情報リテラシ補足資料

1. ストラテジ系
2. マネジメント系
3. **テクノロジ系**（この資料の対象）
   （a）基礎理論
      i. 基礎理論
      ii. アルゴリズムとプログラミング
   （b）コンピュータシステム
      i. コンピュータ構成要素
      ii. システム構成要素
      iii. ソフトウェア
      iv. ハードウェア
   （c）技術要素
      i. ヒューマンインターフェース
      ii. マルチメディア
      iii. データベース
      iv. ネットワーク
      v. セキュリティ

13　基礎理論

13.1　離散数学

問題 1　次の真理値表で示される入力 A，B に対する出力 C が得られる論理演算式を書け。

A	B	C
真	真	偽
真	偽	偽
偽	真	偽
偽	偽	真

問題 2　「(not A) and B and C」が空集合にならないような A, B, C の関係の一例をオイラー図で示せ。

問題 3　以下のド・モルガンの法則をオイラー図を描いて説明せよ。

$$P(\overline{A \cup B}) = P(\overline{A} \cap \overline{B}),$$
$$P(\overline{A \cap B}) = P(\overline{A} \cup \overline{B}).$$

問題 4　2 バイトで 1 文字を表すとき，何種類の文字を表せるか。

問題 5　16 進数の $A3$ を 2 進数，8 進数，10 進数に変換せよ。

問題 6　2 進数 10110_2 を 3_{10} 倍せよ。

13.2　応用数学

問題 7　a，b，c，d, e，f の 6 文字を任意の順で一列に並べたとき，a と b が両端になる場合は，何通りか。

13.3　情報に関する理論

問題 8　世界の主要な言語で使われている文字を一つの文字コード体系で取り扱うための規格を何と呼ぶか。
問題 9　{1k バイト，1M バイト，1G バイト，1T バイト } を小さい順に並べよ。

14　アルゴリズムとプログラミング

14.1　データ構造

問題 10　あるキューに要素 “33”，要素 “27” 及び要素 “12” の三つがこの順序で格納されている。このキューに要素 “45” を追加した後に要素を二つ取り出す。2 番目に取り出される要素はどれか。

14.2　アルゴリズム

問題 11　二つの変数 x と y に対して，次の手続きを 1 から順に実行する。処理が終了したとき，x の値は幾らになるか。

1. x に 2 を代入し，y に 3 を代入する。
2. y の値から 1 を引いたものを y に代入する。
3. x の値と y の値を加えたものを x に代入する。
4. $y \neq 1$ なら 2 に戻り，$y = 1$ なら終了する。

問題 12　コンピュータを利用するとき，アルゴリズムは重要である。アルゴリズムの説明として，適切なものはどれか。

1. コンピュータが直接実行可能な機械語に，プログラムを変換するソフトウェア
2. コンピュータに，ある特定の目的を達成させるための処理手順
3. コンピュータに対する一連の動作を指示するための人工言語の総称
4. コンピュータを使って，建築物や工業製品などの設計をすること

問題 13　変数 A と B に格納されているデータを入れ替えたい。入れ替えの手順を説明せよ。ただし，データを一時的に格納するための変数を TMP とする。

14.3　プログラミング・プログラム言語

問題 14　プログラム言語に関する次の記述のうち，適切なものをすべて選べ。

1. 機械語やアセンブリ言語で作成されたプログラムは，特定の CPU に依存することなく実行できる。
2. プログラムは，コンパイラやインタプリタによって機械語に変換される。
3. 人間の言葉に近い規則をもったプログラム言語（高水準言語）を活用すれば，機械語では実行できない複雑な演算が実行できるプログラムが開発できる。

問題 15　Java 言語に関する記述として，適切なものはどれか。

1. Web ページを記述するためのマークアップ言語である。
2. 科学技術計算向けに開発された言語である。
3. コンピュータの機種や OS に依存しないソフトウェアが開発できる，オブジェクト指向型の言語である。
4. 事務処理計算向けに開発された言語である。

14.4　その他の言語

問題 16　文書の構造などに関する指定を記述する，“<” と “>” に囲まれるタグを，利用者が目的に応じて定義して使うことができる言語は何か。

15　コンピュータ構成要素

15.1　プロセッサ

問題 17　コンピュータの構成要素を 5 つ挙げよ。
問題 18　マルチコアプロセッサに関する記述のうち，最も適切なものはどれか。

1. 1 台の PC に複数のマイクロプロセッサを搭載し，各プロセッサで同時に同じ処理を実行することによって，処理結果の信頼性の向上を図ることを目的とする。
2. 演算装置の構造とクロック周波数が同じであれば，クアッドコアプロセッサはデュアルコアプロセッサの 4 倍の処理能力をもつ。
3. 処理の負荷に応じて一時的にクロック周波数を高くして高速処理を実現する。
4. 一つの CPU 内に演算などを行う処理回路を複数個もち，それぞれが同時に別の処理を実行することによって処理能力の向上を図ることを目的とする。

15.2　メモリ

問題 19　{ 主記憶，補助記憶，キャッシュメモリ，レジスタ } を，データの読み書きが高速な順に並べよ。
問題 20　CPU のキャッシュメモリに関する記述のうち，適切なものはどれか。

1. 1 次キャッシュには，2 次キャッシュよりも低速なメモリが使われる。
2. 1 次キャッシュは演算処理の高速化のために使われ，2 次キャッシュは画像描画の高速化のために使われる。
3. 1 次キャッシュは最初にアクセスされ，2 次キャッシュは 1 次キャッシュにデータがないときにアクセスされる。
4. 1 次キャッシュは主記憶アクセスの高速化のために使われ，2 次キャッシュは仮想記憶の実現のために使われる。

問題 21　PC の補助記憶装置であるハードディスク装置の説明として，適切なものはどれか。

1. CD-ROM 装置に比べて読み書きの速度は遅い。
2. 主記憶装置としても利用される。
3. データの保持に電力供給が必要である。
4. ランダムアクセスが可能である。

問題 22　片面 1 層記録の DVD-R は約 4.7GB の記憶容量をもつ。1 ページ当たり日本語 700 文字が印刷されている本の場合，約何万ページ分をこの DVD-R に保存できるか。ここで，日本語 1 文字を表現するのに 2

バイトが必要であるとし，文字情報だけを記録するものとする。また 1GB は 10 億バイトとする。

15.3　入出力デバイス

問題 23　電車の定期券などとして利用される非接触型 IC カードに用いられている技術はどれか。

1. IrDA (Infrared Data Association) 規格
2. RFID (Radio Frequency IDentification)
3. バーコード
4. 無線 LAN

16　システム構成要素

16.1　システムの構成

問題 24　サーバの仮想化に関する記述として，適切なものはどれか。

1. 現実感を伴った仮想的な世界をコンピュータで作り出す技術
2. 手元のコンピュータからネットワークで接続された他のコンピュータの GUI を操作する技術
3. 一つのコンピュータ上で，仮想的に複数のコンピュータを実現させる技術
4. 補助記憶装置の一部を利用して，主記憶装置の容量よりも大きなメモリ領域を仮想的に利用できる技術

問題 25　シンクライアントの特徴として，適切なものはどれか。

1. 端末内にデータが残らないので，情報漏えい対策として注目されている。
2. データが複数のディスクに分散配置されるので，可用性が高い。
3. ネットワーク上で，複数のサービスを利用する際に，最初に 1 回だけ認証を受ければすべてのサービスを利用できるので，利便性が高い。
4. パスワードに加えて指紋や虹彩による認証を行うので機密性が高い。

問題 26　4 台のハードディスクで，RAID 0，RAID 1，RAID 10，RAID 5，RAID 6 のシステムを構築する。システム全体の故障率が低い順に並べよ。ディスクの故障率は一定とする。

16.2　システムの性能評価

問題 27　2 台の処理装置からなるシステムがある。両方の処理装置が正常に稼働しないとシステムは稼働しない。処理装置の稼働率がいずれも 0.90 であるときのシステムの稼働率は幾らか。ここで，0.90 の稼働率とは，不定期に発生する故障の発生によって運転時間の 10% は停止し，残りの 90% は正常に稼働することを表す。2 台の処理装置の故障には因果関係はないものとする。

問題 28　MTBF（Mean Time Between Failure，平均故障間隔）が 600 時間，MTTR（Mean Time To Repair，平均復旧時間）が 12 時間である場合，稼働率はおおよそ幾らか。

問題 29　(1) 利用者が処理依頼を行ってから結果の出力が始まるまでの時間，(2) 利用者が処理依頼を行ってから結果の出力が終了するまでの時間，(2) 単位時間当たりに処理される仕事の量をそれぞれ何と呼ぶか。{ レイテンシ，ターンアラウンドタイム，スループット } から選べ。

問題 30　コンピュータシステムの性能評価を中立的な立場で行うために，各種ベンチマークテストの開発や評価結果を公開することを目的として設立された団体は，GNU，ISO（International Organization for Standardization），OSI（Open Source Initiative），SPEC（Standard Performance Evaluation Corporation）

のうちのどれか。

17　ソフトウェア

17.1　オペレーディングシステム

問題 31　1 台の CPU と 1 台の出力装置で構成されているシステムで，表の三つのジョブを処理する。三つのジョブはシステムの動作開始時点ではいずれも処理可能状態になっている。CPU と出力装置のそれぞれにおいて，ジョブ 1，ジョブ 2，ジョブ 3 の順に処理する。CPU と出力装置は独立して動作するが，出力処理はそれぞれのジョブの CPU 処理が終了してから実施可能になる。ジョブ 3 の出力が完了するのは，ジョブ 1 の処理開始時点から何秒後か。

	CPU 時間	出力時間
ジョブ 1	35 秒	10 秒
ジョブ 2	20 秒	20 秒
ジョブ 3	5 秒	25 秒

問題 32　PC の OS に関する記述のうち，適切なものはどれか。

1. 1 台の PC にインストールして起動することのできる OS は 1 種類だけである。
2. 64 ビット CPU に対応する PC 用 OS は開発されていない。
3. OS のバージョンアップに伴い，旧バージョンの OS 環境で動作していた全てのアプリケーションソフトは動作しなくなる。
4. PC の OS には，ハードディスク以外の CD-ROM や USB メモリなどの外部記憶装置を利用して起動できるものもある。

問題 33　OS の機能の一つである仮想記憶方式の目的はどれか。

1. OS が使用している主記憶の領域などに，アプリケーションプログラムがアクセスすることを防止する。
2. 主記憶の情報をハードディスクに書き出してから電力供給を停止することで，作業休止中の電力消費を少なくする。
3. 主記憶の容量よりも大きなメモリを必要とするプログラムも実行できるようにする。
4. 主記憶よりもアクセスが高速なメモリを介在させることによって，CPU の処理を高速化する。

17.2　ファイルシステム

問題 34　ある Web サーバにおいて，五つのディレクトリが下のような階層構造になっている。このとき，ディレクトリ B に格納されている HTML 文書からディレクトリ E に格納されているファイル `img.jpg` はどのように指定するか。相対 PATH と絶対 PATH の両方を答えよ。

```
root/
  ├ A/
    ├ B/
    │ └ C/
    └ D/
      └ E/
```

問題 35　ファイルのあるレコードが変更されたときに，変更された内容を特定する方法として，適切なものはどれか。

1. ファイルのサイズ及び更新日時を記録しておく。
2. ファイルの複製をとっておき，後で照合する。
3. レコードの件数をファイル内に記録しておく。
4. レコードをキー項目で昇順に並べておく。

17.3 開発ツール

問題 36 プログラムの実行方式としてインタプリタ方式とコンパイラ方式がある。プログラムの実行時にソースコードを解釈する方式が（　　），プログラムの実行前にソースコードを実行ファイルに変換する方式が（　　）である。

問題 37 表のセル A1～C2 に値が入力されている。この表を CSV 形式で出力した結果を書け。

	A	B	C
1	月	1 月	2 月
2	売上高	500	600

問題 38 URL（Uniform Resource Locator）に関する説明として，適切なものはどれか。

1. Web ページとブラウザとの通信プロトコルである。
2. Web ページの更新履歴を知らせるメッセージである。
3. Web ページのコンテンツ (本文) を記述するための文法である。
4. Web ページの場所を示すための表記法である。

17.4 オープンソースソフトウェア

問題 39 OSS (Open Source Software) の利用に関する記述のうち，適切なものはどれか。

1. OSS の利用者は，開発者にソフトウェアの対価を支払う義務を負う。
2. OSS の利用者は，その OSS を販売したり，無料配布したりすることはできない。
3. OSS を遺伝子研究分野で利用することはできない。
4. 公開されている OSS を改良した派生ソフトウェアを OSS として公開できる。

問題 40 Apache と称されるオープンソースソフトウェアの用途はどれか。

1. DBMS
2. OS
3. Web サーバソフトウェア
4. Web ブラウザ

18 ハードウェア

18.1 コンピュータ・入出力装置

問題 41 サーバの仮想化技術に関する記述として，適切なものはどれか。

1. 1 台のコンピュータ上で複数の仮想的なサーバを動作させるための技術
2. 公衆回線を経由してサーバにアクセスする際に，公衆回線を仮想的に専用回線であるかのように利用するための技術

3. コンピュータグラフィックスや音響技術を駆使して，仮想的に現実感をもつ空間を作り出す機能をサーバにもたせるための技術
4. サーバにおいて，ハードディスクを仮想的に主記憶装置の代わりとして利用するための技術

問題 42　スキャナやプリンタの性能の一つである解像度を表す単位はどれか。

1. bps
2. dpi
3. fps
4. Hz

問題 43　PC に接続された周辺機器を，アプリケーションプログラムから利用するために必要なものはどれか。

1. コンパイラ
2. デバイスドライバ
3. プラグアンドプレイ
4. ホットプラグ

19　ヒューマンインターフェイス

19.1　ヒューマンインターフェイス技術

問題 44　PC の操作画面で使用されているプルダウンメニューに関する記述として，適切なものはどれか。

1. エラーメッセージを表示したり，少量のデータを入力するために用いる。
2. 画面に表示されている複数の選択項目から，必要なものを全て選ぶ。
3. キーボード入力の際，過去の入力履歴を基に次の入力内容を予想し表示する。
4. タイトル部分をクリックすることで選択項目の一覧が表示され，その中から一つ選ぶ。

19.2　インタフェース設計

問題 45　文化，言語，年齢及び性別の違いや，障害の有無や能力の違いなどにかかわらず，できる限り多くの人が快適に利用できることを目指した設計を何というか。

1. バリアフリーデザイン
2. フェールセーフ
3. フールプルーフ
4. ユニバーサルデザイン

20　マルチメディア

20.1　マルチメディア技術

問題 46　ディジタルコンテンツで使用される DRM(Digital Rights Management) の説明として，適切なものはどれか。

1. 映像と音声データの圧縮方式のことで，再生品質に応じた複数の規格がある。
2. コンテンツの著作権を保護し，利用や複製を制限する技術の総称である。
3. ディジタルテレビでデータ放送を制御する XML ベースの記述言語である。
4. 臨場感ある音響効果を再現するための規格である。

問題 47　Web サイトにおける RSS の説明として，適切なものはどれか。

1. HTML で記述された文書にレイアウトスタイルを定義するためのマークアップ言語
2. Web ページの見出しやリンク，要約などを定型に従って記述できるフォーマットの総称
3. インターネット上を流れるデータを暗号化し，プライバシ情報などを保護する技術
4. ネットワーク上にブックマークを登録することによって，利用価値の高い Web サイト情報を他のユーザと共有するサービス

問題 48　クッキー (cookie) に関する以下の記述のうち，適切なものをすべて選べ。

1. Web サイトを前回閲覧した際に入力した ID やパスワードなどは，別の PC を使用して閲覧する場合でもクッキーで引き継がれるので再入力が要らない。
2. インターネットカフェなどで一時的に PC を借用して Web サイトを閲覧したときは，閲覧が終わったらクッキーを消去すべきである。
3. クッキーに個人情報が保存されている場合，クロスサイトスクリプティングなどで，その個人情報が盗まれることがある。

20.2　マルチメディア応用

問題 49　ペイント系ソフトウェアで用いられ，グラフィックスをピクセルと呼ばれる点の集まりとして扱う方法であるラスタグラフィックスの説明のうち，適切なものはどれか。

1. CAD で広く用いられている。
2. 色の種類や明るさが，ピクセルごとに調節できる。
3. 解像度の高低にかかわらずファイル容量は一定である。
4. 拡大しても図形の縁などにジャギー (ギザギザ) が生じない。

21　データベース

21.1　データベース方式

問題 50　データベース管理システムを利用する目的はどれか。

1. OS がなくてもデータを利用可能にする。
2. ディスク障害に備えたバックアップを不要にする。
3. ネットワークで送受信するデータを暗号化する。
4. 複数の利用者がデータの一貫性を確保しながら情報を共有する。

21.2　データベース設計

問題 51　関係データベースを構築するための以下の工程を，実行順に並び替えよ。

1. 管理するデータ項目の洗い出し
2. 対象業務の分析
3. 表の作成

問題 52　関係データベースの表を正規化することによって得られる効果として，適切なものはどれか。

1. 使用頻度の高いデータを同じ表にまとめて，更新時のディスクアクセス回数を減らすことができる。
2. データの重複を排除して，更新時におけるデータの不整合の発生を防止することができる。
3. 表の大きさを均等にすることで，主記憶の使用効率を向上させることができる。
4. 表の数を減らすことで，問合せへの応答時間を短縮することができる。

問題 53　関係データベースの表に設定する主キー，外部キー及びインデックスのうち，一つの表に対して複数設定できるものをすべて選べ。

問題 54　関係データベースの設計で用いられる E-R 図が表現するものは何か。

1. 時間や行動などに応じて変化する状態の動き
2. システムの入力データ，処理，出力データの関係
3. 対象世界を構成する実体 (人，物，場所，事象など) と，実体間の関連
4. データの流れに着目したときの，業務プロセスの動き

21.3　データ操作

問題 55　関係データベースで管理された “売上” 表，“顧客” 表及び “商品” 表がある。1〜3 のうち，これらの表のデータを用いて作成できるものだけを全て挙げたものをすべて選べ。ここで，下線のうち**太字**は主キーを，下線は外部キーを表す。

売上

売上番号	顧客番号	商品番号	売上年月日	売上額

顧客

顧客番号	顧客名

商品

商品番号	商品カテゴリ名	商品名

1. 過去のある期間に一定額以上の売上があった顧客の一覧
2. 前月に在庫切れがあった商品の一覧
3. 直近 1 か月の商品別売上額ランキング

問題 56　関係データベースで管理している “商品” 表及び “売上” 表を結合して商品の売上集計を行う。5 月の売上合計金額が最も大きい商品はどれか。

商品

商品コード	商品名	価格
0001	商品 A	2,000
0002	商品 B	4,000
0003	商品 C	7,000
0004	商品 D	10,000

売上

売上番号	商品コード	数量	売上日	配達日
Z00001	0004	2	4/30	5/2
Z00002	0001	1	5/1	5/3
Z00003	0003	2	5/15	5/17
Z00004	0001	3	5/15	5/18
Z00005	0002	3	5/5	5/18
Z00006	0001	2	5/10	5/20
Z00007	0002	1	5/30	6/2
Z00008	0001	2	6/1	6/9
Z00009	0003	1	6/8	6/10

21.4 トランザクション処理

問題 57　あるトランザクション処理は，①共有領域から値を読み取り，②読み取った値に数値を加算し，③結果を共有領域に書き込む手順からなっている。複数のトランザクションを並列に矛盾なく処理するためには，トランザクション処理のどの時点で共有領域をロックし，どの時点でロックを解除するのが適切か。それぞれ，a から d の中から選べ。

1. (a)
2. ①共有領域から値を読み取り
3. (b)
4. ②読み取った値に数値を加算
5. (c)
6. ③結果を共有領域に書き込む
7. (d)

問題 58　デッドロックの説明として，適切なものはどれか。

1. コンピュータのプロセスが本来アクセスしてはならない情報に，故意あるいは偶発的にアクセスすることを禁止している状態
2. コンピュータの利用開始時に行う利用者認証において，認証の失敗が一定回数以上になったときに，一定期間又はシステム管理者が解除するまで，当該利用者のアクセスが禁止された状態
3. 複数のプロセスが共通の資源を排他的に利用する場合に，お互いに相手のプロセスが占有している資源が解放されるのを待っている状態
4. マルチプログラミング環境で，実行可能な状態にあるプロセスが，OS から割り当てられた CPU 時間を使い切った状態

22 ネットワーク

22.1 ネットワーク方式

問題 59　ネットワークインタフェースカードの役割として，適切なものはどれか。

1. PC やアナログ電話など，そのままでは ISDN に接続できない通信機器を ISDN に接続するための信号変換を行う。
2. PC やプリンタなどを LAN に接続し，通信を行う。

3. 屋内の電力線を使って LAN を構築するときに，電力と通信用信号の重ね合わせや分離を行う。
4. ホスト名を IP アドレスに変換する。

問題 60　あるネットワークに属する PC が，別のネットワークに属するサーバにデータを送信するとき，経路情報が必要である。PC が送信相手のサーバに対する特定の経路情報をもっていないときの送信先として，ある機器の IP アドレスを設定しておく。この機器の役割を何と呼ぶか。

問題 61　ルータの機能の説明として，適切なものはどれか。

1. 写真や絵，文字原稿などを光学的に読み込み，ディジタルデータに変換する。
2. ディジタル信号とアナログ信号の相互変換を行う。
3. データの通信経路を制御し，ネットワーク間を中継する。
4. ネットワークを利用して Web ページのデータ蓄積や提供を行う。

問題 62　通信方式に関する記述のうち，適切なものはどれか。

1. 回線交換方式は，適宜，経路を選びながらデータを相手まで送り届ける動的な経路選択が可能である。
2. パケット交換方式はディジタル信号だけを扱え，回線交換方式はアナログ信号だけを扱える。
3. パケット交換方式は複数の利用者が通信回線を共有できるので，通信回線を効率良く使用することができる。
4. パケット交換方式は無線だけで利用でき，回線交換方式は有線だけで利用できる。

問題 63　無線 LAN の通信は電波で行われるため，適切なセキュリティ対策が欠かせない。無線 LAN のセキュリティ対策のうち，無線 LAN アクセスポイントで行うセキュリティ対策ではないものはどれか。

1. MAC アドレスによるフィルタリングを設定する。
2. 通信内容に暗号化を施す。
3. パーソナルファイアウォールを導入する。
4. 無線 LAN の ESSID のステルス化を行う。

22.2　通信プロトコル

問題 64　通信プロトコルの説明のうち，適切なものはどれか。

1. DHCP は Web 閲覧のプロトコルである。
2. FTP はファイル転送のプロトコルである。
3. NTP は設定する IP アドレスなどの情報をサーバから取得するプロトコルである。
4. POP はメールクライアントがメールを送信するプロトコルである。

問題 65　職場の LAN に PC を接続する。ネットワーク設定情報に基づいて PC に IP アドレスを設定する方法のうち，適切なものはどれか。

〔ネットワーク設定情報〕

- ネットワークアドレス　　192.168.1.0
- サブネットマスク　　255.255.255.0
- デフォルトゲートウェイ　　192.168.1.1
- DNS サーバの IP アドレス　　192.168.1.5
- PC は，DHCP サーバを使用すること

1. IP アドレスとして，192.168.1.0 を設定する。
2. IP アドレスとして，192.168.1.1 を設定する。
3. IP アドレスとして，現在使用されていない 192.168.1.150 を設定する。
4. IP アドレスを自動的に取得する設定にする。

問題 66　TCP/IP のポート番号によって識別されるものはどれか。

1. コンピュータに装着された LAN カード
2. 通信相手のアプリケーションソフトウェア
3. 通信相手のコンピュータ
4. 無線 LAN のアクセスポイント

22.3　ネットワーク応用

問題 67　サブネットマスクの役割として，適切なものはどれか。

1. IP アドレスから Ethernet 上の MAC アドレスを割り出す。
2. IP アドレスに含まれるネットワークアドレスと，そのネットワークに属する個々のコンピュータのホストアドレスを区分する。
3. インターネットと内部ネットワークを中継するときのグローバル IP アドレスとプライベート IP アドレスを対応付ける。
4. 通信相手先のドメイン名と IP アドレスを対応付ける。

問題 68　NAT (Network Address Translation) がもつ機能として，適切なものはどれか。

1. IP アドレスをコンピュータの MAC アドレスに対応付ける。
2. IP アドレスをコンピュータのホスト名に変換する。
3. コンピュータのホスト名を IP アドレスに変換する。
4. プライベート IP アドレスをグローバル IP アドレスに対応付ける。

問題 69　IPv4 を IPv6 に置き換える効果として，適切なものはどれか。

1. インターネットから直接アクセス可能な IP アドレスが他と重複しても，問題が生じなくなる。
2. インターネットから直接アクセス可能な IP アドレスの不足が，解消される。
3. インターネットへの接続に光ファイバが利用できるようになる。
4. インターネットを利用するときの通信速度が速くなる。

問題 70　DNS サーバの機能に関する記述として，適切なものはどれか。

1. 同じ LAN 以外にあるコンピュータ宛てのパケットを中継する。
2. 外部ネットワークへの Web アクセスを中継する。
3. 問合せのあった IP アドレスに対応した MAC アドレスを回答する。
4. 問合せのあったホスト名の IP アドレスを回答する。

問題 71　インターネット上にある情報の所在を表す記述方式で，“https://www.ipa.go.jp/” のような形式をもつものは何か。

問題 72　全文検索型検索エンジンの検索データベースを作成する際に用いられ，Web ページを自動的に巡回・収集するソフトウェアは何と呼ばれるか。

問題 73　100M ビット/秒 (100Mbps) の伝送速度の LAN を使用して，1G バイトのファイルを転送するのに必要な時間はおおよそ何秒か。ここで，1G バイト＝ 10^9 バイトとする。また，LAN の伝送効率は 20% とする。

23　セキュリティ

23.1　情報セキュリティ

問題 74　共通鍵暗号方式では通信の組合せごとに鍵が 1 個必要となる。例えば A, B, C, D の 4 人が相互に通信を行う場合は，AB，AC，AD，BC，BD，CD の組合せの 6 個の鍵が必要である。8 人が相互に通信を行うためには何個の鍵が必要か。

23.2　情報セキュリティ管理

23.3　情報セキュリティ対策・実装技術

問題 75　A さんは B さんの公開鍵をもっている。B さんの公開鍵を使って A さんができることはどれか。

1. A さんのディジタル署名を作成でき，B さんへの通信に付与する。
2. B さんが確実に受け取ったという通知を自動返信させることができる電子メールを送信する。
3. B さんだけが復号できる暗号文を作成する。
4. B さんへの通信の内容が改ざんされた場合に，A さんが検知できる。

問題 76　文書を A さんから B さんに送るとき，A さんの公開鍵が使われる場面はどれか。

1. A さんが送る文書の暗号化
2. A さんが送る文書へのディジタル署名の付与
3. B さんが受け取った文書に付与されたディジタル署名の検証
4. B さんが受け取った文書の復号

問題 77　HTTPS で接続した Web サーバとブラウザ間の暗号化通信に利用されるプロトコルは何か。

問題 78　公開鍵暗号方式と比べた場合の，共通鍵暗号方式の特徴として適切なものはどれか。

1. 暗号化と復号とでは異なる鍵を使用する。
2. 暗号化や復号を高速に行うことができる。
3. 鍵をより安全に配布することができる。
4. 通信相手が多数であっても鍵の管理が容易である。

問題 79　PKI において，電子証明書が正当性を証明しているものは何か。

問題 80　PKI において，ディジタル署名をした電子メールに関する記述として，適切なものをすべて選べ。

1. 送信者が本人であるかを受信者が確認できる。
2. 電子メールが途中で盗み見られることを防止できる。
3. 電子メールの内容が改ざんされていないことを受信者が確認できる。