情報セキュリティ大学院大学
『情報社会の倫理と哲学を考える』シンポジウム
2006年6月14日 後日配布版

技術と倫理
情報ネットワーク技術・社会における倫理とは?

独立行政法人産業技術総合研究所
情報セキュリティ研究センター
高木 浩光
http://staff.aist.go.jp/takagi.hiromitsu/

私の背景

- 1994年 名古屋工業大学大学院工学研究科 博士後期課程修了（電気情報工学専攻）
- 1999年まで 並列分散処理の研究 →「倫理」とは無縁の日々
- 2000年 ソフトウェアのセキュリティ欠陥への企業の対応について感心を持ち行動（Windows, Apple の Java VM 等）
- 2001年～現在 Webサイトのセキュリティ欠陥の問題の解決への取り組み
- 2003年 RFIDタグのプライバシー上の問題について
- 2004年 Winnyの何が問題なのかについて
- 2005年 不正アクセス禁止法の解釈について

2000年の経験

- WindowsのJava VMにセキュリティホールを発見（公開メーリングリストでの議論の過程で発覚）
  - マイクロソフト社に電話
- Apple ComputerのJava VMに同様の問題発見
  - 米Apple Computer社にメール
- 関係各社に電話
  - Netscapeの脆弱性 → Sunに電話、Acrobat Readerの脆弱性 → Adobe社に電話、Windowsの脆弱性 → ソニーに電話など
- インタラクティブエッセイ「Javaセキュリティ・ホールにみる企業責任」, 情報処理学会誌「情報処理」, Vol.41, No.8
  - 各社のJava VMにずさんなセキュリティ・ホールが発覚
  - ソフトウェアにバグは付き物ではあるが...
  - ベンダは本気でユーザに知らせるつもりがあるのか?
  - パソコンメーカは他人事のふり
  - パソコン雑誌の責任は?

情報処理学会倫理綱領

- 1996年5月施行（倫理綱領調査委員会委員長:名和小太郎先生）
- 当時私が思ったこと:「自分には関係ない」

我々情報処理学会会員は，情報処理技術が国境を越えて社会に対して強くかつ広い影響力を持つことを認識し，情報処理技術が社会に貢献し公益に寄与することを願い，情報処理技術の研究，開発および利用にあたっては，適用される法令とともに，次の行動規範を遵守する．
1. 社会人として
1. 1 他者の生命，安全，財産を侵害しない．
1. 2 他者の人格とプライバシーを尊重する．
1. 3 他者の知的財産権と知的成果を尊重する．
1. 4 情報システムや通信ネットワークの運用規則を遵守する．
1. 5 社会における文化の多様性に配慮する．
2. 専門家として
2. 1 たえず専門能力の向上に努め，業務においては最善を尽くす．
2. 2 事実やデータを尊重する．
2. 3 情報処理技術がもたらす社会やユーザへの影響とリスクについて配慮する．
2. 4 依頼者との契約や合意を尊重し，依頼者の秘匿情報を守る．
3. 組織責任者として
3. 1 情報システムの開発と運用によって影響を受けるすべての人々の要求に応じ，その尊厳を損なわないように配慮する．
3. 2 情報システムの相互接続について，管理方針の異なる情報システムの存在することを認め，その接続がいかなる人々の人格をも侵害しないように配慮する．
3. 3 情報システムの開発と運用について，資源の正当かつ適切な利用のための規則を作成し，その実施に責任を持つ．
3. 4 情報処理技術の原則，制約，リスクについて，自己が属する組織の構成員が学ぶ機会を設ける．

- 日本原理力学会倫理規定との比較
  - **「行動の手引」より**
    - 原子力利用の基本方針、平和利用への限定、核拡散への注意、諸課題解決への努力、
      安全確保の努力、安全知識・技術の習得、効率優先への戒め、経済性優先への戒め、安全性向上の努力、慎重さの要求、技術成熟の過信への戒め、安心できる社会の構築、会員の安心への戒め、
      専門能力、新知識の取得、経験からの学習と技術の継承、関係者の専門能力向上、正確な知識の獲得と伝達、能力向上のための環境整備、
      自己能力の把握、所属組織の災害防止、他の組織による監査、公的資格に関する法令遵守、公的資格の尊重、
      正確な情報の取得と確認、情報の公開、守秘義務と情報公開、非公開情報の取り扱い、説明責任、社会との調和、組織の文化、
      科学的事実の尊重、科学的事実の普及、自らの判断、
      誠実な行動、報酬等の正当性、組織の私的利用、利害関係の相反の回避、ルール遵守と形骸化の防止、契約に関する注意、
      指導者の規範、専門分野等の研鑽と協調、社会からの付託

2001年の経験

- Webサイトの脆弱性を発見
  http://securit.gtrc.aist.go.jp/
  - Cookieを使用せずURLに埋め込むIDに頼ったセッション管理方式の脆弱性
  - クロスサイトスクリプティング脆弱性
  - 秘密情報を含まないCOOKIEに頼ったアクセス制御方式の脆弱性
- どのようにして脆弱性存在の事実を確認するか
  - 法による保護(不正アクセス禁止)との衝突
  - 不正アクセス行為(不正アクセス禁止法第3条)を伴わないで確認する方法
- どのようにしてサイト運営者に修正を促すか
  - 直接の連絡? 事実の公表は? 他のサイトは?
- マスコミによる正しい報道の重要性

脆弱性届出制度 経緯

- 2003年1月 情報処理振興事業協会 IPA Winter 基調講演
  「ソフトウェアのセキュリティ欠陥は誰が直すのか」
- 2003年5月～ 経済産業省商務情報政策局長諮問研究会
  「情報セキュリティ総合戦略策定研究会」
- 2003年10月 経済産業省「情報セキュリティ総合戦略」
- 2003年10月～ 情報処理振興事業協会
  「情報システム等の脆弱性情報の取扱いに関する研究会」
- 2003年4月 同研究会報告書
  「脆弱性関連情報流通の枠組み構築に係る提言」
- 2003年4月 経済産業省 パブリックコメント
  「『……取扱基準(案)』等に対する意見の募集」
- 2003年7月 平成16年経済産業省告示 第235号
  「ソフトウエア等脆弱性関連情報取扱基準」
- 2003年7月 IPA, JPCERT/CC, JEITA, JPSA, JISA, JNSA
  「情報セキュリティ早期警戒パートナーシップガイドライン」
- 2003年7月 届出受付開始

期待したこと

- 公的機関による発見者とベンダー/運営者との仲介
  - 匿名掲示板等による暴露の回避
  - 見て見ぬふりしないですむように
  - ベンダー/運営者の責任ある修正対応
  - 実態の解明
- ベンダーによる告知方法の標準化
  (製品の脆弱性の場合)
- 発見者による公表方法の標準化
  (製品の脆弱性の場合)

情報システム等の脆弱性情報の取扱いに関する研究会

- 主な論点（個人的に簡単でないと感じた論点）
  - Webサイトの脆弱性の届出を受け付けられるのか
    - 違法な手段による発見を奨励することはできない
    - 適法/違法の明確な線引きは無理ではないか
    - 適法であっても勝手に調べまわられることを嫌う向きもある
  - 発見者の対応への要請と表現の自由との関係
    - 取り扱いが終わるまで公表しない、脆弱性の詳細情報を公表しないように求めるべきであるとする意見も
    - 技術的進歩のために、詳細情報（具体的な脆弱性再現方法）の公表が必要である場合もあり、一律に制限するべきでない
    - そもそも公的機関が発見者の表現行為を妨げることはできない

Webサイトの脆弱性

- 不正アクセス禁止法との関係
  - 「脆弱性の発見＝侵入＝不正アクセス ではないのか?」
    - 技術の実際をご存じない方によくあると思われる誤解
  - 明らかに不正アクセス禁止法違反にあたらない脆弱性発見がある
  - 不正アクセスなしに発見できるのは、一部の種類の脆弱性に限られる
    - 届出制度ですべての脆弱性を解決できるわけではない
    - どのくらいの範囲がカバーできているのか?
  - 脆弱であると確証を得るまでの確認行為は実施せずに、疑わしい段階での届出
    - 「寸止め」
    - 推定の確度が高いものから低いものまである
    - 届出機関が、当該サイト運営者と協議の上、事実確認をする

「抵触しないと推察される行為の例」

- 「情報セキュリティ早期警戒パートナーシップガイドライン」p.21
  （2）不正アクセス禁止法に抵触しないと推察される行為の例
  - 1）ウェブアプリケーションの利用権者が、正規の手順でログインするなどして通常のアクセスをした際に、ブラウザとサーバとの通信の内容を観察したところ、それだけで脆弱性の存在を推定できた場合。
  - 2）ウェブページのデータ入力欄にHTML のタグを含む文字列を入力したところ、入力した文字列がそのまま表示された。この段階ではアクセス制御機能の制限を回避するに至らなかったが、悪意ある者に別の文字列を入力されれば、このサイトにセキュリティ上の問題が引き起こされかねないと予想できた場合。
  - 3）アクセス制御による制限を免れる目的ではなく、通常の自由なページ閲覧を目的として、日付やページ番号等を表すと推察されるURL中の数字列を、別の数字に差し替えてアクセスしてみたところ、社会通念上、本来は利用できてはならないはずと推定される結果が、偶発的に起きてしまった場合。（ただし、積極的に多数の数字列を変えて試す行為等は、制限を免れる目的とみなされる可能性があります。）

2002年の経験

- 「ファイル丸見え」型個人情報漏洩事件の多発
  - 丸見えファイルのURLが、2ちゃんねる掲示板で暴露される
  - サイト運営者は「不正アクセスされた」と主張
  - 不正アクセス禁止法の解釈 → 警視庁の見解が出る
  - 適切な報道の繰り返しにより、啓発が成功した事例

- GPKI（政府認証基盤）のルート証明書配布問題
  - 電子申請システムが稼動開始
  - SSL暗号化通信に必要なサーバ証明書の署名者が、Webブラウザに登録済みでない認証局
    - Man-in-the-middle攻撃の恐れ
  - 不適切なルート証明書配布方法を国民に指示

「ファイル丸見え」型漏洩

- 2002年に報道された事故
  - 大阪読売テレビ、小学館、高千穂交易、中央証券、TBC、YKKアーキテクチュラルプロダクツ、全日空ワールド、日本テレビエンタープライズ、日本大学通信大学院、三菱ガス化学、TVQ九州放送、砂糖を科学する会、山芳製菓、三井物産ハウステクノ、ブロックライン、アビバ、諏訪市役所、東日本ハウス、カバヤ食品、ブルドックソース、金印わさび、学習舎、名古屋国税局、東京経済大学、モバイルインターネットサービス他
- 多くは当初「ハッカーの仕業」と発表（本当か?）
  - 読売新聞6月30日
    同社によると、このデータは、HP上で暗証番号を入力しなければアクセスできないようになっていたが、何者かがHPを管理している別会社のサーバーを通じて、暗証番号がなくてもアクセスができるようプログラムを書き換えたらしい。
  - NHKニュース7月1日:
    これらの個人情報は会社のホームページのサーバに保管され、閲覧するためには暗証番号の入力が必要で、会社では不正なアクセスによってプログラムが書き換えられたものとみてホームページを閉鎖して原因を調べています。

警視庁「道端に置くのと同じ」

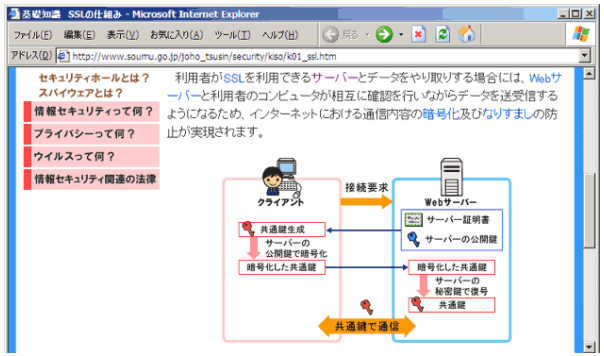
- 中日新聞 2002年7月4日 相次ぐ個人情報流出 "お寒い"企業の危機管理 警視庁 『道に置くのと同じ』
  より引用
  - (略)*ハッカー被害との見方も出たが、背景を探ると多くは「サーバーの設定ミス」(専門家)などで、知識や注意不足が原因。情報技術(IT)社会のお寒い情報セキュリティー事情が浮かび上がる。*
    (略)
    道端に名簿を置いていたのと同じー。原哲也警視庁ハイテク犯罪対策総合センター所長の説明は明快だ。一連の流出情報はサーバーの公開部分に置かれ、誰でも見られた。最低限の防御もしていないケースが多く、企業の相談で「法的に不正アクセスと判断できるものはない」という。

ルート証明書配布問題

- 「GPKIおよびLGPKIにおけるルート証明書配布方式の脆弱性と解決策」 http://staff.aist.go.jp/takagi.hiromitsu/#2002.11.1
  情報処理学会コンピュータセキュリティ研究会, コンピュータセキュリティシンポジウム2002
  - 本論文は，これらの現在稼動中のGPKIおよびLGPKIについて，ルート証明書の配布手段が安全でないとする根拠を示し，このことが電子政府のみならず民間の電子商取引の安全性をも脅かすものであることを示す．また，代替手法について検討し，これが政策的な問題となる以前に技術的問題である（政策的な制約を満たしたまま技術的に解決可能である）ことを示す．
- 総務省のシステムはそれなりに改善された
  - フィンガープリントのFAXによる提供
- 論文で名指しされた東京都は、対応せず
- 多数の地方公共団体が新たに問題あるシステムを公開した

証明書の機能に対する誤解

- 総務省の解説に見られる典型的な誤解パターン
  - 「国民のための情報セキュリティサイト 用語辞典」（総務省）より
    - ■サーバー証明書（サーバー・しょうめいしょ）
      Webサーバーに対して発行される電子証明書のこと。
      Webページの発行元のサーバーを運用しているWebサイトが**実在していることを証明するもの**です。通常は、Webサイトを運営している団体が、信頼できる第三者機関に申請することで発行されます。この証明書には、**暗号化に用いる公開鍵が格納されていて、この鍵を使うことによりクライアントと安全に通信できるようになります**。



その後

- 2005年 地方公共団体が同じことを繰り返した
  - さらにひどいことに、「警告が出ますが問題ありません」という誤った使い方を市民に指示
- 特に酷かった高知県と埼玉県に電話
  - blogでやりとりを公開 → 大きな反響 → 理解は進む → いくらか解決の方向へ
- 民間までもが「警告が出ますが問題ありません」と
  - 「オレオレ証明書」という俗称が誕生 → 効果大
- 他に解決方法はないのか?

RFIDのプライバシー問題

- 2003年4月22日 NIKKEI NET, ネット時評, 特集・電子タグ, 固定IDは"デジタル化された顔"——プライバシー問題の勘所
- 日経産業新聞 12月5日21面, 新産業創生 生活が変わる ITが変える, プライバシー保護 難題 ID技術、安さと両立に時間
- 2003年12月10日 本とコンピュータ, 2003 冬号, 対論「工学化」する書物と社会をめぐって 東浩紀×高木浩光
- 2004年3月20日 よみうりテレビ, ウェークアップ！, SF世界を実現!? 究極のコンピュータ社会
- 2004年10月9日 よみうりテレビ, ウェークアップ！, 時代の天秤, 子供の安全を守る発信機
- 朝日新聞2004年10月20日朝刊第3社会面,
  ICタグ発 ランドセルで「管理」 小学校の登下校 安全求め各地で試行 悪用の危 険性指摘も

RFIDタグの2つの問題

- セキュリティ問題
  - タグに対するなりすまし攻撃の危険性
  - 結論: RFIDタグを認証に使ってはならない
- プライバシー問題
  - タグがプライバシー侵害のインフラとなる危険性
  - 結論: 解決は困難、軽減は可能
- 解決策
  - セキュリティやプライバシーのための標準を設けてタグの性能・性質を表示する

プライバシーの問題: 懸念要因の区別

- 以下は分けて議論する必要がある
  - システム欠陥が原因で守られるべきプライバシー情報が事故で漏えいしたり、故意に盗み出されたりする
  - 内通者が情報を外部に持ち出したり、従業員のミスで漏えいさせる
  - 事業者が情報を外部に提供する予定がある場合に、それを消費者が承知しているかの問題
  - 事業者を信頼してよいかの判断が、普通の消費者にはたして可能なのか
  - 消費者に事業者の選択の余地がなくなる懸念
  - 共通(固有)ID方式という識別アーキテクチャの問題

2種類の懸念

(a) 属性データの内容を読まれる
- よく理解されている
- 技術的対策が可能
  - 暗号を用いたアクセス制御機能をRFIDに持たせる
    - 低コストタグでは非現実的
  - リーダライタ側で暗号化したデータを書き込む
    - 無権限で書き換えられることのなようアクセス制御が必要なため、超低コストタグでは非現実的
  - RFIDには固有IDだけを持たせ、属性データはネットワーク経由でセンターに保存したデータベースを検索して読み書きする

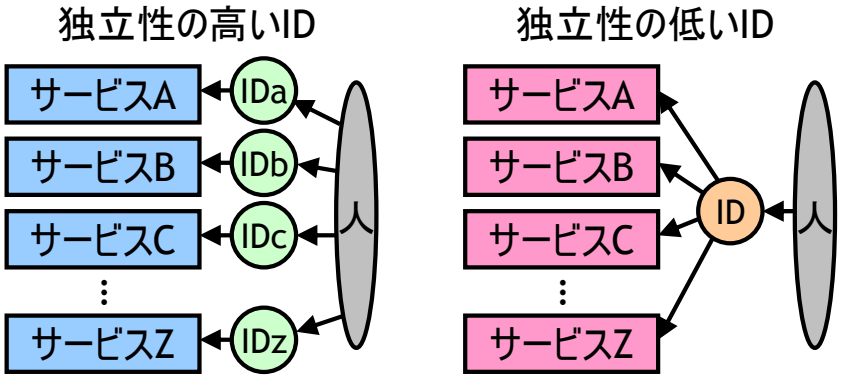
(b) IDでトラッキングされる（識別アーキテクチャの問題）
- あまり理解されていない
- 技術的対策は可能だが、低コストタグでは非現実的

重要なのはトラッキングの懸念

- よくある誤った主張
  - 「IDはただの番号であってプライバシーの問題はない」「センターのデータベースは、厳重にアクセス制限するので悪用されることはない」
  - この主張の欠陥
    - (a)の問題についてしか言及していない
    - (b)の問題は解決しない
- 国際的に、RFIDタグのプライバシー問題として認識されているのは、(b)のトラッキングの懸念
  - (a)も含むが

IDの有効ドメイン範囲

- ID空間のサービス独立性
  - 独立性の低いID（共通ID）は、匿名前提で蓄積された属性情報を、匿名でなくする危険性を高める



IDと個人情報保護法

- 個人情報保護法における個人情報の定義
  - 住所氏名を含まないIDは（直ちに）「個人情報」ではない
    - この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。
- IDにひも付けされたあらゆる情報（私事性のある情報を含む）の記録、蓄積、売買は合法?
  - 住所氏名さえ含まなければ
  - IDが共通IDであっても
  - IDが「他の情報と容易に照合することができ」ないなら
    - 「容易に」とは?

共通ID問題の解決困難性の根源

- 「問題ない」とする人は2枚の舌を使う
  - 〇〇IDは個人情報ではないと主張
    - 「〇〇IDだけでは個人情報が流出することはありません」
  - 〇〇IDが個人情報であることを前提とした主張
    - 名簿屋がIDを売買するといった脅威は法律で禁止すればよい
- 問題ないという意識の人によって問題が作られる
  - 問題のない情報だからとぞんざいに扱う（蓄積される）
  - 蓄積されたことによって、問題のある利用が可能になる
- 「共通IDは個人情報である」という共通認識を作る以外解決しないように思えるが…しかし
  - 「〇〇IDだけでは個人情報が流出することはありません」と、消費者には説明される

総務省・経済産業省のガイドライン

- 電子タグに関するプライバシー保護ガイドライン
  http://www.meti.go.jp/policy/consumer/press/0005294/
  - 第３（電子タグが装着されていることの表示等）
    消費者に物品が手交された後も当該物品に電子タグを装着しておく場合には、事業者は、消費者に対して、当該物品に電子タグが装着されている事実、装着箇所、その性質及び当該電子タグに記録されている情報（以下「電子タグ情報」という。）についてあらかじめ説明し、若しくは掲示し、又は電子タグ情報の内容を消費者が認識できるよう、当該物品又はその包装上に表示を行う必要がある。当該説明又は掲示は、店舗において行うなど消費者が認識できるように努める必要がある。
  - 第４（電子タグの読み取りに関する消費者の最終的な選択権の留保）
    事業者は、消費者に物品が手交された後も当該物品に電子タグを装着しておく場合において、消費者が、当該電子タグの性質を理解した上で、当該電子タグの読み取りをできないようにすることを望むときは、消費者の選択により当該電子タグの読み取りができないようにすることを可能にするため、その方法についてあらかじめ説明し、若しくは掲示し、又は当該物品若しくはその包装の上に当該方法について表示を行う必要がある。

  - 第５（電子タグの社会的利益等に関する情報提供）
    事業者は、第4に基づき消費者が電子タグの読み取りをできないようにした場合であって、物品のリサイクルに必要な情報が失われることにより環境保全上の問題が生じ、又は自動車の修理履歴の情報が失われることにより安全への影響が生じる等、消費者利益又は社会的利益が損なわれる場合には、これらの利益が損なわれることについて表示その他の方法により消費者に対して情報を提供するよう努める必要がある。
  - 第１０（消費者に対する説明及び情報提供）
    事業者、事業者団体及び政府機関等の関係機関は、電子タグの利用目的、性質、そのメリット・デメリット等に関して、消費者が正しい知識を持ち、自ら電子タグの取扱いについて意思決定ができるよう、情報提供を行う等、消費者の電子タグに対する理解を助けるよう努める必要がある。

- SCMに限定しない用途が想定されている

技術的解決の困難性

- 技術的対策にはハードウェアコストがかかる
  - 「あらゆる物にIDチップを」を実現するには、1個数円程度である必要がある
    - 低価格化の実現性が見えてきたから急速に注目を浴び始めた
  - ハードウェアの大規模化は消費電力を増す
    - 通信可能距離が短くなる
- 低コストタグにおける簡略化セキュリティ機構の研究が始まっている

ガイドラインの問題点

- タグの存在表示の義務付けでは問題は解決しない
  - 消費者は、すべてのタイプのタグついて一律に、無効化する/しないの二者択一の選択を迫られる
    - 商品やタグの種類によって、無効化と非無効化を選び分けることができない
    - 選択のために必要な情報が提供されないため
  - 消費者は感情的にしか判断しなくなる
    - 「気にする」者と「気にしない」者という2つのグループに分かれ、どちらを選択するかが感情的に判断される
    - 事業者は、タグのリスクを消費者に説明することを控えたくなる
- プライバシー保護技術の開発が促進されない
  - 消費者に理解されなければ競争が生まれない

ガイドライン案に対する意見

- 2004.6.22 パブリックコメント提出意見,
  電子タグに関するプライバシー保護ガイドライン（案）」に対する意見
  - (1) 電子タグ装着の事実の表示について、「あらかじめ説明若しくは掲示」又は「当該物品若しくはその包装上に表示」が必要としているが、前者について、説明や掲示の手段を明確にするべきである
  - (2) 表示すべきこととして、タグ装着の事実のほかに、「その性質及び当該電子タグに記録されている情報の内容」も含められているが、「性質」や「内容」として何を示す必要があるのかを規定すべきである。
  - (3) 電子タグが物品のどの位置に装着されているかを表示する必要があるとすべきである。
  - (4) 電子タグの読み取り機を設置する際には、読み取り機の存在を表示する必要があるとすべきである。
  - (5) 個人情報を含まないデータベースと連携する場合にも、個人情報保護法に準ずる取扱いが必要であるとするべきである。
  - (6) 電子タグを個人認証に使うには、当該タグが一定水準のセキュリティ機能を搭載していなくてはならないと規定すべきである。

技術者のたしなみ

- 固定ID方式は避けるべきもの とされているという認識
- 日本はこの議論に取り残されてきた
  - いくつかの国では早い時期から国民番号（Social Security Numberなど）を経験し、グローバルユニークIDの問題点を理解している
  - 過去の同様の議論で日本はいつも蚊帳の外だった
    - Intel Pentium IIIのPSN (Processor Serial Number)問題
    - Windows Media Playerのユーザ識別ID
    - IPv6 MACアドレス問題
    - Microsoft Passport vs Liberty Alliance

「ICタグで子どもの安全を」？

- アクティブ型RFIDタグをランドセルに取り付けて……

NHK総合，ニュース10，2004年9月27日22時55分ごろより

別の番組では…

読売テレビ「ウェークアップ！」
2004年10月9日午前9時2分8秒より引用

Winny問題

- 日経デジタルコアでの 2003年2月の発言
  http://www.nikkei.co.jp/digitalcore/online/contents/content005.html#c043
  - マイナーなものは極めて見つかりにくいということですね。しかしその種のものは、1か月かかってでも見つかればいいものかもしれません。また、その種のものは、著作権ビジネス的にはあまり脅威の対象ではないように思えます。**むしろ、名誉毀損やプライバシー侵害にあたるような映像の拡散を止められないといった観点からの懸念があるように思います。**
- 日経産業新聞 2004年5月27日ビジネス総合・国際・IT面,
  ウィニー事件の波紋(3) 慶応大教授の村井純氏と産業技術総合研究所の高木浩光氏に聞く
- 朝日新聞 2006年4月19日朝刊オピニオン面,
  ウィニー問題の本質は「ソフト自体が危険すぎる」
- 朝日新聞社, 論座 2006年5月号,
  ウィニー騒動の本質 あまりにも情報流出のリスクが大きい

「市民の安全を深刻に害し得る装置としてのWinny」(*1)

- 「積極的に他人のプライバシーを侵害する目的で、そのような自作のコンテンツを放流するという行為がなされる可能性」
  - 業務用コンピュータでWinnyを使用したうえ不注意でトロイの木馬を実行したことで機密情報を流出させる昨今の事例とは別に
  - それが起きたということは現時点でもまだ確認されていないが、表沙汰になっていないだけかもしれない
- これは以下のような主張を否定したもの
  「現在の著作権概念は時代の産物でしかなく、技術革命により過去のものとなるのだから、Winnyに有害性は何もない」
  - 仮に「……過去のものとなる」が真であるとしても
- 削除機能のない強力な「放流」システム一般に、この懸念がある（管理不能性）

*1 http://d.hatena.ne.jp/HiromitsuTakagi/20040516#p1

強力な「放流」機能

- 従来の人手を介した流出、流通とは圧倒的に異なる強力さ
- 「良心に蓋をさせ、邪な心を解き放つ —— ファイル放流システム」(*2)
  - 流通の仕組みが受け取る行為と切り離せない構造になっている。受け取る行為によってファイルが拡散するのであり、各ユーザの受け取る行為のひとつひとつが流通の仕組みを支えている。しかし、ユーザはそのことを認識していない。「自分は単に受け取っているだけだ」と勘違いしている。一部の専門的ユーザは認識しているだろうが、大半は理解していない。あるいは、理解することを避けながら使っているだろう。
- これを「P2P」の最大の特性と捉えると……
  - 「P2P」の定義は様々あるが
  - Person to Person と捉えられる（ノードの管理主体が個人）

*2 http://d.hatena.ne.jp/HiromitsuTakagi/20040608#p1

「P2P」技術って何?

- 朝日新聞2004年9月12日朝刊1面の奇妙な記事
  - 無料のIP電話、日本で25万人利用 「ウィニー」と同じ技術転用
    ファイル交換ソフトを転用した無料のIP(インターネット・プロトコル)電話の利用者が、日本でも広がり始めている。「スカイプ」と呼ばれるソフト(略)
    スカイプはそれを電話に応用したもので、KaZaA同様、P2Pという技術を使う。(略)
    【P2P(ピア・ツー・ピア)】 インターネット上で、サーバーを介さずに情報を端末同士で交換する技術。著作権法違反幇助(ほうじょ)の罪で起訴された音楽ファイル交換ソフト「ウィニー」の作者も、この技術を利用していた。

不正アクセス禁止法の解釈

- 「ACCS不正アクセス事件」
  - 東京地裁平16特(わ)752号, 平成17年3月25日刑事10部判決, 判例時報 No.1899 pp.155-161
  - 2003年11月発生
  - 2004年1月朝日新聞報道
  - 2004年2月逮捕、起訴
  - 2005年3月一審判決(確定)
- 不正アクセス禁止法の解釈をめぐって様々な議論をよぶ
  - 不正アクセス行為の定義の曖昧さ
  - 曖昧な領域のど真ん中に位置する行為が行われた
  - 目的は脆弱性の指摘(当時は脆弱性届出制度はなかった)
  - 結果として個人情報の流出を引き起こした
- 「不正アクセス行為の2つの文理解釈について」, 情報ネットワーク法学会, 情報ネットワーク・ローレビュー 第5巻1号

論文の主張

- アクセス制御機能の有無は重要でない
- あるアクセスがあるアクセス制御機能による制限にかかっていたと言えるかは、客観的に判断できない
- 「利用」に二つの解釈が可能
- (A)の解釈
  - 矛盾は生じない
  - 技術的不都合はさほど生じない
  - 「し得る状態にさせる」に必然性がある
- (B)の解釈
  - 矛盾が生ずる、もしくは客観性が失われる
  - 無理に客観性を得ようとすると、技術的不都合が生ずる
  - 「し得る状態にさせる」が不必要

ACCS事件と2002年事件

- ACCS事件判決
  - 「当該顧客の**公開領域へのアクセスは**、当該顧客の承諾(同法3条2項各号)があるか、**当該特定利用を誰にでも認めていることにより**アクセス制御機能による制限のない特定利用であるから(略)、この点で不都合が生じることはない」
- 2002年の一連の事件
  - 管理者はそのようなアクセスを承諾していなかった(推察)
  - 管理者の主観ではアクセス制御機能(FTPアカウント)により制限されていると理解されていた(推察)
- 何らかの条件が存在するはず
  - 2002年の事件が不正アクセス行為にあたらないと判断される
  - 管理者の主観によらない条件

制限されたアクセスか

- ACCS事件判決
  - 否定する(該当しないとする)理由のひとつを否定する根拠
    - 「アクセス制御機能及びこの**『制限』が完全無欠であれば**、識別符号等以外の情報又は指令が入力されてもおよそ特定利用はできず、『制限』された状態が維持され、同法**3条2項2号に掲げる行為は不可能となるから**、同号に定めた行為を処罰する規定を置く意味はないことになる」「**プログラムの瑕疵や設定上の不備があるため**、識別符号を入力する以外の方法によってもこれを入力したときと**同じ特定利用ができることをもって、直ちに**識別符号の入力により特定利用の制限を解除する機能が**アクセス制御機能に該当しなくなるわけではない**と解すべきである。」
  - 肯定する(該当するとする)根拠
    - 「本件の各特定利用ができたのは、**プログラムないし設定上の瑕疵があったためにすぎないのであり**、アクセス管理者が本件アクセス行為のような形で特定利用をすることを**誰にでも認めていたとはいえない**。よって、本件においても、本件CGI及び本件ログファイルの各閲覧は、アクセス制御機能による特定利用の制限にかかっていたものということができる。」
- 2002年の事件も設定上の瑕疵が原因 ⇒ 警視庁判断と矛盾

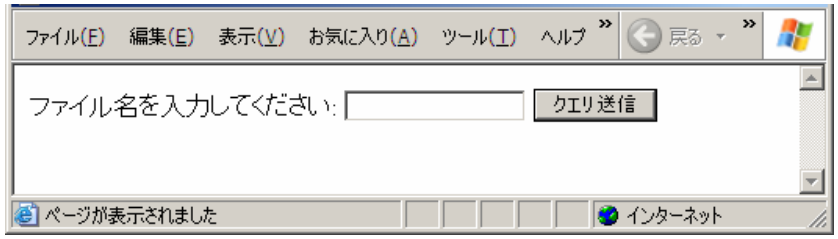
GET=合法 では困る技術的理由

- セッションIDをURLに載せるWebサイトは一般的
  http://example.com/foo.cgi?**sessionid=c62ae61b35b70c8c**
- ログインごとに変化する予測困難な乱数値(受付番号)
- セッションIDを用いたWebアプリケーションの構成は最も一般的な技法
- 有効なセッションIDの値を盗んで
  - パケット傍受や閲覧者側コンピュータへの攻撃により
- セッションハイジャック攻撃
  - 盗んだセッションIDでサーバにアクセス(ログイン状態の乗っ取り)
- 攻撃が可能となる原因
  - **サーバ側にプログラムや設定上の瑕疵があるわけではない**
  - **「拙劣な」アクセス制御方式というわけでもない**
- 「GET=合法」では、セッションハイジャック攻撃を不正アクセスとできない

GET=通常, POST≠通常 ?

- GETの例

```
<form action="http://example.com/foo.cgi" method="GET">
ファイル名を入力してください: <input name="file">
<input type="submit">
</form>
```



- ボタンを押すと次のようなURLにアクセス
  http://example.com/foo.cgi?**file=/usr/local/data/foo.csv**

「リンクは自由」の文化

- 他人の管理するWebページへ無断でリンクするのは不正な行為か?
- リンクするのは自由
  - リンクという紹介行為の結果として不法行為を構成することはあっても、リンク自体が問題なのではない
- <form action=...> もリンクである
- GETもPOSTもリンクである
- 仮説:「GETは自由だが、POSTは自由でない」?
  - GETの例: Google検索リンクの勝手な設置など
  - POSTでは?
- 「リンク 設置方法 method POST」などでWebサイトを検索
  - 自サイトに対してPOSTアクションによるリンク方法を推奨しているサイトが多数存在
- POSTによるリンク⇒直ちに不適切とされているわけではない
  - ただし、無断POSTリンクを許可する例があるというだけ

「不正指令電磁的記録作成罪」の問題

- 犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案
- 第二編第十九章の次に次の一章を加える。
  - 第十九章の二　不正指令電磁的記録に関する罪
    （不正指令電磁的記録作成等）
    第百六十八条の二
    人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、三年以下の懲役又は五十万円以下の罰金に処する。
    一　人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録
    二　前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録
    2　前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。
    3　前項の罪の未遂は、罰する。
    （不正指令電磁的記録取得等）
    第百六十八条の三　前条第一項の目的で、同項各号に掲げる電磁的記録その他の記録を取得し、又は保管した者は、二年以下の懲役又は三十万円以下の罰金に処する。