情報セキュリティと情報倫理に関連する法律

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
基盤ネットワーク研究グループ
嶋田 創

概要

- 法律に関するTips
- 日本国憲法
- 情報セキュリティに強く関連した法
- 情報セキュリティに限るものではないがある程度関連する法
- その他や国際的な法について少し

法律に関するTips

- 優先順位: 憲法 > 法律 > 政令 > 省令など > 企業の約款
  - よく企業が法律を無視した約款を作ってしまうことがあるが、当然、無効となる
- 同じ優先レベルで内容がぶつかることもある
  - 「侵害対象の深刻度」などで判断
- 法律(法令)を見たければe-Govが便利
  - http://www.e-gov.go.jp/ (検索キー e-Gov)
  - 重要なことは前の方にまとまっていることが多いので、前の方だけ読んでみるのもあり
  - 日本法令外国語訳データベースもある

日本国憲法(1/7)

基本的人権に関連して情報倫理が設定されることは多い(プライバシーなど)

- 国民は、すべての基本的人権の享有を妨げられない。この憲法が国民に保障する基本的人権は、侵すことのできない永久の権利として、現在及び将来の国民に与へられる。(第11条)
- 生命、自由及び幸福追求に対する国民の権利については、公共の福祉に反しない限り、立法その他の国政の上で、最大の尊重を必要とする。(第13条)
- 法の下に平等であつて、人種、信条、性別、社会的身分又は門地により、政治的、経済的又は社会的関係において、差別されない。(第14条)

日本国憲法(2/7)

基本的人権関連

- すべて国民は、健康で文化的な最低限度の生活を営む権利を有する。(第25条)
  - 最近では「インターネットに接続する権利」をこれに入れる流れもある
- 財産権は、これを侵してはならない。(第29条)
  - 著作権は財産権に属する

日本国憲法(3/7)

セキュリティに関する検査(≒検閲)で「自由」に関する条文に抵触することは多々起こりうる

- 思想及び良心の自由は、これを侵してはならない。(第19条)
- 信教の自由は、何人に対してもこれを保障する。(第20条)
- 集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。(第21条)
  - 特に表現の自由は規制(人権に関する)とぶつかることが多い
- 学問の自由は、これを保障する。(第23条)

ただし、「公共の福祉に反しない限り」が大前提

日本国憲法(4/7)

犯罪行為もちゃんと法に則って捜査を進めないといけない

- 法律の定める手続によらなければ、その生命若しくは自由を奪はれ、又はその他の刑罰を科せられない。(第31条)
- 現行犯として逮捕される場合を除いては、権限を有する司法官憲が発し、且つ理由となつてゐる犯罪を明示する令状によらなければ、逮捕されない。(第33条)
- 理由を直ちに告げられ、且つ、直ちに弁護人に依頼する権利を与へられなければ、抑留又は拘禁されない。(第34条)
- 何人も、その住居、書類及び所持品について、侵入、捜索及び押収を受けることのない権利は、第33条の場合を除いては、正当な理由に基いて発せられ、且つ捜索する場所及び押収する物を明示する令状がなければ、侵されない。(第35条)

日本国憲法(5/7)

犯罪処理関連

- 何人も、損害の救済、公務員の罷免、法律、命令又は規則の制定、廃止又は改正その他の事項に関し、平穏に請願する権利を有し、何人も、かかる請願をしたためにいかなる差別待遇も受けない。(第16条)
- 何人も、いかなる奴隷的拘束も受けない。又、犯罪に因る処罰の場合を除いては、その意に反する苦役に服させられない。(第18条)
- 何人も、実行の時に適法であつた行為又は既に無罪とされた行為については、刑事上の責任を問はれない。又、同一の犯罪について、重ねて刑事上の責任を問はれない。(第39条)

日本国憲法(6/7)

法律の制定や判断

- 法律案は、この憲法に特別の定のある場合を除いては、両議院で可決したとき法律となる。(第59条)
- 内閣は、他の一般行政事務の外、左の事務を行ふ。(第73条)

  六　この憲法及び法律の規定を実施するために、政令を制定すること。
- 最高裁判所は、一切の法律、命令、規則又は処分が憲法に適合するかしないかを決定する権限を有する終審裁判所である。(第81条)

日本国憲法(7/7)

改めて大事なことを再確認

- この憲法が日本国民に保障する基本的人権は、人類の多年にわたる自由獲得の努力の成果であつて、これらの権利は、過去幾多の試錬に堪へ、現在及び将来の国民に対し、侵すことのできない永久の権利として信託されたものである。(第97条)
- この憲法は、国の最高法規であつて、その条規に反する法律、命令、詔勅及び国務に関するその他の行為の全部又は一部は、その効力を有しない。(第98条)

  ２　日本国が締結した条約及び確立された国際法規は、これを誠実に遵守することを必要とする。
- 天皇又は摂政及び国務大臣、国会議員、裁判官その他の公務員は、この憲法を尊重し擁護する義務を負ふ。(第99条)

概要

- 法律に関するTips
- 日本国憲法
- 情報セキュリティに強く関連した法
- 情報セキュリティに限るものではないがある程度関連する法
- その他や国際的な法について少し

電気通信事業法(1/2)

大部分の条項は事業者が取るべき手続きが占めている

- 通信の秘密
  - 電気通信事業者の取扱中に係る通信は、検閲してはならない。(第3条)
  - 電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。(第4条)
    - 電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。
- 通信の公平性
  - 電気通信事業者は、電気通信役務の提供について、不当な差別的取扱いをしてはならない。(第6条)

電気通信事業法(2/2)

- 電気通信役務: 電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供することをいう。(第2条3)
  - 電気通信事業: 電気通信役務を他人の需要に応ずるために提供する事業(第2条4)
  - このような事業を行う場合、電気通信事業者として届け出が必要
  - 本業に付随するサービスや対価を得ないサービスとかでは電気通信事業の届け出は不要(フリーWiFi、ホテルの宿泊者向けネット接続)
- 昔からよくある「嘘を言って契約させたりする」のは禁止行為と明示されている
  - 電気通信役務の提供に関する契約に関する事項であつて、利用者の判断に影響を及ぼすこととなる重要なものにつき、故意に事実を告げず、又は不実のことを告げる行為(第27条の2の1)

通信の秘密に関する話題(1/2)

- (電気)通信事業は通信の秘密を侵害しないと事業を行えない
  - 「誰から誰に通信をしたか」も通信の秘密になる
    - 「誰々から誰々に頻繁に通信がある」ことをおおっぴらにされたら困る事例は多いはず
  - 「事業の実施に必要となる」範囲で通信の秘密の侵害は許されるという考え方で運用
    - 当然、知った秘密は口外してはならない
- spam/マルウェアメールのメールサーバにおけるフィルタリング
  - 当然、通信の秘密の侵害になる →同意を取って実施
  - 不特定多数に送られるspamについては、メールサーバへのDoS攻撃として扱う考え方もあり

通信の秘密に関する話題(2/2)

- 違法コンテンツに対する通信遮断の是非
  - 通信の秘密よりもその違法コンテンツの遮断が重要かどうか
  - 児童ポルノの遮断: 被害者児童の人権 >> 通信の秘密
    - 被害者児童の「忘れられる権利」などの方がはるかに大きいという判断がされた(そこそこ長きの議論の末)
  - 著作権無視のコンテンツ配信(係争中): 財産権 vs 通信の秘密
    - 個人的には、「財産権をもとに通信遮断を主張している団体は、副作用による損害(コスト増も含め)をちゃんと補償する気がある?」と言いたい
      - 個人的には、過去の音楽関連話を見ると、ろくに補償していない印象が強い
- 「通信の最適化」と称した、通信中の画像を劣化させる行為
  - これ以上もないレベルでのアウトな行為(格安SIM系で再燃した)
  - なんで総務省は動かないんでしょうねぇ…
    - 利用者の利益又は公共の利益を確保するために必要な限度において、業務の方法の改善その他の措置をとるべきことを命ずることができる(第29条)

通信の公平性に関する話題

- 「ネットワークの中立性」とも言う
- 「特定の事業者などの通信のみ優先的な取扱をする」のを禁止する
  - 現状では、「そういう優先扱いがあるサービスです」と明示してあればOKな感じ
    - 優先される所がお金を負担したり
- 格安SIM系で勝手に一部のプロトコルに帯域制限をかけているらしい事例が本当なら…
  - 自分に都合が悪いプロトコルに帯域制限をかけている?
  - 「自分に都合の良いプロトコル(評判に関連)」を良く見せるためだったら、景品表示法第5条1の優良誤認にも関わる?

spam関連

特定電子メールの送信の適正化等に関する法律

- 一応、「同意が無い限りspamは送ってはならない(オプトイン方式)」だが…(第3条)
  - 自己の電子メールアドレスを送信者又は送信委託者に対し通知した者には送ってOK
  - 広告又は宣伝に係る営業を営む者と取引関係にある者には送ってOK
  - 自己の電子メールアドレスを公表している団体又は個人（個人にあっては、営業を営む者に限る。）には送ってOK

→かなりザル(特に仕事をしている人にとって)

  - 展示会やら何やらで電子メール登録が必要になる所とかだと…
- 罰金も最大で法人3000万、個人100万とあまり高くない

(通称)プロバイダ責任制限法 (現在は情報流通プラットホーム対処法)

- 正式名称: 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
- 特定電気通信役務提供者は、提供した物が犯罪に使われた場合において、特定の手続きに従えば損害賠償責任を免除される
  - 特定電気通信役務提供者には、ウェブサービス作成者なども含む
  - 特定の手続き: 大元の情報の開示、適切な情報の遮断、など
    - ただし、無判断で開示や遮断をするわけではない(犯罪を行う側からの請求もありうる)
- 条件が揃えば、以下の責任を負う必要がなくなる
  - (犯罪者による)提供サービス経由の情報発信による、他人の権利侵害の損害
  - (犯罪者による)提供サービス経由の情報発信を防止したことによる、情報発信者の損害

プロバイダ責任制限法の改正は続く(1/2)

- SNSを含めさらに情報発信の安易化に伴って改正は多い
  - 詐欺(詐欺フェイクニュースを含む)や誹謗/中傷への対策
    - 日本国の景気や先行きが微妙になってきているから、この手の物が増えてきている?
    - 罰金が高額かつルールが厳格なEUに比べて日本国は罰金等が手ぬるいから、大手情報サービス側が対応を後回しにしていないか?
- 2022年改正
  - 発信者情報の開示を一つの手続で行うことを可能に
    - 従来は、WebサービスにIPアドレスの開示請求をかけた後に、ISPにIPアドレス(その日時の割り当て)に対する利用者開示請求が必要だった
    - 新たな裁判手続(非訴訟手続)として整備
  - 請求できる発信者情報の強化
    - 問題の投稿を行った時のIPアドレスだけでなく、投稿したユーザ名のログイン時のIPアドレスも開示OK

プロバイダ責任制限法の改正は続く(2/2)

- 2025/4/1から「情報流通プラットホーム対処法」へ
  - SNSのプロバイダの対応を迅速化
    - 削除を申請する窓口を設置すること
    - 申請から一定の期間内に削除の可否や対応結果を示すこと
    - 削除等の基準を公表すること

- まだまだこれからも改正は続くのでは?
  - 個人的にはAIサービスプロバイダ関係でありそう(参考: EUのAI act)

不正アクセス行為の禁止等に関する法律

- 何らかのユーザ識別のユーザごとのアクセス制御(パスワード、生体認証、など)がある計算機システムを対象(第2条)
- 「アクセス制御で制限されている機能を利用可能とする行為」自体を不正アクセスとしている(第2条)
  - 特権昇格攻撃などをカバー
- 認証情報を窃取すること自体も違法(第4条)
- どこかで窃取した認証情報を提供するのも違法(第5条)
  - 正当な理由で一時的に利用することはあるが(第5条)、それを不正利用を目的として保管したら違法(第6条)
- 管理者になりすましてphishingするなども違法(第7条)
- ただし、あまりにもザルな認証(例: パスワードが"password")だと、司法の場で「アクセス制御されている状態に非ず」と判断されることも

個人情報保護法(1/3)

正式名称: 個人情報の保護に関する法律

- 個人情報を取り扱うに当たっては、その利用目的をできる限り特定しなければならない。(第15条)
  - 前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。(第16条)
  - 偽りその他不正の手段により個人情報を取得してはならない。(第17条)
  - あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。(第18条)
- 利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。(第19条)
- 個人データの安全管理のために必要かつ適切な措置を講じなければならない。(第20条)

個人情報保護法(2/3)

- 従業者/委託先の監督(第21条、第22条)
- 次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。(第23条)
- あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。(第24条)
  - 個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるものを除く。
- 第3者への提供、第3者から提供を受ける場合(第25条、第26条)

個人情報保護法(3/3)

- 保有個人データに関し本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置くべきこと(第27条)
- 保有個人データの開示請求(第28条)
- 保有個人データの訂正要求(第29条)
- 違反時の利用停止と消去要求(第30条)
- 匿名加工(第36条から第39条)

ただ、個人的には附則による但し書きが多くてちょっと微妙

2020年の個人情報保護法の改正

- 2020/6/5成立、2022/4施行
- 「違法な行為を助長するための個人情報の利用は禁止」という項目が追加された
  - 例えば、職業安定法違反を助長させるための個人情報の利用とか
- 匿名化したデータ(仮名加工情報)は外部提供はOKに
  - 個人情報保護委員会規則で定める基準に従って個人情報を加工
- 「個人関連情報」という概念の追加と規制
  - 「個人情報ではないが、個人を一意に特定できる情報」の利用を規制
    - Cookie等の個人を追跡するため手法と結果のデータベース化を規制
  - ただし、第三者への提供において(おそらく)
- 個人情報利用停止請求も入ったが、除外条件があったり「無償で請求できる」を明記されていない点が残念
- 罰金の上限も引き上げられたがGDPRに比べて手ぬるい

次の個人情報保護法改正も進行中[1]

- 動向の変化が激しい、短いスパンで見直しは行われている
  - 特に(いわゆる)AIの開発における学習データとか
- 個人的には、「統計等の作成を行う第三者に個人情報を提供する場合等について本人の同意を不要とする等の措置」はいろいろ悪用できそう
  - 統計作成等であると整理できるAI開発等も含まれる
  - わざと移転攻撃で元情報を現像できる形で開発した上で、(特定の所に攻撃方法を教えた上で、)一定期間後に脆弱性修正とか
- 医療AIの開発/適合に向けて、単独の病院でも学術研究機関等に含めて大学病院と同等の利活用を可能に
- 個人的には、よりGDPR参考に制限を入れて欲しかった
  - 相変わらず罰金しょぼく海外超大手級なら罰金払って破った方が得
  - 顔特徴データの扱いについても手ぬるい感じ

[1] https://www.ppc.go.jp/news/press/2026/260407/

概要

- 法律に関するTips
- 日本国憲法
- 情報セキュリティに強く関連した法
- 情報セキュリティに限るものではないがある程度関連する法
- その他や国際的な法について少し

ストーカー関連

- ストーカー行為等の規制等に関する法律
  - 不快な物を送りつける、不快な言動を送りつける、なども対象
  - 電子メールやSNS(コメントやreplyなども含む)も対象になっている
  - ストーカー行為をするおそれがある者であることを知りながら、その者に情報提供することを禁止(第7条)
  - 2021/5/18に「GPSなどの悪用(直接/間接的な位置情報の推定など)」をカバーする改正案が成立(2021/8施行)
- リベンジポルノ被害防止法(通称)
  - プライベートとして撮影された性的画像記録を不特定又は多数の者に提供した場合
  - 正式名称: 私事性的画像記録の提供等による被害の防止に関する法律

消費者保護

- 消費者契約法
  - 消費者契約の基本(詐欺的な契約手続きの禁止、無効な契約)
- 特定商取引に関する法律
  - クーリングオフ、不実告知、特定継続的役務提供(エステや語学の会員権など)規制、ねずみ講亜種、などの中途解約の話
  - かなり積極的に改正されている
- 不当景品類及び不当表示防止法
  - 消費者を誤解させて製品を高く評価させることを禁止
  - 通信サービスだとよくこれに抵触しているのを見かける
- 消費者安全法
  - 製品に関する事故から「虚偽の又は誇大な広告その他の消費者の利益を不当に害するもの」まで広くカバー

刑法(1/3)

犯罪に関して

- 未遂罪(第43条、第44条)
- 教唆(第61条)
- 幇助(第62条)

- 酌量減軽(第66条、第67条)
- 再犯、再犯加重(第56条、第57条)

刑法(2/3)

情報関係で関連の多い犯罪

- 公文書/私文書偽造等(第155条から第161条)
- 電磁的記録の不正(第161条の2、第168条の2,3)
- 支払用カード電磁的記録不正作出等(第163条の2,3,4)
- わいせつ物頒布等(第175条)
- 賭博関連(第185条から第187条)
- 脅迫(第222条)、強要(第223条)
- 名誉毀損(第230条)、侮辱(第231条)
- 偽計業務妨害(第233条)、威力業務妨害(第234条)、電子計算機損壊等業務妨害(第234条の2)
- 詐欺(第246条、第248条)、恐喝(第249条)

刑法(3/3)

関わる可能性があるもの

- 証拠隠滅(第104条)
  - インシデント対応ミスなどでうっかり証拠を破壊してしまった場合?
- 虚偽告訴の罪(第172条、第173条)
  - どちらかというと被害者になる可能性という視点で

概要

- 法律に関するTips
- 日本国憲法
- 情報セキュリティに強く関連した法
- 情報セキュリティに限るものではないがある程度関連する法
- その他や国際的な法について少し

国際(サイバー)犯罪にはどう対応する?

(数を出せそうにないから)あまり期待はできないけど、大きな国際サイバー犯罪の時にはお世話になるかもしれない

- 国際指名手配
  - 国際刑事警察機構(ICPO)を介する手法
- 犯罪人引渡し条約
  - 日本はアメリカと韓国としか条約を締結していない

…が、そもそも(特別に対応の条約が無い限り)国際犯罪の追跡が非常に弱い

デジタルミレニアム著作権法(DMCA: Digital Millennium Copyright Act)

- 著作者を保護することを目的とした強力すぎる法律
  - アメリカの法律だが、アメリカ発のサービスはこの影響下にある
- サービスプロバイダ側に著作権侵害物を早急に削除させる
  - 発信者への調査なしに削除が許される(被害の補償の必要無し)
- 強力なので悪用する事例が多い
  - 人のコンテンツを自分の物として登録してオリジナルを削除させる(個人レベルでの作曲者や絵かきがやられている)
  - 自分の会社に関する悪評に対し、「正当な引用されている部分」を著作権侵害として、記事全体などを削除させる
    - 「人のコンテンツを自分の物として登録」と複合した事例もあり
- 個人的に、悪用者への大ペナルティや誤削除の被害補償をとっとと設けるべきだと思っている

サイバーセキュリティ基本法

- (実は、個人や企業はあまり関係ないことが多い)
- 日本のサイバーセキュリティに関する施策に関して、戦略などの方向性を示す法律
  - いずれ、民間にも降りてくる可能性はあるので、動向を見ておく分には問題ない
  - でも、動向を見るならば米国NISTなどの法を見たほうが…
- 2018年の「サイバーセキュリティ協議会」関係の話は民間にも早く降りてくるかも
  - 「(業種を超えて)集まってお互いに情報公開/情報交換して、サイバーセキュリティ向上しろ」というような形で
  - 現状で国の関係行政機関, 地方公共団体, 重要インフラ事業者, サイバー関連事業者, 大学・教育研究機関が参加可能

デジタル行政に向けての法律

- デジタル手続き法(通称、デジタルファースト法律とも)
  - 2019/5/24成立、2019/12/16施行
  - 行政手続きは基本的にオンラインでできるようになる
    - 「お役所関係は書類書きばっかりで大変」が解消される予定
  - もちろん、オンライン化にあたってセキュリティは担保される…と思う
    - 今でも、第3者が勝手に住民票を移動させたり、勝手に印鑑登録して契約したりと、「窓口だから安全」なんてことは無いが
  - 誤交付とか過去の印鑑証明の発行とかの問題で絶賛逆風中@2023
    - じゃあ、デジタル化する前は問題発生は0だったかというと? (例: 戸籍で使われている特殊異体文字の多くは昔の役所内の手書きミスな噂)
- この後、デジタル改革関連法へ

デジタル改革関連法(1/2)

2021/5に5つの法律(+デジタル庁設置法)が成立

- デジタル社会形成基本法
  - デジタル社会の形成に関し、基本理念、基本方針、国や事業者の責務、重点計画などを規定
- デジタル社会形成整備法(デジタル社会の形成を図るための関係法律の整備に関する法案)
  - 今までの法律が障害になるところを改正を含めて整備
  - 例: 個人情報関係の3法律を個人情報保護法にまとめる
  - 例: 押印・書面交付等を求める手続きを定める48法律を改正
  - マイナンバーカードの利便性向上やマイナンバー(個人番号)活用も
    - スマホ用にマイナンバーカードと結びつけた電子証明書を発行可能に
    - 国家資格とマイナンバーの結びつけて確認を容易に(要マイナンバー法改正)

デジタル改革関連法(2/2)

- 公金受取口座登録法(公的給付の支給などの迅速かつ…)
  - 希望者に対し、マイナンバー(個人番号)と口座を結びつけて児童手当や給付金の迅速な支給を可能とする
  - マイナンバー(個人番号)の社会保障や災害対策に関連
- 預貯金口座管理法(預金者の医師に基づく個人番号の…)
  - 個人番号と複数の口座をひもづけることを可能とする
  - 「本人の同意を前提」としている
  - 相続や災害時の手続きの負担削減が目的
- 自治体システム標準化法
  - 自治体の基幹系情報システムの基準を作成
- デジタル庁設置法案
  - デジタル社会の形成に関する司令塔を作る
  - 「縦割り打破」が掲げられている

その他

- EU一般データ保護規則(GDPR) →情報倫理の回
- EUのAI法(AI Act) →情報倫理の回
- 著作物の正当な利用 →情報倫理の回
- マイナンバー関係 →情報倫理の回
- ネット上の選挙運動 →情報リテラシの回
  - その他、リテラシ系の法律が情報リテラシの回にいくつか出てくる