情報の送受信における倫理

名古屋大学 情報基盤センター
情報基盤ネットワーク研究部門
嶋田 創

概要

- 情報の送受信における倫理
  - 送(受)信してはいけない情報
  - 送(受)信に注意を要する情報
  - 犯罪行為に巻き込まれない/犯罪者にならないために
- 最近の情報倫理における話題
  - ビッグデータ活用と個人情報/プライバシー保護
  - マイナンバー制度

電子社会上の倫理の怖い所

- まだまだ発展途上な所があってやっかい
  - 迷惑行為と犯罪行為の境界が曖昧
  - 法律の整備が追いつかない
  - 企業とかも解釈を間違えていることが多い(特に個人情報やマイナンバー)
- 複数の国にまたがる問題だと倫理の違いがある
  - 日本の法律が適用されない
- 被害者が加害者になることも多い
  - マルウェアに感染したPCが他を攻撃
  - マルウェアに感染したPCから個人情報が漏洩
- 正義感から事を大げさにする(暇)人が多数いる
  - 全世界に向けて情報を発信していることを意識する

送(受)信してはいけない情報

- spam
- チェーンメール
- コンピュータウィルス(マルウェア)
- 詐欺
- 選挙運動(選挙期間中)
- 荒らし行為
- ストーキング行為
- 不正アクセス、DoS攻撃
- 著作権侵害
- 犯行予告/誹謗/中傷
- 法律違反行為を証明する情報
- ニセ情報
- その他、物議を醸す情報

spam

- 迷惑メール(主に宣伝)
- 株(風説の流布)とか薬(薬事法)とか、別の法律に抵触するものもある
- アカウント乗っ取りされて、ばら撒かれることもあります
- SPAMと書くとHormel社に怒られます
  - SPAMはHormel社の製品(右)
- 受け手に無駄な時間を費やさせ、ネットワーク資源などに負荷をかける
  - 全メールトラフィックの40%～60%がspam
  - 最近は、かなり標的を絞るようになってきた
  - きっちり通報したりすると、ターゲットから外してくれる例も

チェーンメール

- 「できるだけ多くの人に回して下さい」が識別点
- 善意に見えてもダメ
  - というか、むしろ愉快犯は善意を利用する
  - 善意で人を間接的に殺せます
    - 病院の機能を麻痺させたりとか
  - 「良いことを推進する目的ならば、嘘でもOKじゃないか」というアレな人がよく出てきますが、めげないように
- 例:
  - 不幸/幸福のメール
  - AB型かつRh-型の血液が不足
  - 東日本に電力を融通するので節電を

マルウェア(コンピュータウィルス)

- コンピュータに不正な処理を行わせるソフトウェア
  - MALicious softWAREの略
  - かつてはコンピュータウィルスと呼ばれていたが、今はこちらが主流
- 感染源の例
  - メールに添付されたものを実行orメール中のURLからダウンロード
  - (広告に)仕込まれたウェブページ閲覧
  - 仕込まれたExcelのマクロを実行
- 不正な処理の例
  - メールなどを介してコピーをばらまく(ワーム)
  - キー入力/通信/ファイル内容の収集
  - アプリケーション(特にアンチウィルスソフトウェア)の起動妨害
  - コンピュータの遠隔操作(RAT: Remote Administration Tool)
    - TeamViewerとかQQとか正規の遠隔操作ソフトもある

フィッシング(phishing)詐欺

- 主にURL偽装などで偽サイトへの誘導
- 例:
  - 「オンラインバンキングのパスワードを変更して下さい」
  - 「サービス終了に伴い、後継サービスに移って下さい」
- クレジットカード番号、ID/パスワードの奪取が目的
- 対策
  - メール中のURLをクリックするのではなく、当該サービスのトップページから利用
  - 正しいSSL証明書か確認
    (右図)

その他の詐欺

- 偽セキュリティ警告:「おまえのPCはコンピュータウィルスにかかっているからこのソフト買え」
- ファイル人質:「ファイルを返して欲しければ金払え」
  - 最近話題のTeslaCryptやLockyはこいつ
- ワンクリック詐欺: URLをクリックしたら「ご利用ありがとう、金払え」
  - 料金提示と支払の確認が無い

- とりあえず、「金払え(ソフト買え)」が合言葉
- 基本的に相手にしなくてよい
  - そもそも、こんなことをやる人間がまともに商取引を行うとは思えない
  - 心配ならば、メディアセンター職員に相談

選挙運動(選挙期間中)

- 2013/4よりインターネットを利用した選挙運動が解禁されました
- ただし、事前に登録された本人or代理人のみOK
- 違反の申し立てがあった場合、2日以内に対応を取る必要がある
  - 大学側も緊急連絡や遮断の措置を取れる体制を準備
- もちろん、なりすましや誹謗/中傷もダメ

荒らし行為

- 意見のゴリ押しなどによる言論の自由の妨害
  - 短期間に電子掲示板等に多数の意見を書き込むなど
- 時には、誹謗/中傷を伴う
- 例: Wikipediaへの荒らし

無期限の投稿規制中です

このIPアドレスを含む、名古屋大学に割り当てられているIPアドレスから荒らし行為が行われました。対応を依頼したところ、ネットカフェ、漫画喫茶など利用者の確認が不可能な不特定多数が利用する環境である事がわかりました。対応をとって頂く事が事実上不可能であるため、本IPアドレスからの投稿をブロックしております。ご了承ください。対応が可能な制度に変更された、あるいは割り当て先が変更された場合はご連絡ください。

ストーキング行為

- 例
  - しつこくメール等を送る
  - しつこく個人ブログや掲示板に書き込む
  - しつこく個人の行動(ネット上を含む)を追跡する
- ストーキングのためのソフトもあるので注意
  - マルウェアの一種
  - メール送信情報出力、GPS情報出力(スマートフォン)、など
- 物理的なストーキングにつながることもある

  →必要に応じて、大学や警察に相談

不正アクセス、DoS攻撃

- 不正アクセス
  - 自分のものではないID/パスワードでサービス利用
- DoS(Denial of Service)攻撃
  - 大量の通信などによる相手サービスの妨害
    - サーバに接続しにくくなる、サーバのプログラムを停止させる
  - 民族意識の対立から，他国の政府機関に対するDoS攻撃も近年では見られる
  - サーバ側が間抜けな実装であったため、DoS攻撃と勘違いされて逮捕された事例もあるので注意
    - 例: 岡崎市立中央図書館事件

      サーバ側のソフトウェアの実装がアレだったために、1秒あたり1回の検索要求でサーバ側が落ちるというマヌケな事態に

著作権侵害

- 自由な配布が許可されていない著作権物の送受信
  - 例: 動画、音楽、ソフトウェア、など
  - 著作権侵害物と知って受信するのも違法です
  - もちろん、送信はもってのほか
    - 友人などに依頼されても送らないこと
    - オンラインストレージに移動させたものをうっかり公開しないこと
      - というか、今のオンラインストレージは検閲が入っているので、移動させたらオンラインストレージのアカウント停止されることが多い
- 著作権侵害はファイル共有ソフトウェアを利用して行われることが多い

→名大内で動かすと警告が来ます

  - 中国で売られているPCにはXunleiがプレインストールされていることが多いので注意

犯行予告/誹謗/中傷

- 犯行予告: 殺人、放火、爆破、など
- 誹謗: 他人を悪く言うこと(謗る: そしる)
- 中傷: 根拠のないことを言い、他人の名誉を傷つけること

- 冗談、遊び、エイプリールフールなどは無罪の理由にならない
- 見た人/聞いた人がどう取るかも考えて情報発信すること
  - できれば、一部を切り取られても誤解されないのが望ましい
    - 情報発信の一部を切り取りって恣意的に見せることがやりやすいTwitterはけっこう怖い

(法律)違反行為を証明する情報

- (法律)違反行為を証明する情報を公開してネット上で騒ぎ(炎上)に
  - ウェブから見れる情報は全世界の人が見ています
    - Twitter, blogなど公開を目的とした情報
    - 設定ミスで全世界に公開してしまった情報
  - 「うっかりやってしまった」、「違反行為とは知らなかった」であっても許さない人は世の中にはいます
- 自分でも思ってもみなかった情報で違反証明されることも
  - 例: 写真撮影で、フラッシュ禁止場所でフラッシュ利用を画像ファイルのexif情報から確認される

ニセ情報

- 人の名誉を毀損すると信用毀損(名誉毀損)になります
- 業務を妨害すると偽計業務妨害となります
  - 法律上の「業務」とは、「継続的に行っている活動」なので、利益を目的としない活動も業務扱いになります
- 株価操作を目的としていると判断されると「風説の流布」で罰せられます
  - 得た利益を全部没収のうえで懲罰

送受信に注意を要する情報

- 個人情報
  - 業務上送受信の必要があるかもしれませんが要注意
- 他の情報が隠されているデータ
  - 例: 写真のexif情報はGPS情報が含まれていることも
    →ストーキング被害
- きわどいアニメ/漫画などのイラスト
  - 国によっては児童ポルノ扱いされます
- 電子メールによる極端に大きなファイルの添付
  - 他のメールの送受信に影響が出ることも
    - メールサーバによってはサイズ制限で出戻りも
  - Dropboxなどのストレージサービスを利用し、そのファイル公開用URLを利用しましょう

犯罪行為に巻き込まれない/犯罪者にならないために

- 電子メールの送信者を疑う
  - 知り合いを騙ってくることもあり
- SSL証明書を確認する
- ID/パスワードの共用は避ける
- マルウェアに感染しないような対策をとる
  - アンチウィルスソフトウェアを利用(無料の物でも良い)
  - OSやソフトウェアを常に最新の状態にする
- お金にからむことは特に冷静になって考える
  - 近年は徹底的にお金を狙ってくる
- 自分の個人情報の公開には充分に注意する

ニセ情報にだまされないために(1/3)

- とりあえず、幅広い知識を身につけよう
  - 単純に過去の詐欺の話だけでなく、「様々な場における人間の判断」に関連した知識を身に付けると良い
    - 失敗知識データベースとかも参考になるかも?
  - 幅広い知識は研究にも使える
  - 目の前のPCで様々な情報(ニセ情報も含む)に触れることができる現在は素晴らしい時代です
    - ニセ情報も、「どう見破るか」の勉強に使えます
- 論理的に考えよう
  - どこかに変な論理展開とか論理的におかしい前提とか、いろいろと穴が見つかることがあります
  - 逆に「その情報が正しければ、世の中の別の部分が筋が通らなくなるのでは?」という逆に考えていくのもあり

ニセ情報にだまされないために(2/3)

- 定量的に考えよう
  - ネズミ講の仲間どもはこれで一掃できる
  - 規模拡大して嬉しいのはコストダウンだけ
    - それでも原材料費などの限度はある
  - 他にも、仕事量プラマイゼロの永久機関とか、化学結合エネルギーがマイナスの合成とか、分子数を数えると1を下回る化学事象、とか
- 事前に思考実験しておくのも面白い
  - 頭の体操と思って、暇な時に、過去のニセ情報に自分ならどう反論するか考える
  - (論理をベースとした)思考実験はこの先の研究等で役に立ちますよ
- オッカムの剃刀は重要
  - ある事柄を説明するために、必要以上に多くを仮定するべきでない
  - 背景知識もある程度必要するし、外れもあるけど、幅広い知識をつければOK

ニセ情報にだまされないために(3/3)

- ソース(source)に当たろう
  - ネット経由で1次情報にあたりやすくなりました
    - 編集されていない動画とか
  - ただし、記録文などでは、1次観測者が混乱している状態で記述することもあるので注意
  - 最近ではニセ出版社まででっち上げられるらしい
- 論文を根拠に出されてもすぐに信用しない
  - 査読無し口頭発表の論文なんて外れも多い
    - というか、それらが全て本当ならば、人類は複数の永久機関を実現していてエネルギー問題はとっくに解決しているはず
  - ニセ情報を出す側が学会を作っていたりもする
    - 乱造された学会がニセ情報を出す側の御用達しになったりもする
  - 有名学会の論文でも発見者とは別人が検証まで待つのは大事
    - 「偶然にノイズが有効なデータみたいに見えた」という事例も多数

ネットの匿名性、誹謗中傷への注意

- 加害者にならないように気をつけるべきこと
  - その情報を広めることは公益に値するか考える事
    - 「公益に値しない」は名誉毀損の成立案件の1つ
  - 誰かのデマを広げて加担してしまうことはあるので、ニセ情報かどうか検証すること
    - Twitterは気軽にRetweetできるので怖い
- 被害者にならないように気をつけるべきこと
  - 君子危うきに近寄らず
  - とはいえ、アレな人は何もなくても寄ってくることはある
  - どうしても被害者になった場合、警察に被害届や被告不明の状態の刑事告訴をしましょう
    - そんなにおおっぴらに動く人の匿名性なんぞたかが知れています
    - 「一旦届けをした後に、さらにエスカレートしてきた」時に警察が本格的に動きやすいです

最近の情報倫理における話題

- 個人情報の話題
  - 狭義の個人情報
  - 広義の個人情報
- 研究と教育に関する情報倫理
- 個人番号(マイナンバー制度)の話題

個人情報とは

- 狭義の個人情報
  - 「個人情報の保護に関する法律」で扱う対象
  - 5,000件以上の個人情報を事業に用いている企業が対象
    - 個人情報取扱事業者
  - 導入当初は、誤解による過剰反応が多かった
- 広義の個人情報
  - 「個人を一意に特定できる情報」
  - 1つの情報だけではなく、複数の情報を組み合わせて個人を特定できることも多い
  - 一部の人に限定することで、特定できることも
    - 例: 1日に100人が利用する駅で、毎日午前11時台に利用する人
    - 対策: 日ごとにIDを変えて匿名化する

狭義の個人情報に関する話題

- 個人情報収集後の約款変更の問題
  - 収集後に約款を変更して用途を広げるのはどうよ?
- 共同利用の問題
  - 「関連企業と共同利用する」という利用は問題が無いか?
  - 実際は、「共同利用」と称して売りつけているだけということも
- 特に悪名高い企業がいくつか存在している

広義の個人情報に関する話題(1/2)

- 最近はビッグデータ処理と関連して問題になることが多い
  - JR東日本のSuica利用履歴の販売問題
  - NICTの大阪駅でのカメラによる顔識別実証
  - 京大による商業施設での人間追跡技術研究
- 最近はビッグデータ処理と関連して問題になることが多い
  - JR東日本のSuicaの利用履歴
- 追跡されるのが嫌いで、追跡の可能性のあるサービスを可能な限り使わない人もセキュリティ業界にはいます
  - 交通系ICカードを使わない
  - ポイントカードなどもっての他
  - ただし、クレジットカードや銀行ATMは必要悪

広義の個人情報に関する話題(2/2)

- 企業は何かと詭弁を弄して(広義の)個人情報では無いと言い張ろうとします
  - 「携帯電話の番号は数字の羅列なので個人情報では無い」
  - 「列車での移動履歴は個人情報では無い」
  - 「車の保管場所の住所から番地を抜けば個人情報では無い」
  - 企業倫理の踏み絵として利用するといいでしょう
- 海外の方が広義の個人情報に関する規制が強い傾向にあります
  - あんまり日本の規則が緩いと、将来的に、「日本企業は我が国の個人情報に携わること禁止」にされる危険性あり
  - 日本でも、特定機密はクラウドを借りてそこに置くことは禁止している
    - クラウドを提供するサーバがどこにあるのかという問題

研究と教育に関する情報(+研究)倫理(1/2)

- 剽窃問題
  - 要は論文やレポートにおけるコピペ問題
  - 現在では、博士論文は剽窃チェッカにかけなくてなりません
  - 先行文献の図を使う時などは、正しく引用して、引用元を明記しましょう
- 講義資料における著作法第35条
  - 学校その他の教育機関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。
  - 出版社等がガイドラインを出しているので、沿って利用しましょう

研究と教育に関する情報(+研究)倫理(2/2)

- 教育研究における検体の個人情報
  - 医学部/薬学部/バイオ系がからみます
  - 検体の個人情報は論文/レポートではちゃんと匿名化しましょう
    - 特に、医学部/薬学部の電子カルテの情報
- 研究における秘密保持契約
  - NDA(Non-Disclosure Agreement)という略語もよく使われる
  - 企業との共同研究において、学生も結ばされたり、誓約書を要求されることが多々あります
- 生命に関する倫理
  - 一番分かりやすいのが、胚性幹細胞問題
    - そのまま育てれば生命になる物を研究に利用して良いのか?
  - 科学研究費補助金の応募書類では、独立した項目として要説明
  - 最近では、人を被験者にする工学的な実験でも求められています

個人番号(マイナンバー)をめぐる話(1/3)

- 個人番号(マイナンバー)とは
  - 日本の市町村に住民票がある人に与えられる12桁の番号(11桁の番号+チェックデジット)
  - 個人番号カード(マイナンバーカード)も同時に運用される
  - 企業側の法人番号も同じスケジュールで利用開始
  - 「国民に番号をつけるとは何事」と一部の人が騒いでいますが…
    - 今どき、顧客管理で(コンピュータ上で)番号を振られるのは当たり前
    - むしろ、運転免許証を個人認証に使うよりははるかに安全だと思う
- 個人番号のスケジュール
  - 2015/10から番号の配布開始
  - 2016/1からマイナンバーカード交付
  - 2016/1/1から利用開始(所得税、法人税、など)
  - 2017/1からマイポータル稼働開始

個人番号(マイナンバー)をめぐる話(2/3)

- 海外での同様の制度
  - アメリカの社会保障番号、台湾の中華民国国民身分証、韓国の住民登録番号、など
  - 海外での漏洩やトラブル事例
    - 2014/1の韓国でのクレジットカード会社による住民登録番号とクレジットカード番号の流出
    - アメリカでも流出した社会保障番号を利用したなりすまし多数
  - 一応、そのようなトラブルがあったことを考慮して設計されている
- マイナンバーカードを利用した個人認証も行われます
  - 国が「マイナンバーカードが本物かどうか」を保証
  - ウェブのSSL/TLSやSSL認証局と同様のシステム
    - 番号ではなく、カード内ICチップに入った秘密鍵を利用
  - こちらは、かなり広く利用することを総知恵しています

個人番号(マイナンバー)をめぐる話(3/3)

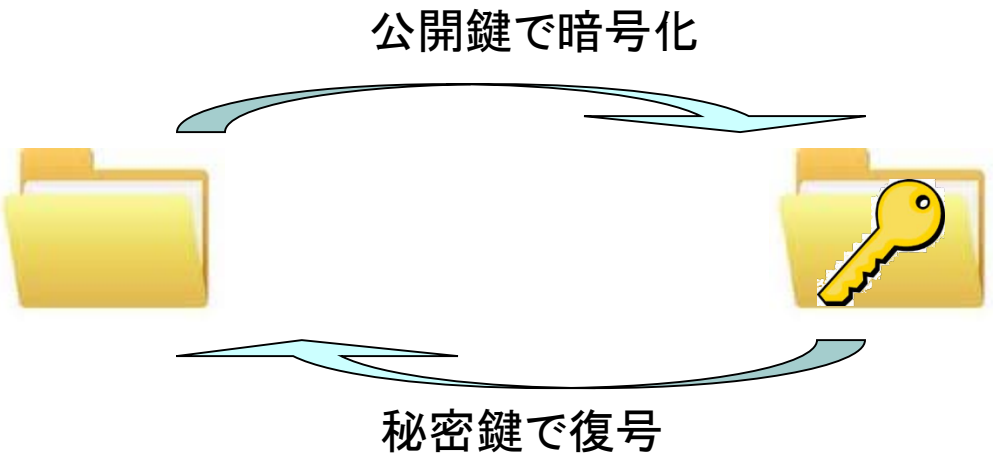
- 「番号」の用途がかなり制限されています
- 「番号」を使っていい用途
  - 社会保障: 年金、雇用保険、ハローワーク、医療保険、生活保護、等
  - 税: 税に関する申告書、等
  - 災害対策: 被災者台帳の作成、支援金の支給
- それ以外では使っていけません
  - ×会社が社員番号の代わりに利用、個人別の売り上げ管理に利用
  - 番号の持ち主本人の同意があっても不可
- 社会保障、税、災害対策以外の用途では、決して他人に教えないこと
  - 変な所で要求をして来る所は、とっとと通報して懲役or罰金送りへ
    - 4年以下の懲役または200万円以下の罰金
  - 漏洩等があれば(あったと思ったら)番号の再発行はいくらでも可能

マイナンバーカードの構成要素

- 個人番号(マイナンバー)
- 氏名、住所、生年月日、性別
  - 運転免許証と差は無い
- 顔写真
- 電子署名用秘密鍵
  - 税金関係の電子申請など、電子文書の改竄防止に利用
- 利用者証明用秘密鍵
  - 公開鍵認証を利用した本人証明に利用

公開鍵暗号: 秘密鍵と公開鍵

- 鍵を、閉めること(暗号化)しかできない鍵と開けること(復号化)しかできない鍵に分けることを考える
  - 複合しかできない鍵は自分で持つ(秘密鍵)
  - 暗号化しかできない鍵は自分に暗号通信をしたい人間に公開する(公開鍵)



実際の公開鍵認証の運用

- 公開鍵暗号の処理速度は共通鍵暗号と3桁ほど違う

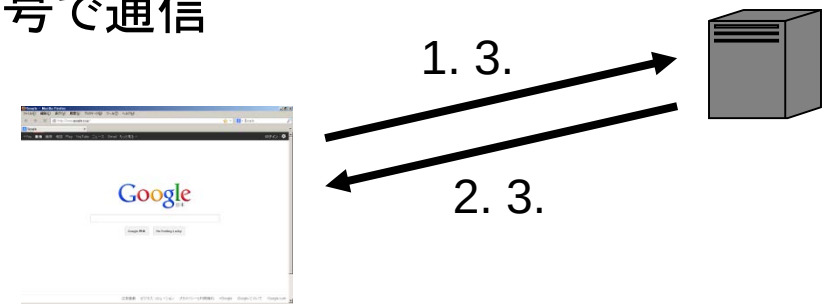
→全て公開鍵暗号で処理していたら遅すぎ

→共通鍵暗号も併用する

  - 共通鍵暗号の共通鍵は使い捨て

- 動作

1. 通信開始する側(例: ウェブブラウザ)が公開鍵で乱数で生成した共通鍵を暗号化して送信
2. 通信を受け取る側(例: Webサーバ)は秘密鍵で送られてきた共通鍵を復号
3. 以降は、共通鍵暗号で通信



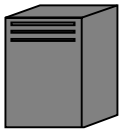
マイナンバーにおける個人認証

- 注: 普通はこういう実装になるという説明で、本当にそのようなシステムになっているかは知りません

サービスを利用したい個人

個人認証を
必要とする
サービス提供者
(例: 図書館)

個人認証サーバ
(国が運営)



サービス利用の希望

個人認証の依頼(カードで)

暗号化通信確立
(サービス提供者抜きで)

公開鍵で暗号化した乱数を送信

秘密鍵で複合した乱数を返信

「本人ですか?」に
「はいそうです」と返すだけ

送信乱数=返信なら
秘密鍵は正しい

間違いなくカード上の
氏名等の本人です

サービスの提供

時系列

設計思想

- 住基ネットに関する裁判記録を尊重してシステム設計
- 住民基本台帳ネットワークシステム最高裁合憲判決の趣旨
  1. 何人も個人に関する情報をみだりに第三者に開示又は公表されない自由を有すること
  2. 個人情報を一元的に管理することができる機関又は主体が存在しないこと
  3. 管理・利用等が法令等の根拠に基づき、正当な行政目的の範囲内で行われるものであること
  4. システム上、情報が容易に漏えいする具体的な危険がないこと
  5. 目的外利用又は秘密の漏えい等は、懲戒処分又は刑罰をもって禁止されること
  6. 第三者機関等の設置により、個人情報の適切な取扱いを担保するための制度的措置を講じていること
- ろくでもない用途かどうかは、上記の趣旨をベースに考える

設計思想への解(実際の実装)(1/2)

- 情報をみだりに第三者に開示又は公表されない自由
  →利用可能な組織の身元確認、用途の限定、など
  - ただし、後々、法律の改正(悪)で範囲が広がる可能性はあるので、今後の運用はきっちり監視すること
- 個人情報を一元的に管理しない
  →サービス提供に関わる情報はサービス提供者が持つ
  - 行政においても同じ
- 正当な行政目的の範囲内での利用
  →法律による制限

設計思想への解(実際の実装)(2/2)

- 情報が容易に漏えいする具体的な危険がないこと
  →…さあ?
  - 個人番号自体は漏洩前提で、がんがん変更していける設計になっている
    - 「漏洩したと思った」時点で変更申請可能
- 目的外利用又は秘密の漏えい等は、懲戒処分又は刑罰
  →そのような法律になっている
- 第三者機関による個人情報の適切な取扱いを担保
  →情報提供等記録開示システム?

情報提供等記録開示システム(マイポータル)

- マイナンバー導入後1年後ぐらいに設置予定
- 機能
  - 自分の特定個人情報をいつ、誰が、なぜ情報提供したのを確認可能
  - 行政機関などが持っている自分の特定個人情報について確認
  - 行政機関などへの手続を一度で済ませる機能
- その他、お知らせなどの余計なお世話な機能も

考えられる悪いことへの利用

- 制度がよく知られていないことを利用した詐欺
- 名寄せによる個人情報集積
  - 名寄せ: 複数のデータの共通項(名前など)を使って巨大データを作ること
  - ただ、すでに免許番号を必要とするようなサービスにおいて、やる所にはやられているので今更な感じ
    - むしろ、法律による制限がかかる分マシな気が…
- マイナンバー普及へのゴリ押し
  - システム改修などでお金が動きますからね
  - 厚生省の人間が収賄容疑で逮捕されましたね

マイナンバーのTips(1/2)

- 最後の1桁はチェックデジットなので、11桁が本体
  - チェックデジット: データの異常を確認するための追加数字
  - 「最後の1桁は秘密のまま番号を提供して」という詐欺が出てきそう
  - チェックデジット計算方法により、チェックデジットの0の出現率が高いという特徴がある(後述)
- 自分で番号を公開するのも法令違反です
  - 罰則はありませんが…
- 嘘で危機を煽る輩が多数いますが、必要に応じて真偽を確認しましょう
  - 設計思想に対して反していたら、自分で真偽を確認しましょう
  - 情報検索の講義で話しますが、今は法律や省令にも簡単にアクセスできます

マイナンバーのチェックデジット

- 算式(総務省令第八十五号 第五条より)

$$11 - \left(\sum_{n=1}^{11} P_n \times Q_n \text{を11で除した余り}\right)$$

ただし、$\sum_{n=1} P_n \times Q_n$を11で除した余り≦１の場合は、０とする。

- Pn: 個人番号を構成する検査用数字以外の11桁の番号の最下位の桁を1桁目としたときのn桁目の数字
- Qn: 1≦n≦6のときn+1、7≦n≦11のときn-5
- 注目点: 11で剰余を取って1以下の場合は0
  - 0は0-1と10-11の2パターンがあるので、0が他の数字の2倍出現
  - 偽データ検出に使えるかも?

マイナンバーのTips(2/2)

- ICチップの空き領域の利用が計画されている
  - 図書館とかの利用者カードの情報を統合したりとかに利用可能
  - …が、あまりICチップの空き領域がありません
- 個人認証の利用では複数の認証レベルが設定できる
  - カードをかざすだけ、カードと短いパスワード、カードと長いパスワード、など
- 中高生向けとして、政府広報が「15歳から学ぶマイナンバー」というものを出しています
  - 検索情報:マイナンバー 政府広報オンライン
- 「個人番号」という正式名称は汎用性が高くてまぎらわしいので他の個人番号と混同しないように注意