ICT基礎知識

テクノロジ領域Ⅱ

19. ヒューマンインタフェース～23. セキュリティ

テクノロジ領域Ⅱ

19. ヒューマンインタフェース

50. ヒューマンインタフェース技術

【目標】

- ヒューマンインタフェースの特徴を理解する。

【説明】

- ✓ ヒューマンインタフェースの特徴と、その代表的なインタフェースであるGUIについて、各構成要素の特徴を理解する。

50.（1）． ヒューマンインタフェース （1/2）

【ヒューマンインタフェース】

- コンピュータとその利用者（通常は人間）との間で、情報をやりとりするためのインタフェースをヒューマンインタフェースという。

＜ヒューマンインタフェースを考慮する側面＞

① 身体的側面
② 頭脳的（情報的）側面
③ 時間的側面
④ 環境的側面
⑤ 運用的側面

- 頭脳的（情報）側面においては、利用者個人により異なる選択的知覚*1を考慮し、ユーザ操作の分析が重要となる。ユーザ操作の分析を行い、コンピュータの動作を人間に近づけることによって、ユーザビリティやアクセシビリティの向上を目指す。

*1：自分にとってわかりやすい情報だけを知覚的に受け入れること。

50.（1）． ヒューマンインタフェース （2/2）

【ヒューマンインタフェースを実現する要件】

- ヒューマンインタフェースを実現する要件として、次の事項がある。

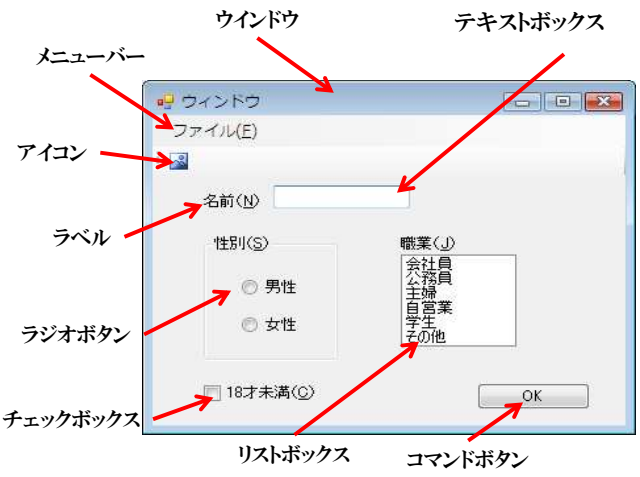
項　目	内　　容
ユーザビリティ	その製品が、心理的適合性（ストレスや戸惑いを感じることなく、なるべく簡単な操作で利用可能であること）が高いかどうかを表す。
アクセシビリティ	その製品が、身体的適合性（どの程度広範囲の人（特に高齢者や障がい者など）が利用可能であること）が高いかどうかを表す
インタラクティブシステム	人間に近い振る舞いを行うシステムをいう。人間の目や耳に相当する入力デバイスを使用して、音声認識や画像認識、動画認識、特徴抽出など、人の動きに近い動作を行う。
自然言語インタフェース	人が使う言語を解釈するヒューマンインタフェースをいう。
ノンバーバルインタフェース	言語以外（身体動作や生理的行為など）の方法（ノンバーバルな動作）を解釈するヒューマンインタフェースをいう。

50.（2）． GUI

【GUI（Graphical User Interface）】

- 出力にグラフィックを多用し、マウスなどのポインティングデバイスで操作が行えるユーザインタフェースをいう。

＜GUIの構成要素＞



その他のGUI	
ポップアップメニュー	利用者がマウスやタッチで指示した位置に出現する操作メニューをさす。
サムネイル	画像を縮小して表示したものをさす。
ヘルプ機能	操作方法や用語などを、画面上で確認できる操作ガイドをさす。

19. ヒューマンインタフェース

51. インタフェース設計

【目標】

- インタフェース設計の考え方を理解する。

【説明】

- ✓ 人とシステムの接点となるインタフェースが、使いやすさや理解しやすさを大きく左右することを理解し、望ましいインタフェースの考え方を理解する。

51.（1）． 画面設計・帳票設計 ① 画面設計

【画面設計】

- 画面を設計する際には、利用者の立場に立った使いやすい画面構成を設計することが重要である。

機　能	内　容
カーソルの移動方法	入力順序にそって左から右、上から下へ移動する
重要項目の強調	大きさ、太字、色、罫線などで強調する
グループ分け	複数の項目がある場合はグループに分ける
音声警告	入力等のエラー発生時に音声警告を入れる
ヘルプ機能	画面の機能を解説したヘルプを用意する
ファンクションキー	機能を1つにまとめたファンクションキーを用意する
ポップアップメニュー	必要な時だけメニューを表示するポップアップメニューを用意する

51.（1）． 画面設計・帳票設計 ② 帳票設計

【帳票設計】

- 出力を印刷物で行う場合に、印刷物の内容を誰にでもわかりやすく、見やすくすることが重要である。

機　能	内　容
レイアウト	複数の帳票が存在する場合でも、全体的なレイアウトは統一する。
順序と位置	項目間の関係を考慮して、順序や位置を設定する。
見出し	印刷内容を適切に表現した見出しをつける。
日付	作成日、報告日、承認日等の日付を明確に区別する。
配置	数値データが並ぶ場合など、適当な適切な区切り（カンマ）を配置する。
スペース	ゆとりを持たせた適切なスペースをとる。
表やグラフ	関係する表やグラフは1枚にまとめる。

51.（2）． Webデザイン

【Webデザイン】

- Webデザインにおいて、訪問者の誰もが同様に情報を取得できるアクセシビリティは、重要な要素であり、Webページの作成にあたって、誰にとってもアクセスしやすく、使いやすいデザインにすることは重要である。

＜Webデザインにおけるユーザビリティ＞

- スタイルシートなどのフレームを活用し、全体のデザインを統一する。
  - ・CSSでHTML文書やXHTML文書にスタイルシートを適用するには、大きく分けて以下の3つの方法がある。
    - <link>要素で外部CSSファイルを呼び出して適用する。
    - <style>要素で文書単位に適用する。
    - 要素にstyle属性を追加して局所的に適用する。
- サイトマップやサイト内検索機能などを用意し、必要な情報にアクセスしやすくする。
- サイト内で迷子にならないように、パンくずリストなどを用いてナビゲーションする。
- 音楽や大きな画像を、そのまま設置してページ全体が重くならないように、見たい聞きたい人だけが確認できるようにする。
- 一部の環境だけでしか表示できないのではなく、Webブラウザの種類に関係なく同じようなレイアウトで表示できるようにする（クロスブラウザ）。

51. (3). ユニバーサルデザイン ①

【ユニバーサルデザイン】

- 年齢、文化、言語、国籍の違いや老若男女、障がいの有無を問わず、できる限り多くの人が快適にシステムを利用できるように設計する考え方をいう。

  例）“〒”は日本人でないと意味がわからないので、利用を控える

＜ユニバーサルデザインの7原則＞

① 誰でも使えて手にいれることが出来る（公平性）
② 柔軟に使用できる（自由度）
③ 使い方が簡単にわかる（単純性）
④ 使う人に必要な情報が簡単に伝わる（わかりやすさ）
⑤ 間違えても重大な結果にならない（安全性）
⑥ 少ない力で効率的に、楽に使える（省体力）
⑦ 使うときに適当な広さがある（スペースの確保）

20. マルチメディア

52. マルチメディア技術

【目標】

- 音声や画像の符号化の種類と特徴を理解する。
- 情報の圧縮と伸張の特徴を理解する。

【説明】

- ✓ マルチメディア技術によって、コンピュータ上で文字、音声、画像などの情報を統合的に扱えるようになったことを理解する。また、マルチメディアの代表的なファイル形式の特徴や情報の圧縮・伸張について理解する。

52.（1）． マルチメディア （1/2）

【マルチメディアとハイパーメディア】

- マルチメディアとハイパメディアを区別する。

名　称	内　　容
マルチメディア	• データを受信しながら同時に再生を行うストリーミングなどのように、文字、画像、動画、音声などの情報を統合して扱う。 • 利用者の操作に応じて情報の表示や再生の仕方に変化が生じる双方向性(インタラクティブ性)を持つ。 • 文字、画像、動画、音声などの統合という概念があり、オーサリング環境を利用して作成する。
ハイパーメディア	• 文書(text)を超越(hyper)したという意味を持ち、関連する情報を含んだ文書同士をリンクしているハイパーテキストから成る。 • 画像、音声、動画などを含む様々な種類の情報を扱う機能を追加し、これらを相互に対応付けた情報の集合体を表現する。 • 文書や情報が相互に関連付けられているという概念があり、Webコンテンツ やPDFとして構築される。

52.（1）． マルチメディア （2/2）

【マルチメディア技術】

- マルチメディア技術は、発展している。

名　称	内　　容
DRM Digital Rights Management	デジタルデータの著作権管理技術のことで、インターネットやCD-ROMなどを通して配信される音楽や画像の違法コピーや配布を防止するために、電子透かしを埋め込んだり、コンテンツを暗号化して再生ソフトで復号させたりするなどの対策をしている。
CPRM Content Protection for Recordable Media	DVDなどに採用されている、記録メディア向けの著作権保護技術の一つで、コンテンツのデジタルコピーをメディアに記録する際の一度だけ許容し、メディアから他の 機器やメディアへのコピー(ダビング)を禁じる「コピーワンス」を実現する。
HTML5	HTML文書を作成する機能が改良されているのに加えて、 Webアプリケーションを開発するための様々な仕様が新たに盛り込まれている。 今までプラグインなどのHTML以外の技術を併用しないと実現できなかった機能のいくつかが、 比較的シンプルに実現できる。

52. (2). マルチメディアのファイル形式 (1/4)

【音声処理】

- 音声データをデジタル化する方法の一つに、PCM(パルス符号変換)がある。

＜代表的な音声ファイル形式＞

名　称	内　容
MIDI Musical Instrument Digital Interface	電子楽器の演奏データをデジタル転送するための規格。 ファイルフォーマットのほか、インタフェースや通信プロトコルの規格も存在する。
WAV Waveform Audio Format	MicrosoftとIBMが開発し、主にWindowsで使用される音声データフォーマット。 通常は圧縮なしで保存される。
MP3 MPEG Audio Layer-3	もともとは、映像データ圧縮方式のMPEG-1で利用されていた、音声データ圧縮形式。 非可逆圧縮方式で、高い圧縮率を誇る。

52. (2). マルチメディアのファイル形式 (2/4)

【静止画処理】

- 画像情報は、色の3原色(Cyan、Magenta、Yellow)や光の3原色(Red、Green、Blue)で構成され、画像表現は、画素(ピクセル)、解像度、階調などに影響される。

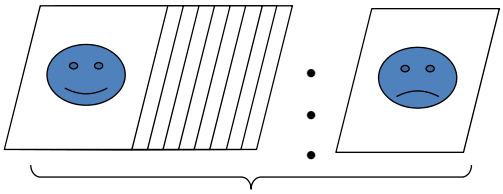
＜主な静止画像形式＞

形式名	内　容
JPEG	ISOが制定した静止画像データの圧縮方式の一つ。圧縮の際に、若干の画質劣化を許容する方式と、まったく劣化のない方式を選ぶことができる。
GIF	256色までの画像を保存することができ、イラストやアイコンなどに向いている。透明色の背景と重ね合わせることができるなどの拡張仕様がある。
PNG	GIFに代わってWWW上で広く使われることを目指しGIFの機能を拡張し新たに開発された画像形式である。
BMP	Windowsが標準でサポートしている画像形式で、白黒の画像からフルカラーまでの色数を指定できる。基本的には無圧縮で画像を保存する。

52.（2）． マルチメディアのファイル形式 （3/4）

【動画処理】

- 少しずつ変化した静止画を、1秒間に30コマ以上（フレームレート30fps）の速度で、順に表示すると、人間の目にはあたかも動いているかのように見える。動画は、この仕組みを利用している。



動画の仕組みはパラパラ漫画と同じ

＜代表的な動画ファイル形式＞

形式名	内　　容
MPEG	ISOで定められた、映像データを圧縮して記録するためのフォーマット形式をいう。 MPEG-1～MPEG-4とMPEG-7の規格がある。
QuickTime	Apple社が開発したパソコンで動画や音声を扱うためのソフトウェアのQuickTimeで使用されているフォーマット形式をいう。現在ではWindows環境でも広く使われている。
AVI	Microsoftが開発した、主にWindowsで映像を扱うためのフォーマット形式をいう。画像データと音声データを交互に折り混ぜた構造になっている。

52.（2）． マルチメディアのファイル形式 （4/4）

【PDF形式】

- 情報の配布・交換・蓄積を電子的に行なうために用いられる。

＜PDF（Portable Document Format）＞

- 紙に印刷するのと同じ状態のページのイメージを保存するためのファイル形式で、仮想のプリンターを使ってアプリケーションの印刷機能から作成する方法が普及している。

- PDF形式ファイルは、PDFリーダー（PDFを表示できるビューアー）を使って表示・印刷する。

52.（3）． 情報の圧縮と伸張

【情報の圧縮・伸張】

- メディアの種類に応じた圧縮・伸張方法が利用されており、効率的なデータ保存，ネットワーク負荷の軽減といった目的や用途に応じ、適切な圧縮方式を選択する。

＜可逆圧縮と非可逆圧縮＞

名　称	内　　容
可逆圧縮	データの欠落を起こさない方法で圧縮すること。 圧縮前のデータを完全に再現できるが、非可逆圧縮に比べて圧縮率が低い。 ZIPやLZHなどのように、汎用的にデータファイルを圧縮する場合は可逆圧縮でなければならない。
非可逆圧縮	圧縮する際に、ある程度データを欠落させること。 高い圧縮率が期待できる反面、修正→保存を繰り返すとデータが劣化する。 非可逆圧縮を使うのは、JPEGやMPEGなどの音声や画像データである。

53. マルチメディア応用

【目標】

- ➢ マルチメディア技術の応用目的や特徴を理解する。

【説明】

- ✓ 表現技術としてのグラフィックス処理の特徴を理解し、マルチメディア技術を応用した様々な分野があることを知る。

53.（1）． グラフィックス処理 ① 色の表現

【色の表現】

- コンピュータでは、光の三原色と色の三原色、および色相、明度、彩度で表現される。

＜色の表現＞

名　称	内　容
RGB （光の三原色）	赤（red）緑（green）青（blue）の3色を組み合わせて表現する。
CMY （色の三原色）	シアン（cyan）マゼンタ（magenta）イエロー（yellow）の3色の配合比率を変えて表現する。 プリンタによっては、3色にブラック（black）を加える（CMYB）こともある。

＜色の三要素＞

名　称	内　容
色相	赤・青・黄といった色合い、色味のこと。
明度	明るい色とか暗い色というように、色の「明るさ」の度合いのこと。
彩度	色相や明度とはまた別に「あざやかさ」を示す度合いのこと。

53.（1）． グラフィックス処理 ② 画像の品質

【画像の品質】

- 画像の品質は、画素（ピクセル）、解像度、諧調で決まる。

＜画素（ピクセル）＞

- デジタル画像を構成する、色情報を持つ最小単位の点。英語のピクセル
- デジタルカメラで、どれだけ細かい画像で撮影できるのかという能力を示す「画素数」として使われる。

＜解像度＞

- ディスプレー、プリンター、スキャナーなどで扱う画像の精細さを表す尺度のこと。
- 画像を構成するピクセルの数で表し、数が大きいほど精細である。

＜諧調＞

- コンピュータが画像を扱う際に、色の濃さや明るさを何段階で表現することができるかを表す数。
- この数が大きいほど細かな色や明るさの違いを表現できるが、画素あたりのデータ量は増大する。

53.（1）． グラフィックス処理 ③ グラフィクスソフトウェア

【グラフィクスソフトウェア】

- グラフィクスソフトウェアには、ペイント系とドロー系に分けられる。

＜グラフィクスソフトウェア＞

名　称	内　　容
ペイント系	ポインティングデバイスを用いて画像を描く「2次元コンピュータグラフィックス」用のソフトウェアである。内部表現は通常ピクセル（画素）を用いたラスタ形式である。
ドロー系	主に、方向と大きさを持つベクトルで処理するベクタ形式での表現を利用する画像描画ソフトウェアである。

＜画像の品質＞

名　称	内　　容
画素	ラスタ画像を構成する一つひとつの点のこと。ドット、ピクセルともいう。
解像度	画素の密度のこと。1インチ当たりの画素数を「ppi」の単位であらわす。
階調	色の濃淡を表すグラデーションのこと。コントラストともいう。

53.（2）． マルチメディア技術の応用

【マルチメディアシステム】

- マルチメディアを応用し、シミュレータやテレビゲームをはじめ、様々な仕組みができ上がっている。
- マルチメディアシステムを統合して実現した例として拡張現実感、仮想現実感がある。＜ARとVR＞

名　称	内　　容
拡張現実感 AR：Artificial Reality	現実の環境から知覚に与えられる情報に、コンピュータが作り出した情報を重ね合わせ、補足的な情報を与える技術をいう。
仮想現実感 VR：Virtual Reality	コンピュータグラフィックスや音響効果を組み合わせて、人工的に現実感を作り出す技術をいう。
3DCG	拡張現実感、仮想現実感において必要となるコンピュータ内部に仮想的な3次元空間を作り出し、空間内にモデルを配置し、動作させる技術をいう。
シミュレータ	現実の現象や物体を模擬的に再現する機能を持った装置やソフトウェア、システムなどのことをいう。
（コンピュータ）ゲーム	アーケードゲーム、コンシューマーゲーム、パソコンゲーム、携帯電話ゲームなどの分類がある。コンピュータの信号をビデオモニターに出力して表示する。
4K/8K	現行のハイビジョン（2K）に比べ、映像・動画の解像度（画素数）が高い映像4Kや8Kの「スーパーハイビジョン」で行われる日本の放送の通称をいう。

21. データベース

54. データベース方式

【目標】

- データベースおよびデータベース管理システム(DBMS:Database Management System)の意義、目的、考え方を理解する。

【説明】

- ✓ データベースは、業務を情報(データ)という観点から表現するための重要な手段であり、データベース管理システムはデータを構造的に蓄積し、それらの一貫性を保ち、効率的に取り出すための機能を備えたものであることに注目し、その意義、目的、考え方を理解する。

54. (1). データベース (1/2)

【データベース】

- あるテーマにそってデータ集約して、再利用できるようにしたものをデータベースという。

＜データベースの目的＞

- データベースを使ってデータを管理する目的には、次のようなものがある。
  - ① 複数のデータをまとめて管理できる
  - ② 目的のデータを簡単に探すことができる
  - ③ 簡単に編集して使うことができる

＜データベースモデル＞

- データベースに格納するデータの配置をモデルとして定義したものをデータベースモデルという。

＜データベースの種類＞

- 主なデータベースには次の種類がある。
  - ① 関係型
  - ② 階層型
  - ③ ネットワーク型
  - ④ NoSQL

54. (1). データベース (2/2)

【ビッグデータ】

- ビッグデータとは、単に量が多いだけでなく、様々な種類や形式が含まれる非構造化データ、非定型的データであり、さらに、日々膨大に生成・記録される時系列性、リアルタイム性のあるようなものを指すことが多い。

＜ビッグデータの分析＞

名　称	内　容
クロス集計	いくつかの質問項目を掛け合わせ(クロス)して集計や分析を行う手法で、アンケート調査やデータ分析にはよく用いられている。
ロジスティック回帰分析	求めている結果になるかどうか(0か1)を導き出す分析手法で、例えば、タバコを吸う人と吸わない人が肺がんになる率の違いといったものに使われる。
決定木分析	一本の木が幹から枝、葉と分かれていくようにグループ分けをしていく分析手法で、グループ分けはYes/Noでそれぞれ2つに分けていくことが多い。
アソシエーション分析	「ビールとおむつ」の法則のように、一緒に買われる可能性が高いものの組合せや割合、統計的に関連があると思われる法則を抽出する分析手法をいう。
クラスター分析	データを共通点ごとに分類し、またその共通点が与える影響度を元に関連の深いグループを作っていく分析方法をいう。

54. (2). データベース管理システム (1/3)

【データベース管理システム(DBMS)】

- データベースを管理し、データに対するアクセス要求に応えるソフトウェアをいい、次の機能を持つ。

名　称	内　容
データベース管理	リカバリ(障害回復)機能を含み、データの保全機能を確保した上で、実際の磁気ディスク装置に格納する機能
データセキュリティ管理	権限を持つユーザだけがデータアクセスできるようにすることで、データの機密を保護する機能
トランザクション管理	排他制御など障害の発生に備え、データベースの更新履歴を利用者からのトランザクションごとに管理する機能
データ管理 (利用者へのサービス)	●データベース定義機能: スキーマを記述し、定義を支援する機能 ●データベース操作機能: データベースを構築し、操作を支援する機能 ●データベース制御機能: 利用者からの要求に安全、正確、迅速に応えるための機能

54. (2). データベース管理システム (2/3)

【RDBMS(リレーショナルデータベース管理システム)】

- リレーショナルデータベースの構築や利用、運用に必要になる利用環境(SQL言語)の提供やアクセス制御、データ保護、障害復旧など、統合的な環境を提供するシステムのこと。

- データ管理方式の一つで、1件のデータ(レコード)を複数の項目(フィールド)の集合として表現し、データの集合をテーブルと呼ばれる表(構造型データベース)で表す。

＜関係データベースの例＞

ID	氏名	部活コード
1	佐藤	A
2	鈴木	A
3	赤井	A
4	斎藤	B
5	山田	B
6	青田	C
7	中村	C
8	田中	C

部活コード	所属部活動
A	サッカー部
B	野球部
C	陸上部

54. (2). データベース管理システム (3/3)

【NoSQL(Not only SQL)】

- 関係データベース管理システム(RDBMS)以外のデータベース管理システムをさす。
- ビッグデータの普及にともなって、RDBMSから、徐々にNoSQLへと移行している。

＜NoSQLの定義＞

- 非RDBMSを指すおおまかな分類語 (杓子定規に適用してきた長い歴史を打破)
- 非RDBMSの利用・発展の促進運動の標語 (構造のデータベースの利用・発展を促進)

＜NoSQLの利点＞

- 関係モデルを必要としないデータを扱う時 (相当量のkey-valueペアや連想配列を格納)
- 大量のデータを扱う時 (大規模なデータを統計的に解析やリアルタイムに解析)

＜NoSQLの特徴＞

- 固定されたスキーマ(属性の関連)に縛られないこと
- 関係モデルの結合操作を利用しないこと
- 水平スケーラビリティ(増大化の適応能力)が確保しやすい事が多いこと
- トランザクション(管理単位)を利用できないものが多いこと、など

21. データベース

55. データベース設計

【目標】

- データベースの分析・設計の考え方を理解する。

【説明】

- ✓ データの分析・設計の必要性や、その基本的なプロセスを理解する。

55. (1). データ分析

【データ分析】

- データベース化にあたっては、現状の業務プロセスを分析し、帳票類などから業務で使用するデータの洗い出しと整理をする。

＜データ分析の留意点＞

- 洗い出したデータごとに、以下の点を書き出す。
  - 項目（フィールド）名
  - データの大きさ
  - 取扱件数
  - 利用頻度、など
- 業務プロセスから、データ同士の関係を明らかにする。

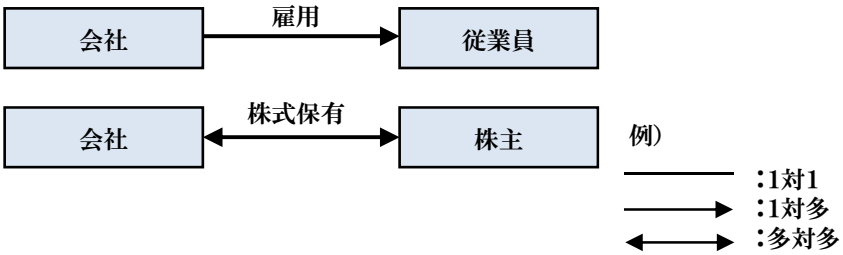
55. (2). データの設計 ①

【データの設計】

- データおよびデータの関連を整理して、データを設計する。
- 関係データベースでは、洗い出して整理したデータをもとにテーブル(表)を作成する。

＜E-R図＞

- DBMSを意識しないデータモデルで、現実世界のデータ構造を忠実に表現することができる。
- ファイルやデータベースを設計する際に、管理対象とデータ項目を把握した結果を表現する。
- エンティティ(実体)の対応関係を次のように記載し、「1対1」「1対多」「多対多」などの関係を表す。

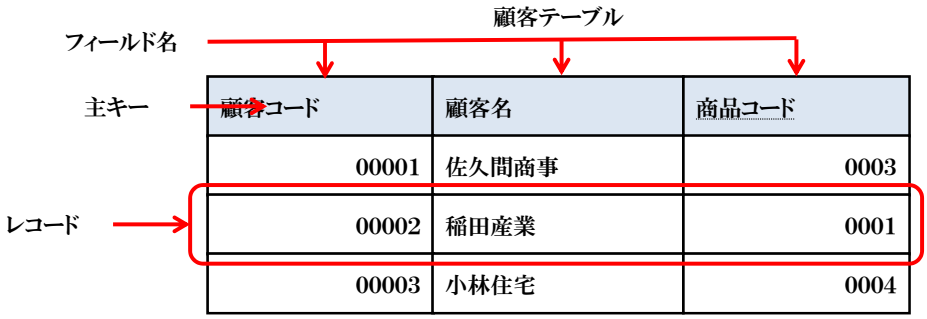


55. (2). データの設計 ②

【テーブルの構造】

- 関係データベースで使用するテーブルは、フィールド(項目)名と、レコード(記録)から構成される。
- また、各レコードを固有のものとして認識するために、一意性を維持するフィールドの「主キー」を設定する。

＜テーブルの構造＞



顧客コード	顧客名	商品コード
00001	佐久間商事	0003
00002	稲田産業	0001
00003	小林住宅	0004

55. (2). データの設計 ③

【コード設計】

- 一般的に、商品コードのように複数のテーブルを関連付けるともき使うものが「コード」である。
- コードは、利用者が理解しやすいように、利用目的や適用分野に合わせて設計する必要がある。

＜インデックス＞

- データの検索を高速化するために作成する索引のこと。
- 検索条件で指定するフィールドの作成する。

＜外部キーと主キー＞

- 2つのテーブルの共通するフィールドのうち、レコードが重複すると矛盾するため、一意性を維持する必要があるレコードを「主キー」といい、他のテーブルから値を参照されるフィールドを「外部キー」という。

外部キー　主キー

売上テーブル

顧客コード	顧客名	商品コード
00001	佐久間商事	0003
00002	稲田産業	0001
00003	小林住宅	0001

商品テーブル

商品コード	商品名	単価
0001	ラーメン	500
0002	チャーハン	450
0003	餃子	300

55. (3). データの正規化

【正規化】

- リレーショナルデータベースで、表の関連性を失わないように項目を整理して表を分離すること。
- 正規化することで、データの更新や削除が容易になり、データを効率的に管理できるようになる。

＜正規化手順＞

- 第一正規化は、繰り返し項目を分離して独立した行にすること。
- 第二正規化は、主キーが決まれば一通り決まる項目を取り出し、表を分離すること。
- 第三正規化は、主キー以外の項目間に従属関係があれば、それらを取り出して分離すること。

学生ID	氏名	資格ID	資格名	合否	資格ID	資格名	合否	学科ID	学科名
1	石橋	3	基本情報	合	N	N	N	5	情報処理科
2	桜井	4	CCNA	合	N	N	N	6	ネットワーク科
3	中山	3	基本情報	否	4	CCNA	合	6	ネットワーク科

第一正規化

学生ID	氏名	資格ID	資格名	合否	学科ID	学科名
1	石橋	3	基本情報	合	5	情報処理科
2	桜井	4	CCNA	合	6	ネットワーク科
3	中山	3	基本情報	否	6	ネットワーク科
3	中山	4	CCNA	合	6	ネットワーク科

第二正規化

学生ID	資格ID	資格名	合否
1	3	基本情報	合
2	4	CCNA	合
3	3	基本情報	否
3	4	CCNA	合

学生ID	氏名	学科ID	学科名
1	石橋	5	情報処理科
2	桜井	6	ネットワーク科
3	中山	6	ネットワーク科

第三正規化

学生ID	氏名	学科ID
1	石橋	5
2	桜井	6
3	中山	6

学科ID	学科名
5	情報処理科
6	ネットワーク科

資格ID	資格名
3	基本情報
4	CCNA

学生ID	資格ID	合否
1	3	合
2	4	合
3	3	否
3	4	合

21. データベース

56. データ操作

【目標】

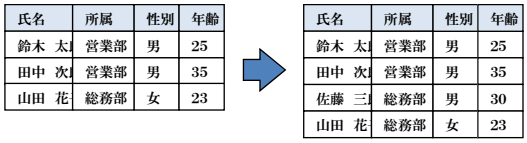
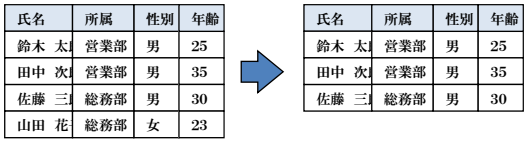
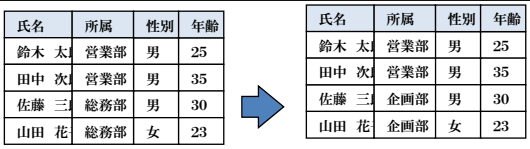
- データの抽出などの操作を理解する。

【説明】

- ✓ 関係データベースを活用するために、必要なデータ操作を理解する。

56.（1）． データ操作 （1/2）

【データベースの操作・1】

方法		内　　容
挿入	 氏名[佐藤三郎]のレコードを挿入	• テーブルに措定したレコードを挿入する
削除	 氏名[山田花子]のレコードを削除	• テーブルから措定したレコードを削除する
更新	 所属[総務部]を[企画部]に更新	• テーブルの措定したレコードを更新する

56.（1）． データ操作 （2/2）

【データベースの操作・2】

方法	内　　容	説明
射影	氏名 / 所属 / 性別 / 年齢 鈴木 太郎 / 営業部 / 男 / 25 田中 次郎 / 営業部 / 男 / 35 佐藤 三郎 / 総務部 / 男 / 30 山田 花子 / 総務部 / 女 / 23 → 列[氏名]で射影 氏名 鈴木 太郎 田中 次郎 佐藤 三郎 山田 花子	• テーブルから指定したフィールドだけを取り出す。
選択	氏名 / 所属 / 性別 / 年齢 鈴木 太郎 / 営業部 / 男 / 25 田中 次郎 / 営業部 / 男 / 35 佐藤 三郎 / 総務部 / 男 / 30 山田 花子 / 総務部 / 女 / 23 → [年齢＝25]で選択 氏名 / 所属 / 性別 / 年齢 鈴木 太郎 / 営業部 / 男 / 25	• テーブルから指定したレコードだけを取り出す。
結合	氏名 / 所属 鈴木 太郎 / 営業部 田中 次郎 / 営業部 佐藤 三郎 / 総務部 山田 花子 / 総務部 氏名 / 性別 鈴木 太郎 / 男 田中 次郎 / 男 佐藤 三郎 / 男 山田 花子 / 女 → 氏名 / 所属 / 性別 鈴木 太郎 / 営業部 / 男 田中 次郎 / 営業部 / 男 佐藤 三郎 / 総務部 / 男 山田 花子 / 総務部 / 女	• 複数のテーブルを共通のフィールドで連結して一つのテーブルとして扱う

21. データベース

57. トランザクション処理

【目標】

- データベースの処理方法を理解する。

【説明】

- ✓ 複数の利用者によるデータの参照や更新に備えて、排他制御とリカバリ機能によってデータベースの一貫性を保つ必要があることを理解する。

57. (1). データベース管理システムの機能

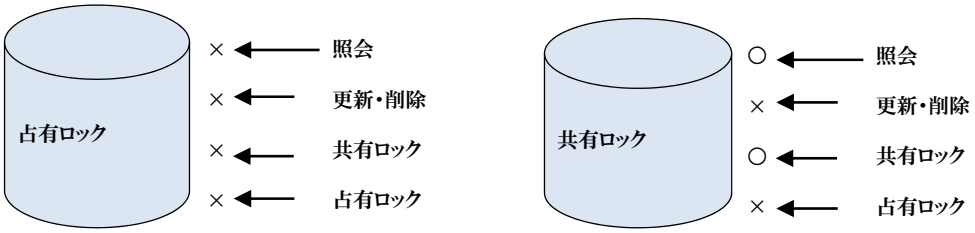
【排他制御】

- データベースの整合性を確保するため、複数の利用者が同時に同一データにアクセスすることを禁止する「排他制御」をしている。
- 対象となる資源についてセマフォ変数という変数を設定し、その変数の値により、他のタスクにこの資源の利用を許すか禁止するかを示すセマフォ方式とロック方式とがある。

＜ロック方式排他制御＞

- データ資源にロック(鍵前)をかけて、別のトランザクションが処理を行えないようにする。
- ロックによる注意点としてはデッドロックが発生する可能性がある。ロックをかける単位(範囲)をロック粒度といい、その大きさは、レコード、ページ、テーブル、データベース全体などがある。

- 占有ロック・・・他の処理からのロックや更新、削除、照会を禁止するロック
- 共有ロック・・・他の処理からの更新や削除を禁止し、照会は許可するロック



22. ネットワーク

58. ネットワーク方式

【目標】

- ネットワークに関するLANやWANという分類を理解する。
- ネットワークを構築するための接続装置の役割を理解する。
- IoTネットワークの関する構成や通信方法を理解する。

【説明】

- ✓ ネットワークは企業などの活動において必要不可欠な基盤であることを認識し、LANやWAN及び代表的なネットワークの構成要素について、役割の概要を理解する。また、上位者の指導の下、身近な社内LANの設定を行う。

58.（1）． ネットワークの構成

【ネットワーク（通信網）】

- 複数のコンピュータをケーブルや通信回線で接続して利用すること。
- 企業のネットワークは、LANやWANで構成され、データのやり取りを行う。

＜ネットワークの種類＞

名　称	解　　説
LAN Local Area Network	同一の建物や敷地内など、比較的狭い範囲で複数のコンピュータを接続したネットワークをいう。 コンピュータを接続するには、主にケーブルを利用する。
WAN Wide Area Network	離れた場所のLAN同氏を相互に接続する広域のネットワークをいう。 LANを接続するには、主に通信回線を利用する。
インターネット	LANやWANなど、さまざまな種類のネットワークを相互に接続したネットワークをいう。

58.（2）． ネットワークの構成要素 （1/5）

【ネットワーク接続機器】

- LANボード（LANカード）やケーブルを利用してLANに接続する。

名　称		解　　説	
LANボード（LANカード）		コンピュータをLANに接続するための拡張ボード（カード）。 LANの規格に合うものを利用する。	
ケーブル	ツイストペアケーブル	2本の細い銅線をより合わせたものを何組かを束ねたケーブルで、「より対線」とのいう。 10BASE-Tや100BASE-TXで利用する。	
	光ファイバーケーブル	光を利用してデータ伝送するケーブルで、電磁波の影響をほとんど受けない。 100BASE-FXやFDDIで利用する。	

58.（2）． ネットワークの構成要素 （2/5）

【LAN接続装置】

- OSI参照モデルに対応し、以下の種類がある。

名　称	OSI参照モデル	説　明
リピータ	物理層	ケーブル上を流れる信号を補正したり増幅したり、伝送距離を延長するための装置。
ハブ	物理層	ここのコンピュータから伸びているケーブルを一つにまとめる集線装置。ハブ同士をカスケード接続してポートを増やすこともできる。
ブリッジ スイッチングハブ	データリンク層	転送先を識別し、特定のコンピュータにしかデータを転送しないフィルタリング機能を持つ蔵置。
ルーター	ネットワーク層	LANを相互に接続する装置。データ転送の最適な経路を判断するルーティング機能やフィルタリング機能を持つ。
ゲートウェイ	全ての層	LANを相互接続できる装置。ネットワークアーキテクチャが異なるLANを接続できる。

58.（2）． ネットワークの構成要素 （3/5）

【通信回線に関する用語】

- 通信回線に関する用語として、以下の種類がある。

名　称	説　明
通信回線	離れた場所にあるコンピューターや端末をつないで、データを送受信するために使う回線をさす。
伝送路	情報や電力の伝送のために使用される媒体をさす。配線の一部として用いる場合には伝送線路ともいう。
無線LAN	無線通信を利用してデータの送受信を行うLANシステムをさす。ワイヤレスLAN、もしくはそれを略してWLANとも呼ばれる
Wi-Fi	Wi-Fi Allianceによって、国際標準規格であるIEEE 802.11規格を使用したデバイス間の相互接続が認められたことを示す無線LANに関する登録商標である。
MACアドレス	ネットワークに接続する機器に設定されている固有の認識番号。通信の宛先を特定するために使用される。製造時にROMに書き込まれて出荷される。
デフォルトゲートウェイ	所属するネットワークの外へアクセスする際に使用する「出入り口」の代表となる装置で、一般的には、ルータがデフォルトゲートウェイになる。
プロキシ（プロキシサーバ）	直接インターネットに接続できない内部のコンピュータに代わって、「代理」としてインターネットとの接続を行うコンピュータのことを

58.（2）． ネットワークの構成要素 （4/5）

【伝送速度】

- データ伝送においては、転送速度と伝送効率により、ネットワーク性能をみることができる。

＜データ伝送速度＞

- 1秒間に伝送できるビット数を表す。bps（bit per second：ビット／秒）

＜データ伝送効率＞

- 伝送時は、実際のデータ以外に伝送制御や誤り制御情報が一緒に送信されるため、伝送効率とは、伝送データのうち実際のデータが占める割合をいう。
- ビット誤り率 ＝ エラービット数／受信したビット数

＜データ伝送時間＞

- データ伝送時間＝伝送するデータ量÷（データ転送速度×データ伝送効率）

58.（2）． ネットワークの構成要素 （5/5）

【移動体通信規格】

- 携帯電話のデータ通信方式のひとつで、携帯電話でブロードバンド並みの高速通信が可能になった。
- LTE（Long Term Evolution）とは、パケット通信に特化し、「高速化」、「低遅延（応答速度向上）」、「多接続（同時に通信できる端末数の増加）」の3点を重視して開発された。
- 5Gは、LTFで使われている周波数帯に加えて、ミリ波を含む高周波数帯の電波を利用することも想定し、大容量化・高速化により、動画や音楽をストリーミング（常時）配信するサービスを普及させる。

【ESSID（Extended Service Set Identifier）】

- 無線LANにおいてネットワークの識別に用いられる文字列で、複数のアクセスポイントと端末または端末どうしの間で混信が生じないよう、個々にESSIDを設定し、この文字列が一致する場合のみ通信できる。

【SDN（Software Defined Network）】

- 単一のソフトウェアによりネットワーク機器を集中的に制御 して、ネットワーク構成や設定などを柔軟に動的に変更することができる技術のこと。

【ビーコン】

- 通信業界では主に無線標識のことで、一般的には、地上にある固定された無線局などから発射される電波を、航空機や船、自動車などの移動体に搭載された機器で受信することで、位置などの情報を取得するために使われる。

22. ネットワーク

59. 通信プロトコル

【目標】

- 通信プロトコルの必要性を理解する。
- 身近で利用されている代表的なプロトコルの役割を理解する。

【説明】

- ✓ 異なるシステム環境間で通信するためには、通信プロトコルが必要であることを理解し、インターネットで使用されている代表的なプロトコルの役割を理解する。

59.（1）． 通信プロトコル （1/2）

【通信プロトコル】

- ネットワークに接続されたコンピュータが、データをやり取りするための決まりごとをプロトコルという。

名　称	説　明
TCP／IP	インターネットで、データ通信をする際に利用されるプロトコル (Transmission Control Protocol)とIP(Internet Protocol)
HTTP	インターネットで、WWWブラウザがデータを送受信するプロトコル (Hypertext Transfer Protocol)
HTTPS	HTTPにSSLによるデータ暗号化機能を付加したプロトコル (Hypertext Transfer Protocol Secure)
SMTP	インターネットで、メールを送信する際に利用されるプロトコル (Simple Mail Transfer Protocol)
POP	インターネットで、メールを受信する際に利用されるプロトコル (Post Office Protocol)
FTP	インターネットで、ファイルを転送する際に利用されるプロトコル (File Transfer Protocol)
NTP	インターネットで、時刻を同期する際に利用されるプロトコル (Network Time Protocol)
ポート番号	インターネット上の通信において、複数の相手と同時に接続を行うため にIPアドレスの下に設けられたサブ(補助)アドレスをさす。

59.（1）． 通信プロトコル （2/2）

【IoTシステムで使用される通信プロトコルの特性】

- IoTの文脈で頻繁に登場する代表的なプロトコルには、次のものがある。

名　称	説　明
MQTT	シンプル・省電力なメッセージキュープロトコル。 1対1、1対N、N対Nのメッセージ配布が可能。
CoAP	制約付きM2Mデバイス（例えば、低電力、損失の多いネットワーク）用 特殊なInternetアプリケーション・プロトコル。
XMPP	メッセンジャーなどでよく使われてきたプロトコル 長い歴史があり、安心して利用できる。 認証を伴った双方向性を持った仕組みが実現できる。
AMQP	高機能・高信頼性なワイヤレベルプロトコル。
SNMP	DARPAモデルに準じた、IPネットワーク上のNW機器の監視・制御用プロトコル。IoT機器の監視・制御にも応用されている。

60. ネットワーク応用

【目標】

- インターネットの基本的な仕組みとサービスの特徴を理解する。
- 通信サービスの特徴、伝達速度などを理解する。

【説明】

- ✓ インターネットの基本的な仕組みを理解し、電子メールなどインターネット上のサービスの特徴を知る。
- ✓ インターネットなどの通信を行うための通信サービスの特徴を理解する。

60.（1）． インターネットの仕組み （1/2）

【インターネット（Internet）】

- インターネットに接続されたコンピュータは、固有のIPアドレスとドメイン名で管理される。

＜ドメイン名＞

- インターネット上のホストに付ける名前のこと。ドメイン名は、DNSによって1つのIPアドレスと対応する。
- また、ドット（.）で区切られた階層構造を持っている。（www.japa.co.jp）

＜DNS（Domain Name System）＞

- IPアドレスとドメイン名の対応を管理する仕組み。
- インターネット上のホストは、IPアドレスを基に通信するため、人間にとってはIPアドレスは不便で覚えづらいが、アルファベットや数字を使ったドメイン名という意味のある文字列に変換し、分かりやすい状態で通信できるようにしている

＜URL（Uniform Resource Locator ）＞

- インターネット上のHTMLや画像などといったリソースの場所を特定するための書式。
- リソースの種類やサーバー名、ドメイン名、ポート番号、フォルダー名、ファイル名などをプロトコルやサーバー・ソフトの違いを超えて統一の書式で指定する。一般には「アドレス」と呼ばれることが多い。

60.（1）． インターネットの仕組み （2/2）

【IPアドレス】

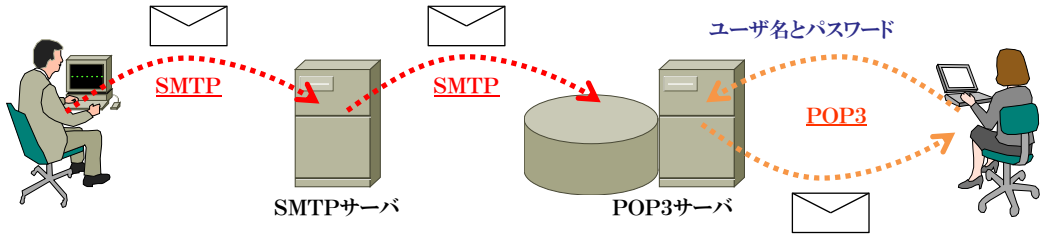
- TCP/IP（IPv4プロトコル）で用いられる32ビットのアドレス。
- 通常、8ビット区切りで10進数表記する。（例：192.168.132.21）
- 32ビットでは不足（枯渇問題）してきているため、IPv6という128ビットのIPアドレスも使われ始めている。

名　称	説　明
IPv4	インターネットの基礎となる通信規約（プロトコル）の第4版。 1990年代後半からのインターネット普及期に使われていたため広く普及し、現在もインターネット上の通信のほとんどはIPv4で行われる。
IPv6	IPv4の次世代規格。 スマートホンや情報家電などが普及するにつれ、アドレス資源の枯渇に備えるため、128ビット表記でアドレス管理をする。
グローバルIPアドレス	インターネットで相手と通信するために持つ、ほかのアドレスと重複しない一意のIPアドレスのこと。TCP/IPでは、通信相手を特定してIPパケットを送信したり、ルーティングするために必要となる。
プライベートIPアドレス	LANなどの企業内ネットワークに存在する端末が、自由に使用できるIPアドレスのこと。自ネットワーク内でのみ一意であるため、ほかのネットワークでは同じプライベートアドレスが利用される。

60.(2). インターネットサービス (1/2)

【電子メール】

- 電子メールは、インターネット上の次のやり取りで行われる。



名　称	説　明
同報メール	同じ内容の文面で、不特定多数の相手に送信する電子メールのこと。4
メーリングリスト	電子メールの活用法のひとつで複数の人に同じメールを配送できる仕組みのこと。
メールボックス	自分あてに届いた電子メールを保存しておく私書箱のこと。
cc	「TO(宛先)の人に送った」という意味。参考・情報共有に使う。
bcc	参考・情報共有に使う。他の受信者にアドレスが見えないように連絡する。

60.(2). インターネットサービス (2/2)

【インターネットサービスの特徴と留意点】

＜cookie＞
- ユーザー情報やアクセス履歴などの情報を、Webブラウザーと Webサーバー間でやり取りするための仕組み。

＜RSS(Really Simple Syndication)＞
- Webサイトの見出しやリンク、要約などを記述できるXMLベースの文書フォーマットの総称。
- ニュースサイトやブログでは、更新情報などをRSSで公開している。

＜オンラインストレージ＞
- ユーザーに貸し出したサーバーマシンのディスクスペースに、ファイルをアップロードすることでインターネット上でファイルを共有するサービスである。

＜クローラ＞
- ロボット型検索エンジンがWeb上のファイル(HTML文書だけでなく、画像・PDFまで含む全般)を収集するためのプログラムのことをいう。

60.（3）． 通信サービス （1/2）

【通信サービス事業者】

- 通信サービスを提供する事業者を回線事業者という。

名　称	説　明
回線事業者	インターネットに接続するための光ファイバーやADSLなどの回線を提供する事業者を指す。キャリアとも呼ばれる。
移動体通信事業者	携帯電話などの電波を使った通信サービスを移動体通信といい、移動体通信サービスを提供している事業者のうち、自社で回線や設備を持っている事業者（現在は実質的に主要携帯電話会社）をいう。
仮想移動体通信事業者	移動体通信事業者から回線や設備の一部を借りて通信サービスを提供している事業者をいう。
インターネット接続サービス事業者	インターネット接続の電気通信役務を 提供する組織のことである。 プロバイダやISPなどと略して呼ばれることが多い。

60.（3）． 通信サービス （2/2）

【その他の通信サービス】

- インターネットを活用した様々なサービスがある。

名　称	説　明
パケット通信	データを小包のように一定の大きさに分割して通信すること。 または、携帯電話などのパケット単位で課金する通信サービスを指す。
モバイル通信	携帯電話会社の回線の電波を利用して、インターネットに接続するサービスのこと。 無線で通信をおこなうため、室内外でもインターネットに接続することができる。
IP電話	IPネットワークの技術を使って音声通話を実現するサービス。 プロバイダーから、付加サービスとして提供されることが多い。
光通信	光ファイバーを通信回線に用いたネットワークの総称をいう。 光通信網の構築には、光信号を電気信号に相互変換する装置が必要になる。
キャリアアグリゲーション	複数の帯域の周波数を用いることで、基地局の負荷分散と通信の安定化を図るもの。第四世代携帯電話のLTEアドバンストで採用される。（CA）
テザリング	モバイル機器を経由して、無線LANなどのネットワーク機能を搭載したパソコンやタブレット端末をインターネットに接続させる機能をさす。
SIMカード	携帯電話ユーザーの加入権情報が保存されているカード。 SIMカードを携帯端末に差し込むと、その携帯電話で通話ができるようになる。
テレマティクス	自動車などの移動体に通信システムを搭載することで、さまざまな情報を送受信できるシステムのこと。

23. セキュリティ
61. 情報セキュリティ

【目標】

- ネットワーク社会において安全に活動するという観点で、情報セキュリティの基本について理解する。

【説明】

- ✓ 情報の収集や活用を安全に行うため、情報セキュリティが必要であることを理解する。
- ✓ 脅威の種類と基本的な対処法、及び脆弱性を理解する。
- ✓ 代表的な攻撃手法、及びそれらへの対策を理解する。

61.（1）． 情報セキュリティの概念

【情報セキュリティの概念】

- コンピューターやコンピューターネットワーク上の仮想的な空間を「サイバー空間」といい、ネットワークを通じて破壊活動やデータの窃取、改ざんなどを行うことを「サイバー攻撃」という。
- サイバー攻撃は、特定の組織や企業、個人を標的にする場合や、不特定多数を無差別に攻撃する場合がある。
- サイバー攻撃から、情報の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）を確保、維持することによって，様々な脅威から情報システムや情報を保護し，情報システムの信頼性を高めることを「情報セキュリティ」という。
- 攻撃者（クラッカー）や自然災害など、安定稼動を損なう要素（脅威）から、コンピュータシステムが安全に保たれていることが必要である。

項　目	機　　能
機密性	アクセスを認可された者だけが情報にアクセスできることを確実にすること。
完全性	情報及び処理方法が、正確であること及び完全であることを保護すること。
可用性	認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

61.（2）． 情報資産

【情報資産】

- 情報資産を、脅威から安全に守ることを情報セキュリティ管理という。

＜情報セキュリティ管理に関する用語＞

項　目	説　　明
資産	情報セキュリティ管理で守る対象になるものをいう
脅威	情報資産の機密性・完全性・可用性を脅かす要素をいう
脆弱性	情報システムに存在するセキュリティ上の弱点をいう

＜情報資産に該当するもの＞

項　目	該 当 例
物理的資産	サーバ、クライアント、ネットワーク機器、設備、建物、回線、など
ソフトウェア資産	オペレーティングシステム、ミドルウェア、アプリケーション、など
データ資産	顧客情報、営業情報、知的財産関連情報、人事情報、財務情報、など

61.（3）． 脅威と脆弱性 ① 人的脅威の種類と特徴

【人的脅威】

- 操作ミス、内部関係者の意図のある情報漏洩、ソーシャルエンジニアリングなど、直接、人が関わるものを人的脅威という。
- 情報セキュリティポリシーに基づく情報管理によって対策される。

名　称	内　　容
漏えい	秘密情報をコピーしたりして持ち出したり、メールの誤送信で情報が流出すること。
紛失	外部にパソコンやUSBメモリ等を持ち出して紛失すること。
破損	データが壊れること。
盗み見	コンピュータ画面を盗み見されること。
なりすまし	他人のIDやパスワードを盗用し、その人の名前を語って行動すること。
クラッキング	ネットワークに繋がれたシステムへ不正に侵入し、破壊・改ざん、不正利用すること。
ソーシャルエンジニアリング	人の弱みや心理につけ込み、巧みに個人情報や機密情報を詐取する手法のこと。
内部不正	内部関係者による意図のあるデータ抜き取りなどの不正行為のこと。
誤操作	誤操作（操作ミス）によるデータ消失すること。

61.（3）． 脅威と脆弱性 ② 技術的脅威の種類と特徴

【技術的脅威】

- 技術的に作成された「悪意あるプログラム」が介在するものを技術的脅威という。
- 偽装してくるもの、プログラム・ソフトウェアの脆弱性を狙ってくるもの、機械的に動作を繰り返し行ってくるものなどがある。

名 称	内 容
マルウェア	不正かつ有害に動作させる意図で作成された悪意あるソフトウェアやコードの総称。
ワーム	自身を複製して他のシステムに拡散する性質を持ったマルウェアのこと。
トロイの木馬	正規のプログラムを装って侵入し、遠隔操作やデータ流出を可能にするマルウェア。
RAT	ネズミのように見えないところから遠隔操作を可能にするツールのこと。
マクロウイルス	オフィスソフトのマクロ機能（自動化プログラム）を悪用して作成されたウイルスのこと。
ガンブラー	ウェブサイトの改ざんを通じて偽サイトに誘導し、感染させて情報を盗みだすこと。
キーロガー	ユーザのキー入力を監視し、記録するタイプのハッキングツールのこと。
バックドア	悪意ある攻撃者が、ターゲットに不正侵入するための入口を作ること。
ファイル交換ソフトウェア	インターネット上の不特定多数のユーザ間でデータを共有できるソフトのこと。
SPAM	無差別かつ大量に一括してばらまかれる、各種ネットメディアのメッセージのこと。

61.（3）． 脅威と脆弱性 ③ 物理的脅威の種類と特徴

【物理的脅威】

- 物理的に破損したり妨害されたりするものをいう。

＜自然災害＞

- 地震・洪水・火災などにより、機器が落ちて破損して使えなくなったり、洪水や豪雨で壊れたりすること。

＜経年劣化＞

- 長く使用していたパソコン、サーバー、システムが経年劣化で故障し、使えなくなること。

＜破壊・妨害行為＞

- パソコンやサーバーなどを直接破壊されたり、業務を直接妨害されたりすること。

61.（3）． 脅威と脆弱性 ④ 脆弱性

【脆弱性】

- 情報システムに存在する、セキュリティ上の弱点や欠陥（セキュリティホール）のことをいう。
- 情報システムに脆弱性が存在すると、脆弱性を悪用されるという脅威が存在する。脅威が現実に起こると、被害が発生する。

＜原因＞

- 想定の範囲を超す利用形態
- ハードウェアの欠陥や故障、ソフトウェアのバグ
- 機密情報、重要情報、情報システムの管理体制の不備
- 社員教育や行動規範、情報セキュリティポリシーの不徹底
- クラッカー（攻撃者）、コンピュータ犯罪者、自然災害の存在
- 人為的ミスや失念（人為的脆弱性）
- 暗号の危殆化
- 会社側の承認なく従業員が勝手に持ち込んだ機器の利用（シャドーIT）

61.（3）． 脅威と脆弱性 ⑤ 不正のメカニズム

【不正のトライアングル】

- 不正行為が発生する要因、内部不正による情報セキュリティ事故・事件の発生を防止するための環境整備の基本的な考え方として、不正のトライアングル（動機、機会、姿勢）がある。

＜不正を犯す動機・プレッシャーの存在＞

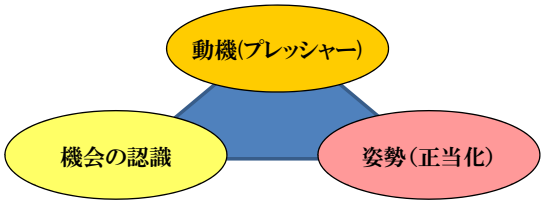
- 合法的なやり方では解決することのできない問題を抱えた者が不正に手を染める可能性がある。
- 動機・プレッシャーとは、不正を実際に行う際の心理的なきっかけのことをいう。

＜不正を犯す機会の存在と認識＞

- 自分への信頼を悪用して秘密裏に問題解決ができ、かつ発覚のリスクが少ない機会を認識する。
- 機会とは、不正を行おうとすれば可能な環境が存在する状態のことをいう。

＜不正を正当化する理由＞

- 自己の行為を自分で受け容れるための事前の納得が必要となる。
- 不正を思いとどませるような倫理観、遵法精神の欠如であり、不正が可能な環境下で不正を働かない堅い意思を保てない状態を意味する。



61.(3). 脅威と脆弱性 ⑤ 攻撃手法 (1/2)

【攻撃手法・1】

- 情報システム、組織および個人への外部からの不正な行為と手法、およびそれらの対策について。

名 称	内 容
辞書攻撃	辞書や人名録などのリストに載っているような既存の単語や、それらの組み合わせを用いる方式で攻撃すること。
総当たり攻撃 (ブルートフォース攻撃)	割り出したい秘密の情報について、考えられるすべてのパターンをリストアップし、片っ端から検証する方式で攻撃すること。
パスワードリスト攻撃	コンピュータの利用者が本人確認に用いるパスワードを探り当てることで、ありとあらゆる文字の組み合わせを試す方法で攻撃するのこと。
クロスサイトスクリプティング	ユーザの入力をそのままエコーバックすることによって生成しているセキュリティ上の不備を利用し、サイト間を横断して悪意のあるスクリプトを注入する攻撃のこと。
ドライブバイダウンロード	Webサイトなどに不正なソフトウェアを隠しておき、閲覧者がアクセスすると気づかないうちに自動でダウンロード・実行する攻撃のこと。
SQLインジェクション	データベースと連動したWebサイトで、問合せや操作を行うSQL文の断片を与え、データベースを改ざんや不正に情報を入手する攻撃のこと。

61.(3). 脅威と脆弱性 ⑤ 攻撃手法 (2/2)

【攻撃手法・2】

- 情報システム、組織および個人への外部からの不正な行為と手法、およびそれらの対策について。

名 称	内 容
キャッシュポイズニング	偽のドメイン情報を発信し、DNSサーバに伝播させ、利用者がそのドメイン内のサーバに到達できないようにしたり、別のサーバにアクセスを誘導する手法をいう。
DoS攻撃	大量のパケットを送信することで、標的となるサーバーのサービスを不能にする攻撃のこと。サービス停止攻撃ともいわれる。
標的型攻撃	標的として狙いを定めた特定の企業や国家の機密情報の詐取を目的に行われるサイバー攻撃のこと。
フィッシング詐欺	金融機関などの正規の通知に偽装したメールを送り、メールに指定されたリンクに接続すると偽装サイトが表示され、個人情報などを搾取する詐欺のこと。
ゼロデイ攻撃	あるセキュリティーホールが発見された際、その情報や対策が告知される前に、そのセキュリティーホールを悪用したウイルスが出回るなどの攻撃を受けた状態をいう。
機能の悪用	ソフトウェアのアップデート機能やクラウド・ストレージのデータ同期の仕組みなどを装って悪用したサイバー攻撃のこと。

23. セキュリティ

62. 情報セキュリティ管理

【目標】

- 情報セキュリティ管理に関する基本的な考え方を理解する。

【説明】

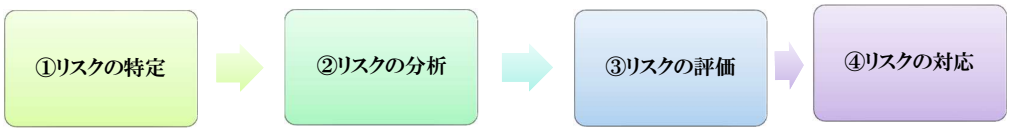
- ✓ リスクマネジメントの必要性を理解する。
- ✓ 情報セキュリティ管理と個人情報保護の目的や基本的な考え方を理解する。
- ✓ 組織内外の代表的な情報セキュリティ組織・期間、及び関連する制度を理解する。

62.（1）． リスクマネジメント （1/2）

【リスクマネジメント】

- リスクマネジメントとは、リスクを組織的に管理（マネジメント）し、損失等の回避又は低減を図るプロセスをいう。
- 企業の価値を維持・増大していくために、企業が経営を行っていく上で障壁となるリスク及びそのリスクが及ぼす影響を正確に把握し、事前に対策を講じることで危機発生を回避するとともに、危機発生時の損失を極小化するための経営管理手法となる。

＜リスクアセスメント＞



- 事故などが発生した際に対処するために、対応マニュアルの整備や教育・訓練などの準備が必要である。

62.（1）． リスクマネジメント （2/2）

【リスク対応】
- リスク対応の種類には、リスクの回避、低減、共有、保有などがある。

＜リスクの回避＞
- リスクを生じさせる要因そのものを中止し、予想されるリスクを遮断する対策をいう。

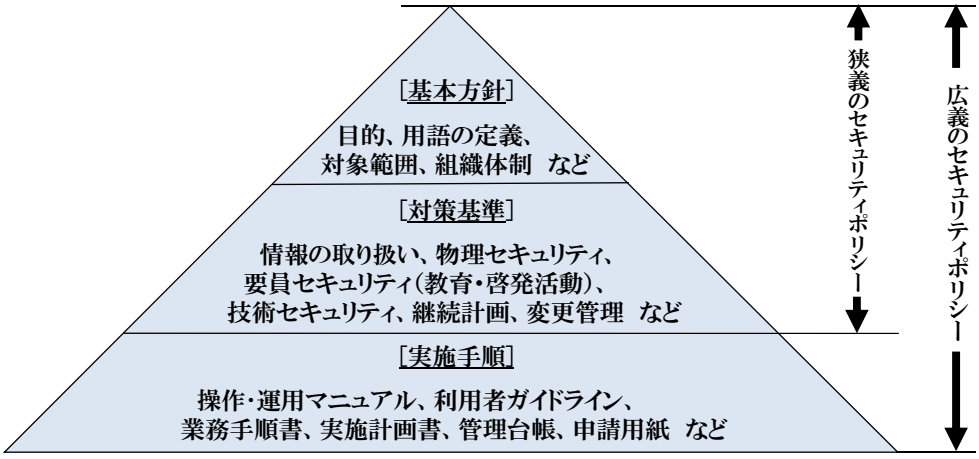
＜リスクの低減＞
- リスクの発生可能性を下げる、もしくはリスクが顕在した際の影響の大きさを小さくする、または、それら両方の対策をいう。

＜リスクの共有＞
- リスクを保険会社に転嫁（または移転）したり、他社と分散させたりする対策をいう。
  - ・リスク転嫁（リスクが顕在化した場合の損失補償を準備すること）
  - ・リスク分散（リスクの源泉を一箇所に集中させず、分離・分散させること）

＜リスク保有＞
- 対策を何もしないこと。リスク受容ともいう。発生頻度が低く、損害も小さいリスクに対して用いる。

62.（2）． 情報セキュリティ管理 （1/2）

【情報セキュリティマネジメントシステム（ISMS）】
- 個別の問題ごとの技術対策の他に、組織のマネジメントとして自らの情報セキュリティリスクのアセスメントにより、情報セキュリティインシデントごとに必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用するために「情報セキュリティマネジメントシステム」を定める。
- 情報セキュリティマネジメントシステムを運用するために、企業全体の情報セキュリティに関する基本方針、対策基準、実施手順で構成された「情報セキュリティポリシー」を定め、継続的改善を行う。



62.（2）． 情報セキュリティ管理 （2/2）

【情報セキュリティの要素】

- 情報セキュリティの要素は「機密性」、「完全性」、「可用性」のほかに、「真正性」、「責任追跡性」、「否認防止」、「信頼性」がある。

項　目	機　　能
機密性	アクセスを認可された者だけが情報にアクセスできることを確実にすること。
完全性	情報及び処理方法が、正確であること及び完全であることを保護すること。
可用性	認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。
真正性	ある主体又は資源が、主張どおりであることを確実にする特性をいう。
責任追跡性	ある動作から動作の主エンティティまで一意に追跡できることを確実にする特性をいう。
否認防止	ある活動又は事象が起きたことを、後になって否認されないように証明する能力をいう。
信頼性	意図した動作及び結果に一致する特性をいう。

62.（3）． 個人情報保護

【個人情報保護法】

- 生存する個人の氏名や生年月日、住所、電話番号などの記述により特定の個人を識別できる情報を個人情報」といい、個人情報を扱う企業・団体、自治体などに対して、適正な取り扱い方法などを定めた法律を「個人情報保護法」といい、個人情報の適正な管理、利用目的の明確化、不正取得の禁止などが定められている。
- 個人情報の中でも人種、信条、社会的身分、病歴、犯罪の経歴、犯罪の被害歴は、不当な差別が生じかねないとして新たな概念「要配慮個人情報」と定義された。

【個人情報保護委員会】

- 個人情報の取り扱いを監督する第三者機関として新たに「個人情報保護委員会」が設置され、すべての事業者に適用されるガイドラインを定め、そのガイドラインにおいて「安全管理措置」が定められた。

項　目	機　　能
プライバシーポリシー	収集した個人情報をどう扱うのか（保護するのか、それとも一定条件の元に利用するのか）などを定めた規範のこと。個人情報保護方針もいう。
プライバシーマーク制度	個人情報について適切な保護措置を講ずる体制を整備している事業者等を評価して、その旨を示すーマークを付与する制度をいう。
サイバー保険	サイバー攻撃などの不正アクセスによる「個人情報の流出」や「業務妨害」などに備えるための保険のことをいう。

62.（4）． 情報セキュリティ組織・機関

【情報セキュリティ組織・機関】

- 不正アクセスによる被害受付の対応、再発防止のための提言、情報セキュリティに対する啓発活動などを行う情報セキュリティ組織や機関があり、それに対応空いた制度がある。

項　目	機　　能
情報セキュリティ委員会	情報セキュリティの全社的な組織で、情報セキュリティポリシーの策定、承認及び見直しも行う。
CSIRT	情報システムのおけるセキュリティの問題に対応するために、専門のスタッフにより編成されたチームで、企業におけるインシデント対応の専門部署となる。
SOC	企業などにおいて情報システムへの脅威の監視や分析などを行う、役割や専門組織をいう。
J-CSIP	公的機関であるIPAを情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取り組みをいう。
J-CRAT	公的機関であるIPAに設置した標的型攻撃対策の組織で、基本的な支援活動は、標的型サイバー攻撃の被害の低減と連鎖の遮断を行う。

- コンピュータ不正アクセス対策基準の「コンピュータ不正アクセス届出制度」に基づき、IPAでは国内の不正アクセス被害の届出を受け付けている。
- コンピュータウイルス対策基準の「コンピュータウイルス届出制度」の基づき、IPAでは国内のウイルス感染被害の届出を受け付けている。
- ソフトウエア製品等脆弱性関連情報取扱基準の「ソフトウエア製品等脆弱性関連情報届出制度」に基づき、IPAでは国内の不正アクセス被害の届出を受け付けている。

23. セキュリティ

63. 情報セキュリティ対策・実装技術

【目標】

- 情報セキュリティ対策の基本的な考え方、及び組織において必要な対策を理解する。
- IoTシステムにおいて情報セキュリティを確保するために必要な取り組みを理解する。

【説明】

- ✓ 情報セキュリティへの様々な脅威に対して、必要な対処を適切に行うために、人的・技術的・物理的セキュリティの側面から基本的な対策を理解する。
- ✓ 情報セキュリティを維持するために必要な暗号、認証、公開鍵基盤などの技術の役割を理解する。
- ✓ IoTシステムの情報セキュリティを確保するために各種の指針・ガイドラインが推奨している事項を理解する。

63.（1）． 情報セキュリティ対策の種類と対策 ① 人的セキュリティ対策の種類

【人的セキュリティ対策】

- 人的セキュリティ対策として、人による誤り、盗難、不正行為のリスクなどを軽減するための情報セキュリティ啓発を目的とした教育と訓練、事件や事故に対して被害を最小限にする対処がある。

対　策	説　明
ルール化	• 「情報セキュリティポリシ」や組織における「内部不正防止ガイドライン」の策定。 • 個人情報保護の体制を整備していることを認定する制度の利用（プライバシーマーク）。 • ログ管理や「監視」するなど予防及び問題発生時の原因を早期に解決できるよう図る。 • 情報セキュリティポリシーや各種社内規程、マニュアルの遵守体制の強化。
社員教育	• 「情報セキュリティ教育・訓練」の実施。
社員による セキュリティ対策	• 定期的にパスワードを変更する（パスワード管理）。 • 電子メールの添付ファイルを、安易に開かない。 • インターネットからプログラムを、安易にダウンロードしない。 • 不審なプログラムは実行しない。 • ソフトウエアなどの著作権物の違法コピーはしない。 • ディスクを共有しない（情報漏えい対策とウイルス対策）。 • 携帯端末は、なるべく持ち出さない。 • むやみにデータを持ち出したり、外部メディア（USBメモリなど）にコピーしない。 • 大事なデータへのアクセス制限をする。（アクセス権の設定や、暗号化、USBキー等） • 情報は必要のある人のみに伝え、必要のない人には伝えない。（need to know）

63.（1）． 情報セキュリティ対策の種類と対策 ② 技術的セキュリティ対策の種類

【技術的セキュリティ対策・1】

- 技術的セキュリティ対策として、ソフトウェア、データ、ネットワークなどに技術的対策を実施することで、システム開発、運用業務などに被害が発生することを防ぐ。

対　策	機　能
コンテンツフィルタリング	好ましくないWebサイトやサービスの閲覧、利用を制限する仕組みで、クライアントのソフトウェアで行う場合と、プロキシによって通信経路上で行う場合がある。
コールバック	電話を受けた側がいったん回線を切り、あらかじめ登録しておいた電話番号にかけ直すことで、情報の漏えいや不正アクセスを防ぐ
アクセス制御	アクセス権を持つユーザだけが、システムやファイルにアクセスできるようにするための機能。
ファイアウォール	LANなどの内部ネットワークと外部のインターネット間に置き、外部からの不正侵入を防ぐための仕組み。
DLP Data Loss Prevention	機密情報を識別して、重要データと認定された情報の送信やコピーを制限し、情報の持ち出しを防ぐ仕組み。
検疫ネットワーク	ネットワークに接続するパソコンを検査するしくみ。安全を確認したパソコンからのみネットワークを利用させることで、企業内のセキュリティを確保する。
DMZ DeMilitarized Zone	悪意に満ちた攻撃から内部ネットワークの機密情報を守るため、信頼できない外部ネットワークからのアクセスを遮断する仕組み。

63.（1）． 情報セキュリティ対策の種類と対策 ② 技術的セキュリティ対策の種類

【技術的セキュリティ対策・2】

対　策	機　能
SSL/TLS Secure Sockets Layer/Transport Layer Security	パソコンとサーバ間の通信データを暗号化することで、第三者によるデータの盗聴や改ざんなどを防ぐ技術をさす。
VPN Virtual Private Network	公衆のネットワークでやり取りする情報を、第三者による盗み見や改ざんを防ぐための技術をさす。（仮想専用線）
MDM Mobile Device Management	スマートフォンやタブレットなどの携帯端末を業務で利用する際に一元的に管理するための仕組みをさす。
電子透かし	電子情報の著作権保護のために用いられる技術をさす。音声や画像データの中に情報を埋め込み、特別な処理をほどこすことでデータの所有者を識別する。
ディジタルフォレンジック	犯罪捜査や法的紛争などで、コンピュータなどの電子機器に残る記録を収集・分析し、その法的な証拠性を明らかにする手段や技術をさす。
ペネトレーションテスト	ネットワークに接続されているコンピュータシステムに対し、実際に既知の技術を用いて侵入を試みることで、システムに脆弱性がないかテストする手法のこと。
ブロックチェーン	「ブロック」と呼ばれるデータの単位を生成し、チェーンのように連結していくことによりデータを保管するデータベースをさす。（分散型台帳技術）
耐タンパ性	機器や装置、ソフトウェアなどが、外部から内部構造や記録されたデータなどを解析、読み取り、改ざんされにくいようになっている状態をさす。

63.（1）． 情報セキュリティ対策の種類と対策 ③ 物理的セキュリティ対策の種類

【物理的セキュリティ対策】

- 物理的セキュリティ対策として、外部からの侵入、盗難、水害、落雷、地震、大気汚染、爆発、火災などから情報システムを保護することによって、情報システムの信頼性、可用性を確保する。
- クリアデスク（離席する際に、机の上に書類や記憶媒体などを放置しないこと）、クリアスクリーン（離席する際に、パソコンの画面を他人がのぞき見したり、操作できる状態のまま放置しないこと）を徹底する。
- 遠隔バックアップなどの対策をとる。

対　策	説　明
不正侵入対策	・入退館（室）管理の実施 ・部外者や、担当者以外の入室や入館を制限（入退室管理） ・鍵管理者の徹底（施錠管理） ・IDカードやバイオメトリクス認証の導入 ・監視カメラの設置
災害対策 （耐震耐火設備）	・耐震構造や免震構造のビルに、サーバを設置 ・サーバ室には、水を使わない消火剤を使用 ・落雷や停電に備え、自家発電設備やUPS（無停電電源装置）の導入
盗難対策	・クライアントPCをセキュリティケーブルで固定し、施錠 ・ノートPCや外部メディアは、なるべく持ち出さない。持ち出すときは、目を離さない。 ・ノートPCやバックアップメディアを使用しないときは、鍵のかかる棚で保管 ・サーバはサーバラックに配置し、窓のない鍵のかかる部屋へ設置

63.（2）． 暗号化技術

【暗号化技術】

－ 情報セキュリティを維持するために必要な暗号技術（暗号化、復号）の基本的な仕組みと暗号強度などの特徴は次の通り。

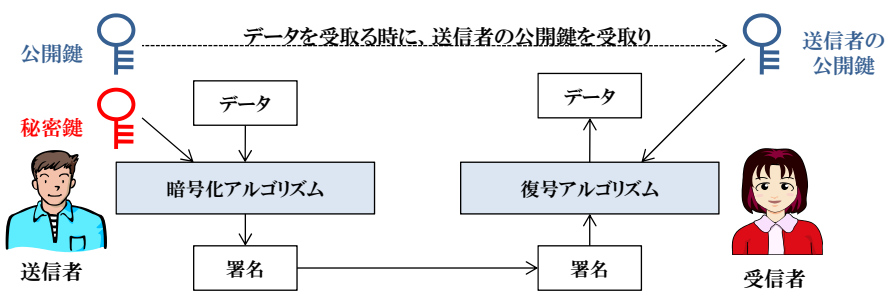
名　称	機　能
共通鍵暗号方式	送信者、受信者の双方が同じ鍵（共通鍵）を持ち、暗号化、復号する。送信者の数だけ「鍵」が必要。処理は高速だが、鍵の配布を安全に行う手立てを別に用意する必要があり、鍵の管理が困難になる点を考慮しなければならない。
公開鍵暗号方式	送信者は受信者の公開鍵を使って暗号化し、受信者は受信者の秘密鍵を使って復号する。暗号化・復号に時間がかかるが、鍵の送付が不要なため、セキュリティが高い。多くの利用者が使える。
ハイブリッド暗号方式	共通鍵暗号方式と公開鍵暗号方式の両方を組み合わせることによって、互いの欠点を補う方式。メッセージそのものの暗号化には、共通かぎ暗号方式を用いて、その共通かぎに対して公開かぎ暗号方式を用いる。
ハードディスク暗号化	社外に持ち出すノートPCの盗難や紛失による情報漏えい対策として行う。 ハードディスク暗号化は、OS領域やシステムファイル領域を含めたハードディスクを丸ごと暗号化する。
ファイル暗号化	PC内のデータのファイル形式を変換することにより、持ち主以外の他のユーザーが文章や画像などのデータファイルを閲覧できなくすることをいう。

63.（3）． 認証技術

【認証技術】

－ 認証技術には「ディジタル署名」や「タイムスタンプ」がある。

名　称	内　容
ディジタル署名 （電子署名・電子捺印）	送信者は自分の秘密鍵を使ってディジタル署名を暗号化し、受信者は送信者の公開鍵を使って復号する。受信者は復号したディジタル署名と電子文書を比較し、送信途中で改ざんされていないかを確認する技術をさす。
タイムスタンプ （時刻認証）	システムの時刻合わせと時刻証明技術を使用して、文書が作成された時刻とその時刻以降、改変されていないことを確認する。



63.（4）． 利用者認証

【利用者認証】

- 利用者認証のために、次の技術が利用される。

項　目	機　　能
ログイン （利用者認証）	通信相手が正当かを確認する技術をいう。 IDとパスワードなどの組み合わせたものが多く使われる。
アクセス管理	適切な権限を持つ者だけが必要なタイミングでアクセスすることを可能にするためのプロセスをいう。
ICカード	極めて薄い半導体集積回路（ICチップ）を埋め込み、情報を記録できるようにしたカードをいう。
ワンタイムパスワード	コンピュータリソースに対するアクセス用に発行される、一度限り有効なパスワードのことをいう。
多要素認証	アクセス権を得るのに必要な本人確認のための要素（証拠）を複数、ユーザーに要求する認証方式をいう。
シングルサインオン	1つのIDとパスワードを入力して、複数のWebサービス等にログインする仕組みで、入力や管理の手間を省き、セキュリティを強化することができる。

63.（5）． 生体認証（バイオメトリクス認証）

【生体認証方式】

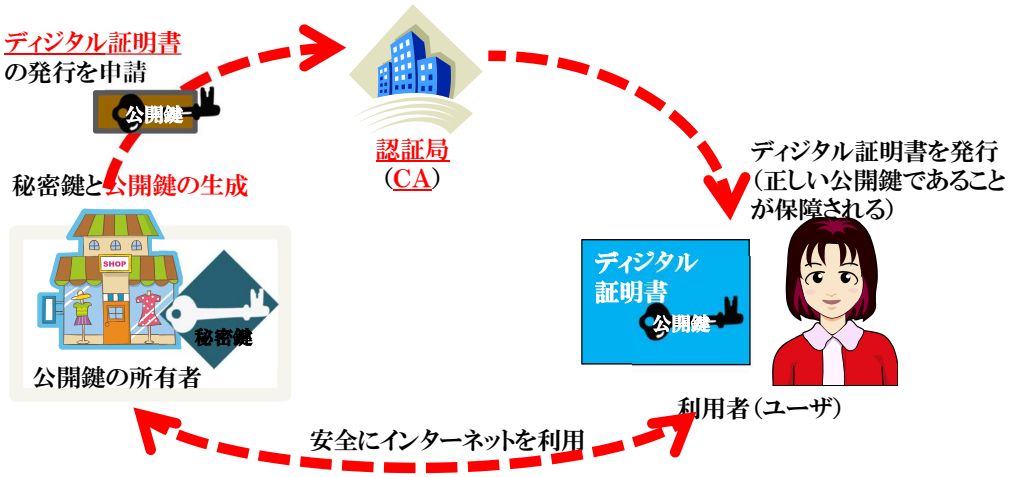
- 利用者の生体の一部を利用して認証する技術。バイオメトリクス認証ともいう。
- 生体認証において、本人を本人でないと誤って認識してしまう確率を「本人拒否率」といい、本人ではないのに本人と認識してしまう確率を「他人受入率」という。
- 「他人受入率」の閾値を上げた場合、誤認証が減るため安全性は高まるが、「本人拒否率」が増えるため利便性は低下する。一方、「他人受入率」の閾値を下げると誤認証が増えるため安全性は低下するが、「本人拒否率」が減るため利用者の利便性は高まる。

項　目	機　　能
指紋認証	指紋の溝のパターンを使って個人を識別する認証方式
静脈パターン認証	指や手の皮膚のすぐ内側を通っている静脈の分岐点や終端点の座標を用いる認証方式
虹彩認証	眼球の瞳孔の外側にある「虹彩」に寄る細かい皺のパターンによる認証方式
声紋認証	声紋、声の周波数波形のパターンによる認証方式
顔認証	鼻や耳や眉や顎などの位置等から抽出した特徴による認証方式

63.（6）． 公開鍵基盤

【公開鍵基盤（PKI：Public Key Infrastructure）】

- 公開鍵暗号方式を利用した、インターネットを安全に利用するための仕組みをいう。



63.（7）． IoTシステムのセキュリティ

【IoTシステムのセキュリティ】

- IoTシステム、IoT機器の設計・開発について策定された各種の指針やガイドラインがある。

名　称	内　容
IoTセキュリティガイドライン	セキュリティが脆弱なIoT機器について、経営者はIoTセキュリティの基本方針を定め、状況の把握とセキュリティの体制作りをすること、内部不正と人為的ミスを防ぎ、もし発生しても安全を守れる対策を検討することなどを定めている。
コンシューマ向け IoTセキュリティガイド	IoTセキュリティWGが、IoTセキュリティの指針、標準や規格などの調査から得た知見を元に、もっともセキュリティの課題が大きいと思われたコンシューマ向けの提言をまとめたガイドをいう。