情報倫理、ソーシャルエンジニアリング

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

- ソーシャルエンジニアリング
- 情報倫理
  - 個人情報問題
  - プライバシーに関わる問題
  - 著作物の利用
  - 欧州一般データ保護規則(GDPR)
  - 個人番号(マイナンバー)
  - COVID-19感染者追跡とプライバシー問題
  - AI応用領域における倫理

ソーシャルエンジニアリング

- 最終的に計算機を使うのは人間
  →人間をセキュリティホールと考えた攻撃
- 今までに説明した、メールでのマルウェア送り込みやニセ情報拡散にも使われている技術
  - フィッシングとして説明済
- あえてこちらに分類するのに特徴的なポイント
  - 目標以外の人間も騙し利用する
  - 電話などのリアルタイム性の高い手段も活用する
- 某有名ソーシャルエンジニアリング悪用者の著書(更生後)の和訳から「欺術」と言われることも
- 振り込め詐欺系の物を考えると分かりやすいかも
  - 高度な物の例: 報告役と警察官役の2人をつかった事故偽装、など

よくあるソーシャルエンジニアリング

- コールセンター(ヘルプデスク)への認証情報問合せ
  - コールセンター側が利用する本人確認情報は、攻撃者によって事前に把握されている
  - 組織内コールセンターに役員などの重役を装っての問合せは、応対者の萎縮や奪取できる権限の強さという点から怖い
  - 攻撃者は非常時を装ったりして応対者を焦らせる
- 電子メールの文面によるソーシャルエンジニアリング
  - 非常に事例が多い
  - 代表例: あなたのXXアカウントが不正利用されたので…
  - 逆に、文面を長くして怪しくなるよりは「領収書送ります(実体まマルウェア)」のようにあえて文面を短くしている事例も

コールセンターを利用したソーシャルエンジニアリングの実例

@Nという1文字Twitterアカウントを持つ人が利用中の独自ドメインの管理権限を奪われた(2014年)

- 攻撃者はTwitterに登録されていた独自ドメイン(example.comなど)のメールアドレスに着目
- 攻撃者はまずPayPalに電話してメールアドレス(ログインID)に対応したクレジットカードの末尾4桁を聞き出した
- ドメインレジストラがクレジットカード末尾6桁で登録者を認証
  - 攻撃者は「末尾4桁は覚えているのだが…」と言って、上位5,6桁目を正解まで試させてもらった
- 最終的に攻撃者はTwitterのアカウント(@N)と独自ドメインの管理権限を交換
  - が、最終的にTwitter社側が事件を知って元に戻してくれた

サービスの設計の穴をついたソーシャルエンジニアリングの実例

- 以前にFacebookが「パスワードを忘れた場合、Facebook上の友人に3人にパスコードを送って認証」という物を導入
  - パスコード送信先は友人リストから送信先を決めることが可能

→攻撃者が複数アカウント利用で3人分の友人を作れば認証できる

  - 2011年ぐらいから問題にされていた
  - 知人や有名人になりすました友人申請が増えているということで、この攻撃が疑われて警告が出た(2013年)
  - というか、友人が共謀してもアカウント乗っ取りができてしまう
- 現在は「信頼できる連絡先(友人)を事前登録する」形で問題を緩和

「配慮して処理」をやりそうな人を狙ったソーシャルエンジニアリングの例

- 大学の秘書宛に偽の国際会議の請求書を送付
  - 「先生の手を煩わせずに処理」されることを狙っている?
    - まあ、普通は「どの予算で支払うか」とか先生とやりとりするが
  - 先生側としても、近くで参加する国際会議があれば、勘違いするかもしれな
  - (まあ、最近の事前支払いはクレジットカードがほとんどで請求書が来ることはあまりない)
- 機材をリース中の会社に対し、偽会社がリース元と偽って偽リース費請求書を送付

  →ビジネスメール詐欺(フィッシングの亜種)

SNSでのつながりから攻めたソーシャルエンジニアリング(+標的型攻撃)の例

- 世の中にはビジネス上のつながりを作るSNSなるカテゴリがある(代表例: Linkedin)
  - 新コラボレーションの模索や転職活動など建設的な使い方も色々
  - 一方で、ソーシャルエンジニアリングを考えている悪人に対して、情報を与えてしまう機会にもなる
- 事例
  - ある社の社員のあるビジネス向けSNS利用者にマルウェア付きメール(SNS登録メールアカウント)が送られてきた
  - 論文の共著者を騙って、ビジネス(というか研究者向け)SNSの登録案内を送ってきた(本物の招待状らしかったが)
- 即座にマルウェア送り込みをするのではなく、長期的なやりとり型攻撃を複合させた事例もある

ソーシャルエンジニアリング防止のポイント

- 焦りは人の判断能力を狂わせることを自覚する
  - 相手はそのことを承知で、電話などのリアルタイム応答を必要な手段で連絡してきたりする
- 本当にそのようなことをやる必要があるかじっくり考える
  - 必要があれば関係箇所に問い合わせる
  - コールセンターなどでは同僚や上司に相談するのもあり
- 相手側が地位などを強く出して急かせようとしている時には特に注意
  - こういう時にソーシャルエンジニアリング防止の観点から慎重に対応した人を褒める形になるのが理想
- 相手側に追加で情報を与えないように注意
  - 他の人の名前や関係部局など
  - 攻撃者の矛先が向かったり、他の人や関係部局から情報を仕入れた上で再度攻撃をしかけてきたり…

ソーシャルエンジニアリングに利用される情報

- ソーシャルエンジニアリングに利用される情報
  - 職業(学校)関連: 勤務先、職種、役割
  - 住所、電話番号、SNSその他の情報サービスのアカウント
  - 過去の情報: 過去の勤務先、出身学校、出身地
  - 趣味、日常的に行っている場所、
- SNSその他の公開情報からこのようなナレッジを構築可能
  - 公開情報からのナレッジ構築はOSINT(Open Source INTelligence)とも呼ばれる
  - (個人レベルでの現実的な被害では、サイバー攻撃よりもネットストーカーの方が怖いかもしれないが)
- 逆に、ソーシャルエンジニアリングで容易に入手できる情報を認証の補助にしている情報サービスのセキュリティ意識は弱いと考えることもできる

概要

- ソーシャルエンジニアリング
- 情報倫理
  - 個人情報問題
  - プライバシーに関わる問題
  - 著作物の利用
  - 欧州一般データ保護規則(GDPR)
  - 個人番号(マイナンバー)
  - COVID-19感染者追跡とプライバシー問題
  - AI応用領域における倫理

情報倫理

- あくまでも「倫理」なものが多く、判断がいろいろと難しかったり時代とともに変化したりする
  - 一部は後から法律に組み込まれたりするが…
- 個人的な情報倫理の考え方: 情報を提供する側と提供された情報を利用する側の落とし所
  - 情報を提供する側としては、提供した情報を濫用されたくないがサービスは便利になって欲しい
  - 提供された情報を利用する側としては、情報を効果的に利用することで利益を上げたりサービスの価値を上げたりしたい
    - 手っ取り早い「情報の利益化」は情報自体を売る(外部に提供する)ことで、いくつかのサービスはその旨を利用規約に書いてあったり
- 「考える機会になってくれれば」というレベルの話題として

個人情報の分類

- 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と呼ばれる
  - 導入当初は、誤解による過剰反応が多かった
  - 必要なくなった個人情報については「事業者は遅滞なく消去するよう努めなければならない」はずだが、なぜか残っていて流出することが
- 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

個人情報に関する話題(1/4)

狭義の個人情報関連

- 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
- サービス提供に必要な物以上の情報の要求してくるサービス提供者
  - ウェブサービスやアプリの利用において
  - 「サービス提供においてそこまでの情報は必要?」と思う物が多数ある

個人情報に関する話題(2/4)

広義の個人情報関連

- 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
  - Facebookで収集した研究用データの某大統領選挙対策利用
- 個人の嗜好の解析をもととした広告等の可否
  - 個人を一意に特定しているわけではないが、個人を「特定のグループ」に特定してはいる
  - 広告と称して変な誘導ができたりしないか?
    - まあ、変な誘導をする広告自体は旧来(電車内の吊り広告とか)からありましたが、それをもっと個々の人に対してカスタマイズ可能
    - 某大統領選挙で誘導するための広告があったという噂も

個人情報に関する話題(3/4)

- 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
- 企業ごとに情報倫理に対する温度差はあるし、事故を起こしても変わらないことが多いと感じる
  - 技術的な物は事件をもとに一気に改善される事例はあるが、倫理側は改善されない事例が多いように見える
    - そういう意識の人間が事件をもとに一掃されるわけではないから?
  - 高い確率で情報倫理上の問題な事件を繰り返している企業はいくつかある

個人情報に関する話題(4/4)

- 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
  - 特に欧州でその傾向が強い →EU一般データ保護規則(後述)
    - 色々なネット上のサービス企業が訴えられて罰金支払いの判決が出たり
    - 日本でもEUからのアクセスを禁止する企業が出た(踏み絵にしましょう)
- 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カードを使わないし、ポイントカードなどもってのほか
- 逆に、サービス間の情報の漏れ(連携)を調べている人も
  - 登録時の住所やメールアドレス(要メール側の対応)の末尾に余分なsuffixをくっつけてみたりとか

ターゲティング広告に関連する個人情報/個人追跡技術やその問題(1/2)

- Cookieの類が追跡に使われる話は以前の講義資料参照
- ウェブビーコンによる追跡
  - (複数ウェブサイトに)ユニークIDを持つ極小の(透明)画像を埋め込み、ウェブサーバに届いたアクセス履歴から解析
  - メール(HTMLメール) に埋め込むことも可能
- ブラウザ上でJavaScriptでいろいろ実行して反応から判別(ブラウザフィンガープリンティング)
  - Fingerprintjs2[1]などオープンソースの実装もあるので、(ダウンロードして)どれだけ情報が取れるか体感することも可能
  - メジャーな端末(iPhoneとか)を使っている人は識別しにくそうだが、マイナー端末とかを使っている人は追跡できそう

[1] https://github.com/Valve/fingerprintjs2/

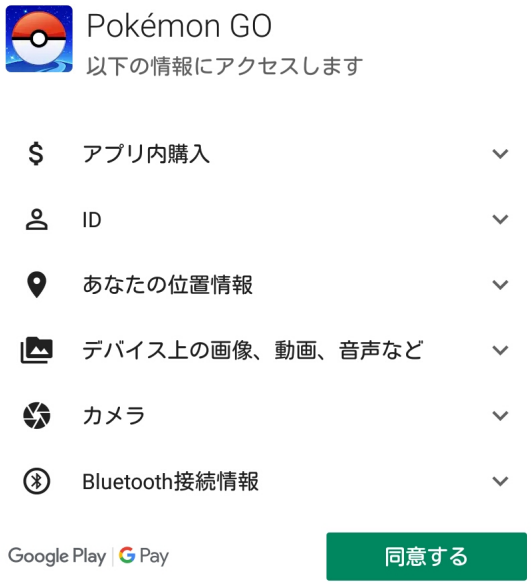
ターゲティング広告に関連する個人情報/個人追跡技術やその問題(2/2)

- ブラウザ側からのアクションを行わせると、さらにデータを取れる
  - ブラウザ側からのアクションも含めて、ウェブサーバ側がブラウザからどれだけ情報取れるか見せてくれるサイトもある[1]
- 訪問者のSNSアカウントを判別する研究もある[2]
- カメラを使った個人判別を広告に使うのも危惧されている
  - タクシーに乗ったら無許可で乗客を撮影して性別を判別して広告
  - 監視カメラの画像を広告利用する話もよく出てくる
  - 個人的には、最近の顔認証の濫用傾向がちょっと嫌(倫理が追いついていなさそうな感じで)

[1] http://webkay.robinlinus.com/
[2] http://www.ntt.co.jp/sc/project/cybersecurity/silhouette.html

スマホ等のアプリにおける個人情報濫用

- アプリストアの利用の一般化により、様々なアプリを手軽に試せるようになった
- アプリインストール時の権限気にしています?
  - 個人情報流出を危惧している人70.6%に対し、アプリの権限を気にしている人は19.3%[1]
  - よく見ると、「これ必要なの?」な権限があることも
- Android 6.0以降やiOS 8.0以降ならば個別に権限設定できます
- ただ、アプリの機能として必要な情報を横流しにされるとねぇ…
  - 例: タクシーの配車アプリが位置情報を広告会社に横流し



[1] IPA "2016年度 情報セキュリティの脅威に対する意識調査," 2016.

個人情報濫用に対しての自衛

- Cookieによる追跡対策
  - 最近のウェブブラウザは「Do not track」意志表示や第3者Cookieの拒否を設定できるので設定
  - 定期的にCookieをクリアする
- Android/iPhoneアプリにもサービス提供に必要以上に権限を取って活用しようとする物は避ける
  - 自分は気になったら他に同等で必要権限の少ないサービスを探す
- Androidスマホ/タブレットで製造会社独自の情報利用に同意しないと利用開始すらできない製品が存在する →避ける
  - うっかり当たってしまったら、小売会社にも相談するなどして返品しましょう

概要

- ソーシャルエンジニアリング
- 情報倫理
  - 個人情報問題
  - プライバシーに関わる問題
  - 著作物の利用
  - 欧州一般データ保護規則(GDPR)
  - 個人番号(マイナンバー)
  - COVID-19感染者追跡とプライバシー問題
  - AI応用領域における倫理

プライバシーの保護

- 個人的に思う情報技術におけるプライバシーの要点は「どこで何をしていたかを追跡されたり公にされないこと」
- 問題となる例
  - 監視カメラ映像の目的外利用
  - 「どこで」の対象となる施設の責任のある立場の人が、個人を特定できる形で情報を発信する
- 「公益性が無いこと」はプライバシー侵害の要件の1つになる
  - 公人の公務中はプライバシー要件から外れる
- 情報技術で長年に渡って情報が残ることで新たな問題も
  - 忘れられる権利: 昔の出来事をどこまでも蒸し返されないように…

忘れられる権利

- 過去に行った愚行とか犯罪とかに対しても
  - 犯罪であっても、刑罰をこなした後の社会復帰の障害になるのは好ましくない
    - 再び犯罪に走らざるを得ない形になっては本末転倒
- これを受けて、いくつかの検索エンジンは削除基準を設けている
- 認められなかった事例: 児童買春・ポルノ禁止法違反事件で罰金の略式命令が出た件の逮捕ニュースの削除の可否
  - 社会的に関心が高い犯罪の逮捕ニュースで、逮捕時からの時間経過が短く、公共の利益の点から削除は望ましく無いと判断された
    - 第2審の判決であり、第1審では削除すべきという判決

データ利用のための匿名化処理

- データの有効利用による社会を利便性向上も重要

→情報の一部を落とし個人を特定できなくしての利用が主流

  - ただし、データの内容によっては処理後に一意に特定できることも

- k-匿名化処理
  - 同一の内容となるデータがk個存在する所まで情報を落とす

名古屋市千種区不老町, 35歳	k=2で 匿名化	名古屋市千種区, 30代
名古屋市昭和区山里町, 23歳		名古屋市昭和区, 20代
名古屋市昭和区八事本町, 31歳		名古屋市昭和区, 30代
名古屋市千種区星が丘, 27歳		名古屋市千種区, 20代
名古屋市千種区東山通, 27歳		名古屋市千種区, 20代
名古屋市昭和区鶴舞, 33歳		名古屋市昭和区, 30代
名古屋市昭和区御器所通, 25歳		名古屋市昭和区, 20代
名古屋市千種区池下, 39歳		名古屋市千種区, 30代

公共の場での顔認識(顔認証)問題

- 顔認識技術の発達で、顔認識の濫用が問題となっている
  - 個人の行動の自由に付随する、「正当な理由なく、個人の行動を追跡したり記録する(ことで萎縮させ自由を奪う)ことの禁止」に抵触
  - 認識精度も低い上、生体情報は変更は難しい →冤罪が連続した話
- 2019/5に米国サンフランシスコ市が「公共機関による顔認証技術の使用を禁止する条例案」を可決[1]
  - その後、米国内で追従する自治体がちらほら出る
- 2021/4にEUで顔認証を含むAI技術規制案を出す[2]
  - 先行している物と同様、公共の場での顔認識の利用を禁止
  - 3年以上の懲役刑になる可能性の物など例外はあり
  - 悪性度の高い「収集した個人情報をもとにしたターゲティング公告」も規制

[1] https://www.bbc.com/japanese/48276999
[2] https://wired.jp/2021/04/26/europes-proposed-limits-ai-global-consequences/

概要

- ソーシャルエンジニアリング
- 情報倫理
  - 個人情報問題
  - プライバシーに関わる問題
  - 著作物の利用
  - 欧州一般データ保護規則(GDPR)
  - 個人番号(マイナンバー)
  - COVID-19感染者追跡とプライバシー問題
  - AI応用領域における倫理

著作物の利用(1/3)

- 著作物のコピーは著作権法で禁止されている
- ただし、著作物の適切な引用は許される
  - 丸々と引用するのはコピーと変わらないので必要な部分だけ
  - ちゃんと出展を明記して引用(許可は不要)
  - (引用しておいて引用内容を言及しないのはよろしくない)
  - 最近は言論封殺に適切な引用を「著作権侵害だ!」と因縁つける人間もいるらしい
- 新たな情報を生成する場合に過去の情報の利用と著作権との兼ね合いが発生する
  - そもそも、過去の経緯を踏まえない、全くの新しい情報というのはほとんど存在しえない

著作物の利用(2/3)

キュレーションメディア問題

- キュレーション: 集積した情報を整理して展示する行為
  - 博物館等のキュレーターが語源
  - 整理された情報は雑多な情報よりもはるかに価値が高い
  - ついでに、古くなっている部分をアップデートしてくれたりすると嬉しい
- これを商業化したことで問題が…
  - キュレーションした情報を掲載するとお金がもらえる

  →お金目当てで質の悪いキュレーションが大量に発生
  - 問題: 丸パクリと変わらない物(書き直し)が大量に、嘘情報掲載が大量に、大量すぎて管理されず検索汚染が発生
  - 「ウェブ上の情報が粗悪な物で汚染されたため、(信頼できる人が書いた)本の復権が進んでいる」と言う人もいる
    - もちろん、質の悪い(自費出版)物を大量に出している所もある

著作物の利用(3/3)

オンライン配信物が急速に増えているため(COVID-19禍もあいまって)、関連して著作権法は改正が頻繁に行われている

- 著作物が内包するデータを利用したサービスOK(2018/5)
- 授業目的公衆送信補償金制度の設定(2018/5)
- 映り込みコンテンツの権利制限強化(2020/5)
- (軽微な物を除いた上で)侵害コンテンツのダウンロードの違法化(2020/5)
  - 軽微な物: 長編の中の数コマ/数行/数秒、サムネイル、など
- 特に意思表示が無ければ、放送番組の権利処理でオンライン配信も同時に処理(2021/5)
- 図書館がデジタル化した絶版本をオンライン貸し出し可能に(2021/5) →2022/5/19から国立国会図書館のサービス開始

研究と教育に関する情報倫理

- 論文やレポートでは剽窃を疑われないよう適切な引用を
  - 要は論文やレポートにおけるコピペ問題
  - 先行文献の図を使う時などは、正しく引用して引用元の出典を明記
- 教育研究における検体の個人情報
  - 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、医療情報における電子カルテの情報
  - 匿名化された情報を提供するサービスもあり
- 研究上の秘密保持契約(NDA: Non-Disclosure Agreement)
  - 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
  - 最近では、ユーザインタフェースの評価とか人を被験者にする種々の実験でも求められる方向に

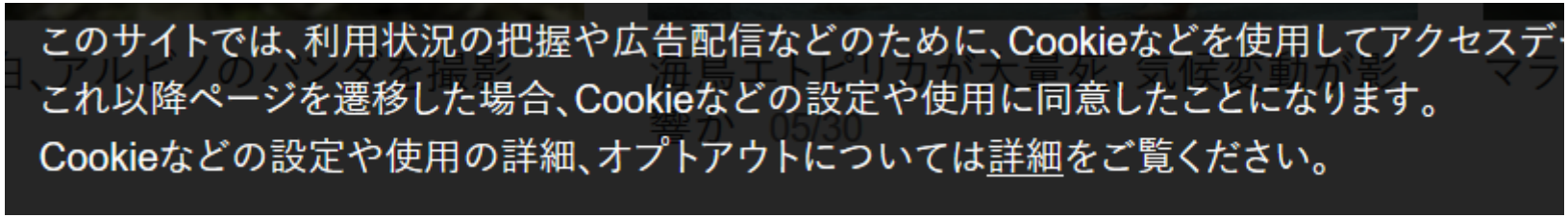
概要

- ソーシャルエンジニアリング
- 情報倫理
  - 個人情報問題
  - プライバシーに関わる問題
  - 著作物の利用
  - 欧州一般データ保護規則(GDPR)
  - 個人番号(マイナンバー)
  - COVID-19感染者追跡とプライバシー問題
  - AI応用領域における倫理

EU一般データ保護規則(1/4)

- 一般には、後ろのGDPR(General Data Protection Regulation)で呼ばれたりしている
- 2018/5/25より施行
- 「EU内居住者の情報」を扱う場合の規制を強化
  - 厳密には、EU内企業がEU外個人のデータ管理/処理する場合も同様の規制が入る
- 逆に、規定を整備することで、適切な形でのデータ利用を活性化させる面もある

↓一昨年からよく見るこれはGDPR逃れの定番文句



EU一般データ保護規則(2/4)

- 違反の罰則は厳しい
  - 最も厳しい物: 企業の場合、2000万ユーロまたは前会計期間の全世界の売上高の4%のうち大きい方
- 一旦同意した個人情報規定の同意を取り消すことができる
  - (今まで、これがある所ってほとんど無かったのでは…)
- 求人情報で集めた情報もGDPR対象
- 情報漏洩時の速やかな(72時間以内)の通知が要求される
- 保持している自分の個人情報の開示請求ができる
  - 無料かつ返答期間制限ありで

EU一般データ保護規則(3/4)

- 必要に応じて個人データの消去を要求できる
  - 個人データを外部サービスなどに持ち出すことの要求もできる
    - 購買データとかを自分の家計簿とかに入れやすくなる?
- 匿名化処理に関する規定がある
  - 匿名化済みのデータの流出等は通知の必要はない
- 基本的に、データの収集等に同意が必要となる
  - トラッキング広告が収集するトラッキング用データにおいても

- いろいろと先進的な規則ため、(当初は?)情報の正当な利用やそれを前提とした運用に問題が出てきそう
  - ドメイン管理者の連絡先を出せない? →インシデント時の連絡先は?

EU一般データ保護規則(4/4)

- 日本企業からして面倒な点(個人的には、対応進んでいるとは思えない)
  - 日本に来たEUの人も対象
    - フリーWiFiとかの登録とかデータ追跡とかどうしましょう…
  - EUからのウェブサイトへのアクセスログ(一見さん)は?
- 日本企業にも影響が大きいので、内閣府外局の個人情報保護委員会がGDPRの日本語訳を出している
  - https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/
- 2018/5に施行開始してさっそくバトル開始
  - 非営利団体がFacebookとその傘下、および、Googleを提訴
  - 「対応できねーからEUからは見えねーよーにするよー」対応
  - その後
    - 2019/1にGDPR違反を理由とするGoogleに5000万ユーロの罰金
    - 「閲覧を続ける人はCookieを受け入れたとみなす」扱いは許さん!
      →最近、各目的のCookieの受け入れ可否を設定できるところが増えた

日本でもGDPRに準じた改正が入りました

- 2020/6/5に改正個人情報保護法が成立[1]
  - GDPRの良い所を導入した感じ
    - 個人データの利用停止や消去を請求の権利の拡充
    - 提携企業先に渡す場合に本人の許諾を取らないといけないし、提供される側もその旨を確認する必要がある
    - 匿名化したデータはOK
  - 同日に改正著作権法も成立(著作物を違反物と知りつつダウンロードした側にも刑事罰)
- リクナビが勝手に内定辞退率を作って企業に売った事件[2,3]が1つの契機になっている雰囲気
  - 提供を受ける側についても妥当性の確認の話が入っている

[1] https://xtech.nikkei.com/atcl/nxt/news/18/08052/
[2] https://www3.nhk.or.jp/news/html/20191226/k10012229231000.html
[3] https://diamond.jp/articles/-/215312

概要

- ソーシャルエンジニアリング
- 情報倫理
  - 個人情報問題
  - プライバシーに関わる問題
  - 著作物の利用
  - 欧州一般データ保護規則(GDPR)
  - 個人番号(マイナンバー)
  - COVID-19感染者追跡とプライバシー問題
  - AI応用領域における倫理

個人番号(マイナンバー)と情報倫理(1/2)

いまだに誤解とか不正利用案件も多いので…

- 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
- 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とその利用者の組が本物かどうか」を保証
  - ウェブのSSOと同様のシステム
  - こちらは、かなり広く利用することを想定しています
    - 2022年になってもなかなか利用が進んでいなくて個人的には不満

個人番号(マイナンバー)と情報倫理(2/2)

- 「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

マイナンバーの設計思想

- 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)

- 情報が容易に漏洩する具体的な危険がないこと
  →…さあ?
  - 自治体によっては運用が甘いことが存在する可能性は高い
  - 一応、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(マイナポータル)

マイナンバーのTips

- 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
- マイナンバーカードのICチップの空き領域の利用が計画中
  - 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
- 情報提供等記録開示システム(マイナポータル)で情報提供状況を確認可能
  - 当初はJava必須だったりして叩かれたが、改善は進んでいる
- 「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

概要

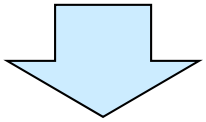
- ソーシャルエンジニアリング
- 情報倫理
  - 個人情報問題
  - プライバシーに関わる問題
  - 著作物の利用
  - 欧州一般データ保護規則(GDPR)
  - 個人番号(マイナンバー)
  - COVID-19感染者追跡とプライバシー問題
  - AI応用領域における倫理

COVID-19の感染者追跡とプライバシー問題(1/2)

- COVID-19の感染爆発を防ぐためには感染者と(三密で)接触した人に検査を受けさせるのが望ましい
- しかしながら、感染者および接触者双方のプライバシーの問題がある

→個人の権利がちゃんとしてる国では強制的にやりにくい

- 逆に、国家体制が優先される国では、個人追跡を積極的にやって封じ込めをやっている



情報技術を利用して、匿名性と接触者追跡を両立させる試みが多数行われている

COVID-19の感染者追跡とプライバシー問題(2/2)

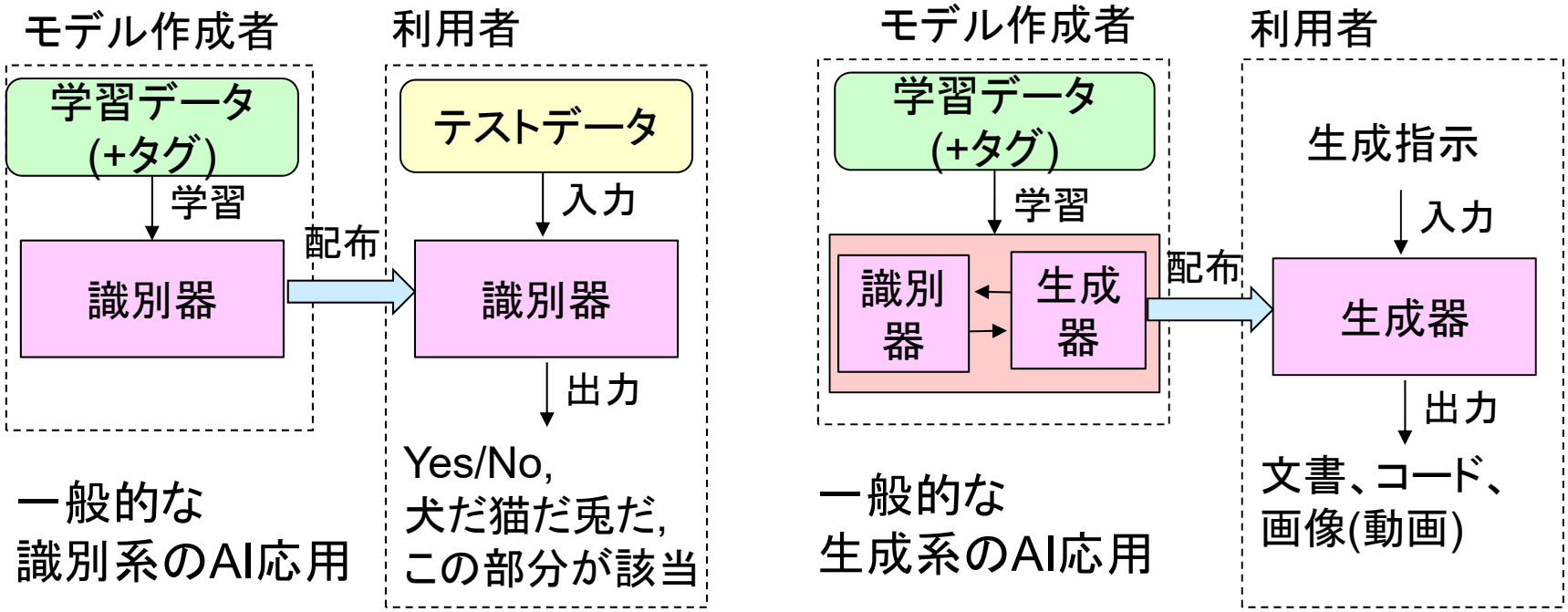
- Googleの接触者警告アプリフレームワーク[1]
  - 匿名化のためにランダム生成のIDで接触者を管理
  - 接触状態はBluetoothで互いのIDをやりとりして管理
    - 接触日、継続時間、接触距離(Bluetooth信号強度)を記録
    - 位置情報はひもづけない
    - IDは一定時間ごとに変更かつ14日間(最長潜伏期間)のみ保持
  - 感染判明者のIDの報告をもとにアプリが脅威度を計算
    - 脅威度が高い場合にはその旨を通知
    - 偽報告対策のため、感染判明者IDは公衆衛生機関でのみ報告可能
- Appleのフレームワークも同じ仕様らしい[2]

[1] https://support.google.com/googleplay/answer/9888358?hl=ja
[2] https://k-tai.watch.impress.co.jp/docs/news/1253705.html

概要

- ソーシャルエンジニアリング
- 情報倫理
  - 個人情報問題
  - プライバシーに関わる問題
  - 著作物の利用
  - 欧州一般データ保護規則(GDPR)
  - 個人番号(マイナンバー)
  - COVID-19感染者追跡とプライバシー問題
  - AI応用領域における倫理

一般的なAI応用のざっくりとした説明



非常にざっくりとした補足説明

- 識別器(Classifier)の学習には教師あり学習と教師なし学習がある(タグがあるか否か)が、多くは教師あり学習
- 生成器の学習には、生成器の出力の識別器による評価を受けての更新を繰り返す

学習およびモデル生成における倫理 (1/2)

- 集めてきた学習データを、本当に学習データとして用いることに倫理的な問題は無いのか?
  - 違法に収集されたデータは含まれていないのか?
  - 学習データの生成者はモデルの学習に利用することを想定して公開しているのか?
  - 学習データの生成者に報酬が何もないのはどうか?
  - EUでは学習データの公開を盛り込んだ法案も[1]
- 学習データから発生する偏りの問題 (公平性の問題)
  - 現状の世の中のデータをそのまま学習に使うと、現状の社会の母集団に対する偏りまで学習してしまう →要学習前の調整
    - 自分の研究でも、悪性サンプルと良性サンプルの調整は重要
  - 例: 職業の絵の出力と人種、家庭内での仕事の絵の出力と性別

[1] https://gigazine.net/news/20230428-eu-new-copyright-rules-for-generative-ai/

学習およびモデル生成における倫理 (2/2)

- モデルから学習データを復元する攻撃で、学習データに含まれていた秘匿性の高い情報とかは大丈夫か?
  - モデルに対する攻撃は「移転攻撃」と言われ、モデルの模倣や学習データ復元などが代表例
  - すでに生成系モデルで、学習に回された以前の入力を復元できたような事例が
- 生成し配布されたモデルは信頼できるのか?
  - 悪意の込められたモデルは配布されたりしないのか?
  - 例: 特定の攻撃パターンのみ反応しない攻撃検知モデル
- (モデルのサイズや学習データ量が大きくなり過ぎて、お金を持っているビッグテックの一人勝ちを加速するのでは?)
  - モデルが大きくなると学習のコストが大きくなったり、そもそもメモリ量で学習に制限がかかったり

モデルからの出力における倫理(1/2)

- 生成器の嘘出力(Hallucination)の問題をどうするか?
  - Hallucination = 幻覚と言われているが、個人的にはAI側に甘い用語な印象なので「嘘」と言いたい
  - 識別器でも誤判別の責任はどこが?
  - とりあえず、(意図的に作って)ばらまいた人が逮捕された事例あり[1]
- 生成器による生成物が著作権を侵害する可能性
  - 特定の人の絵や文章を真似た出力は著作権侵害か?
    - 特に、特定の絵柄に出力を寄せることができる生成器とか
  - 人間による生成でも、悪性度(目的)によって贋作とかパクリとかに
  - このあたりで、オリジナルのクリエイターと生成器作成側での訴訟が多い印象

[1] https://pc.watch.impress.co.jp/docs/news/1499306.html

モデルからの出力における倫理(2/2)

- 教育課程における悪用問題
  - 多くの大学で従来のレポートの(素案)作成への利用を警戒
    - 本人の学習にならないのは自業自得だが、成績評価結果が就職活動や奨学金など他で利用されるので悪用は公平さに問題を起こす
    - 「せっかくなので、それを活用することを前提とした課題にしよう」になる方向?
  - 東北大の教職員向け話の他大学の取り組みのリンク集が便利
    - 教職員向け https://olg.cds.tohoku.ac.jp/forstaff/ai-tools
    - 学生向け https://olg.cds.tohoku.ac.jp/forstudents/ai-tools
- 頭の悪い人による出力の盲信
  - できることできないこと利点欠点を全く理解してない情報発信が山程見られる
  - その情報発信をさらに組織の上層部が盲信するとさらに面倒に
  - まあ、AI関係に限らないが(ブロックチェーン系とか)

AIと倫理の現状

- XAI(eXplainable AI)等で出力結果の保証をする試みはある
  - 「どういう根拠(学習した内容など)から結果を導き出したか」などを結果とともに示す
  - 現状では人間側がXAI出力を見て判断しているが自動化は進むはず
  - (個人的には、SHAPとAttentionの派生物を利用した研究をよく見かける印象)
- 生成系はなんだかんだ言って、分かっている人が素案を作成するコストを減らすには便利
  - 「失礼の無い英語での通知文」とか
- ちょうど現在、ものすごくホットで訴訟とか議論が盛り上がっている分野なので、おっかけると楽しい