

ITリテラシーを高めよう！

～安心・安全な使い方と工夫～

めいまい・セキュア・コミュニティ
大石学



講座のねらい

- ①スマホ、インターネットの知識向上
- ②地域交流、活性化



ITリテラシーの格差を埋め、
困ったときに相談できる仲間・場が
あることを実感する。



1. 自己紹介



<氏名> 大石 学 (オオイシ マナブ) 46才

<職業> 会社員 システムエンジニア

主な業務: 顧客システム保守運用、セキュリティサービスなど

<資格>

登録セキスペ(情報処理安全確保支援士)

SPREAD情報セキュリティサポーター

デジタル庁 デジタル推進委員



第025274号

資格取得が活動のきっかけ



1. 自己紹介



めいまいセキュア・コミュニティ

交流

まなび

地域活性化

活動歴

活動歴1年

活動エリア

明舞団地中心（朝霧エリア）

活動概要

- ・地域交流 月2回（隔週土曜10時～14時半）
- ・高齢者向けパソコン、スマホお悩み相談
- ・こども向けマインクラフト交流クラブ

高齢化率
（松が丘校区）
39%

活動報告

自治体（明石市、神戸市）を問わず、同じ地域に関わる幅広い

地域の交流、まなび、活性化を
目的に活動しています。

が必要と感じました。



1. 自己紹介



①シニア、高齢者向け、②こども向け

- ・松が丘交流ゾーン(写真)
- ・月2回(隔週土曜日)10:00~14:30

- ・お茶、お菓子(参加費:200円)
- ・予約不要、出入り自由

①シニア、高齢者(60~80代)
参加者:2~5名



②こども(2~10歳)
参加者:3~5名



1. 講義説明

①情報量が多いです。

→**気になったことは、メモ**してください。

(途中、意見交換や休憩の時間は取ります)

②頻繁に、質問を投げかけます。

→**意見は、十人十色。気軽に反応**をお願いします。

③各自で復習してください。

→リテラシーは、**反復により身に付きます**。

なお、本資料の学習・演習の内容は、出典を記載しておりますが、記載がない場合は、下記を参考に作成しています。

- ・ 総務省 「デジタル活用支援推進事業 標準教材」
 - ・ スマートフォンを安全に使うための基本的なポイントを知ろう
 - ・ デジタルリテラシーを身につけて安心・安全にインターネットを楽しもう
 - ・ 生成AIを使ってみよう
- ・ 内閣サイバーセキュリティセンター
「インターネットの安全・安心ハンドブック」
- ・ 一般社団法人ソーシャルメディア利用環境整備機構
「フェイク見破りチャレンジ」



2. 講義 スマホ・インターネットの 安心・安全な利用



2-1. スマホとインターネット (10分)

関係についてお話します



2-1. スマホとインターネット



今回、参加者のスマホをお持ちの割合は、
どれくらいでしょうか？

『いつのまにか持っていた(子供に持たされていた)』
なんていうことも…

スマホがいつから普及したか？

総務省『情報通信白書』(令和4年)で、時系列に、
当時を思い出しながら、振り返ってみましょう！

第1章 過去50年間での変化を時系列で振り返る

- 白書刊行から50年間を、ICTの高度化とサービスの多様化等の観点から5期に分けて制度やサービス、技術等の点でどのような変化があったのかを整理

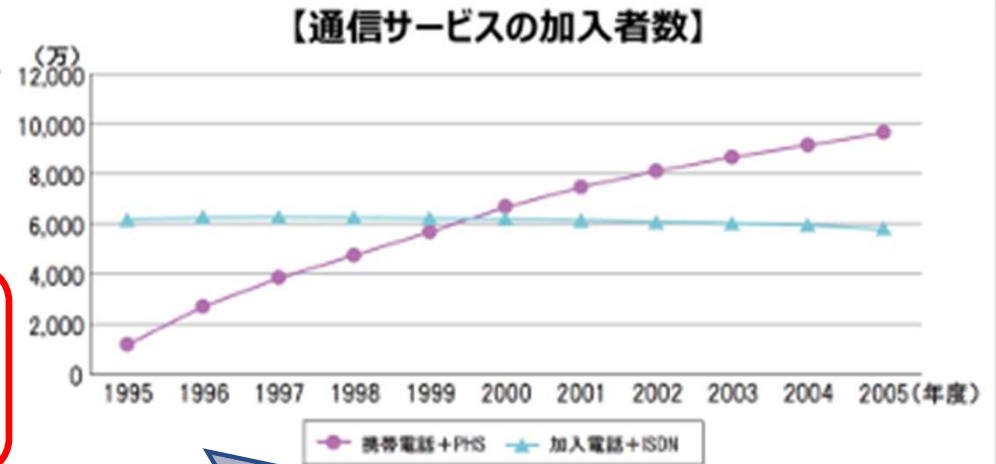
1. 1973－1985年頃：アナログ通信・放送の時代
2. 1985－1995年頃：通信・放送市場の発展と新たなサービスの登場
3. 1995－2005年頃：インターネットと携帯電話の普及
4. 2005－2015年頃：ブロードバンド化とモバイル活用の拡大
5. 2015年－：ICTの社会・経済インフラとしての定着



第3節 1995年-2005年頃：インターネットと携帯電話の普及

4

- インターネットが一般家庭へも急速に普及し、写真等の画像も閲覧可能となる。また、インターネットを用いた新たなビジネス(例:ECモール、ポータルサイト)が拡大。
- 携帯電話も料金の低廉化が進んだこと等により普及が進み、2000年には、移動電話サービスの契約者数が固定電話サービスの契約者数を上回る。



「インターネットが一般家庭に普及し、携帯電話が固定電話の契約者数を上回る」

30～20年前は「ガラケー」の全盛期！
「スマホ」の登場は、まだ・・・



第4節 2005年-2015年頃：ブロードバンド化とモバイル活用の拡大

- ネットワークインフラの高速化・大容量化が進展し、固定通信網ではFTTH、移動通信網ではLTEが普及。
- 2008年にiPhoneが発売され、スマートフォンが急速に普及。SNS、地図、検索等多様なアプリケーションサービス等により、モバイル端末の利用シーンが拡大。
- ネットワークの高度化、センサーの高機能化等を背景に、あらゆるものがネットワークにつながるIoTが進展。

【スマートフォンの世帯保有率の推移】



2021年で88%の世帯が保有。


2008年(17年前)くらいから、利用・普及が始まったようです！

今でも、iPhoneは高価。私も、安いスマホが出るまでガラケーでした。

2-1. スマホとインターネット

第5節 2015年-現在：ICTの社会・経済インフラとしての定着

- ネットワークインフラは更に高度化し、2020年3月、5Gサービスの提供が開始。様々な主体が利用可能な「ローカル5G」の制度が新設され、医療、製造業(工場)など多様な分野での5G利活用の推進に向けて実証実験等を実施。
また、6G/ Beyond5Gに向けた技術戦略等についても検討。
- インターネット動画配信サービスが普及・本格化。
放送事業者は、見逃し配信サービスや番組のリアルタイム配信サービスを提供。
- 新型コロナウイルス感染症の感染拡大に伴い、テレワーク、オンライン学習、オンライン診療等非接触・非対面での生活様式を可能とするICTの利活用が一層進展、ICTはあらゆる社会経済活動を支えるインフラのインフラ。
- グローバルプラットフォームの市場支配力は一層高まりを見せており、データの寡占やその取扱いに関する



現在、「ICT(情報通信技術)」は、ガス、水道、電気など「インフラを支えるインフラ」として重要視されています。
(例：阪神淡路大震災(1995)と、能登半島地震(2024)の復旧の早さにも、情報通信の違いが影響)

今日のポイント

1. スマホとインターネット

さて、そんな情報通信を担う「スマホ」は、「ガラケー」と何が違うのか？

スマートフォンとは、**パソコンのような機能を併せ持った携帯電話機の総称**です。
多機能かつ高性能なため「**smart(賢い)**」+「**phone(電話)**」を合わせて「スマートフォン」と呼ばれています。

従来型携帯電話の主な機能



+

各種アプリケーション



違いは、「**インターネットにつながっていること**」
これを理解することが大切です！

2-2. これからの情報社会 (10分)

前章までは、過去～現在の振り返り。
少しこれからのお話をします。



「Society 5.0」(ソサエティー 5.0)
という言葉聞いたことがありますか？



サイバー空間とフィジカル空間の融合が進んだ、
「新たな社会」を「Society 5.0」と呼んでいます。



情報社会の次に来る「新たな社会」が、Society5.0です。

新たな社会
"Society 5.0"

5.0



1.0
Society 1.0 狩猟

2.0



Society 2.0 農



Society 3.0 工業

3.0

4.0



Society 4.0 情報

Society 5.0

新たな社会

Society 4.0

情報社会

Society 3.0

工業社会

Society 2.0

農耕社会

Society 1.0

狩猟社会

サイバー空間とフィジカル空間の融合とは？

全面的キャッシュレス決済はじまる！
Fully Cashless Payments Begin!
EXPO 2025

※会場内では、現金が使用できませんのでご注意ください。Cash will not be accepted.



万博会場内は、国際博覧会として初めての試みとなる全面的キャッシュレスを導入します。

会場内の買物、飲食ではキャッシュレス決済のみで現金は使用できません。

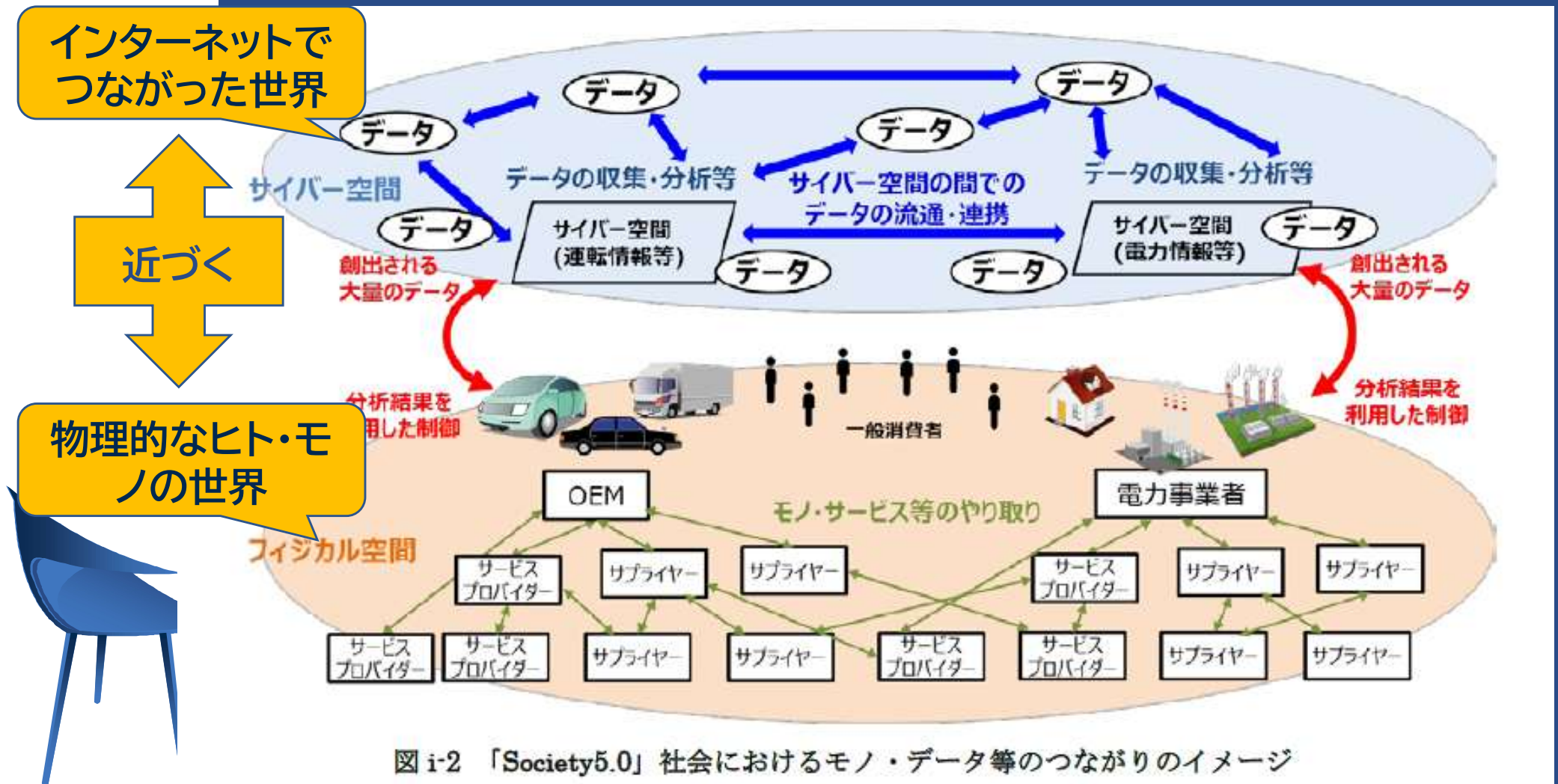
現金以外の決済手段を持たない方は事前にプリペイドカードをご購入いただく必要がございます。



昔は、現金手渡し(フィジカル空間のみ)。
今は、銀行振込が当たり前。将来は、
キャッシュレスのみ(サイバー空間での送金のみ)？！



「サイバー空間＝仮想」と「フィジカル空間＝物理」が、
近づく流れの中にいる→インターネットの役割は増す。



2-2. これからの情報社会



現在、世界中で注目されている**生成AI**も、インターネットを使える環境であれば、スマホやパソコンから利用できます。

(代表的)チャットGPT
<https://chatgpt.com/>

各コミセンでの体験回では、グループで下記のような操作を体験します。

(例1) キーワードから**俳句を生成する**。

(例2) 自分の写真から**似顔絵を生成**。

(例3) 複雑な情報を整理し、**解決案を提案させる**。

など



生成AI(Generative AI)は、

新しいデータを学習することで、過去、困難とされていた課題を解決しています。今後、さらなる活用が期待されています。

生成AIによる課題解決と展望(代表的な例)

分類	過去の課題	生成AIによる現状の変化	今後の展望
言語・情報	翻訳・要約の精度	意味理解に基づく自然文生成	マルチモーダル理解によるリアルタイム翻訳
創造・表現	人間的創造性の限界	画像・音楽・映像生成	AIと人の共同創作文化の確立
教育・社会	情報格差・教育格差	AIチューター・自動要約	個別最適化された学習・医療
産業知識	暗黙知の継承困難	業務記録の自動要約	組織知の「AI化」
政策・社会設計	合意形成の困難	議論要約AIの登場	公共議論支援AIによる民主的プロセス強化

そんな役割を担うインターネットですが、注意も必要です

ニーチェ(1886年。哲学者)

「深淵をのぞく時、深淵もまたこちらをのぞいているのだ」

様々なサービスや個人にアクセスできることは、
攻撃者(悪意を持った利用者)もインターネット(サイバー空間)を介して、企業や個人に**アクセスできる**ということ。



2-3. インターネットの特徴

このインターネット(つながっているスマホ)を、今後、安全・安心に利用するには、どうすれば良いのでしょうか？

インターネットの「特徴」や「攻撃者」について、知ることも大切です。

2-3. インターネットの 特徴

- ① 気を引く表示
- ② ネット上の行動履歴
- ③ フィルターバブル
- ④ 偽情報/誤情報

2-4. インターネットの 攻撃者

- ① 攻撃者の種類
- ② 攻撃の事例
- ③ 身を守るためのパスワード
- ④ 不安なときの相談先

2-3. インターネットの特徴 (10分)



2-3. インターネットの特徴

次の4つを紹介します。

学習の最後に、簡単なチェックにチャレンジしましょう！

- ① 気を引く表示
- ② ネット上の行動履歴
- ③ フィルターバブル
- ④ 偽情報/誤情報

今日のポイント



2-3. インターネットの特徴

実際の、私のYahoo!のトップページ画面を例に説明します。

The screenshot shows the Yahoo! Japan homepage with several annotations:

- ②拡大** (Zoom 2): A green speech bubble pointing to the right sidebar, specifically the "雨雲レーダー" (Rain Cloud Radar) and "地域情報" (Local Information) section.
- ①拡大** (Zoom 1): A green speech bubble pointing to the main content area, specifically the article about the actress "モデルで女優が43歳誕生日「ありがとう、お母さん」" (Model and actress turns 43 on her birthday "Thank you, Mom").

The page layout includes a left sidebar with various services (e.g., LINE, Map, Weather), a main content area with news and sports, and a right sidebar with weather and recommended products.



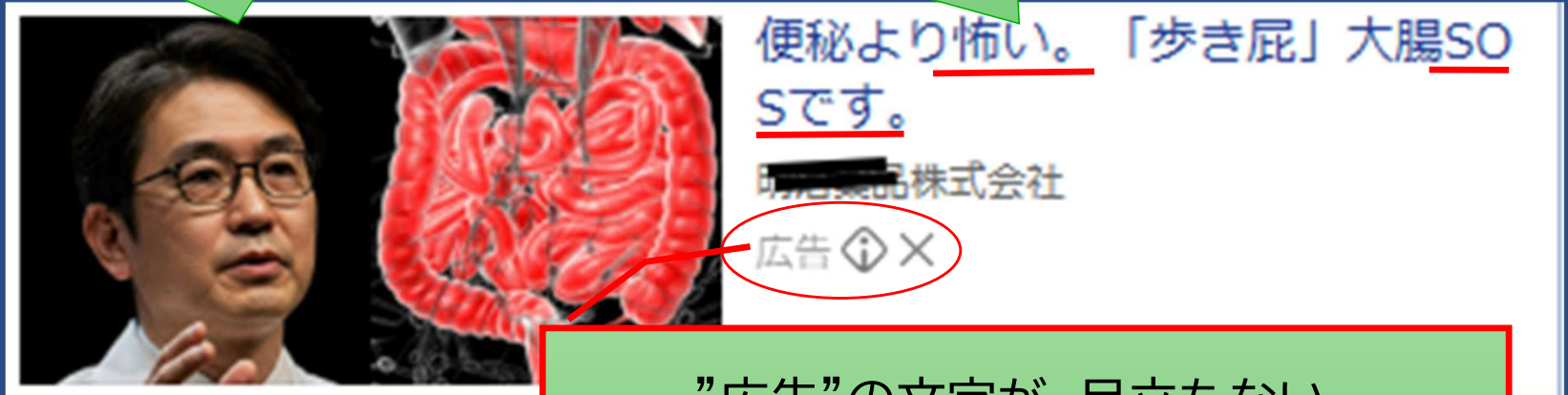
2-3. インターネットの特徴

① 気を引く表示

アテンション・エコノミーという、より多くの広告を見たり、サービスを使ってもらおうとする仕組みがあります。

“学者”や“臓器”の写真

“怖い”、“SOS”などの文字



”広告”の文字が、目立たない。
ニュース記事に紛れて表示される。

広告表示の問題(大きさ、内容など)は、広告主や提供者、利用者等により、常に賛否両論の議論が行われています。



2-3. インターネットの特徴



② ネット上の行動履歴

サーバやブラウザ(PC)上に、**個人の行動履歴が記録されます**
(閲覧、購買履歴など)。
これらに基づいて、**類似情報やおススメ**として表示されます。



あなたにおすすめの商品
8/3時点

Yahoo!フリマ

 The North Fa... 9,000円	 MERRELL メレル... 4,800円	
 トレッキングシ ューズ 登... 3,000円	 未使用 Fashion S... 4,500円	 [ザノースフェイ ス] ト... 13,500円

おすすめの商品をもっと見る

防水の靴を、スマホのYahooフリ
マで検索していたら、
パソコンのYahooにも表示される
ようになりました。

インターネット上に履歴が残る。

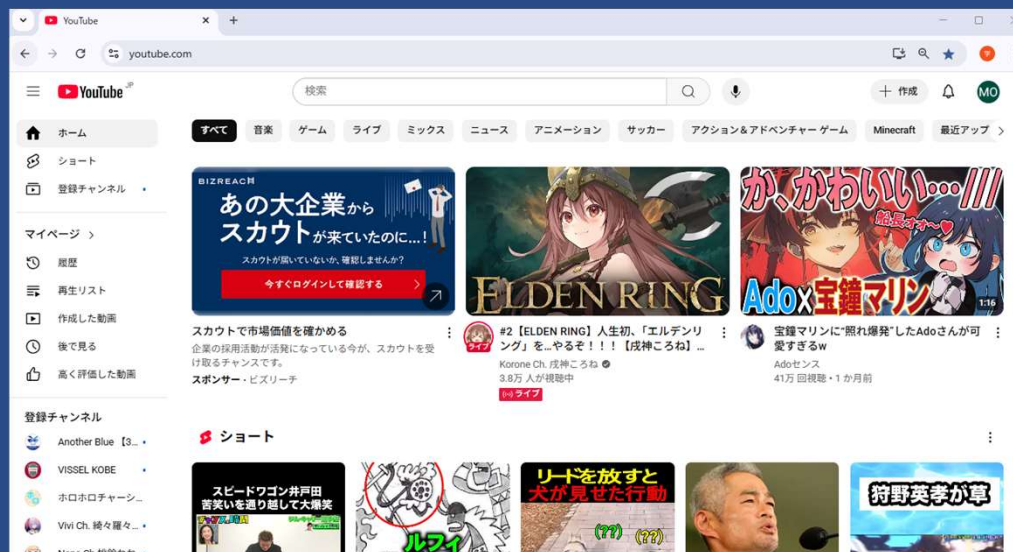


2-3. インターネットの特徴



③フィルターバブル

泡のように、好みに近い情報だけが上がってくる。利用者の行動履歴に基づいて、好みに近い有益であろう情報を予測した結果、類似の情報ばかりしか見えてしまう。



私のYouTubeのホーム
(30動画中※)

- ①Vtuber : 12(40%)
- ②お笑い : 5(17%)
- ③サッカー : 4(13%)
- ④音楽 : 4(13%)
- ⑤その他 : 5(17%)

→8割が「自分の好きなもの・類似のもの」
(※ニュース動画除く)



2-3. インターネットの特徴



④ 偽情報/誤情報

偽情報の拡散。最近では、生成AIによるフェイク画像、動画も増加傾向にある。

ドローンで撮影された静岡県の水害。
マジで悲惨すぎる...



午前4:39 · 2022年9月26日 · Twitter for Android

2022年9月、静岡県
の台風15号による水
害被害の画像がSNS
上で拡散。その後、投
稿者が、画像生成AI
で作成した**偽画像**だっ
たと公表。

<https://news.yahoo.co.jp/articles/95fb66b9baba435063f904f08f19e3646e6186cf?page=1>



2-3. インターネットの特徴



④偽情報/誤情報

嘘つきは泥棒の始まり・・とはいえ人間は、冗談、ユーモア、噂話が大好き！

行為内容	法的リスク	主な根拠法
パロディ・創作目的(誤認させない)	原則なし	表現の自由
虚偽の内容で人の名誉を傷つける	名誉毀損罪	刑法230条
虚偽情報で企業の信用を損なう	信用毀損罪	刑法233条
混乱を狙った虚偽情報拡散	偽計業務妨害罪	刑法233条
他人の写真をAIで改変	肖像権・著作権侵害	民法・著作権法
ディープフェイクポルノ	性的画像記録処罰法	特別法(刑事罰あり)
選挙や政治関連の偽情報	虚偽事項公表罪	公職選挙法

重要なポイント → 「意図」と「影響」が判断基準になる

- ・「誤認を狙って」「被害を与える」目的があると、罪に問われやすいです。
- ・SNSや動画サイトに投稿した場合、投稿者だけでなく、**拡散者も責任を問われる**ケースがあります。



2-3. インターネットの特徴

あなたの「フェイク対処能力」をチェックすることができるサイトです。

<https://fakechallenge.smaj.or.jp/>

(一般社団法人ソーシャルメディア利用環境整備機構のサイトです)

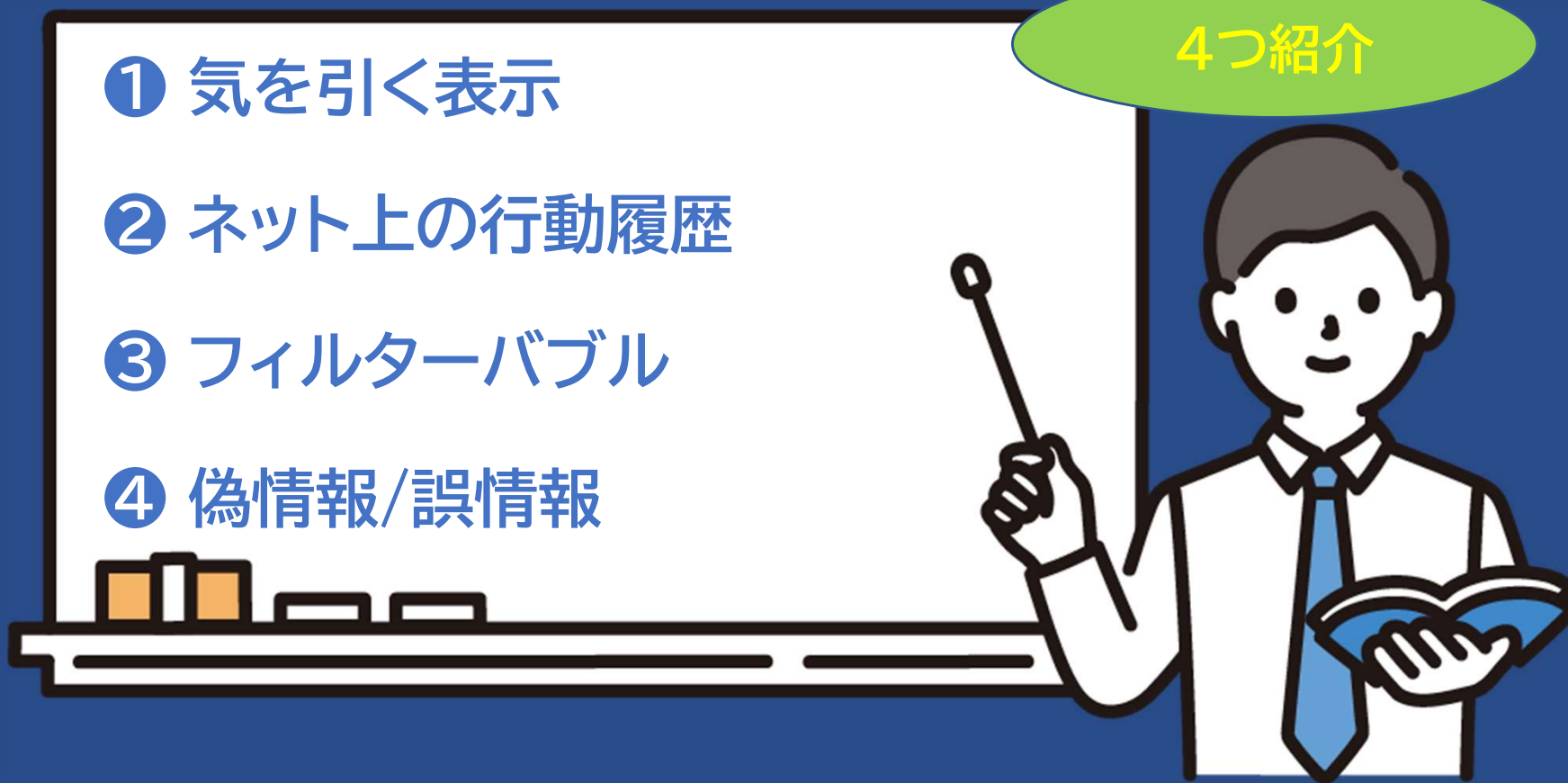


2-3. インターネットの特徴

以上が、インターネットの特徴でした。

4つ紹介

- ① 気を引く表示
- ② ネット上の行動履歴
- ③ フィルターバブル
- ④ 偽情報/誤情報



2-4. インターネットの攻撃者 (10分)



2-4. インターネットの攻撃者



このインターネット(つながっているスマホ)を、今後、安全・安心に利用するには、どうすれば良いのでしょうか？

インターネットの「特徴」や「攻撃者」について、知ることも大切です。

2-3. インターネットの 特徴

- ① 気を引く表示
- ② ネット上の行動履歴
- ③ フィルターバブル
- ④ 偽情報/誤情報

2-4. インターネットの 攻撃者

- ① 攻撃者の種類
- ② 攻撃の事例
- ③ 身を守るためのパスワード
- ④ 不安なときの相談先

2-4. インターネットの攻撃者

インターネット上で、自分の情報を守るには、「攻撃の手口」や「攻撃者がどういう人物か」を知ることが重要です

インターネットの「悪い人」は、何をしてくるのか

インターネットの世界で自分を守るには、「悪い人」が何をしてくるのか、代表的な攻撃手段を知っておくことが有効です。例えばパスワードについては、悪い人は右の図のように見破ってやろうなどと考えています。これを見ると、確かにパスワードは長くて複雑にし、



- ・怪しい場所、危ない人に近づかない
- ・知らない人を信じない
- ・目立たない(自分の情報を出さない)
- ・困ったら警察や信頼できる人に相談する



現実世界では気を付けられるが、
インターネットの世界では、
悪い人や場所が見分けにくい



2-4. インターネットの攻撃者

インターネットの攻撃者が、
「どういう人物」で、「何が活動目的」か知りましょう。

5

攻撃者とはどんな人物なの？

悪意のハッカー
(一般、ビジネス)

国家的ハッカー

攻撃者(アタッカー、クラッカー)とはどんな人物なのか

悪意のハッカー

産業スパイ

国家的ハッカー



コスト優先

目標達成優先

・金銭目的
→コストに見合った技術

・組織活動が目的
→高度、大規模(相手の被害優先)




2-4. インターネットの攻撃者



国家的ハッカーの例

大規模なシステム停止や情報搾取



日本経済新聞

朝刊・夕刊 LIVE Myニュース 日経会社情報 人事ウォッチ NIKKEI

トップ ▾ 速報 ▾ ビジネス ▾ マーケット ▾ 経済 ▾ 国際 ▾ オピニオン ▾ もっと見る ▾

ニコニコ動画、サイバー攻撃で停止 「週末は復旧困難」

情報通信・ネット [+ フォローする](#)

2024年6月9日 11:18 (2024年6月9日 11:48更新)

22年9月には政治的思想を掲げて活動する「ハクティビスト」と呼ばれるロシア系のサイバー攻撃集団「キルネット」が、日本の政府や企業への攻撃を宣言。電子政府の総合窓口「e-Gov」などの政府系サイトや東京地下鉄（東京メトロ）などのインフラ企業のウェブサイトが一時間閲覧しづらい状態になった。

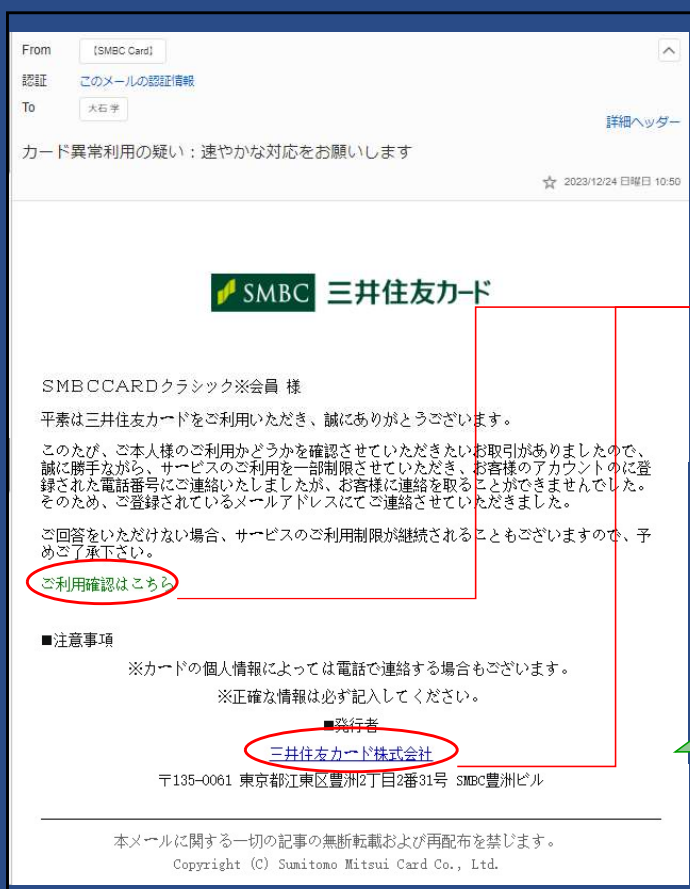
内閣サイバーセキュリティセンター（NISC）などは23年5月、DDoS攻撃だったとする分析結果を公表した。

2-4. インターネットの攻撃者

悪意のハッカーの例
(一般、ビジネス)

事例1: フィッシング詐欺

通販事業者等をかたる偽のメッセージで、本物そっくりのサイトに誘導され、IDやパスワード等の重要な情報を抜き取られる手口です



偽のアドレスにリンクされている
<https://ch-smbc-27.s3.ap-northeast-2.amazonaws.com/ch-smbc-27.html>

<https://www.smbc-card.com/index.jsp>
(正)三井住友カード株式会社のアドレス

画像は、実際の私に送られてきたメール。
「カードが異常利用されている」
という内容で、偽アドレスに誘導していた。

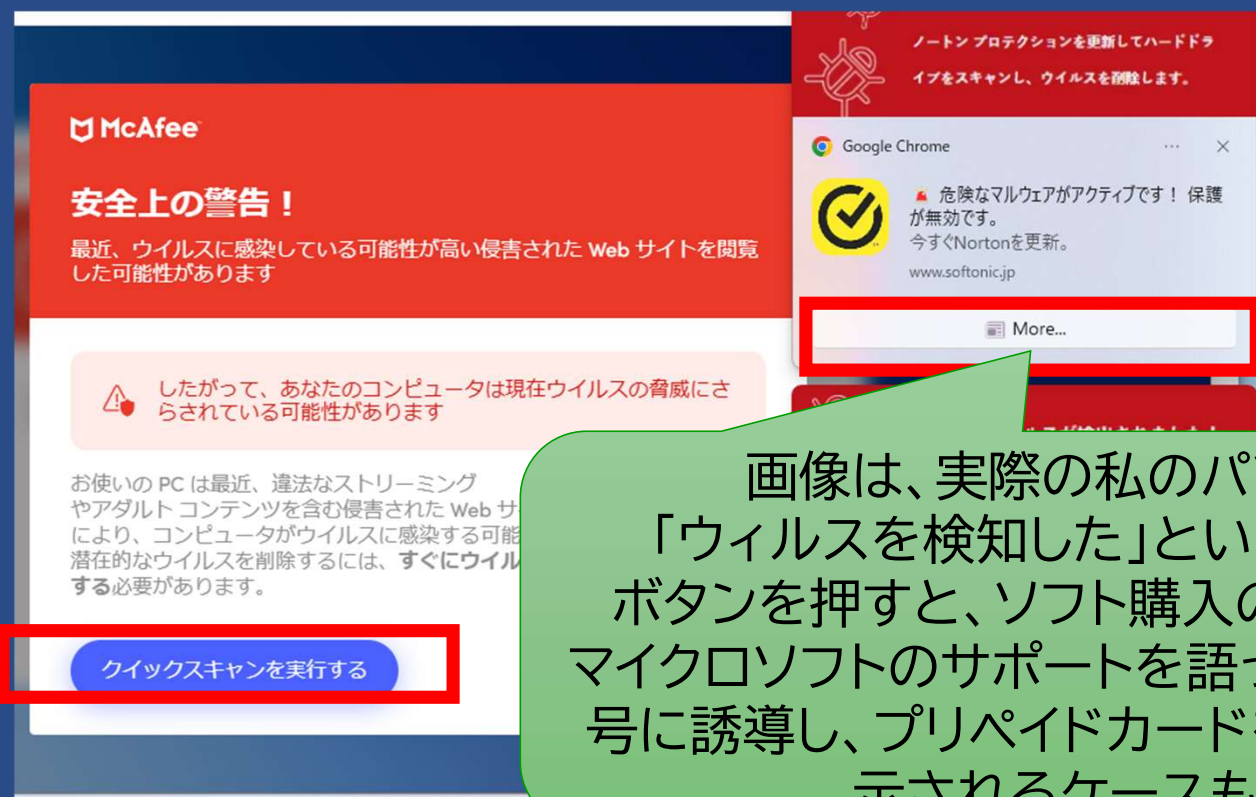


2-4. インターネットの攻撃者

悪意のハッカーの例
(一般、ビジネス)

事例2: 偽のセキュリティ警告

ウェブサイトを開覧中に突然『ウイルスを検出した』などの偽のセキュリティ警告が表示され、指示に従って電話番号に掛けたら、プリペイドカードを購入を指示されたり、攻撃者が用意したサイトに誘導され、IDやパスワード等が抜き取られたりします。



2-4. インターネットの攻撃者

悪意のハッカーの例
(一般、ビジネス)

事例3: アカウント乗っ取り

アカウントを乗っ取った犯人が、SNSの友人や公式アカウントになりすまし、メッセージを送りつけてくる手口です。投資を持ちかけられて、電子マネーの送信を促してきたり、リンクから偽のログインページに誘導され、自分のパスワードやIDが乗っ取られたりします。



※実在のアイコンや色使いを真似ているので、見た目だけで気付くことは難しい

乗っ取り被害に遭わないために
| LINEみんなの使い方ガイド
<https://guide.line.me/ja/cyber-bousai/>
より抜粋

参加者で、似た事例・あやしいと思った・被害に合ったことがある方は、何人くらいいらっしゃいますか？



2-4. インターネットの攻撃者



攻撃者は、パスワード・暗証番号を狙ってきます。

①パスワードは、なるべく複雑で長いものにしましょう

悪いパスワードの例

- 名前や生年月日などを利用したもの
- 「abcd」、「7777」など簡単に類推できるもの
- 文字数が少ないもの

英字4文字のパスワードの場合、理論上総当たりで**数秒で見破られます**。

良いパスワードの例

- 以下を組み合わせたもの
英大文字(ABC...)
英小文字(abc...)
数字(123...)
記号(!?#...)
- 文字数が多いもの
(10文字以上)

上記のパスワード(10文字)の場合、理論上、総当たりで**数百年**かかります。



2-4. インターネットの攻撃者



②パスワードの使いまわしは絶対に避けましょう

パスワードを使いまわさないためのアイデア

サービスごとに冒頭の文字を変えます

abcネット



abc

いろは銀行



irh

IPA信託



IPA

+

共通の核となるパスワードを決めます

terebiGAsuki!!06

独立行政法人情報処理推進機構『安心相談窓口だより』より抜粋

もちろん、
パスワード・暗証番号は、絶対に教えてはいけません。



2-4. インターネットの攻撃者

今日のポイント

そもそもなぜパスワード・暗証番号が必要か？
→ 認証のため。認証とは、他人に自分を認めさせること。

表. 認証の種類

1. 所有認証 本人だけが「持っている」

カード、免許証、携帯電話(スマホ)、印鑑 など

2. 知識認証 本人だけが「知っている」

パスワード、合言葉(本人しか知らない質問) など

3. 生体認証 本人だけが「備えている」

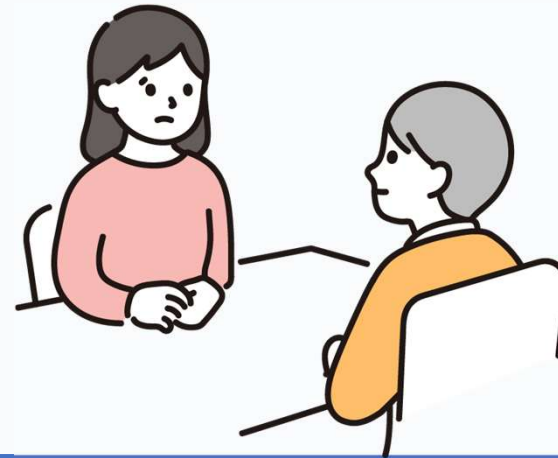
指紋、顔、声など

生体認証は
盗まれ難い

現在は、パスワードと生体認証などを組合せた
「多要素認証」が推奨されています。



不安を感じた場合の 相談先



不安に感じることがあったら



怪しいメールを受け取ったり、不安なことがある場合は、家族やいつも行く携帯ショップのスタッフ等、信頼できる人に相談しましょう

ご家族・ご友人



携帯ショップ



普段からインターネットの安全・安心な利用や、いざという時に誰に相談するのかについて周囲と話しあう機会を設けると良いでしょう。





消費者ホットライン188(いやや!)に電話をすると、地方公共団体が設置している身近な消費生活センターや消費生活相談窓口へご案内されます。

実際のトラブル事例



消費者庁ウェブサイトより抜粋

- ※ 相談は無料ですが、通話料はかかります
- ※ 電話の音声利用が難しい方は、電話リレーサービスを利用し、お住まいの地方公共団体の消費生活相談窓口等にご相談いただくことも可能です



公的な相談先も活用しましょう

情報セキュリティ安心相談窓口

IPA(独立行政法人情報処理推進機構)の運営する情報セキュリティに関する相談窓口です。電話かメールでご相談ください。

■電話:03-5978-7509

■受付時間:10:00~12:00/13:30~17:00

※土日祝日・年末年始は除く

メール:anshin@ipa.go.jp

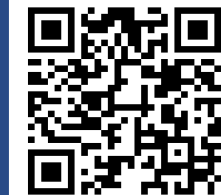
URL:<https://www.ipa.go.jp/security/anshin/index.html>

警察相談窓口

各都道府県警察本部のサイバー犯罪相談窓口、警察相談専用電話の「#9110」または最寄の警察署にご相談ください。

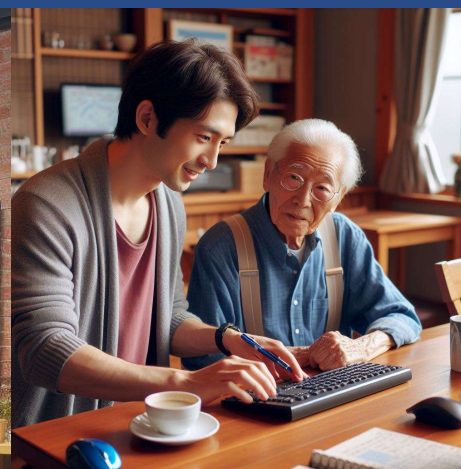
都道府県警察本部のサイバー犯罪窓口
サイバー事案に関する相談窓口 | 警察庁Webサイト (npa.go.jp)

URL:<https://www.npa.go.jp/bureau/cyber/soudan.html>



3. まとめ

これまで学んできた内容を振り返り、皆さんの意識と学びが、生活や地域をより豊かなものにしてくれることを願っています。これからもスマートフォンやインターネットを安心・安全に活用し、世代や地域を超えてともに支え合う社会を築いていきましょう。



■高齢者向けサポート・交流会

■情報セキュリティに対する意識向上



■子供・学生向けセミナー・交流会

■情報マナーやセキュリティの定着化

生成AIにより作成したイメージ

