『医療機器運用管理のための情報セキュリティ』
章末問題の詳解

第 3 章　情報セキュリティ理解のためのコンピュータ・ネットワーク構成

問 1　2 進数 01010101 を 3 倍した 2 進数はどれか。
【正解】5．11111111
　2 進数を 10 進数に変換して考えると良い。
2 進数 01010101 から 10 進数への変換は，桁に応じた重み（2 のべき乗）を，2 進数の各桁の値に掛け，足し合わせることで計算する。

$$0\times2^7+1\times2^6+0\times2^5+1\times2^4+0\times2^3+1\times2^2+0\times2^1+1\times2^0=85$$

　85 を 3 倍すると，255 になる。255 の 2 進数を求めるために，255 に近い 2 のべき乗の数値を考える。2 の 8 乗は 256 であり，2 進数で表現すると，2 の 8 乗を表す 9 桁目が 1，その他の桁は 0 と考え，100000000 となることがわかる。255 は 256 から 1 を引いた数値である。したがって，255 の 2 進数は 256 の 2 進数 100000000 から 1 を引いて，11111111 となる。

　別解として，3 倍＝(2+1)倍なので，1 ビット左シフト（2 倍）して元の数を足すと，3 倍になる。すなわち，01010101 であれば，1 ビット左シフトした，10101010 と 01010101 の足し算で，11111111 が求められる。

問 2　記憶装置について誤っているのはどれか。
【正解】1．フラッシュメモリは揮発性メモリの一種である。
　フラッシュメモリは，電源を切ってもデータが保持される不揮発性メモリである。USB 型やカード型などがある。

2．ハードディスクは，磁性体を塗布した円盤状の磁気ディスクに情報を記録する記憶装置である。
3．RAM は Random Access Memory の略語であり，半導体を用いた記憶装置である。データの読み書き消去が可能である。
4．RAM は，主記憶装置（メインメモリ）として使用される。レジスタやキャッシュメモリには，容量は小さいが処理速度が早い SRAM が使用される。
5．ROM は Read Only Memory の略語であり，電源を切っても情報を保持する。データの読み込みだけが可能であり，書き込みはできない。

問 3　IP アドレスについて誤っているのはどれか。

【正解】3. グローバル IP アドレスは各国の政府機関で管理されている。

グローバル IP アドレスは，インターネットへの接続に利用され，重複しない IP アドレスである。世界中でただ 1 つの IP アドレスとなるよう，非営利法人 ICANN（The Internet Corporation for Assigned Names and Numbers）のインターネット資源を管理する機能である IANA（Internet Assigned Numbers Authority）によって調整され，各国のインターネットレジストリが割り当てを行う。

1. IPv4 は 32 ビットの 2 進数を 8 ビットごとにドット（.）で区切り，区切られた 8 ビットの 2 進数を 10 進数に変換して 192.168.100.1 のように表記する。
2. IP アドレスは，ネットワークアドレス部（またはネットワーク部）とホストアドレス部（またはホスト部）で構成される。ネットワークアドレス部は，属しているネットワークを表し，ホストアドレス部は，属しているネットワーク内の個々の機器を表す。
4. プライベート IP アドレスは，インターネット上では利用できない IP アドレスで，オフィス内や家庭内などの LAN（Local Area Network）内でのみ使用される。
5. IP アドレスの枯渇に対応して，アドレス空間を 128 ビットに拡張した IPv6 への移行が進められている。アドレス空間が 32 ビットで表現される IPv4 では，約 43 億個の IP アドレスを割り当てることができるが，世界的な通信機器の増大により，IANA が管理する IP アドレスの在庫が枯渇した。

問 4　コンピュータの入出力インタフェースについて正しいのはどれか。

【正解】3. USB のデータ転送速度は RS-232C よりも速い。

USB 1.0 のデータ転送速度は 12Mbps，USB 4 のデータ転送速度は 40Gbps である。データ転送速度が 20kbps の RS-232C と比べて，USB のデータ転送速度は速い。

1. IEEE 1394 は，外部デバイスを接続するシリアルバス規格である。
2. USB はシリアルインタフェースである。シリアルは直列を意味し，単一の伝送路でバイナリデータ（1 か 0）を順番に送受信する。
4. シリアル ATA は，コンピュータにハードディスクや光学ドライブを接続するための規格である。複数のコンピュータ間の通信には使用されない。
5. HDMI は，コンピュータとディスプレイ，デジタル家電とテレビなどの接続に使用される。

問 5　コンピュータの構成要素であるハードウェアやソフトウェア資源を管理するために，ソフトウェアが共通に利用する基本的な機能を実装したシステムソフトウェアはどれか。

【正解】2. オペレーティングシステム

オペレーティングシステムは，コンピュータの構成要素であるハードウェアやソフトウェア資源を管理するために，ソフトウェアが共通に利用する基本的な機能を実装したシステムソフトウェアであり，基本ソフトウェアと呼ばれることもある。ハードウェアとソフトウェアの関係は,「3.1.2 ソフトウェア」をご覧ください。

1. アプリケーションソフトウェアは，ソフトウェアの中でも最上位に位置付き，利用者が何かの目的を持ってコンピュータを利用しようとするとき使うソフトウェアであり，応用ソフトウェアと呼ばれることもある。例えば，ワープロソフトや表計算ソフト，ブラウザなどがアプリケーションソフトウェアの例である。
3. カーネルは，オペレーティングシステムの中核機能として，アプリケーションとハードウェアを仲介する。CPU やメモリ，入出力装置などのハードウェアを抽象化し，ハードウェアとアプリケーションがやりとりできるようにする役割がある。
4. デバイスドライバは，コンピュータに接続されている入力装置や出力装置などをオペレーティングシステムが制御するためのソフトウェアである。
5. ミドルウェアは，オペレーティングシステムとアプリケーションの中間に位置付くソフトウェアである。多くのアプリケーションが共通的に利用する機能を提供する，仲介的な役割を果たす。

問 6　192.168.32.0/22 ネットワークが持つホスト部のアドレス数はどれか。

【正解】4. 1,024

スラッシュ（/）以降の数字 22 は，IP アドレスのネットワーク部とホスト部を識別するために用いられるサブネットマスクを意味する CIDR 記法である。サブネットマスクは IPv4 であれば 32 ビットであり，ネットワーク部のビットは 1，ホスト部のビットは 0 で表される。スラッシュ（/）以降の数字が 22 であることから，IP アドレスのネットワーク部は 22 ビットであることがわかる。ホスト部は，32 ビット（サブネットマスクの全ビット数）－22 ビット（ネットワーク部のビット数）＝10 ビットとなる。10 ビットで表現できるアドレス数は，2^{10}＝1024 となる。

IP アドレスの詳細は，「3.2.3 IP アドレス」をご覧ください。

問 7　IP アドレスなどのネットワーク情報を提供するプロトコルはどれか。

【正解】2. DHCP

DHCP（Dynamic Host Configuration Protocol）は，ネットワークに接続した機器に対して，IP アドレスや DNS サーバなどの通信に必要な設定情報を自動的に割り当てるプロトコルである。家庭用ルータには DHCP サーバの機能が内蔵されており，初期設定では有効になっていることが多いため，機器を LAN ケーブルで接続するだけで，インターネットに接続される。

1. FTP（File Transfer Protocol）は，ネットワーク上でファイルを送受信するためのプロトコルである。
3. HTTP（HyperText Transfer Protocol）は，ウェブブラウザでウェブページの内容を表示するために，ウェブサーバと通信するためのプロトコルである。HTTPS（HyperText Transfer Protocol Secure）は，通信が TLS によって暗号化されているプロトコルである。
4. POP3（Post Office Protocol version 3）は，メールサーバから電子メールを受信するためのプロトコルである。
5. SMTP（Simple Mail Transfer Protocol）は，電子メールを転送するためのプロトコルである。

問 8　インターネット上に構築された，あたかも専用線のように使うことができる仮想的なネットワークはどれか。

【正解】4．VPN

VPN（Virtual Private Network）は，物理的に距離が離れている異なる拠点間を接続するインターネット上に構築された仮想の専用線である。VPN には，インターネットを利用するインターネット VPN と，通信事業者が持つ閉域網を利用する IP-VPN がある。

1. LAN（Local Area Network）は，家やオフィスなどの限られた範囲で構成されるネットワークである。
2. NAPT（Network Address Port Translation）は，IP アドレスやポート番号（情報の送受信を行う扉の番号）を変換する技術である。インターネット側のグローバル IP アドレスを，LAN 側の複数のプライベート IP アドレスを持ったネットワーク機器で使えるように変換することで，LAN 側のネットワーク機器がインターネットを利用できるようにする。
3. VLAN（Virtual LAN）は，LAN を論理的に複数のネットワークに分割する技術である。分割されたネットワーク同士は，相互に通信ができなくなるため，マルウェア感染などの問題が生じた場合に，その波及範囲を限定することができる。
5. WAF（Web Application Firewall）は，ウェブアプリケーションを脅威から守るために，アプリケーション層で制御を行うファイアウォールの一種である。

問 9　センサ機器やアクチュエータなどのあらゆるモノが通信機能を持ち，インターネットに接続して，クラウドサービスなどを利用し，相互に情報交換する仕組みはどれか。

【正解】4．IoT

IoT（Internet of Things）は，今までインターネットに接続されていなかったセンサ機器やアクチュエータなどのあらゆるモノが通信機能を持ち，インターネットに接続して，クラウドサービスなどを利用して，相互に情報交換する仕組みである。センサ機器，アクチュエータ，自動車，建物，家電製品，小型電子機器など様々なモノがインターネットを介して接続され，相互に連携することで，今まで収集できなかった情報やデータが収集され，処理され，連携することが可能となる。

1. BEMS（Building Energy Management System）は，IoT 技術を活用し，ビルのエネルギー使用状況などを見える化し，管理するシステムである。人感知センサや温湿度センサなどからデータを収集，蓄積，分析し，エネルギー制御システムによって，空調や照明などの機器を最適に制御する。
2. HEMS（Home Energy Management System）は，IoT 技術を活用し，家庭で使用するエネルギーを管理するシステムである。ドア・窓センサや温湿度センサなどからデータを収集，蓄積，分析し，家電や電気設備などを最適に制御する。
3. IDS（Intrusion Detection System）は侵入検知システムを意味し，不正な通信やサイバー攻撃を検知するセキュリティシステムである。
5. IPS（Intrusion Prevention System は侵入防止システムを意味し，不正な通信やサイバー攻撃を防止するセキュリティシステムである。

問 10　アプリケーションサービスを提供するクラウドサービスモデルはどれか。

【正解】5. SaaS

SaaS（Software as a Service）は，「サービスとしてのソフトウェア」を意味し，クラウドにあるソフトウェアを利用できるクラウドサービスモデルであり，クラウドに接続できれば，利用者の機器や OS によらず，同じように利用することができる。

1. Web サイトや Web アプリの開発は，Web サービスや Web アプリなどの操作画面を開発するフロントエンドと，サーバ側のシステムやデータベース構築などを行うバックエンドに分けられる。BaaS（Backend as a Service）は，バックエンド機能をアプリケーションサーバ側で代行し，開発環境を提供するクラウドサービスモデルである。
2. DaaS（Desktop as a Service）は，仮想デスクトップ環境を提供するクラウドサービスモデルである。
3. IaaS（Infrastructure as a Service）は，クラウドにあるネットワークやサーバなどの計算機資源を利用できるクラウドサービスモデルである。アプリケーションソフトウェアやミドルウェア，オペレーティングシステムは提供されない。
4. PaaS（Platform as a Service）は，クラウドにあるプラットフォームを利用できるクラウドサービスモデルである。サービス提供者からアプリケーションソフトウェアを提供するためのミドルウェアやオペレーティングシステム，ハードウェアなどの環境が提供される。

第 4 章　情報セキュリティにおける脅威

問 1　コンピュータのロックやファイルの暗号化を引き起こし，復元を条件に金銭を要求するマルウェアはどれか。

【正解】5. ランサムウェア

ランサムウェアは，金銭の詐取のために用いられるマルウェアである。ランサムウェアに感染すると，コンピュータ内のファイルが勝手に暗号化され，利用できない状態となる。この暗号化されたファイルを復号するためには金銭を支払えと脅すことで，金銭（身代金，ランサム）を詐取する。

1. ワームは，コンピュータウイルスと同様に，他のコンピュータへ感染を広げるが，コンピュータウイルスとは異なり，自らの力で感染活動を繰り返し，他のコンピュータへ感染を拡大させるプログラムである。
2. マルウェアは大きく分けて，コンピュータウイルス，ワーム，トロイの木馬に分類される。これらマルウェアの機能の 1 つがボットである。ボットは robot の略語であり，ある目的を持った自動化されたプログラムのことである。ボットには，Web 上の情報を自動収集するクローラや，利用者のリクエストに自動応答するチャットボットなど，悪意がないものも多く存在する。
3. トロイの木馬の攻撃対象は，感染したコンピュータ自身であり，利用者の個人情報やパスワードを盗んだり，データの破壊を行ったりする。感染したコンピュータで悪意ある活動を行うが，それ自体が他のコンピュータに感染を広げることはしない。
4. スパイウェアは，ユーザの承認を得ずにコンピュータに不正侵入し，ネットワークの通信内容やキーボードの入力内容からユーザの個人情報を盗み，外部に転送するソフトウェアである。

問 2　ゼロデイアタックについて正しいのはどれか。

【正解】5. セキュリティパッチが公開される前のセキュリティホールを利用する。

ゼロデイアタックは，ソフトウェアが持つセキュリティ上の脆弱性を意味するセキュリティホールが発見された際，脆弱性を解消する修正プログラムであるセキュリティパッチが適用される前に，その脆弱性を狙う攻撃のことである。

1 と 4. メールやファイルなどの大量のデータを送り続けることでサーバを過負荷状態に追い込み，サービスを停止させる DoS 攻撃（Denial of Service attack）である。
2. DoS 攻撃の 1 つである DDoS 攻撃（Distributed Denial of Service attack）である。多数の端末から同時に大量のデータを送信することでサーバを過負荷状態に追い込み，サービスを停止させる。
3. ネットバンキングやネットショッピングなどになりすまして，利用者の個人情報をだまし取るフィッシングである。実在する企業や個人を装った電子メールを送信し，本物の Web サイトと区別がつかない偽の Web サイトに利用者を誘導し，ログインに必要な ID やパスワード，電話番号やクレジットカード番号などを入力させ，その情報をだまし取る。

問 3　Web アプリケーション上で悪意のあるデータを入力し，データベースのデータを改ざんしたり，データを不正に取得したりする攻撃はどれか。

【正解】2. SQL インジェクション攻撃

SQL インジェクション攻撃は，アプリケーションの脆弱性を狙い，不正な SQL 文（データベースを操作する言語）をプログラムに注入することで，データベースのデータを不正に操作する攻撃である。

1. 水飲み場攻撃は，攻撃対象者がよく利用する Web サイトに不正なプログラムを仕込み，マルウェアに感染させる攻撃である。
3. バッファオーバーフロー攻撃は，データを格納するメモリ領域（バッファ）を超えるデータを送りつけることでバッファを溢れさせ，実行中のアプリケーションを強制停止させたり，悪意のあるコードを実行させたりする攻撃である。
4. クロスサイトスクリプティング攻撃は，サイト内検索やブログ，掲示板などの Web サイトの脆弱性を利用し，HTML に悪質なスクリプトを埋め込み，Web サイトに入力されたユーザの情報や Cookie 情報を不正に入手する攻撃である。
5. DNS キャッシュポイズニング攻撃は，IP アドレスとドメイン名を関連付けて，ユーザからの IP アドレスの問合せに答える DNS サーバソフトウェアの不具合や設定間違いなどの脆弱性を狙い，DNS サーバのキャッシュ情報を不正に書き換え，ユーザに誤った IP アドレスを回答することで，偽サイトへ誘導する攻撃である。

問 4　特定の企業や個人を狙ったサイバー攻撃はどれか。

【正解】1. 標的型攻撃

特定の企業や組織，個人を狙ったサイバー攻撃である。業務などに関係するメールと区別がつかない巧妙に作り込まれた添付ファイル付きのメールを利用してマルウェアに感染させる，標的型メール攻撃がよく知られている。

2. ブルートフォース攻撃は，暗号解読方法の 1 つで，パスワード認証に対して，考えられるすべての組合せを試す総当たり攻撃である。
3. バッファオーバフロー攻撃は，データを格納するメモリ領域（バッファ）を超えるデータを送りつけることでバッファを溢れさせ，実行中のアプリケーションを強制停止させたり，悪意のあるコードを実行させたりする攻撃である。
4. SQL インジェクション攻撃は，アプリケーションの脆弱性を狙い，不正な SQL 文（データベースを操作する言語）をプログラムに注入することで，データベースのデータを不正に操作する攻撃である。
5. クロスサイトスクリプティング攻撃は，サイト内検索やブログ，掲示板などの Web サイトの脆弱性を利用し，HTML に悪質なスクリプトを埋め込み，Web サイトに入力されたユーザの情報や Cookie 情報を不正に入手する攻撃である。

問 5　本物そっくりの Web ページに誘導して個人情報を盗む行為はどれか。

【正解】3. フィッシング

フィッシングは，本物の Web サイトと区別がつかない偽の Web サイトを作成し，ネットバンキングやネットショッピングなどになりすまして，利用者の個人情報をだまし取る詐欺行為である。実在する企業や個人を装った電子メールを送信し，本物の Web サイトと区別がつかない偽の Web サイトに利用者を誘導し，ログインに必要な ID やパスワード，電話番号やクレジットカード番号などを入力させ，その情報をだまし取る。

1. マルウェアは大きく分けて，コンピュータウイルス，ワーム，トロイの木馬に分類される。これらマルウェアの機能の 1 つがボットである。ボットは robot の略語であり，ある目的を持った自動化されたプログラムのことである。ボットには，Web 上の情報を自動収集するクローラや，利用者のリクエストに自動応答するチャットボットなど，悪意がないものも多く存在する。
2. アドウェアは，使用時に広告が表示される無料のソフトウェアである。広告表示によって収入を得ている。アドウェアの中には，ユーザを追跡してデータを収集し，第三者に提供する悪質なものもある。
4. スパイウェアは，ユーザの承認を得ずにコンピュータに不正侵入し，ネットワークの通信内容やキーボードの入力内容からユーザの個人情報を盗み，外部に転送するソフトウェアである。
5. ランサムウェアは, 金銭の詐取のために用いられるマルウェアである。ランサムウェアに感染すると，コンピュータ内のファイルが勝手に暗号化され，利用できない状態となる。この暗号化されたファイルを復号するためには金銭を支払えと脅すことで，金銭（身代金，ランサム）を詐取する。

問 6　サイバー攻撃で侵入者が不正行為に利用するために設置するのはどれか。

【正解】4. バックドア

バックドアは，悪意ある第三者がコンピュータに不正侵入した後，いつでも侵入できる入り口を作成するソフトウェアである。コンピュータの外部から正規の手続きを踏むことなく内部に通信を行うため，バックドア（裏口）と呼ばれる。

1. DMZ（DeMilitarized Zone）は，非武装地帯を意味する。DMZ は，外部ネットワークと内部ネットワークの中間に設けられるネットワーク上のセグメントである。外部ネットワークと内部ネットワークの両ネットワークからファイアウォールなどで隔離されているため, DMZ 内に設置されたサーバなどのセキュリティ強化を図ることができる。
2. VPN（Virtual Private Network）は，物理的に距離が離れている異なる拠点間を接続するインターネット上に構築された仮想の専用線である。VPN には，インターネットを利用するインターネット VPN と，通信事業者が持つ閉域網を利用する IP-VPN がある。
3. ルータは，異なるネットワーク間を中継するネットワーク機器である。例えば，オフィス内や家庭内などの LAN（Local Area Network）とインターネットを接続する際に，ルータが用いられる。
5. ファイアウォールは，信頼できるネットワークと信頼できないネットワークの間で通信を制御するネットワーク機器である。本来の意味である火災の燃焼を阻止する防火壁と同様に，信頼できないネットワークからのサイバー攻撃を遮断することで，信頼できるネットワークを守る役割がある。

問 7　パスワード入力履歴などを特定の第三者に送信するマルウェアはどれか。

【正解】2. スパイウェア

スパイウェアは，ユーザの承認を得ずにコンピュータに不正侵入し，ネットワークの通信内容やキーボードの入力内容からユーザの個人情報を盗み，第三者に転送するマルウェアである。

1. アドウェアは，使用時に広告が表示される無料のソフトウェアである。広告表示によって収入を得ている。アドウェアの中には，ユーザを追跡してデータを収集し，第三者に提供する悪質なものもある。
3. フィッシングは，本物の Web サイトと区別がつかない偽の Web サイトを作成し，ネットバンキングやネットショッピングなどになりすまして，利用者の個人情報をだまし取る詐欺行為である。
4. ランサムウェアは, 金銭の詐取のために用いられるマルウェアである。ランサムウェアに感染すると，コンピュータ内のファイルが勝手に暗号化され，利用できない状態となる。この暗号化されたファイルを復号するためには金銭を支払えと脅すことで，金銭（身代金，ランサム）を詐取する。
5. エクスプロイトコードは，脆弱性を利用し，攻撃対象を攻撃するための悪意あるスクリプトやプログラムのことである。

問 8　セキュリティパッチが公開される前のセキュリティホールを利用した攻撃はどれか。

【正解】3. ゼロデイアタック

ゼロデイアタックは，ソフトウェアが持つセキュリティ上の脆弱性を意味するセキュリティホールが発見された際，脆弱性を解消する修正プログラムであるセキュリティパッチが適用される前に，その脆弱性を狙う攻撃のことである。

1. F5 アタックとは，ブラウザの「更新」を実行するキーボードの F5 キーの連打により，多量のデータの再送リクエストをサーバに送信することで，サーバのサービスを停止させる DoS 攻撃である。
2. DDoS アタック（Distributed Denial of Service attack）とは，DoS 攻撃の 1 つである。多数の端末から同時に大量のデータを送信することでサーバを過負荷状態に追い込み，サービスを停止させる。
4.ブルートフォースアタックは，暗号解読方法の 1 つで，パスワード認証に対して，考えられるすべての組合せを試す総当たり攻撃である。
5.バッファオーバーランアタックは，データを格納するメモリ領域（バッファ）を超えるデータを送り付けることでバッファを溢れさせ，実行中のアプリケーションを強制停止させたり，悪意のあるコードを実行させたりする攻撃である。バッファオーバーフロー攻撃とも呼ばれる。

問 9　標的型攻撃メールへの対策として適切なのはどれか。

【正解】1. 不審メールの添付ファイルは開かない。

不正プログラムを送り込まれたり，偽の Web サイトに誘導されたりする危険性があるため，不審なメールの添付ファイルを開いたり，メール本文に記載された Web サイトのリンクにアクセスしてはならない。また被害を拡大しないためにも，不審なメールを他者にそのまま転送してはならない。メール受信時はウイルスチェックなどのセキュリティ対策の実施が重要である。

問 10　大量のリクエストによりサーバのサービスや機能を低下，停止させる攻撃はどれか。

【正解】2．DDoS 攻撃

DDoS 攻撃（Distributed Denial of Service attack）とは，DoS 攻撃の 1 つである。多数の端末から同時に大量のデータを送信することでサーバを過負荷状態に追い込み，サービスを停止させる。

1．辞書攻撃（Dictionary Attack）は，パスワード認証を突破するための攻撃である。パスワードに使用されることが予想される単語や人物名，それらの組合せや派生語などを，パスワード候補の文字列として辞書に登録して，順番に試すことでパスワード認証の突破を試みる。ブルートフォース攻撃よりも，効率が良いことが知られている。

3．ポートスキャン攻撃は，コンピュータへの不正侵入を試みる方法の 1 つである。攻撃対象のコンピュータのポートに順にアクセスし，ポートで動作するサービスからセキュリティホール（ソフトウェアが持つセキュリティ上の脆弱性）を探す攻撃である。

4．ブルートフォース攻撃は，暗号解読方法の 1 つで，パスワード認証に対して，考えられるすべての組合せを試す総当たり攻撃である。

5．SQL インジェクション攻撃は，アプリケーションの脆弱性を狙い，不正な SQL 文（データベースを操作する言語）をプログラムに注入することで，データベースのデータを不正に操作する攻撃である。

第 5 章　情報セキュリティ

問 1　情報セキュリティは機密性，完全性，可用性の 3 つの基本概念で整理できる。可用性を高めるのはどれか。

【正解】4. ハードウェアの二重化

可用性とは，情報を利用したいときに利用できることである。必要な情報に必要なときにアクセスでき，目的を果たすまでアクセスし続けることができることが，可用性である。可用性を高めるために，サーバやストレージ，ハードウェア，ネットワークなどの多重化，無停電電源装置の導入，事業継続対策の検討と実施，院内サーバ（オンプレミス）からクラウドへの移行などが行われる。

1. 電子署名（またはデジタル署名）は，ハンコの電子版と例えられることが多いが，電子署名が付与された電子データは，デジタル署名付与後に，1 ビットでも内容に変化があれば，署名検証に失敗するので，電子データの改ざんを検出することができる。電子署名は，完全性を高めるために行われる。完全性とは，情報や処理が正確であり，改ざんが行われていないことである。完全性を高めるその他の方法としては，情報へのアクセス履歴の記録，変更履歴の記録，バックアップなどがある。
2. 認証とは，認証者と被認証者が，あらかじめ二者間で共有している情報について検証することで，被認証者の真正性を確かめることである。2 段階認証とは，認証の 3 要素である知識による認証，所有物による認証，生体情報による認証のうち，二つの要素を組み合わせる認証である。例えば，パスワードという知識による認証に加えて，本人しか持ち得ない電話番号（スマートフォン）という所有物による認証を組み合わせた認証である。
3. 情報の暗号化は，機密性を高める。機密性とは，アクセスを許可されていない者はアクセスできず，アクセスを許可された者だけがアクセスできることである。機密性を高めるその他の方法としては，アクセス制御の徹底，認証に用いられる利用者のアカウント管理，パスワードや IC カードなどによる利用者認証などがある。
5. 廃棄メディアから情報が漏えいしないよう細断する行為は，機密性を高める。機密性とは，アクセスを許可されていない者はアクセスできず，アクセスを許可された者だけがアクセスできることである。

問 2　正しいのはどれか。

【正解】3. 情報セキュリティにおける完全性とは，情報が正確で改ざんされていないことをいう。

情報セキュリティにおける完全性とは，情報や処理が正確であり，改ざんが行われていないことである。

1. データのバックアップは，情報セキュリティにおける完全性を高めるための 1 つの方法である。完全性を高めるその他の方法としては，情報へのアクセス履歴の記録や変更履歴の記録などがある。
2. 共通鍵暗号方式は，暗号化と復号に共通の鍵を使用するため，第三者に鍵が漏れないよう管理しなければならない。

4. オープンソースソフトウェアは，ソースコードの改変や再配布が可能な無償のソフトウェアである。ソースコードが公開されているため脆弱性を狙われやすいが，プログラムの修正や改善などの対処も早いため，必ずしもセキュリティ上の懸念があるわけではない。
5. ファイアウォールは，信頼できるネットワークと信頼できないネットワークの間で通信を制御するネットワーク機器である。本来の意味である火災の燃焼を阻止する防火壁と同様に，信頼できないネットワークからのサイバー攻撃を遮断することで，信頼できるネットワークを守る役割がある。しかしながら，院内の信頼できるネットワークに個人の PC を自由に接続すると，個人の PC がマルウェアに感染していた場合，院内ネットワーク内で感染が広がるリスクがある。

問 3　外部からの不正アクセスを防ぐ目的で，インターネットと内部のネットワークやシステムの間に置く仕組みはどれか。

【正解】5. ファイアウォール

ファイアウォールは，信頼できるネットワーク（内部のネットワーク）と信頼できないネットワーク（インターネット）の間で通信を制御するネットワーク機器である。本来の意味である火災の燃焼を阻止する防火壁と同様に，信頼できないネットワークからのサイバー攻撃を遮断することで，信頼できるネットワークを守る役割がある。

1. アンチウイルスソフトは，マルウェアを検出・除去するソフトウェアである。
2. スイッチングハブは，有線 LAN で構築したネットワーク内で，複数の機器を中継する装置である。ネットワークケーブルを接続するための複数のポートを備えている。
3. スパイウェアは，ユーザの承認を得ずにコンピュータに不正侵入し，ネットワークの通信内容やキーボードの入力内容からユーザの個人情報を盗み，外部に転送するソフトウェアである。
4. セキュリティパッチは，ソフトウェアの脆弱性を解消するための修正プログラムである。

問 4　ランサムウェア対策として効果がないのはどれか。

【正解】1. ファイルはすべて暗号化して保存する。

ファイルの暗号化は，情報漏えいを防ぐ効果はあるが，ランサムウェアは，感染したコンピュータのファイルを勝手に暗号化することで，ファイルへのアクセスを制限してしまうため，ファイルの暗号化はランサムウェア対策にはならない。

2. 電子メールの添付ファイルや本文中のハイパーリンクは，マルウェアの感染経路として利用されることが多いため，不審なメールの添付ファイルはむやみに開かず，メールを削除することが望ましい。
3. ウイルス対策ソフトやアンチウイルスソフト，ウイルスチェッカは，ウイルス定義ファイルを元にマルウェアを検出，隔離，除去する。常に最新のウイルス定義ファイルに更新することは，ランサムウェアを始めとするマルウェア対策の 1 つである。
4. オペレーティングシステムを更新し，脆弱性を解消することで，脆弱性を狙った攻撃による不正アクセスやマルウェア感染を防ぐことができる。

5. 重要なファイルは定期的にバックアップしておくことで，ランサムウェアに感染し，コンピュータのファイルへのアクセスが制限されてしまったとしても，重要なファイルの可用性は確保される。

問 5　システム障害発生時，病院のシステム担当が最初に行うべきことはどれか。

【正解】1. 各部署から情報を収集し，状況把握を行う。

システム障害発生時は，影響の範囲に応じた対策を行うために，各部署から情報を収集し，状況把握を行うことが重要である。2，3，4，5 は，情報を収集した後で，必要に応じて行う対応である。

問 6　本人確認のための認証技術でないのはどれか。

【正解】2. 電子署名

電子署名（またはデジタル署名）は，電子データの改ざんを検出するための技術である。電子署名が付与された電子データは，デジタル署名付与後に 1 ビットでも内容に変化があれば，署名検証に失敗することで，電子データの改ざんを検出することができる。

1. 生体認証は，指紋や顔など，本人の身体的特徴や行動的特徴によって行われる認証である。本人そのものの特徴を利用した認証なので，忘れたりなくしたりすることがなく，利便性も高いため，スマートフォン等で広く利用されている。
3. 多要素認証は，パスワードのような知識による認証のみでは，安全性に限界があるため，複数の認証要素を組み合わせた認証技術である。
4. ID とパスワードは，情報システムを利用する際の一般的な認証方法である。
5. ワンタイムパスワードは，一度しか使えない使い捨てのパスワードである。あらかじめ登録されている電話番号に SMS で 4 桁〜6 桁程度のワンタイムパスワードが発行され，そのワンタイムパスワードを入力することで認証が行われる。二要素認証で利用されることが多い。

問 7　情報セキュリティの要素である「機密性」に関する技術はどれか。

【正解】2. ユーザー認証

機密性は，アクセスを許可されていない者はアクセスできず，アクセスを許可された者だけがアクセスできることである。機密性を高めるためには，ユーザー認証をはじめ，アクセス制御の徹底，情報の暗号化などが行われる。

1. 負荷分散は，可用性を高めるための技術である。演算処理の負荷を，2 台以上の並列に稼働しているコンピュータ間で，処理を最適なコンピュータに振り分け，負荷を分散させる方法である。1 台のコンピュータに負荷が集中し，処理が停止してしまうことを防ぐ。
3. デジタル署名（または電子署名）は，電子データの改ざんを検出し，データの真正性を高めるための技術である。デジタル署名が付与された電子データは，デジタル署名付与後に 1 ビットでも内容に変化があれば，署名検証に失敗することで，電子データの改ざんを検出することができる。
4. システムログは，責任追跡性と信頼性を確保するための技術である。システムの動作履歴を時系列に記録したものである。

5. タイムスタンプは，真正性を高めるための技術である。タイムスタンプに印された時刻以前にその電子文書が確かに存在していたこと，またその時刻以降に電子文書が改ざんされていないことを証明する。

問 8　医療現場の情報セキュリティを担保する上で，不適切な行動はどれか。

【正解】2. 医療機器を病棟の無線 LAN（パブリックネットワーク）に接続した。

パブリックネットワークは，第三者が使用できるネットワークであるため，医療機器を接続するには適していない。医療機器は，病院内の管理されたプライベートネットワークに接続する必要がある。

1. USB メモリを通した医療機器のマルウェアへの感染や，USB メモリの紛失・盗難などによる情報漏えいの危険があるため，医療機器情報の取得には，例えば病院内の管理されたプライベートネットワークを使用するなどの対応が推奨される。
3. サイバー攻撃に備え，組織内で事前にリスクアセスメント（リスク特定，リスク分析およびリスク評価）を実施することは，組織内のセキュリティ対策の意識を高めるうえで重要である。
4. 脆弱性を解消する修正プログラムであるセキュリティパッチの更新は，脆弱性を狙ったサイバー攻撃を防ぐうえで重要である。
5.病院内のネットワークを，事務用ネットワークと医療機器用ネットワークに分けることは，セキュリティ対策，およびサイバー攻撃を受けた際の被害拡大を防ぐうえで重要である。

問 9　守るべき情報資産にアクセスする際，組織（ネットワーク）の内部と外部を区別せず，すべて信用せずに認証やアクセス制御を適用することでセキュリティリスクに対応するネットワークセキュリティモデルはどれか。

【正解】5. ゼロトラスト

標的型攻撃の攻撃者が目的を達成するために，組織内部のネットワークに長期にわたって潜伏していたり，BYOD（Bring Your Own Device）によって，様々な機器が持ち込まれたり，テレワークによって組織外のネットワークからの組織内のネットワークへアクセスしたりされることで，境界型防御のみで組織内の情報資産を守ることが難しくなってきた。ゼロトラストネットワークでは，境界型防御による安全なトラストゾーンに頼らずに，守るべき情報資産に対するすべてのアクセスを信用することなく，認証やアクセス制御を適用することで，セキュリティリスクに対応する。

1. IDS（Intrusion Detection System）は侵入検知システムを意味し，不正な通信やサイバー攻撃を検知するセキュリティシステムである。
2. IPS（Intrusion Prevention System）は侵入防止システムを意味し，不正な通信やサイバー攻撃を防止するセキュリティシステムである。
3. TLS（Transport Layer Security）は，アプリケーション層とトランスポート層の間に，暗号技術を用いた安全な通信路を利用できるようにするプロトコルである。IoT デバイスとクラウド間の通信の暗号化などに用いられている。

4. WPA2 / WPA3-Enterprise は，暗号化や認証機能を備えた無線 LAN のセキュリティプロトコルである。

問 10　電子カルテシステムの安全性を高めるために，最小限のネットワーク機能と入出力機能のみを有するシンクライアント端末からのみ接続可能とする方式はどれか。

【正解】4. VDI

VDI（Virtual Desktop Infrastructure，仮想デスクトップ方式）は，最小限のネットワーク機能と入出力機能のみを有するシンクライアント端末からのみ接続可能とする，コンピュータの仮想化方式の 1 つである。医師が診察に用いる PC で，サーバ上で実行されているブラウザに表示された画面だけを転送する仮想ブラウザを利用して Web 閲覧を行う方法が採用されることもある。

1. BYOD（Bring Your Own Device）は，個人が所有するコンピュータやスマートフォンを業務に使用する利用形態のことである。
2. LAN（Local Area Network）は，家やオフィスなどの限られた範囲で構成されるネットワークである。
3. UTM（Unified Threat Management)は，ファイアウォールや IDS（Intrusion Detection System，侵入検知システム），IPS（Intrusion Prevention System，侵入防止システム）などのセキュリティ機能を集約したネットワーク機器である。統合脅威管理あるいは統合型脅威管理とも呼ばれる。
5. WAN（Wide Area Network）は，通信事業者が提供するインフラを利用した広域なネットワークである。