アメリカの大学における計算機上の情報に対する プライバシーの保護

吉永敦征

はじめに

システムの維持という観点から考える情報倫理の問題のポイントはシステムのセキュリティーの向上と利用者のプライバシー保護の間のコンフリクトである。このコンフリクトはパブリックとプライバシーの区別に由来すると見ることができる。この論文では大学におけるネットワークセキュリティーとプライバシー保護の問題を取り扱う。

すなわち、プライバシー概念を分析し、プライバシー概念を構成する要素を明らかにし、パブリックとプライバシーの区別に起因する問題(線引き問題と呼ばれる) を概観し、パブリックとプライバシーの区別から生じる線引き問題をセキュリティーとプライバシーの関係としてとらえなおす。アメリカの大学におけるコンピューター利用のポリシーの分類を行ない、ポリシーが階層的に構成されていることを明らかにする。分類した上位の階層のポリシー内容について、分類を行なう。分析したプライバシー概念の構成要素をアメリカの大学におけるコンピューター利用のポリシーに適用し、ポリシーの分析を行なう。最終的に、大学においてはプライバシーを保護することが重要であることを明らかにする。

1 プライバシーについて

本節の目的は一般的なプライバシーの概念をまとめ再構成し、ネットワーク上の現象に対し再構成したプライバシーの概念を適用するための準備を行なうことである。ネットワーク上においてプライバシーの侵害がなされていると主張されることが多い現在、我々はネットワーク上におけるプライバシーの侵害に多大なる不安を覚える。そのさいプライバシーの侵害とはどのような事柄を意味しているのか、またどのような意味あいで用いられているのかを分析し、問題の整理を行なうための準備を行なうことも本節の目的である。

1.1 プライバシーの概念

プライバシーは自由で開かれた社会にとっての基盤であり、個人の発達のために重要なものだと考えられている。またプライバシーは自発性を促進し社会的な抑圧に従うことから個人を隔離し保護する。自律性、創造性、人間関係をつくる能力、個人の責任感を発達させることにプライバシーは寄与する。またプライバシーは個人だけにではなく、家族や集団などにも必要とされているとか、それはプライバシーを持つとしばしば言われている。

プライバシーは自由な考えにとって中心となるものである。それは国自身からの、また他人からの侵害を防ぐことを国が権利として保証しているということである。我々が保持する法的権利としてのプライバシーの観念は最近獲得されたものである。

現在我々が保持している法的なプライバシーの権利は1965 年に行なわれたGriswold対 Connecticut の連邦最高裁判決以降に認められたものである。1879 年に制定されたConnecticut

州法は避妊用の器具の販売、所持を禁止し、またその道具の使用の賛助や支持、また相談をすることをも禁止していた。医師Estelle Griswold がこの法に違反、逮捕され100 ドルの罰金を科せられた。Griswold はこのことに異義申し立てを行ない議論の結果、最高裁によって上記のConnecticut 州法は違憲であると宣言された。

Griswold の判決から8 年後の1973 年、Roe 対Wade の判決を通じて連邦最高裁判所はプライバシーの権利を拡大し、中絶する権利をプライベートなものとする。この判決では「母体の生命の危機をさけるためにのみ中絶は許可される」というテキサス州法の中絶に関する規定を取り除くことになった。[1, Page: 684]

プライバシーの意義、つまり市民の権利としてのプライバシーは人々が望むように自由に振舞うことのできる自立した領域があるということである。

1.1.1 プライバシー概念を構成する３つの要素

プライバシーの概念は次の3 つの要素から成立していると考えられる。

1. 社会[1]から干渉されないこと。
2. 当人にしか知りえない情報を自分で管理すること
3. 当人が公開した情報が保護されること

が存在する。この3 つの項目がプライバシーの概念を構成すると考えられる。またこの3 つの項目を組み合わせたものとして、

4. 創造性の源泉を築くこと

が存在すると考えられる。

社会から干渉されないこと

プライベートな領域内では個人の行為に対し一方的なregulation を受けないこと、自分の信念、思想、好みなどを社会から強制的に変更させられることがないことなどが意味される。信念、思想、嗜好などをまとめて情報と呼ぶならば、個人がプライベートな領域内において所持する情報の内容は統制されることがないということを意味する。この要素の特色は情報内容自体に関わることである。

当人にしか知りえない情報を自分が管理すること

自分の信念、思想、好みなどの公開をする、公開をしないという決定を自分の意志で行なうことである。自分以外の人間により自分の好み、信念、思想などを勝手に知られないことである。自分に関する情報の流れを当人が決定可能であることを意味する。この要素の特色は情報の流通を決定すること、つまりコミュニケーションに関わることである。

当人が公開した情報が保護されること

当人が公開した個人情報を保護することである。特定の人物や集団に公開した情報について、その情報が当人の許可無く無限に公開されないということである。これはconfidentiality とよば

[1]ここでは社会という言葉の外延をひろくとり、自分以外のあらゆる個人や集団を意味することにする。

れる概念である。

confidentiality の概念を"International Encyclopedia of ETHICS"では以下のように定義している。

> confidentiality とは秘密にされるコミュニケーションの状態や特色のことであり、特定の関係における情報の公開がプライベートなまま残るという期待である。ある人がsensitive な情報を、その情報がプライベートなまま残るという信頼を持ったうえで情報を公開することである。通常、ここでのある人とはプロフェッショナルな関係においての依頼人が妥当する。
>
> 今日、多くの職業は、confidentional なコミュニケーションを公開しないことを要求する倫理的ルールを持っている。大まかにいうと秘密を守ることと同じである。
>
> その他の人々が耳にすることができるような情報はconfidential ではない。倫理的ルールは噂話までをコントロールしようと試みるものではない。職業に従事している間にプロフェッショナルに対し公開されたことだけを秘密とする。[1, Page: 180]

confidentiality はコミュニケーションの問題として扱われる。コミュニケーションにおける情報の流れを保護する概念である。典型的な例は医療情報の保護である。医師は患者の利益を損なわないために患者個人について知り得た情報を外部にもらすことをしない。個人情報の流通は当人の決定に基づき保護されるのである。

1.1.2 創造性の源泉を築くこと

この項目は上記3 つの要素を組み合わせることにより導き出される要素である。プライベートな領域は社会から干渉されることがないため、この領域内部ではパブリックな領域に遠慮することなく自由に行動することが可能となる。その結果として自発性が促進され、社会的な抑圧に従うことから個人が解放される。さらに自律性、創造性、人間関係をつくる能力、個人の責任感を発達させることになる。

このような閉じた領域では創造的な思想だけでなく、反社会的思想・行動をも生み出す危険性は当然存在する。しかしながらパブリックな領域から引き離されている領域においては、どのようなかたちであろうとも独自の信念、思想、嗜好などの創造が可能になることは保証されるといえる。

1.2 プライバシー概念における一般的な問題

プライベートな領域、自由に振る舞うことのできる領域の大きさをどのように設定するかこそが最も議論をひき起こす論点となる。プライバシーの領域を獲得するということ、つまりパブリックとプライベートの間に境界線を引くということが問題を生じさせる。境界線を引くことに伴って問題は生じてくるのであり、どこか適切な場所に境界線を引けば問題が生じなくなるということではない。

最近の話題となった事例を取り上げてみるならば、家庭内暴力があげられる。政府が家庭内の教育方針などに規制や統制を行なうのは明らかに家庭に対するプライバシーを侵害しているといえる。しかしながら子供に対し暴力を振るうことによって教育を行なうということが果たしてプライベートな事柄なのかという問題も存在する。また、自殺や安楽死にも境界線を引くことによる問題が生じる。線引きの問題は必ず起こる。それを回避することはできない以上取りうる解決

策は問題を少なくするように線を引くことである。つまり考察すべきことは線の引き場所をどこに設定するかということになる。

すでに述べたが、上記の事例に共通の要素はどこにパブリックとプライベートの線を引くかということである。家庭のプライバシーを大幅に守るように境界線を設定するならば、暴力的な教育方針に対し、家庭外部からの干渉を行なうことはできない。また暴力を禁止するかたちで境界線を引くならば、家庭の教育方針自体が統制を行なわれることになる。

表現の自由にもプライバシーを保護する側面とプライバシーを侵害する側面の両方が存在する。そして表現の自由は境界線の設定によって問題が顕著に現われる。プライバシーを保護する側面としての表現の自由を抑圧する、つまり創造的な言論や思想を抑圧するようなプライバシーの侵害に対しては通常以下のような主張が行なわれる。

> 表現された政治的視点の内容に反対という理由で政府が思想を制限するのは避けるべき悪であり、声を上げることのできない人々をも政府の力で統制してしまうこともまた避けるべき悪である。

プライバシーは守られるべきであるということの考えの基盤の一つの理由は政府による個人への干渉には非常に大きい影響力が伴うということにある。大観を持てば政府の非干渉政策こそが望ましいということになる。

表現の自由という言葉を用いたからといってどのようなことに関しても表現することを無条件に認められるべきではない。表現の自由の名の下にどのような事柄までもが表現されるのを許可するのには強い抵抗を覚える。当然一定の規制がかけられるべきである。このことはパブリックとプライバシーの線引きによってのみならず、プライバシーとプライバシーの問題ともいえる。つまり創造性の源泉としてのプライバシーによるプライバシーへの侵害である。プライベートな領域をいったん設定したならば、その領域とそれ以外との線引きが生じるのである。その際、どの表現は公共の領域において述べることが可能なのかという線引きが必要となる。境界線の引き方によっては思想を統制することになりプライバシーの侵害となる一方で、制限を設けない方針によってもプライバシーを侵害することになる。

繰り返すが、考察すべきことは線の引き場所をどこに設定するかということである。線を引く際には、ただやみくもに線を引くのではなく、またどのような線をひくのかについてもあらかじめ明らかなのではない、またある行為のどこからが善い行為、悪い行為と厳密に定められているものでもない。境界線は目的に従う仕方で、つまりなにを目的としているかにより、その目的が一番尊重されるかたちで線をひく必要がある。目的的に線を引くことによって基準が変わるのであり、許容される行為が導き出されてくるのである。

2 ネットワーク上でのプライバシー

プライバシーとは、個人の情報へ他人が接近することの制限である。なぜシステムのセキュリティーと利用者のプライバシーがコンフリクトを起こすのかという問いは、パブリックとプライバシーの線引き問題としてとらえることができる。パブリックにシステムのセキュリティーが対

応し、プライバシーには利用者のプライバシーがあてはまる。

この節では前節で取り上げた２つの道具を用いてコンピューターやネットワーク上のプライバシー侵害に関する２つの問題を取り扱う。問題は以下の２つである。

1. システムのセキュリティーに対する不安
2. システムアドミニストレーターに対する不安

前節までに一般的なプライバシーの概念を取り扱った。この節では一般的なプライバシーの概念をネットワーク上に適用することを試みる。ネットワーク上一般におけるプライバシー概念について考察した後に教育機関におけるプライバシーの概念へと議論を移行する。一般的なプライバシー概念をネットワーク上に適用すると、以下のようになる。

システムアドミニストレーターは正当な資格を持つ(公認された) 利用者(市民) がコンピューター、ネットワーク上に保持する情報[2]の内容についてregulation を行なうことはせず、どのような情報を持つべきかということについての干渉を行なうべきではない。また知りえた情報について本人の同意無く外部に公開すべきでない。

2.1 セキュリティー自体の不安

セキュリティーとは「正当な資格を持つ利用者に対し、コンピュータやネットワーク、さらには情報システムや情報サービスなどを安心して利用できるようにする[2, Page: 3][3]」ことであり「情報システムや情報サービスといった(システムが保持する) 情報に対する(システム外部からの) 様々な脅威から情報が守られ、安心して利用できる環境を実現する[2, Page: 3][4]」ことである。

ネットワーク上における情報の取得、漏洩などの問題は、比較的容易にしかもかけるコストも少なく大量の情報を手に入れられることから生じる。誰についてであれ、ある人物についての非常に大量な情報を容易に集めることができ、その情報が第３者によって保管され、所持され、回収されることが可能となる。

この不安は「当人にしか知りえない情報を自分が管理すること」というプライバシーの要素の侵害に対する不安となっている。この不安を取り除くことは難しく、解決を図るには長期的な視点を持ち対応を行なうことが必要である。しかしこの問題の根は深く、この問題については本稿では問題の指摘だけにとどめることにする[5]。

2.2 システムアドミニストレーターに対する不安

---

[2]一般的なプライバシー概念における信念、思想、嗜好などを総称して情報とする。

[3]文脈の都合上一部改変した

[4]括弧内は筆者により追加

[5]セキュリティーの不安は技術的なシステムの堅牢性の問題であると考えることができる、と思われるかもしれない。そうではないということは次の点を指摘することで明らかだろう。それは、システムの堅牢性は一つは技術的な側面、もう一つは規範的な側面に依存しているのという事実である。

1. 技術的な側面： 脚注 6 の各項目に対応させた技術を開発することでセキュリティーを向上させることが可能となる。
2. 規範的な側面： 教育により高めるものである。利用者にたいしてシステムに対するセキュリティー意識を向上させる教育や倫理的な教育の両方を実践することによりシステムのセキュリティーを向上すること。この両者がそろってはじめて安全なシステムになるということは明らかであろう。

コンピューターならびにネットワーク管理を行なう上で最も重要なことはシステムの把握[6]である。システムの把握のために大学が行なうとされている項目はいくつか[7]存在する。

それらの管理業務を行なう場合、アドミニストレーターは利用者の個人情報を知ることになる。電子メールの内容、また電子メールの交換相手、利用者が頻繁に訪れるweb サイト、作成するファイルの内容などを付随的、意図的に見ることになる[8]。ネットワークの使用に不安を感じる要素の一つはここに存する。つまり自分の保持する情報をセキュリティーのために勝手に覗かれるという不安である。これは「当人にしか知りえない情報を自分が管理すること」と「社会から干渉されないこと」という２つのプライバシーの要素の侵害への不安である。

「当人にしか知りえない情報を自分が管理すること」への侵害に対する不安は比較的容易に取り除くことができる。システムの利用を認められている利用者がコンピューターやネットワーク上に保持している情報に対しconfidentiality の概念を適用すればセキュリティー管理上のプライバシーの問題は原理上解決される。confidentiality の概念を適用された情報に対して、アドミニストレーターは知りえた情報について情報の所有者のプライバシーを尊重する必要があるからである。

実際にアメリカの大学におけるコンピューターやネットワーク使用に関するポリシーでは、たとえばインディアナ大学のポリシーを引用すると「一般に、コンピューター上に保管されている情報はconfidential であると見なされる。たとえその情報がコンピューターのOS によって保護されている、いないの如何によらない。ただし情報の所持者が他のグループや人々に対し、意図的に公開可能な状態にしている場合は除く。(中略) IU computing center はコンピューター資源上に保管されているすべての情報のco_dentiality を擁護する。[9]」と述べられている。

以上のことからネットワーク使用時にはプライバシーの制限が行われることが明らかになった。ネットワーク上でパブリックとプライバシーの線引きをどこで行うかについては次のような例も考えられうる。つまりパブリックとプライベートの両端で線を引く場合である。一つは全ての内容を規制する立場、もう一つは完全に何も規制をしない立場である。それは、プライバシーのためにシステムの堅牢性、信頼性を制限するというものである。プライバシーを保護するためにネ

---

[6]セキュリティー技術はセキュリティー対策の時間軸に沿って 6 項目存在する。

1. 分析・予測(analysis & assessment)
2. 予防(remediation)
3. 検知(indications & waring)
4. 被害軽減(mitigation)
5. 応急対応(response)
6. 再構築(reconstitution)

[2, Page: 4] 本稿ではこの 6 項目の対策を行なうことをシステムの把握として取り扱う。

[7]項目数は大学によって異なっているので明確な数字を述べる事はできない。

[8] K-State Information Technology Usage Policy には、正当な資格を持つ利用者のファイルにアクセスする場合が記載されている

1. ハードウェアやソフトウェアのトラブルシューティング
2. システムの誤った使用や非権限アクセスの防止
3. ビジネスに関連する情報の検索
4. このポリシーや州法、連邦法の侵害の報告にもとづく調査
5. 情報提供を求める法的請求に従うこと
6. 配達できなかったメールを再配達もしくは廃棄する

[9] “Computer User's Privileges and Responsibilities", The Trustees of Indiana University, 1997, URL:http://www.indiana.edu/ uitspubs/iu001/ (2001 年 3 月には参照可能)

ットワークの提供者が利用者に対し一切の干渉を行なわず、起こりうるすべての責任を利用者に負わせるというポリシーを持つことを考えることも可能である。実際にどのような方針をアメリカの大学が採用しているのかを次節から取り扱うことにする。

3 大学におけるポリシーステイトメントの分類

本節では、主としてアメリカの大学におけるコンピューターおよびネットワークの利用に関する方針、指針を述べる文書(以下、「ポリシーステイトメント」とする) の検討を行なう。ここでの目的は、概念的に混乱が見られるとされる情報化社会における倫理規範についての対応のパターンを明らかにすることである。この検討によって、アメリカの大学におけるポリシーステイトメントと考えられるものには4 つのタイプが存在することを明らかにする。すなわち、

1. コンピューターの使用法を説明するもの
2. いわゆるネチケットを列挙するもの
3. 大学の定める義務、権利などを述べるもの
4. コンピューターやネットワーク管理の規定を述べるもの

の4 種類である。とくに第3、4 番目のタイプについて詳細に検討して、プライバシーとセキュリティとの関係が重要な問題となっていることを示す。それぞれのタイプについて特徴的な文章を引用し、この分類の妥当性を示す。

またプライバシーの観点を考慮して倫理学的に分析することによって、現在のアメリカの大学という状況における情報倫理の実情を解明する。ただし、重要なこととして、本節の目的はコンピューター利用に関する新たな規範を導き出すことではないということがあげられる。したがって、本節の目的は、本格的考察への準備作業として、あくまで現在のコンピューター利用についての規範意識の傾向性についての考察にとどまるものである。

3.1 調査の方法

この調査では、主としてアメリカの大学を対象とした。アメリカの大学の数は1500 に近く、Yahoo USA に登録されている大学の数は1476 (4/19/00 現在) である[10]。今回の調査においては、Yahooに登録されているすべての大学について、ポリシーステイトメントに関連する文書が存在するか否かを点検し、それが存在するときには、その文書の内容を検討した。点検した1476 大学中、そのような文書をオンラインで保持し、外部からのWorld Wide Web による閲覧を可能としていた大学の数は、381 大学である。ただし、そのような措置がとられていたるもかかわらず、リンクの不在､配置の複雑さゆえに該当文書に到達できなかった場合もあると考えられる｡381 という数字は見落としを考慮しても少ない数字である。このことはアメリカの大学に関して、コンピューター資源の利用に関する自覚的な対応がどこでもなされているわけではないことを示している。

[10]分校も一つの大学として数えた。University of California, Berkerey と University of California, Riverside は別の大学として扱った。

3.2 ポリシーステイトメントの4 階層

調査の結果、何らかのコンピューター利用に関するポリシーを設定している大学が相当数存在することが判明した。内容の種類によってでそれぞれのポリシーの分類を試みると4 つの階層に分かれると考えることができる。その種類は以下のとおりである。

1. コンピューターの使用法を説明するもの
2. いわゆるネチケットを列挙するもの
3. 大学の定める独自の義務、規定を述べるもの
4. コンピューターやネットワーク管理の規定を述べるもの

この分類が妥当であることを傍証する事実は存在する。すなわち、4 のパターンに属するポリシーステイトメントを持つ大学は、1、2、3 のパターンの文書も公開し、4 のパターンの文書を持たないが3 のパターンの文書を持つ大学は、1、2 のパターンの文書も公開し、3、4 のパターンの文書を持たないが2 のパターンの文書を持つ大学は、1 のパターンの文書は公開しているという関係が観察される。つまり上記の分類においてコンピューター管理の規定を述べている大学においては、その他の項目、ネチケット、コンピューターの使用法などについて言及し、また規定を設けており、たとえばUniversity of Maryland が公開しているポリシーは”Computer Use Guidelines" “Guidelines for Acceptable Use of Computing Resources" ¥Policy and Ethics" などを含んでいる。逆にネチケットまでの規定を設けている大学では、詳しい利用規定は設けていない。同様に利用規定を設けている大学がコンピューター管理の規定について明確な項目を持っているわけではない。つまりこの4 つのパターンは階層構造をなしているのである。

なお、「コンピューターの使用法を説明するもの」を公開している大学でも、すでに明確になっている一般社会での法の適用を参照している場合は多い。しかし、独自の文書を保持していない場合には、その大学を「コンピューターの使用法を説明するもの」のみの文書を持つものとして分類した。一般社会における法の適用とは、たとえば、著作権[11], 登録商標[12]等の侵害に対する罰則の適用であり、それらには従わなければならないと明記している。この条件はすべてのパターンにも同様に当てはまる。

各項目における大学数はパターン1 では2 校、パターン4 では17 校存在した。パターン2 、パターン3 の明確な区別を行なうことは、顕著な例を除いて困難であるため、残りの大学はネチケットと大学独自の規定を有しているといえる。このことからは、情報倫理とネチケットが混同されていると述べることもできる。

3.2.1 コンピューターの使用法

パターン1 について述べる。このパターンに属するポリシーステートメントを持つ大学は、2 つあった。それはコンピューターの問題をソフトウェアの問題として取り扱うこと、つまりコンピューターの使い方を大学でのコンピューター利用の方針としているものである。その具体例は

---

[11] この問題については次の URL がしばしば参照されている。http://lcweb.loc.gov/copyright/ (2001 年 3 月には参照可能)

[12] この問題については次の URL がしばしば参照されている。http://www.uspto.gov/web/menu/tm.html (2001 年 3 月には参照可能)

University of Alaska, Anchorage[13]である。

1. Introductory: Topics Getting Started
2. E-mail: Pine, Netscape, Outlook Express, Eudora
3. Internet: Connecting to the internet, FTP, Telnet

項目は以上のように分かれ、Introductory にはコンピューターの使用法、E-mail の項目にはそれぞれのアプリケーションの使用法が述べられている。また、Internet の項目にはWeb browser, Telnet, FTP の使用法が述べられている。

しかし、もはや大半の大学では規範的な内容を持つ文章なしには、キャンパス内におけるコンピューター資源の利用についての指導はできなくなっていると考えられる。

3.2.2 ネチケット

パターン2 とはネチケットをポリシーと考えることである。それらのポリシーは"User Netiquette(University of Rochester[14])" 、"Internet Etiquette(Swarthmore College[15])" と呼ばれることが多い。Swarthmore college における規定の具体的な内容を以下に記す。

1. メッセージを送る場合には言葉を慎重に選ぶこと
2. 送信する前に単語や文法の間違いを確認すること
3. 題名はメッセージの内容を的確に述べること
4. Signature は短めにすること
5. メッセージの一行は７０文字以内にすること

などである。これ以外にも、大学によってさまざまに細かい項目が列挙されている。ネチケットはコンピューターを利用する際、他人に迷惑をかけないための指針としては効果を発揮するものである。しかし、そのような迷惑は、かならずしも人々の権利を直接に侵害するものではなく、法的規制においてもそれほど重要視されることもない。また、訴訟が行なわれることもほとんどないものである。

ネチケットではRFC1855 がしばしば参照され、より多くの項目を列挙することは可能である。しかし、すでに述べたようにネチケットだけを有する大学は少なく、より多くの義務、権利の表現を伴うものが多い。

3.2.3 大学の定める義務や規定

パターン3 とパターン2 を厳密に区別することは困難であるが、この調査では、基本的な原則を定めそれに従いより細かな項目をあげる形式をもつものをパターン3 とした。これは、ネチケットがしばしば、根拠、原則の一貫性を欠いた徳目の羅列にとどまることを考慮して、そのような一貫性の認識が存在することが重要であると考えたからである。

さらに、ポリシーに抵触した場合の処分をどうするかという項目で場合分けを行なうことも必要である。ポリシーにはプライバシー、メールの使用に関するもの、ウェブの内容についてなど

---

[13] http://www.uaa.alaska.edu/helpdesk/docs/ (2001 年 3 月には参照可能)
[14] http://www.rochester.edu/UCC/UNIX/sysinfo/usr-agrmt/user-etiq.html (2001 年 3 月には参照可能)
[15] http://www.swarthmore.edu/cc/docs/netiquette.html (2001 年 3 月には参照可能)

が述べられている。また、メールの使用、WEB の作成などコンピューター資源の利用は、権利として認められているのではなく、特権として与えられているにすぎない。

これらは”Acceptable Use Policy(Manchester College)",”Internet Acceptable Use Policy(Lee College)",”Network Policies(Austin College)" ,”Appropriate Use of Computing Resources(University of Alaska)" などとさまざまな名称を持っているが、内容は概して一致しているとみなすことができる。具体例としてCarnegie Mellon の"Policies and Guidelines[16]" を引用する。このポリシーにおいては、プライバシーと資源の公平な共有(fair share of resources) とを基本的な原則と定め、それぞれについて項目を挙げている。

1. プライバシーについて
   1. 利用者には一つのID が与えられる。それを他の誰も使うことはできない
   2. ファイルやディレクトリーはプライベートなものと見なす
   3. メッセージの送信者は特定されなければならない
   4. コンピューターなどの資源を利用した記録はプライベートなものとする
   5. ネットワーク上のデータの流れはプライベートなものである
2. 資源について
   1. 他の利用者の行なうことを邪魔したりシステムの破壊を、派生的にでも行なうべきではない
   2. システムのバグを知っていたり、特別なパスワードを持っているからといってシステムを改造したり他の利用者の資源を手にいれるために使うべきではない
   3. 大学の資源は大学における目的のためにある。商用や個人の資産獲得のために使用する場合には大学の許可が必要である

大学の設ける義務、規定を破った場合には制裁が加えられる場合がある。罰則を明確に公開してある具体例としてUniversity of Illinois, Chicago[17]の罰則規定は以下の通りである。

1. 最高1 週間、最低3 日間のアカウントの停止
   - チェーンメールを送った
   - 相手が望まないメッセージを送った
   - 商用目的の使用
2. 最低3 ヵ月のアカウントの停止
   - 他人にアカウントやディスクスペースを貸す
   - 他人のディスクスペースを使う
3. 最低6 ヵ月のアカウントの停止
   - 盗んだアカウントを使用する
4. 最低1 年のアカウントの停止
   - コンピューター資源の悪意ある使用法をまねる
5. 上記の罰則に加えるさらなる罰則
   - 著作権を侵害した際の法律の適用

[16] http://www.cmu.edu/computing/documentation/unix/Policies.html (2001 年 3 月には参照可能)
[17] http://www.uic.edu/depts/adn/policies/abuse.html (2001 年 3 月には参照可能)

{ 違法な使用に対する罰金
{ 学生の行動規範にある罰則規定の要求を行なう

3.2.4 管理の規定を述べるもの

パターン4 をパターン3 から明確に区別するものは資源管理への言及である。資源管理について言及している大学の数は17 ある。コンピューターやネットワークの保守、点検、維持を行なうのは管理者の業務であり、その業務にも指針、方針が必要である。また利用者にはどのような管理を行なうかをポリシーとして知らせる必要があるとこれらの大学は考えている。ゆえにこの分類を権利関係へ言及しているものとして取り扱う。

細かい規定を明記しているカリフォルニア大学機構(University of California) におけるE-mail Policy を参考例として挙げる[18]。

1. 導入
2. 目的
3. 定義
4. 一般的な規定
5. 個別の規定
   A. 許可される使用法
   B. セキュリティーとコンフィデンシャリティー
   C. 保管や保存
6. ポリシーの侵害
7. ポリシーに対する責任
8. Campus Responsibility for Policy

我々が注目すべき点は5.B である。この項目ではE-mail における利用者のプライバシーについての記述と、コンピューター資源を管理する場合には利用者のプライバシーを尊重し思慮深く行動する必要があるということが述べられている。さらに、管理を行なう際には利用者のプライバシーを侵害するおそれがあるが、管理者は利用者のプライバシーを考慮するとしている。管理の観点を考察に入れることによりプライバシーの問題の複雑性が明らかになる。

3.3 プライバシーと匿名性

カリフォルニア大学機構の例からわかるように、プライバシーの保護は大学における情報管理において重要な課題である。アメリカの大学においてこの点について厳密かつ正確なところが比較的多いという事実は、アメリカの立法政策にも由来すると考えられる。すなわち、学生のプライバシーは連邦法によって守られており、学生個人の情報を公開するにはFERPA(Family Educational Rights and Privacy Act of 1974) に抵触してはならない[19]とされているからである。FERPA とは、大学によって管理、保持されている個人が特定されうるような学生の教育などに

[18] E-mail Policy は次節で詳しく取り扱う。
[19]以下の記述は http://www.wmc.car.md.us/HTMLpages/Administration/Registrar/FERPA.html (2001 年3 月には参照可能)

関する記録[20]を保護する特権、権利を学生に対し認めるものである。そして学生の同意が無ければ情報の公開は行なってはならないと定めている。しかし学生の同意が無くとも個人情報を公開する例外事項が存在する。

1. 記録に正当な教育的関心を持っている学校関係者への公開。
2. 州や連邦政府によって運営されている教育プログラムの関係者への公開。
3. 裁判所命令もしくは合法的な召喚令状に従う場合。ただし前もって学生にその旨を伝える努力がなされた場合。
4. 健康や安全の非常事態の際に適切な団体への公開。
5. 認定された機能を実現するために、認定された組織が情報を必要になったときに、認定された行為者への公開。

学生は入学時にDirectory Information を公開するかどうか[21]への同意が求められる。学生の同意が得られない場合には大学側はこれらの情報を公開することはできない。また、学生の持つプライバシーの権利は大学へ提出した書類だけではなく、コンピューター上で使用しているファイル、コンピューターの利用記録、ディレクトリーの中身にまで及ぶ。この項目はほぼすべての大学に存在している。

大学においてコンピューター資源を利用する際には、アカウント作成のための書類を提出することが原則である。それはコンピューターを利用する人間が、大学の構成員であり、そのことが追跡可能であることを保証するために行なわれることであろう。このような手続きは、利用者側からみるならば、大学の定める義務、権利を遵守するとの宣誓に相当し、大学側から見てみれば責任帰属の主体を明らかにし、電子社会での存在(ユーザID) と実社会の存在(学生個人) との対応を明示化することである。このような行為がほぼつねに要求されるということの意味は、哲学的には電子社会への参入がロックの意味でのtacit consent を帰結しないということである。

Reed College のStudent User Agreement[22] を以下参照する。

1. 提出書類に署名がなされた場合にのみコンピューターの使用は許可される。
2. コンピューターは学問と教育のためにのみ使用される。
3. コンピューターは商用もしくは非営利組織を支持するために利用しない。
4. 利用者は違法な目的のために大学のコンピューター資源を利用しない。権限を持たずに商用のソフトウェアをコピーするのは違法である。
5. 利用者は大学の仲間やインターネットコミュニティーの仲間の権利を配慮する。

その他いくつかの条項があるが、それらの項目の遵守を誓うならば、名前、学生番号、署名と日付を書き入れることによってアカウントの発行が行なわれる。

調査の際に興味深かった点は、原則としてどの大学も匿名のコンピューター利用を許可していないという点であった。

---

[20] Educational Records と呼ばれる。
[21] Directory Information とは学生の名前、誕生地と誕生日、専攻する学問、公式に認められた活動やスポーツへの参加、出席日数、学位や賞の授与、最も最近出席した学会などを意味する。この内容が Educational Records である。
[22] http://www.reed.edu/webdoc/reedspec/student.agree.html (2001 年 3 月には参照可能)

匿名を許可しない理由について、University of California, Berkeley 校では上述のカリフォルニア大学機構のポリシーに加え、finger[23]に関する規定[24]において次のように説明している。

大部分の人はfinger をdirectory service として使っている。なかには「実名」を表示する部分を創造的な自己演出を行なうものだと見なしている人もいる。残念ながら偽名を使う誘惑に堪え難い人も存在し、実名を隠すことは計算機資源の悪用へと導くことになる。

UCLink でのアカウントを取得するために利用者は自分が自分であると証明したのと、多くの人が大学での研究を行なう目的でfinger を用いていることから、ログイン名と利用者の実名を結びつける方針をつくった。

この文言は、finger サービスに限らず、コンピューター利用の匿名性を認めてしまうと、誰がネットワークのトラフィックを生じさせているのか、spam メールを送っているのが誰なのかを特定すること、またソフトウェアのコピーを行なっている利用者を特定することなどが困難になり、結果として大学が定めたポリシーが機能しなくなると考えていると解釈することが可能である。すなわち、匿名性を認めることによって、電子社会では責任の帰属が行なわれないことを帰結してしまうことを恐れているともいえる。逆に大学がすべての責任を負うということで、匿名を許可できるかも知れない。しかし、その場合大学そのものがより大きいネットワークあるいは一般社会から接続を拒否されることになるだろう。このような理由から、ほとんどの大学ではアカウントを作成する際には匿名を許可していないと考えられる。

一方、教職員の個人情報については、公開を原則としているところがほとんどである。アメリカの大学において情報公開するときには教官の所属、内線番号、部屋番号など連絡をとるための情報は公開されている。ほとんどの大学ではウェブのトップページに“ directory search"を設置しており、名前もしくは所属を入力するだけですぐに情報を手に入れることができる。それらの情報はいわば公的なものであり、公開することはその職業に従事することの責任の一部であると考えられている。ちなみに日本の大学を見てみると、研究者の著書、研究分野などについて細かく載せているが、その研究者への連絡方法は掲載されていない場合がほとんどであった[25]。

3.4 セキュリティーとプライバシー

セキュリティーとプライバシーの間にはトレードオフの関係が成り立っている。このことは、次のようなことを意味する。システムの管理者は、システムを維持するためにシステム全体に何が起こっているのか、また利用者が何を行なっているのかを詳細に把握する必要がある。そのためには誰がどのようなファイルを所持しているか、誰がいつ何を行なったかを知る必要がある。ここで、学生の個人情報がシステムを管理する上での問題となってくる。なぜなら学生の利用者のファイル、利用記録、ディレクトリーの内容は学生の個人情報に該当し、学生の許可無しには閲覧することが許可されていない行為だからである。大学のコンピューター利用の制限や方針を

---

[23] finger とはローカルユーザーやリモートユーザー情報を表示するコマンドである。具体的にはログイン名、フルネーム、ログインしている場所、ログインしている時間などが表示される。

[24] http://www-uclink.berkeley.edu/policies.html (2001 年 3 月には参照可能)

[25] しかし研究者の検索が行える大学は進んでいるといえる。多くの国立大学を見てみても研究者の検索を行えるところはほとんどない。あるのは研究業績の検索である。さらに奇妙なこととして研究業績の検索を学外用と学内専用に分けているところも存在した。

設定する際の問題は、学生の個人情報をどのように取り扱うかということである。

この節では全体的な傾向性を見ることに重きを置いているので、ここで制限されているプライバシーとはどのような意味合いのものなのかは次節でポリシーの分析を行なう際に明らかにする。

4 パターンの分析調査

この節ではパターン4 の分析とまとめを行なう。前節での分析で明らかなようにパターン4 にはパターン1 からパターン3 までの全ての項目が内包されている。よってこの節ではパターン4 のまとめを行ない、パターン4 の特徴である大学の管理規定をプライバシーの概念から分析することによって現在の倫理的規範を明らかにする。

パターン4 をまとめると以下の6 つの項目へと分類[26]することができる。

1. 適切な利用のガイドライン
2. ネットワーク使用の責任
3. E-mail のポリシー
4. Web 作成時の注意点
5. Obscene Material への大学の対応
6. 管理方針の説明

この6 つの項目と17 の大学の対応表は以下のようになっている。

	1	2	3	4	5	6
Indiana University	○	○		○	○	
Kansas State University	○		○	○	○	
Ohio University	○					
Reed College	○	○		○		○
St. Cloud State	○	○	○			
University of Arizona	○		○			○
University of California.			○			
UC Berkeley	○	○	○			○
UC Davis	○					
University of Delaware	○	○	○			○
University of Florida	○		○			○
University of Iowa	○	○	○			
University of Maryland	○	○				
University of Michigan	○		○		○	○
University of Minnesota	○	○	○			
University of Missouri	○	○				○

[26] この分類は厳密に述べるならば正確なものではない。それぞれの項目はそれぞれ重なっている部分が少なからず存在する。しかしながら特徴的な部分を列挙した結果、このような分類を行なえた。

University of Virginia　○　○　○　○　○

4.1 適切な利用のガイドライン

この項目の目的は、コンピューターやネットワーク資源を使用するにあたり、適切な利用法を述べることである。この項目と次の項目である「ネットワーク使用の責任」とを明確に区別するのは困難であり、双方で重なっている部分が多々ある。たとえば大学のコンピューターやネットワークを利用してゲームで遊ぶことについての記述は双方に見受けられる。しかしながら「ネットワーク使用の責任」では義務や権利にもとづき、それらを自覚しつつコンピューターやネットワークの利用を求めているのに対し、ガイドラインにおける規定は主に適切な利用の方法を述べているという点で異なっている。つまり、事実の問題であるコンピューターの使い方、または明確な義務や権利によって構成されているわけではないネチケットなどから構成されているのである。具体的には以下の項目が挙げられる。

1. ガイドラインの目的
2. コンピューターを使用できる人についての説明
3. コンピューター使用に際しどのようなポリシーに従うかについての説明
4. どのようにコンピューターを使用するのかについての説明
5. ポリシーの侵害を報告する方法の説明

4.1.1 ガイドラインの目的

特徴的な例としてOhio University におけるガイドラインの目的を引用する。

ポリシーの目的は既存の法律、規則、協定、契約を補完するものとして意図されている。

ここではガイドラインの目的、ならびにコンピューターやネットワークに関する一連のポリシーの位置づけを述べ、利用者に対し公開している。なぜすべてのポリシーを明示化し、利用者に同意を求めるのかについては次のように考えることが可能である。すなわち、電子社会では利用者が参入する電子社会における規範やルールを暗黙の内に受け入れてしまっていることがないように、つまりtacit consent を帰結しないように全てを明示化することが必要であるという判断により、利用者に対しすべてのポリシーが公開されているとみることができる。また一方では、このことは現在の電子社会において統一的、包括的な法の体系が出来上がっていないことや、行為主体と責任を帰属する主体との同定の困難さなどを原因として行なっているad hoc な対応とも見ることができる。

4.1.2 コンピューターを使用できる人についての説明

多くの大学において、コンピューターやネットワークの使用は、教育、研究、大学のサービスのため、そしてこのポリシーに従う仕方でなされる必要があると基本方針が述べられる。また、コンピューター資源を利用可能な権限ある使用者とは

1. 教員、スタッフ、学生
2. 公的情報サービスから大学へ接続しているもの
3. 大学の使命を増進させるようなもの

であると規定される。

4.1.3 コンピューター使用に際しどのようなポリシーに従うかについての説明

全ての大学では、受けいれられる使用方法は既存の大学のポリシー、ガイドライン、行動規範に従うものであると規定している。

4.1.4 どのようにコンピューターを使用するのかについての説明

特徴的な例としてSt. Cloud State University のポリシーを引用する。

1. E-mail で送られるメッセージは実体を持った文章や道具と同じであるかのようになされなければならない。
2. 共有されたネットワーク資源の限界に敏感であるべき。どのようなコンピューターシステムもアクセスを妨げることはできない。SCSU はE-mail の内容を統制することに興味はないが電子ドキュメントのプライバシーや秘匿性は保証できない。
3. 他人の権利を尊重すべきである。
4. ネットワークの本来意図された利用をだめにする、もしくは妨害する利用をしないこと。大学の目的に沿うような利用を行なう。
5. public oÆce(連邦、州、地方のいづれでも) の候補者の支持を行なってはならない。
6. E-mail やその他のネットワークリソースは商用に使われてはならない。使用した場合にはMinnesota 州法違反になる。

4.1.5 ポリシーの侵害を報告する方法の説明

ここではUniversity of Florida のポリシーを引用する。

> コンピューターのすべての利用者、利用団体は非権限アクセスを発見したならば報告すべきである。報告先は"Vice Provost for Academic Services and Technology","Director of Computing & Network Services" もしくは適切な管理者へ。

4.2 ネットワーク使用の責任

大学はこのポリシーを"Who Owns What ?" という問いかけを用いることにより、コンピューター資源の利用者がコンピューター資源に対しアクセスする権利を持つのではなく、ある意味特権を与えられているのだ、と述べる。別の表現では、「特権」は「アカウントに対する排他的アクセス」と述べられている。つまりアカウントを利用する機会を与えられているということである[27]。この特権にまつわる義務、責任などを列挙する。列挙される項目は他に、E-mail 使用時のエチケットやプライバシー、悪意を持った利用についての規定、ホームページについてなどがある。これらはすべてネットワークを使用する上で生じてくる義務や責任について述べている。

1. コンピューター資源へのアクセスにまつわる義務、権利
2. 権利関係に言及したコンピューターの使用法

[27]特権に関する規定は管理方針の説明の中で行われている。ここで述べられていることは、この特権にふさわしい行為についてである。

{ 倫理的使用法
{ 法律に適う使用法
{ セキュリティーを守る使用法

4.2.1 コンピューター資源へのアクセスにまつわる義務、権利

このポリシーは利用者に対しコンピューターにまつわる義務や権利の枠組を述べるものである。ここでは2 つのポリシーの一部を引用する。一つはUC Davis、もう一つはUniversity of Florida のものである。

コンピューター資源へのアクセスは大学の教員、スタッフ、学生に与えられている特権である。大学外への個人にも大学の研究目的のためにそれらへのアクセスは保証されている。この特権にはある種の責任が伴う。そして利用者はそれらを理解することが重要である。教育、研究、公的サービスという大学の目的に沿うようにコンピューターやネットワークは存在するのである。(UC Davis)

学問の自由と表現の自由の権利はコンピューター資源の利用にも当てはまる。それゆえこれら権利への責任と権利への制限もまた同様にあてはまる。技術的に可能などのようなことにもまでそれらの使用が拡大されてはならない。(University of Florida)

4.2.2 権利関係に言及したコンピューターの使用法

ここでは全ての利用者に対し、プライバシーの権利を尊重し、倫理的に振る舞い、他者の所有する情報の使用についての法的な制限に従わなければならないことを述べている。ここで使用されている「倫理的」の意味とは、他者に害を及ぼさない限り利用者が権利の主張を行うことを認めるというものである。以下St. Cloud State University における実際のポリシーとパターン4 におけるこの項目をまとめたものである。

このガイドラインは学生、教員、スタッフ、大学に所属しない利用者、大学の所有するコンピューター、設備に適用される。

1. 州法、連邦法によって禁止されているアクセスは禁止されている
2. 州法、連邦法によって禁止されているアクセスをサポートすることは禁止されている
3. 権限を認められていない人物が買収したアカウントを使用したとしてもその人物に権限を認めるわけではない。

非権限アクセスや使用によってアカウント保持者に損失を招くものは、データ、プログラムなどを復旧することのコストに対する責任を必ず持つ。大学関係者はdisciplinary action の対象となり、大学関係者を含め全員Minnesota computer crime status の対象となる。(St. Cloud State University)

その他の大学におけるポリシーをまとめたものが以下である。

倫理的使用法

1. 大学便覧や学生向けの倫理的行動規範に記述されているような大学の構成員として標準的

な倫理に適うような利用をすべき

2. コンピューターシステムのセキュリティーの侵害
3. アカウントの不正利用
4. 必然的に他人の妨害をすることになる行為
5. 大学の目的に沿わない利用
6. ソフトウェアアグリーメントの侵害
7. ネットワーク利用のポリシーや規則の侵害
8. 他人のプライバシーの侵害

法律に適う使用法

1. 非合法な目的のためにコンピューターやネットワークは使うべきでない
2. 他の利用者への意図的ないやがらせ
3. 備品やソフトウェアの破壊
4. 電子的コミュニケーションの非権限モニタリング
5. ソフトウェアのコピー

セキュリティーを守る使用法

1. 利用者はコンピューターシステムがセキュリティーと秘匿性を維持するように正しく使用する責任がある
2. アカウント、パスワードは個人に割り当てられた特権であるから他人とは共有しない
3. 頻繁にパスワードを変更し、わかりづらいパスワードにすること
4. ウイルスに気をつけ、被害者になること、知らずに加害者になることを避ける
5. コンピューターシステムは自動的にファイルに対し保護をおこなうことを利用者は知ること。必要ならそれを補完しセキュリティーを向上させること

4.3 E-mail のポリシー

この項目はE-mail を大学がどのように取り扱うかについての方針を述べている。E-mail には大学のポリシーや法律の適用されることを明言し、E-mail のプライバシー、E-mail に対するセキュリティー、E-mail がPublic Record として取り扱われること、E-mail に対する大学のアクセスなどについての規定を述べている。各大学がE-mail に対し適用すると明記している法は Electronic Communication Privacy Act of 1986(Title 18. U.S.C section 2510 et. seq)[28]である。

4.3.1 E-mail のプライバシー

E-mail のプライバシーについては以下のように述べられている。具体的な例としてSt. Cloud State University とKansas State University のポリシーから一部を引用する。

> E-mail の本性として、物理的にメッセージの安全は保証できない。それゆえ公的でないメッセージを含むようなメールは送信しないことを勧める。大学の所有するシステム上にデータがある場合、それは¥Minnesota Government Date Practice Act" の対象となる。メッセージ

[28] URL: http://www.cpsr.org/cpsr/privacy/communications/wiretap/electronic commun privacy act.txt (2001 年 3 月には参照可能)

の内容により、そのメッセージが公的なものか私的なものかは決定されるが、基本的にはすべてのメッセージは公的なものとして見なされる。SCSU は常にメールを監視しているわけではないが、大学のポリシー、法の侵害、安全性の侵害が行なわれていると考えられるときには大学は権利としてモニターを行なう。(St. Cloud State University)

プライバシーは最大限に保護されるべきである。しかしながら、現在のコンピューターのセキュリティー上の観点から考えた場合には、大学内のコンピューター資源上にあるデータにプライバシーを期待することはできない。(Kansas State University)

上記の2 つのポリシーから理解されることは、E-mail の秘匿性は保証することができないというものである。完全な秘匿性は、既存の法律や大学のポリシー、また現在のコンピューターの技術を理由として保証することはできないというのがE-mail に対する大学のとる態度の傾向性である。

しかしだからといってプライバシーを無視しているのではない、逆に保護しようとしているように見受けられる。University of California の「E-mail Policy 」の導入部分には次のように書かれている。

大学は、学問の自由、言論の自由、情報のプライバシーの原則が電子メールや電子メールサービスにもあてはまるものだと認識する。電子メールのプライバシー保護を手紙や電話のコミュニケーション保護と同様のものとして提供する。

さらに、ネットワークやコンピューターのオペレーターが職務中にE-mail サービスの配送状況について監視しているが、E-mail の内容を意図的に見たり検索したりすることは禁じられていると明記されており、大学がE-mail にアクセスする場合の細かい規定も定められているからである。

4.3.2 Public Record としてのE-mail

ほとんどすべての大学ではE-mail をPublic Record として取り扱うと明記している。つまり外部からの要請があった場合にはE-mail の内容を公開するということである。そして各大学では閲覧に際しての条件が存在する。

University of Florida の場合では、E-mail はPublic Record として取り扱い、”Florida public record law(Chapter 119)" に従うとする。公的な仕事に関わるE-mail はpublic record law の対象となる。Puclic Record の対象となったメールは個人によっては削除することができない。ただし、Public Record の対象としないものは以下のものである。

1. Florida 州法において秘匿性があるとされている個人情報を含んでいるもの
2. “Directory information" を除く学生の記録
3. ある種の研究の記録

メールが閲覧される前に上記の条件に当てはまる部分はメールの本文から削除される。また、Kansas State University の場合では、「電子メールは¥Kansas open record act" や他の法による公開の対象となる」と明記している。

4.3.3 E-mail に対する大学のアクセス

E-mail に関するポリシーを持つすべての大学は電子メールの使用を推奨し、利用者のプライバシーを尊重すると述べている一方、以下の理由により大学内のコンピューター資源上にあるメールやデータはアクセスされることがあると利用者に注意する大学も存在する。Kansas State University をその例として挙げる。

1. ハードウェアやソフトウェアのトラブルシューティングのため
2. 非権限アクセスやシステムの誤った使用を妨げるため
3. 仕事に関係する情報を検索するため
4. 大学のポリシー、州法、連邦法の侵害を調べるため
5. 情報公開のための法的な要求に従うため
6. 配送できなかったメールを再配送、処理するため

しかし、また同時に大学がメールにアクセスすることに対し制限を設けている場合がほとんどである。カリフォルニア大学機構では大学が利用者のメールにアクセスを行なうことに関して条件を付している。

1. Authorization： 緊急の場合以外には前もって副総長か副学長による書面による承認が必要となる。
2. 緊急の場合：時間こそがもっとも大事な時であり、行動が遅れた場合にはさらなる状況へと陥る場合。しかし後から適切なAuthorization が要求される。
3. 通知： 大学のとった措置とその理由を個人に必ず通知すること。
4. 法に従うこと： 大学のとった措置は完全に法や大学のポリシーに適合しなければならない。つまり、大学は法的な措置以外では利用者の同意無しでは定期的な調査、監視、電子メールの公開などは行なわないのである。

4.3.4 E-mail の保管や保存について

Public Record としてのE-mail の側面を考慮してE-mail もその他の記録と同様の扱いを受けると述べられている。そのためE-mail は保管されることになるがそれは検索のためではなく記録として一定期間保管するということである。保存期間は各大学のポリシーやPublic Record に関する州法の違いなどにより異なっている。

4.4 Web 作成時の注意点

この項目は、World Wide Web 上にファイルを作成する際の注意点、従うべきルールなどを列挙している。University of California, Berkeley が挙げている内容は

1. 大学の名前や印章を用いる場合： 「State of California Education Code 92000」に従う。
2. コピーライト： 既存の大学のポリシーに準ずる[29]。
3. Accessibility： 身体障害者に対してもアクセスを提供する方針の説明。
4. 学生についての情報公開する場合：FERPAによって取り決められているのでそれに従うこ

[29] UC Berkeley の場合には http://www.ucop.edu/ucophome/uwnews/copyr.html を参照。(2001 年 3 月には参照可能)

と。

5. Identi_cation：大学の管轄内にある全てのウェブサイトはサイトの所有者についての情報、つまり連絡する際の名前、E-mail アドレス、最終更新日などの情報を表示しなければならない。

などである。World Wide Web に対するUC Berkeley の態度をまとめると以下のようになる。「大学は表現の自由や学問の探究を行なうための開かれた環境を奨励し支持する。しかしながら、大学の管轄内にある全ての電子的な文書の内容は州法、連邦法そしてUniversity of California のポリシーやルール、規定に従わなければならない。」またリンクの責任に関する規定として「Berkeley から大学外部へのページにリンクがあったとしても、そのことによって大学がそのサイトの製品やサービスを推薦しているわけではない」と述べる。また、大学内に存在する個人のページに対しては、「個人のページも既存の法や大学のポリシーの対象となり」「個人のページは、そのページが大学の意見を表明しているような印象を与えてはならない」と規定する。

Kansas State University の場合

1. 大学内のコンピューターからインターネットに接続するのは、学問のため、研究のため、学習のため管理のためである。
2. 大学の公式ページや大学の公式ファイルを用いてweb を作成するためには、大学の information resources management policy に従わなければならない。
3. 非公式のページをつくるにも大学の規約に従う必要がある。
4. 大学はページやファイルを移動、削除する権利を持つ。
5. 大学の名前、ロゴ、トレードマークやその他の知的所有権のあるものを使用することは別のポリシーによって定められる。権利なき利用者によるweb の作成は禁止されている。

4.5 Obscene Material への大学の対応

Obscene の辞書的な意味は「わいせつな」や「反道徳的な」であるが、インターネット上ではこの単語はポルノグラフィーを指すものとして当初用いられていたようである。University of VerginiaにおいてのObscene の定義は、

> 全体を鑑みて、そのテーマや目的の主たるものが裸への病的な興味やみだらなものであったり、性的な行為や性的興奮、排泄器官や排泄物、またサドマゾ的な虐待であったり文学や芸術、政治、科学的な価値を持たないような、実質的に日常習慣から逸脱した記述や表現をもつもの

である。しかし現在は、以下に挙げるNapster やWarez などをも指すものとして用いられているように思われる。なぜならNapster やWarez が既存の法に抵触するという法的判断が最終的にはまだ下されていないからである。

Napster に関してのIndiana University の対応は以下のようなものである。

> ネットワークの使用を分析してみると、この特定のアプリケーションがネットワークのリソースを大量に消費しており本来の目的であるティーチングやラーニング、リサーチに影響を及ぼしている。インターネットの帯域は高価な物資であり、本来の目的のために保存され

なければならない。

学問上または就職活動のために音楽を集めたり共有することが必要なものはコンピューターセンターへと連絡し、その必要性を議論し、その活動が容易になるようなアレンジをしてもらいなさい。

Indiana University のFair Usage Policy に従い、大学はこのアプリケーションのさらなる使用に対しフィルターを設けることにした。

このフィルターを出し抜こうとした者は大学のポリシーを侵害したものと見なす。

Kansas State University の対応は以下のようなものである。

最近キャンパス内に設置されたWarez のサイトは一分あたりに76,800 通のメールに相当するデータ量をこうむった。この行為が一年中に行なわれたとしたら、かかる費用は$ 160,800になる。

このトラフィックのコストを維持することは大学の情報技術予算に重大な障害を生じさせる。娯楽のためのインターネット利用が継続的に階段状に増加をするにつれネットワークのログ障害や情報技術にかかる費用が倍増するだろうことは明らかである。それゆえ大学の目的にそぐわない利用法は禁止する方針をとることにする。

まとめると、法的規定がないこの種のアプリケーションに対してはネットワークトラフィックが生じるという理由が一つ、さらにこれらのソフトウェアが大学の目的である、研究、教育、サービスの提供に沿わないという理由で使用を禁じ始めている。またわいせつな画像については法的な措置が行なわれるので理由を特に述べてはいない。

4.6 管理方針の説明

この項目は、どのように大学がコンピューターやネットワーク資源を管理運営するのかというポリシーを述べるものである。この項目に大学の方針がそのまま表れている。大学に適用される法や大学のポリシーの説明、データの保存期間、ポリシーに違反した場合のサンクションの設定、プライバシーを侵害されたと思われる場合の訴え方、などを述べている。また利用者が保持する権利について、たとえば言論の自由などを明記する。たとえば、電話、図書館、そのたの施設にあてはまる規約や経営の方針はE-mail やコンピューター、ネットワークにもあてはまると明記する大学が存在する。Indiana University では以下のような専門用語の規定を設け、管理方針の明確な規定のための準備をする。以下Indiana University の実際のポリシーである。

専門用語の規定

Network コンピューターや周辺機器が繋げられている完全な機構

Network capacity ネットワークが測定される量的な規模

Networked computer ネットワークに接続しているコンピューターシステム

Shared computing resource 一人より多くの人によって使用されるネットワークに接続されたコンピューターやその周辺機器

System manager Networked computer のセキュリティーや管理への責任を持つ個人やグループ

System administrator Networked computer に対して管理上の権限を持っている人

General policy

1. Access： 大学内のコンピューター資源や付随するネットワークを必要とする大学のすべてのメンバーに対し、それら資源へのアクセスを提供する。
2. Availability： 大学内におけるコンピューター資源をできる限り干渉が行なわれることなく利用できるようにする。
3. Security： 事故、改ざん、非権限アクセスなどから大学内のコンピューター資源上にあるユーザーのデータを保護する。セキュリティーの手続きはSystem administrator によって行なわれる。
4. Con_dentiality： コンピューター上のファイルは秘匿性を持っている。大学はコンピューター上の情報をすべて秘匿になるようにコンピューター資源を維持する。情報を公開する要求はadministrator によって審査される。州法、連邦法、大学の規約による要求などのときに審査される。
5. Institutional purposes： 教育、研究、公的サービスという大学の目的に沿うようにコンピューターやネットワークは存在する。商用利用はsystem administrator のarrangement があったときにのみ許可される。

表現の自由について

言論の自由の憲法上の権利は全ての正当な利用者に適用される。

University of Florida では、コンピューター上のデータの取り扱い方法についての規定を以下のように行なうと明言する。

General rules

1. 連邦法、州法、大学の規定、ポリシー、ソフトウェアライセンスを含む契約などに従う。ハッキング、クラッキングは”Florida computer crime act", “Electronic communications privacy act",”computer fraud and abuse act" に従う。
2. 利用者は大学のコンピューター資源を使用するために何の権限が必要で、その権限を獲得することを義務づけられている。
3. システムの維持に支障が出るというシステムアドミニストレーターの意見がある場合には制限を設けるが、それ以外の場合利用者は制限を受けない。
4. 権限無しに大学のロゴやトレードマークを使用すること。大学の意見として述べることや何かを意味してはならない。
5. 非権限アクセス、大学のコンピューターやネットワークに損害を与えるような使い方をしてはならない。ウイルスや回線を切断することなど派性的な試みも許されてはいない。
6. このポリシーは大学によって適切だと思われれば改変される。

Enforcement

ポリシーへの侵害は大学のコンピューター資源へのアクセス禁止や大学内外においての罰則、disciplinary action の対象となる。

4.6.1 Sanction

このポリシーは大学の設定するポリシーの侵害に対し大学独自の罰則規定ならびに法の適用をおこなうことを明示するものである。大学の規定により利用者に対しSanction が加えられる場合

は以下のとおりである。

(1) 大学のポリシーを侵害した場合[30]。

たとえばUniversity of Virginia におけるObscene Material についてのポリシーを侵害した場合についての説明は

> コンピューター上にそれを配置した場合には、州法や連邦法以外に大学のポリシーを侵害したものとみなす。その場合のポリシーは「computer usage policy」,「employee standards of conduct」, 学生の行動規範など(これらに限らない) への違反と見なす。

のようになっている。

(2) コンピューターに適用できる法律であると大学が判断をした法律を侵害した場合。

4.7 パターン4 の分析

パターン4 では、計算機利用の目的、利用者が保持する権利、計算機上のデータの取り扱い、既存の法律とコンピューターの関係という4 つの要素が述べられている。

利用者になによりも要求されることは、計算機を利用するために大学の目的(教育、研究、公共のサービス) に沿うようなかたちで計算機を利用することである。利用者は大学の目的に沿うようなかたちの目的を持つかぎりで計算機を利用することが可能であり、その目的に違反しない仕方で計算機を用いて学問の自由、表現の自由などの権利を行使することができる。

これらの要素のなかで情報を取り扱う要素である「計算機上のデータの取り扱い」をより詳しく見てみる。すると計算機上のデータの取り扱いについては

1. 大学は計算機上のデータをすべてプライベートなものとして取り扱う。
2. 大学の計算機上のデータはPublic Record の対象になる。
3. 大学の計算機上のデータは既存の法律によりアクセスされる。
4. 大学の計算機上のデータは技術的側面を考慮すると完全に安全には保てない。
5. 計算機上のデータは保守点検の際に内容を見られることがある。

以上の5 つの項目が述べられている。これらの項目をプライバシーの問題を考慮した観点から考察を行うことにする。1 ついては何も述べる必要はない。プライバシーを尊重するということが述べられているからである。

2 は自分の保有する情報が他人によって見られるということを意味しているので、「当人にしか知りえない情報を自分が管理する」というプライバシーの要素が侵されていることになる。

3 は他の権利とプライバシーの権利との対立であり、計算機に限定された話ではない。そもそもプライバシーの権利自体が存在するかどうかという枠の中の事柄であるのでここでは考察の対象としない。

4 はクラッキングや機器の故障のために情報を完全に守ることができないことを意味しているので、「当人にしか知りえない情報を自分が管理する」と「当人が公開した情報が保護されること」という2 つのプライバシーの要素が侵されていることになる。

5 は情報を見られるおそれがあることを意味しているので「当人にしか知りえない情報を自分が管理する」というプライバシーの要素が侵されていることになる。

---

[30]実際の罰則の内容については 3.2.3 を参照されたい。

アメリカの大学がどのようにプライバシーを取り扱っているのかというと

1. 「当人にしか知りえない情報を自分が管理する」という要素は計算機の特性上、また法的な要請によっても完全に保護することはできない。
2. 「当人が公開した情報が保護されること」は技術的には保証できないがconfidentiality は保証される。
3. 「社会から干渉されない」という意味でのプライバシーは決して侵されていない。

つまり定期的なファイルの検査やデータの盗聴などによって、ある人の持つ信念、思想、嗜好などが他人に知られたとしても、その情報は2 次利用されることがなく、その情報に対して規制や統制が行なわなれることもない。また、法的な要請もしくは大学の方針がない限り、情報そのものの管理は当人にゆだねられているのである。

4.8 プライバシーを保護すべき理由

大学では、教育、研究、大学のサービス提供を滞りなく行なうことが目的として設定される。コンピューターやネットワークの使用は目的に沿うように使用されることが利用者には必要となる。しかし利用方法の制限がそのまま利用者の行為の制限に繋がるわけではないということを指摘することは重要である。というのも、社会においては問題の争点となるような事柄であっても、大学においては研究、教育のためにその事柄の取り扱いが許可されることがあるからである[31]。

大学においてはセキュリティー管理のために必要なことではあっても、管理業務のために行なわれることが、大学の目的を大きく妨げるようなことになってはならない。一見矛盾しているように思えるが、プライバシーの保護を優先することが大学の目的につながるのである。なぜならプライバシーの保護を行なうことによって創造性が増進され、創造性をその構成要素として持つ研究という大学の目的の内の一つが増進されるからである。この点が研究機関としての特徴を考慮したうえでの大学におけるプライバシー保護の特徴ともいえる[32]。

つまり大学においてはプライバシーを保護するようにセキュリティーとプライバシーの間に線を引くことが望まれるのである。

5 結論

アメリカの大学における計算機上の情報はプライバシーとして取り扱われており、またプライバシーを尊重する規範的傾向が存在することが明らかになった。

すなわち、アメリカの大学のポリシーステイメントを分析した結果

---

[31]昨今話題となっている Napster 訴訟に対するアメリカの大学の態度が分かれている。Indiana University および Kansas State University は Napster が連邦地方裁判所で業務差し止め命令を受ける 2000 年 7 月 28 日以前の 5 月 1 日(Kansas State University)、2 月 10 日(Indiana University) から大学内において Napster の利用を禁止していた。禁止の理由は「Napster によるキャンパスネットワークへの負荷が大きい」というものである。この 2 大学と逆の方向の決定を Harvard, MIT, Stanford, Duke, UC が行なった。理由は「大学はキャンパスネットワーク内の情報の内容の regulation を行なわない。」というものである。Indiana, Kansas も Napster を利用することが研究に必要であれば利用を許可するという項目を設けているが、そのためにはコンピューターセンターへと許可を求めなければならないとしている。２つの態度に共通する事は、研究、教育のためには Napster の利用も許可するとしている事であり、目的は滞りない研究、教育である。Indiana, Kansas のポリシーは付録してある。

[32]義務教育課程における生徒のプライバシーとセキュリティーの問題については[4]「教育におけるプライバシーの重要性」を参照されたい。この場合には問題はより複雑となる。というのも、どの程度まで内面の教育を行うかという目的設定、またそれに対応する線引きについての議論が必要となるからである。

1. 大学の目的に違反しない限り、コンピューターやネットワーク資源へのアクセスを認める。

2. 既存の法律や大学の設定しているポリシーとコンフリクトを起こさないようにコンピューターやネットワーク資源のポリシーを定める。

3. 既存のポリシーとの違いとして、ユーザーのプライバシーを保証できないことを明記してある。これはコンピューターの性質上付け加えられたものである。

4. 制限されるプライバシーの要素とは「当人にしか知りえない情報を自分が管理すること」「当人が公開した情報が保護されること」である。

5. 「社会から干渉されないこと」ということはどのような意味合いにおいても認められている。

6. プライバシーを保護することによって大学の目的が増進する。

以上の項目を指摘し、これらの項目がセキュリティーとプライバシー保護の問題を考えるポイントであることを明らかにすることができた。

A 参考URL

ポリシーの分析に使用した大学のURL は以下のとおりである。トップページに設置してある「search」欄で「computer」「usage」「guideline」「policy」「ethics」などをキーワードとして検索を行なうとそれぞれのポリシーにたどり着けるはずである。

Indiana University http://www.itpo.iu.edu/

Kansas State University http://www.ksu.edu/InfoTech/

Ohio University http://www.ohiou.edu/

Reed College http://www.reed.edu/

St. Cloud State http://www.stcloud.msus.edu/

University of Arizona http://www.u.arizona.edu/

University of California http://www.ucop.edu/

University of California, Berkeley http://www.berkeley.edu/

University of California, Davis http://www.ucdavis.edu/

University of Delaware http://www.udel.edu/

University of Florida http://www.u.edu/

University of Iowa http://www.uiowa.edu/

University of Maryland http://www.umd.edu/

University of Michigan http://www.umich.edu/

University of Minnesota http://www.umn.edu/

University of Missouri http://www.missouri.edu/

University of Virginia http://www.virginia.edu/

参考文献

[1] “International Encyclopedia of ETHICS" Fitzroy Dearborn Publishers, 1995

[2] 『情報セキュリティー技術に関する研究開発のあり方について』情報セキュリティー技術研究会, July 2000
[3] “Routledge Encyclopedia of Philosophy"
[4] 江口聡.教育におけるプライバシーの重要性「情報倫理の構築」プロジェクト第2 回国際ワークショップ, Feb. 2001

(千葉大学)