工学倫理　第11回
― 情報倫理 ―

奥 乃　博
京都大学　大学院情報学研究科
知能情報学専攻
知能メディア講座　音声メディア分野
http://winnie.kuis.kyoto-u.ac.jp/~okuno/
okuno@i.kyoto-u.ac.jp, okuno@nue.org
http://winnie.kuis.kyoto-u.ac.jp/~okuno/Lecture/07/ 1

第11回目の目次

1. インターネット・IT技術の影響
2. Software Engineering Code of Ethics and Professional Practice
3. IT業界の特徴
4. プライバシーの考え方
5. セキュリティはトレードオフ
6. プログラムのバグ
7. 京大公式情報倫理

2

講師の紹介

1. NTT研究所のネットワークを手作り
2. 日本最初の電子メイルネットワーク JUNET のボランティア
   - NTT 研究所がJUNETのメイル交換
   - KDD研究所が海外とのメイル交換
3. 日本最初のHTML文書作成
   http://winnie.kuis.kyoto-u.ac.jp/~okuno/1stHTML/
4. ハッカー倫理「すべて自由に」信奉者

3

ハッカー倫理

コンピュータやネットワークは世界をよりよいものにする可能性を持っており，そのためにはコンピュータやネットワークへのアクセスは制限されてはならず，かつ中央集権的なコントロールはすべて拒否されるべきである．

水谷雅彦編『岩波応用倫理学講義3情報』（岩波書店，2005）

これは極論．アクセスコントロールは最小限に抑えるべき．特にインフラは．

4

参考書

1. Johnson著（水谷・江口訳）『コンピュータ倫理学』（オーム社，2002）
2. ブルース・シュナイアー『セキュリティはなぜやぶられたのか』（日経BP社，2006）
3. ブルース・シュナイアー『暗号と秘密のウソ』（日経BP社，2006）
4. 水谷雅彦編『岩波応用倫理学講義3情報』（岩波書店，2005）
5. 京都大学全学情報セキュリティ委員会作成の資料（本資料の最後に添付）

5

情報倫理の講義の到達目標

1. セキュリティはトレードオフの問題
2. 石橋を叩き潰す日本・管理組織
   「石橋を叩いて渡る」のはよいが
   「石橋を叩き過ぎて壊す」のは？
   例）個人情報保護法の弊害
3. IT業界の現状
4. プログラムのバグの影響
5. 安全係数の理解
6. 知的所有権の理解

6

インターネット・IT技術の影響

7

インターネットでの問題行動

- 問題行動：不法侵入，窃盗，破壊，生活妨害，誹謗中傷，ストーキング，妨害行動，...
- インターネットに特有なもの
  1. グローバルな多対多の射程
  2. 匿名性
  3. 複製可能性
- 課題は
  1. 乱用の可能性を制限しつつ
  2. インターネットの膨大な積極的可能性を最大限利用すること.

8

IT技術による記録保存の変化

1. 新しい規模の情報収集を可能にした
2. 新しい種類の情報を作り出した
3. 新しい規模の情報の配布と交換を可能にした
4. 誤った情報の影響が拡大された
5. 人の生涯の情報が以前よりはるかに長く存在するようになった

- 取引記録情報（transaction generated information, TGI）
- データマイニング（data mining），データ照合

9

専門家集団の Code of Ethics

10

Software Engineering's Code of Ethics and Professional Practice (1998)

The Code created by Software Engineers for Software Engineers

The PUBLIC is primary
A SERVICE to others
Accept your OBLIGATIONS to society
Be a PROFESSIONAL
integrity and competence
consider effects on others

Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to it

11

Software Engineering Code of Ethics and Professional Practice

1. PUBLIC - Software engineers shall act consistently with the public interest.
2. CLIENT AND EMPLOYER - Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest.
3. PRODUCT - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
4. JUDGMENT - Software engineers shall maintain integrity and independence in their professional judgment.
5. MANAGEMENT - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
6. PROFESSION - Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
7. COLLEAGUES - Software engineers shall be fair to and supportive of their colleagues.
8. SELF - Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

http://csciwww.etsu.edu/gotterbarn/SECEPP/

12

ACM Code of Ethics 10/16/92

1. General Moral Imperatives.
2. More Specific Professional Responsibilities.
3. Organizational Leadership Imperatives.
4. Compliance with the Code.

Association for Computing Machinery
(世界最大の計算機科学の学会)

13

1. General Moral Imperatives.

1.1 Contribute to society and human well-being.
1.2 Avoid harm to others.
1.3 Be honest and trustworthy.
1.4 Be fair and take action not to discriminate.
1.5 Honor property rights including copyrights and patent.
1.6 Give proper credit for intellectual property.
1.7 Respect the privacy of others.
1.8 Honor confidentiality.

14

2. More Specific Professional Responsibilities

2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.
2.2 Acquire and maintain professional competence.
2.3 Know and respect existing laws pertaining to professional work.
2.4 Accept and provide appropriate professional review.
2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
2.6 Honor contracts, agreements, and assigned responsibilities.
2.7 Improve public understanding of computing and its consequences.
2.8 Access computing and communication resources only when authorized to do so.

15

3. Organizational Leadership Imperatives

3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.

3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life.

3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.

3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.

3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system.

3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.

16

4. Compliance with the Code.

4.1 Uphold and promote the principles of this Code.

4.2 Treat violations of this code as inconsistent with membership in the ACM.

17

Case Studies

1. Intellectual Property
2. Privacy
3. Confidentiality
4. Quality in Professional Work
5. Fairness and Discrimination
6. Liability for Unreliability
7. Software Risks
8. Conflicts of Interest
9. Unauthorized Access

18

日本のIT業界の問題点

20

IT業界における多重下請け

建築業界と同じ構造が存在.

1. **過重労働**, 特に力量のある中堅・若手
2. **品質の担保**, 見えない個人の技術差
3. **セキュリティ課題の進展へのキャッチアップ**
4. **法律遵守**, 例:偽装請負

浜口『社員力』ダイアモンド社

営業の努力で改善可能

逆のケース: IHI

21

IT業界の今後の動向

1. いまよりもシステムが大規模化する
   企業単位から企業間連携
2. 業界内の淘汰が進む
3. ITメーカとITサービス企業との競争が激化する
4. 世界的なアウトソーシングが進む

浜口『社員力』ダイアモンド社

こういう状況下での情報倫理とは？

22

Intermission：バリアーフリー

23

バリアーフリーとPowerPoint

色覚バリアフリープレゼンテーションにおける重要なポイント

- ２重染色 やDNAチップの画像は，緑と赤でなく、緑と赤紫（マゼンタ）で表示する．
- ３重以上 の染色は，全色の重ね合わせだけでなく重要な2色だけの組み合わせも緑と赤紫で表示する（あるいは各チャンネルの図を別々に表示する．）
- グラフや解説図では，離れた2カ所の色を照合するのが非常に難しいので，色分けされた各項目の内容を別に凡例で示すのでなく，図中に直接書き込む．また各項目は，色だけでなく線種やシンボル，ハッチングでも区別する．
- 赤は鮮やかな明るい色に見えないので，暗い背景に赤い文字を使わない．

http://www.nig.ac.jp/color/bio/index.html より引用.

24

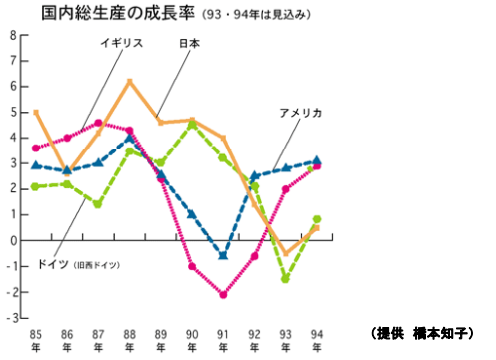
色覚バリアフリーなプレゼンテーション

色覚バリアフリーなプレゼンテーションを準備する上で重要なポイントは以下の２点

1. **書いてあるもの自体が容易に視認できないことを避ける**
   （背景色と図形や文字の色の間で明度の差が少ない，もしくは色盲の人に区別できない色の組み合わせになっている）
2. **重要な情報を区別できないことを避ける．**
   （複数の情報が色の差だけで示されている）

25

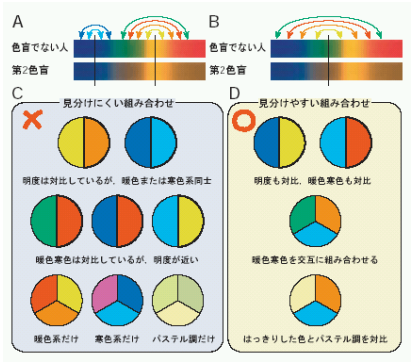
色覚バリアフリーなグラフの例



（提供　橋本知子）

26

色盲の人が見分けやすい配色



27

赤を朱色にする効果

A 色盲でない人
黒字の中に赤色の字
黒字の中に朱色の字
細字だと色が見にくい

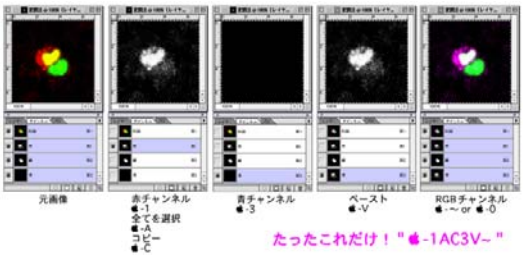
B 第1色盲のシミュレーション
黒字の中に赤色の字
黒字の中に朱色の字
細字だと色が見にくい

C 色盲でない人
白い字は見やすい
赤は鮮やかに明るい
朱色もそう変わらない

D 第1色盲のシミュレーション
白い字は見やすい
赤は暗く沈んで見える
朱色は明るく見える

28

赤緑画像からマゼンタ緑画像への変換



Adobe photoshopで赤チャンネルの絵を青チャンネルにコピーするだけ.

29

セキュリティはトレードオフ

30

セキュリティはトレードオフ

セキュリティとは，意図的で不当な行為の被害を受けないように防止すること.

1. 金庫の規格（等級）は何のため
   - 耐火金庫ー消防隊が到着するまで
   - 防盗金庫ー警察が到着するまで
2. 消防隊や警察が来ない場所での金庫

3. セキュリティ・ツール群も同じ

31

耐火金庫の性能等級

区分		記号
一般紙用	4時間耐火・急加熱・耐衝撃	4TKS
	3時間耐火・急加熱・耐衝撃	3TKS
	2時間耐火・急加熱・耐衝撃	2TKS
	1時間耐火・急加熱・耐衝撃	1TKS
	30分耐火・急加熱・耐衝撃	0.5TKS
	4時間耐火	4T
	3時間耐火	3T
	2時間耐火	2T
	1時間耐火	1T
	30分耐火	0.5T
磁気テープ用及びフレキシブルカートリッジ用	4時間耐火	4T
	3時間耐火	3T
	2時間耐火	2T
	1時間耐火	1T
	30分耐火	0.5T

http://www.nihon-safe.jp/capability/taika_detail1.html#1

32

防盗金庫の性能等級

試験の種類		等級	試験時間（1系列当りの実施時間：分）
防盗試験	耐熔断・耐工具　試験	TRTL−15	15分
		TRTL−30	30分
		TRTL−60	60分
	耐工具　試験	TS−15(*)	15分(*)
		TL−15	15分
		TL−30	30分
		TL−60	60分

(*)JIS S 1037で耐火金庫に適用する耐破壊性能.
バールを中心にした破壊テスト
TL：Tool　　TR：Torch　　TS：Tool　Small

http://www.nihon-safe.jp/capability/boutou_kinko.html

33

セキュリティはトレードオフ

1. 金庫の規格（等級）は何のため
   - 耐火金庫ー消防隊が到着するまで
   - 防盗金庫ー警察が到着するまで
2. 消防隊や警察が来ない場所での金庫
3. **セキュリティ・ツール群も同じ**

■ トレードオフは主観的

■ 力関係と思惑がセキュリティトレードオフを左右

34

安全対策とセキュリティ

安全対策	セキュリティ
同時に発生する偶発的な火災を処理するのに必要な消防署の数を考える	放火魔が消防署の能力を超える数の火災報知機を発報させ，放火という攻撃の効果を高める危険があると考える
機内持ち込み荷物にナイフが間違って入っても，X線検査装置で見つけられると考えられる	X線で検出しにくい材質のナイフを検出しにくいように隠して持ち込もうとする人物がいると考える．
緊急時，安全に避難できる非常口の数を考える	非常口を封印してビルに火をかけ，殺人を行うものがいると考える

35

人の行動への4つの環境的制約

1. **法律**
   国家安全法，プライバシー保護法，
2. **市場の力**
   食品の安全シール
   感覚的なセキュリティに傾きがち
3. **技術・アーキテクチャ**
   監視カメラの普及
4. **社会常識**
   地域社会，生活水準，私有財産制，..

36

セキュリティの考え方

1. **システムに機能不全はつきもの**
2. 敵を知る
3. 攻撃者は楽器を変えても曲は変えない
4. 技術がセキュリティのバランスを崩す
5. セキュリティとは最弱点問題である
6. 剛性はセキュリティを低くする
7. セキュリティの中心は人である
8. 防止できないものは検出する
9. 対応のない検出は意味はない
10. 識別・認証・許可
11. 価値のない対策はないが完璧な対策もない
12. テロリズムとの戦い

37

トレードオフの5段階評価法

ステップ1「守るべき資産は何か」
ステップ2「その資産はどのようなリスクにさらされているのか」
ステップ3「セキュリティ対策によって，リスクはどれだけ低下するのか」
ステップ4「セキュリティ対策によって，どのようなリスクがもたらされるか」
ステップ5「対策にはどれほどのコストとどのようなトレードオフが付随するか」

51

例：インターネットとクレジットカード

ステップ1「守るべき資産は何か」：**カード番号**
ステップ2「その資産はどのようなリスクにさらされているのか」：**クレジットカードの窃盗**
ステップ3「セキュリティ対策によって，リスクはどれだけ低下するのか」：**番号を守るのは不可能**
ステップ4「セキュリティ対策によって，どのようなリスクがもたらされるか」：**特になし**
ステップ5「対策にはどれほどのコストとどのようなトレードオフが付随するか」**インターネットの買物の利便性，価格の競争力というメリットを手放すかどうか．**

52

例：旅行中のセキュリティ

ステップ1「守るべき資産は何か」：**お金，クレジットカード，パスポート**
ステップ2「その資産はどのようなリスクにさらされているのか」：**盗難，盗難からの回復**
ステップ3「セキュリティ対策によって，リスクはどれだけ低下するのか」：**区画化すれば効果的**
ステップ4「セキュリティ対策によって，どのようなリスクがもたらされるか」：**大してなし**
ステップ5「対策にはどれほどのコストとどのようなトレードオフが付随するか」**ほとんどが利便性，若干の手間をかける気になるかどうかを考える必要．**

53

例：クレジットカード用プロファイリング

ステップ1「守るべき資産は何か」：**お金**

ステップ2「その資産はどのようなリスクにさらされているのか」：**盗難から盗難の報告があるまで長い時間がかかること．**

ステップ3「セキュリティ対策によって，リスクはどれだけ低下するのか」：**基本的に優れている**

ステップ4「セキュリティ対策によって，どのようなリスクがもたらされるか」：**プログラマによる不正は小さい．判断基準が知られると大きなリスク．**

ステップ5「対策にはどれほどのコストとどのようなトレードオフが付随するか」**システムの設置と運営，ユーザへの迷惑（受動的失敗と能動的失敗）．**

54

例：家庭用防犯警報器

ステップ1「守るべき資産は何か」：**自宅，財産，居住者**

ステップ2「その資産はどのようなリスクにさらされているのか」：**自宅に押し入ってはたらく盗み**

ステップ3「セキュリティ対策によって，リスクはどれだけ低下するのか」：**家庭用防犯警報器は検出・対応タイプの対策．誤報（能動的失敗）が大きな問題．抑止力にはなる．隣の家を狙う．被害を抑える．**

ステップ4「セキュリティ対策によって，どのようなリスクがもたらされるか」：**小さいのは設置会社の信用．アクセスコードの管理．**

ステップ5「対策にはどれほどのコストとどのようなトレードオフが付随するか」**費用と利便性．感情面．**

55

例：国民身分証明書

ステップ1「守るべき資産は何か」：**あらゆるもの**

ステップ2「その資産はどのようなリスクにさらされているのか」：**あらゆるリスク**

ステップ3「セキュリティ対策によって，リスクはどれだけ低下するのか」：**国民身分証明書は識別と認証．犯罪防止効果は小．運用面での問題．全員が持つわけではない．最大のリスクはデータベース．**

ステップ4「セキュリティ対策によって，どのようなリスクがもたらされるか」：**なりすまし．データベース情報の別目的への流用，乱用．**

ステップ5「対策にはどれほどのコストとどのようなトレードオフが付随するか」**膨大な初期，運用コスト．**

56

人 ー セキュリティの最弱点

1.ソーシャルエンジニアリング （Wikipedia.jp）

2. 元来は、コンピュータ用語で、コンピュータウイルスやスパイウェアなどを用いない（つまりコンピュータ本体に被害を加えない方法）で、パスワードを入手し不正に侵入（クラッキング）するのが目的。この意味で使用される場合は**ソーシャルハッキング**、**ソーシャルクラッキング**とも言う。
3. ソーシャル・エンジニアリングには以下のような方法が、よく用いられる。

- 重役や上司（直属でない・あまり親しくない）、重要顧客、システム管理者などと身分を詐称して電話をかけ、パスワードや重要情報を聞きだす。
- 現金自動預け払い機（ATM）などで端末本体を操作する人の後ろに立ち、パスワード入力の際のキーボード（もしくは画面）を短時間だけ凝視し、暗記する（ショルダーサーフィン）。
- IDやパスワードが書かれた紙（付箋紙など）を瞬間的に見て暗記し、メモする。ディスプレイ周辺やデスクマットに貼り付けられていることが多い。
- 特定のパスワードに変更することで特典が受けられるなどの偽の情報を流し、パスワードを変更させる（日本において、この手法でパスワードを不正入手した未成年が2007年3月に書類送検されている）。

57

パスワードの強度チェック

1. Cops を使用
   “cops” や “cops_104” で googleる

2. Crack を使用
   “c50a” や “crack5.0.tar” で googleる

59

プライバシー

60

電子的プライバシー情報センタ epic.org

1. www.epic.org 米国各州がどのタイプの記録を保護しているかの一覧表
   Privacy Laws by State (http://epic.org/privacy/consumer/states.html)

   California: Arrest Records X, Bank Records X, Cable TV X, Computer Crime X, Credit X, Criminal Justice X, Gov't Data Banks X, Employment X, Insurance X, Mailing Lists X, Medical X, Miscellaneous X, Polygraphing X, Privacy Statutes X, Privileges 0, School Records X, Soc. Security Numbers X, Tax Records 0, Tele. Service/Solicit X, Testing 0, Wiretaps X

   New York: Arrest Records X, Bank Records 0, Cable TV 0, Computer Crime X, Credit X, Criminal Justice 0, Gov't Data Banks X, Employment X, Insurance 0, Mailing Lists X, Medical X, Miscellaneous X, Polygraphing X, Privacy Statutes X, Privileges X, School Records X, Soc. Security Numbers 0, Tax Records X, Tele. Service/Solicit X, Testing 0, Wiretaps X
2. Practical Privacy Tools

   Snoop Proof Email, Anonymous Remailers, Surf Anonymously

61

The Code of Fair Information Practices '73

1. 1974のプライバシー法のモデル. 現在ではプライバシー法は大きく変化.
2. 5つの綱領からなる
   a. 存在を秘匿された個人情報記録システムは許されない.
   b. 個人が自分のどんな個人情報が記録に残されているか, また, どのように使われているかを知る方法が存在しなければならない.
   c. 収集目的以外の目的に, 本人の同意なく個人の情報が使われることを阻止する方法が存在しなければならない.
   d. 自分に関する情報を訂正し修正する方法が存在していなければならない.
   e. 個人情報を作成, 蓄積, 利用, 配布するすべての組織は, その情報の信頼性を保証し, またその誤用濫用の予防措置を取らねばならない.
3. 現実の問題: c. などは守られていない
   d. どうやって個人が自分の情報をチェックできるのか.

62

EU: データの質に関する原則第2章第1節

1. 加盟国は個人データを次のように規定しなければならない
   a. 公正かつ合法的に処理されること
   b. 特定の, 明示的で合法的な目的のために収集され, その目的と相容れいない目的のために利用されてはならない. 歴史的, 統計的, 科学的な目的のための再処理は, 加盟国が適切な保護条件を保証する限りは特定の目的とは相容れないものとは見なさない.
   c. データは, それが収集され, また再処理される目的に適切でなければならず, 過度になってはならない.
   d. データは正確で, 必要な場合には最新のものに更新され続けねばならない. 不正確あるいは不完全なデータは, それが収集され, あるいは再処理される目的に応じて, 消去されるか, あるいは修正されなければならない.
   e. そのデータが収集され再処理される目的に必要である以上にわたっては, データ主体が特定されないようにしなければならない. 加盟国は歴史的, 統計的, 学術的利用のためのより長期間にわたって保存される個人情報のための適切な保護条件を定めなければならない.

63

バグ（Bug）

64

Bugを最初に見つけたのは

- Grace Murray Hopper
  (Dec. 9, 1906 – Jan. 1, 1992)
- 1st women to receive a Ph.D in mathematics.
- Sep. 9, 1945. Mark II の Relay #70, Panel F で発見.
- bug はそれ以前から使用.
- コンパイラ開発にも従事.
- NavyでCOBOL言語の検証ソフト開発.

65

A Bug (moth) in the Mark-II

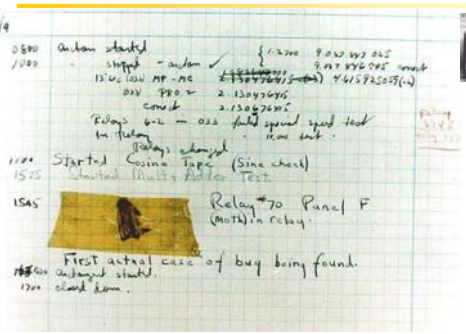


Photo #: NH 96566-KN (Color)

U.S. Naval Historical Center Photograph.

実験ノートをつけること。ルーズリーフはだめ

10大Bugの3個（by Wired News）

1. 1962年7月22日　火星探査機『マリナー1号』:マ リナー1号は打ち上げ時に予定のコースを外れたが、これは飛行ソフトウェアのバグが原因だった。地上の管制センターは大西洋上でロケットを破壊した。事後 調査により、鉛筆で紙に書かれた数式（$\bar{R}_n$）をコンピューターのコードに置き換えるときにミス（－を忘れた）が起き、これが原因でコンピューターが飛行コースの計算を誤ったこと が判明した。
2. 1982年　旧ソ連のガス・パイプライン:シベリアを横断するガス・パイプラインの管理に旧ソ連が購入したカナダ製のコンピューターシステムに、米中央情報局(CIA)のスパイがバグを仕掛けたことがあるという。旧ソ連は当時、米国の機密技術を密かに購入しようと――または盗み出そうと――しており、このシステムを入手したのもその一環だった。だが、計画を察知したCIAはこれを逆手にとり、旧ソ連の検査は問題なく通過するが、いったん運転に入ると機能しなくなるように仕組んだとされる。この結果起きたパイプライン事故は、核爆発以外では地球の歴史でも最大規模の爆発だったという。
3. 1985～1987年　セラック25:複数の医療施設で放射線治療装置が誤作動し、過大な放射線を浴びた患者に死傷者が出た。セラック25は2 種類の放射線――低エネルギーの電子ビーム（ベータ粒子）とX線――を照射できるよう、既存の設計に「改良」を加えた治療装置だった。セラック25では電 子銃と患者の間に置かれた金属製のターゲットに高エネルギーの電子を打ち込み、X線を発生させていた。セラック25のもう1つの「改良」点は、旧モデル『セラック20』の電気機械式の安全保護装置をソフトウェア制御に置き換えたことだった。ソフトウェアの方が信頼性が高いとの考えに基づく判断だった。

   しかし、技術者たちも知らなかった事実があった―セラック20およびセラック25に使われたOSは、正式な訓練も受けていないプログラマーが1人で作成したもので、バグが非常にわかりにくい構成になっていたのだ。「競合状態」と呼ばれる判明しにくいバグが原因で、操作コマンドを素早く打ち込んだ場合、セラック25ではX線用の金属製ターゲットをきちんと配置しないまま高エネルギーの放射線を照射する設定が可能になっていた。これにより少なくとも5人が死亡し、他にも重傷者が出た。

4. 1988年――バークレー版UNIX(BSD)のフィンガーデーモンによるバッファー・オーバーフロー：最初のインターネットワームとなった通称『モーリス・ワーム』は、バッファー・オーバーフローを悪用し、1日 足らずで2000台から6000台のコンピューターに感染した。原因となったのは、標準入出力ライブラリー・ルーチン内の「gets()」という関数の コードだ。「gets()」関数はネットワーク越しにテキストを1行取得するように設計された。しかし、残念ながら「gets()」関数は入力を制限する ように は作られていない。そのため、あまりにも大きな入力があった場合には、接続可能なあらゆるマシンをワームが占拠する元凶になった。

   プログラマーは「gets()」関数を使用コードから排除することで問題に対処しているが、C言語の標準入出力ライブラリーからこれを削除することは拒否しており、この関数は現在も存在している。
5. 1988～1996年――『ケルベロス』の乱数生成アルゴリズム：ケルベロスは暗号を使ったセキュリティーシステムだが、乱数発生器に与えるシード(種)が適切でなく、真にランダムな乱数が生成されていなかった。

   その結果、ケルベロスによる認証を用いているコンピューターについて、非常に簡単な方法で侵入可能な状態が8年間にわたって続いた。このバグが実際に悪用されたかどうかは、今も定かではない。
6. 1990年1月15日―― 米AT&T社のネットワーク停止：米AT& T社の長距離電話用交換機『4ESS』を制御する最新版のソフトウェアにバグが入りこんだ。このため、4ESSは隣接するマシンの1つから、ある特定の メッセージを受け取るとクラッシュするようになってしまった――そしてそのメッセージとは、クラッシュした交換機が復帰した際に、隣接する交換機に送信するものだった。

   ある日、ニューヨークの交換機がクラッシュし再起動した。するとそれが原因で隣接する複数の交換機がクラッシュし、これらの交換機が再起動すると隣接する複数の交換機がさらにクラッシュし、この現象が延々と続いた。しばらくすると、114台の交換機が6秒ごとにクラッ シュと再起動を繰り返すようになった。この影響でおよそ6万人の人々が9時間にわたって長距離通話サービスを利用できなくなった。修復のため、技術者たち は1つ前のソフトウェアをロードした。

7. 1993年――インテル社製『Pentium』(ペンティアム)による浮動小数点数の除算ミス：米インテル社が大々的に売り出したPentiumチップが、特定の浮動小数点数の除算で誤りを引き起こした。たとえば、4195835.0／3145727.0を計算させると、正しい答えの1.33382ではなく1.33374となる。0.006%の違いだ。

   実際にこの問題の影響を受けるユーザーはごくわずかだったが、ユーザーへの対応から、同社にとって悪夢のような事態につながった。概算で300万～500 万個の欠陥チップが流通していた状況で、インテル社は当初、高精度のチップが必要だと証明できる顧客のみをPentiumチップの交換対象とした。しかし、最終的にインテル社は態度を改め、不満を訴えるすべてのユーザーのチップ交換に応じた。この欠陥は結局、インテル社に約4億7500万ドルの損害を与 えた。
8. 1995年／1996年――『Ping of Death』:[ピング・オブ・デス、不正なピングパケットによる攻撃] 分割送信されたIPパケットの再構成を行なうコードのチェックとエラー処理が不十分だったため、インターネット上の好きな場所から不正な形式のピングパケットを飛ばすことで、さまざまなオペレーティング・システム(OS)をクラッシュさせることができた。影響が最も顕著に現れたのはウィンドウズ搭載マシンで、この種のパケットを受け取ると、「死のブルー・スクリーン」と呼ばれる青い画面を表示して動作が停止してしまう。しかしこのバグを利用した攻撃は、ウィンドウズのみならず、マッキントッシュやUNIXを使ったシステムにも多くの被害をもたらした。
9. 1996年6月4日――『アリアン5』フライト501：欧州宇宙機関の開発したロケット、アリアン5には、『アリアン4』で使われていたコードが再利用されていた。しかし、アリアン5ではより強力なロケットエン ジンを採用したことが引き金となり、ロケットに搭載された飛行コンピューター内の計算ルーチンにあったバグが問題を起こした。エラーは64ビットの浮動小 数点数を16ビットの符号付き整数に変換するコードの中で起こった。アリアン5では加速度が大きいため、64ビット浮動小数点で表現される数がアリアン4 のときよりも大きくなってオーバーフローが起こり、最終的には飛行コンピューターがクラッシュしてしまった。

   フライト501では、最初にバックアップ・コンピューターがクラッシュし、それから0.05秒後にメイン・コンピューターがクラッシュした。その結果、エンジンの出力が過剰になり、ロケットは打ち上げ40秒後に空中分解してしまった。

10. 2000年11月――パナマ国立ガン研究所：米マルチデータ・システムズ・インターナショナル社（本社ミズーリ州）が製作した治療計画作成用ソフトウェアを使っていたパナマの国立ガン研究所で、放射線治療で照射する放射線量の計算を誤る一連の事故が起きた。
マルチデータ社のソフトウェアでは、健康な組織を放射線から守るための「ブロック」と呼ばれる金属製のシールドの配置を、コンピューターの画面上に描いて決めるようになっていた。しかし、同社のソフトウェアではシールドが4個しか使えなかったにもかかわらず、パナマ人の技師たちはこれを5個使いたいと考え た。
技師たちは、真ん中に穴を持つ1個の大きなシールドとして、5個のシールドをまとめて表示させれば、ソフトウェアをだますことができることを発見した。だが、そうした配置にした場合、穴の描き方によってこのソフトウェアが返す計算結果が違ってくることにはまったく気づいていなかった。ある方向に向けて描くと正しい照射量が計算されるが、違う方向に描くと必要な照射量の最大2倍の量を推奨してきたのだ。
少なくとも8人の患者が死亡し、さらに20人が過剰照射によって深刻な健康被害を受けたとみられている。技師たちは、コンピュータによる計算結果を手作業で再チェックする法的義務を負っていたため、殺人罪で起訴されることになった。

11. 2003年8月14日――米国北東部の大停電：3分間に21の発電所が脱落し、オハイオ州の系統で電圧異常が起こった.

安全係数は6倍.

71

Safety factor is *six times*.

- Suspension bridgesの設計の例
- John Roebling designed the Brooklyn Bridge which was built from 1869 to 1883.
- He designed the stiffness of the truss on the Brooklyn Bridge roadway to be *six times* what a normal calculation based on known static and dynamic load would have called for.
- *Galloping Gertie* of the Tacoma Narrows Bridge which tore itself apart in a windstorm in 1940, due to the nonlinearities in aerodynamic lift on suspension bridges modeled by the eddy spectrum.

72

Safety factor is *six times*.

- 企業は安全係数・利用予測を大幅に低く見積る
  - 姉歯事件
  - ソフトバンクのMNP（携帯電話番号ポータビリティ）
  - NTT IP電話（民営化の影響，*cf* 黒電話20年耐用）
- 官庁は利用予測・耐用年数を大幅に高く見積る
  - 新幹線栗東新駅利用者予測
  - 神戸空港，北九州空港，静岡空港，…
  - ダムはムダ
  - 防衛省，米軍仕様（秋葉原仕様の方が高性能!!!）

74

レポート課題

- 何か1つセキュリティ問題を取り上げ，その対策案を考えなさい．世の中で議論されているような対策でもよい．その対策について，トレードオフの5段階評価法を使って，有効かどうかを判断しなさい（A4　1ページ以上）．
- 締切：1月10日（木）
- 提出先：桂Aクラスター事務室　or
  吉田　工学部8号館教務窓口

75

参考資料

京都大学全学情報セキュリティ委員会作成の資料

例年，本資料が「情報倫理」の講義資料として使用．

76

情報化社会と倫理

情報化社会と倫理（1）

- 情報通信，デジタルメディア技術の急速な進展，普及
  - コンピュータ，ネットワーク，携帯電話の普及
  - 音声，画像，映像のデジタルメディア化
  - 生命情報（遺伝子など）の利用
- 「情報」の持つ社会的特性
  - 価値の多様性
  - 複製・伝播の容易さ
  - 信憑性の問題

―情報の多様な利用可能性と抱える社会的課題

情報化社会と倫理（2）

- 情報化社会の構築の必要性
  - 急速な変化に対応し
  - 望ましい社会を創出することが求められる
- 情報化社会構築のための方法
  - 技術での対応
  - 法などの社会制度での対応
  - 行動規範での対応
  - 教育による対応

関連法規

- 法は技術の進展，社会的問題の発生に応じて整備される．
- 主な関連法規
  - 刑法：電磁的記録に関連する罪，コンピュータに関連する罪などが定められている．
  - 不正アクセス禁止法：不正アクセスの禁止と罰則などを定めている．
  - 個人情報保護法
  - 著作権法
  - 特許法
  - 商標法
  - 民法：ソフトウェアの利用はライセンス契約に従う．
    「ソフトウェアのライセンス契約に違反した利用を行った場合、民法に従って損害賠償請求を受けるおそれがある。」
  - プロバイダ責任制限法：特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律

参考文献

- セキュリティ研究会著，「最新インターネットセキュリティがわかる」，技術評論社，平成12年3月．
- 情報教育学研究会・情報倫理教育研究グループ編著，「インターネットの光と影 Ver.2 －被害者・加害者にならないための情報倫理入門―」，北大路書房，平成15年3月．
- 情報教育学研究会・情報倫理教育研究グループ,「インターネット社会を生きるための情報倫理」，実教出版，平成14年3月．
- 文部科学省大学共同利用機関メディア教育開発センター，「情報倫理　デジタルビデオ小品集」(CD-ROM)，平成15年．
- ネットロー　URL：http://www.netlaw.co.jp/
- 鮫島正洋　編著「特許戦略ハンドブック」、中央経済社、平成15年4月。
- 谷川英和、河本欣士「特許工学入門」、中央経済社、平成15年5月。

情報セキュリティ

情報システムへの脅威と対策

- 「人為的な脅威」と「物理的な脅威」
- インターネット利用により情報システムの利便性とともに人為的な脅威が増大
  - 盗聴，侵入，なりすまし，改竄，破壊，コンピュータウイルス
- 情報セキュリティ：脅威への系統的な対策

情報セキュリティとは

- 情報システムの機密性，完全性，可用性を確保・維持すること．
  - 機密性(confidentiality)
    - 情報資産（データ）の第三者への漏洩を防ぐ
    - 盗聴・傍受やID・パスワード流出への対処
  - 完全性(integrity)
    - 情報資産（データ）の改変を防ぎ，正確性・完全性を維持すること
    - データ，データベース，ホームページやメールのヘッダー情報の改ざん・破壊への対処
  - 可用性(availability)
    - システムの停止を防ぎ，情報資産が定められた方法でいつでも利用できるようにすること
    - メール爆弾などの破壊攻撃への対処

アカウントとパスワード

- 多数の人が利用する情報システムでは
  - アカウント（銀行の口座番号に相当）と
  - パスワード（暗証番号に相当）で

  利用者を特定し，サービスを提供する．
- アカウントとパスワードの「適正な管理」が利用者とシステムの保護のために必要
  - アカウントやパスワードが悪意を持った人間に知られると何が生じるか？
    - システム管理者の権限で利用されたら？
    - 他の利用者になりすました利用の脅威は？

アカウントとパスワードの管理

- ユーザ側の対策
  - システムのアカウントの適正な利用
  - 類推されやすいパスワードの使用禁止
  - 定期的なパスワードの変更
  - アカウントを不必要に他人に教えない
  - パスワードを他人に教えない，見られないようにする
  - 計算機（端末）にログインしたまま席をはなれない．
- システム側の対策
  - パスワードやパスワードファイルの暗号化
  - 類推されやすいパスワードの入力の制限
  - パスワードの入力エラー許可回数の制限など

類推されやすいパスワード

- 計算機を利用してパスワードを破る脅威
  - 大量の候補を試すことができる
- 類推されやすいパスワードを使用しない
  - 短いパスワード
  - 同一の文字種だけからなるパスワード（例えば数字だけ，英小文字だけ，英大文字だけなど）
  - 辞書に現れる単語，人名，商品名
  - 個人の属性（誕生日など）

電子メールの特性と取り扱い（1）

- 電子メールの特性
  - 平文通信：電子メールはメッセージを平文で送受する（葉書のようなもの）．盗聴の恐れがある．盗聴されると困るものはメッセージの暗号化などで対処．
  - 到達が保証されない：多くの場合，電子メールは受け手側のサーバに即時に配達されるが，システムダウンなどで配送が遅れたり，配送できなかったりするリスクがある．
  - From アドレスは詐称が容易．メール配送システムは差出人が本人であるかどうかは検証しない．

電子メールの特性と取り扱い(2)

- 電子メールの利用上の問題と対応
  - コンピュータウイルス:メールに添付されるファイルを介して伝染するものが多い.
    対策:ウイルス対策ソフト・サービスの導入, 利用
  - SPAM:大量の宣伝メールなどを流す行為.
    対策:不必要に電子メールアドレスを公開しない. SPAMに抗議などの返事を書かない. フィルタリングソフトなどの利用
  - 怪しいメールに記載されている WWW へのリンクは注意が必要. 安易にクリックしてブラウザを起動しない.
  - チェーンメール, デマメール, 詐欺, 脅迫, いやがらせ:電子メールも従来の手紙などと同様に悪用される. 落ちついて対応する.

Webブラウザの扱い

- インターネット上で World Wide Web (WWW)を利用した様々なサービスが展開されている.
  - WWW の特性を理解して利用する.
- コンピュータウィルス対策
  - 不正なプログラムが埋め込まれたホームページへのアクセスによりコンピュータウィルスに感染する危険がある.
    対策:OS, ブラウザの更新, ウィルス対策ソフトの導入
  - ホームページを介したソフトウェアのダウンロードによるウイルス感染.
    対策:信頼のおけるサイトからのダウンロード.

暗号化と「成りすまし」防止(1)

- 暗号化
  - 通常の WWW のプロトコル(http) は平文通信.
  - クレジットカード番号など盗聴されては困る情報は暗号化して通信する.
  - 利用に際しては,
    - SSLなどの暗号化プロトコルが利用されているか,
    - 当該サイトを認証機関が身元確認を行っているかを確認する.

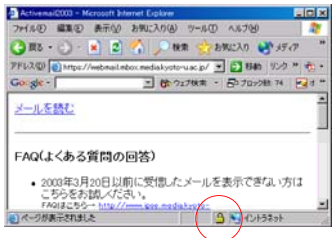
      ⇒スライド20参照

暗号化と「なりすまし」防止(2)

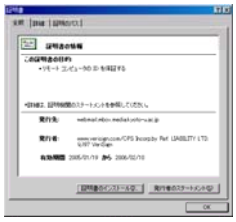
- 公開鍵暗号
  - 暗号化と複号を異なる鍵で実現.
  - 片方を公開し(公開鍵), 暗号化通信や電子署名, 認証に利用.
  - 公開鍵から秘密鍵の推測が困難なように設計.

    PKI(Public Key Infrastructure):公開鍵基盤
- 暗号化プロトコル
  - SSL (Secure Sockets Layer): 米ネットスケープ社によるデータの暗号化プロトコル. Webブラウザに実装されている
  - SET (Secure Electronic Transaction): 米VISA社と米Master社によるクレジットカード決済専用の暗号プロトコル
- 認証機関
  - WWW サーバのなりすましを防止するために第三者として認証機関がサーバの身元確認を行う

Web ブラウザでの暗号化の確認



鍵アイコンをっダブルクリックすると Web サイトの証明書が表示される。
発行先、発行者、有効期限を確認



鍵がかかっている表示は暗号化通信(SSL)であることを表す。
不正な証明書の場合、警告が出るので注意

コンピュータ・ウイルス(1)

フロッピーなどの記録媒体やメールの添付ファイルによる感染する悪意のあるコンピュータプログラム

- 機能
  - 自己伝染機能(自分自身を自動的・大量に複製)
  - 潜伏機能(発病するまでに内部に潜伏し大量にウイルスを複製)
  - 発病機能(プログラム実行回数や日時で発病し実害を与える. パソコンファイルの破壊や電子メールでのウイルス拡散)
- 種類
  - マクロウイルス
  - プログラム感染型ウイルス
  - ブート感染型ウイルス
  - コンピュータワーム
  - トロイの木馬
- 被害
  - 情報漏洩:パソコンファイルをメールに添付して送信.
    ⇒管理者権限奪取にも利用.
  - Botnetへの参加:IRCサーバを介して命令元からの遠隔操作でDDoS攻撃やspam発信などの不正アクセスに加担 ⇒ 加害者となる

コンピュータ・ウイルス(2)

- 対策
  - 対策ソフトの導入（ウィルス発生から対策ソフトの対応までには遅れがあることを理解），OSなどの更新
  - 良く分からないプログラムは実行しない。
  - オフィスソフトなどのマクロ実行の停止。
  - Web ブラウザなどのセキュリティレベルを上げる.
  - ウィルスの侵入しにくいネットワークの構成.
  - ウィルス対策のなされてないパソコンをネットワークに接続しない.
  - OS やオフィスソフトなどソフトウェアの更新，修正プログラムの適用

パソコン等のセキュリティ対策(1)

- パーソナルコンピュータ(PC)の扱い
  - OSのセキュリティ機能の脆弱さ
  - 私物PCなどの組織への持ち込みとネットワーク接続の危険性
  - OS，アプリケーションなどに最新の修正プログラムを適用
  - ウィルス対策ソフトの導入
  - 端末から離れる際には他人に操作されないように
- プリンタ・コピー・FAXの扱い
  - ネットワーク接続されたプリンタからの機密漏洩
  - 放置された印刷出力からの機密漏洩
- 記録メディアの扱い
  - 外部記憶メディア（フロッピー，CD-R, DVD-R, MOなど）によるデータの不正持ち出しやウイルス感染の危険性，ハードディスクを含めた廃棄での機密漏洩への注意

パソコン等のセキュリティ対策(2)

- データのバックアップ
  - データ喪失の危険性
    - ハードディスクなどの機械的故障
    - 誤操作やコンピュータウィルスによる破壊
  - データ喪失のコストの認識
  - 対策
    - データの外部記憶メディアへのバックアップと安全な保管
- 電源のバックアップ
  - 停電時に作業中のデータを失わないために無停電電源などを導入

情報セキュリティポリシー (Security Policy)

- 情報セキュリティ
  - 多面的な活動が必要．系統的な対策とその明文化が求められる.
- セキュリティポリシーとは
  - 組織が情報資産に対してどのようにして取り組み，組織に所属する人々がどのように行動すべきかの方針を明文化した規範
- 基本方針，対策基準，実施手順
  - 実施手順は原則非公開であり，それ自身の漏洩が脅威となることを認識。
  - 組織の構成員は遵守を義務付けられる。

本学の情報セキュリティポリシーに係る規程

- 京都大学の情報セキュリティの基本方針
  http://www.kyoto-u.ac.jp/notice/05_notice/close/common/security/housin.htm
- 京都大学の情報セキュリティ対策に関する規程.
  http://www.kyoto-u.ac.jp/notice/05_jim/j_sec02.htm
- 京都大学情報セキュリティ対策基準
  http://www.kyoto-u.ac.jp/notice/05_jim/j_sec01.htm
- 京都大学情報資産利用のためのルール
  http://www.kyoto-u.ac.jp/notice/05_notice/close/common/security/rule.htm
- コンピュータ不正アクセス対応連絡要領
  （不正アクセス発生時の対応）
  http://www.kuins.kyoto-u.ac.jp/applications/renraku-1.pdf
- 所属部局の情報セキュリティポリシー実施手順遵守

ネットワーク利用に伴う被害への注意

- 電子メールや WWW を利用した詐欺，ストーキングなどの被害を受ける可能性.
  - 日頃からこの種の問題に注意払い，情報を得る.
  - 問題が生じたら落ち着いた対応をとる.
  - 自分だけで解決しようとせず，専門家の助言などを得る.
- 不正アクセスを発見した際の連絡先
  - コンピュータ不正アクセス対応連絡要領に従う.
- 相談窓口
  - 情報環境部情報基盤課情報セキュリティ対策室
    q-a@kuins.kyoto-u.ac.jp (tel: 075-753-7490)

個人情報の保護

個人情報の保護(1)

- 個人情報の流出は大きな問題
- OECDプライバシーガイドライン
  - Organization for Economic Cooperation and Development（経済協力開発機構）の1980年理事会勧告．基本8原則
    - 個人情報の収集（収集制限，データ内容，目的明確化）
    - 個人情報の運用（利用制限，安全保護，開発・実施・政策の公開）
    - 情報主体の権利（個人参加の原則：個人の確認や異議申し立てなど）
    - 収集者の義務（上記の原則の実施責任）
- わが国
  - 個人情報保護法：平成15年5月に制定，平成17年4月に施行
  - 個人情報取扱業者に
    - 個人情報の利用目的の特定，利用目的による制限，
    - 適正な取得，利用目的の通知，
    - 正確性の確保，安全管理措置，従業員の監督，委託先の監督，
    - 第三者提供の制限，
    - 事項の公表，開示，訂正等，利用停止等を求めている．
  - 国や独立行政法人には，よりレベルの高い個人情報の保護を定めている．
    - 京都大学には「独立行政法人等の保有する個人情報の保護に関する法律」が適用される．
    - 京都大学における個人情報の保護に関する規程
      http://www.kyoto-u.ac.jp/uni_int/kitei/reiki_honbun/aw00209631.html

個人情報の保護（2）

- 個人情報に配慮した行動
  - 安易に自分自身の個人情報をネットワークに出さない。
  - 他人の情報の取扱いに注意
- 肖像権への配慮
  - 他人の写真などの公開には本人の許可を得る。
- 専門家としての倫理
  - 大学では専門性からさまざまな個人情報を扱うことが多い，取扱には十分な指導を受ける．
- 公開サーバでの個人情報の掲示に注意

教育・研究における著作物の利用

電子化された著作物の適正な利用

- 著作物は
  - その利用により価値が創出されるが，
  - 著作者の権利を保護した上での利用が必要．
- 著作物は著作権法で保護．ソフトウェアの利用はライセンス契約に従う．
- 電子化された著作物の違法コピー問題
  - 組織内のソフトウエアの違法コピーや電子化された著作物の複製，公衆送信は重大な問題
    - 社会的信用の失墜
    - 組織の倫理，構成員のモラルの失墜
  - ソフトウエアの適切な管理が必要

ソフトウェア・ライセンスの形態

- ソフトウエアライセンスの形態の認識と遵守
  - クライアント・サーバー製品
    - 接続クライアント数型，同時使用ユーザ数型
  - スタンドアロン製品
    - CPU固定型，ユーザ固定型
  - 大規模ユーザ向け製品
    - 特定サイト型（サイト内で制限なしにインストール可能）

研究における著作物の適正引用

- 論文などでの著作権に則った適切な引用
  - 著作権法で著作者の許諾なく引用が可能な条件を理解し，実践する．
    - 公表されていること
    - 引用の目的
    - 出所の明示
    - 必要最小限の引用

著作権法
（引用）
第三十二条　公表された著作物は、引用して利用することができる。この場合において、その引用は、公正な慣行に合致するものであり、かつ、報道、批評、研究その他の引用の目的上正当な範囲内で行なわれるものでなければならない。

著作物の教育用途での複製

- 著作権法では教育機関での一定の条件のもとでの複製等が認められている．平成16年から範囲を拡大．
- 制限を理解した上での利用

著作権法
（学校その他の教育機関における複製等）
第三十五条　学校その他の教育機関（営利を目的として設置されているものを除く。）において教育を担任する者及び授業を受ける者は、その授業の過程における使用に供することを目的とする場合には、必要と認められる限度において、公表された著作物を複製することができる。ただし、当該著作物の種類及び用途並びにその複製の部数及び態様に照らし著作権者の利益を不当に害することとなる場合は、この限りでない。
2 公表された著作物については、前項の教育機関における授業の過程において、当該授業を直接受ける者に対して当該著作物をその原作品若しくは複製物を提供し、若しくは提示して利用する場合又は当該著作物を第三十八条第一項の規定により上演し、演奏し、上映し、若しくは口述して利用する場合には、当該授業が行われる場所以外の場所において当該授業を同時に受ける者に対して公衆送信（自動公衆送信の場合にあつては、送信可能化を含む。）を行うことができる。ただし、当該著作物の種類及び用途並びに当該公衆送信の態様に照らし著作権者の利益を不当に害することとなる場合は、この限りでない。

知的財産権
Intellectual Property Right

知的所有権との邦訳もあり。

知的財産権

- 著作権（表現を保護）
- 特許権（技術的なアイデアを保護）
- 実用新案権（技術的なアイデアを保護）
- 意匠権（物品のデザインを保護）
- 商標権（商品やサービスのマークを保護）
- その他（不正競争防止法など）

著作権法による保護内容

- 著作権（財産権）
  - 著作物の利用を許諾・禁止する権利
  - 複製権、公衆送信権、翻訳権、翻案権、頒布権、など
- 著作者の人格権
  - 著作者の人格的権利を保護する権利
    - 公表権（未公表著作物を公表するかどうか決定する権利）
    - 氏名表示権（著作物に著作者名を付すかどうかの権利）
    - 同一性保持権（著作物の内容や題号を改変されない権利）

著作物性

- 著作物
  - 思想又は感情を創作的に表現したもの
    - 事実，データ，情報は著作物でない．
    - 高度の創作性は要求されない（若干の創作性）
    - 表現物でなければならない．アイデアは保護しないが表現物は保護する．
    - 1アイデアに1表現の法理（1つのアイデアに1つしか表現がない場合，表現も保護しない．Sweat of braw（額に汗）の法理．労働によって集めたデータの集積も単なるデータなので保護しない．
  - 例
    - 地図は図形著作物
      客観的な表現ではあるが，記入項目の取捨選択という創作的行為が含まれる．かつ，専門家が作成したものであることも考慮される．
    - 単純な住宅地図は著作物とはならない。
      家の形と表札情報のみからなる、単純な住宅地図は著作物ではないとされる．上記の1アイデアに1表現の法理による解釈。
    - 事実の報道（記事）：単なる事実は雑報で保護されないが，記事全体は著作物の扱いとなる．

プログラムの著作権

- プログラムの著作権
  - 著作物として著作権の保護対象になっている（著作権法2条1項10号）。
- 著作権 vs 特許権
  - 一つのプログラムであってもその保護の観点がそれぞれの法律で異なる。
    - プログラムの記述が表現であるというとらえ方をすれば著作権での保護が考えられ、システム化した発明としてとらえれば特許権での保護が考えられる。
- プログラムの創作性と類似性
  - 誰が記述しても同じような表現になってしまうようなものは、どんなに苦労して作り上げたものであっても著作権法では保護されない。
    - プリンタの制御プログラムは創作性がないとしたり（システムサイエンス事件）、ハードディスクへのアプリケーションのインストールを行うバッチファイルには創作性がないとして著作権侵害を否定した判決（IBF事件地裁判決）がある。
  - 他人のプログラムのデッドコピー（丸写し）
    - 著作権侵害。他人のプログラムの動作や画面インタフェースを似せて作ったプログラムであっても著作権侵害になる場合がある。（米国：ロータス1-2-3の画面構成や操作感覚を真似たとして後発の表計算ソフトに著作権侵害認定）
  - 他言語によるプログラム書き換え
    - 例えば、BASICで記述されたものをCで書き換え。この行為は原著作権者の権利（複製、翻訳、翻案権）が及ぶので許可を得なければ権利侵害。

データベースの著作権

- データベースは著作権法で保護される（データベース著作物）
  - （著作権法12条の2第1項）。情報の選択的な体系や構成が創作性を有するもののみ保護。
    - 米国ではABC順に名前を並べただけの電話帳は著作物として保護されないとした判決あり（ファイスト判決）。
- データは著作権では保護されていない．
  - 著作権は，表現物・創作物の保護．
  - データ作成のための投下資本の保護は別物．これを著作隣接権で保護する動きあり

ウォール・ストリート事件

- 米国でTHE WALL STREET JOURNALを発行するDow Jones社が、日本においてWSJの記事を抄訳した文書を作成・頒布するノウハウ・ジャパンという会社を提訴。
  - KJは、WSLが発行される毎に、WSJの記事を抄訳した文書を作成し、有料で、これを会員に送付。
  - KJの文書は、「ウォール・ストリート・ジャーナル　89年9月28日木曜日」のように、その表題にWSJの名称、日付け及び曜日を取り入れ、当日の記事の全部又は一部が1行当たり約34字で1行ないし3行程度の日本語に訳されて記載され、WSJに掲載されていない出来事が記載されることはなかった。
  - KJの文書には、WSJの大半の記事が抄訳され、WSJの当該記事の掲載順と同じ順で記載。
- 裁判所の判断：編集著作権の翻案権の侵害
  - WSJの創作性
    ニュース編集者が、送られてきた原稿の採否を決定。一日分のWSJは、A2判数十頁で構成され、その中には数百に及ぶ記事、社説、株式相場、広告等が掲載。WSJのこのような紙面構成は、これらの記事、写真、広告等の選択及び配列について創作性があると判断。
  - KJの文書は、WSJの記事に掲載されていない出来事がKJの文書に記載されていることはなく、また、その配列もほぼ同一。よって、KJは、DJがWSJについて有する編集著作権の翻案件を侵害。

電子地図の著作物性

- 地図をデジタル化するとその著作権は
  - スキャナ読み込みなどの単なる電子化なら権利は生まれない．デジタル化された地図上に名前などを配置しても著作権はない．
- 電子地図はデータベース著作物か？
  - 情報の選択又は体系的な構成によって創作性を有するものは「データベース著作物」として保護する．「データベース」とは，論文，数値，図形その他の情報の集合物で，検索できるように体系的に構築したもの．
  - 検索機能のある電子地図は，データベース著作物とされる．

公衆送信権

- 「公衆送信」
  - 著作権法改正（平成10年1月1日から施行）。「公衆送信」という概念を創設して「インタラクティブ送信」に関する用語の整理を行った。
  - 「公衆によって直接受信されることを目的として無線通信または有線電気通信の送信を行うこと」（改正著作権法2条1項7の2号）。
    - 放送
      「テレビ放送やラジオ放送など、公衆に同一内容を同時に受信させる目的で行う無線による送信」（同法2条1項8号）
    - 有線放送
      「CATV放送や有線音楽放送など、公衆に同一の内容を同時に受信させる目的で行う有線による送信」（同法2条1項9の2号）
    - 自動公衆送信（新たに創設）
      「インターネットのホームページなどを用いて、公衆からの求めに応じて自動的に行う送信」（同法2条1項9の4号）。いわゆる「インタラクティブ送信」がこれに該当。
    - その他の公衆送信
      「放送」「有線放送」「自動公衆送信」の定義に含まれないものでも「公衆によって直接受信されることを目的として無線通信または有線電気通信の送信」を行えば、公衆送信であり、これには、たとえば、電話で申し込みを受け手動でFAX送信する場合などが該当。

公衆送信

- 有線vs無線
  - 有線であろうと無線であろうと公衆に対する送信を「公衆送信」と定義し、「公衆送信」に対して著作権が及ぶ。
- 放送、有線放送、自動公衆送信
  - 「公衆送信」のうち、「同一内容を同時に無線で送信する場合」を「放送」
  - 「同一内容を同時に有線で送信する場合」を「有線放送」
  - WWWのようなインタラクティブな送受信を「自動公衆送信」
    - 「自動公衆送信」とされるようにすることを「送信可能化」と定義して、著作権者だけでなく、実演家やレコード製作者も、勝手に「送信可能化」されない権利、すなわち「送信可能化権」を有するものと規定。

他人のコンテンツのサーバーへのアップロード

- WWW上のサーバーにアップロードする行為は有線送信か？
  - 「有線送信」を行っているのかどうかについては疑義があり、こうしたパソコンの端末からアクセスできる状態にする行為自体は、いまだ有線送信を行っているものではなく、ユーザーの求めに応じてこれが送信された段階で、初めて有線送信が行われたと認めることができるという見解も有力に主張されていた。
- 「送信可能化権」
  - 改正著作権法は、著作者に公衆送信権を与え、この中で、自動公衆送信が行われる場合には、送信可能化権を含むとした（同法23条1項）。
  - 「送信可能化権」とは、たとえば、WWW上のサーバーにアップロードして、パソコンの端末からアクセスできる状態にすることができる権利ということである（同法2条1項9の5号）。
  - したがって、著作者の許諾を得ないでアップロードした場合は、現実のアクセスがない場合でも、著作者の「送信可能化権」の侵害となる。

オープンソースとフリーソフト

- ソフトウェアのソースコードを公開したり，再配布を認めて利用を促進する活動.
- オープンソースやフリーソフトなら何をしてもよいという訳ではない.
- 利用のためのライセンス契約をよく理解しなければならない.
- 複数のオープンスースソフトの組合せはライセンス契約上相互に矛盾することがある.

特許権

- 特許法が保護するもの
  - 特許法第1条「この法律は、発明の保護及び利用を図ることにより、発明を奨励し、もって産業の発達に寄与することを目的とする。」
  - 発明とは「自然法則を利用した技術的思想の創作のうち高度のもの」（特許法第2条）
    - 自然法則：自然界において経験的に見い出される法則。
    - たとえば暗号の作成方法やデパートのショーケース内の商品の陳列方法、ゲームのルール等のように人為的な取り決めは自然法則ではない。
- 新規性と進歩性（要件）
  - 新規性
    - 特許庁に出願する前に一般に知られてしまった発明は特許にはならない（特許法第29条第1項：新規性の要件）。
    - たとえば他社で既に製品化されている場合、他人（または自分）の発明として特許公報に掲載された技術、自分で発明品を展示会で見せてしまったり、新聞発表してしまったりしたものは、一般に知られてしまった発明。
  - 進歩性
    - 今まで知られていない発明であっても、その技術に精通した人間ならば誰でも容易に考えられるような発明（たとえば今までにある技術を単に寄せ集めたようなもの）は特許にはならない（特許法第29条第2項：進歩性の要件）。

ソフトウエア関連特許

- ソフトウエアは特許されるか？
  - プログラム等のソフトウエアは、本来的には人為的な取り決めにしたがって記述された表現物であり、著作権の対象にはなるが、プログラムそのものは特許にはならない。
  - しかし、ソフトウエアもハードウエアと一体になって一定の機能を実現できる場合には発明として特許の対象になる（特許庁、平成5年6月にソフトウエア関連発明の章を設けた新しい審査基準を発表）
    - 「ワープロ学習機能」は特許。審査基準では「ハードウエア資源を論理的に組み合わせた構成であり、自然法則を利用した発明」に該当すると判断。
- ネットワークの通信プロトコルや圧縮アルゴリズムは？
  - 通信プロトコルは通信を行う際の決め事であり、特許や著作権の保護の対象にならない。
  - しかし、特定のコマンドを受領してこのコマンドに対する応答コマンドを送出するというような動作がモデム等のハードウエアやシステムと一体になっている場合、その認識の仕方や送出方法に特別な工夫があればハードウエア資源を利用した発明として特許を受けられる場合がある。またエラーチェック等のように信号系に生じるエラーの物理的性質を利用している場合には発明として成立する（「水平・垂直パリティチェック」の例）

ソフトウエア関連特許

- アルゴリズムは？
  - アルゴリズムそのものは、著作権の対象にはならないのと同様に特許の対象にもならない。
    - しかし、圧縮アルゴリズムに関しては、その圧縮手順がROM等で機能実現手段毎に再構成されて特許出願された場合、データ圧縮装置等という名称で特許される可能性は十分にある。
    - カーマーカー特許(登録番号：特許第2033073号 ）
      線形計画法モデル。この発明を特許とすべきか否か、つまり発明として認めるか否かについては賛否両論った。この事件は審査・審判を経て出願公告、異議申し立てされた後、登録され、その後、再度、無効審判等で争われた結果、平12.12.26に権利が消滅した。
- ソフト特許のまとめ

  ーゲーム方法などの単なる決めごとを実現したアルゴリズムは、特許されないが、技術的効果を奏するアルゴリズム（通信プロトコル、圧縮プロトコルを含む）は特許になり得る。

ビジネスモデル特許

- ビジネスモデル特許とは
  - 情報システムを使って実現したビジネスの仕組みについて与えられる特許
- 米国のビジネスモデル特許
  - 特許第5794207号（プライスライン社の逆オークション）（www.priceline.com、1998年8月11日　特許）
    - コンピュータ・ネットワークを利用して、「①買い手がクレジットカード番号（又は金融機関の口座番号）を特定した上で、希望する商品の購入条件を仲介者（プライスライン）に送信する。②仲介者はこの購入条件を複数の売り手に伝達する。③売り手各社は前記購入条件に基づき見積もりを仲介者に提示する。④仲介者は売り手各社の見積もりを対比して、買い手の希望条件に合致する商品を選択し、その内容を買い手に連絡する。」
    - 本件は、「逆オークション」というビジネスの方法自体新規であるとは言い難いが、インターネットに応用することで特許となってしまう点で、ビジネスモデル特許の進歩性についての問題を提起

ビジネスモデル特許

- 米国のビジネスモデル特許
  - 特許第5960411号（アマゾン．コムのワン・クリック）（www.amazon.com、1999年9月28日　特許）
    - 顧客がWWWサイトで買い物をする際に、顧客名、クレジットカード番号及び送付先住所等を1度入力しておけば、２回目以降の買い物にはこれらの情報を入力しなくてもすむようにする技術。
    - インターネット上のショッピングの方法について、比較的簡単なアイディアではあるが、重要な基本特許ともいえるものについて特許がされたといえる。
- 日本のビジネスモデル特許
  - 広告情報の供給方法およびその登録方法（凸版印刷（株）特許2756483号(1998年3月13日)）
    - コンピュータシステム（例えば、インターネット）により広告情報の供給を行う。広告依頼者には、広告情報（例えば、店名、住所、電話番号、最寄り駅、業種、広告メッセージ）を入力させるとともに、依頼者の店を地図上で特定させる。広告を見るユーザは、地図上に表示された広告依頼者の店を選択することにより、その店における上記広告情報を読むことができる。この広告方法により、広告記載依頼から実際の広告頒布までのタイムラグをできるだけ短くできる等の効果を得ることができる。