応用倫理学　　２００５年度夏学期　　奥田栄教員

＜はじめに＞
まずは、過去問を見てみましょう。

・２００３年度夏学期（持ち込み可）
１　Cyber Space の倫理と Real（あるいは Physical）Space の倫理は「同じ」であるか、「違う」かいずれか一方を選択し、解答用紙の最初に記入しなさい。
２　「同じ」を選択したものは、二つの空間の性質の違いを考慮した上で、同じであるとする根拠を述べなさい。また、それにもかかわらずさまざまな倫理的ジレンマが生じているように見えるのは何故かその理由を述べなさい。
３　「違う」を選択したものは、その違いは二つの空間の性質のどこから生じるのか、倫理上の一番大きな違いは何か、そこからどのような社会的問題が引き起こされるか、その解決法は何かについて述べなさい。
・２００４年度夏学期（持ち込み不可・Ｂ４）
ルーマンの社会システム論では現代の社会システムは様々な機能システムに分化しており、そのシステム境界は道徳の揺らぎにつれて揺れている。こうしたことを考慮した上でインターネットの普及によって可能となった人間の行為が応用倫理の新しい地平を拓くものであるということの意味を考察し、具体的にどのよう地平が拓かれるのかを論じなさい。

このように、大問１問の論述試験が行われているようです。講義の内容を板書を含めて見返すという形なので、しっかりと講義に出て板書を取っている人にはそれほど役に立たないと思います。参考資料に基づき適宜加筆してあり、やや冗長になってしまっているので、必要に応じて読み飛ばして下さい。特に第三回に当てはまります。

＜サイバー倫理：その歴史＞
（１）コンピュータ以前
ＩＢＭの企業倫理とナチスによるホロコーストとの関係をブラックが指摘。
（２）コンピュータと倫理
コンピュータの発明とその社会的影響についてウィーナーが指摘。
（３）コンピュータ倫理の再発見
1960 年代、専門家・オペレーターによる犯罪によりコンピュータの社会的影響が現実味を帯びる。
（４）コンピュータ倫理コース
1970 年代に設置。

（5）コンピュータ倫理の教科書

1980 年代に一般にも情報技術の与える影響が顕在化→1985 年に最初の教科書が作られる。

（6）サイバースペース

ウィリアム・ギブソンの「クローム襲撃」で初めて使用され、「ニューロマンサー」で一般に知られるようになる。これらの中では特殊電極を直接、脳に接続してネットワーク上のデータを幻想的に体験させる空間のことを意味する。映画「マトリックス」の世界に酷似。

（7）インターネットとサイバースペース

サイバースペースの概念が実体を持つことと、インターネットの発展とによりこの二つの言葉は交換可能な言葉として使われる。

＜サイバー倫理の方法論＞

・サイバースペースの特性

サイバースペース内では本人確認ができない→コミュニケーションに依存。

・ルーマンの社会システム論

１　「社会」はコミュニケーションだけからなる。

２　「社会」はコミュニケーションの総体からなる。

３　「社会」はコミュニケーションによりコミュニケーションを再生産する。

・コミュニケーションを可能にするメディア

１　ことば：コミュニケーションの理解を確実にする。

２　拡充メディア：コミュニケーションの到達を確実にする。

３　象徴的に一般化したメディア：コミュニケーションの成果を確実にする。

・サイバー空間の二重性

狭義には拡充メディア（「情報」と「伝達」の差異を埋めるもの）に対応

・経済という部分システム

貨幣は、他者との接触を前提とする将来への支払いというコミュニケーションを前提とするメディアであり、価値決定、交換手段、貯蔵手段としての役割を果たす。

・ルーマンと倫理

道徳＝善悪、良否という区別により作動し、人間的尊厳、軽蔑を表すコミュニケーション。

倫理＝道徳についての反省理論

・メディアミックスの禁止、つまり**機能分化**

ある部分システムには他の部分システムのメディアを混用してはならない。

例としては、金と権力を挙げられる。

・道徳の今日的意義

過去＝社会全体を統合する意義

今日＝機能分化により複雑化するシステムを判断し、昨日の境界設定の準拠となる意義。

＜専門家の倫理綱領＞

・専門家に対する要請

１　訓練された技術と深い知識

２　自律性―専門家は受取り手の確認や同意を得ずにサービスの方法を変えられるため

３　行動規範の遵守

・専門職の４つの規範

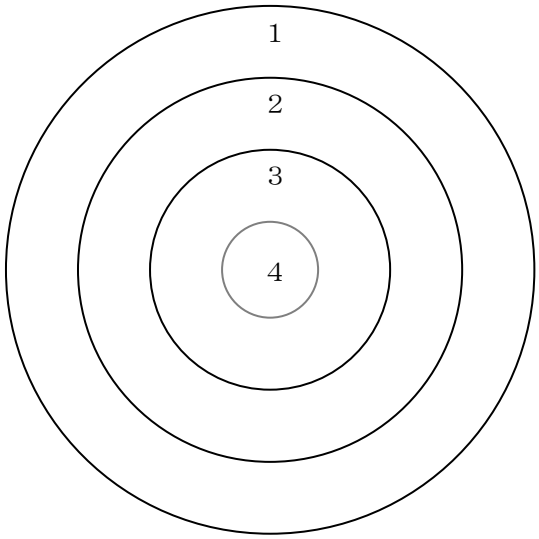
１　専門職規範―その専門職が持つイメージとそのメンバーを守るために何をなすべきか、なさないべきかを規範する。

２　個人規範―専門家個人の生活する文化的環境や宗教的信条による規範。

３　組織規範―組織や雇用者の社会的信用を確立、維持するための組織の規範。

４　コミュニティ規範―専門家が働く地域の住人の宗教・文化に基づく規範。

概念図を以下に示す



・サイバースペースにおける専門家と呼べる人の存在について

１　専門職とはいえない―情報技術による社会的影響を専門家の責任に属する事柄としてコントロールするシステムを持っていないし､そもそも情報技術に専門性があるのかが疑問である。

２　専門職である―情報技術の内容は十分な教育と訓練を受けなければ理解できないという点で、専門家は明らかに「素人」とは区別される存在なのであり、その社会的承認の形態が「専門家」性を決定するものではない。

・専門家の出会う倫理的問題の例

１　電子メールの検閲

２　犯罪予防のためのリスト作り―犯罪防止と人権侵害のジレンマ

３　パッケージソフトのバグと販売時期―デバッグと利益のジレンマ

・専門性を支える４つの柱

１　献身―ハンフリーズによると、献身は以下の６つの特質を備えている必要がある。

１　献身は強制ではなく、自発的に行わなければならない。

２　責任者は自ら献身を果たそうとしなければならない。

３　いつ誰がどこで何をするのかが、合意が得られていなければならない。

４　献身は、公開で公示されたものでなければならない。

５　献身は慎重に行わなければならない。

６　約束が守れないことが事前に明らかな場合はすぐに通知し、再度約束を結び直さなければならない。

２　誠実―個人の信条に対して完全に忠実であること。専門家として不可欠な信念として、ビジョン（何が起こるかを予測して利益を最大化するよう計画する）、自己の行動に対する愛情、自らが成すべき事に対する献身がある。

３　責任―主に４つに分かれる

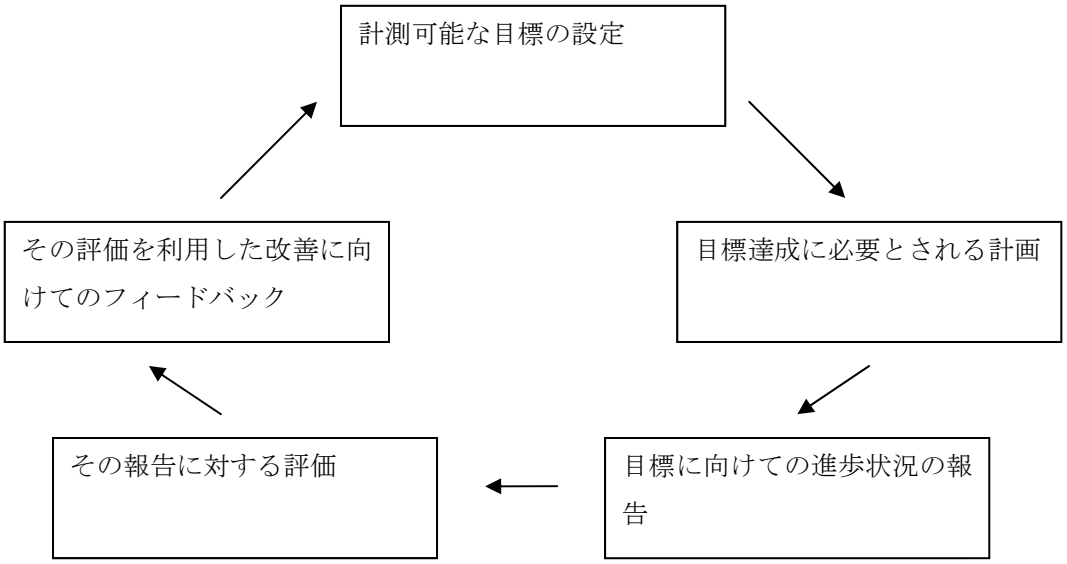
１　供給者責任―提供者としての役割を果たす責任。

２　サービス責任―サービスの提供時間、質、結果に対して持つ特別の責任。

３　製造物責任―クライアントには製品を決められた時間に安全な使用法を示す書類とともに届けなければならない。クライアントはその製品の使用の結果として起こり得るすべての事態に責任を持つ。

４　結果責任―専門職の行為に伴う結果によりクライアントに被害が出た場合、専門職はその結果として生じた事態に対して責任を取る。

４　説明責任―自分に割り当てられた責任を遂行する責務。以下のようなサイクルとなる。



・ＡＣＭの倫理コード

三つの段階の綱領

１　会員として―社会と人類への貢献、他者のプライバシーの尊重等の一般的倫理

２　専門家として―専門能力の習得や維持、不正アクセスをしない等の専門的倫理

３　組織管理者として―１　メンバーが社会的責任を果たすように指導する。

２　職業生活の質を高めるようにする。

３　規則の数と範囲を抑え、かつ完全な効力を持つようにする。

４　事前評価、事後確認を行うようにする。

５　使用者の尊厳を保護するようにする。

６　メンバーがシステムの原則と限界を学ぶ機会を設ける。

このような規定は組織による制度的な保証に基づく。

・倫理綱領に対する批判

１　倫理綱領は少しも倫理的ではない―法のようになってしまい､イメージ作りにすぎない。

２　現在の綱領が狭い視野の上で作られているので、かえって有害である。

＜**ＡＲＰＡネット**の起源＞

・ＮＨＫによると、インターネットとはルータ（ネットワーク上で流れるデータ（パケット）を他のネットワークに中継する機械）と専用線からなる巨大な網の目のようなものである。

・1961 年にソ連が有人宇宙飛行に成功し、同時にユタ州の電話中継局がテロによる被害を受け、空軍が通信システムの研究を**ランド社**（中心：**ポール・バラン**）に依頼した。その解決法は、電話の交換器を使わずに、**パケット**と呼ばれる短いデータを転送するというものであった。それを実行に移したのは**リックライダー**と**ラリー・ロバーツ**であるとＮＨＫは主張する。そのパケットを交換するための機械がＩＭＰ（Interface Message Processor）であり、ＮＨＫはルータの原型であり核爆発に耐える軍事用コンピュータであると報道したが、そのようなコンピュータでないことは言うまでもない。

・ＮＨＫで放送された内容とは異なり、軍はＡＲＰＡネットを黙殺していて、研究に熱心ではなかった。1964 年にランド社から報告書が提出された際に空軍はその存在を隠匿し、1966 年に国防総省国防通信局（ＤＣＡ）に建設を依頼したが失敗し、建設には結びつかなかった。また、ラリー・ロバーツの講演によれば、ＡＲＰＡネット建設の動機に軍事的なものはなかった。さらにＮＨＫは、1967 年にラリー・ロバーツが新しい通信データ通信網の必要性を説く企画を発表した際に実際にパケット交換を行っていた**ドナルド・デイヴィス**を無視した。ちなみに、その企画は負荷、データやプログラムの共有、Ｅメール、遠隔サービスなどを目指すというものであった。これらのうち、ＡＲＰＡネットの成功にもっとも寄与したのは**Ｅメール**である。パケット通信について専門家は自身の基盤を揺るがされかねないので、強固に反対した。結局、ＮＨＫはロバーツとデイヴィスの同時発明を認めず、また発明は必ず実用に結びつくという誤解もしていた。

＜ＡＲＰＡインターネットと倫理＞

・ＡＲＰＡネットが成功した理由としては、ＩＭＰのベースが廉価なコンピュータであったことと、Ｅメールとして利用できたということが揚げられる。また、ＤＣＡが成功していたらＩＰ電話が開発されていた。

・インターネット第一世代

初期の電子メールやＢＢＳによる情報伝達が行われたが､軍と関わりを持ちたくないが電子メールを利用したいという要望からＵＵＣＰネット（ＵＮＩＸ間で発展した「貧乏人のＡＲＰＡネット」)、ＣＳネット等のさまざまなネットワークが建設された。

・インターネット第二世代

コンピュータ同士がメッセージを交換する際の共通言語の規約を**プロトコル**という。

ＩＰプロトコルに準拠したパケット（ＩＰデータグラム）はその構成法と宛て先データの書き方しか指定しなかったので、ルータの容量超過により伝わらないこともあった。

そこで、データが届くことを保証する仕組みとして**ＴＣＰ**（Transmission Control Protocol）が作られた。その特徴は、データを送るたびにタイマーをスタートさせ、応答確認がない時には再送する。これにより入れ替わりや重複のあるデータが届くのでこれを編集して確実にデータが届くことを保証するというものである。

1980 年代中頃にはＡＲＰＡインターネットとは、**ＴＣＰ／ＩＰプロトコル**が走るネットワークを結ぶネットワークを意味した。この時期インターネットは税金やボランティアによる運営であり、商業行為は禁止されていた。

これら二つの世代の中心は研究者共同体であり、それに基づく倫理が構築された。その例が**マートンのエトス**であり、普遍主義（発言者にかかわらずその発言は基準により判断される)、公有制（科学は社会的産物であり共同体に属する)、利害の超越（利害目的の捏造禁止)、系統的懐疑（納得できるまで判断を控え、客観的に懐疑する）という４つの理想によるが、このような倫理は厳密には守られていなかった。当初は情報を隠す必要性が小さかったため、ハッカー行為も彼らの倫理では知識を獲得するひとつの方法であり、必ずしも悪として扱われなかった。

・ハッカーとクラッカー

ＲＦＣ（Request For Comments）1983 によると、ハッカーはシステム、コンピュータやネットワークについて深く理解することに喜びを感じる人物であるが、クラッカーに対してなされる非難や軽蔑の意味を含んで使われてしまうこともあり、クラッカーは悪意を持って不正アクセスしようとする人物である。

・インターネット第三世代

World Wide Web（WWW）による情報提供から今日までを指し、一般の社会へと普及している。

・備考

パケットには送信履歴が残るためインターネットに厳密な意味での匿名性はない。

＜**WWW**の開発とインターネット＞

・**ＲＦＣ**とは、ＩＥＴＦ（Internet Engineering Task Force）が公式に発行したインターネットに関する技術や提案などの公開ドキュメントのことである。当初は単なる文章でしかなかったが、現在ではインターネットの標準を定める文章とみなされることもある。

・WWWが普及する前に普及していたのはＮＳＦ（National Science Foundation）ネットであり、1986 年に作られた時にはＡＵＰ（Acceptable Use Policy）により商業利用が禁止されていたが、1990 年にＡＲＰＡネットを事実上吸収すると、商業利用が可能となった。現在でもインターネットの一部を構成している。

・WWWはＵＲＬ（文章の位置を示す)、ＨＴＭＬ（テキストの書き方)、ＨＴＴＰ（通信の手続き）からなり、開発者は**ティム・バーナーズ・リー**である。彼はこれを改良、普及する目的でインターネットに公開した。それを見た**マーク・アンドリーセン**を中心とするイリノイ大学の学生達は 1993 年に **Mosaic** を作成、公開した。すぐに送られてくる感想により改良も繰り返された。当時はインターネットが拡大し、使用者は漠然とした期待を抱いていたもののその使い方がわからないという時期であったのも成長の原因である。しかし、大学が開発を一元化しようとしたため自由に改良できなくなり、開発者達はネットスケープ社を設立した。

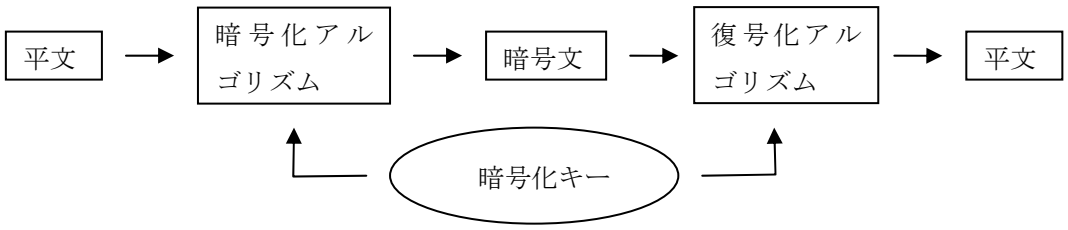
・WWWの開発はコンピュータを簡単に使え、情報を入手しやすくしたため、インターネットの一般への普及の原動力となった。これに伴い研究者と一般社会の倫理あるいは国や宗教間の倫理の衝突を引き起こし、隠す必要のあるデータの出現やデータの改ざんを防ぐ方法等様々な問題を引き起こした。そこで暗号技術が重要になった。

＜セキュリティと安全保障＞

・セキュリティを確保する目的は通信内容の傍受を防ぎ、相手を確認し、改ざんを防止するという３つからなる。

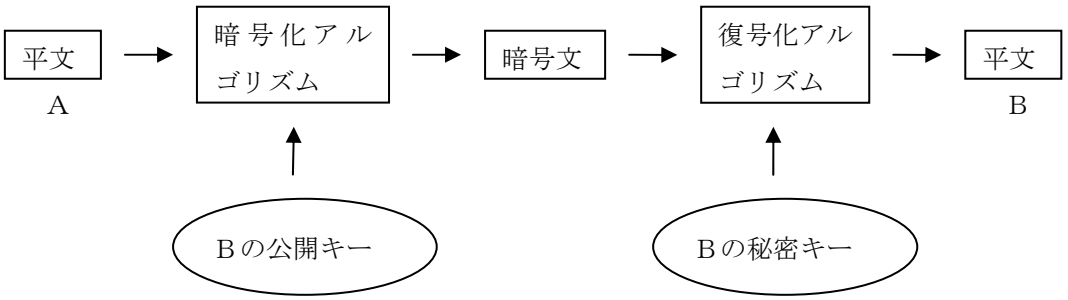
・通常暗号

暗号化アルゴリズムの数に限りがあるので見破られてしまうし、暗号化キーを第三者に知られずに相手に知らせるのは困難である。



・公開キー暗号

ウィットフィールド・ディフィとマーティン・ヘルマンが公開キー暗号法を作り出した動機は反政府活動を政府に知られずに行いたいというものであった。



上図は傍受の防止を目的としたものであり、電子署名にはBの公開キーをAの秘密キーに、Bの秘密キーをAの公開キーに入れ替えればよい。この二つを複合すると、電子署名をしながら通信内容を秘密にできる。

この方法を実用化したのはリベスト、シャミーア、アドルマンの三人であり**ＲＳＡ**と名づけられた。彼らが所属したロータスノーツはＲＳＡアルゴリズムの特許を取得して成功を収め、特許の期限が切れると誰でも使えるようにした。(この特許は他国で認められなかったため若干の問題が起きた)

・暗号と安全保障

国家安全保障局（**ＮＳＡ**）は冷戦期の 1952 年にトルーマンにより、暗号に関わる技術の指導、提供あるいは通信傍受を目的として組織された。最近までその存在は隠されてきたが、1986 年にはＮＳＡビルで 2 万人が働いていたようである。ＮＳＡは、公開キー暗号の普及により傍受ができなくなることを恐れ、輸出規制法を利用したり、マイクロソフトへ圧力をかけた。犯罪組織の人間に暗号技術を使われると困るが、セキュリティへの配慮も必要であるという問題がある。このジレンマの解決方法として、情報を秘匿する必要のある時間の長さと第三者がそれを解読するために要する時間を考慮に入れるということが挙げられる。

・暗号が禁止の方向へ動くのを防ぐため、また自分の身を守るために**フィル・ジマーマン**は暗号化ソフト**ＰＧＰ**（Pretty Good Privacy）を開発した。

＜迷惑メール＞

・**ＳＰＡＭメール**とは勝手に送りつけられてくる宣伝メール、すなわち迷惑メールのことである。ＵＣＥ（Unsolicited Commercial E-mail)、ＵＢＥ（Unsolicited Bulk E-mail）とも呼ばれる。その内容は出会い系、マルチ商法等の宣伝である。メールが届く経緯には、辞書攻撃 (ランダムにアドレスを探す)、ロボット検索による収集、個人情報の流出、売買などが主に挙げられる。これらＳＰＡＭメールは受信者の金銭や時間を使わせるだけでなく、読み手に無関係に送られたり、非合法活動に使われる点で問題である。ＳＰＡＭメールが届いた際には内容を信用したり、返信やリンクをクリックしないようにするべきである。しかし現実にはアメリカで迷惑メールをクリックした割合は 31%であり、

そこにウイルスやワームなどのマルウェアが仕込まれているためにＰＣが感染し、勝手にＳＰＡＭメールの送信やサイバー攻撃に利用されてしまう。このようなＰＣのネットワークを**ゾンビネットワーク**と呼びその動きは中国で顕著である。ＳＰＡＭメール発信元の第一位はアメリカ、第二位は韓国である。

・**架空請求**はＳＰＡＭメールよりも悪質であり、受信者を脅迫して金銭を徴収しようとする。送られてきた場合は基本的には無視していればよい。

・**ワンクリック詐欺**はＳＰＡＭメールに貼られたリンクをクリックするとアドレスの情報が相手に伝わり、それを相手は契約したとみなして金銭を要求してくる。名前や住所は伝わっていないので無視をしたり、アドレスを変えるなどの対策を取ればよい。

＜サイバー攻撃＞

・**サイバーテロ**

現代社会は行政、金融、ライフラインなどあらゆるものがコンピュータネットワークに依存しているため、コンピュータの機能不全は社会の機能不全に直結する。これらに対する電子的攻撃をサイバーテロと呼ぶ。通常のテロとは異なり手軽に実行でき、しかも自分の倫理的葛藤は少なくて済む。一例を挙げると、リチャード・クラークは 1998 年の 4 月にＮＡＴＯのページが書き換えられたことに怒り、ユーゴスラヴィア政府に対して数日間で 50 万通のメールを断続的に送りサーバーをダウンさせた。

・クライシス

1997 年にウースター空港の管制システムにハッカーが侵入し、プログラムを破壊した。墜落という最悪の事態は免れたものの、このことはサイバーテロに対する警鐘として十分な役割を果たした。ライフラインに侵入することでサイバーテロは電話機能の麻痺、停電金融機関への妨害、列車事故や墜落の誘発などを引き起こせる。ランド社はアメリカ本土はサイバーテロに対して脆弱であり、アメリカはもはや聖地ではないと結論づけた。

・サイバー攻撃

1　1990 年の湾岸戦争開戦 10 日前にイラクに輸出されたプリンターにウイルスを仕掛けたとされるが、実行されたか、成功したかは不明。

2　コソボ紛争中にアメリカ軍の偵察機が中国大使館を誤爆したところ、米軍、ＮＡＴＯ軍のネットワークに中国本土のＩＰアドレスから攻撃。

3　日韓サイバー戦争

2004 年 1 月に韓国政府が竹島切手を発行を準備したことに対して日本政府が中止を要請、また同月に小泉首相が靖国神社に参拝していたことも併せて反日感情を煽り、「２ちゃんねる」ハングル板や「Kの国の方式」が韓国を侮辱しているとの報道があると 10 日にネチズン（韓国のインターネットユーザー）がこれらに攻撃を加える。11 日に朝鮮日報が「サイバー壬申倭乱」と報道（壬申倭乱とは、豊臣秀吉の朝鮮侵略のこと）し、２ちゃんねるを煽ったが日本側は落ち着いた報道をした。

4　2005 年 3 月 17 日に外務省ホームページが DoS 攻撃により繋がりにくくなる。それにあわせるように 3 月 20 日には韓国外交通商省のホームページが 10 時間に渡り接続不能になった。この事態を受けて日本は 2008 年までに「第一次情報セキュリティー基本計画」を策定することにしている。

サイバーテロの手法

1　不正アクセス―ホームページの改ざん等により混乱を引き起こす。特定のサーバーを対象にしたものと不特定のセキュリティーホールを対象にしたものがある。ファイアーウオール等を使って防ぐ。

2　ウイルス攻撃―添付ファイルの形で侵入するのでファイアーウオールは役に立たない。自律的に敵のネットワークを探し攻撃するものもある。攻撃者の特定は困難である。

3　トラップドア―あらかじめ故意に侵入口を作っておく。ほとんどのウインドウズにＮＳＡの裏口が組み込まれていると報道されたこともある。

4　Dos 攻撃―外部から大量のデータを送りつけてサービスを妨害する。ゾンビネットワークを利用して行われることもある。手法としては F5 アタック（F5 キーの連打によりサーバーを落とそうとする）や田代砲（元来は TIME 紙の「今年の人」に田代まさし氏を選ぼうと画策した 2 ちゃんねるの人達が画策した投票用スクリプトであり、その威力は TIME 紙のサーバーをダウンさせるほどであったので Dos 攻撃用スクリプトとして扱われるようになった）等がある。