インターネット基礎理論 11
セキュリティ・法律

はじめに

資料置き場

https://sammyppr.github.io

に授業資料を置いていきます。復習に使ってください。

欠席した場合などはスライドを確認して追いつくようにしましょう。

> スライドあるなら授業受けなくていいや

なんてことは思わないようにお願いします。

これまでやってきたこと

以下の説明はできますか？

- コンピュータの仕組みについて以下のキーワードを用いて説明せよ
  ハードウェア・ソフトウェア・プロセッサ・メモリ・I/O・OS・アプリケーション
- インターネットの仕組みについて以下のキーワードを用いて説明せよ
  TCP/IP・IPアドレス・ドメインネーム・DNS・URL・ポート・パケット・サーバ・クライアント・プロトコル
- ホームページの仕組みについて以下のキーワードを用いて説明せよ
  ブラウザ・HTML・CSS・JavaScript・フロントエンド・バックエンド・データベース

セキュリティ

セキュリティとは？

インターネットにおいて

セキュリティ

という言葉がよく使われていますが、これについて説明したいと思います。

もう一度、インターネットとは？

インターネットは誰でも自由にアクセス出来るネットワークです。

様々な情報がオープンに公開され、距離や時間の垣根が世界レベルでなくなりつつあることを意味し、これは本来非常に喜ばしいことです。

インターネットに潜む危険性

一方で、大切な情報が外部に漏れたり、ウイルスに感染してデータが壊れたり、普段使っているサービスが急に使えなくなったりしないように必要な対策をすることが求められています。

情報セキュリティの定義としては

情報の機密性、完全性、可用性を確保すること

となります。

3つの要素

- **機密性:** ある情報へのアクセスを認められた人だけがその情報にアクセスできる状態を確保すること
- **完全性:** 情報が破壊、改ざん又は消去されていない状態を確保すること
- **可用性:** 情報へのアクセスを認められた人が、必要時に中断することなく、情報にアクセスできる状態を確保すること

クラッカー

一方で悪さをする人がいます。

ちなみに、よく混乱して利用されているのですが、

- **ハッカー:** コンピュータ技術に精通する人
- **クラッカー:** コンピュータ・ネットワークに不正に侵入したり、破壊・改ざんなどの悪意を持った行為をする人

と定義されます。マスコミ的には両者を混同し「ハッカー」と呼んだりすることもあります。今回はこの定義で進めていきます。

ちなみに、こんな定義もあるみたいです。

- **ホワイトハッカー：** ノウハウを善良な目的で使用する
- **ブラックハッカー:** 不正行為を目的として使用する(=クラッカー)

クラッカーの目的

彼らの目的は

- 愉快犯
- 知的好奇心の充足
- 本格的な社会に対するテロ

等です。

インターネットでなくても、たくさんの迷惑をかける人がいるため、必要悪とはいいませんが、決していなくなることはありません。

どう対処すればいいの？

これらクラッカーからの脅威を避けるために、セキュリティが必要となります。

どのような対策をとればよいか、ということを考える前に、クラッカーは何をしているかを簡単に説明しましょう。

クラッカーがしていること

だいたい次のようにいえると考えられます。

1. 逆探知されないように、踏み台となるコンピュータをつくる
2. 踏み台となるコンピュータに足跡を残さないように、ログを改ざんする技術を持つ
3. いくつかの踏み台を利用しながら、ターゲットとなるコンピュータへのアクセスを試みる
4. ターゲットとなるコンピュータのアカウント・パスワード(なるべく管理者用)を取得する
5. 違法な情報アクセス（閲覧・改ざん・削除）をする

なぜ、このようなことができるか？

高度なクラッカーは自分でいろいろトライをしながらクラッキングをしますが、クラッキングのための情報は簡単に転がっています。

例えば、

セキュリティアップデート

と呼ばれるものがOS等には必ずあります。これは、開発時には気づかなかったOS等のバグを修正するためのものです。

管理者の怠慢

しかし、世の中のコンピュータ管理者全てがまめにセキュリティアップデートをかけているわけではありません。

よって、セキュリティアップデートが修正している箇所をつついてみれば、管理者のしっかりしていないコンピュータは簡単に破られてしまいます。

皆さんのコンピュータも、頻繁にセキュリティアップデートのお知らせがきていると思いますが、放置した状態で、公衆Wifiなどに接続していると危険です。

クラッカーの対策

対策1

クラッカーはネットワークやコンピュータの弱点を探しながら侵入してきます。

よって、既知のセキュリティホールは必ずセキュリティアップデートをして塞ぐ用にしましょう。

ちなみに、セキュリティ上の弱点のことを「セキュリティホール」、それに対策することを「塞ぐ」といいます。

対策2

パスワードは分かりづらいものにしましょう。

とはいえ、忘れることを恐れて、未だに簡単な単語にしている人も多くいます。

単純な「hello」という単語も「l→1」「o→0」という置き換えをし、「he110」とするだけで、パスワードを破られる可能性はかなり減ります。

「hello world」を「space→s」という置き換えをして「he110sw0r1d」とすれば、かなり複雑なパスワードにすることができます。

- ストリーミングサービスではより単純なパスワードが使われる傾向--リスクを抑えるには

パスワード管理について

総務省が明確にパスワードの定期変更は不要、とアナウンスをしています。

- 総務省から「パスワードの定期変更は不要」と発表|安全なパスワード管理・設定方法を紹介

とはいえ、

- パスワードの複雑化
- パスワードの使い回しをしない

は必須となります。

これを管理するのは大変ですので、パスワード管理ツールを利用するのも一つの手です。ここではbitwardenを紹介します。windows/macOS/Linux/Android/iOS全てに対応しています。

- bitwarden

対策3

不要なポートをルーターで塞ぎましょう。

コンピュータには65536本の手があると説明しました。この中で通常の利用に必要なポートはわずかです。
ですので、それ以外のポートへのアクセスは不可能とすることでかなりの脅威を防ぐことができます。

PCの中ではファイアウォール(防火壁)という機能で防ぐことができます。

- Macの「ファイアウォール」設定を変更する
- Microsoft Defender ファイアウォールを有効または無効にする

ウイルス

ウイルスとは

コンピュータ・ウィルスによる被害も最近では深刻になっています。

コンピュータ・ウィルスとは、コンピュータに被害をもたらす不正なプログラムのことです。

また、生物学的なウィルス同様、自己繁殖していくことが特徴になっています。

主なウィルスの種類

- **ワーム:** 独立したプログラムであり、自身を複製して他のシステムに拡散する性質を持ったウィルス
- **トロイの木馬:** 一見有用なアプリケーションに見えて、その一部にコンピュータのデータを盗み出す等の不正な動作をさせる機能を備えたウィルス。
  破壊目的ではなく、データの収集を集めることが目的のトロイの木馬は「スパイウェア」とも呼ばれる。

人ごとだと思っていませんか？

情報センターに尋ねたところ、この大学のネットワークにおいて利用されるコンピュータから、特にUSBメモリがウィルスに感染している、との報告が頻繁にあがってくるようです。

人事だと思わずに、自分が感染源にならないよう注意してください。

ウイルス対策

対策1

利用するコンピュータにアンチウィルス用のソフトを入れることが必要です。

有償のものも無償のものもあります。どちらにしても、感染しないように日頃からスキャンする癖をつけましょう。

ウイルス定義リストのアップデート

アンチウイルス用ソフトウェアを入れていても、最新の定義リストにしておかなければ感知できないことになります。

そのためアップデートが必要です。

ウイルスを検知した、というアラート

Webを閲覧していると、「ウイルスを検知した」というアラートが出ることが有ります。

これを信じると、そのボタンをクリックしたことによりウイルスに感染するということもあります。気をつけましょう。

0day攻撃

ゼロデイ攻撃とは、アプリケーションやソフトウェアの脆弱性（セキュリティ面の欠陥）をメーカーが発見して対策を打つ前に、その脆弱性に付け込んで、不正アクセスやマルウェア感染などのサイバー攻撃を仕掛ける、サイバー攻撃手法のことです。

- ゼロデイ攻撃とは？手口・対策・事例をわかりやすく紹介

ランサムウェア攻撃

ランサムウェア攻撃はマルウェア攻撃の一種であり、攻撃者がファイルやデータを暗号化したり盗んだりして身代金を要求します。 また、データの破棄や公開が脅迫材料に使われる場合もあります。 被害者が金銭を支払うと、復号キーが提供されたり、盗まれたデータが削除されたりするのが一般的です。

2024年にはKADOKAWAグループが攻撃を受けたとして話題になりました。

- ランサムウェア攻撃による情報漏洩に関するお知らせ

「ウイルス対策ソフトは死んだ」？

Symantec社の幹部が2014年5月にこのようにコメントしました。

- https://gigazine.net/news/20140507-antivirus-software-is-dead/

これは何を意味するのでしょうか？

ウイルスが発見されて、それの対策を取る、ということではイタチごっことなってしまい、根本的に脅威から逃れることは出来ない、ということを意味します。

怪しい挙動をしている通信を検知し、それに対して対処をとれるようなセキュリティソフトが必要な時代になっていることを意味します。

AI・機械学習を使ったNGAV(NextGenerationAntiVirus)と呼ばれるものも出てきていますが、まだあまり普及してないように思えます。

macだから平気？

ウィルスはこれまでWindowsに多く、Macには少ないとの傾向がありました。しかし、macがunixベースのOS Xになってから、事情が変わってきています。

ウィルス作成者には先程いったように愉快犯が多いのです。ですから、多くの市場をとっているコンピュータに対してウィルスを作成する傾向があります。ということで、macも危険になってきています。

スマートフォンは？iOSの場合

iOSを利用しているiPhone, iPad等ではウィルス感染の確率はゼロではありませんが、非常に少なくなっています。

理由としては、App Storeでしかアプリが流通できず、十分な審査がされてから公開されているからです。

しかし、WebサイトからSafari（ブラウザ）に対して攻撃することはできるため、アップデータはまめにかけましょう。

スマートフォンは？Androidの場合

これに較べてAndroidは非常に危険です。

「GooglePlayプロテクト」という機能である程度GooglePlayを守っているようですが、

- Google Playのアプリにマルウェア 2023年は 6 億回以上ダウンロードされる

よって、ウィルス対策を施すのはもちろんのこと、アプリをインストール際には、問題があるかないか、等を確認の上インストールするようにしましょう。

フィッシング

悪意のあるホームページ・メール

ホームページやメールで悪意のあるものがあります。

悪意の第三者が会員制ウェブサイトや有名企業を装い、クレジットカードやID、パスワード等を取得することを目的としています。その結果、

- 架空請求詐欺
- 預金の引き下ろし
- クレジットカードの不正利用

等の問題が多発しています。

フィッシング対策

これらの被害を防止するためには、

- 個人情報を入力する前に、本物のサイトであることを確認する
- URLが本物かどうかの確認
- httpsの証明書が有効であるかの確認
- リンクを踏む前にリンク先のアドレスの確認

等が有効です。

複合的な手口

ネットバンキングでの例

2012年に様々なネットバンキングで不正送金されてしまう事件が起こった。これの仕組みは以下のとおり

- ウィルスに感染したコンピュータから、正規のネットワークバンキングにアクセスをすると、そのウィルスがそれを検知し、新たな偽のポップアップウィンドウを開く
- 偽のポップアップウィンドウを信じたユーザが、第一暗証番号、第二暗証番号、乱数表等を入力
- それらのデータが犯人に送信
- 犯人は簡単に乗っ取った口座から別口座に送金

防げなかったか？

この例では、

- ウィルス対策をしていなかったこと
- 全ての情報を入力することに疑問を持たなかったこと

等の複合的な要素によって詐欺にあってしまいました。

サイバー攻撃

サイバー攻撃・サイバーテロ

サイバー攻撃またはサイバーテロと呼ばれるものがあります。

可視化できるWebページがあるのでみてみましょう。

- CyberThreat

補足：IPアドレスと場所の特定について

IPアドレスが割り振られているため、国についての特定は簡単にできます。が、国の中のどこにいるか、ということは簡単に特定できるわけではありません。

- プロバイダーが位置情報をある程度提供している
- ブラウザが位置情報を自分から提供している

のどちらかになるかと思います。

歴史的に考えれば

詐欺師は、ありとあらゆる手段を用いて、詐欺を働いて来ました。これは、何もインターネット上だけのことではありません。日頃から、

> まさか、自分はひっかかるわけない

などとは思わずに、危険性についてよく考えてみましょう。

情報セキュリティ10大脅威2025

まとめとして、IPA(情報処理推進機構)が発表している情報セキュリティ10大脅威2025を見ておきましょう。

- 情報セキュリティ10大脅威2025

動画化してくれている人がいます。個人編を見てみましょう。組織編も置いておきます。

- 情報セキュリティ10大脅威2025 個人編 #初心者のためのセキュリティ(7:01)
- 情報セキュリティ10大脅威2025 組織編 #初心者のためのセキュリティ

インターネット関連の法律

ネット選挙

法律に関してはネット選挙からはじめます。

> インターネット選挙運動解禁に係る公職選挙法の一部を改正する法律

が成立（平成25年4月19日）しました。

決して、ネットを使って投票が出来るようになったわけではありません！

ネット選挙解禁のポイント

- インターネット選挙運動の解禁に関する情報

こちらまとめ

- インターネットを使った選挙運動が 出来るようになりました。

情報流通プラットフォーム対処法

SNS誹謗中傷対策

2025/4/1に情報流通プラットフォーム対処法が施行しました。
誹謗中傷やプライバシー侵害などの違法・有害情報への対応を強化するための法律です。

- 【SNSの誹謗中傷対策】「削除」進む？ 罰金は最大1億円…“迅速な対応”法的な義務に

まだ施行されたばかりで、よくわからないけど、ここに情報が集まりそうです。

- 情報流通プラットフォーム対処法 関連情報サイト

指定事業者はここに記載があります。

- インターネット上の違法・有害情報に対する対応（情報流通プラットフォーム対処法）

懸念点

- **表現の自由への影響** 削除基準の明確化や迅速な対応義務は、表現の自由を侵害する可能性があるという懸念があります。特に、プラットフォーム事業者が恣意的に情報を削除する可能性や、権利侵害の判断が曖昧な場合、萎縮効果が生じる可能性があります。
- **プラットフォーム事業者の負担増** 大規模プラットフォーム事業者には、削除申出への対応や、運用状況の透明化など、多くの義務が課せられます。これらの対応には、人的・費用的な負担が大きくなる可能性があります。
- **悪意ある利用者の増加** 誹謗中傷などの違法・有害情報が削除されやすくなることで、悪意のある利用者が、新たなアカウントを作成したり、別のプラットフォームを利用したりする可能性があります。
- **削除基準の曖昧さ** 削除基準が明確に定められていない場合、プラットフォーム事業者の判断に委ねられる部分が大きくなり、公平性に欠ける可能性があります。

懸念点続き

- **発信者情報開示のハードル** 発信者情報開示請求は、裁判所を通じた手続きが必要であり、時間と費用がかかるため、被害者が泣き寝入りしてしまうケースも考えられます。
- **海外事業者への対応** 海外に拠点を置くプラットフォーム事業者への対応は、国内法がどこまで適用されるのか、また、各国の法律との関係など、課題が残ります。

いずれにせよ、日頃から誹謗中傷やプライバシー侵害を行わないように留意しましょう。

著作権

著作権

著作権法では著作物を

> 思想又は感情を創作的に表現したものであって、文芸、学術、美術又は音楽の範囲に属するものをいう

と定義しています。

そして、著作権は著作物を創造した者の金銭的な利益を守るための権利であり、日本では原則として創作した時から死後70年間守られています。

> 平成 30（2018）年 12 月 30 日付けで著作者の 死後 50 年から 70 年に延長されることになり、20 年長く著作物が保護されることとなりました。

- 著作物等の保護期間の延長に関するQ&A

著作権侵害

著作権侵害をした者に対しては、損害賠償請求や差止請求のような民事的請求が認められています。また、故意に著作権侵害をした者に対しては、懲役や罰金の刑事罰が科されることもあります。

ただし、

- 私的使用のための複製
- 図書館等における複製
- 引用
- 学校教育に関する複製

については、著作権侵害には当たらないと規定されています。

気をつけるように！

現在ではインターネット・スマートフォン等を利用することで、簡単に著作権を侵害することができます。

- 音楽や映像を不特定の人とファイル交換すること
- 映画DVDなどにかけているコピープロテクトを外すこと
- 上映されている映画を撮影・録画する行為

自分が著作権侵害していないか十分に気をつけて生活するようにしてください。

著作権侵害は犯罪です。

ちなみに、漫画村の運営に積極的に関与していた者は17億円もの損害賠償金の支払いを命じられています。

- 「漫画村」に関する損害賠償請求事件の判決言渡について

パブリックドメイン

- 保護期間の終了
- 著作者が権利を放棄している

等の理由により、著作物を誰でも自由に利用できる状態のことを指します。

「ブラックジャックによろしく」という漫画が作品の二次利用をフリー化したことが話題になりました。インターネットとともに、著作権の考え方もいろいろと変わってきています。

- 「ブラックジャックによろしく」二次利用フリー化10年後報告

コピーレフト

著作権のことをcopyrightと呼びますが、それに対するコピーレフト(copyleft)という考え方があります。
定義は以下のようになります。

- 著作物の利用、コピー、再配布、翻案を制限しない
- 改変したもの(二次的著作物)の再配布を制限しない
- 二次的著作物の利用、コピー、再配布、翻案を制限してはならない
- コピー、再配布の際には、その後の利用と翻案に制限が無いよう、全ての情報を含める必要がある
- 翻案が制限されない反面、原著作物の二次的著作物にも同一のコピーレフトのライセンスを適用し、これを明記しなければならない
  （翻案：既存の事柄の趣旨を生かして作り変えること）

コピーレフト続き

パブリックドメインを二次利用した場合に、その内容について原作者が何ら権利がない、ということが問題になり、それを機会にコピーレフトという考え方が生まれて来ました。

その他にもコンテンツの利用に際して

- creative commons
- GNU Free Documentation

等いくつかの考え方があります。

自分が著作権者になった場合に、どうやって公開するかは慎重に考えましょう。

インターネット利用上の注意

インターネットでは身元が特定できない?

インターネット上で人と出会うときには、なるべくニックネーム等個人を特定されないようにして、発言をするようにしてください。

ツイッターなどはバカッターと呼ばれるように、問題発言をすると、それは世界中からアクセスが可能であり、匿名なつもりでも、その身元を探して炎上することがよくあります。

- 無免許行為
- 万引き行為
- 未成年の飲酒
- 盗撮

等、嘘でも書くと炎上しますから、特に気をつけるように。

小レポート

インターネットを利用する上での危険性について述べよ。(manaba)