

暗記だけで解ける項目

基本情報技術者 科目A / 考えても導けない、覚えていれば確実に取れるものだけ

01 ネットワーク

プライベートIPアドレスは3つだけ 最重要

- 10.00.00.00
- 172.16 ~ 172.31.00.00
- 192.168.00.00

これ以外はすべてグローバルIP。

覚え方 172だけ範囲がある。16〜31の16個で、32以上は入らない。
出題は「172.32」「172.40」のように**範囲の外を混ぜてくるのがほぼ定番**。

OSI基本参照モデル 最重要

層	名前	機器	プロトコル
7	アプリケーション	—	HTTP FTP SMTP POP DNS
6	プレゼンテーション	—	文字コード・暗号の変換
5	セッション	—	通信の開始と終了
4	トランスポート	—	TCP UDP
3	ネットワーク	ルータ	IP ICMP
2	データリンク	スイッチングハブ・ブリッジ	MACアドレス ARP
1	物理	リピータ・ハブ	ケーブル・電気信号

覚え方 機器は下から ハブ → スイッチ → ルータ と1つずつ上がる。

ひっかけ スwitchングハブは2層。名前に「ハブ」が付くが、MACアドレスを見るので1層ではない。ただのハブ（リピータハブ）は1層。

ポート番号

番号	用途	番号	用途
20 / 21	FTP	80	HTTP
22	SSH	110	POP3
23	Telnet	143	IMAP4
25	SMTP（送信）	443	HTTPS
53	DNS	123	NTP（時刻同期）

3文字略語の役割

DNS	ドメイン名 ⇄ IPアドレス
DHCP	IPアドレスを自動で配る
ARP	IPアドレス → MACアドレス
NAT	プライベート ⇄ グローバル（1対1）
NAPT	ポート番号も変換（複数台で1つのIPを共有）
ICMP	疎通確認（ping）

ひっかけ 「複数の端末が同時に1つのグローバルIPで」とあれば必ずNAPT。NATでは1台ずつしか使えない。

メール・通信の対比

	TCP	UDP
確認応答	する（信頼性）	しない（高速）
用途	Web・メール・ファイル	音声・動画のリアルタイム・DNS

SMTP	送信
POP3	受信（ダウンロードして端末に取り込む）
IMAP4	受信（サーバーに残す = 複数端末で同じ状態）

サブネットマスクの区切り

末尾	2進	区切り幅	使えるホスト
128	10000000	128	126
192	11000000	64	62
224	11100000	32	30
240	11110000	16	14
248	11111000	8	6
252	11111100	4	2
0 (/24)	00000000	256	254

覚え方 使えるホスト数は区切り幅 -2。
引く2つ=ホスト部が全部0（ネットワークアドレス）と全部1（ブロードキャスト）。

02 セキュリティ

鍵の向き **最重要**

目的	使う鍵
秘密にして送る（暗号化）	受信者の公開鍵で暗号化 → 受信者の秘密鍵で復号
本人だと証明（署名）	送信者の秘密鍵で署名 → 送信者の公開鍵で検証

覚え方 暗号化は受け取る人の鍵で閉める。署名は送る人の鍵でハンコ。

ひっかけ デジタル署名で分かるのは完全性（改ざんなし）と真正性（本人）の2つだけ。機密性は守れない（署名しても中身は読める）。

共通鍵と公開鍵

	共通鍵	公開鍵
鍵	同じ鍵	別の鍵
速度	速い	遅い
n人での鍵の数	$n(n-1) \div 2$	2n
代表	AES	RSA・楕円曲線

SSL/TLSはハイブリッド=本文は共通鍵（速い）、その鍵を公開鍵で送る（安全）。

攻撃の名前

SQLインジェクション	DBを不正操作。対策=プレースホルダ
XSS	閲覧者のブラウザでスクリプトが動く
CSRF	ログイン中の本人に意図しない操作をさせる
パスワードリスト攻撃	他サイトから漏れた組を試す。原因=使い回し
リバースブルートフォース	PWを固定しIDを変える。アカウントロックが効かない
レインボー攻撃	ハッシュの逆引き表。対策=ソルト
ゼロデイ攻撃	修正プログラム公開前を突く
標的型攻撃	特定組織を狙う自然な日本語のメール
水飲み場攻撃	標的がよく見るサイトを改ざんして待ち伏せ
DNSキャッシュポイズニング	偽の対応表を覚えさせ偽サイトへ誘導
ソーシャルエンジニアリング	技術を使わず人をだます

ひっかけ 暗号化（SSL/TLS）ではSQLインジェクション・XSS・CSRFは防げない。暗号化は盗聴対策。
ファイアウォールでもWebアプリ攻撃は防げない（→ WAFの役割）。

守る技術

ファイアウォール	IPとポートで許可・遮断
WAF	通信の中身を見てWebアプリ攻撃を防ぐ
IDS	検知して知らせるだけ
IPS	検知して遮断する
DMZ	公開サーバを置く隔離区画

VPN	暗号化した専用線のような通信路
-----	-----------------

覚え方 IDSのD=Detection（検知）／IPSのP=Prevention（防止）。「遮断」と書いてあればIPS。

マルウェアの区別

ウイルス	他のプログラムに寄生して増える
ワーム	単独で自己増殖する
トロイの木馬	装うだけで増殖しない
ランサムウェア	暗号化して身代金要求
ボット	遠隔操作。DDoSの踏み台に

3要素とリスク対応

機密性	許可された人だけが見られる
完全性	正確で改ざんされていない
可用性	使いたいときに使える

回避	やめる
低減	対策して小さくする（教育・対策ソフト）
移転	保険・外部委託
受容	そのまま受け入れる

ひっかけ 認証の3要素は知っているもの／持っているもの／本人の特徴。
「パスワード＋秘密の質問」は多要素ではない（どちらも知っているもの＝1要素）。

03 コンピュータの構成

記憶装置の並び **最重要**

レジスタ → キャッシュ → 主記憶 → 補助記憶

上ほど速く・小容量・高価。「最も高速」と書かれたらキャッシュではなくレジスタ。

メモリの種類

	SRAM	DRAM
リフレッシュ	不要	必要
使う場所	キャッシュ	主記憶
速さ・値段	速い・高い	遅い・安い

覚え方 DRAMのDはDynamic＝抜けちゃうからリフレッシュが要る。SはStatic＝そのまま。
SDRAMは名前にSが付くがDRAMの仲間（現在のPCの主記憶）。

マスクROM	書き換え不可
EEPROM	電氣的に何度でも書き換え
フラッシュメモリ	EEPROMの仲間。SSD・USBメモリ

高速化のしくみ

パイプライン	命令を段階に分けて少しずつずらして並行
スーパースカラ	パイプラインを複数本
メモリインタリーブ	主記憶を分けて並行アクセス
DMA	CPUを介さず装置と主記憶が直接転送

覚え方 主語で切る。命令を並行＝パイプライン／主記憶を並行＝メモリインタリーブ。

論理回路

回路	1になるとき
AND	両方1
OR	どちらか1つでも1

XOR	違うとき
NAND	両方1のときだけ0（ANDの逆）

センサ	物理量 → 電気信号
アクチュエータ	電気信号 → 動き（モーター）
FPGA	買った後で回路を書き換えられる
半加算器 / 全加算器	桁上がりを考えない / 考える

04 単位と接頭語

大きい		小さい	
k キロ	10^3	m ミリ	10^{-3}
M メガ	10^6	μ マイクロ	10^{-6}
G ギガ	10^9	n ナノ	10^{-9}
T テラ	10^{12}	p ピコ	10^{-12}

覚え方 GHz → ナノ秒は打ち消し合うので 1 ÷ 数字 でそのまま出る。
2GHz→0.5ns、4GHz→0.25ns、1.6GHz→0.625ns。

ひっかけ bps はビット、ファイルサイズはバイト。伝送時間を出すときは必ず ×8 して単位を揃える。忘れると答えが8分の1になる。

2進接頭語：Ki=2¹⁰（1,024）、Mi=2²⁰、Gi=2³⁰。2¹⁰≒1,000 として概算する。

05 データベース

正規化と関係演算

第1正規形	繰返し項目をなくす
第2正規形	部分関数従属をなくす
第3正規形	推移的関数従属をなくす

選択	行を取り出す
射影	列を取り出す
結合	2つの表を共通項目でつなぐ

ACID特性と復旧

原子性 Atomicity	全部やるか、全部なかったことにするか
一貫性 Consistency	整合が保たれる
独立性 Isolation	同時に動いても干渉しない
耐久性 Durability	完了した結果は失われない

ロールバック	処理前へ戻す（処理の失敗時）
ロールフォワード	ログで進める（媒体障害からの復旧）
排他制御	同時更新の矛盾を防ぐ（ロック）

06 アルゴリズム

速い順	意味
O(1)	データ量に関係なく一定
O(log n)	二分探索。2倍になっても手間は1回増えるだけ
O(n)	線形探索
O(n log n)	クイックソート・マージソート
O(n ²)	バブルソート。10倍で100倍かかる

スタック	後入れ先出し（LIFO）＝積み重ね
キュー	先入れ先出し（FIFO）＝行列

二分探索は整列済みが絶対条件。要素1,024個なら最大10～11回で見つかる（2¹⁰=1,024）。

ウォーターフォール	後戻りしない前提で順に進む
アジャイル	短い反復（イテレーション／スプリント）
プロトタイピング	試作を見せながら固める
スパイラル	部分ごとに反復して完成させる

単体 → 結合 → システム → 運用	テストの順（規模が大きくなる）
ホワイトボックス	内部構造を見る（分岐網羅など）
ブラックボックス	入力と出力だけ見る（同値分割・限界値）
回帰テスト	直した影響で他が壊れていないか

覚え方 結合度は弱いほど良い（最良＝データ結合、最悪＝内容結合）。凝集度は強いほど良い。逆なので注意。

必ず対で出る2つ

最重要

インシデント管理	とにかく早く復旧させる
問題管理	根本原因を究明して再発を防ぐ
変更管理	変更のリスクを評価して承認
構成管理	資産・構成情報を正確に維持
サービスデスク	問合せの単一窓口

SLA	品質水準を合意した 文書
SLM	守れているか測って改善する 活動
BCP	災害時の事業継続計画
WBS	作業を階層的に分解した図
ガントチャート	横棒で進捗を管理
アローダイアグラム	作業の前後関係。 クリティカルパス＝最長経路
TCO	導入から廃棄までの総費用

システム監査の手順：計画 → 予備調査 → 本調査 → 評価・報告。
監査人は**独立性**が必須で、自ら改善作業はしない（勧告まで）。内部統制の責任者は**経営者**。

PPM（4象限）

	シェア高	シェア低
成長率 高	花形	問題児
成長率 低	金のなる木	負け犬

金のなる木で稼いだ資金を、花形と問題児に投資するのが定石。

SWOT	内部	外部
プラス	強み Strength	機会 Opportunity
マイナス	弱み Weakness	脅威 Threat

バランススコアカード	財務／顧客／業務プロセス／学習と成長（ 環境は入らない ）
3C	Customer・Competitor・Company
4P	Product・Price・Place・Promotion
コアコンピタンス	他社が真似できない中核の強み

CRM	顧客関係の管理
SCM	供給連鎖（在庫・調達）の最適化
ERP	企業資源を統合管理

BPR / BPO	業務を作り直す / 外注する
RFI → RFP	情報提供依頼 → 提案依頼
SaaS / PaaS / IaaS	完成品 / 土台 / 箱だけ（右ほど自分でやる）

覚え方 損益分岐点 = 固定費 ÷ (1 - 変動費率)。
個数で聞かれたら固定費 ÷ 1個あたりの限界利益。

10 法務

知的財産権の対応 最重要

著作権	表現（ソースコード・文章・音楽）。申請不要で発生
特許権	発明（技術的アイデア）。申請が必要
商標権	商品・サービスの目印
意匠権	デザイン

ひっかけ プログラム言語・規約・解法（アルゴリズム）そのものは著作権で保護されない。守るのは表現であってアイデアではない。

契約の違い

	指揮命令	義務
派遣	派遣先が行う（雇用は派遣元）	作業を行う
請負	発注者ができない	仕事の完成
準委任	発注者ができない	善管注意義務（完成は不要）

ひっかけ 請負で発注者が作業者に直接指示すると偽装請負。
派遣先による事前面接は原則禁止。

不正アクセス禁止法	他人のID・PWを無断で使う行為（実害がなくても違法）
不正競争防止法	営業秘密（顧客名簿・ノウハウ）を守る
個人情報保護法	第三者提供は原則本人の同意が必要（法令に基づく場合は例外）
下請法	立場の弱い下請事業者を守る
製造物責任法（PL法）	製品の欠陥による被害の責任

職務著作：従業員が職務で作ったものは会社に帰属。外部委託は契約で定めない限り受託側に残る。

11 その他

形式	種類	可逆／非可逆
JPEG	写真	非可逆
PNG	静止画	可逆
GIF	静止画・アニメ	可逆（256色）
MP3	音声	非可逆
MPEG	動画	非可逆
ZIP	ファイル全般	可逆

フルブレード	人の誤操作を防ぐ
フェールセーフ	故障時に安全側へ倒す
フェールソフト	機能を縮小して継続
フォールトトレラント	冗長化して動き続ける

デュアル	2台で同じ処理＝結果を照合
デュプレックス	1台が本番・1台が待機
RAID0 / 1 / 5 / 6	冗長性なし / ミラー / 1台まで復元 / 2台まで復元

覚え方 デュアル＝あわせて確認／デュプレックス＝ふだんは1台。
RAIDの0はゼロ＝守りがゼロ、1は1つコピー。