

# 賠償責任と、無責任と、抑止

## Liability, Irresponsibility, and Deterrent

May 22, 2007

中央大学教授(総合政策学部)  
米国弁護士(ニューヨーク州)

平野 晋

# 不法行為法 (torts) の主要目的

① 「事故抑止」(deterrent)

② 「損害賠償」(compensation)

その他: 「謝罪」(apology) --- 認め、償い、再発防止策を採る、etc. / 「矯正的正義」(corrective justice)

- ②も重要だけれども、これは「事後的」(*ex post*)な問題。
- ①はそもそも事故の発生自体を「事前的」(*ex ante*)に抑えるので、更に重要。
- なお事前的抑止の方法には不法行為法に頼るだけでなく、行政法規制や、技術基準 (*e.g.*, JIS) 等による「行為規範」(rules for players / std. of conducts) の明確化も有効。

# 「効率性」と不法行為法

社会の殆どの資源は「稀少」(scarce)なので...

- 「事故費用」を最小にすべきであり、かつ
- 「事故防止費用」も最小にすべきであるから、

「事故費用+事故防止費用」の総和の極小化を、不法行為法は目指すべき。

Prof. Guido Calabresi.

CBA: Cost-Benefit Analysis

$B < PL$  (Hand formula; B=Burden, P=Probability,  
L=gravity of Loss)

# インターネットの問題

- 「安心・安全」の欠如。
  - *E.g.*, spam, virus, worm, malware, Trojan Horse, phishing, spyware, backdoor, DOS attack, etc. (「cyber-pest」)
- 「外部不経済」の蔓延。
  - *E.g.*, 責任を「内部化」しない環境汚染工場。→過剰生産。
- 望ましくないソフトウェアの外部からの侵入やcracking。
  - 特徴： 張本人(以下「mal-feasor」と言う)が責任回避。  
何故ならば、...
    - ①同定化困難(∴匿名性anonymity) and/or
    - ②無資力。
- 加えて、侵入・蔓延を許してしまった関係者も責任を課されない。  
∴防止策がsub-optimalなレベルに止まったまま。
- すなわち、irresponsible(無責任)な準無法地帯?!

# 対策#1(直接責任)

- 張本人(malfeasors)にこそ責任を課すこと(=direct liability)こそが本筋。
- その為には、まずmalfeasorsが発見されなければならない。
- すなわち、匿名性を排除・制限することが必要。
- しかし、これが困難・不完全な場合に「良化」(better off)を図る為には、次善の策として、「間接責任」(indirect liability)が提言されている。

# 対策#2(間接責任)

間接責任とは...

- *E.g.*, 運転者に飲酒を許容した酒場のオーナーが飲酒運転事故発生の責任を負う。(望ましくない活動により生じる「社会的費用」の「内部化」)  
→ 以降、酒場オーナーと同じ立場の者達は、運転者に飲酒させないような防止策を実行する。  
→ 飲酒事故が減少する。(望ましくない活動の「抑止」)
- *E.g.*, 従業員が業務執行中に第三者を加害した責任を雇用主が負う。(使用者責任: *repondeat superior* = “let the master answer” / 代位責任 *vicarious liability*)  
→ 以降、雇用主と同じ立場の者達は、加害しないような従業員を雇用・業務執行させるような防止策を実行する。  
→ 業務上の第三者への事故が減少する。
- その他: 自動車所有者、attractive nuisance、ラジオ番組、銃の販売、etc.

「EFR」の法理: encourage free radicals

# IP化時代の間接責任

- 匿名性等により、malfeasorに責任を課せられないのであれば、間接責任によって防止措置の向上を奨励すべき。
- 間接責任を課されるべき者とは、効率的に事故を防止でき得る者。すなわち、「最安価事故回避者」(cheapest cost avoider)や「ベスト・リスク・ミニマイザー」(the best [またはbetter] risk minimizer)と呼ばれる関係者(以下「BRM」と言う)。
- リスクへの「管理」(control)をより良く及ぼし得る者。
- すなわち、malfeasorを発見し、抑止し、または彼等に影響を与えることのできる者、または、防止策をより安価・容易に採り得る者。
- 誰がBRMであるのかについては、事業者である場合もあれば、利用者(消費者)の場合もある。事業者の中でも、端末メーカーや、ソフトウェア・ベンダや、ISP等、の場合もある。  
→事案毎に異なる。→責任基準明確化の為には類型化要。
  - E.g., ワクチン注射による感染予防。
- 倫理的にも、「管理」をより良く及ぼし得る者は、回避策を採らなかったことについて非難されるべき(blameworthy)である。(義務の射程＝予見可能性、回避可能性)。かつ、利益を享受する参加者はirresponsibleであってはならないはず。

# 不法行為法による抑止策への懸念

- 司法制度インフラの機能不全。
  - 法曹数(弁護士、判事)が少な過ぎて「法化」社会に対応していない。
- 実定法も、IP通信世界に於ける責任分野は未発達。
  - 責任要件(具体的義務・違反、誰がBRMか、等)が曖昧。
  - 手続法も不完全(個人が権利実現できるとは到底思われぬ)。
  - 工学技術的にも真実発見への障害あり(E.g., anonymity/spoofing、ログ保存)。
- 現状のままでは抑止効果を期待できない。
  - 「運用費用」(administrative cost)が高額過ぎる。
    - 所詮は権利実現されないと見下すからirresponsibleになる。
    - 規範(rule)が不明確だから、争いが助長され、協力・取引が促進されない。／ruleが不明確だと、「rule of law」とは言い難い。
  - malfeasantのみならず、彼等以外のBRMも「事実上の免責」(de facto immunity)が付与されている。
    - sub-optimalな防止策しか実現されていない。
    - 外部不経済が放置されている。／ 救済が実現されていない。



# 司法制度不備への対策案

以下のような対策案の策定を検討することにより、外部不経済を極小化する。(併せて賠償実現等も促進する。)

- 防止策として「事後的」紛争処理のみに委ねるのではなく、「事前的」な行政規制・認証制度や、「協力」解を促す情報開示・情報共有制度を構築して防止効果を上げる。
  - ∵ *E.g.*, 「情報の非対称性」等により、消費者によるセキュリティの適正評価が困難な為に品質がsub-optimalレベルに止まり(lemon mkt.)、かつ、消費者自身もセキュリティの重要性を過小評価しがち。  
*E.g.*, マルチ・ベンダなソフトウェアを消費者がインストールした為に生じる機能不全・誤作動を回避する為には多様な関係者相互の協力が不可欠であるけれども、各プレイヤーは自己利益を優先する為に社会的に最適な解に至らず「外部不経済」が生じ得る。
- 司法インフラの不備を、IP化時代の紛争という分野に特化して改善する。
  - ∵ 全ての司法インフラの改善は非現実的。  
*E.g.*, 間接責任(義務の射程、誰がBRMなのか、等)の明確化・類型化や、JIS規格のような外部「行為規範」(rules for players / std. of conduct)の構築による責任要件の明確化や、ADR制度の構築による「使える手続」の実現、等々。
- 更なる「劇薬」もあり得る。
  - *E.g.*, 刑事責任の強化。(日本は民事司法の不備が刑事司法の拡張を招いている。)
  - 但、活動の自由をできるだけ維持するという原則を要考慮(lawyer joke: 「軍隊が増え過ぎると『平和』が減り、弁護士が増え過ぎると『平穩』が減り、警察が増え過ぎると『〇〇』が減る?!」)

# 対策案:「安心・安全」な選択肢

- 「インターネット+PC」とは異なる多様な選択肢の構築・提供により、「安心・安全」な役務も利用可能にすべき。
  - ∴ より広く大多数なnovice/lay-person利用者(消費者)の期待にも応えるべき。
    - 以下の役務に対し、利用者(消費者)はfree radicalsの侵入を許す世界を期待しているとは思われない。--- 911系緊急通報(110番, 119番, etc.) / 電力網 / ITS / 遠隔医療 / IP-NW家電 / 電子商取引 / 緊急通報以外の(音声)黒電話 / その他。  
→ 中央集権的top-downなセキュリティの維持が望まれる世界。(cyber-governance論@cyber-law)
- 何が「公正」なのかの評価は、「所有効果」「損失回避」「現状執着偏見」等の影響で決まる。
  - ∴ e.g., spamが来ない黒電話への期待は守るのが公正。

# digital divideの回避

- digital divideの回避要。worse off(悪化)回避要。
  - ∴より広く多数のnovice/lay-personが利用するので、[quasi-] learned userのみを対象にした「自己責任」偏重な「インターネット+PC」的制度世界は利用者の現実には合わない。
- 「パターナリズム」と「自己責任」の最適なバランス要。
  - 新たにより広くnovice/lay-personが利用する世界になるという前提で、適切な自助努力をdiscourageさせず、自決権と保護主義との間の最適分岐点を探るべきである。
  - 類型化、行為基準の明確化。

# 「自己責任」と考慮諸要素

- 「自己責任」とは、自己自身が決定することで自己利益を促進／自決権、選択の自由、自律、等。
- その障害は、「情報の非対称性」／「限定合理性」／「リスクの過少評価」、等。→ pro-paternalism.
- 他方、「損失軽減義務」「自助努力」(利用者がBRMな場合等) → pro-personal responsibility.
- 如何なる場合に自己責任となるかを探るべき。→ 類型化・行為規範の明確化。→ 協力の促進。
  - 利用者(消費者)による「自助努力」にどれだけの成果を期待できるか？
    - PCユーザ(learned user) v. 音声(黒)電話利用者(一般消費者)／電力網利用者(一般消費者)／IT S利用者(一般消費者)／NW家電利用者(一般消費者)／ゲーム利用者(ゲーム・ユーザ)／...
    - digital divideの回避要。/ worse off(悪化)回避要。
- 今後の課題例: 「クリックラップ(click-wrap)契約」
  - See 総務省「ユビキタスネット社会の制度問題検討会 報告書 ~活力と創造性を生かし『安心』を提供する枠組みづくりを目指して~」7~8頁(平成18年9月)。

# 非対称性パターンリズム

初期値(default)をパターンリスティックに設定しつつ、オプト・アウトを許容して自決権を担保する。

- より広範囲で大多数のnovice/lay-personたる利用者(消費者)向けには「パターンリズム」な役務を提供。→ 自己利益の他者による保護。  
*E.g., maintenance free、単純機能、高security、etc.*
- 少数のlearned users向けには、上の役務からopt outする権利を付与して、「自己責任」に基づく役務を提供。→ 自決権、自律権等の尊重。  
*E.g., maintenanceの自己管理、高機能、低security、低価格、etc.*

# 警告/指示 v. 設計

- 警告/指示とは...
  - 危険の存在を知らせる、回避方法を知らせる、回避できない危険の場合は引き受けるか否かの自決権を付与する (informed consent)。
- 情報提供 (警告/指示) のみで十分か、または設計的 (paternalistic) に安全性を確保すべきか？
  - インターネット+PCの世界でも、安全性向上策 (e.g., 添付ファイルを開くな、ワクチンを更新しろ、etc.) を警告・指示しても、守らない利用者 (消費者) が多い。ましてや novice/lay-person が大多数を占める世界に於いておや....
  - $B < PL$  ならば設計に組み込むべき。
- 明白な危険は原則として警告不要。しかし...
  - 何が「明白」かは、learned user と novice/lay-person で異なる。  
E.g., 無線LANは傍受が容易という事実。
  - 明白な危険でも  $B < PL$  ならば設計によって回避すべき。