏洩リスクは増すので，情報漏洩リスクへの対策の基本は情報の流通制限であるとも言える。そこで，図4に示すように，漏洩時のリスクの大小，情報の潜在的利用価値の大小により，管理の仕方を考察する。

例えば，漏洩時の被害が甚大なものについて

表6　検討する際の留意点

	留意点	概要
活用と管理	情報共有化による情報活用	情報の利用価値を十分に活かすには，必要とする者が必要とする時に，容易に利用できる状態にしておく。
	管理強化のメリットとデメリット	管理強化により共有化を阻害することがあるので，対策を講じる場合は，漏洩リスク低減効果と共有化阻害損失のバランスを考慮する。
リスク対策	情報一括管理による確実な管理	情報活用を図るグループ内では，対策漏れが無いよう，管理水準を合せるために，一括管理が重要である。
	地域（国）ごとの情報分離	法的リスクを考慮して，例えば，海外特に米国のグループ企業のノウハウ技術情報は米国内でしか閲覧できないようにして，情報が国外に流出しないような対策を行う。
	情報漏洩が前提	対策に完璧は無いので，重要なものほど最悪の事態に備える。
	利用価値とリスクに対応した選別管理	情報の利用価値，リスクの大きさに応じた管理が効率的にできるように，情報の選別管理を行う。
リスク見極め	情報群でのリスク分析	情報の選別管理のため，利用価値に応じて管理水準を決めるため，例えば厳重管理の情報とそうでない情報を区別する。
	許容できるリスクと必要な管理水準	漏洩のリスクが許容できる程度の対策が必要であり，過剰な投資は無駄。リスクに対応した選別管理では，不必要となった情報，リスクの高い情報を消去，又はシステムから切り離し厳重保管して，無駄なリスクを負わないことも考慮に入れる。
見直し	価値評価の適宜実施	技術情報の価値評価が容易に行えないと，利用価値の見直しが難しくなる。
	柔軟な管理水準の見直し	価値評価の結果に応じて，管理水準の見直しができるように考慮する。

は，流出防止に多大の費用をかけるより先に，情報の暗号化により流出した情報を解読できなくすることで漏洩リスクを低減するといった対策を行う一方で，予防対策のために必要な投資に見合うメリットが期待できない情報については，ネットワークから切り離して別室に鍵をかけて管理したり，余計な費用をかけて電子化せずに紙のままで管理するといったことも考えられる。

(6) IT化リスク対策を検討する際の留意点

以上，IT化に伴うリスク対策にあたっては，情報管理の目的を明確にし，必要な所に過不足の無い最適な管理手法を用いることが大切である。

また，情報のもつ意味合いは変化するものであり，その変化に応じた対策がなされているかにも気を配る必要がある。IT化に伴うリスク対策を検討する際の留意点を表6に示す。

4. 終わりに

「米国＝知恵づくり，中国＝モノづくり，日本＝試作づくり」という図式が浸透している。技術流出は，ゼロにするのを目指すのでなく，ある程度の流出は許容せざるを得ず，流出に伴うリスクと，流出防止に対するコストのバランスを考慮した施策が肝要となる。ノウハウを出さない工夫と，出た後の対応も重要である。

グローバル技術情報管理に関しては，確実な知識として体系化されていない面が多いため，議論収束が難航したが，過去の論説を調査した結果，特に次の2点に着目して議論した。

① 日本・米国・中国の法的リスクでは，3国それぞれの法律に対応した論説は多いが，3国の違いを対比して，留意点を総括した論説がほとんど無い。

② IT化リスクでは，個人情報保護法に関連したセキュリティ対策の論説は多いが，グローバル技術情報管理の視点での論説が少ない。

グローバル経営においては，日本への流入リスクや「日本にあるが中国にない」又は「日本にないが米国にある」法的リスクに対して，注意が必要である。情報管理は「業務効率とのトレードオフが課題」であり，コストパフォーマンスにより，取組み度合いが左右される。情報が漏洩して会社が潰れるのであれば，きちんと実行することになる。

最後に，2004年度フェアトレード委員会の竹本委員長（サントリー）と西川委員（凸版印刷）とは，課題検討の方向性を中心に意見交換を行った。謝意を表したい。

なお，本稿は次の2004年度当委員会メンバーが担当した：佐藤修（小委員長，三菱電機），永吉隆司（小委員長補佐，小松製作所），奥田浩司（ポリプラスチックス），小原清隆（日立建機），金村弘（本田技研工業），島貫義太郎（NTTドコモ），霜田進（インフォコム），白髪信一（マツダ），高野孝一（日本電気），田尻浩之（矢崎総業），船渡良（三菱レイヨン），森島浩（東芝テック），薮田昌明（大日本スクリーン製造）。

注　記

1) ワッセナー・アレンジメント（WA）など。経産省の安全保証貿易管理HPが参考となる。
http://www.meti.go.jp/policy/anpo/index.html
2) 国際商事法務 Vol.32，No.2（2004），中国における日系企業の労働契約に秘密保持条項の設置。
3) 広東省羅定市林生化工廠，劉顕馳及び湖南省株洲選鉱薬剤廠の営業秘密侵害紛争上訴事件。出典：人民法院報
http://www.jetro-pkip.org/panli/190305.htm
4) 臨沂市工業品公司の営業秘密侵害をめぐる紛争。出典：最高人民法院民事判決書（1999）知終字第17号
http://www.jetro-pkip.org/panli/190306.htm
5) 2005.1.19『北京晨報』

6) パテント，2002, Vol.55, No.10中国技術輸出入管理条例の改正についての問答

7) IT化に関連した技術情報の漏洩が裁判で争われた例として，以下の事件が挙げられる。
H15.2.27大阪地裁　平成13(ワ)10308等 不正競争 民事訴訟事件判決［不正に取得した電子データを利用したセラミックコンデンサー積層機，印刷機の製造，販売の差止を請求］

8) 月刊情報セキュリティ「情報漏えい事故DB」
http://www.monthlysec.net/
機密情報漏洩に関する事例と対策の状況については，以下の雑誌記事などに紹介されている。
日経コンピュータ2004年11月15日号 特集「セキュリティネットワーク100の新常識」日経BP社。
日経ビジネス2005年2月28日号 特集「なぜ漏れる機密情報」日経BP社。

9) 情報セキュリティ管理に関する国際標準は，ISO/IEC17799や日本情報処理開発協会によるISMS（Information Security Management System）など。

10) 「情報セキュリティポリシーに関するガイドライン」（内閣官房情報セキュリティ対策推進室）や，「2003年度情報セキュリティインシデントに関する調査報告書」（日本ネットワークセキュリティ協会）など。

参考文献（「知財管理」誌から抜粋）

(1) 知財管理第2委員会3小委員会「営業秘密と知的財産管理」Vol.54, No.10, 2004
(2) 知財管理第2委員会3小委員会「中国におけるR&D活動に伴う知的財産管理」Vol.53, No.6, 2003
(3) フェアトレード委員会「秘密情報のマネージメント」Vol.54, No.3, 2004
(4) フェアトレード委員会「不正競争防止法本格活用の時代―21世紀における不正競争行為の企業内管理のあり方―」Vol.48, No.11, 1998
(5) 岡本清秀（オムロン）「企業の多国籍化に伴う知的財産戦略と留意点」Vol.50, No.1, 2000
(6) 張立岩，宋和成「中国における知的財産マネージメントの留意点」Vol.53, No.2, 2003
(7) 魏啓学（中国弁護士）「注目される中国の技術輸出入管理条例」Vol.52, No.8, 2002
(8) 梅田さゆり（NY州弁護士）「米国子会社の技術開発への日本の親会社の関与と米国輸出管理規制及び特許法上の問題点」Vol.50, No.4, 2000

（原稿受領日　2005年4月6日）