

以下の論文は、ChatGPT をカスタマイズした「技術士二次試験三上塾 AI 論文作成ツール」が作成した「概要論文」なので、一般的な合格論文と異なります。

勉強の進め方としては、以下の資料を元に論文の方向性を掴みつつ、概要表や出典などを参考に以下の概要論文を修正すると短時間で効率的な勉強ができます。以下の出典の URL をクリックしてもサイトが表示されない場合は、出典名をネット検索してください。

以下の論文では、観点と課題を章の最初に書いていますが、課題などを最後に書きたい場合は、テンプレート（プロンプト）を変更すれば最後に書くことが可能です。

設問は以下のサイトか日本技術士会のサイトをご覧ください。

https://www.engineer.or.jp/c_categories/index02022.html

=====

以下では、「**選択科目Ⅲ論文作成マニュアル**」の考え方、特に「**観点→技術課題→解決策→リスク→対策**」の因果関係を軸に整理します。同マニュアルでは、選択科目Ⅲは「問題解決能力及び課題遂行能力」を問うものであり、専門的学識、問題解決、評価、コミュニケーション等を意識する必要があります。

今回の問題は、**屋外 IoT だからこそ発生する制約を、情報基盤の専門技術でどう克服し、作業者の安全という社会目的につなげるかが核心です。**

1. 設問のテーマの社会目的

社会目的は、

人員不足や過酷な屋外作業環境の中でも、IoT を活用して作業者の異常を早期に検知・通知し、労働災害の防止と安全な作業環境を実現すること

です。

特に現在は熱中症対策との関連が強いテーマです。厚生労働省によれば、令和 6 年の職場での熱中症による休業 4 日以上死傷災害は 1,195 人で調査開始以来最多となりました。また、2025 年 6 月施行の改正労働安全衛生規則では、一定の暑熱作業について報告体制の整備等が求められています。さらに厚労省は、対策例としてウェアラブルデバイスも挙げ

る一方、それだけでは状態を正確に把握できない場合があるため、他の方法との組合せを推奨しています。(厚生労働省)

したがって、単なる「IoT を作る問題」ではなく、

安全管理を目的とするミッションクリティカルな屋外 IoT 基盤をどう成立させるか

という問題として捉えるべきです。

2. 出題者の意図

選択科目Ⅲでは、社会的ニーズや技術進歩によって生じる複合的問題を把握し、多様な視点から分析して、問題解決のための課題と遂行方策を論理的・合理的に説明する能力が問われます。

今回の出題意図は、主に次の4点です。

第一に、**屋内 IoT と屋外 IoT の違いを認識できるか**です。特に設問には「屋内にはない」「有線ネットワークを引けないなどの屋外での制約」と明記されています。

第二に、**情報基盤の専門家として多面的に課題を抽出できるか**です。単に「通信が不安定」「電池が不足」などの問題を書くのではなく、それを解決方向に転換して「通信可用性の確保」「電源自律性の確保」などの技術課題として表現する必要があります。マニュアルでも、「課題のところに解決策を書かない」「課題抽出過程には問題発生要因・制約要因や根拠を書く」とされています。

第三に、**最重要課題について専門技術を使って具体的に解決できるか**です。

第四に、**解決策を入れれば終わりではなく、その解決策によって新しく生じるリスクを予測し、さらに対策できるか**です。

3. 重要な箇所と注意すべき箇所

最重要ワードは、**「屋内にはない」「屋外」「IoT システム全体の構成」「多面的な観点」「情報基盤」「すべての解決策を実行しても新たに生じうるリスク」**です。

特に注意したいのは、課題を一般的な安全管理論にしないことです。

たとえば、

「人手不足の解消」
「熱中症の防止」
「作業教育の充実」

だけでは、情報基盤の技術課題として弱くなります。

そこで、

通信 → 電源・耐環境 → 安全監視の信頼性

という異なる技術的観点から 3 課題を設定します。

また、「通信環境が悪いことが課題」のように問題を課題として書かないことも重要です。マニュアルの考え方では、「観点」の一部を満たすものが「課題」、さらに課題の一部を満たすものが「解決策」です。

4. 論文作成上のポイント

この問題では、最初に IoT システムを具体化すると、その後が非常に書きやすくなります。

私は、

**ウェアラブルセンサ → 無線アクセス → エッジゲートウェイ → インターネット/VPN
→ クラウド IoT 基盤 → 安全管理ダッシュボード**

と設定します。

センサは心拍、皮膚温、加速度、GNSS、環境側の WBGT 等を対象とします。

そのうえで、論理を、

現状・制約 → 観点 → 技術課題 → 最重要課題 → 解決策 3 つ → 解決策によって新たに生じるリスク → 対策

と一直線につなげます。

マニュアルでも骨子表は文章を書きやすくするだけでなく、論理関係を確認するために作成し、「対策⇒リスク⇒解決策⇒課題⇒現状」と逆方向に「なぜなら」で確認する方法が示されています。

5. 不合格者と合格者の思考の違い

項目	不合格になりやすい思考	合格答案につながる思考
テーマ理解	IoT について知っていることを書く	「屋外×安全管理×情報基盤」の交点を探す
システム構成	センサを付けてクラウドへ送る	端末・無線・エッジ・クラウド・監視まで全体設計する
屋外条件	屋内 IoT とほぼ同じ	圏外、遮蔽、移動、電源、雨水、温度等を制約条件にする
課題 1	電波が弱い	通信可用性の確保
課題 2	バッテリーが足りない	電源自律性・耐環境性の確保
課題 3	誤検知がある	安全監視の信頼性向上
解決策	5G を使う	マルチアクセス＋エッジ＋Store & Forward 等を組み合わせる
リスク	サイバー攻撃がある	解決策を導入した結果、新しく増える攻撃面を考える
全体思考	キーワードの羅列	現状→課題→解決策→リスク→対策を因果で接続

6. 概要表

項目	内容
設問の概要 (現状・問題)	人員不足、暑熱等の過酷な屋外環境で作業者の安全確保が必要。一方、屋外では有線敷設困難、無線品質変動、電源制約、雨水・粉塵・高低温等があり、安全監視 IoT には高い可用性・信頼性が必要。
想定した IoT システム全体の構成	作業者のウェアラブル端末で心拍・皮膚温・加速度・GNSS 等を取得し、WBGT 等の環境センサと合わせて BLE/LPWA/セルラー等でエッジ GW へ送信。GW で異常判定し、5G/LTE 等から VPN 経由でクラウド IoT 基盤へ送る。クラウドで時系列蓄積・分析し、安全管理者のダッシュボード及びスマートフォンへ警報する。
課題①：通信可用性の確保	観点：無線通信品質変動への対応。屋外では地形、建造物、移動、基地局との位置関係等で電波状態が変化する。このため、安全情報を途絶させない通信可用性の確保が課題である。
課題②：電源自律性・耐環境性の確保	観点：屋外設備の継続運用。商用電源が得られない場所があり、端末は降雨、粉塵、高低温、直射日光にも曝される。このため、省電力化と耐環境化による継続稼働の確保が課題である。

項目	内容
課題③：安全監視の信頼性向上	観点：異常検知精度。ウェアラブルの装着状態、個人差、運動、外気条件等でセンサ値が変動する。誤検知・見逃しは安全性を損なうため、複数データを用いた安全監視の信頼性向上が課題である。
最重要課題	通信可用性の確保。理由は、通信が途絶すれば異常を検知できても管理者へ伝達できず、作業者の生命・安全を守るというシステム目的そのものを達成できないため。
解決策①	マルチアクセス通信の導入。5G/LTE、LPWA等を現場条件に応じて組み合わせ、マルチキャリアや通信経路の冗長化、自動フェイルオーバーを行う。
解決策②	エッジコンピューティングの導入。GWで閾値判定等を行い、クラウドとの通信断でも現場で警報する。通信断時はデータをローカル保存し、復旧後にStore & Forwardで再送する。
解決策③	QoSを考慮したデータ伝送制御。緊急警報を最優先とし、平常時ログ等は低優先度化する。送信周期、データ量を動的制御し、帯域が限られる状況でも安全情報を優先する。
リスク	マルチアクセス化、エッジGW、クラウド接続によって接続点・機器・ソフトウェアが増加し、攻撃対象領域が拡大する。GW乗っ取り、偽装端末接続、盗聴・改ざん等により、虚偽の安全情報や警報停止が生じるリスク。
対策	ゼロトラストの考え方にに基づき、端末固有証明書による相互認証、TLS/VPNによる通信暗号化、最小権限、Secure Boot、署名付きOTA更新を行う。さらにSBOMによる脆弱性管理、ログ監視、異常通信検知、鍵失効・交換を実施し、ライフサイクル全体でセキュリティを維持する。

マニュアルが示すように、骨子表では情報を詰め込み過ぎず、現状・課題・解決策・リスク・対策の論理関係が見えることを優先しています。

参考出典

1. 厚生労働省「労働安全衛生規則の一部を改正する省令の施行等について（令和7年5月20日 基発0520第6号）」 [厚生労働省・施行通達](#)（厚生労働省）
2. 厚生労働省「職場における労働衛生対策」 [厚生労働省・熱中症予防対策](#)（厚生労働省）
3. IPA「IoT開発におけるセキュリティ設計の手引き」 [IPA・IoTセキュリティ設計の手引き](#)（情報処理推進機構）
4. IPA「つながる世界の開発指針～安全安心なIoTの実現に向けて開発者に認識してほしい重要ポイント～ 第2版」 [IPA・つながる世界の開発指針 第2版](#)（情報処理推進機構）
5. IPA「『つながる世界の開発指針』の実践に向けた手引き [IoT高信頼化機能編]」 [IPA・IoT高信頼化機能編](#)（情報処理推進機構）

6. IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」 [IPA・JC-STAR（情報処理推進機構）](#)
 7. IPA「制御システムのセキュリティリスク分析ガイド 第2版（2026年4月版）」
[IPA・制御システムのセキュリティリスク分析ガイド（情報処理推進機構）](#)
-

7. 1800文字程度の論文

以下は、ご指定の章立てをそのまま使った答案例です。

想定したIoTシステム全体の構成：作業者に心拍、皮膚温、加速度、GNSS等を計測するウェアラブル端末を装着させ、WBGT等の環境センサとともにデータを収集する。収集データはBLE、LPWA、5G/LTE等によりエッジGWへ送信し、VPN経由でクラウドIoT基盤へ連携する。クラウドで時系列データを蓄積・分析し、異常時には安全管理者のダッシュボード及びスマートフォンへ警報する。

1. 多面的な観点からの技術課題の抽出

1) 通信可用性の確保

無線通信品質変動への対応の観点で考えれば、安全情報を途絶させない通信可用性の確保が課題である。具体的には、屋外では有線ネットワークを敷設できない場所が多く、地形、建造物、作業者の移動等により電波の遮蔽やフェージングが発生する。また、山間部等ではセルラー網の圏外となる場合もある。通信断により異常情報を管理者へ通知できなければ、作業者の安全確保が困難となる。

2) 電源自律性・耐環境性の確保

屋外設備の継続運用の観点で考えれば、省電力化と耐環境化によるIoT機器の継続稼働の確保が課題である。具体的には、屋外では商用電源を利用できない場所があり、ウェアラブル端末やGWはバッテリーに依存する。また、降雨、粉塵、高低温、直射日光等に曝され、故障や電池性能低下が発生する。このため屋内以上に長時間かつ安定した自律運用が求められる。

3) 安全監視の信頼性向上

異常検知精度の観点で考えれば、複数データを活用した安全監視の信頼性向上が課題である。具体的には、ウェアラブルセンサは装着状態、作業強度、個人差、外気温等により測定値が変動する。このため、単一センサや固定閾値だけでは誤検知や見逃しが発生し、不要な作業中断又は重大事故につながるおそれがある。

2. 抽出した技術課題のうち最も重要と考える技術課題と解決策

私は「通信可用性の確保」が最も重要な課題と考える。理由は、通信が途絶すれば異常を検知しても管理者へ伝達できず、作業者の生命・安全を守るというシステム目的を達成できないからである。以下にその解決策を示す。

1) マルチアクセス通信の導入

複数の無線通信手段による通信経路の冗長化が重要である。具体的には、広帯域な 5G/LTE と、省電力・広域通信が可能な LPWA 等を現場条件に応じて組み合わせる。また、複数キャリアを利用可能な通信構成とし、受信電力、遅延、パケット損失率等を監視して通信品質が低下した場合は、自動フェイルオーバーにより経路を切り替える。

2) エッジコンピューティングの導入

クラウドとの通信断時にも安全監視を継続することが重要である。具体的には、エッジ GW で心拍、皮膚温、WBGT 等の閾値判定を行い、異常時は現場で即時警報する。また、通信断時はデータをローカルストレージに蓄積し、回線復旧後に Store & Forward 方式でクラウドへ再送する。これによりクラウド依存による単一障害点を低減する。

3) QoS を考慮したデータ伝送制御

限られた無線帯域を安全情報へ優先配分することが重要である。具体的には、転倒、熱中症兆候、SOS 等の緊急データを最高優先度とし、平常時の位置情報やログは優先度を下げる。また、回線品質に応じてセンサデータの送信周期やデータ量を動的に変更し、低帯域時にも緊急警報を確実に伝送する。

3. 解決策を実行しても新たに生じうるリスクと対策

1) リスク

リスクとしては、通信経路と IoT 機器の増加によるサイバー攻撃対象領域の拡大がある。具体的には、マルチアクセス化やエッジ GW の導入により接続点が増え、偽装端末の接続、通信の盗聴・改ざん、GW の乗っ取り等が生じる可能性がある。その結果、虚偽の安全情報が送信されたり、緊急警報が停止したりするおそれがある。

2) 対策

対策としては、ゼロトラストを基本とした多層防御がある。具体的には、端末固有の電子証明書による相互認証、TLS や VPN による通信暗号化、最小権限によるアクセス制御を行う。また、Secure Boot、署名付き OTA アップデート、SBOM を用いた脆弱性管理を行う。さらに、通信ログを継続監視して異常通信を検知し、侵害端末の証明書を速やかに失効させる。これらを設計・運用・廃棄まで継続し、安全監視 IoT のセキュリティと可用性を両立させる。

この答案で特に狙っているのは、**「屋外だから生じる問題」→「情報基盤としての課題」→「専門技術による解決」**を崩さないことです。また、最重要課題の理由は「公衆・作業者の安全重視」としています。マニュアルでも、最重要課題の理由として「効果重視」「順番重視」「公衆の安全重視」などの考え方が示されています。

さらに答案を強くするなら、次の添削段階では**「この答案を A 評価に近づけるため、課題 3 つ・解決策 3 つ・リスクの論理的つながりを採点者目線でチェックする」**のが効果的です。

上記の様に、自分の受験部門・受験科目のわかりやすい過去問解説や概要論文を作って効率的に勉強したいという方は、以下の「技術士二次試験三上塾 AI 論文作成プログラム」を参考にしてください。

<https://suninfo.co.jp/g2gpt/>

技術士二次試験 三上塾