愛知淑徳大学論集　－コミュニケーション学部篇－　第4号　2003　35－48

コンピュータ倫理のカテゴリー分析

梅　田　敏　文*1

1. はじめに

コンピュータ倫理の個別の論点を洗い出し，論点を関係づける基準を設定してグループ化を試みることは，コンピュータ倫理の内容を総合的に理解するひとつのアプローチである。このアプローチを活用して筆者は，知的財産権，プライバシー，プロフェッショナル倫理，コンピュータ犯罪という4つのカテゴリーを定義した。また，そこに諸論点を集約してカテゴリー相互の関係を論じ，コンピュータ倫理は，法律や技術，一般倫理と密接に関係しつつ，それらとのダイナミックな関係の中で捉えられる課題であることを検討した[1]。

当検討後におけるひとつの課題は，この4つのカテゴリーが，現実に発生している現象，規範，法律上の権利，技術開発など多岐にわたる論点をふくみ，その用語の意味する内容のレベル，用語が持つ価値などが同一のベクトルになく，錯綜して盛り込まれている点であった。

本稿ではこの点に対処し，さらにコンピュータ倫理を総合的に理解する論考をすすめて，コンピュータ倫理の各カテゴリーを統合的なフレームワークの観点から分析した。すなわち，コンピュータ倫理として扱われる課題を，対象，目標，リスク評価という3つのフレームワークの観点から分析し，また，望ましい倫理的な状況を維持し増大させるための対応策も，規範の醸成，法律の制定，技術の開発という3つのフレームワークから考察した。

4つのカテゴリーと6つのフレームワークとで構成される体系によって，現実に発生するコンピュータ倫理の諸問題を分析する試みは，コンピュータ活用に関係する倫理的判断のリスクを低減させるために，どのようなアプローチで諸論点を考察すればよいかを分析者に示すというメリットを持つ。

2. コンピュータ倫理のカテゴリー

(1) カテゴリー区分の基準

筆者が，先に，諸論点の総合的把握のため想定した観点は，一方でコンピュータが物事を可視化する特質を持ちながら，他方で不可視性を促進すること，および，ＩＴ（情報技術）習得者をプロフェッショナル化し一般ユーザーとの責任や地位の格差を広げることであった。

すなわち，コンピュータは，物事を可視化する（膨大な計算を瞬時に行う，遠隔地にある情報を瞬時に収集するなど）と共に，物事を不可視化する（ソフトウェアの形で様々な物の中に埋め込まれ機能する）性質を持つ。また，ソフトウェアを生産，運用するプロフェッショナルは，一般ユーザー（ノンユーザーも含む）を超えた知識やスキルを持ち，その権限と影響力が一般ユーザーを圧倒する特質を持つ。

したがって，コンピュータを使用した情報行動の特質は，図1に示すように，可視性/不可視性の軸，および，プロフェッショナル/一般ユーザーの軸で区分される4つの分野によって識別することができ

*1ビジネスコミュニケーション学科

る。

こうしたコンピュータがもつ特質とは別に，われわれの社会には，公的活動は可視化を求められ（情報共有，説明責任），私的活動では不可視性（秘密性）を保護する規範が存在する。企業は虚偽の商品説明に対して責任を問われ企業活動には情報のディスクロジャーが求められる。同時に，個人の無制限なプライバシー公開は禁じられ，個人情報の流出は問題とされ，個人の創造的なアイディアは保護される。

このようにコンピュータのもたらす影響と，社会が要請する規範が交錯する場合，個人や社会にとって重要な問題が発生する。すなわち，コンピュータの膨大な計算能力や遠隔地での迅速な情報収集，情報配布能力は物事を可視化する機能を持ち，それが社会の可視化を求められる分野に適用される場合は社会全体の効率化に役立つ。しかし，コンピュータの可視化機能が私的活動の不可視性の要求される分野に適用される場合，問題を引き起こす。たとえば，個人のセンシティブ情報がコンピュータネットワークを介して配布されれば，プライバシーの侵害となりその影響は瞬時に大規模なものとなる。

また，ソフトウェアが持つ不可視性を体現するコードを一般ユーザーが容易に理解，検証できないという特質を利用して，悪意を組みこんだコード（サラミプログラムやトロイの木馬プログラムなど）が，社会における公的活動の分野に浸透する場合には，公的活動の可視性は歪められ，不正な活動や不透明な活動がはびこる可能性が生じる[2]。

単純化して言えば，コンピュータの可視化機能が，社会において不可視化が要請される分野に働くときに，また，コンピュータの不可視化機能が，社会の可視化が要請される分野に働くときに，図1のように，コンピュータ倫理の課題が生み出される。

プロフェッショナル

不可視性の要請			可視性の要請
	知的財産権	プロフェッショナル倫理	
	プライバシー	コンピュータ犯罪	

一般ユーザー

図1　コンピュータ倫理のカテゴリー化

(2) カテゴリーの内容

こうしたカテゴリー構築はコンピュータ倫理の諸課題を体系的に理解する上で有効である。プロフェッショナル/可視性の分野では，プロフェッショナル活動を可視化するテーマを示すもの，すなわち，プロフェッショナル倫理が挙げられる。たとえば，システムやソフトウェアの不備，ウィルスの配布，ハッカー行為，情報専門家に要求される倫理的意思決定や情報公開の問題は，プロフェッショナルが可視性を発揮すべき倫理問題として論じられ，倫理綱領の制定は，倫理問題への対応策である[3]。

一般ユーザー/可視性の分野では，ユーザー活動の可視性がテーマとなる。ユーザー活動の内容を可視化すべき場面で，可視化を避け意図的に不可視性を利用する違法行為はコンピュータ犯罪として論議される。たとえば，ネットワーク上の詐欺行為，不正アクセスなどは自らの不可視性を利用した犯罪であり，可視性の仕組を導入しユーザーがその仕組に従って活動すれば違法行為の抑制が期待できる。

一般ユーザー/不可視性の分野では，ユーザーに関係する事柄が見えすぎるために発生するプライバシー問題が論じられる。たとえば，個人情報の漏洩，職場監視，コンピュータマッチングなどは，本来，不可視性で守られるべき情報である個人情報が，可視化されるために発生する問題である。

プロフェッショナル/不可視性の分野は，プロフェッショナルが創造するアイディアやソフトウェアが可視性の下に曝されることにより発生するテーマをふくむ。たとえば，不正なソフトウェアコピー，ビジネスモデル特許侵害などの知的財産権が論議される。不可視性で守られるべきプロフェッショナルの創造的活動の成果が侵害される問題である。ここでは不可視性の維持や，一定の条件の下で不可視性を可視性に変換する仕組が検討される。知的財産権保護技術の開発もこの分野の例である。

3. カテゴリーの問題

(1) カテゴリー区分の非厳密性

図1は，以上の観点から作成されたカテゴリーであるが，そこには2つの留意点がある。第一は，4カテゴリーはコンピュータ倫理が包含する種々のテーマをプロッティングする場合の相対的関係を表しており，厳格な区分ではない点である。たとえば，プライバシーは個人活動のあらゆる分野で問題とされるテーマのみならず，プロフェッショナル活動にも当然，関係する。図1の上部を占めるプロフェッショナルの活動分野とプライバシーの関係は，プロフェッショナル活動にプライバシーはない，という意味ではなく，プライバシーの問題はネットワーク社会において，ネットワークやコンピュータを活用する一般ユーザーに大きな影響を与える問題であり，プロフェッショナルもユーザーもネットワークにアクセスする場合，関連せざるを得ない問題である。

(2) カテゴリーを表す用語

第二の留意点は，各カテゴリーを代表する4つの用語は現実に発生している倫理的課題に関係する現象を記述したものであり，用語そのものは相互に統一性を持たない点である。各テーマが意味する範囲や深さのレベルを考察すると4カテゴリーの用語には整合性が欠けていることがわかる。この用語は，コンピュータ倫理の複数のテキストに共通に用いられる代表的用語を抜き出したものである[4]。しかし，この用語がよく使われる理由は，コンピュータ倫理のさまざまなテーマがこの用語に輻輳しているからとも考えられる。まず，4つの用語を取りあげカテゴリーの内容をみてみよう。

① コンピュータ犯罪

コンピュータ犯罪という表現は，違法行為を表す法律的表現であり，用語自体がネガティブな価値を持つ表現である。他の3つのカテゴリーで使われる用語はどちらかと言えば，プラス価値を持つ用語でありポジティブな表現である。さらに，コンピュータ犯罪という用語はきわめてその範囲が広く，4つの分野で不正な倫理的判断が行なわれ，違法行為が発生した場合に適用可能な用語でもある[5]。

② プロフェッショナル倫理

プロフェッショナル倫理は，職業倫理を意味する。社会で一定の役割，機能，地位を獲得した職業集団が遵守すべき規範であり，コンピュータ倫理では情報技術の専門知識をもつ職業集団が対象となる。プロフェッショナル倫理は法律的な側面よりもプロフェッショナルの倫理綱領，倫理的判断における規

準やガイドに焦点をあてる。また，プロフェッショナル倫理はコンピュータ犯罪の抑止策でもある。

③　知的財産権

知的財産権は，自分のアイディアを守るための権利であり法律の範疇にある用語である。自らの労働で獲得した財産は自分の所有物となるという，近代の所有理論をベースにした権利であり，プログラムなどのソフトウェア保護の権利がその例である。コンピュータ倫理の分野では，情報の価値をいかに保護するかという課題になる。また，一定の手続を経た知的財産権は広く社会で利用できる。

④　プライバシー

プライバシーとは個人の秘密であり，プライバシー権とは，個人の秘密を保護すること，および自分の個人情報を自分でコントロールする権利であるといわれる。法律的なニュアンスが強い表現であり，コンピュータ倫理の分野では個人情報の保護が大きな論点となる。財産権と同じく社会のなかの個人がもつ基本的な権利であり，個人情報は一定の条件下で他者が活用することも可能である。

(3)　カテゴリー定義の問題

このように見ると，図１の各カテゴリー表現には規範や法律的な権利が盛り込まれ，また，左側は保護対象を中心にした用語であり，右側には対象を保護する手段（右上は倫理によって対処し，右下は法律によって対処する方策）を中心にした用語が使われている[6]。

こうしたカテゴリー表現のレベルを統一し，カテゴリーの整合性を確保するには，3つの観点からカテゴリーを分析し内容を明確化することが役立つ。第一は，カテゴリー内での論議の対象を明確にすることである。第二は，論議の対象がめざす目標は何かを分析することである。第三は，目標達成の阻害要因となるリスクと，そのリスク低減のアプローチは何かを分析することである。

この３つの観点のうち，第一の観点では，情報に係る活動に焦点をあてる必要がある。すなわち，情報の生産や入手，生産された情報の蓄積，加工，伝達，情報の管理，廃棄などの活動が考察の対象となる。コンピュータ倫理の知見を充実させるには，情報処理の各局面で必要となる倫理的判断の種類や内容の分析と発生するリスクについてのデータを収集，分析，蓄積する作業が必要である[7]。

第二に，各カテゴリー内の対象が目指す目標状態は何かを検討する。倫理とは，究極的には善きことを目指す（最大幸福に役立つことや，自己の良心に従い善きことを行うこと，人間としての基本的権利を主張することなど）が，実践的な倫理的活動とは，各カテゴリーの情報処理の局面で，具体的にどのような状態を目指して活動すべきことなのか，目標をどう表現すべきなのかを分析する。

第三は，リスク低減のための分析である。目標に到達できない現状を分析しそのリスクやリスクを生み出す原因を因果関係の観点から評価する。リスクを低減させる解決策には，規範，法律，技術という３つの観点，および相互の関係分析からアプローチすることが有効である。

4. コンピュータ倫理のフレームワーク

コンピュータ倫理のフレームワークは，図１のカテゴリーを以上の３つの観点で分析した結果であり，カテゴリーの内容を体系的に理解するための仮説である。このアプローチは，輻輳した構造を持つコンピュータ倫理のテーマを分類し，各テーマを相互に関連付けて理解できるメリットがあり，コンピュー

タ倫理の問題分析や施策策定に役立つ。本稿で提示するフレームワークは，図２で示すように，対象，目標，リスク評価，規範，法律，技術から構成される。

(1) 対象

コンピュータ倫理の対象は，情報行動あるいは情報活動である。情報の生産，入手，蓄積，加工，伝達に関する活動で，いかに情報を保護するか，情報に関する不正な行為を防ぐか，倫理的に行動するかが，その目的である。倫理的行為の目標，目標到達を妨げるリスクを引き起こすさまざまな原因，リスク低減の方策も，情報の生産，入手，蓄積，加工，伝達という具体的な情報活動の分析を通して明らかにする必要がある。図１のカテゴリーは，そうした情報活動から発生する課題を可視性/不可視性，プロフェッショナル/ユーザーの軸で分類する基準であり，その基準をベースに，図２は，情報の生産から伝達までのサイクルを想起し，発生する課題を位置付け，考察を進めることを示す。

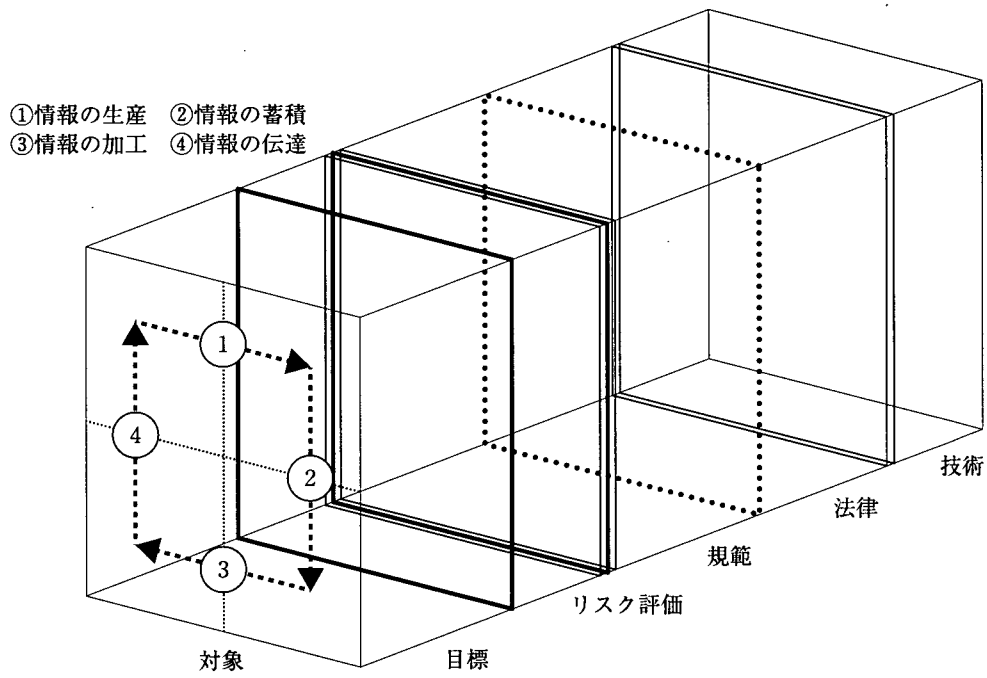

図２　コンピータ倫理のフレームワーク

(2) 目標

情報の生産から伝達に至る局面で，われわれはさまざまな情報活動を行う。利害関係者と複雑に関係した情報活動のなかで，われわれは倫理的な判断が必要とされる事態に遭遇する。

コンピュータ倫理の究極の目的は，情報を取扱う場面で，正，不正や善悪の倫理的判断を行う場合のガイドの提示である。ガイドの提示を行うには，何を達成するためにガイドが必要となるか認識しなければならない。目標が明確でなければガイドを構築する基盤が持つことができないからである。

したがって，図１の４カテゴリーを構成する，プロフェッショナル倫理，コンピュータ犯罪，プライ

バシー，知的財産権の各分野で行われる活動の目標を明確に定義する作業が第一に求められる。そこでは，「善きことを行う」と言う一般的な表現レベルではなく具体的な活動目標を掲げる必要がある。

(3) リスク評価

目標を達成するためには，さまざまな障害を乗り越えなければならない。リスクとは目標に到達するために障害となる現象であり，目標に到達する途中に存在する不確実性である。われわれが情報処理を行う際には，目標達成を阻害するリスクを評価しリスクに対して適正な対応が求められる。

なぜなら，リスクに対する適正な対応が倫理的に望ましい行動でありわれわれの活動の品質を高めて目標達成を推進するからである。また，それがコンピュータ倫理のめざすところだからである[8]。

しかし，活動目標を明確に定義したり活動目標の合意を形成したりすること自体が多大なエネルギーを要し，活動目標も環境変化に対応して変化することもある。その場合，当然，リスクそのものもリスクの捉え方も変化してくるだろう。われわれが情報処理を行う際に直面する倫理的判断は，こうした目標明確化の困難さも考慮しつつ，目標を認識し目標達成のリスクを排除する観点から行う必要がある。

リスク評価の局面では，発生するリスクをカテゴリーごとに記述する。リスクを回避するには活動を停止する方策もある。たとえば，一定の年齢以下の子どもにはインターネットの特定のウェブ閲覧を禁止する方策である。しかし，社会全般でコンピュータを活用した活動を制限することはもはや不可能である。したがってリスクの危険を承知した上でリスクを保有しつつ，対応してゆかねばならない。

リスクを分析し対応策を策定する局面では，リスクの発生状況や発生原因を明確にしてリスクの予防あるいはリスクの低下につながる活動を考える。一定の年齢以下の子どもにはインターネットの特定のウェブ閲覧を禁止することは，リスクを回避するための家庭での取り決めである。これは，規範によるリスク対策と言えるであろう。また，販売されているソフトウェアを無断でコピーすることが法律で罰せられるのは，財産権が侵害されるリスクを公権力で予防するものとも考えられる。暗号化のような対策は，データの機密保護が侵害されるリスクを技術的な観点から予防する方策である。以下では，規範，法律，技術の3つの対応策をみてみよう。

(4) 規範

情報処理を行う場面でどのような倫理的判断を行うか，そのベースとなる考え方，ルール，ガイド，各人の情報行動の内的規制を構築する条件などが規範レベルでの対応策である。われわれは多くの規範に囲まれ活動する。所属する社会の規範，所属する組織の規範，自己の信条が要請する規範，さらには，ネットワーク活用の規範，コンピュータ活用の規範など，活動主体の職務，地位，責任，環境との関係において多くの規範が存在し，われわれは多様な規範を調整しつつ行動する。

情報を取扱う場面のあらゆるケースを想定して個別の行動規範を構築すること（決疑論）は現実的には，全てのケースを網羅できない・ケース相互の矛盾が発生するなどの多くの困難を伴い不可能である。これまでの規範理論をベースにコンピュータ倫理の新たな規範理論を積みあげることが大きな課題である。

(5) 法律

法律とは社会生活における行為の準則であり遵守すべき規範の一部である。また，犯罪発生のリスクを減少させ犯罪行為を予防する法的な対応策が法律である。規範は，行為の前段階でプロアクティブに倫理的判断をガイドする。一方，法律は，主に行為の結果に焦点をあてリアクティブに行為を規制する。法律の論議はコンピュータ倫理のカテゴリーには入れるべきではないかもしれない。

しかし，「法は最小限度の道徳である」と言われ，両者をシームレスな関係として捉えることもできる。倫理や規範を考える場合には，法律の要請する範囲や目標と，倫理の要請する範囲や目標を識別し，両者の錯綜する論点を明確にすることも役立つ。現在，制定されている法律は，図１のカテゴリーに対応して分類できる。

(6) 技術

４つのカテゴリー内で発生するリスクを抑制する仕組を構築するためコンピュータをはじめとする諸技術を活用することが技術的な対応策である。パスワード，アクセスコントロール，ファイヤーウォール，暗号化，電子署名などがその例である。技術的な対応は，図１のカテゴリー全分野に関係するユニバーサルな性格をもつと言える。しかし，たとえば，アクセスコントロールという技術的な考え方はシステムのデータ保護に重点をおいた仕組と位置付けることも可能である。

以上の６つのフレームワークを活用して，われわれは，図１のコンピュータ倫理のカテゴリー内で発生する諸問題を重層的に捉えることができる。コンピュータ倫理のさまざまな問題や論点は，図２のフレームワークのどこかにプロッティングされる。

5. コンピュータ倫理のカテゴリー分析

図１の４つのカテゴリーは，その内容として図２のフレームワークの観点から論じられる重層的構造を持つことを論じてきた。ここでは，図１のカテゴリーごとに，目標，リスク評価，規範，法律，技術の内容を具体的に検討してみよう。この検討によって，各カテゴリーが持つ多様な内容を整理して分析できる概念的な枠組みを得ることができるのである。

(1) 目標

各カテゴリーが目標とするものを，図３に示す。プロフェッショナル/可視性の分野では，不可視性の排除，情報公開などといった透明性が求められる。そこではプロフェッショナルの公的な活動状況が公開されることが望ましい状態である。その背景には，活動の公正，平等，正義などを求める社会の規範や価値観がある。この望ましい状態を，図３で示すように，「プロフェッショナル活動の透明性」と定義する。プロフェッショナル活動の透明性は，プロフェッショナルの公的活動の情報開示を行い，自らの行為の説明責任を果たし，行動の倫理綱領を遵守する。それは，プロフェッショナルの不正行為を防ぎプロフェッショナルへの信頼を高め，その活動を効率化し社会的効用を増大させる。

プロフェッショナル

不可視性の要請	創造した情報の保護	プロフェッショナル活動の透明性	可視性の要請
	秘密，自己情報の管理	ユーザー活動の透明性	

一般ユーザー

図3　各カテゴリーの目標

一般ユーザー / 可視性のカテゴリーでは，「ユーザー活動の透明性」が目標となる。ユーザー活動の透明性とは，一般ユーザーが市場やネットワーク上の公的な場面で活動する際の，自らの活動表明である。ネット取引やコンピュータ利用局面でユーザーが正しく明確に識別されることでユーザー活動の透明性が高まり，不正行為の防止やネットワーク活動の円滑化が進む。

一般ユーザー / 不可視性カテゴリーでは，自分の「秘密，自己情報の管理」が目標である。秘密，自己情報の管理とは，自己の秘密情報を他人に漏洩せず，個人情報を自分でコントロールすることである。自己の秘密が暴露される場合や個人情報が密かに活用される場合，個人の自由が阻害される危険が発生する。この目標は近代社会の構成原理である基本的人権そのものと密接に関連する。

ただし，個人情報の中でも，氏名や住所などは効率的な商取引を推進する場合，開示することの多い情報である。この情報を提示すれば自己のニーズに合致する商品の提供が迅速化し，取引活動を効率化するメリットがある。反対に，センシティブ情報の開示はプライバシー侵害となる。個人情報の中の開示情報とセンシティブ情報の区分けの調整が問題となる。

プロフェッショナル / 不可視性では，自分の「創造した情報の保護」が目標である。創造情報の保護とは，個人が自分で考え出したアイディアや情報は個人のものとして保護されることである。われわれの社会では，生命，自由，財産の不可侵は基本的な権利とされ，プロフェッショナルが情報の生産局面で獲得した情報も個人や組織に所属する。しかし，社会全体の効用の観点から，創造情報を一定条件下で他者に利用させることも望ましい。特許権や著作権などの知的財産権はこの考えのもとに権利，義務が規定される。他者に利用させる場合，知的財産権利用の問題は，プロフェッショナルやユーザー活動の透明性の下におかれる問題となる。

4カテゴリーには，左側の象限の背景には，私的活動における自由，財産の不可侵の価値観がある。右側の象限には，公的活動を行う場合，行為主体に行為規範の遵守を求めるという考えがある。目標の記述では，倫理のあるべき姿を的確に表現することが求められる。図3の目標記述は，一般の企業や諸団体の情報倫理綱領などで明示化されつつある。しかし，さらに具体的に，実行可能かつ評価可能な形にまで分析して組織における情報行動の有効な指針として運用されることが今後の課題である。

(2)　リスク評価

リスクとは目標に到達できない行為，目標達成を阻害する状況の確率である。目標の場合と同じ考察を加え，各カテゴリーで，現在，発生している望ましくない状況，すなわちリスクを含んだ状況を定義したものが図4である。

プロフェッショナル

不可視性の要請	創造された情報の侵害	プロフェッショナルのコンピュータ濫用	可視性の要請
	個人センシティブ情報の侵害	ユーザーのコンピュータ濫用	

一般ユーザー

図4　カテゴリーのリスク評価

プロフェッショナル/可視性のカテゴリーでは，ハッカー行為やウィルス配布，ソフトウェア作成時のコードの不正コピー，ソフトウェアの品質，コンピュータ設計の不十分さなどがプロフェッショナル活動の問題点である。この現象はプロフェッショナル活動の透明性に対するリスクである。これらを「プロフェッショナルのコンピュータ濫用」として定義する。

一般ユーザー/可視性のカテゴリーでは，ソフトウェアの不正コピーやネット取引での詐取行為など，および不正アクセスなどがリスクを引き起こす行為である。個人情報をＷｅｂで公開し，掲示板に他人の名誉毀損の記事を書き込むのも，ユーザーがネットワークの不可視性を利用した不透明な行為である。これらは「ユーザーのコンピュータ濫用」として定義することができる。

一般ユーザー/不可視性のカテゴリーでは，個人情報の不当な収集，蓄積，売買がその代表である。コンピュータの不正なデータマッチングや職場の個人活動監視なども当カテゴリーの目標に対するリスクであると考えられる。この活動を，「個人センシティブ情報の侵害」として定義する。

また，プロフェッショナル/不可視性のカテゴリーでは，知的財産権の不法利用やシステムに侵入して営業秘密を盗み見ることが該当する。この行為は，創造した情報の保護に対するリスクであり「創造された情報の侵害」とまとめられる。創造情報の侵害者は，プロフェッショナル，一般ユーザーともに考えられる。たとえば，ソフトウエアの不正コピーは，一般ユーザーが関わる「創造された情報の侵害」である。しかし，現実には，ＩＴ知識の豊富なプロフェッショナルの関与が大きく，その影響も深甚である。

図1のカテゴリーである，プロフェッショナル倫理，コンピュータ犯罪，プライバシー，知的財産権という用語は，本論文で提示したフレームワーク，すなわち，対象，目標，リスク評価という観点からは，以上のように分析できる。次の課題は，リスクを減少させるため規範，法律，技術の3つの観点から，対応策をどのように捉えるかである。

(3) 規範

現在，発生しているリスクを除去し目標状態に近づけるために種々の方策がある。その第一が規範や規範遵守の意識醸成である。4カテゴリー全てに関わる規範として，たとえば，情報モラルが要求されることが多い。情報モラルはコンピュータに関わる人すべてが遵守すべき規範ともいえる。しかし，ここでは，各カテゴリーの目標を達成するため，より具体的な規範，あるいは行動倫理を論議する。

プロフェッショナル/可視性の分野では，図5に示すように，その職業やグループに特有な倫理として「プロフェッショナル倫理」が求められる。プロフェッショナル倫理とは，プロフェッショナルが情

報に関わる活動で，顧客，同僚，上司，社会などとの関係で新たな責任を獲得することによって求められる倫理である。正当な内部告発を行う場合のルールやガイドも，新しい規範として受け入れられる。

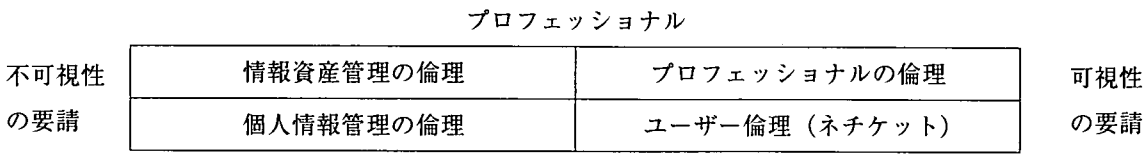

図5　各カテゴリーと関連する規範

一般ユーザー / 可視性の分野は，ユーザーが所属する組織によって多様な規範が考えられるが，どの組織に所属していようとも誰もが守るべきルールとしてネチケットがあげられる。ネチケットはネットワークユーザーが遵守すべきエチケットでありユーザー倫理が目指す規範の一部を示している。したがって，この分野の規範を「ユーザー倫理（ネチケット)」としておこう。

一般ユーザー / 不可視性分野の規範は，「個人情報管理の倫理」と定義できる。個人情報管理の倫理は，ユーザーが入手，利用する他人の個人情報を正しく取扱う規範である。プロフェッショナルであっても一般ユーザーの立場で情報システムを利用するときには，この倫理を遵守すべきである。個人主義的な考えや，個人の自立意識が十分，浸透していない社会では，個人も組織も，個人情報管理の倫理意識は低いと言えるだろう。

プロフェッショナル / 不可視性分野の規範は，「情報資産管理の倫理」と表現できる。情報資産管理の倫理とは，他人の創造情報を正しく取扱う規範であり，著作権や特許権などで保護される場合が多い。。わが国は情報資産の意識においても権利保護においても多くの問題を抱えていると考えられる。

一般ユーザー / 不可視性分野と，プロフェッショナル / 不可視性分野では，それぞれ，プライバシー権，知的財産権という法律的権利が論議の中心となって展開しやすく，規範や倫理としての論議の蓄積は今後の課題である。図5の右側で主導的な役割を果たすのは共生の規範であり，左側では自己の情報行動における内的規制の規範が要請される。

(4)　法律

リスクに対する第二の方策が法律の対応である。各カテゴリーの目標に対するリスク抑制には，背任罪，詐欺罪，特許法の侵害など従来の法律の適用で対応できる部分もあった。しかし，コンピュータの出現は1985年の著作権法改正によるプログラム保護などに見られるように，新たな法整備に影響を与えている。図6では，カテゴリーごとに関係すると思われる法律の例や行動規範を提示している。

プロフェッショナル

不可視性の要請	知的財産法	プロフェッショナル倫理綱領	可視性の要請
	個人情報保護法	電子署名・認証法	

一般ユーザー

図6　各カテゴリーと関連する法律例

プロフェッショナル/可視性の分野では，医師や弁護士のように，情報プロフェッショナルそのものを直接に規定する法律はない。ＡＣＭ（米国）や情報処理学会などで決められている行動指針が，プロフェッショナル倫理綱領として，現在，法律に近い役割を果たしているが，罰則規定はない。

一般ユーザー/可視性の分野における不正な行為に適用できる法律は，刑法の窃盗，詐欺，横領，背任罪などをはじめとして多岐にわたる。インターネットの時代でも，従来の規範や法律は多くが通用するからである。しかし，技術の急速な発展は，従来の規定でカバーできない現象を引き起こし，刑法の改正や新たな法律の制定を促している。コンピュータデータ保護のために不正アクセス行為の禁止等に関する法律や，本人確認のための電子署名・認証法や，電子商取引に関する迷惑メールを規制するための特定商取引に関する法律や法律施行規則などを，その例として挙げることができる。

一般ユーザー/不可視性分野の目標は，「秘密，自己情報の管理」であり，その規範は，「個人情報管理の倫理」である。個人情報の流出や悪用を防ぐ国際的基準として各国の法制に大きな影響を与えたものがＯＥＣＤ８原則である。さらに，1995年，これを具体化する原則としてＥＵ個人情報保護指令が採択され，発効した。わが国では，こうした動きに対応して，個人信用機関や金融機関が個人情報の取扱い指針が作成され，個人情報保護法が制定された[9]。

プロフェッショナル/不可視性分野の法律は，知的財産法としてまとめられる。これは，特許法，実用新案法，意匠法，商標法，不正競争防止法などを含む工業所有権法と，著作物，実演，レコード，放送，有線放送などにおける情報を保護する著作権法から構成される法律群である。

情報に関する法律の規定は，この他に多くのものがあるが，法律の議論そのものは，コンピュータ倫理の範疇ではない。情報を取扱う局面で，どの情報活動を規範や倫理で扱うべきか，不正行為を防止し処罰するためにどの情報活動を法律で規律すべきか，また，取扱いの基準をどのように分けるか，などがコンピュータ倫理の分野で論議すべきテーマの例である。

(5) 技術

リスク対応の第三の方策は技術である。コンピュータネットワークを活用してリスクを引き起こす問題の解決にコンピュータをはじめとする情報技術そのものを活用するアプローチである。

プロフェッショナル

不可視性の要請	セキュリティ	グループウェア	可視性の要請
	暗号化	ワークフロー	

一般ユーザー

図７　各カテゴリーと関連する技術例

コンピュータ倫理のテーマとして，セキュリティや暗号化などが論じられるのは，誤った倫理的判断によって行動を起こす人への技術的な防御策を示していると考えられる。技術の適用範囲は人間活動のあらゆる方向に広がるため，規範や法律のように各カテゴリー別の例を挙げるのは難しい。技術はここで定義されたカテゴリーを越えるとも言える。しかし，あえて区分すれば，図７の右側は情報共有を行う技術，たとえば，グループウェア，ワークフロー，認証技術などに重点がおかれ，左側では安全保護を確保するセキュリティの仕組みや暗号化技術などに重点があると言えよう。

6. 今後の課題

コンピュータ倫理の諸論点を統一的に理解するために，コンピュータの特質である可視性/不可視性の軸と，コンピュータで差別化されるプロフェッショナル/ユーザーの軸で４つのカテゴリーを識別した。２つの対照的な特質でマッピングされたカテゴリーは，コンピュータ倫理課題の分析基準となる。

このカテゴリーは多くの内容を含むため，さらに６つのフレームワークから分析した。最初の３つのフレームワークである，対象，目標，リスク評価は，現実に発生する多くの課題を分析，整理する際に活用できるであろう。また，規範，法律，技術は課題の対応策やリスク低減の方策として総合的に考察すべきであろう。特定の課題を，規範のみ，法律のみ，あるいは，技術のみの対策で対応することは不可能であり，3つの要素が，相互にうまく連携する場合に大きな効果が得られる。

たとえば，あるソフトウェア開発会社でシステム開発の深夜残業が恒常化し心身異常や過労死が発生する状況を考えてみよう。このケースは情報処理の活動を行う場合の倫理的判断としてコンピュータ倫理と関連性を持つと思われる。法律では，所定労働時間が決められ月間の勤務時間の制限があり，また，通常はその会社の残業についてのルールが決められている。しかし，オフィスで働く人々の内面にある規範は，法律や社内ルールと異なるかもしれない。たとえば，上司や同僚が退社しないうちは，自分もオフィスに残るという規範がその部署の構成員に徹底されているような場合である。その結果，深夜12時過ぎまでの残業は恒常的となり，残業時間の申請も少なめに行うことになる。これは明らかに，法律や社内ルールよりも規範が社員をコントロールしていると言えるであろう。

こうした状況に対する技術の関わり方は，たとえば，タイムカードをきちんと押させ，そのデータに基づいて管理を厳しく行う仕組みを徹底させることなどを考えることができる。技術の適用によって，残業と言う事実を明確に管理し，残業の恒常化を減少させるのである。しかし，この効果を維持するには規範や法律との連携が必須となるであろう。

本稿で論じたフレームワークはひとつの理論的な仮説であり，さらに精緻なフレームワークが必要に

なるかもしれない。コンピュータ倫理の諸課題を関係づけて理解するためには，一定の戦略や有効な統合的アプローチが必要だからである。

コンピュータ倫理は，情報の生産，蓄積，加工，伝達場面の活動の具体的な倫理性を問題とする。今後，さらに現実場面の種々の問題を分析し研究成果を積み上げ，コンピュータ倫理の規範を構築する必要がある。その場合，各カテゴリーの目標や規範などを検討するとき，コンピュータ社会における価値を再考する余地もある。また，個人が活動する場合の動機付けをいかに規範に対応するように設定するか，という問題もある。そこでは，近代から現代にかけて確立してきた基本的人権，自由，公正などの価値観などの根本的な再検討や，コンピュータという現代の発明物と，倫理という日本の社会，文化に深く根ざしたものとの折り合いをどう考えるかという点も重要なテーマになると思われる。

（注）

1　この議論については，梅田［2002］を参照のこと。

2　ソフトウェアは，論理的な内容をもつ人間活動をプログラム手順として表現できる性質（論理的順応性：Logical Malleability）を持つ。ソフトウェアはチップの形で多彩なものに組みこまれ外部から内容を容易に理解できない。したがって悪意の埋め込まれたプログラムは，多彩な場面に浸透していく可能性をもつ。論理的順応性については，Moor［1985］を参照のこと。

3　われわれの私的な活動以外は，多くの場合，透明性，すなわち，情報開示が求められる。情報プロフェッショナルの主要活動は，情報生産のための情報システム構築であり公的な活動である。情報システムのソフトウェアに不備や欠陥があり，また悪意のコードが組みこまれると情報システムの価値は低下する。ソフトウェア構築やプロジェクト管理の分野で作業や作業結果を客観的に評価する仕組や倫理綱領は，不可視性を除去し透明性を高める試みである。

4　たとえば，米国の代表的な教科書のひとつである，Deborah G. Johnson［1994］では，Professional Ethics, Privacy, Property Rights, Crime などが記述される（第3版［2001］では Crime の記述は章見出しから無くなった）。Kevin W. Bowyer［2001］や John Weckert and Douglas Adeney［1997］などにも，Professional Ethics, Privacy, Property Rights の3項目は必ず含まれている。

5　コンピュータ犯罪という用語は，コンピュータ倫理関連の文献で当初，よく使われた用語であるが，次第に使われなくなりつつあるように思われる。犯罪という言葉で，倫理より法律との関連性が強く感じられるためであろうか。

6　コンピュータ倫理の歴史を見ると，当初は，生産物としてのソフトウェアの財産権が注目され，それを生産する情報プロフェッショナルの行動が問題となった。やがて，コンピュータやネットワークが社会に浸透すると共に，プライバシー情報の保護や，ユーザーの活動が問題にされたと考えられる。

7　倫理を具体的に考える場合，「これこれをなすべし」という表現ではあまりに漠然としすぎる。また，個別の事例について指針を積み上げていくのは，決疑論に陥りやすい。Mason［1993］は，情報処理の各局面で人々が倫理的に大きな決断をせまられる場面を，決定の瞬間，認識の瞬間と定義し，倫理的活動を構造化して理解しようとしている。

8　望ましい倫理判断ができない場合，それは目標達成に対するリスクとなる。リスクは悪い現象が発生する確率であり，リスクが現実化すると問題となる。コンピュータ倫理は正，不正，善悪の判断基準や行動基準の指針を提供することによって，発生した問題を解決することよりも，問題が発生する以前の状態であるリスクを低減させ問題を防ぐことを目的とする。

9　ＯＥＣＤ８原則は，「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」で1980年に示された８項目の基準である。EU 個人情報保護指令は，「個人データに関わる個人の保護及び当該データに関わる個人の保護及びデータの自由な移動に関する欧州議会および閣僚理事会の指令」であり，EU 参加国に個人情報の保護などに関する立法措置を促している。わが国における個人情報保護法は，2003年５月に，不服申し立てに関する関連法案などと共に，成立した。

参考文献

Bowyer, Kevin W. 2001 *Ethics and Computing Living Responsibility in a Computerized World.* (2 nd ed.) IEEE Press.

ジョンソン D. G. 水野雅彦・江口聡 監訳 2002 コンピュータ倫理学 オーム社
(Johnson, Deborah G. 2001 *Computer Ethics.* (3 rd ed.) Prentice Hall.)

メイソン R. O. 他 坂野 友昭 監訳 1998 個人情報の管理と倫理 敬文堂
(Mason, Richard O., Mason, Florence M., & Culnan, Mary J. 1995 *Ethics of Information Management.* Sage Publications, Inc.)

Moor, James H. 1985 What is Computer Ethics ? *Metaphilosopy16*

梅田敏文 2002 コンピュータ倫理におけるプロフェッショナルと不可視性 愛知淑徳大学論集 - コミュニケーション学部篇 - 第２号 17－33.

Weckert, John & Adeney, Douglas 1997 *Computer and Information Ethics.* Greenwood Press.