情報セキュリティに関連する法律

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
嶋田 創

概要

- 法律の概要
- 日本国憲法とサイバーセキュリティ
- サイバー犯罪と法律
  - 刑法
  - 不正アクセス禁止法
- サイバーセキュリティ強化に関する法律
- ネットワークセキュリティと法律
- プライバシーと法律

法律の概要

- 優先順位: 憲法 > 法律 > 政令 > 省令など > (企業などの組織の約款)
  - 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(http://www.e-gov.go.jp/)が便利
  - e-Gov法令検索: http://law.e-gov.go.jp/
  - 重要なことは法律(法令)の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)

サイバーセキュリティと日本国憲法

- 他の西欧諸国と比べて、公共の福祉よりも通信の秘密が強く運用されている印象
  - 明確な違法性(阻却理由)がない限り、通信の秘密が守られる
  - サイバーセキュリティに関する通信の内容に応じた制御は、規約への同意を行った上で行うことが多い
    - ただし、悪質な規約を強要した上で利用者からの訴訟された場合、上位の憲法が強く優先されることになる(…が世の中の動向で変わるか?)
  - 過去に、一部の理解していないサービス事業者が悪質な憲法違反(電気通信事業法の観点からも)をやっていた事例も
    - 例: 格安携帯回線業者(MVNO)がHTTP通信を検閲して画像データを勝手に高圧縮データに置き換えてMNOの支払いを節約
    - 個人的には、サービス事業者が非常に悪質な場合のサービス事業者側が逮捕/訴追される事例はもっと日本ではもっと増えるべきかと思う
      - あと、犯罪収益を被害者救済に回させる法律はさっさと作れ

概要

- 法律の概要
- 日本国憲法とサイバーセキュリティ
- サイバー犯罪と法律
  - 刑法
  - 不正アクセス禁止法
- サイバーセキュリティ強化に関する法律
- ネットワークセキュリティと法律
- プライバシーと法律

刑法の概要(1/2)

- 第1編「総則」と第2編「罪」から成る
- 刑法第2編「罪」は罪の種類によって章分けされている

  例:
  - 第16章 通貨偽造の罪
  - 第26章 殺人の罪
  - 第27章 傷害の罪
- 後から追加される条文があると、対応する章の中に入れるために「XX条の2」のような条ができる
  - 例: 168条の2(不正指令電磁的記録作成等)、168条の3(不正指令電磁的記録取得等)
  - 168条と169条の間にある、168条(印章偽造の未遂)や169条(偽証)と同じ粒度の条文
  - というか、章も「の2」ができたりする

刑法の概要(2/2)

- 第1編「総則」において特に関係するもの
  - 7条の2(定義)
    - この法律において「電磁的記録」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。
    - 昭和62年(1987)に追加
- 関連する大きな改正
  - 昭和62年(1987): 電磁的記録や電子計算機関係の条文の追加
  - 平成13年(2001): 支払い用カード(クレジットカード)の電磁的記録の不正関係の追加
  - 平成23年(2011): 不正指令電磁的記録(マルウェア)関係の追加、未遂の強化

犯罪および刑法の構成要素

- 犯罪や刑法は以下の構成要素で定義されており、刑法の条文もそれに対応している →考えて読むと分かりやすい
  - 正当な理由の不存在
  - 目的もしくは行為の主体
    - 目的犯: (故意による)行為に目的が付随して犯罪と成るもの
    - 行為犯: (故意による)行為を行うこと自体が犯罪
  - 行為の客体
  - 具体的な行為

  個々の項目の対象が複数あることも

刑法犯の成立要件

- 「違法性阻却事由」に値しないこと
  - 正当行為(35条)
    - 正当業務行為は通信に常につきまとう(通信先を知らないと通信業務を行えないが、通信先は通信の秘密において保護される内容)
  - 正当防衛(36条1項)
  - 緊急避難(37条1項)
    - より深刻度の高い権利(例: 人権)の侵害を防止するため、深刻度の低い権利(例: 財産権)の侵害の行為を許容する
  - たまにこれらがせめぎ合う

刑法における情報セキュリティ関係

- 不正指令電磁的記録関係電磁的記録不正作出関係(163条の2と3)
- 電磁的記録毀棄関係(161条の2)
- 電子計算機損壊等業務妨害関係(234条)
- 電子計算機使用詐欺関係(246条の2)
- 支払い用カード電磁的記録不正作出関係(163条の2～163条の5)

サイバー犯罪には限らないが関連しやすいもの

- わいせつ物頒布等(175条)
  - わいせつな文書、図画、電磁的記録に係る記録媒体その他の物を頒布し、又は公然と陳列した(1項)
  - 有償で頒布する目的で、前項の物を所持し、又は同項の電磁的記録を保管した(2項)
- 公然わいせつ(174条)
  - 公然とわいせつな行為をした(項番無し)
  - Youtuberのような生放送だとこちらになる可能性

古くからこちらの方面の犯罪は技術の進歩を積極的に利用する傾向にある

- 賭博関連(第185条から第187条)

これ刑法じゃないの？

独立した法律になっているもの

- 不正アクセス行為の禁止等に関する法律
- 個人情報の保護に関する法律

独立していた方がフットワークが軽くなるかも

サイバー犯罪に関連しやすいが刑法でないもの

- 商標法
- 著作権法
- 麻薬及び向精神薬取締法
- 医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律(薬事法)
- ストーカー行為等の規制等に関する法律
- 児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律

不正指令電磁的記録関係

- 第19章 不正指令電磁的記録に関する罪
  - 平成23年(2011)に追加
    - マルウェアの被害が増えてきたことが背景
  - 独立した19章になっている
  - 168条の2 不正指令電磁的記録作成等
  - 168条の3 不正指令電磁的記録取得等

168条の2 不正指令電磁的記録作成等

- 不正指令電磁的記録及び提供
  - 正当な理由がないのに、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(1項)
  - ここで「指令電磁的記録」はプログラムと考えれば良い
  - 「不正指令」の部分の解釈でいろいろと分かれる
- 不正指令電磁的記録供用
  - 正当な理由がないのに、前項(不正指令電磁的記録及び提供)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(2項)
  - もらったものを動かしてもだめ
- 不正指令電磁的記録供用未遂
  - 前項(不正指令電磁的記録供用)の罪の未遂は、罰する。(3項)

168条の3 不正指令電磁的記録取得等の内訳

- 不正指令電磁的記録取得
  - 正当な理由がないのに、前条第一項(不正指令電磁的記録及び提供)の目的で、同項(不正指令電磁的記録及び提供)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(1項)
  - アンチウィルスソフト開発とか正当な理由がない限り所持するのを禁止
    - インターネットサービスプロバイダの職員が(業務に関係して)マルウェアを持っていた時にこれで逮捕案件があって物議を醸した

電磁的記録不正作出関係

- 電磁的記録不正作出及び供用
  - 161条の2 電磁的記録不正作出及び供用
  - 昭和62年(1987)に追加
    - 文書の電子化や電子的な決済(ATMによる振込)が増えてきたことが背景
  - 第17章 文書偽造の罪を構成する
  - なお、無印の刑法161条は文書偽造の罪における偽私文書等行使

161条の2 電磁的記録不正作出及び供用の内訳

- 私電磁的記録不正作出
  - 人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を不正に作った(1項)
  - 偽の電子的文書を作ってはいけません
- 公電磁的記録不正作出
  - 前項(私電磁的記録不正作出)の罪が公務所又は公務員により作られるべき電磁的記録に係るとき(2項)
- 不正作出電磁的記録供用
  - 不正に作られた権利、義務又は事実証明に関する電磁的記録を、第1項(私電磁的記録不正作出)の目的で、人の事務処理の用に供した(3項)

電磁的記録毀棄関係

- 第40章 毀棄及び隠匿の罪を構成
- 公用電磁的記録毀棄
  - 公務所の用に供する文書又は電磁的記録を毀棄した(258条)
- 私用電磁的記録毀棄
  - 権利又は義務に関する他人の文書又は電磁的記録を毀棄した(259条)

電子計算機損壊等業務妨害関係

- 第35章 信用及び業務に対する罪を構成
- 電子計算機損壊等業務妨害
  - 人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した(234条2)
- 威力業務妨害(234条)と重複するところも多い
  - 威力を用いて人の業務を妨害した者も、前条(信用毀損及び業務妨害)の例による。(234条)

電子計算機使用詐欺関係

- 第37章 詐欺及び恐喝の罪を構成
- 電子計算機使用詐欺
  - 前条(詐欺)に規定するもののほか、人の事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた(246条の2)
- 246条は(一般的な)詐欺の条項

支払用カード電磁的記録不正作出関係(1/2)

- 第18章の2として章も追加
  - 平成13年(2001)に追加
  - オンラインでのクレジットカード決済などが増えてきたことを受けて
- 支払い用カード電磁的記録不正作出等(163条の2)
  - 人の財産上の事務処理を誤らせる目的で、その事務処理の用に供する電磁的記録であって、クレジットカードその他の代金又は料金の支払用のカードを構成するものを不正に作った(1項)
  - 不正に作られた前項の電磁的記録(支払い用カード)を、同項の目的で、人の財産上の事務処理の用に供した(2項)
  - 不正に作られた第1項の電磁的記録(支払い用カード)をその構成部分とするカードを、同項の目的で、譲り渡し、貸し渡し、又は輸入した(3項)

支払用カード電磁的記録不正作出関係(2/2)

- 不正電磁的記録カード所持
  - 前条(支払い用カード電磁的記録不正作出等)第1項の目的で、同条第3項のカードを所持した(163条の3)
- 支払用カード電磁的記録不正作出準備(163条の4)
  - 第163条の2(支払い用カード電磁的記録不正作出等)第1項の犯罪行為の用に供する目的で、同項の電磁的記録の情報を取得した(1項)
  - 不正に取得された第163条の2(支払い用カード電磁的記録不正作出等)第1項の電磁的記録の情報を、前項の目的で保管した(2項)
  - 第1項の目的で、器械又は原料を準備した(3項)
- 第163条の2(支払い用カード電磁的記録不正作出等)及び前条(支払用カード電磁的記録不正作出準備)第1項の罪の未遂は罰する(163条の5)

不正アクセス行為の禁止等に関する法律

- 平成11年(1999)に新設
- 平成24年(2012)に大幅な改正
  - パスワード窃取関係の処罰を強化

不正アクセス行為の禁止等に関する法律における定義(第2条)(1/2)

- この法律において「アクセス管理者」とは、電気通信回線に接続している電子計算機の利用につき当該特定電子計算機の動作を管理する者をいう。
- この法律において「識別符号」とは、特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者及び当該アクセス管理者に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものをいう。
  - 当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号
  - 当該利用権者等の身体の全部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法により作成される符号
  - 当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号

不正アクセス行為の禁止等に関する法律における定義(第2条)(2/2)

- この法律において「アクセス制御機能」とは、特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号であることを確認して、当該特定利用の制限の全部又は一部を解除するものをいう。

- 要は、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
- 「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

不正アクセス行為の禁止等に関する法律における不正アクセスの定義(第2条)

- この法律において「不正アクセス行為」とは、次の各号のいずれかに該当する行為をいう。
  - アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為
  - アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為
  - 電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

不正アクセス行為の禁止等に関する法律の内訳(1/3)

- 他人の識別符号を不正に取得する行為の禁止
  - 何人も、不正アクセス行為の用に供する目的で、アクセス制御機能に係る他人の識別符号を取得してはならない。(4条)
  - 要は、認証情報を窃取すること自体も違法
- 不正アクセス行為を助長する行為の禁止
  - 何人も、業務その他正当な理由による場合を除いては、アクセス制御機能に係る他人の識別符号を、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。(5条)
  - 要は、どこかで窃取した認証情報を提供するのも違法(第5条)
- 他人の識別符号を不正に保管する行為の禁止
  - 何人も、不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号を保管してはならない。(6条)
  - 正当な理由で一時的に利用することはあるが(5条)、それを不正利用を目的として保管したら違法(6条)

不正アクセス行為の禁止等に関する法律の内訳(2/3)

- 識別符号の入力を不正に要求する行為の禁止
  - 何人も、アクセス制御機能を特定電子計算機に付加したアクセス管理者になりすまし、その他当該アクセス管理者であると誤認させて、次に掲げる行為をしてはならない。ただし、当該アクセス管理者の承諾を得てする場合は、この限りでない。(7条)
    - 該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電気通信回線に接続して行う自動公衆送信を利用して公衆が閲覧することができる状態に置く行為(1項)
    - 当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電子メールにより当該利用権者に送信する行為(2項)
  - 要は、phishing対策
    - 管理者になりすましてphishingするなども違法(第7条)

不正アクセス行為の禁止等に関する法律の内訳(3/3)

- アクセス管理者による防御措置
  - アクセス制御機能を特定電子計算機に付加したアクセス管理者は、当該アクセス制御機能に係る識別符号又はこれを当該アクセス制御機能により確認するために用いる符号の適正な管理に努めるとともに、常に当該アクセス制御機能の有効性を検証し、必要があると認めるときは速やかにその機能の高度化その他当該特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとする。(8条)
  - 要は、サイバーノーガード戦法は許しません
  - 実際に、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

刑事訴訟法

- 刑事訴訟に持っていく時の手続きや原則が書かれている

  例:
  - 捜査に関する原則
  - 公訴・公判手続に関する原則
  - 事実認定・証拠に関する原則
- 例のごとく、コンピュータ関連の話は後から追加されていることが多い
  - 「第〇〇の2条」など

差し押さえるべき物が電磁的記録に係る記録媒体であるとき(110条の2)

- 差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状の執行をする者は、その差押えに代えて次に掲げる処分をすることができる。公判廷で差押えをする場合も、同様である。
  - 差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写し、印刷し、又は移転した上、当該他の記録媒体を差し押さえること。(1項)
  - 差押えを受ける者に差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写させ、印刷させ、又は移転させた上、当該他の記録媒体を差し押さえること。(2項)

差し押さえるべき物が電子計算機であるとき(218条2項)

218条全体は差し押さえと身体捜査に関する手続き

- 差し押さえるべき物が電子計算機であるときは、当該電子計算機に電気通信回線で接続している記録媒体であつて、当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は当該他の記録媒体を差し押さえることができる。(218条2項)

電磁的記録の保全要請(197条)(1/2)

- 1項と2項は取り調べや報告の求めについて
- 検察官、検察事務官又は司法警察員は、差押え又は記録命令付差押えをするため必要があるときは、電気通信を行うための設備を他人の通信の用に供する事業を営む者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対し、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、三十日を超えない期間を定めて、これを消去しないよう、書面で求めることができる。この場合において、当該電磁的記録について差押え又は記録命令付差押えをする必要がないと認めるに至つたときは、当該求めを取り消さなければならない。(3項)

電磁的記録の保全要請(197条)(2/2)

- 前項の規定により消去しないよう求める期間については、特に必要があるときは、三十日を超えない範囲内で延長することができる。ただし、消去しないよう求める期間は、通じて六十日を超えることができない。(4項)
- 第二項又は第三項の規定による求めを行う場合において、必要があるときは、みだりにこれらに関する事項を漏らさないよう求めることができる。(5項)

刑事訴訟において関連してくる可能性のある刑法(1/2)

犯罪の構成に関して

- 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)

刑事訴訟において関連してくる可能性のある刑法(2/2)

犯罪の目的に関わるもの

- 脅迫(第222条)、強要(第223条)
- 名誉毀損(第230条)、侮辱(第231条)
- 詐欺(第246条、第248条)、恐喝(第249条)

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

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

概要

- 法律の概要
- 日本国憲法とサイバーセキュリティ
- サイバー犯罪と法律
  - 刑法
  - 不正アクセス禁止法
- サイバーセキュリティ強化に関する法律
- ネットワークセキュリティと法律
- プライバシーと法律

サイバーセキュリティ基本法(1/2)

- 2014年に成立し、2015年施行(もちろんその後に改正あり)
- 2015年の施行時に内閣官房情報セキュリティセンターはが内閣サイバーセキュリティセンター(NISC)に
  - さらに2025年のサイバー対処能力強化法で国家サイバー統括室(NCO: National Cybersecurity Office)へ
- 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
  - この法律の方向性をもとに、実務的な法律が作成される
  - 当初は個人や企業はあまり関係ないことが多かった…が、サイバー攻撃激化に応じた関連法律整備で関係することが増えてきた
  - 欧米の動向を参考に改正されることが多いので、欧米の動向を先に見ておくのが良い
  - 基本的に、ネット上の自由な活動を尊重している(諸外国と比べ)

サイバーセキュリティ基本法(2/2)

- 2018年改正のサイバーセキュリティ協議会創設関係の話は民間にもISACの増加という形で反映が進んだ
  - 「(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
  - 実際に、合同で演習したりとか、取り組み紹介と悩み相談とかやっている所も
- 2025年改正では、情報システム提供者側からの利用者へのセキュリティ支援(情報提供)の努力が入る
  - ソフトウェア提供者側にもSBOMとかでライブラリを含めたセキュリティ管理の努力が入る

重要経済安保情報保護活用法

- 正式名称: 重要経済安保情報の保護及び活用に関する法律(2024年施行)
- 以下をカバー
  - 重要経済安保情報の指定
  - 重要経済安保情報の提供
  - 重要経済安保情報の取扱者の制限
  - 適性評価
- 特に後ろ2つがセキュリティ・クリアランスで話題
  - 最初のやつはどこでもやっている情報の格付け(機密レベル)の延長だし
- SIEM(Security Information and Event Management)の導入推奨など、他の話も含まれています

セキュリティ・クリアランス(1/2)

- 安全保障上重要な情報として指定された情報に対してアクセスする人が情報を漏らす恐れを評価
  - 人間というセキュリティホールを考えてリスク評価(ある意味、ソーシャルエンジニアリング対策)
  - 2014年施行の特定秘密保護法でも規定
- 海外企業等との共同活動で要求されることもある
  - ならず者国家への流出で世界平和が後退する危険性
- 評価対象のリスク: 犯罪や懲戒の履歴、薬物への意識、精神疾患、飲酒の節度、信用状態や経済状態、など
  - 10年おきに再評価しないといけない
- もちろん、情報の格付けも並行して厳格に行われる

(ちょうどハニートラップでやられたCEOの話題がホットですが)

セキュリティ・クリアランス(2/2)

- 扱う人へのリスク教育も
  - SNSを通じて接触してくるかもしれない
  - SNSで場所を特定して物理的に接触してくるかもしれない
  - 適正評価やったことを口外すると接触してくる可能性が高まる
  - 接触時に弱味になるような行動は避ける
- 適正評価は基本的人権の尊重を厳守しながら実施
  - 法に定められている7つの調査事項以外の調査は禁止
  - 適正評価の目的外利用の禁止
  - プライバシーの保護(評価で記入した個人情報は適正評価に関わる職員しか触ってはいけない)
- 皆様の将来で関わる可能性の高いことなので、自分でも深く調べておいた方が良いと思う

サイバー対処能力強化法(1/

- 正式名称: 重要電子計算機に対する不正な行為による被害の防止に関する法律
- 官民連携の強化
  - 基幹インフラ事業者に対する、一定規模の計算機システムの届出義務、および、サイバー攻撃発生時の報告義務
  - 政府による脆弱性情報の提供制度
- 通信情報の利用
  - 海外と関係する通信情報から攻撃兆候を分析し、C2サーバの発見や早期警戒を実施
  - 基幹インフラ事業者との協定に基づく情報提供とその自動分析や関連行政基幹への分析の協力
    - ESNIなどで通信の暗号化は進むため、「どこにどれぐらいの頻度で通信しているか(集中しているか)」のような振る舞いベース分析が主体だろう
    - すでにAkamaiやIIJとかが定期的にレポート出しているけど、その延長?

サイバー対処能力強化法(2/)

- 攻撃元の無害化
  - 警察や自衛隊が一定条件下で攻撃基盤へアクセスし無害化(能動的サイバー防御)
- サイバー対処能力強化法整備法も同時に施行
  - 正式名称: 重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律
  - NISC（内閣サイバーセキュリティセンター）を発展改組した「国家サイバー統括室（NCO）」の設置
  - サイバー対策の司令塔機能強化
- まあ、欧米ではすでにいろいろ行われている点に追いつくための法整備という面も強い[1]
  - セキュリティ・クリアランス同様、法整備されていないと国際協力もできない

[1] https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf

そもそも能動的サイバー防御と言っても、あまり攻撃的になる必要は無い

- 「管理されておらず脆弱性放置で攻撃者の踏み台で使われまくっている」機器を止めるとかもあり
- すでにホワイトハットワームなる「感染した脆弱性のある機器の穴を塞ぐ」マルウェアのカテゴリがある(もち不正アクセス)
  - Linux.Wifatchあたりが初期のホワイトハットワーム[1]
- そもそも、「IoTマルウェアがIoT機器内で主導権を奪い合っている」現状[2]
  - ハニポ上でIoTマルウェアの活動を観測(侵入成功、ダウンロード試行/成功、プロセスの実行、C2通信発生/サーバ接続の段階分け)
  - 某ブロードバンドルータで「同時に3マルウェアが争っていたことも」「他のマルウェアの活動を妨害することも」「45日目に、(侵入直後に?)再起動コマンド入れて先行マルウェア排除しようとした事例も」

[1] https://japan.zdnet.com/article/35071416/
[2] 安井ら, "モノの中の戦い：IoT機器への攻撃の長期観測によるマルウェアの生存競争の調査," コンピュータセキュリティシンポジウム2023, 2023.

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系で再燃中)
  - 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事例
  - 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?
- アメリカでは2018/4に撤廃された

特定電子メールの送信の適正化等に関する法律

- 要はspam規制
- 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(1/2)

- 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)
    - どうも、犯罪者側(ストーカーなど)からの開示手続きに対して精査せずに対応してしまうプロバイダも存在する印象
- オンラインコミュニケーション機能を持たせる場合は対応必須

(通称)プロバイダ責任制限法(2/2)

- 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
- 2022/10に手続き迅速化のための改正が施行される[1]
  - SNS事業者と通信事業者の双方に情報開示請求が必要な場合でも、1つの開示請求でOKに
  - SNSなどは(必要に応じて)ログイン情報の開示請求も可能
- (個人的には、他の犯罪を野放しにする情報サービスも取り締まる形で運用して欲しい)

[1] https://www.soumu.go.jp/main_content/000777232.pdf

個人情報保護法案(1/3)

- 個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）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)

個人情報保護法案(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)

個人情報保護法案(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

個人情報保護法の改正(2020年+)(1/2)

- 大きな改正は 2020/6(2022/4より全面施行)
- 「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)
  - 2023/10に利用者情報の外部送信規制(Cookie規制)が追加
    - 利用者へ、送信内容や目的を明示

個人情報保護法の改正(2020年+)(2/2)

- 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
  - 個人的には、(他の法律も含めて)手ぬるかった点が(2023年頃からの)海外企業の日本への舐めた対応をさらに助長している印象
- 2024/4に個人情報の流出に対して対応の明確化の改正
  - 委託先、個人、不正JavaScript等によるWebスキミング、など
  - 同時に、不正競争防止法も改正(営業機密の保護の強化)
  - (最近、かなり情報持ち出し事件が多かったため?)

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)も対象になった
  - 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)
- 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

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

公職選挙法

- 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た
- ただし、「選挙運動」は事前登録した本人or代理人のみOK
  - NHKがよく起こりそうな事例にOK/NGをまとめている[1]
- 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
- 個人的には、そろそろアップデートされた方が良いのではと感じている
  - 明確に悪意を持って情報操作を行うグループ(国家を含む)への対応はどうするのか…
    - 言論の自由との兼ね合いがあるため、どの自由陣営も苦労中の印象

[1] https://www.nhk.or.jp/senkyo/chisiki/sangiin-kiso/20190529_3/

デジタル手続き法(通称: デジタルファースト法)

- 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
- この法律を補足する形で「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律」を関連法律改正が2021/9に
  - 国家資格に関連するマイナンバー(個人番号)利用
  - マイナンバーカードの利用の推進
  - 押印の廃止の推進

IoTデバイス(+スマートデバイス)のセキュリティに関する法律

- カリフォルニア州のIoTデバイスを重点対象としたセキュリティに関する法律(2018/9成立、2020/1施行)が先行
  - 「製品に共通の初期パスワードを設定することを禁止」を始め、「コストのためにセキュリティ後回し」を禁止する方針が見える
  - 多くのメーカはカリフォルニア州での販売を考えて先行対応
- 総務省も2020/4に省令で同等の規則を実施[1]
  - 既存の電気通信事業法の条文にある端末設備等規則の要件の厳格化

[1] https://www.soumu.go.jp/main_content/000705080.pdf

その他、セキュリティ強化に関する既存法律の改正

- 医療法施行規則の改正(2023/4)[1]
  - サイバーセキュリティ確保の義務の追加
- 景品表示法によるステルスマーケティング規制の強化(2023/10)
- 地方自治法の改正(2024/6)[2]
  - 情報システムの有効利用と事務のデジタル化の加速
  - セキュリティ確保方針とその運用の強化
  - (感染症を含む災害対応の迅速化や強化)
- 重要経済安保情報保護活用法(2024/5)[3]
  - 重要インフラを含む公共サービス提供に関わる情報の取り扱い関係
  - 個人レベルでの適正評価も含まれる

[1] https://www.mhlw.go.jp/content/10800000/001096955.pdf
[2] https://www.soumu.go.jp/main_content/000931798.pdf
[3] https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/gaiyo.pdf

著作権法(1/11)

- 第1条 目的

この法律は、著作物並びに実演、レコード、放送及び有線放送に関し著作者の権利及びこれに隣接する権利を定め、これらの文化的所産の公正な利用に留意しつつ、著作者等の権利の保護を図り、もつて文化の発展に寄与することを目的とする。

- 第2条 用語の定義
  - 一 著作物

    著作物: 思想又は感情を創作的に表現したものであつて、文芸、学術、美術又は音楽の範囲に属するものをいう。
  - 七の二 公衆送信

    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又は有線電気通信の送信を行うことをいう。

著作権法(2/11)

- 第2条 用語の定義(続き)
  - 九の四 自動公衆送信

公衆送信のうち、公衆からの求めに応じ自動的に行うもの（放送又は有線放送に該当するものを除く。）をいう。

  - 九の五 送信可能化

次のいずれかに掲げる行為により自動公衆送信し得るようにすること。

- イ: 公衆の用に供されている電気通信回線に接続している自動公衆送信装置の公衆送信用記録媒体に情報を記録し、情報が記録された記録媒体を当該自動公衆送信装置の公衆送信用記録媒体として加え、若しくは情報が記録された記録媒体を当該自動公衆送信装置の公衆送信用記録媒体に変換し、又は当該自動公衆送信装置に情報を入力すること。
- ロ: その公衆送信用記録媒体に情報が記録され、又は当該自動公衆送信装置に情報が入力されている自動公衆送信装置について、公衆の用に供されている電気通信回線への接続を行うこと。

著作権法(3/11)

- 第2条 用語の定義(続き)
  - 十一 二次的著作物

    著作物を翻訳し、編曲し、若しくは変形し、又は脚色し、映画化し、その他翻案することにより創作した著作物をいう。
  - 二十 技術的保護手段

    電子的方法、磁気的方法その他の人の知覚によつて認識することができない方法により、著作者人格権若しくは著作権、--snip---侵害する行為の防止又は抑止をする手段で、著作物、実演、レコード、放送又は有線放送の利用に際し、これに用いられる機器が特定の反応をする信号を著作物や信号に載せたもの。
  - 二十一 技術的利用制限手段

    電磁的方法により、著作物等の視聴を制限する手段であつて、著作物等の視聴に際し、これに用いられる機器が特定の反応をする信号を著作物、実演、レコード若しくは放送若しくは(以下二十と同様)

著作権法(4/11)

- 第2条 用語の定義(続き)
  - 二十二: 権利管理情報
  - 著作者人格権若しくは著作権又は権利に関する情報であって、著作物などを特定したり著作物の利用条件に関する情報などを電磁的方法により著作物、実演、レコード又は放送若しくは有線放送に係る音若しくは影像とともに記録媒体に記録され、又は送信されるもの。
  - 第7項 この法律において、「上演」、「演奏」又は「口述」には、著作物の上演、演奏又は口述で録音され、又は録画されたものを再生すること及び著作物の上演、演奏又は口述を電気通信設備を用いて伝達することを含む。

著作権法(5/11)

- 第10条 著作物の例示
  - 九 プログラムの著作物
  - 第3項 プログラムの著作物に対するこの法律による保護は、その著作物を作成するために用いるプログラム言語、規約及び解法に及ばない。この場合において、これらの用語の意義は、次の各号に定めるところによる。
    - 一　プログラム言語

    プログラムを表現する手段としての文字その他の記号及びその体系をいう。
    - 二　規約

    特定のプログラムにおける前号のプログラム言語の用法についての特別の約束をいう。
    - 三　解法

    プログラムにおける電子計算機に対する指令の組合せの方法をいう。

著作権法(6/11)

- 第11条 二次的著作物

二次的著作物に対するこの法律による保護は、その原著作物の著作者の権利に影響を及ぼさない。

- 第12条 編集著作物

編集物でその素材の選択又は配列によつて創作性を有するものは、著作物として保護する。

- 第12条の2 データベースの著作物
  - データベースでその情報の選択又は体系的な構成によつて創作性を有するものは、著作物として保護する。
  - 第2項　前項の規定は、同項のデータベースの部分を構成する著作物の著作者の権利に影響を及ぼさない。

著作権法(7/11)

- 第30条 私的使用のための複製

著作権の目的となつている著作物は、個人的に又は家庭内その他これに準ずる限られた範囲内において使用（私的使用）を目的とするときは、次に掲げる場合を除き、その使用する者が複製することができる。

- 公衆の使用に供することを目的として設置されている自動複製機器を用いて複製する場合
- 技術的保護手段の回避を行うこと又は特定の変換を必要とするよう変換された著作物に対して、当該技術的保護手段によつて防止される行為を可能とし、又は当該技術的保護手段によつて抑止される行為の結果に障害を生じないようにすること。又はその結果に障害が生じないようになつた複製を、その事実を知りながら行う場合。
- 著作権を侵害する自動公衆送信を受信して行うデジタル方式の録音又は録画を、その事実を知りながら行う場合

著作権法(8/11)

- 第32条 引用

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。

- 第37条 視覚障害者等のための複製等
- 第37条の2 聴覚障害者等のための複製等

著作権法(9/11)

- 第47条の3 プログラムの著作物の複製物の所有者による複製等

プログラムの著作物の複製物の所有者は、自ら当該著作物を電子計算機において実行するために必要と認められる限度において、当該著作物を複製することができる

- 第47条の4 電子計算機における著作物の利用に付随する利用等

著作物の電子計算機における利用を円滑又は効率的に行うために当該電子計算機における利用に付随する利用に供することを目的とする場合には、その必要と認められる限度において、いずれの方法によるかを問わず、利用することができる

著作権法(10/11)

- 第47条の5 電子計算機による情報処理及びその結果の提供に付随する軽微利用等

電子計算機を用いた情報処理により新たな知見又は情報を創出することによつて著作物の利用の促進に資する次の各号に掲げる行為を行う者は、公衆への提供又は提示が行われた著作物について、当該各号に掲げる行為の目的上必要と認められる限度において、当該行為に付随して、いずれの方法によるかを問わず、利用を行うことができる。

ただし、当該公衆提供提示著作物に係る公衆への提供又は提示が著作権を侵害するものであることを知りながら当該軽微利用を行う場合その他当該公衆提供提示著作物の種類及び用途並びに当該軽微利用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。

著作権法(11/11)

- 第33条 教科用図書等への掲載
- 第33条の2 教科用図書代替教材への掲載等
- 第33条の3 教科用拡大図書等の作成のための複製等
- 第34条 学校教育番組の放送等
- 第35条 学校その他の教育機関における複製等
- 第36条 試験問題としての複製等

このへんの法律話は情報ネットワーク特論でやったので、講義資料[1]参照

- プライバシー関係
  - 忘れられる権利
  - COVID-19感染者追跡アプリにおけるプライバシーと追跡の両立
- 個人情報関係
  - 個人情報の分類
  - 個人情報に関する動向
  - 匿名化処理
  - EUの一般データ保護規則(GDPR) / AI act
- その他
  - マイナンバーカード(個人番号カード)とマイナンバー(個人番号)

[1] https://www.net.itc.nagoya-u.ac.jp/member/shimada/infoNW2024B/slide/lecture20240709slide_rev1.pdf