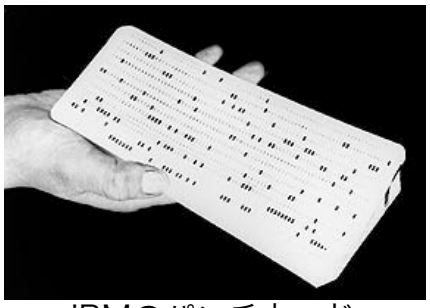
Special Thanks to 木村さん、林さん

第一回　サイバー倫理：その歴史

サイバー倫理学を考える上でコンピュータのあり方の変化について
個人の生活への浸透、ネットワーク化の徹底、公共機関への普及、透明な存在への変化が
起こっている社会で生活する上で、何が本当に正しいのか、どのような態度を取るべきか

1. コンピューター以前
   IBMのパンチカードシステム
   〈技術倫理の問題〉
   ・なし得ることは、なされるべきだ（IBMの特殊な企業倫理）
   ・専門技術者は手段ばかりに目がいき、目的は二の次
   ヒトラーがホロコーストのユダヤ人特定のために膨大な記録の参照作業


IBMのパンチカード

2. コンピューターと倫理
   パンチカードよりもはるかに高速なコンピューターの発明
   ウィーナーの「第二次産業革命」（今日の「情報革命」）

3. コンピューター倫理の再発見
   1960年代になるとコンピュータの社会的影響が現実味を帯び始める
   コンピュータの専門家による様々な犯罪や倫理にもとる行為
   a)イデオロギー的犯罪
   b)オペレーターによる犯罪
   c)専門家によるコンピュータ犯罪

4. コンピュータ倫理コース
   1970年代米国の大学でコンピュータの専門家に対するコンピュータ倫理のコース
   1978年　W.Maner ”Starter Kit in Computer Ethics”を自費出版

クローム襲撃

5. コンピュータ倫理の教科書（一つの学問分野として定着）
   1980年代、コンピュータ犯罪、コンピュータ被害、プライバシーの侵害、ソフト
   ウェアの所有権をめぐる訴訟、など
   一般の人々にも情報技術の与える社会的・倫理的影響がよく知られるようになる
   1985年 D.Johnsonによるコンピュータ倫理の最初の教科書

6. サイバースペース
   ウィリアム・ギブソン「クローム襲撃」でcyberspaceという言葉を初めて使う
   一般的に知られるようになるのは「ニューロマンサー」の発表後

7. インターネットとサイバースペース
   cyberspaceがSFから現実のものになる
   インターネットの発展とWWWの発明
   サイバースペースとインターネットという言葉は交換可能な言葉として使われる

第二回　サイバー倫理の方法論

対立する意見
コンピュータの使用が新たな倫理の局面を開くorコンピュータの技術を使用しなくても、倫理の基本は変わらない
　その違いの生じる原因は議論の出発点
　1)技術の発展によって新たに可能となる人間の行為
　2)倫理理論や道徳理論


"On the Internet, nobody knows you're a dog."

サイバースペースの特性
コミュニケーションがすべて。相手が本当は誰なのか、サイバースペースから抜け出さないとわからない。

ルーマンの社会システム論
「社会」はコミュニケーションだけからなっている。しかも、「社会」はすべてのコミュニケーションだけからなっている。また、「社会」はコミュニケーションによって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ためのもの
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ためのもの
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ためのもの

サイバー空間と社会システム論（サイバー空間の二重性）
狭義には、拡充メディアに対応する
サイバー空間とは、物理空間が人間を包んでいるように人間を包んでいる

経済という部分システム
貨幣というメディアに結びつけられているコミュニケーション

貨幣は何のための存在しているのか？
1.　モノの価値を決める　　ex.労働の対価
2.　モノと交換する　　労働者の消費
3.　富の貯蔵手段

その他の部分システム
　・権力―法で取り締まること
　・真偽と学問―あの人のいうことは正しいか？
　・宗教―信じるか信じないか

ルーマンと倫理
道徳と倫理を区別
道徳とは善悪良否という区別を用いて作動して、人間的な尊敬ないし軽蔑を表現するコミュニケーションであり、倫理学とは、そうした道徳についての反省理論

メディアミックスの禁止
一般に、ある部分システムに属するとされたコミュニケーションに関しては、その部分システムに固有のメディアのみが用いられるべきで、他の部分システムのメディアを混用してはならない
　機能分化…機能ごとに存在する
　象徴的に一般化したメディア
　　互いが交わらなあければ問題は起きないしかし不可分なことも多い

メディアミックスの例　　絵画の売買はいいのに入学許可書の売買はだめ
公共に賄賂がからむ（政治＋金）

道徳の今日的定義
（過去）社会全体を統合する重い役目
（今日）機能分化社会における役割⇒境界管理者としての道徳
機能領域の境界設定によりどころを与え、メディアミックスに警告を発する

サイバー倫理の可能性
国境がなくなる⇒インターネットによる道徳の不統一
お金など、他のメディアの変質

第三回　専門家の倫理綱領

専門職に対する要請
1) その領域でのよく訓練された技術と深い知識　専門職だから
2)自立性　力関係が強く、サービスする人と、受ける人の間に不利、利益が生じるため
3)行動規範の遵守

専門職の４つの規範
1)専門職規範
2)個人規範
3)組織規範
4)コミュニティ規範

サイバースペースでは専門家と呼べる人はいるのか？
(1)専門職とはいえない（水谷雅彦）
　　コンピュータには誰でも接することができるから
(2)専門職である（土屋俊）
　　マニアックになりすぎて素人ではわからないことが多すぎるから

専門家の出会う倫理的問題の例
1)電子メールの検閲–会社等ではいつも監視
2)犯罪予防のためのリスト作り–作っていいのか
3)パッケージソフトのバグと販売期間–先に発売すれば利益が多いがバグも多い

専門性を支える４つの柱
(1)献身　　自分の知識を供給する責任がある→提供者としての役割がある
(2)誠実さ
(3)責任　　サービスをする
　　①提供責任—質
　　②サービス—サービスすること
　　③製造物責任—安全性、時間、形、質⇒書類
　　④結果責任—結果的に生じることに責任
(4)説明責任
目標設定→計画→進行状況報告→評価→評価に対するフィードバック

ACM(Association for Computing Machinery)の倫理コード
三つの段階の綱領
　(1)会員として　　市民としての一般倫理
　(2)専門家として　　特殊な責任、専門知識・技能の獲得維持、不正アクセスの禁止
(3)組織管理者として
　(3-1)社会的責任条項
　(3-2)生活の質条項
　(3-3)運営規則明確化条項
　(3-4)品質保証責任条項
　(3-5)第三者人格権侵害会費条項
　(3-6)教育支援条項
こうした規定は、組織による制度的な保証なしには実現できない

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
(2)現在の綱領がきわめて狭い範囲の視野の倫理的関心の上に作られてため、かえって有害

第四回　ARPAネットの起源

インターネットとは
ルーターと専用線の作っている巨大な網の目

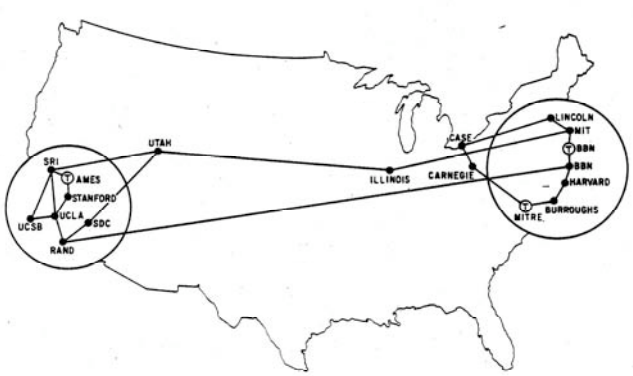
このときの「ルーター」とは
短いパケットと呼ばれるメッセージを備えては転送するコンピューター

インターネットの歴史（1）

1961年　ソ連が有人宇宙飛行に成功
　　ユタ州での電話中継基地爆破テロ
アメリカ国防総省は核戦争時代には従来の電話網は役に立たなくなると考え、ランド(RAND)社に研究を依頼する。
ランド社のポールバランが解決法として考え出したアイデアがパケット交換網
1964年ランド社は米軍に報告書
1965年ランド社が空軍に勧告
1966年空軍がネットワーク建設にゴーサインを出すが、それをまかされたDCA(Defense Communication Agency)は建設に失敗し断念する
当時の通信の専門家はパケット通信に反感を持っていた

ポールバランが論文を発表したとき軍研究機関であるランド社に所属していたためインターネットは核攻撃に耐えられる分散型ネットワークとして開発されたという面が強調されがちである
しかし実際にポールバランのアイデアを実行に移したJ.C.R.LicklideとLarry Robertsは講演でネット建設の動機はコンピュータをつなげたネットワークを作りたかったからだといっている

イギリスのDonald Davisは1965年パケット通信を思いつき（パケットの言葉を使ったのもこの人）、1967年のACMでパッケッと通信の実際に稼働しているデモンストレーションをしていた。
同じシンポジウムでRobertsは新しいデータ通信網の必要性を訴え、そのネットワークARPAnetの企画を発表していた。



ARPAnetは1969年１０月頃に稼働し始める
（一般にこれがインターネットの誕生とされる。最初の通信はUCLA→Stanfordの”logon”で、”LO”まで受信したところで一回コンピューターがフリーズしたそうです。）

ARPAnetの”ルーター”として使われていたのは"IMP(Interface Message Processor)"というコンピュータで製造は予算の都合でBBN社が担当

コンピュータネットワークに期待されていた機能
1)負荷の共有
2)メッセージサービス
3)データの共有
4)プログラムの共有
5)遠隔サービス
実際は2のメッセージサービス（Email）が一番使われていた

第五回　ARPAインターネットと倫理

＜第一世代＞
初期の電子メールや電子掲示板による情報伝達
政府や軍と契約していない個人や組織はARPAnetにアクセスできない
軍と関わりを持ちたくない個人や組織はARPAnetにアクセスできない
それでも便利な電子メールは利用したい→ARPAnet以外のコンピュータネットワークの建設

＜第二世代＞
ARPAnetからARPAinternetへ
コンピュータ同士がメッセージを交換し合うには共通言語を必要とする
この規約のことをプロトコルと言う
IPプロトコルに準拠したパケットをIPデータグラムという（1パケットの構成法や宛先データの書き方などがプロトコルによって決められている）
電報のような扱いだと送信側が送り出してしまえば知らん顔なので途中のルータがあふれたらパケットは捨てられて相手に届かない

プロトコル(protocol)
外交儀礼、儀礼上のしきたり
C-3POはprotocol droid

データが届くことを保証する仕組み
　TCP（トランスミッションコントロールプロトコル）が担当
　タイマーと応答確認で、ネットワークの途中で失われたデータグラムの　　回復を行う仕組み
1.データを送るたびにタイマースタート
2.適当な時間が経過しても応答確認がなかったらパケットを再送
3.そのため受信側ではパケットの順番が入れ替わったり重複して届く
4.データの順番を入れ換えたりしてして元のデータを復元

1980年代頃になるとARPAinternetとはTCP/IPプロトコルが走っているネットワークを結ぶネットワークを意味するようになった（1983年にはTCP/IP以外は禁止）

当初インターネットでは商行為が禁止されていた（税金やボランティアで維持されていたから）

第一世代、第二世代で中心となったのは、大学の教師や研究員などで自立した専門職による建設が行われた。インターネットの倫理は 1.米国社会の倫理 2.研究者共同体の倫理

マートンのエトス
1)普遍主義：誰の発言でもあらかじめ決められた基準で判断
2)公有制：実験データをみんなのものに
3)利害の超越：利益をねつ造しない
4)系統的懐疑：疑い続ける
しかしマートンの当時もこれらは厳密には守られていなかった
情報を共有する仕組みは整っているが情報を隠す仕組みがなかった→ハッカー行為


ハッカーは映画によく登場する
上の写真は"SWORDFISH"

ハッカー行為について
ハッカーとはことにシステムやコンピューター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、クラッカーとは不正にアクセスしようとする悪意を持っている人のことなのでハッカーという言葉が誤用されているだけで本来はクラッカーが正しい
つまりハッカー行為は共同体の倫理では必ずしも悪ではない

＜第三世代＞
World Wide Web(WWW)による情報提供以来、今日まで研究共同体の占有物から、一般社会へと普及

第六回　WWWの開発とインターネット

インターネットを三世代に分ける
1)第一世代　ARPAnet
2)第二世代　WWWによる情報の提供
NSFnet
3)第三世代　一般に普及
第一、第二世代は研究者に利用者が限られておりインターネットの倫理は科学者の倫理だった

パケット,TCP/IP,WWWがインターネットの三大技術といわれる

インターネットの歴史（２）

1984年NSFが大学にスーパーコンピューターセンターを作る案を出す
1986年全米の大学6カ所に設置
　　スーパーコンピューターの処理能力を予算のない大学や研究機関が使えるように
　　ネットワーク(NSFnet)を構築
カーネギーメロン大学からNSFとARPAの二つがつながる
1988年回戦の容量不足から第二NSFnet建設
1990年ARPAnetはNSFnetから切断され廃止される
ほとんどのネットワークはAUP(Acceptable Use Policy)で商業利用を禁止していたので商用ネットワークが建設され始める
しかしAUPのためにNSFに接続できない
1991年商用バックボーンができて全米の商用ネットがつながる。全国的商業利用が可能になる。NSFnetもこの頃なし崩し的に商業利用可能になっていく。1990年NSFnetの管理運用を引き継ぐNPO、ANS(Advanced Network and Services)が設置され、新たな商業顧客の開拓を認める。1991年ANSが営利企業を設置し、その企業はAUPの適用外とする。


Tim Berners-Lee

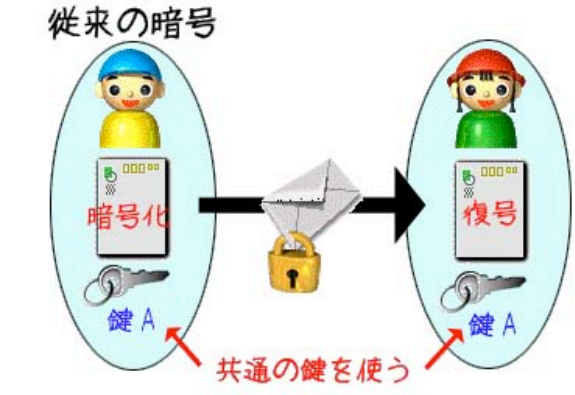
WWW(World Wide Web)の開発
CERN（欧州合同素粒子原子核研究機関）で1989年に完成
CERNの物理学者だったティムバーナーズリー(Tim Berners-Lee)は論文を研究者同士で共有するためにHypertext（他の文書へのリンクを含むテキスト）の概念を取り入れた文章参照システムWWWを一ヶ月で開発する。最初に開発したのは自分が使っていたNeXTSTEPという当時マイナーなOS用のものであった。
1992年イリノイ大学のNCSAのマークアンドリーセンらがインターネットでWWWのことを見てNeXTSTEP以外のもっとメジャーなOSに対応するように移植
さらに画像などを表示できるようにしたWWW閲覧ソフト（ブラウザ）Mosaicを発表しインターネット上で公開
Mosaicはインターネットが整備されつつある時期だったことや、インターネットによってソフトのフィードバックが得られてどんどん改良されたことを受けてどんどん普及する
しかし大学により開発が管理され始めると開発のスピードが落ちる
マークアンドリーセンらはネットスケープ社を設立し新しいブラウザーNetscape(表示エンジンがMozilla)を作る
WWWの開発によりコンピューターの使い方が完全に変わり、インターネットが一般社会で使われるようになる

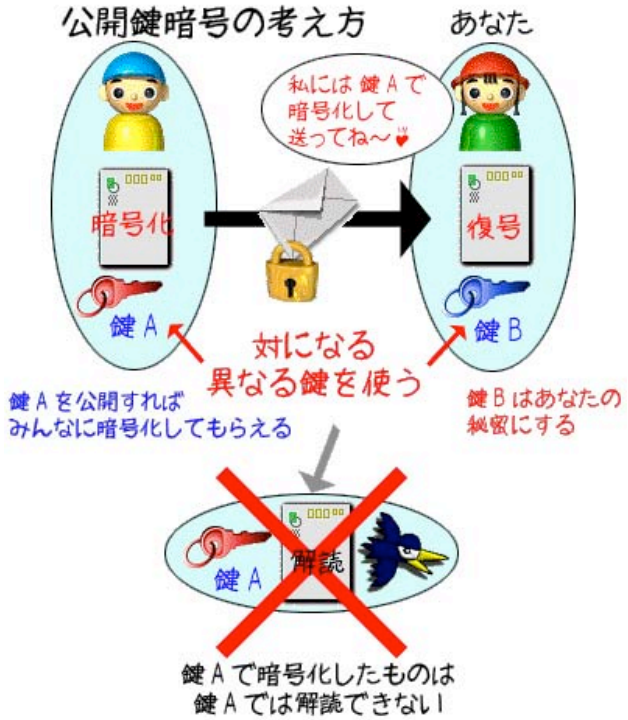
インターネットの一般社会への普及は倫理に関する問題を起こす
研究者の倫理と一般社会の倫理の衝突
国による法や倫理の差異が無視される
電子データの改ざんを防ぐには方法は？
本当に目的の人と話しているかの確認は？
暗号技術

第七回　セキュリティーと安全保障

セキュリティー確保の目的
1)通信の傍受を防ぐ
2)相手の確認
3)改ざんの防止

通常暗号法は共通鍵を使うので送信者と受信者の間であらかじめ共通鍵を何らかの方法で渡しておく必要がある





公開鍵暗号は秘密鍵と公開鍵の二種類鍵を使うことによって通常鍵の問題を解決
さらに電子署名と通信内容の秘密を両立は二重に暗号化すればよい

公開キー暗号の歴史
Witfield DiffieはMartin Hellmanとともに公開鍵暗号法の論文を発表
実際にこの暗号法を実用化したのはRivest、Shamir、Adlemanの三人
それぞれの頭文字をとってRSA暗号と名付けられた暗号法は
1983年9月20日米国内特許を認められるが日本初め他の国では特許として認められず米国特許も17年過ぎてなくなっている
今はパブリックドメイン入りし公開されている

暗号と安全保障
NSA（国家安全保障局）はRSA暗号のような強力な暗号法は脅威
NSAは　(1)暗号技術に関わる技術指導提供(2)通信傍受　を行う極秘機関
NSAはそれまで、あらゆる通信を傍受する能力を持っていたが高度な暗号法が一般に普及するとテロリストなどに使われてもNSAはその通信を傍受することができなくなるので輸出規制法で輸出を禁止しようとしたりマイクロソフトにRSAとの契約をやめるよう電話をかけたりした

フィル・ジマーマンは反政府活動を邪魔されないように公開鍵暗号方式の暗号化ソフトPGPを開発、配布
高度な暗号法の普及は止められなくなる

セキュリティー確保と安全保障のジレンマを解決する一つの案は、情報を秘密にしておく必要のある期間より第三者が暗号解読にかかる時間がわずかに長いくらいにしておく

エシュロンとは
アメリカ、カナダ、イギリス、オーストラリア、ニュージーランドの諜報機関によって運営されている全世界通信傍受・中継システムのコードネーム。電話、ＦＡＸ、電子メール、インターネットのＤＬなどあらゆる通信を傍受し処理を行なう。そして、特定のキーワードを辿り追跡する能力を持つといわれている。

RSA暗号の仕組みと安全性

Fermat の小定理　p:素数,a≠0(mod p)ならば
a^{p-1} =1 (mod p)
よって p,q 素数ならば
$a^{(p-1)(q-1)}$ =1 (mod pq)
∴M=1 (mod(p-1)(q-1))ならば a^{M} =a (mod pq)
素数 p,q を生成し n=pq とする
ed=1(mod(p-1)(q-1))なる e と d を生成
暗号化：a→ a^{e} (mod n)
復号化：a→ a^{d} (modn)
解読は n=pq の p,q が分かれば解ける

現在使われている 1024bit（10 進法で 330 桁）の暗号の安全性は？
ためしに 1 から $\sqrt{n}$ = 10^{165} まで割る計算だと仮定する
パソコンの一番より速めのコンピュータを使って割り算を 10^{10} 回/s 計算できるとする
10^{165} ÷ 10^{10} = 10^{155} 秒≒3× 10^{147} 年
cf.宇宙の年齢=46 億年≒5× 10^{9} 年
宇宙 10^{138} 個分の時間が必要（数桁早いスーパーコンピュータを使っても解けないことが分かった）
しかし素因数分解を地道に計算するよりも数桁早くするアルゴリズムはあるから将来新しいアルゴリズムが発見されれば解かれる可能性がある
RSA 社の解読コンテストでは 174 桁まで素因数分解されている
3107418240490043721350750035888567930037346022842 7
2754572016194882320644051808150455634682967172328 6
7824379162728380334154710731085019195485290073377 2
4822783525742386454014691736602477652346609
今の問題はこれ。解読すると$2,000 もらえます

訂正：46億年は地球の年齢で宇宙の年齢は137億年でした。

第八回　迷惑メール

SPAMメール、USE、UBEはすべて迷惑メールのこと
よくある迷惑メールの内容は出会い系サイト、ドラッグの販売等

SPAMメール送信者がメールアドレスを知る方法
1.辞書攻撃―ランダムにアドレスを生成せいて送りまくる
2.ホームページや掲示板に載せてあるアドレスをツールを使って
3.個人情報がどこからかもれた
4.1から3のいずれかの方法で取得されたメールアドレスが売買された

SPAMメールの問題点は
１）受信者の金銭、時間を無駄に使わせる
２）読み手に無関係に送られる
３）非合法な活動に使われる

届いたときにすること
１）信用しない
２）返信しない
３）クリックしない
　　米国でのアンケートでは迷惑メールに記載されたURLをクリックする人の割合31%

SPAMメールの送信国
　米国　56.8%（特にフロリダ州が多いといわれている）
　韓国　15.7%
ゾンビPCとは
ウイルスに感染したり、不正侵入者にバックドアを仕掛けられたりししたままユーザがそのことに気づかなかったり忘れてしまったりして放置されているパソコン。迷惑メールの送信、ウイルスの感染経路、踏み台、DDosなどの攻撃用などに使われる。世界で一日あたり15万7000台のコンピュータがゾンビ化され、そのうち2割以上が中国といわれる。

ベイズ理論(Bayes Theory)は、古く18世紀の牧師であり数学者であったトーマス・ベイズ(Thomas Bayes)という英国人によって考え出された原理。メールに含まれる単語に迷惑メールらしさの点数をつけていき迷惑メールかどうか判断する。

SPAMメールに対する対策としてはフィルタリングが最も有効。Thunderbird等のベイズ理論による学習機能を持ったメールクライアントを使うことでかなりフィルタリングできる。プロバイダーがとるSPAM対策も海外からのSPAMメールには意味がない。

架空請求は突然知らない業者からメールが送られてきて利用した覚えのないサービスに対する多額の請求をされる。
送られてきた場合には絶対払わず無視するのがよい。相手に情報を与えるだけなので返信は絶対してはならない。

ワンクリック詐欺
ワンクリック詐欺と広告のSPAMメールの違いはワンクリック詐欺のメールは宛先によって違うURLが記載されていること。通常、普通のURLの後ろに暗号になった文字列がついている構造になっている。ワンクリック詐欺の特”長”は受取人が興味本位でクリックするだけでメールを読んだ人のメールアドレスをフィードバックさせれる点。この場合もメールアドレスが知られるため支払いの請求メールが頻繁に送られるようになるだけで、名前・住所は伝わっていないので無視すればよい。

第九回　サイバー攻撃

サイバーテロとは何か。それは現代社会のどのような側面を表しているか。
コンピュータネットワークに依存する現在の行政・金融ライフライン
これらのコンピュータの機能不全は社会の機能不全を意味する
（ex. 2000年問題、ウイルスバスターのパターンファイルのバグによる新幹線の窓口の停止など）
サイバーテロはこれらの施設へ電子的攻撃をすることを言う

バグを含んだウイルスパターンファイルを配信したウイルスバスター

サイバーテロと通常のテロの一番大きな違いは手軽さ（命をかけたりする必要がない）の割に大きな影響を与えることができる。サイバーテロは周到ないたずらと同等。
リチャードクラークの行ったサイバーテロに類する行為、1998年4月にユーゴスラビア政府のウェブサイト宛に数日間で50万通のメールを送ってサーバをダウンさせた

マサチューセッツ州ウースター空港で電話線からの不正アクセスにより航空管制システムの一部のプログラムが消去され、天候が悪ければ飛行機が墜落したかもしれない事態がおこった。
サイバーテロでライフラインに侵入することによって
１）電話の麻痺
２）停電
３）金融業務の混乱　　などを引き起こすことができる
サイバーテロの危険性を分析したRAND社のレポートでは列車管制システムの操作による列車事故、株価操作による株価の大幅下落、飛行機の自動操縦システムに忍ばせたウイルスによる着陸時の事故などの可能性が示唆されている

これまでに行われたサイバー攻撃
１）1990年湾岸戦争（？　実際に行われたかは不明）
　　開戦10日前にアメリカがイラクに輸出されるプリンターにウイルスを入れておき
　　開戦時にイラクのネットワークを麻痺させようとした
２）コソボ紛争
　　アメリカが中国大使館を誤爆
　　中国本土から米軍、NATO軍のネットワークに対する攻撃
３）日韓サイバー戦争（？）
　　2004年1月韓国政府が竹島切手発行を準備
　　日本政府が中止を要請・２ch，Kの国の方式が韓国を侮辱していると報道される
　　1月10日2chのハングル板やKの国の方式に韓国のネチズンからのアクセスが集中し、サイトが重くなったりダウンしたりした
　　韓国ではこれを「サイバー壬申倭乱」と報道
４）2005年3月17日に外務省HPがサイバー攻撃によりつながりにくくなった
　　3月20日韓国外交通商省HPが10時間にわたり接続不能になる

日本は対策として情報セキュリティー政策会議を設置、2008年にもサイバー攻撃への対応など情報保全の指針となる「第一次情報セキュリティー基本計画」を策定する予定。

サイバーテロの手口
１）不正アクセス
　・特定のサーバをターゲット
　・不特定のセキュリティーホールを探す　　の2種類に分類される。

２）ウイルス攻撃

　メールの添付ファイルの形式で侵入することが多く、一度侵入されるとFireWallが役に立たない（FireWallでクレジットカード番号の流出を止めることはできる）
自律的にネットワークを探して攻撃するウィルスも出現
不正アクセスと違いウィルス作者を特定することはかなり困難（犯人がわかる場合はたいてい作者が友達に自慢してしまったとき）

３）トラップドア

故意に侵入口を作っておくこと（バックドアは後からあける侵入口だがトラップドアは最初から故意にプログラムに組み込まれている侵入口）
例えばほとんどのWindowsにNSAのトラップドアが組み込まれていると報道されたことがある

４）DoS攻撃

Denial of Serviceの略。外部からおびただしいデータを送りつけサービスを利用できなくする。さらにコンピュータがクラッシュする寸前にユーザ認証システムだけがクラッシュするため侵入できるようになったりする。
DDoS（分散DoS）はDistributed Denial of Serviceの略で別々のネットワークのたくさんのコンピュータから特定のサーバに対してDoS攻撃を行うことを言う。
最も手軽なDoS攻撃としてF5アタック（ブラウザでF5ボタンを連打することでウェブサーバに負荷をかける）
有名なのは田代砲（投票用スクリプト＝DoS攻撃用スクリプト）

顔を忘れた人のために、田代まさし