「情報リテラシーと処理技術」
～サポート授業～

（1） 2024年11月15日（金） 18：00～21：00

（2） 2024年11月29日（金） 18：00～21：00

※このスライド資料は、2024年11月15日時点のものです。

東北文教大学　眞壁豊　makabe@g-tbunkyo.jp

「情報リテラシーと処理技術」スケジュール

- サポート授業
  - 11月15日（金）18:00-21:00
  - 11月29日（金）18:00-21:00
    - 扱う内容
      - レポート→サポート授業終了後2週間で作成～提出（予定）
- スクーリング授業
  - 12月7日（土）12:50-17:30
  - 12月8日（日）9:00-17:30
    - 扱う内容
      - 単位認定試験→12月8日の最後、筆記試験。
      - 科目試験→2024年2月頃（予定）。問題番号は「1」。

レポートの確認

- 設題
  - 電子マネーを含む**キャッシュレス決済の仕組み**について述べ、不正利用を防ぐためにどのような**対策**が必要であるかを述べなさい。また**現金決済とキャッシュレス決済**について、**それぞれの利点・欠点**を述べつつ、**キャッシュレス決済を積極的に導入すべきか否か**を理由とともに述べてください。

- 主な参考資料
  - 三木紘武（2019）『情報リテラシーと処理技術 第3版』豊岡大学短期大学部通信教育部
    第1章　情報科社会の到来・第3節（p.6-9）
    第7章　情報システムの課題・第1節～第3節（p.68-73）
  - 情報処理推進機構（2023）「情報セキュリティ10大脅威2023」
    https://www.ipa.go.jp/security/10threats/10threats2023.html
    https://www.ipa.go.jp/security/10threats/ps6vr7000000bkle-att/000072668.pdf
    （2023.12.1現在） 参考となるページ…p.16-19, p.57-68

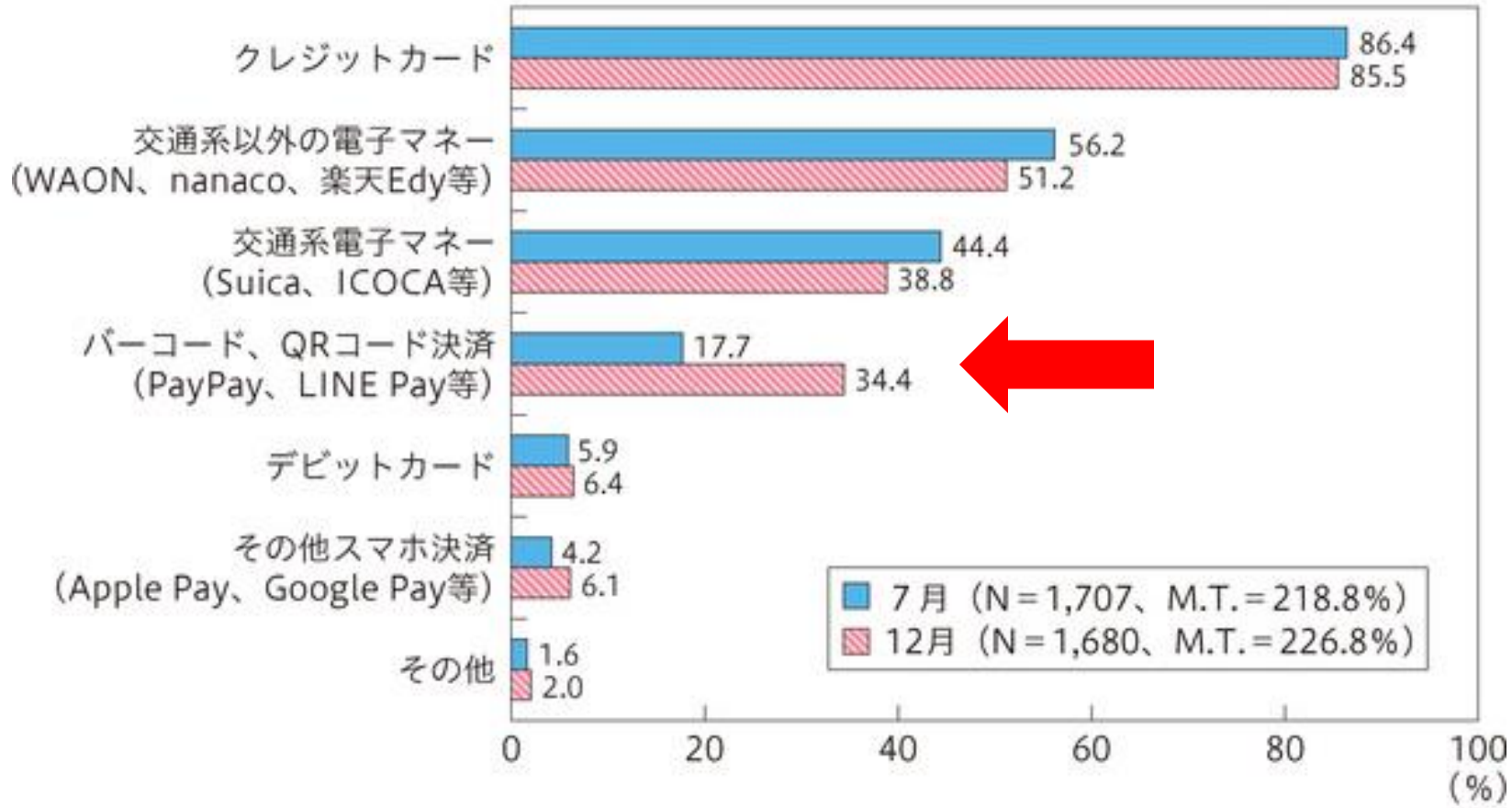
その他参考になりそうな資料（キャッシュレス決済、スマホ決済 等）

- 参議院（2016）「社会保障の安定財源の確保等を図る税制の抜本的な改革を行うための消費税法の一部を改正する等の法律等の一部を改正する法律案」
  - https://www.sangiin.go.jp/japanese/joho1/kousei/gian/192/meisai/m19203192003.htm
  - 消費税率10%引上げ時期の（変更の）決定（2017.4.1→2019.10.1）
- 経済産業省（2019-2020）「キャッシュレス・ポイント還元事業」
  - https://www.meti.go.jp/policy/mono_info_service/cashless/cashless_payment_promotion_program/index.html
  - キャッシュレス決済で最大5%還元。2019.10.1～2020.6.30
- ユーキャン（2019）「「現代用語の基礎知識」選 2019ユーキャン新語・流行語大賞 年間大賞 &トップ10発表！」
  - https://www.u-can.co.jp/company/news/1204054_3482.html
  - 「〇〇ペイ」がトップ10に入る。ノミネート語に「キャッシュレス／ポイント還元」も。

その他参考になりそうな資料（キャッシュレス決済、スマホ決済 等）

- 消費者庁（2020）『令和2年版消費者白書』p.61-62
  - https://www.caa.go.jp/policies/policy/consumer_research/white_paper/2020/white_paper_column_01.html
  - 「**キャッシュレス・ポイント還元事業**」の影響で、キャッシュレス決済の中でもバーコード・QRコード決済が伸びている。
- 総務省（2020）『令和2年版 情報通信白書』p.132-136
  - https://www.soumu.go.jp/johotsusintokei/whitepaper/r02.html
  - 第1部 第2章 第2節に、キャッシュレス決済の手法、年代別や決済手段別の利用動向について述べられている。
- 経済産業省（2024）「キャッシュレス決済について消費者に知っていただきたいこと」
  - https://www.caa.go.jp/policies/council/cepc/meeting_materials_6/assets/meeting_materials_6_240222_04.pdf
  - 資料として見やすい。キャッシュレス決済の種類別も簡潔に記されている。

【図表２】　比較的利用頻度の高いキャッシュレス決済手段



（備考）　1．消費者庁「物価モニター調査」（2019年、確報値）により作成。
2．「あなたはキャッシュレス決済をどの程度利用していますか。」との問で「よく利用している」、「ときどき利用している」、「あまり利用していない」と回答した人を対象とした「あなたが比較的利用する頻度の高いキャッシュレス決済手段は何ですか。」との問に対する回答（複数回答）。

消費者庁（2020）「COLUMN1 キャッシュレス決済に関する消費者の意識(物価モニター調査結果より)」『令和2年版消費者白書』p.61-62
https://www.caa.go.jp/policies/policy/consumer_research/white_paper/2020/white_paper_column_01.html

その他参考になりそうな資料（キャッシュレス決済、スマホ決済 等）

- 消費者庁（2021）「キャッシュレス決済の現状と消費者問題に係る実態調査について」
  - https://www.caa.go.jp/policies/policy/consumer_policy/meeting_materials/assets/internet_committee_211012_0006.pdf
  - キャッシュレス決済の種類別の説明が詳しく掲載されている。
  - それぞれのキャッシュレス決済別に、トラブル、問題・課題、注意喚起事項が簡潔に述べられている。
- 政府広報オンライン（2024）「キャッシュレス決済とは？種類や活用のメリットを解説！」
  - https://www.gov-online.go.jp/useful/article/202309/1.html
  - キャッシュレス決済についての概要、種類、メリットや不安点についてわかりやすく説明
- NHK for School「電子マネーのしくみ」
  - https://www2.nhk.or.jp/school/watch/clip/?das_id=D0005311328_00000
  - 動画で「電子マネー（キャッシュレス決済）」についてわかりやすく説明がされている。

レポートの「評価A」の基準（内容として）

- 電子マネーを含む**キャッシュレス決済の仕組み**を適切に理解し、資料そのままの表現を避けながら、適切な説明がなされている。
- **不正利用を防止するために行うべき事**を理解し、適切な**具体例**を示しながら説明がなされている。
- キャッシュレス決済の**利点・欠点**を理解し、適切な**具体例**を示しながら説明がなされいてる。
- **テキスト以外**の専門的な信頼性の高い資料収集に励み、**テキスト以外の参考文献（資料）**も活用して作成している。

コード決済（スマホ決済）、使ったことありますか？

PayPay株式会社「PayPay」 https://paypay.ne.jp/
NTTドコモ「d払い」 https://service.smt.docomo.ne.jp/keitai_payment/

作成の手引き（1）
キャッシュレス決済の仕組み

- キャッシュレス決済の種類
  - 「**前払い**」と「後払い」で大別
    - 前払い　→　**電子マネー**、**コード払い**、プリペイドカード
    - 後払い　→　クレジットカード
  - 特に「**電子マネー**」は、カードの中に「**IC（集積回路）**」が入っている。

- 電子マネーの利用者情報
  - 電子マネーを用いた**利用者情報・利用履歴**のデータが、事業者側に蓄積することで、利用者への「おすすめ（レコメンド）」の情報を出すことでさらなる利益が期待できる。
  - **販売データ**をもとにした**需要の予測**をもとに、商品の仕入れ等に活かす。（教科書p.8-9）

キャッシュレス決済の定義と決済手段

前払いや即時払いを活用することで、使いすぎを未然に防ぐことが可能

・主なキャッシュレス手段を支払のタイミングで分類すると、「前払い」「即時払い」「後払い」に分類される

・**前払い**は事前に入金した範囲内での利用となるため、**使いすぎ防止や残高管理が可能**

・コード決済は、事前入金の前払い方式の他に、クレジットカードと紐付ける後払いもあり、注意が必要

	前払い		即時払い	後払い
主な サービス 例	電子マネー 	コード決済 	デビットカード 	クレジット カード 
特徴	利用金額を事前にチャージ ※クレジットカードに紐付けの場合は後払い		リアルタイム 取引	後払い、 与信機能
規制法令	資金決済法		銀行法	割賦販売法
監督官庁	金融庁		金融庁	経済産業省

経済産業省（2024）「キャッシュレス決済について消費者に知っていただきたいこと」
https://www.caa.go.jp/policies/council/cepc/meeting_materials_6/assets/meeting_materials_6_240222_04.pdf

電子マネー

- 残高情報が入った、「ICチップ入りのカード」をかざすことで、カードの中の残高が減り、決済が完了する。

図１：接触型ICカード

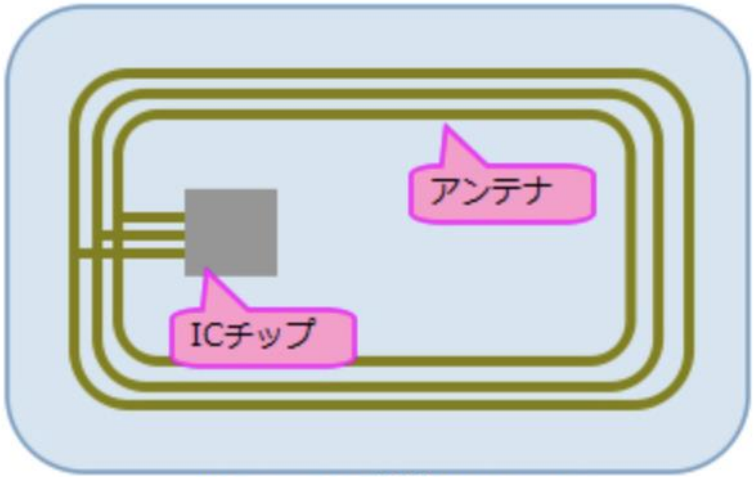


図２：非接触ICカード

※カード内部の様子

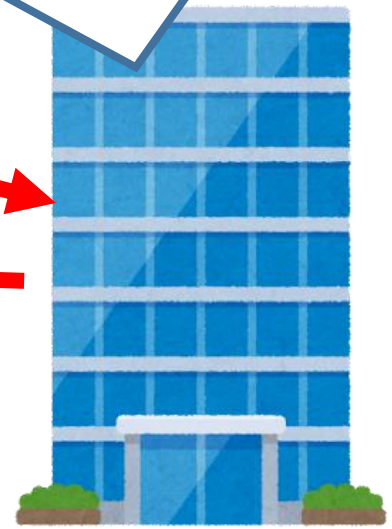
ProEngineer（2016）「実はすごい！交通系ICカードの仕組みとは？」
https://proengineer.internous.co.jp/content/columnfeature/2947

コード決済の事前準備
（残高チャージ～コード提示）

①
残高チャージの手続きを行う。
（現金、銀行口座、クレジットカード）
【ユーザーAが〇〇円チャージ】

②
コード決済会社は、
（チャージ端末やクレジット会社等とやりとりして）
ユーザーAの残高を増やす。
【ユーザーAの残高に〇〇円追加。残高△△円】

ユーザーAが、〇〇円チャージ。



ユーザーAへ、「チャージ完了。残高△△円。」
ユーザーAへ、現在のバーコード（QRコード）はこれ。

コード決済の流れ（1）

①
決済会社から
発行された、
個人に対応した
バーコードを示す

【ユーザーAが…】

②
店舗で
バーコードを
読み取る

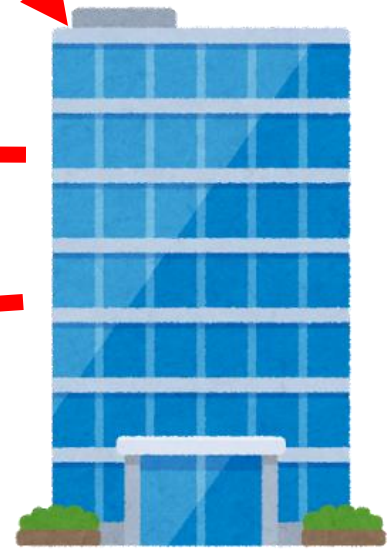
【ユーザーAが、店舗Bで〇〇円支払い】

③
コード決済会社は、
ユーザーAの残高を減らし、
店舗Bに売上を支払う。

ユーザーAが、店舗Bで
〇〇円支払い

店舗Bへ、「決済完了。売上〇〇円。」

ユーザーAへ、
「決済完了。支払い〇〇円、残高△△円。」



コード決済の流れ（2）

①
ユーザーAは、店舗BのQRコードをカメラで読み取り、金額を自分で入力。

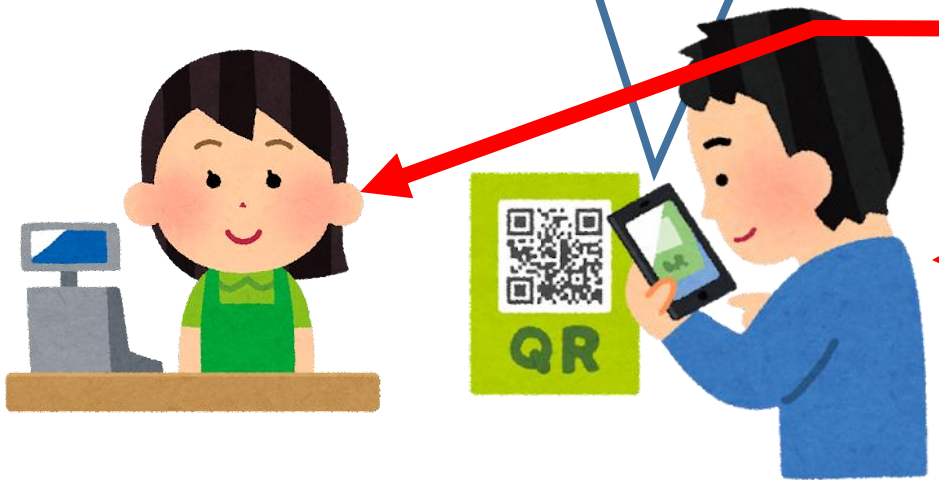
【ユーザーAが、店舗Bで〇〇円支払い】

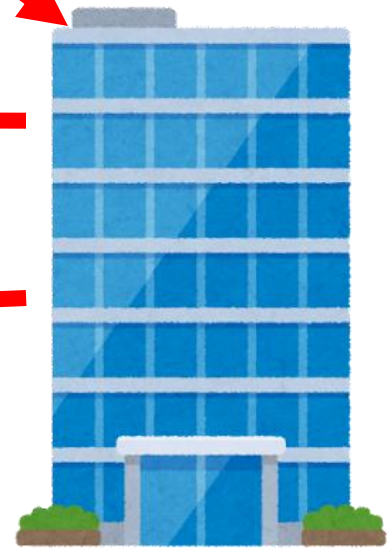
②
コード決済会社は、
ユーザーAの残高を減らし、
店舗Bに売上を支払う。

ユーザーAが、店舗Bで〇〇円支払い

店舗Bへ、「決済完了。売上〇〇円。」

ユーザーAへ、
「決済完了。支払い〇〇円、残高△△円。」





クレジットカード払い

- 消費者の「信用情報」をもとに、「後払い」とする。
  - 信用情報：職業、収入、過去の不払いなど…
    ↓この人は「信用」できる。
    「後払い」可能。
    （カード会社が代わりに支払い、後日カード会社が消費者に請求）
- クレジットカード払いの種類
  - カード情報の入力　（主にネットショップ）
    - カード番号、氏名、有効期限（mm/yyyy）、セキュリティコード（3～4桁数字）
  - カード差し込み＆暗証番号　（主に店頭）

作成の手引き（2）（3）
不正利用と、その対策

- コード決済（スマホ決済）
  - 事例
    - 2022年5月、**フィッシングメールで盗んだIDとパスワード**を使い、メルペイの決済用バーコード画像を示し、商品を不正に購入したとして被疑者逮捕。
    - 2022年9月、**auを装った偽メールを流し、IDとパスワードを不正に入手**。他人名義のアカウントを用い、auPAYで商品を不正に購入したとして、複数の被疑者逮捕。
  - 対策
    - **パスワードの適切な運用**。
    - **フィッシングメールに引っかからない**。
    - 利用していないサービスからの退会。
    - クレジットカードと併用する場合、クレジットカードの「3Dセキュア」を併用する。（3Dセキュア：決済時にSMS等にワンタイムパスワードが届き、それを入力。） など

情報処理推進機構（2023）「情報セキュリティ10大脅威2023」
https://www.ipa.go.jp/security/10threats/10threats2023.html
https://www.ipa.go.jp/security/10threats/ps6vr7000000bkle-att/000072668.pdf

作成の手引き（2）（3）
不正利用と、その対策

- クレジットカード決済
  - 事例
    - 2022年5月、株式会社machattは、「MACHATT ONLINE STORE」において2021年8月～2022年2月にかけて利用された16,093件の**クレジットカード情報流出**。一部不正利用されたおそれがあることを公表。
    - 2022年6月、「スイーツパラダイスオンラインショップ」で2021年8月から12月にかけて利用された7,645件の**クレジットカード情報が流出**。2021年12月頃、クレジットカードを利用した人から不正利用されたとの報告がtwitterに相次いでいた。
  - 対策
    - クレジットカードの「3Dセキュア」を併用する。
    - プリペイドカードの利用を検討。（利用可能限度額の範囲を限定する）
    - **利用頻度が低いサービスではクレジットカード情報を保存しない**。
    - クレジットカード利用明細の定期的な確認。 など

情報処理推進機構（2023）「情報セキュリティ10大脅威2023」
https://www.ipa.go.jp/security/10threats/10threats2023.html
https://www.ipa.go.jp/security/10threats/ps6vr7000000bkle-att/000072668.pdf

フィッシング詐欺の概要

- 実在する公的機関や有名企業を騙ったメールやSMS（ショートメッセージサービス）を送信し、**正規のウェブサイトを模倣したフィッシングサイト（偽のウェブサイト）へ誘導**することで、**個人情報や認証情報等を入力させる詐欺**である。詐取（さしゅ）された情報は悪用され、金銭的な被害が発生することもある。

情報処理推進機構（2021）「情報セキュリティ10大脅威2021」
https://www.ipa.go.jp/files/000088835.pdf

フィッシング詐欺の仕組み

正規サイト

模倣して
偽サイトを作成

偽サイト

①
攻撃者は、正規サイトを参照・模倣し、個人情報、ID、パスワードを入力させる**「偽サイト」（フィッシングサイト）**を作成する。

②
攻撃者は、**フィッシングサイトに誘導**する偽メールを送信する。

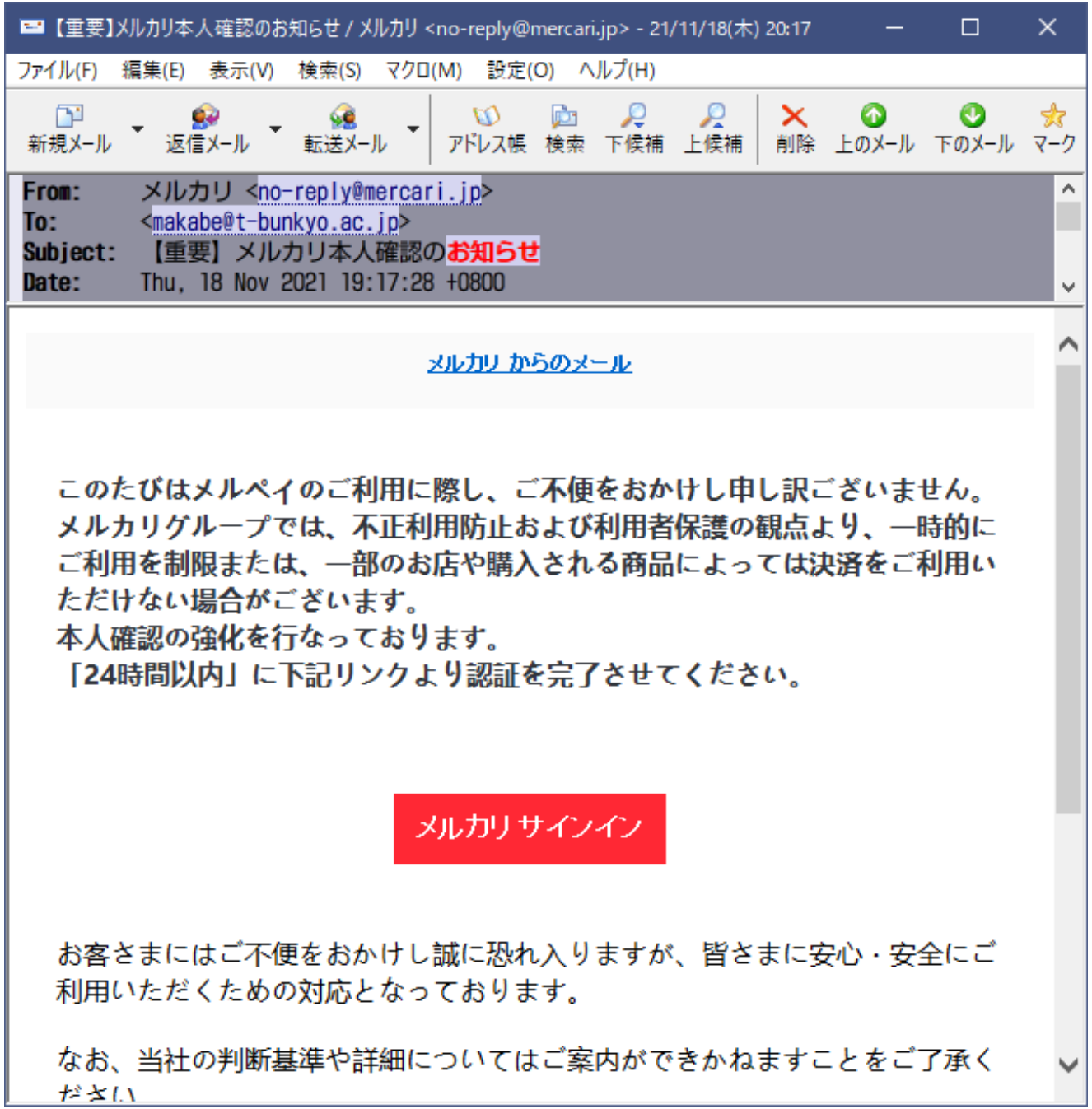
偽メール

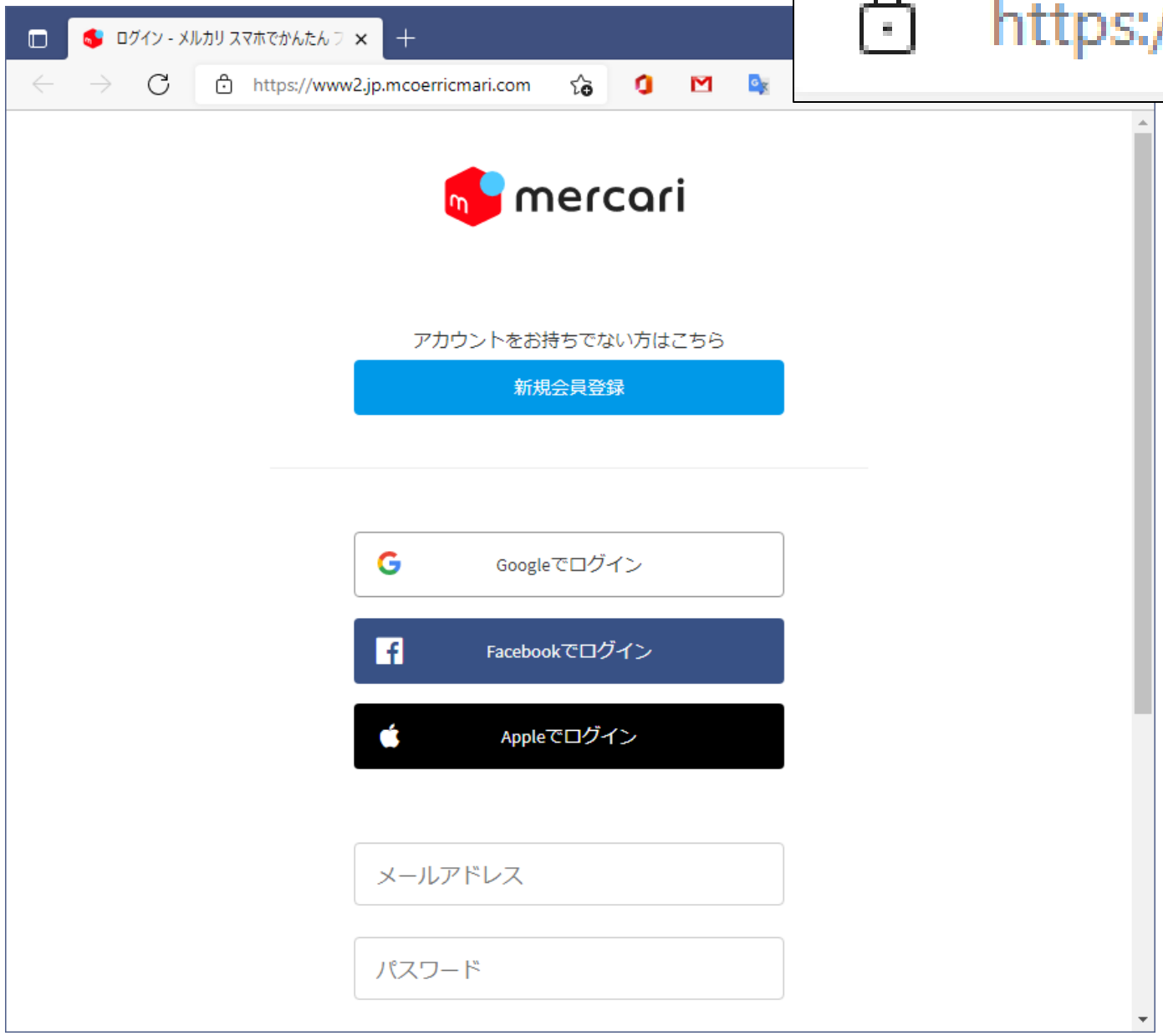
ID : hogehoge
PASS : girhsiurkgs
クレジットカード情報…

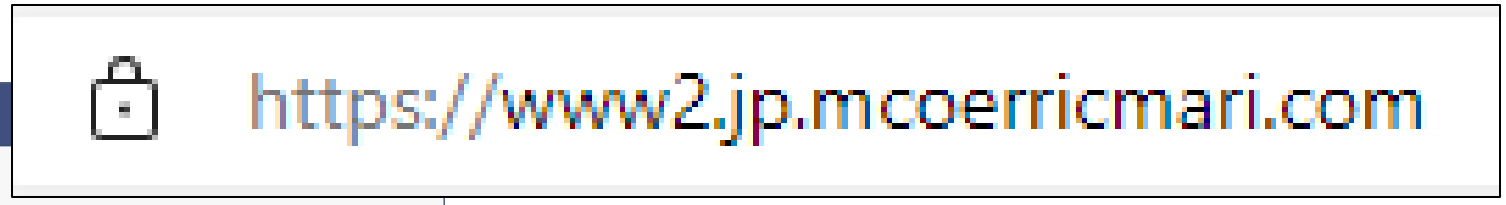
③
被害者は、偽メールの誘導で表示された偽サイトの入力欄（フォーム）に、**IDやパスワード、クレジットカード情報などの認証情報をフォームに入力してしまう**。

偽メール（フィッシングメール）の例

- **フィッシングメール**
  - 大抵は、再ログイン（IDとパスワードの入力）を促す内容のメール。
  - 「入力しないと利用停止（一次停止）になる」等と、**被害者を焦らせよう**とする。（冷静な判断を鈍らせる）
  - メールの送信元（メールアドレス）は、一見正しく見える。（**送信元メールアドレスは簡単に騙せる**）
  - リンク先のURL（アドレス）は、落ち着いて見れば偽サイトと判断できる。







アドレス（ドメイン名）に注目！

アドレス（ドメイン名）に注目！

フィッシング詐欺の事例は、日々出ている。

- フィッシング対策協議会「月次報告書」

  https://www.antiphishing.jp/report/monthly/

  - 月ごとにフィッシング詐欺の情報が報告されている。メール本文やフィッシングサイトのスクリーンショットを掲載し、事例も豊富にある。
- フィッシング対策協議会「緊急情報」

  https://www.antiphishing.jp/news/alert/

  - 随時、直近のフィッシング詐欺（偽メール、偽サイト）の報告が上がっている。

フィッシング対策協議会「緊急情報」
https://www.antiphishing.jp/news/alert/

フィッシング詐欺の防止方法

- **二要素認証**を使う
  - パスワード（記憶）が通ったら、スマホ（所持）に、コードが届くようにする。
  - パスワードが破られた際の検知にもなる。
- メール、SMS、SNSの投稿内URLを安易にクリックしない
- 公式アプリを使う
  - 公式アプリからリンクを開く
- 緊急性を煽る内容で誘導されたウェブサイト上では、重要情報をすぐに入力せず、**ドメイン名等を確認**してサイトの真偽を確かめる。

- 利用するウェブサイトの**ログイン履歴の確認**
- クレジットカードやインターネットバンキング等の**利用明細を確認**

- 被害を受けたら…
  - パスワードの変更をする
  - 利用しているサービス（や、クレジットカード）の利用停止を連絡する
  - 信頼できる機関に相談する
    - 警察、国民生活センター、地域の消費生活センター等に相談

情報処理推進機構（2021）「情報セキュリティ10大脅威2021」
https://www.ipa.go.jp/files/000088835.pdf

バイオメトリックス（バイオメトリックス認証、生体認証）

- **身体的な特徴**を用いて**個人を自動的に認証**する技術。
  - 次の3つを満足する。
    - 普遍性（誰もが持っている特徴）
    - 唯一性（本人以外は同じ特徴を持たない）
    - 永続性（時間とともに変化しない）

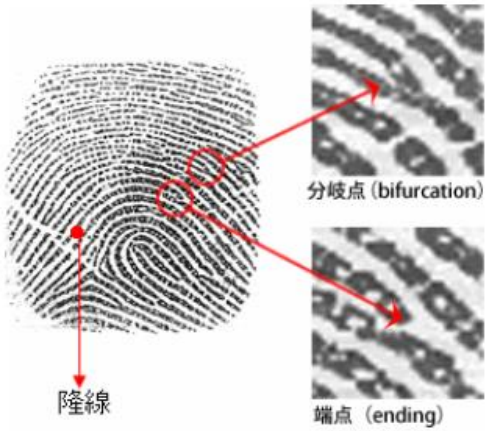
つまり、忘れることがない。
常に身に付けている。

- バイオメトリックス認証に使われる身体的な特徴（生体情報）の例
  - 指紋　（iPhoneでいう「Touch ID」）
  - 声紋（音声の特徴）
  - 指・手のひら静脈パターン
  - 虹彩（目の虹彩模様）
  - 顔認証　（iPhoneでいう「Face ID」）　など。（※「マイナ保険証」でも活用）

三木紘武（2018）『情報リテラシーと処理技術 第3版』豊岡大学短期大学部通信教育部
第7章　情報システムの課題　　特に「第2節　（3）　①バイオメトリックス」（p.69-70）

バイオメトリックス（バイオメトリックス認証、生体認証）

- 例１：指紋認証
  - 基本的に2方式。
    - 指紋の線（隆線）の**特徴的な部分**である、「**分岐**」や「**終端部分**」の位置・種類・方向などを確認する方式
    - **指紋全体（の画像情報）をデータ化**し、パターンマッチングする方式
- 特徴
  - 技術が成熟している（使いやすい）
  - 指の水分などに左右される
  - 偽造ができないわけではない（→「グミ指」）



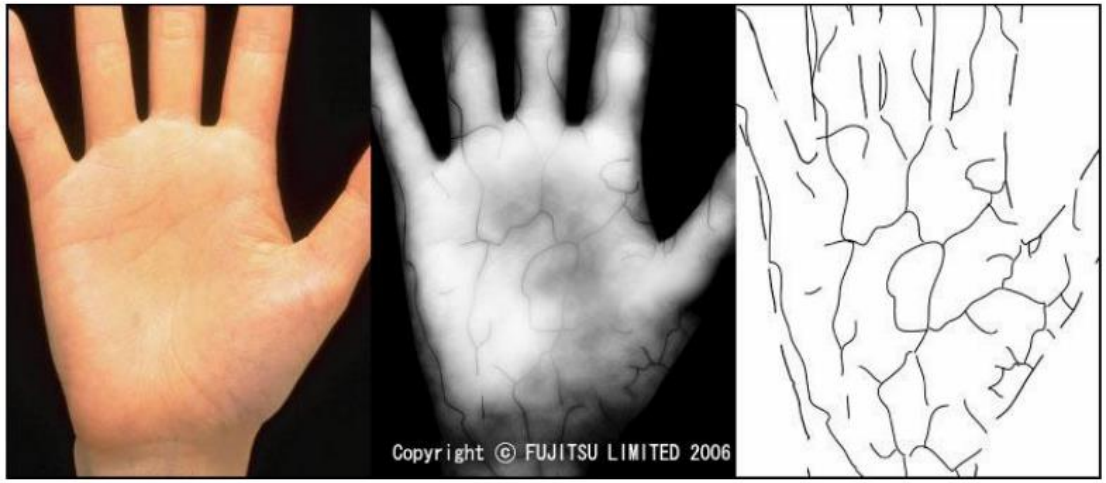
オンラインマガジン「COMZINE」2004 年 3 月号
（http://www.nttcom.co.jp/comzine/no010/dragnet/）に一部加筆

図 1-3　指紋の隆線、分岐点、端点

情報処理推進機構（2013）「生体認証導入・運用の手引き」
https://www.ipa.go.jp/security/fy24/reports/bio_sec/documents/bio_guide_24.pdf

バイオメトリックス（バイオメトリックス認証、生体認証）

- 例２：静脈認証
  - 赤外線カメラで手のひらや指を撮影し、静脈のパターンを抽出。
  - あとは指紋認証と同じように特徴部分の一致か、パターンマッチングで認証する。
- 特徴
  - 偽造が困難（情報が体の内部にある）
  - 導入コストが高い
  - 登録不可能は人が少ない
  - 認証制度が高い



(a) 一般のカメラで撮影した画像　(b) 赤外線カメラで撮影した画像　(c) 手のひらの輪郭および抽出した静脈パターン

図 1-4　手のひらの静脈パターン

情報処理推進機構（2013）「生体認証導入・運用の手引き」
https://www.ipa.go.jp/security/fy24/reports/bio_sec/documents/bio_guide_24.pdf

バイオメトリック（生体認証）による フィッシング被害防止の可能性

- 基本的にバイオメトリック（生体情報）はフィッシングによって詐取される可能性は極めて低いと考えて良い。
- 「センサー」と「本人」がいれば、比較的手間をかけずに本人認証ができる。
  - 生体情報を持つ「本人」、あるいはその「生体情報」を、フィッシング詐欺加害者が得られる可能性は低い。
- **他人による偽造はしづらい**。（**ただし「100%不可能ではない」と考えておく**。）
  - 指紋認証と、（一部）顔認証については抜け道がある？
    - いわゆる**「グミ指」で指紋認証が突破**されてしまう。ただし指紋をどう取得するかという手間を考えると比較的安全ともいえる。
    - Appleの「Face ID」（顔認証）について、顔が似ている双子を通してしまう事例あり。
  - 誘拐＆脅迫が絡む場合、本人の意志に関わらず生体認証を突破される可能性はある。
- 本当に「本人の意志」で行ったものかどうか。
  - 無意識に行っていない？
  - 「本当に自分の意志」に沿って、認証を通過させた？

「二段階認証」と「二要素認証」

- 二段階認証
  - 主に**「記憶」を2回**使う認証方法。
  - 例えば…
    - パスワード（**記憶**）と、「あなたの生年月日は？」という質問（**記憶**）
    - パスワード（**記憶**）と、「あなたの母の旧姓は？」という質問（**記憶**）
    - 暗証番号（**記憶**）と、「あなたの出身中学校は？」という質問（**記憶**）
- **二要素認証**
  - 認証の3要素「**記憶**」「**所持**」「**生体情報**」のうち、**2つの要素**を使う認証方法。
  - 例えば…
    - パスワード（**記憶**）と、SMSに送られたコード（**所持**）
    - 暗証番号（**記憶**）と、キャッシュカード（**所持**）
    - 物理的な鍵（**所持**）と、指紋認証（**生体情報**）

情報処理推進機構（2021）「情報セキュリティ10大脅威2021 知っておきたい用語や仕組み」
https://www.ipa.go.jp/files/000089490.pdf

二段階認証よるフィッシング被害防止の可能性

- パスワード1つよりはまし。
- 基本的に二段階認証は「記憶」と「記憶」（パスワード2つ、パスワードとエピソード記憶など）であるため、それら全てが（フィッシング被害等で）漏れたら、アカウントが破られてしまう。
  - 2つ目のパスワードについては、エピソード記憶（例：「母の旧姓は？」）である場合が多く、人によって尋ねられる質問が違うので、フィッシング詐欺などで破られる可能性は相対的に低い。
- そもそも、アカウント1つに対して2つの記憶を求められ、利用者にとっての利便性を阻害しており、最近は二段階認証を採用しているサービス自体少なくなっている。

二要素認証よるフィッシング被害防止の可能性

- 現在、主にさまざまなサービスで用いられている認証方式。
- 主な方式は「パスワード」（記憶）と「ワンタイムパスワード」（所持：スマートフォン）の組合せ。
  - パスワードが通った場合、ワンタイムパスワード（大抵はランダムな数字数桁）が手元のスマートフォン（SMS、あるいは事前に登録したメールアドレス）に届く。
- 意図しないワンタイムパスワードの案内が、手元のスマートフォンに届いたことで、即ち**「パスワードが破られた」ことを検知**できる。
  - **パスワードが破られただけでは、アカウントが乗っ取られることはない**。
  - **すぐにパスワードの変更をすることで、安全に対処可能**。
  - **パスワードの使い回しは避ける**。
- スマートフォンの盗難（紛失・故障）で、各種サービスにログインできない事態、あるいはアカウント事態が破られる可能性もありうる。
  - ワンタイムパスワードの送信先を複数用意しておく。
    - スマホの電話番号、スマホのメールアドレス、パソコンのメールアドレス

作成の手引き（その他）
自ら行える「被害発見方法」

- （不正な）ログイン履歴の確認
  - ログイン履歴情報を見る方法を確認しておく。
- クレジットカードやポイントの利用履歴の確認
  - 利用の１日後くらいには、クレジットカード会社のWebサービスにも利用履歴が出るので、不正な利用が無いか確認する。
- サービス利用状況の**通知機能**の利用
  - （不正な）ログインが試みられたら、メールなどで通知が届くようにする。
  - 「**二要素認証**」を設定しておく。

作成の手引き（その他）
自ら行える「被害を受けた場合の対応」

- パスワードの変更
  - パスワードが破られた場合、変更をする。
- クレジットカード（や銀行口座）の停止手続き
  - クレジットカード会社の相談窓口は24時間対応。即連絡を。
  - 銀行口座も緊急利用停止の手続が用意されている。
- 信頼できる機関に相談/被害届の提出
  - 各都道府県警察に「サイバー犯罪相談窓口」がある。

情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

- 参考
  - 情報処理推進機構（2023）「情報セキュリティ10大脅威2023」 https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf p.58

そもそも、インターネットが普及したから、問題が出てるんじゃないの？

インターネットは、もはや当たり前の環境

「インターネット」を知る

- 教科書p.60～
  「第6章 インターネットのしくみ」
  を参照しながら歴史・しくみを解説
- 人々によってネットワークを「つなげてきた」歴史である。
  - 「無条件につながる」ことを制限したい側と、バランスを探った歴史でもある。
- 「インターネット」とは(p.60)
  - 通信規約「TCP/IP」に基づいて、世界のコンピュータが相互にネットワーク化されたもの。ネットワークのネットワーク。

インターネットとは（p.60）

- 「TCP/IP」という通信規約（＝通信の約束ごと。別名“プロトコル”）に基づいて、世界のコンピュータが相互にネットワーク化されたもの。ネットワークのネットワーク。
- インターネットに接続している機器は、原則として「TCP/IP」という通信の約束ごとを守って通信している。

- 「TCP/IP」はいつ出来たの？
  - 「1970年半ば」に開発。（教科書p.61）
  - 1983年にARPANETがTCP/IPを標準プロトコルとして採用。事実上インターネットの標準プロトコルとなる。

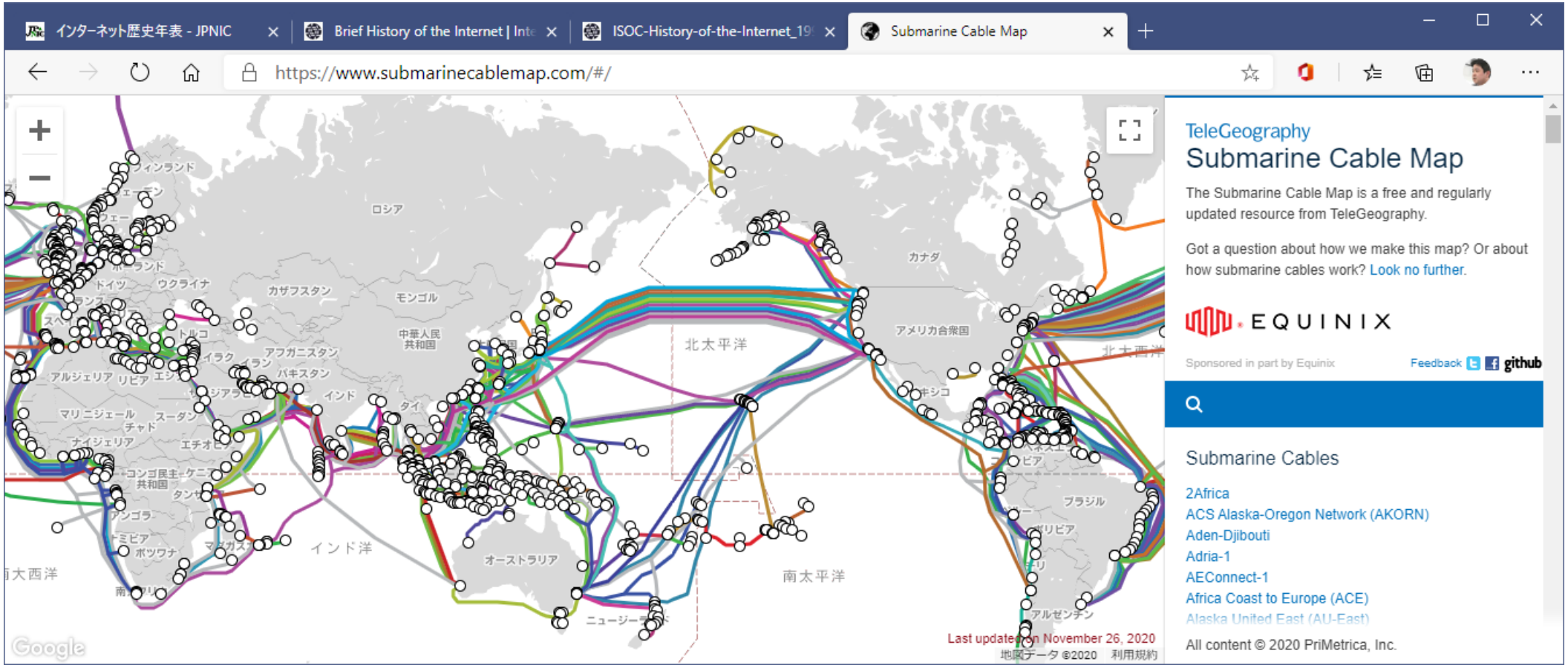
  - なぜ開発する必要があったの？　どこで開発されたの？　どう広まったの？

インターネットの歴史に関する資料

- JPNIC「インターネット歴史年表」 https://www.nic.ad.jp/timeline/

インターネットの現状を示す参考資料（1）

- 「海底ケーブル」が地球上に張り巡らされている。
  - 「Submarine Cable Map」 https://www.submarinecablemap.com

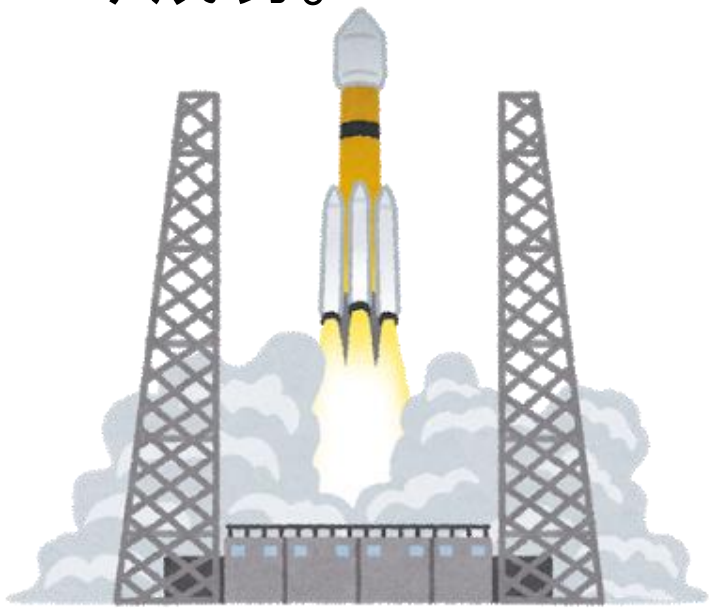


インターネットの現状を示す参考資料（2）

- 総務省「情報通信白書」
  - https://www.soumu.go.jp/johotsusintokei/whitepaper/

米ソ冷戦～ロケット競争（1945年～）

- 1945年～1989年　第二次大戦後、アメリカ・ソ連で「冷戦」状態。
  - 米ソの両者が、常に核兵器の使用ができる状態でにらみ合う。
  - 1989年、ソ連のゴルバチョフ、アメリカのブッシュが会談。冷戦の終結を発表。
- 1957年　ソ連の人工衛星「スプートニク1号」の打ち上げ成功。
  - ロケット技術＝ミサイル技術
  - アメリカは、ソ連のミサイル技術に先を越されたと自覚。
    - 「スプートニクショック」
      アメリカは、宇宙から核攻撃を受ける危険性ありと考える。



ARPANETの誕生（～1969年）

- 1958年　アメリカ国防総省、「ARPA」（高等研究計画局）を発足。
  - 最先端技術の軍事利用への転用のための研究組織
  - 1972年に「DARPA」（国防高等研究計画局）へと改称
- 1962年　ポール・バラン氏、「分散型ネットワーク」の論文を発表
  - 核攻撃を受けても持続可能な通信ネットワーク

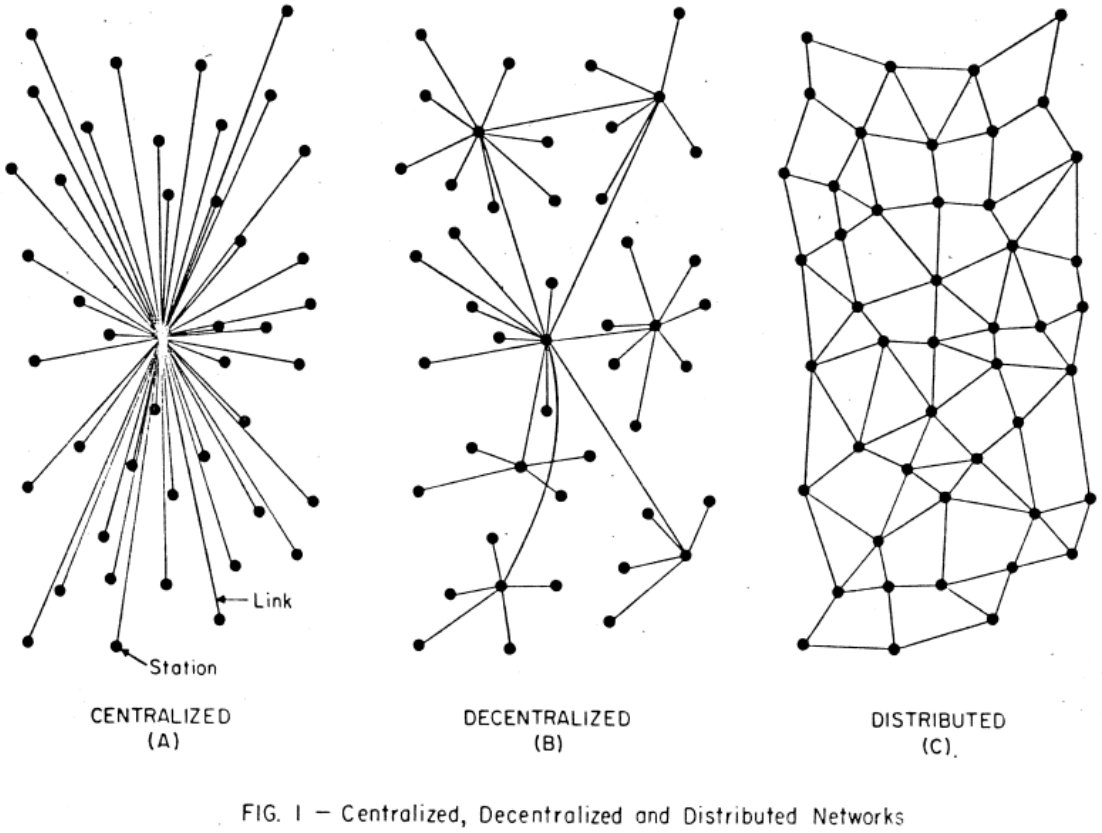
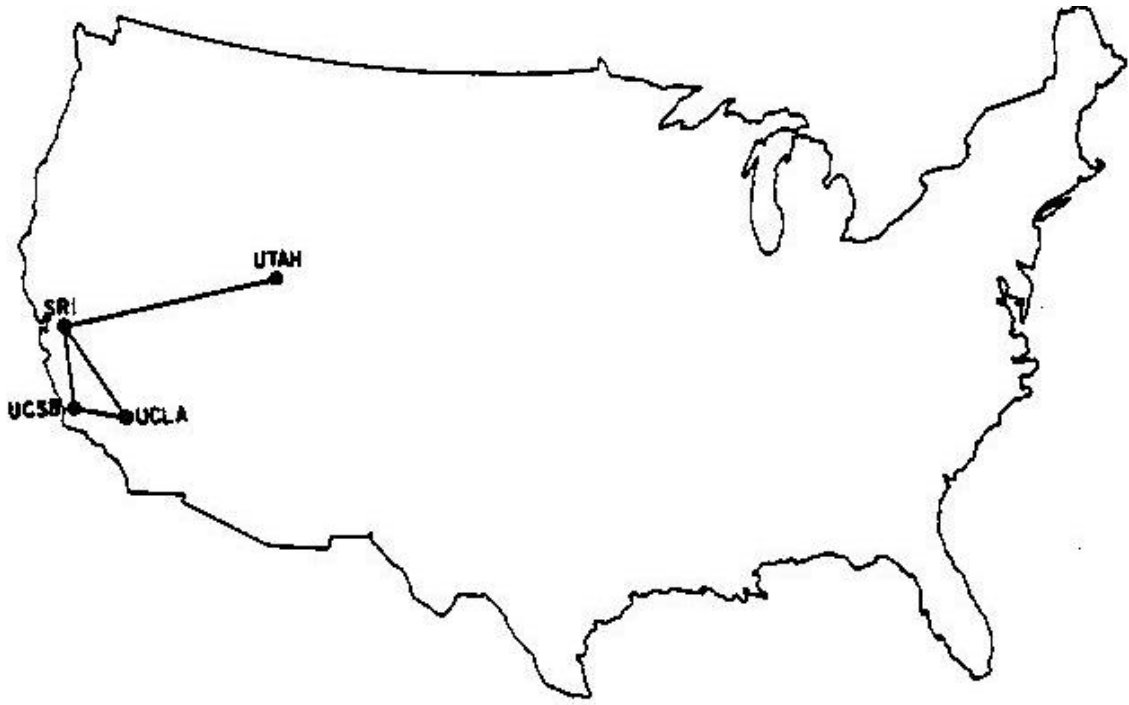


FIG. 1 – Centralized, Decentralized and Distributed Networks

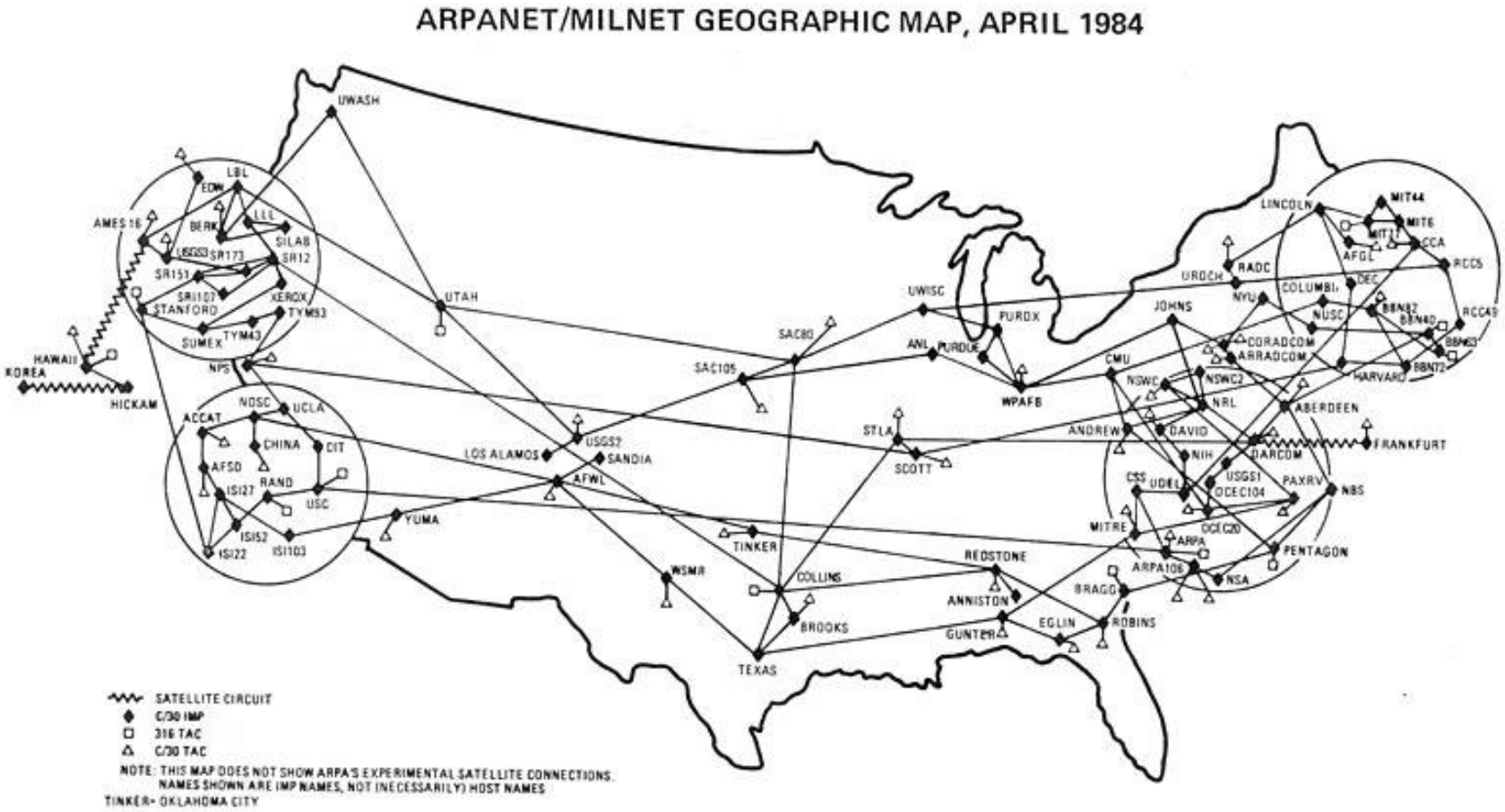
Paul Baran(1962), On Distributed Communications Networks, Rand Corporations
https://www.rand.org/content/dam/rand/pubs/papers/2005/P2626.pdf

ARPANETの誕生（～1969年）

- 1967年　アメリカ国防総省、ARPANET計画がスタート
- 1969年　「ARPANET」誕生
  - カリフォルニア大学ロサンゼルス校、カリフォルニア大学サンタバーバラ校、ユタ大学、スタンフォード研究所の４拠点が専用線で結ばれる。
- 1972年　ARPANET、北大西洋条約機構（NATO）域へ拡大
  - イギリス、ノルウェー。初の国際間接続



1984年、ARPANETなどの接続状況

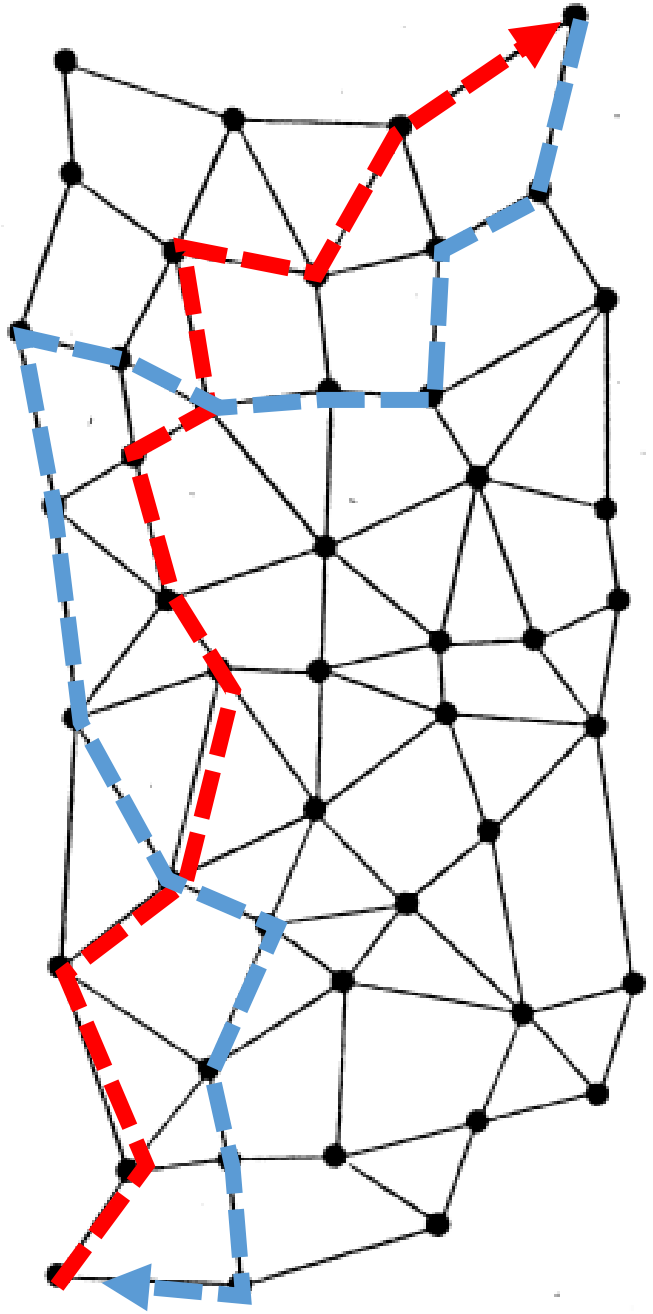


https://commons.wikimedia.org/wiki/File:ARPANET_-_MILNT_Diagram_1984.jpg

「パケット交換方式」とは？（教科書p.63）

- 中央に接続を集中させない
  - 中継点が無くなったら迂回すれば良い
- データを小分け（パケット）にする
  - データが消えたら、消えた部分だけ送り直せば良い。
- どのノード（中継点）を通っても良い
  - 最終的に全てのパケット（データ）が届けば良い。

- つまり、１本の線に複数の「送り主」や「届け先」のパケット（データ）が混在しても良い。

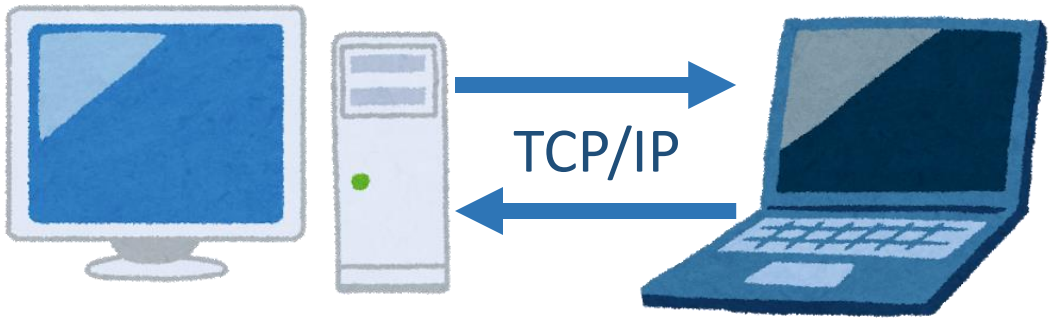


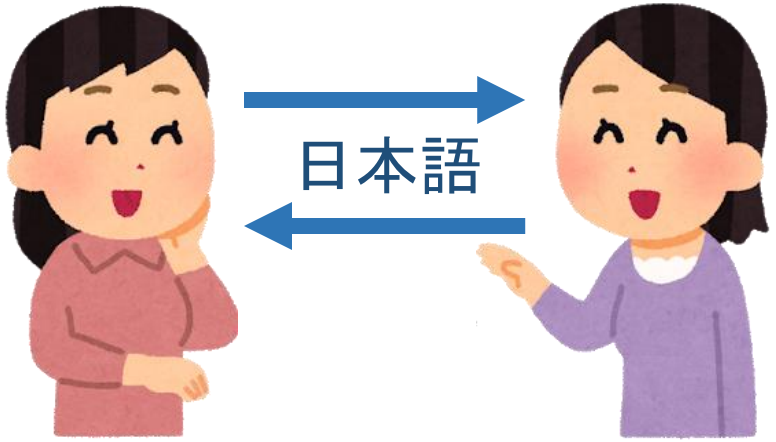
TCP/IPの誕生～インターネットの標準化（1973～1983年）

- 1973年　DARPAのロバート・カーン氏と、スタンフォード大学のヴィントン・サーフ氏の共同で、TCP/IPの最初のバージョンが発表。
- 1981年　ARPANETに未接続の各大学が、独自に大学間ネットワークの運用を始める。「CSNET」、「BITNET」が開始。
  - 後に、1986年にCSNETが「NSFNET」として名称変更。
- 1982年　電子メール（Eメール）が標準化。
- 1983年　ARPANETから軍事部門（MILNET）を分離。
  - ARPANETが、大学間の研究ネットワークが中心となる。
- 1983年　ARPANETでTCP/IPが標準プロトコルとして採用。事実上のインターネット標準プロトコルとなる。

“プロトコル”とは

- コンピュータ同士の通信の約束事。
- 互いのコンピュータで、プロトコルを合わせないと通信できない。
- インターネットで使われている標準プロトコルは「TCP/IP」。
- もちろん、現在使用されているパソコンやスマートフォン、インターネットを使用するゲーム機にも搭載されている。





日本のインターネットの夜明け（1984年～）

- 1984年　村井純氏が中心となって、３大学を結んだ「JUNET」（Japan University Network）を運用開始。
  - 慶應義塾大学、東京大学、東京工業大学。
    - この時点ではNTTではなく“電電公社”（国営）。
    - コンピュータを電話回線に接続することは「違法」だった。
- 1985年　電電公社が民営化。「NTT」となる。
- 1986年　JUNETとNSFNET（旧CSNET）が相互接続。
  - 日本とアメリカが接続。

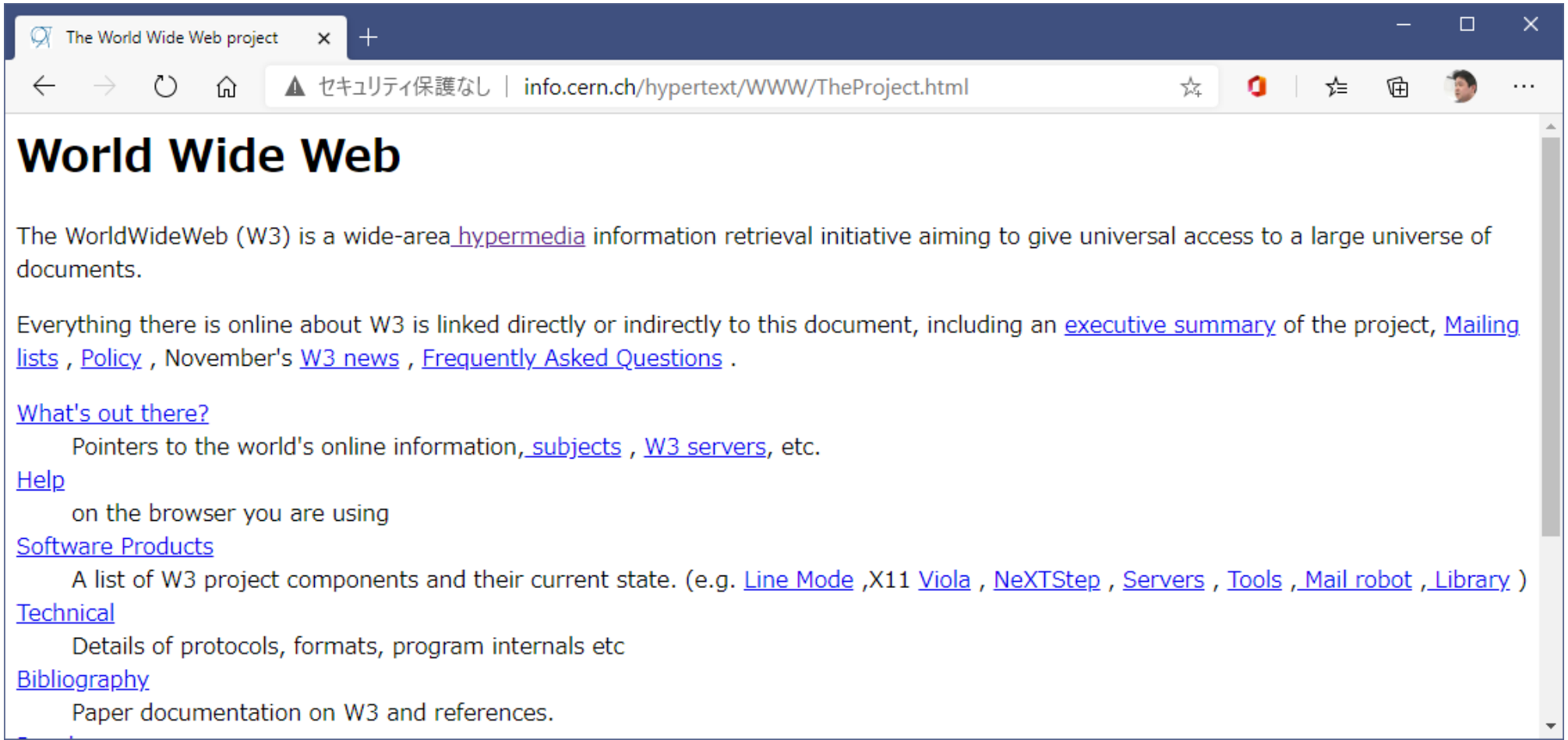
https://www.flickr.com/photos/35034362831@N01/4059709231

商用インターネットと、World Wide Webの夜明け（1989年～）

- 1989年　世界初の商用インターネット接続サービス「PSINet」が設立。
- 1989年　CERN（欧州原子力核研究機構）が、Webページ記述法である「HTML」の原型となる提案が公開。後に「World World Web」となる。
- 1990年　ARPANET終了。
  - 営利団体のインターネットへの参入が可能に。
- 1991年　CERNのティム・バーナーズ・リーにより、世界初のWebサイトが誕生。世界最初のブラウザ「World Wide Web」がリリース。
- 1992年　日本で初のWebサイト誕生。同年、商用インターネット接続サービスが開始。翌1993年、日本の郵政省がインターネットの商用利用を許可。
- 1993年　イリノイ大学のNCSAより、画像が表示できるブラウザである「Mosaic（モザイク）」が公開され、世界で爆発的に普及する。
  - 以後、Webサイトとブラウザによるインターネット活用が当たり前となる。

世界最初のWebサイト

- http://info.cern.ch
- http://info.cern.ch/hypertext/WWW/TheProject.html



一般へのインターネット普及元年（1995年～）

- 1994年　米「Yahoo!」誕生。
- 1995年　「Windows95」発売。TCP/IPが標準採用。
  - 同年、ブラウザの「Internet Explorer」が登場。
- 1995年　「amazon.com」サービス開始。
- 1996年　「Yahoo! Japan」サービス開始。同年、インターネット接続サービスとしてNECが「Biglobe」、NTTが「OCN」の名称でサービス開始。
- 1997年　NTT、検索サービス「Goo」サービス開始。
- 1997年　検索サービス「Google」サービス開始。
  - 翌年、Googleを法人化。
  - 参考：「Google八分」
    - Googleに掲載されない　＝　検索結果に表示されない　＝　ネットに載っていないのと同じ

あとは「Web」を通じて、どこ宛てに、どういうデータを送るか考えるだけ。

サービス主導の時代の幕開け。

携帯電話が主導となる時代は2000年前後から。

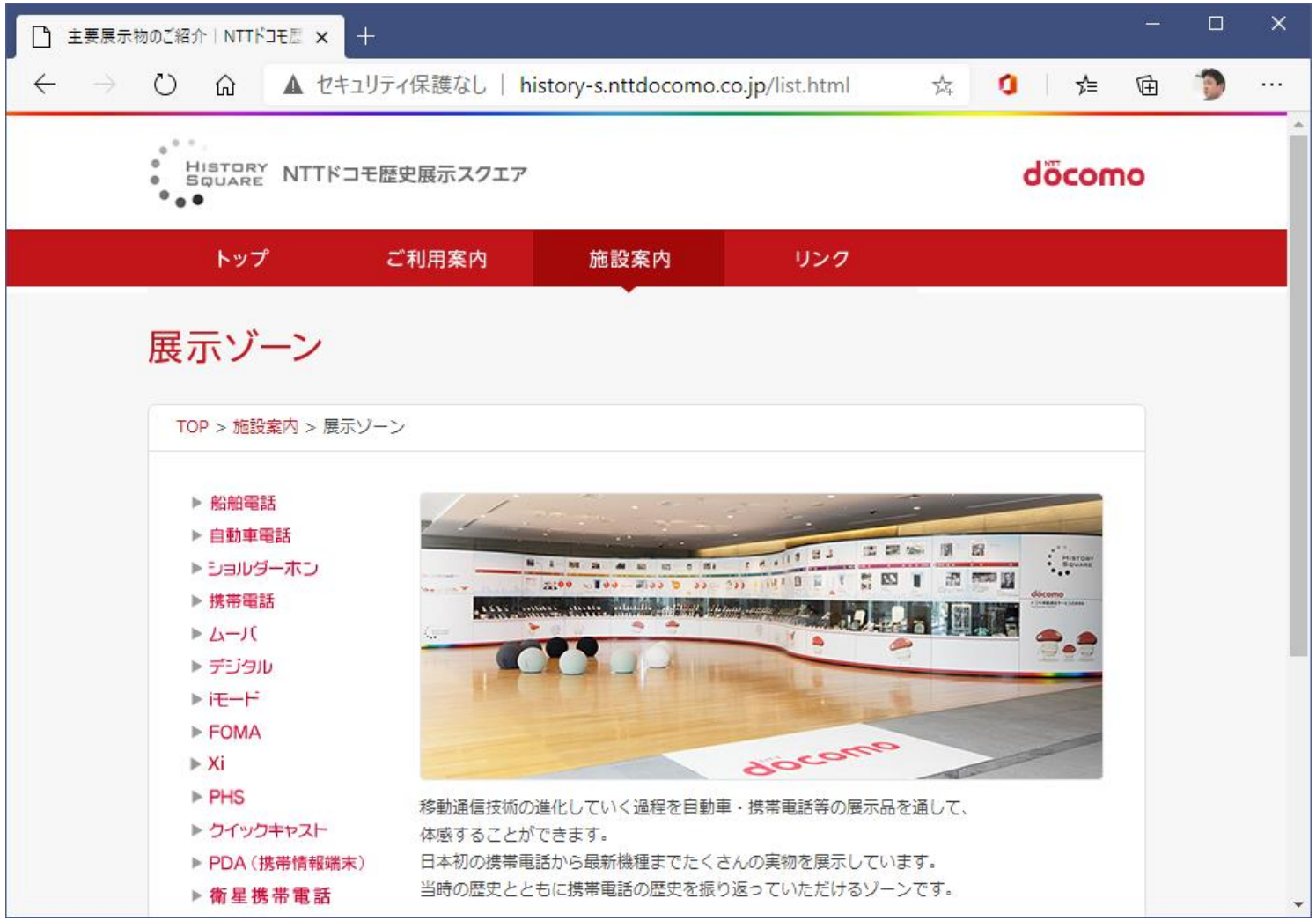
その後のインターネット、携帯電話の時代（1999年～）

- 1999年　NTTドコモ「iモード」サービス開始。
  - 携帯電話がネット端末になる。（インターネットメール、簡単なWebへアクセス）
- 2000年　カメラ内蔵携帯電話発売。
  - 翌2001年、J-PHONE（現：ソフトバンク）が、画像をメールで送れるサービスを「写メール」として売り込んだ。
- 2004年　米「facebook」創業。
- 2005年　米「YouTube」サービス開始
  - 翌2006年、Googleが買収。
- 2006年　JR東日本、2001年から運用していたSuicaを携帯電話に内蔵できる「モバイルSuica」サービス開始。
- 2006年　「ニコニコ動画」サービス開始。
- 2006年　米「twitter」サービス開始。
- 2007年　米アップル、「iPhone」発表～発売。
- 2008年　米Google、スマートフォンOSの「Android」発表。

インターネットの歴史～ここまでのあらすじ

- 1969年　アメリカ、国防総省による「ARPANET」誕生
  - 軍事と大学等が主体 → 後に軍事関係が抜け、大学等の研究機関が主体に。
- 1973～1983年　「TCP/IP」開発～標準化
- 1984年　日本、「JUNET」誕生
- 1986年　日米相互接続
- 1990年～　アメリカをはじめ、インターネットの商用利用が開始
- 1991年　「World Wide Web」誕生
  - 誰もが手軽にネット上の情報を手軽に閲覧できるように。
- 1999年　NTTドコモが「iモード」サービス開始
  - 誰もが携帯（ケータイ）を持ち、ネットに接続する時代へ
- 2007年　米Apple「iPhone」発表～発売。スマートフォン時代の幕開け

携帯電話の歴史、「世代」



http://history-s.nttdocomo.co.jp/list.html

携帯電話の歴史、「世代」(1)

- 1979年　自動車電話
  - 保証金20万円、月額基本料3万円、6秒10円
- 1985年　ショルダーホン
  - 重量3kg
- 1987年　携帯電話サービス開始(第1世代携帯電話)
  - アナログ電波による通話。重量900g。
- 1993年　第2世代携帯電話
  - 通信方式がデジタルに。(9.6Kbps)
  - ここから先、デジタル通信方式の変更による通信速度の上昇が「世代」の交代となる。
- 1995年　PHSサービス開始
  - 携帯電話とは別の電波によるデジタル通信方式。家庭のコードレス電話の技術を流用。
  - 現在は新規受付終了。2023年サービス終了予定。
- 1996年　PHSがショートメッセージ・サービス(SMS)開始
  - 1997年には、全ての携帯電話会社がSMSを開始。

携帯電話の歴史、「世代」(2)

- 1999年　NTTドコモ「iモード」開始
  - 同年にauが「EZweb」、翌2000年にJ-Phone(現ソフトバンク)が「J-スカイ」を開始。
  - 携帯電話の画面で簡易Web(文字＋画像)を閲覧できるようになる。
- 2001年　第3世代携帯電話
  - より速いデジタル通信方式に。(数百Kbps～数Mbps)
  - 2006年、JR東日本が2001年から運用していた「Suica」を携帯電話に内蔵できる「モバイルSuica」のサービスを開始。
  - 2007年、米Apple「iPhone」発表～発売。翌2008年に米GoogleがスマートフォンOSの「Android」発表。スマートフォンの時代が到来。

- 2010年　第3.9～4世代携帯電話
  - 4G(G:Generation…世代)(数十Mbps～数百Mbps)
  - LTE:Long Term Evolution
- 2020年　第5世代携帯電話
  - 5G(数百Mbps～数十Gbps)
  - 超高速、大容量。超低遅延、多地点同時接続。

ユビキタスコンピューティング
モノのインターネット（p.75～77）

- 「いつでも、どこでもコンピュータ」
  - 誰もがコンピュータ（パソコン、スマホ）を持つ。
  - 商品という商品にICタグが付く。
  - モノというモノに、ネット接続環境が付く。
  - いつでも、どこでも、インターネットから便利なサービスを受けられる。

- モノのインターネット（IoT：Internet of Things）
  - あらゆる「モノ」の1つ1つに、インターネット接続環境が付けられ、生活が豊かになり、産業が活発化される。
  - スマート家電
    - スマートスピーカー、スマートロック　など
    - スマート家電の例（ビックカメラ）
      - https://www.biccamera.com/bc/c/topics/smart_kaden/index.jsp

IoT（Internet of Things：モノのインターネット）

- あらゆる「モノ」の1つ1つに、インターネット接続環境が付けられ、生活が豊かになり、産業が活発化される。

IoTの例
～農業で温湿度・土壌水分量などの環境データを取得

ソフトバンク（2018）「農業用IoTソリューション「e-kakashi」を稲作に活用、ベテラン農家の栽培技術を新規参入者へ効率的に継承」
https://www.softbank.jp/biz/customer-success-stories/201807/town-yosano/

IoTの例
～Googleマップの交通（混雑）状況

- 人々が身につけているスマートフォンの位置情報をGoogleが集約。道路の混雑具合を「Googleマップ」へ表示。
  - https://maps.google.co.jp/
- 99個のスマートフォンをカートで引っ張り、わざと「混雑情報」を人工的に偽装する実験をした人も。
  - http://www.simonweckert.com/googlemapshacks.html