0001 4-1 要求分析・アーキテクチャ > HW/SWトレードオフ ｜ 難易度：基礎

一般に、同じ機能を専用ハードウェアへ実装する場合の特徴として最も適切なものはどれか。

ア．高速化・並列化や決定性を得やすい一方、変更柔軟性や開発コストで不利になる場合がある。
イ．必ずソフトウェアより変更が容易である。
ウ．必ず消費電力が高くなる。
エ．ハードウェアでは並列処理できない。

答え・解説 正答：ア

ア：専用回路は特定処理を効率化しやすいが、仕様変更には回路変更が必要となることがある。
イ：回路変更や再設計が必要になる場合があり、一般化できない。
ウ：専用化によりむしろ低消費電力化できる場合もある。
エ：専用回路は並列化が得意な場合がある。
総合解説：専用回路は特定処理を効率化しやすいが、仕様変更には回路変更が必要となることがある。 この問題では「HW/SW基本比較」として、HW実装とSW実装の代表的な利点・制約を比較できる。

対象：2026年度 / 基準日 2026-09-02

0002 4-1 要求分析・アーキテクチャ > HW/SWトレードオフ ｜ 難易度：基礎

市場投入後に機能仕様の変更が見込まれる処理を実装する際、ソフトウェア実装を選ぶ代表的な利点はどれか。

ア．一度実装すると絶対に変更できない。
イ．ファームウェア更新によって機能変更や不具合修正を行いやすい。
ウ．CPU資源を一切使用しない。
エ．必ずハードウェアより高速である。

答え・解説 正答：イ

ア：ソフトウェアの利点と逆である。
イ：ソフトウェアはプログラム更新により機能を変更でき、将来の仕様変更へ柔軟に対応しやすい。
ウ：ソフトウェア実行にはCPUやメモリ資源が必要である。
エ：処理内容によっては専用HWの方が高速である。
総合解説：ソフトウェアはプログラム更新により機能を変更でき、将来の仕様変更へ柔軟に対応しやすい。 この問題では「SW柔軟性」として、ソフトウェア実装が機能変更や更新へ柔軟に対応しやすいことを理解できる。

対象：2026年度 / 基準日 2026-09-02

0003 4-1 要求分析・アーキテクチャ > HW/SWトレードオフ ｜ 難易度：基礎

HW/SW機能分担を決める際の評価項目として最も適切な組合せはどれか。

ア．CPUクロック周波数だけ。
イ．担当者の好みだけ。
ウ．処理性能、リアルタイム性、消費電力、部品コスト、開発期間、変更容易性、信頼性。
エ．ソースコード行数だけ。

答え・解説 正答：ウ

ア：他の重要な制約を無視している。
イ：客観的な要求に基づく必要がある。
ウ：機能分担は単一指標ではなく、製品要求に関わる複数の制約を総合して判断する。
エ：システム全体の実現性を判断できない。
総合解説：機能分担は単一指標ではなく、製品要求に関わる複数の制約を総合して判断する。 この問題では「評価指標」として、トレードオフ評価で性能だけでなくコスト・電力・変更性も考慮できる。

対象：2026年度 / 基準日 2026-09-02

0004 4-1 要求分析・アーキテクチャ > HW/SWトレードオフ ｜ 難易度：基礎

画像処理の一部をCPUから専用アクセラレータへ移す主な狙いとして適切なものはどれか。

ア．機能更新を必ず不可能にするため。
イ．全てのRAMを不要にするため。
ウ．システム要件を定義しなくてよくするため。
エ．反復的で並列化しやすい処理をオフロードし、性能や電力効率を改善する。

答え・解説 正答：エ

ア：アクセラレータ採用の主目的ではない。
イ：アクセラレータでもデータ保持用メモリが必要である。
ウ：要件に基づく設計は依然必要である。
エ：専用アクセラレータは特定演算を効率的に実行し、CPU負荷を低減できる場合がある。
総合解説：専用アクセラレータは特定演算を効率的に実行し、CPU負荷を低減できる場合がある。 この問題では「アクセラレータ」として、専用アクセラレータへ処理を移す目的を理解できる。

対象：2026年度 / 基準日 2026-09-02

0005 4-1 要求分析・アーキテクチャ > HW/SWトレードオフ ｜ 難易度：標準

1ms周期で実行する信号処理がCPU上では最悪1.4ms掛かる。アルゴリズム最適化後も期限を満たせない。次の検討として最も適切なものはどれか。

ア．DSP・FPGA等へのオフロードや並列化を含むHW/SW分担を再検討する。
イ．平均時間だけ1ms未満なら最悪値を無視する。
ウ．周期を測定しない。
エ．処理をさらに低優先度へする。

答え・解説 正答：ア

ア：ソフトウェアだけで期限を満たせない場合、専用演算資源や並列処理を含むアーキテクチャ変更を検討する。
イ：リアルタイム要件では最悪時間が重要である。
ウ：期限適合を判断できない。
エ：期限超過を悪化させる可能性がある。
総合解説：ソフトウェアだけで期限を満たせない場合、専用演算資源や並列処理を含むアーキテクチャ変更を検討する。 この問題では「期限制約による分担」として、周期と処理時間からHW化の必要性を判断できる。

対象：2026年度 / 基準日 2026-09-02

0006 4-1 要求分析・アーキテクチャ > HW/SWトレードオフ ｜ 難易度：標準

通信プロトコルのパケット形式が顧客ごとに頻繁に変わる。実装方針として適切なものはどれか。

ア．顧客ごとに基板配線を全面変更することだけを選ぶ。
イ．固定的な物理処理はHW、変更頻度の高いプロトコル処理は可能な範囲でSWへ分離する。
ウ．仕様変更を想定せず全処理を固定回路化する。
エ．通信仕様を文書化しない。

答え・解説 正答：イ

ア：変更コストが高くなる。
イ：変更頻度の高い機能をソフトウェア化すると派生対応や更新が容易になる。
ウ：頻繁な変更要求へ不利である。
エ：派生管理が困難になる。
総合解説：変更頻度の高い機能をソフトウェア化すると派生対応や更新が容易になる。 この問題では「変更容易性による分担」として、変更頻度の高い機能をSW側へ寄せる判断ができる。

対象：2026年度 / 基準日 2026-09-02

0007 4-1 要求分析・アーキテクチャ > HW/SWトレードオフ ｜ 難易度：標準

暗号処理がCPU時間の60%を占め、専用暗号エンジン使用時はCPU負荷が15%へ低下する。評価として適切なものはどれか。

ア．CPU負荷が下がるので他条件を一切確認せず必ず採用する。

イ．専用回路を使うとデータ転送時間は常に0になる。

ウ．性能だけでなく専用回路使用時の消費電力、転送オーバヘッド、コスト、安全性も含めて採否を判断する。

エ．専用回路使用時はセキュリティ要件を確認しなくてよい。

答え・解説 正答：ウ

ア：消費電力やコスト等を無視している。
イ：オフロードには設定・転送オーバヘッドがある。
ウ：CPU負荷低減は有力だが、周辺条件を含む総合トレードオフが必要である。
エ：鍵保護等の評価が必要である。
総合解説：CPU負荷低減は有力だが、周辺条件を含む総合トレードオフが必要である。 この問題では「CPU負荷トレードオフ」として、CPU利用率と電力からオフロードの効果を評価できる。

対象：2026年度 / 基準日 2026-09-02

0008 4-1 要求分析・アーキテクチャ > HW/SWトレードオフ ｜ 難易度：標準

少量生産機器で専用ASIC化を検討している。ASICは量産単価を下げられるが初期開発費が非常に高い。最も適切な判断はどれか。

ア．単価だけを見てASICを必ず採用する。

イ．初期費用だけを見てASICを必ず否定する。

ウ．生産数量はコスト判断に無関係である。

エ．予定生産数量、NRE、部品単価、開発期間、将来変更リスクを含め総ライフサイクルコストで比較する。

答え・解説 正答：エ

ア：初期費用を無視している。
イ：大量生産では有利になる可能性がある。
ウ：損益分岐に直結する。
エ：少量生産では初期費用を回収できない可能性があり、FPGAや汎用MCUが有利な場合がある。
総合解説：少量生産では初期費用を回収できない可能性があり、FPGAや汎用MCUが有利な場合がある。 この問題では「コストトレードオフ」として、量産数量とNRE・部品単価のトレードオフを判断できる。

対象：2026年度 / 基準日 2026-09-02

0009 4-1 要求分析・アーキテクチャ > HW/SWトレードオフ ｜ 難易度：標準

主CPUの暴走時にもモータ出力を遮断したい。機能分担として適切な考え方はどれか。

ア．主制御はSWで行い、独立したHW監視や安全回路で異常時の出力遮断を担わせることを検討する。

イ．主CPU自身だけが常に正常と仮定する。

ウ．異常時は出力を最大化する。

エ．監視機能を削除する。

答え・解説 正答：ア

ア：主CPUと独立した監視経路を設けると共通故障の影響を抑えられる。

イ：単一故障で安全機能が失われる可能性がある。

ウ：フェールセーフではない。

エ：安全要求を満たしにくい。

総合解説：主CPUと独立した監視経路を設けると共通故障の影響を抑えられる。 この問題では「安全監視分担」として、安全機能で独立ハードウェア監視を組み合わせる意義を判断できる。

対象：2026年度 / 基準日 2026-09-02

0010 4-1 要求分析・アーキテクチャ > HW/SWトレードオフ ｜ 難易度：標準

高速パルス計測は数十ns精度が必要だが、結果の判定ロジックは将来変更が多い。適切な分担はどれか。

ア．全てを低速ポーリングSWだけで実装する。

イ．時間精度が必要な計測部分をFPGA等へ、変更頻度の高い判定ロジックをCPUソフトへ分担する。

ウ．判定ロジックまで全て固定回路にして変更性を無視する。

エ．計測精度要求を削除する。

答え・解説 正答：イ

ア：数十ns精度を満たしにくい。

イ：厳しいタイミングをHWへ、柔軟性が必要な部分をSWへ置く典型的な分担である。

ウ：将来変更要求へ不利である。

エ：要件変更なしには不適切である。

総合解説：厳しいタイミングをHWへ、柔軟性が必要な部分をSWへ置く典型的な分担である。 この問題では「FPGA協調構成」として、FPGAとCPUの協調構成を性能と柔軟性から設計できる。

対象：2026年度 / 基準日 2026-09-02

0011 4-1 要求分析・アーキテクチャ > HW/SWトレードオフ ｜ 難易度：応用

CPUで行っていた画像前処理をFPGAへ移すことになった。変更影響として最も適切なものはどれか。

ア．処理場所だけ変わるのでインタフェースは全く変わらない。

イ．FPGAへ移せばテストは不要になる。

ウ．CPU-FPGA間データ転送、バッファ、レイテンシ、同期、エラー処理、テスト分担を再設計する必要がある。

エ．CPU側の負荷測定は不要になる。

答え・解説 正答：ウ

ア：データ経路や同期が変わり得る。

イ：HW側ロジックと統合試験が必要である。

ウ：機能を別実装主体へ移すと境界インタフェースとタイミング条件も変化するため総合評価が必要である。

エ：オフロード後のシステム性能を再確認する必要がある。

総合解説：機能を別実装主体へ移すと境界インタフェースとタイミング条件も変化するため総合評価が必要である。 この問題では「分担変更影響」として、分担変更がインタフェース・テスト・性能へ波及することを評価できる。

対象：2026年度 / 基準日 2026-09-02

0012 4-1 要求分析・アーキテクチャ > HW/SWトレードオフ ｜ 難易度：応用

案AはCPUのみで部品費1000円・消費電力4W・応答3ms、案BはFPGA追加で部品費1800円・消費電力2W・応答0.5msである。要求は応答1ms以下、消費電力3W以下である。最も適切な判断はどれか。

ア．部品費が安いので案Aを採用する。

イ．応答時間だけ見て案Bを無条件採用する。

ウ．どちらも同等なので評価不要とする。

エ．要求だけを見ると案Bが適合し、さらにコスト上限や開発期間など他要求を確認して採用可否を決める。

答え・解説 正答：エ

ア：必須性能要件を満たしていない。

イ：コスト等の制約確認が残る。

ウ：定量値が明確に異なる。

エ：案Aは応答・電力要件を満たさず、案Bは両方を満たしている。最終判断には残りの制約も必要である。

総合解説：案Aは応答・電力要件を満たさず、案Bは両方を満たしている。最終判断には残りの制約も必要である。 この問題では「定量トレードオフ」として、HW/SW分担を複数案の定量比較で決定できる。

対象：2026年度 / 基準日 2026-09-02

0013 4-1 要求分析・アーキテクチャ > 機能分担・システムアーキテクチャ ｜ 難易度：基礎

システムアーキテクチャ記述で表現すべき内容として最も適切なものはどれか。

ア．主要な構成要素、それらの責務、インタフェース、相互関係、配置など。
イ．ソースコードの全行だけ。
ウ．製品価格だけ。
エ．開発者名簿だけ。

答え・解説 正答：ア

ア：アーキテクチャ記述は関心事に応じたビューやモデルでシステム構造と関係を表現する。
イ：実装詳細だけではアーキテクチャ全体を表せない。
ウ：構造記述ではない。
エ：システム構成とは無関係である。
総合解説：アーキテクチャ記述は関心事に応じたビューやモデルでシステム構造と関係を表現する。 この問題では「Architecture基本」として、システムアーキテクチャが構成要素と関係を表すことを理解できる。

対象：2026年度 / 基準日 2026-09-02

0014 4-1 要求分析・アーキテクチャ > 機能分担・システムアーキテクチャ ｜ 難易度：基礎

同じシステムについて、論理構成、実行時通信、ハードウェア配置を別々の図で表す主な理由はどれか。

ア．図を増やすこと自体が目的だから。
イ．利害関係者の異なる関心事を、それぞれ理解しやすいビューで表現するため。
ウ．全図が同一内容でなければならないから。
エ．アーキテクチャでは関係者の関心事を扱わないから。

答え・解説 正答：イ

ア：表現目的は関心事の明確化である。
イ：ISO 42010では関心事とViewpoint/Viewを用いてアーキテクチャ記述を構成する。
ウ：異なる観点を表す。
エ：むしろ関心事が重要である。
総合解説：ISO 42010では関心事とViewpoint/Viewを用いてアーキテクチャ記述を構成する。 この問題では「Architecture View」として、関心事ごとにビューを分ける意義を理解できる。

対象：2026年度 / 基準日 2026-09-02

0015 4-1 要求分析・アーキテクチャ > 機能分担・システムアーキテクチャ ｜ 難易度：基礎

「衝突を検知して100ms以内に警報を出す」という上位機能を設計するときの適切な進め方はどれか。

ア．要求を分解せず担当者ごとに自由実装する。
イ．警報出力だけ設計し検知処理を考えない。
ウ．検知、判定、通信、警報出力などへ機能分解し、各要素へ時間予算と責務を割り当てる。
エ．100msという時間要求を削除する。

答え・解説 正答：ウ

ア：責務重複や抜けが起こりやすい。
イ：要求全体を満たせない。
ウ：上位要求を実現可能な下位機能へ分解し、責務とインタフェースを明確にする。
エ：要件変更なしには不適切である。
総合解説：上位要求を実現可能な下位機能へ分解し、責務とインタフェースを明確にする。 この問題では「機能分解」として、機能分解で上位要求を下位機能へ割り当てられる。

対象：2026年度 / 基準日 2026-09-02

0016 4-1 要求分析・アーキテクチャ > 機能分担・システムアーキテクチャ ｜ 難易度：標準

アプリケーションロジックが各種デバイスレジスタを直接操作しており、MCU変更時に大規模修正が必要になっている。改善として適切なものはどれか。

ア．さらに多くのレジスタアドレスをアプリへ埋め込む。
イ．MCU変更時は必ず全機能を書き直す。
ウ．層間インタフェースを定義しない。
エ．HAL/ドライバ層を設け、上位層は抽象インタフェースを通じてデバイスを利用する。

答え・解説 正答：エ

ア：依存が強くなる。
イ：アーキテクチャ改善の余地がある。
ウ：依存関係が曖昧になる。
エ：依存を下位層へ閉じ込めることで上位機能の移植性を高められる。
総合解説：依存を下位層へ閉じ込めることで上位機能の移植性を高められる。 この問題では「Layered Architecture」として、レイヤ構造で依存方向を整理できる。

対象：2026年度 / 基準日 2026-09-02

0017 4-1 要求分析・アーキテクチャ > 機能分担・システムアーキテクチャ ｜ 難易度：標準

一つのMCUで全処理を行っていたシステムを二つのECUへ分散する。追加で検討すべき事項はどれか。

ア．ECU間通信遅延、同期、通信障害、データ整合性、起動順序を設計する。
イ．処理を分ければ通信設計は不要になる。
ウ．両ECUの時刻は必ず自動一致する。
エ．通信断は考慮しなくてよい。

答え・解説 正答：ア

ア：分散化するとネットワーク越しの相互作用と部分故障を扱う必要が生じる。
イ：むしろ必要になる。
ウ：時刻同期の設計が必要な場合がある。
エ：分散システムの代表的故障モードである。
総合解説：分散化するとネットワーク越しの相互作用と部分故障を扱う必要が生じる。 この問題では「分散アーキテクチャ」として、分散構成で通信遅延と障害境界を考慮できる。

対象：2026年度 / 基準日 2026-09-02

0018 4-1 要求分析・アーキテクチャ > 機能分担・システムアーキテクチャ ｜ 難易度：標準

複数機能がそれぞれ独自に時刻管理・ログ記録・不揮発保存を実装している。改善として適切なものはどれか。

ア．各機能でさらに別実装を増やす。
イ．共通サービスとして責務とAPIを定義し、各機能から利用できる構成を検討する。
ウ．時刻やログの仕様を機能ごとに無管理で変える。
エ．全共通機能を割込みハンドラへ入れる。

答え・解説 正答：イ

ア：重複と不整合が増える。
イ：横断機能を共通化すると重複実装を減らし、一貫性や再利用性を高められる。
ウ：統合時の整合性が悪化する。
エ：責務分離にならない。
総合解説：横断機能を共通化すると重複実装を減らし、一貫性や再利用性を高められる。 この問題では「共通サービス」として、共有サービスを共通化して重複実装を減らせる。

対象：2026年度 / 基準日 2026-09-02

0019 4-1 要求分析・アーキテクチャ > 機能分担・システムアーキテクチャ ｜ 難易度：標準

安全停止機能とユーザー向けUI機能が同じCPUで動く。UIの暴走が安全機能へ影響しないようにする方策として適切なものはどれか。

ア．全タスクに同じ権限で全メモリ書込みを許可する。
イ．UIタスクを最高優先度に固定する。
ウ．MPU等の保護、優先度・時間予算、通信境界を用いて安全機能を論理的に分離する。
エ．安全機能とUIの境界を定義しない。

答え・解説 正答：ウ

ア：干渉リスクが高い。
イ：安全機能を阻害し得る。
ウ：共有資源を使う場合でも空間・時間の干渉を制御する必要がある。
エ：影響分析ができない。
総合解説：共有資源を使う場合でも空間・時間の干渉を制御する必要がある。 この問題では「安全パーティショニング」として、安全系と非安全系の干渉をアーキテクチャで分離できる。

対象：2026年度 / 基準日 2026-09-02

0020 4-1 要求分析・アーキテクチャ > 機能分担・システムアーキテクチャ ｜ 難易度：標準

カメラ近傍ECUで生成する毎秒100MBの画像を中央ECUへ全量転送して物体検出しているためネットワークが逼迫している。改善案として適切なものはどれか。

ア．通信帯域を測らず同じ全量転送を続ける。
イ．画像を無条件に破棄する。
ウ．全ECUを同じ共有RAMとして扱う。
エ．カメラ側で前処理・特徴抽出を行い、中央ECUへ必要情報だけ送るエッジ処理を検討する。

答え・解説 正答：エ

ア：逼迫問題を解決しない。
イ：機能要件を満たさない。
ウ：物理的に分散しているため成立しない。
エ：データ生成源に近い場所で処理すると通信量と遅延を削減できる場合がある。
総合解説：データ生成源に近い場所で処理すると通信量と遅延を削減できる場合がある。 この問題では「機能配置最適化」として、機能配置でデータ局所性と通信量を考慮できる。

対象：2026年度 / 基準日 2026-09-02

0021 4-1 要求分析・アーキテクチャ > 機能分担・システムアーキテクチャ ｜ 難易度：応用

全センサ情報が一つの通信ゲートウェイを必ず経由し、そのゲートウェイ故障で全機能が停止する。アーキテクチャ上の問題として最も適切なものはどれか。

ア．ゲートウェイが単一障害点となっており、要求に応じて冗長経路や縮退運転を検討すべきである。

イ．中継点が一つなら必ず信頼性が最大になる。

ウ．ゲートウェイ故障はシステムアーキテクチャと無関係である。

エ．全センサを停止すれば解決する。

答え・解説 正答：ア

ア：一要素の故障がシステム全体へ波及する構成は高可用性・安全性の観点で評価が必要である。

イ：単一故障点になり得る。

ウ：機能依存関係の問題である。

エ：機能を失う。

総合解説：一要素の故障がシステム全体へ波及する構成は高可用性・安全性の観点で評価が必要である。 この問題では「Single Point of Failure」として、単一障害点を識別して冗長化やフォールバックを検討できる。

対象：2026年度 / 基準日 2026-09-02

0022 4-1 要求分析・アーキテクチャ > 機能分担・システムアーキテクチャ ｜ 難易度：応用

要求はセンサ入力からアクチュエータ出力まで20ms以内である。センサ5ms、通信4ms、アクチュエータ3msが固定で必要な場合、処理系へ割り当て可能な残り時間は最大何msか。

ア．12ms（固定時間の一部だけを控除）

イ．8ms（20-5-4-3）

ウ．20ms（他要素を控除しない）

エ．2ms（残時間を過小に換算）

答え・解説 正答：イ

ア：通信またはアクチュエータ時間を差し引いていない。

イ：20-5-4-3=8msである。実際にはジッタや安全余裕も考慮する。

ウ：他構成要素の時間を無視している。

エ：計算結果と一致しない。

総合解説：20-5-4-3=8msである。実際にはジッタや安全余裕も考慮する。 この問題では「Latency Budget」として、性能予算を構成要素へ配分してアーキテクチャを評価できる。

対象：2026年度 / 基準日 2026-09-02

0023 4-1 要求分析・アーキテクチャ > インタフェース・要求仕様 ｜ 難易度：基礎

次のうち、検証可能な要求として最も適切なものはどれか。

ア．できるだけ早く起動する。
イ．使いやすくする。
ウ．電源投入後2.0秒以内に通常画面を表示する。
エ．高性能にする。

答え・解説 正答：ウ

ア：基準が曖昧で合否判定できない。
イ：評価基準が不足している。
ウ：時間条件が定量化されており、試験で合否判定できる。
エ：性能指標が定義されていない。
総合解説：時間条件が定量化されており、試験で合否判定できる。 この問題では「検証可能な要求」として、良い要求が明確で検証可能である必要性を理解できる。

対象：2026年度 / 基準日 2026-09-02

0024 4-1 要求分析・アーキテクチャ > インタフェース・要求仕様 ｜ 難易度：基礎

ECU間通信インタフェース仕様に含めるべき情報として最も適切なものはどれか。

ア．信号名だけ。
イ．担当者名だけ。
ウ．配線色だけ。
エ．メッセージID、データ型・単位・範囲、周期、タイムアウト、エラー時の扱い、初期値。

答え・解説 正答：エ

ア：意味・タイミング・異常処理が不明である。
イ：インタフェース契約ではない。
ウ：論理通信仕様として不十分である。
エ：通信相手との契約を定量的に定義すると、独立開発と統合検証がしやすい。
総合解説：通信相手との契約を定量的に定義すると、独立開発と統合検証がしやすい。 この問題では「Interface Requirement」として、外部インタフェース要求にデータ形式・タイミング・異常時動作を含める必要性を理解できる。

対象：2026年度 / 基準日 2026-09-02

0025 4-1 要求分析・アーキテクチャ > インタフェース・要求仕様 ｜ 難易度：標準

要求書に「温度が高くなったら速やかにファンを回す」とある。改善として最も適切なものはどれか。

ア．温度しきい値、判定時間、ファン開始までの許容時間、ヒステリシス等を定量化する。
イ．そのまま実装者の感覚に任せる。
ウ．「速やかに」を「すぐ」に置き換える。
エ．温度条件を削除する。

答え・解説 正答：ア

ア：曖昧語を測定可能な条件へ変換すると設計とテストの基準になる。
イ：実装差と検証困難を招く。
ウ：曖昧さは解消しない。
エ：要求目的を失う。
総合解説：曖昧語を測定可能な条件へ変換すると設計とテストの基準になる。 この問題では「要求具体化」として、要求の曖昧表現を定量条件へ変換できる。

対象：2026年度 / 基準日 2026-09-02

0026 4-1 要求分析・アーキテクチャ > インタフェース・要求仕様 ｜ 難易度：標準

要求Aは「待機時消費電力1W以下」、要求Bは「待機中も全通信器を常時最高出力で動作」と規定しており両立しない。適切な対応はどれか。

ア．両方満たせないまま実装を開始する。
イ．要求の優先度・根拠を確認し、利害関係者と矛盾を解消して更新する。
ウ．担当者が任意に一方を無視する。
エ．矛盾を仕様書に記録せず隠す。

答え・解説 正答：イ

ア：後工程で重大な手戻りとなる。
イ：要求間整合性を確認し、実現不能な組合せを設計へ持ち込まないことが重要である。
ウ：正式な要求変更が必要である。
エ：レビュー・検証性が低下する。
総合解説：要求間整合性を確認し、実現不能な組合せを設計へ持ち込まないことが重要である。 この問題では「要求整合性」として、要求間の矛盾を検出して解消できる。

対象：2026年度 / 基準日 2026-09-02

0027 4-1 要求分析・アーキテクチャ > インタフェース・要求仕様 ｜ 難易度：標準

安全要求変更時に影響する設計要素とテストケースを迅速に特定したい。適切な方策はどれか。

ア．要求IDを付けず文書を自由記述だけにする。
イ．テスト結果だけ保存して要求を削除する。
ウ．要求IDと設計要素、実装、テストケースの対応関係を双方向に管理する。
エ．変更後も古い対応表を更新しない。

答え・解説 正答：ウ

ア：対応関係を追いにくい。
イ：検証根拠を失う。
ウ：トレーサビリティにより変更影響と検証漏れを追跡しやすくなる。
エ：不整合が残る。
総合解説：トレーサビリティにより変更影響と検証漏れを追跡しやすくなる。 この問題では「Requirement Traceability」として、要求トレーサビリティで上位要求と設計・テストを対応付けられる。

対象：2026年度 / 基準日 2026-09-02

0028 4-1 要求分析・アーキテクチャ > インタフェース・要求仕様 ｜ 難易度：標準

ECU Aは速度をkm/h×100の整数、ECU Bはm/sの浮動小数点と解釈している。問題の本質はどれか。

ア．CPUクロックが異なることだけが原因である。
イ．通信周期が同じなら問題はない。
ウ．エラー検出を無効化すれば解決する。
エ．インタフェース仕様で単位・スケーリング・データ型が統一されていない。

答え・解説 正答：エ

ア：データ意味の不一致が直接原因である。
イ：値の解釈は一致しない。
ウ：意味不一致を悪化させる。
エ：同じビット列でも意味の解釈が異なれば重大な統合不具合になる。
総合解説：同じビット列でも意味の解釈が異なれば重大な統合不具合になる。 この問題では「データ表現契約」として、単位・エンディアン・スケーリングの不一致をインタフェース設計で防げる。

対象：2026年度 / 基準日 2026-09-02

0029 4-1 要求分析・アーキテクチャ > インタフェース・要求仕様 ｜ 難易度：応用

センサECUから100ms周期で値を受けるが通信断時の扱いが未定義で、受信側が最後の値を永久使用している。改善として最も適切なものはどれか。

ア．許容更新間隔、タイムアウト、無効値表現、フォールバック動作をインタフェース要求として定義する。

イ．最後の値を無期限に正しいとみなす。

ウ．タイムスタンプを削除する。

エ．通信断は起こらない前提にする。

答え・解説 正答：ア

ア：通信異常時の契約を明示すると受信側が古い値を誤使用する危険を抑えられる。

イ：通信断で実状態と乖離する可能性がある。

ウ：鮮度判定がさらに困難になる。

エ：現実的な故障モードを無視している。

総合解説：通信異常時の契約を明示すると受信側が古い値を誤使用する危険を抑えられる。 この問題では「Timeout契約」として、異常時インタフェース要求を明示して安全な統合ができる。

対象：2026年度 / 基準日 2026-09-02

0030 4-1 要求分析・アーキテクチャ > インタフェース・要求仕様 ｜ 難易度：応用

インタフェース要求が「10ms周期、最大ジッタ1ms、欠損3周期で異常判定、値範囲0〜100」である。適切な検証はどれか。

ア．正常値50を1回送るだけ。

イ．周期・ジッタを計測し、3周期欠損を注入して異常判定を確認し、境界値0と100および範囲外入力を試験する。

ウ．通信内容を目視するだけで合格とする。

エ．ジッタとタイムアウト要求を無視する。

答え・解説 正答：イ

ア：タイミング・欠損・境界条件を検証できない。

イ：各要求を測定可能な試験条件へ展開することでインタフェース適合を総合確認できる。

ウ：定量要求を判定できない。

エ：要求の一部しか検証していない。

総合解説：各要求を測定可能な試験条件へ展開することでインタフェース適合を総合確認できる。 この問題では「Interface Acceptance Criteria」として、複数要求をインタフェース試験へ変換できる。

対象：2026年度 / 基準日 2026-09-02

0031 4-2 制御・性能設計 > フィードバック・PID制御 ｜ 難易度：基礎

負帰還フィードバック制御の基本的な考え方として最も適切なものはどれか。

ア．出力を一切測定せず常に同じ操作量を与える。
イ．偏差が大きいほど目標から離れる方向へ操作する。
ウ．目標値と測定値の偏差を用いて、偏差を小さくする方向へ操作量を調整する。
エ．制御対象の出力を使わないことが必須である。

答え・解説 正答：ウ

ア：これは開ループ制御に近い。
イ：負帰還とは逆である。
ウ：フィードバック制御では出力を測定し、目標との差に基づいて入力を補正する。
エ：フィードバックでは出力情報を利用する。
総合解説：フィードバック制御では出力を測定し、目標との差に基づいて入力を補正する。 この問題では「Feedback Control」として、フィードバック制御が目標値と測定値の偏差を用いて操作量を決めることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0032 4-2 制御・性能設計 > フィードバック・PID制御 ｜ 難易度：基礎

PID制御の積分I項の代表的な効果はどれか。

ア．偏差の変化率だけに反応する。
イ．現在偏差だけに比例する。
ウ．測定値を無視して固定出力を出す。
エ．偏差の累積に反応し、定常偏差を小さくする方向へ働く。

答え・解説 正答：エ

ア：これは微分D項の役割である。
イ：これは比例P項である。
ウ：PIDの説明ではない。
エ：積分項は過去の偏差を蓄積して補償し、定常偏差の除去に寄与する。
総合解説：積分項は過去の偏差を蓄積して補償し、定常偏差の除去に寄与する。 この問題では「PID各項」として、PIDのP・I・D各項の代表的役割を区別できる。

対象：2026年度 / 基準日 2026-09-02

0033 4-2 制御・性能設計 > フィードバック・PID制御 ｜ 難易度：基礎

PID制御の微分D項について最も適切な説明はどれか。

ア．偏差の変化率に応じて作用し、急激な変化を抑える方向の補償に利用される。

イ．偏差を時間積分した値だけを使う。

ウ．現在偏差に比例するだけである。

エ．常にノイズを完全除去する。

答え・解説 正答：ア

ア：微分項は誤差の変化傾向へ反応し、応答性や減衰特性の調整に使われる。

イ：積分I項である。

ウ：比例P項である。

エ：微分は高周波ノイズに敏感であり注意が必要である。

総合解説：微分項は誤差の変化傾向へ反応し、応答性や減衰特性の調整に使われる。 この問題では「Derivative Action」として、微分項が偏差変化に反応し応答の先読み的補償に使われることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0034 4-2 制御・性能設計 > フィードバック・PID制御 ｜ 難易度：標準

比例ゲインKpを大きくして応答を速くしたところ、オーバシュートと振動が増えた。最も適切な判断はどれか。

ア．Kpは大きいほど必ず安定性も高くなる。

イ．Kpを上げすぎると安定余裕が減る場合があり、応答速度とオーバシュートのバランスを再調整する。

ウ．振動はフィードバック制御と無関係である。

エ．Kpを無限大にすれば最適制御になる。

答え・解説 正答：イ

ア：一般にはそうとは限らない。

イ：比例ゲイン増加は偏差修正を強めるが、制御対象によっては振動的になる。

ウ：ゲイン設定が応答特性へ影響する。

エ：飽和や不安定化を招く可能性がある。

総合解説：比例ゲイン増加は偏差修正を強めるが、制御対象によっては振動的になる。 この問題では「Pゲイン調整」として、比例ゲイン増加が応答性と振動・オーバシュートのトレードオフを持つことを判断できる。

対象：2026年度 / 基準日 2026-09-02

0035 4-2 制御・性能設計 > フィードバック・PID制御 ｜ 難易度：標準

アクチュエータ出力が上限に張り付いている間も積分項が増え続け、復帰後に大きなオーバシュートが出る。この現象と対策の組合せはどれか。

ア．Aliasingでありサンプリング周波数だけを上げる。
イ．DeadlockでありMutexを増やす。
ウ．Integral Windupであり、積分制限やBack-calculation等のアンチワインドアップを検討する。
エ．Memory LeakでありHeapを増やす。

答え・解説 正答：ウ

ア：別の現象である。
イ：同期問題ではない。
ウ：出力飽和中の積分蓄積を制御すると復帰時の過大応答を抑えやすい。
エ：メモリ管理問題ではない。
総合解説：出力飽和中の積分蓄積を制御すると復帰時の過大応答を抑えやすい。 この問題では「Integral Windup」として、積分飽和とアンチワインドアップの必要性を理解できる。

対象：2026年度 / 基準日 2026-09-02

0036 4-2 制御・性能設計 > フィードバック・PID制御 ｜ 難易度：標準

位置センサに高周波ノイズが重畳しており、D項を増やしたら操作量が細かく振動するようになった。適切な対応はどれか。

ア．D項をさらに無限大へ増やす。
イ．センサノイズは微分項に影響しないとみなす。
ウ．フィードバックを全て削除する。
エ．微分項のフィルタリング、ゲイン調整、測定ノイズ低減を検討する。

答え・解説 正答：エ

ア：ノイズ影響を悪化させる可能性がある。
イ：変化率計算へ強く影響する。
ウ：要求次第では制御性能を失う。
エ：微分演算は高周波成分を強調しやすいため、ノイズ対策と適切なD設定が必要である。
総合解説：微分演算は高周波成分を強調しやすいため、ノイズ対策と適切なD設定が必要である。 この問題では「D項とノイズ」として、微分項が測定ノイズを増幅しやすいことを判断できる。

対象：2026年度 / 基準日 2026-09-02

0037 4-2 制御・性能設計 > フィードバック・PID制御 ｜ 難易度：標準

同じPIDゲインを使ったまま制御周期を10msから100msへ変更した。注意すべき点はどれか。

ア．離散化された積分・微分の効果と位相遅れが変わるため、安定性と応答を再評価する必要がある。
イ．制御周期はPID挙動に一切影響しない。
ウ．周期を長くするほど必ず安定性が上がる。
エ．ゲインはどの周期でも同一なら必ず最適である。

答え・解説 正答：ア

ア：サンプリング周期は離散制御器の実効特性へ影響する。
イ：離散実装では影響する。
ウ：一般化できない。
エ：再調整が必要になる場合がある。
総合解説：サンプリング周期は離散制御器の実効特性へ影響する。 この問題では「Discrete PID」として、離散PIDでサンプリング周期が制御応答へ影響することを理解できる。

対象：2026年度 / 基準日 2026-09-02

0038 4-2 制御・性能設計 > フィードバック・PID制御 ｜ 難易度：標準

PID計算値がモータ指令範囲-100〜100を超える場合の実装として最も適切なものはどれか。

ア．計算値500をそのまま物理モータへ与えられると仮定する。
イ．出力を物理範囲へ制限し、積分器も飽和を考慮した処理にする。
ウ．範囲外でも積分値を無制限に増やす。
エ．出力制限をするとPIDではなくなる。

答え・解説 正答：イ

ア：アクチュエータ範囲を超えている。
イ：実アクチュエータの制約を制御器へ反映し、Windupを防ぐ必要がある。
ウ：Windupを招く。
エ：実装上必要な制約処理である。
総合解説：実アクチュエータの制約を制御器へ反映し、Windupを防ぐ必要がある。 この問題では「Actuator Saturation」として、制御出力飽和を考慮して実装できる。

対象：2026年度 / 基準日 2026-09-02

0039 4-2 制御・性能設計 > フィードバック・PID制御 ｜ 難易度：応用

1kHz制御ループでセンサ取得200μs、PID計算150μs、通信500μs、出力更新200μs掛かる。単純合計では1周期内に収まるか。

ア．合計950μsなので収まる。
イ．通信時間は制御遅延に含めない。
ウ．合計1050μsで1msを超えるため、そのままでは周期内完了できない。
エ．平均値なら周期超過しても必ず問題ない。

答え・解説 正答：ウ

ア：加算が誤っている。
イ：閉ループ経路に含まれるなら考慮が必要である。
ウ：200+150+500+200=1050μsであり、さらにジッタもあるため改善が必要である。
エ：リアルタイム制御では期限を評価する。
総合解説：200+150+500+200=1050μsであり、さらにジッタもあるため改善が必要である。 この問題では「Control Loop Latency」として、制御周期と計算遅延を含めてPID性能を評価できる。

対象：2026年度 / 基準日 2026-09-02

0040 4-2 制御・性能設計 > フィードバック・PID制御 ｜ 難易度：応用

温度制御で要求が「オーバシュート2℃以下、定常偏差0.5℃以下、整定時間30秒以下」である。適切な調整手順はどれか。

ア．Kpだけ最大にして他要求を測らない。
イ．定常偏差だけ見てオーバシュートを無視する。
ウ．調整後の実機確認を一切行わない。
エ．モデルまたは実機応答を用いてKp・Ki・Kdを調整し、各定量要求をシミュレーションと実測で確認する。

答え・解説 正答：エ

ア：定量要求を満たす保証がない。
イ：複数要求を同時に満たす必要がある。
ウ：モデル誤差や実装影響を確認できない。
エ：PID調整は応答性と安定性をバランスさせ、要求指標で検証する必要がある。
総合解説：PID調整は応答性と安定性をバランスさせ、要求指標で検証する必要がある。 この問題では「PID Tuning Criteria」として、制御要求からPID調整の評価指標を選べる。

対象：2026年度 / 基準日 2026-09-02

0041 4-2 制御・性能設計 > 信号処理・計測制御 ｜ 難易度：基礎

サンプリング周波数が10kHzのADCで、ナイキスト周波数はいくらか。

ア．5kHz（サンプリング周波数の1/2）
イ．10kHz（サンプリング周波数そのもの）
ウ．20kHz（サンプリング周波数の2倍）
エ．1kHz（サンプリング周波数の1/10）

答え・解説 正答：ア

ア：ナイキスト周波数はサンプリング周波数の半分である。
イ：サンプリング周波数そのものである。
ウ：2倍している。
エ：計算結果と一致しない。
総合解説：ナイキスト周波数はサンプリング周波数の半分である。 この問題では「Nyquist Frequency」として、サンプリング周波数とナイキスト周波数の関係を理解できる。

対象：2026年度 / 基準日 2026-09-02

0042 4-2 制御・性能設計 > 信号処理・計測制御 ｜ 難易度：基礎

ADC入力前にアナログローパスフィルタを設ける主な目的はどれか。

ア．ADC分解能を必ず2倍にする。
イ．ナイキスト周波数を超える成分を減衰させ、エイリアシングを抑える。
ウ．サンプリング周波数を自動変更する。
エ．信号を必ず直流へ変換する。

答え・解説 正答：イ

ア：フィルタでビット数は増えない。
イ：高周波成分がサンプリング後に低周波へ折り返すことを防ぐためである。
ウ：フィルタ自体はADCクロックを変更しない。
エ：必要帯域を通過させる設計が一般的である。
総合解説：高周波成分がサンプリング後に低周波へ折り返すことを防ぐためである。 この問題では「Anti-Aliasing」として、アンチエイリアスフィルタの目的を理解できる。

対象：2026年度 / 基準日 2026-09-02

0043 4-2 制御・性能設計 > 信号処理・計測制御 ｜ 難易度：基礎

短周期のランダムノイズを含む温度データを平滑化したい。単純な方法として適切なものはどれか。

ア．毎回最大値だけを出力する。
イ．ADC入力を無条件に0へ固定する。
ウ．複数サンプルの移動平均を取る。
エ．サンプリングを停止する。

答え・解説 正答：ウ

ア：ノイズ除去ではなく上方向に偏る。
イ：計測機能を失う。
ウ：移動平均は有限窓内のサンプルを平均し、短周期変動を平滑化できる。
エ：データが得られない。
総合解説：移動平均は有限窓内のサンプルを平均し、短周期変動を平滑化できる。 この問題では「Moving Average」として、移動平均フィルタがノイズ平滑化に使えることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0044 4-2 制御・性能設計 > 信号処理・計測制御 ｜ 難易度：標準

入力範囲0〜3.3Vの12ビットADCで、理想的な1LSB幅は約何mVか。

ア．約3.3mV（フルスケールを約1000分割）
イ．約12mV（ビット数12を分母に使用）
ウ．約0.081mV（1LSBを約1/10側へ換算）
エ．約0.806mV（3.3V÷4096）

答え・解説 正答：エ

ア：約4倍大きい。
イ：ビット数を分母にしている。
ウ：約10分の1である。
エ：3.3V/4096≈0.000806Vで約0.806mVである。
総合解説：3.3V/4096≈0.000806Vで約0.806mVである。 この問題では「ADC Resolution」として、ADC分解能から1LSBの電圧幅を計算できる。

対象：2026年度 / 基準日 2026-09-02

0045 4-2 制御・性能設計 > 信号処理・計測制御 ｜ 難易度：標準

ADCの量子化誤差について最も適切な説明はどれか。

ア．連続的な入力値を有限段階のデジタル値へ丸めることで生じる誤差。
イ．通信パケットが欠落したことで生じる誤差だけ。
ウ．センサ配線が断線した場合だけ発生する。
エ．浮動小数点を使えばADC量子化は消える。

答え・解説 正答：ア

ア：有限ビット数では入力振幅を離散レベルへ割り当てるため量子化誤差が発生する。
イ：通信欠損とは別である。
ウ：ADC分解能由来の誤差である。
エ：変換段階の有限分解能は残る。
総合解説：有限ビット数では入力振幅を離散レベルへ割り当てるため量子化誤差が発生する。 この問題では「Quantization Error」として、量子化誤差が有限分解能による離散化誤差であることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0046 4-2 制御・性能設計 > 信号処理・計測制御 ｜ 難易度：標準

ノイズ低減のため移動平均窓を4点から100点へ増やしたところ制御応答が遅くなった。理由として適切なものはどれか。

ア．窓を増やすと必ずADC分解能が下がるから。
イ．平滑化が強くなる一方、フィルタによる遅延・位相遅れが増えた。
ウ．移動平均は遅延を一切持たない。
エ．制御応答と信号処理は無関係だから。

答え・解説 正答：イ

ア：直接の理由ではない。
イ：長い窓は高周波ノイズを抑えやすいが、信号変化への追従が遅くなる。
ウ：時間窓を用いるため遅れが生じる。
エ：閉ループ内のフィルタ遅延は応答へ影響する。
総合解説：長い窓は高周波ノイズを抑えやすいが、信号変化への追従が遅くなる。 この問題では「Filter Delay」として、デジタルフィルタによる遅延を制御ループで考慮できる。

対象：2026年度 / 基準日 2026-09-02

0047 4-2 制御・性能設計 > 信号処理・計測制御 ｜ 難易度：標準

最大周波数200Hz程度の振動を計測する。理論的な最低条件だけでなくフィルタ設計余裕も確保したい。適切な考え方はどれか。

ア．100Hzでサンプリングする。

イ．サンプリング周波数は対象帯域と無関係である。

ウ．400Hzを上回る十分高いサンプリング周波数を選び、アンチエイリアスフィルタの遷移帯域も考慮する。

エ．1Hzで十分である。

答え・解説 正答：ウ

ア：200Hz信号を正しく表現できない。

イ：エイリアシングに直結する。

ウ：ナイキスト条件だけぎりぎりでは実フィルタの余裕が少ないため、より高いサンプルレートを選ぶことが多い。

エ：帯域に対して低すぎる。

総合解説：ナイキスト条件だけぎりぎりでは実フィルタの余裕が少ないため、より高いサンプルレートを選ぶことが多い。 この問題では「Sampling Rate Selection」として、サンプリング周期と対象信号帯域を整合させられる。

対象：2026年度 / 基準日 2026-09-02

0048 4-2 制御・性能設計 > 信号処理・計測制御 ｜ 難易度：標準

真値0℃でセンサ出力2℃、真値100℃で出力104℃だった。誤差の特徴として最も適切なものはどれか。

ア．完全に誤差がない。

イ．量子化誤差だけで必ず説明できる。

ウ．通信遅延だけが原因である。

エ．オフセット誤差に加えてゲイン誤差も含まれている可能性がある。

答え・解説 正答：エ

ア：測定値が真値と一致していない。

イ：二点の系統的ずれから校正係数も検討すべきである。

ウ：静的な値のずれを直接説明しない。

エ：0点で2℃ずれ、100℃点では4℃ずれているため単純な一定オフセットだけでは説明しにくい。

総合解説：0点で2℃ずれ、100℃点では4℃ずれているため単純な一定オフセットだけでは説明しにくい。この問題では「Sensor Calibration」として、センサ校正でオフセットとゲイン誤差を補正できる。

対象：2026年度 / 基準日 2026-09-02

0049 4-2 制御・性能設計 > 信号処理・計測制御 ｜ 難易度：応用

浮動小数点FIRをQ15固定小数点へ移植したところ、大振幅入力で出力が異常になった。優先して確認すべきことはどれか。

ア．係数と中間積和のスケーリング、ビット幅、丸め、飽和処理。
イ．変数名の長さ。
ウ．FIRでは固定小数点を使用できない。
エ．入力を常に0へする。

答え・解説 正答：ア

ア：固定小数点では中間演算のオーバフローと量子化を明示的に管理する必要がある。
イ：数値異常とは無関係である。
ウ：CMSIS-DSP等でもQ15/Q31 FIRが提供されている。
エ：問題回避であり機能を失う。
総合解説：固定小数点では中間演算のオーバフローと量子化を明示的に管理する必要がある。 この問題では「Fixed-Point Signal Processing」として、固定小数点実装でスケーリングと飽和を考慮できる。

対象：2026年度 / 基準日 2026-09-02

0050 4-2 制御・性能設計 > 信号処理・計測制御 ｜ 難易度：応用

計測系が「センサ応答3ms、ADC待ち1ms、デジタルフィルタ5ms、通信2ms」で構成され、要求は10ms以内である。単純合計の評価として正しいものはどれか。

ア．合計9msなので適合する。
イ．合計11msで要求を1ms超過しており、各段の遅延短縮または構成見直しが必要である。
ウ．フィルタ遅延は計測遅延へ含めない。
エ．通信遅延だけ評価すればよい。

答え・解説 正答：イ

ア：加算が誤っている。
イ：3+1+5+2=11msとなる。実際にはジッタも考慮する必要がある。
ウ：出力確定までの経路に含まれる。
エ：チェーン全体で判断する。
総合解説：3+1+5+2=11msとなる。実際にはジッタも考慮する必要がある。 この問題では「Measurement Chain Budget」として、信号処理チェーン全体の遅延・ノイズ・分解能を評価できる。

対象：2026年度 / 基準日 2026-09-02

0051 4-2 制御・性能設計 > 性能予測・試作・シミュレーション ｜ 難易度：基礎

設計初期にシミュレーションを行う代表的な利点はどれか。

ア．実機試験を永久に不要にできる。
イ．要求仕様がなくても自動で正しい設計ができる。
ウ．実ハードウェアがなくても多くの条件を試し、設計誤りや性能不足を早期に見つけられる。
エ．シミュレーション結果は必ず現実と完全一致する。

答え・解説 正答：ウ

ア：モデル誤差や実装差を確認する実機検証は必要である。
イ：モデルは要求に基づいて作成する必要がある。
ウ：モデル化とシミュレーションは後工程での手戻り低減に役立つ。
エ：モデル化誤差が存在し得る。
総合解説：モデル化とシミュレーションは後工程での手戻り低減に役立つ。 この問題では「Early Simulation」として、シミュレーションがハードウェア未完成段階の早期検証に有効であることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0052 4-2 制御・性能設計 > 性能予測・試作・シミュレーション ｜ 難易度：基礎

生成コードをターゲットプロセッサ上で実行し、数値一致や実行時間を確認する方式はどれか。

ア．SILだけ
イ．MILだけ
ウ．静的レビューだけ
エ．PIL（Processor-in-the-Loop）

答え・解説 正答：エ

ア：SILは開発PC上で生成コードを実行する。
イ：モデル自身のシミュレーションである。
ウ：実行を伴わない。
エ：PILでは生成コードをターゲットプロセッサまたは等価シミュレータ上で実行する。
総合解説：PILでは生成コードをターゲットプロセッサまたは等価シミュレータ上で実行する。 この問題では「SIL/PIL」として、SILとPILの違いを理解できる。

対象：2026年度 / 基準日 2026-09-02

0053 4-2 制御・性能設計 > 性能予測・試作・シミュレーション ｜ 難易度：基礎

アルゴリズムが製品ハードウェアで十分な応答性を得られるか早期に確認したい。適した方策はどれか。

ア．評価ボードやラピッドプロトタイピング環境で代表処理を実装し、実データと負荷で性能を測定する。

イ．量産完了まで一切性能測定しない。

ウ．性能要求を削除する。

エ．机上の平均値だけで十分とする。

答え・解説 正答：ア

ア：試作によりモデルだけでは把握しにくいI/O、CPU、メモリ、遅延を早期に確認できる。

イ：問題発見が遅れる。

ウ：要件変更なしには不適切である。

エ：実装環境の影響を確認できない。

総合解説：試作によりモデルだけでは把握しにくいI/O、CPU、メモリ、遅延を早期に確認できる。 この問題では「Rapid Prototyping」として、プロトタイプが要求・UI・性能仮説の早期確認に使えることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0054 4-2 制御・性能設計 > 性能予測・試作・シミュレーション ｜ 難易度：標準

周期10msで2ms、周期20msで3ms、周期100msで10ms実行する三つのタスクがある。単純なCPU利用率合計はいくらか。

ア．35%（一つのタスクを未計上）

イ．45%（2/10＋3/20＋10/100）

ウ．55%（合計を10ポイント過大換算）

エ．100%（全CPU時間を使用すると仮定）

答え・解説 正答：イ

ア：一つのタスクを加えていない。

イ：2/10=20%、3/20=15%、10/100=10%で合計45%である。

ウ：計算結果と一致しない。

エ：合計実行率は100%ではない。

総合解説：2/10=20%、3/20=15%、10/100=10%で合計45%である。 この問題では「CPU Load Estimation」として、CPU利用率予測をタスク実行時間と周期から行える。

対象：2026年度 / 基準日 2026-09-02

0055 4-2 制御・性能設計 > 性能予測・試作・シミュレーション ｜ 難易度：標準

リアルタイムHILで詳細な物理モデルを使ったところ、1msステップ内に計算が終わらない。適切な対応はどれか。

ア．ステップ時間を無視して処理完了まで待つ。

イ．モデルは詳細なほど常に良いので変更しない。

ウ．検証目的に必要な精度を保ちながらモデルを簡略化し、リアルタイム実行可能性を再評価する。

エ．実ECUを削除する。

答え・解説 正答：ウ

ア：リアルタイム性を失う。

イ：実行不能ならHIL目的を満たさない。

ウ：HILではモデル精度だけでなく固定時間内に計算完了することが必要である。

エ：HILではテスト対象ハードウェアが必要である。

総合解説：HILではモデル精度だけでなく固定時間内に計算完了することが必要である。 この問題では「Model Fidelity」として、モデル精度と計算コストのトレードオフを判断できる。

対象：2026年度 / 基準日 2026-09-02

0056 4-2 制御・性能設計 > 性能予測・試作・シミュレーション ｜ 難易度：標準

シミュレーションでは処理時間5msと予測したが実機では8msだった。適切な対応はどれか。

ア．実測値を無視して5msとして扱い続ける。

イ．シミュレーションが必ず正しいので実機が誤りとする。

ウ．性能モデルを削除して今後予測しない。

エ．キャッシュ、メモリアクセス、OSオーバヘッド等の差を分析し、性能モデルを校正して再予測する。

答え・解説 正答：エ

ア：期限設計を誤る可能性がある。

イ：実装環境差を分析すべきである。

ウ：早期設計判断が難しくなる。

エ：予測と実測の差をモデル改善へ反映すると後続設計の精度が高まる。

総合解説：予測と実測の差をモデル改善へ反映すると後続設計の精度が高まる。 この問題では「Model Calibration」として、性能予測と実測差をモデル更新へフィードバックできる。

対象：2026年度 / 基準日 2026-09-02

0057 4-2 制御・性能設計 > 性能予測・試作・シミュレーション ｜ 難易度：標準

CPU使用率40%、メモリ帯域95%、ネットワーク30%のシステムで処理遅延が増えている。最初に疑うべき資源はどれか。

ア．メモリ帯域の飽和。

イ．CPUは40%なので必ずCPUクロック不足である。

ウ．ネットワーク30%だけが原因である。

エ．利用率は性能と無関係である。

答え・解説 正答：ア

ア：最も利用率が高く待ち時間を生みやすい資源を優先して計測・分析するのが合理的である。

イ：他資源の方が逼迫している。

ウ：示された値では主ボトルネックとは考えにくい。

エ：待ち時間やスループットへ影響する。

総合解説：最も利用率が高く待ち時間を生みやすい資源を優先して計測・分析するのが合理的である。 この問題では「Performance Bottleneck」として、ボトルネック分析で支配的資源を特定できる。

対象：2026年度 / 基準日 2026-09-02

0058 4-2 制御・性能設計 > 性能予測・試作・シミュレーション ｜ 難易度：標準

シミュレーションを単なる動作確認で終わらせず、設計判断へ使うために適切な方法はどれか。

ア．グラフを眺めて感覚だけで合格とする。

イ．要求ごとに入力条件・期待結果・許容範囲を定義し、シミュレーション結果を要求IDへ紐付ける。

ウ．要求仕様を参照しない。

エ．異常条件を一切シミュレーションしない。

答え・解説 正答：イ

ア：定量判定できない。

イ：要求ベースの試験条件にすると設計適合性とトレーサビリティを確認できる。

ウ：何を満たすべきか判断できない。

エ：重要なコーナーケースを見逃す。

総合解説：要求ベースの試験条件にすると設計適合性とトレーサビリティを確認できる。 この問題では「Requirement-Based Simulation」として、モデルベース設計で要求とシミュレーション結果を対応付けられる。

対象：2026年度 / 基準日 2026-09-02

0059 4-2 制御・性能設計 > 性能予測・試作・シミュレーション ｜ 難易度：応用

モデルとSILの出力は一致するが、PILだけ数値がずれる。優先して確認すべき事項はどれか。

ア．モデルが必ず誤りと断定する。

イ．PIL結果を測定しない。

ウ．ターゲットの数値型、コンパイラ最適化、浮動小数点/固定小数点特性、エンディアン等の実装差。

エ．ターゲット環境は数値結果に影響しないと仮定する。

答え・解説 正答：ウ

ア：SILとの一致情報を無視している。

イ：差異の切分けができない。

ウ：モデル・SIL一致なら生成ロジックよりターゲット実行環境固有の差が有力になる。

エ：数値表現や最適化で差が出ることがある。

総合解説：モデル・SIL一致なら生成ロジックよりターゲット実行環境固有の差が有力になる。 この問題では「Back-to-Back Verification」として、SIL/PILの結果差からコード生成・ターゲット依存問題を切り分けられる。

対象：2026年度 / 基準日 2026-09-02

0060 4-2 制御・性能設計 > 性能予測・試作・シミュレーション ｜ 難易度：応用

新規制御アルゴリズムの性能保証を開発初期から量産前まで段階的に行いたい。適切な流れはどれか。

ア．最終量産機だけで初めて試験する。

イ．モデルが合格すれば実機試験は不要とする。

ウ．実機だけ使い要求との対応を記録しない。

エ．モデルシミュレーションで探索し、SIL/PILやプロトタイプで実装差を確認し、最終的に実機/HILで要求を検証する。

答え・解説 正答：エ

ア：問題発見が遅れ手戻りが大きい。

イ：モデル誤差やI/O影響が残る。

ウ：検証根拠が追跡できない。

エ：段階的に実装へ近づけることで早期検出と実環境確認を両立できる。

総合解説：段階的に実装へ近づけることで早期検出と実環境確認を両立できる。 この問題では「Progressive Verification」として、性能要求からモデル・試作・実機の検証段階を組み合わせられる。

対象：2026年度 / 基準日 2026-09-02

0061 4-3 品質・機能安全・信頼性 > 機能安全・ハザード分析 ｜ 難易度：基礎

機能安全の説明として最も適切なものはどれか。

ア．安全関連E/E/PEシステムが要求された安全機能を正しく実行することに関わる安全の一部。
イ．製品外観の美しさだけを評価する考え方。
ウ．全ての故障を物理的に0件にすること。
エ．暗号強度だけで安全を判断すること。

答え・解説 正答：ア

ア：IEC 61508はE/E/PE安全関連システムの機能安全をライフサイクル全体で扱う。
イ：安全機能とは無関係である。
ウ：機能安全は故障を前提にリスク低減を設計する。
エ：セキュリティは関連し得るが機能安全全体ではない。
総合解説：IEC 61508はE/E/PE安全関連システムの機能安全をライフサイクル全体で扱う。 この問題では「Functional Safety」として、機能安全がE/E/PEシステムの安全機能によって達成される安全の一部であることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0062 4-3 品質・機能安全・信頼性 > 機能安全・ハザード分析 ｜ 難易度：基礎

ハザードとリスクの関係として最も適切なものはどれか。

ア．ハザードとリスクは常に完全に同じ意味である。
イ．ハザードは潜在的な危害源であり、リスクは危害の発生可能性と重大さを考慮した尺度である。
ウ．リスクは発生確率だけで決まり重大度は関係しない。
エ．ハザードは発生後の修理費だけを意味する。

答え・解説 正答：イ

ア：区別して扱う。
イ：安全分析では危険源を識別し、そのリスクを評価して必要な低減策を決める。
ウ：重大さも考慮する。
エ：潜在的危害源の概念である。
総合解説：安全分析では危険源を識別し、そのリスクを評価して必要な低減策を決める。 この問題では「Hazard and Risk」として、ハザードとリスクの違いを理解できる。

対象：2026年度 / 基準日 2026-09-02

0063 4-3 品質・機能安全・信頼性 > 機能安全・ハザード分析 ｜ 難易度：基礎

FMEAの基本的な分析方向として最も適切なものはどれか。

ア．最終事故から原因を論理ゲートだけで遡ることだけ。
イ．正常動作だけを確認する。
ウ．構成要素や機能の故障モードを列挙し、その局所・上位への影響や対策を分析する。
エ．部品価格だけを比較する。

答え・解説 正答：ウ

ア：これはFTAの典型的な方向性である。
イ：故障影響分析ではない。
ウ：IEC 60812は故障モードとその影響を体系的に分析するFMEA/FMECAを扱う。
エ：安全分析にならない。
総合解説：IEC 60812は故障モードとその影響を体系的に分析するFMEA/FMECAを扱う。 この問題では「FMEA基本」として、FMEAが故障モードから影響を分析する手法であることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0064 4-3 品質・機能安全・信頼性 > 機能安全・ハザード分析 ｜ 難易度：基礎

機能安全を確保する活動として最も適切な考え方はどれか。

ア．量産直前の試験1回だけで安全を保証する。
イ．安全要求は設計完了後に初めて作る。
ウ．保守時の変更は安全へ影響しないとみなす。
エ．ハザード分析から安全要求、設計、実装、検証、運用・保守までライフサイクルを通じて管理する。

答え・解説 正答：エ

ア：前工程の要求・設計活動が欠けている。
イ：要求は早期に確立する必要がある。
ウ：変更後も安全性評価が必要である。
エ：機能安全は単一の最終試験だけでなく、ライフサイクル全体の活動として扱う。
総合解説：機能安全は単一の最終試験だけでなく、ライフサイクル全体の活動として扱う。 この問題では「Safety Lifecycle」として、安全ライフサイクルで要求・設計・検証・運用まで扱う必要性を理解できる。

対象：2026年度 / 基準日 2026-09-02

0065 4-3 品質・機能安全・信頼性 > 機能安全・ハザード分析 ｜ 難易度：標準

電動ステアリングで「高速走行中に意図しない最大操舵が発生する」を分析する。最も適切な扱いはどれか。

ア．運転状況と故障による危険な振る舞いを組み合わせた危険事象として評価する。
イ．操舵故障だけを単独で見て走行状況を無視する。
ウ．高速走行でなければ同じリスクと必ずみなす。
エ．ハザード分析では運用条件を扱わない。

答え・解説 正答：ア

ア：危険の重大性はシステム故障だけでなく、発生する運用状況との組合せで変わる。
イ：リスク評価が不十分になる。
ウ：状況により危害可能性が異なる。
エ：使用状況は重要である。
総合解説：危険の重大性はシステム故障だけでなく、発生する運用状況との組合せで変わる。 この問題では「Hazardous Event」として、危険事象を運転状況と故障の組合せで分析できる。

対象：2026年度 / 基準日 2026-09-02

0066 4-3 品質・機能安全・信頼性 > 機能安全・ハザード分析 ｜ 難易度：標準

ハザード分析で「意図しない加速」が高リスクと判定された。次の活動として適切なものはどれか。

ア．危険事象を記録せず削除する。
イ．リスクを許容可能水準へ低減するための上位安全目標を定義する。
ウ．通常機能の性能を上げるだけで安全目標は不要とする。
エ．事故が起こるまで対策を決めない。

答え・解説 正答：イ

ア：安全要求へ反映できない。
イ：危険事象から安全目標を導出し、下位の機能・技術安全要求へ展開する。
ウ：リスク低減方針を明確にする必要がある。
エ：予防的安全設計にならない。
総合解説：危険事象から安全目標を導出し、下位の機能・技術安全要求へ展開する。 この問題では「Safety Goal」として、安全目標をハザード分析結果から導出する考え方を理解できる。

対象：2026年度 / 基準日 2026-09-02

0067 4-3 品質・機能安全・信頼性 > 機能安全・ハザード分析 ｜ 難易度：標準

ISO 26262のHARAでASILの判定に用いる代表的な観点の組合せはどれか。

ア．CPU周波数、RAM容量、ROM容量。
イ．開発人数、コード行数、会議回数。
ウ．Severity、Exposure、Controllability。
エ．部品価格、販売価格、利益率。

答え・解説 正答：ウ

ア：機能安全リスク分類の観点ではない。
イ：ASIL判定項目ではない。
ウ：危害の重大度、状況への暴露頻度、回避・制御可能性を組み合わせてリスクを分類する。
エ：安全リスク評価ではない。
総合解説：危害の重大度、状況への暴露頻度、回避・制御可能性を組み合わせてリスクを分類する。 この問題では「ASIL Assessment」として、ASIL評価で重大度・暴露・制御可能性を考慮することを理解できる。

対象：2026年度 / 基準日 2026-09-02

0068 4-3 品質・機能安全・信頼性 > 機能安全・ハザード分析 ｜ 難易度：標準

主制御CPUと安全監視機能が同じ電源、同じクロック、同じRAMへ依存している。最も重要な懸念はどれか。

ア．同じ部品を使うほど必ず独立性が高くなる。
イ．共通電源は安全分析の対象外である。
ウ．安全監視がソフトウェアならハード故障の影響を受けない。
エ．共通原因故障で主制御と安全監視が同時に失われる可能性。

答え・解説 正答：エ

ア：一般には逆である。
イ：代表的な共通故障要因である。
ウ：共有ハード故障で同時に影響を受け得る。
エ：安全機構が主機能と同じ故障要因に依存すると独立性が不足する。
総合解説：安全機構が主機能と同じ故障要因に依存すると独立性が不足する。 この問題では「Safety Independence」として、安全要求の独立性と共通原因故障を考慮できる。

対象：2026年度 / 基準日 2026-09-02

0069 4-3 品質・機能安全・信頼性 > 機能安全・ハザード分析 ｜ 難易度：標準

二つの独立センサで同じ物理量を測定する安全機能で、片方のセンサ固着を検出したい。適切な方策はどれか。

ア．両センサ値の相互比較、変化率、物理範囲を監視し、不一致時に診断する。
イ．二つの値を比較せず片方だけ永久使用する。
ウ．値が異なれば必ず両方正常と判断する。
エ．診断結果を安全処理へ反映しない。

答え・解説 正答：ア

ア：冗長センサは比較診断と組み合わせて故障検出能力を高める。
イ：冗長化の診断効果を活かせない。
ウ：不一致は故障兆候である。
エ：検出してもリスク低減にならない。
総合解説：冗長センサは比較診断と組み合わせて故障検出能力を高める。 この問題では「Diagnostic Mechanism」として、安全要求違反を検出する診断機構を設計できる。

対象：2026年度 / 基準日 2026-09-02

0070 4-3 品質・機能安全・信頼性 > 機能安全・ハザード分析 ｜ 難易度：標準

FMEAで「電源レギュレータ出力停止」という故障モードを記録した。次に記載すべき内容として適切なものはどれか。

ア．部品名だけで分析を終える。
イ．局所影響・上位影響、原因、検出方法、既存対策、追加対策。
ウ．正常時の消費電力だけを書く。
エ．故障モードを削除して記録しない。

答え・解説 正答：イ

ア：影響評価にならない。
イ：FMEAは故障モードを挙げるだけでなく、影響と処置を体系的に評価する。
ウ：故障影響と対策が不足する。
エ：安全分析の目的に反する。
総合解説：FMEAは故障モードを挙げるだけでなく、影響と処置を体系的に評価する。 この問題では「FMEA Worksheet」として、FMEAで検出手段と対策まで記録する必要性を判断できる。

対象：2026年度 / 基準日 2026-09-02

0071 4-3 品質・機能安全・信頼性 > 機能安全・ハザード分析 ｜ 難易度：応用

過温度検出後500ms以内にヒータを遮断しなければ危険温度に達する。安全要求として最も適切な記述はどれか。

ア．過温度時はなるべく早く停止する。
イ．温度が高ければ何か対応する。
ウ．過温度条件成立から500ms以内にヒータ駆動を停止し、安全状態へ移行する。
エ．停止時間は実装後に決める。

答え・解説 正答：ウ

ア：定量的な合否基準がない。
イ：動作が曖昧である。
ウ：安全要求はトリガ条件、動作、時間制約を検証可能な形で定義する必要がある。
エ：ハザード分析から要求へ展開すべきである。
総合解説：安全要求はトリガ条件、動作、時間制約を検証可能な形で定義する必要がある。 この問題では「Safe State Deadline」として、安全状態への遷移時間を安全要求として定量化できる。

対象：2026年度 / 基準日 2026-09-02

0072 4-3 品質・機能安全・信頼性 > 機能安全・ハザード分析 ｜ 難易度：応用

ハザードH1から安全目標SG1、機能安全要求FSR1、技術安全要求TSR1を導出した。適切な管理はどれか。

ア．各成果物を独立に管理し対応関係を残さない。
イ．テスト結果だけ残して上位安全目標を削除する。
ウ．設計変更時は安全分析を見直さない。
エ．H1→SG1→FSR1→TSR1→設計要素→テストケースの対応を追跡し、変更時に影響を確認する。

答え・解説 正答：エ

ア：変更影響や検証漏れを確認しにくい。
イ：安全根拠が失われる。
ウ：安全への影響が変わり得る。
エ：安全ライフサイクルでは安全要求の分解と検証証拠を追跡可能にすることが重要である。
総合解説：安全ライフサイクルでは安全要求の分解と検証証拠を追跡可能にすることが重要である。 この問題では「Safety Traceability」として、安全分析結果を要求・アーキテクチャ・検証へ追跡できる。

対象：2026年度 / 基準日 2026-09-02

0073 4-3 品質・機能安全・信頼性 > 高信頼化・冗長化・フェールセーフ ｜ 難易度：基礎

冗長化の主な目的として最も適切なものはどれか。

ア．一つの要素が故障しても別要素で機能継続または安全状態移行できるようにする。
イ．故障を物理的に完全消滅させる。
ウ．部品数を必ず減らす。
エ．診断を不要にする。

答え・解説 正答：ア

ア：冗長系は単一故障時の可用性や安全性を高めるために用いられる。
イ：冗長化しても故障は発生し得る。
ウ：一般には増える。
エ：冗長要素の故障検出が重要である。
総合解説：冗長系は単一故障時の可用性や安全性を高めるために用いられる。 この問題では「Redundancy」として、冗長化が単一故障への耐性向上に使われることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0074 4-3 品質・機能安全・信頼性 > 高信頼化・冗長化・フェールセーフ ｜ 難易度：基礎

フェールソフトの考え方として最も適切なものはどれか。

ア．故障時は必ず危険側の最大出力へする。
イ．故障時に全機能停止せず、性能や機能を制限した縮退状態でサービスを継続する。
ウ．故障を検出しない。
エ．必ず完全停止することだけを意味する。

答え・解説 正答：イ

ア：安全設計ではない。
イ：フェールソフトは一部能力を失っても可能な範囲で機能を継続する考え方である。
ウ：縮退判断ができない。
エ：それはフェールセーフの一形態でありフェールソフトとは異なる。
総合解説：フェールソフトは一部能力を失っても可能な範囲で機能を継続する考え方である。 この問題では「Fail-safe / Fail-soft」として、フェールセーフとフェールソフトの違いを理解できる。

対象：2026年度 / 基準日 2026-09-02

0075 4-3 品質・機能安全・信頼性 > 高信頼化・冗長化・フェールセーフ ｜ 難易度：基礎

三つの独立センサのうち二つ以上が一致した値を採用する2oo3構成の狙いはどれか。

ア．全センサが故障しても必ず正しい値を出す。
イ．センサ数を減らしてコストを必ず下げる。
ウ．単一センサの異常値に対して多数決で正しい値を維持しやすくする。
エ．比較診断を行わない。

答え・解説 正答：ウ

ア：複数故障には限界がある。
イ：部品数は増える。
ウ：3系統多数決は一つの異常を切り離し、残り二つの一致で機能継続できる。
エ：多数決には値比較が必要である。
総合解説：3系統多数決は一つの異常を切り離し、残り二つの一致で機能継続できる。 この問題では「2oo3 Voting」として、2oo3多数決が単一センサ故障を許容できることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0076 4-3 品質・機能安全・信頼性 > 高信頼化・冗長化・フェールセーフ ｜ 難易度：標準

独立な二部品が直列機能を構成し、各部品の任務時間中信頼度が0.9である。両方正常で機能する系の信頼度は何か。

ア．0.9（単一部品の信頼度）
イ．0.99（並列冗長として計算）
ウ．1.8（2部品を単純加算）
エ．0.81（直列系として0.9×0.9）

答え・解説 正答：エ

ア：一部品だけの信頼度である。
イ：直列化で信頼度が上がるわけではない。
ウ：確率として1を超えている。
エ：独立な直列系では両方正常の確率0.9×0.9=0.81である。
総合解説：独立な直列系では両方正常の確率0.9×0.9=0.81である。 この問題では「Series Reliability」として、直列系の信頼度が各要素信頼度の積になることを計算できる。

対象：2026年度 / 基準日 2026-09-02

0077 4-3 品質・機能安全・信頼性 > 高信頼化・冗長化・フェールセーフ ｜ 難易度：標準

独立な二系統の信頼度が各0.9で、どちらか一方が動けば機能する単純並列系の信頼度は何か。

ア．0.99（並列系で1-同時故障確率）
イ．0.81（両方同時正常の確率）
ウ．0.90（単一系の信頼度）
エ．1.80（2系統を単純加算）

答え・解説 正答：ア

ア：両方故障する確率は0.1×0.1=0.01なので、少なくとも一方正常は1-0.01=0.99である。
イ：両方正常の確率だけを計算している。
ウ：冗長化の効果を反映していない。
エ：確率として不適切である。
総合解説：両方故障する確率は0.1×0.1=0.01なので、少なくとも一方正常は1-0.01=0.99である。 この問題では「Parallel Reliability」として、並列冗長系の信頼度を計算できる。

対象：2026年度 / 基準日 2026-09-02

0078 4-3 品質・機能安全・信頼性 > 高信頼化・冗長化・フェールセーフ ｜ 難易度：標準

二重化したECUが同じ電源ラインと同じ冷却ファンを共有している。最も重要な懸念はどれか。

ア．ECUを二つにすると共通故障は原理上起こらない。
イ．共有電源や冷却故障で両ECUが同時故障する共通原因故障。
ウ．冷却は信頼性と無関係である。
エ．同一設計ほど常に独立性が高い。

答え・解説 正答：イ

ア：共有要因があるため起こり得る。
イ：冗長化の独立性が不足すると期待した信頼性向上を得られない。
ウ：温度上昇で同時故障を招き得る。
エ：共通設計欠陥の影響を受ける可能性がある。
総合解説：冗長化の独立性が不足すると期待した信頼性向上を得られない。 この問題では「Common Cause Failure」として、共通原因故障が冗長化効果を低下させることを判断できる。

対象：2026年度 / 基準日 2026-09-02

0079 4-3 品質・機能安全・信頼性 > 高信頼化・冗長化・フェールセーフ ｜ 難易度：標準

CPU暴走監視用ウォッチドッグをソフトウェアタイマだけで同じCPU上に実装した。問題点はどれか。

ア．同じCPU上なら必ず独立性が最大になる。
イ．ウォッチドッグはCPU停止を検出する目的には使わない。
ウ．CPU自体が停止すると監視処理も停止するため、独立ハードウェア監視より故障検出範囲が狭い。
エ．ソフトタイマは物理CPU故障を必ず修復できる。

答え・解説 正答：ウ

ア：共通故障で同時停止する。
イ：代表的用途の一つである。
ウ：監視対象と監視機構の独立性が重要である。
エ：修復機能ではない。
総合解説：監視対象と監視機構の独立性が重要である。 この問題では「Watchdog Independence」として、ウォッチドッグを独立監視として使う際の制約を理解できる。

対象：2026年度 / 基準日 2026-09-02

0080 4-3 品質・機能安全・信頼性 > 高信頼化・冗長化・フェールセーフ ｜ 難易度：標準

二系統ブレーキ圧センサの一方が故障した場合、制御を継続しつつ安全余裕を増やしたい。適切な設計はどれか。

ア．故障センサ値を正常として使い続ける。
イ．診断せず性能を最大化する。
ウ．故障発生をログに残さない。
エ．故障を診断し、残存センサで制限付き制御へ移行し、警告と追加監視を行う。

答え・解説 正答：エ

ア：誤制御の危険がある。
イ：安全余裕が低下する。
ウ：保守・診断性が低下する。
エ：残存情報の信頼度に応じて機能を制限する縮退運転を設計できる。
総合解説：残存情報の信頼度に応じて機能を制限する縮退運転を設計できる。 この問題では「Degraded Mode」として、縮退運転へ移る条件と残存機能を定義できる。

対象：2026年度 / 基準日 2026-09-02

0081 4-3 品質・機能安全・信頼性 > 高信頼化・冗長化・フェールセーフ ｜ 難易度：応用

案Aは同一センサ2個を同一電源、案Bは異種センサ2個を独立電源で使用する。安全性評価として最も適切なものはどれか。

ア．案Bは共通原因故障を減らせる可能性があるが、異種センサの特性差・診断・コストも含めて評価する。
イ．個数が同じなので両案の安全性は必ず同じ。
ウ．異種センサなら校正や整合確認は不要である。
エ．同一電源共有は共通原因故障にならない。

答え・解説 正答：ア

ア：冗長性は数だけでなく独立性や多様性、診断設計を含めて判断する。
イ：依存関係が異なる。
ウ：特性差の評価が必要である。
エ：代表的な共通故障要因である。
総合解説：冗長性は数だけでなく独立性や多様性、診断設計を含めて判断する。 この問題では「Redundancy Tradeoff」として、冗長化案を独立性・診断率・コストで比較できる。

対象：2026年度 / 基準日 2026-09-02

0082 4-3 品質・機能安全・信頼性 > 高信頼化・冗長化・フェールセーフ ｜ 難易度：応用

三重化計算機で一系統の出力が多数決から外れた。適切な処理として最も包括的なものはどれか。

ア．不一致系を正常として優先する。
イ．不一致を診断し故障系を隔離し、残存二系統で運転継続可能か評価し、保守情報を記録する。
ウ．多数決結果を無視する。
エ．故障記録を残さない。

答え・解説 正答：イ

ア：誤出力を採用する危険がある。
イ：フォールトトレランスは冗長化だけでなく故障検出・隔離・再構成を含む。
ウ：冗長構成の目的を失う。
エ：保守と原因分析が困難になる。
総合解説：フォールトトレランスは冗長化だけでなく故障検出・隔離・再構成を含む。 この問題では「Fault Tolerance Sequence」として、故障検出・切離し・再構成まで含むフォールトトレラント設計を評価できる。

対象：2026年度 / 基準日 2026-09-02

0083 4-3 品質・機能安全・信頼性 > 保守性・環境安全・品質要件 ｜ 難易度：基礎

組込み製品の保守性を高める設計として最も適切なものはどれか。

ア．障害情報を一切記録しない。
イ．全機能を一つの巨大モジュールにする。
ウ．故障コード、ログ、自己診断、交換可能単位、明確なインタフェースを設ける。
エ．部品番号を管理しない。

答え・解説 正答：ウ

ア：原因特定が困難になる。
イ：変更影響が広くなる。
ウ：故障箇所を特定しやすく、修正・交換しやすい構成は保守性向上に寄与する。
エ：交換・構成確認が困難になる。
総合解説：故障箇所を特定しやすく、修正・交換しやすい構成は保守性向上に寄与する。 この問題では「Maintainability」として、保守性を故障診断・修正・交換の容易さとして理解できる。

対象：2026年度 / 基準日 2026-09-02

0084 4-3 品質・機能安全・信頼性 > 保守性・環境安全・品質要件 ｜ 難易度：基礎

車載ECUの環境試験条件を決める考え方として最も適切なものはどれか。

ア．全ECUを室温静置だけで評価する。
イ．ソフトウェア版番号だけで環境耐性を判断する。
ウ．搭載位置は環境条件と無関係である。
エ．搭載位置で想定される温度、振動、湿度、電気的負荷などの環境ストレスに基づいて試験条件を定める。

答え・解説 正答：エ

ア：実使用環境を反映しない。
イ：物理環境試験が必要である。
ウ：温度・振動等は位置で異なる。
エ：ISO 16750シリーズは車載電気電子機器の環境条件と試験を体系的に扱う。
総合解説：ISO 16750シリーズは車載電気電子機器の環境条件と試験を体系的に扱う。 この問題では「Environmental Qualification」として、環境条件を実使用場所に応じて定義・試験する必要性を理解できる。

対象：2026年度 / 基準日 2026-09-02

0085 4-3 品質・機能安全・信頼性 > 保守性・環境安全・品質要件 ｜ 難易度：標準

「信頼性を高くする」という品質要求を改善する記述として最も適切なものはどれか。

ア．任務時間1000時間における故障率上限や可用率、許容停止時間など具体的な指標を定める。
イ．高品質にする、とだけ書く。
ウ．品質要求は数値化できないと決める。
エ．故障実績を記録しない。

答え・解説 正答：ア

ア：品質特性は測定可能な基準へ展開すると設計目標と検証条件になる。
イ：合否判定できない。
ウ：多くは尺度を定義できる。
エ：評価・改善ができない。
総合解説：品質特性は測定可能な基準へ展開すると設計目標と検証条件になる。 この問題では「Quality Requirement」として、品質要件を定量化して設計・評価へ利用できる。

対象：2026年度 / 基準日 2026-09-02

0086 4-3 品質・機能安全・信頼性 > 保守性・環境安全・品質要件 ｜ 難易度：標準

同じ回路を室温25℃と筐体内85℃で使用する。信頼性評価として最も適切なものはどれか。

ア．温度は電子部品信頼性と一切関係しない。
イ．高温ストレスによる故障率や寿命への影響を部品定格・信頼性モデルで再評価する。
ウ．25℃で動けば85℃でも必ず同じ寿命である。
エ．温度評価をせずクロックだけ上げる。

答え・解説 正答：イ

ア：重要なストレス要因である。
イ：電子部品の故障率は環境ストレス条件で変化するため、実使用条件に基づく予測が必要である。
ウ：定格と信頼性が異なる可能性がある。
エ：熱を悪化させ得る。
総合解説：電子部品の故障率は環境ストレス条件で変化するため、実使用条件に基づく予測が必要である。
この問題では「Thermal Reliability」として、環境温度の上昇が部品信頼性へ影響することを考慮できる。

対象：2026年度 / 基準日 2026-09-02

0087 4-3 品質・機能安全・信頼性 > 保守性・環境安全・品質要件 ｜ 難易度：標準

市場でまれに再起動する製品の原因解析を容易にしたい。ログ設計として適切なものはどれか。

ア．再起動時に全ログを必ず消去する。
イ．製品版を記録しない。
ウ．リセット原因、時刻、主要状態、Fault情報、ソフト版、重要イベント履歴を不揮発領域へ残す。
エ．障害発生時の状態を記録しない。

答え・解説 正答：ウ

ア：原因情報を失う。
イ：既知不具合との照合ができない。
ウ：再現困難な障害では発生時コンテキストを保存すると保守診断性が高まる。
エ：再現性が低い障害を解析しにくい。
総合解説：再現困難な障害では発生時コンテキストを保存すると保守診断性が高まる。 この問題では「Service Diagnostics」として、診断ログに再現に必要な時刻・状態・版情報を記録できる。

対象：2026年度 / 基準日 2026-09-02

0088 4-3 品質・機能安全・信頼性 > 保守性・環境安全・品質要件 ｜ 難易度：標準

量産後のファームウェア更新でログ機能だけを変更した。安全機能コードには触れていない。最も適切な対応はどれか。

ア．安全コードを直接変えていないので検証は一切不要とする。
イ．更新版の構成情報を記録しない。
ウ．変更内容をレビューせず即配布する。
エ．共有資源やタイミングへの間接影響を分析し、必要な回帰テストと安全評価を行う。

答え・解説 正答：エ

ア：間接影響を見逃す。
イ：市場版の追跡ができない。
ウ：品質リスクが高い。
エ：直接変更していない機能でもCPU負荷、メモリ、割込み等を通じて影響する可能性がある。
総合解説：直接変更していない機能でもCPU負荷、メモリ、割込み等を通じて影響する可能性がある。 この問題では「Maintenance Change」として、保守更新で安全・品質回帰を行う必要性を判断できる。

対象：2026年度 / 基準日 2026-09-02

0089 4-3 品質・機能安全・信頼性 > 保守性・環境安全・品質要件 ｜ 難易度：応用

ECUは-40℃〜85℃でCAN通信100ms周期を維持する要求がある。適切な検証はどれか。

ア．低温・高温条件へ曝露しながら通信周期、エラー率、起動性を測定して要求適合を判定する。

イ．室温で通信できれば全温度域合格とする。

ウ．温度試験中は通信機能を停止する。

エ．周期を測定せず目視だけで判定する。

答え・解説 正答：ア

ア：環境耐性は単に壊れないことだけでなく、その条件下で要求機能を維持できるか確認する必要がある。

イ：環境条件を再現していない。

ウ：機能維持要求を検証できない。

エ：100ms要求を定量確認できない。

総合解説：環境耐性は単に壊れないことだけでなく、その条件下で要求機能を維持できるか確認する必要がある。 この問題では「Environmental Functional Test」として、環境ストレスと機能要求を組み合わせた試験を設計できる。

対象：2026年度 / 基準日 2026-09-02

0090 4-3 品質・機能安全・信頼性 > 保守性・環境安全・品質要件 ｜ 難易度：応用

診断ログを増やすと保守性は向上するが、Flash使用量と書込み回数が増える。適切な設計判断はどれか。

ア．保守性だけを最大化しFlash寿命を無視する。

イ．必要な診断情報、保存期間、容量、書換え寿命、性能影響を定量比較し、品質要求の優先度に基づいて設計する。

ウ．Flash寿命だけを優先しログを全廃する。

エ．定量評価を行わず担当者の好みで決める。

答え・解説 正答：イ

ア：別品質要求を損なう。

イ：品質特性は相互にトレードオフを持つため、単一特性を最大化するのではなく要求全体を最適化する。

ウ：診断性を失う。

エ：要求ベースの判断にならない。

総合解説：品質特性は相互にトレードオフを持つため、単一特性を最大化するのではなく要求全体を最適化する。 この問題では「Quality Tradeoff」として、品質特性間のトレードオフを要求優先度に基づき判断できる。

対象：2026年度 / 基準日 2026-09-02

0091 4-4 組込みセキュリティ > 脅威分析・暗号・認証 ｜ 難易度：基礎

組込みIoT製品の脅威分析を開始するときの作業として最も適切なものはどれか。

ア．保護すべき資産、外部インタフェース、データフロー、信頼境界、想定攻撃者を整理する。
イ．ソースコードの行数だけを数える。
ウ．市場投入後まで脅威を検討しない。
エ．通信インタフェースを一覧化せず秘密にしておけば安全とみなす。

答え・解説 正答：ア

ア：脅威分析では何を守るか、どこから攻撃可能か、どの境界を越えるかを明確にしてリスク評価へつなげる。
イ：攻撃経路や資産を把握できない。
ウ：設計段階でのリスク低減機会を失う。
エ：実際の攻撃面は存在するため分析が必要である。
総合解説：脅威分析では何を守るか、どこから攻撃可能か、どの境界を越えるかを明確にしてリスク評価へつなげる。 この問題では「脅威モデリング」として、脅威分析で資産・攻撃面・信頼境界を特定する必要性を理解できる。

対象：2026年度 / 基準日 2026-09-02

0092 4-4 組込みセキュリティ > 脅威分析・暗号・認証 ｜ 難易度：基礎

AESについて正しい説明はどれか。

ア．公開鍵と秘密鍵のペアだけを使う公開鍵暗号である。
イ．共通鍵を用いるブロック暗号で、128ビットのブロックを処理する。
ウ．データの完全性だけを確認し暗号化はできない。
エ．鍵長は必ず64ビットだけである。

答え・解説 正答：イ

ア：AESは共通鍵暗号である。
イ：FIPS 197でAESは128ビットブロックを扱い、128、192、256ビット鍵を使用する共通鍵暗号として定義される。
ウ：AESは暗号化・復号に利用される。
エ：AESの鍵長は128、192、256ビットである。
総合解説：FIPS 197でAESは128ビットブロックを扱い、128、192、256ビット鍵を使用する共通鍵暗号として定義される。 この問題では「AES基本」として、AESが共通鍵ブロック暗号であることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0093 4-4 組込みセキュリティ > 脅威分析・暗号・認証 ｜ 難易度：基礎

通信相手の認証を行う主な目的はどれか。

ア．通信データを必ず圧縮する。
イ．CPU使用率を下げる。
ウ．接続している相手が意図した正当な主体であることを確認する。
エ．センサ分解能を上げる。

答え・解説 正答：ウ

ア：圧縮は認証の目的ではない。
イ：認証の直接目的ではない。
ウ：認証はなりすましを抑止し、アクセス制御や安全な通信チャネル確立の前提となる。
エ：計測性能とは無関係である。
総合解説：認証はなりすましを抑止し、アクセス制御や安全な通信チャネル確立の前提となる。 この問題では「認証の目的」として、認証が通信相手や主体の真正性確認に関係することを理解できる。

対象：2026年度 / 基準日 2026-09-02

0094 4-4 組込みセキュリティ > 脅威分析・暗号・認証 ｜ 難易度：標準

インターネット経由でIoT機器からクラウドへ機密データを送信する。通信路上の盗聴や改ざん、サーバなりすましを抑えたい。適切な方策はどれか。

ア．平文TCPだけを使い、IPアドレスが同じなら相手を信用する。
イ．通信データをBase64化するだけ。
ウ．CRCだけ付加すれば相手認証も保証される。
エ．TLS 1.3を使用し、サーバ証明書の検証を正しく実施する。

答え・解説 正答：エ

ア：盗聴・改ざん・なりすましへの保護が不足する。
イ：Base64は暗号化ではない。
ウ：CRCは偶発誤り検出向けで、暗号学的認証を提供しない。
エ：TLS 1.3は通信の機密性・完全性を保護し、認証された安全なチャネルを構成できる。
総合解説：TLS 1.3は通信の機密性・完全性を保護し、認証された安全なチャネルを構成できる。 この問題では「TLS 1.3」として、TLS 1.3が盗聴・改ざん・なりすまし対策となる安全なチャネルを提供することを判断できる。

対象：2026年度 / 基準日 2026-09-02

0095 4-4 組込みセキュリティ > 脅威分析・暗号・認証 ｜ 難易度：標準

10万台のIoT機器をクラウドへ接続する。全機器で同一の固定IDとパスワードを共有する設計の問題点として最も適切なものはどれか。

ア．一台から資格情報が漏れると多数機器のなりすましへ波及するため、機器ごとの一意な識別・認証情報を検討すべきである。

イ．同じ資格情報を共有するほど侵害範囲は小さくなる。

ウ．台数が多い場合は認証が不要になる。

エ．IDが同じならログ追跡が容易になる。

答え・解説 正答：ア

ア：IoTセキュリティでは個々のデバイスを識別し、認証情報の共有範囲を限定することが重要である。

イ：逆に大規模波及しやすい。

ウ：むしろ管理対象が増える。

エ：どの機器の操作か識別しにくくなる。

総合解説：IoTセキュリティでは個々のデバイスを識別し、認証情報の共有範囲を限定することが重要である。 この問題では「デバイス識別」として、デバイスごとに一意な識別情報を用いる重要性を理解できる。

対象：2026年度 / 基準日 2026-09-02

0096 4-4 組込みセキュリティ > 脅威分析・暗号・認証 ｜ 難易度：標準

正しく署名された「ドア解錠」コマンドを攻撃者が記録し、後でそのまま再送する攻撃を防ぎたい。適切な対策はどれか。

ア．署名が正しければ何度でも実行する。

イ．Nonce、単調増加カウンタ、時刻などの鮮度情報を認証対象へ含め、再使用を拒否する。

ウ．暗号鍵をメッセージ本文へ平文で付ける。

エ．受信時刻を一切確認しない。

答え・解説 正答：イ

ア：リプレイ攻撃を許してしまう。

イ：真正な過去メッセージの再送は署名検証だけでは防げないため、メッセージの新鮮性を確認する必要がある。

ウ：鍵漏えいを招く。

エ：再送判定の材料を失う。

総合解説：真正な過去メッセージの再送は署名検証だけでは防げないため、メッセージの新鮮性を確認する必要がある。 この問題では「リプレイ攻撃」として、リプレイ攻撃をNonce・カウンタ・鮮度確認で防ぐ考え方を理解できる。

対象：2026年度 / 基準日 2026-09-02

0097 4-4 組込みセキュリティ > 脅威分析・暗号・認証 ｜ 難易度：標準

量産製品でJTAG/SWDが認証なしで外部端子から利用でき、Flash読出しも可能である。最も適切なセキュリティ判断はどれか。

ア．有線ポートなので脅威分析対象外である。

イ．Flashを読めても機密性へ影響しない。

ウ．機密情報抽出やコード改変の攻撃面となるため、量産時の無効化・認証・アクセス制御を要件に応じて行う。

エ．デバッグポートは常に出荷時開放が安全である。

答え・解説 正答：ウ

ア：物理アクセス攻撃も考慮する必要がある。
イ：鍵やファームウェアが漏れる可能性がある。
ウ：物理デバッグインタフェースもIoTデバイスの攻撃面であり、不要な機能は制限すべきである。
エ：攻撃面を拡大する。
総合解説：物理デバッグインタフェースもIoTデバイスの攻撃面であり、不要な機能は制限すべきである。この問題では「デバッグI/F脅威」として、デバッグポートが攻撃面になり得ることを分析できる。

対象：2026年度 / 基準日 2026-09-02

0098 4-4 組込みセキュリティ > 脅威分析・暗号・認証 ｜ 難易度：標準

温度センサ機器のクラウド資格情報で、他機器の設定変更や管理者APIまで実行できる。改善として適切なものはどれか。

ア．全機器へ管理者権限を付与する。

イ．認可を廃止し認証だけにする。

ウ．APIの権限を文書化しない。

エ．当該機器が必要とする送信・受信操作だけを許可する最小権限の認可ポリシーへ変更する。

答え・解説 正答：エ

ア：侵害時の影響が大きくなる。
イ：認証後に実行可能操作を制限できない。
ウ：設定誤りを発見しにくい。
エ：資格情報が侵害されても可能な操作を限定することで被害範囲を小さくできる。
総合解説：資格情報が侵害されても可能な操作を限定することで被害範囲を小さくできる。 この問題では「最小権限」として、最小権限に基づく認可で侵害影響を限定できる。

対象：2026年度 / 基準日 2026-09-02

0099 4-4 組込みセキュリティ > 脅威分析・暗号・認証 ｜ 難易度：応用

低消費電力MCUで大量センサデータを暗号化し、セッション確立時には相互認証も必要である。適切な設計方針はどれか。

ア．認証・鍵共有には公開鍵方式等を利用し、確立したセッション鍵による共通鍵暗号で大量データを保護する構成を検討する。

イ．全データを公開鍵演算だけで1バイトずつ暗号化することを必須とする。

ウ．認証を省略して固定共通鍵だけ全製品で共有する。

エ．暗号処理負荷を測定しない。

答え・解説 正答：ア

ア：一般に公開鍵処理は認証や鍵確立に適し、共通鍵暗号は大量データを効率よく処理しやすい。

イ：資源制約下では効率が悪い。

ウ：鍵漏えい時の影響が大きい。

エ：期限・電力要件との両立を判断できない。

総合解説：一般に公開鍵処理は認証や鍵確立に適し、共通鍵暗号は大量データを効率よく処理しやすい。 この問題では「暗号方式選定」として、組込み機器の資源制約を考慮しながら暗号方式を選定できる。

対象：2026年度 / 基準日 2026-09-02

0100 4-4 組込みセキュリティ > 脅威分析・暗号・認証 ｜ 難易度：応用

脅威分析で「攻撃者が偽サーバへ機器を接続させ、設定値を書き換える」が高リスクと判定された。適切なセキュリティ要求の組合せはどれか。

ア．通信先を検証せずDNS応答を常に信頼する。

イ．サーバ真正性検証、通信完全性保護、設定変更の認可、失敗時の安全な拒否と監査ログを要求する。

ウ．設定APIを誰でも呼べるようにする。

エ．異常接続をログに残さない。

答え・解説 正答：イ

ア：偽サーバ接続を防げない。

イ：脅威を防止・検出・影響低減する複数の要求へ具体化することでリスク低減を設計できる。

ウ：不正変更を許す。

エ：検出・追跡能力が低下する。

総合解説：脅威を防止・検出・影響低減する複数の要求へ具体化することでリスク低減を設計できる。 この問題では「脅威から要求への展開」として、脅威分析結果から具体的なセキュリティ要求へ展開できる。

対象：2026年度 / 基準日 2026-09-02

0101 4-4 組込みセキュリティ > セキュアブート・鍵管理・保護機構 ｜ 難易度：基礎

セキュアブートの基本的な動作として最も適切なものはどれか。

ア．起動時に全ての署名検証を無効化する。
イ．ファームウェアのファイル名だけ確認する。
ウ．次段のファームウェアの署名や完全性を検証し、信頼できると確認できた場合だけ実行する。
エ．CRC一致だけで攻撃者による改ざんも防げるとする。

答え・解説 正答：ウ

ア：未承認コードを実行し得る。
イ：真正性・完全性を保証できない。
ウ：信頼の起点から後続コードを検証して起動することで未承認ファームウェアの実行を防ぐ。
エ：CRCは暗号学的真正性を提供しない。
総合解説：信頼の起点から後続コードを検証して起動することで未承認ファームウェアの実行を防ぐ。 この問題では「Secure Boot」として、セキュアブートが起動コードの真正性・完全性を検証してから実行することを理解できる。

対象：2026年度 / 基準日 2026-09-02

0102 4-4 組込みセキュリティ > セキュアブート・鍵管理・保護機構 ｜ 難易度：基礎

セキュアブートの最上位検証鍵を、攻撃者が通常ファームウェアから自由に書き換えられない領域へ保存する主な理由はどれか。

ア．鍵を書き換えやすいほど信頼性が高まるため。
イ．検証鍵は起動後にしか使わないため保護不要だから。
ウ．鍵を公開すると秘密鍵も自動的に安全になるため。
エ．検証鍵が改ざんされると攻撃者自身のファームウェアを正当と認識させられるため。

答え・解説 正答：エ

ア：信頼の起点を攻撃者が変更できてしまう。
イ：起動時の真正性確認に使用する。
ウ：公開鍵の保護目的を誤っている。
エ：信頼の起点は後続の検証全体の前提となるため、強く保護する必要がある。
総合解説：信頼の起点は後続の検証全体の前提となるため、強く保護する必要がある。 この問題では「Root of Trust」として、Root of Trustの検証鍵を保護された領域に置く必要性を理解できる。

対象：2026年度 / 基準日 2026-09-02

0103 4-4 組込みセキュリティ > セキュアブート・鍵管理・保護機構 ｜ 難易度：基礎

暗号鍵管理に含めるべき活動として最も適切なものはどれか。

ア．鍵生成、登録・配布、保存、利用、更新・ローテーション、失効、バックアップ、破棄。

イ．鍵を最初に一度作成した後は永続的に同じ鍵を使うことだけ。

ウ．鍵をソースコードコメントへ記載する。

エ．破棄した鍵を誰でも復元できるようにする。

答え・解説 正答：ア

ア：NIST SP 800-57は鍵材料をライフサイクル全体で管理し、用途に応じた保護を行うことを扱う。

イ：漏えい・有効期限・更新を考慮していない。

ウ：秘密鍵漏えいの危険がある。

エ：安全な破棄の目的に反する。

総合解説：NIST SP 800-57は鍵材料をライフサイクル全体で管理し、用途に応じた保護を行うことを扱う。この問題では「Key Lifecycle」として、鍵管理が生成から破棄までのライフサイクルを含むことを理解できる。

対象：2026年度 / 基準日 2026-09-02

0104 4-4 組込みセキュリティ > セキュアブート・鍵管理・保護機構 ｜ 難易度：標準

同じ共通鍵を通信暗号化、ファームウェア署名相当の認証、データ保存暗号化へ全て使う設計の問題点はどれか。

ア．同一鍵の使い回しは常に最も安全である。

イ．一用途で鍵が漏えいすると複数機能へ被害が波及するため、用途ごとに鍵を分離するのが望ましい。

ウ．鍵の用途数が多いほど鍵強度が自動的に増える。

エ．鍵分離は暗号設計では不要である。

答え・解説 正答：イ

ア：被害範囲を拡大する。

イ：鍵用途を分離すると侵害の影響範囲を限定し、アルゴリズムや更新ポリシーも個別管理できる。

ウ：強度は増えない。

エ：重要な鍵管理原則である。

総合解説：鍵用途を分離すると侵害の影響範囲を限定し、アルゴリズムや更新ポリシーも個別管理できる。この問題では「Key Separation」として、同一鍵の多目的利用を避ける鍵分離の意義を理解できる。

対象：2026年度 / 基準日 2026-09-02

0105 4-4 組込みセキュリティ > セキュアブート・鍵管理・保護機構 ｜ 難易度：標準

100万台すべてに同じ秘密鍵を焼き込む代わりに、機器ごとに異なる秘密を持たせる主な利点はどれか。

ア．製造時の鍵管理が不要になる。
イ．認証処理が不要になる。
ウ．一台の鍵漏えいで全製品が同時に侵害されるリスクを低減できる。
エ．鍵を平文で外部へ表示してよくなる。

答え・解説 正答：ウ

ア：むしろ安全なプロビジョニングが必要である。
イ：固有鍵も認証用途で管理する必要がある。
ウ：鍵共有範囲を小さくすることで侵害の爆発半径を限定できる。
エ：秘密保護は必要である。
総合解説：鍵共有範囲を小さくすることで侵害の爆発半径を限定できる。 この問題では「Device Unique Key」として、デバイス固有鍵を利用して一台の侵害が全台へ波及することを抑えられる。

対象：2026年度 / 基準日 2026-09-02

0106 4-4 組込みセキュリティ > セキュアブート・鍵管理・保護機構 ｜ 難易度：標準

セキュアブートが起動ファームウェアの署名不正を検出した。プラットフォームレジリエンスの観点で適切な動作はどれか。

ア．署名不正でも通常起動を続ける。
イ．回復用イメージも同じ書換え可能領域に無保護で置く。
ウ．異常を記録せず毎回同じ不正イメージを実行する。
エ．不正イメージを実行せず、保護された既知良好イメージや回復モードから安全に復旧する。

答え・解説 正答：エ

ア：未承認コードを実行する危険がある。
イ：攻撃者に同時改ざんされる可能性がある。
ウ：検出機能を無意味にする。
エ：SP 800-193は保護・検出だけでなく、攻撃後の安全な回復を重視している。
総合解説：SP 800-193は保護・検出だけでなく、攻撃後の安全な回復を重視している。 この問題では「Firmware Recovery」として、不正ファームウェア検出後に安全な回復経路を備える必要性を判断できる。

対象：2026年度 / 基準日 2026-09-02

0107 4-4 組込みセキュリティ > セキュアブート・鍵管理・保護機構 ｜ 難易度：標準

セキュアブートと暗号化を実装したが、量産機のデバッグポートからRAM上の秘密鍵を読める。適切な改善はどれか。

ア．デバッグ認証・ロック、メモリ保護、秘密鍵を保護領域へ置くなど物理・論理アクセスを制限する。

イ．セキュアブートがあるのでデバッグポートは無制限でよい。

ウ．秘密鍵をログへ出力する。

エ．鍵保護をせず鍵長だけ長くする。

答え・解説 正答：ア

ア：ブートだけ安全でも実行中の秘密へ別経路からアクセスできればセキュリティは成立しない。

イ：別の攻撃面が残る。

ウ：漏えいを助長する。

エ：鍵自体を取得されれば強度の意味が薄れる。

総合解説：ブートだけ安全でも実行中の秘密へ別経路からアクセスできればセキュリティは成立しない。 この問題では「Debug Protection」として、デバッグ機能を量産時に制限して鍵やメモリを保護できる。

対象：2026年度 / 基準日 2026-09-02

0108 4-4 組込みセキュリティ > セキュアブート・鍵管理・保護機構 ｜ 難易度：標準

攻撃者が正規署名付きだが既知脆弱性を含む古いファームウェアをインストールしようとする。対策として適切なものはどれか。

ア．署名が正しければどんな旧版でも受け入れる。

イ．セキュアに保持したバージョン情報や単調カウンタを用い、許可されない旧版へのロールバックを拒否する。

ウ．バージョン番号をユーザー入力だけで決める。

エ．更新履歴を保存しない。

答え・解説 正答：イ

ア：ロールバック攻撃を許す。

イ：署名が正しいだけでは古い脆弱版を排除できないため、バージョン鮮度の検証も必要である。

ウ：攻撃者が改変できる可能性がある。

エ：旧版判定が困難になる。

総合解説：署名が正しいだけでは古い脆弱版を排除できないため、バージョン鮮度の検証も必要である。 この問題では「Boot Rollback Protection」として、ロールバック保護で脆弱な旧版ファームウェアへの戻しを防止できる。

対象：2026年度 / 基準日 2026-09-02

0109 4-4 組込みセキュリティ > セキュアブート・鍵管理・保護機構 ｜ 難易度：応用

ファームウェア署名用秘密鍵が漏えいした可能性が判明した。今後も製品を安全に更新したい。最も適切な事前設計はどれか。

ア．署名鍵は漏えいしない前提で更新経路を設けない。

イ．漏えいした鍵を永久に使い続ける。

ウ．複数の信頼鍵、鍵バージョン、失効・更新手順を用意し、侵害鍵から新鍵へ安全に移行できるようにする。

エ．署名検証を無効化して対応する。

答え・解説 正答：ウ

ア：侵害時に回復できない。

イ：攻撃者が正規署名を生成できる。

ウ：長期運用製品では鍵漏えいを想定し、信頼の起点を安全に更新・失効できる設計が重要である。

エ：任意コードを受け入れることになる。

総合解説：長期運用製品では鍵漏えいを想定し、信頼の起点を安全に更新・失効できる設計が重要である。この問題では「Signing Key Compromise」として、署名鍵漏えい時に鍵失効・更新の仕組みが必要なことを判断できる。

対象：2026年度 / 基準日 2026-09-02

0110 4-4 組込みセキュリティ > セキュアブート・鍵管理・保護機構 ｜ 難易度：応用

ROMブートローダは改ざん困難だが、次段ブートローダは署名検証し、その次のOSはハッシュ比較だけで起動している。攻撃者が書換え可能Flashを制御できる場合の問題点はどれか。

ア．ROMが安全なら後続段は一切検証不要である。

イ．通常ハッシュは秘密鍵署名と常に同じ真正性を提供する。

ウ．書換え可能Flashはセキュリティ分析対象外である。

エ．OS段で暗号学的な真正性を信頼の連鎖へ結び付けていないため、攻撃者がハッシュ値も含めて改ざんできる構成なら信頼が途切れる。

答え・解説 正答：エ

ア：後続コードも攻撃対象になる。

イ：参照ハッシュ自体の保護が必要である。

ウ：主要な攻撃対象である。

エ：各段が保護された信頼情報を基に次段を検証しなければChain of Trustは成立しない。

総合解説：各段が保護された信頼情報を基に次段を検証しなければChain of Trustは成立しない。 この問題では「Chain of Trust」として、信頼の連鎖全体を保護・検出・回復の観点から評価できる。

対象：2026年度 / 基準日 2026-09-02

0111 4-4 組込みセキュリティ > セキュア更新・OTA・脆弱性対応 ｜ 難易度：基礎

OTAで受信したファームウェアをインストールする前に最も重要な確認の一つはどれか。

ア．信頼された署名鍵で署名が正しく検証でき、対象製品・版として許可されたイメージであること。
イ．ファイル名がupdate.binなら必ず正規品とみなす。
ウ．サイズが大きければ正規品とみなす。
エ．HTTPSで取得したら署名検証は常に不要とする。

答え・解説 正答：ア

ア：通信路だけでなく更新成果物自身の真正性・完全性を検証することで改ざんイメージの導入を防ぐ。
イ：名前は攻撃者も変更できる。
ウ：真正性を保証しない。
エ：配布サーバ侵害等への防御として成果物署名が有効である。
総合解説：通信路だけでなく更新成果物自身の真正性・完全性を検証することで改ざんイメージの導入を防ぐ。 この問題では「OTA署名検証」として、OTA更新でイメージの真正性・完全性検証が必要なことを理解できる。

対象：2026年度 / 基準日 2026-09-02

0112 4-4 組込みセキュリティ > セキュア更新・OTA・脆弱性対応 ｜ 難易度：基礎

ソフトウェア更新システムに対するロールバック攻撃とはどれか。

ア．最新版を正しく配布すること。
イ．クライアントに以前の古い正規版を最新であるかのように提示し、脆弱版へ戻させる攻撃。
ウ．電源を入れ直すこと。
エ．ログを圧縮すること。

答え・解説 正答：イ

ア：攻撃ではない。
イ：TUFでは正規署名済みであっても古い版へ戻す攻撃を明示的に脅威として扱う。
ウ：更新版の鮮度操作とは異なる。
エ：更新攻撃とは無関係である。
総合解説：TUFでは正規署名済みであっても古い版へ戻す攻撃を明示的に脅威として扱う。 この問題では「Rollback Attack」として、ロールバック攻撃が古い脆弱版を再導入する攻撃であることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0113 4-4 組込みセキュリティ > セキュア更新・OTA・脆弱性対応 ｜ 難易度：基礎

製品脆弱性報告を受け付けた後の対応として最も適切なものはどれか。

ア．報告を読まず全て削除する。

イ．報告者へ修正前に秘密鍵を渡す。

ウ．報告を記録・検証し、影響と優先度を評価し、修正・緩和策を準備して必要な情報公開と追跡を行う。

エ．影響評価を行わず必ず全製品を停止する。

答え・解説 正答：ウ

ア：脆弱性を放置する。

イ：セキュリティを悪化させる。

ウ：ISO/IEC 30111は製品・サービスの潜在的脆弱性報告を処理し修復するプロセスを扱う。

エ：リスクに応じた対応ができない。

総合解説：ISO/IEC 30111は製品・サービスの潜在的脆弱性報告を処理し修復するプロセスを扱う。 この問題では「Vulnerability Handling」として、脆弱性対応が受付・評価・修正・公開を含むプロセスであることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0114 4-4 組込みセキュリティ > セキュア更新・OTA・脆弱性対応 ｜ 難易度：標準

OTA更新中に電源が切れると起動不能になる製品を改善したい。適切な方式はどれか。

ア．現用Flashを先に全消去してからダウンロードする。

イ．更新完了前に署名検証結果を成功扱いする。

ウ．回復手段を設けない。

エ．現用イメージを保持したまま別スロットへ新イメージを書き、検証後に起動先を原子的に切り替える。

答え・解説 正答：エ

ア：中断時に起動可能イメージがなくなる。

イ：不完全なイメージを起動し得る。

ウ：フィールドで復旧困難になる。

エ：A/B構成などで既知良好版を残すと、更新途中の電源断から回復しやすい。

総合解説：A/B構成などで既知良好版を残すと、更新途中の電源断から回復しやすい。 この問題では「Power-loss-safe Update」として、更新中電源断に耐えるA/B構成や原子的切替を設計できる。

対象：2026年度 / 基準日 2026-09-02

0115 4-4 組込みセキュリティ > セキュア更新・OTA・脆弱性対応 ｜ 難易度：標準

攻撃者がネットワークを制御し、クライアントへ有効だった古い更新情報を永遠に返し続けて最新版を知らせない。対策として適切なものはどれか。

ア．更新メタデータに有効期限や版情報を持たせ、期限切れ・古い情報を拒否する。
イ．一度取得した更新情報を永久に信頼する。
ウ．端末時刻やメタデータ鮮度を一切確認しない。
エ．更新チェック機能を削除する。

答え・解説 正答：ア

ア：TUFではIndefinite Freezeを脅威とし、期限付きメタデータ等で古い状態へ固定されることを防ぐ。
イ：Freeze攻撃を許す。
ウ：期限判定ができない。
エ：最新版を取得できなくなる。
総合解説：TUFではIndefinite Freezeを脅威とし、期限付きメタデータ等で古い状態へ固定されることを防ぐ。 この問題では「Freeze Attack」として、更新メタデータの期限や版管理でFreeze攻撃を抑止できる。

対象：2026年度 / 基準日 2026-09-02

0116 4-4 組込みセキュリティ > セキュア更新・OTA・脆弱性対応 ｜ 難易度：標準

同じ製品名でもHW Rev.AとRev.Bで周辺回路が異なる。誤ったOTAイメージ配布を防ぐにはどうすべきか。

ア．製品名が似ていれば全イメージを共通適用する。
イ．更新メタデータに対象モデル・HWリビジョン・互換条件を持たせ、端末側でも適合を検証する。
ウ．端末側では何も検証しない。
エ．HWリビジョン情報を削除する。

答え・解説 正答：イ

ア：非互換ハードウェアへ誤適用する危険がある。
イ：真正なファームウェアでも対象ハードウェアが違えば故障するため、対象適合性を確認する必要がある。
ウ：配布系誤設定時の防御がない。
エ：適合判定できない。
総合解説：真正なファームウェアでも対象ハードウェアが違えば故障するため、対象適合性を確認する必要がある。 この問題では「Target Compatibility」として、更新対象のハードウェア互換性を検証できる。

対象：2026年度 / 基準日 2026-09-02

0117 4-4 組込みセキュリティ > セキュア更新・OTA・脆弱性対応 ｜ 難易度：標準

100万台へ新ファームウェアを一斉配布する前に、未知の不具合による大規模障害を抑えたい。適切な運用はどれか。

ア．初回から全端末へ強制更新し監視しない。
イ．更新後のヘルス情報を収集しない。
ウ．少数群へ段階配信し、起動成功率・エラー率等を監視して問題なければ対象を拡大する。
エ．配信停止機能を設けない。

答え・解説 正答：ウ

ア：不具合時の影響が最大化する。
イ：異常検出が遅れる。
ウ：Canary/Staged rolloutにより異常時の影響範囲を限定して配布停止できる。
エ：問題発生時の制御が困難になる。
総合解説：Canary/Staged rolloutにより異常時の影響範囲を限定して配布停止できる。 この問題では「Staged Rollout」として、段階配信とヘルスチェックで更新障害の爆発半径を抑えられる。

対象：2026年度 / 基準日 2026-09-02

0118 4-4 組込みセキュリティ > セキュア更新・OTA・脆弱性対応 ｜ 難易度：標準

二つの脆弱性がある。Aは高CVSSだが外部から到達不能、Bは中程度だがインターネット公開APIで実際の悪用報告がある。対応優先度として適切な考え方はどれか。

ア．数値スコアだけで機械的に決め、露出条件を無視する。
イ．悪用報告があっても中程度なら放置する。
ウ．全脆弱性を同じ期限で扱うことだけが正しい。
エ．スコアだけでなく実際の露出、悪用可能性、製品機能・安全への影響を含めリスクベースで優先する。

答え・解説 正答：エ

ア：実製品リスクを誤る可能性がある。
イ：実際の脅威を無視している。
ウ：リスク差を反映できない。
エ：脆弱性対応では製品固有のリスクを評価して修正・緩和の優先順位を決める必要がある。
総合解説：脆弱性対応では製品固有のリスクを評価して修正・緩和の優先順位を決める必要がある。 この問題では「Vulnerability Prioritization」として、脆弱性の深刻度だけでなく悪用可能性・露出・安全影響を考慮できる。

対象：2026年度 / 基準日 2026-09-02

0119 4-4 組込みセキュリティ > セキュア更新・OTA・脆弱性対応 ｜ 難易度：応用

更新配布サーバが侵害されても、攻撃者が単独で任意ファームウェアを正規更新として公開できないようにしたい。適切な設計はどれか。

ア．配布サーバと署名権限を分離し、重要メタデータに複数鍵・しきい値署名等を用いて単一鍵侵害を耐える。

イ．配布サーバに全Root秘密鍵を平文保存する。

ウ．署名を廃止しHTTPSだけに依存する。

エ．全役割で同じ一つの秘密鍵を共有する。

答え・解説 正答：ア

ア：TUFは役割分離と複数鍵を用いて更新基盤の一部侵害が全信頼を失わせないよう設計する。

イ：サーバ侵害で全信頼が失われる。

ウ：リポジトリ侵害への防御が弱くなる。

エ：単一鍵侵害の影響を広げる。

総合解説：TUFは役割分離と複数鍵を用いて更新基盤の一部侵害が全信頼を失わせないよう設計する。 この問題では「Update Role Separation」として、更新署名鍵の役割分離・しきい値署名で単一鍵侵害への耐性を高められる。

対象：2026年度 / 基準日 2026-09-02

0120 4-4 組込みセキュリティ > セキュア更新・OTA・脆弱性対応 ｜ 難易度：応用

10年間利用される産業IoT製品を設計する。セキュリティ更新体制として最も適切なものはどれか。

ア．出荷時点で開発チームを解散し更新手段も廃止する。

イ．脆弱性受付、資産・依存部品管理、修正配布、顧客通知、サポート終了方針を製品ライフサイクル全体で計画する。

ウ．依存ライブラリの版を記録しない。

エ．サポート終了時期を利用者へ知らせない。

答え・解説 正答：イ

ア：長期利用中の新規脆弱性へ対応できない。

イ：IoT製品では出荷後の脆弱性対応とサポート・EOL情報提供を含む継続的な活動が必要である。

ウ：影響調査が困難になる。

エ：顧客がリスク管理できない。

総合解説：IoT製品では出荷後の脆弱性対応とサポート・EOL情報提供を含む継続的な活動が必要である。 この問題では「Product Security Lifecycle」として、長期運用IoT製品の脆弱性対応をサポート期間・EOLまで含めて設計できる。

対象：2026年度 / 基準日 2026-09-02

0121 4-5 IoT・プラットフォーム > エッジ・クラウド連携 ｜ 難易度：基礎

センサ近傍のエッジ機器でデータ処理を行う代表的な利点はどれか。

ア．必ずクラウドを完全不要にできる。
イ．ネットワーク障害があると必ず全機能が停止する。
ウ．クラウド往復を待たずに低遅延で判断でき、送信データ量も削減できる。
エ．エッジではデータを一切保存できない。

答え・解説 正答：ウ

ア：集中分析や管理にはクラウドが有利な場合がある。
イ：ローカル処理を残せば継続できる。
ウ：エッジ処理はデータ生成源の近くで処理することで遅延・帯域・クラウド依存を抑えられる。
エ：ローカルバッファやストレージを利用できる。
総合解説：エッジ処理はデータ生成源の近くで処理することで遅延・帯域・クラウド依存を抑えられる。 この問題では「Edge Computing」として、エッジ処理が通信遅延とクラウド依存を減らせることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0122 4-5 IoT・プラットフォーム > エッジ・クラウド連携 ｜ 難易度：基礎

多数のIoT機器から長期間データを集約し、全体傾向を分析する処理を配置する場所として一般に適したものはどれか。

ア．各センサの割込みハンドラだけ
イ．デバイスのブートROMだけ
ウ．通信トランシーバだけ
エ．クラウド側の集約・分析基盤

答え・解説 正答：エ

ア：長期・大規模分析には適さない。
イ：用途が異なる。
ウ：分析処理を担う場所ではない。
エ：クラウドは大規模ストレージや計算資源を集中管理し、複数機器の横断分析を行いやすい。
総合解説：クラウドは大規模ストレージや計算資源を集中管理し、複数機器の横断分析を行いやすい。 この問題では「Cloud Aggregation」として、クラウドが多数デバイスの集約・分析・管理に適することを理解できる。

対象：2026年度 / 基準日 2026-09-02

0123 4-5 IoT・プラットフォーム > エッジ・クラウド連携 ｜ 難易度：基礎

BLEセンサ群をインターネット上のクラウドへ接続するIoTゲートウェイの役割として適切なものはどれか。

ア．BLE側通信を終端し、データ集約やプロトコル変換を行ってIPネットワークへ中継する。

イ．必ず全センサのファームウェアを削除する。

ウ．クラウドの認証機能を無効化する。

エ．センサ値を常に同じ値へ固定する。

答え・解説 正答：ア

ア：ゲートウェイは異なるネットワーク・プロトコル間の橋渡しやエッジ処理の実行点として利用できる。

イ：中継機能とは無関係である。

ウ：セキュリティを悪化させる。

エ：データ処理の目的に反する。

総合解説：ゲートウェイは異なるネットワーク・プロトコル間の橋渡しやエッジ処理の実行点として利用できる。 この問題では「IoT Gateway」として、ゲートウェイがプロトコル変換や集約の役割を担えることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0124 4-5 IoT・プラットフォーム > エッジ・クラウド連携 ｜ 難易度：標準

産業ロボットの緊急停止判断をクラウドAIだけで行う設計を検討している。安全性の観点から最も適切な方針はどれか。

ア．クラウド応答が来るまで必ず動作を継続する。

イ．緊急停止のような厳しい時間制約・安全機能はローカルでも成立させ、クラウドは補助判断や分析に用いる。

ウ．ローカル側ではセンサ値を使用しない。

エ．ネットワーク障害は起こらない前提にする。

答え・解説 正答：イ

ア：通信断時に危険となる可能性がある。

イ：ネットワーク遅延・断絶があっても安全機能が成立するようにアーキテクチャを分ける必要がある。

ウ：安全判断能力を失う。

エ：現実的な故障モードを無視している。

総合解説：ネットワーク遅延・断絶があっても安全機能が成立するようにアーキテクチャを分ける必要がある。 この問題では「Local Safety Loop」として、安全クリティカルな閉ループ制御をネットワーク断から独立させられる。

対象：2026年度 / 基準日 2026-09-02

0125 4-5 IoT・プラットフォーム > エッジ・クラウド連携 ｜ 難易度：標準

振動センサが毎秒1MBの生データを出力するが、クラウドでは異常特徴量だけ必要である。適切な設計はどれか。

ア．全生データを無条件に常時送信し帯域を評価しない。
イ．異常データも含め全て破棄する。
ウ．エッジでフィルタ・特徴抽出し、必要な特徴量や異常時データだけをクラウドへ送る。
エ．エッジ処理を使うと必ず計測精度が0になる。

答え・解説 正答：ウ

ア：ネットワーク負荷が大きい。
イ：監視目的を満たさない。
ウ：必要情報へ変換してから送信することで帯域とクラウド保存量を削減できる。
エ：処理設計次第で必要情報を維持できる。
総合解説：必要情報へ変換してから送信することで帯域とクラウド保存量を削減できる。 この問題では「Edge Filtering」として、エッジ側のフィルタリングで帯域とクラウド保存量を削減できる。

対象：2026年度 / 基準日 2026-09-02

0126 4-5 IoT・プラットフォーム > エッジ・クラウド連携 ｜ 難易度：標準

移動体IoT端末で数十分間クラウド接続が失われても計測データを失いたくない。適切な方策はどれか。

ア．送信失敗したデータは即座に全て破棄する。
イ．通信断は起こらないと仮定する。
ウ．RAMだけに保存し電源断も考慮しない。
エ．不揮発バッファへ時刻・連番付きで保存し、再接続後に順序や重複を考慮して再送する。

答え・解説 正答：エ

ア：非損失要求を満たさない。
イ：移動体通信では現実的でない。
ウ：電源断でデータを失う可能性がある。
エ：Store-and-forwardにより一時的な通信断を吸収し、データ欠損を抑えられる。
総合解説：Store-and-forwardにより一時的な通信断を吸収し、データ欠損を抑えられる。 この問題では「Store and Forward」として、通信断に備えてローカルバッファと再送を設計できる。

対象：2026年度 / 基準日 2026-09-02

0127 4-5 IoT・プラットフォーム > エッジ・クラウド連携 ｜ 難易度：標準

クラウドからエッジ機器へ制御パラメータを遠隔変更できる。安全な設計として適切なものはどれか。

ア．送信元を認証し操作権限を確認し、値範囲・版・整合性を検証してから適用する。
イ．受信した値を送信元確認なしに即適用する。
ウ．設定値の範囲を確認しない。
エ．変更履歴を記録しない。

答え・解説 正答：ア

ア：遠隔設定は不正操作や誤設定の影響が大きいため、認証・認可と入力検証を組み合わせる必要がある。
イ：攻撃や誤操作を受けやすい。
ウ：危険な値を適用する可能性がある。
エ：監査・原因追跡が困難になる。
総合解説：遠隔設定は不正操作や誤設定の影響が大きいため、認証・認可と入力検証を組み合わせる必要がある。 この問題では「Cloud-to-Edge Control」として、クラウドからの設定変更を安全に適用するため認証・認可・検証が必要と判断できる。

対象：2026年度 / 基準日 2026-09-02

0128 4-5 IoT・プラットフォーム > エッジ・クラウド連携 ｜ 難易度：標準

カメラIoTでクラウドには人数だけ必要だが、生映像には個人情報が含まれる。適切な設計案はどれか。

ア．全生映像を無期限に外部送信することを唯一の方式とする。
イ．エッジで人数を推定し、必要な集計値のみ送信して生映像の外部送信を最小化する。
ウ．クラウドへ送る前のデータ内容を把握しない。
エ．個人情報が含まれてもアクセス制御を行わない。

答え・解説 正答：イ

ア：必要以上のデータ処理になる。
イ：目的に必要なデータだけを外部へ送ると通信量とプライバシーリスクを同時に減らせる。
ウ：リスク評価できない。
エ：漏えいリスクが高い。
総合解説：目的に必要なデータだけを外部へ送ると通信量とプライバシーリスクを同時に減らせる。 この問題では「Edge Privacy」として、プライバシーと帯域の観点からエッジでデータ最小化できる。

対象：2026年度 / 基準日 2026-09-02

0129 4-5 IoT・プラットフォーム > エッジ・クラウド連携 ｜ 難易度：応用

制御判断は50ms以内が必要だが、クラウド往復遅延は通常80ms、エッジ処理は20msである。長期学習処理は数分掛かってもよい。適切な分担はどれか。

ア．50ms制御を必ずクラウドだけで行う。

イ．学習処理を全て小型端末へ固定し資源を評価しない。

ウ．リアルタイム判断をエッジへ置き、長期的な学習・集約分析をクラウドへ配置する。

エ．遅延要件を測定しない。

答え・解説 正答：ウ

ア：通常往復遅延だけで期限を超える。

イ：計算資源制約を無視している。

ウ：要求時間に応じて処理を配置すると、低遅延制御と大規模分析を両立できる。

エ：分担判断の根拠を失う。

総合解説：要求時間に応じて処理を配置すると、低遅延制御と大規模分析を両立できる。 この問題では「Edge/Cloud Partition」として、エッジ・クラウド分担を遅延と帯域の定量値から判断できる。

対象：2026年度 / 基準日 2026-09-02

0130 4-5 IoT・プラットフォーム > エッジ・クラウド連携 ｜ 難易度：応用

クラウド接続断が1時間続く可能性がある設備監視システムで、ローカル警報は継続し、復旧後に履歴を同期したい。最も適切な構成はどれか。

ア．クラウド断中は全監視を停止する。

イ．履歴を保存せず復旧時に推測する。

ウ．復旧後に順序や重複を確認せず全データを無条件処理する。

エ．警報判定をエッジで継続し、履歴をローカル保存し、再接続後に時刻・連番を使ってクラウドへ再同期する。

答え・解説 正答：エ

ア：継続要求を満たさない。

イ：データ完全性を失う。

ウ：重複・順序逆転の問題が起こり得る。

エ：クラウド非依存の最低限機能とStore-and-forwardを組み合わせることで可用性を確保できる。

総合解説：クラウド非依存の最低限機能とStore-and-forwardを組み合わせることで可用性を確保できる。 この問題では「Cloud Outage Resilience」として、クラウド障害時の縮退運転と再同期を含めた連携設計ができる。

対象：2026年度 / 基準日 2026-09-02

0131 4-5 IoT・プラットフォーム > IoTアーキテクチャ・通信 ｜ 難易度：基礎

MQTTの基本通信モデルとして正しいものはどれか。

ア．PublisherがTopicへメッセージを送り、Brokerが該当TopicのSubscriberへ配送する。
イ．すべてのClientが互いのIPアドレスへ必ず直接送信する。
ウ．共有メモリだけを利用する。
エ．CANアービトレーションをそのままインターネットへ使用する。

答え・解説 正答：ア

ア：MQTTはBrokerを中心としたPublish/Subscribe型のメッセージングプロトコルである。
イ：Broker経由のPub/Subが基本である。
ウ：ネットワークプロトコルである。
エ：別の通信方式である。
総合解説：MQTTはBrokerを中心としたPublish/Subscribe型のメッセージングプロトコルである。 この問題では「MQTT基本」として、MQTTがBrokerを介したPublish/Subscribe方式であることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0132 4-5 IoT・プラットフォーム > IoTアーキテクチャ・通信 ｜ 難易度：基礎

MQTT QoS 1の配送特性として最も適切なものはどれか。

ア．必ず0回だけ配送される。
イ．少なくとも1回配送を目指すため、再送によって重複メッセージが届く可能性がある。
ウ．重複が絶対に発生しないExactly onceである。
エ．配送保証を一切行わないAt most onceである。

答え・解説 正答：イ

ア：QoS 1の説明ではない。
イ：MQTT QoS 1はAt least onceであり、受信側は重複を考慮する必要がある。
ウ：これはQoS 2の目標である。
エ：QoS 0の説明である。
総合解説：MQTT QoS 1はAt least onceであり、受信側は重複を考慮する必要がある。 この問題では「MQTT QoS」として、MQTT QoS 0・1・2の配送特性を区別できる。

対象：2026年度 / 基準日 2026-09-02

0133 4-5 IoT・プラットフォーム > IoTアーキテクチャ・通信 ｜ 難易度：基礎

CoAPの代表的な特徴として最も適切なものはどれか。

ア．大容量動画ストリーミング専用プロトコルである。
イ．必ずTCPだけを使用することを前提とする。
ウ．制約の大きいノードや低電力・損失ネットワーク向けに設計されたWeb転送プロトコルである。
エ．ファイルシステムAPIでありネットワーク通信には使えない。

答え・解説 正答：ウ

ア：主用途とは異なる。
イ：基本CoAPはUDPを利用する。
ウ：RFC 7252はCoAPをconstrained nodes/networks向けの専用Web transfer protocolとして定義する。
エ：アプリケーション層通信プロトコルである。
総合解説：RFC 7252はCoAPをconstrained nodes/networks向けの専用Web transfer protocolとして定義する。 この問題では「CoAP基本」として、CoAPが制約ノード・低電力損失ネットワーク向けのWeb転送プロトコルであることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0134 4-5 IoT・プラットフォーム > IoTアーキテクチャ・通信 ｜ 難易度：標準

温度センサが値を10分に1回だけPublishする。新たに接続した監視Clientへ次回Publishを待たず最新温度を届けたい。適した機能はどれか。

ア．QoSを必ず0にするだけ。
イ．Topic名を毎回ランダムに変える。
ウ．Brokerを使用しない。
エ．Retained Messageを利用する。

答え・解説 正答：エ

ア：最新状態の保存機能ではない。
イ：購読側が最新値を特定しにくくなる。
ウ：MQTTの基本構成を失う。
エ：RETAIN付きメッセージはBrokerがTopicの最新値として保持し、新規購読時に配送できる。
総合解説：RETAIN付きメッセージはBrokerがTopicの最新値として保持し、新規購読時に配送できる。 この問題では「MQTT Retain」として、MQTT retained messageが新規購読者へ最新状態を渡す用途に使えることを理解できる。

対象：2026年度 / 基準日 2026-09-02

0135 4-5 IoT・プラットフォーム > IoTアーキテクチャ・通信 ｜ 難易度：標準

MQTT QoS 1で「料金を100円加算する」コマンドを送ると、再送により同じメッセージが2回届く可能性がある。適切な設計はどれか。

ア．メッセージIDや取引IDを保存し、同一操作を二重適用しないよう冪等性を持たせる。

イ．受信した回数だけ必ず料金を加算する。

ウ．QoS 1では重複は原理上起こらないと仮定する。

エ．メッセージ識別情報を削除する。

答え・解説 正答：ア

ア：At least onceでは重複を前提に受信側で重複排除または冪等処理を設計する必要がある。
イ：再送で二重課金になる可能性がある。
ウ：仕様に反する。
エ：重複判定が困難になる。
総合解説：At least onceでは重複を前提に受信側で重複排除または冪等処理を設計する必要がある。 この問題では「Idempotent Consumer」として、QoS 1の重複を考慮して処理を冪等化できる。

対象：2026年度 / 基準日 2026-09-02

0136 4-5 IoT・プラットフォーム > IoTアーキテクチャ・通信 ｜ 難易度：標準

工場Aと工場Bの機器が同じMQTT Brokerを利用する。工場A機器がBの制御TopicへPublishできないようにしたい。適切な方策はどれか。

ア．全Clientへ#のPublish権限を与える。

イ．工場・機器ごとにTopic名前空間を設計し、Client認証情報に基づくPublish/Subscribe ACLを設定する。

ウ．認証だけ行いTopic権限は制御しない。

エ．工場名をTopicから隠せば認可不要とする。

答え・解説 正答：イ

ア：全Topicへ送信できてしまう。
イ：Topic構造と認可を対応付けることでテナント間の不正アクセスを制限できる。
ウ：認証済み主体の権限逸脱を防げない。
エ：Security by obscurityに過ぎない。
総合解説：Topic構造と認可を対応付けることでテナント間の不正アクセスを制限できる。 この問題では「MQTT Topic ACL」として、Topic設計と認可を組み合わせてデータ分離できる。

対象：2026年度 / 基準日 2026-09-02

0137 4-5 IoT・プラットフォーム > IoTアーキテクチャ・通信 ｜ 難易度：標準

移動通信が一時切断しても、再接続後に購読状態や未完了QoSメッセージを継続したい。MQTT 5.0で関連する設定はどれか。

ア．RETAINだけを設定すれば全Session Stateが永続化される。
イ．ClientIDを毎回ランダム変更する。
ウ．Clean StartとSession Expiry Intervalを要件に応じて設定する。
エ．切断時に必ず全状態を破棄する設定だけを使う。

答え・解説 正答：ウ

ア：Retained MessageとSession Stateは別である。
イ：同じSessionとして再接続しにくくなる。
ウ：MQTT 5.0ではSession Expiry Intervalにより切断後にSession Stateを保持する時間を指定できる。
エ：継続要求を満たさない。
総合解説：MQTT 5.0ではSession Expiry Intervalにより切断後にSession Stateを保持する時間を指定できる。 この問題では「MQTT Session State」として、MQTT Session Expiryを再接続時の状態継続へ利用できる。

対象：2026年度 / 基準日 2026-09-02

0138 4-5 IoT・プラットフォーム > IoTアーキテクチャ・通信 ｜ 難易度：標準

多数センサからBrokerへ非同期イベントを配信し、複数のSubscriberが同じイベントを受け取りたい。MQTTとCoAPのうち一般に適する候補はどれか。

ア．必ずCoAPだけを使用しなければならない。
イ．ネットワークプロトコルを使わず共有RAMだけで全拠点を接続する。
ウ．通信パターンを確認せずプロトコルを決める。
エ．Publish/Subscribeを直接サポートするMQTTを優先候補として評価する。

答え・解説 正答：エ

ア：要求次第でMQTTが適する。
イ：分散機器間では成立しない。
ウ：要件ベースの選定にならない。
エ：複数購読者へのイベント配送という通信パターンにMQTTのBroker型Pub/Subが適合しやすい。
総合解説：複数購読者へのイベント配送という通信パターンにMQTTのBroker型Pub/Subが適合しやすい。この問題では「MQTT/CoAP選定」として、通信プロトコルを機器資源・通信パターンから選択できる。

対象：2026年度 / 基準日 2026-09-02

0139 4-5 IoT・プラットフォーム > IoTアーキテクチャ・通信 ｜ 難易度：応用

1000台のセンサが1秒ごとに1KBのPayloadをクラウドへ送っており、回線帯域が不足している。改善として最も適切な方針はどれか。

ア．送信周期、データ圧縮・集約、イベント駆動化、Payloadサイズ、QoSを見直し必要情報量を削減する。

イ．端末数と送信量を計算せず回線不足を無視する。

ウ．同じデータを複数回重複送信する。

エ．必要データも全て破棄する。

答え・解説 正答：ア

ア：IoT通信では端末台数×頻度×データ量にプロトコルオーバヘッドも加わるため、全体トラフィックを設計する。

イ：輻輳を悪化させる。

ウ：帯域消費が増える。

エ：監視要件を満たさない。

総合解説：IoT通信では端末台数×頻度×データ量にプロトコルオーバヘッドも加わるため、全体トラフィックを設計する。 この問題では「IoT通信帯域設計」として、低帯域ネットワークでPayload・頻度・QoSの組合せを最適化できる。

対象：2026年度 / 基準日 2026-09-02

0140 4-5 IoT・プラットフォーム > IoTアーキテクチャ・通信 ｜ 難易度：応用

IoTクラウドでネットワーク再接続後に古いセンサイベントと新しいイベントが順不同で届くことがある。適切な処理はどれか。

ア．到着順が必ず発生順と同じと仮定する。

イ．イベント時刻・連番・一意IDを持たせ、用途に応じて順序復元、重複排除、期限切れ判定を行う。

ウ．イベント識別子を持たせない。

エ．古い制御イベントも時刻確認せず必ず実行する。

答え・解説 正答：イ

ア：再送・回線断で崩れる可能性がある。

イ：分散通信では遅延・再送・順序変化を前提にデータの鮮度と一意性を管理する必要がある。

ウ：重複や順序を判定しにくい。

エ：危険な古い指令を適用する可能性がある。

総合解説：分散通信では遅延・再送・順序変化を前提にデータの鮮度と一意性を管理する必要がある。 この問題では「Distributed Messaging Robustness」として、通信断・重複・遅延を前提にIoTメッセージ処理を設計できる。

対象：2026年度 / 基準日 2026-09-02

0141 4-5 IoT・プラットフォーム > プラットフォーム・再利用・HMI ｜ 難易度：基礎

AUTOSAR Classic Platformの最上位レベルのソフトウェア層構成として正しいものはどれか。

ア．BIOS、HTML、SQLだけ
イ．CPU、RAM、電源だけ
ウ．Application、Runtime Environment（RTE）、Basic Software（BSW）
エ．Sensor、Cloud、Browserだけ

答え・解説 正答：ウ

ア：AUTOSAR Classicの層構造ではない。
イ：ハードウェア構成要素でありソフトウェア層ではない。
ウ：AUTOSAR ClassicではアプリケーションとBSWの間をRTEが仲介する三層構造を基本とする。
エ：AUTOSARの標準層分類ではない。
総合解説：AUTOSAR ClassicではアプリケーションとBSWの間をRTEが仲介する三層構造を基本とする。この問題では「AUTOSAR Layers」として、AUTOSAR Classic PlatformのApplication・RTE・BSWの層構造を理解できる。

対象：2026年度 / 基準日 2026-09-02

0142 4-5 IoT・プラットフォーム > プラットフォーム・再利用・HMI ｜ 難易度：基礎

AUTOSAR ClassicのRTEの代表的な役割はどれか。

ア．MCUの電源電圧を生成する。
イ．全アプリケーションを一つのISRへ統合する。
ウ．通信データを必ずクラウドへ送る。
エ．Software Component間やApplicationとBSW間の通信を抽象化し、アプリケーションをハードウェア依存から分離する。

答え・解説 正答：エ

ア：ソフトウェア層の役割ではない。
イ：RTEの目的ではない。
ウ：AUTOSAR RTEの必須機能ではない。
エ：RTEはVirtual Function Bus概念を具体ECU上で実現し、SWCのポータブルな統合を支援する。
総合解説：RTEはVirtual Function Bus概念を具体ECU上で実現し、SWCのポータブルな統合を支援する。この問題では「AUTOSAR RTE」として、RTEがアプリケーションSWCを基本ソフト・ハードウェアから分離する役割を理解できる。

対象：2026年度 / 基準日 2026-09-02

0143 4-5 IoT・プラットフォーム > プラットフォーム・再利用・HMI ｜ 難易度：基礎

ISO 9241-210の人間中心設計に沿う考え方として最も適切なものはどれか。

ア．利用者、タスク、利用環境を理解し、利用者を設計へ関与させ、反復的に評価・改善する。
イ．開発者の好みだけでUIを決定する。
ウ．ユーザー評価は製品廃棄後にだけ行う。
エ．HMIではハードウェアとソフトウェアの両方を考慮しない。

答え・解説 正答：ア

ア：人間中心設計は実利用状況とユーザー要求を基に対話システムを反復設計する。
イ：利用者ニーズを反映できない。
ウ：開発ライフサイクル中に反復評価する。
エ：双方が人間との相互作用へ影響する。
総合解説：人間中心設計は実利用状況とユーザー要求を基に対話システムを反復設計する。 この問題では「Human-Centred Design」として、人間中心設計が利用者・利用状況の理解から反復的に設計評価することを理解できる。

対象：2026年度 / 基準日 2026-09-02

0144 4-5 IoT・プラットフォーム > プラットフォーム・再利用・HMI ｜ 難易度：標準

同じアプリケーション機能を三種類のMCUへ展開したい。再利用性を高める方策として適切なものはどれか。

ア．上位アプリへ各MCUレジスタアドレスを直接埋め込む。
イ．MCU固有処理をMCAL/HAL等の下位層へ隔離し、上位機能は安定した共通APIを利用する。
ウ．MCUごとにアプリ全体をコピーして独立改造する。
エ．共通インタフェースを定義しない。

答え・解説 正答：イ

ア：移植性を低下させる。
イ：ハードウェア依存性を抽象化層へ閉じ込めると上位ソフトを複数ターゲットへ再利用しやすい。
ウ：重複コードと保守コストが増える。
エ：再利用境界が不明確になる。
総合解説：ハードウェア依存性を抽象化層へ閉じ込めると上位ソフトを複数ターゲットへ再利用しやすい。 この問題では「Platform API Reuse」として、標準化されたプラットフォームAPIで派生製品間の再利用性を高められる。

対象：2026年度 / 基準日 2026-09-02

0145 4-5 IoT・プラットフォーム > プラットフォーム・再利用・HMI ｜ 難易度：標準

複数製品で共通利用する診断コンポーネントを配布する。再利用時に必要な情報として最も適切なものはどれか。

ア．ソースファイル名だけ。
イ．開発者の口頭説明だけ。
ウ．必要OS機能、メモリ量、API、設定パラメータ、依存ライブラリ、対応版、制約条件。
エ．依存ライブラリ版を記録しない。

答え・解説 正答：ウ

ア：統合条件を判断できない。
イ：再現性が低い。
ウ：再利用側が適合性と統合方法を判断できるよう前提と依存を明示する必要がある。
エ：互換性問題を起こしやすい。
総合解説：再利用側が適合性と統合方法を判断できるよう前提と依存を明示する必要がある。 この問題では「Reusable Component Contract」として、再利用コンポーネントの設定・依存関係を明示して適用可能性を判断できる。

対象：2026年度 / 基準日 2026-09-02

0146 4-5 IoT・プラットフォーム > プラットフォーム・再利用・HMI ｜ 難易度：標準

運転支援画面で安全上重要な「ブレーキ異常」が、広告通知と同じ小さな表示で埋もれている。改善として適切なものはどれか。

ア．全通知を完全に同じ優先度で表示する。
イ．安全警報を設定画面の奥へ隠す。
ウ．警報発生時も画面表示を更新しない。
エ．重要度に応じて視覚・聴覚的優先度を付け、利用者が迅速に認識し行動できる表示へ設計する。

答え・解説 正答：エ

ア：重要警報が見落とされやすい。
イ：迅速な認識を妨げる。
ウ：利用者へ状態を伝えられない。
エ：HMIでは情報の重要性と利用状況を考慮し、必要なフィードバックを適切に提示する必要がある。
総合解説：HMIでは情報の重要性と利用状況を考慮し、必要なフィードバックを適切に提示する必要がある。 この問題では「Alarm HMI」として、HMIで重要警報の可視性と優先度を確保できる。

対象：2026年度 / 基準日 2026-09-02

0147 4-5 IoT・プラットフォーム > プラットフォーム・再利用・HMI ｜ 難易度：標準

ユーザーが「非常停止解除」ボタンを押しても、受付成功・失敗が画面上で分からない。改善として適切なものはどれか。

ア．操作受付、処理中、成功・失敗、現在状態を明確にフィードバックする。
イ．結果を一切表示しない。
ウ．成功・失敗に関係なく常に成功表示する。
エ．ボタンを押すたびランダムな画面へ移動する。

答え・解説 正答：ア

ア：対話システムはユーザーが操作結果とシステム状態を理解できるフィードバックを提供すべきである。
イ：誤操作や重複操作を招きやすい。
ウ：状態認識を誤らせる。
エ：予測可能性を損なう。
総合解説：対話システムはユーザーが操作結果とシステム状態を理解できるフィードバックを提供すべきである。 この問題では「Interaction Feedback」として、HMI操作後のフィードバックでユーザーの操作結果認識を支援できる。

対象：2026年度 / 基準日 2026-09-02

0148 4-5 IoT・プラットフォーム > プラットフォーム・再利用・HMI ｜ 難易度：標準

共通プラットフォームの通信APIを変更すると20製品へ影響する。適切な管理はどれか。

ア．全製品へ予告なしで即時破壊的変更を適用する。
イ．API版と互換性方針を管理し、影響製品を特定して移行期間・回帰テストを計画する。
ウ．API仕様書を更新しない。
エ．影響製品を記録しない。

答え・解説 正答：イ

ア：大量の統合不具合を招く。
イ：共通基盤の変更は再利用範囲が広いほど波及が大きいため、版管理と変更影響分析が重要である。
ウ：利用側が新契約を把握できない。
エ：変更漏れを追跡できない。
総合解説：共通基盤の変更は再利用範囲が広いほど波及が大きいため、版管理と変更影響分析が重要である。 この問題では「Platform Versioning」として、プラットフォーム更新で互換性と派生製品への影響を評価できる。

対象：2026年度 / 基準日 2026-09-02

0149 4-5 IoT・プラットフォーム > プラットフォーム・再利用・HMI ｜ 難易度：応用

走行中に重要設定を変更するため、深い5階層メニューで10回以上の操作が必要で、運転者の視線移動が長い。改善方針として最も適切なものはどれか。

ア．メニュー階層をさらに増やす。

イ．ユーザビリティ評価を行わない。

ウ．利用状況を分析し、走行中に必要な操作を簡略化・制限し、重要機能へのアクセスとフィードバックを人間中心に再設計する。

エ．全設定を走行中でも無制限に変更可能にする。

答え・解説 正答：ウ

ア：認知・操作負荷を高める。

イ：実利用時の問題を発見できない。

ウ：安全に関わるHMIでは操作時間、注意負荷、誤操作の可能性を実利用条件で評価する必要がある。

エ：注意散漫や誤操作リスクを増やす可能性がある。

総合解説：安全に関わるHMIでは操作時間、注意負荷、誤操作の可能性を実利用条件で評価する必要がある。 この問題では「HMI Safety Usability」として、安全クリティカルHMIで操作負荷と誤操作リスクを評価できる。

対象：2026年度 / 基準日 2026-09-02

0150 4-5 IoT・プラットフォーム > プラットフォーム・再利用・HMI ｜ 難易度：応用

10製品で共通プラットフォームを使うが、通信方式・センサ数・UI言語が製品ごとに異なる。最も適切なアーキテクチャはどれか。

ア．製品ごとに全ソースをコピーし独立改造する。

イ．全製品の差異を一つの巨大if文だけで無制限追加する。

ウ．可変条件を文書化しない。

エ．共通機能をプラットフォームへ集約し、差分は設定・プラグイン・抽象インタフェースなど明示的なVariation Pointで扱う。

答え・解説 正答：エ

ア：重複と派生差分管理が増大する。

イ：保守性とテスト性が低下する。

ウ：構成組合せと適用範囲を管理できない。

エ：共通部と可変部を分離するとコード複製を抑えつつ派生製品へ対応できる。

総合解説：共通部と可変部を分離するとコード複製を抑えつつ派生製品へ対応できる。 この問題では「Platform Variability」として、プラットフォーム再利用と製品固有要求の境界を設計できる。

対象：2026年度 / 基準日 2026-09-02